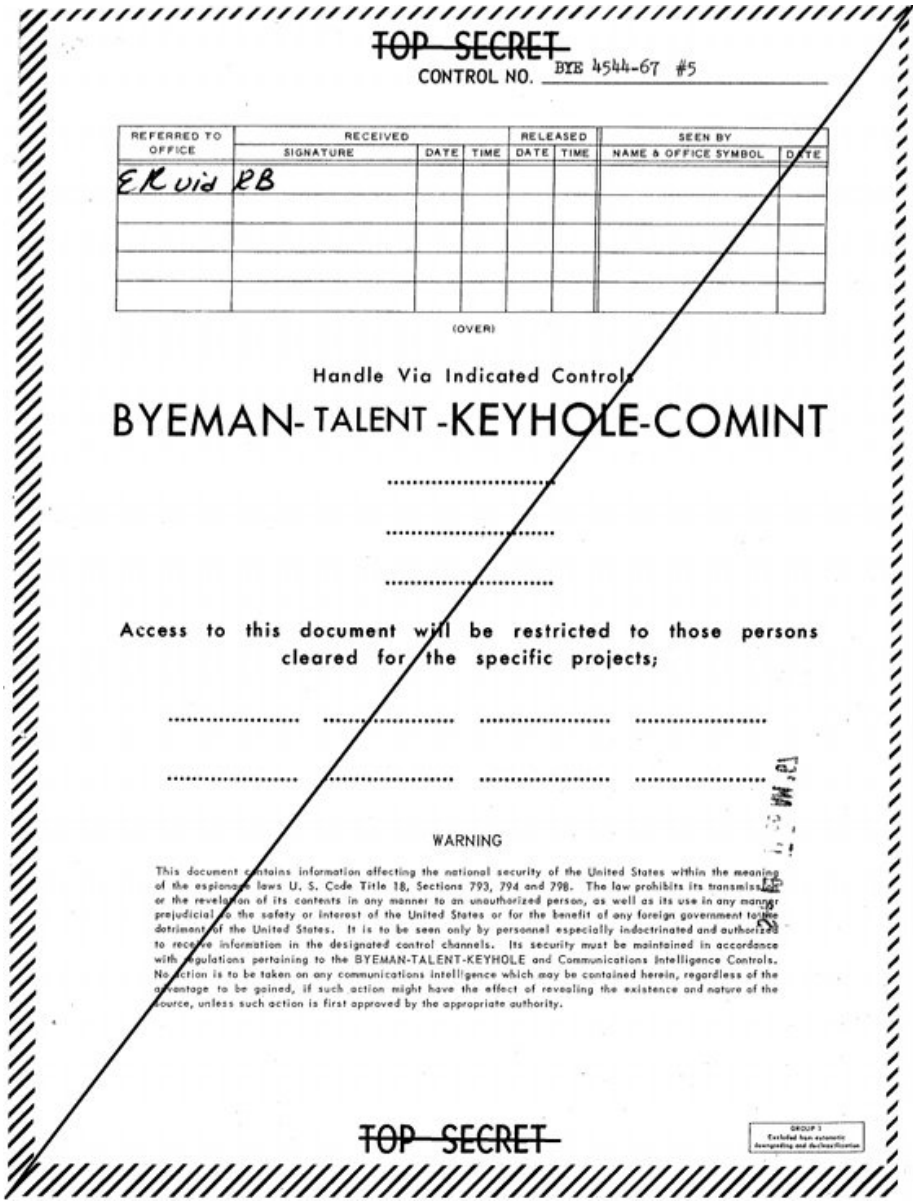
Codex Notitia

The Military Intelligence Process

A Compendium Of Source Material



~~TOP SECRET~~

CONTROL NO. BYE 4544-67 #5

REFERRED TO OFFICE	RECEIVED			RELEASED		SEEN BY	
	SIGNATURE	DATE	TIME	DATE	TIME	NAME & OFFICE SYMBOL	DATE
ER via RB							

(OVER)

Handle Via Indicated Controls

BYEMAN- TALENT -KEYHOLE-COMINT

.....

.....

.....

Access to this document will be restricted to those persons cleared for the specific projects;

....

....

WARNING

This document contains information affecting the national security of the United States within the meaning of the espionage laws U. S. Code Title 18, Sections 793, 794 and 798. The law prohibits its transmission or the revelation of its contents in any manner to an unauthorized person, as well as its use in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States. It is to be seen only by personnel especially indoctrinated and authorized to receive information in the designated control channels. Its security must be maintained in accordance with regulations pertaining to the BYEMAN-TALENT-KEYHOLE and Communications Intelligence Controls. No action is to be taken on any communications intelligence which may be contained herein, regardless of the advantage to be gained, if such action might have the effect of revealing the existence and nature of the source, unless such action is first approved by the appropriate authority.

~~TOP SECRET~~

GROUP 1
Excluded from automatic downgrading and declassification

Compiled And Edited By

David Childers

Creative Common License

This body of work is released under the Attribution-ShareAlike version 3.0, Creative Common License.

The work may be freely distributed or modified for commercial or non commercial purposes.

If this work is modified, compliance with the Attribution-ShareAlike version 3.0, Creative Common License is required.

These requirements include:

- Any derivatives of this work must be attributed to David Childers.

- Any derivatives of this work must reference any additional sources that may be used.

- Alterations, transforming, or building upon this work requires distributing the resulting work only under the same, similar or a compatible license.

For the complete legal code, please refer here:
http://www.creativecommons.org/licenses/by-sa/3.0/legalcode

United States Government Publications

Title 17 USC §105, Subject matter of copyright: United States Government works, provides that "Copyright protection is not available for any work of the United States Government," defined in Title 17 USC §101, as "a work prepared by an officer or employee of the United States Government as part of that person's official duties." Therefore, only those works solely authored by US Federal Government employees are not protected by copyright in the United States.

Cover graphic
http://upload.wikimedia.org/wikipedia/commons/d/dd/SCI_cover_sheet_%281967%29.jpg

Foreword graphic
http://commons.wikimedia.org/wiki/File:Probably_Valentin_de_Boulogne_-_Saint_Paul_Writing_His_Epistles_-_Google_Art_Project.jpg

Foreword

Greetings,

Military Intelligence acquisition is the ability to identify an information need, prioritize the acquisition time table, identify source points for that information and use various methods to reduce the obscurity of ambiguous perceptions. This structured process will allow individuals to understand and arrive at a correct correlation based upon the available information.

It is imperative to clearly define the purpose of pursuing information, what type of information is to be sought and the sources for obtaining that information. This conceptualization will allow the most relevant information to be collected and an accurate reflection of the analytical process used to derive a precise answer for the desired questions that have been asked.

Information and data all have a story to tell, so the intelligence specialist must have the ability to understand the relevance of collected information and data in answering the questions being posed.

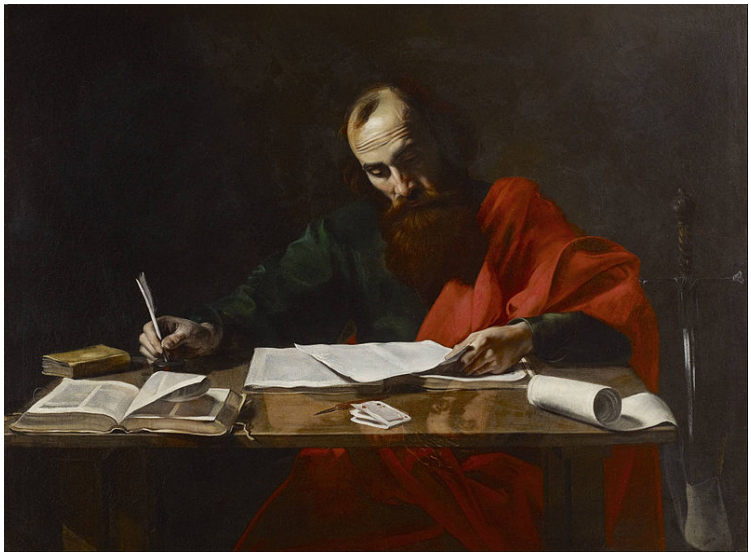
This work was inspired by the artist Madis and their track - Desert Of Lost Souls.

It is my sincere hope that the reader finds this publication useful.

David Childers

February 2018

www.scenictelevision.com



Scientia Ipsa Potentia Est

Other Publications by David Childers

Computer Operating System

FreeBSD Compact Guide

Debian Linux Desktop

Security

Cyber Security

Wireless Network Security

Multimedia Server Security Guide

Technical

Basic Internet Video Production Guide

SHOUTcast Audio And Video Streaming Guide

SHOUTcast Streaming Best Of Technical Support

Tips For Internet Broadcasters

Icecast Streaming Handbook

Internet Broadcasters Information Hndbk 5th Ed.

Linux Applications For Internet Broadcasters

Revenue

Internet Broadcaster Revenue Handbook

Effective Audio Commercials

Marketing

Broadcast Station Imaging

Creating An Effective Media Kit

Creating An Effective Newsletter

Broadcasters Promotion Handbook

Social Media Guide

Website

Website Development

Search Engine Optimization Guide

Audience

Understanding Your Audience

How To Mobilize Your Broadcast Audience

General

Competitive Intelligence For Broadcasters

Techniques For Information Research

Multimedia Influence Campaigns

Creative Commons Licensing For Broadcasters

Scenic Television is an Internet television station that presents the sights and sounds of nature 24 hours a day. Let us soothe and relax you wherever you are. Savor the tropical beaches of Puerto Rico or relax at a rain forest in Costa Rica. Meditate at the Danube River in Germany, or relish the view of Lake Zurich in Switzerland. We have scenic videos from locations all over the world.

Scenic Television originates from the Gulf coast of the United States and broadcasts to a global audience. The television broadcast is accessible on any device with an Internet connection. Such electronic devices include desktop computers, laptops, tablets, smartphones, game platforms, and Internet-connected televisions.

www.ScenicTelevision.com

Index

Fundamentals

MCDP 2 **Page 11**
Intelligence
U.S. Marine Corps

ADP 2-0 **Page 125**
Intelligence
U.S. Army

FM 2-0 **Page 211**
Intelligence
U.S. Army

Operational

MCWP 2-10 **Page 422**
Intelligence Operations
U.S. Marine Corps

FM 2-22.3 **Page 510**
Human Intelligence Collector Operations
U.S. Army

MCWP 2-2 **Page 894**
MAGTF Intelligence Collection
U.S. Marine Corps

Air Force Doctrine Document 2-9 **Page 970**
Intelligence, Surveillance, And Reconnaissance And Operations
U.S. Airforce

MCWP 2-4 **Page 1043**
Marine Air-Ground Task Force Intelligence Dissemination
U.S. Marine Corps

FM 11-30 **Page 1105**
Technical Intelligence
U.S. Army

FM 34-54 **Page 1150**
Technical Intelligence
U.S. Army

Analysis

Critical Thinking And Intelligence Analysis **Page 1341**
National Intelligence Defense College

AFH 14-133 **Page 1500**
Intelligence Analysis
U.S. Airforce

FM 34-3 Page 1604
Intelligence Analysis
U.S. Army

MCRP 2-10B.1 Page 2033
Intelligence Preparation of the Battlefield/Battlespace
U.S. Marine Corps

MCTP 2-10B Page 2246
MAGTF Intelligence Production and Analysis
U.S. Marine Corps

A Compendium of Analytic Tradecraft Notes Page 2526
Central Intelligence Agency

Psychology Of Intelligence Analysis Page 2585
Center For The Study Of Intelligence

Thinking and Writing: Page 2799
Cognitive Science and Intelligence Analysis
Center for the Study of Intelligence

A Tradecraft Primer: Page 2840
Structured Analytic Techniques for Improving Intelligence Analysis
Central Intelligence Agency

Intelligence Essentials For Everyone Page 2885
Joint Military Intelligence College

Radio Communications

MCWP 2-22 Page 2975
Signals Intelligence
U.S. Marine Corps

TM 32-250 Page 3099
Fundamentals Of Traffic Analysis (Radio-Telegraph)
U.S. Army

SubCourse IT0302 Page 3207
Edition C
Introduction To Radio Direction Finding
U.S. Army

TC 9-64 Page 3260
Communications-Electronics Fundamentals
Wave Propagation, Transmission Lines, and Antennas
U.S. Army

MCRP 8-10B.11 Page 3529
Antenna Handbook
U.S. Marine Corps

Imagery

Geospatial Intelligence (GEOINT) Basic Doctrine Page 3722
National System For Geospatial Intelligence

MCWP 2-15.4 Page 3770
Imagery Intelligence
U.S. Marine Corps

MCRP 2-10B.5 Page 3980
Imagery Intelligence
U.S. Marine Corps

FM 30-2 Page 4218
Military Intelligence
Role of Aerial Photography
United States Army

Imagery Intelligence (IMINT) Production Model Page 4323
U.S. Army

Forester's Guide To Aerial Photo Interpretation Page 4485
U.S. Department Of Agriculture

Aerial Photographs In Geologic Interpretation and Mapping Page 4534
U.S. Department Of The Interior

FM 21-25 Page 4771
Elementary Map And Aerial Photograph Reading
U.S. Army

FM 21-26 Page 4877
Advanced Map And Aerial Photograph Reading
U.S. Army

FM 30-10 Page 5072
Terrain Intelligence
U.S. Army

Cryptography

TM 32-220 Page 5255
Basic Cryptography
U.S. Army

Open Source

ATP 2-22.9 Page 5447
Open-Source Intelligence
U.S. Army

NATO Open Source Intelligence Handbook Page 5538
North Atlantic Treaty Organization

Open Source Intelligence **Page 5595**
Professional Handbook
Joint Military Intelligence Training Center

Open Source Intelligence Tools And Resources Handbook 2018 **Page 5913**
Creative Commons CC BY License
I Intelligence

Writing

Style Manual For Intelligence Production **Page 6240**
Defense Intelligence Agency

Style Manual & Writers Guide For Intelligence Publications **Page 6477**
Central Intelligence Agency

Reference

FM 34-8-2 **Page 6667**
Intelligence Officers Handbook
U.S. Army

Directors Reading List 2018 **Page 6879**
Defence Intelligence Agency

Joint Publication 1-02 **Page 6939**
Dictionary of Military and Associated Terms
U.S. Department of Defense

ST 2-50.4 (FM 34-8) **Page 7421**
Combat Commanders Handbook On Intelligence
U.S. Army

Historical

The Most Secret War **Page 7496**
Army Signals Intelligence In Vietnam
U.S. Army

Pub 60 13-1 **Page 7644**
Intelligence
U.S. Army

Pub 70 43 **Page 8195**
U.S. Army Signal Intelligence In WW2
U.S. Army

Additional publications which are noteworthy that cannot be included in the compilation. These publications require a download. (Free to download)

Monitoring Border Conflicts with Satellite Imagery:
A Handbook for Practitioners
https://www.aaas.org/resources/monitoring-border-conflicts-satellite-imagery-handbook-practitioners

Satellite Imagery Interpretation Guide: Displaced Population Camps
Free PDF File Download
https://hhi.harvard.edu/publications/satellite-imagery-interpretation-guide-displaced-population-camps

Satellite Imagery Interpretation Guide: Intentional Burning of Tukuls
Free PDF File Download
https://hhi.harvard.edu/publications/satellite-imagery-interpretation-guide-intentional-burning-tukuls

Imagery Interpretation Guide: Assessing Wind Disaster Damage to Structures
Free PDF File Download
https://hhi.harvard.edu/publications/satellite-imagery-interpretation-guide-assessing-wind-disaster-damage-structures

Radio Monitoring: A How To Guide
Free PDF File Download
http://www.naswa.net/journal/areybook

MCDP 2

Intelligence

U.S. Marine Corps

DISTRIBUTION STATEMENT A:Approved for public release; distribution is unlimited

PCN 142 000005 00

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380-1775

7 June 1997

FOREWORD

Marine Corps Doctrinal Publication (MCDP) 2, *Intelligence*, describes the theory and philosophy of intelligence as practiced by the United States Marine Corps. It provides Marines a conceptual framework for understanding and conducting effective intelligence activities. The Marine Corps' view of intelligence is based on our common understanding of the nature of war and on our warfighting philosophy as described in MCDP 1, *Warfighting*.

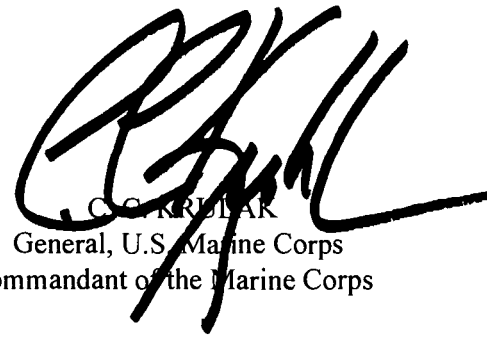
Intelligence discusses the effective use of knowledge about the enemy and the environment in support of military decisionmaking. *Intelligence* acknowledges that uncertainty pervades the battlefield and that our best intelligence efforts can only reduce, not eliminate, uncertainty.

One of the main aims of this manual is to put intelligence into its proper context in relation to other activities of warfighting. The Marine Corps views intelligence as a fundamental component of command and control that is inseparable from operations. The general concepts which apply to effective command and control apply equally to intelligence. This publication, therefore, presumes familiarity with MCDP 6, *Command and Control*, which establishes fundamental doctrine for command and control.

MCDP 2, *Intelligence*, does not supersede any current doctrinal publication. It provides the authoritative basis for the subsequent development of intelligence doctrine, education, training, equipment, procedures, and organization. *Intelligence* affords no specific techniques or procedures for intelligence activities; rather, it offers broad guidance which requires judgment in its application. Other publications in the intelligence series of Marine Corps warfighting publications provide specific tactics, techniques, and procedures.

Marine Corps intelligence doctrine applies across the full spectrum of conflict, from peacekeeping or humanitarian assistance operations on the one hand to general war on the

other. Furthermore, this publication pertains equally to small-unit leaders and senior commanders. Since intelligence is an essential component of any military activity, this manual is meant to guide Marines at all levels of command in both the operating forces and the supporting establishment.



C. C. KRULAK
General, U.S. Marine Corps
Commandant of the Marine Corps

DISTRIBUTION: 142 000005 00

© 1997 United States Government as represented by the Secretary of the Navy. All rights reserved.

Intelligence

Chapter 1. The Nature of Intelligence

How Important Is Intelligence?—The Objectives of Intelligence—Intelligence as Knowledge—Intelligence as a Process—Why the Mystery?—What Makes Intelligence Different?—Expectations of Intelligence—Intelligence in the Information Age—A Case Study: Desert Storm 1990–1991—Conclusion

Chapter 2. Intelligence Theory

What Do We Want to Know About the Enemy?—Characteristics of Good Intelligence—Classes of Intelligence—Capabilities Versus Intentions—Signals and Noise—Levels of Intelligence—Intelligence Requirements—Sources of Intelligence—Functions of Intelligence—Security—The Intelligence Cycle—A Case Study: Vietnam 1972—Conclusion

Chapter 3. Creating Effective Intelligence

The Challenge to Intelligence—Intelligence Is a Command Responsibility—The Command-Intelligence Connection—The Intelligence-Operations Connection—

Intelligence as a Team Effort—Intelligence Is a Product, Not a Provision—A Balanced Approach—Focusing the Intelligence Effort—Generating Tempo Through Intelligence—Intelligence Education and Training—A Case Study: Somalia 1992–1993—Conclusion

Notes

Chapter 1

The Nature of Intelligence

"And therefore I say: Know the enemy, know yourself; your victory will never be endangered. Know the ground, know the weather; your victory will then be total."[1]

—Sun Tzu, *The Art of War*

"For the whole reason-for-being of all military intelligence personnel is to facilitate accomplishment of the mission, and to save lives. When they fail, all the wrong people are hurt."[2]

—Stedman Chandler and Robert W. Robb,
Front-Line Intelligence

To develop effective intelligence, we must first understand its fundamental nature—its purpose and characteristics as well as its relationship to command and operations. This understanding will become the basis for developing a theory and practical philosophy for intelligence.

HOW IMPORTANT IS INTELLIGENCE?

Maneuver warfare requires a firm focus on the enemy. It aims at taking action which avoids enemy strengths and exploits enemy critical vulnerabilities. The identification of these strengths and vulnerabilities is crucial. Maneuver warfare requires acting in a manner to deceive and then striking at a time and place which the enemy does not expect and for which he is not prepared. Identification of an adversary's expectations and preparations is also important. Maneuver warfare requires decision and action based on situational awareness—a keen understanding of the essential factors which make each condition unique—rather than on preconceived schemes or techniques. How is this situational awareness gained?

Accurate and timely intelligence—knowledge of the enemy and the surrounding environment—is a prerequisite for success in war. Certainly, maneuver warfare places a heavy

emphasis on the judgment of leaders at all levels. Nonetheless, judgment, even genius, cannot substitute for good intelligence. Genius may make better sense of available information, and it may provide superior and faster use of the knowledge it gains from that information, but no commander—no matter how brilliant—can operate effectively without good intelligence. A brilliant commander, Field Marshal Erwin Rommel, proclaimed that, "It is not that one general is more brilliant or experienced than the other; it is a question of which general has a better appreciation of the battlefield."[3]

Intelligence, therefore, is at once inseparable from both command and operations. Intelligence contributes to the exercise of effective command during military operations and helps ensure the successful conduct of those operations. By identifying enemy weaknesses susceptible to attack, intelligence also serves as an important element of combat power.

Effective intelligence in the hands of capable commanders has often provided decisive advantages of tactical, operational, and strategic importance. The Battle of Midway in June 1942 was won by a vastly outgunned and outnumbered American fleet because its commanders had received, recognized, and acted upon detailed and accurate intelligence. In 1986, during air strikes conducted in response to Libya's terrorist activity, intelligence provided the detailed understanding of the Libyan air defense system that enabled Marine and Navy aviators to effectively shut it down. Intelligence's identification of critical vulnerabilities in Iraqi air and ground

defenses contributed to the rapid and thorough defeat of Iraqi forces during Operation Desert Storm.

THE OBJECTIVES OF INTELLIGENCE

Understanding the relationship between intelligence and command and control is key to understanding the role of intelligence. Command and control is about making and executing decisions. The main purpose of intelligence is to support the decisionmaking process.

Intelligence strives to accomplish two objectives. First, it *provides accurate, timely, and relevant knowledge about the enemy (or potential enemy) and the surrounding environment.* In other words, the primary objective of intelligence is to support decisionmaking by reducing uncertainty about the hostile situation to a reasonable level—recognizing, of course, that the fog of war renders anything close to absolute certainty impossible.

In achieving its primary objective, intelligence performs four related tasks. First, it identifies and evaluates existing conditions and enemy capabilities. Second, based upon those existing conditions and capabilities, it estimates possible enemy courses of action, providing insight into possible future actions. Third, it aids in identifying friendly vulnerabilities

the enemy may exploit. Finally, intelligence assists in the development and evaluation of friendly courses of action based on the results of the first three tasks.

The second intelligence objective is that it *assists in protecting friendly forces through counterintelligence*. Counterintelligence includes both active and passive measures intended to deny the enemy valuable information about the friendly situation. Counterintelligence also includes activities related to countering hostile espionage, subversion, and terrorism. Counterintelligence directly supports force protection operations by helping the commander deny intelligence to the enemy and plan appropriate security measures.

The two intelligence objectives demonstrate that intelligence possesses both positive—or exploitative—and protective elements. It uncovers conditions which can be exploited and simultaneously provides warning of enemy actions. Intelligence thus provides the basis for our own actions, both offensive and defensive.

INTELLIGENCE AS KNOWLEDGE

Although the objectives of intelligence have been discussed, the term *intelligence* has not been defined. Very simply, intelligence is knowledge—knowledge about the enemy or the

surrounding environment[4] needed to support decisionmaking. Since people understand situations best as images—mental pictures—intelligence aims to create an accurate or meaningful image of the situation confronting a commander. Good intelligence paints a picture—or more accurately, several pictures—of possible realities.[5]

Not all knowledge which goes into military decisionmaking qualifies as intelligence. Knowledge pertaining directly to the friendly situation or to the status of an ally does not constitute intelligence. Knowledge not pertaining directly to the friendly cause generally falls under the category of intelligence.

What do we mean by knowledge? In describing intelligence as knowledge, we are distinguishing intelligence from data or information.[6] Intelligence is developed from information, but it is important to recognize that *intelligence is not simply another term for information.* Information is unevaluated material of any kind—enemy prisoner of war interrogation reports, radio intercepts, reconnaissance reports, photographs—and represents the raw material from which intelligence is ultimately derived. Few pieces of information speak conclusively for themselves. They must be combined and compared with other pieces of information, analyzed, evaluated, and, finally, given meaning. Good intelligence does not simply repeat the information which a source reveals. Rather, it develops this raw material in order to tell us

what that information means and identifies the implications for decisionmaking. In other words, *intelligence is the analysis and synthesis of information into knowledge.* The end result is not more information, but knowledge that gives us a meaningful assessment of the situation.[7]

Since intelligence is derived from information, it shares many attributes of information. Information, and the intelligence which results from it, is perishable. Information will always be incomplete, sometimes confusing, and often contradictory. Not all information will be important or even relevant, and much of it may be inaccurate or misleading. Too much information can be as harmful as too little. With all information, we seek not a large amount, but to have the right information available when needed and in a useful form, and so it is with intelligence.

Finally, we note that knowledge does not exist for its own sake, but as the basis for action. We do not develop lengthy intelligence studies just because we have the ability to do so or because a subject is of academic interest. Intelligence that is not acted upon or that does not provide the potential for future action is useless.[8]

INTELLIGENCE AS A PROCESS

Intelligence should be thought of as not just a product—knowledge—but also the *process* which produces that knowledge. Intelligence is the process which identifies and evaluates existing conditions and capabilities, estimates possible enemy courses of action based upon these conditions and capabilities, and assists in the development and evaluation of friendly courses of action—all in support of the commander's decisionmaking.

Intelligence is thus a central component of the command and control process, which can be described by a simple model known as the observation-orientation-decision-action (OODA) loop. Intelligence activities make up a significant portion of the observation-orientation phases of the OODA loop with the primary purpose of supporting the decision phase. Intelligence also supports the action phase by identifying targets for attack and by assessing results, bringing the OODA loop full circle to the next observation phase in support of a subsequent decision.

Intelligence must not be construed as the exclusive province of intelligence specialists. Intelligence activities are driven by the need to answer questions crucial to the planning and execution of operations. Intelligence is inseparable from operations. Data collected during the course of operations is essential to the development of a timely and accurate intelligence picture. Above all, intelligence shapes (some would say drives) the decisions made during the conduct of operations. *All Marines involved in operations are involved in intelligence in one way or another, and all Marines involved in intelligence are involved in operations.*

WHY THE MYSTERY?

In the past, there has been a perception that intelligence is a highly specialized field shrouded in secrecy and isolated from other warfighting areas. Many misconceptions concerning intelligence have arisen; some even view it as the modern equivalent of wizardry. Why has this aura of mystery developed?

First, intelligence is usually much less concrete than knowledge of the friendly situation, which Marines are likely to know with much more certainty and detail. It is commonly understood that effective intelligence is an important factor—often *the* critical factor—in mission success or failure.

Isolating or measuring the specific effects of intelligence on the mission's outcome, however, is often difficult.

Second, intelligence employs specialized techniques to develop studies and products. Intelligence personnel receive certain specialized training—but hardly more than specialists in other fields. In the normal course of performing their mission, Marine intelligence sections request and receive support from specialized, technical, and sometimes highly compartmented national, theater, or service-level intelligence agencies. While these activities provide access to resources necessary to develop tactical intelligence, the activities themselves may be of limited interest to combat units. In addition, intelligence often involves highly specialized technology, especially in the collection of information.

Finally, to protect the value of a piece of intelligence as well the sources used in developing it, many intelligence products and methods are classified. Out of the legitimate concern for security, a need to know is a basic requirement for access to intelligence products. In order to protect the sensitive nature of some intelligence activities, elements of the intelligence section may be physically separated from other staff sections, with access to these elements being controlled. Unfortunately, the rightful concern over security contributes more to the mystification of intelligence than any other single factor.

The result is a veil of mystery that often surrounds intelligence activities. However, intelligence is not an obscure activity unrelated to other warfighting activities. In fact, intelligence is a central component of command and control, a fundamental responsibility of command, and inseparable from operations. All personnel involved in the conduct and support of operations—commanders, operations officers, logisticians, communicators, etc.—must understand intelligence just as intelligence personnel must comprehend the conduct and support of operations.

There is nothing mysterious about intelligence. While intelligence collection and production may involve the use of high-technology sensors and networks, good intelligence is primarily the result of solid headwork and legwork, not the output of some secret process or compartmented database. Good intelligence begins with commanders clearly identifying their intelligence concerns and needs. It is developed through the focused collection of information, thorough study, and, most importantly, effective analysis and synthesis. The result is an intelligence product that provides knowledge, reduces uncertainty, and supports effective decisionmaking.

WHAT MAKES INTELLIGENCE DIFFERENT?

We have noted that while intelligence uses specialized capabilities and techniques, this alone does not distinguish

intelligence from other command and control functions. What makes intelligence unique? The one feature which distinguishes intelligence from the other command and control functions is that *intelligence deals directly with an independent, hostile will personified by the enemy.* As such, intelligence deals with more unknowns and has less control over its environment than any other aspect of command and control.

A commander may well face unknowns about the friendly situation—uncertainty about the location, activity, or status of friendly forces. Presumably such uncertainty is not the result of a conscious effort on the part of those forces to deny that information to the commander. If commanders have questions about the friendly situation, they can usually obtain the answers directly from the principals involved. In other words, for nearly every question about the friendly situation, there is a reliable source ready to provide an answer.

This is not the case for questions concerning the enemy or the area of operations. Such information by its very nature will be significantly more difficult to obtain. The enemy will do his utmost to deny us knowledge of his capabilities, dispositions, methods, and intentions through the use of security measures and his own counterintelligence. He may intentionally present us with erroneous or ambiguous information. When a foe suspects that we know something significant about his situation, he will likely undertake actions to change that situation.

This is especially true at the tactical level of war. The closer a unit is to contact with the enemy, the greater attention it pays to security, camouflage, dispersion, and deception. Moreover, once execution begins, the rapidity of changes in the tactical situation combines with the friction and fog of war to make it increasingly difficult to develop a coherent image of the enemy situation. This is why it often seems that we have better intelligence about what is happening in the enemy's rear echelon or capital city than we have about what is occurring beyond the next hill.

We have to work much harder to obtain information and knowledge about the enemy than we do concerning the friendly situation. Despite our extensive specialized capabilities designed to collect information about the enemy, the information we collect will normally be less than what we would like to have. Furthermore, collecting information does not by itself provide the needed intelligence. Even when friendly forces are obtaining information directly from the enemy—intercepting enemy signals, interrogating prisoners of war, translating captured documents—we must still confirm, evaluate, interpret, and analyze that information. Follow-on collection, processing, and production activities are normally needed. Finally, it should be emphasized that our need for intelligence usually greatly exceeds our ability to produce it; while questions about the hostile situation are almost infinite, the intelligence resources available to answer those questions are limited.

Once we have obtained the information necessary to build a picture of the enemy situation, we are confronted with other challenges. First, we must properly interpret the information. More important than the volume of information is the value of the information and the abilities of the people interpreting it. Any single item or any collection of information may be interpreted in a number of ways. Many mistakes in intelligence are not the result of a failure to collect the correct information, but rather a failure to discern the correct meaning from the information collected.

Second, even if we can develop a good understanding of the current situation, we cannot know with certainty what will happen in the future. While we can often assess the enemy's capabilities, we can rarely be certain of his intentions. Capabilities are based ultimately on factual conditions, while intentions exist only in the mind of the enemy—assuming the enemy even knows clearly what he wants to do. Thus, any assessment of enemy intentions is ultimately an estimate. While good intelligence can identify the possibilities and probabilities, there will always be an element of uncertainty in these estimates.

Third, because we are dealing directly with a hostile will, we can never be sure we are not being actively deceived. Even if we should gain some type of access to his actual plans, we cannot be certain that the enemy does not want us to see those plans as part of a deliberate deception effort.

Finally, the problems facing intelligence are further complicated by the irony that good intelligence may actually invalidate itself. Consider the following instance. Intelligence estimates that the enemy is preparing to launch an attack in a certain sector. Acting quickly on this intelligence, the commander strengthens that sector. The enemy, however, detects our enhanced defensive preparations, which causes him to cancel the attack. As a result, the intelligence estimate which predicted the attack in the first place appears wrong—but only because it was initially correct. Intelligence is thus a highly imprecise activity at best, and its effects are extremely difficult, if not impossible, to isolate.

For example, consider the U.S. response to a movement of Iraqi troops toward the Kuwaiti border in October 1994. After a period of increasing tension between Iraq and the United Nations over continuing sanctions against Iraq, U.S. intelligence detected the deployment of almost 80,000 troops in the vicinity of the Kuwaiti border, including two elite Republican Guard divisions.[9] The situation appeared similar to the one in August 1990 when Iraq invaded Kuwait. Intelligence warned that another invasion was possible. The United States and other allies responded by immediately dispatching forces to the region. The Iraqi forces were withdrawn, and the threat subsided. Did Saddam Hussein intend to invade Kuwait again? We will probably never know; intentions can seldom be determined with absolute certainty. On the one hand, we could state that intelligence failed because we could not ascertain Hussein's exact intentions and thus were unable to

detect the difference between a provocation and an actual invasion. A more reasonable explanation, however, is that intelligence stimulated appropriate action, action which prevented an invasion. The warning appeared to be incorrect, but only because it was right in the first place.

EXPECTATIONS OF INTELLIGENCE

We expect a great deal from intelligence. We ask intelligence to describe in detail places we have never seen, to identify customs and attitudes of societies fundamentally different from our own, to assess the capabilities of unique and unfamiliar military or paramilitary forces, and to forecast how these societies and forces will act in the future. Most notably, we want intelligence to enter the thought process of an enemy commander and predict, with certainty, what course of action he intends to pursue, possibly even before he knows himself what he is going to do. The standard against which we measure intelligence is also high. We desire a depth and degree of accuracy in our intelligence which approaches perfection. Even when a reasonable response has been provided to almost every intelligence requirement, there is still one more question to be answered, one more detail to be fleshed out, one more estimate to be refined. This is as it should be. The price for failure in intelligence is high. Inadequacies in intelligence

can lead directly to loss of life, destruction of equipment and facilities, failure of a mission, or even defeat.

When properly focused and given adequate time and resources, our intelligence can come close to meeting these standards. We can provide comprehensive depictions of physical terrain and manmade structures or facilities. Our reconnaissance and surveillance systems can detect and track the movements of ships, aircraft, and ground formations, in certain instances even providing real-time images of enemy activity. Our signals and human intelligence capabilities, coupled with expert analysis, can provide insight into both enemy capabilities and intentions.

However, even in the best of circumstances, intelligence still operates in an environment characterized by uncertainty. Uncertainty is a fundamental attribute of war. As discussed in the previous section, intelligence deals directly with the independent, hostile will of the enemy. This makes intelligence more susceptible to uncertainty than any other command and control function. In practical terms, this means that there are very definite limits to what commanders can reasonably expect from intelligence. Not only will more gaps exist in what we know about the enemy than in what we know about our own situation, but the reliability of everything we do know will be subject to greater scrutiny and doubt. Even if we obtain the correct information, there is no guarantee that we will interpret it correctly or that it will not change. We may be the victims of deception, whether it is by a deliberate enemy

effort or by our own preconceptions. Intelligence produces estimates rather than certainties; it is important to remember that "estimating is what you do when you do not know."[10]

Intelligence may be incorrect sometimes and incomplete at other times, and it often lacks the desired degree of detail and reliability. Some of the questions asked are simply beyond knowing—or are beyond knowing given the time and resources available. Gaps in our knowledge of the enemy situation, sometimes sizable, are a natural and unavoidable characteristic of fighting an enemy having an independent, hostile will. We must continually remember that *intelligence can reduce but never eliminate the uncertainty that is an inherent feature of war.*

INTELLIGENCE IN THE INFORMATION AGE

As a result of the ongoing information revolution, more people have access to more information more quickly than ever before. Intelligence has benefited greatly from improvements in information gathering, processing, and dissemination. Sophisticated sensors clandestinely collect vast quantities of data in all regions of the world. Integrated databases allow us to store and rapidly retrieve virtually unlimited numbers of reports, images, and studies. Information processors assist us

in analyzing the data and developing tailored, graphic-enhanced products that convey intelligence in a more meaningful form. Communications systems give us the ability to share databases, exchange intelligence, and disseminate products almost instantaneously on a worldwide basis.

While it is alluring to believe that the information revolution will solve the problems of uncertainty in dealing with the enemy, technology has its shortcomings as well. Systems employed in intelligence can be expensive and complex. Many are controlled at the national or theater levels, where priorities might not be consistent with those of the tactical commanders. Despite their sophistication, these systems are still subject to failure as a result of weather conditions, breakdowns, or enemy countermeasures.

Further, these systems generally provide and manipulate data and information rather than generate knowledge or understanding. The information revolution has created the very real danger of information overload—more available information than can be readily used or understood. Humans have a limited capacity to assimilate information. Even if we are able to collect vast amounts of information, *information alone does not equate to knowledge or understanding*, which are ultimately the product of human cognition and judgment. Since very few pieces of information are decisive by themselves, they must be interpreted and given meaning.

Finally, the seemingly unlimited availability of information does not necessarily help us in determining which information we should collect and develop into intelligence. In an unstable international environment, in which unanticipated crises proliferate, it is difficult to identify the next enemy or potential enemy. This complicates commanders' problems of identifying their concerns and priorities; it may be harder than in the past to focus the intelligence effort. As a result, it may not be possible to develop adequate basic intelligence about potential enemies or regions well in advance.

We must continue to pursue advances offered by technology to enhance our intelligence capabilities. At the same time, we recognize that technology by itself does not produce effective intelligence. Improvements in data collection, information processing, and dissemination are tools which assist in the intelligence effort. These tools increase our capabilities only when they are applied by knowledgeable and skilled Marines focused on producing timely, useful, and relevant intelligence.

A CASE STUDY: DESERT STORM 1990–1991

The development and use of intelligence in support of Marine operations during Desert Storm illustrate the nature of intelligence and its core concepts and challenges. During this

operation, intelligence provided an accurate picture of the situation confronting Marine forces and identified the enemy's critical vulnerabilities which Marine commanders exploited to achieve success.[11]

By mid-January 1991 the situation at the strategic and operational levels was well understood. Iraqi commanders prepared for the expected Coalition assault into Kuwait in a manner that reflected the success of their defensive strategy during the Iran-Iraq War. They constructed two major defensive belts in addition to extensive obstacles and fortifications along the coast.

Intelligence identified three Iraqi centers of gravity at the operational level. The first was their command and control. If rendered unable to direct its military forces, Iraq would not be able to mount an effective defense at the operational level. Second was Iraq's weapons of mass destruction. Degrading this capability would reduce a major aspect of the Iraqi strategic threat to other states in the region. The third center of gravity was the Republican Guard. Destroying or severely degrading the Republican Guard's ability to fight would dramatically diminish Iraq's capability to conduct a coordinated defense or to pose an offensive threat to the region later.

Intelligence likewise provided thorough understanding of Iraq's critical vulnerabilities: a rigid, top-down command and control system, the reluctance of Iraqi commanders to exercise initiative, an overly defensive approach to battle with

limited ability to conduct deep offensive actions, vulnerability to air attack, an overextended logistics system, and extremely limited intelligence capabilities.

This understanding was used to plan the campaign and guide the conduct of air operations during the first few weeks of Desert Storm. Coalition air attacks had devastating effects on the Iraqis, severely disrupting their command and control, eliminating their naval and air forces, and degrading their logistics capabilities.

Nevertheless, the situation facing Marine commanders was less clear. Much of the intelligence developed prior to the start of the operation was focused on strategic- and operational-level objectives and lacked the detailed, tailored intelligence essential for tactical planning. Further, ground force commanders were not permitted to employ most of their organic collection assets within Kuwait due to concerns about potential casualties, operational security, and initiation of engagements before a decision on ground operations had been made. Marines required support from national and theater intelligence agencies to answer many of their critical intelligence requirements. Although these needs were generally recognized as valid by the higher echelons which controlled these assets, Marine tactical requirements tended to fall too low on the priorities list to compete effectively with other requirements. When national sensors were used to support Marine force requirements, the results often did not provide sufficient detail to fully satisfy those requirements.

Still, by January the Marine forces' intelligence estimate provided a fairly accurate assessment of the overall size and disposition of the Iraqi units as well as the strategy and tactics they would employ. The estimate highlighted four potential Iraqi responses to Coalition air attacks: terrorist attacks inside and outside the area of operations, air and naval counter-strikes, surface-to-surface missile and multiple rocket launcher attacks against Marine positions in the forward area, and a limited-objective ground attack or raid. Like most estimates, this assessment proved to be only partially correct. Iraqi air and naval forces offered minimal opposition, and no major terrorist attacks were conducted. However, there were extensive missile and multiple rocket launcher attacks, and a significant ground attack was launched at the end of the month.

The main shortfall of the estimate was that it lacked details required for tactical planning. Determining the effectiveness of Iraqi forces was a critical requirement. The raw numbers indicated that large Iraqi forces remained within Kuwait. Air attacks were damaging the enemy's forward echelon and had severely degraded both his sustainment and command and control capabilities. There were indications that Iraqi front-line infantry troops were demoralized and would not put up much of a fight. Intelligence clearly showed that the Iraqis had been hurt, but in the absence of definitive information detailing how badly they had been hurt, Marine planning continued to reflect a cautious approach.

During a battle from 29 January to 1 February at Al-Khafji, an Iraqi division-sized ground attack was soundly defeated by Coalition forces. Iraqi actions during this battle provided Marine intelligence specialists critical information to fill in the intelligence picture. Analysis confirmed previous assessments of the deteriorating condition of enemy units and the Iraqis' limited capability to coordinate between tactical echelons. From reports by Marine participants, analysts concluded that Iraqi soldiers were unmotivated, poorly trained, and unable to conduct combined arms operations.

With this insight, previous perceptions of the enemy's strengths and ability to mount a formidable defense were called into question. Subsequent intelligence operations further clarified the threat picture. Interrogations of enemy troops lured to surrender reinforced the view that the Iraqi will to fight was far weaker than anyone had anticipated. Artillery raids failed to elicit counterbattery fire, indicating that Iraqi artillery capabilities had been degraded. Unit boundaries along the defensive belts were located, and gaps in the defenses were identified at those points, confirming that coordination between tactical echelons was poor.

From the new intelligence, a new estimate reflected the likelihood that the Iraqis would be unable to conduct an effective defense of the forward positions. It noted that the Iraqis could not coordinate between units, employ supporting arms, or conduct counterattacks with forces larger than a battalion. Finally, it indicated that Iraqi infantry and artillery troops

would probably surrender en masse once the first shot was fired.

This intelligence was used to substantially revise the Marine operation plan. Knowing that the Iraqis would be unable to assess what was happening on the battlefield or to respond effectively, Marine commanders adopted a more aggressive scheme of maneuver. The previous plan called for a sequential attack with one division following the other through the defensive belts using a single breech point. On February 6, the Marine Force commander approved a new plan in which two Marine divisions would conduct a simultaneous, coordinated attack through the defensive belts at points 40 kilometers apart (see figure 1). In addition, a significant force was now assigned to deal with the expected flood of surrendering Iraqi troops.

The intelligence assessment developed and refined during Operation Desert Storm reduced uncertainty, enhanced situational awareness, and aided Marine commanders in planning and decisionmaking. This assessment did not answer every question, but it did identify the enemy's critical vulnerabilities which were exploited to achieve decisive results.

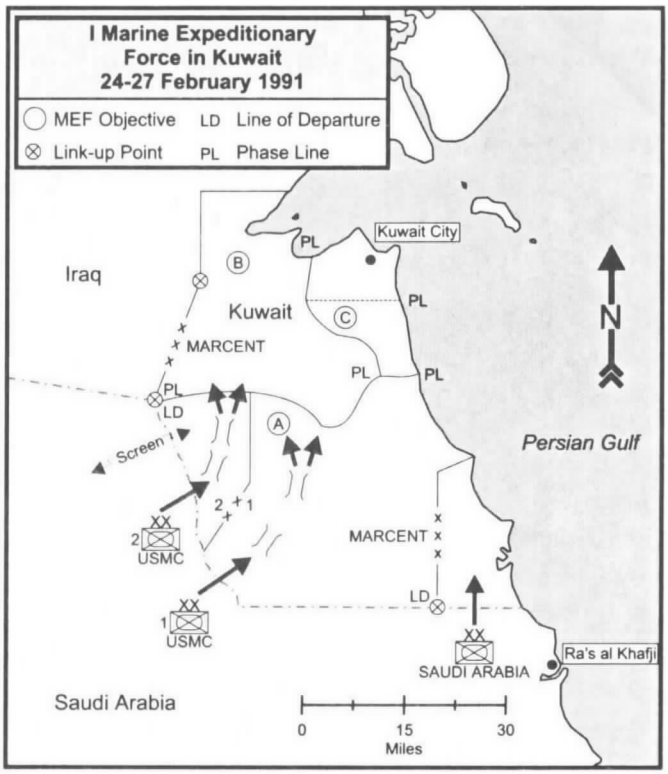

I Marine Expeditionary
Force in Kuwait
24-27 February 1991
MEF Objective
LD Line of Departure
Link-up Point
PL Phase Line
Kuwait City
PL
Iraq
B
Kuwait
C
PL
MARCENT
PL
PL
PL
LD
Screen
A
Persian Gulf
N
2
1
XX
2
USMC
MARCENT
LD
XX
1
USMC
XX
SAUDI ARABIA
Ra's al Khafji
Saudi Arabia
0
15
30
Miles

Figure 1.

CONCLUSION

Intelligence is a fundamental component of command and control—inseparable from both command and operations. Accurate, timely, and relevant intelligence is critical to the planning and conduct of successful operations. Effective intelligence uncovers enemy weaknesses which can be exploited to provide a decisive advantage. Shortfalls in intelligence can lead to confusion, indecision, unnecessary loss of life, mission failure, or even defeat.

Intelligence is knowledge of the enemy and the surrounding environment provided to support the commander's decisionmaking process. Intelligence is more than just information; it is the analysis and synthesis of information which provides a meaningful assessment of the situation. Intelligence evaluates existing conditions and enemy capabilities, estimates possible future conditions and enemy courses of action, assists in the development and evaluation of friendly courses of action, and aids in protecting friendly forces against the effects of enemy action.

While intelligence uses specialized capabilities and techniques in developing a useful product, it is not an obscure process isolated from other warfighting functions. In fact, effective intelligence requires a firm focus on the needs of commanders. This in turn, demands integration with all aspects of operational planning and execution. What separates

intelligence from the other aspects of command and control, however, is the fact that intelligence must deal directly with the independent, hostile will of the enemy. Because intelligence attempts to look into the future despite significant unknowns, the resulting product will always be based on estimates, not certainties. Users of intelligence must always remember that intelligence can reduce, but never eliminate the uncertainty that is an inherent characteristic of war, and act accordingly.

Chapter 2

Intelligence Theory

"Many intelligence reports in war are contradictory; even more are false, and most are uncertain. What one can reasonably ask of an officer is that he should possess a standard of judgment, which he can gain only from knowledge of men and affairs and from common sense. He should be guided by the laws of probability. These are difficult enough to apply when plans are drafted in an office, far from the sphere of action; the task becomes infinitely harder in the thick of fighting itself, with reports streaming in."[1]

—Clausewitz, *On War*

"It will be vital to identify centers of gravity rapidly and determine the critical vulnerabilities that will be our pathways to them. We won't always have the luxury of a passive foe, and there's no natural law that says that every high-tech war must be fought in a desert with unlimited visibility and good weather."[2]

—Carl E. Mundy

Having reached a common understanding of the nature of intelligence, we turn now to developing a theory about the intelligence process that in turn will serve as the basis for creating an effective intelligence system.

WHAT DO WE WANT TO KNOW ABOUT THE ENEMY?

In war, it is easier to defeat an enemy we understand, even partially, than to fight an enemy who is an enigma. Intelligence is the means by which we come to understand the enemy. What is it about the enemy that commanders need to learn? The commander needs to gain knowledge at a variety of levels, ranging from that which is quantifiable to that which is purely intangible.

Obviously, we want to know the measurable things: the number of enemy personnel, armored vehicles, artillery pieces, and aircraft. We hope to learn the dispositions, organization, and locations of enemy forces. We also want to obtain technical specifications: the performance characteristics of enemy tanks and aircraft and the range and effectiveness of opposing weapons. Traditionally, intelligence has focused on these tangible factors. They usually provide a concrete image

of the threat and the nature of its combat power. These tangible factors and images thus provide the foundation for developing a more complete understanding of the enemy based upon other intangible factors.

While numbers definitely matter, they provide only partial insight into enemy capabilities. Less quantifiable and more subjectively deduced is the enemy's level of readiness—the state of his training, the quality of his leadership, and the morale of his forces. Commanders need to know the enemy's methods—his doctrine, tactics, techniques, and procedures—as well as his past performance in training and in combat. Even this is not enough. The successful commander cannot truly know an enemy simply through analysis of his physical environment, material might, and political and military institutions.

We must seek still more deeply for those moral and cultural forces which shape the enemy's actions. War is ultimately a human conflict, and much of human nature is decidedly illogical and incalculable. Developing sound intelligence requires an understanding of the institutions, preferences, and habits of a different culture. Commanders must appreciate the values, goals, and past experiences which motivate the enemy. We must gain insight into *why* he fights. To know what motivates an enemy to action requires an identification and appreciation of what the enemy holds dear.

Coming to grips with the intangible aspects of the enemy situation is much more difficult than assessing those factors

that are quantifiable, but it is essential if commanders are to truly understand an enemy. This is exactly what intelligence must endeavor to do—to understand what factors shape an enemy's behavior in order to describe or explain that behavior.

When we try to understand an enemy, it is important to visualize the enemy as he sees himself and to see the situation as he views it. While gaining an objective appreciation for the enemy's capabilities is important, it is equally important to appreciate how the enemy perceives his own capabilities, since it is this image that will have the greatest influence on his actions. The enemy will do what *he* thinks is possible, not what we think he can do.

Seeing the situation from the opponent's perspective is especially important when confronting an adversary with a significantly different set of cultural or societal values. Enemy behavior which appears irrational—and therefore surprising—to us may in fact reflect perfectly reasonable and even predictable actions, given the enemy's values or the information available to him at the time. Consider the use of the banzai charge and kamikaze attacks by the Japanese in World War II or employment of women and children as shields to cover the actions of Somalian clansmen against U.N. forces. None of these actions is rational when viewed from a Western perspective. However, within the context of Japanese or Somalian societal norms, they are less surprising. A commander who fails to understand the enemy on his own terms risks a

fundamental failure to understand the very nature of the conflict.

Finally, intelligence should strive to determine not only the enemy's capabilities but also his intentions. Intelligence estimates deal in both: they describe what an adversary *can* do, and they attempt to discern what he *will* do based upon possibilities and probabilities. Ideally, intelligence should identify several possible scenarios, answering questions such as: *Which is the most likely enemy course of action? Which is the most dangerous?* Intelligence should also correlate the effect of possible enemy actions on friendly plans.

The goal is, therefore, to obtain as complete an understanding of the enemy as possible. The ultimate purpose in seeking this understanding is to *identify enemy centers of gravity and critical vulnerabilities and other limitations that may be exploited* to defeat him: weaknesses in specific warfighting capabilities, numbers, or dispositions; technical deficiencies in weapon systems; or shortcomings in readiness, leadership, or morale. Conversely, intelligence should provide warning of particularly dangerous enemy capabilities that pose a threat to friendly forces.

There are practical limitations to achieving this level of understanding. The effects of uncertainty on intelligence have already been discussed, but it is worth repeating that gaps in our knowledge of the enemy situation are natural and unavoidable. Furthermore, attaining in-depth knowledge on the

variety of potential threats confronting Marine forces is a significant challenge. Our education, cultural appreciation, and experience may be insufficient to provide detailed insight into an adversary without extensive study. The time required for this study may not be available when responding to a developing crisis. In these situations, we build as complete a picture of the enemy as possible in the time available—relying primarily on known factors and likely capabilities—while striving to fill in that picture rapidly as our understanding of the adversary grows.

An example of this approach can be seen in the history of Marine forces' involvement in Somalia. When the 15th Marine Expeditionary Unit landed in Mogadishu to begin Operation Restore Hope in December 1992, Marines had only a basic understanding of Somalian culture, the clan structure, and the threat it presented to U.S. and U.N. forces. Intensive intelligence development, in particular through human intelligence operations, rapidly increased our level of understanding. This intelligence was used over the course of the campaign to plan and execute numerous successful tactical actions that in turn further enhanced the intelligence picture. When the Marines of I Marine Expeditionary Force (MEF) returned in February of 1995 to assist in the final withdrawal of U.N. forces, they were able to draw on an extensive reservoir of intelligence to plan and execute Operation United Shield. Based on this intelligence, I MEF prepared a "playbook" of responses to cover virtually any Somalian reaction. Further, the playbook evolved as new intelligence was

produced and the intelligence estimate changed. The detailed intelligence available contributed directly to the safe and effective accomplishment of the mission.[3]

CHARACTERISTICS OF GOOD INTELLIGENCE

In the previous chapter, we discussed our expectations of intelligence—its capabilities and limitations as well as what can and cannot be reasonably expected of intelligence. As the next step in developing a theory of intelligence, it is important to describe the characteristics of good intelligence.

First, intelligence should be *objective*—as free as humanly possible of bias or distortion. We have already noted that a significant problem in intelligence is not the lack of information, but the difficulty in interpreting that information correctly. Intelligence can be distorted if we attempt to make it conform to preconceived notions, fail to view the situation from the enemy's perspective, or manipulate the intelligence product to support a particular decision or conclusion. For example, prior to Chinese intervention in the Korean War, there were ample indications and warnings of imminent Chinese involvement. However, despite availability of much factual information to the contrary, strongly held preconceptions led commanders and their intelligence officers to conclude that the Chinese would not intervene.[4] Unfortunately, data and

information are almost always susceptible to more than one interpretation and can be manipulated consciously or unconsciously to support preconceived notions.

Second, intelligence should be *thorough*, meaning that it satisfies the intelligence requirements of the commander. Thoroughness does not imply completeness and certainty to the last detail, but rather sufficient depth to assist the commander in reaching sound decisions and developing effective plans. Intelligence personnel should not only identify for the commander what is known but also what is not known. The commander may then assess the risks and decide what actions are worth these risks.

Third, intelligence should be *accurate*, meaning that it should be factually correct. Sound estimates of the enemy's capabilities and intentions must agree with the facts at hand. Since intelligence cannot be precise to the last detail, commanders must have an appreciation of the reliability of a particular intelligence assessment or product.

Fourth, intelligence must be *timely*, meaning that it must arrive in the hands of appropriate decisionmakers in time to affect tactical decisions. Intelligence does not exist for its own sake, but as the basis for taking effective action. The most accurate and valuable piece of intelligence is of no use if it arrives too late to be acted upon. Some kinds of intelligence are more time-sensitive, or perishable, than others—a warning report, for example, is a type of intelligence product

that tends to be highly perishable. It is important to keep this time-sensitivity in mind when dealing with any intelligence product.

Fifth, intelligence should be *usable*, appearing in a form meaningful to and easily assimilated by decisionmakers. Good intelligence should be concise and clear. It must create coherent images—meaningful mental pictures that are immediately and easily understood—rather than present the commander with a mass of unfocused data. Because we generally understand information better when it is presented in the form of images, we attempt to present intelligence in a visual format whenever possible.

Sixth, intelligence should be *relevant* in that it supports the commander's planning and decisionmaking requirements. Relevance means that intelligence is pertinent to the level of command for which it is intended. Relevance means also that commanders are provided information and intelligence bearing significantly on the situation at hand and that they are not burdened with information and intelligence of minimal or no importance. Intelligence that is tailored appropriately for one commander may be too generic or too detailed for commanders above and below that particular level. However, it may be extremely difficult to know in advance what is relevant and what is not. This leads again to the necessity for commanders to focus the intelligence effort.

The value of providing relevant intelligence is illustrated by the following example. Following the bombing of the Marine Corps compound in Beirut in 1983, Department of Defense investigators faulted commanders and intelligence for inundating on-scene commanders with information and failing to provide them with timely intelligence tailored to their specific operational needs.[5] While information overload was certainly not the only cause of the Beirut tragedy, more focused intelligence might have helped commanders prevent its occurrence or at least take greater security precautions.

Finally, intelligence must be *available*—which means that it is readily accessible to appropriate commanders. Availability is a function of both timeliness and usability, but it is also a function of an effective information management system that allows commanders at various levels to readily access the intelligence they need. Availability also means that relevant basic intelligence has been developed in advance and that intelligence assets are maintained in readiness to develop other intelligence products as needed. Finally, availability is a function of effective use of security classifications that protect sources of information while at the same time ensuring that commanders have reasonable access to intelligence.

This discussion is not meant to specify a checklist for what does or does not constitute good intelligence, but to describe the general characteristics which effective intelligence tends to exhibit to one degree or another. Few intelligence products

will exhibit all the above characteristics. Some of the characteristics such as timeliness, usability, and availability are mutually supportable. Others such as timeliness and thoroughness can be in conflict. The extent to which actual intelligence demonstrates each of these characteristics depends on the particular situation.

CLASSES OF INTELLIGENCE

If we could describe a complete intelligence picture—one that provides us everything we need to know about a given situation—that description would include knowledge of established conditions which have existed in the past, unfolding conditions as they exist in the present, and conditions which may exist in the future. Our complete image would include what has been, what is, and what might be. With this background, two classes of intelligence are defined. The first is *descriptive intelligence,* which describes existing and previously existing conditions. The second class, which attempts to anticipate future possibilities and probabilities, is *estimative intelligence.*

Descriptive intelligence has two components. The first is *basic intelligence.* Basic intelligence is general background knowledge about established and relatively constant conditions. Basic intelligence is often compiled in advance of

potential operations and retained in databases or reference publications. Basic intelligence might describe the geography, culture, economy, and government institutions of a potentially hostile nation or area. With regard to the military capabilities and limitations of potential enemies, basic intelligence might detail the size, organization, and equipment of their military forces. These factors may change, but only slowly.

Basic intelligence is often encyclopedic in nature and is consequently often the most mundane. While it tends to be the easiest to gather, often being available through open sources, the depth and detail of the intelligence required to support most operations makes developing basic intelligence a labor-intensive and time-consuming task. Of all the types of intelligence, basic intelligence tends to be the most accurate and reliable. However, basic intelligence is also the most general and least time-sensitive. By itself it rarely reveals much that is decisive. Further, since basic intelligence does not address specific situations, it rarely provides sufficient knowledge for effective decisionmaking. Nevertheless, basic intelligence establishes the necessary foundation for building a more complete intelligence picture.

Descriptive intelligence also includes *current intelligence,* which is concerned with describing the existing situation. In general, current intelligence describes more changeable factors than those addressed by basic intelligence and is therefore more time-sensitive than basic intelligence. For example, while basic intelligence reports climatic norms, current intelligence describes existing weather conditions and its effects

on operations; while basic intelligence shows enemy doctrine and organization, current intelligence depicts actual dispositions, movements, and patterns of activity. At higher levels, basic intelligence describes economies and forms of government; current intelligence addresses ongoing enemy war preparations or the status of relations with other hostile or potentially hostile nations. As a rule, current intelligence tends to be more specific than basic intelligence but less reliable and harder to obtain. Basic intelligence provides the broad picture upon which current intelligence expands by adding specific details about the existing situation.

Estimative intelligence, the second class of intelligence, focuses on potential developments. Developing estimative intelligence is perhaps the most important and at the same time most demanding task of intelligence. Estimative intelligence evaluates the past as delineated by basic intelligence and the present as described by current intelligence and seeks to anticipate a possible future—or several possible futures. It is concerned with determining when, where, how, or even if an enemy or potential enemy will attack or defend. Commanders cannot reasonably expect estimative intelligence to precisely predict the future; rather, estimative intelligence deals with the realm of possibilities and probabilities. It is inherently the less reliable of the classes of intelligence because it is not based on what actually is or has been, but rather on what *might* occur.

Although described as conceptually distinct, the two classes of intelligence are inseparable. Descriptive intelligence provides the base from which estimative intelligence assesses possible or probable futures. Without both classes of intelligence, it is impossible to develop a full image of a hostile situation.

CAPABILITIES VERSUS INTENTIONS

Another way to frame this same discussion is in terms of capabilities and intentions. Descriptive intelligence attempts to discern enemy capabilities and existing conditions. It attempts to answer the questions: "What conditions currently exist? What *can* the enemy do? What *can't* he do?" Estimative intelligence attempts to discern enemy intentions and future conditions. It asks: "What conditions will probably exist in the future? What are their effects on friendly and enemy capabilities and courses of action? What *might* the enemy do? What is the enemy *most likely* to do?" Although the answers to all these questions are estimates rather than certainties, generally we can assess enemy capabilities with greater precision than enemy intentions.

Estimating enemy capabilities is largely a matter of interpreting the facts. Estimating enemy intentions, however, is a

matter of far less certainty. Intentions exist only in the enemy's mind. In any given situation, an enemy commander will probably have several courses of action available. There may be little or no indication of which one he favors. He may be intentionally attempting to conceal his intentions from us, or he may be trying to keep more than one option open. He may be gripped by indecision and not know what he intends to do. Furthermore, he can change his mind. He can respond to changes in the situation or our own actions in ways we cannot anticipate.

Complicating this problem is the reality that an enemy's intentions are normally the product of thought processes different from our own. We are sometimes surprised when an enemy takes an action which we consider to be irrational. However, when viewed from the perspective of the enemy's cultural norms or values, his actions may be perfectly logical and predictable. Unfortunately, it is extremely difficult to gain the depth of insight needed to understand the thought process of each and every potential adversary we face. Our own values and cultural background will always be a significant obstacle in estimating the intentions of terrorists willing to blow themselves up in suicide bombings or a dictator who would inflict massive damage on the environment by setting hundreds of oil wells on fire.

Enemy capabilities and enemy intentions are closely related. Capabilities establish the limits of intentions; the enemy cannot intend to do something beyond his capabilities

and accomplish it successfully. However, it is crucial to note that it is not actual capabilities that matter, but the enemy's perception of his capabilities. The enemy will act based on his perception of his capabilities. His perception may or may not agree with our evaluation of what he can or cannot do. Our analysis of enemy forces in South Vietnam did not credit the North Vietnamese and Viet Cong with the capability to launch a nationwide offensive in 1968. The Tet offensive of that year clearly demonstrated that the enemy believed otherwise.[6] Again, a key element in assessing both capabilities and intentions is the ability to view the situation as the enemy perceives it.

Analysis of capabilities and analysis of intentions are by no means incompatible. Any effective intelligence picture must provide insight into both. Without some appreciation of enemy intentions, it is extremely difficult to decide on an effective plan of action. However, without an understanding of the enemy's capabilities, it is impossible to estimate his intentions.

SIGNALS AND NOISE

Complicating our ability to assess capabilities and estimate intentions is the problem of interpretation of the information we collect. To develop objective and accurate intelligence, we

must understand this problem. We can examine it through a discussion of *signals* and *noise*.[7]

Signals refer to those pieces of information commanders receive that, if properly interpreted, can lead to valuable insight about the situation. Signals help with our situation assessment. Noise, on the other hand, refers to various pieces of useless information—information which is false, out of date, inaccurate, ambiguous, misleading, or irrelevant. An enemy may intentionally present a foe with noise in order to mislead, but noise is not necessarily the product of an enemy deception. Like static on a radio, noise interferes with our reception and interpretation of valuable signals.

The difficulty is to distinguish signals from noise. Unlike the distinction between radio static and the true signal, the difference between true and false information is rarely easy to distinguish. We endeavor to identify critical enemy vulnerabilities, but signals of such vulnerabilities are rarely clear at the time. The recognition of what is important, relevant, and accurate sometimes becomes clear only in hindsight—if then.

Clausewitz advises that, "A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth."[8] Just as judgment is no substitute for good intelligence, *intelligence is no substitute for good judgment*. The two must go hand in hand.

This point illustrates the importance of mindset to intelligence. A mindset is a set of assumptions, biases, and preconceptions. A mindset reflects a preexisting image of what is reasonable; it serves as a filter that helps to distinguish the signals from the noise. The human tendency is to be more receptive to information that is consistent with one's mindset and more skeptical of information that is not. In other words, information that is consistent with an existing mindset is interpreted as signals, and information that is not is construed as noise.[9]

Every individual possesses a unique mindset. Biases and preconceptions are also indispensable to intelligence. Without them, it would be impossible to make sense of the available mass of confusing and sometimes contradictory information. Mindsets serve as a frame of reference, enabling us to quickly categorize and assess the relevance and reliability of vast amounts of information. Without a preexisting mindset, commanders would likely be overwhelmed by the amount of information and unable to distinguish between signals and noise.

At the same time, mindsets always bring the danger that we will subconsciously interpret intelligence to comply with our preconceived notions rather than with reality. This hazard applies equally to the producers and users of intelligence.

The danger of preconceived notions and their impact on signals and noise is illustrated by this example from the Arab-Israeli War of 1973.[10] In October 1973, a simultaneous Syrian and Egyptian attack caught the Israeli army badly unprepared. There had been plenty of signals of the Egyptian intentions. The Israeli high command had extremely detailed and accurate information on their enemies' order of battle, unit locations, armaments, and readiness status. In fact, Israeli intelligence was fully aware of unprecedented forward deployments of enemy troops and ammunition stocks. Nonetheless, the possibility of war was discounted until just 8 hours prior to the beginning of the Arab offensive.

The problem was not lack of information, but an inability to filter out noise coupled with reliance on a set of rigid and faulty preconceptions. The Egyptians employed a variety of deception activities, both political and military, to create noise. Included were the continued preparation of defensive positions, repeated repositioning of units along the front, and the use of training exercises as a cover for forward deployments.

Despite the effort to deceive, Israeli intelligence detected most of the key preparations for war. However, even though there was information pointing to an impending attack, the Israeli mindset prevented accurate interpretation of it. The Israelis believed that any Arab attack would be based on military rather than political or psychological factors. Since the Israelis felt that Syrian or Egyptian armies had no capability

to conquer substantial territory from Israel, they discounted any possibility that the Arabs would attack. In fact, the Arab objective was not territorial conquest, but creation of a diplomatic crisis that would be resolved in their favor. Compounding the Israelis' misreading of Arab intentions was the failure of Israeli intelligence to objectively assess Egyptian military capabilities. The Israelis' preconception that the Egyptian army was incompetent caused them to dismiss any possibility that the Egyptians could mount an effective attack. Due to Israeli bias and preconceptions, an overwhelming body of first-rate intelligence that would have provided adequate warning of the attack was simply dismissed as irrelevant.

We seek to develop a balanced mindset that provides a sensitive and discriminating judgment which is not so entrenched that it deafens us to alternative signals. One of the most valuable contributions intelligence personnel can provide is unbiased analyses to uncover and guard against dangerous preconceptions.

LEVELS OF INTELLIGENCE

A complete intelligence picture must also provide insight into the enemy as a complete entity or system, not merely as a collection of unrelated individuals, units, or organizations. Companies, batteries, or squadrons normally do not act independently. They conduct operations in accordance with the

plans and orders of a senior headquarters that in turn is attempting to achieve some strategic or operational objective. In order to understand what the enemy unit directly opposite us is doing now or what it might do in the future, it is usually necessary to examine the capabilities and intentions of enemy units and commanders two levels or more above our immediate adversary.

Developing this type of understanding requires us to consider that intelligence cuts across the three levels of war: tactical, operational, and strategic. As this intelligence varies in terms of scope, application, and level of detail, we divide intelligence into levels which correspond to the levels of war. *Tactical intelligence* concerns itself primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather. *Operational intelligence* pertains more broadly to the location, capabilities, and possible intentions of enemy forces within the theater and with the operational aspects of geography. Finally, *strategic intelligence* is broadest of all in scope and addresses the factors needed to formulate policy and military plans at the national and international levels.

Marine Corps intelligence focuses on tactical intelligence, which is the level of intelligence Marines need, generate, and use most often. However, in order to operate effectively, Marine forces require ready access to operational and strategic intelligence, as well as tactical, to comprehend the larger situation and provide appropriate context for the development of tactical intelligence products.

INTELLIGENCE REQUIREMENTS

A unit's intelligence effort begins with receipt of the mission and the commander's guidance. On-hand intelligence is rarely sufficient to support comprehensive planning and decision-making needs—gaps will remain. Such intelligence gaps are known as *intelligence requirements*.

Intelligence requirements are questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. The breadth of potential intelligence gaps, however, will generally far exceed organic intelligence capabilities. Thus, it is important to focus intelligence operations on those intelligence requirements crucial to mission success. We call these requirements *priority intelligence requirements*.[11]

Priority intelligence requirements are intelligence requirements associated with a decision that will critically affect the overall success of the command's mission. Priority intelligence requirements constitute the commander's guidance for the intelligence collection, production, and dissemination efforts.

The nature and scope of intelligence requirements will vary with the level of command and its mission. Further, the type of operation and at what particular phase of planning or execution the commander states a requirement will be major

influences on its breadth and complexity. However, it is the commander who designates the priority intelligence requirements and therefore provides direction to the intelligence effort.

The importance of clear and focused intelligence requirements was demonstrated during the recovery of Air Force pilot Capt Scott O'Grady from Bosnia in June 1995. After Capt O'Grady was shot down, the 24th Marine Expeditionary Unit (Special Operations Capable) afloat in the Adriatic was placed on alert to conduct a tactical recovery of aircraft and personnel (TRAP) mission. Upon notification that a signal had been received from Capt O'Grady's recovery beacon, the MEU commander designated three priority intelligence requirements: determine Capt O'Grady's exact location, update and reassess air defense threats to the TRAP force, and identify and describe flight hazards to the TRAP force. The clear identification of the critical intelligence needed to execute the mission enabled the MEU intelligence section to concentrate its effort on satisfying those requirements in the few hours it had available.[12]

SOURCES OF INTELLIGENCE

Intelligence information comes from a wide variety of information sources, ranging from a reconnaissance Marine with a

pair of binoculars to a sophisticated electronic sensor. Intelligence information may be derived from any Marine, other human sources, imagery, radar, signals, other emissions or signatures, and open-source references. Effective intelligence operations employ all information sources, whether organic or external. The value of a source is not necessarily related to the sophistication or cost of that source. Sources of information must be appropriate to the nature of the particular intelligence requirement; that is, the collection method or capability used must be appropriate to the aspect of the enemy or the environment about which information is needed. For example, electronic intelligence will likely be of little use against a technologically unsophisticated enemy; human intelligence sources will generally be more valuable. We must tailor the sources to the requirement, ensuring that we exploit both the observations of units in direct contact with the enemy and our more sophisticated sensors.

FUNCTIONS OF INTELLIGENCE

Intelligence performs six specific functions in order to provide knowledge of the threat and the surrounding environment as well as to deny that same knowledge to the enemy.

The first function of intelligence is to *support the formulation of the commander's estimate of the situation* by providing as accurate an image of the hostile situation as possible.

Through this function, intelligence helps the commander gain an initial appreciation for the terrain, weather, and other aspects of the operational environment. Intelligence personnel use techniques (such as intelligence preparation of the battlespace) to estimate enemy capabilities, intentions, vulnerabilities, and possible courses of action. In this manner, intelligence supports initial decisionmaking and planning.

The second function of intelligence is to *aid in situation development*—to provide continuing knowledge of unfolding events to help update the commander's image of the hostile situation. While the commander's initial estimate of the situation takes place before execution and provides the basis for the plan, situation development occurs during execution and provides the basis for adjusting plans to adapt to new circumstances or to exploit opportunities as they arise.

The third function of intelligence is to *provide indications and warnings*. Indications and warnings serve a protective purpose, namely to provide early warning of potential hostile action and thereby lessen the chance of being surprised. Properly used, indications and warnings act as alarms. They alert us to developments that run counter to the commander's planning assumptions and understanding of the situation in time to take necessary actions or precautions.

A fourth function of intelligence is to *provide support to force protection*. Force protection includes defensive operations, security measures, and collection activities undertaken

by a commander to guard the force against the effects of enemy action. Intelligence supports the commander's force protection needs by estimating an enemy's intelligence, terrorism, espionage, sabotage, and subversion capabilities as well as recommending countermeasures against those capabilities. Support to force protection requires detailed assessments of both the capabilities and intentions of the enemy. A successful program of force protection lessens the enemy's ability to take offensive action against us.

The fifth intelligence function is to *support targeting*, a function that intelligence shares with operations. Targeting is the process of acquiring information about targets and choosing the best method for attacking those targets. Intelligence supports this process by locating and portraying targets for attack and by estimating the vulnerability and relative importance of those targets. Targets may be physical targets such as a bridge or enemy position, or they may be functional targets such as the enemy's command and control system.

The final role of intelligence is to *support combat assessment*. Combat assessment is the process used to determine the effects of friendly actions on the enemy. It includes battle damage assessment which refers specifically to the effects of friendly fires on enemy targets. It also applies more broadly the overall effects of friendly actions on enemy capabilities and intentions. Combat assessment provides the basis for future friendly actions as well as a dynamic link back to the first step of the intelligence cycle.

SECURITY

Safeguarding intelligence is an essential consideration. Intelligence is normally less valuable if the enemy is aware of what we know. If the enemy concludes that we are in possession of a key piece of intelligence, he will likely change his plans and thus invalidate the intelligence. Security is important not only because it protects a specific piece of intelligence but also because it protects the sources upon which the intelligence is based. Thus, in the interests of security, the dissemination of and access to intelligence is often restricted.

A tension exists between the legitimate need for security and the essential need for dissemination. On the one hand, we must protect not only the value of individual pieces of intelligence but also the sources which we depend upon to provide additional valuable intelligence in the future. On the other hand, intelligence is useless unless it can be acted upon; to be of value, intelligence must be in the hands of the decision-makers who plan and execute military operations. Finding the proper balance between greater security and wider dissemination is a matter of reasoned judgment based upon the situation, the nature of the intelligence, and the sources involved.[13]

An example of the judgments involved in balancing security and dissemination can be seen in the use of signals intelligence during World War II. The Allies had significant

success in breaking both German and Japanese codes during the war. Because of the sensitivity of the intelligence derived from communications intercepts, the desire to ensure continued availability of this source of intelligence, and the ease with which the enemy could have taken measures to protect their communications, access and dissemination were tightly controlled. Commanders were faced with difficult choices in deciding when and how to use this intelligence, weighing the potential gain against the risk of compromising the source of intelligence. For example, when U.S. cryptologists intercepted advance notification of an inspection tour of the forward area by the commander in chief of the Japanese imperial combined fleet, Admiral Isoroku Yamamoto, American commanders had to decide whether or not to ambush Yamamoto's plane. In this case, they deemed the potential gain of eliminating Japan's best military leader worth the risk of compromising the source of the intelligence. U.S. forces were able to shoot down Yamamoto's plane, resulting in his death—without compromising any U.S. intelligence sources.[14]

THE INTELLIGENCE CYCLE

The intelligence cycle describes the general sequence of activities involved in developing intelligence. The cycle is not meant to prescribe a procedure to be followed, but simply to describe a process which generally occurs. The intelligence

cycle has six phases through which information is planned, obtained, assembled, converted into intelligence, provided to decisionmakers, and, ultimately, used in making decisions. (See figure 2.)

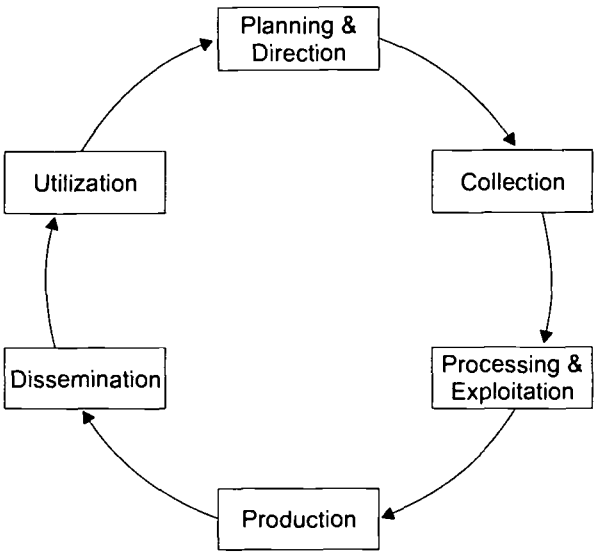


Figure 2.

The first phase in the intelligence cycle is *planning and direction*. This phase consists of the identification of intelligence requirements and the planning of intelligence operations and activities to satisfy those requirements. The

commander directs the intelligence effort; the intelligence officer manages this effort for the commander. In so doing, the intelligence officer is guided by the commander's intent, the established priority intelligence requirements, and specific guidance provided by the commander for the conduct of the intelligence effort. Planning and direction encompasses the supervision of collection, processing, production, and dissemination operations as well as developing the intelligence structure necessary to support planned or ongoing operations.

Collection is the second phase of the intelligence cycle. During collection, organic, attached, and supporting intelligence sources collect and deliver information to the appropriate processing or production unit—or, in some instances, directly to the appropriate commander for immediate action. Effective collection depends upon the use of a variety of mutually reinforcing sources. Necessary, planned redundancy and overlap of sources increase the reliability of information and can reduce the effectiveness of enemy deception or denial efforts.

Processing and exploitation is the third phase of the intelligence cycle, the conversion of raw data into a form suitable for the production of intelligence. Largely a technical function, processing and exploitation converts the data into an understandable form and enhances its presentation. Examples of processing and exploitation include developing and interpreting a piece of film, translating a foreign-language text, or decoding an encrypted radio report. Not all information requires processing; some is collected in a form already suitable for

production. Sometimes processing and exploitation occurs automatically during collection.

The fourth phase of the intelligence cycle is *production*, the activities by which processed data is converted into intelligence. Production involves evaluating the pertinence, reliability, and accuracy of information. It involves analyzing information to isolate significant elements. It includes integrating all relevant information to combine and compare those elements of information with other known information. Finally, production involves interpreting the information to form logical conclusions that bear on the situation and that support the commander's plan to engage the enemy. *Production is a process of synthesis—the most important action in developing usable intelligence for the commander.* Production arranges the intelligence pieces to form coherent images. It is this step which adds meaning to these pieces, creating *knowledge*. Synthesis does not generally create a complete image—totally filling in the gaps and eliminating uncertainty—but it should provide an image from which the commander can reach an acceptable level of understanding. In the end, synthesis answers the all-important question: *"What effect does all of this have on our ability to accomplish the mission?"*

The fifth phase of the intelligence cycle is *dissemination*, the timely conveyance of intelligence in an appropriate form and by a suitable means to those who need it. Depending on

its importance and time-sensitivity, intelligence may be disseminated—*"pushed"*—directly to users, or it can be sent to an accessible data base from which commanders can *"pull"* that intelligence which they need (see figure 3). Intelligence flows by any number of channels or methods. The form intelligence takes can influence dissemination. Some intelligence can be transmitted almost instantaneously to multiple users via a digital communications link, while other intelligence must be physically delivered by courier. The channel or means of dissemination is less important than the arrival of the intelligence at the proper destination on time and in a form readily usable to the commander. Depending on the urgency and time-sensitivity of the intelligence, it may follow established communications channels, or it may be broadcast to the entire force simultaneously as an alert or alarm.

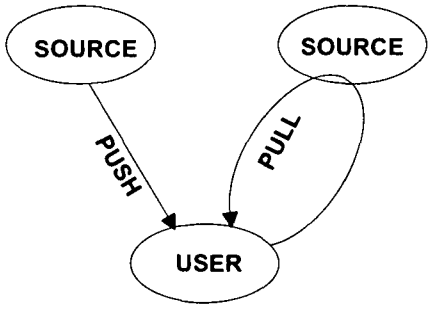


Figure 3.

The final phase in the intelligence cycle is *utilization*. The commander may provide direction, information may be collected and converted into intelligence, and the intelligence may be disseminated, but unless that intelligence is exploited through decision and action, it has served no purpose. Utilization is not a function of intelligence per se, but rather of command and control—making the decision and then carrying it out. This reinforces two important points made earlier: first, intelligence has no value for its own sake but assumes value only when acted upon; and secondly, intelligence is inextricably linked to command and control.

No one phase of the intelligence cycle is more important than the others—they are interdependent. Without proper direction, the other phases will be uncoordinated and ineffective. Without effective collection, there may be too much or too little information, and the information obtained may prove irrelevant. Without processing and production, the resulting mass of information may appear meaningless. Lengthening production time will delay dissemination. The first four phases of the intelligence cycle offer marginal value unless the intelligence arrives to the right person in time and in a useful form to support decisionmaking. Finally, intelligence operations are wasted if commanders fail to understand and act upon the knowledge intelligence offers. For simplicity, the intelligence cycle is described as a sequential method; however, in practice, it is a dynamic process responsive to changes in the situation and the commander's evolving intelligence needs.

A CASE STUDY: VIETNAM 1972

The method used to produce the U.S.'s intelligence assessment of North Vietnam's intentions for 1972 provides an example of the intelligence concepts discussed in this chapter.[15] Forecasting the scope and intensity of the North Vietnamese Army (NVA) and Viet Cong (VC) operations within South Vietnam after the southwest monsoon season ended was the intelligence challenge.[16]

In seeking answers to these questions, intelligence analysts focused on a few key aspects of NVA and VC capabilities. The NVA logistics system often provided a reliable indicator of future activity. The level of NVA resupply activity usually reflected the scope and intensity of planned military operations. A related question was to determine the number of North Vietnamese soldiers moving into South Vietnam and, more specifically, to find out whether these were reinforcements or merely replacements for combat losses of the previous year.

Although there were weaknesses, by 1971 the overall quality of intelligence concerning NVA operations was good. The workings of the enemy's supply system, which had remained relatively unchanged for two decades, were well understood (see figure 4, page 66). Aerial infrared and radar imagery

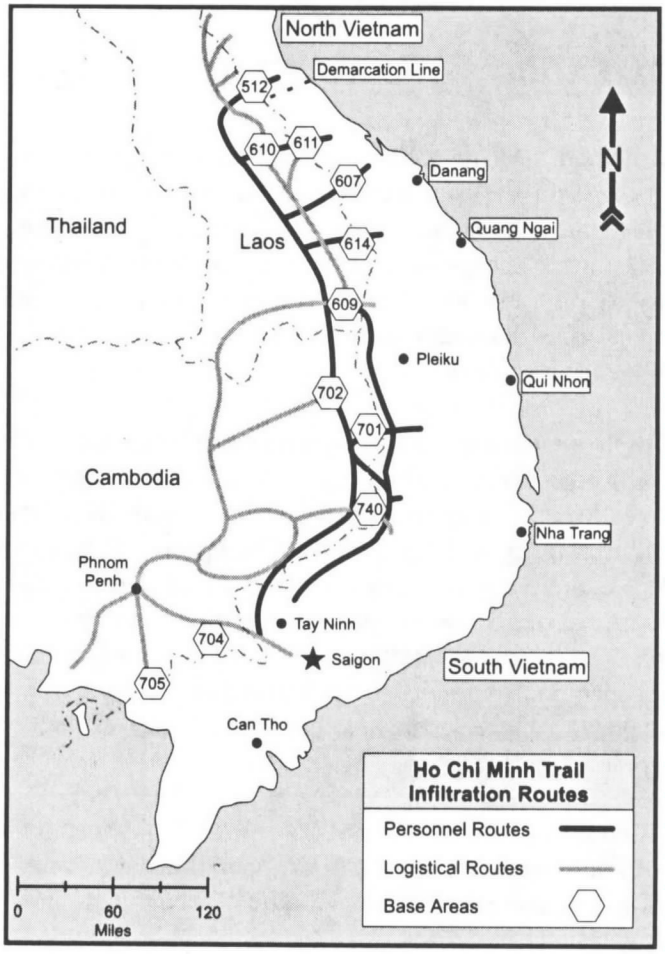

North Vietnam
Demarcation Line
512
610
611
607
Danang
N
Thailand
Laos
614
Quang Ngai
609
Pleiku
Qui Nhon
702
701
Cambodia
740
Nha Trang
Phnom Penh
Tay Ninh
704
Saigon
South Vietnam
705
Can Tho
Ho Chi Minh Trail Infiltration Routes
Personnel Routes
Logistical Routes
Base Areas
0
60
120
Miles

Figure 4.

identified "hot-spots" of activity along the principal NVA resupply route, the Ho Chi Minh trail, and provided indications of the intensity of that activity. Remote ground sensors placed alongside key chokepoints transmitted data on the density and type of vehicular traffic. Long-range ground reconnaissance patrols, signals intelligence, translation of captured documents, and enemy prisoner of war interrogations all helped verify the accuracy of information collected by technical means and improved the overall intelligence picture. There were some problems in the intelligence system as well, one of which was the inability of U.S. intelligence agencies to process, analyze, and synthesize the huge volume of information collected by the technical sensors and other sources.

Analysis of the NVA logistics system did not uncover anything unusual or ominous. As for personnel, they appeared to be predominantly individual replacements with no new NVA or VC units identified. The bottom line of the estimate completed in November 1971 was that 1972 would be "business as usual" without any significant surprises.

By late December, however, new information began to challenge this estimate. The first clues resulted from the analysis of captured documents. A single analyst had detected subtle differences in the tone of South Vietnamese Communist Party documents (which were often filled with hidden messages since the enemy knew some of the documents would be captured) hinting at something big afoot. Shortly thereafter another analyst noted a sudden increase in the flow

of personnel into the south. Further projections showed that if this higher level continued through January, it would greatly exceed numbers needed to replace combat losses.

These two indicators cued new collection operations and a renewed analytical effort. Particularly troubling was a photograph of a tank park located in North Vietnam near the South Vietnamese border. Such a concentration of combat vehicles had never been seen that far south. Finally, additional all-source analysis not only verified continued, unprecedented personnel replacements but also uncovered evidence that two new NVA divisions were headed south and would arrive by late February or early March.

The new intelligence caused a complete overhaul of the previous estimate. The new estimate was published in early January 1972. It concluded that the enemy had the capability to initiate a major escalation of the war during the 1972 dry season, beginning any time after the last week in February, using the equivalent of three new divisions and extensive armor forces. Additional hard intelligence indicated that major attacks would occur from the highlands of central Vietnam south to the delta region.

This revised intelligence estimate provided a minimum of 7 weeks' warning of impending enemy actions. This led to another challenge, one routinely faced by the intelligence professional: the more the user is told, the more the user wants to know. The new intelligence requirement was to determine

more precisely the date the attack would begin. At the same time, operational commanders used the new intelligence to immediately launch an all-out bombing offensive to impede, weaken, or, if possible, destroy the NVA reinforcements. This had the effect of further complicating the intelligence task, as it was impossible to determine what effect the bombing would have on the enemy's plans. The predicted time for the offensive came and went, and the credibility of the estimate began to be challenged.

The bombing had only delayed the attack. On March 30, the NVA and VC launched an unprecedented offensive. Although not as widespread as the 1968 Tet offensive, it brought the commitment of division-sized regular units accompanied by armor and artillery units, some with weapons that outranged those of the U.S. and South Vietnamese. Even with the advance warning, combat actions were prolonged and intense.

Specific indications of the attack were much clearer for the south and central regions of the country and resulted in more effective defensive operations in those regions. Due primarily to the enemy's ability to better conceal his activities in the border region, intelligence did not adequately detect preparations for offensive operations in the northern region. The estimate did not predict major attacks on the north, and the NVA achieved significant successes in the border provinces.

The accuracy and timeliness of the updated January intelligence estimate was a key factor in ultimately repulsing

attacks in the south and central portions of the country. Continuous evaluation of the standing estimate and a willingness on the part of two analysts in particular to challenge conventional wisdom led to this updated assessment. Once initiated, the collection of information from a variety of sources, coupled with in-depth knowledge of the enemy and detailed analysis, provided commanders timely and relevant intelligence they were able to apply to significant advantage.

CONCLUSION

Intelligence strives to build as complete a picture of both the enemy and the area of operations as possible. Such a picture is made up of a variety of factors—the concrete and measurable, the intangible and subjective, the environmental and cultural, the military and political—all of which must be assessed in order to develop the knowledge needed to support the commander's decisionmaking. Building this complete picture requires that we understand and apply the characteristics of good intelligence. Our intelligence picture must be comprehensive; it should combine relevant basic, current, and estimative intelligence from all levels of intelligence. It must include estimates of both capabilities and intentions. Finally, developing an understanding of the situation requires that we be able to distinguish between signals and noise—that we

avoid the pitfalls of bias and preconception while interpreting collected information as objectively as possible.

We employ a variety of conceptual tools to help us in achieving our intelligence objectives. Properly defined intelligence requirements are crucial to providing focus to the intelligence effort. The six intelligence functions outline related tasks which, when accomplished, ensure comprehensive intelligence support to all phases of operational planning and execution. The intelligence cycle provides a process for the development of intelligence. The six steps in the cycle describe a coordinated sequence of activities which results in the production, dissemination, and utilization of accurate, timely, and relevant intelligence.

The object of the intelligence cycle is not to prescribe a procedure which, if successfully applied, will ensure the quality of the intelligence product. The criterion for good intelligence is not whether the different phases have been properly adhered to and whether an accurate, complete, and polished intelligence product has emerged. Likewise, the discussion of the characteristics of good intelligence is not meant as a checklist. These discussions are meant to emphasize that *the sole criterion for good intelligence is whether it provides sufficient knowledge regarding the environment and an understanding of the enemy's capabilities, limitations, and intentions to effectively support the commander's planning and decisionmaking.*

Chapter 3

Creating Effective Intelligence

"To lack intelligence is to be in the ring blindfolded."[1]

—David M. Shoup

"It is refreshing to see things in their proper order—intelligence driving operations, instead of operations driving intelligence . . . As a consequence, we have been able to maintain a constantly high tempo of productive operations."[2]

—Charles E. Wilhelm

Having reached a common understanding of the nature of intelligence and having laid out the main elements of intelligence theory, we can describe the characteristics of effective intelligence. How do we create it within in the Marine Corps?

THE CHALLENGE TO INTELLIGENCE

Before discussing our approach to intelligence, it might be helpful to review the challenges that intelligence faces. What obstacles must intelligence overcome, and what must it accomplish?

Our fundamental premise is that intelligence is not knowledge for its own sake, but instead knowledge for the sole purpose of supporting the commander's decisionmaking needs. Knowledge that cannot be acted upon or that commanders choose to ignore is of little value. Consequently, the Marine Corps recognizes that because intelligence is directly connected to action, it is therefore inseparable from command and operations.

Intelligence attempts to reduce uncertainty about a particular hostile situation. Intelligence is fundamentally an imprecise activity, dealing in estimates and probabilities rather than

certainties. Intelligence must extract meaning from information that is ambiguous, unclear, and sometimes of unknown reliability. It must synthesize disparate information, attempting to create a coherent picture of the enemy and the area of operations. Intelligence should strive to identify enemy centers of gravity and critical vulnerabilities that commanders can exploit. At the same time, it should provide warning of threats to friendly forces.

Intelligence not only provides knowledge of quantitative factors but also, more importantly, affords insight into intangible aspects of the enemy situation such as his goals and motivations. It should not only describe existing conditions and identify enemy capabilities but should also attempt to estimate likely future conditions and enemy intentions. In addition, it should present that knowledge in the form of coherent, meaningful images that are easily assimilated rather than in the form of accumulated lists or texts.

Intelligence strives to answer three basic sets of questions. The first relates to current capabilities and conditions: "What *can* the enemy do? What conditions currently exist?" The second relates to intentions or future conditions: "What *might* the enemy do? What is the enemy *likely* to do? What is the most dangerous thing he may do? What conditions might or are likely to exist in the future?" And the third—and most important—relates to any implications: "What effect might all of this have on our ability to accomplish the mission?"

In short, intelligence must provide the commander with the *practical knowledge that offers exploitable advantages* over the opposition.

INTELLIGENCE IS A COMMAND RESPONSIBILITY

Creating effective intelligence is an inherent and essential responsibility of command. Intelligence failures are failures of command—just as operations failures are command failures.

The Marine Corps' approach to intelligence demands that commanders be personally involved in the conduct of intelligence activities. The commander must specify requirements and provide guidance to ensure a timely and useful product. Commanders must develop an appreciation for the capabilities and limitations of intelligence. This awareness does not mean just an understanding of concepts and theory, but an understanding of the *practical* capabilities and limitations of intelligence personnel, systems, procedures, and products.

The commander begins the process by providing the guidance and direction necessary for the effective conduct of intelligence operations. The commander establishes the priority intelligence requirements that drive collection, production, and dissemination operations. If a commander does not effectively define and prioritize intelligence requirements, the

entire effort may falter. The commander is also required to make the final synthesis of intelligence, arriving at the estimate of the situation which, in turn, serves as the basis for the decision. This is the responsibility of the commander and no one else; while the intelligence officer will provide a recommendation, it is the commander who ultimately determines the meaning of the intelligence provided and how to use it. Additionally, the commander supervises the overall intelligence effort to ensure that the product is timely, relevant, and useful.

Importantly, the commander ensures that intelligence activities support not just the intelligence requirements of the parent unit but the requirements of subordinate commanders as well. The commander should intervene personally when the unit's collection requests or other intelligence support requirements go unsatisfied. Finally, the commander must view the intelligence training of all personnel as a personal command responsibility. This training includes the intelligence awareness of all members of the command as well as the professional development and training of intelligence personnel.

THE COMMAND-INTELLIGENCE CONNECTION

The relationship between the commander and the intelligence officer should be as close as that between the commander and

operations officer. Personal involvement in intelligence does not imply that the commander micromanages the intelligence section or assumes the job of the intelligence officer any more than involvement in operations means that the commander takes over as operations officer. Instead, commanders must provide the guidance and supervision necessary for the intelligence officer to support them while at the same time allowing the intelligence officer sufficient latitude for initiative.

In reality, however, the relationship between a commander and intelligence officer is often more difficult to establish and maintain. One reason is that the commander and operations officer usually have more in common in terms of grade, military occupational specialty, age, and experience. In the perspective of some officers, an operations billet is a prelude to command, and many commanders have previously served tours of duty as operations officers in the very same type of unit they now command. Commanders rarely have had the same sort of practical experience in intelligence billets. Consequently, commanders must promote an environment of cooperation, professional support, and mutual respect between themselves and their intelligence officers in which operations and intelligence officers can work together to execute their commanders' intent.

Intelligence requirements are the commander's requirements and not those of the intelligence officer. The commanding officer must provide early and adequate guidance and revise it when necessary. The commander identifies what

intelligence is needed while the intelligence officer helps in stating the priority intelligence requirements to meet those needs.

The intelligence officer is not simply a researcher waiting for a task from the commanding officer. *An intelligence officer is an operator who understands the intelligence needs of the unit.* The intelligence officer is knowledgeable of the tactical situation and can anticipate the commander's intelligence requirements based on an understanding of the commander's intent and the commander's thought processes. The intelligence officer actively advises the commander on just what intelligence may contribute to success and aggressively carries out intelligence operations to fulfill the intelligence needs of the command.

While the relationship between commander and intelligence officer should be close, they must be careful not to lose their objectivity. The commander and intelligence officer may not always agree on their respective estimates of the hostile situation—this is natural and to be expected. Once the intelligence officer has provided a candid, objective estimate, the commander will assess it and make an independent judgment. Once the commander has made a decision, the intelligence officer must support it fully—while maintaining the detachment necessary to advise the commander if the situation changes or if new evidence indicates that the commander's estimate appears wrong.

During planning and wargaming, the commander will often instruct the intelligence officer to assume the role of an adversary—to attempt to think like the enemy commander—as a means of gaining insights into possible enemy intentions, actions, and reactions. Thus, the intelligence officer often plays the role of devil's advocate, identifying possible ways that the enemy or the environment may interfere with or even defeat friendly plans. In this manner, the intelligence officer helps the commander analyze possibilities and prepare responses to possible developments.

Commanders must exercise caution so as not to judge the effectiveness of intelligence by how accurately it has predicted reality. Commanders must realize that intelligence is the business of estimates, not certainties. A commander harboring unrealistic expectations may discover that the intelligence officer is reluctant to risk any predictions for fear of being wrong. The commander must encourage the intelligence officer to estimate enemy possibilities frankly and not merely provide "safe" facts and figures. Far from being merely a provider of facts and figures—or even a provider of estimates on enemy courses of action—*the intelligence officer should offer trusted advice on friendly courses of action based on knowledge of the hostile situation.*

THE INTELLIGENCE-OPERATIONS CONNECTION

The relationship between intelligence and operations should be as close and direct as that between intelligence and command. In addition to intelligence's influence on the conduct of operations by identifying enemy capabilities and estimating enemy courses of action and possible reactions to friendly courses of action, intelligence also provides important support to operations by helping to identify *friendly critical vulnerabilities* that the enemy may exploit. Thus, the intelligence and operations sections must function in close cooperation throughout the planning and execution of an operation. Neither section can perform effectively without the continuous cooperation of the other.

As in the relationship with the commander, the intelligence officer should cooperate fully with the operations officer but should not develop a personal stake in a particular course of action. Based on knowledge of the hostile situation, the intelligence officer must maintain the freedom to offer advice which disagrees with the advice of the operations staff.[3]

Intelligence officers are themselves operators. The intelligence officer does everything the operations officer does, only in red ink—meaning from the enemy, rather than friendly perspective. The intelligence officer must possess an intimate knowledge of the enemy's methods, capabilities, organizations, and tendencies. At the same time, in order to

effectively plan, coordinate, and execute intelligence operations, the intelligence officer requires an in-depth understanding of friendly tactics, capabilities, and intentions.

The relationship between operations and intelligence necessitates mutual support. Just as intelligence identifies opportunities for exploitation through operations, so can operations provide the stimulus for intelligence. Regardless of the primary mission, all operations have an additional object of gaining information about the enemy and the environment. Some operations possess this goal as the primary mission. For example, the objective of a tactical maneuver such as a reconnaissance in force may be to learn more about enemy capabilities and disposition or to solicit the enemy's reaction to a specific situation.

The importance of the intelligence-operations connection is seen in the contrasting approaches to intelligence used by the Luftwaffe and the Royal Air Force (RAF) during the Battle of Britain. The RAF placed intelligence officers throughout the organization down to the squadron level. Thus aircrews received the latest intelligence during tailored premission briefings, and information collected during combat was immediately available for analysis, dissemination, and utilization. In contrast, the Luftwaffe placed intelligence officers at the wing level only. Intelligence support to flying groups and squadrons was marginal throughout the battle, and its lack contributed to the German defeat.[4]

The direct connection between intelligence and operations results in intelligence shaping or even driving the course of operations. Intelligence operations seek to uncover enemy vulnerabilities we can exploit. Opportunities identified by the intelligence effort are used to develop the concept of operations during planning and to initiate specific tactical actions during execution. Effective intelligence guides us towards enemy weaknesses rather than forcing us to operate against an enemy strength.

The invasion of Tinian during World War II provides an illustration of how intelligence shapes operations. Initial intelligence studies of Tinian identified only one suitable landing area for the amphibious assault. This area was located immediately in front of the island's major settlement, Tinian Town, and was heavily defended by the Japanese. The studies noted the existence of two small inlets on the northern tip of the island but discounted their suitability for a major landing (see figure 5). As planning progressed, new intelligence identified major disadvantages in attacking across the Tinian Town beaches. At the same time, additional studies indicated that a landing on the undefended northern beaches was a viable option. Preassault reconnaissance confirmed the suitability of these beaches. The concept of operations called for regimental-sized landings to be conducted on two small northern beaches (White 1 and White 2) that totaled in width only about 220 yards. The main landing would be supported by an amphibious demonstration conducted near Tinian Town.

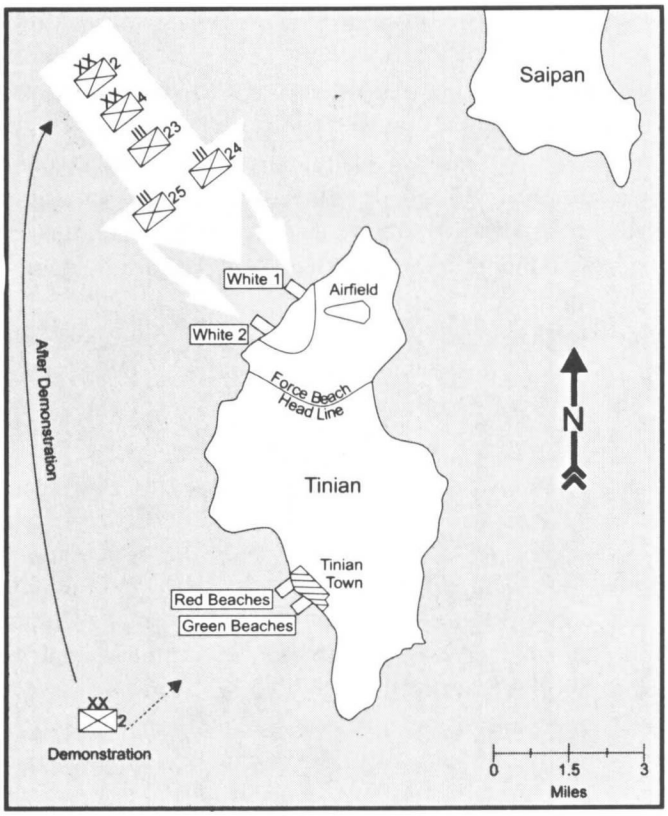


Figure 5.

The amphibious assault achieved complete tactical surprise. Landing against minimal opposition on the northern

beaches, the entire 4th Marine Division was established ashore by the end of the first day. The island was secured in 9 days with minimal casualties suffered by the landing force. The Tinian operation was described by Admiral Raymond Spruance as, "probably the most brilliantly conceived and executed amphibious operation in World War II." Intelligence contributed significantly to the success of this operation, providing commanders with knowledge of a critical vulnerability—the undefended northern beaches—which they exploited to achieve success.[5]

INTELLIGENCE AS A TEAM EFFORT

Intelligence is the commander's responsibility and the intelligence officer's primary duty, but it is also definitely the concern of every Marine. All Marines in the command contribute in one way or another to the intelligence effort. Nearly every Marine, regardless of occupational specialty, has occasion to observe significant facts about the enemy or the environment. Units in contact with the enemy are a particularly valuable source of information. All Marines should consider themselves as potential intelligence sources and, equally important, as counterintelligence assets. Everyone on the battlefield should be alert for important information and bring that information to the attention of the person who needs it by the most direct and expeditious means available.

INTELLIGENCE IS A PRODUCT, NOT A PROVISION

Intelligence is something generated through our own efforts, rather than something provided by some outside source. While we may say that in principle we should have ready access to external sources like satellite imagery, basing our actions on the timely availability of such information is dangerous. Commanders should aim, to the greatest extent possible, to become self-sufficient in satisfying their own intelligence requirements. This approach is particularly important once an operation has commenced. Before operations begin, intelligence from higher echelons may appear to be available in unlimited quantities. However, once execution starts, our organic intelligence and reconnaissance assets generally provide the most reliable and responsive support to Marine units. Marines cannot forget that intelligence is the result of solid headwork and legwork, and it is not provided from some omniscient source of knowledge. Requirements for critical intelligence should be satisfied through organic means whenever possible.

A BALANCED APPROACH

The approach of the Marine Corps to intelligence calls for balance in a number of areas. First is the capability to gather information from a variety of sources. Each source provides a

different type of information. These different sources can compensate for, complement, and confirm one another. Depending on the situation, certain sources will be more valuable than others. Which source we most depend upon in a particular situation is less a matter of our own preference than a matter of the nature and sophistication of the enemy.

Next, balance means that commanders emphasize equally all phases of the intelligence cycle. For example, an overemphasis on collection may result in an overload of information that overwhelms processing and production capacity, thus preventing rapid dissemination. Balance also means that commanders emphasize the development of both classes of intelligence—descriptive and estimative. Balance requires that intelligence personnel work at uncovering both the enemy's capabilities and the enemy's intentions. Balance means that we take into account both quantitative factors—such as numbers, locations, equipment specifications—and qualitative factors—morale, motives, leadership, and cultural values.

Finally, our approach to intelligence should achieve balance in its support to commanders at all levels. At any particular level, the intelligence officer's first duty is to serve the commander's intelligence requirements. However, since questions about the enemy situation and area of operations are practically limitless, an intelligence section can easily spend all its time satisfying intelligence requirements of its own staff or higher headquarters—to the neglect and detriment of subordinate commanders' intelligence needs.

Commanders must provide the necessary guidance to ensure that balance is achieved. Intelligence personnel must remain conscious of the intelligence requirements of all elements of the force with the objective of creating satisfactory intelligence for all supported commanders.

FOCUSING THE INTELLIGENCE EFFORT

Focus, as embodied in the concept of main effort, is central to maneuver warfare. It is particularly critical for intelligence since possible questions about the enemy situation are nearly infinite, while intelligence assets are limited. Commanders must concentrate intelligence operations on those critical requirements upon which mission success depends and prioritize accordingly. *The intelligence effort must support the main effort.* In fact, intelligence is responsible for identifying the enemy's centers of gravity and critical vulnerabilities that are used to determine the main effort.

Focus is a product of direction, which means it is a function of command. The commander provides focus to the intelligence effort by prioritizing intelligence requirements. These requirements establish priorities for all intelligence activities—not only for collection but also for processing, production, and dissemination. The earlier the commander

establishes this guidance, the more focused, timely, and complete the final intelligence product will be.

GENERATING TEMPO THROUGH INTELLIGENCE

Tempo is central to maneuver warfare and our command and control doctrine. We seek to generate a higher operating tempo than that of the enemy. Effective intelligence supports this accelerated tempo. We help create this rapid tempo through a variety of techniques.

First, we generate tempo through *prioritization*. We establish a limited number of priority intelligence requirements that are understood clearly throughout the force. Collection, processing, production, and dissemination operations are conducted in accordance with these priorities. By concentrating on the truly essential requirements, we avoid diluting intelligence operations and clogging dissemination channels with nonessential intelligence.

Another way we use intelligence to accelerate tempo is through *decentralization*—establishing command relationships or task-organizing intelligence assets to directly support subordinate commanders. Decentralizing intelligence resources applies not only to collection assets but to production and dissemination assets as well. Decentralization provides

subordinate elements with the intelligence resources needed to recognize and exploit opportunities as they arise in the battlespace. It also helps ensure intelligence products are tailored to the requirements of commanders at lower echelons. However, decentralization does not mean that intelligence assets will be fully dispersed throughout the force or that each unit will have an equal share of the available intelligence units, systems, or personnel. Since intelligence assets are limited, it is virtually impossible to provide each unit with all the intelligence capabilities its commander may desire. Assets will be allocated based on the commander's intent, the designation of the main effort, and the priority intelligence requirements.

The third technique by which we generate intelligence tempo entails a conscious command decision *to disseminate certain information before it has been fully integrated, analyzed, evaluated, and interpreted*—in other words, before it becomes a comprehensive intelligence product. This approach recognizes that at times a piece of information may be so critical and time-sensitive that it should be disseminated immediately with minimal evaluation and analysis. In a sense, this amounts to decentralizing intelligence production by requiring subordinate units to perform immediate intelligence production. Immediate production rapidly identifies, evaluates, and disseminates intelligence that may have an impact on ongoing operations in order to exploit opportunities and generate tempo. For example, the commander may establish criteria that require the immediate dissemination of any reporting on certain critical enemy targets. The dilemma, which

we must resolve on a case-by-case basis, is between the desire to provide as complete and accurate an intelligence product as possible and the requirement to support the urgency of tactical decisionmaking.

Accessibility is a fourth mechanism by which we may accelerate tempo. Accessibility increases tempo by making intelligence available to commanders for use in decisionmaking. Here we make another conscious command decision—in this case to make intelligence more accessible to users by *minimizing security restrictions or by relying more on open sources*. We can do this by "sanitizing" classified intelligence to protect sources without materially decreasing the value of the intelligence. More important, we should make a conscious effort to ensure that intelligence is classified only to the minimum degree essential to the interests of security.

A fifth way of generating tempo is by ensuring that intelligence products take the *form* most readily understandable by users. This generally means that *intelligence should be presented as meaningful images, rather than reports or lists which require more time to assimilate.* For example, displaying a possible enemy course of action in a graphic with supporting text annotated on the graphic is generally more useful than providing only a text report.

Finally, we can enhance tempo through effective *information management*—taking advantage of all available communication channels and means for disseminating intelligence.

Intelligence, like any other information product, flows not only through established hierarchical channels but also by alarm channels, flowing laterally and diagonally as well as vertically (see figure 6). In other words, rather than simply forwarding information or intelligence via standard channels, we must ask ourselves, "Who really needs this information most?" and transmit that information by the most direct and readily accessible means.

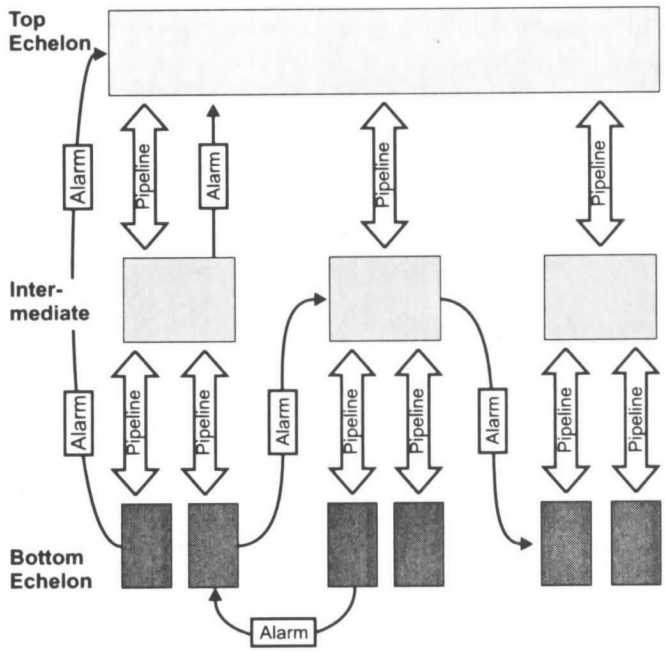


Figure 6.

The ability to generate tempo through intelligence was vividly demonstrated in a series of combat actions during the early years of the Vietnam war. A small number of documents recovered from a Viet Cong commander killed by a Marine ambush patrol identified a likely enemy training base. Using this intelligence, the next day a Marine combined arms assault surprised and effectively destroyed five enemy companies. Immediate searches of the area led to additional intelligence locating another enemy battalion, which was also quickly attacked, causing heavy personnel and material losses. Follow-on all-source intelligence analysis of both engagements swiftly identified the most likely infiltration routes used by these enemy units, allowing a Marine infantry company a few nights later to successfully ambush a reinforced enemy battalion. A few captured documents combined with rapid dissemination and utilization of the resulting intelligence led directly to a series of successful tactical actions.[6]

INTELLIGENCE EDUCATION AND TRAINING

Intelligence education and training are a command responsibility. Professional development programs must give all Marines an understanding of the capabilities and limitations of intelligence as well as the employment of intelligence assets. Education and training should likewise provide intelligence personnel with an in-depth understanding of operations

so that they may better support operations with intelligence. Moreover, education and training programs should seek to strengthen the relationship between intelligence officers and commanders by increasing their mutual understanding.

Commanders must demonstrate personal involvement in intelligence training. They must dedicate adequate training time to it and ensure that intelligence is realistically integrated and balanced with other warfighting activities. The commander is responsible for ensuring that all the unit's Marines have a basic understanding of the threat and the environment in likely areas of deployment. Classroom instruction, professional reading, discussion groups, and use of wargames with realistic scenarios and threat forces are ways to build such knowledge.

Exercises must be used to reinforce and increase the intelligence awareness of the unit. Exercises should incorporate realistic intelligence to the maximum extent possible. This provides participants with the opportunity to identify their intelligence requirements, allows them to see how intelligence is collected, produced, and disseminated, and exposes them to the type and quantity of intelligence support they can expect to receive during actual operations.

The value of incorporating realistic intelligence into exercises was demonstrated during Operation Praying Mantis in

1988. The commander of a Special Purpose Marine Air-Ground Task Force (MAGTF) based his training scenarios on actual intelligence studies of potential raid sites in the Persian Gulf. For the execution of the operation, the MAGTF was directed to attack the "Sassan" gas-oil platform, a target the MAGTF had used in its training exercise the week before. The use of realistic intelligence during training gave the MAGTF commander the necessary background knowledge and situational awareness to rapidly complete the plan.[7]

Opposed, free-play exercises are especially valuable, providing the opportunity to conduct intelligence operations in realistic conditions. To use an intelligence staff to create an exercise scenario, with all the pertinent intelligence already generated in advance, is a misuse of assets. Such a scheme robs an exercise of all-important realism in the development and use of intelligence to support decisionmaking. Within the practical limitations of available resources, "scripted" exercise intelligence should be minimized in favor of intelligence generated during the actual exercise.

In the training and education of intelligence personnel, we seek to achieve a balance between specialization and generalization. *Intelligence officers must possess a broad operational orientation*—an understanding of just how intelligence supports operations in general terms—while also developing the specialized skills required by many intelligence disciplines. We should nurture intelligence officers who can synthesize as well as analyze—who can answer the "So what?" question.

Finally, we should stress the importance of foreign area and foreign language training in order to build our understanding of potential enemies and operating environments.

A CASE STUDY: SOMALIA 1992–1993

In December 1992, lead elements of the 15th Marine Expeditionary Unit landed in Mogadishu, Somalia, initiating Operation Restore Hope, a multinational humanitarian assistance operation. Remaining elements of Marine Forces (MARFOR) Somalia followed shortly thereafter. MARFOR intelligence operations illustrate the importance of a commander's involvement in the intelligence effort and of close coordination between intelligence and operations.[8]

The intelligence situation at the start of Operation Restore Hope was typical of what can be anticipated for most military operations other than war, particularly from the tactical perspective: outdated basic intelligence, sketchy current intelligence regarding the order of battle, capabilities, intentions, and vulnerabilities of potential threat forces, and limited understanding of possible reactions from either the civilian populace or the many nongovernmental organizations long operating in the country.

From the beginning, the commander ensured that MARFOR intelligence and operations elements worked as a team. The commander set the direction for MARFOR intelligence operations by focusing the collection and production efforts. During the initial stabilization phase of operations, intelligence requirements were focused on the organization and leadership of the Somalian clans, boundaries between the clans, and the locations of meeting places, weapons caches, and arms markets. Both intelligence and operations personnel worked to acquire information and develop understanding of the nongovernmental organizations, the status of the local infrastructure, and the cultural aspects of the local population. During the subsequent normalization phase of the operation, intelligence priorities shifted to requirements in support of the civil affairs effort: preserving freedom of movement and commerce throughout the country, determining the effectiveness of civilian authorities, and estimating the attitudes of the clans and the average Somali to U.S. and U.N. efforts.

Collection operations reflected the unique challenges of the humanitarian assistance mission. A considerable amount of information was acquired from foot, motorized, and mechanized patrols. Helicopter visual reconnaissance missions and postmisson debriefs typically provided timely confirmation of information acquired during patrols. The MARFOR's principal human intelligence resources, its counterintelligence and interrogator-translator teams, were exceptionally effective in this environment.

Counterintelligence specialists and interrogator-translators were routinely attached to or placed in direct support of units down to battalion and regimental level. Their immediate availability and integration into unit intelligence collection and other operational activities allowed intelligence officers to rapidly develop pertinent tactical intelligence. In most instances, intelligence was immediately provided to and acted upon by MARFOR operational elements. When more complex targets were identified, intelligence was used to plan and execute sophisticated direct action missions. The effective development and use of intelligence led to the capture of hundreds of weapons and tons of ammunition and supplies. Intelligence contributed directly to the establishment of a secure environment for the conduct of relief activities.

The MARFOR commander characterized human intelligence operations as "providing in-by-nine, out-by-five service on priority intelligence requirements. As a consequence, we have been able to maintain a constantly high tempo of productive operations. The key word here is productive. Patrols, checkpoints, and direct action missions have, for the most part, been directed against clearly defined targets—there have been remarkably few dry holes."[9]

CONCLUSION

The Marine Corps' philosophy of intelligence recognizes that intelligence is an inherent responsibility of command. The commander's direct involvement is required to provide appropriate guidance to the intelligence effort and ensure the full utilization of the intelligence product. Our philosophy also acknowledges that intelligence is inseparable from operations and that effective intelligence shapes or even drives operations. Without close and continuous cooperation, neither intelligence nor operations can function effectively.

Our intelligence philosophy relies on a variety of sources, does not emphasize one phase of intelligence activity at the expense of another, and provides support to all levels of the force. This approach recognizes the importance of qualitative as well as quantitative information requirements. It focuses on priority intelligence requirements, seeking to avoid diffusion of effort. The Marine Corps' intelligence philosophy acknowledges the importance of tempo and uses effective intelligence operations to develop and maintain tempo. Finally, this approach to intelligence recognizes that the obtaining of useful information about an adversary is a team effort and requires that all Marines see themselves as intelligence and counterintelligence resources contributing actively to the intelligence effort.

The Nature of Intelligence

1. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963) p. 129.

2. Stedman Chandler and Robert W. Robb, *Front-Line Intelligence* (Washington, D.C.: Infantry Journal Press, 1946) p. 7. Available to Marine units as FMFRP 12-16, *Front-Line Intelligence.*

3. Erwin Rommel, *The Rommel Papers,* ed. B. H. Liddell Hart, trans. Paul Findlay (New York: Harcourt, Brace, 1953) p. 122.

4. The surrounding environment includes weather, terrain, transportation network, local population, and any other factors needed to describe a potential area of employment.

5. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1966) p. 3.

6. For a detailed explanation of the distinction between data, information, knowledge, and understanding, see MCDP 6, *Command and Control* (October 1996) pp. 66–71.

7. Wayne M. Hall, "Intelligence Analysis in the 21st Century," *Military Intelligence* (January-March 1992) p. 9 and Richard K. Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *Power, Strategy, and Security*, ed. Klaus Knorr (Princeton, NJ: Princeton University Press, 1983) p. 211.

8. Kent, *Strategic Intelligence for American World Policy*, p. 180.

9. Nancy Gibbs, "A Show of a Strength," *Time* (October 1994) pp. 34–38.

10. Sherman Kent, "Estimates and Influence," *Foreign Service Journal* (April 1969) p. 17.

11. Principal sources used in this case study: *Conduct of the Persian Gulf War: Final Report to Congress* (Washington, D.C.: Department of Defense, April 1992); Col Charles J. Quilter, II, *U.S. Marines in the Persian Gulf, 1990–1991: With the I Marine Expeditionary Force in Desert Shield and Desert Storm* (Washington, D.C.: Headquarters, U.S. Marine Corps, History and Museums Division, 1993); LtCol Charles H. Cureton, *U.S. Marines in the Persian Gulf, 1990–1991: With the 1st Marine Division in Desert Shield and Desert Storm* (Washington, D.C.: Headquarters, U.S. Marine Corps, History and Museums Division, 1993) pp. 46; Dennis P. Mroczkowski, *U.S. Marines in the Persian Gulf, 1990–1991: With the 2d Marine Division in Desert Shield and Desert Storm* (Washington, D.C.: Headquarters, U.S. Marine Corps, History and Museums Division, 1993); Interview with Maj-Gen J. M. Myatt, USMC, "The 1st Marine Division in the Attack," *Proceedings* (November 1991) pp. 71–76; Interview 4 Nov 96 with LtCol David Hurley and Mr. Michael H. Decker conducted by Maj Emile Sander (during Operation Desert Shield/Desert Storm, LtCol Hurley served as the officer in charge of the I MEF MAGTF all-source fusion center, while then Capt Decker served as the MAGTF all-source fusion center, Chief Intelligence Analyst).

Intelligence Theory

1. Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984) p. 117.

2. Gen Carl E. Mundy, Jr., "Reflections on the Corps: Some Thoughts on Expeditionary Warfare," *Marine Corps Gazette* (March 1995) p. 27.

3. Maj David L. Shelton, "Intelligence Lessons Known and Revealed During Operation Restore Hope Somalia," *Marine Corps Gazette* (February 1995) pp. 37–40; Capt David Rababy, "Intelligence Support During a Humanitarian Mission," *Marine Corps Gazette* (February 1995) pp. 40–42; LtCol David Shelton, "Intelligence Lessons Known and Revealed During Operation United Shield in Somalia," unpublished manuscript.

4. Richard K. Betts, *Surprise Attack: Lessons for Defense Planning* (Washington, D.C.: Brookings Institution, 1982) pp. 56–62. See also Edwin P. Hoyt, *The Bloody Road to Panmunjorn* (New York: Military Heritage Press, 1985) pp. 17, 31, 45–47, 54–59.

5. U.S. Department of Defense, *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983* (Washington, D.C.: December 20, 1983) pp. 64–66.

6. The senior military intelligence officer in Vietnam at the time of the Tet offensive later declared, "Even had I known exactly what was to take place, it was so preposterous that I probably would have been unable to sell it." Jack Shulimson, *TET–1968* (New York: Bantam Books) p. 45. See also Don Oberdorfer, *Tet!* (New York: Da Capo Press, 1984) pp. 117–121.

7. For a full discussion of signals and noise, see Roberta Wohlstetter, "Cuba and Pearl Harbor: Hindsight and Foresight," *Foreign Affairs* (July 1965) pp. 691–707.

8. Clausewitz, p. 101.

9. Betts, *Surprise Attack: Lessons for Defense Planning*, pp. 68–80.

10. Ephraim Kam, *Surprise Attack: The Victim's Perspective* (Cambridge, MA: Harvard University Press, 1988).

11. The terms *priority intelligence requirement* (PIR) and *intelligence requirement* (IR) replace the terms *essential elements of information* (EEI) and *other intelligence requirements* (OIR) to correspond to joint doctrinal terminology. Priority intelligence requirements are a subset of *commander's critical information requirements* (CCIRs), a term used to describe the information and intelligence requirements a commander deems critical to mission success. CCIRs are discussed in FMFM 6-1, *The Marine Division* (to be redesignated as MCWP 3-11.1).

12. Interview with LtCol Dwight Trafton, Intelligence Officer, 24th Marine Expeditionary Unit, December 30, 1996, conducted by LtCol J. D. Williams.

13. Specific security guidelines—particularly restrictions and information classification guidance—are often dictated by higher echelon commanders in pertinent directives, operation orders, or classification guides.

14. For information on the use of signals intelligence during World War II, see David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: New American Library, 1973); F. W. Winterbotham, *The Ultra Secret* (New York, Harper & Row, 1974); Ronald Lewin, *Ultra Goes to War: The First Account of World War II's Greatest Secret Based on Official Documents* (New York: McGraw-Hill, 1978). For a discussion of the operation against Admiral Yamamoto, see Kahn, pp. 332–338.

15. The principal source used in this case study is Col Peter F. C. Armstrong, USMC (Ret.), "Capabilities and Intentions," *Marine Corps Gazette* (September 1986) pp. 38–47. Additional information was taken from Stanley Karnow, *Vietnam: A History* (New York: Penguin Books, 1984) pp. 639–641.

16. The southwest monsoon season ran from mid-March to mid-September, flooding much of the South Vietnamese delta while turning the Laos and Vietnamese highlands into a quagmire nearly impassable to heavy vehicles. As a result, major military operations could not begin until the ground had dried, normally in December.

Creating Effective Intelligence

1. Gen David M. Shoup, USMC, in Robert Debs Heinl, Jr., *Dictionary of Military and Naval Quotations* (Annapolis, MD: United States Naval Institute, 1966) p. 161. Gen Shoup was the 22nd Commandant of the Marine Corps.

2. MajGen Charles E. Wilhelm, Commander, Marine Forces, Somalia, Situation Report for January 24, 1993.

3. Kent, *Strategic Intelligence for American World Policy*, p. 198.

4. LtCol David Ingram, " 'Fighting Smart' with ACE Intelligence," *Marine Corps Gazette* (May 1989) pp. 38–40. See also Len Deighton, *Fighter: The True Story of the Battle of Britain* (New York: Harper Paperbacks, 1994).

5. Maj Carl Hoffman, *The Seizure of Tinian* (Washington, D.C.: Headquarters, U.S. Marine Corps, Historical Division, 1951).

6. FMFRP 12-40, *Professional Knowledge Gained from Operational Experience in Vietnam, 1965–1966* (September 1991) pp. 139-141.

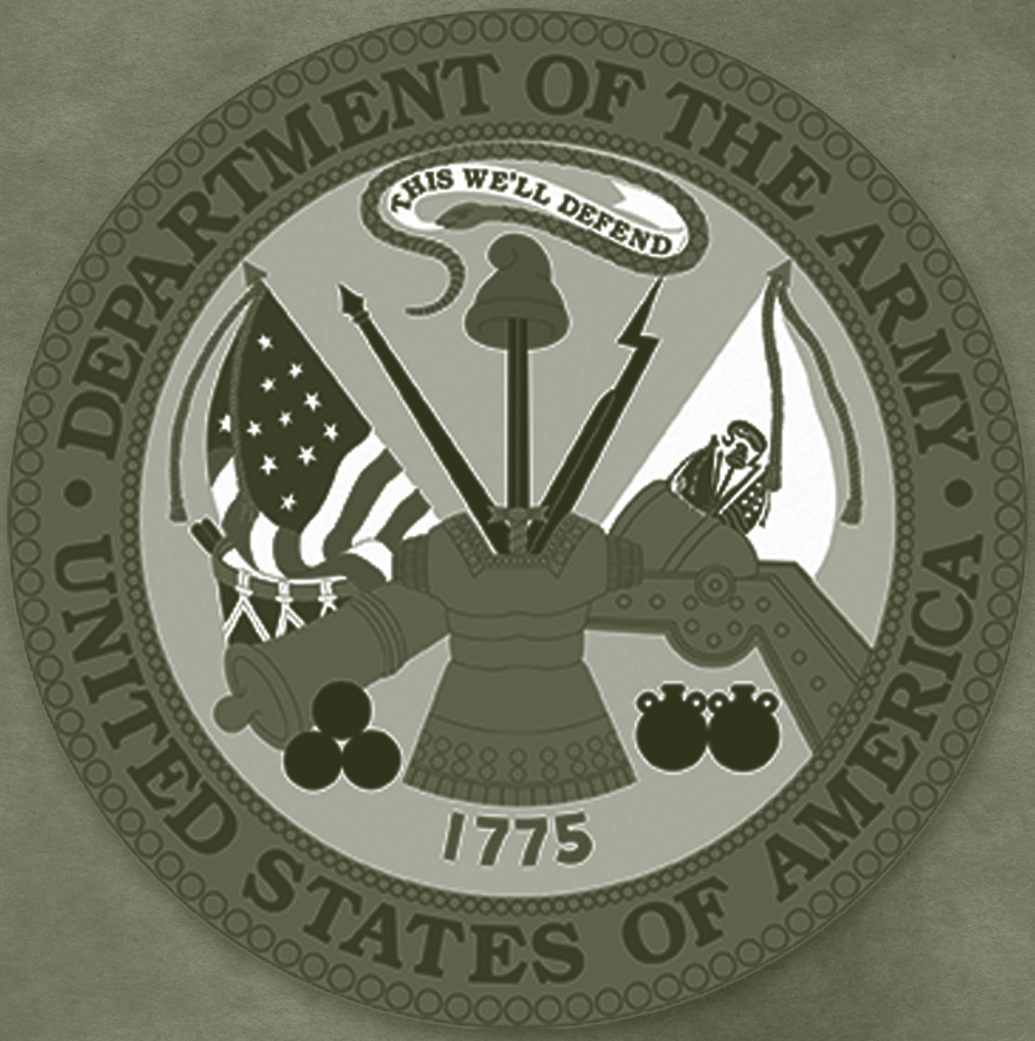
7. Col William M. Rakow, "Marines in the Gulf–1988," *Marine Corps Gazette* (December 1988) pp. 62–68.

8. Principal sources used in this case study are Shelton, "Intelligence Lessons Known and Revealed During Operation Restore

Hope Somalia"; Rababy, "Intelligence Support During a Humanitarian Mission"; Shelton, "Intelligence Lessons Known and Revealed During Operation United Shield in Somalia"; and Award Recommendation for Marine Forces Somalia Counterintelligence/ HUMINT teams, Department of Defense HUMINT Awards Recognition Program, Headquarters Marine Corps, Assistant Chief of Staff, C^4I, September, 1993.

9. MajGen Charles E. Wilhelm, Commander, Marine Forces, "Operation Restore Hope," Situation Report, 24 January 1993.

ADP 2-0
INTELLIGENCE



SEPTEMBER 2018

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes ADP 2-0 and ADRP 2-0, both dated 31 August 2012.

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil/), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

Forward

The future for our Army is challenging. In order to prepare for an unknowable future, the Army must be ready to conduct the full range of military operations, with a focus on large-scale combat operations. The Army will operate across multiple domains with unified action partners. We must deploy and transition rapidly to large-scale combat operations, present multiple dilemmas to the enemy, operate dispersed while maintaining decisive effects, and consolidate gains.

Intelligence, especially warning intelligence and other aspects of setting the theater of operations, is integral to operations, as the theater army competes with peer threats below the level of armed conflict. Friendly forces attempt to maintain an enduring initiative during operations to shape and prevent. However, enemies are likely to initiate hostilities against friendly forces from initial positions of relative advantage.

Therefore, Army forces will conduct operations across multiple domains to gain freedom of action for other members of the joint force. Units must be prepared to fight for intelligence against a range of threats, enemy formations, and unknowns. These challenges include integrated air defense systems and long-range fires, counterreconnaissance, cyberspace and electronic warfare operations, deception operations, and camouflage.

These complexities place a significant demand on intelligence professionals for real-time detailed intelligence to develop situational understanding and answer the commander's priority intelligence requirements. Intelligence enables mission command, facilitates initiative, and allows commanders and staffs to execute tailored solutions for complex problems in the fast-paced environments of the future. From this understanding, commanders can better identify windows of opportunity during operations to converge capabilities for best effect. Ready access to the intelligence networks facilitates timely decision making and provides commanders the flexibility to successfully shape and execute operations.

ADP 2-0, Intelligence, provides a common construct for intelligence support in complex operational environments and a framework to support unified land operations across the range of military operations. This publication serves as the intelligence doctrinal foundation for our Army. Every Army professional must understand the doctrinal principles of Army intelligence.

ROBERT P. WALTERS, JR.
MAJOR GENERAL, UNITED STATES ARMY
COMMANDING

This page intentionally left blank.

*ADP 2-0

Army Doctrine Publication
No. 2-0

Headquarters
Department of the Army
Washington, DC, 4 September 2018

Intelligence

Contents

Page

PREFACE ..... **iii**

INTRODUCTION ..... **vii**

Chapter 1 **OPERATIONS AND INTELLIGENCE** **1-1**
Large-Scale Combat Operations 1-1
The Operational Environment 1-2
Threats and Hazards 1-4
Unified Action and Joint Operations 1-5
The Army's Strategic Roles 1-6
Unified Land Operations 1-6

Chapter 2 **INTELLIGENCE SUPPORT** **2-1**
The Purpose of Intelligence 2-1
The Intelligence Warfighting Function 2-2
National to Tactical Intelligence 2-6

Chapter 3 **THE INTELLIGENCE PROCESS** **3-1**
The Operations Process and the Intelligence Process 3-1
Commander's Guidance 3-3
Intelligence Process Steps 3-3
Intelligence Process Continuing Activities 3-8

Chapter 4 **ARMY INTELLIGENCE CAPABILITIES** **4-1**
All-Source Intelligence 4-1
Single-Source Intelligence 4-2

Chapter 5 **FIGHTING FOR INTELLIGENCE** **5-1**
The Challenge 5-1
The Commander's Role and Staff Integration 5-2
Planning Considerations and Information Requirements 5-5
The Information Collection Plan and the Intelligence Architecture 5-8
Developing the Situation and Continuous Information Collection 5-9

GLOSSARY **Glossary-1**

REFERENCES **References-1**

INDEX **Index-1**

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes ADP 2-0 and ADRP 2-0, both dated 31 August 2012.

Figures

Introductory figure. ADP 2-0 logic chart viii
Figure 1-1. The conflict continuum and the range of military operations 1-1
Figure 1-2. The Army's strategic roles and their relationship to the joint phases 1-6
Figure 2-1. Intelligence across the echelons 2-10
Figure 3-1. The intelligence process 3-2
Figure 3-2. Requirements development 3-4

Tables

Introductory table 1. New and modified Army terms xi
Table 1-1. Decisive action 1-8
Table 2-1. Overview of intelligence warfighting function tasks 2-3
Table 5-1. Intelligence support to targeting 5-3

Preface

ADP 2-0 is the Army's most fundamental publication for Army intelligence. ADP 2-0 provides a common construct for intelligence doctrine from which Army forces adapt to conduct operations. ADP 2-0 augments and is nested with the capstone doctrine from both ADRP 3-0 and FM 3-0.

The principal audience for ADP 2-0 is every Soldier and Department of the Army Civilian who interact with the intelligence warfighting function. This publication is the foundation for the intelligence warfighting function and subsequent doctrine development. It also serves as a reference for personnel who are developing doctrine, leader development, materiel and force structure, and institutional and unit training for intelligence.

Note. The Army does not have a specific military occupational specialty for open-source intelligence; it does not have base tables of organization and equipment for open-source intelligence units or staff elements.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (U.S.), international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See the Department of Defense [DOD] Law of War Manual, CJCSI 3121.01B, and FM 27-10.)

This publication contains copyrighted material.

ADP 2-0 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ADP 2-0 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Definitions for which ADP 2-0 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

ADP 2-0 applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve unless otherwise stated.

The proponent of ADP 2-0 is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Directorate of Doctrine and Intelligence Systems Training, U.S. Army Intelligence Center of Excellence, Fort Huachuca, Arizona. Send comments and recommendations on a DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Intelligence Center of Excellence, ATTN: ATZS-DST-D (ADP 2-0), 550 Cibeque, Fort Huachuca, AZ, 85613-7017; by e-mail to usarmy.huachuca.icoe.mbx.doctrine@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Acknowledgement

The critical thinking material in paragraph 2-30 has been used with permission from the Foundation for Critical Thinking, www.criticalthinking.org, *The Thinker's Guide to Analytic Thinking*, 2017, and *The Miniature Guide to Critical Thinking: Concepts and Tools*, 2014, by Dr. Linda Elder and Dr. Richard Paul. The copyright owners have granted permission to reproduce material from their works. With their permission, some of the text has been paraphrased and adapted for military purposes.

This page intentionally left blank.

Introduction

KEY DOCTRINAL CONCEPTS

Operations and intelligence are closely linked. The intelligence process is continuous and directly drives and supports the operations process. This principle will remain true well into the future. Intelligence will continue to be a critical part of the conduct—planning, preparing, executing, and assessing—of operations. Future operations will be difficult. They will occur in complex operational environments against capable peer threats, who most likely will start from positions of relative advantage. U.S. forces will require effective intelligence to prevail during these operations.

Intelligence supports joint and Army operations across unified action, the Army's strategic roles, unified land operations, and decisive action at each echelon—from the geographic combatant command down to the battalion level. Specifically, intelligence supports commanders and staffs (through mission command) by facilitating situational understanding across all domains and the information environment. Commanders and staffs use situational understanding to identify and exploit multi-domain windows of opportunity and to achieve and exploit positions of relative advantage.

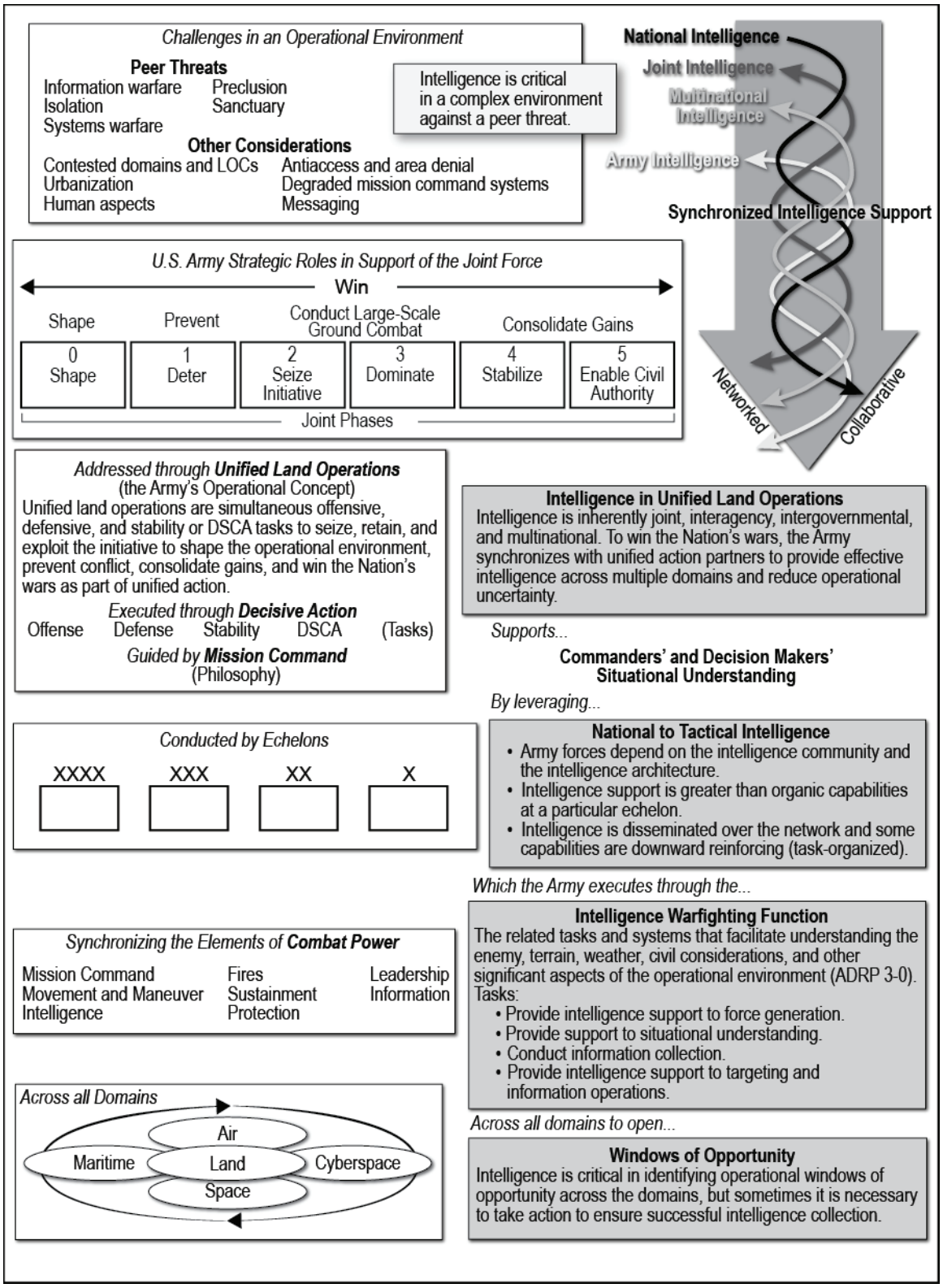
Intelligence is inherently joint, interagency, intergovernmental, and multinational. Every aspect of intelligence is synchronized, networked, and collaborative across all unified action partners. This synchronization occurs through national to tactical intelligence support. The Army both benefits from and contributes to national to tactical intelligence and focuses the Army intelligence effort through the intelligence warfighting function, which is larger than military intelligence. Critical participants within the function include commanders and staffs, decision makers, collection managers, and intelligence leaders.

Despite a thorough understanding of intelligence fundamentals and a proficient staff, an effective intelligence effort is not assured. Large-scale combat operations are characterized by complexity, chaos, fear, violence, fatigue, and uncertainty. The fluid and chaotic nature of large-scale combat operations causes the greatest degree of fog, friction, and stress on the intelligence warfighting function. Threat forces will attempt to counter friendly collection capabilities by using integrated air defense systems, long-range fires, counterreconnaissance, cyberspace and electronic warfare operations, camouflage and concealment, and deception.

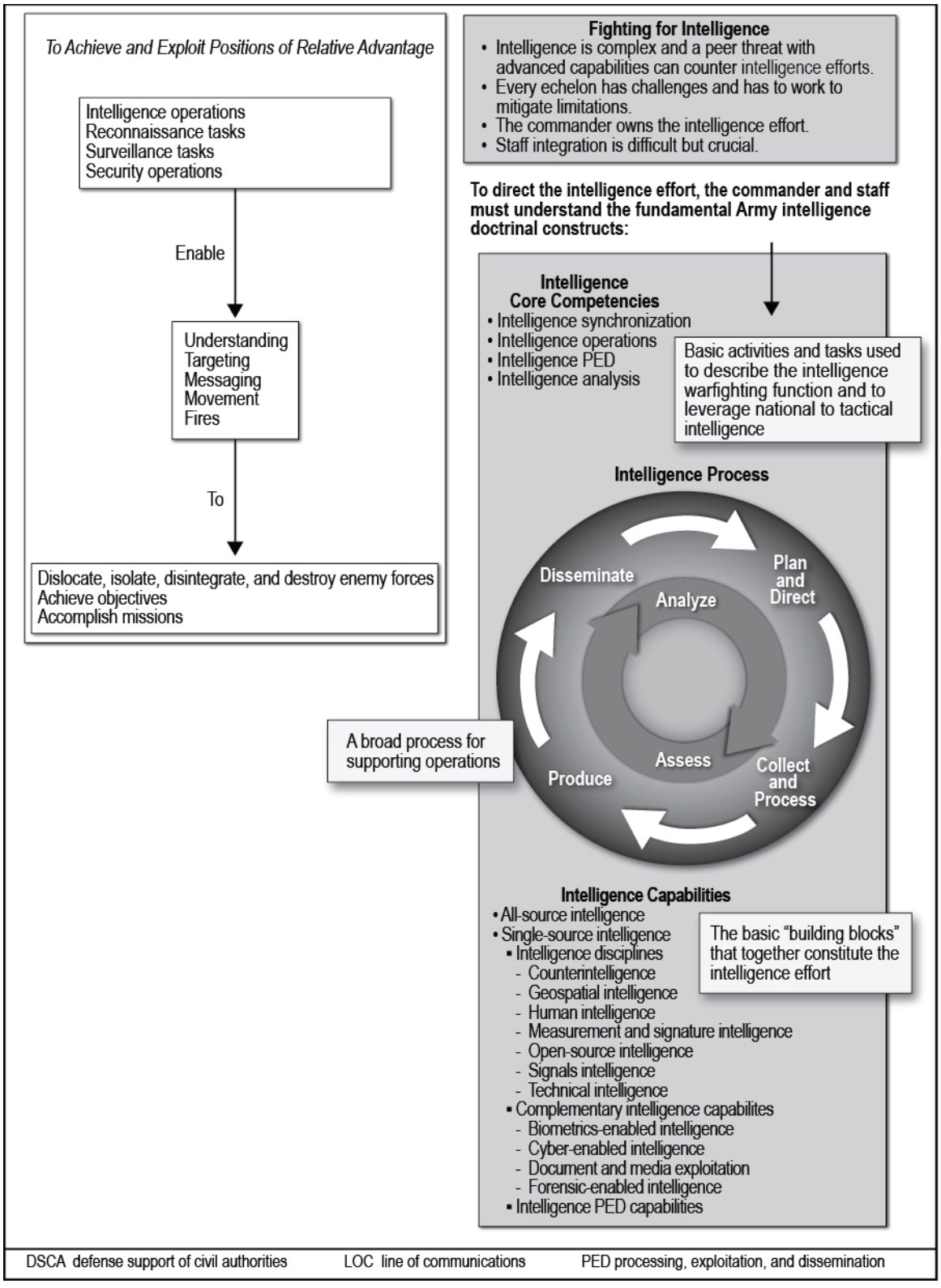
Ensuring an effective intelligence effort is a challenge described as fighting for intelligence. The following aspects of fighting for intelligence are critical:

- Effective intelligence requires developing an effective intelligence architecture well before large-scale combat operations.
- The commander must own the intelligence effort.
- The commander and staff—
  - Must forge an effective relationship and excel in staff integration.
  - Must understand intelligence limitations, especially collection gaps, at their echelon and overcome or mitigate those limitations through effective information collection.
  - At times, may have to conduct combat operations or find creative solutions to enable information collection.
- The unit must adjust the information collection plan, adapt to threat counter-collection measures, and maintain a layered and aggressive information collection effort.

The introductory figure on pages viii and ix illustrates the nesting of intelligence with operations.



Introductory figure. ADP 2-0 logic chart



Introductory figure. ADP 2-0 logic chart (*continued*)

EXECUTIVE SUMMARY

This version of ADP 2-0 marks a significant departure from the August 2012 versions of ADP and ADRP 2-0. The publication was deliberately changed to nest ADP 2-0 with FM 3-0 and to help focus the Army on the new challenges associated with large-scale combat operations. Despite the change in focus, the intelligence fundamental concepts remain but with some modifications.

This executive summary highlights the most important aspects of each chapter and the most significant changes from the last version. Additionally, each bullet includes the page number (in parenthesis) where that topic is discussed in this publication.

ADP 2-0 contains five chapters:

Chapter 1 discusses how intelligence nests with the most fundamental operational doctrinal concepts. In order to understand Army intelligence, it is important to understand intelligence within the larger context of FM 3-0. From national and DOD levels down to the Army battalion level, intelligence is an activity that is never at rest. Army forces are globally engaged, always executing operations and preparing for future operations as part of a joint team.

This chapter—

- Provides an overview of—
  - Large-scale combat operations. (1-1)
  - Unified action and joint operations. (1-5)
  - The Army's strategic roles. (1-6)
  - Unified land operations. (1-6)
  - Decisive action with subordinate discussions on the offense, defense, stability, and defense support of civil authorities. (1-7)
- Updates discussion of the operational environment. (1-2)
- Updates the discussion of the threat. (1-4)
- Discusses intelligence support within *multi-domain operations*. (1-10)

Chapter 2 discusses the most fundamental intelligence doctrinal concepts. Intelligence support is critical to operations and occurs at each echelon, from theater army down to the battalion level. In order to drive intelligence, the commander and staff must understand the intelligence warfighting function, the intelligence core competencies, national to tactical intelligence, setting the theater, and establishing the intelligence architecture.

This chapter—

- Discusses the *purpose of intelligence.* (2-1)
- Updates the discussion of the *intelligence warfighting function.* (2-2)
- Updates the description of the *intelligence core competencies* and introduces *intelligence processing, exploitation, and dissemination (PED)* as a fourth intelligence core competency. (2-4)
- Introduces PED as a term and updates the PED discussion to include intelligence PED. (2-5)
- Introduces *national to tactical intelligence*, which replaces the discussion of *intelligence enterprise* from the August 2012 version of ADRP 2-0. (2-6)
- Introduces and discusses *regionally aligned forces* and *setting the theater* for intelligence in Army forces. (2-8)
- Introduces and discusses *establishing the intelligence architecture* as a capability. (2-8)

Chapter 3 discusses the most important intelligence doctrinal construct—the intelligence process. The intelligence process is a model that describes how the intelligence warfighting function facilitates situational understanding and supports decision making. This process provides a common framework for Army professionals to guide their thoughts, discussions, plans, and assessments.

This chapter—

- Discusses how the *operations process* and *intelligence process* nest. (3-1)
- Discusses the *plan and direct* step. (3-3)

- Modifies the *collect* step to the *collect and process* step, and includes a new figure depicting the revision of the intelligence process. (3-5)
- Discusses the *produce* step. (3-6)
- Discusses the *disseminate* step. (3-6)
- Discusses the *analyze* continuing activity. (3-8)
- Discusses the *assess* continuing activity. (3-8)

Chapter 4 discusses the key capabilities by which the intelligence warfighting function facilitates situational understanding and supports decision making. The intelligence warfighting function executes the intelligence process by employing intelligence capabilities. These key capabilities (building blocks) are all-source intelligence and single-source intelligence. Single-source intelligence comprises the intelligence disciplines, complementary intelligence capabilities, and PED capabilities.

This chapter—

- Updates the discussion of *all-source intelligence* and introduces *identity activities* as an all-source effort. (4-1)
- Updates the discussion of the *intelligence disciplines.* (4-2)
- Updates the discussion of the *complementary intelligence capabilities.* (4-10)
- Replaces the discussion of *PED* with new material found in chapter 2. (2-5)
- Discusses *intelligence PED capabilities* that support information collection. (4-12)

Chapter 5 culminates this publication with an important discussion of fighting for intelligence. Intelligence is never perfect, information collection is never easy, and a single collection capability is never persistent and accurate enough to provide all of the answers. The fluid and chaotic nature of large-scale combat operations will cause the greatest degree of fog, friction, and stress on the intelligence warfighting function. Units must be prepared to fight for intelligence against enemy formations, a range of sophisticated threat capabilities, and many unknown conditions within the operational environment.

This chapter—

- Discusses *fighting for intelligence* during large-scale combat operations, with emphasis on the intelligence challenge. (5-1)
- Updates the description of the *commander's role in intelligence,* including *intelligence and the integrating processes and continuing activities.* (5-2)
- Discusses *planning considerations* and *information requirements* to support the defense and offense, reconnaissance, security operations, and deep operations. (5-4)
- Discusses unique aspects of *developing a flexible information collection plan* and *establishing an effective intelligence architecture.* (5-8)
- Updates the discussion on the continuous nature of information collection. (5-9)

NEW, RESCINDED, AND MODIFIED TERMS

ADP 2-0 becomes the proponent of one Army term, introduces two new Army terms, and modifies three Army terms. (See introductory table 1.)

Introductory table 1. New and modified Army terms

Term	*Remarks*
human intelligence	ADP 2-0 becomes the proponent.
intelligence enterprise	Replaced by national to tactical intelligence.
intelligence processing, exploitation, and dissemination	Modified description.
intelligence operations	Modified definition.
intelligence reach	Modified definition.
intelligence synchronization	Modified definition.
processing, exploitation, and dissemination	New term.

Notes. This publication uses the term *commander's critical information requirements and other requirements* when referring to information collection activities. When referring to the intelligence warfighting function or intelligence analysis, the more specific term, *priority intelligence requirements and other requirements* applies.

Acronyms are introduced at their first use in the front matter of this publication (preface and introduction), and again in the body of the publication (chapters 1 through 5).

ADP 2-0 introduces G-*X* and S-*X* (such as G-2 and S-2) acronyms at their first use without defining them as it hinders readability. Definitions for these acronyms can be found in the glossary of this publication.

Chapter 1

Operations and Intelligence

Throughout modern history, intelligence has been and remains an inherent part of military operations. From national and Department of Defense (DOD) levels down to the Army battalion level, intelligence is an activity that never stops. Army forces are globally engaged, always executing operations and preparing for future operations as part of a joint team. A key part of global engagement is the continuous use of intelligence, the collection and analysis of information, and the production of intelligence. This constant activity, referred to as intelligence, is never at rest. To understand Army intelligence, it is important to understand intelligence within the larger context of large-scale combat operations, the operational environment, unified action, the Army strategic roles, and unified land operations.

> ***Intelligence***
>
> Intelligence is (1) the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations; (2) the activities that result in the product; and (3) the organizations engaged in such activities (JP 2-0).

LARGE-SCALE COMBAT OPERATIONS

1-1. Threats to United States (U.S.) interests worldwide are countered by the U.S. forces' ability to respond to a variety of challenges along a conflict continuum that spans from peace to war as shown in figure 1-1. U.S. forces conduct a range of military operations to respond to these challenges. The conflict continuum does not proceed smoothly from stable peace to general war and back.

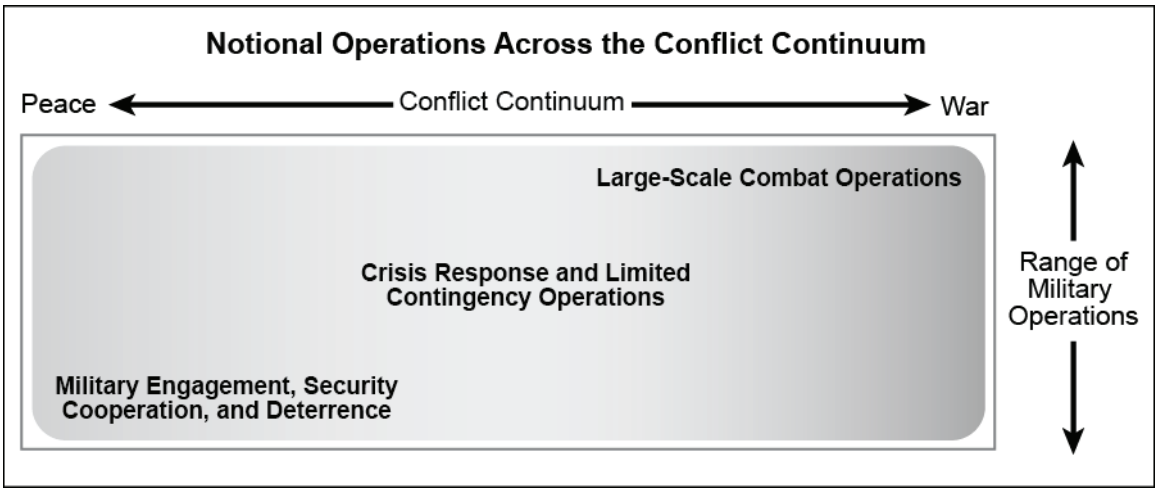


Figure 1-1. The conflict continuum and the range of military operations

1-2. The range of military operations is a fundamental construct that helps relate military activities and operations in scope and purpose within a backdrop of the conflict continuum. All operations along this range share a common fundamental purpose—to achieve or contribute to national objectives. Military engagement, security cooperation, and deterrence activities build networks and relationships with partners, shape regions, keep day-to-day tensions between nations or groups below the threshold of armed conflict, and maintain U.S. global influence. Typically, crisis response and limited contingency operations are focused in scope and scale and conducted to achieve a specific strategic- or operational-level objective in an operational area. Large-scale combat operations are at the far right of the conflict continuum and associated with war. These operations occur in the form of major operations and campaigns aimed at defeating an enemy's armed forces and military capabilities to support national objectives.

1-3. While the Army must be manned, equipped, and trained to operate across the range of military operations, large-scale combat operations present the greatest challenge for Army forces. Large-scale combat operations are intense, lethal, and brutal. Their conditions include complexity, chaos, fear, violence, fatigue, and uncertainty. Future battlefields will include noncombatants, and they will be crowded in and around large and densely populated cities. Enemies will employ a combination of conventional tactics, terrorism, criminal activity, and information warfare to complicate operations. To an ever-increasing degree, activities in the information environment are inseparable from land operations. Large-scale combat operations entail significant operational risk, synchronization, capabilities convergence, and a high operational tempo. These characteristics present a significant challenge for intelligence as a warfighting function. (See FM 3-0 for a more information about large-scale combat operations.)

THE OPERATIONAL ENVIRONMENT

1-4. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Commanders at all levels have their own operational environment for their particular operation. An operational environment for a specific operation comprises more than the interacting variables that exist within a specific physical area. It also involves interconnected influences (for example, politics and economics)—globally or regionally—that impact the conditions and operations within that physical area. Thus, each commander's operational environment is part of a higher commander's operational environment.

1-5. An operational environment is complex and dynamic and consists of many relationships and interactions among interrelated variables. Today's information technology makes the information environment, which includes cyberspace and the electromagnetic spectrum (EMS), indispensable to military operations. The information environment is a key part of any operational environment and will remain congested and contested simultaneously during operations. All groups in the information environment—enemy, friendly, or neutral—remain vulnerable to attack by physical, psychological, cyber, or electronic means. Each complex aspect of the operational environment makes intelligence support that much more complex. (See FM 3-12 for more information on cyberspace operations and the EMS.)

OPERATIONAL AND MISSION VARIABLES

1-6. Analysis of the broad aspects of an operational environment in terms of the operational variables provides relevant information that senior commanders use to understand, visualize, and describe the operational environment. The operational variables are political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). Upon receipt of a warning order or mission, Army leaders filter relevant information and narrow their focus to six mission variables—mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). Extensive analysis of the operational and mission variables involves significant intelligence support as intelligence often provides the critical context and cultural understanding necessary to support staff planning and facilitate situational understanding.

Terrain

1-7. Terrain aspects and weather conditions are inseparable, directly influence each other, and impact military operations based on the mission variables (METT-TC). Terrain analysis, also referred to as

geospatial analysis, involves the study and interpretation of an area's natural and man-made features, their effects on military operations, and the effects of weather and climate on these features. Terrain analysis is a continuous process. The staff geospatial engineer normally analyzes the military aspects of terrain, which include the collection, analysis, evaluation, and interpretation of geospatial information on the terrain's natural and man-made features. Analysts combine other relevant factors with the terrain and weather to predict their effects on military operations. (For more information, see ATP 2-01.3.)

Weather

1-8. Weather analysis is more than just generating weather forecasts. Weather analysis focuses on detailed assessments of weather effects on friendly and threat operations and various systems. Analysts evaluate the effects of each military aspect of weather and focus on the aspects that have the most bearing on operations and decision making. The evaluation of each aspect should begin with operational climatology and current weather forecasts. Analysts fine-tune the evaluation to determine effects based on specific weather sensitivity thresholds for friendly and threat forces and systems. (For more information, see ATP 2-01.3.)

Civil Considerations

1-9. As part of generating intelligence knowledge before receipt of mission, the staff can database and describe civil considerations using the joint systems perspective (see JP 3-0), the operational variables (PMESII-PT), or the ASCOPE (areas, structures, capabilities, organizations, people, and events) characteristics. However, after the receipt of the mission, Army forces use ASCOPE characteristics as part of the mission variables (METT-TC) during intelligence preparation of the battlefield (IPB). The staff and intelligence analysts leverage information from many different sources, including publicly available information, to provide predictive, specific intelligence on ASCOPE characteristics that are significant to the mission. Lower echelon intelligence staffs may have to depend on higher echelon organizations, such as the Defense Intelligence Agency, to provide detailed information and analysis pertaining to civil considerations and sociocultural factors during some types of operations. (For more on ASCOPE and IPB, see ATP 2-01.3.)

MULTI-DOMAIN EXTENDED BATTLEFIELD

1-10. The interrelationship of the air, land, maritime, space, and cyberspace domains, the information environment, and the EMS requires cross-domain situational understanding of the operational environment. Commanders and staffs must understand the friendly and enemy capabilities and vulnerabilities that reside in each domain. From this understanding, commanders can better identify windows of opportunity during operations to converge capabilities for the best effects. Since many capabilities are not organic to Army forces, commanders and staffs plan, coordinate for, and integrate joint and other unified action partner capabilities in a multi-domain approach to operations. Intelligence plays an important role in facilitating situational understanding across all domains. This type of intelligence effort requires time, significant intelligence capabilities, and an analytical focus.

1-11. Since the Army conducts operations across all domains and the information environment, a multi-domain approach to operations is neither new to the Army nor to national to tactical intelligence. Rapid and continued advances in technologies and the military's use of new technologies within the space domain, the EMS, and the information environment (particularly cyberspace) will drive new requirements for special considerations for intelligence, planning, and converging effects from across all domains.

TRENDS

1-12. Several trends will continue to affect future operational environments. The competition for resources, water access, declining birthrates in traditionally allied nations, and disenfranchised groups in many nations contribute to the likelihood of future conflict. Populations will continue to migrate across borders and to urban areas in search of the employment and services urban areas offer. The adversarial use of media platforms to disperse misinformation and propaganda and malign narratives enables adversaries to shape operational environments to their advantage and ferment dissention, unrest, violence, or at the very least, uncertainty.

THREATS AND HAZARDS

1-13. Although threats are a fundamental part of an operational environment for any operation, they are discussed separately here for emphasis; hazard is an important related term that also affects operations:

- A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADRP 3-0). Threats may include individuals, groups of individuals (organized or not organized), paramilitary or military forces, nation-states, or national alliances. In general, a threat can be categorized as an enemy or an adversary.
- An *enemy* is a party identified as hostile against which the use of force is authorized (ADRP 3-0).
- An *adversary* is a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged (JP 3-0).
- A *hazard* is a condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation (JP 3-33).

1-14. While ADRP 3-0 addresses various threats across the range of military operations, FM 3-0 focuses on peer threats in large-scale combat operations. A peer threat is an adversary or enemy with capabilities and capacity to oppose U.S. forces across multiple domains worldwide or in a specific region where they enjoy a position of relative advantage. Peer threats possess roughly equal combat power in geographical proximity to a conflict area with U.S. forces. A peer threat may also have a cultural affinity to specific regions, providing them relative advantages in terms of time, space, and sanctuary. Peer threats generate tactical, operational, and strategic challenges that are an order of magnitude more challenging militarily than those the Army has faced since the end of the Cold War.

1-15. Peer threats employ their resources across multiple domains to attack U.S. vulnerabilities. They use their capabilities to create lethal and nonlethal effects throughout an operational environment. During combat operations, threats seek to inflict significant damage across multiple domains in a short period of time. They seek to delay friendly forces long enough to achieve their goals and end hostilities before friendly forces reach culmination. Peer threats will use various methods to employ their national elements of power to render U.S. military power irrelevant. Five broad peer threat methods, often used in combination, are—

- **Information warfare:** The threat's orchestrated use of information activities (such as cyberspace operations, electronic warfare (EW), and psychological operations) to gain advantage in the information environment.
- **Preclusion:** The threat's use of a wide variety of capabilities to preclude a friendly force's ability to shape the operational environment and mass and sustain combat power. Antiaccess and area denial are two such activities.
- **Isolation:** The threat's containment of a friendly force so the friendly force cannot accomplish its mission. Peer threats will attempt to isolate U.S. forces in several ways. For example, the threat might prevent a friendly force from effectively communicating while also decisively fixing a friendly unit with long-range fires and close combat capabilities.
- **Sanctuary:** The threat's ability to put its forces beyond the reach of friendly forces. It is a form of protection derived by some combination of political, legal, and physical boundaries that restrict freedom of action by a friendly force commander.
- **Systems warfare:** The threat's analysis of the operational environment (including its forces and friendly forces) to identify specific friendly critical capabilities for disruption or destruction in order to cause failure of a larger friendly system.

1-16. The intelligence warfighting function analyzes nation-states, organizations, people, or groups to determine their ability to damage or destroy life, vital resources, and institutions, or to prevent mission accomplishment. Threats are sometimes categorized as traditional, irregular, disruptive, and catastrophic. While helpful in generally describing the nature of the threat, these categories do not precisely describe the threat's goals, organizations, and methods of operating.

1-17. Intelligence provides a deep understanding of the threat and how the threat can affect mission accomplishment, which is essential to conducting operations. Commanders and staffs must understand how current and potential threats organize, equip, train, employ, and control their forces. Therefore, the

intelligence warfighting function must continually identify, monitor, and assess threats as they adapt and change over time. (For more information on threats and hazards see ADRP 3-0 and FM 3-0.)

UNIFIED ACTION AND JOINT OPERATIONS

1-18. *Unified action* is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1). *Unified action partners* are those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations (ADRP 3-0). Army contributions to unified action are called unified land operations (see paragraph 1-26). (For more information, see ADRP 3-0.)

1-19. Intelligence is inherently joint, interagency, intergovernmental, and multinational; it flows up and down through the echelons to provide the most complete, timely, accurate, and detailed intelligence possible. The Army provides adaptable intelligence capabilities that are dedicated to both joint and Army forces operating as a part of the joint team. This intelligence effort is synchronized, networked, and includes collaboration with unified action partners to achieve unity of effort and to meet the commander's intent. Intelligence unity of effort is critical to accomplish the mission. Multinational and interagency partners provide unique capabilities that reinforce and complement Army intelligence capabilities, as well as invaluable cultural awareness and different perspectives on the operational environment. Using the appropriate procedures, foreign disclosure guidance, and established policy, Army intelligence leaders provide information and intelligence support to multinational forces against an array of threats across multiple domains.

1-20. *Joint operations* are military actions conducted by joint forces and those Service forces employed in specific command relationships with each other, which of themselves, do not establish joint forces (JP 3-0). Traditionally, campaigns are the most extensive joint operations. In terms of large-scale combat operations, a campaign is a series of related major operations achieving strategic and operational objectives within a given time and space. A major operation is a series of tactical actions, such as battles, engagements, and strikes and it is the primary building block of a campaign. Army forces conduct supporting operations as part of a joint campaign.

1-21. Most joint operations share certain activities or actions in common. There are six general groups of military activities that typically occur in preparation for and during a large-scale combat operation. These six groups are shape, deter, seize initiative, dominate, stabilize, and enable civil authorities. These six general groups of activities provide a basis for thinking about a joint operation in notional phases. These phases often overlap, and they are not necessarily sequential.

1-22. As a part of joint operations, the Army is the dominant fighting force in the land domain. Across the globe, mission-tailored Army units build partnerships, deter adversaries, and overcome challenges to defeat enemies using simultaneous actions integrated in time, space, and purpose. Army forces both depend on and enable joint forces across all domains and the information environment. This mutual interdependence creates powerful synergies and reflects that all operations have multi-domain components. The Army depends on the other Services for strategic and operational mobility, joint fires, and other key enabling capabilities like information collection in the deep area. The Army supports other Services, combatant commands, and unified action partners with ground-based indirect fires and ballistic missile defense, defensive cyberspace operations, electronic protection, communications, intelligence, rotary-wing aircraft, logistics, and engineering.

1-23. Joint and Army intelligence staffs, units, and organizations within the theater intelligence architecture operate as mutually supporting entities that ensure information and intelligence are shared across echelons to support commanders at all levels. Intelligence, surveillance, and reconnaissance is an important construct in both joint and Army intelligence. Consistent with joint doctrine, *intelligence, surveillance, and reconnaissance* is an integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations (JP 2-01). The Army continually executes intelligence, surveillance, and reconnaissance worldwide through the operations and intelligence processes (with an emphasis on intelligence analysis and leveraging intelligence at each echelon) and information collection.

THE ARMY'S STRATEGIC ROLES

1-24. The Army's primary mission is to organize, train, and equip its forces to conduct prompt and sustained land combat to defeat enemy ground forces and seize, occupy, and defend land areas. The Army accomplishes its missions by supporting the joint force through the Army's four strategic roles: shape operational environments, prevent conflict, prevail in large-scale ground combat, and consolidate gains. The strategic roles clarify the enduring reasons for which the Army is organized, trained, and equipped. Figure 1-2 shows the Army's strategic roles in a general relationship to the joint phasing model.

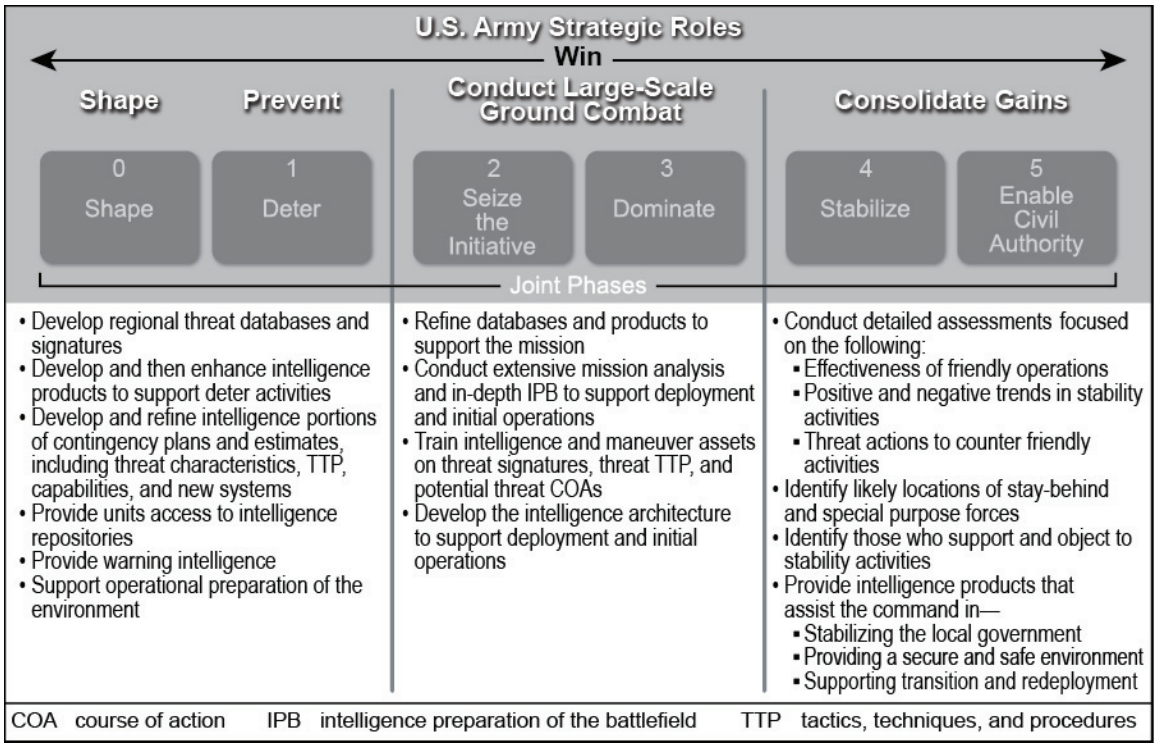


Figure 1-2. The Army's strategic roles and their relationship to the joint phases

1-25. There are requirements for intelligence during each strategic role. Some intelligence activities are specific to certain strategic roles, while others span multiple roles. (See figure 1-2 for some of the most important intelligence tasks for each strategic role.) Commanders and leaders ensure adequate planning for; collection; storage; processing, exploitation, and dissemination (PED); and analysis of information and intelligence during each strategic role. Ideally, regionally aligned forces build on and enhance existing threat data, information, and intelligence during the shaping activities. However, during the shape role, there may be instances in which regionally aligned forces must develop and populate an authoritative database of threat signatures and associated contextual information, in conjunction with joint forces and the Defense Intelligence Agency. This allows units to access, maintain, populate, and continually update the database throughout all subsequent activities. Commands prepare to establish localized intelligence databases during all activities. It is critical for commands to update the intelligence database continually with actual and potential adversaries to maximize the value of intelligence products and reports.

UNIFIED LAND OPERATIONS

1-26. An *operation* is a sequence of tactical actions with a common purpose of unifying theme (JP 1). Army forces, as part of the joint and multinational force, contribute to the joint mission through the conduct of unified land operations. Unified land operations is the Army's operational concept and contribution to unified action; it is how the Army applies combat power. *Unified land operations* are simultaneous offensive, defensive, and stability or defense support of civil authorities tasks to seize, retain, and exploit the initiative to shape the operational environment, prevent conflict, consolidate gains, and win our Nation's wars as part

of unified action (ADRP 3-0). The goal of unified land operations is to establish conditions that achieve the joint force commander's end state by applying landpower as part of a unified action to defeat the enemy. Military forces seek to prevent or deter threats through unified action, and, when necessary, execute operations to defeat aggression.

1-27. Land operations, particularly large-scale combat operations, focus on destroying or dislocating enemy forces or securing key land objectives that reduce the enemy's ability to conduct operations. Five characteristics distinguish land operations: scope, duration, terrain, permanence, and civilian presence. The characteristics of land operations contribute to the complexity and uncertainty of the environment in which Army forces conduct operations. Land operations against a peer threat (highly adaptive and technologically advanced) are especially challenging. At the beginning of a conflict, peer threats often occupy a position that greatly complicates Army forces' ability to conduct operations.

1-28. Peer threats are developing the capability to mass effects across multiple domains at a speed that will impact ongoing operations. They will most likely attempt to deny U.S. and multinational forces access to their territory. Once Army forces achieve access, the threat will attempt to deny them freedom of maneuver. Future adversaries are likely to use offensive cyberspace operations and counter-space measures to deny and degrade U.S. forces' maneuver, communications, intelligence collection, and targeting capabilities. Land-based threats will impede joint force freedom of movement and action across all domains and the information environment.

DECISIVE ACTION

1-29. Within unified land operations, Army forces conduct decisive action. *Decisive action* is the continuous, simultaneous combinations of offensive, defensive, and stability or defense support of civil authorities tasks (ADRP 3-0). In unified land operations, commanders seek to seize, retain, and exploit the initiative while synchronizing their actions to achieve the best effects possible. Operations conducted outside the United States and its territories simultaneously combine three elements—offense, defense, and stability. Within the United States and its territories, decisive action combines the elements of defense support of civil authorities (DSCA) and, as required, offense and defense to support homeland defense. (See table 1-1 on page 1-8.)

1-30. Commanders and staffs at all levels synchronize intelligence with the other warfighting functions to maximize their ability to visualize the operational environment and disrupt the threat simultaneously throughout the area of operations (AO) or perform the necessary stability tasks to consolidate gains. Collecting the intelligence required is often more complex and requires leveraging national to tactical intelligence capabilities. Commanders must be more involved in and knowledgeable of the intelligence warfighting function due to the complexity of operations. The following list provides some basic aspects of intelligence (discussed in more detail in subsequent chapters):

- The Army recognizes the function of intelligence as an element of combat power through the designation of the intelligence warfighting function.
- Intelligence is requirement-driven, and the commander drives intelligence primarily through clear, feasible, and focused requirements.
- The collection of information to support the production of intelligence is called information collection.
- There are many different intelligence analytical tasks such as generate intelligence knowledge, IPB, situation development, and intelligence support to targeting and information operations.
- The general intelligence capabilities employed by the commander and staff are: intelligence analysis elements, PED elements, and military intelligence (MI) units. These general capabilities consist of specific collectors or platforms with specific technical capabilities or sensors.

1-31. It is critical for the intelligence staff to support the commander's ability to visualize threats and relevant aspects of the operational environment during the conduct of decisive operations. However, information requirements, information collection tactics and techniques, the theater intelligence architecture, the nature of intelligence analysis, the employment of MI units, and specific tactics and techniques differ significantly depending on the specific decisive action task.

Table 1-1. Decisive action

Offense	*Defense*
Tasks:	**Tasks:**
• Movement to contact • Attack • Exploitation • Pursuit	• Mobile defense • Area defense • Retrograde
Purposes:	**Purposes:**
• Dislocate, isolate, disrupt, and destroy enemy forces • Seize key terrain • Deprive the enemy of resources • Refine intelligence • Deceive and divert the enemy • Provide a secure environment for stability tasks	• Deter or defeat enemy offense • Gain time • Achieve economy of force • Retain key terrain • Protect the population, critical assets, and infrastructure • Refine intelligence
Stability	***Defense support of civil authorities***
Tasks:	**Tasks:**
• Establish civil security • Establish civil control • Restore essential services • Support to governance • Support to economic and infrastructure development • Conduct security cooperation	• Provide support to domestic disasters • Provide support for domestic, chemical, biological, radiological, and nuclear incidents • Provide support for domestic civilian law enforcement agencies • Provide other designated support
Purposes:	**Purposes:**
• Provide a secure environment • Secure land areas • Meet the critical needs of the population • Gain support for host-nation government • Shape the environment for interagency and host-nation success • Promote security, build partner capacity, and provide access • Refine intelligence	• Save lives • Restore essential services • Maintain or restore law and order • Protect infrastructure and property • Support maintenance or restoration of local government • Shape the environment for intergovernmental success

Offense

1-33. An *offensive task* is a task conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers (ADRP 3-0). Offensive tasks impose the commander's will on the enemy. The offense is the most direct means of seizing, retaining, and exploiting the initiative to gain a physical and psychological advantage. In the offense, the decisive operation is a sudden action directed toward enemy vulnerabilities and capitalizing on speed, surprise, and shock. If that operation fails to destroy the enemy, operations continue until enemy forces are defeated. Executing offensive tasks compels the enemy to react, creating new or larger vulnerabilities the attacking force can exploit. (See ADRP 3-90 for a detailed discussion of offensive tasks.)

1-34. Offensive tasks at all levels require effective intelligence to assist the commander in avoiding the threat's main strength and to deceive and surprise the threat. The entire staff, led by the intelligence staff, develops IPB products to assist the commander in identifying all aspects in the area of interest that can affect mission accomplishment within all domains. The IPB process is collaborative and requires information from all staff elements and some subordinate units that use IPB results and products for planning.

1-35. The intelligence staff supports the commander's use of information collection assets to visualize the terrain, determine threat strengths and dispositions, and confirm or deny threat courses of action (COAs). These assets also collect information concerning the civil considerations within the AO. The G-2/S-2 and G-3/S-3, in coordination with the rest of the staff, develop a synchronized and integrated information collection plan that satisfies the commander's information requirements.

Defense

1-36. A *defensive task* is a task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks (ADRP 3-0). Normally, the defense cannot achieve a decisive victory. However, it sets conditions for a counteroffensive or a counterattack that enables forces to regain the initiative. Defensive tasks are a counter to an enemy offensive action. They defeat attacks, destroying as much of the attacking enemy as possible. They also preserve control over land, resources, and populations. The purpose of defensive tasks is to retain key terrain, guard populations, protect lines of communications, and protect critical capabilities against enemy attacks. Commanders can conduct defensive tasks to gain time and economize forces so offensive tasks can be executed elsewhere. (See ADRP 3-90 for a detailed discussion of defensive tasks.)

1-37. The intelligence staff supports the commander's use of information collection assets to visualize the terrain, determine threat strengths and dispositions, and confirm or deny threat COAs. Defending commanders can then decide where to arrange their forces in an economy-of-force role to defend and shape the battlefield. Intelligence analysis assists commanders in deciding on the precise time and place to counterattack. The G-2/S-2 and G-3/S-3, in coordination with the rest of the staff, develop a synchronized and integrated information collection plan that satisfies the commander's information requirements.

Stability

1-38. *Stability tasks* are tasks conducted as part of operations outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (ADRP 3-07). These tasks support governance, whether it is imposed by a host nation, an interim government, or a military government. Stability tasks involve coercive and constructive actions. They assist in establishing or maintaining a safe and secure environment and facilitate reconciliation among local or regional adversaries. Therefore, diverse and detailed intelligence products are important to support stability tasks.

1-39. For stability tasks, commanders often require more detailed intelligence and IPB products to determine how best to conduct operations and influence the local populace to enhance stability. The identification and analysis of threats, terrain and weather, and civil considerations are critical in determining the most effective missions, tasks, and locations to conduct stability tasks. A lack of knowledge concerning insurgents, local politics, customs, culture, and how to differentiate between local combatants often leads to U.S. actions that can result in unintended and disadvantageous consequences. Consequences can include attacking unsuitable targets or offending or causing mistrust among the local population. This lack of knowledge could potentially threaten mission accomplishment. The G-2/S-2 and G-3/S-3, in coordination with the rest of the staff, develop a synchronized and integrated information collection plan that satisfies the commander's information requirements. (For more information on stability tasks, see ADP 3-07 and ADRP 3-07.)

Defense Support of Civil Authorities

1-40. *Defense support of civil authorities* is support provided by United States Federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events (DODD 3025.18).

1-41. DSCA is a task executed in the homeland and U.S. territories. It is conducted to support another primary agency, lead federal agency, or local authority. When DCSA is authorized, it consists of four tasks (see table 1-1 on page 1-8). (See DODD 3025.18 for the full name and discussion of each task.) National Guard forces—Title 32 or state active forces under the command and control of the governor and adjutant general—are usually the first forces to respond on behalf of state authorities. When Federal military forces are employed for DCSA activities, they remain under Federal military command and control at all times. (See JP 3-28 and ADRP 3-28 for detailed DSCA discussions.)

1-42. The concepts and basic processes used to produce intelligence to support decision making for DSCA are no different from those used during offensive, defensive, and stability tasks. However, the operational environment is significantly different, and all commanders must ensure intelligence support in DSCA remains within the guidelines of U.S. law and applicable policies.

1-43. Following DODM 5240.01, for procedures 1 through 10; DOD 5240.1-R, procedures 11 through 15; and AR 381-10 procedures ensures adherence to regulations, statutes, and laws concerning intelligence activities. In particular, intelligence operations must adhere to regulations and directives that implement restrictions in compliance with intelligence oversight requirements. Further, any use of intelligence capabilities for purposes other than those designated in the Chairman, Joint Chiefs of Staff Standing DSCA Execute Order must be expressly approved by the Secretary of Defense. Information collection conducted to support the commander focuses on saving lives and reducing risk to Army forces. Commanders and intelligence professionals consult with staff judge advocates concerning any unclear areas of intelligence activities.

1-44. The intelligence process, some information collection units and systems, and intelligence analysis may assist in supporting the four DSCA core tasks. Army National Guard activities in Title 32, United States Code (USC), status and Regular Army and Army Reserve intelligence activities in Title 10, USC, status can perform intelligence tasks that support DSCA. (See ATP 2-91.7 for more information.)

INTELLIGENCE SUPPORT WITHIN MULTI-DOMAIN OPERATIONS

1-45. Army operations and battles will invariably involve challenges across multiple domains. All Army operations are multi-domain operations and all battles are multi-domain battles. Examples of Army multi-domain operations and activities include airborne and air assault operations, air and missile defense, fires, aviation, cyberspace electromagnetic activities, information operations, space operations, military deception, and information collection. Key considerations for operating in multiple domains are—

- Mission command.
- Reconnaissance in depth.
- Mobility.
- Cross-domain fires.
- Tempo and convergence of effects.
- Protection.
- Sustainment.
- Information operations.
- Cyberspace electromagnetic activities.

1-46. Army forces may be required to conduct operations across multiple domains to gain freedom of action for other members of the joint force. This is similar to other members of the joint force operating across multiple domains to assist in providing land forces with positions of relative advantage. Examples of these operations include neutralizing enemy integrated air defenses, destroying long-range surface-to-surface fires systems, denying enemy access to an AO, disrupting enemy command and control, protecting friendly networks, conducting tactical deception, or disrupting an enemy's ability to conduct information warfare.

1-47. Every echelon is affected by the multi-domain extended battlefield; each should consider time, geography, decision making, the EMS, and the other domains differently. However, not every echelon is able to effectively conduct operations across multiple domains. Brigade combat teams (BCTs) and lower echelons focused on fighting in the close area generally lack the time and ability to effectively plan and employ multi-domain capabilities other than those already under their control. These echelons focus on fundamental operational aspects such as mobility, lethality, and protection. The division is the first echelon able to effectively plan and coordinate for the employment of all multi-domain capabilities across the operational framework (including the considerations—physical, temporal, virtual, cognitive). Theater army and corps echelons have a broader perspective, better focus, and far more capabilities to orchestrate and converge multi-domain activities and operations in time and space. Through these activities and operations, intelligence is critical in assisting friendly forces to effectively identify and exploit windows of opportunity across the

domains to create and exploit temporary windows of superiority. (See FM 3-0 for more information on the multi-domain extended battlefield and operational framework.)

1-48. These operations require a significant amount of detailed intelligence to facilitate the commander's visualization of the threat, threat capabilities, and relevant aspects of the operational environment in time and space. This intelligence support assists commanders and staffs in deciding when and where to concentrate sufficient combat power to defeat the threat while mitigating risk.

This page intentionally left blank.

Chapter 2
Intelligence Support

Army intelligence as a function supports operations by accomplishing various intelligence tasks and activities for commanders and staffs. To provide this support, the intelligence staff, augmented with an analysis element and capabilities, performs intelligence analysis to support the commander and mission command, including the staff integrating processes. MI units collect information from across the operational environment and in each domain and the information environment. The results from this information collection effort provide information for analysis and production into intelligence. This intelligence support occurs at each echelon, from theater army down to the battalion level, within an overarching national to tactical intelligence architecture. Together with the commander, staff, and all units, this functional system is known as the Army intelligence warfighting function.

THE PURPOSE OF INTELLIGENCE

2-1. Intelligence is a product, a process, and a function that enables the Army to conduct operations by supporting the commander and mission command (which is accomplished by supporting the rest of the staff). Commanders and staffs rely on many different types of intelligence products. The intelligence process is continuous and directly supports the operations process by developing information requirements, collecting on those requirements, processing data into information, analyzing information and intelligence from all sources, producing intelligence, and when necessary, developing the situation through operations. Intelligence is also a complex function.

2-2. Intelligence supports commanders (and in some cases other decision makers) and staffs by providing situational understanding of the threat, terrain and weather, civil considerations, and other aspects of the operational environment. Intelligence supports the commander and staff with analysis and production of effective timely, relevant, accurate, and predictive assessments and products tailored to the commander's and staff's specific needs.

2-3. Intelligence drives operations and operations enable intelligence; this relationship is continuous. Intelligence supports the planning, preparing, execution, and assessment of operations by supporting mission command. The mission command warfighting function integrates the elements of combat power across the warfighting functions. To ensure effective intelligence support, commanders and staffs must understand the interrelationship of mission command, the intelligence warfighting function, and fundamental intelligence doctrine. (See ADRP 6-0.)

2-4. Commanders require intelligence about the threat and other aspects of the operational environment before and during operations to effectively accomplish their missions. Intelligence assists commanders in visualizing the operational environment, organizing their forces, and controlling operations to achieve their objectives by answering specific requirements focused in time and space. These intelligence products enable commanders to make decisions based on all available information, identify and assess potential COAs, plan operations, properly direct their forces, and employ ethical, effective, and efficient tactics and techniques. Additionally, intelligence supports protection by alerting commanders to threats and assisting in preserving and protecting the force.

2-5. Supporting mission command and the staff integrating functions is complex. Operations, targeting, intelligence, and communications are inextricably linked. Therefore, the commander must drive the operations process partially by enabling the intelligence warfighting function. Commanders use their staff to synchronize intelligence with the other warfighting functions to visualize the operations and disrupt the threat simultaneously throughout an AO. Successful intelligence is the result of carefully developed requirements, staff integration and synchronization, continuous information collection, and, when necessary, the willingness to fight for intelligence.

2-6. Intelligence leaders (both in the intelligence staff and in MI units) ensure that the intelligence warfighting function operates effectively and efficiently. They are the commander's primary advisors on information requirements, intelligence analysis, employing information collection assets, and fighting for intelligence. Intelligence analysis is a thorough and deliberate process. Intelligence leaders provide the commander with predictive assessments that consider all aspects of the threat, terrain and weather, and civil considerations, and should provide the commander with an estimate about the degree of confidence the intelligence leader places on each analytic assessment.

THE INTELLIGENCE WARFIGHTING FUNCTION

2-7. The intelligence warfighting function is the Army's contribution to the joint intelligence effort. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment (ADRP 3-0). Specifically, other significant aspects of the operational environment include threats, adversaries, the operational variables, and can include other aspects depending on the nature of operations.

2-8. The intelligence warfighting function encompasses more than the MI branch:

- The commander drives the operations process and focuses the intelligence effort that supports it.
- Intelligence is commander-centric. The commander performs the central role within intelligence and enables the intelligence warfighting function.
- The entire staff is important to the intelligence warfighting function and each staff member contributes to intelligence in a different way.
- During combat operations, the G-2/S-2, G-3/S-3, G-6/S-6, and fire support coordinator form the staff core that is essential to synchronize and integrate intelligence.
- Every Soldier contributes to information collection.

INTELLIGENCE WARFIGHTING FUNCTION TASKS

2-9. The intelligence warfighting function facilitates support to the commander and staff through a broad range of supporting Army Universal Task List (AUTL) tasks. (See ADRP 1-03.) These tasks are interrelated, require the participation of the commander and staff, and are often conducted simultaneously. The intelligence warfighting function tasks facilitate the commander's visualization and understanding of the threat and other relevant aspects of the operational environment. Army units at the Army Service component command (ASCC) level or formed as a joint task force use the Universal Joint Task List (also called UJTL). The intelligence warfighting function includes the following tasks:

- **Provide intelligence support to force generation**—the task of generating intelligence knowledge concerning an operational environment, facilitating future intelligence operations, and tailoring the force.
- **Provide support to situational understanding**—the task of providing information and intelligence to commanders to assist them in achieving a clear understanding of the force's current state with relation to the threat and other relevant aspects of the operational environment.
- **Conduct information collection**—the task that synchronizes and integrates the planning and employment of sensors and assets as well as the PED systems in direct support of current and future operations.
- **Provide intelligence support to targeting and information operations**—the task of providing the commander information and intelligence support for targeting to achieve lethal and nonlethal effects.

2-10. Table 2-1 illustrates how the intelligence warfighting function tasks support the commander. (See ADRP 1-03 for the complete list of tasks and their measures of performance.)

Table 2-1. Overview of intelligence warfighting function tasks

Intelligence tasks ►	*Commander's focus ►*	*Commander's decisions*
Provide intelligence support to force generation: • Provide intelligence readiness. • Establish an intelligence architecture. • Provide intelligence overwatch. • Generate intelligence knowledge. • Tailor the intelligence force.	Orient on contingencies.	• Should the unit's level of readiness be increased? • Should the operation plan be implemented?
Provide support to situational understanding: • Perform IPB. • Perform situation development. • ~~Provide intelligence support to protection.~~ • Provide tactical intelligence overwatch. • Conduct police intelligence operations. • Provide intelligence support to civil affairs operations.	• Plan an operation. • Prepare. • Execute. • Assess. • Secure the force. • Determine 2d and 3d order effects on operations and the populace.	• Which COA will be implemented? • Which enemy actions are expected? • What mitigation strategies should be developed and implemented to reduce the potential impact of operations on the population?
Conduct information collection: • Collection management. • Direct information collection. • Execute collection. • Conduct intelligence-related missions and operations.	• Plan information collection for an operation, including PED requirements. • Prepare. • Execute. • Assess.	• Which DPs, HPTs, and HVTs are linked to the threat's actions? • Are the assets available and in position to collect on the DPs, HPTs, and HVTs? • Have the assets been repositioned for branches or sequels?
Provide intelligence support to targeting and information operations: • Provide intelligence support to targeting. • Provide intelligence support to information operations. • Provide intelligence support to combat assessment.	• Create lethal or nonlethal effects against targets. • Destroy, suppress, disrupt, or neutralize targets. • Reposition intelligence or attack assets.	• Are the unit's lethal and nonlethal actions and maneuver effective? • Which targets should be re-engaged? • Are the unit's information operations effective?

COA	course of action	HVT	high-value target
DP	decision point	IPB	intelligence preparation of the battlefield
HPT	high-payoff target	PED	processing, exploitation, and dissemination

2-11. There are intelligence-related AUTL tasks beyond the four most significant intelligence warfighting tasks in table 2-1. Soldiers, systems, and units from all branches conduct intelligence-related AUTL tasks. Every Soldier, as a part of a small unit, is a potential information collector. Soldiers develop a special awareness simply due to exposure to events occurring in the AO, and they can collect and report information based on their observations and interactions with the local population. The increased awareness that Soldiers develop through personal contact and observation is a critical element of the unit's ability to understand the operational environment more fully.

2-12. Therefore, the Army established the *every Soldier is a sensor* (known as ES2) program, which is accomplished through information collection operations among populations. The AUTL task to establish a mission intelligence briefing and debriefing program is designed to assist units in collecting useful information in their AO more effectively. This task is critical because units often operate in an AO characterized by violence, uncertainty, and complex threats. (See ATP 3-55.4.)

2-13. Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See the DOD Law of War Manual and CJCSI 3121.01B [classified].) In some cases, there are certain sensitivities, ethical considerations, and limitations to personnel conducting information collection—for example, civil affairs and medical Soldiers. Medical personnel cannot be assigned information collection tasks due to their Geneva Convention category status. If medical personnel do gain information through casual observation of activities

in plain sight while conducting their duties, they will report the information to their chain of command. In all cases, Army professionals base their decisions and actions on the moral principles of the Army Ethic, ensuring the protection of the inalienable rights of all people.

INTELLIGENCE CORE COMPETENCIES

2-14. The intelligence core competencies are the most basic activities and tasks the Army uses to describe and drive the intelligence warfighting function and leverage national to tactical intelligence. At the most basic level, the intelligence warfighting function makes observations about the threat and relevant aspects of the operational environment through **collection** resulting in data that it **processes and exploits** into useable information for **analysis and production**. This results in intelligence. Because of the complexity of this undertaking, the entire effort must be **synchronized** carefully. The four aspects (in bold) capture the intelligence core competencies. Commanders and staffs must thoroughly understand the core competencies to apply the intelligence process and leverage national to tactical intelligence. The intelligence core competencies are—

- Intelligence synchronization (**synchronized**).
- Intelligence operations (**collection**).
- Intelligence PED (**processes and exploits**).
- Intelligence analysis (**analysis and production**).

2-15. The intelligence core competencies also serve as those areas that all MI units and Soldiers must continuously train on to maintain a high degree of proficiency. Intelligence professionals have unique technical training, intelligence oversight, and other oversight requirements in order to operate as part of the DOD intelligence effort. MI Soldiers must continuously and rigorously train to thoroughly understand unique authorities and guidelines, terms, and technical channel procedures.

Intelligence Synchronization

2-16. ***Intelligence synchronization*** **is the art of integrating information collection; intelligence processing, exploitation, and dissemination; and intelligence analysis with operations to effectively and efficiently fight for intelligence in support of decision making.** This core competency ensures the intelligence warfighting function supports mission command. Intelligence synchronization balances time with collection, production, required accuracy, and specificity to meet the commander's intent and other requirements.

2-17. Intelligence synchronization requires an effective relationship with the commander, focused information collection, effective dissemination of predictive assessments, and adaptability to changing situations. Some critical aspects of effective intelligence synchronization include—

- Early and continuous teamwork with the commander and across the staff.
- Expertise and proficiency in information collection, PED, and leveraging national to tactical intelligence.
- Mastery of the intelligence process.
- A collaborative environment for flexible, creative analysts to solve complex problems.

Intelligence Operations

2-18. Intelligence operations is one of the four primary means for information collection. The other three are reconnaissance, surveillance, and security operations. ***Intelligence operations*** **are the tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements.** These requirements are normally specified in the information collection plan. Intelligence operations collect information about the intent, activities, and capabilities of threats and relevant aspects of the operational environment to support commanders' decision making.

2-19. Intelligence operations, like reconnaissance, surveillance, and security operations, are shaping operations used by the commander for decisive action. MI units use the operations process to conduct intelligence operations. Intelligence operations are conducted using mission orders and standard command and support relationships. Flexibility and adaptability to changing situations are critical for conducting

effective intelligence operations. To plan and then remain flexible and adaptable, MI units and the intelligence staff must carefully deconflict and coordinate intelligence operations.

2-20. Deconfliction and coordination require a series of related activities that facilitate operations in another unit's AO. These activities facilitate successful intelligence operations and fratricide avoidance. At a minimum, MI units coordinate for and report their presence and request information on any conditions or ongoing situations that may affect how they conduct their mission. When possible, MI units and the intelligence staff should conduct a thorough face-to-face coordination.

2-21. MI units must also coordinate with the appropriate staff elements to establish fire support coordination measures around information collection assets, airspace control measures, and the appropriate weapons control status (in reference to aerial information collection assets). Failure to conduct proper deconfliction and coordination may result in mission failure or unnecessary risk to personnel. MI units' leadership also coordinates with the supported unit's intelligence section for debriefings of returning members, convoy leaders, and others.

2-22. Intelligence coordination is also conducted by the intelligence staff to facilitate active collaboration, laterally and vertically. It includes establishing and maintaining technical channels to direct, refine, and focus intelligence operations. (See paragraphs 4-11 through 4-13 and FM 2-0 for more on technical channels.)

Intelligence Processing, Exploitation, and Dissemination

2-23. Army doctrine has long recognized the functions of processing, initial analysis, and reporting, and the requirement for providing combat information. Joint and Army doctrine currently recognizes these functions under the concept of PED and the core capability of intelligence PED. In joint doctrine, PED is an intelligence concept that facilitates the allocation of assets to support intelligence operations. Under the joint PED concept, planners examine all collection assets and determine if allocation of additional personnel and resources is required to exploit the collected information.

2-24. Beyond doctrine, PED plays an important role in the development of DOD intelligence capabilities. PED began as processing and intelligence exploitation support for unique systems and capabilities—for example, full motion video from unmanned aircraft systems. Unlike previous geospatial intelligence (GEOINT) collection capabilities, full motion video did not have an automated capability to process raw data into a useable format and supporting personnel to perform initial exploitation. Therefore, a separate PED capability was required. Since 2006, PED requirements across multiple disciplines have grown significantly, and DOD has created many different PED capabilities across various echelons.

2-25. ***Processing, exploitation, and dissemination*** **is the execution of the related functions that converts and refines collected data into usable information, distributes the information for further analysis, and, when appropriate, provides combat information to commanders and staffs**. PED is not exclusive to MI organizations; other branches employ sensor collection capabilities. Therefore, PED conducted by intelligence personnel or units is called *intelligence PED*. Intelligence PED facilitates efficient use and distribution of information following collection. In essence, intelligence PED is the way the intelligence warfighting function processes collected data and information, performs an initial analysis (exploitation), and provides information in a useable form for further analysis. During intelligence PED, some information will be identified as combat information. In those cases, the combat information will be disseminated to commanders and staffs.

2-26. An important part of intelligence PED is ensuring information is distributed with adequate context and formatted to facilitate understanding or make subsequent analysis easier. Another important aspect of PED is providing feedback on the effectiveness of collection relative to the information collection plan and expected results. All PED methods are related closely to planning, information collection, control via technical channels, and intelligence analysis and production requirements. Receiving feedback gives leaders and staffs the information needed to maintain synchronization of intelligence operations with the overall operation. This synchronization may include retasking MI collection assets or cueing other MI collection capabilities.

2-27. The current approach to intelligence PED reflects a deliberate solution to the increased complexity of intelligence operations and the explosion of available data and information resulting from information collection. This approach is part of meeting the enduring challenge to get the right information to the right

place at the right time. The amount of available data and information will continue to grow exponentially. In response, the Army is emphasizing PED resourcing, planning, and execution, and maintaining a continuous assessment of its usefulness. This approach is resourced with and executed by a variety of intelligence PED capabilities leveraged throughout the Army and intelligence community.

Intelligence Analysis

2-28. Analysis is the basis for planning and staff activities. Analysis facilitates commanders' and other decision makers' ability to visualize the operational environment, organize their forces, and control operations in order to achieve their objectives.

2-29. Intelligence analysis is specific to the intelligence warfighting function and results in the production of timely, accurate, relevant, and predictive intelligence. ***Intelligence analysis*** **is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production**. The purpose of intelligence analysis is to describe the current—and attempt to proactively assess—threats, terrain and weather, and civil considerations. Intelligence analysis sets the stage for the development of information collection requirements, which result in information collection and then more intelligence analysis; this relationship is continuous. (See ATP 2-33.4 for more on intelligence analysis.)

2-30. Intelligence analysis is continuous, complements intelligence synchronization, and enables operations. Some aspects that enable effective staff support and intelligence analysis include—

- **Critical thinking.** Critical thinking is essential to analysis. Using critical thinking, which is disciplined and self-reflective, provides more holistic, logical, ethical, and unbiased analysis and conclusions. Applying critical thinking ensures analysts fully account for the elements of thought, the standards of thought, and the traits of a critical thinker.
- **Embracing ambiguity.** Well-trained analysts are critical due to the nature of changing threats and operational environments. They must embrace ambiguity, and recognize and mitigate their own or others' biases, challenge their assumptions, and continually learn during analysis.
- **Collaboration.** Commanders, intelligence and other staffs, and intelligence analysts collaborate. They actively share and question information, perceptions, and ideas to better understand situations and produce intelligence. Collaboration is essential to analysis; it ensures analysts work together to effectively and efficiently achieve a common goal. Often analytical collaboration is enabled by DOD intelligence capabilities.

NATIONAL TO TACTICAL INTELLIGENCE

2-31. National to tactical intelligence comprises all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture. While there are many aspects to national to tactical intelligence, the most important element of the intelligence effort is the people that make it work. The intelligence warfighting function is the Army's contribution to national intelligence.

2-32. The value of the national to tactical intelligence effort is the ability it provides to leverage information from all unified action partners, including access to national capabilities, as well as nonintelligence information, larger volumes of information and intelligence, and specialized analysis by unified action partners. Collaboration is the central principle of conducting analysis. Army units provide accurate and detailed intelligence on the threats and relevant aspects of the operational environment (especially those related to Army activities), while other portions of the DOD intelligence effort provide expertise and access not readily available to the Army. Additionally, DOD agencies provide governance over certain intelligence methods and activities. Cooperation benefits everyone.

2-33. Analysts leverage higher-level intelligence organizations to create a more comprehensive and detailed assessment of threats and relevant aspects of the operational environment (such as the multi-domain extended battlefield, civil considerations, and sociocultural factors) to facilitate mission command. An example of achieving greater efficiency between the intelligence and mission command warfighting functions is the creation of fusion centers. Fusion centers are ad hoc cells designed to enable targeting, facilitate current or future operations, and inform decision making. (See FM 2-0 for more information on fusion centers.)

2-34. The effectiveness of the intelligence warfighting function hinges directly on collaboration and unity of effort within the intelligence community. Numerous DOD and non-DOD agencies and organizations in the intelligence community support Army operations by providing specific intelligence products and services. The intelligence community has become increasingly important as new technologies facilitate collaborative analysis and production. DOD members include the Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and Army, Navy, Air Force, and Marine Corps Intelligence. Non-DOD members include the Central Intelligence Agency, Department of State, Department of Energy, Federal Bureau of Investigation, Department of the Treasury, U.S. Coast Guard Intelligence, Department of Homeland Security, the Drug Enforcement Administration, and the Office of Director of National Intelligence. Intelligence community members establish standards in their respective specialties. Effective intelligence staffs are familiar with these organizations and the methods of obtaining information from them as necessary. (See JP 2-0.)

Note. *Intelligence community* is all departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role (JP 2-0).

NATIONAL AND JOINT INTELLIGENCE

2-35. National intelligence organizations employ specialized resources and dedicated personnel to collect intelligence worldwide about trends, threats and threat capabilities, events and activities, and other national intelligence requirements. National intelligence organizations primarily support national decision makers, while also routinely providing support to the joint force commander. However, depending on the situation, the focus of this national-level intelligence collection and production may meet some Army service needs.

2-36. The United States Army Intelligence and Security Command (INSCOM) is a direct reporting unit to the Army Deputy Chief of Staff for Intelligence, who conducts and synchronizes worldwide intelligence collection across all disciplines and all-source analysis activities. The Army, in response to validated requirements, may provide the theater and joint force with intelligence capabilities resident within INSCOM. INSCOM also delivers linguist support and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities to support Army, joint, unified action partners, and the U.S. intelligence community.

2-37. There are two types of units assigned to INSCOM: military intelligence brigades-theater (MIB-Ts) and functional commands. There are seven MIB-Ts, each one tailored for the combatant command it supports. These brigades provide collection, processing, analysis, and dissemination support to the ASCCs, combatant commanders, and the intelligence community. INSCOM MIB-Ts are assigned through the appropriate joint documentation process to geographic combatant commands (GCCs). GCCs routinely provide these brigades in an operational control relationship to the supporting ASCCs.

2-38. INSCOM's functional brigades and groups may provide general support, general support reinforcing, or direct support to theaters of operations through intelligence reach, or they may be force tailored for deployment to support the joint force. These brigades and groups, while not regionally aligned, work in coordination with INSCOM's MIB-Ts to effectively create a seamlessly integrated tactical to national intelligence architecture. Functional commands within INSCOM have missions and capabilities focused on a single discipline or operational function. Examples of this type of command include the—

- 902d MI Group (counterintelligence [CI]).
- Army GEOINT Battalion.
- Army Operations Group (human intelligence [HUMINT]) operating in direct support of Army requirements.
- 704th MI Brigade providing signals intelligence (SIGINT) functional capabilities to support national and Army requirements.
- 116th Aerial Intelligence Brigade (aerial intelligence, surveillance, and reconnaissance and associated PED) to support combatant command and Army requirements.

- National Ground Intelligence Center (NGIC), which is the Army's service intelligence production center in response to national and Army requirements.
- Army Field Support Center.

REGIONALLY ALIGNED FORCES AND SETTING THE THEATER

2-39. *Regionally aligned forces* are those forces that provide a combatant commander at up to joint task force capable headquarters with scalable, tailorable capabilities to enable the combatant commander to shape the environment. They are those Army units assigned to combatant commands, those Army units allocated to a combatant command, and those Army capabilities distributed and prepared by the Army for combatant command regional missions (FM 3-22). Regionally aligned forces also include capabilities that are Service-retained but aligned with a combatant command. Regional missions include theater security cooperation and other shaping efforts. A large portion of joint and Army intelligence is regionally aligned.

2-40. Regionally aligned forces and other specified Army units require ready access to and seamless interaction with their associated combatant command's intelligence architecture. When an Army headquarters enters a GCC theater as a joint force command, joint task force, or combined joint task force, it primarily receives intelligence support through the joint intelligence architecture. Specifically, the GCC joint intelligence center/joint intelligence operations center (also called JIC/JIOC) provides all-source intelligence support unless another support relationship is established. Other Army units within the GCC depend on the combatant command's MIB-T for situational awareness throughout the area of responsibility. This relationship allows units to tailor mission planning and training, establish an effective intelligence architecture, and leverage DOD intelligence effectively. This concept refers to the MIB-T as the anchor point within that specific theater.

2-41. The intelligence warfighting function must constantly set the theater for all Army forces across all echelons of a deployed force in theater. Intelligence staffs and MI units must carefully transition intelligence capabilities and activities to support all engagements and operations as the Army moves from shape to prevent to prevail in large-scale ground combat and to consolidate gains. There are three core tasks involved in setting the theater:

- The intelligence staff plans, builds, and evolves an intelligence architecture based on the information collection, PED, and analysis capabilities allocated or requested to support operations.
- The intelligence staff builds the knowledge needed to understand the operational environment through coordination and collaboration with regionally aligned forces, using the MIB-T as the anchor point. This task includes connecting the intelligence architecture to and incorporating reports and products into the mission command information systems.
- The intelligence staff supports theater security cooperation and engagements that develop context and build relationships with unified action partners through the successful conduct of intelligence operations, intelligence analysis, and intelligence PED.

ESTABLISHING THE INTELLIGENCE ARCHITECTURE

2-42. The intelligence architecture is the compilation and interrelationship of all relevant intelligence and communications capabilities, data centers, organizations, supporting capabilities, concepts of operations, and personnel necessary to ensure the successful execution of the intelligence process. It connects the units, capabilities, PED activities, and analysts whose products and assessments inform decision makers. The architecture consists of more than a unit's organic intelligence capabilities, systems, and personnel. It includes all elements of the intelligence network and associated communications architectures required to enable intelligence operations to support mission requirements. (See FM 2-0 for more on intelligence units, general capabilities, collectors and platforms, and specific technical capabilities and sensors.)

2-43. Planning the intelligence architecture is inseparable from long-range planning for future intelligence operations. It is tied directly to the types and methods of support the commander directs. It is roughly equivalent to developing a blueprint for a house and gathering the materials to build the house. The unit cannot count on support from intelligence capabilities unless they are included in the intelligence architecture and supported by interoperable communications.

2-44. The intelligence staff portrays the intelligence architecture in a series of planning products that map the operational and technical aspects of the interoperability between the many components of the architecture. The architecture includes but is more encompassing than the different intelligence, communications, and technical networks. (Technical networks are those information management and information system connections that allow sharing of resources and information.) Intelligence architecture products capture not only networks and their technical specifications but also how the elements of the architecture relate and interoperate with each other. These products should address mission tasks, technical control, tipping and cueing, maintenance, security measures, medical evacuation, and force protection, among other considerations. General intelligence collection capabilities are captured in detail, including specific collectors or platforms and their specific technical sensors or capabilities, to avoid gaps in collection capabilities.

2-45. Planning and coordinating the intelligence architecture is critical during all types of operations. When developing the intelligence architecture, the intelligence staff considers all personnel, organizations, systems, and procedures necessary for developing intelligence, including those needed for intelligence operations. The architecture must address bandwidth requirements, preparing for operations, collecting the required information and analyzing it, producing the required products, disseminating the resulting intelligence, and assessing both the intelligence produced and the process that produced it. It is critical for the intelligence staff to work with the commander and the staff as early as possible and throughout planning to ensure the intelligence architecture is addressed adequately. The G-2/S-2 also ensures the unit or organization and its subordinates are adequately integrated into their intelligence architecture to enable effective information collection, PED, and analysis to support mission requirements. This ensures the intelligence architecture supports the necessary operational and technical connections between collection assets, control elements, PED nodes, analytical cells, and headquarters to enable an effective and efficient information flow of intelligence to decision makers and the rest of DOD.

2-46. Effective communications connectivity, automation, and interoperability are essential components of the intelligence architecture. These components are especially difficult to establish during large-scale combat operations when tactical forces will not have fixed sites and a robust communications infrastructure is not in place or are severely impacted by an adversary. Establishing the communications network involves many complex technical issues. The intelligence staff collaborates closely with the signal staff to arrange the required communications links. The intelligence staff requires classified and unclassified network connectivity for its equipment. If elements of the intelligence staff will be working outside the range of the unit's communications systems, intelligence architecture planning must include coordination for global or extended-range capabilities.

INTELLIGENCE ACROSS ARMY ECHELONS

2-47. Army intelligence supports decisive action at all echelons. Specifically, the intelligence warfighting function supports operations from the theater army down to the battalion level. The commander and staff need accurate, relevant, and predictive intelligence to understand threat centers of gravity, goals and objectives, and COAs. The commander and staff must also have detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute friendly operations. Precise intelligence is critical to target threat capabilities at the right time and place and to open windows of opportunity to achieve positions of relative advantage.

2-48. The basic intelligence support provided by the G-2/S-2 and intelligence staff at each echelon is the same. What differs is the size, composition, and number of supporting capabilities for the intelligence staff; access to higher-level information and intelligence; number and complexity of the requirements; and time available to answer those requirements. In general, the higher the echelon, the greater the volume, depth, and complexity (for example, detailed intelligence products about threat cyberspace activities) of analysis and intelligence production the intelligence staff can perform. Lower-echelon G-2/S-2s and intelligence staffs often must depend on the higher echelon for certain intelligence products and support. Therefore, the commander and staff must understand the intricacies or specifics of the intelligence warfighting function across each echelon.

2-49. MI unit structures and capabilities differ significantly across theaters and echelons. For example—

- Each theater army MIB-T is structured differently and has different capabilities and capacities.
- The corps expeditionary-military intelligence brigade (E-MIB) is the lowest level with organic CI teams and HUMINT units specifically designated for detainee facility interrogations.
- The theater army, corps, and BCT have organic MI units—the MIB-T, E-MIB, and MI company respectively—but the division and battalion do not have an organic MI unit. ***Note.*** Some of the corps E-MIBs can be task-organized to support the division or even some BCTs.

2-50. These aspects of the intelligence warfighting function matter to the success of operations. Figure 2-1 provides a quick summary of the operations, intelligence staffs, and organic MI units at each level. (For more information on the Army echelons, see FM 3-0; for more on intelligence units and capabilities from theater army to the battalion level, see FM 2-0.)

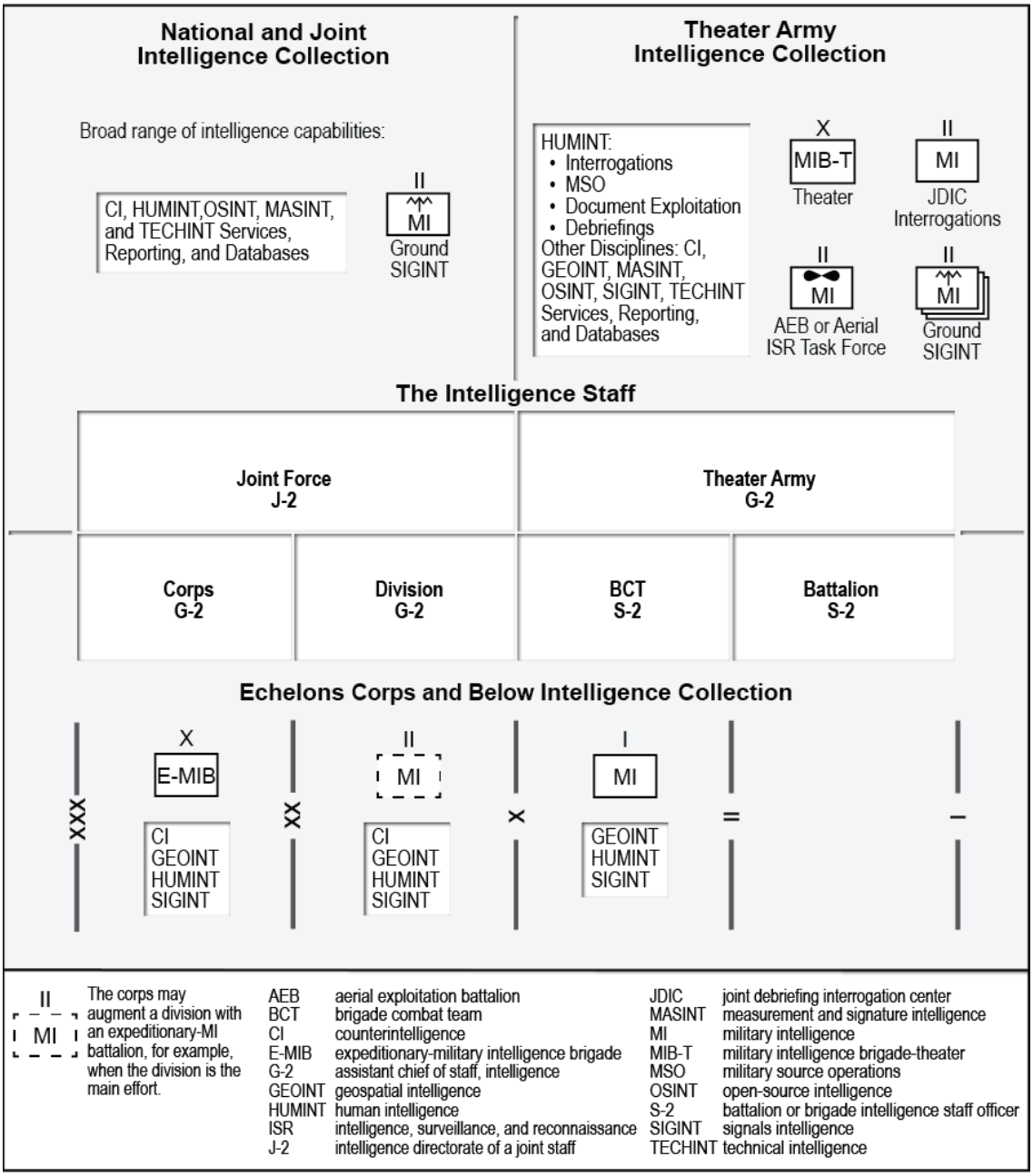


Figure 2-1. Intelligence across the echelons

Chapter 3

The Intelligence Process

The Army views the intelligence process as a model that describes how the intelligence warfighting function facilitates situational understanding and supports decision making. This process provides a common framework for Army professionals to guide their thoughts, discussions, plans, and assessments. Effective execution of the intelligence process depends on commander and staff involvement and effective information collection.

THE OPERATIONS PROCESS AND THE INTELLIGENCE PROCESS

3-1. Commanders use the operations process to drive the planning necessary to understand, visualize, and describe their operational environment; make and articulate decisions; and direct, lead, and assess military operations. Commanders successfully drive the operations process by using information and intelligence. The design and structure of the intelligence process support commanders by providing intelligence needed to support mission command and the commander's situational understanding. The commander provides guidance and focus by defining operational priorities and establishing decision points and commander's critical information requirements (CCIRs).

3-2. The joint intelligence process provides the basis for common intelligence terminology and procedures. (See JP 2-0.) It consists of six interrelated categories of intelligence operations:

- Planning and direction.
- Collection.
- Processing and exploitation.
- Analysis and production.
- Dissemination and integration.
- Evaluation and feedback.

3-3. Due to the unique characteristics of Army operations, the Army intelligence process differs from the joint process in a few subtle ways while accounting for each category of the joint intelligence process. The Army intelligence process consists of four steps (plan and direct, collect and process, produce, and disseminate) and two continuing activities (analyze and assess).

3-4. The commander's guidance drives the intelligence process. This process generates information, products, and knowledge about threats, terrain and weather, and civil considerations for the commander and staff. The intelligence process supports all of the activities of the operations process (plan, prepare, execute, and assess). Although the intelligence process includes unique aspects and activities, it is designed similarly to the operations process:

- The *plan and direct* step of the intelligence process closely corresponds with the *plan* activity of the operations process.
- The *collect and process*, *produce*, and *disseminate* steps of the intelligence process together correspond to the *execute* activity of the operations process.
- *Assess* and *analyze* are continuous. These activities form part of the overall *assessment* activity of the operations process.

3-5. Intelligence support to operations requires leveraging national to tactical intelligence. This support is coordinated through the intelligence staff at each echelon by using the intelligence process. Figure 3-1 on page 3-2 illustrates the intelligence process.

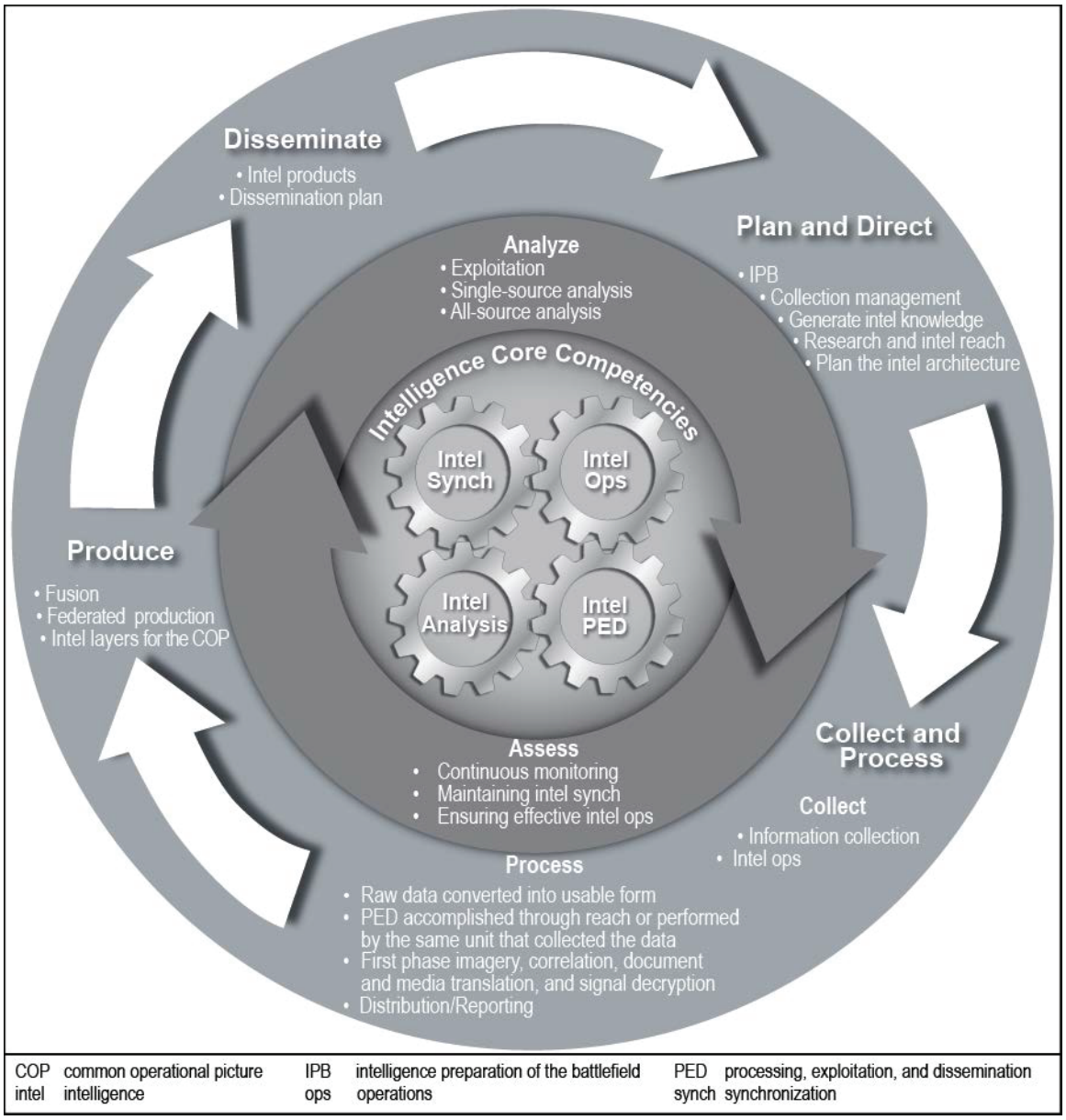


Figure 3-1. The intelligence process

3-6. The G-2/S-2 produces intelligence for the commander as part of a collaborative process. The commander drives the G-2/S-2's intelligence production effort by establishing intelligence and information requirements with clearly defined goals and criteria. Differing unit missions and operational environments dictate numerous and varied production requirements to the G-2/S-2 and staff.

3-7. The G-2/S-2 and staff provide intelligence products that enable the commander to—

- Plan operations and employ maneuver forces effectively.
- Recognize potential COAs.
- Conduct mission preparation.
- Employ effective tactics, techniques, and procedures.
- Take appropriate security measures.
- Focus information collection.
- Conduct effective targeting.

COMMANDER'S GUIDANCE

3-8. Commanders drive the intelligence process by providing commander's guidance and approving priority intelligence requirements (PIRs). While it is not part of the intelligence process, commander's guidance is one of the primary mechanisms used to focus the intelligence process. When approving their PIRs, commanders should limit the number of PIRs so the staff can focus its efforts and allocate sufficient resources. Each commander dictates which intelligence products are required, when they are required, and in what format.

INTELLIGENCE PROCESS STEPS

3-9. The intelligence process leverages all sources of information and expertise, including the intelligence community and nonintelligence entities, to provide situational awareness to the commander and staff. The intelligence warfighting function uses the intelligence process as a management tool to ensure the right information gets to the right users at the right time in a useable format without inundating users. Just as the activities of the operations process overlap and recur as the mission demands, so do the steps of the intelligence process.

3-10. Intelligence activities are enabled by and subject to laws, regulations, and policies to ensure the proper conduct of intelligence operations. While there are too many to list, legal authorities include the USCs, executive orders (EOs), National Security Council and DOD directives, Army regulations, U.S. SIGINT directives, status-of-forces agreements (also called SOFAs), rules of engagement, and other relevant international laws. Commanders will request assistance from their servicing judge advocate to interpret or deconflict these legal authorities.

PLAN AND DIRECT

3-11. Each staff element must conduct analysis before operational planning can begin. Planning consists of two separate but closely related components—conceptual and detailed planning. Conceptual planning involves understanding the operational environment and the problem, determining the operation's end state, and visualizing an operational approach. Detailed planning translates the broad operational approach into a complete and practical plan. (For more information on conceptual and detailed planning, see ADRP 5-0.)

3-12. The initial generation of intelligence knowledge about the operational environment occurs far in advance of detailed planning and orders production. This intelligence assists in focusing information collection once a mission is received or in anticipation of a mission. Commanders and staffs often begin planning in the absence of a complete and approved higher headquarters' operation plan or operation order. In these instances, the headquarters begins a new planning effort based on a warning order and other directives, such as a planning order or an alert order from their higher headquarters.

3-13. Intelligence planning is also an inherent part of the Army design methodology and the military decision-making process. Intelligence analysts must prepare detailed planning products for the commander and staff for orders production and the conduct of operations. Through thorough and accurate planning, the staff allows the commander to focus the unit's combat power to achieve mission success.

3-14. The plan and direct step also includes activities that identify key information requirements and develops the means for satisfying those requirements. The intelligence staff collaborates with the operations and signal staffs to plan the intelligence architecture. Collaboration facilitates parallel planning and enhances all aspects of the intelligence process by enriching analysis, incorporating different points of view, and broadening situational understanding. The staffs produce a synchronized and integrated information collection plan focused on answering PIRs and other requirements. PIRs and other requirements drive the information collection effort.

3-15. Commanders must employ organic collection assets as well as plan, coordinate, and articulate requirements to leverage DOD intelligence capabilities. Commanders and staffs cannot expect higher echelons to automatically provide all of the information and intelligence they need. While intelligence reach is a valuable tool, the push of intelligence products from higher echelons does not relieve subordinate staffs from developing specific and detailed requirements. Commanders and staffs must focus requests for intelligence support by clearly articulating requirements.

3-16. The staff focuses information collection plans on answering CCIRs and other requirements and enables the quick retasking of units and assets as the situation changes. Collection management includes continually identifying intelligence gaps. This ensures the developing threat situation and civil considerations—not only the operation order—drive information collection. Specifically, G-2/S-2s—

- Evaluate information collection assets for suitability (availability, capability, vulnerability, and performance history) to execute information collection tasks and make appropriate recommendations on asset tasking to the primary operations staff officers.
- Assess information collection against CCIRs and other requirements to determine the effectiveness of the information collection plan. They maintain awareness to identify gaps in coverage and identify the need to cue or recommend redirecting information collection assets to the primary operations staff officers.
- Update the collection management tools as requirements are satisfied, added, modified, or deleted. They remove satisfied requirements and recommend new requirements as necessary.

Requirements

3-17. For collection managers, there are three types of requirements resulting from collection management. The following three types of validated information requirements are prioritized for purposes of assigning information collection tasks:

- PIRs.
- Intelligence requirements.
- Information requirements.

3-18. Collection managers must understand how collection and PED assets are distributed as they develop and validate requirements. They must also understand that some requirements can be answered through intelligence reach. Figure 3-2 shows the process of developing requirements and integrating them into the information collection process. (See FM 3-55 and ATP 2-01 for more details on requirements and indicators.)

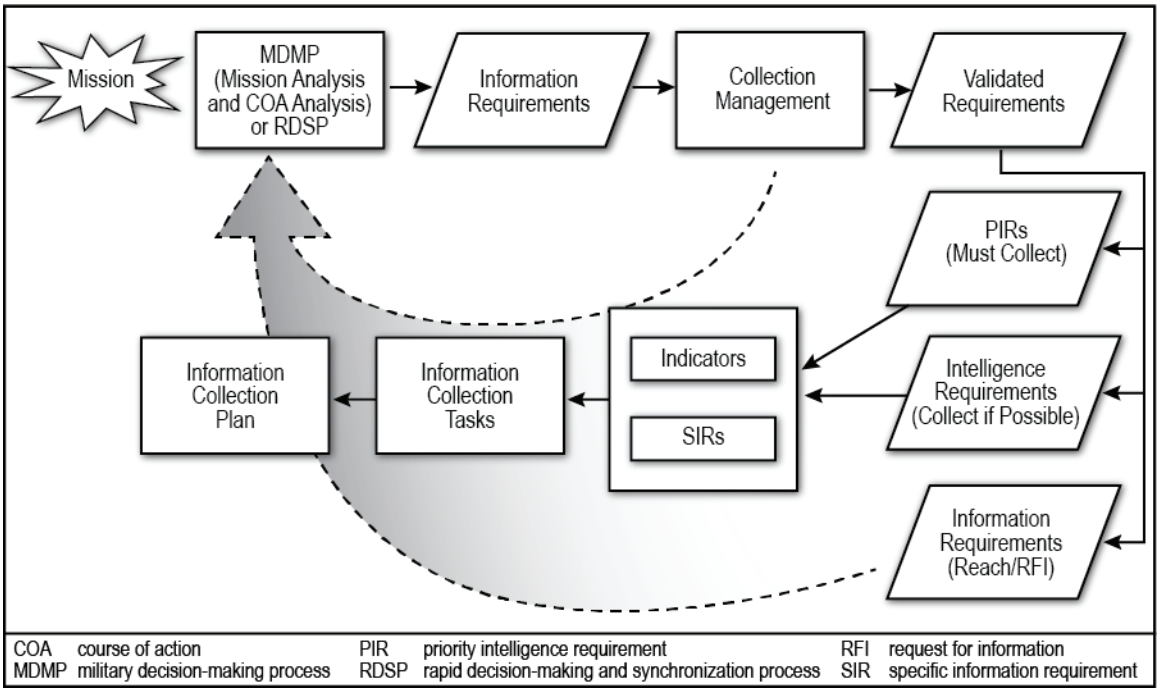


Figure 3-2. Requirements development

Intelligence Reach

3-19. ***Intelligence reach*** **is the activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command**. Information can be acquired through the push and pull of information, databases, homepages, collaborative tools, and broadcast services. Intelligence reach also supports reach PED and distributed analysis. (Reach PED refers to PED capabilities at centralized locations where sensor data is disseminated for intelligence PED support.) Three important aspects of intelligence reach are searches and queries, data mining, and collaboration. (See FM 2-0 for more information on intelligence reach.)

COLLECT AND PROCESS

3-20. The intelligence staff synchronizes collection and processing to provide critical information at key times throughout the phases of an operation. Collection and processing are mutually dependent. Staffs should never allow a seam to emerge between collection and processing, even when elements conducting those functions are separated geographically. The intelligence staff continuously monitors the results not only of information collection but also of processing to continuously assess the effectiveness of the overall information collection effort.

3-21. Information collection and processing activities transition when requirements change, the unit mission changes, the unit proceeds through the phases of an operation, or the unit prepares for future operations. Successful information collection and processing results in timely collection and reporting of relevant and accurate information, which supports the production of intelligence. The intelligence staff coordinates with other unit staffs, subordinate and lateral commands, and higher echelon units to ensure specific units, capabilities, personnel, equipment (especially communications), and procedures are in place.

3-22. *Collection* is, in intelligence usage, the acquisition of information and the provision of this information to processing elements (JP 2-01). Different units and systems collect information and data about threats, terrain and weather, and civil considerations through the four primary means of information collection: reconnaissance, surveillance, security operations, and intelligence operations. Collection includes the maneuver or movement of units and systems to effective locations and the associated force protection measures based on an order or tasking.

3-23. Successfully collecting timely, relevant, and useful information against an adaptive threat is difficult. It is critical for the staff to plan for and use well-developed procedures and flexible planning to track emerging targets, adapt to changing operational requirements, and meet the requirement for combat assessment. A successful collection and processing effort requires the intelligence staff, intelligence analysts, and collectors to form an efficient assessment and feedback loop. Success also requires the staff, analysts, and collectors to watch for threat countermeasures, denial activities, and threat deception. The last step of the feedback loop involves the intelligence staff evaluating reported information for its accuracy and responsiveness to information collection tasks and providing feedback to control elements and collectors.

3-24. Intelligence personnel distribute collected data and information via appropriately classified means and networks for further processing and analysis. During processing, intelligence personnel and systems convert raw data into forms of information commanders, staffs, intelligence analysts, and other consumers can use. Processing may occur immediately within the brain of the data collector, due to the collector's operational knowledge, experience, and situational understanding. However, intelligence personnel and systems often perform processing as a separate but associated function, either at the point of collection or at a separate location.

3-25. Processing includes first-phase imagery exploitation, data conversion and correlation, document and media translation, and signal decryption. For example, processing occurs when the technical parameters (frequency, pulse repetition frequency, and bandwidth) detected by an electronic intelligence (ELINT) collection system are compared and associated with the known parameters of a particular radar system. Rather than providing an analyst with an overwhelming mass of raw ELINT data, the system provides the analyst with the specific type of radar detected.

3-26. Different types of data require different degrees of processing before recipients can understand them. Within SIGINT, processing is increasingly automated and quickly performed by collection systems. Similarly, captured enemy documents may only require translation before an analyst can exploit the information they contain. On the other hand, technical exploitation of an item of enemy equipment may require months of intensive effort to determine its full capabilities. Following established guidelines, analysts must ensure data passes to standardized databases as soon as possible. In some situations, data requires processing to convert it into a format compatible with certain storage means.

3-27. At any point in the intelligence process, intelligence and time-sensitive combat information that affect the current operation are disseminated immediately upon recognition. *Combat information* is unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements (JP 2-01). The routing of combat information proceeds immediately in two directions—directly to the commander and through routine reporting channels for use by intelligence analysis and production elements.

3-28. Generally, intelligence PED capabilities execute processing for intelligence operations. Intelligence PED involves performing initial analysis to provide context, passing the information on for further analysis or reporting of combat information, and providing feedback on the effectiveness of the collection effort. These closely related PED functions are an inherent part of the collection effort. By performing them faster, more efficiently, and more accurately, intelligence personnel improve the entire intelligence process.

PRODUCE

3-29. Production is the development of intelligence through the analysis of collected information and existing intelligence. Analysts create intelligence products, conclusions, or projections regarding threats and relevant aspects of the operational environment to answer known or anticipated requirements in an effective format. The intelligence staff processes and analyzes information from single or multiple sources, disciplines, and complementary intelligence capabilities, and integrates the information with existing intelligence to create finished intelligence products.

3-30. Intelligence products must be timely, relevant, accurate, predictive, and tailored to facilitate situational understanding and support decision making. The accuracy and detail of intelligence products have a direct effect on operational success. Due to time constraints, analysts sometimes develop intelligence products that are not as detailed as they prefer. However, a timely, accurate answer that meets the commander's requirements is better than a more detailed answer that is late.

3-31. The intelligence staff prioritizes and synchronizes the unit's information processing and intelligence production efforts. The intelligence staff addresses numerous and varied production requirements based on PIRs and other requirements; diverse missions, environments, and situations; and user-format requirements. Through analysis, collaboration, and intelligence reach, the G-2/S-2 and staff use the intelligence capability of higher, lateral, and subordinate echelons to meet processing and production requirements.

3-32. Analysis occurs to ensure the information is relevant, to isolate significant elements of information, and to integrate the information into an intelligence product. Additionally, analysis of information and intelligence is important to ensure the focus, prioritization, and synchronization of the unit's intelligence production effort is in accordance with the PIRs and other requirements.

DISSEMINATE

3-33. Commanders and unified action partners must receive combat information and intelligence products in time and in an appropriate format to facilitate situational understanding and support decision making. Central to the successful dissemination to unified action partners is the early and continuous involvement of the foreign disclosure officer and supporting foreign disclosure representatives. Timely dissemination of intelligence and finished intelligence products is critical to the success of operations. Dissemination is deliberate and ensures consumers receive intelligence to support operations.

3-34. This step does not include the normal reporting and technical channels otherwise conducted by intelligence warfighting function organizations and units during the intelligence process. Each echelon with access to relevant information may perform analysis on that information. Thus, each echelon ensures that resulting intelligence products are properly disseminated. Determining the product format and selecting the means to deliver it are key aspects of dissemination.

3-35. The commander and staff must establish and support a seamless intelligence architecture including an effective dissemination plan. A dissemination plan can be a separate product or integrated into existing products, such as the collection management tools. The plan must include provisions for dissemination to unified action partners.

3-36. Intelligence and communications systems continue to evolve in their sophistication, application of technology, and accessibility to the commander, staff, and unified action partners. Their increasing capabilities also create an unprecedented volume of information available to commanders at all echelons. The commander and staff must have a basic understanding of intelligence dissemination systems and their contribution to the intelligence warfighting function.

Dissemination Methods and Techniques

3-37. There are numerous methods and techniques for disseminating information and intelligence. The appropriate technique in any particular situation depends on many factors, such as capabilities and mission requirements. Information presentation may be in a verbal, written, interactive, or graphic format. The type of information, time allocated, and commander's preferences all influence the information format. Answers to PIRs require direct dissemination to the commander, subordinate commanders, and staff. Direct dissemination is conducted person-to-person, by voice communications, or electronic means. Other dissemination methods and techniques include—

- Direct electronic dissemination (a messaging program).
- Instant messaging.
- Web posting (with notification procedures for users).
- Printing or putting the information on a compact disk and sending it.

3-38. Disseminating intelligence simultaneously to multiple recipients is one of the most effective, efficient, and timely methods, and can be accomplished through various means—for example, push or broadcast.

3-39. G-2/S-2s must plan methods and techniques to disseminate information and intelligence when normal methods and techniques are unavailable. For example, information and intelligence can be disseminated using liaisons or regularly scheduled logistic packages as long as any classified information is properly protected and individuals are issued courier orders.

Dissemination Channels

3-40. Intelligence leaders at all levels assess the dissemination of intelligence and intelligence products. Reports and other intelligence products move along specific channels within the intelligence architecture. The staff assists in streamlining information distribution within these channels by ensuring dissemination of the right information in a timely manner to the right person or element. The three channels through which commanders and their staffs communicate are command channels, staff channels, and technical channels.

Presentation Techniques and Procedures

3-41. Presentation is important and serves as the conclusion of the intelligence process. One of the most difficult challenges within mission command is effectively visualizing the operational environment. The intelligence staff must provide the commander with relevant information that supports the commander's visualization, facilitates situational understanding, and enables decision making. The presentation method is based on the commander's guidance but often requires creative solutions to most effectively and efficiently present the intelligence and other information.

3-42. Presentations can be formal or informal. The three general methods the staff uses to present information are written narrative, verbal narrative, and graphic format. Intelligence systems contain standard report formats, maps, and mapping tools that assist the staff in presenting information. Audio and video systems,

such as large format displays and teleconferencing systems, enable the staff to use a combination of these methods in multimedia presentations.

INTELLIGENCE PROCESS CONTINUING ACTIVITIES

3-43. Analyze and assess are two continuing activities that shape the intelligence process. Analyze and assess form part of the overall assessment activity of the operations process and occur continually throughout the intelligence process.

ANALYZE

3-44. Analysis assists commanders, staffs, and intelligence leaders in framing the problem, stating the problem, and solving it. Leaders at all levels conduct analysis to assist in making many types of decisions. Analysis occurs at various stages throughout the intelligence process and is inherent throughout intelligence support to situational understanding and decision making. Collectors and analysts perform initial analysis—often referred to within intelligence as exploitation during the collect and process step—before reporting or otherwise distributing the information to single and all-source analysis elements. For example, a collector may add context to information (analysis) based on previously acquired experience and knowledge, prior to dissemination.

3-45. Analysis in collection management is critical to ensuring information requirements receive the appropriate priority for collection. The intelligence staff analyzes each requirement to determine—

- The requirement's feasibility and whether it supports the commander's guidance.
- The best method of satisfying the requirement (for example, what unit or capability and where to position that capability).
- If the collected information satisfies the requirement.

3-46. Analysis is used in situation development to determine the significance of collected information and its significance relative to predicted threat COAs and PIRs and other requirements. Through predictive analysis, staffs attempt to identify threat activity or trends that present opportunities or risks to the friendly force. They often use indicators developed for each threat COA as the basis for their analysis and conclusions.

ASSESS

3-47. Assess is part of the overall assessment activity of the operations process. For intelligence purposes, assessment is the continuous monitoring and evaluation of the current situation, particularly significant threat activities and changes in the operational environment. Assessing the situation begins upon receipt of the mission and continues throughout the intelligence process. This assessment allows commanders, staffs, and intelligence leaders to ensure intelligence synchronization. Friendly actions, threat actions, civil considerations, and events in the area of interest interact to form a dynamic operational environment. Continuous assessment of the effects of each element on the others, especially the overall effect of threat actions on friendly operations, is essential to situational understanding.

3-48. The intelligence staff continuously produces assessments based on operations, the information collection effort, the threat situation, and the status of relevant aspects of the operational environment. These assessments are critical to—

- Ensure PIRs are answered.
- Ensure intelligence requirements are met.
- Redirect collection assets to support changing requirements.
- Ensure operations run effectively and efficiently.
- Ensure proper use of information and intelligence.
- Identify threat efforts at deception and denial.

3-49. The intelligence staff continuously assesses the effectiveness of the information collection effort. This type of assessment requires sound judgment and a thorough knowledge of friendly military operations; characteristics of the area of interest; and the threat situation, doctrine, patterns, and projected COAs.

Chapter 4
Army Intelligence Capabilities

The intelligence warfighting function executes the intelligence process by employing intelligence capabilities. All-source intelligence and single-source intelligence are the building blocks by which the intelligence warfighting function facilitates situational understanding and supports decision making. The intelligence warfighting function receives information from a variety of capabilities. Some of these capabilities are commonly referred to as single-source capabilities. Single-source capabilities are employed through intelligence operations with the other means of information collection (reconnaissance, surveillance, and security operations). PED capabilities are also necessary to process information and prepare it for subsequent analysis. The intelligence produced based on all of those capabilities is called all-source intelligence.

ALL-SOURCE INTELLIGENCE

4-1. Army forces conduct operations based on all-source intelligence assessments and products developed by the intelligence staff. ***All-source intelligence*** **is the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations.** In joint doctrine, *all-source intelligence* is intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence (JP 2-0).

ALL-SOURCE ANALYSIS

4-2. The fundamentals of all-source intelligence analysis comprise intelligence analysis techniques and the all-source analytical tasks: situation development, generating intelligence knowledge, IPB, and support to targeting and information operations.

4-3. Through the receipt and processing of incoming reports and messages, the intelligence staff determines the significance and reliability of incoming information, integrates incoming information with current intelligence holdings, and through analysis and evaluation determines changes in threat capabilities, vulnerabilities, and probable COAs. The intelligence staff supports the integrating processes (IPB, targeting, and risk management) and continuing activities (information collection) by providing all-source analysis of threats, terrain and weather, and civil considerations.

4-4. All-source intelligence is used to develop the intelligence products necessary to aid situational understanding, support the development of plans and orders, and answer information requirements. Although all-source intelligence normally takes longer to produce, it is more reliable and less susceptible to deception than single-source intelligence.

ALL-SOURCE PRODUCTION

4-5. Fusion facilitates all-source production. For Army purposes, ***fusion*** **is consolidating, combining, and correlating information together**. Fusion occurs as an iterative activity to refine information as an integral part of all-source analysis.

4-6. All-source intelligence production is continuous and occurs throughout the intelligence and operations processes. Most of the products from all-source intelligence are initially developed during planning and updated, as needed, throughout preparation and execution based on information gained from continuous assessment.

ALL-SOURCE AND IDENTITY ACTIVITIES

4-7. Joint doctrine describes identity activities as a collection of functions and actions that appropriately recognize and differentiate one person from another to support decision making. They include the collection of identity attributes and physical materials; their processing and exploitation; all-source analytic efforts, production of identity intelligence and DOD law enforcement criminal intelligence products; and dissemination of those products to inform policy and strategy development, operational planning and assessment, and the appropriate action at the point of encounter. These functions and actions are conducted by maneuver, intelligence, and law enforcement components.

4-8. Within intelligence, identity activities are the responsibility of the personnel within the all-source elements of the intelligence staff. Within all-source, identity activities combine the synchronized application of the complementary intelligence capabilities (biometrics, forensics, and document and media exploitation [DOMEX]) with intelligence and identity management processes. This establishes identity, affiliations, and authorizations in order to deny anonymity to the adversary and protect U.S. and partner nation assets, facilities, and forces. These all-source activities result in the discovery of true identities; link identities to events, locations, and networks; and reveal hostile intent. These outputs enable tasks, missions, and actions that span the range of military operations.

SINGLE-SOURCE INTELLIGENCE

4-9. Single-source intelligence includes the joint intelligence disciplines and complementary intelligence capabilities. Intelligence PED capabilities are a critical aspect of single-source intelligence activities that ensure the results of collection inform single- and all-source analysis. MI units can conduct intelligence operations with a single intelligence discipline or complementary intelligence capability or as a multifunction intelligence operation, which combines activities from two or more intelligence disciplines or complementary intelligence capabilities.

4-10. Information moves throughout various echelons along specific transmission paths or channels. Establishing command and support relationships directs the flow of reported information during intelligence operations. Channels assist in streamlining information dissemination by ensuring the right information passes promptly to the right people. Commanders and staffs normally communicate through three channels: command, staff, and technical. (See ADRP 6-0 and FM 6-02.71.)

TECHNICAL CHANNELS

4-11. Technical channels, while not a command or support relationship, often affect intelligence operations. For intelligence operations, technical channels are the transmission paths between intelligence units (including sections) performing a technical function requiring special expertise. Technical channels control the performance of technical functions. They neither constitute nor bypass command authorities; rather, they serve as the mechanism for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of unified land operations.

4-12. Commanders direct operations but often rely on technical expertise to plan, prepare, execute, and assess the unit's collection effort. Technical channels also involve translating information collection tasks into the specific parameters used to focus highly technical or legally sensitive aspects of the information collection effort. Technical channels include but are not limited to—

- Defining, managing, or prescribing specific employment techniques.
- Identifying critical technical collection criteria such as technical indicators.
- Recommending collection techniques, procedures, or assets.
- Conducting operational reviews.
- Conducting operational coordination.
- Conducting specialized intelligence training.

4-13. Through technical channels, commanders and staffs ensure adherence to applicable laws and policies, ensure proper use of doctrinal techniques, and provide technical support and guidance. Applicable laws and policies include all relevant U.S. law, the law of war, international law, DOD directives and instructions, and

orders. For specific intelligence discipline collection, regulatory authority is maintained by national and DOD intelligence agencies and is passed through technical channels. (See FM 2-0 for more on technical channels.)

THE INTELLIGENCE DISCIPLINES

4-14. In joint operations, intelligence collection and activities are commonly organized around the intelligence disciplines, which include—

- CI.
- GEOINT.
- HUMINT.
- Measurement and signature intelligence (MASINT).
- Open-source intelligence (OSINT).
- SIGINT.
- Technical intelligence (TECHINT).

4-15. The intelligence disciplines are integrated to ensure a multidiscipline approach to intelligence analysis, and ultimately, all-source intelligence facilitates situational understanding and supports decision making. Each discipline applies unique aspects of support and guidance through technical channels. (See JP 2-0.)

Counterintelligence

4-16. Army CI counters or neutralizes foreign intelligence collection efforts through collection, CI investigations, operations, analysis, production, and technical services and support. CI includes all actions taken to detect, identify, disrupt, neutralize, or exploit foreign intelligence entity collection efforts directed against DOD and Army personnel, operations, information, material, facilities, technology, and networks. It is the key intelligence community contributor to protecting U.S. interests and equities.

4-17. *Foreign intelligence entity* is any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire United States information, block or impair United States intelligence collection, influence United States policy, or disrupt United States systems and programs. The term includes foreign intelligence and security services and international terrorists (JP 2-01.2). It also includes insurgents, other adversary intelligence threats, and insider threats targeting or suspected of targeting U.S. forces personnel, operations, facilities, networks, information, and technology for intelligence gathering or planning and preparation for an attack or exploitation. (See ATP 2-22.2-1.)

4-18. The role of Army CI is to conduct aggressive, comprehensive, and coordinated investigations, operations, collection, intelligence PED, analysis and production, and technical services. These functions are conducted worldwide to detect, identify, assess, counter, exploit, or neutralize the foreign intelligence entity collection threat. Army CI has four primary mission areas:

- **Counterespionage.** Counterespionage refers to those CI defensive and offensive endeavors to detect, identify, assess, counter, neutralize, or exploit the foreign intelligence entity threat.
- **CI support to force protection.** While force protection is the responsibility of commanders at all levels, Army CI contributes to protection of the force. CI collection, analysis, investigations, and operations are designed to identify foreign intelligence and international terrorist activities that threaten military personnel, civilian employees, and units. Army CI exercises every available authority to support the force protection plans of Army and supported DOD commanders worldwide in accordance with AR 381-20 (classified), DODM 5240.01 for procedures 1-10, DOD 5240.1-R for procedures 11-15, and AR 381-10. In the performance of this function, CI will collect and report information that satisfies standing CI collection requirements.
- **CI support to research, development, and acquisition.** This support is accomplished to prevent the illegal diversion or loss of critical technology essential to the strategic advantage of the United States in future conflicts.
- **CI-cyber.** CI-cyber refers to the use of techniques and measures to identify, exploit, or neutralize adversary cyberspace espionage that uses the internet, information resources, and digital media as the primary tradecraft methodology.

4-19. CI core functions are interrelated, mutually supporting, and can be derived from one another. No single function can defeat the foreign intelligence entity collection threat. The CI core functions are—

- **Operations.** CI operations are broadly executed CI activities that support a program or specific mission. CI operations use one or more of the CI functions. CI operations can be offensive or defensive, and they are derived from, transitioned to, or used simultaneously—depending on the scope, objective, or continued possibility for operational exploitation.
- **Investigations.** Army CI will conduct aggressive and comprehensive investigations worldwide to detect, identify, assess, and counter, neutralize, or exploit the foreign intelligence entity, foreign and insider threat (as defined in DODI 5240.26) to the Army and DOD whenever such threat is within CI jurisdiction.
- **Collection.** CI collection is the systematic acquisition of information concerning the foreign intelligence entity collection threat. CI elements conduct collection activities to support the overall CI mission. CI collection is conducted by using sources, elicitation, official liaison contacts, debriefings, screenings, and OSINT to obtain information that answers standing CI collection requirements or other collection requirements.
- **Technical services and support.** CI technical services are used to assist the CI core functions of investigations, collections, and operations or to provide specialized technical support to a program or activity. The proliferation of sophisticated collection technology, surveillance, and "eaves-dropping" devices available in commercial markets enable any foreign intelligence entity with the ability to increase its capability and effectiveness.
- **Analysis and production.** CI analysis is used to satisfy the supported commander's intelligence requirements and provide focus and guidance to CI operations. CI analysis and production can be accomplished at any level in which Army CI assets are assigned to support any of the four primary mission areas.

4-20. CI organizations and force structure are designed to support Army forces through scalable team, operations management, and technical channel packages. The CI and HUMINT staff officer (also called G-2X/S-2X) structure supports decentralized CI operations. The establishment of the CI and HUMINT staff element (also called 2X) and the CI coordinating authority throughout the Army ensures a trained and experienced cadre of CI professionals to support operations. (See ATP 2-22.2-1 for more information on CI.)

Geospatial Intelligence

4-21. *Geospatial intelligence* is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information (JP 2-03). (Section 467, Title 10, USC, establishes GEOINT.)

Note. GEOINT consists of any combination of the following components: imagery, and/or imagery intelligence with geospatial information.

4-22. *Imagery* is a likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likenesses and presentations produced by satellites, aircraft platforms, unmanned aircraft systems, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations) (JP 2-03).

4-23. *Imagery intelligence* is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials (JP 2-03).

4-24. *Geospatial information* is information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products (JP 2-03).

4-25. The GEOINT cell provides geospatial data generation, geospatial data analysis, geospatial data management, quality control, and data dissemination. GEOINT supports the multidirectional flow and integration of geospatially referenced data from all sources to achieve shared situational understanding of the operational environment, near real-time tracking, and collaboration between forces.

4-26. GEOINT activities necessary to support operations include the capability to define GEOINT requirements, discover and obtain GEOINT, put GEOINT in a useable form, and then maintain, use, and share GEOINT. The GEOINT cell interfaces directly with the user to define user requirements. Then the cell interfaces with the National System for Geospatial Intelligence to obtain and provide the best quality GEOINT possible directly to the Soldier. (For more information on GEOINT, see ATP 2-22.7, ATP 3-34.80, and AR 115-11.)

4-27. The GEOINT cell supports operations through five tasks:

- Define GEOINT mission requirements.
- Obtain mission-essential GEOINT.
- Evaluate available GEOINT data.
- Use and disseminate GEOINT.
- Maintain and evaluate GEOINT.

Human Intelligence

4-28. ***Human intelligence*** **is the collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities**.

4-29. A HUMINT source is a person from whom foreign information is collected to produce intelligence. HUMINT sources can include friendly, neutral, or hostile personnel. The source may either possess first- or second-hand knowledge normally obtained through sight or hearing. Categories of HUMINT sources include but are not limited to detainees, enemy prisoners of war, refugees, displaced persons, local inhabitants, friendly forces, and members of foreign governmental and nongovernmental organizations.

4-30. A HUMINT collector is a person who is trained, certified, and authorized to collect information from individuals (HUMINT sources) for the purpose of answering information collection requirements. HUMINT collectors are the only personnel authorized to conduct HUMINT collection operations. They are trained and certified enlisted personnel in military occupational specialty 35M, warrant officers in 351M, commissioned officers in 35F, and their Federal civilian employee counterparts. However, in order to conduct intelligence interrogations, trained HUMINT collectors must successfully complete one of the following courses, which are the only accepted interrogation training sources for military personnel:

- 35M Basic HUMINT Collector course at the U.S. Army Intelligence Center of Excellence, Fort Huachuca, Arizona.
- U.S. Marine Corps Basic Marine Air-Ground Task Force CI/HUMINT course at the Navy and Marine Corps Intelligence Center, Dam Neck, Virginia.
- Joint Interrogation Certification course at the HUMINT Training-Joint Center of Excellence, Fort Huachuca, Arizona. (Although this course has been discontinued, successful course graduates are authorized to conduct interrogations.)
- Defense Intelligence Agency I-10 course, Alexandria, Virginia. (Although this course has been discontinued, successful course graduates are authorized to conduct HUMINT interrogations.)

Note. Certification is conducted at the discretion of the combatant commander in accordance with established combatant command policies and directives.

4-31. HUMINT collection operations must be conducted in accordance with all applicable U.S. law and policy, which include EO 12333 as amended; EO 13491; DODM 5240.01 for procedures 1-10; DOD 5240.1-R for procedures 11-15; the law of war; relevant international law; relevant directives, including DODD 2310.01E and DODD 3115.09; DOD instructions; AR 381-100; FM 2-22.3; and military orders, including fragmentary orders. Additional policies and regulations apply to the management of contractors

engaging in HUMINT collection. Commanders will request assistance from their servicing judge advocate to interpret or deconflict these legal authorities. (See FM 2-22.3, ATP 2-22.31 [classified], and AR 381-100.)

4-32. HUMINT operations collect information from human sources through overt and clandestine means. HUMINT operations focus on a wide range of sources (such as detainees, refugees, civilians, friendly forces, and recruited personnel) for information that includes but is not limited to an adversary's plans, intentions, and strategies; research and development goals; physical and cultural infrastructure; and medical information.

4-33. Every HUMINT questioning session, regardless of the methodology used or the type of operation, consists of five phases. The five phases of HUMINT collection are—

- Planning and preparation.
- Approach.
- Questioning.
- Termination.
- Reporting.

4-34. The phases are generally sequential; however, reporting may occur at any point within the process when critical information is obtained and the approach techniques used will be reinforced, as required, through the questioning and termination phases.

4-35. HUMINT collection methodologies include five categories:

- Screening.
- Interrogation.
- Debriefing.
- Military source operations.
- Liaison.

Measurement and Signature Intelligence

4-36. *Measurement and signature intelligence* is information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event (JP 2-0). (For more information on MASINT, see JP 2-0 and ATP 2-22.8 [classified]).

4-37. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical, acoustic, radio frequency, and seismic sensors, as well as techniques for collecting chemical, biological, radiological, and nuclear (CBRN) signatures and other materiel samples.

4-38. MASINT requires the translation of technical data into recognizable and useful target features and performance characteristics. Computer, communications, data, and display processing technologies now provide MASINT to support operations.

4-39. MASINT provides intelligence to the commander to facilitate situational understanding and support targeting. Many sensors can defeat many of the camouflage, concealment, and deception techniques currently used to deceive information collection systems. Specifically, MASINT sensors have unique capabilities to detect missile launches; detect and track aircraft, ships, and vehicles; perform noncooperative target identifications and combat assessments; and detect and track fallout from nuclear detonations. Often, these sensors provide the first indicators of hostile activities.

4-40. The MASINT systems most familiar to Soldiers are employed by ground surveillance and CBRN reconnaissance elements. These systems span the entire EMS and their capabilities complement the other intelligence disciplines. MASINT provides, to varying degrees, the capability to—

- Use automatic target recognition and aided target recognition.
- Penetrate man-made and natural camouflage.
- Penetrate man-made and natural cover, including the ability to detect subterranean anomalies or targets.
- Counter stealth technology.
- Detect recently placed mines.
- Detect natural or man-made environmental disturbances in the Earth's surface not discernible through other intelligence means.
- Provide signatures (target identification) to munitions and sensors.
- Enhance passive identification of friend or foe.

- Detect the presence of CBRN agents including before, during, or after employment.
- Detect signature anomalies that may affect target-sensing systems.

4-41. Within DOD, the Defense Intelligence Agency provides policy and guidance for MASINT. Its policy and guidance do not interfere with Service component operations. Each Service has a primary command or staff activity to develop requirements and coordinate the MASINT effort. The Army G-2 staff is the functional manager for Army MASINT resources, policy, and guidance. Army weapons systems programs that require MASINT information to support system design or operations submit requests through INSCOM channels for data collection and processing.

4-42. The scientific and technical intelligence (S&TI) community also performs MASINT collection and processing primarily to support research and development programs and signature development. Every S&TI center has some involvement in MASINT collection or production that reflects that center's overall mission (for example, NGIC has responsibility for armored vehicles and artillery). Service research and development centers, such as the Communications-Electronics Command Research, Development, and Engineering Center, the Army Research Laboratory, and the Night Vision and Electronic Systems Laboratory, are also involved in developing sensor systems for collecting and processing MASINT. Elements within the Army Space and Missile Defense Command also exploit satellite-collected data for the purpose of MASINT exploitation. In addition to supporting the S&TI mission, INSCOM units also execute limited ground-based operational collection to support the ASCCs and subordinate units.

Open-Source Intelligence

4-43. OSINT is integral to Army intelligence operations. *Open-source intelligence* is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (Public Law 109-163). OSINT is exclusive to intelligence professionals using open-source information to answer specific intelligence requirements. In contrast, open-source *research* is the gathering of data, facts, instructions, or other material that is publicly available and used for general knowledge about a specific person, location, weapons system, or other item of interest. Open-source research is not OSINT. Any staff element may use open-source information to answer many different types of requirements.

4-44. Section 3038, Title 50, USC, and EO 12333 as amended govern OSINT. As such, OSINT is produced by intelligence professionals to support Army commanders in developing an understanding of complex situations, support fused all-source analysis, tip, and support intelligence operations and activities in other intelligence disciplines. (For more information, see ATP 2-22.9.)

4-45. *Open-source information* is information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access (JP 2-0). *Publicly available information* is information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public (DODM 5240.01).

4-46. There are many different forms of open sources, to include social, print, broadcast media; internet; and open public-speaking forums. The collection means (techniques) for obtaining publicly available information from these communications media must be nonintrusive.

Note. When there is any doubt about the conduct of OSINT activities, intelligence personnel consult their unit or organization staff judge advocate. All OSINT operations conducted by intelligence professionals must comply with the legal restrictions in EO 12333 as amended, DODM 5240.01 for procedures 1-10, DOD 5240.1-R for procedures 11-15, Army Directive 2016-37, and AR 381-10. Intelligence personnel conducting OSINT activities must comply with all operations security requirements prescribed in AR 530-1 to prevent disclosure of critical and sensitive information.

4-47. The following characteristics from the role of OSINT in Army operations:

- **OSINT provides the foundation.** Open-source information provides updates to foundation information and real-time ongoing information to assist in developing and enhancing intelligence products and the intelligence disciplines. There is much information about the political, military, economic, social, and infrastructure of a region or local area obtainable from open-source information and readily changed to OSINT products. This foundation information and intelligence products can be essential to generating a clear picture for the commander. The variety of foundational websites associated with social structures, education systems, and news services provides a foundational perspective for intelligence knowledge.
- **OSINT addresses requirements.** The availability, depth, and range of open-source information enable intelligence professionals to satisfy many PIRs and information requirements without the use of specialized human or technical means of collection.
- **OSINT enhances collection.** Open-source information supports other requirements and provides information that optimizes the employment and performance of sensitive human and technical collection means. Examples of this type of information include biographies, cultural information, geospatial information, and technical data.
- **OSINT enhances production.** As part of single-source and all-source intelligence production, the use and integration of OSINT ensure commanders have the benefit of all sources of available information.

Signals Intelligence

4-48. *Signals intelligence* is intelligence derived from communications, electronic, and foreign instrumentation signals (JP 2-0). SIGINT provides unique intelligence information, complements intelligence derived from other sources, and is often used for cueing other sensors to potential targets of interest. For example, SIGINT, which identifies activities of interest, may be used to cue GEOINT to confirm that activity. Conversely, changes detected by GEOINT can cue SIGINT collection. The discipline is subdivided into three subcategories: communications intelligence (also called COMINT), ELINT, and foreign instrumentation signals intelligence (also called FISINT).

4-49. *Communications intelligence* is technical information and intelligence derived from foreign communications by other than the intended recipients (JP 2-0). Communications intelligence includes collecting data from target or adversary automated information systems or networks. It also may include imagery when pictures or diagrams are encoded by a computer network or radio frequency method for storage or transmission. The imagery can be static or streaming.

4-50. *Electronic intelligence* is technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources (JP 3-13.1). ELINT consists of two subcategories:

- **Operational ELINT**—is concerned with operationally relevant information such as the location, movement, employment, tactics, and activity of foreign noncommunications emitters and their associated weapon systems.
- **Technical ELINT**—is concerned with the technical aspects of foreign noncommunications emitters such as signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels.

4-51. *Foreign instrumentation signals intelligence* is a subcategory of signals intelligence consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-United States aerospace, surface, and subsurface systems (JP 2-01).

4-52. SIGINT provides intelligence on threat intentions, capabilities, compositions, and dispositions. In addition, SIGINT provides information for the delivery of fires. The intelligence staff needs to understand how SIGINT assets are organized not only within the Army but also throughout DOD. The majority of SIGINT assets from the Armed Services, combined with national SIGINT assets, collaborate to support commanders from tactical to strategic levels. Only by understanding the SIGINT structure that transcends traditional Service components can the intelligence staff understand how to use SIGINT effectively.

Technical Intelligence

4-53. *Technical intelligence* is intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages (JP 2-0). The role of TECHINT is to ensure Soldiers understand the threat's full technological capabilities. With this understanding, U.S. forces can adopt appropriate countermeasures, operations, and tactics, techniques, and procedures. (For more information, see ATP 2-22.4.)

4-54. A comprehensive TECHINT network is vital to providing precise direction and purpose to DOD research and development and exploitation processes. This ensures quick and efficient neutralization of threat technological advantages and networks in direct support of the commander and S&TI community.

4-55. TECHINT has two primary responsibilities within Army intelligence operations:

- Provide information to supported commands based on the technical analysis of foreign material in accordance with those commands' stated requirements.
- Provide technical assessments of foreign technological threat capabilities, limitations, and vulnerabilities.

4-56. TECHINT includes S&TI, the Army Foreign Materiel Program, and weapons technical intelligence (WTI):

- S&TI organizations track and analyze foreign technological developments. They analyze the performance and operational capabilities of captured materiel that may have military applications.
- The Army Foreign Materiel Program is managed by the Army G-2. It is divided into foreign material acquisition, foreign material exploitation, and disposition of material no longer needed. The Army Foreign Materiel Program responds to U.S. weapons materiel developer TECHINT requirements, tactical requirements, and training requirements.
- As a function of counter-improvised explosive device operations, *weapons technical intelligence* is a subcategory of technical intelligence derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other systems (JP 3-15.1).

4-57. As a specific application of TECHINT, WTI combines technical assessments, forensic science, and other critical enablers with all-source intelligence for use against irregular and nontraditional threats. WTI operationalizes TECHINT and focuses on immediate exploitation of captured weapons to rapidly respond to the tactical commander's PIRs and other requirements. WTI integrates a range of collection, exploitation, and analysis capabilities to support four critical outputs:

- To enable targeting by identifying, selecting, prioritizing, and tracking individuals and matching them with groups, weapons materiel, financiers, suppliers, insurgent leaders, and other related elements.
- To technically and forensically examine events and devices or weapons to identify observables, signatures, and to better understand linkages between technical design and tactical use to guide efforts of the protection warfighting function, as well as tip and cue information collection.
- To provide trend, pattern, and forensic analysis of improvised explosive devices, improvised weapons, and weapons components usage to identify the origin of materiel and components.
- To use information from captured enemy materiel collected during site exploitation activities to further detain and potentially support the prosecution of individuals for criminal activity.

4-58. Every TECHINT mission supports tactical through strategic requirements by the timely collection and processing of materiel and information, follow-on analysis and resulting production of intelligence, and dissemination to a wide range of consumers. Commanders rely on TECHINT to provide them with tactical and technological advantages to successfully synchronize and execute operations. TECHINT combines information to identify specific individuals, groups, and nation-states, matching them to events, places, devices, weapons, equipment, or contraband that associates their involvement in hostile or criminal activity.

COMPLEMENTARY INTELLIGENCE CAPABILITIES

4-59. Complementary intelligence capabilities contribute valuable information for all-source intelligence to facilitate the conduct of operations. The complementary intelligence capabilities are specific to the unit and circumstances at each echelon and can vary across DOD. These capabilities include but are not limited to—

- Biometrics-enabled intelligence (also called BEI).
- Cyber-enabled intelligence.
- DOMEX.
- Forensic-enabled intelligence (also called FEI).

Biometrics-Enabled Intelligence

4-60. Joint doctrine defines *biometrics* as the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics (JP 2-0). Biometrics as a process of confirming identity is not exclusive to the intelligence warfighting function. This enabler supports multiple activities and tasks of other warfighting functions. Army doctrine defines *biometrics-enabled intelligence* as intelligence resulting from the combination of biometric information with other intelligence, threat information, or information relating to other aspects of the operational environment in order to answer intelligence requirements (ATP 2-22.82).

Biometric Analysis

4-61. It is important for commanders, intelligence staffs, and all-source intelligence analysts across all echelons to assist in consolidating identities, other information, and intelligence to support tactical objectives as well as longer-term operational and strategic objectives. The production of biometrics-enabled intelligence products is critical as persons of interest move from location to location (within an AO) or are elevated in status (and move from one position to another) or as they transit from one AO to another. Products derived from biometric collection can provide context that is critical—related to persons of interest and their intent—to analysts across all echelons.

4-62. DOD biometric-enabled watchlist (BEWL) management is a mission assigned to NGIC. As the DOD BEWL mission manager, NGIC is responsible for: discovering threat identities; reviewing unit nominations (to ensure nominations meet DOD and intelligence community standards); maintaining, managing, and disseminating BEWL subsets; and managing encounters. Development and management of the unit watchlist is an intelligence staff duty. In producing their BEWL, units include collected biometric identities, related contextual information, and intelligence for future reference or further analysis in the analytic system. Unit-level and DOD BEWLs are shared through a dissemination process to provide an unclassified data set on handheld devices to the other U.S. Government systems and the DOD biometric network for positive identification of threat personnel.

Biometric Reports

4-63. Division and above echelons develop many biometrics-enabled intelligence products to support operations, including—

- **Biometric intelligence analysis reports (also called BIARs).** This report is an intelligence product that associates a biometric match with an individual in the biometric database. It is produced by sorting, analyzing, and linking the biometric match with the individual's history, along with all-source intelligence. It may contain the identification, background, assessment, and intelligence value of the subject.
- **BEWLs.** The BEWL is the primary analytic product produced through the all-source analysis production of collected and processed identity records. It is exported from the analytic tool and shared with the biometric network to identify persons of interest within biometric matching systems and handheld devices. Establishing the BEWL to support specified missions is an intelligence staff-level responsibility. The intelligence staff can customize the BEWL based on the unit's assigned mission and rules of engagement. Assistance in establishing a new customized BEWL based on a unit's assigned mission can be coordinated through INSCOM and NGIC. After

establishing the customized BEWL, the nomination, removal, or change process is automated through the analytic tool. (For more information, see ATP 2-22.82).

Cyber-Enabled Intelligence

4-64. The cyberspace domain provides another medium for information collection. Cyber-enabled intelligence is a complementary intelligence capability that provides the ability to collect information and produce intelligence products that portray the threat's ability to operate within the cyberspace domain and the effect of the threat on friendly capabilities. Cyber-enabled intelligence is produced through the combination of intelligence analysis and information concerning activities in cyberspace and the EMS. This intelligence supports situational understanding of the cyberspace domain. Cyber-enabled intelligence is based on operations conducted within the cyberspace domain and does not include operations and dominance within the EMS.

Note. The results of cyberspace electromagnetic activities can provide intelligence professionals with a significant amount of information concerning both the physical domain and the information environment.

4-65. Cyber-enabled intelligence facilitates decision making at all levels through the analysis and production of relevant and tailored intelligence on activities in the cyberspace domain that may affect the unit's ability to conduct operations. The intelligence can range from broadly disseminated products focused on general users to very specific and narrowly focused analysis and reports distributed via classified channels. The use of cyber-enabled intelligence facilitates an understanding of the threat's cyberspace electromagnetic capabilities, intentions, potential actions, and vulnerabilities, and their impacts on the environment, friendly operations, and the local populace.

4-66. The mission, authority, and oversight of an activity determine whether the activity is cyber-enabled intelligence or cyberspace-controlled. For example, the use of computers, technology, and networks facilitate all-source intelligence, the intelligence disciplines, and the other complementary intelligence capabilities. However, their use of computers, technology, and networks does not mean these are cyberspace operations. The authority for each discipline or capability governs the guiding methods and regulations for the conduct of each intelligence discipline or complementary intelligence capability.

Document and Media Exploitation

4-67. *Document and media exploitation* is the processing, translation, analysis, and dissemination of collected hardcopy documents and electronic media that are under the U.S. Government's physical control and are not publicly available (ATP 2-91.8). Threat intent, capabilities, and limitations may be derived through the exploitation of captured documents and media.

4-68. DOMEX is an increasingly specialized, full-time mission requiring advanced automation and communications support, analytical support, and expert linguists. When conducted properly, DOMEX—

- Provides the commander an initial assessment of captured information.
- Maximizes the value of intelligence gained from captured enemy documents and media.
- Provides the commander with timely and relevant intelligence to effectively enhance awareness of the threat's capabilities, operational structures, and intent.
- Assists in criminal prosecution or legal proceedings by maintaining chain of custody procedures and preserving the evidentiary value of captured enemy materiel, documents, and media.

4-69. DOMEX products become a force multiplier only when captured materials are rapidly exploited at the lowest echelon possible. DOMEX assets pushed down to the tactical level provide timely and accurate intelligence support. These assets are primarily responsible for screening and tactical exploitation of captured documents and media. This practice not only enables rapid exploitation and evacuation of captured materials but also hastens the feedback commanders receive from the higher echelon analysis. DOMEX assets also deliver items of operational or strategic value to higher level processing facilities for further exploitation.

Intelligence staffs need to use the appropriate communications medium to pass vital information to the lowest echelon, especially to the capturing unit.

4-70. It is essential to pass critical information quickly to those who need it, specifically, tactical commanders. Intelligence staffs are responsible for reporting and disseminating DOMEX-derived information in a manner that ensures the information reaches not only the next higher echelon but also the tactical commander most affected by the information.

4-71. DOMEX personnel are usually not available below the battalion level except in MI organizations. This requires maneuver battalion intelligence staffs to prepare their subordinate units for DOMEX tasks. When intelligence and personnel qualified in the appropriate languages for the AO are available, they can be task-organized as intelligence support teams and placed with companies or platoons. Alternatively, the intelligence section can train company or platoon personnel in specific handling, screening, and inventorying techniques.

4-72. Where tactical assets are insufficient, operational and strategic assets can support a unit's organic assets, either by personnel augmentation or by virtual support from DOMEX support elements, who provide this support worldwide. These organizations use specialized techniques and procedures to extract additional information from captured audio and video materials. Application of specialized processing techniques and procedures may require the classification of the processed information and restrict its dissemination. (For more information on DOMEX, see ATP 2-91.8.)

Forensic-Enabled Intelligence

4-73. Forensics involves the scientific analysis of linking persons, places, things, and events. *Forensic-enabled intelligence* is the intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest (JP 2-0).

4-74. Forensic techniques provide timely and accurate information that facilitates situational understanding and supports decision making. This includes collecting, identifying, and labeling collected items for future exploitation. The collection of latent fingerprints, deoxyribonucleic acid (known as DNA), and other forensic data can aid in more in-depth analysis and better intelligence about the operational environment.

4-75. Forensic-enabled intelligence assists in accurately identifying persons, networks, and complex threats, and attributes them to specific incidents and activities. The effort is often critical in supporting the targeting process. Forensic-enabled intelligence can identify and determine the source of origin of captured materiel, documents, and media. Accurate site documentation of incidents or events, material and structural analysis, and supporting data and information from the various forensic processes and techniques can provide valuable data and enhance operational tactics, techniques, and procedures. For example, timely trace detection or material analysis of unknown substances can assist in protecting the force from contaminants, toxins, and other hazards. Incorporating information obtained via toxicology, pathology and other forensic techniques into forensic-enabled intelligence can assist in identifying health threats within the AO.

Intelligence Processing, Exploitation, and Dissemination Capabilities

4-76. Intelligence PED capabilities are the personnel, specialized intelligence and communications systems, software and advanced technologies that execute the PED functions. Intelligence PED operations can be performed either from a deployed expeditionary location or a reach site in theater or the United States. Intelligence PED capabilities can be organic to the intelligence unit, task-organized, or distributed from a centralized location through the network as required.

4-77. The effort to plan and control intelligence PED is part of mission command. The G-2/S-2 advises the staff on intelligence PED requirements and capabilities when planning information collection operations. The commander and staff resource and prioritize supporting intelligence capabilities, including expeditionary or reach PED capabilities, through thorough staff planning (based on recommendations from the G-2/S-2).

4-78. When requesting intelligence PED capabilities, the gaining G-2/S-2 and intelligence unit commander are responsible for coordinating and planning intelligence PED activities. However, the allocating echelon is also

responsible for ensuring adequate planning, coordination, and use of PED capabilities. Some intelligence PED capability employment considerations for the gaining G-2/S-2 and intelligence unit commander include—

- **Intelligence architecture.** Employment of intelligence PED capabilities depends on how the collection asset and supporting PED element or unit fits into the intelligence architecture. The employment is also specific to the intelligence discipline or complementary intelligence capability and supported echelon. MI units should capture their functional requirements during planning to ensure they request adequate intelligence PED capabilities.
- **Communications.** All intelligence operations depend on integrating multiple communications systems, networks, and information services. It is important to consider and understand hardware and software requirements and compatibility, interoperability issues, bandwidth priority and capacity, and maintenance requirements.
- **Reporting.** Operating effectively within the intelligence architecture requires system operators to understand PED and reporting procedures, requirements, and timelines for operations and intelligence channels as well as for technical channels.
- **Targeting criteria.** Supporting lethal and nonlethal effects require system operators to be thoroughly knowledgeable with the different targeting criteria, including minimum accuracy and timeliness standards for each specific high-payoff target.
- **Technical channels.** System operators must understand how technical channels operate and how to use technical guidance to enhance collection. Additionally, intelligence PED capabilities assist in refining technical guidance.
- **Training.** Intelligence leaders inform the commander and staff on intelligence PED capabilities and limitations. Facilitating the integration of intelligence PED capabilities requires intelligence leaders to conduct training with the intelligence unit and intelligence PED system operators, analysts, and maintainers.
- **Sustainment.** Intelligence PED capabilities and resources can provide a significant maintenance and logistic challenge to the intelligence unit. Reducing these challenges requires the intelligence unit to conduct thorough planning and coordination.

This page intentionally left blank.

Chapter 5

Fighting for Intelligence

Since Army forces compete with an adaptive enemy; perfect planning and information collection seldom occurs. Intelligence is not perfect, information collection is not easy, and a single collection capability is not persistent and accurate enough to provide all of the answers. During large-scale combat operations, Army forces will have to fight for intelligence. To achieve situational understanding against peer threats, friendly forces must strive to identify or open windows of opportunity across domains. Staff integration is difficult but crucial; the staff must collaborate to overcome challenges and mitigate information collection capability and system limitations by developing an integrated information collection plan. Fighting for intelligence also encompasses the basics of establishing an effective intelligence architecture, synchronizing the intelligence warfighting function, and planning and conducting information collection.

THE CHALLENGE

5-1. Producing intelligence and executing information collection differ significantly based on the Army's strategic role. For example, intelligence operations conducted during shaping operations differ drastically from intelligence operations conducted during large-scale combat operations.

5-2. Of the four Army strategic roles (shape, prevent, conduct large-scale ground combat, and consolidate gains), the intelligence warfighting function is most challenged to meet the vast number of large-scale combat operation requirements. Large-scale combat operations are intense, lethal, and brutal—creating conditions, such as complexity, chaos, fear, violence, fatigue, and uncertainty. Battlefields will include noncombatants crowded in and around dense urban areas. To further complicate operations, enemies will employ conventional and unconventional tactics, terrorism, criminal activities, and information warfare. Activities in the information environment, which includes cyberspace, will often be inseparable from land operations. The fluid and chaotic nature of large-scale combat operations will cause the greatest degree of fog, friction, and stress on the intelligence warfighting function.

5-3. When fighting a peer threat during large-scale combat operations, units must be prepared to fight for intelligence against enemy formations, a range of sophisticated threat capabilities, and many unknown conditions within the operational environment. The challenges to information collection include integrated air defense systems, long-range fires, counterreconnaissance, cyberspace and EW operations, and camouflage, concealment, and deception.

5-4. A successful information collection effort is key to achieving and exploiting positions of relative advantage. The intelligence staff can then analyze collected information and provide products, updates, and predictive assessments that support targeting, decision making, and the execution of branches and/or sequels. Staff integration, operational planning, and information collection plans are not foolproof and can become ineffective. Conceptually, fighting for intelligence is not new, but the Army must emphasize this principle due to the complexity of large-scale operations. Conducting information collection requires thorough and creative planning, aggressive execution, and adjustments based on the situation. Key aspects of fighting for intelligence to support operations include the following:

- Commanders drive intelligence.
- Effective staff integration is crucial.
- Effective intelligence requires a comprehensive intelligence architecture.
- A thoroughly developed and flexible information collection plan is critical.

- A successful information collection plan begins with identifying the right requirements.
- Together, commanders, staffs, and subordinate units strive and constantly adjust to develop and execute a layered and aggressive information collection plan.

THE COMMANDER'S ROLE AND STAFF INTEGRATION

5-5. Commanders and staffs need timely, accurate, relevant, and predictive intelligence to understand threat characteristics, goals and objectives, and COAs. Precise intelligence is critical to targeting threat capabilities at the right time and place to open windows of opportunity across domains. Commanders and staffs must have detailed knowledge of the threat's strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute friendly operations.

5-6. Collaboration within and between the entire staff produces integration essential to effective mission command and synchronized operations. While all staff sections have clearly defined functional responsibilities, they cannot work efficiently without complete cooperation and coordination among all sections and cells. Key staff synchronization and integration occur during—

- IPB.
- Army design methodology, the military decision-making process (MDMP), and the rapid decision-making and synchronization process.
- Information collection.
- Targeting.
- Assessments.

5-7. The G-2/S-2 supports the commander's ability to understand the operational environment and visualize operations by leading the IPB process and portraying the enemy throughout the MDMP, developing the information collection plan, updating the intelligence running estimate, and developing intelligence products and reports. The commander's role is to direct the intelligence warfighting function through this relationship with the G-2/S-2. Commanders must stay constantly engaged with their G-2 or S-2; close interaction between them is essential as the intelligence staff supports unit planning and preparation through the integrating processes and continuing activities.

5-8. Commanders and staffs use the integrating processes (IPB, targeting, and risk management) to synchronize specific functions throughout the operations process. They always plan for and coordinate the continuing activities: liaison, information collection, security operations, protection, terrain management, and airspace control. The intelligence staff supports the integrating processes and continuing activities (information collection) by providing all-source analysis of threats, terrain and weather, and civil considerations. (See ADRP 5-0 for more on the integrating processes and continuing activities.)

INTELLIGENCE AND THE INTEGRATING PROCESSES

5-9. There is an ever-growing volume of data and information from numerous sources about the operational environment that can improve the commander's visualization of the battlefield in time and space. Situational understanding enables the commander to better—

- Make decisions.
- Prioritize and allocate resources.
- Assess and take necessary risks.
- Understand the needs of higher and subordinate commanders.

5-10. The commander and staff depend on a skilled intelligence staff to answer PIRs and other requirements through the synchronization of the intelligence warfighting function with mission command. The intelligence staff conducts all-source analysis that facilitates the production of IPB products; supports the information collection effort, the targeting effort, and risk management; and provides all-source intelligence analysis (including conclusions and projections of future conditions or events).

Perform Intelligence Preparation of the Battlefield

5-11. The G-2/S-2 leads the staff through the IPB process. The IPB process considers all threat capabilities within and across each domain within the unit's AO and area of interest and the relevant aspects of the information environment. The other staff sections assist the intelligence staff in developing the IPB products required for planning. The IPB process consists of the following four steps: define the operational environment, describe environmental effects on operations, evaluate the threat, and determine threat COAs. IPB starts immediately upon receipt of the mission, is refined throughout planning, and is updated to support subsequent operational planning. (See ATP 2-01.3 for more on IPB.) The following aspects of IPB support mission analysis:

- Evaluate military aspects of the terrain, weather effects, and civil considerations.
- Identify threat capabilities.
- Develop threat models.
- Develop high-value target lists.
- Develop an event template and matrix.

Provide Intelligence Support to Targeting

5-12. The intelligence staff is essential to targeting (both lethal and nonlethal actions). Intelligence supports the planning (target development), preparation, execution, and assessment of direct and indirect fires and EW. The intelligence staff also ensures the information collection plan supports the finalized targeting plan (target detection). Table 5-1 lists the most important subtasks, products, and considerations associated with intelligence support to targeting. (For more on targeting, see ATP 3-60; for more on intelligence support to targeting, see ADRP 1-03 and ATP 2-01.3.)

Table 5-1. Intelligence support to targeting

Receive guidance on—	• Commander's intent • High-payoff targets • Attack criteria • Rules of engagement	• Lead time between decision points and target areas of interest • Combat assessment requirements
Develop—	• Modified combined obstacle overlay • Situation and event templates	• High-value targets • Information collection plan
Explain—	Threat courses of action, as part of war gaming, based on friendly courses of action: • Refine the event template • Assist in developing the high-payoff target list, target selection standard matrix, and attack guidance matrix	
Produce—	Collection management tools	
Collect—	Information for target nomination, validation, and combat assessment	
Disseminate—	• High-payoff target-related information and intelligence to the fires cell or appropriate location immediately • Pertinent information and battle damage assessment in accordance with standard operating procedures or other instructions	

Provide Intelligence Support to Risk Management

5-13. Risk management is the Army's primary process for identifying and controlling risks during operations. *Risk management* is the process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits (JP 3-0). The chief of protection (or S-3 in units without a protection cell), in coordination with the safety officer, integrates risk management into the MDMP. The intelligence staff participates in the overall risk management process and integrates risk management into collection management when recommending tasks for information collection assets.

5-14. Commanders must focus and use intelligence to explicitly understand the lethality of large-scale combat operations and to preserve their combat power and take the appropriate operational risk to achieve the end state. Using intelligence to see and understand within each domain can reduce risk to the friendly force and enhance success in chaotic and high-tempo operations. The distribution of specific intelligence

collection systems, personnel, and equipment enhances the capability of the combined arms team to concentrate combat power and reduce risk. Intelligence provides the commander the ability to detect adversary capabilities and activities, analyze enemy intentions, and track enemy capabilities across all domains to inform decisions and provide realistic assessments of operational and tactical risk. During situation development, analysts determine the significance of collected information and its significance relative to predicted threat COAs. Through predictive analysis, the staff templates threat activity or trends that present opportunities or risks to the friendly force. This support assists the commander and staff in deciding when and where to concentrate sufficient combat power to defeat the threat while mitigating risk.

INTELLIGENCE AND THE CONTINUING ACTIVITIES: INFORMATION COLLECTION

5-15. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55). Information collection is an integrated intelligence and operations function. The intelligence staff conducts information collection in collaboration with the operations staff to collect, process, and analyze information the commander requires concerning threats, terrain and weather, and civil considerations that affect operations. The primary Army information collection missions/means are reconnaissance, surveillance, security operations, and intelligence operations.

5-16. A successful information collection effort results in the timely collection and reporting of relevant and accurate information, which either supports the production of intelligence or is disseminated as combat information. The information collection effort includes organic units and capabilities and support from DOD intelligence assets, as well as nonintelligence sources, which provide civil considerations and sociocultural information. (See FM 3-55 and ATP 3-55.4.) The information collection tasks are collection management, direct information collection, execute collection, and conduct intelligence-related missions and operations.

Collection Management

5-17. Collection management is the task of analyzing requirements, evaluating available assets (internal and external), recommending taskings to the operations staff for information collection assets, submitting requests for information for adjacent and higher collection support, and assessing the effectiveness of the information collection plan. The continuous functions of collection management identify the best way to satisfy the requirements of the supported commander and staff. These functions are not necessarily sequential. Collection management inherently requires an understanding of the relative priority of incoming requests for collection and PED. Additionally, collection management includes the staff vetting requirements against current intelligence holdings to ensure resources are not wasted collecting information that is already available. (See ATP 2-01.)

Direct Information Collection

5-18. The operations staff (based on recommendations from the rest of the staff) tasks, directs, and when necessary, retasks information collection assets. By tasking and directing information collection assets, the staff ensures the most effective and balanced use of assets across the subordinate units in order to answer all requirements. The operations staff tasks units and information collection assets by issuing warning orders, fragmentary orders, and operation orders. Additionally, they continuously monitor the information collection effort and retask assets as requirements are refined, updated, and added. (See FM 3-55.)

Execute Collection

5-19. Executing collection focuses on specific requirements. This collection is accomplished through the execution of tactical missions (such as the primary means of information collection: reconnaissance, surveillance, security operations, and intelligence operations) based on CCIRs and other requirements. Collection activities acquire data and information about threats and relevant aspects of the AO. They provide that information to intelligence PED and analysis elements. Typically, collection activities begin soon after receipt of the mission and continue throughout preparation and execution of operations. They do not cease after the operation concludes but continue as required. This allows the commander to focus combat power, execute current operations, and prepare for future operations simultaneously.

PLANNING CONSIDERATIONS AND INFORMATION REQUIREMENTS

5-20. By supporting the integrating processes, the intelligence warfighting function supports the commander's decisions, situational understanding, MDMP, targeting, and force protection considerations. During all operations, both friendly and enemy forces will endeavor to set conditions to develop a position of relative advantage.

5-21. Through generating intelligence knowledge, IPB, and situation development, the intelligence staff enables commanders and staffs to develop a realistic and sufficiently flexible plan to account for enemy objectives, COAs, and capabilities. The intelligence staff also provides warning intelligence, which indicates the start of hostilities, a major change or escalation to the nature of the conflict, or the introduction of a significant new capability.

PLANNING CONSIDERATIONS FOR THE INTELLIGENCE WARFIGHTING FUNCTION

5-22. The intelligence warfighting function is designed to systematically answer intelligence requirements. Commanders focus the effort by clearly articulating intent, stating requirements, prioritizing targets, and assessing effectiveness as operations progress. However, in order to drive intelligence, commanders and staffs must have realistic expectations about intelligence capabilities and available assets. The following are intelligence warfighting function planning considerations:

- **Intelligence reduces uncertainty; it does not eliminate it.** The commander has to determine the presence and degree of risk involved in conducting a particular operation. The time available to plan and prepare is directly related to the risk. Usually, the more time allotted to planning and preparation, the lower the risk. One of the commander's considerations is determining the appropriate balance between the time allotted for collection weighed against the operational necessity for quickly executing an operation. It takes time to collect information and develop it into detailed and precise intelligence products.
- **The intelligence warfighting function comprises finite resources and capabilities.** Intelligence systems and Soldiers trained in specific skills are limited. Once lost to action or accident, these systems and Soldiers are not easily replaceable; in some cases, it may not be possible to replace them during the course of the current operation. The loss of Soldiers and equipment can result in the inability to detect or analyze threat actions. Additionally, the loss of qualified language-trained Soldiers, especially those trained in low-density languages or skills, could adversely affect intelligence operations.
- **To provide effective intelligence, the intelligence warfighting function must have adequate communications and network-enabled capabilities.** Commanders and staffs must ensure the allocation of communications support and resources to intelligence is appropriate.

INFORMATION REQUIREMENTS

5-23. Information requirements differ significantly based on the defensive or offensive task, the specific situation, and unique requirements for concurrent supporting operations such as deep operations and missions in the various consolidation areas. During both friendly defensive and offensive tasks, there are consolidation area requirements to detect enemy bypassed or stay-behind forces, special purpose forces, irregular forces, terrorists, and efforts to create an insurgency or conduct information warfare. (See FM 3-0 and FM 2-0 for more detailed discussions on the defensive and offensive tasks and the specific intelligence support to each form of the defense and offense.)

Defensive Tasks

5-24. During friendly defensive tasks, enemy forces employ precision fires, other long-range fires, and nonlethal capabilities (such as cyber and EW) to attack friendly mission command and key supporting and sustaining capabilities. Friendly forces aim to prepare defensive positions and set conditions while the enemy attempts to set the timing of, location of, and conditions for battle. The three basic friendly defensive tasks are area defense, mobile defense, and retrograde.

5-25. Intelligence supports friendly force efforts to protect the force, disburse and reassemble the force as necessary, and answer requirements on when, where, and in what strength the enemy will attack. This intelligence supports decisions on setting the defense, employing various capabilities, repositioning forces, conducting counterattacks, and when possible, transitioning to offensive tasks.

5-26. The intelligence staff leads the rest of the staff in identifying when, where, with what strength, and how the enemy will attack. This allows the commander to identify opportune times to conduct spoiling attacks and reposition forces. The entire staff also identifies threats to support and consolidation areas, such as enemy special purpose forces and irregular activities, which may interfere with control of the defense. The intelligence staff leads the rest of the staff in determining—

- The threat intent, objectives, and associated decision points tied to the decisive and/or key terrain associated with the operation.
- General trafficability and mobility considerations, ground mobility corridors, avenues of approach, intervisibility lines within key areas, specific terrain analysis, and weather effects on the operation.
- The likely composition, focus, routes, and a time window for arrival of enemy reconnaissance formations.
- The likely scheme of maneuver for the attacking enemy force.
- Intent, activities, orientation, and predicted locations for: enemy command and control and communications command posts; enemy artillery formations and air defense systems; enemy aviation units; threat EW capabilities; enemy engineer support, chemical support, and special operations forces; and enemy activities in friendly consolidation areas.
- The likely use and intent for threat cyberspace capabilities and likely enemy use of deception.
- The likely location of and time window to commit enemy reserve forces, likely use of second echelon enemy forces to isolate or encircle friendly forces, and likely times and locations where the friendly commander can launch a spoiling attack.

Offensive Tasks

5-27. During friendly offensive tasks, enemy forces attempt to disrupt friendly activities by employing precision fires, other long-range fires, and nonlethal capabilities (like cyber and EW). Therefore, friendly forces strive to conduct the necessary movements, prepare logistical support, and set other conditions while the enemy attempts to prevent friendly forces from effectively synchronizing adequate combat power. The four basic friendly offensive tasks movement to contact, attack, exploitation, and pursuit.

5-28. Intelligence determines when and where the enemy will concentrate combat power, find gaps and vulnerabilities in enemy defenses, and predict how the enemy will conduct any counterattacks. This intelligence supports decisions on conducting information collection, executing long-range fires, penetrating enemy security areas, overcoming obstacles, avoiding enemy strengths, defeating enemy counterattacks, and when possible, transitioning to exploitation or pursuit.

5-29. The intelligence staff leads the rest of the staff in a careful analysis of the terrain, including ground and air avenues of approach, and other significant factors of the operational environment. Then the staff identifies a broad range of enemy COAs with emphasis on the enemy's most likely and most dangerous COAs in the war-gaming portion of the MDMP. Because of the inherent vulnerability of friendly forces during a movement to contact, the intelligence staff must not underestimate the enemy and complexities of the mission. Predictions of enemy COAs should be thorough; at a minimum, they should account for enemy maneuver units (two echelons below) and all key enemy capabilities and enablers. A thorough IPB and war-gaming effort indicates areas where contact with the enemy is likely, as well as friendly and enemy vulnerabilities by phase of the operation. The intelligence staff leads the rest of the staff in determining—

- The threat intent, objectives, and associated decision points tied to decisive and/or key terrain associated with the operation.
- General trafficability and mobility considerations, ground mobility corridors, avenues of approach, intervisibility lines within key areas, specific terrain analysis, and weather effects on the operation.

- The intent, activities, orientation, and predicted locations for: obstacles, including areas the enemy is likely to use fire support coordination measures; enemy reconnaissance, security forces, and observation posts; enemy aviation units, including forward arming and refueling points; enemy defensive locations with likely close obstacles and engagement areas within the main defensive zone; enemy command and control and communications facilities and systems; enemy artillery, rocket units, and air defense systems; enemy engineer support, chemical support, and special operations forces; threat EW capabilities; enemy reserve forces, including when they would be committed; and enemy activities in friendly consolidation areas.
- The likely use and intent for threat cyberspace capabilities and likely enemy use of deception.
- Indications that the enemy is still conducting movement, possibly turning the operation into a meeting engagement or causing friendly forces to employ a hasty defense.

OTHER KEY TASKS FOR SHAPING LARGE-SCALE COMBAT OPERATIONS

5-30. There are many important aspects of all offensive and defensive tasks, including the tactical enabling tasks. In combat, seizing the initiative involves conducting reconnaissance, maintaining security, performing defensive and offensive tasks at the earliest possible time, forcing the enemy to culminate offensively, and setting the conditions for decisive operations. Operations in the deep area involve efforts to prevent uncommitted or out-of-contact enemy maneuver forces from being committed coherently or preventing enemy enabling capabilities, such as fires and air defense, from creating effects in the close area. The purpose of operations in the deep area is to set conditions for success in the close area or to set conditions for future operations. Therefore, units must execute successful reconnaissance, security operations, and deep operations before or as part of all offensive and defensive tasks:

- **Reconnaissance.** Reconnaissance is typically conducted to gain more information about a terrain feature, geographic area, enemy force, or other operational or mission variable that is important for a commander to formulate, confirm, or modify a COA. Commanders normally assign reconnaissance objectives, which can be information about a specific geographic location, a specific enemy activity to be confirmed or denied, or a specific enemy unit to be located and tracked. Therefore, every reconnaissance is different and there is no general list of information requirements. (See FM 3-0.)
- **Security operations.** The main difference between performing security tasks and reconnaissance tasks is that security tasks orient on the force or facility being protected, while reconnaissance tasks are enemy- and terrain-oriented. The goal of security tasks is protecting a force from surprise and reducing the unknowns in any situation. Commanders may perform security tasks to the front, flanks, or rear of a friendly force. Security tasks are shaping operations. As a shaping operation, economy of force is often a consideration when planning. Intelligence support for security operations simply follows the intelligence considerations for the offensive or defensive task the main unit is conducting. Security operations encompass five tasks: screen, guard, cover, area security, and local security. (See FM 3-0.)
- **Deep operations.** Deep operations are combined arms operations directed against uncommitted enemy forces or capabilities before they can engage friendly forces in the close fight. Deep operations also contribute to setting the conditions to transition to the next phase of an operation (for example, from a defensive to an offensive task). Deep operations are not simply attacking an enemy force in depth. Instead, they are the sum of all activities that influence when, where, and in what condition enemy forces will be committed. Deep operations are normally planned and controlled at theater army, corps, and division levels, and typically include information collection, target acquisition, ground and air maneuver, fires, cyberspace electromagnetic activities, and information operations either singly or in combination. Intelligence support to deep operations is an inherent part of intelligence support to targeting. The intelligence staff leads the rest of the staff in identifying when, where, in what strength, and how the enemy will begin movement, launch attacks, or defend. (See ATP 3-94.2.)

THE INFORMATION COLLECTION PLAN AND THE INTELLIGENCE ARCHITECTURE

5-31. After completing the MDMP (to include developing requirements), the commander and staff complete an information collection plan. Developing the information collection plan involves overlaying the information requirements on the current situation, operational plan, and the existing intelligence architecture.

DEVELOPING THE INFORMATION COLLECTION PLAN

5-32. Commanders and staffs use the principles of information collection, IPB and other key staff products, and knowledge of information collection capabilities and limitations to develop the information collection plan. As commanders and staffs develop the plan, they may encounter information collection gaps due to factors that include but are not limited to inadequate collection range, unfavorable terrain, or lack of technical capabilities.

5-33. PIRs and the most important intelligence requirements and targeting requirements form the basis of an integrated information collection plan. Through analysis, the staff determines the best way to satisfy each requirement. Based on the MDMP, including a thorough war game, the commander and staff develop a detailed and realistic information collection plan to answer as many requirements as possible.

5-34. Staff integration and synchronization ensures the enemy situation and the operational environment (not just a predetermined operational plan) drive the information collection effort. Generally, intelligence units and collectors are allocated based on priorities and the unit's main effort. Additionally, a unit may have to depend on the higher echelon to provide intelligence support during a particular operational phase because the unit is constantly moving or has a high operating tempo and cannot produce its own intelligence.

5-35. The information collection plan must be simple enough to execute, should avoid being predictable to enemy forces, and should include adequate operations security measures to protect friendly operations. Effective information collection planning depends on collaboration across the echelons in order to vertically and horizontally layer the information collection effort. A layered and continuous information collection effort provides better opportunities for detecting enemy formations, fires capabilities, and critical specialized capabilities that pose the greatest threat to friendly forces. (See FM 3-55 and ATP 2-01 for more on developing an information collection plan.)

ESTABLISHING THE INTELLIGENCE ARCHITECTURE

5-36. When the commander and staff start planning, many aspects of and limitations to information collection have already been set based on the specifics of the intelligence architecture and mission command network. While units can change a few components of the intelligence architecture within a short timeframe, most components are already set or require a fairly long lead time to change. Therefore, setting the intelligence architecture is an important aspect of the shape and deter roles.

5-37. The intelligence architecture is developed well before deployment based on future planning and assumptions on the employment of intelligence capabilities. Periodically, units will revise the intelligence architecture based on new planning factors and assumptions, as well as the addition of new capabilities. Before deployment, units task-organize information collection capabilities based on the intelligence architecture and other factors such as the command post structure and other key mission command nodes. Following initial deployment, the intelligence architecture will already be largely established and each unit will develop an information collection plan within the context of the architecture.

5-38. The command and staff must understand the relationship of national to tactical intelligence; theater-specific procedures, networks, and systems; the strengths and vulnerabilities of organic and supporting intelligence units, personnel, and systems; and the overarching operation plan in order to establish the intelligence architecture.

DEVELOPING THE SITUATION AND CONTINUOUS INFORMATION COLLECTION

5-39. The fight for intelligence becomes more difficult as units receive long-range fires and make contact with enemy forces. Information collection and intelligence analysis are integral to developing the situation. Additionally, the corps and division intelligence staffs may attend or watch theater-level collection management boards, giving them insight into national and joint priorities and coverage. This insight, coordination, and preparation create opportunities for tactical units to leverage national and joint capabilities. The theater army, corps, and division G-2s convene an operations and intelligence working group, or some form of synchronization meeting, with key staff and subordinate units. These intelligence synchronization meetings (normally conducted via video teleconferencing) create a common understanding of the enemy, ensure information collection plans address changes in the situation, and coordinate continuous information collection across echelons and units.

5-40. The intelligence staff conducts synchronizing activities to assist the unit in developing the situation and adjusting information collection. Information collection requires airspace, terrain, and space deconfliction and coordination as well as adequate PED capabilities to ensure assets are able to operate efficiently and effectively. The staff considers whether the unit has the intelligence collection and PED capabilities, capacity, and architecture required to support planned and projected operations. There are many requirements for the G-2/S-2 and the intelligence staff to participate in unit battle rhythm activities to synchronize intelligence support and the information collection effort. The intelligence staff provides updates on the situation and briefs changes to the information collection plan during various commander updates, boards, cell meetings, and other meetings. This creates a common understanding of the enemy, ensures information collection plans address changes in the situation, and coordinates continuous information collection across echelons and units.

5-41. Information collection is continuous through the execution of operations and transition to consolidate gains. The all-source analytical effort is key to informing the commander and staff, who in turn support the continued fight for intelligence. Therefore, G-2/S-2s, all-source analysts, and collection managers must collaborate closely. Intelligence analysis assists in discovering collection gaps, generating more information requirements, and driving all operations. Additionally, analysis assists in determining the effectiveness of the information collection effort. That assessment leads to adjustments in the information collection plan, making it more efficient and effective. Thorough planning allows continuous collection planning through all phases, branches, and sequels of an operation.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. The glossary lists terms for which ADP 2-0 is the proponent with an asterisk (*) before the term. For other terms, it lists the proponent publication in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AO	area of operations
AR	Army regulation
ASCC	Army Service component command
ASCOPE	areas, structures, capabilities, organizations, people, and events (civil considerations)
ATP	Army techniques publication
AUTL	Army Universal Task List
BCT	brigade combat team
BEWL	biometric-enabled watchlist
CBRN	chemical, biological, radiological, and nuclear
CCIR	commander's critical information requirement
CI	counterintelligence
CJCSI	Chairman of the Joint Chiefs of Staff instruction
COA	course of action
DOD	Department of Defense
DODD	Department of Defensive directive
DODI	Department of Defense instruction
DODM	Department of Defensive manual
DOMEX	document and media exploitation
DSCA	defense support of civil authorities
ELINT	electronic intelligence
E-MIB	expeditionary-military intelligence brigade
EMS	electromagnetic spectrum
EO	executive order
EW	electronic warfare
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal

GCC	geographic combatant command
GEOINT	geospatial intelligence
HUMINT	human intelligence
INSCOM	United States Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
JP	joint publication
MASINT	measurement and signature intelligence
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (mission variables)
MI	military intelligence
MIB-T	military intelligence brigade-theater
NGIC	National Ground Intelligence Center
OSINT	open-source intelligence
PED	processing, exploitation, and dissemination
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-6	battalion or brigade signal staff officer
S&TI	scientific and technical intelligence
SIGINT	signals intelligence
TECHINT	technical intelligence
U.S.	United States
USC	United States Code
WTI	weapons technical intelligence

SECTION II – TERMS

***all-source intelligence**

(Army) The integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations.

(joint) Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. (JP 2-0)

adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

biometrics

(joint) The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 2-0)

biometrics-enabled intelligence

(Army) Intelligence resulting from the combination of biometric information with other intelligence, threat information, or information relating to other aspects of the operational environment in order to answer intelligence requirements. (ATP 2-22.82)

collection

In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 2-01)

combat information

Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (JP 2-01)

combined arms

The synchronized and simultaneous application of all elements of combat power that together achieve an effect greater than if each arm was used separately or sequentially. (ADRP 3-0)

communications intelligence

Technical information and intelligence derived from foreign communications by other than the intended recipients. (JP 2-0)

decisive action

The continuous, simultaneous combinations of offensive, defensive, and stability or defense support of civil authorities tasks. (ADRP 3-0)

defense support of civil authorities

Support provided by United States Federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. (DODD 3025.18)

defensive task

A task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks. (ADRP 3-0)

document and media exploitation

The processing, translation, analysis, and dissemination of collected hardcopy documents and electronic media that are under the U.S. Government’s physical control and are not publicly available. (ATP 2-91.8)

electronic intelligence

Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 3-13.1)

foreign instrumentation signals intelligence

A subcategory of signals intelligence consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-United States aerospace, surface, and subsurface systems. (JP 2-01)

foreign intelligence entity

Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire United States information, block or impair United States intelligence collection, influence United States policy, or disrupt United States systems and programs. The term includes foreign intelligence and security services and international terrorists. (JP 2-01.2)

forensic-enabled intelligence

The intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest. (JP 2-0)

***fusion**

(Army) Consolidating, combining, and correlating information together.

geospatial information

Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products. (JP 2-03).

geospatial intelligence

The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (JP 2-03)

hazard

A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. (JP 3-33)

***human intelligence**

(Army) The collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities.

imagery

A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likenesses and presentations produced by satellites, aircraft platforms, unmanned aircraft systems, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (JP 2-03)

imagery intelligence

The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. (JP 2-03)

information collection

An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations. (FM 3-55)

intelligence

(1) The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. (2) The activities that result in the product. (3) The organizations engaged in such activities. (JP 2-0)

***intelligence analysis**

The process by which collected information is evaluated and integrated with existing information to facilitate intelligence production.

intelligence community

All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. (JP 2 0)

***intelligence operations**

(Army) The tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements.

***intelligence reach**

The activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command.

intelligence, surveillance, and reconnaissance

An integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. (JP 2-01)

***intelligence synchronization**

The art of integrating information collection; intelligence processing, exploitation, and dissemination; and intelligence analysis with operations to effectively and efficiently fight for intelligence in support of decision making.

intelligence warfighting function

The related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment. (ADRP 3-0)

joint operations

Military actions conducted by joint forces and those Service forces employed in specific command relationships with each other, which of themselves, do not establish joint forces. (JP 3-0)

measurement and signature intelligence

Information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event. (JP 2-0)

offensive task

A task conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers. (ADRP 3-0)

open-source information

(joint) Information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access. (JP 2-0)

open-source intelligence

(DOD) Intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (Public Law 109-163)

operation

A sequence of tactical actions with a common purpose of unifying theme. (JP 1)

operational environment

A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

***processing, exploitation, and dissemination**

The execution of the related functions that converts and refines collected data into usable information, distributes the information for further analysis, and, when appropriate, provides combat information to commanders and staffs.

publicly available information

(DOD) Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public. (DODM 5240.01)

regionally aligned forces

Those forces that provide a combatant commander at up to joint task force capable headquarters with scalable, tailorable capabilities to enable the combatant commander to shape the environment. They are those Army units assigned to combatant commands, those Army units allocated to a combatant command, and those Army capabilities distributed and prepared by the Army for combatant command regional missions. (FM 3-22)

risk management

The process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits. (JP 3-0)

signals intelligence

Intelligence derived from communications, electronic, and foreign instrumentation signals. (JP 2-0)

stability tasks

Tasks conducted as part of operations outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (ADRP 3-07)

technical intelligence

Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. (JP 2-0)

threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADRP 3-0)

unified action

The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1)

unified action partners

Those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations. (ADRP 3-0)

unified land operations

Simultaneous offensive, defensive, and stability or defense support of civil authorities tasks to seize, retain, and exploit the initiative to shape the operational environment, prevent conflict, consolidate gains, and win our Nation's wars as part of unified action. (ADRP 3-0)

weapons technical intelligence

A subcategory of technical intelligence derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other systems. (JP 3-15.1)

References

All URLs accessed on 29 August 2018.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. August 2018.

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

ADRP 3-0. *Operations*. 6 October 2017.

ADRP 5-0. *The Operations Process*. 17 May 2012.

ADRP 6-0. *Mission Command.* 17 May 2012.

FM 2-0. *Intelligence Operations*. 6 July 2018.

FM 3-0. *Operations*. 6 October 2017.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: http://www.jcs.mil/doctrine/.

Most DOD publications are available at the DOD Issuances website: http://www.dtic.mil/whs/directives.

CJCSI 3121.01B. *(U) Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces* (S). 18 June 2008.

DOD Law of War Manual. December 2016. Available online: https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

DOD 5240.1-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons.* 7 December 1982.

DODD 2310.01E. *DOD Detainee Program*. 19 August 2014.

DODD 3025.18. *Defense Support of Civil Authorities (DSCA)*. 29 December 2010.

DODD 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*. 11 October 2012.

DODI 5240.26. *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat.* 4 May 2012.

DODM 5240.01. *Procedures Governing the Conduct of DOD Intelligence Activities.* 8 August 2016.

JP 1. *Doctrine for the Armed Forces of the United States*. 25 March 2013.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 5 July 2017.

JP 2-01.2. *(U) Counterintelligence and Human Intelligence in Joint Operations* (S). 6 April 2016. This publication is classified. Access information is available online: https://jdeis.js.mil/jdeis/index.jsp?pindex=2.

JP 2-03. *Geospatial Intelligence in Joint Operations*. 5 July 2017.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-13.1. *Electronic Warfare*. 8 February 2012.
JP 3-15.1. *Counter-Improvised Explosive Device Operations*. 17 July 2018.
JP 3-28. *Defense Support of Civil Authorities*. 31 July 2013.
JP 3-33. *Joint Task Force Headquarters*. 31 January 2018.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil/.
ADP 3-07. *Stability*. 31 August 2012.
ADP 3-90. *Offense and Defense*. 13 August 2018.
ADRP 1-03. *The Army Universal Task List*. 2 October 2015.
ADRP 3-07. *Stability*. 31 August 2012.
ADRP 3-28. *Defense Support of Civil Authorities*. 14 June 2013.
AR 115-11. *Geospatial Information and Services*. 28 August 2014.
AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.
AR 381-20. *(U) Army Counterintelligence Program* (S). 25 May 2010.
AR 381-100. *(U) Army Human Intelligence Collection Programs* (S). 22 February 2016.
AR 530-1. *Operations Security.* 26 September 2014.
ATP 2-01. *Plan Requirements and Assess Collection.* 19 August 2014.
ATP 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace.* 10 November 2014.
ATP 2-22.2-1. *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities (U)*. 11 December 2015.
ATP 2-22.4. *Technical Intelligence*. 4 November 2013.
ATP 2-22.7. *Geospatial Intelligence*. 26 March 2015.
ATP 2-22.8. *(U) Measurement and Signature Intelligence* (S//NF). 30 May 2014.
ATP 2-22.9. *Open-Source Intelligence (U)*. 30 June 2017.
ATP 2-22.31. *(U) Human Intelligence Military Source Operations Techniques* (S//NF). 17 April 2015.
ATP 2-22.82. *Biometrics-Enabled Intelligence (U)*. 2 November 2015.
ATP 2-33.4. *Intelligence Analysis*. 18 August 2014.
ATP 2-91.7. *Intelligence Support to Defense Support of Civil Authorities*. 29 June 2015.
ATP 2-91.8. *Techniques for Document and Media Exploitation*. 5 May 2015.
ATP 3-34.80. *Geospatial Engineering*. 22 February 2017.
ATP 3-55.4. *Techniques for Information Collection During Operations Among Populations*. 5 April 2016.
ATP 3-60. *Targeting*. 7 May 2015.
ATP 3-94.2. *Deep Operations*. 1 September 2016.
FM 2-22.3. *Human Intelligence Collector Operations*. 6 September 2006.
FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.
FM 3-22. *Army Support to Security Cooperation.* 22 January 2013.
FM 3-55. *Information Collection*. 3 May 2013.
FM 6-02.71. *Network Operations*. 14 July 2009.
FM 27-10. *The Law of Land and Warfare*. 18 July 1956.
U.S. Army Directive 2016-37. *U.S. Army Open-Source Intelligence Activities*. 22 November 2016.

OTHER PUBLICATIONS

EO 12333. *United States Intelligence Activities*. 4 December 1981. Amended by EO 13284 (2003) and 13470 (2008). Available online: http://www.archives.gov/federal-register/executive-orders/disposition.html.

EO 13491. *Ensuring Lawful Interrogations.* 22 January 2009. Available online: http://www.archives.gov/federal-register/executive-orders/disposition.html.

Public Law 109-163. *National Defense Authorization Act for Fiscal Year 2006*. 6 January 2006. Available online: https://www.gpo.gov/fdsys/pkg/PLAW-109publ163/content-detail.html.

Title 10, USC. *Armed Forces*. Available online: http://uscode.house.gov/.

Title 32, USC. *National Guard*. Available online: http://uscode.house.gov/.

Title 50, USC. *War and National Defense*. Available online: http://uscode.house.gov/.

SOURCES USED

Paul, Richard and Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. 2014. Dillon Beach, CA: Foundation for Critical Thinking. 2017. Available online: www.criticalthinking.org.

Elder, Linda and Richard Paul. *The Thinker's Guide to Analytic Thinking*. 2017. Dillon Beach, CA: Foundation for Critical Thinking. 2017. Available online: www.criticalthinking.org.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website: https://armypubs.army.mil/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

This page intentionally left blank.

Index

Entries are by paragraph number unless indicated otherwise.

A

adversary. *See* threat, defined.

all-source intelligence, 4-1
  analysis, 4-2–4-4
  identity activities, 4-7, 4-8
  production, 4-5, 4-6

Army design methodology, 3-13

Army's strategic roles, 1-24, 1-25

Army Universal Task List (AUTL) tasks, 2-9–2-12

B

biometrics-enabled intelligence, 4-60
  biometric analysis, 4-61, 4-62
  biometric reports, 4-63

C

civil considerations, 1-9, 2-7, 2-28, 3-22, 4-3, 5-11

collaboration, 2-30

collection, 3-22. *See also* information collection.

collection management. *See* information collection.

combat information, defined, 3-27

command and support relationships, 2-19, 4-10

commander
  role, 5-5–5-8

commander's critical information requirement. *See* requirements.

commander's guidance, 3-8

communications intelligence, 4-48, 4-49

complementary intelligence capabilities, 4-59
  biometrics-enabled intelligence, 4-60–4-63
  cyber-enabled intelligence, 4-64–4-66
  document and media exploitation, 4-67–4-72
  forensic-enabled intelligence, 4-73–4-75

counterintelligence (CI). *See* intelligence disciplines.

critical thinking, 2-30

cyber-enabled intelligence. *See* complementary intelligence capabilities.

D

decisive action, 1-29–1-31
  defense support of civil authorities, 1-40–1-44
  defensive task, 1-37, 1-37
  offensive task, 1-33–1-35
  stability tasks, 1-38, 1-39

deep operations, 5-30

defense support of civil authorities (DSCA), 1-40–1-44

defensive task, 1-36, 1-37, 5-24–5-26

disseminate, 3-33–3-36 channels, 3-40
  methods and techniques, 3-37–3-39
  presentation techniques and procedures, 3-41, 3-42

document and media exploitation. *See* complementary intelligence capabilities.

domains (air, land, maritime, space, and cyberspace), 1-10

E

echelons, Army, 2-47–2-50

electronic intelligence (ELINT), 4-48, 4-50

enemy. *See* threat, defined.

expeditionary-military intelligence brigade. *See* echelons, Army.

expeditionary PED. *See* PED.

F

fighting for intelligence
  the challenge, 5-1–5-4

foreign instrumentation signals intelligence, 4-48, 4-51

foreign intelligence entity, 4-16–4-19

forensic-enabled intelligence. *See* complementary intelligence capabilities.

fusion, defined, 4-5

G

G-2/S-2, 3-7

generating intelligence knowledge, 1-9, 2-9, 4-2, 5-21

geospatial information, 4-24

geospatial intelligence (GEOINT). *See* intelligence disciplines.

H

hazard, 1-13, 4-75

human intelligence (HUMINT). *See* intelligence disciplines.

I

identity activities. *See* all-source intelligence.

imagery, 4-22

imagery intelligence, 4-23

information collection, 2-9
  collection management, 5-17
  continuous information collection, 5-39–5-41
  defined, 5-15
  direct information collection, 5-18
  execute collection, 5-19
  primary means of, 3-22

information collection plan
  developing, 5-31–5-35

information environment, 1-5, 1-10, 5-11

information operations, 2-9, 4-2

information requirement, 5-20, 5-23. *See also* requirements.

INSCOM, 2-36–2-38

integrating processes, 5-9, 5-10
  IPB, 5-11
  risk management, 5-13, 5-14
  targeting, 5-12

Entries are by paragraph number unless indicated otherwise.

intelligence
  across the echelons, 2-47–2-50
  national and joint, 2-35–2-46
  purpose of, 2-1–2-6
intelligence analysis, 2-14, 2-28–2-30
intelligence architecture, 4-78
  establishing, 2-42–2-46, 5-36–5-38
intelligence community, 2-34, 2-36, 2-37
intelligence core competencies, 2-14, 2-15
  intelligence analysis, 2-28–2-30
  intelligence operations, 2-18–2-22
  intelligence PED, 2-23–2-27
  intelligence synchronization, 2-16, 2-17
intelligence disciplines, 4-14, 4-15
  counterintelligence, 4-16–4-20
  geospatial intelligence, 4-21–4-27
  human intelligence, 4-28–4-35
  measurement and signature intelligence, 4-36–4-42
  open-source intelligence, 4-43–4-47
  signals intelligence, 4-48–4-52
  technical intelligence, 4-53–4-58
intelligence operations, 2-14, 2-18–2-22
  as a primary means for information collection, 3-22
  interrelated categories of, 3-2
intelligence PED, 2-14, 2-23–2-27
  capabilities, 4-76–4-78, 3-28
intelligence preparation of the battlefield. *See* IPB.
intelligence process, 3-4–3-7
  joint intelligence process, 3-2
intelligence process continuing activities, 3-43
  analyze, 3-44–3-46
  assess, 3-47–3-49
intelligence process steps, 3-9, 3-10
  collect and process, 3-20–3-28
  disseminate, 3-33–3-36
  plan and direct, 3-11–3-16
  produce, 3-29–3-32
intelligence products, 3-7
intelligence reach, 3-19
intelligence synchronization, 2-14, 2-16, 2-17
intelligence warfighting function, 2-7, 2-8, 5-20–5-22
intelligence warfighting function tasks, 2-9–2-13
intelligence, surveillance, and reconnaissance, 1-23
IPB, 4-2, 5-21. *See also* integrating processes.

J

joint operations, 1-18–1-23

L

large-scale combat operations, 1-1–1-3, 1-14, 1-21, 2-46, 5-1, 5-2, 5-14, 5-30

M

measurement and signature intelligence (MASINT). *See* intelligence disciplines.
military decision-making process, 3-13
military intelligence brigade-theater. *See* echelons, Army.
mission variables, 1-6, 1-7, 1-9
multi-domain extended battlefield. *See* operational environment.
multi-domain operations, 1-45–1-48

N

national to tactical intelligence, 2-31–2-34
  intelligence architecture, establishing, 2-42–2-46
  intelligence across the echelons, 2-47–2-50
  national and joint intelligence, 2-35–38
  regionally aligned forces, 2-39–2-41
  setting the theater, 2-39–2-41

O

offensive task, 1-33–1-35, 5-27–5-29
open-source information, 4-45
open-source intelligence (OSINT). *See* intelligence disciplines.
operational environment, 1-4, 1-5
  mission variables, 1-6
  multi-domain extended battlefield, 1-10, 1-11
  operational variables, 1-6
  trends, 1-12
operational variables, 1-6,1-9, 2-7
operations process, 3-4

P

PED
  defined, 2-25
  expeditionary PED, 4-77
  reach PED, 3-19, 4-77
peer threat. *See* threat.
priority intelligence requirement. *See* requirements.
processing, exploitation, and dissemination. *See* PED.
publicly available information, 4-45

R

reach PED. *See* PED.
reconnaissance, 5-30
regionally aligned forces. *See* national to tactical intelligence.
requirements, 3-17, 3-18
risk management. *See* integrating processes.

S

scientific and technical intelligence, 4-42
security operations, 5-30
setting the theater. *See* national to tactical intelligence.
signals intelligence (SIGINT). *See* intelligence disciplines.
single-source intelligence, 4-9, 4-10
  complementary intelligence capabilities, 4-59
  intelligence disciplines, 4-14, 4-15
situational understanding, 2-9
situation development, 4-2, 5-21
stability tasks, 1-38, 1-39
staff integration, 5-5–5-8

T

targeting, 2-9, 4-2, 4-78, 5-12
technical channels, 4-11–4-13, 4-78
technical intelligence (TECHINT). *See* intelligence disciplines.
terrain, 1-7, 2-7, 2-28, 3-22, 4-3, 5-11
threat, 1-13-1-17
  defined, 1-13
  peer threat, 1-14, 1-15

Entries are by paragraph number unless indicated otherwise.

U

U.S. Intelligence and Security Command. *See* INSCOM.
unified action partner, 1-18
unified action, 1-18–1-23
unified land operations, 1-26–1-28
  decisive action, 1-29–1-44
  multi-domain operations, 1-45–1-48

W

weapons technical intelligence, 4-56, 4-57
weather, 1-8, 2-7, 2-28, 3-22, 4-3, 5-11

This page intentionally left blank.

ADP 2-0
4 September 2018

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Acting Administrative Assistant
to the Secretary of the Army
1824203

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: To be distributed in accordance with the initial distrubution number (IDN) 111117, requirements for ADP 2-0.

PIN:103029-000

FM 2-0

INTELLIGENCE

MAY 2004

DISTRIBUTION RESTRICTION:
Approved for public release, distribution is unlimited

HEADQUARTERS
DEPARTMENT OF THE ARMY

***FM 2-0**

Field Manual
No. 2-0

Headquarters
Department of the Army
Washington, DC, 17 May 2004

Intelligence

Contents

Page

PREFACE v

PART ONE **INTELLIGENCE IN THE OPERATIONAL ENVIRONMENT**

Chapter 1 **INTELLIGENCE AND THE OPERATIONAL ENVIRONMENT** 1-1
Role of Intelligence 1-1
The Intelligence Battlefield Operating System 1-2
Intelligence Tasks (METL) 1-3
The Operational Environment 1-19
Dimensions of the Operational Environment 1-20
Critical Variables of the Contemporary Operational Environment 1-23
The Intelligence Process 1-27
Intelligence Disciplines 1-30
Force Projection Operations 1-31

Chapter 2 **INTELLIGENCE AND UNIFIED ACTION** 2-1
Unified Action 2-1
The Levels of War 2-1
Categories of Intelligence 2-5
Intelligence Community 2-7
Unified Action Intelligence Operations 2-12
Intelligence Reach 2-19

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes FM 34-1, 27 September 1994.

PART TWO INTELLIGENCE IN FULL SPECTRUM OPERATIONS

Chapter 3 FUNDAMENTALS IN FULL SPECTRUM OPERATIONS 3-1
Full Spectrum Operations 3-1
Elements of Combat Power 3-3
The Foundations of Army Operations 3-4
The Operational Framework 3-4
Army Capabilities 3-7

Chapter 4 INTELLIGENCE PROCESS IN FULL SPECTRUM OPERATIONS 4-1
The Intelligence Process 4-1
Plan 4-3
Prepare 4-4
Collect 4-8
Process 4-10
Produce 4-10
Common Intelligence Process Tasks 4-11

PART THREE MILITARY INTELLIGENCE DISCIPLINES

Chapter 5 ALL-SOURCE INTELLIGENCE 5-1
Definition 5-1
Role 5-1
Fundamentals 5-2

Chapter 6 HUMAN INTELLIGENCE 6-1
Definition 6-1
Role 6-1
HUMINT Functions 6-1
Operational Employment 6-4
HUMINT Equipment 6-7
Integration of Linguists 6-9
Battle Hand-Off 6-10
Organization 6-10

Chapter 7 IMAGERY INTELLIGENCE 7-1
Definition 7-1
Role 7-1
Fundamentals 7-1

Chapter 8 **SIGNALS INTELLIGENCE** 8-1
Definition 8-1
Role 8-1
Fundamentals 8-1

Chapter 9 **MEASUREMENT AND SIGNATURES INTELLIGENCE** 9-1
Definition 9-1
Role 9-3
Fundamentals 9-4

Chapter 10 **TECHNICAL INTELLIGENCE** 10-1
Definition 10-1
Role 10-1
Fundamentals 10-1

Chapter 11 **COUNTERINTELLIGENCE** 11-1
Definition 11-1
Role 11-1
Counterintelligence Functions 11-2
Operational Employment 11-6
Counterintelligence Equipment 11-9
Integration of Linguists 11-11
Battle Hand-Off 11-12
Organization 11-12

Appendix A **INTELLIGENCE AND INFORMATION OPERATIONS** A-1
The Information Environment A-1
The Commander and Information A-1
Information Superiority A-1

Appendix B **LINGUIST SUPPORT** B-1
Role of Linguists B-1
Linguistic Support Categories B-1
Determining Linguist Requirements B-1
Planning and Managing Linguist Support B-2
Sources of Linguists B-8
Evaluating Linguist Proficiency B-10
Sustaining Military Linguist Proficiency B-11

GLOSSARY Glossary-1
BIBLIOGRAPHY Bibliography-1
INDEX Index-1

Preface

FM 2-0 is the Army's keystone manual for military intelligence (MI) doctrine. It describes—

- The fundamentals of intelligence operations.
- The operational environment (OE).
- Intelligence in unified action.
- The Intelligence Battlefield Operating System (BOS).
- Intelligence considerations in strategic readiness.
- The intelligence process.
- MI roles and functions within the context of Army operations.

This manual conforms to the overarching doctrinal precepts presented in FM 3-0.

This manual provides doctrinal guidance for the Intelligence BOS actions in support of commanders and staffs. It also serves as a reference for personnel who are developing doctrine; tactics, techniques, and procedures (TTP); materiel and force structure; and institutional and unit training for intelligence operations.

This manual provides MI guidance for all commanders, staffs, trainers, and MI personnel at all echelons. It forms the foundation for MI and the Intelligence BOS doctrine development, and applies equally to the Active Component (AC), United States Army Reserve (USAR), and Army National Guard (ARNG). It is also intended for commanders and staffs of joint and combined commands, US Naval and Marine Forces, units of the US Air Force, and the military forces of multinational partners.

Headquarters, US Army Training and Doctrine Command is the proponent for this publication. The preparing agency is the US Army Intelligence Center and School. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: Commander, ATZS-FDT-D (FM 2-0), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017. Send comments and recommendations by e-mail to *ATZS-FDC-D@hua.army.mil*. Follow the DA Form 2028 format or submit an electronic DA Form 2028.

Unless otherwise stated, masculine nouns and pronouns do not refer exclusively to men.

This manual contains Army tactical task (ART) description taken verbatim from the *Army Universal Task List* (AUTL). ART task descriptions are followed by a reference to FM 7-15 in parentheses and the ART number; for example (See FM 7-15, ART 5.1.1.).

PART ONE

Intelligence in the Operational Environment

Part One discusses MI's role in peace, conflict, and war. Supporting the warfighter with effective intelligence is the primary focus of Military Intelligence. Intelligence provides commanders and decisionmakers with the requisite information facilitating their situational understanding so that they may successfully accomplish their missions in full spectrum operations.

Chapter 1 describes the operational environment and the roles of MI within the operational environment. It introduces the Intelligence BOS, the intelligence tasks, and the intelligence process, which are the mechanisms through which MI supports the warfighter. This chapter also introduces the intelligence disciplines, which are explained in detail in Part Three of this manual.

Chapter 2 describes the interaction of MI within the nation's intelligence community structure, providing an overview of the intelligence community at the national level and the unified action level—joint, multinational, and interagency aspects of full spectrum operations. This chapter also discusses the concepts and components of intelligence reach.

Chapter 1

Intelligence and the Operational Environment

ROLE OF INTELLIGENCE

1-1. The commander requires intelligence about the enemy and the battlespace prior to engaging in operations in order to effectively execute battles, engagements, and other missions across the full spectrum of operations. Intelligence assists the commander in visualizing his battlespace, organizing his forces, and controlling operations to achieve the desired tactical objectives or end-state. Intelligence supports force protection (FP) by alerting the commander to emerging threats and assisting in security operations.

1-2. The unit may need to deal with multiple threats. The commander must understand how current and potential enemies organize, equip, train, employ, and control their forces. Intelligence provides an understanding of the enemy, which assists in planning, preparing, and executing military operations. The commander must also understand his OE and its effects on both his own and enemy operations. The commander receives mission-oriented intelligence on enemy forces and the area of operations (AO) from

the G2/S2. The G2/S2 depends upon the intelligence, surveillance, and reconnaissance (ISR) effort to collect and provide information on the enemy and battlespace.

1-3. One of the most significant contributions that intelligence personnel can accomplish is to accurately predict future enemy events. Although this is an extremely difficult task, predictive intelligence enables the commander and staff to anticipate key enemy events or reactions and develop corresponding plans or counteractions. The most important purpose of intelligence is to influence decisionmaking. Commanders must receive the intelligence, understand it (because it is tailored to the commander's requirements), believe it, and act on it. Through this doctrinal concept, intelligence drives operations.

THE INTELLIGENCE BATTLEFIELD OPERATING SYSTEM

1-4. The Intelligence Battlefield Operating System (BOS) is one of seven battlefield operating systems—intelligence, maneuver, fire support (FS), air defense, mobility/countermobility/survivability, combat service support (CSS), and command and control (C2)—that enable commanders to build, employ, direct, and sustain combat power. The Intelligence BOS is a flexible force of personnel, organizations, and equipment that, individually or collectively, provide commanders with the timely, relevant, and accurate intelligence required to visualize the battlefield, assess the situation, and direct military actions. Additionally, the Intelligence BOS is—

- A complex system that operates worldwide, from "mud-to-space," in support of an operation, to include the ability to leverage theater and national capabilities.
- Cooperation and division of labor internally, higher, lower, adjacent, and across components and the coalition.

1-5. The Intelligence BOS not only includes assets within the MI branch but also includes the assets of all branches or BOS that conduct Intelligence BOS tasks. Every soldier, as a part of a small unit, is a potential information collector and an essential component to help reach situational understanding. Each soldier develops a special level of awareness simply due to exposure to events occurring in the AO and has the opportunity to collect information by observation and interaction with the population.

1-6. Planning and executing military operations will require intelligence regarding the enemy and the battlefield environment. The Intelligence BOS generates intelligence and intelligence products that portray the enemy and aspects of the battlespace. These intelligence products enable the commander to identify potential courses of action (COAs), plan operations, employ forces effectively, employ effective tactics and techniques, and take appropriate security measures.

1-7. The Intelligence BOS is always engaged in supporting the commander in offensive, defensive, stability, and support operations. We must posture the Army for success through hard training, thorough planning, meticulous preparation, and aggressive execution. We can no longer allow a "crawl, walk, run" cycle in preparation for operations. In our current environment we must maintain intelligence readiness to support operations on "no notice." This

support is comprehensive and reaches across full spectrum operations and levels of war to produce the intelligence required to win on the battlefield. A combination of space, aerial, seaborne, and ground-based systems provide the most comprehensive intelligence possible. During force projection operations, the Intelligence BOS supports the commander with accurate and responsive intelligence from predeployment through redeployment.

1-8. The Intelligence BOS architecture provides specific intelligence and communications structures at each echelon from the national level through the tactical level. These structures include intelligence organizations, systems, and procedures for collecting, processing, analyzing, and delivering intelligence and other critical information in a useable form to those who need it, when they need it. Effective communications connectivity and automation are essential components of this architecture.

INTELLIGENCE TASKS (METL)

1-9. The personnel and organizations within the Intelligence BOS conduct four primary intelligence tasks that facilitate the commander's visualization and understanding of the threat and the battlespace. These tasks are interactive and often take place simultaneously. (Refer to FM 7-15 for the complete subordinate task listing.) Figure 1-1 shows these tasks tailored to the commander's needs.

INTELLIGENCE TASKS	COMMANDER'S FOCUS	COMMANDER'S DECISIONS
Support to Situational Understanding - Perform IPB - Perform Situation Development - Provide Intelligence Support to Force Protection - Conduct Police Intelligence Operations	**Plan a mission.** **Execute the operation.** **Secure the force.**	**Which COA will I implement?** **Which enemy actions are expected?**
Support to Strategic Responsiveness - Perform I&W - Ensure Intelligence Readiness - Conduct Area Studies of Foreign Countries - Support Sensitive Site Exploitation	**Orient on contingencies.**	**Should I increase the unit's level of readiness?** **Should I implement the OPLAN?**
Conduct Intelligence, Surveillance, and Reconnaissance - Perform Intelligence Synchronization - Perform ISR Integration - Conduct Tactical Reconnaissance - Conduct Surveillance	**Plan the mission.** **Prepare.** **Execute.** **Assess.**	**Which DPs, HPTs, etc., are linked to the enemy actions?** **Are the assets available and in position to collect on the DPs, HPTs, etc.?** **Have the assets been repositioned for contingency mission?**
Provide Intelligence Support to Effects - Provide Intelligence Support to Targeting - Provide Intelligence Support to IO - Provide Intelligence Support to Combat Assessment	**Destroy/suppress/ neutralize targets.** **Reposition intelligence or attack assets.**	**Is my fire (lethal or non-lethal) and maneuver effective?** **Should I refire the same targets?**

Figure 1-1. Intelligence Tailored to the Commander's Needs.

SUPPORT TO SITUATIONAL UNDERSTANDING

1-10. This task centers on providing information and intelligence to the commander, which facilitates his achieving understanding of the enemy and

the environment. It supports the command's ability to make sound decisions. Support to situational understanding comprises four subtasks: perform intelligence preparation of the battlefield (IPB), perform situation development, provide intelligence support to FP, and conduct police intelligence operations.

Perform Intelligence Preparation of the Battlefield

1-11. The G2/S2 is the staff proponent for IPB. IPB is the staff planning activity undertaken by the entire staff to define and understand the battlespace and the options it presents to friendly and threat forces. IPB includes input from the whole staff. There is only one IPB in each headquarters with inputs from all affected staff cells; they are not separate BOS or staff section IPBs throughout the headquarters. It is a systematic process of analyzing and visualizing the threat and battlespace in a specific geographic area for a specific mission or in anticipation of a specific mission. By applying IPB, the commander and staff gain the information necessary to selectively apply and maximize combat power at critical points in time and space. IPB is most effective when it integrates each staff element's expertise into the final products. To conduct effective IPB, the G2/S2 must—

- Produce IPB products that support the staff's preparation of estimates and the military decision-making process (MDMP).
- Identify characteristics of the AO, including the information environment, that will influence friendly and threat operations.
- Establish the area of interest (AOI) in accordance with the commander's guidance.
- Identify gaps in current intelligence holdings.
- Determine multiple enemy COAs (ECOAs) by employing predictive analysis techniques to anticipate future enemy actions, capabilities, or situations.
- Establish a database that encompasses all relevant data sets within and related to the battlespace.
- Determine the enemy order of battle (OB), doctrine, and TTP. Identify any patterns in enemy behavior or activities.
- Accurately identify and report hazards within the AO, including the medical threat and toxic industrial material (TIM).
- Accurately identify threat capabilities, high-value targets (HVTs), and threat models.
- Integrate IPB information into COA analysis and the MDMP.
- Update IPB products as information becomes available.

Perform Situation Development

1-12. Situation development is a process for analyzing information and producing current intelligence about the enemy and environment during operations. The process helps the intelligence officer recognize and interpret the indicators of enemy intentions, objectives, combat effectiveness, and potential ECOAs. Situation development—

- Confirms or denies threat COAs.
- Provides threat locations.

- Explains what the threat is doing in relation to the friendly force operations.
- Provides an estimate of threat combat effectiveness.

1-13. Through situation development, the intelligence officer is able to quickly identify information gaps, and explain enemy activities in relation to the unit's own operations, thereby assisting the commander in gaining situational understanding. Situation development helps the commander make decisions and execute branches and sequels. This reduces risk and uncertainty in the execution of the plan. The intelligence officer maintains, presents, and disseminates the results of situation development through intelligence input to the common operational picture (COP) and other intelligence products.

Provide Intelligence Support to Force Protection

1-14. Provide intelligence in support of protecting the tactical force's fighting potential so that it can be applied at the appropriate time and place. This task includes the measures the force takes to remain viable and functional by protecting itself from the effects of or recovery from enemy activities. FP consists of those actions taken to prevent or mitigate hostile actions against Department of Defense (DOD) personnel (to include Department of Army [DA] civilians, contractors, uniformed personnel, and family members), resources, facilities, and critical information. These actions—

- Conserve the force's fighting potential for application at the decisive time and place.
- Incorporate coordinated and synchronized offensive and defensive measures.
- Facilitate the effective employment of the joint force while degrading the capabilities of and opportunities for the threat.

1-15. Intelligence to FP consists of monitoring and reporting the activities, intentions, and capabilities of adversarial groups and determining their possible COAs. Detecting the adversary's methods in today's OE requires a higher level of situational understanding, informed by current and precise intelligence. This type of threat drives the need for predictive intelligence based on analysis of focused information from intelligence, law enforcement, and security activities.

1-16. Intelligence analysis in support of FP employs analytical methodologies and tools to provide situational understanding and to predict the adversary's actions. Modified or standard time-event charts, association matrixes, activity matrixes, link diagrams, and overlays are beneficial in monitoring the actions of the adversary. Overlays may include (but are not limited to) threat training camps, organizations, finances, personalities, industrial sites, information systems, decisionmaking infrastructures, specific activities, and locations of previous attacks.

Conduct Police Intelligence Operations

1-17. Police intelligence operations (PIO) are a military police (MP) function that supports, enhances, and contributes to the commander's force protection program, COP, and situational understanding. The PIO function ensures that

information collected during the conduct of other MP functions—maneuver and mobility support, area security, law and order, and internment and resettlement—is provided as input to the intelligence collection effort and turned into action or reports. PIO has three components: (See FM 7-15, ART 1.1.4)

- Collect police information.
- Conduct Police Information Assessment Program (PIAP).
- Develop police intelligence products.

Notes:

US Code, Executive Orders, DOD Directives, and Army Regulations contain specific guidance regarding prohibition on the collection of intelligence information on US citizens, US corporations, and resident aliens. These laws and regulations include criminal penalties for their violation. Any PIO directed against US citizens should undergo competent legal review prior to their initiation.

The inclusion of the PIO task branch in the Intelligence BOS does not change the intelligence process described in this manual.

SUPPORT TO STRATEGIC RESPONSIVENESS

1-18. Intelligence support to strategic responsiveness supports staff planning and preparation by defining the full spectrum of threats, forecasting future threats, and forewarning the commander of enemy actions and intentions. Support to strategic responsiveness consists of four subtasks: Perform I&W, ensure intelligence readiness, conduct area studies of foreign countries, and support sensitive site exploitation. (See FM 7-15, ART 1.2)

Perform Indications and Warnings

1-19. This activity provides the commander with forewarning of enemy actions or intentions; the imminence of threat actions. The intelligence officer develops I&W in order to rapidly alert the commander of events or activities that would change the basic nature of the operations. It enables the commander to quickly reorient the force to unexpected contingencies and shape the battlefield. (See FM 7-15, ART 1.2.1)

1-20. The G2/S2 at the operational and strategic levels develops I&W in order to rapidly alert the commander of events or activities that would change the basic nature of the operations so the commander can initiate the appropriate action in a timely manner. I&W reduce the risk of enemy actions that are counter to planning assumptions. I&W enable the commander to quickly reorient the force to unexpected events and to shape the battlefield by manipulating enemy activities.

Ensure Intelligence Readiness

1-21. Intelligence readiness operations support contingency planning and preparation by developing baseline knowledge of multiple potential threats and operational environments. These operations and related intelligence training activities engage the Intelligence BOS to respond effectively to the

commander's contingency planning intelligence requirements. (See FM 7-15, ART 1.2.2) While still in garrison, intelligence defines the full spectrum of threats and forecasts future threats and dangers. Intelligence readiness operations accomplish the following:

- Provide intelligence to support contingency-based training and staff planning.
- Identify, consider, and evaluate all potential threats to the entire unit.
- Provide a broad understanding of the operational environment of the contingency area, which is developed through continuous exchange of information and intelligence with higher echelon and joint intelligence organizations.

Conduct Area Studies of Foreign Countries

1-22. Study and understand the cultural, social, political, religious, and moral beliefs and attitudes of allied, host nation (HN), or indigenous forces to assist in accomplishing goals and objectives. (See FM 7-15, ART 1.2.3)

Note: The inclusion of this task does not change the support to strategic responsiveness provided by MI organizations described in this manual.

Support Sensitive Site Exploitation

1-23. Sensitive site exploitation consists of a related series of activities inside a sensitive site captured from an adversary. A sensitive site is a designated, geographically limited area with special military, diplomatic, economic, or information sensitivity for the United States. This includes factories with technical data on enemy weapon systems, war crimes sites, critical hostile government facilities, areas suspected of containing persons of high rank in a hostile government or organization, terrorist money laundering, and document storage areas for secret police forces. These activities exploit personnel, documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site or its contents. While the physical process of exploiting the sensitive site begins at the site itself, full exploitation may involve teams of experts located around the world. (See FM 7-15, ART 1.2.4)

Note: The inclusion of this task does not change the support to strategic responsiveness provided by MI organizations described in this manual.

CONDUCT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

1-24. With staff participation, the intelligence officer synchronizes intelligence support to the ISR effort by focusing the collection, processing, analysis, and intelligence products on the critical needs of the commander. The operations officer, in coordination with the intelligence officer, tasks and directs the available ISR assets to answer the commander's critical information requirements (CCIRs). Through various detection methods and systematic observation, reconnaissance and surveillance obtains the required information. A continuous process, this task has four subtasks: perform intelligence synchronization, perform ISR integration, conduct tactical reconnaissance, and conduct surveillance. (See FM 7-15, ART 1.3, and FM 3-90).

Perform Intelligence Synchronization

1-25. The intelligence officer, with staff participation, synchronizes the entire collection effort to include all assets the commander controls, assets of lateral units and higher echelon units and organizations, and intelligence reach to answer the commander's priority intelligence requirements (PIRs) and information requirements (IRs). (See FM 7-15, ART 1.3.1)

1-26. The intelligence officer, with staff participation, supports the G3/S3 in orchestrating the entire ISR effort to include all assets the commander controls, assets of lateral units and higher echelon units and organizations, and intelligence reach to answer the CCIRs (PIRs and friendly force information requirements [FFIRs]) and other intelligence requirements. Intelligence synchronization activities include the following:

- Conducting requirements management (RM): anticipate, develop, analyze, validate, and prioritize intelligence requirements. Recommend PIRs to the commander. Manage the commander's intelligence requirements, requests for information (RFIs) from subordinate and lateral organizations, and tasks from higher headquarters. Eliminate satisfied requirements and add new requirements as necessary.
- Developing indicators.
- Developing specific IRs (specific information requirements [SIRs]).
- Converting the SIRs into intelligence tasks or ISR tasks. (See Figure 1-2 for the ISR task development process.) The S2/G2 assigns intelligence production and reach tasks to subordinate intelligence ele-ments or personnel, submits RFIs to higher and lateral echelons, and coordinates with (or assists) the G3/S3 to develop and assign ISR tasks.
- Comparing the ISR tasks to the capabilities and limitations of the available ISR assets (in coordination with the operations officer).
- Forwarding SIRs that cannot be answered by available assets to higher or lateral organizations as RFIs.
- Assessing collection asset reporting and intelligence production to evaluate the effectiveness of the ISR effort.
- Maintaining situational understanding to identify gaps in coverage and to identify the need to cue or redirect ISR assets.
- Updating the intelligence synchronization plan. The G2/S2 manages and updates the intelligence synchronization plan as PIRs are answered and new requirements arise.

1-27. **Intelligence Synchronization Considerations.** The G2/S2 gen-erally follows six considerations in planning intelligence synchronization and ISR activities: anticipate, integrate, prioritize, balance, control, and reach. Refer to FM 2-01 for more information regarding intelligence synchro-nization.

- Anticipate. The intelligence staff must recognize when and where to shift collection or identify new intelligence requirements. The overall intent of this principle is to identify a new or adjust an existing requirement and present it to the commander for approval before waiting for the commander or his staff to identify it.

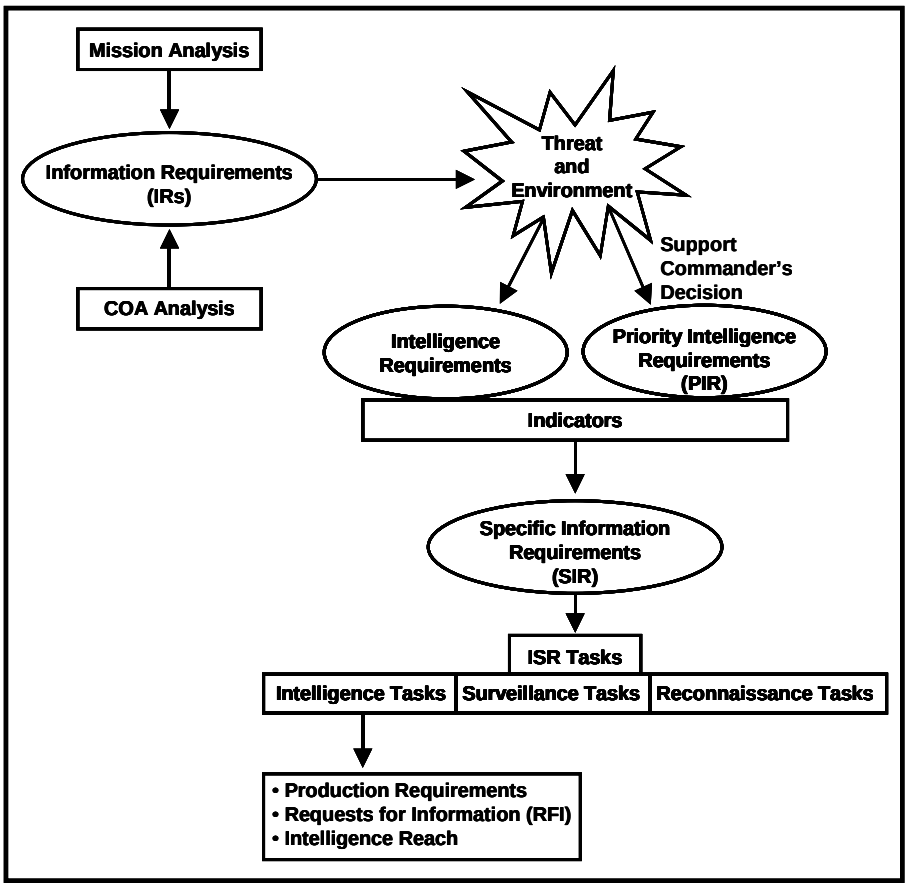


Figure 1-2. ISR Task Development Process.

- Integrate. The intelligence staff must be fully and continuously integrated into the unit's orders production and planning activities to ensure early identification of intelligence requirements. Early and continuous consideration of collection factors enhances the unit's ability to direct collection assets in a timely manner, ensures thorough planning, and increases flexibility in selecting assets.
- Prioritize. Prioritize each intelligence requirement based on its importance in supporting the commander's intent and decisions. Prioritization, based on the commander's guidance and the current situation, ensures that limited ISR assets and resources are directed against the most critical requirements.
- Balance. ISR capabilities complement each other. The intelligence staff should resist favoring or becoming too reliant on a particular unit, discipline, or system. Balance is simply planning redundancy, when required, eliminating redundancy when not desired, and ensuring an appropriate mix of ISR assets or types. The intelligence synchronization matrix (ISM) is useful in determining or evaluating balance.
- Control. To ensure timely and effective responses to intelligence requirements, a unit should first use ISR assets it controls. These

assets usually are more responsive to their respective commander and also serve to lessen the burden on the ISR assets of other units, agencies, and organizations.

- Reach. Although usually not as responsive as a unit's own assets, intelligence reach may be the only way to satisfy an intelligence requirement. If at all possible, one should not depend solely on intelligence reach to answer a PIR.

1-28. **Develop IRs**. The intelligence staff develops a prioritized list of what information needs to be collected and produced into intelligence. Additionally, the intelligence staff dynamically updates and adjusts those requirements in response to mission adjustments and changes. This list is placed against a latest time intelligence is of value to ensure intelligence and information are reported to meet operational requirements. (See FM 7-15, ART 1.3.1) Figure 1-3 shows a comparison of IR, PIR, and intelligence requirements.

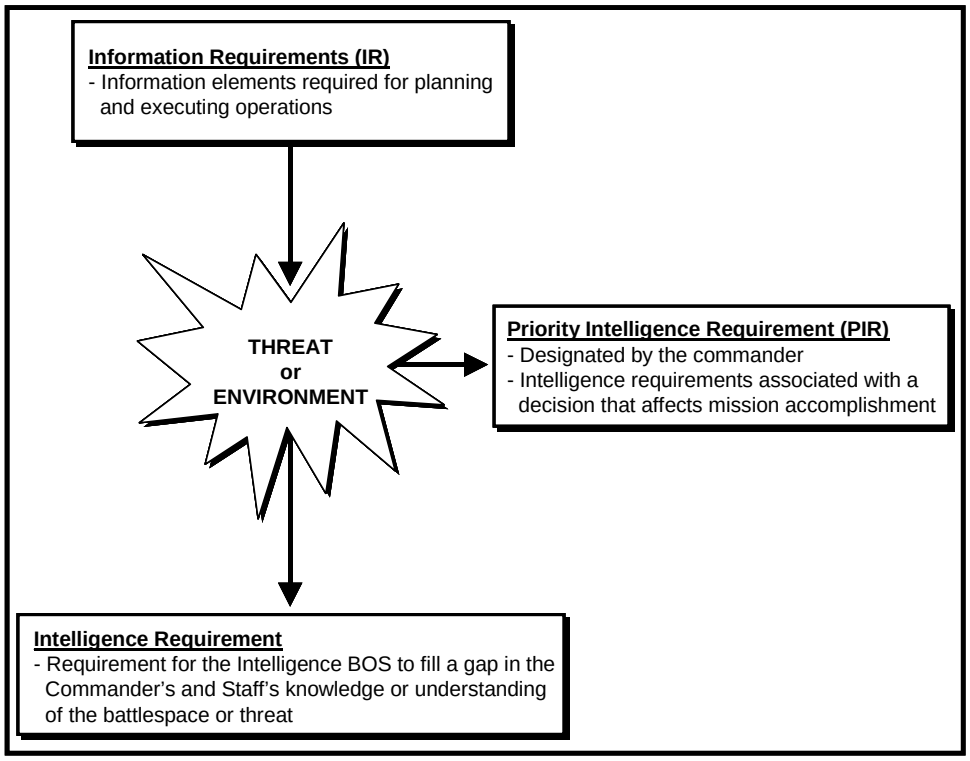


Figure 1-3. IR, PIR, and Intelligence Requirements Comparison

1-29. An effective discussion of ISR has to include an understanding of the CCIRs. The CCIRs are elements of information required by commanders that directly affect decisionmaking and dictate the successful execution of military operations. The commander decides what information is critical based on his experience, the mission, the higher commander's intent, and the staff's input (initial IPB, information, intelligence, and recommendations). Refer to FM 3-0 for more information regarding CCIRs.

1-30. Based on the CCIRs, two types of supporting IRs are generated: PIRs and FFIRs. However, commanders may determine that they need to know whether one or more essential elements of friendly information (EEFI) have been compromised or that the enemy is collecting against a designated EEFI. In those cases, commanders may designate that question as one of their CCIRs. Figure 1-4 shows the CCIR composition.

1-31. IRs are all of the information elements required by the commander and his staff for the successful planning and execution of operations; that is, all elements necessary to address the factors of mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC). Vetting by the commander or his designated represen-tative turns an IR into either a PIR or an intelligence requirement. IRs are developed during COA analysis based on the factors of METT-TC.

1-32. PIRs are those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. PIRs are associated with a decision based on an enemy action or inaction or the battlespace that will affect the overall success of the commander's mission. **The commander designates intelligence require-ments tied directly to his decisions as CCIR (PIR and FFIR)**. Answers to the PIRs help produce intelligence essential to the commander's sit-uational understanding and decisionmaking. For information on PIR devel-opment, see FM 2-01.

1-33. The G2/S2 recommends to the commander those IRs produced during the MDMP that meet the criteria for PIR. They do not become CCIR (PIR and FFIR) until approved by the commander. Additionally, The commander may unilaterally designate PIRs. The IRs that are not designated by the commander as PIRs become intelligence requirements. The intelligence requirement is a gap in the command's knowledge or understanding of the battlespace or threat that the Intelligence BOS must fill.

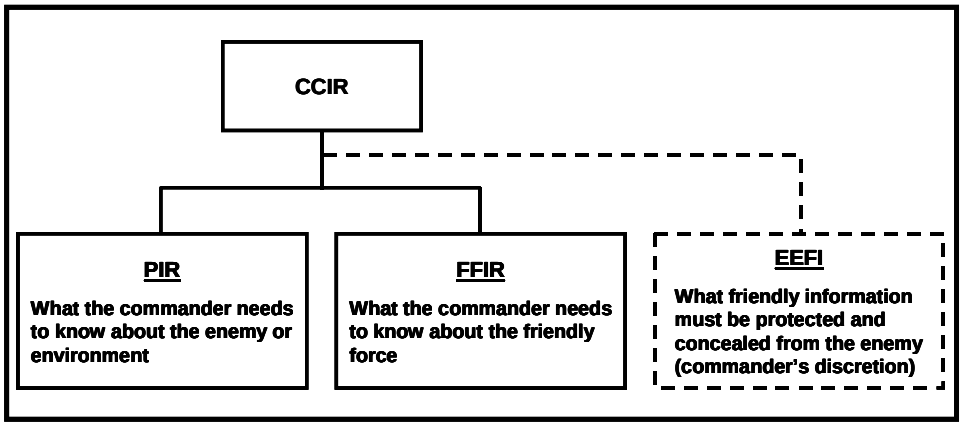


Figure 1-4. Commander's Critical Information Requirements Composition.

1-34. The G3/S3 then tasks the unit's assets to answer both the PIR and intelligence requirements through the ISR plan. PIR should—

- Ask only one question.
- Support a decision.
- Identify a specific fact, event, activity (or absence thereof) which can be collected.
- If linked to an ECOA, indicate an ECOA prior to, or as early as possible in, its implementation.
- Indicate the latest time the information is of value (LTIOV). The LTIOV is the absolute latest time the information can be used by the commander in making the decision the PIR supports. The LTIOV can be linked to time, an event, or a point in the battle or operation.

1-35. **Friendly Force IRs.** The staff also develops FFIRs which, when answered, provide friendly force information that the commander and staff need to achieve situational understanding and to make decisions.

1-36. **Essential Elements of Friendly Information**. EEFI establish information to protect, not information to obtain. However, commanders may determine that they need to know whether one or more EEFI have been compromised or that the enemy is collecting against a designated EEFI. In those cases, commanders may designate that question as one of their CCIRs, which generates PIRs and/or FFIRs. For example, a commander may determine that if the enemy discovers the location and movement of the friendly reserve, the operation is at risk. In this case, the location and movement of the friendly reserve are EEFI. He designates determining whether the enemy has discovered the location and movement of the friendly reserve as one of his CCIR. That CCIR, in turn, generates PIR and FFIR to support staff actions in determining whether the EEFI has been compromised.

1-37. **Develop the Intelligence Synchronization Plan.** The entire unit staff develops their IRs and determines how best to satisfy them. The staff uses reconnaissance and surveillance assets to collect information. The intelligence synchronization plan includes all assets that the operations officer can task or request and coordination mechanisms to ensure adequate coverage of the AOIs. (See FM 7-15, ART 1.3.1.2)

1-38. The intelligence synchronization plan, often presented in a matrix format as an ISM, aids in synchronizing the entire ISR effort with the overall operation and the commander's decisions and/or decision points (DPs). The intelligence synchronization plan is often produced in conjunction with the ISR plan. However, before performing intelligence synchronization and finalizing the intelligence synchronization plan, the G2/S2 must have—

- The CCIR (PIR and FFIR).
- A prioritized list of the remaining intelligence requirements.
- Evaluated ISR assets and resources.
- All of the assigned ISR tasks.

Perform ISR Integration

1-39. The operations officer, in coordination with the intelligence officer and other staff members, orchestrates the tasking and directing of available ISR

assets to answer the CCIR. The operations officer, with input from the intelligence officer, develops tasks from the SIRs which coincide with the capabilities and limitations of the available ISR assets and the latest time information is of value (LTIOV). Intelligence requirements are identified, prioritized, and validated and an ISR plan is developed and synchronized with the scheme of maneuver. (See FM 7-15, ART 1.3.2, and FM 3-90)

1-40. The G3/S3, in coordination with the G2/S2 and other staff members, orchestrates the tasking and directing of available ISR assets to answer the CCIRs (PIRs and FFIRs) and IRs. The result of this process is the forming of the ISR plan. The ISR plan provides a list of all the ISR tasks to be accomplished. The G2/S2 and the G3/S3 develop tasks from the SIRs. These tasks are then assigned based on the capabilities and limitations of the available ISR assets and the LTIOV.

1-41. **Develop the ISR Plan.** The operations officer is responsible for developing the ISR plan. The entire unit staff analyzes each requirement to determine how best to satisfy it. The staff will receive orders and RFIs from both subordinate and adjacent units and higher headquarters. The ISR plan includes all assets that the operations officer can task or request and coordination mechanisms to ensure adequate coverage of the area of interest. (See FM 7-15, ART 1.3.2.1, and FM 3-90)

1-42. **The ISR Plan**. The ISR plan is usually produced as the ISR Annex to an OPORD (Annex L, Intelligence Surveillance, and Reconnaissance). Refer to FM 5-0 for specific and authoritative information on the ISR Annex. ISR is a continuous combined arms effort led by the operations and intelligence staffs in coordination with the entire staff that sets reconnaissance and surveillance in motion. The PIRs and other intelligence requirements drive the ISR effort. The commander takes every opportunity to improve his situational understanding and the fidelity of the COP about the enemy and terrain through the deployment of his ISR assets. Commanders integrate reconnaissance and surveillance to form an integrated ISR plan that capitalizes on their different capabilities. The ISR plan is often the most important part of providing information and intelligence that contributes to answering the CCIRs. For the G2/S2, an effective ISR plan is critical in answering the PIR. Also see FM 3-55 for more information on the ISR plan.

1-43. The ISR plan is not an MI-specific product—the G3/S3 is the staff proponent of the ISR plan— it is an integrated staff product executed by the unit at the direction of the commander. The G2/S2, however, must maintain his situational understanding in order to recommend to the commander and G3/S3 changes or further development of the ISR plan. Based on the initial IPB and CCIRs, the staff—primarily the G2/S2—identifies gaps in the intelligence effort and develops an initial ISR plan based on available ISR assets. The G3/S3 turns this into an initial ISR Annex that tasks ISR assets as soon as possible to begin the collection effort.

1-44. The G3/S3, assisted by the G2/S2, uses the ISR plan to task and direct the available ISR assets to answer the CCIRs (PIRs and FFIRs) and intelligence requirements. Conversely, the staff revises the plan as other intelligence gaps are identified if the information is required to fulfill the

CCIRs or in anticipation of future intelligence requirements. With staff participation, the G2/S2 intelligence officer synchronizes the ISR effort through a complementary product to the ISR plan—the intelligence synchronization plan.

1-45. **Execute and Update the ISR Plan**. The operations officer updates the ISR plan based on information he receives from the intelligence officer. The operations officer is the integrator and manager of the ISR effort through an integrated staff process and procedures. As PIRs are answered and new information requirements arise, the intelligence officer updates intelligence synchronization requirements and provides the new input to the operations officer who updates the ISR plan. He works closely with all staff elements to ensure the unit's organic collectors receive appropriate taskings. This ISR reflects an integrated collection strategy and employment, production and dissemination scheme that will effectively answer the commander's PIR. (See FM 7-15, ART 1.3.2.2, and FM 3-90)

Conduct Tactical Reconnaissance

1-46. To obtain, by visual observation or other detection methods, such as signals, imagery, measurement of signature or other technical characteristics, human interaction and other detection methods about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics and the indigenous population of a particular area. This task includes the conduct of NBC reconnaissance and the tactical aspects of SOF special reconnaissance. The five subtasks are—

- Conduct a Zone Reconnaissance.
- Conduct an Area Reconnaissance.
- Conduct a Reconnaissance in Force.
- Conduct a Route Reconnaissance.
- Conduct a Reconnaissance Patrol.

Note: This task branch includes techniques by which ART 1.1.4.1 (Collect Police Information) may be performed. (FM 7-15)

1-47. Reconnaissance is a mission undertaken to obtain by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, and about the meteorological, hydrographic, or geographic characteristics of an AO. MI personnel and organizations can conduct reconnaissance through obtaining information derived from signals, imagery, measurement of signatures, technical characteristics, human interaction, and other detection methods. When performing reconnaissance, it is important to—

- Orient the reconnaissance asset on the named area of interest (NAI) and/or reconnaissance objective in a timely manner.
- Report all information rapidly and accurately.
- Complete the reconnaissance mission not later than (NLT) the time specified in the order.
- Answer the requirement that prompted the reconnaissance task.

Conduct Surveillance

1-48. To systematically observe the airspace, surface, or subsurface areas, places, persons, or things in the AO by visual, aural (audio), electronic, photographic, or other means. Other means may include but are not limited to space-based systems, and using special NBC, artillery, engineer, SOF, and air defense equipment. (See FM 7-15, ART 1.3.4, and FM 3-90)

Note: This task is a technique by which ART 1.1.4.1 (Collect Police Information) may be performed.

1-49. Conducting surveillance is systematically observing the airspace, surface, or subsurface areas, places, persons, or things in the AO by visual, aural, electronic, photographic, or other means. Surveillance activities include—

- Orienting the surveillance asset on the NAI and/or the surveillance objective in a timely manner.
- Reporting all information rapidly and accurately.
- Completing the surveillance mission NLT the time specified in the order.
- Answering the requirement that prompted the surveillance task.

PROVIDE INTELLIGENCE SUPPORT TO EFFECTS

1-50. The task of providing the commander information and intelligence support for targeting of the threat's forces, threat organizations, units and systems through lethal and non-lethal fires to include electronic attack and information operations. This task includes three subtasks: provide intelligence support to targeting, provide intelligence support to information operations, and provide intelligence support to combat assessment. (See FM 7-15, ART 1.4)

Provide Intelligence Support to Targeting

1-51. The intelligence officer, supported by the entire staff, provides the commander information and intelligence support for targeting the threat's forces and systems through employment of direct, indirect lethal, and non-lethal fires. It includes identification of threat capabilities and limitations. The Intelligence BOS plays a crucial role by providing intelligence throughout the steps of the targeting process: decide, detect, deliver, assess. Support to targeting includes identifying threat capabilities and limitations. The G2/S2 supports the unit's lethal and non-lethal targeting effort through target development, target acquisition (TA), electronic warfare (EW), and combat assessment. This task has two subtasks:

- *Provide Intelligence Support to Target Development* is the systematic analysis of the enemy forces and operations to determine HVTs, systems, and system components for potential attack through maneuver, fires, or information.
- *Provide Intelligence Support to Target Detection* establishes procedures for dissemination of targeting information. The targeting team develops the sensor/attack system matrix to determine the sensor

required to detect and locate targets. The intelligence officer places the following requirements into the integrated ISR plan.

- Requires reconnaissance and surveillance operations to identify, locate, and track high-payoff targets (HPTs) for delivery of lethal or non-lethal effects.
- Includes employing fires, offensive IO, and other attack capabilities against enemy C2 systems as part of the unit's FS plan and IO objectives.

Provide Intelligence Support to Information Operations

1-52. IO are actions taken to affect adversary information, influence other's decisionmaking processes and information systems while protecting one's own information and information systems. Overall operational continuity and mission success requires close, mutual coordination and synchronization of intelligence plans and operations with IO elements and related activities. Refer to Appendix A, this manual, for more information. This task has three subordinate tasks: (See FM 7-15, ART 1.4.2)

- Provide Intelligence Support to Offensive IO.
- Provide Intelligence Support to Defensive IO.
- Provide Intelligence Support to Activities Related to IO.

Provide Intelligence Support to Combat Assessment

1-53. Combat assessment is the determination of the overall effectiveness of force employment during military operations. The objective of combat assessment is to identify recommendations for the course of military operations. It answers the question, "Were the objectives met by force employment?" Although the assessment is primarily an intelligence responsibility, it requires input from and coordination with operations and fire support staffs. Combat assessment consists of conducting physical damage, functional damage, and target system assessments. (See FM 7-15, ART 1.4.3)

1-54. The staff determines how combat assessment relates to a specific target by conducting physical damage, functional damage, and target system assessments.

- Conduct Physical Damage Assessment (PDA). A PDA is an estimate of the extent of physical damage to a target based upon observed or interpreted damage. This post-attack target analysis is a coordinated effort among all units.
- Conduct Functional Damage Assessment (FDA). The FDA estimates the remaining functional or operational capability of a targeted facility or object. The staff bases FDA on the assessed physical damage and estimates of the threat's ability to recuperate (to include the time required to resume normal operations). Multiple echelons typically conduct this all-source analysis. The targeting or combat assessment cell integrates the initial target analyses with other sources, including intelligence, and then compares the original objective with the current status of the target to determine if the objective has been met.
- Conduct Target System Assessment (TSA). The TSA is an estimate of the overall impact of force employment against an adversary's target

system. The unit, supported by higher echelon assets, normally conducts this assessment. The analyst combines all combat assessment reporting on functional damage to targets within a target system and assesses the overall impact on that system's capabilities. This process lays the groundwork for future recommendations for military operations in support of operational objectives.

1-55. **Munitions Effects Assessment (MEA)**. MEA takes place concur-rently and interactively with combat assessment since the same signatures used to determine the level of physical damage also give clues to munitions effectiveness. MEA is primarily the responsibility of operations and FS personnel, with input from the G2/S2. After the same weapon is used to attack several targets of a specific type, MEA should be accomplished to evaluate weapon performance. MEA analysts seek to identify through systematic trend analysis any deficiencies in weapon system and munitions performance or combat tactics by answering the question, "Did the weapons employed perform as expected?" Using a variety of input (targeting analysts, imagery analysts, structural engineers, and mission planners) analysts prepare a report assessing munitions performance. If combat troops capture attacked targets, it is then possible to collect detailed information on the target. Reports should detail weapon performance against specified target types. This information could have a crucial impact on future operations.

1-56. **Re-attack Recommendation**. Re-attack recommendations follow directly from both battle damage assessment (BDA) and MEA efforts. Basically re-attack recommendations answer the question, "Have we achieved the desired effects against our targeted objectives?" Evolving objectives, target selection, timing, tactics, weapons, vulnerabilities, and munitions are all factors in the new recommendations, combining both operations and intelligence functions.

1-57. **Targeting Meeting**. The role of the G2/S2 in targeting meetings is critical to ensuring intelligence supports the targeting process. The G2/S2 must come to the targeting meeting prepared. Additionally, the G2/S2 must understand the steps of the targeting process and tailor the intelligence products and G2/S2 participation according to the targeting process steps of: decide, detect, deliver, and assess.

1-58. There are two major areas in which the G2/S2 must prepare in order to support the targeting meeting.

- Analysis: Determine what the enemy is doing (current situation) and anticipated threat models; ECOA situation templates, ECOA sketches and statements, HVTs, and other associated products.
- IPB Products: Updated from the initial IPB effort, including analytical results (see above bullet), and tailored to the targeting requirements.

1-59. **Decide**. At the targeting meeting, the G2/S2 should be prepared to do the following:

- Brief the current and projected future enemy situation with an event template.

- Brief any combat assessments.
- Brief HVTs for potential selection of HPTs.
- Brief the current PIR portion of CCIRs, the PIRs of the CCIRs for the next phase or in accordance with the same timeframe of the targeting meeting.
- Brief the current ISM or intelligence synchronization plan.
- Participate in wargaming.
- Refine the initial ISR plan (in conjunction with the FS and G3/S3 representatives).

1-60. **Detect**. Based on information from the decide portion of the targeting meeting, the G2/S2 should be prepared to do the following:

- Identify specific ISR assets.
- Develop IRs and propose pertinent IRs to the commander for designation as PIRs.
- Complete the initial ISR plan; ensure it addresses the HPTs.

1-61. **Electronic Warfare**. EW provides targeting information to the commander based on transmitter location data. There are three major subdivisions within EW: electronic support (ES), electronic protection (EP), and electronic attack (EA).

- ES – Also referred to as electronic warfare support (EWS) in JP 1-02, involves actions to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy. In addition to supporting the overall ISR effort, ES is needed to produce intelligence required to support EA missions.
- EP – Involves passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrades, neutralizes, or destroys friendly combat capabilities.
- EA – Involves the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum (EMS), such as jamming and electromagnetic deception.

1-62. **Deliver**. The G2/S2 should be prepared to do the following:

- Brief how the Intelligence BOS will work to detect and track the target through the entire targeting process.
- Brief the implementation of the intelligence synchronization and ISR plans, including the LTIOV and communications structure.

1-63. **Assess**. Depending on the factors of METT-TC and the PIRs, the same ISR assets that detect and track the targets may be required to support combat assessments in order to determine if re-attack is required. Conversely, if re-attack is a decision that the commander will make based upon the

effects on the enemy, combat assessment should be reflected in the PIR, and supported in the corresponding ISR plan.

THE OPERATIONAL ENVIRONMENT

1-64. US military forces face a dynamic, multidimensional, and increasingly interconnected global OE. The world situation is complicated and split into many different factions with many possible conflicts. In addition, the characteristics of warfare continue to change as the nature of conflict changes. Different threats require intelligence operations to adapt to the ever-changing OE. This necessitates that all MI personnel maintain or very quickly build cultural awareness (to a high level of detail) specific to the regional and local environment in the AO. These conditions greatly affect MI, as they increase the degree of difficulty and complexity in determining not only who constitutes the enemy but also which of the many possible ECOAs the enemy could implement.

1-65. If the US can dominate an adversary through its size or technological, organizational, and strategic capabilities, the adversary will resort to unconventional and adaptive ways and means to achieve his ends, which may themselves change at times. MI personnel (uniformed and civilian) must also adapt their operations and thinking to understand and predict or anticipate the enemy's next move. MI personnel must remain vigilant, as any likely adversary is a thinking, adaptive threat with extensive resources which he cultivates through ingenuity, purchase of niche capabilities, and the support of his allies. For example, the adversary—

- May use tactics designed to inflict large numbers of military or civilian casualties or attack high-profile persons.
- May target and destroy subsystems of a BOS individually or collectively.
- May use the local civilian population for cover and support.
- May use the characteristics of the natural environment, industry, and enterprise against our forces in unexpected manners.
- May study every aspect of US doctrine, training, and technological capabilities.
- May quickly overcome any countermeasures and subsequent countermeasures that US forces emplace to deter his activities.
- May employ many personnel to conduct reconnaissance as well as those in the local civilian population who support the threat.
- May attack US information, information systems, and decisionmaking infrastructures in order to discredit or provoke the US, weaken alliances and coalitions, erode public support, incite nation-state and/or international condemnation, and degrade US C2 and/or ISR capabilities.

1-66. The overall ability of US forces to defeat such adversaries depends upon the ability of MI personnel to analyze the current and future methods and capabilities of potential adversaries and incorporate those considerations into training, planning, and executing military operations. The OE will continue to change, thus the US military forces and MI must evolve to provide intelligence.

DIMENSIONS OF THE OPERATIONAL ENVIRONMENT

1-67. The OE has six dimensions: threat, political, unified action, land combat operations, information, and technology. Each affects how Army forces (ARFOR) and MI units plan, prepare, execute, and assess military operations. (See FM 3-0, Chapter 1.)

THREAT

1-68. Extremism, ethnic disputes, poverty, and religious rivalries create unstable conditions within and among states. Rarely are only two sides involved in modern conflicts. More often, one ethno-national group opposes other groups with conflicting interests. This poses a significantly more complex set of enemy or potential adversaries (threat), entities that MI personnel must understand.

1-69. Adversaries will try to create conditions to defeat US operations and to slow the advance of US forces. They will use complex terrain, urban environments, and force dispersal methods—similar to those used by enemies the US has faced before—to offset US advantages. These methods increase the difficulty for MI personnel to identify or locate the enemy's HVTs and may result in US forces' wasting precision weapons on relatively unimportant assets. MI personnel must be aware of the following general concepts that the enemy may use against US forces:

- Conduct force-oriented operations.
- Inflict unacceptable casualties.
- Optimize the use of standoff weaponry and techniques.
- Attempt to control the tempo.
- Create conditions to defeat US forcible entry operations.
- Transition to a defensive framework that avoids decisive battle, preserves capability, and prolongs the conflict. If US forces deploy, the threat may use terrorist and/or information warfare tactics and other measures to erode public support, erode or fracture alliance or multinational cohesion, and the will to fight.
- Conduct effective ISR.
- Use weapons of mass destruction (WMD) to conduct sophisticated ambushes.
- Attack key operating systems or inflict mass casualties within and outside the theater of operations.
- Employ TIM or other toxic substances or pollutants in unconventional manners.
- Use terrain and urban areas to conceal or shield mechanized and armored units. The threat may concentrate and disperse them as opportunities allow, particularly maneuvering forces during periods of reduced exposure to US ISR technology.
- Use effective camouflage and deception techniques.
- Form coalitions against the US.
- Acquire or modify advanced technology systems to create surprise and limited duration superiority in specific areas.

1-70. Additionally, MI personnel must be aware of how to produce intelligence on the many transnational groups that conduct a range of activities that threaten US interests and citizens at home and abroad. Such activities include terrorism, information warfare, illegal drug trafficking, illicit arms and strategic material trafficking, international organized crime, piracy, and deliberate environmental damage.

POLITICAL

1-71. The national security strategy defines how the US meets challenges in the complex and dynamic global environment. It establishes broad strategic guidance for advancing US interests through the instruments of national power. The military components of the National Security Strategy and the National Military Strategy focus on using military force as an instrument of national power. The President and the Secretary of Defense (formerly referred to as National Command Authorities [NCA]) combine using military force with accurate intelligence to preserve, protect, and advance US interests. Translating political decisions into missions depends on informed and candid assessments.

UNIFIED ACTION

1-72. Unified action is a broad generic term that describes the wide scope of actions (including the synchronization of activities with governmental and non-governmental agencies) taking place within unified commands, subordinate unified commands, or joint task forces under the overall direction of the commanders of those commands. (See Chapter 2.) The "Mud to Space" intelligence structure calls for MI to act as part of a fully interoperable and integrated joint intelligence structure. Consequently, the employment of MI in campaigns and major operations must be viewed from a joint perspective. Joint force commanders (JFCs) synchronize the complementary capabilities of the service components that comprise the joint force. They exploit service intelligence capabilities and create an effective joint intelligence team. Often, ARFOR intelligence assets work with multinational and interagency partners to accomplish their missions. Ideally, multinational and interagency intelligence partners provide cultures, perspectives, and capabilities that reinforce and complement Army MI strengths and capabilities. Close intelligence coordination is the foundation of successful unified action.

LAND COMBAT OPERATIONS

1-73. Land combat continues to be the salient feature of conflict. It usually involves destroying or defeating enemy forces or taking land objectives that reduce the enemy's effectiveness or will to fight. The axiom "intelligence drives operations" continues to be true; operations and intelligence are complementary. Four characteristics distinguish land combat. The support MI provides is covered in each:

- Scope. Intelligence considers and strives to understand an enemy throughout the depth of an operational area. Commanders rely on intelligence in order to use maneuver, fires, and other elements of combat power to defeat or destroy enemy forces.

- Duration. Intelligence assets routinely conduct missions prior to, during, and after the commitment of land combat forces. Intelligence is always engaged.
- Terrain. Intelligence missions occur among a complex variety of natural and manmade features. Employing intelligence assets in the complexity of the ground environment requires thorough planning. Employing intelligence assets must account for the visibility and clutter of the terrain and the effects of weather and climate.
- Permanence. MI forces are integrated with, or assigned to, land combat forces as they seize or secure ground. MI assets with these land combat forces make permanent the temporary intelligence capabilities of other operations.

INFORMATION

1-74. Many intelligence operations take place within an information environment that is largely outside the control of military forces. The information environment is the aggregate of individuals, organizations, and systems that collect, process, store, display, and disseminate information; also included is the information itself. (See JP 3-13 and FM 3-13). National, international, and non-state actors use the information environment to collect, process, and disseminate information. The media's use of real-time technology affects public opinion, both in the US and abroad, and alters the conduct and perceived legitimacy of military operations. Now, more than ever, every soldier is a potential representative of America to a global audience. The adaptive thinking adversary will often seek to exploit the information environment in an effort to counter, weaken, and defeat the US. Information warfare will be directed against the US and US interests. While the level of sophistication of such attacks may vary, they nonetheless will take place and over time will take their toll.

1-75. Historically, information superiority has enabled decisive ARFOR operations. Information superiority enables ARFOR to see first, understand the situation more quickly and accurately, and act faster than their adversaries. Information superiority, which is derived from the effective synchronization of ISR, information management (IM), and IO, is an operational advantage that results in friendly forces gaining and retaining the initiative. Effective ISR operations and IM identify the information commanders require, collect it, and get it to them when they need it. Offensive IO degrade an adversary's will to resist and ability to fight while simultaneously denying him relevant friendly force information. Defensive IO protect friendly information and C2 systems. Information superiority means commanders receive accurate and timely information that enables them to make better decisions and act faster than their adversaries.

TECHNOLOGY

1-76. Technology greatly enables intelligence operations. It enhances the intelligence leader, unit, and soldier performance and affects intelligence operations in full spectrum operations. Intelligence system interoperability is a major concern for the G2/S2, commanders, and staffs as they plan, prepare forces, and weigh employment options. Quality intelligence provided by

advanced ISR capabilities and communications, coupled with sound IM, assists commanders in making decisions.

1-77. Battle command benefits from the ability of modern intelligence and telecommunications systems to provide intelligence products faster and more precisely. Technology improves all facets of intelligence, thereby increasing the potential for mission accomplishment. MI personnel must be able to operate their respective systems at their maximum potential. An MI soldier who can use technology to improve the quality, timeliness, and method of presentation of intelligence products provided to the commander is extremely valuable.

1-78. In all operations, MI personnel must determine the extent to which their adversaries possess at least some advanced weaponry. Their weaponry may range from a computer connected to the Internet to WMD. Adversaries may also possess information-based technologies or capabilities, such as satellite imagery, night vision devices (NVDs), or precision-delivery systems. The potential for asymmetric threats puts a premium on IPB and the other intelligence tasks, to include situation development and providing I&W. Operational success requires identifying and evaluating enemy capabilities (strengths and vulnerabilities), intentions, and potential ECOAs.

CRITICAL VARIABLES OF THE CONTEMPORARY OPERATIONAL ENVIRONMENT

1-79. The contemporary operational environment (COE) is the operational environment that exists in the world today and is expected to exist until a peer competitor arises. There are eleven critical variables, as shown in Figure 1-5, that facilitate understanding the threat and define the OE. These variables are interrelated, and different variables will be more or less important in relation to each other in different situations. Only by studying and understanding these variables—and incorporating them into training—will the US Army be able to both keep adversaries from gaining an operational advantage against the US and to find ways to use them to our own advantage. Figure 1-5 not only depicts the critical variable of the OE but it also shows that they are linked to all the dimensions of the OE.

NATURE AND STABILITY OF THE STATE

1-80. This variable refers to how strong or weak a country is. It is important to determine where the real strength of the state lies; it may be in the political leadership, the military, the police, or some other element of the population—or in some combination of these factors. Intelligence will provide the information crucial in defining the battlefield environment and allow US forces to better understand all aspects of the AO, the nature of the military campaign, and the true aims of an enemy campaign, operation, or action. Intelligence will inform the commander of threats that may be present in a particular country. The most direct and potentially lethal threat to US forces may come from elements other than the threat's military forces. Intelligence must also be aware of the condition of, or conditions leading to, a failed state.

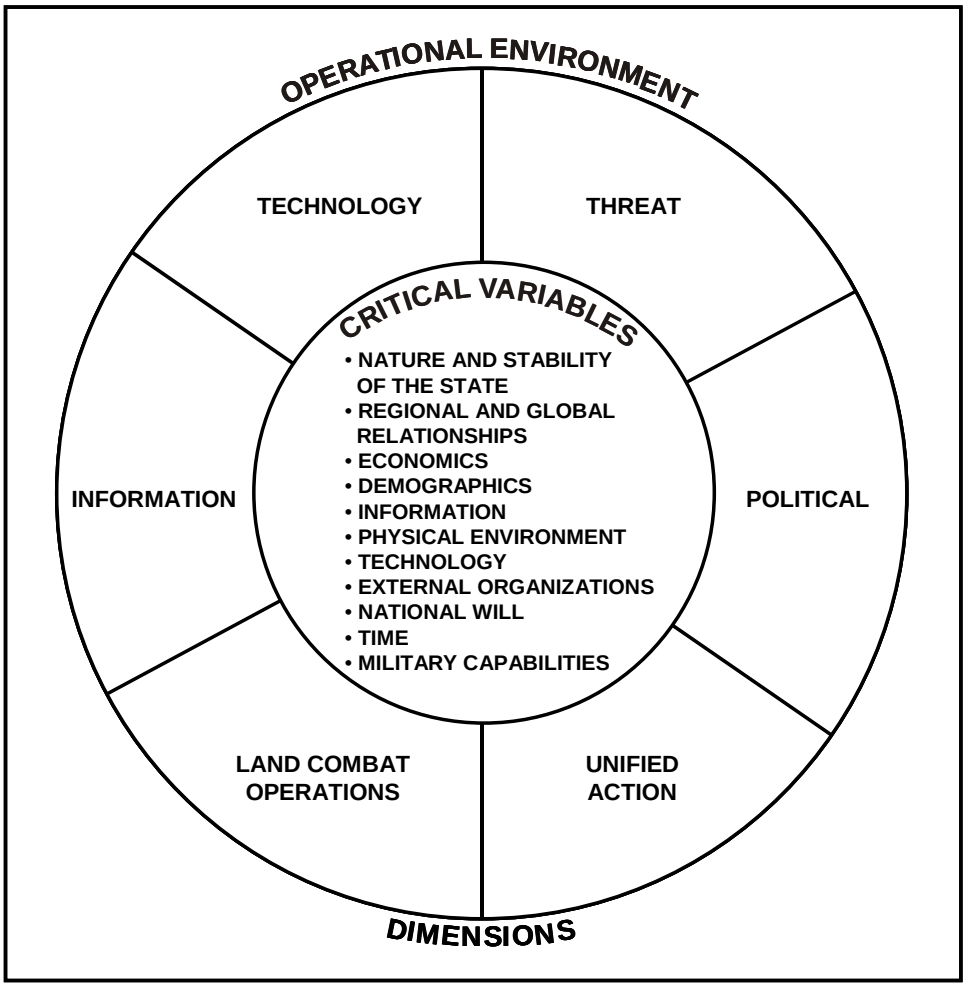


Figure 1-5. Critical Variables And Dimensions of the Operational Environment

REGIONAL AND GLOBAL RELATIONSHIPS

1-81. Nation-states and/or non-state actors often enter into relationships, which can be regional or global. These partnerships support common objectives, which can be political, economic, military, or cultural. When actors create regional or global alliances, it can add to their collective capability and broaden the scale of operations and actions. Intelligence will provide the commander with a visualization of all real and/or potential adversaries and the various aspects of their cooperation that could impact on the operation.

ECONOMICS

1-82. The economic variable consists of economic conditions in the region and economic ties between regional states and other world regions or other countries; the role that economic power plays in the operational environment; and the ability of the United States and its allies to apply economic power in the specific situation. A significant gap in the economic conditions among nation-states and other actors can be a source of conflict. Economic power

provides the enemy with increased flexibility and adaptability. It can provide an enemy with the ability to purchase modern technology that can be used to counter US operations and prolong operations. In some cases, economic superiority, rather than military superiority, may be the key to power or dominance within a region. The IPB process identifies those elements of economic power that may be a significant characteristic of the battlefield. However, the application of the economic instrument of national power lies primarily outside the military sphere.

DEMOGRAPHICS

1-83. The demographics variable includes the cultural, religious, and ethnic makeup of a given region, nation, or non-state actor; additionally, such factors as public health and other population trends must be considered. Intelligence and information enable the commander to understand the influences of the demographic features of his AO. An evaluation of the situation and possible threats with these factors in mind will provide the commander with knowledge concerning underlying demographics that could affect operations in the region. Additionally, intelligence can provide information on whether the population is sympathetic to the US or the enemy cause or is uncommitted in its views to either the US or the enemy.

INFORMATION

1-84. Broadcast media and other information means can make combat operations visible to a global audience. Various actors seek to use perceptions to control and manipulate how the public views events. The enemy will exploit US mistakes and failures, create disinformation based on falsehoods, and use propaganda to sway the local population to support their cause, to alienate world opinion, and to influence US public opinion. Media coverage can affect US political decisionmaking, internal opinion, or the sensitivities of multinational members. Intelligence can determine the enemy's ability to manage and manipulate information as well as assess the enemy's ability to access or disrupt US systems (for example, satellite communications [SATCOM] and imagery). Intelligence can also inform the commander on the enemy's communication infrastructure, to include its capabilities and vulnerabilities.

PHYSICAL ENVIRONMENT

1-85. The main elements of the physical environment are terrain and weather, including the medical threat. Intelligence often considers terrain and weather effects on not only the earth's surface but also subterranean, aerospace, and space. Potential enemies understand that less complex and open environments favor a US force. Therefore, the enemy may try to operate in urban environments, in complex terrain, and in weather conditions that may adversely affect US military operations and mitigate technological advantages. Intelligence provides a thorough analysis and evaluation of the effects of weather, prevalent diseases, and terrain on military operations. Analysis of the adversary provides information on his preferred tactics, weapons systems, and other capabilities and vulnerabilities.

TECHNOLOGY

1-86. Even adversaries lacking a research and development (R&D) capability can purchase sophisticated systems, or gain access to such systems, in the global marketplace. Commanders and staffs should prepare for adversaries who use technology in sophisticated ways. These ways may differ sharply from the ways that US forces use similar technologies. The technology that nations or non-state actors can bring to the OE includes what they can develop, as well as what they can acquire through purchase or capture. MI —

- Provides intelligence on the enemy's technological capabilities and vulnerabilities.
- Provides the commander with intelligence regarding the enemy's potential technological ability to achieve equality or even superiority against the US in selected areas.
- Indicates whether or not the enemy is employing dual-use technologies.

EXTERNAL ORGANIZATIONS

1-87. When the US Army conducts operations of any kind in a failed state or areas torn by conflict, it is likely to find non-governmental organizations (NGOs), international humanitarian organizations, multinational corporations, and other civilian organizations at work there. These organizations and/or their members can have both stated and hidden interests and objectives that can either assist or hinder US mission accomplishment. Defining the battlefield environment should provide the commander with information as to the impact civilians on the battlefield will have on mission accomplishment. Intelligence, in conjunction with other members of the commander's staff, can inform the commander on the number and types of humanitarian organizations and multinational corporations operating in the country or region and whether those organizations are supporting or hindering US mission accomplishment.

NATIONAL WILL

1-88. The willingness of the people to submit to enemy operations can be a significant characteristic of the battlefield. The intensity and durability of this support can influence the objectives of a conflict, its duration, the type and intensity of the enemy's operations in opposition to US operations, and the conditions for ending the conflict. Intelligence about the national will could affect the conduct of information operations.

TIME

1-89. Potential adversaries of the US generally view time as being to their advantage. An adversary may see prolonging combat operations for an extended period as a means of tying down US forces, increasing opportunities to inflict casualties on US forces, stirring public opinion in the area of responsibility (AOR) against the US presence and operations, and creating dissatisfaction in US public opinion. For example, an adversary can use the time required for US forces to deploy into an area to manipulate the nature of the conflict, attempting to control the tempo of operations by influencing early entry operations and prolonging operations with the desire to increase friendly casualties. Once US forces have deployed and begun operations in an

AOR, the adversary may adopt modes of operation that seek to avoid decisive conflict to inflict casualties on US forces and create more favorable conditions for future combat. Intelligence provides the commander with information on the enemy's ability to use the time factor to impact on the commander's mission.

MILITARY CAPABILITIES

1-90. Intelligence supports the commander's understanding of the adversary's military capabilities and ability to use conventional and unconventional tactics. The adversary will be flexible, thinking, adaptive, and capable of using a combination of conventional and unconventional warfare tactics. Modern technology will enhance his capabilities. Terrorism, suicide bombings, WMD, sabotage, information warfare, and assassinations are but a few of the tactics within the adversary's arsenal.

THE INTELLIGENCE PROCESS

1-91. Intelligence operations generally include the five functions that constitute the intelligence process: **plan, prepare, collect, process,** and **produce**. Additionally, there are three common tasks that occur across the five functions of the intelligence process: **analyze, disseminat*e,*** and **assess**. The three common tasks are discussed after the last function, produce. The intelligence process functions are not necessarily sequential; this is what differentiates the Army's intelligence process from the Joint intelligence cycle. The intelligence process provides a common model with which to guide one's thinking, discussing, planning, and assessing about the threat or AOI environment. The intelligence process generates information about the threat, the AOI, and the situation, which allows the commander and staff to develop a plan, seize and retain the initiative, build and maintain momentum, and exploit success.

PLAN

1-92. The plan step consists of the activities that identify pertinent IRs and develop the means for satisfying those requirements. The CCIRs (PIRs and FFIRs) drive the planning of the ISR effort. The intelligence officer supports the G3/S3 in arranging the ISR effort, based on staff planning, to achieve the desired collection effects. Planning activities include, but are not limited to—

- Conducting IPB.
- Managing requirements.
- Submitting RFIs and using intelligence reach to fill information gaps.
- Evaluating reported information.
- Establishing the intelligence communications and dissemination architecture.
- Developing, managing, and revising the intelligence synchronization plan and the ISR plan as mission requirements change.

PREPARE

1-93. The failure of MI units or personnel to accomplish their tasks or missions can often be attributed to their failure to prepare. The prepare step includes those staff and leader activities which take place upon receiving

the operation order (OPORD), operation plan (OPLAN), warning order (WARNO), or commander's intent in order to improve the unit's ability to execute tasks or missions.

1-94. The most habitual and egregious preparation failures committed by leaders (as evidenced by performance at the combat training centers) is not the conduct of specific tasks, but the failure to adequately coordinate for more generic combat requirements such as—

- Friendly forward unit liaison.
- Departing or reentering friendly lines or AOs.
- Fire support: enroute, at mission location, and return.
- Casualty evacuation procedures.
- Passwords (running, forward of friendly lines), recognition signals, call signs, and frequencies.
- Resupply.
- Movement through friendly AOs.

COLLECT

1-95. The collect step involves collecting and reporting information in response to ISR tasking. ISR assets collect information and data about threat forces, activities, facilities, and resources as well as information concerning the environmental and geographical characteristics of a particular battlespace. A successful ISR effort results in the timely collection and reporting of relevant and accurate information. This collected information forms the foundation of intelligence databases, intelligence production, and the G2's/S2's situational understanding. The requirements manager evaluates the reported information for its responsiveness to the CCIRs (PIRs and FFIRs).

PROCESS

1-96. Processing involves converting collected data and information into a form that is suitable for analyzing and producing intelligence. Examples of processing include developing film, enhancing imagery, translating a document from a foreign language, converting electronic data into a standardized report that can be analyzed by a system operator, and correlating information.

1-97. Processing data and information is performed unilaterally and cooperatively by both humans and automated systems.

PRODUCE

1-98. The produce step involves evaluating, analyzing, interpreting, synthesizing, and combining information and intelligence from single or multiple sources into intelligence or intelligence products in support of known or anticipated requirements. Production also involves combining new information and intelligence with existing intelligence in order to produce intelligence in a form that the commander and staff can apply to the MDMP and that supports and helps facilitate situational understanding. During the produce step, the intelligence staff manipulates information by—

- Analyzing the information to isolate significant elements.

- Evaluating the information to determine accuracy, timeliness, usability, completeness, precision, and reliability.
- Combining the information with other relevant information and previously developed intelligence.
- Applying the information to estimate possible outcomes.
- Presenting the information in a format that will be most useful to its eventual user.

1-99. The intelligence staff deals with numerous and varied production requirements based on PIRs and intelligence requirements; diverse missions, environments, and situations; and presentation requirements. Through analysis, collaboration, and intelligence reach, the G2/S2 and the staff use the collective intelligence production capability of higher, lateral, and subordinate echelons to meet the production requirements. Proficiency in these techniques and procedures facilitates the intelligence staff's ability to answer command and staff requirements regardless of the factors of METT-TC.

1-100. The three common tasks, discussed below, can occur throughout the intelligence process.

Analyze

1-101. The intelligence staff analyzes intelligence and information about the enemy's capabilities, friendly vulnerabilities, and the battlefield environment as well as issues and problems that arise within the intelligence process itself to determine their nature, origin, and interrelationships. This analysis enables commanders, staffs, and leaders to determine the appropriate action or reaction and to focus or redirect assets and resources to fill information gaps or alleviate pitfalls. It is also within the analyze function that intelligence analysts sort through large amounts of collected information and intelligence to obtain only that information which pertains to the CCIRs (PIRs and FFIRs), maintenance of the COP, and facilitates the commander's situational understanding.

Disseminate

1-102. Disseminating is communicating relevant information of any kind from one person or place to another in a usable form by any means to improve understanding or to initiate or govern action. Disseminating intelligence entails using information management techniques and procedures to deliver timely, relevant, accurate, predictive, and usable intelligence to the commander. Determining the product format and selecting the means to deliver it are key aspects of dissemination. Information presentation may be in a verbal, written, interactive, or graphic format. The type of information, the time allocated, and the individual preference of the commander all influence the information format.

Assess

1-103. Assessment plays an integral role in all aspects of the intelligence process. Assessing includes evaluating the effectiveness of intelligence in supporting the operation. Assessing the situation and available information begins upon receipt of the mission and continues throughout the intelligence

process. The continual assessment of intelligence operations and ISR efforts, available information and intelligence, and various aspects of the factors of METT-TC are critical to ensure—

- The G2/S2 answers all CCIRs (PIRs and FFIRs).
- The G2/S2 and G3/S3 redirect ISR assets to support changing requirements.
- Using information and intelligence properly.

INTELLIGENCE DISCIPLINES

1-104. Intelligence disciplines are categories of intelligence functions. The Army's intelligence disciplines are All-Source Intelligence, Human Intelligence (HUMINT), Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Measurement and Signatures Intelligence (MASINT), Technical Intelligence (TECHINT), and Counterintelligence (CI). Although JP 2-0 defines these intelligence disciplines, it also includes Open-Source Intelligence (OSINT) as a separate intelligence discipline. Because OSINT is more appropriately defined as a category of information, used singly or integrated into an all-source analytical approach, it is not defined in this manual as an intelligence discipline. For more information regarding the intelligence disciplines, see Part Three of this manual, as well as the respective manuals, which covers each individual intelligence discipline.

ALL-SOURCE INTELLIGENCE

1-105. All-source intelligence is defined as the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open-source information, in the production of intelligence. All-source intelligence is a separate intelligence discipline, as well as the name of the task used to produce intelligence from multiple intelligence or information sources.

HUMAN INTELLIGENCE

1-106. HUMINT is the collection of foreign information—by a trained HUMINT Collector—from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool, and a variety of collection methods, both passively and actively, to collect information.

IMAGERY INTELLIGENCE

1-107. IMINT is intelligence derived from the exploitation of imagery collected by visual photography, infrared, lasers, multi-spectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media.

SIGNALS INTELLIGENCE

1-108. SIGINT is a category of intelligence comprising either individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however transmitted. SIGINT is derived from communications, electronics, and foreign instrumentation signals.

MEASUREMENT AND SIGNATURES INTELLIGENCE

1-109. MASINT is technically derived intelligence that detects, locates, tracks, identifies, and/or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from IMINT and SIGINT collection. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical (E-O), acoustic, radio frequency (RF), nuclear detection, and seismic sensors, as well as techniques for gathering chemical, biological, radiological, and nuclear (CBRN), and other material samples.

TECHNICAL INTELLIGENCE

1-110. TECHINT is intelligence derived from the collection and analysis of threat and foreign military equipment and associated materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical (S&T) capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages.

COUNTERINTELLIGENCE

1-111. CI counters or neutralizes intelligence collection efforts through collection, counter-intelligence investigations, operations, analysis, and production, and functional and technical services. CI includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies; and is the key intelligence community contributor to protect US interests and equities. CI assists in identifying EEFI, identifying vulnerabilities to threat collection, and actions taken to counter collection and operations against US forces.

FORCE PROJECTION OPERATIONS

1-112. Force projection is the military component of power projection. It is a central element of the national military strategy. Army organizations and installations, linked with joint forces and industry, form a strategic platform to maintain, project, and sustain ARFOR, wherever they deploy. Force projection operations are inherently joint and require detailed planning and synchronization. Force projection encompasses a range of processes—mobilization, deployment, employment, sustainment, and redeployment—discussed below.

1-113. The Army must change its mindset from depending on an "intelligence buildup" to performing intelligence readiness on a daily basis in order to meet the requirements for strategic responsiveness. MI personnel, even in garrison at the lowest tactical echelons, must use their analytic and other systems and prepare for possible operations on a daily basis.

1-114. Built on a foundation of intelligence readiness, the Intelligence BOS provides the commander with the intelligence he needs to plan, prepare, and execute force projection operations. Successful intelligence during force projection operations relies on continuous collection and intelligence production before and during the operation. In a force projection operation,

higher echelons will provide intelligence to lower echelons until the tactical ground force completes entry and secures the lodgment area. The joint force J2 must exercise judgment when providing information to subordinate G2s/S2s so not to overwhelm them. Figure 1-6 is an example of force projection intelligence.

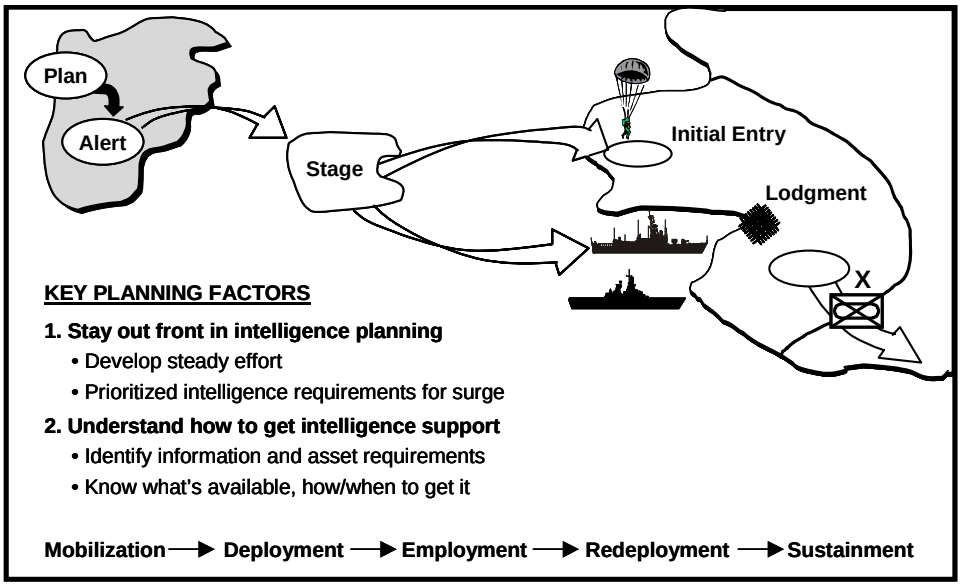


Figure 1-6. Force Projection Intelligence.

1-115. The G2/S2 must anticipate, identify, consider, and evaluate all threats to the entire unit throughout force projection operations. This is critical during the deployment and entry operations stages of force projection. During these stages, the unit is particularly vulnerable to enemy actions because of its limited combat power and knowledge of the AO. Intelligence personnel must, therefore, emphasize the delivery of combat information and intelligence products that indicate changes to the threat or battlespace developed during predeployment IPB.

1-116. The G2/S2 should—

- Review available databases on assigned contingency AOIs, conduct IPB on these AOIs, and develop appropriate IPB products.
- Comply with higher headquarters standing operating procedures (SOPs) and manuals for specific intelligence operations guidance.
- Coordinate for and rehearse electronic message transfers (for example, Internet Protocol addresses, routing indicators) using the same communications protocols with theater, higher headquarters, subordinate, and lateral units that the unit would use when deployed.
- Plan, train, and practice surging intelligence functions on likely or developing contingency crises.
- Prepare and practice coordination from predeployment through redeployment with other elements and organizations (for example, HUMINT, IMINT, SIGINT, MASINT, IO, staff weather officer [SWO],

civil affairs [CA], psychological operations [PSYOP], and special operations forces [SOF] units, to include databases and connectivity).

- Include the following as a part of daily (sustainment) operations:
  - RC and other augmentation.
  - A linguist plan with proficiency requirements. (Alert linguists through early entry phases of deployment.)
  - Training (individual and collective).
- Establish formal or informal intelligence links, relationships, and networks to meet developing contingencies.
- Forward all RFIs to higher headquarters in accordance with SOPs.
- Establish statements of intelligence interests (SIIs), other production, and I&W requirements.

1-117. To draw intelligence from higher echelons and focus intelligence downward, based on the commander's needs, the G2/S2 must—

- Understand the J2's multiple echelon and broadcast dissemination capability to ensure near-real time (NRT) reporting to all deployed, in transit, or preparing to deploy forces.
- Maintain or build intelligence databases on the environment and threats for each probable contingency.
- State and record the CCIR (as a minimum, list the PIRs and ISR tasks or requests).

1-118. Until the unit's collection assets become operational in the AO, the G2/S2 will depend upon intelligence from the ARFOR or JTF to answer the unit's intelligence needs. The following paragraphs describe the intelligence and ISR considerations during force projection.

MOBILIZATION

1-119. Mobilization is the process by which the armed forces or part of them are brought to a state of readiness for war or other national emergency. It assembles and organizes resources to support national objectives. Mobilization includes activating all or part of the RC, and assembling and organizing personnel, supplies, and materiel. A unit may be brought to a state of readiness for a specific mission or other national emergency. This process, called mobilization, is where specific AC or RC units, capabilities, and personnel are identified and integrated into the unit. During mobilization, the G2/S2 must—

- Monitor intelligence reporting on threat activity and I&W data.
- Manage IRs and RFIs from their unit and subordinate units to include updating ISR planning.
- Establish habitual training relationships with their AC and RC augmentation units and personnel as well as higher echelon intelligence organizations as identified in the existing OPLAN. Support the RC units and augmentation personnel by preparing and conducting intelligence training and threat update briefings and by disseminating intelligence.
- Identify ISR force requirements for the different types of operations and contingency plans (CONPLANs).

- Identify individual military, civilian, and contractor augmentation requirements for intelligence operations. The Army, and the Intelligence BOS in particular, cannot perform its missions without the support of its Department of the Army Civilians (DACs) and contractors. The force increasingly relies on the experience, expertise, and performance of non-uniformed personnel and has fully integrated these non-uniformed personnel into the warfighting team.

1-120. During mobilization the G2/S2, in conjunction with the rest of the staff, must ensure the adequacy of training and equipping of AC and RC MI organizations and individual augmentees to conduct intelligence operations.

1-121. The G2/S2 supports peacetime contingency planning with IPB products and databases on likely contingency areas. The G2/S2 establishes an intelligence synchronization plan that will activate upon alert notification. For smooth transition from predeployment to entry, the G2/S2 must coordinate intelligence synchronization and communications plans before the crisis occurs. The intelligence synchronization plan identifies the intelligence requirements supporting those plans, to include—

- ISR assets providing support throughout the AOI.
- Command and support relationships of ISR assets at each echelon.
- Report and request procedures not covered in unit SOPs.
- Sequence of deployment of ISR personnel and equipment. Early deployment of key ISR personnel and equipment is essential for force protection and combat readiness. Composition of initial and follow-on deploying assets is influenced by the factors of METT-TC, availability of communications, and availability of lift.
- Communications architecture supporting both intelligence staffs and ISR assets.
- Friendly vulnerabilities to hostile intelligence threats and plans for conducting FP measures. The staff must begin this type of planning as early as possible to ensure adequate support to FP of deploying and initial entry forces.
- Monitor time-phased force and deployment data (TPFDD) and recommend changes in priority of movement, unit, or capability to enable ISR operations.

1-122. The G2/S2 must continually monitor and update the OPLANs to reflect the evolving situation, especially during crisis situations. National intelligence activities monitor regional threats throughout the world and can answer some intelligence requirements supporting the development of OPLANs.

1-123. Upon alert notification, the G2/S2 updates estimates, databases, IPB products, and other intelligence products needed to support command decisions on force composition, deployment priorities and sequence, and the AOI. Units reassess their collection requirements immediately after alert notification. The G2/S2 begins verifying planning assumptions within the OPLANs. CI and ISR personnel provide FP support and antiterrorism measures.

1-124. Throughout mobilization, unit intelligence activities will provide the deploying forces with the most recent intelligence on the AO. The intelligence staff will also update databases and situation graphics. The G2/S2 must—

- Fully understand the unit, ARFOR, and joint force intelligence organizations.
- Revise intelligence and intelligence-related communications architecture and delete or integrate any new systems and software with the current architecture.
- Support 24-hour operations and provide continuous intelligence.
- Plan all required intelligence reach procedures.
- Determine transportation availability for deployment and availability when deployed.
- Determine all sustainability requirements.
- Determine intelligence release requirements and restrictions; releasability to multinational and HN sources.
- Review status of forces agreements (SOFAs), rules of engagement (ROE), international laws, and other agreements, emphasizing the effect that they have on intelligence collection operations. (Coordinate with the staff judge advocate [SJA] on these issues.)
- Ensure ISR force deployment priorities are reflected in the TPFDD to support ISR operations based upon the factors of METT-TC.
- Ensure intelligence links provide the early entry commander vital access to multi-source army and joint intelligence collection assets, processing systems, and databases.
- Review the supporting unit commanders' specified tasks, implied tasks, task organization, scheme of support, and coordination requirements with forward maneuver units. Address issues or shortfalls and direct or coordinate changes.
- Establish access to national HUMINT, IMINT, SIGINT, MASINT, and CI databases, as well as automated links to joint service, multinational, and HN sources.

DEPLOYMENT

1-125. Deployment is the movement of forces and materiel from their point of origin to the AO. This process has four supporting components: predeployment activities, fort to port, port to port, and port to destination; these components are known collectively as reception, staging, onward movement, and integration (RSO&I) activities. Success in force projection operations hinges on timely deployment. The size and composition of forces requiring lift are based on the factors of METT-TC, availability of prepositioned assets, the capabilities of HN support, and the forward presence of US forces. Force or tactical tailoring is the process used to determine the correct mix and sequence of deploying units.

1-126. During deployment, intelligence organizations at home station or in the rear area take advantage of modern SATCOM, broadcast technology, and automated data processing (ADP) systems to provide graphic and textual intelligence updates to the forces enroute. Enroute updates help eliminate

information voids and, if appropriate, allow the commander to adjust the plan prior to arrival in theater in response to changes in the OE or enemy actions.

1-127. Intelligence units extend established networks to connect intelligence staffs and collection assets at various stages of the deployment flow. Where necessary, units establish new communications paths to meet unique demands of the mission. The theater and corps analysis and control elements (ACEs) play a critical role in making communications paths, networks, and intelligence databases available to deploying forces.

1-128. Space-based systems are key to supporting intelligence during the deployment and the subsequent stages of force projection operations by—

- Monitoring terrestrial AOIs through ISR assets to help reveal enemy location and disposition, attempting to identify the enemy's intent.
- Providing communications links between forces enroute and in the continental United States (CONUS).
- Permitting MI collection assets to accurately determine their position through the Global Positioning System (GPS).
- Providing timely and accurate data on meteorological, oceanographic, and space environmental factors that might affect operations.
- Providing warning of theater ballistic missile launches.
- Providing timely and accurate weather information to all commanders through the Integrated Meteorological System (IMETS).

1-129. Situation development dominates intelligence operations activities during initial entry operations. The G2/S2 attempts to identify all threats to arriving forces and assists the commander in developing FP measures. During entry operations, echelons above corps (EAC) organizations provide intelligence. This support includes providing access to departmental and joint intelligence and deploying scalable EAC intelligence assets. The entire effort focuses downwardly to provide tailored support to deploying and deployed echelons in response to their CCIRs (PIRs and FFIR).

1-130. Collection and processing capabilities are enhanced, as collection assets build up in the deployment area, with emphasis on the build-up of the in-theater capability required to conduct sustained ISR operations. As the build-up continues, the G2/S2 strives to reduce total dependence on extended split-based intelligence from outside the AO. As assigned collection assets arrive into the theater, the G2/S2 begins to rely on them for tactical intelligence although higher organizations remain a source of intelligence.

1-131. As the ARFOR enter the theater of operations, the joint force J2 implements and, where necessary, modifies the theater intelligence architecture. Deploying intelligence assets establishes liaison with staffs and units already present in the AO. Liaison personnel and basic communications should be in place prior to the scheduled arrival of parent commands. ISR units establish intelligence communications networks.

1-132. CONUS and other relatively secure intelligence bases outside the AO continue to support deployed units. Systems capable of rapid receipt and processing of intelligence from national systems and high capacity, long-haul communications systems are critical to the success of split-based support of a

force projection operation. These systems provide a continuous flow of intelligence to satisfy many operational needs.

1-133. The G2/S2, in coordination with the G3/S3, participates in planning to create conditions for decisive operations. The G2/S2 also adjusts collection activities as combat strength builds. During entry operations the G2/S2—

- Monitors FP indicators.
- Monitors the ISR capability required to conduct sustained intelligence operations.
- Monitors intelligence reporting on threat activity and I&W data.
- Develops measurable criteria to evaluate the results of the intelligence synchronization plan.
- Assesses—
  - Push versus pull requirements of intelligence reach.
  - Effectiveness of the intelligence communications architecture.
  - Reporting procedures and timelines.
  - Intelligence to OPLANs and OPORDs, branches, and sequels (to include planning follow-on forces).

EMPLOYMENT

1-134. Employment is the conduct of operations to support a JFC commander. Employment encompasses an array of operations, including but not limited to—

- Entry operations (opposed or unopposed).
- Shaping operations (lethal and non-lethal).
- Decisive operations (combat or support).
- Postconflict operations (prepare for follow-on missions or redeployment).

Entry Operations

1-135. Enemies often possess the motives and means to interrupt the deployment flow of ARFOR. Threats to deploying forces may include advanced conventional weaponry (air defense, mines, etc.) and WMD. Sea and air ports of debarkation (PODs) should be regarded as enemy HPTs because they are the entry points for forces and equipment. PODs are vulnerable because they are fixed targets with significant machinery and equipment that is vulnerable to attack; in addition to military forces and materiel, HN support personnel, contractors, and civilians may all be working there. An enemy attack, or even the threat of an enemy attack, on a POD can have a major impact on force projection momentum. Commanders at all levels require predictive intelligence so that they may focus attention on security actions that reduce vulnerabilities. To avoid, neutralize, or counter threats to entry operations, the commanders rely on the ability of the G2/S2 to support future operations by accurately identifying enemy reactions to US actions, anticipating their response to our counteractions and predicting additional ECOAs.

1-136. Predictive intelligence also supports the decisions the commander and staff must make about the size, composition, structure, and deployment

sequence of the force in order to create the conditions for success. Commanders rely on predictive intelligence to identify potential friendly decisions before the actual event. While thorough planning develops friendly COAs to meet possible situations, the nature of an operation can change significantly before execution. The G2/S2 must provide timely, accurate, and predictive intelligence to ensure the commander can retain the initiative to implement his plan or his decisions before he loses the opportunity to do so.

Shaping Operations

1-137. Shaping operations create and preserve conditions for the success of the decisive operation. Shaping operations include lethal and non-lethal activities conducted throughout the AO. They support the decisive operation by affecting enemy capabilities and forces, or by influencing enemy decisions. G2/S2 intelligence analysis and ISR activities support the development and execution of shaping operations by identifying threat centers of gravity and decisive points on the battlefield. The G2/S2 also ensures the intelligence process focuses on the CCIRs (PIRs and FFIRs). It is critical that the G2/S2 provide timely, accurate, and predictive intelligence to the commander so that he may execute shaping operations. Predictive intelligence should provide sufficient time for the commander to understand how the enemy will react to US COAs so that appropriate shaping operations can be implemented.

Decisive Operations

1-138. Decisive operations are those that directly accomplish the task assigned by the higher headquarters. Decisive operations conclusively determine the outcome of major operations, battles, and engagements. Continuously synchronized ISR activities, coupled with predictive intelligence results and products during all stages of force projection, combine to ensure the commander is prepared to employ the right forces with the right support to conduct decisive operations at the most appropriate place and time. In addition to coordinating with the G3/S3 to synchronize all ISR activities, the G2/S2 must answer the CCIRs (PIRs and FFIRs) and provide continuous assessments of the enemy's current situation and predict the enemy's subsequent COA, branches, and/or sequels.

Postconflict Operations

1-139. Upon cessation of hostilities or truce, deployed forces enter a new stage of force projection operations. Postconflict operations focus on restoring order, reestablishing HN infrastructure, preparing for redeployment of forces, and planning residual presence of US forces. While postconflict operations strive to transition from conflict to peace, there remains a possibility of resurgent hostilities by individuals and forces. The ISR effort, particularly predictive intelligence analysis, remains just as critical in postconflict operations as in the other employment operations. ISR operations support the postconflict emphasis on restoration operations exemplified by commanders redirecting their CCIRs (PIRs and FFIRs) and IRs to support units conducting these missions. These operations might include—

- Engineer units conducting mine clearing or infrastructure reconstruction operations.

- Medical and logistics units providing humanitarian relief.
- MP units providing law and order assistance.
- CA units reestablishing local control and preparing for the orderly transition of local governments and to support civil-military operations (CMO).

SUSTAINMENT

1-140. Sustainment involves providing and maintaining levels of personnel and materiel required to sustain the operation throughout its duration. It is essential to generating combat power. CSS may be split-based between locations within and outside CONUS. These operations include ensuring units have the MI assets required to accomplish the mission, such as personnel (including linguists), communications systems, ISR systems, and appropriate maintenance support.

REDEPLOYMENT

1-141. Redeployment is the process by which units and materiel reposture themselves in the same theater; transfer forces and materiel to support another JFC's operational requirements; or return personnel and materiel to the home or demobilization station upon completion of the mission. Redeployment operations encompass four phases:

- Recovery, reconstitution, and pre-deployment activities.
- Movement to and activities at the port of embarkation (POE).
- Movement to the POD.
- Movement to homestation.

1-142. As combat power and resources decrease in the AO, FP and I&W become the focus of the commander's intelligence requirements. This in turn drives the selection of those assets that must remain deployed until the end of the operation and those that may redeploy earlier. The S2—

- Monitors intelligence reporting on threat activity and I&W data.
- Continues to conduct intelligence to FP.
- Requests ISR support (theater and national systems) and intelligence in support of redeployment.

1-143. After redeployment, MI personnel and units recover and return to predeployment activities. ISR units resume contingency-oriented peacetime intelligence operations. RC ISR units demobilize and return to peacetime activities. G2/S2s must—

- Monitor intelligence reporting on threat activity and I&W data.
- Update or consolidate databases.
- Maintain intelligence readiness.
- Provide their input into the Force Design Update (FDU) process to refine modified table of organizations and equipment (MTOE) and evaluate the need for Individual Mobilization Augmentee (IMA) personnel.

Chapter 2

Intelligence and Unified Action

UNIFIED ACTION

2-1. As discussed in JP 1-02 and Chapter 1, unified action describes the wide scope of actions (including the synchronization of activities with governmental and NGO agencies) taking place within unified commands, subordinate unified commands, or JTFs under the overall direction of the commanders of those commands. Under unified action, commanders integrate joint, single-service, special, and supporting intelligence operations with interagency, nongovernmental, and multinational operations. The ARFOR often brings unique ISR capabilities to unified action operations.

2-2. In a unified action, the intelligence staff takes on additional responsibilities, relationships, and infrastructure to execute multi-service and multinational intelligence operations. This chapter discusses the synchronization of Army intelligence efforts with joint and other national and international partners to achieve unity of effort and to accomplish the commander's intent.

THE LEVELS OF WAR

2-3. The levels of war are doctrinal perspectives that clarify the links between strategic objectives and tactical actions. Although there are no finite limits or boundaries between them, the three levels of war are strategic, operational, and tactical (see Figure 2-1).

- The strategic level is that level at which a nation, often as one of a group of nations, determines national and multinational security objectives and guidance and develops and uses national resources to accomplish them.
- The operational level is the level at which campaigns and major operations are conducted and sustained to accomplish strategic objectives within theaters or AOs. It links the tactical employment of forces to strategic objectives.
- The tactical level is the employment of units in combat. It includes the ordered arrangement and maneuver of units in relation to each other, the terrain, and the enemy to translate potential combat power into victorious battles and engagements.

2-4. Understanding the interdependent relationship of all three levels of war helps commanders visualize a logical flow of operations, allocate resources, and assign tasks. Actions within the three levels are not associated with a particular command level, unit size, equipment type, or force or component type. The concept of strategic, operational, and tactical intelligence operations aids JFCs and their J2s in visualizing the flow of intelligence from one level to the next. The concept facilitates allocating required collection, analysis, production, and dissemination resources; and facilitates the

assignment of appropriate intelligence tasks to national, theater, component, and supporting intelligence elements.

STRATEGIC

2-5. The President and the Secretary of Defense use strategic intelligence to develop national strategy and policy, monitor the international situation, prepare military plans, determine major weapon systems and force structure requirements, and conduct strategic operations.

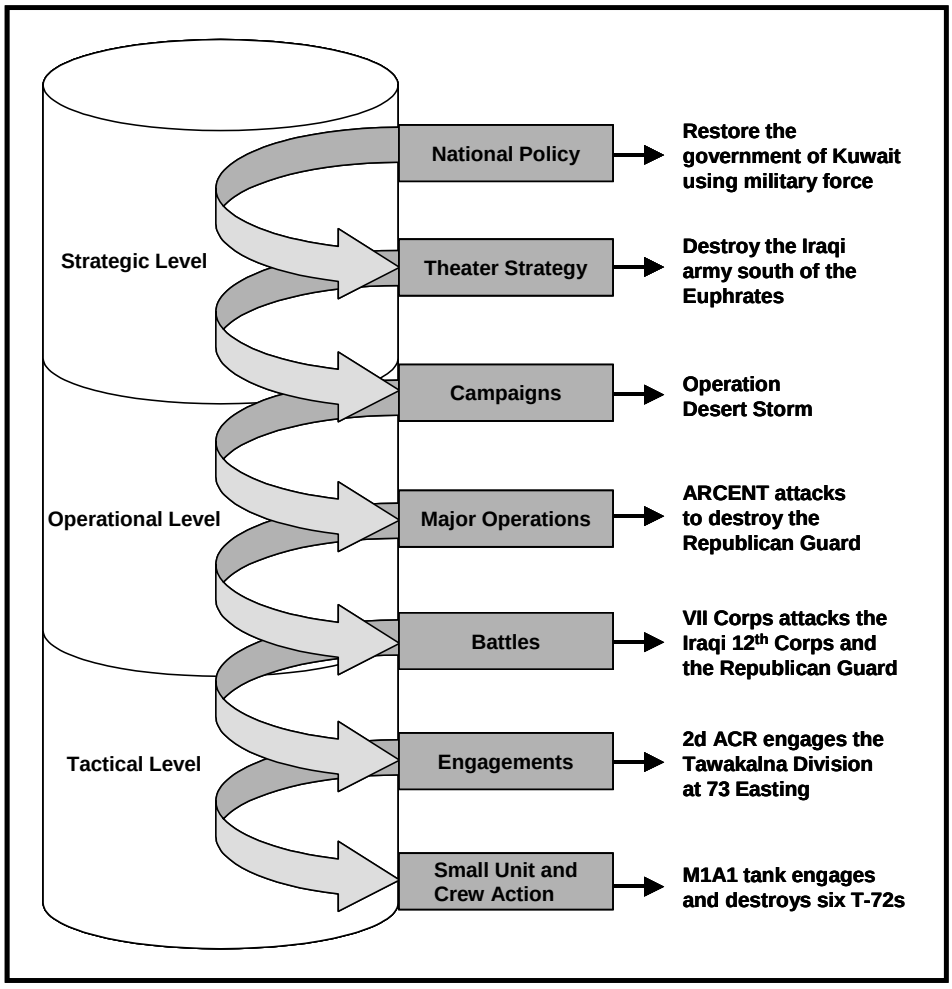


Figure 2-1. The Levels of War.

2-6. Intelligence supports joint operations across the full spectrum of military operations. It determines the current capabilities, and forecasts future developments, of adversaries or potential adversaries that could affect the national security and interests. A strategic operation also produces the intelligence required by combatant commanders to prepare strategic estimates, strategies, and plans to accomplish missions assigned by higher authorities. Theater intelligence includes determining when, where, and in what strength the adversary will stage and conduct theater level campaigns

and strategic unified operations. The intelligence staff should also focus predictive analysis efforts on identifying strategic threat events and how these events will impact US actions at the strategic, operational, and tactical levels. Intelligence operations support IO as well. Intelligence operations support strategic planning by—

- Developing strategic intelligence policy.
- Preparing the strategic collection plan.
- Allocating national intelligence resources.

2-7. Intelligence requirements are those requirements generated from the staff's IRs regarding the enemy and environment that are not a part of the CCIRs (PIRs and FFIRs). Intelligence requirements require collection and can provide answers in order to identify indicators of enemy actions or intent, which reduce the uncertainties associated with an operation. Significant changes (that is, branches and sequels) with an operation usually lead to changes in intelligence requirements. Of particular importance is information relating to enemy or threat strategic vulnerabilities, strategic forces, strategic centers of gravity, and any capabilities relating to the development and employment of CBRNE.

2-8. Global and regional issues and threats are identified and reported to the President and the Secretary of Defense, as well as to the senior military leadership and the combatant commanders. Intelligence requirements include any foreign developments that could threaten the US, its citizens abroad, or multinational military, political, or economic interests. Intelligence also includes identifying hostile reactions to US reconnaissance activities and indications of impending terrorist attacks (I&W). For a complete listing of strategic tasks, refer to CJCSM 3500.04C.

OPERATIONAL

2-9. Combatant commanders and subordinate JFCs and their component commanders are the primary users of intelligence. At the operational echelons, intelligence—

- Focuses on the military capabilities and intentions of enemies and threats.
- Provides analysis of events within the AOI and helps commanders determine when, where, and in what strength the adversary might stage and conduct campaigns and major operations.
- Supports all phases of military operations, from mobilization all the way through redeployment of US forces, and continues during sustainment.
- Supports all aspects of the joint campaign.
- Identifies adversary centers of gravity and HVTs.
- Provides critical support to friendly IO.

2-10. The JFC and staff allocate intelligence resources and request support from national agencies, other theaters, and multinational partners. During stability operations and support operations, operational intelligence includes training and assisting multinational partners in conducting intelligence operations.

2-11. Combatant commanders use intelligence concerning the nature and characteristics of the battlespace to determine the type and scale of operations. Intelligence also aids in determining the impact of significant regional features and hazards on the conduct of both friendly and adversary operations. Significant regional factors include the natural environment, political, informational, economic, industrial, infrastructure, geographic, demographic, topographic, hydrographic, climatic, populace, cultural, medical, lingual, historical, and psychological aspects of the AOI. Intelligence analysis also assists in determining the ROE and other restrictions which will affect operations in the JFC's AO.

2-12. Intelligence relating to the adversary's military and nonmilitary capabilities assists in determining the adversary's ability to conduct military operations. Factors that operational intelligence addresses include mobilization potential, force structure (including alliance forces), force dispositions, equipment, military doctrine, C2 structure, and their MDMP. Intelligence includes the continuous refinement of the OBs for the entire array of the enemy's forces in the AOI. For a complete listing of operational tasks, refer to CJCSM 3500.04C.

US Army Intelligence and Security Command (INSCOM)

2-13. The U.S. Army has vested its intelligence at the operational level with INSCOM, the major Army command (MACOM) responsible for the Army's intelligence forces above Corps. INSCOM's mission is to conduct and support dominant intelligence, security, and information operations for military commanders and national decisionmakers. The INSCOM strategy is to provide superior information and information capabilities to Army commanders, while denying the same to adversaries. Headquarters (HQ), INSCOM, in coordination with its major subordinate commands (MSCs), provides a myriad of general intelligence support operations. INSCOM is providing a globally focused, rapidly deployable, knowledge based, adaptively force packaged capability, supporting commanders and leaders with actionable intelligence at the point of decision. INSCOM serves as the national to tactical Intelligence bridge.

Army Space Program Office (ASPO)

2-14. ASPO executes the Army's Tactical Exploitation of National Capabilities Program (TENCAP). The program focuses on exploiting current and future tactical potential of national systems and integrating the capabilities into the Army's tactical decisionmaking process. Army TENCAP systems enable the tactical commander maximum flexibility to satisfy intelligence needs under a wide range of operational scenarios. ASPO is the point of contact (POC) for all tactical activities between MACOMs or users and the National Reconnaissance Office (NRO).

TACTICAL

2-15. Tactical commanders use intelligence for planning and conducting battles and engagements. Relevant, accurate, predictive, and timely intelligence allows tactical units to achieve an advantage over their adversaries. Precise and predictive intelligence, on the threat and targets, is

essential for mission success. Predictive intelligence also enables the staff to better identify or develop ECOAs. Tactical intelligence—

- Identifies and assesses the enemy's capabilities, COAs, and vulnerabilities, as well as describes the battlespace.
- Seeks to identify when, where, and in what strength the enemy will conduct tactical level operations.
- Provides the commander with information on imminent threats to the force including those from terrorists, saboteurs, insurgents, and foreign intelligence collection.
- Provides critical support to friendly IO.
- Develops and disseminates targeting information and intelligence.

2-16. Intelligence provides the tactical commander with the information and intelligence he requires to successfully employ combat forces against enemy forces. Thus, intelligence tasks support the execution of battles and engagements. These intelligence tasks are different from those at other levels due to their ability to immediately influence the outcome of the tactical commander's mission. They include information gathered from tactical sources, such as combat information, interrogations, debriefings, and eliciting information from captured or misplaced personnel. For a complete listing of tactical tasks, refer to FM 7-15.

CATEGORIES OF INTELLIGENCE

2-17. Directly or indirectly, the unit receives intelligence from throughout the US intelligence community. The intelligence operations and products of national, joint, and service organizations that make up the intelligence community fall into one of six categories:

- I&W.
- Current intelligence.
- GMI.
- Target intelligence.
- S&T intelligence.
- CI.

2-18. The categories of intelligence are distinguishable from each other primarily by the purpose of the intelligence product. The categories can overlap and some of the same intelligence is useful in more than one category. Depending upon the echelon, intelligence organizations use specialized procedures to develop each category of intelligence. The following information describes each category.

INDICATIONS AND WARNINGS

2-19. Indications and warnings (I&W) are those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the US or allied and/or coalition military, political, or economic interests or to US citizens abroad. I&W includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear or non-nuclear attack on the US, its overseas

forces, or alliled and/or coalition nations; hostile reactions to US reconnaissance activities; terrorist attacks; and other similar events. (JP 3-13). I&W comes from time-sensitive information and analysis of developments that could involve a threat to the US and multinational military forces, US political or economic interests, or to US citizens. While the G2/S2 is primarily responsible for producing I&W intelligence, each element, such as the MPs conducting PIO, within every unit contributes to I&W through awareness of the CCIRs and reporting related information.

CURRENT INTELLIGENCE

2-20. Current intelligence involves the integration of time-sensitive, all-source intelligence and information into concise, accurate, and objective reporting on the battlespace and current enemy situation. One of the most important forms of current intelligence is the enemy situation portion of the COP. The G2/S2 is responsible for producing current intelligence for the unit. Current intelligence supports ongoing operations across full spectrum operations. In addition to the current situation, current intelligence should provide projections of the enemy's anticipated situations (estimates) and their implications on the friendly operation.

GENERAL MILITARY INTELLIGENCE

2-21. GMI is intelligence concerning military capabilities of foreign countries or organizations or topics affecting potential US or multinational military operations relating to armed forces capabilities, including OB, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness and area and terrain intelligence. This broad category of intelligence is normally associated with long-term planning at the national level. However, GMI is also an essential tool for the intelligence staff and should be in place long before the start of preparations for a particular military operation. An up-to-date, comprehensive intelligence database is critical to the unit's ability to plan and prepare rapidly for the range of operations and global environments in which it may operate. GMI supports the requirement to quickly respond to differing crisis situations with corresponding intelligence spanning the globe. One of the many places to get information for GMI is the medical intelligence database. The G2/S2 planner develops his initial IPB from GMI products.

2-22. The G2/S2 develops and maintains the unit's GMI database on potential threat forces and environments based on the commander's guidance. As an essential component of intelligence readiness, this database supports the unit's planning, preparation, execution, and assessment of operations. The G2/S2 applies and updates the database as it executes its intelligence production tasks.

TARGET INTELLIGENCE

2-23. Target intelligence is the analysis of enemy units, dispositions, facilities, and systems to identify and nominate specific assets or vulnerabilities for attack, re-attack, or exploitation (for intelligence). It consists of two mutually supporting production tasks: target development and combat assessment.

- **Target development** is the systematic evaluation and analysis of target systems, system components, and component elements to determine HVTs for potential attack through maneuver, fires, or non-lethal means.
- Once attacked, **combat assessment** provides a timely and accurate estimate of the affects of the application of military force (lethal or non-lethal) an IO on targets and target systems based on predetermined objectives.

SCIENTIFIC AND TECHNICAL INTELLIGENCE

2-24. Scientific and technical intelligence (S&TI) is the product resulting from the collection, evaluation, analysis, and interpretation of foreign S&T information which covers foreign developments in basic and applied research and in applied engineering techniques and S&T characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the research and development (R&D) related thereto, and the production methods employed for their manufacture.

2-25. S&T intelligence concerns foreign developments in basic and applied sciences and technologies with warfare potential. It includes characteristics, capabilities, vulnerabilities, and limitations of all weapon systems, subsystems, and associated materiel, as well as related R&D. S&T intelligence also addresses overall weapon systems and equipment effectiveness. Specialized organizations—such as the Defense Intelligence Agency (DIA) Missile and Space Intelligence Center (MSIC), INSCOM, Air Missile Defense (AMD), Area Air and Missile Defense Command (AAMDC), and National Ground Intelligence Center (NGIC)—produce this category of intelligence. The G2/S2 establishes instructions within SOPs, orders, and plans for handling and evacuating captured enemy materiel (CEM) for S&T intelligence (S&TI) exploitation.

COUNTERINTELLIGENCE

2-26. As previously defined at the end of Chapter 1, CI attempts to identify and recommend countermeasures to the threat posed by foreign intelligence security services (FISS) and the ISR activities of non-state entities such as organized crime, terrorist groups, and drug traffickers. CI analysis incorporates information from all sources as well as the results of CI collection, investigations, and operations to analyze the multidiscipline threat posed by foreign intelligence services and activities.

INTELLIGENCE COMMUNITY

2-27. There are many organizations in the intelligence community that support military operations by providing specific intelligence products and services. The J2/G2/S2 and his staff must be familiar with these organizations and the methods of obtaining information from them as necessary. Figure 2-2 shows organizations that compose the intelligence community.

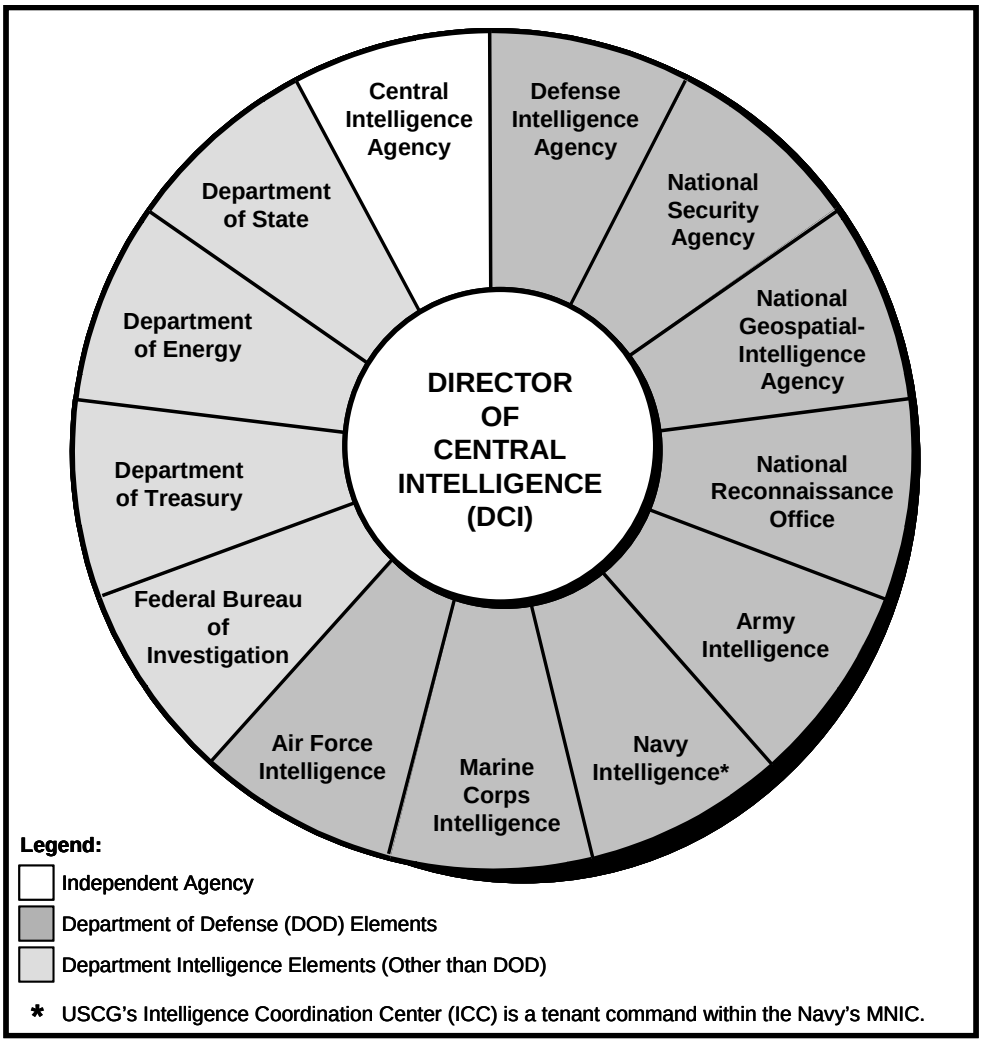


Figure 2-2. Intelligence Community Membership.

DOD AGENCIES

Defense Intelligence Agency (DIA)

2-28. DIA is a combat support agency and a major collector and producer in the defense intelligence community. The DIA supports the full spectrum of operations to include basic MI, counterterrorism, counterdrugs, medical intelligence, WMD and proliferation, United Nations (UN) peacekeeping and multinational support, missile and space intelligence, noncombatant evacuation operations (NEOs), targeting, combat assessment, and battle damage assessment (BDA).

National Security Agency (NSA)

2-29. NSA ensures cryptologic planning and support for joint operations. Working with the tactical cryptologic units of a command, the NSA provides SIGINT and information security (INFOSEC), encompassing communications security (COMSEC) and computer security, as well as telecommunications

support and operations security (OPSEC). The people and equipment providing SIGINT, INFOSEC, and OPSEC constitute the United States Cryptologic System (USCS). The NSA, through the USCS, fulfills cryptologic command and/or management, readiness, and operational responsibilities in support of military operations according to the Secretary of Defense tasking, priorities, and standards of timeliness.

National Geospatial-Intelligence Agency (NGA)

2-30. The NGA (formerly National Imagery and Mapping Agency [(NIMA)] mission is to provide timely, relevant, and accurate intelligence and geospatial information in support of national security objectives of the United States. The Director of NGA advises the Secretary of Defense, Director Central Intelligence (DCI), Chairman of the Joint Chiefs of Staff (JCS), and the combatant commanders on imagery, IMINT, and geospatial information. The Operations Directorate, Customer Support Office, is the focal point for interface with external customers, including the JCS, combatant commands, services, and national and defense agencies.

National Reconnaissance Office (NRO)

2-31. The NRO develops and operates unique and innovative space reconnaissance systems and conducts intelligence-related activities essential for US security. The role of the NRO is to enhance US government and military information superiority across full spectrum operations. NRO responsibilities include supporting I&W, monitoring arms control agreements, and performing crisis support to the planning and conduct of military operations. The NRO accomplishes its mission by building and operating IMINT and SIGINT reconnaissance satellites and associated communications systems

US Navy (USN)

2-32. Naval intelligence products and services support the operating naval forces, the Department of the Navy, and the maritime intelligence requirements of national level agencies. Naval intelligence operates the National Maritime Intelligence Center (NMIC). Naval intelligence responsibilities include maritime intelligence on global merchant affairs, counter-narcotics, fishing issues, ocean dumping of radioactive waste, technology transfer, counter-proliferation, cryptologic related functions, CI, I&W support, management of Coast Guard collection, and development of new weapons systems and countermeasures.

US Marine Corps (USMC)

2-33. USMC intelligence provides pre-deployment training and force contingency planning for requirements that are not satisfied by theater, other service, or national capabilities. The Marine Corps Intelligence Agency (MCIA) handles the integration, development, and application of GMI, technical information, all-source production, and open-source information.

US Air Force (USAF)

2-34. USAF ISR assets fill a variety of roles to meet US national security requirements. The USAF operates worldwide ground sites and an array of

airborne ISR platforms to meet national level intelligence requirements. To support day-to-day USAF operations and to meet specific USAF requirements, intelligence professionals at the wing and squadron levels use suites of interoperable analysis tools and dissemination systems to tailor information received from all levels and agencies in the intelligence community. USAF responsibilities include all-source information on aerospace systems and potential adversaries' capabilities and intentions, cryptologic operations, I&W, IO, and criminal investigative and CI services.

NON-DOD AGENCIES

2-35. Although the primary focus of non-DOD members of the intelligence community is strategic intelligence and support to the President and the Secretary of Defense, these agencies also produce intelligence and intelligence products that support operational and tactical ARFOR. This responsibility includes assessing potential issues and situations that could impact US national security interests and objectives. These agencies identify global and regional issues and threats. Some of the intelligence products and services these agencies provide are essential to accurate assessment of the threat and battlespace, particularly during stability operations and support operations.

Central Intelligence Agency (CIA)

2-36. The CIA's primary areas of expertise are in HUMINT collection, imagery, all-source analysis, and the production of political and economic intelligence. CIA and military personnel staff the CIA's Office of Military Affairs (OMA). As the CIA's single POC for military support, OMA negotiates, coordinates, manages, and monitors all aspects of agency support for military operations. This support is a continuous process, which the agency enhances or modifies to respond to a crisis or developing operation. Interaction between OMA and the DCI representatives to the Office of the Secretary of Defense (OSD), the Joint Staff, and the combatant commands facilitates providing national level intelligence in support of joint operations, contingency and operations planning, and exercises.

Department of State, Bureau of Intelligence and Research

2-37. The Bureau of Intelligence and Research coordinates programs for intelligence, analysis, and research; it produces intelligence studies and current intelligence analyses essential to foreign policy determination and execution. Its subordinate Bureau of International Narcotics Matters develops, coordinates, and implements international narcotics control assistance activities. It is the principal POC and provides policy advice on international narcotics control matters for the Office of Management and Budget (OMB), the NSC, and the White House Office of National Drug Control Policy (ONDCP). The Bureau also oversees and coordinates the international narcotics control policies, programs, and activities of US agencies.

Department of Energy, Office of Nonproliferation and National Security

2-38. The Department of Energy's Office of Nonproliferation and National Security assists in the development of the State Department's policy, plans,

and procedures relating to arms control, nonproliferation, export controls, and safeguard activities. Additionally, this office is responsible for—

- Managing the department's R&D program.
- Verifying and monitoring arms implementation and compliance activities.
- Providing threat assessments and support to headquarters and field offices.

Department of the Treasury

2-39. The US Treasury Department's intelligence-related missions include producing and disseminating foreign intelligence relating to US economic policy and participating with the Department of State in the overt collection of general foreign economic information.

Federal Bureau of Investigation (FBI)

2-40. The FBI is the principal investigative arm of the Department of Justice (DOJ) and has primary responsibility for CI and counterterrorism operations conducted in the US. CI operations contemplated by any other organizations in the US must be coordinated with the FBI. Any overseas CI operation conducted by the FBI must be coordinated with the CIA.

Department of Homeland Security

2-41. The mission of the Department of Homeland Security is to develop and coordinate the implementation of a comprehensive national strategy to secure the US from terrorist threats or attacks. The organizational construct of homeland security mission is a framework of prepare, deter, preempt, defend, and respond. Component agencies will analyze threats and intelligence, guard our borders and airports, protect our critical infrastructure, and coordinate the response of our nation for future emergencies. The component agencies of the department include—

- US Coast Guard (USCG).
- US Customs Service.
- US Border Patrol.
- Federal Emergency Management Agency (FEMA).
- Immigration and Naturalization Service (INS).
- Transportation Security Administration.
- Federal Protective Service.
- Office of Domestic Preparedness.

United States Coast Guard (USCG)

2-42. The USCG, subordinate to the Department of Homeland Security, has unique missions and responsibilities as both an armed force and a law enforcement agency (LEA), which makes it a significant player in several national security issues. The USCG intelligence program supports counter-drug operations, mass seaborne migration operations, alien migration interdiction operations, living marine resource enforcement, maritime intercept operations, port status and/or safety, counterterrorism, coastal and

harbor defense operations, and marine safety and/or environmental protection.

Other Agencies

2-43. There are a number of US Government agencies and organizations, not members of the intelligence community, that are responsible for collecting and maintaining information and statistics related to foreign governments and international affairs. Organizations such as the Library of Congress, the Departments of Agriculture and Commerce, the National Technical Information Center, US Information Agency, US Information Service, and the US Patent Office are potential sources of specialized information on political, economic, and military-related topics. The intelligence community may draw on these organizations to support and enhance research and analysis and to provide relevant information and intelligence for planners and decisionmakers. Many other US Government agencies may become directly involved in supporting DOD especially during stability operations and support operations. (See JP 2-02 for a description of agency support to joint operations and intelligence.) These organizations include—

- Department of Transportation.
- Disaster Assistance Response Team within the Office of Foreign Disaster.
- US Agency for International Development.
- NGA.

UNIFIED ACTION INTELLIGENCE OPERATIONS

2-44. In unified action, ARFOR synchronize their actions with those of other participants to achieve unity of effort and to accomplish the combatant commander's objectives. Unified action links subordinates to the combatant commander under combatant command (command authority) (COCOM). Multinational, interagency, and nonmilitary forces work with the combatant commander through cooperation and coordination. Combatant commanders form theater strategies and campaigns, organize joint forces, designate operational areas, and provide strategic guidance and operational focus to subordinates. The aim is to achieve unity of effort among many diverse agencies in a complex environment. Subordinate JFCs synchronize joint operations in time and space, direct the action of foreign military forces (multinational operations), and coordinate with governmental and NGOs (interagency coordination) to achieve the same goal.

2-45. The J2 staff provides intelligence promptly, in an appropriate form, and by any suitable means to those who need it. Intelligence personnel ensure that the consumers understand the intelligence and assist them as they apply the intelligence to their operations.

2-46. Dissemination requires establishing appropriate communications systems and procedures. The J2 and other intelligence personnel must fully participate in all operation planning and execution, and develop close working relationships with the JFC and other staff elements.

2-47. The commander and staff assess intelligence operations to determine their effectiveness and to make any necessary improvements. The intelligence process functions presented in Chapter 4 provide the criteria for evaluating intelligence operations.

JOINT INTELLIGENCE OPERATIONS

2-48. The JTF commanders and his intelligence staff must—

- Understand the intelligence requirements of superior, subordinate, and component commands.
- Identify organic intelligence capabilities and shortfalls.
- Access theater and national systems to ensure appropriate intelligence and CI products are available to the JTF.

2-49. The JTF's intelligence effort focuses on integrating multi-source information and multi-echelon intelligence into all-source intelligence products that provide clear, relevant, and timely knowledge of the enemy and battlespace. These products must be in formats that are readily understood and directly usable by the recipient in a timely manner. They must neither overload the user nor the communications architecture.

2-50. The J2 is the JTF commander's focal point for intelligence. The J2 directly supports the JFC's responsibilities for determining objectives, directing operations, and evaluating the effects of those operations. The J2 supports the execution of the plan with the intelligence needed to sustain the operation, attain joint force objectives, provide support to subordinate commands, and continually support FP efforts. The J2 analyzes the potential threat situation and provides assessments to support friendly opportunities. The J2 then supports the execution of the plan with the operational intelligence needed to sustain the operations, attain joint force objectives, and support FP. To maintain the initiative, the JFC will seek to get inside the adversary's decisionmaking cycle; that is, the JFC will seek to develop procedures and an organization in order to receive new and accurate intelligence and respond to the new situation faster than the adversary. The J2 must help in identifying the adversary's decisionmaking cycle and identifying vulnerabilities that may be exploited. The J2 also—

- Ensures the provision of the required ISR support to the JTF and its subordinate functional and service components.
- Assists the JTF commander in defining intelligence responsibilities and PIRs.
- Actively participates in joint staff planning and in planning, preparing, executing, and assessing ISR efforts. This includes leading the JTF's joint collection board and providing representation at the joint targeting board.

2-51. Figure 2-3 shows a typical JTF J2 organization. The overall organization of the JTF and operations will dictate actual composition of the J2. At a minimum, a core element of analytical, ISR management, and administrative capabilities is required.

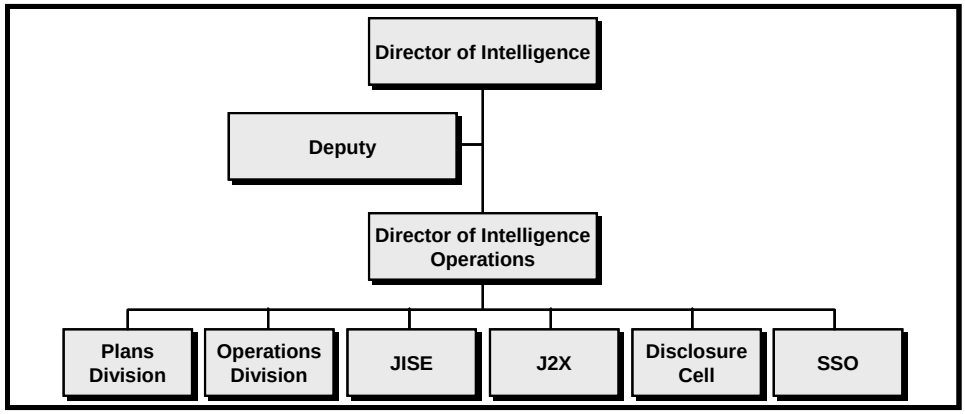


Figure 2-3. Typical Joint Task Force J2 Organization.

Considerations In Joint Intelligence Operations

2-52. The Army, Air Force, Navy, Marine Corps, and SOF must provide globally responsive assets to support the combatant commanders' theater strategies and the national security strategy. The capabilities of the other armed forces complement those of ARFOR. During joint operations, they provide support consistent with JFC-directed missions. When conducting joint intelligence operations, there are a number of unique problems that can arise due to the complexity of integrating the efforts of the different services and commands. Elements affecting joint intelligence operations among the different services include the following:

- Intelligence liaison is critical to the success of intelligence operations and requires early establishment, particularly between units that have not routinely trained together and possess differing capabilities. As a minimum, organizations exchange liaison teams with the higher echelon organization. Additional liaison may be necessary to facilitate joint force collection, production, or dissemination requirements. Liaison teams—
  - Support planning and C2 of intelligence operations.
  - Ensure timely two-way flow of intelligence between commands.
  - Manage intelligence and resource requirements of the subordinate command.
  - Advise the commander on service ISR capabilities, limitations, and employment.
- Commanders and staffs use IPB to understand the battlespace and develop or refine plans and orders. IPB products exchanged between echelons ensure a common picture of the battlespace and estimate of the situation.
- Communications considerations for joint operations include—
  - Planning for intelligence communications transition to facilitate execution of branches or sequels to the plan or to accommodate shifting of the main effort from one force to another.

  - Identifying the initial communications architecture to include establishing procedures and protocols for information exchanges (databases, text, imagery, voice, and video).
  - Balancing the availability of service-unique intelligence systems between echelons or services. This may require each service providing additional resources. The senior commander is responsible for allocating resources.
  - Disseminating intelligence between commands and services. Additional communications equipment, intelligence terminals, and personnel may be required to balance capabilities between services.
- Identifying the databases each service possesses or has access to; determining which databases will support the operation and, if necessary, merge them into a single database; and ensure access by the entire force.
- Providing a focal point for subordinate command access to national or joint intelligence is essential. The senior commander will request and allocate resources required to support this access.

2-53. The JFC's intelligence requirements, concept of operation, and intent drive the ISR effort. The different organizations and services participating in joint intelligence operations must continuously share information, intelligence, and products to satisfy requirements. See FM 2-01 for details on intelligence requirements and RM. Activities required to facilitate an effective joint collection effort include—

- Coordinating intelligence and ISR operations to optimize capabilities of collection assets and reduce duplication of effort.
- Integrating supporting national and theater intelligence collection assets into the intelligence synchronization plan.
- Establishing procedures for tracking and handing off HPTs between services and echelons.
- Establishing procedures for cueing Army and other service collection assets.
- Coordinating airspace for ISR assets.
- Maximizing available linguist capabilities. Shortages of military linguists trained in target languages may require cross-leveling Army and other service linguists.

2-54. Reporting and intelligence production considerations in joint operations include—

- Establishing production criteria and thresholds that produce timely and relevant intelligence keyed to the commander's intelligence and targeting requirements. The ISM, attack guidance matrix (AGM), and HPT list are examples of tools used to support joint intelligence and targeting efforts. The sharing of these products to all echelons and services is crucial.
- Establishing common methodology and criteria for producing the BDA and supporting the combat assessment function.
- Establishing set standards for the number and frequency of periodic reports such as intelligence summaries (INTSUMs).

Joint Intelligence Architecture

2-55. In addition to the J2 staffs at every joint level of command, the key organizations in the joint intelligence architecture are the National Military Joint Intelligence Center (NMJIC) (see Figure 2-4), the Joint Intelligence Centers (JICs) or Joint Analysis Centers (JACs) of the unified commands, and, when formed, the JTF's joint intelligence support element (JISE). Working together, these organizations play the primary role in managing and controlling joint intelligence operations. The formal relationships which link these organizations facilitate information management and optimize complementary intelligence functions by echelon without obstructing the timely flow of intelligence up, down, or laterally.

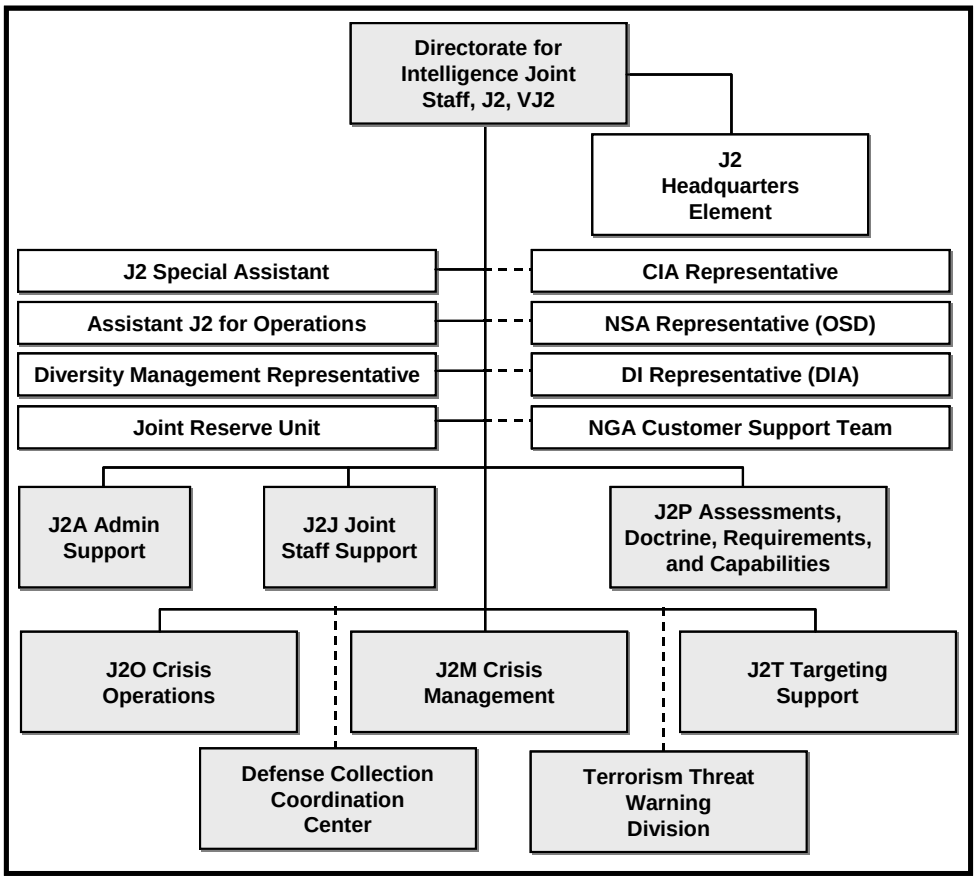


Figure 2-4. National Military Joint Intelligence Center.

2-56. The NMJIC is the focal point for intelligence activities in support of joint operations. The NMJIC is the CJCS J2 intelligence watch within the National Military Command Center (NMCC) in the Pentagon. When the assigned or attached assets cannot satisfy the combatant commander and the JTF commander's crisis-related and time-sensitive intelligence requirements, the NMJIC, as part of the J2's staff, sends tasks to appropriate agencies to fill the requirements. During crises, the NMJIC expands as necessary to establish a working group, intelligence task force, or an expanded intelligence task force. The NMJIC participates in targeting by developing national level

target lists. When requested, the NMJIC supports the theater in performing BDA. Besides supporting the combatant commands and JTFs, the NMJIC supports any multinational partners and prescribed international organizations.

2-57. The JIC is organized in accordance with the combatant commander's prerogatives, but normally performs the general functions described in JP 2-0 and specific unified command intelligence TTP. The JIC is responsible for providing intelligence to JTF and its subordinates during military operations. If the JIC cannot meet the combatant commander's requirements, the JIC forwards requests to the NMJIC or to subordinate command levels through established channels, using standard command procedures. In some cases, the JIC may also ensure timely support by approving a direct communication path, in advance, between requesters such as the JTF JISE and outside producers. In this case, the parties must inform the JIC of all requests as they occur. This method is most appropriate when the parties require products and services, which the JIC does not routinely produce.

2-58. At the discretion of the JTF commander, the J2 can establish a JISE during the crisis or preparation stage for operations to augment the J2 staff. The JISE is a tailored subset of the JIC or the intelligence organization of the service component designated as the JTF headquarters.

2-59. Under the direction of the J2, the JISE normally manages the intelligence collection, production, and dissemination for the JTF. The JISE provides intelligence to JTF operational forces and performs common intelligence functions. By design, the JISE is scaleable and can expand to meet the needs of the JTF and the operating environment. It is composed of analytical experts, analysis teams, and ISR managers that provide services and products, which the JTF, JTF staff, and subordinate components require. These experts, mentioned above, focus on solving the operational intelligence problems of concern to the JTF commander. The JISE's capability to perform all-source analysis and ISR synchronization is key to producing operational intelligence that is timely, relevant, and complete. Figure 2-5 illustrates the features of a typical JISE.

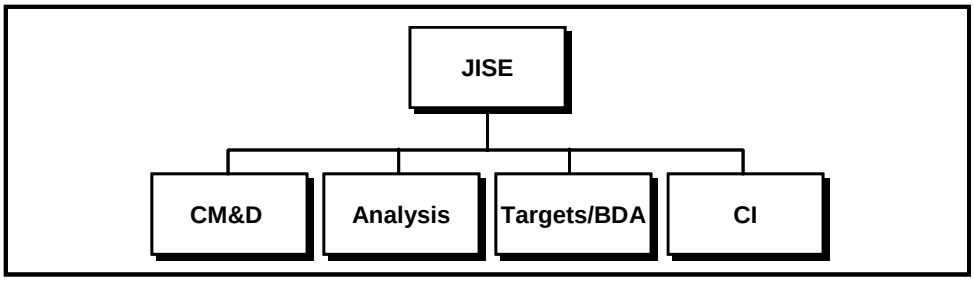


Figure 2-5. Typical Joint Intelligence Support Element.

Joint Task Force Intelligence Organizations

2-60. In addition to the JISE, the JTF commander and J2 may require other supporting JICs or teams based on projected operations. The JTF commander may make a request to the NMJIC for specific national intelligence agency capabilities. The NMJIC evaluates and coordinates the JTF commander's requirements with the J3, J5, and national intelligence agencies and tailors

the composition of the deployment packages to meet those needs. The deployment packages, such as the National Intelligence Support Team (NIST), provide access to the entire range of capabilities resident in the national intelligence agencies and can focus those capabilities on the JTF commander's intelligence requirements. The J2X manages and coordinates the HUMINT and CI activities of national, theater, and service components operating within the JTF's JOA. The Joint Captured Materiel Exploitation Center (JCMEC) assists in management of recovery, exploitation, and disposal of captured enemy equipment (CEE). The JTF commander's requirements dictate the composition and tailoring of such deployment packages.

Augmentation Considerations

2-61. Depending on the scale of the operations, the intelligence organizations described above and those of the JTF's subordinate command may require personnel augmentation. Optimum use of available intelligence assets is essential to ensure quality support in meeting the JTF commander's requirements.

2-62. The demand for additional intelligence increases significantly during crisis and wartime operations. As the need arises for more intelligence personnel, the intelligence presence also increases at all command levels. Locating additional intelligence personnel and knowing how to integrate those personnel into the operation is vital. The JTF J2 should identify intelligence personnel augmentation requirements in accordance with the Chairman, Joint Chiefs of Staff (CJCS) Instruction 1301.01. The combatant commander's joint table of mobilization and distribution (JTMD) also contains the standing augmentation requirements. The JTMD should reflect the need for either IMA or Individual Ready Reserve (IRR) personnel. The combatant commander and the JTF refine personnel requirements and initiate requests when they anticipate or start an operation.

2-63. A consideration for the JTF when requesting support or augmentation is that these national level teams and individual augmentees are not totally self-contained elements; rather they require logistic, information, and other support from the supported command. Each deployment is unique based on mission, duration, team composition, and capabilities required. A full NIST, for example, requires a private, access-controlled area within a sensitive compartmented information facility (SCIF) work environment and dedicated secure communications.

2-64. For more information on intelligence operations as they apply to other armed services, see the individual service intelligence doctrine. See also JP 2-0 series, JP 3-0, JP 3-55, and JP 5-0 for more details on joint intelligence operations and considerations.

Multinational Intelligence

2-65. Multinational intelligence operations take place within the structure of an alliance or coalition. Some multinational military organizations, such as the North Atlantic Treaty Organization (NATO) and the UN Command in the Republic of Korea (ROK), are highly structured and enduring. Others, such as the coalition formed during the Gulf War, are less formal and temporary.

2-66. In multinational operations, the multinational force commander (MNFC) exercises command authority over a military force composed of elements from two or more nations. Therefore, in most multinational operations, the JTF must share intelligence, as necessary, for mission accomplishment with foreign military forces and coordinate exchange of intelligence with those forces.

2-67. In some circumstances, the JTF may need to seek authority to go outside the usual political-military channels to provide information to NGOs. The JTF must tailor intelligence policy and dissemination criteria to each multinational operation.

INTELLIGENCE REACH

2-68. Military forces use intelligence reach to rapidly access information, receive support, and conduct collaboration and information sharing with other units and organizations unconstrained by geographic proximity, echelon, or command.

2-69. Intelligence reach supports minimizing the deployed footprint of ISR assets. By providing enhanced information and tailored intelligence products, intelligence reach can greatly enhance the intelligence capabilities of the unit and play a significant role in improving the commander's ability to make decisions on the battlefield. It allows the commander to harness national, joint, foreign, and other military organization resources. Table 2-1 shows examples of partners and sources for intelligence reach.

2-70. Detailed planning and training are critical to the success of intelligence reach operations. The following are steps that the staff can take to ensure optimal use, operability, and effectiveness of intelligence reach:

- Establish data exchange methods and procedures.
- Establish electronic message transfer procedures.
- Establish homepages for identified forces.
- Establish POCs for I&W centers, production centers, Theater JICs, DIA, INSCOM, and their major subordinate commands such as NGIC and the theater intelligence brigades and groups.
- Ensure the intelligence staff has the necessary personnel, training, automated systems, bandwidth, and resources to conduct intelligence reach.
- Determine IRs through staff planning. Develop production requirements for identified intelligence gaps.
- Order geospatial products for the projected joint AOI.
- Establish and maintain a comprehensive directory of intelligence reach resources before deployment and throughout operations. The value of intelligence reach will greatly increase as the staff develops and maintains ready access to rich information resources. These resources are numerous and may include, for example, Army, Joint, DOD, non-DOD, national, commercial, foreign, and university research programs. Know what types of information the resources can provide. Continuously expand the resource directory through identification of new resources.

- Use intelligence reach first to fill intelligence gaps and requirements and answer RFIs. This technique can preclude unnecessary tasking or risk to limited ISR assets.
- Maintain continuous situational understanding and anticipate intelligence requirements. Use intelligence reach to fulfill these requirements and provide the results to the commander and staff for planning and decisionmaking.
- Exchange intelligence reach strategies with other units.
- Present the information retrieved through intelligence reach in a usable form. Share the information derived from intelligence reach with subordinate, lateral, and higher echelons. Ensure follow-on forces have all information as well.

Table 2-1. Examples of Intelligence and Reach Partners and Sources.

ARMY	SERVICES	JOINT	DOD
ACE ISE TSE (TIB/TIG) 902d NGIC ATCAE ARISCs	ONI NMIC AIA NAIC MCIA	USEUCOM JAC USSOUTHCOM JIC USSOCOM JIC USSPACECOM CIC USJFCOM AIC USCENTCOM JIC USTRANSCOM JIC USSTRATCOM USPACOM JIC USNORTHCOM JIC	DIA CMO MSIC AFMIC DHS NGA NSA RSOCs
NON-DOD	**NATIONAL**	**COMMERICAL**	**FOREIGN**
DOE FBI DOS DEA FEMA INS	DCI NIC CIA NRO INR DOT, Office of Intel Support	RAND Jane's Defence Weekly Economic Intelligence Unit CNN Reuters Associated Press United Press International	DIS NFHQ DIO

INTELLIGENCE REACH COMPONENTS

2-71. Intelligence reach requires the G2/S2 to develop a strategy on how best to support the unit's mission with intelligence reach capabilities. There are six basic components of the strategy:

- Push
- Database Access.
- Pull.
- Broadcast Services.
- Collaborative Tools.
- Requirements Management.

Push

2-72. Push occurs when the producers of intelligence or information are knowledgeable of the customer's requirements and are able to send the desired intelligence to the customer without further requests. Push is accomplished through the most appropriate or efficient dissemination means. Unless coordinated as an acceptable dissemination method, push is not accomplished solely by posting intelligence products on a web page. The entity that posts the document must ensure the intended recipient is aware of the product's location or has received the product.

2-73. Push begins with the statement of intelligence interest (SII). The SII establishes the unit's intelligence and IRs. The SII is prepared by intelligence staff organizations to register their interest in receiving recurring hardcopy and softcopy reports, studies, and publications covering a wide variety of intelligence subjects. The J2/G2/S2 works with the Department of the Army Production and Dissemination Management (DAPDM) to establish a profile for information transfer. Intelligence reports or information meeting the unit's requirements are then automatically sent directly to the unit's classified or unclassified networks or communication systems.

2-74. Organizations that push information and data down to subordinate units must be careful of the amount, detail, and focus of the information they are sending. Too much information will overwhelm the subordinate unit. Crucial information may be lost in the midst of an overabundant flow of information, much of which is of little use. Intelligence reach often runs more efficiently if the user pulls the information or at least focuses the intelligence producers to send the appropriate information with the correct level of detail at the appropriate time.

Database Access

2-75. Access to local, theater, DOD, non-DOD, and commercial databases allows analysts to leverage stored knowledge on topics ranging from basic demographics to OB information. A validated DIA Customer Number (acquired by the J2/G2/S2) in combination with Secret Internet Protocol Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS) connectivity establishes access to most of the databases online. The challenge for an analyst is to gain an understanding of the structure, contents, strengths, and weaknesses of the database regardless of database type. Additionally, the procedures are often difficult for extracting portions or downloading and transferring the database to unit level automated information systems.

2-76. Each intelligence discipline has unique databases established and maintained by a variety of agencies. Database access is accomplished through unit or agency homepages via SIPRNET (Intelink-S) and JWICS (Intelink). The DAPDM office, upon approving the unit's SII, validates the requirement for access to the majority of these databases. Units coordinate with the DA dissemination and program manager (DPM) and/or the agency for access to those databases requiring passwords and permissions beyond normal Intelink-S and Intelink access.

Pull

2-77. Pull occurs when the requestor is familiar enough with existing databases and products to be able to anticipate the location of the desired information. Knowledge of both the types and locations of intelligence databases can greatly increase the efficiency of the Intelligence BOS by saving time and effort on the part of analysts at every echelon.

2-78. The G2/S2 must also ensure that intelligence reach capability extends to multinational forces, augmentees, and other services or organizations working as part of the JTF. The G2/S2 must forward relevant intelligence to units which do not possess the necessary automation to conduct intelligence reach.

Broadcast Services

2-79. Broadcast services are an integrated, interactive dissemination system, focusing on tactical user's IRs using joint message formats. The theater broadcast's data prioritization and processing occur through information management. Selected tactical, theater, DOD, and national collectors broadcast their messages using prescribed message formats. The analyst decides which types of messages are required. Broadcast service data is responsive to the operational commander's information needs and allows tactical users to construct successively detailed pictures of the battlespace.

2-80. Tactical users require intelligence and information to be available at the lowest classification level possible (for example, collateral SECRET) and releasable, as necessary, to multinational partners. Broadcast service information management will adhere to national policy as it relates to the provision of data to NATO or multinational partners.

Collaborative Tools

2-81. Collaboration is the sharing of knowledge, expertise, and information, normally online, and may take numerous forms. Collaborative tools are computer-based tools (groupware) that help individuals work together and share information. They allow for virtual online meetings and data sharing. As an example of the use of collaborative tools, the President or the Secretary of Defense and DOD during a crisis situation will establish a number of crisis action teams (CATs) or joint interagency working groups (JIAWGs). These groups or teams are formed to address specified subjects or topics in support of the warfighter or decisionmaker. The groups will focus on the crisis and normally publish their products on a homepage. Analysts with online access can participate in a number of ways. This includes passively accessing the homepages to study the products, sending queries to the identified POCs, or by having their organization join the CAT or JIAWG. Table 2-2 shows some examples of collaborative tools.

Requirements Management

2-82. The RM system provides a mechanism for submitting RFIs, tasking, and managing ISR assets. Analysts who are trained and familiar with the RM process and the various tasking procedures can leverage its systems for refined information. Each intelligence discipline has established procedures

for requesting specific information. It is therefore advantageous to have someone familiar with each discipline's procedures to participate in synchronizing the ISR effort. For example, an analyst receives a HUMINT-based intelligence information report, which provides information on an event or subject. If he requires more refined data or clarification, he should submit a time-sensitive requirement or a source-directed requirement. This creates a two-way communication from the field to the collectors without creating additional standing requirements. The more familiar the analyst is with the RM process, the better he can leverage it.

2-83. The intelligence reach component of RM includes the ability of an intelligence officer at any level to request information, which is beyond what is available at his location. The normal procedure for obtaining intelligence or information not obtainable through the use of available ISR assets is to submit an RFI to the next higher echelon. Users enter RFIs into the RM system. See ST 2-33.5 for more information on intelligence reach operations and FM 2-01 for more information on RM.

Table 2-2. Examples of Collaborative Tools.

Tool	Description
Chat (Audio and Text)	Used to conduct conversations online.
Whiteboard	Permits real-time display of drawings, pictures, or documents for group discussion and comment. Participants can annotate in real time as well.
Bulletin Board	Used to post notices and facilitate discussions on any topic.
Video	Used at a desktop computer or a video teleconferencing (VTC) center to allow the person or group to see with whom they are communicating.
Discussion Groups (Newsgroups)	Topics are posted to a website for discussion and comment where participants can follow a line of discussion on a topic.
File-Sharing Tools	Virtual file cabinets allow information to be stored on web servers, and are available to anyone having access to the site and electronic permission to use the files.
Presentation Tools	Used in a virtual auditorium to allow lectures and briefings to be given to an audience.
Application Sharing	An entire team can use an application running on one computer to revise documents.
Text Tools	Allows live text input and editing by group members. Once complete, the text document can be copied into word processing software.
E-mail	Electronic mail.
Persistent Capability	The ability to preserve files, briefings, or other team or project material for future reference. Properly organized, it becomes an information management device and is invaluable to a long-term effort.
Instant Messaging	This allows real-time exchange of notes and messages.

PART TWO

Intelligence in Full Spectrum Operations

Part Two provides a primer of what and who constitutes both MI and the Intelligence BOS and the process that these entities use in order to provide warfighters and decisionmakers with the intelligence they require in order to accomplish their respective missions.

Chapter 3 discusses the role of MI and the Intelligence BOS within full spectrum operations. It provides an overview of intelligence readiness, particularly the intelligence requirements associated with force projection. The concept of MI asset technical control is discussed as a complement to, not a replacement of, the Army's command and support relationships.

Chapter 4 presents the Intelligence Process—the Intelligence BOS methodology that accomplishes the primary focus of intelligence in full spectrum operations, which provides the warfighter with effective intelligence.

Chapter 3

Fundamentals in Full Spectrum Operations

FULL SPECTRUM OPERATIONS

3-1. Army commanders at all echelons may combine different types of operations simultaneously and sequentially to accomplish missions. Full spectrum operations include offensive, defensive, stability, and support operations. Missions in any environment require ARFOR that are prepared to conduct any combination of these operations:

- **Offensive operations** aim to destroy or defeat an enemy. Their purpose is to impose US will on the enemy and achieve decisive victory.
- **Defensive operations** defeat an enemy attack, buy time, economize forces, or develop conditions favorable for offensive operations. Defensive operations alone normally cannot achieve a decision. Their purpose is to create conditions for a counteroffensive that allow ARFOR to regain the initiative.
- **Stability operations** promote and protect US national interests by influencing the threat, political, and information dimensions of the OE through a combination of peacetime developmental, cooperative activities, and coercive actions in response to crises. Regional security is supported by a balanced approach that enhances regional stability

and economic prosperity simultaneously. ARFOR presence promotes a stable environment.

- **Support operations** employ ARFOR to assist civil authorities, foreign or domestic, as they prepare for or respond to crises and relieve suffering. Domestically, ARFOR respond only when the President or Secretary of Defense direct. ARFOR operate under the lead federal agency and comply with provisions of US law, to include the Posse Comitatus and Stafford Acts. (See FM 3-0.)

3-2. Intelligence supports the commander across full spectrum operations. It helps the commander decide when and where to concentrate sufficient combat power to overwhelm the enemy. ISR is essential for the commander to preclude surprise from the enemy, maintain the initiative on the battlefield, and win battles. Commanders at all levels synchronize intelligence with the other BOSs to maximize their ability to see and strike the enemy simultaneously throughout the AO.

3-3. Every soldier in the command is responsible for detecting and reporting enemy activities, dispositions, and capabilities. This task is critical because the environment we operate in is characterized by violence, uncertainty, complexity, and asymmetric methods by the threat. The increased situational awareness that soldiers develop through personal contact and observation is a critical element of that unit's ability to more fully understand the OE. However, soldiers collect information, they are not intelligence collectors. While medical personnel cannot be assigned ISR tasks due to their Geneva Convention category status, medical personnel who gain information through casual observation of activities in plain view while discharging their humanitarian duties will report the information to their supporting intelligence element.

OFFENSIVE OPERATIONS

3-4. Offensive operations at all levels require effective intelligence to help the commander avoid the enemy's main strength and to deceive and surprise the enemy. During offensive operations, intelligence must provide the commander with the composition, disposition, limitations, employment characteristics, and anticipated enemy actions in a timely enough manner for the commander to significantly affect the enemy commander's decision cycle. It ensures commanders have the intelligence they need to conduct offensive operations with minimum risk of surprise.

DEFENSIVE OPERATIONS

3-5. The immediate purpose of defensive operations is to defeat an enemy attack. Commanders defend to buy time, hold key terrain, hold the enemy in one place while attacking in another, or destroy enemy combat power while reinforcing friendly forces. Intelligence should determine the enemy's strength, COAs, and location of enemy follow-on forces. The defending commander can then decide where to arrange his forces in an economy-of-force role to defend and shape the battlefield. Intelligence support affords him the time necessary to commit the striking force precisely.

3-6. Intelligence in area defensive operations identifies, locates, and tracks the enemy's main attack and provides the commander time to allocate

sufficient combat power to strengthen the defense at the point of the enemy's main effort. Intelligence should also identify where and when the commander can most decisively counterattack the enemy's main effort or exploit enemy vulnerabilities.

3-7. Although the battlefield is normally organized as decisive, shaping, and sustaining operations, commanders conducting defensive operations may delineate intelligence in battlefield organizational terms of deep area, close area, and rear area.

STABILITY OPERATIONS

3-8. The environment is often much more complex during stability operations and as a result intelligence is often more complex. In fact, intelligence is even more important a factor (or operational multiplier) during stability operations. As a result, the commander must be even more involved in and knowledgeable of ISR (to include ISR operations the commander controls and other higher level ISR operations that may be occurring within his AO) during stability operations. For example, the commanders must understand the complex details of HUMINT and special access program (SAP) operations.

3-9. The commander requires the appropriate intelligence and IPB products in order to determine how best to influence the threat, political and information dimensions of the operational environment, and enhance regional stability. The identification and analysis of characteristics of the terrain and weather, politics, infrastructure, health status, civilian press, attitudes, and culture of the local populace and all possible threats are important in conducting stability operations. A lack of knowledge concerning local politics, customs, and culture could lead to US actions which attack inappropriate targets or which may offend or cause mistrust among the local population.

SUPPORT OPERATIONS

3-10. Support operations are usually nonlinear and noncontiguous. Commanders designate the decisive, shaping, and sustaining operations necessary for mission success. However, determining the intelligence requirements that drive the ISR effort intending to identify any potential threat's centers of gravity and decisive points may require a more complex and unorthodox thought process than that used in offensive and defensive operations. The G2/S2 may have to define the enemy differently. In support operations, the adversary is often the effects of disease, hunger, or disaster on a civilian population. US forces conducting support operations must also fully understand the organization and identity of key figures or groups within the region where they are operating, as these figures may influence greatly the actions of the population—both civilian and military.

ELEMENTS OF COMBAT POWER

3-11. Combat power is the ability to fight. It is the total means of destructive or disruptive force, or both, that a military unit or formation can apply against the adversary at a given time. Commanders combine the elements of

combat power to meet constantly changing requirements and defeat an enemy. The elements of combat power are—

- **Manuever** is the employment of forces, through movement combined with fire or fire potential, to achieve a position of advantage with respect to the enemy to accomplish the mission. Maneuver is the means by which commanders concentrate combat power to achieve surprise, shock, momentum, and dominance.
- **Firepower** provides the destructive force essential to overcoming the enemy's ability and will to fight. Firepower magnifies the effects of maneuver by destroying enemy forces and restricting his ability to counter friendly actions; maneuver creates the conditions for the effective use of firepower.
- **Leadership** is the most dynamic element of combat power. Confident, audacious, and competent leadership focuses on the other elements of combat power and serves as the catalyst that creates conditions for success. Leadership provides purpose, direction, and motivation in all operations.
- **Protection** is the preservation of fighting potential of a force so the commander can apply maximum force at the decisive time and place. Protection is neither timidity nor risk avoidance.
- **Information** enhances leadership and magnifies the effects of maneuver, firepower, and protection. Today, ARFOR use information collected to increase their situational understanding before engaging the enemy. Information from the COP and running estimates, transformed into situational understanding, allows commanders to combine the elements of combat power in new ways.

THE FOUNDATIONS OF ARMY OPERATIONS

3-12. Understanding the principles of war and tenets of Army operations is fundamental to operating successfully across the range of military operations. The principles of war and tenets of Army operations form the foundation of Army operational doctrine. (Refer to FM 3-0 for a full description of the Principles of War and Tenets of Army Operations.)

- **The Principles of War** provide general guidance for conducting war and military operations other than war at the strategic, operational, and tactical levels. The principles are the enduring bedrock of Army doctrine.
- **The Tenets of Army Operations** build upon the principles of war. They further describe the characteristics of successful operations. These tenets are essential to victory.

THE OPERATIONAL FRAMEWORK

3-13. The operational framework consists of the arrangement of friendly forces and resources in time, space, and purpose with respect to each other and the enemy or situation. It consists of the **AO, battlespace**, and the **battlefield organization**. The framework establishes an area of geographic and operational responsibility and provides a way for commanders to visualize how to employ forces against the enemy. Commanders design an

operational framework to accomplish their mission by defining and arranging its three components. They use the framework to focus combat power. The operational framework provides a mechanism through which the commander can focus the Intelligence BOS effort. Understanding the operational framework, AOIR, and intelligence coordination line (ICL) and their relationship to each other is key to planning and executing ISR operations.

- **AO** is an operational area defined by the JFC for land and naval forces. AOs do not typically encompass the entire operational area of the JFC but should be large enough for component commanders to accomplish their missions and protect their forces. AOs should also allow component commanders to employ their available systems to the limits of their capabilities. The AO is the basic control measure for all operations that defines the geographical area for which a particular unit is responsible. The commander—
  - Assumes responsibility for intelligence, maneuver, fires, terrain management, security, and movement within his AO.
  - Establishes control measures within his AO to assign responsibilities, coordinate intelligence, fires, and maneuver, and to control other activities.
- **Battlespace** is the environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the EMS; and the information environment within the operational areas and AOIs. The G2/S2 performs IPB and synchronizes ISR activities throughout the battlespace as determined by the commander's METT-TC considerations.
  - Area of influence is the geographical area in which a commander can directly influence operations by maneuver of FS systems normally under the commander's command or control. Areas of influence surround and include the associated AO.
  - AOI is that area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of this mission. (See JP 1-02.)
  - Information environment refers to a commander's battlespace that encompasses information activity affecting the operation. To envision that part of the information environment that is within their battlespace, commanders determine the information activities that affect their own operational capabilities and opposing C2 and information systems.
  - Force Projection Bases are the intermediate staging bases and power projection platforms.
  - Home Stations are the permanent locations of active and RC units. To a significant degree, events occurring at home station affect the morale and performance of deployed forces. Thus, the commander's battlespace encompasses all home station functions.

- **Battlefield Organization** is the allocation of forces in the AO by purpose. It consists of three all-encompassing categories of operations:
  - Decisive Operations are those that directly accomplish the task assigned by higher headquarters. Decisive operations conclusively determine the outcome of major operations, battles, and engagements.
  - Shaping Operations are operations at any echelon that create and preserve conditions for the success of decisive operations.
  - Sustaining Operations are operations at any echelon that enable shaping and decisive operations by providing CSS, rear area and base security, movement control, terrain management, and infrastructure development.

3-14. AOIs extend into enemy territory, to the objectives of current or planned operations. They include areas occupied by enemy forces that could jeopardize the accomplishment of the mission. AOIs also serve to focus intelligence development and IO directed at factors outside the AO that may affect the operation. (FM 3-0, para 4-79) The scheme of support includes the coordination of reconnaissance and surveillance missions and AOIs with a joint force or higher headquarters and lateral units to answer the intelligence requirements within the AOI. The G2/S2 monitors enemy activities within the AOI and provides intelligence on enemy activities that may affect the unit.

3-15. The AOIR is an area allocated to a commander in which the commander is responsible for the provision of intelligence within the means at the commander's disposal. It is an area allocated to the commander in which the commander is responsible for the collection of information concerning the threat and the environment and the analysis of that information in order to produce intelligence. Higher headquarters also ensure through intelligence handovers, collection management, and deconfliction that problems with duplication, confliction, and command and control do not occur in the AOIR. (FM 2-19.402/FM 34-80-2) They include the available ISR assets, capability of the G2/S2 section, available intelligence architecture, and METT-TC considerations. The AOIR cannot extend beyond a unit's AOI; however, it can be smaller than its AO as well as vary (expand or contract) during an operation. An example of when a unit's AOIR is smaller than its AO is when a higher headquarters ISR effort covers an area within the unit's AO.

3-16. ICLs designate the boundary between AOIRs. The G2/S2 establishes ICLs to facilitate coordination between higher, lateral, and subordinate units; coordinates with the G3/S3 to direct subordinates to track enemy units and HPTs in their areas; and hands over intelligence responsibility for areas of the battlefield. The establishment of ICLs ensures that there are no gaps in the collection effort; that all echelons are aware of the location, mission, and capabilities of other assets. The G2/S2 keeps abreast of collection activities in progress (all echelons) and battlefield developments through the ICLs. ICLs help—

- Facilitate coordination between higher, lateral, and subordinate units.

- Ensure higher, lateral, and subordinate units share information and intelligence as enemy entities and HPTs move into, within, or transition between AOIRs.
- Specify intelligence responsibility for areas of the battlefield.

ARMY CAPABILITIES

3-17. Commanders combine AC and RC ARFOR—consisting of different types of units with varying degrees of modernization—with multinational forces and civilian agencies to achieve effective and efficient unified action. A broad range of organizations makes up the institutional Army that supports the field Army. Institutional Army organizations design, staff, train, and equip the force. The institutional Army assists in effectively integrating Army capabilities. It does this through leadership and guidance regarding force structure, doctrine, modernization, and budget. (See FM 100-11.)

TASK ORGANIZATION

3-18. The Army supports JFCs by providing tailored force packages to accomplish joint missions and dominate enemies and situations on land. Trained and equipped AC and RC units comprise these force packages. Within these force packages, Army commanders organize groups of units for specific missions. They reorganize for subsequent missions when necessary. This process of allocating available assets to subordinate commanders and establishing their command and support relationships is called task organizing. A temporary grouping of forces designed to accomplish a particular mission is a task organization. The ability of ARFOR to tailor (select forces based upon a mission) and task organize (temporarily organize units to accomplish a tactical mission) gives them extraordinary agility. It allows operational and tactical level commanders to organize their units to make the best use of available resources. The ability to task organize means ARFOR can shift rapidly among offensive, defensive, stability, and support operations.

COMBINED ARMS

3-19. The fundamental basis for the organization and operations of ARFOR is combined arms. Combined arms is the synchronized or simultaneous application of several arms—such as infantry, armor, field artillery, engineers, air defense, and aviation—to achieve an effect on the enemy that is greater than if each arm was used against the enemy separately or sequentially. The ultimate goal of Army organization for operations remains success in joint and combined arms warfare. Its combined arms capability allows commanders to form Army combat, combat support (CS), and CSS forces into cohesive teams focused on common goals.

COMMAND AND SUPPORT RELATIONSHIPS

3-20. Establishing clean command and support relationships is fundamental in organizing for all operations. These relationships can achieve clear responsibilities and authorities among subordinate and supporting units. The commander designates command and support relationships within his authority to weigh the decisive operation and support his scheme of maneuver. Some forces available to a commander are given command or support relationships that limit his authority to prescribe additional relationships. Command and support relationships carry with them varying responsibilities to the subordinate unit by parent and gaining units. By knowing the inherent responsibilities of each command and support relationship, a commander may organize his force to establish clear relationships.

3-21. Command relationships establish the degree of control and responsibility commanders have for forces operating under their tactical control (TACON). When commanders establish command relationships, they determine if the command relationship includes administrative control (ADCON). Figure 3-1 shows command and support relationships.

3-22. Support relationships define the purpose, scope, and effect desired when one capability supports another. Support relationships establish specific responsibilities between supporting and supported unit. Army support relationships are direct support (DS), general support (GS), general support-reinforcing (GSR), and reinforcing.

3-23. While not an actual C2 function, technical control often affects certain intelligence operations. Technical control ensures adherence to existing policies or regulations and provides technical guidance for MI activities, particularly HUMINT, SIGINT, and CI operations. Commanders direct operations but often rely on technical expertise to plan, prepare, execute, and assess portions of the unit's collection effort. Technical control also involves translating ISR tasks into the specific parameters used to focus highly technical or legally sensitive aspects of the ISR effort. Technical control includes, but is not limited to—

- Defining, managing, or guiding the employment of specific ISR assets.
- Identifying critical technical collection criteria such as technical indicators.
- Recommending collection techniques, procedures, or assets.
- Conducting operational reviews.
- Conducting operational coordination.
- Conducting specialized training for specific MI personnel or units.

3-24. An example of technical control is the Prophet control team converting the PIR and SOR sets from the MDMP process and assigning times and anticipated enemy frequencies for subordinate Prophets to collect.

IF RELATIONSHIP IS:		INHERENT RESPONSIBILITIES ARE:							
		Has Command Relationship with:	May Be Task Organized by:	Receives CSS from:	Assigned Position or AO By:	Provides Liaison To:	Establishes/ Maintains Communications with:	Has Priorities Established by:	Gaining Unit Can Impose Further Command or Support Relationship of:
COMMAND	Attached	Gaining unit	Gaining unit	Gaining unit	Gaining unit	As required by gaining unit	Unit to which attached	Gaining unit	Attached; OPCON; TACON; GS; GSR; R; DS
	OPCON	Gaining unit	Parent unit and gaining unit; gaining unit may pass OPCON to lower HQ. Note 1	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	OPCON; TACON; GS; GSR; R; DS
	TACON	Gaining unit	Parent unit	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	GS; GSR; R; DS
	Assigned	Parent unit	Parent unit	Parent unit	Gaining unit	As required by parent unit	As required by parent unit	Parent unit	Not Applicable
SUPPORT	Direct Support (DS)	Parent unit	Parent unit	Parent unit	Supported unit	Supported unit	Parent unit; Supported unit	Supported unit	Note 2
	Reinforcing (R)	Parent unit	Parent unit	Parent unit	Reinforced unit	Reinforced unit	Parent unit; reinforced unit	Reinforced unit: then parent unit	Not Applicable
	General Support Reinforcing (GSR)	Parent unit	Parent unit	Parent unit	Parent unit	Reinforced unit and as required by parent unit	Reinforced unit and as required by parent unit	Parent unit; then reinforced unit	Not Applicable
	General Support (GS)	Parent unit	Parent unit	Parent unit	Parent unit	As required by parent unit	As required by parent unit	Parent unit	Not Applicable

NOTE 1. In NATO, the gaining unit may not task organize a multinational unit (see TACON).

NOTE 2. Commanders of units in DS may further assign support relationships between their subordinate units and elements of the supported unit after coordination with the supported commander.

Figure 3-1. Army Command and Support Relationships and Inherent Responsibilities.

Chapter 4

Intelligence Process in Full Spectrum Operations

THE INTELLIGENCE PROCESS

4-1. Commanders use the operations process of plan, prepare, execute, and assess to continuously design and conduct operations (see Figure 4-1). The commander cannot successfully accomplish the activities involved in the operations process without information and intelligence. The design and structure of intelligence operations support the commander's operations process by providing him with intelligence regarding the enemy, the battlefield environment, and the situation.

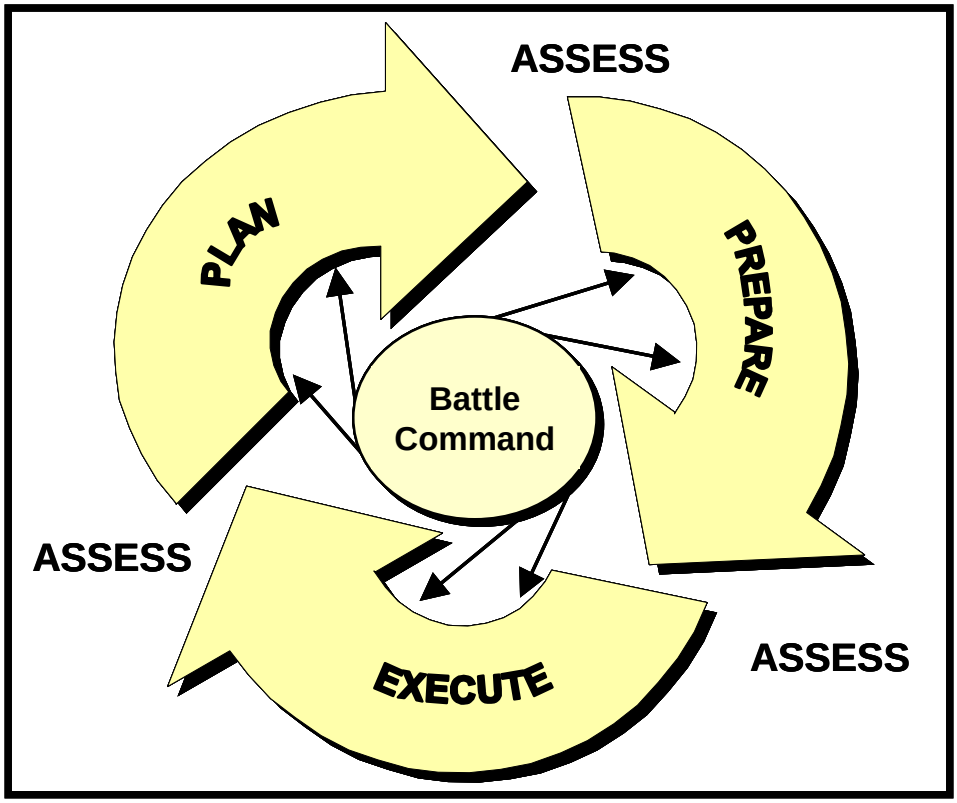


Figure 4-1. The Operations Process.

4-2. Intelligence operations consist of the functions that constitute the intelligence process: **plan, prepare, collect, process, produce**, and the three common tasks of **analyze, disseminate,** and **assess**. Just as the activities of the operations process overlap and recur as circumstances demand, so do the functions of the intelligence process. Additionally, the analyze, disseminate, and assess functions of the intelligence process occur continuously throughout the intelligence process.

4-3. The operations process and the intelligence process are mutually dependent. The commander, through the operations process, provides the guidance and focus through CCIRs and PIRs that drives the intelligence process; the intelligence process provides the continuous intelligence essential to the operations process. Intelligence about the enemy, the battlefield environment, and the situation allows the commander and staff to develop a plan, seize and retain the initiative, build and maintain momentum, and exploit success (see Figure 4-2). The intelligence process is just one of the mechanisms that provides input to build the COP and facilitate the commander's situational understanding.

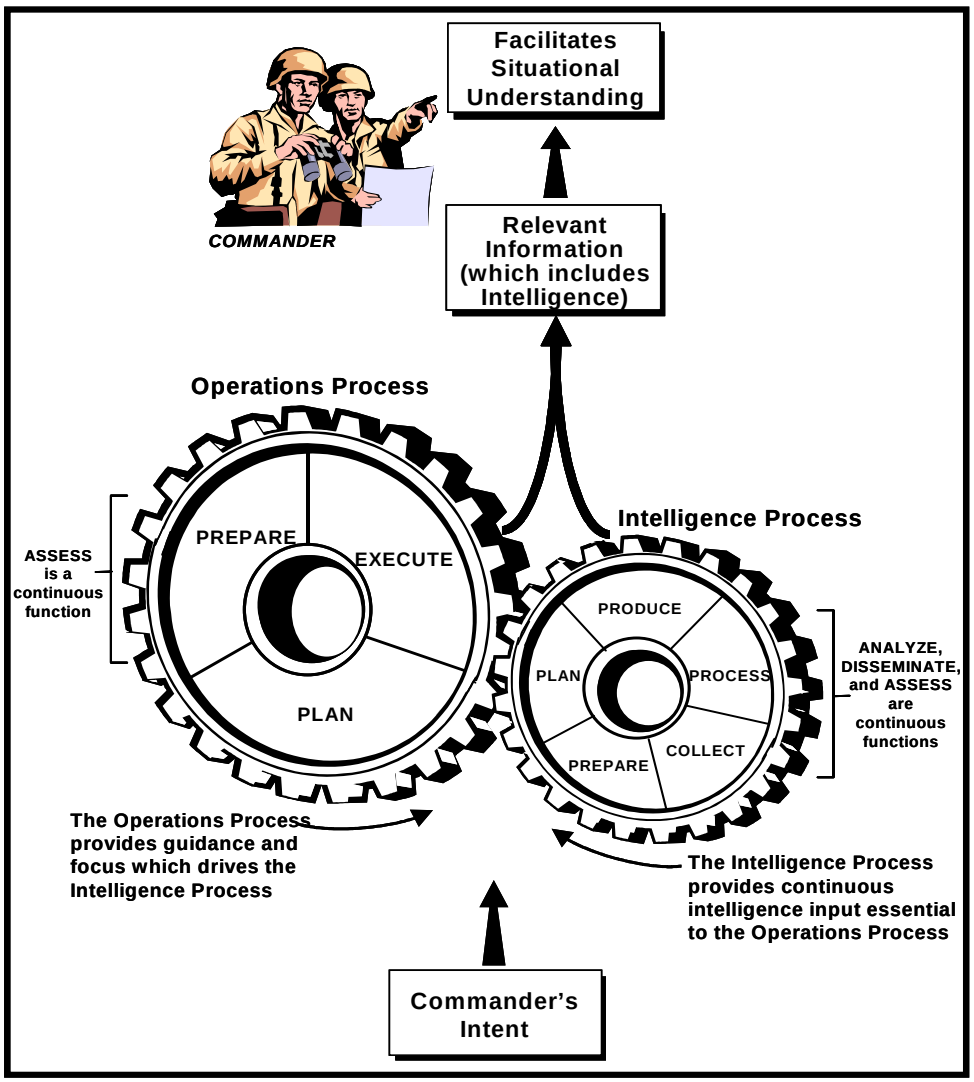


Figure 4-2. The Relationship Between the Operations and Intelligence Processes.

PLAN

4-4. The planning step of the intelligence process consists of activities that include assessing the situation, envisioning a desired outcome (also known as setting the vision), identifying pertinent information and intelligence requirements, developing a strategy for ISR operations to satisfy those requirements, directing intelligence operations, and synchronizing the ISR effort. The commander's intent, planning guidance, and CCIRs (PIRs and FIRs) drive the planning of intelligence operations. Planning, managing, and coordinating these operations are continuous activities necessary to obtain information and produce intelligence essential to decisionmaking.

COORDINATE

4-5. Staff and leaders coordinate with various elements, units, and organizations to ensure the necessary resources, linguist support (see Appendix B), information, intelligence, training, and procedures are in place to facilitate effective intelligence operations.

- Coordination for Movement of ISR Assets. All ISR assets at one time or another will move through or near another unit's AO. To avoid fratricide, ISR elements must coordinate with units, G3/S3, G2/S2, and each other, as well as coordinate with the fire support officer (FSO) to establish no-fire areas and/or other control measures around ISR assets and the air defense officer (ADO) in reference to aerial ISR assets in order to establish the appropriate weapons control status.
- Coordination for Information and Intelligence. The intelligence staff must prepare and practice coordination with personnel from all MI units, non-MI units, other service components, and multinational organizations that may contribute to or facilitate the collection effort. This coordination enables the G2/S2 to share and update databases, information, and intelligence and ensures connectivity with those organizations. All units are sources of relevant information regarding the enemy and the operational environment.
- Liaison. In order to accomplish the mission, exchange information and intelligence, move through certain areas and ensure FP, it may be necessary to coordinate with many different elements, organizations, and local nationals of the country in which friendly forces are conducting operations. Local nationals include police, town officials, foreign military forces, and political and other key figures within the AO. Operations may also necessitate coordination with other US and multinational forces; for example, the International Police Task Force (IPTF), Joint Commission Observers (JCO), Organization for Security and Cooperation in Europe (OSCE), Allied Military Intelligence Battalion (AMIB), and Defense HUMINT Service (DHS).
- Movement. Coordination with the G3/S3 ensures ease of movement and safe passage of friendly forces through an area. Coordinating movement also helps avoid fratricide.

INTELLIGENCE BOS CONSIDERATIONS

4-6. The Intelligence BOS is a unified system that anticipates and satisfies intelligence needs. Commanders ensure its proper employment by clearly articulating intent, designating CCIRs (PIRs and FFIRs), and prioritizing targets. Commanders must, however, understand the limitations of the Intelligence BOS to preclude unrealistic expectations of the system. The following are Intelligence BOS limitations:

- Intelligence only reduces uncertainty on the battlefield; it does not eliminate it entirely. The commander will always have to determine the presence and degree of risk involved in conducting a particular mission.
- The Intelligence BOS is composed of finite resources and capabilities. Intelligence systems and soldiers trained in specific ISR skills are limited in any unit. Once lost to action or accident, these soldiers and systems are not easily replaceable; for some, it may not be possible to replace them during the course of the current operation. The loss of soldiers and equipment can result in the inability to detect or analyze enemy actions. The loss of qualified language-trained soldiers, especially soldiers trained in low-density languages or skills, could adversely affect intelligence operations as well.
- The Intelligence BOS cannot effectively and efficiently provide intelligence without adequate communications equipment, capacity, and connectivity. Commanders and G2/S2s must ensure communications support to intelligence has the appropriate priority.
- Commanders and G2/S2s cannot expect that higher echelons will automatically send them everything they need. While intelligence reach is a valuable tool, the push of intelligence products from higher echelons does not relieve subordinate staffs from conducting detailed analysis and focusing the efforts of higher headquarters. Nor can they expect products pushed to them to be always at the level of detail they require. Commanders and G2/S2s must focus higher echelons by clearly articulating and actively pursuing intelligence requirements. By providing higher echelons with a clear picture of the required intelligence products, commanders can also narrow the flow of intelligence and information and preclude being overwhelmed by too much information.

4-7. Commanders should be aware that intelligence collection is enabled by, and subject to, laws, regulations, and policies to ensure proper conduct of intelligence operations. While there are too many to list here specifically, categories of these legal considerations include United States Codes (USCs), Executive Orders, National Security Council Intelligence Directives (NCSIDs), Army Regulations, United States Signal Intelligence Directives (USSIDs), SOFAs, ROE, and other international laws and directives.

PREPARE

4-8. The prepare step includes those staff and leader activities which take place upon receiving the OPORD, OPLAN, WARNO, or commander's intent

to improve the unit's ability to execute tasks or missions and survive on the battlefield. These activities include—

- Effecting necessary coordination in accordance with the OPORD, METT-TC, unit SOP.
- Establishing and testing the intelligence architecture. This activity includes complex and technical issues like hardware, software, communications, COMSEC materials, network classification, technicians, database access, liaison officers (LNOs), training, funding, and TTP.
- Establishing an intelligence team attitude. This activity includes knowing different unit's and organization's capabilities, training the necessary collective skills, establishing effective relationships with different units and organizations, developing mutual battle rhythms and TTP, and leveraging the right architectures and collaboration tools.
- Coordinating effective analytic collaboration. Effective analytic collaboration is necessary to maximize the complementary analytic capabilities of different units and organizations that produce intelligence within the same theater of operations. Coordinating this collaboration is an effort-intensive activity that requires careful mutual planning, division of labor, defined responsibilities, and procedures for adapting to changing circumstances as they develop.
- Establishing reporting procedures.
- Conducting IPB.
- Producing Intelligence Estimates.
- Presenting briefings.
- Ensuring staff and personnel are trained. If personnel are not adequately trained at this point, they must be trained or the leader must evaluate the risk they bring to the operation.
- Planning refinement, brief-backs, SOP reviews, rehearsals, and coordinating with various elements and organizations.
- Establishing other troop-leading procedures (TLPs) or coordination, as necessary, in accordance with METT-TC factors.

G2/S2 PREPARATION ACTIVITIES

4-9. The G2/S2 takes numerous steps before mission execution to ensure intelligence operations run smoothly and effectively. These steps include, but are not limited to, the following:

- Conduct rehearsals.
- Conduct communication rehearsals.
- Review and update available databases and IPB products.
- Review applicable SOPs, Army Regulations, DA Pamphlets, Field Manuals, and ROE for guidance in conducting intelligence operations.
- Plan and practice actions supporting likely contingencies, or the branches or sequels to an operation.
- Ensure coordination measures are still in effect.
- Ensure training (individual and collective).

- Verify communications protocols with theater and higher headquarters and subordinate and lateral units.
- Update intelligence databases.
- Update the forces with the most recent intelligence on the AO immediately before mission execution.

VERIFICATION

4-10. Coordination for or requesting provisions or services is only the first step in acquiring them. It is crucial that staff and leaders check to verify that procedures, personnel, equipment, and services are in place and ready for mission execution.

REHEARSALS

4-11. Rehearsals help units prepare for operations by either verifying that provisions and procedures are in place and functioning or identifying inadequacies, which staff and leaders must remedy. They allow participants in an operation to become familiar with and to translate the plan into specific actions that orient them to their environment and other units when executing the mission. They also imprint a mental picture of the sequence of key actions within the operation and provide a forum for subordinate and supporting leaders and units to coordinate. (FM 6-0)

REPORTING PROCEDURES

4-12. The timely and accurate reporting of CCIRs (PIRs and FFIRs) and IRs is key to successful operations. All assets should know when, how often, and what format to use when reporting. The G2/S2 must verify the frequencies, alternate frequencies, and reactions during jamming, as well as the LTIOV for specific information to be reported. Unit SOPs provide the proper reporting procedures.

4-13. The G2/S2 coordinates with the unit staff, subordinate and lateral commands, and higher echelon units to ensure that specific reporting assets, personnel, equipment (especially communications), and procedures are in place. The G2/S2 requests or establishes the appropriate message addresses, routing indicators, mailing addresses, and special security office (SSO) security accreditation for units.

COMMUNICATIONS

4-14. Staff and leaders must work closely with the G6/S6 or signal officer (SIGO) to coordinate for the required communication links. The unit may require classified and unclassified network connections for their equipment. If elements of the unit will be working outside the range of the unit's communications systems, then it is necessary to coordinate for global or extended range communications. Leaders must obtain the required type and amount of communications equipment and related components as well as the latest fills and frequencies. They must possess and be familiar with all the instructions, passwords, policies, regulations, and directives conducive to OPSEC. They must also ensure soldiers are trained in the use and procedures involved in operating communications equipment.

SITUATION UPDATES

4-15. Each staff section and element conducts activities to maximize the operational effectiveness of the force. Coordination and preparation are just as important, if not more important, as developing the plan. Staff preparation includes assembling and continuously updating estimates. For example, continuous IPB provides accurate situational updates for commanders.

INTELLIGENCE HANDOFF

4-16. A well-executed intelligence hand-off will ensure a smooth and seamless transition between units. It is important that the incoming unit becomes familiar with the operation as soon as possible to avoid compromising the intelligence production and flow of the mission. The following are points to consider during a mission hand-off:

- Briefings and reports (learn what briefings are required and when as well as report formats and requirements).
- Past, present, and planned activities within the AOI.
- Established SOPs (know procedures for reporting; intelligence contingency funds [ICFs] and incentive use if applicable; emplacement and use of ISR equipment).
- Key personalities (introductions are required; establish rapport and a good working relationship with all key personalities).
  - Key personnel on the base or camp (their responsibilities; how to contact them).
  - Key personnel in other US and multinational service components (coordinate for exchange of information and intelligence).
  - Key personalities from surrounding towns (local figures).
  - Key national level political and military figures.
- Supporting units (know where to go for provisions, information, or assistance and POCs within those organizations).
- Current attitudes (understand current attitudes and perspectives of the local populace).
- Equipment operation and idiosyncrasies (equipment may run on different applications; personnel may need to train on specific equipment and procedures).
- Area familiarization (identify NAIs, key terrain, minefields, and boundaries; know camp locations, routes and route names, checkpoints, towns, and troubled resettlement areas).

RULES OF ENGAGEMENT

4-17. Although ROE training was presented during the plan function of the intelligence process, leaders at all levels can take the opportunity during the prepare function to ensure their subordinates completely understand the ROE. It is also during this function that commanders may need to consider exceptions to, or modifications of, the ROE to facilitate HUMINT and CI collection or to enable the placement of ISR assets.

COLLECT

4-18. Recent ISR doctrine necessitates that the entire staff, especially the G3/S3 and G2/S2, must change their reconnaissance and surveillance mind-set to conducting ISR. The staff must carefully focus ISR on the CCIR (PIR and FFIR) but also enable the quick retasking of units and assets as the situation changes. This doctrinal requirement ensures that the enemy situation not just our OPLAN "drives" ISR operations. Well-developed procedures and carefully planned flexibility to support emerging targets, changing requirements, and the need to support combat assessment is critical. The G2/S2 and G3/S3 play a critical role in this challenging task that is sometimes referred to as "fighting ISR" because it is so staff intensive during planning and execution (it is an operation within the operation). Elements of all units on the battlefield obtain information and data about enemy forces, activities, facilities, and resources as well as information concerning the environmental and geographical characteristics of a particular area.

ISR TASKS

4-19. ISR tasks are the actions of the intelligence collection effort. ISR tasks consists of three categories:

- Intelligence.
- Surveillance.
- Reconnaissance.

4-20. Intelligence tasks are included in Annex B of the OPORD under Scheme of Intelligence. They include the following:

- **Intelligence Production**. Intelligence production includes analyzing information and intelligence and presenting intelligence products, conclusions, or projections regarding the OE and enemy forces in a format that enables the commander to achieve situational understanding.
- **Request for Information**. Submitting an RFI to the next higher or lateral echelon is the normal procedure for obtaining intelligence information not available through the use of available ISR assets. Users enter RFIs into an RFI management system where every other user of that system can see it. Hence, an echelon several echelons above the actual requester becomes aware of the request and may be able to answer it. A G2/S2 who receives an RFI from a subordinate element may use intelligence reach to answer RFIs.
- **Intelligence Reach**. Intelligence reach allows the commander to access the resources of national, joint, foreign, and other military organizations and units. Requestors can acquire information through push and pull of information, databases, homepages, collaborative tools, and broadcast services. (See Chapter 2 for more information on intelligence reach.)

4-21. For information on reconnaissance or surveillance tasks, refer to FM 7-15 and FM 3-55.

SPECIAL RECONNAISSANCE

4-22. Special reconnaissance (SR) is the complementing of national and theater intelligence collection assets and systems by obtaining specific, well-defined, and time-sensitive information of strategic or operational significance. It may complement other collection methods where there are constraints of weather, terrain, hostile countermeasures, and/or other systems availability. SR places US or US-controlled personnel conducting direct observation in hostile, denied, or politically sensitive territory when authorized. SOF may conduct these missions unilaterally or in support of conventional operations. (See JP 3-05 and FM 101-5-1.)

4-23. Army Special Operations Forces (ARSOF) elements conduct SR missions to obtain information not available through other means. SR operations encompass a broad range of collection activities to include reconnaissance, surveillance, and TA. SR complements national and theater collection systems that are more vulnerable to weather, terrain masking, and hostile countermeasures. SR missions provide intelligence or information that is often not available through other means. Typical SR missions include—

- TA and surveillance of hostile C2 systems, troop concentrations, deep-strike weapons, lines of communication (LOCs), WMD systems, and other targets.
- Location and surveillance of hostage, prisoner of war, or political prisoner detention facilities.
- Post-strike reconnaissance for BDA.
- Meteorologic, geographic, or hydrographic reconnaissance to support specific air, land, or sea operations.

4-24. For more information on special reconnaissance, see FM 3-05.102.

REPORTING

4-25. The most critical information collected is worthless if not reported in a timely manner. Collectors may report information via verbal, written, graphic, or electronic means. Unit SOPs must clearly state the transmission means of different types of reports (for example, sent by voice frequency modulated [FM] radios or by automated means). In general, the transmission of reports for enemy contact and actions, CCIRs, exceptional information, and NBC reports is by voice FM, and then followed up with automated reports. Commanders and staffs must remember that timely reporting, especially of enemy activity, is critical in fast-moving operations. Collectors must report accurate information as quickly as possible. Commanders and staff must not delay reports for the sole purpose of editing and ensuring the correct format. This is particularly true for reporting information or intelligence that answers the PIR.

TIME-SENSITIVE REPORTING

4-26. Intelligence and time-sensitive combat information that affects the current operation is disseminated immediately upon recognition. Combat information is unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the

criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. Thus combat information is provided directly to the tactical commander (see JP 1-02). The routing of combat information proceeds immediately in two directions: directly to the commander and through routine reporting channels, which include intelligence analysis and production elements.

4-27. Time-sensitive information usually includes reports concerning enemy contact and actions and CCIRs.

PROCESS

4-28. The process function converts relevant information into a form suitable for analysis, production, or immediate use by the commander. Processing also includes sorting through large amounts of collected information and intelligence (multidiscipline reports from the unit's ISR assets, lateral and higher echelon units and organizations, and non-MI elements in the battlespace). Processing identifies and exploits that information which is pertinent to the commander's intelligence requirements and facilitates situational understanding. Examples of processing include developing film, enhancing imagery, translating a document from a foreign language, converting electronic data into a standardized report that can be analyzed by a system operator, and correlating dissimilar or jumbled information by assembling like elements before the information is forwarded for analysis.

4-29. Often collection assets must collect and process their data prior to disseminating it. MI systems have their own reporting and processing systems, the details of which are in the appropriate MI system manuals and technical manuals. Some collection assets, particularly air reconnaissance and ground scouts, can report relevant information that is immediately usable by the tactical commander (for example, for targeting purposes). However, the personnel in the reporting chain still process these reports by evaluating their relevancy and accuracy. In many cases, the output of a collection asset is data, or information of limited immediate use to a commander. Also, in certain situations ROE dictate a requirement for target confirmation by other sources.

4-30. The intelligence staff processes information collected by the unit's assets as well as that received from higher echelons. The intelligence staff processes many types of information and data from intelligence reach, unmanned aerial vehicle (UAV) imagery, radar imagery, mobile target indicators (MTIs), and HUMINT and SIGINT reports.

PRODUCE

4-31. In the production step, the G2/S2 integrates evaluated, analyzed, and interpreted information from single or multiple sources and disciplines into finished intelligence products. Like collection operations, the G2/S2 must ensure the unit's information processing and intelligence production are prioritized and synchronized to support answering the CCIRs (PIRs and FFIRs).

4-32. Intelligence products must be timely, relevant, accurate, predictive, and usable. The accuracy and detail of every intelligence product has a direct

effect on how well the unit plans and prepares for operations. However, the G2/S2 and unit must use intelligence (no matter what form the intelligence is in) that meets the requirements but might not be as detailed or refined as possible or in a better form. A good answer on time is better than a more refined answer that is late.

4-33. The G2/S2 produces intelligence for the commander as part of a collaborative process. The commander drives the G2/S2's intelligence production effort by establishing intelligence and IRs with clearly defined goals and criteria. Differing unit missions, environments, and situations impose numerous and varied production requirements on the G2/S2 and his staff.

4-34. The G2/S2 must employ collaborative analysis techniques and procedures that leverage intelligence production capability of higher and subordinate echelons to meet these requirements. Proficiency in these techniques and procedures enables the G2/S2 to answer the commander's and staff's requirements regardless of the mission, environment, and situation. The G2/S2 and staff intelligence products enable the commander to—

- Plan operations and employ maneuver forces effectively.
- Recognize potential COAs.
- Employ effective tactics and techniques.
- Take appropriate security measures.
- Focus ISR.

COMMON INTELLIGENCE PROCESS TASKS

ANALYZE

4-35. Analysis occurs at various stages throughout the intelligence process. Personnel conducting intelligence operations at all levels analyze intelligence, information, and problems to produce intelligence, solve problems and, most importantly, answer the PIRs. Leaders at all levels conduct analysis to assist in making many types of decisions. An example is a HUMINT collector analyzing an intelligence requirement in order to determine the best possible collection strategy to use against a specific source.

4-36. Analysis in RM is critical to ensuring the IRs receive the appropriate priority for collection. The intelligence staff analyzes each requirement to determine its feasibility, whether or not it supports the commander's intent, and to determine the best method of satisfying the IRs. The staff also analyzes collected information to determine if it satisfies requirements.

4-37. During the produce function, the intelligence staff analyzes information from multiple sources to develop all-source intelligence products. The intelligence staff analyzes information and intelligence to ensure the focus, prioritization, and synchronization of the unit's intelligence production is in accordance with the PIRs.

4-38. In situation development, the intelligence staff analyzes information to determine its significance relative to predicted ECOAs and the CCIRs (PIRs and FFIRs). Through predictive analysis, the staff attempts to identify enemy activity or trends that represent opportunities or risks to the friendly force.

They use the indicators developed for each ECOA and CCIRs (PIRs and FFIRs) during the MDMP as the basis for their analysis and conclusions.

DISSEMINATE

4-39. Successful operations at the tactical and operational levels require an increased ability to synchronize fires, have faster access to intelligence, and enhance situational understanding and effective FP. Timely and accurate dissemination of intelligence is key to the success of these and other operations. Commanders must receive combat information and intelligence products in time and in an appropriate format to support decisionmaking. Additionally, sharing the most current all-source information and intelligence at all echelons is essential for commanders to maintain situational understanding.

4-40. To achieve this, it is imperative that the commander and staff establish and support a seamless intelligence architecture—including an effective dissemination plan—across all echelons to ensure information and intelligence flow in a timely manner to all those who need them. Intelligence and communications systems continue to evolve in their sophistication, application of technology, and accessibility to the commander. Their increasing capabilities also create an unprecedented volume of information available to commanders at all echelons. Finally, the commander and staff must have a basic understanding of these systems and how they contribute to the Intelligence BOS. A dissemination plan can be a separate product, or integrated into existing products such as the ISR synchronization plan or ISM, the decision support template (DST), or decision support matrix (DSM).

Dissemination Procedures

4-41. The G2/S2 and intelligence personnel at all levels assess the dissemination of intelligence and intelligence products.

4-42. Disseminating intelligence simultaneously to multiple recipients is one of the most effective, efficient, and timely methods. This can be accomplished through various means; for example, push, broadcast. However, within the current tactical intelligence architecture, reports and other intelligence products move along specific channels. The staff helps streamline information distribution within these channels by ensuring dissemination of the right information in a timely manner to the right person or element. There are three channels through which commanders and their staffs communicate: command, staff, and technical.

4-43. **Command Channel**. The command channel is the direct chain-of-command link that commanders, or authorized staff officers, use for command-related activities. Command channels include command radio nets (CRNs), video teleconferences (VTC), and the Maneuver Control System (MCS).

4-44. **Staff Channel**. The staff channel is the staff-to-staff link within and between headquarters. The staff uses the staff channel for control-related activities. Through the staff channel, the staff coordinates and transmits intelligence, controlling instructions, planning information, provides early warning information, and other information to support C2. Examples of staff

channels include the operations and intelligence radio net, telephone, the staff huddle, VTC, and the BOS-specific components of the Army Battle Command System (ABCS).

4-45. **Technical Channel**. Staffs typically use technical channels to control specific combat, CS, and CSS activities. These activities include fire direction and the technical support and sensitive compartmented information (SCI) reporting channels of intelligence and ISR operations. The SIGINT tasking and reporting radio net, intelligence broadcast communications, and the wide area networks (WANs) supporting single intelligence discipline collection, processing, and production are examples of technical channels.

Presentation Techniques and Procedures

4-46. The staff's objective in presenting information is to provide the commander with relevant information. Table 4-1 lists the three general methods that the staff uses to present information and meet its information objective. Systems within the ABCS contain standard report formats, maps, and mapping tools that assist the staff in presenting information in written, verbal, and graphic form. Audio and video systems such as large format displays and teleconferencing systems enable the staff to use a combination of the methods in multimedia presentations.

Table 4-1. Presentation Methods and Products.

Method	Products
Written Narrative	Reports, Estimates, and Studies
Verbal Narrative	Briefing (information, decision, mission, and staff)
Graphic	Charts, Overlays, and Electronic Displays

Intelligence Communications Architecture

4-47. The intelligence communications architecture transmits intelligence and information to and from various ISR elements, units, and agencies by means of automation and communication systems. With the continued development of sensors, processors, and communications systems, it is increasingly important to understand the requirements of establishing an effective communications architecture. The G2/S2 must identify the Intelligence BOS specific requirements of the unit's overall communications architecture. Refer to FM 2-33.5 for more information on intelligence communications reach. The following are some (but not all) of the questions which the staff must answer in order to establish the intelligence communications architecture:

- Where are the unit's collectors?
- What and where are the unit's processors?
- Where are the unit's intelligence production elements?
- Where are the unit's decisionmakers?
- How does the unit disseminate information from its producers to its decisionmakers and/or consumers?

- Are the systems which the unit's collectors, producers, processors, and consumers use compatible with each other? If not, what is the plan to overcome this challenge?
- How can the unit access databases and information from higher and other agencies?

ASSESS

4-48. Assessment is the continuous monitoring—throughout planning, preparation, and execution—of the current situation and progress of an operation, and the evaluation of it against criteria of success to make decisions and adjustments. Assessment plays an integral role in all aspects of the intelligence process. Assessing the situation and available information begins upon receipt of the mission and continues throughout the intelligence process. The continual assessment of intelligence operations and ISR assets, available information and intelligence, the various aspects of the battlefield environment, and the situation are critical to—

- Ensure the CCIRs (PIRs and FFIRs) are answered.
- Ensure intelligence requirements are met.
- Redirect collection assets to support changing requirements.
- Ensure operations run effectively and efficiently.
- Ensure proper use of information and intelligence.
- Identify enemy efforts at deception and denial.

4-49. During planning, the intelligence staff conducts a quick initial assessment of the unit's intelligence posture and holdings, status of intelligence estimates, and any other available intelligence products. From this assessment the commander issues his initial guidance and a WARNO.

4-50. While the majority of the unit is engaged in preparation, the ISR effort should already have begun. It is during this period when the prepare and execute activities of the operations process overlap, that the G2/S2 assesses the current situation as well as the progress of ISR operations.

4-51. During execution the intelligence staff continues assessing the effectiveness of the ISR effort while at the same time assessing the results and products derived from the collection effort. The critical aspects of assessment at this point include determining whether the PIRs have been answered, will be answered with the current ISR operations, or which ISR operations to adjust in order to answer the CCIRs (PIRs and FFIRs). This type of assessment requires sound judgment and a thorough knowledge of friendly military operations, characteristics of the AO and AOI, and the threat situation, doctrine, patterns, and projected future COAs.

PART THREE

Military Intelligence Disciplines

Part Three provides a more detailed explanation of the intelligence disciplines introduced in Part One of this manual.

Chapter 5 defines and discusses the roles and fundamentals of the all-source intelligence discipline.

Chapter 6 defines and discusses the roles, fundamentals, and generic organization of the HUMINT discipline.

Chapter 7 defines and discusses the roles, fundamentals, and generic organization of the IMINT discipline.

Chapter 8 defines and discusses the roles, fundamentals, and generic organization of the SIGINT discipline.

Chapter 9 defines and discusses the roles, fundamentals, and generic organization of the MASINT intelligence discipline.

Chapter 10 defines and discusses the roles, fundamentals, and generic organization of the TECHINT discipline.

Chapter 11 defines and discusses the roles, fundamentals, and generic organization of the CI discipline.

Chapter 5

All-Source Intelligence

DEFINITION

5-1. All-source intelligence is defined as the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open-source information, in the production of intelligence. All-source intelligence is a separate intelligence discipline, as well as the name of the function used to produce intelligence from multiple intelligence or information sources.

ROLE

5-2. The operational environment provides an ever-growing volume of data and information available from numerous sources, from which the commander can use to achieve situational understanding. His situational

understanding enables him to make decisions in order to influence the outcome of the operation; prioritize and allocate resources; assess and take risks; and understand the needs of the higher and subordinate commanders. The commander depends upon a skilled G2/S2 working within his intent to support his ISR effort and provide all-source intelligence analysis conclusions and projections of future conditions or events.

FUNDAMENTALS

5-3. All-source intelligence production satisfies intelligence requirements. It provides an overall picture of the adversary and the battlespace. It reduces the possibility of error, bias, and misinformation through the use of multiple sources of information and intelligence.

PLAN

5-4. The utilization of all-source intelligence facilitates the development of accurate and concise contingency-specific plans, orders, and intelligence products. Additionally, the G2/S2 must retrieve, update, or develop any required intelligence databases. The most important all-source products are the modified combined obstacle overlay (MCOO), event templates, ECOA sketches, and the HPT list provided during initial IPB in support of the plan function. Through all-source intelligence, the commander can make informed decisions about COAs and adversary capabilities.

5-5. The intelligence staff coordinates its efforts with other elements such as the engineer terrain team, the unit surgeon, the Air Force weather team, and other assets or elements that can support the analytical effort.

5-6. IPB plays a significant role in the planning phase of the intelligence process. It is a systematic, continuous process of analyzing the threat and environment and is designed to support staff estimates and the MDMP. The IPB is led by the G2/S2, with participation by the entire staff. IPB allows the commander and staff to make informed decisions, develop COAs, and focus ISR efforts where they are most needed. IPB continuously assists the commander and staff in focusing ISR assets on the appropriate targets at critical points in time and space.

5-7. The time available for the IPB process may not permit the luxury of conducting each step in detail. Overcoming time limitations requires the commander to identify those parts of IPB that are most important to the commander in planning and executing his mission. Applying the specific steps or degree of detail performed varies according to METT-TC. There are four steps in the IPB process: define the battlefield environment, describe the battlefield's effects, evaluate the threat, and determine ECOAs.

Define the Battlefield Environment

5-8. In this step, the G2/S2—

- Identifies characteristics of the battlefield that will influence friendly and threat operations including terrain (mobility), weather, hydrological data, infrastructure, and civilian demographics. Produces accurate, timely, and predictive IPB products that depict the aspects of the battlefield.

- Identifies the limits of the command's AO and AOI.
- Identifies gaps in current intelligence holdings, identifies IRs, and recommends CCIRs (PIRs and FFIRs).

5-9. Defining the battlefield environment includes identifying enemy forces (their location, mobility, general capabilities, and weapon ranges) and all other aspects of the environment that could have an effect on the unit's ability to accomplish the mission. Depending on the situation, these considerations may also include—

- Geography, terrain, and weather of the area.
- Information environment to include but not limited to computer and communications systems and capabilities, data acquisition systems and capabilities, media access and distribution, areas prone to electromagnetic interferences, and systems to generate electromagnetic interference.
- Population demographics (ethnic groups, religious sects, age distribution, health status, income groups).
- Medical threat to include but not limited to endemic and epidemic diseases, occupational and environmental health hazards, and poisonous and toxic plants and animals.
- Political or socio-economic factors, including factions, clans, and gangs.
- Infrastructures, such as transportation or telecommunications, and critical decisionmaking infrastructures and supporting information systems.
- ROE or legal restrictions, such as international treaties or agreements.

Describe the Battlefield's Effects

5-10. This IPB step deals with the effects of the battlefield environment on the current operations and potential enemy and friendly COAs. It begins with the assessment of existing and projected conditions of the battlefield environment, which the staff accomplishes through terrain analysis, weather analysis, and analysis of other characteristics of the battlefield. To conduct terrain analysis, the staff uses maps, reconnaissance, and other specialized terrain products (maps, overlays, databases, software). These products address such factors as wet or dry cross-country mobility, transportation systems (road and bridge information), vegetation type and distribution, surface drainage and configuration, surface materials (soils), ground water, manmade structures, and obstacles. The results of evaluating the terrain's effects should be expressed by identifying areas of the battlefield that influence each COA.

Evaluate the Threat

5-11. Evaluating the threat involves determining the threat force capabilities and the doctrinal principles and TTP that threat forces prefer to employ. The result of this evaluation produces a threat model, which portrays how threat forces normally execute operations and how they have reacted to similar situations in the past. The threat model includes an evaluation of the threat's strengths, weaknesses, and vulnerabilities, including an evaluation of typical HVTs.

Determine ECOAs

5-12. Determining ECOAs involves the identification and development of likely ECOAs that will influence accomplishing the friendly mission. Developing ECOAs is a form of predictive intelligence analysis and production. The procedures for this step include—

- Identifying the enemy's likely objectives and predicting the desired end-state.
- Identifying the full set of COAs available to the enemy.
- Predicting the enemy's most likely and most dangerous COAs.
- Evaluating and prioritizing each COA.
- Developing each COA in the amount of detail that time permits.
- Identifying initial ISR and collection requirements.

5-13. After conducting the initial IPB, the staff, primarily the G2/S2, identifies gaps in the available intelligence, develops the initial PIRs and IRs, and develops the initial input to the ISR plan based on the commander's guidance.

5-14. Indicators are the basis for situation development. Indicators are activities that will confirm or deny the event specified in an intelligence requirement. They are any positive or negative evidence of enemy activity or characteristic of the AO that points toward enemy capabilities, vulnerabilities, or intentions. Individual indicators cannot stand alone. Each indicator is integrated with other factors and indicators before patterns are detected and enemy intentions established. Indicators are developed by the analysts in the G2/S2 section. The event matrix shows the threat activities, or indicators, to look for in each NAI, and the timelines during which each NAI should be active. All indicators are developed to answer the commander's PIRs and IRs. The analyst uses indicators to correlate particular events or activities with probable ECOAs and to determine what events or activities must occur for an enemy to follow a particular COA. The ability to read indicators (including recognition of enemy deception indicators) contributes to the success of friendly operations. The analyst integrates information from all sources to confirm indicators of enemy activities. As indicators are detected and confirmed, PIRs are answered.

PREPARE

Activities

5-15. All-source activities during the prepare function include—

- Conducting rehearsals.
- Conducting communications rehearsals and verifiying communications protocols with higher, lateral, and subordinate units.
- Planning and practicing actions that support likely contingencies, branches, or sequels.
- Reviewing and updating available databases and IPB products.
- Ensuring control and coordination measures are still in effect.

- Updating the force with the most recent intelligence before mission execution.

Intelligence Estimates

5-16. The intelligence estimate is a continuous process that is the product of all actions the intelligence staff performs throughout the MDMP. The intelligence estimate provides a timely and accurate evaluation of the enemy and the AO (and often the AOIR) at a given time. It provides the background the G2/S2 uses to portray enemy actions during COA analysis.

5-17. The G2/S2 must clearly understand the weather and terrain effects and the ability to visualize the battlespace before producing the intelligence estimate. This understanding facilitates accurate assessments and projections regarding the enemy: enemy situation (including strengths and weaknesses), enemy capabilities and an analysis of those capabilities (COAs available to the enemy), and conclusions drawn from that analysis. The intelligence estimate's conclusion identifies the enemy's most likely COA and most dangerous COA. ECOAs must include a sketch of the COA with a task and purpose for the enemy's actions. Any gaps in the intelligence estimate are identified as information requirements.

5-18. The intelligence estimate may be written or oral. At the tactical level, especially during operations and exercises, intelligence estimates are usually delivered orally, supported by graphic displays and other decision support tools. During contingency planning, especially at corps level and above, estimates are usually written. During deliberate planning at joint headquarters, estimates are always written (see JP 5-00.2). However, the intelligence estimate should always be prepared as thoroughly as time and circumstances permit. A comprehensive intelligence estimate considers both the tangible (quantifiable) and the intangible aspects of the enemy's operations. It translates enemy strengths, weapon systems, training, morale, and leadership into combat capabilities and projections of future enemy actions.

5-19. Different sections of the intelligence estimate receive more emphasis during different activities within the operations process.

- During planning, the most important decision the commander makes is selecting a COA on which to base the plan. Thus, the sections of the intelligence estimate that focus on the commander's selecting the most appropriate COA are the most important at that time.
- During preparation, the intelligence estimate must focus on the commander's decisions that affect the ability of the unit to execute the upcoming operation. The intelligence estimate—and functions—that supports these decisions must focus on answering the CCIRs (PIRs and FFIRs) and guiding the ISR effort.
- During execution, the intelligence estimate focus is to support the anticipated command decisions. The most important action of the intelligence estimate—and the ISR effort— is to answer the PIR. However, it is also during the execution phase that the intelligence estimate must look ahead: anticipating branches or sequels to the

current operation, transition to other operations, changes in the ECOAs, and required adjustments to the ISR effort.

5-20. Refer to FM 2-01 for examples of intelligence estimates.

COLLECT

5-21. The collect intelligence process function within the all-source intelligence discipline is limited to gathering the necessary information, intelligence, and intelligence products required to perform analysis. Thus, all-source intelligence depends upon the other intelligence disciplines to perform collection. This is also the primary reason why OSINT is defined as a source of information and intelligence and not a separate intelligence discipline.

PROCESS

5-22. The process function converts relevant information into a form suitable for analysis, production, or immediate use by the commander. Processing also includes sorting through large amounts of collected information and intelligence to identify and exploit the information which is pertinent to the commander's intelligence requirements and facilitates situational understanding.

PRODUCE

5-23. All-source intelligence analysis and production—

- Drives collection to answer the PIR.
- Provides the enemy situation.
- Provides INTSUMs and other intelligence reports.
- Supports situational understanding.
- Provides predictive estimates of enemy actions; specifically, ECOAs.
- Provides continuously updated IPB.
- Provides all-source target packages (or folders).

5-24. As previously stated, the intelligence estimate is a continuous process. The commander and staff constantly collect, process, store, display, and disseminate information. Staff members update their estimates as they receive new information, such as—

- When they recognize new facts.
- When they replace assumptions with facts or find their assumptions invalid.
- When they receive changes to the mission or when changes are indicated.

5-25. Technological advances and NRT information allow estimates to be continuously updated; the running estimate and its intelligence component, the intelligence running estimate, exemplify this.

Running Estimate

5-26. Running estimates are continuously updated estimates based on new information as the operation proceeds. They serve as a staff technique to support the commander's visualization and decisionmaking, as well as the

staff's tool for assessing during preparation and execution. In the running estimate, staff officers continuously update their conclusions and recommendations as they evaluate the impact of new facts. Current doctrine emphasizes the COP as the primary tool that provides the current situation and, when merged with the running estimates, facilitates commanders achieving situational understanding. All staff sections (BOSs) provide their respective input to the COP. The COP as used today, combined with the running estimate, is predictive and enhances our current ability to collect, process, store, display, and disseminate information.

5-27. The portion of the COP that depicts the enemy situation is currently limited to displaying the locations and dispositions of enemy and threat forces in a relatively static manner, sometimes referred to as snapshots in time. The enemy situation portion of the COP requires analysis to provide the required level of detail. The COP and running estimates sufficiently provide effective support for battle command of knowledge-based organizations.

5-28. The main differentiation between the running estimate and the old staff estimates is the emphasis on not only continuously updating the facts of the estimate but also continuously updating the conclusions and recommendations while including projections of future conditions of the entire battlespace. While the COP is primarily a display of current intelligence and information, the running estimate requires the merging of the staff's cognitive processes with automation applications. The primary focus of the staff's cognitive process is to present predictive or anticipatory intelligence in support of the commander's decisionmaking or situational understanding. See Figure 5-1.

5-29. The running estimate is a product of the entire battle staff. Just as all BOSs contribute to the COP, they will also contribute their portion of the running estimate. The running estimate integrates the running estimates from each BOS. The Intelligence BOS input to the running estimate is the intelligence running estimate.

Intelligence Running Estimate

5-30. The intelligence running estimate is a continuous flow and presentation of relevant information and predictive intelligence that, when combined with the other staff running estimates, enables the decisionmaker's visualization and situational understanding of the AOI in order to achieve information superiority. The intelligence running estimate requires constant verification to support situational understanding of the current situation as well as predictive assessments for future operations.

5-31. While it is possible to employ the concept of the intelligence running estimate today, the true seamless and continuous update feature will be achieved with technological enablers that are not yet present in the force. In the future, technology should allow the information from the running estimate to become implanted as a part of the COP. However, there will always be a place for some separate context, orally or written, separate from the COP display to add fidelity and assist in the commander's visualization and decisionmaking. Additional training must be implemented not just

within MI but also throughout the force in order to institute the running estimate concept.

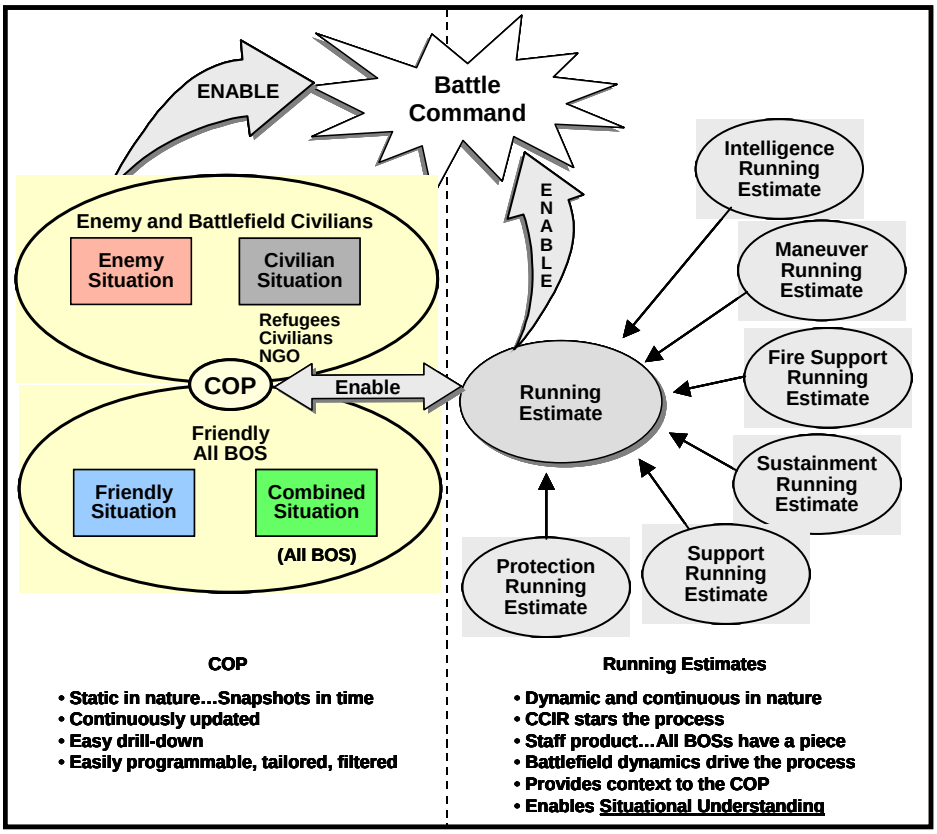


Figure 5-1. Example of the COP and a Running Estimate.

ANALYZE

5-32. Analysis is key in converting combat information and all intelligence from each discipline into all-source intelligence products and targeting information. From the multiple sources of information received, the staff analyzes and identifies critical information; determines the relevancy and accuracy of the information; and reaches conclusions about the information. These conclusions are either immediately disseminated or are used to form the basis of intelligence analysis products.

DISSEMINATE

5-33. The intelligence staff extracts and disseminates pertinent intelligence from products developed as a result of all-source analysis. The intelligence staff—

- Rapidly disseminates time-sensitive, all-source analysis intelligence and intelligence products to higher, lateral, and subordinate commands in order to keep all commanders abreast of current developments in the situation and battlespace in accordance with unit SOPs.

- Disseminates all-source analysis intelligence to other G2/S2 intelligence activities for additional processing or detailed analysis and exploitation in accordance with unit SOPs.

5-34. For intelligence reach operations all-source intelligence products are available and disseminated in a variety of forms. It is incumbent on the requestor to ensure that the all-source product can be transmitted over the available communications systems. This includes verifying the appropriate security level of the communication system.

ASSESS

5-35. The commander, the intelligence staff, and the intelligence consumers assess the analysis, production, and dissemination of all-source intelligence. The staff identifies intelligence gaps, emerging operational requirements, duplication of effort, or new targets or threats and redirects all-source activities as appropriate to meet intelligence requirements. Throughout the assessment process, the G2/S2, the intelligence staff, and intelligence users should be alert for evidence of possible enemy denial and deception efforts. The staff assesses intelligence and information for—

- Consistency with the current situation and threat trends.
- Accuracy and confirmation by other intelligence sources or disciplines.
- Source reliability and credibility.
- Pertinence to PIRs, intelligence requirements, RFIs, and other intelligence tasks or requests.

Chapter 6

Human Intelligence

DEFINITION

6-1. HUMINT is the collection by a trained HUMINT Collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool and a variety of collection methods, both passively and actively, to gather information to satisfy the commander's intelligence requirements and cross-cue other intelligence disciplines.

ROLE

6-2. The role of HUMINT Collectors is to gather foreign information from people and multiple media sources to identify adversary elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources and a variety of collection methods to gather information to satisfy the commander's intelligence requirements, and cross-cue other intelligence disciplines.

HUMINT FUNCTIONS

6-3. HUMINT functions are interrelated, mutually supporting, and can be derived from one another. No single function or technical capability can provide a full understanding of our adversaries. HUMINT functions are defined below and shown in Figure 6-1.

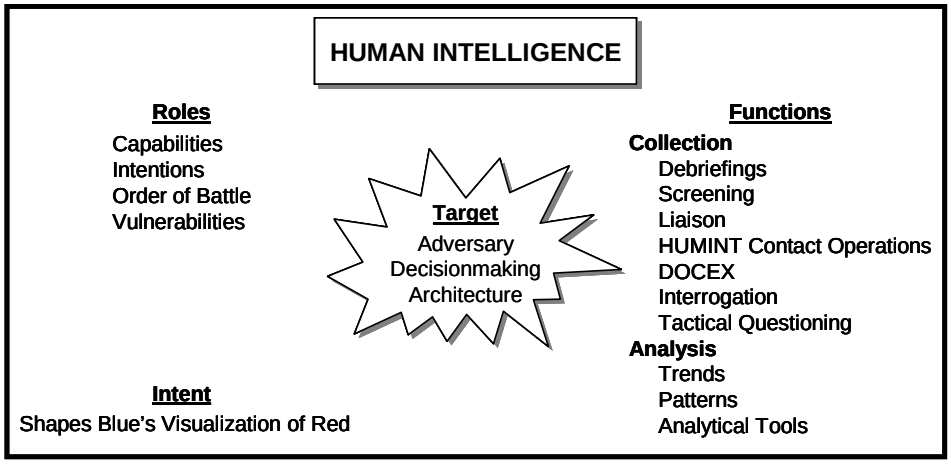


Figure 6-1. HUMINT Roles and Functions.

COLLECTION

6-4. HUMINT collection methods and operations include—

- **Debriefings.** Debriefings are the systematic questioning of individuals to procure information to answer specific collection requirements by direct and indirect questioning techniques. Sources for debriefings are categorized as friendly forces, US and non-US civilians to include refugees, displaced persons, and local inhabitants.
- **Screening.** Screening is the process of evaluating and selecting human and media sources for the prioritized collection of information in support of commander's PIRs and IRs. Screening categorizes and prioritizes sources based on the probability of a particular source having priority information and the degree of difficulty of extracting that information from the source. While screening is not in itself an information collection technique, it is vital to the rapid collection of information.
- **Liaison.** HUMINT elements conduct liaison with US, multinational, and HN military and civilian agencies, to include NGOs. Liaison is conducted to obtain information of interest and to coordinate or deconflict HUMINT activities.
- **HUMINT Contact Operations.** HUMINT contact operations are tactically oriented, overt collection activities that use human sources to identify attitude, intentions, composition, strength, dispositions, tactics, equipment, target development, personnel, and capabilities of those elements that pose a potential or actual threat to US and multinational forces. These forces provide early warning of imminent danger to US and multinational forces and contribute to the MDMP.
- **Document Exploitation (DOCEX).** DOCEX is the systematic extraction of information from all media formats in response to collection requirements.
- **Interrogation.** Interrogation is the systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of persons who are in the custody of the forces conducting the questioning.

UNIT SUPPORT TO HUMINT COLLECTION

6-5. Small units contribute to HUMINT collection through a number of different ways.

Tactical Questioning

6-6. Tactical questioning can provide critical information for situational understanding. Tactical questioning is the expedient initial questioning for information of immediate tactical value. Soldiers conduct tactical questioning based on the unit's SOP, ROE, and the order for that mission. Unit leaders must include specific guidance for tactical questioning in the order for appropriate missions. The unit S3 and S2 must also provide specific guidance down to the unit level to help guide tactical questioning. For a more detailed discussion of tactical questioning, see ST 2-91.6.

Combat Patrolling

6-7. Through observing and interacting with the local environment during the conduct of missions, handling EPWs/detainees, and handling captured documents, soldiers serve as the commander's "eyes and ears" whether—

- Performing traditional offensive or defensive operations.
- Performing a patrol in a stability operation.
- Manning a TCP or a roadblock in a support operation.
- Occupying an observation post.
- Passing through an area in a convoy.
- Performing any operation that involves observing and reporting on elements of the environment and activities in the AO.

ISR Operations

6-8. The information that the soldier reports as a result of completed missions up the chain of command forms a vital part of planning and operations. Careful and quick handling of EPWs/detainees and documents also helps the ISR effort. Unit headquarters must ensure that the reports they receive and forward contain all the subtle detail provided by the small unit. For tactical operations, there are four levels of reporting:

- Immediate reporting of information of critical tactical value, based either on predetermined criteria or common sense.
- Normal reporting, submitted before the unit S2 section performs the debriefing.
- Debriefing performed by the S2 section.
- Follow-up reporting, submitted after the unit S2 section performs the debriefing.

6-9. The four levels of reporting facilitate the unit S2 section capturing all the fine details of the small unit's activities for all-source analysis and future planning. The unit S2 must ensure that information of HUMINT and CI value is reported to the G2X.

ANALYSIS

6-10. IPB, all-source, and single-source analysis are used to template adversarial OB. HUMINT elements analyze operational taskings to determine the best collection methods to employ in satisfying CCIRs (PIRs and FFIRs) and IRs. As information is collected, it is analyzed for completeness and accuracy to identify significant facts for subsequent interpretation and inclusion in intelligence products, and passing to other collectors. This analysis also helps to identify collection gaps and focus or refocus collection efforts. Analysis provides the commander with situational understanding of the battlespace to execute operations. Raw information, open-source material, and finished intelligence products are analyzed in response to local and national requirements. Analysis occurs at all levels from tactical to strategic.

- At the tactical level, HUMINT teams focus their efforts on supporting mission requirements and contributing to the all-source COP.

- Operational analysis is used to assess adversary intentions, capabilities, dispositions, and their regional impacts.
- Strategic analysis supports national and Army programs through compilation of local and regional analysis into global assessments; identifies technology development trends and patterns in military activities and capabilities.

6-11. HUMINT products consist of, but are not limited to, target nomination, input to threat and vulnerability assessments, intelligence estimates, and intelligence information reports. Finalized intelligence derived from HUMINT activities is incorporated into joint and national intelligence databases, assessments, and analysis products. HUMINT products are also incorporated into the COP to support situational awareness. HUMINT production takes place at all levels.

- Operational and tactical production includes tactical alerts, spot reports, and current intelligence; input to threat and/or vulnerability assessments tailored to specific activities, units, installations, programs or geographic areas, and target studies to support contingency planning and major exercises; studies of military activities and capabilities.
- Strategic products include assessments supporting national and Army information requirements on foreign technology development; worldwide assessments of the organization, location, funding, training, operations capabilities and intentions of terrorist organizations; analyses of the capabilities of international narcotics trafficking organizations.

OPERATIONAL EMPLOYMENT

6-12. Army HUMINT must support the full spectrum of military operations. Commanders require a well-trained HUMINT force consisting of AC, RC, civilian government, and contractor personnel. The HUMINT force is focused on and dedicated to the collection of data and information relevant to the commander's PIRs and IRs. Effective employment of Army HUMINT elements in all phases of operations and at all levels from tactical to strategic will remain paramount to ensuring that commanders have the best pictures possible of their adversaries. HUMINT Collectors use the following collection methods.

LEVELS OF EMPLOYMENT

6-13. **Strategic and Departmental.** Strategic and departmental operations will be conducted by HUMINT elements supporting national, DOD, and DA required missions (for example, support to NATO and special operations and missions). The Army strategic HUMINT force resides in DHS. Trained Army HUMINT professionals must be available to augment DOD HUMINT efforts and coordinate between Army and Joint or DOD elements during crisis and war. Strategic HUMINT activities are generally carried out by departmental level HUMINT elements or Army HUMINT assets directly assigned to DOD and Joint positions. The Army overt HUMINT capability at the strategic

level will be deployed and under operational control (OPCON) of the Army Service Component Commander (ASCC).

6-14. **Operational.** HUMINT operational missions must support combatant commanders, generally in geographic AORs. Operational HUMINT assets provide capabilities to support theater requirements for HUMINT collection. Operational HUMINT elements will focus on threat identification and capabilities. As with all levels of employment, HUMINT activities and functions will include DOCEX, collection, operations, analysis, and production. HUMINT elements must be capable of quickly transitioning from a peacetime mission to crisis operations to support combatant commander requirements. Operational elements may also be deployed to support or reinforce tactical forces in CONOPS.

6-15. **Tactical.** Army HUMINT play a crucial role in supporting tactical forces. HUMINT teams conduct operations throughout the battlespace during CONOPS. CONOPS support activities include debriefings, screenings, contact operations, and interrogations. HUMINT activities in CONOPS focus on the threat and assisting the senior intelligence officer (SIO) and commander in understanding the threat's decisionmaking process. During peacetime, organic tactical HUMINT teams conduct activities pursuant with approved regulations and command guidance.

SUPPORT TO CONTINGENCY OPERATIONS

6-16. **Initial Phase.** The initial phase of operations from peacetime military engagement (PME) to major theater war (MTW) lays the foundation of future team operations. In general, the priority of effort focuses inward on security of operating bases, areas of troop concentration, and C2 nodes to identify the collection threat to US forces that could be used by adversarial elements to plan hostile acts against US activities and locations.

6-17. **Continuation Phase.** Once security of the operating bases has been established, the operational focus of HUMINT teams shifts outside the operating base to continue to detect, identify, and neutralize the collection threat to US forces as well as to provide I&W of hostile acts targeting US activities. The HUMINT team uses several collection methods, to include HUMINT contact operations, elicitation, and liaison, to answer the supported commander's requirements.

6-18. **HUMINT Team.** A key element to the HUMINT team's success is the opportunity to spot, assess, and develop relationships with potential sources of information. Operating as independent teams, without being tied to combat assets, enables the HUMINT team's maximum interaction with the local population, thereby maximizing the pool of potential sources of information. A second key element of a HUMINT team's success is its approachability to the local population. A soft posture enables a HUMINT team to appear as non-threatening as possible. Experience has shown that the local population in general is apprehensive of fully and openly armed patrols and soldiers moving around population centers. During some operations civilian attire or non-tactical vehicles may be used to lower the

HUMINT team profile. NOTE: In some special situations, these measures are taken to make the operation less visible to the casual observer. Also, in some cultures, sharing food and beverages among friends is expected; exceptions to restrictions or general orders should be considered to facilitate successful HUMINT team operations, many of which are geared towards developing relationships with potential sources of information.

SUPPORT TO INSTALLATIONS AND OPERATING BASES

6-19. Commanders may restrict personnel to base camps and installations during the initial stages of operations (PME to MTW), when the operational environment is being assessed, or as a temporary expedient when the threat level exceeds the ability to provide reasonable FP. Operational restrictions minimize the risk to the HUMINT team, but minimizing its collection potential may increase the risk to the force as a whole. While confined to an installation or a base camp, the HUMINT team can maintain a limited level of information collection by—

- Screening locally employed personnel.
- Debriefing combat and ISR patrols.
- Debriefing friendly force personnel who are in contact with the local population.
- Conducting limited local open-source information collection.
- Contributing to the threat and vulnerability assessments of the base camp.

TACTICS, TECHNIQUES, AND PROCEDURES

6-20. At the HUMINT team level, team members conduct mission analysis and planning specific to their AO. Backwards planning and source profiling are used extensively to choose HUMINT targets. To verify adequate area coverage, the HUMINT team may periodically develop and use HUMINT target overlays and other HUMINT analytical tools that illustrate the HUMINT situation, identify gaps, and help refocus the collection effort.

6-21. The HUMINT team is also in constant contact with the supported S2 and the other ISR assets (Scouts, PSYOP, CA, and MPs) in order to coordinate and deconflict operations and to cross-check collected information. The supported unit S2, with the help of the HUMINT team, regularly and systematically debriefs all ISR assets.

6-22. The HUMINT team must be integrated into the supported unit's ISR plan. The HUMINT operational management team (OMT) chief will advise the supported unit on the specific capabilities and requirements of the team to maximize mission success.

OPERATIONAL RISK MITIGATION

6-23. The employment of HUMINT teams includes varying degrees of contact with the local population. As the degree of contact with the population increases, both the quantity and quality of collection increases. In many instances, however, there is a risk to the team inherent with increased exposure to the local population. The decision at what level to employ a team is METT-TC dependent. The risk to HUMINT assets must be balanced with

the need to collect priority information and to protect the force as a whole. ROE, SOFA, direction from higher headquarters, and the overall threat level may also restrict the deployment and use of HUMINT teams. The commander should consider exceptions to the ROE to facilitate HUMINT collection.

6-24. Risks are minimized through the situational awareness of HUMINT team members. They plan and rehearse to readily react to any situation and carry the necessary firepower to disengage from difficult situations. If it becomes necessary to call for assistance, adequate and redundant communications equipment is critical. These scenarios and actions should be trained prior to deployment into a contingency area and rehearsed continuously throughout the deployment.

6-25. A supported unit commander is often tempted to keep the HUMINT team "inside the wire" when the threat condition (THREATCON) level increases. The supported commander must weigh the risk versus potential information gain when establishing operational parameters of supporting HUMINT teams. This is necessary especially during high THREATCON levels when the supported unit commander needs as complete a picture as possible of the threat arrayed against US and multinational forces.

6-26. When it is not expedient to deploy the HUMINT team independently due to threat levels or other restrictions, the team can be integrated into other ongoing operations. The HUMINT team may be employed as part of a combat, ISR, or MP patrol or used to support CA, PSYOP, engineer, or other operations. This method reduces the risk to the team while allowing a limited ability to collect information. It has the advantage of placing the team in contact with the local population and allowing it to spot, assess, and interact with potential sources of information. However, this deployment method restricts collection by subordinating the team's efforts to the requirements, locations, and timetables of the unit or operation into which it is integrated and does not allow for the conduct of sensitive source operations. **This method of employment should be considered a last resort.**

HUMINT EQUIPMENT

6-27. Basic C2, transportation, and weapons requirements do not differ significantly from most soldier requirements and are available as unit issue items. However, HUMINT teams have unique communications, collection, processing, and mission-specific requirements.

COMMUNICATIONS

6-28. Dedicated and secure long-range communications are key to the success of the HUMINT team mission. HUMINT team operations require a secure, three-tiered communications architecture consisting of inter/intra-team radios, vehicle-based communications, and a CI and HUMINT base station.

6-29. The HUMINT team must have access to existing communications networks such as the tactical local area network (LAN). The HUMINT team must also be equipped with its own COMSEC devices. It is imperative that the HUMINT team acquire access to the public communication system of the HN. This can be in the form of either landlines or cellular telephones. Such

access enables the HUMINT team to develop leads which can provide early indicators to US forces.

Interoperability

6-30. Communications systems must be equipped with an open-ended architecture to allow for expansion and compatibility with other service elements, government organizations, NGOs, and multinational elements to effectively communicate during CONOPS. All ISR systems must be vertically and horizontally integrated to be compatible across all BOSs and with Legacy and Interim Force elements.

Satellite Communications On-The-Move (SOTM)

6-31. To provide real time or NRT information reporting, HUMINT elements must have the capability to transmit voice, data, imagery, and video while on the move. HUMINT teams must be able to transmit while geographically separated from their parent unit while operating remotely. This broadband requirement can only be achieved through a SATCOM capability and must be achievable while mobile.

HUMINT COLLECTION AND PROCESSING SYSTEMS

6-32. The HUMINT team must rely on automation to achieve and maintain information dominance in a given operation. With time, effective collection planning and management at all echelons, the HUMINT team can collect a wealth of information. The sorting and analysis of this information in a timely and efficient manner is crucial to operations. Automation helps the HUMINT team to report, database, analyze, and evaluate the collected information quickly and to provide the supported unit with accurate data in the form of timely, relevant, accurate, and predictive intelligence.

6-33. Automation hardware and software must be user friendly as well as interoperable among different echelons and services. They must interface with the communications equipment of the HUMINT team as well as facilitate the interface of audiovisual devices. Technical support for hardware and software must be available and responsive.

6-34. The demand for accurate and timely HUMINT reporting, DOCEX, and open-source information has grown tremendously. Biometric (physiological, neurological, thermal analysis, facial and fingerprint recognition) technologies will allow rapid identification; coding and tracking of adversaries and human sources; and cataloging of information concerning enemy prisoners of war (EPWs), detainees, and civilians of HUMINT interest on the battlefield. Biometrics will also provide secure authentication of individuals seeking network or facility access.

6-35. HUMINT teams work with multinational forces, and other foreign nationals, and require the ability to communicate in their respective languages. Often HUMINT personnel have little or no training in the target language, and lack of skilled interpreters can hinder HUMINT activities. HUMINT teams require textual and voice translation devices, source verification, and deception detection machines (biometrics) to improve collection capability and accuracy.

6-36. HUMINT teams require dynamic machine language translation (MLT) tools that provide both non-linguists and those with limited linguist skills a comprehensive, accurate means to conduct initial screenings and basic interviews in a variety of situations. HUMINT elements will focus on in-depth interviews and communications with persons of higher priority. MLT tools will minimize reliance on contract linguists and will allow soldiers to concentrate on mission accomplishment.

MISSION SPECIFIC

6-37. The HUMINT team may conduct night operations and must be equipped with NVDs for its members and photographic and weapons systems. The HUMINT team also may operate in urban and rural areas, where the threat level can vary from semi-hostile to hostile. The safety of the HUMINT team can be enhanced with equipment that can detect, locate, suppress, illuminate, and designate hostile optical and E-O devices. In addition, high power, gyro-stabilized binoculars, which can be used from a moving vehicle, also increase the survivability of the HUMINT team. It also gives the team another surveillance and collection device.

6-38. Some of the HUMINT team missions may require the documentation of incidents. The teams can use the following equipment in their open-source collection efforts.

- Small, rugged, battery-operated digital camcorders and cameras which are able to interface with the collection and processing systems as well as communication devices.
- GPSs that can be mounted and dismounted to move in the AO efficiently.
- Short-range multichannel RF scanning devices that can also identify frequencies which enhance their security.

6-39. In some cases HUMINT teams require a stand-off, high resolution optical surveillance and recording capability that can provide target identification at extended ranges to protect the intelligence collector while avoiding detection by the adversary target. An advanced optical capability provides intelligence collectors the ability to locate and track adversarial targets (passive and hostile) for identification, collection, and target exploitations.

INTEGRATION OF LINGUISTS

6-40. Integrating linguists into the HUMINT team should take place as soon as possible. Security clearances and contractual agreements will help the team determine the level of integration.

6-41. Along with the basic briefing of what is expected of the civilian linguists as interpreters, HUMINT teams should be informed about the civilians' chain of command and the scope of their duties beyond interpreting. The HUMINT team leader must ensure that linguists are trained and capable of completing all tasks expected of them.

BATTLE HAND-OFF

6-42. HUMINT teams are always engaged. A good battle hand-off is critical to smooth transition and mission success. The battle hand-off can directly contribute to mission success or failure of the outgoing team, but especially of the incoming team. The battle hand-off begins the first day the HUMINT team begins to operate in an AO. Regardless of how long the team believes it will operate within the AO, it must ensure there is a seamless transition to an incoming team, other US unit, or agency. The HUMINT team accomplishes this transition by establishing procedures for source administration, database maintenance, and report files.

6-43. Teams must plan and implement a logical and systematic sequence of tasks to enable an incoming team to assume the operations in the AO. Adequate time must be allotted for an effective battle hand-off. In some environments, a few weeks may be necessary to accomplish an effective battle hand-off. Introductions to sources of information, especially HUMINT contact operations sources, are critical and teams must prioritize their time. During this time the outgoing HUMINT team must familiarize the new HUMINT team with all aspects of the operation, which includes past, present, and planned activities within the AO. Area orientation is critical. These include major routes, population centers, potential hot spots, and other points of interest (such as police stations, political centers, and social centers).

ORGANIZATION

6-44. HUMINT activities require a complex C2 relationship to ensure that the requirements of the supported commander are fulfilled while balancing the need for strict integrity and legality of HUMINT operations. This complex relationship balances the role of the SIO as the requirements manager and the *2X as the mission manager with the MI commander as the asset manager. ("*2X" indicates 2X functions at all levels.)

COMMAND VERSUS CONTROL

6-45. ARFOR will normally deploy as part of a joint and/or multinational operation. In all cases, commanders at each echelon will exercise command over the forces assigned to their organization. Command includes the authority and responsibility for effectively using resources, planning for and employment of forces, and ensuring that forces accomplish assigned missions. Leaders and staffs exercise control to facilitate mission accomplishment.

6-46. While the MI commander supervises subordinates and produces reports, the *2X synchronizes activities between intelligence units and provides single-source processing and limited analysis. While the MI commander takes care of the operators executing missions, the *2X obtains the data and reports from higher echelons required to execute the missions.

STAFF RESPONSIBILITIES AND FUNCTIONS

*2X Staff

6-47. The *2X staff is responsible for the integration, correlation, and fusion of all Human Sensor information into the Intelligence BOS within the *2X

AOIR. The *2X is also responsible for analyzing adversary collection, terrorist and sabotage activities, developing countermeasures to defeat threat collection activities, identifying and submitting collection requirements to fill collection gaps, and providing input to the all-source picture regarding adversary intelligence activities.

*2X Staff Officer

6-48. The *2X Staff Officer provides CI and HUMINT collection expertise. The *2X—

- Is the single focal point for all matters associated with CI and HUMINT in the AOIR.
- Is the CI and HUMINT advisor to the G2 and commander.
- Is an extension of the collection manager and ensures that the best asset or combinations of assets are used to satisfy information requirements.
- Along with his subordinate elements (CICA, HOC, OSC, CI Analysis Cell [CIAC], and HAC), exercises technical control over his assigned Army CI and HUMINT elements in the designated AOIR.
- Is the principal representative of the G2 and the commander when coordinating and deconflicting CI and HUMINT activities with national or theater agencies operating in the AOIR.
- Supports specific RM efforts in conjunction with the requirements manager through—
  - Planning and coordinating CI and HUMINT operations.
  - Reviewing and validating HUMINT requirements.
  - Recommending assignment of tasks to specific collectors.
  - Conducting liaison with non-organic HUMINT collection. This liaison includes national level and multinational force assets for source deconfliction and special activities outside the *2X AOIR.
- Will provide OMTs with capability to reach back to current database information, technical information and guidance, and source deconfliction necessary to monitor the collection activities of the HUMINT teams.

The HUMINT Analysis Cell (HAC)

6-49. The HAC is the single-source fusion point for all HUMINT reporting and operational analysis. It determines gaps in reporting and coordinates with other analysis teams and technical controllers to cross-cue other collection sensor systems. The HAC—

- Uses analytical tools to develop long-term collection plans and provides reporting feedback that supports all HUMINT and CI entities in the supported command's AOIR.
- Produces and disseminates HUMINT products and provides input to intelligence summaries.
- Uses analytical tools found at the ACE or JISE to develop long-term analyses and provides reporting feedback that supports the J/G/S2X, HUMINT operations section, OMTs, and HUMINT teams.
- Produces country and regional studies tailored to HUMINT collection.

- Compiles target folders to assist J/G/S2X assets in focusing collection efforts.
- Analyzes and reports on trends and patterns found in HUMINT reporting.
- Analyzes source reliability and credibility as reflected in reporting and communicating that analysis to the collector.
- Develops and maintains databases specific to HUMINT collection activities that directly support the collection efforts of HUMINT teams and are directly accessible by HUMINT teams.
- Provides collection requirements input to the HOC.
- Supports RM through the development of HUMINT SIRs based on command PIRs.
- Answers HUMINT-related RFIs.

6-50. For intelligence reach operations, HUMINT products are available and disseminated in a variety of forms. It is incumbent on the requestor to ensure that the HUMINT product can be transmitted over the available communications systems. This includes verifying the appropriate security level of the communications systems.

HUMINT Operations Cell (HOC)

6-51. The HOC in the *2X coordinates and synchronizes all HUMINT activities in the AOIR. The HOC exercises technical control over all HUMINT entities in the designated AOIR and deconflicts HUMINT activities with higher, lower, and adjacent HUMINT elements. The HOC accomplishes all responsibilities through coordination with the operational units and the CICA and operations support cell (OSC). The HOC tracks all HUMINT activities in the AOR. The J/G2X uses this information to advise the SIO on all HUMINT activities conducted within the AO. The HOC—

- Exercises technical control of all HUMINT assets and coordinates and deconflicts HUMINT activities in the deployed AO.
- Establishes and maintains a HUMINT source database.
- Coordinates and supervises HUMINT FP source operations conducted by all services and components in the AO.
- Develops and manages collection requirements for HUMINT in coordination with the requirements manager.
- Develops and provides the HUMINT portion of the intelligence synchronization plan to the J/G/S2X and requirements manager for inclusion in the intelligence synchronization plan.
- Coordinates the activities of HUMINT collectors assigned or attached to interrogations and debriefing facilities.
- Expedites preparation of intelligence information reports and their distribution to consumers at all levels.
- Performs liaison with HN and US national HUMINT organizations.

Operations Support Cell

6-52. The OSC in the *2X staff maintains the source registry for all HUMINT activities in the designated AOIR. The OSC provides management of intelligence property book operations, source incentive programs, and ICFs.

6-53. Integrating linguists and DOD emergency-essential civilians, such as technical support contractors, into the HUMINT team should take place as soon as possible. Security clearances and contractual agreements will help the team determine the level of integration.

6-54. Along with the basic briefing of what is expected of the civilian linguists as interpreters and the emergency-essential civilians as support personnel, HUMINT teams should be informed about the civilians' chain of command and the scope of their duties beyond interpreting and technical support. The HUMINT team leader must ensure that linguists and emergency-essential civilians are trained and capable of completing all tasks expected of them.

Counterintelligence Coordinating Authority

6-55. The CICA coordinates all CI activities for a deployed force. There can be only one CICA in a theater of operations. When multiple echelons exist, the highest echelon has the CICA and subordinate G2X offices have a CICA. Depending on the size and scope of the operation, the CICA could be the unified command's CI staff officer; the CI or HUMINT staff officer from corps or division; or a senior warrant officer or branch CI officer designated by the unified command CI staff officer or task force commander. For more information about the CICA functions, see Chapter 11.

HUMINT TEAM STRUCTURE

Operational Management Team

6-56. The OMT is a four-person team consisting of a warrant officer (WO), two noncommissioned officers (NCOs), and a junior enlisted soldier. Civilians may be inserted into this structure when appropriate. Rank structure and standards of grade for OMTs vary depending upon the skill sets required and mission focus. HUMINT OMTs provide operational guidance for two to four HUMINT teams, depending on mission focus and operational tempo. When two or more HUMINT teams are deployed in DS of a maneuver element, an OMT also deploys to provide technical control. The OMT works closely with the supported S2 and analysis and control team (ACT) to furnish current threat information and answer the supported commander's PIRs and IRs. OMTs coordinate with the supported 2X and manage subordinate HUMINT team echelons to—

- Provide guidance and technical control of operational activity.
- Provide the collection and operational focus for HUMINT teams.
- Provide quality control and dissemination of reports for subordinate HUMINT teams.
- Conduct single-discipline HUMINT analysis, and assist in mission analysis for the supported commander.

- Act as a conduit between subordinate HUMINT teams, the HOC, and supported unit headquarters.
- Provide administrative support for subordinate HUMINT teams, to include reporting mission and equipment status to the HOC and the supported unit headquarters.
- Educate the supported commander on the capabilities of the HUMINT teams.
- Integrate the HUMINT teams directly into the maneuver commander's ISR planning.

HUMINT Team

6-57. The HUMINT team is a four-person team consisting of two NCOs and two junior enlisted personnel. Civilians may be inserted into this structure when appropriate. Rank structure and standards of grade for HUMINT teams vary depending upon the skill sets required and the mission focus. HUMINT teams are trained to execute the full range of HUMINT functions as defined in **HUMINT FUNCTIONS** section. However, they may be assigned to mission-focused elements such as DOCEX, interrogation, debriefing, or contact operations.

Chapter 7

Imagery Intelligence

DEFINITION

7-1. IMINT is intelligence derived from the exploitation of imagery collected by visual photography, infrared, lasers, multi-spectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media.

ROLE

7-2. The role of imagery is to assist the commander in focusing and protecting his combat power. Imagery often enhances the commander's situational understanding of the battlespace. Other than direct human observation, imagery is the only intelligence discipline that allows the commander to see the battlefield in real time as the operation progresses. In those cases where maps are not available, digital imagery in hardcopy or softcopy can be used as a substitute. Imagery can also be used to update maps or produce grid-referenced graphics. Detailed mission planning often requires imagery, to include three-dimensional stereo images, in order to provide the degree of resolution necessary to support such specialized planning.

FUNDAMENTALS

7-3. Some imagery assets are very responsive to the individual commander's intelligence requirements. Some imagery systems can directly transmit imagery into the tactical operations center (TOC); examples include imagery from UAVs and the Joint Surveillance Target Attack Radar System (JSTARS). This direct downlink enables the G2/S2 to use the imagery as soon as possible instead of having to wait for finished imagery products. A note of caution is required, however, if not a trained imagery analyst because the G2/S2 could incorrectly interpret the imagery.

7-4. Imagery-related equipment has undergone a reduction in size as well as a reduction in the time it takes to provide products, particularly softcopy imagery. The modularity and size reduction of imagery analysis, processing, and display systems make transport easier; they also allow the commander to bring lesser amounts than in the past, while still retaining those systems (or subsystems) required to complete the mission. Additionally, data compression allows faster transmission of imagery products directly to the warfighter.

SOURCES OF IMAGERY

7-5. There are three general sources of imagery: national, civil, and commercial. National imagery traditionally refers to imagery collected by DOD imagery systems. However, there are other sources of imagery provided

by non-national sources such as handheld photography (film, digital, and video), UAV imagery, and gun-camera images.

National

7-6. National systems are developed specifically for supporting the President of the United States, the Secretary of Defense, other national agencies, and US military forces. These systems respond to the needs of the nation and those of the combatant commands.

Civil

7-7. Civil imagery systems are usually government funded in terms of building, launching, and operating the system. In many, but not all, cases the agencies operating these civil imagery systems also process, distribute, and archive the imagery data or images.

Commercial

7-8. Commercial companies build, launch, and operate imagery systems for profit. In times of crises, license agreements with the US Government obligate US commercial satellite imaging systems to provide data only to the US Government at the market value. This protects information concerning US operations from adversarial exploitation from commercial systems such as the ACE Imagery Company. However, foreign commercial imagery systems are not bound to this arrangement, and thus may be used by our nation's adversaries. Commercial imagery has become increasingly valuable for many reasons:

- Due to its unclassified nature, civil and commercial imagery is useful in an open environment, may be released to multinational partners, and can be made available to the press. They are especially useful for geospatial products. Their use allows national systems more time to focus on other intelligence functions.
- Civil and commercial imagery offer radar and multi-spectral. Some offer large area collection useful for broad area coverage purposes.
- Commercial satellite imagery resolution varies from less than one meter to several kilometers.

7-9. The Central Imagery Tasking Office (CITO) is responsible for ordering commercial imagery. The Commercial Satellite Imagery Library is available to research DOD purchased commercial imagery. The G2/S2 should consult the CITO when forming commercial imagery requests. NGA will deliver the imagery primarily on CD-ROM media via courier or mail service. Limited digital or electronic delivery is available as well.

TYPES OF IMAGERY SENSORS

7-10. There are four types of imagery sensors: visible (optical), infrared, radar, and multi-spectral. Each sensor has a unique capability, with distinct advantages and disadvantages. The G2/S2 must understand each sensor's capability in order to select the best sensor for the mission and thus enable the user to better understand the intelligence received. Certain sensors are better suited for military operations than others. (See Table 7-1.)

Table 7-1. Sensor Characteristics Matrix.

SENSORS	ADVANTAGES	DISADVANTAGES
Visible (Optical) Best tool for daytime, clear weather, detailed analysis. Includes video and electro-optical.	• Affords a familiar view of a scene. • Offers system resolution that cannot be achieved in other optical systems or in thermal images and radars. • Preferred for detailed analysis and mensuration. • Offers stereoscopic viewing.	• Restricted by terrain and vegetation. • Limited to daytime use only. • Reduced picture size.
Infrared Best tool for nighttime, clear weather, detailed analysis. Includes Overhead Non-Imaging Infrared (ONIR).	• A passive sensor and is impossible to jam. • Offers camouflage penetration. • Provides good resolution. • Nighttime imaging capability.	• Not effective during thermal crossover periods. • Product not easily interpretable. • Requires skilled analysis. • Cannot penetrate clouds.
Radar Useful for detecting presence of objects at night and in bad weather. Includes synthetic aperture radar (SAR), coherent change detection (CCD), and MTI.	• All weather; can penetrate fog, haze, clouds, smoke. • Day or night use. • Does not rely on visible light nor thermal radiation. • Good standoff capability. • Large area coverage. • Allows moving target detection. • Foliage and ground penetration.	• Product not easily interpretable. • Requires skilled analysis. • Terrain masking inhibits use.
Multi-Spectral Imagery (MSI) Best tool for mapping purposes and terrain analysis.	• Large database available. • Band combinations can be manipulated to display desired requirements. • Images can be merged with other digital data to provide higher resolution.	• Product not easily interpretable. • Requires skilled analysis. • Computer manipulation requires large amounts of memory and storage; requires large processing capabilities.

PLAN

7-11. The first step in planning for IMINT is determining the need for IMINT products based on the PIRs and the initial IPB. The G2/S2 should research targets using online imagery databases early and request those imagery products that are not perishable for contingency planning. National and COCOM imagery databases may hold recently imaged targets that could meet the commander's immediate needs instead of requesting new imagery. The staff must clearly articulate their intelligence requirements to include communicating what the mission is and how the requested product will aid in mission accomplishment. The G2/S2 should submit the imagery requirement

using established procedures such as those in the unit's SOP or as established by the COCOM.

7-12. The G2/S2 must also determine the specific imagery requirements so as not to burden the system with unnecessary requests. The desire for imagery products often exceeds the capabilities of the IMINT system. Therefore, it is imperative that the G2/S2 consider what type of analysis they require, and request only that which they require. The specifications of the request for IMINT products often affect the timeliness of the response. For example, determining if vehicles are tanks takes less time and requires less resolution than determining if a tank is a T-64 or a T-72.

7-13. Here are some of the roles IMINT can perform that the G2/S2 may consider when determining IMINT requirements:

- Imagery can detect and/or identify and locate specific unit types, equipment, obstacles, potential field fortifications, etc., from which intelligence analysts are able to analyze enemy capabilities and develop possible COAs.
- Imagery can also update maps and enhance the interpretation of information from maps. Detailed mission planning uses imagery to include stereo images for three-dimensional viewing of the terrain and many other geospatial uses.
- Imagery can be used as a substitute for maps when maps are not available. The most common application of this technique is by constructing imagery mosaics: a combination of two or more overlapping photographic prints that form a single picture.
- MTI displays or products can provide an NRT picture of an entity's movement by indicating its speed, location, and direction of travel. MTI systems do not differentiate friendly from enemy. Imagery assets, particularly MTI systems, are useful in cueing other ISR systems.
- Imagery can be used to support protection of the force by helping the commander visualize how his forces look—including their disposition, composition, and vulnerabilities—as exploited by enemy IMINT systems.
- Imagery analysts use combat assessment imagery to confirm destruction, determine the percentage of destruction, or whether the target was unaffected.

PREPARE

7-14. The G2/S2 IMINT-related actions during the prepare function of the intelligence process include establishing or verifying the portion of the intelligence communications architecture that supports IMINT display and analysis functions properly. Additionally, the G2/S2 must ensure that required IMINT analytical assets and resources are prepared to provide support or are available through intelligence reach. Lastly, the G2/S2 must also ensure IMINT reporting and dissemination channels and procedures are in place and rehearsals are conducted with all pertinent IMINT elements to ensure interoperability.

COLLECT

7-15. As previously mentioned, there are four types of imagery sensors. Depending on the type of sensor, it can record hardcopy or softcopy single frame or continuous (video). A given imagery target will not necessarily receive continuous coverage due to the possible conflict between the number and priority of targets and the number and availability of imagery assets. However, a commander may decide to have continuous surveillance of certain targets, for specified periods of time, usually using his own imagery assets (for example, UAV) even though this detracts from the commander's ability to use these assets for other imagery targets within his AOI.

PROCESS

7-16. The process function regarding IMINT involves converting imagery data into a form that is suitable for performing analysis and producing intelligence. Examples of IMINT processing include developing film, enhancing imagery, converting electronic data into visual displays or graphics, and constructing electronic images from IMINT data.

PRODUCE

7-17. The IMINT producer must ensure the IMINT product satisfies the associated intelligence requirements and that the product is in the required format. The quality and resolution of the product is highly dependent upon the type of sensor, the time of day, and the weather conditions, as well as the imagery analyst's ability to identify items, vehicles, equipment, and personnel within the images. Specific IMINT products are discussed in the ANALYZE section below.

ANALYZE

7-18. Timeliness is critical not only to IMINT collection but also to IMINT analysis and reporting. It is difficult to separate IMINT reporting from IMINT analysis in this discussion. This is demonstrated by the three phases of IMINT reporting presented below; all are dependent upon the timeliness requirements. Each phase represents a different degree of analysis and period of time available to accomplish the exploitation of the imagery.

- First Phase imagery analysis is the rapid exploitation of newly acquired imagery and reporting of imagery-derived information within a specified time from receipt of imagery. This phase satisfies priority requirements of immediate need and/or identifies changes or activity of immediate significance. First Phase imagery analysis results in an Initial Phase Imagery Report (IPIR).
- Second Phase imagery analysis is the detailed exploitation of newly acquired imagery and the reporting of imagery-derived intelligence and information while meeting the production and timeliness requirements. Other intelligence discipline source material may support phase two imagery as appropriate. Second phase imagery analysis results in a Supplemental Imagery Report (SUPR).
- Third Phase imagery analysis is the detailed analysis of all available imagery pertinent to an SIR, and the subsequent production and reporting resulting from this analysis within a specified time. This

phase provides an organized detailed analysis of an imagery target or topic, using imagery as the primary data source but incorporating data from other sources as appropriate.

7-19. The two types of imagery exploitation are national and direct support (DS).

- National exploitation is imagery exploitation that supports presidential requirements, National Security Council (NSC) requirements, congressional requirements, or requirements of a common concern to the intelligence community.
- DS exploitation is imagery exploitation that supports assigned missions of a single agency, department, or command (the warfighter).

7-20. IMINT assets will complete DS exploitation in order to satisfy (First Phase) requirements and report the results as soon as possible, but not later than 24 hours after receipt of the imagery. Collectors will complete national exploitation in order to satisfy (Second and Third Phases) requirements and report the results within the time specifications of each individual requirement.

DISSEMINATE

7-21. IMINT products are distributed or disseminated in hardcopy, softcopy, or direct viewing such as through remote terminals. The distribution of hardcopy products will be via couriers or other type of mail system. The dissemination of softcopy products will be either as hardcopy products (for example, CD-ROM and 3.5-inch disks) or electronically. The requestor must ensure that the requested product is transmittable over the available communications systems.

ASSESS

7-22. The requestor should immediately assess the imagery product upon receipt for accuracy and relevance to the original request. The requestor must then notify the producer and inform him of the extent to which the product answered the PIR. Providing feedback to the producer regarding the product helps ensure the producer will provide the required information in the correct format. The following are some of the questions which the requestor should consider when providing feedback to the producer.

- Is the format of the product acceptable?
- Is additional information needed on the product or future products?
- Is excess information included on the product?

Chapter 8

Signals Intelligence

DEFINITION

8-1. SIGINT is a category of intelligence comprising either individually or in combination all COMINT, ELINT, and FISINT, however transmitted; intelligence is derived from communications, electronics, and foreign instrumentation signals. SIGINT has three subcategories:

- COMINT – The intelligence derived from foreign communications by other than the intended recipients.
- ELINT – The technical and geo-location intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.
- FISINT – Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. (See JP 1-02)

8-2. SIGINT provides intelligence to the commander based upon intercepted communications and provides transmitter location data.

ROLE

8-3. SIGINT provides intelligence on threat capabilities, disposition, composition, and intentions. In addition, SIGINT provides targeting information for the delivery of lethal and non-lethal effects.

FUNDAMENTALS

8-4. It is important that the G2/S2 understand how SIGINT assets are organized not only within the Army but also throughout the DOD. The majority of SIGINT assets are located at EAC. SIGINT assets from all the armed services, combined with national SIGINT assets, work together to support commanders from the tactical to the strategic level. Only by understanding the SIGINT structure that transcends traditional service component boundaries can the G2/S2 understand how to use SIGINT effectively.

TECHNICAL CONTROL AND ANALYSIS ELEMENT (TCAE) ARCHITECTURE

8-5. The TCAE architecture supports Army SIGINT collectors and analysts by providing SIGINT-specific intelligence and guidance to SIGINT personnel. The SIGINT technical architecture complements existing C2 relationships; it does not replace the commander's authority or chain of command.

8-6. There is a TCAE at each Army operational echelon. The TCAE at each echelon provides a single POC and resource dedicated to supporting the commander at that level. TCAEs or SIGINT elements at varying echelons draw information from each other in order to provide a more complete and detailed intelligence picture for their respective commanders.

ARMY TCAE (ATCAE)

8-7. The ATCAE, established at the national level, plays a significant role in TCAE operations by providing technical support oversight and providing access to national databases—in coordination with the NSA and other intelligence organizations. Additionally, the ATCAE works closely with NSA's IO element assisting in operations, monitoring technical capabilities, and providing liaison with Army's 1st Information Operations Command (Land). (This unit was previously called Land Information Warfare Activity.)

8-8. The ATCAE supports the Army's Quick Reaction Capability (QRC) SIGINT and signals research and target development (SRTD) operations. The QRC systems are responsive to the ground force commander's requirements and allow the ability to conduct SIGINT operations against modern communications systems.

REGIONAL TCAE (RTCAE)

8-9. The Army established RTCAEs to allow supported units at all echelons access to SIGINT regarding their respective AOI. The Army placed an RTCAE within each Regional Security Operations Center (RSOC). An RSOC is a joint service facility established by the Director, NSA, to conduct continuous security operations on selected targets in support of national and warfighter intelligence requirements using remoting technologies. The RSOC embeds a focus on the tactical commander's SIGINT requirements at a national level. It also creates a framework for enhanced interoperability among service SIGINT activities, especially within the context of a deployed JTF.

8-10. In addition to each RSOC, the RTCAE works closely with Theater TCAEs as well as Corps and Division SIGINT elements with the same regional focus. It provides analytic support and tailored products and answers RFIs. During peacetime and real-world operations RTCAEs facilitate intelligence reach support. They provide tailored technical support packages, support for surge and survey operations, analytic expertise, and signal data access and digital file transfers of live collection for Army tactical units.

THEATER TCAE

8-11. The Theater TCAE performs SIGINT and EW technical control and analysis and management. It provides SIGINT technical support for assigned, OPCON, and lower echelon SIGINT resources deployed in the theater. This includes mission tasking, processing, analyzing, and reporting of SIGINT data, information, and intelligence. The TCAE provides direction for the Theater Collection and Exploitation Battalion's SIGINT mission and for other theater tactical SIGINT assets.

SIGINT THEATER INTELLIGENCE BRIGADE/GROUP (TIB/TIG)

8-12. The TIB/TIG conducts operational level multidiscipline SIGINT operations. It provides timely intelligence to the commander throughout the full spectrum of operations. The TIB/TIG is structured to provide ground and aerial SIGINT support. It executes the full range of SIGINT missions or tasks.

SIGINT AT ECHELONS CORPS AND BELOW

8-13. There is a varying mixture of SIGINT assets within each corps. A reference listing the types of SIGINT assets found at echelons corps and below is listed in ST 2-50.

PLAN

8-14. An important SIGINT planning consideration is that if at all possible, SIGINT collection should be employed in conjunction with another intelligence discipline collection system. SIGINT is often used to cue, and be cued by, other ISR assets.

8-15. During planning, the G2/S2 should retrieve, update, or develop any required SIGINT databases. This includes effecting coordination with other SIGINT assets or elements that can support the operation.

8-16. SIGINT ground collection assets are usually placed in proximity to enemy signal sources due to the limited height of collector antennas, the low power output of threat or enemy emitters, and the line-of-sight (LOS) constraints imposed by terrain. Ground-based SIGINT teams are most effective when positioned to—

- Maximize threat emitter interception. This allows teams to overcome the constraints of threat emitter characteristics usually allowed by proximity to the threat.
- Minimize system receiver interference. This increases the potential capability of the team to acquire threat emitters in a timely manner.
- Optimize overlapping areas of intercept coverage. This ensures coverage of the AOIR and allows targets to be handed off from team to team if necessary.

8-17. Aerial SIGINT assets have additional planning requirements. Coordination must be effected with Army Airspace Command and Control (A2C2) for ingress and egress routes, restricted operating zones (ROZs) where the aircraft can travel on an intercept track, as well as with the supporting air operations center to determine the availability of asset types and times.

PREPARE

8-18. The G2/S2 ensures the SIGINT unit and asset leaders have effected all necessary coordination and conducted rehearsals. This includes establishing or verifying the operation of the SIGINT technical architecture. The G2/S2 also ensures all required SIGINT assets and resources are available, SIGINT reporting and dissemination channels and procedures are in place, and connectivity and interoperability exist with all pertinent SIGINT elements.

8-19. SIGINT OPCON is the authoritative direction of SIGINT activities, including tasking and allocation of effort, and the authoritative prescription

of those uniform techniques and standards by which SIGINT information is collected, processed, and reported.

8-20. SIGINT operational tasking is the authoritative operational direction of and direct levying of SIGINT information needs by a military commander on designated SIGINT resources. These requirements are directive, regardless of other priorities, and are conditioned only by the capability of those resources to produce such information. Operational tasking includes authority to deploy all or part of the SIGINT resources for which SIGINT operational tasking authority (SOTA) has been delegated.

8-21. SOTA is the military commander's authority to operationally direct and levy SIGINT requirements on designated SIGINT resources; it includes authority to deploy and redeploy all or part of the SIGINT resources for which SOTA has been delegated.

COLLECT

8-22. SIGINT performs two major collection activities: signals intercept and direction finding (DF).

Signals Intercept

8-23. Signals intercept are those SIGINT actions used to search for, intercept, and identify threat electromagnetic signals for the purpose of immediate threat recognition. Signals intercept provides information required to answer PIRs, and other intelligence requirements in support of the ISR effort.

Direction Finding

8-24. Even when threat radio operators use COMSEC procedures, SIGINT teams can often intercept and approximate the location of the threat's signals. Specifically, SIGINT teams can use DF to determine—

- Movement of threat personnel or equipment.
- Locations of emitters associated with weapon systems and units.
- New emitter locations and confirm known emitter locations.
- Possible friendly targets the enemy intends to attack (lethal and non-lethal).

8-25. In addition to finding threat forces, DF operations can assist the (radio-equipped) friendly force by—

- Locating and vectoring assets or units during limited visibility.
- Locating downed aircraft and personnel radio beacons.
- Conducting signal security assessments.
- Locating sources of communication interference and jamming.

PROCESS

8-26. SIGINT processing involves converting intercepts of SIGINT into written and verbal reports, automated message, graphic displays, recordings, and other forms suitable for analysis and intelligence production. Since US forces routinely conduct operations against adversaries who speak languages other than English, SIGINT processing often also includes translation of these intercepts.

8-27. Due to the complexity of many SIGINT systems, automated processing may occur several times before SIGINT data or information receives any human interaction.

PRODUCE

8-28. The SIGINT producer must ensure the SIGINT product satisfies the associated intelligence requirements and that the product is in the required format. The quality, fidelity, and timeliness of SIGINT products are highly dependent upon the type of intercept, the collection system, the system's position in relation to the threat emitter, the weather (including space-based weather), as well as the SIGINT operator's ability to identify the appropriate threat signal activity.

8-29. SIGINT production results in some of the reports and formats mentioned in the process section above; however, the objective for SIGINT is to be used in an all-source analytical approach.

ANALYZE

8-30. The intelligence staff analyzes intelligence and information about the enemy's communications capabilities to determine appropriate SIGINT collection strategies. Conversely, a corresponding analysis of the friendly forces' SIGINT capabilities must be conducted to ensure the continued effectiveness of, or to improve upon, SIGINT collection.

8-31. SIGINT analysts also sort through large amounts of SIGINT and information and intelligence to identify and use only that which is pertinent to the CCIRs (PIRs and FFIRs).

DISSEMINATE

8-32. SIGINT of critical importance to the force, including answers to the CCIRs (PIRs and FFIRs), is disseminated via the most expeditious means possible. Due to the usually highly perishable nature of SIGINT, the most expeditious reporting means is often immediately augmented with a follow-up report or augmented by a report transmitted through additional means, enhancing the probability of receipt. Sometimes the most expeditious means of reporting critical SIGINT information to the commander is face to face.

8-33. For intelligence reach operations, SIGINT products are available and disseminated in a variety of forms: hardcopy, softcopy, direct viewing, or listening (television or radio). It is incumbent on the requestor to ensure that the SIGINT product can be transmitted over the available communications systems. This includes verifying the appropriate security level of the communications system.

ASSESS

8-34. The primary goal of the assess function when applied to SIGINT is to determine whether the results of SIGINT collection meet the requirements of the unit's ISR effort. SIGINT producers must assess all facets of SIGINT operations, from receipt of the ISR task to the dissemination of SIGINT, in an effort to determine their effectiveness. This assessment is not only directed at each SIGINT asset individually but also throughout the supporting SIGINT architecture and the unit's entire ISR effort.

8-35. The G2/S2 immediately assesses SIGINT products upon receipt for accuracy and relevance. He must inform the SIGINT producer of the extent to which the product answered the PIR or intelligence requirement. Providing feedback to the SIGINT producer—and collector—helps improve the effectiveness and efficiency of SIGINT.

Chapter 9

Measurement and Signatures Intelligence

DEFINITION

9-1. MASINT is technically derived intelligence that detects, locates, tracks, identifies, and/or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from IMINT and SIGINT collection.

9-2. MASINT collection systems include but are not limited to radar, spectroradiometric, E-O, acoustic, RF, nuclear detection, and seismic sensors, as well as techniques for gathering NBC and other material samples.

9-3. It requires the translation of technical data into recognizable and useful target features and performance characteristics. Computer, communication, data, and display processing technologies now provide MASINT in support of commanders throughout the full spectrum of operations.

9-4. The subdisciplines within MASINT include, but are not limited to, the following:

- **Radar Intelligence (RADINT).** The active or passive collection of energy reflected from a target or object by LOS, bistatic, or over-the-horizon radar systems. RADINT collection provides information on radar cross-sections, tracking, precise spatial measurements of components, motion and radar reflectance, and absorption characteristics for dynamic targets and objectives. A SAR system, coupled with advanced MASINT processing techniques—
  - Provides a high resolution, day and night collection capability.
  - Can produce a variety of intelligence products that identify or provide change detection, terrain mapping, underwater obstacles, dynamic sensing of targets in clutter, and radar cross-section signature measurements.
- **Frequency Intelligence.** The collection, processing, and exploitation of electromagnetic emissions from a radio frequency weapon (RFW), an RFW precursor, or an RFW simulator; collateral signals from other weapons, weapon precursors, or weapon simulators (for example, electromagnetic pulse signals associated with nuclear bursts); and spurious or unintentional signals.
  - *Electromagnetic Pulses*. Measurable bursts of energy that result from a rapid change in a material or medium, resulting in an explosive force, produces RF emissions. The RF pulse emissions associated with nuclear testing, advanced technology devices, power and propulsion systems, or other impulsive events can be used to detect, locate, identify, characterize, and target threats.

- *Unintentional Radiation Intelligence (RINT).* The integration and specialized application of MASINT techniques against unintentional radiation sources that are incidental to the RF propagation and operating characteristics of military and civil engines, power sources, weapons systems, electronic systems, machinery, equipment, or instruments. These techniques may be valuable in detecting, tracking, and monitoring a variety of activities of interest.

- **E-O Intelligence.** The collection, processing, exploitation, and analysis of emitted or reflected energy across the optical portion (ultraviolet, visible, and infrared) of the EMS. MASINT E-O provides detailed information on the radiant intensities, dynamic motion, spectral and spatial characteristics, and the materials composition of a target. E-O data collection has broad application to a variety of military, civil, economic, and environmental targets. E-O sensor devices include radiometers, spectrometers, non-literal imaging systems, lasers, or laser radar (LIDAR).
  - *Infrared Intelligence (IRINT).* A subcategory of E-O that includes data collection across the infrared portion of the EMS where spectral and thermal properties are measured.
  - *LASER Intelligence (LASINT).* Integration and specialized application of MASINT E-O and other collection to gather data on laser systems. The focus of the collection is on laser detection, laser threat warning, and precise measurement of the frequencies, power levels, wave propagation, determination of power source, and other technical and operating characteristics associated with laser systems—strategic and tactical weapons, range finders, and illuminators.
  - *Hyperspectral Imagery (HSI).* A subcategory of E-O intelligence produced from reflected or emitted energy in the visible and near infrared spectrum used to improve target detection, discrimination, and recognition. HSI can detect specific types of foliage—supporting drug-crop identification; disturbed soil—supporting the identification of mass graves, minefields, caches, underground facilities or cut foliage; and variances in soil, foliage, and hydrologic features—often supporting NBC contaminant detection.

- **Spectroradiometric Products.** Include E-O spectral (frequency) and radiometric (energy) measurements. A spectral plot represents radiant intensity versus wavelength at an instant in time. The number of spectral bands in a sensor system determines the amount of detail that can be obtained about the source of the object being viewed. Sensor systems range from multispectral (2 to 100 bands) to hyperspectral (100 to 1,000 bands) to ultraspectral (1,000+ bands). More bands provide more discrete information, or greater resolution. The characteristic emission and absorption spectra serve to fingerprint or define the makeup of the feature that was observed. A radiometric plot represents the radiant intensity versus time. An example is the radiant intensity plot of a missile exhaust plume as the missile is in flight. The intensity or brightness of the object is a function of several conditions including its temperature, surface properties or material, and how fast it is moving. For each point along a time-intensity

radiometric plot, a spectral plot can be generated based on the number of spectral bands in the collector.

- **Geophysical Intelligence.** Geophysical MASINT involves phenomena transmitted through the earth (ground, water, atmosphere) and manmade structures including emitted or reflected sounds, pressure waves, vibrations, and magnetic field or ionosphere disturbances.
  - *Seismic Intelligence*. The passive collection and measurement of seismic waves or vibrations in the earth surface.
  - *Acoustic Intelligence*. The collection of passive or active emitted or reflected sounds, pressure waves or vibrations in the atmosphere (ACOUSTINT) or in the water (ACINT). ACINT systems detect, identify, and track ships and submarines operating in the ocean.
  - *Magnetic Intelligence*. The collection of detectable magnetic field anomalies in the earth's magnetic field (land and sea). An example is a Remotely Emplaced Battlefield Surveillance System (REMBASS) sensor detection indicating the presence and direction of travel of a ferrous object.
- **Nuclear Intelligence (NUCINT).** The information derived from nuclear radiation and other physical phenomena associated with nuclear weapons, reactors, processes, materials, devices, and facilities. Nuclear monitoring can be done remotely or during onsite inspections of nuclear facilities. Data exploitation results in characterization of nuclear weapons, reactors, and materials. A number of systems detect and monitor the world for nuclear explosions, as well as nuclear materials production.
- **Materials Intelligence.** The collection, processing, and analysis of gas, liquid, or solid samples. Materials intelligence is critical to collection against NBC warfare threats. It is also important to analyzing military and civil manufacturing activities, public health concerns, and environmental problems. Samples are both collected by automatic equipment, such as air samplers, and directly by humans. Samples, once collected, may be rapidly characterized or undergo extensive forensic laboratory analysis to determine the identity and characteristics of the sources of the samples.

ROLE

9-5. MASINT provides intelligence to the commander throughout the full spectrum of operations to facilitate situational understanding. MASINT can thwart many of the camouflage, concealment, and deception techniques currently used to deceive ISR systems.

9-6. MASINT is perceived as a "strategic" discipline with limited "tactical" support capabilities. But, by application of real-time analysis and dissemination, MASINT has a potential ability to provide real-time situation awareness and targeting not necessarily available to the classic disciplines. Specifically, MASINT "sensors" have unique capabilities to detect missile launch, detect and track aircraft, ships, and vehicles; do non-cooperative target identification (NCTI), combat assessment, and BDA; and detect and track fallout from nuclear detonations. Often, these contributions are the first indicators of hostile activities. For example, two EXOCET-equipped

Mirage F-1s were shot down during the Operation DESERT STORM due to MASINT collection and analysis. As evidenced by Operation IRAQI FREEDOM (OIF), MASINT will play a decisive role in the targeting of smart munitions with the signatures (fingerprint) of the targets they are seeking (for example, infrared signatures).

9-7. The MASINT systems most familiar on today's battlefield are employed by ground surveillance and NBC reconnaissance elements.

9-8. MASINT spans the entire EMS and its capabilities complement, rather than compete with, the other intelligence disciplines. MASINT provides, to varying degrees, the capability to—

- Use automatic target recognition (ATR) and aided target recognition (AiTR).
- Penetrate manmade and/or natural camouflage.
- Penetrate manmade and/or natural cover, including the ability to detect subterranean anomalies or targets.
- Counter stealth technology.
- Detect recently placed mines.
- Detect natural or manmade environmental disturbances in the earth's surface not discernible through other intelligence means.
- Provide signatures (target identification) to munitions and sensors.
- Enhance passive identification of friend or foe.
- Detect the presence of NBC agents to include prior to, during, or after employment.
- Detect signature anomalies that may affect target-sensing systems.

FUNDAMENTALS

9-9. Before discussing the functions of the intelligence process within a MASINT, the following paragraph provides an overview of organizational structure of MASINT.

9-10. Within DOD, the DIA provides central coordination for MASINT collection efforts through the Central MASINT Office. Each service, in turn, has a primary command or staff activity to develop requirements and coordinate MASINT effort. Army responsibility currently resides with INSCOM. Army weapons systems programs that require MASINT information to support system design or operations submit requests through the Army Reprogramming Analysis Team (ARAT) or INSCOM channels for data collection and processing. The S&TI community also performs MASINT collection and processing primarily to support R&D programs and signature development. Every S&TI center has some involvement in MASINT collection or production that reflects that center's overall mission (for example, NGIC does work on armored vehicles and artillery). Service R&D centers such as the Communications-Electronics Command (CECOM) Research, Development, and Engineering Center (RDEC), and Night Vision and Electronic Systems Laboratory are also involved in developing sensor systems for collecting and processing MASINT.

9-11. In addition to supporting the S&TI mission, INSCOM units also execute limited ground-based operational collection to support Theater and ASCC PIRs. This capability will expand upon the standup of INSCOM TIBs and TIGs.

PLAN

9-12. Some MASINT sensors can provide extremely specific information about detected targets, whereas other sensors may only be capable of providing an indication that an entity was detected. Additionally, there are varying capabilities of detection, identification, and classification among MASINT sensors. It is these varying capabilities that require synchronizing the employment of MASINT sensors both within the MASINT discipline and within the ISR effort as a whole. See FM 2-01 for more specific information on ISR synchronization.

9-13. As previously mentioned, there are many types of MASINT sensors. Depending on the type of sensor employed, a given MASINT collection target or NAI may not necessarily receive continuous coverage due to the possible conflict between the number and priority of targets and the number and availability of MASINT assets. However, a commander may decide to have continuous surveillance of certain targets by using his own MASINT assets (for example, REMBASS or Improved-REMBASS).

9-14. Another consideration when planning MASINT missions is whether to use active, passive, or a combination of both when planning MASINT coverage.

PREPARE

9-15. The G2/S2 MASINT related actions during the prepare function of the intelligence process include properly establishing or verifying the MASINT portion of the intelligence communications architecture functions. Additionally, the G2/S2 must ensure that required MASINT analytical assets and resources are prepared to provide support or are available through intelligence reach. Since the products of MASINT are not as well known as products from other intelligence disciplines, the G2/S2 must be aware of the types of MASINT products available to support the operation, and then educate the rest of his unit's staff on the use of these MASINT products. Lastly, the G2/S2 must also ensure MASINT reporting and dissemination channels and procedures are in place and rehearsals are conducted with all pertinent MASINT elements to ensure interoperability.

COLLECT

9-16. MASINT provides information required to answer PIRs and other intelligence requirements in support of the ISR effort. As stated earlier in this chapter, MASINT collection must not only be synchronized within its own discipline but also be synchronized and integrated into the unit's overall ISR effort in order to be effective.

9-17. MASINT sensors are employed throughout the full spectrum of operations from a variety of platforms—sub-surface, ground, marine, and aerospace.

PROCESS

9-18. Just as in the other intelligence disciplines, MASINT involves dealing with huge volumes of data that have to be processed before beginning analysis and production. The process function regarding MASINT involves converting esoteric data into a form that is suitable for performing analysis and producing intelligence. MASINT processing can include relatively simple actions such as converting a REMBASS sensor activation into a report, to a complex task such as processing HSI into a report identifying the composition and concentrations of carcinogenic chemicals present in the emissions from a factory upwind from a US forces encampment.

PRODUCE

9-19. Effective and timely MASINT requires personnel with diverse skill sets. The MASINT producer must ensure the MASINT product satisfies the associated intelligence requirements and that the product is in the required format. The quality, fidelity, and timeliness of MASINT products are highly dependent upon the type of target, the collection system, the system's position in relation to the target or NAI, and the weather, as well as the MASINT system operator's ability to identify the appropriate threat activity.

9-20. The objective of MASINT production is to be used in an all-source analytical approach.

ANALYZE

9-21. The intelligence staff analyzes intelligence and information about the enemy's equipment, doctrine, and TTP to determine appropriate MASINT collection strategies. Conversely, a corresponding analysis of the friendly force's MASINT capabilities must be conducted to ensure the continued effectiveness of, or to improve upon, MASINT collection.

DISSEMINATE

9-22. MASINT of critical importance to the force, including answers to the PIRs, is disseminated via the most expeditious means possible.

9-23. For intelligence reach operations, MASINT products are available and disseminated in a variety of forms. The requestor must ensure that the MASINT product can be transmitted over the available communications systems. This includes verifying the appropriate security level of the communications system.

ASSESS

9-24. The primary goal of the MASINT assess function is to determine whether the results of MASINT collection and production meet the requirements of the unit's ISR effort. MASINT producers must assess all facets of MASINT operations, from receipt of the ISR task to the dissemination of MASINT, in an effort to determine the effectiveness of MASINT. This assessment is not only directed at each MASINT asset individually but also throughout the supporting intelligence communications architecture, to include intelligence reach and the unit's entire ISR effort.

9-25. Also, the G2/S2 immediately assesses MASINT products upon receipt for accuracy and relevance. He must inform the MASINT producer of the extent to which the product answered the PIR or intelligence requirement. Providing feedback to the MASINT producer—and collector—helps improve the effectiveness and efficiency of MASINT.

Chapter 10

Technical Intelligence

DEFINITION

10-1. TECHINT is intelligence derived from the collection and analysis of threat and foreign military equipment and associated materiel.

ROLE

10-2. The strength of the US military lies, in part, to the diversity and extent of its technology base. While the US aspires to be the leader in integrating technology, the threat can achieve temporary technological advantage in certain areas by acquiring modern systems or capabilities. The world arms market is willing to provide these advanced systems to countries or individuals with the resources to pay for them. A concerted TECHINT program is vital to providing precise direction and purpose within the US R&D process to ensure quick and efficient neutralization of this advantage.

10-3. The role of TECHINT is to ensure that the warfighter understands the full technological capabilities of the threat. With this understanding, the warfighter can adopt appropriate countermeasures, operations, and tactics.

10-4. TECHINT has two goals within its role:

- To ensure the US armed forces maintain technological advantage against any adversary.
- To provide tailored, timely, and accurate TECHINT support to the warfighter throughout the entire range of military operations. This includes providing US forces intelligence, information, and training on foreign weapons systems to an extent that allows their use of CEE.

FUNDAMENTALS

10-5. The G2/S2 must understand how TECHINT assets are organized in order to properly apply the intelligence process, as the majority of TECHINT assets are located at EAC.

DEFENSE INTELLIGENCE AGENCY

10-6. DIA manages and reviews overall TECHINT activities. The S&TI Directorate within DIA is the action element for TECHINT. This directorate coordinates with external TECHINT agencies on non-policy matters concerning the production of S&TI. The following organizations provide TECHINT support under the control of DIA:

- **Armed Forces Medical Intelligence Center (AFMIC).** AFMIC, based at Fort Detrick, MD, is a DOD intelligence production center under DIA control. AFMIC is responsible for exploiting foreign medical materiel. The director supports the Army Foreign Materiel Exploi-tation

Program (FMEP) and Army medical R&D requirements. The director coordinates planning, programming, and budgeting with the Army Deputy Chief of Staff, Intelligence (DCS, G2).

- **Missile and Space Intelligence Center (MSIC).** MSIC, based at Redstone Arsenal, AL, is a DOD intelligence production center under DIA control and supports the FMEP. The MSIC acquires, produces, maintains, and disseminates S&TI pertaining to missile and space weapons systems, subsystems, components, and activities. The S&TI produced at MSIC also covers foreign state-of-the-art technology and research applicable to missiles.
- **Defense HUMINT Service.** DHS conducts worldwide HUMINT operations in support of foreign materiel acquisition (FMA) and foreign materiel exploitation (FME).

10-7. The organizations and agencies discussed below constitute the Army TECHINT structure.

ARMY DCS, G2

10-8. The Army DCS, G2 exercises general staff responsibility for all Army TECHINT activities. The Army DCS, G2 forms policies and procedures for S&TI activities, supervises and carries out the Army S&TI program, coordinates DA staff and MSC requirements for TECHINT, and is responsible for the Army Foreign Materiel Program (FMP).

INSCOM

10-9. Under the direction of Headquarters, Department of the Army (HQDA), INSCOM is responsible for peacetime TECHINT operations. HQ, INSCOM, fulfills its responsibilities through its TECHINT oversight function and manages the Army's Foreign Materiel for Training (FMT) Program and FMEP. It provides the interface with strategic S&TI agencies in support of FME and organizes, trains, and equips EAC TECHINT organizations during peacetime. TECHINT exploitation within INSCOM is performed by the following elements:

- **National Ground Intelligence Center.** HQ, INSCOM, exercises direct OPCON over the NGIC. NGIC produces and maintains intelligence on foreign scientific developments, ground force weapons systems, and associated technologies. NGIC analysis includes but is not limited to military communications electronics systems, types of aircraft used by foreign ground forces, NBC systems, and basic research in civilian technologies with possible military applications.
- **203d Military Intelligence Battalion.** The 203d MI Battalion is a multicomponent unit headquartered at Aberdeen Proving Ground, MD, and is the Army's sole TECHINT battalion. It performs the following functions:
  - Conducts TECHINT collection and reporting in support of validated S&TI objectives.
  - Acts as the HQDA executive agent for foreign materiel used for training purposes.

- Conducts TECHINT training for DOD analysts and RC TECHINT personnel.
- Supports INSCOM's FMA and FME operations as directed.
- Analyzes and exploits foreign captured enemy documents (CEDs), equipment, weapon systems, and other war materiel.
- Reports on the capabilities and limitations of enemy combat materiel.
- Provides reports alerting the command to the tactical threat posed by technical advances in new or recently discovered foreign or enemy materiel.
- Provides countermeasures to any enemy technical advantage.
- Provides foreign or enemy equipment for troop familiarization and training.
- Provides recommendations on the reuse of CEM.
- Supervises evacuating items of TECHINT interest.
- Provides task-organized battlefield TECHINT teams to support a subordinate command's TECHINT effort.

US ARMY MATERIEL COMMAND (AMC)

10-10. AMC plays a significant support role in TECHINT. Among AMC elements are a series of RDECs, the Army Research Laboratory System, and the Test and Evaluation Command (TECOM). Each conducts highly technical evaluations of foreign equipment. In peacetime, the AMC conducts FME on equipment purchased by each laboratory and RDEC for the intelligence community and for DOD as part of the International Materiel Evaluation Program (IMEP). AMC elements include—

- The Foreign Ordnance Exploitation Team, which is located at the Fire Support Armaments Center (FSAC) in the Picatinny Arsenal. This team exploits foreign ground ordnance and develops render safe procedures (RSPs) for foreign ordnance. It also prepares detailed intelligence reports to support explosive ordnance disposal (EOD), MI, and US munitions developers.
- The Science and Technology Center Europe and the Science and Technology Center Far East, which have the responsibility of collecting information on foreign technical developments by attending arms shows and technology exhibitions.
- The Soldier Biological Chemical Defense Command, which is the headquarters for the US Army Technical Escort Unit (TEU). The mission of the TEU is to collect and escort (transport) chemical, biological, radiological, and nuclear (CBRN) samples for testing and evaluation.

10-11. There are many other agencies with TECHINT responsibilities within the DOD. Refer to FM 34-54 for more information on TECHINT.

PLAN

10-12. TECHINT collection usually begins when an organization or individual reports the recovery or acquisition of unusual, new, or newly

employed threat materiel. However, there are often indications that the threat may be using materiel not yet associated with the threat among the myriad intelligence products available. Conversely, it may be known that the threat is using a particular item, the capabilities of which are unknown to US forces. It is in these cases that a unit may receive a TECHINT related ISR task. It is conceivable that such a task may be reflected in the PIR. An example of such a task is the identification or verification of suspected external modifications on a particular model of an enemy's main battle tank; the results of which are linked to a commander's decision.

10-13. TECHINT related ISR tasks should include a mission or target folder. At a minimum, this folder should include a description of the item, with its associated major combat systems, as well as handling instructions, reporting instructions, and a photograph or sketch of the item if available.

10-14. Additionally, the G2/S2 is responsible for ensuring the staff coordinates and establishes a plan for evacuating the desired materiel.

PREPARE

10-15. The G2/S2 must ensure that required TECHINT analytical assets, resources, and evacuation means are prepared to provide support. This includes verifying coordination effected with the task-organized battlefield TECHINT teams from the 203d MI Battalion. The G2/S2 must also ensure the means to report and disseminate TECHINT results to the unit and its soldiers are in place so that they can immediately adopt appropriate countermeasures, operations, or tactics in order to enhance their survival and mission accomplishment.

COLLECT

10-16. TECHINT collection includes capturing, reporting, and evacuating CEM. TECHINT collection begins when an organization or individual reports the recovery or acquisition of threat materiel. An item of materiel is exploited at each level, and continues on through succeeding higher levels until an appropriate countermeasure to neutralize the item's capabilities is identified or developed.

10-17. Army personnel (soldiers and civilian) and units will normally safeguard CEM and report it through intelligence channels to the first TECHINT element in the reporting chain. The location of this TECHINT element will be in accordance with the METT-TC factors; however, there will usually be TECHINT representation at the Corps G2 or the COCOM J2. The TECHINT representative or element will verify if the type of materiel is of intelligence value and determine its further disposition in conjunction with the unit's staff.

PROCESS

10-18. TECHINT processing starts (simultaneously with collection) with the capture of a piece of equipment of TECHINT value. This confirms that the enemy is indeed employing this materiel. In accordance with METT-TC factors, a TECHINT team may move to the location of the item at the capture site or wait until the item is evacuated before conducting a hasty exploitation. After hasty exploitation, the team decides if further processing

is required. If it is, the items are sent to the first (or nearest) Captured Materiel Exploitation Center (CMEC). If the item is deemed to yield no immediate tactical intelligence value, it may still be evacuated to the S&TI centers in CONUS for further analysis if the systems represent a change in the technological posture of an enemy.

PRODUCE

10-19. Battlefield TECHINT teams normally report initial and secondary examinations of CEM using either a preliminary technical report or a complementary technical report.

- A preliminary technical report—
  - Includes a general description of the item reported and recommended RSP.
  - Alerts others to information that can be used immediately by tactical units.
- A complementary technical report is more in-depth and—
  - Follows a secondary or an in-depth initial examination.
  - Allows the CMEC to compare new information with intelligence holdings.

10-20. At each successive echelon of exploitation, TECHINT analysts add to the overall body of information on an item by either adding to previous reports or by preparing new reports. The CMEC or other national level S&TI activities prepare more advanced technical reports and analyses. These reports include—

- Detailed technical reports.
- Translation reports.
- Special technical reports.

10-21. Other TECHINT products include—

- CMEC publications such as operator manuals, maintenance manuals, TECHINT bulletins, and tactical user bulletins.
- S&TI analysis bulletins.
- Foreign materiel exploitation reports.

ANALYZE

10-22. TECHINT analysts use checklists established by S&TI agencies and the CMECs to analyze each type of the adversary's equipment for which requirements exist. Analysis always begins with what is, and what is not, known about the piece of equipment. TECHINT units maintain procedures and plans for sampling, analyzing, and handling materiel.

DISSEMINATE

10-23. TECHINT of critical importance to the force, including answers to the PIR, is disseminated via the most expeditious means possible.

10-24. Routine TECHINT reports and products are usually transmitted through the unit's existing intelligence communications architecture in the format of an intelligence information report (IIR) format. For intelligence

reach operations, TECHINT products are available and disseminated in a variety of forms. The requestor must ensure that the TECHINT product can be transmitted over the available communications systems. This includes verifying the appropriate security level of the communications systems.

ASSESS

10-25. The primary goal of the TECHINT assess function is to determine whether the results of TECHINT production meet the unit's PIR or intelligence requirements. The G2/S2 immediately assesses TECHINT products upon receipt for accuracy and relevance. He must inform the TECHINT producer of the extent to which the product answered the PIR or intelligence requirement. Providing feedback to TECHINT analysts helps improve the effectiveness and efficiency of TECHINT.

10-26. The G2/S2 also assesses the success of the unit's ISR effort in accomplishing any TECHINT associated ISR task and shares his assessment with the staff and the pertinent units or personnel.

Chapter 11

Counterintelligence

DEFINITION

11-1. CI counters or neutralizes intelligence collection efforts through collection, CI investigations, operations, analysis and production, and functional and technical services. CI includes all actions taken to detect, identify, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies. It is the key intelligence community contributor to protect US interests and equities. Figure 11-1 shows the CI overview.

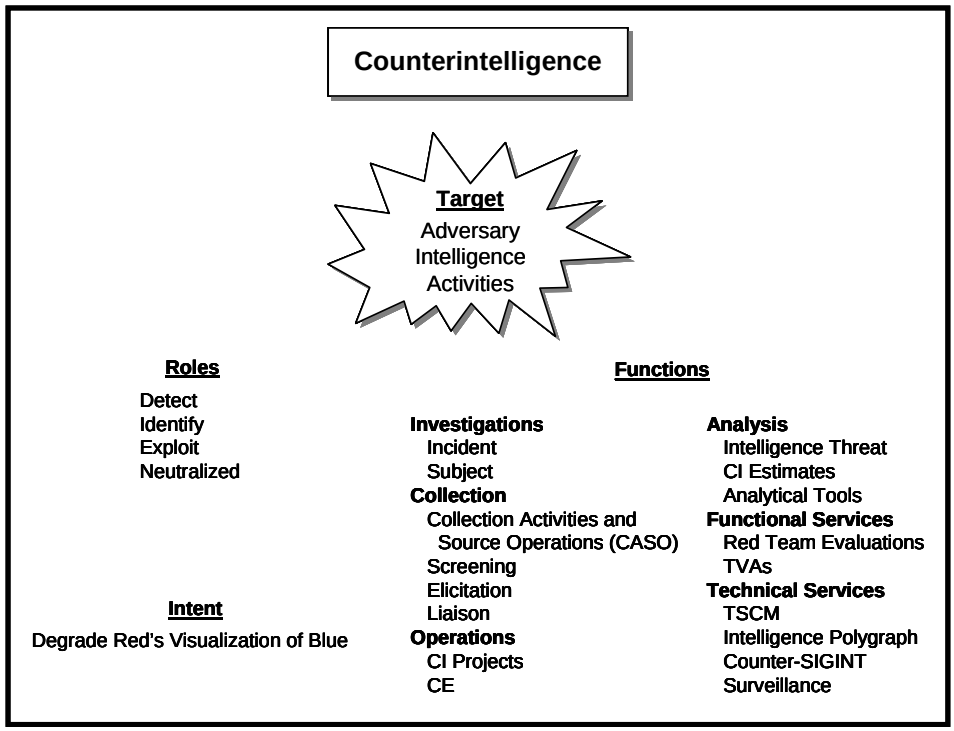


Figure 11-1. Counterintelligence Overview.

ROLE

11-2. The role of CI is to detect, identify, exploit, and neutralize all adversary intelligence entities targeting US and multinational interests. CI will focus on countering adversary intelligence collection activities targeting information or material concerning US personnel, activities, operations, plans, equipment, facilities, publications, technology, or documents—either classified or unclassified—without official consent of designated US release

authorities, for any purpose that could cause damage or otherwise adversely impact the interests of national security of the US ability to fulfill national policy and objectives. Adversary intelligence threats include but are not limited to any (US, multinational, friendly, competitor, opponent, adversary, or recognized enemy) government or NGOs, companies, businesses, corporations, consortiums, groups, agencies, cells or persons, terrorists, insurgents, guerrilla entities, and persons whose demonstrated actions, views, or opinions are inimical to US interests.

11-3. CI elements are instrumental in contributing to situational awareness in the AOI. CI elements may corroborate other intelligence discipline information as well as cue other intelligence assets through the CI core competencies and through CI technical services. The CI core competencies are collection, investigations of national security crimes within the purview of CI, operations, and analysis and production. CI technical services include computer network operations, technical surveillance countermeasures (TSCM), and polygraph. CI focuses on combating adversary intelligence activities targeting Army personnel, plans, operations, activities, technologies, and other critical information and infrastructure.

COUNTERINTELLIGENCE FUNCTIONS

11-4. CI functions are interrelated, mutually supporting, and can be derived from one another. No single function or technical capability can defeat adversary intelligence efforts to target US interests. CI functions are discussed below.

CI INVESTIGATIONS

11-5. Investigative activity is essential to countering the adversary intelligence threat to Army interests. CI places emphasis on investigative activity to support force, infrastructure and technology protection, homeland defense, information assurance, and security programs. CI investigations focus on resolving allegations of known or suspected acts that may constitute National Security Crimes under US law. The primary objective in any CI investigation is the detection, identification, exploitation, and/or neutralization of adversary intelligence threats directed against the US Army. CI investigations are also conducted to identify systemic security problems that may have damaging repercussions to Army operations and national security interests. All CI investigations are conducted within guidelines established in AR 381-10, AR 381-12, AR 381-20, applicable DOD policy and directives, and US laws.

CI OPERATIONS

11-6. CI operations are characterized as those activities that are not solely associated with investigative, collection, analysis, or production functions. CI operations can be either offensive or defensive in nature; they are derived from or transition to a collection or investigative activity depending on the scope, objective, or continued possibility for operational exploitation. CI operations fall into two categories: CI support operations and CI sensitive operations.

- **CI Support Operations**. These are defensive operations used to support ARFOR and technology protection, security projects, and programs. They include technical services support, support to acquisition, FP, special access, international security, foreign visitor or contact, treaty verification, information assurance, homeland defense, and other approved projects and programs.
- **CI Sensitive Operations**. These operations are generally offensive in nature and involve direct or indirect operations against a known adversary intelligence threat. These operations include counter-espionage (CE) and CI projects and are conducted by designated units.

CI COLLECTION

11-7. **Collection Activities**. CI elements conduct collection activities focused on adversary intelligence threats that target US and multinational interests. CI collection is conducted through the use of sources, assets, official contacts, and other human or multimedia sources to obtain information that impacts the supported unit. CI will not be used as a substitute for Army HUMINT collection. These activities are designed to collect specific information or develop leads concerning adversary intelligence collection requirements, capabilities, efforts, operations, structure, personalities, and methods of operation targeting US and multinational interests. CI collection can result from ongoing CI investigations or operations or serve to initiate CI investigations and/or operations.

11-8. **Liaison**. CI elements conduct liaison with US, multinational, and HN military and civilian agencies, to include NGO, for the purpose of obtaining information of CI interest and coordinating or deconflicting CI activities. Liaison activities are designed to ensure a cooperative operating environment for CI elements and to develop CI leads for further exploitation.

11-9. **CI Collection Activities and Source Operations (CASO)**. CASO is used to collect information on direct threats to US Army installations, organizations, activities, and personnel. The CASO program is not intended to be used as a substitute for tactical HUMINT contact operations. CASO can be used to initiate CI investigations, identify potential leads for offensive operations, or develop additional CASO leads. **Only designated units, in accordance with applicable policy, will be authorized to pursue investigative and offensive operational leads from ongoing CASO operations.**

11-10. **Screening**. CI Special Agents work jointly with HUMINT Collectors during screening operations to identify civilians on the battlefield, EPWs, detainees, and other noncombatants who may have information of CI interest or to develop CI leads. CI screening is also conducted during the process of hiring HN citizens for Army and DOD employment. Information obtained during screening operations may be used to initiate CI investigations and operations or to cue other intelligence collection disciplines such as HUMINT, IMINT, SIGINT, and MASINT.

11-11. **Debriefing**. CI Special Agents conduct debriefings of friendly force, HN, or the local population who may have information of CI interest regarding adversary intelligence collection or targeting efforts focused on US and multinational interests.

11-12. **Functional Services**. CI elements conduct functional services to assist traditional CI activities of investigations, collection, operations, analysis, and production; they also provide tailored support to US, DOD, and Army protection and security programs for commanders at all echelons. CI elements may use one or several of the functional services simultaneously to provide tailored support to a particular CI mission or supported program. CI functional services consist of—

- CI threat vulnerability assessments (TVAs).
- Adversary intelligence simulation (Red Team Evaluation).
- Covering agent support.

11-13. **CI Technical Services**. CI technical services are used to assist the CI functions of investigations, collections, and operations or to support functional services conducted by CI elements. For additional information on CI technical services, refer to AR 381-20 (SECRET/NOFORN) and FM 34-5. CI technical services consist of—

- Surveillance.
- Intelligence polygraphs.
- TSCM.
- Computer Network Operations (CNO).
- IO.
- Counter-Signals Intelligence (C-SIGINT).

ANALYSIS

11-14. IPB, all-source, and single-source analysis are used to template adversary intelligence activities. Analysis is also used to make recommendations to the commander on how to counter adversary intelligence efforts and to refine CI activities to potentially neutralize and/or exploit those efforts and to continually focus the efforts of CI teams. CI analysis focuses on the multidiscipline adversary intelligence collection threat targeting information on US multinational personnel, operations, activities, technology, and intentions. Raw information, open-source material, and finished intelligence products are analyzed in response to local and national requirements. Analysis occurs at all levels from tactical to strategic.

- At the tactical level, CI teams focus their efforts on supporting mission requirements and contributing to the all-source COP.
- Operational analysis is used to assess how adversary intelligence views and targets US interests; identify US vulnerabilities that could be exploited or targeted; and to determine adversary intelligence targeting methods of operation (MOs).
- CI collection priorities; assessing adversary intelligence technical options for countering US weapons and intelligence systems; and

assessing the impact of technology transfer activities on the US military's technological overmatch.

PRODUCTION

11-15. CI products consist of, but are not limited to, target nomination, CI input to TVAs, CI estimates, and investigative and intelligence information reports. Finalized intelligence derived from CI activities are incorporated into joint and national intelligence databases, assessments, and analysis products. CI products are also incorporated into the COP to support battlefield situational awareness. CI production takes place at all levels.

- Operational and tactical production includes tactical alerts, spot reports, and current intelligence; CI threat and/or vulnerability assessments tailored to specific activities, units, installations, programs, or geographic areas; CI studies to support contingency planning and major exercises; studies of adversary intelligence organization, MO, personnel, activities, and intentions that pose a current or potential threat to the supported command.
- Strategic products include assessments supporting national and Army programs including SAPs and acquisition programs; worldwide assessments of the organization, location, funding, training, operations capabilities, and intentions of terrorist organizations; global trends in adversary intelligence MO; after-action studies of individual espionage cases; analyses of the intelligence collection capabilities of international narcotics trafficking organizations; and multimedia threat products to support Army CI awareness programs.

TECHNICAL SERVICES

11-16. CI organizations with technically trained CI Special Agents are chartered with providing unique technical capabilities to augment CI investigations, collection, and operations. These technical capabilities are not used as substitutes for CI activities, but support traditional CI techniques employed to counter and neutralize adversary intelligence activities targeting US interests.

11-17. Selected CI Special Agents are trained to identify human deception indicators during the course of investigations, operations, and collection missions. Required training and skills include the use of polygraph and emerging biometric technologies that can recognize indications of deception by human sources, contacts, and subjects of investigations, as well as analysis and reporting of results.

11-18. TSCM CI Special Agents are trained in sophisticated electronic and sensing equipment to identify technical collection activities carried out by adversary intelligence entities. The use of TSCM is critical to ensuring that sensitive and/or restricted areas are clear of any adversary intelligence-placed active or passive electronic sensing, or eavesdropping or collection devices. These areas include SCIF, secure working and planning areas, and C2 facilities.

11-19. CNO consist of computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE). CI Special Agents

are specially trained in the areas of computer operation, network theory and administration, and forensics, along with IO in order to ensure US information dominance. The reliance on networked systems will result in greater emphasis being placed on information assurance. Specially selected CI agents will be trained in CNO in order to assist in protecting US information and information systems while exploiting and/or attacking adversary information and information systems.

11-20. For more information on technical services, refer AR 381-20 and FM 34-5.

OPERATIONAL EMPLOYMENT

11-21. Army CI supports the full spectrum of military operations. The Army requires a well-trained CI force consisting of AC, RC, civilian government employee, and contractor personnel. CI elements are focused on and dedicated to detecting, identifying, neutralizing, and/or exploiting adversary intelligence elements attempting to collect information on US forces. Effective employment of Army CI elements in all phases of operations and at all levels from tactical to strategic is paramount to countering any adversary intelligence threat to US interests and resources. Moreover, Army CI protects special programs that provide R&D, acquisition, and integration of technologies leading to future technological overmatch. CI elements have the capability and authority to conduct complex, nontraditional operations in this Information Age to CE, to both protect critical technologies and satisfy Army, DOD, and national level CI objectives.

LEVELS OF EMPLOYMENT

Strategic and Departmental

11-22. Strategic and departmental operations will be conducted by CI elements supporting national, DOD, and DA required missions (for example, support to NATO and special operations and missions). Strategic and departmental CI will conduct compartmented investigations and operations to affect the knowledge of adversary intelligence regarding CONOPS and defense information. Army CI will execute the full range of CI functions and missions at the strategic and departmental level including CI investigations and operations, CE, technology protection, SAP support, treaty verification, and technical CI services (polygraph, TSCM, and computer forensics). Strategic and departmental CI will also support SOF and special mission units (SMUs) within the scope of applicable national, DOD, and DA security policies and regulations.

Operational

11-23. Operational missions of CI elements will support combatant commanders, generally in geographic AOIR. Operational CI elements will focus on threat identification and countering regional adversary intelligence threats. Operational level CI activities and functions include CI investigations and operations, CE, technology protection, SAP support, treaty verification, and technical CI services (polygraph, TSCM, and computer

forensics). CI elements must be capable of quickly transitioning from a peacetime mission to crisis operations to support combatant commander requirements. Theater CI assets will conduct unilateral to multinational operations in designated theaters. Operational elements may also be deployed to support or reinforce tactical forces in CONOPS.

Tactical

11-24. CI teams will conduct operations throughout the battlespace during CONOPS. CONOPS support activities include conduct of CASO, limited CI investigative capability, personnel security investigations, screenings, and debriefings. CI activities in CONOPS focus on countering the adversary intelligence threat and assisting in conducting TVAs. TVAs will be conducted in conjunction with MPs, Engineers, and Medical Service personnel to provide the commander with a comprehensive FP assessment. During peacetime, organic tactical CI teams conduct activities in accordance with approved regulations and command guidance.

SUPPORT TO CONTINGENCY OPERATIONS

11-25. The initial phase of operations from PME to MTW lays the foundation of future team operations. In general, the priority of effort focuses inward on security of operating bases, areas of troop concentration, and C2 nodes to identify the collection threat to US forces that could be used by adversary elements to plan hostile acts against US activities and locations.

11-26. Once security of the operating bases has been established, the operational focus of CI teams shifts outside the operating base to continue to detect, identify, and neutralize the collection threat to US forces as well as to provide I&W of hostile acts targeting US activities. The CI team uses several collection methods, to include CASO, elicitation, and liaison, to answer the supported commander's requirements. This is referred to as the continuation phase. The CI team conducts CI investigations to identify, neutralize, and exploit reported threat intelligence collection efforts.

11-27. A key element to the CI team's success is the opportunity to spot, assess, and develop relationships with potential sources of information. Operating as independent teams, without being tied to ISR or combat assets, enables the CI team's maximum interaction with the local population, thereby maximizing the pool of potential sources of information. Along with the opportunity to spot, assess, and interact with potential sources of information, a second key element of a CI team's success is its approach-ability to the local population. A soft posture enables a CI team to appear as non-threatening as possible. Experience has shown that the local population in general is apprehensive of fully and openly armed patrols and soldiers moving around population centers.

11-28. During some operations, civilian attire or nontactical vehicles may be used to lower the CI team profile. In some special situations, these measures are taken to make the operation less visible to the casual observer. Also, in some cultures, sharing food and beverages among friends is expected; exceptions to restrictions or general orders should be considered to facilitate

successful CI team operations, many of which are geared towards developing relationships with potential sources of information.

SUPPORT TO INSTALLATIONS AND OPERATING BASES

11-29. CI teams, as part of a multi-agency team consisting of MPs, CA, medical, and EOD, support the conduct of TVAs of installations and operating bases to identify the intelligence threat to the operating locations. Detailed TVAs identify weaknesses in operational and physical security procedures and recommend countermeasures to mitigate intelligence collection on friendly forces limiting the ability to plan hostile acts on US activities and locations. CI activities supporting installations and operating bases include—

- Interviewing walk-in sources and locally employed personnel.
- Screening local national (LN) hires. Commanders, staff planners, and SIOs should always provide input to personnel assigned to establish and negotiate contracts using local national (LN) hires. This requirement ensures that LN hires can be screened, interviewed, and in some instances used as CI sources or assets in order to provide intelligence information that impacts the security of the base camp.
- Debriefing friendly force personnel who are in contact with the local population, such as—
  - ISR patrols.
  - MP patrols.
  - Combat patrols.
  - Liaison personnel.
  - CA and PSYOP teams.
- Conducting limited local open-source information collection.
- Providing support to TVAs of the base camp.

TACTICS, TECHNIQUES, AND PROCEDURES

11-30. At the CI team level, team members conduct mission analysis and planning specific to their AO. Backwards planning and source profiling are used extensively to choose CI targets. To verify adequate area coverage, the CI team may periodically develop and use CI target overlays and other CI analytical tools that illustrate the CI situation, identify CI gaps, and help refocus the collection effort.

11-31. The CI team is also in constant contact with the supported S2 and the other ISR assets (Scouts, PSYOP, CA, and MP) in order to coordinate and deconflict operations and to cross-check collected information. The supported unit S2, with the help of the CI team, regularly and systematically debriefs all ISR assets.

11-32. The CI team must be integrated into the supported unit's ISR plan. The CI OMT chief will advise the supported unit on the specific capabilities and requirements of the team to maximize mission success.

OPERATIONAL RISK MITIGATION

11-33. The employment of CI teams includes varying degrees of contact with the local population. As the degree of contact with the population increases, both the quantity and quality of CI collection increases. In many instances, however, there is a risk to the CI team inherent with increased exposure to the local population. The decision at what level to employ a CI team is METT-TC dependent. The risk to the CI assets must be balanced with the need to collect priority information and to protect the force as a whole. ROE, SOFA, direction from higher headquarters, and the overall threat level may also restrict the deployment and use of CI teams. The commander should consider exceptions to the ROE to facilitate CI collection.

11-34. Risks are minimized through the situational awareness of CI team members. They plan and rehearse to readily react to any situation and carry the necessary firepower to disengage from difficult situations. If it becomes necessary to call for assistance, adequate and redundant communications equipment is critical. These scenarios and actions should be trained prior to deployment into a contingency area and rehearsed continuously throughout the deployment.

11-35. A supported unit commander is often tempted to keep the CI team "inside the wire" when the THREATCON level increases. The supported commander must weigh the risk versus potential information gain when establishing operational parameters of supporting CI teams. This is necessary especially during high THREATCON levels when the supported unit commander needs as complete a picture as possible of the threat arrayed against US and multinational forces.

11-36. When it is not expedient to deploy the CI team independently due to threat levels or other restrictions, the team can be integrated into other ongoing operations. The CI team may be employed as part of a combat, ISR, or MP patrol or used to support CA, PSYOP, engineer, or other operations. This method reduces the risk to the team while allowing a limited ability to collect information. It has the advantage of placing the team in contact with the local population and allowing it to spot, assess, and interact with potential sources of information. However, this deployment method restricts collection by subordinating the team's efforts to the requirements, locations, and timetables of the unit or operation into which it is integrated and does not allow for the conduct of sensitive source operations. **This method of employment should be considered a last resort**.

COUNTERINTELLIGENCE EQUIPMENT

11-37. Basic C2, transportation, and weapons requirements do not differ significantly from most soldier requirements and are available as unit issue items. However, CI teams have unique communications, collection, processing, and mission-specific requirements.

COMMUNICATIONS

11-38. **Dedicated and Secure Long-Range Communications.** These are keys to the success of the CI team mission. CI team operations require a secure, three-tiered communications architecture consisting of inter/intra-team radios, vehicle-based communications, and a CI and HUMINT base station.

11-39. **Communications Network.** The CI team must have access to existing communications networks such as the tactical LAN. The CI team must also be equipped with its own COMSEC devices. It is imperative that the CI team acquire access to the public communication system of the HN. This can be in the form of either landlines or cellular telephones. Such access enables the CI team to develop leads which can provide early indicators to US forces.

11-40. **Interoperability.** Communications systems must be equipped with an open-ended architecture to allow for expansion and compatibility with other service elements, government organizations, NGOs, and multinational elements to effectively communicate during CONOPS. All ISR systems must be vertically and horizontally integrated to be compatible across all BOSs and with Legacy and Interim Force elements.

11-41. **SOTM.** To provide real-time and NRT information reporting, CI elements must have the capability to transmit voice, data, imagery, and video while on the move. CI teams must be able to transmit while geographically separated from their parent unit while operating remotely. This broadband requirement can only be achieved through a SATCOM capability and must be achievable while mobile.

CI COLLECTION AND PROCESSING SYSTEMS

11-42. The CI team must rely on automation to achieve and maintain information dominance in a given operation. With time, effective collection planning and management at all echelons, the CI team can collect a wealth of information. The sorting and analysis of this information in a timely and efficient manner is crucial to operations. Automation helps the CI team to report, database, analyze, and evaluate the collected information quickly and to provide the supported unit with accurate data in the form of timely, relevant, accurate, and predictive intelligence.

11-43. Automation hardware and software must be user friendly as well as interoperable among different echelons and services. They must interface with the communications equipment of the CI team as well as facilitate the interface of audiovisual devices. Technical support for hardware and software must be available and responsive.

11-44. The demand for accurate and timely CI reporting, DOCEX, and open-source information has grown tremendously. Biometric (physiological, neurological, thermal analysis, facial and fingerprint recognition) technologies will allow rapid identification, coding, and tracking of adversaries and human sources; as well as cataloging of information concerning EPWs, detainees, and civilians of CI interest on the battlefield. Biometrics will also provide secure authentication of individuals seeking network or facility access.

11-45. CI teams work with multinational forces and other foreign nationals and require the ability to communicate in their respective languages. Often CI personnel have little or no training in the target language, and lack of skilled interpreters can hinder CI activities. CI teams require textual and voice translation devices, source verification, and deception detection machines (biometrics) to improve collection capability and accuracy.

11-46. CI teams require dynamic MLT tools that provide both non-linguists and those with limited linguist skills a comprehensive, accurate means to conduct initial CI screenings and basic interviews in a variety of situations. CI elements will focus on in-depth interviews and communications with persons of higher priority. MLT tools minimize reliance on contract linguists and allow soldiers to concentrate on mission accomplishment.

MISSION SPECIFIC

11-47. The CI team may conduct night operations and must be equipped with NVDs for its members, and photographic and weapons systems. The CI team also may operate in urban and rural areas, where the threat level can vary from semi-hostile to hostile. The safety of the CI team can be enhanced with equipment that can detect, locate, suppress, illuminate, and designate hostile optical and E-O devices. In addition, high power, gyro-stabilized binoculars, which can be used from a moving vehicle, increases the survivability of the CI team and also gives the team another surveillance and collection device.

11-48. Some of the CI team missions may require the documentation of incidents. The CI teams can use the following equipment in their open-source collection efforts.

- Small, rugged, battery-operated digital camcorders and cameras which are able to interface with the collection and processing systems as well as communication devices.
- GPSs that can be mounted and dismounted to move in the AO efficiently.
- Short-range multichannel RF scanning devices that can also identify frequencies which enhance their security.
- In some cases CI teams require a stand-off, high resolution optical surveillance and recording capability that can provide target identification at extended ranges to protect the intelligence collector while avoiding detection by the adversary target. An advanced optical capability provides intelligence collectors the ability to locate and track adversary targets (passive and hostile) for identification, collection, and target exploitations.

INTEGRATION OF LINGUISTS

11-49. Integrating linguists into the CI team should take place as soon as possible. Security clearances and contractual agreements will help the team determine the level of integration.

11-50. Along with the basic briefing of what is expected of the civilian linguists as interpreters, CI teams should be informed about the civilians' chain of command and the scope of their duties beyond interpreting. The CI

team leader must ensure that linguists are trained and capable of completing all tasks expected of them.

BATTLE HAND-OFF

11-51. CI teams are always engaged. A good battle hand-off is critical to smooth transition and mission success. The battle hand-off can directly contribute to mission success or failure of the outgoing team, but especially of the incoming team. The battle hand-off begins the first day the CI team begins to operate in an AO. Regardless of how long the team believes it will operate within the AO, it must ensure there is a seamless transition to an incoming team, other US unit, or agency. The CI team accomplishes this transition by establishing procedures for source administration, database maintenance, and report files.

11-52. Teams must plan and implement a logical and systematic sequence of tasks that enables an incoming team to assume the operations in the AO. Adequate time must be allotted for an effective battle hand-off. In some environments, a few weeks may be necessary to accomplish an effective battle hand-off. Introductions to sources of information, especially CASO sources, are critical, and teams must prioritize their time. During this time the outgoing CI team must familiarize the new CI team with all aspects of the operation, which include past, present, and planned activities within the AO. Area orientation is critical. These include major routes, population centers, potential hot spots, and other points of interest (such as police stations, political centers, and social centers).

ORGANIZATION

11-53. CI activities require a complex C2 relationship to ensure that the requirements of the supported commander are fulfilled while balancing the need for strict integrity and legality of CI operations. This complex relationship balances the role of the SIO as the requirements manager and the 2X as the mission manager with the MI commander as the asset manager.

COMMAND VERSUS CONTROL

11-54. ARFOR will normally deploy as part of a joint, multinational, and/or combined operation. In all cases, commanders at each echelon will exercise command over the forces assigned to their organization. Command includes the authority and responsibility for effectively using resources, planning for and employment of forces, and ensuring that forces accomplish assigned missions. Leaders and staffs exercise control to facilitate mission accomplishment.

11-55. While the MI commander supervises subordinates and produces reports, the *2X synchronizes activities between intelligence units and provides single-source processing and limited analysis. **(*2X " indicates 2X functions at all levels.)** While the MI commander takes care of the operators executing missions, the *2X obtains the data and reports from higher echelons required to execute the missions.

STAFF RESPONSIBILITIES AND FUNCTIONS

11-56. The *2X staff is responsible for the integration, correlation, and fusion of all Human Sensor information into the Intelligence BOS within the *2X AOIR. The *2X is also responsible for analyzing adversary intelligence collection, terrorist and sabotage activities, developing countermeasures to defeat threat collection activities, identifying and submitting collection requirements to fill CI collection gaps, and providing input to the all-source picture regarding adversary intelligence activities.

11-57. The *2X Staff Officer provides CI and HUMINT collection expertise. The *2X—

- Is the single focal point for all matters associated with CI and HUMINT in the AOIR.
- Is the CI and HUMINT advisor to the G2 and commander.
- Is an extension of the collection manager and ensures that the best asset or combinations of assets are used to satisfy information requirements.
- Along with his subordinate elements—CICA, HOC, OSC, CIAC, and HAC—exercises technical control over his assigned Army CI and HUMINT elements in the designated AOIR.
- Is the principal representative of the G2 and the commander when coordinating and deconflicting CI and HUMINT activities with national or theater agencies operating in the AOIR.
- Supports specific RM efforts in conjunction with the requirements manager through the planning and coordination of CI and HUMINT operations; the review and validation of CI requirements; the recommendation for assignment of tasks to specific collectors; and the conduct of liaison with non-organic HUMINT collection. This liaison includes national level and multinational force assets for source deconfliction and special activities outside the *2X AOIR.
- Will provide OMTs with capability to reach back to current database information, technical information and guidance, and source deconfliction necessary to monitor the collection activities of the CI teams.
  - *CICA*. The CICA is responsible for coordinating and synchronizing all CI activities in the designated AOIR. The CICA exercises technical control over all CI entities in the designated AOIR and deconflicts CI activities with higher, lower, and adjacent CI elements. The CICA accomplishes all responsibilities through coordination with the operational units and other *2X staff elements.
  - *OSC*. The OSC in the *2X staff maintains the source registry for all CI activities in the designated AOIR. The OSC provides management of intelligence property book operations, source incentive programs, and ICFs.
  - *CIAC*. The CIAC analyzes adversary intelligence collection capabilities. The CIAC leverages all intelligence discipline reporting and analysis to counter threat collection capabilities against the deployed force. CIAC analysis provides information and analysis to the COP.

11-58. The ACE and JISE CI analysis team analyzes threat intelligence collection and the intelligence collection efforts of foreign organizations involved in terrorism and sabotage in order to develop countermeasures against them. CI analysis cross-cues IMINT, SIGINT, MASINT, and TECHINT resources in addition to CI-related HUMINT reporting and analysis to counter threat collection capabilities against the deployed force. While the HAC supports the positive collection efforts of the force, the CI analysis team supports the "defend" aspects of the commander's FP program.

11-59. CI analysis is the analysis of the adversary's HUMINT, IMINT, SIGINT, and MASINT capabilities in support of intelligence collection, terrorism, and sabotage in order to develop countermeasures against them. It involves a reverse IPB process in which the analyst looks at US forces and operations from the threat's perspective. CI analytical products are an important tool in the COA development in the MDMP. This analytical tool supports the commander's FP program and facilitates the nomination of CI targets for neutralization or exploitation. (See FM 2-01.2 (FM 34-60) for more information on CI analysis.) Specifically, CI analysis—

- Produces and disseminates CI products and provides input to INTSUMs.
- Provides collection requirements input to the CICA.
- Analyzes source reliability and credibility as reflected in reporting and communicating that analysis to the collector.
- Nominates CI targets for neutralization or exploitation.
- Identifies and submits CI-related requirements to fill collection gaps.
- Assists HAC personnel in focusing the CI aspects of the HUMINT collection program.
- Presents CI analysis products such as CI estimates, target lists, reports, and graphics that support the commander.

11-60. For intelligence reach operations, CI products are available and disseminated in a variety of forms. It is incumbent on the requestor to ensure the CI product can be transmitted over the available communications systems. This includes verifying the appropriate security level of the communications systems.

CI TEAM STRUCTURE

11-61. **OMT.** The OMT is a four-person team consisting of a WO, two NCOs, and a junior enlisted soldier. (Civilians may be inserted into this structure as appropriate.) Rank structure and standards of grade for OMTs will vary depending upon the skill sets required and mission focus. CI OMTs will provide operational guidance for 1 to 4 CI teams, depending on mission focus and operational tempo. When two or more CI teams are deployed in a DS role, an OMT is also deployed to provide technical control. The OMT works closely with the supported S2 and ACT to furnish current threat information and to answer the supported commander's PIRs and IRs. OMTs coordinate with the supported 2X and manage subordinate CI teams to—

- Provide guidance and technical control of operational activity.
- Provide the collection and operational focus for CI teams.

- Provide quality control and dissemination of reports for subordinate CI teams.
- Conduct single-discipline CI analysis and assist in mission analysis for the supported commander.
- Act as a conduit between subordinate CI teams, the CICA, and supported unit headquarters.
- Provide administrative support for subordinate CI teams to include reporting mission and equipment status to the CICA and the supported unit headquarters.
- Educate the supported commander on the capabilities of the CI teams.
- Integrate the CI teams directly into the maneuver commander's ISR planning.

11-62. **CI Team.** The CI team is a four-person team consisting of two NCOs and two junior enlisted personnel. Rank structure and standards of grade for CI teams will vary depending upon the skill sets required and mission focus. CI teams are trained to execute the full range of CI functions; however, they may be assigned to mission-focused elements (for example, CE, CI projects). Assignment to a TSCM, polygraph, or information warfare team requires additional, specialized technical training.

Appendix A

Intelligence and Information Operations

THE INFORMATION ENVIRONMENT

A-1. The information environment is the aggregate of individuals, organizations, and systems that collect, process, store, display, and disseminate information; also included is the information itself. (FM 3-0) The information environment, it should be noted, is not an exclusively military one; in fact, the military applications of information are almost obscured in today's universal usage of the information spectrum by national, international, and non-state players.

THE COMMANDER AND INFORMATION

A-2. Information is facts, data, or instructions in any medium or form; the meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02) Information provides the key to battlefield success in the 21st century. Commanders must have detailed information to command. Information is the medium that allows the commander's decisionmaking and execution cycle to function. Information gives direction to actions by the force, identifies the enemy's centers of gravity, provides COAs for force activity, and enables the force to accomplish its operational mission.

INFORMATION SUPERIORITY

A-3. Information superiority is the operational advantage derived from the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (FM 3-0) Relevant information drawn from intelligence supports the creation and development of situational understanding that contributes directly to information superiority during decisive operations. The requirement for information superiority is not new; what is new is that today's information technologies are creating a base of knowledge for military planning and execution that is unprecedented in scope, volume, accuracy, and timeliness. This means commanders receive accurate, timely information that enables them to make better decisions and act faster than their adversaries.

A-4. Information superiority, however, is neither a staple in today's battlespace nor is it necessary in military operations as a constant condition; rather, at specific times during operations, information superiority becomes a key enabler for assuring military success. At the operational level of predominant interest to the land component commander (LCC), information superiority is realized through the integration of operational level, interdependent ISR, information management, and IO to gain and maintain operational initiative and to achieve an operational advantage.

INFORMATION OPERATIONS

A-5. IO are the employment of core capabilities of electronic warfare, computer network operations, PSYOP, military deception, and operations security, in concert with specified supporting and related capabilities to affect or defend information and information systems, and to influence decisionmaking…. Information systems are…the equipment and facilities that collect, process, store, display, disseminate information. These include computers, hardware, software, and communications, as well as policies and procedures for their use. (FM 3-0). Offensive IO are capable of degrading an adversary's will to resist and ability to fight. Defensive IO measures passively and actively protect friendly information and C2 systems and limit their vulnerability.

A-6. Offensive and defensive IO are conducted as a fully coordinated effort to ensure the complementary, asymmetric, and reinforcing effects to attack enemy forces, influence others, and protect friendly forces. Relevant information assures that the right person has the right information at the right time for decisionmaking and execution.

THE ELEMENTS OF IO

A-7. Full-spectrum IO incorporates, integrates, and synchronizes traditionally independent capabilities and activities in support of the commander's mission. (See FM 3-0 and FM 3-13.) The Army's doctrinal view of full-spectrum IO as evolving core capabilities are—

- PSYOP.
- OPSEC.
- EW.
- Military deception.
- CNO.
  - CNA.
  - CND.
  - CNE.

A-8. Supporting IO capabilities are—

- Physical destruction.
- Physical security.
- Information assurance.
- Counterpropaganda.
- Counterdeception.
- Counterintelligence.

IO-RELATED ELEMENTS

A-9. The IO-related activities of PA and CMO are closely associated and integrated with the elements of IO as key contributors to information superiority.

INTELLIGENCE SUPPORT TO IO

A-10. All-source intelligence support, encompassing all of its forms, is the principal enabler for successful IO. The commander's capability to synchronize military operations can be heavily influenced by the ability to identify the threat and understand the adversary's capabilities and intentions in the information environment.

A-11. It is essential that the elements of the command's IO capabilities and vulnerabilities are integrated into the command intelligence plan. This leads to COAs that synchronize the elements of IO and IO-related activities into the commander's warfighting plans. Integration of the full-spectrum aspects of IO ensures that the relative importance of information is recognized in the development of a synchronized OPLAN. Further, integration of IO into the planning process provides a methodology for analyzing the threat from a knowledge base that enhances protection of friendly systems and assets while exposing windows of opportunity for attack or exploitation. IPB is the best process we have for understanding the battlefield and the options it presents to friendly and threat forces.

A-12. Provide Intelligence support to IO includes, but is not limited to, the following:

- **Provide Intelligence Support to Offensive IO**. The Intelligence BOS supports offensive IO by providing information to identify critical enemy C2 nodes. Intelligence also helps to identify enemy systems and procedures that may be vulnerable for offensive IO. Additionally, intelligence plays a key role in evaluating and assessing the effectiveness of offensive IO.
  - *Provide Intelligence Support to PSYOP*. This task identifies the cultural, social, economic, and political environment of the AO. It identifies target groups and subgroups and their location, conditions, vulnerabilities, susceptibilities, cultures, attitudes, and behaviors. PSYOP influence foreign target audiences in the AO to support achieving the commander's goals in the AO.
    - Identify the cultural, social, economic, and political environment of the AOI; for example, adversary mechanisms for political control, adversary communication and broadcast systems used to elicit support from the populace, and current and past adversary propaganda activities and their effectiveness.
    - Identify target groups and subgroups and their location, conditions, vulnerabilities, susceptibilities, cultures, attitudes, and behaviors. This includes determining the audience demographics of popular radio and television programs and periodicals; groups influenced by media personalities and political cartoons.
    - Identify impact of planned PSYOP on individuals outside the targeted group (for example, multinational partners, neighboring populations).
  - *Provide Intelligence Support to Military Deception*. This task identifies the capabilities and limitations of the adversary's

intelligence-gathering systems and identifies adversary biases and perceptions.
  - Profiles of key adversary leaders.
  - Cultural, religious, social, and political characteristics of the country and region.
  - Sources of military, economic, or political support.
  - Adversary decisionmaking processes, patterns, and biases.
  - Adversary perceptions of the military situation in the AO.
  - Capabilities and limitations of adversary CI and security services.
- *Provide Intelligence Support to Electronic Attack*. This task supports electronic attack employing jamming, electromagnetic energy, or directed energy against personnel, facilities, or equipment. It identifies critical adversary information systems and C2 nodes. It includes determining and presenting the adversary's electronic OB and their information system infrastructure. The enemy's C2 system vulnerabilities and the means they use to protect their C2 systems is part of the electronic OB.

- **Provide Intelligence Support to Defensive IO**. The Intelligence BOS supports defensive IO by providing information to identify threat IO capabilities and tactics. Intelligence provides information relating to CND, physical security, OPSEC, counterdeception, and counterpropaganda. The Intelligence BOS supports defensive IO by providing information to identify threat IO capabilities and tactics. Intelligence provides information relating to CND. Provide Intelligence Support to OPSEC—identify capabilities and limitations of the adversary's intelligence system to include adversary intelligence objectives and the means, methods, and facilities used by the threat to collect, process, and analyze information—supports the identification of indicators that could be interpreted or pieced together to penetrate EEFI in time to be useful to adversaries.
- **Provide Intelligence Support to Activities Related to IO**. The Intelligence BOS when operating outside US territories supports activities related to IO under some circumstances.
  - *Provide Intelligence Support to CMO*. This task allows military intelligence organizations to collect and provide information and intelligence products concerning foreign cultural, social, economic, and political elements within an IO in support of CMO. Identify cultural, social, economic, and political environment of the AOI, including—
    - Population demographics.
    - Civilian populace attitudes, alliances, and behavior.
    - Availability of basic necessities (food, clothing, water, shelter, medical care) and the ability of the populace to care for itself.
    - Access to medical care.
    - Locations and potential routes, destinations, and assembly areas or sites of displaced persons.
    - Local government type, status, organization, and capabilities.

  - Availability of local material and personnel to support military operations.
  - NGOs in the AOI, their agenda, resources, and capabilities.
- *Provide Intelligence Support to Public Affairs*. This task identifies the multinational and foreign public physical and social environment, as well as world, HN national, and HN local public opinion, in addition to the propaganda and misinformation capabilities, activities, targets, themes, and dissemination means of the adversary. Identify world, national, and local public opinion (location, biases or predispositions, and agenda of national and international media representatives in the AOI, and trends reflected by the national and international media).

Appendix B

Linguist Support

ROLE OF LINGUISTS

B-1. Military operations are highly dependent on foreign language support. The requirement to communicate with and serve on multinational staffs, communicate with local populations, and exploit enemy forces necessitates the use of linguists. The growing focus on multinational operations increases the competition for limited linguist resources that are vital for mission success. This appendix establishes the framework and process to access, prioritize, and employ the Army's limited organic linguist resources.

LINGUISTIC SUPPORT CATEGORIES

B-2. Foreign language support requirements of US Armed Forces typically fall into one of four broad categories:

- Intelligence and Information Gathering. This category includes the traditional SIGINT and HUMINT disciplines, as well as foreign language support to FP and exploitation of open-source information.
- CMO. This category encompasses all functions relating to military interaction with the civilian population. Foreign language support is critical to CMO in areas such as government liaison, legal agreements, medical support and operations, law enforcement, engineering projects, public safety, security and population control, CA, and PSYOP.
- Logistics. This category consists of foreign language support to sustainment or transportation functions. These include logistical contracting, port, railhead, airhead, or transshipment operations and convoy operations.
- Multinational Operations and Liaison. This category includes the coordination of military operations and liaison with multinational partners, previously unaffiliated nations, and at times adversary or former adversary nations. Multinational operations are becoming more common and increasingly important.

DETERMINING LINGUIST REQUIREMENTS

B-3. To identify linguist requirements, the staff conducts mission analysis and identifies specified or implied tasks requiring foreign language support. Other critical factors are the organization or echelon of command and the location of the mission. The staff uses these criteria to determine the allocation of linguists, such as one linguist team per echelon of command, one linguist per piece of equipment, or one linguist team per location where the function is to be performed. The staff then applies task organization and scheme of maneuver to determine the number of linguists needed for an operation.

B-4. The staff must analyze each linguist assignment to determine the minimum level of foreign language proficiency needed. While interpretation for a peace negotiation requires not only outstanding linguistic capability but also cultural acumen, the translation of routine documents (with the aid of a dictionary) requires a much different skill set. Poor identification of linguist proficiency requirements can tie up the best linguists in less effective roles, creating linguist shortfalls in other areas.

B-5. The relative importance of each of the four linguist support categories is mission dependent. For example, during a NEO civil and military coordination would probably not be as critical as intelligence and information gathering. However, the situation is reversed for a humanitarian assistance mission in which CMOs have a significant impact on mission success. Identifying these "dynamics" helps the commander and staff prioritize linguist requirements.

B-6. Determining linguist requirements for any operation can be difficult because each operation is unique. However, commanders and staffs with a basic knowledge of organic Army linguistic assets, foreign language resource alternatives, and MI skills can successfully assess, prioritize, and employ linguists in support of their military operations.

PLANNING AND MANAGING LINGUIST SUPPORT

B-7. Commanders must consider the linguist requirements as part of their MDMP for every CONPLAN and OPLAN assigned to their commands. Prior staff planning and identification of linguist requirements should prompt commanders to initiate linguist support requests and identify command relationships prior to actual operations. If the mission analysis reveals requirements for linguistic support, the commander must identify what foreign languages are needed, the foreign language proficiency levels needed for each assignment, and the best source of linguists. In addition, if the mission includes intelligence and information collection, the commander must identify MI collection skills required. During mission analysis, the commander should consider linguist requirements for every CONPLAN and OPLAN assigned to his command.

LINGUIST CATEGORIES

B-8. The commander and staff must identify linguist requirements by category:

- Category I – Have native proficiency in the target language (level 4-5) and an advanced working proficiency (Interagency Language Round Table [ILRT] level 2+) in English. They may be locally hired or from a region outside the AO. They do not require a security clearance. They must be screened by the Army CI support team.
- Category II – Are US citizens screened by Army CI personnel and are granted access to SECRET by the designated US government personnel security authority. Have native proficiency in the target language (level 4-5) and an advanced working proficiency (ILRT 2+) in English.
- Category III – Are US citizens screened by Army CI personnel and are granted either TS/SCI clearance or an interim TS/SCI clearance by the

designated US government personnel security authority. Meet a minimum requirement of ILRT level 3. They are capable of understanding the essentials of all speech in a standard dialect. They must be able to follow accurately the essentials of conversation, make and answer phone calls, understand radio broadcasts and news stories, and oral reports (both of a technical and non-technical nature).

PRIMARY STAFF RESPONSIBILITIES

B-9. Primary staff at each echelon has responsibilities for evaluating requirements and managing linguist support. The responsibilities include but are not limited to those discussed below. In addition, each staff section is responsible for determining its linguist support required to meet its operational missions.

Assistant Chief of Staff, G1 (S1):

- Identify linguist requirements needed to support G1/S1 functions in all contingency areas. G1/S1 requirements for linguist support include but are not limited to the following:
  - Coordinate with local authorities on matters of civilian hire, finance, and recordkeeping.
  - Contract for local hire personnel.
  - Coordinate for local morale support and community activities.
  - Coordinate with local authorities for postal operations.
  - Support for administration, counseling, personal affairs, and leave for LN and third-country national (TCN) personnel.
  - Coordinate for local medical support.
  - Liaison with multinational counterparts.
- Linguist staffing and linguist replacement management.
- Identify foreign language skill identifiers for all assigned, attached, or OPCON Army linguists.
- Identify all Army foreign language skilled soldiers not identified on electronic Military Personnel Office System (eMILPO) and Defense Integrated Management Human Resource System (DIMHRS). The Standard Installation Division Personnel System (SIDPERS) was replaced by eMILPO.
- Deploy and provide administrative support of DA and DOD civilian linguists.
- Hire, contract for, and provide administrative support of LN linguists.
- Procure Army foreign language support personnel for screening local labor resources.

Assistant Chief of Staff, G2 (S2):

- Identify linguist requirements needed to support G2/S2 functions in all contingency areas. G2/S2 requirements for linguist support include but are not limited to—
  - Evaluate and/or use local maps and terrain products in operations.
  - Process for MI purposes material taken from EPWs or civilian internees.

  - At lower echelons, conduct tactical questioning of refugees, detainees, and EPWs.
  - Assess local open-source information for intelligence value.
  - Coordinate intelligence and liaison with multinational and HN counterpart.
- Determine, during the initial IPB, all foreign languages (spoken and written) and dialects needed for mission accomplishment.
- Collect, process, produce, and disseminate information derived from linguist sources.
- Provide intelligence training for MI linguists employed in AOs.
- Coordinate for security investigations, as necessary, for local hire linguists.
- Provide support to CI screening of contracted linguists and LN labor force.

Assistant Chief of Staff, G3 (S3):

- Identify linguist requirements needed to support G3/S3 functions in all contingency areas. G3/S3 requirements for linguist support include but are not limited to—
  - Operational coordination and liaison with multinational and HN counterparts.
  - Translate OPORDs and OPLANs for use by multinational counterparts.
- Consolidate unit linguistic requirements and establish priorities.
- Develop linguist deployment and employment plans.
- Develop plans to train linguists and to use linguists for training the force in AO's foreign language survival skills. In addition to global language skills, linguists must have training in specific vocabulary used in the AO; for example, terms used for military, paramilitary, civilian or terrorist organizations, and ethnic groups within the area, nomenclatures of equipment used, and other military or technical vocabulary. Training in the specific dialect used in the AO would also be beneficial.
- Assign, attach, and detach linguists and linguist teams.
- Integrate additional or replacement linguists through operational channels.
- Recommend modernization and development of linguist systems and methods.
- Coordinate mobilization and demobilization of RC linguist support.
- Plan linguist usage for deception operations.
- Plan linguist support for movement of EPWs, detainees, and refugees.
- Coordinate evaluation of linguist support by all staff elements.

Assistant Chief of Staff, G4 (S4):

- Identify linguist requirements needed to support G4/S4 functions in all contingency areas. G4/S4 linguist requirements for linguist support include but are not limited to—

- Procure local supply, maintenance, transportation, and services.
- Coordinate logistics at air and seaports of debarkation.
- Contract with local governments, agencies, and individuals for sites and storage.

- Provide logistical, supply, maintenance, and transportation support to attached linguists.

Assistant Chief of Staff, G5 (S5):

- Identify linguist requirements needed to support G5/S5 functions in all contingency areas. G5/S5 linguist requirements for linguist support include but are not limited to—
  - Determine civilian impact on military operations.
  - Minimize civilian interference with combat operations.
  - Inform civilians of curfews, movement restrictions, and relocations.
  - Provide assistance to liaison with HN and multinational agencies, dignitaries, and authorities.
  - Promote positive community programs to win over support.
  - Determine if multinational operations PSYOP efforts are mutually planned and synchronized.
  - Interpret support to assist resolution of civilian claims against the US Government.
  - Solicit linguistic and cultural knowledge support to protect culturally significant sites.
  - Use linguistic and cultural support to identify cultural and religious customs.
- Assist the G1 in the contracting of local hire linguists.
- Identify foreign language requirements for CMOs.

Assistant Chief of Staff, G6 (S6):

- Identify linguist requirements needed to support G6/S6 functions in all contingency areas. G6/S6 linguist requirements for linguist support include but are not limited to—
  - Coordinate suitable commercial information systems and services.
  - Coordinate with multinational forces on command frequency lists.
  - Coordinate signal support interfaces with HN and multinational forces.
- Manage RF assignments for supporting SIGINT linguist elements.
- Support linguist operations with internal document reproduction, distribution, and message services.
- Integrate automation management systems of linguist units.

SPECIAL STAFF OFFICER RESPONSIBILITIES

B-10. If no special staff officer is assigned the duties below, the corresponding coordinating staff officer should assume those responsibilities. Linguist requirements for special staff officers include but are not limited to the following staff officers.

Liaison Officer:

- Should speak the required foreign language. If not, he requires a translator or interpreter for all aspects of his duties.
- Request interpreters to assist when representing the multinational operations.
- Translate orders, maps, traces, overlays, and documents into multinational foreign languages.

Civilian Personnel Officer:

- Recruit, interview for suitability, and hire civilian local labor force if required.
- Negotiate host country on labor agreements.

Dental Surgeon:

- Administer dental care to support humanitarian mission requirements.
- Rehabilitate, construct, and gain usage of existing dental facilities as required.

Finance Officer:

- Support the procurement process of local goods and services not readily available through normal logistical channels.
- Ensure limited non-US and US pay functions to foreign national, HN, civilian internees, and EPWs are provided.
- Ensure all necessary banking functions are performed in theater.

Surgeon:

- Support medical humanitarian assistance and disaster relief operations.
- Provide medical care of EPWs and civilians within the command's AO.
- Coordinate medical laboratory access in AO.
- Determine the nature of local health threats to the force through populace interviews.
- Determine the identity of local or captured medical supplies.

Veterinary Officer:

- Determine source and suitability of local foods.
- Assist the local population with veterinary service needs.

Chemical Officer:

- Identify enemy force chemical weapons and equipment.
- Communicate NBC risks to supported populations.

Engineer Coordinator:

- Procure proper local materials to support engineering missions.
- Communicate engineering project requirements to contracted local work force.

- Communicate engineering project impact on local landowners and other affected parties.
- Determine, in coordination with G2/S2, suitability of local topographic maps and terrain products.
- Assess environmental concerns of HN and local populations in combined operations.

Provost Marshal:

- Support dislocated and civilian straggler control activities.
- Support internment and resettlement operations, to include displaced civilians.
- Support weapons buy-back programs, as required, and work closely with civil-military liaisons for payments to local officials.
- Support counter-drug and customs activities.
- When authorized, help foreign civil authorities maintain control.
- Conduct liaison with local LEAs.

PSYOP Officer:

- Produce approved PSYOP propaganda and counter-propaganda media.
- Evaluate PSYOP impact on target audience.

Air Defense Coordinator:

- Identify enemy air defense artillery (ADA) weapons and radars.
- Communicate air defense warnings to supported populations.
- Communicate air defense project requirements to contracted local work force.

Safety Officer:

- Provide safety training to local labor force.
- Communicate warnings of dangerous military operations and other hazards to local populace.

Transportation Officer:

- Coordinate commercial and local transportation needs.
- Coordinate movement scheduling and routes with multinational forces and/or HN.

PERSONAL STAFF OFFICER RESPONSIBILITIES

B-11. Personal staff officers are under immediate control of the commander and have direct access to the commander. Most personal staff officers also perform special staff officer duties, working with a coordinating staff officer. These assignments are on a case-by-case basis, depending on the commander's guidance and the nature of the mission; they are very common in stability operations and support operations. Linguist requirements for special staff officers include but are not limited to the following staff officers.

Chaplain:

- Coordinate religious support with multinational partners.
- Determine the impact of local population religious group faiths and practices on military operations.
- Provide religious support to the community to include hospital patients, EPWs, refugees, and civilian detainees.
- Conduct liaison with local population religious leaders in close coordination with the G5.

Public Affairs Officer:

- Act as the commander's spokesman for all communication with external media.
- Assess the accuracy of foreign media interpretation of Public Affairs Office (PAO) releases.
- Assess and recommend news, entertainment, and other information (assisting G5) for contracted services foreign nationals.

Staff Judge Advocate:

- Translate and interpret foreign legal codes, SOFAs, and international laws.
- Determine local environmental laws and treaties through translation services.
- Assess the treatment of EPWs and civilian internees.
- Translate documents to support G4 in local contracts.

SOURCES OF LINGUISTS

B-12. There are various sources that a commander can use to obtain the linguists necessary to support operations. It is vital to know the advantages and disadvantages of each type of linguist and to carefully match the available linguists to the various aspects of the operation.

ARMY LANGUAGE-QUALIFIED MOSs

B-13. The AC MI language-dependent military occupational specialities (MOSs) are 98G with a skill qualification identifier (SQI) of L/352G (Cryptologic Communications Interceptor/ Locator), and their related WO fields. Some soldiers in MOS 96B (All-Source Intelligence Analyst), MOS 97B (CI Agent), MOS 97E/351E (HUMINT Collector) and MOS 98C (SIGINT Analyst), and their related WO fields are trained in foreign languages. Using soldiers in the MOSs mentioned above has many advantages. They are already trained in the military system, are not subject to deployment restrictions (a limiting factor with civilian linguists), have a security clearance and, as US personnel, support the command's interests. The major disadvantage to utilizing these individuals for general foreign language support is that in doing so, they are removed from their primary MI functions. They should be used only in linguistic duties that include intelligence potential. For example, a HUMINT collector (97E) provides linguist support to a medical assistance team as a method to provide access to the local population to determine their attitudes toward US Forces.

B-14. Non-MI Army language qualified MOSs include some enlisted and WOs in career management fields 18 (Special Forces), 37 (PSYOP), 180A (Special Forces); and commissioned officers with a branch code 18 (Special Forces); and functional areas 39 (PSYOP and CA) and 48 (Foreign Area Officer). Particular attention must be paid to the recorded language proficiency and test date of these individuals since the standards vary by field. The same advantages and disadvantages apply as with the AC MI linguists.

B-15. RC language-dependent MOSs include those listed above in the AC. RC linguists have the same set of advantages and disadvantages as listed above for AC language-dependent MOSs. The RC also includes linguists in MOS 97L (translator/interpreter). The 97Ls are specifically trained to be a translator and interpreter. They have the same advantages as the AC linguists. An added advantage is that since their sole job is translation and interpretation, they do not have to be removed from another job in order to be used as a linguist. Their major disadvantage is that they have no additional skill that gives them dual functionality.

Army Linguists Not DOD Trained

B-16. The Army also includes numerous soldiers of all grades who are proficient in a foreign language and are receiving Foreign Language Proficiency Pay (FLPP) but whose primary duties do not require foreign language proficiency. They may have attended a civilian school to learn a foreign language, or they may have acquired proficiency through their heritage. They have the advantage of being trained soldiers and are therefore readily deployable to all areas of the battlefield.

B-17. These soldiers may have the specific vocabulary and military skill knowledge for certain linguist support missions. For example, a supply sergeant who speaks the local language would be an invaluable asset to the G4. There are disadvantages in that they already have another job and units are reluctant to give up personnel especially if they are in key positions. Their capabilities are difficult to assess. Since they are not required to take the Defense Language Proficiency Test (DLPT) if they are not receiving FLPP, it is often difficult for the G1/S1 to identify them as a linguist or for a non-linguist to judge the level of their foreign language capability.

Other Service Linguists

B-18. Other service linguists have the advantage of deployability, loyalty, and clearance, but must often learn the Army system and specific Army vocabulary. They are also difficult to obtain since their parent service probably also lacks a sufficient number of trained linguists. Other service linguists, however, will be valuable in joint operation centers and joint activities. When serving the JTF headquarters, Army commanders and staffs must be aware of the linguists in the other services in order to plan for the participation and optimize their employment.

US Contract Linguists

B-19. US civilians can be contracted to provide linguist support. They have an advantage over LN hires in that their loyalty to the US is more readily evaluated, and it is easier for them to be granted the necessary security

clearance. However, there are usually severe limitations on the deployment and use of civilians. A careful assessment of their language ability is important because, in many cases, they use "old fashioned" terms, or interject US idioms. If the linguists are recent émigrés, the use of the language in their country of origin could be dangerous to them, or their loyalty may reside with their own country when at odds with US interests.

Multinational Linguists

B-20. Multinational linguists have their own set of advantages and disadvantages. These linguists may be unfamiliar with the US military system unless they have previously participated in a multinational operation with US forces. They may have a security clearance, but clearances are not necessarily equal or reciprocal, automatically guaranteeing access to classified or sensitive information between nations. They support the command's interest but may have differing priorities or responsibilities within their assigned AOs. These linguists also are already fulfilling specific duties for their own nation, which may also have a shortage of linguists. The major disadvantage to acquiring and maintaining multinational linguist support is that they are outside the C2 (via military authority or military contract) of the US forces. These linguists will be valuable in multinational operations centers and activities.

Local National Contract Linguists

B-21. LN hires will provide the bulk of your linguist support. They are usually less expensive to hire than US civilians and will know the local dialect, idioms, and culture. The expertise of these linguists in particular areas or subject matters can be an asset. However, there are several potential problems with using LN hires, to include limited English skills and loyalty considerations. Therefore, a screening interview or test is necessary to determine their proficiency in English. These individuals must also be carefully selected and screened by CI personnel (with US linguist support) initially and periodically throughout their employment. Their loyalty is always questionable. Local prejudices may influence them, and they may place their own interests above those of the US.

EVALUATING LINGUIST PROFICIENCY

B-22. Commanders and staffs must understand the Army linguist proficiency evaluation system in order to effectively plan for and employ linguists. Evaluation and reevaluation of linguist proficiency is covered in detail in AR 611-6, Section III. Language testing is required for all Army personnel in a language-dependent MOS, who have received foreign language training at government expense, who are receiving FLPP, or who are in a language-required position regardless of MOS. Other Army personnel who have knowledge of a foreign language are encouraged to take the proficiency test and may work as linguists.

B-23. The Army uses the DLPT to determine foreign language proficiency levels. DLPTs are listed by foreign language in DA Pam 611-16. In foreign languages where no printed or recorded test exists, oral interview tests are arranged. The DLPT is an indication of foreign language capability, but it is

not the definitive evaluation of an individual's ability to perform linguist support.

B-24. AR 611-6, Appendix D, Sections 1 through 4, describes the proficiency levels for the skills of speaking, listening, reading, and writing a foreign language based on the interagency roundtable descriptions. The plus-level designators, shown as a "+" symbol, are used to designate when a linguist is above a base level, but not yet to the capability of the next level. For example, 2+ would indicate a better than limited working proficiency in the foreign language. The six "base levels" of proficiency, as established by DLPT and/or oral exam, are—

- Level 0 (No proficiency). The soldier has no functional foreign language ability. Level 0+. The minimum standard for Special Forces personnel indicates a memorized proficiency only.
- Level 1 (Elementary proficiency). The soldier has limited control of the foreign language skill area to meet limited practical needs and elementary foreign language requirements.
- Level 2 (Limited working proficiency). The linguist is sufficiently skilled to be able to satisfy routine foreign language demands and limited work requirements.
- Level 3 (General professional proficiency). The linguist is capable of performing most general, technical, formal, and informal foreign language tasks on a practical, social, and professional level.
- Level 4 (Advanced professional proficiency). The linguist is capable of performing advanced professional foreign language tasks fluently and accurately on all levels.
- Level 5 (Functionally native proficiency). The linguist is functionally equivalent to an articulate and well-educated native in all foreign language skills; and reflects the cultural standards of the country where the foreign language is natively spoken.

B-25. The above proficiency base levels designate proficiency in any of the four language skills: listening, reading, speaking, and writing. The most evaluated skills on the DLPT are reading and listening. These tests are <u>not</u> for use in evaluating linguists above the 3 proficiency level. Most Army linguist DLPT scores show only two skill levels: listening and reading (for example, 2+/3, or 3/1+).

SUSTAINING MILITARY LINGUIST PROFICIENCY

B-26. Language proficiency diminishes with lack of use and absence of exposure to the foreign language. To ensure combat readiness, commanders should require all military linguists receive periodic language training. In-country language immersion training, in-garrison contracted language instructors, on-line foreign newspapers, and foreign radio broadcasts are all examples of language training resources. Funding for language training is available through MACOM language training program funds.

Glossary

The glossary lists acronyms and terms with Army or joint definitions, and other selected terms. Where Army and joint definitions are different, (Army) follows the term. Terms for which FM 2-0 is the proponent FM (authority) are marked with an asterisk (*) and followed by the number of the paragraph (¶) where they are discussed. For other terms, the number of the proponent FM follows the definition. JP 1-02 and FM 1-02 are posted in the Joint Electronic Library, which is available online and on CD-ROM.

- Use this URL to access JP 1-02 online: http://www.dtic.mil/doctrine/jel/doddict/.
- Use this URL to access FM 1-02 online: http://www.dtic.mil/doctrine/jel/service_pubs/101_5_1.pdf.
- Follow this path to access JP 1-02 on the Joint Electronic Library CD-ROM: Mainmenu>Joint Electronic Library>DOD Dictionary.
- Follow this path to access FM 1-02 on the Joint Electronic Library CD-ROM: Mainmenu>Joint Electronic Library>Service Publications>Multiservice Pubs> FM 101-5-1.

A2C2	Army Airspace Command and Control
AA	avenue of approach
AAMDC	Area Air and Missile Defense Command
ABCS	Army Battle Command System
AC	Active Component
ACE	analysis and control element
ACINT	acoustic intelligence (water)
ACOUSTINT	acoustic intelligence (atmosphere)
ACR	armored cavalry regiment
ACT	analysis and control team
ADA	air defense artillery
ADCON	administrative control
ADDO	assistant deputy director for operations
ADO	air defense officer
ADP	automated data processing
AFACSI	Air Force Assistant Chief of Staff for Intelligence
AFIWC	Air Force Information Warfare Center
AFMIC	Armed Forces Medical Intelligence Center
AFOSI	Air Force Office of Special Investigation
AGM	attack guidance matrix

AIA	Air Force Intelligence Agency
AITR	aided target recognition
ALOC	administrative and logistics operations center
AMC	US Army Materiel Command
AMD	Air Missile Defense
AMHS	Automated Message Handling System
AMIB	Allied Military Intelligence Battalion
***analysis**	Determination of the significance of the information, relative to information and intelligence already known, and drawing deductions about the probable meaning of the evaluated information. (¶1-58)
AO	area of operations
AOC	area of concentration
AOI	area of interest
AOIR	area of intelligence responsibility
AOR	area of responsibility
AR	Army Regulation
ARAT	Army Reprogramming Analysis Team
ARCENT	US Army Central Command
ARFOR	Army forces
ARISC	Army Reserve Intelligence Support Center
ARL	airborne reconnaissance low
ARNG	US Army National Guard
ARSOF	Army Special Operations Forces
ASCC	Army Service Component Commander
ASPO	Army Space Program Office
AT	antiterrorism
ATCAE	Army Technical Control Analysis Element
ATCCS	Army Tactical Command and Control System
ATR	automatic target recognition
ART	Army tactical task
BDA	battle damage assessment
BDU	battle-dress uniform
BFACS	Battlefield Functional Area Control System
BOS	Battlefield Operating System

C/J2	combined J2
C2	command and control
CA	civil affairs
CASO	Collection Activities and Source Operations
CAT	crisis action team
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosive
CCD	coherent change detection
CCIR	commander's critical information requirement
CD-ROM	compact disc-read only memory
CE	counterespionage
CECOM	Communications-Electronics Command
CED	captured enemy document
CEE	captured enemy equipment
CEM	captured enemy materiel
CFSO	counterintelligence force protection source operations
CGS	common ground station
CI	counterintelligence
CIA	Central Intelligence Agency
CIAC	counterintelligence analysis cell
CICA	Counterintelligence Coordinating Authority
CITO	Central Imagery Tasking Office
CJCS	Chairman, Joint Chiefs of Staff
CMEC	Captured Materiel Exploitation Center
CMF	career management field
CMISE	Corps Military Intelligence Support Element
CMO	civil-military operations
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNN	Cable News Network
CNO	computer network operations
COA	course of action

COCOM	combatant command (command authority)
COG	center of gravity
COMINT	communications intelligence
COMSEC	communications security
CONOPS	contingency operations
CONPLAN	contingency plan
CONUS	continental United States
COP	common operational picture
COSCOM	Corps Support Command
***counterintelligence**	**1.** Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02) **2.** (Army) Counterintelligence counters or neutralizes intelligence collection efforts through collection, CI investigations, operations, analysis and production, and functional and technical services. CI includes all actions taken to detect, identify, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies; and is the key intelligence community contributor to protect US interests and equities. (FM 2-0) (¶1-111)
CP	command post
CRN	command radio net
CS	combat support
CSG	cryptologic support group
CSS	combat service support
CSSCS	Combat Service Support Control System
CT	Counterterrorism
***cueing**	The use of one or more sensor systems to provide data that directs collection by other systems. (¶2-53)
CWT	combat weather team
DA	Department of the Army
DAC	Department of the Army Civilian
DAPDM	Department of the Army Production and Dissemination Management
DCI	Director of Central Intelligence
DCS, G2	Deputy Chief of Staff, Intelligence

***debriefing**	The systematic questioning of individuals to procure information to answer specific collection requirements by direct and indirect questioning techniques. (¶6-4)
DF	direction finding
DHS	Defense HUMINT Service
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIMHRS	Defense Integrated Management Human Resource System
DIO	Defensive Information Operations
DISCOM	Division Support Command
DISUM	daily intelligence summary
DLPT	Defense Language Proficiency Test
DMS	Director of Military Support
DOCEX	document exploitation
***document exploitation**	The systematic extraction of information from all media formats in response to collection requirements. (¶6-4)
DOD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
DP	decision point
DPM	dissemination program manager
DS	direct support
DSM	decision support matrix
DST	decision support template
EA	electronic attack
EAC	echelons above corps
ECOA	enemy course of action
EEFI	essential elements of friendly information
ELINT	electronic intelligence
EM	electromagnetic
eMILPO	electronic Military Personnel Office System
EMS	electromagnetic spectrum
E-O	electro-optical
EOB	electronic order of battle
EOD	explosive ordinance disposal

EP	electronic protection
EPW	enemy prisoner of war
ES	electronic warfare support (Army)
***evaluating**	**1.** Comparing relevant information (RI) on the situation or operation against criteria to determine success or progress. (FM 6-0) **2.** In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (FM 2-0) (¶1-26 and 1-98)
EW	electronic warfare
EWS	electronic warfare support (joint)
FBI	Federal Bureau of Investigation
FDA	functional damage assessment
FDU	Force Design Update
FEMA	Federal Emergency Management Agency
FFIR	friendly force information requirement
FISINT	foreign instrumentation signals intelligence
FISS	Foreign Intelligence Security Service
FLPP	Foreign Language Proficiency Pay
FM	Field Manual
FMA	foreign materiel acquisition
FME	foreign materiel exploitation
FMEP	Foreign Materiel Exploitation Program
FMP	Foreign Materiel Program
FMT	Foreign Materiel for Training
FP	force protection
FRAGO	fragmentary order
FS	fire support
FSAC	Fire Support Armaments Center
FSE	fire support element
FSO	fire support officer
G1	Assistant Chief of Staff, Personnel
G2	Assistant Chief of Staff, Intelligence
G3	Assistant Chief of Staff, Operations
G4	Assistant Chief of Staff, Logistics
G5	Assistant Chief of Staff, Civil/Military Affairs

G6	Assistant Chief of Staff, Command, Control, Communications, and Computer Operations
G7	Assistant Chief of Staff, Information Operations
GMI	general military intelligence
GPS	Global Positioning System
GS	general support
GS-R	general support-reinforcing
HN	host nation
HOC	HUMINT operations cell
HPT	high-payoff target
HQ	headquarters
HQDA	Headquarters, Department of the Army
HSI	hyperspectral imaging
HUMINT	human intelligence
***human intelligence**	Collection by a trained HUMINT collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources and a variety of collection methods, both passively and actively, to gather information to satisfy the commander's intelligence requirements and cross-cue other intelligence disciplines. (¶1-106 and ¶6-1)
HVT	high-value target
I/R	internment and resettlement (operations)
I&W	indications and warnings
ICC	Intelligence Coordination Center (US Coast Guard)
ICF	intelligence contingency fund
ICL	intelligence coordination line
IDC	Information Dominance Center
IIR	intelligence information report
IM	information management
IMA	individual mobilization augmentee
IMEP	International Materiel Evaluation Program
IMETS	Integrated Meteorological System
IMINT	imagery intelligence
***indications and warning**	(joint) Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or

allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear or non-nuclear attack on the United States, its overseas forces, or allied and/or coalition nations; hostile reactions to US reconnaissance activities; terrorists attacks; and other similar events. (¶2-19)

***indicator** (Army) Positive or negative evidence of threat activity or any characteristic of the AO which points toward threat vulnerabilities or the adoption or rejection by the threat of a particular capability, or which may influence the commander's selection of a COA. Indicators may result from previous actions or from threat failure to take action. (FM 2-0) (¶5-14)

INFOSEC information security

***infrastructure** **1.** (joint) All building and permanent installations necessary for support, redeployment, and military forces operations (e.g., barracks, headquarters, airfields, communications facilities, stores, port installations, and maintenance stations). (JP 4-01.8) **2.** (Army) In intelligence usage, the basic underlying framework or feature of a thing; in economics, basic resources, communications, industries, and so forth, upon which others depend; in insurgency, the organization (usually hidden) of insurgent leadership. (FM 2-0) (¶5-8)

INR Bureau of Intelligence and Research, Department of State

INS Immigration and Naturalization Service

INSCOM US Army Intelligence and Security Command

intelligence **1.** (joint) The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. **2.** Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (¶1-3)

***intelligence coordination line** A line that designates the boundary between AOIRs. The G2/S2 establishes ICLs to facilitate coordination between higher, lateral, and subordinate units; coordinates with the G3/S3 to direct subordinates to track enemy units and HPTs in their areas; and hands over intelligence responsibility for areas of the battlefield. The establishment of ICLs ensures that there are no gaps in the collection effort; that all echelons are aware of the location, mission, and capabilities of other assets; facilitates asset cueing, and provides timely exchange of information between assets. The G2/S2 keeps abreast of collection activities in progress (all echelons) and battlefield developments through the ICLs. (¶3-13)

intelligence discipline (joint) A well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are seven major disciplines: human

intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), all-source intelligence, technical intelligence, and counterintelligence. (¶1-104)

***intelligence process** — A theoretical model used to describe intelligence operations. The intelligence process is not a framework for actual operations because the functions and common tasks occur in parallel as opposed to sequentially. (¶1-91)

***intelligence products** — Intelligence products are generally placed in one of six categories: I&W, current, general military, target, S&T, and CI. The categories are distinguished from each other primarily by the purpose for which the intelligence was produced. The categories often overlap, and the same intelligence data can be used in each of the categories. (¶1-5)

INTREP — intelligence report

INTSUM — intelligence summary

***intelligence requirements** — (Army) Those requirements generated from the staff's IRs regarding the enemy and environment that are not a part of the CCIR (PIR and FFIR). Intelligence requirements require collection and can pro-vide answers in order to identify indicators of enemy actions or intent, which reduce the uncertainties associated with an operation. Significant changes (i.e., branches and sequels) with an operation usually lead to changes in intelligence requirements. (¶2-7)

***intelligence running estimate** — The intelligence running estimate is a continuous flow and presentation of relevant information and predictive intelligence that, when combined with the other staff running estimates, enable the decisionmaker's visualization and situational understanding of the AOI in order to achieve information superiority. The intelligence running estimate requires constant verification to support situational understanding of the current situation as well as predictive assessments for future operations. (¶5-30)

***intelligence synchronization** — The task that ensures ISR operations are linked to the commander's requirements and respond in time to influence decisions and operations. The intelligence officer, with staff participation, synchronizes the entire collection effort to include all assets the commander controls, assets of lateral units and higher echelons units and organizations, and intelligence reach to answer the commander's CCIR (PIR and FFIR). (¶1-24)

***intelligence synchronization plan** — The plan the intelligence officer uses, with staff input, to synchronize the entire collection effort to include all assets the commander controls, assets of lateral units, and higher echelon units and organizations, and intelligence reach to answer the commander's CCIR (PIR and FFIR). (¶1-38)

IO — information operations

IPB	intelligence preparation of the battlefield
IPIR	Initial Phase Imagery Report
IPTF	international police task force
IR	information requirement
IRINT	infrared intelligence
IRR	Individual Ready Reserve
ISM	intelligence synchronization matrix
ISR	intelligence, surveillance, and reconnaissance
J2	Joint Staff Directorate, Intelligence
J2A	Joint Staff Directorate, Intelligence (Administrative)
J2J	Joint Staff Directorate, Intelligence (Joint)
J2M	Joint Staff Directorate, Intelligence (Management)
J2O	Joint Staff Directorate, Intelligence (Operations)
J2P	Joint Staff Directorate, Intelligence (Assessments, Doctrine)
J2T	Joint Staff Directorate, Intelligence (Targeting)
J2X	Joint Staff Directorate, Intelligence (CI & HUMINT)
J3	Joint Staff Directorate, Operations
J5	Joint Staff Directorate, Civil Affairs
JAC	Joint Analysis Center
JCMEC	Joint Captured Materiel Exploitation Center
JCO	Joint Commission Observers
JCS	Joint Chiefs of Staff
JDEC	Joint Document Exploitation Center
JDISS	Joint Deployable Intelligence Support System
JFC	joint force commander
JIAWG	joint interagency working group
JIC	Joint Intelligence Center
JIF	Joint Interrogation Facility
JISE	joint intelligence support element
JOA	joint operations area
JP	Joint Publication
JSTARS	Joint Surveillance Target Attack Radar System
JTF	joint task force
JTMD	joint table of mobilization and distribution

JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LASINT	laser intelligence
LCC	land component commander
LEA	law enforcement agency
LIDAR	laser radar
LN	local national
LNO	liaison officer
LOC	line of communication
LOS	line of sight
LPT	logistics preparation of the theater
LTIOV	latest time information is of value
MACOM	major Army command
MASINT	measurement and signature intelligence
***materiel**	(Army) In intelligence usage, the all-encompassing term for the weapons systems, equipment, apparatus, documents, and supplies of a foreign military force or nonmilitary organization. (¶2-24)
MCIA	Marine Corps Intelligence Agency
MCOO	modified combined obstacle overlay
MCS	Maneuver Control System
MDMP	military decisionmaking process
MEA	munitions effects assessment
METL	mission-essential task list
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, civil considerations
MI	military intelligence
MLT	machine language translation
MNFC	multinational force commander
MO	method of operation
MOPP	mission-oriented protective posture
MOS	military occupational specialty
MP	military police
MSC	major subordinate command
MSE	mobile subscriber equipment

MSI	multi-spectral imagery
MSIC	Missile and Space Intelligence Center
MTI	moving target indicator
MTOE	modified table of organization and equipment
MTW	major theater war
NAI	named area of interest
NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCA	National Command Authorities
NCO	noncommissioned officer
NCR	national cryptologic representative
NCTI	non-cooperative target identification
NEO	noncombatant evacuation operation
NFH	National Defense Headquarters, Canada
NGA	National Geospatial-Intelligence Agency
NGO	non-governmental organization
NIC	National Intelligence Center
NIIRS	National Imagery Interpretability Rating Scale
NIMA	National Imagery and Mapping Agency
NIST	National Intelligence Support Team
NLT	not later than
NMCC	National Military Command
NMIC	National Maritime Intelligence Center
NMJIC	National Military Joint Intelligence Center
NRO	National Reconnaissance Office
NRT	near-real time
NSA	National Security Agency
NSC	National Security Council
NUCINT	Nuclear Intelligence
NVD	night vision device
OB	order of battle
OE	operational environment
OMA	Office of Military Affairs

OMB	Office of Management and Budget
OMT	operational management team
ONDCP	Office of National Drug Control Policy
ONI	Office of Naval Intelligence
ONIR	overhead non-imaging infrared
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSC	operations support cell
OSCE	Organization for Security and Cooperation in Europe
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
PAO	Public Affairs Office
PDA	physical damage assessment
PIAP	Police Information Assessment Program
PIO	police intelligence operations
PIR	priority intelligence requirement
PME	peacetime military engagement
POC	point of contact
POD	port of debarkation
POE	port of embarkation
***predictive intelligence**	Intelligence analysis conclusions, assessments or products that attempt to define, describe, present, or portray the future situation or condition of the enemy or battlespace. (¶1-3)
***priority intelligence requirements**	(joint) Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision-making. (FM 2-0) (¶1-32)
***process/ processing**	A function of the intelligence process that involves converting collected data, which is not already in a comprehensible form when it is reported, into a form that is understandable and suitable for analysis and production of intelligence. Examples of processing include developing film, enhancing imagery, translating a document from a foreign language, converting electronic data into a standardized report that can be analyzed by a system operator, and correlating dissimilar or jumbled information by assembling like elements before the information is forwarded for analysis. (FM 2-0) (¶1-96)

***production**	In intelligence usage, conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (¶4-20)
PSYOP	psychological operations
QRC	quick reaction capability
QRF	quick reaction force
R&D	research and development
RADINT	radar intelligence
RC	reserve component
RDEC	Research, Development, and Engineering Center
REMBASS	Remotely Monitored Battlefield Sensor System
***requirements management**	The intelligence task that develops a prioritized list of what information needs to be collected and produced into intelligence, dynamically updates and adjusts those requirements in response to mission adjustments/changes, and places a latest time intelligence is of value to ensure intelligence and information is reported to meet operational requirements. (¶2-83)
RF	radio frequency
RFI	request for information
RFW	radio frequency weapon
RI	relevant information
RM	requirements management
ROE	rules of engagement
ROK	Republic of Korea
ROZ	restricted operating zone
RSO&I	reception, staging, onward movement, and integration
RSOC	Regional Security Operations Center
RSP	render safe procedure
RTCAE	Regional Technical Control and Analysis Element
running estimate	A staff estimate, continuously updated, based on new information as the operation proceeds. (FM 6-0) (¶5-28)
S&T	scientific and technical
S&TI	scientific and technical intelligence
S1	Staff Officer, Personnel
S2	Staff Officer, Intelligence
S2X	Staff Officer, Intelligence (CI & HUMINT)

S3	Staff Officer, Operations
S4	Staff Officer, Logistics
S5	Staff Officer, Civil Affairs
S6	Staff Officer, Command, Control, Communications, and Computer Operations
SAP	special access program
SAR	synthetic aperture radar
SATCOM	satellite communications
SBCCOM	Chemical and Biological Defense Command
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SIDPERS	Standard Installation Division Personnel System
SIGINT	signals intelligence
SIGO	signal officer
SII	statement of intelligence interest
SIO	senior intelligence officer
SIPRNET	Secret Internet Protocol Router Network
SIR	specific information requirement
SITMAP	situation map
***situation template**	(Army) A depiction of a potential adversary course of action as part of a particular adversary operation. Situation templates are developed on the adversary's current situation (for example, training and experience levels, logistic status, losses, and disposition), the environment, and adversary doctrine or patterns of operations. The commander dictates the level to depict the adversary based on the factors of METT-TC (at minimum two levels of command below the friendly force) as a part of his guidance for mission analysis. (FM 2-0) (¶1-58)
SJA	staff judge advocate
SMU	special mission unit
SOCOM	satellite communications on-the-move
SOF	special operations forces
SOFA	status of forces agreement
SOP	standing operating procedure
SOTA	SIGINT operational tasking authority
SR	special reconnaissance
SRTD	signals research and target development

SSO	special security office
STANAG	standardization agreement (NATO)
STICEUR	Scientific and Technology Intelligence Center Europe
SUPR	supplemental imagery report
SWO	staff weather officer
TA	target acquisition
TACON	tactical control
***tactical questioning**	The expedient initial questioning for information of immediate tactical value. (FM 2-0) (¶6-6)
TAI	target area of interest
TCAE	technical control and analysis element
TCN	third-country national
***technical control**	The technical function to ensure adherence to existing policies or regulations and provide technical guidance for MI activities, particularly HUMINT, SIGINT, and CI operations. (FM 2-0) (¶3-23)
TECHINT	technical intelligence
TECOM	Test and Evaluation Command
TENCAP	Tactical Exploitation of National Capabilities
TEU	Technical Escort Unit
THREATCON	threat condition
TIB	Theater Intelligence Brigade
TIG	Theater Intelligence Group
TIM	toxic industrial material
TLP	troop-leading procedure
TOC	tactical operations center
TPFDD	Time Phased Force Deployment Data
TRADOC	US Army Training and Doctrine Command
TSA	target system assessment
TSCM	Technical Surveillance Countermeasures
TSE	theater support element
TTP	tactics, techniques, and procedures
TVA	threat vulnerability assessment
UAV	unmanned aerial vehicle
UN	United Nations

US	United States
USAF	United States Air Force
USAR	United States Army Reserve
USC	United States Code
USCENTCOM	United States Central Command
USCG	United States Coast Guard
USCS	United States Cryptologic System
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USNORTHCOM	United States Northern Command
USPACECOM	United States Space Command
USPACOM	United States Pacific Command
USSID	United States Signal Intelligence Directive
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command
USSPACECOM	United States Space Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
VJ2	Vice J2
VTC	video teleconference
WAN	wide area network
WARNO	warning order
WMD	weapons of mass destruction
WO	warrant officer

Bibliography

The bibliography lists field manuals published with new numbers followed by old number.

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. June 1999. [Online] Available http://www.dtic.mil/doctrine/jel/doddict/

FM 1-02/MCRP 5-2A. *Operational Terms and Symbols* (Drag Draft). 21 February 2003.

READINGS RECOMMENDED

These sources contain relevant supplemental information.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online:
http://155.217.58.58/atdls.htm

AR 381-10. *US Army Intelligence Activities*. 1 July 1984.

AR 381-12. *Subversion and Espionage Directed Against the U.S. Army (SAEDA).* 15 January 1993.

AR 381-20. *The Army Counterintelligence Program*. 15 November 1993.

AR 611-6. *Army Linguist Management*. 16 February 1996.

AR 715-9. *Contractors Accompanying the Force*. 29 October 1999.

FM 1 (100-1). *The Army*. 14 June 2001.

FM 2-19.402. *STRYKER Brigade Combat Team Intelligence Operations*. 1 March 2003.

FM 2-19.602. *Surveillance Troop*. 1 March 2003.

FM 2-33.5/ST. *Intelligence Reach Operations*. 1 June 2001.

FM 3-0. *Operations*. 14 June 2001.

FM 3-05.102. *Army Special Operations Forces Intelligence*. 31 August 2001 (formerly FM 34-36).

FM 3-05.30. *Psychological Operations*. 19 June 2000.

FM 3-06.11. *Combined Arms Operations in Urban Terrain*. 28 February 2002.

FM 3-13. *Information Operations*. 28 November 2003 (formerly FM 100-6).

FM 3-19. *NBC Reconnaissance*. 19 November 1993.

FM 3-19.1. *Military Police Operations*. 22 March 2001.

FM 3-19.4. *Military Police Leaders' Handbook*. 4 March 2002.

FM 3-19.40. *Military Police Internment/Resettlement Operations*. 30 September 1987.

FM 3-20.98. *Reconnaissance Platoon*. May 2001.

FM 34-2. *Collection Management and Synchronization Planning*. 8 March 1994.

FM 34-52. (FM 2-22-3) *Human Intelligence*. 28 September 1992.

FM 3-90. *Tactics*. 4 July 2001.

FM 3-90.3. *The Mounted Brigade Combat Team*. 1 November 2001.

FM 3-100.4. *Environmental Considerations in Military Operations*. 15 June 2000, Change 1, 11 May 2001.

FM 3-100.21. *Contractors on the Battlefield*. 26 March 2000.

FM 5-170. *Engineer Reconnaissance*. 5 May 1998.

FM 6-0. *Mission Command: Command and Control of Army Forces*. 11 August 2003.

FM 6-20-10. *Tactics. Techniques, and Procedures for the Targeting Process*. 8 May 1996.

FM 6-121. *Tactics, Techniques, and Procedures for Field Artillery Target Acquisition*. 25 September 1990.

FM 7-0. *Training the Force*. 22 October 2002.

FM 7-10. *The Infantry Rifle Company*. 14 December 1990.

FM 7-15. *Army Universal Task List*. 31 August 2003.

FM 7-92. *The Infantry Reconnaissance Platoon and Squad (Airborne, Air Assault, Light Infantry)*. 23 December 1992.

FM 7-100. *Opposing Force Doctrinal Framework and Strategy*. 1 May 2003.

FM 17-97. *Cavalry Troop*. 3 October 1995.

FM 17-98. *Scout Platoon*. 10 April 1999.

FM 19-1. *Military Police Support for the Airland Battle*. 23 May 1988.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

FM 31-20-5. *Special Reconnaissance Tactics, Techniques, and Procedures for Special Forces*. 23 March 1993.

FM 34-2-1. *Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence to Counterreconnaissance*. 19 June 1991.

FM 34-3. *Intelligence Analysis*. 15 March 1990.

FM 34-8-2. *Intelligence Officer's Handbook*. 1 May 1998.

FM 34-10. *Division Intelligence and Electronic Warfare Operations*. 25 November 1986.

FM 34-25. *Corps Intelligence and Electronic Warfare Operations*. 30 September 1987.

FM 34-37. *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations*. 15 January 1991.

FM 34-54. *Technical Intelligence*. 30 January 1998.

FM 34-80. *Brigade and Battalion Intelligence and Electronic Warfare Operations*. 15 April 1986.

FM 34-130. *Intelligence Preparation of the Battlefield*. 8 July 1994.

FM 4-0. *Combat Service Support*. 29 August 2003.

FM 41-10. *Civil Affairs Operations*. 14 February 2000.

FM 100-25. *Doctrine for Army Special Operations Forces*. August 1999.

FM 101-5. *Staff Organization and Operations*. 31 May 1997.

FM 101-5-1. *Operational Terms and Graphics*. 30 September 1997.

FM 101-5-2. *US Army Report and Message Formats*. 29 June 1999.

ST 2-22.7. *Tactical Human Intelligence and Counterintelligence Operations*. April 2002.

ST 2-33.5. *Intelligence Reach Operations*. 1 June 2001.

ST 2-50. *Intelligence and Electronic Warfare Assets*. June 2002.

ST 2-50.4. *Combat Commanders' Handbook on Intelligence*. September 2001 (formerly FM 34-81, 28 September 1992).

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/jel/

JP 0-2. *Unified Action Armed Forces (UNAAF)*. 10 July 2001.

JP 1. *Joint Warfare for the US Armed Forces*. 14 November 2000.

JP 1-06. *Joint Tactics, Techniques, and Procedures for Financial Management During Joint Operations*. 22 December 1999.

JP 2-0. *Joint Doctrine for Intelligence to Operations*. January 2000.

JP 2-01. *Joint Intelligence Support to Military Operations*. 20 November 1996.

JP 2-01.1. *Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting*. 9 January 2003.

JP 2-01.3. *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*, 24 May 2000.

JP 2-02. *National Intelligence to Joint Operations*. 28 September 1998.

JP 2-03. *Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations*. 31 March 1999.

JP 3-0. *Doctrine and Joint Operations*. 1 February 1995.

JP 3-07. *Joint Doctrine for Military Operations Other Than War*. 16 June 1995.

JP 3-07.2. *JTTP for Antiterrorism*. 17 March 1998.

JP 3-08. *Interagency Coordination During Joint Operations,* Volume II. 9 October 1996.

JP 3-09. *Doctrine for Joint Fire Support*. 12 May 1998.

JP 3-09.1. *Joint Tactics, Techniques and Procedures for Laser Designation Operations*. 28 May 1999.

JP 3-11. *Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments*. 11 July 2000.

JP 3-13. *Joint Doctrine for Information Operations*. 9 October 1998.

JP 3-18. *Joint Doctrine for Forcible Entry Operations*. 16 July 2001.

JP 3-35. *Joint Deployment and Redeployment Operations*. 7 September 1999.

JP 3-51. *Joint Doctrine for Electronic Warfare*. 7 April 2000.

JP 3-55. *Doctrine for Reconnaissance, Surveillance, and Target Acquisition Support for Joint Operations (RSTA)*. 14 April 1993.

JP 3-57. *Joint Doctrine for Civil-Military Operations*. 8 February 2001.

JP 3-60. *Joint Doctrine for Targeting*. 17 January 2002.

JP 4-0. *Doctrine for Logistic Support of Joint Operations*. 6 April 2000.

JP 5-0. *Doctrine for Planning Joint Operations*. 13 April 1995.

JP 5-00.2. *Joint Task Force Planning Guidance and Procedures*. 13 January 1999.

PUBLIC LAWS AND OTHER PUBLICATIONS

The United States Code is available online: http://uscode.house.gov/usc.htm

EO 12333. *United States Intelligence Activities*. 4 December 1981.

CJCS Instruction 1301.01, Policy and Procedures to Assign Individuals to Meet Combatant Command Mission-Related Temporary Duty Requirements. 1 July 2001.

CJCSM 3500.04C. *Universal Joint Task List*. 1 July 2002.

Military Standard 2525B, *DOD Interface Standard, Common Warfighting Symbology*. 30 January 1999.

PUBLICATIONS UNDER DEVELOPMENT

FM 2-01. *Intelligence Synchronization*. When published tentatively in July 2004, FM 2-01 will supersede FM 34-2, 8 March 1994, and FM 34-2-1, 19 June 1991.

FM 2-01.2. *Counterintelligence Analysis*. When published tentatively in April 2005, FM 2-01.2 will supersede FM 34-60, 3 October 1995.

FM 2-01.3. *Intelligence Preparation of the Battlefield*. When published tentatively December 2004, FM 2-01.3 will supersede FM 34-130, 8 July 1994.

FM 3-07.2. *Force Protection.* To be published tentatively in August 2005.

FM 5-0. *Army Planning and Orders Production*. When published tentatively in November 2004, FM 5-0 will supersede that portion of FM 101-5 not superseded by FM 6-0.

ST 2-91.6. *Small Unit Support to Intelligence*. To be published tentatively in April 2004.

Index

Entries are by paragraph number

A

Air defense. *See* Battlefield Operating System.

All-Source Intelligence. *See also* Intelligence Disciplines.
- Definition, 1-105, 5-1
- Fundamentals, 5-3
- Products, 5-4
  - ECOA sketches, 5-4
  - Event templates, 5-4
  - Databases, 5-4
  - HPT lists, 5-4
  - Intelligence estimate, 5-16
  - MCOO, 5-4
  - Running estimate, 5-26
  - Role, 5-2

Analysis, 1-55, 1-58, 1-85, 4-26, 6-10, 6-32
- All-source, 1-50, 2-36, 2-60, 5-2, 5-23, 5-32, 5-33, 6-9
- BOS, 4-6
- CI, 1-111, 2-26, 11-14, 11-42, 11-58, 11-59
- COA, 1-11, 1-31, 5-16
- Collection, 5-21
- COP, 5-27
- HUMINT, 6-49, 6-56
- I&W, 2-19
- Imagery, 7-4, 7-12, 7-14, 7-18, 7-19
- In AO, 2-11, 3-9, 3-15
- In support of FP, 1-16
- IPB, 5-10, 6-10
- MASINT, 9-4, 9-6, 9-18, 9-21
- Mission, 6-20, 11-30, 11-61, B-3, B-7
- NGIC, 10-9
- Operational, 5-35, 6-10, 6-14, 11-14
- Predictive, 1-11, 1-15, 2-6, 4-38, 5-12
- Process, 4-26, 4-28, 4-34, 4-35, 5-22, 8-26
- Requirements management, 4-36
- S&T, 2-24
- Strategic, 6-10, 11-14
- Target development, 2-23
- Teams, 2-59
- TECHINT, 10-1, 10-21

Analyze. *See* Intelligence Process.

Armed Forces Medical Intelligence Center (AFMIC), 10-6

Army DCS, 10-8

Assess. *See* Intelligence Process.

Area Studies of Foreign Countries, 1-22, Figure 1-1. *See also* Intelligence Tasks; Support to Strategic Responsiveness.

Army capabilities, 3-17
- Combined arms, 3-19
- Command and support relationships, 3-20, Figure 3-1

B

Battlefield Operating System (BOS). *See also* Intelligence BOS.
- Air defense, 1-4
- Combat service support, 1-4
- Command and control, 1-4
- Fire support, 1-4
- In support of operations, 1-7
- Intelligence, 1-4
- Maneuver, 1-4
- Mobility/countermobility/ survivability, 1-4

C

Categories of Intelligence, 2-17

Central Imagery Tasking Office (CITO), 7-9

Combat assessment, 1-53, Figure 1-1

Combat power
- Elements of, 3-11

Combat service support. *See* Battlefield Operating System.

Command and control. *See* Battlefield Operating System.

Common tasks. *See also* Intelligence Tasks.
- Analyze, 1-101, 4-35
- Assess, 1-103
- Disseminate, 1-102, 4-39

Conduct ISR. *See also* Intelligence Tasks.
- Conduct Surveillance, 1-48
- Conduct Tactical Reconnaissance, 1-46
- Perform Intelligence Synchronization, 1-25
- Perform ISR Integration, 1-39

Conduct surveillance, 1-48, Figure 1-1. *See also* Intelligence Tasks; Conduct ISR.

Counterintelligence. *See also* Intelligence Disciplines.

Counterintelligence (*continued*)
Category of Intelligence, 2-26
Command and control relationship, 11-53
Definition, 1-111, 11-1
Equipment, 11-37
Functions, 11-4 thru 11-15
Levels of employment, 11-22
Operational employment, 11-21
Role, 11-2
Staff responsibilities, 11-56 thru 11-62
Support to contingency operations, 11-25
Support to installations and operating bases, 11-29
Teams, 11-29 thru 11-52, 11-61, 11-62
Counterintelligence Coordinating Authority (CICA), 11-57
Current Intelligence
Category of Intelligence, 2-20

D-E-F

Department of Energy, 2-38
Department of Homeland Security Mission, 2-41
Department of Justice, 2-40
Disseminate. *See* Intelligence Process; common tasks.
Elements of IO. *See* information operations.
Essential Elements of Friendly Information, 1-36
Fire Support, 1-55. *See also* Battlefield Operating System.
Force projection operations, 1-112
Deployment, 1-125
Employment, 1-134
Mobilization, 1-119
Redeployment, 1-141
Sustainment, 1-140
Full spectrum operations, 3-1
Defensive operations, 3-5
Offensive operations, 3-4
Stability operations, 3-8
Support operations, 3-10
Functional damage assessment (FDA), 1-54

G-H

G2/S2. *See* Responsibilities.
General Military Intelligence
Category of Intelligence, 2-21
Human Intelligence (HUMINT) *See also* Intelligence Disciplines.
Collection methods, 6-4
Combat patrolling, 6-7
Definition, 1-106, 6-1
Equipment, 6-27
Functions, 6-3
ISR operations, 6-8
Products, 6-11
Role, 6-2
Staff responsibilities, 6-47 thru 6-55
Support to contingency operations, 6-16
Support to installations and operating bases, 6-19
Strategic and departmental employment, 6-13
Tactical Questioning, 6-6
Teams, 6-20 thru 6-43, 6-56, 6-57

I

Imagery Intelligence (IMINT). *See also* Intelligence Disciplines.
Definition, 1-107, 7-1
Functions, 7-11, 7-14 through 7-22
Fundamentals, 7-3
Role, 7-2, 7-13
Sources of imagery, 7-5
Types of imagery sensors, 7-10, 7-15, Table 7-1
Indications and Warnings, 1-19, Figure 1-1
Category of Intelligence, 2-19
Information
Dimension of OE, 1-67, 1-74
Information Operations, A-1
Definition, A-1, A-5
Elements of, A-2, A-9
Intelligence support to, A-10
Information requirements, 1-28
Comparison, Figure 1-3, 1-30, 1-31
Friendly force, 1-35
Information Superiority, A-3
INSCOM. *See* Responsibilities.
Intelligence. *See also* Intelligence BOS.
BOS, 1-4
Categories of, 2-17
In full spectrum operations, 3-1
Role of, 1-1
Intelligence BOS, 1-4
and the COP, 5-29
Considerations, 4-6
Human sensor information, 6-47, 11-56
In full spectrum operations, 3-2
In offensive operations, 1-7, A-12
In defensive operations, 1-7, A-12
In stability operations, 1-7
In support operations, 1-7
Interoperability, 6-30, 11-40, 11-56
Limitations, 4-6
Requirements, 4-47
Role, 1-51, 1-62, 1-114

Intelligence Community organizations, 2-27, Figure 2-2
Intelligence Disciplines, 1-104
All-source Intelligence, 1-105, 5-1, 5-2 thru 5-4, 5-16, 5-26
CI, 1-111, 2-26, 11-1 thru 11-52, 11-61, 11-62
HUMINT, 1-106, 6-1 thru 6-3, 6-4 thru 6-8, 6-11, 6-13, 6-19 thru 6-43, 6-56, 6-57
IMINT, 1-107, 7-1 thru 7-5, 7-11 thru 7-22, Table 7-1
MASINT, 1-109, 9-1, 9-4, 9-5, 9-9 thru 9-24
SIGINT, 1-108, 8-1, 8-3 thru 8-5, 8-13, 8-14 thru 8-34
TECHINT, 1-110, 10-1, 10-6 thru 10-10, 10-12 thru 10-25
Intelligence estimates, 5-5
Intelligence Preparation of the Battlefield. *See also* Intelligence Tasks; Support to Situational Understanding.
G2/S2 responsible for, 1-11
Intelligence Process, 1-91, 4-1, 4-2, Figure 4-2
Collect, 1-95, 4-18, 5-21, 7-15, 8-22, 9-16, 10-16
Common tasks, 1-91, 4-2
Analyze, 1-101, 4-35, 5-32, 6-10, 7-18, 8-30, 9-21, 10-22
Assess, 1-103, 4-48, 5-35, 7-22, 8-34, 9-24, 10-25
Disseminate, 1-102, 4-39, 5-33, 7-21, 8-32, 9-22, 10-23
Functions, 4-2
Plan, 1-91, 1-92, 4-1, 4-4, 4-8, 5-4, 5-19, 7-11, 8-14, 9-12, 10-12
Prepare, 1-93, 4-8, 5-15, 7-14, 8-18, 9-15, 10-15
Process, 1-96, 4-28, 5-22, 7-16, 8-26, 9-18, 10-18
Produce, 1-98, 4-31, 5-23, 7-17, 8-28, 9-19, 10-19
Intelligence Reach, 2-69
Components, 2-72
Broadcast Services, 2-80
Collaborative Tools, 2-82, Table 2-2
Database Access, 2-80
Pull, 2-73
Push, 2-73
Requirements Management, 2-83
Partners and sources, Table 2-1
Intelligence Readiness, 1-21, Figure 1-1
Intelligence support to IO, 1-52, Figure 1-1
Intelligence support to targeting, 1-51, Figure 1-1
Intelligence synchronization
Activities, 1-26
Considerations, 1-27
Definition, 1-25
Plan, 1-26, 1-37
Intelligence synchronization plan, 1-59, 1-92, 1-121, 1-133, 2-53
Development, 1-41, 5-51
Intelligence Support to Force Protection, 1-14
Intelligence Tasks, 1-9
Support to Situational Understanding, 1-10 thru 1-17
Support to Strategic Responsiveness, 1-18 thru 1-23
Conduct Intelligence, Surveillance, and Reconnaissance, 1-24 thru 1-49
Provide Intelligence Support to Effects, 1-50 thru 1-63
ISR Integration, 1-39, Figure 1-1
ISR Tasks, 4-19
ISR Plan, 1-34, 1-39 thru 1-51, 1-59 thru 1-63, 1-92, 4-40, 6-22, 6-56

J-L

Joint intelligence
Architecture, 2-55
Augmentation considerations, 2-62
Considerations in, 2-52
Operations, 2-48
Organizations, 2-61
Joint Intelligence Center (JIC), 2-57
Joint Task Force J2 Organization, Figure 2-3
Land combat operations
Dimension of OE, 1-67, 1-73
Levels of war, 2-3, Figure 2-1
Operational, 2-9
Strategic, 2-5
Tactical, 2-15
Linguist Support, B-1
Categories, B-1, B-8
Proficiency, B-22, B-26
Responsibilities
Personal Staff Officer , B-11
Special Staff Officer , B-10
Primary Staff , B-9
Requirements, B-3
Sources, B-12

M-O

Maneuver. *See* Battlefield Operating System.
Measurement and Signatures Intelligence (MASINT). *See also* Intelligence Disciplines.
Definition, 9-1
Functions, 9-12 thru 9-24
Fundamentals, 9-9
Role, 9-5

MASINT (continued)
Subdisciplines, 9-4
Mobility/countermobility/ survivability. *See* Battlefield Operating System.
Munitions effects assessment (MEA), 1-55
Office of Nonproliferation and National Security, 2-38
Operational Environment
Critical Variables of, 1-79, Figure 1-5
Dimensions of, 1-67, 1-72
Operational framework, 3-13
Area of operations, 3-13
Battlefield organization, 3-13
Battlespace, 3-13
Operations officer. *See* Responsibilities.

P

Physical damage assessment (PDA), 1-54
Plan. *See* Intelligence Process.
Police Intelligence Operations, 1-17, Figure 1-1
Political
Dimension of OE, 1-67, 1-71
Prepare. *See* Intelligence Process.
Principles of war, 3-12
Priority intelligence requirements, 1-32
Comparison, Figure 1-3
Development, 1-33
Process. *See* Intelligence Process.
Produce. *See* Intelligence Process.
Provide Intelligence Support to Effects. *See also* Intelligence Tasks.
Provide Intelligence Support to Combat Assessment, 1-53
Provide Intelligence Support to Information Operations, 1-52
Provide Intelligence Support to Targeting, 1-51

R-S

Responsibilities
*2X staff, 6-47
AFMIC, 10-6
Army DCS, 10-8
CICA, 11-57
CITO, 7-9
Commander's, 3-5, 3-13, 3-15, 3-21, 6-45, 11-54
Department of Justice, 2-40
Fire support personnel, 1-55
G2/S2, 1-11, 2-19, 2-20, 3-16, 10-14
INSCOM, 2-13, 9-10, 10-9
JIC, 2-57
Office of Nonproliferation & National Security, 2-38
Operations officer, 1-41
Staff sections, B-9
Running estimate, 5-26, 5-30
S&T Intelligence
Category of Intelligence, 2-24
Sensitive Site Exploitation, 1-23, Figure 1-1
Signals Intelligence (SIGINT), 1-108, 8-1. *See also* Intelligence Disciplines.
At Echelons Corps and Below, 8-13
Definition, 8-1
Functions, 8-14 thru 8-34
Fundamentals, 8-4
Role, 8-3
TCAE Architecture, 8-5
Situation Development, 1-12 Figure 1-1. *See also* Intelligence tasks; support to situational understanding.
Situational Understanding, 1-10
Staff sections. *See* Responsibilities.
Support to Situational Understanding. *See also* Intelligence Tasks.
Perform IPB, 1-11
Perform Situation Development 1-12
Provide Intelligence Support to Force Protection, 1-14
Conduct Police Intelligence Operations, 1-17
Support to Strategic Responsiveness. *See also* Intelligence Tasks.
Perform I&W, 1-19
Ensure Intelligence Readiness, 1-21
Conduct Area Studies of Foreign Countries, 1-22
Support Sensitive Site Exploitation, 1-23

T

Tactical Reconnaissance, 1-46, Figure 1-1. *See also* Intelligence Tasks; Conduct ISR.
Tactical questioning. *See* Human Intelligence.
Target Intelligence
Category of Intelligence, 2-23
Target system assessment (TSA), 1-54
Task organization, 3-18
Technical Intelligence (TECHINT). *See also* Intelligence Disciplines.
Assets, 10-6 through 10-10
Definition, 1-110, 10-1
Functions, 10-12 thru 10-25
Fundamentals, 10-5
Technology
Dimension of OE, 1-67, 1-76
Tenets of Army operations, 3-12

Threat
Dimension of OE, 1-67, 1-68

U

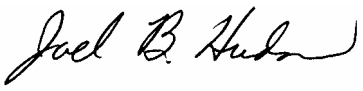
Unified Action
Intelligence and, 2-1
Intelligence operations, 2-11, 2-44
Joint intelligence operations, 2-48
Architecture, 2-15
Augmentation considerations, 2-62
Considerations in, 2-52
JTF organizations, 2-61
Multinational Intelligence, 2-66

FM 2-0
17 MAY 2004

By order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:



JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
0412505

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number 111117, requirements for FM 2-0.

PIN: 081441-000

MCWP 2-10
(Formerly MCWP 2-1)

Intelligence Operations

US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 143 000036 00

CD&I (C 116)

2 May 2016

ERRATUM

to

MCWP 2-1

INTELLIGENCE OPERATIONS

1. Change all instances of MCWP 2-1, *Intelligence Operations*, to MCWP 2-10, *Intelligence Operations.*

2. File this transmittal sheet in the front of this publication.

PCN 143 000036 80

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to **morgann@mccdc.usmc.mil**. Recommendations should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Add, delete
  - Proposed new text, preferably double-spaced and typewritten
- Justification and/or source of change

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status.* An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: **http://www.doctrine.usmc.mil**.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

10 September 2003

FOREWORD

Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations*, builds on the doctrinal foundation established in Marine Corps Doctrinal Publication (MCDP) 2, *Intelligence*. It provides tactics, techniques, and procedures (TTP) for Marine air-ground task force (MAGTF) intelligence operations. This publication is intended for commanders, other users of intelligence, and intelligence personnel who plan and execute intelligence operations.

This publication supersedes MCWP 2-1, *Intelligence Operations,* dated 19 February 1998.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

EDWARD HANLON, JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

Publication Control Number: 143 000036 00

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

MCWP 2-1, INTELLIGENCE OPERATIONS

TABLE OF CONTENTS

Chapter 1. Fundamentals

Intelligence Objectives 1-1
Maneuver Warfare 1-2
Developing Intelligence 1-2
    Data, Information, and Intelligence 1-2
    The Intelligence Cycle 1-3
Intelligence Operations 1-4
    Relationship to Command and Control. 1-4
    Relationship to Operations 1-5
Principles of Intelligence Operations 1-5
Intelligence Functions 1-6
    Support the Commander's Estimate 1-6
    Develop the Situation 1-7
    Provide Indications and Warning 1-7
    Support Force Protection 1-7
    Support Targeting 1-7
    Support Combat Assessment 1-7
The Commander's Role in the Intelligence Process 1-8
    Focus the Intelligence Effort. 1-8
    Participate in the Intelligence Process 1-8
    Use Intelligence in Decisionmaking 1-8
    Support the Intelligence Effort 1-8
    Evaluate the Results of Intelligence Activities 1-9
Information Operations 1-9
    Planning 1-9
    Intelligence Preparation of the Battlespace. 1-9
    IO-Related Force Protection 1-9
    The Role of Intelligence in IO is Continual 1-10
Required Intelligence Capabilities 1-10

Chapter 2. Command and Control

Decisionmaking 2-1
    Observe, Orient, Decide, and Act Loop 2-1
    Intelligence and the OODA Loop 2-2
    Decisionmaking Approaches: Analytical and Intuitive 2-2

The Planning, Decision, Execution, and Assessment Cycle 2-3
Intelligence Support to Planning 2-3
Planning Models 2-3
Mission Analysis 2-4
COA Development 2-5
COA War Game 2-6
Orders Development 2-6
Execution 2-7
Resource Allocation 2-8
Linkage to Operations 2-8
Generation of Tempo 2-8

Chapter 3. Developing Intelligence

Intelligence Requirements 3-2
Priority Intelligence Requirement 3-4
Characteristics 3-4
Planning and Direction 3-4
Requirements Development 3-4
Requirements Management 3-5
Directing the Intelligence Effort 3-6
Collection Management 3-7
Production Management 3-7
Dissemination Management 3-7
Planning the Intelligence Support System 3-7
Collection 3-7
Imagery Intelligence 3-8
Signals Intelligence 3-8
Human Intelligence 3-9
Measurement and Signature Intelligence 3-9
Open-Source Intelligence 3-9
Counterintelligence 3-10
Processing and Exploitation 3-10
Production 3-10
Intelligence Preparation of the Battlespace 3-10
Levels of Production 3-11
Dissemination 3-12
Form 3-12
Delivery 3-13
Channels 3-14
Architectures 3-15
Utilization 3-15
Application of the Intelligence Cycle 3-17
Counterintelligence 3-17
Responsibilities 3-17
CI Planning 3-18
CI Measures 3-19

Chapter 4. Concept of MAGTF Intelligence Support

Role of the Organic Intelligence Section 4-2
The Unit Intelligence Officer 4-2
The Unit Intelligence Section 4-3
Required Capabilities 4-3
The MAGTF Intelligence Section 4-3
MAGTF Intelligence Officer 4-3
Special Staff Officers under Staff Cognizance of G-2 Officer 4-4
MAGTF Intelligence Units 4-9
Organization of MAGTF-Level Intelligence Units 4-9
Employment of MAGTF Intelligence Units 4-11
Focused Intelligence Support 4-12
Intelligence Nodes 4-12
Split-basing 4-12
Task Organization of Intelligence Support Units 4-13
Intelligence DSTs 4-13
Intelligence Coordination 4-13
External Intelligence Support to the MAGTF 4-14
MARFOR Component Intelligence Section 4-14
National, Theater, Joint, and Other Service Intelligence Support 4-16
Augmentation 4-17
Supporting Establishment 4-17
Marine Corps Intelligence Activity 4-17
Marine Cryptologic Support Battalion 4-18
Navy Marine Corps Intelligence Training Center 4-18
Personnel Augmentation 4-18
Marine Corps Forces Reserve 4-18

Chapter 5. Operational Maneuver from the Sea

Required Intelligence Capabilitites 5-1
Planning and Direction 5-1
Collection 5-2
Processing, Exploitation, and Production 5-2
Dissemination 5-3
Utilization 5-3
Planning and Direction 5-3
Collection 5-4
Processing, Exploitation, and Production 5-4
Dissemination 5-4
Utilization 5-5

Chapter 6. Sustained Operations Ashore

Required Intelligence Capabilities 6-1
Planning and Direction 6-1
Collection 6-2

Processing, Exploitation, and Production 6-3
Dissemination 6-3
Utilization 6-4

Chapter 7. Military Operations Other Than War

Required Intelligence Capabilities 7-1
Planning and Direction 7-2
Collection 7-2
Processing, Exploitation, and Production 7-3
Dissemination 7-3
Utilization 7-3

Chapter 8. Joint Operations and Multinational Operations

JFC and Component Commander Responsibilities 8-1
Joint Intelligence Structure 8-1
Procedures 8-2
Marine Intelligence Section and Unit Responsibilities 8-2
MARFOR Component Headquarters or
MAGTF CE as a JTF Headquarters 8-2
Multinational Operations 8-2

Appendices

A. Glossary A-1
B. References B-1

List of Figures

1-1. The Information Hierarchy 1-3
1-2. Key Considerations of the Intelligence Cycle 1-3
1-3. Relationship Between Intelligence Functions and Operations 1-7

2-1. The Observe, Orient, Decide, and Act Loop 2-1
2-2. Intelligence Support to Planning 2-4

3-1. The Marine Corps Intelligence Cycle 3-1
3-2. The Intelligence Cycle—Macro View 3-2
3-3. The Intelligence Cycle—Micro View 3-2
3-4. Intelligence Development and the Intelligence Cycle 3-3
3-5. Planning and Direction Phase Functions 3-4
3-6. Intelligence Requirements Management 3-5
3-7. Requirements Satisfaction 3-6
3-8. MAGTF Primary Organic Collection Assets 3-8
3-9. Intelligence Preparation of the Battlespace 3-11
3-10. Graphic Climatology Study 3-13
3-11. Graphic Intelligence Estimate 3-14
3-12. Notional Marine Expeditionary Force Intelligence Architecture 3-16

3-13. Application of the Intelligence Cycle 3-18
3-14. The Counterintelligence Process 3-20

4-1. Special Staff Officers and Relationships under the Staff Cognizance of the MEF G-2 4-5
4-2. AC/S G-2's Principal Subordinate Staff Officers and their Responsibilities 4-7
4-3. Intelligence Battalion 4-10
4-4. Intelligence Operations Center 4-14
4-5. The National Intelligence Community 4-16

5-1. Intelligence Considerations During OMFTS 5-2

6-1. Intelligence Considerations During Sustained Operations Ashore 6-2

7-1. Intelligence Factors in MOOTW 7-2

CHAPTER 1
FUNDAMENTALS

Intelligence is knowledge of the battlespace and of the threat forces in that battlespace. Knowledge is generated in support of the commander's decisionmaking process and is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat.

Intelligence Objectives

Intelligence has two objectives: to reduce uncertainty by providing accurate, timely, and relevant knowledge about the threat and the surrounding environment, and to assist in protecting friendly forces (to include Department of Defense [DOD] personnel, family members, resources, facilities and critical information) through counterintelligence (CI).

Uncertainty pervades the battlespace—it is a fundamental attribute of war. First and foremost, intelligence should support the commander's decisionmaking process by reducing uncertainty about the hostile situation. Intelligence should accomplish the following actions to achieve this objective:

- Identify and evaluate existing conditions and capabilities.
- On the basis of those existing conditions and capabilities, estimate possible enemy courses of action (COAs) and provide insight into possible future actions.
- Aid in identifying friendly critical vulnerabilities that the threat may exploit.
- Assist in developing and evaluating friendly COAs.

The fog and friction of war will never allow the commander to have a perfect picture of the battlespace. Because intelligence deals with the greatest number of unknowns—questions about an unfamiliar area and a hostile enemy who is actively trying to conceal information about his forces and intentions—there will almost always be gaps in intelligence, and the knowledge provided will lack the desired degree of detail and reliability. Intelligence cannot provide absolute certainty. It attempts to reduce the uncertainty facing the commander to a reasonable level by collecting relevant information, placing it in context to provide knowledge, and conveying it in the form of images to enhance understanding.

CI is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons or international terrorist activities.

CI activities consist of active and passive measures, functions, and services. CI measures, functions, and services are intended to deny a potential adversary information that might increase the effectiveness of hostile operations against friendly forces; detect and neutralize foreign intelligence collection; and deceive the enemy as to friendly capabilities and intentions. In so doing, CI increases uncertainty for the enemy, thereby making a significant contribution to the success of operations. CI services identify friendly vulnerabilities, evaluate security measures, and assist in implementing appropriate plans to enhance a unit's force protection posture against the threats of sabotage, subversion, and terrorism.

Maneuver Warfare

The essence of war is a violent clash between independent wills, each trying to impose itself on the other. War's defining attributes of friction, uncertainty, fluidity, disorder, and complexity combine with the various dimensions of human nature to make war a fundamentally unpredictable activity. To succeed in war, Marines must be able to operate effectively in this uncertain, chaotic, complex, and fluid environment.

The Marine Corps philosophy for winning under these conditions is based on rapid, flexible, and opportune maneuver. MCDP 1, *Warfighting*, states that, "Maneuver warfare is a warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope." Maneuver warfare requires maneuver in time and space to achieve superiority over the enemy. It concentrates on those actions that present the enemy with a series of dilemmas where events happen unexpectedly and faster than the enemy can react. Concepts central to executing maneuver warfare follow:

- **Orienting on the enemy.** Maneuver warfare attacks the enemy "system," the combination of physical, moral, and mental components that make up an enemy or an enemy force. This means focusing outward on the particular characteristics of the enemy.
- **Centers of gravity (COG) and critical vulnerabilities.** COG are sources of moral or physical strength, power or resistance that are critical to the enemy's ability to resist. Critical vulnerabilities are components of the enemy system that are both crucial to the functioning of the system and vulnerable to exploitation. Identifying and exploiting an enemy's COG and critical vulnerabilities help focus combat power toward a decisive aim.
- **Main effort.** The main effort is the unit assigned responsibility to accomplish the key mission within the command. It is directed where there is the best opportunity to succeed and at the objective that will have the most significant effect on the enemy, normally a critical vulnerability.
- **Commander's intent.** Commander's intent describes the purpose behind the task assigned in a mission. It provides continuing guidance when the tactical situation changes and permits the exercise of initiative in harmony with the commander's desires.
- **Mission tactics.** Mission tactics assign subordinates a task without specifying how it must be accomplished. They permit subordinates to exercise initiative in adapting to ever-changing situations.
- **Tempo.** Tempo keeps the enemy off balance, thereby increasing his friction. Speed, initiative, and flexibility generate and maintain a tempo that the enemy cannot match.

Accurate and timely intelligence is a prerequisite for success in maneuver warfare. Maneuver warfare is based on a firm focus on the enemy and on taking action that avoids enemy strengths and exploits enemy critical vulnerabilities. It means acting in a manner and at a time and place that the enemy does not expect and is not prepared. It requires decision and action based on situational awareness—a keen understanding of the factors that make each situation unique. Intelligence provides the knowledge of the enemy and the battlespace that permits the commander to reduce uncertainty, identify opportunities for success, assess risk, outline intent, and make decisions that provide focus, generate speed and tempo, and achieve decisive results.

Developing Intelligence

Data, Information, and Intelligence

Intelligence is not simply another term for information. Intelligence is more than an element of

data or a grouping of information; it is a body of knowledge. Knowledge occupies a unique place in the information hierarchy, which is a framework to distinguish between various classes of information. (See figure 1-1.)

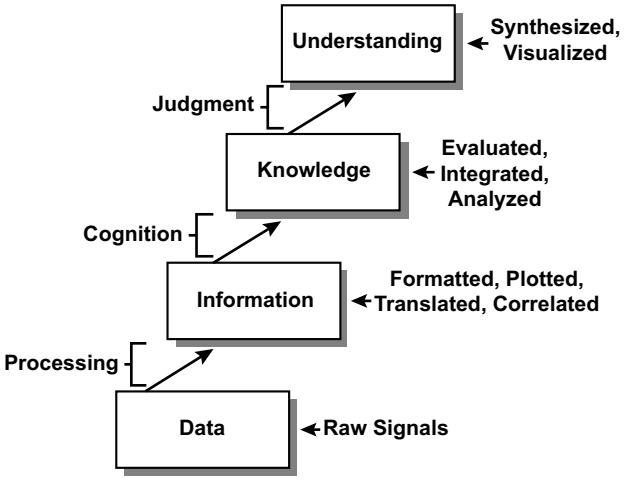


Figure 1-1. The Information Hierarchy.

There is a clear and important distinction between raw data, information, and intelligence. Intelligence is not a mass of unfocused data or even a collection of related facts. In fact, giving a commander every piece of data without providing meaning can increase uncertainty by overloading the commander with incomplete, contradictory or irrelevant information. To be intelligence, data must be placed in context to provide an accurate and meaningful image of the hostile situation. Intelligence is developed by analyzing and synthesizing data and information to produce knowledge about the threat and the environment. The commander combines this knowledge with knowledge of the friendly situation and employs experience, judgment, and intuition to understand the situation. The commander then applies this understanding in making decisions.

The Intelligence Cycle

Intelligence is the output of a process that converts data and information into knowledge that applies to a specific military decision. The process used to develop intelligence is called the intelligence cycle. This cycle is the process by which information is planned for, obtained, assembled, converted through analysis into intelligence, provided to decisionmakers, and, ultimately, used in making decisions. (See figure 1-2.)

Intelligence Cycle	Key Considerations
Planning and direction.	Identify intelligence requirements. Plan intelligence operations and activities. Support the formulation of the commander's estimate of the situation.
Collection.	Develop the required intelligence structure. Use organic, attached, and supporting intelligence sources to collect intelligence.
Processing, exploitation, and production.	Conversion of raw data and information into a suitable form of intelligence.
Dissemination.	Timely provision of intelligence, in appropriate form, to those who need it.
Utilization.	Use of intelligence.

Figure 1-2. Key Considerations of the Intelligence Cycle.

The intelligence cycle consists of a series of related activities that translate the need for intelligence about a particular aspect of the battlespace or threat into a knowledge-based product that is provided to the commander for use in the decisionmaking process. In this sequence, intelligence needs are identified and a plan is developed for satisfying those needs. Data are collected, processed into information, and converted into intelligence through analysis and synthesis. The resulting knowledge is then provided to the commander as an intelligence product that is used in making decisions. The information used to produce intelligence is derived from a variety of sources. Intelligence information; i.e., information used to generate intelligence, is commonly drawn from three types of data: intelligence, sensor or combat.

Intelligence data is derived from assets primarily dedicated to intelligence collection; e.g., imagery systems, electronic intercept equipment or human intelligence (HUMINT) sources.

Sensor data is derived from sensors whose primary mission is surveillance or target acquisition; e.g., air surveillance radars, counterbattery radars, and remote ground sensors.

Combat data is derived from reporting by operational units. Because of their highly perishable or critical nature, combat data and sensor data are sometimes used to effect decisions without being converted into intelligence. Although the demands of the ongoing battle may require rapid action, decisions based on raw, unprocessed data or single pieces of data should be avoided.

Processing, analysis, and synthesis of data and information into intelligence can be accomplished rapidly at all levels. We seek knowledge—*accurate intelligence, not incomplete, unfocused, or unevaluated information*—to enhance our understanding and base our decisions. The intelligence cycle works continuously to satisfy intelligence shortfalls and confirm or refute fragmentary information. Once collected and processed, information is converted into intelligence through the application of experience and judgment. Information is analyzed to determine its significance and is synthesized with other relevant information to build a coherent picture of existing conditions and capabilities. This picture is then used to predict possible outcomes of environmental conditions and enemy actions. Results are conveyed to the commander in an intelligence product. Because humans understand situations best as images—mental pictures—intelligence is produced and disseminated in graphic form whenever possible. The process is completed when the knowledge provided is applied to influence decisionmaking.

Intelligence Operations

Intelligence personnel and organizations perform a number of separate and distinct activities and functions that are collectively known as intelligence operations. Intelligence operations are conducted to provide intelligence in support of the decisionmaking process of commanders down to the small-unit level. The primary focus of Marine Corps intelligence operations is generating *tactical intelligence*; i.e., intelligence that supports the planning and conduct of tactical actions. Although the focus is on tactical intelligence, the Marine Corps must draw on both strategic and operational intelligence resources and, in certain circumstances, be prepared to conduct intelligence operations at the operational and even strategic level. Intelligence reduces uncertainty and supports the decisionmaking process by—

- Describing the battlespace.
- Identifying key factors in the battlespace that can influence operations.
- Defining and evaluating threat capabilities.
- Identifying the enemy's COG and critical vulnerabilities.
- Assessing enemy intentions.

Relationship to Command and Control

Intelligence is a fundamental component of command and control (C2). C2 is the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. A principal aim of C2 is to enhance the commander's ability to make sound and timely decisions. Intelligence facilitates the commander's decisionmaking process by making a major contribution to the understanding of the battlespace and the threat. Intelligence is also an

integral element of the process through which the commander implements decisions. Inadequate or imperfect intelligence can significantly inhibit the ability of a commander or subordinates to carry out these decisions. Lack of a continuous, effective intelligence effort also degrades the quality of feedback to the commander about the unfolding situation; it is this feedback that allows the commander to modify the actions of the command as needed.

Because intelligence is crucial to success on the battlefield, it must be given command attention. The commander drives intelligence by focusing the intelligence effort through the definition of the mission, articulation of his intent, and designating priority intelligence requirements (PIRs). A PIR is an intelligence requirement (IR) associated with a decision that will critically affect the overall success of the command's mission. PIRs are a subset of commander's critical information requirements (CCIRs) and are focused on the environment and the threat.

Relationship to Operations

Intelligence is inseparable from operations. Intelligence drives operations by shaping the planning and execution of operations. It provides a menu of factors that the commander considers when making a decision. Specifically, intelligence—

- Identifies potential advantages offered by the environment.
- Describes limitations imposed by the environment.
- Ascertains and assesses enemy strengths to be avoided.
- Uncovers enemy critical vulnerabilities that can be exploited.
- Recommends COAs based on factors of the battlespace and threat.
- Enables rapid decisionmaking and generating and maintaining tempo.

Operational actions develop logically from intelligence. A commander with effective intelligence knows the nature of the terrain, weather conditions, the composition and status of the infrastructure in the area of operations, the makeup and attitude of the population that will be encountered, and how the combined effects of these factors will influence mission accomplishment. Intelligence provides knowledge of threat capabilities, strengths, COG, and critical vulnerabilities, along with insight into the enemy's intentions. Integrating intelligence on the threat and the battlespace helps to provide the commander with situational awareness, which is used to determine the decisive time and place to strike.

Intelligence and operations must be linked throughout the planning, decision, execution, and assessment (PDE&A) cycle at all levels. Intelligence shapes the plan and provides the knowledge that facilitates execution. It identifies changes in the situation that require modification of the plan or that trigger decisions during the conduct of the operation. At the same time, the nature of the mission and the concept of operations focus and shape the intelligence effort; intelligence that is not relevant to the mission is useless. IRs and intelligence operations are continually evaluated to ensure that they are focused on supporting mission accomplishment.

Principles of Intelligence Operations

- **The focus is on tactical intelligence.** The focus of Marine Corps intelligence operations is on the generation of tactical intelligence. However, there are no sharp boundaries between levels of intelligence; they merge and form a continuum. In some instances Marine Corps tactical intelligence operations will support operational and strategic IRs.
- **Intelligence is focused downward.** Intelligence must be available to commanders at all

levels. Although the management of intelligence collection and production is centralized in the MAGTF command element (CE), the focus is on providing the intelligence needed to plan and execute the mission to every unit involved in the operation. Requirements of the entire force will be considered in directing the intelligence effort. Critical products will be *pushed* down to the tactical commander, who will be able to *pull* additional intelligence support as needed.

- **Intelligence drives operations.** The Marine Corps' warfighting philosophy depends on timely, accurate intelligence for success. Intelligence is the critical underpinning for each phase of the PDE&A cycle.
- **Intelligence activities require centralized management.** Good intelligence is the result of the integration of many separate and specialized collection, processing, and analytical resources. The scarcity of these assets, coupled with the requirement to focus on the commander's PIRs, creates the need for centralized coordination and management. This centralization will be done in the MAGTF CE, under the direction of intelligence officers who are trained and experienced in the management of multidiscipline, all-source intelligence operations. (All-source intelligence is intelligence that incorporates all available sources of information in the development of the finished intelligence product.) *Although centralized coordination and management is required for efficient and effective use of intelligence assets, it is critical for the commander who is exercising centralized control to allocate appropriate resources to ensure that needs of subordinate commands that are crucial to mission accomplishment are properly addressed.*
- **The G-2/S-2 facilitates use of intelligence.** The intelligence officer enables effective use of intelligence throughout the command. As the principal disseminator of intelligence, the intelligence officer ensures that the full implications of the intelligence picture are understood. To do this, the intelligence officer must be a *full and continuous* participant in the planning process.
- **Intelligence must be tailored and timely.** Intelligence must be tailored to the requirements of the user, provided in a useful format, and received in time to affect the decisionmaking process. Delivery of the right intelligence—not simply data or information—to the right place at the right time must be the guiding principle of all dissemination efforts.
- **Utilization is the final step of the intelligence cycle.** Intelligence has no inherent value; its value is derived from its support of decisionmaking. The intelligence cycle is not complete until the intelligence that has been developed is used to plan and/or execute operations.

Intelligence Functions

All six functions are carried out continually during the PDE&A cycle at all levels throughout the force. However, particular functions may be stressed more during one phase of the cycle. Different units may emphasize one or two functions over the others based on individual missions. (See figure 1-3.)

Support the Commander's Estimate

Intelligence supports the formulation and subsequent modification of the commander's estimate of the situation by providing as accurate an image of the battlespace and the threat as possible. Intelligence supports initial planning and decisionmaking. One of the principal tools used in this function is intelligence preparation of the battlespace (IPB). IPB is a systematic, continuous process of analyzing the threat and environment in a specific geographic area. IPB helps to provide an appreciation for the characteristics of the area of operations and the enemy capabilities, weaknesses, and COAs. This knowledge affords the commander an understanding of the battlespace and the opportunity to exploit enemy critical vulnerabilities.

Intelligence Functions	Decisionmaking	Operational Activities
Support to commander's estimate.	Plan a mission.	Develop and analyze COAs.
Situation development.	Execute the mission.	Monitor execution. Modify plan as necessary.
Indications and warning.	Orient on contingencies.	Increase readiness. Develop contingency plans.
Support to force protection.	Force protection.	Support operations security (OPSEC). Nuclear, chemical, and biological defense. Support deception plan.
Support to targeting.	Plan fire support.	Attack targets.
Support to combat assessment.	Reorient forces. Plan future operations.	Consolidate, pursue, exploit. Reattack targets.

Figure 1-3. Relationship Between Intelligence Functions and Operations.

Develop the Situation

Situation development provides continuing knowledge of unfolding events to help update the estimate of the situation. It is a dynamic process that assesses the current situation and confirms or denies the adoption of specific COAs by the enemy. It helps refine our understanding of the battlespace and reduces uncertainty and risk. Situation development occurs during execution and provides the basis for adapting plans or exploiting opportunities.

Provide Indications and Warning

Indications and warning (I&W) serve a protective purpose, providing early warning of potential hostile action. They help prevent surprise and reduce risk from enemy actions that run counter to planning assumptions.

Support Force Protection

Force protection is the set of comprehensive security measures, collection activities, and operations that are undertaken to guard the force against the effects of enemy action. Intelligence supports force protection by identifying, locating, and countering foreign intelligence collection, sabotage, subversion, and terrorism capabilities. Support to force protection requires detailed and accurate assessments of threat force capabilities and intentions and facilitates efforts to deny the enemy the opportunity to take offensive action against our forces.

Support Targeting

Intelligence supports targeting by identifying target systems, critical nodes, and high-value and high-payoff targets as well as by providing the intelligence required to most effectively engage these targets.

Support Combat Assessment

Combat assessment is the process used to determine the overall effectiveness of military operations and identify requirements for future actions. Intelligence supports the entire combat assessment process and is directly responsible for battle damage assessment (BDA), which is one of the principal components of combat assessment. BDA is the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations.

The Commander's Role in the Intelligence Process

Intelligence is an inherent and essential responsibility of command. Commanders must come to think of command and intelligence as inseparable, just as they commonly think of command and operations as inseparable. They must study and understand the theory and the practice of intelligence doctrine. They must be personally involved in the conduct of intelligence activities, and provide guidance, supervision, judgment, and authority to ensure a timely and useful product.

Focus the Intelligence Effort

The commander must provide the guidance and direction necessary for the effective conduct of intelligence activities. Intelligence assets will rarely be sufficient to satisfy every requirement. Thus, the intelligence effort must be focused on clearly articulated priorities that drive the concept of intelligence support and the collection, production, and dissemination efforts. The commander provides this focus through articulating the commander's intent, planning guidance, and the command's PIRs.

Participate in the Intelligence Process

Although the intelligence officer manages the intelligence effort for the commander, the commander is responsible for the results. Effective participation requires an understanding of the practical capabilities and limitations of intelligence personnel, equipment, procedures, and products. The commander should supervise the process, interjecting guidance and direction at key points to ensure that the process is responding to the commander's intent; e.g., the commander should define the scope of the IPB effort, identify the preferred intelligence product format, and establish priorities among subordinate commands' IRs.

Use Intelligence in Decisionmaking

Intelligence exists for the primary purpose of aiding the commander's decisionmaking process. Although the intelligence officer facilitates the use of intelligence throughout the command by providing timely dissemination of the intelligence product and ensuring that the meaning of the intelligence is understood, the commander makes the judgment of its operational impact. The commander makes a personal analysis of the intelligence product and arrives at the estimate of the situation that serves as the basis for the decision. This act is the responsibility of the commander and no one else.

Support the Intelligence Effort

Intelligence is a team effort. Good intelligence is the result of integrating many separate and specialized collection, processing, and analytical resources. Some of these resources are organic to the unit; many are provided by units or agencies outside the command. Intelligence operations by organic assets normally cannot succeed without support from throughout the command. Reconnaissance teams must be inserted, sensors implanted, and communications assets provided for dissemination. Timely and effective intelligence dissemination requires dedicating significant C2 assets. Once an operation begins, nearly every Marine will have the occasion to observe significant facts about the enemy and environment. All personnel should understand and carry out their responsibility to collect and report information. The commander must ensure that all members of the unit understand the importance placed on intelligence and the requirement to support the intelligence effort. External support must be requested and coordinated. The intelligence staff executes the procedures to obtain the required support, but does so in the name of the commander. When the command's support requirements go unsatisfied, the commander must intervene, lending command authority to obtain the support.

Evaluate the Results of Intelligence Activities

The commander must provide feedback to the intelligence support system. Feedback should identify where the intelligence provided met expectations and where and how it fell short. Key areas to evaluate include product content, presentation, timeliness, and overall usefulness. Meaningful evaluation of the intelligence effort provides the basis for its continual improvement.

Information Operations

Intelligence support is required to conduct information operations (IO). Specific intelligence is required for planning and deconfliction and for employing military disciplines available to achieve IO effects. Intelligence is inextricably linked to facilitating core and supporting IO disciplines in offensive or defensive postures. As a product, intelligence supports IO in the same manner provided to all operations. Planning for IO cannot be conducted without intelligence on adversary information and information systems, perceptions, and critical vulnerabilities in their C2 process. Each capability used in an IO context will have separate and continuous intelligence support requirements. The psychological profiles of adversary commanders and forces are themselves an important element within the overall assessment process.

Planning

Intelligence support to IO planning is conducted as part of the IPB process. One of the key outputs from IPB is an analysis of the desired objectives and/or end states of stakeholders. These desires are usually categorized relative to broad capability. The categories may be elements of national power such as politics, economics, military, and society. Capability analysis processes within IPB also provide detail on stakeholder capacity and intent to conduct or sustain defensive and offensive IO. Intelligence support will aim to define critical nodes and vulnerabilities within the adversary's information structure; these include the key personnel, equipment, procedures and protocols involved in the transfer of information required for successful C2. Such intelligence support will orient key aspects of the operation plan towards the systematic disruption of critical nodes and information bearers. Friendly force staff advice, linked to intelligence advice on adversary COAs and CI advice on the threats to security, provide the operations planning process with the background to decide the protective measures required for own nodes and information bearers. Accurate, timely, and directed intelligence provides the foundation that IO decisions are based.

Intelligence Preparation of the Battlespace

IPB is a continuous process used to develop a detailed knowledge of the adversary's use of information and information systems. Intelligence support for IO planning builds upon traditional IPB and provides the essential basis for planning IO through the following considerations:

- The adversary commander's freedom of action and the freedom of action allowed to subordinates (decisionmaking process). This includes adversary perceptions of the situation (political, social, and cultural influences) and developments.
- Adversary IO capability, intent, morale, and vulnerability to offensive IO.
- C2 aspects such as key personnel, target audiences, headquarters, communications nodes, databases or intelligence collection systems. C2 nodes that appear in more than one adversary COA should be highlighted for targeting.
- Technical knowledge of a wide array of information, C2, intelligence, and media systems.
- Assessments of friendly vulnerability to adversary IO.

IO-Related Force Protection

Knowledge of the threat—adversaries, their intent, and capabilities—is a key consideration in the risk

management process. CI and counterreconnaissance contribute directly to force protection by denying critical information to potential adversaries. Many IO IRs require significant lead-time to develop collection sources, access, and databases. Potential intelligence collection sources should be developed as early as possible; a clear statement of MAGTF IRs is essential. IO will require development of extensive intelligence analytical products to obtain a detailed knowledge of cultural factors, and adversary use of information and information systems.

The Role of Intelligence in IO is Continual

Changes in attitudes, actions, operating patterns, and enemy information systems must be detected, analyzed, and reported to ensure that IO continues to achieve the desired operational effect. Assessing ongoing IO activities is a crucial and extremely challenging responsibility of intelligence as targets must be monitored to determine the effectiveness of the IO efforts. To achieve complete synthesis, IO must be incorporated into the MAGTF's intelligence, BDA, and targeting cycles. The impact of many IO actions may be difficult to measure. Indicators of success or failure must be carefully crafted in advance. Since IO will often not produce the same directly observable effects used for traditional BDA, IO execution will challenge the intelligence system to develop other measures of effectiveness. Once detected, these indicators should be integrated into operational planning and targeting systems, and appropriate action can be taken.

Intelligence enables the planning and execution of successful operations. MAGTF operations are characterized by unity of effort, high tempo, timely decisionmaking, rapid execution, and the relentless exploitation of opportunities. Intelligence operations must have the flexibility, agility, and sustainability to support these types of operations. Expeditionary Maneuver Warfare, as the Marine Corps' current capstone concept, lays the foundation for MAGTF operations. MAGTF operations include--

- Operational maneuver from the sea (OMFTS).
- Sustained operations ashore.
- Military operations other than war (MOOTW).
- Joint.
- Multinational.

Each operation presents unique challenges and considerations for intelligence support. Many MAGTF operations will be executed as joint operations and with allies, coalition or multinational partners. Intelligence activities in joint and multinational operations require special planning and coordination.

Required Intelligence Capabilities

As a warfighting function, intelligence applies broadly across the full range of military operations. The following required intelligence capabilities are common to all operations:

- Conduct intelligence planning and direction.
- Perform intelligence collection management.
- Process and exploit intelligence.
- Produce intelligence.
- Disseminate intelligence.
- Facilitate intelligence's use.
- Perform intelligence, surveillance, reconnaissance, and CI operations.

CHAPTER 2
COMMAND AND CONTROL

C2 aims to reduce the amount of uncertainty that commanders must accept—to a reasonable point— to make sound decisions. Intelligence is a principal component of C2. Intelligence is a process conducted specifically to aid the commander in decisionmaking by reducing this uncertainty. Intelligence operations support the commander's PDE&A cycle by helping to build situational awareness and providing insight into the nature of the problem facing the commander.

Intelligence provides knowledge concerning the environment and the enemy while furnishing an estimate of potential enemy activities. This knowledge is used by the commander to devise workable, flexible plans; make sound and timely decisions; monitor events to ensure proper execution; and modify decisions quickly in response to changing situations or to exploit fleeting opportunities.

Decisionmaking

The principal aim of C2 is to enhance the commander's ability to make sound and timely decisions. Decisionmaking is a time-competitive process that depends in part on the availability of the right elements of information at the right time and place. Without the information that provides the basis of situational awareness, no commander can make sound decisions. Intelligence operations focus on providing the right elements of information concerning the threat and the environment; i.e, intelligence, required to generate situational awareness and fuel the decisionmaking process.

Observe, Orient, Decide, and Act Loop

A simple model that is known as the observe, orient, decide, and act (OODA) loop is used to describe the C2 process. (See figure 2-1.)

The OODA loop applies to any two-sided conflict, whether combatants are individuals or large military formations. When engaged in conflict, participants—

- **Observe.** Take in information about the environment, the friendly status, and the threat.
- **Orient.** Make estimates, assumptions, analyses, and judgments about the situation to create a cohesive mental image.
- **Decide.** Determine what needs to be done, whether it is an immediate reaction or a deliberate plan.
- **Act.** Put the decision into action.

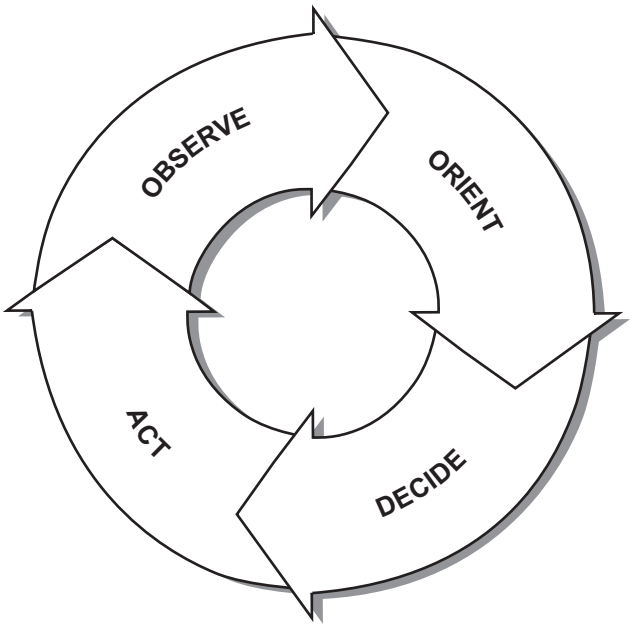


Figure 2-1. The Observe, Orient, Decide, and Act Loop.

The OODA loop reflects how decisionmaking is a continual, cyclical process. In any conflict, the participant who can consistently and effectively cycle through the OODA loop faster—who can maintain a higher tempo of action—gains an increasing advantage with each cycle. The essential lesson of the OODA loop is the importance of generating and maintaining tempo.

Intelligence and the OODA Loop

Intelligence supports all phases of the OODA loop. Intelligence operations facilitate the exercise of C2 by helping to reduce the uncertainty confronting the commander, providing a significant part of the knowledge needed to reach the decision, and assisting in monitoring the implementation and effects of that decision.

- **Observe.** Intelligence collection operations observe threat activity and current environmental conditions. All-source analysis of the collected intelligence information is provided to enhance the commander's situational awareness and understanding of the battlespace.
- **Orient.** The image of the battlespace presented by intelligence, coupled with the predictive analysis of the IPB process, helps orient the commander. It aids in comparing the current situation to the desired end state and in identifying COAs to achieve that end state.
- **Decide.** Intelligence enables decisionmaking by helping define what is operationally possible and most advantageous. It provides the framework for assessing the potential COAs against existing environmental conditions and threat capabilities, vulnerabilities, and likely responses.
- **Act.** Intelligence supports execution by providing a shared picture of the battlespace to all levels of command and by meeting the intelligence needs of all levels of commanders involved in the conduct of operations. Once the concept of operations has been formulated, the focus of intelligence activities shifts from developing the wide-scope intelligence required for COA selection to providing detailed, tailored intelligence to support mission planning and execution. Intelligence is also critical to generating and maintaining tempo in C2. During execution, supporting intelligence operations are conducted to monitor enemy reactions, protect the force from enemy counteraction, and assess the effects of ongoing operations. The continuing intelligence development effort aids the commander in effectively cycling through the OODA loop faster to gain an increasing advantage over the enemy.

Decisionmaking Approaches: Analytical and Intuitive

In analytical decisionmaking, several options for solving the problem at hand are identified, studied, and compared to arrive at the best solution. In intuitive decisionmaking, the commander assesses the situation to recognize a pattern. Once a pattern is identified, experience and judgment guide the commander in evaluating the key elements of the problem and rapidly determining a satisfactory solution. Each approach has different strengths and weaknesses; although conceptually distinct, the two are rarely mutually exclusive.

Intelligence supports analytical decisionmaking by helping to identify the options available and provide the framework (in the form of estimates and studies focused on the threat and key factors of the battlespace) for analysis and comparison of those options. Intelligence supports intuitive decisionmaking by providing the knowledge that helps the commander to recognize emerging patterns. The same methodology is used to develop intelligence support for both decisionmaking approaches. Application of that methodology will vary based on the specifics of each situation and the decisionmaking style of the supported commander. The goal remains the same: to provide a knowledge-based intelligence product that can be applied to make a sound decision.

The Planning, Decision, Execution, and Assessment Cycle

The PDE&A cycle provides a framework for implementing C2. It translates the cognitive process of the OODA loop into a concrete series of actions taken by the commander and the staff to plan and execute an operation. To be effective, intelligence operations must be linked to the commander's decisionmaking process and the resulting operational activity. Therefore, intelligence operations are integrated with the PDE&A cycle. Specific intelligence tasks are carried out to support each phase of this cycle. While the level of command, time available, and specific tactical situation will influence how the PDE&A cycle is carried out and the degree of detail applied in performing intelligence activities, the same basic intelligence development process is employed in deliberate and rapid planning scenarios and supports analytical and intuitive decisionmaking.

Intelligence support to planning begins with providing a basic description of the environmental conditions and enemy situation in the projected area of operations (AO). As plans are developed and refined, the intelligence effort becomes more narrowly focused on identifying the enemy's critical vulnerabilities and potential COAs and generating mission-specific intelligence products that support detailed planning and execution of specific operational activities. Finally, during mission execution, intelligence operations concentrate on the satisfaction of requirements linked to key operational decisions and the recognition of exploitable opportunities as they arise in the battlespace.

Intelligence Support to Planning

Planning is the process of developing practical schemes for taking future actions. It represents an effort to project operational concepts and designs forward in time and space. During the planning process, the commander assesses the situation, builds a vision of the battlespace, and develops the desired outcome of the battle or campaign. Planning is oriented on the future because the primary objective of intelligence is to reduce uncertainty about the future. Intelligence makes a critical contribution to this process. Much of the intelligence effort is "front loaded" to support planning; a substantial portion of intelligence development must be completed during this phase. Intelligence provides a comprehensive image of the battlespace and the threat and helps commanders to provide for constant or predictable aspects of the environment, come to an understanding on the general direction of future actions, and anticipate possible threat force actions and reactions.

Planning Models

The choice of planning model is made on the basis of a variety of factors, including the mission, level of command, command relationships, time available, and preferences of individual commanders. All planning models have the same basic elements in common. They—

- Determine what needs to be done.
- Identify one or more COAs to accomplish the required tasks.
- Study the COAs to test feasibility, identify support requirements, and select the most promising alternative.
- Convey instructions to subordinates to execute the plan.

Intelligence development follows the same basic process, no matter which planning model is used. While the specific steps and sequence used in planning may vary, the requirement to provide focused, continuous intelligence to shape the planning process remains constant. A generic planning model will be used to outline the baseline methodology for providing intelligence support to planning. The components of this generic

model are mission analysis, COA development, COA analysis, and plan/orders development. For a more complete discussion of planning and the planning process, see MCDP 5, Planning, and MCWP 5-1, *Marine Corps Planning Process*. (See figure 2-2.)

Mission Analysis

Mission analysis is conducted to identify the tasks required to accomplish the mission, develop baseline knowledge of the situation, and determine what additional information is required to facilitate the planning process. Intelligence supports mission analysis through providing basic intelligence on the nature of the AO and the threat. Intelligence operations are guided by the results of mission analysis: formulation of initial commander's intent, planning guidance, and PIRs.

Mission Receipt

The receipt of the mission starts the formal planning cycle. However, preliminary planning is normally conducted before the receipt of a mission to anticipate future taskings and potential actions required to accomplish those taskings. Intelligence, in performing its I&W function, will monitor a command's area of interest and identify developing crisis situations and/or potential missions. The commander uses this information to anticipate future missions and to direct the staff to accomplish preliminary planning and intelligence development before the arrival of formal mission tasking. Much of this preliminary

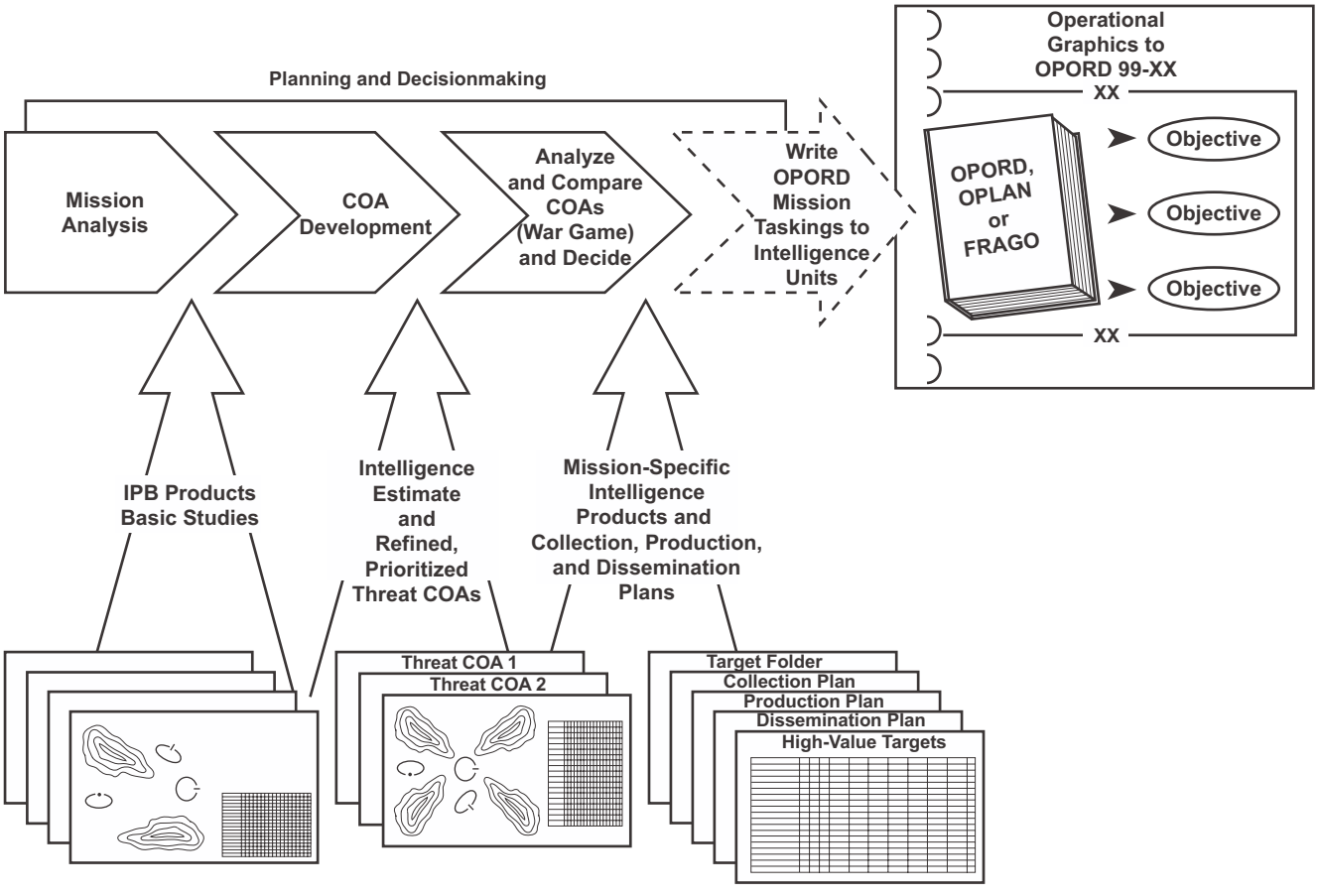


Figure 2-2. Intelligence Support to Planning.

work is carried out by the intelligence section, including collecting basic data on the threat and the environment, IPB analysis, and disseminating intelligence throughout the staff.

Information Requirements and Exchange

The process of identifying IRs and gathering and distributing information within the staff, and throughout the command, begins during preliminary planning and intensifies once the mission is received. Intelligence is provided about threat forces and the AO, focusing on the advantages and limitations presented by the environment and the strengths and critical vulnerabilities of the threat. This intelligence is disseminated through a variety of media: the distribution of basic products (maps, imagery, and threat forces studies); the conduct of orientation briefings, and IPB analysis. The continuous, interactive process of IR development also begins. Products provided by the intelligence section stimulate additional questions from the commander and members of the staff. These questions are translated into new or refined IRs. The new requirements are then used to focus the intelligence development process.

Mission Analysis

The commander makes a critical contribution to the operation during this step, setting the stage for the completion of planning and mission execution. During mission analysis, the commander and the staff draw together all available intelligence and information, focus it on the assigned mission, develop an understanding of the tasks to be accomplished, and formulate a rough concept of how to best accomplish those tasks. The result is an initial statement of commander's intent and commander's planning guidance that focuses the remainder of the planning process.

The intelligence officer is a full participant in mission analysis. During mission analysis, the intelligence officer does the following:

- Orients the commander and the other members of the staff to the battlespace and the nature of the threat.
- Aids in forming the commander's intent by helping to define what is operationally possible and most advantageous. This is accomplished primarily through IPB and the analytical process. These results identify the threat's COG, strengths, and critical vulnerabilities and indicate the potential advantages and limitations imposed by the environment.
- Receives guidance from the commander to help shape the intelligence effort. Guidance can take a variety of forms: a statement of commander's intent, a list of PIRs or direct instructions from the commander about intelligence needs or concerns.

COA Development

Building on the knowledge gained through mission analysis, the commander and staff next develop a concept for carrying out the required tasks that embodies the commander's intent and planning guidance. This concept (or COA) encompasses general schemes for the execution of maneuver, fires, logistics, and other supporting functions necessary for successful implementation of the basic concept.

When time permits, the staff usually develops several COAs on the basis of the commander's intent and planning guidance. Intelligence supports this process by the following:

- Continuously updating the view of the battlespace.
- Defining operational possibilities through the IPB process.
- Identifying intelligence gaps that cannot be filled by organic collection assets.
- Providing the focus on the enemy through identifying the threat's COG, critical vulnerabilities, and potential COAs, emphasizing the most likely and most dangerous of these COAs.
- Ensuring that the commander and staff receive, understand, and use relevant, focused, knowledge-based intelligence that enhances their understanding of the situation, rather than a stream of unfocused information.

The intelligence officer interacts with the staff throughout the COA development process, integrating continuing intelligence development efforts with the potential COAs in an effort to ensure that intelligence will be available to support any COA selected.

When an intuitive approach is used, intelligence helps the commander recognize emerging patterns, identify a workable solution, and rapidly evaluate that solution. Products developed through the IPB process present intelligence in the form of images that permit decisionmakers to quickly visualize the situation, see patterns, and assess potential alternatives.

COA War Game

After COAs are developed, they are analyzed and compared to identify the best COA and the concept of operations to implement that COA. Time permitting, the staff conducts a detailed analysis of each COA; each principal staff officer prepares a formal estimate of supportability. When possible, COAs should be wargamed to predict the action, reaction, and counterreaction dynamics of each COA.

Intelligence assists COA analysis by the following:

- Identifying and refining threat COAs and actions/reactions to friendly COAs under consideration.
- Playing the role of the enemy in the wargaming process.
- Developing an independent evaluation of each friendly COA based on an understanding of the environment and the potential threat response and the ability to provide intelligence support to that COA.
- Helping to focus the staff on the factors of the environment and the enemy, emphasizing the degree of uncertainty and resulting risk associated with each COA.

The intelligence officer's full participation is crucial to successful COA analysis. It is during this step that the full implications of the intelligence estimate are absorbed and applied. To maximize this contribution, the intelligence officer must be able to "think red"—analyze the situation from the enemy's perspective—and "think blue"—understand the intent and construct of friendly plans and operations. Combining these two perspectives enables the intelligence officer to assess the potential effects of threat force actions on the potential COAs.

When time is not available to wargame and conduct a complete COA analysis, the commander makes a rapid mental assessment of available options. The situational awareness that is provided in large part through intelligence guides the commander in evaluating these options and quickly selecting one that offers potential for success.

Orders Development

Based on the COA analysis, the commander selects a COA, refines the intent, and gives further guidance on developing the detailed concept of operations and supporting plans or orders. The emphasis of the intelligence effort, which is focused on the commander's intent, the selected COA, and the identified PIRs, shifts from developing basic and broad-scope intelligence in support of conceptual planning to providing specific intelligence that facilitates functional planning, detailed planning, and mission execution. The intelligence tasks of I&W and supporting the commander's estimate continue, but situation development, support to targeting, and support to force protection now receive increased emphasis.

A concept of intelligence support is prepared to allocate intelligence resources in accordance with the main effort and the concept of operations. COA analysis and wargaming results are used to develop and implement collection, production, and dissemination plans to support the chosen COA. IPB efforts are intensified in an effort to satisfy PIRs and develop the in-depth intelligence required for the detailed planning of specific operational activities. Intelligence sections prepare and disseminate products that embody

the results of the IPB process and intelligence collection activities to provide a shared view of the battlespace at all levels of the force. At the same time, they deliver mission-specific intelligence in response to the extensive and precise functional and detailed planning requirements of units that will execute the operation. CI plans and measures are prepared and implemented to conceal our intentions and protect the force. Results of these intelligence activities shape and develop the overall plan/order and the plan's comprehensive supporting annexes and appendices.

Execution

During execution, the plan is refined, implemented, and adapted in response to changes in the situation and action/reaction of the enemy. C2 is a process that generates swift, appropriate, and decisive action and provides a means of continuously assessing developments that provide the basis for adapting. The commander uses a variety of techniques and measures to supervise, monitor, and modify the execution of the plan, thereby shaping the battle and maintaining unity of effort. The intelligence effort must be responsive to the needs of mission execution and ensure a continuous flow of intelligence throughout the force to maintain a shared picture of the battlespace and satisfy new requirements developed by the operating forces.

Intelligence operations are integrated with the concept of operations to enhance force protection, develop situational awareness, and support combat assessment. The results of these operations are used to modify the plan or exercise tactical options, thereby enabling rapid decisionmaking as well as generating and maintaining tempo. The information developed through these activities is entered into the continuous intelligence development process, which provides the basis for planning future operations.

Intelligence support to execution differs in significant ways from intelligence support to planning. First, while intelligence support to planning requires developing a large volume of basic intelligence and preparing broad-scope estimates to develop and analyze COAs, intelligence support to execution involves the satisfaction of a much larger body of IRs in a significantly greater degree of detail. For example, during COA development, it may be sufficient to tell a MAGTF or ground combat element (GCE) commander that an enemy mechanized force is located in a general area and has an approximate number of tanks and armored personnel carriers of various types. However, the subordinate unit tasked with establishing a blocking position opposite that enemy force will require more detailed information on enemy disposition. In another example, the nature of the intelligence required by a Marine Expeditionary Unit (MEU) commander to decide if a raid or tactical recovery of aircraft and personnel (TRAP) mission is feasible is fundamentally different from the type and detail of intelligence required by the raid or TRAP personnel force commander who will execute that mission.

A second major difference between intelligence support to planning and intelligence support to execution is the time available for developing the intelligence product. Often days, weeks, and sometimes months are available to provide intelligence support to planning, but intelligence support to execution must normally be developed in hours, minutes or even seconds. Success in execution often depends on the ability to provide immediate answers to critical questions concerning threat force dispositions, actions, and intentions.

Finally, the uncertainty and disorder that are inherent in the nature of war manifest themselves primarily during execution. Once execution begins, interaction between the opposing wills of friendly and enemy forces normally causes significant and fundamental changes in

the situation. Discerning environmental conditions and enemy capabilities and intentions becomes increasingly difficult once these forces are set in motion. Yet it is at precisely this time that commanders require detailed and accurate intelligence to help cope with the uncertainty.

The combined factors of the extensive nature of the IRs, the degree of detail required, the limited time available, and the uncertainty inherent during execution make providing intelligence support to execution the most significant intelligence challenge. Intelligence operations must be prepared to meet this challenge and to provide the flexibility and agility required to deliver continuous situational awareness, identify opportunities, and facilitate rapid decisionmaking.

Intelligence support during execution focuses on providing the commander with practical knowledge that gives an exploitable advantage over the enemy. Although eliminating uncertainty during execution is impossible, focused intelligence operations can reduce uncertainty by providing situational awareness and identifying opportunities as they present themselves in the battlespace. Intelligence provides I&W of new or unexpected enemy activities, enhances efforts to engage the enemy through support to targeting, assists in protecting the force through CI measures and operations, and supports the planning of future operations by providing timely and accurate BDA. Three key factors for ensuring effective intelligence support during execution are resource allocation, linkage to operations, and generation of tempo.

Resource Allocation

Since IRs will always exceed available intelligence resources, intelligence operations must focus where they can have the greatest effect. A detailed and well-thought-out concept of intelligence support, developed in accordance with the commander's intent and concept of operations, will provide an appropriate allocation of intelligence capabilities between the main effort and supporting efforts. It is particularly important that Marine Corps forces (MARFOR), MAGTF, and major subordinate commands (MSCs) who control the tasking of intelligence units and capabilities provide access to critical intelligence resources for their subordinate elements. Those intelligence resources best suited to satisfying current, tactical, mission-specific IRs, such as unmanned aerial vehicles (UAVs) or terrain analysts, should be allocated to units responsible for executing the mission.

Linkage to Operations

To provide effective support to execution, intelligence operations must be linked to planned and ongoing operational activity. Intelligence operations are conducted based on the results of the IPB process, wargaming, and the planning process. Collection, production, and dissemination plans are developed to support execution of specific tactical options, engagement of targets, and selecting branches and sequels to the operation plan. Intelligence personnel must have continuous awareness of planned and ongoing operations to monitor potential enemy reactions, identify new opportunities, and assess the effects of actions on the enemy. Close and continuous synchronization of intelligence activities and operations is essential to developing timely, tailored, and relevant intelligence that facilitates rapid decisionmaking and exploitating opportunities in the battlespace.

Generation of Tempo

Intelligence operations during execution must facilitate the generation of tempo. First, intelligence operations generate tempo through prioritization. By focusing intelligence operations on satisfying PIRs and supporting the main effort, intelligence is developed that is directly linked to the commander's intent and C2 effort. Next, intelligence facilitates tempo by supporting the decisionmaking process. Intelligence that provides situational awareness and the ability to recognize emerging patterns enables the commander to employ intuitive decisionmaking to make rapid

decisions that help generate tempo. Finally, intelligence facilitates tempo by providing knowledge—key elements of data and information that have been analyzed, synthesized, and placed in context to help provide situational awareness—not just a mass of unprocessed information or unrelated pieces of data. The critical factor is not the amount of information provided, but key, focused intelligence that is available when needed and in a useful form that improves the commander's knowledge of the hostile situation and his ability to act. Intelligence operations must have the flexibility, agility, and responsiveness to rapidly collect and process relevant information, develop a focused product, and deliver that product to the affected commander in an easily understandable form and in time for the commander to take appropriate action.

CHAPTER 3
DEVELOPING INTELLIGENCE

Intelligence is developed through the use of the intelligence cycle. This process consists of a sequence of related activities that translate requirements for various types of information into intelligence that is furnished to the commander for use in the decisionmaking cycle. During this sequence, intelligence needs are identified; a *plan* is formulated and *directions* are given for satisfying those needs, data is *collected, processed, and exploited* for usable information that is then transformed into a tailored, useful intelligence product that is *disseminated* to and *utilized* by the appropriate commander or unit. This process is called the intelligence cycle. At the same time, a parallel process is used to develop CI plans and measures that deny information to an adversary to protect our forces and help ensure the effectiveness of our operations.

Figure 3-1 shows the six steps of the Marine Corps intelligence cycle. These steps define a sequential and interdependent process for the development of intelligence. Intelligence operations are conducted within the framework of the intelligence cycle; the entire cycle or a specific step within the cycle may be the focus of a particular intelligence activity. Moreover, *all* intelligence, regardless of the scope of the requirement or level of command, is developed by following these steps. (See figures 3-2 and 3-3, page 3-2.)

No single phase of the cycle is more important than the others. All of the phases are interdependent. Without proper direction, the other phases will not focus on the correct objectives. Without effective collection, there may be too much or too little information and what information there is may prove to be irrelevant. Without processing and production, there is a mass of random data instead of the knowledge needed for the planning and execution of operations. Intelligence is meaningless unless it reaches the right people in time to affect the decisionmaking process and in an understandable form.

An understanding of the process used to develop intelligence is critical to the execution of successful intelligence operations. All personnel involved in the *development* and *use* of intelligence must be aware of their role in the process. They must understand the relationship between the steps in the process to ensure that intelligence focuses on the mission and facilitates rapid decisionmaking in

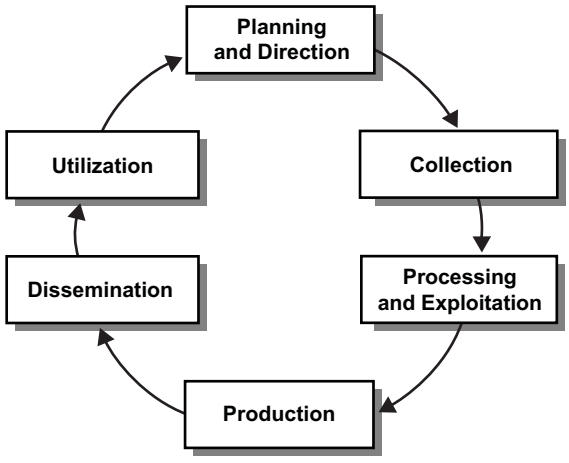


Figure 3-1. The Marine Corps Intelligence Cycle.

the execution of successful combat operations. (See figure 3-4.)

The Intelligence Cycle — Macro View

During a routine review of the situation in the Marine Expeditionary Force's (MEF's) area of interest, the G-2 notes that a recent change in government in one of the countries has created the potential for instability over the next year. The G-2 directs the development of an intelligence estimate to support potential contingency operations in this country. Working with the Marine Corps force G-2 section and the pertinent combatant command's joint intelligence center, the MEF collections section submits requests for imagery intelligence (IMINT), signals intelligence (SIGINT), and HUMINT support. As information is received, the MEF G-2 section's all-source fusion platoon (AFP), with the assistance of the topographic platoon, the imagery intelligence platoon (IIP), and the radio battalion, processes and exploits the information to produce the estimate and supporting studies. The estimate is completed within a month. The G-2 directs that copies be forwarded to all major subordinate commands (MSCs) and staff sections, with priority to the forward-deployed MEU. The G-2 also recommends to the commanding general that the scenario for the MEF's upcoming command post (CP) exercise be based on this estimate to introduce MEF personnel to this contingency area, identify planning requirements, and develop potential COAs. The MEF G-2 has *directed* the development of a comprehensive intelligence product that is focused on an operational requirement. Extensive organic capabilities as well as external resources were integrated to *collect* data, *process* it into information, and *produce* the finished intelligence. The product was then *disseminated* to and *utilized* by the units and staff sections with contingency responsibility for the identified area. The intelligence formulated focuses on the mission and facilitates rapid decisionmaking in the execution of successful combat operations.

Figure 3-2. The Intelligence Cycle—Macro View.

Intelligence Requirements

An intelligence requirement (IR) is a requirement for intelligence to fill a gap in the command's knowledge and understanding of the battlespace or enemy forces. (JP 1-02)

IRs *drive* the intelligence cycle. Properly articulated, mission-oriented requirements focus the intelligence effort and provide the foundation for successful intelligence operations.

The Intelligence Cycle—Micro View

The regiment S-2 section receives a report from one of their reconnaissance teams that an enemy artillery battery has just passed their observation post (OP) and turned off the road. Knowing that enemy artillery is the top targeting priority, the intelligence watch immediately begins developing the target. The S-2 chief checks the map and notes that there are three potential firing positions (identified through the IPB process) close to, but out of visual range of, the reconnaissance OP. The S-2 chief also knows that UAVs are in direct support of the regiment at this time. The S-2 chief alerts the fire support coordination center (FSCC) concerning the potential target and works with the FSCC and air officer to divert an ongoing UAV mission to search the potential firing positions. The UAV quickly locates the enemy artillery in the second firing position. The S-2 chief confirms that the enemy weapons can range friendly positions and, based on their observed activity, are preparing to attack. Using this intelligence, the FSCC coordinates a counterfire mission against the enemy artillery. The S-2 chief successfully executed the intelligence cycle in a matter of minutes. He understood the requirement to develop targeting information, directed the *collection* of information, *processed* the information and *produced* the desired intelligence, that is, a target, and *disseminated* that target to the FSCC, who *utilized* that intelligence to engage the target.

Figure 3-3. The Intelligence Cycle—Micro View.

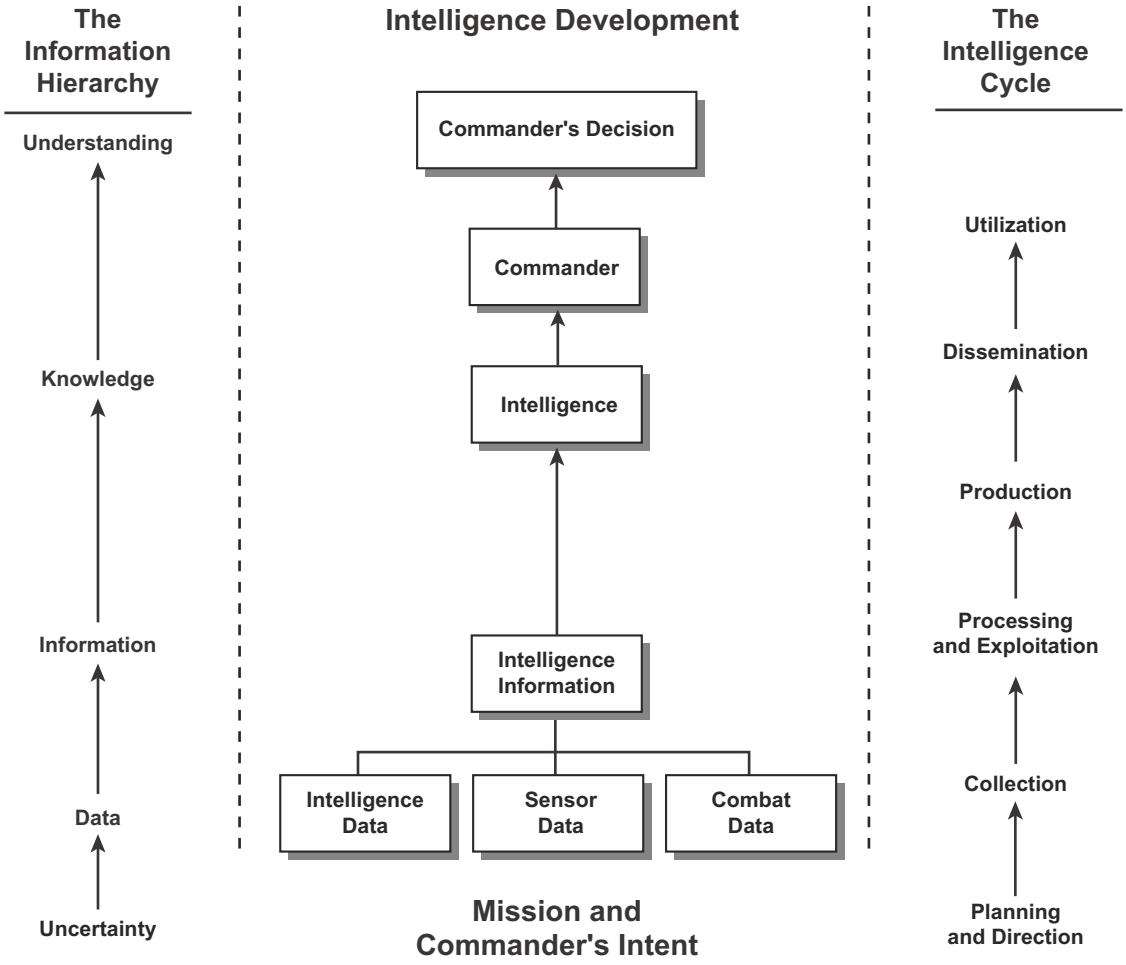


Figure 3-4. Intelligence Development and the Intelligence Cycle.

An IR is a missing piece of information about the enemy or environment that a commander needs to know to make a sound decision. In its simplest form, an IR is a question about the threat or the battlespace, the answer to which is required for the planning and execution of an operation. Examples follow:

- Will the highway bridge support assault amphibious vehicles?
- Will weather conditions interfere with planned air operations?
- Are port facilities and conditions suitable for a maritime prepositioning force pierside offload?
- Can the enemy air defense system threaten low-flying helicopters?
- What is the reaction time of the enemy garrison located south of the amphibious objective area?

Requirements fall into two categories: IRs and PIRs. PIRs and IRs replace the terms essential elements of information and IRs.

Priority Intelligence Requirement

A PIR is an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCDP 2)

IRs cover the entire spectrum of information that is needed concerning the battlespace and the threat. The scarce intelligence assets and limited time available will rarely permit the satisfaction of all of a command's IRs; thus, it is important to focus the intelligence effort on those requirements that are critical to mission success. These critical IRs are designated as PIRs. PIRs are the subset of the CCIRs that focus on the threat and the environment. CCIRs are intelligence and information requirements the satisfaction of which the commander deems critical to decisionmaking and mission success. PIRs are linked to specific decisions and, in effect, constitute the commander's guidance for intelligence. Notional PIRs follow:

- What size force is defending amphibious force objective B?
- Which bridges over the Sand River are intact?
- Will the enemy use chemical weapons against the beach support area on D-day?

There is no standard list or set rule for determining PIRs. Each tactical situation poses distinct problems and specific gaps in intelligence. However, the commander will often have PIRs that concern the most likely enemy COA, the most dangerous enemy COA, and critical enemy vulnerabilities that can be exploited.

Characteristics

PIRs and IRs have the following characteristics. Each PIR or IR—

- Asks only one question.
- Focuses on specific facts, events or activities concerning the enemy or the battlespace.
- Is tied to mission planning, decisionmaking, and execution.
- Provides a clear, concise statement of what intelligence is required.
- Contains geographic and time elements to limit the scope of the requirement.

Requirements may be simple or complex. It is important to understand that the nature and scope of PIRs and IRs will vary with the mission and the level of command, and on the particular phase in the PDE&A cycle. Requirements will generally become more focused as the intelligence cycle is executed. During execution, the intelligence effort should be directed against a small number of PIRs that are closely linked to the concept of operations.

Planning and Direction

The planning and direction phase of the intelligence cycle consists of those activities that identify pertinent IRs and provide the means for satisfying those requirements. (See figure 3-5.) Intelligence planning and direction is a continuous function and a command responsibility. The commander directs the intelligence effort. The intelligence officer manages this effort for the commander based on the intent, designation of PIRs, and specific guidance provided during the planning process.

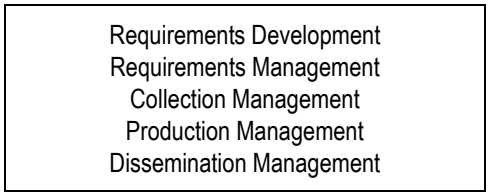


Figure 3-5. Planning and Direction Phase Functions.

Requirements Development

Identification of Requirements

Concise, mission-oriented IRs provide clear direction to the intelligence effort. The entire staff and all subordinate commanders play a role in developing the command's IRs. The intelligence officer formulates most of the initial requirements by using the original mission

tasking together with knowledge of the threat, familiarity with the operating area, and experience derived from participation in the commander's decisionmaking process to anticipate the majority of the basic intelligence needs. As the planning process continues, the commander, other staff officers, and subordinate commands expand on previously identified requirements and develop new ones. Requirements are generally linked to proposed COAs or potential decisions. The intelligence officer records, collates, and refines these requirements as they are identified and maintains a consolidated list of requirements.

Designation of PIRs

The commander makes a critical contribution to the intelligence effort by designating the PIRs. As COAs and supporting information requirements are developed, the satisfaction of certain IRs will be essential to mission success. The identification of these "show stoppers" forms the basis for designating PIRs. The intelligence officer, with input from other members of the staff, draws up a recommended list of PIRs. PIRs will be listed in priority order relative to their importance to mission accomplishment. In forming this list, the G-2/S-2 considers the requirements of his own command, subordinate commands, adjacent commands, and any direction received from higher headquarters. Recommendations are submitted to the commander who reviews, refines, and approves the command's PIRs. In designating PIRs, the commander establishes the following:

- What he wants to know (intelligence required).
- Why he wants it (linked to operational decisionmaking).
- When he needs it (latest time that the information will be of value).
- How he wants it (format, method of delivery).

Once approved and distributed, PIRs constitute the core of the commander's guidance for the intelligence process.

Requirements Management

Management of IRs is a dynamic process that encompasses the continuous evaluation of the following:

- Importance of each requirement to mission success.
- Information and assets needed to satisfy each requirement.
- Resources that are presently committed toward fulfilling that requirement.
- Degree that the requirement has been satisfied by completed intelligence activities.

Processing Requirements

Developing requirements and designating PIRs are not one-time efforts. There is a dynamic flow of new requirements, existing requirements are satisfied or no longer relevant, and the relative importance of each requirement changes as the PDE&A cycle progresses. (See figure 3-6.) As requirements are developed, the intelligence officer validates, refines, and enters them into the management system.

Validation ensures that the requirement is relevant to the mission, has not already been satisfied, and does not duplicate other requirements.

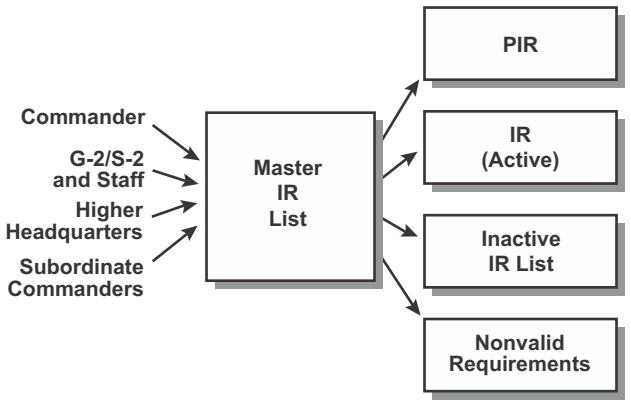


Figure 3-6. Intelligence Requirements Management.

Refining the requirement entails placing it in the proper format, identifying all information components related to the requirement, and adding appropriate qualifiers such as geographic limitations or time constraints. During refinement, similar or related requirements may be combined into a single, comprehensive requirement.

A requirements management system is an essential tool that provides a means to monitor the effort to satisfy each requirement. Each intelligence section must develop a system appropriate to its mission and echelon. Minimal components of any system are a numbering system, identification of who submitted the requirement, designation of collection and production resources committed to satisfying the requirement (or noting when it was submitted to higher headquarters or supporting forces, if organic assets are not available), timeliness requirements, dissemination instructions and information, and a mechanism to ensure user satisfaction.

Determining Priorities

The intelligence officer must continually reassess the emphasis given to each requirement and realign the priorities according to commander's intent and the current phase of the PDE&A cycle. The intelligence officer must also periodically confirm assignment of priorities with the commander to ensure that the intelligence effort is focused in accordance with the commander's desires.

Requirements Satisfaction

Once a requirement has been identified, validated, refined, and prioritized, the intelligence officer must determine how to satisfy the requirement and, if it can be satisfied by organic assets, allocate the appropriate intelligence assets to develop the desired intelligence. If the requirement cannot be satisfied by organic assets, it must be submitted to higher headquarters or supporting forces/agencies for satisfaction. In determining how to satisfy a requirement, the intelligence officer must consider each step in the intelligence cycle to ensure that the plan encompasses the entire process from collection through utilization. The intelligence officer must identify the information needed, where and how to get it, how to package the intelligence into an appropriate product, and how to deliver that product. Normally, an IR will generate a requirement to do the following:

- Collect data or information.
- Process and produce intelligence in the scope and form that answers the question.
- Disseminate the information to a particular user by a specific time. (See figure 3-7.)

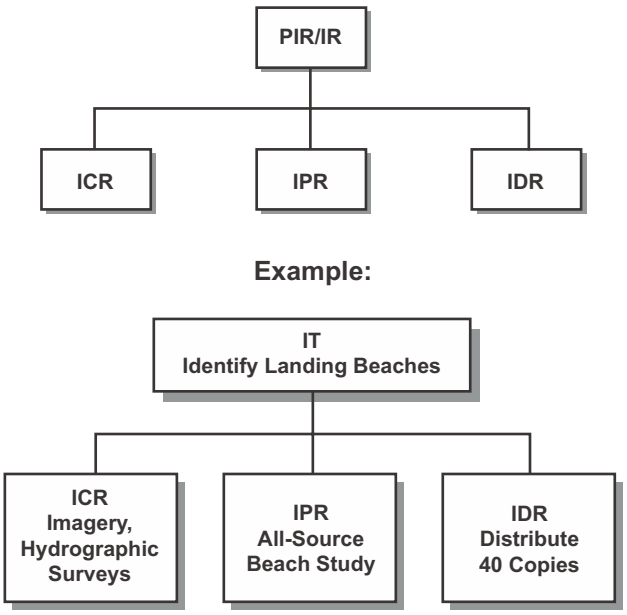


Figure 3-7. Requirements Satisfaction.

Directing the Intelligence Effort

Intelligence direction consists of the requirements development and management process described above combined with the associated functions of collection management, production management, and dissemination management. Because the possible questions about the enemy and the AO are practically infinite but intelligence assets are limited, the intelligence effort must be managed at each step in the process. Management of requirements, collection, production, and dissemination ensures that the effort is focused on the PIRs and delivers knowledge that facilitates sound tactical decisionmaking.

Collection Management

Collection management is the process of converting IRs into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. Its purpose is to conduct an effective effort to collect all necessary data while ensuring the efficient use of limited and valuable collection assets.

Production Management

Production management encompasses determining the scope, content, and format of each product; developing a plan and schedule for the development of each product; assigning priorities among the various intelligence production requirements; allocating processing, exploitation, and production resources; and integrating production efforts with collection and dissemination. As with collection management, the goal is to make effective and efficient use of limited resources and ensure that the production effort is properly focused on established priorities.

Dissemination Management

Dissemination management involves establishing dissemination priorities, selecting dissemination means, and monitoring the flow of intelligence throughout the command. Its objective is to deliver the required intelligence to the appropriate user in the proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded by attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls that do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods.

Planning the Intelligence Support System

This activity includes designing and establishing the structure that is necessary to provide intelligence support throughout the course of an operation. The intelligence officer looks at the entire body of IRs rather than at individual IRs or PIRs. The intelligence officer anticipates the continuing intelligence needs of the force as it carries out its mission and designs an intelligence support system that has the capability, flexibility, and redundancy to satisfy these needs. After the support system concept is developed, the resources needed to build the system are identified, requested, and acquired. Factors taken into consideration during this effort follow:

- Task organization of intelligence units.
- Identification of personnel and equipment requirements.
- Requirement for liaison teams.
- Connectivity with national, theater, joint, and multinational force intelligence assets.
- Communications and information systems (CIS) requirements.
- Logistic requirements.
- The need for specialized capabilities; e.g., linguists.

Collection

Collection is the gathering of intelligence data and information to satisfy the identified requirements. The collection phase encompasses assembling relevant information from sources that are already on hand or available from other intelligence organizations: intelligence databases, studies, maps, and a workbook or situation map. Collection consists of the activities of organic, attached, and supporting intelligence collection assets to gather new data and deliver it to the appropriate processing or production agency; i.e., the execution of collection operations. Functions carried out during the execution of collection operations follow:

- Mission planning.
- Positioning of assets to locations that are favorable to satisfying collection objectives.

- Data collection.
- Reporting.
- Supervision of individual collection missions.

Intelligence data and information are collected by a variety of intelligence assets, each with unique capabilities and limitations. (See figure 3-8.)

Figure 3-8. MAGTF Primary Organic Collection Assets.

The value of a collection source is not necessarily related to the sophistication or cost of that source, but rather to its ability to gather pertinent data from the collection target—the enemy or environmental consideration that is the subject of the particular intelligence collection requirement. Successful intelligence operations require access to data from all types of collection resources: organic, joint, national, and multinational. Collection operations are executed to gather data from all suitable and capable assets, balancing the capabilities of one type of collector against the limitations of another to provide "all-source" data input to the processing and exploitation and production phases. The primary types of intelligence data used to produce tactical intelligence are described in the following paragraphs.

Imagery Intelligence

Imagery intelligence is intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. (JP 1-02)

Principal sources of imagery are national overhead reconnaissance systems; manned aircraft such as the F-14 or F/A-18 with the Advanced Tactical Airborne Reconnaissance System, the U-2 or the Joint Surveillance Target Attack Radar System; and UAVs. IMINT provides concrete, detailed, and precise information on the location and physical characteristics of the environment and the threat. It is the primary source of information concerning key terrain features, installations, and infrastructure used to build detailed intelligence studies and target materials. The main limitation of IMINT is the time required to task, collect, process, and analyze the imagery. Detailed planning and coordination is required to ensure that the results of imagery collection missions are received in time to affect the decisionmaking process. Imagery operations can be hampered by weather, the enemy's air defense capability, and his camouflage, cover, and deception activities.

Signals Intelligence

SIGINT is intelligence information derived from the interception, processing, and analysis of foreign communications, noncommunications electronic emissions, and instrumentation signals. SIGINT is provided by the radio battalion; the Marine tactical electronic warfare squadron; and an integrated network of national, theater, and joint force SIGINT support agencies. SIGINT provides timely and accurate data on enemy forces that may include details on enemy composition, identification, and location. It can also give insight into the enemy's current status and activities and future intentions. SIGINT is one of the primary means for providing I&W of enemy actions. It is also a principal contributor to intelligence support to IO through its analysis and exploitation of the enemy's C2 system. Principal limitations of SIGINT are that the enemy must transmit signals that can be exploited and that

collection assets must be capable of intercepting and positioned to intercept those signals.

Human Intelligence

HUMINT is a category of intelligence derived from information collected and provided by human sources. (JP 1-02)

HUMINT operations cover a wide range of activities, including reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, and interrogations of enemy prisoners of war. Principal dedicated HUMINT resources are ground reconnaissance units; the CI and interrogator-translator assets of the MEF CI/HUMINT company; and national, theater, and other Service HUMINT elements. All Marines participating in an operation can obtain significant information about the threat and environment. Intelligence operations must aggressively employ Marines as HUMINT sources by teaching them the importance of observing and reporting.

HUMINT can provide insight into intangible factors such as tactics, training, morale, and combat effectiveness that cannot be collected by technical means and offers the best potential source to discern future plans and intentions. HUMINT is particularly important in MOOTW, in which the nature of the mission and of the threat generally provide a lucrative environment for HUMINT operations.

HUMINT has two main limitations as follows:

- HUMINT operations generally require placing humans at risk to gain access to their targets. For that reason, IRs should be satisfied through technical collection means, if possible, before considering the use of human resources.
- HUMINT responsiveness can be limited in certain circumstances because of the time it takes to plan the activities, position the assets, collect the data from what are often hostile or noncooperative sources, and report the information to exploitation and production centers, which are often located a significant distance from the collection site.

Measurement and Signature Intelligence

Measurement and signature intelligence (MASINT) is intelligence information gathered by technical instruments such as radars, passive electro-optical sensors, radiation detectors, and remote ground sensors. Although the primary tactical application of these devices is to collect sensor data, which is generally provided directly to operations centers for immediate decisionmaking, the data collected can also provide significant intelligence information on enemy movements and activities. Key MAGTF MASINT capabilities are remote ground sensors, weapons locating radars, and air surveillance radars. These sensors provide an efficient means to maintain surveillance over large portions of the battlespace. Their limitations include the logistic support required to maintain the equipment, the requirement to place the sensors in proximity to the surveillance area, and the exploitable electronic signatures associated with some of the sensors.

Open-Source Intelligence

Open-source intelligence (OSINT) is information of potential intelligence value that is available to the general public. (JP 1-02)

OSINT sources include books, magazines, newspapers, maps, commercial electronic networks and databases, and radio and television broadcasts. OSINT involves no information that is classified at its origin or acquired through controlled collection. National and theater intelligence production centers have access to a range of OSINT sources. MAGTF intelligence agencies can receive OSINT through these centers in addition to collecting information from open sources that are available in the AO. OSINT can be a valuable source of geographic, political, economic, sociological, and cultural information, particularly in security, humanitarian assistance or peace operations. In multinational operations, OSINT provides intelligence that can be readily shared with members of a multinational force. However, the sources of OSINT should be carefully evaluated to determine the accuracy and reliability of the information provided.

Counterintelligence

CI is the intelligence function concerned with identifying and counteracting the threat posed by foreign intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion or terrorism. The principal objective of CI is to assist with protecting DOD personnel, family members, resources, facilities, and critical infrastructure. CI provides critical intelligence support to command force protection efforts by helping identify potential threats, threat capabilities, and planned intentions to friendly operations while helping deceive the adversary as to friendly capabilities, vulnerabilities, and intentions. CI increases uncertainty for the enemy, thereby making a significant contribution to the success of friendly operations. CI also identifies friendly vulnerabilities, evaluates security measures, and assists with implementing appropriate security plans. The integration of other intelligence disciplines, CI, and operations culminates in a cohesive unit force protection program.

Processing and Exploitation

Processing and exploitation involves the conversion of collected data into information that is suitable for the production of intelligence. Processing is largely a technical function that does not add meaning to the data but that is necessary to convert the data into a form that people can understand. Examples of processing include developing a piece of film, translating a document or communications intercept from a foreign language or converting electronic data into a standardized report that can be analyzed by a system operator. Some types of data require minimal processing. They may be collected in a form that is already suitable for production. Processing may also take place automatically during collection. Other types of data require extensive processing, which can affect the timeliness and accuracy of the resulting information.

Data may be further exploited to gain the fullest possible advantage. For example, an aerial photograph or a frame of UAV video may be exploited by imagery interpreters to identify specific pieces of equipment or measure the dimensions of structures found on that image. When resources are required to accomplish the processing and exploitation phase, it is crucial that processing requirements be prioritized and managed according to the PIRs to ensure that critical information is extracted first.

Production

Production is the activity that converts information into intelligence. It involves the evaluation, interpretation, integration, analysis, and synthesis of all information that is relevant to a particular IR to answer the question that has been asked. Production fuses new information and existing intelligence from all sources to provide meaningful knowledge that can be applied to the decisionmaking process. During the production phase, information is—

- Evaluated to determine pertinence, reliability, and accuracy.
- Analyzed to isolate significant elements.
- Integrated with other relevant information and previously developed intelligence.
- Interpreted to form logical conclusions that bears on the situation and supports the commander's decisionmaking process.
- Applied to estimate possible outcomes.
- Placed into the product format that will be most useful to its eventual user.

Intelligence Preparation of the Battlespace

IPB is the primary analytical methodology used to produce intelligence in support of the decisionmaking process. It furnishes a framework for integrating intelligence and operations throughout the PDE&A cycle. IPB is a systematic, continuous, mission-focused process of analyzing the

environment and the threat in a specific geographic area. (See figure 3-9.)

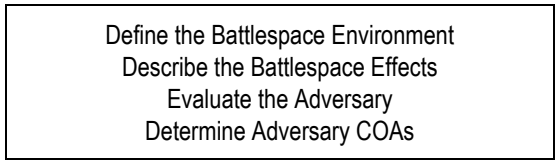


Figure 3-9. Intelligence Preparation of the Battlespace.

IPB provides a means to interpret information and understand the battlespace that can be applied in any operational situation. Through the IPB process, information that has been collected and processed is analyzed, synthesized, and used to estimate possible outcomes that can affect mission accomplishment. The result is knowledge-based intelligence that is incorporated into a variety of intelligence products.

Although IPB is fundamentally an intelligence process, successful application of the process to support planning and execution depends on the participation of the commander and the entire staff. The commander is responsible for intelligence production and IPB. The commander focuses the IPB effort by defining the area and key factors to be studied. The commander's guidance and the complete involvement of the staff are necessary to ensure that the IPB effort encompasses aspects of concern for all warfighting functions and provides detailed and accurate intelligence for COA development and detailed planning. Finally, the commander ensures that the IPB process is fully integrated with mission planning and execution. IPB is an effective tool only when the results are used to develop plans and support decisionmaking during execution.

IPB emphasizes providing intelligence in the form of graphics and images—formats that help the commander to rapidly visualize, assimilate, and apply the intelligence in the decisionmaking process. During planning, products generated from IPB place large volumes of intelligence in context, providing situational awareness for everyone involved in the planning effort. These products form the basis of, or are combined with, the planning tools and decision support aids prepared by other staff sections to provide an integrated planning and execution support product. During execution, the use of graphics display intelligence increases the commander's ability to discern patterns as they are emerging and to conduct intuitive decisionmaking, thereby increasing operational tempo.

Levels of Production

Intelligence production can be extremely simple or incredibly complex. At the MAGTF CE level, particularly during deliberate planning, production normally entails developing detailed, all-source estimates and studies through the combined efforts of several intelligence support elements. During tactical execution, time constraints and the demands of the ongoing battle require rapid processing and production, with an emphasis on developing simple, mission-focused intelligence products such as a hand-annotated image of a helicopter landing zone (HLZ), a target description or an overlay depicting current and future enemy dispositions. An enlisted intelligence specialist on duty in an infantry battalion command post may develop dozens of intelligence products during his watch in the form of answers to questions concerning the enemy situation, targets or terrain to be traversed. Valuable intelligence does not result solely from the investment of time or resources. It is developed by placing relevant information in context, converting it into knowledge through analysis and synthesis, and applying that knowledge to the decisionmaking process.

There is inherent friction between the desire to provide as complete and accurate an intelligence product as possible and the continuous requirement to support the time-sensitive urgency of tactical decisionmaking. In practice, these conflicting demands must be balanced by using

stated direction, such as the commander's intent and PIRs, and knowledge of the operational situation to determine when to finish and disseminate the product. To provide a framework to make these determinations, intelligence production can be viewed as occurring on two levels: deliberate and immediate.

Deliberate production is employed when there is sufficient time to thoroughly evaluate, analyze, and synthesize all available information and produce a formal intelligence product such as a written intelligence estimate, scheduled report or detailed target/objective area study.

Immediate production is conducted to identify, process, and place in context elements of data, information, and intelligence that have a direct effect on ongoing or near-term operations. These elements are subjected to a compressed version of the production process, and the resulting product is rapidly disseminated to those who are affected. Immediate production is normally conducted during execution and results in simple, mission-specific intelligence products: situational assessments or answers to specific, individual IRs. There is no absolute distinction between the two levels. The nature of the situation and pertinent IRs will dictate the amount of time available to complete each production effort. Likewise, IPB methodology should be used during both types of production. However, during immediate production, a rapid mental evaluation and integration of the relevant factors of the threat and environment are used, usually building on a deliberate production effort that has already been completed.

Dissemination

Dissemination is the timely conveyance of intelligence to users in an appropriate form. Many times, intelligence operations focus almost exclusively on the collection and production phases, with the intelligence cycle often breaking down because insufficient attention is given to the dissemination phase. Dissemination must be planned and supervised to the same degree as collection and production or we risk failure of the intelligence support function. Determining the form and selection of the means to deliver the product are key aspects of the dissemination process.

Form

Determining the form to be used in disseminating the intelligence product is a function of several factors: the purpose of the intelligence product, the urgency and relevance of the intelligence to ongoing operations, the type and volume of the intelligence, the user's capability to receive intelligence products, and the dissemination means available. Because decisionmaking is a mental process and human beings think and understand primarily in the form of images, the goal of intelligence dissemination is to convey an accurate image of the battlespace or threat to the decisionmaker in a form that facilitates rapid understanding of that image. For this reason, graphics are the preferred dissemination form. (See figure 3-10 and figure 3-11 on page 3-14.)

Although oral briefings and written reports are the primary dissemination forms used today, the use of automated systems is increasing the capability to develop graphic products. Imagery, overlays, diagrams, and schematics enhanced with appropriate textual data and annotations will be used as the baseline dissemination format whenever possible. However, in time-sensitive situations, the verbal report or short text message may be the most expeditious dissemination form. Whether oral, text or graphic, intelligence products should use standard formats whenever possible. Standard formats facilitate ease of preparation and dissemination, as well as usability of the intelligence product.

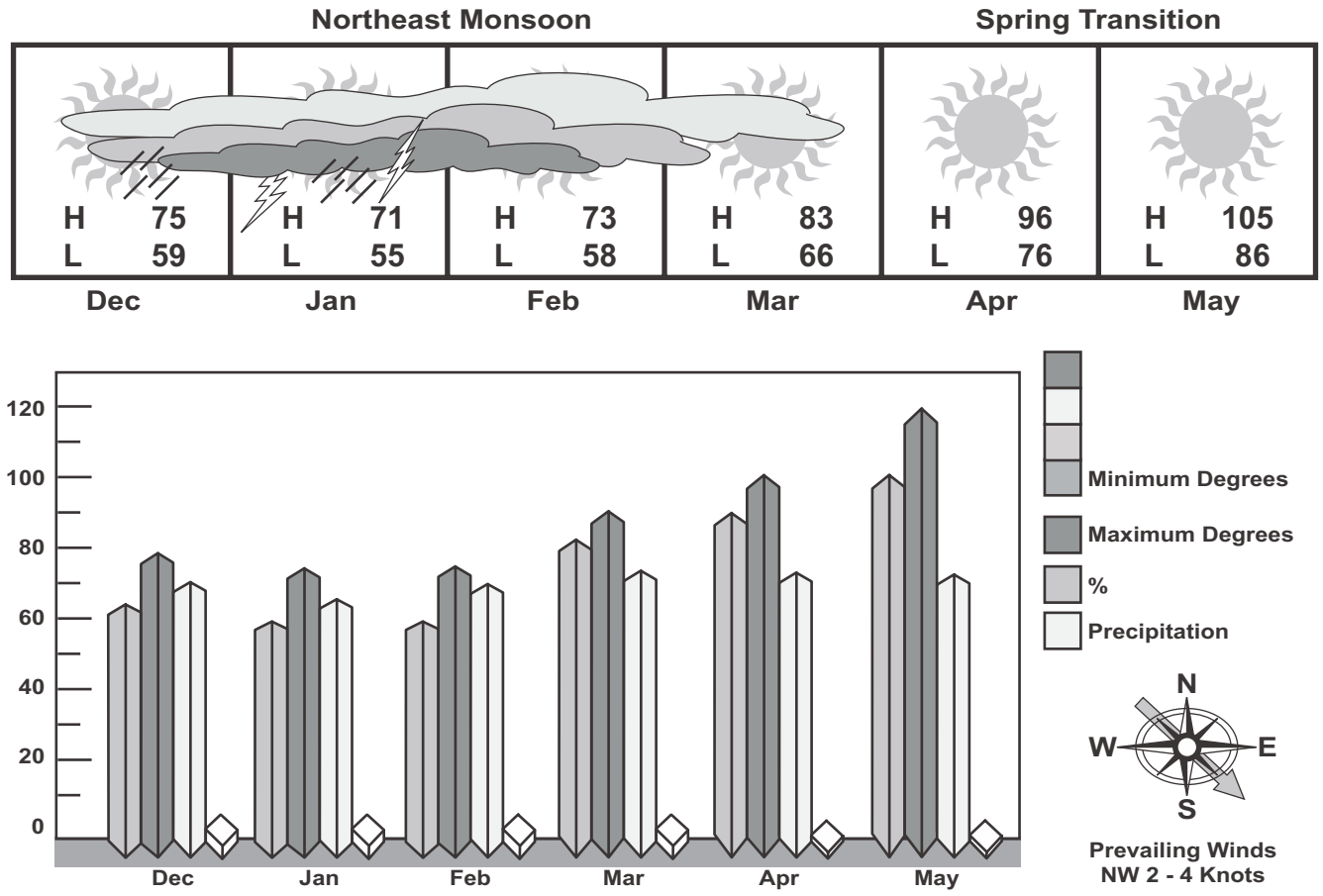


Figure 3-10. Graphic Climatology Study.

Delivery

Delivery of the intelligence product to the right person in a timely manner is directly related to the choice of the means used to disseminate that product. Dissemination is managed by using a combination of methods, channels, and modes to convey the product to the user.

Methods

There are two basic methods used to disseminate intelligence: supply-push and demand-pull. A supply-push system pushes intelligence from the collectors/producers to the users as it becomes available. The main advantage to this method is that users do not have to initiate requests to receive products. However, there is potential for information overload in a supply-push system. To prevent information overload, the dissemination node should tailor what it is passing through the system, not simply dump everything that it has received or developed.

The demand-pull mode provides access to intelligence on an as-needed basis. The user draws the required intelligence from the intelligence support system through a series of searches or inquiries. The use of demand-pull decreases the volume of intelligence being transmitted and diminishes the possibility of overwhelming units with superfluous products. However, demand-pull can also reduce the timeliness of dissemination by developing and providing intelligence only after a request has been received.

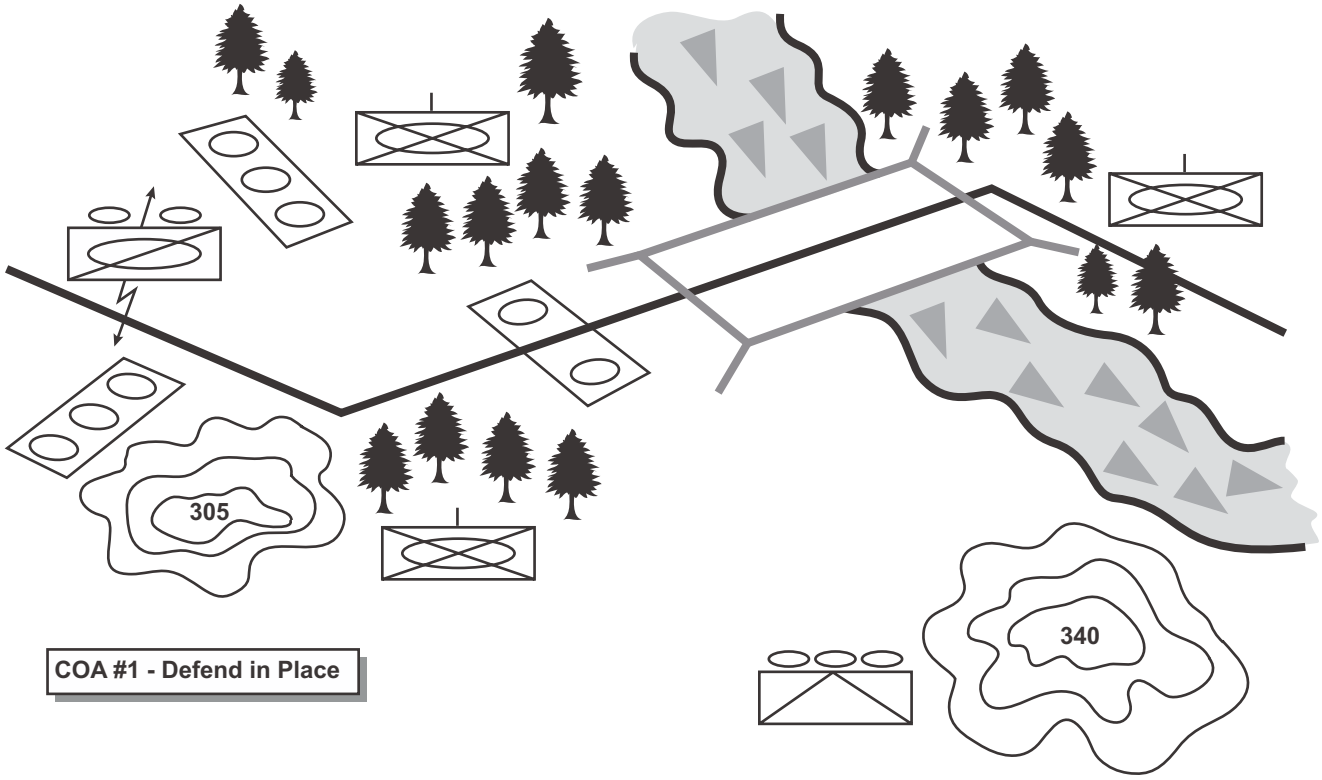


Figure 3-11. Graphic Intelligence Estimate.

The dissemination system must provide the flexibility to use either method, "pushing" important or time-sensitive intelligence directly to the users, while at the same time permitting them to "pull" other relevant intelligence as needed from readily accessible sources such as a database or a watch section at an intelligence center.

Channels

Intelligence is disseminated by using two types of channels: *standard* and *alarm*. Standard dissemination is used for routine intelligence and is transmitted according to a set order and format, usually along established command or staff channels. Examples include the formal staff briefing and standardized reports. The alarm channel is used to disseminate critical, time-sensitive intelligence that can have an immediate effect on the conduct of the operation, such as I&W of hostile activity. I&W alarms must be disseminated rapidly to all units that are affected by that intelligence. Although the standard channel is used to satisfy the majority of dissemination requirements, care must be taken to monitor the flow of what is passing through the pipeline to ensure that the intelligence provided is timely and pertinent to the units receiving it. A particularly important connection that is often neglected in standard dissemination is *lateral dissemination*; intelligence must flow laterally between units as well as up and down the chain of command. The exchange of intelligence between the GCE, aviation combat element (ACE), and combat service support element (CSSE) is an especially important link in ensuring that all commanders have a shared picture of the battlespace.

Modes

Finally, intelligence is disseminated in one of two modes: *broadcast* or *point-to-point*. In broadcast

dissemination, intelligence that affects the majority of units is sent simultaneously to a broad audience. Examples include I&W alarms, intelligence products developed by the MAGTF G-2 section that support the entire MAGTF, and reporting from organic collection assets. Broadcast dissemination may be web-based. Successful use of the broadcast mode depends on several factors, including judicious selection of what intelligence is broadcast, the ability of the appropriate users to monitor the broadcast, and employment of a processing methodology or system to filter and select for detailed examination only those broadcast items that are pertinent to the user's requirements. Undisciplined use of this mode can quickly lead to information overload. In the point-to-point mode, intelligence is sent to a specific user or users, normally in response to a specific request or requirement, and is passed along sequentially as appropriate. Dissemination across the system is slower but is more focused and can provide intelligence that is tailored to the needs of each individual unit. Point-to-point dissemination may be enhanced through the use of classified e-mail systems.

Architectures

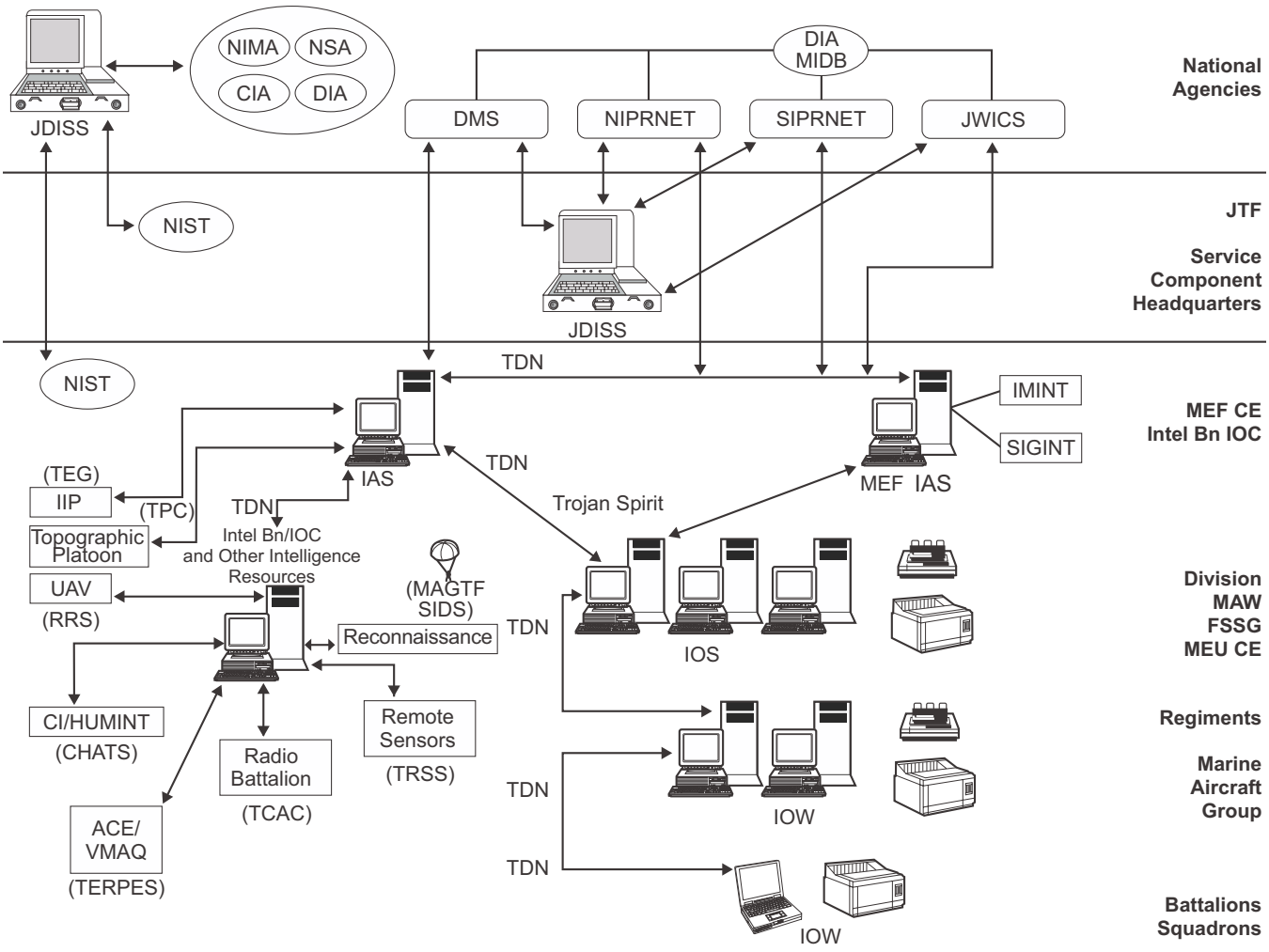
Intelligence architectures provide the means to disseminate intelligence. (See figure 3-12 on page 3-16.) Dissemination planning analyzes and anticipates the dissemination requirements and designs the appropriate architecture to meet those requirements. The architecture should employ all methods, channels, and modes in a flexible, integrated system. The objective is to provide the right intelligence to the appropriate user in a timely manner, while at the same time not overwhelming him with a massive amount of unfocused data.

Architectures will be developed with the objective of facilitating the exchange of *graphic* intelligence throughout the force, down to the lowest tactical echelon. The means will consist of a combination of procedures, CIS, and communications networks, effectively supervised by intelligence specialists to ensure that the dissemination requirements are being satisfied. The intelligence architecture must be interoperable with the overall CIS architecture employed by the MAGTF and the joint force.

Utilization

Intelligence has no inherent value. Its value is realized through its support to operations. Thus, the intelligence cycle is not complete until the intelligence that has been developed is used in decisionmaking during planning and/or execution. The commander is responsible for the effective use of intelligence and for ensuring that decisions are based on the foundation provided by intelligence. The intelligence officer facilitates the effective use of intelligence, supervises the entire intelligence development effort, and assists the commander and the staff in understanding the intelligence product and its application.

The utilization phase also provides the basis for the continuous functioning of the intelligence cycle. On one hand, utilization will determine whether a requirement has been completely satisfied; requirements that have not been met will require additional intelligence development efforts. On the other hand, the satisfaction of one requirement normally generates new or additional requirements, the answers to which are needed to further refine or focus the decisionmaking process. In either case, utilization provides guidance and feedback that are used to initiate the next iteration of the cycle.



CHATS=CI/HUMINT automated tool set	NIMA=National Imagery and Mapping Agency
CIA=Central Intelligence Agency	NIPRNET=Non-Secure Internet Protocol Router Network
CI/HUMINT=counterintelligence/human intelligence	NIST=National Intelligence Support Team
DIA=Defense Intelligence Agency	NSA=National Security Agency
DMS=Defense Message System	RRS=remote receive station
IAS=Intelligence analysis system	SIDS=secondary imagery dissemination system
IIP=imagery intelligence platoon	SIPRNET=Secret Internet Protocol Router Network
intel bn=intelligence battalion	TCAC=Technical Control and Analysis Center
IOS=intelligence operations server	TDN=tactical data network
IOW=intelligence operations workstation	TEG=Technical Exploitation Group
JWICS=Joint Worldwide Intelligence Communication System	TERPES=tactical electronic reconnaissance processing and evaluation system
MAW FSSG=Marine Aircraft Wing Force Serv ice Support Group (USMC)	TPC=topographic production capability
MIDB=modernized integrated database	TRSS=tactical remote sensor system

Figure 3-12. Notional Marine Expeditionary Force Intelligence Architecture.

Application of the Intelligence Cycle

The intelligence cycle is a procedural framework for developing mission-focused intelligence support. It is not an end in itself, nor should it be viewed as a rigid set of procedures that must be carried out in an identical manner on all occasions. The commander and the intelligence officer must consider each IR individually and apply the intelligence cycle in a manner that develops the required intelligence in the most effective way.

Application of the intelligence cycle will vary with the phase of the PDE&A cycle. In theory, a unique iteration of the intelligence cycle is carried out for each individual requirement. In practice, particularly during the planning phase, requirements are grouped together and satisfied through a single, concurrent intelligence development process. During the planning phase, intelligence development is generally carried out through two major iterations of the intelligence cycle.

The first primarily supports decision planning. Completing this iteration of the intelligence cycle results in preparing and using basic intelligence products—an intelligence estimate, supporting studies, and IPB analysis—that describe the battlespace and threat. These products form the basis for developing and selecting COAs.

The second iteration of the intelligence cycle supports execution planning. Decision and execution planning are defined and discussed in MCDP 5. It is an outgrowth of selecting the COA and forming a concept of operations. Implementing the collection plan, refinement of IPB analysis, and generating mission-specific intelligence products are integrated with the concept of operations to support mission execution. During execution, requirements are satisfied on a more individualized basis. New requirements are usually generated in response to a specific operational need. Each requirement is unique and must be satisfied in a timely manner to facilitate rapid decisionmaking and generating or maintaining tempo. (See figure 3-13 on page 3-18.)

The intelligence cycle will also be applied differently depending on the mission and the organizational level of the unit. For example, a MAGTF G-2 section will normally have a separate section that is specifically responsible for each phase of the intelligence cycle—a collections section, processing and exploitation agencies, a production element, and a dissemination section—with an intelligence operations section providing planning and direction for the overall effort. At the MAGTF level, intelligence is normally developed to satisfy multiple requirements concurrently, with simultaneous collection, processing, production, and utilization efforts being carried out by the separate functional sections. In contrast, a battalion or squadron S-2 section must carry out the cycle with a limited number of resources. It will generally focus on a single requirement or a small number of closely related requirements, moving through each phase of the cycle sequentially until that requirement is satisfied.

Counterintelligence

CI is the function of intelligence that is concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion, or terrorism. The objective of CI is to enhance the security of the command by denying an adversary information that might be used to conduct effective operations against friendly forces and to protect the command by identifying and neutralizing espionage, sabotage, subversion, or terrorism efforts. (MCWP 2-14, *Counterintelligence*)

Responsibilities

CI, like all intelligence matters, is a command responsibility. In preparing for operations, all units must develop a CI plan and implement appropriate

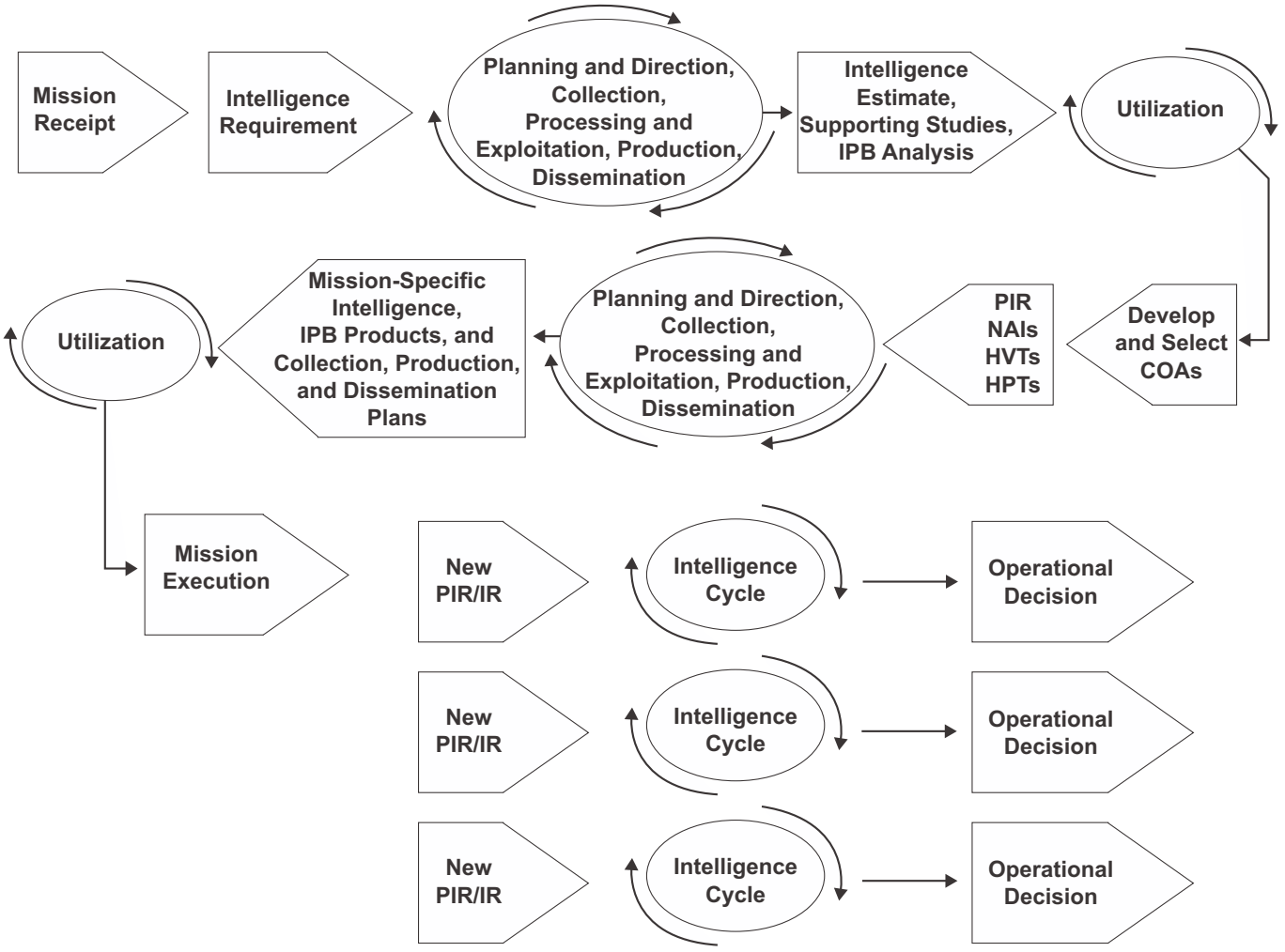


Figure 3-13. Application of the Intelligence Cycle.

CI measures to protect themselves from potential threats. The unit intelligence officer plans, implements, and supervises the CI effort for the commander. The G-2/S-2 may have access to or request support from MAGTF CI units and specialists to assist in developing CI estimates and plans. All members of the command are involved in executing the CI plan and implementing appropriate CI measures. Key participants in this process and their specific responsibilities follow:

- G-3/S-3-overall security and force protection, OPSEC, counterreconnaissance, and deception.
- G-6/S-6-CIS security.
- G-1/S-1-information security.
- Headquarters commandant-physical security of unit CP and echelons.

CI Planning

CI planning at all levels is conducted by using a standard methodology that consists of three steps: developing a CI estimate, conducting a CI survey, and developing the CI plan.

The CI Estimate

The CI estimate details the capabilities and limitations of foreign intelligence, subversive, and terrorist organizations that could carry out actions

against friendly units and facilities or against individuals, groups or locations of concern to our forces, such as the local population or civilian organizations operating in the area. It also provides an estimate of possible and probable COAs that these threat organizations will adopt. Intelligence and CI analysts of the MAGTF CE and CI/HUMINT company will normally prepare a comprehensive CI estimate that addresses threats to the MARFOR or MAGTF by using an IPB methodology that is focused on CI factors and the CI threat. However, each level of command must conduct its own evaluation to determine which of the adversary's capabilities identified in the MAGTF CI estimate represent a threat to their particular unit. The CI estimate must be updated on a regular basis. The revised estimate or appropriate CI warning reports must be disseminated to all units involved in the operation.

The CI Survey

The CI survey assesses a unit's security posture against the threats detailed in the CI estimate. The CI survey should identify vulnerabilities to specific foreign intelligence, espionage, sabotage, subversion or terrorist capabilities and provide recommendations on how to eliminate or minimize these vulnerabilities. The survey should be as detailed as possible. During the planning phase of an operation, it may be possible to do a formal, written survey. CI specialists from the CI/HUMINT company may be available to assist in this effort. In a time-compressed situation, the survey will likely result from a brief discussion between the appropriate intelligence, operations, communications, and security personnel. In either case, it is critical that the survey look forward in space and time to support developing the CI measures necessary to protect the unit as it carries out successive phases of the operation; i.e., the survey makes recommendations to improve the CI posture of the command for now and in the future.

The CI Plan

The CI plan details the activities and operations that the command will use to counter the CI threat. It includes procedures for detecting and monitoring the activities of foreign intelligence and terrorist organizations and directs the implementation of active and passive measures that are intended to protect the force from these activities. The CI plan is based on the threats identified in the CI estimate and the vulnerabilities detected by the CI survey. The MAGTF staff CI officer normally prepares a detailed, comprehensive CI plan that addresses the entire MAGTF. Included in the MAGTF CI plan are details of the employment of dedicated CI capabilities and the conduct of specialized CI operations intended to detect and neutralize or eliminate specific CI threats. Plans of subordinate MAGTF elements closely follow the MAGTF plan, normally adding only security measures that apply to their specific units. As with all plans, CI plans must be continually updated to ensure they are current and support ongoing and future operations.

CI Measures

CI measures encompass a broad range of activities designed to protect against the CI threat. The two general categories of CI measures are active and passive.

Active CI measures are those measures that are designed to neutralize or eliminate the foreign intelligence effort and adversary sabotage, subversion, and terrorism capabilities. Counterreconnaissance operations and deception activities are examples of active measures that are routinely employed by all units. Complex active CI measures such as counterespionage operations, counterterrorism operations, screening and interrogations, and CI force protection source operations are conducted only by CI personnel or other specialized organizations following the direction of the joint force and/or MAGTF commanders.

Passive CI measures are designed to conceal and deny information to foreign intelligence personnel and protect friendly personnel and installations from sabotage, subversion, and terrorism. Camouflage, security of classified material, emission control, information systems security, noise and light discipline, and physical access control are examples of passive CI measures that are employed extensively by all units.

The CI process is summarized in figure 3-14. For further details on CI responsibilities, planning, measures, and operations, see MCWP 2-14.

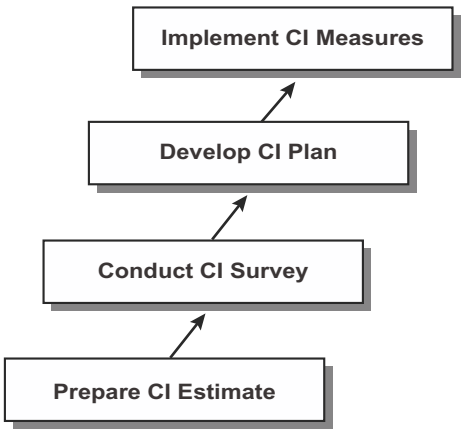


Figure 3-14. The Counterintelligence Process.

CHAPTER 4
CONCEPT OF MAGTF INTELLIGENCE SUPPORT

Marine intelligence operations are conducted primarily to facilitate the planning and execution of MAGTF operations through the development of tactical intelligence. The concept of MAGTF intelligence support ensures that the required intelligence is available to commanders at all levels throughout the force in time to influence their decisionmaking process. Key elements of this concept follow:

- Fully manned and capable organic intelligence sections down to maneuver battalion/squadron level.
- Directing the intelligence effort and maintenance of a robust collection, production, and dissemination capability at the MAGTF level.
- Employing specialized intelligence units to provide dedicated collection, processing, exploitation, and production of all-source intelligence.
- Creating key intelligence nodes at any level to concentrate intelligence support at critical times and locations. (These nodes are created through task organization, split-basing, and the use of intelligence direct support teams [DSTs].) An intelligence DST provides an enhanced intelligence capability to a supported intelligence section. A DST consists of one officer and several enlisted intelligence specialists. DSTs are organic to the MEF and each MSC G-2 sections.
- Full use of the intelligence support available from national, theater, joint, other Service component, and multinational forces to enhance MAGTF intelligence capabilities.
- Augmentation from global sourcing (noncommitted operating forces, the supporting establishment, and the Reserves) to enhance intelligence support to the MAGTF.

This intelligence support concept provides organic intelligence sections to commanders at all levels. These sections develop intelligence to satisfy their units' unique requirements. This intelligence supports their commander's tactical decisionmaking process and generates tailored intelligence products to facilitate mission execution.

Unit intelligence sections are supported by a primary MAGTF intelligence node that can perform all types of intelligence operations. The MAGTF G-2, through its combat intelligence center (CIC), provides centralized direction for the collection, production, and dissemination efforts of organic and supporting intelligence assets and ensures that these efforts remain focused on satisfying the PIRs that are essential to mission success. At the MEF CE level, the intelligence operations center (IOC) is the primary MAGTF intelligence node. Concentration of specialized intelligence capabilities in the radio battalion, the intelligence battalion, and the force reconnaissance company under this centralized direction facilitates unity of effort, effective employment of limited assets, and the collection and production of all-source intelligence.

The concept of intelligence support acknowledges the need to focus intelligence efforts in support of particular MAGTF elements during different phases of an operation. The MAGTF intelligence structure has the flexibility to provide such focused support through task organization. Enhanced support can be provided employing DSTs and integrating MAGTF intelligence assets.

Recognizing that organic intelligence capabilities may be limited in particular environments, the MAGTF can draw on the full range of national, theater, joint, other Service, allied, and multinational intelligence assets. When available, these capabilities will be fully integrated into MAGTF intelligence operations. If a separate Marine component

headquarters is established, it will support the MAGTF by performing those intelligence functions not directly related to warfighting, to include the following:

- Conducting detailed operational-level intelligence planning.
- Providing Marine intelligence liaison to joint task force (JTF) and other component intelligence elements.
- Monitoring the status of MAGTF intelligence collection and production requests for supporting and external support requirements.
- Planning the development and monitoring the adequacy of the JTF/MAGTF's intelligence architectures and the flow of intelligence to the MAGTF.
- Supporting Marine participation in intelligence support to the joint targeting process.

If a separate Marine component headquarters is not established, then the MAGTF CE's CIC will perform these functions. MSCs and other MAGTF elements will be able to access these external capabilities through the MAGTF intelligence architecture to pull available intelligence products on demand. Specialized intelligence units; e.g., the radio battalion or intelligence battalion, will have connectivity with appropriate external agencies to coordinate tasking or support.

Any MAGTF that is committed to an operation can be supported by intelligence assets of nondeployed MAGTFs, the supporting establishment or the Reserves. This support could consist of augmentation to fill shortfalls in manpower, equipment or specialized capabilities and assistance in developing intelligence in response to a Service-unique requirement. Flexibility to draw on assets from across the Marine Corps provides the ability to tailor and enhance particular intelligence capabilities based on the requirements of the committed MAGTF commander.

Role of the Organic Intelligence Section

Most commands from the battalion/squadron level and above in the operating forces have an organic intelligence section. The unit intelligence officer and section occupy the central role in the concept of MAGTF intelligence support. They focus the intelligence effort to develop, disseminate, and ensure effective use of intelligence in support of tactical operations. Intelligence drives operations and remains responsive to mission requirements through close and direct contact with the commander, key staff officers, and subordinate unit leaders.

The Unit Intelligence Officer

The commander directs the intelligence effort. The intelligence officer manages this effort for the commander, acting as the principal advisor on intelligence and implementing activities that carry out the commander's intelligence responsibilities. *The intelligence officer is a full participant in the commander's decisionmaking process, ensuring that intelligence is effectively used throughout the command during all phases of mission planning and execution*. Key responsibilities follow:

- Facilitate understanding and use of intelligence in the planning and execution of operations.
- Support situation development and the commander's estimate of the situation by identifying enemy capabilities, strengths, and critical vulnerabilities and opportunities and limitations presented by the environment.
- Assist the commander in developing PIRs.
- Ensure that the command's IRs are received, understood, and acted on by organic and supporting intelligence assets.
- Develop and disseminate all-source intelligence products that are tailored to the unit's mission and concept of operations.

- Monitor the effective flow of intelligence throughout the command.
- Provide BDA data and analysis to assist the combat assessment process.

The Unit Intelligence Section

The unit intelligence section supports the commander, the intelligence officer, and the entire command through the production and dissemination of mission-oriented intelligence products. Primary functions follow:

- Conduct IPB analysis for the unit's AO and interest.
- Develop and maintain a comprehensive intelligence estimate.
- Tailor intelligence produced at all levels to meet specific unit requirements.
- Form collection plans and support requests to satisfy unit PIRs and IRs.
- Maintain an accurate image of the battlespace and enemy situation.
- Prepare target analysis and target intelligence products.
- Recommend CI and force protection measures.
- Provide linkage to supporting intelligence assets.

Each organic intelligence section performs all six intelligence functions described in chapter 1. However, the priority and level of effort applied to the different functions will vary with the type of unit, level of command, and assigned mission. For example, an infantry battalion S-2 section will normally focus on support of the commander's estimate and situation development, while the S-2 of a combat service support (CSS) unit may concentrate on support of force protection, and the intelligence section of a fixed-wing Marine aircraft group usually places priority on support of targeting and combat assessment (particularly BDA).

Required Capabilities

To carry out these responsibilities, organic intelligence sections must have the following capabilities:

- Sufficient manning to carry out assigned responsibilities.
- Training in all aspects of tactical intelligence development, emphasizing the production of tailored, all-source, mission-specific intelligence products.
- Organic collection, processing, production, and dissemination assets appropriate to its mission and level of command.
- Connectivity to other MAGTF intelligence assets to provide a common picture of the battlespace, receive warning and other critical intelligence, and achieve access for "pulling" pertinent intelligence in response to unit requirements.
- Formation as a base for developing a larger intelligence support node, task-organized to provide expanded intelligence capabilities during particular phases of an operation.

The MAGTF Intelligence Section

The MAGTF intelligence section resident in the MAGTF CE is the focal point for intelligence operations and development in the MAGTF.

MAGTF Intelligence Officer

The MAGTF G-2/S-2, supported by the CIC and its subordinate sections, provides centralized direction for the MAGTF's comprehensive intelligence effort. The G-2/S-2 serves as the intelligence officer for the MAGTF commander. The CIC serves as the primary intelligence node for the entire MAGTF. As such, the CIC must remain responsive to the requirements of all MAGTF elements. The MAGTF intelligence section performs the following tasks:

- Provides centralized direction for MAGTF intelligence operations.

- Plans and implements a concept for intelligence support based on the mission, concept of operations, and commander's intent.
- Consolidates, validates, and prioritizes IRs of the MAGTF.
- Recommends MAGTF PIRs to the MAGTF commander.
- Maintains a consolidated, all-source production center in the MAGTF all-source fusion center (AFC).
- Plans, develops, and directs the MAGTF collection, production, and dissemination plans and operations.
- Directs the employment of MAGTF organic collection assets through the surveillance and reconnaissance cell (SARC) and the operations control and analysis center (OCAC).
- Submits consolidated requests for external intelligence support through the Marine component headquarters to appropriate agencies.
- Links the MAGTF to national, theater, joint, other Service, and multinational intelligence assets and operations.
- Prepares a comprehensive CI plan with recommended force protection measures.
- Supervises the execution of appropriate active and passive CI measures, CI functions, and CI services.

In addition to the responsibilities of all MAGTF intelligence officers, the MEF assistant chief of staff (AC/S) G-2 exercises staff cognizance over several special staff officers and their intelligence units/organizations. (See figure 4-1.)

The AC/S G-2 has staff responsibility for intelligence and intelligence operations. The commander relies on the intelligence officer to provide information on weather, terrain, and enemy capabilities, status, and intentions. Through the intelligence OPLAN and supporting intelligence, CI, and reconnaissance and surveillance (R&S) plans, the G-2 validates and plans information requirements; coordinates intelligence priorities, integrates collection, production, and dissemination activities; allocates resources; assigns specific intelligence and reconnaissance missions to subordinate elements; and supervises the overall intelligence, CI, and reconnaissance efforts. Specific responsibilities follow:

- Develop and answer outstanding MEF and subordinate units' priority information requirements and information requirements by planning, directing, integrating, and supervising organic multidiscipline MEF and supporting intelligence operations.
- Prepare appropriate intelligence, CI, and reconnaissance plans and orders for the MEF and review and coordinate the all-source intelligence CI and reconnaissance plans of JTFs, theaters, and other organizations.
- Submit and coordinate all-source collection, production, and dissemination requirements beyond the capability of the MEF to satisfy to higher headquarters for JTF, theater or national intelligence support.
- Ensure intelligence information is rapidly processed, analyzed, and incorporated where appropriate in all-source intelligence products, and rapidly disseminated to all MEF and external units requiring these.
- Evaluate JTF, theater, and national all-source intelligence support and adjusting stated IRs, if necessary.
- Identify and correct deficiencies in intelligence, CI, and reconnaissance personnel and equipment resources.
- Incorporate intelligence in training exercises to improve MEF individual, collective, and unit readiness.
- Facilitate understanding and use of intelligence in support of the planning and execution of MEF operations.

Special Staff Officers under the Staff Cognizance of G-2 Officer

G-2 Operations Officer

The G-2 operations officer has primary responsibility for intelligence support to the commanding officer and the remainder of the CE in support of

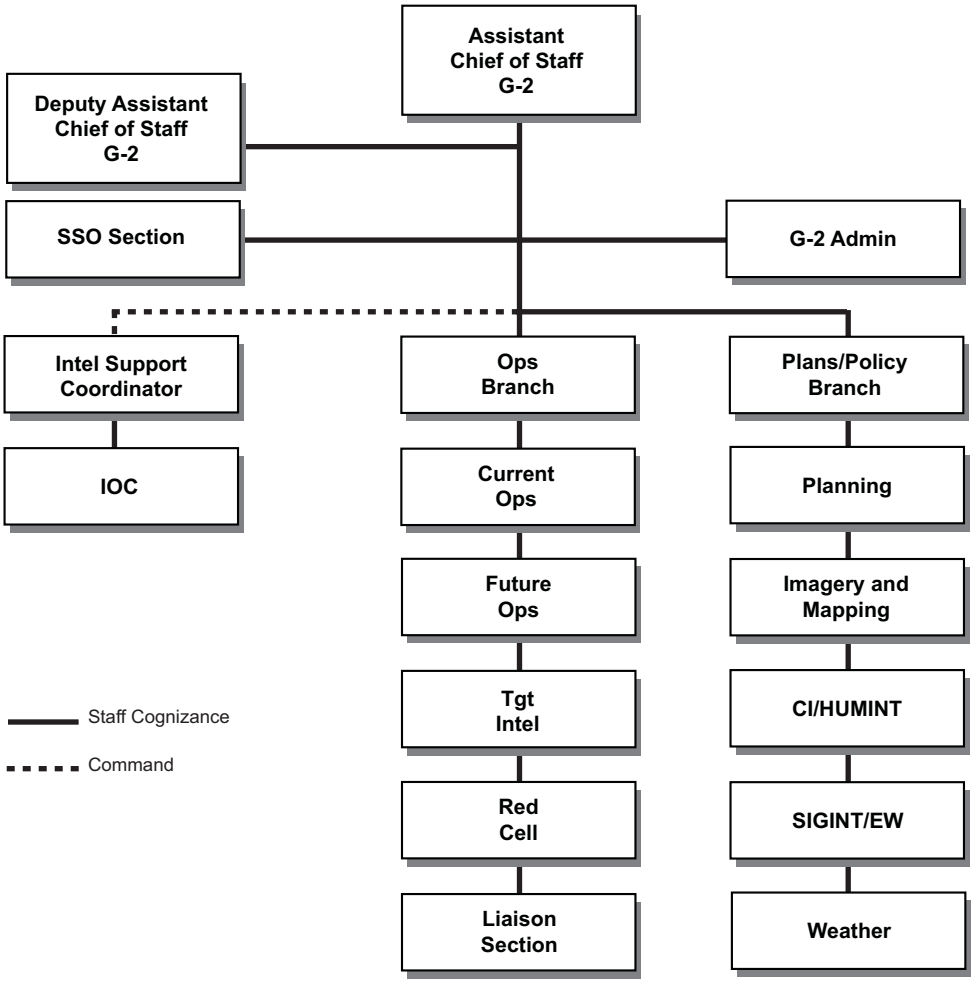


Figure 4-1. Special Staff Officers and Relationships under the Staff Cognizance of the MEF G-2.

current and future operations. Specific responsibilities include the following:

- Coordinate and provide intelligence support to the commander, the G-3 operations section, and the rest of the commander's battle staff.
- Serve as the G-2 representative to the MEF CE crisis action team.
- Coordinate, provide, and supervise intelligence support to the MEF CE current operations center, future operations center, and force fires.
- Plan, direct, and supervise the Red Cell.
- Provide recommendations on PIR and IR validation, prioritization, and taskings to the AC/S G-2 and the intelligence support coordinator (ISC). The intelligence battalion commander is dual-hatted as the ISC.
- Coordinate and supervise the transition of intelligence planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations, to effectively support the MEF's "single battle" transition process.
- Plan, direct, and supervise MEF liaison teams to external commands; e.g., the JTF and joint

functional components headquarters, and intelligence organizations.
- Coordinate with the ISC and MEF MSCs' G-2 operations officers to ensure unity of effort of MEF intelligence operations.
- Provide intelligence input and other support to MEF warning and fragmentary orders and to operations related reporting; e.g., periodic situation reports.
- Coordinate intelligence training for the MEF G-2 section and providing G-2 oversight for and integration of the entire MEF intelligence training program.
- Perform other intelligence support and tasks as directed by the AC/S G-2.

G-2 Plans Officer

The G-2 plans officer has primary responsibility for intelligence support to the future plans cell. Specific responsibilities follow:
- Plan the MEF concept of intelligence operations for approval by the AC/S G-2 and subsequent implementation by the integrated staff cell based upon the mission, threat, commander's intent, guidance, and concept of operations.
- Lead, coordinate, and provide intelligence support to MEF G-5 future plans section.
- Plan and coordinate intelligence support requirements for and the deployment of intelligence elements and resources into the AO.
- Provide recommendations on PIR and IR validation, prioritization, and taskings to the AC/S G-2 and the ISC.
- Coordinate, in conjunction with the ISC, G-2 development of Annex B (Intelligence) and Annex M (Geospatial Information and Services) to MEF OPLANs.
- Keep the G-2 section, other CE staff sections, intelligence liaison personnel, augmentees, and others apprised of MEF intelligence planning actions and requirements.
- Identify requirements and provide recommendations to the G-2 operations officer for MEF intelligence liaison teams to external commands; e.g., the JTF or other components' headquarters and intelligence agencies.
- Coordinate and develop policies for MEF intelligence, CI, and reconnaissance operations.
- Plan, direct, and supervise the MEF G-2's imagery and mapping, CI/HUMINT, SIGINT, and weather sections.
- Perform other intelligence support and tasks as directed by the AC/S G-2.

Intelligence Battalion Commander/ Intelligence Support Coordinator

The intelligence battalion commander is responsible for planning, directing, collecting, processing, producing and disseminating intelligence, and providing CI support to the MEF, MEF MSCs, subordinate MAGTFs, and other commands as directed.

Garrison. In garrison the principal task of the intelligence battalion commander is to organize, train, and equip detachments that support MAGTFs or other designated commands to execute integrated collection, intelligence analysis, production, and dissemination of intelligence products.

During Operations. During operations the intelligence battalion commander is dual-hatted as the ISC, serving as such under the direct staff cognizance of the MEF AC/S G-2. The intelligence battalion's S-3 section, along with the operations center element of the MEF G-2, form the core of the ISC support effort, with planning, direction, and C2 conducted within the IOC's support cell. As the ISC, he is responsible to the MEF AC/S G-2 for the overall planning and execution of MEF all-source intelligence operations. Specific responsibilities of the ISC during actual operations follow:
- Implement the concept of intelligence operations developed by the G-2 plans officer and approved by the AC/S G-2.
- Establish and supervise operation of the MEF IOC, which includes the support cell, the

SARC, and the production and analysis (P&A) cell. Generally the IOC will be collocated with the MEF CE's main CP.

- Develop, consolidate, validate, and prioritize recommended PIRs and IRs to support MAGTF planning and operations. The ISC is tasked to perform PIR and IR validation and prioritization *only* during operations when the IOC is activated. During routine peacetime operations, the PIR/IR validation and prioritization tasks are the responsibility of the MEF CE's G-2 operations officer.
- Plan, develop, integrate, and coordinate MEF intelligence collection, production, and dissemination plans, to include the effective organic and external integration and employment and staff cognizance of MEF SIGINT, CI, HUMINT, geographic intelligence, IMINT, ground remote sensors, ground reconnaissance, and tactical air reconnaissance intelligence collections, production, and dissemination operations.
- Develop, in conjunction with the G-2 plans officer and G-2 operations officer, and complete Annex B (Intelligence) and Annex M (Geospatial Information and Services) to MEF operation orders (OPORDs).
- Plan, develop, integrate, and coordinate intelligence and CI support to the commander's estimate, situation development, I&W, force protection, targeting, and combat assessment.
- Manage and fuse the threat (or *red*) common operational picture (COP)/common tactical picture (CTP) inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.
- Provide intelligence support to the MEF CE G-2 section and the MSCs.
- Prepare the intelligence and CI estimates to support G-2 plans.
- Plan, develop, and coordinate intelligence CIS architecture, to include its integration with and support of MEF IMINT and other intelligence and reconnaissance requirements.
- Coordinate and integrate all-source intelligence operations with other Service components, JTF joint intelligence support element (JISE), theater joint intelligence center (JIC) or joint analysis center, and national intelligence agencies and operations to include all aspects of intelligence reach back support.
- Assist with the evaluation and improvement of MEF all-source intelligence, CI, and reconnaissance operations.
- Perform other intelligence support and tasks as directed by the AC/S G-2.

Figure 4-2 is a summary of the principal responsibilities of the AC/S G-2's three principal subordinate staff officers.

Intelligence Support Coordinator

- Plan and execute intelligence operations to support all MEF IRs.
- Establish and direct the IOC (P&A cell, SARC, and support cell).
- IR management (collection, production and dissemination) validation, prioritization, and tasking per AC/S G-2 direction.
- Intelligence operations command of intelligence battalion and staff cognizance over SIGINT, CI, HUMINT, MASINT, IMINT, and air/ground reconnaissance (or designated G-2 elements).

G-2 Operations Officer

- Intelligence support to MEF CE battlestaff and current operations center agencies.
- Coordination and support to higher and adjacent headquarters and agencies.
- Recommends IR validation, prioritization, and tasking to AC/S G-2.
- Establish and direct intelligence elements and support to the current operations center, future operations center, target intelligence section, force fires, Red Cell, and MEF intelligence liaison teams.

G-2 Plans Officer

- Intelligence support to the G-5 future planning team for future planning IRs.
- Recommend IR validation, prioritization, and tasking to AC/S G-2.
- Establish and direct the G-2 future planning intelligence element.
- G-2 section's imagery & mapping, CI/HUMINT, SIGINT, and weather sections (less that under the staff cognizance of the ISC).

Figure 4-2. AC/S G-2's Principal Subordinate Staff Officers and their Responsibilities.

Collection Management/Dissemination Officer. The collection management/dissemination officer (CMDO) is sourced from the intelligence battalion's S-3 section and is a key subordinate to the intelligence battalion commander/ISC during operations. The CMDO is

responsible for formulating detailed intelligence collection requirements and intelligence dissemination requirements and tasking and coordinating internal and external operations to satisfy these. The CMDO receives validated PIRs and IRs and direction from the ISC, and then plans and manages the best methods to employ organic and supporting collection and dissemination resources through the intelligence collection and dissemination plans (tabs to Appendix 16, *Intelligence Operations Plan*, to Annex B.) The CMDO is also responsible for validating and forwarding national and theater intelligence collection requests from the MEF and MSCs typically using appropriate intelligence tools and TTP. He also is responsible for coordinating intelligence CIS requirements and maintaining awareness of available CIS connectivity throughout the MAGTF and with key external organizations.

During operations the CMDO works within the support cell. In coordination with the P&A cell officer in charge (OIC), the SARC OIC, G-2 operations officer, intelligence/reconnaissance commanding officers/OICs, and the MEF G-6, the CMDO is responsible to the ISC for the following tasks:

- Determine and coordinate the collection effort of PIRs/IRs that may be collected via intelligence, CI, and reconnaissance resources.
- Determine PIRs/IRs and prepare requests for intelligence that are beyond organic capabilities and prepare submissions to higher headquarters and external agencies for support.
- Recommend dissemination priorities, development of intelligence reporting criteria, and advise on and selecting dissemination means.
- Develop and coordinate all-source intelligence collection plans, coordinate and integrate these with MEF, other components, JTF, theater, and national intelligence production operations.
- Develop and coordinate all-source intelligence dissemination plans and supporting architectures for voice and data networked communications, and coordinate and integrate these with MEF, other components, JTF, theater, and national intelligence CIS and dissemination operations.
- Monitor the flow of intelligence throughout the MEF and ensure that it is delivered to intended recipients in a timely fashion and satisfactorily meet their needs.
- Evaluate the effectiveness of MEF and supporting intelligence collection and dissemination operations.

SARC OIC

The SARC OIC is also an immediate subordinate of the ISC and is responsible for supervising the execution of the integrated organic, attached, and direct support intelligence collection and reconnaissance operations. The SARC OIC is responsible to the ISC for accomplishing the following specific responsibilities:

- Coordinate, monitor, and maintain the status of all ongoing intelligence, CI, and reconnaissance collection operations. This includes—
  - Missions, tasked intelligence collection requirements, and reporting criteria for all collection missions.
  - Locations and times for all pertinent fire support control measures.
  - Primary and alternate CIS plans for routine and time-sensitive requirements for intelligence users (collectors, the SARC, and key MEF, CE, and MSC C2 nodes) to support ongoing C2 of collection operations and dissemination of acquired data and intelligence via the most expeditious means.
- Conduct detailed intelligence collection planning and coordination with the MSCs and intelligence, CI, and reconnaissance organizations' planners, with emphasis on ensuring understanding of the collection plan and specified intelligence reporting criteria.
- Ensure other MAGTF C2 nodes; e.g., the current operations center or force fires are apprised of ongoing intelligence, CI, and reconnaissance operations.

- Receive routine and time-sensitive intelligence reports from deployed collection elements; cross-cueing among intelligence collectors, as appropriate; and the rapid dissemination of intelligence reports to MAGTF C2 nodes and others in accordance with standing PIRs/IRs, intelligence reporting criteria and dissemination plan, and the current tactical situation.

P&A Cell OIC

The P&A cell OIC is the third principal subordinate to the ISC, with primary responsibility for managing and supervising the MEF's all-source intelligence processing and production efforts. Key responsibilities follow:

- Plan, direct, and manage operations of the AFP (to include the fusion, order of battle, IPB, and target intelligence/battle damage assessment teams), the topographic platoon, the IIP, the DSTs, and other P&A elements as directed.
- Coordinate and integrate P&A cell operations, estimates, and products with the MEF G-2 section's G-2 operations branch and its Red Cell operations and estimates.
- Maintain all-source automated intelligence databases, files, workbooks, country studies, and other intelligence studies.
- Plan and maintain imagery, mapping, and topographic resources and other intelligence references.
- Administer, integrate, operate, and maintain intelligence processing and production systems, unclassified general service and senstitive compartmented information systems; e.g., the intelligence analysis system or the image product library.
- Analyze and fuse intelligence and other information into tailored all-source intelligence products to satisfy all supported commanders' stated or anticipated PIRs and IRs.
- Develop and maintain current and future intelligence situational, threat, and environmental assessments and target intelligence based upon all-source analysis, interpretation, and integration.

Manage and fuse the threat COP/CTP inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.

MAGTF Intelligence Units

The limited number of specialized intelligence assets, coupled with the requirement to integrate and focus intelligence operations on the satisfaction of the command's PIRs, creates the need for centralized management. Intelligence units whose capabilities support the entire MAGTF are employed in general support of the MAGTF with staff cognizance exercised through the G-2/S-2. Certain intelligence units are capable of performing operational tasks in addition to their primary intelligence functions. For example, a force reconnaissance team may carry out a laser target designation mission or a UAV may be used to assist in maneuver control. Likewise, radio battalion may support maneuver and fires through electronic attack operations. The MAGTF G-2/S-2 provides centralized direction for these assets and facilitates unity of effort, the production of all-source intelligence, and the effective use of limited resources in support of the requirements of the entire force. Direction is provided primarily through MAGTF-level intelligence C2 agencies; e.g., the SARC and the OCAC. Subordinate elements of the MAGTF retain organic intelligence assets and OPCON appropriate to their mission and level of command; e.g., division ground reconnaissance units remain under the OPCON of the division commander.

Organization of MAGTF-Level Intelligence Units

Radio Battalion

The radio battalion provides ground-based SIGINT, electronic warfare (EW), communications security

monitoring, and special intelligence communications capability to support MAGTF operations. In addition to directing the employment of its subordinate elements, the radio battalion is the focal point for MAGTF ground-based SIGINT operations. It plans and coordinates these activities through the OCAC.

Intelligence Battalion

The intelligence battalion plans, directs, collects, produces, and disseminates intelligence and provides CI support to the MEF, MSCs, subordinate MAGTFs and other commands as directed. This support is usually provided by a task-organized detachment sent to the supported command. Within the intelligence battalion is a headquarters company, a P&A company, and a CI/HUMINT company. (See figure 4-3.).

Headquarters Company

The headquarters company consists of a systems support platoon, collections platoon, and the GSP. The systems support platoon maintains the intelligence systems within the battalion in garrison and in the field should the battalion deploy. The collections platoon manages intelligence requirements for the battalion. The GSP is responsible for planning, controlling, and managing the employment of unattended ground remote sensor equipment in support of MAGTF operations or other commands as directed.

P&A Company

The P&A company consists of an AFP, a topographic platoon, and an IIP. The AFP provides fused intelligence to the supported MAGTF and

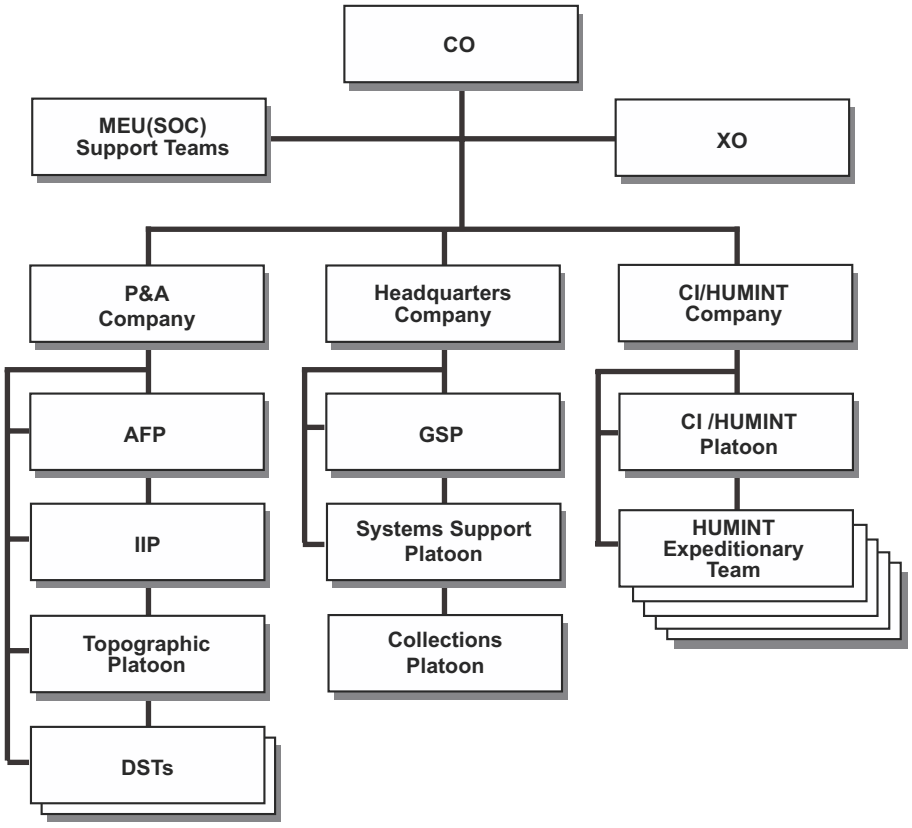


Figure 4-3. Intelligence Battalion.

assists MSC intelligence sections in providing situational awareness to their commanders and staff. The topographic platoon provides geographic intelligence products and services, geodetic and topographic surveys, and hydrographic analysis. The IIP provides imagery analysis support and dissemination to the MAGTF and other commands as directed.

CI/HUMINT Company

The CI/HUMINT company provides CI and HUMINT support to MAGTF operations. This support encompasses the full range of tactical CI and HUMINT operations, including screening operations, interrogation/debriefing of enemy prisoners of war and persons of intelligence interest, conduct of CI force protection source operations, conduct of CI surveys and investigations, preparation of CI estimates and plans, translation of documents, and limited exploitation of captured material. In addition, the CI/HUMINT company maintains a technical surveillance countermeasures team with equipment. CI/HUMINT Marines deploy as a task-organized HUMINT exploitation team (HET) in direct support of MAGTF's and subordinate elements.

Force Reconnaissance Company

The force reconnaissance company conducts preassault and deep postassault R&S in support of MAGTF operations. The company uses specialized insertion, patrolling, reporting, and extraction techniques to carry out amphibious and deep R&S tasks in support of the MAGTF. The company can perform a variety of other operational tasks. When a conflict exists between the requirements for R&S and other missions, the MAGTF commander determines the priority of tasking for the company based on recommendations from the G-2/S-2 and G-3/S-3.

Marine Unmanned Aerial Vehicle Squadron (VMU)

VMUs provide day/night, real-time imagery reconnaissance, surveillance, and target acquisition in support of the MAGTF. The unique capabilities of the UAV can also be used to support target engagement, assisting in the control of fires/supporting arms and maneuver. Squadrons are under the administrative control of the Marine aircraft wing (MAW). However, because of the limited number of assets and the critical capabilities they provide to the entire force, the MAGTF commander retains OPCON of the VMUs.

Employment of MAGTF Intelligence Units

MAGTF intelligence units are employed to meet the requirements of the entire force. The MAGTF G-2/S-2 develops a concept of intelligence support, which employs these units on the basis of the MAGTF mission, PIRs, concept of operations, and commander's intent. This concept must integrate intelligence activities with operations to provide key intelligence to commanders to enable rapid and effective decisionmaking. Based on the results of IPB analysis and the concept of operations, assets are positioned to satisfy PIRs, expose enemy vulnerabilities, monitor key locations, detect and assist in the engagement of targets, and identify opportunities as they arise in the battlespace.

Intelligence units are employed in either general or direct support. Under general support, units are tasked by the MAGTF commander through his G-2/S-2 to satisfy the requirements of the entire force. Because of the limited number of specialized intelligence assets and their ability to develop intelligence that is relevant to current and future operations in all areas of the battlespace (deep, close, and rear), general support is the preferred support relationship. Under direct support, the requirements of a supported commander are given priority. Direct support is used to focus intelligence support for particular phases of an operation or to create enhanced intelligence nodes in support of MAGTF subordinate elements. When MAGTFs smaller than a full MEF are deployed, they will normally be supported by

attached, task-organized detachments from the intelligence battalion, the force reconnaissance company, and the radio battalion.

Focused Intelligence Support

Intelligence must be integrated with the mission, commander's intent, and concept of operations and should normally be weighted to support the main effort. The MAGTF intelligence structure has the flexibility to tailor its capabilities to meet the requirements of various types of expeditionary operations and to adapt to changing operational needs during the execution. For each operation, the MAGTF G-2/S-2 will assess the IRs and develop a concept of intelligence support that positions assets where they can best satisfy those requirements. Intelligence nodes will be used to focus support within the MAGTF. Split-basing will be used to build intelligence nodes within and outside the AO to deliver comprehensive and reliable intelligence support while reducing the size of the deployed force. Intelligence units and DSTs are employed to tailor and enhance the capabilities of organic intelligence sections or to create task-organized intelligence nodes in response to specific requirements.

Intelligence Nodes

The MAGTF can create a series of intelligence nodes, thereby providing focused intelligence support to specific units or areas based on the tactical situation. In the concept of intelligence support, the MAGTF G-2/S-2, in conjunction with the MSC intelligence officers, task-organizes the MAGTF's intelligence units and uses intelligence DSTs to deliver the required intelligence capabilities at key points and times. Although these nodes normally support a specific unit, they can also be used in an area-support mode where an intelligence node is established to support all units operating in a particular sector of the battlespace. For example, during sustained operations ashore, an intelligence node could be built to support units operating in the MAGTF's rear area. Such a node could be built around a DST and specialists from the CI/HUMINT company and topographic platoon. This node might support the rear area operations center, CSSE units operating in the area or any security detachments located within the node's area of responsibility.

Split-basing

Intelligence nodes can also be used to tailor the footprint of the intelligence organization within and outside of a designated AO. Intelligence assets are positioned where they can best carry out their assigned functions. In many cases, it may not be necessary or desirable to forward deploy the entire MAGTF intelligence structure. The concept of operations, C2 support system, physical space limitations, and resource and/or logistical or other constraints may require the split-basing of intelligence assets.

Split-basing is the positioning of critical capabilities within the AO to support the deployed commander and forces, while maintaining in-depth intelligence management, processing, exploitation, analysis, and production elements in rear areas, intermediate support bases, staging areas or garrison locations. Split-basing enables reach back capabilities and can enhance the intelligence effort by providing continued access to sophisticated, nondeployable intelligence capabilities and resources. At the same time, it reduces the footprint of the deployed force, diminishing risk from enemy action and decreasing the administrative and logistic support requirements.

Split-basing is especially useful—

- When operations are conducted in areas with minimal infrastructure and support.
- When there are limitations on the number of personnel who can be deployed within the operating area.

- During the deployment phase when it may not be possible to immediately move all required elements of the intelligence structure to the forward area.

However, the advantages of split-basing must be assessed against its costs, particularly its critical dependence on responsive and reliable communications support.

Task Organization of Intelligence Support Units

Task organization of intelligence support units is one of the principal means for the MAGTF commander to shape the intelligence effort. The collection, exploitation, and unique production capabilities of specialized intelligence units significantly enhance the ability of supported G-2/S-2 sections to develop timely, mission-focused intelligence.

Intelligence battalion, force reconnaissance company, and radio battalion elements are task-organized to provide tailored intelligence capabilities. Specific capabilities provided are based on the threat, the supported unit's anticipated requirements (as determined through IPB), and the concept of operations. Elements from some or all of the intelligence battalion's subordinate companies are combined into intelligence battalion detachments. The CI/HUMINT company provides HETs. The radio battalion forms task-organized SIGINT support units (SSUs), which provide a mix of SIGINT and EW capabilities.

When MAGTFs smaller than a full MEF deploy, an intelligence battalion detachment, a HET, force reconnaissance platoons, and a radio battalion SSU will normally be attached to the MAGTF CE. In MEF operations, when the entire radio battalion, intelligence battalion, and force reconnaissance company are employed, detachments, HETs, SSUs, and platoons may be placed in direct support as required to provide tailored intelligence capabilities or to create an enhanced intelligence node in support of an MSC or other MAGTF element.

Intelligence DSTs

Intelligence DSTs are organic to the intelligence battalion and each of the division, MAW, and force service support group G-2 sections. Teams are made up of one officer and several enlisted personnel who have a mix of intelligence specialty skills. DSTs are used to provide an enhanced analytical and dissemination capability to a unit intelligence section and to link the intelligence structure to the supported units. As assigned by the G-2, they augment the supported unit's intelligence section to carry out the following tasks:

- Perform P&A in support of future operations.
- Tailor AFC and other external source intelligence products to the needs of the supported commander.
- Assist in the management of external intelligence support requirements.
- Facilitate dissemination of intelligence received from external sources.

The MEF and MSC G-2s use their DSTs to tailor and focus intelligence support to units designated as the main effort or to create enhanced intelligence nodes at key times and places in the battlespace.

Intelligence Coordination

Establishing and supervising operation of the MEF IOC, which includes the support cell, the SARC, and the P&A cell, requires a high degree of coordination at all levels. Generally the IOC will be collocated with the MEF CE's main CP. See figure 4-4 on page 4-14 for the basic IOC organization.

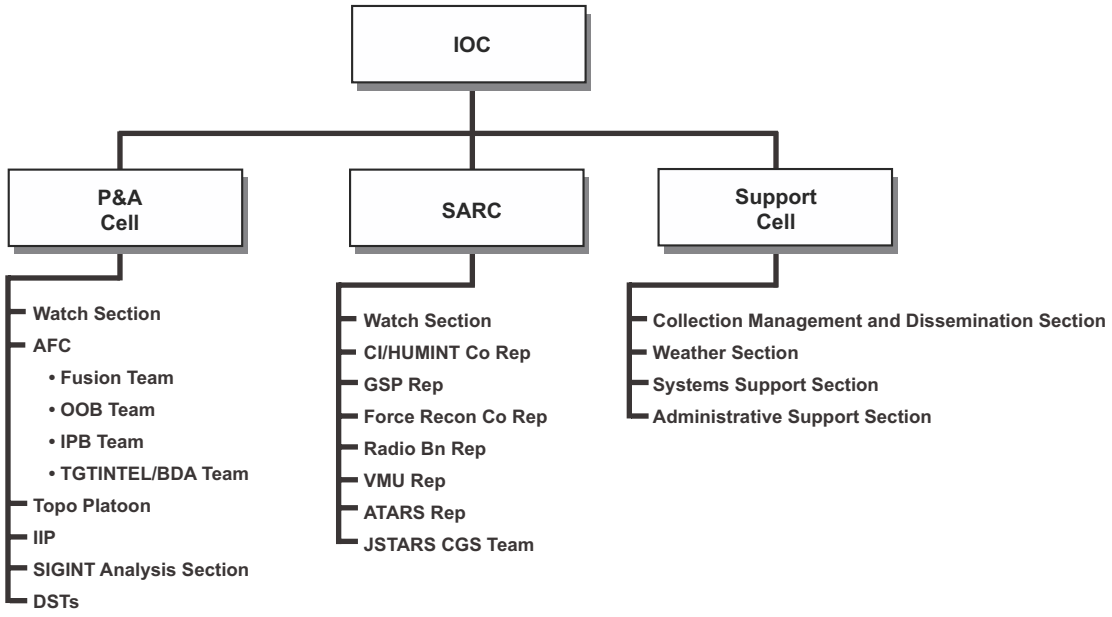


Figure 4-4. Intelligence Operations Center.

External Intelligence Support to the MAGTF

MARFOR Component Intelligence Section

Future military operations will normally be joint operations and may require establishing a MARFOR component headquarters. The Marine component is the level of command that deals directly with the JFC—the theater combatant commander or JTF commander—for MARFORs assigned to combatant command or the JTF. The Marine component functions at the operational level of war to advise and assist the JFC in employing MARFORs while supporting the MAGTF. The Marine component commander coordinates operational actions with the JFC and the other component commanders so that the MAGTF commander can concentrate on warfighting.

Responsibilities

The Marine component intelligence section plays a crucial role in supporting the component commander and staff and in providing intelligence support to the MAGTF. The Marine component supports and enhances the planning and execution of MAGTF intelligence operations through close and continuous coordination with the JFC, joint force headquarters, and other component intelligence organizations. The Marine component G-2 section maintains situational awareness and provides a limited analytical capability to support the component future planning responsibility. It does not normally conduct collection operations or engage in detailed, formal intelligence production. It facilitates, but does not control, the flow of intelligence to the MAGTF. The component relieves the MAGTF commander of intelligence functions that are not directly related to warfighting.

Functions

The size of the Marine component G-2 section will vary with the size of the JTF and the scope of the operation. For major joint operations, the Marine component intelligence section provides the following functions:

- **Planning.** The intelligence section plans and coordinates component and MAGTF connectivity to national, theater, and JTF intelligence architectures. The Marine component develops the architecture to provide the MAGTF with timely, tailored national and theater intelligence. The component G-2 coordinates the provision of additional Service intelligence support (units, personnel, and equipment) to the MAGTF through the Service chain of command.
- **Collection management.** The intelligence section monitors the status of MAGTF collection requests for supporting and external collection resources. The MARFOR leverages joint and national collection resources in support of the MAGTF. It advocates Service component and MAGTF requirements in theater and JTF collection forums and recommends the allocation and tasking of national, JTF, and other component assets to meet MAGTF requirements.
- **P&A.** The intelligence section provides situational awareness to the component commander and staff and limited P&A to support the future planning responsibilities of the component headquarters. This function requires the establishment of a watch section and an analytical element that can tailor operational-level intelligence products to satisfy the needs of component planning cells. The component G-2 monitors the status of and coordinates support for MAGTF production requirements and requests for intelligence that are submitted to joint force or supporting intelligence agencies.
- **Dissemination.** The intelligence section monitors the adequacy of the intelligence architecture and the flow of intelligence to the MAGTF. Intelligence is disseminated directly to the appropriate MAGTF elements, not through the component headquarters unless specifically required. However, the MARFOR facilitates and accelerates the flow of critical intelligence to the MAGTF. The component intelligence section remains aware of current MAGTF requirements and ensures that intelligence that is developed or received by the theater or JTF that can satisfy those requirements is disseminated to the MAGTF.
- **Support of targeting.** The intelligence section supports Marine component participation in the joint targeting process, including representation at various joint target intelligence and/or targeting forums as required. Performing this function ensures that MAGTF target intelligence collection and production requirements as well as collection requirements for support of combat assessment/BDA are adequately supported.

Liaison

The intelligence section provides liaison elements and personnel augmentation to various JTF and other component intelligence organizations. Liaison elements may be provided to the following:

- JISE.
- Other Service or functional component intelligence sections.
- The regional SIGINT operations center.
- The joint force J-2 CI/HUMINT staff element.
- The HUMINT operations cell.
- Task force CI coordinating authority, other joint intelligence organizations such as the joint interrogation and debriefing center or the joint document exploitation center.
- The intelligence elements of various alliance or coalition partners.

Liaison teams or personnel augmentation may be sourced from the Marine component G-2 section, Service augmentation to the component G-2 section, the MAGTF, or some combination of the above.

National, Theater, Joint, and Other Service Intelligence Support

Marine Corps intelligence assets are optimized for the production of tactical intelligence in support of MAGTF operations. National, theater, joint, and other Service intelligence assets provide unique capabilities that are not duplicated in the MAGTF intelligence support structure. (See figure 4-5.) The MAGTF has the ability to use external intelligence assets to enhance its organic capabilities, bringing the full range of these resources to bear on MAGTF requirements. The following are key external capabilities that support MAGTF operations:

- National- and theater-level intelligence analysis and production.
- Geospatial information and services (GI&S). GI&S describes the collection, production, and dissemination of information about the earth, and replaces the term mapping, charting, and geodesy.

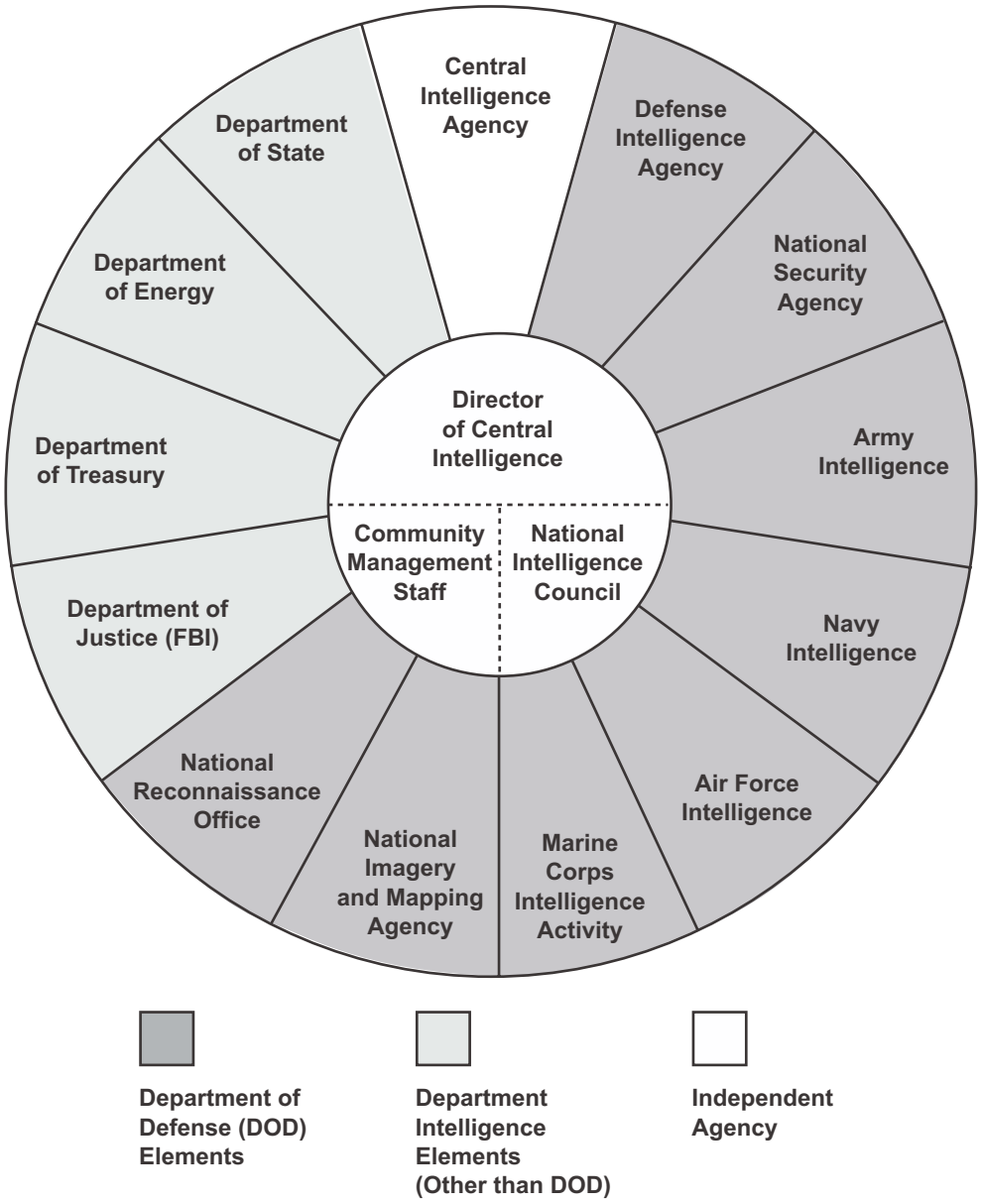


Figure 4-5. The National Intelligence Community.

- Analysis and production of target intelligence and target materials.
- National imagery collection and exploitation.
- SIGINT support from the National Security Agency and the US Cryptologic System.
- National- and theater-level CI and HUMINT collection.
- Liaison elements from national and theater intelligence agencies.

MAGTF Access to External Support. The Marine component headquarters or the MAGTF intelligence section will be the focal point for all external intelligence support to the MAGTF. In major joint operations, a Marine Service component headquarters will be established, and the component G-2 performs this function. When no Service component headquarters is established, the MAGTF acts in this role. Intelligence derived from external sources is used to build a common picture of the battlespace and is incorporated into other intelligence products that are provided to all MAGTF elements. MSCs and other subordinate units will be able to access external intelligence support resources through the MAGTF's intelligence architecture.

Required Capabilities

The following capabilities are required to fully use the resources of external intelligence support assets:

- Personnel trained and experienced in the capabilities, limitations, tasking, and employment procedures of external intelligence support assets.
- Sufficient, reliable CIS connectivity and interoperability with national, theater, and other Service intelligence C2 centers and architectures.
- The ability to receive, process, and disseminate information gathered by national and theater collection assets.
- Integrating Marine intelligence specialists into national, theater, and Service intelligence organizations to articulate Marine Corps capabilities and requirements and to optimize intelligence support to expeditionary forces.
- Establishing liaison between the MARFOR/MAGTF and supporting intelligence agencies through dedicated communications and the exchange of liaison officers.

Augmentation

Like all MAGTF components, intelligence support assets are flexible and respond to a variety of operational missions. They are configured for rapid deployment and can be tailored to meet the requirements of a particular operation. Although each MAGTF is furnished with a baseline intelligence capability to accomplish its anticipated mission, changes in the situation or mission tasking may require augmentation. When a MAGTF is committed to an operation, the intelligence assets of any remaining units in the operating forces can be called on to provide this augmentation. MAGTFs smaller than a MEF will normally be supported by their parent MEF; a fully deployed MEF can be augmented by the assets of any other MEF. Augmentation may consist of providing entire intelligence units, selected equipment or individual personnel with specialized skills. Support may also consist of providing intelligence products that cannot be developed by the deployed MAGTF or its supporting joint intelligence activity.

Supporting Establishment

Marine intelligence personnel and organizations of the supporting establishment enhance and sustain the intelligence activities of the operating forces.

Marine Corps Intelligence Activity

The Marine Corps maintains a Service-level intelligence capability in the Marine Corps Intelligence Activity (MCIA). MCIA focuses on crisis and predeployment support to expeditionary warfare. It complements the efforts of theater, other Service, and national intelligence organizations. It provides

unique threat, technical, and geographic intelligence products that are tailored to Marine Corps operating forces preparing for deployment. It also coordinates Marine Corps Service collection, production, and dissemination requirements by acting as the Service collection, production, and dissemination manager. MCIA is collocated with the National Maritime Intelligence Center, Suitland, MD and at Marine Corps Base, Quantico, VA.

Marine Cryptologic Support Battalion

The Marine cryptologic support battalion provides Marine Corps participation in national and Department of the Navy cryptologic activities worldwide. These Marines perform tasks that are directly related to their military occupational specialty, contributing to the national, theater, and Department of the Navy SIGINT collection, production, and dissemination effort while gaining invaluable skill maintenance and enhancement opportunities. The battalion is collocated with the Naval Security Group, Fort Meade, MD and augments the operating forces with trained SIGINT personnel during crises and exercises.

Navy Marine Corps Intelligence Training Center

The Navy Marine Corps Intelligence Training Center (NMITC), Dam Neck, VA trains Navy and Marine Corps personnel in basic, intermediate, and advanced intelligence methods and applications. During contingency operations, NMITC supports the operating forces through the provision of intelligence training via mobile training teams and/or selective personnel augmentation.

Personnel Augmentation

The supporting establishment is also a source of experienced intelligence personnel who can be called on to fill contingency billets in the intelligence structure of a deploying or committed MAGTF.

Marine Corps Forces Reserve

The mission of Marine Corps Forces Reserve is to provide trained units and/or personnel to augment, reinforce or reconstitute active duty MARFORs during times of war or national emergency. Intelligence capabilities of the Marine Corps Reserve are complementary to those of the active component. This includes individual mobilization augmentee and individual ready reserve personnel and selected Marine Corps Reserve units (including two force reconnaissance companies), a GSP, an imagery interpretation unit, and several interrogator-translator and CI teams, which provide increased depth to limited active component capabilities.

Individual mobilization augmentee members of the Marine Corps Reserve Intelligence Program and the Marine Corps Reserve Cryptologic Program routinely support the training and operational activities of the active component.

CHAPTER 5
OPERATIONAL MANEUVER FROM THE SEA

OMFTS is the maneuver of naval forces at the operational level that projects sea-based power ashore to deal a decisive blow. OMFTS is a bold bid for victory that aims to exploit a significant enemy weakness. It embodies the application of the principles of maneuver warfare to a maritime campaign. Success in OMFTS depends on the ability to seize fleeting opportunities and quickly take advantage of exposed enemy vulnerabilities. See MCDP 1-0, *Marine Corps Operations*.

OMFTS relies on intelligence to drive planning, option selection, and maneuver execution. To support OMFTS, intelligence operations must be conducted across the strategic, operational, and tactical levels of war. Starting with strategic considerations and working down to tactical dispositions, intelligence uncovers the threat's COG, strengths, and weaknesses, thereby exposing critical vulnerabilities to be exploited by naval forces operating from the sea. Intelligence also assesses the potential for maneuver offered by the battlespace, including identifying entry points where the force can establish itself ashore. The term entry point encompasses beaches, boat landing sites, HLZs, and drop zones that can establish elements of the force ashore. Intelligence also provides the foundation for effective force protection and IO efforts. These efforts help surprise, preempt, disrupt, and disorient the enemy during OMFTS execution.

Required Intelligence Capabilitites

- Perform IPB and situation development covering a broad maneuver space.
- Analyze threat forces to determine COG and critical vulnerabilities.
- Conduct detailed terrain and hydrographic analysis to identify suitable entry points.
- Ensure connectivity and interoperability with national, theater, and joint forces' intelligence assets, which provide intelligence support before the arrival of naval forces in the objective area.
- Provide stand-off collection assets that can satisfy force requirements from over-the-horizon.
- Provide organic imagery, SIGINT, HUMINT, CI, remote sensor, GI&S, and ground and aerial reconnaissance assets that can satisfy MAGTF tactical collection requirements as the force transitions ashore.
- Provide responsive processing, exploitation, and production capabilities that can rapidly develop the critical intelligence required to support timely decisionmaking.
- Provide dissemination systems that link widely dispersed forces afloat and ashore.
- Provide flexible intelligence units and organizations that can rapidly transition ashore with minimal degradation of support.
- Provide in-depth support to force protection and information operations activities.

Planning and Direction

There are a number of unique intelligence considerations for OMFTS. (See figure 5-1 on page 5-2.) During the planning phase, the MAGTF intelligence officer provides centralized direction for the intelligence efforts of the entire MAGTF. Navy and Marine intelligence assets operate together from an afloat amphibious force intelligence center, which is normally located on the amphibious force flagship. Initial requirements are broad in scope and are aimed at providing a general description of the battlespace and the threat. As planning progresses, requirements become increasingly focused on uncovering critical vulnerabilities and providing

intelligence that is relevant to the COAs under consideration. The intelligence flow will be predominately from the top down—from national and theater activities—until organic naval intelligence capabilities can be brought to bear. A comprehensive, systematic management effort is required to ensure that the necessary support is requested and received. At the same time, Navy and Marine intelligence officers must also develop detailed plans for the positioning and employment of the organic intelligence assets to support the concept of operations.

Intelligence Cycle	Key Considerations
Planning and direction.	Centralized direction from ATFIC. Transitioning of key capabilities ashore.
Collection.	Initial dependence on national/theater capabilities. Employment of organic assets in advance force/ preassault operations.
Processing, exploitation, and production.	Broad-based effort focusing on entry points and enemy vulnerabilities. Extensive support to CI and IO.
Dissemination.	Widely dispersed units afloat and ashore. Need for rapid intelligence flow to exploit fleeting opportunities.
Utilization.	COA selection shaped by intelligence. Choice of entry points, objectives, and targets driven by intelligence.

Figure 5-1. Intelligence Considerations During OMFTS.

Collection

Collection operations in the planning phase are conducted primarily by national and theater assets. These assets can collect information in denied areas without compromising operational security and/or perform their missions at significant stand-off distances. However, the small number of these systems and inherent limitations on their capabilities normally result in developing an incomplete intelligence picture. Advance force or preassault collection operations by naval assets will often be required to confirm and further develop the situation. An intensive intelligence effort must be provided in support of advance force or preassault operations; this intelligence support is required to select the proper targets for advance force or preassault collection operations, and ensure that these activities do not reveal the intent of the overall operation.

Processing, Exploitation, and Production

Initial production efforts are directed at providing an extensive description of the battlespace and threat. This description is required to focus the planning effort. Under the direction of senior Navy and Marine intelligence officers, the MAGTF, GCE, ACE, CSSE, Navy amphibious staff, and flagship intelligence sections engage in a cooperative effort to develop intelligence products that support the entire force. Individual intelligence sections will normally concentrate on their particular areas of expertise, thereby satisfying their units' requirements while contributing a broad-scope product to the general intelligence production effort. For example, the MAGTF G-2/AFC may focus on describing the battlespace and the enemy's C2, logistics, and reserves, while the GCE studies enemy ground forces, the ACE looks at the air and air defense threats, and the flagship intelligence department concentrates on the naval and coastal defense threat. From this effort, the ATFIC provides a comprehensive IPB analysis, an intelligence estimate, and supporting intelligence studies and products. As the planning phase continues, production efforts concentrate on identifying enemy vulnerabilities to be exploited and providing estimates and other intelligence products to support the specific COAs that are under consideration.

In the final stages of the OMFTS planning process, the production effort shifts to developing mission-specific intelligence products that focus on the selected COAs. These products include

IPB graphics, beach and HLZ studies, and target/objective area studies. An extensive all-source intelligence effort is conducted to support deception, OPSEC, psychological operations (PSYOP), and EW planning in accordance with the MAGTF commander's overall IO strategy. During this stage, the production effort becomes increasingly decentralized as GCE, ACE, and CSSE intelligence sections focus on specific requirements of their units. The MAGTF intelligence section continues to provide products to support the entire force, with efforts concentrated on those MAGTF elements designated as the main effort.

Dissemination

Dissemination in OMFTS presents significant challenges. Naval forces can be widely dispersed and may not assemble until late in the planning phase, if at all. Advances in technology have improved the capability to disseminate information between forces afloat, but there continue to be limitations on the quantity and quality of intelligence that can be exchanged. In particular, dissemination systems will be taxed by the volume of intelligence products, especially critical graphic products that must be distributed during the planning phase. Intelligence officers at all levels, working in coordination with unit operations and CIS officers, must develop plans that provide for dissemination of key intelligence in a timely manner to all elements of the MAGTF. They must be particularly careful to include in these plans units located on ships that are not equipped with the latest C2 or intelligence systems.

Utilization

During the planning phase, intelligence is used to develop and select COAs and prepare detailed plans for implementing the selected COAs. After providing an initial orientation to the battlespace and the threat, the intelligence officer assists the commander and the staff in analyzing the enemy's strengths and weaknesses to identify COG and critical vulnerabilities that can be exploited. COAs are developed that take advantage of identified weaknesses to accomplish the assigned objective. The intelligence effort is refined on the basis of the COAs under consideration, providing answers to IRs generated during COA development. The intelligence developed through this interactive process aids the commander in selecting a favorable COA. Once the COA is chosen, intelligence shapes the concept of operations and supporting plans. Designation of objectives; selecting entry means, points, and times; and identifying targets are all based primarily on intelligence. Particular attention is given to steps that preserve surprise and that preempt, disrupt or disorient the enemy's response to our actions; e.g., force protection measures, and IO (including, but not limited to, physical destruction, military deception, OPSEC, PSYOP, and EW) plans.

Planning and Direction

The ATFIC will continue to act as the central node for the direction of the intelligence effort. As the operation unfolds, intelligence nodes can be established ashore to support units carrying out mission tasking. Depending on the nature and scope of the operation, most of the MAGTF intelligence structure can remain afloat or all of it may transition ashore. Movement of significant portions of the MAGTF intelligence structure ashore must be planned in detail to ensure a rapid transition with minimal degradation of support capability. If it is fully established ashore, the MAGTF intelligence section becomes the central node for intelligence direction. The ATFIC acts in a supporting capacity and continues to provide connectivity and services that cannot be readily established ashore.

IRs that arise during execution are normally time sensitive. Intelligence direction must anticipate these requirements and establish a responsive collection, production, and dissemination structure to satisfy them. Designation of PIRs that are based on the results of IPB analysis, the commander's intent, and the concept of operations is critical. Using these factors to designate PIRs ensures that the intelligence effort remains focused on providing key intelligence to decisionmakers in a timely manner.

Collection

Collection operations transition from depending on national and theater capabilities to relying primarily on organic assets. Collection activities are integrated with the concept of operations. The objective is to develop the intelligence required to make key decisions regarding maneuver, targeting, and future plans. Collection assets are focused on key areas that are associated with the scheme of maneuver, location and development of critical targets, and combat assessment. Reports of units maneuvering through the battlespace and/or in contact with the enemy are a significant source of information. This information must be transmitted to the appropriate intelligence section to help maintain situational awareness and refine the threat assessment. The MAGTF continues to employ national and theater-level collection support against targets located deep in the area of influence, throughout the area of interest, and against less time-sensitive requirements.

Processing, Exploitation, and Production

Rapid processing and production of intelligence are emphasized to support timely decisionmaking. OMFTS depends on decisive action and generating rapid operational tempo to break the enemy's cohesion and ability to resist. Intelligence sections must demonstrate the flexibility, agility, and responsiveness to quickly recognize enemy vulnerabilities and identify opportunities as they develop during the battle. To do this, intelligence sections at all levels must be aware of ongoing tactical activities and potential enemy reactions. They must be able to rapidly integrate all-source intelligence information with sensor data and combat reporting to develop and maintain a coherent picture of enemy dispositions and an assessment of enemy intentions. They must be able to convey this picture and assessment (preferably in graphic form) to commanders in time to exploit identified opportunities. In addition to supporting the ongoing battle, intelligence sections must also be fully engaged in planning for future operations (continuing IPB analysis, delivering combat assessment inputs and BDA results, satisfying new IRs, and participating in the decisionmaking process).

Dissemination

Dissemination is an even greater challenge during OMFTS execution than during planning. Intelligence developed during the processing, exploitation, and production step must be rapidly disseminated to the units that are able to act on that intelligence. These forces may be widely dispersed afloat, airborne, and ashore while engaging in rapid maneuver and contact with the enemy. The dissemination system must be flexible and reliable and focus on the importance and quality of the intelligence distributed rather than on its volume. Dissemination plans must provide alarm channels for warning data and must ensure that pathways remain open for passing critical intelligence that directly affects PIRs or identified decision points. Measures that can help to reduce the volume of intelligence traffic follow:

- Limit routine reporting.
- Set filters to eliminate information that is not pertinent to the tactical situation.
- Establishing minimal reporting thresholds for the generation of intelligence reports.
- Providing alternate means for collection and other intelligence support requests.

Dissemination plans must permit two-way dissemination, providing a means for subordinate

elements to pass along data, information or intelligence that they collect or develop that identifies new enemy vulnerabilities or enhances situation development for the entire force.

Utilization

Utilization of intelligence during the execution of OMFTS is rapid and decentralized. Intelligence identifies enemy vulnerabilities as the battle unfolds.Once developed, this intelligence is quickly disseminated to the MAGTF elements that can act on it, thereby enhancing the ability of individual units to exploit opportunities as they arise. Through integration with operations, assets are positioned to develop new intelligence as the concept of operations is carried out and the enemy responds. Timely collection, analysis, and dissemination of intelligence provides commanders with an accurate picture of the battlespace and the ability to recognize new opportunities as they arise. Commanders use this intelligence to select branches and sequels to the COA, attack targets, protect their own forces, assess the results of their actions, and plan future operations.

CHAPTER 6
SUSTAINED OPERATIONS ASHORE

Sustained operations ashore require broad-based intelligence support that bridges the operational and tactical levels. Tactical plans are based on the results of operational-level intelligence assessments, which identify the enemy's COG and critical vulnerabilities throughout the theater of operations. MAGTF intelligence operations contribute to the operational-level assessments while translating the conclusions from these assessments into relevant tactical intelligence. Considerations for developing intelligence in support of sustained operations ashore are similar to those for OMFTS. Intelligence support during the execution of sustained operations ashore requires the same agility and responsiveness as in OMFTS, with the focus on providing critical intelligence to support timely decisionmaking. However, sustained operations ashore are normally conducted over a greater land area and with a larger force than in OMFTS, creating the requirement for a larger and more widely distributed intelligence support structure. The need for integration with theater, joint, multinational, and other Service intelligence assets is also greater.

Required Intelligence Capabilities

- Field and sustain intelligence structure to support MEF-level operations over extended periods.
- Execute all intelligence functions of a Service component headquarters, including full participation in theater or JTF intelligence activities.
- Ensure sufficient and reliable CIS systems connectivity and interoperability with theater, joint, and other Service intelligence assets participating in the operation.
- Conduct IPB and situation development in support of operational- and tactical-level planning.
- Provide organic imagery, SIGINT, CI, HUMINT, remote sensor, GI&S, and ground and aerial reconnaissance assets that can satisfy MAGTF tactical requirements.
- Provide processing, exploitation, and production capabilities that can supply the extensive products required to support MEF-level planning and execution.
- Provide dissemination systems that link widely dispersed and rapidly maneuvering forces.
- Provide area specialists and linguists with skills that are pertinent to the AO.
- Support force sustainment operations through detailed logistic intelligence.
- Support force protection efforts conducted throughout a large operating area, with emphasis on the security of critical rear area C2 and logistic facilities.

Planning and Direction

Intelligence direction during sustained operations ashore will be centralized during the planning phase and increasingly decentralized during execution. IRs are extensive and cover all aspects of the threat and the battlespace. Comprehensive collection, production, and dissemination efforts will be required to satisfy these requirements. Detailed management is necessary to ensure that these efforts are properly focused and integrated to meet the needs of the entire force. The MAGTF intelligence section will act as the primary intelligence node, developing intelligence to support the MAGTF commander, staff, and subordinate elements. The Marine component headquarters serves as the focal point for connectivity with the theater or JTF intelligence structure. During the planning phase, timeliness of

intelligence production may not be as critical because the planning process for sustained operations ashore normally takes place over an extended period and offers the opportunity to use more time and resources to answer those requirements. (See figure 6-1.)

Intelligence Cycle	Key Considerations
Planning and direction.	MAGTF acting as central mode. Need for broad intelligence structure with extensive liaison requirements.
Collection.	Competition for national, theater, and JTF support. Reliance on organic assets to satisfy many tactical requirements. Support to BDA.
Processing, exploitation, and production	Wide-scope effort that bridges operational and tactical levels. Importance of target and geographic intelligence.
Dissemination.	Extensive CIS infrastructure. Widely dispersed units. Timely support.
Utilization.	Need to integrate operational and tactical levels of intelligence and operations. Support to sustainability functions.

Figure 6-1. Intelligence Considerations During Sustained Operations Ashore.

Once execution begins, the emphasis is on satisfaction of time-sensitive requirements to support operational and tactical decisionmaking. Intelligence nodes will be created at selected times and places to provide tailored intelligence support to units executing specific phases or aspects of the concept of operations. Intelligence direction must balance the support provided among close, deep, and rear operations and the support to current and future operations.

The intelligence structure required to support sustained operations ashore is normally more extensive than that used in other types of MAGTF operations. A detailed planning effort must be undertaken to ensure that the necessary assets are tasked, deployed, and positioned where and when they are required. Sustained operations ashore are frequently based on a theater combatant commander's approved operations plan or other standing contingency plans that include provisions for a baseline intelligence support structure. These plans must be adapted and tailored to the particulars of the current and projected operational situation. Intelligence plans use a building-block approach, phasing in capabilities to keep pace with the buildup of operational forces. Planners must remain aware that intelligence capabilities must be in place to support the earliest steps of the planning phase; therefore, a robust intelligence structure is normally required in the initial stages of the deployment.

Many of the intelligence activities conducted during sustained operations ashore will be joint. Intelligence plans must provide for connectivity with the theater or joint and other component intelligence assets and for participation in theater or JTF intelligence mechanisms. An extensive liaison effort will be required to ensure that MAGTF IRs and operations are fully coordinated with those of joint and other Service intelligence activities. The MARFOR and MAGTF will require significant personnel augmentation to meet the broad scope of intelligence activities in sustained operations ashore and provide liaison teams to the numerous joint and supporting force intelligence agencies. This augmentation can be drawn from residual forces, the supporting establishment or the Reserves.

Collection

Sustained operations ashore will normally be supported by the full range of national- and theater-level collection capabilities and by the organic assets of the participating component forces. Collection priorities for national and theater assets will be determined by the JFC. The bulk of these assets will usually be targeted against overall theater/JTF objectives. Marines must participate in the joint collection management and production processes to ensure that MAGTF PIRs receive

appropriate support from the theater/JTF level. However, even if MAGTF requirements are given priority, the results of national and theater collection operations cannot be relied on to completely satisfy the number of requirements developed during extended sustained operations ashore or to provide the level of detail needed for tactical planning and execution. For this reason, the MAGTF must depend on its organic collection assets to provide the bulk of its tactical intelligence information, particularly during the execution phase. The MAGTF must be prepared to plan and execute imagery, SIGINT, HUMINT, ground reconnaissance, and CI force protection source operations throughout its AO. This includes collection activities in support of deep operations and the planning of future operations. MAGTF collection plans must be coordinated with those of higher, adjacent, and supporting commands to ensure the following:

- All requirements receive adequate coverage.
- Collection assets are employed efficiently with minimal overlaps.
- Collection operations are sufficiently integrated to permit free exchange of collection targeting data and tracking of collection targets as they move through the battlespace.

Processing, Exploitation, and Production

Processing, exploitation, and production efforts in support of sustained operations ashore parallel those for OMFTS. The scope of the initial production is broad, with the focus narrowing as particular COAs are selected and a concept of operations is developed. Geographic intelligence production takes on added importance. Geographic intelligence helps identify opportunities for ground and air maneuver and determine line-of-sight profiles for observation, weapons employment, and the effective use of communications-electronic equipment. Mapping enhancements, lines-of communications studies, and IPB graphics (such as cross-country mobility, weather effects, and combined obstacle overlays) are key intelligence products that support sustained operations ashore.

Threat analysis must be comprehensive and generally deals with large ground and air formations. This analysis covers reserves and committed forces and must consider all factors that affect the enemy's ability to fight at the operational and tactical levels, including leadership, doctrine, training, readiness, and sustainability. An extensive production effort is devoted to supporting CSS operations. The main components of this effort are studies on the local climate, infrastructure, and resources and on the threat to our rear area and lines of communications. Products from national, theater, and JTF intelligence agencies contribute to the production effort, but many of these products will have to be tailored by the AFC and GCE, ACE, and CSSE intelligence sections to satisfy particular MAGTF requirements. During execution, emphasis is placed on rapid processing and production of tactical intelligence to support decisionmaking in the current battle, while at the same time providing detailed intelligence to shape plans for future operations.

Dissemination

The ability to develop and maintain a shared picture of the battlespace among the diverse components of the joint force is essential. MAGTF and Marine component dissemination architectures not only must provide for distributing intelligence within the MAGTF, but also must permit the timely exchange of intelligence with the theater or JTF headquarters, other component commands, and adjacent and supporting units. Marine intelligence architectures must be

fully integrated with the theater or JTF structures. This requires detailed planning and coordination because each theater and JTF has a unique architecture and sometimes separate channels are used for the dissemination of finished intelligence, imagery, SIGINT, HUMINT, and CI information. Dissemination during the early phases is normally simplified by establishing a reliable, redundant communications system between fixed or semi-fixed CPs. However, even a robust communications system will be challenged by the requirement to distribute a large volume of maps, imagery, and other graphic products during the planning stage.

During execution, the dissemination challenges are similar to those of OMFTS; i.e., ensuring the rapid distribution of time sensitive, mission-critical intelligence to widely dispersed units on the move or in contact with the enemy. A number of techniques can be used to prevent the loss of intelligence that is needed for timely decision-making in the stream of intelligence data and information. Some follow:

- Establishing alarm dissemination channels.
- Using broadcast mode for specialized intelligence reporting.
- Employing DSTs or designating a specific element of the intelligence section as a dissemination team.
- Linking dissemination to factors developed in the other phases of intelligence development, such as PIRs, named areas of interest, high-value targets, and high-payoff targets.
- Giving particular attention to the distribution of updated imagery and graphic intelligence products to units that cannot be supported from fixed or semi-fixed intelligence support nodes.

Utilization

The use of intelligence in sustained operations ashore follows the same principles as its use in OMFTS. The difference lies in the scope of the effort required and the need to integrate intelligence and operations simultaneously at multiple levels: theater or JTF, MARFOR, MAGTF, MSC, and tactical units (regiments/groups/battalions/squadrons/detachments).

In sustained operations ashore, intelligence is used to form operational and tactical plans that will accomplish campaign objectives. Broad-based strategic, operational, and tactical intelligence on the enemy and the AO is used by intelligence and operational planners in an interactive process to identify COG and critical vulnerabilities that can be attacked or exploited to achieve campaign objectives. This in turn leads to COA development, selection, and refinement, an effort that must be coordinated and integrated from the theater/JTF down to the tactical level. Intelligence helps determine the main and supporting efforts; designate objectives, times, and locations for these efforts; and identify the support required for each to succeed. During execution, intelligence helps develop the situation, supporting decisions on whether to continue or modify the plan and whether to exploit success or take advantage of new opportunities. At the same time, intelligence facilitates the planning of follow-on operations through support to combat assessment and providing continuing IPB analysis. Intelligence helps plan and conduct critical sustainability functions, contributing key logistic intelligence and force protection recommendations.

CHAPTER 7
MILITARY OPERATIONS OTHER THAN WAR

MOOTW refers to the conduct of Marine and naval expeditionary operations across the range of military operations short of war. MOOTW encompass a wide variety of activities intended to deter war, resolve conflict, promote peace, and support civil authorities. MOOTW encompass a broad range of 16 possible missions and tasks, each of which has its own unique IRs. (See MCDP 1-0.)

Intelligence activities in MOOTW are characterized by the following:

- The initial lack of detailed intelligence databases on the AO.
- An extensive list of nonstandard IRs that must be satisfied to support planning and execution.
- A rapidly changing situation resulting from crisis conditions in the AO.
- A compressed time frame for intelligence development.
- Restrictions on collection operations.

Intelligence shapes operations during MOOTW as it does during other types of expeditionary operations. However, in addition to understanding the physical environment and the threat, the commander must have intelligence on political, economic, and sociological conditions to develop sound military plans that will accomplish the assigned mission.

To support MOOTW, MAGTF intelligence operations and supporting assets must be maintained in a high state of readiness. MAGTF intelligence sections must focus on areas with the greatest potential for executing contingency operations and must be able to respond with minimal warning and preparation. They must also be flexibile to adapt to the wide variety of potential missions, possessing the expertise and specialized capabilities to provide intelligence across the full range of MOOTW.

Required Intelligence Capabilities

- Forward-deployed intelligence sections that are manned, trained, and equipped to respond to a variety of short-notice contingency operations.
- Deployable intelligence assets that can be rapidly "surged" to augment the capabilities of a forward-deployed MAGTF committed to MOOTW.
- Specialized knowledge concerning infrastructure, political, economic, cultural, and sociological conditions in a variety of geographic areas.
- The ability to perform IPB and situation development that focuses on unconventional threat forces, such as security forces, paramilitary groups, insurgents, and terrorists.
- Organic CI and HUMINT capability that is prepared for operation in a variety of MOOTW scenarios.
- SIGINT assets that can collect information from nontraditional targets.
- Dissemination systems that link widely dispersed forces.
- Connectivity to national, theater, joint, and multinational force intelligence assets to provide intelligence support during planning and execution.
- Area specialists and linguists with skills that are pertinent to the AO.
- Expertise in the operations and functioning of non-DOD government agencies, international coalitions, and nongovernmental organizations (NGOs). (An NGO is a transnational organization of private citizens that maintains a consultative status with the United Nations. NGOs may be professional associations, foundations, businesses or groups with a common interest in humanitarian assistance. Examples include the Red Cross and the Cooperative for Assistance and Relief Everywhere.)

Planning and Direction

There are certain unique intelligence considerations during MOOTW. (See figure 7-1.) Direction of the intelligence effort in MOOTW will generally be highly decentralized. During MOOTW, MAGTF elements can be spread across a wide area, each with a different mission and facing a unique situation. While a central node will be needed to direct the efforts of MAGTF intelligence assets and coordinate external support, the bulk of intelligence will be provided by subordinate intelligence sections supporting their individual units. Consideration should be given to directing the intelligence effort on an area-support basis rather than a unit support basis. In an area-support system, intelligence nodes are created to support all units operating in the designated area. IRs will be extensive and diverse. Many will deal with topics and threats that are not normally confronted during conventional operations. Individual intelligence sections and nodes must be provided with expertise or with access to resources that can satisfy these nonstandard requirements.

MOOTW are often generated as a result of fast-moving crisis situations. Intelligence plans must emphasize readiness and flexibility to respond to MOOTW requirements in a timely manner. MAGTF intelligence sections at all levels must maintain an awareness of potential contingency missions and adopt a "lean forward" approach toward anticipating requirements. Forward-deployed MAGTFs must possess all required intelligence capabilities to function in a wide variety of MOOTW missions. The active Marine service components (Marine Forces Atlantic or Pacific) must be prepared to rapidly deploy additional or specialized assets to augment the capabilities of the forward-deployed MAGTF.

In planning the intelligence structure required to support a particular MOOTW, several factors must be considered. The MAGTF intelligence section, whether afloat or ashore, must have connectivity to all supporting external intelligence agencies. It is often necessary to augment subordinate intelligence sections to provide an enhanced capability to support the independent activities of their units. There are normally extensive contacts with organizations outside the US military command structure during MOOTW. Liaison and information exchange with non-DOD agencies and NGOs and multinational and/or host nation military and security forces must be anticipated.

Intelligence Cycle	Key Considerations
Planning and direction.	Decentralized direction. Need for muliple intelligence support nodes with specialized capabilities.
Collection.	Nonstandard requirements. Importance of HUMINT, CI, and nontraditional collection activities.
Processing, exploitation, and production.	Focus on infrastructure, political, economic, and sociological factors. Use of nonstandard production formats.
Dissemination.	Large number of independent units operating throughout the area. Intelligence exchange with joint, multinational, and nonmilitary units.
Utilization.	Need to monitor effectiveness and effect of ongoing operations. Support to force protection, civil affairs, PSYOP, and sustainability.

Figure 7-1. Intelligence Considerations in MOOTW.

Collection

Because MOOTW present nontraditional targets, collection operations must blend the capabilities and limitations of all available assets. Satisfaction of unique MOOTW requirements often requires the use of specialized capabilities or innovative approaches to the employment of standard assets.

During the planning and initial phases of the operation, national and theater assets will be relied on to satisfy basic requirements concerning entry points, infrastructure, and conventional

aspects of the threat. Because supporting intelligence agencies often have limited capabilities in MOOTW situations, organic assets are brought to bear as early as possible, including being employed as part of the advance party or lead element of the force. The nature of the MOOTW environment, threat, and requirements often present a lucrative opportunity for the conduct of HUMINT and CI collections operations. A MAGTF committed to a MOOTW must have a robust CI and HUMINT capability, augmented by appropriate area specialist and linguist support. This capability should be deployed as soon as practical to initiate force protection collection operations and establish necessary liaisons. The MAGTF must also exploit open sources and maintain contact with non-DOD government agencies and NGOs.

Processing, Exploitation, and Production

Intelligence production requirements in MOOTW are normally focused on nontraditional subject areas. For example, detailed knowledge of the host nation's economic, transportation, medical, and public works infrastructure will be required to develop plans for humanitarian assistance operations. Threat studies to support a peacekeeping mission must encompass an extensive treatment of political, cultural, and sociological factors related to various insurgent or paramilitary factions in addition to the threat's military capabilities. Use of area specialists and expertise from external intelligence organizations, non-DOD agencies (State Department, US Agency for International Development, etc.), and NGOs is crucial to satisfying these requirements. Production formats must be adapted to the requirements of a particular situation. Normal IPB analysis must be modified to highlight factors crucial to the specific MOOTW mission. Processing and production in MOOTW must be responsive to the needs of the numerous small elements that may be conducting independent activities throughout the AO. Production in support of these elements must be tailored to specific mission requirements and provide details pertinent to the small-unit level. Intelligence that increases the situational awareness of individual Marines, such as information on local customs, language, and health and sanitation, is an important part of this effort.

Dissemination

Dissemination during MOOTW must provide for the timely distribution of intelligence to a large number of elements that are widely dispersed throughout the AO. Creating intelligence support nodes for a specific area or region will aid the dissemination effort, but only if these nodes are equipped to receive all-source intelligence (in particular imagery and graphic products) from supporting collection and production agencies. Dissemination plans must also include provisions for the exchange of intelligence with other Service and multinational units participating in the operation, non-DOD agencies, and NGOs. Interoperability, sanitation, declassification, and releasability must all be considered and determined before such exchanges can occur.

Utilization

Intelligence shapes the planning and execution of MOOTW just as it does in other types of operations. During planning, intelligence helps determine the nature and scope of the operations and tasks required to accomplish the mission, the size and type of forces required, and the location and duration of the effort required. During execution, intelligence is used to enhance the effectiveness of ongoing operations, assess the results of completed activities, and identify follow-on missions and tasks that will help accomplish the overall objective. Emphasis is also placed on intelligence support of specialized functions that have enhanced importance during MOOTW: logistics, force protection, civil affairs, and PSYOP.

CHAPTER 8
JOINT OPERATIONS AND MULTINATIONAL OPERATIONS

A coordinated intelligence effort makes a critical contribution to the success of joint operations. MAGTFs participate in full partnership with other Services in joint operations. MAGTF intelligence operations are fully integrated with joint intelligence activities to ensure unity of effort, mutual support, and effective employment of limited intelligence resources.

Multinational operations are "military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance." (JP 1-02) MARFORs may participate in a wide variety of multinational operations, ranging from routine bilateral exercises to coalition warfare in major regional contingencies. Instances of unilateral US military operations are becoming less frequent, particularly in MOOTW. Marine units must be prepared to carry out intelligence operations in the context of multinational operations.

Effective intelligence support in joint operations depends on the following:

- Agreement on policies and procedures.
- Mutual intelligence support.
- Shared intelligence capabilities and assets.
- Full interoperability and connectivity among participants.
- Robust liaison.

JFC and Component Commander Responsibilities

JFCs are responsible for all aspects of intelligence support within their commands. They have the responsibility and authority to determine, direct, and coordinate all mission-related collection and analysis activities through centralized or apportioned collection and production management efforts. Component commanders remain responsible for the intelligence function within their commands and use organic intelligence capabilities to support their assigned missions. The JFC makes national, theater, and joint force intelligence assets available to support the efforts of the component commanders. At the same time, component capabilities must be available to assist the joint intelligence effort.

Joint Intelligence Structure

The JFC is assisted in carrying out intelligence responsibilities by the joint force J-2. The J-2 exercises many of the JFC's intelligence functions while acting as the senior intelligence officer in the joint force. Intelligence assets of the joint force headquarters are consolidated in a JISE. The combatant (theater) command is supported by a JIC, which is a standing intelligence element. A JISE is a temporary agency established to provide support to a particular JTF. The JISE provides intelligence support to the JFC and the entire joint force. Marine intelligence specialists will be assigned to the JISE to articulate Marine capabilities and requirements, influence decisions, and optimize intelligence support to the Marine component. Key functions performed by the JISE follow:

- Centralized collection, production, and dissemination management for joint force and supporting intelligence assets.
- All-source intelligence production to satisfy JFC and component requirements.
- Developing and maintaining data bases that support planning, operations, and targeting.

- Producing target studies and materials.
- Providing access to supporting national and theater intelligence assets.

Each theater establishes its own intelligence architecture, providing connectivity between the national- and theater-level intelligence organizations, the JTF, and its component commands. MARFOR and MAGTF intelligence architectures must be able to plug into the architectures of any theater where they might be employed.

Procedures

Joint intelligence activities are governed by joint intelligence doctrine contained in JP 2-0, *Joint Doctrine for Intelligence Support to Operations*, and supporting manuals in the 2-series of JPs. Joint intelligence doctrine is supplemented by combatant commanders' TTP for intelligence developed by each theater command. During joint operations, Marine intelligence activities will adhere to joint doctrine and any published theater TTP pertaining to that operation.

Marine Intelligence Section and Unit Responsibilities

- Operate in accordance with joint intelligence doctrine, theater TTP, and individual JTF procedures.
- Participate in joint intelligence mechanisms to coordinate collection management, intelligence production, HUMINT and SIGINT collection operations, target intelligence support, intelligence architectures, CI activities and collection operations, and other intelligence operations.
- Provide intelligence support to the joint force headquarters or other JTF components as directed.
- Contribute personnel and other assets to augment the J-2 section and JISE if requested.
- Employ joint or other component intelligence assets.
- Enter the JTF intelligence architecture.
- Exchange liaison elements with the J-2, JISE, and/or other JTF components as required.

MARFOR Component Headquarters or MAGTF CE as a JTF Headquarters

A Marine component headquarters or a MAGTF CE may be designated to provide the nucleus of a JTF headquarters.The MARFOR or MAGTF G-2 must be prepared to function as the JTF J-2, with the G-2's intelligence section serving as the base for establishing a JISE. To carry out this function, MARFOR and MEF G-2 sections must prepare plans for operating as a JTF J-2 and conduct the training to be able to execute these plans. Plans should be based on joint doctrine and theater TTP and should include J-2/JISE organization, personnel and equipment requirements (with their augmentation sources), a baseline intelligence architecture, and standing operating procedures. Each MARFOR and MEF G-2 section should establish a standing JTF intelligence planning cell made up of intelligence specialists who are knowledgeable in joint force and other Service intelligence capabilities, limitations, and operating procedures to develop these plans.

Multinational Operations

There is no single intelligence doctrine for multinational operations. Each coalition or alliance must develop its own doctrine. The coalition commander determines standardized procedures for coalition forces. NATO standardization agreements (STANAGs) and quadripartite standing agreements among US, British, Canadian, and Australian forces provide standards and guidance to conduct military operations by forces in these alliances. STANAG 2936, *Intelligence Doctrine*, governs intelligence operations. Joint intelligence doctrine and architectures provide a framework for developing the multinational intelligence support structure. Multinational intelligence operations are based on the following principles:

- Maintain unity of effort. Intelligence operations must be directed at the common threat. A threat to one alliance member should be considered a threat to all.
- Make adjustments. Effective multinational operations require minimizing the differences in national concepts of intelligence support. Commanders and their intelligence officers must be willing to make adjustments to national procedures to share intelligence and integrate intelligence operations. Special arrangements should be considered for developing, communicating, and using intelligence where there are differences in nations' language, culture, doctrine, terminology, organization, and equipment.
- Plan early and concurrently. Multinational forces' IRs and procedures should be identified, planned, coordinated, and exercised before execution.
- Share all necessary intelligence. Each coalition member should share intelligence that supports planning and execution. However, information about intelligence sources and methods should not be shared unless absolutely necessary. The methodology for exchanging intelligence should be developed and exercised before operations begin. Authorization for foreign disclosure should be obtained and procedures for sanitation and declassification should be developed as part of this planning process. During execution, the exchange must be monitored and adapted to ensure that it is meeting the needs of all coalition partners.
- Conduct complementary intelligence operations. Each nation's intelligence assets capitalize on their strengths and offset the weaknesses of other members' assets, providing the coalition with the most effective blend of capabilities.

Many potential allies may not possess the range of US intelligence capabilities; therefore, US intelligence sections must expect to take the lead in developing intelligence during multinational operations. Particular attention must be given to provisions for sanitation, declassification, and releasability of intelligence developed by US forces and agencies to coalition partners. Personnel who are knowledgeable in these techniques and procedures must be included in the MAGTF or Marine component intelligence section. Intelligence plans must provide for connectivity with multinational forces and liaison elements with appropriate linguistic and area specialist skills.

APPENDIX A
GLOSSARY

Section I. Acronyms

ACE . . . . . aviation combat element
AC/S . . . . . .assistant chief of staff
AFC. . . . . all-source fusion center
AFP . . . . . all-source fusion platoon
AIntP. . . . . Allied Intelligence Publication
AO. . . . . .area of operations
ATARS . . . . . advanced tactical airborne reconnaissance system
ATFIC. . . . . amphibious task force intelligence center

BDA . . . . . battle damage assessment

C2 . . . . . .command and control
C2W . . . . . command and control warfare
CCIR. . . . . commander's critical information requirements
CE . . . . . command element
CGS. . . . . common ground station
CHATS . . . . . CI/HUMINT automated tool set
CI . . . . . .counterintelligence
CIA . . . . . Central Intelligence Agency
CIC . . . . . combat intelligence center
CIS . . . . . communications and information systems
CMDO . . . . . collection management/ dissemination officer
Co . . . . . .company
COA . . . . . course of action
COG . . . . . .center of gravity
COP. . . . . common operational picture
CP . . . . . command post
CSS . . . . . combat service support
CSSE. . . . . .combat service support element
CTP. . . . . .common tactical picture
CV. . . . . .critical vulnerability

DIA . . . . . .Defense Intelligence Agency
DMS . . . . . .Defense Message System
DOD . . . . . Department of Defense
DST. . . . . .direct support team

EW . . . . . .electronic warfare
FBI . . . . . .Federal Bureau of Investigation
FRAGO. . . . . .fragmentary order
FSCC. . . . . .fire support coordination center
FSSG. . . . . force service support group

GCE . . . . . ground combat element
GI&S. . . . . .geospatial information and services
GSP. . . . . ground sensor platoon

HET. . . . . .HUMINT exploitation team
HLZ. . . . . helicopter landing zone
HUMINT . . . . . .human intelligence

I&W . . . . . .indications and warning
IAS . . . . . .intelligence analysis system
ICR . . . . . intelligence collection requirement
IDR . . . . . intelligence dissemination requirement
IIP . . . . . imagery intelligence platoon
IMA. . . . . individual mobilization augmentee
IMINT. . . . . .imagery intelligence
intel bn . . . . . intelligence battalion
IO . . . . . .information operations
IOC . . . . . .intelligence operations center
IOS . . . . . .intelligence operations server
IOW . . . . . .intelligence operations workstation
IPB . . . . . .intelligence preparation of the battlespace
IPR . . . . . intelligence production requirement
IR . . . . . .intelligence requirement
ISC . . . . . intelligence support coordinator

JIC. . . . . joint intelligence center
JISE. . . . . joint intelligence support element
JSTARS . . . . . .Joint Surveillance Target Attack Radar System
JTF . . . . . .joint task force
JWICS. . . . . .Joint Worldwide Intelligence Communication System

MAGTF . . . . . Marine air-ground task force

MARFOR . . . . . .Marine Corps forces
MARFORRES . . . . . Marine Forces Reserve
MASINT . . . . . measurement and signature intelligence
MAW . . . . . Marine aircraft wing
MCDP . . . . . Marine Corps doctrinal publication
MCIA . . . . . Marine Corps Intelligence Activity
MCWP . . . . . Marine Corps warfighting publication
MEB . . . . . .Marine Expeditionary Brigade
MEF . . . . . Marine Expeditionary Force
MEU . . . . . Marine Expeditionary Unit
MEU(SOC) . . . . . Marine Expeditionary Unit (Special Operations Capable)
MIDB . . . . . .modernized integrated database
MOOTW . . . . .military operations other than war
MSC . . . . . major subordinate command

NGO . . . . . .nongovernmental organization
NIMA . . National Imagery and Mapping Agency
NMITC . . . . . Navy-Marine Corps Intelligence Training Center
NIPRNET . . . . . Nonsecure Internet Protocol Router Network
NIST . . . . . National Intelligence Support Team
NSA . . . . . National Security Agency

OCAC . . . .operations control and analysis center
OIC . . . . . .officer in charge
OMFTS . . . . . operational maneuver from the sea
OODA . . . . . observe, orient, decide, and act
OP . . . . . .observation post
OPCON . . . . . .operational control
OPLAN . . . . . .operation plan
OPORD . . . . . operational order
OPSEC . . . . . .operations security
OSINT . . . . . open-source intelligence

P&A . . . . . production and analysis
PDE&A . . . . . planning, decision, execution, and assessment
PIR . . . . . priority intelligence requirements
PSYOP . . . . . psychological operations

R&S . . . . . reconaissance and surveillance
recon . . . . . reconaissance
rep . . . . . .representative
RRS . . . . . .remote receiver station

SARC . . . . . surveillance and reconnaissance cell
SIDS . . secondary imagery dissemination system
SIGINT . . . . . .signals intelligence
SIPRNET . . . . . Secret Internet Protocol Router Network
SSU . . . . . SIGINT support unit
STANAG . . . . . standardization agreement

TCAC . . . Technical Control and Analysis Center
TDN . . . . . tactical data network
TEG. . . . . Technical Exploitation Group
TERPES . . . . . tactical electronic reconnaissance processing and evaluation system
TGTINTEL . . . . . .target intelligence
TRAP . . . . . .tactical recovery of aircraft and personnel
TPC . . . . . topographic production capability
TRSS . . . . . .tactical remote sensor system
TTP . . . . . tactics, techniques, and procedures

UAV . . . . . .unmanned aerial vehicle
VMU . . . . . .Marine unmanned aerial vehicle squadron

Section II. Definitions

all-source intelligence—Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. (JP 1-02)

battle damage assessment—1. The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage

assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (JP 1-02) **2.** The timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCWP 2-1)

centers of gravity—1. Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. Also called COG. (JP 1-02) **2.** A key source of strength without which an enemy cannot function. (MCDP 1-2)

collection—The gathering of intelligence data and information to satisfy the identified requirements. (MCWP 2-1)

collection management—1. The process of converting intelligence requirements into collection requirements, establishing priorities, and tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required. (JP 1-02) **2.** Its purpose is to conduct an effective effort to collect all necessary data while ensuring the efficient use of limited and valuable collection assets. (MCWP 2-1)

combat data—Data derived from reporting by operational units. (MCWP 2-1)

command and control—1. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1-02) **2.** The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCDP 6) commander's critical information requirements—Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR. (MCRP 5-12C)

commander's intent—A commander's clear, concise personal articulation of the reason(s) behind one or more tasks assigned to a subordinate. It is one of two components of every mission statement which supports the higher and/or supported commander's intent and guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

counterintelligence—Within the Marine Corps, CI constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. Also called CI. (MCWP 2-1)

critical vulnerability—An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. Also called CV. (MCRP 5-12C)

descriptive intelligence—Class of intelligence which describes existing and previously existing conditions intended to promote situational awareness. Descriptive intelligence has two components: basic intelligence, which is general background knowledge about established and relatively constant conditions; and current intelligence, which is concerned with describing the existing situation. (MCRP 5-12C)

dissemination—Conveyance of intelligence to users in a suitable form. (JP 1-02)

dissemination management—Involves establishing dissemination priorities, selecting dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded by attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls that do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCWP 2-1)

estimative intelligence—Class of intelligence which attempts to anticipate future possibilities and probabilities based upon descriptive intelligence in the context of planned enemy and friendly operations. (MCRP 5-12C)

human intelligence—1. A category of intelligence derived from information collected and provided by human sources. (JP 1-02) **2.** HUMINT operations cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of CI force protection source operations. Also called HUMINT. (MCWP 2-1)

imagery intelligence—Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called IMINT. (JP 1-02)

indications and warning—Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (JP 1-02)

intelligence—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. **2.** Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02) **3.** Knowledge of the enemy and the surrounding environment that is needed to support decisionmaking. (MCDP 2)

intelligence cycle—The steps by which information is converted into intelligence and made available to users. (JP 1-02)

intelligence data—Data derived from assets primarily dedicated to intelligence collection: imagery systems, electronic intercept equipment, human intelligence sources, and so on. (MCWP 2-1)

intelligence discipline—A well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), and open-source intelligence. (JP 1-02)

intelligence operations—The variety of intelligence tasks that are carried out by various intelligence organizations and activities. (JP 1-02)

intelligence preparation of the battlespace—**1.** An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (JP 1-02) **2.** A systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCWP 2-1)

intelligence requirement—**1.** Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. Also called IR. (JP 1-02) **2.** Questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. (MCDP 2)

joint force—A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (JP 1-02)

joint intelligence center—The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (JP 1-02)

joint operations—A general term to describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces. (JP 1-02)

main effort—The designated subordinate unit whose mission at a given point in time is most critical to the overall mission success. (MCRP 5-12C)

maneuver warfare—A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. (MCDP 1)

measurement and signature intelligence—**1.** Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. Also called MASINT. (JP 1-02) **2.** Intelligence information gathered by technical instruments such as radars, passive electrooptical sensors, radiation detectors, and remote ground sensors. (MCWP 2-1)

open-source intelligence—**1.** Information of potential intelligence value that is available to the general public. Also called OSINT. (JP 1-02) **2.** OSINT sources include books, magazines, newspapers, maps, commercial electronic networks and databases, and radio and television broadcasts. OSINT involves no information that is classified at its origin or acquired through controlled collection. (MCWP 2-1)

priority intelligence requirements—**1.** Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called PIR. (JP 1-02) **2.** An intelligence requirement MCWP 2-1 Intelligence Operations A-5 associated with a

decision that will critically affect the overall success of the command's mission. (MCDP 2)

production management—Encompasses determining the scope, content, and format of each product; developing a plan and schedule for the development of each product; assigning priorities among the various IPRs; allocating processing, exploitation, and production resources; and integrating production efforts with collection and dissemination. (MCWP 2-1)

sensor data—Data derived from sensors whose primary mission is surveillance or target acquisition: air surveillance radars, counterbattery radars, and remote ground sensors. (MCWP 2-1)

signals intelligence—1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. **2.** Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT (JP 1-02)

situational awareness—Knowledge and understanding of the current situation which provides timely, relevant and accurate assessment of friendly, enemy and other operations within the battlespace. Also called SA. (MCRP 5-12C)

tactical intelligence—1. Intelligence that is required for planning and conducting tactical operations. (JP 1-02) **2.** Tactical intelligence concerns itself primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather. (MCDP 2)

warfighting functions—The six mutually supporting military activities integrated in the conduct of all military operations: command and control, intelligence, maneuver, fires, logistics, and force protection. (MCRP 5-12C)

APPENDIX B
REFERENCES

Standardization Agreement (STANAG)

2936	Intelligence Doctrine - AIntP-1(A)

Joint Publication (JP)

2-0	Joint Doctrine for Intelligence Support to Operations

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-0	Marine Corps Operations
2	Intelligence
5	Planning

Marine Corps Warfighting Publications (MCWPs)

2-14	Counterintelligence
5-1	Marine Corps Planning Process

FM 2-22.3 (FM 34-52)

HUMAN INTELLIGENCE COLLECTOR OPERATIONS

HEADQUARTERS, DEPARTMENT OF THE ARMY

September 2006

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

NOTE: All previous versions of this manual are obsolete. This document is identical in content to the version dated 6 September 2006. All previous versions of this manual should be destroyed in accordance with appropriate Army policies and regulations.

This publication is available at
Army Knowledge Online (www.us.army.mil) and
General Dennis J. Reimer Training and Doctrine
Digital Library at (www.train.army.mil).

Field Manual
No. 2-22.3

*FM 2-22.3 (FM 34-52)
Headquarters
Department of the Army
Washington, DC, 6 September 2006

Human Intelligence Collector Operations

Contents

		Page
	PREFACE	vi
PART ONE	**HUMINT SUPPORT, PLANNING, AND MANAGEMENT**	
Chapter 1	**INTRODUCTION**	1-1
	Intelligence Battlefield Operating System	1-1
	Intelligence Process	1-1
	Human Intelligence	1-4
	HUMINT Source	1-4
	HUMINT Collection and Related Activities	1-7
	Traits of a HUMINT Collector	1-10
	Required Areas of Knowledge	1-12
	Capabilities and Limitations	1-13
Chapter 2	**HUMAN INTELLIGENCE STRUCTURE**	2-1
	Organization and Structure	2-1
	HUMINT Control Organizations	2-2
	HUMINT Analysis and Production Organizations	2-6

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

NOTE: All previous versions of this manual are obsolete. This document is identical in content to the version dated 6 September 2006. All previous versions of this manual should be destroyed in accordance with appropriate Army policies and regulations.

*This publication supersedes FM 34-52, 28 September 1992, and ST 2-22.7, Tactical Human Intelligence and Counterintelligence Operations, April 2002.

Chapter 3 **HUMINT IN SUPPORT OF ARMY OPERATIONS** 3-1
Offensive Operations 3-1
Defensive Operations 3-2
Stability and Reconstruction Operations 3-3
Civil Support Operations 3-7
Military Operations in Urban Environment 3-8
HUMINT Collection Environments 3-8
EAC HUMINT 3-9
Joint, Combined, and DOD HUMINT Organizations 3-10

Chapter 4 **HUMINT OPERATIONS PLANNING AND MANAGEMENT** 4-1
HUMINT and the Operations Process 4-1
HUMINT Command and Control 4-3
Technical Control 4-4
Command and Support Relationships 4-4
HUMINT Requirements Management 4-5
HUMINT Mission Planning 4-15
Task Organization 4-18
Operational Considerations 4-19
Operations Plans, Operations Orders, and Annexes 4-21
Operational Coordination 4-22

PART TWO **HUMINT COLLECTION IN MILITARY SOURCE OPERATIONS**

Chapter 5 **HUMINT COLLECTION** 5-1
HUMINT Collection Operations 5-1
Human Source Contact Operations 5-2
Debriefing Operations 5-7
Liaison Operations 5-12
Interrogation Operations 5-13
Types of Interrogation Operations 5-27

PART THREE **THE HUMINT COLLECTION PROCESS**

Chapter 6 **SCREENING** 6-1
Human Source Screening 6-1
Screening Operations 6-2
Screening Process 6-9
Screening Methodologies 6-11
Screening Requirements 6-12

Initial Data and Observations 6-13
Source Assessment 6-14
Other Types of Screening Operations 6-15

Chapter 7 PLANNING AND PREPARATION 7-1
Collection Objectives 7-1
Research 7-1
HUMINT Collection Plan 7-8
Final Preparations 7-13

Chapter 8 APPROACH TECHNIQUES AND TERMINATION STRATEGIES 8-1
Approach Phase 8-1
Developing Rapport 8-3
Approach Techniques 8-6
Approach Strategies for Interrogation 8-20
Approach Strategies for Debriefing 8-21
Approach Strategies for Elicitation 8-22
Termination Phase 8-23

Chapter 9 QUESTIONING 9-1
General Questioning Principles 9-1
Direct Questions 9-1
Elicitation 9-5
Leads 9-5
Detecting Deceit 9-6
HUMINT Collection Aids 9-9
Recording Techniques 9-9
Questioning With an Analyst or a Technical Expert 9-11
Third-Party Official and Hearsay Information 9-12
Conducting Map Tracking 9-13
Special Source Categories 9-16

Chapter 10 REPORTING 10-1
Reporting Principles 10-1
Report Types 10-1
Reporting Architecture 10-5

Chapter 11 **HUMINT COLLECTION WITH AN INTERPRETER** 11-1
Advantages and Disadvantages of Interpreter Use 11-1
Methods of Interpreter Use 11-2
Sources of Interpreters 11-4
Interpretation Techniques 11-5
Training and Briefing the Interpreter 11-5
Placement of the Interpreter 11-6
Interactions With and Correction of the Interpreter 11-7
Interpreter Support in Report Writing 11-8
Evaluating the Interpreter 11-8
Managing an Interpreter Program 11-9

PART FOUR **ANALYSIS AND TOOLS**

Chapter 12 **HUMINT ANALYSIS AND PRODUCTION** 12-1
Analytical Support to Operational Planning 12-1
Operational Analysis and Assessment 12-3
Source Analysis 12-4
Single-Discipline HUMINT Analysis and Production 12-4
HUMINT Source Selection 12-19

Chapter 13 **AUTOMATION AND COMMUNICATION** 13-1
Automation 13-1
Collection Support Automation Requirements 13-2
Analytical Automation Requirements 13-3
Automation Systems 13-7
Communications 13-8

APPENDIX A **GENEVA CONVENTIONS** A-1
Section I. Geneva Conventions Relative to the Treatment of Prisoners of War (Third Geneva Convention) A-1
Section II. Geneva Conventions Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) A-47

APPENDIX B **SOURCE AND INFORMATION RELIABILITY MATRIX** B-1

APPENDIX C **PRE-DEPLOYMENT PLANNING** C-1

APPENDIX D **S2 GUIDE FOR HANDLING DETAINEES, CAPTURED ENEMY DOCUMENTS, AND CAPTURED ENEMY EQUIPMENT** D-1

APPENDIX E **EXTRACTS FROM ALLIED JOINT PUBLICATION (AJP)-2.5** E-1

APPENDIX F **NATO SYSTEM OF ALLOCATING INTERROGATION SERIAL NUMBERS** ... F-1

APPENDIX G **QUESTIONING QUICK REFERENCE** G-1

APPENDIX H **SALUTE REPORTING** H-1

APPENDIX I **DOCUMENT EXPLOITATION AND HANDLING** I-1

APPENDIX J **REFERENCES** J-1

APPENDIX K **CONTRACT INTERROGATORS** K-1

APPENDIX L **SAMPLE EQUIPMENT FOR HCT OPERATIONS** L-1

APPENDIX M **RESTRICTED INTERROGATION TECHNIQUE - SEPARATION** M-1

GLOSSARY Glossary-1

BIBLIOGRAPHY Bibliography-1

INDEX Index-1

Preface

This manual provides doctrinal guidance, techniques, and procedures governing the employment of human intelligence (HUMINT) collection and analytical assets in support of the commander's intelligence needs. It outlines—

- HUMINT operations.
- The HUMINT collector's role within the intelligence operating system.
- The roles and responsibilities of the HUMINT collectors and the roles of those providing the command, control, and technical support of HUMINT collection operations.

This manual expands upon the information contained in FM 2-0. It supersedes FM 34-52 and rescinds ST 2-22.7. It is consistent with doctrine in FM 3-0, FM 5-0, FM 6-0, and JP 2-0. In accordance with the Detainee Treatment Act of 2005, the only interrogation approaches and techniques that are authorized for use against any detainee, regardless of status or characterization, are those authorized and listed in this Field Manual. Some of the approaches and techniques authorized and listed in this Field Manual also require additional specified approval before implementation.

This manual will be reviewed annually and may be amended or updated from time to time to account for changes in doctrine, policy, or law, and to address lessons learned.

This manual provides the doctrinal guidance for HUMINT collectors and commanders and staffs of the MI organizations responsible for planning and executing HUMINT operations. This manual also serves as a reference for personnel developing doctrine, tactics, techniques, and procedures (TTP); materiel and force structure; institutional and unit training; and standing operating procedures (SOPs), for HUMINT operations at all army echelons. In accordance with TRADOC Regulation 25-36, the doctrine in this field manual is not policy (in and of itself), but is "…a body of thought on how Army forces operate….[It] provides an authoritative guide for leaders and soldiers, while allowing freedom to adapt to circumstances."

This manual applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the United States Army Reserve unless otherwise stated. This manual also applies to DOD civilian employees and contractors with responsibility to engage in HUMINT collection activities. It is also intended for commanders and staffs of joint and combined commands, and Service Component Commands (SCC). Although this is Army doctrine, adaptations will have to be made by other Military Departments, based on each of their organizations and specific doctrine.

Material in this manual applies to the full range of military operations. Principles outlined also are valid under conditions involving use of electronic warfare (EW) or nuclear, biological, or chemical (NBC) weapons.

This manual is intended for use by military, civilian, and civilian contractor HUMINT collectors, as well as commanders, staff officers, and military intelligence (MI) personnel charged with the responsibility of the HUMINT collection effort.

HUMINT operations vary depending on the source of the information. It is essential that all HUMINT collectors understand that, whereas operations and sources may

differ, the handling and treatment of sources must be accomplished in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including fragmentary orders (FRAGOs).

Interrogation, the HUMINT subdiscipline responsible for MI exploitation of enemy personnel and their documents to answer the supported specific information requirements (SIRs), requires the HUMINT collector to be fully familiar with both the classification of the source and applicable law. The principles and techniques of HUMINT collection are to be used within the constraints established by US law including the following:

- The Uniform Code of Military Justice (UCMJ).
- Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (including Common Article III), August 12, 1949; hereinafter referred to as GWS.
- Geneva Convention Relative to the Treatment of Prisoners of War (including Common Article III), August 12, 1949; hereinafter referred to as GPW.
- Geneva Convention Relative to the Protection of Civilian Persons in Time of War (including Common Article III), August 12, 1949; hereinafter referred to as GC.
- Detainee Treatment Act of 2005, Public Law No. 109-163, Title XIV.

HUMINT collectors must understand specific terms used to identify categories of personnel when referring to the principles and techniques of interrogation. Determination of a detainee's status may take a significant time and may not be completed until well after the time of capture. Therefore, there will be no difference in the treatment of a detainee of any status from the moment of capture until such a determination is made. The following terms are presented here and in the glossary.

- Civilian Internee: A person detained or interned in the United States or in occupied territory for security reasons, or for protection, or because he or she has committed an offense against the detaining power, and who is entitled to "protected person" status under the GC.
- Enemy Prisoner of War (EPW): A detained person, as defined in Articles 4 and 5 of the GPW. In particular, one who, while engaged in combat under orders of his or her government, is captured by the armed forces of the enemy. As such, he or she is entitled to the combatant's privilege of immunity from the municipal law of the capturing state for warlike acts that do not amount to breaches of the law of armed conflict. For example, an EPW may be, but is not limited to, any person belonging to one of the following categories of personnel who have fallen into the power of the enemy; a member of the armed forces, organized militia or volunteer corps; a person who accompanies the armed forces, without actually being a member thereof; a member of a merchant marine or civilian aircraft crew not qualifying for more favorable treatment; or individuals who, on the approach of the enemy, spontaneously take up arms to resist invading forces.
- Other Detainees: Persons in the custody of the US Armed Forces who have not been classified as an EPW (Article 4, GPW), retained personnel (Article 33, GPW), and Civilian Internee (Articles 27, 41, 48, and 78, GC) shall be treated as EPWs until a legal status is ascertained by competent authority; for example, by Article 5 Tribunal.
- Retained Personnel: (See Articles 24 and 26, GWS.)

  - Official medical personnel of the armed forces exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and staff exclusively engaged in the administration of medical units and facilities.
  - Chaplains attached to the armed forces.
  - Staff of National Red Cross Societies and that of other Volunteer Aid Societies, duly recognized and authorized by their governments to assist Medical Service personnel of their own armed forces, provided they are exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and provided that the staff of such societies are subject to military laws and regulations.

- Protected Persons: Include civilians entitled to protection under the GC, including those we retain in the course of a conflict, no matter what the reason.
- Enemy Combatant: In general, a person engaged in hostilities against the United States or its coalition partners during an armed conflict. The term "enemy combatant" includes both "lawful enemy combatants" and "unlawful enemy combatants." All captured or detained personnel, regardless of status, shall be treated humanely, and in accordance with the Detainee Treatment Act of 2005 and DOD Directive 2310.1E, "Department of Defense Detainee Program", and no person in the custody or under the control of DOD, regardless of nationality or physical location, shall be subject to torture or cruel, inhuman, or degrading treatment or punishment, in accordance with and as defined in US law.
  - **Lawful Enemy Combatant:** Lawful enemy combatants, who are entitled to protections under the Geneva Conventions, include members of the regular armed forces of a State Party to the conflict; militia, volunteer corps, and organized resistance movements belonging to a State Party to the conflict, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the laws of war; and members of regular armed forces who profess allegiance to a government or an authority not recognized by the detaining power.
  - **Unlawful Enemy Combatant:** Unlawful enemy combatants are persons not entitled to combatant immunity, who engage in acts against the United States or its coalition partners in violation of the laws and customs of war during an armed conflict. For the purposes of the war on terrorism, the term "unlawful enemy combatant" is defined to include, but is not limited to, an individual who is or was part of or supporting Taliban or al Qaeda forces, or associated forces that are engaged in hostilities against the United States or its coalition partners.

Headquarters, U.S. Army Training and Doctrine Command (TRADOC) is the proponent for this publication. The preparing agency is the US Army Intelligence Center and Fort Huachuca, Fort Huachuca, AZ. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, ATZS-CDI-D (FM 2-22.3), U.S. Army Intelligence Center and Fort Huachuca, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017. Send comments and recommendations by e-mail to ATZS-FDT-D@hua.army.mil. Follow the DA Form 2028 format or submit an electronic DA Form 2028.

Unless otherwise stated, masculine nouns and pronouns do not refer exclusively to men. Use of the terms "he" and "him" in this manual should be read as referring to both males and females unless otherwise expressly noted.

PART ONE

HUMINT Support, Planning, and Management

HUMINT collection activities include three general categories: screening, interrogation, and debriefing. In some cases these may be distinguished by legal distinctions between source categories such as between interrogation and debriefing. In others, the distinction is in the purpose of the questioning. Regardless of the type of activity, or goal of the collection effort, HUMINT collection operations must be characterized by effective support, planning, and management.

Chapter 1

Introduction

INTELLIGENCE BATTLEFIELD OPERATING SYSTEM

1-1. The Intelligence battlefield operating system (BOS) is one of seven operating systems—Intelligence, maneuver, fire support, air defense, mobility/countermobility/survivability, combat service support (CSS), and command and control—that enable commanders to build, employ, direct, and sustain combat power. The Intelligence BOS is a flexible force of Intelligence personnel, organizations, and equipment. Individually and collectively, these assets generate knowledge of and products portraying the enemy and the environmental features required by a command planning, preparing, executing, and assessing operations. Inherent within the Intelligence BOS is the capability to plan, direct, and synchronize intelligence, surveillance, and reconnaissance (ISR) operations; collect and process information; produce relevant intelligence; and disseminate intelligence and critical information in an understandable and presentable form to those who need it, when they need it. As one of the seven disciplines of the Intelligence BOS, HUMINT provides a capability to the supported commander in achieving information superiority on the battlefield.

INTELLIGENCE PROCESS

1-2. Intelligence operations consist of the functions that constitute the intelligence process: **plan, prepare, collect, process, produce**, and the common tasks of **analyze, disseminate,** and **assess** that occur throughout the intelligence process. Just as the activities of the operations process overlap and recur as circumstances demand, so do the functions of the intelligence process. Additionally, the analyze, disseminate, and assess tasks

of the intelligence process occur continuously throughout the intelligence process. (See Figure 1-1.)

- **Plan**. This step of the intelligence process consists of activities that include assessing the situation, envisioning a desired outcome (also known as setting the vision), identifying pertinent information and intelligence requirements, developing a strategy for ISR operations to satisfy those requirements, directing intelligence operations, and synchronizing the ISR effort. The commander's intent, planning guidance, and commander's critical information requirements (CCIRs) (priority information requirements [PIRs] and friendly force information requirements [FFIRs]) drive the planning of intelligence operations. Commanders must involve their supporting staff judge advocate (SJA) when planning intelligence operations (especially HUMINT operations). Planning, managing, and coordinating these operations are continuous activities necessary to obtain information and produce intelligence essential to decisionmaking.
- **Prepare**. This step includes those staff and leader activities that take place upon receiving the operations plan (OPLAN), operations order (OPORD), warning order (WARNO), or commander's intent to improve the unit's ability to execute tasks or missions and survive on the battlefield.
- **Collect.** Recent ISR doctrine necessitates that the entire staff, especially the G3/S3 and G2/S2, must change their reconnaissance and surveillance (R&S) mindset to conducting ISR. The staff must carefully focus ISR on the CCIR but also enable the quick re-tasking of units and assets as the situation changes. This doctrinal requirement ensures that the enemy situation, not just our OPLAN, "drives" ISR operations. Well-developed procedures and carefully planned flexibility to support emerging targets, changing requirements, and the need to support combat assessment are critical. The G3/S3 and G2/S2 play a critical role in this challenging task that is sometimes referred to as "fighting ISR" because it is so staff intensive during planning and execution (it is an operation within the operation). Elements of all units on the battlefield obtain information and data about enemy forces, activities, facilities, and resources as well as information concerning the environmental and geographical characteristics of a particular area.
- **Process.** This step converts relevant information into a form suitable for analysis, production, or immediate use by the commander. Processing also includes sorting through large amounts of collected information and intelligence (multidiscipline reports from the unit's ISR assets, lateral and higher echelon units and organizations, and non-MI elements in the battlespace). Processing identifies and exploits that information which is pertinent to the commander's intelligence requirements and facilitates situational understanding. Examples of processing include developing film, enhancing imagery, translating a document from a foreign language, converting electronic data into a standardized report that can be analyzed by a system operator, and

correlating dissimilar or jumbled information by assembling like elements before the information is forwarded for analysis.

- **Produce.** In this step, the G2/S2 integrates evaluated, analyzed, and interpreted information from single or multiple sources and disciplines into finished intelligence products. Like collection operations, the G2/S2 must ensure the unit's information processing and intelligence production are prioritized and synchronized to support answering the collection requirements.

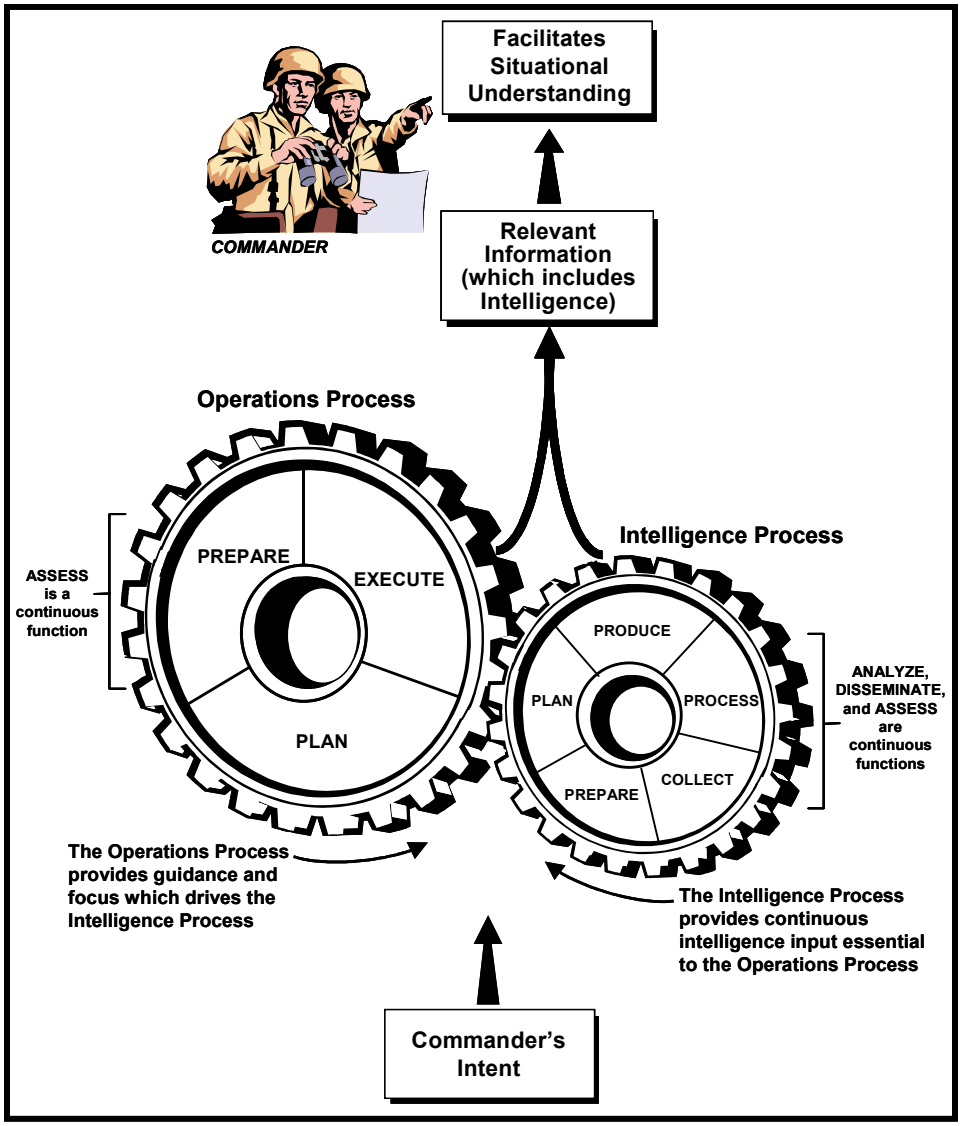


Figure 1-1. Intelligence Process.

1-3. For more information on the Intelligence process, see FM 2-0.

HUMAN INTELLIGENCE

1-4. HUMINT is the collection of information by a trained HUMINT collector (military occupational specialties [MOSs] 97E, 351Y [formerly 351C], 351M [formerly 351E], 35E, and 35F), from people and their associated documents and media sources to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool and a variety of collection methods, both passively and actively, to gather information to satisfy the commander's intelligence requirements and cross-cue other intelligence disciplines.

1-5. HUMINT tasks include but are not limited to—

- Conducting source operations.
- Liaising with host nation (HN) officials and allied counterparts.
- Eliciting information from select sources.
- Debriefing US and allied forces and civilian personnel including refugees, displaced persons (DPs), third-country nationals, and local inhabitants.
- Interrogating EPWs and other detainees.
- Initially exploiting documents, media, and materiel.

Note. In accordance with Army regulatory and policy guidance, a select set of intelligence personnel may be trained and certified to conduct certain HUMINT tasks outside of those which are standard for their primary MOS. Such selection and training will qualify these personnel to conduct only those specific additional tasks, and will not constitute qualifications as a HUMINT collector.

HUMINT SOURCE

1-6. A HUMINT source is a person from whom information can be obtained. The source may either possess first- or second-hand knowledge normally obtained through sight or hearing. Potential HUMINT sources include threat, neutral, and friendly military and civilian personnel. Categories of HUMINT sources include but are not limited to detainees, refugees, DPs, local inhabitants, friendly forces, and members of foreign governmental and non-governmental organizations (NGOs).

HUMINT COLLECTOR

1-7. For the purpose of this manual, a HUMINT collector is a person who is specifically trained and certified for, tasked with, and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. HUMINT collectors specifically include enlisted personnel in MOS 97E, Warrant Officers (WOs) in MOS 351M (351E) and MOS 351Y (351C), commissioned officers in MOS 35E and MOS 35F, select other specially trained MOSs, and their Federal civilian employee and civilian contractor counterparts. These specially trained and certified individuals are the **only** personnel authorized to conduct HUMINT collection operations, although CI agents also use HUMINT collection techniques in the conduct of CI operations. HUMINT

collection operations must be conducted in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Additional policies and regulations apply to management of contractors engaged in HUMINT collection. (See Bibliography for additional references on contractor management.) HUMINT collectors are not to be confused with CI agents, MOS 97B and WO MOS 351L (351B). CI agents are trained and certified for, tasked with, and carry out the mission of denying the enemy the ability to collect information on the activities and intentions of friendly forces. Although personnel in 97E and 97B MOSs may use similar methods to carry out their missions, commanders should not use them interchangeably. See Figure 1-2 for HUMINT and CI functions.

PHASES OF HUMINT COLLECTION

1-8. Every HUMINT questioning session, regardless of the methodology used or the type of operation, consists of five phases. The five phases of HUMINT collection are planning and preparation, approach, questioning, termination, and reporting. They are generally sequential; however, reporting may occur at any point within the process when critical information is obtained and the approach techniques used will be reinforced as required through the questioning and termination phases.

Planning and Preparation

1-9. During this phase, the HUMINT collector conducts the necessary research and operational planning in preparation for a specific collection effort with a specific source. Chapter 7 discusses this phase in detail.

Approach

1-10. During the approach phase, the HUMINT collector establishes the conditions of control and rapport to gain the cooperation of the source and to facilitate information collection. Chapter 8 discusses approach and termination strategies in detail.

Questioning

1-11. During the questioning phase, the HUMINT collector uses an interrogation, debriefing, or elicitation methodology to ask a source questions systematically on relevant topics, collect information in response to the intelligence tasking, and ascertain source veracity. Chapter 9 discusses questioning techniques in detail. (See Appendix B for a source and reliability matrix.)

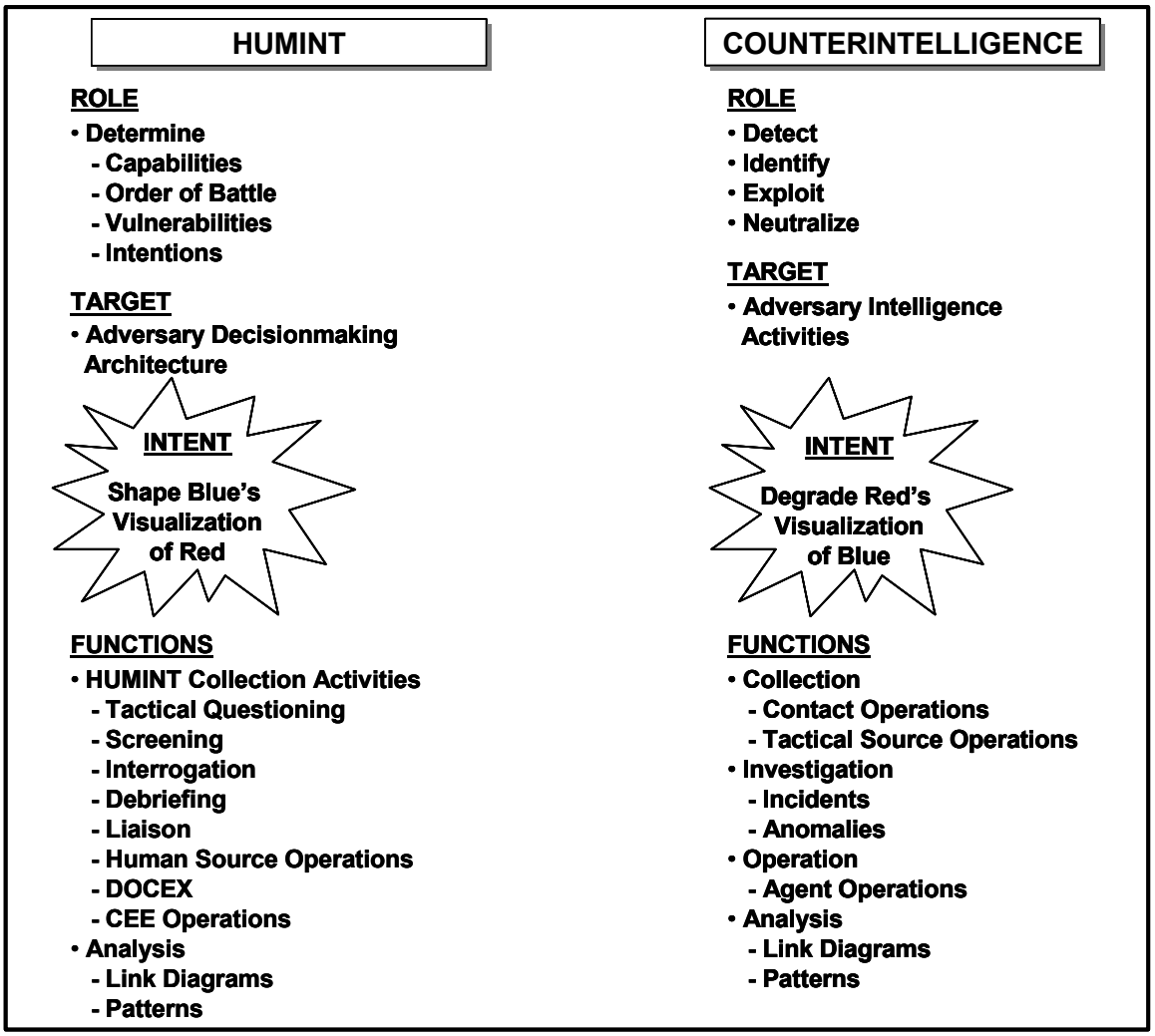


Figure 1-2. HUMINT and CI Functions.

Termination

1-12. During the termination phase, the HUMINT collector completes a questioning session and establishes the necessary conditions for future collection from the same source by himself or another HUMINT collector. (See Chapter 8.)

Reporting

1-13. During the reporting phase, the HUMINT collector writes, edits, and submits written, and possibly oral, reports on information collected in the course of a HUMINT collection effort. These reports will be reviewed, edited, and analyzed as they are forwarded through the appropriate channels. Chapter 10 discusses reporting in detail.

HUMINT COLLECTION AND RELATED ACTIVITIES

1-14. HUMINT collection activities include these categories: tactical questioning, screening, interrogation, debriefing, liaison, human source contact operations (SCOs), document exploitation (DOCEX), and captured enemy equipment (CEE) operations. DOCEX and CEE operations are activities supported by HUMINT collection but usually are only conducted by HUMINT collectors when the CEE or captured enemy document (CED) is associated with a source being questioned. In some cases, these determinations may depend on legal distinctions between collection methods such as interrogation and debriefing. In others, the distinction is in the purpose of the questioning. For example, screening is used to identify the knowledgeability and cooperation of a source, as opposed to the other activities that are used to collect information for intelligence purposes.

1-15. The activities may be conducted interactively. For example, a HUMINT collector may be screening a potential source. During the course of the screening, the HUMINT collector identifies that the individual has information that can answer requirements. He might at that point debrief or interrogate the source on that specific area. He will then return to screening the source to identify other potential areas of interest.

1-16. HUMINT collection activities vary depending on the source of the information. Once the type of activity has been determined, leaders use the process of plan, prepare, execute, and assess to conduct the activity. The following are the different types of HUMINT collection activities.

TACTICAL QUESTIONING

1-17. Tactical questioning is expedient initial questioning for information of immediate tactical value. Tactical questioning is generally performed by members of patrols, but can be done by any DOD personnel. (See ST 2-91.6.)

SCREENING

1-18. Screening is the process of identifying and assessing the areas of knowledge, cooperation, and possible approach techniques for an individual who has information of intelligence value. Indicators and discriminators used in screening can range from general appearance, possessions, and attitude to specific questions to assess areas of knowledge and degree of cooperation to establish if an individual matches a predetermined source profile. Screening is not in itself an intelligence collection technique but a timesaving measure that identifies those individuals most likely to have information of value.

1-19. Screening operations are conducted to identify the level of knowledge, level of cooperation, and the placement and access of a given source. Screening operations can also assist in the determination of which discipline or agency can best conduct the exploitation. Chapter 6 discusses screening in detail. Screening operations include but are not limited to—

- Mobile and static checkpoint screening, including screening of refugees and DPs.
- Locally employed personnel screening.

- Screening as part of a cordon and search operation.
- EPW and detainee screening.

INTERROGATION

1-20. Interrogation is the systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. Some examples of interrogation sources include EPWs and other detainees. Interrogation sources range from totally cooperative to highly antagonistic. Interrogations may be conducted at all echelons in all operational environments. Detainee interrogation operations conducted at a Military Police (MP) facility, coalition-operated facility, or other agency-operated collection facility are more robust and require greater planning, but have greater logistical support. Interrogations may only be conducted by personnel trained and certified in the interrogation methodology, including personnel in MOSs 97E, 351M (351E), or select others as may be approved by DOD policy. Interrogations are always to be conducted in accordance with the Law of War, regardless of the echelon or operational environment in which the HUMINT collector is operating.

DEBRIEFING

1-21. Debriefing is the process of questioning cooperating human sources to satisfy intelligence requirements, consistent with applicable law. The source usually is not in custody and usually is willing to cooperate. Debriefing may be conducted at all echelons and in all operational environments. The primary categories of sources for debriefing are refugees, émigrés, DPs, and local civilians; and friendly forces.

- **Refugees, Émigrés, DPs, and Local Civilians Debriefing Operations.** Refugee, émigré, and DP debriefing operations are the process of questioning cooperating refugees and émigrés to satisfy intelligence requirements. The refugee may or may not be in custody, and a refugee or émigré's willingness to cooperate need not be immediate or constant. Refugee debriefings are usually conducted at refugee collection points or checkpoints and may be conducted in coordination with civil affairs (CA) or MP operations. Local civilian debriefing operations are the process of questioning cooperating local civilians to satisfy intelligence requirements. As with refugees and émigrés, the local civilians being debriefed may or may not be in custody and the civilian's willingness to cooperate may not be immediate or constant. Debriefing operations must be conducted consistent with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.
- **Friendly Force Debriefing Operations.** Friendly force debriefing operations are the systematic debriefing of US forces to answer

collection requirements. These operations must be coordinated with US units. (See Chapter 6.)

LIAISON OPERATIONS

1-22. Liaison operations are programs to coordinate activities and exchange information with host country and allied military and civilian agencies and NGOs.

HUMAN SOURCE CONTACT OPERATIONS

1-23. Human SCO are operations directed toward the establishment of human sources who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. Within the Army, SCO are conducted by trained personnel under the direction of military commanders. The entire range of HUMINT collection operations can be employed. SCO sources include one-time contacts, continuous contacts, and formal contacts from debriefings, liaison, and contact operations. SCO consist of collection activities that utilize human sources to identify attitude, intentions, composition, strength, dispositions, tactics, equipment, target development, personnel, and capabilities of those elements that pose a potential or actual threat to US and coalition forces. SCO are also employed to develop local source or informant networks that provide early warning of imminent danger to US and coalition forces and contribute to the Military Decision-Making Process (MDMP). See Chapter 5 for discussion of approval, coordination, and review for each type of activity.

DOCEX OPERATIONS

1-24. DOCEX operations are the systematic extraction of information from open, closed, published, and electronic source documents. These documents may include documents or data inside electronic communications equipment, including computers, telephones, Personal Digital Assistants (PDAs), and Global Positioning System (GPS) terminals. This operation is not solely a HUMINT function, but may be conducted by any intelligence personnel with appropriate language support.

1-25. Many CEDs are associated with EPWs and other human sources. Consequently, a HUMINT collector is often the first person to screen them. HUMINT collectors will screen the documents associated with human sources and will extract information of use to them in their immediate collection operation. Any information discovered during this initial screening that might cross-cue another collection effort will be forwarded to the appropriate unit.

1-26. A captured document is usually something that the enemy has written for his own use. For this reason, captured documents are usually truthful and accurate. There are cases in which falsified documents have been permitted to fall into enemy hands as a means of deception but these cases are not the norm. Normal policy of not relying on single-source information should help prevent deceptions of this type from being effective. Documents also do not forget or misinterpret information although it must be remembered that their authors may have. Usually, each document provides a portion of a

larger body of information. Each captured document, much like a single piece of a puzzle, contributes to the whole. In addition to tactical intelligence, technical data and political indicators that are important to strategic and national level agencies can sometimes be extracted from captured documents. Captured documents, while not affected by memory loss, are often time sensitive; therefore, they are to be quickly screened for possible exploitation.

CEE OPERATIONS

1-27. CEE includes all types of foreign and non-foreign materiel found on a detainee or on the battlefield that may have a military application or answer a collection requirement. The capturing unit must—

- Recognize certain CEE as having immediate intelligence value, and immediately forward such CEE to the unit's S2. Such items include—
  - All electronic communications equipment with a memory card, including computers, telephones, PDAs, and GPS terminals.
  - All video or photographic equipment.
- Recognize certain CEE as having technical intelligence (TECHINT) value. Such items include—
  - New weapons.
  - All communications equipment not immediately exploitable for HUMINT value.
  - Track vehicles.
  - Equipment manuals.
  - All CEE known or believed to be of TECHINT interest.
- Evacuate the equipment with the detainee.
- Confiscate, tag, and evacuate weapons and other equipment found on the detainee the same as CEDs. (See Appendix D.)
- Secure and report the capture of TECHINT items to the unit's S2 for disposition instructions.

TRAITS OF A HUMINT COLLECTOR

1-28. HUMINT collection is a science and an art. Although many HUMINT collection skills may be taught, the development of a skilled HUMINT collector requires experience in dealing with people in all conditions and under all circumstances. Although there are many intangibles in the definition of a "good" HUMINT collector, certain character traits are invaluable:

- **Alertness.** The HUMINT collector must be alert on several levels while conducting HUMINT collection. He must concentrate on the information being provided by the source and be constantly evaluating the information for both value and veracity based on collection requirements, current intelligence, and other information obtained from the source. Simultaneously, he must be alert not only to what the source says but also to how it is said and the accompanying body language to assess the source's truthfulness, degree of cooperation, and current mood. He needs to know when to give the source a break and

when to press the source harder. In addition, the HUMINT collector constantly must be alert to his environment to ensure his personal security and that of his source.

- **Patience and Tact.** The HUMINT collector must have patience and tact in creating and maintaining rapport between himself and the source, thereby enhancing the success of the questioning. Displaying impatience may—
  - Encourage a difficult source to think that if he remains unresponsive for a little longer, the HUMINT collector will stop questioning.
  - Cause the source to lose respect for the HUMINT collector, thereby reducing the HUMINT collector's effectiveness.
- **Credibility.** The HUMINT collector must provide a clear, accurate, and professional product and an accurate assessment of his capabilities. He must be able to clearly articulate complex situations and concepts. The HUMINT collector must also maintain credibility with his source. He must present himself in a believable and consistent manner, and follow through on any promises made as well as never to promise what cannot be delivered.
- **Objectivity and Self-control.** The HUMINT collector must also be totally objective in evaluating the information obtained. The HUMINT collector must maintain an objective and dispassionate attitude regardless of the emotional reactions he may actually experience or simulate during a questioning session. Without objectivity, he may unconsciously distort the information acquired. He may also be unable to vary his questioning and approach techniques effectively. He must have exceptional self-control to avoid displays of genuine anger, irritation, sympathy, or weariness that may cause him to lose the initiative during questioning but be able to fake any of these emotions as necessary. He must not become emotionally involved with the source.
- **Adaptability.** A HUMINT collector must adapt to the many and varied personalities which he will encounter. He must also adapt to all types of locations, operational tempos, and operational environments. He should try to imagine himself in the source's position. By being adaptable, he can smoothly shift his questioning and approach techniques according to the operational environment and the personality of the source.
- **Perseverance.** A tenacity of purpose can be the difference between a HUMINT collector who is merely good and one who is superior. A HUMINT collector who becomes easily discouraged by opposition, non-cooperation, or other difficulties will not aggressively pursue the objective to a successful conclusion or exploit leads to other valuable information.
- **Appearance and Demeanor.** The HUMINT collector's personal appearance may greatly influence the conduct of any HUMINT collection operation and attitude of the source toward the HUMINT collector. Usually an organized and professional appearance will favorably influence the source. If the HUMINT collector's manner

reflects fairness, strength, and efficiency, the source may prove more cooperative and more receptive to questioning.

- **Initiative.** Achieving and maintaining the initiative are essential to a successful questioning session just as the offensive is the key to success in combat operations. The HUMINT collector must grasp the initiative and maintain it throughout all questioning phases. This does not mean he has to dominate the source physically; rather, it means that the HUMINT collector knows his requirements and continues to direct the collection toward those requirements.

REQUIRED AREAS OF KNOWLEDGE

1-29. The HUMINT collector must be knowledgeable in a variety of areas in order to question sources effectively. The collector must prepare himself for operations in a particular theater or area of intelligence responsibility (AOIR) by conducting research. The G2 can be a valuable source of information for this preparatory research. The HUMINT collector should consult with order of battle (OB) technicians and analysts and collect information from open sources and from the Secret Internet Protocol Router Network (SIPRNET) to enhance his knowledge of the AOIR. Some of these areas of required knowledge are—

- **The area of operations (AO)** including the social, political, and economic institutions; geography; history; language; and culture of the target area. Collectors must be aware of all ethnic, social, religious, political, criminal, tribal, and economic groups and the interrelationships between these groups.
- **All current and potential threat forces** within the AOIR and their organization, equipment, motivation, capabilities, limitations, and normal operational methodology.
- **Applicable law and policy that might affect HUMINT collection activities. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.** HUMINT collectors are subject to applicable law, which includes US law, the law of war (including the Geneva Conventions as applicable), and relevant international law. Additionally, local agreements with HNs or allies and the applicable execute orders and rules of engagement (ROE) may further restrict HUMINT collection activities. However, these documents cannot permit interrogation actions that would be illegal under applicable US or international law.
- **The collection requirements,** including all specific information requirements (SIRs) and indicators that will lead to the answering of the intelligence requirements.

- **Cultural awareness** in the various AOs will have different social and regional considerations that affect communications and can affect the conduct of operations. These may include social taboos, desired behaviors, customs, and courtesies. The staff must include this information in pre-deployment training at all levels to ensure that personnel are properly equipped to interact with the local populace.

1-30. There are other areas of knowledge that help to develop more effective questioning:

- **Proficiency in the target language**. The HUMINT collector can normally use an interpreter (see Chapter 11) and machine translation as they are developed to conduct questioning. Language proficiency is a benefit to the HUMINT collector in a number of ways: He can save time in questioning, be more aware of nuances in the language that might verify or deny truthfulness, and better control and evaluate interpreters.
- **Understanding basic human behavior**. A HUMINT collector can best adapt himself to the source's personality and control of the source's reactions when he understands basic behavioral factors, traits, attitudes, drives, motivations, and inhibitions. He must not only understand basic behavioral principles but also know how these principles are manifested in the area and culture in which he is operating.
- **Neurolinguistics**. Neurolinguistics is a behavioral communication model and a set of procedures that improve communication skills. The HUMINT collector should read and react to nonverbal communications. He must be aware of the specific neurolinguistic clues of the cultural framework in which he is operating.

CAPABILITIES AND LIMITATIONS

CAPABILITIES

1-31. HUMINT collection capabilities include the ability to—

- Collect information and cross-cue from an almost endless variety of potential sources including friendly forces, civilians, detainees, and source-related documents.
- Focus on the collection of detailed information not available by other means. This includes information on threat intentions and local civilian and threat force attitudes and morale. It also includes building interiors and facilities that cannot be collected on by other means due to restrictive terrain.
- Corroborate or refute information collected from other R&S assets.
- Operate with minimal equipment and deploy in all operational environments in support of offensive, defensive, stability and reconstruction operations, or civil support operations. Based on solid planning and preparation, HUMINT collection can provide timely information if deployed forward in support of maneuver elements.

LIMITATIONS

1-32. HUMINT collection limitations include—

- Interpersonal abilities. HUMINT is dependent on the subjective interpersonal capabilities of the individual rather than on the abilities to operate collection equipment. HUMINT collection capability is based on experience within a specific AO that can only be developed over time.
- Identification of knowledgeable sources. There is often a multitude of potential HUMINT sources. Information in response to specific requirements can only be collected if sources are available and identified that have that information.
- Limited numbers. There are never enough HUMINT collectors to meet all requirements. Limited assets must be prioritized in support of units and operations based on their criticality.
- Time limitations. HUMINT collection, particularly source operations, takes time to develop. Collection requirements must be developed with sufficient lead-time for collection.
- Language limitations. Although HUMINT collectors can normally use an interpreter, a lack of language proficiency by the collector can significantly slow collection efforts. Such language proficiency takes time to develop.
- Misunderstanding of the HUMINT mission. HUMINT collectors are frequently used incorrectly and assigned missions that belong to CA, MP, interpreter or translators, CI, or other operational specialties.
- Commanders' risk management. Maneuver commanders, in weighing the risks associated with employing HUMINT collection teams (HCTs), should seriously consider the potential loss of a wealth of information such as enemy activities, locations of high-value personnel, and threats to the force that they will incur if they restrict HCT collection activities. J/G2Xs, operational management teams (OMTs), and HCT leaders must educate maneuver commanders on the benefits of providing security for HCTs and employing them in accordance with their capabilities.
- Legal obligations. Applicable law and policy govern HUMINT collection operations. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. HUMINT operations may be further restricted by Status of Forces Agreements (SOFAs) and other agreements, execute orders and ROE, local laws, and an operational umbrella concept. Such documents, however, cannot permit interrogation actions that are illegal under applicable law.
- Connectivity and bandwidth requirements. With the exception of the size, activity, location, unit, time, equipment (SALUTE) report, most HUMINT reporting requires considerable bandwidth. Deployed

HUMINT teams must be able to travel to, and report from, all areas of the battlefield. Digital communication equipment must be able to provide reliable connectivity with teams' reporting channels and sufficient bandwidth for transmission of reports, including digital imagery.

- Timely reporting and immediate access to sources. Except in tactical situations when HUMINT collectors are in immediate support of maneuver units, HUMINT collection and reporting takes time. In stability and reconstruction operations, sources need to be assessed and developed. Once they are developed, they need to be contacted which often takes time and coordination. In offensive and defensive operations, HUMINT collection at detainee holding areas sometimes may still be timely enough to meet tactical and operational requirements. See paragraphs 3-2 and 3-7 for more information on offensive and defensive operations.

This page intentionally left blank.

Chapter 2

Human Intelligence Structure

ORGANIZATION AND STRUCTURE

2-1. The success of the HUMINT collection effort depends on a complex interrelationship between command and control (C2) elements, requirements, technical control and support, and collection assets. Each echelon of command has its supporting HUMINT elements although no MI organization in the Army is robust enough to conduct sustained HUMINT operations under all operational environments using only its organic HUMINT assets. HUMINT units have specific support requirements to the commander. HUMINT units must be flexible, versatile, and prepared to conduct HUMINT collection and analysis operations in support of any echelon of command. A coherent C2 structure within these HUMINT organizations is necessary in order to ensure successful, disciplined, and legal HUMINT operations. This structure must include experienced commissioned officers, warrant officers, and senior NCOs conscientiously discharging their responsibilities and providing HUMINT collectors with guidance from higher headquarters.

2-2. Regardless of the echelon, there are four basic elements that work together to provide the deployed commander with well-focused, thoroughly planned HUMINT support. The four elements are staff support, analysis, C2, and collection. Each piece of the infrastructure builds on the next and is based on the size, complexity, and type of operation as shown in Figure 2-1.

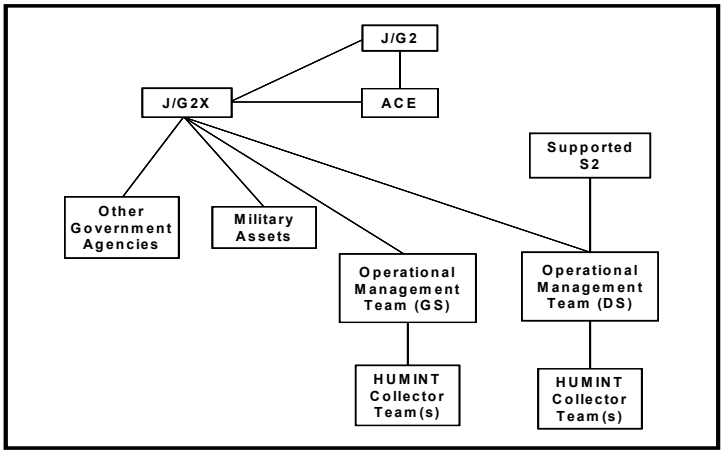


Figure 2-1. Tactical HUMINT Organization.

HUMINT CONTROL ORGANIZATIONS

2-3. HUMINT control organizations are the means by which a commander exercises command of a unit's operations. HUMINT control organizations are vital to the effective use of HUMINT collection assets. HUMINT control organizations consist of the C/J/G/S2X and the HUMINT operations cell (HOC) at the brigade and above level and the OMTs at the battalion and below level.

C/J/G/S2X

2-4. The C/J/G/S2X is a staff element subordinate to the C/J/G/S2, is the primary advisor on HUMINT and CI, and is the focal point for all HUMINT and CI activities within a joint task force (JTF) (J2X), an Army component task force (G2X) or a brigade combat team (BCT) (S2X). The 2X can be organic to the unit staff or can be attached or under operational control (OPCON) to the staff from another organization such as the theater MI brigade. The C/J/G/S2X is part of a coherent architecture that includes organic HUMINT assets and HUMINT resources from national, theater, and non-DOD HUMINT organizations.

2-5. The C/J2X is responsible for controlling Joint Force HUMINT assets, coordinating all HUMINT and CI collection activities, and keeping the joint force C/J/2 informed on all HUMINT and CI activities conducted in the joint force area of responsibility (AOR). The C/J2X is also part of the review and recommendation process concerned with the retention or release of detainees. HUMINT reports maintained at the C/J2X are considered during the review for release process. The C/J2X consists of the 2X Officer, a HOC, a Counterintelligence Coordination Authority (CICA), a HUMINT Analysis Cell (HAC), and a CI Analysis Cell (CIAC). At all echelons, the 2X should also include an Operational Support Cell (OSC) staffed to operate 24 hours a day. The authority and operational responsibilities of a C/J2X in combined or joint contingency operations (CONOP) takes precedence over service-specific CI and HUMINT technical control agencies. Specifically, the C/J/G/S2X—

- Accomplishes technical control and support, and deconfliction of all HUMINT and CI assets through the Army component G2X, the HUMINT and CI operations sections, or the OMTs.
- Participates in planning for deployment of HUMINT and CI assets in support of operations.
- Coordinates, through the HOC and the CICA, all HUMINT and CI activities to support intelligence collection and the intelligence aspects of force protection for the deployed commander.
- Coordinates and deconflicts all HUMINT and CI operations within the operational area.
- Coordinates with the senior US national intelligence representative for specific operational approval when required by standing agreements.
- Is the release authority for HUMINT reporting at his echelon and only releases reports to the all-source system after ensuring all technical control measures for reporting have been met.

- Coordinates with other HUMINT collection agencies not under the control of the command, such as Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), and Federal Bureau of Investigation (FBI).
- Does not exercise OPCON over HUMINT and CI assets assigned, attached, or reinforcing the unit; however, he is the staff support responsible for creating a cohesive HUMINT and CI effort.
- Coordinates with non-DOD agencies conducting HUMINT collection operations in the joint area of operations (JAO) to ensure deconfliction of sources, informants, or contacts and the HUMINT reporting that is generated by these collection operations.

2-6. The J2X will maintain technical control (see para 4-10) of all CI investigative actions within its AOIR; however, all investigative matters will be in accordance with DOD policies, joint or Military Department doctrine, applicable US law and policy, SOFAs, or other International Standardization Agreements (ISAs). The J2X will advise the responsible Theater CICA (TCICA) of any Army CI element conducting investigative activities that fall under the purview of AR 381-20.

OPERATIONS SUPPORT CELL (OSC)

2-7. The OSC in the C/J/G/S2X staff will maintain the consolidated source registry for all HUMINT and CI activities in the unit's designated AOIR. The OSC will provide management of intelligence property book operations, source incentive programs, and intelligence contingency funds (ICFs) for subordinate HUMINT and CI elements. The OSC responsibilities also include requests for information (RFIs) and/or source-directed requirements (SDRs) management and the release of intelligence information reports (IIRs).

COUNTERINTELLIGENCE COORDINATION AUTHORITY

2-8. The CICA is assigned under the J/G2X and coordinates all CI activities within its designated AOIR. (See FM 34-60 for a detailed explanation of the CI mission.) The CICA—

- Provides technical support to all CI assets and coordinates and deconflicts CI activities in the deployed AOIR.
- Coordinates and supervises CI investigations and collection activities conducted by all services and components in the AOIR.
- Establishes and maintains the theater CI source database.
- Coordinates with the HOC for CI support to detention, interrogation, refugee, and other facilities.
- Manages requirements and taskings for CI collectors in the AO in coordination with the HOC.
- Expedites preparation of CI reports and their distribution to consumers at all levels.
- Coordinates CI activities with senior CI officers from all CI organizations on the battlefield.

- Performs liaison with HN and US national level CI organizations.
- Informs the appropriate TCICA when Army CI elements are conducting CI investigative activities within the purview of AR 381-20.

HUMINT OPERATIONS CELL

2-9. The HOC is assigned under the J/G2X to track all HUMINT activities in the AOIR. The J/G2X uses this information to advise the senior intelligence officer (SIO) on all HUMINT activities conducted within the AOIR. The HOC—

- Provides technical support to all HUMINT collection operations and deconflicts HUMINT collection operations in the designated AOIR.
- Establishes and maintains a consolidated HUMINT source database in coordination with the CICA.
- Coordinates with collection managers and the HAC to identify collection requirements and to ensure requirements are met.
- Coordinates the activities of HUMINT collectors assigned or attached to interrogation, debriefing, refugee, DOCEX, and other facilities.
- Manages requirements and taskings for HUMINT collectors in the AOIR, in coordination with the CICA.
- Expedites preparation of intelligence reports and their distribution to consumers at all levels.
- Performs liaison with HN and US national HUMINT organizations.

OPERATIONAL MANAGEMENT TEAM

2-10. A HUMINT OMT consists of senior individuals in MOS 351M (351E) and MOS 97E. Each OMT can control 2 to 4 HCTs depending upon assigned mission and operational tempo (OPTEMPO). The OMT performs a necessary function when two or more HCTs deploy by assisting the HUMINT element commander in tasking and providing technical support to assigned or attached HCTs. The OMT is optimally collocated with the command post (CP) of the supported unit. However, it must be located where it can provide oversight of team operations and best support the dissemination of tasking, reports, and technical data between the unit and the deployed collection assets. When a higher echelon augments subordinate elements with collection teams, it should include proportional OMT augmentation. When a single collection team is attached in direct support (DS) of a subordinate element, the senior team member exerts mission and technical control over the team. The OMT—

- Provides operational and technical control and guidance to deployed HCTs.
- Normally consists of a WO and noncommissioned officers (NCOs) whose experience and knowledge provide the necessary guidance for effective team collection operations.
- Manages the use of ICFs and incentives for the HCTs.
- Provides the collection focus for HCTs.

- Provides quality control and dissemination of reports for subordinate HCTs.
- Directs the activities of subordinate HCTs and controls their operations.
- Conducts limited single-discipline HUMINT analysis and mission analysis for the supported commander.
- Acts as a conduit between subordinate HCTs, the HOC, and the C/J/G/S2X.
- Reports the HCT mission and equipment status to the HOC and the command element.

HUMINT COLLECTION TEAM

2-11. HCTs are the elements that collect information from human sources. The HUMINT collectors deploy in teams of approximately four personnel in MOS 97E (HUMINT Collector) and MOS 351M (351E) (HUMINT Technician).

2-12. The HCT may be augmented based on factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). Interpreters from the RC or civilian contractors with appropriate security clearances are added when necessary. TECHINT personnel or other specific subject-matter experts (SMEs) may augment the team to meet technical collection requirements. Another example would be pairing HUMINT collectors with dedicated analysts to provide sharper focus to the interrogation effort. In fixed detention facilities, these HUMINT collector or analyst relationships may become more enduring. Commanders are not encouraged to mix HUMINT collectors and CI agents on a single team. Doing so seriously undermines the ability to conduct both the HUMINT collection and CI missions simultaneously. However, commanders may find times when METT-TC factors make it reasonable to augment a CI team with HUMINT support for a mission, or vice versa.

COMMAND DEBRIEFING TEAM

2-13. A command debriefing team is normally not a table of organization and equipment (TOE) organization but may be task organized to meet mission requirements. This task-organized team is normally OPCON to the HOC. Although more prevalent during stability and reconstruction operations, senior personnel will often acquire information of intelligence interest during the normal course of their duties. The HUMINT collection assets, particularly at division echelon or higher, will normally task organize a team of more senior, experienced individuals to debrief these senior unit personnel. In offensive and defensive operations, this same team is prepared to interrogate high-value detainees (including EPWs) or debrief senior civilians. The command debriefing team should not be confused with the G2/S2 debriefing program, which also is critical and is an important conduit of information.

DOCUMENT EXPLOITATION TEAM

2-14. DOCEX teams are normally found at theater and national level organizations. Lower echelon HCTs may also be designated to perform the DOCEX mission based upon mission parameters and linguist availability. However, if organic assets are used, there will be a mission tradeoff. Dependent on the priority of exploitation and volume of documents, HCTs assigned the DOCEX mission may be augmented by military, civilian, or contractor personnel to accomplish their assigned mission. During operations, the DOCEX team will normally screen documents, extract information, and expedite the evacuation of documents to the Joint or Theater Document Exploitation Facility.

HUMINT ANALYSIS AND PRODUCTION ORGANIZATIONS

2-15. HUMINT analysis and production organizations analyze information collected from HUMINT sources, support the requirements management (RM) system, and produce single-discipline intelligence products. HUMINT analysis and production are conducted at all echelons, separate brigades, and higher. (See Chapter 12 for a description of the HUMINT analysis system and methodologies.)

HUMINT ANALYSIS CELL

2-16. The HAC is part of the J/G2X; however, it may be collocated with an analysis and control element (ACE) or Joint Intelligence Support Element (JISE) single-source enclave depending on facilities and operational environment considerations. The HAC works closely with the all-source intelligence elements and the CIAC to ensure that HUMINT reporting is incorporated into the all-source analysis and common operational picture (COP). The HAC is the "fusion point" for all HUMINT reporting and operational analysis in the JISE and ACE. It determines gaps in reporting and coordinates with the RM to cross-cue other intelligence sensor systems. The HAC—

- Produces and disseminates HUMINT products and provides input to intelligence summaries (INTSUMs).
- Uses analytical tools found at the ACE or JISE to develop long-term analyses and provides reporting feedback that supports the HOC, OMTs, and HCTs.
- Provides analytical expertise to the C/J/G/S2X, HOC, and OMTs.
- Produces country and regional studies tailored to HUMINT collection.
- Compiles target folders to assist C/J/G/S2X assets in focusing collection efforts.
- Analyzes and reports on trends and patterns found in HUMINT reporting.
- Analyzes source reliability and credibility as reflected in reporting and communicates that analysis to the collector.
- Develops and maintains databases specific to HUMINT collection activities.
- Produces HUMINT requirements.

- Answers HUMINT-related RFIs.
- Identifies collection gaps and provides context for better collection at their echelon.

JOINT INTERROGATION AND DEBRIEFING CENTER ANALYSIS SECTION

2-17. This section ensures that all members of the Joint Interrogation and Debriefing Center (JIDC) (see para 5-102) are aware of the current situation through the distribution of INTSUMs and products from external agencies. The Analysis Section also supports the JIDC by—

- Providing situation update briefings to all facility personnel every 12 hours.
- Preparing research and background packets and briefings for interrogations and debriefings.
- Developing indicators for each intelligence requirement to support screening operations.
- Conducting single-discipline HUMINT analysis based on collected information to support further collection efforts.
- Correlating reports produced by the JIDC to facilitate analysis at higher levels.
- Answering RFIs from interrogators and formulating RFIs that cannot be answered by the analytical section on behalf of the interrogators.
- Reviewing IIRs and extracting information into analysis tools tailored to support the interrogation process.
- Pursuing products and resources to support the interrogation effort.

HUMINT ANALYSIS TEAM

2-18. The HUMINT analysis team (HAT) is subordinate to the G2 ACE. The HAT supports the G2 in the development of IPB products and in developing and tailoring SIRs to match HUMINT collection capabilities.

This page intentionally left blank.

Chapter 3

HUMINT in Support of Army Operations

3-1. Army doctrine for full spectrum operations recognizes four types of military operations: offensive, defensive, stability and reconstruction, and civil support. Missions in any environment require the Army to conduct or be prepared to conduct any combination of these operations. HUMINT assets will be called on to provide information in support of all four operations. Simultaneous operations, for example elements of a force conducting offensive operations while other elements are engaged in stability and reconstruction operations, will cause a similar division of the limited HUMINT assets based on METT-TC.

OFFENSIVE OPERATIONS

3-2. Offensive operations aim at destroying or defeating the enemy. Rapid maneuver, constantly changing situations, and a vital need for intelligence support at the point of contact influence HUMINT missions during offensive operations. The guiding principle to the use of HUMINT in support of offensive operations is to minimize the time between when friendly forces encounter potential sources (detainees, refugees, and local civilians) and when a HUMINT collector screens them.

3-3. During offensive operations, at echelons corps and below, HCTs normally operate in the engaged maneuver brigades' AOs and are further deployed in support of maneuver battalions based on advice from the OMTs. These collection assets may be in general support (GS) of the parent brigade or in DS of the maneuver battalions, reconnaissance squadrons, and other forward-deployed maneuver assets. The HCTs and their supporting control structure are deployed in accordance with METT-TC based on three principles:

- The relative importance of that subordinate element's operations to the overall parent unit's scheme of maneuver and the overall ISR plan.
- The potential for that subordinate element to capture detainees, media and materiel, or to encounter civilians on the battlefield.
- The criticality of information that could be obtained from those sources to the success of the parent unit's overall OPLANs.

3-4. HUMINT missions in support of offensive operations include screening and interrogating EPWs and other detainees, questioning and debriefing civilians in the supported unit's AO, and conducting DOCEX, limited to extracting information of immediate tactical value. EAC assets normally support offensive operations through theater interrogation and debriefing facility operations and mobile interrogation teams. These facilities are better equipped to conduct in-depth interrogations and DOCEX, so it is imperative

that EPWs and other detainees who will be evacuated to theater facilities be transported there as soon as possible.

HUMINT IN SUPPORT OF FORCED ENTRY OPERATIONS

3-5. Forced entry operations (FEOs) are offensive operations conducted to establish an initial military presence in a target area in the face of expected enemy opposition. HUMINT collection assets may be able to provide vital information to tactical commanders in the critical early stages of the entry operation. Key considerations for HUMINT support to FEOs include:

- HUMINT collectors attached or under OPCON of the initial force package to provide HUMINT collection support for the entry force. Collection teams will normally operate in support of battalion-sized or smaller elements. HUMINT collection assets should be integrated early and should participate in all aspects of planning and training, including rehearsals, to smoothly integrate and execute operations.
- HUMINT assets supporting the entry force must include proportional OMT elements. For example, if 2 to 4 teams are attached to a maneuver brigade, an OMT also needs to be attached. Even if the teams are further attached to maneuver battalions, there must be an OMT at the brigade level to coordinate and control HUMINT collection activities.
- HCTs and OMTs must be as mobile and as survivable as the entry forces. Team leaders should ensure that the supported unit will be able to provide maintenance support to the team vehicles, as appropriate, in accordance with the support relationship.
- Attached or OPCON HUMINT teams must have robust communications connectivity with the supported unit and must have reach connectivity through their OMT.
- HCTs must contain organic or attached language capability in order to conduct HUMINT collection effectively during FEO. It is unlikely that the teams can be augmented with attached civilian interpreters during this type of operation.

HUMINT IN SUPPORT OF EARLY ENTRY OPERATIONS

3-6. Early entry operations differ from FEOs in that early entry operations do not anticipate large-scale armed opposition. Early entry operations establish or enhance US presence, stabilize the situation, and shape the environment for follow-on forces. HUMINT collection provides critical support to defining the operational environment and assessing the threat to US forces. The considerations listed above for FEOs apply equally to early entry operations.

DEFENSIVE OPERATIONS

3-7. Defensive operations defeat an enemy attack, buy time, economize forces, hold the enemy in one area while attacking in another, or develop conditions favorable for offensive operations. Forces conducting defensive

operations must be able to identify rapidly the enemy's main effort and rapidly assess the operational conditions to determine the timing of counter-offensive or other operations. HUMINT support to defensive operations centers on the ability to provide the forward-deployed maneuver commander with information and intelligence of immediate tactical value. HUMINT assets should be placed in the AO of the forward elements to minimize the time between when friendly forces encounter potential sources (detainees, refugees, local civilians) and when a HUMINT collector screens them. HUMINT collectors are placed where the potential for HUMINT collection and the criticality of the information are greatest.

3-8. In defensive operations, it may be necessary to divide the HUMINT assets equally among the subordinate elements to provide area coverage until the primary enemy threat is identified. The HUMINT C2 elements (team leader, OMTs, and unit C2) must be prepared to task organize rapidly and shift resources as the situation dictates, based on the changing situation and higher headquarters FRAGO. HUMINT missions in defensive operations normally include interrogation of detainees, refugee debriefings, and assisting in friendly force patrol debriefings.

STABILITY AND RECONSTRUCTION OPERATIONS

3-9. Stability and reconstruction operations sustain and exploit security and control over areas, populations, and resources. They employ military and civilian capabilities to help establish order that advances US interests and values. The immediate goal often is to provide the local populace with security, restore essential services, and meet humanitarian needs. The long-term goal is to help develop indigenous capacity for securing essential services, a viable market economy, rule of law, democratic institutions, and robust civil society. Stability and reconstruction operations involve both coercive and cooperative actions. They may occur before, during, and after offensive and defensive operations; however, they also occur separately, usually at the lower end of the range of military operations. The primary focus of the HCTs during stability and reconstruction operations is to answer the commander's information requirements (IRs) and provide support to force protection. In stability and reconstruction operations, the HUMINT collectors must be able to maintain daily contact with the local population. The nature of the threat in stability operations can range from conventional forces to terrorists and organized crime and civil disturbances. Consequently, intelligence requirements can vary greatly. Examples of HUMINT collection requirements include TECHINT to support arms control; extensive political information and demographic data; order of battle (OB) regarding several different former warring factions during peace operations; or extremely detailed target data. HUMINT collectors also help to ascertain the feelings, attitudes, and activities of the local populace. Stability and reconstruction operations may be conducted in coordination with other US departments and agencies, and in conjunction with other countries and international organizations.

3-10. Centralized management and databasing are key to successful HUMINT operations. The HUMINT assets may operate in GS to the parent unit or operate in the AO of subordinate elements of the parent unit. For

example, in a division AO, the HCTs would normally operate in DS to the division but each team would normally have an AOIR that corresponds to the AO of the division's brigades or battalion task forces. There is close coordination between the HUMINT staff officer (C/J/G/S2X) and the OMTs to synchronize HUMINT operations properly, to develop the overall threat awareness, and to deconflict sources. The HCTs screen and debrief contacts to increase the security posture of US forces, to provide information in response to command collection requirements, and to provide early warning of threats to US forces. They may also interrogate detainees if permitted to do so by the mission-specific orders and in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

3-11. Many stability and reconstruction operations are initiated with the establishment of a lodgment or base area. There is a subsequent expansion of operations to encompass the entire AO. The general concept of an HCT's operation is that of a two-phased effort. In the initial phase, the HCT establishes concentric rings of operations around the US forces starting from the supported unit's base of operations and working outward. Each ring is based on the threat environment and the commander's need to develop his knowledge of the tactical situation. The second, or continuation phase, begins once the initial information collection ring is established. The initial ring is not abandoned but rather is added to as the HCT shifts its focus to expand and establish the second and successive rings. The amount of time spent establishing each ring is situationally dependent.

INITIAL PHASE

3-12. The initial phase of stability and reconstruction operations is used to lay the foundation for future team operations. In general, the priority of effort is focused inward on security. The HCT conducts initial and follow-up screenings of locally employed personnel, to establish base data for subsequent source operations. The supported unit S2, with the assistance of the HUMINT team leader, establishes procedures to debrief reconnaissance and surveillance assets operating in the supported unit AO, as well as regular combat patrols or logistics convoys. The HCT lays the groundwork for future collection efforts by establishing liaison with local authorities, as well as developing plans and profiles for HUMINT collection. While establishing the initial and subsequent rings, the HCT actively seeks to collect PIR information, whether it pertains to the current ring or any other geographic location.

CONTINUATION PHASE

3-13. Following the initial phase, the HCT's focus shifts outward. While the HCT continues performing HUMINT collection and analysis functions within the base camp, it also expands its collection effort to outside the base camp to answer the supported unit's requirements. During the continuation phase, the HCT conducts contact operations with local personnel who may be able to

provide information of interest to the local commander or to satisfy the requirements of the tasking or request. The HCT also conducts liaison with local authorities, coalition forces (if present), NGOs, and others whose knowledge or activities may affect the success of the US mission. Any time the HCT is outside the base camp, it must be careful to observe the local population and report what it sees. The activities and attitudes of the general population will often have an effect on the commander's decisions on how to conduct US missions in the area.

LEVELS OF EMPLOYMENT

3-14. HCTs may be employed with varying degrees of contact with the local population. As the degree of contact with the population increases, the quantity and diversity of HUMINT collection increases. In many instances, however, there is a risk to the HCT inherent with increased exposure to the local population. The ability of the HCT members to fit in with the local populace can become very important to their safety. Consequently, the commander should consider exceptions to the ROE, as well as relaxed grooming and uniform standards, to help HCT members blend in and provide additional security. Commanders must consider the culture in which the HCT members will be operating. In some cultures, bearded men are more highly respected than clean-shaven men. Relaxing grooming standards for HCTs in these situations will support the team's ability to collect information. The decision regarding what level to employ an HCT is METT-TC dependent. The risk to the collection assets must be balanced with the need to collect information and to protect the force as a whole. The deployment and use of HUMINT collection assets may be limited by legal restrictions, mission-specific orders, directions from higher headquarters, and the overall threat level. The four basic levels of employment for the HCT are discussed below. Figure 3-1 shows these levels as well as their collection potential versus team security.

Base Camp

- Restricting the HCT to operations within the base camp minimizes the risk to the team. This action, however, minimizes the collection potential and maximizes the risk to the force as a whole. While restricted to a base camp, the HCT can maintain an extremely limited level of information collection by—
  - Interviewing walk-in sources and locally employed personnel.
  - Debriefing combat and ISR patrols.
  - Conducting limited local open-source information collection.
- This mode of deployment should be used only when dictated by operational restrictions. These would be at the initial stages of stability and reconstruction operations when the operational environment is being assessed, or as a temporary expedient when the force protection level exceeds the ability to provide reasonable protection for the collectors. A supported unit commander is often tempted to keep the HCT "inside the wire" when the force protection level or threat

condition (THREATCON) level increases. The supported unit and parent commanders must compare the gains of the HCT collection effort with the risks posed. This is necessary especially during high THREATCON levels when the supported unit commander needs as complete a picture as possible of the threat arrayed against US or multinational forces.

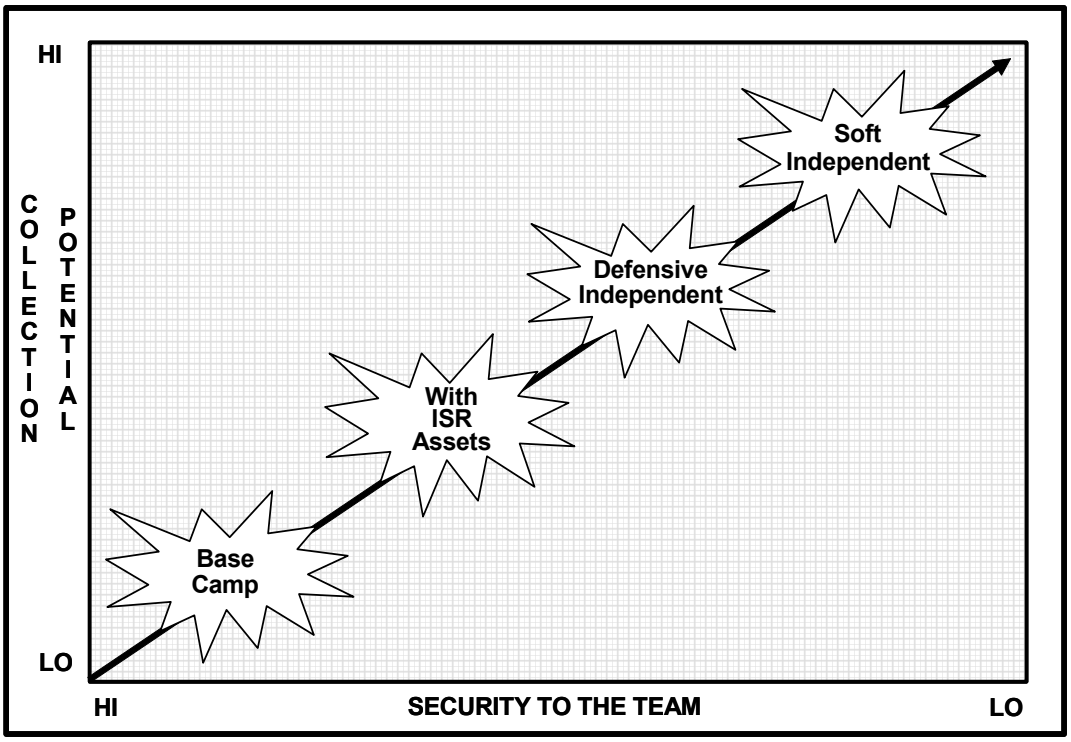


Figure 3-1. Team Level of Employment.

Integrated with Other Operations

- Under some circumstances, when it is not expedient to deploy the HCT independently due to threat levels or other restrictions, it can be integrated into other ongoing operations. The HCT may be employed as part of a combat patrol, ISR patrol, or in support of an MP patrol or stationed at a checkpoint or roadblock. It can also be used to support CA, psychological operations (PSYOP), engineer, or other operations. This method reduces the risk to the team while greatly increasing its collection potential over the confined-to-base-camp method. It has the advantage of placing the team in contact with the local population and allowing it to spot, assess, and interact with potential sources of information.
- The integration into other operations can also facilitate the elicitation of information. However, this deployment method restricts collection by subordinating the team's efforts to the requirements, locations, and timetables of the unit or operation into which it is integrated. Integration can be done at the team or individual collector level. HUMINT collectors should be used only in situations with an

intelligence collection potential. It is a waste of a valuable asset to use them in a function that could be performed by a civilian translator.

As an Independent Patrol

- Defensive. One of the key elements of the HCT success is the opportunity to spot, assess, and develop relationships with potential sources of information. Operating as independent patrols, without being tied to ISR or combat assets, enables the HCTs maximum interaction with the local population, thereby maximizing the pool of potential sources of information. The HCT must be integrated into the supported unit's ISR plan and be provided with other command elements as needed to support the collection mission. The team leader will advise the supported unit on the specific capabilities and requirements of the team to maximize mission success. This method also increases the risk to the team. HCT members must carry the necessary firepower for self-protection. They must also have adequate communications equipment to call for help if needed. The team's posture, equipment, and appearance will be dictated by overall force restrictions and posture. When operating as an independent patrol, the HCT should not stand out from overall US forces operations. If US forces are in battle-dress uniforms and operating out of military vehicles, so should the HUMINT collectors.
- Soft. If the threat situation is such that soldiers are authorized to wear civilian clothes when outside base areas, the HUMINT collectors should also move among the civilian population in civilian clothes, so that they do not stand out from others in the area.

CIVIL SUPPORT OPERATIONS

3-15. Army support supplements the efforts and resources of state and local governments and organizations. If a presidential declaration initiates civil support for a major disaster or emergency, involvement of DOD intelligence components would be by exception. Civil support requires extensive coordination and liaison among many organizations—interagency, joint, AC, and RC—as well as with state and local governments, and in any case will require compliance with the Posse Comitatus Act, 18 U.S.C., § 1385, when US forces are employed to assist Federal, state, or local law enforcement agencies (LEAs). The National Response Plan provides a national level architecture to coordinate the actions of all supporting agencies.

MILITARY OPERATIONS IN URBAN ENVIRONMENT

3-16. Units are often task organized with additional ISR units and assets to meet the detailed collection requirements in the urban operations. The complexities of urban terrain cause degradation in the capabilities of many of the sensor systems. HUMINT collectors may have to be placed in DS of lower echelon combat maneuver forces (battalion and lower) to support operations. HUMINT and combat reporting by units in direct contact with threat forces and local inhabitants becomes the means of collection. For successful ISR

planning, the S2 must be aware of the capabilities and limitations of the various organic and attached collection systems as they apply to urban operations. As in all environments, commanders must assess the risk involved in the forward deployment of HUMINT assets.

3-17. In urban operations, people (for example, detainees and civilians) are the preeminent source of information. HUMINT collection provides information not otherwise available through signals intelligence (SIGINT) and imagery intelligence (IMINT) such as threat and local population intentions. They collect information on, for example, floor plans, defensive plans, locations of combatants and noncombatants, including civilians in the buildings and surrounding neighborhoods, and other information. The collected information is passed directly to the individuals conducting the combat operation.

3-18. In small-scale contingencies (SSCs) and in peacetime military engagements (PMEs), contact with local officials and populace by the HUMINT collectors can be a prime source of information about the local environment and is a vital component of intelligence support to force protection. During routine patrolling of urban areas it is often expedient to place a HUMINT collector with individual patrols. The key difference between urban and other operations, from major theater war (MTW) to PME, is the number of HUMINT collectors required. The need for HUMINT collectors is a function of population density. Whereas in a rural environment, a HUMINT team may be able to cover an area in excess of 1,200 square kilometers; the same team in a dense urban environment may be able to cover only 10 square blocks or less.

HUMINT COLLECTION ENVIRONMENTS

HUMINT COLLECTION IN A PERMISSIVE ENVIRONMENT

3-19. In a permissive environment, HCTs normally travel throughout their specific AOR as separate teams or as part of a larger reconnaissance team. HUMINT collectors may frequently make direct contact with the individual, view the activity, or visit the area that is the subject of the ISR effort. They normally use debriefing and elicitation to obtain first-hand information from local civilians and officials as their primary collection techniques. Additional information can be obtained from exploitation of open-source material such as newspapers, television, and other media. The priority requirements in this environment are normally linked to force protection. HCTs should establish liaison and casual source contacts throughout their AOIR. Reporting is normally via IIRs, although SALUTE reports are used for critical time-sensitive reporting. Even in a permissive environment, the HUMINT collector conducts the majority of his collection through the debriefing of individuals who have first-hand knowledge of the information they are reporting.

HUMINT COLLECTION IN A SEMI-PERMISSIVE ENVIRONMENT

3-20. In a semi-permissive environment, security considerations increase, but the risk to the collector still must be weighed against the potential intelligence gain. HCTs should still be used throughout their AOIR but will normally be integrated into other ground reconnaissance operations or other planned operations. For example, a HUMINT collector may accompany a CA team or PSYOP team visiting a village. Security for the team and their sources is a prime consideration. The HCTs are careful not to establish a fixed pattern of activity and arrange contacts in a manner that could compromise the source or the collector. Debriefing and elicitation are still the primary collection techniques. Teams are frequently deployed to conduct collection at roadblocks, refugee collection points, and detainee collection points. They may conduct interrogations of EPWs and other detainees within the limits of the mission-specific orders, and applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. DOCEX is also used to accomplish exploitation of threat documents. Reporting is normally via SALUTE report and IIR.

HUMINT COLLECTION IN A HOSTILE ENVIRONMENT

3-21. In a hostile environment, the three concerns for HUMINT collection are access to the sources of information, timeliness of reporting, and security for the HUMINT collectors. Prior to the entry of a force into a hostile AO, HUMINT collectors are used to debrief civilians, particularly refugees, and to interrogate EPWs and other detainees who have been in the AO. HCTs are normally located with the friendly units on the peripheries of the AO to facilitate timely collection and reporting. If a refugee or EPW/detainee population exists prior to this mission, they are screened to determine knowledgability of the AO and are debriefed or interrogated as appropriate. HUMINT collectors accompany the friendly ground reconnaissance elements as they enter the AO. As part of the ground reconnaissance force, they interrogate EPWs and other detainees and debrief refugees, displaced persons, and friendly force patrols. Reporting is normally via oral or written SALUTE reports with more detailed information reported via IIRs. They may also support the S2 through the systematic debriefing of friendly ground reconnaissance assets and the translation of any documents collected by them.

EAC HUMINT

MI BRIGADES AND MI GROUPS SUPPORTING COMPONENT COMMANDS

3-22. Each SCC with an outside continental United States (OCONUS) responsibility has an US Army Intelligence and Security Command (INSCOM) MI brigade or group to provide operational HUMINT support to that command. These MI elements provide peacetime support to the unified

command and add a consistent, forward-deployed presence in a particular theater of operations. Theater MI brigade and group assets provide HUMINT support during contingency operations. These HCTs can support a JTF, an army combatant command, or any deployed element that requires augmentation.

JOINT, COMBINED, AND DOD HUMINT ORGANIZATIONS

3-23. The Departments of the Air Force and the Navy have limited HUMINT collection capability. They will normally provide strategic debriefing trained and certified personnel to joint interrogation and debriefing facilities primarily to collect information on areas of particular interest to that Military Department. Within the Department of the Navy, however, the US Marine Corps has a robust tactical HUMINT collection capability that operates primarily in support of engaged Marine Corps forces. Marine expeditionary elements deploy with human exploitation teams (HETs) that provide organic HUMINT and CI support to the deployed Marine force. Marine HETs are rapidly deployable and fully equipped to conduct the full range of tactical HUMINT and CI functions. They can provide support to either the deployed Marine force or as part of JTF HUMINT or CI teams. Each Marine Expeditionary Force (MEF) has organic HETs. HETs can also be attached to a Marine Air-Ground Task Force (MAGTF) for a particular operation.

SUPPORT AGENCIES

3-24. HUMINT agencies from DOD, national level intelligence agencies, and LEAs can support the battlefield commander. In a JTF, a national intelligence support team (NIST) works with the J2X to coordinate national level activities with JTF and component HUMINT and analytical assets. Sometimes liaison officers (LNOs) are assigned directly to the C/J/2X to facilitate collection activities.

- **Defense Intelligence Agency (DIA).** The DIA is a DOD combat support (CS) agency and an important member of the United States Intelligence Community. With more than 7,000 military and civilian employees worldwide, DIA is a major producer and manager of foreign military intelligence. DIA provides military intelligence to warfighters, defense policymakers and force planners in DOD and the Intelligence Community in support of US military planning and operations and weapon systems acquisition.
  - **Defense HUMINT (DH) Service.** The DH Service, a branch of the DIA, is the force provider for strategic HUMINT forces and capabilities. During operations, elements from DH form a partnership within the supported JTF headquarters J2X element for the coordination and deconfliction of HUMINT source-related collection activities. DH support to a joint force is outlined in the classified DIAM 58-11 and DIAM 58-12.
- **Central Intelligence Agency (CIA).** The CIA supports US national security policy by providing accurate, evidence-based, comprehensive, and timely foreign intelligence related to national security. The CIA

conducts CI activities, HUMINT collection, special activities, and other functions related to foreign intelligence and national security as directed by the President. Joint Pub 2-01.2 (S//NF) contains details of CIA contributions to the deployed force.

- **Department of State.** The State Department's Bureau of Diplomatic Security provides CI support to diplomatic missions worldwide and gathers extensive information on intelligence capabilities of adversaries within that diplomatic mission's area of concern. The Bureau of Intelligence and Research is the State Department's primary source for interpretive analysis of global developments. It is also the focal point in the State Department for all policy issues and activities involving the Intelligence Community.
- **National Security Agency (NSA).** The NSA is a DOD agency that coordinates, directs, and performs highly specialized activities to protect US information systems and produce foreign intelligence information. It is also one of the most important centers of foreign language analysis and research within the Government.
- **Defense Criminal Investigative Service (DCIS).** The DCIS is the criminal investigative arm of the Inspector General (IG) of DOD. The DCIS's mission is to protect America's warfighters by initiating, conducting, and supervising investigations in support of crucial National Defense priorities.
- **Department of Justice**:
  - Federal Bureau of Investigation. The FBI may provide the deployed commander with national level expertise on criminal and CI issues if currently operating in a task force (TF) AO and liaison is established early.
  - Drug Enforcement Agency (DEA). The DEA provides counterdrug operational expertise to a deployed TF and coordinates its operations with those of a deployed TF.
- **Department of Homeland Security (DHS).** The DHS mission is to prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, protect the homeland, its citizens, and critical infrastructure and key resources against terrorist attack. DHS provides a lead for Federal incident response, management, and recovery in the event of terrorist attack and natural disasters. The Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. DHS operates the Homeland Security Operations Center (HSOC) and the DHS-led Interagency Incident Management Group (IIMG). The DHS AOR is the US and its territories. DHS secures and protects the entry points to the nation, the areas between the entry points, land and water, for people, and cargo or conveyances. DHS enforces immigration, customs, and transportation security laws and

regulations, counter-narcotics, counterfeiting, financial crimes, and threats to the President. As legislated in the Homeland Security Act of 2002, DHS is chartered as the primary outreach Federal activity for state, local, and tribal governments, and the private sector. Although DHS has no direct role in support of a "battlefield commander" outside the United States, DHS component organizations have representatives deployed in support of US Government missions in the US Central Command (USCENTCOM) AOR.

- **Department of Energy (DOE).** The DOE can assist with the—
  - Exploitation of weapons of mass destruction (WMD).
  - Protection or elimination of weapons and weapons-useable (dual-use) nuclear material or infrastructure.
  - Redirection of excess foreign weapons expertise to civilian enterprises.
  - Prevention and reversal of the proliferation of WMD.
  - Reduction of the risk of accidents in nuclear fuel cycle facilities worldwide.
  - The capability enhancement of WMD detection including nuclear, biological, and chemical (NBC).
- **National Geospatial Intelligence Agency (NGA).** The NGA is a member of the US Intelligence Community and a DOD Combat Support Agency. NGA provides timely, relevant, and accurate geospatial intelligence in support of national security objectives. Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth.
- **Counterintelligence Field Agency (CIFA).** The mission of CIFA is to develop and manage DOD CI programs and functions that support the protection of the Department. These programs and functions include CI support to protect DOD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and US interests against foreign influence and manipulation, as well as to detect and neutralize espionage against the Department.

3-25. Most potential coalition partners have some type of HUMINT capability. Less developed nations may use HUMINT as their primary collection system and may be quite skilled in HUMINT operations. These assets will be present on the battlefield, and US assets are likely to work with them. HCTs should perform regular liaison with coalition HUMINT personnel. It is likely that some coalition partners will be more knowledgeable of the culture in the AO and be able to share insights with US HCTs.

Chapter 4

HUMINT Operations Planning and Management

4-1. HUMINT operations planning and management are supported by a robust structure that includes staff elements such as the C2X when working with non-US forces at the Joint intelligence staff level, G2X at the Division, Corps intelligence staff, the HUMINT operations section in the MI Battalion, and HAT in the Division and Corps ACE. It also includes C2 elements at the MI battalion, company, platoon, and team levels. The OMT provides the first level of staff and C2 functions when two or more HCTs deploy in support of an operation. (See Table 4-1.)

Table 4-1. HUMINT Operations.

ECHELON	ISR PLANNING	TECHNICAL SUPPORT AND DECONFLICTION	MISSION EXECUTION
COMBINED	C2/ACE	C2X/OMT	MI CDR
JOINT	J2/ACE	J2X/OMT	MI CDR (AMIB or MI Battalion)
CORPS/DIVISION	G2/ACE	G2X/OMT	MI CDR/OMT
BRIGADE	S2	MI CDR/OMT	MI CDR/OMT

HUMINT AND THE OPERATIONS PROCESS

4-2. Following the operations process defined in FM 3-0, Chapter 6, there are four components within HUMINT operations: Plan, Prepare, Execute, and Assess.

PLAN

4-3. HUMINT planning defines collection objectives, when to collect it, and which resources will be tasked to do the collection. Commanders with HUMINT collection assets in their units receive collection tasking based on requirements developed during ISR planning. The commander and staff, in concert with their supporting OMTs, assess the requirements and task the team or teams best capable of answering the requirement based on contact placement and access.

4-4. Another aspect to consider carefully during the Plan phase of the operational cycle is technical control. Technical control is ensuring adherence to existing policies and regulations, providing information and guidance of a technical nature, and supervising the MOS-specific TTP required in

conducting collection missions. Planning must take into account that technical control does not interfere with or supersede any C2 that a commander has over an asset or unit nor does it interfere with collection of the commander's requirements. For HUMINT collectors, the technical control network includes the C/J/G/S2X, the HOC, and OMTs. Technical control includes the management of source and other sensitive data and databases, the management of intelligence contingency and incentive funds, the liaison with other HUMINT organizations, and the deconfliction of operations. Technical control provides HCTs with specific requirements and data that they need to conduct operations and, in certain circumstances, specific instructions on how to execute missions.

PREPARE

4-5. During this phase, commanders and staff, including HUMINT management sections, review HUMINT mission plans. This review is to ensure all areas of the mission are considered and addressed in the plan and included in rehearsals. Items to cover include but are not limited to—

- Route (primary and alternate).
- Communications.
- Security plan.
- Convoy procedures including actions on contact and rally points.
- Initial requirements to be covered.
- Mission duration.

4-6. The HUMINT collector then researches the topic area addressing the requirement and prepares a questioning plan. The HCTs and OMTs must coordinate all mission requirements. It is important that HUMINT elements are included in all rehearsals conducted by their supported unit. These rehearsals will enable HCTs to carry out essential coordination with other units and ensure that they are included in and familiar with procedures such as resupply, communications, casualty evacuation, fire support, and fratricide avoidance. Rehearsals and briefbacks will allow the supported command to see and correct problems with their support to the HUMINT elements prior to deployment.

EXECUTE

4-7. Mission execution consists of the collection of information in accordance with the integrated ISR plan. The requirements manager validates the requirements based on command guidance. The G3 tasks the requirements to the units and the individual asset managers (that is, OMT) to identify the assets best capable to answer the requirement. When requirements are levied against a specific HCT, the HCT leader decides which of his team's contacts can best answer the requirements. He then turns the requirement into specific team tasks.

ASSESS

4-8. Assessment is the continuous monitoring—throughout planning, preparation, and execution—of the current situation and progress of an

operation, and the evaluation of it against criteria of success to make decisions and adjustments. Assessment plays an integral role in all aspects of the intelligence process (see FM 2-0).

HUMINT COMMAND AND CONTROL

4-9. Commanders of organizations that conduct HUMINT operations are responsible for task organization, mission tasking, execution, mission accomplishment, and designation of subordinate AOs (within the guidelines of the OPORD or OPLAN**).** MI unit commanders who exercise direct control of HUMINT operations, including interrogation operations, at all levels are responsible for and stand accountable to ensure HUMINT collection activities comply with this manual and applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. The MI unit commanders must ensure mission accomplishment by properly allocating resources and logistics in support of all HUMINT collection assets assigned to their units. Commanders must ensure that their HUMINT collection personnel are trained and ready for the mission. There is a need for a partnership between the J/G2X, who exercises technical direction and oversight responsibility and the MI commander, who exercises direct command authority and responsibility. The MI unit commander analyzes the higher headquarters mission, concept of operations, and the specified and implied tasks given to his unit. He restates the unit mission, designs the concept of operations, task organizes his assets, and provides support to subordinate units. Specifically, the MI unit commander—

- Issues mission orders with sufficient details and time for subordinate commanders and leaders to plan and lead their units.
- Must know the threat, his organization, ISR systems, counter-ISR systems, operations, and terrain over which his units will operate and how that terrain enhances or limits HUMINT collection operations.
- Must be aware of the operational and technical limitations of his unit and ensures that all assets are task organized, properly positioned, and fully synchronized to accomplish the mission.
- Oversees the collective and individual training within his unit.
- Coordinates continuously with the higher headquarters staff, the supported maneuver unit staff, and other commanders to ensure integrated R&S operations and support.
- Establishes clear, consistent standards and guidance for current and future operations in order to adhere to policy and the higher headquarters commander's intent without his constant personal supervision.
- Continually assesses his unit's ability to sustain its internal operations and its ability to support assigned missions and keeps the higher headquarters staff informed of unit, equipment, and personnel status that affect collection operations.

- Advises his higher headquarters commander and staff on the capabilities, limitations, and most effective employment of his assets.
- Remains flexible during operations to adjust or execute missions upon receipt of new orders and when the situation changes.
- Ensures personnel are working within legal, regulatory, and policy guidelines.

TECHNICAL CONTROL

4-10. Technical control refers to supervision of the TTP of HUMINT collection. Technical control ensures adherence to existing policies or regulations and provides technical guidance for HUMINT operations. The elements that provide technical control also assist teams in translating collection requirements into executable tasks. Commanders rely on the expertise of intelligence personnel organic to their unit and within higher echelons to plan, execute, and assess the HUMINT collection effort. The OMTs, HATs, and the HOC of the C/J/G/S2X provide technical control. They—

- Define and manage operational coverage and direction.
- Identify critical collection criteria such as indicators associated with targeting.
- Prioritize collection missions in accordance with collection requirements.
- Advise teams on collection techniques and procedures in accordance with policy, regulations, and law.
- Register and deconflict sources.
- Conduct operational reviews.
- Advise commanders.
- Conduct operational coordination with staff elements and other intelligence agencies.
- Manage ICF and incentive usage.

COMMAND AND SUPPORT RELATIONSHIPS

4-11. The activities of HUMINT assets are governed by their command or support relationship. There are subtle differences in the Joint versus the Army description of some of the command and support relationships. Tables 4-2 through 4-4 show these relationships.

4-12. During interrogation operations, close coordination must occur between intelligence personnel and personnel responsible for detainee operations including MP security forces, Master at Arms, and other individuals providing security for detainees. The facility commander is responsible for all actions involving the humane treatment, custody, evacuation, and administration of detainees, and force protection. Whereas, the intelligence commander is responsible for the conduct of interrogation operations.

COMMAND AND SUPPORT RELATIONSHIPS FOR HUMINT OPERATIONS

4-13. Clear command and support relationships are fundamental in organizing for all operations. These relationships identify responsibilities and authorities among subordinate and supporting units. The commander designates command and support relationships within his authority to weight the decisive operation and support his scheme of maneuver. Some forces available to a commander are given command or support relationships that limit his authority to prescribe additional relationships. Command and support relationships carry with them varying responsibilities to the subordinate unit by parent and gaining units. By knowing the inherent responsibilities, a commander may organize his forces to establish clear relationships.

4-14. Command relationships establish the degree of control and responsibility commanders have for forces operating under their tactical control (TACON). When commanders establish command relationships, they determine if the command relationship includes administrative control (ADCON). Table 4-2 shows Army command and support relationships and Table 4-3 shows joint command relationships chart from FM 3-0 (derived from JP 0-2 and JP 3-0).

4-15. Support relationships define the purpose, scope, and effect desired when one capability supports another. Support relationships establish specific responsibilities between supporting and supported units. Table 4-2 shows Army command and support relationships and Table 4-4 shows joint support relationships from FM 3-0 (derived from JP 0-2 and JP 3-0).

HUMINT REQUIREMENTS MANAGEMENT

4-16. The G2/S2 is responsible for RM. He uses the requirements management (RM) process to orchestrate the actions of the unit's organic and supporting ISR capabilities into a unified effort to gain situational understanding and answer the commander's PIRs. Through centralized planning and decentralized execution, RM optimizes the integration of ISR operations into the commander's scheme of maneuver and fire and into the unit's long- and short-range planning. Control mechanisms within the RM structure facilitate the identification of information shortfalls and the redirection of ISR assets to new intelligence production, reconnaissance, or surveillance missions.

Table 4-2. Army Command and Support Relationships.

IF RELATIONSHIP IS:		INHERENT RESPONSIBILITIES ARE:							
		Has Command Relationship with:	May Be Task Organized by:	Receives CSS from:	Assigned Position or AO By:	Provides Liaison To:	Establishes/ Maintains Communications with:	Has Priorities Established by:	Gaining Unit Can Impose Further Command or Support Relationship of:
COMMAND	**Attached**	Gaining unit	Gaining unit	Gaining unit	Gaining unit	As required by gaining unit	Unit to which attached	Gaining unit	Attached; OPCON; TACON; GS; GSR; R; DS
	OPCON	Gaining unit	Parent unit and gaining unit; gaining unit may pass OPCON to lower HQ. Note 1	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	OPCON; TACON; GS; GSR; R; DS
	TACON	Gaining unit	Parent unit	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	GS; GSR; R; DS
	Assigned	Parent unit	Parent unit	Parent unit	Gaining unit	As required by parent unit	As required by parent unit	Parent unit	Not Applicable
SUPPORT	**Direct Support (DS)**	Parent unit	Parent unit	Parent unit	Supported unit	Supported unit	Parent unit; Supported unit	Supported unit	Note 2
	Reinforcing (R)	Parent unit	Parent unit	Parent unit	Reinforced unit	Reinforced unit	Parent unit; reinforced unit	Reinforced unit: then parent unit	Not Applicable
	General Support Reinforcing (GSR)	Parent unit	Parent unit	Parent unit	Parent unit	Reinforced unit and as required by parent unit	Reinforced unit and as required by parent unit	Parent unit; then reinforced unit	Not Applicable
	General Support (GS)	Parent unit	Parent unit	Parent unit	Parent unit	As required by parent unit	As required by parent unit	Parent unit	Not Applicable

NOTE 1. In NATO, the gaining unit may not task organize a multinational unit (see TACON).

NOTE 2. Commanders of units in DS may further assign support relationships between their subordinate units and elements of the supported unit after coordination with the supported commander.

Table 4-3. Joint Command Relationships and Inherent Responsibilities.

(from FM 3-0, derived from JP 0-2 and JP 3-0)

Inherent Responsibilities Are:	If relationship is:		
	COCOM	OPCON	TACON
Has command Relationship with:	Gaining combatant commander; gaining service component commander	Gaining Command	Gaining Command
May be task organized by:	Gaining combatant commander; gaining service component commander	Gaining Command	Parent Unit
Receives logistic support from:	Gaining service component commander	Service component command; parent unit	Parent Unit
Assigned position or AO by:	Gaining component commander	Gaining Command	Gaining Command
Provides liaison to:	As required by gaining component commander	As required by gaining command	As required by gaining command
Establishes and maintains communications with:	As required by gaining component commander	As required by gaining command	As required by gaining command and parent units
Has priorities established by:	Gaining component commander	Gaining Command	Gaining Command
Gaining unit can impose further command relationship/authority of:	OPCON; TACON; direct support; mutual support ; general support; close support	OPCON; TACON; direct support; mutual support; general support; close support	Direct support; mutual support; general support; close support

Table 4-4. Joint Support Categories.

(from FM 3-0, derived from JP 0-2 and JP 3-0)

CATEGORY	DEFINITION
General Support	The action given to the supported force as a whole rather than to a particular subdivision thereof.
Mutual Support	The action that units render each other against an enemy because of their assigned tasks, their position relative to each other and to the enemy, and their inherent capabilities.
Direct Support	A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance.
Close Support	The action of the supporting force against targets or objectives that are sufficiently near the supported force as to require detailed integration or coordination of the supporting action with fire, movement, or other actions of the supported force.

DEVELOP HUMINT REQUIREMENTS

4-17. The first step in the RM process is to develop intelligence requirements that accurately identify and prioritize the commander's concerns about the threat and the battlefield environment that must be resolved to accomplish the mission. The G2/S2X, or his representative, normally supports the G2/S2 by identifying HUMINT collection requirements and opportunities and advises the command and staff on HUMINT capabilities. The HUMINT representative must be able to discuss any delays or risks involved in using HUMINT assets. Through participation in the requirements development process, the HUMINT representative has a thorough understanding of the commander's intent and concept of operations and is better able to support the overall ISR effort.

4-18. The analysis of HUMINT requirements is normally a coordinated effort between the HUMINT and CI staff officer (C/J/G/S2X) and the HAT of the supporting analysis element. The C/J/G/S2X team—

- Records all HUMINT requirements whether generated internally (Specific Orders) or received from other echelons or units (Requests).
- Tracks each requirement from receipt to final satisfaction.
- Reviews each requirement for its—
  - **Feasibility.** Feasibility is a determination if a requirement can be answered given available time and resources.
  - **Completeness.** Does the requirement contain all the specifics needed for collection, such as: What the collection requirement is? When the latest time information is of value (LTIOV)? Why it needs to be collected? Who needs the results of the collection?
  - **Necessity.** The C/J/G/S2X team, with the assistance of the HAT, checks available intelligence databases to determine if the required

information has already been collected or is included in an intelligence product.

4-19. The RM team, with the assistance of the C/J/G/S2X team and the HAT, breaks the HUMINT-related PIR into SIRs. Each SIR describes the indicator of threat activity linked to an area or specific location and time. The HOC evaluates—

- Reportable criteria that are linked to the threat activity. The HOC associates these characteristics with a SIR, and compares the characteristics to a particular HUMINT asset's capability to collect.
- Range, which is the distance from the current location of the HUMINT asset or resource to the source. In other words, are there sources available that had or have access to relevant information on the area or activity in question, and can the HUMINT team contact them in a timely manner?
- Timeliness, which is when the information must reach the commander to be of value; that is, the LTIOV.

4-20. The RM team, supported by the C/J/G/S2X and the HAT, attempts to answer the SIRs with intelligence products developed from information available within the existing intelligence databases or pulled from other organizations within the intelligence architecture. If the requirement can be answered in this manner, the intelligence is immediately disseminated. When the required information is neither available nor extractable from archived information or from lower, lateral, or higher echelons, the C/J/G/S2X team develops it into an RFI to higher or an ISR tasking for organic or attached HUMINT assets. The compilation of unanswered requirements and how to answer them form the basis of the ISR plan. The tasking may be in the form of an SDR. An SDR is a specific request or tasking for a collector to question a source on a particular collection requirement. This request involves analysis that results in the conclusion that a specific source possibly has the placement and access to answer a SIR. SDRs are specific; whereas, HUMINT collection requirements (HCRs) are general.

DEVELOP THE HUMINT PORTION OF THE INTEGRATED ISR PLAN

4-21. The HOC within the C/J/G/S2X section assists the G3/G2 in developing the HUMINT portion of the ISR plan in coordination with the HAT and the RM team. The HOC ensures that the HUMINT capabilities and taskings are included in the plan although the plan often will not contain the specifics of HUMINT operations due to the sensitivity of the sources and techniques. The HOC will coordinate with the Office of the SJA to ensure the HUMINT portion of the integrated ISR plan complies with applicable law and policy prior to its implementation. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. The HOC coordinates with C/J/G/S2X for mission deconfliction at that echelon to specify the collection capability and current

status of the various HUMINT organizations to better enable him to select the "best" organization to collect on various SIRs. HUMINT collection generally requires time to develop the environment and access sources.

4-22. The HUMINT collection environment during an SSC is different from an MTW. During an MTW where the force is moving, a division normally plans 48 hours out; a corps plans 72 hours out. In contrast, the planning focus for units supporting an SSC may be 3 to 6 months out. The longer HCTs are in an area, the better the collector is able to develop leads to answer collection requirements. Requirements may be continuous or may be concerned with specific upcoming events such as national elections. HUMINT is a key asset to determine adversary intentions; however, it is highly dependent on the ability to cultivate or locate sources with the desired information. HUMINT in support of stability and reconstruction operations is not a short-term undertaking. [Example: National level elections are taking place in the AO in 3 months. As a part of integrated ISR planning, an assessment must be conducted to determine the capability to answer post-election collection requirements based upon current contacts and HUMINT leads. If there are no leads or contacts that could answer election-related collection requirements, it is necessary to spot, assess, and contact sources to meet requirements.]

4-23. A second part of the HUMINT portion of the integrated ISR plan is the HUMINT collection focus, which—

- Designates which collection requirements comprise the emphasis for collectors' missions.
- Prioritizes collection requirements based upon the operational environment in the AO and future missions in the AO.
- Includes future operational collection tasks which aid in causing a gap or pause in collection as the unit transitions to the next operational phase or the next operation.

4-24. In addition to specific requirements, a statement of intelligence interest (SII) at the joint level or a collection emphasis message at division or corps is issued to identify the overall collection goals for a time period. As the collection request or requirement is passed down, each echelon performs additional planning for its own specific requirements.

Evaluate HUMINT Resources

4-25. After identifying the SIRs, the HOC and the C/J/G/S2X determine the availability and capability of HUMINT assets and resources that might contribute to requirement satisfaction and which are most suited to collect against each SIR. This does not necessarily imply that the C/J/G/S2X assigns a tasking to a specific team; rather, it develops the requirements or requests for an organization that then executes the mission. The HOC and C/J/G/S2X should also consult the HAT for its analysis of additional potential HUMINT assets and resources which might be available, both on and off the battlefield, to contribute to requirement satisfaction. For example, the HAT may be aware of a group of émigrés now living elsewhere who previously lived near a target site, and who might be able to provide answers to collection requirements if debriefed.

Determine Asset or Resource Capabilities

4-26. The HOC translates the capabilities and limitations of the available HUMINT assets into a set of factors that they can compare to the SIR characteristics. Asset capability factors are technical or performance characteristics, location, and source access. Each HUMINT asset is evaluated for its—

- **Availability.** The HOC reviews the list of viable HUMINT assets for current availability and the addition or deletion of capabilities. This includes considerations such as maintenance time and previous taskings. Coordination with adjacent and higher headquarters and national level agencies by the C/J/G/S2X will determine the availability of higher echelon resources.
- **Survivability**. Survivability must be commensurate with the threats to which the HUMINT assets will be exposed during the course of operations. These assets must be as survivable as, or in certain circumstances more survivable than, the forces they support. The HOC and the commander must weigh the risk versus the gain in using HUMINT assets.
- **Reliability.** Reliability is the ability of the asset to overcome threat deception measures such as misinformation or false information. In HUMINT there are two areas of reliability: source and collector. Source reliability is the determination on the part of the collector if the source is providing accurate information. Collector reliability is a determination on the part of the HOC that the HUMINT collectors within a particular organization have the level of training and experience to collect against a given requirement.
- **Suitability**. Tasking must be based on an asset's capability and on its suitability within the context of the overall plan. For example, HUMINT assets may be capable of collecting against a single target but have unique capabilities against a second target. Intelligence requirements may necessitate tasking these HUMINT assets against the second target if other assets can maintain adequate coverage of the first target.
- **Connectivity.** Connectivity is a critical aspect of any R&S operation. Interoperability, reliability, and robustness of sensors, communications, and supporting automated data processing (ADP) are crucial to the responsiveness, survivability, and overall combat effectiveness of a HUMINT asset. If the automation and communications systems of a HUMINT asset are dissimilar to those of other units in the AO, or if connectivity among assets, supporting systems, and supported systems and elements is too fragile to withstand the stress of operations, commanders will be deprived of important information essential to conducting tactical operations. The HUMINT asset must be able to transmit accurate and timely information to those who must receive it when they need it. Report formats should adhere to established standards in order to ensure that information is easily retrieval at the user desktop through automated queries (push/pull). Planners must look carefully at systems compatibility and the degree of interoperability among the components

of the communications architecture. The better the interoperability of assets and the more robust and redundant the communications links, the better the cross-cueing and analytical exchange.

Develop the Scheme of Support

4-27. The scheme of support is the orchestration of HUMINT assets, resources, and requirements to facilitate the collection of information most effectively. It includes all assets that the G3/S3 can task (organic, attached, and DS) and the G2 can request (from higher or adjacent units). By reviewing available HUMINT assets and higher echelon resources, the HOC and the G/S2X determine whether unit assets or higher echelon resources are best able to answer the requirements. If another echelon can answer an SIR, then the J/G/S2, normally through the C/J/G/S2X, requests them to collect the information and deliver the intelligence product. When planning the HUMINT portion of the ISR plan, the HOC should consider the following:

- **Cueing** is using one asset to tip off another to a possible target. The HOC should look for opportunities for HUMINT assets to cue other collection assets and vice versa.
- **Asset redundancy** uses a combination of the same type of assets against a high-priority collection target. This is vital in HUMINT collection since, in dealing with human sources, the information collected is often part of the overall picture or is influenced by the perception and prejudice of the source. The collection on the same target from a number of different assets gives a more accurate intelligence picture and is a method to validate source reporting.
- **Asset mix** uses a combination of different types of assets against a high-priority collection target. When the probability of success of one asset to satisfy the requirement completely is lower than acceptable, the use of multiple capabilities of different assets increases the likelihood of success; for example, using SIGINT assets to intercept voice communications while HUMINT assets observe activities. Neither can collect all the available information, but the information collected by both can be fused into a more complete picture. Like asset redundancy, asset mix places greater demands on the limited assets available, both collection and analysis, and has to be clearly justified by the potential intelligence gain.
- **Integration of new requirements** into ongoing missions may make it possible to reduce timelines, make collection more responsive to the request, and decrease cost and risk. This is critical in HUMINT due to the long time that it takes to develop sources. The use of an existing source to answer new requirements often facilitates collection.

Develop and Prioritize Taskings and Requests for Information

4-28. After the G2/S2X and the G2/S2 approve the HUMINT portion of the ISR plan, the HOC develops specific orders to task assets, develop additional assets, and/or requests to seek higher and lateral support and production. Specific taskings or RFIs are tailored to that specific ISR asset's capabilities and limitations. The G2/S2X supports the requirements manager and the G2/S2 in developing and prioritizing HUMINT taskings. The HOC works

with the unit requirements manager to incorporate the HUMINT plan into the overall unit ISR plan and works with the G3/S3 as necessary to help develop OPORDs or FRAGOs to organic or attached ISR units. HUMINT taskings will often include technical data that cannot be passed through normal tasking channels. The HOC will pass that information directly to the applicable HUMINT OMT or unit operations section.

4-29. The HOC and G2/S2X cannot provide operational taskings to a unit for collection. Collection is a stated mission that the commander executes. However, the technical control the HOC can provide as the HUMINT manager affords the J2/G2X the ability to steer and direct collection assets and operations. The MI commander and OMT determine specifically which teams will collect on a given requirement and are responsible for the TTP used. They report on the status and availability of their collection assets. On the HCT level, the team chief determines which sources will be contacted and the details of how the information will be collected from a given source. A specific plan is developed for each source. This plan should—

- Identify the requirement.
- Identify the proposed source.
- Identify questions to be asked during the source meeting.
- Contain an outline of how the meeting should proceed.
- Identify which collector will conduct the source meeting.

4-30. At the HCT level, the senior team member reviews each plan to ensure the proper planning for the collection mission. The plan is a minimum goal for the collection. The collector must be fully aware of the overall collection priorities and be prepared to take advantage of any additional leads.

DIRECT PRODUCTION

4-31. The G2 coordinates intelligence production to provide non-duplicative all-source intelligence products to the commander, staff, and subordinate forces. Some type of production occurs in the intelligence staff or separate analysis element at every echelon from national to battalion level. The HCT of the ACE at echelon's division and higher will support the intelligence production process through the analysis of HUMINT information and the development of single-discipline HUMINT products.

DISSEMINATE INFORMATION

4-32. The 2X element at each level is normally the release authority for HUMINT reporting and products, ensuring that reporting, products, and data are disseminated to the lowest appropriate level. The G/S2X should preplan criteria for the immediate release of combat information on high-value targets, impending attacks, or other time-sensitive requirements. This preplanning will ensure that commanders and other users quickly receive the information in a format that supports situational understanding, strategic responsiveness, and ISR and provides support to effects. Special effort is also made to ensure that information obtained from detainees is passed back down to the unit that detained them. This measure will support the efforts of the commander as well as building trust in the intelligence process.

EVALUATE REPORTING

4-33. The HAT and the HOC provide the requirements manager and the G2/S2 with expertise to support report evaluation. An important part of the evaluation process is providing feedback to the collectors. Feedback is important in HUMINT operations since the same source may be contacted again for additional information. The collector needs feedback on the accuracy, reliability, and appropriateness of the information reported. The G/S2X team tracks reporting to determine how well the HUMINT collection and production efforts are satisfying the PIRs. The G/S2X team supports the RM team's requirements to—

- **Monitor and Maintain Synchronization.** Through coordination with the G2/S2, the G/S2X, and the HAT, the HOC knows when and what critical pieces of information are missing from the commander's estimate of the situation. The HOC uses the HUMINT portion of the ISR plan to ensure synchronization with the overall operation and scheme of maneuver. The other critical tool for the HOC is the decision support template (DST). The HOC must have a complete copy of this document, ensuring the HUMINT assets do not miss a collection requirement.
- **Correlate Reports to Requirements.** The HOC tracks which specific order or group of specific orders originates from which PIR to ensure that the collected information was provided to the original requester. This also allows the HOC to rapidly determine which asset is available for retasking.
- **Screen Reports.** Each report received is screened for accuracy, timeliness, and applicability to the original tasking or request. If the HOC determines that it completely fulfills the tasking or request, the HOC informs the G/S2X and G2/S2 so that the tasking or request can be closed and the information provided to the original requesting unit.
- **Provide Feedback to Collectors and Analysts.** The HOC provides feedback to all the HUMINT R&S assets. This is normally provided through the C2 element of that unit. By doing so, the HOC quickly reinforces if the reporting is answering the original order or request, or the HOC can provide guidance if it is not. This feedback is essential. The RM team may provide additional information on its collection or analysis if the HOC tells the team exactly what is needed or has been missed in the original report.

UPDATE ISR PLAN

4-34. This step aids the G2/G3 in updating the ISR plan by eliminating satisfied collection requirements, redirecting assets to cover non-satisfied requirements, cross-cueing requirements, and adding new collection requirements to the ISR. This process is accomplished by adjusting the HUMINT portion of the overall integrated ISR plan. It maintains intelligence synchronization and optimizes the exploitation of information in response to situation changes in the AO. The updated HUMINT plan is distributed to the G/S2X requirements manager to ensure its incorporation into the overall unit ISR plan. Continuously updating the HUMINT portion of the ISR plan is vital due to the time involved in redirecting HUMINT assets.

HUMINT MISSION PLANNING

4-35. HUMINT mission planning begins when a unit receives a tasking to conduct HUMINT collection in support of a specific mission, operation, or collection plan. The mission analysis portion of the MDMP is explained in FM 5-0. Special factors must be considered when applying the MDMP to HUMINT operations as discussed below.

RECEIVE AND ANALYZE THE HIGHER HEADQUARTERS ORDER

4-36. Attention must be paid to the support relationship (GS or DS) that exists between HUMINT assets and the unit. The operational environment, including applicable law and policy under which the units are operating must be understood, as this affects the ability of the units to perform certain missions. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Because of frequently overlapping AOIRs in HUMINT operations, other unit missions and potential areas of conflict must be identified. Missions of other non-HUMINT units must be understood for coordination and possible integration of HUMINT assets. The availability of assets from higher echelons, requirements to provide support to lower echelons, and the existence of technical control from higher echelons must be identified. Tasking, reporting, and communications channels must be clearly understood.

ISSUE A WARNING ORDER

4-37. After the commander has analyzed his orders and worked out the mission and related tasks, he must quickly pass on this information to his team. This is accomplished through the WARNO. As a minimum, the WARNO must include to whom the order applies, time and nature of the operation, the earliest time of movement, and the time and place where the OPORD will be issued. Unit members should prepare for movement while the leader is performing the remaining preparatory tasks.

MAKE A TENTATIVE PLAN

4-38. When determining how the mission will be carried out, the commander works with the factors of METT-TC. When planning for HUMINT collection missions, focus must be placed on the human beings (threat, friendly, and neutral) as well as the key terrain on the battlefield, including information on—

- The demographics of both the AO and AOI.
- The organization and structure of all opposition in the AO and AOI.
- The history of the AO and AOI pertinent to the current situation.
- The economic and social data of all groups in the AO and AOI.

- All key leaders (political, military, social, religious, tribal), opinion leaders, and other influences on public opinion.
- The media and its influence on the population of both the AO and AOI.
- The primary and secondary languages and dialects spoken in all parts of the AO.

4-39. A target folder, if one is used, provides valuable up-to-date intelligence information about the AO for mission analysis and planning. Once intelligence products identify the contentious areas, trends, capabilities, and latest issues concerning the AO, the commander may request a target folder prepared on specific items, such as a hostile organization with the inclination and potential to cause harm to friendly forces. Target folders may include—

- Imagery of the AO and personalities.
- Terrain models of the AO.
- Latest information reports from the AO.
- Biographical data on key leaders in the AO.

Review Available Assets

4-40. The commander and staff, including the OMTs or HUMINT operations section, must look at organic assets and consider factors such as language capability, experience in various aspects of collection, analysis, and management. If organic assets are inadequate, the commander and staff should consider additional available assets within the organization and resources from higher echelons. The commander and staff must consider the analysis and management structure of a HUMINT operations section in addition to the OMT and HCTs. During this step the mission analysis and planning group should determine, among other things—

- The number of HUMINT collectors available.
- The number of collectors who are qualified linguists.
- The number of linguists available to support the collectors.
- Force protection considerations.
- The optimal number of HCTs, OMTs, and HUMINT operations sections that can be configured from the available assets.
- Whether additional assets such as CI agents, TECHINT personnel, analysts, additional linguists, or other experts need to be added to some or all the HCTs to meet mission requirements.

Determine Constraints

4-41. This is a critical step in HUMINT mission analysis. HUMINT collection operations are affected by applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. The degree of restriction may depend on the type of operation being conducted. Constraints are normally found in the scheme of maneuver, the concept of operations, and coordinating instructions. Specific to intelligence interrogation operations, in

accordance with DOD Directive 3115.09, "all captured or detained personnel shall be treated humanely, and all intelligence interrogations or debriefings to gain intelligence from captured or detained personnel shall be conducted humanely, in accordance with applicable law and policy. Acts of physical or mental torture are prohibited."

Identify Critical Facts and Assumptions

4-42. The human factor is preeminent in this step. Assumptions and facts include—

- How HUMINT collectors can interact with the local population.
- What types of sources are available.
- What types of adversary intelligence and unconventional threats are present.

Conduct Risk Assessment

4-43. There are inherent risks involved in HUMINT collection. HUMINT collectors need access to the local population to perform their mission. Rules that restrict all forces to base areas to protect the force may be prudent; however, these restrictions can severely degrade HUMINT collection capabilities, particularly in support of force protection requirements. This measure deprives the collectors of sources needed to anticipate and prevent violent incidents. HUMINT collectors receive cultural training as well as security training to allow them to minimize the dangers of interacting with the local population. Commanders must weigh the risk to collectors against the risk to the force as a whole, and determine whether to provide additional security to the HCT in order to allow the team to perform missions outside the base area to gain needed intelligence. DA Pam 385-1 provides guidance for risk assessment.

Select Courses of Action (COAs)

4-44. During COA development the staff, under the commander's guidance, analyzes various options for deploying and implementing HUMINT assets. Input from HUMINT senior NCOs and WOs is vital to COA development and analysis. Items to consider during COA development include—

- The distribution of the HCTs and OMTs within the AO.
- The support relationship (GS and DS) that exists for the deployed teams.
- The command relationship in effect for the HCTs and OMTs (assigned, attached, or OPCON).
- The manner in which the HUMINT assets are phased into the theater.
- The tactical configuration (personnel and equipment) of the HCT.
- The actual number of the HCTs and OMTs and the size of the supporting HUMINT operations section (if any) deployed.
- The priority of the OMT's efforts.
- The priority of linguist support.

COLLECTION PRIORITY

4-45. During the MDMP, the MI commander advises his higher headquarters on the most efficient use of the HUMINT collectors to meet collection requirements. Depending on the particular higher echelon mission and the capabilities of the specific personnel under his command, the supported S2 must decide whether to concentrate collection efforts on source, debriefing, interrogation, tactical questioning, liaison, or DOCEX operations to answer collection requirements. (See Chapter 5 for a description of these operations.) The MI commander may be required by his operational tasking to support any or all of these operations. He must decide how to task organize his assets to meet these requirements. When faced with limited assets, prioritization of collection is paramount.

4-46. A commander normally must prioritize HUMINT collections and DOCEX. Although the decision is primarily dependent on which type of source (human or document) is most likely to give the priority information, other factors such as phase of operation, ROE, source availability, and collection resource capabilities may influence his decision. At the tactical level, both human sources and documents are screened and the senior HUMINT soldier establishes the priorities. If documents and human sources are determined to be equally likely of containing priority information, human sources are normally exploited first due to—

- The ability of the HUMINT collector to get a human source to elaborate and explain his information, which cannot be done with a document.
- The rate at which people forget detailed information.
- The fact that an individual's resistance is easier to bypass immediately after undergoing a significant traumatic experience (capture). Capture thrusts them into an unfamiliar environment over which they have no control and are vulnerable to various approach techniques. This initial vulnerability passes quickly. An individual's established values begin to assert themselves again within a day or two, and the individual's willingness to cooperate might also decrease.

TASK ORGANIZATION

4-47. Because of the need to place HUMINT collectors in contact with the local population and the need in many cases to integrate the HUMINT collection process into other operations, the planning and analysis staff for HUMINT missions is somewhat expanded from the norm. They should include the C/J/G/S2X, SJA, S1, S2, S3, S4, S5, S6, other staff officers, as necessary, Provost Marshal, MP, and US Army Criminal Investigation Command, CA, unit HUMINT commanders, and senior HUMINT technicians of the deploying unit. If the unit's mission is to replace a currently deployed HUMINT unit, a representative of that unit should be included.

4-48. The challenge to the MI commander is the proper training during operations, task organization, placement, and coordination of movement of HUMINT elements to meet collection requirements. The unit modified table of organization and equipment (MTOE) organization, which is designed for an MTW, may have to be modified to meet the specific requirements of

operations in PMEs and SSCs. Augmentation is often needed and must be requested. Task organization must be flexible to adjust to the dynamic mission objectives. Commanders must allow for the augmentation of HCT with other MI specialties and non-MI personnel as mission analysis and planning indicate the need. Mission analysis and planning identify the specific requirements for the HUMINT operations section, HAT, OMTs, and HCTs.

4-49. The composition of the HUMINT elements must be based on METT-TC factors. The number of HCTs and OMTs in the theater depends on the intensity of the collection effort and the geographical coverage of the AO. HCT members should be prepared to support any HUMINT missions they may receive through command channels. They must have the skills to shift easily from one set of functions to another based on the dynamic mission requirements. The number of OMTs in a designated theater will depend on the type and nature of the mission. A single OMT is capable of managing and controlling 2 to 4 HCTs. The size and staffing of the OMT will depend on a number of factors:

- Whether a HUMINT operations section is deployed and how many HCTs are subordinate to it.
- If a single HCT deploys to support a small contingency, there may be no need for an OMT. In this case the team leader must serve as the OMT.
- If three or more OMTs deploy, then a tactical HUMINT operations section should be deployed.
- For every 3 to 4 HCTs and their designated OMT, there should be one headquarters element composed of a platoon leader and a platoon sergeant to handle all administrative and logistical matters.

OPERATIONAL CONSIDERATIONS

RESERVE COMPONENT INTEGRATION

4-50. Given the Army's OPTEMPO and force structure, the integration of RC forces into the AC is highly likely for future operational deployments. Commanders must identify their requirements early and establish proactive coordination (both in garrison and while deployed) with their RC counterparts to fully integrate them during all phases of training and operations. During operations that include significant RC participation, an RC liaison officer normally will be assigned, either temporarily or permanently (at higher echelons), at the appropriate level of command. The commander and staff must ensure that the RC LNO is involved in all aspects of operational planning and execution.

4-51. There are three general categories of RC augmentation:

- Category 1: Formation of specialized units that include a fully integrated AC and RC TOE. The activation of the RC of these units is required for their full operational capability.
- Category 2: Augmentation of active duty units by RC units to fill out unit strength levels or to provide additional functionality. For example, an AC division might require additional HUMINT teams to support it

during a stability operation. If a division required one additional team, it should request a team and not request four HUMINT collectors. If the requirement is for three additional teams, it should request a HUMINT platoon with its organic C2 and OMTs.

- Category 3: The requirement for individual augmentees. This usually occurs when a unit has the C2 structure but needs either additional personnel or additional capability within the command structure. For example, a unit may have a HUMINT platoon but the platoon is at 50 percent strength. Individual augmentation is the easiest method of integration since the individual is integrated in the same manner as any replacement. The augmented unit normally is required to provide all equipment other than initial issue-type equipment.

4-52. There are several items to consider in unit augmentation:

- Accurate Identification of Requirements: During the MDMP, units need to identify those mission-essential capabilities not already present in the unit. The G3/S3, working in conjunction with the G1/S1, considers options that may include RC augmentation of organic units although the final decision to employ RC units is usually determined at Headquarters, Department of Army (HQDA). The requirement for augmentation is forwarded through appropriate personnel channels to US Army Forces Command (FORSCOM) and HQDA, which will identify the appropriate units or personnel. If approved, they will work with the appropriate agencies to establish the timeline in which the units can respond on the Time-Phased Forces Deployment Data List (TPFDDL). When developing requirements, the requesting unit must be sure to articulate its needs accurately, specifying required skills, numbers, and any additional skill identifiers (ASI). [Example: Request augmentation by a HUMINT platoon consisting of at least a platoon headquarters, three HCTs, one OMT, two linguists, and one CI/HUMINT Automated Tool Set (CHATS) proficient operator. The augmenting element will be operating in support of the commander's force protection program in the gaining unit's AOR.]
- Activation Timeline: Units need time to mobilize and conduct any additional collective and individual training that may be specific to the unit's mission or operational environment. The requesting unit needs to be aware of the time required to activate the requested RC and that there may be differences in levels of training or equipment. Timelines should be established by FORSCOM to allow resolution of these problems and should be reflected in the commander's operational planning sequence. Timelines will vary from unit to unit and mission to mission.
- Training: USAR and ARNG units usually cannot train their units or individuals to the same proficiency as the AC. Normally, this is due to the limited amount of training time. Because of this limitation, a certain degree of train-up prior to deployment may be necessary. Commanders should identify available training opportunities and request the participation of personnel identified for augmentation. For an ongoing mission, you should also plan for an extended "right seat

ride" mission handover period once the individuals or unit arrives in the theater of operations.

- Command and Control: If the RC augmentation requires activation of an entire unit, it should include their C2 element. If the augmentation is by individuals, then they will fall under the command and control of the gaining units.
- Time on Active Status: USAR and ARNG soldiers are restricted as to the amount of time they can remain on active status. This timeline begins on the date of mobilization and ends on the day the soldier leaves active duty status. Deployed units must take this into account when conducting continuous operations and must identify the requirement to replace RC forces early enough to allow for the required training and handoff procedures.
- Experience: While RC personnel normally lack current military experience, they often perform jobs in the civilian sector that either mitigate this lack of experience or they are able to bring a new and useful capability with them. Care should be taken that reservists who have civilian jobs which are similar to their HUMINT MOS (such as police officers or investigators) recognize the different constraints under which they operate in the military environment. For example, police officers who might normally task informants with minimal oversight cannot do that in their position as a HUMINT collector. Commanders should try to capitalize on these skills, but ensure proper training and understanding of the policies and regulations that govern HUMINT collection operations.

OPERATIONS PLANS, OPERATIONS ORDERS, AND ANNEXES

4-53. An OPLAN is any plan for the conduct of military operations. When a commander issues a directive for the coordinated execution of a military operation, it becomes an OPORD. Although plans are based on specific conditions or assumptions, they are not static. Plans are changed, refined, and updated as a result of continuous estimates and studies. It is critical to include HUMINT plans in the Intelligence Annex to the OPLAN.

4-54. The OPORD gives the HUMINT element approval to execute its mission. OPORDs define the mission, set the parameters of operations, identify who is responsible for what, and how it is to be supported. Additions that are necessary to amplify an OPLAN or OPORD are contained in annexes, appendices, tabs, and enclosures. Tasking for units to conduct HUMINT collection operations is listed in the main body of the OPORD under **Tasks to Subordinate Units**. The HUMINT appendix to Annex B provides the technical guidance for HUMINT collection including the umbrella concept for HUMINT operations.

4-55. The HUMINT appendices provide details on planning, coordinating, approving, and managing HUMINT operations as they relate to the unit's overall mission. These appendices serve as the basic document authorizing most HUMINT operations and programs. They must be reviewed and approved by the appropriate office or commander. The HUMINT appendix to the ISR Annex is necessary to ensure that augmentation of HUMINT assets

from other components and agencies are integrated throughout the TF as required to facilitate their specialized collection requirements. Specific tabs may include joint debriefing and interrogation facility operations, source operations, DOCEX, or open-source information.

OPERATIONAL COORDINATION

4-56. HUMINT collection is not conducted in a vacuum. Coordination with MI organizations and non-MI agencies, units, and staff organizations is often critical to expedite and complete HUMINT collection operations. (See Appendix C for predeployment planning.)

MI ORGANIZATIONS

4-57. Elements involved in HUMINT planning, execution, and analysis need to maintain close coordination with their counterparts in the other intelligence disciplines. Coordination includes but is not limited to the disciplines shown below.

Imagery Intelligence:

- Support imagery analysis by using HUMINT sources to identify or confirm the identification of items in imagery. This includes, for example, using human sources to identify the functions of buildings that have been tentatively identified through external imagery.
- Coordinate for current military or civilian imagery to use in the questioning of sources.
- Cue requirements managers and others involved in imagery tasking on locations or activities for imagery collection.
- Coordinate for IMINT information to verify information obtained through HUMINT collection.
- Provide imagery for analysis (through still and video photography and captured imagery).
- Coordinate for technical support as required when questioning personnel on subjects related to imagery.
- Obtain imagery-related collection requirements that can be answered by human sources.

Signals Intelligence:

- Support signals analysis by using HUMINT sources to identify or confirm the information obtained through SIGINT collection.
- Coordinate for current SIGINT information to use in the questioning of sources.
- Cue requirements managers and others involved in SIGINT tasking on locations or activities (including communications types and frequencies) for SIGINT collection.
- Coordinate for information to verify information obtained through HUMINT collection.
- Provide SIGINT-related CEDs for SIGINT analysis.

- Coordinate for technical support as required when questioning personnel on SIGINT-related topics.
- Obtain SIGINT-related collection requirements that can be answered by human sources.

Measurement and Signature Intelligence:

- Support measurement and signature intelligence (MASINT) analysis by using HUMINT sources to identify or confirm the information obtained through MASINT collection.
- Cue requirements managers and others involved in MASINT tasking on locations or activities for the location of MASINT sensors.
- Coordinate for information to verify information obtained through HUMINT collection.
- Provide MASINT-related CEDs for MASINT analysis.
- Coordinate for technical support as required when questioning personnel on MASINT-related topics.
- Obtain MASINT-related collection requirements that can be answered by human sources.

Technical Intelligence:

- Support TECHINT analysis by using HUMINT sources and documents to provide information concerning threat equipment and to support TECHINT materiel analysis. This includes, for example, the interrogation or debriefing of equipment operators of the translation of operators manuals for a piece of equipment being investigated.
- Coordinate for current information on equipment capabilities to use in the questioning of sources.
- Cue requirements managers and others involved in TECHINT tasking on locations or activities for TECHINT collection. This includes forwarding the identification and location of equipment of TECHINT interest obtained during HUMINT collection operations.
- Coordinate for TECHINT information to verify information obtained through HUMINT collection.
- Provide information from CEDs in support of TECHINT.
- Coordinate for technical support as required when questioning personnel on subjects related to areas of TECHINT interest.
- Obtain TECHINT-related collection requirements that can be answered by human sources.

Counterintelligence:

- Support CI analysis by using HUMINT sources to provide information concerning adversary intelligence collection capabilities and operations.
- Identify human and document sources that have information of CI interest.

- Cue requirements managers and others involved in CI tasking individuals or activities of CI interest.
- Coordinate for CI information to verify information obtained through HUMINT collection.
- Provide information from CEDs in support of CI.
- Coordinate for CI support as required when questioning personnel on topics related to areas of CI interest.
- Obtain CI-related collection requirements that can be answered by human sources.
- Integrate CI elements into HUMINT collection operations as applicable.

Open-Source Intelligence:

- Support open-source intelligence (OSINT).
- Provide open source maps, charts, phone directories, business directories, newspapers, video and audio media (including tapes and compact discs) to the appropriate J/G/S2X and Intelligence Community agencies and liaison officers.

OTHER ORGANIZATIONS

4-58. In addition to MI units, HUMINT collection organizations frequently conduct coordination with other military organizations.

- **Military Police Units:** Close coordination between HUMINT collectors and MPs is mutually beneficial. The MPs are responsible for maneuver and mobility support, area security, internment and resettlement, law and order, and police intelligence operations. Both activities (HUMINT collection and MP operations) require close contact with the local civilian, refugee, and detainee populations. HUMINT collection at checkpoints and at EPW and other detainee collection points must be coordinated with the MPs, who are normally responsible for internment and resettlement operations. In return, the HUMINT collectors, because of their screening and questioning of these population groups, can help facilitate the MP's population control missions by providing information about the population's activities and intentions that may be of MP concern. At EPW/detainee collection points, HUMINT collectors should arrange with the MP leadership to be allowed to debrief MPs since MPs are in regular contact with the detainees. This does not constitute tasking. Information collected in this manner may provide valuable insight, which can aid the collector in formulating approach strategies. MPs should be debriefed in such a way so as not to interfere with their mission. Liaison with the MP chain of command is vital to gain their support and assure them that HUMINT collection will not interfere with MP operations. Joint patrols containing MPs and HUMINT collectors can also be mutually beneficial in many situations.
- **Criminal Investigation Division (CID) and Provost Marshal Office (PMO):** The goals of HUMINT collection and those of the MPs (particularly CID) are different. CID and PMO are concerned with

identification and apprehension of criminal elements. The goal of HUMINT collection is the collection of information in response to PIRs that in many situations are centered on force protection. In the situation where the threat includes a criminal element, the HCTs might collect OB type information on the criminal element to ascertain their activities and threat to friendly forces. HUMINT collectors are not trained to conduct criminal investigations and must not be used for this purpose. Criminal investigators and HUMINT collectors must carefully coordinate their activities as necessary. HUMINT collectors are required to report to the proper agency information collected on criminal activities that the HUMINT collectors uncover in the normal course of their activities.

- **Psychological Operations Units:** As with the MP force, HUMINT collectors and PSYOP units are often interested in the same target audience but for different reasons. PSYOP units are interested in modifying the target audience beliefs and actions to be more supportive of US goals. Normally, HUMINT collection elements coordinate with PSYOP elements to obtain information concerning the motivational factors and cultural value systems of the individuals to be questioned. PSYOP units, as a part of their normal operations, develop detailed analysis concerning psychological and cultural factors of friendly and hostile elements in the AO. Such information will help HUMINT collection personnel to understand the source's attitude, value system, and perception; it will also help to obtain information more rapidly. At the same time, PSYOP units often will develop collection requirements to determine local attitudes and for information on the effectiveness of PSYOP campaigns. HUMINT collectors can be tasked to collect on these requirements if they are included as PIRs.
- **Civil Affairs Units:** The CA mission often places CA units in contact with the HUMINT collection target audience. If possible, HUMINT collection missions can be established in coordination with CA missions. If the HUMINT collection mission is viewed as having the potential of interfering with the CA mission and coordinated operations are not possible, CA personnel can still be sensitized to intelligence collection requirements and debriefed by HUMINT collectors as part of a friendly force debriefing operation.
- **Drug and Law Enforcement Agency Operations:** Personnel who are employees of DOD intelligence components may be assigned to assist Federal law enforcement authorities and, when lives are endangered, state and local law enforcement authorities; provided such use is consistent with, and has been approved by an official authorized pursuant to DOD Directive 5525.5, Enclosure 4 (reference (i)). Such official shall ensure that the General Counsel of the providing DOD component concurs in such use. Assistance may be rendered to LEAs and security services of foreign governments or international organizations in accordance with established policy and applicable SOFAs, provided that DOD intelligence components may not request or participate in activities of such agencies undertaken against US persons that would not be permitted activities of such components under the procedures of AR 381-10. HUMINT collectors may assist

foreign law enforcement authorities, with prior approval of the J2X. Under no circumstances will HUMINT collectors assist any US or foreign law enforcement authorities in any manner without prior approval by competent authority after a legal review of the proposal.

- **Maneuver Units:** HCTs may be utilized in GS for coverage of an AOIR or in DS to support a specific maneuver unit. The type of coordination needed with maneuver units will vary depending on the type of support relationship the HCT has. HCTs operating in GS should coordinate with maneuver unit commanders when the HCT will be operating in that unit's AO. At a minimum, the HCTs should announce their presence and request information on any conditions or ongoing situations that may affect on the conduct of their mission. An HCT operating in DS of a specific unit will coordinate with the unit for force augmentation to HUMINT patrols as needed in accordance with force protection requirements. The HCT leader should also coordinate with the supported unit's S2 for involvement in debriefings of returning patrol members, checkpoint personnel, convoy leaders and others. HCT leaders may also coordinate to be included in the unit's reconnaissance patrols, as appropriate.
- **Combat Service Support Units:** Current and future combat operations will be conducted in a noncontiguous battlespace. CSS formations and units may be an excellent source for HUMINT collectors. In many situations, DPs and refugees will perceive CSS activities as non-threatening and an activity which can provide them with aid and comfort. CSS operations will naturally draw DPs and refugees hoping to receive support. This could provide opportunities for HUMINT collectors to access this sector of the population. CSS unit S2s should conduct patrol debriefings of returning convoy personnel to capture observations made during convoys, with the goal of cross-cueing the supporting HCT, CI team, or law enforcement element as appropriate.

STAFF COORDINATION

4-59. Successful HUMINT collection operations require support from the staff elements of the supported unit. These elements are collectively responsible for the planning that results in HUMINT tasking. Below is a partial list of the staff responsibilities that affect HUMINT collection:

- G1/S1 HUMINT-related responsibilities include but are not limited to—
  - Supervising the medical support furnished to EPW/detainees.
  - Maintaining a list (by language and proficiency) of qualified linguists within their command.
  - Coordinating with the G4 or G5 for procurement and payment of other interpreters and translators needed to perform intelligence and non-intelligence duties.
  - Ensuring the echelon's OPLAN contains complete provisions for handling and evacuating detainees, refugees, DPs, and local civilians

as required. This plan must satisfy the interests of all other staff officers and provide for—

- Ensuring humane treatment of all personnel.
- Promptly evacuating personnel from the combat zone.
- Integrating procedures for the evacuation, control, and administration of personnel with other combat service (CS) and CSS operations.
- Ensuring delivery of mail to EPWs and other detainees.
- Maintaining detainee (including EPW) statistics.
- Providing administration and control of detainee currency and pay records, including coordinating with appropriate intelligence authorities about investigating large sums of money.

- G2/S2 is responsible for developing intelligence in support of unit operations. The G2/S2 at division and higher and in the interim BCT is supported by a G/S2X and normally a HAT in the performance of his HUMINT-related functions. His HUMINT-related responsibilities include but are not limited to—
  - Obtaining intelligence through intelligence reach to support HUMINT collection.
  - Incorporating HUMINT into the ISR plan.
  - Developing the HUMINT annex to the OPORD and OPLAN.
  - Coordinating to provide technical support for all HUMINT collection operations.
  - Ensuring deconfliction and synchronization for all HUMINT collection assets within the unit's AO. A particular effort must be made to coordinate with all DOD military source operations (MSO), and DOD and other government agencies (OGAs) that may be operating in the AO; with the theater J2X, as part of deconfliction. Failure to deconflict with DOD MSO and OGAs may result in compromise of assets and interruption of collection operations and potentially unintended casualties.
    - Obtaining documents and materials of intelligence interest, including visual and audio media and electronic equipment (such as computers, phones, PDAs) taken from detainees, or seized or loaned, in coordination with the Provost Marshal and other elements.
    - Recording, evaluating, and analyzing collected information and providing feedback to HUMINT collectors.
    - Ensuring adequate HUMINT collection and reporting nets and systems are available.
    - Coordinating with the G3 to ensure plans for HUMINT collection operations are included in unit OPLANs.
    - Coordinating with the G3 to ensure that HUMINT collectors are included in unit training plans, rehearsals, and briefbacks.
    - Drafting instructions for handling, evacuating, and exploiting captured enemy personnel and CEDs. (They coordinate with the G3 to ensure draft instructions are included in the command standing operating procedures (SOPs), OPLANs, and OPORDs.)
    - Projecting capture rates as well as refugee and DP rates.

  - Determining the number of interpreters and translators needed to perform intelligence duties.
  - Coordinating with other agencies and HUMINT collectors for intelligence sharing.
  - Controlling the procedures used to process and grant clearances to the interpreters and translators as required.
  - Coordinating with the civil-military operations (CMO) officer for intelligence screening of local nationals, refugees, and DPs.
  - Coordinating with SJA for legal review of proposed operations.
- G3/S3 is responsible for operations, plans, organization, and training. His HUMINT collection-related responsibilities include but are not limited to—
  - Ensuring the inclusion of HUMINT collection units in the main body of OPLANs and OPORDs under **Tasks to Subordinate Units** and **Task Organization**.
  - Ensuring instructions for handling, evacuating, and exploiting captured enemy personnel and CEDs in all unit command SOPs, OPLANs, and OPORDs.
  - Incorporating HUMINT collection operations into future plans and operations.
  - Ensuring subordinate units are trained in proper handling and evacuation of captured enemy personnel, materiel, and CEDs.
  - Ensuring that the subordinate elements are trained in OPORDs including ROE and the proper handling of local civilians, foreign nationals, refugees, and DPs.
  - Obtaining, organizing, and supervising employment of additional personnel as guards for EPWs and other detainees where MP assets are not available or insufficient.
  - Tasking the Division/Brigade Engineer Officer in conjunction with the G2/S2 to conduct a site survey for possible EPW/detainee holding area facilities within the operational area. Priority should go to existing facilities needing little or no renovation to meet operational requirements. If suitable facilities cannot be found, the engineer officer should provide detailed facilities design specifications to the G4/S4 for coordination and development of contracted resources.
- G4/S4 responsibilities related to HUMINT collection include but are not limited to—
  - Developing command policy for evacuation and internment of captured enemy personnel, and evacuation and safekeeping of CEE and CEDs.
  - Coordinating contracts for real estate and construction of source-holding facilities if local capabilities are not available. Ideally, existing facilities will be occupied and renovated whenever possible.
  - Collecting and distributing captured enemy supplies. (This is coordinated with the intelligence and operations staffs.)
  - Procuring and distributing rations to personnel holding areas.
  - Transporting EPWs and other detainees in a timely, safe manner to the appropriate facility for processing.

- Determining requirements for use of source labor for the logistical support needed in source-handling operations.
- Providing logistical support to interpreter personnel.

- G5/S5 responsibilities related to HUMINT collection include but are not limited to—
  - Coordinating with local US government, personnel staff representatives, and HN armed forces for procuring native linguists for interpreter support.
  - Coordinating military support of populous.
  - Providing technical advice and assistance in reorientation of sources and enemy defectors.
  - Coordinating MI aspects of CMO activities with the G2.

ADDITIONAL SUPPORT

4-60. In addition to the major staff elements, a HUMINT collection element requires support from several other elements in order to conduct operations. These elements are discussed below.

- The US Army Criminal Investigation Command is the organization with primary responsibility for investigating allegations of criminal acts or reportable incidents committed by or against detainees.
- The SJA can provide legal support and advice on the interpretation and application of applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOS. The SJA is also a channel for reporting known or suspected reportable incidents of abuse or inhumane treatment.
- The Inspector General is a channel for reporting known or suspected reportable incidents of abuse or inhumane treatment.
- The PMO is the channel for reporting criminal activity other than reportable incidents, but also can be used for reporting known or suspected reportable incidents.
- The Chaplain can also receive reports of reportable incidents.
- The G7 provides information on Information Operations and conducts liaison with PSYOP, the Electronic Warfare Officer, the Military Deception Officer, and Operations Security personnel.

This page intentionally left blank.

PART TWO

HUMINT Collection In Military Source Operations

Part Two discusses HUMINT collection as it pertains to MSO. The Secretary of Defense (SECDEF) has established a DOD-wide HUMINT Enterprise consisting of the following executors: The Office of the Secretary of Defense (OSD), the Combatant Commands (COCOMs), the Military Departments, the Defense Intelligence Agency (DIA). All Defense HUMINT Enterprise executors support and satisfy Defense requirements by employing their available resources and capabilities.

MSO refer to the collection of foreign military and military-related intelligence by humans from humans. MSO are conducted under SECDEF authorities, to satisfy DOD needs in compliance with DOD policy. Within the Army, MSO are conducted by trained personnel under the direction of military commanders. These specially trained personnel may employ the entire range of HUMINT collection operations. MSO sources include one-time, continuous, and formal contacts, from contact operations; and sources from interrogations, debriefings, and liaison activities.

Each type of MSO activity has specific operational requirements, specific legal restrictions, and operational guidelines. HUMINT collection activities in each of these categories require specific approval, coordination, and review. MSO include human source contact operations, debriefing, liaison, and interrogations. This chapter introduces each of these collection operations.

Chapter 5

HUMINT Collection

HUMINT COLLECTION OPERATIONS

5-1. Full spectrum operations require focused MSO with strong capabilities dispersed across the battlefield. In offensive and defensive operations, the HCTs need to be placed in support of the engaged maneuver battalions. In stability and reconstruction operations and civil support operations, the HUMINT teams need to be located in battalion AOs throughout the AOIR.

5-2. The rapid pace of operations, the need to provide near-real time (NRT) support of command decisions and the inherent time delays in moving detainees, including EPWs and civilian refugees to centralized locations, necessitate the dispersion of HUMINT collection assets to forward areas in

support of critical operations rather than their retention at detainee and refugee holding facilities at echelons corps and below. This forward deployment gives HUMINT collectors earlier access to sources and is facilitated by enhanced communication and automation capabilities down to the collection team level.

5-3. All operations are different, and deployment of HUMINT assets is METT-TC dependent. Brigades need the capability to provide 24-hour HUMINT collection capability to each battalion AO. The command relationship of the HUMINT collection capability is also METT-TC dependent. The OMT should be located at the echelon that is best able to manage and support the HCTs and to provide the best capability to answer the commander's PIRs.

5-4. The Division and Corps elements should cover their respective areas not covered by their subordinate commands. They also, as needed, reinforce those target areas that are most effective in answering their respective command PIRs already covered by subordinate command capability. EAC HUMINT units normally are responsible for supporting theater or national requirements and providing HUMINT support at theater level facilities such as the JIDC. The EAC units will also augment the echelon below corps units and conduct source operations in the Corps area as required. Operations, particularly in challenging terrain and in stability and reconstruction environments, may require additional HUMINT assets normally obtained from the RC.

HUMAN SOURCE CONTACT OPERATIONS

5-5. HUMINT collection requires the contact between the HUMINT collector, who attempts to gather information through a variety of HUMINT collection techniques, and a human contact, who hopefully has the information that the HUMINT collector wants and who can be convinced to divulge the information. Operations with formal contacts are only conducted by HUMINT collectors and CI agents who are specifically trained and authorized to do so. There are three levels of contacts:

- One-time contact.
- Continuous contact.
- Formal contact.

5-6. The basic goal of all levels of contact is to collect information in response to collection tasking; however, only under certain conditions can HUMINT collectors task contacts to get information for them (see para 5-28). Understanding the types of contacts is key to understanding each type of human source contact operation. The following levels are not all-inclusive nor are the listed categories exclusive. For example, a contact who was initially a one-time contact (such as a walk-in) may later be developed into a continuous contact. A continuous contact may be developed into a formal contact, who can then be tasked, trained, and paid. There is no limit on the number of times a team can meet contacts without recruiting them and making them into a formal contact.

ONE-TIME CONTACT

5-7. The one-time contact is a source of information of value that was, and will be, encountered only once. In all operational environments the HUMINT collector will frequently encounter a source only once, particularly at lower echelons. This may be a local civilian encountered during a patrol, a detainee who is quickly questioned and then evacuated, or a refugee at a checkpoint.

5-8. In addition to the information obtained from a one-time contact, the HUMINT collector must make a reasonable effort to obtain as much basic data as possible about the one-time contact. Complete name, occupation, address, and other basic data of this source are crucial for a thorough analysis of the information provided. The one-time contact and the information he provides cannot be assessed and evaluated independently; however, the information provided by a one-time contact must be reported and corroborated through other HUMINT sources and even other intelligence disciplines.

5-9. Contact reports must be filed with the OMT and source registries maintained in accordance with FM 34-5 (S//NF), AR 381-100 (S//NF), and DIAM 58-11 (S//NF) in order to support analysis of information obtained. If a one-time contact is encountered for a second time and again provides information of value, then the contact may be thereafter treated as a continuous contact.

5-10. A walk-in is a one-time contact who volunteers information of value to US forces on his own initiative. The walk-in source may volunteer information by approaching an HCT, other ISR elements, or US forces or civilian personnel anywhere in the AO. Each unit must have in place a program to identify, safeguard, and direct the walk-in to the appropriate collection asset, to be screened and debriefed as required. For example, a walk-in who wanted to report a crime would be directed to the PMO rather than to a HUMINT collector.

5-11. The collection asset will screen the walk-in to determine the type of information the source has and to determine and evaluate the reliability of the individual. After identifying the type of information, the collector determines if he has the jurisdiction to collect that information. If, for example, the walk-in wishes to report a crime, the collector refers that individual to the proper criminal investigative agency.

5-12. Systematic questioning, deception detection techniques, and cross-checking of information are used extensively in the evaluation process. Concurrently, there are national level directives, DOD directives, and Army regulations that direct specific actions to be taken with a walk-in. When dealing with a walk-in source, HUMINT collectors must guard against adversary intelligence collection. They must also protect legitimate sources of information. The walk-in is thoroughly debriefed on all areas of information relevant to collection requirements, and any information of value is reported.

5-13. On occasion, the HUMINT collector may determine that a one-time contact has the potential to become a continuous contact or a formal contact. This is referred to as a developmental lead. A developmental lead is an

individual identified through social and professional status, leads, source profiling, or other techniques, who has knowledge required by the commander. A developmental lead is any person the HUMINT collector expects to see or would like to see again, or a person who indicates that they intend to return in the future.

5-14. When a HUMINT collector identifies a developmental lead, he reports his interest in elevating the source to continuous or formal contact status as soon as possible to the OMT. Although not every developmental lead becomes a source of information, the HUMINT collector should see each developmental lead as a potential source of information and apply the appropriate security measures. The developmental lead is continuously assessed to verify his placement and access to the type of information the HCT is seeking. Additionally, the HUMINT collector continuously assesses the motivation and characteristics of the developmental lead.

5-15. A one-time source cannot be tasked to collect information, but can be sensitized to information in which the HUMINT collector is interested. For example, if a walk-in source provides information on activity in a house in his neighborhood, he might ask if the collector would be interested in more of the same type information in the future. The HUMINT collector cannot tell him to go get more information, but can indicate that he would listen if the walk-in returned with more information on the topic. If the walk-in returns a second time, he must be handled as a continuous contact.

CONTINUOUS CONTACTS

5-16. Continuous contacts are individuals who have been identified as having more information than could be obtained through a one-time contact, and have been met again by HUMINT collection personnel for the purpose of collecting additional information. HUMINT collectors do **not** task continuous contacts, but they can be sensitized in the same way as one-time contacts. Continuous contacts provide their knowledge through informal debriefings and elicitation.

5-17. All contacts who are seen more than once by HUMINT collectors must be tracked by registering them in the Source Registry and reporting the contacts to the OMT. As an example, a one-time contact who reported information to a HCT contacts them again with follow-up information. That person will now be registered as a continuous contact and tracked by the OMT. This registration process helps to prevent the same information from being collected by multiple collectors from the same contact without realizing it. See AR 381-172 (S//NF) and FM 34-5 (S//NF) for further information on source registration and for the required forms. Types of continuous contacts are discussed below.

Local National and Third-Country National Employees

5-18. Local national and third-country national employees are non-US personnel from either the country in which the US forces are operating or a third country who are either employed by US forces directly or through a contractor to provide logistical support and services. One of the purposes of locally employed personnel screening is to assess these individuals as

potential sources of information. Local national and third-country national employees can be a prolific source of information about local attitudes and events, particularly in a restrictive environment where US contact with the local population is curtailed. Their information can also be significant in a force protection role. The HUMINT collector must register these individuals with the J/G2X. While the HUMINT collector is assessing the local national employee as an intelligence source, CI agents are assessing the same source pool as potential security risks.

5-19. Coordination between HUMINT collectors and CI elements is essential for deconfliction and to avoid duplication of effort. If the HUMINT collector identifies an employee that may be of CI interest, he should immediately notify the appropriate CI unit.

Displaced Personnel and Refugees

5-20. DPs and refugees are excellent sources of information about denied areas and can be used to help identify threat agents and infiltrators. The degree of access HUMINT collectors have to DPs is dependent on the OPORDs, ROE, and SOFAs in effect. HUMINT collectors can work with CA or other programs dealing with DPs or refugees.

5-21. DPs and refugees are normally considered one-time sources but may be incorporated into other long-term collection programs if their degree of knowledge warrants this. In this case, adherence to the restrictions involving source operations is necessary. Those restrictions can be found in AR 380-10, AR 381-100 (S//NF), DIAM 58-11 (S//NF), DIAM 58-12 (S//NF), and other publications as well as existing ROE and SOFAs.

US Forces

5-22. US forces have many opportunities to interact with the local population in the normal course of their duties in operations. This source perhaps is the most under-utilized HUMINT collection resource. Some US forces, such as combat and reconnaissance patrols, are routinely tasked and debriefed by the appropriate level G2/S2. Others, such as medical teams or engineers who have extensive contact with the local population, should also be debriefed.

5-23. Commanders and staff members who serve as liaison with the local population and local government officials can be fruitful sources of information. CA, PSYOP, MP, and other elements also have legitimate reasons to conduct liaison with local authorities and should be debriefed as appropriate. The friendly force debriefing effort can succeed only with command emphasis.

5-24. HUMINT collection elements need to coordinate with local units to identify those individuals who would be most profitable to debrief and to further coordinate with them for time to conduct the debriefing. Although the S2 and S3 can and should task their soldiers to conduct collection tasks during the course of their normal duties, HUMINT collectors must ensure that their friendly force debriefing effort does not interfere with the primary mission accomplishment of the soldiers being debriefed. HCTs should ensure that the necessary staff S2s and S3s are aware of the HUMINT collection

requirements and request that the staffs incorporate these into their respective collection taskings. The results of debriefings by units should also be disseminated to the HCTs for source development, collection targeting, and analysis.

Official Liaison

5-25. Liaison with local military, government, or civilian agency officials provides an opportunity to collect information required by the commander. The HUMINT collector meets with these officials to conduct liaison, coordinate certain operations, collect information, and obtain leads to potential sources of information. Elicitation is the primary technique used with liaison contacts, although in many cases there is a more formal exchange of information. Information obtained by these elements through liaison normally tends to reflect the official positions of their superiors and may not be entirely accurate or complete.

Detainees

5-26. A detainee is any person captured or otherwise detained by an armed force. An EPW is a detainee who meets the criteria of Articles 4 and 5 of the GPW. (See Appendix A.) Detainees may be interrogated. They are frequently excellent sources of information but in many instances the access of the HUMINT collector to the detainees may be curtailed.

5-27. For example, when supporting a counterinsurgency, the supported government may consider all captured insurgents to be criminals and not allow US forces access to them. In these instances, US HUMINT collectors should attempt to sit in during local questioning; they could submit questions or, at a minimum, coordinate to receive the reports from local authority questioning. US HUMINT collectors must remember that regardless of the legal status of the detainees they must be treated in a manner consistent with the Geneva Conventions. (See Appendix A.)

FORMAL CONTACT

5-28. Formal contacts are individuals who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. HUMINT collectors who have met with a particular continuous contact three or more times should consider assessing him for use as a formal contact. Formal contacts meet repeatedly with HUMINT collectors, and their operation and tasking must be carried out in accordance with AR 381-172 (S//NF), DIAM 58-11 (S//NF), and DIAM 58-12 (S//NF).

5-29. Formal contacts are generally local nationals or third-country national employees. Knowledge of their meeting with HUMINT collectors is restricted. This can be accomplished by either disguising the fact that the HUMINT collection personnel are indeed HUMINT personnel, or by concealing the purpose of overt meetings with HUMINT personnel. HCTs take extraordinary measures to protect their relationship with these contacts. Depending on METT-TC factors, meetings with formal contacts may range from overt meetings, which are conducted discreetly in order to protect the

relationship between the source and HUMINT collectors, to meetings whereby only the collector and the source know the meeting has occurred. When contact operations are conducted using this methodology, the operation must be coordinated in accordance with the Under Secretary of Defense for Intelligence (USD(I)) policy cited in Appendix J. Specific direction regarding documentation required for recruitment, and the designation of approval authority (usually the J/G2X) for recruitment of a formal contact, will be specified in Appendix 5 (HUMINT) of Annex B (Intelligence) to the governing OPLAN or OPORD.

DEBRIEFING OPERATIONS

5-30. Debriefing operations refer to the systematic questioning of individuals not in the custody of the US, to procure information to answer collection tasks by direct and indirect questioning techniques. The primary categories of sources for debriefings are friendly forces and civilians including refugees, DPs, and local inhabitants.

5-31. Debriefing operations are those operations directed towards collecting information from a segment of the target population using primarily debriefing techniques. These debriefing operations are separate from the G2/S2 debriefing program to debrief personnel returning from missions. Debriefing operations often include the debriefing of personnel who may not usually be debriefed as part of their assigned duties.

5-32. Normally Army debriefing operations will be directly related to collection tasks at the operational and tactical levels. Strategic debriefing of high-level personnel in response to theater and national level requirements is often under the purview of the DIA/DH. Army HUMINT collectors frequently participate in this type of collection, which is under the control, rules, regulations, and operational guidance of DH.

PRINCIPLES AND GUIDELINES

5-33. Debriefing operations are conducted under the guidelines of DIAM 58-11 (S//NF) and DIAM 58-12 (S//NF). They are further subject to applicable execute orders and the specific ROE and classified "umbrella concept" that apply to the specific AO.

OPERATIONAL CONSIDERATIONS AND REQUIREMENTS

5-34. Debriefing requires relatively unconstrained access to the target audience. Debriefing operations are frequently constrained by the umbrella concept, overt operational proposal (OVOP), and OPORDs. Debriefing is a time- and resource-demanding operation that often shows limited immediate results. Since the potential target audience is so large, debriefing operations require careful planning and careful screening and selection of specific targets.

DEBRIEFING OPERATIONS AT THE TACTICAL LEVEL

5-35. Debriefing operations at the tactical level include the debriefing of elements of the local and transient civilian population in support of ongoing tactical operations. This is different from but often supportive of tactical SCOs as described in Chapter 1. Although tactical SCOs use specific identified sources to obtain and report information, tactical debriefing operations use one-time and continuous contacts to answer requirements. Tactical debriefing operations are frequently combined with tactical interrogation operations and may identify potential sources for tactical SCOs.

REFUGEE FACILITY AND CHECKPOINT OPERATIONS

5-36. Refugee facility and checkpoint operations involve placing HCTs at points where US forces expect to encounter large numbers of refugees. Deployment of HUMINT collectors at checkpoints is normally preferred due to their ability to collect and report more timely information. As in the questioning of detainees, the debriefing of refugees should not delay their movement out of the danger area.

5-37. Checkpoint debriefing is normally done in coordination with MP or combat forces that are manning the checkpoint. Debriefing at refugee camps is used to obtain longer term and less immediate information. HUMINT collection units established at refugee camps coordinate their activities with the CA, MP, NGO, or other organizations that has responsibility for operating the refugee camp.

5-38. In internment facilities operated by the MPs, HUMINT collectors coordinate with MPs for access to the detainees and for guard support. In facilities operated by NGOs, HUMINT collectors coordinate with NGOs for permission to speak to the refugees. NGOs are civilian agencies and may decide not to permit HUMINT collectors to have access to refugees.

FRIENDLY FORCE DEBRIEFING

5-39. Every member of the friendly force is a potential source for HUMINT collection. Friendly force personnel frequently have contact with the threat, civilian population, or the environment. Although many individuals report their information in the form of combat information, many do not report the information, do not realize its significance, or do not know how to report key information. Frequently a systematic questioning by a trained HUMINT collector will identify key information that can contribute to the intelligence picture and help an individual recall details. It also helps to place his information into a systematic format for the analyst to use.

5-40. HUMINT collectors debrief selected friendly force personnel including combat patrols, aircraft pilots and crew, long-range surveillance teams, deep insert special forces teams, and other high-risk mission personnel. Often the personnel assigned to a sector of responsibility are the first to notice changes in the attitude of the local populace or differences in the mission environment.

5-41. They are also able to provide indicators concerning the mission environment. HUMINT collectors also conduct debriefings of returned

prisoners of war (POWs), freed hostages, returned US defectors, and soldiers reported as missing in action. These debriefings help to determine enemy methods of operations, enemy intentions, POW handling and interrogations, enemy weaknesses, information concerning other POWs not returned, and battle damage assessment (BDA).

5-42. HUMINT assets lose access to valuable information if they are not regularly coordinating with the following elements:

- **Cavalry Troops, Unit Patrols, and Scouts.** Unit patrols and scouts have a unique view of the battle area that sensors cannot detect. During operations, units and scouts often patrol villages or populated areas that are contentious and therefore of interest. The unit will gain valuable information on the current status of the AO, potentially answering intelligence requirements, through mission reporting and debriefing by their unit S2 or HUMINT collector.
- **Military Police.** HUMINT collection assets work with the MPs who gain area knowledge through their extensive foot patrols and vehicular convoys. MPs also staff checkpoints and traffic control points (TCPs) where they interact with large numbers of the civilian populace and encounter people and situations that often answer intelligence requirements. MP guards at any internment facility are a valuable source of information on the attitude and behavior of detainees. HUMINT collectors should coordinate with the MP detainee facility commander in order to obtain information on detainees obtained through custodial observation and conversations.
- **Civil Affairs.** CA units have daily interaction with the civilian populace including key members of the civilian community such as politicians, technical personnel, and military leadership.
- **Psychological Operations.** PSYOP teams often interview civilians on the battlefield to determine the effectiveness of friendly and threat PSYOP campaigns. PSYOP elements also gather information on political, social, and other PSYOP requirements. PSYOP elements produce and disseminate intelligence products based partially on their interaction with the civilian populace.
- **Special Operations Forces.** The Special Operations Forces (SOF) team often has greater access to humans and areas on a battlefield than any other collection asset. Their observation of and interaction with the local population provides them access to information that often answers collection requirements. The following are examples of these types of collection missions:
  - Special reconnaissance missions into denied territory to satisfy intelligence gaps or to confirm information from another source.
  - Unconventional warfare (UW) missions normally of a long duration. SOF are inserted into hostile territory to conduct sensitive operations that support US tactical and national objectives. During these missions, SOF units often come in contact with the local population and gather information that meets intelligence requirements.
- **Long-Range Surveillance.** Direct observation and reporting on targets such as activities and facilities may provide timely and

accurate intelligence to support a decision or cross-cue other collection capabilities. Long-range surveillance (LRS) is often employed when discreet observation of an activity is necessary over a long period of time or when a collection system that can respond to redirection is necessary.

- **Criminal Intelligence Operations.** CID personnel, in cooperation with MP soldiers, play a key role by linking criminal intelligence to specific groups and events. The criminal intelligence collection effort specifically targets weapons, drugs, organized crime, and identities of smuggling routes. The identification of smuggling routes results in a significant increase in numbers of weapons being confiscated. The timely transfer of criminal intelligence products to tactical units enables a rapid response to serious confrontations, increased confiscation of arms and ammunition, and improved stability in a TF and AO. The Fusion Cell within the ACE develops intelligence products from national, theater, and operational sources. Due to the significant threat that criminal elements pose, CID military agents and CID civilian analysts may be attached to the Fusion Cell to facilitate the police intelligence function.

STRATEGIC DEBRIEFING OPERATIONS

5-43. Strategic debriefing is debriefing activity conducted to collect information or to verify previously collected information in response to national or theater level collection priorities. This avoids surprises of a strategic nature and is used to support long-range strategic planning. Strategic debriefing is conducted in peacetime as well as in wartime. It often fills intelligence gaps on extremely sensitive topics or areas. The sources for strategic debriefing include but are not limited to émigrés, refugees, displaced persons, defectors, and selected US personnel. Strategic debriefing guidance is provided in DIAM 58-11 (S//NF), DIAM 58-12 (S//NF), and DODD 3115.09, "DOD Intelligence, Interrogations, Detainee Debriefings, and Tactical Questioning."

5-44. Strategic debriefing is conducted in a non-hostile, business-like manner. The rapport posture is usually amicable as the source is usually willingly answering national level intelligence needs. Although voluntary sources may not be motivated by a desire for money or other material incentives, it is necessary to ensure that any promised incentives are delivered. The time used in a strategic debriefing can range from days to years. Sources typically have high-level backgrounds in scientific, industrial, political, or military areas.

5-45. Information gathered as strategic intelligence is categorized into eight components. Each of these components can be divided into subcomponents. These components and subcomponents are neither all-encompassing nor mutually exclusive. This approach enhances familiarization with the types of information included in strategic intelligence. An easy way to remember these components is the acronym "**BEST MAPS**":

Biographic Intelligence
Economic Intelligence
Sociological Intelligence
Transportation and Telecommunications Intelligence

Military Geographic Intelligence
Armed Forces Intelligence
Political Intelligence
Science and Technological Intelligence

- **Biographic intelligence** is the study of individuals of actual or potential importance through knowledge of their personalities and backgrounds. For further guidance on collecting and reporting biographic intelligence, see DIAM 58-12 (S//NF). The subcomponents are—
  - Educational and occupational history—civilian and military backgrounds of individuals.
  - Individual accomplishment—notable accomplishments of an individual's professional or private life.
  - Idiosyncrasies and habits—mannerisms and unusual lifestyles.
  - Position, influence, and potential—present and/or future positions of power or influence.
  - Attitudes and hobbies—significant interests that may affect an individual's accessibility.
- **Economic intelligence** studies economic strengths and weaknesses of a country. The subcomponents are—
  - Economic warfare—information on the diplomatic or financial steps a country may take to induce neutral countries to cease trading with its enemies.
  - Economic vulnerabilities—the degree to which a country's military would be hampered by the loss of materials or facilities.
  - Manufacturing—information on processes, facilities, logistics, and raw materials.
  - Source of economic capability—any means a country has to sustain its economy (for example, black market trade, legitimate business or trades, and imports and exports).
- **Sociological intelligence** deals with people, customs, behaviors, and institutions. The subcomponents are—
  - Population—rates of increase, decrease, or migrations.
  - Social characteristics—customs, morals, and values.
  - Manpower—divisions and distribution within the workforce.
  - Welfare—health and education.
  - Public information—information services within the country.
- **Transportation and telecommunications intelligence** studies systems dedicated to and used during military emergencies and peacetime.

- **Military geographic intelligence** studies all geographic factors (physical and cultural) that may affect military operations. Physical geography is concerned with natural or manmade geophysical features. Cultural geography provides demographics information.
- **Armed forces intelligence** is the integrated study of the ground, sea, and air forces of the country. The subcomponents are—
  - Strategy—military alternatives in terms of position, terrain, economics, and politics.
  - Tactics—military deployments and operations doctrine.
  - OB—location, organization, weapons, strengths.
  - Equipment—analysis of all military materiel.
  - Logistics—procurement, storage, and distribution.
  - Training—as carried out at all echelons to support doctrine.
  - Organization—detailed analysis of command structures.
  - Manpower—available resources and their conditioning.
- **Political intelligence** studies all political aspects which may affect military operations. The subcomponents are—
  - Government structure—organization of departments and ministries.
  - National policies—government actions and decisions.
  - Political dynamics—government views and reactions to events.
  - Propaganda—information and disinformation programs.
  - Policy and intelligence services—organization and functions.
  - Subversion—subversive acts sponsored by the government.
- **Science and technological intelligence** studies the country's potential and capability to support objectives through development of new processes, equipment, and weapons systems. The subcomponents are—
  - Weapons and weapon systems.
  - Missile and space programs.
  - Nuclear energy and weapons technology.
  - NBC developments.
  - Basic applied science.
  - Research and development systems.

LIAISON OPERATIONS

5-46. Liaison is conducted to obtain information and assistance, to coordinate or procure material, and to develop views necessary to understand counterparts. Liaison contacts are normally members of the government, military, law enforcement, or other member of the local or coalition infrastructure. The basic tenet of liaison is *quid pro quo*. An exchange of information, services, material, or other assistance is usually a part of the transaction. The nature of this exchange varies widely depending upon the culture, location, and personalities involved.

5-47. Because the nature of liaison tasks varies widely, the general goals of the liaison operation and the objective of each liaison contact should be

clearly defined. The objective should include the type of information to be collected, methods of operations unique to the area, and the command objectives. Additionally, the collector should know limitations on liaison activities. These limitations include—

- Prohibitions against collecting certain types of information or contacting certain types of individuals or organizations.
- Memorandums of understanding with other echelons which delineate each echelon's AOR and AORs for subordinate units.
- Coordination requirements per DCID 5/1 dated 19 December 1984, which are required for selected types of liaison activities.

5-48. Administrative considerations include—

- Type, method, and channels of reporting information obtained from liaison activities.
- Project and contingency fund site numbers to be used.
- Funding and incentive acquisition procedures.
- Limitations on the use of ICFs or incentives.
- Reporting system used.
- Authority under which the specific liaison program is conducted and guidelines for joint and combined operations are set.

5-49. Benefits of liaison include—

- Establishing working relations with various commands, agencies, or governments.
- Arranging for and coordinating joint and combined operations.
- Exchanging operational information and intelligence within legal limits.
- Facilitating access to records and personnel of other agencies not otherwise accessible.
- Acquiring information to satisfy US requirements.
- Accessing a larger pool of information.

INTERROGATION OPERATIONS

5-50. HUMINT interrogation is the systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Interrogation is to be conducted by personnel trained and certified to use legal, approved methods of convincing EPWs/detainees to give their cooperation. Interrogation sources are detainees, including EPWs.

5-51. Definitions of EPWs and rules for their treatment are contained in the Geneva Convention Relative to the Treatment of Prisoners of War (GPW). The definition and rules for the treatment of civilians are contained in the

Geneva Conventions Relative to the Protection of Civilian Persons in Time of War (GC). (See Appendix A.) For persons covered by those Conventions, applicable GPW and GC provisions must be adhered to at all times. (Regarding treatment of detained personnel, see also paragraph 5-74.)

5-52. There is an additional protocol to the Geneva Conventions called Protocol I Additional to the Geneva Conventions, 1977, which also contains definitions of who is a civilian and who is an EPW (Articles 50 and 44). The US has not ratified Protocol I nor does it accept the expanded definition of EPWs that it contains. Requirements managers, J/G/S2X personnel, and HUMINT collectors should understand, however, that coalition military personnel with whom they may work may be bound by Protocol I, and those coalition personnel may be required to treat additional personnel as EPWs. Any questions concerning the GPW and Protocol I must be directed to the SJA office for clarification.

5-53. Interrogation operations are specific operations normally conducted at detainee collection facilities directed at the wide-scale collection of information from detainees using interrogation techniques. Although field interrogations are conducted at all echelons and during all operations in which there are detainees, detention facilities where interrogation operations occur are normally located only at theater or JTF level.

5-54. Compliance with laws and regulations, including proper treatment of detainees, is a matter of command responsibility. Commanders have an affirmative duty to ensure their subordinates are not mistreating detainees or their property. HCT leaders must effectively supervise their subordinate collectors during all interrogation operations. Supervisors must ensure that each HUMINT collector has properly completed an interrogation plan and sound collection strategy, and fully understands the intelligence requirements he is seeking to satisfy prior to beginning an interrogation. NCOs and WOs should regularly participate in interrogations with their subordinates to ensure that the highest standards of conduct are maintained. Interrogation supervisors should also monitor interrogations by video, where video monitoring is available. The production, use, and dissemination of interrogation videos must be tightly controlled by HCT leaders. Such videos must not be released for dissemination outside the Intelligence Community without the express permission of the SECDEF or his delegate.

NON-DOD AGENCIES

5-55. Non-DOD agencies may on occasion request permission to conduct interrogations in Army facilities. These requests must be approved by the JTF commander or, if there is no JTF commander, the theater commander or appropriate higher level official. The interrogation activity commander will assign a trained and certified interrogator to escort non-DOD interrogators to observe their interrogation operations. The non-DOD personnel will sign for any detainee they want to question from the MPs, following the same established procedures that DOD personnel must follow. In all instances, interrogations or debriefings conducted by non-DOD agencies will be observed by DOD personnel. In all instances, non-DOD agencies must observe the same standards for the conduct of interrogation operations and

treatment of detainees as do Army personnel. All personnel who observe or become aware of violations of Army interrogation operation standards will report the infractions immediately to the commander. The personnel who become aware of mistreatment of detainees will report the infractions immediately and suspend the access of non-DOD personnel to the facility until the matter has been referred to higher headquarters. Non-DOD personnel conducting interrogation operations in an Army facility must sign a statement acknowledging receipt of these rules, and agree to follow them prior to conducting any interrogation operations. Non-DOD personnel working in DOD interrogation facilities have no authority over Army interrogators. Army interrogators (active duty, civilian, or contractor employees) will only use DOD-approved interrogation approaches and techniques.

FOREIGN GOVERNMENT INTERROGATORS

5-56. Foreign governments may request to participate, or may be invited to participate in interrogations in Army facilities. Requests for foreign government access to detainees will be forwarded through the operational chain of command for appropriate action pursuant to DOD policy. Foreign government personnel must comply with US DOD policies and observe the same standards for the conduct of interrogation operations and treatment of detainees as do Army personnel. The interrogation activity commander will assign a trained and certified interrogator to escort foreign government interrogators to observe their interrogation operations. The foreign government personnel will sign for any detainee they want to question from the MPs, following the same established procedures that US DOD personnel must follow. In all instances, interrogations or debriefings conducted by foreign government interrogators will be observed by US DOD personnel. In all instances, foreign government interrogators must observe the same standards for the conduct of interrogation operations and treatment of detainees as do US Army personnel.

MP FUNCTIONS IN ASSOCIATION WITH INTERROGATION OPERATIONS

5-57. MP and MI personnel both have responsibilities with regard to EPW/detainees, but with different goals and responsibilities. (See DOD Directive 3115.09.) Therefore, close coordination must occur between MP and MI personnel in order to facilitate the effective accomplishment of the MP and MI missions. Both MP and MI personnel must ensure that they treat detainees in accordance with the baseline standards of humane treatment.

5-58. MPs are responsible for the humane treatment, evacuation, custody and control (reception, processing, administration, internment, and safety) of detainees; force protection; and the operation of the internment facility, under the supervision of the provost marshal. The MPs do not conduct intelligence interrogations. Intelligence interrogation is strictly a HUMINT function. DOD policy requires that all detainees in its control, whether or not interrogation has commenced, are assigned an internment serial number as soon as possible, normally within 14 days of capture. (See AR 190-8.)

5-59. The standard MP security and internment functions are the only involvement the MPs have in the interrogation process. MPs will not take any actions to set conditions for interrogations (for example, "softening up" a detainee). For purposes of interrogation, military working dogs will not be used.

5-60. MPs may support interrogators as requested for detainee custody, control, escort, and/or additional security (for example, for combative detainees). When interrogators promise an incentive to a detainee, the interrogators must coordinate with the MPs to ensure that the detainee receives the incentive and is allowed to retain it. MPs may provide incentives in support of interrogation operations under the following conditions:

- Using incentives is coordinated with and approved by the MP facility commander.
- Providing and withdrawing incentives does not affect the baseline standards of humane treatment. This means that MPs can provide incentives such as special food items. However, when the incentive is withdrawn, the MPs still must provide the normal rations.
- Using incentives does not violate detainee custody and control or facility security. This means that if a HUMINT collector requests MPs to provide an incentive (for instance, specialty food) but the detainee has been spitting on the guards, then MPs would not provide the incentive because it might reinforce inappropriate behavior.

5-61. MPs exercise the overall responsibility for the safety of detainees, even in those cases in which detainees are in the temporary custody of HUMINT collectors or other agency personnel for the purpose of interrogation. HUMINT collectors should arrange with the MP supervisor to debrief MP guards. Guards who observe and interact with detainees can report the detainees' disposition, activities, mood, and other observable characteristics.

5-62. HUMINT collectors conduct interrogations for intelligence information. They normally work within the confines of the detainee detention facility, but have no involvement in the mission of the security of detainees. MPs follow a strict protocol concerning access to detainees. Accompanied and unaccompanied access to detainees must be coordinated and approved in advance by the MP commander responsible for the detainees or that commander's designated representative.

5-63. When HUMINT collectors coordinate for a detainee interrogation in an internment facility, the MPs escort the detainee to the interrogation site, which is collocated with, or located within the internment facility. MPs verify that the HUMINT collector is authorized access to the detainee. Depending on security concerns, the HUMINT collector may request that the MP remain, or he may request the MP depart until the detainee needs to be returned to the living area. If the MP remains, his functions are to maintain the security, accountability, and safety of the detainee and the safety of the interrogator, interpreter, and others in the interrogation site. The MP will perform no role in the interrogation. When conducting interrogations in a holding area such as a detainee collection point (DCP), MPs may not be available to provide security for interrogation operations. In that case, the

HUMINT collector will need to arrange for security from the unit that has established the holding area.

5-64. If the MP departs the immediate area where the detainee is being questioned (for example, asked to wait outside the interrogation room), the HUMINT collector will assume custody and responsibility for the detainee by signing for the detainee, noting the detainee's physical condition.

5-65. SOPs should be written to comply with a requirement that interrogation operations will always be under observation, whether conducted in fixed sites, holding areas, or in the field. Physical setup and logistical availability will dictate whether observation is conducted directly, from a concealed location, or by video monitoring. HUMINT collectors should never be alone with a detainee without being under observation.

5-66. Once a HUMINT collector has assumed custody of a detainee, he will not turn the detainee over to anyone other than an MP. Specifically, he will not allow another government agency to assume custody from him. The HUMINT collector will instead return the detainee to the custody of the MP, and the agency seeking custody of the detainee will then be required to do so from the MP. Likewise, HUMINT collectors will not assume custody of a detainee directly from another government agency, but will require them to return the detainee directly to the custody of the MP.

LEGAL, REGULATORY, AND POLICY PRINCIPLES AND GUIDELINES

5-67. The GPW (Appendix A, Section I), the GC (Appendix A, Section III), and the UCMJ are relevant documents pertaining to interrogations of detainees.

5-68. The approaches, psychological techniques, and other principles presented in this manual must be conducted in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. US policy is to treat all detainees and conduct all interrogations, wherever they may occur, in a manner consistent with this commitment. Authority for conducting interrogations of personnel detained by military forces rests primarily upon the traditional concept that the commander may use all available resources and lawful means to accomplish the mission and to protect and secure the unit.

"Prisoners of war do not belong to the power for which they have fought; they are all under the safeguard of honor and generosity of the nation that has disarmed them."

—Napoleon, The Military Maxims of Napoleon 1927, ed. Burnod

POINT OF CAPTURE THROUGH EVACUATION

MP Functions	HUMINT Functions
• Maneuver and Mobility Support Operations • Area Security • Internment and Resettlement Operations • Law and Order Operations • Police Intelligence Operations • Ensure detainee abuse is avoided and reported	• Screen and question detainees at TCPs and checkpoints • Question contacts, local civilians, refugees, and EPWs • Conduct liaison with military and civilian agencies • Report information obtained • Ensure detainee abuse is avoided and reported • Support DOCEX

DETENTION FACILITY

MP Functions	HUMINT Functions
• Detain and guard EPWs, civilian internees, and other detainees • Conduct reception and processing • Coordinate Classes I, II, and VIII supplies • Coordinate NGOs, PVOs, and interagency visits • Ensure detainee abuse is avoided and reported • Transport detainees within the detention facility to interrogation area • Maintain security during interrogation operations	• Debrief guards • Screen detainees and EPWs for PIR and IR • Provide linguist support when possible • Observe detainees under MP control • Ensure detainee abuse is avoided and reported • Conduct interrogations • Report information obtained • Cross-cue other intelligence disciplines (as needed) • Support DOCEX

Figure 5-1. MP vs HUMINT Responsibilities.

5-69. The Geneva Conventions establish specific standards for humane care and treatment of enemy personnel captured, retained, or detained by US military forces and its allies. All persons who have knowledge of suspected or alleged violations of the Geneva Conventions are obligated by regulation to report such matters through command channels or to designated individuals, such as the SJA or IG. For example, HUMINT collectors who are working with others must ensure that no incidents of detainee abuse occur, whether committed by a fellow HUMINT collector, an interpreter, HN or coalition personnel, MP, representative of another government agency, or anyone else.

5-70. Failure to report a suspected or alleged violation of the law of war may subject the service member to disciplinary actions. Violations of the Geneva Conventions committed by US personnel may constitute violations of the UCMJ. The commander is responsible for ensuring that the forces under his command comply with the Geneva Conventions. If violations occur in the conduct of warfare, the commander bears primary responsibility for investigating and taking appropriate action with respect to the violators.

5-71. Every soldier has the duty to report serious incidents, whether observed or suspected, in accordance with AR 190-40. Such incidents are reported to the chain of command. If the chain of command itself is

implicated, the soldier can report the incident to the SJA, IG, chaplain, or provost marshal.

5-72. There are reasons for reporting serious incidents beyond those related to legal requirements. For instance, the publishing of enemy war crimes can be used to influence public opinion against the enemy. Also, reporting war crimes of other countries provides important information that may become relevant, since we would not be able to transfer detainees to any power that we could not rely on to treat them appropriately under the law of war, including the Geneva Conventions.

5-73. Several articles of the GPW apply to HUMINT collectors and interrogation operations. Excerpts from some of the most relevant articles of the Geneva Conventions are listed below. Although the following excerpts are specific to EPWs, service members must treat all detainees captured during armed conflict consistent with the provisions of the GPW unless a determination to the contrary is made. Moreover, US policy requires that US forces apply the principles of the Geneva Conventions, during military operations. (See Appendix A.)

- Article 5 - Should any doubt arise as to whether persons having committed a belligerent act and having fallen into the hands of the enemy, belong to any of the categories enumerated in Article 4, such persons shall enjoy the protection of the present Convention until such time as their status has been determined by a competent tribunal.
- Article 13 - PWs must at all times be treated humanely. Any unlawful act or omission by the Detaining Power causing death or seriously endangering the health of a PW in its custody is prohibited. Likewise, PWs must at all times be protected, particularly against acts of violence or intimidation and against insults and public curiosity.
- Article 14 - PWs are entitled, in all circumstances, to respect for their persons and honor. Women shall be treated with all regard due to their sex, and shall in all cases benefit by treatment as favorable as that granted to men.
- Article 15 - The Power detaining PWs shall be bound to provide, free of charge, for their maintenance and medical attention required by their state of health.
- Article 17 - This article covers several requirements with direct impact on interrogation.
  - Every PW, when questioned on the subject, is bound to give only his surname, first names and rank, date of birth, and army, regimental, personal or serial number, or failing this, equivalent information. If he willfully infringes this rule, he may render himself liable to a restriction of the privileges (emphasis added) accorded to his rank or status.
  - For example, this does not mean if a prisoner fails to give this information he loses status as a prisoner, only special privileges. An example might be an officer who fails to identify himself as such. An officer cannot be compelled to work (Article 49). An officer who fails to identify himself as such could lose this privilege.

  - The questioning of PWs shall be carried out in a language they understand.
  - No physical or mental torture or any other form of coercion may be inflicted on EPWs to secure from them information of any kind whatever. PWs who refuse to answer may not be threatened, insulted, or exposed to unpleasant or disadvantageous treatment of any kind.
- Article 18 - All effects and articles of personal use, except arms, horses, military equipment and documents, shall remain in the possession of PWs, likewise their metal helmets and protective masks and like articles issued for personal protection. Effects and articles used for their clothing or feeding shall also remain in their possession, even if such effects and articles belong to their regulation military equipment.
  - Badges of rank and nationality, decorations and articles having above all a personal or sentimental value may not be taken from PWs.
  - Sums of money carried by PWs may not be taken away from them except by order of an officer, and after the amount and particulars of the owner have been recorded in a special register and an itemized receipt has been given, legibly inscribed with the name, rank, and unit of the person issuing said receipt. (Note: Unit SOP should require initial impounding of all sums of money from detainees, properly documented and accounted for, in order to prevent detainees from using money to buy influence of any kind, or participate in black market or other improper activity.)
- Article 19 - PWs shall be evacuated, as soon as possible after their capture, to camps situated in an area far enough from the combat zone for them to be out of danger. Only those PWs, who, owing to wounds and sickness, would run greater risks by being evacuated than by remaining where they are, may be temporarily kept back in a danger zone.
- Article 33 - Medical personnel and chaplains, while retained by the Detaining Power with a view to assisting PWs, shall not be considered as PWs. They shall, however, receive as a minimum, the benefits and protection of the Geneva Convention. They shall continue to exercise their medical and spiritual functions for the benefits of PWs.

5-74. **All captured or detained personnel, regardless of status, shall be treated humanely, and in accordance with the Detainee Treatment Act of 2005 and DOD Directive 2310.1E, "Department of Defense Detainee Program," and no person in the custody or under the control of DOD, regardless of nationality or physical location, shall be subject to torture or cruel, inhuman, or degrading treatment or punishment, in accordance with and as defined in US law.** All intelligence interrogations, debriefings, or tactical questioning to gain intelligence from captured or detained personnel shall be conducted in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E,

"The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Use of torture is not only illegal but also it is a poor technique that yields unreliable results, may damage subsequent collection efforts, and can induce the source to say what he thinks the HUMINT collector wants to hear. Use of torture can also have many possible negative consequences at national and international levels.

Cruel, Inhuman or Degrading Treatment Prohibited

All prisoners and detainees, regardless of status, will be treated humanely. Cruel, inhuman and degrading treatment is prohibited. The Detainee Treatment Act of 2005 defines "cruel, inhuman or degrading treatment" as the cruel unusual, and inhumane treatment or punishment prohibited by the Fifth, Eighth, and Fourteenth Amendments to the U.S. Constitution. This definition refers to an extensive body of law developed by the courts of the United States to determine when, under various circumstances, treatment of individuals would be inconsistent with American constitutional standards related to concepts of dignity, civilization, humanity, decency and fundamental fairness. All DOD procedures for treatment of prisoners and detainees have been reviewed and are consistent with these standards, as well as our obligations under international law as interpreted by the United States.[1]

Questions about applications not resolved in the field by reference to DOD publications, must be forwarded to higher headquarters for legal review and specific approval by the appropriate authority before application.

The following actions will not be approved and cannot be condoned in any circumstances: forcing an individual to perform or simulate sexual acts or to pose in a sexual manner; exposing an individual to outrageously lewd and sexually provocative behavior; intentionally damaging or destroying an individual's religious articles.

[1] Nothing in this enclosure should be understood to affect the U.S. obligations under the law of war.

5-75. **If used in conjunction with intelligence interrogations, prohibited actions include, but are not limited to—**

- Forcing the detainee to be naked, perform sexual acts, or pose in a sexual manner.
- Placing hoods or sacks over the head of a detainee; using duct tape over the eyes.
- Applying beatings, electric shock, burns, or other forms of physical pain.
- "Waterboarding."
- Using military working dogs.
- Inducing hypothermia or heat injury.
- Conducting mock executions.
- Depriving the detainee of necessary food, water, or medical care.

5-76. While using legitimate interrogation techniques, certain applications of approaches and techniques may approach the line between permissible actions and prohibited actions. It may often be difficult to determine where

permissible actions end and prohibited actions begin. In attempting to determine if a contemplated approach or technique should be considered prohibited, and therefore should not be included in an interrogation plan, consider these two tests before submitting the plan for approval:

- If the proposed approach technique were used by the enemy against one of your fellow soldiers, would you believe the soldier had been abused?
- Could your conduct in carrying out the proposed technique violate a law or regulation? Keep in mind that even if you personally would not consider your actions to constitute abuse, the law may be more restrictive.

5-77. If you answer yes to either of these tests, the contemplated action should not be conducted. If the HUMINT collector has any doubt that an interrogation approach contained in an approved interrogation plan is consistent with applicable law, or if he believes that he is being told to use an illegal technique, the HUMINT collector should seek immediate guidance from the chain of command and consult with the SJA to obtain a legal review of the proposed approach or technique. (See paras 5-80 and 5-81 for information on responding to illegal orders.) If the HUMINT collector believes that an interrogation approach or technique is unlawful during the interrogation of a detainee, the HUMINT collector must stop the interrogation immediately and contact the chain of command for additional guidance.

CAUTION: Although no single comprehensive source defines impermissible coercion, certain acts are clearly prohibited. Certain prohibited physical coercion may be obvious, such as physically abusing the subject of the screening or interrogation. Other forms of impermissible coercion may be more subtle, and may include threats to turn the individual over to others to be abused; subjecting the individual to impermissible humiliating or degrading treatment; implying harm to the individual or his property. Other prohibited actions include implying a deprivation of applicable protections guaranteed by law because of a failure to cooperate; threatening to separate parents from their children; or forcing a protected person to guide US forces in a dangerous area. Where there is doubt, you should consult your supervisor or servicing judge advocate.

5-78. Security internees are detainees who are not combatants but who pose a security threat, may be under investigation, or who pose a threat to US forces if released. HUMINT collectors are required to treat all detainees humanely. EPWs are entitled to additional protections guaranteed by the GPW that security internees may not be eligible for. For example, allowing a security internee to communicate with a family member (a right that an EPW has under the Geneva Conventions) could allow him to pass information that would compromise a sensitive investigation and endanger the lives of soldiers and civilians. HUMINT collectors should consult with their SJA for clarification of detainees' status and rights.

5-79. HUMINT collectors are employed below brigade level when the combat situation requires limited tactical interrogation at battalion or lower.

HUMINT collectors should also provide training in the area of tactical questioning to designated S2 personnel. The potential for abuse of the detainee is greatest at initial capture and tactical questioning phase. With the excitement and stress of the battlefield, unskilled personnel may exercise poor judgment or be careless and thus resort to illegal techniques to elicit critical information. Personnel who are not trained HUMINT collectors will not attempt to use approach techniques. Instructions must stress the importance of the proper treatment of detainees. Emphasize that in addition to legal requirements, the abuse of a detainee at the initial stage of contact often renders future interrogation futile. All treatment of detainees must be consistent with the Geneva Conventions. (See ST 2-91.6 for further information on tactical questioning.)

5-80. Orders given to treat detainees in any way that violate the Law of War, including the Geneva Conventions, or that result in detainees being treated in any prohibited manner are unlawful. Every soldier must know how to respond to orders that he perceives to be unlawful. If a soldier receives an order that he knows to be unlawful, or that a person of ordinary sense and understanding would know to be unlawful, or if the order is not clear enough to determine if it is legal or not, he should follow the steps set out below (preferably in the order listed):

- Ask for clarification.
- State that the order is illegal if he knows that it is.
- Use moral arguments against the order.
- State the intent to report the act.
- Ask the senior interrogator to stop the act.
- Report the incident or order if the order is not withdrawn or the act in question is committed.
- If there appears to be no other recourse, refuse to obey the unlawful order.

NOTE: If the order is a lawful order, it should be obeyed. Failure to obey a lawful order is an offense under the UCMJ.

5-81. None of the above actions should be taken in the presence of any detainee. Witnessing actions taken to determine the legality of an order may lead to increased resistance of the detainee and could lead to increased resistance throughout the detainee population if they believe they are being treated unlawfully.

5-82. Illegal orders or incidents must be reported to the chain of command. However, if the chain of command itself is implicated, report the incident or order to the SJA, IG, chaplain, or provost marshal.

OPERATIONAL CONSIDERATIONS AND REQUIREMENTS

EPW Evacuation System

5-83. The MPs are responsible for evacuating detainees, civilian internees, and other detainees, as stipulated in AR 190-8. HUMINT collection assets must be placed to take advantage of the evacuation system the MPs will put into place. The evacuation of detainees and civilian internees normally is a slow and cumbersome process that can severely tax a maneuver unit's resources. Appendix D explains the handling of detainees in detail, including the 5Ss—Search, Silence, Safeguard, Segregate, and Speed to the Rear. The 5Ss are authorized with respect to handling detainees for the purposes of movement of detainees and security. The 5Ss are not authorized for use as interrogation approach techniques.

5-84. The initial evacuation of detainees and civilian internees is the responsibility of the capturing unit. That unit is normally responsible for moving the detainees and civilian internees from the point of capture to the nearest DCP. Under MP doctrine, the MPs are responsible for the detention, security, processing, safety, well-being, accountability, and humane treatment of detainees and civilian internees.

5-85. Normally the MPs assume responsibility for the further evacuation of the detainees and civilian internees; however, under certain circumstances, other units could be charged with this task. The detainees are normally evacuated from a DCP to a short-term collection facility and then finally to a theater internment facility. Once the theater internment facility (joint) is established, dependent on METT-TC factors, the internment facility escort guard units may go forward as far as the initial collection points and escort detainees and civilian internees to a short-term collection facility or straight to a theater internment facility.

5-86. Senior MP commanders coordinate and synchronize transportation and security requirements with MP divisional and BCT leaders. It may take 8 hours for a detainee to reach the DCP; 8 to 16 hours more to reach a short-term collection facility; and 24 additional hours to reach the theater internment facility. Mandatory timelines will be determined in command policy guidance. Critical during this process is that MPs work closely with MI, SJA, and interagency personnel to determine the proper status of individuals detained. Determining whether an individual is an EPW, a criminal insurgent, or in another status is crucial to facilitate the release or transportation, holding, and security requirements. This determination will be used when the individual's biometric data is taken and entered into the Biometric Automated Toolset (BAT).

5-87. The HUMINT collection assets need to be positioned to maximize their collection potential and take advantage of the time available during evacuation. The rapidity of operations and the need to facilitate the commander's situational understanding—coupled with the technological innovations that link the HUMINT collector to databases, analysts, and technical support from anywhere on the battlefield—require placing the HCTs forward into brigade and even maneuver battalion areas to provide

immediate access to EPWs/detainees. EPWs/detainees are normally interrogated for tactical information in the maneuver battalion trains areas and then questioned in detail at the theater JIDC.

Security

5-88. When dealing with detainees, the HUMINT collector faces two security considerations: his own physical security and information security. Particularly when operating in support of tactical operations, the HUMINT collector is in close contact with enemy soldiers who could attempt to escape and may attack the HUMINT collector in doing so. Detainees during a stability and reconstruction operation are often people committed to a cause who find themselves in desperate circumstances. Although the detainees are normally under guard, the HUMINT collector must always be alert to any physical threat posed by these individuals. He must also ensure that his own actions do not provide the detainee with the means with which to harm the collector or anyone else.

5-89. The HUMINT collector should also be aware that EPWs and other detainees may attempt to elicit information. Since HUMINT collectors, by virtue of their position, may possess a great deal of classified information, they must be careful not to reveal it unwittingly in the process of questioning a detainee.

PROHIBITION AGAINST USE OF FORCE

Acts of violence or intimidation, including physical or mental torture, or exposure to inhumane treatment as a means of or aid to interrogation are expressly prohibited. Acts in violation of these prohibitions may be a violation of US law and regulation and the law of war, including the Geneva Conventions of 1949, and may be criminal acts punishable under the UCMJ and other US law. Moreover, information obtained by the use of these prohibited means is of questionable value. If there is doubt as to the legality of a proposed form of interrogation, the advice of the SJA must be sought before using the method in question.

Limitations on the use of methods identified herein as expressly prohibited should not be confused with psychological ploys, verbal trickery, or other nonviolent or non-coercive subterfuge used by the trained HUMINT collector in the successful interrogation of hesitant or uncooperative sources. Use of torture by US personnel would bring discredit upon the US and its armed forces while undermining domestic and international support for the war effort. It also could place US and allied personnel in enemy hands at a greater risk of abuse by their captors. Conversely, knowing the enemy has abused US and allied POWs does not justify using methods of interrogation specifically prohibited by law, treaty, agreement, and policy. In conducting intelligence interrogations, the J2/G2/S2 has primary staff responsibility to ensure that these activities are performed in accordance with these laws and regulations. **[*The commander bears the responsibility to ensure that these activities are performed in accordance with applicable law, regulations, and policy. The unit must have an internal SOP for execution of the interrogation mission.]**

The psychological techniques and principles in this manual should neither be confused with, nor construed to be synonymous with, unauthorized techniques such as brainwashing, physical or mental torture, including drugs that may induce lasting or permanent mental alteration or damage. Physical or mental torture and coercion revolve around eliminating the source's free will, and are expressly prohibited by GWS, Article 13; GPW, Articles 13 and 17; and GC, Articles 31 and 32.

> *Torture is an act committed by a person under the color of law specifically intended to inflict severe physical or mental pain and suffering (other than pain or suffering incidental to lawful sanctions) upon another person within his custody or physical control. (Extracted from Title 18 of the United States Code, Section 2340A).*

*Emphasis added for use in this manual.

Capture Rates

5-90. Anticipating not only overall capture rates but also capture rates linked to specific operations is vital to the correct placement of HUMINT collectors supporting interrogation operations. Defensive and stability and reconstructions operations normally provide a small but steady flow of detainees while successful offensive operations can overwhelm HCTs. To be successful, HUMINT collection support to tactical operations must be carefully planned and prioritized. Available HUMINT collection assets must be balanced against the operations objective, enemy situation estimate, and projected EPW capture rates. The unit S2 is responsible for projecting capture rates.

Interrogating Wounded and Injured Detainees

5-91. Commanders are responsible to ensure that detainees receive adequate health care. Decisions regarding appropriate medical treatment of detainees and the sequence and timing of that treatment are the province of medical personnel. Detainees will be checked periodically in accordance with

command health care directives, guidance, and SOPs, applicable to all detainees to ensure they are fit for interrogations. Detainees determined by medical personnel to be medically unfit to undergo interrogation will not be interrogated. Health care personnel will be on call should a medical emergency arise during interrogation. Health care personnel will report detainees' conditions, as appropriate, to the commander. Health care providers shall not be placed in a position to advise on the application or duration of interrogation approach techniques.

5-92. Wounded and otherwise injured detainees can be a valuable source of information. For evacuation purposes, medical personnel may classify detainees as walking wounded or sick or as non-walking wounded or sick. Walking wounded detainees are evacuated through normal evacuation channels. Non-walking wounded are delivered to the nearest medical aid station and evacuated through medical channels.

5-93. HUMINT collectors may interrogate a wounded or injured detainee provided that they obtain permission from a competent medical authority and that the questioning will not delay or hinder medical treatment. Questioning will not delay the administration of medication to reduce pain or the evacuation of the detainee to where they may receive medical treatment, nor will interrogation be allowed if it would cause a worsening of the condition of the detainee. In most cases, this simply requires the HUMINT collector to ask the doctor, medic, or other medical personnel if it is all right to talk to the detainee.

5-94. With the doctor's permission, the HUMINT collector may talk to the detainee before, after, or during medical treatment. The HUMINT collector cannot at any time represent himself as being a doctor or any other type of medical personnel. Nor can he state, imply, or otherwise give the impression that any type of medical treatment is conditional on the detainee's cooperation in answering questions.

TYPES OF INTERROGATION OPERATIONS

5-95. There are two general categories of interrogation operations: **field interrogation operations** and **interrogation facility operations**.

FIELD INTERROGATION OPERATIONS

5-96. Field interrogation operations constitute the vast majority of interrogation operations at echelons corps and below. Field interrogations include all interrogation operations not conducted at a fixed facility. Current doctrine emphasizes the placement of HCTs forward with maneuver units to provide immediate interrogation support while the information is fresh and the detainee may still be susceptible to approaches, due to the shock of capture. The rationale for this method of employment is twofold:

- First, the pace of the modern battlefield no longer allows the luxury of waiting for a detainee to reach a collection point prior to interrogation. Commanders need more timely information, including HUMINT. Also, automated tools and improved communications now permit rapid transmittal of information from forward-deployed HCTs.

- Second, current MP doctrine has the theater level EPW escort companies picking up detainees as far forward as the division forward collection points and bypassing the intervening collection points.

5-97. An added benefit of placing the HCTs with maneuver units is that it allows them to conduct other HUMINT collection activities, such as the debriefing of local civilians and refugees concurrently with interrogation operations. HCTs are allocated to maneuver units based on—

- The relative importance of that subordinate element's operations to the unit's overall scheme of maneuver.
- The potential for that subordinate element to capture detainees, documents, and materiel or encounter civilians on the battlefield.
- The criticality of information obtained from those sources to the success of the parent unit's overall OPLANs.

5-98. As the mission and situation change, the HCTs are redistributed. As MI assets, they should never be kept in reserve.

5-99. During offensive and defensive operations, HCTs normally operate with maneuver brigades and battalions. HUMINT collectors with battalions or brigades should be equipped with vehicles and communications systems that are compatible with the systems organic to the supported unit. HUMINT collectors with brigades and battalions receive their collection priorities from the S2 of the supported unit. In stability and reconstruction operations, the HCTs normally operate in the AOs of battalion and brigade TFs.

INTERROGATION FACILITY OPERATIONS

5-100. Joint interrogation operations are operations conducted at higher echelons, usually at, and in coordination with, EPW and detainee internment facilities. The Joint Forces Commander (JFC) normally tasks the Army component commander to establish, secure, and maintain the EPW internment facility system. The corps may have the mission of establishing an interrogation facility when it is acting as the Army Forces (ARFOR) or Land Component Command (LCC) element.

5-101. An echelon above corps (EAC) MP brigade normally operates the theater internment facility. The subordinate JFC with a J2 staff lead establishes a Joint Interrogation and Debriefing Center as an activity within the theater internment facility. The MI Brigade Commander or other named SIO is normally designated as the JIDC commander. Army interrogation operations are normally carried out in an area of the MP-operated internment facility set aside for that use.

5-102. The JIDC is normally administratively and operationally self-sufficient. A JIDC will function as part of an overall detainee command and control structure as outlined in FM 3-19.40 and/or by policy. Continuous coordination between the JIDC commander and internment facility commander is essential. The JIDC will—

- Normally consist of facility headquarters, operations, analysis, editorial, interrogation, screening, and DOCEX elements.

- Collocate with the theater detainee internment facility.
- Organizationally structure itself to meet METT-TC requirements within the theater.
- Include HUMINT collectors, CI personnel, technical experts, personnel for CEDs and DOCEX, and intelligence analysts, as applicable, from the Army, Air Force, Marine Corps, Navy, and other government agencies.
- Maintain the capability to deploy HCTs forward, as needed, to conduct interrogations or debriefings of sources of interest who cannot be readily evacuated to the JIDC.
- Often establish a combined interrogation facility with allied HUMINT collector or interrogator augmentation if operating as part of a multinational operation.
- Receive collection guidance from the C/J/G2X and send its intelligence reports to the C/J/G2X and to the supported C/J/G/S2.

5-103. The exact size and organizational structure of these elements will vary dependent on METT-TC.

Headquarters Element

5-104. The activity headquarters provides all command, administrative, logistic, and maintenance support to the JIDC. It coordinates with—

- Higher headquarters for personnel, intelligence, and operational and logistical support prior to and after deployment.
- Theater J2 for reporting procedures, operational situation updates, theater and national level intelligence requirements, and collection priorities.
- Provost marshal for location of theater detainee internment facilities and for procedures to be followed by HUMINT collectors and MPs for the processing, interrogating, and internment of EPWs.
- Commanders of theater medical support units and internment facility for procedures to treat, and clear for questioning, wounded EPWs.
- Commanders of supporting CI and TECHINT assets to establish support requirements and procedures.
- The servicing SJA.
- Magistrate for Article 78 issues.
- Commanders of Air Force, Marine, Navy, and national level organizations to arrange administrative and logistic interoperability.

Operations Element

5-105. The operations element controls the daily activities within the JIDC. The JIDC operations element—

- Ensures that work areas are available for all JIDC elements.
- Establishes and maintains JIDC functional files, logs, and journals.
- Makes detainee files available to detainee release boards to assist the board members in their determinations.
- Establishes interrogation priorities.

- Disseminates incoming and outgoing distribution.
- Conducts coordination with local officials, adjacent and subordinate intelligence activities, CI, MP, PSYOP, the Joint Captured Materiel Exploitation Center (JCMEC), Plans and Policy Directorate (J5), and provost marshal.
- Conducts coordination with holding area officer in charge (OIC) for screening site, medical support, access, movement, and evacuation procedures for detainees.
- Conducts operations briefings when required.
- Supervises all JIDC operations and establishes SOPs.
- Supervises all intelligence collection activities within the JIDC.
- Ensures observers are present when OGAs use the JIDC's interrogation rooms.

Analytical Element

5-106. The analytical element normally is directly subordinate to the operations element. The JIDC analytical element ensures that collection requirements are current and validated. It reviews reports to ensure that the information reported is in response to validated collection requirements. In addition, they ensure an up-to-date common operational picture (COP) by maintaining digital mapping of the current tactical situation and with OB updates to help HUMINT collectors maintain their situational awareness. At locations where digital mapping is not possible, paper situation maps (SITMAPs) are maintained. This element also—

- Obtains, updates, and maintains the database.
- Works with interrogators to provide collection focus for interrogations.
- Establishes and maintains OB workbooks and files including data generated by intelligence information which has not been verified.
- Maintains digital or paper SITMAPs, as available, displaying enemy and friendly situations.
- Catalogs, cross-references, and disseminates collection requirements to JIDC collection elements.
- Reviews interrogation reports for inclusion into the database.
- Conducts situation briefings when required.
- Conducts intelligence reach with the J2 analytical cell and other analytical elements, such as INSCOM Information Dominance Center, for relevant information and analysis.

Editorial Element

5-107. The editorial element is normally directly subordinate to the operations element. It reviews all outgoing reports for format, content, and completeness.

DOCEX Element

5-108. At a minimum, the JIDC will contain a small DOCEX element to translate, screen, and extract information from and report on information of

intelligence interest from source-associated documents. The theater joint document exploitation facility (JDEF) may be collocated with the JIDC. In this instance, the JDEF will translate, screen, categorize, and exploit all types of CEDs.

Screening Element

5-109. The JIDC normally has a separate screening element to receive and screen all incoming detainees and their personal effects. The screening element will review previous screening reports, which should have been sent along with the detainees; recommend priorities for interrogation; identify individuals of interest to other agencies; and may conduct limited interrogations for PIR information. The exact size of the element will vary based on detainee capture rates and detainee flow. Interrogation elements should use their most experienced interrogators as screeners in order to quickly and effectively select the detainees for interrogation who are most likely to possess useful information.

Interrogation Element

5-110. The interrogation element assigns HUMINT collectors to specific detainees, uses interrogation and other HUMINT collection methods to obtain information in response to intelligence requirements, and produces intelligence reports (IIRs and SALUTE reports) as well as source-related operational reports. The interrogation element may also debrief returning US POWs and other personnel as deemed relevant.

This page intentionally left blank.

PART THREE

The HUMINT Collection Process

Part Three discusses the logical progression of phases involved in all HUMINT collection. There are five phases and the related task of screening that are critical to HUMINT collection. This remains consistent with previous doctrine as captured in the interrogation process but adds screening as a phase and combines approach and termination. The five phases are screening, planning and preparation, approach and termination strategies, questioning, and reporting.

Chapter 6

Screening

6-1. Available human sources and documents almost always exceed the qualified HUMINT collection assets and resources that can be applied against them. Screening facilitates the efficient application of these limited assets and resources to maximize the collection of relevant information.

HUMAN SOURCE SCREENING

6-2. As it applies to HUMINT operations, screening is the process of evaluating and selecting human sources and documents for the prioritized collection of information based on the collection requirements and mission of the unit conducting the screening or its higher headquarters. Screening categorizes and prioritizes sources based on the probability of a particular source having priority information and the level of cooperation of the source. Screening is also used to determine if a source matches certain criteria that indicate that the source should be referred to another agency. Screening is conducted at all echelons of command and in all operational environments. There are two general categories of screening: human source screening and document screening. Human source screening will be explained in depth in this chapter. Document screening is explained in Appendix I.

6-3. The resources (time and personnel) allocated to screening must be balanced against those required for interrogations, debriefings, and other collection methodologies. Although screening is not in itself an information collection technique, it is vital to the rapid collection of information. Through screening, the effectiveness of limited collection assets can be maximized by targeting those assets against the sources with the highest potential of providing key information. Screening requires experienced individuals with

maturity and judgment who are totally knowledgeable of the collection requirements and able to make well-reasoned decisions based on limited information. Collection (interrogation, debriefing, and elicitation) can be integrated into screening activities; however, it slows the screening process and decreases the number of potential sources that can be screened.

6-4. Human source screening is the evaluation of an individual or a group of individuals to determine their potential to answer collection requirements or to identify individuals who match a predetermined source profile. The purpose of screening is to—

- Identify those select individuals among the target audience who have information of potential value and who are willing or can be persuaded to cooperate.
- Identify individuals who match certain criteria that indicate them as being potential subjects for source operations or matching the profile for collection by special interest groups such as TECHINT or CI.

6-5. Screening requires the development of criteria that are indicators of potential information. These might include rank, position, gender, ethnic group, appearance, and location.

6-6. Screening is an integral part to all HUMINT collection operations. While questioning an individual source, a HUMINT collector may switch between screening (finding out general source areas of knowledge) to interrogation, debriefing, or elicitation (finding out detailed information about a specific topic). In operations, such as EPW or refugee operations that involve large numbers of potential sources, screening will normally be conducted as a separate but collocated operation as part of the overall interrogation or debriefing effort. The high number of potential sources being dealt with in most human source screening operations requires a systematic approach be developed and utilized to make the most effective use of the personnel and resources being allocated to the source screening operation.

SCREENING OPERATIONS

6-7. Like all intelligence operations, human source screening operations are focused on certain targets. Although the exact target population group will depend on the requirements of the theater of operations, the target focus of source screening operations is best described as the permanent and transitory population in the AO. This definition includes local indigenous populations, refugees, and travelers in the area, and detainees (including EPWs). Specifically excluded from this definition are members of the HN forces (military and paramilitary), members of allied forces, and members of HN government agencies who are available to US forces through liaison operations. Other personnel not indigenous to the AO (such as legitimate NGOs, humanitarian organizations, UN personnel) are available to US forces for voluntary debriefing and should be excluded from screening operations.

6-8. Screening operations may be conducted in a variety of situations and are dependent on the operational situation and the population. Although every source screening operation has the same basic purpose, each can be directed against different segments of the population in different locations throughout

the AO. In order to accommodate the differences in the screening audience and location, different types of source screening operations are employed.

- Tactical Screening. Tactical screening is conducted in support of combat or contingency operations. It can include the screening of EPWs or detainees at the point of capture, the screening of refugees, or the screening of local civilians in cordon and search. At the tactical level, there is no time for elaborate approach techniques so the degree of cooperation becomes a prime concern. Tactical area screening is characterized by rapidly changing requirements, the need to evacuate noncombatants and detainees to a secure area, and the need to collect priority tactical information while operations are in progress. Although the most lucrative type of source is often the detainee, all available sources should be screened for priority tactical information. In tactical screening, the HUMINT collector normally accompanies the maneuver force (OPCON or DS). If the HUMINT collector establishes that the source has information of value during screening, he immediately questions the source. Information collected is passed to the maneuver commander, normally via SALUTE reports. The HUMINT collector may recommend to the commander that individual sources be further detained for additional questioning. Screening must be done accurately in order that a commander can make a decision to detain or release possibly hostile personnel, based on the recommendation of a HUMINT collector.
- Checkpoint Screening. Checkpoints are often established to screen the local populations as they transit through and within the AO or to screen large numbers of individuals such as refugees or DPs as they enter the AO. Screening checkpoints can be static or mobile. HUMINT collectors must pay particular attention to refugees leaving the area ahead of friendly forces (AO or AOI). It is likely that refugees can provide information of tactical value more quickly and easily than detainees. Refugees know the area and may be able to identify for the collector anything that is out of the ordinary, such as insurgent or terrorist activities.
- Local Population Screening. This refers to the screening of the local population within their own neighborhoods. When HUMINT collectors move into a new area, they must observe the local population and determine who may be able and willing to provide the information they have been tasked to collect. Once this determination is made, the collectors must engage those individuals in conversation to assess their level of knowledge.
- Collection Facility Screening. Screening is conducted as a normal part of HUMINT collection operations at collection facilities such as theater interrogation and debriefing facilities and refugee camps. Screening is coordinated with the unit, normally an MP unit that is responsible for the operation of the facility.
- Local Employee Screening. CI personnel periodically screen local employees to determine possible security risks. Concurrently, local employee screening may identify sources who can provide information to answer the CCIRs. Close coordination between HUMINT and CI collection assets is a must in local employee screening.

- Variations and Combinations. All types of screening can be adapted to meet specific circumstances slightly different from those for which they were designed. Additionally, it is possible to use more than one type of screening in an operation if the specific circumstances require it.

6-9. Screening of refugees, EPWs, and other detainees normally occurs at two locations: initially at the point where friendly forces first encounter them and again when they arrive at the theater and other holding areas or refugee camps. The capturing or detaining forces should enforce segregation of EPWs from refugees and other detained civilians; they should be screened in separate operations, one screening for EPWs and one for refugees and other detained civilians. Depending on METT-TC factors, segregation should be conducted as follows:

- Refugees: Refugees, even if of the same nationality as the enemy, are not treated as enemies exclusively based on their nationality and are not automatically subject to control measures. If refugees are encountered on the battlefield, they are segregated from EPWs and screened separately. They are generally not detained further unless some additional reason requires their detention. At a refugee camp, screening will be done in coordination with the NGO operating the refugee camp. If there is a reason to detain refugees for further questioning for intelligence purposes, or because they pose a security threat, they will then be treated as a detainee. Under all circumstances, refugees will be treated humanely. If they are transported to an internment facility, they will be in-processed by MPs and their Geneva Conventions status will be determined. Their status under the Geneva Conventions will afford them certain privileges.
- EPWs: Officers are segregated from enlisted. The enlisted are divided into NCOs and lower enlisted. Males are segregated from females. This segregation facilitates rapid screening for EPWs who may have information to answer PIRs and IRs as well as prohibits officers from influencing enlisted personnel to resist questioning.
- Other Detainees: Civilians should be screened separately from EPWs. As with refugees, if there is a reason to detain civilians for further questioning for intelligence purposes, or because they pose a security threat, they will then be treated as a detainee. Whether or not civilian detainees are released or detained further, screeners should ensure that the civilian detainees are treated humanely. If the civilian detainees are transported to an internment facility, they will be in-processed by MPs and their Geneva Conventions status will be determined. Once detainees are in-processed into an internment facility, they are then considered to be civilian internees and their status as such will afford them certain privileges under the Geneva Conventions.

SCREENING AT FORWARD LOCATIONS

6-10. The initial screening and subsequent questioning should be accomplished as far forward as is operationally expedient. If a HUMINT collector is not available, the unit S2 must ensure initial screening and questioning of sources are completed by qualified personnel. At this level, the individual (military or civilian) is questioned for job, unit (if applicable),

mission, PIR and IR, and supporting information (JUMPS). If time allows, the HUMINT collector may collect additional information, such as the source's name, to start a formal source file to preclude duplication at higher echelons. S2s and personnel other than HUMINT collectors should not attempt an approach at this stage.

6-11. HUMINT collectors will only use approach techniques as time and circumstance allow. The prime requirement is to identify the individuals with information of immediate tactical value, to collect that information expediently, and to evacuate the source. In this case, tactical questioning is normally integrated seamlessly into the screening process. This initial screening can also be used to identify individuals for immediate evacuation to a higher echelon facility for detailed questioning. Any screening reports or information reports generated at this level must accompany the EPWs or detainees as they are evacuated. Typically, battlefield screening reports, such as the screening sheet shown in Figure 6-1, will be done on paper in order to allow multiple screeners to work simultaneously. If automation support is available for each screener, an electronic version of the screening report is used, or the "KB Easy" (Figure 10-2), which allows the screener to easily put screening information into a DIA report format and transmit it electronically. (See Chapter 10 for a KB-EZ worksheet.)

6-12. US forces capturing enemy forces or detaining civilians on the battlefield search each individual for weapons, documents, or other material of intelligence interest. Each individual receives a Capture Tag which records basic biographic data such as name, rank, serial number, unit of assignment (military), location of capture, and any special circumstances concerning the capture. (See Appendices E and F.) Each document or item removed from the captive is also "bagged and tagged" to identify from whom it was taken. This initial step is vital, as properly processing captives and their equipment greatly simplifies the screening process. All documents associated with the source and any possessions taken from him must be evacuated with the source, but not on his person. This is to ensure that the next echelon of screeners and interrogators will have the ability to exploit these items for intelligence value, or to support determination of approach strategies.

SCREENING AT REFUGEE CAMPS OR DETENTION FACILITIES

6-13. When a detainee or refugee arrives at an internment facility, refugee camp, or similar facility, a more extensive screening is conducted. The screening sheet is used to facilitate this process. This screening is normally done in conjunction with in-processing into the facility. During in-processing, the MP will assign an Internment Serial Number (ISN) that is registered with the Theater Detainee Reporting Center (TDRC). The ISN will be used to track the detainee throughout the MP detention system. The ISN should not be used in intelligence channels; however, HUMINT collectors should record the ISN on the screening sheet to aid in locating the detainee again. For intelligence reporting purposes, HUMINT collectors will assign the detainee a source reporting number that will be used to identify the detainee and information associated with him, regardless of whether or not the detainee is transported to another facility. The J2 issues source reporting numbers to HUMINT collectors through the OMT.

MP ISN NUMBER:			EVACUATION DATE:
PERSONAL	LNAME(P): _____ LNAME(M): _____ FNAME: _____ MNAME: _____ SVC/ID NO: _____ DOB: _____ LANGUAGES: _____ MARITAL STATUS: M S W D	CAPTURE DATA	DATE: _____ TIME: _____ PLACE: _____ CAP UNIT: _____ CIRCUMSTANCES: _____ _____ DOCUMENTS: _____ _____ WPNS/EQUIP: _____ _____
***	STATUS: M = Military C = Civilian P = Paramilitary ? = Other		
MILITARY	BRANCH: AF AR CG MC NY ___ RANK: _____ FULL UNIT DSG: _____ _____ DUTY PPSN: _____ JOB: _____ STATION: _____ SKILLS: _____ EXPERIENCE: _____	ASSESSMENT DATA	PHYSICAL CONDITION: SEX: M F WOUNDED: Y N _____ REMARKS: _____ _____ MENTAL CONDITION: EDUCATION = _____YRS INTELLIGENCE: AVG+ AVG AVG- MENTAL STATE: _____ _____
CIVILIAN	JOB: _____ ORG: _____ DUTIES: _____ _____ SKILLS: _____ _____		SCREENER: _____ DATE: _____ TIME: _____ COOPERATION: 1(High) 2 3(Low) KNOWLEDGE: A(High) B C(Low) BGW LIST: Y N BGW CODE: ____ SOURCE CATEGORY: A B C D APPROACH: _____
SPECIAL HANDLING REQUIREMENT CODES: _____ _____			
PIR & IR	_____ _____ _____ _____ _____ _____ _____	REMARKS	_____ _____ _____ _____ _____ _____ _____

SAMPLE

Figure 6-1. Screening Sheet.

6-14. When a detainee is in-processed into an internment facility, MPs will assign the detainee's status as an EPW, retained person, protected person, or other status under the Geneva Conventions. Figure 6-2 provides excerpts from FMI 3-19.40 on MP internment and resettlement operations. In an international conflict, individuals entitled to POW status (EPWs) include—

- Members of the regular armed forces.
- Other militias or volunteer corps, and organized resistance movements of a State Party to a conflict, provided they meet each of the following criteria:
  - Commanded by a person responsible for his subordinates.
  - Having a fixed distinctive sign recognizable at a distance.
  - Carrying arms openly.
  - Conducting operations in accordance with the law of war.
- Civilians who accompany the force.
- Crew members of the merchant marine and crews of civilian aircraft of a State Party to the conflict, who do not benefit by more favorable treatment under any other provisions of international law.

6-15. There are other categories specified in Article 4, GPW. Questions with respect to an individual's entitlement to EPW status should be directed to your SJA.

6-16. Retained personnel (see Articles 24 and 26, GWS):

- Official medical personnel of the armed forces exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and staff exclusively engaged in the administration of medical units and facilities.
- Chaplains attached to the armed forces.
- Staff of National Red Cross Societies and that of other Volunteer Aid Societies, duly recognized and authorized by their governments to assist Medical Service personnel of their own armed forces, provided they are exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and provided that the staff of such societies are subject to military laws and regulations.

6-17. Protected persons include civilians entitled to protection under the GC, including those we retain in the course of a conflict, no matter what the reason. A "civilian internee" is a person detained or interned in the United States or in occupied territory for security reasons, or for protection, or because they have committed an offense against the detaining power, and who is entitled to "protected person" status under the GC.

6-18. The term "detainee" may also refer to enemy combatants. In general, an enemy combatant is a person engaged in hostilities against the United States or its coalition partners during an armed conflict. The term "enemy combatant" includes both "lawful enemy combatants" and "unlawful enemy combatants."

- **Lawful enemy combatants:** Lawful enemy combatants, who are entitled to protections under the Geneva Conventions, include members of the regular armed forces of a State Party to the conflict;

militia, volunteer corps, and organized resistance movements belonging to a State Party to the conflict, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the laws of war; and, members of regular armed forces who profess allegiance to a government or an authority not recognized by the detaining power.

- **Unlawful enemy combatants:** Unlawful enemy combatants are persons not entitled to combatant immunity, who engage in acts against the United States or its coalition partners in violation of the laws and customs of war during armed conflict. For purposes of the war on terrorism, the term "unlawful enemy combatant" is defined to include, but is not limited to, an individual who is or was part of supporting Taliban or al Qaida forces, or associated forces that are engaged in hostilities against the United States or its coalition partners.

Excerpts from FMI 3-19.40, Military Police Internment/Resettlement Operations

ACTIVITIES

The MPs assist MI screeners by identifying captives who may have answers that support PIR and IR. Because MPs are in constant contact with captives, they see how certain captives respond to orders and see the types of requests they make. The MPs ensure that searches requested by MI personnel are conducted out of sight of other captives and that guards conduct same-gender searches.

The MI screeners examine captured documents, equipment and, in some cases, personal papers (journals, diaries, and letters from home). They are looking for information that identifies a captive and his organization, mission, and personal background (family, knowledge, and experience). Knowledge of a captive's physical and emotional status or other information helps screeners determine his willingness to cooperate.

LOCATION

Consider the following when planning an MI screening site:

- The site is located where screeners can observe captives as they are segregated and processed. It is shielded from the direct view of captives and is far enough away that captives cannot overhear screeners' conversations.
- The site has an operation, administrative, and interrogation area. The interrogation area accommodates an interrogator, a captive, a guard, and an interpreter as well as furniture. Lights are available for night operations.
- Procedures are implemented to verify that sick and wounded captives have been treated and released by authorized medical personnel.
- Guards are available and procedures are implemented for escorting captives to the interrogation site.
- Procedures are published to inform screeners who will be moved and when they will be moved.
- Accountability procedures are implemented and required forms are available.

Figure 6-2. MP Support to Screening.

6-19. It may not be immediately evident in a particular theater of operation whether an individual is an unlawful enemy combatant or is associated with or supporting the unlawful enemy combatants of the United States. Consult your J/G/S2 and servicing SJA for information relevant to your theater of operations.

6-20. All captured or detained personnel, regardless of status, shall be treated humanely, and in accordance with the Detainee Treatment Act of 2005 and DOD Directive 2310.1E, "Department of Defense Detainee Program", and no person in the custody or under the control of DOD, regardless of nationality or physical location, shall be subject to torture or cruel, inhuman, or degrading treatment or punishment, in accordance with and as defined in US law. (See Appendix A, GPW Articles 3, 4, 5, 13, and 14.)

6-21. The rights of EPWs are stated in the GPW. They include the right to quarters, rations, clothing, hygiene and medical attention, property, and other rights. EPWs may not renounce their rights to renounce EPW status. (See Appendix A, GPW Article 7, Section I.)

6-22. Retained personnel must receive at least the same benefits as EPWs. They may only be required to perform religious or medical duties, and they may only be retained as long as required for the health and spiritual needs of the EPWs. Retained persons must be returned to their home country when no longer needed.

6-23. Protected persons' rights include protection from physical or moral coercion and from being taken hostage. Protected persons are protected from murder, torture, corporal punishment, mutilation, medical experimentation, and any form of brutality. Protected persons rights are limited, though. They do not have the right to leave captivity and are not immune from prosecution. Protected persons can be screened and identified for intelligence purposes.

SCREENING PROCESS

6-24. At the internment facility, the screening process normally is distinct from the questioning (interrogation or debriefing) process. Dependent on the criticality of the information identified, the source may be questioned immediately for relevant information but will more likely be identified for future questioning. The screening is a more formal process in which the screener attempts to obtain basic biographic data, areas of general knowledge, source cooperation, and vulnerability to select approach techniques in addition to identifying knowledge of critical intelligence tasks. Once the screener has established the basics (source identification, cooperation, and knowledge), he normally passes the source on to the personnel that conduct the questioning. The screener will complete a screening report that will be forwarded in accordance with unit SOPs (see Chapter 10). If a detainee's knowledge is of Joint Forces interest, a knowledgeability brief (KB) should be written and submitted electronically. (A short form KB worksheet is shown at Figure 10-2.) Complete guidance on KBs is contained in DIAM 58-12 (S//NF).

6-25. If the source freely discusses information of PIR value, the screener normally exploits the information fully and completes a SALUTE report. (See Appendices H and I.) If the source's knowledge of PIR information is extensive and he is freely giving the information, the senior screener and the OIC or noncommissioned officer in charge (NCOIC) of the interrogation or debriefing element are notified immediately. They decide if the screener should continue questioning the source or if the source should be handed off to another HUMINT collector. If source-associated documents contain PIR information, the collector will exploit them as fully as possible and write a SALUTE report. (See Appendix H.)

6-26. The source normally is assigned a standard screening code. The screening code is an alphanumeric designation that reflects the level of cooperation expected from the source and the level of knowledgeability the source may possess. Table 6-1 shows the codes for assessing sources. Those sources assigned to the same category are interrogated in any order deemed appropriate by the interrogation or debriefing element.

Table 6-1. Source Screening Codes.

CODE	COOPERATION LEVEL
1	Responds to direct questions.
2	Responds hesitantly to questioning.
3	Does not respond to questioning.
	KNOWLEDGEABILITY LEVEL
A	Very likely to possess PIR information.
B	Might have IR information.
C	Does not appear to have pertinent information.

6-27. Figure 6-3 shows the order in which detainees in the assessed screening categories should be interrogated. Category 1-A sources normally should be the first priority to be questioned. Category 1-B and 2-A would be Priority II. Category 1-C, 2-B and 3-A would be next as Priority III sources, with 2-C, and 3-B being in the fourth group to be interrogated. Category 3-C sources are normally not questioned. This order ensures the highest probability of obtaining the greatest amount of relevant information within the available time. Screening codes may change with the echelon. The higher the echelon, the more time is available to conduct an approach. Appendix B discusses the reliability ratings of information obtained.

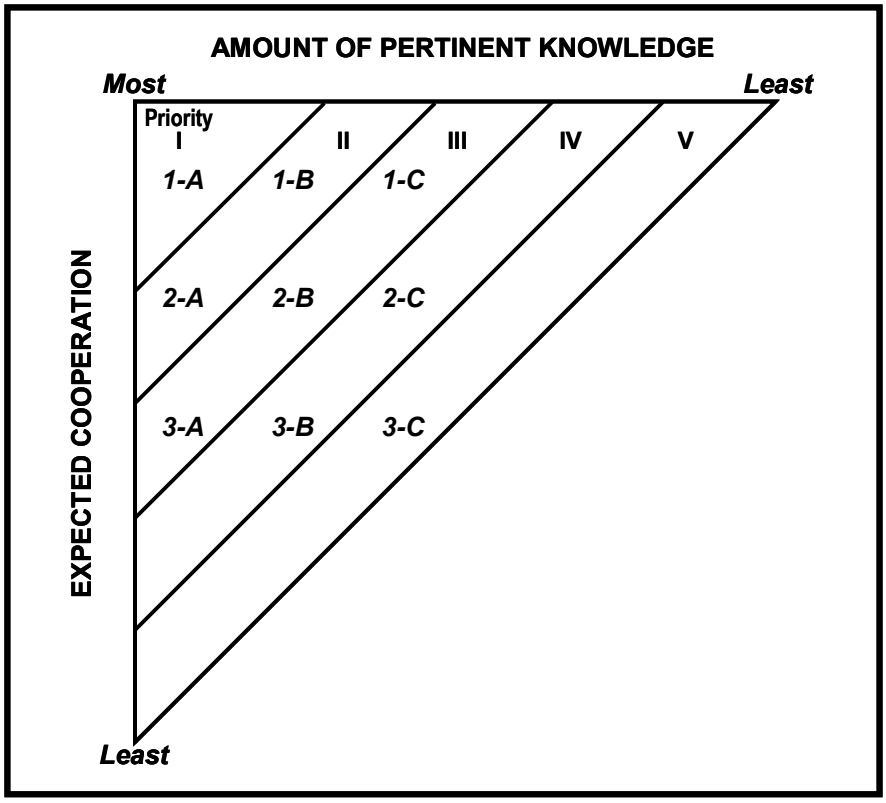


Figure 6-3. Interrogation Priorities by Screening Category.

SCREENING METHODOLOGIES

6-28. Depending on the specific operation or echelon, screening may be a separate operation or may be integrated into a specific collection mission. For example, a HUMINT collector accompanying a patrol encounters a civilian who may have information that is relevant to collection requirements. The HUMINT collector screens the source (that is, asks some general questions to determine the source's level of cooperation and knowledge). Upon receiving a positive response, the HUMINT collector may debrief the civilian on a specific topic or question him on areas of PIR interest. He then reverts to the screening role to determine other relevant knowledge. If the HUMINT collector determines through screening that the source either has no relevant information or cannot be persuaded to cooperate within an operationally expedient timeframe, he is not debriefed as part of the screening process. In detainee or refugee operations, a separate element will normally conduct all screenings. They establish a prioritized list of sources who are then systematically questioned on specific topics by other HUMINT collectors or other technical specialists.

SCREENING REQUIREMENTS

6-29. In addition to potential sources, screening requires several components.

- Collection Requirements. Without a clear list of specific collection requirements, screening becomes virtually impossible. The concept behind screening is to rapidly identify source knowledgeability as it relates to requirements. Screeners should obtain a copy of the supported element's collection requirements and become familiar with the intelligence indicators listed therein. Screeners must use their experience and imagination to devise ways to identify EPWs and detainees who might possess information pertinent to these indicators. Vague requirements (such as "What is the threat doing?") do not provide the focus necessary to make a source selection. The HUMINT collection element must break these SIRs into indicators if the supported intelligence officer has not already done this. The indicators must take into account the type of sources anticipated. For example, a refugee probably will not know if the threat intends to defend a particular ridgeline. However, he might know whether or not there are threat forces on the ridge, if an improvised explosive device (IED) is being employed on a route, if they are digging in, or if engineer type equipment is in the area.
- Selection Criteria. After reviewing the collection requirements, the HUMINT collection element will develop preliminary criteria to identify the source type that will most likely have the required information. The source type may include gender, appearance, military rank, age, or occupation. Some of these criteria are determined by visual observation, thereby saving time in not having to question everyone. Other criteria such as occupation or place of residence may require brief questions.
- Trained Screeners. Screening is possibly the most difficult HUMINT skill. A HUMINT collector must use his experience, questioning skill, cultural knowledge, and knowledge of human nature to decide in a matter of minutes or possibly seconds whether limited HUMINT collection assets and valuable time should be spent talking to an individual based on the way he looks and the answers to a few questions. A wrong decision will mean wasted assets and valuable information missed.
- Language Capability and Cultural Awareness. Screening involves more than asking a series of questions. The HUMINT collector must be able to evaluate the answers, the specific language used, and other clues such as body language to determine the value of an individual to the collection effort. This requires a mature and experienced screener. If the HUMINT collector does not possess the target language, he and his interpreter must be able to work together quickly with mutual trust and confidence.
- Area Conducive to Screening Operations. Effective screening operations must allow the HUMINT collector to speak to the source where the source is not exposed to outside influences or dangers that may inhibit his responses. For that reason, sources should never be screened within the sight or hearing of other potential sources.

HUMINT collectors can use rooms within a building, tents, or other field-expedient methods to isolate the individual being screened. Screening a source within view or hearing of other potential sources may not only pose a danger to the source but also will tend to inhibit the source from freely cooperating.

- Security. The personnel conducting the screening need to be able to concentrate on the individual being screened. Although the collector is ultimately responsible for his own personal security, screening is facilitated by having dedicated personnel present (for example, MPs) who are responsible for security. Screeners coordinate with MP or other security personnel concerning their role in the screening process.

INITIAL DATA AND OBSERVATIONS

6-30. Screening is a filtering process whereby, under ideal circumstances, all potential sources would be questioned to determine if they have information of intelligence interest. In actuality this is often impossible. Screeners often use visual and other aids to "prescreen" the sources in order to eliminate a substantial portion of the target population before conducting detailed screening. For example, if the HUMINT collector at a checkpoint is only interested in information concerning a specific denied geographic area, screeners may ask all refugees if they are from or have been in that denied area recently. A less experienced screener could do this allowing the experienced screener to conduct more extensive screening of the select target audience.

6-31. If time and circumstances permit, screeners should question any friendly personnel who have had extensive contact with the persons to be screened. In the case of detainees, this could include holding area personnel or personnel from the capturing unit. These personnel may be able to help identify sources that might answer the collection requirements or who might match a particular source profile.

6-32. Normally the screener will not have time to conduct any extended observation of the person to be screened; however, the screener should make a quick visual observation of the source prior to questioning him. He should note anything in the source's appearance and behavior that indicates he is willing to cooperate immediately or is unlikely to cooperate. The screener should also note any physical indicators that the source may have the type of information or belong to a certain source profile category.

6-33. Physical indicators include overall appearance such as rank, insignia, and condition of the uniform and type and condition of equipment for military sources and general type and condition of dress (for example, business suit as opposed to work clothes) for civilians. Certain physical indicators (dress, medals such as religious medals, physical type) may be indicators that the source belongs to a specific ethnic or religious group. The source's physical reactions may also indicate a willingness or lack of willingness to cooperate. For example, does the source move forward in the group or attempt to hide within the group; does he intentionally place himself in the wrong segregation group; or does he show any overt signs of nervousness, anxiety, or fright?

6-34. The screeners will also examine all documents and possessions found on the source (if any) and all documents pertaining to the source (if any). **At a minimum, a detainee should have a properly filled out capture tag, which will indicate to the screener where the detainee was captured, by which unit, and under what circumstance.** (See para 6-12 and Appendix D.) Documents such as personal letters, orders, rosters, signal operating instructions (SOIs) and map sections can provide information that identify the source, his organization, mission, and other personal background information (family, knowledge, experience, education). They may in themselves provide information, may identify a source for questioning, and may provide information helpful in assessing a source's susceptibility to an approach.

6-35. Documents pertaining to the source, beginning at the point of capture throughout the evacuation process, such as previous screening and intelligence reports and administrative documents (such as source personnel records prepared by the MPs) help the screener by providing information concerning the source's physical status, emotional status, level of knowledge, level of experience, and other background data. Making timely use of reports from lower echelons can be difficult for the screener, especially when dealing with large numbers of potential sources.

SOURCE ASSESSMENT

6-36. Screeners use standard reporting formats to identify the results of their screening (see Chapter 10). The determination must be made as to whether the source is of any intelligence value to the HUMINT collector. The HUMINT collector will basically place the source within one of four categories.

- Of Immediate Intelligence Interest. This category includes personnel who are assessed, based upon the screening process, who possess information in response to requirements. They are interrogated or debriefed (dependent on their status) to retrieve relevant information. This questioning may be conducted by the same person conducting the screening or by another HUMINT collector.
- Of Interest to Other Agencies. In most cases, the HUMINT collector will be provided with collection requirements by other agencies or disciplines such as TECHINT or CI. In this case the HUMINT collector will question the source on these requirements and report the information appropriately. However, in some instances, particularly in the case of CI, the HUMINT collector may be given a list of topics or a profile of personnel who are of interest to CI. The HUMINT collector will notify the local CI representative when a person matching the "CI profile" is identified. After the HUMINT collector has extracted any relevant intelligence information, he will "pass" the individual off to the CI agents. In many cases, particularly with individuals of TECHINT or other specialized interest, the HUMINT collector will be asked to conduct the questioning with the technical support of the individual from the interested agency. This is coordinated through the HUMINT collector's OMT and the chain of command.

- Of Potential Interest as a Contact Source. On occasion, especially during stability and reconstruction operations, the HUMINT collector may identify an individual who has the potential to provide information in the future, due to his placement or access. Although the individual may not have information of immediate interest, the HUMINT collector will pass his recommendation to the appropriate office, normally the C/J/G/S2X, provided that source operations are authorized (see Chapter 5).
- Of No Interest. This category includes sources who prove (based upon the screening process) to be of no interest to the HUMINT collector or other agencies. Their biographic data is recorded, but they are not questioned further. This category will likely include the bulk of individuals screened. Individuals who have been screened are kept separated from those who have not yet been screened.

OTHER TYPES OF SCREENING OPERATIONS

LOCAL EMPLOYEE SCREENING

6-37. CI personnel conduct local employee screening, primarily to identify individuals who may be a security risk. HUMINT collectors also can use local employee screening as a means to obtain intelligence information or to identify personnel with placement and access to answer information requirements. Employee screening must be conducted in a secure environment and out of the hearing and sight of other employees. Formal written reports of the screening must be maintained.

LOCAL COMMUNITY OR AREA SCREENING

6-38. Local area screening is normally done in coordination with other operations such as a cordon and search operation. The HUMINT collectors accompany the forces conducting the operation and screen the general population to identify individuals of intelligence or CI interest.

SCREENING FOR CI REQUIREMENTS

6-39. Before initiating the screening process, the HUMINT collector establishes liaison with supporting CI agents. The CI element provides CI requirements and provides a profile of personnel of CI interest. CI is normally interested in personnel who—

- Have no identification documents.
- Have excessive or modified identification documents.
- Possess unexplainable large amounts of cash or valuables.
- Are illegal border-crossers.
- Attempt to avoid checkpoints.
- Are on the CI personalities list, which includes members of an intelligence service.
- Request to see CI personnel.
- Have family in the denied area.
- Speak a different language or dialect than is spoken in the area.

6-40. Personnel of CI interest include two general categories of people: The first type of "person of interest" is any individual or group involved in adversary intelligence collection operations or who is attempting to enter the AO to conduct such operations. Examples of these individuals include but are not limited to—

- Known or suspected members and/or supporters of foreign intelligence and security services and known or suspected members and/or supporters of the intelligence activities of non-state entities such as organized crime, terrorist groups, and drug traffickers.
- Known or suspected hostile espionage agents, saboteurs, subversives, or hostile political figures.
- Known or suspected enemy collaborators and sympathizers who may pose a security threat to US forces.
- Personnel known to have engaged in intelligence, CI, security, police, or political indoctrination activities.
- Known or suspected officials of enemy governments whose presence poses a security threat to US forces.
- Political leaders known or suspected to be hostile to the military and political objectives of the US or an allied nation.

6-41. The second type of "person of CI interest" is any individual who possesses information concerning the identification, location, or activities of personnel in the first category.

SCREENING FOR OTHER TECHNICAL COLLECTION REQUIREMENTS

6-42. Other technical areas such as TECHINT, SIGINT, IMINT, MASINT, or other services need to supply the HUMINT collectors with a profile of the individuals with whom they wish to speak. The HUMINT collectors upon identifying such an individual will contact the requesting agency after extracting PIR information.

Chapter 7

Planning and Preparation

7-1. Planning and preparation is one of the five phases of HUMINT collection. HUMINT collection, regardless of the methodology employed, must be a systematic, carefully prepared enterprise. The HUMINT collector engages in general preparation throughout his career. He focuses that preparation to a specific area of the world, specific mission, and specific collection requirements as those become available. Finally, the HUMINT collector focuses his planning and preparation on a specific collection effort with a specific source.

COLLECTION OBJECTIVES

7-2. Each HUMINT collection mission is conducted for a definite purpose. The HUMINT collector must keep this purpose firmly in mind as he proceeds to obtain usable information to satisfy the requirements, and thus contributes to the success of the unit's mission. The HUMINT collector must use the objective as a basis for planning and conducting questioning. The HUMINT collector should not concentrate on the objective to the extent he overlooks or fails to recognize and exploit other valuable information extracted from the source. For example, during HUMINT collection, the HUMINT collector learns of the presence of a heretofore unknown, highly destructive weapon. Although this information may not be in line with his specific objective, the HUMINT collector must develop this important lead to obtain all possible information concerning this weapon.

RESEARCH

7-3. The key to good HUMINT collection is preparation on the part of the collector. The HUMINT collector must understand the environment and particularly its human component, the mission of the supported unit, that unit’s intelligence requirements, his source, and the cultural environment. The ultimate success of a questioning session is often decided before the HUMINT collector even meets the source.

GENERAL RESEARCH

7-4. Due to the quickly changing world circumstances, it is impossible to conduct all the specific research required immediately prior to questioning a source. General research should be completed before entering an AO and continues until operation completion. Areas of research include but are not limited to—

- OPLANs and OPORDs. The HUMINT collector must be familiar with the unit OPLAN and that of its higher headquarters. By thoroughly understanding the unit OPLAN and OPORD, the HUMINT collector

and HUMINT commanders and leaders can anticipate collection requirements, develop source profiles, recommend deployment strategies, and otherwise integrate HUMINT operations into the overall unit operation. Although the OPORD needs to be read and understood in its entirety, certain areas are of critical importance to the HUMINT collection effort. They include—

- Task organization. This will show where HUMINT C2, staff support, and collection assets will fit into the organizational structure.
- Situation. This gives the friendly and enemy situation.
- Mission. This gives the HUMINT collectors insight into how their operations will integrate into the parent unit's operation.
- Execution. The four execution subparagraphs explain the commander's intent on how the mission is to be carried out:
  - Subparagraph 3a (Concept of Operation) includes how subordinate units' operations will be included in the overall plan.
  - Subparagraph 3a(3) (Reconnaissance and Surveillance) details how HUMINT collection operations will integrate into the overall ISR plan. Additional information on ISR is found in Annex L.
  - Subparagraph 3a(4) (Intelligence), along with Annex A (Task Organization) and Annex B (Intelligence), explains how the Intelligence BOS will support the scheme of maneuver.
  - Subparagraph 3d (Coordinating Instructions) lists the CCIRs and initial PIRs.

- Current events. The HUMINT collector must be knowledgeable about current events in all potential operational areas, especially those events that indicate the populace's feelings or intentions toward the US. This will facilitate a better understanding of the cultural, political, and socio-economic conditions that could influence the attitude and behavior of a source. This knowledge can be obtained and updated through classified periodic intelligence publications and/or military or civilian open sources, including both print and broadcast media, CA and PSYOP databases, and the J/G/S2 analytical elements.
- SOPs. The HUMINT collector must be familiar not only with his own unit's SOP but also with that of any supported unit. The HUMINT collector will be able to obtain specific information about report numbers and formats, as well as information about distribution channels for reports from these SOPs. The SOP will also explain unit policy on source exploitation and evacuation procedures, logistic and maintenance functions, and other C2 and support issues.
- Umbrella concept. The TF commander through the J/G2 and J/G2X issues an umbrella concept for HUMINT operations. When operating under this concept, collection parameters will be established in writing, and it is imperative that the HUMINT collector understands his role. Types of sources will be outlined concerning placement, motivation, and access. The umbrella concept will also specify the types of information against which the HUMINT collector can collect. The umbrella concept is governed by AR 381-100 (S//NF), AR 381-172 (S//NF), DIAM 58-11 (S//NF), and DIAM 58-12 (S//NF).

- Legal guides, SOFAs, operations and execute orders, ROE, and other legal and administrative requirements. The HUMINT collector must be thoroughly familiar with all documents that may set the legal parameters for his collection operations. These are available through the chain of command and from the SJA office. He must know how these requirements apply and to what type of sources each is applied.
- Collection requirements. The HUMINT collector needs not only to know but also to understand the requirements that he will be attempting to answer. These requirements can include CCIRs (PIRs and IRs), essential elements of friendly information (EEFIs), Intelligence Priorities for Strategic Planning (IPSP), specific requests from national level consumers such as HUMINT collection requirements (HCRs), SDRs, or even vocal orders given by the local commander. These all will determine the objective of the questioning plan.
- Databases. Intelligence databases can give the HUMINT collector detailed information about the source's unit, its organization, and its capabilities. They also have information on personalities. The HUMINT collector will use information obtained from databases to control the source and assess his answers for truthfulness. They will also give the HUMINT collector ideas of other areas to research. For example, if the threat is primarily a lightly armed insurgent force, studying similar organizations will provide the HUMINT collector with valuable insights into the possible methods of operation of the current target organization.
- SITMAP and COP. The current situation, both friendly and enemy, is vital for the movement of the HCT and for its collection operations. It reflects enemy unit identification, disposition, and boundaries; major roads or trails for movement of personnel, equipment, weapons; and locations of artillery, minefields, roadblocks, entrenchments, obstacles, staging areas, NBC contaminated areas, and ground surveillance devices. All of this information can be used in source questioning as control questions or in otherwise determining source veracity. The HUMINT collector will be able to identify indicators and predict what should be PIRs and IRs.
- INTSUM. The INTSUM provides a summary of the intelligence situation covering a specific period as dictated by the commander. It is already analyzed intelligence.
- Intelligence estimate. The intelligence estimate is derived from the intelligence preparation of the battlefield (IPB). It is based on all available intelligence and considers everything of operational significance. It will help point out gaps in the intelligence database. It is from these gaps that requirements are derived. It will provide information on the mission, AO, weather, terrain, enemy situation, enemy capabilities, and conclusions. It will cover all of the standard OB topics.
- Weapons and equipment guides. Weapons and equipment guides can assist the HUMINT collector in becoming familiar with the type of equipment employed in the AO. Guides are available in hardcopy and softcopy.

- Area handbooks. These handbooks provide detailed information about a specific area of the world. They provide information on political, economic, sociological, cultural, military, biographic, transportation, and geographic topics. The CIA and other agencies publish area handbooks annually. The US Department of State website also has continuously updated information on trouble spots around the world.
- Previous HUMINT reporting. The HUMINT collector should familiarize himself with all previous relevant reporting from the AO. This will provide him with insight into current operations, the types of information collected, and may help identify information gaps.
- Photographs, maps, and other geospatial products. In conducting general research, the HUMINT collector should become familiar with the AOs. This not only will help identify specific areas of HUMINT collection potential but also will be invaluable in both the questioning of specific sources and the maneuver of the HCT.
- Subject matter experts (SMEs) and technical research. Before deploying to an AO or before supporting on a particular mission, the HUMINT collector may identify particular areas in which he lacks critical knowledge. For example, a HUMINT collector who has previously been operating in an area with a conventional enemy may be deployed to an area with an unconventional threat from irregular forces. Also, intelligence requirements may focus on equipment that is unfamiliar to the HUMINT collector. In order to prepare himself, the HUMINT collector contacts SMEs or analysts or uses technical materials to gain background information.
- Other reports. Intelligence agencies publish numerous reports and summaries that are readily available to the HUMINT collector.

CLOSED AND OPEN-SOURCE INFORMATION (USE OF REACH)

7-5. Reach is a process by which deployed military forces rapidly access information from, receive support from, and conduct collaboration and information sharing with other units and organizations (deployed in theater and from outside the theater) unconstrained by geographic proximity, echelon, or command. Intelligence support is established based on requirements that will help the commanders (regardless of echelon) make decisions. Reach can be accomplished in various ways. There is no requirement for all intelligence functional areas or echelons to use the same approach; hence, there is no common standard for all units to use. Each organization or section should develop its strategy on using the various intelligence reach components. Standard enabling tools will provide for easier access than ever before (for example, access to the INSCOM Information Dominance Center).

INTELLIGENCE REACH COMPONENTS

7-6. Intelligence reach requires the G2/S2 to develop a strategy on how best to support the unit's mission with intelligence reach capabilities. There are eight basic elements of the strategy:

- Push: Push occurs when the producers of intelligence or information are knowledgeable of the customer's requirements and are able to send the desired intelligence to the customer without further requests. Push is accomplished through the Joint Dissemination System (JDS) and/or the Automated Message Handling System (AMHS).
- Pull: Pull occurs when the customer is familiar enough with existing databases to be able to anticipate the location of the desired information. Pull is greatly enhanced through the use of portals and homepages with hyperlinks to the various categories of information available to the user. This requires the establishment of such a homepage at each echelon, thus enabling higher echelons to research and pull from lower databases and homepages.
- Database Access: Access to local, theater, DOD, non-DOD, and commercial databases allows analysts to leverage stored knowledge on topics ranging from basic demographics to OB information. A validated DIA Customer Number (acquired by the J2/G2/S2) in combination with SIPRNET and Joint Worldwide Intelligence Communications System (JWICS) connectivity establishes access to most of the databases online.
- Integrated Broadcast Services (IBS): IBS is an integrated, interactive dissemination system, focusing on tactical user's information requirements using a common message Data Element Dictionary (DED) and J-series family of message formats. The goal of IBS is to resolve the uncoordinated proliferation of "stovepiped" intelligence or information broadcasts by providing the tactical commander with integrated time-sensitive tactical information.
- Collaborative Tools: Collaborative tools are computer-based tools (groupware) that help individuals work together and share information. They allow for virtual on-line meetings and data sharing. As much as possible, collaborative tools should be emplaced with all necessary echelons and centers prior to deployment.
- Request for Information: Reach includes the ability of an intelligence officer at any level to request information that is beyond what is available at his location, using the Community On-Line Intelligence System for End Users and Managers (COLISEUM) System. Once an RFI is entered into the system every other user of that system can see it. Hence, an echelon several echelons above the actual requester can and often does become aware of the request and may, in fact, answer it. Reach is also provided through INSCOM's Information Dominance Center and other nodes at J2 and G2.
- Leveraging Collection Management: The collection and ISR management system is established to provide a mechanism for tasking and managing collection assets for required information. Analysts who are trained and familiar with the system and the various tasking procedures can leverage the system for refined information.

- Distributed Common Ground System-Army (DCGS-A): DCGS-A is the ISR fusion and processing system for the future, as part of the overarching DOD-directed DCGS-A surface system family of systems. It will bring national and joint ISR capabilities down to JTF level, corps and division levels and BCT level to provide leaders with NRT information and visualization of threat, weather, and terrain information and intelligence. DCGS-A consolidates the capabilities of the following current-force ground processing systems:
  - All-Source Analysis System (ASAS).
  - Counterintelligence and Human Intelligence (CI/HUMINT) Single-Source Workstation.
  - Tactical Exploitation System (TES).
  - Guardrail Information Node (GRIFN).
  - Guardrail Common Sensor (GRCS) Intelligence Processing Facility (IPF).
  - Prophet Control.
  - Joint STARS Common Ground Sensor (CGS).

7-7. For more information on Intelligence Reach, see FM 2-33.5/ST.

SOURCE-SPECIFIC RESEARCH

7-8. Source-specific research is done immediately prior to questioning the source. The HUMINT collector may have to respond spontaneously in the case of a walk-in source in tactical operations, or if the HUMINT collector has advanced warning as in the case of a planned meeting with a source, a long-term debriefing, or an invitational source. Areas of research include but are not limited to—

- Screening Reports, KBs, Other Reports: Reports about the source not only can provide specific information about the type of information the source can provide to answer specific collection requirements but also can give the HUMINT collector extensive background information about the source. This background information can give clues to information the source might possess and to possible approach techniques. Information contained in screening reports and KBs may provide insight into—
  - Geographic Area: This area may show information about the source's ethnic background, political affiliation, religion, and customs. Information can be obtained from databases, locally registered vital statistics, and residence registries.
  - Languages: Determining the languages and dialects spoken, written, and understood by a source can provide valuable insights into that source's geographic and ethnic or tribal background, education, and social status. This determination of languages and dialects can be facilitated by the use of "flash cards" specific to the battlefield.
  - Other Reports: This can include other reports collected from this source at other echelons or reports from other sources from the same unit or location as the source. It can also include reports or documents published by the ACE at your request.

  - Political Group: This area can provide information on the source's beliefs as well as provide information on political leaders and goals. Additionally, political affiliation can sometimes provide information about subversive groups and paramilitary ties. Knowing the goals of the political organization can also assist the HUMINT collector in choosing an approach or establishing rapport.
  - Religious Affiliation: The source's religious affiliation may provide insight into his motivation, moral strengths and weaknesses, and other motivational factors.
  - Technical Field: Having knowledge about the source's technical field can assist the HUMINT collector in deciding upon which questions to ask. It will also assist the HUMINT collector in verifying the source's truthfulness because the HUMINT collector will have an understanding of the source's specialty.
  - Employment: By researching the source's employment history, the HUMINT collector can discover other areas of information that the source may be able to provide.
  - Education: The source's education level and educational history can not only give the HUMINT collector insight into the possible information the source can provide but also provide insight into possible approach strategies.
  - Social Status: Knowledge of the source's social status may provide a clue to a good approach strategy because the source may be accustomed to a certain type of treatment. It may also provide a clue to biographical information that the source may be able to provide.
  - Criminal Records: Criminal records may also indicate possible approach strategies. Additionally, they may indicate which groups or organizations the source may have knowledge about.
- Documents and Other Media Captured on or in Immediate Association with a Detainee or Brought in by a Debriefing Source: Documents captured with or otherwise pertaining to the source may give the HUMINT collector information about the source, his unit, or his role within that unit. They may answer requirements or indicate knowledge of PIRs. Personal letters, for example, could be used during the approach phase. If a source comes in voluntarily and provides documents, they should be reviewed prior to debriefing the source.
- Photographs, Maps, and Other Geospatial Products: Maps and photographs of the area about which the source is being questioned can give the HUMINT collector an idea of where the source has been and in what kind of terrain he operated, which might indicate knowledge or use of certain tactics. If the HUMINT collector is not familiar with the area the source was in, the HUMINT collector should take some time to look over the map so he can more readily relate when the source mentions locations or dispositions. Aerial photographs show more detailed up-to-date information than maps. They will not normally be as readily available as maps. Maps and other geospatial products will also be needed for use in the map-tracking portion of an interrogation. The HUMINT collector should work with the ACE of the supported unit to obtain them for the AO.

- SMEs: There will be occasions when the HUMINT collector will talk to sources about subjects of which the HUMINT collector has no knowledge. In that case, the HUMINT collector will want to talk to personnel who are SMEs. Depending on the depth of knowledge that the source is expected to have and the time available to prepare, the HUMINT collector may arrange for a technical expert to support the questioning (see Chapter 9).
- Technical Manuals: There are various weapon and equipment identification guides available in hardcopy, softcopy, and off the Internet that can assist the HUMINT collector in identifying any equipment mentioned by the source.
- Source Physical and Mental Condition: HUMINT collectors should observe the source prior to questioning if possible and also talk to anyone available who has relevant information concerning the source. MP guards can be an especially valuable source of information based on source observation and should be debriefed periodically. This can prevent surprises at the onset of the questioning session and can help the HUMINT collector assess the source's physical and mental condition as well as provide insights to possible approaches.
- Databases: Collectors should review source information and reports contained in the various databases available to them. The CHATS system, BAT database, and other databases can provide collectors with source information and previous reporting.

HUMINT COLLECTION PLAN

7-9. After conducting appropriate research, the HUMINT collector working with an analyst, if available, develops a source-based collection plan. This is geared to the specific source that is going to be questioned. The amount of time spent in preparing this plan depends on the operational circumstances. This may range from a quick mental review by an experienced HUMINT collector in a tactical environment to a formal written plan submitted by a subordinate to a team leader. The source collection plan will vary from source to source. It will also vary with the conditions under which the source is questioned. It serves as a checklist to ensure that all steps necessary to prepare for questioning are conducted. Whether written or oral, the HUMINT collection plan should contain at least the following items:

- HUMINT collection requirements.
- Serial number of EPW/detainee to be questioned.
- Location and time for the questioning.
- Primary and alternate approaches.
- Questioning plan including topics to be covered and the planned sequence of these topics.
- Prepared questions for unfamiliar or highly technical topics.
- Method of recording and reporting information obtained.

OBJECTIVE

7-10. The HUMINT collector will first determine the objective of his questioning. The objective is the set of collection requirements that the HUMINT collector will attempt to satisfy during the questioning session. A number of circumstances including the intelligence requirements, the time available, and the source will set the objective. Determining the objective consists of three parts:

- Identify the intelligence requirements. The primary objective of any questioning session is to answer or confirm PIR or other collection requirements.
- Identify the subject: The HUMINT collector will want to consider the source; for example, who he is, what he may know. The HUMINT collector will also want to consider the legal and other restrictions based on the type of source (contact source, EPW, refugee, strategic). For a military source (EPW) this includes rank, position specialty, and unit of assignment. For a civilian source it includes job, placement and access, associations, area of residence, and employment.
- Identify the intelligence requirements that the source may be able to answer. The HUMINT collector cannot normally waste time "fishing" for information. He must determine based on screening, what collection requirements the source can answer. The HUMINT collector compares the information that he gathered through his general and source-specific research and compares it to his list of collection requirements. He compares that list to the identity of the source and refines the list including all requirements that the source can be expected to be able to answer. The HUMINT collector will approach those areas first while staying aware of leads into other collection topics.

LOCATION

7-11. In most cases, the location for the questioning will be determined by operational requirements. However, the HUMINT collector should ensure some basic requirements are met:

- Each questioning session should be conducted outside the hearing and view of third parties. Even in the case of a source meeting in a public place, the HUMINT collector should choose a location where they cannot be overheard and where their meeting will not arouse suspicion.
- The location should be in a place that has reasonable security for the HUMINT collector and the source. In contact operations, the risk cannot always be eliminated but the acceptable risk levels should be based on the expected intelligence gain. In combat operations, most questioning (interrogation, debriefing of civilians on the battlefield) will take place in forward combat areas, but it cannot be done if it increases the risk to the source. Safe evacuation of the sources has priority over questioning.
- The location should provide ready access to the chosen method of recording and reporting the information.

7-12. When conducting military source operations, the location of the questioning will have psychological effects on the source. The questioning location should be chosen and set up to correspond to the effect that the HUMINT collector wants to project and his planned approach techniques. For example, meeting in a social type situation such as a restaurant may place the source at ease. Meeting in an apartment projects informality while meeting in an office projects more formality. Meeting at the source's home normally places him at a psychological advantage, while meeting in the HUMINT collector's work area gives the collector a psychological edge. The HUMINT collector should consider the status and level of the source, security, the workspace available, furnishings, the amount of lighting provided, and the ability to heat or cool the room as needed.

TIME

7-13. Time to conduct questioning should be estimated based on the source, the type of information that the HUMINT collector expects to get, and the complexity of that information. Other considerations include expected evacuation times for sources in tactical situations, the number of other sources that need to be spoken to; and in contact operations, the estimated time that the HUMINT collector can meet with the source without increasing the risk.

7-14. The HUMINT collector must also consider the physical conditions of the source and himself. After extended operations, there may be a limit on how long either the HUMINT collector or source can concentrate on a given subject. Even if the HUMINT collector has an unlimited time period (such as at a joint interrogation and debriefing facility), he must break his questioning down into topical sessions to maximize effectiveness. Time is only an estimate and should be modified based on the circumstances. It may be extended, for example, if the source has a greater than expected amount of information, or critical information in unforeseen areas. The time may be curtailed if the HUMINT collector has met his requirements, the source does not possess the expected information, or a more valuable source is identified.

PRIMARY AND ALTERNATE APPROACHES

7-15. In most circumstances, if the HUMINT collector is meeting with the source for the first time, he should select at least two alternate approaches to use if the direct approach is unsuccessful (see Chapter 8). These approaches need to be based on the HUMINT collector's source-specific research, his general area research, knowledge of the current situation, and knowledge of human nature. There are four primary factors that must be considered when selecting tentative approaches:

- The source's mental and physical state. Is the source injured, angry, crying, arrogant, cocky, or frightened?
- The source's background. What is the source's age and level of military or civilian experience? Consider cultural, ethnic, and religious factors.
- The objective of the HUMINT collection. How valuable is the source's potential information? Is it beneficial to spend more effort convincing this source to talk?

- The HUMINT collector himself. What abilities does he have that can be brought into play? What weaknesses does he have that may interfere with the HUMINT collection? Are there social or ethnic barriers to communication? Can his personality adapt to the personality of the source?

7-16. If the HUMINT collector has a screening sheet or KB, he can use it to help select his approaches. After reviewing the information, the HUMINT collector will analyze the information for indicators of psychological and/or physical weakness that would make a source susceptible to a specific approach. The HUMINT collector also needs to consider his particular strengths and weaknesses in conducting specific approaches. He must consider what immediate incentives he may possibly need and ensure that they are available. Also, if incentives had been previously offered or promised, the collector needs to know if they were in fact provided. If the HUMINT collector has previously questioned the source, he must evaluate the approaches he used and decide if they need to be modified or if additional approach techniques will be needed (see Chapter 8.)

ADDITIONAL SUPPORT REQUIRED

7-17. The HUMINT collector must decide if he will need technical support to include interpreter support.

- Technical support. The HUMINT collector must decide if he will need additional support including analytical, technical, or interpreter support.
- Analytical or technical support. The HUMINT collector must decide if he has the analytical or technical capability to question a specific source. If not, he must decide what degree of support from advice to participation is required of the analyst or technical expert. Any request for analytical or technical support must be coordinated with the 2X. On rare occasions, it may be desirable for the HUMINT collector to seek polygraph support or support from a Behavioral Science Consultant (BSC). BSCs are authorized to make psychological assessments of the character, personality, social interactions, and other behavioral characteristics of interrogation subjects and advise HUMINT collectors of their assessments, as needed.
- Interpreter support. If the HUMINT collector does not speak the needed language or does not speak the needed language well enough to conduct questioning, an interpreter will be required. If the HUMINT collector will need an interpreter, the HUMINT collector will also have to consider the clearance needed to complete the questioning and the availability of the interpreter, as well as the extra time necessary to complete the questioning session. The HUMINT collector will also have to brief the interpreter on the method of interpretation and the HUMINT exploitation plan. Also, he should determine whether there are any cultural aspects associated with the interpreter that may enhance or detract from the success of the meet. (See Chapter 11 for detailed information on HUMINT collection using an interpreter.)

DEVELOP A QUESTIONING PLAN

7-18. The HUMINT collector must develop a plan that will guide his questioning of the source. This includes general topics to be exploited and the sequence in which they will be covered.

7-19. There are two general sequences used in questioning: topical and chronological.

- Topical questioning is used when time is a prime concern, when the source is believed to possess key information in a limited area, when the questioning is concerning a technical topic, or when the source has been talked to previously and this is a subsequent questioning to expand on earlier topics.
- Chronological questioning normally is used when the HUMINT collector is uncertain of the areas of source knowledge, when time is not a factor in questioning, during initial questioning when the source is believed to have knowledge on a large number of topics, and in friendly force mission debriefing.

7-20. A topical sequence is an outline of topics to be questioned in a selected sequence and is based on intelligence requirements or HCRs, as well as a specific source's potential to provide information pertinent to those requirements. The plan serves as a checklist for the HUMINT collector to ensure that all subjects pertinent to the collection objective are questioned in an efficient and organized manner. The HUMINT collector uses his estimate of the type and extent of knowledge possessed by the source to modify the basic topical sequence of questioning. He selects only those topics in which he believes the source has pertinent knowledge. In this way, the HUMINT collector refines his element's overall objective into a set of specific HUMINT collection subjects. In OB factors questioning in either a tactical or strategic setting, and across the full spectrum of operations, the topics covered include missions and the nine major OB factors:

- Composition.
- Strength.
- Dispositions.
- Tactics.
- Training.
- Combat effectiveness.
- Logistics.
- Electronic technical data.
- Miscellaneous.

7-21. See Appendix G for questioning quick reference examples of topics covered under the nine OB factors.

7-22. In strategic and operational debriefing operations the relevant HCR or SDR will guide the HUMINT collector. Regardless of which tasking document is referenced, the topical sequence is established by collection requirements, modified or sequenced, based on source knowledge and time.

7-23. The nine OB factors are not the only guideline that may be used by the HUMINT collector. If the collection objective is something other than a

military unit, many of the OB factors will not fit the collection plan. A helpful memory aid, in this case, is mission, identification, location, and organization (MILO). MILO gives a short, easily remembered structure for questioning nonmilitary or strategic topics. The MILO factors can be questioned in any order, but often the most logical sequence of MILO questioning is identification, organization, location, and mission. Many of the nine OB factors can also fit into the MILO format.

IDENTIFY MEANS OF RECORDING AND REPORTING

7-24. The HUMINT collector will want to decide upon a means of recording the information obtained through source questioning. If the HUMINT collector is planning to use a sound or video recorder, he will also have to consider the availability of the equipment and its positioning (see Chapter 9). Along with the method of recording the information, the HUMINT collector will have to decide on the means of reporting the information (see Chapter 10). Tapes of interrogations must be safeguarded in accordance with DOD Regulation 5200.1-R.

FINAL PREPARATIONS

7-25. After the source-specific questioning plan is developed, the HUMINT collector takes some final preparatory steps.

- Review plan. The HUMINT collector should always go over his collection plan with his supervisor. This review can be written or oral. In addition to the obvious requirements to keep the chain of command informed, this review helps identify any weaknesses in the plan and is a means to effect required coordination and support.
- Collect questioning support materials. The HUMINT collector will want to collect the various references and other guides that he will use to support his questioning. These materials may include source documents, maps, aerial photographs, imagery, OB data, extra lights, extra tables, drawing templates, graph paper, questioning guides, technical reference manuals, city plans and handbooks, and recording devices.
- Conduct required coordination. The HUMINT collector coordinates any support requirements including analytical, technical, or interpreter support, questioning location, ICFs, recording equipment, security, and transportation.
- Organize. The HUMINT collector organizes his materials in a logical manner that will complement his topical sequence. By being organized, the HUMINT collector will not waste time trying to locate the correct manual or guide. Additionally, the HUMINT collector will present a professional appearance to his source.
- Reconnoiter the questioning location. If the questioning location is to be somewhere other than the HUMINT collector's normal AO, such as a public restaurant, the HUMINT collector should conduct an unobtrusive reconnaissance of the site. If at all possible, this should be at the same time and day of the week as the planned meeting. This allows the HUMINT collector to assess the possible security problems

of the location, judge the traffic flow, and identify any other items that might affect the questioning. He can also judge where within the meeting site he can set up for maximum security and psychological advantage. He must be careful that in doing so he does not set up patterns of operation that will increase rather than decrease security problems.

- Set up questioning site. If the HUMINT collector has control over the site where the collection is being conducted, the last step in preparing is the actual setup of the questioning site. The HUMINT collector will want to decide on the placement of the furniture and lighting and where everyone will be seated and decide where he will place his technical support materials.
- Question guards. If the person to be questioned is a detainee, the HUMINT collector should arrange to question MP guards who have been in contact with the detainee to ascertain source behavior, attitude, and other useful information that guards may be able to provide.
- Check with medical personnel. If the detainee was injured or ill, ensure that he was treated by medical authorities and released for questioning.

7-26. The supervisor reviews each plan for legal considerations, appropriate goals in accordance with the collection objectives of the supported unit, and makes any changes he thinks are necessary. The supervisor ensures that contract interrogators are utilized in accordance with the scope of their contract and current policy. (See Appendix K.) After the plan is approved, the collection operation is executed. Prior to execution, the supervisor ensures mission brief back, rehearsal, and pre-combat inspections are conducted.

Chapter 8

Approach Techniques and Termination Strategies

8-1. Regardless of the type of operation, the initial impression that the HUMINT collector makes on the source and the approach he takes to gain the source's cooperation will have a lasting effect on the continuing relationship and the degree of success in collecting information. The approach used will vary based on the type of operation; the operational environment; the status of the source; the personality, position, and identity of the source; and the personality and experience level of the HUMINT collector and the time available.

8-2. The MPs will not take any actions to set conditions for interrogations (for example, "softening up" a detainee). Additionally, in accordance with DOD Directive 3115.09, military working dogs, contracted dogs, or any other dog in use by a government agency shall not be used as a part of an interrogation approach nor to harass, intimidate, threaten, or coerce a detainee for interrogation purposes. Leadership throughout the chain of command is responsible to ensure that HUMINT operations are in compliance with these governing regulations and guidelines, whether the HUMINT collection is to take place as part of HCT operations or in an internment facility.

8-3. The only authorized interrogation approaches and techniques are those authorized by and listed in this manual, in accordance with the Detainee Treatment Act of 2005. Two approaches, Mutt and Jeff and False Flag, require approval by the first O-6 in the interrogator's chain of command. The restricted interrogation technique "Separation" requires COCOM commander approval for use, and approval of each interrogation plan using "Separation" by the first General Officer/Flag Officer (GO/FO) in the chain of command. Coordination may also be required with the C/J/G2X, security, legal, or other personnel. Regardless of the coordination efforts required, use of all techniques at all locations must carefully comply with this manual and additional instructions contained in the latest DOD and COCOM policies.

NOTE: The word "source" will be used in this chapter to mean any person who is the objective of the HUMINT collector's approach, and is applicable in any collection situation unless otherwise noted in the text. This use of the term "source" is consistent with US Army Intelligence Center HUMINT collector training.

APPROACH PHASE

8-4. During the approach phase, the HUMINT collector establishes the conditions of control and rapport to facilitate information collection. The approach begins with initial contact between the source and the HUMINT collector. Extreme care is required since the success of the collection effort

hinges, to a large degree, on the early development of the source's willingness to communicate. Interrogators must have a deep understanding of the cultural norms, anomalies, and emotional triggers of the person being interrogated in order to select appropriate approach strategies and to interrogate effectively.

8-5. The HUMINT collector's objective during this phase is to establish a relationship with the source that results in the source providing accurate and reliable information in response to the HUMINT collector's questions. The HUMINT collector adopts an appropriate persona based on his appraisal of the source but remains alert for verbal and non-verbal clues that indicate the need for a change in the approach techniques. The amount of time spent on this phase will depend mostly on the probable quantity and value of information the source possesses, the availability of other sources with knowledge on the same topics, and available time. At the initial contact, a businesslike relationship should be maintained. As the source assumes a cooperative attitude, a more relaxed atmosphere may be advantageous. The HUMINT collector must carefully determine which of the various approach techniques to employ.

8-6. Sources will cooperate with the HUMINT collector for various reasons ranging from patriotic duty to personal gain, such as material gifts or money. They may also respond to emotion or logic. Regardless of the type of source and his outward personality, every source possesses exploitable characteristics that, if recognized by the HUMINT collector, can be used to facilitate the collection process. These characteristics may be readily apparent or may have to be extrapolated from the source's speech, mannerisms, facial expressions, physical movements, involuntary responses (perspiration, changes in breathing, eye movement), and other overt indications that vary from source to source. From a psychological standpoint, the HUMINT collector must be cognizant of the following behaviors. People tend to—

- Want to talk when they are under stress and respond to kindness and understanding during trying circumstances. For example, enemy soldiers who have just been captured have experienced a significant stress-producing episode. The natural inclination is for people to want to talk about this sort of experience. If the EPW has been properly segregated and silenced, the HUMINT collector will be the first person the EPW has a chance to talk to. This is a powerful tool for the collector to use to get the subject talking. The desire to talk may also be manifested in refugees, DPs, and even local civilians when confronted by an unsettled situation.
- Show deference when confronted by superior authority. This is culturally dependent but in most areas of the world people are used to responding to questions from a variety of government and quasi-government officials.
- Operate within a framework of personal and culturally derived values. People tend to respond positively to individuals who display the same value system and negatively when their core values are challenged.
- Respond to physical and, more importantly, emotional self-interest. This may be as simple as responding to material rewards such as extra

food or luxury items for their personal comfort or as complex as responding to support in rationalizing guilt.

- Fail to apply or remember lessons they may have been taught regarding security if confronted with a disorganized or strange situation.
- Be more willing to discuss a topic about which the HUMINT collector demonstrates identical or related experience or knowledge.
- Appreciate flattery and exoneration from guilt.
- Attach less importance to a topic if it is treated routinely by the HUMINT collector.
- Resent having someone or something they respect belittled, especially by someone they dislike.

8-7. HUMINT collectors do not "run" an approach by following a set pattern or routine. Each approach is different, but all approaches have the following in common. They—

- Establish and maintain control over the source and collection effort. This does not necessarily equate to physical control. Rather it means that the HUMINT collector directs the conversation to cover the topics that are of interest to him. This may be overt in a debriefing or an interrogation or subtle in an elicitation. In a very basic sense, the HUMINT collector is in control if he is asking questions and receiving answers. If the source is asking questions, refusing to answer questions, or directing or attempting to direct the exchange, he is challenging for control. If the source challenges this control, the HUMINT collector must act quickly and firmly to reestablish control.
- Establish and maintain a rapport between the HUMINT collector and the source. Rapport is a condition established by the HUMINT collector that is characterized by source confidence in the HUMINT collector and a willingness to cooperate with him. This does not necessarily equate to a friendly atmosphere. It means that a relationship is established and maintained that facilitates the collection of information by the HUMINT collector. The HUMINT collector may establish a relationship as superior, equal, or even inferior to the source. The relationship may be based on friendship, mutual gain, or even fear.
- Identify the source's primary emotions, values, traditions, and characteristics and use them to gain the source's willing cooperation.

8-8. The successful application of approach techniques, coupled with measures to ensure source veracity, results in the source providing accurate information in response to the HUMINT collector's requirements. The source may or may not be aware that he is providing the HUMINT collector with needed information. The approach does not end when the source begins providing information but is reinforced as necessary throughout the questioning.

DEVELOPING RAPPORT

8-9. The basis of rapport is source confidence in the HUMINT collector, which leads to a willingness to cooperate. Rapport does not necessarily mean a friendly relationship, although that may be the case. It means an establishment of a relationship in which the HUMINT collector presents a realistic persona designed to evoke cooperation from the source. The source responds with relevant, truthful information. Rapport is established during the approach and must be maintained throughout the questioning of the source. If the HUMINT collector has established good rapport initially and then abandons the effort, the source would rightfully begin to question the HUMINT collector's sincerity and may cease answering questions.

BUILDING RAPPORT

8-10. Building rapport is an integral part of the approach phase. The establishment of rapport begins when the HUMINT collector first encounters the source. Depending on the situation, the HUMINT collector may introduce himself to the source. In debriefing and liaison operations, this will normally be the collector's true name and affiliation. In elicitation, the requirement and type of introduction depends on the operation. In interrogation operations, the HUMINT collector normally will not introduce himself unless he is laying the groundwork for an approach. If he does introduce himself, normally he will adopt a duty position and rank supportive of the approach strategy selected during the planning and preparation phase. The HUMINT collector must select a rank and duty position that is believable based on the HUMINT collector's age, appearance, and experience. A HUMINT collector may, according to international law, use ruses of war to build rapport with interrogation sources, and this may include posing or "passing himself off" as someone other than a military interrogator. However, the collector must not pose as—

- A doctor, medic, or any other type of medical personnel.
- Any member of the International Committee of the Red Cross (ICRC) or its affiliates. Such a ruse is a violation of US treaty obligations.
- A chaplain or clergyman.
- A journalist.
- A member of the US Congress.

8-11. The HUMINT collector should seek advice from his SJA concerning representing himself as holding any other sensitive position.

8-12. A good source assessment is the basis for the approach and vital to the success of the collection effort. The HUMINT collector continually assesses the source to see if the approaches—and later the questioning techniques—chosen in the planning and preparation phase will indeed work. Approaches chosen in planning and preparation are tentative and based on the limited information available from documents, guards, and personal observation. This may lead the HUMINT collector to select approaches that may be totally incorrect for obtaining this source's willing cooperation. Thus, careful assessment of the source is critical to avoid wasting valuable time in the approach phase. Whether the HUMINT collector is using reasoned argument

or emotion to get the source to cooperate, he must be convincing and believable and appear sincere.

RAPPORT POSTURE

8-13. Unless there is rationale for acting otherwise, the HUMINT collector will begin his interaction with the source in a businesslike manner. He will be neither hostile nor overly friendly. Based on the tentative approaches developed during planning and preparation and the verbal and physical clues from the source, the HUMINT collector will modify this posture to facilitate collection.

8-14. Based on planning and preparation, the HUMINT collector may decide to adopt a stern posture. He presents himself as a person in a superior position to the interrogation source and demands proper deference and obedience by the interrogation source. In the case of an EPW this is manifested by having the source remain at attention and address the HUMINT collector as "Sir." This can be effective in dealing with lower ranking military personnel or members of oppressed ethnic, tribal, or religious groups who are conditioned to respond to authority or civilians in lower economic or social positions who are used to responding to directions from various bureaucrats and civilian superiors. This posture can have negative results since many persons in the positions mentioned above have developed mechanisms for dealing with superiors that mostly involve giving minimal information and agreeing with whatever the authority figure says.

8-15. In most cases, either initially or after the interrogation source has begun answering questions, the HUMINT collector will adopt a more relaxed or even sympathetic posture. The HUMINT collector addresses the interrogation source in a friendly fashion, striving to put him at ease. Regardless of the posture selected by the HUMINT collector, he must stay detached emotionally while maintaining the appearance of total involvement and stay within his adopted persona. The HUMINT collector must control his temper at all times. He must not show distaste, disgust, or unease at anything the source says unless that reaction is a planned part of the approach strategy. He should not show surprise at anything that the interrogation source says since it might undermine source confidence in the HUMINT collector and their relationship.

8-16. The HUMINT collector must support his verbal approaches with appropriate body language. Just as the HUMINT collector is observing the source to identify non-verbal clues that support or contradict the verbal message, the HUMINT collector is being scrutinized by the source to identify the same clues. The techniques used in an approach are a totality of effort, not just verbal conversation between the HUMINT collector and the source. Body language is in many instances culturally dependent. Standing at a given distance from an individual may be perceived as comforting in some societies and hostile in others. The HUMINT collector must adapt his body language to the culture in which he is working rather than expect the source to adapt to his.

APPROACH TECHNIQUES

8-17. The approaches listed are not guaranteed solutions for every situation. Some individual approaches that may be suitable for one operating environment, such as when conducting HUMINT contact operations, may be ineffective in another, such as interrogation. Some will be successful with one source and ineffective with another. In any case, everything the HUMINT collector says and does must be in compliance with the applicable law and policy under which the HUMINT collector is operating. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

8-18. There are 18 approach techniques that can be employed on any detainee regardless of status or characterization, including EPWs. Additionally, there is one restricted interrogation technique called separation (see Appendix M). Separation cannot be employed on EPWs. With the exception of the direct approach, which may be effective by itself, approach techniques are used in combination with other approaches and techniques. Transitions from one approach to another must be smooth, logical, and convincing.

DIRECT APPROACH

8-19. (Interrogation and Other MSO) Almost all HUMINT collection begins with the direct approach. The exception to this is during elicitation operations that by their very nature are indirect. In using the direct approach, the HUMINT collector asks direct questions (see Chapter 9). The initial questions may be administrative or nonpertinent but the HUMINT collector quickly begins asking pertinent questions. The HUMINT collector will continue to use direct questions as long as the source is answering the questions in a truthful manner. When the source refuses to answer, avoids answering, or falsely answers a pertinent question, the HUMINT collector will begin an alternate approach strategy. The fact that the source is answering questions does not preclude the HUMINT collector from providing an incentive to reward the source and continue his cooperation as long as that incentive does not slow down the collection. For example, a HUMINT collector might offer the source coffee or cigarettes to reward his cooperation. See Chapter 9 for the use of Repeat and Control questions in detecting deception.

8-20. Statistics from interrogation operations in World War II show that the direct approach was effective 90 percent of the time. In Vietnam and in Operations URGENT FURY (Grenada, 1983), JUST CAUSE (Panama, 1989), and DESERT STORM (Kuwait and Iraq, 1991), the direct approach was 95 percent effective. The effectiveness of the direct approach in Operations ENDURING FREEDOM (Afghanistan, 2001-2002) and IRAQI FREEDOM (Iraq, 2003) are still being studied; however, unofficial studies indicate that in these operations, the direct approach has been dramatically less successful. The direct approach is frequently employed at lower echelons when the tactical situation precludes selecting other techniques, and where

the EPW's or detainee's mental state is one of confusion or extreme shock. However, the HUMINT collector must remember that just because a source is answering a direct question does not mean he is being truthful.

INCENTIVE APPROACH

8-21. (Interrogation and Other MSO) The incentive approach is trading something that the source wants for information. The thing that you give up may be a material reward, an emotional reward, or the removal of a real or perceived negative stimulus. The exchange of the incentive may be blatant or subtle. On one extreme, the exchange may be a formal cash payment for information during some contact operations while on the other extreme it may be as subtle as offering the source a cigarette. Even when the direct approach is successful, the HUMINT collector may use incentives to enhance rapport and to reward the source for cooperation and truthfulness. The HUMINT collector must be extremely careful in selecting the options offered to a detainee source. He cannot deny the detainee anything that he is entitled to by law.

8-22. The HUMINT collector also should not offer anything that is not in his power to give. Although this might be expedient in the short term, in the long run it will eliminate source cooperation. When asked to provide something beyond his authority, the HUMINT collector can agree to help, check into, or otherwise support the request without committing himself to its successful accomplishment. HUMINT collectors must be cautious in the use of incentives for the following reasons:

- There is an inherent suspicion of the truthfulness of "bought" information. Sources may manufacture information in order to receive or maintain an incentive. Sources may also "hold back" information in the hopes of trading it at a later date for greater incentives. They may also hold back information if the incentive is not immediately available or guaranteed.
- The incentive must be believable and attainable. The incentive must be within the capability of the HUMINT collector's assumed persona to achieve. For example, if the detainee was captured after killing a US soldier, an incentive of release would not be realistic or believable. Likewise, if the interrogator is presenting himself as being a "harmless clerk" at the detention center, it would be unrealistic to expect a detainee to believe that a clerk could arrange to have the detainee's girlfriend brought to visit him. Such a visit might be possible, but the interrogator's assumed persona would not seemingly provide him with the authority to make it happen.
- The HUMINT collector must provide any promised incentive. A simple promise of an incentive may be sufficient to obtain immediate cooperation. If, however, the HUMINT collector does not follow through on providing the incentive, he will lose credibility and rapport with his source. This may end the cooperation of not only that source but also possibly any potential source who has contact with that source.
- The HUMINT collector may not state or even imply that the basic human rights guaranteed by applicable national and international

laws, regulations, and agreements will be contingent on a detained source's cooperation. An incentive for cooperation is viable only if the HUMINT collector has or is perceived to have the authority to withhold the incentive if the source is not cooperative. A HUMINT collector cannot promise an EPW that he will be treated in accordance with the GPW if he cooperates. This statement implies that the EPW will not be treated properly if he does not cooperate. Since the EPW must be treated in accordance with the GPW whether he cooperates or not, the HUMINT collector will rapidly lose credibility.

EMOTIONAL APPROACHES

8-23. (Interrogation and Other MSO) Emotional approaches are centered on how the source views himself and his interrelationships with others. Through source observation and initial questioning, the HUMINT collector can often identify dominant emotions that motivate the EPW/detainee. The motivating emotion may be greed, love, hate, revenge, or others. The emotion may be directed inward (feelings of pride or helplessness) or outward (love of family). The HUMINT collector employs verbal and emotional ruses in applying pressure to the source's dominant emotions. He then links the satisfaction of these emotions to the source's cooperation. Often, the presentation of like experiences and presenting the source with an opportunity to express his emotions is sufficient to result in cooperation. However, sometimes the source must be presented with a specific action or tangible manifestation of support.

8-24. Although the emotion is the key factor, an emotional approach is normally worthless without an attached incentive. The incentive must meet the criteria listed above for the incentive approach to ensure that the incentive is believable and attainable. For example, this technique can be used on the EPW/detainee who has a great love for his unit and fellow soldiers. Simply having the source express this emotion is not enough. After the source expresses this emotion, the HUMINT collector can take advantage of this by telling the EPW/detainee that by providing pertinent information, he may shorten the war or battle in progress and save many of his comrades' lives, but his refusal to talk may cause their deaths. This gives the source the alternatives of facing the status quo or expressing love of comrades through cooperating with the HUMINT collector.

8-25. Religion is an especially difficult topic to use in any emotional approach. An approach using religion may encourage the source to be further motivated by love, remorse, futility, or even pride to cooperate with the interrogator. On the other hand, an approach using religion may also encourage the source to end any rapport and cooperation with the interrogator. Although it is acceptable to use religion in all interrogation approaches, even to express doubts about a religion, an interrogator is not permitted to denigrate a religion's symbols (for example, a Koran, prayer rug, icon, or religious statue) or violate a religion's tenets, except where appropriate for health, safety, and security reasons. Supervisors should carefully consider the experience level of their subordinates before permitting the use of religion in any interrogation approach.

8-26. Similarly, supervisors should question the appropriateness of demeaning any racial group, including the source's, to elicit an emotional response during an interrogation approach.

8-27. One common danger to the use of emotional approaches is the development of an emotional attachment on the part of the HUMINT collector. It is natural that a source will develop an emotional attachment to the HUMINT collector. The HUMINT collector will often foster this attachment. However, it is vital the HUMINT collector not develop a corresponding emotional attachment to the source. This problem normally develops when a HUMINT collector has contact with one source or a group of similar sources over an extended period of time. There is transference of the source's problems to the HUMINT collector. For example, HUMINT collectors working in a refugee camp frequently begin to view the welfare of the refugees as a greater concern than HUMINT collection. The HUMINT collector, while developing emotion within the source, must act believably but at the same time he must remain detached. He must remember that the emotion is a means to an end (that is, information collection). Supervisors must carefully observe HUMINT collectors for signs of this emotional attachment to the source and take appropriate action ranging from counseling to reassignment.

8-28. The following are types of emotional approaches.

Emotional Love Approach

8-29. (Interrogation and Other MSO) Love in its many forms (friendship, comradeship, patriotism, love of family) is a dominant emotion for most people. The HUMINT collector focuses on the anxiety felt by the source about the circumstances in which he finds himself, his isolation from those he loves, and his feelings of helplessness. The HUMINT collector directs the love the source feels toward the appropriate object: family, homeland, or comrades. If the HUMINT collector can show the source what the source himself can do to alter or improve his situation or the situation of the object of his emotion, the approach has a chance of success.

8-30. The key to the successful use of this approach is to identify an action that can realistically evoke this emotion (an incentive) that can be tied to a detained source's cooperation. For example, if the source cooperates, he can see his family sooner, end the war, protect his comrades, help his country, help his ethnic group. A good HUMINT collector will usually orchestrate some futility with an emotional love approach to hasten the source's reaching the breaking point. In other words if the source does not cooperate, these things may never happen or be delayed in happening. Sincerity and conviction are critical in a successful attempt at an emotional love approach as the HUMINT collector must show genuine concern for the source, and for the object at which the HUMINT collector is directing the source's emotion. The emotional love approach may be used in any MSO where the source's state of mind indicates that the approach may be effective.

Emotional Hate Approach

8-31. (Interrogation and Other MSO) The emotional hate approach focuses on any genuine hate, or possibly a desire for revenge, the source may feel. The HUMINT collector must clearly identify the object of the source's hate and, if necessary, build on those feelings so the emotion overrides the source's rational side. The source may have negative feelings about his country's regime, immediate superiors, officers in general, or fellow soldiers. The emotional hate approach may be used in any MSO where the source's state of mind indicates that the approach may be effective.

8-32. The emotional hate approach may be effective on members of racial or religious minorities who have or feel that they have faced discrimination in military and civilian life. The "hate" may be very specific. For example, a source may have great love for his country, but may hate the regime in control. The HUMINT collector must be sure to correctly identify the specific object of the hate. The emotional hate approach is most effective with the immature or timid source who may have had no opportunity up to this point for revenge, or never had the courage to voice his feelings.

8-33. As in the emotional love approach, the key to the successful application is the linking of the emotion with a tangible manifestation of that emotion. The HUMINT collector must be extremely careful that he does not promise anything that would be contrary to national or international law or US interests or goals. For example, if an EPW feels he has been treated unfairly in his unit, the HUMINT collector can point out that, if the source cooperates and divulges the location of that unit, the unit can be destroyed, thus affording the source revenge. But he cannot promise that the unit if attacked would not be allowed to surrender or that the unit if it surrenders will be treated badly.

8-34. The HUMINT collector must be careful that he does not assume that casual negative comments equate to a strong hate. Many soldiers will make negative comments against their army but will support and defend their army against any "outsider." The HUMINT collector should also not assume generalities; for example, assuming that a member of an ethnic minority hates the ethnic majority just because most ethnic minorities hate those in the ethnic majority.

Emotional Fear-Up Approach

8-35. (Interrogation and Other MSO) Fear is another dominant emotion that can be exploited by the HUMINT collector. In the fear-up approach, the HUMINT collector identifies a preexisting fear or creates a fear within the source. He then links the elimination or reduction of the fear to cooperation on the part of the source. The HUMINT collector must be extremely careful that he does not threaten or coerce a source. Conveying a threat may be a violation of the UCMJ. The HUMINT collector should also be extremely careful that he does not create so much fear that the source becomes unresponsive. The HUMINT collector should never act as if he is out of control or set himself up as the object or focal point of the source's fear. If the HUMINT collector acts in this manner, it is extremely difficult to then act as

the outlet for the fear. Supervisors should consider the experience level of their subordinates before approving their use of this approach.

8-36. If there is a justifiable fear, the HUMINT collector should present it and present a plan to mitigate it if the source cooperates (combination of emotional and incentive approaches). For example, an EPW source says that he will not cooperate because if he does his fellow prisoners will kill him or, if a contact source says that if people find out he is cooperating, his family will suffer. In these cases, the HUMINT collector can point out that the source has already placed himself at risk and he or his family may suffer whether he cooperates or not (justified fear). But if he cooperates, the HUMINT collector will do his best to ensure that either no one will find out or that he will be protected (incentive).

8-37. If there is no justified fear, the HUMINT collector can make use of non-specific fears. "You know what can happen to you here?" A fear-up approach is normally presented in a level, unemotional tone of voice. For example, "We have heard many allegations of atrocities committed in your area and anyone that was involved will be severely punished" (non-specific fear). "If you cooperate with me and answer all of my questions truthfully, I can make sure you are not falsely accused" (incentive). The source should demonstrate some indication of fear, whether verbal or non-verbal, prior to using this approach. If a fear is pre-existing, the approach will work and is legal. If there is no indication of fear, another approach should be considered.

8-38. It is often very effective to use the detainee's own imagination against him. The detainee can often visualize exactly what he is afraid of better than the HUMINT collector can express it.

8-39. The "fear-up" approach is frequently used in conjunction with the emotional love or hate approaches. For example, the HUMINT collector has already established that a detainee source has a strong love of family but is now separated from them. He may state, "I wonder how your family is getting along without you?" (fear of the unknown). He then promises to allow the detainee more than the minimum two letters a month required by the GPW.

Emotional Fear-Down Approach

8-40. (Interrogation and Other MSO) The emotion of fear may dominate the source to the point where he is unable to respond rationally to questioning, especially in interrogation sources. However, the fear-down approach may be used in any MSO where the source's state of mind indicates that it would be an appropriate approach to use. In the fear-down approach the HUMINT collector mitigates existing fear in exchange for cooperation on the part of the source. This is not normally a formal or even voiced agreement. Instead, the HUMINT collector through verbal and physical actions calms the source. Psychologically, the source then views the HUMINT collector as the protector or the one who is providing the calm and wishes to help the HUMINT collector in gratitude and in order to maintain the HUMINT collector as the protector. When used with a soothing, calm tone of voice and appropriate body language, a fear-down approach often creates rapport and nothing else may be needed to get the source to cooperate. At times, however, the

HUMINT collector must describe concrete actions that he will take in order to remove the source's fear.

8-41. Frequently the object of the fear is too traumatic for the source to face directly. While calming the source, the HUMINT collector may initially ask nonpertinent questions and avoid the subject that has caused the source's fear. This develops rapport and establishes communication. The HUMINT collector must remember that his goal is collecting information, not concern with the psychological well being of the source. He will be concerned with the latter only insofar as it helps him obtain the former. This approach technique may backfire if allowed to go too far. After convincing the source he has nothing to fear, the source may cease to be afraid and may feel secure enough to resist the HUMINT collector's pertinent question.

Emotional-Pride and Ego-Up Approach

8-42. (Interrogation and Other MSO) The emotional-pride and ego-up approach may be used in any MSO. It exploits a source's low self-esteem. Many HUMINT sources including EPWs and other detainees, retained persons, civilian internees, or refugees may suffer from low self-esteem and feelings of helplessness due to their immediate circumstances. Others, such as individuals or members of social or ethnic groups that have been discriminated against or low-ranking members of organizations (including the military), may also show low self-worth. In this technique, the source is flattered into providing certain information in order to gain credit and build his ego. The HUMINT collector must take care to use a flattering somewhat-in-awe tone of voice, and speak highly of the source throughout this approach while remaining believable. This should produce positive feelings on the source's part as he receives desired recognition. The source will eventually reveal pertinent information to solicit more favorable comments from the HUMINT collector.

8-43. This technique can also be employed in another manner—by flattering the source into admitting certain information in order to gain credit. For example, while interrogating a suspected saboteur, the HUMINT collector states: "This was a smooth operation. I have seen many previous attempts fail. I bet you planned this. Who else but a clever person like you would have planned it? When did you first decide to do the job?"

8-44. A variation of this approach can also be used on individuals with strong egos. It is based on the premise that everyone likes to talk about what they do best. The HUMINT collector shows interest in and asks the source to explain an aspect of his job. The questioning begins with nonpertinent aspects of the source's job. The HUMINT collector displays interest and asks increasingly technical and pertinent questions. For example, if the source is an EPW who was a pilot, the HUMINT collector might begin by asking him what it is like to fly. As the source talks about this, the collector demonstrates interest and gradually uses questions to lead the conversation to capabilities of specific aircraft, specific missions that the pilot has flown, tactics, or whatever topic is a priority for collection.

Emotional-Pride and Ego-Down Approach

8-45. (Interrogation) The emotional-pride and ego-down approach is based on attacking the source's ego or self-image. The source, in defending his ego, reveals information to justify or rationalize his actions. This information may be valuable in answering collection requirements or may give the HUMINT collector insight into the viability of other approaches. This approach is effective with sources who have displayed weakness or feelings of inferiority. A real or imaginary deficiency voiced about the source, loyalty to his organization, or any other feature can provide a basis for this technique.

8-46. The HUMINT collector accuses the source of weakness or implies he is unable to do a certain thing. This type of source is also prone to excuses and rationalizations, often shifting the blame to others. An example of this technique is opening the collection effort with the question, "Why did you surrender so easily when you could have escaped by crossing the nearby ford in the river?" The source is likely to provide a basis for further questions or to reveal significant information if he attempts to explain his surrender in order to vindicate himself. He may give an answer such as, "No one could cross the ford because it is mined."

8-47. The objective is for the HUMINT collector to use the source's sense of pride by attacking his loyalty, intelligence, abilities, leadership qualities, slovenly appearance, or any other perceived weakness. This will usually goad the source into becoming defensive, and he will try to convince the HUMINT collector he is wrong. In his attempt to redeem his pride and explain his actions, the source may provide pertinent information. Possible targets for the emotional-pride and ego-down approach are the source's—

- Loyalty.
- Technical competence.
- Leadership abilities.
- Soldierly qualities.
- Appearance.

8-48. There is a risk associated with this approach. If the emotional-pride and ego-down approach fails, it is difficult for the HUMINT collector to recover and move to another approach without losing his credibility. Also, there is potential for application of the pride and ego approach to cross the line into humiliating and degrading treatment of the detainee. Supervisors should consider the experience level of their subordinates and determine specifically how the interrogator intends to apply the approach technique before approving the interrogation plan.

Emotional-Futility

8-49. (Interrogation and Other MSO) The emotional-futility approach is generally used in an interrogation setting, but may also be used for other MSO, if indicated by the source's state of mind. In the emotional-futility approach, the HUMINT collector convinces the source that resistance to questioning is futile. This engenders a feeling of hopelessness and helplessness on the part of the source. Again as with the other emotional approaches, the HUMINT collector gives the source a "way out" of the

helpless situation. For example "it is hopeless for your forces to continue fighting because they can no longer get supplies, but you can help end the war and their suffering." When employing this technique, the HUMINT collector must have factual information. The HUMINT collector presents these facts in a persuasive, logical manner. He should be aware of and able to exploit the source's psychological and moral weaknesses, as well as weaknesses inherent in his society.

8-50. The futility approach is effective when the HUMINT collector can play on doubts that already exist in the source's mind. Factual or seemingly factual information must be presented in a persuasive, logical manner, and in a matter-of-fact tone of voice. Making the situation appear hopeless allows the source to rationalize his actions, especially if that action is cooperating with the HUMINT collector. When employing this technique, the HUMINT collector must not only have factual information but also be aware of and exploit the source's psychological, moral, and sociological weaknesses. Another way of using the futility approach is to blow things out of proportion. If the source's unit was low on, or had exhausted, all food supplies, he can be easily led to believe all of his forces had run out of food. If the source is verging on cooperating, it may aid the collection effort if he is told all the other sources have cooperated.

8-51. The futility approach must be orchestrated with other approach techniques (for example, love of comrades). A source who may want to help save his comrades' lives may be convinced the battlefield situation is hopeless and they will die without his assistance. The futility approach is used to paint a bleak picture for the prisoner, but it is not normally effective in and of itself in gaining the source's cooperation.

Other Approaches

8-52. There are numerous other approaches but most require considerable time and resources. Most are more appropriate for use with sources who are detainees, but some, such as change of scenery, may have application for elicitation or MSO.

8-53. **We Know All**. (Interrogation) In the "we know all" approach technique, the HUMINT collector subtly convinces the source that his questioning of the source is perfunctory because any information that the source has is already known. This approach may be employed in conjunction with the "file and dossier" technique or by itself. If used alone, the HUMINT collector must first become thoroughly familiar with available data concerning the source and the current situation. To begin the collection effort, the HUMINT collector asks questions based on this known data.

8-54. When the source hesitates, refuses to answer, or provides an incorrect or incomplete reply, the HUMINT collector provides the detailed answer himself. The HUMINT collector may even complete a source's answer, as if he is bored and just "going through the motions." When the source begins to give accurate and complete information, the HUMINT collector interjects pertinent questions. Questions to which answers are already known are also asked periodically to test the source's truthfulness and to maintain the deception that the information is already known. There are some inherent

problems with the use of the "we know all" approach. The HUMINT collector is required to prepare everything in detail, which is time consuming. He must commit much of the information to memory, as working from notes may show the limits of the information actually known. It is also only usable when sufficient prior information exists to convince the source that "we know all."

8-55. **File and Dossier**. (Interrogation) The file and dossier approach is a variation of the "we know all" approach. The HUMINT collector prepares a dossier containing all available information concerning the source or his organization. The information is carefully arranged within a file to give the illusion that it contains more data than actually there. The file may be padded with extra paper if necessary. Index tabs with titles such as education, employment, criminal record, military service, and others are particularly effective. It is also effective if the HUMINT collector is reviewing the dossier when the source enters the room and the source is able to read his name on the dossier and sees the numerous topics and supposed extent of the files.

8-56. The HUMINT collector proceeds as in the "we know all" approach. He refers to the particular labeled segment of the dossier before, during, or after asking a question. In the early stages of questioning, the HUMINT collector asks questions to which he has the answer. He may answer along with the source, complete the information for the source, or even show the source where the information is entered in the dossier. He never lets the source physically handle the dossier. As the source becomes convinced that all the information that he knows is contained within the dossier, the HUMINT collector proceeds to topics on which he has no or little information. In doing so, he still refers to the appropriate section of the dossier and may even nod his head knowingly or tell the source that the information the source is providing still matches what is in the dossier.

8-57. This technique has several limitations and drawbacks. The preparation time in developing the dossier is extensive. The success of this technique is largely dependent on the naiveté of the source, volume of data on the subject, and skill of the HUMINT collector in convincing the source that the dossier is more complete than it actually is. There is also the risk that a less naïve source will refuse to cooperate, claiming that, if the collector already knows everything, there is no need for him to talk. Also with this technique, the HUMINT collector is limited in the method he may use to record new information. If the HUMINT collector writes down information, it destroys the illusion that all the information has already been obtained. The HUMINT collector is normally limited to using electronic recording devices or his memory. The HUMINT collector can also arrange ahead of time for another interrogator or analyst to take notes for him, undetected by the source. This could be especially effective in a situation where a separate monitoring area (for oversight) is used by the analyst.

8-58. **Establish Your Identity**. (Interrogation) In using this approach, the HUMINT collector insists the detained source has been correctly identified as an infamous individual wanted by higher authorities on serious charges, and he is not the person he purports to be. In an effort to clear himself of this

allegation, the source makes a genuine and detailed effort to establish or substantiate his true identity. In so doing, he may provide the HUMINT collector with information and leads for further development. The HUMINT collector should initially refuse to believe the source and insist he is the individual wanted by the ambiguous higher authorities. This will force the source to give even more detailed information in order to convince the HUMINT collector he is who he says he is.

8-59. **Repetition**. (Interrogation) The repetition approach is used to induce cooperation from a hostile source. In one variation of this approach, the HUMINT collector listens carefully to a source's answer to a question, and then repeats the question and answer several times. He does this with each succeeding question until the source becomes so thoroughly bored with the procedure, he answers questions fully and candidly to satisfy the HUMINT collector and gain relief from the monotony of this method. The repetition technique must be judiciously used, as it will generally be ineffective when employed against introverted sources or those having great self-control. It may also provide an opportunity for a source to regain his composure and delay the collection effort. In this approach, the use of more than one HUMINT collector or a tape recorder has proven effective.

8-60. **Rapid Fire**. (Interrogation) The rapid-fire approach is based upon the principles that—

- Everyone likes to be heard when he speaks.
- It is confusing to be interrupted in mid-sentence with an unrelated question.

8-61. This approach may be used by one, two, or more HUMINT collectors to question the source. In employing this technique, the HUMINT collectors ask a series of questions in such a manner that the source does not have time to answer a question completely before the next one is asked. This confuses the source, and he will tend to contradict himself as he has little time to formulate his answers. The HUMINT collectors then confront the source with the inconsistencies causing further contradictions. In many instances, the source will begin to talk freely in an attempt to explain himself and deny the HUMINT collector's claims of inconsistencies. In this attempt, the source is likely to reveal more than he intends, thus creating additional leads for further exploitation. This approach may be orchestrated with the emotional-pride and ego-down or fear-up approaches. Besides extensive preparation, this approach requires experienced and competent HUMINT collectors, with comprehensive case knowledge and fluency in the source's language.

8-62. **Silent**. (Interrogation) The silent approach may be successful when used against either a nervous or confident source. When employing this technique, the HUMINT collector says nothing to the source, but looks him squarely in the eye, preferably with a slight smile on his face. It is important not to look away from the source but force him to break eye contact first. The source may become nervous, begin to shift in his chair, cross and re-cross his legs, and look away. He may ask questions, but the HUMINT collector should not answer until he is ready to break the silence. The source may blurt out questions such as, "Come on now, what do you want with me?" When the HUMINT collector is ready to break silence, he may do so with questions

such as, "You planned this operation for a long time, didn't you? Was it your idea?" The HUMINT collector must be patient when using this technique. It may appear the technique is not succeeding, but usually will when given a reasonable chance.

8-63. **Change of Scenery**. (Interrogation and Other MSO) The change-of-scenery approach may be used in any type of MSO to remove the source from an intimidating atmosphere such as an "interrogation" room type of setting and to place him in a setting where he feels more comfortable speaking. Bringing a source into a formal setting to conduct an interrogation or debriefing has psychological implications. On the positive side, it places the HUMINT collector in a superior position since he is operating on his "home turf" and has set the conditions for the meeting. It allows the HUMINT collector control over the immediate environment including the positioning of the participants, to establish the desired atmosphere for the approach.

8-64. However, there are potential negative factors in the conduct of questioning in an "Interrogation Room" environment. The source may be intimidated and more guarded; he may consider the formal setting in terms of an adversarial relationship; and he may limit his answers as a mode of self-protection. In some circumstances, the HUMINT collector may be able to invite the source to a different setting for coffee and pleasant conversation. When removed from the formal environment, the source may experience a feeling of leaving the interrogation behind. The perceived reduced pressure may lower his guard and allow him to attach less significance to conversation that occurs outside the formal setting, even though pertinent information is still being discussed. During the conversation in this more relaxed environment, the HUMINT collector steers the conversation to the topic of interest. Through this somewhat indirect method, he attempts to elicit the desired information. The source may never realize he is still being questioned.

8-65. **Mutt and Jeff. (Interrogation)** The goal of this technique is to make the source identify with one of the interrogators and thereby establish rapport and cooperation. This technique involves a psychological ploy that takes advantage of the natural uncertainty and guilt that a source has as a result of being detained and questioned. Use of this technique requires two experienced HUMINT collectors who are convincing actors. The two HUMINT collectors will display opposing personalities and attitudes toward the source. For example, the first HUMINT collector is very formal and displays an unsympathetic attitude toward the source. He may, for instance, be very strict and order the source to follow all military courtesies during questioning. Although he conveys an unfeeling attitude, the HUMINT collector is careful not to threaten or coerce the source. Conveying a threat of violence is a violation of the UCMJ.

8-66. At the point when the interrogator senses the source is vulnerable, the second HUMINT collector appears (having received his cue by a signal, hidden from the source, or by listening and observing out of view of the source), and scolds the first HUMINT collector for his uncaring behavior and orders him from the room. The second HUMINT collector then apologizes to soothe the source, perhaps offering him a beverage and a cigarette. He

explains that the actions of the first HUMINT collector were largely the result of an inferior intellect and lack of sensitivity. The inference is that the second HUMINT collector and the source share a high degree of intelligence and sensitivity.

8-67. The source is normally inclined to have a feeling of gratitude towards the second HUMINT collector, who continues to show sympathy in an effort to increase rapport and control for the questioning that will follow. If the source's cooperation begins to fade, the second HUMINT collector can hint that he is a busy person of high rank, and therefore cannot afford to waste time on an uncooperative source. He can broadly imply that the first HUMINT collector might return to continue the questioning. The Mutt and Jeff approach may be effective when orchestrated with Pride and Ego Up and Down, Fear Up and Down, Futility, or Emotional Love or Hate.

8-68. **Oversight Considerations:** Planned use of the Mutt and Jeff approach must be approved by the first O-6 in the interrogator's chain of command. The HUMINT collector must include as a part of the interrogation plan—

- No violence, threats, or impermissible or unlawful physical contact.
- No threatening the removal of protections afforded by law.
- Regular monitoring of the interrogation shall be performed by interrogation personnel.

8-69. **False Flag.** (Interrogation) The goal of this technique is to convince the detainee that individuals from a country other than the United States are interrogating him, and trick the detainee into cooperating with US forces. For example, using an interrogator who speaks with a particular accent, making the detainee believe that he is actually talking to representatives from a different country, such as a country that is friendly to the detainee's country or organization. The False Flag approach may be effectively orchestrated with the Fear Down approach and the Pride and Ego Up.

8-70. **Oversight Considerations:** The interrogation chain of command must coordinate an interrogation plan that uses the False Flag approach with the legal representative and the 2X, and receive approval from the first O-6 in the interrogator's chain of command for each specific use of the False Flag approach.

- The use of the False Flag approach must complement the overall interrogation strategy and other approach techniques listed in the interrogation plan.
- When a HUMINT collector intends to pose as a national of a third-party country, that country must be identified in the interrogation plan.
- No implied or explicit threats that non-cooperation will result in harsh interrogation by non-US entities.
- HUMINT collectors will not pose or portray themselves as any person prohibited by this manual, paragraphs 8-10 and 8-11 (for example, an ICRC representative).

8-71. **Separation.** See Appendix M, Restricted Interrogation Technique – Separation.

Selecting an Approach

8-72. There often is insufficient information available to determine an approach other than the direct approach. In this case where the source answers questions but will not discuss pertinent issues, the HUMINT collector may ask direct but nonpertinent questions to obtain sufficient information to develop an approach strategy. This technique is also useful in debriefing to establish rapport. Nonpertinent questions may include—

- Asking about immediate past events. This includes asking an EPW about the circumstances of his capture or asking a refugee about the circumstances concerning his arrival at the refugee point or checkpoint. By doing this, the HUMINT collector can gain insight into the source's current state of mind and, more importantly, he can ascertain his possible approach techniques.
- Asking background questions. This includes asking about the source's family, work, friends, likes, and dislikes. These types of questions can develop rapport and provide clues as to the source's areas of knowledge or reveal possibilities for incentives or emotional approaches.
- Considering what are culturally and socially acceptable topics of discussion. For example, asking an Arab male about his wife could be considered extremely rude, whereas not asking an American the same question might be seen as insensitive.

Making Smooth Transitions

8-73. With the exception of the direct approach, no other approach is effective by itself. HUMINT collectors use different approach techniques or combine them into a cohesive, logical technique. Smooth transitions, sincerity, logic, and conviction are needed to make a strategy work. HUMINT collectors must carefully assess the source's verbal or nonverbal clues to determine when a change in approach strategy is required. The HUMINT collector must guide the conversation smoothly and logically, especially when moving from one approach technique to another. Using transitional phrases can make logical and smooth tie-ins to another approach. By using nonpertinent questions, the HUMINT collector can move the conversation in the desired direction and, as previously stated, sometimes can obtain leads and hints about the source's stresses or weaknesses or other approach strategies that may be more successful.

Recognizing Source Cooperation

8-74. Each source has a point where he will begin to cooperate and answer questions. Some sources will begin answering questions completely and truthfully with no preparation; others might require hours or even days of work. The amount of time that a HUMINT collector spends on an approach depends on a variety of factors. These include—

- The quality and criticality of the information believed to be possessed by the source.
- The presence or absence of other sources that probably possess that information.
- The number of HUMINT collectors and sources available.
- The LTIOV that the HUMINT collector is attempting to obtain.

8-75. The HUMINT collector needs to identify the signs that the source is approaching or has reached the point of cooperation. For example, if during the approach the source leans forward with his facial expression indicating an interest in the proposal or is more hesitant in his argument, he is probably nearing the point where he will cooperate. The HUMINT collector must also be aware of the fact that a source can begin to cooperate in certain areas while continuing to resist strongly in other areas. The HUMINT collector should recognize the reason for refusal, overcome the objection, and stress the benefit of cooperating (reinforce the approach). Once the HUMINT collector determines the source is cooperating, he should interject pertinent questions. If the source does not answer the question, the HUMINT collector should continue with his approach or switch to an alternate approach technique and continue to work until he again believes the source will cooperate. If the source answers the pertinent question, the HUMINT collector continues asking relevant questions until the questioning session is completed.

8-76. If a cooperative source balks at answering a specific line of questions, the HUMINT collector must assess the reason for the refusal. The HUMINT collector may have arrived at a topic that the source finds particularly sensitive. Other reasons that might cause a source to stop answering questions are fatigue or unfamiliarity with the new topic. If this topic is critical, the HUMINT collector may have to reinforce the previously successful approach or may have to use a different approach.

APPROACH STRATEGIES FOR INTERROGATION

8-77. Interrogation does not mean a hostile relationship between the HUMINT collector and the source. In fact, most interrogation sources (90 percent or more) cooperate in response to the direct approach. Unfortunately, those sources who have the placement and access to make them high priority sources are also the ones with the highest degree of security awareness. A source who uses counter-interrogation techniques such as delaying, trying to control the conversation, or interrogating the HUMINT collector himself may—

- Be an intelligence trained soldier.
- Be survival, evasion, resistance, and escape (SERE) trained.
- Be a terrorist.
- Have been a detainee or previously incarcerated.

8-78. In stability and reconstruction operations and civil support operations, detainees are often politically motivated and resistant to most approaches.

8-79. EPWs are normally vulnerable to basic incentive and emotional approach techniques. Most EPWs are traumatized to various degrees by the events preceding or surrounding their capture. They tend to be disoriented and exhibit high degrees of fear and anxiety. This vulnerable state fades over time, and it is vital for HUMINT collectors to interrogate EPWs as soon as and as close to the point of capture as possible. The earlier that an EPW is questioned the more likely he is to cooperate. And the earlier that he begins to cooperate, the more likely he is to continue to cooperate. It is also vital that the HUMINT collector be the first person that the EPW has a chance to talk to. This means that proper silencing and segregation of the sources by whoever is transporting them is an important part of a successful approach.

8-80. The vulnerability of civilian detainees to approach techniques available to the HUMINT collector may be dependent on the exact nature of the conflict. US HUMINT collectors are obligated to treat all detainees in accordance with applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Detainees and, in particular, EPWs are guaranteed certain rights and privileges. The HUMINT collector may not take any action to remove, state that he will remove, or imply that he will remove any guaranteed right if a detainee fails to cooperate. Under the GPW, EPWs cannot be denied their rights or their privileges accorded them by rank as guaranteed by the GPW. Privileges afforded to them, however, which are not guaranteed by the Geneva Conventions or other applicable law or agreements, may be withheld. (See Appendix A, Section I.) Consult your SJA for questions concerning rights and privileges.

8-81. The HUMINT collector is frequently under a great deal of pressure to "produce results." This situation, coupled with the facts that the HUMINT collector is dealing with threat personnel who may have been attempting to kill US personnel just minutes before questioning and the fact that the source is in a vulnerable state, leads to a tendency to use fear-up techniques. This may, in some circumstances, be the proper approach; however, the HUMINT collector must ensure that in doing so he neither loses control of his own emotions nor uses physical or mental coercion.

APPROACH STRATEGIES FOR DEBRIEFING

8-82. Sources who are debriefed vary even more widely than those who are interrogated. Since debriefing is the systematic questioning of individuals not in the custody of the questioning forces, the HUMINT collector needs to engender an atmosphere of cooperation and mutual benefit. Some sources for debriefing include members of the friendly forces and local personnel. HUMINT collectors often believe that approach techniques are not required for friendly forces and that friendly forces should view debriefing as part of their duties and in their own best interest. However, this is not necessarily the case.

8-83. Many people see debriefing as an interruption in their normal duties and a waste of their time. HUMINT collectors must be sure to stay focused on the purpose and goals of the debriefing. They should be businesslike and must maintain the proper relationship with the source based on his rank and position. The HUMINT collector should allow senior sources more latitude to interpose their opinions and evaluations. A change of scene often facilitates the debriefing of a high-level source since it removes him from his normal distractions, such as the telephone, and allows him to concentrate on the topics being discussed.

8-84. Refugees and DPs are subject to many of the same anxieties and trauma that are experienced by EPWs or other detainees, with the added benefit to the HUMINT collector that they normally have an obvious vested interest in cooperating. Basic incentives usually are sufficient to induce their willing cooperation. The emotional support that can be provided by the HUMINT collector by simply listening and commiserating with their hardship is often sufficient to gain cooperation. The emotional approaches such as love of family and hate toward those who made them refugees are strong motivators toward cooperation.

8-85. The approach techniques used in the questioning of local civilians are probably the most difficult. The approach techniques chosen must take into consideration the attitude of the local population toward the US and its presence and cultural considerations. The local population must see their cooperation as self-beneficial.

APPROACH STRATEGIES FOR ELICITATION

8-86. Elicitation is a sophisticated technique used when conventional collection techniques cannot be used effectively. Of all the collection methods, this one is the least obvious. However, it is important to note that elicitation is a planned, systematic process that requires careful preparation. It is always applied with a specific purpose in mind. This objective is the key factor in determining the subject (which source to question), the elicitor, and the setting. The subject will be selected based on access to or knowledge of the desired information.

8-87. Before approaching the subject, it is necessary to review all available intelligence files and records, personality dossiers, and knowledge possessed by others who have previously dealt with the subject. This will help determine the subject's background, motivation, emotions, and psychological nature. It also may require unobtrusive observation of the subject to establish such things as patterns of activity and likes and dislikes. The setting can be any number of social or official areas. It is important to note that the source should be approached in his natural surroundings, as this will diminish suspicion.

8-88. The key to elicitation is the establishment of a rapport between the elicitor and the source, normally based on shared interests. In the initial stages of an elicitation, the collector confines his conversations to innocuous subjects such as sports and social commentary. Dependent on the value of the source, the collection environment, and the security consciousness of the

source the initial stage could last from a few minutes to numerous seemingly accidental meetings over a period of weeks or months. The HUMINT collector will gradually shift the conversation to topics of collection interest but will be prepared to return to more unthreatening topics based on negative reactions on the part of the subject. Once a topic of interest has been introduced, the HUMINT collector keeps the conversation going by asking for clarification (for example, "I agree, however, what did you mean by….?") or expressing a hypothetical situation.

8-89. There are two basic elicitation approaches: mild flattery and provocation.

- Mild Flattery: Most people like talking about their interests and like talking to those who are knowledgeable and interested in the same topics. People also like to speak to someone who values their opinion on shared interests. The HUMINT collector takes advantage of this. The HUMINT collector leads the conversation into areas that he wishes to collect but does it in such a way that it appears to the source that the source is leading the conversation. Above all in elicitation, the HUMINT collector plays the role of the rapt, attentive, and inquisitive listener.
- Provocation: This is a more dangerous approach and, if used too early in an operation, can alienate the source. Once the HUMINT collector has established shared interests with the source, he can selectively challenge some of the source's statements, encouraging the source to provide more information in support of his view. The HUMINT collector can also insert bits of actual information into the conversation to cause the source to confirm and expound on the topic. Care must be taken so as not to give away more information than is gained.

TERMINATION PHASE

8-90. When it is necessary or prudent, the HUMINT collector will terminate the questioning of a particular source. Whatever the reason for terminating, the HUMINT collector must remember there is a possibility that someone may want to question the source at a later date. There are many reasons why a HUMINT collector may want or need to terminate questioning:

- The source remains uncooperative during the approach phase.
- The collection objective cannot be met in one questioning session.
- The HUMINT collector fails to maintain rapport and loses control of the questioning.
- The collection objectives have been satisfied.
- The HUMINT collector or the source becomes physically or mentally unable to continue.
- Information possessed by the source is of such value that his immediate evacuation to the next echelon is required.
- The HUMINT collector's presence is required elsewhere.

8-91. There are many ways to conduct a termination, but the following points must be conveyed to the source:

- The HUMINT collector should sincerely and convincingly reinforce successful approaches. All promised incentives should be rendered.
- The source must be told the information he gave will be checked for truthfulness and accuracy. His reaction to this statement should be closely monitored. The exact form of this statement will be dependent on the situation. It should not be done in a manner to alienate a cooperative source.
- The source must be told that the same or another individual may speak to him again. This sets the stage for future contacts.
- Any identification must be returned to the source. If the HUMINT collector has other documents or belongings of the detainee (such as letters or photographs), he will either return them to the detainee, if appropriate, or will turn them over to the MP guard. Depending on the circumstances and the legal status of the detainee, the MPs will retain the detainee's property and return the property to him at the end of his internment.
- In a debriefing, the HUMINT collector will normally ask the source not to discuss the subject of the questioning for his own protection. In interrogation operations, the HUMINT collector normally coordinates with the holding area guards to have the detainees who have been interrogated kept separate from sources who have not yet been interrogated if the situation allows.

Chapter 9

Questioning

9-1. Questioning is one of the five phases of HUMINT collection. Developing and using good questioning techniques enable the HUMINT collector to obtain accurate and pertinent information and to extract the maximum amount of information in the minimum amount of time. The HUMINT collector must know when to use different types of questions.

GENERAL QUESTIONING PRINCIPLES

9-2. Questions should be presented in a logical sequence to avoid neglecting significant topics. The HUMINT collector begins the questioning phase with the first topic in the sequence he tentatively established as part of his questioning plan. He obtains all of the source's pertinent knowledge in this topical area before moving on to the next topic in his sequence. The only exception is exploiting a hot lead, which is discussed in paragraph 9-21.

9-3. The HUMINT collector must at all times remember that his mission is the rapid collection and dissemination of accurate information. He must not allow himself to be sidetracked into nonpertinent discussions or debates nor should he express distaste or value judgments on the information being supplied unless that is a planned part of his approach technique. The HUMINT collector uses vocabulary that is clear, unambiguous, and understandable by the source. The source may not be on the same intellectual level or have the same degree of education as the HUMINT collector, so the HUMINT collector must adapt his questioning to the level of the source. The source may also have specific technical knowledge, more education and/or a higher intellectual level than the HUMINT collector. In this case, the HUMINT collector normally relies on prepared questions or technical support for his questioning. Without good systematic questioning techniques, even the most cooperative source may provide only minimal usable information.

DIRECT QUESTIONS

9-4. Direct questions are basic questions normally beginning with an interrogative (who, what, where, when, how, or why) and requiring a narrative answer. They are brief, precise, and simply worded to avoid confusion. The HUMINT collector must consider the probable response of the source to a particular question or line of questioning and should not, if at all possible, ask direct questions likely to evoke a refusal to answer or to antagonize the source.

TYPES OF DIRECT QUESTIONS

9-5. The HUMINT collector must be able to use the following types of direct questions:

- Initial, topical.
- Follow-up.
- Nonpertinent.
- Repeat.
- Control.
- Prepared.

Initial Questions

9-6. The HUMINT collector begins his questioning with the first topic in his collection plan and asks all the basic questions necessary to cover the topic. The answers to the basic questions will determine the requirements for follow-up questioning. The initial questions are directed toward obtaining the basic information on the topic. In other words, they are the "who, what, where, when, how, and why" of each topic.

Follow-up Questions

9-7. Follow-up questions are used to expand on and complete the information obtained from the initial questions. Often even if the initial question is a well-constructed direct question, it will elicit only a partial answer. For example, when asked, "Who is going to attack?" The source might say, "My unit." Follow-up questions are used to determine precisely what the source means by "my unit" and what other units may also attack. The answer to follow-up questions may lead to more follow-ups until the source's knowledge on a given topic is exhausted. At a minimum, upon receiving a positive answer to an initial question, the HUMINT collector needs to ask "Who (what, where, when, why, how) else?" For example, if the HUMINT collector asks the source, "Who, in the local government is collaborating with the insurgents?" and is told a name in response, he will ask follow-up questions to determine all the required information about this individual and then will ask, "Who else, in the local government is collaborating with the insurgents?" This will continue until the source's knowledge in this area is exhausted.

Nonpertinent Questions

9-8. Nonpertinent questions are questions that do not pertain to the collection objectives. They are used to conceal the collection objectives or to strengthen rapport with the source. They are essential when the collector is using the elicitation technique. Nonpertinent questions may be used to gain time for the HUMINT collector to formulate pertinent questions and may also be used to break the source's concentration, particularly, if the HUMINT collector suspects the source is lying. It is hard for a source to be a convincing liar if his concentration is frequently interrupted.

Repeat Questions

9-9. Repeat questions ask the source for the same information obtained in response to earlier questions. They are a method to confirm accuracy of important details such as place names, dates, and component parts of technical equipment and to test truthfulness. Repeat questions should not be exact repetitions of an earlier question. The HUMINT collector must rephrase or otherwise disguise the previous question. The repeat question also needs to be separated in time from the original question so that the source cannot easily remember what he said. Repeat questions may also be used to develop a topic the source had refused to talk about earlier.

Control Questions

9-10. Control questions are developed from recently confirmed information from other sources that is not likely to have changed. They are used to check the truthfulness of the source's responses and should be mixed in with other questions throughout the questioning. If a source fails to answer a control question as expected, it may be an indicator that he is lying. However, there are other possible explanations. The source—

- Could have misunderstood the question.
- Could be making up information in order to please the questioner and/or receive a promised incentive.
- Could have answered the question truthfully to the best of his ability, but his information could be wrong or outdated.
- May be correct and the information that the control question was based on is no longer true.

9-11. It is the responsibility of the HUMINT collector to determine, through follow-up questions, which of the possibilities is the case. The HUMINT collector should also consult with the HAT for assistance in verifying the source reporting through all-source analysis.

Prepared Questions

9-12. Prepared questions are questions developed by the HUMINT collector, normally in writing, prior to the questioning. Prepared questions are used primarily when dealing with information of a technical nature or specific topic, which requires the HUMINT collector to formulate precise and detailed questions beforehand. The HUMINT collector may have to research analytical or technical material or contact SMEs to assist him in preparing questions. HUMINT collectors must not allow the use of prepared questions or any limitations to their education or training to restrict the scope and flexibility of their questioning. In many instances, the HUMINT collector should have an analyst or technical expert “sit in” on the questioning as well.

9-13. The HUMINT collector must be able to use the different types of questions effectively. Active listening and maximum eye-to-eye contact with the source will provide excellent indicators for when to use follow-up, repeat, control, and nonpertinent questions. The HUMINT collector must use direct and follow-up questions to fully exploit subjects pertinent to his interrogation objectives. He should periodically include control, repeat, and nonpertinent

questions in order to check the truthfulness and consistency of the source's responses and to strengthen rapport.

TYPES OF QUESTIONS TO AVOID

9-14. When using the questioning methodologies of interrogation, HUMINT collectors should avoid using negative, compound, or vague questions. Leading questions are usually to be avoided, but some special questioning techniques, such as use of a polygraph, require the use of leading questions.

Leading Questions

9-15. Leading questions are questions that are constructed so as to require a yes or no answer rather than a narrative response. They generally begin with a form of the verb "to be" (such as "is," "was," "were," "will," "are"). For example, "Is the mayor working with the insurgents?" Leading questions should generally be avoided for the following reasons:

- They make it easier for the source to lie since the source only provides minimal information.
- It takes longer to acquire information.
- A source, particularly one that is frightened or trying to get an incentive, will tend to answer in the way that he thinks the HUMINT collector wants him to answer.

9-16. Although normally avoided during questioning, an experienced HUMINT collector may use leading questions when the technical nature of the subject matter or the specific information needed leaves no alternatives. Leading questions can be used to—

- Verify specific facts.
- Pinpoint map locations.
- Confirm information obtained during map tracking.
- Transition from one topic area to another.

Negative Questions

9-17. Negative questions are questions that contain a negative word in the question itself such as, "Didn't you go to the pick-up point?" If the source says "yes," the HUMINT collector is faced with the question of whether he means "yes, I went to the pick-up point" or "yes, I didn't go to the pick-up point." When the source answers, the HUMINT collector cannot be sure what the answer means; therefore, he must ask additional questions. This can be particularly confusing when working with an interpreter. Other cultures may interpret a negative question in a way other than what the HUMINT collector meant. Negative questions should never be used during questioning unless they are being used deliberately during the approach to make the source appear to contradict himself. In other instances, the insertion of negative words within the question makes them impossibly open-ended. For example, "Who didn't attend the meeting?"

Compound Questions

9-18. Compound questions consist of two questions asked at the same time; for example, "Before you were captured today, were you traveling north or south?" Or “Where were you going after work and who were you to meet there?” They are easily misunderstood and may confuse the source or force him to give an ambiguous answer. Compound questions allow the source to evade a part of the question or to give an incomplete answer.

Vague Questions

9-19. Vague questions do not have enough information for the source to understand exactly what the HUMINT collector is asking. They may be incomplete, general, or otherwise nonspecific and create doubt in the source's mind. Vague questions confuse the source, waste time, and are easily evaded. They result in answers that may confuse or mislead the HUMINT collector and require further follow-up questions.

ELICITATION

9-20. Elicitation is the gaining of information through direct interaction with a human source where the source is not aware of the specific purpose for the conversation. Elicitation is a sophisticated technique used when conventional questioning techniques cannot be used effectively. Of all the collection methods, this one is the least obvious. However, it is important to note that elicitation is a planned, systematic process that requires careful preparation. Elicitation is always applied with a specific objective in mind and normally directed toward a specific source.

LEADS

9-20. A lead is a statement made by a source spontaneously or in response to questioning that leads the questioner to believe that the source has information on a topic other than the one currently under discussion. Documents captured with or on the source may also be exploited as sources of leads. Leads are referred to as either “hot” or “cold.”

HOT LEADS

9-21. A hot lead is a statement made by a source either spontaneously or in response to questioning that indicates he has information that could answer intelligence requirements on a topic other than the one currently under discussion. The lead could also be on a topic that although not listed as a requirement is, based on the HUMINT collector’s experience, of critical importance. Information on WMD and information on US personnel being held by threat forces are normally considered hot leads even if not listed as requirements. The HUMINT collector will normally question the source immediately on a hot lead, unless he is already asking questions on another topic. In this case, he completes questioning and reports the information on the priority topic, as appropriate, and then immediately questions on the hot lead. As soon as the HUMINT collector is sure he has obtained and recorded all the details known to the source, he reports the hot lead information by the

most expedient means available, normally in SALUTE report format. The HUMINT collector then resumes his questioning of the source at the point where the hot lead was obtained.

COLD LEADS

9-22. A cold lead is a statement made by a source either spontaneously or in response to questioning that indicates he has information on a topic of interest other than the one currently under discussion but that would not answer PIRs. The HUMINT collector makes note of the cold lead and exploits it after the planned questioning objectives have been satisfied or at the appropriate time during the questioning sequence.

DETECTING DECEIT

9-23. HUMINT information often has the capability to be more accurate and reliable than other disciplines. SIGINT information, for example, is not always able to return to the original source of the information to determine the reliability of the information, and interpretation of IMINT information may be uncertain. However, while HUMINT can be reviewed for reliability, determining the reliability of human sources is a continuous process accomplished by carefully assessing not only the sources of information but also assessing the information itself.

9-24. Detection of deception is not a simple process, and it normally takes years of experience before a HUMINT collector can readily identify deliberate deceit. Inconsistencies in the source's actions or words do not necessarily indicate a lie, just as consistency is not necessarily a guarantee of the truth. However, a pattern of inconsistencies or unexplainable inconsistencies normally indicate deceit.

TECHNIQUES FOR IDENTIFYING DECEIT

9-25. Techniques for identifying deceit include but are not limited to the following:

- Repeat and control questions (see paras 9-9 and 9-10).
- Internal inconsistencies. Frequently when a source is lying, the HUMINT collector will be able to identify inconsistencies in the timeline, the circumstances surrounding key events, or other areas within the questioning. For example, the source may spend a long time explaining something that took a short time to happen, or a short time telling of an event that took a relatively long time to happen. These internal inconsistencies often indicate deception.
- Body language does not match verbal message. An extreme example of this would be the source relating a harrowing experience while sitting back in a relaxed position. The HUMINT collector must be careful in using this clue since body language is culturally dependent. Failing to make eye contact in the US is considered a sign of deceit while in some Asian countries it is considered polite.
- Knowledge does not match duty position or access. Based on the source's job, duty position, or access the HUMINT collector should have

developed a basic idea of the type and degree of information that an individual source should know. When the source's answers show that he does not have the expected level of information (too much or too little or different information than expected), this may be an indicator of deceit. The HUMINT collector needs to determine the source of unexpected information.

- Information is self-serving. Reporting of information that is self-serving to an individual or his group should be suspect. For example, a member of one ethnic group reporting generic atrocities by an opposing ethnic group or a source reporting exactly the right information needed to receive a promised incentive should be suspect. That is not to say that the information is necessarily false, just that the HUMINT collector needs to be sure to verify the information.
- Lack of extraneous detail. Often false information will lack the detail of truthful information, especially when the lie is spontaneous. The HUMINT collector needs to ask follow-up questions to obtain the detail. When the source is unable to provide the details that they should know, it is an indicator of deceit. If the source does provide this additional information, it needs to be checked for internal inconsistencies and verified by repeat questions.
- Repeated answers with exact wording and details. Often if a source plans on lying about a topic, he will memorize what he is going to say. If the source always relates an incident using exactly the same wording or answers repeat questions identically (word for word) to the original question, it may be an indicator of deceit. In an extreme case, if the source is interrupted in the middle of a statement on a given topic, he will have to start at the beginning in order to "get his story straight."
- Source appearance does not match story. If the source's physical appearance does not match his story, it may be an indication of deceit. Examples of this include the source who says he is a farmer but lacks calluses on his hands or the supposed private who has a tailored uniform.
- Source's language usage does not match story**.** If the type of language, including sentence structure and vocabulary, does not match the source's story, this may be an indicator of deceit. Examples of this include a farmer using university level language or a civilian using military slang.
- Lack of technical vocabulary. Every occupation has its own jargon and technical vocabulary. If the source does not use the proper technical vocabulary to match his story, this may be an indictor of deceit. The HUMINT collector may require the support of an analyst or technical expert to identify this type of deceit.
- Physical cues. The source may display physical signs of nervousness such as sweating or nervous movement. These signs may be indicators of deceit. The fact that an individual is being questioned may in itself be cause for some individuals to display nervousness. The HUMINT collector must be able to distinguish between this type of activity and nervous activity related to a particular topic. Physical reaction to a

particular topic may simply indicate a strong emotional response rather than lying, but it should key the HUMINT collector to look for other indicators of deceit.

- Failure to answer the question asked. When a source wishes to evade a topic, he will often provide an answer that is evasive and not in response to the question asked. For example, if the source is asked, "Are you a member of the insurgent organization?" and he replies, "I support the opposition party in the legislature," he has truthfully answered a question, but not the question that was asked. This is a subtle form of deceit since the source is seemingly cooperative but is in fact evading providing complete answers.

ACTIONS UPON IDENTIFYING INDICATORS OF DECEIT

9-26. The exact actions by the HUMINT collector when identifying possible deceit are dependent on the type of collection, the circumstances of the collection, the specific sign of deceit observed, the type of approach used, and cultural factors. The HUMINT collector may—

- Question the topic in more detail looking for additional indicators.
- Reinforce the approach.
- Move to another topic and revisit the original topic later with repeat questions. Ask control questions (confirmed by known data) and questions to which the source should know the answer to see if he answers honestly.
- Point out the inconsistency to the source and ask for an explanation.
- Seek assistance from a more experienced HUMINT collector, analyst, or a technical expert on the culture or the topic being questioned.
- Conduct continuous assessments of source (see FM 34-5 (S//NF)).
- Research established databases.
- Ask yourself if the information makes sense; if not, conduct more research.
- Consider how the information was obtained.
- Compare the information provided to the source's placement and access.
- Compare answers with other sources with similar placement and access. Be aware that this method is merely a rough tool to check veracity and should not be used by the collector to confirm intelligence.
- Use the polygraph.
- Consider that a source motivated primarily by money will likely be tempted to fabricate information in order to get paid.
- Be aware that a source may read the local newspaper to report information that is already known or may also be providing information to another agency.

9-27. The one thing that the HUMINT collector cannot do is to ignore signs of deceit.

HUMINT COLLECTION AIDS

9-28. There are numerous procedural and recording aids that can assist the HUMINT collector in conducting rapid, accurate, yet systematic questioning. They include—

- HUMINT Collector's Guide. This guide is a pamphlet or notebook designed to guide the HUMINT collector through the questioning. The HUMINT team leader should ensure that team members prepare a HUMINT collector's guide, which could be included in the unit's SOP. The guide is made based on the AO and supported command intelligence requirements. The HUMINT collector and available intelligence analysts should jointly prepare the guide. Appendix G provides the basic topics and example questions that can be adapted to construct a HUMINT collector's guide. The guide must be updated for each interrogation as part of planning and preparation. The guide should contain information such as—
  - Intelligence requirements and ISR tasks.
  - Topical questioning sequence format.
  - Actual prepared questions to be used during questioning.
  - Guidelines for employing the various approach techniques.
  - Formats or samples of completed reports used by HUMINT collectors.
- Time Event Chart. A timeline, or event chart, is a graphic display upon which the HUMINT collector enters chronological information as it is collected. This facilitates the HUMINT collector in understanding and organizing the collected information. It also enables the HUMINT collector to identify gaps in information, to sequence events properly to facilitate follow-up questions, and to identify deception. The HUMINT collector can develop a basic timeline prior to questioning. The source should not be able to observe the timeline since doing so will help a deceptive source "keep his story straight." See Chapter 12 for how to create and use a time event chart.
- Organizational Chart. An organizational chart is a graphic representation of an organization. It is the equivalent of a military line-and-block chart. This is used to facilitate the questioning of organizations and in establishing their hierarchical and lateral linkages. A basic chart can be developed prior to the questioning based on the expected organizational questioning.

RECORDING TECHNIQUES

9-29. Accuracy and completeness are vital principles to reporting. However, it is usually not possible to completely record all information in a questioning session. Recording techniques may involve memory, handwritten or typed notes, tape recordings, and video recordings. Each has its advantage and corresponding disadvantage.

- Memory: Relying on one's memory has certain advantages. It does not require any equipment or extra time, and is the least intrusive method of recording information. It allows maximum interaction with the source and projects sincerity. An individual can train himself to

remember highly detailed information. Often in elicitation, memory is the only viable recording method. However, in general, using the memory exclusively to record information is the most inaccurate methodology. Particularly in a long questioning session, details are forgotten and information tends to be generalized.

- Handwritten notes: Handwritten notes require minimal equipment (a pad and pencil), are not intimidating to most sources, and can be as detailed as the HUMINT collector desires. If an analyst or second interrogator is present, he should also take notes. This second set of notes can aid in report writing. The interrogator should not rely solely on an analyst's notes unless absolutely necessary. However, writing notes while questioning an individual often interferes with the rapport between the collector and the source. The collector loses eye contact and can easily miss subtle body language that might indicate lying. Detailed note taking can be extremely time consuming and many sources will, over time, begin to limit their responses so they do not have to repeat information or wait for the collector to write it down. It is somewhat intrusive and inhibiting to the source and is totally inappropriate in certain situations such as liaison and most casual source contacts. Handwritten notes can also be inaccurate, have limited details, and can be hard to read after the fact.
- Computer notes: With the proliferation of computer equipment, particularly laptops and handheld devices, note taking on computers is increasingly commonplace. A computer can provide access to data-based information that may support questioning such as foreign language dictionaries or technical support manuals, either through the Internet (if connected) or on its harddrive. If the computer is linked to a communications system, it also allows the HUMINT collector to transmit data, including SALUTE reports, during the course of the questioning. Notes taken on a computer, however, have many of the same disadvantages as handwritten notes. In addition, computer notetaking requires more equipment and technological support and access to either electricity or a plentiful supply of batteries. Computers may be intimidating to some sources and the fact that what the source says is being entered into a computer may cause the source to alter the information he is providing. Computers tend to isolate the collector from the source by dividing the collector's attention between the computer and the source, and again may cause the collector to miss critical body language clues. Finally, the computer is even more inappropriate to casual and controlled source operations than are handwritten notes.
- Audiotapes: If recording equipment is discrete and functioning properly, audiotapes can be extremely accurate. Use of tapes also allows the HUMINT collector to place his entire attention on the source. This not only enhances rapport but also allows the HUMINT collector to observe the source's body language. Taping a questioning session, if done overtly though, tends to be extremely inhibiting to the source and may seriously curtail the information obtained. Surreptitious taping can be illegal in some situations and dangerous in some situations as well. Consult your legal advisor to determine if

taping is legal. Taped information can also be seriously affected by ambient noise and the relative positioning of the source and collector to the microphone. Writing a report based on a taped session can be extremely time consuming, since it takes as long to listen to a tape as it took to record it. This drawback can be reduced somewhat through the use of voice activated recording devices. Exclusive dependence on audiotapes tends to make the collector less attentive and more likely to miss follow-up questions. Also, if the tape is lost or damaged or does not function properly, the collector has no backup.

- Video recording: Video recording is possibly the most accurate method of recording a questioning session since it records not only the voices but also can be examined for details of body language and source and collector interaction. It is also the most resource intensive requiring proper lighting, cameras, viewing equipment, and possibly trained operators. If done overtly, video recording can be by far the most inhibiting to the source. Even if the source is willing to be videotaped, there is a tendency for both the source and the collector to "play to the camera," creating an artificiality to the questioning. Consult your legal advisor to determine the legality of overt or covert videotaping.

QUESTIONING WITH AN ANALYST OR A TECHNICAL EXPERT

9-30. The HUMINT collector may often find himself in the position where he needs to use an analyst or a technical expert, or both, in order to conduct questioning. Many of the techniques involved in using an analyst or technical expert are the same as those with using an interpreter (see Chapter 11). The HUMINT collector must pre-brief these supporting personnel. The degree to which the analyst or technical expert is involved in the actual questioning is dependent on the established relationship between the analyst or technical expert and the HUMINT collector. The HUMINT collector will always remain in charge of the questioning, be present throughout the questioning, and ensure that the questioning follows his questioning plan. He must ensure that the supporting analyst or technical expert has the proper security clearance.

9-31. An analyst or technical expert can participate in the questioning to various degrees listed below from least intrusive to most intrusive. As the degree of participation by the analyst or technical expert increases, the technical fidelity of the information collected usually increases but the rapport between the HUMINT collector and the source decreases as does the HUMINT collector's ability to control the content and judge the truthfulness of the information. The analyst or technical expert may provide—

- Advice Only: The HUMINT collector does the questioning. The expert provides information prior to the meeting and may review the collected information after the meeting. The technical expert is not present at the actual questioning.
- Remote Support: The HUMINT collector does the questioning. In addition to the above, the expert monitors the questioning and provides input to the HUMINT collector after the questioning as required. Based on the technological support, this can involve the expert sitting in on, but not participating in the questioning (which

may make the source uncomfortable), or the expert viewing and listening to the questioning through a remote video and sound hook-up.

- Local Support: The HUMINT collector does the questioning. The expert sits in on the questioning and provides input to the HUMINT collector during the course of the questioning. This can break both the source's and the HUMINT collector's trains of thought and confuse the lines of control in the questioning.
- Expert Participation: The HUMINT collector initiates the questioning, but the expert participates throughout the questioning, asking for clarification and additional information as required. Unless properly trained, the expert can seriously taint the quality of the information through the use of poor questioning techniques. The HUMINT collector can lose rapport and control.
- Trained Expert Questioning: In rare instances, with particularly difficult technical topics or those areas of questioning that require a high degree of technical expertise, it may be easier to train the expert in basic questioning techniques than it is to train the HUMINT collector on the technical topic. In this instance, the HUMINT collector sits in on the questioning to ensure proper procedures and techniques are used and to advise the technical expert. The technical expert does most of the questioning.

9-32. In any case, if the source is to receive compensation for his time, it must come from the HUMINT collector, not the analyst or technical expert. This continues to reinforce that the HUMINT collector is in charge, and does not transfer the source's trust to the expert.

THIRD-PARTY OFFICIAL AND HEARSAY INFORMATION

9-33. The source may have information that he did not observe firsthand. While this information is not as reliable as firsthand knowledge, it is often significant enough to report. The HUMINT collector must be careful to identify this information as to its origin, type, and the time and manner that the information was obtained by the source. This information will be entered into the report as a source comment or a collector comment. This will include—

- The origin of the information. This may be the name, rank, and duty position or job of an individual or may be an official or unofficial document such as an OPORD, official memorandum, or party newspaper.
- The complete organization to which the person who provided the information belongs or the identity of the organization that produced the official or unofficial document from which the source obtained the information.
- Date-time group (DTG) when the source obtained the information.
- The circumstances under which the source obtained the information.

9-34. Comparing the details of the hearsay information, such as DTG, where the information was obtained and the circumstances under which the source

claimed to have received it, to the source's known activities, may provide indications of truthfulness or deception on the part of the source.

CONDUCTING MAP TRACKING

9-35. Map tracking is a specific questioning skill that the HUMINT collector uses in all operations. It is a vital skill in supporting targeting and operational planning. Map tracking identifies and verifies key information by tracking the source's movement and activities within a specific area over a fixed period using a map or similar graphic aid. The area and the time involved are dependent on the collection requirements and the source's knowledge level. Map tracking can occur at any point in the questioning process. Normally, the HUMINT collector begins map tracking as soon as his questioning identifies a priority disposition or activity that the source's information can locate on the map.

9-36. Map-tracking techniques, if properly applied, can extract information from friendly, neutral, or threat sources and can be used with individuals ranging from those with detailed map skills to illiterates, and those who have never seen a map. Through map tracking, the HUMINT collector pinpoints locations of any threat activity, threat dispositions, or any other priority terrain-related information, such as trafficability, known to the source.

9-37. The HUMINT collector will determine these locations with the degree of fidelity needed to support operational requirements. The degree of detail needed may range from an 8-digit grid coordinate for unit locations to locations of specific buildings, rooms, or even items within a room. The HUMINT collector uses a variety of map-tracking aids including standard military maps, aerial photographs, commercial imagery, building blueprints and diagrams, and commercial road maps. Some advantages to map-tracking techniques include—

- The source is led through his memory in a logical manner.
- Discrepancies in the source's statements are easier to detect.
- Locations are identified to support targeting and battlefield visualization.
- Map tracking is a four-step process:
  - Step 1: Determine the source's map-reading skills.
  - Step 2: Establish and exploit common points of reference (CPRs).
  - Step 3: Establish routes of travel.
  - Step 4: Identify and exploit key dispositions.

DETERMINE THE SOURCE'S MAP-READING SKILLS

9-38. The first step in the map-tracking process is to determine the specific map-reading skills of the source. This step only occurs the first time that the HUMINT collector map tracks a particular source. This information will determine what methodology will be used for the rest of the process. In this step the HUMINT collector is determining existing skills; he should not attempt to teach the source additional map skills at this time. The HUMINT collector can use prior knowledge, such as the fact that the source is illiterate or cannot read a map, to skip some of the specific parts of the process. Below

is a detailed description of the process to establish the map-reading skills of the source.

- The HUMINT collector asks the source if he can read the map being used. If the source answers in the affirmative, the HUMINT collector asks some key questions to verify this.
- If the source cannot read the map being used, the HUMINT collector determines if the source can read another type of available map or graphic representation. For example, a source may not be able to read a military map but might be able to use a commercial map or an imagery product.
- The HUMINT collector then establishes the method that will be used to describe movement (direction and distance) on the map. If the source knows how to use compass directions, that may be the most expedient method for determining direction. Again, the HUMINT collector must verify that the source knows how to use compass directions. This can be done best by having the source tell the compass directions between known points. Distance is normally determined by using the standard units of measurement with which the source is familiar, such as kilometers or miles. This can cause some problems, for example, if the map is measured in kilometers and the source normally expresses distance in miles. The HUMINT collector must make the adjustment rather than trying to teach the source the unfamiliar system.
- Compass directions and standard units of measure are not the only method or necessarily even the best method of indicating direction and distance in all circumstances. When using an urban map, direction and distance can often be described by indicating blocks traveled and turns made (right or left) at intersections. Direction of travel can be indicated in reference to key features such as going toward the downtown area or moving toward the river. When describing the interior of a building, references may be to upstairs, downstairs, floor number, or other descriptive terms. When map tracking in rural areas, especially when questioning someone who does not know how to use compass directions, terrain association is normally the best method of establishing direction of travel and distance. Questions such as "Were you traveling uphill at that time?" "What prominent terrain features could you see from that location?" "What was the nearest town?" or "Was the sun behind you?" help to identify locations on the map. The HUMINT collector should allow the source to use his own frames of reference. However, the HUMINT collector must ensure he understands the source.

ESTABLISH AND EXPLOIT COMMON POINTS OF REFERENCE

9-39. The second step of map tracking is to establish CPRs. It is important in accurate map tracking to talk the source through his past activities in the sequence in which they occurred and his movements in the direction in which they were traveled. Attempting to track a source backward in time and space is time consuming, inaccurate, and is often confusing to both the source and the HUMINT collector. Future activities should be tracked in the direction in

which they are planned to occur. The HUMINT collector will normally establish various CPRs throughout the questioning of the source.

9-40. For certain sources such as friendly forces, tasked sources, or other instances where the starting and ending points of the mission being questioned are easily established, the first point of reference is normally where that source began the mission. For other sources such as detainees, line crossers, informers, and refugees, it is often more difficult to establish a "starting point." In these instances the HUMINT collector uses a sequential approach to the map tracking. He establishes a point of reference that is a logical end point for the subject being discussed. This may be, for example, the point of capture for a detainee, the point where a line crosser entered the friendly force area, or where a refugee left the area of intelligence interest. Second and subsequent points of reference are established during questioning when the source mentions a disposition, activity, or location of interest that can be located on the map. The HUMINT collector locates the reference point on the map through direct questioning and terrain association. He uses leading questions as necessary to establish an exact location. He then establishes the route of travel.

ESTABLISH ROUTES OF TRAVEL

9-41. Once the CPR is established, the HUMINT collector questions the source until he has extracted all pertinent information on the CPR and its immediate surroundings. For past missions and activities, the HUMINT collector then establishes the route the source traveled between the newly established CPR and a previously established CPR and exploits the route. For future missions or activities, the route is established from the previously established CPR toward the future mission CPR.

9-42. The HUMINT collector should establish the route traveled by determining the source's direction and physical description of the route of travel. The description should include details such as surface on which the source traveled and prominent terrain features along the route of travel and the distance the source traveled or, in the case of future locations, would travel. The HUMINT collector should also identify any pertinent dispositions or any activities of military significance, belonging to the opposition forces, along or in the vicinity of the route of travel. For longer routes, the HUMINT collector may divide the route into segments for ease of questioning.

IDENTIFY AND EXPLOIT KEY DISPOSITIONS

9-43. The HUMINT collector must obtain the exact location and description of every pertinent disposition known to the source. This includes the locations established as CPRs and any other pertinent disposition established during map tracking. At a minimum, the collector should—

- Establish a physical description of the disposition. The degree of fidelity will depend on the collection requirements. This may be as detailed as the physical layout of a room to the general description of a training area. This will include security measures and modus operandi at the location as appropriate.

- Identify and describe the significance of the disposition in terms of ongoing and future threat operations.
- Identify and describe key activities, equipment, or organizations at the location, as well as people and leaders.
- Identify and describe all pertinent collocated activities, locations, or organizations, as well as people and leaders.
- Identify the basis (hearsay or personal experience) and DTG of the source's knowledge of each disposition.

SPECIAL SOURCE CATEGORIES

9-44. Questioning of every source is unique and requires specific preparation. Special consideration and preparation must be made for some specific categories of sources. Some examples of special source categories include but are not limited to wounded or injured sources or illiterates.

WOUNDED OR INJURED SOURCES

9-45. HUMINT collectors may question (interrogate, debrief, or elicit information from) a wounded or injured source provided that they obtain certification from a competent medical authority that the questioning will not delay or hinder medical treatment or cause a worsening of the condition of the source. The HUMINT collector can question the source before, after, or during medical treatment. The HUMINT collector cannot at any time represent himself as being a doctor or any other type of medical personnel or member of the ICRC. Nor can he state, imply, or otherwise give the impression that any type of medical treatment is conditional on the source's cooperation in answering questions.

ILLITERATES

9-46. HUMINT collectors should never make the mistake of equating illiteracy with a lack of intelligence or an inability to provide meaningful information. In fact, many illiterates have developed extremely good memories to compensate for their inability to rely on the written word. An illiterate's frame of reference does not include street signs, mile markers, and calendars. It also will probably not include conventional time and distance measurements. The HUMINT collector must compensate for these differences. Map tracking, for example, must normally be accomplished by terrain association. If the source cannot tell time, time of day can be determined by the position of the sun.

Chapter 10

Reporting

10-1. Reporting is the final and in many cases the most vital phase in HUMINT collection. If the collected information is not reported accurately, in a timely manner, in the proper format, and to the correct recipient, it cannot become part of the all-source intelligence product or tip in time to affect operational decisions. Information that would support targeting must be reported by the fastest means possible.

REPORTING PRINCIPLES

10-2. The HUMINT collector must be able, in a written report, to convey to the user the information obtained from a source. Therefore, the following principles of good report writing are to be followed:

- Accuracy. Accurately reflect the information obtained from the source. Reporter comments and conclusions must be clearly identified as such.
- Brevity. Report all relevant information; however, the report should be brief, to the point, and avoid unnecessary words.
- Clarity. Use simple sentences and understandable language. Proper grammar and punctuation are a must. Another team member, if possible, should read the reports to ensure clarity.
- Coherence. Present the information in a logical pattern based on standard reporting formats.
- Completeness. Report all information collected. The collector should not filter information since all information is of interest to an analyst. Report negative responses to pertinent topics to prevent a misunderstanding or duplication of effort in subsequent questioning based on SDRs.
- Timeliness. Report information as soon as operationally feasible. Most collection requirements contain a LTIOV as part of the requirement. While written reports are preferable, critical or time-sensitive information is passed by the most expedient means available.
- Releasability. Include only releasable information in reports that are to be shared with multinational units. When possible, reports to be shared with multinational units should be kept to the appropriate classification to ensure the widest dissemination of the reported information.

REPORT TYPES

10-3. There are two major categories for reporting information: operational reports and source administrative reports. Figure 10-1 shows the HUMINT

reporting channels. Refer to DIAM 58-11 (S//NF) and DIAM 58-12 (S//NF) for specific guidance in using these reports.

OPERATIONAL REPORTS

10-4. Operational reports is a broad category that encompasses all reports that do not contain information collected in response to intelligence requirements or the reporting of the technical, and usually sensitive, aspects of HUMINT collection. It includes but is not limited to all administrative and logistical reports. Unit SOPs and directives from higher headquarters establish operational reporting requirements, formats, and procedures. Operational reporting—

- Tells the commander where and when assets are conducting missions.
- Describes unit mission capability.
- Responds to administrative and logistical requirements.
- Describes support requirements.
- Includes but is not limited to unit status reports, mission planning reports, mission status reports, and equipment status.
- Reports ICF usage at any echelon where the use of ICFs is authorized.

SOURCE ADMINISTRATIVE REPORTS

10-5. Source administrative reports include intelligence reports that are used to pass or request information in order to answer intelligence requirements, and reports that address the HUMINT collector's contacts with the source. Intelligence reports include but are not limited to IIRs and SALUTE reports.

Intelligence Information Reports

10-6. The IIR is used to report all HUMINT information in response to collection requirements. It is used to expand on information previously reported by a SALUTE report or to report information that is either too extensive or not critical enough for SALUTE reporting. IIRs are written at any echelon and "released" by the appropriate authority before they enter the general Intelligence Community. Normally the G2X will be the release authority for IIRs.

10-7. At the tactical level, the HUMINT collectors will fill out the complete IIR; however, the requirements section may link the information collected against a unit requirement rather than against national requirements. In any case, the report will be forwarded to the OMT.

10-8. The team leader will review the IIR, place a copy of the IIR in the detainee's or source's local file and forward the IIR to the OMT. (When a detainee is transferred to another facility or evacuated to a higher echelon, a copy of each IIR written from interrogations of that detainee is forwarded with him.) The OMT reviews the report, requests additional information as necessary from the originator, adds additional administrative detail, and forwards the report to the HOC of the supporting C/J/G/S2X. The HOC and the 2X review the report, request additional information as required, add any

final required information including linking it to national requirements, and then the 2X releases the report.

10-9. In addition to the above, the text information from the IIR can be forwarded to the unit's analytical elements and when it contains critical time-sensitive information, such as an impending attack, it is sent to units which may be affected by the information; however, it must be clearly marked "unevaluated information, not finally evaluated intelligence." The use of IIRs and the formats are covered in DIAM 58-12 (S//NF).

SALUTE Reports

10-10. The SALUTE report is a standard Army format used to report information of immediate interest by individuals at any echelon. (See Appendix H for a SALUTE report format.) The SALUTE report is the primary means used to report combat information to units that could be affected by that information. After review by the team leader, SALUTE reports are sent simultaneously to the supported unit S2, to the OMT in control of the HCT, and to the intelligence staff officer of any other tactical unit that may be affected by the information contained in the SALUTE report.

10-11. The OMT reviews the report and forwards it to the supporting HAT and supporting J/G/S2X for inclusion in the analysis picture. The supported S2 will—

- Review the information.
- Incorporate it into his unit intelligence products, as applicable.
- Forward the information to his higher echelon intelligence staff officer.
- Ensure that all affected units are notified.

10-12. Units must develop SOPs for the passing of information and intelligence to multinational units. Report writers and editors must ensure that reports that are to be shared with multinational units contain only releasable information. This will enable reports to have the widest dissemination. Arrangements are made through the C/J2X/LNO for distribution. When possible, reports to be shared with multinational units should be kept to the appropriate classification to ensure the widest dissemination of the reported information.

Basic Source Data Reports

10-13. The basic source data (BSD) reports provide the HUMINT chain with biographic and operational information related to a source. BSDs are used at all echelons to collect biographic information on all contacts. The use of BSDs and BSD formats are covered in DIAM 58-11 (S//NF).

Contact Reports

10-14. Collectors use contact reports to inform their technical chain (from OMT through J/G/S2X) of all relevant information concerning specific meetings with HUMINT sources. Information typically includes the circumstances of the contact (purpose, locations, time), the operational

matters relative to the contact (topics discussed, taskings given), reports produced as a result of the contact, and logistics expended.

Other Reports

10-15. HUMINT collectors also use a number of other reports to administer source contacts and to report information. Copies of the following reports should be maintained in the detainee's permanent file for future reference. HUMINT collectors will review these reports when planning additional collection activities; release committees or tribunals can use the reports to help evaluate if a detainee can be released or not. These reports include—

- Screening Reports. Screening reports are used to report BSDs, knowledge areas and levels, cooperation, vulnerabilities to approaches, and other relevant source information between HUMINT collectors. It is normally filled out either electronically or manually by the initial HUMINT collector to speak to a source. The screening report is normally forwarded electronically to higher echelon HUMINT collection organizations and other MI organizations that might have interest in the source. Higher echelon organizations may add information to the screening sheet extracted through subsequent screenings. Available digital screening reports contained in the HUMINT collector's mission support software (for example, BAT or CI/HUMINT Automated Management System [CHAMS]) should be used whenever possible to ensure rapid transfer of data. If screening reports have to be handwritten, the information collected should conform to theater requirements and local SOPs.
- Knowledgeability Briefs. The KB is used to inform the Intelligence Community of a source's full identity, past history, and areas of knowledge, as well as to set a suspense date for the submission of intelligence requirements. It is normally only used at the strategic and operational echelons. When completed, a KB will be classified at least Confidential in accordance with the DIA Classification Guide to protect the identity of the source. The use of KBs and the formats are covered in DIAM 58-11 (S//NF). See Figure 10-2 for an example of a short form KB that can be used for screening at all echelons, and can also be prepared and published like the full KB. This allows the entire intelligence community to see who is either in custody or to whom US intelligence has access so that SDRs can be issued to help focus the intelligence collection effort.
- Notice of Intelligence Potential (NIP). A NIP is used to inform the US Intelligence Community of the availability of a source of potential interest and to notify them of what agency has responsibility for questioning that source and where to forward questions and requests for information from that agency. The use of NIPs and the formats are covered in DIAM 58-11 (S//NF).
- Lead Development Report (LDR). The LDR is used to inform the HUMINT chain of ongoing operations directed toward a specific source. It notifies them as to what element spotted the potential source, the

current steps in assessing of the source, and the general information on the potential source.

- Interrogation Summary. An interrogation summary may be written to record relevant facts concerning the interrogation. The summary may include the attitude of the source; approach techniques that were tried and which ones were effective; incentives promised and whether or not they were delivered yet; recommended topics for further exploitation; and any other topics the HUMINT collector considers relevant. Local SOPs will dictate the use of the interrogation summary.
- Interrogation Plan. The interrogation plan is a report prepared by the HUMINT collector to organize his plan to approach and question a source. It lists collection objectives, approach techniques, preparation and liaison tasks, and interpreter usage plan. The interrogation plan also has approval blocks for interrogation supervisor approval of selected approaches and medical release for questioning. The last part of the form has termination, approach effectiveness, recommendations for further exploitation, and a summary of information obtained and reports expected to be published. Figure 10-3 is an example of an interrogation plan format.
- Termination Report. The termination report is used at all echelons to inform the technical chain of the termination of a contact relationship between a HUMINT collector and a source.
- Biographic Report. The biographic report is a formatted IIR used at all echelons to report information collected from one human source about another individual of actual or potential intelligence interest. The biographic report format is found in DIAM 58-11 (S//NF).

REPORTING ARCHITECTURE

10-16. There are three basic reporting channels (see Figure 10-1):

- The operational reporting chain consists of primarily the C2 elements for the HUMINT collection element. It includes the OMTs, unit commanders, and unit S3 and operation sections.
- The technical chain includes the OMTs, HOC, and the C/J/G/S2X, and in certain circumstances, the unit G2/S2s.
- The intelligence reporting chain includes the OMTs, HATS, C/J/G/S2Xs, and unit G2/S2s.

10-17. Many elements serve multiple and overlapping functions within the reporting architecture. Each element must be aware of its function within the architecture to ensure that information is disseminated expeditiously to the right place in the right format. This architecture should be established and published prior to implementation in order to avoid confusion.

OPERATIONAL REPORTING

10-18. Operational reporting is sent via the organic communications architecture (see Chapter 13). Operational reports are normally sent per unit SOP or based on direction from higher headquarters. HCTs normally send all

operational reports through their OMT to the command element of the unit to which they are assigned. If an HCT is attached, it will normally send its operational reports to the unit to which it is attached with courtesy copies to their assigned unit as required. If there is an administrative or logistics relationship established with the supported unit, HCTs that are in DS send the principal copy of all related administrative and logistic reports to the supported unit with a courtesy copy to their parent unit. If the HCT is operating in GS, a courtesy copy of operational reports should be forwarded to all affected unit commanders in the supported AO.

TECHNICAL REPORTING

10-19. Technical reporting includes the forwarding of source information and technical parameters of collection operations from lower to higher and the passing of tasking specifics, source information, technical control measures, and other information from higher to lower. Technical reporting is conducted through the technical chain that extends from the HCT through the OMT and Operations Section (if one exists) to the C/J/G/S2X.

INTELLIGENCE REPORTING

10-20. The key to intelligence reporting is to balance the need for accurate reporting with the need to inform affected units as quickly as possible. The J/G/S2 and MI commander are key to ensuring the right balance.

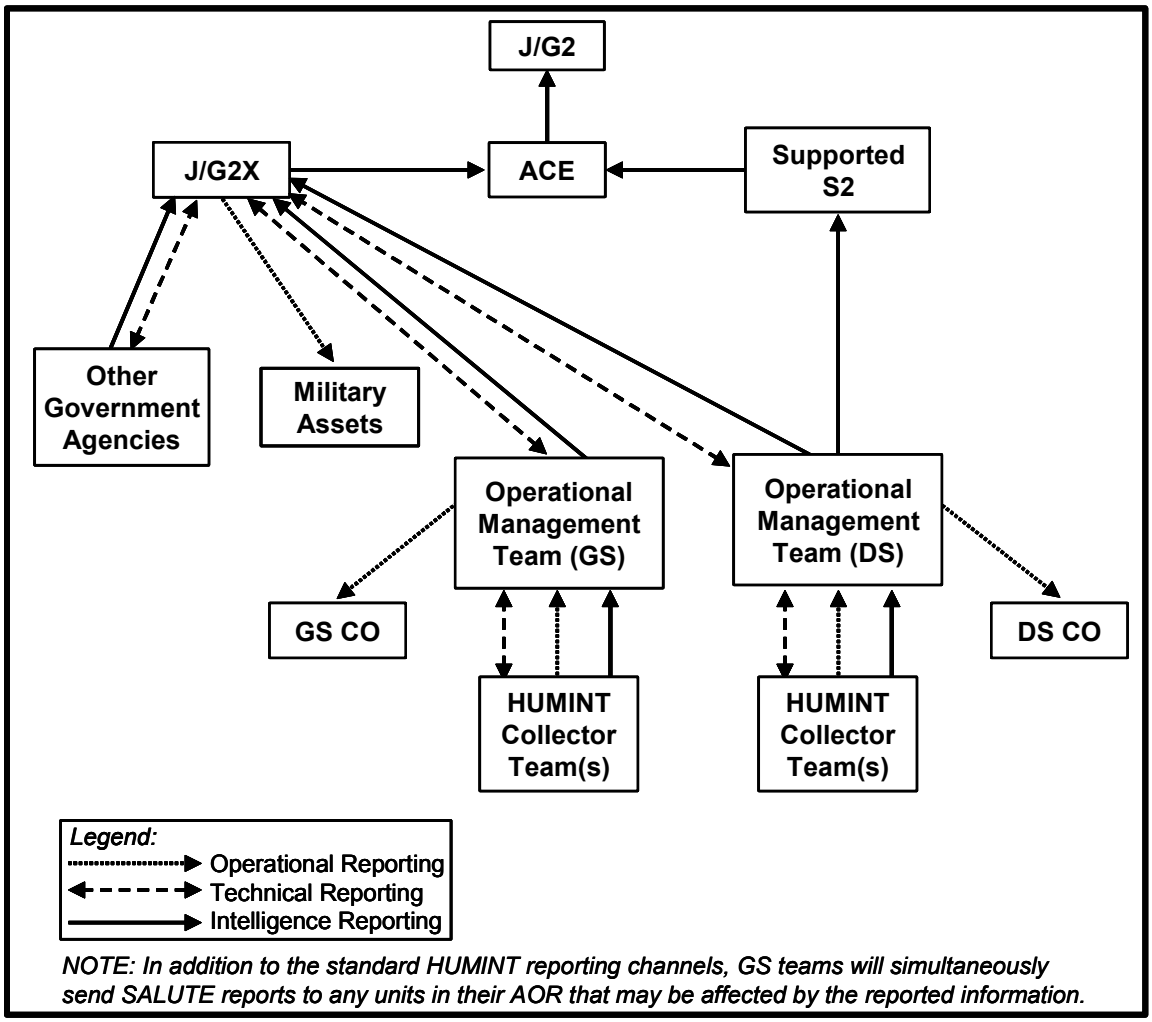


Figure 10-1. HUMINT Reporting Channels.

KB-EZ WORKSHEET

1. PERSONAL DATA:

1A. Name:

1B. Source Number (Capturing Unit):

1C. Source Number (MPs):

1D. Source Number (Other):

1E. Source Number (MI):

1F. Country of Citizenship:

1G. Birth City:

1H. Birth Country:

1I. Birth Date:

1K. Date Departed Country of Origin/Date of Capture:

1N. Last County of Residence:

1O. Language Competency:

2. Education: (Most Recent to Oldest)

2A. Military or Civilian:

2B. Dates of Attendance:

2C. Name of Institution:

2D. City Location of Institution:

2E. Country Location of Institution:

2F: Completion Status/Degree Type:

3. EMPLOYMENT: (Most Recent to Oldest)

3A. Dates of Employment:

3B. Name of Place of Employment:

3C. City Location of Place of Employment:

3D. Country of Place of Employment:

3E. Employment Duty Position:

3F. Security Clearance:

SAMPLE

Figure 10-2. KB-EZ Worksheet.

4. MILITARY SERVICE: (Most Recent to Oldest)

4A. Dates of Service:

4B. Name of Post/Base:

4C. Armed Service Component:

4D. Rank of Equivalent:

4E. Name of Unit/Group:

4F. City Location of Unit/Group:

4G. Country Location of Unit/Group:

4H. Military/Group Duty Position/Title:

4I. Security Clearance:

5. Comments: (Character, intelligence, motivation, personality, cooperativeness)

5A. CIRCUMSTANCES OF CAPTURE: Capture date, capturing unit, circumstances, documents, weapons, and equipment.

5B. ASSESSMENT: Physical condition, mental condition, intelligence, cooperation (1, 2, 3), knowledgeability (A, B, C), personality.

5C. ADDITIONAL PERSONAL INFORMATION: (Skills, experience, marital status, other).

6. NAME OF SCREENER:

SAMPLE

Theater-specific collection requirements may require modification of the KB-EZ format. Consider adding entries for:

- Race
- Ethnicity
- Tribal Affiliation
- Religion and Sect
- Language and Dialect Spoken

Entries for "Location" may need to include a village or even neighborhood.

Figure 10-2. KB-EZ Worksheet (continued).

INTERROGATION PLAN

PLANNING: **DTG:**_____

Collector Name:_____ **FRN:**_____

Detainee Name:_____

Detainee MP Number:_____ **Other Identifying Numbers (specify):** _____

Number of Times Interrogated:_____

Interrogation Objectives:_____
(Include PIR, SDR, RFI, IPSP, etc.)

Fit to undergo interrogation: YES_____ **NO** _____

Health concerns to be reported to the commander:_____

_____

Approach Strategies (Attach separate sheet if needed for additional approaches):

Initial Approach: _____

Rationale: _____

Additional Approach: _____

Rationale: _____

Additional Approach: _____

Rationale: _____

REVIEW: Interrogation Supervisor_____ **MI Unit Commander**_____
SJA_____ **BSC (as appropriate)** _____

APPROVAL AUTHORITY:	**PRINTED NAME**	**DTG OF APPROVAL**	**SIGNATURE**
First O-6 (as required):	_____	_____	_____
Interrogation Unit OIC	_____	_____	_____
Interrogation Supervisor	_____	_____	_____

Interpreter Name and Interpretation Method: _____

Other Participants:_____

Lead Agency: _____

Recording Method:_____Monitoring Method:_____

SAMPLE

Figure 10-3. Interrogation Plan Format.

PREPARATION:

Coordinate with MP for access to the detainee.

Prepare for exploitation topics:
- Obtain appropriate map sheet(s)
- Obtain references
- Review previous reports, detainee correspondence
- Research collection topics
- Prepare questions

Prepare interrogation site (furnishings, lighting, climate, security, monitoring).

Ask Guard Questions.

Review Detainee Documentation:
- ID Card
- Capture Tag
- Documents captured with the detainee

Post-Interrogation Report

Effectiveness of Approaches:

Attitude and Behavior of Detainee:

Summary of Topics Exploited:

Expected Reports Production in Response to Requirements:

Termination:
- Reason:
- Approach Reinforced:
- Incentive Promised:
- Delivered:

Recommendation for Further Interrogation and Rationale:

- Recommended Approach(es):

- Topics for Further Exploitation (Leads):

Disposition of Source:_____

Additional Comments:_____

_____

_____

_____

_____

SAMPLE

Figure 10-3. Interrogation Plan Format (continued).

This page intentionally left blank.

Chapter 11

HUMINT Collection With An Interpreter

11-1. The use of interpreters is an integral part of the HUMINT collection effort. It is vital that the HUMINT collection skills be paired up with a qualified interpreter. Use of an interpreter is time consuming and potentially confusing. Proper use and control of an interpreter is a skill that must be learned and practiced to maximize the potential of HUMINT collection. It is also vital for the HUMINT collector to confirm that the interpreter he intends to use holds the required clearance for the level of information that will be discussed or potentially collected, and is authorized access to the detainee. This chapter deals strictly with the use of interpreters to support HUMINT collection; it is not intended to be applied to more routine uses of interpreters in support of administrative, logistical, or other operational requirements.

ADVANTAGES AND DISADVANTAGES OF INTERPRETER USE

ADVANTAGES

11-2. Interpreters are frequently a necessary aid to HUMINT collection. There are certain advantages to using an interpreter. The most obvious is that without an interpreter, a HUMINT collector without the proper language or necessary proficiency in that language is severely limited. Furthermore, if properly trained, briefed, and assessed, the interpreter can be a valuable assistant to the HUMINT collector. The interpreter—

- Probably has a greater knowledge of the local culture and language usage than could be developed by the HUMINT collector.
- Can identify language and culturally based clues that can help the HUMINT collector confirm or refute the veracity of the source's statements.
- Can interpret not only the literal meaning of a statement but also the intent and emotion of a sentence.

DISADVANTAGES

11-3. There are, however, several significant disadvantages to using interpreters. Disadvantages may include—

- A significant increase in time to conduct the collection. Since the interpreter must repeat each phrase, the time for a given questioning session or meeting is normally at least doubled.
- Since there is now a third person in the communications loop, the potential for confusion or misunderstanding increases significantly. This is especially true when the interpreter is deficient in his command of either language.

- The establishment of rapport and the use of some approach techniques (see Chapter 8) are made difficult or even impossible when working through an interpreter.
- The ability of the HUMINT collector to interpret the source's veracity through the analysis of word usage, nuances of speech, and body language is curtailed.
- The interpreter will have his own set of biases that could influence the manner in which the dialogue is interpreted.
- The source may be culturally biased against the interpreter. This is especially possible if the interpreter was locally hired and is of a different ethnic, social, or religious group than the source.
- The interpreter may be culturally biased against the source and intentionally misinterpret the meaning to obtain a desired effect.
- There may be mission or subject matter classification problems involved.

CAUTIONS

11-4. Be careful of comments made in the presence of your interpreter. Although you plan comprehensively with your interpreter, you should only share information with your interpreter on a need-to-know basis. Obviously the exchange of information concerning the "what, where, when, with whom, and how" of each meeting must be discussed with your interpreter, but sometimes the "real why" is none of his business! You may be meeting with a source or contact because the commander believes this individual has lied. The real purpose (the why) of the meeting is to pose control questions and to determine whether the source or contact lied in the past or whether there was simply a miscommunication.

11-5. Be careful of sensitive or personal conversations when the interpreter is present. This applies to conversations en route to or from meetings, conversations over lunch or dinner in the operational area, and conversations in the team area. It is easy to get used to the presence of the interpreter and to overlook his presence. An interpreter is a necessary tool but we must remember that most are only very lightly screened for the sensitive access they have. If your interpreter turned out to be working for the other side, what information beyond "the necessary" could he provide?

METHODS OF INTERPRETER USE

11-6. There is a basic method and advanced method of interaction between the HUMINT collector and the interpreter. As the collector and the interpreter become experienced at working together and gain confidence in each other's abilities, they may use more advanced interactive techniques. It is the HUMINT collector's decision whether or not to use more advanced techniques.

BASIC METHOD

11-7. The basic method of interaction is used when—

- The interpreter and HUMINT collectors have not worked together extensively.
- The interpreter has language skills but no interpreter training or experience.
- The interpreter's skill in English or the target language is suspect.
- The HUMINT collector has limited experience using an interpreter.
- The interpreter's capabilities, loyalty, or cultural knowledge are not known or suspect.

11-8. Using the basic method, the interpreter is used solely as an interpretation device. When initial contact is made, the interpreter instructs the source to maintain eye contact with the HUMINT collector. The interpreter is briefed on the general course of the collection but usually is not advised of the specific purpose or collection goals. While the interpreter will be instructed to reflect the attitude, behavior, and tone of voice of both the collector and the source, he is told to *not* interpose comments or personal opinions at all in the conversation.

11-9. The questioning phase is conducted in the same way it would be if no interpreter were used with the obvious increase in time due to the interpretation. The interpreter uses the same person and tense as the HUMINT collector or source and neither adds nor subtracts anything from the dialogue. He does his best to fade into the background. When reports are written, the interpreter will only be asked questions based on the actual translation of the dialogue.

ADVANCED METHOD

11-10. The advanced method of interaction requires additional training on the part of the HUMINT collector and the interpreter, extensive experience working together, and a rapport between the HUMINT collector and the interpreter. The HUMINT collector must trust both the capabilities and the judgment of the interpreter. At this level of interaction, the interpreter becomes a more active participant in the HUMINT activities. The HUMINT collector remains in charge and makes it clear to the interpreter that he (the HUMINT collector) is responsible for the substance and direction of the questioning. The interpreter is normally briefed as to the specific goals of the collection.

11-11. The interpreter becomes a more active participant in the approach and termination phases to the point of even making planned comments to the source supportive of the HUMINT collector's approach. For example, if the HUMINT collector is using an incentive approach, the interpreter in an aside to the source can tell him that the HUMINT collector always keeps his promises. This type of technique should only be used if both planned and rehearsed.

11-12. During the questioning phase, the interpreter supports the collector by not only translating the word of the source but also cueing the collector when there are language or culturally based nuances to what the source is

saying that might add credence or doubt as to the veracity of the statements. For example, the interpreter could point out that although the source claims to be a factory worker, his language use indicates that the source has a university education. In another example, the interpreter could indicate that the dialect or pronunciation that the source is using does not match the area that he claims to be from. During report writing, the interpreter supports the HUMINT collector by not only answering questions on the literal interpretation but also adds, when appropriate, comments on the significance of both what was said and how it was said.

SOURCES OF INTERPRETERS

11-13. There are almost never sufficient interpreters to meet all unit mission requirements. Interpreters in support of HUMINT collection require a security clearance and knowledge of the operational situation. While any qualified interpreter can be used to support HUMINT collection, the HUMINT collectors maximize the collection potential if the interpreter has received specific training. The number of interpreters needed to support a HUMINT collection mission is METT-TC driven based primarily on the number of HUMINT collectors, the dispersion of the HUMINT collectors in the AO, and the number of sources. Normally one interpreter for every two non-language qualified HUMINT collectors is sufficient; however, in situations where a large number of high-value sources must be questioned in a limited time, a ratio of 1 to 1 may be required. Interpreters are obtained from within the military and from the US and local civilian populations or other English-speaking countries.

MILITARY

11-14. There are many soldiers, including non-US citizens, who have native language abilities due to their upbringing. Their parent unit may identify these language abilities, or these soldiers may volunteer their abilities when a contingency arises. The ARNG, USAR, other US military services, and even coalition militaries, have language-trained and certified personnel in Military Intelligence MOSs, such as 98G or 09L, who may be called upon to serve as interpreters for the HUMINT collection effort.

CIVILIAN

11-15. Civilian corporations may be contracted by the military to provide interpreters for an operation. These interpreters are divided into three categories:

- CAT I Linguists - Locally hired personnel with an understanding of the English language. These personnel undergo a limited screening and are hired in-theater. They do not possess a security clearance and are used for unclassified work. During most operations, CAT I linguists are required to be re-screened on a scheduled basis. CAT I linguists should not be used for HUMINT collection operations.
- CAT II Linguists - US citizens who have native command of the target language and near-native command of the English language. These personnel undergo a screening process, which includes a national

agency check (NAC). Upon favorable findings, these personnel are granted an equivalent of a Secret collateral clearance. This is the category of linguist most used by HUMINT collectors.

- CAT III Linguists - US citizens who have native command of the target language and native command of the English language. These personnel undergo a screening process, which includes a special background investigation (SBI). Upon favorable findings, these personnel are granted an equivalent of a Top Secret (TS) clearance. CAT III linguists are used mostly for high-ranking official meetings and by strategic collectors.

INTERPRETATION TECHNIQUES

11-16. During the planning and preparation phase, the HUMINT collector, in collaboration with the interpreter, selects a method of interpretation. There are two methods:

- Alternate Interpretation. The interpreter listens to the entire phrase, sentence, or paragraph. The interpreter then translates it during natural pauses in speech.
- Simultaneous Interpretation. The interpreter listens to the source and translates what he says, just a phrase or a few words behind. The HUMINT collector should select the simultaneous method only if all the following criteria are met:
  - The sentence structure of the target language is parallel to English.
  - The interpreter can understand and speak English as well as the target language with ease.
  - The interpreter has special vocabulary skills for the topics to be covered.
  - The interpreter can easily imitate the HUMINT collector's tone of voice and attitude for the approaches and questioning technique selected.
  - Neither the collector nor the interpreter tends to get confused when using the simultaneous method of interpretation.

11-17. If any of the above-mentioned criteria in the simultaneous method cannot be met, the HUMINT collector should use the alternate method. The alternate method should also be used when a high degree of precision is required.

TRAINING AND BRIEFING THE INTERPRETER

11-18. The HUMINT collector will need to train an individual who has no interpreter experience as well as remind a trained and certified interpreter of the basic interpreter requirements. The requirements include—

- Statements made by the interpreter and the source should be interpreted in the first person, using the same content, tone of voice, inflection, and intent. The interpreter must not interject his or her own personality, ideas, or questions into the interview.

- The interpreter should inform the HUMINT collector if there are any inconsistencies in the language used by the source. The HUMINT collector will use this information in his assessment of the source.
- The interpreter needs to assist with the preparation of reports and administrative documents relevant to the source and meeting.

11-19. Once the HUMINT collector has chosen a method of interpretation, he must brief the interpreter. This briefing must cover—

- The current situation.
- Background information on the source (if available).
- The administrative particulars of the meeting such as where it will be held, the room setup, how long it will last.
- The specific positioning of the interpreter, collector, and source.
- The general or (if advanced method of interaction is being used) the specific collection objectives.
- The selected approach and possible alternate approaches that the HUMINT collector plans on using. If time allows, the collector and interpreter should rehearse the approaches.
- Any special topic or technical language that is anticipated. If time allows, the interpreter should research any anticipated technical vocabulary with which he is unfamiliar.

11-20. Throughout the briefing, the HUMINT collector fully and clearly answers questions the interpreter may have. This helps ensure the interpreter completely understands his role in the HUMINT collection process. With a more advanced interaction plan, the HUMINT collector and the interpreter should "wargame" their plan and rehearse their actions as necessary.

PLACEMENT OF THE INTERPRETER

11-21. The interpreter should be placed in a position that enhances the mood or general impression that the HUMINT collector wants to establish. When dealing with detainees or EPWs, the HUMINT collector generally wants to establish a dominant position, maintain a direct relationship with the source, and increase or at least maintain the anxiety level of the source. Having the HUMINT collector and the source facing each other with the interpreter located behind the source normally facilitates this. It allows the HUMINT collector to maximize control of both the source and interpreter. If desired, having the interpreter enter the room after the source, so the source never sees the interpreter, can further heighten the anxiety of the source.

11-22. Having the interpreter sit to the side of the HUMINT collector creates a more relaxed atmosphere. This is the norm for debriefings and official meetings. Having the interpreter at his side also facilities "off line" exchanges between the HUMINT collector and the interpreter. The collector should avoid having the interpreter sit beside the source since this has a tendency of establishing a stronger bond between the source and the interpreter and makes "off line" comments between the collector and the interpreter more difficult.

11-23. When conducting source meetings in a public setting, a more natural appearance is desirable. The seating needs to conform to the norm at the location where the meeting is taking place. For example, if meeting at a restaurant, the HUMINT collector, interpreter, and source will sit naturally around the table.

INTERACTIONS WITH AND CORRECTION OF THE INTERPRETER

11-24. The HUMINT collector must control the interpreter. He must be professional but firm and establish that he is in charge. During a questioning session, the HUMINT collector corrects the interpreter if he violates any standards that the pre-mission briefing covered. For example, if the interpreter interjects his own ideas into the meeting, he must be corrected. Corrections should be made in a low-key manner as to not alienate the interpreter, interrupt the flow of the questioning, or give the source the impression that there is an exploitable difference of opinion between the HUMINT collector and the interpreter. At no time should the HUMINT collector rebuke the interpreter sternly or loudly while they are with the source. The HUMINT collector should never argue with the interpreter in the presence of the source. If a major correction must be made, the HUMINT collector should temporarily terminate the meeting and leave the site temporarily to make the correction. The HUMINT collector needs to document any difficulties as part of his interpreter evaluation. The HUMINT collector must always ensure that the conduct and actions of the interpreter are within the bounds of applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

11-25. The HUMINT collector must be alert for any signs that the interpreter is not performing as required. The following are some indicators of possible problems.

- Long-to-short. If you take 20 seconds to express yourself and the interpreter reduces it to a 3-second translation, it may indicate that something has been omitted, and you should not proceed until you have resolved the issue. There is nothing wrong with stating that you would "prefer" the interpreter translate everything that was just said. If you have trained your interpreter properly, this should not be an issue. If it arises even with the training you have given the interpreter, then it has significance and you must not let it pass.
- Short-to-long. If you take 5 seconds to express yourself and the interpreter expands it to a 30-second translation, it may indicate that something has been added, and you should not proceed until you have resolved the issue.
- Body-language shift. If the interpreter's body language suddenly has a significant shift from his normal behavior, you should look for the reason. (It is advisable for you to determine a base line of behavior for your interpreter to facilitate recognition of the changes.) Perhaps he is reluctant to translate what you just said. Be aware that the body shift

means that something is happening—your task is to find out what it means.

- Unusual pauses. Look for a longer delay than usual before the translation begins. Unless it is a vocabulary or concept issue, the long delay means that the interpreter is "thinking" before he translates. Any thinking beyond what is needed to translate, as closely as possible, what was just said represents a potential problem. Again, you should establish a base line of behavior for your interpreter so you can recognize these unusual pauses.
- "Wrong" reactions. If you say something humorous that should provoke a positive response from the source, and you do not get that response, then you should wonder if the message got through. If the source becomes upset in response to something (positive) you said, then you should begin to wonder what message was passed by the interpreter. Did you fail to express yourself clearly, or was it an accidental or deliberate mistranslation?

11-26. A trusted linguist should periodically review the accuracy of the interpreter's translations by monitoring an interrogation or debriefing and critiquing the monitored interpreter's performance.

INTERPRETER SUPPORT IN REPORT WRITING

11-27. The interpreter assists the HUMINT collector in preparing all required reports. He may be able to fill gaps and unclear details in the HUMINT collector's notes. He may also assist in transliterating, translating, and explaining foreign terms.

EVALUATING THE INTERPRETER

11-28. After submitting all reports, the HUMINT collector evaluates the performance of his interpreter. This should be done in writing, and copies should be given to the interpreter and placed on file with the individual managing the HUMINT collection portion of the interpreter program. The interpreter program manager needs to develop a standard evaluation format for inclusion in the unit SOP. The evaluation forms should note at a minimum:

- Administrative data (for example, date, time, interpreter's name).
- Strengths and weaknesses of the interpreter with any problems and corrective actions taken.
- Type of interpretation used (simultaneous or alternate).
- Type of HUMINT operation the interpretation was supporting (that is, an interrogation, a debriefing, a liaison meeting).
- Ability or lack of ability of the interpreter to use specific technical language that may have been required.
- Name or collector number of the HUMINT collector.

11-29. The interpreter program manager uses these forms to decide on future use of the interpreters, to develop training programs for the interpreters, and to assign interpreters to make maximum use of their specific capabilities.

The HUMINT collector should also review these files before using an unfamiliar interpreter.

MANAGING AN INTERPRETER PROGRAM

11-30. Units requiring interpretation support need to identify an individual or individuals to manage the interpreter program. In most units, this will be someone in the G3/S3 section. Division and Corps-level units will have a language manager. In MI units whose specific function is HUMINT collection, it will normally be a senior Warrant Officer within that unit. The functions of the interpreter program manager include but are not limited to—

- Consolidating and prioritizing interpreter requirements.
- Coordinating with G2 or INSCOM to contract for qualified interpreters.
- Coordinating with the G1/S1 to identify personnel in the unit with language skills who can be used as interpreters.
- Coordinating with the G1/S1 and G5 to obtain qualified local-hire interpreters.
- Coordinating with G2/S2 for clearances.
- Coordinating with the G3/S3 to establish training for both the interpreters and those that will be using interpreters.
- Coordinating with the G3/S3 for language testing of the interpreters in both English and the target language as required.
- Coordinating with the G1/S1 and G4/S4 to ensure that all administrative and logistical requirements for the interpreters are met.
- Establishing and maintaining the administrative, operational, and evaluation files on the interpreters.
- Assigning or recommending the assignment of interpreters to operational missions based on their specific capabilities.

This page intentionally left blank.

PART FOUR

Analysis and Tools

Part Four discusses HUMINT analysis and the automation and communication tools needed to support the HUMINT collection effort.

HUMINT analysis supports operational planning and provides direction to HUMINT collection operations. Analysts determine if information from a single human source is internally consistent based on factors such as placement and access of source, prior information from the source, and existing holdings. Source analysis is used to determine if the information from a source is complete, truthful, and responsive to collection requirements. Operational analysis consists of those actions taken to determine how to best meet requirements.

Modern automation and communications systems are vital to HUMINT collection. Real-time collaboration, detailed operational planning and ISR integration, as well as enhanced collection and source exploitation tools, must support team efforts. Emerging technology continues to allow the entire HUMINT collection system to operate more effectively. Commanders must be prepared to supply their HUMINT collection assets with the best possible technology.

Chapter 12

HUMINT Analysis and Production

12-1. Analytical processes provide information to support the commander, his staff, and his unit. Analysis is an integral part of HUMINT collection. Analysis occurs throughout the HUMINT collection process but can be divided into four primary categories: analytical support to operational planning and targeting, operational analysis and assessment, source analysis, and single-discipline HUMINT analysis and production.

ANALYTICAL SUPPORT TO OPERATIONAL PLANNING

12-2. Several elements provide analytical support at various echelons, including the following:

- The HAT is subordinate to the G2 ACE. The HAT supports the G2 in developing IPB products and in developing and tailoring SIRs to match HUMINT collection capabilities.

- The HAC is subordinate to the C/J/G/S2X and functions in the same capacity for the C/J/G/S2X as the HAT does for the ACE.
- The HOC of the C/J/G/S2X supports the C/J/G/S2 and C/J/G/S2X in the identification of HUMINT collection opportunities, the development of taskings and RFIs for HUMINT collection assets, as well as the development of a HUMINT database.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

12-3. The HAT assists the G2 in the identification and characterization of the human component of operations and its effects on friendly and enemy operations. As part of its assistance to the G2, the HAT compiles and analyzes data about the local civilian population including its political, ethnic, religious, cultural, tribal, economic, and other social components. It carefully examines the various component groups and their predicted reaction to friendly force operations.

12-4. The HAT also provides input to all-source analysis by identifying specific actions and motivational factors that should strengthen the local population's support of the US or at least weaken its support of the enemy and by providing information on transient (refugees, DPs, third-country nationals) population and its effects on friendly and enemy operations. In addition to the above, the HAT—

- Closely examines the current and potential threat to identify all factors, such as morale, motivation, training, and beliefs that would affect both positively and negatively on enemy and opposing force capabilities.
- Identifies formal and informal leaders of hostile, neutral, and friendly groups and how their influence is likely to affect operations.
- Develops overlays, databases, and matrices, as required, to support IPB. These overlays may represent a wide variety of intelligence issues, including battlefield infrastructure (for example, electrical power grid), population density, ethnic, religious, or tribal affiliation, and no-strike or collateral damage.
- Provides its products to the C/J/G/S2, the all-source analysts and CI analysts of the ACE, the HOC, the C/J/G/S2X, and HUMINT collection units as required.

ISR TASK DEVELOPMENT

12-5. The HAT and the C/J/G/S2X support the C/J/G/S2 by expanding the PIRs that can be answered through HUMINT collection into ISR tasks that can be answered by a human source and that can be tasked to a specific collection entity. The HAT and the C/J/G/S2X provide this information to support the development of the HUMINT collection plan and its integration into the overarching ISR plan. The HAT normally establishes a list of prioritized standing indicators, and supplements this with ISR tasks developed to answer specific PIRs. The standing indicators are incorporated into the ACE's all-source analysis team's list of indicators that point to a pattern or COA. Each standing indicator is integrated with other indicators

and factors so that analysts can detect patterns and establish threat intentions.

SUPPORT TO HUMINT TASKING

12-6. The C/J/G/S2X supports the C/J/G/S2 and the C/J/G/S2 requirements manager by developing tasking for specific organic or attached HUMINT collection assets and by developing requests and coordinating for support from higher and lateral echelon HUMINT collection elements. The C/J/G/S2X matches specific collection requirements to collection units and sources. If current sources cannot answer the requirement, he develops profiles for new sources that guide the collection teams in the development of new sources. The C/J/G/S2X also determines the best method to achieve collection requirements. The C/J/G/S2X supplies any required technical support to the HUMINT operations section, OMTs, and HCTs.

HUMINT DATABASE DEVELOPMENT

12-7. The C/J/G/S2X maintains the source database, which receives input from HUMINT collection and CI operations. The C/J/G2X is responsible for maintaining the source database.

OPERATIONAL ANALYSIS AND ASSESSMENT

12-8. Operational analysis consists of those actions taken to determine how to best meet requirements. Assessment evaluates the effectiveness of the requirement effort. Operational analysis begins with the C/J/G/S2X when he determines the best collection assets and sources needed to answer collection requirements. For **analysis**, the C/J/G/S2X section and specifically the HOC—

- Provides higher echelon coordination and deconfliction for collection operations.
- Provides required technical support to the HUMINT operations sections, OMTs, and HCTs.
- Facilitates feedback and evaluations.

12-9. For **assessment**, the C/J/G/S2X section and specifically the HOC—

- Monitors all HUMINT reporting to ensure that requirements are being met.
- Refocuses efforts of assigned assets as needed.

12-10. The HUMINT operations section (if one exists) and the OMTs of tasked collection units determine which HCTs are best suited to meet specific collection requirements. They also conduct operational coordination for the HCT, provide technical support, and monitor all reporting to ensure that reports are properly formatted and support collection requirements. The team leader of the tasked HCT selects the specific collectors and sources to meet collection requirements, reviews the collection plan, provides technical support to the collectors, coordinates with the supported unit, and monitors all team reporting for format and content. He identifies additional lines of questioning and approaches required to fulfill collection requirements.

SOURCE ANALYSIS

12-11. Source analysis involves the actions taken to determine if information from a single human source is internally consistent based on factors such as placement and access of source, prior information from the source, and existing holdings. Source analysis is used to determine if the information from a source is complete, truthful, and responsive to collection requirements. Preliminarily source analysis is the responsibility of the individual HUMINT collector.

12-12. The HUMINT collector evaluates all source statements within the context of the information known about the source and the current situation to determine both the veracity and the validity of source statements. That is not to say that the HUMINT collector ignores any information that does not fit into expected pattern; rather that he treats that information with skepticism and uses appropriate questioning methodology to validate the statements (see Chapter 9). Source analysis is supported by the HCT leader, the OMTs, and the HOC. Each echelon reviews the intelligence and operational reports, identifies inconsistencies, evaluates veracity, and recommends additional lines of questioning as appropriate.

12-13. Analysts can assign an alphanumeric designator to collected information based on an analyst's determination of the reliability of the source and the probable accuracy of the information reported. A letter from A to F is assigned reflecting the level of reliability, with A representing the highest degree of reliability. The letter designation is then coupled with a number from 1 to 6. The number 1 represents confirmed intelligence and the numbers 2 through 6 represent increasing degrees of uncertainty as to the veracity of the information. A complete explanation if this rating system is contained in Appendix B. [NOTE: This system of labeling the reliability of sources and their reported information should not be confused with the alphanumeric rating scheme for source-screening operations as described in Chapter 6.]

SINGLE-DISCIPLINE HUMINT ANALYSIS AND PRODUCTION

12-14. Single-discipline HUMINT analysis involves the actions taken to evaluate the information provided by all HUMINT sources at a given echelon to determine interrelationships, trends, and contextual meaning. While called "single discipline," the analyst reviews and incorporates, as necessary, information from other disciplines and all-source analysis to provide a contextual basis for the HUMINT analysis. Single-discipline HUMINT analysis is conducted primarily by the HAT of the ACE. HUMINT operations sections and OMTs also conduct analysis to a lesser degree, based on the information from HUMINT sources at their echelon.

12-15. Analysis does more than simply restate facts. The analyst formulates a hypothesis based on available data, assesses the situation, and explains what the data means in logical terms that the user can understand. There are two basic thought processes used by analysts to study problems and reach conclusions: induction and deduction.

- Induction is the process of formulating hypotheses on the basis of observation or other evidence. It can best be characterized as a process of discovery when the analyst is able to establish a relationship between events under observation or study. Induction, or plausible reasoning, normally precedes deduction and is the type of reasoning analysts are required to perform most frequently.
- Deduction is the process of reasoning from general rules to particular cases. The analyst must draw out, or analyze, the premises to form a conclusion. Deductive reasoning is sometimes referred to as demonstrative reasoning because it is used to demonstrate the truth or validity of a conclusion based on certain premises.

ANALYTICAL TECHNIQUES AND TOOLS

12-16. There are three basic analytical techniques and automated tools that are particularly useful to single-discipline HUMINT analysis. Each of these tools takes fragmented bits of information and organizes them to create a chart or graph that can easily be read. They are the time event chart, matrices, and the link analysis diagram. HUMINT collectors and analysts can use automated computer programs such as Analyst Notebook or Crime Link to produce these tools or they can create them on paper. Computer programs are faster to use than previous methods and have the added advantage of producing a product that can be shared easily and rapidly over networks and portals. The diagrams in this chapter represent the tools that can be produced using automated programs.

Time Event Chart

12-17. A time event chart is a method for placing and representing individual or group actions in chronological form. It uses symbols to represent events, dates, and the flow of time. Normally, triangles are used to depict the beginning and end of the chart and may be used within the chart to indicate particularly critical events such as an ideological shift or change. Rectangles, used as event nodes, store administrative data and indicate significant events or activities. Drawing an "X" through the event node may highlight noteworthy or important events. Each of these symbols contains a sequence number, date (day, month, and year of the event), and may, if desired, contain a file reference number. The incident description written below the event node is a brief explanation of the incident and may include team size and type of incident. Arrows indicate time flow. By using these symbols and brief descriptions, it is possible to analyze the group's activities, transitions, trends, and particularly operational patterns in both time and activity. If desired, the event nodes may be color coded to indicate a particular event or type of event to aid in pattern recognition. The time event chart is the best analytical tool for pattern analysis. The example at Figure 12-1 depicts the history of the group, including most major players, which carried out the World Trade Center bombing in February 1993.

Matrices

12-18. Construction of a matrix is the easiest and simplest way to show the relationships between a number of similar or dissimilar associated items. The items can be anything that is important to a collection effort such as people, places, organizations, automobile license plates, weapons, telephone numbers, or locations. In analysis, matrices are often used to identify "who knows whom," or "who has been where or done what" in a clear concise manner. There are two types of matrices used in human analysis: the association matrix, used to determine existence of relationships between individual human beings, and the activities matrix, used to determine connectivity between individuals and any organization, event, address, activity, or any other non-personal entity. The graphics involved in constructing the two types of matrices differ slightly, but the principles are identical.

12-19. The association matrix (Figure 12-2) shows connections between key individuals involved in any event or activity. It shows associations within a group or associated activity. Normally, this type of matrix is constructed in the form of an equilateral triangle having the same number of rows and columns. Personalities must be listed in exactly the same order along both the rows and columns to ensure that all possible associations are correctly depicted. An alternate method is to list the names along the diagonal side of the matrix. This type of matrix does not show the nature, degree, or duration of a relationship, only that a relationship exists. The purpose of the matrix is to show the analyst who knows whom and who are suspected to know whom. In the event that a person of interest dies, a diamond is drawn next to his or her name on the matrix.

12-20. The analyst uses a dot or closed (filled-in) circle to depict a strong or known association. A known association is determined by direct contact between one or more persons. Direct contact is determined by several factors. *Direct associations* include—

- Face-to-face meetings.
- Telephonic conversations in which the analyst is sure who was conversing with whom.
- Members of a cell or other group who are involved in the same operations.

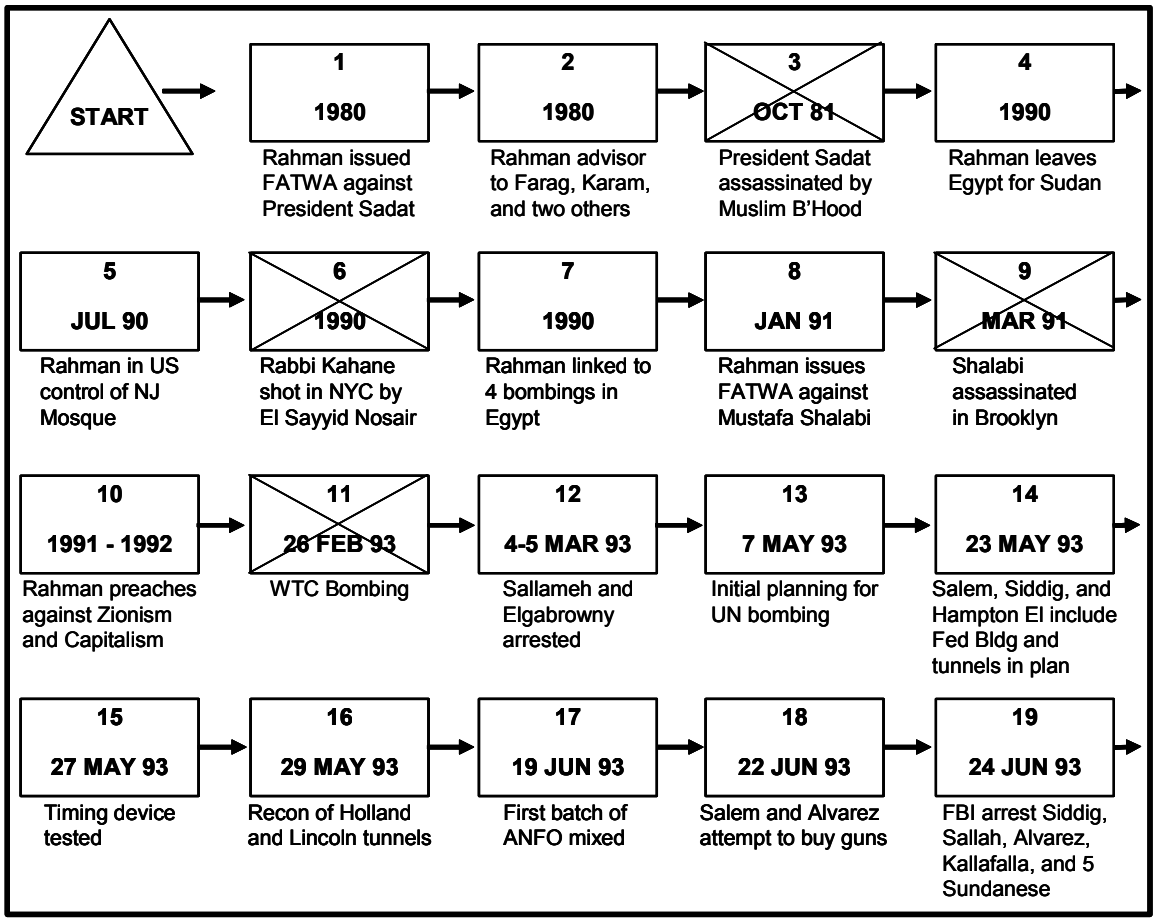


Figure 12-1. Example of a Time Event Chart.

12-21. Suspected or weak associations are those associations in which there are indicators that individuals may have had associations but there is no way to confirm that association; this is depicted with an open circle. Examples of *suspected associations* are—

- A known party calling a known telephone number (the analyst knows to whom the telephone number is listed) but it cannot be determined with certainty who answered the call.
- A face-to-face meeting where one party can be identified, but the other party can only be tentatively identified.

12-22. The rationale for depicting suspected associations is to get as close as possible to an objective analytic solution while staying as close as possible to known or confirmed facts. If a suspected association is later confirmed, the appropriate adjustment may be made on the association matrix. A secondary reason for depicting suspected associations is that it may give the analyst a focus for tasking limited intelligence collections assets in order to confirm the suspected association. An important point to remember about using the association matrix is that it will, without modification, show only the

existence of relationships; not the nature, degree, or duration of those relationships.

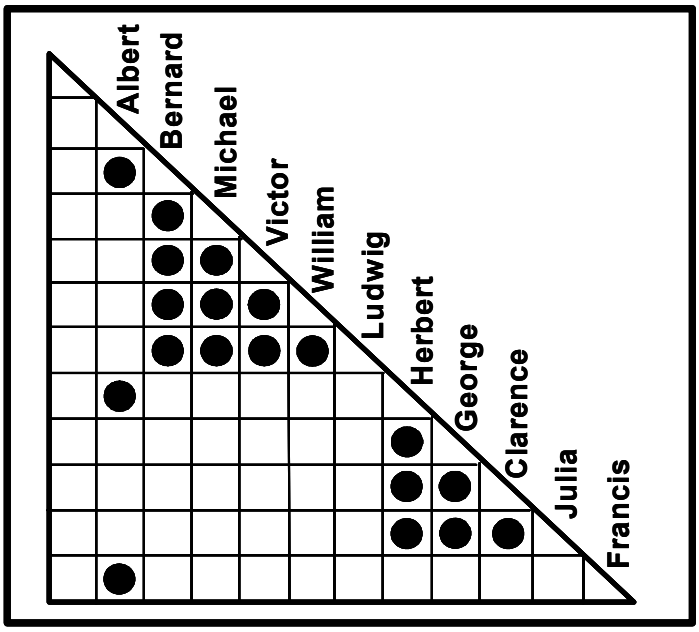


Figure 12-2. Example of an Association Matrix.

12-23. The activities matrix (Figure 12-3) is a rectangular array of personalities compared against activities, locations, events, or other appropriate information. The kind and quality of data that is available to the collector determines the number of rows and columns and their content. The analyst may tailor the matrix to fit the needs of the problem at hand or he may add to it as the problem expands in scope. This matrix normally is constructed with personalities arranged in a vertical listing on the left side of the matrix, and events, activities, organizations, addresses, or any other common denominator arranged along the bottom of the matrix. This matrix is critical for the study of a group's internal and external activities, external ties and linkages, and even modus operandi. As with the association matrix, confirmed or "strong" associations between individuals and non-personal entities are shown with a solid circle or dot, while suspected or "weak" associations are illustrated by an open circle.

12-24. Using matrices, the analyst can pinpoint the optimal targets for further intelligence collection, identify key personalities within an organization, and considerably increase the analyst's understanding of an organization and its structure. Matrices can be used to present briefings or to store information in a concise and understandable manner within a database. Matrices augment but cannot replace SOPs or standard database files. It is possible, and sometimes productive, to use one matrix for all associations. This is done routinely using the automated systems mentioned in paragraph 13-6.

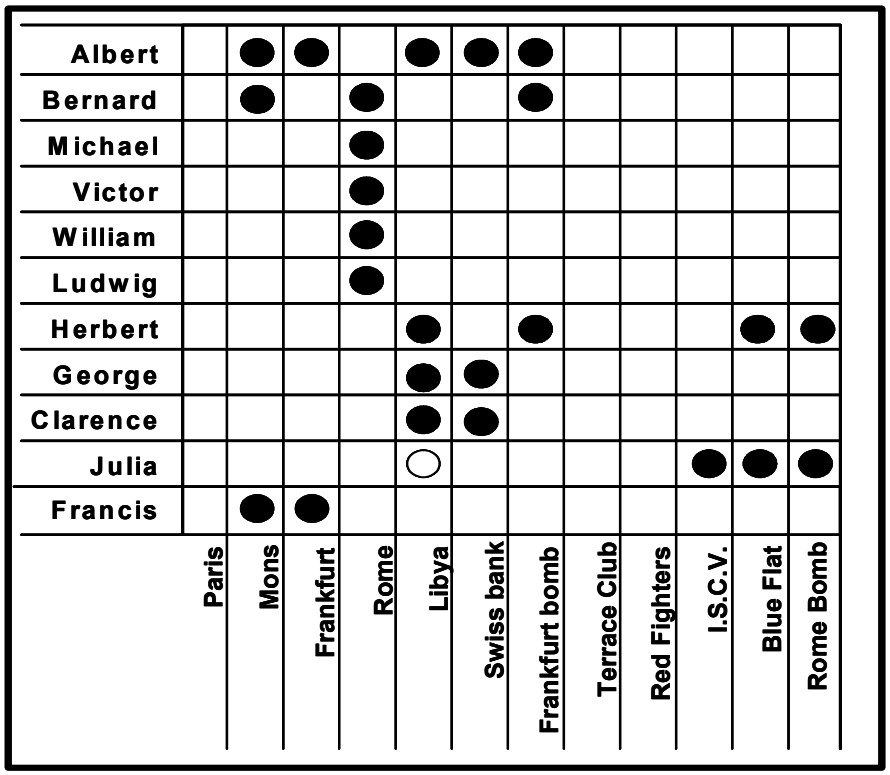


Figure 12-3. Example of an Activities Matrix.

12-25. The link analysis diagram (Figure 12-4) shows the connections between people, groups, or activities. The difference between matrices and link analysis is roughly the same as the difference between a mileage chart and a road map. The mileage chart (matrix) shows the connections between cities using numbers to represent travel distances. The map (link analysis diagram) uses symbols that represent cities, locations, and roads to show how two or more locations are linked to each other.

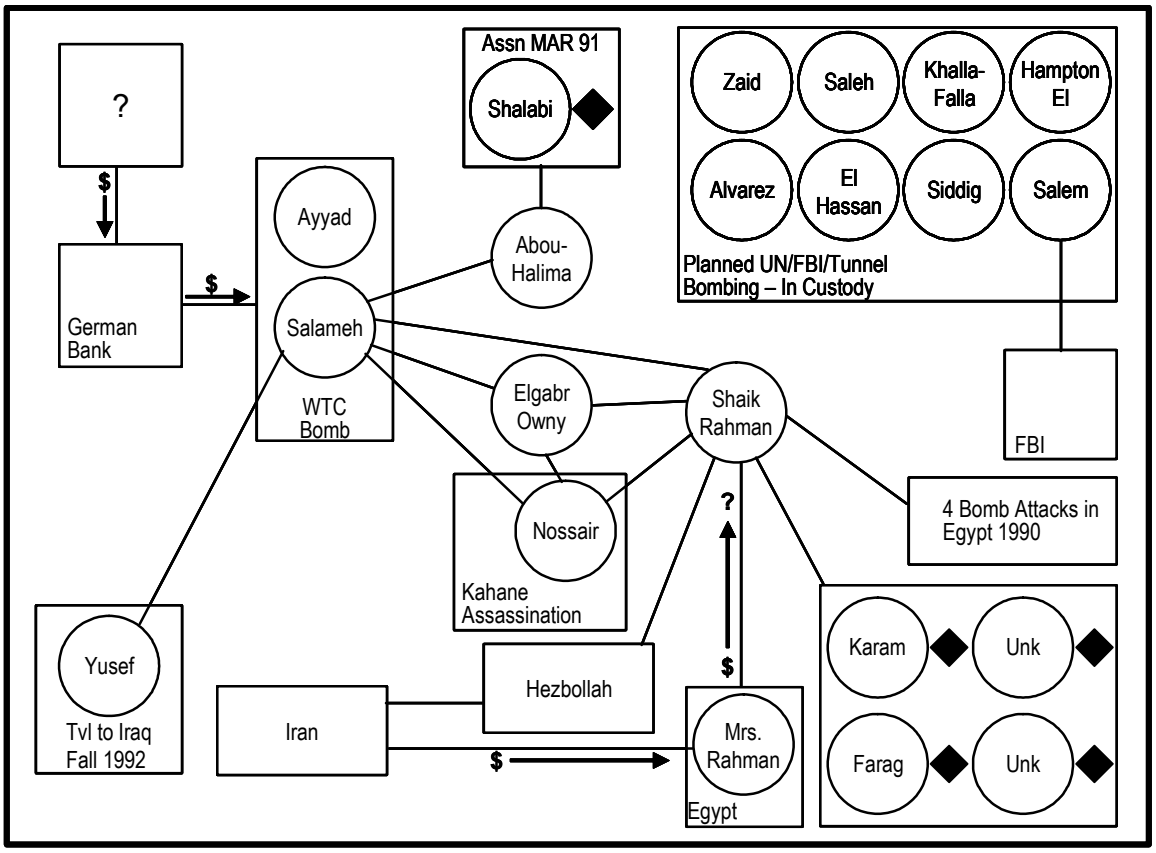
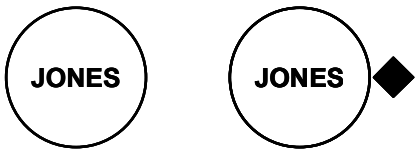


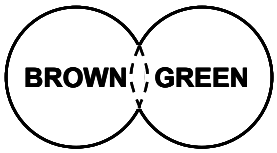
Figure 12-4. Example of a Link Analysis Diagram.

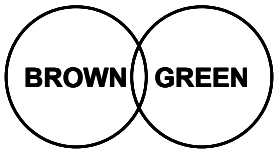
12-26. As with construction of association matrices, there are certain rules of graphics, symbology, and construction that must be followed. Standardization is critical to ensuring that everyone constructing, using, or reading a link analysis diagram understands exactly what the diagram depicts. Circles and lines are arranged so that no lines cross whenever possible. Often, especially when dealing with large groups, it is very difficult to construct a line diagram in which no lines cross. In these cases, every effort should be made to keep the number of crossings at an absolute minimum. The standard rules are as follows:

- Persons are shown as open circles with the name written inside the circle. Deceased persons are depicted in either open circles, with a diamond next to the circle representing that person (as in Figure 12-4) or as open diamonds with the name written inside the diamond.



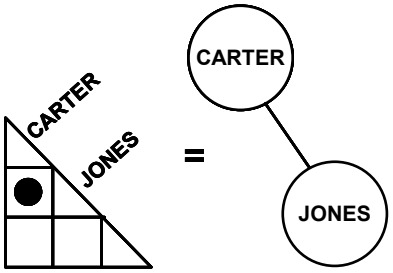
- Persons known by more than one name (alias or AKA) are shown as overlapping circles with names in each circle (as shown below) or both names are simply listed in the same circle. If the alias is suspected, a dotted line is used to depict the intersection. If the alias is confirmed, the intersection is shown with a solid line.

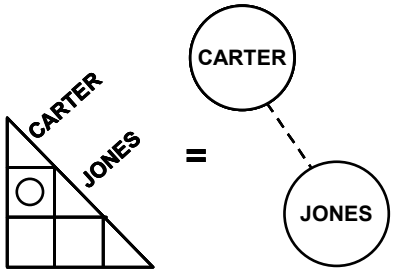




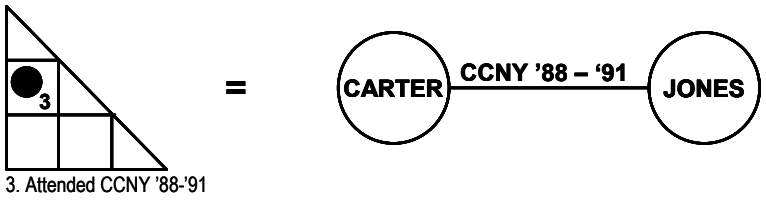
- Non-personal entities (organizations, governments, events, locations) are shown as appropriately labeled rectangles.

- Solid lines denote confirmed linkages or associations and dotted lines show suspected linkages and associations.



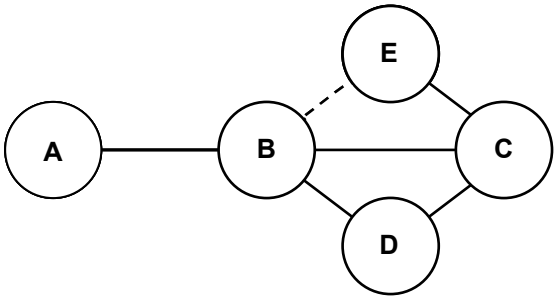


- Footnotes on the matrices can be shown as a brief legend on the connectivity line.



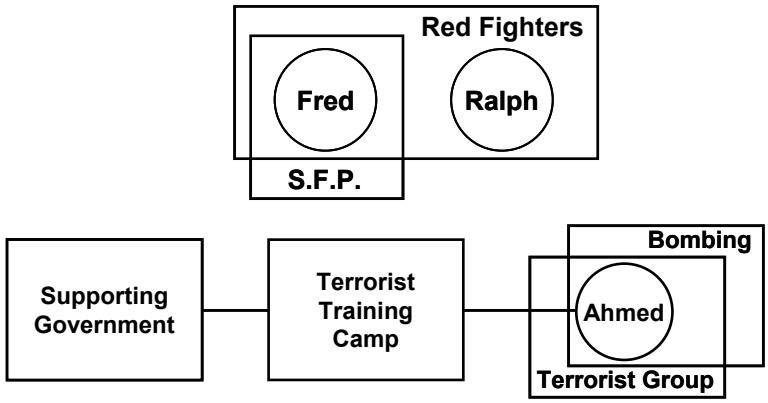
- Each person or non-personal entity is depicted only once in a link analysis diagram.

12-27. The following diagram shows only connectivity between persons:



12-28. The analyst can easily determine from the diagram that Alpha knows Bravo, Bravo knows Charlie and Delta. Bravo is suspected of knowing Echo and Charlie knows Delta, Bravo, and Echo. Although the same information could be shown on a matrix, it is easier to understand when depicted on a link analysis diagram. As situations or investigations become more complex, the ease in understanding a link analysis diagram becomes more apparent. In almost all cases, the available information is first depicted and analyzed on both types of matrices, which are then used to construct a link analysis diagram for further analysis.

12-29. Link analysis diagrams can show organizations, membership within the organization, action teams or cells, or participants in an event. Since each individual depicted on a link analysis diagram can be shown only once, and some individuals may belong to more than one organization or take part in more than one event, squares or rectangles representing non-personal entities may have to overlap. The following illustration demonstrates that Ralph and Fred are both members of the "Red Fighters," and that Fred also is a member of the "Students for Peace." Further, since Ralph and Fred are shown in the same “box,” it is a given that they are mutually associated.



12-30. There is more to overlapping organizations than is immediately obvious. At first glance, the overlap indicates only that an individual may belong to more than one organization or has taken part in multiple activities. Further study and analysis would reveal connections between organizations, connections between events, or connections between organizations and events, either directly or through persons. The above diagram reveals a more

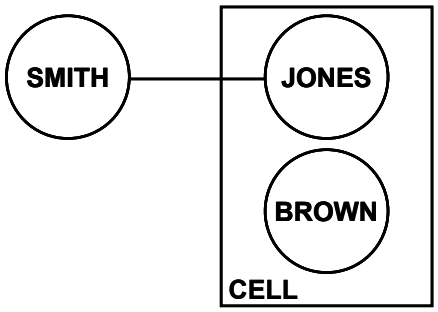
complex connection between organizations, personal connections, and linkages.

12-31. The analysis diagram in paragraph 12-29 shows a connection between organizations and events to which an individual belongs or is associated. In this case, a national government runs a training camp for terrorists. Ahmed, a member of the terrorist group, is associated with the training camp, and participated in the bombing attack. From this diagram, one can link the supporting government to the bombing through the camp and the participant.

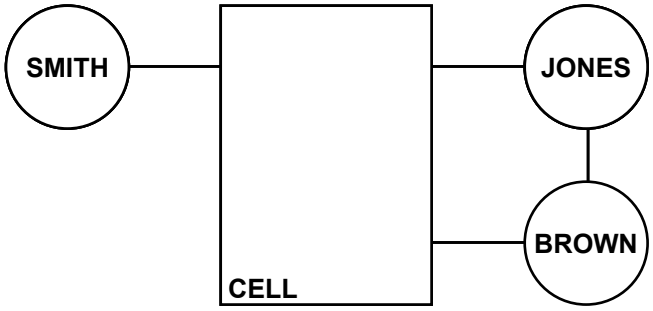
12-32. When, as is often the case, an organization or incident depicted in a link analysis diagram contains the names of more than one individual, it is not necessary to draw a solid line between those individuals to indicate connectivity. It is assumed that individual members of the same cell or participants in the same activity know each other, and the connection between them is therefore implied. If the persons are **not** mutually associated, they cannot be placed in the same "box." Another solution must be found to depict the situation; that is, show the persons as associated with a subordinate or different organization or activity.

12-33. A final set of rules for link analysis diagrams concerns connectivity between individuals who are not members of an organization or participants in an activity, but who are somehow connected to that entity. Two possibilities exist: First, the individual knows a member or members of the organization but is not associated with the organization itself; or second, the person is somehow connected with the organization or activity but cannot be directly linked with any particular member of that entity.

12-34. In the first case, the connectivity line is drawn only between the persons concerned as depicted here:



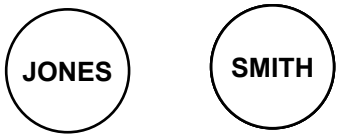
12-35. In the second case, where Smith is associated with the entity, but not the persons who are members of entity, the situation is shown as depicted here:



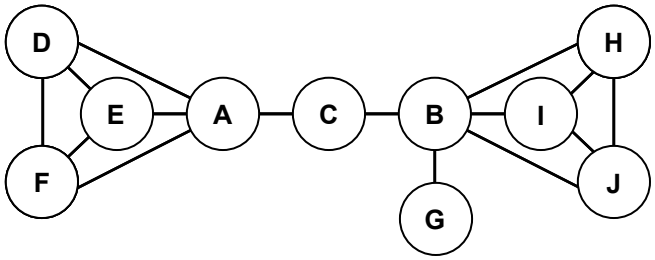
12-36. The steps in constructing a link analysis diagram are as follows:

- **Step 1**. Raw data or fragments of information are organized into logical order. Names of individuals, organizations, events, and locations are compiled on appropriate lists. At this point, a time event chart may be completed to assist in understanding the information and to arrange events into chronological order.
- **Step 2**. Information is entered onto the appropriate matrices, graphically displaying "who is associated with whom" and "who is associated with what."
- **Step 3.** Drawing information from the database and intelligence reports, and relationships from the matrices, the link analysis diagram can be constructed. The best method to start the link analysis diagram is to—
  - Start with the association matrix and determine which person has the greatest number of personal associations. Depict that person in the center of the page.

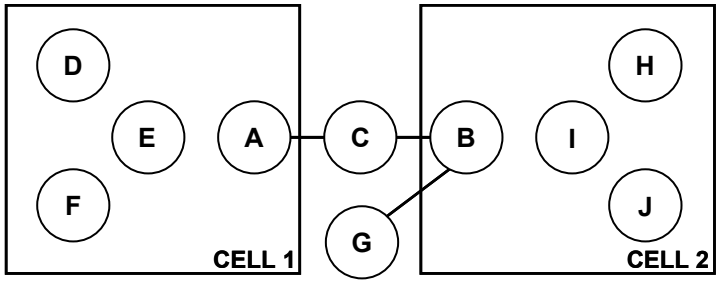
  - Determine which person has the next highest number of personal associations. Depict that person near the first person.



12-37. Use the association matrix and show all confirmed and suspected personal associations.



- After all personal associations have been shown on the link analysis diagram, the analyst uses the activities matrix to determine which activities, organizations, or other non-personal entities need to be depicted by appropriate rectangles. Having done so, the lines of connectivity between persons within the rectangles may be removed to prevent clutter. (It is assumed that participants in the same activity or members of the same cell are acquainted.)



12-38. As shown in Figure 12-4, the link analysis diagram depicts the membership, organization, activities, and connections of the group that, under the leadership of Sheik Omar Abdul Rahman, carried out the bombing of the World Trade Center in New York City and planned other bombing attacks. Together with the time event chart (Figure 12-1), one can gain a basic understanding of the group and its activities, and develop working hypotheses for additional collection and analysis efforts.

12-39. After completion of the matrices and the link analysis diagram, the analyst makes recommendations about the group's structure, and areas can be identified for further collection. Collection assets are employed to verify suspected connections, ID key personalities, and substantiate or refute the conclusions and assessments drawn from the link analysis that has been done. The link analysis diagram and thorough analysis of the information it contains can reveal a great deal about an organization. It can identify the group's leadership, its strong and weak points, and operational patterns. The analyst can use these to predict future activities.

OTHER ANALYSIS TOOLS

12-40. Pattern analysis is the process of deducing the doctrine and TTP that threat forces prefer to employ by careful observation and evaluation of patterns in its activities. This technique is based on the premise that threat COAs reflect certain characteristic patterns that can be identified and interpreted. Pattern analysis can be critically important when facing a threat whose doctrine is unknown and it is necessary to create new threat model and doctrinal templates. Three additional tools that can help the analyst to determine operational patterns and create and update their threat model are the coordinates register, pattern analysis plot sheet, and OB factors.

Coordinates Register

12-41. The coordinates register, or incident map, is one type of pattern analysis tool (Figure 12-5). It illustrates cumulative events that have occurred within the AO and focuses on the "where" of an event. The analyst may use multiple coordinates registers that focus on a different subject or blend subjects. Normally, the coordinates register includes additional information such as notes or graphics. The analyst should use the coordinates register in conjunction with the pattern analysis plot sheet.

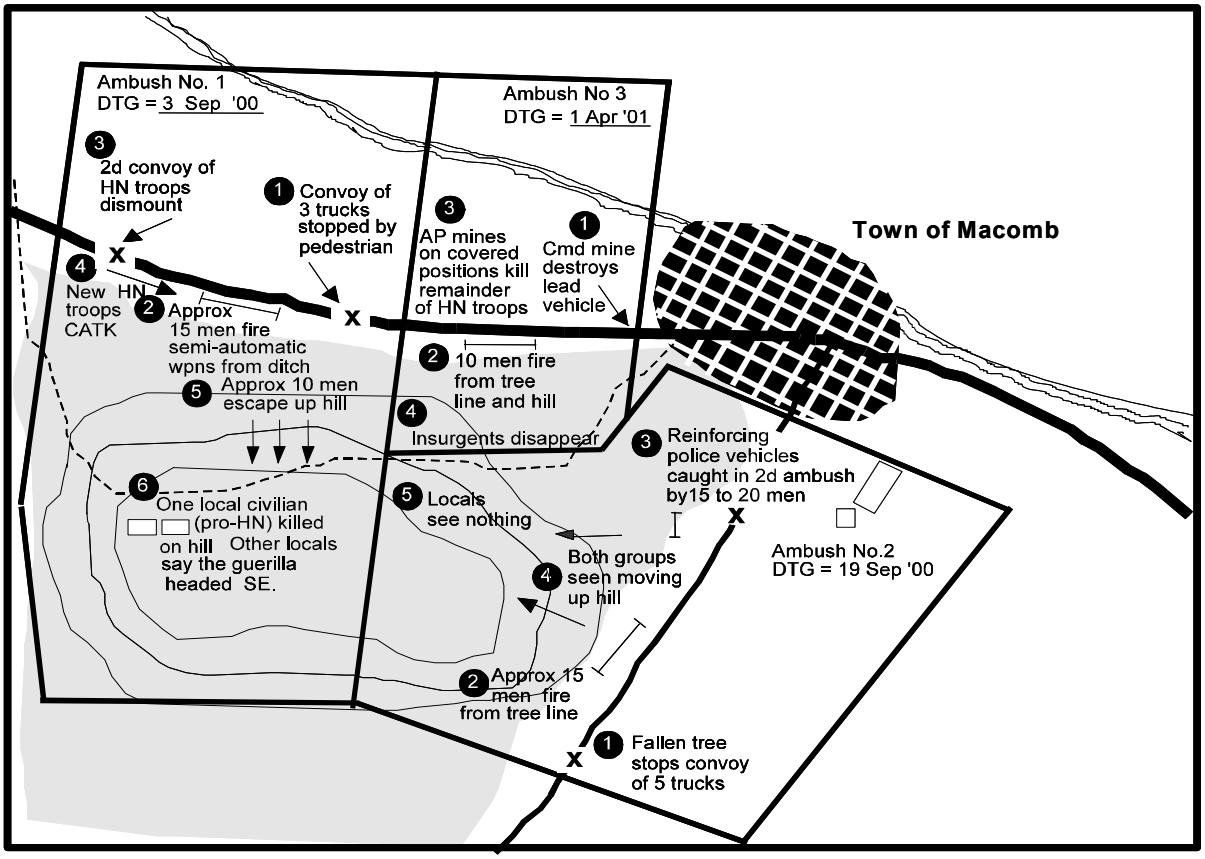


Figure 12-5. Coordinates Register.

Pattern Analysis Plot Sheet

12-42. The analyst uses a pattern analysis plot sheet to focus on the time and date of each serious incident that takes place within the AO (Figure 12-6) The rings depict days of the month; the segments depict the hours of the day As shown in the sheet's legend, the event itself is identified by using an alphanumeric designation and directly corresponds to the legend used on the coordinates register. Another type of the pattern analysis plot sheet helps distinguish patterns in activities that are tied to particular days, dates, or times. When used in conjunction with the coordinates register and any doctrinal templates, a pattern analysis plot sheet supplies the bulk of the data needed to complete an event template.

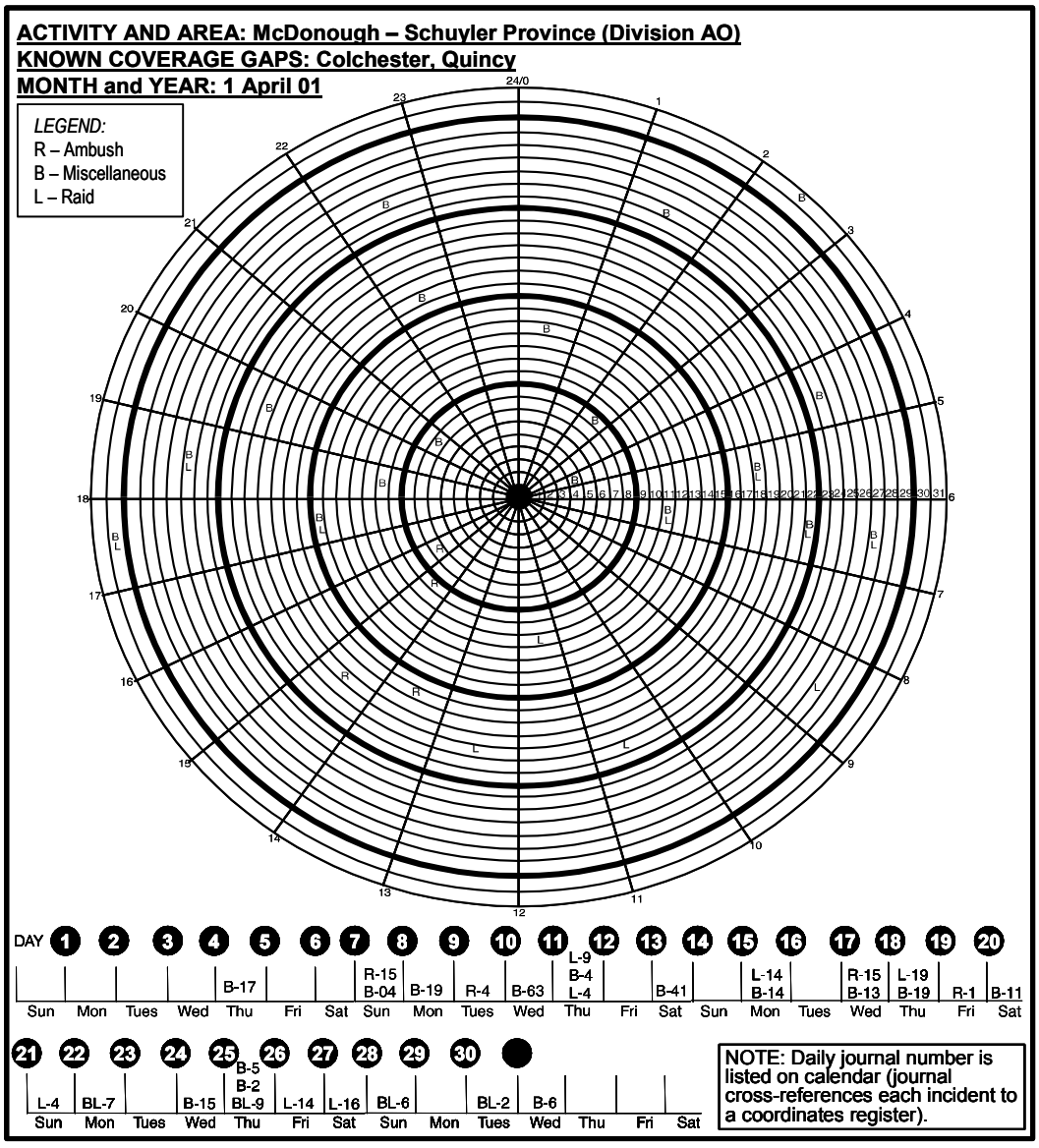


Figure 12-6. Pattern Analysis Plot Sheet.

OB Factors

12-43. A final analytical tool is OB. The OB does not predict enemy intentions or probable COAs but is a means of cataloging intelligence data that qualifies and quantifies certain aspects of threat units. The analyst uses nine factors shown in Table 12-1 to focus the analysis. These help the analyst determine threat capabilities, vulnerabilities, and COAs. Although the situation may dictate that one or more of the factors are given a higher priority, generally speaking, they are all of equal importance. The OB framework, while initially developed to support force-on-force offensive and defensive operations, is easily adapted to support stability and reconstruction operations and to depict "unconventional" forces or even civilian organizations.

Table 12-1. Order of Battle Factors.

Factor	Component
Composition	• Unit identification • Organization
Disposition	• Geographical Location • Tactical Deployment • Movements
Strength	• Personnel • Weapons and Equipment • Types of Units
Tactics	• Tactical Doctrine • Special Operations
Training	• Individual • Unit • Specialized
Logistics	• Systems • Status • Funding
Combat Effectiveness	• Combat Experience • Morale • Tactics • Logistics
Electronic Technical Data/Emitter Nomenclature	• Emitter Type • Mode of Emission • Frequency Range • Location Accuracy for Direction Finding • Associated Use (Units or Weapons)
Miscellaneous	• Personalities/Leadership • Unit History • Uniforms and Insignia • Code Names and Numbers

12-44. The OB is based on the premise that there are certain constants to any group activity. All groups whether they are conventional military forces, insurgent groups, or civilian organizations must have an organizational structure (composition). This structure may not be easily discernable but it will exist. Likewise, any organization has a location or locations in which it operates, personnel and equipment numbers, a system for training, getting supplies, judging efficiency and effectiveness of its operations, communi-

cating, and taking care of other intangibles such as morale. The OB gives the analyst a framework to organize information. The analyst adapts the topic headings to match the particular environment.

HUMINT SOURCE SELECTION

12-45. HUMINT source selection involves identifying, researching, and actively locating a specific group, organization, or individual for the purpose of collecting information in response to intelligence requirements. The HUMINT source selection process includes the C/J/G/S2X, the HOC, the HAT, the OMT, and the HCT. The source selection process allows the HUMINT team leader to identify the most likely source of information, eliminating the uncertainty of the access and placement of sources. Source selection also helps optimize the HUMINT collection effort. Any individual, group, organization, or agency that can be approached for information regarding intelligence requirements is a potential source. Sources are chosen according to their reliability, level of cooperation, and placement and access. Selection is particularly important in stability and reconstruction operations where the HUMINT collectors have access to a large potential source pool. Source selection establishes which current sources can best answer requirements and establishes source profiles to support the screening and selection of new sources.

ESTABLISH DATABASES AND TARGET FOLDERS

12-46. The establishment of local databases, target folders, and personality files is normally the responsibility of the OMT. This is done in coordination with the supporting ACE or analysis control team (ACT). Databases are required to manage the information. By using databases one can identify gaps in the information. The HCT and OMT access higher databases through intelligence reach to share and deconflict locally maintained data with higher level databases. Local databases can be created and used to help track source production, knowledge, reliability, and accuracy, and they simplify cross-reference data that is of primarily local interest. It is ideal to review and update databases at least weekly.

12-47. A target folder provides the collector with up-to-date intelligence information about details of the target. It includes anything of HUMINT value including biographies, descriptions, photographs, and previous information reports. The information can be gained from the ACE or ACT, past reports, INTSUMs, and databases; it can then be organized into easily accessible automated folders. Information on people is categorized and recorded in a personality file. The file serves as reference material for collectors. Information on key military and civilian figures can be of significant value when establishing unit or group identification, tactics, and combat effectiveness. The file should not only provide information on cultural, religious, tribal, political, military, criminal, and governmental background but also contain specific personalities for collectors to focus their collection effort on. This allows the collectors to concentrate on mission planning and to conduct their mission rather than to research information.

COMPARE SOURCE LIST WITH REQUIREMENTS

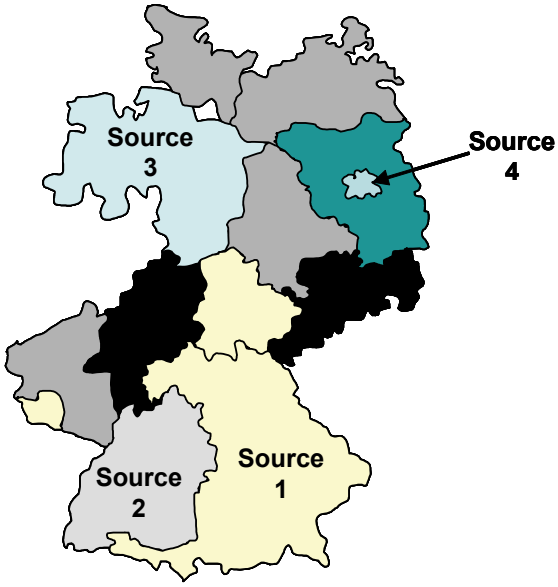
12-48. As target folders are compiled, a list of high-value sources will emerge. It is a simple matter to compare the source list with the PIRs and/or SIRs. This will lead to efficient and time-saving missions for the collectors. Rather than spend time meeting with sources who may have information concerning certain subjects, the HCT is able to tackle the collection process with foresight. Upon receipt of the mission, the OMT conducts mission analysis to determine the optimal way to meet mission requirements. Proper mission analysis enables the collector to properly focus his assets (sources) to gain the maximum amount of intelligence from those sources most likely to possess the highest quality information.

12-49. The following products, which will focus the HCT's collection efforts, can be prepared in conjunction with the ACE and joint intelligence centers:

- Time event charts.
- Source coverage overlays or matrices (see Figure 12-7).
- Link analysis diagrams.
- HUMINT portions of OPORDs and situation reports.

12-50. The source coverage overlay or matrix helps tie in the source coverage to the requirements. It also helps identify gaps in collection. A collection matrix serves the same purpose. It supplies a quick reference when answering intelligence requirements. The matrices must cover both the geographical area and the placement and access of the source. A demographic overlay helps to identify ethnic groups in an area and to track events and patterns based on religious or ethnic differences. The overlay and matrix are examples of how source coverage can be tied to intelligence requirements.

12-51. Source profiles are vital to screening sources for HUMINT collection operations and to identifying personnel that might be of interest to other agencies such as CI and TECHINT. As the situation changes, the HCT might be tasked with new collection requirements that cannot be answered by the current sources. The HCT is constantly looking for new and better sources. When presented with new requirements, the OMT develops a source profile of the type of individual that would most likely be able to provide the information required. This profiling can include placement, access, age, ethnic type, gender, location, occupation, and military specialty. The OMT first searches through existing local databases to try to get a source match. If not, it passes the profile to the HCTs along with the requirements to facilitate their screening of potential sources.



		L AREA	PIR 1	PIR 2	PIR 3	PIR 4	PIR 5	PIR 6
0001	Police	Village 1	X					
0002	Municipal Government	Village 1 and National		X	X			
0003	Political Party 1	City 1 and 2			X		X	
0004	Political Party 2	City 3 and 4		X		X		X

Figure 12-7. Example of a Source Coverage Overlay or Matrix.

This page intentionally left blank.

Chapter 13

Automation and Communication

13-1. Modern automation and communications systems are vital to HUMINT collection. Real-time collaboration, detailed operational planning and ISR integration, as well as enhanced collection and source exploitation tools, must support team efforts. Emerging technology continues to allow the entire HUMINT collection system to operate more effectively. Commanders must be prepared to supply their HUMINT collection assets with the best possible technology not only to enhance collection but also to optimize the survivability of the collectors. (See Appendix L.) Commanders may not be able to rely solely on standard military equipment but must be prepared to bridge the inevitable technological development gap through the identification and adaptation of commercially available products and technologies. For specific system components and capabilities, see ST 2-50.

AUTOMATION

13-2. HUMINT automation uses common hardware and software solutions with a flexible interactive user interface to provide standardization of equipment and processes across all operational environments and conditions. HUMINT automation must be deployable and scalable to fit the mission or force package. System components must be capable of intelligence reach to support forward-deployed elements. HUMINT automation allows integration and interaction with existing intelligence operations, HUMINT operational systems, and databases. This integration allows operations personnel and analysts to develop plans and levy collection and operational requirements, as well as to manage, control, analyze, and report the information collected. HUMINT automation—

- Provides connectivity and reach capability between all echelons of HUMINT activity.
- Receives higher echelon requirements and transmits requests for information.
- Converts HUMINT reporting into formats for JTF or coalition task force (CTF), theater, or national consumption.
- Pushes requirements, requests, and plans for HUMINT operations in theater as required.
- Maintains the central HUMINT database for the theater or AO.
- Leverages JTF or CTF, theater, and national level requirements and products for strategic, operational, and tactical HUMINT assets in theater.

- Enables HUMINT to provide accurate and timely correlated information to supported commanders through established reporting channels.
- Provides automated analysis tools.

13-3. Systems such as Trusted Workstation (TWS) can convert HUMINT reporting into formats for JTF or CTF, theater, or national consumption. TWS can also connect between the SIPRNET and any lower level networks, such as coalition, multinational, or NATO, or unclassified networks such as NIPRNET or the Internet.

COLLECTION SUPPORT AUTOMATION REQUIREMENTS

BIOMETRICS

13-4. Biometrics is the study of measurable biological characteristics. In HUMINT collection, biometric devices, usually computer based, enable the HUMINT collector to use biological data to support the collection and analysis effort. Biometrics can also be used in non-HUMINT efforts to collect and maintain evidence for criminal prosecution. The two major types of biometric data that are useful to the HUMINT collector are identification data and data that indicate source truthfulness. Identification devices use biological information such as fingerprints, voiceprints, facial scans, and retinal scans to match an individual to a source database. They can verify the identity of a specific individual from the target population during screening.

13-5. HCTs may be equipped with portable equipment for collecting, storing, analyzing, forwarding, and retrieving biometric information. The BAT is able to identify personnel by using identifying characteristics of their irises, fingerprints, or facial photograph. The structured query language (SQL) server-based database links identifying characteristics with all previous reports related to the person. Once a person's identifying characteristics are entered into the database, if that person is again detained and scanned, the system has a probability of identifying them that approaches 100 percent. This ability is especially useful for determining if a source is providing the same information to multiple collectors; thereby avoiding false confirmation of information. HUMINT collectors primarily use BAT during screening operations at all echelons; from checkpoint screening, to screening at a DCP, to screening at a JIDC. MPs use the Detainee Reporting System (DRS) during in-processing at internment facilities. The DRS records data for detainee processing and tracking and is intended to interact with the BAT system to avoid duplication of effort.

13-6. The hardware that makes up the system, which is given to MI teams, consists of a commercial off-the-shelf (COTS) semi-hardened laptop computer running an operating system with a graphical user interface. It has a camera and an iris scanner, each of which is portable and can be used independent of the computer to collect and temporarily store information. The system also includes a fingerprint scanner that conforms to FBI requirements for admissible evidence. The fingerprint scanner must be attached to the computer during use.

13-7. Biometric devices such as voice stress analyzer and polygraph support the determination of the truthfulness of a source. The polygraph is of limited usefulness in general HUMINT collection due to the level of expertise needed to operate it and the lack of general availability of the device to the field. As devices are developed that can remotely collect and report information to the HUMINT collector on subtle changes in the source's respiration, heartbeat, perspiration, and eye movement that can be indicators of deceit, they can be used to support HUMINT collection.

MACHINE TRANSLATION AND INTERPRETATION

13-8. Understanding oral and written communication in a foreign language is often the center of effective HUMINT collection operations. The optimal solution is to have an individual who is a trained collector of native proficiency, totally versed in the local situation and US requirements, with the requisite security clearance, who is capable of reporting accurately in English. Commanders' access to such individuals is usually problematic. This requirement is met through a combination of MI linguists, contractors, native speakers within the DOD system, and locally hired civilian translators. Difficulties arise if the proficiency levels of MI linguists are not up to mission requirements, or if the linguists do not possess the proper language for the theater of operation. Using locally hired translators raises security problems. In light of these conditions, an increasingly viable solution for the commander is the use of machine translation devices to meet some of these requirements.

13-9. Voice and text translation machines or software are critical in augmenting available linguists. This includes natural language processing, artificial intelligence, and optical character recognition (OCR) capabilities. The basic application of machine translation, such as speech recognition and OCRs, dramatically increases the speed of processing information. Software programs are becoming widely available that allow a non-linguist to determine the intelligence significance of a foreign document, aid linguists with laborious tasks, and add consistency to human translation.

13-10. Machine interpretation is the use of a machine to interpret the spoken word between the HUMINT collectors and another individual speaking a foreign language. Linguists are in high demand during operations and usually limited in number. As machine interpretation devices that address this problem become available to the field, they will improve the communication ability of non-linguists.

ANALYTICAL AUTOMATION REQUIREMENTS

13-11. The requirement for a robust HUMINT single-discipline analytical capability extends through all echelons from national level to the OMTs. Communication between HUMINT analysts at the operational level and analysts at the staff level may best be accomplished through a web-based communication capability. Web-based visual analytical tools allow maximum analyst participation in the development of products geared to mission planning, targeting, and information analysis at all echelons.

Analytical products must be responsive to the special needs of a specific collection operation, project, or element.

13-12. HUMINT collectors run operations in terrain made up of persons, organizations, and installations of interest. Intelligence analysis support determines the specific terrain in each team area and how it differs from one team's named area of interest (NAI) to another. Specific products include studies on nominated targets (persons, organizations, and installations) and trends based on HUMINT reporting, as appropriate, and visual analysis products (time event charts, matrices, link analysis diagrams, and organizational diagrams).

AUTOMATED ANALYSIS TOOLS

13-13. Automation of HUMINT analytical tools such as time event charts, association matrices, activity matrices, and link analysis diagrams dramatically increase predictive analysis capability. Automation saves time and permits access to more complete information thus producing a more accurate, timely product. Automated analysis techniques, aided by computerized virtual-viewing programs, allow the analyst better battlefield visualization. Automated analysis, linked to data and databases, includes artificial intelligence programs. These programs assist the analyst in developing predictions and identifying information gaps to support targeting and collection. Automation and web-based tools allow the analyst to—

- Track and cross-cue HUMINT reports.
- Incorporate data extraction technology, retrieval, automated data organization, content analysis, and visualization.
- Share analytical conclusions with HUMINT teams and other analysts in real time.
- Apply multidimensional technologies, content analysis techniques, and web-based collaborations.
- Display analytical results and view HUMINT operations in real time.
- Share resources such as models, queries, visualizations, map overlays, geospatial images, and tool outputs through a common interface.
- Apply clustering (a nonlinear search that compiles the results based on search parameters) and rapid spatial graphical and geographic visualization tools to determine the meaning of large informational streams.
- Rapidly discover links, patterns, relationships, and trends in text to use in predictive analysis.
- Capture analytical conclusions and automatically transfer to intelligence databases and systems.

SEARCH ENGINES

13-14. Search engines provide access to previously collected or known information facilitating the development of comprehensive analytical and intelligence products and avoiding unnecessary collection tasking redundancy. A tool set for data visualization, search, and discovery is required, which is embedded with several software programs for manipulating data from multiple databases. The types of modules in visualization packages should include search engines and knowledge discovery (semantic clustering) for unformatted data, applications for extracting and organizing formatted data, and data labeling. The package should also include a model building tool to enable users to make their archives more efficient with respect to search, retrieval, and compatibility to other applications as well as archiving and maintenance tools to support what will eventually become a large data warehouse. Search engines should be—

- Multilingual and able to query multiple classified and unclassified databases.
- Capable of developing, querying, and manipulating stored information.

WEB-BASED REPORTING AND PORTALS

13-15. Web-based reporting employs current Internet portal technology. The web-based portal is an efficient and effective means of developing a repository of HUMINT information. It employs an interactive graphic interface using client browser technology, search engines, hyperlinks, and intelligent software agents for searching, finding, viewing, and maintaining databases and supporting HUMINT work, data, and information flows. It supports collaborative analysis at multiple echelons through connectivity on the SIPRNET. The following pertains to web-based reporting:

- Web-based databases work with any computer hardware, operating system, or software and can be made accessible through web portals.
- Firewalls and information access are controlled at each level with an approving systems administrator at each level conducting quality control through release authority procedures.
- Graphic user interface uses standard Army and DOD report formats.
- Graphic user interface walks the user through a critical task and is able to identify Army and DOD reports as required. Reports must be Army and DOD platform compatible and transferable through and to their respective systems.
- Multimedia supports applications for attaching, associating, and hyperlinking video, still photographs, voice, scanned objects, graphics, and maps to records and files.

13-16. Web-based reporting and web pages developed for specific products allow the user to—

- Leverage their effort and expertise against all requirements, not just the ones that must be met immediately.

- Identify timely intelligence gaps and the leads to fill those gaps.
- Ensure immediate analytical feedback on collector reports to—
  - Post questions directly to a web page to enable all HCTs to answer or be cued to the specific request.
  - Identify or request clarification on questionable data for quality control.
- Fuse HUMINT information and all-source information as required.
- Focus collection teams supporting maneuver commanders' requirements more effectively.
- Immediately extract information for crisis reaction.

13-17. If HCTs use web portals to submit reports directly to theater level, they must also send the reports through their OMT for submission to the 2X. Failure to do so may deny the 2X the ability to deconflict and cross-reference reports. HUMINT collectors must ensure that they follow the theater-specific methodology for access to the theater web portal.

DATABASES

13-18. Without databases, information is difficult or impossible to retrieve quickly, especially under adverse conditions. Databases allow access to data in a distributed environment and support many complex HUMINT functions and requirements, including—

- Mission deconfliction.
- RM.
- RFIs.
- HUMINT analysis.
- Summary, report, and assessment preparation.
- Threat and friendly situation tracking.
- Targeting.

13-19. Databases interact with other tools to support predictive analysis, prepare graphic analytical products, and provide situational understanding down to the HCT. These databases—

- Support time event charts, association matrices, link analysis, and other analysis tools.
- Require a designated systems administrator at each. To ensure a high degree of integrity, discrepancies must be verified for accuracy.
- Allow operators, managers, and analysts to—
  - Compartment (protect) source-sensitive operational database segments, files, records, and fields.
  - Create, update, and maintain databases from locally generated information.
  - Import complete or partial databases from larger or peer databases.
  - Export complete or partial databases to peer or larger databases.

  - Share data and databases between peers, subordinates, or higher with appropriate access authorization.
- Provide systematic processing and automated parsing using standardized forms in intelligence operations, which are automatically parsed into appropriate databases for information storing, sharing, retrieval, and analysis.
- Allow query functions for decisionmaking as well as operational and analytical support.
- Provide analytical programs able to correlate data that facilitate information retrieval from any data repository.
- Incorporate information retrieval functions such as browsing (that is, point and click), key word searching, concepts, and similar functions.
- Support a suite of specialized decision support software (DSS)—a set of tools which supports HUMINT source administration, analysis, and risk management decisions. DSS tools should produce a set of HUMINT reports specifically tailored to the HUMINT decisionmaking, analysis, and assessment process.

13-20. HARMONY is the national intelligence database for foreign DOCEX and translations management. HARMONY is the single, comprehensive bibliographic reference for all available primary source foreign technical and military documents and their translations. This single database concept eliminates duplicate collection, translation, and reporting of primary source foreign technical and military documents and greatly streamlines the process of providing exploited documents to consumers. The HARMONY database application uses the DOD Information Infrastructure (DII) Common Operating Environment (COE) guidance. The HARMONY database is web-enabled and can be readily accessed, easily used, and responsive to the needs of analysts and other consumers within the US Government community.

AUTOMATION SYSTEMS

13-21. The HUMINT collection automation systems are normally shared systems used by both the HUMINT and CI communities. They must have connectivity with lateral units as well as higher and subordinate elements.

C/J/G/S2X, HOC, AND HAT AUTOMATION REQUIREMENTS

13-22. The HUMINT staff elements need to receive input from the OMTs and HCTs as well as input from higher and lateral echelons. They must be able to conduct HUMINT planning, RM, and report dissemination. They must transmit technical support information, interface with ACE and automated analysis systems, manipulate HUMINT databases, conduct reach, and have access to HUMINT analytical tools.

OMT AND COLLECTION TEAM LEADER REQUIREMENTS

13-23. The OMT must be able to track teams and team members; receive and transmit data including graphic data to and from higher, lateral, and lower HUMINT elements; create, receive, edit, and transmit reports; conduct single-discipline HUMINT analysis; receive and transmit technical support information and tasking information; conduct reach; and conduct mission planning.

INDIVIDUAL COLLECTOR AUTOMATION REQUIREMENTS

13-24. The key to effective HUMINT collection is unimpeded communication between the collector and the source of information. Any technological support to HUMINT collection must be as unobtrusive as possible to minimize the intimidation factor when dealing with human sources. The individual collector must be able to—

- Record (both video and voice) conversations with sources.
- Scan, translate, and transmit documents and photographs.
- Instantaneously locate themselves in both rural and urban environments.
- Immediately access local, theater, and even national level databases.
- Communicate instantaneously with other team elements.

HUMINT AND CI WORKSTATION REQUIREMENTS

13-25. The CI and HUMINT teams have organic computer and data processing equipment. These workstations provide HUMINT and CI teams with both productivity and management and analysis tools. They also provide SIPRNET connectivity and processing capability to identify requirements and facilitate reporting into other DOD systems as required. The HUMINT and CI workstation is able to use standard Army, DOD, and HUMINT and CI reporting programs, standard symbols, programs to produce map overlays, and map plotting software; all of which are included.

13-26. Teams use workstations to—

- Provide quality control and dissemination of reports from the subordinate HCTs.
- Direct activities of subordinate HCTs and provide management to them.
- Perform single-discipline HUMINT analysis for the supported commander.
- Transmit intelligence and administrative reports in NRT to higher headquarters.
- Receive tasking and administrative reports from higher headquarters and distribute to HCTs as required.
- Consolidate local databases and provide database input to higher headquarters.
- Receive database and digital information from higher headquarters and pass to lower and vice versa.

COMMUNICATIONS

13-27. Successful HUMINT operations must be supported by multi-echelon technical control and a communications system that provides internal team communications, links HCTs to OMTs, and links OMTs to higher headquarters, analytical elements, and theater and national agencies.

COMMUNICATION ARCHITECTURE

13-28. The HUMINT collection architecture requires operation on several communications and processing nets. These nets provide the framework needed to coordinate the tasking, reporting, C2, and service support of HUMINT collection units spread across the width and depth of the battlefield. Under most operational scenarios, HCTs are not stationary. They are constantly moving throughout their supported command's AO and are able to communicate on the move. They cannot rely on fixed communications nodes for support. Communications redundancy ensures the loss of any one system does not severely disrupt HUMINT operations. HCTs and OMTs normally operate at the collateral security level to ensure the timely dissemination of combat information and targeting data to organizations operating outside MI channels. The C/J/G/S2X normally requires access to Top Secret (SCI) communications capabilities to maintain coordination with national level agencies.

13-29. The HUMINT collection assets use three basic communications nets: the operations and intelligence (O/I) net, a command net, and a HUMINT-specific technical net. Dependent on their mission and battlefield location, the HCTs may also need to monitor the fire support element (FSE), aviation, or air defense artillery (ADA) communications nets.

- The O/I net links the collectors and producers of intelligence to the consumers of the intelligence information. It is used to pass information of immediate value to the affected unit and to analytical elements at the supported unit.
- The command nets exist at every echelon of command. They link the superior headquarters with its subordinate elements. Normally a unit will operate on two command nets; the one that links that unit to its higher headquarters and the one that links that unit to its subordinate elements. HUMINT elements will also use their unit's command net to coordinate logistic and administrative support.
- The technical nets link the control team to all of their subordinate collection teams and to the centers or organizations that provide the databases and technical guidance necessary for single-discipline collection and analysis. For example, the technical net would connect HCTs through their control teams to the S2X and higher echelon HUMINT analysis organizations.

MOBILE COMMUNICATIONS REQUIREMENTS

13-30. HUMINT mobile communications requirements augment the network connectivity that elements should have when at a base camp or facility; they vary with each element's mission and location as follows:

- Individual HUMINT collectors must maintain communications capability with the other team members and the team leader while dismounted. HUMINT collectors, especially when supporting offensive and defensive operations, may be deployed as individuals. They need to maintain contact with their team leader for technical and operational support.
- The HCT may operate anywhere within the supported unit's AO. They may operate mounted or dismounted. If supporting airmobile, airborne, amphibious, or other mobile operations, they may not have access to their vehicle-mounted communications systems for the critical early stages of these operations. They receive and report operational and technical information, as well as report intelligence information to the OMT using their unit's command net. They monitor their superior unit's O/I net. If in DS to a maneuver element, they also monitor the command net of the unit they are supporting.
- OMTs normally operate on the superior unit O/I net, their unit C2 net, and the HUMINT technical net. If the OMT is in DS, it must also operate on the C2 net of the supported unit.
- The C/J/G/S2X operates on the C2 net, monitors the O/I net, and controls its echelon HUMINT technical net. The 2X needs secure (SCI) communications capability to coordinate operations and pass data between themselves and higher HUMINT organizations.

Appendix A

Geneva Conventions

SECTION I. GENEVA CONVENTIONS RELATIVE TO THE TREATMENT OF PRISONERS OF WAR (THIRD GENEVA CONVENTION)

The articles in this section are extracted from the Geneva Convention Relative to the Treatment of Prisoners of War, 12 August 1949.

PART I GENERAL PROVISIONS

ARTICLE 1

The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances.

ARTICLE 2

In addition to the provisions which shall be implemented in peace time, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.

Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof.

ARTICLE 3

In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each party to the conflict shall be bound to apply, as a minimum, the following provisions:

1. Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, color, religion or faith, sex, birth or wealth, or any other similar criteria. To this end the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:

(a) Violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;

(b) Taking of hostages;

(c) Outrages upon personal dignity, in particular, humiliating and degrading treatment;

(d) The passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples.

2. The wounded and sick shall be collected and cared for.

An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict.

The Parties to the conflict should further endeavor to bring into force, by means of special agreements, all or part of the other provisions of the present Convention.

The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.

ARTICLE 4

A. Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy:

1. Members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces.

2. Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfill the following conditions:

(a) That of being commanded by a person responsible for his subordinates;

(b) That of having a fixed distinctive sign recognizable at a distance;

(c) That of carrying arms openly;

(d) That of conducting their operations in accordance with the laws and customs of war.

3. Members of regular armed forces who profess allegiance to a government or an authority not recognized by the Detaining Power.

4. Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labor units or of services responsible for the welfare of the armed forces, provided that they have received authorization from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model.

5. Members of crews, including masters, pilots and apprentices, of the merchant marine and the crews of civil aircraft of the Parties to the conflict, who do not benefit by more favorable treatment under any other provisions of international law.

6. Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.

B. The following shall likewise be treated as prisoners of war under the present Convention:

1. Persons belonging, or having belonged, to the armed forces of the occupied country, if the occupying Power considers it necessary by reason of such allegiance to intern them, even though it has originally liberated them while hostilities were going on outside the territory it occupies, in particular where such persons have made an unsuccessful attempt to rejoin the armed forces to which they belong and which are engaged in combat, or where they fail to comply with a summons made to them with a view to internment.

2. The persons belonging to one of the categories enumerated in the present Article, who have been received by neutral or non-belligerent Powers on their territory and whom these Powers are required to intern under international law, without prejudice to any more favorable treatment which these Powers may choose to give and with the exception of Articles 8, 10, 15, 30, fifth paragraph, 58-67, 92, 126 and, where diplomatic relations exist between the Parties to the conflict and the neutral or non-belligerent Power concerned, those Articles concerning the Protecting Power. Where such diplomatic relations exist, the Parties to a conflict on whom these persons depend shall be allowed to perform towards them the functions of a Protecting Power as provided in the present Convention, without prejudice to the functions which these Parties normally exercise in conformity with diplomatic and consular usage and treaties.

C. This Article shall in no way affect the status of medical personnel and chaplains as provided for in Article 33 of the present Convention.

ARTICLE 5

The present Convention shall apply to the persons referred to in Article 4 from the time they fall into the power of the enemy and until their final release and repatriation.

Should any doubt arise as to whether persons, having committed a belligerent act and having fallen into the hands of the enemy, belong to any of the categories enumerated in Article 4, such persons shall enjoy the protection of the present Convention until such time as their status has been determined by a competent tribunal.

ARTICLE 6

In addition to the agreements expressly provided for in Articles 10, 23, 28, 33, 60, 65, 66, 67, 72, 73, 75, 109, 110, 118, 119, 122 and 132, the High Contracting Parties may conclude other special agreements for all matters concerning which they may deem it suitable to make separate provision. No special agreement shall adversely affect the situation of prisoners of war, as defined by the present Convention, nor restrict the rights which it confers upon them.

Prisoners of war shall continue to have the benefit of such agreements as long as the Convention is applicable to them, except where express provisions to the contrary are contained in the aforesaid or in subsequent agreements, or where more favorable measures have been taken with regard to them by one or other of the Parties to the conflict.

ARTICLE 7

Prisoners of war may in no circumstances renounce in part or in entirety the rights secured to them by the present Convention, and by the special agreements referred to in the foregoing Article, if such there be.

ARTICLE 8

The present Convention shall be applied with the cooperation and under the scrutiny of the Protecting Powers whose duty it is to safeguard the interests of the Parties to the conflict. For this purpose, the Protecting Powers may appoint, apart from their diplomatic or consular staff, delegates from amongst their own nationals or the nationals of other neutral Powers. The said delegates shall be subject to the approval of the Power with which they are to carry out their duties.

The Parties to the conflict shall facilitate to the greatest extent possible the task of the representatives or delegates of the Protecting Powers.

The representatives or delegates of the Protecting Powers shall not in any case exceed their mission under the present Convention. They shall, in particular, take account of the imperative necessities of security of the State wherein they carry out their duties.

ARTICLE 9

The provisions of the present Convention constitute no obstacle to the humanitarian activities which the International Committee of the Red Cross or any other impartial humanitarian organization may, subject to the consent of the Parties to the conflict concerned, undertake for the protection of prisoners of war and for their relief.

ARTICLE 10

The High Contracting Parties may at any time agree to entrust to an organization which offers all guarantees of impartiality and efficacy the duties incumbent on the Protecting Powers by virtue of the present Convention.

When prisoners of war do not benefit or cease to benefit, no matter for what reason, by the activities of a Protecting Power or of an organization provided for in the first paragraph above, the Detaining Power shall request a neutral State, or such an organization, to undertake the functions performed under the present Convention by a Protecting Power designated by the Parties to a conflict.

If protection cannot be arranged accordingly, the Detaining Power shall request or shall accept, subject to the provisions of this Article, the offer of the services of a humanitarian organization, such as the International Committee of the Red Cross, to assume the humanitarian functions performed by Protecting Powers under the present Convention.

Any neutral Power or any organization invited by the Power concerned or offering itself for these purposes, shall be required to act with a sense of responsibility towards the Party to the conflict on which persons protected by the present Convention depend, and shall be required to furnish sufficient assurances that it is in a position to undertake the appropriate functions and to discharge them impartially.

No derogation from the preceding provisions shall be made by special agreements between Powers one of which is restricted, even temporarily, in its freedom to negotiate with the other Power or its allies by reason of military events, more particularly where the whole, or a substantial part, of the territory of the said Power is occupied.

Whenever in the present Convention mention is made of a Protecting Power, such mention applies to substitute organizations in the sense of the present Article.

ARTICLE 11

In cases where they deem it advisable in the interest of protected persons, particularly in cases of disagreement between the Parties to the conflict as to the application or interpretation of the provisions of the present Convention, the Protecting Powers shall lend their good offices with a view to settling the disagreement.

For this purpose, each propose to the Parties of the Protecting Powers may, either at the invitation of one Party or on its own initiative, to the conflict a meeting of their representatives, and in particular of the authorities responsible for prisoners of war, possibly on neutral territory suitably chosen. The Parties to the conflict shall be bound to give effect to the proposals made to them for this purpose. The Protecting Powers may, if necessary, propose for approval by the Parties to the conflict a person belonging to a neutral Power, or delegated by the International Committee of the Red Cross, who shall be invited to take part in such a meeting.

PART II GENERAL PROTECTION OF PRISONERS OF WAR

ARTICLE 12

Prisoners of war are in the hands of the enemy Power, but not of the individuals or military units who have captured them. Irrespective of the individual responsibilities that may exist, the Detaining Power is responsible for the treatment given them.

Prisoners of war may only be transferred by the Detaining Power to a Power which is a party to the Convention and after the Detaining Power has satisfied itself of the willingness and ability of such transferee Power to apply the Convention. When prisoners of war are transferred under such circumstances, responsibility for the application of the Convention rests on the Power accepting them while they are in its custody.

Nevertheless if that Power fails to carry out the provisions of the Convention in any important respect, the Power by whom the prisoners of war were transferred shall, upon being notified by the PROTECTING Power, take effective measures to correct the situation or shall request the return of the prisoners of war. Such requests must be complied with.

ARTICLE 13

Prisoners of war must at all times be humanely treated. Any unlawful act or omission by the Detaining Power causing death or seriously endangering the health of a prisoner of war in its custody is prohibited, and will be regarded as a serious breach of the present Convention. In particular, no prisoner of war may be subjected to physical mutilation or to medical or scientific experiments of any kind which are not justified by the medical, dental or hospital treatment of the prisoner concerned and carried out in his interest.

Likewise, prisoners of war must at all times be protected, particularly against acts of violence or intimidation and against insults and public curiosity.

Measures of reprisal against prisoners of war are prohibited.

ARTICLE 14

Prisoners of war are entitled in all circumstances to respect for their persons and their honor. Women shall be treated with all the regard due to their sex and shall in all cases benefit by treatment as favorable as that granted to men. Prisoners of war shall retain the full civil capacity which they enjoyed at the time of their capture. The Detaining Power may not restrict the exercise, either within or without its own territory, of the rights such capacity confers except in so far as the captivity requires.

ARTICLE 15

The Power detaining prisoners of war shall be bound to provide free of charge for their maintenance and for the medical attention required by their state of health.

ARTICLE 16

Taking into consideration the provisions of the present Convention relating to rank and sex, and subject to any privileged treatment which may be accorded to them by reason of their state of health, age or professional qualifications, all prisoners of war shall be treated alike by the Detaining Power, without any adverse distinction based on race, nationality, religious belief or political opinions, or any other distinction founded on similar criteria.

PART III CAPTIVITY

SECTION I BEGINNING OF CAPTIVITY

ARTICLE 17

Every prisoner of war, when questioned on the subject, is bound to give only his surname, first names and rank, date of birth, and army, regimental, personal or serial number, or failing this, equivalent information. If he willfully infringes this rule, he may render himself liable to a restriction of the privileges accorded to his rank or status.

Each Party to a conflict is required to furnish the persons under its jurisdiction who are liable to become prisoners of war, with an identity card showing the owner's surname, first names, rank, army, regimental, personal or serial number or equivalent information, and date of birth. The

identity card may, furthermore, bear the signature or the fingerprints, or both, of the owner, and may bear, as well, any other information the Party to the conflict may wish to add concerning persons belonging to its armed forces. As far as possible the card shall measure 6.5 x 10 cm. and shall be issued in duplicate. The identity card shall be shown by the prisoner of war upon demand, but may in no case be taken away from him.

No physical or mental torture, nor any other form of coercion, may be inflicted on prisoners of war to secure from them information of any kind whatever. Prisoners of war who refuse to answer may not be threatened, insulted, or exposed to any unpleasant or disadvantageous treatment of any kind.

Prisoners of war who, owing to their physical or mental condition, are unable to state their identity, shall be handed over to the medical service. The identity of such prisoners shall be established by all possible means, subject to the provisions of the preceding paragraph.

The questioning of prisoners of war shall be carried out in a language which they understand.

ARTICLE 18

All effects and articles of personal use, except arms, horses, military equipment and military documents shall remain in the possession of prisoners of war, likewise their metal helmets and gas masks and like articles issued for personal protection. Effects and articles used for their clothing or feeding shall likewise remain in their possession, even if such effects and articles belong to their regulation military equipment.

At no time should prisoners of war be without identity documents. The Detaining Power shall supply such documents to prisoners of war who possess none.

Badges of rank and nationality, decorations and articles having above all a personal or sentimental value may not be taken from prisoners of war.

Sums of money carried by prisoners of war may not be taken away from them except by order of an officer, and after the amount and particulars of the owner have been recorded in a special register and an itemized receipt has been given, legibly inscribed with the name, rank and unit of the person issuing the said receipt. Sums in the currency of the Detaining Power, or which are changed into such currency at the prisoner's request, shall be placed to the credit of the prisoner's account as provided in Article 64.

The Detaining Power may withdraw articles of value from prisoners of war only for reasons of security; when such articles are withdrawn, the procedure laid down for sums of money impounded shall apply.

Such objects, likewise the sums taken away in any currency other than that of the Detaining Power and the conversion of which has not been asked for by the owners, shall be kept in the custody of the Detaining Power and shall be returned in their initial shape to prisoners of war at the end of their captivity.

ARTICLE 19

Prisoners of war shall be evacuated, as soon as possible after their capture, to camps situated in an area far enough from the combat zone for them to be out of danger.

Only those prisoners of war who, owing to wounds or sickness, would run greater risks by being evacuated than by remaining where they are, may be temporarily kept back in a danger zone.

Prisoners of war shall not be unnecessarily exposed to danger while awaiting evacuation from a fighting zone.

ARTICLE 20

The evacuation of prisoners of war shall always be effected humanely and in conditions similar to those for the forces of the Detaining Power in their changes of station.

The Detaining Power shall supply prisoners of war who are being evacuated with sufficient food and potable water, and with the necessary clothing and medical attention. The Detaining Power shall take all suitable precautions to ensure their safety during evacuation, and shall establish as soon as possible a list of the prisoners of war who are evacuated.

If prisoners of war must, during evacuation, pass through transit camps, their stay in such camps shall be as brief as possible.

SECTION II INTERNMENT OF PRISONERS OF WAR

CHAPTER I GENERAL OBSERVATIONS

ARTICLE 21

The Detaining Power may subject prisoners of war to internment. It may impose on them the obligation of not leaving, beyond certain limits, the camp where they are interned, or if the said camp is fenced in, of not going outside its perimeter. Subject to the provisions of the present Convention relative to penal and disciplinary sanctions, prisoners of war may not be held in close confinement except where necessary to safeguard their health and then only during the continuation of the circumstances which make such confinement necessary.

Prisoners of war may be partially or wholly released on parole or promise, in so far as is allowed by the laws of the Power on which they depend. Such measures shall be taken particularly in cases where this may contribute to the improvement of their state of health. No prisoner of war shall be compelled to accept liberty on parole or promise.

Upon the outbreak of hostilities, each Party to the conflict shall notify the adverse Party of the laws and regulations allowing or forbidding its own nationals to accept liberty on parole or promise. Prisoners of war who are paroled or who have given their promise in conformity with the laws and regulations so notified, are bound on their personal honor scrupulously to fulfil, both towards the Power on which they depend and towards the Power which has captured them, the engagements of their paroles or promises. In such cases, the Power on which they depend is bound neither to require nor to accept from them any service incompatible with the parole or promise given.

ARTICLE 22

Prisoners of war may be interned only in premises located on land and affording every guarantee of hygiene and healthfulness. Except in particular cases which are justified by the interest of the prisoners themselves, they shall not be interned in penitentiaries.

Prisoners of war interned in unhealthy areas, or where the climate is injurious for them, shall be removed as soon as possible to a more favorable climate.

The Detaining Power shall assemble prisoners of war in camps or camp compounds according to their nationality, language and customs, provided that such prisoners shall not be separated from prisoners of war belonging to the armed forces with which they were serving at the time of their capture, except with their consent.

ARTICLE 23

No prisoner of war may at any time be sent to or detained in areas where he may be exposed to the fire of the combat zone, nor may his presence be used to render certain points or areas immune from military operations.

Prisoners of war shall have shelters against air bombardment and other hazards of war, to the same extent as the local civilian population. With the exception of those engaged in the protection of their quarters against the aforesaid hazards, they may enter such shelters as soon as possible after the giving of the alarm. Any other protective measure taken in favor of the population shall also apply to them.

Detaining Powers shall give the Powers concerned, through the intermediary of the Protecting Powers, all useful information regarding the geographical location of prisoner of war camps.

Whenever military considerations permit, prisoner of war camps shall be indicated in the daytime by the letters PW or PG, placed so as to be clearly visible from the air. The Powers concerned may, however, agree upon any other system of marking. Only prisoner of war camps shall be marked as such.

ARTICLE 24

Transit or screening camps of a permanent kind shall be fitted out under conditions similar to those described in the present Section, and the prisoners therein shall have the same treatment as in other camps.

CHAPTER II QUARTERS, FOOD AND CLOTHING OF PRISONERS OF WAR

ARTICLE 25

Prisoners of war shall be quartered under conditions as favorable as those for the forces of the Detaining Power who are billeted in the same area. The said conditions shall make allowance for the habits and customs of the prisoners and shall in no case be prejudicial to their health.

The foregoing provisions shall apply in particular to the dormitories of prisoners of war as regards both total surface and minimum cubic space, and the general installations, bedding and blankets.

The premises provided for the use of prisoners of war individually or collectively, shall be entirely protected from dampness and adequately heated and lighted, in particular between dusk and lights out. All precautions must be taken against the danger of fire.

In any camps in which women prisoners of war, as well as men, are accommodated, separate dormitories shall be provided for them.

ARTICLE 26

The basic daily food rations shall be sufficient in quantity, quality and variety to keep prisoners of war in good health and to prevent loss of weight or the development of nutritional deficiencies. Account shall also be taken of the habitual diet of the prisoners.

The Detaining Power shall supply prisoners of war who work with such additional rations as are necessary for the labor on which they are employed.

Sufficient drinking water shall be supplied to prisoners of war. The use of tobacco shall be permitted.

Prisoners of war shall, as far as possible, be associated with the preparation of their meals; they may be employed for that purpose in the kitchens. Furthermore, they shall be given the means of preparing, themselves, the additional food in their possession.

Adequate premises shall be provided for messing.

Collective disciplinary measures affecting food are prohibited.

ARTICLE 27

Clothing, underwear and footwear shall be supplied to prisoners of war in sufficient quantities by the Detaining Power, which shall make allowance for the climate of the region where the prisoners are detained. Uniforms of enemy armed forces captured by the Detaining Power should, if suitable for the climate, be made available to clothe prisoners of war.

The regular replacement and repair of the above articles shall be assured by the Detaining Power. In addition, prisoners of war who work shall receive appropriate clothing, wherever the nature of the work demands.

ARTICLE 28

Canteens shall be installed in all camps, where prisoners of war may procure foodstuffs, soap and tobacco and ordinary articles in daily use. The tariff shall never be in excess of local market prices. The profits made by camp canteens shall be used for the benefit of the prisoners; a special fund shall be created for this purpose. The prisoners' representative shall have the right to collaborate in the management of the canteen and of this fund.

When a camp is closed down, the credit balance of the special fund shall be handed to an international welfare organization, to be employed for the benefit of prisoners of war of the same

nationality as those who have contributed to the fund. In case of a general repatriation, such profits shall be kept by the Detaining Power, subject to any agreement to the contrary between the Powers concerned

CHAPTER III HYGIENE AND MEDICAL ATTENTION

ARTICLE 29

The Detaining Power shall be bound to take all sanitary measures necessary to ensure the cleanliness and healthfulness of camps and to prevent epidemics.

Prisoners of war shall have for their use, day and night, conveniences which conform to the rules of hygiene and are maintained in a constant state of cleanliness. In any camps in which women prisoners of war are accommodated, separate conveniences shall be provided for them.

Also, apart from the baths and showers with which the camps shall be furnished, prisoners of war shall be provided with sufficient water and soap for their personal toilet and for washing their personal laundry; the necessary installations, facilities and time shall be granted them for that purpose.

ARTICLE 30

Every camp shall have an adequate infirmary where prisoners of war may have the attention they require, as well as appropriate diet. Isolation wards shall, if necessary, be set aside for cases of contagious or mental disease.

Prisoners of war suffering from serious disease, or whose condition necessitates special treatment, a surgical operation or hospital care, must be admitted to any military or civilian medical unit where such treatment can be given, even if their repatriation is contemplated in the near future. Special facilities shall be afforded for the care to be given to the disabled, in particular to the blind, and for their rehabilitation, pending repatriation.

Prisoners of war shall have the attention, preferably, of medical personnel of the Power on which they depend and, if possible, of their nationality.

Prisoners of war may not be prevented from presenting themselves to the medical authorities for examination. The detaining authorities shall, upon request, issue to every prisoner who has undergone treatment, an official certificate indicating the nature of his illness or injury, and the duration and kind of treatment received. A duplicate of this certificate shall be forwarded to the Central Prisoners of War Agency.

The costs of treatment, including those of any apparatus necessary for the maintenance of prisoners of war in good health, particularly dentures and other artificial appliances, and spectacles, shall be borne by the Detaining Power.

ARTICLE 31

Medical inspections of prisoners of war shall be held at least once a month. They shall include the checking and the recording of the weight of each prisoner of war. Their purpose shall be, in particular, to supervise the general state of health, nutrition and cleanliness of prisoners and to detect contagious diseases, especially tuberculosis, malaria and venereal disease. For this

purpose the most efficient methods available shall be employed, e.g. periodic mass miniature radiography for the early detection of tuberculosis.

ARTICLE 32

Prisoners of war who, though not attached to the medical service of their armed forces, are physicians, surgeons, dentists, nurses or medical orderlies, may be required by the Detaining Power to exercise their medical functions in the interests of prisoners of war dependent on the same Power. In that case they shall continue to be prisoners of war, but shall receive the same treatment as corresponding medical personnel retained by the Detaining Power. They shall be exempted from any other work under Article 49.

Chapter IV Medical Personnel and Chaplains Retained To Assist Prisoners Of War

ARTICLE 33

Members of the medical personnel and chaplains while retained by the Detaining Power with a view to assisting prisoners of war, shall not be considered as prisoners of war. They shall, however, receive as a minimum the benefits and protection of the present Convention, and shall also be granted all facilities necessary to provide for the medical care of, and religious ministration to, prisoners of war.

They shall continue to exercise their medical and spiritual functions for the benefit of prisoners of war, preferably those belonging to the armed forces upon which they depend, within the scope of the military laws and regulations of the Detaining Power and under the control of its competent services, in accordance with their professional etiquette. They shall also benefit by the following facilities in the exercise of their medical or spiritual functions:

(a) They shall be authorized to visit periodically prisoners of war situated in working detachments or in hospitals outside the camp. For this purpose, the Detaining Power shall place at their disposal the necessary means of transport.

(b) The senior medical officer in each camp shall be responsible to the camp military authorities for everything connected with the activities of retained medical personnel. For this purpose, Parties to the conflict shall agree at the outbreak of hostilities on the subject of the corresponding ranks of the medical personnel, including that of societies mentioned in Article 26 of the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of August 12, 1949. This senior medical officer, as well as chaplains, shall have the right to deal with the competent authorities of the camp on all questions relating to their duties. Such authorities shall afford them all necessary facilities for correspondence relating to these questions.

(c) Although they shall be subject to the internal discipline of the camp in which they are retained, such personnel may not be compelled to carry out any work other than that concerned with their medical or religious duties.

During hostilities, the Parties to the conflict shall agree concerning the possible relief of retained personnel and shall settle the procedure to be followed.

None of the preceding provisions shall relieve the Detaining Power of its obligations with regard to prisoners of war from the medical or spiritual point of view.

CHAPTER V RELIGIOUS, INTELLECTUAL AND PHYSICAL ACTIVITIES

ARTICLE 34

Prisoners of war shall enjoy complete latitude in the exercise of their religious duties, including attendance at the service of their faith, on condition that they comply with the disciplinary routine prescribed by the military authorities.

Adequate premises shall be provided where religious services may be held.

ARTICLE 35

Chaplains who fall into the hands of the enemy Power and who remain or are retained with a view to assisting prisoners of war, shall be allowed to minister to them and to exercise freely their ministry amongst prisoners of war of the same religion, in accordance with their religious conscience. They shall be allocated among the various camps and labor detachments containing prisoners of war belonging to the same forces, speaking the same language or practicing the same religion. They shall enjoy the necessary facilities, including the means of transport provided for in Article 33, for visiting the prisoners of war outside their camp. They shall be free to correspond, subject to censorship, on matters concerning their religious duties with the ecclesiastical authorities in the country of detention and with international religious organizations. Letters and cards which they may send for this purpose shall be in addition to the quota provided for in Article 71.

ARTICLE 36

Prisoners of war who are ministers of religion, without having officiated as chaplains to their own forces, shall be at liberty, whatever their denomination, to minister freely to the members of their community. For this purpose, they shall receive the same treatment as the chaplains retained by the Detaining Power. They shall not be obliged to do any other work.

ARTICLE 37

When prisoners of war have not the assistance of a retained chaplain or of a prisoner of war minister of their faith, a minister belonging to the prisoners' or a similar denomination, or in his absence a qualified layman, if such a course is feasible from a confessional point of view, shall be appointed, at the request of the prisoners concerned, to fill this office. This appointment, subject to the approval of the Detaining Power, shall take place with the agreement of the community of prisoners concerned and, wherever necessary, with the approval of the local religious authorities of the same faith. The person thus appointed shall comply with all regulations established by the Detaining Power in the interests of discipline and military security.

ARTICLE 38

While respecting the individual preferences of every prisoner, the Detaining Power shall encourage the practice of intellectual, educational, and recreational pursuits, sports and games amongst prisoners, and shall take the measures necessary to ensure the exercise thereof by providing them with adequate premises and necessary equipment.

Prisoners shall have opportunities for taking physical exercise, including sports and games, and for being out of doors. Sufficient open spaces shall be provided for this purpose in all camps.

CHAPTER VI DISCIPLINE

ARTICLE 39

Every prisoner of war camp shall be put under the immediate authority of a responsible commissioned officer belonging to the regular armed forces of the Detaining Power. Such officer shall have in his possession a copy of the present Convention; he shall ensure that its provisions are known to the camp staff and the guard and shall be responsible, under the direction of his government, for its application.

Prisoners of war, with the exception of officers, must salute and show to all officers of the Detaining Power the external marks of respect provided for by the regulations applying in their own forces.

Officer prisoners of war are bound to salute only officers of a higher rank of the Detaining Power; they must, however, salute the camp commander regardless of his rank.

ARTICLE 40

The wearing of badges of rank and nationality, as well as of decorations, shall be permitted.

ARTICLE 41

In every camp the text of the present Convention and its Annexes and the contents of any special agreement provided for in Article 6, shall be posted, in the prisoners' own language, at places where all may read them. Copies shall be supplied, on request, to the prisoners who cannot have access to the copy which has been posted.

Regulations, orders, notices and publications of every kind relating to the conduct of prisoners of war shall be issued to them in a language which they understand. Such regulations, orders and publications shall be posted in the manner described above and copies shall be handed to the prisoners' representative. Every order and command addressed to prisoners of war individually must likewise be given in a language which they understand.

ARTICLE 42

The use of weapons against prisoners of war, especially against those who are escaping or attempting to escape, shall constitute an extreme measure, which shall always be preceded by warnings appropriate to the circumstances.

CHAPTER VII RANK OF PRISONERS OF WAR

ARTICLE 43

Upon the outbreak of hostilities, the Parties to the conflict shall communicate to one another the titles and ranks of all the persons mentioned in Article 4 of the present Convention, in order to ensure equality of treatment between prisoners of equivalent rank. Titles and ranks which are subsequently created shall form the subject of similar communications.

The Detaining Power shall recognize promotions in rank which have been accorded to prisoners of war and which have been duly notified by the Power on which these prisoners depend.

ARTICLE 44

Officers and prisoners of equivalent status shall be treated with the regard due to their rank and age.

In order to ensure service in officers' camps, other ranks of the same armed forces who, as far as possible, speak the same language, shall be assigned in sufficient numbers, account being taken of the rank of officers and prisoners of equivalent status. Such orderlies shall not be required to perform any other work.

Supervision of the mess by the officers themselves shall be facilitated in every way.

ARTICLE 45

Prisoners of war other than officers and prisoners of equivalent status shall be treated with the regard due to their rank and age.

Supervision of the mess by the prisoners themselves shall be facilitated in every way.

CHAPTER VIII TRANSFER OF PRISONERS OF WAR AFTER THEIR ARRIVAL IN CAMP

ARTICLE 46

The Detaining Power, when deciding upon the transfer of prisoners of war, shall take into account the interests of the prisoners themselves, more especially so as not to increase the difficulty of their repatriation.

The transfer of prisoners of war shall always be effected humanely and in conditions not less favorable than those under which the forces of the Detaining Power are transferred. Account shall always be taken of the climatic conditions to which the prisoners of war are accustomed and the conditions of transfer shall in no case be prejudicial to their health.

The Detaining Power shall supply prisoners of war during transfer with sufficient food and drinking water to keep them in good health, likewise with the necessary clothing, shelter and medical attention. The Detaining Power shall take adequate precautions especially in case of transport by sea or by air, to ensure their safety during transfer, and shall draw up a complete list of all transferred prisoners before their departure.

ARTICLE 47

Sick or wounded prisoners of war shall not be transferred as long as their recovery may be endangered by the journey, unless their safety imperatively demands it.

If the combat zone draws closer to a camp, the prisoners of war in the said camp shall not be transferred unless their transfer can be carried out in adequate conditions of safety, or if they are exposed to greater risks by remaining on the spot than by being transferred.

ARTICLE 48

In the event of transfer, prisoners of war shall be officially advised of their departure and of their new postal address. Such notifications shall be given in time for them to pack their luggage and inform their next of kin.

They shall be allowed to take with them their personal effects, and the correspondence and parcels which have arrived for them. The weight of such baggage may be limited, if the conditions of transfer so require, to what each prisoner can reasonably carry, which shall in no case be more than twenty-five kilograms per head.

Mail and parcels addressed to their former camp shall be forwarded to them without delay. The camp commander shall take, in agreement with the prisoners' representative, any measures needed to ensure the transport of the prisoners' community property and of the luggage they are unable to take with them in consequence of restrictions imposed by virtue of the second paragraph of this Article.

The costs of transfers shall be borne by the Detaining Power.

SECTION III LABOR OF PRISONERS OF WAR

ARTICLE 49

The Detaining Power may utilize the labor of prisoners of war who are physically fit, taking into account their age, sex, rank and physical aptitude, and with a view particularly to maintaining them in a good state of physical and mental health.

Non-commissioned officers who are prisoners of war shall only be required to do supervisory work. Those not so required may ask for other suitable work which shall, so far as possible, be found for them.

If officers or persons of equivalent status ask for suitable work, it shall be found for them, so far as possible, but they may in no circumstances be compelled to work.

ARTICLE 50

Besides work connected with camp administration, installation or maintenance, prisoners of war may be compelled to do only such work as is included in the following classes:

(a) Agriculture;

(b) Industries connected with the production or the extraction of raw materials, and manufacturing industries, with the exception of metallurgical, machinery and chemical industries; public works and building operations which have no military character or purpose;

(c) Transport and handling of stores which are not military in character or purpose;

(d) Commercial business, and arts and crafts;

(e) Domestic service;

(f) Public utility services having no military character or purpose.

Should the above provisions be infringed, prisoners of war shall be allowed to exercise their right of complaint, in conformity with Article 78.

ARTICLE 51

Prisoners of war must be granted suitable working conditions, especially as regards accommodation, food, clothing and equipment; such conditions shall not be inferior to those enjoyed by nationals of the Detaining Power employed in similar work; account shall also be taken of climatic conditions.

The Detaining Power, in utilizing the labor of prisoners of war, shall ensure that in areas in which prisoners are employed, the national legislation concerning the protection of labor, and, more particularly, the regulations for the safety of workers, are duly applied.

Prisoners of war shall receive training and be provided with the means of protection suitable to the work they will have to do and similar to those accorded to the nationals of the Detaining Power. Subject to the provisions of Article 52, prisoners may be submitted to the normal risks run by these civilian workers.

Conditions of labor shall in no case be rendered more arduous by disciplinary measures.

ARTICLE 52

Unless he be a volunteer, no prisoner of war may be employed on labor which is of an unhealthy or dangerous nature.

No prisoner of war shall be assigned to labor which would be looked upon as humiliating for a member of the Detaining Power's own forces.

The removal of mines or similar devices shall be considered as dangerous labor.

ARTICLE 53

The duration of the daily labor of prisoners of war, including the time of the journey to and fro, shall not be excessive, and must in no case exceed that permitted for civilian workers in the district, who are nationals of the Detaining Power and employed on the same work.

Prisoners of war must be allowed, in the middle of the day's work, a rest of not less than one hour. This rest will be the same as that to which workers of the Detaining Power are entitled, if the latter is of longer duration. They shall be allowed in addition a rest of twenty-four consecutive hours every week, preferably on Sunday or the day of rest in their country of origin. Furthermore, every prisoner who has worked for one year shall be granted a rest of eight consecutive days, during which his working pay shall be paid him.

If methods of labor such as piecework are employed, the length of the working period shall not be rendered excessive thereby.

ARTICLE 54

The working pay due to prisoners of war shall be fixed in accordance with the provisions of Article 62 of the present Convention.

Prisoners of war who sustain accidents in connection with work, or who contract a disease in the course, or in consequence of their work, shall receive all the care their condition may require. The Detaining Power shall furthermore deliver to such prisoners of war a medical certificate enabling them to submit their claims to the Power on which they depend, and shall send a duplicate to the Central Prisoners of War Agency provided for in Article 123.

ARTICLE 55

The fitness of prisoners of war for work shall be periodically verified by medical examinations at least once a month. The examinations shall have particular regard to the nature of the work which prisoners of war are required to do.

If any prisoner of war considers himself incapable of working, he shall be permitted to appear before the medical authorities of his camp. Physicians or surgeons may recommend that the prisoners who are, in their opinion, unfit for work, be exempted therefrom.

ARTICLE 56

The organization and administration of labor detachments shall be similar to those of prisoner of war camps.

Every labor detachment shall remain under the control of and administratively part of a prisoner of war camp. The military authorities and the commander of the said camp shall be responsible, under the direction of their government, for the observance of the provisions of the present Convention in labor detachments.

The camp commander shall keep an up-to-date record of the labor detachments dependent on his camp, and shall communicate it to the delegates of the Protecting Power, of the International Committee of the Red Cross, or of other agencies giving relief to prisoners of war, who may visit the camp.

ARTICLE 57

The treatment of prisoners of war who work for private persons, even if the latter are responsible for guarding and protecting them, shall not be inferior to that which is provided for by the present Convention. The Detaining Power, the military authorities and the commander of the camp to which such prisoners belong shall be entirely responsible for the maintenance, care, treatment, and payment of the working pay of such prisoners of war.

Such prisoners of war shall have the right to remain in communication with the prisoners' representatives in the camps on which they depend.

SECTION IV FINANCIAL RESOURCES OF PRISONERS OF WAR

ARTICLE 58

Upon the outbreak of hostilities, and pending an arrangement on this matter with the Protecting Power, the Detaining Power may determine the maximum amount of money in cash or in any similar form that prisoners may have in their possession. Any amount in excess, which was properly in their possession and which has been taken or withheld from them, shall be placed to their account, together with any monies deposited by them, and shall not be converted into any other currency without their consent.

If prisoners of war are permitted to purchase services or commodities outside the camp against payment in cash, such payments shall be made by the prisoner himself or by the camp administration who will charge them to the accounts of the prisoners concerned. The Detaining Power will establish the necessary rules in this respect.

ARTICLE 59

Cash which was taken from prisoners of war, in accordance with Article 18, at the time of their capture, and which is in the currency of the Detaining Power, shall be placed to their separate accounts, in accordance with the provisions of Article 64 of the present Section.

The amounts, in the currency of the Detaining Power, due to the conversion of sums in other currencies that are taken from the prisoners of war at the same time, shall also be credited to their separate accounts.

ARTICLE 60

The Detaining Power shall grant all prisoners of war a monthly advance of pay, the amount of which shall be fixed by conversion, into the currency of the said Power, of the following amounts:

Category I: Prisoners ranking below sergeant: eight Swiss francs.

Category II: Sergeants and other non-commissioned officers, or prisoners of equivalent rank: twelve Swiss francs.

Category III: Warrant officers and commissioned officers below the rank of major or prisoners of equivalent rank: fifty Swiss francs.

Category IV: Majors, lieutenant colonels, colonels or prisoners of equivalent rank: sixty Swiss francs.

Category V: General officers or prisoners of equivalent rank: seventy-five Swiss francs.

However, the Parties to the conflict concerned may by special agreement modify the amount of advances of pay due to prisoners of the preceding categories.

Furthermore, if the amounts indicated in the first paragraph above would be unduly high compared with the pay of the Detaining Power's armed forces or would, for any reason, seriously embarrass the Detaining Power, then, pending the conclusion of a special agreement with the Power on which the prisoners depend to vary the amounts indicated above, the Detaining Power:

(a) Shall continue to credit the accounts of the prisoners with the amounts indicated in the first paragraph above;

(b) May temporarily limit the amount made available from these advances of pay to prisoners of war for their own use, to sums which are reasonable, but which, for Category I, shall never be inferior to the amount that the Detaining Power gives to the members of its own armed forces.

The reasons for any limitations will be given without delay to the Protecting Power.

ARTICLE 61

The Detaining Power shall accept for distribution as supplementary pay to prisoners of war sums which the Power on which the prisoners depend may forward to them, on condition that the sums to be paid shall be the same for each prisoner of the same category, shall be payable to all prisoners of that category depending on that Power, and shall be placed in their separate accounts, at the earliest opportunity, in accordance with the provisions of Article 64. Such supplementary pay shall not relieve the Detaining Power of any obligation under this Convention.

ARTICLE 62

Prisoners of war shall be paid a fair working rate of pay by the detaining authorities direct. The rate shall be fixed by the said authorities, but shall at no time be less than one-fourth of one Swiss franc for a full working day. The Detaining Power shall inform prisoners of war, as well as the Power on which they depend, through the intermediary of the Protecting Power, of the rate of daily working pay that it has fixed.

Working pay shall likewise be paid by the detaining authorities to prisoners of war permanently detailed to duties or to a skilled or semi-skilled occupation in connection with the administration, installation or maintenance of camps, and to the prisoners who are required to carry out spiritual or medical duties on behalf of their comrades.

The working pay of the prisoners' representative, of his advisers, if any, and of his assistants, shall be paid out of the fund maintained by canteen profits. The scale of this working pay shall be fixed by the prisoners' representative and approved by the camp commander. If there is no such fund, the detaining authorities shall pay these prisoners a fair working rate of pay.

ARTICLE 63

Prisoners of war shall be permitted to receive remittances of money addressed to them individually or collectively.

Every prisoner of war shall have at his disposal the credit balance of his account as provided for in the following Article, within the limits fixed by the Detaining Power, which shall make such payments as are requested. Subject to financial or monetary restrictions which the Detaining Power regards as essential, prisoners of war may also have payments made abroad. In this case payments addressed by prisoners of war to dependants shall be given priority.

In any event, and subject to the consent of the Power on which they depend, prisoners may have payments made in their own country, as follows: the Detaining Power shall send to the aforesaid

Power through the Protecting Power a notification giving all the necessary particulars concerning the prisoners of war, the beneficiaries of the payments, and the amount of the sums to be paid, expressed in the Detaining Power's currency. The said notification shall be signed by the prisoners and countersigned by the camp commander. The Detaining Power shall debit the prisoners' account by a corresponding amount; the sums thus debited shall be placed by it to the credit of the Power on which the prisoners depend.

To apply the foregoing provisions, the Detaining Power may usefully consult the Model Regulations in Annex V of the present Convention.

ARTICLE 64

The Detaining Power shall hold an account for each prisoner of war, showing at least the following:

1. The amounts due to the prisoner or received by him as advances of pay, as working pay or derived from any other source; the sums in the currency of the Detaining Power which were taken from him; the sums taken from him and converted at his request into the currency of the said Power.

2. The payments made to the prisoner in cash, or in any other similar form; the payments made on his behalf and at his request; the sums transferred under Article 63, third paragraph.

ARTICLE 65

Every item entered in the account of a prisoner of war shall be countersigned or initialed by him, or by the prisoners' representative acting on his behalf.

Prisoners of war shall at all times be afforded reasonable facilities for consulting and obtaining copies of their accounts, which may likewise be inspected by the representatives of the Protecting Powers at the time of visits to the camp.

When prisoners of war are transferred from one camp to another, their personal accounts will follow them. In case of transfer from one Detaining Power to another, the monies which are their property and are not in the currency of the Detaining Power will follow them. They shall be given certificates for any other monies standing to the credit of their accounts.

The Parties to the conflict concerned may agree to notify to each other at specific intervals through the Protecting Power, the amount of the accounts of the prisoners of war.

ARTICLE 66

On the termination of captivity, through the release of a prisoner of war or his repatriation, the Detaining Power shall give him a statement, signed by an authorized officer of that Power, showing the credit balance then due to him. The Detaining Power shall also send through the Protecting Power to the government upon which the prisoner of war depends, lists giving all appropriate particulars of all prisoners of war whose captivity has been terminated by repatriation, release, escape, death or any other means, and showing the amount of their credit balances. Such lists shall be certified on each sheet by an authorized representative of the Detaining Power.

Any of the above provisions of this Article may be varied by mutual agreement between any two Parties to the conflict.

The Power on which the prisoner of war depends shall be responsible for settling with him any credit balance due to him from the Detaining Power on the termination of his captivity.

ARTICLE 67

Advances of pay, issued to prisoners of war in conformity with Article 60, shall be considered as made on behalf of the Power on which they depend. Such advances of pay, as well as all payments made by the said Power under Article 63, third paragraph, and Article 68, shall form the subject of arrangements between the Powers concerned, at the close of hostilities.

ARTICLE 68

Any claim by a prisoner of war for compensation in respect of any injury or other disability arising out of work shall be referred to the Power on which he depends, through the Protecting Power. In accordance with Article 54, the Detaining Power will, in all cases, provide the prisoner of war concerned with a statement showing the nature of the injury or disability, the circumstances in which it arose and particulars of medical or hospital treatment given for it. This statement will be signed by a responsible officer of the Detaining Power and the medical particulars certified by a medical officer.

Any claim by a prisoner of war for compensation in respect of personal effects, monies or valuables impounded by the Detaining Power under Article 18 and not forthcoming on his repatriation, or in respect of loss alleged to be due to the fault of the Detaining Power or any of its servants, shall likewise be referred to the Power on which he depends. Nevertheless, any such personal effects required for use by the prisoners of war whilst in captivity shall be replaced at the expense of the Detaining Power. The Detaining Power will, in all cases, provide the prisoner of war with a statement, signed by a responsible officer, showing all available information regarding the reasons why such effects, monies or valuables have not been restored to him. A copy of this statement will be forwarded to the Power on which he depends through the Central Prisoners of War Agency provided for in Article 123.

SECTION V RELATIONS OF PRISONERS OF WAR WITH THE EXTERIOR

ARTICLE 69

Immediately upon prisoners of war falling into its power, the Detaining Power shall inform them and the Powers on which they depend, through the Protecting Power, of the measures taken to carry out the provisions of the present Section. They shall likewise inform the parties concerned of any subsequent modifications of such measures.

ARTICLE 70

Immediately upon capture, or not more than one week after arrival at a camp, even if it is a transit camp, likewise in case of sickness or transfer to hospital or another camp, every prisoner of war shall be enabled to write direct to his family, on the one hand, and to the Central

Prisoners of War Agency provided for in Article 123, on the other hand, a card similar, if possible, to the model annexed to the present Convention, informing his relatives of his capture, address and state of health. The said cards shall be forwarded as rapidly as possible and may not be delayed in any manner.

ARTICLE 71

Prisoners of war shall be allowed to send and receive letters and cards. If the Detaining Power deems it necessary to limit the number of letters and cards sent by each prisoner of war, the said number shall not be less than two letters and four cards monthly, exclusive of the capture cards provided for in Article 70, and conforming as closely as possible to the models annexed to the present Convention. Further limitations may be imposed only if the Protecting Power is satisfied that it would be in the interests of the prisoners of war concerned to do so owing to difficulties of translation caused by the Detaining Power's inability to find sufficient qualified linguists to carry out the necessary censorship. If limitations must be placed on the correspondence addressed to prisoners of war, they may be ordered only by the Power on which the prisoners depend, possibly at the request of the Detaining Power. Such letters and cards must be conveyed by the most rapid method at the disposal of the Detaining Power; they may not be delayed or retained for disciplinary reasons.

Prisoners of war who have been without news for a long period, or who are unable to receive news from their next of kin or to give them news by the ordinary postal route, as well as those who are at a great distance from their homes, shall be permitted to send telegrams, the fees being charged against the prisoners of war's accounts with the Detaining Power or paid in the currency at their disposal. They shall likewise benefit by this measure in cases of urgency.

As a general rule, the correspondence of prisoners of war shall be written in their native language. The Parties to the conflict may allow correspondence in other languages.

Sacks containing prisoner of war mail must be securely sealed and labeled so as clearly to indicate their contents, and must be addressed to offices of destination.

ARTICLE 72

Prisoners of war shall be allowed to receive by post or by any other means individual parcels or collective shipments containing, in particular, foodstuffs, clothing, medical supplies and articles of a religious, educational or recreational character which may meet their needs, including books, devotional articles, scientific equipment, examination papers, musical instruments, sports outfits and materials allowing prisoners of war to pursue their studies or their cultural activities.

Such shipments shall in no way free the Detaining Power from the obligations imposed upon it by virtue of the present Convention.

The only limits which may be placed on these shipments shall be those proposed by the Protecting Power in the interest of the prisoners themselves, or by the International Committee of the Red Cross or any other organization giving assistance to the prisoners, in respect of their own shipments only, on account of exceptional strain on transport or communications.

The conditions for the sending of individual parcels and collective relief shall, if necessary, be the subject of special agreements between the Powers concerned, which may in no case delay the

receipt by the prisoners of relief supplies. Books may not be included in parcels of clothing and foodstuffs. Medical supplies shall, as a rule, be sent in collective parcels.

ARTICLE 73

In the absence of special agreements between the Powers concerned on the conditions for the receipt and distribution of collective relief shipments, the rules and regulations concerning collective shipments, which are annexed to the present Convention, shall be applied.

The special agreements referred to above shall in no case restrict the right of prisoners' representatives to take possession of collective relief shipments intended for prisoners of war, to proceed to their distribution or to dispose of them in the interest of the prisoners.

Nor shall such agreements restrict the right of representatives of the Protecting Power, the International Committee of the Red Cross or any other organization giving assistance to prisoners of war and responsible for the forwarding of collective shipments, to supervise their distribution to the recipients.

ARTICLE 74

All relief shipments for prisoners of war shall be exempt from import, customs and other dues.

Correspondence, relief shipments and authorized remittances of money addressed to prisoners of war or dispatched by them through the post office, either direct or through the Information Bureau provided for in Article 122 and the Central Prisoners of War Agency provided for in Article 123, shall be exempt from any postal dues, both in the countries of origin and destination, and in intermediate countries.

If relief shipments intended for prisoners of war cannot be sent through the post office by reason of weight or for any other cause, the cost of transportation shall be borne by the Detaining Power in all the territories under its control. The other Powers party to the Convention shall bear the cost of transport in their respective territories.

In the absence of special agreements between the Parties concerned, the costs connected with transport of such shipments, other than costs covered by the above exemption, shall be charged to the senders.

The High Contracting Parties shall endeavor to reduce, so far as possible, the rates charged for telegrams sent by prisoners of war, or addressed to them.

ARTICLE 75

Should military operations prevent the Powers concerned from fulfilling their obligation to assure the transport of the shipments referred to in Articles 70, 71, 72 and 77, the Protecting Powers concerned, the International Committee of the Red Cross or any other organization duly approved by the Parties to the conflict may undertake to ensure the conveyance of such shipments by suitable means (railway wagons, motor vehicles, vessels or aircraft, etc.). For this purpose, the High Contracting Parties shall endeavor to supply them with such transport and to allow its circulation, especially by granting the necessary safe-conducts.

Such transport may also be used to convey:

(a) Correspondence, lists and reports exchanged between the Central Information Agency referred to in Article 123 and the National Bureau referred to in Article 122;

(b) Correspondence and reports relating to prisoners of war which the Protecting Powers, the International Committee of the Red Cross or any other body assisting the prisoners, exchange either with their own delegates or with the Parties to the conflict.

These provisions in no way detract from the right of any Party to the conflict to arrange other means of transport, if it should so prefer, nor preclude the granting of safe-conducts, under mutually agreed conditions, to such means of transport.

In the absence of special agreements, the costs occasioned by the use of such means of transport shall be borne proportionally by the Parties to the conflict whose nationals are benefited thereby.

ARTICLE 76

The censoring of correspondence addressed to prisoners of war or dispatched by them shall be done as quickly as possible. Mail shall be censored only by the dispatching State and the receiving State, and once only by each.

The examination of consignments intended for prisoners of war shall not be carried out under conditions that will expose the goods contained in them to deterioration; except in the case of written or printed matter, it shall be done in the presence of the addressee, or of a fellow-prisoner duly delegated by him. The delivery to prisoners of individual or collective consignments shall not be delayed under the pretext of difficulties of censorship.

Any prohibition of correspondence ordered by Parties to the conflict, either for military or political reasons, shall be only temporary and its duration shall be as short as possible.

ARTICLE 77

The Detaining Powers shall provide all facilities for the transmission, through the Protecting Power or the Central Prisoners of War Agency provided for in Article 123, of instruments, papers or documents intended for prisoners of war or dispatched by them, especially powers of attorney and wills.

In all cases they shall facilitate the preparation and execution of such documents on behalf of prisoners of war; in particular, they shall allow them to consult a lawyer and shall take what measures are necessary for the authentication of their signatures.

SECTION VI RELATIONS BETWEEN PRISONERS OF WAR AND THE AUTHORITIES

CHAPTER I COMPLAINTS OF PRISONERS OF WAR RESPECTING THE CONDITIONS OF CAPTIVITY

ARTICLE 78

Prisoners of war shall have the right to make known to the military authorities in whose power they are, their requests regarding the conditions of captivity to which they are subjected.

They shall also have the unrestricted right to apply to the representatives of the Protecting Powers either through their prisoners' representative or, if they consider it necessary, direct, in order to draw their attention to any points on which they may have complaints to make regarding their conditions of captivity.

These requests and complaints shall not be limited nor considered to be a part of the correspondence quota referred to in Article 71. They must be transmitted immediately. Even if they are recognized to be unfounded, they may not give rise to any punishment.

Prisoners' representatives may send periodic reports on the situation in the camps and the needs of the prisoners of war to the representatives of the Protecting Powers.

CHAPTER II PRISONER OF WAR REPRESENTATIVES

ARTICLE 79

In all places where there are prisoners of war, except in those where there are officers, the prisoners shall freely elect by secret ballot, every six months, and also in case of vacancies, prisoners' representatives entrusted with representing them before the military authorities, the Protecting Powers, the International Committee of the Red Cross and any other organization which may assist them. These prisoners' representatives shall be eligible for re-election.

In camps for officers and persons of equivalent status or in mixed camps, the senior officer among the prisoners of war shall be recognized as the camp prisoners' representative. In camps for officers, he shall be assisted by one or more advisers chosen by the officers; in mixed camps, his assistants shall be chosen from among the prisoners of war who are not officers and shall be elected by them.

Officer prisoners of war of the same nationality shall be stationed in labor camps for prisoners of war, for the purpose of carrying out the camp administration duties for which the prisoners of war are responsible. These officers may be elected as prisoners' representatives under the first paragraph of this Article. In such a case the assistants to the prisoners' representatives shall be chosen from among those prisoners of war who are not officers.

Every representative elected must be approved by the Detaining Power before he has the right to commence his duties. Where the Detaining Power refuses to approve a prisoner of war elected by his fellow prisoners of war, it must inform the Protecting Power of the reason for such refusal.

In all cases the prisoners' representative must have the same nationality, language and customs as the prisoners of war whom he represents. Thus, prisoners of war distributed in different sections of a camp, according to their nationality, language or customs, shall have for each section their own prisoners' representative, in accordance with the foregoing paragraphs.

ARTICLE 80

Prisoners' representatives shall further the physical, spiritual and intellectual well being of prisoners of war.

In particular, where the prisoners decide to organize amongst themselves a system of mutual assistance, this organization will be within the province of the prisoners' representative, in addition to the special duties entrusted to him by other provisions of the present Convention.

Prisoners' representatives shall not be held responsible, simply by reason of their duties, for any offences committed by prisoners of war.

ARTICLE 81

Prisoners' representatives shall not be required to perform any other work, if the accomplishment of their duties is thereby made more difficult.

Prisoners' representatives may appoint from amongst the prisoners such assistants as they may require. All material facilities shall be granted them, particularly a certain freedom of movement necessary for the accomplishment of their duties (inspection of labor detachments, receipt of supplies, etc.).

Prisoners' representatives shall be permitted to visit premises where prisoners of war are detained, and every prisoner of war shall have the right to consult freely his prisoners' representative.

All facilities shall likewise be accorded to the prisoners' representatives for communication by post and telegraph with the detaining authorities, the Protecting Powers, the International Committee of the Red Cross and their delegates, the Mixed Medical Commissions and with the bodies which give assistance to prisoners of war. Prisoners' representatives of labor detachments shall enjoy the same facilities for communication with the prisoners' representatives of the principal camp. Such communications shall not be restricted, nor considered as forming a part of the quota mentioned in Article 71.

Prisoners' representatives who are transferred shall be allowed a reasonable time to acquaint their successors with current affairs.

In case of dismissal, the reasons therefor shall be communicated to the Protecting Power.

CHAPTER III PENAL AND DISCIPLINARY SANCTIONS

I. GENERAL PROVISIONS

ARTICLE 82

A prisoner of war shall be subject to the laws, regulations and orders in force in the armed forces of the Detaining Power; the Detaining Power shall be justified in taking judicial or disciplinary measures in respect of any offence committed by a prisoner of war against such laws, regulations or orders. However, no proceedings or punishments contrary to the provisions of this Chapter shall be allowed.

If any law, regulation or order of the Detaining Power shall declare acts committed by a prisoner of war to be punishable, whereas the same acts would not be punishable if committed by a member of the forces of the Detaining Power, such acts shall entail disciplinary punishments only.

ARTICLE 83

In deciding whether proceedings in respect of an offence alleged to have been committed by a prisoner of war shall be judicial or disciplinary, the Detaining Power shall ensure that the competent authorities exercise the greatest leniency and adopt, wherever possible, disciplinary rather than judicial measures.

ARTICLE 84

A prisoner of war shall be tried only by a military court, unless the existing laws of the Detaining Power expressly permit the civil courts to try a member of the armed forces of the Detaining Power in respect of the particular offence alleged to have been committed by the prisoner of war.

In no circumstances whatever shall a prisoner of war be tried by a court of any kind which does not offer the essential guarantees of independence and impartiality as generally recognized, and, in particular, the procedure of which does not afford the accused the rights and means of defense provided for in Article 105.

ARTICLE 85

Prisoners of war prosecuted under the laws of the Detaining Power for acts committed prior to capture shall retain, even if convicted, the benefits of the present Convention.

ARTICLE 86

No prisoner of war may be punished more than once for the same act, or on the same charge.

ARTICLE 87

Prisoners of war may not be sentenced by the military authorities and courts of the Detaining Power to any penalties except those provided for in respect of members of the armed forces of the said Power who have committed the same acts.

When fixing the penalty, the courts or authorities of the Detaining Power shall take into consideration, to the widest extent possible, the fact that the accused, not being a national of the Detaining Power, is not bound to it by any duty of allegiance, and that he is in its power as the result of circumstances independent of his own will. The said courts or authorities shall be at liberty to reduce the penalty provided for the violation of which the prisoner of war is accused, and shall therefore not be bound to apply the minimum penalty prescribed.

Collective punishment for individual acts, corporal punishments, imprisonment in premises without daylight and, in general, any form of torture or cruelty, are forbidden.

No prisoner of war may be deprived of his rank by the Detaining Power, or prevented from wearing his badges.

ARTICLE 88

Officers, non-commissioned officers and men who are prisoners of war undergoing a disciplinary or judicial punishment, shall not be subjected to more severe treatment than that applied in respect of the same punishment to members of the armed forces of the Detaining Power of equivalent rank.

A woman prisoner of war shall not be awarded or sentenced to a punishment more severe, or treated whilst undergoing punishment more severely, than a woman member of the armed forces of the Detaining Power dealt with for a similar offence.

In no case may a woman prisoner of war be awarded or sentenced to a punishment more severe, or treated whilst undergoing punishment more severely, than a male member of the armed forces of the Detaining Power dealt with for a similar offence.

Prisoners of war who have served disciplinary or judicial sentences may not be treated differently from other prisoners of war.

II. DISCIPLINARY SANCTIONS

ARTICLE 89

The disciplinary punishments applicable to prisoners of war are the following:

1. A fine which shall not exceed 50 per cent of the advances of pay and working pay which the prisoner of war would otherwise receive under the provisions of Articles 60 and 62 during a period of not more than thirty days.

2. Discontinuance of privileges granted over and above the treatment provided for by the present Convention.

3. Fatigue duties not exceeding two hours daily.

4. Confinement.

The punishment referred to under (3) shall not be applied to officers.

In no case shall disciplinary punishments be inhuman, brutal or dangerous to the health of prisoners of war.

ARTICLE 90

The duration of any single punishment shall in no case exceed thirty days. Any period of confinement awaiting the hearing of a disciplinary offence or the award of disciplinary punishment shall be deducted from an award pronounced against a prisoner of war.

The maximum of thirty days provided above may not be exceeded, even if the prisoner of war is answerable for several acts at the same time when he is awarded punishment, whether such acts are related or not.

The period between the pronouncing of an award of disciplinary punishment and its execution shall not exceed one month.

When a prisoner of war is awarded a further disciplinary punishment, a period of at least three days shall elapse between the execution of any two of the punishments, if the duration of one of these is ten days or more.

ARTICLE 91

The escape of a prisoner of war shall be deemed to have succeeded when:

1. He has joined the armed forces of the Power on which he depends, or those of an allied Power;

2. He has left the territory under the control of the Detaining Power, or of an ally of the said Power;

3. He has joined a ship flying the flag of the Power on which he depends, or of an allied Power, in the territorial waters of the Detaining Power, the said ship not being under the control of the last-named Power.

Prisoners of war who have made good their escape in the sense of this Article and who are recaptured, shall not be liable to any punishment in respect of their previous escape.

ARTICLE 92

A prisoner of war who attempts to escape and is recaptured before having made good his escape in the sense of Article 91 shall be liable only to a disciplinary punishment in respect of this act, even if it is a repeated offence.

A prisoner of war who is recaptured shall be handed over without delay to the competent military authority.

Article 88, fourth paragraph, notwithstanding, prisoners of war punished as a result of an unsuccessful escape may be subjected to special surveillance. Such surveillance must not affect the state of their health, must be undergone in a prisoner of war camp, and must not entail the suppression of any of the safeguards granted them by the present Convention.

ARTICLE 93

Escape or attempt to escape, even if it is a repeated offence, shall not be deemed an aggravating circumstance if the prisoner of war is subjected to trial by judicial proceedings in respect of an offence committed during his escape or attempt to escape.

In conformity with the principle stated in Article 83, offences committed by prisoners of war with the sole intention of facilitating their escape and which do not entail any violence against life or limb, such as offences against public property, theft without intention of self-enrichment, the drawing up or use of false papers, the wearing of civilian clothing, shall occasion disciplinary punishment only.

Prisoners of war who aid or abet an escape or an attempt to escape shall be liable on this count to disciplinary punishment only.

ARTICLE 94

If an escaped prisoner of war is recaptured, the Power on which he depends shall be notified thereof in the manner defined in Article 122, provided notification of his escape has been made.

ARTICLE 95

A prisoner of war accused of an offence against discipline shall not be kept in confinement pending the hearing unless a member of the armed forces of the Detaining Power would be so kept if he were accused of a similar offence, or if it is essential in the interests of camp order and discipline.

Any period spent by a prisoner of war in confinement awaiting the disposal of an offence against discipline shall be reduced to an absolute minimum and shall not exceed fourteen days.

The provisions of Articles 97 and 98 of this Chapter shall apply to prisoners of war who are in confinement awaiting the disposal of offences against discipline.

ARTICLE 96

Acts which constitute offences against discipline shall be investigated immediately.

Without prejudice to the competence of courts and superior military authorities, disciplinary punishment may be ordered only by an officer having disciplinary powers in his capacity as camp commander, or by a responsible officer who replaces him or to whom he has delegated his disciplinary powers.

In no case may such powers be delegated to a prisoner of war or be exercised by a prisoner of war.

Before any disciplinary award is pronounced, the accused shall be given precise information regarding the offences of which he is accused, and given an opportunity of explaining his conduct and of defending himself. He shall be permitted, in particular, to call witnesses and to have recourse, if necessary, to the services of a qualified interpreter. The decision shall be announced to the accused prisoner of war and to the prisoners' representative.

A record of disciplinary punishments shall be maintained by the camp commander and shall be open to inspection by representatives of the Protecting Power.

ARTICLE 97

Prisoners of war shall not in any case be transferred to penitentiary establishments (prisons, penitentiaries, convict prisons, etc.) to undergo disciplinary punishment therein.

All premises in which disciplinary punishments are undergone shall conform to the sanitary requirements set forth in Article 25. A prisoner of war undergoing punishment shall be enabled to keep himself in a state of cleanliness, in conformity with Article 29.

Officers and persons of equivalent status shall not be lodged in the same quarters as non-commissioned officers or men.

Women prisoners of war undergoing disciplinary punishment shall be confined in separate quarters from male prisoners of war and shall be under the immediate supervision of women.

ARTICLE 98

A prisoner of war undergoing confinement as a disciplinary punishment, shall continue to enjoy the benefits of the provisions of this Convention except in so far as these are necessarily rendered inapplicable by the mere fact that he is confined. In no case may he be deprived of the benefits of the provisions of Articles 78 and 126.

A prisoner of war awarded disciplinary punishment may not be deprived of the prerogatives attached to his rank.

Prisoners of war awarded disciplinary punishment shall be allowed to exercise and to stay in the open air at least two hours daily.

They shall be allowed, on their request, to be present at the daily medical inspections. They shall receive the attention which their state of health requires and, if necessary, shall be removed to the camp infirmary or to a hospital.

They shall have permission to read and write, likewise to send and receive letters. Parcels and remittances of money, however, may be withheld from them until the completion of the punishment; they shall meanwhile be entrusted to the prisoners' representative, who will hand over to the infirmary the perishable goods contained in such parcels.

III. JUDICIAL PROCEEDINGS

ARTICLE 99

No prisoner of war may be tried or sentenced for an act which is not forbidden by the law of the Detaining Power or by international law, in force at the time the said act was committed.

No moral or physical coercion may be exerted on a prisoner of war in order to induce him to admit himself guilty of the act of which he is accused.

No prisoner of war may be convicted without having had an opportunity to present his defense and the assistance of a qualified advocate or counsel.

ARTICLE 100

Prisoners of war and the Protecting Powers shall be informed as soon as possible of the offences which are punishable by the death sentence under the laws of the Detaining Power.

Other offences shall not thereafter be made punishable by the death penalty without the concurrence of the Power upon which the prisoners of war depend.

The death sentence cannot be pronounced on a prisoner of war unless the attention of the court has, in accordance with Article 87, second paragraph, been particularly called to the fact that since the accused is not a national of the Detaining Power, he is not bound to it by any duty of allegiance, and that he is in its power as the result of circumstances independent of his own will.

ARTICLE 101

If the death penalty is pronounced on a prisoner of war, the sentence shall not be executed before the expiration of a period of at least six months from the date when the Protecting Power receives, at an indicated address, the detailed communication provided for in Article 107.

ARTICLE 102

A prisoner of war can be validly sentenced only if the sentence has been pronounced by the same courts according to the same procedure as in the case of members of the armed forces of the Detaining Power, and if, furthermore, the provisions of the present Chapter have been observed.

ARTICLE 103

Judicial investigations relating to a prisoner of war shall be conducted as rapidly as circumstances permit and so that his trial shall take place as soon as possible. A prisoner of war shall not be confined while awaiting trial unless a member of the armed forces of the Detaining Power would be so confined if he were accused of a similar offence, or if it is essential to do so in the interests of national security. In no circumstances shall this confinement exceed three months.

Any period spent by a prisoner of war in confinement awaiting trial shall be deducted from any sentence of imprisonment passed upon him and taken into account in fixing any penalty.

The provisions of Articles 97 and 98 of this Chapter shall apply to a prisoner of war whilst in confinement awaiting trial.

ARTICLE 104

In any case in which the Detaining Power has decided to institute judicial proceedings against a prisoner of war, it shall notify the Protecting Power as soon as possible and at least three weeks before the opening of the trial. This period of three weeks shall run as from the day on which such notification reaches the Protecting Power at the address previously indicated by the latter to the Detaining Power.

The said notification shall contain the following information:

1. Surname and first names of the prisoner of war, his rank, his army, regimental, personal or serial number, his date of birth, and his profession or trade, if any;

2. Place of internment or confinement;

3. Specification of the charge or charges on which the prisoner of war is to be arraigned, giving the legal provisions applicable;

4 . Designation of the court which will try the case, likewise the date and place fixed for the opening of the trial.

The same communication shall be made by the Detaining Power to the prisoners' representative.

If no evidence is submitted, at the opening of a trial, that the notification referred to above was received by the Protecting Power, by the prisoner of war and by the prisoners' representative concerned, at least three weeks before the opening of the trial, then the latter cannot take place and must be adjourned.

ARTICLE 105

The prisoner of war shall be entitled to assistance by one of his prisoner comrades, to defense by a qualified advocate or counsel of his own choice, to the calling of witnesses and, if he deems necessary, to the services of a competent interpreter. He shall be advised of these rights by the Detaining Power in due time before the trial.

Failing a choice by the prisoner of war, the Protecting Power shall find him an advocate or counsel, and shall have at least one week at its disposal for the purpose. The Detaining Power shall deliver to the said Power, on request, a list of persons qualified to present the defense. Failing a choice of an advocate or counsel by the prisoner of war or the Protecting Power, the Detaining Power shall appoint a competent advocate or counsel to conduct the defense.

The advocate or counsel conducting the defense on behalf of the prisoner of war shall have at his disposal a period of two weeks at least before the opening of the trial, as well as the necessary facilities to prepare the defense of the accused. He may, in particular, freely visit the accused and interview him in private. He may also confer with any witnesses for the defense, including prisoners of war. He shall have the benefit of these facilities until the term of appeal or petition has expired.

Particulars of the charge or charges on which the prisoner of war is to be arraigned, as well as the documents which are generally communicated to the accused by virtue of the laws in force in the armed forces of the Detaining Power, shall be communicated to the accused prisoner of war in a language which he understands, and in good time before the opening of the trial. The same communication in the same circumstances shall be made to the advocate or counsel conducting the defense on behalf of the prisoner of war.

The representatives of the Protecting Power shall be entitled to attend the trial of the case, unless, exceptionally, this is held in camera in the interest of State security. In such a case the Detaining Power shall advise the Protecting Power accordingly.

ARTICLE 106

Every prisoner of war shall have, in the same manner as the members of the armed forces of the Detaining Power, the right of appeal or petition from any sentence pronounced upon him, with a view to the quashing or revising of the sentence or the reopening of the trial. He shall be fully informed of his right to appeal or petition and of the time limit within which he may do so.

ARTICLE 107

Any judgment and sentence pronounced upon a prisoner of war shall be immediately reported to the Protecting Power in the form of a summary communication, which shall also indicate whether he has the right of appeal with a view to the quashing of the sentence or the reopening of the trial. This communication shall likewise be sent to the prisoners' representative concerned. It shall also be sent to the accused prisoner of war in a language he understands, if the sentence was not pronounced in his presence. The Detaining Power shall also immediately communicate to the Protecting Power the decision of the prisoner of war to use or to waive his right of appeal.

Furthermore, if a prisoner of war is finally convicted or if a sentence pronounced on a prisoner of war in the first instance is a death sentence, the Detaining Power shall as soon as possible address to the Protecting Power a detailed communication containing:

1. The precise wording of the finding and sentence;

2. A summarized report of any preliminary investigation and of the trial, emphasizing in particular the elements of the prosecution and the defense;

3. Notification, where applicable, of the establishment where the sentence will be served.

The communications provided for in the foregoing subparagraphs shall be sent to the Protecting Power at the address previously made known to the Detaining Power.

ARTICLE 108

Sentences pronounced on prisoners of war after a conviction has become duly enforceable, shall be served in the same establishments and under the same conditions as in the case of members of the armed forces of the Detaining Power. These conditions shall in all cases conform to the requirements of health and humanity.

A woman prisoner of war on whom such a sentence has been pronounced shall be confined in separate quarters and shall be under the supervision of women.

In any case, prisoners of war sentenced to a penalty depriving them of their liberty shall retain the benefit of the provisions of Articles 78 and 126 of the present Convention. Furthermore, they shall be entitled to receive and dispatch correspondence, to receive at least one relief parcel monthly, to take regular exercise in the open air, to have the medical care required by their state of health, and the spiritual assistance they may desire. Penalties to which they may be subjected shall be in accordance with the provisions of Article 87, third paragraph.

PART IV TERMINATION OF CAPTIVITY

SECTION I DIRECT REPATRIATION AND ACCOMMODATION IN NEUTRAL COUNTRIES

ARTICLE 109

Subject to the provisions of the third paragraph of this Article, Parties to the conflict are bound to send back to their own country, regardless of number or rank, seriously wounded and seriously sick prisoners of war, after having cared for them until they are fit to travel, in accordance with the first paragraph of the following Article.

Throughout the duration of hostilities, Parties to the conflict shall endeavor, with the cooperation of the neutral Powers concerned, to make arrangements for the accommodation in neutral countries of the sick and wounded prisoners of war referred to in the second paragraph of the following Article. They may, in addition, conclude agreements with a view to the direct repatriation or internment in a neutral country of able-bodied prisoners of war who have undergone a long period of captivity.

No sick or injured prisoner of war who is eligible for repatriation under the first paragraph of this Article, may be repatriated against his will during hostilities.

ARTICLE 110

The following shall be repatriated direct:

1. Incurably wounded and sick whose mental or physical fitness seems to have been gravely diminished.

2. Wounded and sick who, according to medical opinion, are not likely to recover within one year, whose condition requires treatment and whose mental or physical fitness seems to have been gravely diminished.

3. Wounded and sick who have recovered, but whose mental or physical fitness seems to have been gravely and permanently diminished.

The following may be accommodated in a neutral country:

1. Wounded and sick whose recovery may be expected within one year of the date of the wound or the beginning of the illness, if treatment in a neutral country might increase the prospects of a more certain and speedy recovery.

2. Prisoners of war whose mental or physical health, according to medical opinion, is seriously threatened by continued captivity, but whose accommodation in a neutral country might remove such a threat.

The conditions which prisoners of war accommodated in a neutral country must fulfil in order to permit their repatriation shall be fixed, as shall likewise their status, by agreement between the Powers concerned. In general, prisoners of war who have been accommodated in a neutral country, and who belong to the following categories, should be repatriated:

1. Those whose state of health has deteriorated so as to fulfil the conditions laid down for direct repatriation;

2. Those whose mental or physical powers remain, even after treatment, considerably impaired.

If no special agreements are concluded between the Parties to the conflict concerned, to determine the cases of disablement or sickness entailing direct repatriation or accommodation in a neutral country, such cases shall be settled in accordance with the principles laid down in the Model Agreement concerning direct repatriation and accommodation in neutral countries of wounded and sick prisoners of war and in the Regulations concerning Mixed Medical Commissions annexed to the present Convention.

ARTICLE 111

The Detaining Power, the Power on which the prisoners of war depend, and a neutral Power agreed upon by these two Powers, shall endeavor to conclude agreements which will enable prisoners of war to be interned in the territory of the said neutral Power until the close of hostilities.

ARTICLE 112

Upon the outbreak of hostilities, Mixed Medical Commissions shall be appointed to examine sick and wounded prisoners of war, and to make all appropriate decisions regarding them. The appointment, duties and functioning of these Commissions shall be in conformity with the provisions of the Regulations annexed to the present Convention.

However, prisoners of war who, in the opinion of the medical authorities of the Detaining Power, are manifestly seriously injured or seriously sick, may be repatriated without having to be examined by a Mixed Medical Commission.

ARTICLE 113

Besides those who are designated by the medical authorities of the Detaining Power, wounded or sick prisoners of war belonging to the categories listed below shall be entitled to present themselves for examination by the Mixed Medical Commissions provided for in the foregoing Article:

1. Wounded and sick proposed by a physician or surgeon who is of the same nationality, or a national of a Party to the conflict allied with the Power on which the said prisoners depend, and who exercises his functions in the camp.

2. Wounded and sick proposed by their prisoners' representative.

3. Wounded and sick proposed by the Power on which they depend, or by an organization duly recognized by the said Power and giving assistance to the prisoners.

Prisoners of war who do not belong to one of the three foregoing categories may nevertheless present themselves for examination by Mixed Medical Commissions, but shall be examined only after those belonging to the said categories.

The physician or surgeon of the same nationality as the prisoners who present themselves for examination by the Mixed Medical Commission, likewise the prisoners' representative of the said prisoners, shall have permission to be present at the examination.

ARTICLE 114

Prisoners of war who meet with accidents shall, unless the injury is self-inflicted, have the benefit of the provisions of this Convention as regards repatriation or accommodation in a neutral country.

ARTICLE 115

No prisoner of war on whom a disciplinary punishment has been imposed and who is eligible for repatriation or for accommodation in a neutral country, may be kept back on the plea that he has not undergone his punishment.

Prisoners of war detained in connection with a judicial prosecution or conviction and who are designated for repatriation or accommodation in a neutral country, may benefit by such measures before the end of the proceedings or the completion of the punishment, if the Detaining Power consents.

Parties to the conflict shall communicate to each other the names of those who will be detained until the end of the proceedings or the completion of the punishment.

ARTICLE 116

The costs of repatriating prisoners of war or of transporting them to a neutral country shall be borne, from the frontiers of the Detaining Power, by the Power on which the said prisoners depend.

ARTICLE 117

No repatriated person may be employed on active military service.

SECTION II RELEASE AND REPATRIATION OF PRISONERS OF WAR AT THE CLOSE OF HOSTILITIES

ARTICLE 118

Prisoners of war shall be released and repatriated without delay after the cessation of active hostilities.

In the absence of stipulations to the above effect in any agreement concluded between the Parties to the conflict with a view to the cessation of hostilities, or failing any such agreement, each of the Detaining Powers shall itself establish and execute without delay a plan of repatriation in conformity with the principle laid down in the foregoing paragraph.

In either case, the measures adopted shall be brought to the knowledge of the prisoners of war.

The costs of repatriation of prisoners of war shall in all cases be equitably apportioned between the Detaining Power and the Power on which the prisoners depend. This apportionment shall be carried out on the following basis:

(a) If the two Powers are contiguous, the Power on which the prisoners of war depend shall bear the costs of repatriation from the frontiers of the Detaining Power.

(b) If the two Powers are not contiguous, the Detaining Power shall bear the costs of transport of prisoners of war over its own territory as far as its frontier or its port of embarkation nearest to the territory of the Power on which the prisoners of war depend. The Parties concerned shall agree between themselves as to the equitable apportionment of the remaining costs of the repatriation. The conclusion of this agreement shall in no circumstances justify any delay in the repatriation of the prisoners of war.

ARTICLE 119

Repatriation shall be effected in conditions similar to those laid down in Articles 46 to 48 inclusive of the present Convention for the transfer of prisoners of war, having regard to the provisions of Article 118 and to those of the following paragraphs.

On repatriation, any articles of value impounded from prisoners of war under Article 18, and any foreign currency which has not been converted into the currency of the Detaining Power, shall be restored to them. Articles of value and foreign currency which, for any reason whatever, are not restored to prisoners of war on repatriation, shall be dispatched to the Information Bureau set up under Article 122.

Prisoners of war shall be allowed to take with them their personal effects, and any correspondence and parcels which have arrived for them. The weight of such baggage may be limited, if the conditions of repatriation so require, to what each prisoner can reasonably carry. Each prisoner shall in all cases be authorized to carry at least twenty-five kilograms.

The other personal effects of the repatriated prisoner shall be left in the charge of the Detaining Power which shall have them forwarded to him as soon as it has concluded an agreement to this effect, regulating the conditions of transport and the payment of the costs involved, with the Power on which the prisoner depends.

Prisoners of war against whom criminal proceedings for an indictable offence are pending may be detained until the end of such proceedings, and, if necessary, until the completion of the punishment. The same shall apply to prisoners of war already convicted for an indictable offence.

Parties to the conflict shall communicate to each other the names of any prisoners of war who are detained until the end of the proceedings or until punishment has been completed.

By agreement between the Parties to the conflict, commissions shall be established for the purpose of searching for dispersed prisoners of war and of assuring their repatriation with the least possible delay.

SECTION III DEATH OF PRISONERS OF WAR

ARTICLE 120

Wills of prisoners of war shall be drawn up so as to satisfy the conditions of validity required by the legislation of their country of origin, which will take steps to inform the Detaining Power of its requirements in this respect. At the request of the prisoner of war and, in all cases, after death, the will shall be transmitted without delay to the Protecting Power; a certified copy shall be sent to the Central Agency.

Death certificates in the form annexed to the present Convention, or lists certified by a responsible officer, of all persons who die as prisoners of war shall be forwarded as rapidly as possible to the Prisoner of War Information Bureau established in accordance with Article 122. The death certificates or certified lists shall show particulars of identity as set out in the third paragraph of Article 17, and also the date and place of death, the cause of death, the date and place of burial and all particulars necessary to identify the graves.

The burial or cremation of a prisoner of war shall be preceded by a medical examination of the body with a view to confirming death and enabling a report to be made and, where necessary, establishing identity.

The detaining authorities shall ensure that prisoners of war who have died in captivity are honorably buried, if possible according to the rites of the religion to which they belonged, and that their graves are respected, suitably maintained and marked so as to be found at any time. Wherever possible, deceased prisoners of war who depended on the same Power shall be interred in the same place.

Deceased prisoners of war shall be buried in individual graves unless unavoidable circumstances require the use of collective graves. Bodies may be cremated only for imperative reasons of hygiene, on account of the religion of the deceased or in accordance with his express wish to this effect. In case of cremation, the fact shall be stated and the reasons given in the death certificate of the deceased.

In order that graves may always be found, all particulars of burials and graves shall be recorded with a Graves Registration Service established by the Detaining Power. Lists of graves and particulars of the prisoners of war interred in cemeteries and elsewhere shall be transmitted to the Power on which such prisoners of war depended. Responsibility for the care of these graves and for records of any subsequent moves of the bodies shall rest on the Power controlling the territory, if a Party to the present Convention. These provisions shall also apply to the ashes, which shall be kept by the Graves Registration Service until proper disposal thereof in accordance with the wishes of the home country.

ARTICLE 121

Every death or serious injury of a prisoner of war caused or suspected to have been caused by a sentry, another prisoner of war, or any other person, as well as any death the cause of which is unknown, shall be immediately followed by an official enquiry by the Detaining Power.

A communication on this subject shall be sent immediately to the Protecting Power. Statements shall be taken from witnesses, especially from those who are prisoners of war, and a report including such statements shall be forwarded to the Protecting Power.

If the enquiry indicates the guilt of one or more persons, the Detaining Power shall take all measures for the prosecution of the person or persons responsible.

PART V INFORMATION BUREAU AND RELIEF SOCIETIES FOR PRISONERS OF WAR

ARTICLE 122

Upon the outbreak of a conflict and in all cases of occupation, each of the Parties to the conflict shall institute an official Information Bureau for prisoners of war who are in its power. Neutral or non-belligerent Powers who may have received within their territory persons belonging to one of the categories referred to in Article 4, shall take the same action with respect to such persons. The Power concerned shall ensure that the Prisoners of War Information Bureau is provided with the necessary accommodation, equipment and staff to ensure its efficient working. It shall be at liberty to employ prisoners of war in such a Bureau under the conditions laid down in the Section of the present Convention dealing with work by prisoners of war.

Within the shortest possible period, each of the Parties to the conflict shall give its Bureau the information referred to in the fourth, fifth and sixth paragraphs of this Article regarding any enemy person belonging to one of the categories referred to in Article 4, who has fallen into its power. Neutral or non-belligerent Powers shall take the same action with regard to persons belonging to such categories whom they have received within their territory.

The Bureau shall immediately forward such information by the most rapid means to the Powers concerned, through the intermediary of the Protecting Powers and likewise of the Central Agency provided for in Article 123.

This information shall make it possible quickly to advise the next of kin concerned. Subject to the provisions of Article 17, the information shall include, in so far as available to the Information Bureau, in respect of each prisoner of war, his surname, first names, rank, army, regimental, personal or serial number, place and full date of birth, indication of the Power on which he depends, first name of the father and maiden name of the mother, name and address of the person to be informed and the address to which correspondence for the prisoner may be sent.

The Information Bureau shall receive from the various departments concerned information regarding transfers, releases, repatriations, escapes, admissions to hospital, and deaths, and shall transmit such information in the manner described in the third paragraph above.

Likewise, information regarding the state of health of prisoners of war who are seriously ill or seriously wounded shall be supplied regularly, every week if possible.

The Information Bureau shall also be responsible for replying to all inquiries sent to it concerning prisoners of war, including those who have died in captivity; it will make any inquiries necessary to obtain the information which is asked for if this is not in its possession.

All written communications made by the Bureau shall be authenticated by a signature or a seal.

The Information Bureau shall furthermore be charged with collecting all personal valuables, including sums in currencies other than that of the Detaining Power and documents of importance to the next of kin, left by prisoners of war who have been repatriated or released, or who have escaped or died, and shall forward the said valuables to the Powers concerned. Such articles shall be sent by the Bureau in sealed packets which shall be accompanied by statements giving clear and full particulars of the identity of the person to whom the articles belonged, and by a complete list of the contents of the parcel. Other personal effects of such prisoners of war shall be transmitted under arrangements agreed upon between the Parties to the conflict concerned.

ARTICLE 123

A Central Prisoners of War Information Agency shall be created in a neutral country. The International Committee of the Red Cross shall, if it deems necessary, propose to the Powers concerned the organization of such an Agency.

The function of the Agency shall be to collect all the information it may obtain through official or private channels respecting prisoners of war, and to transmit it as rapidly as possible to the country of origin of the prisoners of war or to the Power on which they depend. It shall receive from the Parties to the conflict all facilities for effecting such transmissions.

The High Contracting Parties, and in particular those whose nationals benefit by the services of the Central Agency, are requested to give the said Agency the financial aid it may require.

The foregoing provisions shall in no way be interpreted as restricting the humanitarian activities of the International Committee of the Red Cross, or of the relief Societies provided for in Article 125.

ARTICLE 124

The national Information Bureau and the Central Information Agency shall enjoy free postage for mail, likewise all the exemptions provided for in Article 74, and further, so far as possible, exemption from telegraphic charges or, at least, greatly reduced rates.

ARTICLE 125

Subject to the measures which the Detaining Powers may consider essential to ensure their security or to meet any other reasonable need, the representatives of religious organizations, relief societies, or any other organization assisting prisoners of war, shall receive from the said Powers, for themselves and their duly accredited agents, all necessary facilities for visiting the prisoners, distributing relief supplies and material, from any source, intended for religious, educational or recreative purposes, and for assisting them in organizing their leisure time within the camps. Such societies or organizations may be constituted in the territory of the Detaining Power or in any other country, or they may have an international character.

The Detaining Power may limit the number of societies and organizations whose delegates are allowed to carry out their activities in its territory and under its supervision, on condition, however, that such limitation shall not hinder the effective operation of adequate relief to all prisoners of war.

The special position of the International Committee of the Red Cross in this field shall be recognized and respected at all times.

As soon as relief supplies or material intended for the above-mentioned purposes are handed over to prisoners of war, or very shortly afterwards, receipts for each consignment, signed by the prisoners' representative, shall be forwarded to the relief society or organization making the shipment. At the same time, receipts for these consignments shall be supplied by the administrative authorities responsible for guarding the prisoners.

PART VI EXECUTION OF THE CONVENTION

SECTION I GENERAL PROVISIONS

ARTICLE 126

Representatives or delegates of the Protecting Powers shall have permission to go to all places where prisoners of war may be, particularly to places of internment, imprisonment and labor, and shall have access to all premises occupied by prisoners of war; they shall also be allowed to go to the places of departure, passage and arrival of prisoners who are being transferred. They shall be able to interview the prisoners, and in particular the prisoners' representatives, without witnesses, either personally or through an interpreter.

Representatives and delegates of the Protecting Powers shall have full liberty to select the places they wish to visit. The duration and frequency of these visits shall not be restricted. Visits may not be prohibited except for reasons of imperative military necessity, and then only as an exceptional and temporary measure.

The Detaining Power and the Power on which the said prisoners of war depend may agree, if necessary, that compatriots of these prisoners of war be permitted to participate in the visits.

The delegates of the International Committee of the Red Cross shall enjoy the same prerogatives. The appointment of such delegates shall be submitted to the approval of the Power detaining the prisoners of war to be visited.

ARTICLE 127

The High Contracting Parties undertake, in time of peace as in time of war, to disseminate the text of the present Convention as widely as possible in their respective countries, and, in particular, to include the study thereof in their programs of military and, if possible, civil instruction, so that the principles thereof may become known to all their armed forces and to the entire population.

Any military or other authorities, who in time of war assume responsibilities in respect of prisoners of war, must possess the text of the Convention and be specially instructed as to its provisions.

ARTICLE 128

The High Contracting Parties shall communicate to one another through the Swiss Federal Council and, during hostilities, through the Protecting Powers, the official translations of the

present Convention, as well as the laws and regulations which they may adopt to ensure the application thereof.

ARTICLE 129

The High Contracting Parties undertake to enact any legislation necessary to provide effective penal sanctions for persons committing, or ordering to be committed, any of the grave breaches of the present Convention defined in the following Article.

Each High Contracting Party shall be under the obligation to search for persons alleged to have committed, or to have ordered to be committed, such grave breaches, and shall bring such persons, regardless of their nationality, before its own courts. It may also, if it prefers, and in accordance with the provisions of its own legislation, hand such persons over for trial to another High Contracting Party concerned, provided such High Contracting Party has made out a prima facie case.

Each High Contracting Party shall take measures necessary for the suppression of all acts contrary to the provisions of the present Convention other than the grave breaches defined in the following Article.

In all circumstances, the accused persons shall benefit by safeguards of proper trial and defense, which shall not be less favorable than those provided by Article 105 and those following of the present Convention.

ARTICLE 130

Grave breaches to which the preceding Article relates shall be those involving any of the following acts, if committed against persons or property protected by the Convention: willful killing, torture or inhuman treatment, including biological experiments, willfully causing great suffering or serious injury to body or health, compelling a prisoner of war to serve in the forces of the hostile Power, or willfully depriving a prisoner of war of the rights of fair and regular trial prescribed in this Convention.

ARTICLE 131

No High Contracting Party shall be allowed to absolve itself or any other High Contracting Party of any liability incurred by itself or by another High Contracting Party in respect of breaches referred to in the preceding Article.

ARTICLE 132

At the request of a Party to the conflict, an enquiry shall be instituted, in a manner to be decided between the interested Parties, concerning any alleged violation of the Convention.

If agreement has not been reached concerning the procedure for the enquiry, the Parties should agree on the choice of an umpire who will decide upon the procedure to be followed.

Once the violation has been established, the Parties to the conflict shall put an end to it and shall repress it with the least possible delay.

SECTION II FINAL PROVISIONS

ARTICLE 133

The present Convention is established in English and in French. Both texts are equally authentic. The Swiss Federal Council shall arrange for official translations of the Convention to be made in the Russian and Spanish languages.

ARTICLE 134

The present Convention replaces the Convention of 27 July 1929, in relations between the High Contracting Parties.

ARTICLE 135

In the relations between the Powers which are bound by The Hague Convention respecting the Laws and Customs of War on Land, whether that of July 29, 1899, or that of October 18, 1907, and which are parties to the present Convention, this last Convention shall be complementary to Chapter II of the Regulations annexed to the above-mentioned Conventions of The Hague.

ARTICLE 136

The present Convention, which bears the date of this day, is open to signature until February 12, 1950, in the name of the Powers represented at the Conference which opened at Geneva on April 21, 1949; furthermore, by Powers not represented at that Conference, but which are parties to the Convention of July 27, 1929.

ARTICLE 137

The present Convention shall be ratified as soon as possible and the ratifications shall be deposited at Berne.

A record shall be drawn up of the deposit of each instrument of ratification and certified copies of this record shall be transmitted by the Swiss Federal Council to all the Powers in whose name the Convention has been signed, or whose accession has been notified.

ARTICLE 138

The present Convention shall come into force six months after not less than two instruments of ratification have been deposited.

Thereafter, it shall come into force for each High Contracting Party six months after the deposit of the instrument of ratification.

ARTICLE 139

From the date of its coming into force, it shall be open to any Power in whose name the present Convention has not been signed, to accede to this Convention.

ARTICLE 140

Accessions shall be notified in writing to the Swiss Federal Council, and shall take effect six months after the date on which they are received.

The Swiss Federal Council shall communicate the accessions to all the Powers in whose name the Convention has been signed, or whose accession has been notified.

ARTICLE 141

The situations provided for in Articles 2 and 3 shall give immediate effect to ratifications deposited and accessions notified by the Parties to the conflict before or after the beginning of hostilities or occupation. The Swiss Federal Council shall communicate by the quickest method any ratifications or accessions received from Parties to the conflict.

ARTICLE 142

Each of the High Contracting Parties shall be at liberty to denounce the present Convention.

The denunciation shall be notified in writing to the Swiss Federal Council, which shall transmit it to the Governments of all the High Contracting Parties.

The denunciation shall take effect one year after the notification thereof has been made to the Swiss Federal Council. However, a denunciation of which notification has been made at a time when the denouncing Power is involved in a conflict shall not take effect until peace has been concluded, and until after operations connected with the release and repatriation of the persons protected by the present Convention have been terminated.

The denunciation shall have effect only in respect of the denouncing Power. It shall in no way impair the obligations which the Parties to the conflict shall remain bound to fulfill by virtue of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity and the dictates of the public conscience.

ARTICLE 143

The Swiss Federal Council shall register the present Convention with the Secretariat of the United Nations. The Swiss Federal Council shall also inform the Secretariat of the United Nations of all ratifications, accessions and denunciations received by it with respect to the present Convention.

IN WITNESS WHEREOF the undersigned, having deposited their respective full powers, have signed the present Convention.

DONE at Geneva this twelfth day of August 1949, in the English and French languages. The original shall be deposited in the Archives of the Swiss Confederation. The Swiss Federal Council shall transmit certified copies thereof to each of the signatory and acceding States.

SECTION II. GENEVA CONVENTIONS RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR (FOURTH GENEVA CONVENTION)

The following excerpted articles from the Geneva Conventions contain requirements concerning the treatment of civilians during time of war. Violations of these articles can constitute war crimes and should be treated as such.

PART I

GENERAL PROVISIONS

Article 1

The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances.

Article 2

In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.

Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof.

Article 3

In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions:

1. Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria.

To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:

(a) Violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;

(b) Taking of hostages;

(c) Outrages upon personal dignity, in particular humiliating and degrading treatment;

(d) The passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.

2. The wounded and sick shall be collected and cared for.

An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict.

The Parties to the conflict should further endeavour to bring into force, by means of special agreements, all or part of the other provisions of the present Convention.

The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.

Article 4

Persons protected by the Convention are those who, at a given moment and in any manner whatsoever, find themselves, in case of a conflict or occupation, in the hands of a Party to the conflict or Occupying Power of which they are not nationals.
Nationals of a State which is not bound by the Convention are not protected by it.

Nationals of a neutral State who find themselves in the territory of a belligerent State, and nationals of a co-belligerent State, shall not be regarded as protected persons while the State of which they are nationals has normal diplomatic representation in the State in whose hands they are.

The provisions of Part II are, however, wider in application, as defined in Article 13.

Persons protected by the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of August 12, 1949, or by the Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of August 12, 1949, or by the Geneva Convention relative to the Treatment of Prisoners of War of August 12, 1949, shall not be considered as protected persons within the meaning of the present Convention.

Article 5

Where, in the territory of a Party to the conflict, the latter is satisfied that an individual protected person is definitely suspected of or engaged in activities hostile to the security of the State, such individual person shall not be entitled to claim such rights and privileges under the present Convention as would, if exercised in the favour of such individual person, be prejudicial to the security of such State.

Where in occupied territory an individual protected person is detained as a spy or saboteur, or as a person under definite suspicion of activity hostile to the security of the Occupying Power, such person shall, in those cases where absolute military security so requires, be regarded as having forfeited rights of communication under the present Convention.

In each case, such persons shall nevertheless be treated with humanity, and in case of trial, shall not be deprived of the rights of fair and regular trial prescribed by the present Convention. They shall also be granted the full rights and privileges of a protected person under the present Convention at the earliest date consistent with the security of the State or Occupying Power, as the case may be.

Article 25

All persons in the territory of a Party to the conflict, or in a territory occupied by it, shall be enabled to give news of a strictly personal nature to members of their families, wherever they may be, and to receive news from them. This correspondence shall be forwarded speedily and without undue delay.

If, as a result of circumstances, it becomes difficult or impossible to exchange family correspondence by the ordinary post, the Parties to the conflict concerned shall apply to a neutral intermediary, such as the Central Agency provided for in Article 140, and shall decide in consultation with it how to ensure the fulfillment of their obligations under the best possible conditions, in particular with the cooperation of the National Red Cross (Red Crescent, Red Lion and Sun) Societies.

If the Parties to the conflict deem it necessary to restrict family correspondence, such restrictions shall be confined to the compulsory use of standard forms containing twenty-five freely chosen words, and to the limitation of the number of these forms dispatched to one each month.

PART III

STATUS AND TREATMENT OF PROTECTED PERSONS

SECTION I

PROVISIONS COMMON TO THE TERRITORIES OF THE PARTIES
TO THE CONFLICT AND TO OCCUPIED TERRITORIES

Article 27

Protected persons are entitled, in all circumstances, to respect for their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs. They shall at all times be humanely treated, and shall be protected especially against all acts of violence or threats thereof and against insults and public curiosity.

Women shall be especially protected against any attack on their honour, in particular against rape, enforced prostitution, or any form of indecent assault.

Without prejudice to the provisions relating to their state of health, age and sex, all protected persons shall be treated with the same consideration by the Party to the conflict in whose power they are, without any adverse distinction based, in particular, on race, religion or political opinion.

However, the Parties to the conflict may take such measures of control and security in regard to protected persons as may be necessary as a result of the war.

Article 28

The presence of a protected person may not be used to render certain points or areas immune from military operations.

Article 29

The Party to the conflict in whose hands protected persons may be is responsible for the treatment accorded to them by its agents, irrespective of any individual responsibility which may be incurred.

Article 30

Protected persons shall have every facility for making application to the Protecting Powers, the International Committee of the Red Cross, the National Red Cross (Red Crescent, Red Lion and Sun) Society of the country where they may be, as well as to any organization that might assist them.

These several organizations shall be granted all facilities for that purpose by the authorities, within the bounds set by military or security considerations.

Apart from the visits of the delegates of the Protecting Powers and of the International Committee of the Red Cross, provided for by Article 143, the Detaining or Occupying Powers shall facilitate as much as possible visits to protected persons by the representatives of other organizations whose object is to give spiritual aid or material relief to such persons.

Article 31

No physical or moral coercion shall be exercised against protected persons, in particular to obtain information from them or from third parties.

Article 32

The High Contracting Parties specifically agree that each of them is prohibited from taking any measure of such a character as to cause the physical suffering or extermination of protected persons in their hands. This prohibition applies not only to murder, torture, corporal punishment, mutilation and medical or scientific experiments not necessitated by the medical treatment of a protected person but also to any other measures of brutality whether applied by civilian or military agents.

Article 33

No protected person may be punished for an offence he or she has not personally committed. Collective penalties and likewise all measures of intimidation or of terrorism are prohibited.

Pillage is prohibited.

Reprisals against protected persons and their property are prohibited.

Article 34

The taking of hostages is prohibited.

SECTION II

ALIENS IN THE TERRORITY OF A PARTY TO THE CONFLICT

Article 41

Should the Power in whose hands protected persons may be consider the measures of control mentioned in the present Convention to be inadequate, it may not have recourse to any other measure of control more severe than that of assigned residence or internment, in accordance with the provisions of Articles 42 and 43.

In applying the provisions of Article 39, second paragraph, to the cases of persons required to leave their usual places of residences by virtue of a decision placing them in assigned residence elsewhere, the Detaining Power shall be guided as closely as possible by the standards of welfare set forth in Part III, Section IV of this Convention.

Article 42

The internment or placing in assigned residence of protected persons may be ordered only if the security of the Detaining Power makes it absolutely necessary.

If any person, acting through the representatives of the Protecting Power, voluntarily demands internment, and if his situation renders this step necessary, he shall be interned by the Power in whose hands he may be.

Article 43

Any protected person who has been interned or placed in assigned residence shall be entitled to have such action reconsidered as soon as possible by an appropriate court or administrative board designated by the Detaining Power for that purpose. If the internment or placing in assigned residence is maintained, the court or administrative board shall periodically, and at least twice yearly, give consideration to his or her case, with a view to the favourable amendment of the initial decision, if circumstances permit.

Unless the protected persons concerned object, the Detaining Power shall, as rapidly as possible, give the Protecting Power the names of any protected persons who have been interned or subjected to assigned residence, or who have been released from internment or assigned residence. The decisions of the courts or boards mentioned in the first paragraph of the present Article shall also, subject to the same conditions, be notified as rapidly as possible to the Protecting Power.

Article 44

In applying the measures of control mentioned in the present Convention, the Detaining Power shall not treat as enemy aliens exclusively on the basis of their nationality de jure of an enemy State, refugees who do not, in fact, enjoy the protection of any government.

Appendix B

Source and Information Reliability Matrix

SOURCE RELIABILITY

B-1. Reliability ratings range from "Reliable" (A) to "Unreliable" (E) as shown in Table B-1. In every instance the rating is based on previous reporting from that source. If there has been no previous reporting, the source must be rated as "F". [NOTE: An "F" rating does not necessarily mean that the source cannot be trusted, but that there is no reporting history and therefore no basis for making a determination.]

Table B-1. Evaluation of Source Reliability.

A	**Reliable**	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability
B	**Usually Reliable**	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	**Fairly Reliable**	**Doubt** of authenticity, trustworthiness, or competency but has provided valid information in the past
D	**Not Usually Reliable**	**Significant doubt** about authenticity, trustworthiness, or competency but has provided valid information in the past
E	**Unreliable**	**Lacking** in authenticity, trustworthiness, and competency; history of invalid information
F	**Cannot Be Judged**	**No basis** exists for evaluating the reliability of the source

INFORMATION CONTENT

B-2. The highest degree of confidence in reported information is given to that which has been confirmed by outside sources, "1". Table B-2 shows evaluation of information content. The degree of confidence decreases if the information is not confirmed, and/or does not seem to make sense. The lowest evaluated rating of "5" means that the information is considered to be false. [NOTE: A rating of "6" does not necessarily mean false information, but is generally used to indicate that no determination can be made since the information is completely new.]

Table B-2. Evaluation of Information Content.

1	**Confirmed**	**Confirmed** by other independent sources; **logical** in itself; **Consistent** with other information on the subject
2	**Probably True**	Not confirmed; **logical** in itself; **consistent** with other information on the subject
3	**Possibly True**	Not confirmed; **reasonably logical** in itself; **agrees with some** other information on the subject
4	**Doubtfully True**	Not confirmed; possible but **not logical**; **no other information** on the subject
5	**Improbable**	Not confirmed; **not logical** in itself; **contradicted** by other information on the subject
6	**Cannot Be Judged**	**No basis** exists for evaluating the validity of the information

Appendix C

Pre-Deployment Planning

HUMINT leaders must anticipate, identify, consider, and evaluate all potential threats. They must take advantage of enhanced information flow through hierarchical and nonhierarchical networks (computer, communications, and personnel). HCTs should—

- Review available databases on assigned contingency AOIs; review existing IPB products, conduct IPB on these AOIs; and develop appropriate IPB products. Information on databases created for specific contingencies can be gotten from the J2X.
- Continually monitor and update their OPLANs to reflect the evolving situation.
- Be aware of higher headquarters SOPs and DIA manuals for specific ISR management guidance.
- Prepare and practice an intelligence "surge" on likely contingency crises.
- Prepare and practice coordination from pre-deployment through redeployment with personnel from HUMINT, IMINT, MASINT, SIGINT, CA, PSYOP, SOF units, MP, and Engineers.
- Plan for requirements to support 24-hour operations: automation, communications capacity, and personnel necessary to provide continuous intelligence information collection and RM, processing, and reporting.
- Plan and coordinate for linguistic support.
- Forward all RFIs to higher headquarters in accordance with SOPs.
- Prepare and practice coordination with units they will support during pre-deployment exercises. Liaison must be conducted with commanders, S2s, administrative support personnel, logistical support personnel, communications personnel, and others. Obtain supported unit's briefing slide formats.
- Obtain copies of the supported unit's SOPs and ensure all team members are aware of the procedures governing HUMINT interface.
- Ensure that team data processing equipment is compatible with the supported unit's network structure and that appropriate interfaces are available.
- Exercise unit deployment SOPs, load plans, and packing lists.

Helpful Unclassified Links:

- https://portal.rccb.osis.gov/index.jsp Foreign Broadcast Information Service home page.
- http://wnc.fedworld.gov/ International news compiled by the US Department of Commerce.

- http://www.state.gov/s/inr/ Department of State's Bureau of Intelligence and Research home page. Contains country and region-specific information, policies, and warnings.
- http://ebird.afis.osd.mil/ Early Bird News Service of the Armed Forces Information Service.
- http://164.214.2.59/ National Geospatial-Intelligence Agency (NGA) (formerly National Imagery and Mapping Agency).
- http://memory.loc.gov/frd/cs/cshome.html#toc Country Studies from the Federal Research Division of the Library of Congress.

Appendix D

S2 Guide for Handling Detainees, Captured Enemy Documents, and Captured Enemy Equipment

D-1. Detainees, retained personnel, CEDs, and CEE are critical sources of combat intelligence. Often the Maneuver Battalion S2 is the first MI officer to encounter these sources. His actions are critical to the exploitation system. Information from these items is time sensitive, and these information sources need to be exploited at as low an echelon as possible. The S2 should anticipate requirements for support based on planned missions and request HUMINT collector support as necessary. If unable to receive HUMINT collector support, the S2 must be prepared to exploit these sources of information to the best of his ability and more importantly expedite their evacuation to locations and units where they can be exploited.

PURPOSE

D-2. This guide is for battalion and brigade S2s. It explains standard procedures on what the S2 should do when his unit—

- Captures an enemy soldier or other detainee.
- Encounters a civilian on the battlefield.
- Finds or captures an enemy document.
- Discovers an unusual enemy weapon or other unusual piece of equipment during tactical operations.

PERSONNEL HANDLING

D-3. The GPW defines persons entitled to treatment as prisoners of war upon capture, in Article 4 (see Appendix A, Section I).

D-4. The GC defines the civilian population (exclusive of those civilian persons listed in GPW, Article 4) who benefit to varying degrees from the provisions of the Geneva Conventions. (See Appendix A, Sections II and III.)

D-5. Persons in each of these categories have distinct rights, duties, and restrictions. Persons who are not members of the Armed Forces, as defined in Article 4, GPW, who bear arms or engage in other conduct hostile to the enemy thereby deprive themselves of many of the privileges attaching to the members of the civilian population. The capturing unit treats all combatants and noncombatants who are suspected of being part of the threat force as EPWs or retained personnel until their status can be determined. This determination normally occurs at the detainee collection point or at a higher echelon. Noncombatants are handled, questioned, detained, evacuated, and released in accordance with theater policy. In all cases, detainees are treated humanely.

D-6. Detainees are treated humanely but with firmness at all times. High standards of discipline are required not only of detainees but also of capturing and escort forces. Fraternization with detainees or mistreatment or abuse of them is not only a violation but also is not conducive to good discipline. In addition to not being conducive to good discipline, the mistreatment or abuse of detainees is a violation of the UCMJ for which violators may be punished. The control of detainees is exercised through the issuance and firm enforcement of necessary instructions in their own language. Instructions relating to their control during evacuation from the combat zone should be as brief as possible. Care must be taken to ensure that detainees have a clear understanding of all instructions to them.

D-7. At the capture point, the capturing element performs the following steps on detainees. The senior soldier will ensure that the steps are performed. The steps are referred to as the "Five S's and a T".

STEP 1. SEARCH

D-8. The capturing unit's first job is to disarm, search, and maintain positive control over all detainees. The detainees are disarmed and searched for concealed weapons and for equipment and documents of particular intelligence value immediately upon capture, unless the number of detainees captured, enemy action, or other circumstances make such a search impracticable. Until each detainee is searched, the responsible forces must be alert to prevent the use of concealed weapons or destruction of documents or equipment.

D-9. The capturing unit gathers all loose CEDs and CEE in the area. Identification documents and protective military equipment such as helmets or NBC gear stay with the detainee unless otherwise directed by the battalion S2.

- Equipment. Items of personal or individual equipment that are new or appear to be of a type not previously observed may be of intelligence value and should be processed and reported in accordance with the unit's SOP, specific evacuation instructions in Annex B (Intelligence) of the OPORD, and theater policy. Equipment for personal protection such as protective masks or protective clothing may not be taken unless replaced with equivalent equipment.
- Documents. A CED is any piece of recorded information that has been in the hands of the enemy. CEDs include but are not limited to maps, sketches, photographs, orders, tactical and technical manuals and instructions, code books, log books, maintenance records, shipping and packing slips and lists, war and field diaries, personal diaries, pay books, newspapers, service records, postal savings books, payrolls, postcards and letters, and any written, printed, engraved, or photographic matter that may contain information relative to the enemy and to weather and terrain data. A capturing unit is normally not able to accurately determine the potential intelligence value of any documents found on the detainee. It is therefore normally expedient to remove all documents, with the exception of the detainee's primary identification document. These documents are sealed in a waterproof

container and tagged with part C of the capture tag. If capture tags are not available, the document bag must be marked at a minimum to identify the detainee to whom the documents belong (see Appendix I).

- Personal effects. Except as provided in Step 1, detainees should be permitted to retain all of their personal effects including money; valuables; protective equipment, such as helmets, protective masks, and like items; effects and articles used for clothing or eating, except knives and forks; identification cards or tags; badges of grade and nationality; and articles having a personal or sentimental value. When items of equipment issued for the personal protection of detainees are taken from them, they must be replaced with equivalent items serving the same purpose. Although money and other valuables may be taken from detainees as a security measure, they must then be receipted for and a record thereof maintained in a special register. These administrative steps normally are not practical to accomplish prior to arrival of the detainee at an EPW camp.

STEP 2. SILENCE

D-10. Detainees are kept silent so that they cannot plan deception or encourage each other to resist. Keeping the detainees silent also prevents them from relieving the stress and shock of capture by talking with others. If the shock of capture is preserved, HUMINT collectors can take advantage of it in an approach. The capturing unit instructs or signals the detainees to be silent. If that does not work, the detainee is gagged. Guards give orders to detainees, but do not converse with them or give them any comfort items.

STEP 3. SAFEGUARD

D-11. All detainees are promptly evacuated out of the "danger" zone. Their presence may not be used to render points or areas immune to attack, nor should they be retained for participation in psychological warfare or other activities. The capturing forces must protect detainees from reprisals. Detainees will not be denied food, potable water, or appropriate clothing and shelter. Necessary medical attention will not be delayed. Those detainees held in an area should be provided protective facilities and equipment and should be oriented as to procedures to be followed in case of chemical, biological, and radiological agent attack.

STEP 4. SEGREGATE

D-12. The capturing unit separates officers from enlisted, senior from junior, male from female, and civilian from military within their capabilities to both guard and safeguard the detainees. (Physical segregation at this point is not always possible.) Deserters and people of different nationalities and ideologies should be further segregated. The capturing unit prepares a capture tag and puts one on each detainee (see Figure D-1). Tagging procedures are discussed in paragraph D-16.

STEP 5. SPEED TO THE REAR

D-13. The capturing unit moves detainees and CEDs to the unit supply point or other area where transportation to the rear is available for evacuation. Evacuation of detainees from the combat zone should be effected within the minimum time after capture. While in the combat zone, not only may detainees become casualties as the result of enemy fire but also the fluidity of operations, the wide dispersion of units, and the austerity of facilities may necessitate their rapid evacuation.

D-14. The normal evacuation channel is from the detainee collection point through intermediate detainee holding areas to an internment facility at a higher echelon. Available returning transportation, however, may bypass any intermediate detainee holding area and proceed directly to a corps or theater internment facility. Detainees will then be processed directly into the corps or theater internment facility. Evacuation may be by foot, vehicle, rail, aircraft, or ship. Evacuate detainees who are litter patients through medical channels.

D-15. The command (brigade and above) from which the detainees are being evacuated is responsible to provide transportation and rations and for coordinating all other matters related to the evacuation. Escort guards are furnished by the command (division and above) to which the detainees are being evacuated.

STEP 6. TAG

D-16. When the detainees have been searched and segregated, the capturing unit prepares a capture tag and puts one on each detainee. It is very important that the capturing unit fill out the Capture Tag as accurately and completely as possible. HUMINT collectors will use the information from the tag when preparing to interrogate detainees. The "capturing unit" and "location of capture" information will be used to provide direct feedback to the capturing unit when information of immediate tactical value is obtained. Each EPW tag has a different serial number used for the purpose of accountability and cannot be reproduced. The EPW tag is perforated into three parts: Part A is attached to the detainee, Part B is retained by the capturing unit, and Part C is attached to the detainee's property (see Figure D-1).

DOCUMENT HANDLING

DOCUMENTS FOUND ON ENEMY PRISONER OF WAR

D-17. The battalion S2 and subordinate unit commander ensure that CEDs found on detainees are handled as follows. The capturing unit will—

- Search each detainee.
- Return identification documents to detainees. It may be preferable to return only one identity document, to preclude the detainee from spreading extras around to cause confusion. The preferred ID document to return to the detainee is a picture ID (such as a military

or government ID card). If the detainee has several identification documents, the S2 returns the ID that most accurately reflects the detainee's official status. This might be a military ID for a soldier and a passport or government-issue ID for a civilian. If the detainee has several identification documents with different names, this may be an indicator of CI interest. The S2 notifies the nearest CI unit.

- Write the following on the top and bottom half of the EPW capture tag: Number of documents taken, date and time, location and circumstances of capture, capturing unit's designation.
- Put CEDs in a waterproof bag, one per detainee.
- Affix Part C of the capture tag to the bag.
- Give CEDs to the senior escort.
- Direct the senior escort to evacuate CEDs with the detainee.

DOCUMENTS FOUND IN THE AO

D-18. An example of CEDs found in the AO is paperwork discovered in an overrun CP, but not on a detainee. The capturing unit will—

- Put CEDs in a waterproof bag.
- Follow the same procedures described above, and tag the bag.
- Evacuate the CEDs to the battalion S2.
- Evacuate all CEDs as dictated by Annex B of the OPORD. This is normally through the MI chain (for example, from Battalion S2 to Brigade S2, to the first HUMINT collection or DOCEX unit in the MI chain). The S2 normally coordinates with the S4 for the use of supply vehicles returning empty to the rear for the transportation of large numbers of documents.

INITIAL DOCUMENT EXPLOITATION

D-19. A combat unit without language-qualified personnel can perform limited battlefield DOCEX, mainly on maps and overlays. The unit S2 is normally responsible for any initial exploitation by the capturing unit. The S2 safeguards the items pending disposition. At the same time he—

- Looks over the document.
- Does not mark or harm it in anyway.
- Uses whatever resources are available to decipher it; for example, dictionaries and enemy map symbol guides.
- Looks for information that has a direct bearing on his current mission.

D-20. The S2 extracts the combat information and uses the SALUTE format as a template to organize the information.

EQUIPMENT HANDLING PROCEDURES

D-21. CEE includes all types of foreign materiel found on a detainee or in the AO that may have military application. The capturing unit—

- Always permits the detainee to keep protective equipment and equipment for his personal well being unless this gear is replaced by equivalent items by the capturing unit. This equipment includes helmet, NBC gear, mess gear (excluding knife and fork).
- Disposes of equipment in accordance with unit SOPs and instructions in Annex B of the OPORD. Most routine equipment is normally destroyed in place. Unusual or new equipment or equipment identified as being of TECHINT interest is tagged with a CEE tag (Part C of DD Form 2745) and evacuated to the nearest TECHINT unit. Communications equipment is also tagged and evacuated to the nearest SIGINT unit.
- Identifies equipment that cannot be easily evacuated; its location is passed through intelligence channels to the nearest unit that will be involved in its exploitation.

FIELD-EXPEDIENT TAGGING PROCEDURES

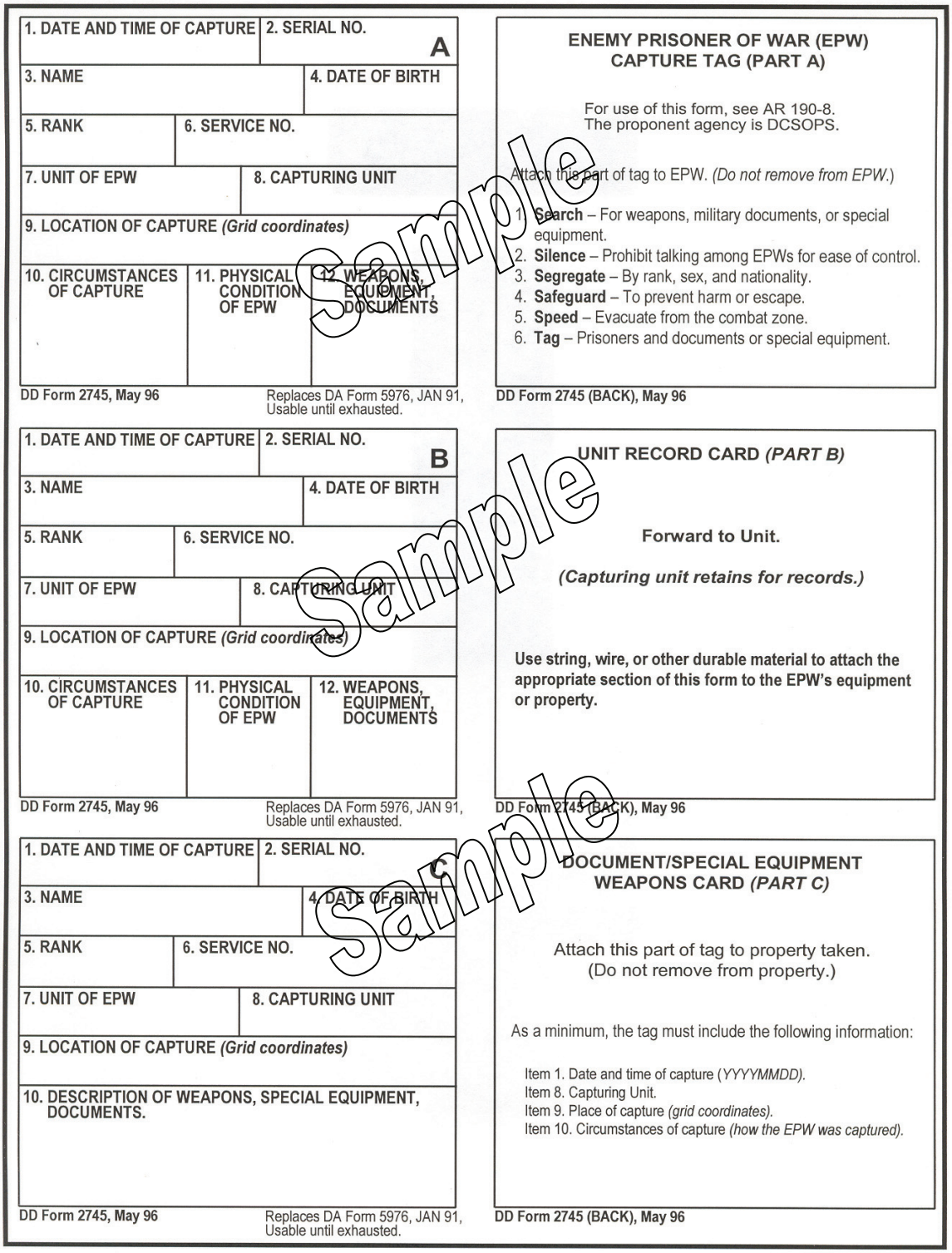
D-22. When no standard tag forms are available, the following field-expedient methods may be used:

- Use meals, ready-to-eat (MRE) cardboard or other type of paper.
- Write the capturing unit's designation.
- Write data and time of capture.
- Write POC coordinates.
- Write circumstances of capture.
- Identify EPW, captured document, or equipment captured.
- Put tag, without damaging the CED, in a waterproof bag.
- Attach EPW and CEE tags so they will not come off.

MEDICAL CARE

D-23. Medical equipment and supplies to permit the administering of emergency first aid should be available at each EPW collecting point and EPW holding area. A qualified medical retained person, if available, may administer first aid to other detainees. All detainees suspected of having communicable diseases are isolated for examination by a medical officer. Wounded detainees may be questioned by intelligence personnel once the detainees are cleared by competent medical authority for questioning.

D-24. For evacuation purposes, detainees may be classified as walking wounded or sick, or as non-walking wounded or sick. Walking wounded detainees are evacuated through MP EPW evacuation channels. Non-walking wounded are delivered to the nearest medical aid station and evacuated through medical channels.



1. DATE AND TIME OF CAPTURE | 2. SERIAL NO. A
3. NAME | 4. DATE OF BIRTH
5. RANK | 6. SERVICE NO.
7. UNIT OF EPW | 8. CAPTURING UNIT
9. LOCATION OF CAPTURE *(Grid coordinates)*
10. CIRCUMSTANCES OF CAPTURE | 11. PHYSICAL CONDITION OF EPW | 12. WEAPONS, EQUIPMENT, DOCUMENTS

DD Form 2745, May 96 — Replaces DA Form 5976, JAN 91, Usable until exhausted.

ENEMY PRISONER OF WAR (EPW) CAPTURE TAG (PART A)

For use of this form, see AR 190-8.
The proponent agency is DCSOPS.

Attach this part of tag to EPW. *(Do not remove from EPW.)*

1. **Search** – For weapons, military documents, or special equipment.
2. **Silence** – Prohibit talking among EPWs for ease of control.
3. **Segregate** – By rank, sex, and nationality.
4. **Safeguard** – To prevent harm or escape.
5. **Speed** – Evacuate from the combat zone.
6. **Tag** – Prisoners and documents or special equipment.

DD Form 2745 (BACK), May 96

1. DATE AND TIME OF CAPTURE | 2. SERIAL NO. B
3. NAME | 4. DATE OF BIRTH
5. RANK | 6. SERVICE NO.
7. UNIT OF EPW | 8. CAPTURING UNIT
9. LOCATION OF CAPTURE *(Grid coordinates)*
10. CIRCUMSTANCES OF CAPTURE | 11. PHYSICAL CONDITION OF EPW | 12. WEAPONS, EQUIPMENT, DOCUMENTS

DD Form 2745, May 96 — Replaces DA Form 5976, JAN 91, Usable until exhausted.

UNIT RECORD CARD *(PART B)*

Forward to Unit.

(Capturing unit retains for records.)

Use string, wire, or other durable material to attach the appropriate section of this form to the EPW's equipment or property.

DD Form 2745 (BACK), May 96

1. DATE AND TIME OF CAPTURE | 2. SERIAL NO. C
3. NAME | 4. DATE OF BIRTH
5. RANK | 6. SERVICE NO.
7. UNIT OF EPW | 8. CAPTURING UNIT
9. LOCATION OF CAPTURE *(Grid coordinates)*
10. DESCRIPTION OF WEAPONS, SPECIAL EQUIPMENT, DOCUMENTS.

DD Form 2745, May 96 — Replaces DA Form 5976, JAN 91, Usable until exhausted.

DOCUMENT/SPECIAL EQUIPMENT WEAPONS CARD *(PART C)*

Attach this part of tag to property taken.
(Do not remove from property.)

As a minimum, the tag must include the following information:

Item 1. Date and time of capture (*YYYYMMDD*).
Item 8. Capturing Unit.
Item 9. Place of capture *(grid coordinates)*.
Item 10. Circumstances of capture *(how the EPW was captured)*.

DD Form 2745 (BACK), May 96

Sample
Sample
Sample

Figure D-1. DD Form 2745 (Enemy Prisoner of War Capture Tag).

This page intentionally left blank.

Appendix E

Extracts from Allied Joint Publication (AJP)-2.5

Following are excerpts from Allied Joint Publication-2.5, Handling of Captured Personnel, Equipment and Documents. AJP-2.5 is primarily an amalgamation of procedures outlined in STANAG 2033, STANAG 2044, and STANAG 2084, and will be used as the authoritative source for matters governed by those STANAGs. S2s and HUMINT collectors should maintain a copy on hand.

THE GENEVA CONVENTIONS

E-1. Treatment of prisoners of war (PWs) and other detainees as well as the handling of personal possessions including personal documents belonging to them will at all times be in accordance with the 1949 Geneva Conventions and, if ratified by the nations concerned, with the 1977 Protocols.

THE DETAINING POWER

E-2. The responsibilities of the "Detaining Power" as set out in GC3 shall rest with the nation or the deployed NATO command which initiated the capture or detention of the person or persons in question.

E-3. Transfers of PWs between NATO nations must be in accordance with GC3, Article 12, as interpreted but not superseded by national agreements.

KNOWLEDGE OF THE GENEVA CONVENTIONS AND THE 1977 PROTOCOLS

E-4. The Geneva Conventions require the signatories in time of both peace and war to circulate the text of the Conventions as widely as possible within their countries. They are especially required to ensure that the provisions and implications of the Conventions are clearly understood by the members of their armed forces and by the civilians attached to them. In order to assist this process, it is suggested in the Conventions that instruction in them is included in the syllabus of appropriate military and civilian courses of instruction.

E-5. The conventions also state that any military or other authority assuming responsibility for dealing with PWs in time of war or armed conflict must be in possession of the text of the Conventions and that its personnel must be instructed in how the Conventions affect them in the execution of their duties with PWs.

E-6. If ratified by the nations concerned, these requirements are, by inference, also applicable to the 1977 Protocols.

PRISONER-OF-WAR STATUS

E-7. Captured personnel (CPERS) can be divided into two categories: Captured personnel who are PWs and other detainees.

E-8. Prisoner-of-war status is conferred on captured personnel who fall within the categories listed in Article 4 of GC3, which is reproduced in Annex A, or, if ratified by the nations concerned, those who meet the expanded definition of a PW as stated in Protocol I of the 1977 Protocols.

E-9. Other detainees are personnel being held by NATO forces until their status can be determined and their further disposition can be decided.

E-10. Furthermore, when NATO forces are engaged in Peacetime Support Operations (PSOs), the operational plan should contain specific instructions as to which individuals will have PW status. Directions for handling other detainees, including those suspected of crimes against humanity and war crimes, are also to be included in the operational plan or in the Standing Operating Procedures used in the operation.

PERSONNEL

E-11. Conditions allowing, the following procedures should be followed by the capturing unit:

a. CPERS should be disarmed immediately, and all documents and effects of military or investigative interest except for necessary clothing, identity documents and protective equipment (Geneva Convention Relative to the Treatment of Prisoners of War (GC3), Article 18) should be removed. CPERS should then be tagged in accordance with the procedures outlined at Annex B. A Common Capture Report should also be completed and forwarded in accordance with the procedure set out in Annex C. It is important that the documents, equipment, maps, etc., taken from a CPERS accompany him to the next receiving unit. Valuable information may be lost by not having these items available during processing and interrogation.

b. Within the confines of the tactical situation, CPERS are to be segregated according to rank, grade, service, sex and nationality or ethnic group/warring faction to minimize the opportunity to prepare counter-interrogation measures. Furthermore, deserters, civilians and political indoctrination personnel will be individually segregated from other CPERS. Such segregation shall be undertaken in a manner which does not violate GC3, Article 16.

c. Talking or fraternization between CPERS is to be prevented in order not to prejudice future intelligence collection operations. CPERS will be allowed no opportunity to exchange information between themselves, to exchange identities or to dispose of articles of intelligence interest.

d. Interrogation operations must not be compromised by contact between CPERS and personnel not concerned with interrogation duties.

e. CPERS will also be prevented from observing sensitive and critical activities, equipment and procedures involving NATO, national or allied forces.

f. CPERS are to be guarded in a manner which shall deny them the opportunity for escape or sabotage.

g. Defectors and political refugees should also be segregated from other CPERS wherever possible. These personnel shall be screened by the nearest Interrogation Unit (IU), which will decide on their value to the intelligence organization and consequent future movements. In all cases, defectors are to be treated in accordance with the Geneva Convention Relative to the Protection of Civilians in Time of War (GC4). National policy may provide defectors treatment in accordance with GC3 where such treatment provides greater protection than GC4.

h. Personnel claiming to be agents of an allied power shall also be segregated from other CPERS. The intelligence organization (G2 or CJ2) is to be informed of all such individuals as soon as possible and will arrange for their screening to determine their future disposition.

i. CPERS suspected of crimes against humanity and war crimes will also be segregated from other prisoners. Legal authorities and the intelligence organization are to be informed of such suspects as soon as possible. They will be taken into custody by law enforcement personnel. Intelligence exploitation should be undertaken in cooperation with the legal authorities.

j. All CPERS are to be treated humanely.

k. Naval and Air Force personnel are to be identified and the intelligence organization is to be notified in order that interrogation by naval/air force personnel may take place at the earliest opportunity.

l. CPERS are to be escorted to the nearest Collecting Point or Holding Area as quickly as possible.

m. Should any doubt arise as to whether any persons, including those appearing to be PWs, having committed a belligerent act and having fallen into Allied hands, belong to any of the categories of persons entitled to PW status pursuant to Article 4 of GC3, such persons shall enjoy the protection of GC3 until such time as their status has been determined by a competent tribunal. If such a tribunal determines that an individual does not qualify for PW status, then the detaining commander must determine whether the detainee qualifies as a ”protected person” pursuant to GC4, and obtain legal advice relative to the proper course of action for dealing with such detainees.

DOCUMENTS

E-12. Captured documents (CDOC) considered of intelligence interest will be handled by the capturing unit in the following manner:

a. The capturing unit will conduct a preliminary screening to obtain information of immediate technical or tactical value.

b. An intelligence report (INTREP) identifying the CDOC and its disposition as well as giving information considered to be of immediate tactical value will be prepared and submitted by the capturing unit. (See STANAG 2022.)

c. The capturing unit will tag or otherwise mark the CDOC as follows:

- National identifying letters of capturing unit as prescribed in STANAG 1059.
- Designation of capturing unit including service.
- Serial number of the CDOC. This will consist of a number allocated sequentially by the capturing unit.
- DTG of capture.
- Location of capture (geographic coordinates or UTM grid reference including grid zone designation and 100,000-meter square identification).
- Captured from Unit (enemy or warring faction) (including national identifying letters in accordance with STANAG 1059).
- Summary of circumstances under which the CDOC was obtained. Interrogation serial number of any associated CPERS, if appropriate or known.
- CED associated with a captured person should be marked with part C of the Standardized EPW Capture and Personal Equipment Tag.

d. CED to be used as evidence in legal proceedings against CPERS suspected of crimes against humanity and war crimes will be kept under guard or in a secure area separate from other CED.

EQUIPMENT

E-13. Captured Equipment (CE) and Associated Technical Documents (ATDs) considered of intelligence interest will be handled by the capturing unit in the following manner:

a. A Capture Report as set out in Annex C of the OPORD will be prepared by the capturing unit upon the discovery or capture of CE or ATD believed to be of intelligence interest. The reporting channels are from the capturing unit through the chain of command to the first TECHINT element.

b. The capturing unit will conduct a preliminary screening to obtain information of immediate technical or tactical value. A Preliminary Technical Report (PRETECHREP) as set out in Annex D of the OPORD will be prepared and submitted through established intelligence channels.

c. Intelligence Reports (INTREP) may, as circumstances dictate, be submitted in advance but not in lieu of the Capture Report and PRETECHREP. (See STANAG 2022.)

d. CE and ATD will be tagged or marked by the capturing unit as follows:

- National identifying letters of capturing unit as prescribed in STANAG 1059.
- Designation of capturing unit including service.
- DTG of capture.
- Location of capture (geographic coordinates or UTM grid reference including grid zone designation and 100,000-meter square identification).

- Captured from Unit (enemy or warring faction) (including national identifying letters in accordance with STANAG 1059).
- Summary of circumstances of capture.
- Associated CPERS.

e. CE and ATD to be used as evidence in legal proceedings against CPERS suspected of crimes against humanity and war crimes will be kept under guard separate from other CE and ATD.

This page intentionally left blank.

Appendix F

NATO System of Allocating Interrogation Serial Numbers

1. Every captured person selected for interrogation will be given an Interrogation Serial Number. This number shall be allocated by the Interrogation Unit conducting the **first** interrogation of the captured person.

2. The number should not be confused with the Prisoner of War Internment Serial Number (ISN), which is to be used for administrative purposes only.

3. The purpose of the Interrogation Serial Number is to identify the source of information to ensure its proper evaluation, processing, and follow-up action. It will also identify the nationality and location of the interrogation unit.

4. The number shall be constituted as follows:

a. 2 letters to indicate the Nationality of the captured person (see para 6).

b. 2 letters to indicate the Service of the captured person (see para 7).

c. 1 letter to indicate the Arm of Service of the captured person (see para 8).

d. 4 numbers to indicate the Interrogation Sequence Number of the captured person (see para 9).

e. 4 numbers to indicate the Day and Month of Capture.

f. A dash (-) to show a sequence break.

g. 4 letters to indicate the Nationality and Service of the Interrogation Unit (see para 10).

h. 4 letters to indicate the Interrogation Unit.

5. Each group shall be separated by a dash. The final number shall therefore appear as in the following examples:

LS – NV – B – 0012 – 2105 – USNV – 0159

Liechtenstein – Naval prisoner – Seaman – 12th captured person interrogated - captured 21 May – interrogated by US Navy – team 159

AN – AF – H – 0357 – 0211 – GEAF – 0007

Andorra – Air force prisoner – Intelligence – 357th captured person interrogated – captured 2 Nov – interrogated by GE Air Force – team 7

SM – AR – X – 0431 – 0707 – UKAR – 0019

San Marino – Army prisoner – One star or above – 431st captured person interrogated – captured 7 Jul – interrogated by UK Army – team 19

6. The two letters used for indicating the Nationality of the captured person will be in accordance with established NATO Country codes in STANAG 1059.

7. The following list of letters is to be used to indicate the Service of the captured person:

AR	- Army	NI	- Naval Infantry
NV	- Navy	AB	- Airborne Forces
NA	- Naval Air Arm	SF	- Special Purpose Forces
AF	- Air Force	PL	- Police
IR	- Irregular	CV	- Civilian (other than Police)

8. The following list of letters is to be used to indicate the Arm of Service of the captured person:

Navy (A)	**Army (B)**	**Air Force (C)**	**Other/Partisan Forces (D)**
A. Aircrew	Aircrew	Aircrew	Aircrew
B. Seamen	Infantry	Ground Crew	Merchant Marine
C. Communications	Signals	Communications	Radio Officers/Operators
D. Weapons/ Electronic Engineer	Electrical/Electronic Engineer	Electrical/Electronic Engineer	
E. Mechanical/ Marine/Engineers	Engineers	Mechanical/Air Frame/Engineers	
F. Gunnery	Artillery	Ordnance	Weapons/Ordnance Explosives
G. *HQ Staff	*HQ Staff	*HQ Staff	*HQ Staff
H. Intelligence	Intelligence	Intelligence	Intelligence
I. Marines	Airborne Forces	Airfield Defense	
J. Cooks/Stewards	Catering	Catering	Catering
K. Legal/Political	Legal/Political	Legal/Political	Legal/Political
L. Medical/Dental/ Nursing	Medical/Dental/ Nursing	Medical/Dental/ Nursing	Medical/Dental/ Nursing
M. Electronic Warfare	Electronic Warfare	Electronic Warfare	Electronic Warfare
N. Operations	Operations	Operations	Operations
O. Police	Police	Police	Police
P. Supply	Quartermaster	Supply	Supply
Q. Strategic Weapons	Strategic Weapons	Strategic Weapons	Strategic Weapons
R. Special Purpose Forces	Special Purpose Forces	Special Purpose Forces	Special Purpose Forces
S. Air Traffic Control	Armored	Air Traffic Control	Air Traffic Control
T. *Unknown	*Unknown	*Unknown	*Unknown

Navy (A)	Army (B)	Air Force (C)	Other/Partisan Forces (D)
U. Instructors	Education	Education	Instructors
V. Ministers of Religion	Ministers of Religion	Ministers of Religion	Ministers of Religion
W. *Submarines	Artillery Spotters	Forward Air Controllers	Couriers, etc.
X. *One Star +	*One Star +	*One Star +	*Officers in Command of Irregular Forces
Y. *Other	*Other	*Other	*Other
*Notes: G – Headquarters staffs below one star rank T – Captured Person's arm of service not known to report writer W – To be used in respect of all submarines regardless of arm or specialization X – To be used in respect of all ONE STAR or above officers regardless of army Y – PW arm of service not included in the appropriate list			

9. The sequence number of the interrogated captured personnel shall be of four digits allocated in numerical order of interrogation by the team first interrogating the captured person.

10. Country, services and team codes.

a. Country codes, as laid down in STANAG 1059, are to be used for indication of the Nationality of the Interrogation Team.

b. The following lists of letters are to be used for indicating the Service of the Interrogation Team:

ARMY	- AR	AIR FORCE	- AF
NAVY	- NV	MARINE	- MR
COAST GUARD	- CG	PARA-MILITARY	- PM

c. NATO teams will use the following abbreviations: (These will be determined as command changes are implemented and STANAG 1059 is revised).

SC EUROPE	RC SOUTH
RC NORTH	JHQ SOUTHWEST
JHQ NORTH	JHQ SOUTH
JHQ NORTHEAST	JHQ SOUTH CENTER
JHQ CENTER	JHQ SOUTHEAST
CC AIR NORTH	CC AIR SOUTH
CC NAV NORTH	CC NAV SOUTH
SC ATLANTIC	RC EAST
RC WEST	STRIK FLTLANT
RC SOUTHEAST	SUB ACLANT

11. Nations will allocate 4-digit serial numbers to their interrogation teams. NATO Commands will issue similar numbers to subordinate national interrogation teams under their command.

This page intentionally left blank.

Appendix G

Questioning Quick Reference

This appendix offers a quick reference for the trained HUMINT collector. It is not meant to be all-inclusive, nor instructive in proper questioning technique, but lays out frequently used requirements grouped logically by OB factor. Proper formation of questions is covered in detail in Chapter 9.

Missions: Mission questioning consists of three areas: Time of Capture Mission, Future Mission, and Past Mission. Missions are questioned in that order, to ensure that the information is collected in the order of importance to a supported commander. Logical follow-up questioning may lead the collector into any of the OB factors at any time during questioning in order to provide complete information.

Offensive Missions:
When will the enemy attack?
Where will they attack?
What is the main objective of the attack?
What units will participate in the attack?
What tactics will be employed?
What artillery, air, and other units will support the attack?

Defensive Missions:
Where will the enemy establish lines of defense?
What units have been assigned to the defensive lines?
What obstacles have been emplaced (mines, trenches, wire, etc.)?
What artillery support is there for the defensive operation?

Retrograde Operations:
What units will take part in the retreat?
What are the current positions of the retreating units?
When will they start to retreat?
What routes will be used?
What is the planned destination of the retreating units?
What units will cover the retreat?

Composition:
What is the command and control element of (the target unit)?
What types of units are directly subordinate to (the target unit)?
What is the designation of (each of the subordinate units)?
How many units of that type are directly subordinate to (target unit)?
What units are attached? When? Why? What unit(s) are they detached from?
What units are detached? When? Why? What unit(s) are they attached to now?

Weapons and Equipment Strength:

Individual Weapons:
What individual weapons are there in (target unit)?
How many?
What is the distribution of the weapons?
Crew-Served Weapons: What crew-served weapons are in (target unit)?
How many?
What is the distribution of the weapons?
Other Weapons: What other weapons are there in (target unit)?
What types?
How many?
How are they distributed?
Vehicles: What armored vehicles are in (unit)?
How many?
What nomenclature?
What other vehicles are in (unit)?

Dispositions:

Disposition questioning is ideally done with the aid of a map.
Where is (the target disposition)?
Show (on the map) the location of (the target disposition).
What enemy units, activities, or equipment are at that location?
What security measures are being employed at that location?
Additionally, specific types of dispositions require additional follow-up:

Area-Type Dispositions: (Staging Areas, Assembly Areas, Trains, etc.)
Show on the map (or describe) the perimeter of the disposition.
Where are units or activities located within it?
Where are the approaches/entrance?
What unit is in charge?
What vehicles or equipment are located within the disposition?
What is the date of information?

Line-Type Dispositions: (Line of Departure, Artillery emplacement, etc.)
Show on the map (or describe) the location of the disposition.
Define and locate both ends of the disposition.
What equipment is located there?
In the case of artillery, describe the placement and orientation of the guns, ammunition, radar, and support vehicles.

Tactics:

Offensive: What offensive tactics are being employed by (unit)?
What other units are involved?
When did (unit) begin employing these tactics?
What are the major objectives?
Defensive: What defensive tactics are being employed by (unit)?
What other units are involved?
When did (unit) begin employing these tactics?
Special Operations: What special operations tactics are being employed by (unit)?
What are the designations of the units employing special operations tactics? When did (unit) begin employing special operations tactics?
Where/Why are these tactics being employed?

Training:

Individual Training: What individual training is being conducted by (unit)?
Who is being trained?
How effective is the training?
Where is the training conducted?
What are the training standards?
Unit Training: What unit training is being conducted by (unit)?
Who is being trained?
How effective is the training?
Where is the training conducted?
What are the training standards?
Specialized Training: What specialized training is being conducted by (unit)?
Who is being trained?
How effective is the training?
Where is the training conducted?
What are the training standards?
What specialized equipment is used in the conduct of the training?

Combat Effectiveness:

Losses:
Personnel: What personnel losses have been incurred by (unit)?
When? Where? How?
What were the duty positions/ranks of the lost personnel?
Equipment: What equipment losses have been sustained by (unit)?
What type of equipment was lost?
When? Where? How many?
How were they lost?

Replacements (Personnel):

Received: What replacements have been received by (unit)?
What replacements are available to (unit)?
How many?
From where were the replacements received?
Available: What personnel replacements are available to (unit)?
From where are replacements available?
How many? What ranks?
How long would it take for replacements to arrive once requested?

Replacements (Equipment):

Received: What equipment replacements have been received by (unit)?
How many?
From where were the replacements received?
How does the quality of the replacement equipment compare to that of the original equipment?
What is the level of confidence in the replacement equipment, compared to the original?
Available: What equipment replacements are available to (unit)?
From where are replacements available?
How long would it take to receive replacement equipment once requested?
How many of each type of equipment are available?

Reinforcements:

Received: What reinforcements have been received by (unit)?
What type was the reinforcing unit?
What is the designation of the reinforcing unit?
What equipment did the reinforcing unit bring?
To which unit was the reinforcing unit further assigned?
Why did (receiving unit) receive reinforcements?
How long will the reinforcing unit be assigned as reinforcement to (unit)?
Available: What reinforcements are available to (unit)?
From where (parent unit/location) are reinforcements available?
What types of units are available to reinforce (unit)?
How long would it take for reinforcements to arrive, once requested?

Morale:

Describe the morale of the members of (unit).
How long has the morale been…?
What is the unit leadership doing to (maintain/improve) the morale?
What effect has (high/low) morale had on the behavior or performance of the unit members?

Logistics:

Weapons: What is the condition of the (specific weapons) in (the unit)?
Why are (the weapons) in that condition?
What is being done to improve the condition of (the weapons)?
How often is maintenance performed? By whom?
Who inspects weapons? How often?
Is there an increased emphasis on maintenance? If so, why?
What is done to prevent/alleviate a shortage while weapons are being maintained?
What spare parts are there for weapons in (unit)?
What shortages of spare parts are there?
What problems are there with spare parts (quality, fit, delays, etc)?
Ammunition: What types of ammunition are available for the (weapon/weapon system) in the (unit)?
What problems are being experienced with ammunition for (weapon or weapon system) in (unit)? Why? Since when?
What is being done to correct the problem(s)?
What shortages of ammunition for (weapon or weapon system) are there in (unit)?
What is being done to correct the shortage?
When was the last issue of ammunition for the (weapon or weapon system) in the (unit)?
How much was issued?
When is the next issue of ammunition planned?
(For insurgents/irregulars - Where is funding obtained for ammunition/explosive purchases?
Where are ammunition/explosives obtained?
How are ammunition/explosives transported/delivered?
Vehicles: What is the condition of the (specific vehicle) in (the unit)?
Why are (the vehicles) in that condition?
What is being done to improve the condition of (the vehicles)?
How often is maintenance performed? By whom?
Who inspects vehicles? How often?

Is there an increased emphasis on maintenance? If so, why?
What is done to prevent/alleviate a shortage while vehicles are being maintained?
What spare parts are there for vehicles in (unit)?
What shortages of spare parts are there?
What problems are there with spare parts (quality, fit, delays, etc)?

POL:

What problems have been experienced with the petroleum, oils, and lubricants (POL) for the (vehicle type) in the (unit)?
Why are there problems?
Since when have there been problems?
What is being done to correct the problems?
What shortages of POL are there? Why?
What is being done to alleviate the shortages?
When was the last resupply of POL in (unit)? Where? How much?
When is the next resupply of POL planned?

Communications Equipment:

What is the condition of the (specific radio set) in (the unit)?
Why are (the radios) in that condition?
What is being done to improve the condition of (the radios)?
How often is maintenance performed? By whom?
Who inspects communication equipment? How often?
Is there an increased emphasis on maintenance? If so, why?
What is done to prevent/alleviate a shortage while radios are being maintained? What spare parts are there for communication equipment in (unit)?
What shortages of spare parts are there?
What problems are there with spare parts (quality, fit, delays, etc)?

Medical:

Equipment: What individual medical equipment is in (unit)? How many?
What is the distribution?
What are the contents of individual medical kits in the (unit)?
What is the quality?
What shortages are there?
What problems are there with the individual medical equipment/supplies in (unit)?
What vehicular medical equipment is in (unit)? How many?
What is the distribution?
What are the contents of vehicular medical kits in (unit)?
What is the quality?
What shortages are there?
What problems are there with the vehicular medical equipment/supplies in (unit)?

Personnel: What medical personnel are assigned to (unit)?
What medical personnel are available to treat members of (unit)? How many? What are the duty positions of the medical personnel?
What level of medical care are the medical personnel able to provide to members of (unit)?

Facilities: What medical facilities are available to members of (unit)?
Where are the medical facilities?
What level of care is available there?
What higher echelons of medical care are available?

Medical Evacuation (MEDEVAC) Procedures: What MEDEVAC procedures are available to members of (unit)?
Where are MEDEVAC collection points?
What different MEDEVAC procedures are used for more seriously wounded personnel, compared to lightly wounded?
Food: What rations are members of (unit) eating?
What shortages are there of food?
What is the quality?
What problems have been encountered with the rations provided to (unit)?
When was the last issue of rations to members of (unit)?
When is the next issue?
What reserve stocks of field rations are there in (unit)?
Water: What is the source of drinking water for members of (unit)?
What problems have been encountered with quality, shortages, or contamination of drinking water?
What water purification methods are available to members of (unit)?
Under what circumstances will they be used?
If water purification tablets are used, what color are they?

Electronic Technical Data:

Radio Frequencies: What are the primary and alternate frequencies for radios in (each unit)?
Under what circumstances will alternate frequencies be used?
What networks operate on the various frequencies?
Call Signs: What is the call sign of (unit)?
What is the call sign of (each) person of authority in the unit?
When do call signs change?
What informal call signs are in use?

Miscellaneous:

Personalities: Question for name, rank, unit, duty position, and unit of key leaders.
Collect identifying characteristics such as age, height, weight, build, hair and eye color, writing hand, facial hair and teeth.
Report contact information such as work and home addresses, telephone numbers, fax number, and email address.
Complete biographical IIR format is in DIAM 58-12 (S//NF).
Code Names: What is the code name of (each unit)?
What code names are being used for specific operations?
Passwords: What is the current challenge/password for (unit)?
When did it go into effect?
When will it change?
What will the next challenge/password be?
What other (informal, "run in") passwords are in use?

Obstacles:

Enemy: What obstacles have the enemy forces emplaced?
Where, when, what type of obstacles?
What safe lanes are there through or around the obstacles?
(If mine fields, collect type, pattern, quantity, and method of emplacement of mines.)
How are the obstacles being covered (artillery, ambush, etc.)?

Why have the obstacles been emplaced where they are (denial of terrain, canalization into a fire sack, etc.)?

Friendly: What friendly obstacles have enemy forces encountered? Where? When?

Have those obstacles been breached or otherwise neutralized?

What effect have the friendly obstacles had on enemy maneuver?

PSYOP:

Enemy: What PSYOP are being conducted by (unit)?

What is the text of the messages?

Who is the target audience?

Where are the PSYOP materials prepared?

Where and how are they delivered? What is the hoped-for effect?

Friendly: What PSYOP have members of (unit) encountered? Where? When?

What form of PSYOP was encountered?

What effect have the PSYOP had on the officers/NCOs/enlisted of (unit)?

What is the leadership of (unit) doing to counter the effects of friendly PSYOP?

This page intentionally left blank.

Appendix H

SALUTE Reporting

H-1. The SALUTE report format requires brief entries which require the collector to break information down into basic elements: who, what, where, when, why, and how. This allows for efficient reporting via electronic or hardcopy medium. It also allows the analyst to quickly scan multiple reports to find specific information.

H-2. Figure H-1 provides guidance and is not to be construed as strict requirements. SALUTE reports of combat activity may only contain a word or two in each entry, whereas Intelligence reports tend to include more detail.

TO: Usually the address of the supported S2/G2 (according to unit SOP)

FROM: Your unit or team designation, or your duty position, as appropriate

DTG: The date-time group of when the report is being submitted

Report Number: From local SOP

1. (S)ize/Who: Expressed as a quantity, and echelon, or size (e.g., 1 x BDE). If multiple echelons are involved in the activity being reported, there can be multiple entries (e.g.,1 x BDE; 2 x BN). Non-standard units are reported as such (e.g., bomb-making class; support staff).

2. (A)ctivity/What: This line is the focal point of the report and relates to the PIR or important non-PIR information being reported. It should be a concise bullet statement.

3. (L)ocation/Where: Generally a grid coordinate, including the 100,000 meter grid zone designator. The entry can also be an address, if appropriate, but still should include an 8-digit grid coordinate. City names will always be followed by the two-character country code. If the activity being reported involves movement (advance, withdrawal, etc.) the location entry will include "From" and "To" entries. The route used will be reported under "Equipment/How."

4. (U)nit/Who: This entry identifies who is performing the activity described in the "Activity/What" entry. Include the complete designation of a military unit, identification of a civilian or insurgent group, or the full name of an individual, as appropriate.

5. (T)ime/When: For a future event, this is when the activity will initiate. Past events are usually not the subject of SALUTE reports, but if a past event is to be reported, the Time/When entry will generally reflect when the event ended. Ongoing events are reported as such. Reports of composition of forces, morale, and Electronic Technical Data and other non-event topics are reported as ongoing. When reporting on a disposition, the "Time/When" entry is generally the last time the source was at the disposition.

6. (E)quipment/How: The information reported in this entry clarifies, completes, and/or expands upon information reported in any of the previous entries. It includes information concerning equipment involved, tactics used, and any essential elements of information not reported in the previous paragraphs.

7. Remarks: Use this entry to report the source of the information, whether a person, a CED, open-source media, or other source. Include the date of information and the PIR that the reported information addresses. Map data for coordinates given in the "Location/Where" entry are included, stating map series name, sheet number, scale and edition. If there are enclosures to the SALUTE report, such as sketches, they are annotated here.

Figure H-1. Example of a Written SALUTE Report.

Appendix I

Document Exploitation and Handling

I-1. DOCEX is a vital information source in the development of the all-source intelligence picture. Unless planned for and carefully monitored, the volume of CEDs in all operations can rapidly overwhelm a unit's capability to extract meaningful information.

DEFINITIONS

I-2. A document, as defined by AJP 2.5, is any piece of recorded information, regardless of form. Documents include printed material such as books, newspapers, pamphlets, OPORDs, and identity cards as well as handwritten materials such as letters, diaries, and notes. Documents also include electronically recorded media such as computer files, tape recordings, and video recordings and the electronic equipment which contains documents or other vitally important intelligence. Examples include hard drives, operating systems, and personal electronic devices, including phones, PDAs, and GPS devices. A CED may be needed by several collection or exploitation activities at the same time, requiring copies to be made. Collectors must have ready access to copying equipment. Documents often must be evacuated through two different channels for proper exploitation, which also makes copying necessary. Such documents and equipment require special handling to assure that they are returned to their owners.

I-3. DOCEX is the systematic extraction of information from threat documents for the purpose of producing intelligence or answering IRs. A threat document has been in the possession of the threat, written by the threat, or is directly related to a future threat situation. DOCEX can occur in conjunction with HUMINT collection activities or as a separate activity.

I-4. A CED is any document that was in the possession of an enemy force that subsequently comes into the hands of a friendly force, regardless of the origin of that document. There are three types of CEDs.

- Official - documents of government or military origin.
- Identity - personal items such as identification (ID) cards or books, passports, driver licenses.
- Personal - documents of a private nature such as diaries, letters, and photographs.

I-5. Open-source documents are documents that are available to the general public including but not limited to newspapers, books, videotapes, public records, and documents available on the Internet or other publicly available electronic media.

I-6. Source-associated documents are documents that are encountered on or in immediate association with a human source. These may include both official and personal documents. Documents associated with human sources are normally exploited, at least initially, during the interrogation or debriefing of the source. Interrogators typically use these documents during planning and preparation for interrogation of the associated EPW. These personal documents and source identification documents are therefore evacuated in conjunction with the associated source and sent through prisoner, detainee, or refugee evacuation channels rather than through intelligence channels. If the duplication capability exists, collectors should copy personal documents that contain intelligence information and evacuate the copy through intelligence channels. The original personal document should be evacuated with the detainee but not on his person until the HUMINT collector has exploited it. Collectors evacuate official documents through intelligence channels after initial exploitation. If possible, the collector will copy official documents and evacuate the copy with, but not on, the source.

OPEN-SOURCE INFORMATION

I-7. Open-source information is publicly available information appearing in print or electronic form. Open-source information may be transmitted via radio, television, newspapers, commercial databases, electronic mail networks, or other electronic media like CD-ROMs. Whatever form they take, open sources are not—

- Classified at their origin.
- Subject to proprietary constraints.
- The product of sensitive contacts with US or foreign persons.

I-8. In all operations, open-source collection can be a valuable addition to the overall intelligence collection and each intelligence discipline's efforts. Open-source information supplements the HUMINT collection effort, and all types of open sources must be considered for exploitation.

I-9. Open sources are evaluated and categorized as friendly, neutral, or hostile. Certain high-value, open-source information sources may be identified for continuous monitoring. Other open-source information sources may be identified to screen for the presence or lack of specific indicators. In addition, the information obtained from open sources is extremely helpful for the HCT members to be current with the latest developments in the AO, which enables them to establish rapport and effectively converse with their sources. Open-source documents are exploited in the same manner as CEDs.

OPEN-SOURCE DOCUMENT OPERATIONS

I-10. Open-source document operations are the systematic extraction of information from publicly available documents in response to command IRs. Open-source document operations can be separate operations or can be included as part of other ongoing operations. Open-source documents are significant in the planning of all operations, especially during the execution

of stability and reconstruction operations and civil support operations. As well as hard data, open-source information can provide valuable background information on the opinions, values, cultural nuances, and other sociopolitical aspects in AOIs. In evaluating open-source documents, collectors and analysts must be careful to determine the origin of the document and the possibilities of inherent biases contained within the document.

CAPTURED DOCUMENT OPERATIONS

I-11. One of the significant characteristics of operations is the proliferation of recordkeeping and communications by digital methods (faxes, e-mails, typed, or computer-generated documents). The rapid and accurate extraction of information from these documents contributes significantly to the commander's accurate visualization of his battlefield. Documents may be captured on or in immediate association with EPWs and detainees, may be found on or turned in by refugees, line crossers, DPs or local civilians, or may be found in abandoned enemy positions or anywhere on the battlefield.

DOCUMENT EVACUATION AND HANDLING

I-12. The rapid evacuation and exploitation of documents is a shared responsibility. It originates with the capturing unit and continues to the complete extraction of pertinent information and the arrival of the document at a permanent repository, normally at the joint level, either within the theater of operations or outside of it. Documents captured in association with detainees and EPWs, with the exception of identity documents, are removed from the individual to ensure that documents of intelligence interest are not destroyed. These documents are evacuated through EPW evacuation channels with, but not on the person of, the detainee. With the exception of official documents, all documents are eventually returned to the detainee.

I-13. CEDs not associated with a detainee are evacuated through MI channels, generally starting with the capturing unit's S2. Depending on the type of documents, they may eventually be evacuated to the National Center for Document Exploitation. HUMINT collectors and translators can extract information of intelligence interest from CEDs at every echelon; they will make an attempt to exploit CEDs within their expertise and technical support constraints. Collectors evacuate CEDs to different elements based upon the information contained and the type of document concerned. For example, documents related to criminal activity may be evacuated to the nearest criminal investigative unit. Direct evacuation to an element outside the chain of command takes place at the lowest practical echelon but is normally done by the first MI unit in the chain of command. Document evacuation procedures are outlined in Annex B (Intelligence) of the unit's OPORD and SOPs.

Actions by the Capturing Unit

I-14. Document accountability begins at the time the document comes into US possession. Original documents must not be marked, altered, or defaced in any way. The capturing unit attaches a DD Form 2745 (Enemy Prisoner of War Capture Tag), Part C, to each document. Only in the case where a

capturing unit does not have the time nor the manpower to mark each document due to ongoing combat operations should the capturing unit fill out one capture tag for a group of documents. In this case, the capturing unit should place the documents in a weatherproof container (box or plastic bag). The capturing unit should fill out two copies of the DD Form 2745, placing one copy inside the container and attaching one to the outside of the container. If these forms are not available, the capturing unit records the required data on any piece of paper. Figure I-1 shows an example of a field expedient tag. At a minimum, the capturing unit should record the information as follows:

- Time the document was captured as a DTG.
- Place document was captured, including an 8-digit coordinate, and description of the location. This should be as detailed as time allows. For example, if a terrorist safe house was searched, documents might be "bagged and tagged" based on what room of the house they were in, what file cabinet, what desk, and so forth.
- Identity of the capturing unit.
- Identity of the source from whom the document was taken, if applicable.
- Summary of the circumstances under which the document was found.

I-15. Document evacuation procedures are listed in Annex B (Intelligence) to the OPORD. If the capturing unit does not contain a supporting HCT, it forwards any CEDs found on the battlefield directly to its S2. The S2 extracts PIR information as practicable, ensures that the documents are properly tagged, and ensures speedy evacuation to the next higher echelon through intelligence channels. Normally, a capturing unit will use any available vehicle, and in particular empty returning supply vehicles, to evacuate documents. Documents captured on or in association with detainees, including EPWs, should be tagged and removed from the detainee. They are evacuated with (but not on) the detainees to an MP escort unit or an EPW holding facility.

I-16. When large numbers of documents are captured in a single location, it is often more expedient for the capturing unit to request a DOCEX team or HCT from the supporting MI unit be sent to the documents rather than attempting to evacuate all the documents. This reduces the burden on the capturing unit, facilitates the rapid extraction of information, and enables the priority evacuation of documents of importance to higher echelons. This method should only be used if the capturing unit can adequately secure the documents until the arrival of the DOCEX team and if the battlefield situation and MI resources permit the dispatch of a team. The capturing unit should include in its request the following:

- The identification of the capturing unit.
- Its location and the location of the documents.

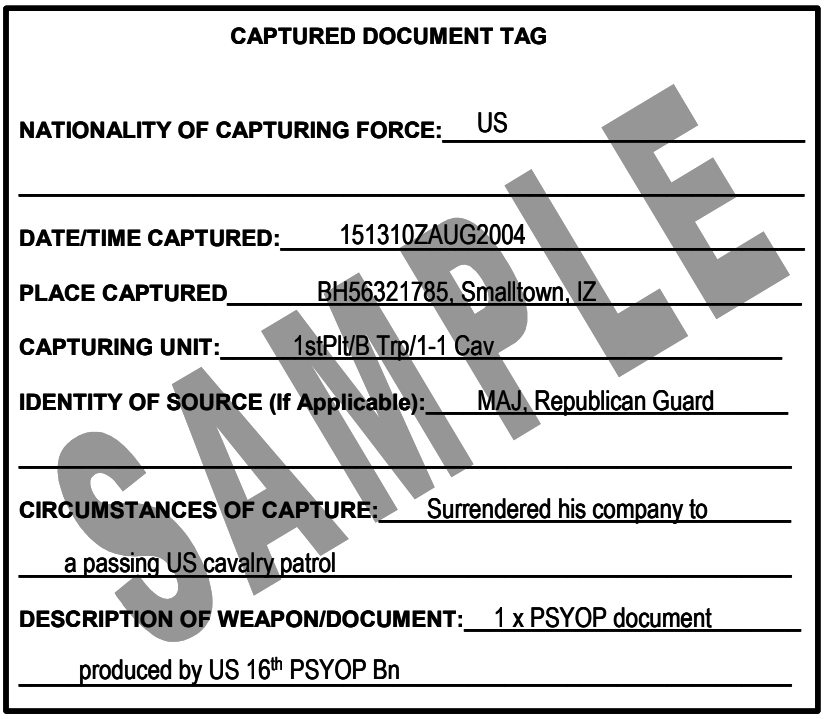


Figure I-1. Example of a Field Expedient Capture Document Tag.

- The general description of the document site (such as an enemy brigade headquarters).
- The approximate number and type of documents.
- The presence of captured computers or similar equipment.

I-17. The MI unit dispatching the team should notify the requesting team as soon as possible to provide them an estimated time of arrival and to coordinate the arrival of the team. There is no set time for how long any particular echelon may keep a document for study. The primary aim of speedy evacuation to the rear for examination by qualified DOCEX elements remains. Each echelon is responsible to prevent recapture, loss, or destruction of the CEDs.

ACTIONS BY THE FIRST HUMINT COLLECTION OR DOCEX UNIT

I-18. The first HUMINT collection or DOCEX unit to receive CEDs should log, categorize, and exploit the documents to the best of its abilities based on METT-TC factors. They should rapidly identify documents requiring special handling or special expertise to exploit and evacuate those documents to the appropriate agencies. The MI unit SOP or OPORD should list special document evacuation requirements and priorities.

Accountability

I-19. The capturing unit and each higher echelon take steps to ensure that they maintain CED accountability during document evacuation. To establish accountability, the responsible element inventories all incoming CEDs. Anyone who captures, evacuates, processes, or handles CEDs must maintain accountability. All CEDs should have completed captured document tags. An incoming batch of documents should include a captured document transmittal. Figure I-2 shows this format. The exact format for a document transmittal is a matter of local SOP, but it should contain the information listed below:

- The identity of the element to which the CEDs are to be evacuated.
- The identity of the unit forwarding the CEDs.
- The identification number of the document transmittal.
- Whether or not CEDs in the package have been screened and the screening category. (If not screened, NA is circled.) Document handlers should package documents that have been screened separately, by category.
- A list of the document serial numbers of the CEDs in the package.

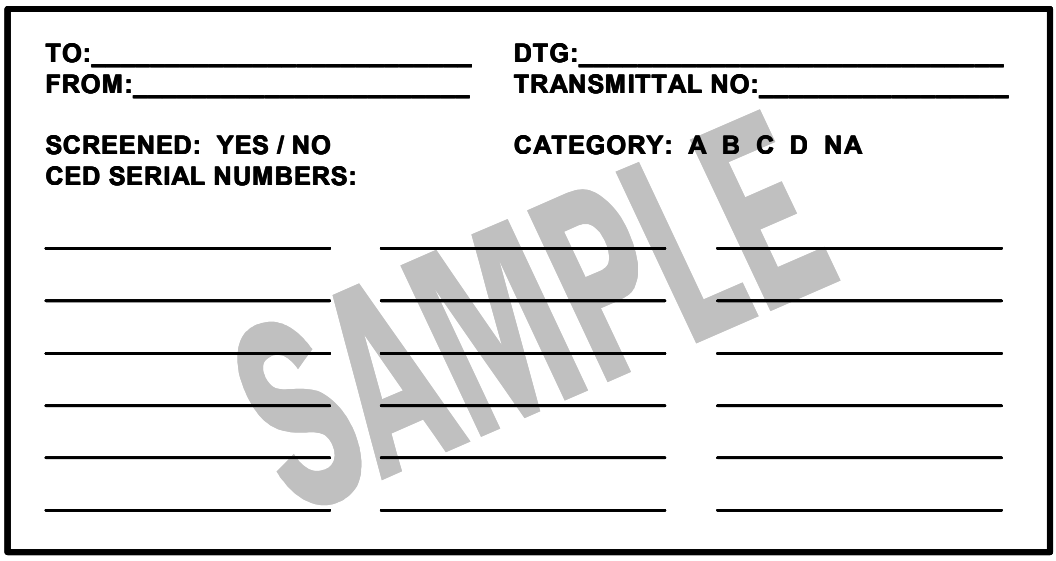


Figure I-2. Example of a Captured Document Transmittal Sheet.

I-20. When a batch is received without a transmittal, the HUMINT collection element contacts the forwarding units and obtains a list of document serial numbers (if possible). The HUMINT collection element records all trace actions in its journal. Accountability includes—

- Inventorying the CEDs as they arrive.
- Initiating necessary trace actions.

- Maintaining the captured document log. (See Figure I-3.)

I-21. When a collector includes intelligence derived from a CED in an intelligence report, he references the identification letters and number of the document concerned to avoid false confirmation.

Inventory

I-22. The receiving element conducts an initial inventory of incoming CEDs by comparing the CED to the captured document tag and accompanying transmittal documents. This comparison identifies—

- Transmittals that list missing CEDs.
- Document tags not attached to CEDs.
- CEDs not attached to document tags.
- CEDs not listed on the accompanying transmittal documents.

UNIT:_____

FILE NUMBER	RECEIVED DOCUMENT DTG SERIAL #	INCOMING TRANSMITTAL#	FORWARDING UNIT	RECEIVED BY	DTG AND PLACE OF CAPTURE
1501	150830AUG99 0102368	1T08	1/82d Abn Div	SSG KIM	150500AUG99/EK030949
1502	150930AUG99 0110443	2T11	2/82d Abn Div	SSG KIM	150620AUG99/EK045860
1503	150930AUG99 1039964	2T11	2/82d Abn Div	SSG KIM	150725AUG99/EK058383
1504	150930AUG99 1192583	2T11	2/82d Abn Div	SSG KIM	150725AUG99/EK058383

CAPTURING UNIT	SCREENING CATEGORY	DESCRIPTION OF DOCUMENT	DESTINATION/ TRANSMITTAL #	REMARKS
Co A, 1/504th, 1 Bde, 82d	A	Letter of promotion, KP, 1Pg	JDEC, 15T01	SALUTE written
Co B, 2/504th, 2 Bde, 82d	A	Letter describing attack, RU, 3 Pg	JDEC, 15T01	SALUTE written
Co B, 2/504th, 2 Bde, 82d	B	List of call signs, RU, 1Pg	JDEC, 15T03	None
Co B, 2/504th, 2 Bde, 82d	C	Personal letter, KP, 2 Pg	JDEC 15T02	Translation end

SAMPLE

Figure I-3. Example of a Captured Document Log.

Trace Actions

I-23. The receiving unit initiates trace actions on all missing CEDs, missing captured document tags, and all information missing from the captured document tags. They initiate trace actions by contacting elements from which the documents were received. The receiving unit can complete this corrective action swiftly if that unit's captured document log was filled out completely. If necessary, the trace action continues to other elements that have handled the document. If a captured document tag is unavailable from elements that have previously handled the CED, the document examiner fills out a

captured document tag for the document using whatever information is available. Attempts to obtain missing CEDs are critical because of the information those CEDs might contain.

Document Logs

I-24. The captured document log is a record of what an element knows about a CED. After trace actions are initiated for any missing documents, the CEDs are entered in the REMARKS section of the captured document log. This log must contain the following:

- Name of capturing unit.
- File number (a sequential number to identify the order of entry).
- DTG the CED was received at this element.
- Document serial number of the captured document tag.
- Identification number of the transmittal document accompanying the CED.
- Complete designation of the unit that forwarded the CED.
- Name and rank of individual that received the CED.
- DTG and place of capture (as listed on the captured document tag).
- Identity of the capturing units (as listed on the captured document tag).
- Document category (after screening).
- Description of the CED. (At a minimum, the description includes the original language; number of pages; type of document such as a map, letter, or photograph; and the enemy's identification number for the CED, if available.)
- Destination and identification number of the outgoing transmittal.
- Remarks to include any other information that can assist the unit in identifying the CED including processing codes. These are set up by local SOPs to denote all actions taken with the document while at the element, including intelligence reports, translations, reproductions, or return of the CED to the source from whom it was taken.

DOCUMENT SCREENING

I-25. Document screening is the rapid but systematic evaluation of documents to determine which documents contain priority information. Selected priority documents will be exploited immediately for PIR information and evacuated expeditiously (often electronically) to a DOCEX facility. Document screening can be done manually (requiring a linguist who is well versed in the current collection requirements) or through the use of scanning devices with key word identification capability. Document processing does not require the complete translation of a document but requires sufficient translation to

determine the significance of the document. A non-linguist may be able to do a degree of preliminary screening based on document format and the location where the document was found.

I-26. As screeners screen each document, they assign one of four category designations. The assigned category determines the document's priority for exploitation and evacuation. Document screening requires that the screening units receive the most current PIR and intelligence requirements; current friendly and enemy situation update; and relevant OB information. Screeners at higher echelons can re-categorize CEDs, to more accurately reflect the requirements at that level or information that has past its LTIOV.

DOCUMENT CATEGORIES

I-27. Documents are divided into categories to prioritize their evacuation and the extraction of information from them for intelligence purposes. Document categories are discussed below.

Category A

I-28. Category A documents are those that require priority evacuation and/or special handling because of their special intelligence value. They contain SALUTE reportable information. Category A documents also include those that are of interest to another command, collecting agency, or other agency (for example, TECHINT, Air Force, Navy, PSYOP, Cryptography).

I-29. What determines if a document is a Category A document changes according to the operational environment and will be set forth in each DOCEX element's SOP and in Annex B (Intelligence) of the unit's OPORD. Documents that are evidence in legal proceedings against captured personnel suspected of crimes against humanity and war crimes will be handled as Category A documents. All Category A documents are handled as SECRET. Standard Category A documents include but are not limited to—

- Unmarked maps.
- Maps and charts containing any operational graphics, which are sent to the G2/S2. From G2/S2, they would be evacuated to the all-source analysis center.
- Air Force related documents, which should go to the nearest Air Force headquarters.
- Navy related documents, which should be sent to the nearest Navy headquarters.
- TECHINT-related documents, which are evacuated to the nearest TECHINT unit.
- Cryptographic and communications-related documents, which are evacuated to the nearest SIGINT analysis unit.
- Documents constituting evidence to be used in legal proceedings against persons suspected of crimes against humanity and war crimes,

which will be marked "CRIMINAL EVIDENCE." Such documents will be kept separate from other documents and will be stored under guard or in a secure area until turned over to a war crimes investigative unit. SJA should be consulted concerning chain of custody requirements.

Category B

I-30. Category B documents contain information of intelligence interest to the supported command. The lowest echelon possible exploits the documents and evacuates them through intelligence channels. Category B documents are handled as SECRET.

Category C

I-31. Category C documents and items contain no information of intelligence interest but still require special administrative accountability (for example, currency, works of art, narcotics). Currency is accounted for on DA Form 4137 (Evidence/Property Custody Document).

Category D

I-32. Category D documents contain no information of intelligence value. Only the theater or higher document repository can categorize documents as Category D.

GROUP DOCUMENTS

I-33. CEDs are first grouped according to their assigned screening category. Personnel must be careful when sorting CEDs to ensure no CED is separated from its associated documents. These large groupings can be broken down into smaller groups. Each of these smaller groupings consists of CEDs that were—

- Captured by the same unit.
- Captured in the same place.
- Captured on the same day at the same time.
- Received at the DOCEX element at the same time.

TRANSMITTAL OF CEDS FROM FIRST AND SUBSEQUENT MI UNITS

I-34. Unless they have an HCT in DS, most units that capture or find documents normally have no way of evaluating, categorizing, or otherwise differentiating documents. They are all tagged and evacuated together by the most expedient means through MI channels. Once these documents arrive at a HUMINT collection or DOCEX unit, the unit can screen, categorize, and extract information from the documents. The degree that documents are exploited at each echelon is dependent on mission priorities and available resources. Document handlers must note any attempts to exploit CEDs on the transmittal documents to prevent unnecessary duplication of effort by higher echelons.

I-35. When transportation assets are limited, CEDs are evacuated according to priority based on document categorization. All Category A CEDs will be evacuated first, followed in order by Categories B, C, and D. Documents that have not yet been screened will be evacuated as Category C documents, but the transmittal slip will clearly indicate that the documents have not been screened.

I-36. Documents will be evacuated in accordance with unit SOP and Annex B (Intelligence) in the unit OPORD. Lower priority CEDs, no matter how old, are never evacuated ahead of those with higher priority. CEDs are packaged so that a package of documents contains CEDs of only one category. If the CED cannot be screened because of time or language constraints, it should be treated as a Category C, but kept separate from screened Category C CEDs.

I-37. When CEDs are evacuated from any echelon, a document transmittal sheet is used (Figure I-2). A separate transmittal document is prepared for each group of CEDs to be evacuated. The sending unit prepares a separate transmittal document for each separate addressee. The transmittal identification number is recorded in the captured document log (Figure I-3) as part of the entry for each captured document. Copies of all translations should accompany the documents to avoid duplication of effort. If the sending unit submitted intelligence reports electronically, it should note the report number or include a copy of the report with the document to avoid duplicate reporting.

I-38. All CEDs being evacuated must be accompanied with the appropriate—

- Technical document (TECHDOC) cover sheet.
- SECRET cover sheet on Categories A and B documents.
- Translation reports and hardcopy reports accompanying translated documents.
- Captured document tags.

JOINT DOCUMENT EXPLOITATION FACILITY

I-39. The Theater MI brigade or group is normally tasked with the establishment of the theater JDEF. The JDEF is staffed by Army linguists, supported by technical experts from the Army and from the other services, and supplemented as required by military and civilian contract translators. The JDEF will normally contain MI experts from SIGINT, CI, TECHINT, and other areas as required to identify and exploit documents of interest to these specialties.

I-40. Military and civilian translators must have security clearances appropriate to their mission requirements. This normally equates to at least a Secret clearance since the translators must be made aware of US collection requirements to facilitate their work. The JDEF performs a final examination of all documents of possible theater intelligence value before storing or evacuating them. The DIA sets procedures for exploitation of documents above theater Army level.

DOCUMENT PROCESSING (RECOVERY AND TRANSLATION)

I-41. Units must normally process documents prior to exploiting them. Document processing includes the translation of foreign language documents into English, the recovery of damaged documents, the decryption of encrypted documents, and the extraction of documents from electronic media such as the extraction or downloading of files from a computer disc or hard drive. This need for processing frequently limits the amount of DOCEX that can be done outside a DOCEX facility.

DOCUMENT RECOVERY

I-42. At a minimum, the JDEF manning includes teams trained in extracting and downloading information from electronic media such as computer hard drives. These individuals work in conjunction with TECHINT personnel responsible for the evaluation of captured computer hardware and software. These teams are prepared to deploy forward as necessary to accomplish their mission.

DOCUMENT TRANSLATION

I-43. Translations are not intelligence information reports. They are, however, often a precondition for DOCEX. Once translated, intelligence information can be extracted and reported on an IIR, SALUTE, or similar report. A translation should accompany the original foreign language document; a copy of the translation should accompany any copies of the original foreign language document and, as required, the intelligence reports. A translation report should contain the following information:

- Where the report will be sent.
- Which element prepared the report.
- DTG of the document translation.
- Report number as designated by local SOPs.
- Document number taken from the captured document tag.
- Document description including type of document, number of pages, physical construction of document, and enemy identification number, if applicable.
- Original captured document language.
- DTG document was received at element preparing the report.
- DTG document was captured.
- Place document was captured.
- Identity of capturing unit.
- Circumstances under which document was captured.
- Name of translator.

- Type of translation: full, extract, or summary.
- Remarks for clarification or explanation, including the identification of the portions of the document translated in an extract translation.
- Classification and downgrading instructions in accordance with AR 380-5.

TYPES OF TRANSLATION

I-44. There are three types of translations:

- Full—one in which the entire document is translated. This is both time and manpower intensive, especially for lengthy or highly technical documents. Normally only a DOCEX facility at theater or national level will do full translations, and then only when the value of the information, technical complexity, or political sensitivity of the document requires a full translation. Even when dealing with Category A documents, it may not be necessary to translate the entire document to gain the relevant information it contains.
- Extract—one in which only a portion of the document is translated. For instance, a TECHINT analyst may decide that only a few paragraphs in the middle of a 600-page helicopter maintenance manual merit translation, and that a full translation is not necessary. The analyst would request only what he needed.
- Summary—one in which a translator begins by reading the entire document. He then summarizes the main points of information instead of rendering a full or extract translation. A summary translation is normally written, but may be presented orally, particularly at the tactical level. Summary translations may be done as part of the document screening process. A summary translation requires a translator have more analytical abilities. The translator must balance the need for complete exploitation of the document against time available in combat operations. Translators working in languages of which they have a limited working knowledge may also use a summary translation. For instance, a Russian linguist may not be able to accurately deliver a full translation of a Bulgarian language document. However, he can probably render a usable summary of its content.

TRANSLATOR SUPPORT TO DOCEX

I-45. When HUMINT collectors are not available due to shortages or other mission requirements, DOCEX can be performed by military or civilian linguists under the management of a cadre of HUMINT collectors.

SECURITY REQUIREMENTS

I-46. Document translators will usually need to have a clearance in order to conduct document translation. An exception is that open-source document translation does not require a security clearance unless the information collected from the open-source documents is linked to specific US collection

requirements, plans, or operations. In this case the translator will need a clearance appropriate to the level of the particular contingency plan or operation to which the information is linked. Individuals without a security clearance should not be used in the exploitation of a closed source or CEDs. By their very nature, the translation of these documents gives keys into the level of US knowledge and the direction of US planning and intentions that precludes their translation by individuals without a security clearance.

SOURCES OF TRANSLATORS

I-47. There are various sources that a commander can use to obtain the linguists necessary to support DOCEX operations.

- RC and AC MI linguists. Dependent on their mission requirements, any MI soldiers with the required language qualification may be used as document translators. The advantage of using MI soldiers is that they have the appropriate security clearance and have a firm grasp of collection requirements. The DOCEX operation will usually require MI officers to manage the administrative portions.
- Other linguists. Non-MI Army linguists include numerous soldiers who have proficiency in a foreign language, regardless of MOS. US civilians can be contracted to provide translator support as can local nationals. Local national hires will provide the bulk of the translator support.

REQUIREMENTS FOR A DOCEX OPERATION

I-48. The number of personnel required to conduct DOCEX varies with the echelon and with the volume of documents. Regardless of the size of the operation, certain basic functions must occur:

- Supervision and Administration. These are the C2 and logistical aspects of the DOCEX operation that ensure that operations are smooth and uninterrupted.
- Accountability. Accountability includes logging documents in and out, copying documents as required, storing documents, receiving and transmitting documents, maintaining files, and other routine activities. This ranges from a parttime task for one individual at a low echelon, to warehouse-sized operations involving tons of documents at an EAC document repository.
- Screening. Screening involves the review and categorization of all documents, the prioritization for translation and exploitation, and the identification of documents for special handling and immediate transmittal to specialized units for exploitation. Screening requires senior, experienced individuals well versed in the target language and the collection requirements, capable of making rapid decisions based on minimal information. The number of screeners required depends on the document flow that may range from only a few per day at a low echelon, to literally thousands of documents a day at a theater-level activity.

- Security Requirements. Security requirements include ensuring that the personnel dealing with the documents have the appropriate security level and that they do not pose a security risk to the US. This is particularly important when dealing with non-US translators. Security also evolves ensuring that the documents are marked in accordance with regulation and that proper security measures are in place to prevent compromise of information. At higher echelons, dealing with large numbers of non-US translators normally requires a designated CI team conducting recurring personnel security evaluations.
- Translation. This function involves the directed translation of documents from the target language to English. It requires personnel with the appropriate clearance level who have a working idiomatic knowledge of the target language and English. Higher echelon activities, such as the EAC document repository, group their translation efforts by subject area. For example, one person or group could translate all medical-related documents. At lower echelons, the translators require a more general knowledge. At lower echelons, the same person may translate a document, extract the pertinent information, and report that information. At higher echelons, these are often separate functions.
- Exploitation and Reporting. This task is the identification and extraction of information in response to collection requirements and requires a high level of expertise. The individual must be totally knowledgeable of collection requirements and must be able to readily identify indicators of activity or identify the significance of minute pieces of information that could contribute to answering requirements. Reporting involves placing that extracted information into a coherent, properly formatted report so that the all-source analyst can add it to the intelligence picture.
- Quality Control. This aspect includes ensuring that all aspects of the DOCEX operation—including accounting for, screening, translating, exploiting, and reporting—are functioning correctly.

REPORTING

I-49. Information collected from documents is normally reported in a SALUTE report or an IIR. Reporting through other reporting formats is discouraged. Intelligence reports are normally forwarded electronically or as otherwise directed by SOPs and operational instructions. Normally an electronic or hardcopy file of each report is maintained at the unit of origin; one electronic or hardcopy is submitted through intelligence reporting channels; and one is forwarded with evacuated documents to the next unit to receive the document to prevent redundant reporting. In the event that the document itself cannot be evacuated in a timely manner, a verified copy of a translation report can be forwarded separately from the original document to an exploitation agency.

DOCUMENT EXPLOITATION IN SUPPORT OF HUMINT COLLECTION

I-50. Documents found on detainees, including EPWs—that can be exploited more efficiently when combined with HUMINT collection—are forwarded with the detainee to the next echelon in the EPW/detainee evacuation channel. In exceptional cases, documents may be evacuated ahead of the EPW or other detainee for advance study by intelligence units. A notation should be made on the EPW's capture tag or accompanying administrative papers about the existence of such documents and their location if they become separated from the detainee.

SOURCE-ASSOCIATED DOCUMENTS

I-51. Documents captured on or in association with a human source play an important role in the HUMINT collection process. These documents may contain reportable information the same as with any other CED. The information is immediately extracted from the documents and forwarded in the appropriate intelligence report. In addition to reportable information, documents (in particular personal documents) may provide valuable insight into the attitude and motivation of the source and can be effectively used by the HUMINT collector in the approach process (see Chapter 8). Guidelines for the disposition of the detainee's documents and valuables are set by international agreements and discussed in more detail in AR 190-8 and FM 19-4.

I-52. The capturing unit removes all documents, with the exception of the source's primary identification document, from an EPW or other detainee to prevent their destruction. These are placed in a waterproof container (usually a plastic bag) and Part C of the capture tag is placed in the bag. Documents from each source should be placed in a separate bag. These documents are turned over to the first MP EPW handling unit in the chain of command. The MPs will inventory all documents and prepare a handreceipt and provide a copy to the EPW or detainee.

I-53. To ensure proper handling and expeditious disposition of these documents, the first HUMINT collection element to see the detainee should review the documents as part of the source screening process. If an official document is confiscated and evacuated through MI channels, the HUMINT collector must obtain a receipt for that document from the MPs. If possible, the HUMINT collection unit copies any documents that contain information of intelligence interest and forwards the copies through MI channels. With the exception of an identification document, documents are normally kept separate from the detainee until the detainee arrives at a permanent confinement facility, at which time documents are returned to them per AR 190-8.

I-54. Three possible actions may be taken with documents captured with a source. The documents may be confiscated, impounded, or returned to the source.

Confiscated

I-55. Documents confiscated from a source are taken away with no intention of returning them. Official documents, except identification documents, are confiscated and appropriately evacuated. The intelligence value of the document should be weighed against the document's support in the HUMINT collection of the source. The HUMINT collector must comply with the accounting procedures established for CEDs by the MPs in accordance with AR 190-8.

Impounded

I-56. Some CEDs will contain information that must be exploited at higher echelons. These documents may be impounded by the HUMINT collector and evacuated through intelligence channels. The HUMINT collector must issue a receipt to the source for any personal documents that he impounds. He must comply with the accounting procedures established for CEDs impounded by the MPs in accordance with AR 190-8. When a CED is impounded, it is taken with the intent of eventual return. Personal documents with military information will be impounded if the military value is greater than the sentimental value. An example of a personal document whose military value might outweigh the sentimental value could be a personal photograph that includes military installations or equipment.

I-57. When a CED is impounded, it must be receipted. The receipt will include an itemized list of all the items taken from the prisoner, and the name, rank, and unit of the person issuing the receipt. Items of high value may be impounded for security reasons. For instance, an EPW or detainee apprehended with an unusually large amount of money would have the money impounded and receipted. The MPs will establish and maintain a DA Form 4237-R (Detainee Personnel Record) for impounded items. The register will identity the owner of the impounded items and provide a detailed description of the items impounded. A receipt will be given to anyone who has items impounded. Also, the OIC or authorized representative will complete and sign DA Form 1132-R (Prisoner's Personal Property List – Personal Deposit Fund). A copy will be provided the source. See AR 190-8 for procedures on handling personal effects.

Returned

I-58. Returned CEDs are usually personal in nature. They are taken only to be inspected for information of interest and are given back to the source. Personal documents belonging to a source will be returned to the source after examination in accordance with the GPW. These documents are CEDs whose sentimental value outweighs their military value and may be returned to the source. Copies of these documents may be made and forwarded if deemed necessary. Except for an identification document (which is always returned to the source), documents are evacuated with the source, rather than on the source, until the source reaches a permanent confinement facility at EAC.

This page intentionally left blank.

Appendix J

References

The following references are provided to assist HUMINT collectors, commanders, and trainers in obtaining regulatory guidance for HUMINT collection operations. These and other references are in the bibliography.

1. AR 350-1. *Army Training and Education.* 9 April 2003.
2. AR 380-5. *Department of the Army Information Security Program.* September 2000.
3. AR 380-10. *Technology Transfer, Disclosure of Information, and Contacts with Foreign Representatives.* 15 February 2001.
4. AR 380-15. *(C) Safeguarding NATO Classified Information.* 1 March 1984.
5. AR 380-28. *Department of the Army Special Security System*. 12 December 1991.
6. AR 380-40. *Policy for Controlling and Safeguarding Communications Security (COMSEC) Material.* 22 October 1990.
7. AR 380-49. *Industrial Security.* 15 April 1982.
8. AR 380-53. *Telecommunications Security Monitoring*. 29 April 1998.
9. AR 380-67. *Personnel Security Program*. 9 September 1988.
10. AR 381-1. *Security Controls on Dissemination of Intelligence Information.* 12 February 1990.
11. AR 381-10. *U.S. Army Intelligence Activities*. 1 July 1984.
12. AR 381-12. *Subversion and Espionage Directed Against the US Army (SAEDA).* 15 January 1993.
13. AR 381-14. *Technical Counterintelligence (TCI).* 30 September 2002.
14. AR 381-20. *(U) US Army Counterintelligence Activities (S).* 26 September 1986.
15. AR 381-45. *Investigative Records Repository*. 25 August 1989.
16. AR 381-47. *(U) US Army Offensive Counterespionage Activities (S).* 30 July 1990.
17. AR 381-100. *(U) Army Human Intelligence Collection Program (S).* 15 May 1988.
18. AR 381-102. *(U) US Army Cover Support Program (S).* 10 January 1991.
19. AR 381-143. *Military Intelligence Nonstandard Material Policies and Procedures.* 1 December 1986.

20. AR 381-172. *Counterintelligence Force Protection Source Operations and Low-Level Source Operations*. 30 December 1994.

21. AR 614-115. *Military Intelligence Excepted Career Program*. 12 April 2004.

22. AR 614-200. *Military Intelligence Civilian Excepted Career Program*. 30 September 2004.

23. DA Pam 381-15. *Foreign Military Intelligence Collection Activities Program*. 1 June 1988.

24. Executive Order 12333. *United States Intelligence Activities*. 4 December 1981.

25. DOD Directive 2310.1. *DOD Program for Enemy Prisoners of War (EPOW) and Detainees (Short Title: DOD Enemy POW Detainee Program)*. 18 August 1994.

26. DOD Directive 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*. 3 November 2005.

27. DOD Directive 5100.77. *DOD Law of War Program*. 9 December 1998.

28. DOD Directive 5240.1. *DOD Intelligence Activities*. 3 December 1982.

29. DOD Instruction 3020.41. *Contractor Personnel Authorized to Accompany the U.S. Armed Forces*. 3 October 2005.

30. The Under Secretary of Defense for Intelligence (USD(I) Memorandum, *Guidance for the Conduct and Oversight of Defense Human Intelligence (HUMINT) (U)*. 14 December 2004.

31. USD(I) Memorandum, Implementation Instructions for USD(I) Memorandum, *Guidance for the Conduct and Oversight of Defense Human Intelligence HUMINT* (U). 7 September 2005.

32. DOD Regulation 5240.0-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*. December 1982.

33. Detainee Treatment Act of 2005, Public Law No. 109-163, Title XIV.

Further information and links to many of the above publications can be found at: http://www.dami.army.pentagon.mil/offices/dami-cd/

ARTEPS, MTPs, and other intelligence training products are available at the Reimer Digital Library http://www.adtdl.army.mil.

Appendix K

Contract Interrogators

INTRODUCTION

K-1. Contractors are used increasingly to augment existing capabilities and bridge gaps in the deployed force structure. With the increased use of contractors comes the need to identify the doctrine and procedures affecting their employment. Leaders and those working with contractors must understand that contractors are civilians authorized to accompany the force in the field and should be provided with an ID card as proof of their authorization. In accordance with GPW Article 4, contractors are to be accorded POW status if captured.

KEY TERMS

K-2. **Contract Interrogator.** A contract interrogator is a contractor who is specifically trained and DOD certified for, tasked with, and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. Their operations must be conducted in accordance with all applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Contract interrogators will operate only in fixed facilities and not in tactical operations. See DOD Instruction 3020.41 for additional information.

K-3. **External Support Contractor.** Contract interrogators fall into the category of External Support Contractor**.** They work under contracts awarded by contracting officers serving under the command and procurement authority of supporting headquarters outside the theater. Their support augments the commander's organic capability.

K-4. **Contracting Officer Representative (COR).** A COR is the contracting officer's designated representative who assists in the technical monitoring and administration of a contract. Typically, a COR is responsible for assisting the contracting officer in contractor-employee day-to-day management of issues that may affect contractor or unit requirements.

K-5. Statement of Work (SOW) or Performance Work Statement:

- Contractor roles and functional requirements, as well as security issues and the relationship to the military chain of command, must be accurately and adequately defined in the SOW. The SOW should include a description of the essential service and require the contractor

to prepare contingency plans to reasonably ensure continuation. Contractors are required to perform all tasks identified within the SOW and all other provisions defined within the contract. The SOW may also stipulate the appointment of a senior contractor at each echelon or facility to be the point of contact for the commander and the COR for resolving contract performance and scheduling challenges.

- The contract must stipulate whether the duty of a senior contractor is an additional duty or the full-time job of the selected contractor. Considering that contractors are "managed" rather than "commanded," having a senior contractor will assist the commander in managing the contract. Without an onsite contractor supervisor, the default chain of command for contract interrogators might otherwise reside in CONUS, at the contractor's headquarters.

CIVILIAN STATUS

K-6. A contract employee cannot be made to engage in any activity inconsistent with his civilian status such as serving as a crew member on a weapon system. Interrogations are presumptively consistent with civilian contractor status, but other tasks should be vetted with the command's legal advisor to ensure they are legally permissible.

COMMAND CONSIDERATIONS

K-7. Theaters in which large-scale operations are conducted are very likely to employ contract interrogators, due to limited numbers of Army HUMINT collectors available. The presence of contractors in the AO adds an additional dimension to the commander's planning process. Force protection is a critical issue. Even in "permissive" environments such as in the case of humanitarian operations, contractors may be placed in danger. The commander must protect his contractors since they have limited capacity to protect themselves.

K-8. The commander has no command authority over contractor personnel. Their relationship with the Government is governed by the terms and conditions of their contract. In short, the commander must "manage" contractor personnel through the contracting process. He has no authority to command or discipline them unless it is a declared war, at which time contractors may fall under the provisions of the UCMJ. This distinction between command and management does not prohibit the commander from directing contractors to carry out essential activities, such as activities related to security and safety, consistent with the terms of their contracts.

K-9. The terms and conditions of any contract must be constructed so as to include provisions requiring contractor personnel to abide by all guidance and obey all instructions and general orders applicable to US Armed Forces and DOD civilians including those issued by the Theater Commander. The contractor can be required to "take reasonable steps" to ensure his personnel comply with the above and to ensure "the good conduct" of his employees. Furthermore, the contractor can be required to promptly resolve, to the satisfaction of the COR, all contractor employee performance and conduct problems identified by the COR. The COR can direct the

contractor, at the contractor's expense (for example, a non-allowable charge to the contract) to remove and replace any contractor employee failing to comply with the above. This provides a significant tool to aid in achieving good order and discipline within an AO. The commander also has the authority to initiate proceedings that could lead to charges under Military Extraterritorial Jurisdiction Act (MEJA) or the War Crimes Act.

K-10. Contractors will be subject to the extraterritorial jurisdiction of the United States and will comply with all applicable law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs. Contractor misconduct may be subject to prosecution under federal jurisdiction pursuant to the MEJA or the War Crimes Act, or both. Procedures for initiating investigation into such misconduct will normally be established by the operational command.

K-11. The operational command will also establish procedures for referral to federal civilian authorities and necessary pre-trial confinement. Contractors normally will also be subject to the criminal jurisdiction of the HN unless granted immunity from jurisdiction through the provisions of a SOFA or equivalent agreement, or unless the HN waives jurisdiction. As a general rule, contractors are not subject to the UCMJ (with the possible exception for periods of formally declared war).

K-12. The commander should expect contractors to use all means at their disposal to continue to provide essential services, in accordance with the terms and conditions of contracts, until the military releases them. The combatant commander determines when to execute contingency plans for essential services and when to release a contractor.

INTERROGATOR CONTRACT CONSIDERATIONS

K-13. Contracts should be written with the following principles and considerations:

- Contractors will be deployable under all operational scenarios. They will be subject to the same time-phased force deployment data requirements as deploying military units.
- The contractor information system will interface with the Standard Army Management Information System at both retail and wholesale levels. Army units should not have to contend with two separate information systems.
- The contractors will provide interrogation support at fixed facilities as needed. During deployments, the commander (subject to contract terms and conditions) will determine where contractors operate in their AO.
- The contractors will not replace force structure. They will augment Army capabilities and provide an additional option for meeting support requirements.

- Force protection, including the protection of contractors, is the responsibility of commanders.
- The unit must integrate contractor support into the overall support plan. Transportation of contractors on the battlefield must be planned.
- Command and control of contract personnel is dependent upon terms and conditions of the contract. The contracting officer or his designated representative is the appointed liaison for monitoring contractor performance requirements and will ensure that contractors move material and personnel according to the combatant commander's plan. A good technique is for the command to designate and train a unit COR or Contracting Officer's Technical Representative (COTR) at each facility where contract interrogators will be working. Because international and domestic law, including SOFAs, affect the relationship between commanders and contract personnel, commanders and CORs should seek legal advice concerning issues arising during operations.
- The unit must establish a contractor personnel reporting and accountability system. Again, a good technique is for the command to designate and train a unit COR or TCOR at each facility where contract interrogators will be working.
- During deployments, contractors will live and work in field conditions comparable to those for the supported ARFOR. Living arrangements, transportation requirements, food, medical, and other support services will be provided according to the contract. These services may include but are not limited to—
  - Non-routine medical and dental care.
  - Mess.
  - Quarters.
  - Special clothing, equipment, weapons, or training mandated by the applicable commander.
  - Mail.
  - Emergency notification.
- Planning must be accomplished to ensure agreed upon support to contractors is available to the responsible commander.

CONTRACT INTERROGATOR REQUIREMENTS

SELECTION AND EMPLOYMENT CRITERIA

K-14. Contract personnel must meet certain minimum requirements to be qualified to work as contract interrogators. It is the responsibility of the hiring contracting company to ensure that these criteria, set by the Government, are met by the personnel they hire.

K-15. Policy will dictate employment criteria such as minimum education, military service, security clearance, and previous training. Certain civilian experience and training may also meet the policy requirements for contract

interrogator qualifications. Commanders and CORs should refer to the current DA policy on contract interrogators for appropriate guidance.

TRAINING REQUIREMENTS

K-16. All contractor interrogators must successfully complete a training program approved by the United States Army Intelligence Center and Fort Huachuca, or the Defense HUMINT Management Office, which will serve as validation to perform MI interrogations (see DODD 3115.09). The organization Commander or Director initiating the contract must certify that the training has been completed. The training program will ensure that contract interrogators are trained and certified on—

- The most current TTP of interrogation as promulgated by DOD.
- The applicable law and policy related to the treatment of detainees. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

K-17. Contract interrogators must also receive training on the supported unit's mission and Interrogation Counter-Resistance Policy pertinent to the AOR they are supporting. This training will be conducted in-theater by the gaining unit.

EQUIPMENT

K-18. Contractors must be issued personal protection gear appropriate for the threat environment. This may include ballistic helmet, personal body armor, NBC protective gear, and in certain circumstances a personal weapon. Contract interrogators must have access to automation equipment to support their mission of intelligence collection and reporting.

UTILIZATION

K-19. Only trained and certified contractors working under the supervision of MI personnel are authorized to conduct interrogations. Contract interrogators may conduct interrogations with an interpreter in the room; however, an OIC or NCO will monitor the interrogation by personal presence or by means of live video camera feed.

K-20. Contract interrogators—

- Will not supervise any military personnel or federal government employees, nor will they be in charge of interrogation facilities.
- Will operate only in fixed facilities. This requirement provides a measure of force protection to the contract interrogator and frees up Army HUMINT collectors for tactical missions.
- Must submit a written interrogation plan to the OIC or NCOIC, and receive approval for the plan, in advance of each interrogation. The plan will specify the information desired and identify what techniques

and approaches for obtaining information will be used to conduct the interrogations.

WORK LOCATIONS

K-21. The commander may position contract interrogators in fixed detention facilities anywhere in the theater, in accordance with the terms and conditions of their contract.

ATTIRE

K-22. Contractors accompanying the force should be visibly distinct from soldiers so as not to jeopardize their status. The JTF or combatant commander may direct contract personnel to wear civilian clothing or a uniform that says "civilian." Specific items of military attire required for safety or security may also be worn, such as chemical defense equipment, cold weather equipment, or mission specific safety equipment.

FIRE ARMS

K-23. A contractor authorized to accompany the force in the field is *not entitled* to be issued a firearm. However, a contract employee may be armed only if **all** of following conditions are met:

- The theater commander grants his approval.
- The employee's corporate policy allows it.
- The employee agrees.

K-24. If all three conditions are met, then the employee must pass proper military side-arm training and will be issued a military specification weapon and ammunition (generally, a 9-millimeter pistol) for *personal protection*. The contractor must also comply with all applicable DOD, service, and local command policies on weapons.

RECOMMENDED READING

DOD Instruction 3020.41. *Contractor Personnel Authorized to Accompany the U.S. Armed Forces.* 3 October 2005.

AR 715-9. *Contractors Accompanying the Force*. 29 October 1999.

DA Pamphlet 715-16. *Contractor Deployment Guide*. 27 February 1998.

FM 3-100.21. *Contractors on the Battlefield*. 3 January 2003.

FM 63-11. *Logistics Support Element Tactics, Techniques, and Procedures*. 8 October 1996.

AMC Pamphlet 715-18. *AMC Contracts and Contractors Supporting Military Operations*. June 2000.

Appendix L

Sample Equipment for HCT Operations

L-1. This materiel and equipment list is provided as a sample of what an HCT may require to support the commander's intelligence requirements. Some of the equipment that is intended to be given to a source should be considered expendable.

L-2. HCT Kit Bag - Assumes four-person configuration for each echelon. Regardless of support relationship (Organic/DS/GS/GSR), HCTs inherently require the following.

L-3. Movement/Survivability/Security:

- Two M998 1-¼ ton vehicle (or non-tactical vehicle as appropriate for mission) per team.
- One crew/squad served weapon per team.
- One M16A2 per team.
- Three M4s per team.
- Four 9mms per team.
- M68 Aim-point System.
- One x body armor with protective plate per team member.

L-4. Collection and Reporting System - Hardware 1 x System per HCT:

- Scaleable collection and reporting tool that changes configuration depending on where it is on the battlefield.
- Should include an individual collection and reporting tool.
- Should include a tool for stand-alone SIPRNET connectivity via satellite or other.

L-5. Collection and Reporting System - Software 1 x per System:

- Simple, intuitive Graphic User Interface (GUI).
- Standardized Reports - SALUTE, IIR, Tactical Interrogation Report, Contact Report, BSD Report. (Policy states that once filled out, the BSD becomes classified; therefore, change policy or make the collection or reporting tool classified as well.)
- Source Management Tool.
- CI Investigations Reports.
- Link Analysis (capable of interface with coalition systems—in this case, Analyst Notebook).
- Mapping - Single, standardized tool (down to 1:12,500 scale maps, operational graphics, GPS interface).

- Biometrics Integration/Biometrics Enrollment Tools (Integrated Automated Fingerprint Identification System [IAFIS]-compliant 10-print fingerprint scanners, iris scanners, photographing station).
- Basic DOCEX application.
- Foreign Language Translation.
- Mission Planning Software.
- Query Tools: basic, advanced, multi-entity, multi-media, save user-defined queries.

L-6. Collection and Reporting System - Peripherals 1 x HCT:

- Digital video/still.
- Printer with print and scanner head (photo quality with ports for flash cards/memory sticks).
- Separate collection kit for biometrics (ink/card packets and/or IAFIS-compliant live scanner, iris scanner). Must be FBI compliant and portable).
- GPS.
- Digital voice recorder (Universal Serial Bus [USB] interface).

L-7. Communications - Requires organic communications systems to higher and laterally (non-line of sight and line of sight):

- Intra-team communications - 1 x individual:
  - Secure or nonsecure (prefer secure).
  - Hands-free and/or handheld.
- Team to all - 1 x HCT:
  - Secure.
  - FM/UHF/Microwave.
  - Line of sight.
  - Non-line of sight.
  - Voice.
  - Digital.
  - Cellular telephone:
    - Voice.
    - Backup for transmitting data.
    - GPS enabled.
  - Friendly force identification and tracking system.
- HCT to Source - 2 sets x HCT:
  - Phone cards.
  - Cell phones.
  - Radios.
  - Email or “Blackberry-like” communications.
  - One-way pager.
  - Clandestine signaling.

L-8. Source Support - 2 sets x HCT:

- Source tracking (blue-force tracker-like capability).
- Digital Voice Recorder (micro, USB interface).
- Digital video or still camera, with telephoto lenses.
- GPS.
- 1 x 1Gb Thumb Drive.

L-9. Data Storage - 1 x HCT:

- 2 x hard drives (one for UNCLASS, one for SECRET).
- 2 x Micro/Thumb, 1Gb drive (one for UNCLASS, one for SECRET).

L-10. Power Generation - 1 x liquid fuel generator or high-capacity (12-hour) (battery - silent, vehicle recharge), power source - 1 x HCT.

L-11. 1 x Universal Power Conversion Kit per HCT and OMT.

L-12. Vision Enhancement:

- 2 x night vision goggles (NVG) per HCT.
- 1 x thermal sensor per HCT.
- 1 x binoculars per individual (4 each).
- 1 x laser range finder per HCT.

This page intentionally left blank.

Appendix M

Restricted Interrogation Technique – Separation

INTRODUCTION

M-1. As part of the Army's efforts to gain actionable intelligence in the war on terrorism, HUMINT collectors may be authorized, in accordance with this appendix, to employ the separation interrogation technique, by exception, to meet unique and critical operational requirements. The purpose of separation is to deny the detainee the opportunity to communicate with other detainees in order to keep him from learning counter-resistance techniques or gathering new information to support a cover story; decreasing the detainee's resistance to interrogation. Separation, further described in paragraphs M-2 and M-28, is the only restricted interrogation technique that may be authorized for use. Separation will only be used during the interrogation of specific unlawful enemy combatants for whom proper approvals have been granted in accordance with this appendix. However, separation may **not** be employed on detainees covered by Geneva Convention Relative to the Treatment of Prisoners of War (GPW), primarily enemy prisoners of war (EPWs). The separation technique will be used only at COCOM-approved locations. Separation may be employed in combination with authorized interrogation approaches—

- On specific unlawful enemy combatants.
- To help overcome resistance and gain actionable intelligence.
- To safeguard US and coalition forces.
- To protect US interests.

GENERAL

M-2. This appendix provides doctrinal guidance for the use of separation as an interrogation technique. Separation involves removing the detainee from other detainees and their environment, while still complying with the basic standards of humane treatment and prohibitions against torture or cruel, inhuman, or degrading treatment or punishment, as defined in the Detainee Treatment Act of 2005 and addressed in GPW Article 3 (Common Article III). Separation is to be distinguished from segregation, which refers to removing a detainee from other detainees and their environment for legitimate purposes unrelated to interrogation, such as when necessary for the movement, health, safety and/or security of the detainee, or the detention facility or its personnel. This appendix—

- Will be reviewed annually and may be amended or updated from time to time to account for changes in doctrine, policy, or law, and to address lessons learned.
- Is not a stand-alone doctrinal product and must be used in conjunction with the main portion of this manual.

M-3. Careful consideration should be given prior to employing separation as an interrogation technique in order to mitigate the risks associated with its use. The use of separation should not be confused with the detainee-handling techniques approved in Appendix D. Specifically, the use of segregation during prisoner handling (Search, Silence, Segregate, Speed, Safeguard, and Tag [5 S's and a T]) should not be confused with the use of separation as a restricted interrogation technique.

M-4. Members of all DOD Components are required to comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations. Proper application of separation as a restricted interrogation technique in selective cases involving specific unlawful enemy combatants and in accordance with the safeguards outlined in this manual is consistent with the minimum humane standards of treatment required by US law, the law of war; and does not constitute cruel, inhuman, or degrading treatment or punishment as defined in the Detainee Treatment Act of 2005 and addressed in GPW Common Article III.

M-5. Use of separation for interrogation is authorized by exception. Separation will be applied on a case-by-case basis when there is a good basis to believe that the detainee is likely to possess important intelligence and the interrogation approach techniques provided in Chapter 8 are insufficient. Separation should be used as part of a well-orchestrated strategy involving the innovative application of unrestricted approach techniques. Separation requires special approval, judicious execution, special control measures, and rigorous oversight.

M-6. Additionally, the use of separation as a restricted interrogation technique shall be conducted humanely in accordance with applicable law and policy. Applicable law and policy for purposes of this appendix include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, "The Department of Defense Detainee Program"; DOD instructions; and military execute orders including FRAGOs.

M-7. More stringent than normal safeguards must be applied when using the separation technique. Use of separation is subject to USD(I) oversight. Compared to approach techniques, there are two additional steps in the approval process (see Figure M-l) for the use of the separation technique:

- First, the COCOM Commander approves (after SJA review) use of the separation technique in theater.
- Second, following the COCOM Commander's approval, the first General Officer/Flag Officer (GO/FO) in an interrogator's chain of command approves each specific use of separation and the interrogation plan that implements separation (this is non-delegable). Interrogation supervisors shall have their servicing SJA review the interrogation plan before submitting it to the GO/FO for approval.

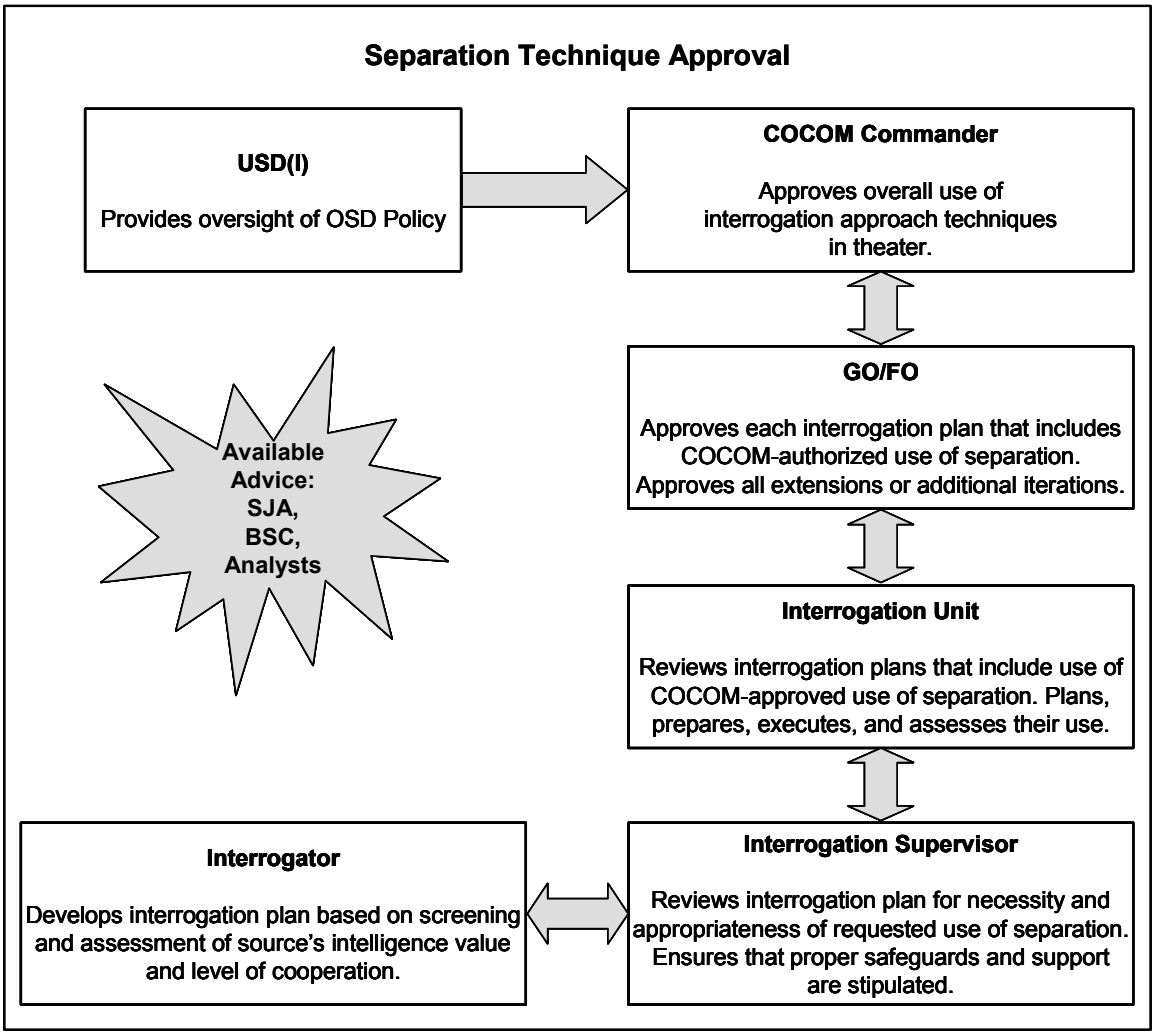


Figure M-1. Separation Approval Process.

M-8. The employment of separation requires notification, acknowledgment, and periodic review, in accordance with USD(I) Memorandum, "(S//NF) Guidance for the Conduct and Oversight of Defense Human Intelligence (HUMINT) (U)," dated 14 December 2004. This means that after the separation is approved for use by COCOMs, the I&WS must be notified as soon as practical. The Office of the Secretary of Defense will review these activities periodically in accordance with DOD Directive 3115.09.

M-9. The planning process for the employment of standard interrogation operations also applies to the employment of the separation technique (see Chapter 4).

RESPONSIBILITIES

M-10. Commanders of interrogation or detention facilities and forces employing the approved separation technique are responsible for compliance with applicable law and policy. Commanders must understand that separation poses a higher risk to the detainee than do standard techniques, and so require strenuous oversight to avoid misapplication and potential abuse.

M-11. The interrogation chain of command must coordinate the interrogation plan with the detention operations commander. Close coordination must occur between intelligence personnel and personnel responsible for detainee operations, including MP, security forces, Master at Arms, and other individuals providing security for detainees (hereafter referred to as guards). Guards do not conduct intelligence interrogations and, in accordance with DOD Directive 3115.09, will not set the conditions for interrogations. Guards may support interrogators as requested for detainee custody, control, escort, and/or additional security (for example, for combative detainees), in accordance with paragraphs 5-57 through 5-66 and FM 3-19.40, JP 3-63, and the approved interrogation plan.

M-12. The detention operations commander (in conjunction with the MI commander) may convene a multidiscipline custody and control oversight team including, but not limited to, MP, MI, BSC (if available), and legal representatives. The team can advise and provide measures to ensure effective custody and control in compliance with applicable law and policy.

M-13. Commanders must consider the following when employing separation:

- Is separation directed against the appropriate individual and is it necessary for collecting important intelligence?
- Does separation complement the overall interrogation strategy and interrogation approach technique or techniques?
- Is the application of separation with the specific detainee at issue consistent with humane treatment and in accordance with applicable law and policy?

M-14. Planning for the use of separation requires coordination with staff elements that provide support to interrogation operations. Staff elements that support interrogation facilities and forces employing separation will comply with paragraphs 4-59 and 4-60 and all controls and safeguards identified in paragraphs M-17 through M-26.

GENERAL CONTROLS AND SAFEGUARDS

HUMANE TREATMENT

M-15. All captured or detained personnel shall be treated humanely at all times and in accordance with DOD Directive 3115.09, "DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning"; DOD Directive 2310.1E, “Department of Defense Detainee Program,” and no person in the custody or under the control of the DOD, regardless of nationality or physical location, shall be subject to cruel, inhuman, or degrading treatment or punishment as defined in US law, including the

Detainee Treatment Act of 2005. All intelligence interrogations, debriefings, or tactical questioning to gain intelligence from captured or detained personnel shall be conducted in accordance with applicable law and policy.

M-16. Any inhumane treatment—including abusive practices, torture, or cruel, inhuman, or degrading treatment or punishment as defined in US law, including the Detainee Treatment Act of 2005—is prohibited and all instances of such treatment will be reported immediately in accordance with paragraph 5-69 thru 5-72. Beyond being impermissible, these unlawful and unauthorized forms of treatment are unproductive because they may yield unreliable results, damage subsequent collection efforts, and result in extremely negative consequences at national and international levels. Review by the servicing SJA is required prior to using separation. Each interrogation plan must include specific safeguards to be followed: limits on duration, interval between applications, and termination criteria. Medical personnel will be available to respond in the event a medical emergency occurs.

FM 2-22.3 REQUIREMENTS

M-17. Separation must be employed in accordance with the standards in this manual. These standards include the following:

- Prohibitions against abusive and unlawful actions (see para 5-75) and against the employment of military working dogs in the conduct of interrogation (see paras 5-59 and 8-2).
- Requirement for non-DOD agencies to observe the same standards for the conduct of interrogation operations and treatment of detainees when in DOD facilities (see para 5-55).
- Prohibition on guards conducting intelligence interrogations or taking any actions to set the conditions for interrogations. Humane treatment, evacuation, custody and control (reception, processing, administration, internment, and safety) of detainees; force protection; and the operation of the internment facility are discussed in paragraphs 5-57 through 5-66. (FM 3-19 .40 and JP 3-63 also thoroughly discuss detainee operations.)
- Assignment of ISNs to all detainees in DOD control, whether or not interrogation has commenced, as soon as possible; normally within 14 days of capture. (See AR 190-8 and Secretary of Defense Memorandum dated 20 September 2005, "(S//NF) Policy on Assigning Detainee Internment Serial Numbers (ISN)(U)."
- Access to detainees by the ICRC.

REPORTING OF ABUSES AND SUSPECTED ABUSES

M-18. As an interrogation technique, separation is particularly sensitive due to the possibility that it could be perceived as an impermissible act. Interrogators applying the separation technique and the chain of command supervising must be acutely sensitive to the application of the technique to ensure that the line between permissible or lawful actions and impermissible or unlawful actions is distinct and maintained. Therefore, HUMINT collectors should have heightened awareness and understanding of the risks,

control measures, and safeguards associated with the use of separation. Any interrogation technique that appears to be cruel, inhuman, or degrading as defined in US law; or impermissibly coercive, or is not listed in this manual, is prohibited and should be reported immediately to the chain of command or other appropriate channels for resolution. Orders given to treat detainees inhumanely are unlawful. Every interrogator must know how to respond to orders that the individual interrogator perceives to be unlawful (see paras 5-80 through 5-82).

M-19. If the order is a lawful order, it should be obeyed. Failure to obey a lawful order is an offense under the UCMJ.

COMMAND POLICY AND OPERATION ORDERS

M-20. The provisions of this appendix must be written into COCOM policy and/or OPORDs when using the restricted interrogation technique of separation.

MEDICAL

M-21. Commanders are responsible to ensure that detainees undergoing separation during interrogation receive adequate health care as described in greater detail in paragraph 5-91.

TRAINING AND CERTIFICATION

M-22. Only those DOD interrogators who have been trained and certified by the United States Army Intelligence Center (USAIC), or other Defense HUMINT Management Office (DHMO) designated agency, in accordance with guidance established by USD(I) to use separation, are authorized to employ this technique. The training must meet certification standards established by the Defense HUMINT Manager in coordination with applicable DOD components. Properly trained and certified contract interrogators are authorized to initiate interrogation plans that request the use separation, and, once the plan is approved, to employ the technique in accordance with the provisions of this appendix and Appendix K. Contract interrogators will always be utilized under the supervision and control of US government or military personnel (see para K-19 and K- 20). Non-DOD personnel conducting interrogations in DOD facilities must be certified by their agency and separately gain approval (through their agency's chain of command) for the additional technique described in this appendix. They must present this written certification and agency approval to the COCOM before use is permitted (see para 5-55).

PLANNING

M-23. Planning for the use of separation must include—

- An interrogation plan that addresses safeguards, limits of duration, interval between applications, termination criteria, and presence of qualified medical personnel for emergencies (see Figure M-2).
- A provision for detainees to be checked periodically in accordance with command health care directives, guidance, and SOPs applicable to all detainees.
- A legal review.

Page _____ of _____

INTERROGATION PLAN
FOR USE OF
RESTRICTED SEPARATION TECHNIQUE

THIS FORM IS TO BE COMPLETED IN CONJUNCTION WITH, AND MAINTAINED WITH, THE BASE INTERROGATION PLAN, FIGURE 10-3, FM 2-22.3. USE ADDITIONAL FORMS AS NEDED.

COCOM/SECDEF ORDER OR PLAN #:_____

RESTRICTED TECHNIQUE STRATEGY:

JUSTIFICATION:_____

_____

_____

_____

USED IN CONJUNCTION WITH THE FOLLOWING APPROACH STRATEGIES:_____

_____

SPECIFIC DESCRIPTION OF THE SEPARATION TECHNIQUE EMPLOYMENT STRATEGY:_____

_____

_____

_____

_____

PROPOSED DURATION:_____ REQUIRED BREAK:_____

SPECIFIC SAFEGUARDS AND OVERSIGHT TO BE EMPLOYED:

GUARDS:_____

_____

_____

INTERROGATORS:_____

_____

OTHER:_____

_____

DOCUMENTATION OF USE: (PHOTOS, VIDEO, NOTES)_____

_____

TERMINATION CRITERIA TECHNIQUE:_____

REVIEW: Interrogation Supervisor:_____ MI Unit Cdr:_____ GO/OF SJA_____

APPROVAL AUTHORITY:	PRINTED NAME	DTG OF APPROVAL
GENERAL OFFICER/FLAG OFFICER	_____	_____
APPROVED FOR _____		DURATION
MI UNIT COMMANDER	_____	_____
INTERROGATION SUPERVISOR	_____	_____

SAMPLE

Figure M-2. Installation Plan for Restricted Separation Techniques.

- Documentation of the use of separation, including photographs and/or videotaping, if appropriate and available (see para 5-54).

M-24. Separation is only authorized for use in interrogation operations, not for other Military Source Operations. Separation may be approved for use in combination with authorized approach techniques. General controls and safeguards contained in this manual must be applied during the use separation, in conjunction with the safeguards specific to the separation technique. **Planning must consider the possible cumulative effect of using multiple techniques and take into account the age, sex, and health of detainees, as appropriate.**

TECHNICAL CONTROL

M-25. Requests for approval of separation will be forwarded (for information purposes only) via secure means through intelligence technical channels at the same time as they are sent through command channels. Intelligence technical channels are those used for forwarding of source information and technical parameters of collection operations from lower to higher and passing tasking specifics, source information, technical control measures, and other sensitive information from higher to lower. The technical chain extends from the HCT through the OMT and Operations Section (if one exists) to the C/J/G/S2X.

APPLICATION OF SEPARATION TECHNIQUE

M-26. The purpose of separation is to deny the detainee the opportunity to communicate with other detainees in order to keep him from learning counter-resistance techniques or gathering new information to support a cover story, decreasing the detainee's resistance to interrogation. Separation does not constitute sensory deprivation, which is prohibited. For the purposes of this manual, sensory deprivation is defined as an arranged situation causing significant psychological distress due to a prolonged absence, or significant reduction, of the usual external stimuli and perceptual opportunities. Sensory deprivation may result in extreme anxiety, hallucinations, bizarre thoughts, depression, and anti-social behavior. Detainees will not be subjected to sensory deprivation.

M-27. Physical separation is the best and preferred method of separation. As a last resort, when physical separation of detainees is not feasible, goggles or blindfolds and earmuffs may be utilized as a field expedient method to generate a perception of separation.

M-28. Objectives:

- Physical Separation: Prevent the detainee from communicating with other detainees (which might increase the detainee's resistance to interrogation) and foster a feeling of futility.
- Field Expedient Separation: Prolong the shock of capture. Prevent the detainee from communicating with other detainees (which might increase the detainee's resistance to interrogation) and foster a feeling of futility.

M-29. Safeguards:

- **Duration:** Self-explanatory.
- **Physical Separation:** Limited to 30 days of initial duration.
- **Field Expedient Separation:** Limited to 12 hours of initial duration at the initial interrogation site. This limit on duration does not include the time that goggles or blindfolds and earmuffs are used on detainees for security purposes during transit and evacuation.
- **Oversight Considerations for Field Expedient Separation:**
  - The intended use of field expedient means of separation must be specified on the interrogation plan that is submitted to the GO/FO for approval.
  - Detainees must be protected from self-injury when field expedient means of separation are used. The effect of the application of field expedient separation means on the detainee must be monitored to detect any possible health concerns.

M-30. The following safeguards apply to both Physical Separation and Field Expedient Separation.

- **Break:** Additional periods of separation will not be applied without the approving GO/FO's determination of the length of a break between iterations.
- **Extension:**
  - **Physical Separation Method**: Extensions of this technique past 30 days must be reviewed by the servicing SJA and approved by the original approving GO/FO or his replacement in that position.
  - **Field Expedient Method:** Extensions past 12 hours of initial duration at the initial interrogation site must be reviewed by the servicing SJA and approved by the original approving/replacement GO/FO.
  - **Medical:** Detainees will be checked periodically in accordance with command health care directives, guidance, and SOPs applicable to all detainees.
  - **Custody and Control:** The interrogation chain of command must coordinate the interrogation plan with the Detention Operations Commander. The Detention Operations Commander (in conjunction with the MI commander) may convene a multidiscipline custody and control oversight team including, but not limited to, MP, MI, BSC (if available), and legal representatives. The team can advise and provide measures to ensure effective custody and control in compliance with the requirements of applicable law and policy.
- **Oversight Considerations:**
  - Use of hoods (sacks) over the head, or of duct tape or adhesive tape over the eyes, as a separation method is prohibited.
  - If separation has been approved, and the interrogator subsequently determines that there may be a problem, the interrogator should seek further guidance through the chain of command before applying the technique.

- Care should be taken to protect the detainee from exposure (in accordance with all appropriate standards addressing excessive or inadequate environmental conditions) to—
  - Excessive noise.
  - Excessive dampness.
  - Excessive or inadequate heat, light, or ventilation.
  - Inadequate bedding and blankets.
  - Interrogation activity leadership will periodically monitor the application of this technique.
- Use of separation must not preclude the detainee getting four hours of continuous sleep every 24 hours.
- Oversight should account for moving a detainee from one environment to another (thus a different location) or arrangements to modify the environment within the same location in accordance with the approved interrogation plan.

M-31. Suggested Approach Combinations:

- Futility.
- Incentive.
- Fear Up.

Glossary

The glossary lists acronyms and terms with Army or joint definitions, and other selected terms. Where Army and joint definitions are different, (*Army*) follows the term. Terms for which FM 2-22.3 is the proponent manual (the authority) are marked with an asterisk (*) and followed by the number of the paragraph (¶) or page where they are defined. For other terms, refer to the manual listed. JP 1-02, Dictionary of Military and Associated Terms and FM 1-02 Operational Terms and Graphics are posted on the Joint Electronic Library, which is available online and on CD ROM.

- Use this URL to access JP 1-02 online: http://atiam.train.army.mil/soldierPortal/atia/adlsc/view/public/11444-1/FM/1-02/TOC.HTM
- Use this URL to access FM 1-02 online: http://atiam.train.army.mil/soldierPortal/atia/adlsc/view/public/11444-1/FM/1-02/TOC.HTM
- /jel/service_pubs/101_5_1.pdf
- Follow this path to access JP 1-02 on the Joint Electronic Library CD-ROM: Mainmenu>Joint Electronic Library>DOD Dictionary.
- Follow this path to access FM 1-02 on the Joint Electronic Library CD-ROM: Mainmenu>Joint Electronic Library>Service Publications>Multiservice Pubs> FM 101-5-1.

*2X	The *2X Staff conducts mission and RM for all HUMINT and CI entities located within the designated AOIR. It coordinates, deconflicts, and synchronizes all HUMINT and CI activities in the designated AOIR. ("*2X" indicates 2X functions at all levels.)
AC	Active Component
ACCO	Army Central Control Office
ACE	analysis and control element
ACT	Analysis Control Team
ADA	Air Defense Artillery
ADP	automated data processing
ADCON	administrative control
aka	also known as
AMHS	Automated Message Handling System
AMID	allied military intelligence battalion
AO	area of operations
AOI	area of interest
AOIR	area of intelligence responsibility
AOR	area of responsibility

approx	approximately
ARNG	Army Reserve National Guard
ASAS	All-Source Analysis System
ASCC	Army Service Component Command
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASI	additional skill identifier
assn	assassination
ATD	associated technical document
BAT	Biometric Automated Toolset
BCT	brigade combat team
BDA	battle damage assessment
BOS	Battlefield Operating System
BSC	Behavioral Science Consultant
BSD	basic source data
C2	command and control
CA	civil affairs
CAT	category
CCIR	commander's critical information requirement
CCNY	City College of New York
CDOC	captured document
CDR	commander
CGS	common ground station
CE	captured equipment (STANAG term)
CED	captured enemy document
CEE	captured enemy equipment
CENTCOM	US Central Command
CFSO	Counterintelligence Force Protection Source Operations
CHAMS	CI/HUMINT Automated Management System
CHATS	CI/HUMINT Automated Tool Set
CI	counterintelligence
CIA	Central Intelligence Agency
CICA	Counterintelligence Coordination Authority
CIAC	Counterintelligence Analysis Cell

CID	Criminal Investigation Division
CIFA	Counterintelligence Field Agency
C2X	Coalition Intelligence Staff Officer
C/J2X LNO	Coalition/Joint Intelligence Staff Liaison Officer
C/J/G2X	Coalition/Joint/Corps/Division Intelligence Staff Officer
C/J/G/S2	Coalition/Joint/Corps/Division/Brigade and Below Intelligence Staff Officer
C/J/G/S2X	Coalition/Joint/Corps/Division/Brigade and Below Intelligence Staff Officer
CMO	civil-military operations
COA	course of action
COCOM	Combatant Command
COE	common operating environment
COLISEUM	Community On-Line Intelligence System for End Users and Managers
COMMZ	communications zone
CONUS	continental United States
CONOP	contingency operations
COP	common operational picture
COR	contracting officer representative
COT	commercial off-the-shelf
COTR	Contracting Officer's Technical Representative
counterintelligence	Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (FM 2-0)
Counterintelligence Coordinating Authority	Subordinate to the J/G2X and coordinates all CI activities for a deployed force. It provides technical support to all CI assets and coordinates and deconflicts CI activities in the deployed AO. (FM 2-0)
CP	command post
CPERS	captured personnel (JP-2.5)
CPR	Common Point of Reference
CS	combat support
CSS	combat service support
CTF	coalition task force

DA	Department of the Army
DCGS-A	Distributed Common Ground System-Army
DCIS	Defense Criminal Investigative Service
DCISS	Defense Intelligence Agency CI Information System
DCP	detainee collection point
DEA	Drug Enforcement Agency
debriefing	The systematic questioning of individuals to procure information to answer specific collection requirements by direct and indirect questioning techniques. (FM 2-0)
DED	Data Element Dictionary
DH	Defense HUMINT
DHMO	Defense HUMINT Management Office
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DII	DOD Information Infrastructure
DISCOM	Division Support Command
DOCEX	document exploitation
document exploitation	The systematic extraction of information from all media formats in response to collection requirements. (FM 2-0)
DOD	Department of Defense
DOE	Department of Energy
DP	displaced person
DRP	Detainee Reporting
DRS	Detainee Report System
DS	direct support
DSCA	defense support of civilian authorities
DSS	decision support software
DST	decision support template
DTG	date-time group
EAC	echelons above corps
EEFI	essential elements of friendly information
EPW	enemy prisoner of war
evaluating	In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (FM 2-0)

EW	electronic warfare
FBI	Federal Bureau of Investigation
FEO	forced entry operations
FFIR	friendly force information requirement
FHA	foreign humanitarian assistance
FISS	Foreign Intelligence Security Service
Five S's	search, seize, segregate, safeguard, and silence
FORSCOM	US Army Forces Command
FRAGO	fragmentary order
FRN	field reporting number
FSE	fire support element
Gb	gigabyte
GC	Geneva Convention Relative to the Protection of Civilian Persons in Time of War
GPS	Global Positioning System
GPW	Geneva Convention Relative to the Treatment of Prisoners of War
GRCS	Guardrail Common Sensor
GRIFN	Guardrail Information Node
GS	general support
GSR	general support-reinforcing
GUI	graphic user interface
GWS	Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field
HAC	HUMINT analysis cell
HAT	HUMINT analysis team
HCR	HUMINT collection requirement
HCT	HUMINT collection team
HET	human exploitation team
HN	host nation
HOC	HUMINT operations cell
HSOC	Homeland Security Operations Center
HQ	headquarters
HQDA	Headquarters, Department of the Army

human intelligence	The collection by a trained HUMINT collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities. (FM 2-0)
HUMINT	Human Intelligence
HUMINT Analysis Cell	The "fusion point" for all HUMINT reporting and operational analysis in the ACE and JISE. It determines gaps in reporting and coordinates with the requirements manager to cross-cue other intelligence sensor systems.
HUMINT Analysis Team	Sub-element of the G2 ACE that supports the G2 development of IPB products and developing and tailoring requirements to match HUMINT collection capabilities.
HUMINT Operations Cell	Assigned under the J/G2X to track all HUMINT activities in the area of intelligence responsibility (AOIR). It provides technical support to all HUMINT collection operations and deconflicts HUMINT collection operations in the AO. (FM 2-0)
I&WS	Deputy Under Secretary of Defense for Intelligence and Warfighting Support
IAFIS	Integrated Automated Fingerprint Identification System
IBS	Integrated Broadcast Services
ICF	intelligence contingency fund
ICRC	International Committee of the Red Cross
ID	identification
IED	improvised explosive device
IG	Inspector General
IIMG	Interagency Incident Management Group
IIR	intelligence information report
IMINT	imagery intelligence
INTREP	intelligence report
INTSUM	intelligence summary
IPB	intelligence preparation of the battlefield
IPF	Intelligence Processing Facility
IPSP	Intelligence Priorities for Strategic Planning
IR	information requirements
ISA	International Standardization Agreement
ISN	Internment Serial Number
ISR	intelligence, surveillance, and reconnaissance
IU	Interrogation Unit (AJP-2.5)

J2	Joint Intelligence Directorate/Staff
J2X	Joint Intelligence Staff Officer
J2X	Responsible for controlling, coordinating and deconflicting all HUMINT and CI collection activities and keeping the joint force J2 informed on all HUMINT and CI activities conducted in the joint force AOR. (*2X Staff Handbook) Umbrella organization consisting of human intelligence operation cell and the task force counterintelligence coordinating authority. The J2X is responsible for coordination and deconfliction of all human source-related activity. See also counterintelligence; human intelligence. (JP 2-01)
J5	Joint Staff Directorate, Civil Affairs
J/G2	Joint/Corps/Division Intelligence Staff Officer
J/G/S2	Joint/Corps/Division/Brigade and Below Intelligence Staff Officer
J/G/S2X	Joint/Corps/Division/Brigade and Below Intelligence Staff Officer
JAC	Joint Analysis Center
JAO	joint area of operations
JCMEC	Joint Captured Materiel Exploitation Center
JDEF	joint document exploitation facility
JDS	Joint Dissemination System
JFC	Joint Forces Commander
JIC	Joint Interrogation Center
JIDC	Joint Interrogation and Debriefing Center
JISE	Joint Intelligence Support Element
JTF	joint task force
JUMPS	job, unit, mission, PIR and IR, and supporting information
JWICS	Joint Worldwide Intelligence Communications System
KB	knowledgeability brief
LCC	Land Component Command
LDR	Lead Development Report
LEA	law enforcement agency
LNO	Liaison Officer
LRS	long-range surveillance
LTIOV	latest time information is of value
MAGTF	Marine Air-Ground Task Force
MASINT	measurement and signature intelligence
MDMP	Military Decisionmaking Process

MEDEVAC	medical evacuation
MEF	Marine expeditionary force
MEJA	Military Extraterritorial Jurisdiction Act
METT-TC	mission, equipment, terrain and weather, troops and support available, time available, and civil considerations
MI	Military Intelligence
MILO	mission, identification, location, and organization
MSO	military source operations
MOS	military occupation specialty
MP	Military Police
MTOE	modified table of organization and equipment
MTW	major theater war
NA	not applicable
NAC	national agency check
NAI	named area of interest
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCO	noncommissioned officer
NCOIC	noncommissioned officer in charge
NGA	National Geospatial-Intelligence Agency
NGO	non-governmental organization
NIP	Notice of Intelligence Potential
NIST	national intelligence support team
NOFORN	no foreign dissemination
NRT	near-real time
NSA	National Security Agency
NVG	night vision goggles
OB	order of battle
OCONUS	outside continental United States
OCR	optical character recognition
OGA	other government agencies
O/I	operations and intelligence
OIC	officer in charge
OMT	operational management team

OPCON	operational control
OPLAN	operations plan
OPORD	operations order
OSC	operations support cell
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
OPTEMPO	operational tempo
OVOP	overt operational proposal
PDA	Personal Digital Assistant
PIR	priority intelligence requirement
PME	peacetime military engagement
PMO	Provost Marshal Office
POL	petroleum, oils, and lubricants
POW	prisoner of war
PRETECHREP	preliminary technical report
priority intelligence requirements	Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decisionmaking. (JP 1-02)
PSO	peacetime stability operation (STANAG term)
PSYOP	Psychological Operations
PVO	private volunteer organization
PW	Prisoner of War (as used in the GPW)
R	reinforcing
R&S	reconnaissance and surveillance
RC	Reserve Components
RFI	request for information
RM	requirements management
ROE	rules of engagement
RSR	Resource Status Report
SALUTE	Size, Activity, Location, Unit, Time, Equipment
SBI	special background investigation
SCC	Service Component Commands
SCI	sensitive compartmented information
SCO	Sub-Control Office
SDR	Source-Directed Requirement

security detainee	Those detainees who are not combatants, but who may be under investigation or pose a threat to US forces if released.
SE	southeast
SECDEF	Secretary of Defense
SERE	survival, evasion, resistance, and escape
S.F.P.	Students for Peace
SIGINT	signals intelligence
SII	statement of intelligence interest
SIO	senior intelligence officer
SIPRNET	Secret Internet Protocol Router Network
SIR	specific information requirement
SITMAP	situation map
SJA	Staff Judge Advocate
SME	subject matter expert
SOF	Special Operations Forces
SOFA	Status of Forces Agreement
SOI	signal operating instruction
SOP	standing operating procedure
SOW	statement of work
Source (DOD)	1. A person, thing, or activity from which information is obtained. 2. In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. 3. In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. See also agent; collection agency. (JP 1-02)
SQL	structured query language
SSC	small-scale contingency
Stability and Reconstruction Operations	Those operations that sustain and exploit security and control over areas, populations, and resources. They employ military capabilities to reconstruct or establish services and support civilian agencies. Stability and reconstruction operations involve both coercive and cooperative actions.
STANAG	Standardization Agreement

TACON	tactical control
tactical questioning	The expedient initial questioning for information of immediate tactical value. Soldiers conduct tactical questioning based on the unit's SOP, ROE, and the order for that mission. Unit leaders must include specific guidance for tactical questioning in the order for appropriate missions. The unit S3 and S2 must also provide specific guidance down to the unit level to help guide tactical questioning. (FM 2-0)
TCICA	Theater Counterintelligence Coordination Authority
TCP	traffic control point
TDA	table of distribution and allowances
TDRC	Theater Detainee Reporting Center
TECHDOC	technical document
TECHNINT	technical intelligence
TES	Tactical Exploitation System
TF	task force
THREATCON	threat condition
TOE	table of organization and equipment
TPFDDL	Time-Phased Forces Deployment Data List
TTP	tactics, techniques, and procedures
TS	Top Secret
tvl	travel
TWS	Trusted Workstation
UCMJ	Uniform Code of Military Justice
UNCLASS	unclassified
unk	unknown
USAR	US Army Reserve
USB	Universal Serial Bus
USCENTCOM	US Central Command
USD(I)	Under Secretary of Defense for Intelligence
UTM	universal transverse mercator (grid)
UW	unconventional warfare
WARNO	warning order
WMD	weapons of mass destruction
WO	warrant officer
WTC	World Trade Center

This page intentionally left blank.

Bibliography

The bibliography lists field manuals by new number followed by old number, as indicated.

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

JP 0-2. *Unified Action Armed Forces.* 10 July 2001.

JP 2-0. *Doctrine for Intelligence Support to Joint* Operations. 9 March 2000.

JP 2-01.2. *(U) Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations (S//NF).* 13 June 2006.

JP 3-0. *Doctrine for Joint Operations*. 10 September 2001.

JP 3-63. *Joint Doctrine for Detainee Operations.* September 2005.

JP 4-0. *Doctrine for Logistic Support of Joint Operations*. 6 April 2000.

AR 40-25. *Nutrition Standards and Education.* 15 June 2001.

AR 715-9. *Contractors Accompanying the Force*. 29 October 1999.

DA Pam 715-16. *Contractor Deployment Guide.* 27 February 1998.

FM 1. *The Army.* 14 June 2005.

FM 1-02. *Operational Terms and Graphics.* 21 September 2004.

FM 2-0. *Intelligence.* 17 May 2004.

FM 3-0. *Operations*. 14 June 2001.

FM 3-100.21. *Contractors on the Battlefield*. 3 January 2003.

FM 5-0. *Army Planning and Orders Production.* 20 January 2005.

FM 6-0. *Mission Command: Command and Control of Army Forces.* 11 August 2003.

FM 27-10. *Law of Land Warfare.* July 1956.

FM 34-5. (U) *Human Intelligence and Related Counterintelligence Operations* (S//NF). 29 July 1994.

FM 34-130. *Intelligence Preparation of the Battlefield*. 8 July 1994.

FM 63-11. *Logistics Support Element Tactics, Techniques, and Procedures*. 8 October 1996.

FM 71-100. *Division Operations.* 28 August 1996.

FM 100-15. *Corps Operations.* 13 September 1989.

FM 101-5. *Staff Organization and Operations*. 31 May 1997.

AMC Pam 715-18. *AMC Contracts and Contractors Supporting Military Operations*. June 2000.

READINGS RECOMMENDED

These sources contain relevant supplemental information.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online:
http://155.217.58.58/atdls.htm

AR 190-8. *Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees*. 1 October 1997.

AR 190-40. *Serious Incident Report.* 15 July 2005.

AR 195-5. *Criminal Investigation Evidence Procedures*. 28 August 1982.

AR 380-5. *Department of the Army Information Security Program*. September 2000.

AR 380-10. *Technology Transfer, Disclosure of Information, and Contacts with Foreign Representatives.* 15 February 2001.

AR 380-15. *(C) Safeguarding Classified NATO Information.* 1 March 1984.

AR 380-28. *Department of the Army Special Security System*. 12 December 1991.

AR 380-40. *Policy for Controlling and Safeguarding Communications Security (COMSEC) Material.* 22 October 1990.

AR 380-49. *Industrial Security*. 15 April 1982.

AR 380-53. *Telecommunications Security Monitoring*. 29 April 1998.

AR 380-67. *Personnel Security Program*. 9 September 1988.

AR 381-1. *Security Controls on Dissemination of Intelligence Information*. 12 February 1990.

AR 381-10. *US Army Intelligence Activities*. 1 July 1984.

AR 381-12. *Subversion and Espionage Directed Against the US Army (SAEDA).* 15 January 1993.

AR 381-14. *Technical Counterintelligence (TCI).* 30 September 2002.

AR 381-20. *(U) US Army Counterintelligence Activities (S).* 26 September 1986.

AR 381-45. *Investigative Records Repository*. 25 August 1989.

AR 381-47. *(U) US Army Offensive Counterespionage Activities (S).* 30 July 1990.

AR 381-100. *(U) Army Human Intelligence Collection Program (S//NF).* 15 May 1988.

AR 381-102. *(U) US Army Cover Support Program (S).* 10 January 1991.

AR 381-143. *Military Intelligence Nonstandard Material Polices and Procedures*. 1 December 1986.

AR 381-172. (U) *Counterintelligence Force Protection Operations (CFSO) and Low Level Source Operations (LLSO) (S//NF).* 30 December 1994.

AR 385-10. *The Army Safety Program*. 23 May 1988.

AR 614-115. *Military Intelligence Excepted Career Program*. 12 April 2004.

AR 614-200. *Military Intelligence Civilian Excepted Career Program*. 30 September 2004.

AR 715-9. *Contractors Accompanying the Force.* 29 October 1999.

DA Pam 381-15. *Foreign Military Intelligence Collection Activities Program.* 1 June 1988.

DA Pam 385-1. *Small Unit Safety Officer/NCO Guide*. 29 November 2001.

TRADOC Reg 25-36. *The TRADOC Doctrinal Literature Program (DLP).* 1 October 2004.

FM 2-0. *Intelligence.* 17 May 2004.

FM 3-19.4. *Military Police Leader's Handbook*. March 2002.

FM 3-19-40. *Military Police Internment/Resettlement Operations*. August 2001.

FM 4-02.21. *Division and Brigade Surgeon's Handbook of Tactics, Techniques and Procedures*. November 2000.

FM 5-0. *Staff Organizations and Operations.* 31 May 1997.

FM 19-4. *Military Police Battlefield Circulation Control, Area Security, and Enemy Prisoner of War Operations.* 7 May 1993.

FM 27-10. *Law of Land Warfare*. July 1956.

FM 34-3. *Intelligence Analysis*. March 1990.

FM 34-7-1. *Tactical Human Intelligence and Counterintelligence Operations.* April 2002.

FM 34-8. *Combat Commander's Handbook for Intelligence*. September 1992.

FM 34-54. *Technical Intelligence*. January 1998.

FM 34-60. *Counterintelligence*. 3 October 1995.

FM 41-10. *Civil Affairs Operations*. 11 January 1993.

FMI 3-19.40. *Military Police Internment/Resettlement Operations.* 30 September 2005.

TC 25-20. *A Leader's Guide to After-Action Reviews.* 30 September 1993.

ST 2-22.7. *Tactical Human Intelligence and Counterintelligence Operations.* April 2002.

ST 2-33.5. *US Army Intelligence Reach Operations.* 1 June 2001.

ST 2-50. *Intelligence and Electronic Warfare Assets.* June 2002.

ST 2-91.6. *Small Unit Support to Intelligence.* March 2004.

OTHER PUBLICATIONS

JP 2-01. *Joint Intelligence Support to Military Operations*. November 1996.

AR 350-1. *Army Training and Education*. 9 April 2003.

DIAM 58-11. (U*) DOD HUMINT Policies and Procedures (S//NF).* August 1993.

DIAM 58-12. *(U) DOD HUMINT Management Systems (S//NF).* June 1997.

AJP-2.5. *Handling of Captured Personnel, Materiel, and Documents*. September 2001.

DOD Directive 2310.1. *DOD Program for Enemy Prisoners of War (POW) and Other Detainees (Short Title: DOD Enemy POW Detainee Program).* 18 August 1994.

DOD Directive 2310.1E. *The Department of Defense Detainee Program*.

DOD Directive 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning.* 3 November 2005.

DOD Directive 5100.77. *DOD Law of War Program.* 9 December 1998.

DOD Directive 5240.1. *DOD Intelligence Activities.* 3 December 1982.

DOD Directive 5525.5. *DOD Cooperation with Civilian Law Enforcement Officials.* 15 January 1986.

DOD Instruction 3020.41. *Contractor Personnel Authorized to Accompany the U.S. Armed Forces.* 3 October 2005

DOD Regulation 5200.1-R. *Information Security Program,* 1977.

DOD Regulation 5240.0-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons.* December 1982.

DOD SOP for Collecting and Processing Detainee Biometric Data. 11 February 05

Protocol 1 Additional to the Geneva Conventions. *Part IV: Civilian Population, Section 1: General Protection Against Effects of Hostilities*. 1977.

Executive Order 12333, *United States Intelligence Activities*. 4 December 1981.

Under Secretary of Defense for Intelligence (USD(I) Memorandum, "*Guidance for the Conduct and Oversight of Defense Human Intelligence (HUMINT) (U).*" 14 December 2004.

Implementing Instructions to the USD(I) Memorandum. "*Guidance for the Conduct and Oversight of Defense Human Intelligence (HUMINT) (U).*" 7 September 2004.

SECDEF Memorandum, *Policy on Assigning Detainee Serial Numbers (ISN) (*U). 20 September 2005.

18 U.S.C. *Posse Comitatus Act of 1878,* § 1385.

Homeland Security Act of 2002.

Detainee Treatment Act of 2005, Public Law No. 109-163, Title XIV.

DA Form 1132-R. *Prisoner's Personal Property List – Personal Deposit Fund (LRA).* April 1986.

DA Form 4137. *Evidence/Property Custody Document. July* 1976.

DA Form 4237-R. *Detainee Personal Record*. August 1995.

DD Form 2745. *Enemy Prisoner of War Capture Tag*. May 1996.

Standardization Agreements (STANAG):

STANAG 1059. *Distinguishing Letters for Geographic Entities for Use by NATO Armed Forces.* Edition 8. April 2003.

STANAG 2022. *Intelligence Reports.* 29 September 1988.

STANAG 2033. *Interrogation of Prisoners of War (PW).* Edition 6. December 1994.

STANAG 2044. *Procedures for Dealing with Prisoners of War (PW).* Edition 5. June 1994.

STANAG 2084. *Handling and Reporting of Captured Enemy Equipment and Documents.* June 1986.

This page intentionally left blank.

Index

Entries are by paragraph number

A

ACE. See analysis and control element.
AJP 2.5, Appendix E
AO. See area of operations.
Activities matrix, 12-23, Figure 12-3. See also Automation analysis tools.
Analysis and control element, 2-16
Analyst support, 9-30.
Analytical
  Support, 12-2
  Tools, 12-16
Approach, 1-10, 7-15, 8-1
  Phase, 8-4
  Rapport, 8-9
  Strategies, 8-77
    Debriefing, 8-82
    Elicitation, 8-86
    Interrogation, 8-77
  Techniques, 8-17
  Transitions, 8-73
Approaches
  Change of Scenery, 8-63
  Direct, 8-19
  Emotional, 8-23
  Establish Your Identity, 8-58
  False Flag, 8-69
  File and Dossier, 8-55
  Incentive, 8-21
  Mutt and Jeff, 8-65
  Rapid Fire, 8-60
  Repetition, 8-59
  Silent, 8-62
  We Know All, 8-53
Area Handbook, 7-4
Area of operations, 1-29
Assets, HUMINT Collection, 4-40
Association Matrix, 12-19, Figure 12-2
Audio recording, 9-29
Automation, 13-2
  Analysis tools, 13-13
  Requirements for collectors, 13-24
  Systems, 13-21, L-3
  Workstation requirements, 13-25

B

Basic Source Data Reports (BSD), 10-13
Battlefield Operating System (BOS), 1-1
BEST MAPS, 5-45
Biographic Intelligence, 5-45
Biometrics, 13-4

C

C2X, 2-4
CA. *See* Civil Affairs.
Capabilities, 1-31
Capture Rates, 5-90
Capture tag, Figure D-1
Captured document
  Handling, I-12
  Log, I-24, Figure I-3
  Transmittal sheet, I-19, Figure I-2
Captured equipment handling, D-21
Central Intelligence Agency, 3-24
Change of Scenery Approach, 8-63
Checkpoint Operations, 5-7, 5-36, 5-42
CIA. *See* Central Intelligence Agency.
CICA. *See* Counterintelligence Coordination Authority.
CID. *See* Criminal Investigation Division.
Civil Affairs (CA) Units, 4-47, 4-58
Cold leads, 9-22
Collect, 1-2
Collection
  Objectives, 7-2
  Priority, 4-45
  Requirements, 7-4
Combat Service Support Units, 4-58
Combatants, viii
  Lawful, 6-18
  Unlawful, 6-18
Command Debriefing Team, 2-13
Command Relationships, (HUMINT) 4-11
  Army, Table 4-2
  Joint, Table 4-3
Common points of reference, 9-39. *See also* Map tracking.
Communication requirements, 13-27, 13-30, L-7
Contact reports, 10-14
Continuous Contacts, 5-16
Contractor, 1-7, K-1
Control Questions, 9-10
Coordinates register, 12-41

Coordination with other units and operations, 5-42, 5-56, 5-102
Counterintelligence
Coordination Authority, 2-8
Functions, 1-7, Figure 1-2
Screening, 6-39, table 6-1
Courses of Action, 4-44
Criminal Investigation Division, 4-58, 4-60, 5-42
Cultural Awareness, 1-29, 8-4

D

DEA. *See* Drug Enforcement Agency.
Databases, 12-46, 13-18
Debriefing, 1-21
Debriefing Operations, 1-21, 5-30
Legal Guidelines, 5-33
Operational Considerations, 5-34
Deceit, 9-23, 9-25, 9-26
Defensive Operations, 3-7
Detainee, 5-26
Geneva Convention categories, 6-14
Security, 5-58, 5-78
Interrogation Operations, 1-20
Direct Approach, 8-19
Direct Questioning, 9-4
Document
Accountability, I-19
Associated with a source, I-51
Categories, I-27
Exploitation (DOCEX) Operations, 1-24, 4-51, E-12, I-1, I-11, I-48
Exploitation Team, 2-14
Evacuation, I-12
Handling, I-14
Screening, I-25
Tag, I-14
Translation, I-43
Transmittal, I-34
Drug Enforcement Agency, 4-58

E

EAC HUMINT, 3-22
Emotional Approach, 8-23
EPW
Serial number, 6-12, 6-13
Status, 6-14
Early Entry Operations. *See also* HUMINT operations.
HUMINT Support of, 3-6
Economic Intelligence, 5-45
Elicitation, 8-80
Establish Your Identity Approach, 8-58
Exploit dispositions, 9-43

F

False Flag, 8-69
Field Interrogations Operations, 5-95
File and Dossier Approach, 8-55
Fingerprint scanner, 13-4
Five S's, D-7
Forced Entry Operations. *See also* HUMINT operations.
HUMINT Support of , 3-5
Formal Contacts, 5-28
Friendly Force Debriefing Operations, 1-21, 5-39

G

G2X, 2-4
Geneva Conventions, 5-68, 5-72
Categories of detainees, 6-15
Excerpts, Appendix A

H

HCT, 2-11. *See also* HUMINT Collection Team.
As an Independent Patrol, 3-14
Integrated with other operations, 3-14
Restricted to Base Camp, 3-14
Hot leads, 9-21
Human Intelligence, 1-4,
Structure, 2-1
HUMINT, 1-4
Agencies, 3-24
Analysis, 12-1
Analysis Cell, 2-16
Asset Capabilities, 4-17, 4-26, 4-45
HUMINT Collection, 1-8, 5-1
Aids, 9-28
Constraints, 4-41
In a Hostile Environment, 3-21
In Permissive Environment, 3-19
In Semi-permissive Environment, 3-20
Phases, 1-8
Plan, 7-9
HUMINT Collection Team, 2-11
Allocation to maneuver units, 5-96
HUMINT Collector, 1-7
Traits, 1-28
HUMINT Command and Control, 4-9
HUMINT Contacts, 5-5
One Time Contact, 5-7
Continuous Contacts, 5-16
Formal Contact, 5-28
HUMINT Control Organizations, 2-3 through 2-14
HUMINT Collection and Related Activities, 1-14
HUMINT Methodology, 1-14, 1-18
HUMINT Mission Planning, 4-35, 4-44
HUMINT Operations, 1-23
Assessing, 4-8
Executing, 4-7
Planning, 4-3
Preparing, 4-5

HUMINT Organization, Figure 2-1
HUMINT Requirements Analysis, 4-18
HUMINT Requirements Management, 4-16
HUMINT Source, 1-6
Database, 2-9, 12-7
Collection Activities, 1-16
Selection, 12-45
HUMINT Structure, 2-1
HUMINT Tasks, 1-5
HUMINT Technical Control, 4-10

I

Imagery Intelligence, 4-57
Incentive Approach, 8-21
Information Dissemination, 4-32
INSCOM, 3-22
Intelligence Battlefield Operating System, 1-1
Intelligence Estimate, 7-4
Intelligence information reports, 10-6
Intelligence preparation of the battlefield, 12-3
Intelligence Process, 1-2, Figure 1-1
Intelligence Production, 4-31
Intelligence Reach, 7-5, 7-6
Interrogation, 1-20, 5-50
Of wounded detainees, 5-91
Priorities, Figure, 6-3
Prohibited techniques, 5-68, 5-74
Prohibition against use of force, 5-73
Serial number allocation, Appendix F
Interrogation Operations, 5-50
Field, 5-96
Joint, 5-100
Interpreter program, 11-28, 11-29, 11-30
Interpreter use, 11-2
Advantages, 11-2
Briefing, 11-18
Cautions, 11-4
Controlling and correcting, 11-24
Disadvantages, 11-3
Evaluating, 11-28
Methods, 11-6, 11-7
Placement, 11-21
Techniques, 11-16
Interpreters, 11-1, 11-26
Civilian, 11-15
Evaluating, 11-28
Military, 11-14
INTSUM, 7-4
Iris scanner, 13-6
ISR Plan (Integrated), 4-3, 4-27, 4-28
Updating, 4-34

J

J2X, 2-4
JIDC Analysis Section, 2-17
Joint HUMINT, 3-23, 5-91
Joint Interrogation and Debriefing Center (JIDC), 5-102
Joint interrogation operations, 5-99

K

Knowledgeability Brief, 10-15

L

Lawful enemy combatants, 6-18
Lead development report, 10-15
Leads, 9-20
Levels of Employment, 3-14
Liaison Operations, 1-22, 5-46
Link analysis diagram, 12-16, 12-25, Figure 12-4
Limitations, 1-32
Local civilian debriefing operations, 1-21
Long-Range Surveillance, 5-42

M

Machine translation, 13-8
Maneuver unit support, 4-9
Map tracking, 9-35
Matrices, 12-18
Measurement and Signals Intelligence (MASINT), 4-57
Military geographic intelligence, 5-46
Military Intelligence Organizations, 4-57
Military Police in Association with Interrogation Operations, 5-56, Figure 6-2
Internment/resettlement operations, 6-14, Figure 6-2
Units, 4-58, 5-42
Mutt and Jeff, 8-65

N

National level intelligence agencies, 3-24
Notice of intelligence potential, 10-15

O

OB Factors, 12-43
Offensive Operations, 3-2
One-Time Contact, 5-7
Open source documents, I-10
Operational analysis and assessment, 12-8
Operational Coordination, 4-9
Operational Management Team (OMT), 2-10
Team leader requirements, 13-23
Operational reports, 10-4
Operations Orders, 4-53
Operations Plans, 4-54
Operations Support Cell, 2-7
Orders
Illegal, 5-80, 5-82
Organizational Chart, 9-28, Figure 2-1

P

Pattern analysis, 12-40, 12-42
Plan, 1-2
Planning and Preparation, 1-9, 7-1
Political intelligence, 5-45
Polygraph, 13-7
Detainee status, 6-14 through 6-23, E-8
Pre-deployment planning, Appendix C
Prepare, 1-2
Primary approach strategy, 7-15
Process, 1-2
Produce, 1-2
Protected persons, 6-17
Protocol I Additional to the Geneva Conventions, Appendix B
Psychological Operations (PSYOP) Units, 4-58, 5-42

Q

Questioning, 1-11
  Illiterates, 9-46
  Plan, 7-18
  Principles, 9-2
  Quick reference guide, Appendix G
  Sequence, 7-19, 7-20
Questions, 9-2
  Direct, 9-4
  Follow Up, 9-7
  Non-pertinent, 9-8
  Prepared, 9-12
  Repeat, 9-9
  To avoid, 9-14

R

Rapid Fire Approach, 8-60
Reach. *See* Intelligence Reach.
Recording principles and techniques, 9-29
References, Appendix J
Refugee debriefing operations, 1-21, 5-31
Repetition Approach, 8-59
Reporting, 1-13, 7-24, 10-1
  Channels, 10-3, 10-16, Figure 10-1
  Evaluation, 4-33
  Principles, 10-2
Report types, 10-3
Required areas of knowledge, 1-29
Research, 7-3
  Source-specific, 7-8, 7-25
Reserve component integration, 4-50
Restricted Interrogation Techniques, 8-71
Retained personnel, 6-22
Risk assessment, 4-43

S

S2 Guide for Handling Detainees, Appendix D
S2X, 2-4
SALUTE reports, 10-10
  Format, Appendix H
Science and technical intelligence, 5-45
Screening, 1-18, 6-1
  Codes, Table 6-1
  Community, 6-38
  Documents, I-25
  Local employees, 6-37
  Methodologies, 6-9
  MP support, 6-14, Figure 6-2
  Observations, 6-30
  Operations, 1-19, 6-7, 6-8
  Prisoner of war and refugee, 6-9 , 6-13
  Reports, 10-15
  Requirements, 6-7
  Sheet, Figure 6-1
Search engine, 13-14
Separation, M-1
Signals Intelligence, 4-57
Silent Approach, 8-62
Single-discipline HUMINT analysis and production, 12-14
Situation Map (SITMAP), 7-4
Sociological Intelligence, 5-45
SOF. *See* Special operation forces.
SOR development, 12-5
Source, 1-6
  Administrative reports, 10-5
  Analysis, 12-11
  Assessment, 6-36
  Coverage overlay, 12-50
  Map reading skills, 9-38
  Profiles, 12-51
  Reliability matrix, B-1
Special Operation Forces, 5-42
Stability and reconstruction operations, 3-9
Staff coordination, 4-59
Strategic Debriefing Operations, 5-43
Subject matter expert (SME), 7-4
Support Operations, 3-15
Support Relationships (HUMINT), 4-13
  Direct Support, Table 4-2
  General Support, Table 4-2
Support Scheme Development, 4-27, 4-60

T

Tactical Debriefing Operations, 5-35
Tactical questioning, 1-17
Target Folder, 4-39, 12-47
Task Organization, 4-47
Taskings and Requests, 4-28
Technical expert support, 9-30
Technical intelligence (TECHINT), 4-57
  Screening requirements for, 6-42
  Support, 7-17
Termination, 1-12

Phase, 8-84
Report, 10-15
Third-party information, 9-33
Time Event Chart, 9-28, 12-17, Figure 12-1
Traits of a HUMINT Collector, 1-28
Translation machines, 13-8
Translators, I-47
Transportation and telecommunication intelligence, 5-45
Trusted Workstation (TWS), 13-3

U

Umbrella concept, 7-4
Unit Augmentation, 4-58
Unlawful enemy combatant, viii, 6-18
Urban Operations, 3-16

V

Video Recording, 9-29
Warning Order, 4-37

W

We Know All Approach, 8-53
Web-based reporting, 13-15
Wounded detainees
Interrogation of, 5-91, 9-45

This page intentionally left blank.

FM 2-22.3 (FM 34-52)
6 September 2006

I have approved FM 2-22.3 in accordance with DOD Directive 3115.09, DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning.

STEPHEN A. CAMBONE
Under Secretary of Defense
for Intelligence

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0516001

DISTRIBUTION:

Regular Army, Army National Guard, and the Army Reserve: To be distributed in accordance with the initial distribution number (IDN) 111130, requirements for FM 2-22.3.

This page intentionally left blank.

PIN: 082535-000

MCWP 2-2

MAGTF Intelligence Collection

U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 143 000148 00

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to **nancy.morgan@usmc.mil**. Recommendations should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Add, delete
  - Proposed new text, preferably double-spaced and typewritten
- Justification and/or source of change

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status.* An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: **https://www.doctrine.usmc.mil**.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

30 July 2004

FOREWORD

Marine Corps Warfighting Publication (MCWP) 2-2, *MAGTF Intelligence Collection*, builds on the doctrinal foundation established by Marine Corps Doctrinal Publication (MCDP) 2, *Intelligence,* and Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations*, detailing specific doctrine and tactics, techniques, and procedures (TTP) to conduct intelligence collection to support the Marine air-ground task force (MAGTF).

MCWP 2-2 is primarily for intelligence personnel who plan and execute intelligence collection activities. Personnel who support intelligence collection activities or use their results may also find this publication useful.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

EDWARD HANLON, JR.
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development
Marine Corps Combat Development Command

Publication Control Number: 143 000148 00

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

TABLE OF CONTENTS

Page

Chapter 1 Fundamentals

Intelligence Staff (G-2/S-2)Responsibilities....1-1
Specific G-2/S-2 Responsibilities....1-1
Special Staff Officers under Staff Cognizance of the G-2 Officer....1-2
- G-2 Operations Officer....1-2
- G-2 Plans Officer....1-2
- Intelligence Battalion Commander/ISC....1-3

MEF MSC and Unit Responsibilities....1-5
MAGTF Intelligence and Reconnaissance Collection Assets....1-6
Intelligence Collection within the Marine Corps Intelligence Cycle....1-6
Collection Principles....1-7
- Early Involvement....1-7
- Prioritization....1-7
- Multidiscipline Approach....1-7
- Task Organic Assets First....1-7

Collection Management Process....1-8

Chapter 2 Collection Requirements Management

Requirements Analysis Criteria....2-1
- Pertinence....2-1
- Feasibility....2-1
- Completeness....2-2
- Validation....2-2
- Priority....2-2

Intelligence Requirements....2-2
Requirements Management....2-3
- Processing IRs....2-3
- Validating IRs....2-3
- Refining IRs....2-3
- Managing IRs System....2-3
- Reviewing Priorities....2-4
- Satisfying IRs....2-4
- Organizing the Collection Effort Around Requirements....2-4

ICR Development Process....2-5
- Step1, Identify, Validate, and Prioritize PIRs and IRs....2-5
- Step 2, Identify Indicators....2-6
- Step 3, Derive Specific Information Requirements....2-6
- Step 4, Develop SORs....2-8

Collection Assets/Resource Selection Factors....2-9
Capability....2-9
Suitability (or Feasibility)....2-9
Redundancy/Multiplicity....2-9
Balance....2-9
Target Key Elements....2-9
Collection Capabilities....2-10
Correlation....2-10
Environment....2-10
Intelligence Collection Planning....2-11
IRs Worksheet....2-11
Intelligence Collection Worksheet....2-12
Reporting....2-12
Collection and Related Planning Tools....2-12
Intelligence and Reconnaissance Assets Tasking....2-14
Standard Formats for Asset Tasking....2-14
Guidelines for Requesting National/Theater Collection Support....2-14
Production Requests....2-15
Production Request Format....2-16

Chapter 3 Intelligence Collection Operations Management

Mission Planning and Collection Plan Development....3-1
Collection Asset Tasking....3-2
Tasking Organic Collections and Production Assets or Supporting Collection and Production Resources....3-2
Requesting Support from External MAGTF Collection and Production Resources....3-2
Tasking Subordinate Elements....3-3
MAGTF Collection Tasking....3-3
Exploitation and Reporting....3-3
Cueing....3-4
Redundancy....3-4
Mix....3-4
Integration....3-5
Coordination....3-5
Report Formats....3-5
Supervision of the Collection Effort....3-8
Functions....3-8
Duties....3-8
Updating the Collection Plan During Execution....3-9

Chapter 4 Planning and Execution

Terrain....4-1
Weather....4-1
Threat....4-1
Coordination with Maneuver and Fires....4-1
Communications and Information Systems....4-2

Combat Service Support Availability 4-2
Employment of MAGTF Intelligence Units 4-3
Focused Intelligence Support 4-3
Task Organization of Intelligence Support Units 4-3
Intelligence Direct Support Teams 4-4
Precrisis (Garrison/Peacetime) Intelligence Collection 4-4
The Planning Phase 4-4
Intelligence Collection During Execution 4-5
Current Operations 4-5
Future Operations 4-6

Appendices

A Sample Intelligence Requirements Worksheet A-1
B Sample Intelligence Collection Worksheet Description B-1
C Sample Intelligence Collection Plan C-1
D Sample Collection Status Update Paragraph Format D-1
E Sample Collection Emphasis Message E-1
F Glossary F-1
G References G-1

Figures

1-1 The Marine Corps Intelligence Cycle 1-7
2-1 Requirements Satisfaction 2-5
2-2 ICR Development Process 2-5
2-3 Sample Intelligence Requirements Worksheet 2-12
2-4 Intelligence Collection Tasking Worksheet 2-13
3-1 Notional Intelligence Synchronization Matrix 3-6
B-1 Sample Intelligence Collection Worksheet B-4

CHAPTER 1
FUNDAMENTALS

Intelligence collection is the acquisition of information and the provision of this information to processing elements (Joint Publication [JP] 1-02, *Department of Defense Dictionary of Military and Associated Terms*). In Marine Corps usage, collection is the gathering of intelligence data and information to satisfy the identified requirements (MCRP 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*). Successful MAGTF intelligence collection seeks to help reduce uncertainty regarding the enemy, weather, terrain, and operational environment. MAGTF intelligence collection activities form detailed intelligence collection requirements (ICRs), task organic collection assets, and request external collection resources to satisfy the warfighting commander's priority intelligence requirements (PIRs) and other intelligence requirements (IRs).

Intelligence Staff (G-2/S-2) Responsibilities

The intelligence staff (G-2/S-2) has responsibility for intelligence and intelligence operations. The commander relies on the intelligence officer to provide information on weather, terrain, and enemy capabilities, status, and intentions. Through the intelligence annex and supporting appendices, the G-2/S-2 does the following:

- Validates and plans information requirements.
- Coordinates intelligence priorities.
- Integrates collection, production, and dissemination activities.
- Allocates resources.
- Assigns specific intelligence and reconnaissance missions to subordinate elements.
- Supervises the overall intelligence, counterintelligence (CI), and reconnaissance efforts.

See also MCWP 3-40.1, *Marine Air-Ground Task Force Command and Control*, and MCWP 2-1, *Intelligence Operations*.

Specific G-2/S-2 Responsibilities

- Develops and answers outstanding intelligence-related PIRs.
- Prioritizes PIRs and IRs by planning, directing, integrating, and supervising organic multidiscipline MAGTF and supporting intelligence operations.
- Prepares appropriate intelligence, CI, and reconnaissance plans and orders:
  - Reviews and coordinates the all-source intelligence, CI, and reconnaissance plans of joint task forces (JTFs), theaters, and other organizations.
  - Submits and coordinates all-source collection, production, and dissemination requirements beyond the capability of the MAGTF through higher headquarters for JTF, theater or national intelligence support.
- Ensures intelligence information is rapidly processed, analyzed, and incorporated where appropriate in all-source intelligence products, and rapidly disseminates to all MAGTF and external units requiring these.
- Evaluates JTF, theater, and national all-source intelligence support and adjusts stated IRs.
- Identifies deficiencies in intelligence, CI, and reconnaissance personnel and equipment resources.
- Incorporates exercise intelligence in training exercises to improve individual, collective, and unit readiness.
- Facilitates understanding and use of intelligence in support of the planning and execution of operations.

Special Staff Officers under Staff Cognizance of the G-2 Officer

G-2 Operations Officer

The G-2 operations officer has primary responsibility for intelligence support to current and future operations. Specific responsibilities include the following:

- Coordinates and provides intelligence support to the commander, the G-3 operations section, and the rest of the commander's battle staff.
- Serves as the G-2 representative to the MAGTF command element (CE) crisis action team.
- Coordinates, provides, and supervises intelligence support to the MAGTF CE, combat operations center, future operations center, and force fires.
- Plans, directs, and supervises the red cell.
- Provides recommendations on PIR and IR validation, prioritization, and tasking to the G-2 and the intelligence support coordinator (ISC).
- Coordinates and supervises the transition of intelligence planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations to effectively support operations.
- Plans, directs, and supervises MAGTF liaison teams to external commands; e.g., the JTF and joint functional components headquarters and intelligence organizations.
- Coordinates with the ISC and MAGTF major subordinate commands' (MSCs') G-2 operations officers for unity of effort of MAGTF intelligence operations.
- Provides intelligence input and other support to MAGTF warning and fragmentary orders (FRAGOs) and to operations-related reporting; e.g., periodic situation reports.
- Coordinates intelligence training for the MAGTF G-2 section and provides G-2 oversight for and integration of the entire MAGTF intelligence training program.
- Performs other intelligence support and tasks as directed by the G-2.

G-2 Plans Officer

The G-2 plans officer has primary responsibility for intelligence support to the future plans cell. Specific responsibilities include the following:

- Plans the MAGTF concept of intelligence operations for approval by the G-2 and subsequent implementation by the integrated staff cell based on the mission, threat, commander's intent, guidance, and concept of operations.
- Leads, coordinates, and provides intelligence support to G-5 future plans section.
- Plans and coordinates intelligence support requirements for and the deployment of intelligence elements and resources into the area of operations (AO).
- Provides recommendations on PIR and IR validation, prioritization, and taskings to the G-2 and the ISC.
- With the ISC, coordinates G-2 development of Annex B (Intelligence) and Annex M (Geospatial Information and Services) to the operation plan/operation order (OPLAN/OPORD).
- Keeps the G-2 section, other CE staff sections, intelligence liaison personnel, augmentees, and others apprised of MAGTF intelligence planning actions and requirements.
- Identifies requirements and provides recommendations to the G-2 operations officer for MAGTF intelligence liaison teams to external commands; e.g., the JTF or other components' headquarters and intelligence agencies.
- Coordinates and develops policies for intelligence, CI, and reconnaissance operations.
- Plans, directs, and supervises the G-2's imagery and mapping, CI/human intelligence (HUMINT), signals intelligence (SIGINT), and weather sections.

- Performs other intelligence support and tasks as directed by the G-2.

Intelligence Battalion Commander/ISC

The intelligence battalion commander plans, directs, collects, processes, produces, and disseminates intelligence, and provides CI support to the Marine expeditionary force (MEF), MEF MSCs, subordinate MAGTFs, and other commands as directed.

In garrison, the principal task of the intelligence battalion commander is to organize, train, and equip detachments that support MAGTFs or other designated commands to execute integrated collection, intelligence analysis, production, and dissemination of intelligence products.

During operations, the intelligence battalion commander is dual-hatted as the ISC, serving under the direct staff cognizance of the G-2. The S-3 section and the operations center element of the G-2 form the core of the ISC support effort, with planning, direction, and command and control (C2) conducted within the intelligence operation center's (IOC's) support cell. As the ISC, the commander is responsible to the G-2 for the overall planning and execution of all-source intelligence operations. Specific ISC responsibilities during actual operations include the following:

- Implements the concept of intelligence operations developed by the G-2 plans officer and approved by the G-2.
- Establishes and supervises operation of the MAGTF IOC, which includes the support cell, the surveillance and reconnaissance cell (SARC), and the production and analysis (P&A) cell. Generally, the IOC will be collocated with the MAGTF CE's main command post.
- Develops, consolidates, validates, and prioritizes recommended PIRs and IRs to support MAGTF planning and operations. The ISC is tasked to perform PIR and IR validation and prioritization only during actual operations when the IOC is activated. During routine peacetime operations, PIR and IR validation and prioritization tasks are the responsibility of the G-2 operations officer.
- Plans, develops, integrates, and coordinates intelligence collection, production, and dissemination plans. This includes the effective organic and external integration and employment and staff cognizance of SIGINT; CI; HUMINT; geographic intelligence; imagery intelligence (IMINT); ground remote sensors; ground reconnaissance; and tactical air reconnaissance intelligence collections, production, and dissemination operations.
- Develops (with the G-2 plans officer and G-2 operations officer) and completes Annex B (Intelligence) and Annex M (Geospatial Information and Services) to the OPLAN/OPORD.
- Plans, develops, integrates, and coordinates intelligence and CI support to the commander's estimate; situation development; indications and warning; force protection; targeting; and combat assessment.
- Manages and fuses the threat (or red) common operational picture/common tactical picture (COP/CTP) inputs from subordinate units and external commands and intelligence agencies into the COP/CTP.
- Provides intelligence support to the MAGTF G-2 section and the MSCs.
- Prepares the intelligence and CI estimates to support G-2 plans.
- Plans, develops, and coordinates intelligence communications and information systems (CIS) architecture, including its integration with and support of IMINT and other intelligence and reconnaissance requirements.
- Coordinates and integrates all-source intelligence operations with other Service components; the JTF joint intelligence support element; the theater joint intelligence center or joint analysis center; and national intelligence agencies and operations to include all aspects of intelligence reachback support.
- Assists with the evaluation and improvement of all-source intelligence, CI, and reconnaissance operations.

- Provides other intelligence support and tasks as directed by the G-2.

Collection Management/Dissemination Officer

The collection management/dissemination officer (CM/DO) is sourced from the intelligence battalion's S-3 section and is a key subordinate to the intelligence battalion commander/ISC during operations. The CM/DO forms detailed ICRs and intelligence dissemination requirements (IDRs), and tasking and coordinating internal and external operations to satisfy these. The CM/DO receives validated PIRs and IRs and direction from the ISC, and then plans and manages the best methods to employ organic and supporting collection and dissemination resources through the intelligence collection and dissemination plans.

The CM/DO also validates and forwards national and theater intelligence collection requests from the MAGTF and MSCs typically using appropriate intelligence tools and TTP. He also coordinates intelligence CIS requirements and maintains awareness of available CIS connectivity throughout the MAGTF and with key external organizations. During operations, the CM/DO works within the support cell. In coordination with the P&A cell officer in charge (OIC), the SARC OIC, the G-2 operations officer, the intelligence/reconnaissance commanders, and the G-6, the CM/DO is responsible to the ISC for the following tasks:

- Determines and coordinates the collection effort of PIRs/IRs that may be collected via intelligence, CI, and reconnaissance resources.
- Determines PIRs/IRs and prepares requests for intelligence (RFIs) that are beyond organic capabilities; prepares submissions to higher headquarters and external agencies for support.
- Recommends dissemination priorities, develops intelligence reporting criteria, and advises on and selects dissemination means.
- Uses the Collection Management Board (if established) to develops and coordinates all-source intelligence collection plans, and coordinates and integrates these with MAGTF, other components, JTF, theater, and national intelligence production operations.
- Develops and coordinates all-source intelligence dissemination plans and supporting architectures for voice and data networked communications; coordinates and integrates these with MAGTF, other components, JTF, theater, and national intelligence CIS and dissemination operations.
- Monitors the flow of intelligence throughout the MAGTF; ensures that it is delivered to intended recipients in a timely fashion and satisfactorily meets their needs.
- Evaluates the effectiveness of MAGTF and supporting intelligence collection and dissemination operations.

SARC OIC

The SARC OIC is also an immediate subordinate of the ISC and is responsible for supervising the execution of the integrated organic, attached, and direct support (DS) intelligence collection and reconnaissance operations. The SARC OIC is responsible to the ISC for the following:

- Coordinates, monitors, and maintains the status of all ongoing intelligence, CI, and reconnaissance collection operations. This includes the following:
  - Missions, tasked ICRs, and reporting criteria for all collection missions.
  - Locations and times for all pertinent fire support control measures.
  - Primary and alternate CIS plans for routine and time-sensitive requirements (for collectors and between the collectors or the SARC and key MAGTF CE and MSC C2 nodes) to support ongoing C2 of collection operations and dissemination of acquired data and intelligence to those needing it by the most expeditious means.
- Conducts detailed intelligence collection planning and coordination with the MSCs and intelligence, CI, and reconnaissance organizations'

planners, with emphasis on ensuring understanding of the collection plan and specified intelligence reporting criteria.
- Ensures other MAGTF C2 nodes; e.g., the current operations center or force fires, are apprised of ongoing intelligence, CI, and reconnaissance operations.
- Receives routine and time-sensitive intelligence reports from deployed collection elements; cross-cueing among intelligence collectors, as appropriate; and the rapid dissemination of intelligence reports to MAGTF C2 nodes and others in accordance with IRs, intelligence reporting criteria and dissemination plans, and the current tactical situation.

P&A Cell OIC

The P&A cell OIC's primary responsibility is to manage and supervise the MAGTF's all-source intelligence processing and production efforts. Key responsibilities include the following:

- Plans, directs, and manages operations of the all-source fusion platoon to include the fusion, order of battle, intelligence preparation of the battlespace (IPB), and target intelligence/battle damage assessment (BDA) teams; the topographic platoon; the IMINT platoon; DS teams; and other P&A elements as directed.
- Coordinates and integrates P&A cell operations, estimates, and products with the G-2 section's G-2 operations branch and its red cell operations and estimates.
- Maintains all-source automated intelligence databases, files, workbooks, country studies, and other intelligence studies.
- Plans and maintains imagery, mapping, and topographic resources and other intelligence references.
- Administers, integrates, operates, and maintains intelligence processing and production systems and unclassified general service (message) and sensitive compartmented information systems; e.g., the intelligence analysis system or the image product library.
- Analyzes and fuses intelligence and other information into tailored all-source intelligence products to satisfy all supported commanders' stated or anticipated PIRs and IRs.
- Develops and maintains current and future intelligence situational, threat, and environmental assessments and target intelligence based on all-source analysis, interpretation, and integration.
- Manages and fuses the threat (or red) COP/CTP inputs from subordinate units and external commands and intelligence agencies into the COP/CTP.

For additional information on staff and unit intelligence responsibilities, see MCWP 3-40.1 and MCWP 2-1.

MEF MSC and Unit Responsibilities

Intelligence collection responsibilities also extend to MEF MSCs and units. Key tasks of the MEF MSC intelligence officers include the following:

- Consolidates, validates, and prioritizes MSC IRs and collection needs.
- Submits consolidated requests for external intelligence support.
- Coordinates intelligence activities within their unit.

The unit intelligence officer is generally responsible for the following tasks:

- Coordinates with unit production personnel to verify that the needed information or intelligence is not already available.
- Identifies requirements beyond the unit's capability to satisfy. The unit intelligence section identifies requirements it cannot satisfy internally and forwards these up the chain of command for satisfaction. Detailed justification and the latest time intelligence is of value (LTIOV) should be included so that ICRs can successfully compete with other ICRs for priority collection support.

- Develops unit intelligence collection plans, which must be thoroughly coordinated and integrated with the unit's intelligence production and dissemination plans. Ensures the intelligence plan is responsive to operational needs by analyzing incoming information, determining its value and relevance, and refining future collection needs.
- Integrates collection operations with unit maneuver, fires, communications, and logistics operations. To be effective, collection operations must be coordinated with other operations of the command.
- Plans and supervises operations of organic collection assets and coordinating internal support; e.g., communications, logistics, and security.

MAGTF Intelligence and Reconnaissance Collection Assets

Intelligence data and information are collected by a wide range of MAGTF intelligence and reconnaissance assets. These assets include, but may not be limited to, the following:

- Marine tactical electronic warfare (EW) squadron (VMAQ).
- Radio battalion.
- CI/HUMINT company.
- Ground sensor platoon (GSP).
- Force reconnaissance company.
- Light armored reconnaissance battalion.
- Unmanned aerial vehicle (UAV) squadron.
- Ground combat element reconnaissance battalion/company/platoon.
- Joint surveillance target attack radar system (JSTARS) common ground station.
- F/A-18D reconnaissance capable with advanced tactical airborne reconnaissance system (ATARS).

For additional information on unit capabilities, see the following MCWPs:

- 2-14, *Counterintelligence* (CI/HUMINT).
- 2-15.1, *Remote Sensor Operations* (GSP).
- 2-15.2, *Signals Intelligence* (radio battalion).
- 2-15.4, *Imagery Intelligence* (JSTARS).
- 3-26, *Air Reconnaissance* (F/A-18D ATARS).
- 3-40.5, *Electronic Warfare* (VMAQ and radio battalion).
- 3-42.1, *Unmanned Aerial Vehicle Operations* (UAV).

Intelligence Collection within the Marine Corps Intelligence Cycle

The process used to develop intelligence is called the intelligence cycle. See figure 1-1. The Marine Corps intelligence cycle consists of six sequential yet interdependent steps: planning and direction; collection; processing and exploitation; production; dissemination; and utilization. Collection is the second step, yet collection management is a continuing process and occurs concurrently throughout the cycle. Intelligence collection is a process that helps identify and validate IRs, prioritize them, determine effective means for acquiring information to help satisfy them, and develop, execute, and supervise intelligence and reconnaissance operations.

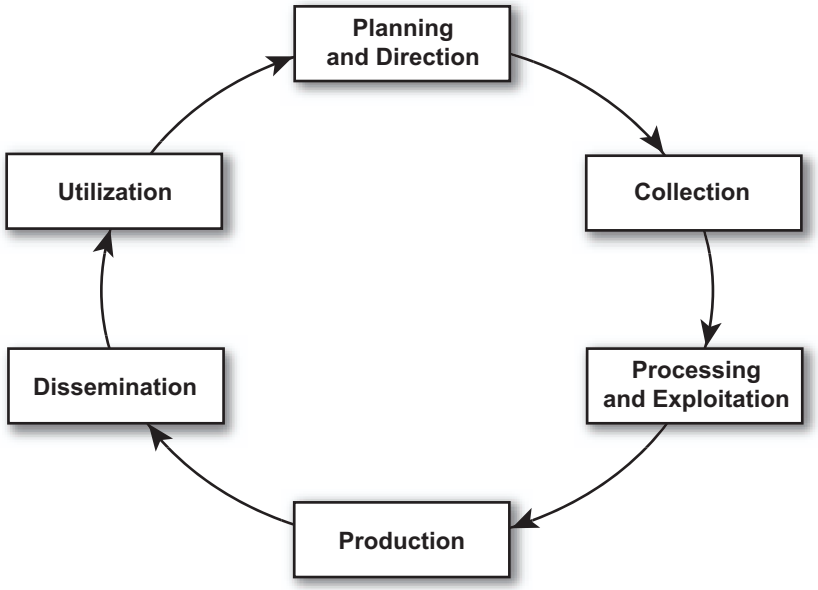


Figure 1-1. The Marine Corps Intelligence Cycle.

Collection Principles

Collection managers may use the following general principles when planning and executing intelligence collection activities. See also JP 2-01, *Joint Intelligence Support to Military Operations*.

Early Involvement

A collection manager must get involved with IRs identification and management early in planning. This ensures thorough consideration and increased flexibility in choosing intelligence collection assets and resources, enhancing the quality and timeliness of collected information.

Prioritization

Prioritization assigns a distinct ranking to each collection requirement. Prioritization must be based on the commander's guidance and the current situation to ensure that assets/resources are directed against the most critical requirements.

Multidiscipline Approach

Collection managers must avoid overreliance on a single collection system or intelligence discipline. Each intelligence collection asset/resource has unique strengths and weaknesses. However, each asset's limitations can be mitigated through the capabilities of other resources. Overreliance on a single asset may result in mission failure if that asset becomes unavailable or the adversary can ascertain its employment pattern and implement countermeasures. A fully integrated collection plan uses collection resources in a complementary manner, adding depth to collection activities.

Task Organic Assets First

Use of organic collection assets allows a timely and tailored response to collection requirements and lessens the burden on collection resources controlled by other units, agencies, and organizations. However, if the requirement cannot be satisfied with organic assets, the collection manager should not hesitate to request external collection

support. The collection manager should have an integrated collection plan, including national, theater, and organic collection assets, to ensure ICRs are collected in a timely, accurate manner.

Collection Management Process

Collection management is, in intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required (JP 1-02). Its purpose is to effectively collect all required intelligence while ensuring the best use of limited and valuable collection assets.

There are two distinct phases of collection management: *collection requirements management (CRM)*, defining what information collections disciplines must collect; and *collection operations management (COM)*, specifying how the collection disciplines will collect. CRM focuses on the IR, is all-source oriented, and generally interacts with intelligence production elements. COM focuses on selecting the specific intelligence disciplines and specific assets to be used to collect information that satisfies IRs. COM establishes a collection strategy and determines how to collect against requirements.

In the MAGTF, CRM and COM are planned, directed, and coordinated by the MAGTF G-2/S-2. However, each MAGTF element has an intelligence staff officer and performs collection management functions. Each unit interacts with levels above and below, and among units, organizations, and agencies on the same level. The further up the chain, the broader the perspective and scope of responsibility and the more organic collection assets and access to collection resources; the lower down the chain, the more specific the function and narrow the scope of collection activities.

CHAPTER 2
COLLECTION REQUIREMENTS MANAGEMENT

Properly articulated, mission-oriented requirements focus the intelligence effort and provide the foundation for successful MAGTF intelligence collection operations.

CRM is the authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission (JP 1-02).

CRM focuses on the requirements of the commander, planner or supported units, is oriented at providing all-source intelligence, and generally interacts with intelligence production elements.

CRM organizes, prioritizes, validates, and manages the ICRs that the collection effort must fulfill. CRM is designed to ensure the high priority ICRs get the attention they deserve and determine what specific collection operations and characteristics must be planned and executed to answer these. CRM begins with initial efforts to determine and answer the commander's PIRs established during the planning and direction phase of the intelligence cycle. The compilation of ICRs is the basis for the collection plan. CRM works in cooperation with COM. During CRM a plan is developed to satisfy the requirements, which then transitions to COM for execution. During execution, CRM continues by checking with those supported to determine whether collection operations are actually satisfying their IRs. The CRM process is used to derive, organize, state, and manage IRs.

Requirements Analysis Criteria

IRs are developed as the commanders and staffs work through the Marine Corps Planning Process. Even in the early stages of mission analysis, the collection manager has compiled a number of questions submitted by the staffs and subordinate commanders. In his initial attempts to organize the collection effort, the collection manager analyzes all ICRs he has received. The collection manager helps identify ICRs that can be answered by currently available intelligence and those that will be incorporated in the collection plan. Criteria used to determine the questions that will be converted into collection tasks will be situation-dependent.

Pertinence

Pertinence demands that only ICRs that are relevant to current operations or operations being planned should be planned and executed. Often a proactive commander or staff may submit an ICR in support of an anticipated but not actually assigned follow-on mission or other nonmission-essential task. The collection manager ensures that only relevant ICRs are acted on.

Feasibility

Feasibility demands that only those ICRs that actually can be collected on should be planned and executed. This refers to MAGTF or supporting assets/resources' ability to perform the collection mission, and also to the existence of collectible or "observable" data that the collector will be able to observe, update, and report.

Completeness

Completeness demands that a proposed ICR is complete; i.e., does it ask only one question? The IR should focus on a specific fact, activity or event. The collection manager should identify those questions that are incomplete and coordinate with the originating commander or staff section for refinement. Collection managers must make all efforts to assist commanders and staffs in drafting questions and refining them if returned.

Validation

Validation checks if the proposed ICR has already been answered and/or if it duplicates existing IRs and ICRs. Questions that pass this criterion are said to be "validated." For those not passing this test, collection personnel will initiate coordination with the production element.

Priority

Priority demands that difficult decisions be made regarding the relative importance of some IRs and PIRs compared to others. PIRs must be rank-ordered by the commander in terms of their relative importance to his decisionmaking. There are no "ties" in PIR priorities. If everything is top priority, then effectively nothing is a priority. All IRs that are not designated PIRs but pass all other criteria likewise must be prioritized. The collection manager must prioritize these also, rank-ordering requirements against each other. The collection manager should do the following:

- Always reprioritize dynamically. The collection manager must have a system in place that allows easy reprioritization based on the commander's guidance and tactical needs.
- Keep the commander informed. It is important that the commander knows when a PIR from a subordinate commander will receive lower priority.
- Be prepared to justify priorities. The collection manager must be prepared to explain what factors influenced the prioritization decisions. Commanders and intelligence officers on other staffs should understand the rationale for the prioritization.
- Continuously communicate current priorities and justifications. Using a database or spreadsheet, subordinate units should be able to monitor the status of their requirements and assess priorities and planned operations. The MAGTF CE should publish and disseminate an updated list as part of an intelligence summary or other periodic product in message format to help lower-echelon commanders and units maintain awareness of higher headquarters' plans and operations. This will also provide an opportunity to adjust for changes in critical situations.

Intelligence Requirements

Intelligence gaps or information needs are formally labeled intelligence requirements. An intelligence requirement is any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence (JP 1-02). In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions (MCRP 5-12C). IRs drive the collections process and the overall intelligence cycle. IRs are initially developed during the planning process. These are the relevant IRs, related to the enemy, threat or battlespace environment, that commanders deem essential for the successful accomplishment of the mission. IRs are categorized as PIRs and IRs.

PIRs are those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decisionmaking (JP 1-02). In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission (MCRP 5-12C). PIRs are prioritized among themselves and may change in priority over the course of an evolution. Only the commander designates PIRs.

Generally, the difference between a PIR and an IR is that a commander must have the answer to the PIR to make a decision. At any one time there are not many PIRs in effect.

The lowest priority PIR takes precedence over the highest priority IR. IRs are questions typically generated by the staff but not ones that the commander feels he needs answered before making decisions. While there are ideally a few PIRs, there may be many IRs. Like PIRs, IRs should be prioritized against each other to support effective intelligence planning and operations.

PIRs and IRs have the following characteristics. Each PIR or IR—

- Asks only one question.
- Focuses on specific facts, events or activities concerning the enemy or the battlespace.
- Is tied to mission planning, decisionmaking, and execution.
- Provides a clear, concise statement of what intelligence is required.
- Contains geographic and time elements to limit the scope of the requirement.

See also MCWP 2-1.

Requirements Management

Management of IRs is a dynamic process that encompasses the continuous evaluation of the following:

- The importance of each requirement to mission success.
- Continued relevance based upon the current situation and plans.
- Information and assets needed to satisfy each requirement.
- Resources that are presently committed toward fulfilling that requirement.
- The degree to which the requirement has been satisfied by intelligence activities.

Processing IRs

Development of IRs and designation of PIRs is continuous. There is a dynamic flow of new IRs—existing requirements are satisfied or are no longer relevant—and the relative importance of each requirement changes as planning, decisionmaking, execution, and assessment progress. As IRs are developed, the collection manager validates, refines, and enters them into the collection management system.

Validating IRs

Validation ensures that the IR is relevant to the mission, has not already been satisfied, and does not duplicate any other requirements.

Refining IRs

Refining the IR entails placing it in the proper format, identifying all related information components, and adding appropriate qualifiers such as geographic limitations or time constraints. During refinement, similar or related IRs may be combined into a single, comprehensive IR.

Managing IRs System

A requirements management system is an essential tool that provides a means to monitor the effort to satisfy each IR. Each intelligence section must develop a system appropriate to its mission and echelon. Minimal components of any IR management system follow:

- A numbering system.
- Identifying who submitted the requirement.
- Designating collection and production assets committed to satisfying the IR or noting when the IR was submitted to higher headquarters or supporting agencies, if organic assets are not available.
- Timeliness requirements.
- Dissemination instructions and information.
- A mechanism to track user satisfaction.

Reviewing Priorities

The collection manager must continually reassess the emphasis given to each IR and realign the priorities according to the commander's intent, current situation, and the planning cycle phase. The intelligence officer must also periodically confirm the assignment of priorities with the commander to ensure that the intelligence effort is focused in accordance with the commander's desires. In addition to IRs of his own command, the collection manager usually receives requests for information from outside agencies (subordinate, adjacent, and senior). Given that MAGTF intelligence operations are centrally managed by the MAGTF CE, the collection manager must continually solicit, assess, and integrate the IR needs of subordinate commanders.

Satisfying IRs

Once an IR has been identified, validated, refined, and prioritized, the collection manager must determine how to satisfy it and allocate the appropriate intelligence and reconnaissance assets to obtain the desired information and intelligence. If the IR cannot be satisfied by organic assets, it must be submitted to higher headquarters or supporting forces/agencies for satisfaction. In determining how to satisfy an IR, the collection manager must consider each step in the intelligence cycle to ensure that the plan encompasses the entire process from collection through utilization. In conjunction with the P&A cell OIC and the CM/DO, the collection team must identify the information needed, where and how to get it, how to package the intelligence into an appropriate product, and how to deliver that product.

Normally, an IR will generate tasks to collect data or information; process/produce tactical intelligence to answer the question; and disseminate the intelligence to all users needing it by a specific time.

Organizing the Collection Effort Around Requirements

Each IR will generally have an associated ICR, intelligence production requirement (IPR), and IDR. See figure 2-1. However, in practice, an intelligence development effort is rarely concentrated on a single IR. Normally, related IRs are grouped together and synchronized to ensure that intelligence operations are focused on the PIRs and satisfy as many IRs as possible. This grouping also helps with the need to employ intelligence resources in the most effective and efficient manner.

Assets/resources to requirements must be matched. Once the ICRs, IPRs, and IDRs have been identified, the intelligence officer allocates the necessary collection, processing and exploitation, production, and dissemination assets to carry out the task.

Collection agencies and production requirements must be assigned. The remainder of the planning and direction effort entails managing the intelligence effort to ensure that intelligence assets stay focused on the PIRs and that the results are being delivered and used to effect tactical decisions. Principles of assigning collection agencies and analytical production to requirements include the following:

- Requirement research: to ensure previously acquired/developed intelligence does not answer current requirements, to include exploiting ongoing/planned collection operations of other friendly forces.

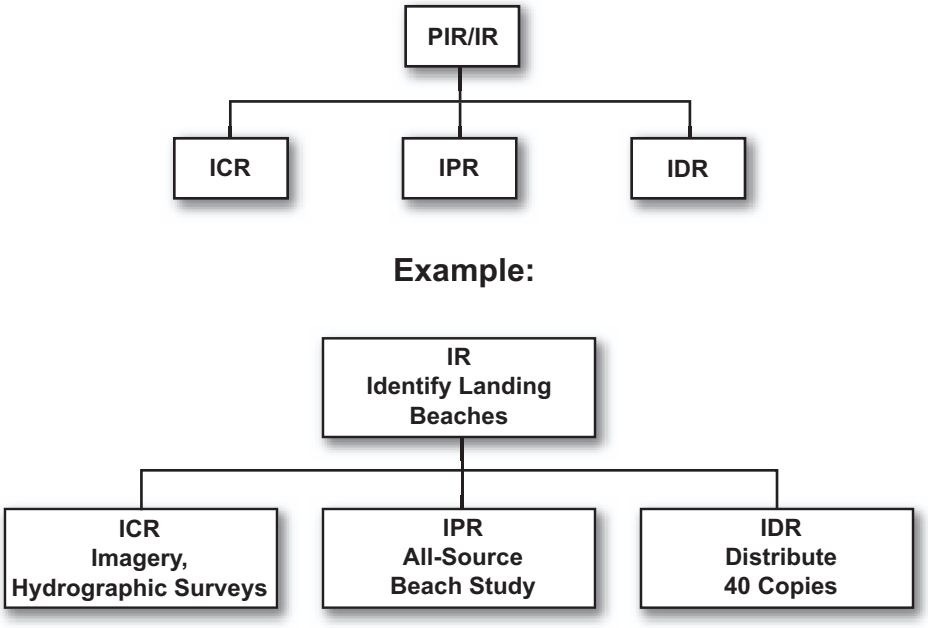


Figure 2-1. Requirements Satisfaction.

- Assessing collectability of the target versus available sensors and other collectors. This identifies the capability of the asset/resource to collect and suitability of the asset/resource to collect. Often what is marginally capable is not necessarily the most suitable to collect, but might be tasked if necessary.
- Conceptualizing multiplicity of collection: to ensure redundancy and as a hedge in case of single asset/resource or single collections discipline failure.

ICR Development Process

The ICR development process uses a building block approach of four steps that translates broad questions into concrete questions, tasks, and orders for collection agencies to perform. See figure 2-2.

Step 1, Identify, Validate, and Prioritize PIRs and IRs

This is the foundation of the ICR development process. It is the basis for collection planning and execution. A common mistake in regard to PIRs

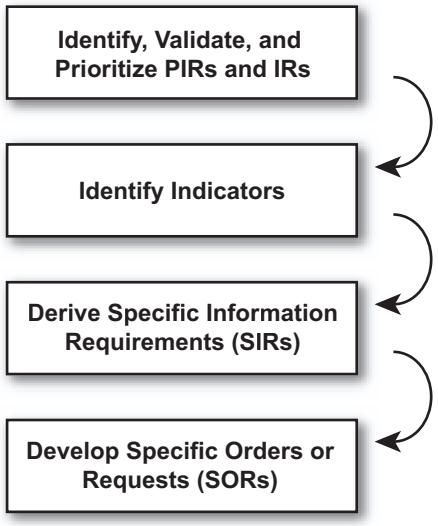


Figure 2-2. ICR Development Process.

and IRs in general is that they lack adequate specificity. Poorly developed PIRs increase the potential of failure regarding timely, pertinent collection, and follow-on intelligence operations. Focused, specific requirements are needed to make informed, effective plans and decisions. Below are examples of common PIRs, with an evaluation of each one's effectiveness.

PIR 1: "Where is the enemy going to attack?" This PIR is too broad, leaving too much open to interpretation in terms of critical considerations, such as specific—

- Threat unit.
- Threat equipment.
- Threat activity.
- Place and time.

PIR 2: "Will the enemy tank division attack our Obj A along Highway 66 prior to D-2?" This PIR provides enough specificity to enable effective collection of the required information and shows how to write a good IR.

Step 2, Identify Indicators

Once the critical IR question has been determined, the next step is to identify the activities that will confirm (or help deny if missing) the event specified in each PIR and IR. These activities, called indicators, are usually stated in general terms, such as "forward deployment of artillery." Indicators provide positive or negative evidence of threat activity or a characteristic of the environment that may influence the commander's selection of a particular course of action (COA). An indicator will often be associated with a named area of interest (NAI), which is a geographical area where activity is expected to occur that will confirm or deny an enemy COA. Guiding principles for indicator development follow:

- Collect on environment conditions or indicators. Developing an indicator related to a characteristic of the environment may be difficult because often there is no activity that describes a characteristic of the AO. It may be useful to evaluate these kinds of indicators in terms of a condition rather than an activity.
- Indicators must be focused and specific. Good requirements, whether PIRs or IRs, ask only one question, focusing on a specific fact, event or activity. The intelligence analyst uses indicators to correlate particular events or activities that occur—or fail to occur—to determine probable enemy COAs.
- Don't overlook the value of negative results. Negative information can be as important as positive information. Negative or disconfirming evidence can provide the intelligence analyst insight about the enemy's rejection of a COA. Negative information could lead to further investigation of a possible branch COA.

Step 3, Derive Specific Information Requirements

Each PIR/IR generates sets of associated specific information requirements (SIRs). SIRs are the observable or "collectible" bits of information that describe the information required to answer all or part of an ICR. A completed SIR describes the information required, the location where the required information can be collected, and the timeframe when it can be collected.

Drafting SIRs is an analytical, time-consuming process requiring a thorough understanding of the particular PIR or IR.

Marine Corps Intelligence Activity (MCIA) 1540-002-95, *Generic Intelligence Requirements Handbook (GIRH),* facilitates rapid, time-sensitive, crisis intelligence planning for MAGTFs. The GIRH is a compendium of frequently asked IRs, organized by mission profile, orders of battle, and terrain. The GIRH is used primarily as a checklist to rapidly organize planning and to determine gaps in information. It may be used as a sort of brevity code to efficiently request information. It may also be used as a baseline intelligence support tool for intelligence centers providing operational intelligence to forward

deployed forces. The GIRH is not a stand-alone substitute for SIR development. Collection managers should not "cut and paste" lists of requirements from the GIRH into their collection requirements list without going through the IR development criteria.

Having linked IRs to an indicator, that indicator must be broken down into very specific questions. This process consists of identifying the specific sets of information that will provide an answer—partial or complete—to each IR. Steps for developing SIRs include the following:

- Further narrow the focus of each indicator to identify "where to collect" (tying it to a specific point on the battlefield). We may use a specific NAI to replace the general idea of "forward" in the indicator, "forward deployment of artillery" and rewrite it as "artillery deployed in NAI 12."
- Refine the time to be observed. Starting from the LTIOV, collections personnel plan backward to determine collection times, taking into account time requirements to sort through collected data, report it, process it, analyze it, and further disseminate it to those needing it. If no LTIOV is specified, it must be requested from the originator of the requirement.
- Determine the specific observables. Next consider the "what to collect," building more detail by identifying the specific information that supports the indicator. For example, the specific information that supports the indicator, "artillery deployed in NAI 12," might include the presence of the following:
  - Artillery weapons.
  - Fire direction control equipment or vehicles.
  - Artillery-associated communications equipment.
  - Artillery ammunition carriers.
- Complete the SIR. A complete SIR describes the information required, the location where the required information can be collected, the time when it can be collected, reporting criteria, and principal and secondary recipients. Generally, each IR generates sets of SIRs.
- Refine the SIR. Develop each indicator further by identifying the specific types of equipment or other collectible/observable characteristic associated with each SIR. For example, replace—
  - "Artillery weapons" with specifics such as "120mm mortars" or "107mm multiple rocket launcher battery," if that is what should be present within the NAI and enemy force composition.
  - "Artillery-associated communications" with "the ABC data signal," if that is the type used by the enemy unit in question. This specificity will aid the collection or asset managers to optimize their collection capabilities against the target in question.

These SIRs have been properly developed. The collection manager has taken a focused PIR, matched indicators to it, i.e., activities that will confirm an event specified in the intelligence requirement, and developed SIR sets to support focused collection. A well-developed IR will contain all information needed to develop supporting SIRs. In this case, the IR often states the "where" and "when" to collect; the requirements manager needs only to refine the "what to collect" into specific items of information. A poorly developed SIR often results in requirements that do not contain the information needed to identify "where" and "when" to collect. Further coordination with the requester of information is then needed to obtain the "where and when." The following scenario is an example of identifying the previous steps of developing SIRs.

During wargaming, a regimental commander tells the S-2 "In order to commit our reserve I need to know if that tank regiment will turn east or west at Tonbak." The collection manager refines this into the PIR "Will the 3d Tank Division enter NAI 8 or NAI 9 on the evening of 5 May?" (triggers regimental reserve)

Note how the PIR is tied to a decision. The results of collection, i.e., the friendly responses, are stated as a *decision trigger.* The IR, as received and worded, is a good one for beginning focused requirements development. It already contains a reasonably detailed description of *what* the commander needs to know, *where* to find the intelligence, and *when* the event is expected to occur. However, the CRM needs to supply the COM and collection mission planners with more detail to support their planning and the subsequent development of SORs. Thus, the CRM concentrates on identifying good indicators to confirm or deny the information desired. One indicator is "movement south of the enemy's 3d Tank Division." The collection manager then develops the following sets of SIRs designed to support the *same* PIR:

- **"Will more than 220 combat vehicles of the 3d Tank Division pass through NAI 8 or NAI 9 between 051400 and 060400 March?"**
- **"Will more than 17 reconnaissance vehicles subordinate to the 3d Tank Division or its regiments pass through NAI 8 or NAI 9 between 041800 and 052000 March?"**
- **"Will more than 38 artillery weapons subordinate to the 3d Tank Division enter NAI 8 or NAI 9 between 015200 and 060200 March?"**
- **"Are more than 2 R-XYZ radios active in NAI 8 or NAI 9 before 060200 March?"**

Step 4, Develop SORs

Each indicator generates a number (sets) of SIRs. Each SIR will, in turn, generate a SOR that can be used to task collection assets or request collection resource support from external assets in the COM process. A well-written SIR is easily translated into an effective SOR by making a directive vice inquisitive statement. In other words, if a SIR is a question, the SOR directs a collection asset or resource to find an answer.

A SOR is the order or request that generates planning and execution of a collection mission or analysis of database information and intelligence. SORs sent to subordinate commands, to include collection assets, are orders. SORs sent to other commands, usually collection resources, are requests. After SORs have been developed, the collection manager is ready to develop the collection plan. The collection plan will reflect the SORs assigned to selected collectors for each IR.

Avoid overly restrictive reporting criteria and guidelines. Allowing collectors appropriate latitude will enable them to provide not only the requested information, but possibly other valuable information not specifically requested. A sample SIR follows.

SIR: "Will more than 17 reconnaissance vehicles subordinate to the 3d Tank Division or its regiments pass through NAI 8 or NAI 9 between 041800 and 052000 May? LTIOV: 052000 May."

SOR 1A: "Report the presence of reconnaissance vehicles in NAI 8 or NAI 9 between 041800 and 052000 May. Specify direction of movement and numbers and types of vehicles. LTIOV: 052000 May."

SOR 1B: "Report the presence of communications nodes associated with reconnaissance elements of the 3d Tank Division or its subordinate regiments in NAI 8 or NAI 9 between 041800 and 52000 May. LTIOV: 052000 May."

Collection Assets/Resource Selection Factors

After defining ICRs and supporting SIRs/SORs, the collection manager must determine the availability and capability of collection assets and resources that may contribute to ICR satisfaction. The collection manager compares the characteristics of the target with the specific aspects of the requirement and the characteristics of available assets or resources to determine the collectors to select. This step involves a cooperative and coordinated effort for both the CRM and COM processes.

The four basic factors that influence selection are capability, suitability (or feasibility), redundancy/multiplicity, and balance. Other factors to consider are target key elements, collection capabilities, correlation, and the environment.

Capability

Is the asset/resource physically and technically capable of collecting the required information on the particular target of interest within the limitations imposed by the requirement? To decide if an asset or resource can collect the data, the collection manager considers a range of operational and technical factors that include key element sets of the target, geography, weather conditions, and threat activity. These factors are then correlated or compared to asset and/or resource availability and capability factors; e.g., platform and sensor range, preparation and system timeliness or characteristics of sensor.

Suitability (or Feasibility)

Is the asset/resource actually suitable to perform the mission, whether alone or in combination with other collectors? The collection manager determines if the different collection/intelligence disciplines have a high confidence level of successfully executing assigned missions given their unique capabilities and limitations. These capabilities and limitations are generally focused on technical or performance characteristics, range, dwell time, and timeliness.

Redundancy/Multiplicity

Should another collector be tasked to collect against the same requirement to provide redundancy or to pose a detection dilemma for the enemy? In some cases a collection asset or resource may not be able to fully satisfy a requirement. To achieve a greater degree of satisfaction, the collection manager employs redundancy of tasking to other collectors. Redundancy employs a collection strategy that involves the use of several same-discipline assets to cover the same target. Redundancy is used on high priority targets when the probability of any one system adequately collecting is low. The collection manager also mixes different sensors in different intelligence disciplines to achieve combined arms effects on an enemy target.

Balance

Are any collection assets/resources overtasked and others underutilized? Proper balance ensures the efficient tasking and employment of all organic and supporting intelligence and reconnaissance assets without overburdening/overcommiting any or underusing others.

Target Key Elements

Key element sets are the parameters of the target's characteristics that can be compared with characteristics of the available collection assets and/or resources to serve as discriminators in discipline or sensor selection. The key elements commonly considered are target characteristics, range to the target, and timeliness.

Target characteristics are the discernible physical, operational, and technical features of a unit, object, event or other intelligence target. These characteristics may be observable and collectible. Observables are the unique descriptive features associated with the visible description (or

signature) of the target, whether it is specific units, equipment or facilities. Collectibles are unique descriptive features associated with emanations from the target. Observables are associated with emanations via IMINT, HUMINT, CI and ground/air reconnaissance; collectibles with SIGINT and CI; both associated with measurement and SIGINT.

Range is measured as distance from a predetermined reference point to the target location. The range to the target can be used to quickly eliminate from consideration those standoff sensors that cannot cover the target area and those sensors on penetration platforms that cannot reach the target area.

Timeliness refers to a comparison of the demonstrated system timeliness of a collection asset or system with the time the ICR must be satisfied by the published LTIOV.

Collection Capabilities

The collection manager translates the capabilities and limitations of available collectors into a set of collection capability factors that can be directly compared to the key target element sets. The capabilities and limitations of the various collectors are considered, together with their availability, to determine if they should be tasked. Sensor capability factors are technical or performance characteristics, range, dwell time, and timeliness.

Performance characteristics are concerned with the system's ability to collect the needed information, output quality, and geolocational accuracy. A collector within a particular discipline may or may not be able to collect information on a particular target. The data quality relates to the level of detail derived from the collected information; e.g., different imagery systems provide varying degrees of imagery resolution. The importance of geolocational accuracy depends on the planned use of the information collected; e.g., targeting demands greater locational accuracy than information collected for threat unit identification and order of battle updates.

Range deals with the collector's ability to provide target coverage. For airborne systems, range is determined by considering the actual range capabilities of the aircraft and its collection system to provide detailed information sufficient to satisfy the requirement and any operational or fire support restrictions placed on it. The CRM process assesses combinations of these range factors to determine the collector's potential to meet the tactical ICR.

Dwell time is the length of time a given collector can maintain access to the target, an important consideration during collection monitoring, particularly during high tempo operations.

Timeliness considers the time required to complete each collection event and is calculated or estimated for each available sensor based on the tactical situation. Times vary depending on mission priority assigned, specific system availability, time required to plan the mission, and related information processing and dissemination means. These times are added to find an overall elapsed time, then compared with the latest timeliness information stated by the requirement originator.

Correlation

Correlation is the process that associates and combines independent data on a single subject to improve collection reliability or credibility. Key target element sets are compared with collection capability factors to provide a preliminary list of units and sensors that are technically able to collect the desired data within range to the target and time required.

Environment

After correlation, candidate sensors are compared with environmental factors to support final sensor selection. Environmental factors include collector vulnerability to the threat, weather and light conditions, and terrain that might influence the collector's ability to acquire the necessary information. Depending on the environment, a technically capable sensor may be dropped from consideration.

Sensor vulnerability is the degree to which adversary fires countermeasures (deception, camouflage, and operations security) will affect sensor selection and depends on the vulnerability of the sensor platform. In general, the platforms of penetrating sensors are the most vulnerable, stand-off sensors less so, and satellite sensors the least vulnerable. Threat assessment is an evaluation of risk versus potential intelligence gain.

Weather and light conditions are considerations, particularly with imagery and visual collection sensors. Weather conditions in and around the target area affect the sensor capability to collect and exploit data.

Terrain is also a consideration. It may mask a target, thereby dictating the direction a sensor must point or locate, which will influence ingress/egress route planning for penetration sensors, flight paths, loiter tracks for standoff sensors and/or satellites, SIGINT collection/direction finding site selection or additional radio communications relay needs.

Intelligence Collection Planning

Compilation of ICRs and SIRs is the basis of the collection plan. Collection planning is defined as a continuous process that coordinates and integrates the efforts of all collection assets and resources. The CRM cycle begins with initial efforts to answer the IRs, particularly the commander's PIRs, established during the planning and direction phase of the intelligence cycle. Based on these requirements, intelligence analysts prepare RFIs. In the context of collection management, RFIs are queries to see if the information and intelligence already exists. If not, they form the basis for the ICRs and IPRs. When the RFI manager positively determines that the information is neither available nor extractable from archived information or from other intelligence sources, an intelligence gap is identified. It then becomes the responsibility of the collection manager to obtain the information.

The collection plan includes the supported IRs, SIRs, when the information is needed, reporting criteria, who is to receive the finished intelligence, and how it is to be used. The information collected to satisfy these ICRs will answer the IR or be used in intelligence analysis and production. The collection plan forms the basis for further collection actions. The collection plan is integrated and coordinated, selecting the best collectors to satisfy each requirement. It will be a text, graphic or combined representation of the collection strategy. The collection plan may be a simple hardcopy or automated worksheet used solely by the intelligence section, or a more formal, comprehensive document, depending on the complexity of the requirements to be satisfied. Regardless of whether automated or manual tools are used, the basic content of the collection plan includes the following:

- IRs.
- Indicators.
- SIRs.
- Collection assets and resources to be employed.
- Reporting criteria and instructions.
- Remarks.

IRs Worksheet

The IRs worksheet is a useful tool for tracking the status of IRs. The format is established by unit procedures or may be established within the OPLAN/OPORD. See figure 2-3 on page 2-12 and appendix A for a detailed description.

MEF IR Number	Requester Number	DTG Received	Subject	Action	Status
04-1012	1st Marine Division Number 04-001	090830 Jan	Recon Activity in NAI 32	SOR Numbers 04-1462 (UAV) 04-1463 (GSP) 04-1464 (Force Reconnaissance)	Closed 091630 Jan
04-1014	MEF G-2/P&A Cell	101100 Jan	Imagery of landing beaches	Forwarded to JTF J-2 or national collection	Pending

Figure 2-3. Sample Intelligence Requirements Worksheet.

Intelligence Collection Worksheet

The intelligence collection worksheet is a useful tool for linking IRs to collection assets. The format is established by unit procedures or may be established within the OPLAN/OPORD. See appendix B for a sample intelligence collection worksheet.

Reporting

Specific reporting criteria instructions are included. Normally, the place where information is reported is the unit that submitted the requirement.

Collection and Related Planning Tools

Although the collection management process has been formalized for quite some time, it remains dynamic and continually evolving. Technological advances have increased the timeliness of collections planning, direction, and execution. Many collection planning tools have emerged that provide significant improvements to the process. The most important of these follow:

- Standard collection plan format. The collection plan establishes guidance for intelligence collection activities and tasks collection assets. See appendix C for a sample intelligence collection plan. It contains specific orders for subordinate elements to collect and report information.
- Collection tasking worksheet. This management tool assists the collection manager in identifying a specific collector, system or discipline best suited to collect against a particular information requirement. See figure 2-4.

COLLECTION TASKING WORKSHEET

Organization: **Registration:**

DTG: **Collection Manager:**

SIRs:

Time: **Target Range:**

Characteristics:

Assets/ Resources	Range	Timeliness	Characteristic	Weather	Geography	Threat	Capability	Remarks
HUMINT								
CI								
IMINT								
COMINT								
ELINT								
MASINT								
OSINT								

Assets/Resource Selected: **HUMINT:** **COMINT:** **MASINT:** **CI:**

IMINT: **ELINT:** **OSINT:**

Figure 2-4. Intelligence Collection Tasking Worksheet.

- IPB collection techniques. When properly conducted, the results of IPB are an exceptional aid in identifying critical gaps of information and focusing collection requirements. The event template and event matrix together describe the indicators and activity expected to occur in NAIs, targeted areas of interest, and decision points. Using the decision support template and a graphical or written record of COA wargaming, the collection manager can determine where collection is required, what is to be collected, and when the information is required.
- Collection status update paragraph. The use of collection status update paragraphs as part of an intelligence summary is an effective technique to ensure all within the MAGTF are aware of planned collection missions. In it the collection manager provides a summary of the unit's collection priorities and planned operations for a specified period. The collection status paragraph can update a unit's active and cancelled requirements, and is a good way to inform subordinate, adjacent, and higher headquarters units of the a MAGTF's planned collection requirements and operations. Appendix D provides an example of a collection status update paragraph to a MEF intelligence summary. Items that may be included are intelligence collection priorities, cancelled requirements, and planned intelligence collection missions.

Intelligence and Reconnaissance Assets Tasking

The tasking mechanism for MAGTF intelligence and reconnaissance assets is situation-dependent and shaped by a number of variables. The collection manager issues orders to those assets that are in DS or attached to his unit. Certain external collection resources are tasked only through structured and rigorously enforced standards for collection requests; e.g., national IMINT and SIGINT systems. The intent of these collections tasking guidelines is to standardize the process to improve the quality and timeliness of collection operations.

Standard Formats for Asset Tasking

Tasking request formats or messages depend on the tactical situation, type of sensor, and type of asset or resource; i.e., organic, supporting, theater, national or multinational. Many specific data elements in these requests and the transmission procedures are classified. In the case of MAGTF organic and DS, requesters follow combatant command instructions provided in the unit standing operating procedures (SOPs), theater procedures, and OPLAN/OPORD intelligence annexes. The Joint Tactical Exploitation of National Systems manual and the 58-series of the Defense Intelligence Agency Manuals (DIAMs) provide guidance for requesting collection support from national resources.

Guidelines for Requesting National/ Theater Collection Support

Formats to request national and theater collection are in various DIAMs (58-series), Joint Tactical Exploitation of National Systems manual, and combatant and theater command TTP. Regardless of the formats used or the mechanisms for tasking those national/theater resources, CRM should be guided by the following principles:

- Areas of interest. National systems are best employed against high-priority targets outside the range of organic or theater sensors, beyond standoff collection range, and/or in high areas.
- Exploitation and/or analysis timeliness. Targets must be chosen such that, under applicable timeliness constraints, exploitation reports will reach the commander in time to react or influence decisionmaking.

- Justifications. Request justifications must fully explain the need for information and support the priority assigned by the requester.
- Sensor capabilities. Target descriptions must place minimum restrictions on the employment of collection systems.
- Sensor accessibility. The targets' accessibility must be determined when possible before a collection request is forwarded.
- Exploitation and/or analysis requirements clarity (concise, explicit statements of actual information needed).
- Exploitation and/or analysis requirement purpose (state the purpose of the information desired when it will benefit the interpreter and/or analyst).
- Preplanned collection. Preplanned target sets submitted in advance of an operation can relieve the workload and must be considered where the tactical situation permits.

Production Requests

Once the unit intelligence officer determines that the requirement cannot be met with local resources, the requirement is forwarded up the chain of command for satisfaction. The intelligence officer determines whether to submit the requirement as RFI, ICR, IPR or production request (PR).

Generally, an RFI is submitted if the requirement is a fairly straightforward question. In a noncombatant evacuation operation, an RFI may be, "How many personnel require evacuation?" In this case, no extensive collection or production is required because the intelligence is generally available.

A PR is more appropriate when the IR is complex or substantial; e.g., "What is the capability of country X to defend its coastline against an amphibious assault?" This requirement may result in an IPR for the MEF CE or a PR to the JTF headquarters because the answer will require the collection and analysis of a large amount of information ranging from hydrographic conditions to available threat weapon systems. Such analysis may be beyond the capabilities of a small unit intelligence section and more appropriately performed at the theater or Service level where access to information and ability to task collection resources are greater.

A PR is also appropriate to satisfy a requirement that may be recurring in nature or in a denied area; e.g., "How many aircraft are maintained on alert status at airfield Y?" If organic assets are not available, the unit intelligence officer will submit a request for theater and national production assets to monitor the airfield to determine the answer. As an RFI travels up the chain of command, it is satisfied (from available information or intelligence or by collecting new data), converted into a PR or forwarded to the next higher level for satisfaction. Each unit in the chain of command validates the PR and satisfies it from within or passes the requirement to the next higher authority for action.

Most IPRs are levied on the intelligence battalion, P&A company's P&A cell, which is the MAGTF's principal deliberate production asset. Based on the commander's guidance and the G-2/S-2's direction, the intelligence battalion commander or ISC does the following:

- Plans, manages, and conducts MAGTF IPR management.
- Exercises staff cognizance over MEF collection and production elements to fulfill PRs.
- Determines PRs that are produced locally and PRs that are forwarded to the appropriate theater, Service or national Department of Defense Intelligence Production Program (DODIPP) production center validation officer (VO).

The VO reviews the PR, determines if to accept and satisfy it, forward to another production center or invalidate the PR. The combatant commander, the joint force commander or the MAGTF commander directs PR and RFI procedures, which vary from theater to theater; e.g., a

MAGTF preparing to deploy submits PRs through the normal Service chain of command to the MCIA VO. However, a MAGTF operationally assigned to a combatant commander submits PRs through the established operational chain of command to the VO supporting that theater. A theater intelligence directorate (J-2) may delegate validation authority to a JTF J-2 during a crisis, providing the JTF J-2 a streamlined path for joint intelligence center production support and priority over other noncrisis production requirements. For most crises and contingencies, annex B to the joint force commander's OPLAN/OPORD specifies policies and procedures for requesting intelligence production support.

Production Request Format

The same basic format is generally used for RFIs and PRs. This facilitates conversion of an RFI into a PR at a later time. A basic level PR must include the following:

- Organizations and specific offices or individuals requesting the product.
- A statement describing the required information and intelligence and sources consulted by the requester and source shortcomings relative to the request.
- LTIOV.
- Product form; e.g., hardcopy text, electronic file on disk, and total quantity of each.
- Requirements prioritization for multiple elements.

The basic format is sufficient at lower tactical levels. At higher levels the format becomes more structured. Defense Intelligence Management Document 0000-151C-95, *Department of Defense Intelligence Production Program (DODIPP): Production Procedures*, stipulates the format for PRs, which ultimately will be forwarded to a DODIPP VO and production center. Each combatant command defines formats and procedures in their applicable intelligence procedure documents. The MEF CE and MSC headquarters SOP define formats for their headquarters and subordinate elements. See also MCWP 2-12, *MAGTF Intelligence Production and Analysis*.

CHAPTER 3
INTELLIGENCE COLLECTION OPERATIONS MANAGEMENT

Collection operations management is the authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. (JP 1-02)

The COM process organizes, directs, and monitors the units, equipment, and personnel that actually collect the data to satisfy the ICRs. Strategies and plans are developed for collection to accomplish the following:

- Estimate how well a collection asset or resource can satisfy requirements.
- Evaluate the performance of collection assets and resources.
- Allocate and task assets or request resources.
- Monitor and report the results and status of collection efforts, organizations, and systems.

Actions taken by units explicitly to satisfy IRs are collection operations. Considerations are similar to any other kind of operation. Intelligence COM is concerned with the mission management (how to employ collection resources) and asset management (execution of collection missions) functions of the collection cycle and includes the following:

- Mission planning and collection plan development.
- Collection asset tasking.
- Exploitation and reporting.
- Supervision of the collection effort.
- Updating the collection plan during execution.

Mission Planning and Collection Plan Development

Mission planning is based on the requirements generated by the CRM process. It plans and executes operations to satisfy those requirements. It supports the entire intelligence cycle, focusing on the processing and exploitation, production, and dissemination steps of the intelligence cycle and the collection process. As an integral step in the CRM/COM process, the collection manager must be informed of the requirement originator's guidance for production and dissemination. Any specific constraints or restraints should be identified during the CRM process and factored into COM mission planning.

COM mission planning is concerned with identifying, scheduling, and controlling collection assets and/or resources. The COM planner reviews the mission requirements for system responsiveness, weather, threat data, and intelligence reporting requirements. These elements are considered with the detailed technical, CIS, administrative, and logistical data of each tasked asset or collection system to determine asset availability and capability. Requirements are then translated into specific mission tasking orders.

CRM and COM processes use similar intelligence collection planning and management tools including the following:

- Intelligence collection worksheet.
- Intelligence collection plan.
- Collection reports.
- Collection status update paragraph.
- Collection emphasis message.

In simple terms, COM allocates and tasks assets and resources and monitors and reports the status of collection operations.

Collection Asset Tasking

Key considerations that affect the planning and scheduling of intelligence collection operations follow:

- Clear communication of mission, intent, concept of operations, and tasks to those units that must execute them.
- Ensuring suitability of intelligence collection resources to accomplish missions and achieve objectives, to include that of the unit and all subordinate and supported commands.
- Ensuring sustainability of intelligence collection operations to support current and anticipated future operations.
- Monitoring progress of intelligence collection operations and adjusting plans to achieve collection objectives.

While much of the responsibility for most of overall planning and direction effort rests with the G-2/S-2's intelligence operations officer, the collection manager must maintain concurrent awareness of these factors and their impact on collection planning and operations.

After a thorough study of availability, capability, and performance history, the collection manager selects the resource most capable to satisfy the requirement. Various approaches to collection exist. They center around three strategies or a combination of them:

- Tasking organic or supporting intelligence and reconnaissance resources.
- Requesting intelligence and reconnaissance collection support from external MAGTF forces.
- Recommending other collection tasking to subordinate elements.

Tasking Organic Collections and Production Assets or Supporting Collection and Production Resources

Although the strategy adopted by the collection manager will always vary based on the mission and the IRs to be satisfied, tasking organic assets should be considered first. The advantage to this is that the collection manager has the most control over these assets and they are generally more responsive. The collection manager usually understands their capabilities, limitations, and performance history well. Generally, reconnaissance assets should not be held in reserve. A possible exception to the policy of employing all reconnaissance assets without a reserve is when the collection manager is aware of a future requirement that will need to be addressed.

Requesting Support from External MAGTF Collection and Production Resources

The IRs generated in the planning cycle often mandate employment of external resources. When selected, requests for support from higher headquarters, e.g., JTF, theater or national assets, should be prepared and submitted up the chain of command. Although external collection resources may be more capable than some organic assets, the collection manager runs the risk that those external assets may already be tasked to other competing IRs and his needs will go unmet. Various tasking documents levy IRs on collection resources. Some tasking mechanisms are theater- or intelligence systems-unique. The Joint Tactical Exploitation of National Systems and various DIAMs specify procedures and formats for requesting support from national systems or agencies. Combatant commands will also modify, clarify or add to these procedures in their local intelligence SOPs or TTP.

Tasking Subordinate Elements

Recommending collection tasking to subordinate elements can be a lucrative source for satisfying IRs. Even Marines not assigned to an intelligence collection unit can provide valuable information, especially when in contact.

Often times at units below the MEF CE level-particularly at the battalion or squadron level-these taskings take the form of reconnaissance and surveillance (R&S) plans.

A mission tasking order goes to the unit selected to accomplish a particular collection mission. The selected unit makes the final determination of specific platforms, schedules, equipment, and personnel to be employed.

MAGTF Collection Tasking

There are many ways to task collection assets. The primary means to task MAGTF collection assets include the following:

- OPLAN/OPORD Intelligence Annex. Annex B, Intelligence, of the OPLAN/OPORD is the most commonly used vehicle for initial collection taskings. Appendix 10, Intelligence Operation Plan, contains the intelligence collection plan (appendix 10, Tab A).
- OPORD/FRAGO Execution Paragraph. Another tool for disseminating collection taskings is to include those taskings in paragraph 3 of the unit's warning, fragmentary or OPORD or in a standalone collection unit FRAGO. Detailed coordination must be conducted with the G-3/S-3 for this technique to succeed. Amplifying or supporting details can be included in annex B or its appendices as required.
- RFI. RFIs are any specific, time-sensitive IRs to support ongoing operations. It is not necessarily related to standing collection requirements or scheduled intelligence production. An RFI is initiated to respond to tactical requirements (critical information gaps and is validated in accordance with the unit's SOPs); e.g., a regimental S-2 may submit a time-sensitive RFI requesting confirmation of the size and composition of an enemy formation (no further information) reported by one of its battalions at a specific location. This would then be researched by higher headquarters G-2 staff and answered immediately if the information or intelligence exists. If the information or intelligence does not exist, the RFI would form the basis for an ICR that may result in a request for UAV support.
- Collection Emphasis Message. A collection emphasis message is another tool to broadly disseminate the MAGTF's collection focus. It is disseminated to higher, lower, and adjacent units; intelligence collectors; and intelligence exploitation and processing centers. It details the unit's PIR's and associated SIRs and SORs. The primary benefit of communicating collection intent is the operational perspective it provides organizations that may otherwise be isolated from the planning process. An informed collector can often amplify reporting to provide an answer that goes beyond immediate questions. See appendix E for a sample message.
- Statement of Intelligence Interest. A statement of intelligence interest (SII) is a comprehensive listing of a unit's IRs for a specified time period. The SII usually addresses long periods of time (2 to 3 years) and identifies broad areas of interest rather than specific information requirements addressed by SORs. All commands larger than battalions/squadrons should submit an SII and update it periodically. These SIIs are used to develop dissemination requirements for the DODIPP. The dissemination scheme may result in hardcopy or softcopy dissemination to units.

Exploitation and Reporting

Exploitation of collected information and reporting is closely associated with the management of collection assets and resources. Generally, the staff allocated a collection capability also controls the

supporting processing, exploitation, analysis, and production response. The collection manager shares a responsibility for evaluating the collected information. The consumer—the supported commander or his users of intelligence—ultimately determines how well the IRs have been satisfied.

Techniques that assist in effective exploitations include cueing, redundancy, mix, integration, and coordination.

Cueing

Cueing uses one or more intelligence or reconnaissance asset to provide data directing collection by other intelligence or reconnaissance elements. Cueing maximizes the efficient use of finite collection assets in support of multiple, often competing, intelligence collection priorities.

Collection managers should plan to create opportunities for cued collection as part of the collection strategy; e.g., a HUMINT source may be employed 24 hours before a UAV mission to confirm or deny activity along a key corridor. If the HUMINT source reports the absence of activity, the UAV mission can be redirected to another area or used to confirm the absence of activity, depending on the relative priority of IRs. If the HUMINT source reports significant activity earlier than anticipated, the UAV mission may be accelerated to collect supporting detail, or instead retasked to another mission.

Cueing may occur dynamically (outside the collection strategy) as one intelligence or reconnaissance collector tips off another collector to a collection opportunity. Intelligence collection systems can drive operational tasking. This is most common when collection on a particular NAI triggers a decision corresponding to a decision point or fires at a target area of interest. Examples follow:

- An aviation ground attack mission is "tipped off" to specific threat air defense activity and flies a different ingress-egress profile.
- Indirect artillery fires are "cued" to more precise target areas.
- Ground maneuver elements are "tipped off" to changes in an expected enemy COA.

These examples illustrate the need for coordinating intelligence with other operations and demand the collection manager's active participation in the wargaming process when requirements are initially developed, and for close coordination with current operational intelligence, operations, and fires elements.

Redundancy

Redundancy planning is part of a collection strategy using several same-discipline assets to cover the same target. Redundancy is often used on high priority targets when the probability of any one intelligence or reconnaissance element adequately collecting is low. The probability of detection increases as a function of the number of collectors; e.g., if several SIGINT collectors focus on a designated emitter at different times, the probability of intercept improves, even if the emitter operates intermittently. The chance of acquiring accurate geolocational information using direction finding equipment is also improved through redundant collection tasking.

Mix

Mix means planning for complementary coverage by a combination of assets from multiple disciplines. Intelligence and reconnaissance mix techniques increase the probability of collection, reduce the risk of successful enemy deception, can facilitate cueing, and provide more complete intelligence reporting. The best mix of collectors puts the enemy in a dilemma. No matter what the enemy does (stays still or moves out), he is detected, identified, and possibly located; e.g., reconnaissance reports resupply activity within a known assembly area; SIGINT intercept of the associated logistics net provides unit identity, subordination, and indications of future activity.

Integration

Integration is the resource management aspect of collection strategy development. It involves integrating new requirements into planned or ongoing missions. Barring a decision to use redundant coverage for a critical target, collection managers must integrate new missions with previous planned or ongoing missions. Integration helps to avoid undertasking capable collectors. Resource integration examples are:

- Adding ICRs to a light armored reconnaissance battalion performing a zone reconnaissance mission.
- Inserting a new ICR during a preplanned UAV mission or replacing an existing requirement with one of higher priority.

Coordination

The collection manager must ensure the plan is coordinated. The collection manager develops SIR sets from the consolidated, validated, and prioritized list of PIRs and IRs. SIRs complete the collection strategy by associating each requirement with the corresponding decisions and time lines. Starting at the point that the commander requires intelligence to support a decision, the collection manager backward plans the collection mission to account for mission preparation, collection, reporting, processing, analysis, production, and dissemination.

One tool to coordinate the collection strategy with the planned friendly and estimated enemy operations is the intelligence synchronization matrix. In addition to the LTIOV determined by the prioritized IRs and associated decision and reporting criteria, the matrix records NAIs from the event template and reflects timelines of expected enemy activity from the IPB event template and the event matrix. The intelligence synchronization matrix provides the basic structure for the more detailed collection plan. See figure 3-1.

Report Formats

Standardized report formats support common understanding, interoperability, and efficient dissemination of collection results and other intelligence products. Standardized formats simplify and speed along the accurate, timely flow of reports from information collectors to intelligence analysts and allow their rapid incorporation via information systems into databases. Some of the more common reports used in collection reporting follow.

SIGINT

Most SIGINT reports are formatted and classified. Common reports include:

- SIGINT spot.
- SIGINT summary.
- Tactical.
- Tactical electronic intelligence.
- Critical intelligence.

These reports disseminate time-sensitive SIGINT information from collectors to requesters or intelligence consumers. However, information may also be disseminated using noncodeword reports. Unlike standard SIGINT product reports, noncodeword reports may be passed directly to commanders to allow immediate tactical use. Specific procedures for noncodeword reporting during operations should be in the SIGINT appendix to annex B of the OPORD. See MCWP 2-15.2.

Ground Reconnaissance

Reconnaissance teams report to their higher echelon of command. These reports are received in the SARC. The SARC also establishes priority reporting criteria for each committed team based on that team's information requirements. Normally, teams do not maintain constant radio communication while moving and sometimes while in observation posts, but they do monitor and transmit messages during the established windows.

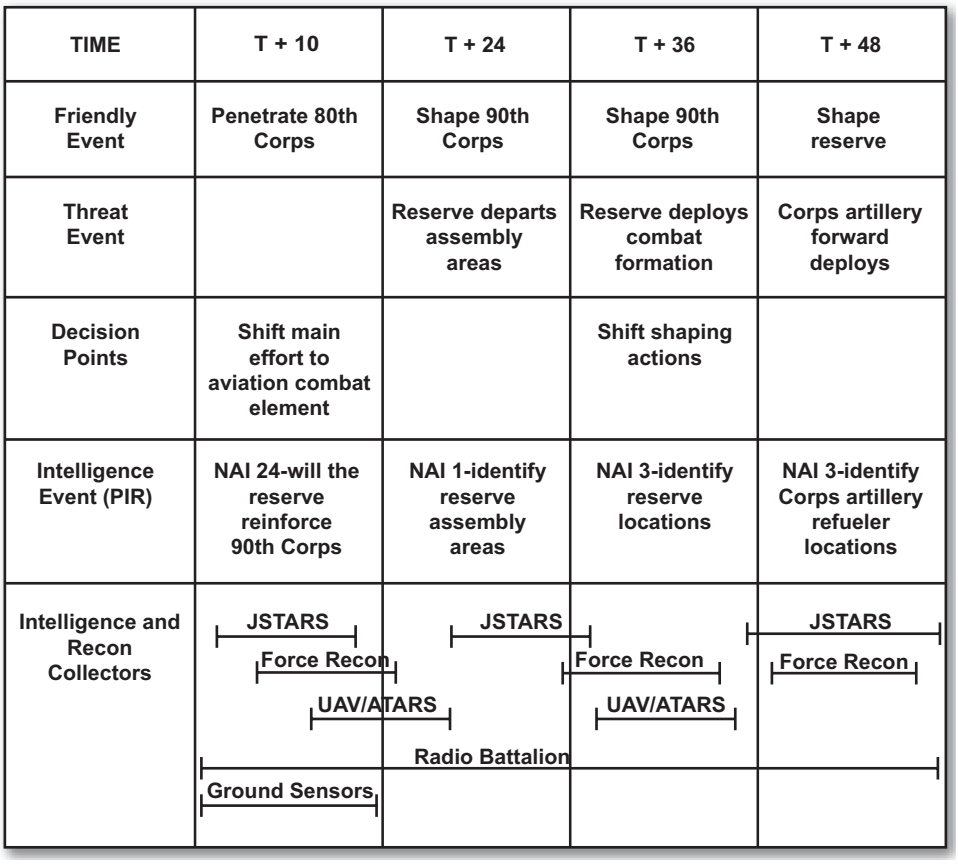


Figure 3-1. Notional Intelligence Synchronization Matrix.

The SARC, however, establishes around-the-clock radio watches over primary and alternate nets so that teams can communicate immediately if necessary. Reporting windows may be established for the transmission of routine traffic or routine reports, such as situation reports. Other primary reconnaissance reports include:

- Size.
- Activity.
- Location.
- Unit.
- Time.
- Equipment.
- Hydrographic.
- Beach survey.
- Confirmatory beach.
- Surf.
- Landing zone.
- Road and route.
- Bridge.
- River/estuary.

See also MCRP 2-15.3B, *Reconnaissance Reports Guide*.

Measurement and SIGINT

Sensor information is like any intelligence information. It is analyzed and combined with other intelligence information to build a complete picture of the AO and the threat. The sensor report is the standard format used to report sensor data. This format is used for voice, data, and hardcopy reports. The general state of the sensor network, changes in the status of specific strings and

relays, and planned sensor operations can be reported using the sensor status report. See MCWP 2-15.1.

Interrogator/Translator Operations

Results of interrogation of enemy prisoners of war and detainees provide a valuable source of intelligence information. The tactical interrogation report may provide a written summary of initial or subsequent interrogations. The document translation report may disseminate information resulting from captured enemy document exploitation. The intelligence information report format may also disseminate information derived from interrogation or translation. A HUMINT appendix may be included within Annex B, Intelligence, of the OPLAN/OPORD to establish standardized reporting procedures.

CI

CI assists in accomplishing three major objectives:

- Screening out refugees whose very presence threatens overall security of the force.
- Detecting enemy agents' intent on espionage, sabotage, terrorist or subversive missions against the force.
- Collecting information of value to other intelligence and security agencies.

The principal reports are the CI spot report, CI information report, and CI interrogation report. The CI spot report is a quick response report to get information into the all-source correlated database. The CI information report is a standard report used to report tactical CI information. The interrogation report is used to report interrogation information. MCWP 2-14 contains formats and specific instructions for completing these reports.

IMINT

IMINT mission results are reported in various reports. The specific type of report used is driven by the requirement originator's timeliness/currency concerns; i.e., LTIOV, and the type of mission being reported. All imagery reports are submitted via data or hardcopy format from the processing or exploitation center to the supported unit. IMINT reports are disseminated to adjacent and higher units. The reconnaissance exploitation report expeditiously reports results of an aerial imagery mission. Results should be disseminated within 1 hour of receipt of the imagery at the processing facility and focus exclusively on immediate information requirements. The initial photo interpretation report provides information on imagery collection missions not previously reported and can follow up any issued reconnaissance exploitation report with amplifying details. The supplemental photo interpretation report provides information not previously included in a reconnaissance exploitation report or initial photo interpretation report. See DIAM 57-05, *DOD Exploitation of Multi-Sensor Imagery*, and MCWP 2-15.4.

Miscellaneous Reports

- Response to RFI.
- Patrol.
- Mission.
- Ground reconnaissance or aircrew debriefing.
- Spot.
- Bombing, shelling, and mortaring location report.

The response to RFI report is generally submitted via data or hardcopy formats. The ground reconnaissance and aircrew debriefs are usually submitted via voice, however, aircrew debriefs are often submitted via message as mission

reports. The bombing, shelling, and mortaring location report contains observance of enemy indirect fire weapons. This report is submitted via voice communications.

Supervision of the Collection Effort

Direction of the collection effort does not end with issuing SORs. The collection effort is continually supervised by the collection manager and coordinated with the C2 elements of the collection asset or resources. The focus is to ensure that collection agencies have received SORs and that they are clearly understood. Coordination is conducted with processing and exploitation centers and among MAGTF collection operations officers and those of higher, adjacent, and subordinate units.

Functions

Monitoring

Monitoring of ongoing collection operations is conducted to ensure that PIRs and other IRs are being satisfied and that they are done so in a timely manner. Intelligence reports received are reconciled with the requested LTIOV of requirements to assess the timeliness and responsiveness of the collection operations. Monitoring is conducted by the requester, the collection manager, and the production and exploitation centers.

Evaluating

The evaluation process tracks the status of collection requirements and provides feedback to the requesters. When collection results are provided, the collection manager evaluates the reports for the following:

- Completeness.
- Clarity.
- Adherence to specified reporting criteria.
- Responsiveness to users' intelligence and timeliness satisfaction.
- Identification of opportunities to cue other intelligence and reconnaissance collection resources.

Requester feedback establishes customer satisfaction, permits tasker deletion, and frees collection assets and resources to be redirected to satisfy other active requirements.

Updating

Based on the requester's assessment of requirement satisfaction, the collection manager reviews priorities for currency. The collection plan is updated to include retasking (if the requirement is not satisfied), adding new requirements based on the impact of changes in planned friendly operations, changes in known or assessed enemy operations or canceling satisfied requirements. It is imperative that the collection plan be continually updated and those changes communicated to higher, lower, and adjacent units to maximize collection operations efficiencies.

Duties

Collection Manager

The collection manager should prioritize IRs, convert them into collection requirements, and coordinate actions with appropriate collections agencies. The collection manager must continually seek to maximize the effectiveness of limited collection resources within operational time constraints.

P&A Cell OIC

Primary responsibility is to manage and supervise the MAGTFs all-source intelligence processing and production efforts.

SARC OIC

As one of the focal points for intelligence reporting from organic assets, the SARC OIC must screen the intelligence reporting and interface with intelligence analysts to see if reporting is satisfying stated requirements.

Subordinate Unit Intelligence Officers

Supervisory responsibilities at the tactical level include ensuring that IRs are correctly prioritized and submitted and that feedback in the form of an evaluation is provided to the collection manager and/or collectors. This two-way communication enables requestors to clarify issues that may not be understood by collectors.

Updating the Collection Plan During Execution

As information is reported from collectors and new IRs are generated throughout the MAGTF, IRs and the collection plan require updating. If the data is insufficient, additional collection may be coordinated with the collection manager. At this point, the processed requirement transitions out of the COM cycle. The collection manager and the P&A cell OIC, in coordination with the SARC OIC and requesters, continually assess the effectiveness of collection operations and how quality and timeliness may be improved. As the collection plan is updated, all subordinate commanders and their intelligence officers must be informed so they may be apprised of ongoing MAGTF intelligence collection operations. Direct communication with those directly affected is critical. Broad dissemination of intelligence collection plan updates may be accomplished by web-based or other automated means.

CHAPTER 4
PLANNING AND EXECUTION

The intelligence collection effort must support and adapt to the MAGTF commander's intent, concepts of intelligence and operations, and the supporting scheme of maneuver. Key questions for operational integration include the following:

- What is the MAGTF AO and the area of interest?
- What is the MAGTF concept of operations, task organization, and main and supporting efforts?
- What are the standing PIRs and IRs? Which have been tasked to supporting units? What specific information is the commander most interested in; i.e., enemy ground operations, enemy air operations, target BDA, friendly force protection or enemy future intentions?
- What is the concept of MAGTF fires support? How will MAGTF target development and target intelligence be conducted? What are the specific collection needs to support these?
- What are the concepts of intelligence and operations of other JTF, component, and theater resources? What are the task organization and command/support relationships for all MAGTF intelligence and reconnaissance units?
- How can naval collection assets and other Services, JTF, theater, and national collection assets be employed and integrated to support MAGTF operations?

Terrain

Terrain factors have a significant impact on intelligence collection operations, particularly on the ability of certain sensors to "see" through vegetation; requirements for line of sight communications; and employment considerations in intelligence collection operations and for the time-sensitive dissemination of collected intelligence products by MAGTF CIS. Many intelligence collection systems require line of sight with the target area to be effective. Accordingly, collection planners must assess the effects of mountains, defilade, vegetation, and other potential terrain obstacles on planned collection operations.

Weather

Weather is a key limiting factor in some collection operations. Bad weather may degrade identifying and locating targets. Weather can also limit the type of collection capabilities that may be employed. Low ceilings and poor visibility can decrease visual reconnaissance effectiveness and the resolution of photographic systems.

Threat

Detailed threat analysis must be conducted to determine the intelligence collection sensors and platforms that can be employed effectively against a given enemy and how to employ limited MAGTF and external resources to obtain the best possible intelligence. Collection operations can be hampered by the enemy's air defense capability and his camouflage, cover, concealment, and deception activities. Threat EW capabilities must be determined to assess their effects on UAVs, manned platforms radio uplink, and various downlinks.

Coordination with Maneuver and Fires

Maneuver and fires considerations include many issues requiring precoordination and several organizations and command echelons needed for the coordination. The detailed procedures needed to

execute maneuver and fires to collection and integration of collection operations into the MAGTF maneuver and fires scheme should be included in unit SOPs. Main operational issues follow:

- Requests and coordination of air support and integration within the air tasking order.
- Fires planning and necessary fire control measures (restricted fire areas and no fire areas).
- Necessary maneuver control measures (insertion and extraction requirements and plans to include short-notice emergency extractions).
- Collectors operating within subordinate unit AO under a wide range of command relationships.
- Collection missions being tasked to nonprimary intelligence collectors; i.e., infantry battalions, combat engineers, and pilots.
- Emergency action planning, to include escape and evasion planning.
- Other tasks to be performed or supported by other MAGTF units; e.g., sensor inserts.
- Integrating collectors within landing and other movement plans.
- Coordination, deconfliction, and management of UAV operations with other MAGTF air operations.

Communications and Information Systems

Whether communications are analog or digital, voice or data, secure or nonsecure, there are hosts of technical details to be addressed in the planning stages to ensure collection activities succeed. Key CIS requirements and planning considerations to support MAGTF collection operations follow:

- Ensure that the MAGTF CE G-2/S-2, intelligence battalion, intelligence collection elements, and other MAGTF units are included in the distribution of intelligence-related address indicator groups to receive pertinent JTF, theater, and national intelligence and CI products.
- Determine and coordinate radio nets requirements, supporting frequencies, and operational procedures; e.g., external to MAGTF, internal MAGTF, intelligence broadcasts, retransmission sites, routine and time-sensitive operations.
- Coordination of CIS activation and restoration priorities and supporting procedures.
- Communications security material system requirements for unique collection-related communications and related security material.
- Determine and coordinate wire communications, including telephones.
- Establish, operate, and manage unique collection communications.
- Determine and coordinate local and wide area networks and unique intelligence networks information systems requirements; e.g., hardware, software, Internet protocol addresses.
- Integrate collection element CIS operations with those of other MAGTF and pertinent JTF and other components intelligence and reconnaissance units; e.g., mutual support, cueing.
- Communications integration of collection elements employed in general support (GS) with other MAGTF elements; e.g., to provide time-sensitive reporting, coordination of maneuver.
- Coordination of collection CIS and dissemination operations and procedures with allied and coalition forces.
- Manual dissemination procedures; e.g., courier must be established and practiced.

Combat Service Support Availability

Logistical considerations affecting collection operations include the following:

- Batteries and other power requirements.
- Transportation.
- Water.
- Food.
- Ammunition.
- Integration of collector's embarkation and load plans into those of the supported unit.

Employment of MAGTF Intelligence Units

MAGTF intelligence units are employed to meet the requirements of the entire force. The MAGTF G-2/S-2 develops a concept of intelligence support, which employs these units on the basis of the MAGTF mission, PIRs, concept of operations, and commander's intent. This concept must integrate intelligence activities with operations to provide key intelligence to commanders to enable rapid and effective decisionmaking. Based on the results of IPB analysis and the concept of operations, assets are positioned to—

- Satisfy PIRs.
- Expose enemy vulnerabilities.
- Monitor key locations.
- Detect and assist in the engagement of targets.
- Identify opportunities as they arise in the battlespace.

Intelligence units are employed in GS or DS. Under GS, units are tasked by the MAGTF commander through his G-2/S-2 to satisfy the requirements of the entire force. Because of the limited number of specialized intelligence assets and their ability to develop intelligence that is relevant to current and future operations in all areas of the battlespace (deep, close, and rear), GS is the preferred support relationship. Under DS, the requirements of a supported commander are given priority. DS is used to focus intelligence support for particular phases of an operation or create enhanced intelligence nodes to support MAGTF subordinate elements. When MAGTFs smaller than a full MEF are deployed, they will normally be supported by attached, task-organized detachments from the intelligence battalion, the force reconnaissance company, and the radio battalion.

Focused Intelligence Support

Intelligence must be integrated with the mission, commander's intent, and concept of operations and should normally be weighted to support the main effort. The MAGTF intelligence structure has the flexibility to tailor its capabilities to meet the requirements of various types of expeditionary operations, and adapt to changing operational needs during execution. For each operation, the MAGTF G-2/S-2 will assess IRs and develop a concept of intelligence support that positions assets where they can best satisfy those requirements. Intelligence nodes will focus support within the MAGTF. Split-basing will build intelligence nodes within and outside the AO to deliver comprehensive and reliable intelligence support while reducing the size of the deployed force. Intelligence units and DS teams are employed to tailor and enhance the capabilities of organic intelligence sections or to create task-organized intelligence nodes in response to specific requirements.

Task Organization of Intelligence Support Units

Task organization of intelligence support units is one of the principal means for the MAGTF commander to shape the intelligence effort. Collection, exploitation, and unique production capabilities of specialized intelligence units significantly enhance the ability of supported G-2/S-2 sections to develop timely, mission-focused intelligence. Intelligence battalion, force reconnaissance company, and radio battalion elements task-organize to provide tailored intelligence capabilities. Specific capabilities

provided are based on the threat, the supported unit's anticipated requirements (as determined through IPB), and the concept of operations.

Elements from some or all of the intelligence battalion's subordinate companies combine into intelligence battalion detachments. The CI/HUMINT company provides HUMINT exploitation teams (HETs). The radio battalion forms task-organized SIGINT support units (SSUs), which provide a mix of SIGINT and EW capabilities. When MAGTFs smaller than a full MEF deploy, an intelligence battalion detachment, a HET, force reconnaissance platoons, and a radio battalion SSU will normally be attached to the MAGTF CE. In MEF operations, when the entire radio battalion, intelligence battalion, and force reconnaissance company are employed, detachments, HETs, SSUs, and platoons may be placed in DS as required. Those subordinate units provide tailored intelligence capabilities to create an enhanced intelligence node to support an MSC or other MAGTF element.

Intelligence Direct Support Teams

Intelligence DS teams are organic to the intelligence battalion and each of the division, Marine aircraft wing (MAW), and force service support group G-2/S-2 sections. Teams are made up of one officer and several enlisted personnel who have a mix of intelligence specialty skills. DS teams provide an enhanced analytical and dissemination capability to a unit intelligence section and link the intelligence structure to the supported units. As assigned by the G-2/S-2, they augment the supported unit's intelligence section to carry out the following tasks:

- Perform analysis and production to support future operations.
- Tailor all-source fusion center and other external source intelligence products to the needs of the supported commander.
- Assist in the management of external intelligence support requirements.
- Facilitate dissemination of intelligence received from external sources.

The MEF and MSC G-2/S-2s use their DS teams to tailor and focus intelligence support to units designated as the main effort or to create enhanced intelligence nodes at key times and places in the battlespace. See MCWP 2-1.

Precrisis (Garrison/Peacetime) Intelligence Collection

The predominant collection focus during precrisis phases is obtaining basic or encyclopedic intelligence on the AO and current intelligence on the threat. In researching current or basic intelligence, intelligence analysts will consult various databases or online sources. National and theater resources are relied on heavily.

The Planning Phase

The planning phase is a critical phase where the foundation of intelligence preparation is set for the duration of the operation. There is an enormous demand for intelligence information and pressure to produce a high volume of intelligence in a very short time. The paradox is that although requirements will be very high, intelligence personnel are constrained by a lack of physical ability to collect before actual contact and a short time span to produce results. The lack of time is complicated by a need to prepare the intelligence collection section and units to conduct predeployment activities. Reliance on national and theater intelligence resources is still the predominant theme. The primary focus of collection is on basic or encyclopedic intelligence if this was not adequately done during the precrisis phase; otherwise the collection effort is

concentrated more on supporting current and estimative intelligence in support of operational planning. During planning, intelligence focuses on describing the battlespace through IPB and satisfying the commander's critical IRs and related PIRs. See MCWP 5-1, *Marine Corps Planning Process*.

Intelligence Collection During Execution

Intelligence collection during execution differs significantly from intelligence collection during planning.

Intelligence collection support during the precrisis or warning phases requires developing a large volume of basic intelligence and preparation of broad-scope estimates needed to develop and analyze COAs. However, *intelligence collection support during the execution phase must try to satisfy a much larger body of IRs in a significantly greater degree of detail*. For example, the nature of the intelligence required by a MAGTF commander to decide if a noncombatant evacuation operation is feasible differs radically from the type and detail of intelligence required by the mission commander who will execute the operation.

Another major difference is the time available to satisfy IRs. In the *execution phase there is a significant increase of time-sensitive IRs. Intelligence must often be developed in hours, minutes or even seconds*. Success often depends on the ability to provide immediate answers to critical questions regarding threat force dispositions and intentions.

Once the execution phase begins, the clash of opposing forces normally causes significant changes in the situation. *The changing nature of requirements accelerates*. Predicting enemy capabilities and intentions becomes increasingly difficult once the execution phase begins, but it is specifically during this period that the commander requires detailed and accurate intelligence to reduce uncertainty.

National and theater resources continue to be employed but a greater reliance may be placed on organic assets, particularly those in support of forward-deployed forces. Collection planning remains centralized but may be decentralized once a main effort is established and assets are attached to or placed to support the main effort.

The combined factors of the wide-ranging nature of IRs, the degree of detail required, the limited time available, and the uncertainty inherent during execution combine to make collection support to execution the most significant intelligence challenge. Collection managers must be prepared to meet this challenge and provide the flexibility required to deliver continuous situational awareness, identify opportunities, and facilitate rapid decisionmaking during execution.

Current Operations

The collection support effort during current operations consists primarily of answering previously developed intelligence reporting criteria and emerging requirements that arise as opposing forces clash. Coordination of ongoing and planned collection operations with other intelligence collectors and all current operation centers or battlefield agencies is emphasized. Factors critical to ensuring timely and effective dissemination are established and intelligence reporting criteria are widely disseminated. Each intelligence collector or the reporting unit; i.e., SARC or reconnaissance operations center, must be able to evaluate and assess the relevance of information to the ongoing operations. Each piece of collected data must undergo an immediate tactical processing and assessment before dissemination. A keen situational awareness and understanding of the unit's OPLAN/OPORD is required by all intelligence personnel, including collection managers and SARC personnel. Support must include intelligence collection to support deep and rear operations, resisting the natural tendency to focus on the close battle. Support to current operations

must be balanced against the requirement to support future operations. All assets cannot be devoted to current operations at the expense of supporting planning for future operations.

Future Operations

Intelligence collection support to future operations represents only a small portion of the collection effort, but merits discussion. Support is influenced by the timeframe and scope of the operation, level of command, identification of PIRs, and availability of collectors. One collection strategy discussed earlier endorsed "fencing of collection assets." One of the primary contributions of intelligence collection support to future operations is support to BDA that inputs to combat assessment, which in turn helps determine the nature of future operations. The collection operations officer's role is crucial. Continuous interaction by the collection operations officer and the intelligence plans officer in the future operations cell and the MAGTF P&A cell OIC is key to focusing intelligence collection efforts to support future operations. As decisions are made, ICRs and priorities for specific collection missions and tasks are generated and assessed against previously identified requirements.

APPENDIX A
SAMPLE INTELLIGENCE REQUIREMENTS WORKSHEET

MEF IR Number (1)	Requester IR Number (2)	DTG Received (3)	Subject (4)	Action (5)	Status (6)
04-1012	1st Marine Division Number 04-001	090830 Jan	Reconnaissance activity in NAI 32	SOR Numbers 04-1462 (UAV) 04-1463 (GSP) 04-1464 (Force Reconnaissance)	
04-1013	MEF Engineer	090900 Jan	Obstacle system at Objective SCHMIDT	For situation template	Closed 091630 Jan
04-1014	MEF G-2/P&A Cell	101100 Jan	Imagery of landing beaches	Forwarded to JTF J-2 for national collection	Pending

Column 1: The MEF IR number for ease of tracking.

Column 2: The originating requester IR number is posted to correlate subordinate requirements with the MAGTF. If the requirement is generated by the MAGTF CE, list that office. *Note: for requirements that are forwarded to higher headquarters, no notation is made.*

Column 3: When the information requirement is received.

Column 4: A succinct description indicating the information requirement subject.

Column 5: What SORs are germane to this requirement. *Note: one example identifies the collection system tasked to satisfy each SOR.*

Column 6: The information requirement is still active, pending or closed.

APPENDIX B
SAMPLE INTELLIGENCE COLLECTION WORKSHEET DESCRIPTION

Period Covered (From 21 Jan ____ to Seizure of Objective Schmidt)

Collection planning for a particular operation commences with the receipt or deduction of a mission by the commander and continues until the mission is accomplished. The collection worksheet covers the period from initiation of planning until accomplishment of the mission. However, in an amphibious operation, certain IRs may be directly related to various phases of the operation or must be satisfied as a prerequisite to other planning; e.g., IRs about location of suitable beaches or helicopter landing zones must be satisfied long before the actual assault. Therefore, the period entered at the top of the form may be less than that of the plan as a whole. The worksheet must be revised as IRs develop or no longer apply, as available collection agencies change in number and type, and as specific collection missions become obsolete. To accommodate the revisions, a collection worksheet should be maintained in loose leaf form.

Column 1, PIRs

Lists the IRs that must be satisfied. These include the PIRs and other IRs.

Column 2, Indicators

For each PIR and IR, the intelligence officer lists the indicators derived from an analysis of the enemy and the characteristics of the objective area or target indicator for each PIR/IR. Indications are positive or negative evidence. There usually is more than one indicator for each PIR/IR. When available, they will satisfy the particular requirement. Indications form the basis for developing SIRs and SORs for the collection of information.

Column 3, SIRs

Contains the specific information required; i.e., "the collectible info" that will substantiate or refute each indication listed in column 2.

Having determined what indications point to the solution of a particular IR, the intelligence officer next determines what information is needed to substantiate or refute each indication. For example, if removal of mines and obstacles is an indication of an enemy attack, then the SIR is if the enemy is actually removing mines and obstacles.

Reluctance of prisoners to remain in forward areas may be an indication of enemy preparations to employ nuclear weapons. The SIR is whether or not prisoners demonstrate any marked eagerness to be evacuated from the combat area.

Improvement of enemy positions may be an indication of defense. The SIR is if the enemy is actually improving his positions.

Information to be sought then becomes the basis for SORs for collection of information. A collection agency in most cases is not assigned full responsibility for establishing that any particular indication exists.

For example, increased patrolling may be an indication that an enemy is preparing to attack. A rifle company would not be asked if there was an increase in enemy patrol activity in its sector. Instead, the specific information to be sought that forms the basis for an order to the company would be to report the frequency of enemy patrols encountered in its sector.

Another indication of attack might be forward echeloning of artillery. The specific information to be sought by a collection agency is not if artillery is being echeloned forward but to report the location of artillery in certain forward areas.

In the above two examples, the intelligence officer is the one in the best position to make proper deductions. From the information he receives and after comparison with information already available, the intelligence officer can deduce if there has been an increase in enemy patrolling, and if the enemy artillery is being echeloned forward to support the attack.

The intelligence officer carefully studies the AO and the known enemy situation to focus the collection effort on a specific area; e.g., in developing specific information to be sought on possible enemy reinforcement, the intelligence officer studies the road nets and suitable avenues of approach to determine logical routes that enemy reinforcements would move. The specific information to be sought then becomes the volume and type of traffic along a particular road or in a particular area. The intelligence officer then has a basis for developing plans for aerial reconnaissance or establishing observation posts.

Column 4, Agencies to be Employed

List all currently available agencies. The list includes not only subordinate units but also higher and adjacent commands that gather information of value. In addition to troop units, the list of agencies includes intelligence specialists such as CI, imagery interpretation, and interrogation-translator personnel. The listing of troop units is not restricted to combat elements.

Following his determination of the specific information to be sought, the intelligence officer selects the collection agencies that will be tasked to furnish information. In making his selections, he is guided by considerations of capability, suitability, multiplicity, and balance.

Orders and RFIs are issued only to those agencies that are physically capable of providing it in time of use. The intelligence officer must be cognizant of the location, status, and current and projected missions of all available agencies.

Agencies selected to gather information are those best suited for the task; e.g., a trained force reconnaissance unit is normally better suited for amphibious reconnaissance than a patrol from a rifle company. An information collection mission is consistent with the tactical or logistics officer. Suitability also includes consideration of economy of force. Before an agency is selected for a particular task, the intelligence officer considers what other collection tasks the agency might accomplish simultaneously.

Information is evaluated and interpreted to derive intelligence. Accurate evaluation requires comparison of information obtained from several sources and agencies. Whenever possible, the intelligence officer selects more than one agency to collect information (redundancy).

Finally, the intelligence officer endeavors to balance the collection workload among available agencies. Although desirable, balance is the least important consideration in the selection of agencies, and more often, careful consideration of capabilities and suitability results in adequate distribution of the workload.

Column 5, Place and Time to Report

Reflects the place and time that information is to be reported. Information that arrives too late is of no value. The intelligence officer must effectively meet the needs of the commander, other staff officers, and higher, adjacent, and subordinate units.

- Be specific, especially for electronic reporting. When reporting via automated information and communications systems, a requester should be very specific; e.g., if an actual image

is requested, how should it be disseminated? Posted on a classified web page? Posted on an imagery dissemination server? If so, which one? If an electronic file transfer is desired, what is the Internet protocol address and circuit the requester uses? Any special report formatting requirements should be included if a nonstandard product is requested.

- One-time versus periodic reporting. For reconnaissance missions, one-time reporting may be sufficient. For surveillance missions, periodic reporting is usually required. Requirements supporting target or area surveillance should have details on how frequently reports are to be generated.
- Include LTIOV. The LTIOV is an appropriate entry in the reporting column. Entries may specify an exact time for reporting and/or not-later-than times for periodic reports (or at such times that information is obtained). Negative reports, if desired, are also indicated.
- Routine vs time-sensitive. Clearly identify criteria and reporting channels for routine and time-sensitive reports.

Column 6, Remarks

Miscellaneous remarks on the progress of the collection are recorded in column 6 of the worksheet. The intelligence officer develops a simple code to indicate PIRs/IRs that require revision or cancellation. Prompt cancellation of orders and requests for collection of information, including PIRs, is mandatory if the efforts of collection agencies are to be focused properly. A unit SOP for intelligence functioning normally provides for routine reporting of certain types of information. A note is made in the collection worksheet when certain information requirements are covered by the SOPs; e.g., the reporting of minefields may be prescribed by the unit SOP. A requirement for information on the enemy's use of mines can be handled by placing "SOP" in column 6, and responsibility need not be indicated under agencies. However, a requirement for reporting the location of minefields in the vicinity of a specific area is not treated as an SOP item. Finally, the intelligence officer notes those specific information requirements that can be combined into a single order of request to an agency.

PIRs	Indicators	SIRs	Agencies to be Employed									Place and Time to Report	Remarks
			DIV	MAW	FSSG	CI/HUMINT	VMU	RadBn	VMAQ	ForceRecon	GSP		
Will the 3d Tank Division enter NAI 8 or 9 on the evening of 22 January?	Dispersal of tanks and self-propelled artillery to forward positions.	Will more than 220 combat vehicles of 3d Tank Division pass through NAI 8 or 9 between 221600 and 230400 January? Will more than 38 artillery weapons subordinate to 3d Tank Division enter NAI 8 or 9 between 221600 and 230400 January?	X	X	X	X	X			X	X	Report by fastest means to MEF G-2 LTIOV: 230400 January	
	Increased communications by 3d Tank Division elements.	Are enemy tactical radios active in NAI 8 or 9 before 230400 January?	X	X	X			X	X			Report by fastest means to MEF G-2 LTIOV: 230400 January	

Figure B-1. Sample Intelligence Collection Worksheet.

APPENDIX C
SAMPLE INTELLIGENCE COLLECTION PLAN

CLASSIFICATION

Copy no.___ of___ copies
Headquarters, (MAGTF)
PLACE OF ISSUE
Date/time group
Message reference number

TAB A (Intelligence Collection Plan) TO APPENDIX 10 (Intelligence OPLAN) TO ANNEX B (Intelligence) TO OPLAN

(U) REFERENCES:

(a) Theater TTP
(b) MEF Tactical SOP
(c) MCWP 2-1

1. (U) Situation. Remaining Orange Force is defending against the Blue Force's advance to prevent the destruction of the ruling regime in the capital city of Orangeville. They intend to delay and attrite Blue Force to such an extent that US resolve to continue the war will fail, allowing the Orange regime to survive through diplomatic means.

(a) (U) See FRAGO.
(b) (U) Enemy situation.
(c) (U) Most dangerous COA.
(d) (U) Most likely COA.

2. (U) Mission. To provide R&S of MEF battlespace to support Blue Force attacks in zone, confirm conditions for amphibious landing, and determine status of Orange Force's location.

3. (U) Execution

a. (U) National and theater collection will be requested to support MEF deep IRs (beyond forward boundary/deep battle synchronization line), threats to MEF flanks and logistic support bases, and against threats within MEF's boundaries beyond organic collection capabilities. Of particular in-

CLASSIFICATION

terest are enemy strategic and operational reserve forces that could influence MEF advance, and indications of Orange Force use of weapons of mass destruction.

(1) (U) In accordance with references (a) and (b), and as the Blue Force supporting effort during this operation, MEF battlespace R&S will rely heavily on organic aviation and battlefield surveillance/collection assets to satisfy IRs to support the close and deep fight.

(2) (U) Due to the location of the ground component commander to the flank and rear, and the commander, amphibious task force (CATF)/commander, landing force (CLF) relationship to execute an amphibious landing, MEF will request lateral intelligence reporting from the ground and naval component commanders. Lateral ground component commander intelligence reporting to MEF will facilitate cross-boundry operations and rear area operations/support requirements. Lateral naval component commanders intelligence reporting will support the movement of MEF's operating in littoral areas, and assist in determining enemy activity within the battlespace.

(3) (U) Upon chop of the CLF to MEF, selected R&S assets DS of CATF will become operational control to the MEF G-2.

(4) (U) Organic Focus. All organic R&S assets will focus on satisfying MEF PIRs/IRs. Ground-based SIGINT collection will focus on indications and warning force protection reporting to the supported commander. Forward CI and HUMINT assets will provide the supported commander with tactical interrogations and refugee debriefs; rear area CI assets will provide CI force protection source operations. MEF ground R&S operations will provide continuous observation and operate in vicinity of MEF NAIs and targeted areas of interest as directed. Visual aerial reconnaissance will provide timely battlespace awareness within the MEF AO, and support time-sensitive and ad hoc emerging IRs utilizing in-flight and post mission reporting. Ground sensor operations will be focused along major lines of communications (LOCs) and boundaries within and along the MEF area of responsibility. Organic MEF UAVs will be flown in GS of MEF operating forces. All collection disciplines will support personnel recovery operations as required.

b. (U) Concept Of Operations

(1) (U) The MEF R&S Plan will be divided in the following three stages:

- Stage A: Prechop of landing force.
- Stage B: Postchop of landing force.
- Stage C: Seizure of Orangeville.

CLASSIFICATION

(2) (U) Stage A: Prechop of Landing Force. During Stage A, R&S focus will be—

- Protection of our MEF units.
- Intentions of enemy forces able to influence MEF flanks, the amphibious landing zone or moving into adjacent units.
- Determining if conditions are met for MEF to assume operational control of landing force.
- Disposition of Orange Force's operational reserve forces that could move to impede MEF's movement.
- Status of LOCs.
- Disposition of enemy forces in the vicinity of Orangeville.

(3) (U) Stage B: Postchop of Landing Force. During Stage B, R&S focus will be—

- Disposition of Orange Force's operational reserves that could impede the MEF's movement or move into an adjacent unit's zone.
- Orange Force's operational reserves that could attack MEF's flanks.
- Status of LOCs from Badguyburg to Orangeville.
- Threats to MEF's rear area.
- Potential areas for interdiction west of Orangeville.

(4) (U) Stage C: Seizure of Orangeville. During Stage C, R&S focus will be—

- Disposition of enemy forces in the vicinity Orangeville.
- Enemy forces that can influence LOCs.
- Identification of enemy units able to attack Blue Force's flanks.
- Threats to Blue Force rear area.
- Potential areas for interdiction west of Orangeville.
- Suspected movement of Orange Force.

(5) (U) Concept for SIGINT Collection. MEF organic ground-based SIGINT collection assets are in GS of MEF and DS of the supported commander. Theater and national SIGINT collection will be requested as required.

(a) (U) Communications Intelligence. MEF organic ground-based communications intelligence collection will focus on indications, warning reporting, and force protection to the supported commander. Collection emphasis will be—

- Range Force's corps and C2 divisions.
- Artillery fire direction nets.
- Success of Blue Force's deception plan as to actual location of amphibious landing site.

CLASSIFICATION

(b) (U) Electronic Intelligence. Blue Force electronic intelligence surveillance support will focus on indications and warning reporting and force protection of Blue Force. Collection emphasis will be—

- PIR support.
- Locating remaining radar guided air defense weapons.
- Indications of possible air attacks within MEF AO.
- Indications of possible employment of weapons of mass destruction.

(6) (U) Concept for CI/HUMINT Collection. Forward CI/HUMINT assets will focus on—

- Force protection.
- Assisting in Blue Force deception plan as to actual location of amphibious landing site.
- Assisting in Blue Force deception plan to convince Orange Force national-level commanders that MEF is the Blue Force main effort.
- Conducting tactical interrogations to support the commander's PIRs/IRs. Rear area CI assets will provide CI force protection source operations. Postchop, selected CATF assets will become operational control to MEF and report and receive tasking from the MEF G-2.

(7) (U) Concept for Ground R&S Collection. MEF ground R&S operations will be conducted with—

- MSC ground reconnaissance assets having collection responsibility from forward line of troops to other phase lines in effect.
- MEF force reconnaissance assets (force reconnaissance companies and radio battalion radio reconnaissance teams) having collection responsibility from fire support coordination line to forward boundary/deep battle synchronization line.
- DS unconventional warfare forces having collection responsibility beyond the forward boundary/deep battle synchronization line. Cross-boundary ground R&S operations will be conducted by MEF vice MSC ground R&S assets. Postchop, selected CATF ground R&S assets will become operational control to MEF, and report and receive tasking from the Blue Force G-2.

(8) (U) Concept for Aerial Visual R&S Collection. MEF aerial visual R&S collection will center on the aviation assets of the MAW. Because of the dynamic reporting capability of aircraft operating within the Blue Force battlespace, aerial visual R&S will provide timely battlespace awareness, and support time-sensitive

CLASSIFICATION

and adhoc emerging IRs utilizing in-flight and post mission reporting. Time-critical ad hoc IRs will be forwarded to the tactical aircraft command center via the MEF air officer. When directed, positive and negative reporting is required in specific collection requirements or emphasis.

(9) (U) Concept for Ground Sensor Collection. MEF will provide GSP squads to ground maneuver commands in DS to facilitate close battle operations. GSP assets retained by the MEF collection management and dissemination officer will be focused along major LOCs and command boundaries within and along the MEF area of responsibility. Postchop, selected CATF ground sensor assets will become operational control to MEF, and report and receive tasking from the MEF G-2.

(10) (U) Concept for UAV Collection. Organic MEF UAV will be flown in DS and GS of MEF maneuver forces. Remote receive stations will be collocated with maneuver forces to allow rapid transfer of time-critical information. The aviation combat element commander will recommend possible forward base locations for future operations.

(11) (U) Concept for Aerial Imagery Collection. Requests for national and theater imagery collection will be forwarded to higher headquarters for satisfaction. Aerial imagery collection will support recurring IRs along LOCs or against point targets.

c. (U) Tasks

(1) (U) GCEs

(a) (U) 1st Marine Division (MARDIV)

1 (U) Conduct organic R&S operations in zone to the intelligence handover line in effect.

2 (U) Debrief all organic R&S teams providing intelligence reports to MEF G-2 operations within 6 hours.

3 (U) Receive and incorporate one squad from the GSP in DS for R&S operations. Implanting of sensors is the responsibility of supported unit.

4 (U) Assist in recovery of MEF and unconventional warfare R&S assets in zone.

5 (U) Evacuate captured personnel and materiel from the forward collection point to the central collection point by most expeditious means possible. Enforce tagging procedures in accordance with reference (b). Interrogations will only be conducted by MEF HUMINT personnel.

CLASSIFICATION

6 (U) Receive and incorporate one company (1st/2d) Radio Battalion (-) (Reinforced) in DS.

7 (U) Receive remote receive station team from Marine unmanned aerial vehicle squadron (VMU)-1.

8 (U) Receive CI/HUMINT elements in GS.

(b) (U) 2d MARDIV

1 (U) Conduct organic R&S operations in zone to the intelligence handover line in effect.

2 (U) Debrief all organic R&S teams providing summary reports to MEF G-2 operations within 6 hours.

3 (U) Assist in recovery of MEF and unconventional warfare R&S assets in zone.

4 (U) Evacuate captured personnel and materiel from the forward collection point to the central collection point by most expeditious means possible. Enforce tagging procedures in accordance with reference (b). Interrogations will only be conducted by Blue Force HUMINT personnel.

5 (U) Receive remote receive station team from VMU-1.

6 (U) Receive and incorporate one squad from the ground sensor platoon in GS for R&S operations. Implanting of sensors is the responsibility of supported unit.

(c) (U) 3d MARDIV (Stages B and C)

1 (U) Maintain DS R&S units until notified otherwise by this HQ.

2 (U) Conduct organic R&S operations in zone as directed.

3 (U) Debrief all organic R&S teams providing intelligence reports to the MEF G-2 operations within 6 hours.

4 (U) Assist in recovery of MEF and unconventional warfare R&S assets in zone.

5 (U) Evacuate captured personnel and materiel from the forward collection point to the central collection point by most expeditious means possible. Enforce tagging procedures in accordance with reference (b). Interrogations will only be conducted by MEF HUMINT personnel.

6 (U) Receive remote receive station team from VMU-1.

CLASSIFICATION

(d) (U) 4th MARDIV (Stages B and C)

1 (U) Conduct organic R&S operations in zone to established phase lines in effect.

2 (U) Debrief all organic R&S teams providing summary reports to MEF G-2 operations within 6 hours.

3 (U) Assist in recovery of MEF and unconventional warfare forces R&S assets in zone.

4 (U) Evacuate captured personnel and materiel from the forward collection point to the central collection point most expeditious means possible. Enforce tagging procedures in accordance with reference (b). Interrogations will only be conducted by MEF HUMINT personnel.

5 (U) Receive remote receive station team from VMU-1.

(2) (U) MAW

(a) (U) Provide timely intelligence reports as required to MEF G-2 operations officer.

(b) (U) Use strike camera to greatest extent possible to support first phase BDA.

(c) (U) Conduct UAV operations from Texaco forward arming and refueling point until a forward site for control can safely be established and maintained.

(d) (U) Provide two man operation planning/liaison team (UAV detachment) to MEF SARC.

(e) (U) Provide emergency extract package of ground R&S units as required.

(f) (U) Receive a CI element in GS.

(g) (U) Conduct preplanned and ad hoc visual aerial reconnaissance.

(h) (U) Provide remote receive station team to MEF CE.

(i) (U) Provide remote receive station team to 1st MARDIV.

(j) (U) Provide remote receive station team to 2d MARDIV.

(k) (U) Provide remote receive station team to 3d MARDIV.

(l) (U) Provide remote receive station team to 4th MARDIV.

CLASSIFICATION

(m) (U) Provide two-man UAV liaison teams to MEF SARC.

(n) (U) Conduct UAV displacement operations with minimal reduction of battlespace surveillance.

(o) (U) Receive ground sensor platoon liaison team to support airborne sensor implant planning.

(p) (U) Conduct airborne sensor implant when directed.

(3) (U) FSSG (-)(Reinforced)

(a) (U) Provide intelligence reporting of any enemy activity within AO to MEF G-2 operations officer.

(b) (U) Provide bridge, route, ford, and other mobility reports in accordance with reference (c) for all main/critical routes to MEF G-2 P&A cell.

(c) (U) Receive a CI element in GS.

(d) (U) Conduct ground sensor recovery operations when directed.

(4) (U) Rear Area Operations Group

(a) (U) Provide R&S reporting from adjacent headquarters/units to MEF G-2 operations officer as soon as feasible.

(b) (U) Evacuate captured personnel and materiel from the forward collection point to the central collection point by most expeditious means possible. Enforce tagging procedures in accordance with reference (b). Interrogations will only be conducted by MEF HUMINT personnel.

(c) (U) Receive a CI element in GS.

(d) (U) Conduct ground sensor recovery operations when directed.

(5) (U) Marine Engineer Group

(a) (U) Provide bridge, route, ford, and other mobility reports in accordance with reference (c) for all main/critical routes to MEF G-2 P&A cell.

(b) (U) Evacuate captured personnel and materiel from the forward collection point to the central collection point by most expeditious means possible. Enforce tagging procedures in accordance with reference (b). Interrogations will only be conducted by MEF HUMINT.

CLASSIFICATION

(6) (U) Force Artillery Headquarters

(a) (U) Provide counterfire battery radar reports to MEF SARC OIC as soon as possible.

(b) (U) Evacuate captured personnel and materiel from the forward collection point to the central collection point by most expeditious means possible. Enforce tagging procedures in accordance with reference (b). Interrogations will only be conducted by MEF HUMINT personnel.

(7) (U) MEF Organic Collection Elements

(a) (U) Force Reconnaissance Company (-) (Reinforced)

1 (U) Implant ground sensor strings and relays as directed.

2 (U) Provide two-man operational planning liaison team (force reconnaissance detachment) to MEF SARC.

3 (U) Conduct simultaneous operations to support MEF Alpha and Bravo command post displacement.

4 (U) Provide restricted fire area coordination and deconfliction of all ground R&S assets within MEF AO.

5 (U) Provide strategic and theater ground reconnaissance planning support as required.

6 (U) Assume operational control of selected CATF ground R&S assets postchop.

7 (U) Engage targets of opportunity with MEF force fires authorization.

8 (U) Provide targeting for fire support systems.

(b) (U) Intelligence Battalion. Provide the following R&S support:

1 (U) GSP (-) (Reinforced)

a (U) Provide one GSP squad in DS of 1st MARDIV.

b (U) Provide one GSP squad in GS of 2d MARDIV.

c (U) Provide two-man operational planning liaison team (GSP detachment) to the MEF SARC.

d (U) (U) Be prepared to conduct simultaneous operations to support MEF Alpha and Bravo command post displacement.

CLASSIFICATION

e (U) Provide GSP liaison team to MAW for airborne sensor implant planning.

f (U) Assume operational control of selected CATF ground sensor assets postchop.

2 (U) CI/HUMINT Unit

a (U) Conduct CI/force protection operations in MEF AO.

b (U) Conduct HUMINT operations supporting R&S plan.

c (U) Conduct tactical interrogations to support MEF PIRs/IRs.

(c) (U) Radio Battalion (-)(Reinforced)

1 (U) Provide one company (1st/2d) Radio Battalion (-)(Reinforced) in DS of 1stMARDIV.

2 (U) Provide a SIGINT support platoon in GS to 2dMARDIV.

3 (U) Radio reconnaissance teams will be in DS of MEF.

4 (U) Coordinate operational planning for insertion/extraction of radio reconnaissance teams with force reconnaissance company.

5 (U) Provide two-man operational planning liaison team (radio battalion detachment) to the MEF SARC.

6 (U) Conduct simultaneous operations to support MEF Alpha and Bravo command post displacement.

7 (U) Provide electronic intelligence support for battlespace surveillance in accordance with internal SOPs.

d. (U) Coordinating Instructions

(1) (U) Assignment of Responsibility for Drafting of Tabs to this appendix. The MEF CM/DO will conduct a working group comprised of MSC collection requirement managers and MEF collection operation managers to discuss this appendix and to identify and assign initial responsibilities to execute this R&S plan. On completion of the working group, each command or unit responsible for the development of a supporting tab that addresses the operations management of the specific collector will draft and forward this tab to the MEF CM/DO for review and dissemination. When applicable, tabs should address the tasking, processing, exploitation, and dissemination of collected information from the collector to the MEF G-2. Command/unit responsibility for specific tabs are:

CLASSIFICATION

(a) (U) Tab A: SIGINT Employment Plan. MEF SIGINT officer coordinated with radio battalion.

(b) (U) Tab B: CI/HUMINT Employment Plan. MEF CI/HUMINT coordinated with intelligence battalion.

(c) (U) Tab C: Ground R&S Plan. Force Reconnaissance Company coordinated with MEF SIGINT officer.

(d) (U) Tab D: Visual Aerial Reconnaissance and Surveillance Plan. MAW.

(e) (U) Tab E: Ground Sensor Surveillance Plan. Intelligence battalion.

(f) (U) Tab F: UAV Employment Plan. MAW.

(2) (U) PIRs

(a) (U) Determine if the 7th Division will attack the MEF flank from H-Hour to H+24.

(b) (U) Determine if the 1st Armored Brigade will displace to counter amphibious landing from H-Hour To H+36.

(c) (U) Determine if the 1st Provincial Guard Corps will defend in the vicinity of Badguyburg in regiment or larger strength from H+36 To H+96.

(d) (U) As soon as practical, MSCs will identify PIRs and submit requests for collection support in accordance with this appendix.

(3) (U) IRs

(a) (U) Determine the movement of major Orange Force's units in MEF's area of responsibility.

(b) (U) Location of Orange Force's long-range artillery that can range MEF forces.

(c) (U) Projected weather conditions.

(d) (U) Any other changes to the assessed enemy COAs.

(4) (U) NAIs. (Read across Number/Location/Description/Activity)

(a) (U) 1/Grid location/southwest movement from Nashville by 1st Armored Brigade.

CLASSIFICATION

(b) (U) 2/Grid location/road junction Route 20/movement west of 1st Armored Brigade.

(c) (U) 3/Grid location/road junction I-95 and north/south Country Road/ movement west of 7th Division.

(d) (U) 4/Grid location/road/movement south of 1st Armored Brigade.

(e) (U) 5/Grid Location/Intersection Route 1 and Bangor Road/enemy movement southwest or southeast from Badguyburg.

(f) (U) 6/Grid location/Intersection Route 1 and Highway 101/east movement of 1st Provincial Guard Corps.

(g) (U) 7/Grid location /road junction Route 66 and unidentified road/southeast movement of 1st Provincial Guard Corps.

(5) (U) MEF CM/DO will coordinate and deconflict with higher headquarters MEF NAIs that correspond to or have been identified as a combatant commander's NAI. The MEF CM/DO will also coordinate and deconflict MEF NAIs.

(6) (U) MEF subordinate commands will prepare organic R&S plans to satisfy organic PIRs/IRs. MEF MSCs will submit organic R&S plans to the MEF CM/DO as directed.

4. (U) Logistics

5. (U) Command And Communications

a. (U) Command

(1) (U) Command Relationships

(a) (U) J-2 has staff responsibility for employment of theater and national intelligence collection assets.

(b) (U) MEF G-2 CM/DO is responsible for coordinating the employment of MEF organic R&S assets and requesting R&S support through appropriate channels to cover gaps in organic collection capability to support combatant commander and MEF PIRs.

(c) (U) The MEF SARC is responsible for:

1 (U) Initial planning and coordination for the operational employment of MEF organic collection assets to support this operations plan.

CLASSIFICATION

2 (U) Monitoring and reporting the status and location of MEF organic collection assets

3 (U) Collecting and reporting combat intelligence/information to the MEF P&A cell.

(d) (U) The MEF SARC OIC will assist the MEF CM/DO in developing, publishing, and revising this appendix as required.

b. (U) Communications. MSC R&S assets will establish communications connectivity between tasked organic units and the MEF SARC via G-2 unclassified or secret networks.

c. (U) Reporting. Timely reporting from organic collection operation centers via established communications paths and procedures will support reactive targeting opportunities and analysis of perishable tactical information.

d. (U) Requesting Procedures. Requests for intelligence support beyond the capabilities of MSCs will be submitted as a production requirement/collection requirement via the chain of command to MEF using the procedures outlined in reference (b).

APPENDIX D
SAMPLE COLLECTION STATUS UPDATE PARAGRAPH FORMAT

Collection Status Update Paragraph. A collection status update paragraph may be included as part of a unit's daily intelligence summary (INTSUM) in order to notify higher, adjacent, and critically, lower units of the MAGTF's current ICRs and planned collection operations over some specified future period. As a snapshot of the near term requirements, it can be used to review active and cancelled requirements and update a unit's collection priorities and collection plan daily. Using the basic format, units can tailor the INTSUM to fit the situation. With new automated information systems, INTSUMs are increasingly produced in graphic form and posted on networks for wide dissemination, with links to detailed supporting intelligence products, reports, and databases. An example of a written collection status update paragraph follows:

COLLECTION STATUS UPDATE

A. DURING THE PERIOD 040800T TO 050759T MAR 2004, THE MEF COLLECTION PRIORITIES ARE AS FOLLOWS:

PRIORITY	PIR/IR NO.	ITEM
1	1	SIGINT SUPPORT TEAM (SST) A TO EXECUTE MISSION BRAVO VIC NAI 003.
2	1	AVIATION SST UNIT TO EXECUTE MISSION CHARLIE VIC NAI 003.
3	1	AERIAL RECON MISSIONS TO PROVIDE COVERAGE OF I MEF AO ACCORDING TO AERIAL SURV PLAN (TRACKS NASHVILLE AND DAYTONA) IN MOBILITY CORRIDOR CHARLIE.
4	2	SST TEAM C TO EXECUTE MISSION ECHO VIC NAI 005.

B. CANCELLED REQUIREMENTS. THE FOLLOWING PRIORITY INTELLIGENCE REQUIREMENTS HAVE BEEN SATISFIED OR CANCELLED.

PIR NO.	DESCRIPTION
5	IMAGERY AND TEXT STUDIES OF POINT OF ENTRY VIC PORT HIDALGO. SPECIAL ATTENTION TO COASTAL LANDING BEACHES AND HELICOPTER LANDING ZONES.

C. PLANNED INTELLIGENCE COLLECTION MISSIONS. THE FOLLOWING MEF INTELLIGENCE COLLECTION MISSIONS ARE PLANNED FOR EXECUTION DURING THE PERIOD 050800T TO 060759T MAR 2004.

PRIORITY	PIR/IR NO.	ITEM
1	2	EA-6B/PROWLER UNIT A TO COLLECT IAW TASKING PER AIR TASKING ORDER.
2	3	HELO INSERTION OF GROUND RECON TEAM 111 INTO RESTRICTED AREA OF OPERATIONS 111 VIC NAI 006.
3	3	3RD GSP TO CONDUCT SENSOR EMPLACEMENT OPERATIONS IN MOBILITY CORRIDOR MESA.

APPENDIX E
SAMPLE COLLECTION EMPHASIS MESSAGE

FM CG I MEF//G2//CMDO//

TO CG FIRST MARDIV//G2/CM//

CG FIRST FSSG//G2/CM//

CG THIRD MAW//G2/CM//

INFO CG II MEF//G2/CM//

CG III MEF//G2/CM

CJTF BLUE

UNCLAS N03800//

EXERCISE EXERCISE EXERCISE

MSGID/CEM/I MEF G2/001//

SUBJ/COLLECTION EMPHASIS MESSAGE//

REF/A/DOC/I MEF EXERCISE OPORD 04

REF/B/MAP/NIMA/-//

NARR/REF A IS I MEF OPORD FOR EXERCISE 04. APP 1, ANNEX B, CONTAINS MEF PIRS FOR EXERCISE. REF B ARE MAPS FOR EXERCISE AREAS; SERIES, SHEETS, EDITION AND SCALE//

POC/BOSS, I.M./MAJ/USMC/CMDO/DSN 492-0283//

RMKS/1. (U) AS DISSEMINATED IN REF A, THE FOLLOWING PIRS ARE THE FOCUS OF I MEF G2 INTELLIGENCE COLLECTION STRATEGY DURING PHASE ONE OF THE EXERCISE. REQUEST WIDEST DISSEMINATION OF THESE PIRS TO ALL SUBORDINATE UNITS.

2. (U) PIR 1. WILL 3D ARMOR DIV CROSS LINE OF DEPARTURE PRIOR TO I MEF AMPHIB ASSLT ON D PLUS FOUR.

A. SIGINT. REPORT INCREASE IN ENEMY COMMS BTWN 3D ARMOR DIV UNITS. SPECIFIC ATTN TO COMMS BTWN HQ, 3D ARMOR DIV AND HQ, 4TH CORPS. PROVIDE INDICATIONS AND WARNING OF ENEMY APPROACH VIC NAIS 001, 002.

B. IMINT. PROVIDE COVERAGE OF I MEF AO ACCORDING TO PRIORITIZED IMAGERY TARGET LIST.

C. GROUND RECON. REPORT ENEMY ACTIVITY IN VIC NAIS 001, 002. REPORT LOCATION, NUMBER, HEADING AND SPEED OF VEHICLES.

D. AERIAL RECON. PROVIDE COVERAGE OF I MEF AO ACCORDING TO AERIAL SURV PLAN (TRACKS NASHVILLE AND LINCOLN) IN MOBILITY CORRIDORS LAVA AND DELTA. REPORT LOCATION, NUMBER, HEADING, AND SPEED OF VEHICLES.

E. HUMINT. REPORT INDICATIONS OF 3D ARMOR DIV PLANS TO DEPLOY.

F. CI. REPORT INDICATIONS OF ENEMY ACTIVITY IN I MEF AO. SPECIFIC ATTN TO BEACH SUPPORT AREA (NAI 004).

G. MASINT. CONDUCT SENSOR MONITORING AND REPORTING TO PROVIDE I&W OF ENEMY ACTIVITY IN MOBILITY CORRIDORS LAVA AND DELTA. REPORT ENEMY ACTIVITY. DETERMINE NUMBER, TYPE, HEADING, AND SPEED OF VEHICLES.

3. (U) PIR 2. WILL 4TH CORPS RESERVE DEPLOY TO ASSEMBLY AREA (AA) MULE PRIOR TO D PLUS FOUR.

A. SIGINT. REPORT INCREASE IN ENEMY COMMS BY AND BTWN 11 MECH INF BDE. SPECIFIC ATTN TO COMMS BTWN HQ, 11 MECH INF BDE AND HQ, 4TH CORPS. PROVIDE I&W OF ENEMY APPROACH VIC NAIS 006, 007.

B. IMINT. PROVIDE COVERAGE OF I MEF AO ACCORDING TO PRIORITIZED IMAGERY LIST.

C. GROUND RECON. REPORT ENEMY ACTIVITY IN VIC NAIS 006, 007. REPORT LOCATION, NUMBER, HEADING, AND SPEED OF VEHICLES.

D. AERIAL RECON. PROVIDE COVERAGE OF I MEF AO ACCORDING TO AERIAL SURV PLAN (TRACKS KNOXVILLE AND OMAHA) IN MOBILITY CORRIDOR MAIN. REPORT LOCATION, NUMBER, HEADING, AND SPEED OF VEHICLES.

E. HUMINT. REPORT INDICATIONS OF 11TH MECH INF BDE PLANS TO DEPLOY TO AA MULE.

F. CI.

G. MASINT. CONDUCT SENSOR MONITORING AND REPORTING TO PROVIDE I&W OF ENEMY ACTIVITY IN MOBILITY CORRIDOR MAIN. REPORT ENEMY ACTIVITY. DETERMINE NUMBER, TYPE, HEADING, AND SPEED OF VEHICLES.

4. (U) PIR 3. WILL 4TH CORPS EMPLOY NUCLEAR, BIOLOGICAL OR CHEMICAL (NBC) WEAPONS IN THE VICINITY OF THE LANDING BEACHES DURING I MEF AMPHIB ASSLT.

A. SIGINT. REPORT INDICATIONS OF ENEMY USE OR EMPLOYMENT OF NBC WEAPONS. SPECIFIC ATTN TO HQ, 4TH CORPS COMMS. PROVIDE I&W OF NBC EMPLOYMENT VIC NAI 004.

B. IMINT.

C. GROUND RECON. REPORT INDICATIONS THAT ENEMY IS PREPARING TO EMPLOY NBC WEAPONS WITHIN MEF AO. SPECIFIC ATTN TO ENEMY GROUND FORCE UNITS ISSUING NBC PROTECTIVE GEAR.

D. AERIAL RECON.

E. HUMINT. REPORT INDICATIONS THAT ENEMY IS PREPARING TO EMPLOY NBC WEAPONS WITHIN MEF AO. SPECIFIC ATTN TO CIVIL MEASURES OR PREPARATIONS FOR NBC EMPLOYMENT.

F. CI. REPORT INDICATIONS THAT ENEMY IS PREPARING TO EMPLOY NBC WEAPONS WITHIN MEF AO. SPECIFIC ATTN TO CIVIL MEASURES OR PREPARATIONS FOR NBC EMPLOYMENT.

G. MASINT.

5. (U) PLANNED INTELLIGENCE COLLECTION MISSIONS FOR THE PERIOD 040800T TO 060759T MAR 04 ARE AS FOLLOWS (REFERENCE MEF COLLECTION PLAN ON THE MEF S-TDN WEB SITE.)

A. SIGINT. SST TEAM A TO EXECUTE MISSION BRAVO VIC NAI 003. AVIATION SST UNIT C TO EXECUTE MISSION CHARLIE VIC NAI 003.

EA-6B/PROWLER UNIT A TO COLLECT AGAINST PIR #2 (TASKING PER ITO/ATO).

B. IMINT.

C. GROUND RECON. HELO INSERTION OF TEAM 111 INTO RAO 111 VIC NAI 006.

D. AERIAL RECON. PROVIDE COVERAGE OF I MEF AO ACCORDING TO AERIAL SURV PLAN (TRACKS NASHVILLE AND DAYTONA) IN MOBILITY CORRIDOR CHARLIE.

E. HUMINT.

F. CI.

G. MASINT. 3D GSP TO CONDUCT SENSOR EMPLACEMENT OPERATIONS INMOBILITY CORRIDOR MESA.

6. (U) UPDATES TO THE COLLECTION STRATEGY WILL BE DISSEMINATED IN COLLECTION STATUS UPDATE PARAGRAPH OF MEF INTSUMS, ON-LINE VIA MEF GRAPHICAL COLLECTION PLAN ON THE MEF S-TDN WEB SITE, AND IN FUTURE COLLECTION EMPHASIS MESSAGES.

BT

#0001

NNNN

APPENDIX F
GLOSSARY

SECTION I
ACRONYMS AND ABBREVIATIONS

AO . . . . . area of operations
ATARS . . . . . advanced tactical airborne reconnaissance system

BDA . . . . . battle damage assessment

C2 . . . . . command and control
CATF . . . . . commander, amphibious task force
CE . . . . . command element
CI . . . . . counterintelligence
CIS . . . communications and information systems
CLF . . . . . commander, landing force
CM/DO . . . . . collection management/ dissemination officer
COA . . . . . course of action
COM . . . . . collection operations management
COMINT . . . . . communications intelligence
COP . . . . . common operational picture
CRM . . . . . collection requirements management
CTP . . . . . common tactical picture

DIAM . . . . Defense Intelligence Agency Manual
DODIPP . . . Department of Defense Intelligence Production Program
DS . . . . . direct support

ELINT . . . . . electronic intelligence
EW . . . . . electronic warfare

FRAGO . . . . . fragmentary order
FSSG . . . . . force service support group

G-2 . . . . . intelligence staff officer (brigade or higher)
G-3 . . . . . operations staff officer
G-5 . . . . . plans staff officer
GIRH . . . . . generic intelligence requirements handbook
GS . . . . . general support
GSP . . . . . ground sensor platoon

HET . . . . . HUMINT exploitation team
HUMINT . . . . . human intelligence

ICR . . . . . intelligence collection requirement
IDR . . . . . intelligence dissemination requirement
IMINT . . . . . imagery intelligence
INTSUM . . . . . intelligence summary
IOC . . . . . intelligence operations center
IPB . . . intelligence preparation of the battlespace
IPR . . . . . intelligence production requirement
IR . . . . . intelligence requirement
ISC . . . . . intelligence support coordinator

J-2 . . . . . intelligence directorate of a joint staff
JP . . . . . joint publication
JSTARS . . . . . joint surveillance target attack radar system
JTF . . . . . joint task force

LOC . . . . . line of communications
LTIOV . . . . . latest time intelligence is of value

MAGTF . . . . . Marine air-ground task force
MARDIV . . . . . Marine division
MASINT . . . . . measurement and signature intelligence
MAW . . . . . Marine aircraft wing
MCDP . . . . . Marine Corps doctrinal publication
MCIA . . . . . Marine Corps Intelligence Activity
MCRP . . . . . Marine Corps reference publication
MCWP . . . Marine Corps warfighting publication
MEF . . . . . Marine expeditionary force
mm . . . . . millimeter
MSC . . . . . major subordinate command

NAI . . . . . named area of interest

OIC . . . . . officer in charge
OPLAN . . . . . .operation plan
OPORD . . . . . .operation order
OSINT . . . . . open-source intelligence

P&A . . . . . production and analysis
PIR . . . . . priority intelligence requirement
PR . . . . . production request

R&S . . . . . reconnaissance and surveillance
RadBn . . . . . radio battalion
RECON . . . . . reconnaissance
RFI . . . . . .request for intelligence

S-2 . . . . . intelligence staff officer (battalion or regiment)
S-3 . . . . . plans staff officer (battalion or regiment)
SARC . . . . . surveillance and reconnaissance cell
SIGINT . . . . . .signals intelligence
SII . . . . . statement of intelligence interest
SIR . . . . . .specific information requirement
SOP . . . . . .standing operating procedure
SOR . . . . . .specific order or request
SST . . . . . .SIGINT support team
SSU . . . . . SIGINT support unit

TTP . . . . . tactics, techniques, and procedures

UAV . . . . . .unmanned aerial vehicle

VIC . . . . . vicinity
VMAQ . . . . . .Marine tactical electronic warfare squadron
VMU . . . . . .Marine unmanned aerial vehicle squadron
VO . . . . . validation officer

SECTION II
DEFINITIONS

area of operations—An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. Also called **AO**. (JP 1-02)

battle damage assessment—The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. (JP 1-02) In Marine Corps usage, the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. Also called **BDA**. (MCRP 5-12C)

collection—Acquisition of information and the provision of this information to processing (JP 1-02) In Marine Corps usage, the gathering of intelligence data and information to satisfy the identified requirements. (MCRP 5-12C)

collection management—In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required. (JP 1-02)

collection operations management—The authoritative direction, scheduling, and control of specific collection operations and associated

processing, exploitation, and reporting resources. Also called **COM**. (JP 1-02)

collection plan—A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02)

collection requirement—An established intelligence need considered in the allocation of intelligence resources to fulfill the priority intelligence requirements and other intelligence needs of a commander. (This definition modifies the JP 1-02 entry and will be included in the next edition of MCRP 5-12C.)

collection requirements management—The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. Also called **CRM**. (JP 1-02)

combatant command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

command and control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP 1-02) Also in Marine Corps usage, the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. Also called **C2**. (MCRP 5-12C)

command element—The core element of a Marine air-ground task force (MAGTF) that is the headquarters. The command element (CE) is composed of the commander, general or executive and special staff sections, headquarters section, and requisite communications support, intelligence and reconnaissance forces, necessary to accomplish the MAGTF's mission. The CE provides command and control, intelligence, and other support essential for effective planning and execution of operations by the other elements of the MAGTF. The CE varies in size and composition and may contain other Service or foreign military forces assigned or attached to the MAGTF. Also called **CE.** (This definition modifies the JP 1-02 entry and will be included in the next edition of MCRP 5-12C.)

counterintelligence—1. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02) 2. Within the Marine Corps, counterintelligence constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. Also called **CI**. (MCRP 5-12C)

dissemination—Conveyance of intelligence to users in a suitable form. (JP 1-02)

dissemination management—Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination

system are not overloaded attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12C)

force protection—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. (JP 1-02)

geographic intelligence—The process of collecting, organizing, analyzing, synthesizing, disseminating, and using all-source geospatial and other intelligence information with regard to the military aspects of the terrain in support of MAGTF operations. (MCWP 2-12.1)

human intelligence—A category of intelligence derived from information collected and provided by human sources. (JP1-02) In Marine Corps usage, human intelligence operations cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations. Also called **HUMINT.** (MCRP 5-12C)

imagery intelligence—Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called **IMINT**. (JP 1-02)

indications and warning—Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear or non-nuclear attack on the United States, its overseas forces, or allied and/or coalition nations; hostile reactions to US reconnaissance activities; terrorists' attacks; and other similar events. Also called **I&W**. (JP 1-02)

indications (intelligence)—Information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (JP 1-02)

indicator—In intelligence usage, an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action. (JP 1-02)

intelligence—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02) Also in Marine Corps usage, intelligence is knowledge about the enemy or the surrounding environment needed to support decisionmaking. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence cycle—A six-step process by which information is converted into intelligence and made available to users. The six steps are planning and direction, collection, processing and exploitation, production, dissemination, and utilization. (MCWP 2-1) (This definition modifies the JP 1-02 entry and will be included in the next edition of MCRP 5-12C.)

intelligence preparation of the battlespace—An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. (JP 1-02) In Marine Corps usage, the systematic, continuous process of analyzing the threat and environment in a specific geographic area. Also called **IPB**. (MCRP 5-12C)

intelligence report—A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called **INTREP**. (JP 1-02)

intelligence requirement—1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the battlespace or threat forces. (JP 1-02) In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called **IR**. (MCRP 5-12C)

joint intelligence center—The intelligence center of the combatant command headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the combatant commander and staff, components, subordinate joint forces and elements, and the national intelligence community. Also called **JIC**. (JP 1-02)

Marine air-ground task force—The Marine Corps principal organization for all missions across the range of military operations, composed of forces task-organized under a single commander capable of responding rapidly to a contingency anywhere in the world. The types of forces in the Marine air-ground task force (MAGTF) are functionally grouped into four core elements: a command element, an aviation combat element, a ground combat element, and a combat service support element. The four core elements are categories of forces, not formal commands. The basic structure of the MAGTF never varies, though the number, size, and type of Marine Corps units comprising each of its four elements will always be mission dependent. The flexibility of the organizational structure allows for one or more subordinate MAGTFs, other Service, and/or foreign military forces to be assigned or attached. Also called **MAGTF**. (This definition modifies the JP 1-02 entry and will be included in the next edition of MCRP 5-12C.)

Marine expeditionary force—The largest Marine air-ground task force (MAGTF) and the Marine Corps principal warfighting organization, particularly for larger crises or contingencies. It is task-organized around a permanent command element and normally contains one or more Marine divisions, Marine aircraft wings, and Marine force service support groups. The Marine expeditionary force is capable of missions across the range of military operations, including amphibious assault and sustained operations ashore in any environment. It can operate from a sea base, a land base, or both. It may also contain other Service or foreign military forces assigned or attached. Also called **MEF**. (This definition modifies the JP 1-02 entry and will be included in the next edition of MCRP 5-12C.)

measurement and signature intelligence—Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target, source emitter, or sender measurement of the same. The detected feature may be either reflected or emitted. Also called **MASINT**. (JP 1-02)

priority intelligence requirements—Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decisionmaking. (JP 1-02) In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. Also called **PIRs**. (MCRP 5-12C)

signals intelligence—1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT**. (JP 1-02)

split base—Two or more portions of the same force conducting or supporting operations from separate physical locations. (MCRP 5-12C)

surveillance and reconnaissance cell—Primary element responsible for the supervision of MAGTF intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called **SARC**. (Change approved for inclusion in the next version of MCRP 5-12C.)

validation—A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. (JP 1-02 part 1)

APPENDIX G
REFERENCES

Department of Defense Publications

Defense Intelligence Management Document 0000-151C-95, *Department of Defense Intelligence Production Program (DODIPP): Production Procedures (U)*

Defense Intelligence Agency Manual 57-05, *DOD Exploitation of Multi-Sensor Imagery*

Joint Publications (JPs)

1-02	Department of Defense Dictionary of Military and Associated Terms
2-0	Doctrine for Intelligence Support to Joint Operations
2-01	Joint Intelligence Support to Military Operations

Marine Corps Doctrinal Publications (MCDPs)

2	Intelligence
5	Planning

Marine Corps Warfighting Publications (MCWPs)

2-1	Intelligence Operations
2-12	MAGTF Intelligence Production and Analysis
2-14	Counterintelligence
2-15.1	Remote Sensor Operations
2-15.2	Signals Intelligence
2-15.4	Imagery Intelligence
3-26	Air Reconnaissance
3-40.1	Marine Air-Ground Task Force Command and Control
3-40.5	Electronic Warfare
3-42.1	Unmanned Aerial Vehicle Operations
5-1	Marine Corps Planning Process

Marine Corps Reference Publications (MCRPs)

2-12A	Intelligence Preparation of the Battlefield
2-15.3B	Reconnaissance Reports Guide
5-12C	Marine Corps Supplement to the DOD Dictionary of Military and Associated Terms

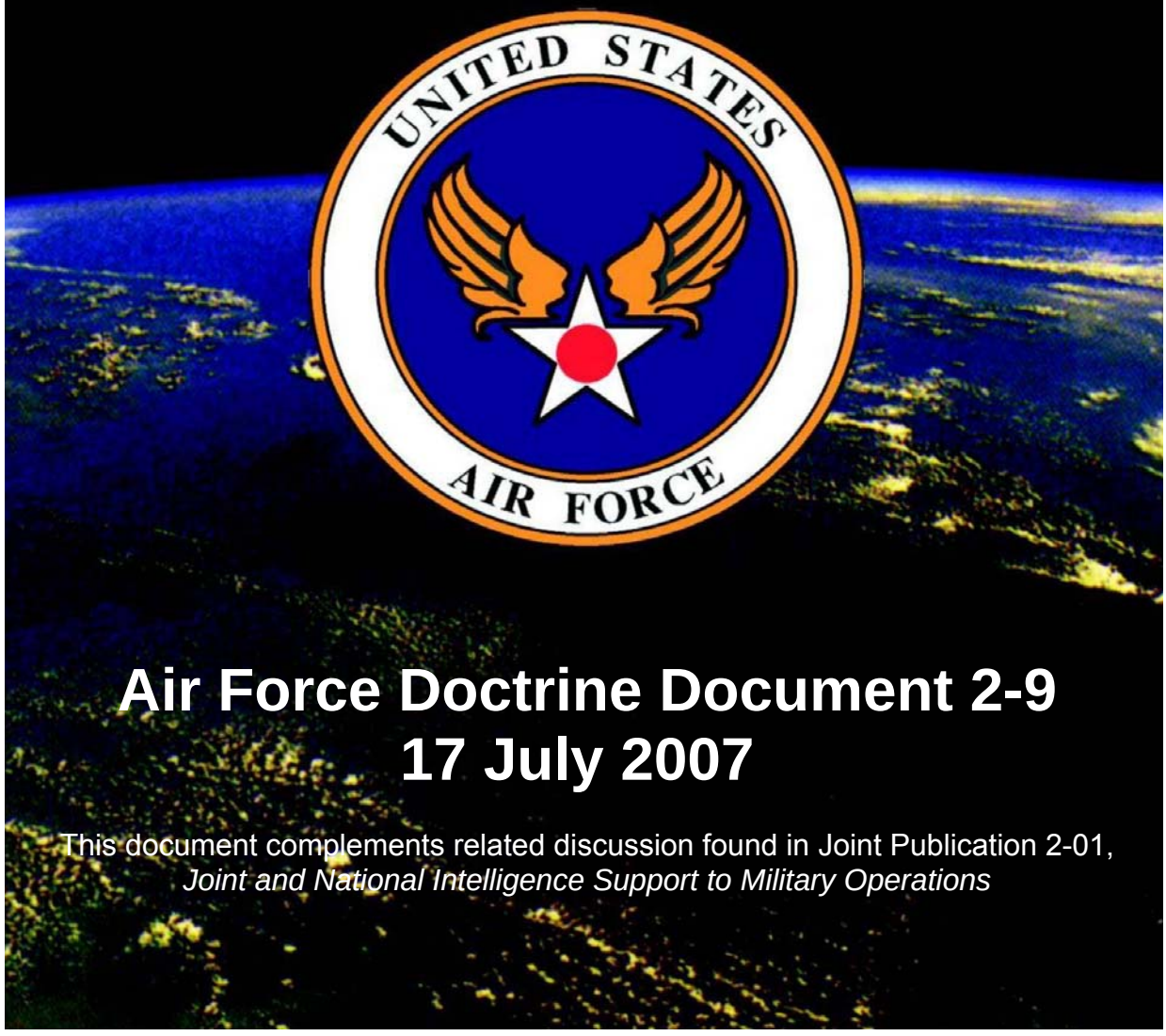
Marine Corps Intelligence Activity (MCIA) Publication

1540-002-95	Generic Intelligence Requirements Handbook (GIRH)

Army Field Manual (FM)

34-2	Collection Management and Synchronization Planning

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE OPERATIONS



Air Force Doctrine Document 2-9
17 July 2007

This document complements related discussion found in Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE DOCTRINE DOCUMENT 2-9
17July 2007

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. It updates the definition of intelligence, surveillance, and reconnaissance (ISR) to mirror the joint definition (Chapter 1). In an effort to refocus the document on operational-level doctrine, the ISR application section was deleted in its entirety, and more emphasis was placed on ISR principles by expanding this section to include the principles of persistence, global reach, and network centricity. Chapter 2 introduces predictive battlespace awareness and its association with the ISR process. The terms used to identify the ISR process are updated to match the joint process, with each step in the process expanded. The effects-based approach to operations and the ISR process are introduced. The section on unmanned or remotely piloted vehicles is updated to reflect new capabilities and expanded employment (Chapter 3). Tasking, processing, exploitation, and dissemination systems are introduced, as well as a discussion on alternative sources for surveillance and reconnaissance. Finally, the new structure for assessment is introduced and mirrors Air Force Doctrine Document 2-1.9, *Targeting*. Chapter 4 is completely revised to more clearly illustrate command relationships. A new section on the ISR division of the air and space operations center is provided to show the organization and its role. A new section that discusses intelligence authorities is provided. With the increased availability of surveillance and reconnaissance capable airborne platforms, a new section is provided to discuss the multi-role platform employment and sensor control.

Supersedes: AFDD 2-5.2, 21 April 1999
OPR: HQ AFDC/DD
Certified by: HQ AFDC/CC (Maj Gen Allen G. Peck)
Pages: 73
Accessibility: Available on the e-publishing website at www.e-publishing.af.mil for downloading
Releasability: There are no releasability restrictions on this publication
Approved by: T. MICHAEL MOSELEY, General, USAF
Chief of Staff, United States Air Force

FOREWORD

Intelligence, surveillance, and reconnaissance (ISR) functions from the air first date back to the use of balloons to observe the adversary during the French Revolution. One of the first missions for military aircraft was observation. Today, as in the past, we observe and analyze the meaning and impact of a wide variety of events and convey useful, timely intelligence on our adversaries' capabilities and intentions to our commanders.

Using doctrine as the foundation, the Air Force is following a transformational vision of networked and linked sensors that is shrinking the sensor-to-shooter cycle and is giving commanders greater situational awareness and better predictive intelligence necessary to achieve decision superiority and battlefield dominance. ISR technology provides us a clear advantage and no commander would want to reverse the direction the Air Force is following. However, our greatest ISR resource is our Airmen. In the best tradition of American ingenuity, our Airmen are constantly finding new and innovative uses for current and developing technology that give commanders a competitive advantage and enable them to create effects across the range of military operations. We have come a long way from the days of wondering what is going on just over the next hill, or half a world away. Through proper employment and integration of ISR capabilities, the Air Force will continue to provide decision makers at all levels of command the intelligence information needed to make policy, acquire capabilities, create strategy, conduct operations, and protect America from its adversaries.

T. MICHAEL MOSELEY
General, USAF
Chief of Staff

TABLE OF CONTENTS

INTRODUCTION v

FOUNDATIONAL DOCTRINE STATEMENTS vi

CHAPTER ONE—Intelligence, Surveillance, and Reconnaissance (ISR) Value to Operations 1
- ISR Defined 1
- Strategic, Operational, and Tactical ISR 3
  - Strategic 3
  - Operational 3
  - Tactical 3
- ISR Principles 4
  - Integrated 4
  - Accurate 4
  - Relevant 5
  - Timely 5
  - Fused 5
  - Accessible 6
  - Secure 6
  - Survivable, Sustainable, and Deployable 6
  - Unified Effort 7
  - Persistent and Global Reach 7
  - Network Centric 8

CHAPTER TWO—The ISR Process 9
- Planning and Direction 9
- Collection 13
- Processing and Exploitation 16
- Analysis and Production 17
- Dissemination and Integration 19
- Evaluation and Feedback 21

CHAPTER THREE—ISR Elements 22
- Intelligence Collection Disciplines 22
  - Geospatial Intelligence 22
  - Signals Intelligence 24
  - Measurement and Signature Intelligence 24
  - Human Resources Intelligence 25
  - Open-Source Intelligence 25
- ISR Resources 25
  - Airborne Systems 25
  - Space-based Systems 28
  - Ground-based Systems 30
  - Human Intelligence Sources 31
  - Non-Traditional ISR Resources 32
  - Tasking, Collecting, Processing, Exploitation, and Dissemination Systems 33

Products 33
Indications and Warning 34
Current Intelligence 34
General Military Intelligence 35
Situational Awareness 35
Intelligence Preparation of the Operational Environment 36
Defense and Penetration Analysis 36
Scientific and Technical Intelligence 36
Target Intelligence 36
Assessment 37
CHAPTER FOUR—Commanding, Organizing, and Employing ISR Forces 39
Command Relationships 39
The Combatant Commander's Role 39
The Joint Force Commander's Role 40
The Joint Force Air and Space Component Commander's (JFACC's) Role 40
The Commander, Air Force Forces' Role 40
National Support 41
Organization and Employment 41
Role of the Air and Space Component's A-2 42
Role of the ISR Division 43
ISR Authorities 44
ISR and Multi-role Aircraft Employment 46
Direct and Reachback Support to JFACC ISR Employment 47
Air Force Intelligence, Surveillance, and Reconnaissance Agency 47
Air and Space Centers of Excellence 48
Wing, Group, and Squadron Intelligence Support 48
Air Control Squadrons 49
Reconnaissance Units 49
Space Operations Units 49
Other Air Force Intelligence Units 49
Multinational Intelligence Operations 50
SUGGESTED READINGS 51
GLOSSARY 52

INTRODUCTION

PURPOSE

This Air Force doctrine document (AFDD) establishes doctrinal guidance for fundamental principles and operational-level Air Force doctrine for intelligence, surveillance, and reconnaissance (ISR) and supports basic Air Force doctrine. It should be used to plan, prioritize, task, coordinate, and execute ISR operations.

APPLICATION

This AFDD applies to the Total Force: all Air Force military and civilian personnel, including active duty, Air Force Reserve Command, and Air National Guard units and members.

The doctrine in this document is authoritative, but not directive. Therefore, commanders need to consider the contents of this AFDD and the particular situation when accomplishing their missions. Airmen should read it, discuss it, and apply it.

SCOPE

Air Force intelligence, surveillance, and reconnaissance doctrine provides guidance for ISR participation in Air Force missions. A common doctrine, shared by all elements of a Service, helps ensure intelligence, surveillance, and reconnaissance organizations provide their commanders and forces with timely, accurate, and relevant information. Doctrine is a guide for the exercise of professional judgment rather than a set of inflexible rules. It describes our understanding of the best way to do the job. The doctrinal statements in this document are general—they are to be implemented through tactics, techniques, and procedures. These are articulated in unified and major command and field operating agency publications, as well as unit concepts of operations, operations plans, and other supporting documents.

FOUNDATIONAL DOCTRINE STATEMENTS

Foundational doctrine statements are the basic principles and beliefs upon which Air Force doctrine documents (AFDDs) are built. Other information in the AFDDs expands on or supports these statements.

- The goal of intelligence, surveillance, and reconnaissance (ISR) operations is to provide accurate, relevant, and timely intelligence to decision makers. The Air Force best achieves this goal through effective employment of ISR capabilities, and by capitalizing on the interoperability existing among our ISR systems, as well as non-traditional sources, to create synergy through integration. (Page 1)

- Air Force surveillance and reconnaissance assets are not inherently strategic, operational, or tactical in nature; they can be used to gather information to meet requirements at all levels of warfare. (Page 2)

- Intelligence products must enable strategic, operational, and tactical users to visualize the operational environment systematically, spatially, and temporally, allowing them to orient themselves to the current and predicted situation to enable decisive action. (Page 4)

- Planning and direction of ISR operations start with the identification of needs for intelligence regarding all aspects of the operational environment. (Page 9)

- The joint force air and space component commander (JFACC) typically serves as the supported commander for theater airborne and spaceborne reconnaissance and surveillance and provides integrated airborne ISR for the joint force commander (JFC). (Page 13)

- The JFC normally delegates operational control to the commander of Air Force forces or tactical control to the JFACC of airborne ISR assets who will task them to support combat operations via the air tasking order. (Page 40)

- The air and space operations center is the best facility to integrate the JFC's theaterwide airborne ISR capabilities, to include reachback and distributed operations ISR support. (Page 41)

- Mission objectives, priorities, and guidance for multi-role systems employment and the authority to task the weapon system must be clear and preferably worked out well in advance of mission execution. (Page 46)

CHAPTER ONE

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR) VALUE TO OPERATIONS

What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge.

—Sun Tzu
The Art of War

ISR DEFINED

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms,* defines intelligence, surveillance, and reconnaissance as an activity that synchronizes and integrates the planning and operation of sensors, assets, processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

The goal of ISR operations is to provide accurate, relevant, and timely intelligence to decision makers. The Air Force best achieves this goal through effective employment of ISR capabilities, and by capitalizing on the interoperability existing among our ISR systems, as well as non-traditional sources, to create synergy through integration. Synergy is defined as the interaction of individual parts so that the total effect produced by working together is greater than the sum of individual efforts. Together, ISR operations provide the commander the intelligence and situational awareness necessary to successfully plan and conduct operations.

ISR operations are a significant part of the overall goal of achieving decision superiority. Decision superiority is the competitive advantage, enabled by an ongoing situational awareness, that allows commanders and their forces to make better-informed decisions and implement them as fast and effectively as the situation warrants. Decision superiority is about improving our ability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. ISR is the life blood of effective decision making.

Intelligence, surveillance, and reconnaissance are often referred to as a collective whole, though the capabilities are distinctive and each fulfills a different purpose. These distinctive capabilities are defined below:

"Intelligence is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; it is the information and knowledge about a topic obtained through observation, investigation, analysis, or understanding." (JP 1-02)

"Surveillance is the systematic observation of aerospace [sic], surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means." (JP 1-02) The Air Force perspective emphasizes that surveillance operations are sustained operations designed to gather information by a collector, or series of collectors, having timely response and persistent observation capabilities, a long dwell time and clear continuous collection capability.

"Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area." (JP 1-02) The Air Force perspective emphasizes that reconnaissance operations are transitory in nature and generally designed to collect information for a specified time by a collector that does not dwell over the target or in the area.

The information derived from surveillance and reconnaissance, converted into intelligence by exploitation and analysis, is used to formulate strategy, policy, and military plans; to develop and conduct campaigns; guide acquisition of future capabilities; and to protect, prevent, and prevail against threats and aggression aimed at the US and its interests. **Air Force surveillance and reconnaissance assets are not inherently strategic, operational, or tactical in nature; they can be used to gather information to meet requirements at all levels of warfare.** ISR operations are conducted across the range of military operations from peace, to war, to conflict resolution. Combatant commanders typically employ assigned and attached forces through their J-2 staff for day-to-day management of ISR forces. When a joint task force (JTF) is created, the joint force commander (JFC) integrates the actions of assigned, attached, and supporting ISR forces within the operational area. Command and control (C2) of airborne ISR is usually delegated to the joint force air and space component commander (JFACC).

To be more specific, the JFC employs forces assigned or attached to the JTF to achieve campaign objectives. The JFC may retain operational control (OPCON) over airborne ISR assets or delegate it to the JFACC. The JFACC is in the best position to integrate space ISR assets through the air and space operations center (AOC). The JFC's staff develops an overall collection strategy and posture for the execution of the ISR mission. The JTF J-2 reviews, validates, and prioritizes all outstanding intelligence requirements, whether originating from the JTF J-2 staff or a component. The JFC

normally delegates OPCON or tactical control (TACON) of theater controlled, airborne ISR assets (except those organic to combat units) to the JFACC who will allocate them to support operations via the air tasking order (ATO).

STRATEGIC, OPERATIONAL, AND TACTICAL ISR

ISR supports strategic, operational, and tactical operations by providing intelligence and services to a diverse set of consumers, to include national agencies; geographic, functional, or Service components; and unit-level decision makers. Air Force ISR professionals provide valuable contributions at all levels of operations.

Strategic

Air Force ISR systems provide intelligence required at the strategic level to formulate national strategy, policy, and plans. The goal of strategic-level ISR is to provide accurate, timely, and predictive intelligence to enable decision makers to take appropriate actions before crises develop and to support the decision makers as crises unfold. Intelligence is also a key player in research and development, weapon system acquisition, force protection planning and programming, and other national-level programs.

Operational

Air Force ISR systems provide intelligence crucial to planning and executing theaterwide operations to accomplish the JFC's objectives. For example, campaign planners rely on ISR to provide the intelligence crucial to understanding an adversary's weaknesses and key nodes that can be affected by air, space, land, maritime, and information operations. Intelligence analysis helps detect/discover, identify, locate, and describe the vulnerable, vital elements of an adversary's physical and virtual structure and their centers of gravity (COG). Finally, ISR provides the means to assess the effects of current operations.

Tactical

ISR support at the tactical level of operations is primarily focused on tactical threat warning, mission planning, targeting, and assessment. Threat assessment, although performed at every level of military operations, is most common and critical at the tactical level. ISR tasks such as current assessment and defense penetration and warning are guided at the unit level by tailored tactics, techniques, and procedures. Required intelligence, such as target imagery, should be immediately available to support the ATO and mission planning cycle. Wing and squadron personnel also provide valuable information to the ISR process with annotated aircraft cockpit videos and reports based on aircraft sensors and aircrew debriefs. These inputs directly impact campaign assessment and reattack targeting decisions.

ISR PRINCIPLES

ISR operations provide intelligence information to commanders and decision makers at all levels, helping them reduce uncertainties in the decision-making process. It is precisely because intelligence supports all levels of policy, planning, and decision making that ISR is now presented in Air Force doctrine as a keystone publication (previously organized under information operations).

To be effective, ISR products must be responsive to the commander's or decision maker's needs. **Intelligence products must enable strategic, operational, and tactical users to better understand the operational environment systematically, spatially, and temporally, allowing them to orient themselves to the current and predicted situation to enable decisive action.** By adhering to the principles listed below, ISR personnel and systems can maximize intelligence support to consumers.

Integrated

Surveillance and reconnaissance operations and the intelligence process should be fully integrated to meet the timeliness and accuracy requirements of air, space, and cyberspace power. A close relationship between the ISR process and strategy, planning, and execution functions will foster the flow of essential information. The commander considers both the capabilities and limitations of ISR systems and organizations in the decision-making, planning, preparation, execution, and assessment processes. Similarly, as an essential element of all Air Force operations, ISR personnel should be fully aware of mission goals and objectives and integrated into the operational environment at all levels.

Accurate

To best support Air Force operations, ISR-derived products should be as accurate as possible. Accuracy implies reliability and precision. This requires corroboration and analysis of all available information. Extensive knowledge of adversary strategy, tactics, capabilities, and culture enables ISR personnel to anticipate actions and provide the most complete and exact picture possible to planners and operators. Accuracy also aids commanders in defeating adversary deception efforts. Geoposition accuracy is a crucial requirement for targeting, especially with the employment of precision-guided munitions. Sensors acquire information that enables targeteers to produce target locations or aim points suitable for the accurate employment of specific weapon systems. Lastly, one of the most demanding tasks for ISR personnel during emerging crises is the need to balance requirements for accuracy with timeliness (defined below). Judging the appropriate balance between accuracy and expediency requires very close coordination with operations planners.

Relevant

Relevance in ISR means the ISR product is tailored to the requestor's needs. Intelligence and collection requirements should directly apply to determining, planning, conducting, and evaluating operations. Intelligence should focus on the commander's potential, planned, and ongoing courses of action. Ensuring the relevance of intelligence to the requestor means that ISR planners should consider the suitability of specific surveillance and reconnaissance assets to achieve the commander's objectives. Planning the employment of surveillance and reconnaissance assets is based on an asset's capability and its suitability, within the context of the overall collection plan, to meet user requirements. Suitability also applies to the format of the processed intelligence. Both the information and the format should be useful to the user.

Timely

ISR products should be available in time to plan and execute operations as required. This principle applies to identifying and stating requirements, collecting information, and producing actionable intelligence. Timely intelligence is essential to prevent the use of surprise by the adversary, conduct defense, seize the initiative, and use forces effectively. The dynamic nature of ISR can provide information to aid in a commander's decision-making cycle and constantly improve the commander's view of the operational environment. The responsive nature of Air Force surveillance and reconnaissance assets is an essential enabler of timeliness if Air Force assets are made available to collect information when and where required. Collected information is disseminated to the appropriate processing agency or user based on established collection or reporting requirements. As technology evolves, every effort should be made to streamline and automate processes to reduce timelines from tasking through product dissemination. However, since surveillance and reconnaissance assets are limited, responsiveness is often driven by the commander's objectives and priorities. Commanders must ensure proper asset utilization based on the range of missions. Finally, ensuring communications connectivity throughout the ISR "system" is key to delivering timely intelligence to consumers.

Fused

ISR-derived information from many sources is combined, evaluated, and analyzed to produce accurate intelligence. This process is called fusion. Fusion helps defeat adversary efforts to deny information. Intelligence personnel use fusion analysis to increase assessment accuracy and counter adversary denial and deception efforts. Analysts fuse intelligence by considering as many types of target signatures and indicators collected over time as practical. Considering intelligence from multiple collection systems (preferably from different disciplines) over time may reveal activity concealed from a single sensor or discipline. Fusing multiple sources with historic trends and previous assessments enables analysts to generate a more complete and accurate assessment of the operational environment. However, care should be taken not to promote fusion at the expense of timeliness. For example, significant single-source information that relates directly to a current or planned operation, such as a

previously undetected surface-to-air missile site near the target or a credible report of an imminent airfield attack, should be sent to users immediately.

Accessible

ISR-derived information must be readily accessible to be usable. First, intelligence should be easily retrievable; ISR personnel should be able to "get at the information" before they can disseminate, process, exploit, or analyze it. Second, both ISR personnel and the consumer should have the appropriate clearances to access and use the information. Third, ISR products should always be classified at the lowest possible classification consistent with security. Understandably, some intelligence requires extraordinary protection such as sensitive sources and methods or the fact that certain knowledge is held.

Secure

Personnel working with classified material must protect the information and sensitive sources while still managing to keep commanders and their staffs fully informed. Protection of classified information and sources must be consistent with established Department of Defense (DOD) policies and procedures, even if operations are conducted with coalition partners. The difference between peacetime and contingency policies and priorities should be determined ahead of time and be well understood. Criteria, authority, and procedures for declassifying or sanitizing intelligence should be available at appropriate levels and tested during selected exercises. Classification authorities should avoid overclassification and unnecessary compartmentalization that can prevent commanders and staff from accessing needed intelligence. If directives are too restrictive to meet current operational requirements, additional guidance or authorization from the appropriate classification authority should be requested.

Survivable, Sustainable, and Deployable

ISR resources, activities, and communications should be survivable to ensure support is available when needed. Important components of survivability include redundancy of critical intelligence, protection against the adversary's asymmetrical threats, information assurance measures, and hardening of communications capabilities. Therefore, commanders should develop concepts of ISR operations that provide for continuity even if communications are severely stressed or lost. Sustainability is vital for all surveillance and reconnaissance systems. A system's ability to maintain the necessary level and duration of operations depends on ready forces and resources in sufficient quantities to support stated requirements. Deployability has to be built into systems. With the exception of aircraft and space-based ISR platforms, most ISR assets are rugged, small, and lightweight. They should be easy to transport and set up and capable of immediate connectivity and interoperability. Finally, from a macro view, ISR-derived intelligence is a large part of the support that goes into the survivability and sustainability of every weapon system acquired and maintained by the Air Force.

Unified Effort

Organizations at all levels should have clearly defined functions that minimize duplication, maximize sharing of information among Services agencies and allies, and are mutually supportive. Unity of effort requires a focus on joint and allied forces' ISR requirements and production. These potential requirements and the support they need should be agreed upon and tested in advance of operations. Finally, collaboration among operators, targeteers, analysts and specialists result in synchronized, efficient target development and assessment.

Persistent and Global Reach

Commanders require the ability to achieve on-demand reconnaissance and persistent surveillance throughout the operational environment. Modern collection requirements are increasingly focused on fleeting, dispersed targets that present a markedly different signature from industrial-age targets such as large military formations and complex industrial facilities. Commanders should, therefore, consider, plan for and ensure diplomatic arrangements are in place for immediate deployment and employment of ISR assets that must overfly sovereign nations en route to targets. To deny enemy sanctuaries of movement, Air Force ISR capabilities focus detailed collection against broad target areas for long periods of

Battle of Fallujah

Although Air Force reconnaissance planes had been circling over Fallujah, the Marines surrounding the Iraqi city could not view what the sensors on the Air Force MQ-1 Predators and C-130E/H Scathe View were seeing. Then, a tactical air control party showed up with the first laptop computer and antenna ROVER II (Remote Operations Video Enhanced Receiver) system. On the laptop's screen appeared the video image downlinked by a circling Predator. This direct support of actionable imagery to the tactical user was invaluable and has saved many lives. In another example, Airmen and Soldiers at Balad Air Base, Iraq, used ROVER to help direct a Predator scouting for insurgents launching mortar attacks on the base. On 11 April 2004, the night after a fatal mortar attack on the base, a Predator spotted two mortars being fired at the base. Before a third round was launched, the unmanned aircraft (UA) crew in close coordination with ground units using ROVER, scored a direct hit on the insurgents. With urban close air support a growing concern, ROVER technology is a valuable tool for warfighters on the ground and aircrews to see the same operating picture without being in harm's way.

time, either through long-dwell sensors or a combination of more numerous short-dwell collectors. Commanders defeat denial strategies and create ISR reach throughout the operational environment through a combination of space-based sensors, remotely piloted systems, and tactically survivable platforms. The combination of persistence and reach complicates enemy planning and reduces enemy choices while creating options for commanders.

Network Centric

Network centricity is a key principle for all Air Force ISR efforts. It is the natural progression of technology and employment that aids in the efficient exchange of actionable information to operators at all levels. Net-centric ISR capabilities, designed from the ground up to plug into a secure global information network that extends out to the tactical edge, provide users tailored information and actionable intelligence that increase situational awareness and foster the capacity to conduct operations more flexibly and rapidly. Networking will enable information derived from a wide variety of sensors on shooters, battle management assets, and dedicated intelligence systems to be directly available to any networked warfighter (i.e., sensor-to-shooter). This capability will also create a high fidelity fused common operational picture which is the cornerstone of battlespace awareness dominance. Net-centric collaborative environments support creation of "virtual organizations" where personnel from numerous agencies around the world horizontally align as a team, quickly focus analytic effort on a problem, and deliver a solution or recommended course of action for employment under the C2 of a vertically aligned organizational construct. Often transparent to the commander of Air Force forces (COMAFFOR), such collaborative efforts (often spontaneous) should be encouraged to make the most efficient use of available resources.

Through net-centric operations, a wide variety of detailed sensor data can be posted to compatible, joint intelligence information stores, and continually searched in order to cross-cue and refine collection operations. Intelligence analysts combine, evaluate, and analyze collected information from a variety of sources in a collaborative environment, then provide fused products for use by decision makers. Combining multiple resources in a variety of spectra works to defeat enemy concealment, denial, and deception strategies. Strategic, operational, and tactical users employ tailored searches to gain access to the right information at the right time to support operations. Ideally, both C2 and ISR planning systems access common databases to synchronize collection and operations requirements. Network-centric ISR capabilities contribute to achieving information superiority.

CHAPTER TWO

THE ISR PROCESS

> *True genius resides in the capacity for the evaluation of uncertain, hazardous, and conflicting information.*
>
> ***—Winston Churchill***

The ISR process is comprised of a wide variety of intelligence operations: planning and direction; collection, processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback. It should focus on the commander's mission and concept of operations. The process is not a linear or even cyclic operation, but rather represents a network of interrelated, simultaneous operations that can, at any given time, be fed by and feed other intelligence operations. The output of the overall process is actionable intelligence—timely, accurate, and complete—that supports decision making at all levels of war.

PLANNING AND DIRECTION

Planning and direction of ISR operations start with the identification of needs for intelligence regarding all aspects of the operational environment. The President and Secretary of Defense direct JFCs to engage in adaptive planning for the conduct of operations. The JFC should provide the commander's critical information requirements (CCIRs) to the joint staff and components. CCIRs comprise a comprehensive list of information requirements identified by the commander as being critical to facilitating timely information management and the decision-making process. There are numerous legal issues associated with ISR, especially if it could impact US citizens. ISR activities should be coordinated with the servicing judge advocate general (JAG) to ensure compliance with the law and any existing rules of engagement (ROE).

Intelligence preparation of the operational environment (IPOE) alerts decision makers at all echelons of command to emerging situations and threats. JFC guidance provided during planning shapes the overall concept of operations, which in turn drives requirements for air and space strategy. The JFACC's challenge is determining where and when to focus attention in order to influence events early, ready forces, and begin setting conditions for future operations. Therefore, preparation of the operational environment is essential to supporting the commander's visualization process, determining (component-level) CCIRs, anticipating critical decision points during operations, and prescribing ROE. IPOE and target development processes identify and assess the adversary's COGs, key capabilities and vulnerabilities, intentions, and potential courses of action (COAs). By identifying known adversary capabilities, IPOE provides the conceptual basis for the JFACC to visualize how the adversary might threaten the command or interfere with mission accomplishment. By identifying specific adversary COAs and COGs, IPOE provides the basis for friendly and adversary COA comparisons, often referred to as wargaming sessions, in which the staff "fights" each

friendly and adversary COA. This wargaming process assists intelligence and operations in identifying specific indicators that could confirm or deny a given adversary COA or are otherwise required to support a friendly COA

Using knowledge gained via intelligence analysis (IPOE and target development) and the wargaming process, commanders can anticipate when and where action will occur, enabling them to focus on broad friendly, hostile, and neutral force interactions to determine the most effective way to apply Air Force capabilities to achieve desired effects. With this foundation, an optimal ISR strategy designed to sequence ISR operations is derived. ISR strategy is encapsulated in the joint air operations plan (JAOP) and is synchronized with theater and national ISR architectures and strategy. It provides the foundation for development and validation of intelligence requirements, captures the framework for planning and direction of ISR operations, and establishes guidance for the operation of all other elements of the ISR process. Anticipating where and when important events will take place provides a framework in which to orchestrate national, theater, and tactical assets to focus surveillance on specific target elements and guide decisions on how, when, and where to engage adversary forces to achieve the JFC's objectives.

Requirements for intelligence to support operations are identified by the commander and the staff. In the course of intelligence planning and direction, intelligence planners identify the intelligence required to answer the CCIRs. Those intelligence requirements deemed most important to mission

Predictive Battlespace Awareness

Predictive battlespace awareness (PBA) influences all elements of the intelligence process. PBA is a multidimensional understanding of the battlespace in time, space, and effect. It is the capability to correlate and fuse patterns of enemy activity and subsequent events to predict adversary intent or potential future enemy courses of action. PBA is continuous and achieved by the commander through possession of relevant, comprehensive knowledge, including an accurate forecast of pertinent influences in the battlespace. This knowledge of the operational environment, in concert with C2, permits commanders to anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities. Our ability to act with a degree of speed and certainty not matched by our adversaries permits commanders to shape the battlespace to our advantage.

To achieve this level of awareness requires the development of five key elements: intelligence preparation of the operational environment, target development, ISR strategy and planning, ISR employment, and assessment. These elements are continuously refined, in parallel, to provide a comprehensive view of the battlespace which provides commanders with the capability to anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions.

accomplishment are identified as priority intelligence requirements (PIRs). PIRs are general statements of intelligence need, such as "what is the operational status of the adversary's integrated air defense system?" or "what terrorist groups are active within the area of responsibility/interest (AOR/AOI)?" They provide the framework for prioritization of all ISR operations. PIRs are driven by, and in turn drive, the IPOE process to refine information requirements and support the commander's potential courses of action. The PIRs drive the development of detailed essential elements of information (EEIs). The designation of intelligence requirements helps ensure ISR efforts are focused on the most critical information needed to support warfighters in addition to Air Force acquisition efforts and defense policy-making. The EEIs define intelligence consumers' specific information requirements. A sample EEI would be, "what is the current location of the adversary SA-20 battery?" EEIs are linked to PIRs in order to maintain traceability for all ISR operations back to commander priorities. Over time, as new direction and guidance evolve, ISR planners will develop new requirements or modify existing requirements.

Information requirements should be validated before collectors can be tasked to fill the requirement. ISR requirements are validated by theater collection management authorities embedded in the JFC's staff. Theater collection managers will typically answer the following questions before validating an information requirement: Does the information requirement meet the commander's concept of operations? Has the information already been acquired but not distributed to the requester? Are there other ongoing operations that might satisfy the requirement? If any of these conditions is met, new ISR collection missions may not be necessary. Once validated, an information requirement becomes a collection requirement and the ISR planning process begins. The process for developing and validating ISR collection requirements is essentially the same during peacetime, crisis, and war—only the nature of the requirements and the timeliness in which they should be satisfied varies. Though the process remains the same across the range of military operations, carefully crafted intelligence requirements are essential in an effects-based approach to operations.

An effects-based approach to operations (EBAO) is one in which operations are planned, executed, assessed, and adapted to influence or change systems or capabilities in order to achieve desired results. EBAO seeks to understand and exploit the complex connections among individual actions, the effects—direct and indirect—that those actions produce, how those effects influence the states and behaviors of complex systems in the operating environment, and how these effects contribute to the accomplishment of desired outcomes. Under an effects-based approach, IPOE and target development products will enable the entire process. Throughout the intelligence process, refinement of information requirements should continuously evaluate whether or not the intelligence provided will satisfy the needs of planning, employment, and assessment. Since EBAO starts with desired outcomes (the end state, objectives and related effects), requests for information should be tailored to ensure the desired effects can be measured—something that is not always easily anticipated or quantified depending upon the capability employed. Assessment of operations will include all efforts to evaluate performance (measures of performance [MOPs]) and progress

toward effects and objectives (measures of effectiveness [MOEs]). Assessment also seeks to anticipate outcomes and answer both questions "are we doing things right (MOPs)," and "where do we go from here?" Assessment requires stringent adherence to apportionment and allocation procedures when employing ISR assets to ensure the correct measurement of the obtained effect. (See AFDD 2, *Operations and Organization*, and AFDD 2-1.9, *Targeting,* for more on the effects-based approach and assessment.)

The process of planning ISR operations begins once requirements have been established, validated, and prioritized. As intelligence collection requirements are aligned with available collection capabilities, the planning process addresses factors such as the availability of ISR assets, platform and sensor capabilities, adversary threats to ISR assets, and timeliness of the ISR response. These factors, when weighed together, affect how ISR assets are tasked and employed. In order to make the planning process more efficient, information requesters should clearly articulate their collection requirements and allow the collection managers and operations planners to decide the best way to meet the requirements. ISR operations planners at every level should coordinate closely with each other to effectively plan ISR operations. ISR planners should thoroughly analyze the combination of the commander's objectives and guidance, potential threats, force capabilities, and ISR systems availability.

Collection managers should first coordinate with operations planners to determine if organic ISR assets are capable of satisfying the requirement. If organic assets are available, then the appropriate unit will be tasked by the proper authority who exercises OPCON or TACON over the collection asset. If organic assets are not available to satisfy the request then the request is forwarded to a higher echelon for consideration.

- At the national level, the Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), National Security Agency (NSA), and the National Geospatial-Intelligence Agency (NGA) conduct long-range ISR planning and form intelligence task forces in response to crises. These agencies may also augment joint force ISR staffs with joint staff-directed national intelligence support teams (NIST) if requested. These teams, in addition to other duties, help focus ISR planning and collection requirements and provide an additional conduit for two-way communication between theater and national-level ISR collection management efforts.

- At the theater or joint force level, the JFC will provide collection, processing, exploitation, production, and dissemination capabilities. The JFC also establishes priorities for ISR operations that align with national and theater objectives. Further, the JFC's staff produces theater plans, such as the operations plans (OPLAN) and concept plans (CONPLAN), and tailors theater ISR assets to meet crisis requirements. Lower echelon collection requirements are often passed to theater collection managers where the redundant requirements are deconflicted. For peacetime, contingency, and wartime operations without an established JTF, the theater collection managers and operations planners coordinate their efforts in the ISR planning process. If a JTF is established, the JFC's collection managers and

operations planners coordinate their efforts with AOC collection managers and operations planners. The results of these efforts are included in the ATO and other tasking mechanisms as they are developed. The JFC's staff is responsible for development of a federated architecture for intelligence exploitation and analysis, leveraging the support of organic capabilities at the component and JTF level, other combatant commanders, and national agencies to ensure complete coverage of all exploitation and analysis requirements. Finally, in conjunction with functional and service components and coalition partners, the JFC will request ISR capabilities (personnel, platforms, etc.) to support current and planned requirements that exceed on-hand capabilities.

- At the operational level, **the JFACC typically serves as the supported commander for theater airborne and spaceborne reconnaissance and surveillance and provides integrated airborne ISR for the JFC.** If no JFACC is appointed, the COMAFFOR should normally serve as the supported commander for theater Air Force airborne and spaceborne reconnaissance and surveillance. At the operational level, the process of planning and directing ISR operations includes identifying and validating the need for ISR missions, and if a need is determined, prioritizing the missions. At this level, ISR planners consider the tradeoffs of survivability, weather effects, and information acquisition. For example, if land operations are of primary concern, the COMAFFOR/JFACC will position airborne ISR assets to ensure they provide the best possible support to ground operations. However, if the adversary poses a significant threat to these assets, the COMAFFOR/JFACC may need to disperse or reposition assets to improve their survivability. If organic ISR assets are not available, then alternative arrangements should be developed with outside supporting agencies to satisfy the information requirement.

COLLECTION

The collection portion of the intelligence process involves tasking appropriate collection assets or resources to acquire the data and information required to accomplish collection tasking. Collection includes the identification, coordination, and positioning of assets or resources to satisfy intelligence requirements.

Collection managers develop collection plans based on the validated intelligence requirements of commanders and decision makers. The collection manager's task is to first verify the requirements have been validated. Once verified, the collection manager:

- Develops and manages a collection plan that integrates requirements with target characteristics.

- Determines the capabilities and limitations of the available organic collection assets and compares them to the collection plan.

- Develops a collection strategy to optimize the effective and efficient use of all available, capable, and suitable collection assets and resources.

- ✪ Identifies collection requirements that cannot be met by organic assets and forwards them up the chain of command for validation and tasking of non-organic intelligence resources.

- ✪ Directs processing and dissemination of collected data. Collection managers should understand the capabilities and limitations of each discipline and the procedures for ensuring target coverage by the appropriate collection asset and/or resource. Collection managers keep requesters informed of collection status and capabilities so there are realistic expectations of what can be collected and what level of confidence can be placed in the information.

The key to the collection manager's job is selection of the right combination of collection assets for a particular information requirement. Collection managers should focus on a multidisciplinary approach to collection tasking. Collection capabilities complement each other, and the collection manager should resist favoring or becoming too reliant on a particular sensor, source, system, or technique. Each system's limitations can be mitigated through the capabilities of the others, as different systems provide additional insights into the requirement. While a sensor, source, or system may seem to be an obvious choice to satisfy a requirement, flexibility is the key. Collection managers should match collection resources to the type of adversary activity most likely to be captured by collection operations. Rigid dependence on a single source may result in mission failure, especially if that source becomes unavailable or if the adversary takes measures to counter it. Lack of a multidisciplinary approach may also result in discernible patterns that may play into the adversary's counterintelligence or denial and deception efforts.

Collection managers should seek to maximize the use of existing collections. This requires full access to national databases. Collection managers should look first to organic assets as the primary choice for collection tasking. Use of organic collection assets allows a timely and tailored response to collection requirements and serves to lessen the burden on collection resources controlled by other units, agencies, and organizations. However, if requirements cannot be satisfied by organic assets, the collection manager should not hesitate to request collection support from higher, adjacent, and subordinate units, agencies, and organizations. Each echelon in the collection management architecture has specific capabilities and responsibilities:

- ✪ At the strategic level, DIA coordinates requirements through NGA, National Reconnaissance Office (NRO) and NSA for tasking of national reconnaissance systems, manages the DOD human intelligence (HUMINT) program, coordinates with the intelligence community on other collection programs, and responds to requests for information (RFIs) submitted by theater intelligence centers.

- ✪ At the theater level, the geographic combatant commander (CCDR) exercises collection management authority (CMA) for collection operations in his theater. CMA involves two complementary functions: collection requirements management (CRM), defining what intelligence systems should collect; and collection operations management (COM), specifying how to satisfy the requirement. CRM focuses on

the requirements of the customer, is all-source oriented, and advocates what information is necessary for collection. COM focuses on the selection of the specific intelligence discipline(s) and specific systems within a discipline to collect information addressing the customer's requirement. For specified operations, the JFC will normally retain CRM responsibilities and delegate the responsibility for COM for the joint operations area (JOA) to the COMAFFOR or JFACC as supported commander for theater ISR.

- At the operational level, for peacetime operations, ISR managers communicate the COMAFFOR's or JFACC's tasking through scheduling messages and assembling a prioritized list of collection objectives for sensor use. During contingency operations and wartime, the JFACC tasks airborne and spaceborne platforms through the ATO and ISR managers assemble a prioritized list of collection objectives for sensor use. Specific collection tasking is captured in the reconnaissance, surveillance, and target acquisition (RSTA) annex to the ATO, guided by the ISR strategy developed during the JAOP process.

- Increasingly, airborne ISR capabilities rely on multiple units to execute the mission. For example, a Predator flown by a reconnaissance squadron provides data for exploitation to a distributed common ground system (DCGS) unit. For ground-based systems, like special operations forces (SOF) or HUMINT, the responsibility lies with the competent authority at the tactical level. In all cases, tactical-level commanders should evaluate the risks (threat, tactics, weather, safety, and logistics, for example) involved to complete the mission successfully. The COMAFFOR or JFACC is the final authority on determining whether the benefits of successfully accomplishing the mission outweigh the risks involved for those forces and assets over which he exercises OPCON or TACON. However, the executing tactical commander normally provides inputs concerning these risks during the decision-making process.

- Collection management is not just a pre-mission function. Assets may also be tasked while the mission is ongoing. Changing situations may require that ISR assets be dynamically retasked from their preplanned mission to support new mission requirements. The capabilities of the asset being retasked will determine the success of the reassigned mission. For example, ISR assets with long loiter times or frequent revisit rates generally have the flexibility to respond to dynamic retasking. Dynamic retasking occurs when the requester identifies a time-sensitive need after the appropriate ISR asset has already been tasked. Dynamic retasking does not necessarily imply that a track or an ISR mission must be changed; rather it means that a higher priority collection requirement has emerged that an active platform may have the capability to collect. However, the same asset may not have the right sensor configuration to successfully accomplish the new tasking. Thus, commanders should carefully consider the advantages and disadvantages before deciding to retask assets executing their pre-planned mission. The parameters under which dynamic tasking takes place are a part of ISR strategy development, and are documented in the JAOP and RSTA annex.

PROCESSING AND EXPLOITATION

Once the data satisfying the requirements are collected, they undergo processing and exploitation. Through processing and exploitation, the collected raw data are transformed into information that can be readily disseminated, used, transmitted, and exploited by intelligence analysts to produce multidisciplinary intelligence products. Relevant critical information should also be disseminated to the commander and joint force staff to facilitate time-sensitive decision making. Processing and exploitation time varies depending on the characteristics of specific collection assets. For example, some ISR systems accomplish processing and exploitation automatically and nearly simultaneous with collection, while other collection assets, such as HUMINT teams, may require substantially more time. Processing and exploitation requirements are prioritized and synchronized with the commander's PIRs.

During processing and exploitation, collected data are correlated and converted into a format suitable for subsequent analysis and production of intelligence. Processing remains distinct from analysis and production in that the resulting information receives only a cursory analysis for time-critical exploitation and has not yet been subjected to full analytical assessment. Relevant time-sensitive information resulting from this step in the process (especially targeting, personnel recovery, or threat warning information) should be immediately disseminated through intelligence broadcasts, secure information workspace or internet relay chat channels, imagery product libraries (IPLs), intelligence databases, or message reporting. Additionally, some information is suitable in its raw form to meet user requirements. For example, joint terminal attack controllers (JTACs) can receive a direct feed via ROVER from a Predator or other full-motion video collection source to provide an invaluable "over the next hill" look to support close air support operations. Raw information should be made available to users with the capability to receive it, the knowledge to understand the information they are receiving, and the authority to take action on it.

IPOE provides a disciplined and dynamic framework for processing and exploiting large amounts of data. The knowledge gained as a result of comprehensive IPOE and target development, as well as our capability to anticipate adversary actions, depend on our ability to leverage and fuse all available information. Processing and exploitation architectures should take advantage of network centricity to enable the first part of intelligence fusion—the correlation of multiple source collection into a single, fused report of the operational environment activity. IPOE enables operators and intelligence analysts alike to remain focused on the most critical aspects of the operational environment and adversary. Incoming information and reports can be rapidly incorporated into critical decision-making processes and provide a convenient medium for displaying the most up-to-date information and for identifying critical information gaps.

ANALYSIS AND PRODUCTION

Information is converted into intelligence products through analysis and production, a structured series of actions which, although planned or usually occurring sequentially, may also take place concurrently. These actions include the integration, evaluation, analysis, and interpretation of information in response to known or anticipated intelligence production requirements.

- **Integration.** Information from single or multiple sources is received, collated, and entered into appropriate databases by the analysis and production elements of intelligence community organizations, the theater joint intelligence centers or equivalents, or subordinate joint force elements like the ISR division. Information is integrated and grouped with related pieces of information according to predetermined criteria to facilitate the evaluation of newly received information.

- **Evaluation.** Each new item of information is evaluated by the appropriate analysis and production element with respect to the reliability of the source and the credibility of the information. The reliability of the source and the credibility of the information should be assessed independently of each other to avoid the possibility of one factor evaluation biasing the other.

- **Analysis.** During analysis, deductions are made by comparing integrated and evaluated information with known facts and predetermined assumptions. These deductions are combined and assessed to discern patterns, links or recognized events.

- **Interpretation.** Interpretation is an objective mental process in which the significance of information is judged in relation to the current body of knowledge, covering both adversary and friendly forces, and existing information and intelligence. This mental process involves the identification of new activity and a postulation regarding the significance of that activity.

Taken together, these actions enable intelligence fusion—the synthesis of multiple event reports into an assessment of the nature of ongoing operational environment activity; the extrapolation of all operational environment activity into a predictive assessment of future activities; and the shaping of ongoing ISR operations to refine these assessments. To enable this level of fusion, analysts should work in collaborative environments which provide access to recognized, and often geographically separated, subject matter experts. Through collaboration, intelligence analysts are able to share information, discuss opinions, debate hypotheses, and identify or resolve analytic disagreements. Net-centric connectivity and access greatly enhance an analyst's ability to share, compare, and assess information. Intelligence analysis organizations at all echelons make unique contributions to analysis and production.

- At the strategic level, the joint staff director of intelligence (JS/J2) provides analytic estimates, reports on adversary capabilities, and activates an interagency

Circular Reporting
During Bosnia Operations

Several times during Operations PROVIDE PROMISE and DENY FLIGHT, (US operations in Bosnia) information collected from US sources was passed to NATO officials, who later reported the information back into the US intelligence system. The same thing happened in reverse. This "circular reporting" was especially true of air defense radar indications.

On occasion, intelligence officers were led to believe that there were more SAM radars active than there really were, and it took time to deconflict apparently different reports about seemingly distinct radar sites.

SA–6 GAINFUL SAM

F–16 FIGHTING FALCON

assessment cell to directly support targeting missions. In cases in which the JS/J2 needs additional expertise or resources, the JS/J2 requests assistance from the DIA.

- At the theater or joint force level, the JFC staff provides theater assessments, maintains databases, produces some target materials for operating forces in an area of responsibility (AOR), acts as overall battle damage assessment (BDA) validation authority, and supports the J–3 in the assessment process. Joint force J–2s maintain knowledge of adversary and terrain, conduct target development and nomination, and report operational BDA.

- At the operational and tactical level, intelligence personnel update databases; perform target analysis, development, and nomination; produce target materials; and report tactical and operational assessment. Intelligence personnel, through reachback and distributed operations, provide air and space-related intelligence and information operations analytical products and services unavailable in the theater or through the normal chain of command.

Additionally, analysts should have access to intelligence databases—repositories of collected data, processed information, and finished intelligence products which provide analysts with the technological means to rapidly retrieve, sort, and correlate

relevant information. Intelligence databases are usually designed to support specific requirements and functions, and are therefore often "stovepiped" according to intelligence disciplines. For example the NGA national exploitation system is a repository for imagery analysis and production, and the signals intelligence (SIGINT) on-line information system contains current and historical finished SIGINT products. The "stovepiping" of information by intelligence discipline or production category limits the potential timeliness and quality of intelligence production, as analysts are forced to search multiple databases for relevant information. Furthermore, as databases grow in volume and complexity, potentially vital pieces of information may become increasingly difficult for analysts to find and retrieve. In order to overcome this limitation, virtual knowledge bases have been designed to serve as integrated repositories of multiple databases as well as reference documents and open-source material.

Battlespace awareness products provide the foundation for the commander's estimate process as well as a baseline for long-term analysis essential to understanding the multidimensional aspects of the operating environment. The daily demand to support immediate decision-making needs often exceeds existing analytic capabilities, particularly in the forward area. Resources, therefore, should be carefully allocated and made available for the long-term analysis required to sustain operations. The necessary degree of predictive awareness can only be achieved through full participation of our joint, interagency, and multinational/coalition partners in a collaborative environment linking all command echelons and coordinating different functional nodes (e.g., reachback to analytic centers of excellence). In addition, every level of command should define and document the information it requires to build battlespace awareness, creating a deliberate information flow that is responsive to the commander's requirements.

DISSEMINATION AND INTEGRATION

Dissemination of ISR products continues the process by giving the user information required for application in a timely manner. Dissemination may take the form of electronic transmission, hardcopy annotated imagery or maps, direct threat warnings, oral and written reports, or briefings. The dissemination process requires continuous management. Without effective management, communications paths can become saturated by information from single sources being retransmitted by many intermediate collection agencies, resulting in "circular reporting." Advances in technology are also affecting dissemination. Computers and modern communication systems have reduced the information–to–production timeline for delivering ISR products. Likewise, some collection systems are capable of disseminating collected information to requesters on a real- or near real-time basis, vastly increasing their responsiveness. This is especially important for those collection operations supporting ongoing military operations in which the situation may be evolving rapidly and perishable information may lose its usefulness within a matter of minutes or seconds. Implementing new "information profiles" technologies and capabilities puts power in the hands of the warfighter to obtain only pertinent information exactly when and where it is needed. Ancillary to the discussion of classified information dissemination is the need

to expedite dissemination of declassified information. Commercial technology that enables continuous live media coverage of military operations may require expedited declassification and public dissemination of intelligence products in order to counter enemy propaganda or support other operational objectives. ISR planning should include local procedures for rapidly coordinating public release of select intelligence.

This expanding collection capability makes network centricity all the more important because real-time planning and targeting systems depend on tailored intelligence information. Requesters integrate the intelligence into their decision-making and planning processes, and technical barriers to rapid integration, such as system incompatibility or security barricades, complicate operations. Information superiority requires the timely integration of intelligence with operations in an easily understood format that facilitates decision-making at all levels while at the same time maximizing the amount of relevant information available. In the case of threat warning alerts essential to the preservation of life and/or vital resources, such information should be immediately communicated directly to and acknowledged by those forces, platforms, or personnel identified at risk so the appropriate responsive action can be taken. More generally, the integration of intelligence and operations on a continuous basis allows commanders and all operational planners access to the most current information available, thereby optimizing intelligence support to operation planning, preparation, execution, and assessment functions.

The primary vehicle for integrating intelligence and operations is the common operational picture (COP). Intelligence should be disseminated in such a manner that it can be automatically rendered or visualized in the COP and facilitate a shared operations/intelligence view of the operational environment. The COP is a broad merging of inputs from a wide variety of tactical, operational, and national sources into a single picture that serves a broad set of users for multiple purposes. Wide area surveillance radar systems resident on battle management, command and control (BMC2) platforms such as E-3, E-2, E-8, and CRC form the underlying foundation of the COP. These weapons systems use their organic wide-area surveillance radars to develop battlespace situational awareness for battle managers executing real-time tactical battle management decisions and operations. This information is shared near-real time with other networked shooters, warfighters and intelligence centers through tactical data links. It facilitates decision making and planning at all levels, from Secretary of Defense policy decisions to joint force operation planning. The COP depicts friendly, adversary, and third-party (gray/unknown) force dispositions and contacts on tailored graphical backgrounds. It includes a variety of near-real time friendly and adversary air, ground, space and maritime tracks, threat/warning data, and intelligence broadcasts. The COP provides the means for automatically integrating relevant information and finished intelligence into the graphic—not just electronic intelligence (ELINT) and radar tracks. Annotations should facilitate linkage to order of battle (OB) databases, message traffic, and the ATO. This linkage between imagery and other collateral-level intelligence and operational databases facilitates intelligence analysis, battlespace awareness, operations planning, and assessment by providing intelligence and operations staffs with simultaneous access to the same information.

EVALUATION AND FEEDBACK

After receiving the ISR products, the user evaluates the products to ensure they satisfy the requirement. The user then provides feedback to ISR planners, collection managers, and analysts to ensure the process continues to satisfy the requirement.

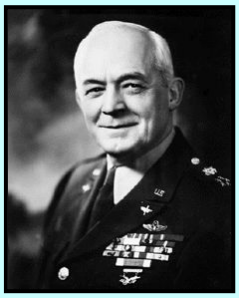
It is imperative that intelligence personnel and consumers at all levels honestly evaluate and provide immediate feedback throughout the intelligence process on how well the various intelligence operations perform to meet the commander's intelligence requirements. All operations in the intelligence process are interrelated and should be evaluated to determine the degree to which they facilitate each other and ultimately succeed in meeting the customer's requirements. For example, planning and direction establish the groundwork for all other intelligence operations, but they are also dependent on the results achieved by other operations in the intelligence process. The collection manager evaluates collection reports, ensures the appropriate requesters receive a copy, and determines, in conjunction with the requesters, if the requirements have been satisfied. Requester feedback establishes customer satisfaction and frees collection assets and resources to be redirected to satisfy other active requirements. Processing and exploitation and analysis and production are evaluated based on the degree to which customers are satisfied that the resulting information or intelligence answers their requirements. Intelligence personnel and consumers at all levels evaluate the quality of intelligence products relative to all the attributes of good intelligence. These attributes include the degree to which intelligence anticipates the needs of the commander, and is timely, accurate, usable, complete, relevant, objective, and available. Finally, intelligence and operations personnel jointly evaluate how well intelligence is disseminated and integrated with operations, and make changes as needed to improve the overall intelligence process.

CHAPTER THREE

ISR ELEMENTS

Strategic air warfare can be neither soundly planned nor efficiently executed without a continuous flow of detailed (intelligence) information....

—General Hap Arnold, USAF

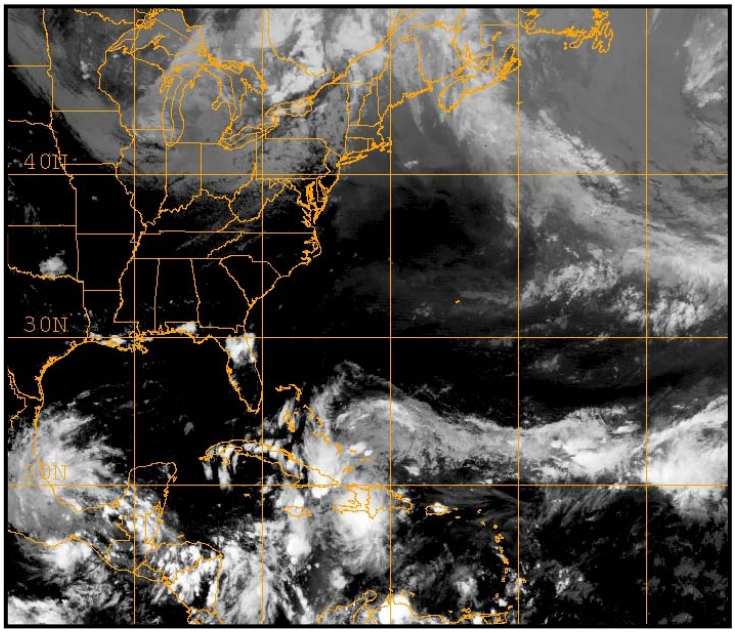


INTELLIGENCE COLLECTION DISCIPLINES

ISR resources collect data that become finished intelligence when processed, analyzed, and integrated. These data can be collected through a wide variety of means. The following is a list of intelligence collection disciplines relevant to Air Force ISR operations.

Geospatial Intelligence

Geospatial intelligence (GEOINT) is defined as exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Imagery intelligence involves the collection of images that are recorded and stored (on film, digitally, on tape, etc.). These images can be used to help identify and locate adversary military forces and facilities and give the commander insight into the adversary's capabilities. GEOINT can also help provide commanders environmental and geospatial information.



Infrared Weather Imagery of the eastern United States

The principal image types are optical literal image and non-optical non-literal image. Optical literal imagery is essentially traditional visual photos (recorded on film, tape, or electronically) using visible light to illuminate the objects photographed. Optical literal imagery uses natural illumination in the portion of the spectrum that humans can perceive unaided. Non-optical non-literal imagery includes infrared, multispectral, and radar imagery.

Both optical literal and non-optical non-literal imagery have advantages and limitations. For example, optical literal sensor systems that use photographic film are not as responsive since a significantly longer time is required to produce a usable image. Infrared, radar, and multispectral sensors detect emissions in the nonvisual portion of the electromagnetic spectrum. However, infrared signatures can be distorted by aerosols, moisture, and other atmospheric gases, much like the optical portion of the spectrum. Radar imagery requires active illumination by a radio frequency pulse; the reflected return provides an image of the target. Radar will work at night and through rain and cloud cover, unlike optical and infrared imagery. Radar imagery can also detect or differentiate moving vehicles using moving target indicator systems. Multispectral imagery uses data collected simultaneously from two or more spectral regions or bands of the electromagnetic spectrum—in other words, the same scene is imaged in several spectral bands at the same time by the same sensor. The resulting image contains more detailed information than can be obtained through the use of only one band.

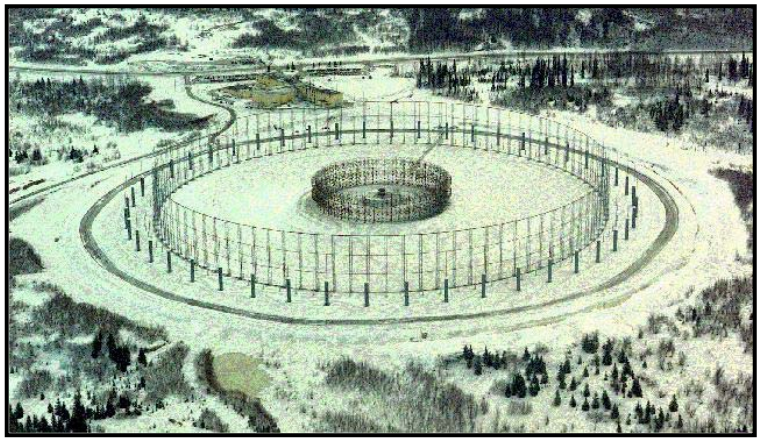
Examples of vertical (left) and oblique imagery

Images can be divided into vertical, oblique, and panoramic imagery. Vertical imagery provides a two-dimensional, overhead view of the target. Oblique imagery provides an angled view of the target area which shows perspective and can be perceived as a three-dimensional view. Panoramic imagery combines the features of both vertical and oblique imagery by scanning from horizon to horizon.

Full-motion video is a new imagery capability that is shortening the sensor-to-shooter cycle by providing the warfighter imagery in real time. Use of full-motion video provided by RQ-1/MQ-1 Predator unmanned aircraft assists commanders in maintaining situational awareness and identification and tracking of targets, and presents the opportunity for our forces to respond as required.

Non-imaging assets also play a key role in GEOINT. Though not as intuitive to the non-intelligence professional, non-imaging assets can provide additional dimensions to an intelligence product. For example, a Defense Support Program (DSP) satellite may provide the first indications of the existence of a previously unlocated rocket test stand (e.g., thermal signature of a rocket engine test). This information, combined with imagery, can reveal much more than either product alone.

Signals Intelligence



SIGINT ground sites remain an important part of global situational awareness.

SIGINT is defined in JP 1-02 as a category of intelligence comprising either individually or in combination all communications intelligence (COMINT), ELINT, and foreign instrumentation signals intelligence (FISINT), however transmitted. More specifically, SIGINT uses intercepted electromagnetic emissions to provide information on the capabilities, intentions, form-actions, and locations of adversary forces. COMINT consists of information derived from intercepting, monitoring, and locating the adversary's communications systems. COMINT exploits the adversary's communications, revealing the adversary's intentions. ELINT consists of information derived from intercepting, monitoring, and locating the adversary's noncommunication emitters. It exploits the adversary's radar, beacon, and other noncommunication signals, allowing friendly forces to locate adversary radars and air defense systems over a wide area. FISINT consists of technical information derived from the intercept of electromagnetic emissions, such as telemetry, associated with the testing and operational deployment of foreign air and space, surface, and subsurface systems. FISINT can provide technical details of foreign weapons system development so US forces can respond quickly to new technological developments.

Measurement and Signature Intelligence

Measurement and signature intelligence (MASINT) is scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived

from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. Examples of MASINT might include distinctive infrared signatures, electronic signals, or unique sound characteristics. MASINT can be collected by ground, airborne, sea, and space-based systems. MASINT can be used to monitor potential adversary technical developments and deployments, as well as emerging weapons of mass destruction (WMD) threats. While MASINT is often used in scientific and technical intelligence (S&TI) products, it is becoming increasingly important in the operational area.

Human Resources Intelligence

HUMINT is the intelligence collection discipline that uses people in the area of interest to identify or provide insight into adversary plans and intentions, research and development, strategy, doctrine, and capabilities. Some examples of HUMINT collection include clandestine acquisition of photography, documents, and other material; overt collection by air attaches in diplomatic and consular posts; debriefing of foreign nationals and US citizens who travel abroad; official contacts with foreign governments, aircrew and ground personnel debriefing, and SOF intelligence collection missions.

Open-Source Intelligence

Open-source intelligence (OSINT) is the intelligence collection discipline that uses information of intelligence value that is available to the general public. Particular sources are newspapers, other publications, radio and television media, and the internet. OSINT processing transforms text, graphics, sound, and video into useable information in response to user requirements. For example, at the national level, the Directorate of National Intelligence (DNI) Open Source Center provides translations of foreign broadcast and print media.

ISR RESOURCES

This section describes the types of resources employed to satisfy information requirements through the ISR process. Many of the systems that provide input to the ISR process are not dedicated ISR resources or systems. System ownership may be less important than the actual information satisfying the consumer's requirements.

Airborne Systems

Airborne systems are among the primary sources of ISR capabilities available to support the joint force's intelligence requirements. These systems have varying, but complementary, operating characteristics and restrictions.

Unmanned Aircraft Systems (UAS)

UAS provide significant advantages over other reconnaissance assets, but commanders must be aware of their limitations. The greatest advantage of these systems is that they normally do not put friendly personnel at risk, can have relatively long loiter times, and are generally less expensive than today's high-value manned assets. UAS limitations vary according to system and operational requirements. UAS technology is maturing rapidly, and platforms can be configured with a broad range of imagery sensors or weapons payloads. Because control authorities and mission priorities can shift between users during multi-role UAS missions, commanders should carefully delineate clear lines of authority (See the section on ISR and multi-role aircraft employment, Chapter 4).

Most UAS are tactical in nature, characterized by specific mission capabilities and relatively small area coverage. A new breed of UAS is designed to expand the capabilities to meet the ever increasing demands for intelligence on today's fast-paced battlefield. The Global Hawk high altitude endurance UAS provides broad area coverage and an extended mission range. With enhanced sensor payloads such as an electro-optical/infrared sensor and synthetic aperture radar (SAR) with moving target indicator (MTI) capability, Global Hawk is a day/night, all-weather reconnaissance system. The 14,000 nautical mile range and 35 hour endurance of the air vehicle, combined with satellite and line-of-sight communication links to ground forces, permits world-wide operation of the system. Sensor data can be rapidly processed, correlated to a geographical grid and merged with live and stored images. Spatial information can be presented over common map displays, showing a detailed multi-dimensional situational picture.

UAS flight paths can be preprogrammed or remotely controlled. Recent campaigns have taught us the value of these assets and new systems are envisioned with even greater capabilities to include signals intelligence sensors. Commanders should understand UAS capabilities to support mission requirements as well as their limitations.

UAS come in all shapes and sizes. While they provide valuable surveillance and reconnaissance capabilities, the proliferation of these assets requires definitive command and control relationships and airspace control.

Manned Platforms

Manned airborne ISR platforms and their associated ground stations generally are among the most responsive assets available. They are capable of carrying out critical missions by collecting vital information in near-real time. Aircrews can recognize and respond to changing conditions and are able to modify missions while they are in progress. With their ability to fly long distances, manned platforms can cover a large area with a mix of sensors. Many of these assets have a common data link between aircraft or with ground stations allowing them to distribute large volumes of information in near-real time. Manned airborne ISR capabilities can be divided into two groups: standoff and penetrating.

During peacetime, the majority of airborne ISR missions are accomplished using standoff techniques. The standoff mode is used during military operations when the threat is too great to allow high value assets to penetrate adversary territory or when overflight of an area cannot be completed due to political sensitivities. The primary advantage of the standoff mode is that assets are relatively free from adversary surface-to-air and air-to-air attacks. The primary disadvantage is the limited range and depth of sensor coverage. An example of an ISR platform that uses standoff techniques is the RC-135 RIVET JOINT. Additional examples of standoff battle management, command and control systems with organic surveillance sensors are the E-8 joint surveillance target attack radar system (JSTARS) and E-3 airborne warning and control system (AWACS). (Refer to the Air Force Tactics, Techniques, and Procedures [AFTTP] 3-1 series for individual systems.)

The JSTARS uses a multi-mode side looking radar to detect, track, and classify moving ground vehicles in all conditions deep behind enemy lines.

If necessary, manned BMC2 and ISR aircraft may, upon proper authorization, penetrate threat areas when the target is beyond standoff range and other systems are not available to provide the required coverage, or when weather conditions are such that standoff systems are ineffective. Standoff systems may penetrate hostile airspace when the threat has been suppressed or when mission priority justifies the risk. Because they are high value assets and exist in small numbers, the main disadvantage of manned ISR systems is

the exposure or potential exposure of personnel and equipment to adversary threats. Like UAS, some manned airborne assets are also susceptible to adverse weather conditions. Other collection capabilities, such as targeting pods on the F-16, will allow under-the-weather imaging in a threat environment. As UAS development continues, manned reconnaissance in hostile airspace will likely be limited to a relatively small set of high priority targets. However, UAS and manned aircraft will continue to be subject to host nation overflight and access restrictions en route to and within the AOR based on international law, custom and practice, and arrangements outlined in the DOD 4500.54-G, *DOD Foreign Clearance Guide*.

Space-based Systems

Space-based ISR systems are an integral part of military forces providing support across the range of military operations. Space systems help provide information to commanders allowing them to quickly assess the situation, develop concepts of operation, and distribute changes to their forces. However, commanders must also be aware of the advantages and limitations of these systems. The prime advantage of these systems is their ability to provide worldwide coverage, especially those remote or hostile areas where little or no data can be obtained from ground and airborne sources. Other advantages these systems possess include mission longevity and relative immunity from adversary action.

While able to provide worldwide coverage, demands on individual space-based systems often exceed their capacity and their associated orbit requirements may limit their ability to meet operational requirements. Space systems are divided into military, nonmilitary, and national systems.

A Titan IVB space launch vehicle carrying a DSP satellite that will add to a constellation of similar satellites the Air Force uses to provide early warning of missile launches worldwide.

Military Systems

Military space ISR systems employ a variety of sensor suites and provide a broad range of capabilities. During peacetime, space systems routinely support activities such as training exercises, peacekeeping operations, indications and warning (I&W), disaster and humanitarian relief efforts, counterterrorism, and counternarcotics operations.

Space-based ISR systems' unique advantage of near global coverage allows commanders to observe areas of interest over great distances and where other ISR systems cannot be employed. Detection and warning sensors provide early detection of ballistic missile attack and downlink this information to the appropriate ground stations, allowing commanders to take the appropriate actions against ballistic missile attack. Environmental monitoring systems are crucial to providing an asymmetric warfighting advantage in which we anticipate and exploit the condition of the atmosphere, oceans, soil, and the space environment in order to support friendly and adversary military operations. Awareness of environmental conditions can be the difference between the success or failure of an operation or mission. Accurate weather forecasting also helps commanders anticipate conditions and exploit weather to their advantage.

Space-based ISR systems can also provide military forces with geographic and detailed terrain information that enhances mission planning capabilities. Additionally, these systems can often cue or be cued by other ISR systems to watch a specific area of interest, enhancing accuracy and reaction times for the users of that information. Finally, space communications support ISR operations by distributing the products generated from ISR systems while navigation systems provide ISR sensors with accurate positioning information.

Nonmilitary Systems

Nonmilitary space systems normally complement military space systems and include civil, commercial, and allied capabilities. These systems possess a variety of capabilities; however, in some cases their availability may be limited. Two examples of these systems are weather and multispectral imagery satellites. Theater commanders may be able to task these systems directly, depending on the terms of share-use agreements with the owners.

National Satellite Systems

National satellite systems are controlled by the US intelligence community and provide support to the President, the Secretary of Defense and the military at all levels. These resources provide critical data and are becoming increasingly responsive to military information needs. National systems provide critical support when aircraft are denied access or when access is limited by the capability or range of other systems.

Ground-based Systems

Air Force ground-based ISR systems are not limited to traditional intelligence collection architectures. They also include the space surveillance network (SSN), the ground-based missile warning sensor system, and those systems used by the theater air control system (TACS) for battle management, airspace management, aircraft control, and surveillance.

Missile Early Warning System—Ground-based collection can come from many sources.

Other ground-based "systems" include SOF and other HUMINT collection capabilities. Normally, these systems are not tasked as ISR assets but provide surveillance information as a by-product of their primary mission.

Traditional Ground-based Collection

Ground sites around the world are equipped and tasked to collect information within any of the disciplines previously described (e.g., SIGINT, MASINT, etc.). These sites may satisfy national, theater, or local information requirements, or any combination of these.

- Air Surveillance and Acquisition Radars. Ground-based surveillance systems used to control the movement of aircraft provide a degree of warning and control over air resources within a designated airspace control area. Examples of these systems are ground control intercept (GCI), early warning radars, and tracking and acquisition radars. The advantage of these systems is that they provide an additional layer of control and observation that may not be available with other surveillance systems. Although some ground-based GCI systems are highly mobile, one of the primary disadvantages is their lack of mobility. Also, some of the ground-based warning sensors have unique sensor limitations and are susceptible to adverse atmospheric conditions. In addition, air defense sensors are limited to line-of-sight surveillance.

- Missile Warning and Space Surveillance. Significant ground-based ISR resources are the SSN and ground-based missile warning sensor system. The SSN's purpose is to find, fix, track, and characterize manmade objects in space. An example of an SSN system is the ground-based electro-optical deep space surveillance (GEODSS)

system. SSN data are used to help determine adversary space OB, adversary satellite overflight warning, and adversary satellite status. This information is available to theater commanders. Although ground-based missile warning sensors primarily provide missile warning and attack assessment of a ballistic missile attack, they also contribute to space surveillance. One example of this type of system is the ballistic missile early warning system. The SSN and ground-based missile warning sensors can provide advance notice of hostile over flights to theater commanders. Combatant commanders or JFCs may be called upon to protect these systems from adversary attack within their AOR.

Human Intelligence Sources

Despite the sophistication of long-range sensors and overhead platforms, there are circumstances in which the precision, timeliness, or access requirements (e.g., underground facilities) for reporting critical information requires a skilled eye on the target. Following are some forms of human-resourced information of ISR value.

- Dedicated HUMINT Collectors. Dedicated human resources may be tasked to support theater commanders or national-level agencies. Dedicated HUMINT collectors can also contribute information to the overall ISR picture and can often amplify, clarify, or verify information collected by other airborne, ground-based, or space-based assets. In many cases, HUMINT, along with counterintelligence activities, are the best and only sources of adversary intentions. The Air Force currently relies primarily on DOD and other national-level agencies to provide operational and strategic HUMINT support.

SOF can provide valuable HUMINT to commanders.

- Special Operations Forces. SOF conduct special reconnaissance (SR) operations to obtain or verify information about adversary capabilities, intentions, and activities, or to gather data about meteorological, hydrographic, or geographical characteristics of an area. SR operations complement national and theater ISR resources by obtaining specific, time-sensitive information of strategic and operational significance. SOF have technically knowledgeable observers who may be able to verify critical information about targets or target complexes. These observers attempt to defeat adversary deception efforts and transmit a more complete picture of what is happening at the target area.

- Aircrews and Ground Personnel. Human visual surveillance and reconnaissance are the most basic and the oldest methods of intelligence gathering. Today, visual surveillance and reconnaissance information come from a wide range of sources and often simply entail observer reporting and debriefing activities. While there are some limitations, observers can include aircrews flying any type of aircraft or SOF conducting assigned missions as described above. Additionally, information gained from onboard aircraft systems such as weapon system, video, and defensive countermeasure suites can provide invaluable ISR information during operations. Security forces, explosive ordnance personnel, and other Airmen who operate outside the base perimeter are also sources of information that are of intelligence value.

Combat Camera supports DOD and Air Force senior leadership.

- Combat Camera. While not a dedicated ISR asset, Combat Camera and their products can play a significant role in the fusion process or in providing graphic support to intelligence assessments. The mission of Combat Camera is to support DOD and Air Force senior leadership with timely and informative visual imagery that will enhance their daily operational decisions and assessments during both combat and peacetime contingencies. Combat Camera technicians operate still and video imagery systems that can distribute images within a six-hour response time.

Non-Traditional ISR Resources

When developing collection plans, to include addressing immediate operational environment needs, collection managers should keep in mind that available resources are not limited to platforms or sensors that were specifically designed to collect intelligence. Ground based radars for GCI, early warning, tracking, and acquisition are used to control the movement of aircraft and provide a degree of warning within designated airspace. The air picture they provide can be simultaneously exploited for real-time data of potential intelligence value. With the increasing sophistication of airborne sensors, many, if not all, aircraft can conduct reconnaissance or surveillance to varying degrees, even if intelligence collection is not their primary mission. Some examples of non-traditional capabilities include F-16 tactical airborne reconnaissance systems, F-16CJs collecting SIGINT, F-15Es collecting imagery via their targeting pods, and AC-130s using video capabilities to monitor a particular building. Understanding how to integrate these capabilities into the collection plan is increasingly important, as traditional intelligence collection-only assets can rarely satisfy all collection requirements. Typically, collection managers will not be able to directly

New systems, like the F-22, are designed with sensors that collect valuable intelligence.

task such assets, and will need to coordinate with operations personnel in the strategy, combat plans, or combat operations division of the AOC to do so. As such, collection managers should understand the broad range of collection capabilities associated with such aircraft and, based on this knowledge, articulate the intelligence these assets can provide. Depending on the operation, these assets can be called upon to provide a wide range of intelligence collection support, from providing GEOINT for IPOE, collecting post-strike intelligence for assessment to performing ad hoc collection for emerging threats. The availability of these assets may be haphazard, at best, and collection managers should have knowledge of the current operational environment to take advantage of these capabilities when they become available. ISR professionals may require additional training and on-the-job experience in order to gain the greatest benefit from these capabilities.

Tasking, Collecting, Processing, Exploitation, and Dissemination Systems

Many of the ISR systems mentioned above send the data they collect to tasking, collecting, processing, exploitation, and dissemination (TCPED) systems. The Air Force's primary TCPED system is the AF DCGS, a network-centric, global enterprise designated as the Air Force AN/GSQ-272 SENTINEL ISR weapon system. It is tasked and managed to support CCDRs and forces—primarily at the JTF level and below—with actionable, decision-quality information in accordance with established priorities as approved by the Secretary of Defense via the Joint Chiefs of Staff deployment order process. It operates with the full flexibility of the established intelligence process, as detailed in JP 2-01, *Joint and National Intelligence Support to Military Operations*, in order to make usable information immediately and simultaneously available to both engaged forces and intelligence analysts. AF DCGS takes advantage of Air Force, sister-Service, national, and coalition sensors in the air, on land, in space, and at sea spanning multiple intelligence (multi-INT) sources and provides tailored, correlated information to those who need it in the formats, timelines, and channels they need it, at all levels across the globe in peace and in combat. It is scalable and comprised of fixed and deployable total force components capable of forward-based activities and robust, full-scale reachback operations. AF DCGS is a component of the larger DOD DCGS enterprise.

PRODUCTS

Intelligence products can be used in a variety of ways to support national-level decision makers, theater commanders, and individual warfighters. In a general sense, situational awareness (SA) is a major goal of ISR operations. SA is provided at a number of levels. For example, it could mean passing direct threat warning information to a pilot in near-real time or providing a combatant commander with a comprehensive picture of the AOR's operational environment. Information must be communicated to be effective. Intelligence can be tailored through formal reporting methods, informal or formal briefings, memos or background papers, annotated imagery, graphic or video presentations, dynamic databases, and near-real time displays. Dissemination of

intelligence products depends on the commander's requirements and, to a lesser extent, on the kind of information communicated. For example, it may be best to present current intelligence with a formal or informal briefing instead of a written product, whereas technical intelligence may be best presented as a written document. Below are some of the capabilities, processes, and products that contribute to SA at all levels and highlight the ISR contribution to Air Force forces.

Indications and Warning (I & W)

ISR performs vital I&W functions. Through continuous surveillance or as required reconnaissance, ISR provides timely and near-real time information necessary to assess potential threats to the US and its allies. The space-based infrared system which detects missile launches is one example of continuous surveillance.

I&W products are derived from a worldwide I&W system that analyzes and integrates operations and intelligence to assess the probability of hostile actions, and provides sufficient warning to preempt, counter, or otherwise moderate their outcome. I&W systems rely on tip-offs from sources at all levels. An integrated and responsive intelligence architecture should be established to satisfy theater requirements. The focus of I&W products varies at each echelon and is most specific at the operational and tactical levels. In general, I&W products focus on the following:

- ✪ Emerging crisis situations and foreign government responses to them.
- ✪ A potential adversary's politico-military intentions, past behaviors, motivations, and doctrine.
- ✪ Significant political, economic, or social situations that could lead to crisis-triggering events in both friendly and adversary states.
- ✪ Changes in adversary force dispositions, military activities, and mobilization status.
- ✪ Adversary information operations capabilities in the region.
- ✪ Key civil or bureaucratic activities that suggest follow-on military activity.
- ✪ Status of other military forces in the AOR or operations.

Current Intelligence

Current intelligence involves producing and disseminating all-source intelligence products on the current situation in a particular area or on activities of specific groups. It is similar to I&W in that both depend upon continuous monitoring of world events and specific activities in an AOR. Information required to produce current intelligence products includes, but is not limited to, the following:

- ✪ Adversary intentions, capabilities, and will to use military force.

- ✪ Potential adversaries' centers of gravity, operational plans, and vulnerabilities.
- ✪ Geographic, environmental, and social analysis of the operational area.
- ✪ Current and forecasted weather conditions that affect potential operational areas.
- ✪ Significant military and political events.
- ✪ Status of strategic transportation nodes (major airfields, seaports, and surface networks).

The information gained during development of current intelligence forms the basis for the general military intelligence (GMI) effort and other analytical products. Conversely, GMI provides the threat backbone through OB, tactics, technology, etc., for producing accurate and meaningful current intelligence.

General Military Intelligence

Current intelligence and GMI efforts are interdependent. GMI produces information concerning the political, economic, and social aspects of foreign countries as well as all information on the organization, operations, and capabilities of selected foreign military forces or groups. GMI products can be tailored to specific air and space force missions. For example, some GMI products support operational planning, while other products may support Air Force modeling and simulation or acquisition efforts. Here are some examples of GMI products:

- ✪ Military-related Infrastructure Assessments. These assessments can provide detailed indicators of an opposing force's capabilities and vulnerabilities, including its warfighting sustainability. Examples include assessments on adversary C2 systems, defense industries, energy production and distribution networks, and transportation systems.
- ✪ Military Capabilities Assessments. Determining the adversary's potential military capability includes identifying forces and dispositions, evaluating their vulnerabilities, and assessing their ability to employ military force to counter friendly force objectives. Specifically, military capability assessments focus on adversary leadership and C2, orders of battle, readiness, sustainability, and technical sophistication.

Situational Awareness

A number of dissemination systems provide near-real time and real time threat, target and friendly status to the JFACC, operational units, and other operators. Air Force surveillance and reconnaissance systems will contribute to building a common operating picture in all domains—land, air, sea, space, and cyberspace. Information from various intelligence disciplines may be fused to form the threat picture. The threat picture can be conveyed to tactical users via audio, video, or data links. In the current

environment of rapidly improving technologies, having the capability to provide rapid, accurate, and timely information is vital.

Intelligence Preparation of the Operational Environment

IPOE is a systematic continuous process of analyzing the threat and environment to help the commander better understand the operational environment. The IPOE methodology is an effective analytical process used during peacetime and during hostilities at all levels of command.

IPOE is a valuable methodology for focusing intelligence on the commander and the commander's supporting C2 elements. IPOE facilitates getting "inside" the enemy's decision-making cycle. Specifically, IPOE focuses on the interrelationship between the threat and environment and the effect of that interaction on both friendly and enemy courses of action. IPOE results in the production of adversary courses of action, named areas of interest, and high-value targets, which are inputs to the JFACC planning, intelligence collection, and targeting processes. Additional advantages of the IPOE process include integrating analysis, collection management, and targeting processes, as well as providing a standardized analytic approach for training purposes. Air Force intelligence entities at all levels of command should use IPOE principles, focusing on environmental and threat characteristics and activities that significantly influence Air Force operations.

Defense and Penetration Analysis

Defense and penetration analysis provides the basis for detailed mission planning and defense suppression, as well as for assessments of friendly force vulnerabilities. For example, intelligence personnel analyze adversary force capabilities to penetrate or operate over or within friendly territory.

Scientific and Technical Intelligence (S&TI)

S&TI products address foreign scientific and technical developments that have warfare potential. These developments include weapon system characteristics, capabilities, vulnerabilities, limitations, and effectiveness; research and development activities related to those systems; and related manufacturing information. ISR-generated S&TI products play a vital role in the acquisition process by allowing the acquisition community to develop new systems or upgrade existing ones to meet current, developing, and potential future threats.

Target Intelligence

ISR operations play a prominent role in the targeting cycle by detecting, locating, and identifying targets, as well as supporting mission planning and assessment. Successful employment of precision munitions against mobile targets often requires near-real time targeting information.

Detection is an ongoing process using surveillance and reconnaissance assets to identify potential targets or significant changes to existing targets. Once detected, a

target should be accurately and precisely located within a designated geospatial reference system.

Identification involves recognizing and classifying targets in sufficient detail to give commanders the ability to make informed decisions on targeting and tactics. Multiple surveillance and reconnaissance missions may be necessary to identify and verify a target. ISR assets can provide the level of detail necessary to support the precision engagement of specific high-value targets.

Examples of targeting production requirements include target threat characteristics and vulnerabilities, adversary capabilities and intentions, adversary centers of gravity, analysis of IW and other non-lethal weapons, and precise target location information and target signatures. Target intelligence products also include current imagery and geospatial information.

Advances in technology have increased the capability for intelligence to be passed directly to the cockpit ("sensor-to-shooter"). For example, RC-135 RIVET JOINT can provide threat information to aircraft performing both counterair and counterland missions. Target imagery can be provided directly to the same aircraft. To effectively use target information, commanders and planners should ensure proper procedures and systems are in place.

Assessment

Assessment is not strictly an ISR responsibility, though ISR forces play a leading role. Assessment encompasses all efforts to evaluate effects and gauge progress toward accomplishment of actions, effects, and objectives. It also helps evaluate requirements for future action. It helps answer several questions: “What happened and what is its impact?” “How is the conflict going?” and “What needs to be done next?” In an effects-based approach, it is not possible to think about actions and their effects without considering how accomplishment of those effects should be measured. Effects and objectives should always be measurable and planning for them should always include a means of measurement and evaluation. It is important to understand assessment as an integral component of the air and space tasking cycle to help define the direction and emphasis of the campaign. Assessment is an inseparable and integral component of the effects-based approach to operations.

Any comprehensive view of assessment should tie evaluation of progress at the tactical level to all other levels of war. An effective assessment construct should also support commanders’ objectives at all levels, support commanders’ decision cycles in real time, and provide the basis for predictive analysis. The proper focus of assessment conducted by the JFACC should be at the operational level of war. An effective assessment construct should address the entire spectrum of operations and all levels of war, permit component validation of assessment elements, focus on effects, standardize federated intelligence support, utilize intelligence specialties effectively, and integrate analysis efforts to the maximum extent possible. This suggests a four-tiered approach that is illustrated in Figure 3.1 and explained further below.

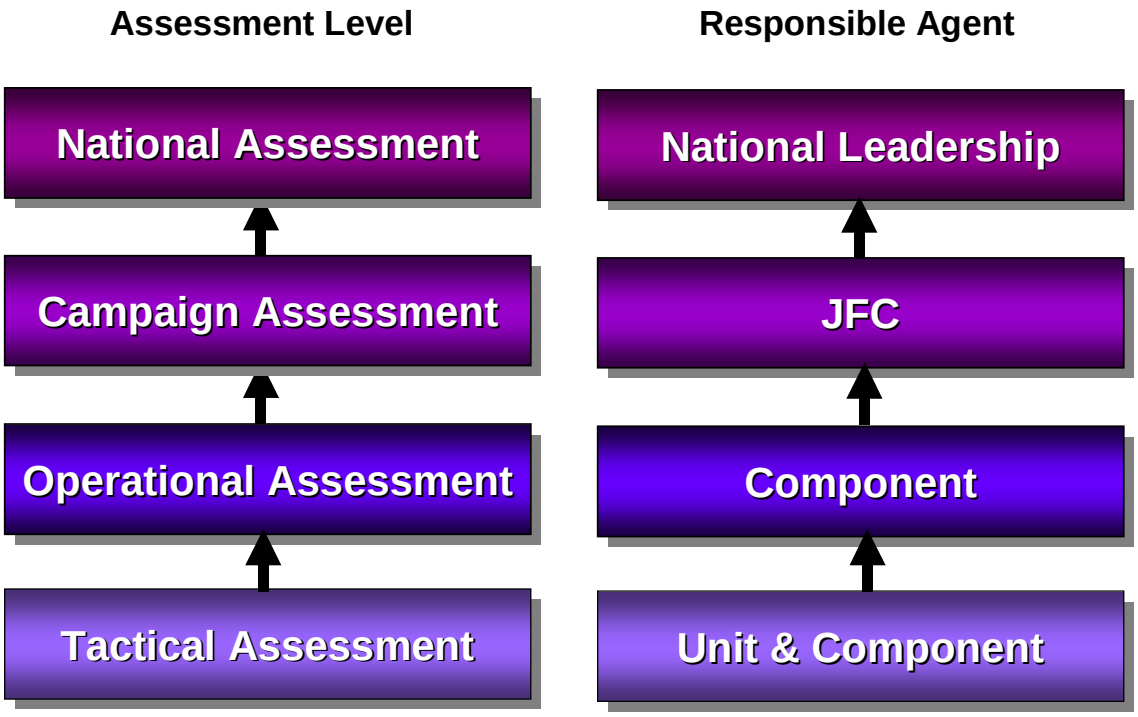


Figure 3.1. Four Levels of Assessment

The Four Levels of Assessment

Assessment consists of four distinct but interrelated levels:

- Tactical Assessment: Determination of the effectiveness of kinetic and non-kinetic tactical military operations through empirical and objective methods.
- Operational Assessment: Evaluation of effects generated by tactical actions and other operational environment influences toward achieving component operational objectives and recommendations for future action. Usually conducted for the JFACC at the AOC by the strategic division's operational assessment team, manned by a mix of operational, ISR, and analysis subject matter experts.
- Campaign Assessment: The JFC's broad qualitative and analytical determination of the overall effectiveness of military operations and recommendations for future action.
- National Assessment: Broad review of the effectiveness of national security strategy and whether national leadership's objectives for a particular crisis or contingency are being met.

For a more detailed description of assessment, see AFDD 2-1.9, *Targeting*.

CHAPTER FOUR

COMMANDING, ORGANIZING, AND EMPLOYING ISR FORCES

Experience in combat theaters has proven the requirement for centralized control by the air commander, of reconnaissance aviation….

—Field Manual 100-20
Command and Employment of Air Power, 1943

Allied "AOC" at Uxbridge, England 1944

Typical AOC Today

COMMAND RELATIONSHIPS

Command relationships delineate the degree of authority commanders have over forces. This chapter discusses ISR command relationships from the combatant commander, JFC, JFACC, COMAFFOR, and national perspectives. Refer to AFDD 2, *Operations and Organization*, for a detailed discussion of command relationships.

The Combatant Commander's Role

The combatant commander employs assigned and attached ISR forces to achieve national and theater objectives. When airborne ISR assets arrive in theater, OPCON may be delegated to the COMAFFOR. The combatant commander is responsible for employment of these assets, to satisfy national, theater, and outstanding component requirements. If necessary the combatant commander will coordinate with other combatant commands to utilize ISR assets not normally assigned to his/her theater, or coordinate the cooperative use of assets to improve coverage. Based on guidance and direction from the combatant commander, the combatant commander's J-2 staff develops an overall collection strategy and posture for the execution of the ISR mission.

The Joint Force Commander's Role

The JFC employs forces attached to the JTF to achieve campaign objectives. The JFC may retain OPCON authority over ISR assets or delegate it to the COMAFFOR. The JFC's staff develops an overall collection strategy and posture for the execution of the ISR mission in coordination with national agencies. The JTF J-2 reviews, validates, and prioritizes all outstanding intelligence requirements, whether originating from the JTF J-2 staff or a component**. The JFC normally delegates OPCON to the COMAFFOR or TACON to the JFACC of airborne ISR assets who will task them to support combat operations via the ATO.**

The Joint Force Air and Space Component Commander's Role

The authority and command relationships of the JFACC are established by the JFC. Normally, the JFACC serves as the supported commander for theater airborne reconnaissance and surveillance and provides integrated ISR for the JFC. The JFACC will exercise TACON authority, as delegated by the JFC, of all Air Force forces assigned or attached to the joint force air component, and over those assets made available for tasking by the other Services. In general, the JFACC's responsibility is to satisfy the JFC's requirements. If the JFACC does not have the available assets or capabilities on hand to satisfy these requirements, the ISR division within the AOC will identify unfulfilled information requirements and forward them to higher headquarters for resolution. Regardless of how the information is eventually gathered, it is imperative the JFACC remains aware of all available surveillance and reconnaissance capabilities that can be integrated into air, space, and information operations

The COMAFFOR’s Role

Through the Forces For Unified Commands memorandum, each combatant commander is assigned a COMAFFOR. As the Service component commander, the COMAFFOR is under the combatant command (COCOM) of the combatant commander to whom he is assigned and directly responsible to that combatant commander for missions and functions that may be assigned to the Air Force component. The combatant commander should normally delegate OPCON over assigned and attached Air Force forces to the COMAFFOR, who also holds administrative control (ADCON) authority over Air Force forces through the Service chain. If the JFC elects to designate an Air Force officer as the JFACC, the COMAFFOR, as the Service component commander with the preponderance of air and space assets and the ability to effectively command and control joint air and space assets, will be dual-hatted as the JFACC and will exercise authority through a joint or combined air and space operations center. The JFACC should normally be the supported commander for theater airborne reconnaissance and surveillance, as well as the area air defense commander, and the airspace control authority. These functions demand integration to ensure unity of command and effort.

National Support

National and non-DOD ISR resources are not a part of the JFC's OPCON authority. These resources may provide support to the JFC or one of the components, either full-time or on-call, but are normally shared with other commands, components, or government agencies. The supported commander will be provided liaison teams upon request, such as the NIST. The NIST mission is to provide national level, all-source intelligence support throughout the intelligence community to deployed commanders during crisis or contingency operations. NISTs are comprised of intelligence and communications experts from DIA, CIA, NGA, NSA, and other agencies as required. These teams will normally be the points of contact for coordinating their specific ISR resources and associated capabilities with the supported commander's collection managers. Collection managers forward the requirements to the appropriate command authority for action. In the event of war or periods of crisis, the President may direct the military to exercise greater responsibility for tasking of collections systems. National intelligence collection tasking authority may pass from the Director of National Intelligence to the Secretary of Defense. The JFC may request CMA from the Secretary of Defense and SIGINT operational tasking authority (SOTA) from the Director of the National Security Agency if required to carry out missions assigned to the command.

ORGANIZATION AND EMPLOYMENT

The AOC is the best location to integrate the JFC's theaterwide airborne ISR capabilities, to include reachback and distributed operations ISR support. AFDD 2, *Operations and Organization*, states that one of the responsibilities of the AOC is to plan, task, and execute the theater airborne ISR mission. Subtasks of this responsibility include:

- ✪ Identify and manage JFACC requirements.
- ✪ Manage JFC (theater-level) requirements in conjunction with other Service components and with validation from the JFC.
- ✪ Integrate and synchronize use of air and space assets.
- ✪ Task theater airborne ISR assets to satisfy the JFC's requirements.

JP 3-30, *Command and Control for Joint Air Operations*, states the responsibilities of the JFACC include "planning, coordinating, allocating, and tasking assigned airborne ISR assets to accomplish and fulfill JFC tasks and requirements." Whenever joint and Service mission needs dictate, it is more advantageous to the warfighter to train, equip, organize, and operate centralized ISR under the JFACC and within the AOC structure. The JFACC can best support ISR operations in strategy development and can best execute the planning, tasking, and direction of ISR missions.

Role of the Air and Space Component's A-2

As the Air Force Service component commander for the joint force, the COMAFFOR is responsible for presenting Air Force ISR capabilities to the JFC. The COMAFFOR's A-2 directs Air Force intelligence forces by recommending policy and guidance and ensuring coordination among various intelligence functions. The intelligence structure should be designed to expedite tailored intelligence to operational units. The A-2 exercises day-to-day responsibility for intelligence support to the COMAFFOR and assigned/attached Air Force forces. This includes the following:

- Serves as Air Force forces senior intelligence officer. Advises the COMAFFOR on all intelligence matters impacting mission accomplishment. Recommends Air Force intelligence policy and guidance for operations within the JOA.
- Establishes, coordinates, and monitors AFFOR ISR requirements and capabilities to support operations in the JOA. Coordinates and monitors JFC ISR requirements.
- Coordinates with JFC staff to establish relationships governing federated ISR operations and distributed operations in theater.
- Validates unit intelligence and systems requirements and manages fielding and operation of automated intelligence systems.
- Participates in the contingency planning processes and development of Annex B, Intelligence; Annex M, Geospatial Information; and Services annexes to OPLANs, CONPLANs, and operation orders (OPORDs). Assists the A-3 in developing the COMAFFOR's CCIR by developing PIRs.
- Coordinates the COMAFFOR's current intelligence and situational awareness support, to include briefings and situation report inputs.
- Coordinates with allied/coalition host nations regarding support systems and intelligence infrastructure.
- Plans intelligence architecture support to satisfy Service-specific weapon system employment requirements in accordance with theater/JOA operations plans.
- Establishes procedures for and manages theater/JOA production requests and RFIs. Validates, prioritizes, and sources unit requirements for intelligence information.
- Establishes, conducts, and maintains liaison with Air Staff A-2 and national intelligence community organizations.
- Supports the threat working group and force protection working group providing threat warning, threat analysis and defensive measures recommendations

Role of the ISR Division

The ISR division (ISRD) within the AOC is responsible for effectively orienting the COMAFFOR and AOC to current and emerging enemy capabilities, threats, COAs, and COGs with predictive and actionable intelligence, and to provide the JFACC with ISR operations management and targeting intelligence support. Within the AOC, the ISRD provides information crucial to the air mobility, strategy, combat plans, and combat operations divisions that are planning and executing theater-wide operations. This information helps accomplish the commander's objectives as well as provides the means by which the effects of the operations are measured. Figure 4.1 shows the organization of the ISRD within the AOC and its responsibilities, including:

- Providing analyses of the enemy and a common threat picture to the JFACC and staff planners, other AOC divisions and other Air Force elements in theater.
- Providing, in conjunction with the strategy, combat plans, and combat operations divisions, for planning and executing airborne ISR operations and providing combat ISR support assessment activities for air, space, and information operations planning and execution.
- Directing the AOC's distributed and reachback ISR processes by working with the JTF, national agencies, Air Force organizations, and the TCPED architecture to optimize ISR contributions to the effort.
- Providing direct targeting support to the ATO cycle in response to JFACC guidance.
- Providing all-source intelligence support to other AOC divisions to enhance the execution of their core processes.
- Ensuring actionable, decision quality, all-source IPOE and threat information depicted in the JFACC and AOC picture of the operational environment is consistent with that used by national, joint, component, and theater entities. Aggressively acts to resolve significant differences.
- Ensuring Air Force ISR is optimally managed to operate within the context of large and complex national and joint intelligence architectures. Serves as the focal point for multiple nodes to work together in order to meet the high demand for information.
- Serving as the senior intelligence element of the TACS, to integrate ISR platforms and other Air Force ISR elements external to the AOC in support of the joint force.

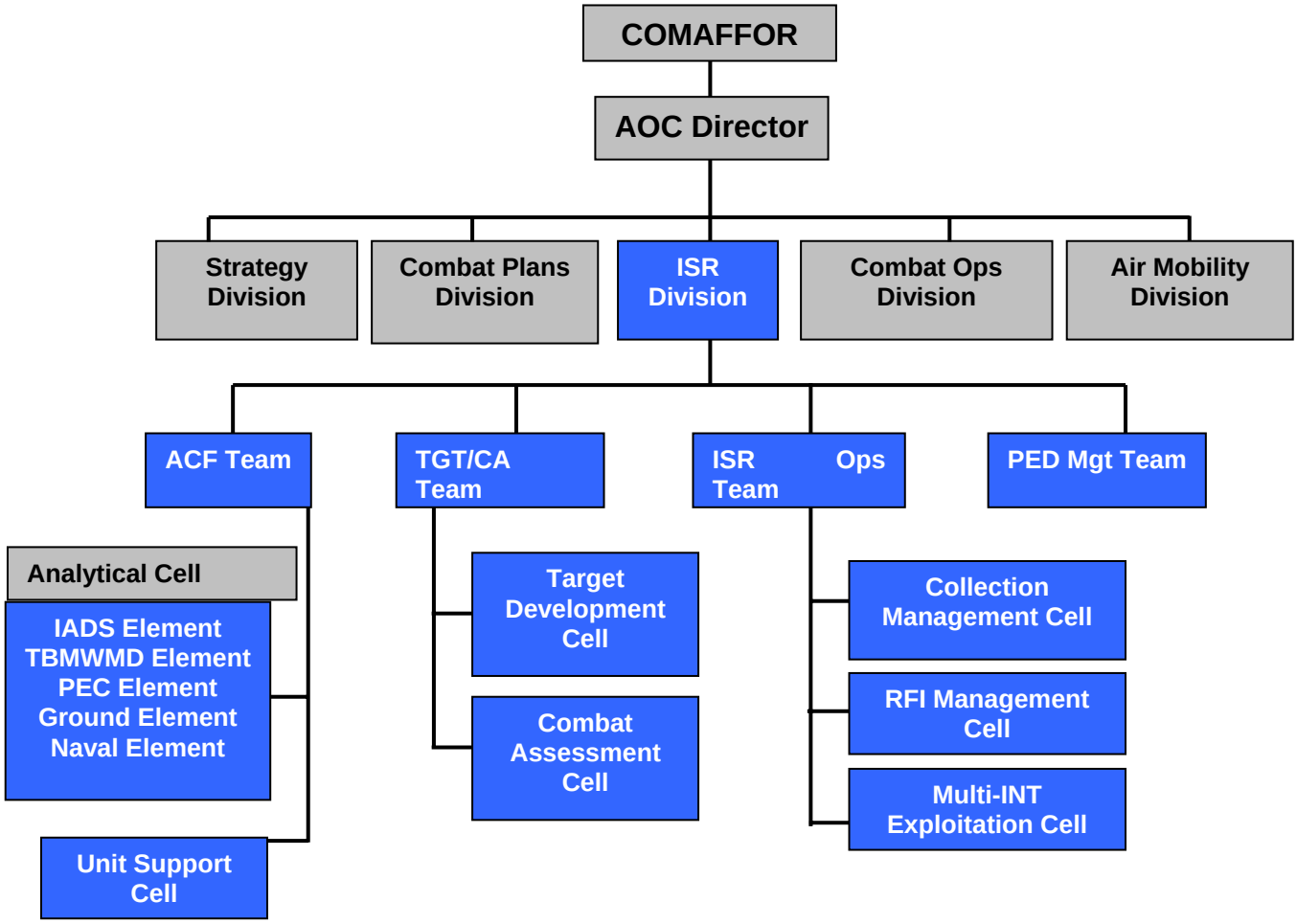


Figure 4.1. The ISR Division's Core Teams

ISR Authorities

Various military missions may be operating within a single AOR that require ISR support. While modern ISR capabilities provide the flexibility to distribute direction and control to a number of users, this flexibility creates challenges for command and control that are not addressed by the basic command relationships described in JP 1, *Doctrine for the Armed Forces of the United States*. This section provides definitions, derived from basic command relationships, for authorities associated with direction and control of ISR operations.

Operational missions in theater vary in composition. If there are needs for more than one service or joint component, a JTF may be established in theater and the JFC may be delegated OPCON over forces attached or assigned. Most often, joint forces are organized with a combination of Service and functional component commands and subordinate task forces with operational responsibilities. The theater J-2 should remain informed of all intelligence collection requirements being levied on assets and resources

within the combatant commander's AOR. The theater J-2 retains full management authority (i.e., to validate, to modify, or to nonconcur) over all intelligence collection requirements within the AOR. This authority may be delegated to a subordinate JFC. The JFC, if allocated a specific set of ISR assets from the combatant commander, will be delegated the necessary authority to employ these assets. However, tasking and employment of any ISR asset required to support more than one JTF commander will be coordinated and deconflicted by a common superior commander to the JTF commanders.

CMA is the authority to determine the priority, focus, and weight of ISR efforts across multiple theater missions and tasks by validating theater collection requirements, establishing sensor tasking guidance, and developing theater collection plans. Commanders delegated OPCON over ISR forces may or may not assume CMA of tasking these ISR assets as part of the delegation of authority. Even if a commander has CMA, it does not necessarily mean that CMA extends to authorities over all theater SIGINT ISR assets. CMA usually includes authority to task ISR GEOINT sensors and lower echelon SIGINT collection systems that have more localized collection capabilities. NSA still retains authority over the tasking of strategic-capable SIGINT ISR systems unless the combatant commander has specifically requested and received SOTA over theater-wide capable platforms and sensors. The delegation of SOTA to the combatant commander and subsequent delegation of this authority to the JFC ensures the theater has the ability to prioritize requirements and focus SIGINT collection where it is needed to carry out the mission assigned to the command.

CRM and validation of collection requirement requests for a theater resides at the combatant command level. CRM focuses on the requirements of the customer, is all-source oriented, and advocates what information is necessary for collection. The COM process organizes, directs, and monitors the equipment and personnel that actually collect the data to satisfy requirements. COM develops strategies for collection against requirements in cooperation with CRM; predicts how well a system can satisfy requirements; evaluates the performance of the collection systems; allocates and tasks collection assets and/or resources and processing and/or exploitation systems; and monitors and reports the operational status of collection systems. The COM process is directly linked to collection plan execution through ISR visualization.

JFCs exercise control over an impressive array of organic and attached intelligence collection and analysis resources. Nevertheless, these alone will not be capable of satisfying all the joint force's information requirements. Some theater missions may require ISR resources not organic to the theater or to the components of the subordinate joint force. ISR resources are typically in high demand and requirements usually exceed platform capabilities and inventory. The joint force J-2 relies on both theater and national intelligence organizations for support in order to provide the JFC with the most accurate intelligence possible. Collection requirements should be satisfied at the lowest possible level. Requirements that cannot be satisfied, and that have been validated by the command's collection manager or J-2, should be forwarded to the next higher echelon for action. This process continues until the

requirement is satisfied, the intelligence is no longer needed, or it is determined that the requirement cannot be satisfied. Validated collection requirements and collection requests for theater and national systems will be forwarded for action to the combatant command theater intelligence CMA. Validated collection requirements from components will become part of the theater collection plan and will be collected by theater collectors or forwarded to the combatant command for national collection consideration and prioritization.

The combatant commander may delegate OPCON or TACON over some theater ISR assets to the JFC. The combatant commander, however, retains the authority to validate and prioritize requirements that will be collected by theater ISR assets not provided to the JFC, and for all requirements forwarded for national collection consideration. The portion of the ISR planning process whereby the JFC identifies all theater and national collection requirements to the combatant commander is when the JFC briefs a draft ISR collection plan to the combatant commander at the joint collection management board (JCMB). The product resulting from this board is a validated multi-source theater collection plan, consisting of collection requirements that are allocated to multiple theater and national collection platforms and sensor capabilities. The requirement allocation effort is usually a JFC-delegated task, performed by the JFACC, prior to the JCMB. The JFACC is also the joint force component commander responsible for the execution of ISR forces via the ATO and therefore should be delegated TACON over these executing forces in theater. High priority, time-sensitive requirements are identified and pre-validated by the JFC for the JFACC to consider for dynamic retasking during execution of ISR forces. Two significant command and control responsibilities of ISR authorities are employment and organization of assigned forces.

ISR and Multi-role Aircraft Employment

Roles and missions for many Air Force assets have expanded beyond what was envisioned in their initial concept of employment to include a variety of innovative functions, often employed during the same mission. Today it is not unusual to find strike aircraft employed in a non-traditional ISR role, and some traditional ISR assets have become weapons platforms. Whether the aircraft is dedicated to providing ISR for the entire mission or performing ISR during part of the strike mission, the **mission objectives, priorities, and guidance for multi-role aircraft employment and the authority to task the weapon system should be clear and preferably worked out well in advance of mission execution.** The JFACC should ensure the following authorities are defined to ensure clear lines of control during multi-role missions:

- **Aircraft Control:** Organization or individual in authority and technically capable of controlling the aircraft.

- **Sensor Control:** Organization or individual in authority and technically capable of controlling the aircraft sensor.

- **Sensor Tasking:** Organization with the authority to direct sensor control and aircraft control to execute ISR tasking.

An example of a multi-role platform is the Predator. On a single mission the Predator can shift between reconnaissance, strike, surveillance, force protection, and other roles. By defining control authorities, and mission priorities, the shift in employment between different organizations or customers will expedite smooth transitions. While the Predator is used as the example, there are many platforms that have similar capabilities where the same principles would apply.

Modern ISR assets, such as the Predator UAS, present opportunities for control of the aircraft, weapons, and sensors by many different agencies. Proper definition of authorities for direction and control of these assets is critical.

Direct and Reachback Support to JFACC ISR Employment

Much of today's intelligence support comes from dedicated centers of excellence or agencies where intelligence professionals practice the art of discerning adversary intent and capabilities. Though not always forward deployed, commanders can still rely on the fact that they are working diligently to provide the intelligence JFCs need to achieve battlefield dominance.

Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA)

The AFISRA is a forward operating agency subordinate to the Deputy Chief of Staff (DCS), Intelligence, Surveillance, and Reconnaissance (AF/A2). It is responsible for executing AF/A2 responsibilities in intelligence collection, analysis, and production. AFISRA organizes, trains, equips, presents, and integrates all-source intelligence (e.g., SIGINT, GEOINT, MASINT, HUMINT, etc.) full-spectrum capabilities to the intelligence community, and to JFCs through the COMAFFOR. It provides customers at all echelons with multi-source intelligence products, applications, and services and provides intelligence expertise in the areas of SIGINT, IO (to include information protection), acquisition, foreign weapons systems and technology, and treaty monitoring. When Air Force component intelligence requirements exceed the theater's capabilities, AFISRA may reinforce the combatant command with analytical expertise and products.

Additionally, AFISRA's "centers of excellence" provide detailed analyses and products for Air Force and DOD customers. Specific functions of these centers include vulnerabilities and capabilities analysis on foreign air and space weapons systems and organizations; production of tailored, customer-specific products; and support to US weapon treaty negotiations and compliance verification. Other centers provide leadership in IO and ISR-related activities to support operations, campaign planning, acquisition, and testing.

Wing, Group, and Squadron Intelligence Support

The primary focus of ISR at the operational wing, group, and squadron levels is the application of all-source intelligence information to sustain combat air operations. Although the wing's intelligence capability is focused within a flight of the unit's operations support squadron, intelligence personnel and assets are assigned to each operational squadron or may be assigned or attached to other wing staffs. This ISR capability supports unit deployments, readiness training, mission planning, and other wing-level mission execution functions. Most unit-level intelligence organizations are composed of two branches—operational intelligence (also termed "combat" intelligence) and target intelligence. Each performs a specific function. First, operational intelligence keeps the commander and aircrews informed of intelligence matters needed to perform the mission. It maintains intelligence database holdings, provides briefings and training, and helps with mission planning. Second, target intelligence assembles and maintains mission or planning folders with related target planning documentation. Important ISR functions that may be performed at the unit level include:

- Mission planning and IPOE support.
- Air and space expeditionary task force command element intelligence support.
- Defensive threat capabilities and penetration analysis.
- Mission folder construction and maintenance.
- Aircrew target study, threat training, and certification.
- Debriefing, assessment, aircraft weapons system recorded media exploitation, and intelligence reporting.
- EEI and RFI management.
- Maintenance and operation of intelligence databases, systems, and special security office programs.
- Identification of unit support requirements to include identifying, requisitioning, and safeguarding target materials and geospatial data for combat and training missions.

Air Control Squadrons

Air control units provide surveillance, early warning, airspace control, and airborne battle management capabilities for operations across the spectrum of conflict. While these units do not generally produce raw data specifically designed for the ISR process, much of the information generated by these units is germane and useful to the ISR process and can be used in all-source fusion to create a more accurate picture of the operational environment.

Reconnaissance Units

Air Force reconnaissance units collect and process raw data for input into the ISR process. They are responsible for providing national and theater command authorities with a wide array of timely, reliable, high-quality, reconnaissance products. Air Force reconnaissance units train and equip personnel for worldwide employment in situations across the full range of military operations. Reconnaissance products or data generated by these units are often the chief input into the ISR process; additionally, critical, perishable reconnaissance data can also be routed directly to the shooter in near-real time. Reconnaissance data is often fused together with other intelligence to form a variety of ISR-related products that range from I&W products to long-range assessments of adversary capabilities.

Space Operations Units

Space operations units typically operate military and national-level satellites that collect information to support strategic-, operational-, and tactical-level decision making. These units typically generate raw data for intelligence processing. Forward units can access these data through reachback. Space planning products, like reconnaissance products from manned and unmanned airborne systems, are also fused with various other inputs from the ISR process to create intelligence products.

Other Air Force Intelligence Units

Other Air Force intelligence organizations include the intelligence wing, intelligence group, intelligence squadron and intelligence divisions. The intelligence wing manages the planning of all-source intelligence and assists Air Force components in the development of concepts, exercises, and employment of forces to support the full range of military operations.

Air Force intelligence groups perform a variety of functions. Most intelligence groups are collocated with the MAJCOM they support and often manage intelligence infrastructure and programs and perform lower-echelon unit support. Other specific functions may include the production of tailored intelligence for weapons systems acquisition, mission planning and targeting, collection management, logistics and readiness issues, and communications/computer system support. Some groups manage military and civilian personnel actions and programs, while others maintain imagery data bases, develop aircrew training materials, and provide reachback linkage for deployed intelligence units. Finally, some intelligence groups have specific

operational missions that relate to C2; acquisition/research and development; space surveillance; threat warning and technical analysis; and SIGINT-oriented cryptologic and S&TI support.

Intelligence squadrons collect, process, exploit, and disseminate intelligence in response to taskings from national authorities, theater commanders, and the JFACC. Intelligence squadrons conduct various missions including military capabilities and OB analysis, unit support, targeting support, and GEOINT and SIGINT collection, processing, exploitation, and dissemination.

Intelligence divisions provide intelligence support to technology, acquisition, test, and sustainment organizations. Besides supporting operations, as necessary, intelligence divisions: (1) provide special security; (2) make available intelligence production and applications such as for system threat assessments, program protection, and models and simulations; and (3) facilitate access to foreign materiel and geospatial information and services.

Multinational Intelligence Operations

Multinational operations are becoming the norm for military operations, making intelligence-sharing with allies and coalition partners increasingly important. In some multinational operations or campaigns, JFCs will be able to use existing international standardization agreements (STANAGs) (e.g., NATO STANAGs) as a basis for establishing rules and policies for conducting joint intelligence operations. Since each multinational operation will be unique, such agreements may have to be modified or amended based on the situation. A JFC participating in a coalition or alliance should tailor the policy and procedures for that particular operation based on theater guidance and national policy as contained in National Disclosure Policy (NDP) 1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*. NDP 1 provides policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance. The disclosure of classified information is never automatic. Any disclosure should be consistent with US national policy and US military objectives, be done with security assurances in place, present a clearly defined US advantage, and be limited to only necessary information.

At the very Heart of Warfare lies Doctrine…

SUGGESTED READINGS

Air Force Publications

Note: All Air Force doctrine documents are available on the Air Force Doctrine Center web page at https://www.doctrine.af.mil; All Air Land Sea Application (ALSA) documents are available on the their website https://wwwmil.alsa.mil/index.html

AFDD 1, *Air Force Basic Doctrine*

AFDD 2, *Operations and Organization*

AFDD 2-1.9, *Targeting*

AFDD 2-4.1, *Force Protection*

AFTTP 3-3.36, *Information Warfare Planning, Integration, and Employment Considerations*

AFTTP 3-10.1, *Integrated Base Defense*

AFTTP 3-3.60, *Operational Employment - Air and Space Operations Center*

Joint Publications

JP 1, *Doctrine for the Armed Forces of the United States*

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*

JP 2-0, *Doctrine for Intelligence Support to Joint Operations*

JP 2-0.1 *Joint and National Intelligence Support to Military Operations*

JP 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*

JP 2-03, *Geospatial Intelligence Support to Joint Operations*

JP 3-0, *Joint Operations*

JP 3-30, *Command and Control for Joint Air Operations*

JP 3-60, *Joint Targeting*

Other Publications

AFMAN 37-123, *Management of Records*[1]

GEOINT Publication 1, *Geospatial Intelligence (GEOINT) Basic Doctrine,* (National Geospatial-Intelligence Agency), June 2004

[1] Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://afrims.amc.af.mil/

GLOSSARY

Abbreviations and Acronyms

ACF	analysis, correlation, and fusion
ADCON	administrative control
AFDD	Air Force doctrine document
AFISRA	Air Force Intelligence, Surveillance and Reconnaissance Agency
AFTTP	Air Force tactics, techniques, and procedures
AOC	air and space operations center
AOR	area of responsibility
ATO	air tasking order
AWACS	airborne warning and control system
BDA	battle damage assessment
BMC2	battle management, command and control
C2	command and control
CA	combat assessment
CCDR	combatant commander
CCIR	commander's critical intelligence requirement
CIA	Central Intelligence Agency
CMA	collection management authority
COA	course of action
COCOM	combatant command (command authority)
COG	center of gravity
COM	collection operations management
COMAFFOR	commander, Air Force forces
COMINT	communications intelligence
CONPLAN	concept plans
COP	common operating picture
CRM	collection requirements management
DCGS	distributed common ground system
DIA	Defense Intelligence Agency
DNI	Directorate of National Intelligence
DOD	Department of Defense
DSP	Defense Support Program
EBAO	effects-based approach to operations
EEI	essential elements of information
ELINT	electronic intelligence
FISINT	foreign instrumentation signals intelligence
GCI	ground control intercept

GEODSS	electro-optical deep space surveillance
GEOINT	geospatial intelligence
GMI	general military intelligence
HUMINT	human resources intelligence
I&W	indications & warning
IADS	Integrated air defense system
INTSUM	intelligence summary
IPL	imagery product library
IPOE	intelligence preparation of the operational environment
ISR	intelligence, surveillance, and reconnaissance
ISRD	intelligence, surveillance, and reconnaissance division
JAOC	joint air and space operations center
JCMB	joint collection management board
JFACC	joint force air and space component commander
JFC	joint force commander
JOA	joint operational area
JP	joint publication
JTAC	joint terminal attack controller
JTF	joint task force
JS/J2	joint staff/director of intelligence
JSTARS	joint surveillance target attack radar system
MASINT	measurement and signature intelligence
MOE	measure of effectiveness
MOP	measure of performance
MTI	moving target indicator
multi-INT	multiple intelligence
NATO	North Atlantic Treaty Organization
NDP	national disclosure policy
NGA	National Geospatial-Intelligence Agency
NIST	national intelligence support team
NRO	National Reconnaissance Office
NSA	National Security Agency
OB	order of battle
OODA	observe, orient, decide, act
OPCON	operational control
OPLAN	operation plan
OPORD	operation orders
OSINT	open-source intelligence

PBA	predictive battlespace awareness
PEC	pre-authorized engagement criteria
PED	processing, exploration and dissemination
PIR	priority intelligence requirements
PR	personnel recovery
RFI	request for information
ROE	rules of engagement
ROVER	remote operations video enhanced receiver
RSTA	reconnaissance, surveillance, and target acquisition
S&TI	scientific and technical intelligence
SAM	surface-to-air missile
SA	situational awareness
SAR	synthetic aperture radar
SIGINT	signals intelligence
SOF	special operations forces
SOTA	signals intelligence (SIGINT) operational tasking authority
SR	special reconnaissance
SSN	space surveillance network
STANAG	standardization agreement (NATO)
TACON	tactical control
TACS	theater air control system
TBMWMD	tactical ballistic missile weapon of mass destruction
TCPED	tasking, collecting, processing, exploitation and dissemination
UAS	unmanned aircraft system
WMD	weapons of mass destruction

Definitions

administrative control. Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. Also called **ADCON**.
(JP 1-02)

all-source intelligence. 1. Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 1-02)

analysis and production. In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (JP 1-02)

air and space operations center. The senior agency of the Air Force component commander that provides command and control of Air Force air and space operations and coordinates with other components and Services. Also called **AOC** (AFDD 2)

air tasking order. A method used to task and disseminate to components, subordinate units, and command and control agencies projected sorties/capabilities/forces to targets and specific missions. Normally provides specific instructions to include call signs, targets, controlling agencies, etc., as well as general instructions. Also called **ATO**. (JP 1-02)

battle damage assessment. The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called **BDA**. (JP 1-02)

battlespace. The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest.
(JP 1-02)

collection. In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 1-02)

collection asset. A collection system, platform, or capability that is supporting,

assigned, or attached to a particular commander. (JP 1-02)

collection management authority. Constitutes the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater collection plans. Also called **CMA**. (JP 1-02)

collection manager. An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. (JP 1-02)

collection management. In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 1-02)

collection operations management. The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. Also called **COM**. See also collection management; collections requirements management. (JP 1-02)

collection plan. A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02)

collection requirement. An established intelligence need considered in the allocation of intelligence resources to fulfill the essential elements of information and other intelligence needs of a commander. (JP 1-02)

collection requirements management. The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. Also called **CRM**. (JP 1-02)

collection resource. A collection system, platform, or capability that is not assigned or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. (JP 1-02)

combat assessment. The determination of the overall effectiveness of force employment during military operations. Combat assessment is composed of three major components: (a) battle damage assessment; (b) munitions effectiveness assessment; and (c) reattack recommendation. Also called **CA**. (JP 1-02)

combatant command (command authority). The nontransferable command authority established by Title 10 ("Armed Forces"), USC, Section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint commanders and Service and /or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command. Also called **COCOM**. (JP 1-02)

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called **C2**. (JP 1-02)

commander's critical information requirements. Commander's critical information requirements comprise information requirements identified by the commander as being critical in facilitating timely information management and the decision-making process that affect successful mission accomplishment. The two key subcomponents are critical friendly force information and priority intelligence requirements. Also called **CCIR**. (JP 1-02)

common operational picture. A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called **COP**. (JP 1-02)

communications intelligence. Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called **COMINT**. (JP 1-02)

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

critical information. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02)

current intelligence. One of two categories of descriptive intelligence that is concerned with describing the existing situation. (JP 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. See also **counterdeception.** (JP 1-02)

distributed operations. The process of conducting operations from independent or interdependent nodes in a teaming manner. Some operational planning or decision-making may occur from outside the joint area of operations. The goal of a distributed operation is to support the operational commander in the field; it is not a method of command from the rear. (AFDD 2-8)

electronic intelligence. Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called **ELINT**. (JP 1-02)

essential elements of information. The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. Also called **EEI**. (JP 1-02)

estimate. 1. An analysis of a foreign situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and the prospective results of the various actions that might be taken. 2. An appraisal of the capabilities, vulnerabilities, and potential courses of action of a foreign nation or combination of nations in consequence of a specific national plan, policy, decision, or contemplated course of action. 3. An analysis of an actual or contemplated clandestine operation in relation to the situation in which it is or would be conducted in order to identify and appraise such factors as available as well as needed assets and potential obstacles, accomplishments, and consequences. See also **intelligence estimate.** (JP 1-02)

evaluation and feedback. In intelligence usage, continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. See **intelligence process**. (JP 1-02)

exploitation. Taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already achieved.

2. Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. 3. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. See also attack; pursuit. (JP 1-02)

foreign instrumentation signals intelligence. Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. Also called **FISINT**. (JP 1-02)

fusion. In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 1-02)

general military intelligence. Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or multinational military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries; military and civilian command, control, communications, computers, and intelligence systems; military economics, including foreign military assistance; insurgency and terrorism; military-political-sociological intelligence; location, identification, and description of military-related installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence.) Also called **GMI**. (JP 1-02)

geospatial intelligence. The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Also called **GEOINT**. (GEOINT Publication 1)

human intelligence. (DOD, NATO) A category of intelligence derived from information collected and provided by human sources. Also called **HUMINT**. See also human resources intelligence.(JP 1-02)

imagery. Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. (JP 1-02)

indications and warning. Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic

interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to the United States reconnaissance activities; terrorists' attacks; and other similar events. Also called **I&W**. (JP 1-02)

information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

information requirements. Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 1-02)

infrared imagery. That imagery produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared position of the electromagnetic spectrum (approximately 0.72 to 1,000 microns).
(JP 1-02)

intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.
(JP 1-02)

intelligence federation. A formal agreement in which a combatant command joint intelligence center receives preplanned intelligence support from other joint intelligence centers, Service intelligence organizations, Reserve organizations, and national agencies during crisis or contingency operations. (JP 1-02)

intelligence process. The process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. See also analysis and production; collection; dissemination and integration; evaluation and feedback; intelligence; planning and direction; processing and exploitation. (JP 1-02)

intelligence preparation of the operational environment. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the operational environment builds an extensive data base for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the operational environment is a continuing process. Also called **IPOE**. (JP 1-02)

intelligence requirement. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (JP 1-02)

intelligence summary. A specific report providing a summary of items of intelligence at frequent intervals. Also called **INTSUM**. (JP 1-02)

intelligence, surveillance, and reconnaissance. An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. Also called **ISR**. (JP 1-02)

interoperability. 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (JP 1-02)

interpretation. A stage in the intelligence cycle in which the significance of information is judged in relation to the current body of knowledge. (JP 1-02)

joint force. A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. See also **joint force commander**. (JP 1-02)

joint force air component commander. The joint force air component commander derives authority from the joint force commander who has the authority to exercise operational control, assign missions, direct coordination among subordinate commanders, redirect and organize forces to ensure unity of effort in the accomplishment of the overall mission. The joint force commander will normally designate a joint force air component commander. The joint force air component commander's responsibilities will be assigned by the joint force commander (normally these would include, but not be limited to, planning, coordination, allocation, and tasking based on the joint force commander's apportionment decision). Using the joint force commander's guidance and authority, and in coordination with other Service component commanders and other assigned or supporting commanders, the joint force air component commander will recommend to the joint force commander apportionment of air sorties to various missions or geographic areas. Also called **JFACC**. See also **joint force commander**. (JP 1-02) [*The joint force air and space component commander (JFACC) uses the joint air and space operations center to command and control the integrated air and space effort to meet the joint force commander's objectives. This title emphasizes the Air Force position that air power and space power together create effects that cannot be achieved through air or space power alone.*] [AFDD 2] {Italicized words in brackets apply only to the Air Force and are offered for clarity.}

joint force commander. A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. Also called **JFC**. See also **joint force**. (JP 1-02)

joint task force. A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. Also called **JTF**. (JP 1-02)

measurement and signature intelligence. Technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. Measurement and signature intelligence capabilities include radar, laser, optical, infrared, acoustic, nuclear radiation, radio frequency, spectroradiometric, and seismic sensing systems as well as gas, liquid, and solid materials sampling and analysis. Also called **MASINT**. (JP 1-02)

monitoring. The act of listening, carrying out surveillance on, and/or recording of enemy emissions for intelligence purposes. (JP 1-02)

national intelligence support team. A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. Also called **NIST**. (JP 1-02)

near-real time. Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. Also called **NRT**. See also **real time**. (JP 1-02)

open-source intelligence. Information of potential intelligence value that is available to the general public. Also called **OSINT**. (JP 1-02)

operational control. Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders.

Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called **OPCON**. (JP 1-02)

operational environment. A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 1-02)

operational intelligence. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. See also **intelligence**; **strategic intelligence**; **tactical intelligence**. (JP 1-02)

planning and direction. In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. See also intelligence process. (JP 1-02)

priority intelligence requirements. Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision making. Also called **PIR**. See also information requirements; intelligence; intelligence process; intelligence requirement. (JP 1-02)

processing and exploitation. In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence (JP 2-01)

radar imagery. Imagery produced by recording radar waves reflected from a given target surface. (JP 1-02)

reachback. The process of obtaining products, services, and applications, or forces, equipment, or material from Air Force organizations that are not forward deployed. (AFDD 2)

real time. Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. See also **near-real time**. (JP 1-02)

reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. Also called **RECON**. (JP 1-02) [*A transitory mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an*

adversary or potential adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.] (AFDD 2-9) {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

request for information. 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures. 2. The National Security Agency/Central Security Service uses this term to state ad hoc signals intelligence requirements. Also called **RFI**. See also information; intelligence. (JP 1-02)

scientific and technical intelligence. The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information that covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture. Also called **S&TI**. (JP 1-02)

sensor. An equipment which detects, and may indicate, and/or record objects and activities by means of energy or particles emitted, reflected, or modified by objects. (JP 1-02)

SIGINT operational tasking authority. A military commander's authority to operationally direct and levy signals intelligence (SIGINT) requirements on designated SIGINT resources; includes authority to deploy and redeploy all or part of the SIGINT resources for which SIGINT operational tasking authority has been delegated. Also called **SOTA**. (JP 1-02, DODD 5100.20)

signals intelligence. 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT**. (JP 1-02)

special operations. Operations conducted in hostile, denied, or politically sensitive environments to achieve military, diplomatic, informational, and/or economic objectives employing military capabilities for which there is no broad conventional force requirement. These operations often require covert, clandestine, or low visibility capabilities. Special operations are applicable across the range of military operations. They can be conducted independently or in conjunction with operations of conventional forces or other government agencies

and may include operations through, with, or by indigenous or surrogate forces. Special operations differ from conventional operations in degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets. Also called **SO**. (JP 1-02)

surveillance. The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (JP 1-02)

tactical control. Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and, usually, local direction and control of movements or maneuvers necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. Also called **TACON**. (JP 1-02)

target. 1. A geographical area, complex, or installation planned for capture or destruction by military forces. 2. In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. (JP 1-02)

targeting. The process of selecting targets and matching the appropriate response to them, taking account of operational requirements and capabilities. (JP 1-02)

technical intelligence. Intelligence derived from exploitation of foreign material, produced for strategic, operational, and tactical level commanders. Technical intelligence begins when an individual service member finds something new on the battlefield and takes the proper steps to report it. The item is then exploited at succeedingly higher levels until a countermeasure is produced to neutralize the adversary's technological advantage. Also called **TECHINT**. See also exploitation; intelligence.

validation. A process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. 2. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. 3. Execution procedure used by combatant command components, supporting combatant commanders, and providing organizations to confirm to the supported commander and US Transportation Command that all the information records in a time-phased force and deployment data not only are error free for automation purposes, but also accurately reflect the current status, attributes, and availability of units and requirements. Unit readiness, movement dates, passengers, and

cargo details should be confirmed with the unit before validation occurs. See also **independent review; time-phased force and deployment data; verification**. (JP 1-02)

MCWP 2-4

Marine Air-Ground Task Force Intelligence Dissemination

U.S. Marine Corps

DISTRIBUTION STATEMENT A:Approved for public release; distribution is unlimited

PCN 143 000150 00

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to **morgann@mccdc.usmc.mil**. Recommendations should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Add, delete
  - Proposed new text, preferably double-spaced and typewritten
- Justification and/or source of change

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status.* An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: **http://www.doctrine.usmc.mil**.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

MCCDC (C 42)
13 Jul 2004

E R R A T U M

to

MCWP 2-4

MARINE AIR-GROUND TASK FORCE INTELLIGENCE DISSEMINATION

1. Change the publication short title to read "MCWP 2-4" (vice MCRP 2-1C) and change PCN to 143 000150 00 (vice 144 000134 00).

PCN 143 000150 80

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

1 July 2003

FOREWORD

Marine Corps Doctrinal Publication 2, *Intelligence,* and Marine Corps Warfighting Publication 2-1, *Intelligence Operations*, provide doctrine and tactics, techniques, and procedures for intelligence operations. Marine Corps Warfighting Publication (MCWP) 2-4 *Marine Air-Ground Task Force Intelligence Dissemination*, complements and expands upon this information by detailing specific doctrine, tactics, techniques, and procedures for conducting intelligence dissemination in support of the Marine air-ground task force (MAGTF). The primary target audience of this publication is intelligence personnel responsible for planning and executing intelligence dissemination operations, as well as personnel who provide support to intelligence dissemination or who use results from intelligence operations.

MCWP 2-4 describes aspects of intelligence dissemination operations including doctrinal fundamentals, responsibilities, management, methodology and planning, and common forms of dissemination, such as estimates, studies, briefings, and reports. MCWP 2-4 provides the information needed by Marines to understand, plan, and execute intelligence dissemination operations in support of the MAGTF across the range of military operations.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

EDWARD HANLON, JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

Publication Control Number: 144 000134 00

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

MARINE AIR-GROUND TASK FORCE INTELLIGENCE DISSEMINATION

TABLE OF CONTENTS

Chapter 1. Intelligence Dissemination Overview

Objective 1-1
Communications and Information System Factors 1-1
Intelligence Dissemination Capabilities and Challenges 1-2
- Dissemation Assets 1-2
- Internal Dissemination 1-2
- External Dissemination 1-2
- Major Subordinate Command Level and Below 1-2

Responsibilities 1-2
Dissemination Guidelines 1-3
Intelligence Dissemination and Intelligence Functions 1-3
Intelligence Dissemination within the Intelligence Cycle 1-4
Intelligence Dissemination Criteria 1-4
- Pertinence 1-4
- Usability of Form 1-5
- Timeliness 1-5
- Security 1-6

Chapter 2. Intelligence Dissemination Management

Dissemination Management Functions 2-1
- Dissemination Requirements Management 2-1
- Dissemination Operations Management 2-2

Intelligence Dissemination Means 2-2
- Dissemination Methods 2-2
- Dissemination Channels 2-2
- Dissemination Modes 2-4
- Dissemination Forms 2-5
- Reports 2-5
- Databases 2-5
- Sensor Data and Information Streams 2-5
- Graphical Products 2-6

Chapter 3. Intelligence Dissemination Methodology

Determine Dissemination Requirements 3-1
Determine Dissemination Forms 3-1
Determine Dissemination Modes 3-1
Allocate Resources 3-2
Disseminate 3-2
Considerations During Dissemination 3-2
Quality Control of Dissemination 3-2
Evaluate Effectiveness 3-3
Train Personnel 3-3

Chapter 4. Intelligence Dissemination Planning

Planning Factors 4-1
MAGTF Dissemination Standing Operating Procedures, Plans, and Orders 4-1
Dissemination Planning Process 4-1
Identify Dissemination Requirements 4-2
Develop the Intelligence and Information Flow 4-3
Develop the Dissemination Plan 4-3
Allocate Resources 4-5
Monitor Execution 4-5

Chapter 5. Intelligence Estimates and Studies

Dissemination 5-1
Advantages versus Disadvantages 5-1
Intelligence Estimate 5-1
MAGTF Contingency Intelligence Study 5-2
Intelligence Studies 5-2
Target/Objective Studies 5-2
Intelligence Preparation of the Battlespace Products 5-2

Chapter 6. Intelligence Briefings

Dissemination 6-1
Advantages versus Disadvantages 6-1
Information Brief 6-1
Initial Staff Orientation Brief 6-1
Commander's Daily Update Brief 6-2
Intelligence Update Brief 6-2
Intelligence Estimate of Supportability 6-2
Mission/Target Intelligence Brief 6-2
Technical Intelligence Brief 6-3

Chapter 7. Intelligence Reports

Summary Intelligence Reports 7-1
Intelligence Summary 7-1
Daily Intelligence Summary 7-1
Periodic Intelligence Summary 7-2
Specialized Intelligence Reports 7-2
Intelligence Report 7-2
Battle Damage Assessment Reporting 7-2
Mission Report 7-3
Response to a Request for Intelligence 7-3
Intelligence Reports Plan and Matrix 7-3

Appendices

A. MAGTF Intelligence Dissemination Plan Appendix Format A-1
B. Intelligence Communications and Information Systems Plan Appendix Format B-1
C. Sample Intelligence Dissemination Requirements Planning Matrix C-1
D. Intelligence Reports Dissemination Matrix Format D-1
E. Glossary E-1
F. References F-1

Figures

1-1. The Marine Corps Intelligence Cycle 1-4
2-1. Requirements Satisfaction 2-1
2-2. Intelligence Dissemination Channels 2-3
2-3. Intelligence Dissemination Modes 2-4
3-1. Dissemination Methodology 3-1
4-1. Sample Dissemination Tracking Matrix 4-5

CHAPTER 1
INTELLIGENCE DISSEMINATION OVERVIEW

Intelligence dissemination is the delivery of intelligence to users in a suitable form. (Marine Corps Warfighting Publication [MCWP] 2-1, *MAGTF Intelligence Operations*) Successful Marine air-ground task force (MAGTF) intelligence dissemination reduces uncertainty and provides knowledge to battlefield decisionmakers when and where required. Dissemination management involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. (Marine Corps Reference Publication [MCRP] 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*)

Objective

Dissemination management involves dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in the proper form at the right time, while ensuring that individual consumers and the dissemination system are not overloaded by attempting to move unneeded or irrelevant information. Dissemination management also provides for the use of security controls, which do not impede the timely delivery or subsequent use of intelligence, while protecting intelligence sources and methods. (MCRP 5-12C)

Communications and Information System Factors

The MAGTF must ensure that sufficient communications and information systems (CIS) connectivity, with supporting intelligence resources, are integrated throughout the MAGTF staff intelligence element (G-2/S-2), and within the MAGTF's command and control (C2) structure. All sources of intelligence pertinent to the MAGTF's assigned mission(s) must be identified, quickly retrieved, processed, tailored to the supported requirement, and made available to planners and decisionmakers at all MAGTF echelons in sufficient time to be of value in their operations.

The fielding of numerous operational and intelligence-related automated systems and the challenges of joint, combined, and multinational operations make MAGTF intelligence dissemination a complicated endeavor. The MAGTF CIS architecture must link production with supported commanders. In addition to transmitting imagery and other intelligence products with large data files, the dissemination requirement includes the capability to disseminate sensitive compartmented information (SCI), and general service (GENSER) reports digitally via fiber-optics, wire or radio formats; and the capability to disseminate intelligence in voice formats.

Key MAGTF CIS resources include the following:

- Tactical data network (TDN).
- Nonsecure Internet Protocol Router Network (NIPRNET).
- SECRET Internet Protocol Router Network (SIPRNET).
- Defense Switched Network (DSN).
- Defense Secure Network (DSNET).
- Joint Worldwide Intelligence Communications System (JWICS).
- Intelligence analysis system (IAS).
- Command and control personal computer (C2PC).
- Intelligence operations workstation (IOW).

- Joint deployable intelligence support system (JDISS).
- Satellite communications (SATCOM).

For detailed descriptions of MAGTF CIS, see MCWP 3-40.3, *Communications and Information Systems*.

Intelligence Dissemination Capabilities and Challenges

Dissemination Assets

The intelligence battalion collection management and dissemination section provides the core C2 for Marine Expeditionary Force (MEF) intelligence dissemination operations by developing and coordinating the dissemination plan and reporting criteria. The surveillance and reconnaissance cell (SARC) executes reporting criteria. The production and analysis (P&A) cell receives collected intelligence data and information, analyzes it, produces intelligence products, and executes dissemination criteria. Key CIS resources required include IAS and JDISS, with access to the full range of MAGTF communications (JWICS, SIPRNET, NIPRNET or DSN) for external dissemination; and IAS via the TDN and other MAGTF communications resources for internal dissemination.

Internal Dissemination

The IAS, the IOW, and MAGTF TDN are the key tools for electronic dissemination between the command element (CE) and major subordinate commands (MSCs). Communications connectivity between the MAGTF CE and its major subordinate element (MSE) headquarters are predominantly provided by SATCOM, supplemented where practical with high frequency/ultra high frequency (UHF) radios, troposcatter multichannel radio systems, telephone systems, and couriers. IAS will be available at all command echelons down to the maneuver bn/squadron levels.

External Dissemination

The MAGTF CE will attempt to exploit all available external capabilities (national, theater or joint) to satisfy its intelligence requirements (IRs). Intelligence agencies and Department of Defense (DOD) organizations have varying connectivity and procedural requirements. These may be planned for and coordinated through the joint staff intelligence element (J-2) and the joint CIS staff element (J-6) or the Marine Corps forces (MARFOR) headquarters (HQ).

Major Subordinate Command Level and Below

Connectivity at the MSC level and below is principally via the TDN, single-channel radio, multichannel radio, telephone, and courier. Communications connectivity below the regiment/group level depends on a combination of tactical data systems and single channel radio. The ability to exchange data traffic may be limited due to the availability of bandwidth.

Responsibilities

Meeting MAGTF intelligence dissemination requirements requires extensive planning, coordination, situational awareness, flexibility, and perseverance. The CIS officer's focus is on providing the necessary communication channels, interfaces, and media necessary to move intelligence throughout the MAGTF, and to lateral elements and higher echelons. The intelligence officer remains focused on the employment of allocated CIS resources that support intelligence dissemination requirements while maintaining close coordination with the operations officer to monitor current and future operational missions and requirements.

Intelligence officers at every level of the MAGTF have dissemination responsibilities. At the MEF level, the intelligence battalion directs intelligence dissemination operations. The intelligence battalion commander/intelligence support coordinator (ISC) has principal staff responsibility for the dissemination architecture. The intelligence battalion commander is dual-hatted as the ISC. The collection management/dissemination officer (CM/DO) plays a key role in ensuring intel dissemination.

The CM/DO is sourced from the intelligence battalion's S-3 section. The CM/DO is responsible for the following:

- Formulating detailed intelligence collection requirements (ICRs) and intelligence dissemination requirements (IDRs) and tasking and coordinating internal and external operations to satisfy these.
- Receiving validated priority intelligence requirements (PIRs) and IRs and direction from the ISC, and then planning and managing the best methods to employ organic and supporting collection and dissemination resources through the intelligence collection and dissemination plans.
- Validating and forwarding MEF and MSC requests for national and theater collection and dissemination support using appropriate intelligence tools and procedures.
- Coordinating intelligence-related CIS requirements and maintaining awareness of available CIS connectivity throughout the MAGTF and with key external organizations.

The CIS officer (G-6/S-6) is responsible for the management and functioning of MAGTF CIS circuits, such as MEF radio nets and SIPRNET connectivity. The G-2/S-2 is responsible for the management and maintenance of dedicated intelligence systems. Regardless of the status of CIS support, the intelligence officer is responsible for the timely dissemination of critical intelligence.

Dissemination Guidelines

Guidelines for intelligence dissemination include the following:

- Dissemination formats; either verbal, text or graphical.
- Whether verbal, text or graphic, intelligence products should use standard formats whenever possible to facilitate ease of preparation, usability, and dissemination.
- Transmission can be either hardcopy or electronic, regardless of the format.
- Dissemination of too few or too many intelligence products can adversely affect operations.
- Intelligence dissemination requires sound judgment when applying information management techniques.
- Effective intelligence dissemination requires that intelligence personnel be aware of enemy capabilities and probable courses of action (COAs), as well as friendly missions, the commander's intent, and the concepts of operations.
- Successful MAGTF intelligence dissemination requires planning, management, and flexibility.
- Executing intelligence dissemination requires knowledge of manual and automated dissemination means available to the MAGTF.

Intelligence Dissemination and Intelligence Functions

MAGTF intelligence dissemination must support the following six specific intelligence functions:

- Support to the commander's estimate.
- Situation development.
- Indications and warning (I&W).
- Support to force protection.
- Support to targeting.
- Support to combat assessment.

Intelligence Dissemination within the Intelligence Cycle

The process used to develop intelligence is called the intelligence cycle (see fig. 1-1). The intelligence cycle consists of six sequential yet interdependent steps: planning and direction; collection; processing and exploitation; production; dissemination; and utilization. While consistent with the joint intelligence cycle, the Marine Corps cycle emphasizes the importance of intelligence utilization. MAGTF intelligence dissemination must be planned for and supervised to the same degree as direction, collection, processing, and production to ensure that intelligence operations are successful.

Intelligence Dissemination Criteria

The following criteria determine how well disseminated intelligence contributes to tactical success:

- Pertinence.
- Usability of form.
- Timeliness.
- Security.

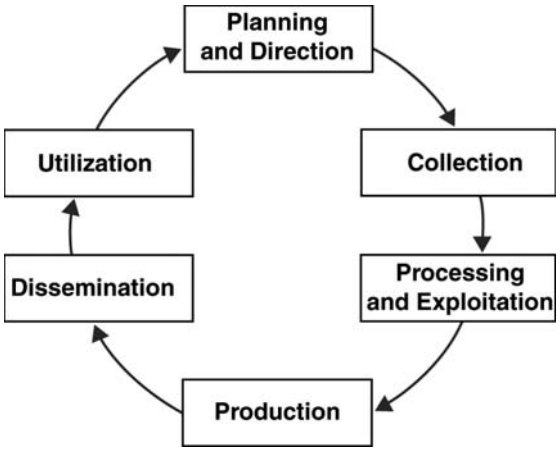


Figure 1-1. The Marine Corps Intelligence Cycle.

Pertinence

The dissemination system must provide the flexibility to use a supply-push system (which pushes important or time-sensitive intelligence directly to users), while also permitting users to demand-pull (allowing users to access information) relevant intelligence as needed from readily accessible sources, such as a database or a watch section at an intelligence center. The following principles guide successful dissemination of pertinent intelligence:

- *Relevant intelligence must be disseminated to all units or agencies that require it.* Intelligence must be tailored to the needs of the commander. Stated requirements are a minimum, and often change. Aggressive management of the dissemination strategy, a thorough understanding of user needs, sound judgment, and continuous monitoring of the dissemination architecture are required. Tactical judgment is important to disseminate pertinent intelligence to affected users, whether a requirement for it is a stated requirement or not.
- *Disseminate critical information and intelligence.* Disseminate intelligence, not simply information, to supported decisionmakers. However, because of its highly perishable or critical nature, combat data (derived from reporting by operational units) and sensor data may be disseminated without being converted into intelligence. Caution is required since warnings and combat and sensor data may later be explained in ways other than reflected in the original report. Additionally, this type of information has the potential to be over-disseminated. Operational rules of engagement must match the command's time-sensitive targeting policy.
- *Crisis situations may preclude some or all of the normal filtering process.* Filtering is a responsibility shared among intelligence collectors, producers, and disseminators, as well as among intelligence and other warfighting

personnel. When time-sensitive crisis situations preclude deliberate intelligence processing and necessitate dissemination of untailored intelligence or unevaluated information, intelligence personnel must ensure that tactical commanders are aware that they are receiving unevaluated intelligence.

- *Dissemination downward should be selective and well planned.* Units should not receive irrelevant intelligence or voluminous amounts of information that can tie up their communication channels or overload their organic analytical capability. This is especially valid in the case of dissemination to lower tactical units whose capabilities for processing and producing information are limited. However, broad dissemination that results in the occasional delivery of intelligence to a non pertinent unit preferable to selective dissemination in which units may fail to receive available intelligence when they need it.

Usability of Form

Disseminated intelligence must be in a form suitable for immediate use by the recipient and should be tailored for the intended consumer. Standard formats for intelligence products—such as the intelligence estimate, intelligence studies, briefings, and reports—must be established, understood, and used by intelligence personnel and users. Basic MAGTF intelligence products have established formats. Individual units may modify formats if necessary, but modifications must be thoroughly coordinated as they may impact interoperability. Intelligence personnel should complement textual data with graphics when appropriate. Forms of dissemination include the following:

- *Written documents.* Intelligence estimates, operation plan/operation order (OPLAN/OPORD) annexes, studies, and reports are useful for general dissemination of large amounts of intelligence to many users—particularly within larger organizations when time is not critical and when deliberate planning is possible—and for all organizations in support of specified wartime contingency planning.
- *Messages.* Textual and voice messages may be effective for either routine or time-critical situations, particularly if restricted to a single intelligence subject, issue or action. It is important, however, that formats be standardized and understood by all—particularly if abbreviations or codes are used to aid with brevity.
- *Oral briefings.* Oral briefings, especially when built around a situation map and focused supporting graphics and imagery, are often used during deliberate and rapid planning and are the norm for intelligence dissemination to the immediate commander and his staff.
- *Electronic dissemination.* Automated technologies, including web-based technologies and information systems, are advancing opportunities for intelligence personnel at all command echelons to employ capabilities such as demand-pull, video-teleconferencing, and enhanced graphical techniques to access intelligence community resources.

Timeliness

Intelligence must be disseminated in time to influence planning, decisionmaking, and execution. Rapid dissemination of critical, time-sensitive intelligence is particularly vital. The commander's intent and the commander's critical intelligence requirements (CCIRs) guide the intelligence staff in identifying PIRs and anticipating future IRs. Many factors influence the timeliness of disseminated intelligence, including the following:

- Date desired is the date-time-group of when the requester requires the intelligence product and is a key dissemination planning factor.
- Latest time intelligence is of value (LTIOV) should be designated in cases where the value of intelligence collection would still be of use even if received after the specified date desired. LTIOVs should be written into PIRs for incorporation into dissemination operations planning and management.

- A high volume of intelligence reporting can degrade the performance of available intelligence communication networks and overwhelm scarce analytical resources.
- Distance, mobility, and terrain factors often limit available CIS options, such as automated wide-area networks (WANs), thereby increasing reliance upon less effective single channel radio and courier methods.
- The communications means available.
- The need to reformat certain intelligence products into user-friendly formats prior to dissemination.
- A heightened tempo that usually produces a greater quantity of IRs and customers.
- Hardware and software requirements that may pose interoperability or security problems, especially in joint or multinational operations.

The timeliness of intelligence dissemination may be improved by—

- Assigning priorities to intelligence requiring dissemination.
- Targeting specific recipients for each intelligence product.
- Reducing volume.
- Developing well-defined procedures.
- Training.

Security

Transmitting intelligence securely precludes the enemy from ascertaining MAGTF intelligence sources, estimating the effectiveness of MAGTF intelligence operations, and altering his actions or strengthening his counterintelligence (CI) efforts. Secure intelligence dissemination must be planned for and integrated with all command security programs: operations, information, communications, personnel, and physical security. Intelligence can be disseminated by any system available that provides adequate information security.

Secure dissemination methods must be used whenever possible. However, if the situation and intelligence are time-sensitive, intelligence may be disseminated via any available means. In such cases, the unit security manager and intelligence officer are immediately informed and will assess any possible damage and initiate necessary remedial corrective actions.

The majority of today's tactical CIS have integral or supporting features that provide security protection. For more restricted operational or SCI communications, detailed procedures exist that allow for sanitization and timely, broader dissemination when necessary. The principal security challenge that may be faced during tactical or crisis situations is when events occur that disrupt or degrade these unit CIS, necessitating a potential trade-off between security and dissemination. Multilateral operations raise additional dissemination challenges regarding the sharing of intelligence among allied and coalition forces.

Tailored intelligence will be disseminated via the best means available consistent with the operational situation. Although most intelligence will be classified, even some unclassified intelligence may require security protection due to operational security considerations. Resolving these challenges will be situationally dependent. Relevant factors to consider include the following:

- The enemy's own intelligence collection, processing, and dissemination capabilities.
- Phase of the operation's planning or execution.
- Significance of current intelligence gaps, particularly at lower tactical units.
- How the intelligence may support the exploitation of threat vulnerabilities and tactical opportunities.

CHAPTER 2
INTELLIGENCE DISSEMINATION MANAGEMENT

Dissemination management ensures that the required intelligence is provided to the appropriate user in the proper form and at the right time.

Dissemination Management Functions

The two distinct functions within dissemination management are dissemination requirements management, and dissemination operations management. Dissemination requirements management defines what intelligence will be disseminated and who needs it; dissemination operations management specifies how the intelligence will be disseminated. Management of dissemination requirements and operations is performed at all levels of the MAGTF. Within the MEF, management is coordinated by the intelligence battalion in accordance with the direction of the MEF intelligence officer.

Dissemination Requirements Management

Managing intelligence requirements is the first step in dissemination planning. Intelligence collection, production, and dissemination all flow from an integrated intelligence planning and direction process that is built upon IR management. Each IR will generally have an associated ICR, intelligence production requirement (IPR), and IDR. (See fig. 2-1) See also MCWP 2-1.

Dissemination requirements management is framed by the dissemination strategy, which incorporates commander's intent, CCIRs, PIRs, IRs,

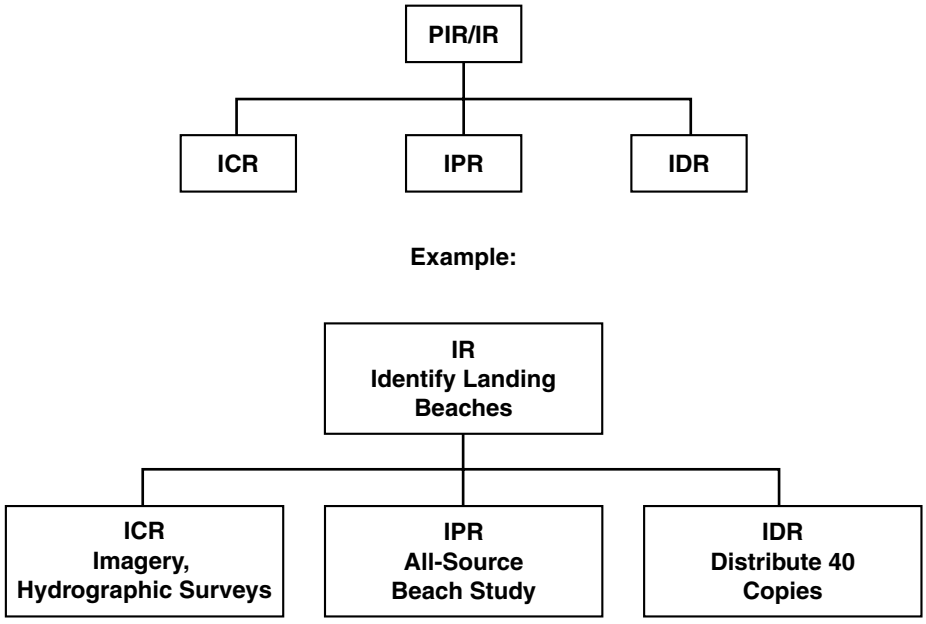


Figure 2-1. Requirements Satisfaction.

concepts of operation, and requests for information (RFIs). A preplanned dissemination strategy familiarizes the MAGTF with which intelligence products will be disseminated and by what means. It also describes alternate means of dissemination.

Dissemination Operations Management

Dissemination operations are managed by using a combination of methods (supply-push and demand-pull), channels (standard and alarm), modes (broadcast and point-to-point), and forms (verbal, text, and graphic) to convey the product to users.

Intelligence Dissemination Means

The ability to deliver tailored intelligence products and support to the right people in a timely manner is a direct result of the means of dissemination available. Within the MAGTF, no single way of disseminating will be satisfactory for all recipients and for all situations.

A combination of methods, channels, modes, and forms are planned, managed, and employed to accomplish the intelligence dissemination goal. These will vary according to the following:

- Situation.
- Location of the recipient.
- Urgency of the intelligence.
- Complexity or nature of the intelligence.
- Disseminating and receiving intelligence sections' capabilities.
- Available dissemination means.

Dissemination Methods

The two basic methods used to disseminate intelligence are supply-push and demand-pull. Intelligence planners must develop and implement intelligence dissemination plans with the flexibility to exploit either methodology, pushing time-sensitive intelligence directly to users while simultaneously allowing them to pull other intelligence products as needed.

The supply-push method disseminates intelligence to users as it becomes available (or on a schedule) from an intelligence collector or producer. This method is need-driven and is triggered by the availability of required intelligence and an understanding of its need by specific users.

The demand-pull method exploits technological improvements by giving users either direct electronic access to intelligence databases, files, servers or intelligence products through detailed search procedures or via direct queries to intelligence planners and producers, such as the MEF's P&A cell or the joint intelligence center (JIC).

Demand-pull dissemination is primarily used when there is a need by a subordinate command to access intelligence archives at higher HQ, such as databases and technical files maintained at JIC and the P&A cell for amplifying intelligence to support its planning activities (for example, basic/descriptive intelligence, technical information). It may also be employed by higher echelons to satisfy IRs when the amplifying data can best be accessed from subordinate units.

Dissemination Channels

Intelligence is disseminated using two types of channels: standard and alarm (see fig. 2-2).

Standard Channel

Standard channel dissemination consists of transmission of intelligence according to a set order and format. It is used for routine intelligence dissemination and is the channel used for the majority of dissemination requirements. Dissemination generally occurs on a regular schedule or intervals. Examples of standard intelligence dissemination include studies,

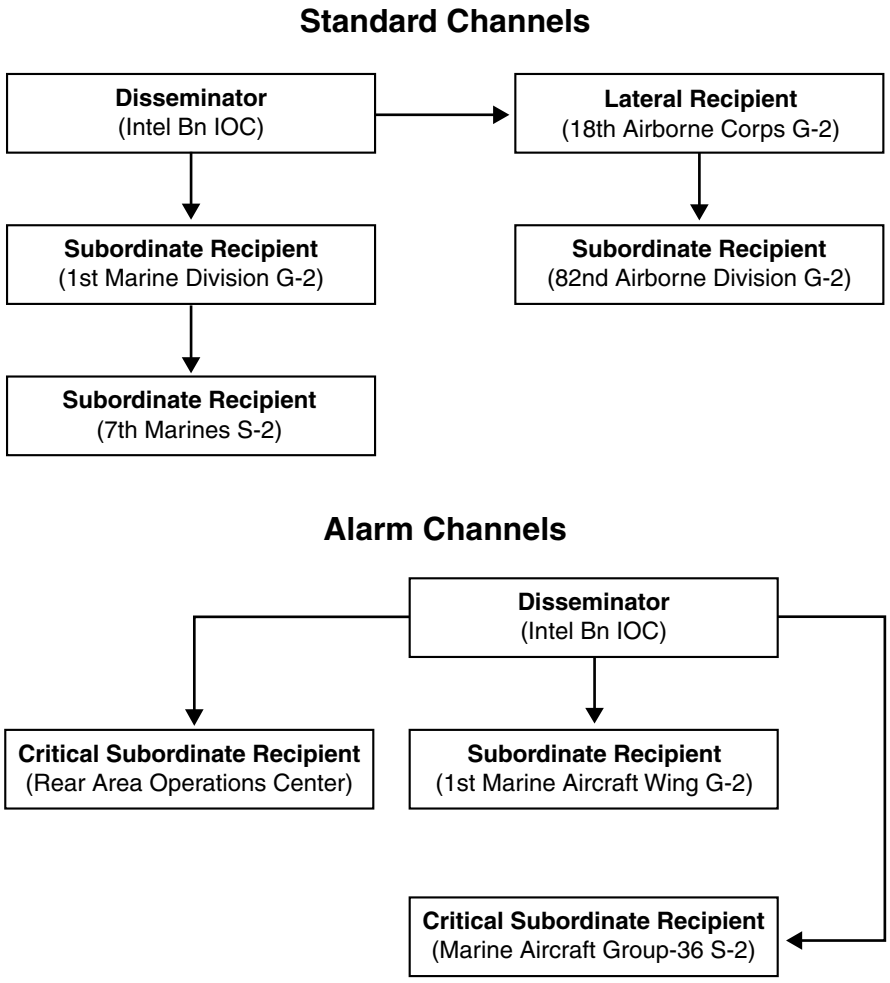


Figure 2-2. Intelligence Dissemination Channels.

reports, routine message intelligence summaries, and formal staff briefings. Standard dissemination employs normal MAGTF command and staff channels and supporting CIS.

Alarm Channel

Alarm channel dissemination is used for critical, time-sensitive intelligence that can have an immediate effect on operations. This type of dissemination has no set format or schedule and is activated only when critical intelligence is received that requires immediate decision or action. When an alarm-triggering event occurs, intelligence must go to the units or sections most affected by the most direct means possible, even if it means skipping echelons of command. CIS connectivity may be either the standard MAGTF CIS architecture or by dedicated intelligence CIS. Because alarm intelligence is time-sensitive, dissemination should include a means for verifying receipt and understanding. Filters and thresholds for alarm-triggering events must be developed, understood, and practiced in advance. Effectively disseminating intelligence via alarm channels requires the following:

- Detailed intelligence collection, production, and reporting direction.

- Accurate knowledge of MAGTF CIS.
- Frequent interoperability training (to include other Service and joint organizations).
- Training for intelligence, operations and unit personnel to immediately recognize, act upon received intelligence, and disseminate it.

Dissemination Modes

Intelligence is disseminated via broadcast or point-to-point modes (see fig. 2-3).

Broadcast Mode

When using the broadcast mode, intelligence that affects the majority of units is disseminated simultaneously to a broad audience. Examples include dissemination of the initial MAGTF intelligence estimate or an I&W report of an enemy surface-to-surface missile launch. Successful use of broadcast modes depends on judicious selection of what intelligence is disseminated, the ability of all pertinent recipients to monitor the broadcast, and the ability of users to filter and select relevant intelligence for detailed examination. The broadcast mode improves dissemination timeliness, but must be used with discipline to avoid overloading MAGTF CIS pathways or intelligence processing capabilities.

Point-to-Point Mode

In the point-to-point mode, intelligence is disseminated to a specific user, normally in response

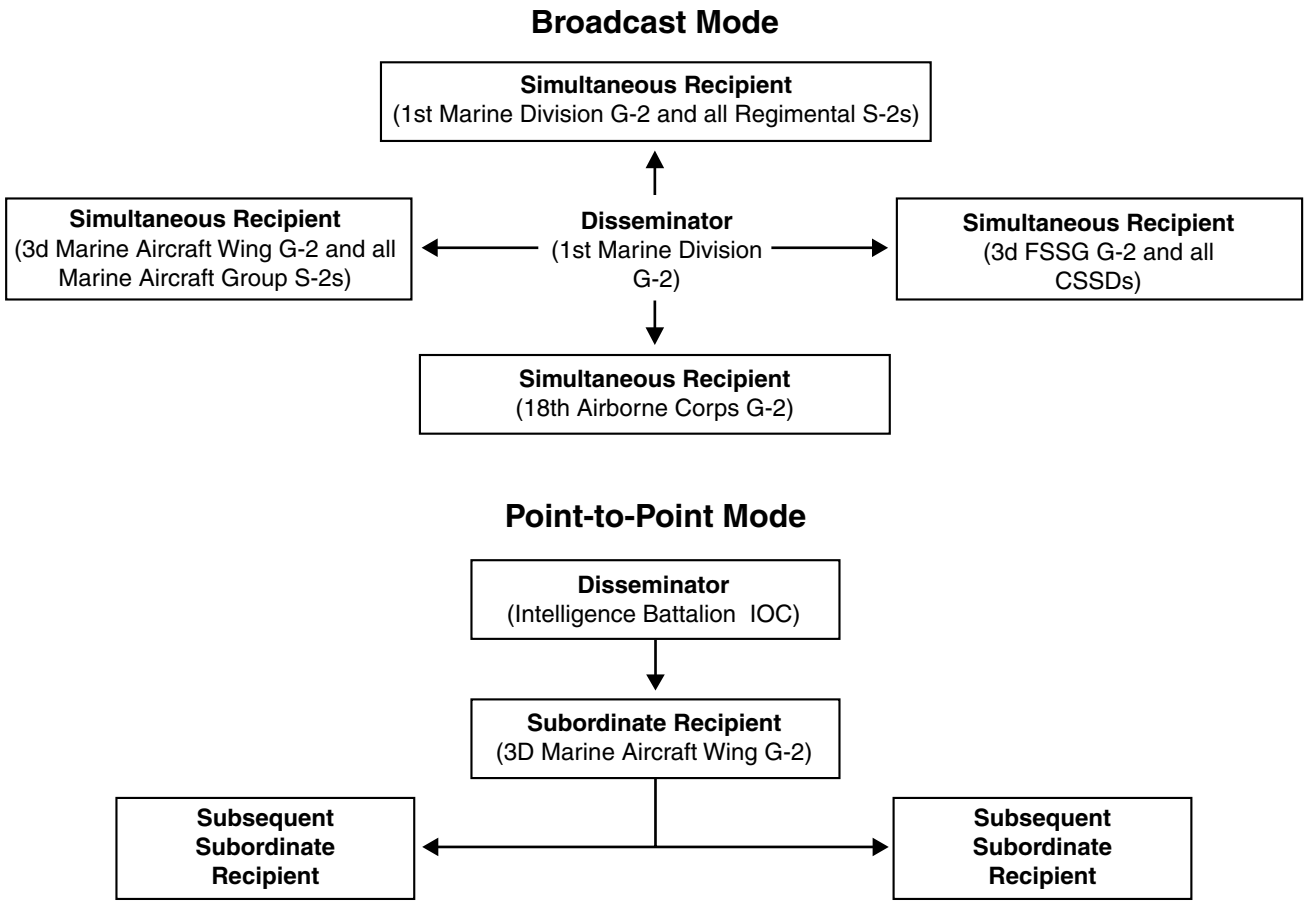


Figure 2-3. Intelligence Dissemination Modes.

to previously stated IRs. From there it may be further disseminated by users to others as appropriate. Although this mode is generally slower than the broadcast mode, it allows for intelligence to focus on specific user needs and allows the recipient to act as a control mechanism, filtering and integrating intelligence prior to disseminating it further. This control mechanism, however, adds risk as the intelligence meaning may become distorted as it is conveyed from one command to another. Examples of point-to-point modes include email, voice radio or telephone, and courier. When a secure WAN or local area network (LAN) is operational, a majority of intelligence disseminated between the MEF and its MSCs may be via email. Below the MSC level, the majority of point-to-point dissemination is by radio, wire communications or courier.

Dissemination Forms

The most suitable format for intelligence dissemination depends primarily on the needs of the recipient, the nature and urgency of the intelligence, and the means available to convey the information. The unit intelligence officer should specify a desired format (such as verbal, text, electronic) whenever stating an IPR and or/IDR.

Verbal

Verbal formats include dissemination via radio or telephone, face-to-face briefings, and discussions or via video-teleconferencing. The primary benefit of verbal formats is timeliness, in getting the information to the user, and by the disseminator having immediate, positive verification of delivery. Verbal forms can also enhance communication through subtle factors, such as tone of voice, inflection, facial expressions, body language, and gestures, which may convey greater meaning than the words alone. Verbal formats may be part of formal briefings that require complex graphics, detailed scripting, and rehearsals, which can monopolize personnel and material resources.

Text

Much intelligence is disseminated via documents, which may take many formats: plans, studies, analyses, estimates, assessments, reports, and electronic messages. Document dissemination provides a ready reference source, but may become obsolete, and may be difficult to rapidly and broadly disseminate during tactical operations.

Electronic

Many intelligence reports, databases, and sensor data are disseminated and updated electronically to improve timeliness and enable near real time connectivity between intelligence collectors, producers, and users. Examples include tactical LANs and WANs, and systems such as the JDISS and the IAS.

Reports

Intelligence reports and summaries are normally used to broadcast information electronically to a wide audience to update a current situation or subject of interest. Normally released according to a predetermined time schedule, reports continuously “refresh” databases but may lag in timeliness during a fast-moving crisis or battle.

Databases

Many intelligence-related databases are available for electronic dissemination. Threat and environmental databases are maintained within the intelligence battalion’s P&A cell. Subordinate units establish and maintain their own databases, tailored to their units’ intelligence needs.

Sensor Data and Information Streams

The G-2/S-2, G-3/S-3, and G-6/S-6 must coordinate sensor data and information management and dissemination-related issues, weigh the advantages and risks, and develop procedures. One example is the potential dissemination of

intelligence information (for example, video footage) directly from a collector (for example, an unmanned aerial vehicle) to a targeting or operational node perhaps via an intelligence operations node.

Graphical Products

Graphics, such as those used in map enhancements or contained in annotated imagery, portray vast amounts of intelligence in a condensed form more easily interpreted by the human mind. When appropriate, they should be incorporated in intelligence production and dissemination. The chief benefit of graphical dissemination formats, such as maps, overlays, annotated imagery, briefing graphics, and topographic products, is that they may be assimilated and understood by people more quickly than textually-based formats. Effective use of graphical product dissemination requires standards, procedures, and training. In most cases intelligence disseminated via graphics must be reinforced with supporting documents or supplemental information.

CHAPTER 3
INTELLIGENCE DISSEMINATION METHODOLOGY

Dissemination planning begins with an understanding of basic dissemination methodology. The three parts of IR are ICR, IPR, and IDR. Each IDR should be processed individually, using the methodology described in figure 3-1.

Determine Dissemination Requirements

Identify what intelligence is needed, who needs it, location, date required, and assign priority. Disseminators should—

- Optimize utilization.
- Stay in contact with commanders and other intelligence requestors.

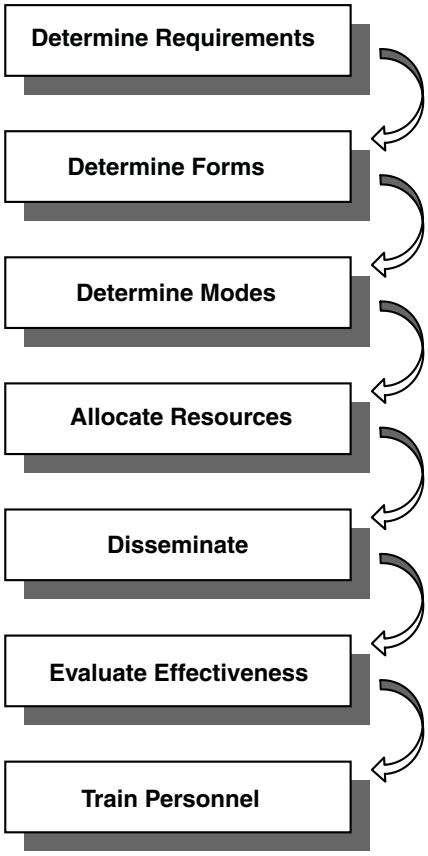


Figure 3-1. Dissemination Methodology.

- Determine common IRs.
- Develop planning tools.

Determine Dissemination Forms

Intelligence may be disseminated in a variety of formats and via verbal, text or graphical formats. The optimal form for dissemination best meets the needs of the user. It must answer the user's needs in the timeliest manner consistent with the urgency of the tactical situation.

A well-designed dissemination plan will take formatting factors into account and save man-hours otherwise spent on re-drafting and copying. Disseminators must be able to prepare and transmit the formatted intelligence in time to satisfy the user's LTIOVs. The format of the intelligence product must be compatible with the mode of transmission.

Dissemination planners must know the CIS capabilities and status of all supported elements. Since the CIS status of recipients may change at any time, disseminators must plan for alternate means of dissemination. Intended recipients in a highly mobile situation may be reliant on point-to-point phone or radio communications.

Determine Dissemination Modes

MAGTF intelligence staffs must identify dissemination channels and capabilities and plan for primary and alternate dissemination via common communication pathways. Available CIS bandwidth must be economized. Dissemination planners should—

- Identify and select both routine and time-sensitive modes.

- Determine and prioritize both dissemination point-to-point and broadcast modes for the widest possible range of tactical situations, to include standard and alarm situations and also criteria.
- Maintain awareness of the status of all MAGTF and key external CIS plans and operations.

Allocate Resources

The commander and intelligence officer exercising centralized control of intelligence dissemination must allocate resources to ensure that the needs of subordinate commanders are properly addressed and supported. Detachments from one or more intelligence/reconnaissance/CI unit may be placed in direct support (DS) or attached to subordinate units. They may also be used to create intelligence nodes to support a subordinate unit or center (for example, the rear area operations center; civil-military operations center). This must be done in coordination with the G-3/S-3 (for unit concept of operations and tactical task organization); the G-6/S-6 (for CIS resources); the G-1/S-1 (for personnel augmentation and courier support); the G-4/S-4 (for unique intelligence element's combat service support); and within the G-2/S-2 section for effective management of dissemination personnel and assets.

Disseminate

Intelligence products must be disseminated as quickly as possible to all relevant users. Dissemination planners should anticipate overloaded or disabled communication links by planning alternate distribution means. Redundancy must be planned for and used as needed.

Good reporting and dissemination flow diagrams and matrices assist in dissemination development, planning, and execution. They also provide combat operations center (COC), P&A cell, and SARC watch personnel with references to guide them in dissemination decisions.

Considerations During Dissemination

Current Tactical Situation

The dissemination plan will provide guidance for when, to whom, and how to disseminate the various types of intelligence and products.

Disseminators must always evaluate the IR against the current tactical situation; in addition to planned recipients ask who has a need for the intelligence; and initiate necessary action.

Status of Current Communications and Information Systems Readiness

Dissemination managers must continuously monitor the status of all CIS resources and pathways, primary and alternate. Continuous coordination with the G-2/S-2 COC watch officer and the G-6/S-6's systems control (SYSCON) and technical control (TECHCON) centers is mandatory to rapidly assess problems and determine availability of alternate communication means.

Quality Control of Dissemination

Dissemination planning is generally centrally managed. Dissemination execution is decentralized and conducted by a wide variety of individuals—P&A cell, SARC, and COC intelligence personnel; intelligence, CI, and reconnaissance collectors; and even operations, fires, and other nonintelligence personnel. New CIS technologies allow greater intelligence access to and dissemination from commands and organizations external to the MAGTF as well as command echelons within the MAGTF. Additionally, the ability of users to pull information from nonmilitary or intelligence sources (for example, news media, academia, nongovernmental organizations [NGOs]) and use it as intelligence presents a quality control challenge. Data may be incorrect, misleading, dated or incomplete, excessive or wrongly perceived as conclusive. Users may use this data without understanding the basis. Detailed, well-designed standing operating procedures (SOPs) and continuous coordination are critical to successfully dealing with these challenges.

Evaluate Effectiveness

After disseminating an intelligence product, disseminators must ensure that it was received and understood by all intended recipients. Intelligence products are occasionally misrouted or not transmitted completely. Verification of receipt can be accomplished through a telephone call or email confirmation from select addressees. Follow-on contact should be made to determine if intelligence needs were met or if the provided intelligence led to any new IRs.

Train Personnel

Regular and realistic training of all intelligence personnel and users is needed to improve their understanding of dissemination operational capabilities and limitations, their tactical abilities and judgments, and their technical skills and expertise.

Intelligence dissemination capabilities must be exercised under a variety of realistic tactical scenarios and operating conditions. Training must emphasizes unit SOPs, as well as other Service, joint, and intelligence agency procedures. Training must develop the following procedures:

- Ensure that dissemination problems experienced anywhere within the MAGTF are immediately brought to the attention of the appropriate personnel for corrective action.
- Maintain awareness of the current operational status of key intelligence-related and CIS resources.
- Confirm the receipt of disseminated intelligence.
- Quickly verify that CCIRS, PIRs, and IRs have been fully satisfied, and whether they generate or affect any new IRs.
- Enable commanders, planners, and other nonintelligence personnel to pull intelligence from databases, Web sites, publications, and other intelligence resources.
- Rehearse time-sensitive dissemination procedures, to include using alternate communication means.
- Disseminate intelligence to other Services, joint, multinational forces, and NGOs.
- Integrate intelligence and reconnaissance units' intelligence, C2, and CIS operations in HQs of all subordinate organizations down to the battalion, squadron, and combat service support detachment level.
- Execute specialized and unique intelligence dissemination CIS capabilities (for example, SCI sanitization and reporting of DOD clandestine collection activities).

CHAPTER 4
INTELLIGENCE DISSEMINATION PLANNING

The MAGTF intelligence section develops and implements intelligence dissemination plans. While written from the MEF intelligence section perspective, the guidelines addressed in this chapter may be tailored to any echelon. Appendix A provides a sample intelligence dissemination plan format. Appendix B provides a sample intelligence CIS plan format. Appendix C provides an IDR planning matrix format.

Planning Factors

Intelligence dissemination plans and procedures must incorporate the following:

- IDR priorities, to include integrated linkage with ICRs and IPRs.
- Grouping IRs by type of intelligence and echelon of intended recipient.
- Anticipated IDRs.
- Preferred intelligence product.
- Primary and alternate communication means with all supported units.
- Routine and time-sensitive dissemination means and responsibilities.
- Communications security (COMSEC) considerations.
- Procedures to verify that the intelligence has been received by the intended recipients.

MAGTF Dissemination Standing Operating Procedures, Plans, and Orders

The assistant chief of staff (AC/S) G-2 has overall responsibility for MAGTF intelligence dissemination SOPs, plans, and orders. The ISC is responsible for the preparation of the intelligence dissemination plan and the intelligence CIS plan. The CM/DO is responsible for execution.

The principal intelligence CIS planning guide/tool for a MAGTF operation is tab D, Intelligence CIS Plan, to Appendix 16 (Intelligence Operations Plan) of Annex B of the OPLAN/OPORD. Other portions of Annex B, however, also include key intelligence CIS information. For example, tabs A, B, and C to Appendix 16 (respectively, the collections, production and dissemination plans); tab E (Intelligence Reports) to Appendix 16; and paragraph 5 (Intelligence C2) to Annex B of the basic plan.

In addition to Annex B, portions of Annex K (CIS) influence intelligence CIS architecture planning. The following are included:

- Appendix 14, Communications Restoration.
- Appendix 23, Task Organization/Communications Guard Shifts.
- Appendix 26, Radio Battalion/special security officer (SSO) Communications.
- Appendix 31, Communications Support for Intelligence.
- Appendix 34, Internet Protocol Assignments.
- Appendix 35, CIS Support for Information Management.

Dissemination Planning Process

Intelligence dissemination should be—

- Preplanned.
- Tailored for specific recipients based on unit mission.
- Automated to the greatest degree possible.
- Included with back-up plans and manual means of dissemination.

Identify Dissemination Requirements

Validated and prioritized CCIRs, PIRs, and IRs drive IDR planning. When identifying requirements, the four W's—who, where, what, and when—provide a usable, four-step process for identifying dissemination needs.

Who

Identify and group who may need dissemination support, not only those specifically involved with an IR. These units may include higher HQ (for example, joint task force (JTF); external intelligence units (for example, JIC, joint interrogation and debriefing center or joint document exploitation center); adjacent units (for example, United States Army units); and internal elements of the MAGTF (current operations center, force fires coordination center, rear area operations center or civil-military operations center).

Where

Where intelligence is disseminated will likely correspond to the location of the intended recipient; however, command relationships, operational phase, task-organization or other factors may determine other locations for dissemination requirements. Intelligence dissemination planners must pay particular attention to special dissemination requirements during any of the following situations:

- Intelligence support provided via reach back or involving split-base operations.
- Location of unit C2 facilities during tactical displacements.
- When the unit can utilize communications provided by a collocated unit.
- Operations afloat and ship-shore movement phases.
- Heliborne or air movement operations.
- Terrain, weather or atmospheric conditions that may affect dissemination.

What

The next step is to determine what type intelligence support (for example, finished deliberate intelligence, time-sensitive intelligence products or particular formats) each recipient requires. The who and what are cross-referenced with the following:

- Finished intelligence products (intelligence studies, estimates or reports).
- Addressee indicator groups, Defense Special Security Communications System address groups, collective address designators, and MAGTF units.
- Alarm intelligence support (for example, I&W report or time-sensitive target of opportunity reporting).
- Imagery IRs.
- Signals intelligence (SIGINT) (for example, requirement for time-sensitive/non-codeword reporting; sanitized version SCI products).
- Human intelligence (HUMINT) (for example, CI time-sensitive reports, tactical interrogation reports, special CI reporting).
- Geographic intelligence (for example, planning and operational map allowance requirements, terrain models and analyses, geospatial information needed for automated systems).
- Reconnaissance and surveillance requirements.
- Level(s) of classified information that the user requires.
- Releasability and formats for sharing intelligence with multinational units.

When

The final basic dissemination planning step is to identify timeliness requirements. In general, intelligence should be disseminated as soon as possible. Planning considerations include the following:

- Rapidly assessing the feasibility of satisfying the commander's stated LTIOV requirement.
- Nature of the IR (for example, routine, time sensitive, CCIR).

- Communication transmission means desired by the user (for example, voice, text, electronic).
- Capabilities and current status of the MAGTF CIS system.

Develop the Intelligence and Information Flow

Intelligence Flow

Dissemination planning must begin with an analysis of intelligence and information processes. Visualization of the flow of intelligence flow can contribute to detailed planning. The use of various types of flow diagrams and dissemination planning matrices can assist in the process. When building a MAGTF dissemination matrix, key dissemination recipients, such as the MSCs, must always be depicted. No standard dissemination matrix has been developed for all dissemination planning functions; however, some examples are provided in Appendix C (Intelligence Dissemination Requirements Planning Matrix) and Appendix D (Intelligence Reports Dissemination Matrix Format).

Intelligence Reporting

An intelligence report matrix depicting standard and time-sensitive reporting guidance should be prepared for every operation. The particular format will be tailored to meet unit needs. The matrix should detail the flow of intelligence reports to be prepared or handled by the intelligence section and the IOC. For MAGTF elements, this should show the flow from the original reporter (collector, SARC or P&A cell) to recipients for each type intelligence report. Appendix D shows an example of an intelligence report matrix.

IDR Planning Matrix

The IDR planning matrix is a tool that assists the CM/DO in managing the MAGTF intelligence dissemination effort. Using an IDR planning matrix helps keep the focus on the commander's decision points, PIRs, and other key IRs. This format may be tailored as needed per unit SOP. See appendix C.

Develop the Dissemination Plan

The intelligence dissemination plan must be fully integrated with MEF collections and production operations; clearly state how the intelligence will

EXAMPLE

Notional MEF Intelligence Support to Targeting Flow

Targeting Related IR Management. Targeting-related IRs will be submitted by higher, adjacent, and subordinate elements. These will be submitted to the CM/DO in the intelligence operations center (IOC). The CM/DO will consult with the P&A cell and other producers to determine if they can answer the request. If yes, they will do so per either the production or dissemination plan, disseminate products as appropriate, and also post the answer or the product on the intelligence homepage. If the analysts cannot answer the request, they will so notify the CM/DO who will then prioritize and request collection.

Support to Time-Sensitive Targeting. Each potential source of time-sensitive targeting intelligence must make decisions on whether the combat information received constitutes high-payoff target reporting (HPTR), and if it is targetable. Daily guidance reflecting changes to the commander's intent, G-3 force fires targeting priorities, the daily targeting board, and the G-2/IOC's PIRs, and intelligence reporting criteria provides this. A tracking and identification code/system should be established for these reports. Reactive targeting occurs when high-payoff targets (HPTs) are located. This time-sensitive intelligence is collected and disseminated through the organization responsible for reporting from the sensor concerned. Generally, information will come to the MEF G-2 and its IOC through the SARC or the COC intelligence watch (point of contact for friendly unit intelligence and combat information reporting). In special cases and when authorized, this flow may be direct from a specialized intelligence unit to designated recipients (for example, from the radio battalion's operational control and analysis center to the COC).

Immediate Dissemination of High-Value Target Reporting. If the information is not an HPT or battle damage assessment (BDA) report, it is moved to the P&A cell for analysis. The P&A cell will review all reports to determine if they are high-value, time-sensitive intelligence. If yes, it will note who needs to see it and immediately disseminate it per the dissemination plan and intelligence reporting criteria. If no, it will determine who needs to see it, internal to the G-2, for use in subsequent intelligence P&AO.

Analysis and Dissemination of Intelligence Products. P&A cell analysts will process the information against the current and estimated future enemy situation using other relevant intelligence and databases as appropriate. Time-sensitive intelligence will rapidly be incorporated by the analyst into an intelligence report that is disseminated immediately per the dissemination plan and current reporting criteria. Where immediate dissemination is not required, the analyst will likely forward the intelligence for possible inclusion in the intelligence summary or other intelligence products. Where targets are developed through the analytical process, the analysts will forward all targets to P&A cell's target analysis/BDA team for follow-on support to the targeting process.

be delivered to the requestor; and be flexible enough to adapt to ongoing tactical developments. The dissemination plan must determine both the physical means of dissemination and procedures to be followed in transmission.

Design and Coordinate the Dissemination Architecture

An intelligence dissemination architecture should be designed schematically so that it depicts links from the source to the recipient. It should depict organizations, intelligence systems, and CIS connectivity among the forces' intelligence collectors/producers and the supported decision makers/planners and C2 nodes. It must encompass the different types of intelligence support, from higher HQ produced all-source intelligence through time-sensitive tactical intelligence information. To account for different types of data and intelligence, several linkages may need to be constructed. It must also depict both primary and alternate channels for standard and broadcast dissemination. The following must be incorporated:

- Detail the various means for dissemination: digital networks, radio, wire, and courier communications channels, to include MAGTF common as well as dedicated intelligence systems and architectures.
- Provide primary and alternate plans for standard, alarm, supply-push, and demand-pull capabilities.
- Account for different types of data forms and intelligence, to include that requiring special or unique security controls (for example, SCI).

The ISC has principal staff responsibility for the dissemination architecture. IDR architecture needs should be stated within the broader intelligence C2 and CIS requirements, approved by the G-2 and the commander, and then provided in a prioritized list to appropriate G-3/S-3, G-5/S-5, and G-6/S-6 planners. Tailored copies may also be provided to higher and subordinate intelligence officers to support collaborative detailed planning.

Establish Dissemination Procedures

Dissemination procedures should be established for the delivery of intelligence from producers. The precedence of transmission (for example, routine and flash) should be agreed upon by all involved parties in advance. Audiences should be predetermined by defining broadcast parameters. Reporting thresholds and filters should be identified early.

Plan and Manage the Common Tactical Picture, Common Operational Picture

The dissemination of common tactical picture (CTP) track data, its subsequent processing, and further dissemination must be planned for, monitored, and managed. Track management procedures must be established to achieve a useful CTP within the higher level common operational picture (COP) environment. Each echelon of command, beginning at the tactical maneuver battalion/aviation squadron level, reports and manages the track database for its own units and those attached or in DS. Track data should be auto-forwarded via broadcast up to the next higher echelon until it reaches the MAGTF CE. Once correlated, track data is rebroadcast back down to each subsequent echelon as the MAGTF CTP. As track data is updated it automatically updates each echelon database and CTP. This dissemination process must be carefully managed.

Communications Security

The effective dissemination of intelligence requires secure communication means. COMSEC planning considerations include the following:

- Coordinate with the appointed SSOs in all units authorized to receive and use SCI.
- Adhere to SCI security handling, processing, and storage requirements.

- Obtain authority and establish procedures for the sanitization of SCI products, reports, and other information.
- Determine and coordinate SCI and GENSER LANs and WANs.
- Determine and coordinate both SCI and GENSER courier requirements and operations.
- Determine COMSEC materiel system requirements for intelligence and SCI communications.
- Determine communication requirements between sensitive compartmented information facilities (SCIFs), tactical sensitive compartmented information facilities (TSCIFs), supporting security forces, and supported units.

Allocate Resources

The intelligence officer, in coordination with the unit's communications officer, should allocate available personnel and equipment resources to support the dissemination requested. Requirements must be estimated and resources allocated for routine and time-sensitive operations, with sufficient redundant capabilities for each.

Monitor Execution

A wide range of intelligence dissemination will be occurring simultaneously. It is critical to constantly evaluate its effectiveness, the quality of support provided to commanders, and rapidly identify and resolve problems as follows:

- Develop a dissemination tracking matrix to record receipt of major and/or critical intelligence and products by intended recipients. (See fig. 4-1)
- Determine if the user is satisfied with the quality and quantity of intelligence.
- Supervise adherence to specified dissemination priorities and reporting criteria.
- Ensure that no precedence abuse exists or information overload occurs to degrade or overload communication channels.

Maintain awareness of the operational status of all supporting CIS, as well as the status of PIRs, IRs, and IDRs, to rapidly make necessary changes consistent with ongoing operations.

Unit	Watch Officer		HQ BN		G-1		TAC UNIT		**MOBILE**		G-3		G-4		G-6		**2d Mar**		**6th Mar**
PRODUCT	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent

Figure 4-1. Sample Dissemination Tracking Matrix.

CHAPTER 5
INTELLIGENCE ESTIMATES AND STUDIES

Intelligence estimates, studies, reports, and briefings are the principal intelligence products disseminated during MAGTF operations. Detailed information on preparing each is contained in MCWP 2-12, *MAGTF Intelligence Production and Analysis*.

Dissemination

Disseminating intelligence estimates and studies provides large amounts of detailed data in support of general operational planning. Many estimates and studies are scheduled production documents; however, estimates and studies may be produced and distributed quickly during a rapidly developing crisis. Intelligence estimates and studies may be disseminated via paper copy or a computer diskette mailed to a predetermined distribution list or electronically via a secure datalink. In most cases, broader dissemination will be possible by posting these products on Web pages accessible by the intended recipient.

Advantages versus Disadvantages

Intelligence estimates and studies are often accompanied by overlays, color graphics, and other aids in a standardized format. Once disseminated, these documents are available for continuous reference. But while intelligence estimates and studies can serve as invaluable background references, they require significant time and resources to produce. These products are prepared with a specific information cut-off time and may be difficult to update quickly. In a crisis, intelligence estimates and studies may be difficult to reproduce mechanically for rapid dissemination to all necessary subordinate units. Reproduction or reformatting of imagery and geospatial information materials can be particularly difficult.

Intelligence Estimate

The intelligence estimate is the primary means for providing basic and current intelligence and results of the intelligence preparation of the battlespace (IPB) effort focused on a specific mission. It is usually the first significant intelligence product developed to support initial orientation, immediate mission analysis, and other planning needs. The scope and detail of the estimate will be determined by the following:

- Resources of the command preparing it.
- Nature of the operation.
- Available intelligence.
- Identified IRs.
- Prior contingency planning.
- Time and resources available.

The intelligence estimate should be succinct, yet provide commanders and staffs the necessary intelligence for planning and early decisionmaking. A summary of basic intelligence, the estimate normally uses supporting studies for in-depth treatment of specific aspects of the enemy situation or the area of operations (AO). Whenever possible, the intelligence estimate should clearly present the analysis and conclusions developed during IPB. When contained in an OPLAN or OPORD, the intelligence estimate is typically found in Appendix 11 to Annex B. The finished estimate may be written, graphic or verbal in form. Subparagraphs and tabs may be added and omitted, based on their relevance to the stated mission. For topics that require a large

amount of data, information and intelligence (for example, beaches, weapons capabilities, and technical characteristics), the salient facts, and conclusions should be summarized in the body of the estimate with details included as a tab(s).

MAGTF Contingency Intelligence Study

This is a baseline intelligence study prepared in advance for standing OPLANs and likely contingencies. It is based on the intelligence estimate format and can be updated relatively quickly and converted into an intelligence estimate when an alert or warning order is received.

Intelligence Studies

Intelligence studies deliver detailed intelligence on specific aspects of the AO or threat (for example, beaches, minefields, helicopter landing zones (HLZ)s, hydrography or airfields). Studies directly support intelligence estimates. Wherever possible, standardized formats should be used and essential intelligence should be transformed into graphics. Unit intelligence studies should be disseminated at least two echelons upward and downward, especially if the intelligence contained in the study is derived from organic collection assets.

Target/Objective Studies

Target/objective studies are focused, detailed intelligence products that aid in the application of fires or the maneuver of forces against a specific target set or area. These studies can also be used by small units for mission preparation and execution. Target/objective studies are graphically oriented and may use many of the graphics derived during the IPB process. This intelligence product provides tailored, detailed, mission-specific intelligence in support of small unit execution. It usually consists of text descriptions that are supported by graphics. Graphics may include annotated imagery, map enhancements, terrain models, blueprints, diagrams, and schematics. Target folders contain textual descriptions and graphics, but annotated imagery, map enhancements, diagrams, schematics, and mapping products are key elements. In a tactical situation, target intelligence becomes highly perishable and must be disseminated as quickly as possible to controlling, coordinating, and delivering units.

Intelligence Preparation of the Battlespace Products

IPB is a continuous, systemic process of analyzing the threat and environment presented in the intelligence estimate. IPB products provide supported commanders and planners with a graphic portrayal of the battlespace. By integrating, analyzing, evaluating, interpreting, and fusing vast amounts of textual information into symbols, IPB products convey easily understood overlays to operators and planners with detailed intelligence available in supporting text products or intelligence databases. Overlays, such as the modified combined obstacle and fields of fire overlays, quickly and effectively depict such key terrain and enemy characteristics as mobility corridors, obstacles, terrain trafficability, and threat COAs. IPB overlay updates should always be disseminated as rapidly as possible to other staff sections and subordinate units.

Standardized formats for IPB products should be used to the maximum extent possible and tailored according to the situation or a user's unique needs.

CHAPTER 6
INTELLIGENCE BRIEFINGS

The ability to prepare and convey intelligence in a clear, concise manner is an essential skill for intelligence personnel. For the operational intelligence officer, the briefings will be the most common way to disseminate intelligence to the command. However, intelligence personnel at all command levels frequently use intelligence briefings, formal and informal, to disseminate intelligence to commanders, staffs, and others.

Intelligence briefings are used to convey information in a concise, mission-oriented format. Depending on available preparation time, briefing styles can range from formal presentations with detailed hand-outs and graphics to concise verbal updates.

Dissemination

In nontactical situations, given sufficient lead-time, formal briefings can be supplemented with multimedia products. During operations, intelligence can be relayed rapidly through short verbal updates. To convey a large amount of intelligence, paper hand-outs, electronic presentations, graphics or other supplemental material covering key briefing points may accompany the verbal presentation.

The intelligence brief should focus on the intelligence and events that correspond to the CCIRs and other PIRs. Doing so ensures that the commander is given the most essential information in the shortest amount of time. This does not preclude additional information being presented. If something of significance occurs that affects the current or future plans, the commander must be informed. Good judgment must prevail.

Advantages versus Disadvantages

Briefings are an effective way to disseminate intelligence quickly. They permit interaction with the user and allow the user to provide instant feedback to the briefer on content and conclusions or to ask questions. Preparation for briefings can be time-consuming, however; and briefings usually reach only a selected audience, such as the commander's staff.

Information Brief

The most common form of briefing is the information brief. Its primary purposes are initial situation orientation for planning and enhancing situational awareness and understanding. Common examples are the initial staff orientation brief, the commander's daily update, intelligence update, intelligence estimate of supportability, mission/target intelligence brief, and the technical intelligence brief.

Initial Staff Orientation Brief

The initial staff intelligence orientation brief disseminates important characteristics of the AO and the threat. Its goal is to indoctrinate key personnel to the overall intelligence perspective concerning an impending operation and to rapidly focus commanders and key planners on mission critical factors. The initial intelligence orientation brief should generally follow the intelligence estimate format, supplying all relevant intelligence on the AO and the enemy. Much of the content of this type briefing is derived from

higher-echelon studies and estimates and is presented as basic background intelligence. Because this type briefing can easily become too long or too detailed for timely dissemination, graphics should be used wherever possible.

Commander's Daily Update Brief

Morning or evening update briefs may be formal and detailed. They are scheduled for set times once or twice per day. Intelligence may be only part of the overall briefing. The intelligence topics include the following:

- The current situation and significant events.
- CCIRs, PIRs, and IRs.
- Collection, production, and dissemination plans and their status.
- Weather.
- Estimates of future threat actions.
- At a minimum, most likely and most dangerous enemy COAs.

Intelligence Update Brief

The intelligence update brief reviews intelligence activity since the last briefing, presents the current intelligence situation, and estimates anticipated enemy activities that may affect friendly COAs. Intelligence updates are usually scheduled briefings and are designed to address predetermined periods of time such as every 12 or 24 hours. Examples include watch turnover briefs in the unit COC, IOC or SARC. The intelligence update brief follows a temporal outline, commencing with the reporting of any significant enemy activity, including any enemy losses since the last update. It presents the current enemy situation, followed by weather forecasts, as well as intelligence estimates of enemy COAs and activity during the next reporting period. The update should also address friendly intelligence collection, production, and dissemination operations.

Intelligence Estimate of Supportability

An intelligence estimate of supportability briefing evaluates friendly COAs based on the capabilities and limitations of organic and supporting intelligence, counterintelligence, and reconnaissance forces. Its goal is to assist the commander in understanding intelligence operations capabilities, with all other friendly functional capabilities, to decide the most promising friendly COA and to identify IRs. The intelligence estimate of supportability brief addresses key factors identified by intelligence personnel that may influence friendly intelligence operations that include the following:

- Terrain.
- Weather.
- Current political situation.
- Possible reactions from the civilian populace.
- Enemy's relative strengths and weaknesses.
- Susceptibility to friendly deception or psychological operations.

The briefing addresses enemy COAs, analyzes enemy COAs versus friendly COAs based on the key factors, identifies the preferred friendly COA, and offers any other recommendations to the commander.

Mission/Target Intelligence Brief

The mission/target intelligence brief provides detailed and tailored intelligence to support execution of a specific mission. The mission/target intelligence brief has no prescribed format but should contain all pertinent intelligence impacting on a specific mission or target. Normally, this type briefing provides any intelligence and other information on activity occurring or expected to occur within a predetermined radius from a target or mission area and within a predetermined amount of time from mission execution. At a

minimum, it should include an area orientation and detailed descriptions of entry points, the objective area, and the expected threat, including enemy locations, dispositions, capabilities, and vulnerabilities. Graphics should be employed extensively to portray potential enemy strengths, vulnerabilities, and potential COAs.

Technical Intelligence Brief

The technical intelligence brief provides detailed intelligence on a specific enemy weapon system, piece of equipment or functional capability and limitations. This type of briefing disseminates a substantial amount of technical and scientific intelligence in a condensed format. The technical intelligence brief has no prescribed form but should, at a minimum, provide a detailed description of the threat or weapon system and its attendant characteristics, capabilities, and vulnerabilities. If the system has associated unique visual or electronic signatures, ensure all known operating parameters are disseminated to intelligence, targeting, and key maneuver personnel. The briefing should also describe how the enemy employs the system (for example, tactics, processes, and procedures) and where it is currently deployed (for example, order of battle). Graphics should be used wherever possible to quickly convey this type of complex information.

CHAPTER 7
INTELLIGENCE REPORTS

Intelligence reports disseminate intelligence quickly to a wide audience for immediate use. Because reports contain sensitive information, they are usually transmitted by a secure communication means. Intelligence reports should be disseminated in accordance with either collection or reporting criteria or the dissemination plan. MCWP 2-12 and other MCWP and MCRP intelligence series publications provide the basic formats for these reports.

Summary Intelligence Reports

Summary intelligence reports provide the commander with an overview of significant enemy activity within a specified period of time and project anticipated enemy actions during the next reporting period. Summary reports are usually scheduled products disseminated at specific times as dictated by unit SOPs or OPLANS/OPORDs. Standard summary reports, disseminated at scheduled times, are well-suited for demand-pull dissemination, such as being posted on the MAGTF secure TDN.

Intelligence Summary

The intelligence summary (INTSUM) is a text-based or text and graphic intelligence report that provides a summary of the intelligence situation covering a specific period, normally prescribed by the unit SOP for intelligence or the intelligence annex to the OPORD (for a MEF-level operation, typically every 12 or 24 hours). It is used to report threat activities, changes to threat capabilities, and the results of further P&A. It is designed to update the original and subsequent intelligence estimates. INTSUM distribution will be in accordance with the dissemination plan, but generally will be disseminated at least to immediate higher and subordinate commands. Using the basic format, units can tailor the INTSUM to fit the situation. With new automated information systems, INTSUMs are increasingly produced in graphic form and posted on networks for wide dissemination, with links to detailed supporting intelligence products, reports, and databases. The graphic INTSUM is maintained on computer screens linked to intelligence databases or on conventional maps with displayed/accessible supporting information.

Daily Intelligence Summary

A daily intelligence summary (DISUM) is a report prepared in message form at the JTF HQ that provides higher, lateral, and subordinate headquarters with a summary of all significant intelligence produced during the previous 24-hour period. The "as of" time for the information, content, and submission time for the report will be as specified by the joint force commander. (JP 1-02)

At higher command levels, particularly JTFs and unified commands, a DISUM will usually be published every 24 hours. While INTSUMs, particularly at lower tactical echelons, provide a tactical perspective, the DISUM is broader in scope, potentially encompasses more aspects of the threat country's elements of national power, and focuses on operational-level intelligence analysis and estimates. MAGTF command elements tasked as JTF HQ will generally be required to submit DISUMs to the combatant command HQ. See the combatant command's tactics, techniques, and procedures for the DISUM format. Although generally the same, formats may vary from theater to theater.

Periodic Intelligence Summary

The periodic intelligence summary (PERINTSUM) is a report of the intelligence situation in a tactical operation (normally produced at corps level or its equivalent and higher) usually at intervals of 24 hours or as directed by the commander. (JP 1-02)

The PERINTSUM is an expanded INTSUM covering a greater period of time as dictated by the commander. It is a means for disseminating more detailed intelligence than that provided in INTSUMs or DISUMs. PERINTSUMs are normally issued by the MAGTF CE for dissemination to higher, lower, and adjacent commands. Subordinate units may also be tasked to prepare them if directed by the commander. The format for PERINTSUMs generally is the same as used for DISUMs.

Specialized Intelligence Reports

Specialized reports include event-driven intelligence reports, such as size, activity, location, unit, time, and equipment (SALUTE) reports, and various intelligence discipline-unique intelligence reports, such as tactical electronic intelligence reports, initial photographic intelligence reports, CI spot reports, surf observation reports, and bridge reports. The purpose of generating event-driven intelligence reports is to disseminate significant intelligence to the commander or to intelligence operations personnel that could immediately alter the tactical situation or to support situation development. Event-driven and other specialized intelligence reports are disseminated as required.

Intelligence Report

The intelligence report is a standardized report that is prepared and disseminated based on its importance to the current situation rather than on a specific time schedule. It is the primary means for transmitting new and significant intelligence when facts influencing threat capabilities have been observed or when a change in threat capabilities has taken place. It is prepared at all echelons by the first intelligence element acquiring the information and forming the intelligence estimate, and is disseminated as rapidly as possible to all units that need the reported information. It may be prepared on any item of intelligence, regardless of source. Each report will concern only a single item of interest.

Battle Damage Assessment Reporting

The intelligence officer (at the MEF CE level, the ISC) ensures BDA reports conform to the OPLAN, report the nature of damage inflicted or unit/systems destroyed, and assess the degree of mission success as it relates to the initial objective. When possible, BDA reporting includes the physical damage assessment (PDA) and an analysis of the consequence of the damage on the threat unit.

At each echelon, the intelligence officer compiles, refines, and validates the various sources of BDA and develops consolidated PDAs and/or combat strength assessments. Commands will forward consolidated BDA reporting of their subordinates. MSCs will typically forward a summary BDA report to the MEF, usually covering set time periods.

At the MEF level, the P&A company, intelligence battalion, is responsible for adjusting the master order of battle databases to reflect threat combat losses. The BDA cell will prepare and disseminate formal Phase I BDA reports in accordance with theater and national policies and procedures. See MCWP 2-12 for information on BDA analysis and reporting.

Mission Report

Mission reports (MISREPs) are used by aviation units to report significant results of aircraft missions and nonimagery sightings along flight routes. They employ a standardized format that includes air task/mission number or nickname, location identifiers, time on target/time of sighting, results/sighting information, and remarks. Upon completion of post-flight debriefing, squadron S-2s should disseminate MISREPs to the MAGTF G-2/S-2 by the most expeditious means possible.

Response to a Request for Intelligence

Responses to a request for intelligence (RRFIs) are nonscheduled products designed to fill gaps in knowledge identified by subordinate tactical units. RRFIs should be answered and disseminated as quickly as possible.

Intelligence Reports Plan and Matrix

Detailed guidance and instructions for dissemination of intelligence reports must be established to ensure effective, efficient, and accurate intelligence dissemination. This may be accomplished through the use of an intelligence report matrix. The CM/DO develops and updates dissemination procedures, architectures, and reporting matrixes. The intelligence report matrix is an exhibit to the intelligence reports tab to Annex B of intelligence OPLAN/OPORD. Report matrixes may be adjusted by unit SOP. See appendix D for a sample format.

APPENDIX A
MAGTF INTELLIGENCE DISSEMINATION PLAN
APPENDIX FORMAT

Tab C (Intelligence Dissemination Plan) to Appendix 16 (Intelligence Operations Plan) to Annex B (Intelligence) explains how intelligence dissemination elements supporting the MAGTF will be used to support the operation.

CLASSIFICATION

Copy no. ___ of ___ copies
ISSUING HEADQUARTERS
PLACE OF ISSUE
Date/time group
Message reference number

TAB C TO APPENDIX 16 (INTELLIGENCE OPERATIONS PLAN) TO ANNEX B (INTELLIGENCE) TO MAGTF OPORD X (U)
INTELLIGENCE DISSEMINATION PLAN (U)

(U) REFERENCES: Identify organic DOD; Director, National Security Agency; National Imagery and Mapping Agency, and other directives; combatant commander, JTF, joint force maritime component commander/joint force land component commander/joint force air component commander or other higher authorities'OPORDs, tactics, techniques, and procedures), and SOPs for intelligence dissemination operations; intelligence reporting formats or any other relevant documents that pertain to anticipated intelligence dissemination operations.

1. (U) Situation

   a. (U) Define the AO and Area of Interest. Describe the limits of the AO and area of interest. Summarize pertinent weather, terrain, and other AO characteristics and conditions as they may influence the conduct of intelligence dissemination operations.

   b. (U) Enemy. Refer to Annex B (Intelligence) and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and order of battle pertinent to intelligence dissemination operations.

CLASSIFICATION

c. (U) Assigned MAGTF Organic and Supporting Intelligence Dissemination Assets. Identify organic and supporting forces available to perform intelligence dissemination functions.

d. (U) Assumptions. (Derived during the mission analysis step of the Marine Corps Planning Process.)

e. (U) Intelligence Dissemination Considerations. List key intelligence dissemination, CIS and interoperability considerations that impact this OPLAN/OPORD.

(1) (U) Availability of national and commercial intelligence and multipurpose CIS resources.

(2) (U) Intelligence C2 and dissemination support to and from JTF or component HQ and other external commands and/or intelligence organizations.

(3) (U) Creation and manning of forward intelligence C2 and operations elements.

2. (U) Mission. State concisely the intelligence dissemination mission as it relates to the command's planned operations.

3. (U) Execution

a. (U) Concept of Operations. Summarize command relationships, task-organization, main and supporting efforts, and the scope of MAGTF and supporting intelligence dissemination operations. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations Plan) to Annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall concept of operations as they relate to intelligence operations. Outline the purpose and concept of intelligence dissemination operations, specified priorities, and summarize the means and agencies to be employed to support the operations and intelligence concepts of operations. Address the integration of JTF, other components, theater, national, and allied intelligence operations, dissemination, and CIS support.

b. (U) Dissemination Tasks for Intelligence Units and Organizations, Subordinate Units, and Detachment Commanders/Officers in Charge.

(1) (U) Orders to Subordinate, Attached, and Supporting Units. Use separate subparagraphs to list detailed instructions for each unit conducting intelligence-related dissemination operations, including the originating HQ, subordinate commands, and separate intelligence support units.

CLASSIFICATION

(a) (U) Marine division(s).

(b) (U) Marine aircraft wing(s).

(c) (U) Force service support group(s).

(d) (U) Commanding officer, intelligence battalion/intelligence support coordinator.

1 (U) Officer in charge (OIC), support cell.

2 (U) OIC, P&A cell.

3 (U) OIC, surveillance and reconnaissance cell.

4 (U) Intelligence systems officer.

5 (U) Commanding officer, CI/HUMINT company.

6 (U) Platoon commander, imagery intelligence platoon.

7 (U) Platoon commander, topographic platoon.

8 (U) OIC, joint surveillance target attack radar system common ground station.

(e) (U) Commanding officer, Marine unmanned aerial vehicle squadron.

(f) (U) Commanding officer, Marine tactical electronic warfare squadron.

(g) (U) Commanding officer, radio battalion.

(h) (U) Commanding officer, force reconnaissance company.

(i) (U) OIC, national intelligence support team (if attached).

(2) (U) Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached or supporting and from which intelligence dissemination support is requested, including other components, JTF HQ, allied or coalition forces, theater, and national operational and intelligence elements.

CLASSIFICATION

c. (U) Coordinating Instructions. Reference Appendix 16 (Intelligence Operations Plan), Annex K (CIS), Annex J (C2), as well as command, other unit, intelligence and CI SOPs. Detail here or in supporting tabs key changes to unit SOPs. Additional topics to include are as follows:

- Requesting dissemination support.
- Timely reporting procedures for intelligence CIS problems.
- Coordinating switchover to backup dissemination paths.
- Intelligence operations.
- C2.
- CIS hand over between command echelons.

(1) (U) General Dissemination Guidance and Procedures. Use separate subparagraphs to list detailed instructions for routine and time-sensitive dissemination, precedence of transmissions, predetermined recipient lists, general and specific broadcast parameters, reporting thresholds and reporting filters.

(2) (U) Intelligence Reporting Criteria

(3) (U) Resource Allocation. Discuss dissemination resource allocation between the main and supporting efforts, and between support to current operations and support to future operations.

(4) (U) Intranet Management. List detailed instructions for homepage and database management, to include authorities for posting, updating, and removing information and intelligence.

(5) (U) Common Operational Picture/Common Tactical Picture. List detailed instructions for track data and auto-forwarding, broadcast times, and boundary/ track ownership responsibilities.

(6) (U) Formats and Standardization. Provide formats for internal and external MAGTF intelligence dissemination and reporting, preformatted templates and/or where to find these referenced elsewhere in the OPORD. Include standards and limits on size and composition of files attached to electronic mail.

CLASSIFICATION

4. (U) Administration and Logistics

a. (U) Logistics. Reference Annex D (Logistics). Identify intelligence dissemination logistics requirements and concerns, such as follows:

- Unique combat service support requirements (batteries, unique replacement parts).
- Procedures, and other guidance to support MAGTF intelligence units and operations.
- Procedures for specialized technical logistics support necessary from external organizations.
- Map distribution.
- Requirements for courier runs.

b. (U) Personnel. Identify personnel requirements and concerns that affect intelligence dissemination operations and support (systems administrators or global sourcing requirements).

5. (U) Command and Control

a. (U) Command Relationships. Reference Annex J (Command Relationships). Provide any instructions necessary regarding MAGTF command relationships that will influence intelligence operations and dissemination support.

b. (U) Information Management. Reference Annex U (Information Management), Annex C (Operations) and Appendix 16 (Intelligence Operations Plan). Provide any instructions necessary regarding information management (time-sensitive and routine reporting criteria, intelligence databases, reports) that will influence MAGTF intelligence dissemination, reporting, and other operations.

c. (U) Communications and Information Systems. Reference Appendix 16 (Intelligence Operations Plan) and Annex K (CIS). Provide any instructions necessary regarding CIS that will influence MAGTF intelligence dissemination operations. List intelligence dissemination priorities (by operational phase, intelligence units, operational intelligence and C2 nodes, and intelligence activities. Choose the most effective approach for the operation.

CLASSIFICATION

d. (U) Intelligence C2 Nodes and Facilities. Reference the unit's SOP and Appendix 16 (Intelligence Operations Plan). Provide any guidance and instructions necessary regarding establishment and operation of intelligence C2 nodes and facilities and dissemination support and priorities to these to include as follows:

- G-2/S-2 elements within future plans.
- Future operations.
- Current operations, and force fires centers.
- IOC's support cell.
- SARC and P&A cell.
- CI/HUMINT company command post.
- Reconnaissance operations center.
- Operations control and analysis center.
- Command element tactical or rear echelons.
- Intelligence liaison elements.

TABS:
A Intelligence Dissemination Flow Diagram(s)
B Intelligence Dissemination Requirements Matrix

CLASSIFICATION

APPENDIX B
INTELLIGENCE COMMUNICATIONS AND INFORMATION SYSTEMS PLAN APPENDIX FORMAT

Tab D (Intelligence CIS Plan) to Appendix 16 (Intelligence Operations Plan) to Annex B (Intelligence) explains how intelligence CIS elements supporting the MAGTF will be used to support the operation.

CLASSIFICATION

Copy no. __ of __ copies
Copy no. ___ of ___ copies
ISSUING HEADQUARTERS
PLACE OF ISSUE
Date/time group
Message reference number

Tab D TO APPENDIX 16 (INTELLIGENCE OPERATIONS PLAN) TO ANNEX B (INTELLIGENCE) TO MAGTF OPORD X (U)
INTELLIGENCE COMMUNICATIONS AND INFORMATION SYSTEMS PLAN (U)

REFERENCES: Identify organic DOD; Director, National Security Agency; National Imagery and Mapping Agency; and other directives; combatant commander, JTF, joint force maritime component commander/joint force land component commander/joint force air component commander or other higher authorities' OPORDS, TTP, and SOP for intelligence CIS operations; formats; and any other relevant documents that pertain to anticipated intelligence operations.

1. (U) Situation

a. (U) Define the AO and Area of Interest. Describe the limits of the AO and area of interest. Summarize pertinent weather, terrain, and other AO characteristics and conditions as they may influence the conduct of intelligence CIS operations.

b. (U) Enemy. Refer to Annex B (Intelligence) and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and order of battle pertinent to intelligence CIS operations.

CLASSIFICATION

c. (U) Assigned MAGTF Organic and Supporting Intelligence CIS Assets. Identify organic and supporting forces available to perform C2 or intelligence CIS functions.

d. (U) Assumptions. Derived during the mission analysis step of the Marine Corps planning process.

e. (U) Intelligence CIS Considerations. List key intelligence CIS and interoperability considerations that impact this OPLAN/OPORD.

(1) (U) Availability of national and commercial intelligence and multipurpose CIS resources.

(2) (U) Intelligence C2 and dissemination support to and from JTF/component HQ and other external commands and intelligence organizations.

(3) (U) Creation and manning of forward intelligence C2 and operations elements.

2. (U) MISSION. State concisely the intelligence CIS mission as it relates to the command's planned operations.

3. (U) Execution

a. (U) Concept of Operations. Summarize command relationships, task organization, main and supporting efforts, and the scope of MAGTF and supporting intelligence CIS operations. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations Plan) to Annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall concept of operations as they relate to intelligence operations. Outline the purpose and concept of intelligence CIS operations, specified priorities, and summarize the means and agencies to be employed to support the operations and intelligence concepts of operations. Address the integration of JTF, other components, theater, national, and allied intelligence operations and CIS support.

b. (U) CIS Tasks for Intelligence Units and Organizations, Subordinate Units, and Detachment Commanders/Officers in Charge.

(1) (U) Orders to Subordinate, Attached, and Supporting Units. Use separate sub-paragraphs to list detailed instructions for each unit conducting intelligence-related dissemination operations, including the originating HQ, subordinate commands, and separate intelligence support units.

CLASSIFICATION

(a) (U) Marine division(s).

(b) (U) Marine aircraft wing(s).

(c) (U) Force service support group(s).

(d) (U) Commanding officer, intelligence battalion/intelligence support coordinator.

1 (U) OIC, support cell.

2 (U) OIC, P&A cell.

3 (U) OIC, SARC.

4 (U) Intelligence systems officer.

5 (U) Commanding officer, CI/HUMINT company.

6 (U) Platoon commander, imagery intelligence platoon.

7 (U) Platoon commander, topographic platoon.

8 (U) OIC, joint surveillance target attack radar system common ground station.

(e) (U) Commanding officer, Marine unmanned aerial vehicle squadron.

(f) (U) Commanding officer, Marine tactical electronic warfare squadron.

(g) (U) Commanding officer, radio battalion.

(h) (U) Commanding officer, force reconnaissance company.

(i) (U) OIC, national intelligence support team (if attached).

(2) (U) Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached or supporting and from which intelligence CIS support is requested, including other components, JTF HQ, allied or coalition forces, theater, and national operational and intelligence elements.

CLASSIFICATION

c. (U) Coordinating Instructions. Reference Appendix 16 (Intelligence Operations Plan), Annex K (CIS), Annex J (C2), and command, other unit, intelligence and CI SOPs. Detail here or in supporting tabs key changes to unit SOPs. Additional topics to include are as follows:

- Requesting CIS support.
- Timely reporting procedures for intelligence CIS problems.
- Coordinating switchover to backup dissemination paths.
- Intelligence operations.
- C2.
- CIS hand over between command echelons.

4. (U) Administration and Logistics

a. (U) Logistics. Reference Annex D (Logistics). Identify intelligence CIS logistics requirements and concerns, such as follows:

- Unique combat service support requirements (batteries, unique replacement art).
- Procedures, and other guidance to support MAGTF intelligence units and operations.
- Procedures for specialized technical logistics support necessary from external organizations.
- Requirements for courier runs.

b. (U) Personnel. Identify personnel requirements and concerns that affect intelligence CIS operations and support (systems administrators, global sourcing requirements).

5. (U) Command and Control

a. (U) Command Relationships. Reference Annex J (Command Relationships). Provide any instructions necessary regarding MAGTF command relationships that will influence intelligence operations and CIS support.

b. (U) Information Management. Reference Annex U (Information Management), Annex C (Operations) and Appendix 16 (Intelligence Operations Plan). Provide any instructions necessary regarding information management (time-sensitive and routine reporting criteria, intelligence databases, reports) that will influence MAGTF intelligence CIS, reporting, and other operations.

CLASSIFICATION

c. (U) Communications and Information Systems. Reference Appendix 16 (Intelligence Operations Plan) and Annex K (CIS). Provide any instructions necessary regarding CIS that will influence MAGTF intelligence dissemination operations. List intelligence CIS priorities by operational phase, intelligence units, intelligence operations and C2 nodes, and intelligence activities. Use the most effective approach for the operation.

d. (U) Intelligence C2 Nodes and Facilities. Reference the unit's SOP and Appendix 16 (Intelligence Operations Plan). Provide any guidance and instructions necessary regarding establishment and operation of intelligence C2 nodes and facilities and CIS support and priorities to these to include as follows:

- G-2/S-2 elements within future plans.
- Future operations.
- Current operations, and force fires centers.
- IOC's support cell.
- SARC and P&A cell.
- CI/HUMINT company command post.
- Reconnaissance operations center.
- Operations control and analysis center.
- Command element tactical or rear echelons.
- Intelligence liaison elements.

TABS:

A Intelligence CIS Architecture Diagrams

- Include an diagram for the overall, overarching intelligence CIS architecture.
- Include diagrams by intelligence discipline (imagery intelligence, signals intelligence, HUMINT) if possible and useful for the operation.
- Include blueprints and CIS wire diagrams for all intelligence C2 and operations nodes and facilities, as appropriate.

B Intelligence Information Management Flow Diagram(s)

APPENDIX C
SAMPLE INTELLIGENCE DISSEMINATION REQUIREMENTS PLANNING MATRIX

The sample IDR planning matrix is developed to assist in dissemination planning and includes the following information.

Requestor: identify the unit name or staff section that requested the intelligence or products. If the requestor has assigned the IR a control number, also list the control number here.

CCIR/PIR/IR: identify the supported CCIR, PIR or IR. This may be either a short text description or its control number.

Likely Collection Timeframe: ranges from "anytime" to specific windows of opportunity for collection (for example, related to anticipated time or operational phase requirements).

Source: source of intelligence collection. This may be depicted either by intelligence discipline (for example, SIGNET, ground reconnaissance) or by specific collector (for example, unmanner aerial vehicle, EA-6B, HUMINT exploitation team).

Who Needs Intelligence First: most immediate distribution recipient(s). This may be the original requestor and/or a list of units identified during COA wargaming. Specifically identify each unit by unit name, staff section or node.

Timeliness: (hours, minutes, seconds). Factor in users who need finished analysis and who needs semi-finished, single-source analysis.

Currency: (hours, minutes, seconds): Usually there is a direct proportional relationship between timeliness and currency requirements. Basic intelligence analysts, for example, may need current information for event by event analysis, but their timeliness requirements are less critical than that needed by I&W analysts or the G-3.

Periodicity of Reporting: (days, hours, minutes, seconds or as event occurs): Usually used when reporting surveillance results or tracking critical threat targets or emerging events. Nothing significant to report or negative reports are required unless otherwise directed.

General Product Type: Some examples follow:

- Structured text—usually to fill a database (e.g., order of battle database) or correlator (e.g., electronic intelligence correlator).
- Unstructured text—freeform.
- Raw digital stream—usually to fill a database or correlator.
- Analog voice.
- Digital voice.
- Video (tape or digital stream).
- Raster graphic (scanned/bitmapped photos, maps).
- Vector graphic (vector maps, some imagery products).
- Combination of formats.

Specific/Unique Product Requirements: for each general product type, identify any specific or unique product or format requirements.

Standard Channel(s): identify the primary and first alternate communication channel for standard reporting.

Alarm Channel(s): identify the primary and first alternate communication channel for time-sensitive dissemination.

Quantity: usually only used for hardcopy dissemination. Identify specific quantity for each recipient.

Deliberate Follow-up: identify if positive personal follow-up is required with any recipient subsequent to dissemination. If so, state who is responsible, with whom and when. Such follow-up is typically required when answering a CCIR.

Acknowledge Receipt Necessary? Yes or No. The communications data network may do this automatically.

APPENDIX D
INTELLIGENCE REPORTS
DISSEMINATION MATRIX FORMAT

This appendix provides a sample of an intelligence report dissemination matrix, used to ensure understanding and efficiency in dissemination of intelligence reports. It may be used as an exhibit to Tab E (Intelligence Reports) to Appendix 16 (Intelligence Operations Plan) to Annex B (Intelligence).

INTEL REPORT	ORIGIN	DISSEMINATION METHOD	VIA	COMMS PATH	MEF G-2/IOC FILTER

APPENDIX E
GLOSSARY

Section I. Acronyms

AC/S . . . . . assistant chief of staff
AO. . . . . area of operations

BDA . . . . . battle damage assessment

C2 . . . . . command and control
C2PC. . . . . command and control personal computer
CCIR . . . . . commander's critical information requirements
CE . . . . . command element
CI . . . . . counterintelligence
CIS . . . . . communications and information systems
CM/DO . . . . . collection management/ dissemination officer
COA . . . . . course of action
COC . . . . . combat operations center
COMSEC . . . . . communications security
COP. . . . . common operational picture
CTP . . . . . common tactical picture

DISUM . . . . . daily intelligence summary
DOD . . . . . Department of Defense
DS . . . . . direct support
DSN . . . . . Defense Switched Network
DSNET . . . . . Defense Secure Network

G-1 . . . . . manpower or personnel officer (major subordinate commands and larger organizations)
G-2 . . . . . intelligence officer (major subordinate commands and larger organizations)
G-3 . . . . . operations officer (major subordinate commands and larger organizations)
G-4 . . . . . logistics officer (major subordinate commands and larger organizations)
G-5 . . . . . plans officer (major subordinate commands and larger organizations)
G-6 . . . . . communications and information systems officer (major subordinate commands and larger organizations)
GENSER. . . . . general service

HLZ. . . . . helicopter landing zone
HPT . . . . . high-payoff targets
HPTR . . . . . high-pay off target reporting
HQ. . . . . headquarters
HUMINT . . . . . human intelligence

I&W . . . . . indications and warning
IAS . . . . . intelligence analysis system
ICR . . . . . intelligence collection requirement
IDR . . . . . intelligence dissemination requirement
IOC . . . . . intelligence operations center
IOW . . . . . intelligence operations workstation
INTSUM . . . . . intelligence summary
IPB . . . . . intelligence preparation of the battlespace
IPR . . . . . intelligence production requirement
IR . . . . . intelligence requirement
ISC . . . . . intelligence support coordinator

J-2 . . . . . intelligence directorate of a joint staff
J-6 . . . . . command, control, communications, and computer systems directorate of a joint staff
JDISS . . . . . joint deployable intelligence support system
JIC . . . . . joint intelligence center
JTF . . . . . joint task force
JWICS. . . . . Joint Worldwide Intelligence Communications System

LAN . . . . . local area network
LTIOV . . . . . latest time intelligence is of value

MAG . . . . . Marine aircraft group

MAGTF . . . . . Marine air-ground task force
MARDIV . . . . . Marine division
MARFOR . . . . . Marine Corps Forces
MAW . . . . . Marine aircraft wing
MCDP . . . . . Marine Corps doctrinal publication
MCRP . . . . . Marine Corps reference publication
MCWP . . . Marine Corps warfighting publication
MEF . . . . . Marine Expeditionary Force
MISREP . . . . . mission report
MSC . . . . . major subordinate command

MSE . . . . . major subordinate element

NGO . . . . . nongovernmental organization
NIPRNET . . . . . Nonsecure Internet Protocol Router Network

OIC . . . . . officer in charge
OPLAN . . . . . operation plan
OPORD . . . . . operation order

P&A . . . . . production and analysis
PDA . . . . . physical damage assessment
PERINTSUM . . . . periodic intelligence summary
PIR . . . . . priority intelligence requirement

RFI . . . . . request for information
RRFI . . . . . response to request for information

SALUTE . . . . . size, activity, location, unit, time, and equipment
S-2 . . . . . intelligence officer (units and organizations below the major subordinate command level)
S-3 . . . . . operations officer (units and organizations below the major subordinate command level)
S-4 . . . . . logistics officer (units and organizations below the major subordinate command level)
S-6 . . . . . communications and information systems officer (units and organizations below the major subordinate command level)
SARC . . . . . surveillance and reconnaissance cell
SATCOM . . . . . satellite communications
SCI . . . . . sensitive compartmented information
SCIF . . . . . sensitive compartmented information facility
SIGINT . . . . . signals intelligence
SIPRNET . . . . . SECRET Internet Protocol Router Network
SOP . . . . . standing operating procedure
SSO . . . . . special security officer
SYSCON . . . . . systems control

TDN . . . . . tactical data network
TECHCON . . . . . technical control
TSCIF . . . . . tactical sensitive compartmented information facility

UHF . . . . . ultra high frequency

WAN . . . . . wide-area network

Section II. Definitions

area of operations—An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. Also called **AO**. (JP 1-02)

basic intelligence—Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (JP 1-02)

battle damage assessment—1. The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. Battle

damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. (JP 1-02) **2.** In Marine Corps usage, the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. Also called **BDA**. (MCRP 5-12C)

battlespace—All aspects of air, surface, subsurface, land, space, and electromagnetic spectrum which encompass the area of influence and area of interest. (MCRP 5-12C)

collection—In Marine Corps usage, the gathering of intelligence data and information to satisfy the identified requirements. (MCRP 5-12C)

collection asset—A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02)

collection management—1. In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 1-02)

combatant command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

combat data—Data derived from reporting by operational units. (MCRP 5-12C)

combat information—Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. See also **information**. (JP 1-02)

command and control—1. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP 1-02) **2.** Also in Marine Corps usage, the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. Also called **C2**. (MCRP 5-12C)

commander's critical information requirements—Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called **CCIR**. **NOTE**: CCIRs are normally divided into three primary subcategories: priority intelligence requirements; friendly force information requirements; and essential elements of friendly information. (MCRP 5-12C)

commander's intent—A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one

of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

commander's planning guidance—Directions and/or instructions which focus the staff's course of action development during the planning process. Also called **CPG**. (MCRP 5-12C)

component—One of the subordinate organizations that constitute a joint force. Normally a joint force is organized with a combination of Service and functional components. (JP 1-02)

coordination—The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (MCRP 5-12C)

counterintelligence—1. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02) **2.** Within the Marine Corps, counterintelligence constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. Also called **CI**. (MCRP 5-12C)

critical information—Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02)

critical intelligence—Intelligence that is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential or actual enemy. It includes but is not limited to the following: a. strong indications of the imminent outbreak of hostilities of any type (warning of attack); b. aggression of any nature against a friendly country; c. indications or use of nuclear, biological, and chemical weapons (targets); and d. significant events within potential enemy countries that may lead to modification of nuclear strike plans. (JP 1-02)

critical vulnerability—An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. Also called **CV**. (MCRP 5-12C)

daily intelligence summary—A report prepared in message form at the joint force headquarters that provides higher, lateral, and subordinate headquarters with a summary of all significant intelligence produced during the previous 24-hour period. The "as of" time for information, content, and submission time for the report will be specified by the joint force commander. Also called **DISUM**. (JP 1-02)

data—Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (JP 1-02)

database—Information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (JP 1-02)

debriefing—Interviewing of an individual who has completed an intelligence or reconnaissance assignment or who has knowledge, whether through observation, participation, or otherwise, of operational or intelligence significance. (MCRP5-12C)

decision point—An event, area, or point in the battlespace where and when the friendly commander will make a critical decision. Also called **DP**. (MCRP 5-12C)

deliberate planning—A planning process for the deployment and employment of apportioned forces and resources that occurs in response to a hypothetical situation. Deliberate planners rely heavily on assumptions regarding the circumstances that will exist when the plan is executed. (JP 1-02)

descriptive intelligence—Class of intelligence which describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: basic intelligence, which is general background knowledge about established and relatively constant conditions; and current intelligence, which is concerned with describing the existing situation. (MCRP 5-12C)

detachment—1. A part of a unit separated from its main organization for duty elsewhere. **2.** A temporary military or naval unit formed from other units or parts of units. (JP 1-02)

direct support—A mission requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance. Also called **DS**. (JP 1-02)

dissemination—Delivery of intelligence to users in a suitable form. (This term and its definition are proposed for inclusion in the next edition of MCRP 5-12C.)

dissemination management—Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12C)

electronic reconnaissance—The detection, location, identification, and evaluation of foreign electromagnetic radiations. (JP 1-02)

electronic warfare—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support. Also called **EW**. (JP 1-02)

essential elements of friendly information—1. Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. (JP 1-02) **2.** Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. Also called **EEFI**. (MCRP 5-12C)

fires—The effects of lethal or nonlethal weapons. (JP 1-02)

force protection—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the

enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called **FP**. (JP 1-02)

force reconnaissance company—A unit whose mission is to conduct preassault and deep postassault reconnaissance operations in support of a landing force and its subordinate elements. (MCRP 5-12C)

friendly force information requirements—Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition, readiness, personnel status, and logistics status could become a friendly force information requirement. Also called **FFIR**. (MCRP 5-12C)

geographic intelligence—The process of collecting, organizing, analyzing, synthesizing, disseminating, and using all-source geospatial and other intelligence information with regard to the military aspects of the terrain in support of MAGTF operations. GEOINT can include cross-country movement studies, line of sight analysis, natural and manmade obstacles, and various terrain studies (e.g., road, railroad, airfield, bridges, ports, helicopter landing zones). Also called **GEOINT**. (This term and its definition are proposed for inclusion in the next edition of MCRP 5-12C.)

global sourcing—A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

helicopter landing zone—A specified ground area for landing assault helicopters to embark or disembark troops and/or cargo. A landing zone may contain one or more landing sites. Also called **HLZ**. (JP 1-02)

high-payoff target—A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets that must be acquired and successfully attacked for the success of the friendly commander's mission. Also called **HPT**. See also **high-value target**. (JP 1-02)

high-value target—A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. Also called **HVT**. See also **high-payoff target**. (JP 1-02)

human intelligence—1. A category of intelligence derived from information collected and provided by human sources. (JP 1-02) **2.** In Marine Corps usage, human intelligence operations cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations. Also called **HUMINT**. (MCRP 5-12C)

hydrography—The science which deals with the measurements and description of the physical features of the oceans, seas, lakes, rivers, and their adjoining coastal areas, with particular reference to their use for navigational purposes. (JP 1-02)

imagery intelligence—Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called **IMINT**. (JP 1-02)

indications and warning—Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the US or allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the US, its overseas

forces, or allied and/or coalition nations; hostile reactions to US reconnaissance activities; terrorists' attacks; and other similar events. Also called **I&W**. See **information**; **intelligence**. (JP 1-02)

information—1. Facts, data, or instructions in any medium or form. **2.** The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

integration—A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. (This term and its definition are proposed for inclusion in the next edition of MCRP 5-12C.)

intelligence—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. **2.** Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02) 3. Also, in Marine Corps usage, intelligence is knowledge about the enemy or the surrounding environment needed to support decisionmaking. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence annex—A supporting document of an operation plan or order that provides detailed information on the enemy situation, assignment of intelligence tasks, and intelligence administrative procedures. (JP 1-02)

intelligence cycle—The process by which information is converted into intelligence and made available to users. (JP 1-02)

intelligence data—Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline—A well defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are seven major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), open-source intelligence, technical intelligence, and counterintelligence. (JP 1-02)

intelligence estimate—The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (JP 1-02)

intelligence operations—The variety of intelligence tasks that are carried out by various intelligence organizations and activities. Predominantly, it refers to either intelligence collection or intelligence production activities. When used in the context of intelligence collection activities, intelligence operations refer to collection, processing, exploitation, and reporting of information. When used in the context of intelligence production activities, it refers to collation, integration, interpretation, and analysis, leading to the dissemination of a finished product. (JP 1-02)

intelligence preparation of the battlespace—1. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. (JP 1-02) **2.** In Marine Corps usage, the systematic, continuous process

of analyzing the threat and environment in a specific geographic area. Also called **IPB**. (MCRP 5-12C)

intelligence report—A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called **INTREP**. (JP 1-02)

intelligence requirement—1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. **2.** A requirement for intelligence to fill a gap in the command's knowledge or understanding of the battlespace or threat forces. (JP 1-02) **3.** In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called **IR**. (MCRP 5-12C)

joint deployable intelligence support system—A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called **JDISS**. (JP 1-02)

joint force—A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (JP 1-02)

joint intelligence center—The intelligence center of the combatant command headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the combatant commander and staff, components, subordinate joint forces and elements, and the national intelligence community. Also called **JIC**. (JP 1-02)

joint intelligence support element—A subordinate joint force forms a joint intelligence support element as the focus for intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called **JISE**. (JP 1-02)

joint operations—A general term to describe military actions conducted by joint forces or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces. (JP 1-02)

joint task force—A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. Also called **JTF**. (JP 1-02)

Joint Worldwide Intelligence Communications System—The sensitive, compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called **JWICS**. (JP 1-02)

Marine Corps Planning Process—A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of mission analysis, course of action development, course of action analysis, comparison/decision, orders development, and transition. Also called **MCPP**. **NOTE**: Tenets of the MCPP include top down planning, single battle concept, and integrated planning. (MCRP 5-12C)

military operations other than war—Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to

complement any combination of the other instruments of national power and occur before, during, and after war. Also called **MOOTW**. (JP 1-02)

multinational operations—A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance. (JP 1-02)

national intelligence support team—A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. Also called **NIST**. (JP 1-02)

near real time—Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. Also called **NRT**. (JP 1-02)

noncombatant evacuation operations—Operations directed by the Department of State, the Department of Defense, or other appropriate authority whereby noncombatants are evacuated from foreign countries when their lives are endangered by war, civil unrest, or natural disaster to safe havens or the United States. Also called **NEO**. (JP 1-02)

operational control—Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called **OPCON**. (JP 1-02)

operations control and analysis center—Main node for the command and control of radio battalion signals intelligence operations and the overall coordination of MAGTF signals intelligence operations. Processes, analyzes, produces, and disseminates signals intelligence-derived information and directs the ground-based electronic warfare activities of the radio battalion. Also called **OCAC**. (MCRP 5-12C)

order of battle—The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called **OOB**. (JP 1-02)

priority intelligence requirements—1. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. (JP 1-02) **2.** In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. Also called **PIR**. (MCRP 5-12C)

production—Conversion of processed information into intelligence through the integration, analysis, evaluation, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user

requirements. (Term and definition proposed for next edition of MCRP 5-12C.)

production management—Encompasses determining the scope, content, and format of each intelligence product, developing a plan and schedule for the development of each product, assigning priorities among the various production requirements, allocating processing, exploitation, and production resources, and integrating production efforts with intelligence collection and dissemination. (MCRP 5-12C)

reach back—The ability to exploit resources, capabilities, expertise, etc., not physically located in the theater or a joint operations area, when established. (MCRP 5-12C)

reactive target—The method used for targeting targets of opportunity. It is used when time and situation do not allow for targeting; i.e., during deliberate targeting, during an attack, when defending against an attack, or upon discovery of the location of a target such as a radio jammer, tank, or antiaircraft weapon. (MCRP 5-12C)

SECRET Internet Protocol Router Network—Worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called **SIPRNET**. (JP 1-02)

sensitive compartmented information—All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are ever and above the provisions of DOD 5200.1R, *Information Security Program Regulation*.) Also called **SCI**. (JP 1-02)

sensitive compartmented information facility—An accredited area, room, group of rooms, or installation where sensitive compartmented information (SCI) may be stored, used, discussed, and/or electroncially processed. Sensitive compartmented information facility (SCIF) procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. Also called **SCIF**. (JP 1-02)

sensor data—Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radars, counterbattery radars, and remote ground sensors. (MCRP 5-12C)

signals intelligence—1. A category of intelligence information comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals, however transmitted. **2.** Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT**. (JP 1-02)

situational awareness—Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, enemy, and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. (MCRP 5-12C)

surveillance and reconnaissance cell—Primary element responsible for the supervision of MAGTF intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called **SARC**. (MCRP 5-12C)

tactical intelligence—1. Intelligence that is required for planning and conducting tactical operations. (JP 1-02) **2.** In Marine Corps usage, tactical intelligence is concerned primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather within the battlespace. Also called **TACINTEL**. (MCRP 5-12C)

target—1. An area, complex, installation, force, equipment, capability, function, or behavior identified for possible action to support the commander's objectives, guidance, and intent. Targets fall into two general categories: planned and immediate. **2.** In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. **3.** An area designated and numbered for future firing. **4.** In gunfire support usage, an impact burst that hits the target. Also called **TGT**. (JP 1-02)

target intelligence—Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. See also **target**. (JP 1-02)

track management—Defined set of procedures whereby the commander ensures accurate friendly and enemy unit and/or platform locations, and a dissemination procedure for filtering, combining, and passing that information to higher, adjacent, and subordinate commanders. (JP 1-02)

warfighting functions—The six mutually supporting military activities integrated in the conduct of all military operations are: **1. command and control—**The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. **2. maneuver—**The movement of forces for the purpose of gaining an advantage over the enemy. **3. fires—**Those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight. **4. intelligence—**Knowledge about the enemy or the surrounding environment needed to support decisionmaking. **5. logistics—**All activities required to move and sustain military forces. **6. force protection—**Actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. Also called **WF**. (MCRP 5-12C)

APPENDIX F
REFERENCES

Joint Publications (JPs)

1-02	Department of Defense Dictionary of Military and Associated Terms
2-0	Doctrine for Intelligence Support to Joint Operations
2-01	Joint Intelligence Support to Military Operations
2-02	National Intelligence Support to Joint Operations
2-03	Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-0	Marine Corps Operations
1-1	Strategy
1-2	Campaigning
1-3	Tactics
2	Intelligence
3	Expeditionary Operations
4	Logistics
5	Planning
6	Command and Control

Marine Corps Warfighting Publications (MCWPs)

2-1	Intelligence Operations
2-12	MAGTF Intelligence Production and Analysis
2-12.1	Geographic Intelligence
2-14	Counterintelligence
2-15.1	Remote Sensor Operations
2-15.2	Signals Intelligence
2-15.4	Imagery Intelligence
3-2	Aviation Operations

3-40.2 Information Management
3-40.3 Communications and Information Systems
5-1 Marine Corps Planning Process

Marine Corps Reference Publications (MCRPs)

2-1D Multi-Service Procedures for Requesting Reconnaissance Information in Joint Environment (RECCE-J)
2-1E Multi-Service Procedures for the Joint Surveillance Target Attack Radar System (J-STARS)
2-12A Intelligence Preparation of the Battlespace
2-15.3B Reconnaissance Reports Guide
5-12A Operational Terms and Graphics
5-12C Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms
5-12D Organization of Marine Corps Forces

University of Nebraska - Lincoln
DigitalCommons@University of Nebraska - Lincoln

DOD Military Intelligence | U.S. Department of Defense

8-1956

Field Manual, FM 11-30, Signal Corps Technical Intelligence, August 1956

Robert Bolin , depositor
University of Nebraska - Lincoln, rbolin2@unl.edu

Follow this and additional works at: http://digitalcommons.unl.edu/dodmilintel

Part of the Defense and Security Studies Commons, Military and Veterans Studies Commons, Other Engineering Commons, Peace and Conflict Studies Commons, and the Soviet and Post-Soviet Studies Commons

Bolin, Robert , depositor, "Field Manual, FM 11-30, Signal Corps Technical Intelligence, August 1956" (1956). *DOD Military Intelligence*. 47.
http://digitalcommons.unl.edu/dodmilintel/47

This Article is brought to you for free and open access by the U.S. Department of Defense at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in DOD Military Intelligence by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

FM 11-30

DEPARTMENT OF THE ARMY FIELD MANUAL

U. S. Army Military History Institute

MHRC FILE-ROOM
COPY 1

SIGNAL CORPS TECHNICAL INTELLIGENCE

DEPARTMENT OF THE ARMY • AUGUST 1956

*FM 11–30

FIELD MANUAL
No. 11–30

DEPARTMENT OF THE ARMY
WASHINGTON 25, D. C., *13 August 1956*

SIGNAL CORPS TECHNICAL INTELLIGENCE

		Paragraphs	Page
CHAPTER 1.	INTRODUCTION	1–5	3
2.	SIGNAL INTELLIGENCE RESPONSIBILITIES	6–14	6
3.	SIGNAL INTELLIGENCE ORGANIZATION		
Section I.	Signal Corps Intelligence Agency	15, 16	14
II.	Signal Intelligence Units	17–22	15
CHAPTER 4.	SIGNAL INTELLIGENCE OPERATIONS		
Section I.	Planning	23–26	21
II.	Sources of signal information	27–31	23
III.	Collection of signal information	32–41	25
IV.	Souvenir control	42–47	34
V.	Processing of signal information	48–54	37
VI.	Dissemination of signal intelligence	55–59	41
VII.	Signal intelligence reports	60–63	44
CHAPTER 5.	TRAINING	64–66	48
APPENDIX I.	REFERENCES		51
II.	SPOT REPORT		53
III.	EQUIPMENT EVALUATION REPORT		55
IV.	PRELIMINARY REPORT		59
V.	PERIODIC REPORT		62
VI.	EXAMPLE, TECHNICAL INTELLIGENCE PLAN		65
INDEX			69

*This manual supersedes FM 11–35, 2 September 1942.

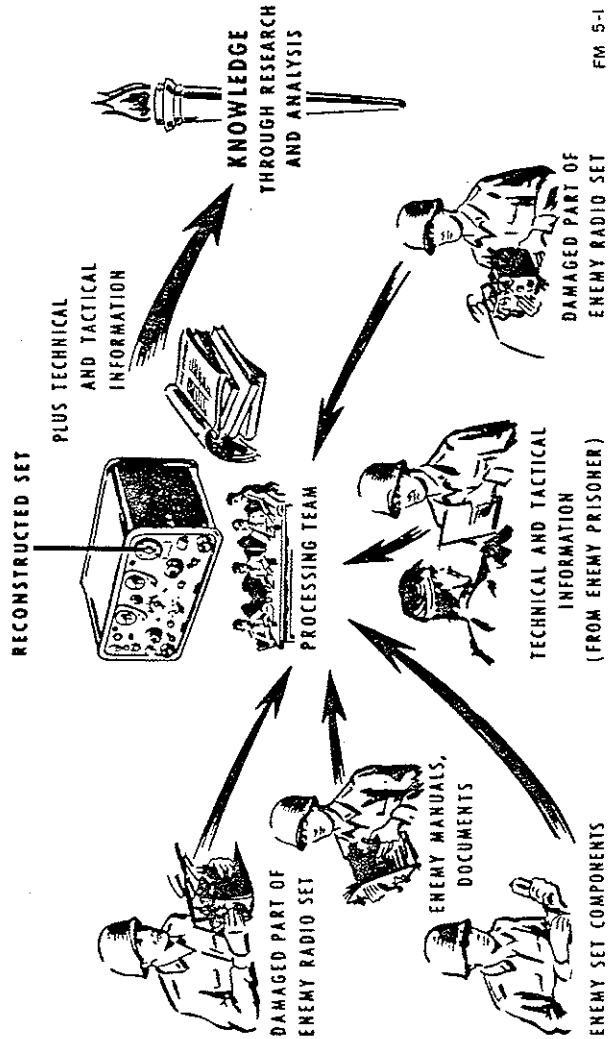


Figure 1. Signal Corps technical intelligence.

CHAPTER 1
INTRODUCTION

1. Purpose

This manual is a guide for the use of personnel concerned with signal intelligence (Signal Corps technical intelligence), and should be used in conjunction with FM 30–16.

2. Scope

The manual covers the principal phases of signal intelligence at various echelons. It describes the intelligence responsibilities of the Signal Corps, the mission, organization, and operation of signal intelligence units, and the means and methods of obtaining and processing information to produce signal intelligence (fig. 1).

3. References

Publications and training films pertaining to subjects within the scope of this manual are listed in appendix I.

4. Definitions

Signal intelligence as defined in SR 320–5–1 is to be sharply distinguished from communication intelligence, and electronic intelligence.

a. Signal intelligence is that portion of technical and scientific intelligence that is concerned with signal

and electronic equipment, systems, installations, organizations, doctrines, tactics, and techniques of foreign nations, both military and civil. It is a function of the Signal Corps and a vital element of the overall technical intelligence pattern coordinated by the Assistant Chief of Staff, Intelligence (ACSI).

b. Communication intelligence consists of information obtained by intercepting enemy traffic and by applying electronic position finding techniques to enemy radio and radar stations. It also includes the study of the enemy's communication means, procedures, and security systems. This form of intelligence lies outside the scope of this manual. It is not a function of the Signal Corps.

c. Electronic intelligence is the collection and the technical processing for intelligence purposes, of information on non-communications, electro magnetic radiations emanating from other than atomic detonation sources. This form of intelligence functioning is not a responsibility of the Signal Corps.

5. Objectives of Signal Intelligence

The objectives of signal intelligence are—

a. To provide the army with signal intelligence concerning the vulnerability and capability of foreign communication systems, both civil and military.

b. To provide the army with signal intelligence required for the prompt and efficient use of captured signal equipment and communication systems.

c. To provide research and development laboratories with technical intelligence for possible application in developing new signal equipment and electronic countermeasures devices.

d. To provide staff officers with signal intelligence for possible inclusion in long-range strategic planning.

e. To arrive at an estimate of a foreign nation's military capabilities in the field of telecommunication, at both tactical and strategic level.

CHAPTER 2

SIGNAL INTELLIGENCE RESPONSIBILITIES

6. General

The Signal Corps is responsible for supplying signal intelligence to the Department of the Army (DA), to theater commanders, and to other authorized agencies. To meet its responsibility in this respect, the Signal Corps—

a. Trains specialists in methods of collecting and processing signal information.

b. Directs the prompt and complete study of captured signal equipment, supplies, installations, and documents, to abstract information of both tactical and strategic value.

c. Studies foreign research and development activities in the fields of radio, wire, radar, television, photography, sound and visual communication, meteorological instrumentation, radio beacons, and other communication equipment and services.

d. Maintains signal intelligence liaison with other branches.

7. Chief Signal Officer

a. Under the general supervision of the AC of S, Intelligence, the Chief Signal Officer (CSigO) controls all signal intelligence operations. The staff intelligence element of Office of the Chief Signal Officer is responsible for advising the CSigO, all staff and technical

divisions of OCSigO, and all field activities of OCSigO, on signal intelligence matters; for maintaining liaison with ACSI on technical intelligence affecting the Signal Corps; and for exercising staff supervision over field intelligence activities of the Signal Corps.

b. The Signal Corps Intelligence Agency (SCIA) is the principal field intelligence activity. The SCIA is responsible for—

(1) Producing, and keeping current files of information and intelligence for the use of both the Signal Corps and the Office of the ACSI. This includes intelligence concerning all activities in all foreign countries which parallel the U.S. Army Signal Corps, such as:

(*a*) Foreign equipment design, performance, manufacture, storage, maintenance, capabilities, and limitations.

(*b*) Foreign military communication organizations, installations, signal doctrines and techniques.

(*c*) Foreign civilian communication facilities: their nature, operating characteristics, capabilities, limitations, vulnerabilities, and military use potential, including the effects of weather, terrain, and other environmental factors.

(2) Disseminating intelligence to ACSI and to elements of the Signal Corps.

(3) Exercising technical supervision over the collection and use of signal intelligence information in theaters of operation.

(4) Processing and abstracting information from

foreign equipment received from oversea theaters.

(5) Originating and processing collection requirements for signal information and foreign signal equipment and supplies and forwarding them to ACSI for consideration at that level, or concurrently through channels, to appropriate Signal Corps elements in theaters of operation.

(6) Training personnel and units for specialization in technical analysis and the preparation of technical reports, studies, and estimates.

8. Theater, Field Army, and Corps Signal Officers

Theater, field army, and corps signal officers are responsible for—

a. Providing their respective commanders with accurate and timely signal intelligence. This is accomplished by producing and maintaining signal intelligence reports and studies, and by acquiring, producing and maintaining information and intelligence concerning foreign signal materiel, communication installations, facilities, and other fields of interest to the Signal Corps. Signal intelligence operations are coordinated with the technical requirements of G2.

b. Providing technical supervision of signal intelligence personnel in the collection, examination, and reporting on captured enemy signal materiel, communication installations, and facilities in accordance with policies and priorities established by G2.

c. Maintaining estimates of the enemy signal situation.

d. Insuring the proper dissemination of signal intelligence concurrently through the G2 and Signal Corps technical channels, except for that required exclusively for the Signal Corps.

e. Determining the extent to which captured enemy signal installations and materiel can be exploited by friendly troops.

f. Developing techniques and preparing directives for the collection of information on enemy signal installations and materiel.

g. Forwarding signal intelligence files to the SCIA upon the deactivation of assigned intelligence units.

h. Training signal personnel and units for specialization in technical analysis and the preparation of signal intelligence reports and studies.

i. Implementing and operating the system of evacuation of captured signal materiel.

j. Advising the G2 on signal technical matters and providing such assistance as may be required.

k. Providing information for training of signal personnel to foreign signal materiel to include recognition characteristics, use, and interchangeability with United States or allied signal equipment.

9. Division Signal Officer

The division signal officer supervises signal intelligence activities at division level. His duties include the dissemination of signal intelligence to higher, lower, and lateral headquarters, in conformance with G2 policy.

10. Signal Intelligence Officers

Any Signal Corps officer may—by reason of his training or his association with military or signal

intelligence activities—be selected as a signal intelligence officer. He may serve in a dual capacity, as commander of a signal intelligence unit under the operational control of the staff signal officer, and as a staff member of the signal section of the command to which he is assigned or attached. Under the direction of the staff signal officer and in accordance with G2, his responsibilities may include any or all of the following:

a. Training personnel in signal intelligence practices.

b. Evacuating captured signal equipment for intelligence purposes.

c. Training personnel in the characteristics of enemy signal equipment and its interchangeability with, or adaptability to, our own equipment.

d. Exploiting signal intelligence derived from captured maps, diagrams, and other signal intelligence targets.

e. Interrogating captured enemy signal personnel.

f. Reviewing interrogation reports for the purpose of directing additional technical interrogation of specially qualified prisoners of war (POW).

g. Implementing that portion of the collection plan that pertains to the Signal Corps' field of interest.

h. Preparing or supervising the preparation of field reports.

i. Collecting information and producing signal intelligence concerning foreign signal materiel, communication facilities, and installations required by the staff signal officer for fulfillment of G2's requirement.

11. Signal Intelligence Units

Signal Corps intelligence units are normally assigned or attached to corps, army, theater, or certain types of logistical commands. The units are responsible for exploiting any signal situation or captured signal equipment, supplies, documents, and other material that may expedite the immediate tactical mission or aid in long-range strategic planning. These units are described in paragraphs 17 through 22.

12. Signal Units

In addition to general intelligence responsibilities common to all combat and service units, signal units at all levels have specific technical responsibilities in assisting signal intelligence personnel and intelligence officers. These responsibilities normally include:

a. Reporting the capture of enemy signal installations to the nearest signal intelligence unit or officer. This report should include all available information pertaining to the location, quantity, condition, design, identification, manufacture, operation, and maintenance of equipment.

b. Safeguarding captured supplies and equipment to an extent consistent with the assigned mission of the unit.

c. Destroying captured equipment when recapture by the enemy is imminent.

d. Reporting information pertaining to captured cryptographic materiel to agencies concerned with communication intelligence and security.

13. Other Units

a. Although signal intelligence is the direct concern of specially organized units and agencies, all unit commanders should impress upon their personnel

the necessity for recognizing and reporting promptly any information pertaining to signal intelligence. By such action, individuals contribute to the production of signal intelligence and to the accomplishment of major military objectives.

b. Individuals may obtain information accidently while performing a routine mission or they may be directed to seek some particular item of information through reconnaissance or other means. In either case, considerable initiative is required. In reporting and processing information, no detail should be omitted. Information that seems unimportant at first glance or during initial processing may assume primary importance when correlated with other information. The value of information is increased when the circumstances concerning its origin—including the time it was obtained—are known. Failure to report these circumstances often renders the information valueless.

c. Individuals must also be able to recognize and report negative information. Knowledge of enemy inactivity in a given direction may have great intelligence value.

14. Intelligence Officers

Intelligence officers at all echelons are responsible for the coordination of all functions pertaining to technical intelligence. Where appropriate, intelligence sections of the general staffs of higher headquarters may have a technical intelligence officer assigned or attached to assist the G2 with the technical intelligence plan and the staff coordinating effort. At corps level and higher, the G2 is usually assisted by a technical intelligence staff officer for the purpose of supervising collection activities of a technical and scientific nature. This coordinator does not supersede the signal officer, who continues to function as the commander's technical advisor. Specific duties of the various intelligence officers are outlined in publications listed in appendix I.

CHAPTER 3
SIGNAL INTELLIGENCE ORGANIZATION

Section I. SIGNAL CORPS INTELLIGENCE AGENCY

15. General

The SCIA is a class II activity under the control of the Chief Signal Officer through the staff intelligence element of the OCSigO. The SCIA:

a. Coordinates the collection of signal intelligence.

b. Evaluates and correlates the information received.

c. Prepares signal intelligence studies.

d. Disseminates intelligence information through Signal Corps command and technical channels.

e. Maintains a research and reference service for technical signal intelligence.

f. Provides assistance on matters of organization and training of Signal Corps intelligence units.

g. Maintains liaison with other intelligence activities.

16. Operations

The SCIA:

a. Evaluates and interprets information and produces intelligence on foreign communications systems and equipment, both civilian and military.

b. Evaluates and interprets information concerning foreign electronic research and development, as well as the natural and industrial resources that provide the civilian and military communication installations, equipment, and supplies of foreign nations.

c. Exploits intelligence derived from studies of captured communication equipment and scientific information.

d. Prepares bibliographies concerning signal intelligence information required by a theater or task force signal officer.

e. Produces and maintains current intelligence concerning technical details and performance data of captured materiel.

f. Assists in the planning, activating, and training of signal intelligence units.

g. Supervises the processing and distributing of captured signal materiel as directed by the Chief of Staff, U.S. Army, to meet training requirements within the CONUS.

h. Supervises the preparation of signal intelligence manuals and training aids.

i. Disseminates completed intelligence to agencies under control of the Chief Signal Officer and supervises the transmission of such intelligence to the ACSI.

Section II. SIGNAL INTELLIGENCE UNITS

17. General

Signal Corps intelligence units are employed in the field to procure and process information promptly and to disseminate the resultant intelligence. These units serve as the basic operating and coordinating elements of signal intelligence activities.

18. Mission

Signal intelligence units are normally assigned or attached to the various echelons of command as required. These units are under the operational control of the signal officer of the command and are under the staff supervision of the appropriate G2. The general mission of the units are:

a. Collection of foreign electronic and communication equipment and materiel; study of their components, use, effectiveness, and intelligence value, including research and development; selecting, reporting, and evacuating foreign equipment and materiel for intelligence purposes, including research and development.

b. Identifying, photographing, and reporting foreign telecommunication installations, electronic equipment, documents (in coordination with G2) and similiar materiel required for signal intelligence purposes.

c. Assisting in the location, evaluation, intelligence exploitation, and reporting on foreign Signal installations and facilities, personnel, and agencies. Other activities of interest are those associated with or contributing to the planning, design, research and development, testing and production, storage, and maintenance of signal equipment. Construction of signal installations and other facilities that would be of interest to signal intelligence are also included.

d. Conducting signal intelligence exploitation of information repositories, in coordination with G2, and participating in the production and maintenance of intelligence peculiar to the needs of the Signal Corps.

e. Assisting in or conducting training of units in the special responsibilities and techniques by which those units may aid the signal technical intelligence collection effort.

19. Organization

a. There are five types of signal intelligence teams organic to a theater. These teams—TA, TB, TC, TD, and TE—are organized and equipped in accordance with TOE 11–500R. There is also a sixth type—Signal Technical Intelligence Team (class II)—attached to a major ovearsea command.

b. Each team has at least one signal intelligence officer assigned to it.

c. When required, any of these units can be augmented by administrative, mess, and automotive maintenance teams from TOE 11–500R.

20. Theater Headquarters

The TE-type team is normally attached or assigned to the theater or to a type C logistical command (fig. 2). This team—

a. Coordinates the activities of the TA-, TB-, TC-, and TD-type teams.

b. Disseminates signal intelligence within the theater of operations., in accordance with G2 dissemination policy.

c. Supervises the storage, issue, and shipment to CONUS of collected communication material.

21. Army

One TC-type team and one TD-type team are normally allocated to a field army or to a type C logistical command (fig. 3).

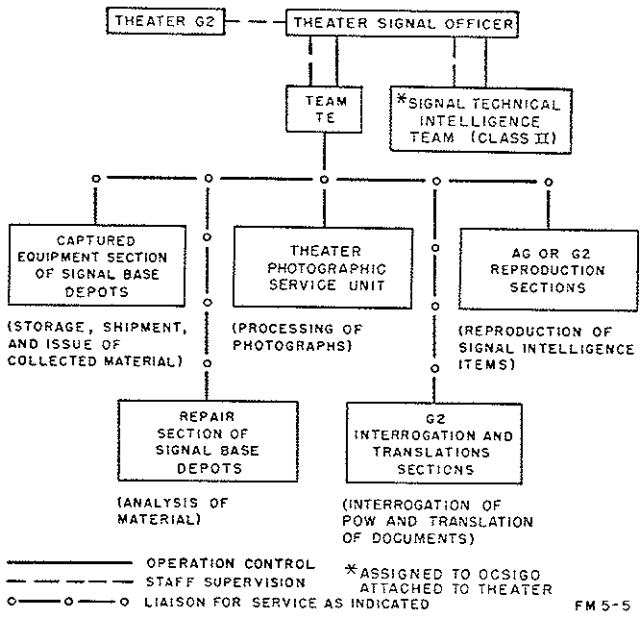


Figure 2. Signal intelligence teams at theater.

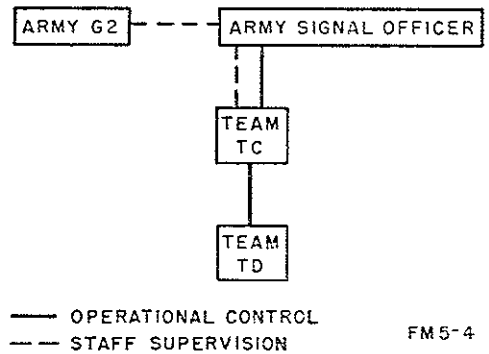


Figure 3. Signal intelligence teams at army.

a. Team TC. This team—

(1) Coordinates the activities of the TA-, TB-, and TD-type teams.

(2) Supervises the storage, issue, processing, and shipment to the rear of collected communication materiel.

b. Team TD. This team—

(1) Performs technical examination and evaluation of fixed plant communication installations and other special communication installations and equipment.

(2) Recommends the disposition of these signal installations.

22. Corps

One TA-type team and two TB-type teams normally are allocated to the headquarters of each corps or to a type B logistical command (fig. 4).

a. Team TA. This team—

(1) Coordinates the activities of two or more collection teams TB.

(2) Processes intelligence reports and forwards them to higher headquarters, within limitations of G2 policy.

(3) Provides the necessary liaison between the signal officer of the command and the G2.

b. Teams TB. These teams—

(1) Accompany advance combat elements for the capture of special communication targets.

(2) Tour afterbattle areas for the purpose of locating and safeguarding signal equipment abandoned by the enemy.

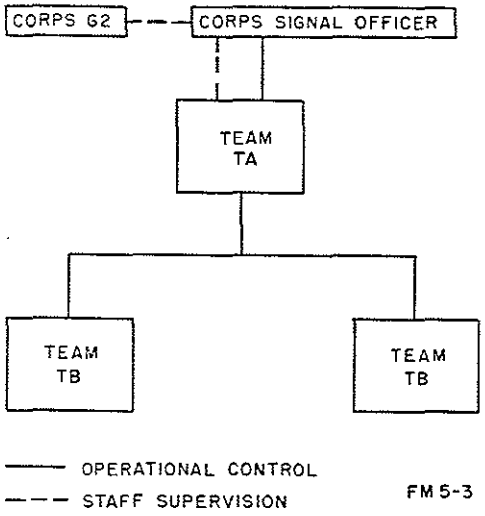


Figure 4. Signal intelligence teams at corps.

(3) Collect, photograph, and identify items of captured signal materiel.

(4) Prepare spot reports on all items collected.

(5) Process and evacuate, through team TA, items of signal intelligence.

CHAPTER 4
SIGNAL INTELLIGENCE OPERATIONS

Section I. PLANNING

23. General

Signal intelligence planning is designed to expedite the collection and exploitation of signal information and intelligence. It is a systematic process that follows a prescribed form as outlined in FM 30–16. When initial operational planning has been completed and the estimate of the signal situation has been formulated, the signal intelligence operational plan can take shape. It is based on the G2 technical intelligence and collection plans and is primarily concerned with the signal intelligence collection mission.

24. Technical Intelligence Plan

a. The theater technical intelligence plan is prepared by the theater G2 in coordination with the theater chiefs of technical services. Lower level supporting plans are prepared by the appropriate G2 in coordination with the technical service special staff officers.

b. The technical intelligence plan encompasses the operations of all technical intelligence personnel. It covers—

(1) Collection and processing of technical intelligence information.

(2) Handling of foreign materiel.
(3) Dissemination of technical intelligence.
(4) Organization for an intelligence task force operation.
(5) Employment of technical service intelligence units.

25. Collection Plan

The collection plan is prepared by the G2 to direct the overall collection program. It is prepared to cover any specific period of operation and is modified when necessary to conform to new requests and decisions made by the commander as the operation develops. The collection scheme outlined by the plan is based on an analysis of the *essential elements of information* (EEI) required by the commander.

26. Coordination of Plans

All signal intelligence planning must be coordinated with the commander's immediate plan of operation and with the G2 technical intelligence plan. At corps, army, and theater headquarters, the G2 keeps the planning section—including the signal officer—advised of all matters pertaining to enemy or indigenous communications. In turn, the signal officer keeps the G2 informed of all pertinent activities of the signal intelligence teams. At division level, the G2 coordinates his planning with the division signal officer, who coordinates with the corps signal officer and with any corps signal intelligence personnel operating within the division area.

Section II. SOURCES OF SIGNAL INFORMATION

27. General

The reliability of the *source* of any intelligence information must be carefully evaluated. The accuracy of the information itself must also be carefully evaluated by comparison with known facts. When a human factor is involved, the evaluation of the source becomes particularly important. For example, overzealous local inhabitants, in an effort to please, may give distorted information. Or the enemy may plant false deserters to deliberately distort intelligence information. Some of the more common sources of technical signal information are—

a. Captured signal equipment and installations.
b. Local inhabitants.
c. Captured enemy personnel.
d. Captured photographs, charts, diagrams, manuals, weather and terrain maps, and other documents.
e. Aerial and ground photographs made by friendly forces.
f. Weather and terrain maps made by friendly forces.

28. Captured Signal Equipment and Installations

Captured signal equipment and installations—both military and civilian—may be the best sources of technical signal information available in a theater of operations. Such information may be of technical, tactical, and strategic value. By analysis of this information:

a. Use of the equipment may be determined and effective countermeasures may be developed.

b. It may be established whether or not the enemy is in short supply of certain strategic materials.

c. It can be learned when, where, and how many units of the equipment were produced.

d. Superior qualities of workmanship may be studied and parts may be introduced into our own equipment for increased efficiency.

e. A basis may be established for the production of training literature to instruct friendly troops in the use of enemy equipment.

29. Local Inhabitants and Enemy Personnel

a. Local inhabitants of an area of operation may be willing sources of information. One of the best sources of information is the personnel of underground organizations, who are usually trained for specific information-collecting missions.

b. If skillfully interrogated, POW's may willingly or inadvertently divulge information. Technicians who have become prisoners may unintentionally reveal information because of their interest in the technical aspects of certain equipment. Prisoners may be carrying personal or official documents that furnish new information or confirm information already on hand. In addition to data on troop dispositions, communication lines, arms and equipment, information on the morale of the enemy, and the effects of psychological warfare can be obtained from prisoners.

30. Photographs

Official aerial and ground photographs may provide reliable information on the enemy's equipment, use of terrain, indigenous facilities, and lines of communication. Such photographs suggest profitable targets for specialized technical intelligence team assignments.

31. Miscellaneous

Other sources of information include such things as—

Weather forecasts and studies.
Strategic and tactical terrain surveys.
Reference data.
Studies prepared by other intelligence agencies.

Section III. COLLECTION OF SIGNAL INFORMATION

32. Introduction

Collecting captured signal equipment is one of the most important parts of the signal intelligence program. However, the program may be delayed or negated if the captured equipment is not handled and processed correctly.

a. Up to and including division, the collecting opportunities are mainly for individuals or teams whose collection activities are curtailed both by the time factor and the tactical situation. Their efforts are restricted mainly to the collection of tactical signal information.

b. At echelons above division, the information trend gradually shifts from tactical to strategic. Intelligence personnel at corps, army, and theater have more time to search larger installations and facilities.

c. To collect signal information at any level, it is necessary to know *what* to look for and *where* to find it. Basic intelligence operations and doctrine—applicable to all types of intelligence work—are

treated in detail in pertinent publications listed in appendix I.

33. Fields of Interest

Signal intelligence is concerned with information pertaining to—

Radio equipment.
Wire equipment.
Sound and visual communication equipment.
Facsimile equipment.
Television equipment.
Ground radar and recognition equipment.
Direction-finding equipment.
Power and auxiliary equipment.
Photographic equipment.
Meteorological equipment.
Proximity fuses.
Radiological detection devices.
Electronic countermeasures equipment and devices.
Guided missile guidance and control systems.

34. Targets

Any nation normally has characteristic procedures for the location of equipment and documents and for the storage and issue of supplies. Peculiarities of procedures should be studied by signal intelligence personnel. Collection methods based on such studies greatly facilitate the signal intelligence effort. Certain aspects of signal intelligence are of tactical value, certain others are of strategic value, and many overlap both fields. Tactical and strategic equipment and information are usually found in the following locations:

a. Tactical.

(1) Forward observation points.
(2) Command posts.
(3) Unit headquarters.
(4) Communication centers.
(5) Unit supply agencies and facilities.
(6) Artillery positions.
(7) Various types of signal units operating in the forward areas.

b. Strategic.

(1) Unit headquarters.
(2) Other military installations.
(3) Communication centers.
(4) Radio stations.
(5) Radar stations.
(6) Power stations.
(7) Meteorological stations.
(8) Telephone and telegraph switching centers.
(9) Laboratories, research centers, and experimental stations.
(10) Supply warehouses and storage dumps.
(11) Police and security headquarters.
(12) Railroad stations, railheads, rail centers, and other logistical control points.
(13) Civilian industrial installations.

35. Selection of Equipment and Documents for Evacuation

a. Captured equipment for evacuation should be carefully selected, and, as a rule, only those items in

the best condition should be forwarded to higher headquarters for evaluation. Quantities of equipment in excess of intelligence requirements are evacuated through normal signal supply channels. Signal documents, wherever found, should be evacuated for evaluation purposes.

b. When possible, only equipment having all of its component parts or units should be selected for intelligence purposes. Where a complete set of equipment is not available, an attempt should be made to assemble a complete set by using sound parts from damaged equipment of the same type. To determine how many pieces make up a complete set or how parts or components fit together, captured enemy signal personnel may be interrogated by arrangement with the intelligence section of the responsible headquarters.

36. Photographic Coverage

If possible, equipment and documents to be collected for intelligence purposes are photographed intact *before removal.* These photographs are made inclosures to the report relating to the collected item.

37. Equipment Tag

Frequently an item cannot be evacuated immediately. To prevent duplication of effort and to deter appropriation by souvenir hunters, the equipment is tagged as having been inspected or earmarked for collection. A typical equipment tag is shown in figure 5.

a. The tag designates the item for further signal intelligence processing, gives pertinent information concerning the item, and prevents it from being sent to disinterested agencies.

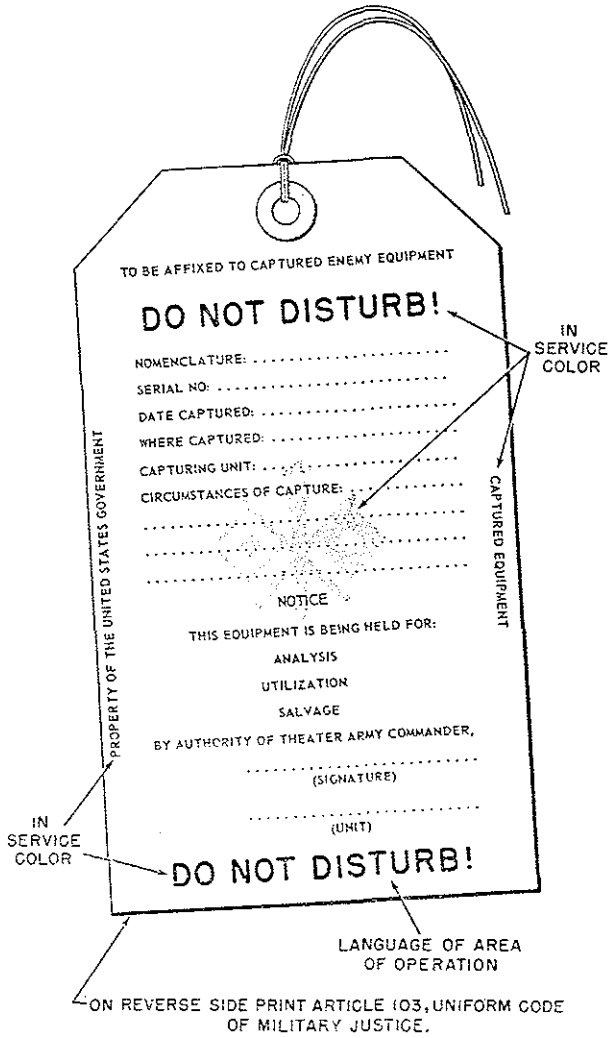


Figure 5. Typical equipment tag.

b. The tag should include Article 103 of the Uniform Code of Military Justice and provide space for the following information:

(1) Nomenclature and type number, if any.
(2) Serial number.
(3) Date, place, and circumstances of capture.
(4) Equipment identification.
(5) Notice of intended use.
(6) Authority for collection.
(7) Signature of person preparing the tag and designation of his unit.
(8) Other identifying information.

38. Collection at Different Echelons

Most of the collection of signal intelligence is done at corps level by TB collection teams, under the direction of the TA team. At army level, the TC signal intelligence team and the TD equipment evaluation team collect much less equipment and material—their major effort is in the processing of intelligence materiel collected and forwarded from corps. At theater level, collection is practically nonexistent. The flow of signal intelligence material and reports is shown in figure 6.

39. Guides to Collecting Signal Information

The amount and kind of signal intelligence to be collected differs according to whether the captured installation is military or civilian. Checklists aid individuals, teams, or other collection agencies during inspection of such installations. DA Pam 30–100 is an excellent instrument to aid all collecting agencies concerned with signal intelligence.

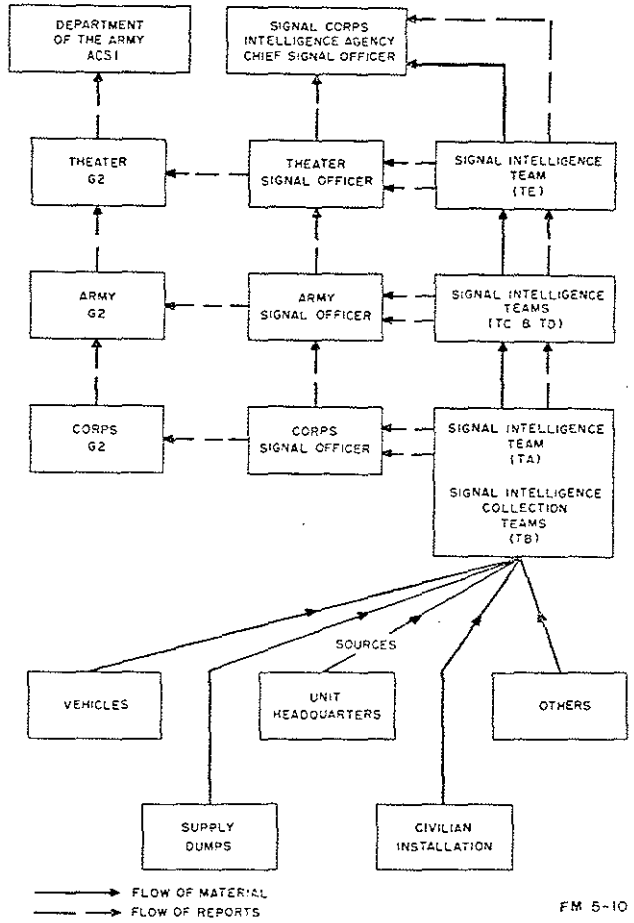


Figure 6. Flow of signal intelligence material and reports.

40. Checklist for Collecting Military Communication Information

a. Organization and Equipment of Enemy Units.

(1) Signal equipment in use by each military unit.

(2) Qualifications of personnel in enemy communication units.

(3) Communication specialist shortages.

(4) Communication terminology and map symbols.

(5) All documents pertaining to military communication and communication equipment.

b. Methods of Operation.

(1) Responsibility within the unit.

(2) Responsibility to higher units.

(3) Responsibility to lower and adjacent units.

(4) Types of radio and wire nets in use.

(5) Types of communication in use—such as telephone, telegraph, visual, and messenger facilities.

c. Telephone and Telegraph Equipment.

(1) Switchboards.

(2) Carrier and repeater equipment.

(3) Users' equipment—such as telephone, telegraph, and teletypewriter end instruments.

(4) Line materials.

(5) Line routes.

(6) Auxiliary equipment—such as power supplies, test equipment, and tools.

d. Radio Equipment.

(1) Transmitters and receivers.

(2) Remote control equipment.

(3) Antennas.

(4) Vacuum tubes and component parts.

(5) Direction-finding equipment.

(6) Special equipment, such as tone keyers, demodulators, special multiplexers, and converters.

e. Radar Equipment. Use the same checklist as for radio equipment (*d* above).

f. Meteorological and Navigational Equipment.

(1) Measuring devices.

(2) Recording devices.

(3) Special radio equipment (use checklist in *d* above).

g. Photographic Equipment.

(1) Cameras.

(2) Film.

(3) Processing equipment.

h. Other Equipment. Any other equipment used or controlled by the Signal Corps—such as visual, sonic, infrared, and flash ranging equipment.

41. Checklist for Collecting Information on Nonmilitary Civilian Communication Facilities

a. Wire Facilities.

(1) Name and location.

(2) Description.

(3) Amount, type, and capacity of equipment.
(4) Interconnection with other systems.
(5) Condition and recommendations.
(6) Outside plant.
(*a*) Open wire lines—poles, pole fixtures, number of circuits, wire gage, and transpositions.
(*b*) Aerial cable—poles, method of suspension, conductor gage and composition, and number of pairs.
(*c*) Underground cable—method and depth of laying, conductor gage and composition, and number of pairs.

b. Radio Facilities (Including Broadcasting Stations).

(1) Name and location.
(2) Description.
(3) Antenna installation.
(4) Station equipment—nomenclature of radio sets and auxiliary equipment.
(5) Current operational condition.
(6) Individual items of equipment—complete description of each item.

Section IV. SOUVENIR CONTROL

42. Introduction

Souvenir control is important to the general military intelligence mission for the prevention of unauthorized acquisition, mutilation, or cannibalization of captured enemy equipment, documents, and supplies. The need for this control is proportionate to the amount of damage that souvenir hunting may do to the intelligence effort. In combat areas, strict souvenir control is an immediate and continuing requirement.

43. Reasons for Control

a. Successful intelligence processing of captured equipment and information—both military and civilian—is expedited when the materiel is obtained in its entirety. Removal, by souvenir hunters, of any equipment components, documents, or photographs may break or prolong the intelligence process and delay vital intelligence functions.

b. Unwarranted rummaging through captured equipment and documents hampers the intelligence mission by complicating the collecting and processing of information.

c. Identifying data on captured equipment are often as vital to the success of an intelligence mission as the equipment itself. When souvenir hunters remove tags or nameplates from captured equipment, they needlessly complicate the job of intelligence personnel.

44. Signal Equipment Control

Captured signal equipment attracts the attention of equipment scavengers, as well as that of souvenir hunters.

a. Stringent controls must be exerted over captured optical equipment such as cameras, lenses, prisms, meteorological instruments, theodolites, range finders, tracking and sighting devices, and binoculars. Strict control over this type of equipment is necessary because of its small size, general attractiveness, and ease of acquisition.

b. Controls are also required over captured com-

munication equipment, such as radio sets, teletypewriters, repeaters, switchboards, and other apparatus. This equipment constitutes valuable sources of information and must not be removed, disassembled, or dismantled by unauthorized personnel.

c. Communication centers, facilities, supply depots, and technical installations seized by combat elements or an intelligence task force warrant particular precautions and provisions to prevent unintentional destruction by combat troops, delayed enemy demolition, looting, or removal by souvenir hunters. If necessary, a guard unit from an appropriate rear area organization should be provided. Since combat troops must be released as soon as the target is out of proximity to the enemy, another unit must provide normal interior guard. This may be accomplished by the provost marshal or by drawing troops from Signal Corps units, which should be prepared to remain until duly relieved.

45. Dangers of Souvenir Hunting

The individual soldier must be made to realize the dangers of souvenir hunting both to himself and to his command.

a. Booby traps present the greatest immediate personal danger to the souvenir hunter. When souvenir discipline is relaxed, the enemy will make expeditious use of this knowledge, and excessive casualties may result. Developments in chemical, bacteriological, and radiological warfare methods tend to make souvenir hunting an increasingly more dangerous activity.

b. The unwarranted destruction of captured equipment, supplies, and installations by friendly troops engaged in souvenir hunting deprives friendly forces of certain materiel that might be urgently needed for research, and also deprives intelligence personnel of potentially important sources of information.

46. Responsibility

The unit commander is responsible for the enforcement of souvenir control regulations. To stimulate interest in the collection effort, commanders must implement directives from higher headquarters governing the return of trophies turned in by members of their commands. Items that cease to be of military value should be returned to individuals after approval of G2, with a certificate, in duplicate, authorizing their retention.

47. Authority

The primary authority for souvenir control is contained in Article 103 of the Uniform Code of Military Justice. It states that enemy property—both military and civilian—becomes the property of the United States immediately upon its capture, and must not be sold or otherwise disposed of without proper authority. During combat operations, DA regulations are frequently issued to cover particular situations and to clarify control procedures relative to individual items of equipment.

Section V. PROCESSING OF SIGNAL INFORMATION

48. General

Processing includes the collation, evaluation, and interpretation of collected information. At corps

level, processing plays a relatively minor role, with increasing importance at army and theater levels. At army, it consists primarily of collating equipment and information received from teams attached to corps and from individuals and units operating below corps level, and forwarding this to theater. At theater, processing assumes a major role in the development of materiel and information into usable and timely intelligence.

49. Collation

Signal information is collated to keep data of the same categories together for convenience of selection. comparison, and coordination. In the collation of information, no facts can be disregarded. Items that seem trivial at first glance may assume primary importance upon comparison with other facts.

50. Evaluation

An item of information must be appraised in order to determine its pertinence, the reliability of the source or agency, and the accuracy of the information. A close and expeditious examination of the received information establishes its degree of relevancy and its possible value. The reliability of the source and collecting agency is also determined before the information can be evaluated. The accuracy or truth of the information itself must be determined separately from the reliability of the source and agency. The rating of the information is done in accordance with pertinent paragraphs of FM 30–5.

51. Interpretation

Interpretation is the critical analysis of the evaluated information to determine its significance with respect to information or intelligence already at hand. There are two phases to consider—first, establishing the conformity or nonconformity of new information with existing information, and second, determining its significance.

a. The purpose of interpreting signal information is not to draw conclusions as to the enemy's communication capabilities or probable courses of action, but to establish accurately the facts of the enemy situation. Proper interpretation of collected information results in intelligence that is accurate and concise, free from irrelevant matter, and ready for immediate use.

b. The probable significance of processed information must be determined in terms of past, present, and future factors. When the reliability of the source and the accuracy of an item of information have been established, the question arises as to what the information means in the light of other available information. In answering this question, important points to consider are—

(1) Does the item alter or add significance to any information previously received?
(2) Does the information tend to confirm the estimate of the enemy situation or does it tend to indicate that the estimate is incorrect?
(3) Does the information suggest that any previous information was purposely planted by the enemy for deception?

52. Processing at Corps

At corps level, processing consists principally of consolidating the information and materiel obtained

by the collection teams and other sources. It includes the intermediate steps of preparing equipment and documents for shipment to army and the dissemination of reports of immediate tactical value to the interested agencies.

53. Processing at Army

In addition to coordinating the activities of the teams attached to lower echelons, signal intelligence personnel at army level are responsible for forwarding to theater headquarters enemy signal materiel that is not authorized for retention within the army command. Equipment arriving from field collecting agencies is checked and identified for purposes of signal intelligence and for possible issue to troops. Technical installations and equipment bypassed by combat units are exploited for intelligence purposes. This is done by team TD, which analyzes and recommends disposition or use of the installation or equipment. Copies of this equipment evaluation report are disseminated to interested agencies.

54. Processing at Theater

At theater level, processing is a detailed operation that includes the steps of collation, evaluation, and interpretation. Actual procedures depend upon the signal intelligence officer, the theater signal officer, and the theater G2. In addition, signal intelligence processing activity at this level includes the supervision of the packing and shipment to CONUS of captured signal equipment in such quantities as may be required for intelligence purposes. The details of equipment evacuation are explained in applicable manuals (app. I).

Section VI. DISSEMINATION OF SIGNAL INTELLIGENCE

55. Requirements

Dissemination of signal intelligence (fig. 7) is as essential as any of the steps in its processing. Signal intelligence is of no value unless it reaches the individuals or units concerned in time to serve its purpose. To meet this requirement, dissemination of intelligence must be:

a. Specific and timely.

b. Adequate to fill the needs of the situation.

c. Broad enough to assure that the information is received by all interested agencies but limited enough to prevent its reception by agencies not requiring the information.

d. In such form that the recipients may rapidly locate details of interest to them.

e. Disseminated in accordance with established AC of S Intelligence or G2 dissemination policy at each command echelon.

56. Department of the Army

The SCIA disseminates signal intelligence outside the Signal Corps to all interested agencies authorized to receive such intelligence after approval by the Office of the Assistant Chief of Staff, Intelligence, Department of the Army. Technical bulletins and other reports are distributed through command channels to theaters of operations as required.

57. Theater

The major signal intelligence dissemination effort

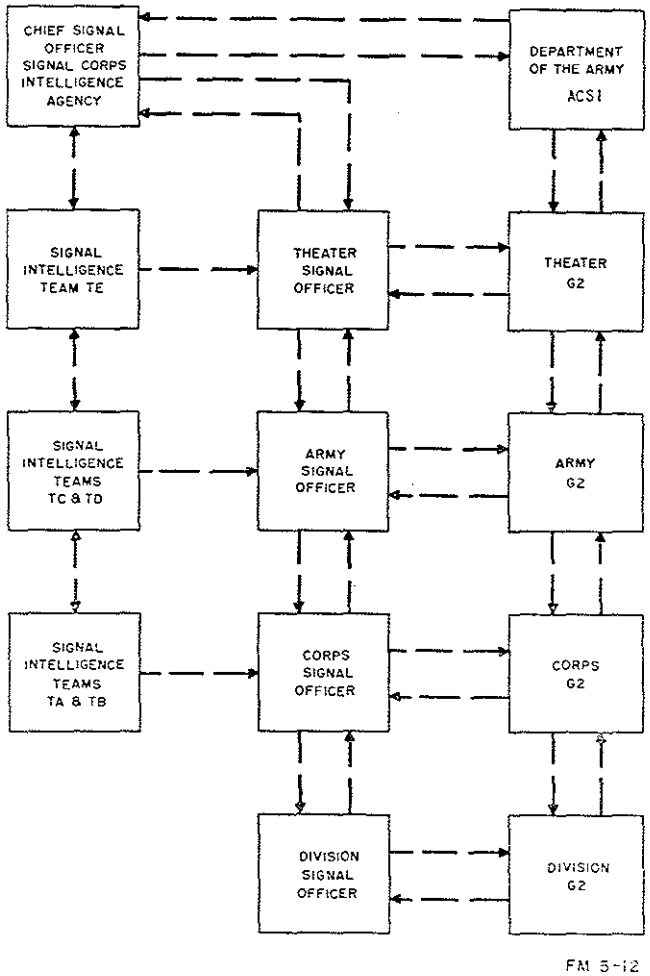


Figure 7. Dissemination of signal intelligence.

is conducted at theater level, where the TE team becomes the source of signal intelligence for all commanders within the theater. This effort is directed at all reports required to put the intelligence into the hands of the users. Normally, the periodic intelligence reports compiled and processed by the TE team are the means of dissemination. These reports are distributed to all interested commands through the theater signal officer. Information copies of all intelligence summaries, reports, and estimates are also disseminated by the theater signal intelligence officer to other signal intelligence teams as required.

58. Army

Dissemination of signal intelligence at army level is normally confined to equipment evaluation and periodic reports. These reports are distributed to—

a. Army signal officer.
b. Army G2.
c. Theater TE team.
d. Other interested commands (through the army signal officer).

59. Corps

At corps level, dissemination of signal intelligence is in the form of spot and periodic reports that have been prepared on collected items of information or equipment and that summarize signal intelligence over a given period. These reports are distributed to—

a. Corps signal officer.
b. Corps G2.
c. Army TC team.
d. Other interested commands (through corps signal officer.)

Section VII. SIGNAL INTELLIGENCE REPORTS

60. Introduction

All signal intelligence teams prepare reports. These reports are submitted to the appropriate staff signal officer and the unit G2. In turn, the signal officer transmits these reports—through technical channels—to the signal officer of his superior headquarters. Reports of interest to other commands are similarly transmitted to the appropriate signal or communications officer. Samples of various reports are given in appendixes II through V.

61. Coordination

a. To carry out their missions, signal intelligence teams must obtain much of their information and virtually all of their logistical support from units and agencies of the headquarters to which they are attached or from units subordinate to that headquarters.

b. To insure full cooperation and to maintain a good working relationship between the signal intelligence teams and their supporting agencies, the plans and operations of the teams must be coordinated at the headquarters to which they are attached. Most of this staff coordination can be arranged with G2 through the signal officer.

c. Other staff sections are often concerned with signal intelligence team activities, and they must be kept informed. For this reason, the distribution or routing of information copies of reports should be frequently reviewed.

62. Types of Reports

Special and periodic reports are prepared by the various units and agencies concerned with signal intelligence. These reports are disseminated in accordance with G2 policy.

a. Special reports are prepared whenever a useful item of information becomes available. Several different types of special reports are prepared by the different echelons of signal intelligence.

b. Periodic reports are prepared at specific intervals to keep interested echelons and agencies currently informed of the overall intelligence effort. They are prepared by signal intelligence teams at all echelons.

c. Specific types of reports are listed in the following table. This table also shows who prepares each type of report, to whom the report is normally distributed, and the general content of each type of report.

Type and designation	Prepared by—	Directed to—	General content
Spot (special).	Teams TA and TB	Corps SigO Team TC Corps G2	On-the-spot report. Brief information about newly collected materiel.
Equipment evaluation (special).	Team TD	Army SigO Teams TC and TE Army G2	Detailed description of capabilities of captured fixed plant installations, civil and military, and other special items of equipment.
Preliminary (special).	Teams TE and TD	SCIA Theater SigO Theater G2	Detailed report on selected items.

Type and designation	Prepared by—	Directed to—	General content
Periodic	All teams at periodic intervals	As required to higher, lower, and adjacent units and headquarters	Basic signal intelligence report. Summarization of collected materiel. All new signal intelligence items.
Technical bulletins.	SCIA	All interested headquarters	Detailed reports on selected items of equipment.
Other studies, summaries, and estimates.	All teams and SCIA	As required	As required

63. Requirements

Four principal characteristics of reports are brevity, clarity, pertinence, and interest.

a. Intelligence reports should be brief but complete. Thus, two conflicting aims must be satisfied.

(1) Brevity is needed for the commanders, staff officers, and others who require a brief summary of the enemy's operations and the significance of these operations in relation to probable future courses of enemy action.

(2) Detail is required by many other recipients, who must have the most complete information concerning specific aspects of enemy activity.

b. Clarity may be increased by stating known intelligence and admitting the lack of other desired information. Unconfirmed information must be so labeled. Unless this is done, units using the information as a basis for plans may become victims of false indications of the enemy's capabilities.

c. All intelligence reports must be both relevant and timely. The scope of enemy activity included in these reports varies with each headquarters for which the report is prepared. A small tactical unit usually requires information in considerable detail about the enemy. A higher headquarters is more concerned with information more appropriate to its operational requirements.

d. Illustrative material—such as photographs, maps, and sketches—add to the value and interest of a report. Readability can be maintained by elimination of unfamiliar abbreviations and unnecessary references. Excessive use of coordinates should be avoided, especially when a map is not included in the report.

CHAPTER 5
TRAINING

64. General

Signal intelligence training follows the methods of instruction prescribed by FM 21–5 and FM 21–6. The principles of *preparation, explanation, demonstration, application, examination,* and *discussion* can be followed throughout all phases of intelligence training. This training is best accomplished by centralized instruction, therefore every effort should be made to include pertinent aspects of signal intelligence in the course of instruction at all schools.

65. Scope of Training

a. Military intelligence training is a staff responsibility of the Intelligence Officer in coordination with the Operations Officer at each Command Level and is conducted in accordance with DA directives and training programs. This training is received by all members of the army during their basic and specialist training.

b. Basic signal intelligence training is given to all members of the Signal Corps and communications personnel of other arms and services. It covers—

(1) Responsibility of the Signal Corps for technical intelligence.
(2) Sources and methods of collecting and reporting signal information.
(3) The importance of preservation of captured communication equipment and material for examination.

c. Specialized individual intelligence training is given to officer and enlisted personnel selected for duty with a Signal Corps intelligence unit or agency. It may be given through special intelligence courses, through field training with a signal intelligence team, or through an assignment with the SCIA. Normally, this training includes—

(1) Principles of intelligence.
(2) Organization and mission of the signal intelligence teams and the SCIA.
(3) Value of signal intelligence.
(4) Composition of signal intelligence reports covering the tactical and strategic aspects of communication.
(5) Means of communication and a study of recognition factors of communication equipment.
(6) Organization of corps, army, and theater headquarters and of signal units operating in a theater of operations.
(7) Sources, collection, processing, and dissemination of signal intelligence information.
(8) Basic photography.
(9) Orientation in the language of the area of operation.

d. Specialized unit signal intelligence training begins on completion of individual training. Signal intelligence personnel are assigned to teams and the unit training begins. The officers assigned to the individual units are responsible for this phase of training.

(1) Usually, several teams are activated and trained as a complete unit in anticipation of assignment to a specific theater of operation. However, teams may be activated and trained individually.

(2) The training program for signal intelligence teams is based on an 8-week cycle. It is, essentially, an extension of the specialized individual program and a specialized course in each of the subjects listed under *c* above—covering each subject as it applies to the specific mission.

66. Responsibility

a. The *unit commander* must insure that all officers and enlisted personnel have an understanding of their intelligence duties.

b. The *signal intelligence officer* must correct deficiencies and increase the intelligence consciousness of personnel in his area of operation. Each soldier is potentially an information collector who should be trained to report on such matters as the location of captured or abandoned communication equipment and installations; the enemy's signal operating procedures, efficiency, and morale; the techniques of construction of communication centers; and the use of visual and sound communication methods by the enemy. Intelligence consciousness instilled in these men increases the flow of captured signal equipment through intelligence channels and decreases souveniring and needless destruction of valuable equipment. Training does not end with the completion of a program or school. It must be continued on-the-job training to be effective.

APPENDIX I
REFERENCES

AR 380–5	Safeguarding Defense Information.
AR 381–45	(Classified).
AR 381–220	(Classified).
AR 614–46	Assignment to Field Operations Intelligence Duties.
ATP 30–201	Army Training Program for Military Intelligence Headquarters and Administrative Teams, Interrogator Teams, Translator Teams and Document Teams, Interpreter Teams, Order of Battle Teams, Aerial Photo Interpretation Teams, Technical Intelligence Coordinator Teams, Guard Teams, Microphone and Recording Teams and Above Specialists Personnel, Organic to Division and Higher Headquarters.
DA Pam 30–11–1	Foreign Military Weapons and Equipment. Vol. VI. Signal Equipment. (Section I. U.S.S.R.)
DA Pam 30–11–2	Foreign Military Weapons and Equipment, Signal Equipment Section II. Soviet Satellites.
DA Pam 30–26	A Guide to the Collection of Technical Intelligence.
DA Pam 30–100	Intelligence Collection Guide, Telecommunication.
DA Pam 310–4	Index of Technical Manuals, Technical Regulations, Technical Bulletins, Supply Bulletins, Lubrication Orders, and Modification Work Orders.
FM 19–40	Handling Prisoners of War.
FM 21–5	Military Training.

FM 21–6	Techniques of Military Training.
FM 21–30	Military Symbols.
FM 30–5	Combat Intelligence.
FM 30–15	Examination of Personnel and Documents.
FM 30–16	Technical Intelligence.
FM 100–11	Signal Communications Doctrine.
FM 101–5	Staff Officer's Field Manual; Staff Organization and Procedure.
SR 10–3S0–1	Organization and Functions, Department of the Army, Office of the Chief Signal Officer.
SR 320–5–1	Dictionary of United States Army Terms.
AR 345–274	Records Administration; Maintenance and Disposition of Intelligence and Security Administration Files.
SR 3S0–305–10	Standardization of Photo Intelligence Reports, Designation and Content.
SR 605–150–30	Intelligence Specialization, Officers.
TF 7–295	Military Training.
TF 19–1S09	Geneva Conventions, Handling Prisoners of War.
TF 30–1493	Prisoner of War for Intelligence.
TF 30–1494	Production of Combat Intelligence.
TF 30–1S96	Technical Intelligence in Action.
TOE 11–500R	Signal Service Organization.
TM 32–250	Fundamentals of Traffic Analysis (Radiotelegraph).

APPENDIX II
SPOT REPORT

1. Preparation

After selecting and tagging an item of signal equipment, an on-the-spot report is prepared by a member of the collection team.

a. The report should be concise and complete and should incorporate the following information:

(1) Item.
(2) Description.
(3) Condition.
(4) How and where obtained.
(5) Disposition.
(6) Remarks.

b. At the corps signal section, team TA consolidates and reproduces spot reports in sufficient quantities for dissemination. Reports normally contain information as indicated in *a* above, but may be supplemented as circumstances permit or require.

2. Example of Spot Report

CLASSIFICATION

Spot Report No. 15

2 October 1952

1. ITEM: Field switchboard.

2. DESCRIPTION:

a. General. Ten drop field switchboard, encased in a gray metal case about 17" x 8" x 6".

b. Weight. Approximately 15 lb with batteries.

c. Nomenclature. Type K–10, serial No. 4509751.

3. CONDITION: Generally good—two broken line terminals.

4. HOW OBTAINED: This item was captured by unknown elements of the ROK infantry when they routed an enemy company near Taegu on 9 October 1950.

5. DISPOSITION: This item has been evacuated to army.

6. REMARKS: This appears to be a new type switchboard, used by forward combat elements down to and including company. Photographs are attached.

/s/ E. G. Groth
E. G. GROTH
1st Lt, Signal Corps

CLASSIFICATION

APPENDIX III
EQUIPMENT EVALUATION REPORT

1. Content

After discovery or capture of an enemy military or civilian communication installation, the army signal officer requires knowledge of its condition and capabilities for possible use or integration into the communication system. This will require a thorough inspection and evaluation by the equipment evaluation team TD. This evaluation and inspection can also be made on special items of equipment collected by intelligence teams for purposes of furnishing such information to interested agencies at army. The resultant report is prepared by team TD after analysis. The report should disclose:

a. Name of installation.

b. Location (town, street, number, etc.).

c. Type (radio station, telephone central, etc.).

d. Circumstances of discovery or capture.

e. Complete description.

f. Recommendations for use or disposition.

g. Photographs, charts, diagrams, and sketches of the installation.

2. Example of Equipment Evaluation Report

CLASSIFICATION

HEADQUARTERS
174th Signal Intelligence Team
APO 112

2 Oct 1952

SUBJECT: Evaluation Report of Captured Radio Station
TO: See Distribution.

1. On 1 October 1952, elements of the 3rd Infantry Battalion, advancing through Genco, captured (almost intact) a radio station on the outskirts of the city.

2. The station, located on the top floor of an office building at No. 399 Darec Street, in the south end of Genco, was apparently used as a police or security force station. This station probably served to dispatch various radio-equipped elements and also operated in a net with a higher headquarters, probably located in Hostilia, about 250 miles to the southeast. Sufficient equipment was found to operate effectively in two separate nets within a 25-mile radius, and also to maintain point-to-point communications with a distant station, possibly in the city of Amigia.

3. This station is a semipermanent installation in fairly good condition, although tubes are smashed and interconnecting cables are cut. At present, the station is inoperative, but it could be rehabilitated with several days' work, since the tubes can be replaced with standard Signal Corps types. Following is a list of the major components of the station:

a. Three (3) Radio Transmitters, Type S–28–A.
Serial No. 487168–P, 487178–P, and 487034–P.
2.5 to 17.5 megacycle, voice and cw, 50-watt output.
Power: 220-volt, 1-phase, 60-cycle.

b. One (1) Radio Transmitter, Type S–11–F.
Serial No. 4916–A.
1.75 to 15.5 megacycles, voice and cw, 500-watt output.
Power: 220-volt, 3-phase, 60-cycle.

CLASSIFICATION

CLASSIFICATION

c. Four (4) Radio Receivers, Type R–33–C.
Serial No. 7465, 9382, 8675, and 8576.
.5 to 20 megacycles, voice and cw receivers.
Power: 110-volt, 1-phase, 60-cycle.

d. One (1) Frequency Meter, Type C–05–L.
Serial No. 95843–L.
.5 to 20 megacycle heterodyne frequency meter.
Power: 110-volt, 1-phase, 60-cycle.

e. One (1) Control Panel, Type B–17–D.
Serial No. 5011–P.
(This panel permits one operator to modulate or key any one of four transmitters at will, or to connect any transmitter to remote control lines as desired.)

f. Two (2) Generator Sets, Type P–155–B.
Serial No. 9382–F and 9383–F.
Diesel engine driven, skid mounted.
Output: 220-volt, 3-phase, 25-kva, 60-cycle.

g. Three (3) Antennas, Type R–78–X.
No serial numbers.
Vertical whip 22 feet long.
72-ohm coaxial cable to transmitters S–28–A.

h. One (1) Antenna, no type number.
No serial number.
Horizontal doublet 100 feet long on 60-foot poles running NE to SW.
600-ohm two-wire transmission line to transmitter type S–11–F.

i. Miscellaneous maintenance equipment and supplies.

4. Because of its nature, this station with its existing facilities would be well suited for use by the Military Police in traffic control. The equipment cannot be used with standard Signal Corps frequency-modulated vhf tactical radios. The high-powered transmitter could be removed and, with slight modification, could be used with frequency shift radioteletype keying. It is recommended that the power equipment be left

CLASSIFICATION

in place, because the 220-volt, 3-phase power required for the large transmitter is available at most fixed transmitter stations.

5. Arrangements have been made with the 14th Military Police Company to place a guard on the installation until disposition is confirmed.

6. Attached as inclosures are sketches of antenna systems and layout of equipment in the building. Photographs of major equipment items are also included.

/s/ E. X. James
E. X. JAMES
Major, Signal Corps

APPENDIX IV
PRELIMINARY REPORT

1. General

The preliminary report on captured equipment is made on selected items of equipment at theater level. Its primary purpose is to disseminate information on new or unusual items of equipment or material to interested agencies in the theater and to the SCIA in CONUS.

2. Content

The preliminary report should include:

a. Brief description.

b. How obtained.

c. Documentary material, if any.

d. Brief technical characteristics of the item and component parts.

e. Usage—normal and special.

f. Comparison with United States materiel and possible use by United States forces.

g. Recommendation and disposition.

h. Other information as may be required by the theater commander.

3. Example of Preliminary Report

CLASSIFICATION

HEADQUARTERS
APO 111
175th Signal Intelligence Team

20 October 1952

SUBJECT: Preliminary Report on Captured Field Radio Type RBM-1.

TO: See Distribution

1. One complete unit of this field radio, type RBM-1, was captured by unknown elements of the ROK infantry about 1 October 1952, in the vicinity of SEISNU (42.7-05.3).

a. The equipment is divided into four sections for pack transportation; two sections are in metal cases and two sections are in canvas bags. When transported by truck, the equipment is packed into one wooden chest. The basic transmitter-receiver section is housed in a metal case which measures 13 x 7 x 10½ inches and weighs about 25 pounds. The battery case, type UP, is similar to the transmitter-receiver unit. The normal battery complement used with Radio Set RBM-1 consists of one storage battery, type 2NKN-22, and four dry battery units, type BAS-60, or three dry battery units, type BAS-80. The battery case, complete with batteries, weighs about 27 pounds. A canvas bag contains the headset, handset, telegraph key, and connecting cables. The antenna kit is packed in a second canvas bag. In addition, there are two small, wooden boxes for spare parts.

b. No documentary material relating to this unit was captured with this set.

2. This radio set is a complete transmitter-receiver on one chassis covering the frequency range of 1.5 to 5.0 megacycles, and it is battery operated. Receiver and transmitter dials are identical. In each case, only the scale corresponding to the band in use is exposed. Band ranges are: BAND I, from 1.5 to 3.0 megacycles; and BAND II, from 3.0 to 5.0 megacycles. Separate band switches are provided for the transmitter and receiver. All operating controls are located on the front panel.

CLASSIFICATION

CLASSIFICATION

a. Three type SO-257 tubes are used in the transmitter. Power output is about .5 watt on radiotelegraph and .3 watt on radiotelephone.

b. The receiver employs a type SB-242 tube as the mixer-oscillator and five type 2K2M tubes in the remainder of the receiver. Audio power output of the receiver averages .03 watts. Telephone line connections are provided so that the radio set may be used from a distant point if an operator is present to control the send-receive switch.

c. Both transmitter and receiver use a battery power supply that is carried in the case marked UP. A terminal strip is provided at one end of the case for connecting batteries to the jack serving the power cord from the radio set. An additional two-contact jack is provided on the outside of the case, supplying 2 volts.

d. The antenna is a rod-type screwed into the antenna socket on the panel, and consists of six 1-foot sections and a top section of five flat metal fingers, about 9½ inches long, fanned out to form a star.

e. No test equipment was captured with this set.

3. At the time of capture, the set was in use at a command post; however, it appears that it can also be used from a vehicle or on the march. If captured in quantity, it could be used by United States forces, netting with the SCR-694 and the SCR-536. It appears to be rugged and simple in design as compared with the United States sets.

4. Photographs accompanying this report indicate details of serial numbers, nomenclature, etc. Recommend that the unit be air-shipped to the CONUS at an early date for further examination and analysis.

/s/ F. J. Hill
F. J. HILL
Captain, Signal Corps

CLASSIFICATION

APPENDIX V
PERIODIC REPORT

1. General

The periodic report is the basic and primary means of disseminating signal intelligence. Used at all levels, it sums up the information that has been collected, evaluated, and interpreted during a given period. It is a convenient means of keeping higher, lower, and adjacent units informed of the enemy situation. It frequently contains important information that has been disseminated by means of special messages and reports. Distribution of periodic intelligence reports usually is made to staff sections of the unit headquarters, headquarters of the next two higher and subordinate echelons, and adjacent units. Further dissemination may be made as required and in accordance with G2 policy.

2. Content

No standard content for this report can be formulated. The content, format, and preparation depend on the procedures of the headquarters to which the team is assigned and upon the type and amount of intelligence available at the time of preparation. However, the periodic report should include:

a. Summaries of all items of signal equipment and information collected—quantity, condition, and disposition.

b. Summaries of all signal intelligence items collected during the period covered by the report—intelligence concerning enemy signal operations, usage of equipment, type of communications, nets, quality, and morale of enemy signal personnel.

c. Comments by the signal intelligence officer interpreting new intelligence, and old intelligence in light of new information.

d. Other information as required by the commander of the headquarters to which the team is attached.

3. Example of Periodic Report

CLASSIFICATION

HEADQUARTERS
175th Signal Intelligence Team
APO 111

20 October 1952

SUBJECT: Periodic Report No. 10, Period 1 Oct 52 to 15 Oct 52.

TO: See Distribution

1. During the period covered by this report, the following items of signal equipment and materiel have been collected by Signal Intelligence Collection Teams. Samples of all items have been evacuated for further inspection and analysis.

Item	*Quantity*	*Location or disposition*
1. Field Switchboard Type RBM–1–K	9 complete	Evacuated to CONUS 10 Oct 52
2. Field Radio Set Type K–42T5	15 less power supply	Stored at 147 Signal Depot
3. Field Telephone Type RBL–17	22 new, in original containers.	Stored at 147 Signal Depot
4. Field Telephone Type RBL–105	1	Evacuated to CONUS 2 Oct 52
5. Field Wire Type TLB	Twenty ½-mile reels	Stored at 147 Signal Depot
6. Radio Receiver Type PCR	2	Evacuated to CONUS 2 Oct 52
7. Batteries Type T3B4	500 (2½-volt, original containers).	Stored at 147 Signal Depot

2. As evidenced by numerous reports from varied sources, the previous high quality of enemy signal communications has deteriorated to some extent. This appears to be especially true on the central front. There appears to be a shortage of fully trained operators, primarily radio. In general, along all fronts, the morale of enemy signal personnel is low.

CLASSIFICATION

CLASSIFICATION

a. Extensive interrogation of enemy radio operators, captured in a recent probing attack on the central front, reveals that the enemy is now using partially trained personnel to make up losses suffered in recent reversals.

b. Reports of POW's in subparagraph *a* above have been confirmed by interrogation of another prisoner of war, who was captured in action on the eastern front. This POW confirmed that the enemy is generally in short supply of critical signal items, which has caused communication personnel to complain and take a defeatist attitude.

c. Preliminary analysis of Field Telephone RBL–102 Type, captured in September 1952, reveals that improved equipment may soon be used in greater quantities by combat elements. The RBL–102 type telephone has an increased audio range of up to 5 miles over previous models; it is sturdier, more compact, and lighter than telephones in use. Similar trends toward smaller, compact units have been noted in other items of captured equipment.

d. A POW recently interrogated by G2 asserted that future attacks will be preceded by absolute radio silence, followed by a sudden increase in sound and visual signals, including pyrotechnics, in the forward areas. These signals will be used to transmit prearranged messages between commanders of forward elements. Armored vehicles will use pyrotechnic signals up to and into the initial stage of attack. This information was confirmed by a document from another source. This ties in with recent information that pyrotechnics are being brought up to forward areas in greater quantities.

Comment: Although enemy signal communications seem to have deteriorated somewhat, it is believed that this is a temporary condition due to recent intensified air strikes against the enemy's lines of communication. For planning purposes, it is felt that the capability of the enemy communications to support a major offensive has been somewhat neutralized, but is still stable.

/s/ Charles A. Fuller
CHARLES A. FULLER
Major, Signal Corps

CLASSIFICATION

APPENDIX VI
EXAMPLE
TECHNICAL INTELLIGENCE PLAN
(ALL ECHELONS)

CLASSIFICATION

Issuing Headquarters
Place
Time/Date

Appendix.....to Annex.....(Intelligence) to Opn Plan.....

1. General

A statement of the purpose, references, period covered, and designation of subordinate elements required to prepare similar plans.

2. Organization

A statement of the mission, organization, allotment of Signal Corps technical intelligence detachments, responsibilities and functions, as well as designation of Signal Corps Depots.

3. Personnel

a. Military. Policy concerning: special passes; taking custody of captured enemy materiel; movements in forward areas; reporting to command posts; cooperation with combat intelligence personnel; relationship between intelligence and Signal Corps technical intelligence personnel.

b. Civilian.

(1) Authority for presence in theater of operations; passes required.

(2) Policies concerning sponsors for individuals and groups.

(3) Responsibility of sponsor for logistical support.

CLASSIFICATION

(4) Limitations on activities of individuals and groups.

4. Direction

Policies governing publishing requirements and Items Wanted Lists; designation of special targets; direction to be provided by subordinate echelons and technical services.

5. Collection

a. Documents. Procedures for collecting and forwarding documents; responsibilities for evaluating importance and timeliness of data; channels for forwarding.

b. Prisoners. Procedures for selection and interrogation of personnel with technical knowledge; channels for evacuation; ultimate disposition (civilians, neutrals, deserters, etc.).

c. Materiel.

(1) Disposition of information concerning captured enemy materiel.

(2) Policies for safeguarding, evacuation, examination and ultimate disposition.

d. Facilities. Procedures for collecting and reporting information, responsibility and preparing EEI; channels for forwarding or disposition of facilities data.

6. Processing

a. Records required to be maintained.

b. Policies governing preparation of preliminary and final field reports.

c. Liaison and coordination between intelligence agencies and Signal Corps concerning evaluation and interpretation of technical intelligence information.

7. Dissemination

a. Purpose, scope, language, content, and type of periodic and special reports to be submitted.

b. Policies governing dissemination.

8. Scientific/Technical Intelligence Task Force Operations

a. Theater and theater army policy concerning scope and effort that may be expended on missions.

b. Authority to determine whether an intelligence target should be saved for capture or destroyed.

c. Procedures for collecting and reporting data.

d. Responsibility for direction of operations.

e. Limitation on units and individuals authorized to participate.

f. General provisions for security of planned operations; safeguarding components of intelligence and other value; priorities concerning exploitation.

.....
Commander

Distribution:
Authentication:

INDEX

	Paragraph	Page
Army:		
Dissemination of intelligence	58	43
Intelligence processing	48,53	37,40
Signal intelligence functions	21	17
Signal officer, responsibilities	8	8
Assignment, signal intelligence officer	10	9
Authority, souvenir control	44	35
Booby traps	45	36
Captured equipment	6,25,28	6,22,23
Chief Signal Officer, intelligence responsibilities	7	6
Collation, information	49	38
Collection:		
Plan	25	22
Signal intelligence:		
Checklists	39–41	30
Echelons	38	30
Fields of interest	33	26
Location	34	26
Photographic coverage	36	28
Program	32	25
Selection	35	27
Tagging equipment	37	28
Corps:		
Dissemination of signal intelligence	59	43
Intelligence processing	48,52	37,39
Signal intelligence functions	22	19
Signal officer, responsibilities	8	8
Dangers of souveniring	45	36
Dissemination of signal intelligence:		
Army	58	43
Corps	59	43
Department of the Army	56	41
Requirements	55	41
SCIA	56	41
Theater	57	41
Division signal officer, responsibilities	9	9

	Paragraph	Page
EEI	25	22
Enemy research and development	6	6
Equipment evaluation report	App. III, 62	55,44
Equipment tags, collected items	37	28
Evaluation	50	38
Fields of interest, signal intelligence	33	26
Functions:		
SCIA	15	14
Signal intelligence teams	18	16
TA-type team	22	19
TB-type team	22	19
TC-type team	21	17
TD-type team	21	17
TE-type team	20	17
Signal Technical Intelligence	19	17
Intelligence:		
Communication	4	3
Officers, responsibilities	14	12
Signal. (*See* also Signal intelligence.)	4	3
Teams. (*See also* Signal intelligence teams.)	19–22,38	17,30
Interpretation	51	38
Interrogation of POW	10,27,29	9,23,24
Interrogation reports	10	9
Location of intelligence items	34	26
Mission, signal intelligence teams	18	16
Native personnel, intelligence source	10,27,29	9,23,24
Negative information	13	11
Objectives, signal intelligence	5	4
Operations, SCIA	16	14
Organization, signal intelligence:		
Army	21	17
Corps	22	19
Teams	19	17
Theater	20	17
Periodic reports	App. V, 62	62,44
Photographic coverage	36	28
Photographs	27,30	23,24
Plan, collection	25	22
Plan, field, technical intelligence	24	21
Planning, signal intelligence:		
Basis	23	21
Collection plan	25	22
Coordination	26	22
Technical intelligence field plan	24	21
POW interrogation	27,29	23,24
Preliminary report	App. IV, 62	59,44
Processing:		
Army	48,53	37,40
Collation	49	38
Corps	48,52	37,39
Evaluation	50	38
Interpretation	51	38
Theater	48,54	37,40
Program, collection	32	25
Radio position finding	25,28	22,23
References	App. I	51
Reports:		
Coordination	61	44
Equipment evaluation	App. III, 62	55,44
Interrogation	10	9
Miscellaneous	62	44
Periodic	App. V, 62	62,44
Preliminary	App. IV, 62	59,44
Requirements	63	46
Special	62	44
Spot	App. II, 62	53,44
Technical bulletins	62	44
Types	62	44
Requirements, intelligence dissemination	55	41
Research and development	6	6
Responsibility:		
Army signal officer	8	8
Chief Signal Officer	7	6
Corps signal officer	8	8
Division signal officer	9	9
Intelligence officer	14	12
Signal intelligence officer	10	9
Signal intelligence units	11	10
Signal units	12	11
Souvenir control	46	37
Theater signal officer	8	8
Training	66	50
Units other than signal	13	11
SCIA:		
Definition	8	8
Dissemination of information	56	41
Functions	15	14
Operations	16	14
Reports	62	44

	Paragraph	Page
Selection of items for collection	35	27
Signal equipment, souvenir control	44	35
Signal intelligence:		
Collection. (*See also* Collection, signal intelligence.)	32–41	25
Dissemination. (*See also* Dissemination.)	55–59	41
Objectives	5	4
Officer	10	9
Organization. (*See also* Organization, signal intelligence.)	15–22	14
Planning. (*See also* Planning, signal intelligence.)	23–26	21
Processing. (*See also* Processing.)	48–54	37
Responsibilities. (*See also* Responsibility.)	6–14	6
Reports. (*See also* Reports.)	60–62	44
Sources. (*See also* Sources, signal intelligence.)	27–31	23
Souvenir control. (*See also* Souvenir control.)	42–47	34
Teams:		
Assignment	20–22	17
Collection	38	30
Functions	18–22.38	16.30
Mission	18	16
Organization	19	17
Types	20–22	17
Training. (*See also* Training.)	64–66	48
Unit responsibilities	11	10
Signal unit responsibilities	12	11
Sources, signal intelligence:		
Captured equipment	27.28	23
Charts	27	23
Diagrams	27	23
Documents	27	23
Manuals	27	23
Maps	27	23
Native personnel	27.29	23.24
Photographs	27.30	23.24
POW	27.29	23.24
Souvenir control:		
Authority	47	37
Dangers	45	36
Purpose	42	34
Reasons	43	35
Responsibility	46	37
Signal equipment	44	35
Special reports	62	44

	Paragraph	Page
Specialized training	65	48
Spot reports	App. II, 62	53,44
Tagging collected items	37	28
Teams, signal intelligence:		
TA-type	19.22.38	17,19.30
TB-type	19,22.38	17,19.30
TC-type	19,21.38	17.30
TD-type	19,21.38	17.30
TE-type	19,20.38	17.30
Signal Technical Intelligence	19	17
Technical bulletins	62	44
Technical intelligence plan	App. VI, 24	65.21
Theater:		
Dissemination of intelligence	57	41
Processing of intelligence	48,54	37.40
Signal intelligence functions	20	17
Signal officer, responsibilities	8	8
Team TE	20	17
Training:		
Methods	64	48
Responsibility	10.66	9,50
Scope	65	48
Signal intelligence specialists	6	6
Specialized	65	48
Unit	65	48
Unit responsibility for intelligence	13	11
Unit training	65	48

[AG 350.09 (6 Jun 56)]

By Order of *Wilber M. Brucker*, Secretary of the Army:

MAXWELL D. TAYLOR,
General, United States Army,
Chief of Staff.

Official:

JOHN A. KLEIN,
Major General, United States Army,
The Adjutant General.

Distribution:

Active Army:

Gen Staff (5) except ACSI (15)
Tec Svc, DA (1) except CSigO (25)
Tec Svc Bd (1) except Sig Bd (2)
Hq CONARC (15)
Army AA Comd (3)
OS Maj Comd (25)
OS Base Comd (3)
Log Comd (3)
MDW (3)
Armies (5)
Corps (5)
Div (5)
Brig (2)
Regt (4)
Cml Bn (1)
Engr Bn (1)
Ord Bn (1)
Qm Bn (1)
Sig Bn (10)
MP Bn (1)
Mil Intel Bn (10)
Cml Co (1)
Engr Co (1)
Ord Co (1)
Qm Co (1)
Sig Co (10)
MP Co (1)
Mil Intel Co (10)
USMA (25)
CGSC (25)
Ft & Cp (2)
Gen & Br Svc Sch (5) except Sig Sch (500)
Specialist Sch (5)
Joint Sch (5)
Gen Depot (2)
Sup Sec, Gen Depot (2)
Depot (2)
Army Terminal (5)
Trans Terminal Comd (5)
POE (OS) (5)
OS Sup Agencies (3)
PG (2)
Arsenal (2)
Mil Dist (2)
MAAG (1)
Mil Msn (1)
APMA (1)
Units org under the fol. TOE:
11-500R (TA-TE) Sig Svc Org (3)
30-600C (AA, BA, CA, CL) MI Svc Org (2)

NG: None.

USAR: None.

For explanation of abbreviations used, see SR 320-50-1.

☆ U. S. GOVERNMENT PRINTING OFFICE: 1956—400633

U. S. Army Military History Institute

FM 11–30
C 1

FIELD MANUAL

SIGNAL CORPS TECHNICAL INTELLIGENCE

FM 11–30
CHANGES No. 1

HEADQUARTERS,
DEPARTMENT OF THE ARMY
WASHINGTON 25, D.C., *1 November 1961*

FM 11–30, 13 August 1956, is changed as follows:

Wherever "Signal Corps Intelligence Agency" or its abbreviation "SCIA" appears, change to United States Army Signal Intelligence Agency and USASIA respectively.

4. Definitions

Signal intelligence as defined in **AR 320–5** is to be sharply distinguished from communication intelligence, and electronic intelligence.

* * * * *

b. Communication intelligence consists * * * of this manual. **It is a function for which the Signal Corps has partial responsibility in certain areas of intelligence.**

* * * * *

15. General

The **USASIA** is a class II activity under the control of the Chief Signal Officer through the **Research and Development Division** of the OCSigO. The **USASIA:**

* * * * *

16. Operations

The **USASIA:**

* * * * *

i. (Superseded) Disseminates completed intelligence to agencies under control of the Chief Signal Officer, and to the ACSI.

20. Theater Headquarters

The TE-type team * * * (fig. 2). This team—

* * * * *

c. Supervises the storage, issue, and shipment to CONUS of collected **signal** material.

33. Fields of Interest

Signal intelligence is concerned with information pertaining to—

* * * * *

Infrared devices. (Added)

Space vehicle communications equpipment. (Added)

Automatic data processing equipment. (Added)

34. Targets

Any nation normally * * * the following locations:

* * * * *

b. Strategic.

* * * * *

(14) (Added) Television stations.

40. Checklist for Collecting Military Communication Information

a. Organization and Equipment of Enemy Units.

* * * * *

(6) (Added) Name of Signal Officer.

* * * * *

h. Other Equipment. Any other equipment used or controlled by the Signal Corps—such as visual, sonic, infrared, **television,** and flash ranging equipment.

41. Checklist for Collecting Information on Nonmilitary Civilian Communication Facilities

* * * * *

b. Radio ***and television*** *facilities* (*including broadcasting stations*).

* * * * *

c. (Added) *Communications-Electronics Manufacturing Plants.*

(1) Name and location.

(2) Type equipment produced.

(3) Current operational condition.

(4) Inventory of completed equipment, parts, and raw materials.

d. (Added) *Communications-Electronics Research and Development Laboratories.*

(1) Name and location.

(2) Type of equipment under development.

e. (Added) *Photographs and Documents Pertaining to Communications-Electronics Facilities, Manufacturing Plants and Research Laboratories.*

44. Signal Equipment Control

Captured signal equipment * * * of souvenir hunters.

* * * * *

c. Communication centers, facilities, supply depots, technical installations, **research and development laboratories and manufacturing plants,** or an intelligence task force warrant particular precau-

tions and provisions to prevent unintentional destruction by combat troops, delayed enemy demolition, looting, or removal by souvenir hunters.

65. Scope of Training

* * * * *

d. (Superseded) *Specialized unit signal intelligence training* begins on completion of individual training. The officers assigned to the individual units are responsible for this phase of training.

(1) Normally, personnel selected for assignment to a signal intelligence unit will be assigned initially to a lower echelon team—Team TA for administrative personnel, and Team TB for Signal Corps technicians. As training and experience are gained, qualified personnel will be selected for subsequent assignment to a higher echelon team—Team TC, TD, or TE—to meet normal replacement requirements in appropriate military occupational specialties.

(2) When required, several teams may be activated and trained as a complete unit for assignment to a specific theater of operations. However, teams may be activated and trained individually. Individual replacements normally can be integrated into a team and receive on-the-job training on an individual basis with no loss to unit effectiveness.

(3) For newly activated teams the training program is based on an 8-week cycle. It may also be desirable to retrain teams under this program, when warranted by a large turnover of personnel. The program is, essentially, an extension of the specialized course in each of the subjects listed under *c*, above—covering each subject as it applies to the specific mission.

APPENDIX II (Superseded)

SPOT REPORT

1. Preparation

After selecting, photographing, and tagging an item of signal equipment, an on-the-spot report is prepared by a member of the collection team.

a. The report should incorporate the following information:

(1) Nomenclature of item.
(2) Description.
(3) Condition.
(4) How and where obtained.
(5) Cross-reference to photographs, if any.
(6) Disposition.
(7) Remarks.

b. Since the lower echelon collection team has limited administrative capability, forms may be reproduced and kept on hand so that the report can be expeditiously completed in pencil. Reports normally contain information as indicated in *a*, above, but may be supplemented as circumstances permit or require. An example of a spot report is shown in paragraph 2.

c. At the corps signal section, team TA screens and forwards the reports with recommendations to the corps signal officer as to distribution of information which has not been previously reported.

d. At each successive echelon in signal intelligence channels, the responsible team or agency will screen the reports and forward to the next higher echelon those which contain newly acquired information.

2. Example of Spot Report

CLASSIFICATION

SPOT REPORT NO. 15 DATE: 2 Oct 52

1. ITEM NOMENCLATURE:
Field Switchboard, K–10.

2. DESCRIPTION:
Ten drop switchboard in a gray metal case. 17″ x 8″ x 6″. Weight: 15 lbs w/batteries. Ser. Nr. 45Ø9751.

3. CONDITION:
Good ~~Fair~~ ~~Poor~~

4. HOW AND WHERE OBTAINED:
2d ROK Inf. Regt; 3 miles NW of TAEGU.

5. PHOTOGRAPHER:
Pfc Spencer
Pack Nr. 4 Exp. Nr. 6

6. DISPOSITION:
Evacuated to Army.

7. REMARKS:
Captured from company level unit. Appears to be new type switchboard for forward combat units down to and including company.

UNIT: 95th Sig Det

SIGNATURE: /s/ E. G. Groth
E. G. GROTH
1st Lt, SC

CLASSIFICATION

BY ORDER OF THE SECRETARY OF THE ARMY:

G. H. DECKER,
General, United States Army,
Chief of Staff.

Official:

J. C. LAMBERT,
Major General, United States Army,
The Adjutant General.

Distribution:

Active Army:

USASA (5)
DCSPER (5)
ACSI (15)
DCSOPS (5)
DCSLOG (5)
ACSRC (5)
CNGB (50)
Tech Stf, DA (1) except CSigO (25)
Tech Stf Bd (1) except Sig Bd (2)
USCONARC (15)
ARADCOM (3)
OS Maj Comd (25)
OS Base Comd (3)
LOGCOMD (3)
MDW (3)
Armies (5)
Corps (5)
Div (5)
Bde (2)
Bg (4)
Cml Bn (1)
Engr Bn (1)
Ord Bn (1)
QM Bn (1)
Sig Bn (10)
MP Bn (1)
Mil Intel Bn (10)
Cml Co (1)
Engr Co (1)
Ord Co (1)
QM Co (1)
Sig Co (10)
MP Co (1)
Mil Intel Co (10)
Instl (2)
USMA (25)
USACGSC (25)
USAWC (5)
Br Svc Sch (5) except USASCS (300)
Specialist Sch (5)
Joint Sch (5)
GENDEP (2)
Sup Sec, GENDEP (2)
Dep (2)
Army Tml (5)
USA Trans Tml Comd (5)
POE (5)
OSA (3)
PG (2)
Arsenals (2)
USA Corps (2)
Mil Msn (1)
MAAG (1)
USARMA (1)
Units organized under following TOE's:
11-500 (TA-TE) (3)
17-22 (4)
30-600 (AA, BA, CA, CL) (2)

NG: State AG (3); units—same as Active Army except allowance is one copy to each unit.

USAR: Same as Active Army except allowance is one copy to each unit.

For explanation of abbreviations used, see AR 320-50.

U.S. GOVERNMENT PRINTING OFFICE: 1961

FM 34-54

TECHNICAL INTELLIGENCE

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

PREFACE

This field manual provides guidance to commanders and staffs of military intelligence (MI) and other units responsible for technical intelligence (TECHINT) or having an association with TECHINT. It provides general guidance and identifies the tactics, techniques, and procedures (TTP) used in the collection, exploitation, and dissemination of TECHINT in satisfying the warfighter's requirements.

TECHINT is an integral part of the overall battlefield operating system (BOS) and supports Army operations through the analysis and exploitation of foreign equipment, weapons, and other war materiel.

This field manual describes the TECHINT process at all echelons and identifies responsibilities. It further describes the MI TECHINT organizations, other services, and the strategic level intelligence agencies supporting the process.

On today's battlefield, Army forces will likely deploy as part of a joint or combined military operation. For that reason, while this manual supports Army operations, it does so in the context of Army operations as part of a joint or combined task force.

This field manual applies to all Army personnel, to include Active Component (AC) and Reserve Components (RC) commanders and their staffs, US Army Training and Doctrine Command (TRADOC) Centers and Schools, and MI elements.

The proponent of this publication is US Army Intelligence Center and Fort Huachuca (USAIC&FH). Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, US Army Intelligence Center and School, ATTN: ATZS-TDL-D, Fort Huachuca, AZ 85613-6000.

The doctrine in this publication conforms with and supports the principles in FM 34-1 and FM 100-5. This manual does not implement any international standardization agreements but complies with the following Standardization Agreements:

STANAG 1059 - National Distinguishing Letters for Use by NATO Forces (Edition 6).
STANAG 2014 - Operations Plans, Warning Orders, and Administrative/Logistics Orders (Edition 7).
STANAG 2044 - Procedures for Dealing With Prisoners of War (Edition 5).
STANAG 2084 - Handling and Reporting of Captured Enemy Equipment and Documents (Edition 5).
STANAG 2097 - Nomenclature and Classification of Equipment (Edition 6).
STANAG 2143 - Explosive Ordnance Reconnaissance/Explosive Ordnance Disposal (Edition 4).
STANAG 2389 - Minimum Standards of Proficiency for Trained Explosive Ordnance Disposal Personnel (Edition 1).
STANAG 2834 - The Operation of the Explosive Ordnance Disposal Technical Information Center (EODTIC) (Edition 2).

Unless this publication states otherwise, masculine nouns and pronouns do not refer

exclusively to men. The use or mention of any commercial or private organization's name or trademark and the organization's services and/or funds by the US Army does not express or imply an endorsement of the sponsor or its products and services by the US Army.

FIELD MANUAL
No. 34-54

Headquarters
Department of the Army
Washington, DC, 30 January 1998

TECHNICAL INTELLIGENCE

TABLE OF CONTENTS

Page

PREFACE v

CHAPTER 1 – TECHNICAL INTELLIGENCE MISSION AND SUPPORT 1-1
General 1-1
Mission 1-1
TECHINT Support to the Warfighter 1-1
Historical Perspective 1-2
Lessons Learned 1-8

CHAPTER 2 – SCIENTIFIC AND TECHNICAL INTELLIGENCE 2-1
Introduction 2-1
The S&TI Community 2-1
Structure 2-3

CHAPTER 3 – BATTLEFIELD TECHNICAL INTELLIGENCE OPERATIONS 3-1
Introduction 3-1
203d MI Battalion (TECHINT) 3-3
Battlefield TECHINT Channels 3-6
Joint Technical Intelligence Branch 3-6
Captured Materiel Exploitation Center 3-7
JCMEC and CJCMEC 3-8
TECHINT Liaison Elements 3-8
Corps CMEC (Forward) 3-9
Battlefield TECHINT Collection Teams 3-9

CHAPTER 4 – INTELLIGENCE CYCLE APPLIED TO TECHNICAL INTELLIGENCE OPERATIONS 4-1
Plan and Direct 4-1
Collect 4-3
Process 4-6
Produce 4-6

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes FM 34-54, 5 April 1990.

Page

Disseminate 4-6
Battlefield TECHINT Reporting Sequence 4-7
Battlefield TECHINT Analysis 4-8

CHAPTER 5 – RESPONSIBILITIES 5-1
Introduction 5-1
Staff Sections 5-1
Assistant Chief of Staff, J1/G1, Personnel 5-1
Assistant Chief of Staff, J2/G2, Intelligence 5-2
Assistant Chief of Staff, J3/G3, Operations 5-3
Assistant Chief of Staff, J4/G4, Logistics 5-4
Assistant Chief of Staff, J5/G5, Civil Affairs 5-4
Special Staff Officers 5-5
Units and Organizations 5-7

APPENDIX A – MEASUREMENT AND SIGNATURE INTELLIGENCE A-1
APPENDIX B – JCMEC OPERATIONS B-1
APPENDIX C – HANDLING AND EVACUATION C-1
APPENDIX D – INTELLIGENCE ANNEX WITH TECHINT INPUT D-1
APPENDIX E – TECHNICAL INTELLIGENCE REPORTS E-1
APPENDIX F – COLLECTION AND EXPLOITATION REQUIREMENTS F-1
APPENDIX G – FOREIGN LANGUAGE TEXT RECOGNITION G-1
APPENDIX H – CHEMICAL AND BIOLOGICAL WARFARE SAMPLING PROCEDURES H-1
APPENDIX I – FACILITY EXPLOITATION CHECKLISTS I-1

GLOSSARY
Acronyms Glossary-1
Terms and Definitions Glossary-12

REFERENCES References-1

INDEX Index-1

LIST OF FIGURES

Page

Figure 2-1. Department of Defense S&TI community. 2-2
Figure 3-1. TECHINT operations 3-2
Figure 3-2. The 203d MI Battalion (TECHINT) organization. 3-3
Figure 3-3. TECHINT team organization 3-5
Figure 3-4. Possible locations of TECHINT LNEs when supporting a JTF. 3-9
Figure 4-1. Planning and directing 4-1
Figure 4-2. TECHINT target folder. 4-2
Figure 4-3. Flow of CEM guidance and decisions 4-4
Figure 4-4. Transportation operations 4-5
Figure 5-1. Staff sections responsibilities 5-2
Figure A-1. HQDA agencies and their MASINT responsibilities. A-3
Figure B-1. Joint Captured Materiel Exploitation Center (JCMEC) Organization. B-4
Figure B-2. TECHINT communications architecture B-7
Figure C-1. Evacuation of captured petroleum, oils, and lubricants C-4
Figure C-2. Evacuation of captured ammunition and explosives C-4
Figure C-3. Captured medical materiel evacuation system C-5
Figure C-4. Evacuation of captured aviation items C-5
Figure C-5. Front and reverse sides of an EPW tag. C-11
Figure C-6. Front and reverse sides of a CEE tag. C-12
Figure C-7. Example of a CEE tag flagged for TECHDOCs. C-13
Figure D-1. Example of an extract from a Theater Army Intelligence Annex D-1
Figure D-2. Example of a Joint Theater TECHINT Appendix D-4
Figure D-3. Example of a TAB D to a TECHINT Appendix of a Theater Army Intelligence Annex. D-11
Figure E-1. Example of a SALUTE report. E-2
Figure E-2. Format for a PRETECHREP. E-3
Figure E-3. Format for a COMTECHREP - Type A. E-4
Figure E-4. Format for a COMTECHREP - Type B. E-7
Figure E-5. Format for a COMTECHREP - Type C. E-9
Figure G-1. A partial list of spoken languages and locations where they are spoken. . . . G-3
Figure G-2. Table of diacritics. G-4
Figure G-3. The occurrence of diacritics in various languages. G-5
Figure G-4. Distinguishing major Slavic languages from Russian. G-10
Figure G-5. Cyrillic alphabet and transliteration chart. G-12
Figure G-6. International, Arabic, and Persian numbers. G-16
Figure G-7. The Arabic alphabet. G-17
Figure G-8. The diacritics of Arabic and Persian. G-18
Figure G-9. Printed Arabic. G-18
Figure G-10. Typewritten Arabic. G-19
Figure G-11. Printed Persian (arrows indicate distinguishing features). G-19
Figure G-12. Sample of Chinese text. G-21
Figure G-13. Sample of Japanese text. G-21
Figure G-14. Shows Korean with fewer Chinese symbols used. G-22
Figure G-15. The fifty most common Chinese character radicals. G-23
Figure G-16. The Japanese Hiragana syllabary. G-24
Figure G-17. The Japanese Katakana syllabary. G-24

Figure G-18. The Korean alphabet. G-25
Figure H-1. Sample DA Form 1971-6-R (Chemical/Biological Sample Documentation) . H-4
Figure H-2. Example of an equipment list. H-5
Figure H-3. Description of responsibilities for a sample evacuation. H-10
Figure H-4. Sample collection guidelines. H-13
Figure H-5. Sample identification and control. H-14
Figure I-1. Collection Checklist-Airfields. I-1
Figure I-2. Collection Checklist-Electric Power. I-5
Figure I-3. Checklist-Petroleum and Natural Fields. I-8
Figure I-4. Facility Physical Security Checklist. I-11
Figure I-5. Checklist-Railways. I-14
Figure I-6. Checklist-Underground Facilities. I-18

Chapter 1

TECHNICAL INTELLIGENCE MISSION AND SUPPORT

GENERAL

This chapter describes the TECHINT mission, how it supports the warfighter, and presents TECHINT in a historical perspective. TECHINT results from the collection, evaluation, and analysis of foreign warfighting equipment and associated materiel. At the strategic level, the exploitation and interpretation of foreign weapons systems, materiel, and technologies is referred to as scientific and technical intelligence (S&TI). This S&TI covers—

- Foreign developments in basic and applied research and in applied engineering techniques.
- Scientific and technical (S&T) characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and material.
- Research and development (R&D) related to these systems and the production methods employed for their manufacture.

MISSION

The TECHINT mission ensures that the warfighter has a clear understanding of the full technological capabilities residing in his opponent's equipment. With this knowledge, the warfighter adopts countermeasures, operations, and tactics, as necessary, to be successful in any assigned mission.

TECHINT SUPPORT TO THE WARFIGHTER

STRATEGIC LEVEL:

The US has relied on its military strength as a strategic deterrent to war. The strength of the US military lies, in part, to the diversity and extent of its technology base. While the US aspires to be the leader in integrating technology, the actual products are available to any buyer. An adversary can achieve temporary technological parity or advantage by acquiring modern systems or capabilities. The world arms market is willing to provide these advanced systems to countries or individuals with the resources to

pay for them. A concerted TECHINT program is vital to providing precise direction and purpose within the US R&D process to ensure that this parity or advantage is neutralized quickly and efficiently.

OPERATIONAL AND TACTICAL LEVEL:

For the Army, technology is changing how we organize, how we train and develop leaders, and how we conduct operations. Advances in electronics, communications, automation, reconnaissance and surveillance (R&S), contamination avoidance, precision-guided munitions, and the exploitation of space-based capabilities have increased the lethality, range, accuracy, and reliability of our weaponry.

Operational and tactical commanders rely on this technological advantage to successfully synchronize and execute complex modern Army operations. The introduction of a surprise technological capability by an adversary causes confusion and delay mission accomplishment until the capability is understood and countered. TECHINT is the key to the early identification of an adversary's technical capabilities and the development of countermeasures for the operational and tactical commander.

HISTORICAL PERSPECTIVE

In the 1920's, Germany was developing the weapons and systems it would use against the Allies in the 1940's. Because Allied nations did not integrate TECHINT into peacetime collection efforts, German S&T advances went largely unnoticed. When information did come to light, Washington and London ignored or ridiculed it. Later, when the Germans fielded their advanced weapons and systems in war, the resulting technological surprise on the battlefield was devastating.

WORLD WAR II:

During the air battle for Europe, the British used TECHINT to counter the German antiaircraft and night-fighter defenses. This was accomplished by exploiting captured aircraft radios and a captured radar station. (See below a discussion of the Bruneval Raid.)

The Allies captured many German and Italian weapons in North Africa. This collection led to the publishing of new technical material, such as—

- Technical manual E9 series handbooks on enemy weapons.
- Special series publications on German weapons.
- Training aids.

- Updates to handbooks on the German and Italian armies.

TECHINT exploitation of captured German Tiger and Panther tanks led to several important battlefield countermeasures. One of these was the adoption of new armor tactics while another was the development of more powerful antitank rockets.

The United States started a successful TECHINT program in the fall of 1943 called the ALSOS mission. This unit was made up of Counterintelligence (CI) Corps agents, scientists, and interpreters. Their mission was to capture and exploit personnel and material of S&T value.

The successes of this unit included:

- Exploitation of Italian and German nuclear scientists.
- Removal of significant quantities of uranium ore from the Albert Canal.
- Recovery of the international radium standards from what was to be the Soviet occupied sector of Germany.

Throughout the remainder of the 1940's a Foreign Materiel Intelligence Branch at the Ordnance Center, Aberdeen Proving Grounds, MD, continued to conduct exploitation work on captured German and Japanese equipment.

THE RAID ON BRUNEVAL—AN OFFENSIVE TECHINT OPERATION:

At 2100Z on 27 February 1942, 119 British soldiers of Company C, 2nd Battalion, the Parachute Regiment, parachuted into a drop zone near the small village of Bruneval, in Occupied France. The company's mission was to raid a suspected German radar site on a cliff a few hundred yards from an accessible beach to bring back an item of extreme TECHINT interest—the WUERZBURG radar.

The WUERZBURG radar was believed to be a mobile, short-range, high-precision radar responsible for the sudden and serious increase in Allied heavy bomber losses. Routine Allied photographic reconnaissance originally discovered the installation in January 1942. French resistance forces were sent to investigate. They confirmed the site as well as a garrison troop strength of nearly 200 enemy signal, support, and security troops. They also reported that the nearby beach was not mined.

It was the intelligence and urgent need to protect Allied planes that resulted in the commando raid that night. Once on the ground, the commandos moved quickly and split into three equal groups. The first group secured

the beach. The second group spread out and took up positions to act as a reserve or blocking force. The last group, the collection team and a special radar technical expert, moved forward to take the target.

The collection team slipped through enemy defender positions, entered the installation, and found the radar. They used hacksaws, crowbars, and precision hand tools to dismantle the main components. As each part of the radar was exposed, it was sketched and photographed. The team also captured a German signalman—the radar operator.

When they finished, the team destroyed what they couldn't take with them and began their move to the beach under progressively heavy fire. The surviving commandos were picked up by Allied landing craft and escaped across the Channel to England.

Exactly three and one-half hours after the mission began it was over. Although two men were killed, six wounded, and six more listed as missing in action, the raid was deemed a great success. Not only was it the first raid on the continent following the disaster at Dunkirk but also it resulted in the successful capture of a valuable piece of enemy material—material that later proved to be of vital TECHINT interest.

Allied TECHINT experts examined the material as soon as they got it. The exploitation of this radar, along with the sketches and the photographs, quickly began to provide valuable TECHINT. For example, just from the recovered metal manufacturer's plates, analysts accurately determined how many Wuerzburg radars had been produced and their current rate of production. When the German signalman was interrogated, he provided valuable information about the level of operator skills and operator training. Most important, though, TECHINT scientists
used the captured material to build an operational Wuerzburg radar mockup.

When the mockup was completed, they had a multifrequency radar that seemed, at first, to be almost impossible to jam. Scientists went to work to develop countermeasures to neutralize the radar's capabilities. Their efforts resulted in thin metallic strips cut to different lengths that could be dropped from airplanes. These strips reflected radar signals and effectively jammed the new radars. They dubbed these strips *chaff*. CHAFF turned out to be one of the most successful countermeasures developed during World War II—being particularly useful during the Normandy Invasion.

THE KOREAN WAR:

It wasn't until the beginning of the Korean War, when North Korean troops in Soviet-designed and Chinese-built armor rolled south, that the United States discovered it had little confirmed data on enemy weapons systems.

We realized that to be able to develop effective countermeasures, TECHINT had to be an ongoing process. As a result, we once again began a concerted TECHINT effort, with the Foreign Material Intelligence Branch at Aberdeen Proving Grounds training and fielding TECHINT teams to Korea.

In the Korean War, the warfighters found that their 2.36-inch bazooka rockets could not penetrate the T-34/85 tanks' frontal armor. With this combat deficit identified, commanders began to support the TECHINT process by evacuating captured T-34/85 tanks and other material to TECHINT elements for exploitation. TECHINT both in the theater and back in the United States at the Chrysler Corporation analyzed the captured material. The US Army responded by giving combat commanders new tactics, a redesigned M-48 tank, and a 3.5-inch bazooka.

The TECHINT effort also supported the political effort to prove Soviet involvement on behalf of the North Korean aggressor. Captured modern Soviet weapons were regularly paraded before the UN Security Council as evidence of Soviet support.

THE VIETNAM WAR:

Following the Korean War, the United States did not disband its TECHINT capability completely, as had been done at the conclusion of all previous hostilities. But neither did we maintain it at its wartime level. Three small TECHINT detachments remained in place at the Army's research and development centers. By 1962 two of the detachments merged to form the Army's Foreign Science and Technology Center. The third detachment established the Missile Intelligence Agency at Redstone Arsenal. The Surgeon General also operated a Medical Intelligence Center at Fort Detrick, MD.

An agency called the Captured Materiel Exploitation Center (CMEC) came into being in 1966. Its wartime mission was to manage, coordinate, and analyze captured enemy equipment (CEE), and technical captured enemy documents (CEDs). The CMEC did this on a tactical level by dispatching teams of experts and analysts into the tactical zone of each corps. These teams analyzed captured materiel in the field and recommended countermeasures to tactical commanders. American personnel working in the CMEC were assigned to Delta Company, 519th MI Battalion.

The North Vietnamese employed Soviet designed man-portable systems with considerable success. The Soviet AT-3 Sagger antitank guided missile (ATGM) was used against South Vietnamese armored vehicles, communications bunkers, and even small outposts. In addition, the SA-7 heat-seeking surface-to-air missile (SAM) was employed and became an even more serious threat because it could disrupt allied control of the air

space over the battlefield. Lastly, the 122-mm rocket was employed as the North Vietnamese Army's (NVA) primary artillery weapon in a variety of configurations. While samples of these weapons undoubtedly fell into the hands of the South Vietnamese, nothing was done with them because of the September 1969 inactivation of American TECHINT units in Vietnam. And, by October 1971, the 55th Military Intelligence Detachment, a corps support unit with a TECHINT capability, had also been inactivated.

GRENADA (OPERATION URGENT FURY):

Following the commitment of US forces to Grenada on 25 October 1983, large quantities of foreign military equipment were discovered thus requiring TECHINT support.

Two elements of the 203d MI Battalion, 513th MI Group, were deployed to Grenada. Five soldiers participated as members of a Defense Intelligence Agency (DIA) Team formed at the request of the Commander in Chief, Atlantic (CINCLANT) operational commander for URGENT FURY. The first element arrived in Grenada on 31 October 1983 and was tasked to identify, sort, and provide approximate inventories of foreign material and to establish priorities for shipment to the United States. Nineteen other soldiers established the 203d MI Battalion (Forward) and operated a modified CMEC. Together the 203d soldiers type-classified and developed inventories; assisted combat units in searches for materiel; operated a collection point for CEE and captured enemy materiel (CEM); and shipped appropriate items to the continental United States (CONUS).

In 1985 the 203d MI Battalion was redesignated the Foreign Materiel Intelligence Group. In 1989 it was again redesignated as the Foreign Materiel Intelligence Battalion (FMIB).

THE GULF WAR (OPERATIONS DESERT SHIELD and DESERT STORM):

DESERT SHIELD and DESERT STORM were the largest battlefield TECHINT operations since the Vietnam War, and the largest joint and combined TECHINT operations since World War II. The Joint Captured Materiel Exploitation Center (JCMEC) was formed with the Army's FMIB to serve as the nucleus and headquarters. Augmentation to the FMIB included TECHINT personnel from every element of the Department of Defense (DOD), the national S&TI community, Great Britain, Canada, and Australia.

During Sadaam Hussein's attack on the Saudi Arabian city of Khafji in February 1991, a previously unseen and highly modified tank was captured. This tank, a modified T-55, had vastly improved external armor and possibly new fire control, weapons, and optical systems. A team from the JCMEC was dispatched forward to conduct a hasty exploitation and to

find out if this tank required a tactical capabilities reassessment. In layman's terms, could this new tank, with its improved armor, defeat a broader array of friendly weaponry? Within 2 days, the TECHINT collection team soldiers, analysts at the JCMEC, and national S&TI agencies in the United States were able to report their findings to the theater commander and his staff.

DESERT SHIELD and DESERT STORM produced the largest amount of CEM in the shortest amount of time since World War II. As a result of lessons learned from prior deployments, TECHINT provided unprecedented timely and accurate information to the warfighter and the national S&TI community.

SOMALIA (OPERATION RESTORE HOPE):

On 4 December 1992, the FMIB alerted a TECHINT liaison element (LNE) for deployment in support of the US Marine Corps (USMC) II Expeditionary Force, the core headquarters for Joint Task Force (JTF) Somalia.

The TECHINT LNE deployed to Somalia on 16 December and established operations at the US Embassy compound in southwest Mogadishu on 18 December. The TECHINT LNE made several significant contributions to the operations and intelligence efforts in Somalia.

On 21 December, the LNE accompanied a delegation from the JTF Somalia headquarters on a tour of compounds controlled by rival warlords in Mogadishu. During the 5 to 10 minutes the LNE was inside of each of the five compounds, the TECHINT LNE personnel compiled lists of the foreign and US weapons, equipment, and ordnance controlled by the warlords. This order of battle (OB) intelligence was key in planning the eventual US forces attack against one of those compounds.

After determining there was no theater-wide plan for the collection and processing of CEM, the TECHINT LNE established the Centralized Weapons Collection Center (CWCC). In conjunction with explosive ordnance disposal (EOD) personnel, the CWCC processed, screened for intelligence value, and disposed of thousands of captured weapons and hundreds of thousands of rounds of ammunition.

On 6 January, several SA-7 man-portable SAMs were captured in the Mogadishu area. In conjunction with EOD personnel, and with input from the US Missile and Space Intelligence Center (MSIC), the TECHINT LNE reported that the missiles were functional. This intelligence prompted a change in the air defense artillery (ADA) threat status and flight operations in Somalia.

On 14 January, several French MILAN antitank missiles were captured in

the Mogadishu area. The TECHINT LNE conducted testing and evaluation of captured missiles with personnel from the French contingent of Commander, Joint Task Force (CJTF) Somalia. The missiles were functional and capable of defeating all but the heaviest armor in the Somali theater of operations.

HAITI (OPERATIONS RESTORE DEMOCRACY and UPHOLD DEMOCRACY) :

In September 1994 FMIB deployed a 14-soldier TECHINT contingency support detachment (CSD) and a 2-soldier LNE in support of US Operation RESTORE DEMOCRACY. TECHINT LNE personnel, in conjunction with JTF 180 and JTF 190 planners, developed handling and processing procedures for CEM, including weapons received as part of the "Cash for Guns" program.

The CSD established the JCMEC (Forward) in Port-au-Prince. The CSD screened, processed, and inventoried over 10,000 weapons and thousands of rounds of ammunition by hand without the benefit of materiel-handling equipment. The resulting database provided OB analysts a tool for assessing the threat to US forces as well as the success of the "Cash for Guns" program. Additionally, the "by serial number" inventory was forwarded to national law enforcement agencies via CI liaison channels to aid in arms smuggling investigations.

At the time of redeployment, CSD personnel had accomplished all assigned national TECHINT collection requirements, and through intelligence discipline integration, played key roles in various signals intelligence (SIGINT) and human intelligence (HUMINT) operations.

LESSONS LEARNED

The historical experience of the nation in times of peace and war clearly demonstrates the need for a fully operational Army TECHINT capability. A robust TECHINT collection and analysis capability, with dynamic links to S&TI centers in the United States is especially vital in the future's technologically sophisticated battlefield. This capability is required to correctly portray the battlespace for warfighting commanders. Furthermore, TECHINT enhances force protection. To neglect TECHINT during the planning and execution of Army operations invites the possibility of technological surprise.

Chapter 2

SCIENTIFIC AND TECHNICAL INTELLIGENCE

INTRODUCTION

TECHINT is the end product of a complex process. It is the result of collecting, analyzing, and processing information on foreign technological developments. It is also the result of studying the performance of foreign materiel and its operational capabilities.

TECHINT has two goals:

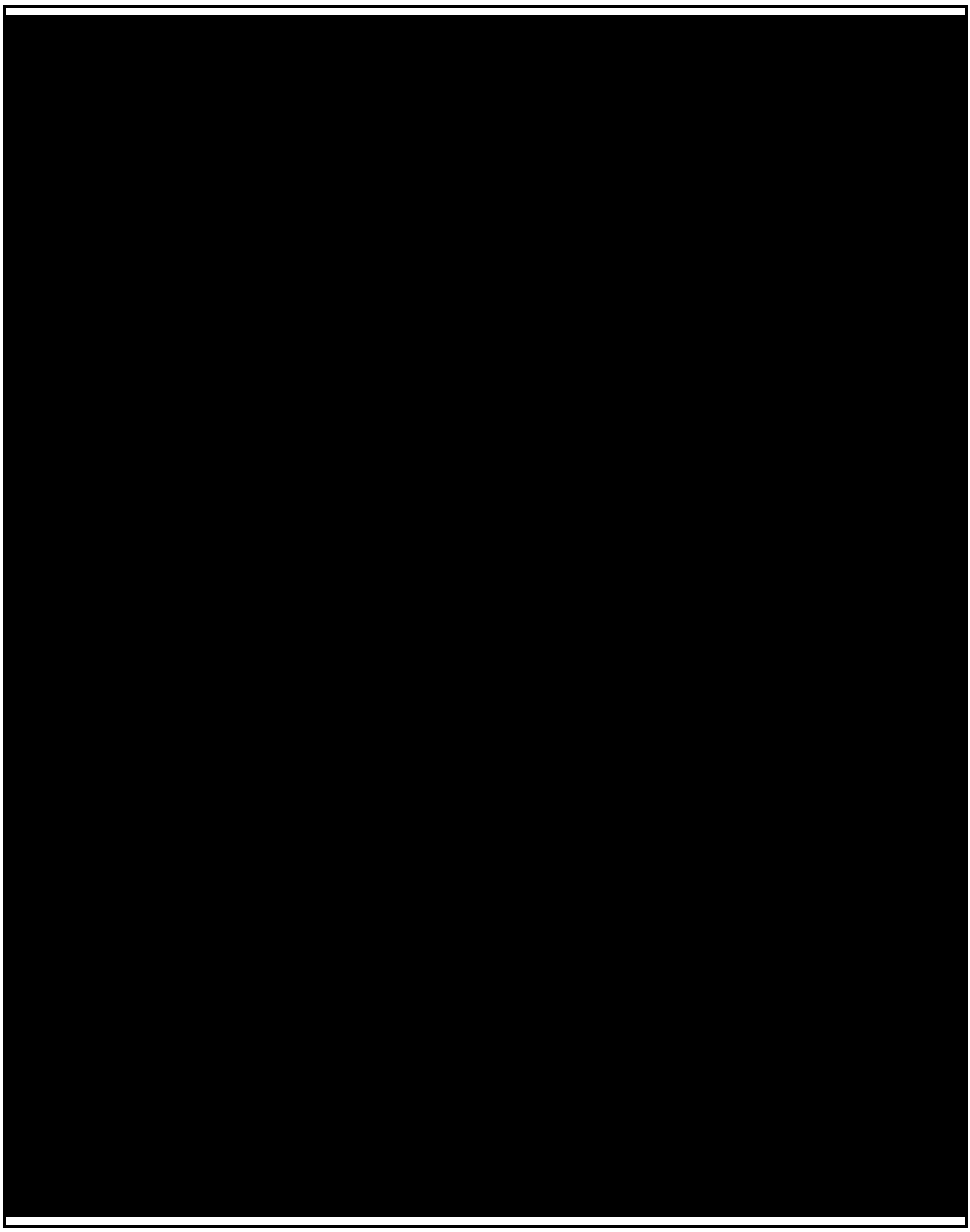
- To ensure the US armed forces maintain technological advantage against any adversary.
- To provide tailored, timely, and accurate TECHINT support to the warfighter throughout the entire range of military operations.

This support includes providing US forces information and training on foreign weapons systems to an extent that allows use of the CEE. The TECHINT system accomplishes both missions.

THE S&TI COMMUNITY

The S&TI community satisfies the nation's overall TECHINT objectives during peacetime, and the strategic TECHINT requirements in wartime. The S&TI community starts at the DOD level. Figure 2-1 shows this organizational structure.

S&TI is designed to track and analyze foreign technological developments. It is used to analyze the performance and operational capabilities of foreign materiel that may have military application.
Although the primary function of the S&TI community is to satisfy strategic TECHINT objectives, it also makes significant contributions toward fulfilling operational and tactical TECHINT requirements. Strategic communications between battlefield TECHINT units and S&TI centers allow the use of their comprehensive databases and expertise to rapidly satisfy the TECHINT requirements of the warfighter.



STRUCTURE

DEFENSE INTELLIGENCE AGENCY:

DIA manages and reviews overall TECHINT activities throughout DOD during peacetime and war. The S&TI directorate within DIA is the action element for TECHINT. This directorate coordinates with external TECHINT agencies on nonpolicy matters concerning the production of S&TI.

Armed Forces Medical Intelligence Center (AFMIC). AFMIC, based at Fort Detrick, MD, is a DOD intelligence production center under control of DIA. AFMIC is responsible for exploiting foreign medical materiel. The director supports the Army Foreign Materiel Exploitation Program (FMEP) and Army medical R&D requirements. The director coordinates with the Deputy Chief of Staff, Intelligence (DCSINT) in planning, programming, and budgeting. AFMIC—

- Studies and reports foreign medical S&TI and general medical intelligence to DOD and other Federal agencies.
- Studies and reports foreign biological warfare S&TI capabilities.
- Administers the DOD Foreign Medical Materiel Exploitation Program (FMMEP).
- Provides "quick response" foreign medical intelligence support to DOD and other Federal agencies.
- Maintains a mutually beneficial S&TI exchange with the US Army Intelligence and Security Command (INSCOM) to complement Army capabilities.

***Missile and Space Intelligence Center (MSIC)*.** MSIC, based at Redstone Arsenal, AL, is a DOD intelligence production center under control of DIA and supports the FMEP. The MSIC acquires, produces, maintains, and disseminates S&TI pertaining to missile and space weapons systems, subsystems, components, and activities. The S&TI produced at MSIC also covers foreign state-of-the-art technology and research applicable to missiles. MSIC analyzes—

- Directed energy weapons.
- Antisatellite technology.
- Tactical air defense.

- Short-range ballistic missiles (SRBMs).
- Antitank guided missiles (ATGMs).

Defense HUMINT Service (DHS). DHS conducts worldwide HUMINT operations in support of foreign materiel acquisition and exploitation.

NATIONAL SECURITY AGENCY (NSA):

NSA is the SIGINT organization of the US Government. It is responsible for exploiting cryptologic and electronic warfare (EW) materiel.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA):

DARPA is the central R&D organization for DOD. It manages and directs selected basic and applied R&D projects for DOD and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions. DARPA sponsors R&D in all aspects of TECHINT, including imagery intelligence (IMINT), SIGINT, HUMINT, and measurement and signature intelligence (MASINT). For the latest description of DARPA projects, visit the DARPA World Wide Web site on the Internet: http://www.arpa.mil/.

AIR FORCE:

National Air Intelligence Center (NAIC). NAIC is the primary DOD agency producing foreign aerospace S&TI. It satisfies DIA requirements and supports the Air Force Assistant Chief of Staff for Intelligence (AFACSI). NAIC acquires, analyzes, produces, and disseminates S&TI related to current and future enemy aerospace capabilities.

NAVY:

Naval EOD Technical Division and Fire Support and Armament Command EOD. These are the primary training centers of all Joint EOD personnel. Augmented by Army EOD specialists from Picatinny Arsenal, they act as primary centers establishing identification, render safe procedures (RSPs) and demolition procedures for foreign ordnance.

Office of Naval Intelligence. The Navy proponent for TECHINT in the Office of Naval Intelligence (ONI) is designated ONI-23. ONI-23 provides

S&TI on technical characteristics and capabilities of foreign naval forces and merchant systems. It provides S&TI support to the Commander of the ONI and the Chief of Naval Operations.

ARMY:

Office of the Deputy Chief of Staff, Intelligence (ODCSINT). Although ODCSINT does not produce intelligence, it does have general staff responsibility for all Army TECHINT activities. The ODCSINT—

- Formulates policies and procedures for S&TI activities.
- Supervises and carries out the Army S&TI program.
- Coordinates Department of the Army (DA) staff and major subordinate command requirements for TECHINT.
- Is responsible for the Army Foreign Materiel Program (FMP).

US Army Materiel Command (AMC). AMC is a major Army command (MACOM) with a significant support role in TECHINT. Among AMC elements are a series of research, development, and engineering centers (RDECs), the Army Research Laboratory System, and the US Army Test and Evaluation Command (TECOM). Each plays a role in wartime in conducting highly technical evaluations of foreign equipment. In peacetime, the AMC conducts foreign materiel exploitation (FME) on equipment purchased by each laboratory and RDEC for the intelligence community and for DOD as part of the International Materiel Evaluation Program (IMEP).

AMC's Foreign Ordnance exploitation team is at the Fire Support Armaments Center (FSAC) EOD (Picatinny Arsenal). They exploit foreign ground ordnance and develop RSP for foreign ordnance. They also prepare detailed intelligence reports to support EOD, Intelligence, and US munitions developer communities.

Additionally, AMC operates the Scientific Intelligence Center Europe (STICEUR) and Scientific Intelligence Center Far East (STICFE) with the purpose of overtly collecting information on foreign technical developments by attending arms shows and technology exhibitions.

AMC's Chemical and Biological Defense Command (CBDCOM) is the headquarters for the US Army Technical Escort Unit (TEU). This unit has the mission to collect and escort nuclear, biological, and chemical (NBC) samples from the battlefield to CONUS for testing and evaluation.

US Army Intelligence and Security Command **(INSCOM).** Under the direction of Headquarters, Department of the Army (HQDA), INSCOM is responsible for peacetime TECHINT operations. Headquarters, INSCOM, fulfills its responsibilities through its TECHINT oversight function and manages the Army's Foreign Materiel for Training (FMT) Program and FMEP. It does this by—

- Providing the interface with strategic S&TI agencies in support of foreign materiel exploitation.
- Organizing, training, and equipping echelons above corps (EAC) TECHINT organizations during peacetime.

Headquarters, INSCOM, controls two organizations that facilitate TECHINT: National Ground Intelligence Center (NGIC) and the 203d MI Battalion.

National Ground Intelligence Center:

Headquarters, INSCOM, exercises direct operational control over the NGIC. NGIC produces and maintains intelligence on foreign scientific developments, ground force weapons systems, and associated technologies. NGIC analysis includes, but is not limited to, military communications-electronics (C-E) systems which include—

- Types of aircraft used by foreign ground forces (usually rotary wing).
- NBC systems.
- Basic research in civilian technologies with possible military applications.

203d Military Intelligence Battalion:

The 203d MI Battalion, headquartered at Aberdeen Proving Ground, MD, is the only AC TECHINT battalion. The 203d MI Battalion is subordinate to the Force Projection Brigade (FPB) supporting national level S&TI. It—

- Conducts TECHINT and MASINT collection and reporting in support of validated S&TI objectives and MASINT data requirements (MDRs).
- Acts as the HQDA executive agent for foreign materiel used for training purposes.
- Conducts formalized TECHINT and MASINT training for DOD analysts

and RC TECHINT personnel.

- Supports INSCOM's foreign materiel acquisition (FMA) operations and FME operations as directed.

- Supports the Technical Reconnaissance and Surveillance (TECRAS) Program through its MASINT detachment. See Appendix A for MASINT support to TECHINT operations.

All TECHINT assets that reside in the RC are Wartraced to the 203d MI Battalion. Their primary peacetime mission focuses on training. However, certain RC TECHINT units and individuals are tasked to augment real world S&TI missions.

Chapter 3

BATTLEFIELD TECHNICAL INTELLIGENCE OPERATIONS

INTRODUCTION

This chapter describes battlefield TECHINT operations, functions, and procedures. Battlefield TECHINT operations consist of collection, hasty exploitation, initial TECHINT reporting, analysis, evacuation (as necessary), detailed exploitation and analysis, and production and dissemination of final TECHINT products. The term "battlefield" includes any area of operation that US forces occupy while conducting the full range of military operations.

Battlefield TECHINT can start with one conscientious soldier identifying something new in the area of operations and taking the proper steps to report it. The information or item is initially exploited to ascertain if it represents an advantage for the enemy. If it does, the information or item then undergoes increasing levels of analysis until a countermeasure is developed and the technological advantage is neutralized. While a single weapon or technology seldom means the difference between final victory or defeat, it can give one side a battlefield advantage.

A mutually dependent relationship exists between the support the warfighter gets from the TECHINT process and the support TECHINT gets from the warfighter. Operational and tactical commanders identify, capture, protect, and evacuate CEM that undergoes analysis for TECHINT value. TECHINT analysts receive CEM, conduct detailed exploitation, and recommend countermeasures to overcome an enemy's technological advantage.

Another result of this analysis is the development of a new US technology or an enhancement to an existing technology. In any case the end result is the neutralization of the adversary’s technological advantage.

Commanders further ensure the success of the process by demanding TECHINT support to accomplish their assigned missions.

203D MI BATTALION (TECHINT):

The 203d MI Battalion (TECHINT) mission during conflict and war is to provide near-real-time (NRT) intelligence derived from the exploitation of weapons, equipment, and other materiel found, captured, or acquired within the theater area of operations. This includes all items of an S&T nature. This battalion is the centerpiece of the theater TECHINT mission; task-organizing personnel and equipment to support several echelons. Figure 3-2 shows the 203d MI Battalion (TECHINT) organization. The HHC and the TECHINT Exploitation Company form the CMEC. This union is discussed below.

HEADQUARTERS AND HEADQUARTERS COMPANY (HHC):

HHC conducts normal service support operations. In addition, its personnel may be tasked to perform duties as LNEs at various echelons. The S4 section, besides its normal maintenance and logistics staff responsibilities, also plays a significant role in the TECHINT concept of operations. The S4—

- Conducts warehouse operations for all CEE maintained at the CMEC.
- Monitors CEE at the Corps level collection points.
- Monitors captured ammunition and ordnance at Corps ammunition points.
- Assists in the transportation and tracking of equipment from theater to CONUS.

TECHINT EXPLOITATION COMPANY:

The TECHINT Exploitation Company consists of TECHINT collection managers and senior technical analysts in weapons and armaments, mobility systems, EW and communications systems, and chemical, medical, and logistics systems.

During joint and/or combined operations the CMEC may receive joint and/or combined augmentees. In this case, the CMEC is redesignated as the JCMEC or Combined Joint Captured Materiel Exploitation Center (CJCMEC). In all three configurations, the CMEC is commanded by the Commander, 203d MI Battalion. See Appendix B for JCMEC operations and responsibilities.

TECHINT COLLECTION COMPANY:

The TECHINT Collection Company consists of three TECHINT collection teams that normally are attached one per Corps MI brigade. The teams' mission is to conduct the initial identification and exploitation of foreign equipment in support of the Corps and, when directed, theater and national requirements. Additionally, the teams help monitor evacuation of the equipment off the battlefield.

The MI Team (TECHINT) (Collection) serves as the intelligence collection system for the battalion. It consists of TECHINT-qualified soldiers trained in the military occupational specialties (MOSs) shown in Figure 3-3. These teams, trained in TECHINT analysis, deploy forward of the JCMEC

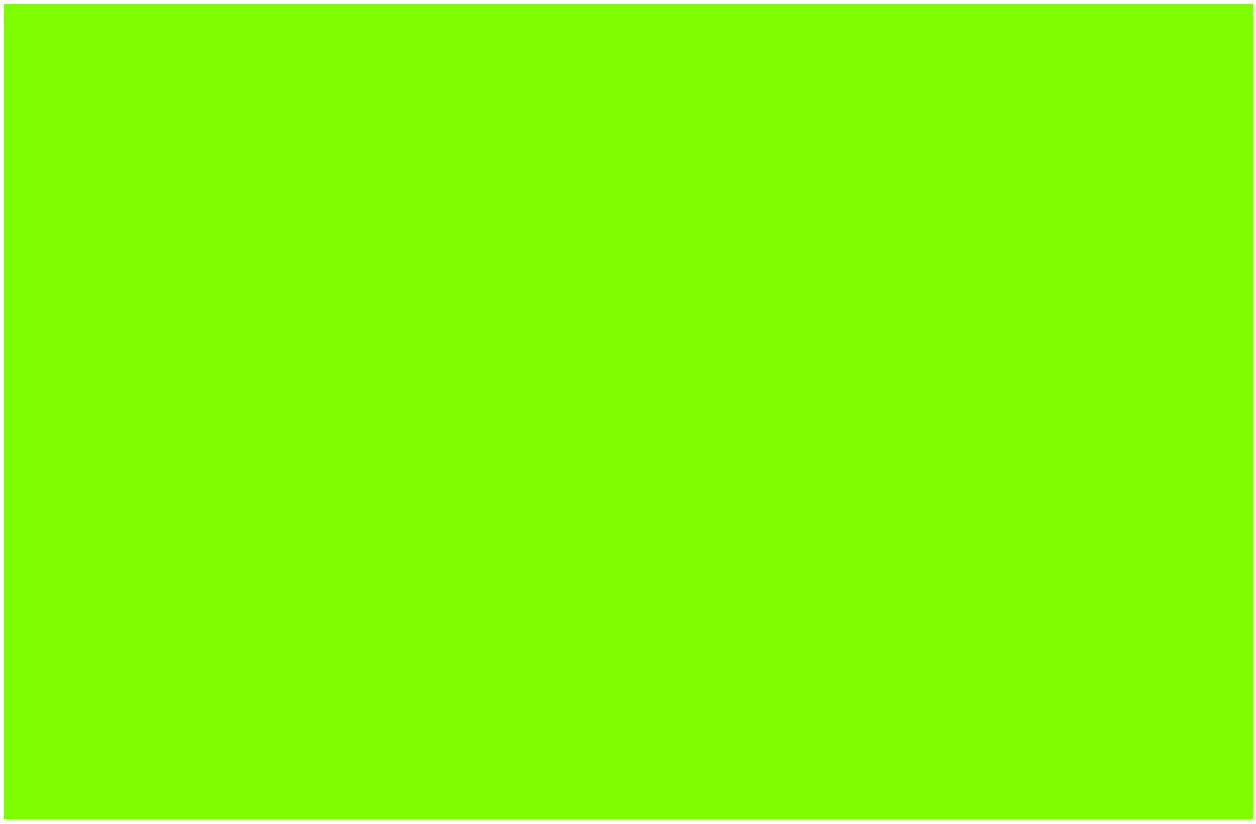
into the Corps area and receive their taskings from the CMEC through

TECHINT LNEs at the Corps G2. CEE is stored in the theater COSCOM.

NTC AND MASINT DETACHMENTS:

The Naval Technical Center (NTC) TECHINT Detachment, currently C Detachment, 203d MI Battalion (TECHINT), is similar to the TECHINT Collection Company in its mission to conduct initial identification and exploitation of foreign equipment in support of Corps, theater, and national requirements. It is organized similar to the TECHINT collection teams that are subordinate to the TECHINT Collection Company. During wartime or contingency it would have the same command and control relationships as a TECHINT collection team. It also has the additional mission of supporting INSCOM's FMT Program at the National Training Center.

The MASINT Detachment attaches MASINT analysts to the TECHINT collection teams and also provides senior analysts to the TECHINT Collection Company.



BATTLEFIELD TECHINT CHANNELS

The battlefield TECHINT channels are designed to support both operational and tactical levels of war. They support warfighting commanders at all levels (see Figure 2-1).

EAC TECHINT support consists of the Joint Technical Intelligence Branch (JTIB) located at the Theater Joint Intelligence Center (JIC), the CMEC formed around the 203d MI Battalion, and TECHINT LNEs located at various EAC analysis and control elements (ACEs). These EAC TECHINT assets provide general support to the theater.

Echelons corps and below (ECB) TECHINT support initially consists of TECHINT collection teams and TECHINT LNEs detached from the 203d MI Battalion. At a minimum, one TECHINT collection team is attached to each Corps MI Brigade. The team takes operational direction from the G2 via the TECHINT liaison officer (LNO) in providing direct support to ECB units from forward locations on the battlefield. A TECHINT LNE is attached to each Corps G2 or component equivalent. Upon mobilization, RC TECHINT units augment the 203d MI Battalion.

Regardless of the echelon, TECHINT elements are equipped to give the supported commander timely, relevant, accurate, and predictive information and recommended countermeasures based on CEM exploitation. This exploitation includes identifying, analyzing, and coordinating the evacuation of CEE, CED, and other CEM. See
Appendix C for procedures for handling and evacuating CEM.

JOINT TECHNICAL INTELLIGENCE BRANCH

The JTIB is formed during joint operations. The JTIB is located at the Theater JIC and is composed of military and civilian TECHINT subject matter experts (SMEs). The JTIB chief is normally the DIA representative and serves as the senior advisor on TECHINT matters to the Theater Commander and the J2.

The JTIB conducts the following missions:

- Coordinates all national, operational, and tactical TECHINT requirements for the theater.
- Develops the theater TECHINT collection plan.
- Coordinates with the J2 and the JCMEC to execute all TECHINT

requirements.

- Provides liaison and coordination support for the JCMEC and the TECHINT collection teams at the JTF level.

CAPTURED MATERIEL EXPLOITATION CENTER

The main effort of the TECHINT mission is executed through a CMEC formed from TECHINT personnel from the 203d MI Battalion. The CMEC is the first major processor of CEM of TECHINT value. The CMEC—

- Exploits CEM based on national, Theater, and supported commanders' requirements.
- Produces TECHINT reports (including countermeasures) for tactical commanders.
- In coordination with EOD, provides render safe procedures (RSPs) for foreign munitions to combat units.
- Coordinates the safe handling and evacuation of CEM.
- Coordinates evacuation of special-interest CEM from ECB locations to the CMEC.
- Supervises evacuation of CEM from theater to CONUS.
- Coordinates with the Theater or Joint Interrogation Facility for the selection and technical interrogation of enemy prisoners of war (EPWs) assessed to have TECHINT-related knowledge. TECHINT analysts may assist interrogators and strategic debriefers during interrogation of a wide range of HUMINT sources of TECHINT interest by conducting "quarterback" debriefing operations with the debriefers.
- Provides accountability for CEE and CEDs within the theater TECHINT structure.
- Recommends CEM disposition to the Theater and Corps commands.
- Maintains the theater TECHINT database.
- Maintains the theater S&TI and battlefield TECHINT requirements.

The CMEC normally is located in the theater rear area near main supply routes (MSRs) and air and sea ports to accommodate rapid evacuation of

equipment. Every effort should be made to collocate the CMEC with the Theater Interrogation Facility to enhance the integration of HUMINT and TECHINT operations.

Additionally, being collocated provides a single geographical area where subordinate units bring captured personnel and CEM, as well as consolidating many transportation and security requirements. Regardless of its location, it is fully equipped with sensitive and sophisticated test and communication equipment. Analyst teams use this equipment to perform detailed in-theater exploitations.

The CMEC can also organize a team from organic CMEC assets to meet immediate requirements of echelons without TECHINT support. These teams can deploy forward or support rear area units as required.

JCMEC AND CJCMEC

The JCMEC and CJCMEC are organized and conduct the same missions as the CMEC. The JCMEC and CJCMEC differ as follows. They—

- Allow a free flow of information, reports, and TECHINT exploitation summaries between joint forces and/or allies; this is because the intelligence support staff is joint and/or combined.
- Coordinate scientific exploitation assistance from joint and/or allied TECHINT analysts.
- May provide direct support US and allied TECHINT teams to joint and/or allied ECB units as required.

TECHINT LIAISON ELEMENTS

The TECHINT LNEs are composed of TECHINT personnel from the 203d MI Battalion. The LNEs serve as advisors on all TECHINT-related matters. The TECHINT LNEs provide coordination and tasking support for the CMEC and the theater TECHINT effort. The TECHINT LNEs consist of one to three TECHINT personnel. Figure 3-4 shows the possible locations of TECHINT LNEs if deployed as part of a JTF.

CORPS CMEC (FORWARD)

An RC TECHINT section may staff a Corps level CMEC (Forward) normally located at the Corps Support Command (COSCOM) area Class VII collection point. Its primary mission is to inventory and identify CEE located at the COSCOM Class VII collection point and screen it for items of TECHINT value.

After identifying an item of TECHINT value, the CMEC (Forward) coordinates with the Corps G4 through the supporting TECHINT LNE for the transportation of the item back to the CMEC. The CMEC (Forward) supports the movement of the CEE by packing or crating it when required. The RC TECHINT section conducts preliminary exploitation and reporting on the identified materiel and assists the Corps TECHINT teams as required.

The RC TECHINT section normally consists of 15 personnel with organic transportation. The section's detailed analysis of CEE may be limited due to number of personnel and organic equipment.

BATTLEFIELD TECHINT COLLECTION TEAMS

The 203d MI Battalion provides direct support TECHINT collection teams to ECB MI Brigades or Marine Expeditionary Force (MEF) intelligence elements. These teams are mobile and organized according to available resources and subordinate command requirements.

TECHINT collection teams perform their mission as a tactical extension of the CMEC. They concentrate on the initial identification and exploitation of CEM and provide TECHINT assistance to Corps and Division G2s. Detailed analysis by these teams is limited due to personnel limitations and lack of extensive diagnostic equipment. The TECHINT collection team normally will have 14 TECHINT analysts and 2 MASINT analysts.

TECHINT collection teams are usually staffed with analysts capable of exploiting threat equipment and documents in eight functional areas: C-E, automation systems, weapons, munitions, NBC, medical, mobility, and signatures analysis. The areas are described below:

- C-E TECHINT is the analysis and exploitation of foreign and threat communications, computers, radars, intercept and jamming equipment, and like systems, including electro-optic and directed-energy technology.

- Automation systems TECHINT is the analysis and exploitation of foreign automation hardware and software.

- Weapons TECHINT involves the analysis of threat weapons and weapon systems, including rocket, tube artillery, mortars, small arms, ATGMs, other missiles, and associated fire control.

- Munitions TECHINT involves the analysis of threat munitions including missiles, NBC munitions, direct and indirect fire weapons ammunition, explosives, and mines.

- NBC TECHINT is based on the analysis of threat offensive and defensive NBC material including NBC samples, flame materials, and obscurants. This analysis determines threat strengths and vulnerabilities in relation to NBC operations.

- Medical TECHINT focuses on the identification, evaluation, and exploitation of medical materiel, general purpose systems modified for medical support, and biological agents sampling.

- Mobility TECHINT exploits threat vehicles, engineer equipment, materiel handling equipment, and power generation. Mobility TECHINT determines the capabilities and vulnerabilities of the enemy to maneuver and support its combat forces on the battlefield.

- Signatures analysis involves collecting and analyzing the acoustic, infrared, and hyperspectral and seismic signatures of foreign equipment.

Historical Vignette

The XVIII Airborne Corps in support of a JTF is engaged in military operations in the country of Zula. During search operations, Company A of the 1st Battalion, 25th Infantry, discovers a recently vacated facility that contains chemicals.

The commander notifies the 1st Battalion S2 and secures the facility until a permanent security force arrives. The Battalion S2 notifies the Brigade S2, who in turn requests that the battlefield TECHINT collection team investigates the facility.

The battlefield TECHINT collection team arrives at the facility and does a cursory evaluation. Upon initial identification, several chemical samples are removed and transported to the Corps CMEC (Forward). The battlefield TECHINT collection team submits a report through channels to the JTF J2 stating that certain suspect chemicals have been found; they've been identified as nerve gas; they will be moved to the Corps CMEC (Forward), and the team will confirm its initial findings in a follow-up report within 4 hours.

Upon receipt, the Corps CMEC (Forward) coordinates with the Corps G4, through the supporting TECHINT LNE, to transport the chemicals to the Corps CMEC.

If identification is made at the Corps CMEC, then the Corps G2 submits a report through the Corps ACE to the JTF J2, for dissemination to the XVIII Airborne Corps G2, 1st Brigade S2, and 1st Battalion S2 for further dissemination to the Commander of Company A (the unit that found the chemicals). The Corps G2 also provides the report to other commanders and staffs within the AO. If identification or further analysis is required, the Corps CMEC coordinates the safe handling and evacuation of chemicals to CONUS for identification and reporting.

Chapter 4

INTELLIGENCE CYCLE APPLIED TO TECHNICAL INTELLIGENCE OPERATIONS

The five-step process known as the intelligence cycle is applied to TECHINT operations to ensure synchronization with the overall all-source intelligence mission and collection plan.

PLAN AND DIRECT

Intelligence preparation of the battlefield (IPB) is the primary intelligence task which helps the J2/G2 focus and direct this step of TECHINT and the remaining steps of the intelligence cycle. Figure 4-1 shows an example of planning and directing.

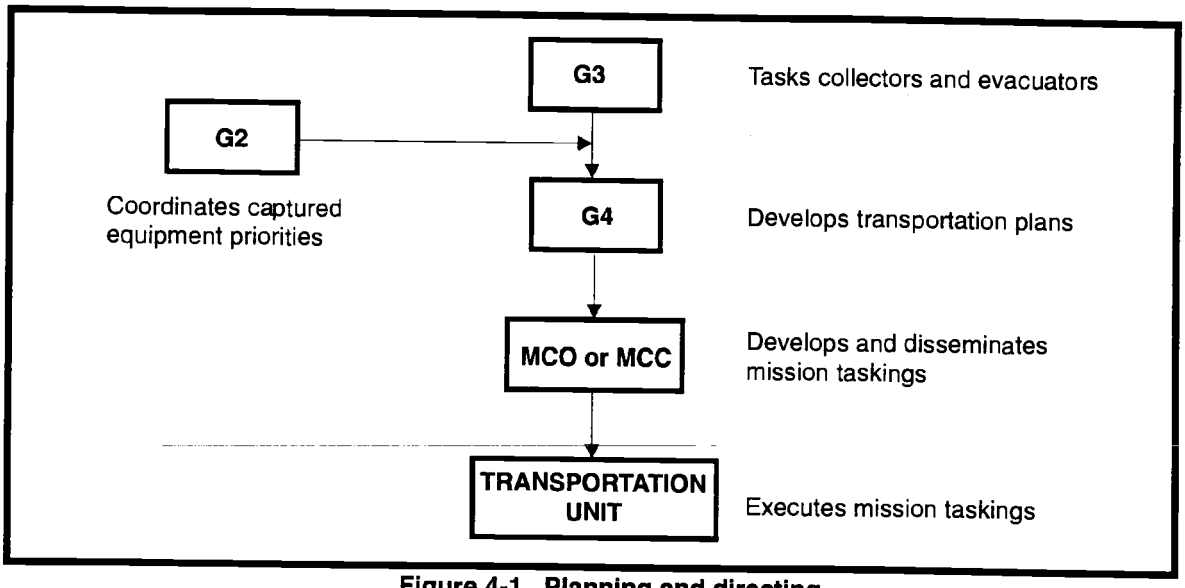


Figure 4-1. Planning and directing.

The JTIB develops the commander's TECHINT priority intelligence requirements (PIR), TECHINT information requirements (IR), and specific information requests (SIR). The JTIB helps develop TECHINT commander's critical information requirements (CCIR) and SIR of a TECHINT nature. The JTIB ensures requirements are closely coordinated with combatant command J2, or theater Army G2 as well as major subordinate commands; for example, corps G2. The JTIB then integrates and deconflicts these CCIR and SIR with other items of special interest to the S&TI community and develops a prioritized TECHINT collection list.

The TECHINT CCIR and SIR and the prioritized TECHINT collection list normally are found in the TECHINT Appendix to the Intelligence Annex to the operations order (OPORD) at all echelons maneuver brigade or group and above.

Through all-source analysis, the JTIB and JCMEC template are where items of TECHINT interest are most likely to be found on the battlefield. This is referred to as "TECHINT templating." Appropriate units are notified, through intelligence, that these items may be within their areas of operations and are tasked for collection through collection management channels. The taskings must be translated into terms that combat, support, and specific collectors can understand.

The taskings should include a TECHINT target folder (TTF). Figure 4-2 shows an example of a TTF. At a minimum, the TTF should include a description of the item, with what major combat systems the item is associated, as well as handling instructions, reporting instructions, and a photograph or sketch if available. The JCMEC and Corps level CMEC (Forward) are responsible for producing TTFs.

1. General information:
    a. Target folder inventory/index.
    b. Record of changes/updates.
    c. Validation/review sheet.
    d. Target identification data—
        (1) Name.
        (2) Description.
        (3) Photographs or sketches (imagery showing location on major end item if TECHINT item is subcomponent).
        (4) Country of origin.
        (5) Other equipment associated with materiel.
        (6) General description/significance (brief explanation of importance of materiel in terms of direct results should its use be denied partially or totally).
        (7) Type of unit materiel is associated with (unit designation if available).
        (8) Disposition instructions.
        (9) References.

Figure 4-2. TECHINT target folder.

Additionally, the JCMEC must develop TECHINT-related indicators and SOR for other intelligence disciplines to augment and complement the single-source TECHINT effort. One example would be the development of TECHINT-related screening questions for EPWs as they are processed. Another might be to request that imagery analysts keep an

eye out for a suspected external modification on a particular model of main battle tank during the normal course of their duty.

COLLECT

TECHINT collection is acquiring foreign materiel, associated technical documents, or other information of TECHINT interest and providing these to the processing and production elements. It includes the maneuver and positioning of intelligence assets to locations favorable to satisfying TECHINT collection objectives.

All TECHINT collection is guided by CCIR, SIR, and the TECHINT collection list. Battlefield TECHINT collection includes capturing, reporting, and evacuating CEM. For that reason, tactical TECHINT and intelligence planners must include a CEM appendix in the Logistics Annex to the OPORD. Logistics is critical in TECHINT collection operations.

Forward deployed units capture or collect items of known or possible TECHINT interest. Capturing units will normally safeguard CEM and report it through intelligence channels to the first TECHINT element in the reporting chain, normally the TECHINT LNE at Corps G2. The Corps TECHINT LNE then forwards the report simultaneously to the JCMEC and JTIB and verifies if the type of materiel captured is required. Further disposition is determined, appropriate coordination is made by the Corps TECHINT LNE with G2/G3 staff, and the capturing unit receives guidance through operational (G3/S3) channels. Figure 4-3 describes the flow of CEM guidance and decisions.

A TECHINT collection team may be sent forward to confirm the identification and conduct initial exploitation of the materiel at the site. Often the items of TECHINT value are subcomponents of major end items. In this case, the collection team removes and evacuates the items using organic transportation, as shown in Figure 4-4.

The capturing unit may be ordered to evacuate the materiel with its organic equipment. In this instance, they will receive detailed instructions from the Corps LNE or direct support TECHINT collection team via G3/S3 channels. The Corps LNE or TECHINT collection team moves to the materiel's location at the Corps CEM collection point when the materiel is not taken directly to a Corps CMEC (Forward) or Theater JCMEC.

TECHINT collection can prove to be a significant force protection multiplier. One example is TECHINT team identification of NBC materiel prior to transport, handling, or destruction of munitions or samples.

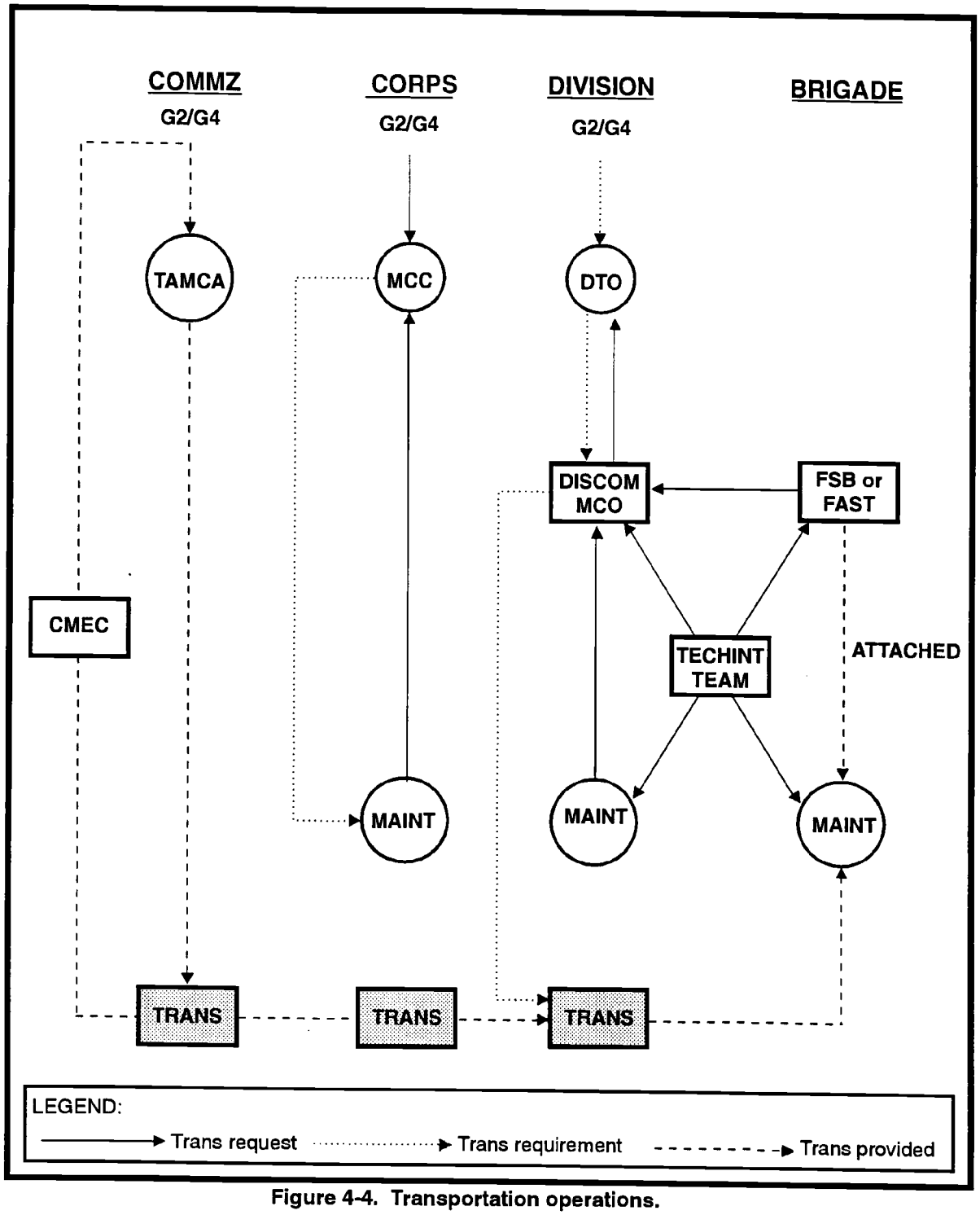


Figure 4-4. Transportation operations.

PROCESS

Processing is the conversion of collected information into a suitable form that can be readily used to produce intelligence. Processing includes data from conversion, photographic development, and transcription and translation of foreign language materiel. Effective processing management ensures that critical information is extracted and processed ahead of information of lesser immediate value. Reports are generated and sent to all appropriate theater and national assets during this process.

TECHINT processing starts with the capture of a piece of equipment of TECHINT value. This confirms that the enemy is indeed employing this materiel. A TECHINT collection team normally conducts a hasty exploitation at the capture site. After the hasty exploitation, a decision is made at the JCMEC or JTIB as to whether the process continues. If it does, the items are sent to the Corps CMEC (Forward) or Theater JCMEC. If the item is deemed to yield no immediate tactical intelligence value, it may still be evacuated to the S&TI centers in CONUS for further analysis if the systems represent a change in the technological posture of an enemy.

PRODUCE

Producing involves the integration, evaluation, analysis, and synthesis of information from single or multiple sources into intelligence. At the tactical level, time constraints and demands of the battle tend to make the processing and producing steps indistinguishable.

TECHINT reports (along with interrogation reports from EPWs with TECHINT knowledge) and digital imagery both funnel into the JCMEC where they undergo the dynamics of production mentioned above. They are then sent to the JTIB and Theater ACE as a single-source TECHINT product.

DISSEMINATE

Dissemination is the timely conveyance of intelligence to users in an easily consumable form. The diversity of forms and means requires interoperability among command, control, communications, and intelligence (C^3I) systems. TECHINT reporting from JCMEC to the Theater ACE will be conducted through existing communications links (See Appendix B for communications architecture).

The JCMEC sends its completed products to the JTIB and to the Theater ACE. This report is based on the standard intelligence information report

(IIR) format. TECHINT reports are then disseminated through two channels. The ACE fuses the TECHINT single-source product into its all-source reports and disseminates them through normal J2/G2/S2 channels. While the TECHINT single-source product is being integrated into the ACE all-source product, the JTIB disseminates the single-source TECHINT product through TECHINT communications channels to the national S&TI centers in CONUS. This ensures both the rapid dissemination of TECHINT and the fusion of TECHINT into all-source products.

The intelligence cycle is a continuous process in which steps are executed concurrently, although not always sequentially. For example, while new information is being collected to satisfy one set of TECHINT requirements, a new TECHINT item may be reported on the battlefield. The JTIB plans and redirects efforts while the intelligence produced from the previously collected materiel or information is disseminated. One or several iterations of the intelligence cycle may be conducted depending on the time constraints of the mission.

BATTLEFIELD TECHINT REPORTING SEQUENCE

THE CAPTURE:

A soldier either captures or observes an item of possible TECHINT interest and does not tamper with it. The soldier quickly reports the encounter via the size, activity, location, unit, time, and equipment (SALUTE) spot report format through the chain of command to the Battalion S2. The soldier then either safeguards the items or continues the mission as directed (see Figure 3-1).

BATTALION S2:

The battalion S2 coordinates security or continued observation of the item with the S3 and ensures the item is not tampered with in any way.

WARNING

Components, control knobs, and switches on C-E equipment **MUST NOT** be touched until the equipment is photographed or positions recorded by TECHINT or other trained personnel to avoid the possibility of immediate personal injury or damage to equipment.

The battalion S2 reports the items in the SALUTE format to the brigade S2, and continues security or observation of the items until receiving further instructions. When possible, the capturing units identify associated items requiring immediate screening for combat information by other supporting

MI elements. This could include C-E systems, code books, or technical documents such as operator manuals.

TECHINT LNE:

The TECHINT LNE at Corps (or lowest level) receives the SALUTE report through intelligence reporting channels. He then compares report information with outstanding requirements to see if collection is necessary. Depending on the priority of the requirement and tactical situation, the Corps LNE may—

- Coordinate with the G3 and MI Brigade Commander to dispatch the Corps direct support TECHINT collection team to the capture site.
- Give further instructions for exploitation and/or evacuation procedures to the capturing unit S2.

If an intelligence requirement no longer exists for the captured equipment, the LNE informs the capturing S2 who disposes of the materiel within normal logistics channels.

In any case, the Corps TECHINT LNE forwards an information copy of the SALUTE report with details of initial actions taken to the JTIB, JCMEC, and other TECHINT LNEs.

BATTLEFIELD TECHINT ANALYSIS

Once a TECHINT unit takes custody of a TECHINT item, battlefield TECHINT exploitation begins. TECHINT analysts and specialists use checklists established by S&TI agencies and the JCMEC to exploit each type of threat equipment for which requirements exist. S&TI and the JCMEC develop battlefield exploitation procedures from four sources:

- The US Army Test and Evaluation Command's international test operation procedures.
- Coordination with S&TI analysts.
- Theater and Corps TECHINT requirements.
- Their own experience.

Exploitation procedures are standardized yet constantly updated and included in different exploitation plans based on the type of equipment or documents being exploited. These plans steer the analysis process.

As the materiel moves through the TECHINT chain, each succeeding level of the exploitation process is completed. TECHINT units maintain procedures and plans for sampling, exploiting, and handling materiel in the following categories:

- Missile guidance systems, warheads, fuses, and propellants.
- Munitions, mines, explosives, and their effects.
- Direct and indirect fire systems of all types and their effects.
- Tracked and wheeled vehicles and transports.
- Various types of armor, radios, and radar.
- EW, intercept, and jamming equipment.
- Communications, antenna, relay, and telephone equipment.
- Teletypes.
- Directed energy weapons.
- Automated data processing (ADP) hardware and software.
- NBC offensive and defensive equipment.
- Tactical aviation.
- Medical equipment capabilities and vulnerabilities.

Although exploitation plans are extremely useful, it is the analyst who determines the actual steps to use in each procedure. Analysis always begins with what is, and what is not, known about the piece of equipment.

Chapter 5

RESPONSIBILITIES

INTRODUCTION

This chapter outlines the various responsibilities of each staff element in units on the battlefield when supporting the overall battlefield TECHINT effort. Battlefield TECHINT elements are resourced and responsible for collecting and processing CEM. Yet to work properly, the battlefield TECHINT structure relies on many other units for mission support, such as combat units which capture items, and the transportation units which evacuate items of TECHINT interest. Figure 5-1 shows staff responsibilities.

STAFF SECTIONS

The duties of coordination staff sections and how they relate to TECHINT direction, collection, processing, production, and dissemination are discussed below. From the J1/G1 to the J5/G5, every staff section contributes in some way to the successful production and use of TECHINT.

ASSISTANT CHIEF OF STAFF, J1/G1, PERSONNEL

The J1/G1 is the principal staff element for the commander on all matters concerning human resources. The J1/G1's involvement in the battlefield TECHINT effort is a result of their primary staff responsibilities for—

- Planning and handling EPW evacuation and processing. The prisoner evacuation channel is one of the richest sources of CEM. All J1/G1 annexes to OPORDs and operations plans (OPLANs) need to state that all CEE will be inspected by TECHINT personnel, and/or be transported to the Corps Captured Equipment Point by the transportation unit within the Corps.

- Directing the command surgeon in captured medical supply disposition and medical intelligence responsibilities.

- Coordinating with the J3/G3 to identify and assign special duty personnel such as JCMEC translators and SMEs.

ASSISTANT CHIEF OF STAFF, J2/G2, INTELLIGENCE

The J2/G2 is the principal staff section for the commander on all intelligence matters and, as such, has primary responsibility for the command's battlefield TECHINT effort. The J2/G2's primary battlefield TECHINT responsibilities include, but are not limited to—

- Providing staff supervision over captured and detained persons with S&T expertise and exploiting CEM.
- Supervising battlefield TECHINT planning, directing, processing, producing, and disseminating.
- Exercising staff supervision over the JCMEC or attached battlefield TECHINT team operations.
- Coordinating battlefield TECHINT collection tasking, with the J3/G3, MI, EOD, NBC, and other combat and combat support units.
- Coordinating with the JCMEC to provide instructions to units capturing enemy materiel, captured medical materiel exploitation, evacuation, and disposition with the command surgeon.
- Coordinating CEM evacuation with the J4/G4. This includes coordinating transportation priorities, disposition, and opportunities to screen CEM in logistic channels.

- Coordinating with the J5/G5 the TECHINT screening of materiel obtained from local nationals, displaced persons, and civilian detainees.

- Coordinating with the staff judge advocate (SJA) to ensure compliance with the Geneva Conventions regarding exploitation of captured personnel and materiel. Ensure that the SJA includes instructions on CEM in the legal annex to OPORDs and OPLANs regarding war trophies and souvenirs.

- Coordinating with the military historical officer to ensure all items of possible historical value are initially screened for TECHINT value.

ASSISTANT CHIEF OF STAFF, J3/G3, OPERATIONS

The J3/G3 is the principal staff section for the commander in matters concerning operations, plans, organization, and training. The J3/G3's involvement in the battlefield TECHINT effort is a result of their primary staff responsibilities. As they relate to battlefield TECHINT, these responsibilities include—

- Coordinating terrain management and clearance or movement issues for TECHINT teams to move about the battlefield as missions dictate.

- Exercising primary staff responsibility over the supporting aviation, chemical, engineer, fire support coordination officers, and the provost marshal (PM).

- Preparing, coordinating, and publishing the command standing operating procedures (SOPs), OPLANs, and OPORDs. This includes instructions for handling CEM, such as collection, reporting, exploitation, evacuation, and disposition.

- Reviewing subordinate command SOPs, OPLANs, and OPORDs to ensure provisions for battlefield TECHINT are included.

- Incorporating TECHINT into current and future operations and plans.

- Assigning, attaching, and detaching battlefield TECHINT assets to subordinate and adjacent commands.

- Advising the commander on friendly use of CEM. This includes to whom the materiel should be allocated, such as irregular or other local national forces.

- Training US troops in the safe disposition and use of CEM.

ASSISTANT CHIEF OF STAFF, J4/G4, LOGISTICS

The J4/G4 is the principal staff section for the commander in matters concerning supply, maintenance, transportation, and services. As the logistical planner, the J4/G4 conducts vital coordination for the TECHINT system. This includes—

- Exercising primary staff responsibility over the EOD officer and the transportation officer.
- Coordinating with the Support Command Commander, who is responsible for logistical support operations; and the J3/G3 for support of battlefield TECHINT collection operations.
- Coordinating and developing command policy for the evacuation and disposition of CEM. Give particular attention to "back-haul" transportation plans for CEM.
- Ensuring that the Service Support Annex to the OPORD has an appendix that addresses CEM.
- Recommending to the J3/G3 the MSR and the main evacuation route of EPWs and CEM.
- Supervising the establishment and the operation of CEM collection points in the unit support area, normally near the Class VII collection point.
- Coordinating the setup and support of the JCMEC and CMEC (Forward) at the Corps collection points.
- Ensuring inventory and storage location records are properly maintained and are reported through materiel management centers (MMC) and TECHINT or JCMEC channels.
- Recommending policies and procedures for the use of captured nonintelligence-value equipment and providing technical staff assistance to the command's MI unit.

ASSISTANT CHIEF OF STAFF, J5/G5, CIVIL AFFAIRS

The J5/G5 is the commander's principal staff officer in all matters

concerning civilians and their impact on military operations. This includes the political, economic, and social effects of military operations on civilian personnel. The J5/G5's involvement in the battlefield TECHINT effort is a result of their primary coordinating staff responsibilities for civilian liaison and Civil Affairs (CA). These responsibilities include—

- Supervising CA functions of the command regarding care and handling of displaced persons, refugees, and any incidental foreign S&T materiel CA personnel may secure.
- Ensuring inclusion of TECHINT collection and notification procedures in all CA SOPs, OPLANs, and OPORDs.
- Coordinating with the command's battlefield TECHINT unit for the screening, exploitation, and evacuation of any CA-secured CEM.
- Coordinating with the J2/G2 and J4/G4 for the return of CEM to the civilian populace.

SPECIAL STAFF OFFICERS

Because TECHINT covers such a broad spectrum of disciplines, activities, and operations performed on the battlefield, the following special staff officers also play an important role in battlefield TECHINT.

AVIATION OFFICER:

- Coordinates with staff movement and transportation personnel for air evacuations of CEM and chemical and biological (CB) samples.

CHEMICAL OFFICER:

- Advises the commander on NBC intelligence matters.
- Recommends employment of chemical troops in support of battlefield TECHINT teams, analysis, and collection operations.
- Plays a key role in the success of the CB sampling mission; ensures that the mission is explained in the chemical Annex of the OPORD.

ENGINEER OFFICER:

- Plans and constructs engineering requirements.
- Incorporates battlefield TECHINT analyses and studies regarding

mobility and survivability characteristics of enemy weapon systems into these OPLANs and OPORDs.

- Provides construction support to JCMEC activities.

EXPLOSIVE ORDNANCE DISPOSAL OFFICER:

- Establishes, operates, and supervises EOD-related TECHINT reporting procedures; includes these reporting procedures in the EOD portion of the OPLAN.

- Coordinates with EOD TECHINT personnel at the JTIB, JCMEC, and TECHINT collection teams for dissemination of EOD TECHINT information.

PROVOST MARSHAL:

- Provides security for designated units, facilities, and convoys, including CEM, along the evacuation route and for TECHINT facilities when tasked by the J3/G3.

- Coordinates with customs for the TECHINT screening of all CEM found at US redeployment or staging sites.

- Establishes procedures to ensure military police confiscate, tag, report, and turn over to TECHINT personnel new or unidentified CEM discovered incidental to EPW handling operations.

THEATER AND SUPPORTING COMMAND SURGEON:

- Uses TECHINT when advising the commander on medical effects of NBC weapons on personnel.

- Coordinates with the theater chemical officer to implement CB sampling procedures.

- Includes CB sampling procedures in the medical portion of the OPLAN.

- Coordinates TECHINT support to examine and process captured medical supplies and equipment; this includes planning and coordinating medical laboratories and personnel to assist in sample analyses.

- Recommends medically related TECHINT PIR and IR to the J2/G2.

- Coordinates the analysis of biological warfare agent specimens collected on the battlefield at the theater medical laboratory.

Coordinates with the J2/G2 and J3/G3 and provides countermeasures, quarantine recommendations, and other appropriate actions to safeguard friendly forces.

AMMUNITION OFFICER:

- Establishes policies for the safe storage and accountability of foreign munitions; also is responsible for the safety certification of foreign munitions designated for reissue to friendly troops.

STAFF JUDGE ADVOCATE:

- Coordinates the Theater war souvenir policy with the JCMEC Commander, JTIB, and the J2. This policy is determined by the deploying commander, based upon recommendations from JAG, G4, and TECHINT procedures.

- Advises on legal matters concerning the movement of CEM out of the Theater.

UNITS AND ORGANIZATIONS

This section describes the responsibilities and duties of specific organizations and units on the battlefield that support TECHINT operations.

JOINT CAPTURED MATERIEL EXPLOITATION CENTER:

The JCMEC's primary function is processing CEM into combat information and TECHINT. The JCMEC is organized around the 203d MI Battalion. When it is further augmented by experts from other nations, it becomes a CJCMEC. Regardless of the command or echelon it supports, it has the same capabilities. The JCMEC—

- Exploits CEE, CED, and CEM.

- Produces TECHINT reports, that include countermeasures, for tactical commanders.

- Provides studies, OPLANs, OPORDs, maps, and special reports to disseminate the JCMEC findings.

- Provides RSPs to combat units for found enemy weapons and enemy munitions, with coordination through joint EOD.

- Coordinates the safe handling and evacuation of CEM with EOD elements.

- Coordinates evacuation of special-interest CEM from ECB locations to JCMEC.
- Supervises evacuation of CEM from theater to CONUS.
- Coordinates with the joint interrogation facility the selection of EPWs for TECHINT exploitation. Supplies interrogators with TECHINT requirements for EPW interrogation.
- Provides accountability for CEM within the theater TECHINT structure.
- Recommends CEM disposition to the Theater and Corps commands.
- Maintains the theater TECHINT database.
- Maintains S&TI and battlefield PIR, IR, and list of special interest items.

CAPTURING UNITS:

Combat units are usually the first to encounter new or modified threat materiel. However, other units such as engineers, military police, NBC teams, and logistic units may also encounter or capture such materiel. This materiel often comes with operating instructions and other technical documents. The intelligence officer at each echelon coordinates with J2/G2/S2 regarding TECHINT and captured or encountered threat materiel and documents. Together, they establish unit security, RSPs, reporting, and dissemination procedures for CEM.

Capturing units must strive not to destroy TECHINT materiel known or believed to answer PIR, IR, special interest lists, or unidentified or new items before receiving disposition instructions. CEM and logistics complexes must be safeguarded and reported through intelligence channels. Captured items known or believed to answer TECHINT requirements are reported via SALUTE format to higher command normally to the Corps TECHINT LNE.

MILITARY INTELLIGENCE UNITS:

The attachments of TECHINT teams less operational control (OPCON) to MI units (for example, one TECHINT team per corps MI brigade) enhances TECHINT operations, as well as improves coordination and synergy among all MI disciplines. MI units are normally best able to provide administrative and logistical support to forward deployed TECHINT teams due to like missions and collocation.

All MI units are responsible for establishing SOPs and having procedures for handling, screening, and reporting TECHINT-related items or

information encountered incidental to normal organizational activities. The following items relate to enemy C-E systems:

- Code books.
- Frequency tables.
- C-E operations instructions.
- C-E standing instructions.
- Cryptographic data.
- Cryptographic items.
- Encrypted items.
- C-E hardware or software.
- Examples of materiel, including CEE and CED, requiring immediate MI screening.

SPECIAL OPERATIONS FORCES:

Special Operations Forces consist of special forces and ranger units, special operations aviation units, psychological operations (PSYOP) teams, and CA elements.

Special Forces and Ranger Units. These forces usually operate deep in enemy-controlled areas. This means they are generally the first to discover, identify, and provide information on a variety of TECHINT-related CEE, CEDs, or facilities. They can provide—

- New or previously unacquired materiel.
- Locations of enemy materiel.
- Other technical data.
- Capture of enemy S&T personnel.

***Special Operations Aviation Units*.** Special operations aviation units provide aviation support to units conducting special operations missions usually deep within enemy-controlled areas. These units can provide technical data on enemy radars, as well as on observed enemy equipment. Incidental to assigned air missions, special operations aviation units can often "back-haul" limited amounts of priority CEM to rear areas.

Psychological Operations Teams. PSYOP personnel support theater, corps, and division. Historically, PSYOP has supported TECHINT collection through creative PSYOP designed to secure TECHINT-related CEM, information, and/or personnel.

An example of a PSYOP success comes from the Korean War. A North Korean pilot was paid a $100,000 bounty for flying his Soviet MiG-15 to the south, after the bounty was offered by leaflet and radio. The benefits were enormous. The Communists grounded all MiG flights for eight days; and getting the MiG turned out to be a TECHINT windfall.

PSYOP specifically designed to provide TECHINT occurred during the Vietnam War. A PSYOP campaign encouraged enemy soldiers to surrender with their weapons and equipment intact; rewards were offered and paid to Viet Cong and NVA troops who did this. This type of campaign not only reduced the number of weapons available to the enemy but also provided a continuous source of materiel for the CMEC to exploit.

Civil Affairs Elements. These elements provide support to tactical and operational commanders by coordinating between military forces, civil authorities, and area of operations personnel. CA support to the battlefield TECHINT process includes—

- Providing SMEs to assist in the TECHINT analysis of food and agriculture; public communications, health, transportation, and supply; public works and utilities; and centers of commerce and industry.

- Securing TECHINT-related materiel and foreign experts having CA wartime responsibility for civil administration and refugee handling.

ENGINEER TOPOGRAPHIC AND TERRAIN UNITS:

These units are responsible for collecting, evaluating, and disseminating topographic information and terrain intelligence. They normally function at theater, corps, and division levels. TECHINT units use engineer topographic and terrain products to support TECHINT collection planning. Engineers also support analysis and exploitation of CEM and facilities when this materiel is within their field of expertise.

MILITARY POLICE:

The military police fulfill a wide range of duties on the battlefield, to include providing route security for evacuating CEM and handling EPWs. In performance of these duties they often confiscate CEM from EPWs. Military police follow specific procedures for notifying MI personnel of equipment or documents of intelligence interest discovered incidental to EPW handling operations.

If not done previously, military police mark or tag all CEM and personnel in their custody. Since EPWs and materiel may become separated, military police use a three-part capture tag to clearly identify which prisoner the CEM came from. Accurate identification of the capture tag helps TECHINT analysts and interrogators match materiel with associated EPWs. It also makes it easier to return certain property to the EPW. (See Appendix C for an example of an EPW capture tag.)

NBC RECONNAISSANCE TEAMS:

NBC reconnaissance teams locate, identify, and mark contaminated areas. They collect, identify, and evacuate suspected samples of nuclear materials and CB warfare agents. This function is an important supplement to normal TECHINT collection capabilities. Collecting, handling, storing, and shipping these samples must be done using SOPs developed in a coordinated effort between the command surgeon, the staff NBC officer, and the staff S2. All parties involved must ensure they maintain a legal chain of custody of NBC samples for later possible war crimes processing.

MEDICAL UNITS:

Combat zone and communications zone medical support units are capable of giving specialized medical, laboratory, and medical intelligence assistance to TECHINT and other MI disciplines. The medical unit's S2 coordinates this assistance to MI units.

EXPLOSIVE ORDNANCE DISPOSAL:

One of the most critical and early sources of TECHINT on the battlefield is explosive ordnance. To safely exploit this source, EOD units provide specially trained personnel to support TECHINT collection teams and units in the area of operations. EOD personnel examine existing databases and prepare reports on new and unusual items of explosive ordnance for TECHINT purposes.

TECHINT personnel should be familiar with EOD activities, capabilities, and responsibilities, as described in AR 75-15. Foreign explosive ordnance is extremely important to TECHINT analysts. TECHINT personnel coordinate closely with EOD personnel for proper disposal and evacuation of explosive ordnance, particularly when conducting initial inspections during hasty exploitations of CEM on the battlefield.

DANGER

Exercise extreme care and awareness when encountering possible booby-trapped CEM. Materiel may be booby trapped and cause immediate death or permanent injury.

Only EOD personnel actually handle explosive ordnance. Conversely, EOD units must notify TECHINT personnel of the types and locations of foreign equipment and munitions they encounter.

Appendix A

MEASUREMENT AND SIGNATURE INTELLIGENCE

INTRODUCTION

This appendix describes the MASINT mission, organization, responsibilities, and their relevance to TECHINT. Specific definitions are in the glossary. This appendix delineates MASINT's dual mission of supporting the S&TI community as well as providing unique time-critical information to the supported tactical commander that contributes to battlespace dominance.

MISSION

PEACETIME:

The mission of MASINT operations in peacetime includes fulfillment of intelligence collection and transition to war requirements. Army MASINT efforts are focused at EAC MI force at the force projection brigades. Technical reconnaissance and surveillance (TECRAS) systems fielded at EAC demonstrate the feasibility of MASINT support at that level.

Successful demonstration is expected to lead to the development of tactical intelligence and related activities (TIARA) systems and their progressive fielding at appropriate EAC and ECB units. EAC conducts operations to fulfill collection requirements levied by the Army component command, theater, DOD, or national levels. The force projection brigade's mission includes the collection of S&TI to support baseline signature requirements for reprogrammable munitions in support of Army, DOD, and national requirements.

WARTIME:

In addition to its contributions to S&TI, MASINT also serves the warfighting commander. MASINT collection of threat battlefield equipment signatures aids in the prevention of technological surprise and is critical to US ability to produce effective countermeasures. Continued signature collection by MASINT sensors permits reprogramming of precision-guided, smart, or brilliant munitions. Specific MASINT missions are to—

- Detect, identify, and locate targets with sufficient timeliness and accuracy for operational planning, targeting, and combat action.

- Support IPB.
- Support force protection via identification, friend or foe (IFF) systems.
- Support terrain visualization and geographic intelligence.
- Provide intelligence on threat signatures and equipment and technological advances not discernible by other intelligence collection means.
- Support indications and warnings (I&W) intelligence in peacetime and provide an indication of threat escalation from conventional to nuclear war.
- Provide intelligence to support the commanders' demands for situation development, target development, battle damage assessment (BDA), and intelligence operations in close, deep, and rear operations.
- Provide information to detect or confirm enemy deception operations.
- Provide information of threat strategic facilities, such as power plants, design bureaus, production facilities, proving grounds, and test areas.
- Provide commanders with information of friendly signature profiles. This information will be used for IFF to minimize fratricide and to alter signatures for operations security (OPSEC) or friendly deception operations.

ORGANIZATION

The Army’s MASINT organization is shown at Figure 2-1.

RESPONSIBILITIES

Figure A-1 shows the responsible agencies, along with their MASINT functions.

AGENCY	RESPONSIBILITY

DIA, Central MASINT Office	Executive agent for MASINT.
HQDA, DCSINT	Functional manager of TECRAS Program.
AMC, DCSINT	Materiel developer.
INSCOM, DCSOPS	Manages and oversees operational MASINT EAC collection operations. Develops operational requirements documents and mission needs statements.
NGIC, Signatures Division	Primary consumer of TECRAS data.
Force Projection Brigades	Ensure national MASINT sensors are tasked to support commander's PIR. Serve as focal point for collection management and dissemination for MASINT. Collect baseline signatures in support of the TECRAS Program. Augment the Theater IPC upon request. Act as the conduit for fielding selected RDTE MASINT systems.

Figure A-1. HQDA agencies and their MASINT responsibilities.

DEFINITIONS

The definitions for MASINT and electro-optical intelligence (ELECTRO-OPTINT), as defined in JCS Publication 1-02, are shown in the terms and definitions section of the glossary.

ELECTRO-OPTINT:

ELECTRO-OPTINT may provide detailed information on the radiant intensities, dynamic motion, spectral and spatial characteristics, and the materials composition of the targeted objective. Electro-optical data collected has broad applications to a variety of tasks. Data may be collected by a variety of optically sensitive devices, such as radiometers, spectrometers, non-literal imaging systems, lasers or laser radar—laser detection and ranging (LIDAR).

RADAR INTELLIGENCE (RADINT):

RADINT is the collection, processing, analysis, and exploitation of radar energy reflected (re-radiated) from a target or objective. Instruments for active target illuminations may include monostatic or bistatic, line-of-sight (LOS) phased array, synthetic aperture radar (SAR), and over-the-horizon systems. RADINT collection provides information on radar cross-sections, tracking, precise spatial measurements of components, motion, and radar reflectance and absorption characteristics for dynamic targets and objectives.

RADIO FREQUENCY INTELLIGENCE:

This includes radio frequency/electromagnetic pulse intelligence (RF/EMPINT) and unintentional radiation intelligence (RINT).

- RF/EMPINT is the collection, processing, analysis, and exploitation of radio frequency electromagnetic pulse emissions associated with nuclear testing or other high energy events for the purpose of determining power levels, operating characteristics, and signatures of advanced technologic weapons, power, or propulsion systems.

- RINT is the integration and specialized application of multiple MASINT collection, processing, analysis, and exploitation techniques against unintentional radiation sources that are incidental to the design and operating characteristics of military and civil propulsion units, power sources, weapons systems, electronic systems, machinery, equipment, or instruments. These techniques may be valuable in detecting, tracking, and monitoring a variety of activities of interest.

GEOPHYSICAL INTELLIGENCE:

This is the collection, processing, exploitation, and analysis of emitted or reflected sounds, pressure waves, or vibration in the atmosphere (acoustic), in the water (acoustical intelligence), or in the earth's surface (seismic). Acoustic and seismic sensors may be valuable in target detection and classification, measuring aircraft and ship performance characteristics, detecting weapons testing and large military movements.

MATERIALS INTELLIGENCE:

This is the physical collection, processing, analysis, and exploitation of atmospheric trace elements; gaseous, liquid, or solid particulate; effluents; or debris. Materials intelligence has specific applications to NBC warfare, military and civil production, and economic and environmental problems.

NUCLEAR INTELLIGENCE (NUCINT):

NUCINT is intelligence information derived from the collection and analysis of radiation and other effects resulting from radioactive sources, such as nuclear weapons, processes, materials, devices, or facilities. Nuclear monitoring includes nuclear radiation detection, identification, and characterization of sources and events. Data exploitation results in nuclear signature of weapons or materials.

TECHNICAL RECONNAISSANCE AND SURVEILLANCE:

TECRAS is DA's special program using a low density of instrumented collection sensors which provide a quick-reaction capability for collection.

ARMY REPROGRAMMING ANALYSIS TEAM (ARAT):

The ARAT is involved in altered signatures identification and associated weapon systems impact. The US Army target sensing systems (TSSs) incorporate software algorithms used to make threat identification based on embedded preprogrammed threat parameter data.

As the threat capabilities change, or as new threats become operational, there is a risk that these systems will not correctly identify the threats. To the extent the threat is misidentified, incorrect countermeasures may be implemented putting friendly forces at risk.

Reprogramming the weapon systems provides the commander an essential element in battle space dominance by allowing him to defeat enemy countermeasures. The production centers and the intermediate processing centers (IPCs) validate suspected change signatures or countermeasures. The ARAT receives data upon which the threat change is identified and system assessments made. The ARAT determines impact of validated threat changes on assigned Army equipment and weapon systems and develops a suitable and achievable counter to the changes. The mission requirements center (MRC) within the systems manager’s organization determines requirements for Army systems. The software support center (SSC) is responsible for developing the change program and validating the change.

CONCLUSIONS

MASINT’s chief contribution to the Army to date has been support to force modernization, a role which is likely to continue. However, it is also an evolving discipline which holds significant potential for warfighting intelligence as adversaries develop means to deceive or evade imagery

and signals sensors.

Much can be gained by integrating MASINT and TECHINT. The disciplines are not competing but complementary. Many MASINT technologies and subdisciplines lend themselves towards bringing traditional TECHINT into the information age. Sensors are used to derive information in NRT, so that it can be fed to the supported commander in time to effect the decision cycle.

Appendix B

JCMEC OPERATIONS

This appendix provides an overview of JCMEC operations and responsibilities; it is used as an example for an annex to a combatant command's TTP document. Each reference to the "supported Theater Commander" may be replaced by the appropriate unified or joint combatant command acronym (for example, ACOM, PACOM, CENTCOM).

INTRODUCTION

The JCMEC (in part or whole) normally will be established for any operation where significant amounts or types of CEM will be available and/or require field exploitation. The supported Theater commander has the mission of establishing and operating a JCMEC through the 203d MI Battalion (TECHINT), FPB, and provides for the day-to-day operation of the JCMEC to include administration, logistics, systems, communications, and maintenance.

The supported Theater commander also has staff responsibility for—

- Ensuring security of the materiel.
- Arranging for the evacuation and movement of CEM.
- Providing legal guidance concerning disposition of certain CEM, structures, and facilities.
- Coordinating for EOD.
- Coordinating the issue of CEM to US forces.

The Theater J2 exercises operational control of the JCMEC through the JTIB located at the JIC. The JTIB consists of the senior TECHINT representatives from DIA's Technical Directorate and Service TECHINT organizations (National Ground, Air, and Maritime Intelligence Centers as needed). The JTIB will be augmented with an LNE from the 203d MI Battalion (TECHINT).

The purpose of a JCMEC is to provide a central in-theater location for the collection, safeguarding, identification, battlefield exploitation and

reporting, and destruction and/or evacuation of specified captured foreign and US manufactured materiel. The JTIB—

- Provides TECHINT advice and assistance to the Theater J2.
- Acts as the TECHINT collection manager for the Theater J2.

CONCEPT

The JCMEC will be sited by the supported Theater commander. The site should facilitate evacuating, storing, and shipping CEM. The JCMEC also will—

- Locate to facilitate security.
- Ensure safety for nearby forces and the local populace.
- Provide easy access to communications, transportation, and other support facilities.
- Locate near the Theater ordnance storage site.

JCMEC facilities have common site selection criteria and complementary functions which provide efficient allocation of assets for evacuation, movement, safeguarding, and exploitation of EPWs and CEM.

JCMEC will be staffed by the 203d MI Battalion (TECHINT) and augmented by selected service technical representatives and support personnel. Through the supported Theater commander, the JCMEC will have support from military police or security forces, ground and aviation transportation elements, EOD, and other activities as needed.

In accordance with DOD directives, service regulations, and other established policies, all units will collect, identify, tag, secure, and evacuate CEM to designated collection points.

In coordination with the JCMEC, and through technical teams and liaisons, Corps and equivalent units will transport or arrange for the transportation of selected items to the JCMEC. In cases of the reported capture of designated CEM of high TECHINT priority and/or time sensitivity, a TECHINT collection team will be deployed to the capture site to conduct initial exploitation and then coordinate and prepare the materiel for hasty evacuation directly to the JCMEC.

JCMEC will function as the Theater's central captured materiel exploitation facility. As such it will—

- Establish procedures for the exploitation, destruction, or other

disposition of CEM in coordination with the J4.

- Recommend the theater souvenir and war trophy policy, to include demilitarization procedures.
- Issue and provide training on the operation of CEM to US forces, allied, and host nation forces based upon J3 requirements and priorities.
- Return specified CEM to the sovereign nation at the end of the conflict as directed.

ORGANIZATION

The JCMEC and its components can and will be tailored for each operation depending on types and quantities of CEM. Although operationally responsible through the supported Theater commander for the JCMEC, the commander and deputy are responsible to the J2 through the JTIB for intelligence collection management and oversight of the JCMEC. Figure B-1 shows the JCMEC organization. Following are specific functions of the JCMEC components.

COMMANDER AND THE DEPUTY:

The 203d MI Battalion (TECHINT) commander is dual hatted also as the JCMEC commander and is assisted by a deputy, battalion S3, or Executive Officer (XO). The commander will tailor the CMECs to meet the worldwide mission.

LIAISON ELEMENTS:

FME LNEs will be attached to each component G2, Air Force and Navy Intelligence, and Corps, or the equivalent subordinate command. These LNEs will advise the supported command on CEM handling, control, and evacuation procedures and coordinate these efforts with the JCMEC.

OPERATIONS CENTER (OPCEN):

The OPCEN director works directly for the JCMEC commander. The OPCEN is responsible for planning and coordinating all current and projected JCMEC operations, to include deploying TECHINT collection teams and maintaining the current intelligence situation.

SUPPORT CENTER (SUPCEN):

The SUPCEN director works directly for the JCMEC commander. The SUPCEN provides administrative and logistics support to all JCMEC elements.

The warehouse section chief works directly for the SUPCEN director. This section maintains all records on CEM, structures, and facilities that are processed through or by the JCMEC. Specifically, the Warehouse Section—

- Serves as the point of contact (POC) for the various units or organizations delivering and/or transferring materiel.

- Ensures that documents, manuals, inventory records, and other related items are cataloged and properly exploited.

- Ensures exploitation elements are informed of materiel and documents received at the JCMEC.

- Coordinates and monitors the shipping of materiel to CONUS and/or issuance to US forces, allies, or host nation as directed.

EXPLOITATION CENTER (EXCEN):

The EXCEN director works directly for the JCMEC commander. The EXCEN director prioritizes, coordinates, and deconflicts the efforts of his subordinate elements based on the JCMEC commander's guidance. Elements subordinate to the EXCEN director and their functions are as follows:

- Ground Exploitation Element. This element processes validated requirements; exploits captured ground materiel (to include helicopters and ground-based missile systems); produces tactical TECHINT reports; ensures that reports are forwarded to the CM&D section expeditiously; and participates in technical interrogations in coordination with the joint interrogation facility.

- Air and Missile Exploitation Element. The structure and functions are the same as for the Ground Exploitation Element except that the focus is on aviation (aircraft, air delivered weapons systems, and associated radar and tracking systems) and missile-related materiel.

- Maritime Exploitation Element. The structure and function are the same as the Ground Exploitation Element except that the focus is on naval and marine materiel (to include naval mines, vessels, naval aviation, and naval-related missile systems).

- Medical and NBC Exploitation Element. This element's function, in addition to exploitation and reporting on NBC weapons and materiel, is to be responsible for removal and shipment of samples from the area of operation. This element will ship suspected samples to the Theater Army Medical Laboratory (TAML), if available, or to CONUS- based laboratories for analysis.

- C-E and IEW Exploitation Element. This element focuses on

communications, computers, intelligence and electronic warfare (IEW), and related systems.

- CM&D Element. The collection management and dissemination (CM&D) element provides a single POC to ensure that effective coordination is maintained between the JCMEC and the numerous component, theater, national, allied, and host government units. This element will ensure the receipt and satisfaction of all requirements. Specific functions are as follows:

  — Operate joint and Army automated file servers and associated work stations that are used for receiving requirements and disseminating technical reports. Figure B-2 shows the TECHINT communications architecture.

  — Coordinate directly with the J2 TECHINT collection manager for receipt of validated requirements (collection and production). Ensure that exploitation elements receive these requirements; monitor the status of the requirements; and close them when appropriate.

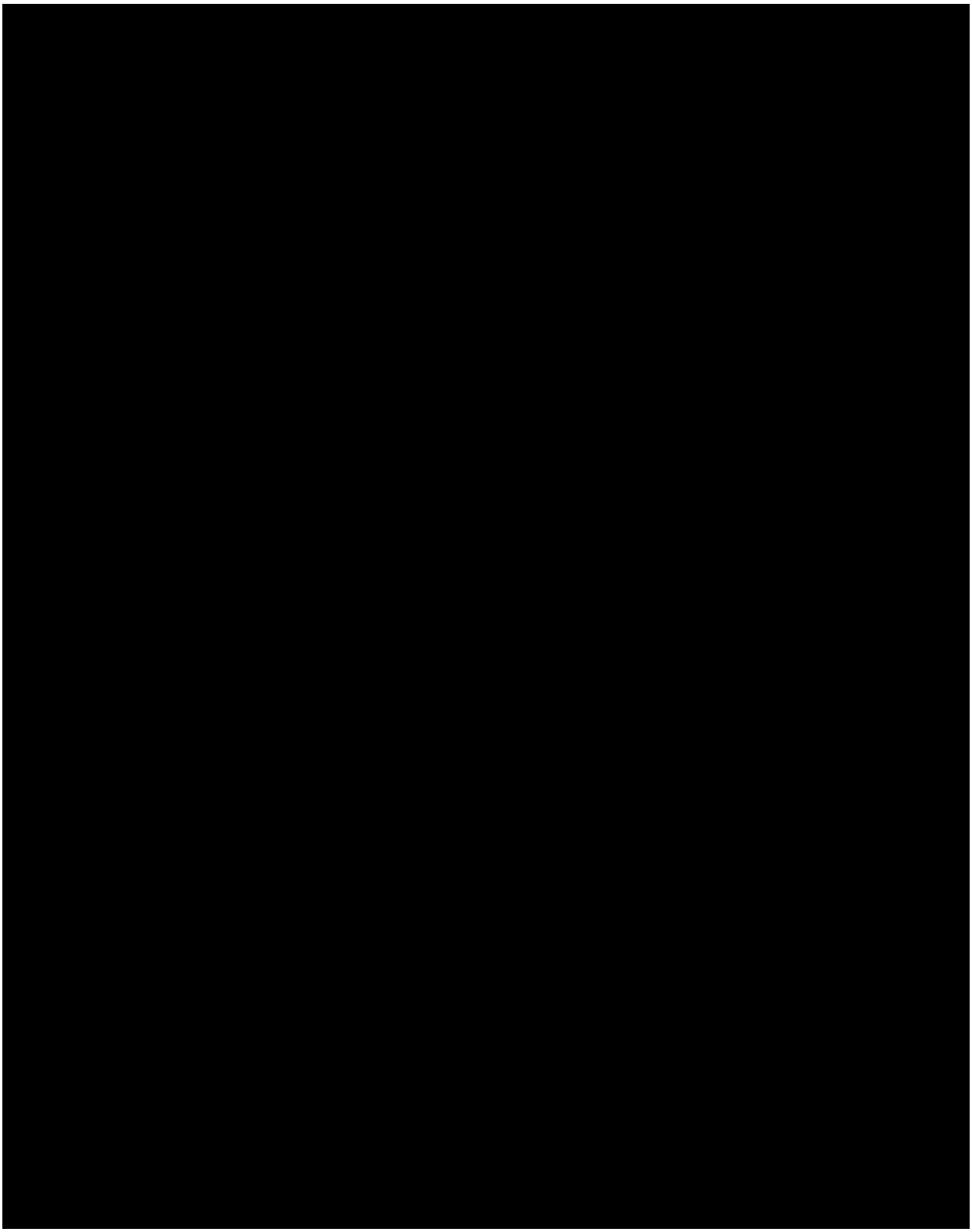
  — Take reports from the elements and ensure that they are disseminated expeditiously to units and organizations that need the information. Dissemination can be by any or all means; for example, secure voice, facsimile, message, Joint Deployable Intelligence Support System (JDISS). Information should be given the widest dissemination possible.

SIGNAL CENTER (SIGCEN):

The SIGCEN director works directly for the JCMEC commander. The SIGCEN provides communications, systems, and related maintenance support to all of the JCMEC elements. It acts as the focal point for all communications in and out of the JCMEC.

COLLECTION COMPANY:

The commander of the TECHINT Collection Company works directly for the JCMEC commander. This company is augmented by a Joint EOD detachment and forward deploys three TECHINT collection teams. The collection teams assist in recovering, processing, tagging, and shipping materiel to the JCMEC. They also perform screening and make field assessments of "first seen" materiel encountered by US personnel. The EOD detachment consists of personnel from the Services who are familiar with weapons systems, ammunition, and ordnance related to their



respective areas. This detachment works for the TECHINT Collection Company commander but provides EOD support to all JCMEC elements.

SPECIAL ACTIVITIES:

There will be times and places where other US, allied, or host nation government agencies, organizations, or elements may be required to support the foreign materiel efforts of the JCMEC.

COMMUNICATIONS

The supported commander provides communications for the JCMEC. The J2/G2 validates all requirements and coordinates with the J6 to ensure that the required bandwidth and types of circuits are provided.

Normal JCMEC operations will require the following minimum intelligence processors and connective communications capabilities:

- JDISS and/or a compatible file server and workstations. This system is essential for access to databases, collection and production requirements processing, and dissemination. Since there will be a requirement for a Sensitive Compartmented Information Facility (SCIF), and split-based operations to and from Aberdeen Proving Ground, MD, both DSNET 1 and DSNET 3 connectivity with a minimum of 32 Kb bandwith will be essential.
- Disk operating system (DOS) stand-alone terminals for report writing and records administration.
- Automated message access.
- Dial-up STU-III secure telephone.
- Classified and unclassified facsimile.
- Other specialized communications as required to support the forward teams (such as tactical high frequency, ultra high frequency, super high frequency, and satellite communications [SATCOM]).

OTHER REQUIREMENTS

See DIAMs 58-4, 58-13, and 75-1 and references herein for procedures and requirements for identifying, safeguarding, controlling, and disposing of CEM.

Appendix C

HANDLING AND EVACUATION

INTRODUCTION

This appendix covers the procedures for handling and evacuating routine CEM, as well as TECHINT CEM. Some basic guidelines and procedures on how to handle TECHINT interest items follow:

- CEM evacuation channels and handling procedures are usually the same as similar US end items. A captured tank generally will go to the same location as a US tank at the Class VII point. (Definitions for classes of supply are in the glossary.)

- The element requiring a specific type item is responsible for coordinating and tasking evacuation and handling.

- As time permits, as much CEM should be collected from the battlefield and taken to the echelon's CEM points for disposition.

- The capturing unit always notifies higher command of capture and then safeguards the known or possible TECHINT item, if possible, until higher command provides disposition instructions.

- All echelons will establish CEM points and keep logistical and intelligence channels informed of their status.

- Special handling and evacuation procedures are often situation dependent and cannot always be included in SOPs and OPORDs.

The plans, policies, and procedures for evacuating foreign materiel are prescribed by joint, unified, and theater headquarters. These plans are based on DA and DOD policies and guidance. Each command echelon in theater must ensure that its plans comply with theater directives and the Joint TECHINT plan. The final disposition of CEM and associated technical documents rests with the theater commander.

As stated before, the CMEC is responsible for coordinating the handling and evacuation of CEM of TECHINT value. Routine CEM evacuation guidance, such as raw material found in railroad yards, is best established in advance in the command's various OPORDs and SOPs. CEM should be policed off the battlefield to the prescribed collection points as soon as possible. Special situations, as in the case of high priority TECHINT

interest items, require active coordination among the JCMEC and the command's different assets to move the item quickly.

Coordinating and tasking is the job of the echelon commander's staff for normal CEM movement. Their ability to coordinate between the logistic units that move the item and the specialist elements such as TECHINT, EOD, and NBC is the key to the reuse, intelligence exploitation, and removal of CEM.

LOGISTIC CHAIN OF RESPONSIBILITIES AND FUNCTIONS

Logistic assets will evacuate CEM to the collection points, Corps CMEC (Forward), theater CMEC, or CONUS. They do this according to available assets and the priorities set by the commander and staff. The J4/G4 is the principal staff element charged with coordinating this task. The command surgeon, responsible for medical items, coordinates disposition of Class VIII not of TECHINT value.

The J4/G4 provides staff guidance to the MMC and the movement control office (MCO) or the movement control center (MCC). The MMC controls combat service support (CSS) and maintenance inventories and is the management arm that ensures proper accountability of CEM during transit.

The support commands are the Division Support Command (DISCOM), COSCOM, and Theater Army Area Command (TAACOM). They exercise command and control over supporting units in carrying out the directives issued by the J4/G4. The division medical supply officer (DMSO) or the medical, supply, optical, and maintenance (MEDSOM) are the first elements that manage the command's collection, inventory, and evacuation procedures and functions for captured medical materiel.

The MMC manages the command's collection, inventory, and evacuation functions. This includes the operation of the CEM point. The MMC operations staff is organized by function and commodity, Class I through Class VII, and Class IX materiels. CEM will normally be managed by the Class VII operations staff. The MMC keeps the records of the CEM at the CEM point. TECHINT elements, such as the Corps CMEC (Forward) or TECHINT teams, would provide support to logistical personnel operating the CEM point for identification of CEM.

TRANSPORTATION PLANNING AND ALLOCATION

The J4/G4 coordinates logistic support for evacuation of CEM operations by developing a command transportation plan. The command transportation officer and the movement control element use the transportation plan to task individual transportation units. Transportation elements can be effectively used to backhaul CEM to the CEM points on their return trips from forward units. Transportation elements are tasked to support critical TECHINT missions when required.

EVACUATION CHANNELS

As stated in the introduction, US forces will usually evacuate CEM along the same channels as like US items. The system must, however, have the flexibility to evacuate high priority intelligence items directly from division collection points to the Theater CMEC and CONUS when required. This evacuation will be described in the logistical and intelligence appendixes to OPLANs. The routine evacuation channels are described below. Figures C-1 to C-4 provide examples of evacuation channels for CEM.

Abandoned or unserviceable US and captured foreign materiel are evacuated to each echelon's collection points for classification, segregation, and disposition. Collection points operate wherever needed throughout the theater of operations and should always be planned for ahead of time. In stability and support operations (SASO), it may take more time to evacuate larger items due to limited resources and environment.

In the Corps area, at least one materiel collection point is established. Other points are established in the TAACOM. Collection points in the communications zone (COMMZ) are generally operated by the collection and classification element of the general support maintenance battalion near the Class VII point.

In the division areas, DISCOM maintenance companies operate CEM points. During offensive operations, these points will be temporary until the Corps elements take control. CEM is handled and processed the same way as similar US items.

Salvage points, including Class VII, established by related supply units are located near unit maintenance collection points. These two points handle the collection, classification, inventory, and disposition of Classes II, VII, and IX materiel. The heavy division and Corps have the most

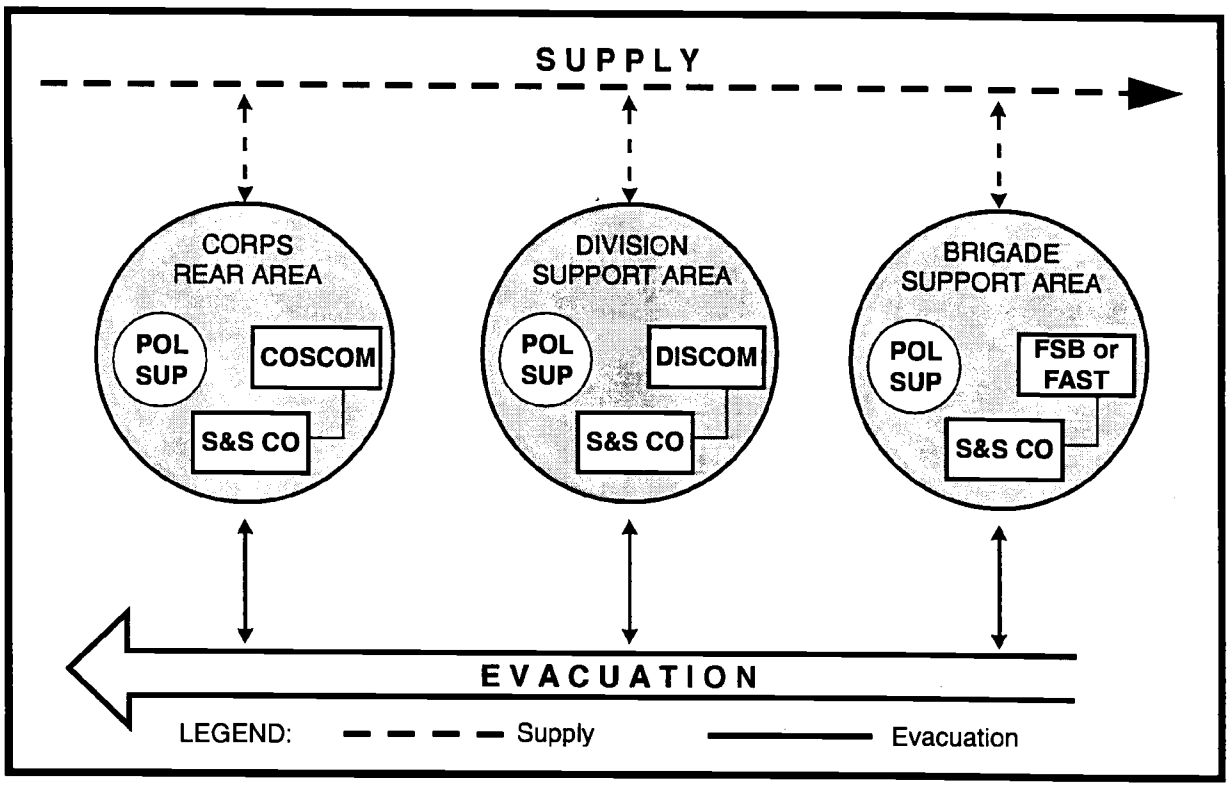


Figure C-1. Evacuation of captured petroleum, oils, and lubricants.

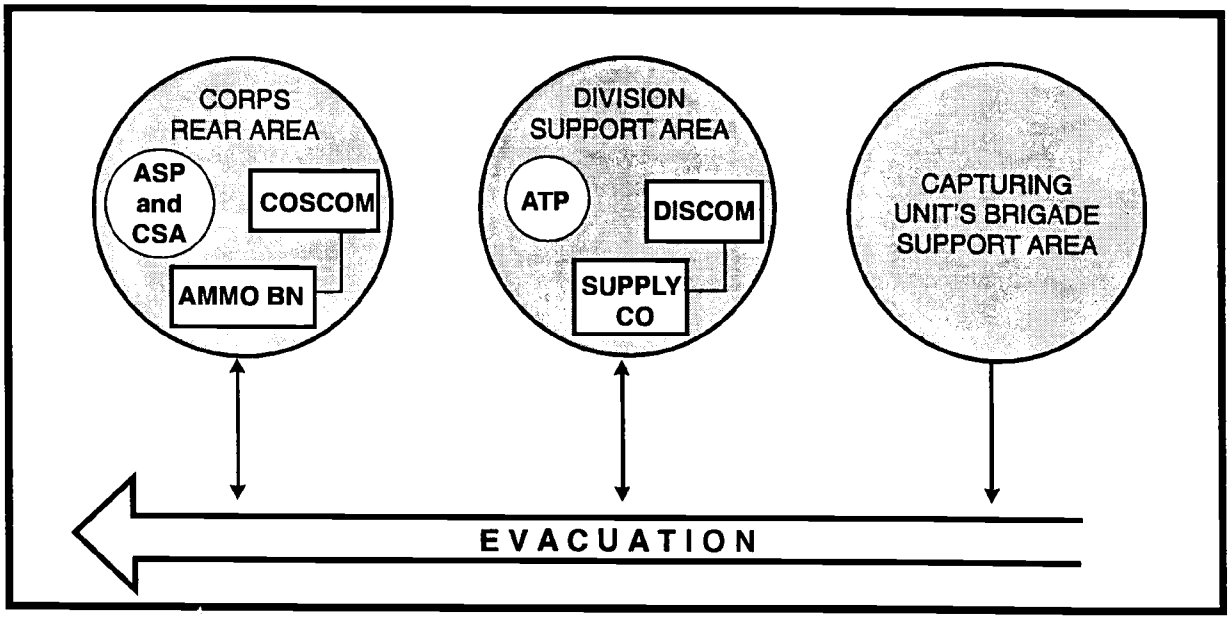
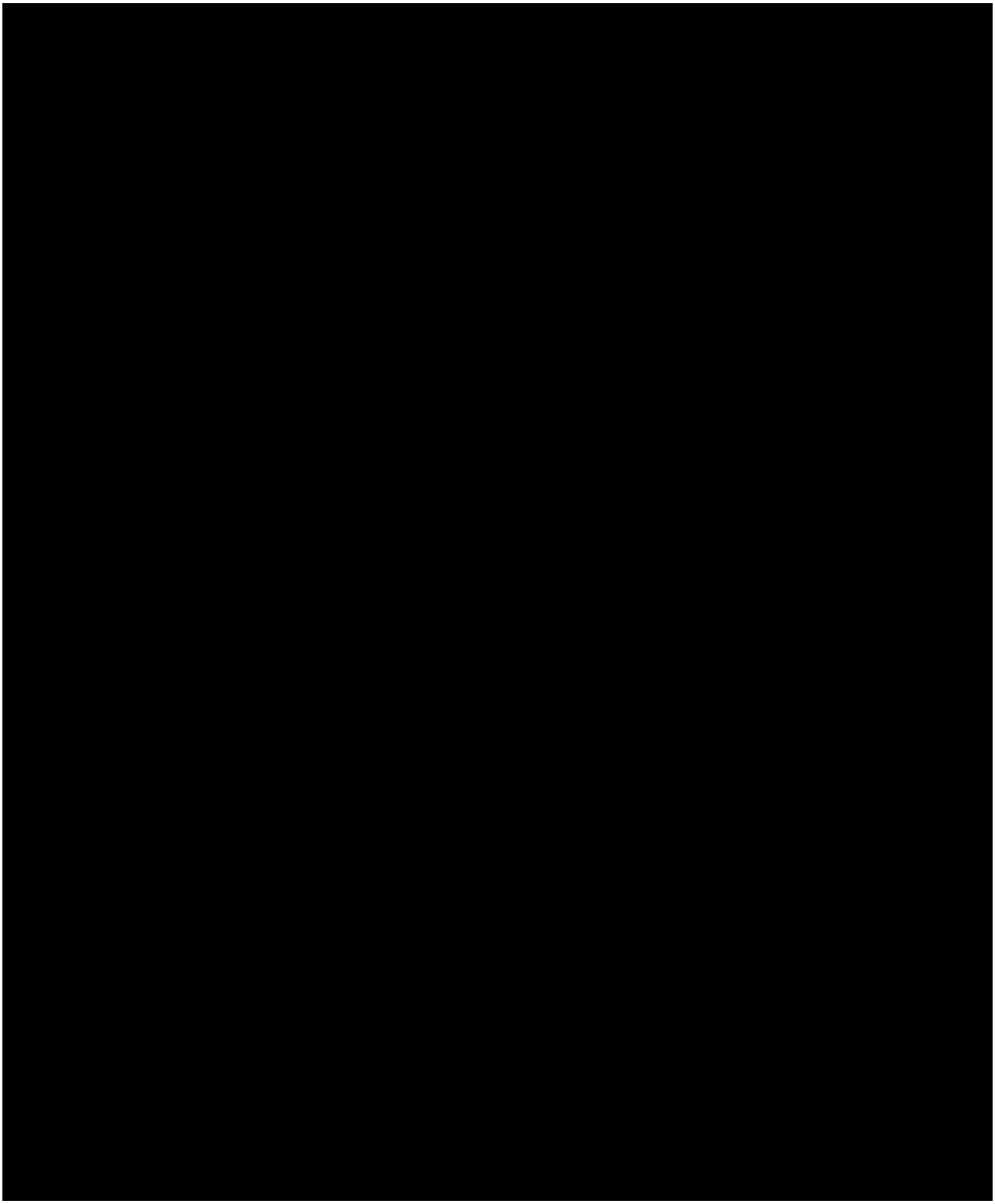


Figure C-2. Evacuation of captured ammunition and explosives.



suitable assets for evacuation of large amounts of foreign materiel, such as tanks. The process is much the same in the light divisions. However, evacuation of the heavier items will be normally handled by COSCOM assets since the division lacks heavy transportation elements.

Petroleum, oils, and lubricants (POL) units establish their own collection sites to handle captured POL materiel. Supply units can also establish POL collection sites. Commanders will test and use captured POL at the lowest echelon possible. Samples will always be taken and sent to the Corps CMEC or TECHINT collection teams.

Class V ordnance, including missiles, is evacuated through conventional ammunition supply points (ASPs). Ammunition supply units will establish their own collection sites to handle captured Class V. It is critical that the CEM ASPs provide a detailed inventory of ammunition to logistical and intelligence channels. TECHINT elements must move assets to the CEM ASP to assist in identifying ammunition of intelligence value.

Class VIII medical items are evacuated through established medical supply points, the DMSO, and the MEDSOM elements. TECHINT elements must have full access to the medical materiel to identify items of medical value.

Captured aviation items, especially airframes, are evacuated to either the Class VIII CEM collection points, or the nearest aviation units airfield. All CEM, except NBC hazardous materiel and war trophies, that require evacuation to CONUS are eventually shipped to the Transportation Officer, Military Operations Division, Aberdeen Proving Ground, MD.

RESPONSIBILITIES

The personnel, activities, and elements responsible for the recovery and evacuation of CEM are usually the same as those responsible for handling like US items. A good example is the military police responsibilities.

Since military police are responsible for controlling prisoners, they have similar evacuation responsibilities for EPW and CEM. MI interrogators and TECHINT analysts exploit these sources of intelligence along the evacuation chain.

THE CAPTURING UNIT

The capturing unit always is responsible for reporting, safeguarding, and initiating accountability of CEM. The capturing unit reports the capture with a SALUTE report (see Figure E-1). It safeguards the materiel, within its mission parameters, until relieved or as long as possible. It initiates accountability by marking and tagging the item according to established procedures.

The capturing unit may be tasked to move CEM wanted for intelligence exploitation to a collection point. If the capturing unit is tasked with evacuation, it coordinates any assistance with the command responsible for direct support maintenance at their echelon.

The capturing unit may be tasked with the destruction of the item. This may require coordination with either EOD or NBC assets to do it safely. It is illegal to destroy captured enemy medical materiel. According to the Laws of Land Warfare, if friendly forces cannot use it for EPWs, refugees, and indigenous population, the medical materiel will remain in place and unharmed.

The capturing unit must report the discovery of unusual mechanisms used as booby traps through intelligence channels to the nearest TECHINT element and EOD by SALUTE report. Countermeasures must be coordinated with EOD personnel. EOD personnel are responsible for the final disposition of explosive components or hazardous materials associated with such devices and recovered ammunition.

EXPLOSIVE ORDNANCE DISPOSAL

As discussed, TECHINT units have a profound interest in foreign explosive ordnance. The assistance of EOD personnel in the examination, movement, and evacuation of explosive ordnance cannot be overemphasized. All items of foreign ordnance should first be rendered safe by EOD personnel. If this is not feasible, the item should be rendered safe in place by any destructive method that minimizes damage to the item.

Collection of TECHINT data may require dismantling of ordnance and stripping fuses and other dangerous components. These operations will be performed only by experienced personnel. Dismantling and stripping are conducted only in response to a specific requirement for such action. The request must be placed through TECHINT and EOD staffs. Only

trained weapons and munitions specialists should analyze or test captured mines and booby traps.

DANGER
Exercise extreme caution when encountering taut wire, pull releases, or similar devices due to the possibility of immediate death or permanent injury.

NUCLEAR, BIOLOGICAL, AND CHEMICAL

All CB hazardous items are handled and shipped in accordance with command SOPs, national policy, and theater TECHINT plan. Evacuation is best handled after coordination with either an NBC reconnaissance team, NBC qualified TECHINT team, or a task-organized medical element. NBC samples, after theater tactical exploitation, will be shipped to CONUS laboratories.

TECHINT ELEMENTS ECB, EAC, AND THE CMEC

When evacuation is either unknown or is delayed, TECHINT personnel will be tasked to perform onsite analysis. This can provide immediate tactical information and countermeasures vital to the combat force commander. Onsite analysis also ensures the recovery of intact components which become useless once wires are clipped and subcomponents have been disturbed. This type of analysis is limited by the battlefield situation and available assets.

During onsite analysis, TECHINT teams look for—

- Equipment operational characteristics, performance, capabilities, and vulnerabilities.
- New weapons and devices.
- Modifications.
- Possible countermeasures.
- Identification and proper handling of radioactive materiel.
- Specific orientation and siting of equipment.
- Recovery and evacuation of explosive ordnance and NBC munitions.

At times, a large number of like items will be acquired. The TECHINT teams or elements must have the opportunity to examine the materiel

thoroughly. They will be especially interested in any modifications done to the equipment.

TECHINT teams may also be tasked to supervise the materiel handling and evacuation onsite. The Corps TECHINT LNE or theater TECHINT elements will coordinate with appropriate staffs to evaluate the need to use TECHINT personnel to—

- Supervise the evacuation.
- Arrange necessary technical escorts to the Corps CMEC (Forward), CMEC, or CONUS.

TECHINT elements are capable of coordinating the handling and shipping with necessary medical, intelligence, NBC, and strategic level elements for captured CB materiel.

MARKING AND TAGGING

Labeling CEM properly is vital to the timely exploitation of the item. It speeds up the often slow process of producing effective countermeasures for the soldier in combat. Proper labeling provides the analyst information necessary for the item's timely exploitation. It also allows interrogators and TECHINT elements to match up knowledgeable prisoners with the CEM from which they became separated in the evacuation process.

RESPONSIBILITIES:

The capturing unit is responsible for properly marking and tagging CEM. The responsibilities must be clearly established by command SOP. The equipment and document tags accompany the materiel to its final destination. Article 103 of the Uniform Code of Military Justice is printed on the reverse side of the tag to prevent indiscriminate tampering.

As part of core training, all personnel should be instructed on how to tag CEM. They should know the consequences when personnel and equipment are not properly tagged. Training should stress protecting and preserving the original markings on materiel at the time of capture. Weather-resistant capture tags are used. They are normally produced within the theater. They are securely attached to the item itself and to the shipping container. If weather-resistant tags are not available, use any material (for example, rations packing) on which pertinent capture data can be recorded.

There are two procedures for marking and tagging CEM. The procedure used depends on whether or not the captured item is associated with a

captured person.

CEM WITH EPWs:

For CEM with personnel, tag the captured person and any associated CEM with the three-part tag (Form PE 96C-18). An example of this tag is at Figure C-5.

CEM BY ITSELF:

For CEM by itself, tag the piece of equipment and associated document with the tag shown at Figure C-6. Be careful to use this tag to label ONLY items captured with or known to be associated with a particular EPW. In addition, label all documents believed to be of a technical nature (such as operator manuals) with the flag word “TECHDOC." An example is shown in Figure C-7.

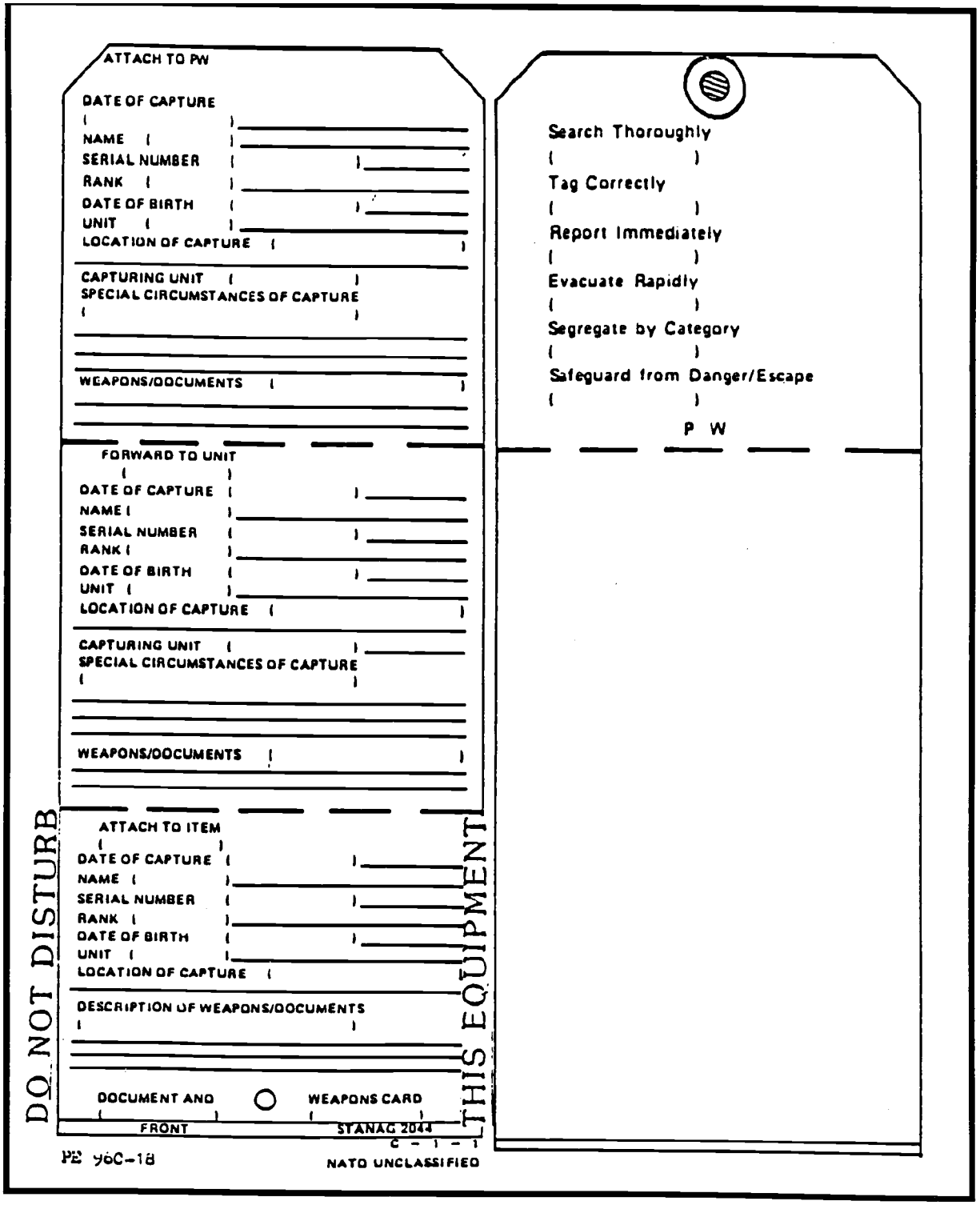


Figure C-5. Front and reverse sides of an EPW tag.

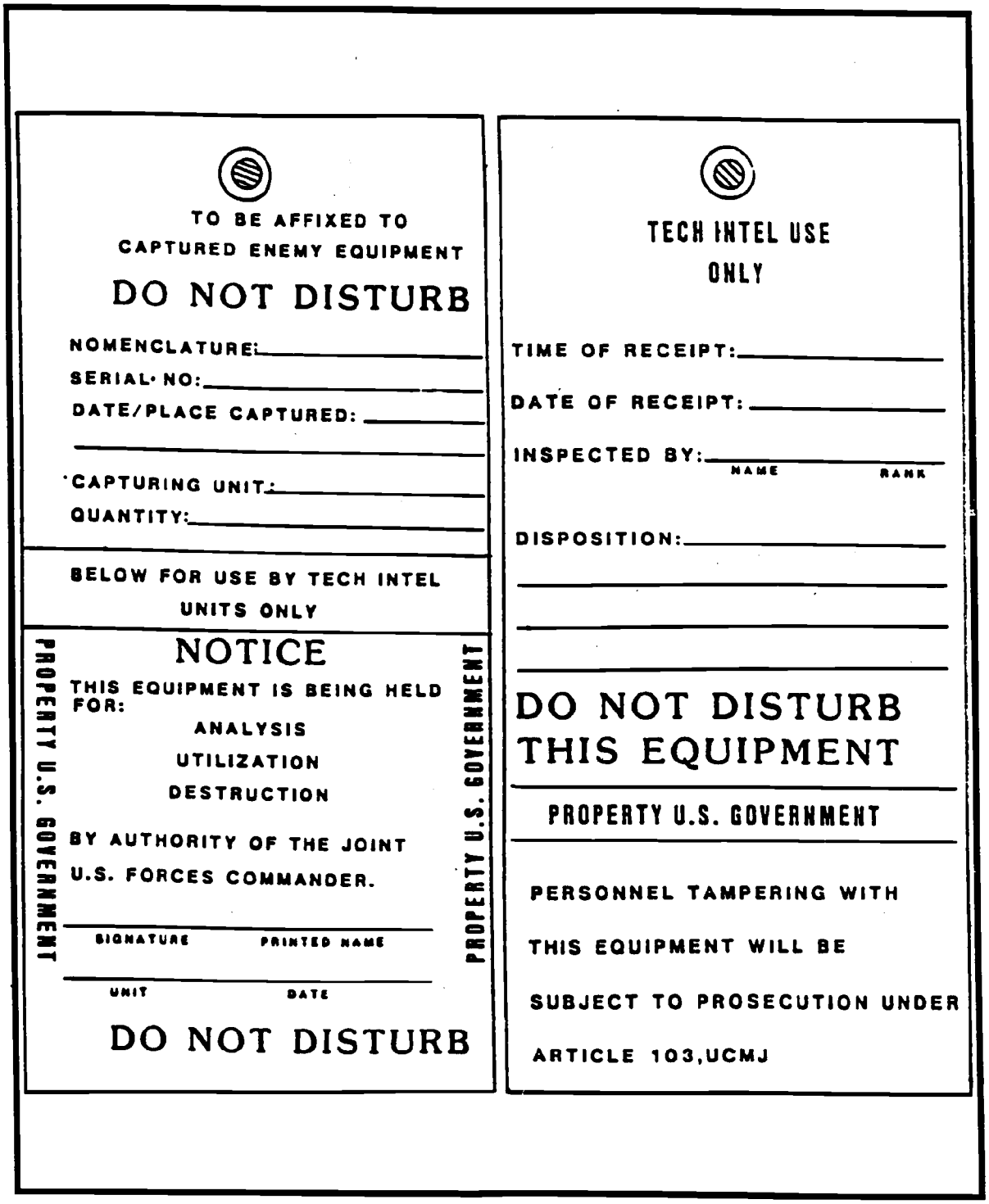


Figure C-6. Front and reverse sides of a CEE tag.

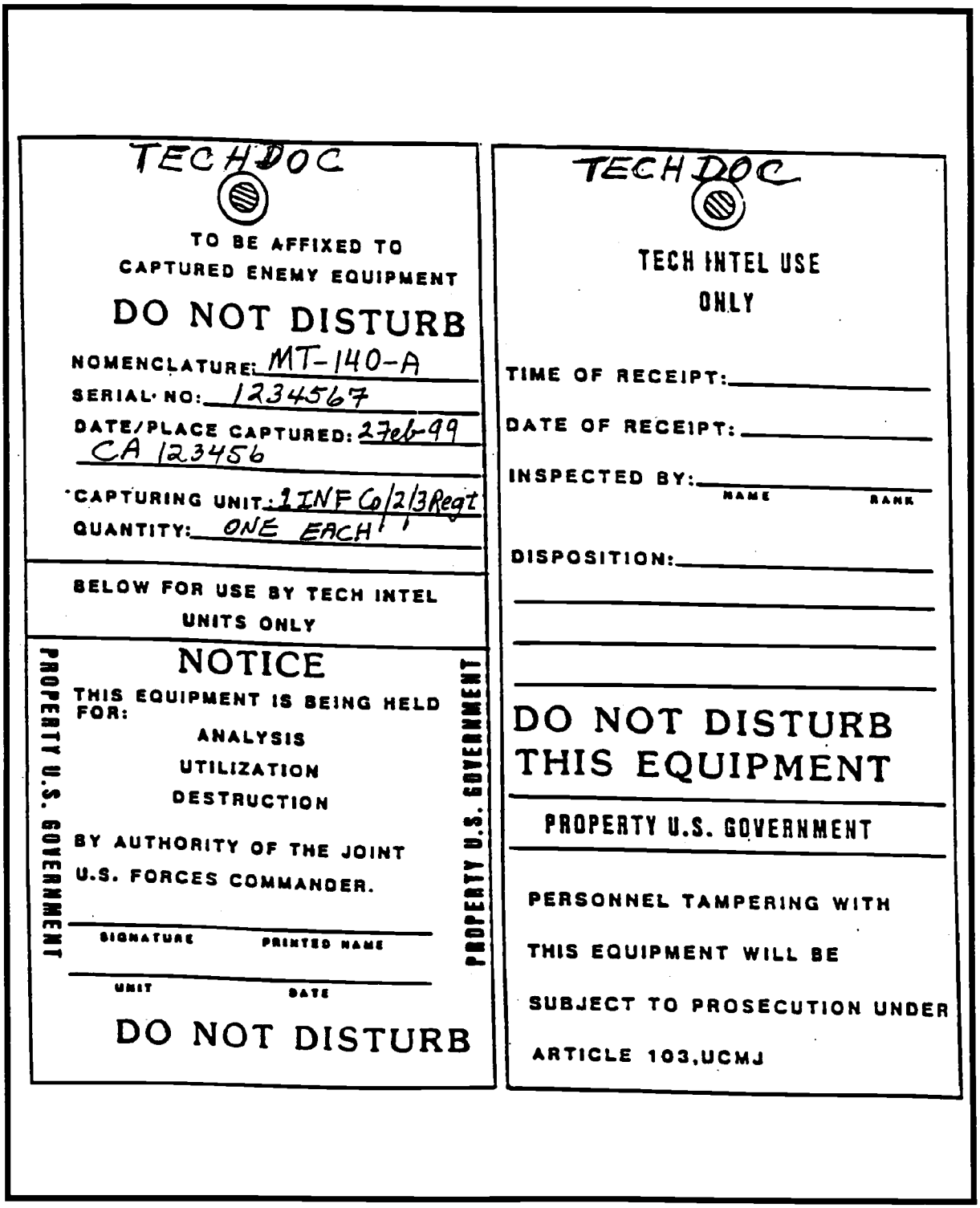


Figure C-7. Example of a CEE tag flagged for TECHDOCs.

SECURITY AND ESCORT

Many items of foreign materiel acquired by US forces and determined to be of TECHINT value require safeguarding in storage as well as during evacuation. Such items may be sensitive due to their criticality or because of the US classification assigned. At all stages during the exploitation process, CEM will be placed under guard to prevent looting, misuse, or destruction.

Initially, the capturing unit is responsible for safeguarding materiel, based on instruction from the next higher headquarters. When foreign materiel is sensitive or of special value, military police elements normally provide physical security during its evacuation.

RECOVERY AND EVACUATION OF TECHNICAL DOCUMENTS

Technical publications and manuscripts of concern to TECHINT relate to the technical design or operation of the materiel. Such documents may be acquired from the materiel to which they refer. Therefore, it is essential that TECHINT personnel coordinate with interrogation elements to exchange information about related documents.

CEM BY ITSELF:

All enemy documents captured on the battlefield are sent immediately to the first intelligence staff officer in the chain. The S2/G2 routes all CEDs to the nearest interrogation element for tactical exploitation. Interrogators screen the documents for immediate information and forward them to higher command, as required.

In any case, all known or suspected technical documents are marked "TECHDOC" and treated with highest priority and forwarded through intelligence channels to the higher command until their value has been determined.

CEM ASSOCIATED WITH EPWs:

Documents obtained through liaison with interrogation elements should be accompanied by pertinent interrogation reports. These reports can be in—

- SALUTE reports.
- Tactical interrogation reports.

- Special interrogation reports.
- Intelligence information reports.
- Biographic reports in accordance with DIAM 58-13.
- Knowledgeability briefs.

CRYPTOGRAPHIC AND OTHER ELECTRONIC EQUIPMENT AND DOCUMENTS

TECHINT units use special procedures for handling captured C-E equipment and documents. These items are tagged and evacuated to the nearest target exploitation (TAREX) element as soon as possible after the initial tactical exploitation.

WAR TROPHIES

Foreign equipment is frequently a target of souvenir hunters. An effective war trophy policy must be established to ensure that these items are not retained by the capturing unit.

FOREIGN MATERIEL NUMBERING SYSTEM

It is the responsibility of the COSCOM and Theater support command to tag all CEE that is sent to them in accordance with the foreign materiel numbering system. All inventories of CEE will use this system to keep track of materiel.

THIS APPENDIX COMPLIES WITH STANAG 2044 AND IMPLEMENTS STANAG 2084.

Appendix D

INTELLIGENCE ANNEX WITH TECHINT INPUT

INTRODUCTION

This appendix provides examples of TECHINT input to an intelligence annex and TECHINT-related tabs to that annex. The TECHINT appendix is used—

- As the primary example for the J4/G4 appendix on captured weapons.
- As the example for the J1/G1 appendix on equipment taken from EPWs. (See Figures C-1 through C-3 for CEE and EPW tags.)

THEATER ARMY INTELLIGENCE ANNEX:

Figure D-1 shows input for TECHINT operations. This example is tailored for a Theater Army headquarters. All headquarters, however, should include TECHINT operations input.

1. SUMMARY OF ENEMY SITUATION.

2. INTELLIGENCE REQUIREMENTS.

a. PIR:
(1) Does the enemy have significant quantities of night vision devices?
(2) Is there unusual or unexplained damage to US equipment and materiel?
(3) Has there been unexpected defensive and/or offensive capabilities of enemy equipment?

b. IR:
(1) What are the capabilities and/or limitations of the AT-5 ATGM?

3. INTELLIGENCE ACQUISITION TASKS.

Figure D-1. Example of an extract from a Theater Army Intelligence Annex.

a. General: Capture of any enemy materiel will be immediately reported through intelligence channels in accordance with priorities described below.

(1) 15th Corps. Priority of collection on foreign equipment is T-64B, AT-5, and SA-13.

(2) 25th Corps. Priority of collection on foreign equipment is BTR-70, BMP-l, and individual protective vest (body armor).

(3) 23d MI Brigade (EAC).

(a) 1st Battalion.

(b) 2d Battalion.

(c) 3d Battalion.

1 One TECHINT collection team and TECHINT LNE to operate within each corps area, attached to each corps MI brigade (command less OPCON).

2 Screening and exploitation of captured IEW priorities described in FM 34-54, Appendix B.

3 Fully integrate TECHINT operations and teams with IEW and EPW operations.

4. MEASURES FOR HANDLING PERSONNEL, DOCUMENTS, AND MATERIEL.

a. Personnel.

b. Documents.

c. Materiel.

(1) All materiel will be reported in accordance with procedures and priorities described in Appendix _, TECHINT.

(2) All materiel will be evacuated to the nearest collection point and held for TECHINT screening in accordance with Appendix _, TECHINT.

(3) Items designated by TECHINT personnel as possessing intelligence value will be evacuated to destinations designated by TECHINT personnel in accordance with priorities described in Appendix _, TECHINT.

Figure D-1. Example of an extract from a Theater Army Intelligence Annex (continued).

(4) No materiel will be diverted for other uses until screened and released by TECHINT personnel.

5. REPORTS AND DISTRIBUTION. All equipment-related intelligence, SALUTE, and EPW reports will include the J2/G2 and CMEC as an addressee.

Figure D-1. Example of an extract from a Theater Army Intelligence Annex (continued).

(TAB B) JOINT THEATER TECHNICAL INTELLIGENCE APPENDIX:

Figure D-2 is an example of a Joint Theater TECHINT appendix. It shows how CEM must be handled, reported, and disposed of.

Appendix___, TECHINT, to Annex___, Intelligence, to OPLAN/OPORD___.

REFERENCES:

a. OPLAN _____

b. FM 34-54.

c. FM 3-19-1.

d. Chemical and Biological Sampling, Transport, and Evaluation Management Procedures, dated February 1986.

1. PURPOSE: This appendix establishes policy and prescribes responsibilities and procedures for the proper handling, reporting, intelligence assessment, and disposition of CEM. Additionally, it establishes the procedures for the safe and expedient collection of suspected CB agents to the laboratory for processing, analysis, and identification.

2. POLICY:

a. The J2 controls and directs the theater captured materiel exploitation program. The CMEC OPCON to the J2 carries out exploitation activities.

b. The CMEC will be formed from elements of the 203d MI Battalion (TECHINT), _____ MI Brigade.

c. The _____ J2 exercises staff responsibility over the intelligence exploitation of CEM throughout the area of operations and establishes requirements for evacuation of specific items to CONUS for further exploitation. An LNE from the JCMEC will be located in the J2.

d. Commander, 203d MI Battalion (TECHINT)—

(1) Establishes the CMEC and attaches a TECHINT team to each Corps; positions an LNE with the J2, each Corps G2, the theater MI Brigade, and theater interrogation.

(2) In coordination with the Theater/Army Surgeon General, advises the J2/G2 on all matters of CB sampling.

Figure D-2. Example of a Joint Theater TECHINT Appendix.

(3) Recommends a theater souvenir and war trophy policy in accordance with FM 34-54, Appendix C.

e. The J3—

(1) In coordination with the J2, approves requests and assigns priorities for issue of CEM to US units engaged in special missions or training based on the following prioritized uses of captured materiel:

(a) Intelligence.

(b) Special warfare.

(c) Special Operation Forces.

(d) Issue to friendly forces.

(e) Internal defense.

(f) Substitutes or supplements to US equipment.

(g) Distribution to friendly foreign units or groups.

(2) Coordinates provisions of EOD support as required in the exploitation of CEM in accordance with AR 75-15 and to fill requirements stated by the J2.

f. The J4 exercises staff supervision over the evacuation and movement of CEM of intelligence value in the theater to the JCMEC, and coordinates evacuation of high priority items back to CONUS.

g. The Staff Judge Advocate provides legal guidance concerning the disposition of certain categories of enemy materiel, structures, and facilities.

h. See Tab D of this appendix for CB sampling responsibilities.

3. RESPONSIBILITIES:

a. The CMEC is charged with the conduct and coordination of assessment of CEM within the command. Support in the assessment of enemy naval and aerodynamic systems and materiel will be provided by intelligence personnel from the Navy and Air Force components attached to the CMEC. The scope of responsibilities include:

(1) Assign an LNE to the J2, G2, and the theater interrogation facility.

Figure D-2. Example of a Joint Theater TECHINT Appendix (continued) .

(2) Deploy TECHINT collection teams forward to each deployed Corps to conduct preliminary screening of evacuated materiel and to respond to targets of opportunity which cannot be processed in a normal manner.

(3) Receive and process validated intelligence requirements for items of enemy materiel.

(4) Participate in the technical interrogation of EPWs and assist in screening CEDs.

(5) Examine and evaluate TECHINT reporting and classification of CEM.

(6) Participate with TAREX elements to fully integrate the exploitation of specified C-E items.

(7) Participate with medical, NBC, and Special Operations units for coordinating the delivery of CB samples through MI channels to the TAML.

b. Subordinate Commands:

(1) Each Corps will—

(a) Designate and operate collection points. Report locations of collection points where CEM will be stored and amounts and types stored at each location. Forward reports to Cdr, CMEC, with an information copy to the J2/G2 and J4/G4s. The collection point will receive, store and, only upon direction, dispose or issue CEM.

(b) Designate and operate ammunition storage areas for the storage of captured ammunition and explosive items, as required. Store captured chemical munitions similarly to like US chemical munitions. Report locations of ammunition storage areas and amounts and types stored to Cdr, CMEC, with an information copy to J2/G2 and J4/G4.

(c) Provide necessary logistics support, as required, to evacuate CEM and CB samples needed for intelligence operations, or other purposes, from collection points to the CMEC.

(d) Ensure all CEM is promptly tagged.

(e) Provide logistics and administrative support for all TECHINT assets operating within their areas.

(2) NBC reconnaissance units, Special Operations units, and medical units are responsible for the transfer of CB samples to TEUs or TECHINT collection teams at Corps, or directly to the TAML.

Figure D-2. Example of a Joint Theater TECHINT Appendix (continued) .

4. PROCEDURES:

a. Procedures for handling and processing CEM.

(1) The recovery and evacuation of CEM is a command responsibility at all levels. The prescribed method of evacuation is through normal logistics channels and in accordance with priorities established in Tab A and Tab B to this Appendix.

(2) Enemy materiel captured by US military personnel is the property of the United States and must be protected from pilferage, cannibalizing, and souvenir hunters. Commanders at all levels will provide adequate security for CEM until it has been screened by TECHINT personnel.

(3) Specific intelligence collection requirements and Top Ten End Item requirements items of enemy materiel for which the tactical commander and intelligence agencies have a need are listed at Tab A and Tab B to this Appendix. These Tabs will be published upon execution of the OPLAN.

(a) When items listed in Tab A and Tab B or any of their updates are captured or otherwise obtained, commanders will ensure that the acquisition is reported through intelligence channels to the Corps TECHINT LNE to Cdr, CMEC, with an information copy to J2/G2.

(b) Report as in (a) above (at a PRIORITY precedence) the capture of standard types of foreign materiel that have been apparently modified in a major way or are having a greater impact on combat operations than expected. These items will be evacuated to COSCOM collection points by available backhaul capabilities on a PRIORITY basis. Equipment will be held pending further disposition instructions from the J2 through the Corps TECHINT LNE.

(c) The capture of items listed in Tab A and Tab B will be reported by IMMEDIATE precedence through intelligence channels and expeditiously evacuated to at least the supporting collection point to await further disposition instructions from J2.

(d) Report as in (a) above (at a ROUTINE precedence) all CEM. These items will be evacuated to collection points by available backhaul capabilities on a space-available basis. They will be held at the collection point until screened by TECHINT personnel. Disposition will be per paragraph 4d below.

(e) The J2, in coordination with the J4, is the focal point for evacuation of key items of intelligence interest to CONUS for national exploitation.

Figure D-2. Example of a Joint Theater TECHINT Appendix (continued) .

(4) The assessment of CEM below division and separate brigade levels will be limited. Their primary responsibility is the recovery, reporting the capture, and initial evacuation of enemy materiel from the capture location to the nearest collection point. Exception is for medical supplies which will be handled through medical supply channels. Significant items of CEM which cannot be evacuated, either because of the tactical situation or due to their size, will be left in place and reported immediately.

(5) Assessment of CEM at division and separate brigade level is performed by intelligence and operations personnel to the extent necessary to determine the immediate tactical significance of the materiel. Assessment at this level does not replace the need for detailed evaluation and analysis of CEM by technical specialists from the JCMEC. For this reason, the prompt evacuation of significant items of CEM must not be delayed.

(6) Screening and preliminary field assessment of CEM is performed by JCMEC TECHINT collection teams. These teams will operate in the Corps areas and are attached (command less OPCON) to the Corps MI Brigade. When required, these teams can also provide assistance to capturing units. Assessment functions are normally carried out at the Corps support area collection points. Items of intelligence interest or items needed to fill other requirements by the JCMEC are selected for evacuation. Selected items will be evacuated to the JCMEC, or a designated location, by collection point personnel through logistics channels.

(7) Selected CEM evacuated to the CMEC is subjected to detailed examination and evaluation to—

(a) Determine enemy materiel threats, performance capabilities, and limitations.

(b) Produce information from which military countermeasures may be developed.

(c) Provide inputs continuously to the national and integrated S&TI Program in accordance with DIA and Theater policies.

(d) Provide intelligence that can be of timely use to the tactical commander.

b. Materiel Requiring Special Handling.

(1) C-E Equipment. All CEM in this category must be evacuated immediately with their dial settings, frequencies, and so forth, and recorded and sent to the supporting EW unit by the quickest and most secure means possible. All such materiel will be evacuated to Corps support area collection points for screening by TECHINT and other specialized personnel.

Figure D-2. Example of a Joint Theater TECHINT Appendix (continued) .

(2) Ammunition and Explosives. The complete recovery and expeditious evacuation of enemy ammunition and components is essential to the identification of known or new enemy weapons systems and the threat posed by each. EOD teams are responsible for preparing PRETECHREPs on first-time-seen enemy ammunition or explosives. If there are no TECHINT personnel to assist in the area, EOD teams will also be responsible for preparing COMTECHREPs.

(3) Medical Materiel. Medical materiel normally will not be destroyed. It will be left in place if it cannot be evacuated. It will be handled in accordance with normal Class VIII procedures.

(4) Significant Items: All intelligence requirements specified in Tab A and Tab B will be afforded special handling as described in paragraph 4a above.

(5) Technical Documents: Captured or recovered technical documents consist of firing tables, logbooks, packing slips, and other documentation. If the tactical situation does not permit the equipment to be evacuated, the documents will be forwarded to the JCMEC and will include a description of the equipment.

(6) CB Samples. See Tab D to this appendix.

c. Requirements.

(1) DIA provides national intelligence requirements for CEM to the Theater. In-theater intelligence requirements for enemy materiel are submitted through J2 and G2.

(2) In-theater operational and training requirements for other than Army subordinate units are submitted through J3 to the J2 for review, approval, and assignment of priority.

(3) The intelligence requirements are published in Tab A and Tab B.

d. Disposition.

(1) Items required in support of operational requirements or for distribution to host-country forces will be separately designated by the J3. Tab C to this Appendix contains such equipment.

(2) Items determined by the J2 to have no intelligence significance and by the J3 to have no operational need will then be identified and reported through logistics channels to the J4. Items will be retained within designated collection points for further disposition by the J4. No items will be released for war trophies until released by J2.

Figure D-2. Example of a Joint Theater TECHINT Appendix (continued) .

e. Destruction. The destruction of CEM, excluding medical items, will be accomplished only in the event that recapture is imminent, due to its location, or in those cases where materiel is declared by EOD or TECHINT personnel to be hazardous to the safety of troops. In the event destruction of materiel is necessary, all factory markings should be carefully recorded and photographs taken, if possible, before the materiel is destroyed. Medical items normally will not be destroyed, but left in place.

OFFICIAL:

TABS:
A = Top Ten Priority Items (TBP)
B = General Collection Requirements (TBP)
C = Equipment Releasable to Allies (TBP)
D = Chemical, Biological, and Biomedical Sampling

Figure D-2. Example of a Joint Theater TECHINT Appendix (continued) .

(TAB D) CHEMICAL, BIOLOGICAL, AND BIOLOGICAL SAMPLING PROCEDURES:

Figure D-3 is an example of a Tab D to a TECHINT Appendix of a Theater Army Intelligence Annex. It shows disposition instructions for CB samples.

1. PURPOSE: To establish the procedures for the safe and expedient collection and evacuation of suspected CB agents to the laboratory for processing, analysis, and identification.

2. RESPONSIBILITY:

a. The Cdr, JCMEC, with the Army and Theater Surgeon General, are responsible for advising the J2/G2 and J3/G3 on all matters of CB samplings.

b. Corps G2, SOCCENT J2, MARCENT G2, Navy intelligence, and Air Force intelligence will be responsible for transferring samples to MI channels via TEU teams or TECHINT collection teams.

c. Medical personnel will coordinate with combat units and Graves Registration Service units through local medical units and hospitals for obtaining biomedical samples, for the expedient transfer of personnel deceased as a result of a CB attack.

d. The Cdr, JCMEC, will be responsible for coordinating shipment of suspected biological samples to the TAML for preliminary analysis, and suspected chemical or biological-chemical mixed to CONUS-based laboratories.

e. The TEU is responsible for coordinating shipment to the US Army Chemical Research Development and Engineering Center (ERDEC) at Aberdeen Proving Ground, MD, if it is a chemical sample; or to the US Army Research Institute of Infectious Diseases (USARIID) at Fort Detrick, MD, if it is a combination CB sample or if it is a suspected biological sample only.

3. SAMPLING RESPONSIBILITY: Samples suspected of containing CB agents are divided into environmental and biomedical samples on the basis of their origin. Both medical and nonmedical teams are responsible for collecting samples suspected of containing CB agents.

a. ENVIRONMENTAL SAMPLES. Environmental CB agent samples are collected in the field. They include samples like aerosols or vapors; liquids other than water, soil, vegetation; water; used chemical equipment; and ordnance. The acquisition of these samples is the responsibility of—

(1) NBC reconnaissance teams.

Figure D-3. Example of a TAB D to a TECHINT Appendix of a Theater Army Intelligence Annex.

(2) Technical escort field teams.

(3) TECHINT collection teams.

(4) Preventative medicine units (potable water sources only).

(5) Special operation teams.

b. BIOMEDICAL SAMPLES. Biomedical samples are derived primarily from acutely ill soldiers who exhibit symptoms of CB agent intoxication or from personnel who were killed in an attack. Collection of the biomedical samples will be the responsibility of personnel in—

(1) Battalion-level medical units.

(2) Division-level medical treatment facilities.

(3) Combat support hospitals.

(4) Evacuation hospitals.

(5) Theater medical hospitals.

(6) NBC reconnaissance teams (small animals only).

(7) Technical escort field teams.

(8) TECHINT collection teams.

4. SAMPLING: Sampling will be initiated if the following are observed:

a. Significant numbers of unexplained sickness or death of personnel or animals occur.

b. Ordnance (munitions) are found which contain known or suspected CB agents.

c. An attack is suspected or is known to have occurred but the causative agent cannot be identified.

d. The widespread outbreak of unusual mission-degrading behavior occurs.

e. Sampling of known identified agents to verify first use is required.

Figure D-3. Example of a TAB D to a TECHINT Appendix of a Theater Army Intelligence Annex (continued).

5. PROCEDURES:

a. Procedures for the collection, packaging, documentation, and transporting of CB samples to laboratories must be precise to ensure the credibility of the analysis conducted on the samples. Ensuring the credible analysis of suspected CB samples is critical for both battlefield commanders concerned with possible retaliation and contamination avoidance, and medical personnel concerned with prophylactic or post-contamination treatments.

b. When possible, a background sample from "clean" areas beyond the perimeter of the attack site should be obtained as baseline data for comparison; collection should be identified to sample collected data from contaminated areas and packaged separately.

c. The best biomedical sample is an acutely ill soldier or a cadaver which is sent back to CONUS immediately. A copy of the physical examination or an extract of significant findings will be enclosed with biomedical samples. Samples will be collected in triplicate, distributing two to CONUS and one to the TAML.

d. All samples will be forwarded from the TAML to either ERDEC or USAMRIID laboratories 12 to 24 hours after collection; delay beyond 24 hours rapidly degrades the intelligence value of the samples.

6. NOTIFICATION MESSAGE: A notification message will be sent from the TAML or TECHINT unit by PRIORITY precedence upon receipt and screening of samples to the Theater Surgeon General, J2, J3, and CDR, ERDEC APG MD//CBATEB//: The notification message will contain the following information:

a. The sample identification number and details which relate to the acquisition of the sample. This message will be confirmed to provide the following information:

(1) Background information.

(2) Physical description.

(3) Results of preliminary tests after sample collection.

(4) Where, when, and under what conditions the sample was acquired.

(5) Description of incident.

(6) Casualty symptoms (if applicable).

(7) Shipment information, such as—

Figure D-3. Example of a TAB D to a TECHINT Appendix of a Theater Army Intelligence Annex (continued).

(a) Date of shipment.

(b) Mode of transportation.

(c) Flight number and destination.

(d) Estimated time of arrival CONUS.

(e) Description of shipment (for example, size and weight).

(f) Names of escort personnel.

Figure D-3. Example of a TAB D to a TECHINT Appendix of a Theater Army Intelligence Annex (continued).

Appendix E

TECHNICAL INTELLIGENCE REPORTS

INTRODUCTION

This appendix describes the nine basic reports, which are listed below, that battlefield TECHINT analysts use.

- SALUTE report (Figure E-1).
- Preliminary Technical Report (PRETECHREP) (Figure E-2).
- Complementary Technical Intelligence Report (COMTECHREP) (Figures E-3, E-4, and E-5).
- Detailed Technical Report (DETECHREP).
- Technical Intelligence Update Report.
- Technical Intelligence Summary (TECHSUM).
- Technical Intelligence Report (TIR).
- Special technical reports. These reports are generated in response to requests for information. The formats vary by request and usually address a specific question or requirement from a TECHINT consumer.
- Other equipment information reports. These reports focus on aspects of equipment that do not necessarily relate to intelligence needs per se. For example, the Theater commander may have a war trophy policy that permits units to evacuate certain equipment to their home stations for static displays. These reports may include driver's instructions, handling considerations, render-safe procedures, and demilitarization standards for equipment.

The SALUTE report is an oral or written report prepared by the acquiring units or intermediate command echelons. It is used to report rapidly, by electrical or other means, the capture of foreign materiel. These reports are forwarded to either the TECHINT LNEs at Corps, other TECHINT LNEs, or directly to the JCMEC. As a result of this information, a TECHINT team could be dispatched or the CEM could be moved to the Corps CMEC or the theater JCMEC. Figure E-1 gives an example of a completed SALUTE report.

SALUTE REPORT

TO: G2 V Corps DTG: 230900Z Aug 98
FROM: G2 24th Inf Div (Mech) REPORT NO: 07-0623

1. SIZE: NA.

2. ACTIVITY: Capture of shoulder-fired laser target designator by 1/64th Armor Bn 2d Bde 24th Inf Div (Mech) **(include capturing unit)**.

3. LOCATION: Town of Al-Dahran (UTM EH556937) **(as a minimum always give grid coordinates)**.

4. UNIT: 3d Republican Guards Regiment **(include enemy unit if known).**

5. TIME: Item captured on 230230Z AUG 98 **(always use ZULU time)**.

6. EQUIPMENT: One laser target designator and sighting device **(give best possible description).**

Figure E-1. Example of a SALUTE report.

PRELIMINARY TECHNICAL REPORT

The PRETECHREP contains a general description of the CEE. It alerts the CMEC, other technical elements, and the tactical units to significant technical information of immediate tactical importance. It can also be used for reporting inventories at collection points through intelligence channels so that location, quantities, and type of equipment can be monitored. Figure E-2 shows an example of a PRETECHREP.

Corps TECHINT teams and possibly CMEC teams will prepare a PRETECHREP on all CEM after preliminary screening. This report is first transmitted by radio directly to the Corps TECHINT LNE, from the captured equipment site. It is then forwarded to the CMEC. The report will normally be treated as unclassified during this transmission.

The CMEC's technical analysts determine what is of importance from the report, and give the team instructions through the LNE on what items need more detailed reporting or evacuation. During this time the team will collect all documents off the CEE and will record—

(Classification)

PRETECHREP

A. Type of equipment and quantity.

B. Date and time of capture.

C. Location (map reference).

D. Capturing unit and circumstances of capture.

E. Enemy formation from which captured and origin.

F. Brief description with serial numbers and, if possible, manufacturer.

G. Technical characteristics with an immediate value, including information or any photographs available.

H. Time and origin of message.

I. Present location of CEE.

(Classification)

Figure E-2. Format for a PRETECHREP.

- All radio frequencies of communication equipment.
- All serial markings of important equipment.
- The battle damage done to the CEE.

These information requirements and actions will be taken at all CEE sites. The radio frequencies will be sent only by secured means.

COMPLEMENTARY TECHNICAL INTELLIGENCE REPORT

The COMTECHREP is categorized by Types A, B, or C, depending on what type of CEE is being reported. The COMTECHREP contains a more detailed description of the CEE than the PRETECHREP. It alerts the JCMEC, other technical elements, and the tactical units to significant detailed technical information of immediate tactical and technical importance.

Corps TECHINT teams, and possibly JCMEC teams, will prepare a COMTECHREP on all CEM that the JCMEC tells it to do. If the TECHINT collection team is out of contact with the JCMEC, it will follow the TECHINT collection plan and use its best judgment on reporting.

This report is first transmitted normally by secure computer data transmission over landline to the Corps TECHINT LNE from the team's base. If possible, it is transmitted from the CEE site over secure computer or radio data transmission via satellite. It is then transmitted to the JCMEC. The report normally will be treated as classified during this transmission.

All electronic images of the CEE and computer scanning of critical CED will be transmitted with the COMTECHREP. If data transmission is not on hand, the report will be transmitted by the nearest message center at no less than PRIORITY precedence.

COMPLEMENTARY INTELLIGENCE TECHNICAL REPORT - TYPE A

The COMTECHREP - Type A is provided to Air Force TECHINT personnel. Air Force teams usually are not on the scene of captured or downed enemy aircraft before destruction, recapture, or loss. Army TECHINT personnel usually are the first elements on the scene and will examine the CEM and submit a COMTECHREP - Type A. This report often constitutes the only information that can be provided to Air Force TECHINT. If naval CEM is acquired, the Type A report format can be modified for reporting such acquisition. Figure E-3 shows an example of a COMTECHREP - Type A.

(Classification)

COMTECHREP - TYPE A

The COMTECHREP - Type A is used to report information about aircraft. The JCMEC normally will require this report to be done right after the PRETECHREP on the aircraft.

A. Type of Aircraft, fixed wing (examples):
   (1) Air-superiority (F-15C, SU-27B)
   (2) Multi-role fighter (F-l6, MiG-29C)

(Classification)

Figure E-3. Format for a COMTECHREP - Type A.

(Classification)

(3) Fighter-bomber (F-111, YAK-141)
(4) Close Air Support/Ground Attack (A-10, SU-25, SU-22)
(5) Bomber (B-2, TU-160)
(6) Observation (OV-10)
(7) Transport (C-130, IL-76)
(8) Airborne Early Warning (AWACS, Israeli PHZ)
(9) Electronic Warfare/Suppression of Enemy Air Defense (EA-63, F-4G)
(10) Special Mission (for example, Intelligence Collection)

B. General Aircraft Configuration:
(1) Overall length
(2) Wingspan
(3) Wing sweep angle
(4) Variable geometry wings
(5) Number of vertical stabilizers and orientation
(6) Number of seats and orientation
(7) Number of engines
(8) Intake type and location
(9) Landing gear type and orientation
(10) Distinct control surfaces present (flaperons, elevons)
(11) Other distinguishing features (wing fences, wingtip winglets, antennas, canards)

C. Identifying Marks:
(1) Fin flashes
(2) Paint scheme
(3) Individual or squadron markings

D. Overall Condition:
(1) Describe extent of damage and salvageable parts
(2) Assess cause of crash, if possible
(3) Did Aircrew survive

E. Cockpit Avionics (not all equipment is present in every aircraft):
(1) Type (brand and model) of airborne intercept, bombing and navigation, weather radars
(2) Type of communications gear, frequency settings if possible
(3) IFF or Transponder type, settings
(4) Type EA equipment
(5) Type of RWR gear
(6) Type of weapon guidance gear (laser designation equipment, TV guidance equipment)

(Classification)

Figure E-3. Format for a COMTECHREP-Type A (continued).

(Classification)

(7) Type of IRSTS if present
(8) Are the following flight controls present: HUD, fly-by-wire controls, MFD, HOTAS (9) Type of chaff or flare dispenser system

F. Armament:
(1) Number of cannons present, caliber, and location
(2) Bombs or rockets present
(3) Air-to-air missiles present
(4) Air-to-surface missiles present
(5) Number of launch rails or weapon mounts present and location

G. General remarks and special points or unusual features not mentioned.

H. Photos of at least:
(1) Airframe
(2) Engine
(3) All other items that could be of importance

I. Designation of TECHINT collection team conducting exploitation:

J. Time and origin of message:

(Classification)

Figure E-3. Format for a COMTECHREP - Type A (continued).

COMPLEMENTARY TECHNICAL INTELLIGENCE REPORT - TYPE B

The COMTECHREP - Type B is used to report information about explosive ordnance. TECHINT teams prepare these reports, normally done by the EOD member of the team. EOD companies will also prepare them in absence of TECHINT personnel or when required by higher headquarters. This report must be as complete and detailed as possible. EOD personnel prepare and send this report by the fastest means through an EOD control unit. The JCMEC coordinates with EOD battalions to receive copies of these reports as soon as possible.

NOTE: Initial overall classification of EOD Reports. Non-nuclear (COMTECHREP B) will be in accordance with OPNAVINST S5513.3B-24.1.

The initial classification of the COMTECHREP B with RSP is Confidential and will not be released to non-US personnel without the written consent of Commanding Officer, NAVEODTECHDIV. The release of RSP to non-EOD qualified personnel is forbidden.

A complete and accurate report is essential; lives of other EOD personnel rely on this report, strive for the most complete report possible. However, when a detailed report might result in serious delay and the items are of extreme significance, complete as much of the report as possible. Items of EOD interest will at a minimum be photographed (with electronic imaging systems if available), X-rays (digital) and have detailed drawings with measurements (metric). Figure E-4 shows an example of a COMTECHREP - TYPE B.

The unit completing the report will distribute copies of the COMTECHREP - TYPE B (EOD Report) to all deployed US EOD units and provide copies to:

Commander
USATECHDET
2008 Stump Neck Road
Indian Head, MD 20640

Commander
USAARDEC
ATTN: AMSTA-AR-FSX
Picatinny Arsenal, NJ 07806-5000

Commanding Officer
NAVEODTECHDIV
2008 Stump Neck Road
Indian Head, MD 20640

Commander
NGIC
ATTN: IANGIC-RMS
220 7th Street, NE
Charlottesville, VA 22901-5396

(Confidential when filled in)

COMTECHREP-TYPE B (EOD Report)

Section I. (U) DESCRIPTIVE INFORMATION

1. (U) IDENTIFICATION. See Figure __ for physical appearance and dimensions.
NOTE: This will be an external view (when possible) and not show internal components.

a. (U) Designation. Ordnance designation (if known) with transliteration of foreign alphabet.
Example: M45.

b. (U) Type. Used to summarize the key functional aspects of the items.
Example: This is a High Explosive Rocket Assist (HERA) projectile.

Figure E-4. Format for a COMTECHREP - TYPE B.

c. (U) Painting and Markings. Record all paintings, surface treatments, and markings.

d. (U) Features. Point out unique or distinguishing external features of the item that are not obvious in the drawings.

2. (U) DESCRIPTION.

a. (U) Material. Include information pertaining to the major external components; for example, "plastic," "aluminum."

b. (U) Weight. Give the approximate weight if known.

3. (U) HAZARDOUS COMPONENTS.

ITEM QTY LOCATION EXPLOSIVE HE WEIGHT

List Hazardous components (if known).

4. (U) FUNCTIONING. Explain the operation of the ordnance, particularly the components of the ordnance involved with initiating the explosive train.

5. (U) APPEARANCE. It must be known for certain that the item is unarmed if the item is to be treated as such.

a. (U) Unarmed Condition. Example: The item is unarmed if not fired.

b. (U) Armed Condition. Example: Consider the item armed if it has been fired.

Section II. (C) EOD PROCEDURES. (EOD USE ONLY)

6. (U) RENDER SAFE PROCEDURE FOR THE UNARMED CONDITION.

a. (C) PROPOSED: (Develop and record prior to completing RSP).

b. (U) Proceed to disposal.

7. (U) RENDER SAFE PROCEDURE FOR THE ARMED CONDITION WARNINGS.

a. (C) PROPOSED: (Develop and record prior to completing RSP).

b. (U) Proceed to Disposal.
continued:

8. (U) DISPOSAL PROCEDURE.

Figure E-4. Format for a COMTECHREP - Type B (continued).

a. (U) Unarmed. Transport hazardous components to safe disposal area and dispose of by detonation.

b. (C) Armed.

(1) (Include quantity of explosives used to dispose of item).

(2) Detonate remotely.

(Confidential when filled in)

Figure E-4. Format for a COMTECHREP - Type B (continued).

COMPLEMENTARY TECHNICAL INTELLIGENCE REPORT - TYPE C

The COMTECHREP - Type C is used to report items not reported under COMTECHREP (Types A and B). COMTECHREP - Type C is submitted as soon as possible. Figure E-5 shows an example of a COMTECHREP - Type C.

(Classification)

COMTECHREP - TYPE C

A. Date found and location (map reference).

B. Type of equipment and quantity.

C. Origin.

D. Description with distinguishing marks (additional details).

E. Condition of equipment.

F. Technical characteristics of immediate tactical value (additional details).

G. Recommended disposal.

H. Name plates photographed.

I. Photographs taken.

(Classification)

Figure E-5. Format for a COMTECHREP - Type C.

(Classification)

J. Other information.

K. Designation of TECHINT collection team doing this initial exploitation.

L. Time and origin of message.

(Classification)

Figure E-5. Format for a COMTECHREP - Type C (continued).

DETAILED TECHNICAL REPORT

The DETECHREP normally is prepared at the JCMEC by the Exploitation Company, with the assistance of the national S&TI analysis personnel at the JCMEC. The DECTECHREP normally is classified. The CM&D section of the Exploitation Company sends the DETECHREP through the JTIB to the national S&TI community. They also send a summary of the report to Theater units.

TECHNICAL INTELLIGENCE UPDATE REPORT

The TECHINT Update Report is a one- to two-paragraph report on an item of equipment that has an impact on tactical operations. The report comes from information provided in PRETECHREPs and COMTECHREPs, and is unclassified. The goal of the report is to reach the lowest level—the soldier—with information of value to the soldier. The CM&D section of the Operations Company sends the report by electronic message and computer data transmission.

TECHNICAL INTELLIGENCE SUMMARY

The TECHINT Summary is a collection of information on more than one item of equipment that has an impact on theater tactical operations. The information comes from PRETECHREPs and COMTECHREPs from over a period of time or from a large CEE location. The report normally is unclassified, but if put into an overall intelligence summary, it can be classified. The CM&D section of the Exploitation Company sends the report by electronic message and computer data transmission to the JTIB. The JTIB then makes dissemination to the lowest possible level with JTF C^3I assets.

TECHNICAL INTELLIGENCE REPORT

The TIR is a critical report which goes to the highest levels of the intelligence hierarchy. The report comes from information from PRETECHREPs, COMTECHREPs, and DETECHREPs. This report is always classified and follows the format in DIAM 58-13. The CM&D section sends TIRs by electronic message to the JTIB. The JTIB disseminates them to the highest and lowest intelligence units and agencies possible.

Appendix F

COLLECTION AND EXPLOITATION REQUIREMENTS

INTRODUCTION

This appendix includes guidance on how to develop a TECHINT collection plan, and a listing of general exploitation categories regarding items of interest to battlefield TECHINT. It is included only as a field guide, and is not an all-inclusive exploitation plan.

TECHINT COLLECTION PLAN GUIDANCE

TECHINT elements are a very limited resource requiring specific collection planning to be effective. The most critical TECHINT items for collection are found in the TECHINT Appendix to the OPLAN or OPORD. The following steps help determine pertinent items in the collection plan before it is accepted.

STEP 1. Identify the equipment OB for the threat; for example, items such as individual soldier's equipment, maps, small arms, heavy weapons, and explosives. Also include every type of equipment the threat could have on the battlefield. This is an ongoing effort, with the OB always being updated. In addition to the collection plan, include overlays of locations of ASPs, maintenance points, SAMs, communications centers, and other locations that contain quantities of equipment for collection.

STEP 2. In coordination with DIA, national S&TI requirements, and Theater and Corps PIR and IR, the TECHINT unit prioritizes collection of items from the OB. If coordination is not possible, the equipment that is the greatest threat to the conduct of tactical operations is prioritized.

STEP 3. The DOD Foreign Acquisition List is used to guide TECHINT priorities. These collection priorities are published in the Intelligence Annex to the OPORD in the form of a collection plan. As collection takes place, the updated collection plan is then sent to TECHINT and theater units in message format.

STEP 4. The TECHINT collection requirements are then cross-referenced to the known threat OB. TECHINT elements are then tasked, if possible, with specific collection of items from the threat units that they are facing. In addition, the Corps TECHINT LNE coordinates with the Corps G2 to give specific collection requirements to the Corps units. The JTIB coordinates

with the Theater J2 to give collection requirements to theater units such as Special Operations units.

STEP 5. In addition to the TECHINT collection priority list for equipment, TECHINT elements are tasked to collect, inspect, or develop the following items:

- Threat equipment manuals or documents.
- Threat installations.
- Listing of TECHINT questions for the interrogation of EPWs.
- CB laboratories and samples.

STEP 6. The 203d MI Battalion, in coordination with national S&TI agencies, maintains contingency TECHINT collection plans for possible threat forces. When a TECHINT element deploys, it is given the TECHINT collection plan in order to prepare and train for operations.

EXPLOITATION PLANS AND REQUIREMENTS

GENERAL EXPLOITATION PLAN:

The JCMEC is expected to conduct this level of exploitation on all equipment in theater. The Corps RC TECHINT sections at the CMEC conduct this level on equipment that matched the MOSs in their elements. The TECHINT collection teams are prepared to do this, but normally would not do it on a large scale.

Preliminary requirements for exploitation include—

- Preliminary photographs of CEM outside and inside (to shows status of equipment before assessment).
- An inventory.
  - — Examine system for any written information (documents, operator manuals, maps), markings, data plates, or operating instructions.
  - — Identify all individual equipment components requiring separate analysis.
- If equipment requires further analysis beyond initial exploitation, begin planning for further detailed exploitation with national S&TI personnel.

- The exploitation, with finished report, is accomplished within 48 hours.

The JCMEC normally is the primary center for all detailed exploitations in theater.

Once the general exploitation is accomplished, a more detailed exploitation begins. This is in coordination with the national S&TI SME at the JCMEC. The plan is provided by the national S&TI community.

The JCMEC maintains in the Exploitation Company detailed exploitation plans for collection priority equipment. These plans are part of the contingency database for the threat equipment. The time limit for a detailed exploitation is determined by the tactical needs of the theater and national requirements.

Appendix G

FOREIGN LANGUAGE TEXT RECOGNITION

INTRODUCTION

When TECHINT personnel are able to correctly identify foreign languages used in documents or equipment, it has two immediate benefits. First, it helps identify the equipment or type of document and where or who is using it. Second, it ensures that TECHINT personnel request the correct linguistic support.

This appendix contains language identification hints that will enable TECHINT personnel to quickly identify some of the many languages used in documents, on equipment plates, and on other materiel. TECHINT personnel can speed up the entire battlefield TECHINT process by following the guidance herein.

The language identification hints were compiled by NGIC. There are thousands of languages and dialects in use in the world today; therefore, this material is not complete. The following include examples of the use of language identification during TECHINT operations.

- A TECHINT team discovers an ADA system that looks like a Russian ZPU-4 ADA gun. But on closer examination, the technical analysis identifies Chinese characters on a data plate and on the tires. This could mean that this ADA gun is from China, and this observation needs to be reported to TECHINT elements and to the CMEC.

- TECHINT personnel find a document in Arabic, but the country they are in speak and write only Spanish. This document could be of intelligence value and would require being reported to TECHINT elements and to document exploitation (DOCEX) personnel.

LANGUAGE SYSTEMS

The world's written languages can be divided into alphabet languages and character languages. The only present-day character system is the Chinese system, which has been borrowed by other languages. But there are many alphabets. The most important alphabets currently in use are—

- The Roman alphabet (used by English and many other languages).

- The Cyrillic alphabet (used by Russian, some other Slavic languages, and most of the minority languages of Russia).

- The Arabic alphabet (used in the Middle East and other areas influenced by Islam).

Other alphabets exist, but their use is more restricted. (Figure G-1 shows some of these spoken languages and some of the locations where they are spoken.)

- The Hebrew alphabet for Hebrew and Yiddish; the Greek alphabet for Greek.

- The Devanagari alphabet for Sanskrit and other languages of India.

In addition, there are special alphabets for languages like Georgian, Telugu, the other Dravidian languages in southern India, Laos, and other languages in southeast Asia, and Amharic in Ethiopia.

Illustrations of the main alphabets are normally available in standard desktop dictionaries. Many unusual scripts are illustrated in Romanization Guides, revised and enlarged edition, put out by the Office of the Geographer, Directorate for Functional Research, Bureau of Intelligence and Research, US Department of State, and the US Board on Geographic Names, dated 1 April 1972.

Reliable detailed information about foreign languages for people who cannot actually read them is available in manuals compiled for professional librarians. These manuals can be found at your local library.

ROMAN ALPHABET LANGUAGES

The most complex language recognition problem is to distinguish between the numerous languages that use the Roman alphabet. The 26-letter alphabet is used here as the basic alphabet. The other Roman alphabet languages use these same letters, but many use fewer than 26 and a few use more.

Unfortunately, just because a letter is not used is not a very useful language recognition criterion. This is because it is difficult to know whether a letter is absent because it is never used or because it simply was not needed to write the text in question.

Language	Location
Chinese	People's Republic of China, Taiwan, Hong Kong, Thailand
English	United States, Canada, Great Britain, Ireland, Australia, New Zealand
Spanish	Spain, South America, Central America, Mexico
Hindi	North Central India
Russian	Soviet Union, Europe
Arabic	Saudi Arabia, Yemen, South Yemen, United Arab Emirates, Oman, Kuwait, Bahrain, Qatar, Iraq, Syria, Jordan, Lebanon, Egypt, Sudan, Libya, Tunisia, Algeria, Morocco
Portuguese	Portugal, Brazil, Africa, Asia
Japanese	Japan
German	Germany, Austria, Switzerland
Urdu	Pakistan, India
French	France, Belgium, Switzerland, Canada, Morocco, Tunisia, Algeria, Lebanon, Syria, Laos, Cambodia, Vietnam
Korean	Korea, China, Japan
Italian	Italy, Switzerland
Vietnamese	Vietnam
Turkish	Turkey, Bulgaria, Greece, Cyprus
Persian (Farsi, Dari)	Iran, Afghanistan (Tadzhik, USSR)
Polish	Poland, United States, Soviet Union
Ukrainian	Ukrainian SSR
Rumanian	Romania, Moldavian SSR
Serbian (Croatian)	Yugoslavia
Pashto	Afghanistan, Northwest Pakistan
Czech (Slovak)	Czechoslovakia
Dutch	Netherlands, Suriname, Belgium
Hungarian	Hungary, Romania, Czechoslovakia, Yugoslavia
Danish (Norwegian)	Denmark, Norway
Bulgarian	Bulgaria
Swedish	Sweden
Belorussian	Belorussian SSR
Finnish	Finland
Albanian	Albania, Yugoslavia
Lithuanian	Lithuanian SSR
Latvian	Latvian SSR
Slovenian	Slovenia (Northwest Yugoslavia)
Estonian	Estonian SSR
Macedonian	Macedonia (Yugoslavia)

Figure G-1. A partial list of spoken languages and locations where they are spoken.

Five of the letters <a, e, i, o, u> are referred to collectively as "vowels," while the rest are called collectively "consonants." The rules designating letters as vowels or consonants vary from language to language. Some languages, for instance, consider <l>, <r>, or <y> to be vowels. Most of the Roman alphabet languages modify letters by putting extra marks above, in, or below them. **These marks are called diacritics. They are among the best criteria for language recognition.**

DIACRITICS

Figure G-2 shows the principal diacritics used by various languages to modify the Roman alphabet. Figure G-3 shows the languages that use these diacritics. It also summarizes the occurrence of various diacritics in selected Roman alphabet languages and gives examples of letters with diacritics on them. The diacritics are divided into three groups, depending on whether they are written above, in, or below the letter. They are given standard names for convenience; their actual names vary from language to language.

DIACRITICS ABOVE THE LETTER

Grave	<` >	Acute	<´>	Circumflex	<^>
Hacek	<ˇ>	Breve	<˘ >	Macron	<¯>
Tilde	<~>	Krouzek	<°>	Dot	<˙>
Dieresis	<u>	Double Acute	<˝>	Apostrophe	<'>
Question	<?>	Umlaut	<ä>	Back Apostrophe	<ë>

DIACRITICS IN THE LETTER

Bar	<->	Slash	</>	Horn	<’ >

DIACRITICS UNDER THE LETTER

Cedilla	<î>	Ogonek	< >	Comma	<,>
		Low Dot	<.>		

Figure G-2. Table of diacritics.

WESTERN EUROPEAN LANGUAGES

Western European languages include those commonly called Romance and Germanic languages.

DIACRITICS WRITTEN ABOVE THE LETTER	
<`> grave:	French, Italian, Portuguese, Vietnamese, e.g., <à>
<´>acute:	Croatian, Czech, French, Greek, Hungarian, Italian, Polish <N, O, S, C, Z>, Slovak, Spanish, Portuguese, Vietnamese; e.g., <á, ó>
<^> circumflex:	French, Italian, Portuguese, Rumanian, Vietnamese, Turkish, e.g.,<â, ô>
<v> hacek:	Croatian, Czech, Estonian, Latvian, Lithuanian <S, Z, C>,Slovak, Slovenian, e.g., <č, ě>
< > breve:	Rumanian, Turkish, Vietnamese; e.g., <ă, ğ>
<¯ > macron:	Latvian, Lithuanian; e.g., <ā, ū>
<~> tilde:	Estonian, Portuguese, Spanish, Vietnamese; e.g., <ã, ñ>
<°> krouzek:	Czech, Danish, Norwegian, Swedish; e.g., <å, e>
<.> dot:	Lithuanian <e>, Polish, Turkish, e.g., <ė, ż>
<u> dieresis:	Albanian, Estonian, Finnish, French, German, Hungarian, Slovak, Portuguese <ü>, Spanish, Swedish, Turkish; e.g., <ä, ë>
<"> double acute:	Hungarian; e.g., <ő, ű>
<'> apostrophe:	Czech, French, Slovak; e.g., <ď, ť>
<?> question:	Vietnamese; e.g., <a, e>
<{> back apostrophe:	Latvian; e.g., <g>
DIACRITICS WRITTEN IN (OR TOUCHING) THE LETTER	
<-> bar:	Croatian, Polish, Vietnamese; e.g., <d,1, a>
</> slash:	Danish, Norwegian, Polish; e.g., <1, 0>
<»> horn:	Vietnamese; e.g., <ũ, õ>
DIACRITICS WRITTEN UNDER THE SEAT	
<¸> cedilla:	Albanian, French, Portuguese, Turkish, e.g., <ç, ş>
<˛> ogonek:	Lithuanian
<,> comma:	Latvian, Rumanian; e.g., <k, ş>
<.> low dot:	Vietnamese; e.g., <a, e>

Figure G-3. The occurrence of diacritics in various languages.

DISTINGUISHING FRENCH, GERMAN, AND DUTCH

FRENCH:

French is generally easiest to recognize because it is so familiar and has so many words in common with English. French uses acute <´> and grave <`> on <e>. Acute is not used on any other letters, but grave is used occasionally on <a> and <u>. Circumflex <^> is used on <a, e, i, o, u> and cedilla <¸> is used under <c>. The French commonly omit diacritics over capital letters and in typescript. Definite article forms: le, la, les. French also uses a trëma <oe, ï, ë>.

GERMAN:

German uses the umlaut <¨u> on <a, o, u>. This is the language's only diacritic. German also uses a special letter, the Eszett < >, which does not begin a word. In regular prose, capitalization is rather frequent since all nouns are capitalized. Definite article forms: der, die, das, des, dem, den.

DUTCH:

Dutch can be mistaken for German; however, Dutch does not capitalize its nouns in regular prose. Dutch adopted a few diacritical forms from the French language. These include: acute <een>; grave <crepe>; apostrophe <'t, z'n, d'r, etc.>; dieresis <België>; and sometimes the cedilla <¸>. Definite article forms: de and het.

DISTINGUISHING SPANISH, PORTUGUESE, AND ITALIAN

For Spanish, look for acutes occasionally over vowels, tilde <~> over <n> but not over vowels, no grave accents, and words that end in <n>. For Portuguese look for the tilde over <a> and <o> but not over <n>, the cedilla under <c>, and some words that end in <m>. For Italian look for occasional graves over vowels, no tildes or cedillas, and numerous doubled consonants; for example, <tt>, <gg>, <pp>, <vv>, and so forth. Of course, look for the definite articles; they are frequently used and mostly different in the three languages.

SPANISH:

Spanish uses acute <´> on vowels <a, e, i, o, u> and tilde <~> on <n>. Since the acute marks irregular word accent, there will normally be no more than one acute per word and it will appear on the last vowel or third from last vowel. Dieresis <¨u> is used occasionally over <u>. Grave <`> and circumflex <^> are not used. Definite article forms: el, la, los, las.

PORTUGUESE:

Portuguese uses acute <'>, grave <'>, and circumflex <^> occasionally over vowels, and tilde <~> frequently over <a> and <o>. Cedilla < ¸> is used under <c>. Dieresis <¨u> is used over vowels occasionally. Definite article forms: o, os, a, as.

ITALIAN:

Italian uses acute <´> on <e> and grave <`> on vowels <a, e, i, o, u> to indicate unusual accent. Some type fonts may substitute circumflex <^> for grave. Normally there will be no more than one grave per word, and it will appear on the last vowel or third from last vowel. Definite article forms: il, lo, i, gli, la, le.

NORTHERN EUROPEAN LANGUAGES

Northern European languages include North Germanic and Slavic, as well as unique languages of the Finno-Ugric family. The distinguishing features of each are described below.

SWEDISH:

Swedish uses dieresis <¨u> on <a> and <o> and krouzek <^{O}> on <a>. A frequent word is och; meaning "and."

DANISH AND NORWEGIAN:

Danish and Norwegian use the same alphabet as Swedan. They use krouzek <^{O}> on <a> and slash </> on <o>, and a special letter, the ae digraph <Æ, æ>. Written Danish and Norwegian are difficult to tell apart, but anyone who can read one can make sense out of the other. A frequent word in both languages is og; meaning "and."

FINNISH:

Finnish is very different from the other northern European languages, but it is similar to Estonian. Finnish uses dieresis <¨u> on <a> and <o>. About 60 percent of the average text consists of vowels (including <y>). Look for frequent double vowels; <aa>, <ee>, <ii>, etc.

ESTONIAN:

Estonian uses tilde <~> on <o>, dieresis <¨u> on <a, o, u>, and hacek <^{V}> on <s, z> infrequently in foreign words. At first glance Estonian looks very much like Finnish, and both are of the Finno-Ugric family. To tell the two languages apart, look for <y> (Finnish) or <u> with dieresis (Estonian).

HUNGARIAN:

Hungarian uses acute <´> on <a, e, i, o, u>, dieresis <¨u> on <o, u>, and double acute <˝> on <o, u>. These three diacritics are very frequent and should all appear in an average paragraph. Definite article forms: a, az. Although not Northern European, Hungarian is listed here because it is in the Finno-Ugric family.

ROMAN ALPHABET SLAVIC LANGUAGES

It is often difficult to distinguish between the Roman alphabet Slavic languages. Of these languages, Polish is easiest to distinguish from the rest because it does not use hacek <^{V}>, whereas the others do; and because it uses <w> frequently and <v> almost never, whereas the opposite situation occurs in the other languages.

The languages of Czechoslovakia—Czech and Slovak—can be distinguished from the Roman alphabet languages of the former Yugoslavia, Croatia, and Serbia because Czech and Slovak use acute <'> on vowels (including <y>) and Croatian and Slovenian do not. Acutes are so frequent in Czech and Slovak that the absence of acutes in an average-length sentence can be taken as a valid negative test.

The presence of the diacritics listed above for Croatian indicate that it may be Croatian; but there is no convenient way to test for Slovenian against Croatian. If in doubt between Croatian and Slovenian, assume Croatian unless it can be established that the text was published in Ljubljana.

POLISH:

Polish uses acute <´> on <c, n, o, s, z>; ogonek <˛> on <a, e>; bar <-> (occasionally depending on font as a substitute for slash) on <L,1, Z>, such as <L, 1, Z>; and < > dot on <z>. Letters <w> and <z> are very frequent in Polish, and the <v> almost never occurs.

CZECH:

Czech uses acute <´> on <a, e, i, o, u, y>, hacek <^{V}> on <c, d, e, n, r, s, t, z>, krouzek <^{O}> on <u>. The letter <r> with hacek is frequent in Czech and lacking in Slovak.

SLOVAK:

Slovak uses acute <´> on <a, e, i, l, r, o, u, y>; dieresis <¨> on <a>; circumflex <^> on <o>; hacek <^{V}> on <c, d, l, n, s, t, z>; and apostrophe <'> on <d, l, t>. The digraph <ie> is fairly frequent in Slovak and very infrequent in Czech. Slovak is used in eastern Czechoslovakia. Suspect Slovak if Bratislava is the origin.

CROATIAN:

Croatian uses acute <´> on <c>, hacek <^{V}> on <c, s, z>, and bar <-> on <d>. Croatian is used in northern and coastal Yugoslavia around the city of Zargreb.

SLOVENIAN:

Slovenian uses hacek <ˇ> on <c, s, z> and no other diacritics. Slovenian is used in extreme northwest Yugoslavia around the city of Ljubljana.

RUMANIAN:

Rumanian uses breve <ˇ> on <a>, circumflex <^> on <a, i>, and comma <,> under <s, t>.

ALBANIAN:

Albanian uses dieresis <u> on <e> and cedilla <¸> under <c>. The <e> with dieresis is very common. Another recognition mark of Albanian is the use of <q> without <u>.

LITHUANIAN:

Lithuanian uses hacek <ˇ> on <c, s, z>, macron <¯> on <u>, dot < > on <e>, and ogonek <˛> under <a, e, i, u>. The frequent occurrence of ogonek is a good recognition sign for Lithuanian.

LATVIAN:

Latvian uses hacek <ˇ> on <c, s, z>, macron <¯> on <a, e, i, o, u>, and comma <,> under <k, l, n>. Comma is also used under <G> (upper case letter only), while back apostrophe <`> is used on <g> (lower case letter only). In this case the two marks are variant forms of the same diacritic. The macrons and commas are a good recognition sign for Latvian.

OTHER ROMAN ALPHABET LANGUAGES

Turkish and Vietnamese use the Roman alphabet with unusual diacritics.

TURKISH:

Turkish uses breve <ˇ> on <g>, dieresis <u> on <o, u>, and cedilla <¸> on <c>. Turkish has two forms of the letter <i>. One has the upper case < > and a corresponding lower < > that looks like an "i" without the dot.
The other letter has the lower case form <i> (the same as English) and a corresponding upper case form that looks like English " " with a dot < >.
Turkish also uses circumflex <^ > <latif> <lugat>.

VIETNAMESE:

Vietnamese uses a very complex system of diacritics. It uses breve <ˇ> on <a>, circumflex <^> on <a, e, o>, horn <˝> on <o, u>, and bar <-> on <d>. In addition to these, the following five diacritics are used with vowels to indicate tone: grave <`>, acute <´>, low dot <.>, question <?>, and tilde <~>. Vowels with breve, circumflex, and horn can, and often do, have a tone diacritic. So, in Vietnamese, one letter can have two diacritics on it.

CYRILLIC ALPHABET LANGUAGES

The Cyrillic alphabet is used to write Russian, Ukrainian, Belorussian, and many minority languages from the former Soviet Union. It is also used to write Bulgarian and Serbian. The Cyrillic alphabet and the Roman alphabet are both derived from forms of the Greek alphabet so there is a general resemblance. Some Cyrillic letters seem to Americans to be backwards or oddly shaped. Figure G-4 shows the characters and diacritics not found in Russian. With the exception of one letter, , which is only used sometimes in Russian, none of these letters appear in the normal Russian text.

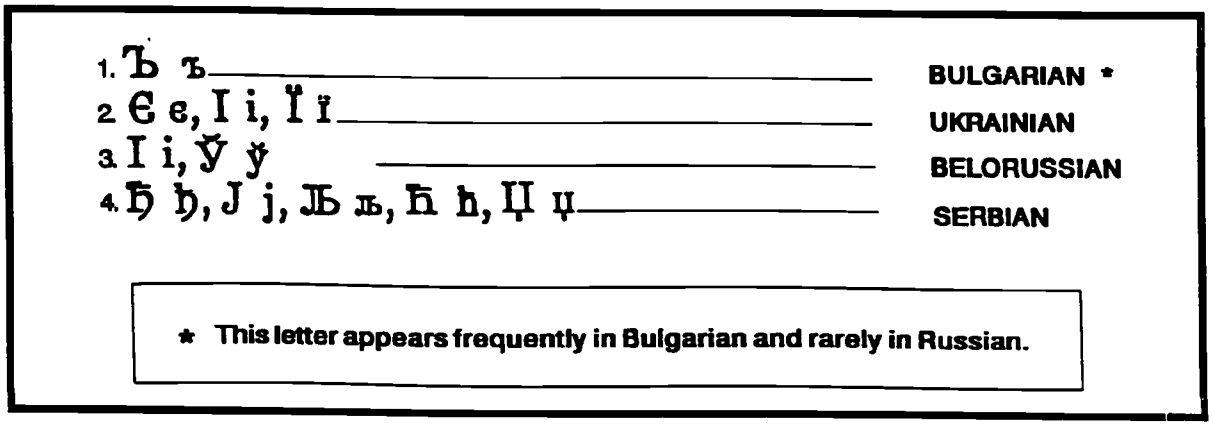


Figure G-4. Distinguishing major Slavic languages from Russian.

SLAVIC LANGUAGES:

Figure G-4 gives the simplest recognition guide for identifying documents that look like Russian but are actually other Slavic languages or minority languages.

TRANSLITERATION:

Figure G-5 shows the different forms of the Cyrillic alphabet for five principal Cyrillic alphabet languages and the recommended transliterations for each letter. Pay particular attention to the transliteration of Russian. These equivalents must be used when reporting on materiel bearing Russian nameplates. DO NOT REPORT ON FOREIGN EQUIPMENT AND DOCUMENTS USING THE ORIGINAL CYRILLIC CHARACTER. The Figure classifies each letter as "C" for consonant or "N" for nonconsonant.

RUSSIAN:

Russian is the most frequently encountered Cyrillic alphabet language and should always be the prime suspect. The key to recognizing Russian is the fact that it uses both letter 12 and letter 39 and does not use letter 13 at all. (See Figure G-5.)

BULGARIAN:

Bulgarian is perhaps the second most frequently encountered Cyrillic alphabet language and the most difficult for the nonspecialists to differentiate from Russian. Bulgarian uses fewer letters than Russian.

NOTE: In the following discussion, the letters are referred to by their numbers on the chart in Figure G-5.

For example, a letter used often in Russian and never in Bulgarian is the letter 39; however, the way to be sure that it is not Bulgarian is to see if the letter 38 comes before a consonant or "C" letter. Note that letter 38 is frequent in Bulgarian and rare in Russian; moreover, when letter 38 occurs in Russian, it always occurs before an "N" letter.

Proper transliteration is very important. When an analyst reads a Russian nameplate and writes down P-105A, but it is actually an R-105D (P is not P, rather "R," and < > is wrongly symbolized by A); then it results in incorrect reporting.

The column in Figure G-5 marked "Other" is not supplied with any transliteration equivalents. This column contains similar letters that are encountered in the written languages of various minority nationalities in the former USSR. These languages belong mainly to the Uralic family or the Altaic family, and a Russian linguist will be unable to make any sense out of them. Recognition of any documents in these languages as non-Slavic is a helpful first step in DOCEX.

No.	Russian		Ukrainian		Belorussian		Bulgarian		Serbian		Other
1. N	А а	a	А а	a	А а	a	А а	a	А а	a	Ă ă Ā ā Ӕ ӕ
2. C	Б б	b	Б б	b	Б б	b	Б б	b	Б б	b	-
3. C	В в	v	В в	v	В в	v	В в	v	В в	v	-
4. C	Г г	g	Г г	g	Г г	g	Г г	g	Г г	g	Ґ ґ Ѓ ѓ
5. C	Д д	d	Д д	d	Д д	d	Д д	d	Д д	d	-
6. C	-	-	-	-	-	-	-	-	Ђ ђ	đ	-
7. N	Е е	e/ye	Е е	e	Е е	e/ye	Е е	e	Е е	e	Ё ё Ə ə
8. N	Ё е	ë/yë	-	-	Ё е	ë/yë	-	-	-	-	-
9. N	-	-	Є є	ye	-	-	-	-	-	-	-
10. C	Ж ж	zh	Ж ж	zh	Ж ж	zh	Ж ж	zh	Ж ж	ž	Ӂ ӂ Ӝ ӝ
11. C	З з	z	З з	z	З з	z	З з	z	З з	z	Ӟ ӟ Ҙ ҙ
12. N	И и	i	И и	y	-	-	И и	i	И и	i	Й й Й й
13. N	-	-	І і	i	І і	i	-	-	-	-	І і І і
14. N	-	-	Ї ї	yi	-	-	-	-	-	-	-
15. C	Й й	y	Й й	y	Й й	y	Й й	y	-	-	-
16. C	-	-	-	-	-	-	-	-	-	-	-
17. C	К к	k	К к	k	К к	k	К к	k	Ј ј	j	-
18. C	Л л	l	Л л	l	Л л	l	Л л	l	К к	k	Қ қ Ҡ ҡ
19. C	-	-	-	-	-	-	-	-	Л л	l	Љ љ
20. C	М м	m	М м	m	М м	m	М м	m	Љ љ	lj	-
21. C	Н н	n	Н н	n	Н н	n	Н н	n	М м	m	-
22. C	-	-	-	-	-	-	-	-	Н н	n	Ң ң Ҥ ҥ Ӈ ӈ
23. N	О о	o	О о	o	О о	o	О о	o	Њ њ	nj	-
24. C	П п	p	П п	p	П п	p	П п	p	О о	o	Ӧ ӧ Ө ө Ꙩ ꙩ
25. C	Р р	r	Р р	r	Р р	r	Р р	r	П п	p	-
26. C	С с	s	С с	s	С с	s	С с	s	Р р	r	-
27. C	Т т	t	Т т	t	Т т	t	Т т	t	С с	s	Ҫ ҫ
28 C	-	-	-	-	-	-	-	-	Т т	t	Ҭ ҭ
29. N	У у	u	У у	u	У у	u	У у	u	Ћ ћ	ć	-
30. C	-	-	-	-	Ў ў	w	-	-	У у	u	Ӯ ӯ Ӱ ӱ Ӳ ӳ
31. C	Ф ф	f	Ф ф	f	Ф ф	f	Ф ф	f	-	-	Ү ү Ѵ ѵ Ѷ ѷ
32. C	Х х	kh	Х х	kh	Х х	kh	Х х	kh	Ф ф	f	-
33. C	Ц ц	ts	Ц ц	ts	Ц ц	ts	Ц ц	ts	Х х	h	Ҳ ҳ
34. C	Ч ч	ch	Ч ч	ch	Ч ч	ch	Ч ч	ch	Ц ц	c	-
35. C	-	-	-	-	-	-	-	-	Ч ч	č	Ҷ ҷ Ӌ ӌ Ҹ ҹ
36. C	Ш ш	sh	Ш ш	sh	Ш ш	sh	Ш ш	sh	Џ џ	dž	h h
37. C	Щ щ	shch	Щ щ	shch	-	-	Щ щ	sht	Ш ш	š	-
38. N	Ъ ъ	"	-	-	-	-	Ъ ъ	ŭ	-	-	-
39. N	Ы ы	y	-	-	Ы ы	y	-	-	-	-	-
40. N	Ь ь	'	Ь ь	'	Ь ь	'	Ь ь	'	-	-	-
41. N	Э э	e	-	-	Э э	e	-	-	-	-	Ы ы
42. N	Ю ю	yu	Ю ю	yu	Ю ю	yu	Ю ю	yu	-	-	-
43. N	Я я	ya	Я я	ya	Я я	ya	Я я	ya	-	-	-

Figure G-5. Cyrillic alphabet and transliteration chart.

NOTES:

1. The letters are numbered sequentially for ease of reference. The alphabetic order given is the convenient one, which is not necessarily the traditional one.

2. The letters marked "N" are nonconsonants; and the letters marked "C" are consonants.

3. Letters 7 and 8 have alternate transliterations for Russian and Belorussian. In all cases, the first transliteration is used when the letter occurs after a "C" letter; the second transliteration is used in all other cases, including when the letter begins the word.

4. Letter 8 is not considered a separate letter and its dieresis is often omitted.

5. Letter 4 is pronounced something like "h" in Ukrainian and Belorussian and "h" is often the recommended transliteration. However, transliteration "g" is recommended here to eliminate confusion with the letters transliterated "sh" and "zh."

6. The "Other" category refers to various minority languages in the Soviet Union, many of which are Uralic or Altaic languages.

Figure G-5. Cyrillic alphabet and transliteration chart (continued) .

UKRAINIAN:

Ukrainian is distinguished by the use of letters 12 and 13 and the non-use of letter 39. Letters 9 and 14 also are unique to Ukrainian, but their frequency is low and their absence may be accidental. When Ukrainian is identified, pay particular attention to the transliteration of letter 12. The recommended transliteration for letter 4 is "g" even though its pronunciation is closer to English "h."

BELORUSSIAN:

Belorussian is distinguished by the use of letters 13 and 39 and the non-use of letter 12. Letter 30 is unique to Belorussian, but its frequency is not high enough to use it as an identification sign. As in Ukrainian, letter 4 in Belorussian is transliterated "g" and pronounced like "h."

SERBIAN:

Serbian is spotted easily by the several unique letters it uses: letters 6, 16, 19, 22, 28, and 35. Serbian is conventionally transliterated into Croatian, and this is what the chart gives. The diacritics of the Croatian script are discussed in the **"ROMAN ALPHABET LANGUAGES"** section above.

MACEDONIAN:

Macedonian is spoken by perhaps two million people in southeastern Yugoslavia. The Macedonian alphabet is similar to the Serbian, except that letters 6 and 28 are not used and three other letters are added. The added letters are letter 4 with an acute <ˉ>, letter 17 with an acute <ˉ>, and <S, s>. Macedonian language documents are rare.

ARABIC ALPHABET LANGUAGES

The Arabic alphabet has generally followed the spread of Islam and has been used to write numerous languages, some of which (notably Turkish) no longer use it. This alphabet, appropriately modified, currently is used for all the dialects of Arabic and for Persian, Urdu, and other Indo-Iranian languages, such as Dari, Pashto, and Kurdish. The Russian and Cyrillic alphabets seem even more related to one another when compared to Arabic.

ARABIC AND PERSIAN:

The best distinction a nonlinguist can make is to separate Persian documents from Arabic documents. Persian linguists cannot read Arabic, and vice versa, unless they know both languages.

ARABIC:

Arabic is spoken over a large area extending from Morocco on the west to borders of ancient Persia (modern Iran) on the east. The spoken language varies widely in this area, but the written language is fairly standard. Only a specialist could hope to distinguish the varieties of Arabic, but a sharp-eyed nonlinguist can learn to recognize Arabic and distinguish it from Persian. The best indication is perhaps the presence of letter 32, which is not used in Persian. The next best indication is perhaps the frequent occurrence of the definite article < >, which is spelled with letter 1 (initial) and letter 27 (initial). A final characteristic is the absence of the special Persian letters: letters 3, 7, 14 , and 26. Since this is a negative indication, however, it cannot be used by itself to prove that a text is Arabic.

PERSIAN:

Persian is used in Iran. It is indicated by the presence of the special Persian letters 3, 7, 14, and 26, and by the absence of letter 32. Other indications are a paucity of letter 1 and 27 combinations (the Arabic definite article) and a slightly different preference in numeral usage.

ARABIC NUMERALS:

In school, the numerals used in the United States and most of the rest of the world are often called "Arabic numerals," but these are not the same forms used in Arabic alphabet languages. The real Arabic numerals are illustrated in Figure G-6. This figure also shows Arabic and Persian variants of the numerals along with their international equivalents. Unlike the Arabic alphabet (which is, of course, read from right to left), **ARABIC NUMERALS ARE READ FROM LEFT TO RIGHT, THE SAME WAY AS OUR OWN NUMERALS ARE READ.**

Document collectors should familiarize themselves with the Arabic numerals so they can read page numbers in collected documents and properly reassemble documents that have come apart. Collectors should remember that one of the results of the right-to-left orientation of the Arabic alphabet is that the apparent "back" of a document is actually the front.

Figure G-7 illustrates the Arabic alphabet in its Arabic and Persian variants. Notice that each letter has four forms, labeled "alone," "final," "medial," and "initial." Notice that "initial" is to the right of "final." These column labels indicate two of the main differences between Arabic script and Roman script: First, the letters change in order to connect to other letters, and second, **THE SCRIPT IS WRITTEN FROM RIGHT TO LEFT.**
The letters with asterisks by their numbers cannot connect to a following letter. The initial form is used to begin a word or when the letter follows a nonconnectable letter. The medial form is used after a connectable letter or when it is used by itself; for example, to letter paragraphs in a document.

DIACRITICS:

Another feature of the Arabic alphabet is the use of diacritics to differentiate many of the letters. Figure G-8 illustrates the diacritics used in Arabic and Persian.

Using Figures G-7 and G-8, note that letters 2, 3, 4, 5, 29, and (partially) 33 have the same base form with the following diacritics: high dot < ˙>, letter 29; low dot <**$**>, letter 2; high double dot <¨>, letter 4; low double dot <‗>, letter 33, initial and medial only; high triple dot < ˆ>, letter 5; and low triple dot <‡>, letter 3.

Letter 8 is the base form for another diacritic set: High dot < ˙>, letter 9; low dot <**$**>, letter 6; low triple dot **<**‡>, letter 7. Letter 10 is the base form, and letter 11 adds high dot < ˙>. Letter 12 is the base form. A Letter 13 adds high dot < ˙>, and letter 14 adds high triple dot < ˆ>. Letter 15 is the base form and letter 16 adds high triple dot < ˆ>.

International	Arabic	Persian	International	Arabic	Persian
0	٠	٥ or ٠	6	٦	۶ or ٦
1	١	١	7	٧	٧
2	٢	٢	8	٨	٨
3	٣	٣	9	٩	٩
4	٤	۴ or ٤	10	١٠	١٥ or ١٠
5	٥	۵ or ٥	20	٢٠	٢٥ or ٢٠

Figure G-6. International, Arabic, and Persian numbers.

Letters 17, 19, and 21 are the base forms for letters 18, 20, and 22 respectively; the added diacritic for all three is high dot <˙>. Letters 23 and 24 have approximately the same base form with high dot <˙> on letter 23 and high double dot <¨> on letter 24. Letters 25 and 26 have the same base form. Letter 25 uses flag <´> on its initial and medial forms and hamza sign <À> on its final and alone forms.

Letter 26 uses double flag <˝> on all its forms and hamza sign <¸> on its final and alone forms. Letter 31 is the base form, and letter 32 uses high double dot <¨>. For grammatical reasons, letter 32 is not used initially or medially.

SAMPLES OF ARABIC AND PERSIAN

Figure G-9 gives a sample of printed Arabic. Note the frequent occurrences of letter 1 and letter 27: the definite article at word beginnings. Remember, words begin on the right. The seventh line from the top, for instance, has four obvious occurrences and two other occurrences in modified forms that have not been discussed here. There are 18 occurrences of letter 32, at least one occurrence in every line except lines 9 and 11 and four occurrences in lines 3 and 8.

No.	Arabic				Persian			
	Alone	Final	Medial	Initial	Alone	Final	Medial	Initial
1.	ا	ا	ا	ا	ا	ا	ا	ا
2.	ب	ب	ب	ب	ب	ب	ب	ب
3.	-	-	-	-	پ	پ	پ	پ
4.	ت	ت	ت	ت	ت	ت	ت	ت
5.	ث	ث	ث	ث	ث	ث	ث	ث
6.	ج	ج	ج	ج	ج	ج	ج	ج
7.	چ	چ	چ	چ	چ	چ	چ	چ
8.	ح	ح	ح	ح	ح	ح	ح	ح
9.	خ	خ	خ	خ	خ	خ	خ	خ
10.	د	د	د	د	د	د	د	د
11.	ذ	ذ	ذ	ذ	ذ	ذ	ذ	ذ
12.	ر	ر	ر	ر	ر	ر	ر	ر
13.	ز	ز	ز	ز	ز	ز	ز	ز
14.	-	-	-	-	ژ	ژ	ژ	ژ
15.	س	س	س	س	س	س	س	س
16.	ش	ش	ش	ش	ش	ش	ش	ش
17.	ص	ص	ص	ص	ص	ص	ص	ص
18.	ض	ض	ض	ض	ض	ض	ض	ض
19.	ط	ط	ط	ط	ط	ط	ط	ط
20.	ظ	ظ	ظ	ظ	ظ	ظ	ظ	ظ
21.	ع	ع	ع	ع	ع	ع	ع	ع
22.	غ	غ	غ	غ	غ	غ	غ	غ
23.	ف	ف	ف	ف	ف	ف	ف	ف
24.	ق	ق	ق	ق	ق	ق	ق	ق
25.	ك	ك	ك	ك	ك	ك	ك	ك
26.	-	-	-	-	ک	ک	ک	ک
27.	ل	ل	ل	ل	ل	ل	ل	ل
28.	م	م	م	م	م	م	م	م
29.	ن	ن	ن	ن	ن	ن	ن	ن
30.	و	و	و	و	و	و	و	و
31.	ه	ه	ه	ه	ه	ه	ه	ه
32.	ة	ة	-	-	-	-	-	-
33.	ى	ى	ى	ى	ى	ى	ى	ى

Figure G-7. The Arabic alphabet.

< ◌̇ > High Dot	< ◌̈ > High Double Dot	< ◌⃛ > High Triple Dot
< ◌̣ > Low Dot	< ◌̤ > Low Double Dot	< ◌̰ > Low Triple Dot
< ◌̄ > Flag High	< ◌̋ > Double Flag High	< ◌ٔ > Hamza Sign Persian
< ◌̱ > Flag Low	< ◌̳ > Double Flag Low	< ◌ٕ > Hamza Sign Arabic

Figure G-8. The diacritics of Arabic and Persian.

وفضـلا عن ذلـك فلقد كان فى كل القوانين القائمة ما يكفى لمواجهة الأحداث والاضطرابات التى وقعت وكذلك للنظر فى أمر ما نسبه رئيس الجمهورية فى خطابه إلى أحزاب الأقلية ، وإلى الجماعات الإسلامية ، وإلى بعض الشخصيات المدنية المسلمة ، والمسيحية . . فالقـوانين القائمة تكفل الحفاظ على أمن البلاد وسلامتها ضد ما يهدد وحدتها الوطنية من أخطار وبالتالى فان القرار المطعون فيه لايمكن أن يعتبر - بحال - عملا من أعمال الضرورة - كما أن القرار المطعون فيه خالف صريح نص المادة ٤١ من الدستور التى تنص على عدم جواز القبض أو تقييد الحريات فى غير حالة التلبس إلا بأمر من القـاضى المختص أو النيابـة العامة ، تستلزمه ضرورةالتحقيق وصيانة أمن المجتمع وفقا لأحكام القانون - وأنه لم يرد فى أوراق الدعوى أى دليل على أن المتحفظ عليهم ضبطوا فى حالة تلبس أو أنه أجرى معهم تحقيق سابق على التحفظ ، حتى يتضح منه أن هذا التحفظ كان اجراء لازما .

Figure G-9. Printed Arabic.

Figure G-10 illustrates typewritten Arabic. Note that lines 1, 2 5, and 10 begin (on the right) with the definite article (letter 1 and letter 27). There are 20 other obvious occurrences of these letters at the beginning of words and several others that are less obvious. Lines 1, 2, and 9 end (on the left) with letter 32. Letter 32 occurs five other times in the sample. Arabic script permits some letters to be stretched in order to even out text on the left. The long lines at the left of the sample are instances of this.

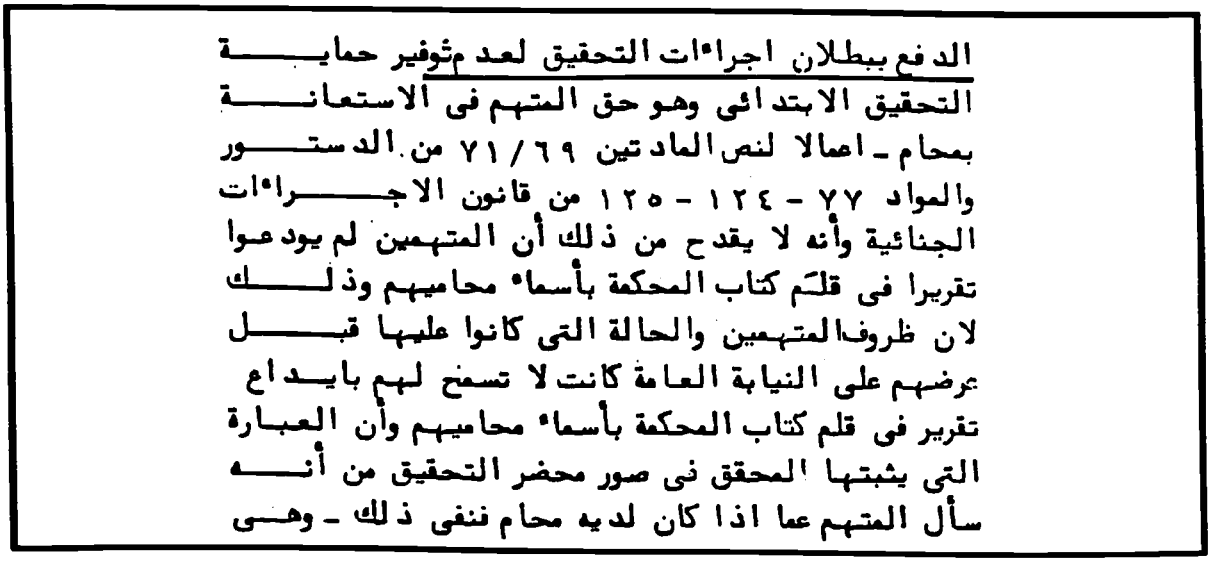

الدفع ببطلان اجراءات التحقيق لعدم توفير حماية
التحقيق الابتدائي وهو حق المتهم في الاستعانة
بمحام - اعمالا لنص المادتين ٦٩ / ٧١ من الدستور
والمواد ٧٧ - ١٢٤ - ١٢٥ من قانون الاجراءات
الجنائية وأنه لا يقدح من ذلك أن المتهمين لم يودعوا
تقريرا في قلم كتاب المحكمة بأسماء محاميهم وذلك
لان ظروف المتهمين والحالة التي كانوا عليها قبل
عرضهم على النيابة العامة كانت لا تسمح لهم بايداع
تقرير في قلم كتاب المحكمة بأسماء محاميهم وأن العبارة
التي يثبتها المحقق في صور محضر التحقيق من أنه
سأل المتهم عما اذا كان لديه محام فنفى ذلك - وهي

Figure G-10. Typewritten Arabic.

Figure G-11 illustrates printed Persian. Note the double flags <˝>, two in the first line and eight more in the rest of the sample. Note the low triple dots <$_{\ddagger}$>, one in the first line and eight more in the rest of the sample. Neither of these diacritics occurs in Arabic.

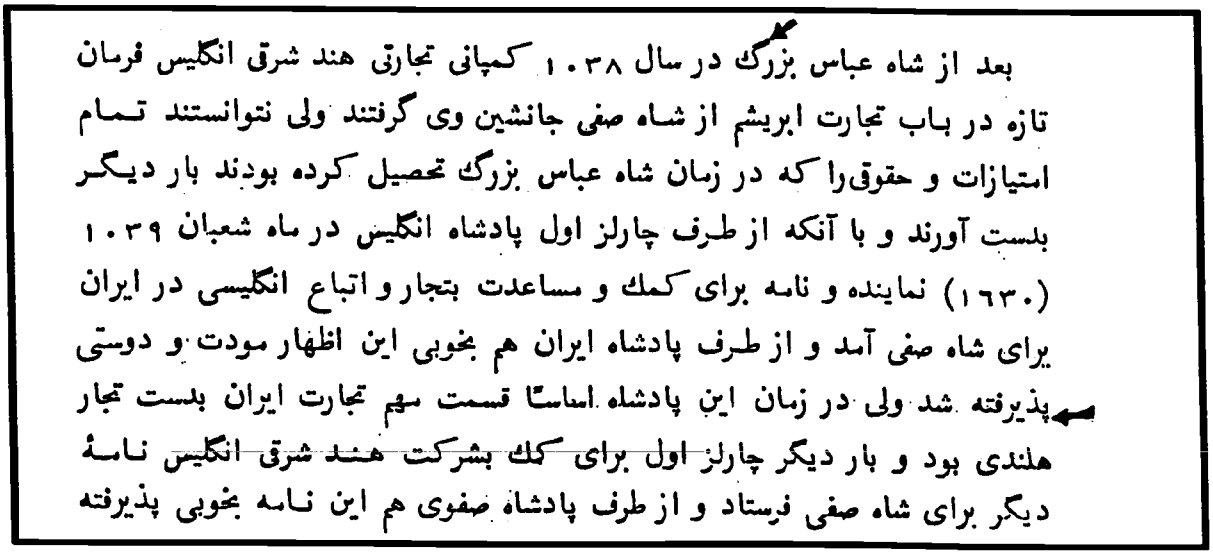

بعد از شاه عباس بزرگ در سال ۱۰۳۸ کمپانی تجارتی هند شرق انگلیس فرمان
تازه در باب تجارت ابریشم از شاه صفی جانشین وی گرفتند ولی نتوانستند تمام
امتیازات و حقوق‌را که در زمان شاه عباس بزرگ تحصیل کرده بودند بار دیگر
بدست آورند و با آنکه از طرف چارلز اول پادشاه انگلیس در ماه شعبان ۱۰۳۹
(۱۶۳۰) نماینده و نامه برای کمك و مساعدت بتجار و اتباع انگلیسی در ایران
برای شاه صفی آمد و از طرف پادشاه ایران هم بخوبی این اظهار مودت و دوستی
پذیرفته شد ولی در زمان این پادشاه اساساً قسمت مهم تجارت ایران بدست تجار
هلندی بود و بار دیگر چارلز اول برای کمك بشرکت هند شرق انگلیس نامهٔ
دیگر برای شاه صفی فرستاد و از طرف پادشاه صفوی هم این نامه بخوبی پذیرفته

Figure G-11. Printed Persian (arrows indicate distinguishing features).

OTHER ARABIC ALPHABET LANGUAGES

DARI:

Dari is used in Afghanistan and favored by the government. Since its written form is heavily influenced by Persian models, there is no easy way for the nonspecialist to distinguish it from Persian.

KURDISH, PASHTO, AND URDU:

The other notable Arabic alphabet languages are Kurdish, Pashto, and Urdu. Kurdish is spoken by the Kurdish tribes of Iraq, Iran, and Turkey. Pashto is used widely in Afghanistan, and Urdu is the predominant language of Pakistan. These languages contain letters and diacritics not listed for Arabic or Persian. If one of these languages is suspected, refer the problem to a linguist.

CHARACTER LANGUAGES

Character languages use writing systems with symbols that stand for words or meaningful elements of words rather than for sounds. Character languages, such as hieroglyphic Egyptian, existed in earlier times; but today, the only character languages are Chinese and languages that have wholly or partially borrowed the Chinese system, such as Japanese and Korean.

DISTINGUISHING CHINESE, JAPANESE, AND KOREAN:

The easy way to distinguish the three languages is to look for the distinctive phonetic symbols of Japanese and Korean. If these symbols are not present, conclude that the language is Chinese. Chinese is the model for the other two, and these languages borrow freely from Chinese. Figures G-12, G-13, and G-14 give sample texts of Chinese, Japanese, and Korean.

Figure G-12 shows Chinese characters. They are more detailed, complex, and square or precise than Japanese or Korean.

Korean and Japanese language texts use Chinese characters whenever it might be unclear to use one of their own symbols. This means that the higher or more academic a text is the more Chinese characters it will have.

出 版 说 明

《汉英词典》是由北京外国语学院英语系编写的。编写工作于一九七一年开始，一九七八年夏完成，历时八载。先后参加编写、修改等工作的中外专家共五十余人。

本书的主编为北京外国语学院英语系系主任吴景荣教授。除编写组编辑人员外，还有不少专家和学者先后参加过这项工作。周珏良主持了初稿的编写，弗兰克·怀利（Frank Wylie）和何南喜（Nancy Hodes）参加了英语修改工作。在组内工作了较长时间的还有初大告、水天同、王锡钧、张道真、王瑞、俞天民、吴国瑞、杨志才、吴石牧、陈国成、张月平等。在词典编写过程中，还得到丘茉莉（Elsie Fairfax-Cholmeley）、舒裕禄（Norman Shulman）和裘克安等对本书的编辑和出版提出了许多宝贵的意见。

本书是一部中型语文工具书，全书收汉语单字条目六千多，其中包括极少数的音变字，收入的多字条目五万余，连同合成词、词化短语、及例证等共达十二万余。

除一般词语外，还收一些常见的文言词语、方言、成语、谚语，以及自然科学和社会科学的常用词语。

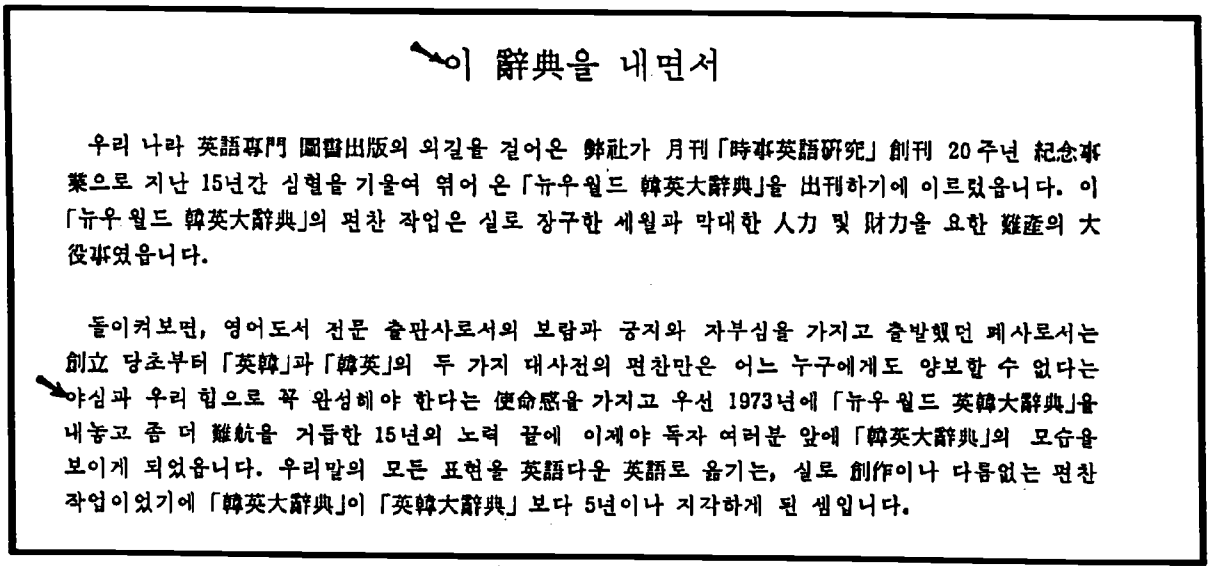
Figure G-12. Sample of Chinese text.

改訂増補の序

辞書は造られた日から古くなりつつある．こう言えば，辞書編集者には，まことに皮肉に響くのであるが，しかも半面の真理を含んでいる．研究社「新英和大辞典」については，1953 年版の発行と同時に，改訂のため待機の姿勢が整えられたのであるが，誤植の訂正はもちろんのこと，内容と形式の統一について一層適切な処置を施すことに，たゆみない努力がなされた．これについては，使用者各位の懇切な指示に負うものもあった点感謝するところであるが，それとは別に，開巻第 1 ページから順を追うて校訂が進められたのであって，河村重治郎氏はもっぱらその任に当られ，年余にわたって本辞典の内容改善のため尽力された．この改訂にはページの変動増加を来さない範囲という枠がはめられていた．

ところが時日の経過につれて，世界情勢の進展に伴い改訂の項目は増進し新語句・新語義の追加すべきものも急増して来たので，漸く巻末に増補追加の案が台頭したのであるが，その間，当用漢字表・かなづかい法の改正に伴う校訂の業も加わって来た．さらに印刷の面からは金属字を新鋳して版面の面目を一新し，また版面を拡大するという大掛りな改良案も登場するに至った．ここにおいて，終に，なんらの枠を設けない全面的改訂に踏みきることとなり，以来鋭意その業が継続せられ，勉励数年，このたび漸く完成の日を迎えるに至った．

Figure G-13. Sample of Japanese text.



이 辭典을 내면서

우리 나라 英語專門 圖書出版의 외길을 걸어온 弊社가 月刊「時事英語硏究」創刊 20주년 紀念事業으로 지난 15년간 심혈을 기울여 엮어 온「뉴우월드 韓英大辭典」을 出刊하기에 이르렀읍니다. 이「뉴우월드 韓英大辭典」의 편찬 작업은 실로 장구한 세월과 막대한 人力 및 財力을 요한 難産의 大役事였읍니다.

돌이켜보면, 영어도서 전문 출판사로서의 보람과 긍지와 자부심을 가지고 출발했던 폐사로서는 創立 당초부터「英韓」과「韓英」의 두 가지 대사전의 편찬만은 어느 누구에게도 양보할 수 없다는 야심과 우리 힘으로 꼭 완성해야 한다는 使命感을 가지고 우선 1973년에「뉴우월드 英韓大辭典」을 내놓고 좀 더 難航을 거듭한 15년의 노력 끝에 이제야 독자 여러분 앞에「韓英大辭典」의 모습을 보이게 되었읍니다. 우리말의 모든 표현을 英語다운 英語로 옮기는, 실로 創作이나 다름없는 편찬 작업이었기에「韓英大辭典」이「英韓大辭典」보다 5년이나 지각하게 된 셈입니다.

Figure G-14. Shows Korean with fewer Chinese symbols used.

NOTE: North Korean text seldom has any Chinese characters as a matter of official policy.

CHINESE:

Chinese is written with several thousand symbols called characters. International numerals are widely used and scientific and technical Chinese will contain quoted European words in Roman letters. The characters are constructed according to a complex system based on the use of only a few different stroke types (less than 10) and a large set of elements called "radicals" (about 200). Radicals are made up of one or more elements associated with them. These radicals and strokes are used to construct the characters. The characters are thought of as occupying a rectangular space and good calligraphy allots about the same area to each character, regardless of complexity.

Figure G-15 shows the 50 most common radicals in Chinese. Some will occur by themselves as characters. Most will more frequently occur as constituents of more complex characters. The People's Republic of China has recently changed the form of some of these elements, but most are unchanged and the traditional forms still occur even there.

Except for numerical zeroes and the small circles that are used as punctuation marks to indicate the end of a sentence, printed Chinese does not have any circles. If the text has a lot of circles and curves, suspect some language other than Chinese.

Figure G-15. The fifty most common Chinese character radicals.

JAPANESE:

Japanese has a mixed writing system. Like the Chinese, the Japanese normally use international numerals in their S&T literature; but this is not the real reason their writing system is mixed. Japanese writing is mixed because, in general, it uses Chinese characters to write the lexical stem of nouns and verbs (the part of the word that conveys the basic meaning); and a set of phonetic symbols invented in Japan called **hiragana** to write the grammatical affixes of the nouns and verbs as well as entire auxiliary words.

Japanese also use another set of phonetic symbols, also invented in Japan, called **katakana** to write words borrowed from European languages. The presence of these katakana symbols distinguishes Japanese. Normal prose will contain perhaps 60 to 70 percent hiragana symbols. Unlike Chinese characters, hiragana are written with curved strokes. Katakana are less frequent.

The hiragana are illustrated in Figure G-16 and the katakana are illustrated in Figure G-17. Pay particular attention to the fifth symbol from the left in the bottom row of the hiragana (Figure G-16), the one labeled "no." This symbol is used to write a very common grammatical affix. It will almost always occur frequently in any Japanese text.

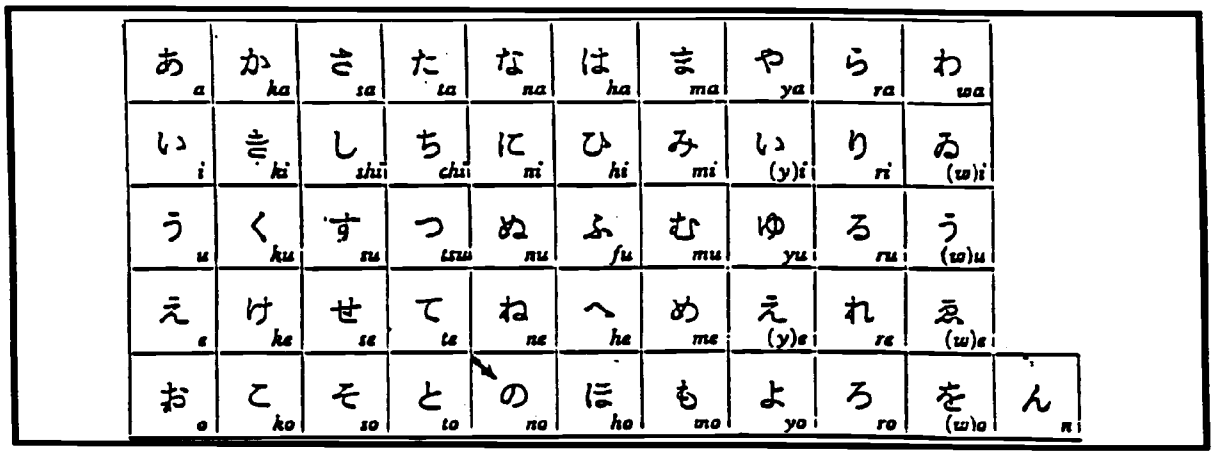


Figure G-16. The Japanese Hiragana syllabary.

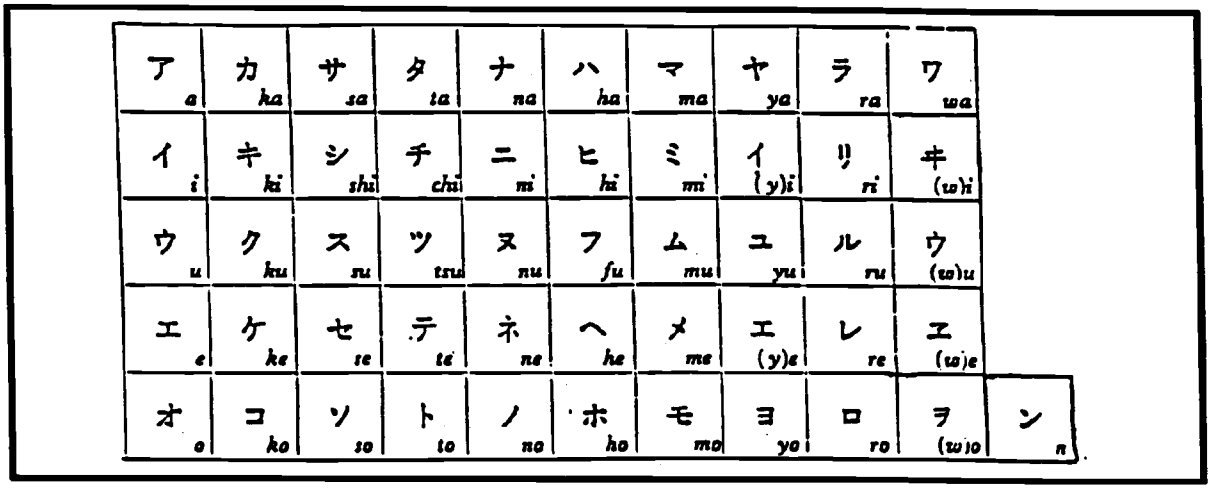


Figure G-17. The Japanese Katakana syllabary.

KOREAN:

Korean can be written entirely in its native alphabet. Therefore, symbols from this script will overwhelmingly predominate in any normal Korean text. Chinese characters, however, are considered learned and prestigious, so a certain number of them will be encountered in quantities that vary with the pretensions of the author.

The Korean alphabet was developed under the influence of Chinese writing models, so to the untrained eye Korean alphabetic writing looks like Chinese characters. The letters of European alphabets form words, but the symbols of the Korean alphabet are grouped together to form a syllable. This means that a Korean word may extend over several groupings.
Also, while the letters of European words are read horizontally, Korean

alphabetic symbols are read vertically—from the top to the bottom of each group—with the left preceding the right when the symbols are side-by-side.

Figure G-18 illustrates the symbols of the Korean alphabet. Pay close attention to the second symbol from the left in the third row, the one that looks like a circle with a stem at the 12 o'clock position. It is a very frequent symbol and does not look like anything that occurs in Chinese or Japanese.

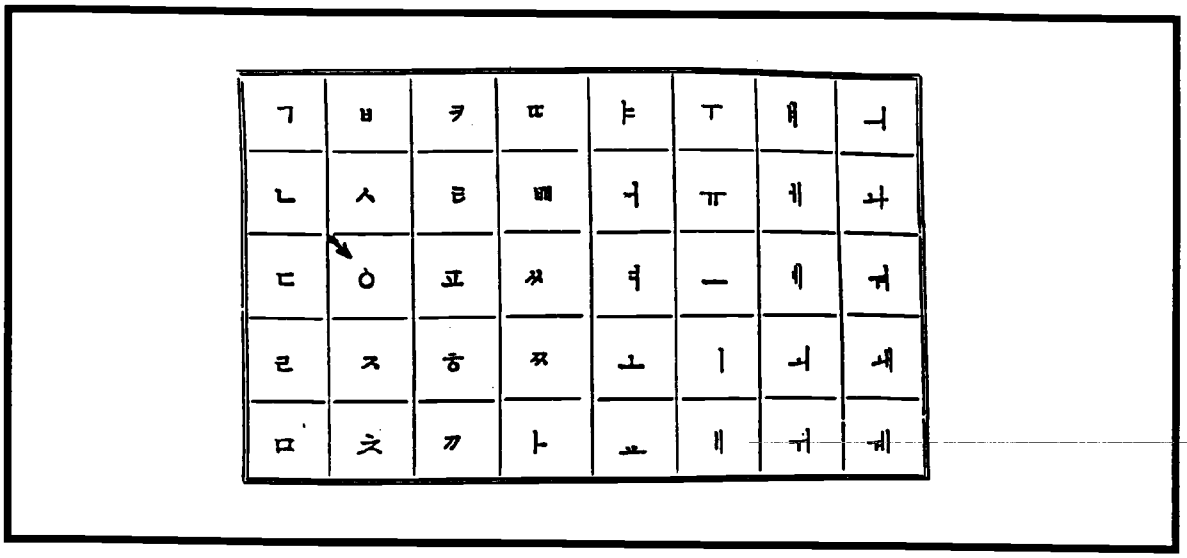


Figure G-18. The Korean alphabet.

Appendix H

CHEMICAL AND BIOLOGICAL WARFARE SAMPLING PROCEDURES

INTRODUCTION

This appendix provides procedures for the safe and expeditious collection, transportation, and receipt of suspected CB agent samples from the integrated battlefield to approved CONUS and OCONUS laboratories for processing, analysis, and identification.

BACKGROUND

During the 1980's, at the time of the Soviet occupation of Afghanistan and the Iran-Iraq War, the ability of US forces to collect and analyze toxic agents was questionable.

In response to this concern, an examination was conducted on the mechanisms in place to preserve the integrity of the suspected CB samples collected on the battlefield.

Procedures for collecting, packaging, documenting, and transporting CB samples to laboratories must be precise to ensure the credibility of the analysis conducted on the samples.

The credible analysis of suspected CB samples is critical for both battlefield commanders concerned with chemical retaliation and contamination avoidance, and medical personnel concerned with prophylactic or post-contamination treatment.

OPERATIONAL CONCEPT

SITUATION:

Current battle doctrine describes a nonlinear battlefield where the Threat NBC weapons are tactically integrated. The principles of NBC reconnaissance and detection and TECHINT teams apply equally across the battlefield.

SAMPLING:

Sampling will be initiated when the following are observed:

- Significant numbers of unexplained sickness or death of personnel or animals occur.
- Ordnance (munitions) are found which contain known or suspected CB agents.
- An attack is suspected or is known to have occurred but the causative agent cannot be identified.
- The widespread outbreak of unusual mission-degrading behavior occurs.
- Sampling of known or identified agents to verify first use is required.

SAMPLING RESPONSIBILITY:

Samples suspected of containing CB agents are divided into environmental and biomedical samples on the basis of their origin. Both medical and nonmedical units and teams have the responsibility for collecting samples suspected of containing CB agents.

- Environmental Samples. Environmental CB agent samples are collected in the field. They include samples of aerosols or vapors, liquids other than water, soil, vegetation, water, used equipment, and ordnance. The acquisition of these samples is the responsibility of—
  - — NBC reconnaissance teams.
  - — TEU field teams.
  - — Preventive medicine units (potable water sources only).
  - — TECHINT collection teams.
  - — Biological Integrated Detection System (BIDS) team.
- Biomedical Samples. Biomedical samples are derived primarily from acutely ill soldiers who exhibit symptoms of CB agent intoxication or from personnel who were killed in an attack. Collection of the biomedical samples will be the responsibility of personnel in—
  - — Battalion-level medical units.
  - — Division-level medical treatment facilities.

- — Combat support hospitals.
- — Evacuation hospitals.
- — NBC reconnaissance teams (small animals only).
- — TECHINT collection teams.
- — BIDS teams.

SAMPLE ACQUISITION

ENVIRONMENTAL SAMPLES:

Responsible personnel for collection:

- Commander, NBC reconnaissance teams.
- Commander, TEU.
  - — Commander, CMEC.
  - — Commander, preventive medicine units.

NOTE: When possible, background samples from "clean" areas beyond the perimeter of the attack site should be obtained as baseline data for comparisons. Collect these identically to samples from contaminated areas and package them separately.

The methodology for collecting environmental samples in order to analyze them for CB-agent presence will be specific for the type of sample (for example, liquid aerosols or vapors, soil, vegetation, water, other liquids, ordnance, equipment). Complete DA Form 1971-6-R for all environmental samples. A sample form is at Figure H-1.

In conjunction with collection of environmental samples, any positive results using the chemical agent detector kits should be recorded on DA Form 1971-6-R. Sampling will be accomplished as instructed. Figure H-2 is an example of an equipment list containing components of a suggested environmental sampling kit. (See FM 3-3.)

Chemical/Biological Specimen Documentation

For use of this form, see FM 3-3; the proponent agency is TRADOC.

INSTRUCTIONS

Place the biological sample inside a refrigerator, ice chest, or insulated container; and keep it as cool as possible at all times.

Specimen Identification Number: 0001

Date and Time Specimen Collected: 121500 JUL 97

Reason for Collection (check those that apply):

- ☑ Chem/Bio Attack
- ☐ Chem/Bio Alarm Activated
- ☐ Positive M256 Chemical Detection
- ☒ Positive Recon Team Findings
- ☐ Soldiers Becoming Sick
- ☐ Soldiers Dying
- ☐ Other _____

Location of Attack DHAHRAN (UTM or place)

Unit Identification BCO, 203d MI BN, 515th MI Bde (Co, Bn, Bde, Div, Corps)

Date and Time of Attack 121345 JUL 97

SAMPLE

Terrain Description (check those that apply):

- ☑ Flat
- ☐ Hills
- ☐ Mountains
- ☐ Desert
- ☐ Jungle
- ☐ Forest
- ☐ Urban
- ☑ Grassy
- ☐ Sparse Trees/Shrubs
- ☐ Other _____

Weather (check those that apply):

- ☐ Clear
- ☑ Cloudy
- ☐ Rain
- ☐ Fog
- ☐ Snow
- ☐ Dust
- ☐ Mist
- ☐ Other _____

Wind at Collection Site (check only one):

- ☐ None/Calm
- ☐ Mild Breeze
- ☑ Windy
- ☐ Gusts

Odor (check those that apply):

- ☐ None
- ☐ Sweet
- ☐ Fruity
- ☑ Irritating
- ☐ Pepper
- ☐ Flower
- ☐ Changing
- ☐ Other _____

Symptoms (check those that apply):

- ☐ None
- ☐ Skin Swelling
- ☐ Difficulty Breathing
- ☐ Blurred Vision
- ☑ Dizziness
- ☑ Skin Rash
- ☐ Nausea
- ☐ Dry Mouth
- ☐ Fever
- ☐ Dark Skin Blotches
- ☐ Unconscious
- ☑ Headache
- ☐ Bleeding Sores
- ☐ Other _____

Symptoms:

Time of Onset: 121400 JUL 97 Duration (of Symptoms): 15 Minutes

DA Form 1971-6-R, AUG 92

Figure H-1. Sample DA Form 1971-6-R (Chemical/Biological Specimen Documentation).

Delivery Method (check those that apply):

☐ Unknown ☑ Artillery ☐ Mortar ☐ RPG/Grenade ☐ Rocket

☐ Aircraft ☐ Aerosol ☐ Generator ☐ Other _____

State of Agent at Time of Collection (check only one):

☐ Liquid ☑ Vapor ☐ Powder ☐ Solid ☐ Smoke ☐ Mist

☐ Dust (cloud) ☐ Gel ☐ Other _____

Description of Sample (check only one):

☐ Vegetation

☑ Soil ☐ Other _____

Biomedical: ☐ Urine ☐ Blood ☐ Tissue

Color of Sample _____

Size of Sample _____

Other _____

Additional Remarks:

DA Form 1971-6-R, AUG 92

Figure H-1. Sample DA Form 1971-6-R (Chemical/Biological

Description:	
labels, paper, pressure sensitive	7530-00-577-4376
Edmont Wilson gloves 8-9	8415-00-J02-2802
Edmont Wilson goves 9-9	8415-00-634-4639
tape, pressure, sensitive, adhesive 1"	7510-00-582-4772
pliers #47 8"	8820-00-543-5350
screwdriver, flat tip 1/4 inch	5120-00-596-5653
tongs, Teflon tips	AF 15-202-5
micro spatula with Teflon ends AF 21-401-50A	
scissors, universal type	AF 08-951-30
sterile sampler scoops 2 oz	AF 14-241-10A
spoon spatula with Teflon	AF 14-356-10
knife, pocket	5110-00-526-8740
PFA sample bottles, 6 oz	CP J-6103-50
pipet, jumbo transfer type	AF 13-711-7
pipet, graduated transfer type	AF 13-711-9A
insulated bag, type 1	AF 01-814-8
insulated bag, type 2	AF 01-814-10
whirl/pak bag, 6 oz	AF 01-812-6B
ph paper; non-bleeding plastic strip	SW 8-65271
SEP-PAK C18	
syringe, hyp 50 or 60 mL	6515-00-168-8913
R3602 clear laboratory tubing	AF 14-169-3B
marking pen, waterproof	AF 13-381
Tenax tubes	EC ST-023
blade surgical knife detach no. 21	6515-00-860-0007
blade surgical os 21 1508	6515-01-009-5297
igloo type container	
ice pack	CP TR-6345-20
pad, non-adherent 3 x 4 100s	6510-00-111-0708
pad, cooling chemical 49	6530-00-133-4299
piglette	
tape, antiseizing	8030-00-889-3535
personal air sampler	LSS G4980 +
methanol	GJ4981
distilled water	
matches, waterproof	
myler bags	
Field Expedient Packing Materials	
tin foil	
Saran wrap polyethylene without plasticizers	
Thermos bottles	
pressure sensitive tape	
Cool Paks	
butcher paper	
newspaper	
igloo cooler	
canteens	
Mess kits	
glass bottles	
packing material	
Teflon plumbers tape	
medical supplies	

Figure H-2. Example of an equipment list.

Contaminated sampling equipment not transported with the sample will be decontaminated and double wrapped in plastic and undergo a sampling protocol to certify the items as "XXX." The XXX refers to decontamination to the point that equipment can be reused, but is not releasable from DOD.

Liquid Aerosol and Vapor Samples:

- Use an electric or hand pump (record the run time for electric pump or number of aspirations for hand pump to determine volume), collect the liquid aerosol remove (LAR) in two Tenax GC-Type Sorbent Tubes.

- Return the sampling tube to the piglette, mark on the outside with a sample identification code and close the ends tightly. Attach a DA Form 1971-6-R. Pack the sample.

Vegetation Samples:

- Collect vegetation which appears in any way to be different from normal, nearby vegetation (for example, discolored or withered vegetation, or vegetation having powder or droplets present).

- Collect vegetation samples at several locations within suspected contaminated areas.

- Cut several affected leaves and/or a handful of grass. Do not crush the sample. Instead, place it in a mylar bag and seal. Collect similar reference vegetation from an unaffected area and place it in a separate mylar bag and seal it. The minimum sample size of value is three leaves or three handfuls of grass. One leaf is of little value (but it is better than nothing). Bark is acceptable but not preferred.

- Mark the bag with a sample identification number.

Soil Samples: Collect samples from areas stained with oils or powders, from areas that are discolored, or from areas that are otherwise different in appearance from the surrounding soil. A similar soil sample from an unaffected area is required for reference (soil of the same type and texture is preferred). The minimum sample volume is approximately that of a cigarette pack laying on its side.

- Use a knife, spoon, spatula, or piece of metal to collect the sample.

- Place the sample in a mylar bag.

- Mark the bag with a sample identification number.

Water Samples: Use the M272 water test kit or other appropriate test kit to determine the presence of chemical agents, record the test results on a DA Form 1971-6-R. Take samples at standing pools or along streams where dead animals are observed.

- Collect bulk water samples (preferred when oily globules or suspended solids are present) as follows:
  - — Skim surface water into Teflon bottle.
  - — Fill the bottle, screw on the top, and ensure that the seal is leak proof with parrafin wax or plumber's antiseize tape.
  - — Mark a sample identification number on the bottle.
- When using the SepPak Cartridge for liquid sampling, consider the following:
  - — The C-18 SepPak cartridge extracts and concentrates contaminants from a water source.
  - — Methanol and distilled water are used to prime the SepPak.
  - — 200 milliliter (mL) of sample water is drawn slowly through cartridge with a 50 mL syringe. Discard liquid and syringe.
  - — The cartridge is placed in a Teflon bottle marked with a sample identification number.
- When obtaining a sample of sludge on the shore or in a shallow bottom, scoop the top of solids with an open bottle; close the bottle and seal it with parrafin wax. Mark the bottle with an identification number.

Packaging Samples: Place several sample bags in one mylar bag. Place the reference samples in a separate mylar bag. Do not overfill. Press excess air from the bag and seal the adhesive end. Seal the package with tape, and mark sample identification numbers. Include the DA Form 1971-6-R.

Packaging Small Animals (Mammals Preferred): Place the animal in a mylar bag, press excess air from the bag, and seal it. Mark the bag with the sample identification number and place the marked bag into a second mylar bag. Press excess air from the bag, seal the adhesive flap, and seal the bag with tape. Mark with sample identification numbers and attach the DA Form 1971-6-R.

Packaging Ordnance or Protective Equipment or Clothing: Prior to approaching or handling any ordnance, exploded or unexploded, contact the EOD unit in the area for assistance. The EOD unit will attempt to identify the ordnance by physical characteristics or markings and render it safe. If the ordnance is CB in origin, EOD will perform initial packing in the

field and transfer the sample to an MI unit for transfer to CONUS. The sample must be marked with a sample identification number and documented with the DA Form 1971-6-R and DD Form 1911.

Protective equipment and clothing from casualties can be an important source of a CB agent for identification purposes. To do this, place the equipment or clothing in a large mylar bag, fold, expel excess air from the bag, and seal it. Mark the bag with a sample identification number. Place the bag in a second mylar bag, seal, and mark with a sample identification number. Then complete and attach the DA Form 1971-6-R. Finally, forward the sample to Technical Intelligence for transfer to Corps G2. Document the transfer on DA Form 3147.

BIOMEDICAL SAMPLES:

Responsible personnel for collecting samples are located in—

- Battalion-level medical units.
- Division-level medical treatment facilities.
- Combat support hospitals.
- Evacuation hospitals.
- TECHINT collection teams. In the theater of operations, the TECHINT teams will have the capability to obtain biomedical samples from patients and cadavers.

The best biomedical sample is an acutely ill soldier sent back to CONUS immediately. DA Form 1971-6-R is to be completed on all biomedical samples. In addition, a copy of the physical examination or an extract of significant findings are to be enclosed with the biomedical samples.

Additionally, the following samples should be collected whenever casualties occur and should be collected in triplicate, distributing two within CONUS and one to the TAML. Once collected, the samples should be refrigerated or chilled immediately. DO NOT FREEZE.

DA Form 1971-6-R will be completed on all biomedical samples. Medical personnel should perform biomedical sample collection to obtain a valid sample.

Use the following guidance to collect samples:

- Collect samples from patients during acute phase and at day 7.

- Collect urine samples (20 to 50 mL per sample x 3) in urine specimen cups, the top secured with wide tape, and placed in individual sealable bags.

- Collect whole blood or serum samples (5 mL per sample x 3) in red-top blood tubes and placed in individual, sealable bags.

- Collect sputum only from acutely ill patients (x 3). They should be collected in urine cups. Secure the cup with wide tape and place in individual sealable mylar bags.

- Collect cerebral spinal fluid (2 mL per sample x 3) in red-top blood tubes and placed in individual, sealable bags.

- Take at least 30 grams of organs and tissues (human, post-mortem x 3), place in a sterile container in individual, sealable bags, and refrigerate immediately: liver, spleen, lung, subcutaneous fat, cerebral spinal fluid, kidney, heart, and brain.

- Collect at least two mediastinal lymph nodes.

- Take animal tissue samples as a lower priority to human samples. Animals should be mammalian (no birds).

- Once critical and significant biomedical samples are identified in OCONUS, these samples should be turned over to the tactical intelligence channel for disposition to appropriate laboratories (CONUS or OCONUS).

- Sample and corroborative information is provided for on DA Form 1971-6-R.

Packaging Biomedical Samples: Place the mylar bags or sample containers in a plastic bag. Remove excess air and seal tightly. Mark the container with a sample identification number. Place 1 to 2 inches of packing material (for example vermiculate or foam) around the sample bag in a rigid container. Wrap jars, tubes, or specimen cups in bubble wrap or other suitable material so they do not move in the container. Place a lid on the container and seal with wide tape. Place a warning on the outside of the container as follows:

DANGER
Do not open. Contains hazardous material or suspected CB agents which may cause immediate death or personal injury.

DISPOSITION OF ENVIRONMENTAL AND BIOMEDICAL SAMPLES:

Place the environmental and biomedical samples in an insulated chest; ensure that the sample is packed tightly and an adequate supply of refrigerant is available. Seal the chest and label accordingly prior to its departure from the OCONUS theater of operation to CONUS.

The procedure should further meet the specifications contained in TM 38-250, paragraph 10-51, for etiologic agents. Document all samples with DA Form 1971-6-R. Number the samples. Units are responsible for forwarding samples through intelligence channels to Corps G2. Document the sample transfer with DA Form 3147. Figures H-3 through H-5 are examples of responsibilities, collection guidelines, and identification and control for a sample evacuation.

SAMPLE EVACUATION

A. RESPONSIBILITY:

1. Field units are responsible for the transfer of samples to MI channels for forwarding to Corps G2. Additional packaging and consolidation of double-contained samples, if required, will be accomplished prior to shipping to CONUS. Complete the sample identification. Document sample transfers on DA Form 3147.

2. Corps or Division surgeons are responsible for coordinating the delivery of samples from MI channels to Corps G2. The Corps and/or Division Surgeon will coordinate with combat units and graves registration units for expedient transfer of personnel deceased as a result of a CB attack to battalion, division, or corps level medical units and hospitals for obtaining biomedical samples. Document the sample transfers on DA Form 3147.

3. Corps G2 is responsible for coordinating shipment of samples to approved CONUS and OCONUS laboratories and the TAML, as well as dispatching the required notification messages. Notification to the US Army Chemical and Biological Agent Technical Evaluation Board (CBATEB) of the acquisition of a sample suspected of containing CB agents is requested within 1 hour of receipt by Corps G2.

Figure H-3. Description of responsibilities for a sample evacuation.

IMPORTANT NOTES

(a) Properly packaged samples do not constitute a hazard to personnel.

(b) All outer packaging is to be inspected visually for physical evidence of leakage or loss of envelope integrity.

(c) DO NOT UNWRAP. Overwrap if any irregularities exist.

(d) If overwrapping is required, provide the time, date, place, and the reason.

(e) Refrigerate or chill (DO NOT FREEZE) all samples.

(f) Delay must be minimized.

(g) All samples will be forwarded from the theater to approved CONUS and OCONUS laboratories and TAML 12 to 24 hours after collection. Delay beyond 24 hours rapidly degrades the operational and intelligence value of the samples. The most efficient means of shipment will be used; address all samples to CBATEB, Aberdeen Proving Ground, MD, and TAML.

B. DOCUMENTATION REQUIRED ON ALL SAMPLES:

1. DA Form 1971-6-R.

2. DA Form 3147.

C. NOTIFICATION MESSAGE: The notification message sent by Corps G2 should be sent as an IMMEDIATE precedence and with appropriate security classification. The action addressee is Technical Director, ERDEC APG MD//CBATEB//. The notification message will contain the sample identification number and details which relate to the acquisition of the sample. The message will be configured to provide the following information:

1. Background information.

2. Physical description.

3. Results of preliminary tests after sample collection.

4. Where, when, and under what conditions the sample was acquired.

Figure H-3. Description of responsibilities for a sample evacuation (continued).

5. Description of incident.

6. Casualty symptoms (if applicable).

7. Shipment information, such as—

   (a) Date of shipment.

   (b) Mode of transportation.

   (c) Flight number and destination.

   (d) Estimated time of arrival CONUS.

   (e) Description of shipment (size, weight, and so forth).

D. NOTIFICATION: Upon receipt of the notification message, the Chairman, CBATEB, is responsible for notifying the appropriate agencies.

REFERENCES:

1. FM 3-3 Chemical and Biological Contamination Avoidance, 16 Nov 92.

2. FM 3-5 NBC Decontamination, 17 Nov 93.

3. FM 3-101-2 NBC Reconnaissance Squad/Platoon Operations Tactics, Techniques, and Procedures, 10 Aug 94.

4. AR 59-8 Department of Defense (DOD) Common User Airlift, 20 Aug 82.

5. TM 38-250 Preparing of Hazardous Materials for Military Air Shipments, 25 Nov 94.

Figure H-3. Description of responsibilities for a sample evacuation (continued).

SAMPLE COLLECTION GUIDELINES

1. PROTECT YOURSELF:

   Do not handle contaminated samples with your bare hands. If neoprene gloves are not available, use a stick or other object to move a sample into a container. Respiratory and/or skin protective equipment may also be required.

2. TAKE THE SAMPLE:

   If an area appears to have been contaminated, use whatever field expediency is necessary to get a sample.

3. LABEL THE SAMPLE:

   Once a sample is collected, the container should be labeled immediately so that it is not confused with another sample.

4. PROTECT THE SAMPLE:

   Most environmental and biomedical samples should be sealed and chilled to avoid cross-contamination and decomposition. Samples should not be frozen if possible. Above all, avoid freeze-and-thaw situations.

5. DOCUMENT THE SAMPLE:

   Record the circumstances surrounding the collection of the sample. Data such as how, where, when, why, and by whom is required. Diagrams and maps of areas are useful.

6. FORWARD THE SAMPLE:

   CB samples are time sensitive. They should be reported and forwarded for analysis as quickly as possible (within 12 to 24 hours).

7. PROTECT YOUR SOURCE:

   All transactions involving CBW samples are highly sensitive. All knowledge and information (written and verbal) pertaining to the source are automatically considered SECRET. All samples and associated papers and diagrams, for example, will be released only to individuals known to be cleared and having a need to know; and they will be SIGNED FOR. All samples and associated papers must remain in the physical custody of authorized US persons only.

Figure H-4. Sample collection guidelines.

SAMPLE IDENTIFICATION AND CONTROL

1. Samples acquired by a governmental source or provided by another source must be carefully controlled to be of the greatest value. To accomplish this, physical custody of the sample is maintained by a government representative. A sample identification number is also assigned and affixed to the sample or its container.

2. To prevent confusion, the sample number must be used when referring to the sample or to information concerning its acquisition. A sample number consists of the following elements:

(a) Country of Acquisition. This is a 2-digit alphabetic code for the country in which the sample was collected. The codes are found in DIAM 58-13, Volume II, Section E, dated 28 March 1988.

(b) Date Acquired. DTG sample acquired (local or Zulu time, as directed by higher headquarters).

(c) Sample Sequence Number. This is a 3-digit numerical code which is assigned per collector, and begins each collection day. The first sample collected is 001, the second is 002, and so forth.

(d) Unit Identification Code. UIC of the unit that the collector is assigned to.

(e) Collector Identification. The initials of the collector.

EXAMPLE

LA-12l300Z FEB 90-002-WH60AA-JD

LA	= Sample was acquired in Laos
121300Z FEB 9	= DTG sample was collected
002	= This is the second sample obtained on the date above by the collector
WH60AA	= Unit of assignment of collector
JD	= The sample was collected by John Doe

Figure H-5. Sample identification and control.

Appendix I

FACILITY EXPLOITATION CHECKLISTS

The following sample checklists can be used to guide the actual eyes-on or hands-on exploitation of facilities or to guide the interrogation of EPWs with knowledge of facilities.

COLLECTION CHECKLIST-AIRFIELDS

1. IDENTIFICATION. Local name (both romanized and ideograph) and military designation.

2. LOCATION.

   a. Map reference. Include series and sheet number(s) of both tactical and air-ground series.
   b. Political unit, area, nearest town, and specified reference point (both UTM and geographic coordinates).

3. AIRFIELD CATEGORY. Liaison, surveillance, light lift, medium lift, tactical, or heavy lift.

4. STATUS.

5. TYPE. Civilian, military, or joint.

6. PRINCIPAL USE.

7. LAYOUT.

8. ELEVATION (feet and meters).

9. NUMBER OF RUNWAYS.

10. EACH RUNWAY.

   a. Identification.
   b. Azimuth.
   c. Length and width.
   d. Surface, base, subbase course (material, thickness, and condition).
   e. Longitudinal grade (minimum and maximum change per 100 feet).
   f. Transverse grade (maximum).

Figure I-1. Collection Checklist-Airfields.

g. Shoulders, clear area, and overrun (width, transverse grade, and surface material).
h. Lateral safety zone (width, transverse slope, and obstacles).
i. End clear zones (length, width, and maximum slope).
j. Approach zones (length, width, glide slope, and obstacles).
k. Condition.

11. EACH TAXIWAY.

a. Identification.
b. Azimuth.
c. Length and width.
d. Grade (maximum longitudinal and transverse).
e. Surface, base, subbase material (thickness).
f. Bearing capacity (pounds per square inch).
g. Shoulders and clear area (width, transverse grade, surface, and obstacles).
h. Turn radii.
i. Condition.

12. PARKING AND WARM-UP APRONS.

a. Number.
b. Total area and individual area.
c. Description of each apron.
d. Total capacity (specify aircraft type).

13. HARDSTANDS.

a. Total number.
b. Aircraft capacity (specify).
c. Description of each hardstand.

14. PETROLEUM, OIL, AND LUBRICANTS. Describe facilities and storage.

a. Jet fuel by type (J rating).
b. Aviation gasoline.
c. Jet oil.
d. Aviation oil.
e. Lubricants.
f. Pipelines (cross-reference to pipeline collection file).

15. NAVIGATION FACILITIES. Describe the type of facility.

16. LIGHTING FACILITIES. Describe all lighting at airfield.

Figure I-1. Collection Checklist-Airfields (continued).

17. COMMUNICATION FACILITIES. Cross-reference to communication collection file.

18. MAINTENANCE FACILITIES (aircraft).

19. OXYGEN AVAILABILITY.

20. SPECIAL EQUIPMENT.

    a. Crash and fire.
    b. Construction and ground maintenance.

21. COVERED STORAGE.

22. SANITATION.

23. HANGARS.

    a. Number and locations.
    b. Type and material.
    c. Condition.

24. HOUSING FACILITIES.

    a. Type, location, and number.
    b. Capacity and condition.

25. MUNITIONS STORAGE.

    a. Type and location.
    b. Cubage, normal use, and condition.

26. ADMINISTRATION BUILDINGS (identify).

27. ELECTRICITY. Cross-reference to electric power collection file.

    a. Sources.
    b. Current characteristics.

28. JET STARTING UNITS.

29. AUXILIARY POWER UNITS.

Figure I-1. Collection Checklist-Airfields (continued).

30. ANTI-DETONATION FLUID OR WATER-ALCOHOL.

    a. Type and location.
    b. Quantities.

31. DEFENSES.

32. ADJACENT TERRAIN. Cross-reference to appropriate collection files.

33. MEDICAL FACILITIES.

    a. Type and location.
    b. Capacity and characteristics.

34. WEATHER FACILITIES. Cross-reference to weather collection file.

    a. Type and location.
    b. Characteristics and condition.

Figure I-1. Collection Checklist-Airfields (continued).

COLLECTION CHECKLIST-ELECTRIC POWER

POWERPLANTS

1. IDENTIFICATION. Local name and military designation.

   a. Map reference. Include series and sheet numbers of both tactical and air-ground series.
   b. Political unit, area, nearest town, UTM coordinates, and geographical coordinates.

2. TYPE. Conventional-steam thermal, nuclear-steam thermal, internal combustion-thermal, hydro-turbine storage, hydro-turbine run-of-river, solar, wind, tidal, and so forth.

3. OWNERSHIP. Government or private.

4. FUNCTION. Public utility, industrial, or both.

5. AREA SERVED.

6. PURPOSE. Base load, peak load, or stand-by.

7. STATISTICS.

   a. Total capacity (kW or kVA) and annual production (kWh).
   b. Generators (numbers, type, and rating of each).

8. CURRENT CHARACTERISTICS.

   a. Type (direct current; alternating current).
   b. Generating voltage.
   c. Phase and hertz.

9. OVERALL CONDITION AND AGE.

10. POWERHOUSE CONSTRUCTION. Material, number of stories, windows, and so forth.

11. TRANSMISSION LINE CONNECTIONS. Number and voltage.

12. FUEL DATA (thermal plants only).

   a. Type (by grades).
   b. Quantity used per annum (tons, gallons, cubic feet, pounds, and so forth).
   c. Sources.

Figure I-2. Collection Checklist-Electric Power.

d. Calorific content (conventional-steam).
e. Waste disposal (nuclear-steam).

13. BOILER, REACTOR OR ENGINE DATA (thermal powerplants only).

a. Number, manufacturer, and rating (kW; hp).
b. Cooling facilities (type and source).
c. Steam pressure in psi (conventional-steam only).
d. Efficiency (calories; Btu/kWh) (conventional-steam only).
e. Operating temperature (conventional-steam only).
f. Neutron flux (nuclear-steam only).
g. Shielding and control mechanism (nuclear-steam only).

14. WATER SOURCE, HYDRO-TURBINE POWERPLANTS.

a. Identification.
b. Flow, cubic feet per second (average, minimum, and maximum).
c. Reservoirs (location, volume, area, head, and so forth).
d. Dams (name, location, dimensions, diversion canal).

15. HYDRO-TURBINES (HYDRO-TURBINE POWERPLANTS ONLY).

a. Type, number, and rating (hp).
b. Heat (feet; meters) and Flow (cubic meters per second).

SUBSTATION

1. IDENTIFICATION. Local name and military designation.

2. LOCATION.

a. Map reference. Include series and map sheet numbers of both tactical and air-ground series.
b. Political unit, area, UTM coordinates, and geographic coordinates.

3. TYPE. Transmission, distribution, or industrial.

4. FUNCTION. Switching, transforming, converting, or inverting.

5. OWNERSHIP. Government or private.

6. TRANSFORMERS. Number, capacity (kVA), and voltage ratio (220/110, and so forth).

7. CONVERTERS OR INVERTERS. Number and capacity (kW; kVA).

Figure I-2. Collection Checklist-Electric Power (continued).

8. LINES. Number and voltage (kV).

9. AREA SERVED.

TRANSMISSION LINES

1. LOCATION. (Same as 2 above.)

2. NUMBER OF LINES.

3. OWNERSHIP. Government or private.

4. PLACEMENT. Overhead, underground, submarine cable, and so forth.

5. WIRE CHARACTERISTICS.

6. TYPE OF TOWER. Metal, wood, or concrete.

7. ALIGNMENT AND LENGTH.

8. VOLTAGE (kV).

9. PHASE.

10. MAINTENANCE. Failure causes, effects, and frequency.

Figure I-2. Collection Checklist-Electric Power (continued).

CHECKLIST-PETROLEUM AND NATURAL GAS FIELDS

1. IDENTIFICATION. Local name and military designation.

2. LOCATION.

a. Map reference. Include series and sheet numbers of both tactical and air-ground series.
b. Political unit, area, nearest town, UTM coordinates, and geographic coordinates.

3. OWNERSHIP. Government or private.

4. TYPE. Wet or dry.

5. AREA EXTENT.

6. STATUS. Exploited or unexploited.

7. PRODUCTION. Barrels, tons, cubic feet, per time unit.

8. NUMBER OF PRODUCING WELLS.

9. PERCENTAGE OF NATIONAL PRODUCTION.

10. PRODUCT. Type and characteristics.

11. RESERVES. Proven and unproven.

12. PLANNED EXPANSION. Expected increase, date, and method.

13. TRANSPORTATION.

a. Method (pipeline, railroad, road, water).
b. Identification and destination.

PROCESSING PLANTS

1. IDENTIFICATION. (Same as 1 above.)

2. LOCATION. (Same as 2 above.)

3. TYPE OF PLANT. Complete, skimming, cracking, distilling, synthetic, and so forth (oil or gas).

Figure I-3. Checklist-Petroleum and Natural Fields.

4. OWNERSHIP. Government or private.

5. PERCENTAGE OF NATIONAL REFINING OR CRACKING CAPACITY.

6. YEAR COMPLETED.

7. GENERAL CONDITION.

8. RATED PRODUCTION CAPACITY. Barrels, tons, cubic feet, per time unit.

9. EQUIPMENT.

   a. Number and type.
   b. Rated capacity and condition.

10. OUTPUT. Product, quantity, and quality.

11. POWER SOURCE.

12. WATER SOURCE.

13. TRANSPORTATION.

    a. Raw materials in (identification, method, and origin).
    b. Finished products out (identification, method, and destination).

14. PLANNED EXPANSION.

15. BUILDINGS. Type, number, and characteristics.

STORAGE FACILITIES

1. IDENTIFICATION. (Same as 1 above.)

2. LOCATION. (Same as 2 above.)

3. TYPE. Gas or petroleum.

4. OWNERSHIP. Government or private.

5. TOTAL STORAGE CAPACITY. Barrels, tons, or cubic meters.

6. PERCENTAGES OF NATIONAL TOTAL.

Figure I-3. Checklist-Petroleum and Natural Fields (continued).

7. GENERAL CONDITION.

8. STORAGE TANKS.

9. STORAGE DRUMS.

   a. Manufacturing (location and capacity).
   b. Cleaning and reclamation (location and capacity).
   c. Filling facilities (location, equipment, and capacity).

10. TRANSPORTATION.

    a. In (method and origin).
    b. Out (method and destination).

11. BUILDINGS. Number, type, and characteristic.

Figure I-3. Checklist-Petroleum and Natural Fields (continued).

FACILITY PHYSICAL SECURITY CHECKLIST

1. IDENTIFICATION.

   a. Local and official name.
   b. Functional description.
   c. Local address.
   d. Map reference.
   e. Geographic coordinates.
   f. Additional information.

2. BUILDING DESCRIPTION.

   a. Identification.
   b. Type of construction material.
   c. Type of roof.
   d. Blueprints.
   e. Floor plans.
   f. Description of roof.

      (1) Entrances to building.
      (2) Skylights.
      (3) Air-conditioning ducts.
      (4) Maintenance accesses.
      (5) Elevator shafts.
      (6) Emergency exits and fire escapes.
      (7) Ventilation systems.
      (8) Ladders.
      (9) Additional information.

   g. Entrances to building.

      (1) Main entrance.
      (2) Other entrances or exits.
      (3) Non-standard access points.

   h. Sewage and drainage systems.
   i. Water system.
   j. Interior description of building.

      (1) Floors.
      (2) Corridors.
      (3) Doors.
      (4) Windows.

Figure I-4. Facility Physical Security Checklist.

(5) Locks.
(6) Stairways.
(7) Elevators.
(8) Physical barriers.
(9) Lighting

k. Active security.

(1) Security guards.

(a) Posts.
(b) Arms
(c) Ammunition.
(d) Riot control devices.
(e) Additional information.

(2) Contract watchmen.
(3) National police agents.
(4) Additional information.

l. Communications equipment available.

MODEL	TYPE	NUMBER	LOCATION	FREQUENCY/CHANNELS	ANTENNAS

m. Telephone system.
n. Emergency lighting and power system.
o. Additional information.

3. DESCRIPTION OF GROUNDS.

a. Structures.
b. Entrances to grounds.
c. Perimeter fence.
d. Terrain.
e. Vegetation.
f. Lighting-external.
g. Map or sketch.

4. DESCRIPTION OF SURROUNDING AREA (24 Block Area).

a. Possible observation points.
b. Relative distances of key terrain.
c. Additional information.

Figure I-4. Facility Physical Security Checklist (continued).

5. KEY TERRAIN.

   a. Predominant terrain.
   b. Drop zones.
   c. Landing and Pickup Zones.
   d. Airfields.
   e. Critical lines of communications.
   f. Additional information.

6. MEDICAL CONSIDERATIONS.

   a. Medical staff and facilities.
   b. Civilian hospitals.
   c. Additional information.

Figure I-4. Facility Physical Security Checklist (continued).

CHECKLIST-RAILWAYS

1. IDENTIFICATION. Route designation (native, military, or other) and segment being studied.

2. LOCATION.

a. Map reference. Include series and sheet numbers on both tactical and air-ground series.
b. End points of segment. Political unit, area, UTM coordinates, and geographical coordinates.

3. OWNERSHIP.

4. TOTAL TRACK LENGTH. Double and single tracks in kilometers.

5. END POINTS OF DOUBLE TRACK SECTIONS. Location (UTM) and area name.

6. TRACK.

a. Gage (millimeters).
b. Rails.
c. Roadway (total width and double or single track).
d. Ditches (depth, width, side slope, lining, condition, cross-section, and structures).

7. ROADBED. Material, total width, and width of shoulders.

8. SUBBALLAST. Material and thickness.

9. BALLAST. Material, size, thickness, and condition.

10. TIES. Material, length, width, depth, and spacing.

11. SPACING OF TRACKS. Centerline-to-centerline.

12. RADIUS OF TIGHTEST CURVE. Location (UTM) and radius.

13. MAXIMUM GRADE. Direction of travel and location.

14. BRIDGES. Cross-reference to bridge collection file.

a. Total number of bridges in segment.
b. Total length of bridging in segment.

Figure I-5. Checklist-Railways.

15. FERRIES. Cross-reference to ferry collection file.

16. TUNNELS, GALLERIES, AND SNOW SHEDS (TGSS). Cross-reference to TGSS collection file.

17. UNDERPASSES. Cross-reference to bridge collection file.

18. MINIMUM CLEARANCES. Horizontal and vertical.

19. AXLE LOAD LIMIT. Metric tons.

20. CULVERTS. Location (UTM) and total number, type, construction material, and bypasses.

21. ELECTRIFICATION.

a. End points of electrified sections (UTM).
b. Power feed (overhead or third rail).
c. Current characteristics (direct current; alternating current).
d. Source of power.

22. MAINLINE JUNCTIONS. Location (UTM), identification of connecting line, and type switch.

23. CROSSOVERS. Location (UTM) and type of switch.

24. PASSING SIDINGS. Locations (UTM), number, double-end or single-end, length, and type of turn.

25. STATIONS.

a. Location (local name and UTM coordinates).
b. Function (passenger, freight, or both).
c. Facilities.

26. FREIGHT-HANDLING FACILITIES.

a. Location (local name and UTM coordinates).
b. Side-loading platforms (number and length).
c. End-loading bays.
d. Sidings with access roads.
e. Freight sheds.

Figure I-5. Checklist-Railways (continued).

f. Turntables (number and diameter).
g. Cranes (type, number, and capacity).

27. YARDS.

a. Location (local name and UTM coordinates).
b. Function (receiving, classification, departure, storage, and so forth).
c. Hump or flat.
d. Number of tracks.
e. Fuel facilities (type of fuel, quantity normally on hand, and maximum storage capacity).
f. Other facilities (water, sand, compressed air, and so forth).
g. Electrification (overhead or third rail).

28. FUEL FACILITIES.

a. Location (local name and UTM coordinates).
b. Type of fuel.
c. Type of storage and capacity.
d. Quantity of fuel normally on hand.
e. Method of loading.

29. REPAIR SHOPS AND LOCOMOTIVE TERMINALS.

a. Location (local name and UTM coordinates).
b. Engine house or turntable.
c. Service facilities.

30. WATERING FACILITIES.

a. Location (local name and UTM coordinates).
b. Source and type of storage.

31. SIGNALS AND TRAIN CONTROL. Location (UTM) and type.

32. CRITICAL POINTS.

a. Type (points subject to rock slides, snow slides, flooding, or subject to interdiction and ambush).
b. Location (local name and UTM coordinates).

33. USE. Average number of trains per day (both passenger and freight).

Figure I-5. Checklist-Railways (continued).

34. SECTIONS IN NEED OF REPAIR. Location and nature of repair, and effort required to repair.

35. CONSTRUCTION, MAINTENANCE, AND REPAIR EQUIPMENT.

    a. Type and characteristics of equipment.
    b. Location of park where kept (UTM coordinates).

36. MAINTENANCE SCHEDULE.

37. PLANNED EXTENSIONS AND IMPROVEMENTS.

38. MAINTENANCE AND CONSTRUCTION STANDARDS.

39. SAFETY AND SECURITY STANDARDS.

40. ROLLING STOCK.

Figure I-5. Checklist-Railways (continued).

CHECKLIST-UNDERGROUND FACILITIES

1. IDENTIFICATION. Native name, military designation, and tunnel number.

2. LOCATION OF PORTALS.

a. Map reference. Include series and sheet numbers of both tactical and air-ground series.
b. Political unit, kilometer points, UTM coordinates, and geographic coordinates.
c. Landmark reference. Description and location of landmark, and azimuth and distance from landmark to nearest portal.

3. LENGTH (portal to portal).

4. TYPE. TGSS.

5. CROSS-SECTION.

a. Shape (semicircular, elliptical, horseshoe, square with arched ceiling).
b. Width of traveled way.
c. Width at widest part.
d. Height of widest part.
e. Height of ceiling at center.
f. Height of ceiling at edge of traveled way.
g. Rise of arch.

6. CONSTRUCTIONS (HORIZONTAL AND VERTICAL). Type, least clearance, and location (meters from nearest portal).

7. RAILROAD TRACKS.

a. Number for which tunnel was designed.
b. Number in use.
c. Gage.
d. Center-to-center spacing.
e. Cross-reference to railway collection file.

8. HIGHWAY.

a. Wearing surface (material, thickness, and condition).
b. Base course.
c. Subgrade.
d. Cross-reference to highway collection file.

Figure I-6. Checklist-Underground Facilities.

9. CHANNEL (water tunnels).

    a. Cross-section dimensioned.
    b. Sides (material and thickness).
    c. Bottom (material and thickness).
    d. Normal depth.
    e. Normal current velocity.

10. ALIGNMENT.

    a. Horizontal (position, curve radius, and curve location).
    b. Vertical (grade percent, length, and location).

11. NUMBER OF MANWAYS. Dimensions and spacing.

12. OBSTACLE TUNNELED.

13. PORTAL. Design and material.

14. LINING MATERIAL. Type, thickness, condition, and points of change.

15. SHORING AND BRACING.

    a. Location and spacing.
    b. Design.
    c. Materials.
    d. Dimensions of members.
    e. Arrangement and spacing of members.

16. STRUCTURAL DESIGN, MATERIALS, AND DIMENSIONS OF GALLERIES AND SNOWSHEDS.

17. GEOLOGICAL DATA.

    a. Material through which tunnel passes.
    b. Geology of adjacent areas.

18. OVERHEAD COVER. Material and depth.

19. DEMOLITION CHAMBERS. Location and dimensions.

20. VENTILATION. Description and adequacy.

Figure I-6. Checklist-Underground Facilities (continued).

21. DRAINAGE. Description, location, and adequacy.

22. LIGHTING FACILITIES. Type, location, and power source.

23. YEAR COMPLETED.

24. BYPASSES. Location, condition, effort required to establish.

25. ALTERNATE ROUTES. (Cross-reference to highway collection file).

26. TRAFFIC CONTROL MARKINGS.

27. APPROACHES. Characteristics, grade, surface, curves, turnouts, and parking areas.

28. SURFACE FEATURES OVER TUNNELS. Vegetation, structures, and surface configuration.

29. EFFECTS OF CLIMATE AND WEATHER.

a. Snow blockage (probable occurrence, effects, and duration).
b. Flooding (periods of occurrence, effects, and duration).

30. SPECIAL GEOPHYSICAL PHENOMENA.

31. SUSCEPTIBILITY TO ABOVE-GROUND DEMOLITIONS.

32. CAMOUFLAGE AND DEFENSES.

33. PRESENT USE.

Figure I-6. Checklist-Underground Facilities (continued).

GLOSSARY

ACRONYMS

AC	Active Component
ACE	analysis and control element
ACOM	US Atlantic Command
ADA	air defense artillery
ADP	automated data processing
AFACSI	Air Force Assistant Chief of Staff for Intelligence
AFMIC	Armed Forces Medical Intelligence Center
AL	Alabama
AMB	aviation maintenance battalion
AMC	US Army Materiel Command
ammo	ammunition
APG	Aberdeen Proving Ground
ARAT	Army Reprogramming Analysis Team
ARCENT	US Army Central Command
ASP	ammunition supply point
ATGM	antitank guided missile
ATP	ammunition transfer point
Aug	August
AVIM	aviation intermediate maintenance
AWACS	Airborne Early Warning
AZ	Arizona
BDA	battle damage assessment
BIDS	Biological Integrated Detection System
bn	battalion
BOS	battlefield operating system
Btu	British thermal unit
C^3I	command, control, communications, and intelligence
CA	Civil Affairs
CB	chemical and biological
CBATEB	US Army Chemical and Biological Agent Technical Evaluation Board
CBDCOM	Chemical and Biological Defense Command
CCIR	commander's critical information requirements
C-E	communications-electronics
CED	captured enemy document
CEE	captured enemy equipment
CEM	captured enemy materiel
CENTCOM	US Central Command
CHATS	CI/HUMINT Automation Tool Set
CI	counterintelligence
CINCLANT	Commander in Chief, Atlantic
CJCMEC	Combined Joint Captured Materiel Exploitation Center
CJTF	Commander, Joint Task Force
CM&D	collection management and dissemination
CMEC	Captured Materiel Exploitation Center
COMTECHREP	Complementary Technical Intelligence Report
COMMZ	communication zone
CONUS	continental United States
COSCOM	Corps Support Command
CSA	corps storage area
CSD	contingency support detachment
CSS	combat service support
CWCC	Centralized Weapons Collection Center
DA	Department of the Army
DARPA	Defense Advanced Research Projects Agency
DCSINT	Deputy Chief of Staff, Intelligence
DCSOPS	Deputy Chief of Staff for Operations
DETECHREP	Detailed Technical Report
DHS	Defense HUMINT Service
DIA	Defense Intelligence Agency
DIAM	Defense Intelligence Agency Manual

DISCOM	Division Support Command
DISE	Deployable Intelligence Support Element
div	division
DMSO	division medical supply officer
DOD	Department of Defense
DOCEX	document exploitation
DOS	disk operating system
DSNET	Defense Secure Network
DTG	date-time group
DTO	district transportation officer
EA	electronic attack
EAC	echelons above corps
EACIC	echelons above corps intelligence center
ECB	echelons corps and below
ELECTRO-OPTINT	electro-optical intelligence
EOD	explosive ordnance disposal
EODTIC	Explosive Ordnance Disposal Technical Information Center
EP	electronic protection
EPW	enemy prisoner of war
ERDEC	US Army Chemical Research Development and Engineering Center
EW	electronic warfare
EXCEN	exploitation center
FSAC	Fire Support Armaments Center
FMA	foreign materiel acquisition
FME	foreign materiel exploitation
FMEP	Foreign Materiel Exploitation Program
FMMEP	Foreign Medical Materiel Exploitation Program
FMIB	Foreign Materiel Intelligence Branch
FMP	Foreign Materiel Program
FMT	Foreign Materiel for Training
FPB	Force Projection Brigade
G1	Assistant Chief of Staff, G1, Personnel
G2	Assistant Chief of Staff, G2, Intelligence
G3	Assistant Chief of Staff, G3, Operations
G4	Assistant Chief of Staff, G4, Logistics
G5	Assistant Chief of Staff, G5, Civil Affairs
HERA	High Explosive Rocket Assist
HHC	headquarters and headquarters company
HOTAS	hands on throttle and stick
HQDA	Headquarters, Department of the Army
hp	horsepower
HUD	heads-up display
HUMINT	human intelligence
I&W	indications and warnings
IEW	intelligence and electronic warfare
IFF	identification, friend or foe
IIR	intelligence information report
IMEP	International Materiel Evaluation Program
IMINT	imagery intelligence
inf	infantry
INSCOM	US Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
IPC	intermediate processing center
IR	information requirements
IRSTS	infrared search and track set
J1	Assistant Chief of Staff, J1, Personnel
J2	Assistant Chief of Staff, J2, Intelligence
J3	Operations Directorate
J4	Logistics Directorate
J5	Joint staff plans and policy
J6	Communications-Electronic Directorate
JCMEC	Joint Captured Materiel

	Exploitation Center
JDISS	Joint Deployable Intelligence Support System
JIC	Joint Intelligence Center
JTF	Joint Task Force
JTIB	Joint Technical Intelligence Branch
Kb	kilobyte
kV	kilovolt
kVA	kilovoltampere
kW	kilowatt
kWh	kilowatthour
LAR	liquid aerosol remove
LIDAR	laser detection and ranging
LNE	liaison element
LNO	liaison officer
LOS	line-of-sight
MACOM	major Army command
MASINT	measurement and signature intelligence
MCC	movement control center
MCO	movement control office
MD	Maryland
MDR	MASINT data requirements
mech	mechanized
med	medical
MEDLOG	medical logistic battalion
MEDSOM	medical, supply, optical, and maintenance
MEF	Marine Expeditionary Force
MFD	multifunctional display
MI	military intelligence
mL	milliliter
MMC	materiel management center
MOS	military occupational specialty
MRC	mission requirements center
MSB	maintenance support battalion
MSE	mobile subscriber equipment
MSIC	US Missile and Space Intelligence Center
MSR	main supply route
NA	not applicable
NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NAVEODTECHDIV	Naval EOD Technical Division
NBC	nuclear, biological, and chemical
NETC	see NAVEODTECHCEN
NGIC	National Ground Intelligence Center
NO	number
NRT	near-real time
NSA	National Security Agency
NTC	Naval Technical Center
NUCINT	nuclear intelligence
NVA	North Vietnamese Army
OB	order of battle
OCONUS	outside continental United States
ODCSINT	Office of the Deputy Chief of Staff, Intelligence
ONI	Office of Naval Intelligence
OPCON	operational control
OPCEN	operations center
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security
PACOM	US Pacific Command
PIR	priority intelligence requirements
POC	point of contact
POL	petroleum, oils, and lubricants
PM	provost marshal
PRETECHREP	Preliminary Technical Intelligence Report
PSYOP	psychological operations
psi	pounds per square inch
RADINT	radar intelligence

RC	Reserve Components
RDTE	research, development, test, and evaluation
R&D	research and development
R&S	reconnaissance and surveillance
RDEC	research, development, and engineering center
RF/EMPINT	radiofrequency/ electromagnetic pulse intelligence
RINT	radiation intelligence
RSP	render safe procedure
RWR	radar warning receiver
S2	Intelligence Officer (US Army)
S3	Operations and Training Officer (US Army)
S4	Supply Officer (US Army)
S&T	scientific and technical
S&TI	scientific and technical intelligence
SALUTE	size, activity, location, unit, time, equipment (spot report format)
SAM	surface-to-air missile
SAR	synthetic aperture radar
SASO	stability and support operations
SATCOM	satellite communications
SCIF	Sensitive Compartmented Information Facility
SIGCEN	signal center
SIGINT	signals intelligence
SIR	specific information requests
SJA	Staff Judge Advocate
SME	subject matter expert
SOP	standing operating procedure
SOR	specific orders and requests
SRBM	short-range ballistic missile
SSC	software support center
STANAG	Standardization Agreement
STICEUR	Scientific Intelligence Center Europe
STICFE	Scientific Intelligence Center Far East
STU-III	Secure Telephone Unit-Third Generation
sup	supply
SUPCEN	support center
TA	Theater Army
TAACOM	Theater Army Area Command
TAMCA	Theater Army Movement Control Agency
TAML	Theater Army Medical Laboratory
TAREX	target exploitation
TBP	to be published
TECHSUM	Technical Intelligence Summary
TECHINT	technical intelligence
TECOM	US Army Test and Evaluation Command
TECRAS	technical reconnaissance and surveillance
TEU	US Army Technical Escort Unit
TGSS	tunnels, galleries, and snow sheds
TIARA	tactical intelligence and related activities
TIR	Technical Intelligence Report
TRADOC	US Army Training and Doctrine Command
trans	transportation
TSS	target sensing system
TTF	TECHINT target folder
TTP	tactics, techniques, and procedures
TV	television
UAV	unmanned aerial vehicle
UIC	unit identification code
US	United States
USAARDEC	US Army Armament Research, Development, and Engineering Center
USAF	US Air Force
USAIC&FH	US Army Intelligence Center and Fort Huachuca

USAMRIID	US Army Medical Research Institute of Infectious Diseases
USATECHDET	US Army Technical Detachment
USMC	US Marine Corps
UTM	universal transverse mercator
XO	Executive Officer

TERMS AND DEFINITIONS

acoustic intelligence	Intelligence derived from the collection and processing of acoustic phenomena.
captured enemy document	Documents captured from the enemy.
captured enemy equipment	Equipment captured from the enemy.
captured enemy materiel	The combination of documents, equipment, and material captured from the enemy.
Class I	Subsistence items and gratuitous health and welfare items (B-rations; meals, ready to eat; fresh fruits; and vegetables).
Class II	Equipment, other than principal items, prescribed in authorization and allowance tables (individual equipment, clothing items, tentage, tool sets, administrative supplies, housekeeping supplies).
Class III	POL, which are petroleum fuels, hydraulic and insulating oils, chemical products, antifreeze compounds, compressed gases, and coal. Class III (bulk) is normally fuel; for example, diesel, motor gasoline, and aviation fuel. Class III (package) is other elements such as lubricants, antifreeze, and fog oil.
Class IV	Construction and barrier materials (lumber, sandbags, and barbed wire).
Class V	Ammunition (small-arms ammunition, artillery rounds, hand grenades, explosives, mines, fuzes, detonators, missiles, and bombs, including special ammunition—chemical and nuclear rounds).
Class VI	Personal demand items; the items that are normally sold through the exchange system

	(cigarettes, candy, soap, and so forth, contained in ration supplemental sundries packs).
Class VII	Major end items (final combinations of items that are assembled for their intended use: vehicles, self-propelled artillery pieces, missile launchers, and major weapon systems—the weapons themselves, not the crews).
Class VIII	Medical material (medicines, stretchers, surgical instruments, and medical equipment repair parts).
Class IX	Repair parts and components, including kits and assemblies, and items required for maintenance support of all equipment (batteries, spark plugs, and axles).
Class X	Material required to support nonmilitary programs; the items used to support CA operations (commercial design tractor for use by local civilians, farms tools, and so forth).
combined operations	Operations conducted by forces of two or more allied nations acting together for the accomplishment of a single mission.
communications intelligence	Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT.
etiologic agent	The cause of a disorder or disease as determined by medical diagnosis.
electro-optical intelligence	Intelligence other than signal intelligence derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (0.01 micrometers) through far infrared (1,000 micrometers). Also called ELECTRO-OPTINT. The collection, processing, exploitation, and analysis of emitted or reflected energy across the optical portion (infrared, visible, and ultraviolet) of the electromagnetic spectrum.
foreign materiel	The all-encompassing term for the weapons

	systems, equipment, apparatus, documents, and supplies of a foreign military force or nonmilitary organization.
Foreign Material Program	The Army program for exploiting, developing, or providing foreign military materiel, commercial representations of foreign materiel with potential miliary application, related foreign documents in the Army inventory, and exploitation reports on this materiel of value to US intelligence, RDTE, and military planning, operations, and training. This includes planning concerning intelligence and non-intelligence acquisition requirements, management of signature and simulator programs, participation in evacuation efforts, and support to the Opposing Forces Program.
joint operations	The integrated military activities of two or more service components—Army, Navy, Air Force, Marine Corps—of the US military.
measurement and signature intelligence	S&TI information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same. Also called MASINT.
materials	Raw substances, scrap, semifinished and finished; supplies.
materiel	All items (including ships, tanks, self-propelled weapons, aircraft, and so forth, and related spares, repair parts and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes.

medical intelligence	That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information which is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors.
nuclear intelligence	Intelligence information derived from the collection and analysis of radiation and other effects resulting from radioactive sources. Also called NUCINT.
radar intelligence	Intelligence derived from data collected by radar. Also called RADINT.
scientific and technical intelligence	The product resulting from the collection, evaluation, intelligence analysis, and interpretation of foreign scientific and technical information which covers: a. foreign developments in basic applied research and in applied engineering techniques; and b. scientific and techical characteristics, capabilities, and limitations of all foreign military systems, and materiel, the research and development related thereto, and the production methods employed for their manufacture. Also called S&TI.
technical intelligence	Intelligence derived from exploitation of foreign material, produced for strategic, operational, and tactical level commanders. Technical intelligence begins when an individual service member finds something new on the battlefield and takes the proper steps to report it. The item is then exploited at succeedingly higher levels until a countermeasure is produced to neutralize the adversary's technological advantage. Also called TECHINT.
unintentional radiation intelligence	Intelligence derived from the collection and analysis of noninformation-bearing elements extracted from the electromagnetic energy unintentionally emanated by foreign devices, equipment, and systems, excluding those

generated by the detonation of nuclear weapons. Also called RINT.

REFERENCES

REQUIRED PUBLICATIONS

Required publications are sources that users must read in order to understand or to comply with this publication.

Field Manuals (FMs)

3-3	Chemical and Biological Contamination Avoidance, 16 Nov 92.
3-5	NBC Decontamination, 17 Nov 93.
34-1	Intelligence and Electronic Warfare Operations, 27 Sep 94.
34-37	Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations, 15 Jan 91.
100-5	Operations, 14 Jun 93.
101-5-1	Operational Terms and Symbols, 21 Oct 85.

RELATED PUBLICATIONS

Related publications are sources of additional information. They are not required in order to understand this publication.

Army Regulations (ARs)

27-52	Consular Protection of Foreign Nationals Subject to the Uniform Code of Military Justice, 5 Nov 68.
59-8	Department of Defense (DOD) Common User Airlift, 20 Aug 82.
75-15	Responsibilities and Procedures for Explosive Ordnance Disposal, 1 Nov 78.
350-2	Opposing Force Program, 15 Jun 83.
380-5	Department of the Army Information Security Program, 25 Feb 88.
380-6	Laser Guidance System Security Classification Guide, 1 Dec 83.
(S) 381-26	Army Foreign Materiel Exploitation Program (U), 27 May 91.
700-99	Acquisition, Accounting, Control, and Disposal of Captured Enemy Equipment and Foreign Materiel, 27 Apr 76.

Defense Intelligence Agency Manual (DIAM)

(S) 58-4	Defense Intelligence Collection Operations Manual (DICOM) (U) Jun 65.
(U) 58-8	Measurements and Signature Intelligence (MASINT) Requirements, 30 Jul 87.
(C) 75-1	Scientific and Technical Intelligence Production (U), 24 Oct 88

Forms

DA Form 1971-6-R	Chemical/Biological Specimen Documentation, Aug 92.
DA Form 2028	Recommended Changes to Publications and Blank Forms, 1 Feb 74.
DD Form 1911	Materiel Courier Receipt, May 82.

Field Manuals (FMs)

3-101-2	NBC Reconnaissance Squad/Platoon Operations, Tactics, Techniques, and Procedures, 10 Aug 94.
5-30	Engineer Intelligence, 22 Sep 67.
9-15	Explosive Ordnance Disposal Service and Unit Operations, 8 May 96.
21-3	Soldier's Manual of Common Tasks (Skill Levels 2, 3, and 4), 1 May 81.
34-3	Intelligence Analysis, 15 Mar 90.
34-52	Intelligence Interrogation, 2 Sep 92.
34-130	Intelligence Preparation of the Battlefield, 8 Jul 94.
101-5	Staff Organization and Operations, 25 May 84.

Joint Chiefs of Staff Publication (JCS Pub)

1-02	Department of Defense Dictionary of Military and Associated Terms, 23 Mar 94.

Standardization Agreements (STANAGs)

1059	National Distinguishing Letters for Use by NATO Forces, Edition 5
2014	Operations Orders, Warning Orders, and Administrative/Logistics Orders, Edition 5
2044	Procedures for Dealing with Prisoners of War, Edition 4
2084	Handling and Reporting of Captured Enemy Equipment and Documents, Edition 5
2097	Nomenclature for Soviet Bloc Army Weapons and Equipment, Edition 5

Supply Bulletin (SB)

708-21	Federal Supply Classification: Part I, Groups and Classes, 1 Jan 89.

Technical Manual (TM)

38-250	Preparing of Hazardous Materials for Military Air Shipments, 25 Nov 94.

INDEX

AFMIC, 2-2, 2-3

Air and Missile Exploitation Element, B-4, B-5, *See also* JCMEC

Air Force, 2-2, 2-4

ammunition officer, 5-7

ARAT. *See also* MASINT
IPC, A-5
production centers, A-5
TSS, A-5

areas of exploitation, 3-8

Army, 2-2, 2-5
AMC, 2-2, 2-5
INSCOM, 2-2, 2-3, 2-5, 2-6
ODCSINT, 2-2, 2-5

Army Foreign Materiel Program, 2-5

Army Materiel Command
CBDCOM, 2-2, 2-5
STICEUR, 2-2, 2-5, A-3
STICFE, 2-2, 2-5
TECOM, 2-2, 2-5
TEU, 2-2, 2-5

automation systems, 3-9

aviation officer, 5-5

battlefield TECHINT, 3-1
203d MI Battalion role, 3-1, 3-3
ammunition officer role, 5-7
analysis, 4-8
aviation officer role, 5-5
channels, 3-5
chemical officer role, 5-5
CMEC role, 3-2, 3-6
Collection Company, 3-3
command surgeon role, 5-6
definition, 3-1
elements, 5-1
engineer officer role, 5-5
EOD role, 5-6
exploitation, 4-7
Exploitation Company, 3-3
JCMEC role, 5-7
MASINT Detachment, 3-3
NTC Detachment, 3-3
provost marshal role, 5-6
reporting sequence, 4-7
reports, E-1
responsibilities, 5-1
Staff Judge Advocate role, 5-7

BDA, A-2. *See also* MASINT

biomedical samples, Appendix H

CA elements, 5-10

CB sampling
enviornmental, H-2
liquid and vapor, H-7
packaging, H-8
procedures, H-1
soil, H-7
vegetation, H-7
water, H-7

CBDCOM, 2-5

CCIR, 4-1

C-E and IEW Exploitation Element, B-4, B-6, *See also* JCMEC

C-E TECHINT, 3-10

CED. *See* CEM

CEE. *See* CEM

CEM, 1-6, 1-7, 3-1
aviation officer role, 5-5
battlefield TECHINT responsibilities for, 3-1, 4-3, 5-1,
CMEC responsibilities, 3-3 through 3-9, D-5
command responsibilities, D-6
disposition and destruction, D-9, D-10
exploitation of, 3-4, 3-5
exploitation requirements, F-2
handling and evacuation of, Appendix C, D-4
handling and processing, B-2 through D-8,
information flow, 4-4
JCMEC responsibilities, 5-7, Appendix B
marking and tagging, B-2, C-9 through C-13, D-6
policy, D-4
provost marshal role, 5-6
recovery, C-14
reporting, D-3, D-4, Appendix E
reporting procedures, Appendix E
requirements, D-9
S4 responsibilities, 3-4
SJA role, 5-7
staff responsibilities, 5-1 through 5-4

checklists, Appendix I

chemical officer, 5-5

CJCMEC, 3-3, 3-4, 3-8, 5-7. *See also* CMEC and JCMEC

CM&D element, B-4, B-6. *See also* JCMEC

CMEC, 1-5, 3-2, C-1, C-2, C-6, C-8, F-2
See also CJCMEC; JCMEC; JTIB
functions, 3-3 through 3-10, D-6
S4 responsibilities, 3-4

CMEC (Forward)
functions, 3-7
handling CEM, 4-3, 4-5, C-9
J4/G4 responsibilities, 5-4
logistic functions, C-2
responsibilities, 4-2, 4-6

collection. *See* TECHINT collection

collection company, B-4, B-6. *See Also* JCMEC

collection managers, 3-3

collection plan, F-1

command surgeon, 5-6

COMTECHREP, E-1, E-3
Type A, E-4
Type B, E-6
Type C, E-9

conflict. *See* military environments

DARPA, 2-2, 2-4

Defense Intelligence Agency
AFMIC, 2-2, 2-3
DHS, 2-2, 2-4
MSIC, 2-2, 2-3

DETECHREP, E-1, E-10

DHS, 2-2, 2-4

dissemination, *See also* TECHINT
definition, 4-6
of CEM, 5-8
of EOD information, 5-6
of TECHINT products, 3-1, 4-6
of TIRs, E-1, E-11
staff section duties, 5-1

DOD S&TI community, 2-2

EAC, 2-6
at force projection brigades, A-1
TECHINT support, 3-6, D-2

ELECTRO-OPTINT, A-3

engineer officer, 5-6

engineer topographic and terrain units, 5-11

EPW
evacuation and processing, 5-1, C-6
tags, C-9 through C-13

EXCEN, B-4, B-5. *See also* JCMEC
Air and Missile Exploitation Element, B-5
C-E and IEW Exploitation Element, B-6
CM&D Element, B-6
Ground Exploitation Element, B-5
Maritime Exploitation Element, B-5
Medical and NBC Exploitation Element, B-5

force projection brigades, 2-2, 2-6, A-3

foreign materiel exploitation, 2-5, 2-7, B-3

Foreign Materiel Exploitation Program, 2-3, 2-6

Foreign Materiel for Training Program, 2-6, 3-5

Foreign Materiel Intelligence Branch, 1-6

Foreign Medical Materiel Exploitation Program, 2-3

foreign technological developments, 2-1

geophysical intelligence, A-4

Ground Exploitation Element, B-4, B-5. *See also* JCMEC

historical perspectives
Grenada, 1-6
Gulf War, 1-6
Haiti, 1-8
Korean War, 1-5
Raid on Bruneval, 1-3
Somalia, 1-7
Vietnam, 1-5
World War II, 1-2

information requirements, 5-6, D-1, F-1
developed by JTIB, 4-1
JCMEC role, 5-7

INSCOM functions, 2-6
FPB, 2-2, 2-6
FMEP 2-3, 2-6
FMT Program, 2-5
MASINT responsibilities, A-2
NGIC, 2-2, 2-6
S&TI exchange, 2-3
TECHINT operations responsibilities, 2-5

intelligence collection
management, B-3
MASINT mission, A-1

intelligence cycle, 4-1, 4-6

intelligence production center
AFMIC, 2-3
MSIC, 2-3

intermediate processing centers, A-5

J1/G1
responsibilities, 5-1, D-1

J2/G2, 3-2
compliance with Geneva Convention, 5-3
relationship with capturing units, 5-8
relationship with Command Surgeon, 5-6, D-4
responsibilities, 4-1, 5-2

J3/G3 responsibilities, 5-1 through 5-6

J4/G4 responsibilities, 5-4, C-3

J5/G5 responsibilities, 5-5

JCMEC, 1-6, 3-4, 3-8. *See also* JTIB; CMEC; CJCMEC
exploitation requirements, 3-7, F-2,
in joint or combined operations, 3-4
LNE, 4-8, D-4
organization, 3-3, B-4
purpose, B-1
responsibilities, 3-8, 4-2, 5-7, B-1, D-11
role in intelligence cycle, 4-1 through 4-8
required reports, 4-7, Appendix E

JTIB, 4-1, B-1, B-2. *See also* JCMEC; CMEC; CJCMEC
in joint operations, 3-6
missions, 3-6, 4-7
TECHINT reports, 4-6, E-1

lessons learned, 1-8

liaison elements. *See also* TECHINT
composition, 3-2, 3-8, B-1, B-3
responsibilities, 3-4, 3-5, 4-3, 4-8, B-3, E-1

Maritime Exploitation Element, B-4, B-5. *See also JCMEC*

MASINT, 2-4, 2-6, A-1
agency responsibilities, A-2
BDA, A-2
data requirements, 2-6
in support of
collection teams, 3-4, 3-8
force modernization, A-6
S&TI, 2-6
TECRAS, 2-6
mission, 3-3, A-1
RINT integration, A-4
TIARA systems, A-1
training, 2-7

materials intelligence, A-4

Medical and NBC Exploitation Element, B-4, B-5. *See also JCMEC*

medical TECHINT, 3-10

medical units, 5-11, D-12
collection of samples, H-2, H-9, H-11

MEF intelligence element, 3-9

military environments
conflict, 1-2, 3-3, B-3
peacetime, 1-2, 2-5, A-1
war, 1-2, 1-5, 1-8, 3-3, 3-6, A-1

military police, 5-6, C-6
CEM role, 5-6, 5-8, 5-11, C-6, C-14
duties on the battlefield, 5-11
in support of JCMEC, B-2
responsibilities of, 5-6, 5-11, C-6, C-14

mobility TECHINT, 3-10

MSIC, 2-2, 2-3

munitions TECHINT, 3-10

NAIC, 2-2, 2-4

National Ground Intelligence Center, 2-2, 2-6, A-3, G-1

Navy, 2-2, 2-4
MCIA, 2-2
ONI, 2-2, 2-4
EOD training, 2-4

NBC, B-5, C-2, C-6, C-8, H-1, H-3, H-13
capturing unit role, 5-8
chemical officer role, 5-5
command surgeon role, 5-6
equipment, 4-9
functional area of TECHINT, 3-10, 4-3, 4-9, C-7
J2/G2 responsibilities, 5-2
materials intelligence, A-4

NBC *(continued)*
role of TEU, 2-2,2-5
samples, 5-11, D-11, H-3

NBC reconnaissance teams
responsibilities, 5-11, H-2, H-3, D-6, D-11, D-12

NBC TECHINT, 3-10

NSA, 2-2, 2-4

NTC mission, 3-5

NUCINT, A-5

ODCSINT, 2-2
responsibilities, 2-3, 2-5, A-3

OPCEN, B-4. *See also* JCMEC

operational support, H-1, 3-4 through 3-10
role of commanders, 1-2, B-3
TECHINT requirements, 2-1, 3-4, 3-5

peacetime engagement. *See* military environments

PIR, D-1, F-1
capturing units, 5-8
command surgeon, 5-6
JCMEC, 5-8

POL, C-4, C-6, I-2

PRETECHREP, E-1, E-2, E-3

processing. *See* TECHINT

production. *See* TECHINT

provost marshal, 5-6

PSYOP teams, 5-9, 5-10

radar intelligence, A-4

radio frequency intelligence, A-4

RC TECHINT, 3-6, 3-9

RDEC, 2-5

responsibilities of
capturing units, 5-8
engineer topographic and terrain units, 5-10
EOD, 5-6, 5-12
J1/G1, 5-1
J2/G2, 5-2
J3/G3, 5-3
J4/G4, 5-4
J5/G5, 5-5
JCMEC, 3-8, 4-2, 5-7, B-1, D-11
military police, 5-6, 5-11, C-6, C-14
MI units, 5-9
NBC reconnaissance teams, 5-11
SOF, 5-9
staff officers, 5-5

S&TI. *See also* S&T
203d MI Bn, 2-6, 2-7
AFMIC role, 2-3
Air Force role, 2-4
Army role, 2-5
characteristics, 1-1
CMEC role, 3-7
community structure, 2-1, 2-2, F-3
definition of, 1-1
DIA role, 2-3, F-1
directorate responsibilities, 2-3
exploitation of, 4-8
fulfilling TECHINT requirements, 2-3
historical perspective, 1-6, 1-7, 1-8
JCMEC role, 5-8, F-3
JTIB role, 4-2, 4-6
MSIC role, 2-3
NAIC role, 2-4
Navy role, 2-4
ODCSINT responsibilities, 2-5
process and procedures, 4-6, 4-8
purpose of, 2-1

S&TI community, 2-1, 2-2, 4-2

S&TI directorate, 2-3

SALUTE
example of, E-1, E-2
reporting, 4-7, 5-8, C-7, C-14, D-3

scientific and technical information.
See S&TI

SIGCEN, B-4, B-6. *See also* JCMEC

signatures analysis, 3-10

SIR, 4-1, 4-3

SJA, 5-3. *See also* J2/G2

SOF
aviation units, 5-10
CA elements, 5-10
PSYOP teams, 5-10
ranger units, 5-9

Special Forces and Ranger Units, 5-9

Special Operations Aviation Units, 5-10

special technical reports, E-1

SUPCEN, B-4

STICEUR, 2-5

203d MI Battalion, 2-6
CMEC function, 3-3, 3-4
collection company, 3-3, 3-4
exploitation company, 3-3, 3-4
HHC, 3-3
JCMEC and CJCMEC, 3-3, 3-8
MASINT Detachment, 3-3, 3-5
mission, 2-6, 3-3, F-2
NGIC, 3-3
NTC Detachment, 3-3, 3-5
organization, 3-3

TAML, B-5, D-6, D-13, H-9, H-11, H-12

target folder, 4-2

target sensing systems, A-5

TECHINT
at operational level, 1-2
at strategic level, 1-1, 2-1
at tactical level, 1-2
battlefield operations, 3-1, 3-2
CEM, C-1
collection, 3-1 through 3-10 4-3, F-1
definition, 2-1
dissemination, 4-6
goals, 2-1
historical perspective, 1-1 through 1-9
in force protection, 1-9
input to Intelligence Annex, D-1
in relation to MASINT, A-1, A-6
intelligence cycle, 4-1, 4-7
lessons learned, 1-8
liaison elements, 3-5, 3-9, 4-3, 4-8, D-2, F-1
mission, 1-1
objectives, 2-1
processing, 4-6
production, 4-6
reports, E-1
responsibilities, 5-1
support to the warfighter, 1-1
target folder, 4-2
templating, 4-2

TECHINT analysts, 3-7
CEM responsibilities, 3-1, 5-12
exploitation function, 3-4, 3-8, 4-8, 4-9, C-6
reports, E-1

TECHINT collection, 3-1 through 3-10, 5-11
chemical officer role, 5-5
CM&D, B-6
definition, 4-3
historical perspective, 1-8
TECHINT Collection *(continued)*
intelligence cycle, 4-1 through 4-7
J2/G2 role, 5-2

J4/G4 role, 5-4
J5/G5 role, 5-5
JCMEC role, B-1 through B-6
JTIB role, B-2
NBC reconnaissance role, 5-11
of CB samples, D-11 through D-14
of CEM, D-4, B-2
POL unit role, C-4, C-6
priorities, D-7

TECHINT Collection Company, 3-4, B-6

TECHINT collection plan, F-1

TECHINT collection teams
automation systems, 3-10
C-E, 3-10
Medical, 3-10
Mobility, 3-10
Munitions, 3-10
NBC, 3-10
Weapons, 3-10

TECHINT Exploitation Company, 3-3. *See also* HHC and CMEC

TECHINT LNEs, 3-2 through 3-8
at Corps, 4-8, 5-8, C-9, E-1, E-4
composition, 3-8

TECHINT operations, 3-2

TECHINT reports
COMTECHREP, E-1 through E-10
DETECHREP, E-1, E-10
PRETECHREP, E-1, E-2, E-3
SALUTE, E-1, E-2
special technical reports, E-1
Technical Intelligence Update Report, E-1, E-10
TECHSUM, E-1, E-10
TIR, E-1, E-11

TECHINT training, 2-6

technical escort unit, 2-5, H-2, H-3

technical intelligence. *See* TECHINT

Technical Intelligence Update Report. See TECHINT reports

TECHSUM. *See* TECHINT reports

TECOM, 2-5

TECRAS, 2-7, A-1, A-3

templating, 4-2

Theater ACE, 4-6

Theater and Supporting Command Surgeon, 5-6

Theater Surgeon General, D-4, D-11, D-13

TIARA, A-1

TIR. *See* TECHINT reports

war. *See* military environments

warfighter
mission, 1-1
TECHINT support, 1-1, 1-7, 2-1, 3-1

war trophies, 5-3, B-3, C-6, C-15

weapons TECHINT, 3-10

By Order of the Secretary of the Army:

DENNIS J. REIMER
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
04298

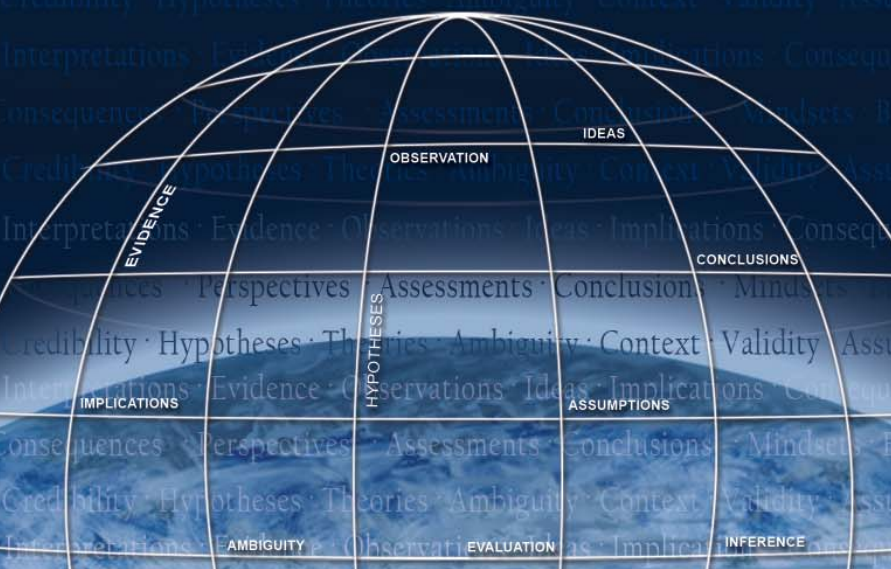
DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number 111132, requirements for FM 34-54.

*U.S. Government Printing Office: 1997 - 628-027/80040

National Defense Intelligence College

Occasional Paper Number Fourteen



Critical Thinking and Intelligence Analysis

Consequences · Perspectives · Assessments · Conclusions · Mindsets · Bia
Credibility · Hypotheses · Theories · Ambiguity · Context · Validity · Assu
Interpretations · Evidence · Observations · Ideas · Implications · Consequ

David T. Moore

Interpretations · Evidence · Observations · Ideas · Implications · Consequen
Consequences · Perspectives · Assessments · Conclusions · Mindsets · Biase
Credibility · Hypotheses · Theories · Ambiguity · Context · Validity · Assu

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Critical Thinking and Intelligence Analysis	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense Intelligence College,Washington,DC,20340-5100**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**158**	

The National Defense Intelligence College supports and encourages research on intelligence issues that distills lessons and improves Intelligence Community capabilities for policy-level and operational consumers

Critical Thinking and Intelligence Analysis, Second Printing (with revisions)
David T. Moore

This series of Occasional Papers presents the work of faculty, students and others whose research on intelligence issues is supported or otherwise encouraged by the National Defense Intelligence College (NDIC) through its Center for Strategic Intelligence Research. Occasional Papers are distributed to Department of Defense schools and to the Intelligence Community, and unclassified papers are available to the public through the National Technical Information Service (www.ntis.gov). Selected papers are also available through the U.S. Government Printing Office (www.gpo.gov).

This work builds on earlier publications in this series, particularly Occasional Papers Two, Six, and Seven; *Getting Intelligence Right: The Power of Logical Procedure*, *Intelligence Essentials for Everyone*, and *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*. The author's insights have been developed through years of creative interaction with the Community's leaders in analytic methododology, and tested for practicality by successive waves of students in training and education courses throughout the Community.

Proposed manuscripts for these papers are submitted for consideration to the NDIC Press Editorial Board. Papers undergo review by senior officials in Defense, Intelligence and civilian academic or business communities. Manuscripts or requests for additional copies of Occasional Papers should be addressed to Defense Intelligence Agency, National Defense Intelligence College, MC-X, Bolling AFB, Washington, DC 20340-5100.

This publication has been approved for unrestricted distribution by the Office of Security Review, Department of Defense.

Russell Swenson@dia.mil, Editor and Director
Center for Strategic Intelligence Research

Critical Thinking and Intelligence Analysis

Occasional Paper Number Fourteen

David T. Moore

National Defense Intelligence College
Washington, DC
March 2007

The opinions expressed in this paper are those of the author. They do not represent the official position of the National Security Agency, the Department of Defense, or any other agency of the U.S. Government.

Contents

Figures and Tables v

Preface vii

Foreword
Mark M. Lowenthal ix

Commentary
Jeffrey R. Cooper xiii
Francis J. Hughes xvi
Gregory F. Treverton xvii

Acknowledgments xix

Abstract 1

Definitions 2

Introduction: How Do People Reason? 3

What Is Critical Thinking? 8
Defining Critical Thinking 8
Standards for Critical Thinking 10
Skill-Based Definitions 13
A Disposition to Think Critically 15
The Role of Questions 17
Pseudo-Critical Thinking 18

What Can Be Learned from the Past?
Thinking Critically about Cuba 20
Deploying the Missiles 20
Assessing the Implications 24
Between Dogmatism and Refutation 26
Lacking: Disconfirmation 29
The Roles of Critical Thinking in the Cuban Crisis 33
Winners and Losers: The Crisis in Context 37
Ten Years Later, They Meet Again 45
Judgment: Critical Thinking Would
Have Made a Difference 46

How Can Intelligence Analysts Employ Critical Thinking? 48
The Poor Record 48
Assessing Evidence 51
Facilitating Evidentiary Assessment 56
Embracing a Methodology 57
Creating Better Inferences 58
Producing Intelligence 59

How can Analysts be Taught to Think Critically? 61
Critical Thinking Education
Outside the Intelligence Community 61
Critical Thinking Education
Inside the Intelligence Community 64
Implications of Teaching Critical Thinking 66
Evaluating Teaching Models 68
Encouraging Analysts to Think Critically 69
Persuading to Improve Analysis 70

How Does Critical Thinking Transform? 74
Transforming Intelligence Corporations 74
Learning from Early Adopters 75
The Costs and Benefits of Thinking Critically 76
Validation 84

What Other Points of View Exist? 86

What Does the Future Hold? 90

Conclusion 95

Appendix: NSA's Critical Thinking
and Structured Analysis Class Syllabus 97

Bibliography 117

About the Author 133

Colophon 134

Figures and Tables

Figure 1: A Comparison of Inductive, Deductive, and Abductive Reasoning 5

Figure 2: Elements of Thought..... 9

Figure 3: A Continuum of Intellectual Standards. 10

Figure 4: Levels of Questioning: Critical Thinking in a Social Setting. 17

Figure 5: Respective Ranges of Soviet SS-4 MRBM and SS-5 IRBM Missiles..... 22

Figure 6: A Place for Analysis between Dogmatism and Criticism 28

Figure 7: Detail of a U-2 Photograph of an SS-4 MRBM Launch Site, San Cristobal, Cuba, 14 October 1962 30

Figure 8: U-2 Tracks over Cuba, 4–14 October 1962 32

Table 1: A Comparison of Different Sets of Critical Thinker's Competencies 14

Table 2: Applying Paul and Elder's Critical Thinking Model to the Situation in Cuba, August–September 1962 27

Table 3: A Comparative Assessment of Rival Motivations 38

Table 4: Goals and Outcomes in the Cuban Missile Crisis..... 44

Table 5: How Analysts Decide 50

Table 6: Cooper's Analytic Pathologies..... 82

Table 7: Analysis: Past, Present and Future 92

Preface

The world in which intelligence analysts work has changed dramatically over the 67 years since the beginning of the Second World War. Adversaries have shifted from large armies arrayed on battlefields to individuals lurking in the shadows or in plain sight. Further, plagues and pandemics, as well as floods and famines, pose threats not only to national stability but even to human existence. To paraphrase a Chinese curse, we certainly live in interesting times.

Our times demand fresh, critical reasoning on the part of those tasked to assess and warn about threats *as well as those tasked to act on those threats*. Education in the bases and practices of intelligence foraging and sensemaking – often called intelligence collection and analysis – is a means by which this can be accomplished. Indeed, the Intelligence Reform and Terrorism Prevention Act of 2004 legislates improved education for intelligence analysis. But, that education is not specifically defined. This volume provides a framework for one area of the act's educational requirement: improving how analysts think – and by extension, how policymakers act. It asserts that people who are skilled critical thinkers are better able to cope with interesting times than those who are not.

The model for thinking developed here also provides specific tools for coping with accelerating disruptive technologies. Such technologies routinely appear in the hands of adversaries. They also offer intelligence professionals capabilities to counter adversaries in novel ways. The key is knowing which technologies are truly disruptive in advance, which pose threats, and which can be harnessed to mitigate threats. Critical thinking – as it is here defined and developed – provides part of the solution as it encourages careful consideration of the available evidence, close examination of presuppositions and assumptions, review of the alternate implications of decisions, and finally, discussion of alternative solutions and possibilities. In short, it equips intelligence professionals with an essential tool for their work.

Foreword

Mark M. Lowenthal
Former Assistant Director of Central Intelligence
for Analysis and Production
President, Intelligence & Security Academy, LLC

Some years ago, when I worked at the Congressional Research Service, my colleague next door had a sign in his office: "Thinking is hard work. That's why so few people do it." Indeed. As sentient beings we think all the time. Our waking, conscious hours are full of thoughts: what to wear; what to eat; how to respond to someone. These all take thought. One might venture to say that we think almost unconsciously through most of our day.

And then there is that *other* thinking: Thinking about the conundrums that we face, the alternatives and choices we have to make on larger issues, the dilemmas we wish to resolve. This *is* hard work. And if the work you do is largely intellectual in nature, then you are thinking that much more often about these more difficult problems. This is not to suggest that those who work with their hands or in crafts or industry do not think. Of course they do. But these people, in the end, have something physical to show for their thought and its execution. Intellectuals only have their thoughts to show, presumably expressed for others in some way.

Intelligence officers are engaged in an intellectual pursuit. They are trying to solve puzzles, resolve uncertainties, discover the nature and meaning of things that others would keep secret. They must have an entire intellectual apparatus to help them identify the problem, assess the parts they know and the parts they do not, come up with an explanation of what is going on and then express it in a way that others – including an audience not steeped in their own techniques – can understand.

As one would expect, the Intelligence Community has spent a fair amount of time thinking about how it does analysis. But most of this has been spent on techniques, presentation and outcomes; much less has been spent on what happens intellectually while you are thinking. That, indeed, is what critical thinking is about: the ability to step out of one's thoughts, if you will, to examine them and the process that brought them about even while you are thinking them. It does not require some higher level of cosmic consciousness or a split personality. It does require training and thought! So now we are thinking about our thinking while we are thinking – a mental triple play, if you will. This is no mean feat and it is a very crucial skill for intelligence analysts.

John McLaughlin, a former Deputy Director of Central Intelligence, has observed that one of the major perceptions that separates intelligence officers from the policy makers is that policy makers tend to be optimists, believing they can get things done, while intelligence officers tend to be skeptics, knowing that little is known with certainty. Like everyone else, however, intelligence analysts can be adamant about their conclusions, understanding the path they took to reach them, and well-satisfied that they have done the right work and come to the right end. That is where critical thinking comes in. The ability to examine how you came to your conclusion is an important adjunct to your other intellectual work. You may be certain or you may not – which is also acceptable. But you owe it to yourself and to your readers to have examined how you got there.

This is not as easy as it sounds for intelligence analysts for the simple reason that they are usually very pressed for time. There are not a lot of lulls in the analyst's work week, which makes it very difficult to be introspective. This means that critical thinking ought to be something that is ingrained in analysts as part of their training, so that it becomes reflexive. But to do that, one must first understand critical thinking – what it is, how to do it, how to teach or learn it. That is the outstanding value of this monograph by David Moore.

The Intelligence Community is filled with people happily working away under a cloak of anonymity, satisfied in making their contribution to part of a larger activity about which very few beyond their immediate circle of co-workers will know. David Moore has long been one of these contributors. In addition to his duties as an intelligence officer at the National Security Agency, David Moore has devoted many fruitful hours to the intellectual underpinnings of intelligence, especially to what makes analysts and what makes better analysts. His work on analytic core competencies, written with his colleague Lisa Krizan, is a fascinating dissection of the intellectual attributes that make up an intelligence analyst. It was also a very influential work, becoming a prime motivator in the creation of the Analytic Resources Catalog created under Director of Central Intelligence George Tenet and now much touted by Director of National Intelligence John Negroponte.

This new monograph on critical thinking will serve a similar purpose. Much has been written in the last five years about intelligence and about the errors that it can make. Some of this has been diagnostic; much of it has been blithely condemnatory. Prescriptions about connecting dots better (an absurd metaphor), about the need to share information better and alarms about groupthink do not get us closer to improvements in the art, craft and profession of intelligence. New ways of thinking about our profession, new ways of doing our work and new ways of assessing it will be useful. Critical thinking needs to be at the top of this list of desiderata.

I would like to believe that we are on the verge of a renaissance in intelligence studies, and more specifically in the intellectual basis of intelligence analysis. There are many straws in the wind: discussions about a national intelligence university and a lessons learned center, more schools offering serious courses about intelligence and books like this. Critical thinking is and should be critical for all analysts and they will profit from this book.

Commentary:

Jeffrey R. Cooper
SAIC Technical Fellow
Science Applications International Corporation

David Moore has written an elegant and largely persuasive argument for the Intelligence Community to move forthrightly and adopt critical thinking in order to improve the quality both of its analytic processes and its intelligence judgments. Since I have recently written about the need for the Community to identify and cure deep-seated and systemic "analytic pathologies," I am obviously sympathetic to the general case for incorporating more rigorous analytic processes—among which "critical thinking" is one attractive approach.[1] Along with Moore, I also believe strongly that the traits often associated with critical thinking need to become fundamental characteristics of every analyst and to be practiced consistently in their work habits. Moore discusses these aspects at some length and highlights their value to making sounder judgments.

In doing so, he makes a compelling case that critical thinking can help analysts reshape their methods in ways that help to avoid damaging errors and enhance judgment. He and I agree with Rieber and Thomason that we should validate the potential improvement before widespread deployment.[2] The need for validation raises some related points concerning the criteria for evaluation and measurement. As Philip Tetlock has noted, on the one hand, one can do evaluation by assessing whether a process (assumed to be good) has been followed; one the other hand, one can also assess

1 Jeffrey R. Cooper, "*Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*" (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005). Cited hereafter as Cooper, *Pathologies*.

2 Steven Rieber and Neil Thomason, "Toward Improving Intelligence Analysis: Creation of a National Institute for Analytic Methods," *Studies in Intelligence* 49, no. 4 (Winter 2006), 71.

quality by looking at the products themselves.[3] However, following a good process does not guarantee good products, nor does a good judgment necessarily validate the quality of the analysis or the analyst. Both approaches have flaws as methods of validation.

I urge the leadership of the Intelligence Community to place far more emphasis on structured analytic methods. In my view, the transformation of the intelligence enterprise demands a more curious, more agile, and more deeply thoughtful cadre of intelligence analysts—but it should also require the same traits among its intelligence organizations and the intelligence enterprise as a whole. Moore notes that "Investment in critical thinking as part of the analysis process minimizes the likelihood of specific failures" (page 81). However, from my perspective, critical thinking (and other structured methods) are more important for changing the organization's overall approach to analysis, rather than in improving specific judgments or preventing particular failures.

I believe such methods are crucial in preventing systemic analytic pathologies from developing, exactly because the Community lacks many of the desirable self-corrective mechanisms found in science. Second, while Moore focuses on the role of critical thinking in improving an individual analyst's ability to make good judgments, my view emphasizes the importance of more rigorous processes for the organization as a whole if it is to improve its capacity to meet user needs. Indeed, given my emphasis on the systemic nature of the pathologies that afflict intelligence analysis, structured analytic methods become a first line of defense in preventing networks of errors—they are like "ripstops" that keep problems from propagating into wider "error-inducing systems," in Perrow's terms. The quality of "mindfulness" and a more self-reflective process are essential if the intelligence organizations are to acquire some of the desirable characteristics of high-reliability organizations. While critical thinking can clearly assist individual analysts, and these "memes" can be spread through viral dissemination, I would place far more emphasis on fomenting social and organizational changes as remedies.

---

3 Philip E. Tetlock, *Expert Political Judgment: How Good Is It? How Can We Know?* (Princeton, NJ: Princeton University Press, 2005).

Finally, exactly because Moore focuses so tightly on the value of critical thinking to improve how individual analysts reason, he largely ignores the important role such habits should, and could, play in the "social construction" of intelligence analysis *and its communication to users of that intelligence*. The use of more structured techniques "to present more effective assessments" should go beyond simply convincing policymakers "to question their own assumptions on the issues" (page 80). By restructuring both the analytic process and the modalities of interactions with policy users, critical thinking techniques can draw policy users into "co-creating" important judgments and, by doing so, get them to adopt some of the important attributes of critical thinking. This internalization would be more powerful than hoping the exquisite brilliance of the improved analytic judgments might make them more palatable.

These minor quibbles aside, David Moore has highlighted for the Intelligence Community and its users some tangible methods for improving intelligence analysis and addressing systemic analytic pathologies.

Commentary

Francis J. Hughes
Professor, National Defense Intelligence College

> The truly difficult problems of the information age are not technological; rather, they concern ourselves – what it is to think, to reason, and to engage in conversation [using] … new analytic techniques, new conceptual tools with which to analyze and understand the workings of the human mind.
>
> —Keith Devlin, *Goodbye Descartes: The End of Logic and the Search for a New Cosmology of the Mind*, 1997

David Moore has undertaken a valuable initiative on behalf of the Intelligence Community by producing this monograph on critical thinking. In doing so, he has addressed the concerns of Keith Devlin and many other scholarly writers on the subject of human reasoning. By contextualizing the concept and practices of critical thinking within intelligence analysis, he has set forth a much-needed cognitive linkage between intelligence analysis and the human thought process, which, as he states, remains otherwise "poorly understood."

Mr. Moore has developed a methods-of-thinking course, outlined in the Appendix to this paper, which should guide the collection of evidence, the reasoning from evidence to argument, and the application of objective decision-making judgment. Critical thinking in intelligence depends primarily on a conscious application of suitable habits of thought, and the course certainly promises to advance the education of intelligence professionals.

Commentary

Gregory F. Treverton
RAND Corporation
Former Assistant Director of Central Intelligence for
Analysis and Production
and Vice-Chairman, National Intelligence Council

David Moore has added his powerful voice to those calling for America's intelligence analysts to be more self-conscious about their methods and more venturesome in applying more formal methods. His starting point is critical thinking, but his strong case embraces a range of techniques from Paul and Elder's checklist, to analysis of competing hypotheses (ACH), to Factions analysis, which is really a way to be more systematic in aggregating subjective judgments, to techniques such as those developed by the Novel Intelligence from Massive Data (NIMD) project. These help analysts search for patterns and test hypotheses. Moore's discussion pays particular attention to critical thinking about *evidence* – that is perhaps natural given that the National Security Agency is his home agency, but it is also a welcome emphasis.

My own explorations of the analytic agencies over the last few years confirm my own experience managing the National Intelligence Council (NIC): In general, U.S. intelligence analysis has been neither very self-conscious about its methods, nor made much use of machines and formal analytic tools. That is Moore's point of departure, and it is a case made graphically by Rob Johnston, on whose work Moore draws. The state of affairs Moore and others describe is changing, and his work should contribute to accelerating that change, in a variety of experiments and pilot projects.

Moore's paper raises at least two intriguing questions at its edges. He rightly takes issue with Malcolm Gladwell's book about the power of unconscious thought or "deliberation without attention."

That said, clever defense lawyers often discredit ballistic experts by asking them to be explicit about how they reached their conclusions. Likewise, chess masters can be reduced to middle-weights by having to explain the logic of their moves. In both cases, the decisions result from patterns as much sensed as seen, the result of thousands of previous cases. I sometimes worried at the NIC that the more we required analysts to be explicit about their methods, the more we risked turning them into middle-weights.

Finding ways to incorporate not just expertise, but also hunch and sense into intelligence analysis is a challenge that lies ahead. The Defense Advanced Research Projects Agency's ill-fated experiment a few years ago seeking to establish a terrorism futures market was testimony to how hard the challenge will be. When the idea became public, every politician – right, left and center – quickly denounced it as borderline immoral. Over the ensuing days, however, a wide range of analysis commented on what a good idea it might have been when information is in short supply and there is a premium on sensing patterns before they become facts.

The second issue is consumers of intelligence, who figure only at the margins of Moore's discussion. We can only hope he is right that better analysis will find, and perhaps help create, a better audience. But the unboundedness of the terrorist threat we now face means that intelligence and policy no longer share a "story" comparable to that about state threats, like the Soviet Union. In principle, that would suggest that policy should accord more time and attention to intelligence, but that is not likely to happen in Washington's whirligig.

Thus, intelligence will need to be as creative in finding new ways to work and communicate with policy officials as it is in improving its analytic techniques. In the process, it will need to rethink what it regards as its *product.* I came to think at the NIC that our product was not really National Intelligence Estimates but, rather, National Intelligence *Officers* – people, not paper, and people in a position to come to know their policy counterparts and to make their expertise available informally, in meetings or at lunch.

Acknowledgments

The first notes for this paper were begun a year prior to the 11 September 2001 terrorist attacks in New York and Virginia as part of research conducted with a peer, Lisa Krizan, on a set of core competencies – knowledge, skills, abilities, and an associated set of personal characteristics – for successful intelligence analysis. At the time, the notion of critical thinking was at best vaguely understood by members of the Intelligence Community, and the National Security Agency (NSA) was no exception. Six years later critical thinking is a recognized key skill by which intelligence readiness is defined at NSA. Similar growth in its importance is recognized elsewhere in the Community. This recognition is due in part to the work of Dr. Linda Elder, Dr. Gerald Nosich and Dr. Richard Paul, all of the Foundation for Critical Thinking. They have created a practical model for critical thinking that is both effective and easy to teach.

That the Paul and Elder model is known within the Intelligence Community is due in no small part to Professor Francis J. Hughes of the National Defense Intelligence College (NDIC). It was he who introduced the author to the model and encouraged attendance at Paul and Elder's annual conference on critical thinking. He kindly also provided a commentary on the paper. Dax Norman, of the NSA Associate Directorate for Education and Training, a number of NSA colleagues, and approximately 250 participants in the NSA critical thinking and structured analysis course helped make that course a reality and additionally provided valuable insights into the nuances of critical thinking. Comments from LT Robert D. Folker, USAF, also provided insight into the teaching of critical thinking. LT Folker developed a similar course while a student at the NDIC that unfortunately did not remain in the curriculum.

As the paper progressed, a number of colleagues and peers provided feedback, comments, and challenges to the arguments presented. They include, in alphabetical order, Solveig Brownfeld, NDIC; James Bruce, SAIC; Jan Goldman, NDIC; Mary Rose Grossman, the John F. Kennedy Presidential Library and Museum; Alexandra Hamlet; Noel Hendrickson, James Madison University;

Robert Heibel, Mercyhurst College; Richards J. Heuer, Jr., Central Intelligence Agency (retired); Norval J. Hilmer, Defense Intelligence Agency; LTCOL James Holden-Rhodes, USMC (retired); Morgan D. Jones, Central Intelligence Agency (retired); Hugo Keesing, Defense Intelligence Agency (retired); Mark Marshall, NDIC; Stephen Marrin, University of Virginia; Montgomery McFate, Institute for Defense Analysis; William Reynolds, Least Squares Software; the staff of the Central Intelligence Agency's Sherman Kent Center; and the staff of the John F. Kennedy Presidential Library and Museum. Several other colleagues at the National Security Agency – who wish to remain anonymous – also offered valuable insight and suggestions.

Three colleagues, Mark Lowenthal, president of the Intelligence & Security Academy, LLC; Jeffrey Cooper, Science Applications International Corporation; and Gregory Treverton, Rand Corporation, also deserve mention. Mark kindly agreed to write the foreword and offered valuable suggestions. His quip about really good analysts set up much of the arguments presented herein. Both Jeff and Greg provided critical comments and suggestions late in the game. They also kindly agreed to write commentaries on the paper.

Russell Swenson, Director of NDIC's Center for Strategic Intelligence Research and NDIC Press editor, did what a really good editor is supposed to do: His input and recommendations ensured that the arguments that follow were focused and strong. The Center's William Spracher also provided valuable technical editing services. Colleague Lisa Krizan provided a final review of the text that proved extremely valuable. This paper would not have been published if not for their dedicated assistance to the author.

Acknowledgment is due to four other people. Peter and Mary Moore encouraged their son to be inquisitive and to always look beyond the obvious for answers. Anthropologist John McDaniel first introduced the author – then a student at Washington and Lee University – to an analogy for intelligence sensemaking: science-based field archaeology. Finally, Elizabeth Moore provided tremendous encouragement. She also graciously tolerated the many nights and weekends spent writing, listening to, and commenting on, ideas as

they occurred, sharpening the resulting arguments. It is to these people that this work is dedicated.

While the author was privileged to receive assistance of others, this remains his work and any errors are his. The author may be reached via electronic mail at dtmoore@nsa.gov.

CRITICAL THINKING AND INTELLIGENCE ANALYSIS

David T. Moore

Examples included in this paper were selected to illustrate points raised by the author. No interest by the National Security Agency, the Department of Defense, or any other agency of the U.S. Government should be inferred from their inclusion.

Abstract

Analysts and analysts alone create intelligence. Although technological marvels assist analysts by cataloguing and presenting data, information and evidence in new ways, they do not do analysis. To be most effective, analysts need an overarching, reflective framework to add structured reasoning to sound, intuitive thinking. "Critical thinking" provides such a framework and goes further, positively influencing the entire intelligence analysis process. Analysts who adopt critical thinking stand to improve their analyses. This paper defines critical thinking in the context of intelligence analysis, explains how it influences the entire intelligence process, explores how it toughens the art of intelligence analysis, suggests how it may be taught, and deduces how analysts can be persuaded to adopt this habit.

Definitions

Thinking – or reasoning – involves objectively connecting present beliefs with evidence in order to believe something else.

Critical Thinking is a deliberate meta-cognitive *(thinking about thinking)* and cognitive *(thinking)* act whereby a person reflects on the quality of the reasoning process simultaneously while reasoning to a conclusion. The thinker has two equally important goals: coming to a solution and improving the way she or he reasons.

Intelligence is a specialized form of knowledge, an activity, and an organization. As knowledge, intelligence informs leaders, uniquely aiding their judgment and decision-making. As an activity, it is the means by which data and information are collected, their relevance to an issue established, interpreted to determine likely outcomes, and disseminated to individuals and organizations who can make use of it, otherwise known as "consumers of intelligence." An intelligence organization directs and manages these activities to create such knowledge as effectively as possible.

CRITICAL THINKING AND INTELLIGENCE ANALYSIS

Introduction: How Do People Reason?

The best analytical tool remains a really good analyst.

—Mark Lowenthal, Former Assistant Director of Central Intelligence for Analysis and Production

To create intelligence requires transformations resulting from an intellectual endeavor that sorts the "significant from [the] insignificant, assessing them severally and jointly, and arriving at a conclusion by the exercise of judgment: part induction, part deduction," and part abduction.[4] That endeavor is known as *thinking*, or "that operation in which present facts suggest other facts (or truths)."[5] Thinking – or as it is sometimes known, reasoning – creates an "objective connection" between our present beliefs and "the ground, warrant, [or] evidence, for believing something else."[6]

These three reasoning processes trace the development of analytic beliefs along different paths. Whereas inductive reasoning reveals "that something is probably true," deductive reasoning demonstrates "that something is necessarily true."[7] However, both are limited:

4 William Millward, "Life in and out of Hut 3," in F. H. Hinsley and Alan Stripp, *Codebreakers: The Inside Story of Bletchley Park* (Oxford, UK: Oxford University Press, 1993), 17. The author adds "abduction" for reasons that will shortly become evident.

5 John Dewey, *How We Think: A Restatement of the Relation of Reflective Thinking to the Educative Process* (New York, NY: D.C. Heath and Company, 1910), 12. Cited hereafter as Dewey, *How We Think*.

6 Dewey, *How We Think*, 12.

7 David A. Schum, "Species of Abductive Reasoning in Fact Investigation in Law," *Cardozo Law Review* 22, nos. 5–6, July 2001, 1645, emphasis added. Cited

inductive reasoning leads to multiple, equally likely solutions and deductive reasoning is subject to deception. Therefore, a third aid to judgment, abductive reasoning, showing "that something is plausibly true," can offset the limitations of the others.[8] While analysts who employ all three guides to sound judgment stand to be the most persuasive, fallacious reasoning or mischaracterization of rules, cases, or results in any of the three can affect reasoning using the others.

Inductive reasoning, moving from the specific to the general, suggests many possible outcomes, or the range of what adversaries may do in the future. However, inductive reasoning lacks a means to distinguish among each outcome – all are possible. An analyst has no way of knowing whether a solution is correct.

Deductive reasoning on the other hand, moving from the general to the specific, addresses questions about adversarial behavior and intentions. Deductive reasoning becomes essential for warning. Based on past perceptions, certain facts indicate specific outcomes. If, for example, troops are deployed to the border, communications are increased, and leadership is in defensive bunkers, then war is imminent. However, if leadership remains in the public eye then these preparations indicate that an exercise is imminent.

Abductive reasoning reveals plausible outcomes to the intelligence analyst. When an adversary's actions defy accurate interpretation through existing paradigms, abductive reasoning generates novel means of explanation. In the case of intelligence warning, an abductive process presents policy–making intelligence consumers with an "assessment of probabilities." Although abduction provides no guarantee that the analyst has chosen the correct hypothesis, the probative force of the accompanying argument indicates that the most likely hypothesis is known and that elusive, actionable intelligence is on tap.

---

hereafter as Schum, "Species." American mathematician, logician, semiotician, and philosopher Charles Sanders Peirce (1839–1914) developed the concept of abductive reasoning. See Joseph Brent, *Charles Sanders Peirce: A Life* (Bloomington, IN: Indiana University Press, 1998).

8 Schum, "Species," 1645.

Figure 1 models analysts' thinking about HUMINT received during the summer of 1962 regarding reports of foreigners in Cuba. An initial (fallacious) conclusion derived from inductive reasoning apparently was reapplied through deductive reasoning as explained in the case study incorporated in this paper.[9] Something else was needed – but not considered – to challenge the initial conclusion that "All HUMINT from Cuba was false."

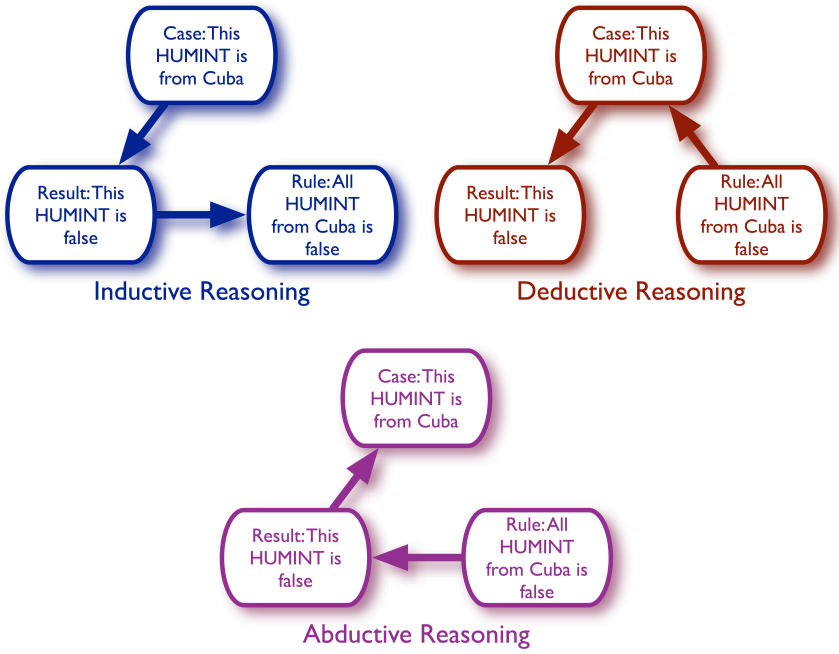


Figure 1: A Comparison of Inductive, Deductive, and Abductive Reasoning

Sources: Adapted from Thomas A. Sebeok, "One, Two, Three Spells UBERTY," in Umberto Eco and Thomas A. Sebeok, *The Sign of Three: Dupin, Holmes, Pierce* (Bloomington, IN: Indiana University Press, 1988), 8; and James H. Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence*, 46, no. 1 (2002), 56.

If analysts can model an adversary's intentions based on observable actions, adversaries also can deduce how those analysts will have

9 While there is no evidence it was applied in the Cuban case, abductive reasoning is included in the figure for purposes of illustration.

moved toward these conclusions. Under these circumstances, the adversary then can engage in deceptive practices that can lead an intelligence service to misinterpret that adversary's intentions.[10] For example, the Indian government deceived the U.S. Intelligence Community before the former's 1998 nuclear test. Through a 1995 demarche from the U.S. government, the Indian government knew what indicators the U.S. sought and was able to obscure them until after the test. Then, the Indian government boasted of its success.[11]

Abduction forces a close consideration of the evidence at hand. Given competing estimates – such as "war is imminent" or "an exercise will occur" – the body of facts and inferences must be examined to determine "whether there are facts which falsify one of the estimates."[12] Only then can an assessment of accuracy be determined. Even then, the selected estimate remains only the "most likely."[13]

Despite their individual limitations, induction, deduction, and abduction taken together offer a means of thoroughly examining evidence in order to arrive at accurate intelligence conclusions. However, as becomes obvious from studying figure 1, in order to be successful, intelligence analysis requires something more: an overarching framework is needed to ensure reasoning relies on valid assertions, is not fallacious, and is self–consciously objective. Critical thinking provides that framework by ensuring that each form of reasoning is appropriately used. Critical thinking extends to the entire intelligence analysis process. The claim here is that analysts who

---

10 Isaac Ben-Israel explores the duality of estimation in considerable detail. See "Philosophy and Methodology of Intelligence: The Logic of the Estimate Process, *Intelligence and National Security* 4, no. 4 (October 1989), 660–718. Cited hereafter as Ben-Israel, "Logic of the Estimate Process."

11 Paul J. Raasa, "The Denial and Deception Challenge to Intelligence," in Roy Godson and James J. Wirtz, *Strategic Denial and Deception* (New Brunswick, NJ: Transaction Publishers, 2002), 178, 223–224.

12 Ben-Israel, "Logic of the Estimate Process," 668.

13 Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: National Defense Intelligence College, 2002), 13.

become better critical thinkers will improve their analyses, helping to lessen the likelihood of intelligence failures. In the example above, critically thinking analysts would have questioned the generalizing of their initial conclusion by asking, "Was all the HUMINT from Cuba *really* false?" To avoid the tautological problem of equating quality analysis with the concept of "critical thinking" requires a careful assessment of cognition in the intelligence environment. The underlying question is "How can the intelligence analysts to whom Lowenthal's epigraph refers be 'really good'?"

Defining Critical Thinking

Defining critical thinking is a first step to understanding how it contributes to intelligence analysis. Richard Paul and Linda Elder, of the Foundation for Critical Thinking, consider it to be

> that mode of thinking – about any subject, content, or problem – in which the [solitary] thinker improves the quality of his or her thinking by skillfully taking charge of the structures inherent in thinking and imposing intellectual standards upon them.[14]

In other words, critical thinking is both a deliberate meta-cognitive *(thinking about thinking)* and cognitive *(thinking)* act whereby a person reflects on the *quality* of the reasoning process simultaneously while reasoning to a conclusion. The thinker has two equally important goals: improving the way she or he reasons and coming to a correct solution.[15]

To accomplish these goals, the reasoner requires assisting structures. Paul and Elder define eight elements of reasoning, shown in figure 2. These elements lead thinkers to ask focused questions about the topic being considered and the thinking process itself. Paul and Elder assert that whenever people reason, they do so for a purpose. This reasoning exists within a point of view and is shaped by both conscious and unconscious assumptions. Reasoning involves the creation of inferences based on conceptual frameworks about reality. These inferences are generated as people consider evidence necessary to answer questions or solve problems. Further, reasoning leads to decision points with implications – things that might happen

14 Richard Paul and Linda Elder, *The Miniature Guide to Critical Thinking Concepts and Tools*, 4th Edition (Dillon Beach, CA: The Foundation for Critical Thinking, 2004), 1. Cited hereafter as Paul and Elder, *Concepts and Tools*.

15 Exactly what is the "correct solution" is issue and context dependent. What is important here is that the process of reasoning is enhanced.

– *and* consequences – things that do happen once the decision has been made. Finally, Paul and Elder insist that "learning to analyze thinking requires practice in identifying the structures in use."[16]

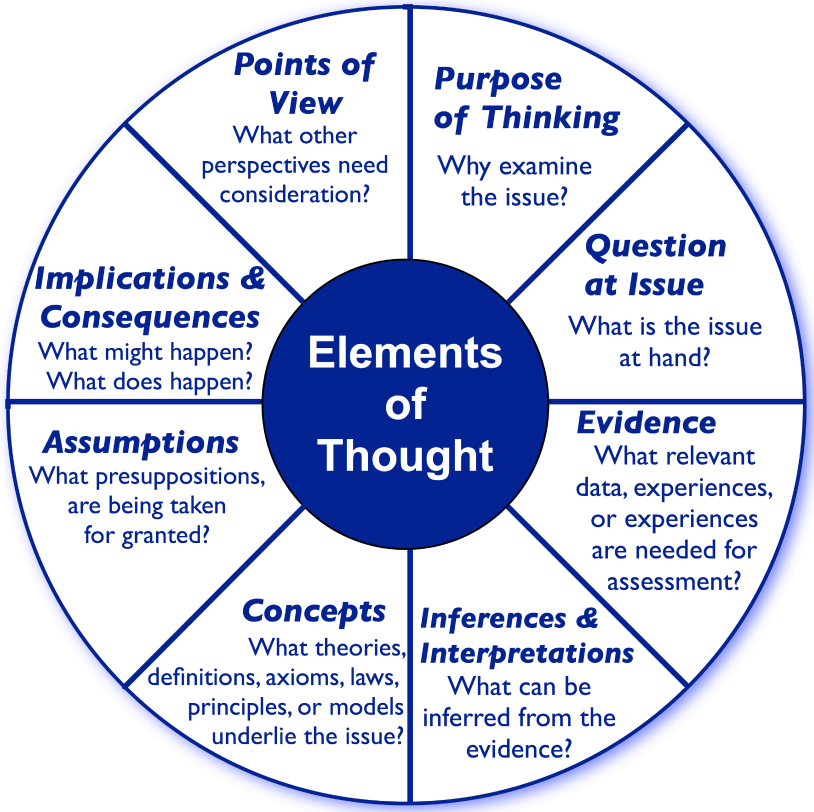


Figure 2: Elements of Thought

Source: Derived from Richard Paul and Linda Elder, *The Miniature Guide to Critical Thinking Concepts and Tools*, 4th Edition (Dillon Beach, CA: The Foundation for Critical Thinking, 2004), 2.

16 Linda Elder and Richard Paul, *The Foundations of Analytic Thinking: How to Take Thinking Apart and What to Look for When You Do* (Dillon Beach, CA: The Foundation for Critical Thinking, 2003), 5. Cited hereafter as Elder and Paul, *Analytic Thinking*. Paul and Elder, *Concepts and Tools*, 2.

Standards for Critical Thinking

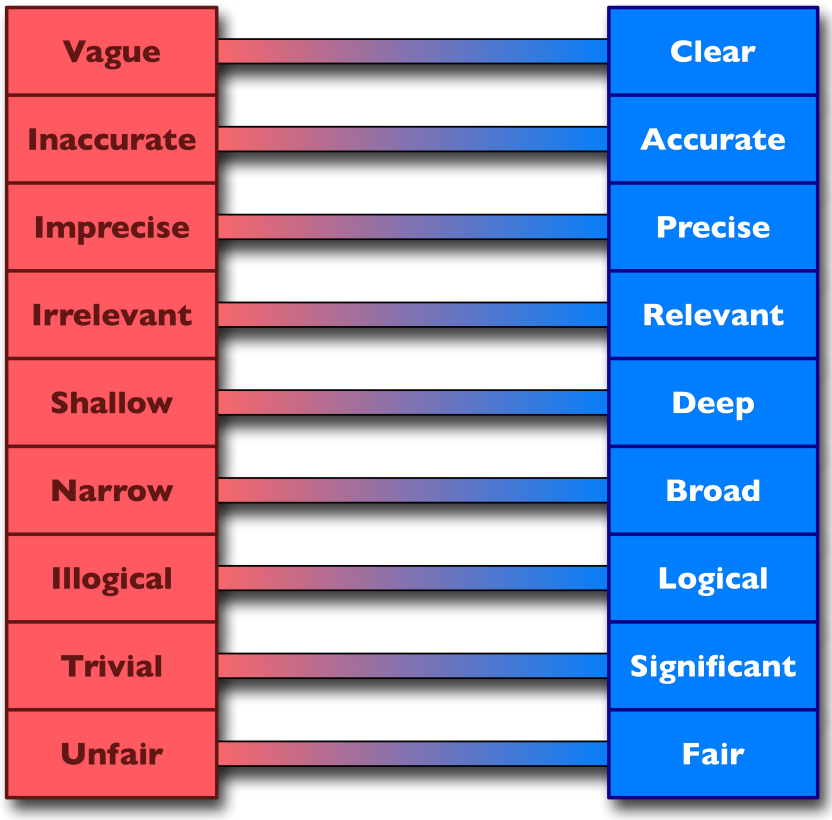


Figure 3: A Continuum of Intellectual Standards

Source: Derived from Paul and Elder, *Concepts and Tools*, 9.

Paul and Elder also establish a set of intellectual standards that offer criteria for assessing the level and quality of thinking. These form a continuum as shown in figure 3.[17] Active – or Socratic – questioning in a social setting becomes the means of critically exploring a topic or discipline as well as assessing the thinking on that topic. Questions assessing the issue delve into purpose, assumptions, inferences, as well as points of view on a topic.[18] Paul and Elder's

17 Elder and Paul, *Analytic Thinking*, 1–17.

18 Paul and Elder, *Concepts and Tools*, 2–9.

approach ensures that a topic or issue is thoroughly, logically, and objectively developed. Their continuum provides qualitative metrics to inform the thinker and others who may evaluate the object of the thinking along with the process employed. Each standard is related to but independent of the others. The object of consideration might be vaguely or clearly presented. But it also might be inaccurate. An example of this would be "the world is flat." This clear statement of reality is false.

The reasoning or its object might be clearly and accurately presented but remain imprecise, the level of detail required depending on the issue itself. Precision becomes important in assessing the location of an adversary or a threat as in "terrorists placed the improvised explosive device (IED) near the highway."

It is possible to create clear, accurate, and precise answers that are irrelevant. If one is considering the IED along the highway but the issue is how best to fly the troops in question from one location to another then the answer is irrelevant. Similarly, topics and their accompanying reasoning need to consider both the complexities involved (depth) and other points of view (breadth).[19] Such reasoning becomes essential when systems must be assessed because in systems "chains of consequences extend over time and many areas: The effects of action are always multiple."[20] Intelligence often must assess such systems – terrorist networks are but one example. Additionally, as sociologist Emile Durkheim observes, the combinations of elements related to an issue "combine and thereby produce, by the fact of their combination, new phenomena."[21]

When the correct phenomena or questions – and related alternative explanations – are not fully considered, intelligence failures occur. For instance, the Senate Select Committee on Intelligence

19 Elder and Paul, *Analytic Thinking,* 7.

20 Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997), 10. Cited hereafter as Jervis, System Effects.

21 Emile Durkheim, *The Rules of Sociological Method* (Glencoe, IL: Free Press, 1938), xlvii.

found such reasoning to be among the causes of the Intelligence Community's failure to assess accurately Iraq's alleged programs to develop weapons of mass destruction (WMD). The senators noted that "Intelligence Community managers…did not encourage analysts to challenge their assumptions, fully consider alternative arguments, accurately characterize the intelligence reporting, or counsel analysts who lost their objectivity."[22]

Logic and significance also come into play. If the evidence presented does not imply the conclusions then the results are illogical. Focusing on appropriate evidence maintains significance. For example, evidence that terrorists who place an IED also have Stinger surface–to–air missiles bears on how troops can move across hostile territory.

Fairness deals with the agendas – hidden and expressed – of the thinker, her collaborative peers, and her customers. Knowing who has a stake in an issue as well as the stakes themselves helps ensure that issues are fairly reasoned and presented. Such considerations also reflect the analyst's own biases or opinions. In considering this point, Paul and Elder offer the evaluative question, "Am I misrepresenting a view with which I disagree?"[23]

Finally, while getting to the right-hand side of the spectrum on each of these standards in figure 3 is highly desirable, the standard of thinking on an issue will vary based on the skills of the thinkers and the issues under scrutiny. Assessing the resulting shortfalls in thinking reveals gaps that can be corrected. The continuum therefore provides a detailed assessment by which thinking on issues can be improved.

---

22 Senate Select Committee On Intelligence, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq,* United States Senate, 108th Congress, 7 July 2004, 23. Cited hereafter as SSCI, *Iraq.*

23 Elder and Paul, *Analytic Thinking,*, 7.

Skill-Based Definitions

Other approaches to defining critical thinking focus on the specific skills. For example, Diane Halpern considers that

> [critical] thinking is the use of those cognitive skills or strategies that increase the probability of a desirable outcome. It is… thinking that is purposeful, reasoned, and goal directed – the kind of thinking involved in solving problems, formulating inferences, calculating likelihoods, and making decisions, when the thinker is using skills that are thoughtful and effective to the particular context and type of thinking task.[24]

Additional advocates of skills-based critical thinking include Edward Glaser and Alec Fisher, and their sets of critical thinking skills include a number of elements common to those identified by Halpern. The overlapping competencies of critical thinkers as advanced by Paul and Elder and these three other proponents are summarized in table 1. The comparison reveals the completeness of the Paul and Elder model.

These competencies assist intelligence analysts who contribute to the solution of threats to national security by ensuring the formulation of sound inferences about adversarial capabilities and intentions. Resulting findings are disseminated in reports that are often referred to as "assessments." At their best, they offer choices to decision-making consumers, as well as a clear outline of the implications of those choices.[25]

---

24 Diane Halpern, *Thought and Knowledge: An Introduction to Critical Thinking*, 4th Edition (Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 2002), 37. Cited hereafter as Halpern, *Thought and Knowledge.*

25 The term "assessment" describes the result of an intelligence production process but is not universally used within the Intelligence Community. Assessments are created at the Central Intelligence Agency and at the Defense Intelligence Agency. Other names for the reports that analysts produce include "products" at the National Security Agency (NSA) and "estimates" at the National Intelligence Council (NIC). Regardless of how they are named, they record and disseminate the results of analysts' work.

Competencies of Critical Thinkers	Paul and Elder	Fisher	Glaser	Halpern
Recognize problems or questions and find effective means of solution	✓		✓	✓
Engage in meta-cognitive activities that identify assumptions, biases, and performance as solutions are developed	✓	✓	✓	✓
Interpret data, appraise evidence, and evaluate statements in order to recognize logical relationships between propositions	✓		✓	✓
Infer warranted conclusions and generalizations from evidence	✓	✓	✓	✓
Test generalizations and conclusions by seeking out contradictory evidence that enables them to judge the credibility of claims	✓	✓	✓	✓
Convey sound, well-reasoned arguments	✓	✓	✓	✓
Focus on the process of reasoning with the intention of improving the process	✓			

Table 1: A Comparison of Different Sets of Critical Thinker's Competencies

Sources: Compiled by author from Linda Elder and Richard Paul, *The Foundations of Analytic Thinking: How to Take Thinking Apart and What to Look for When You Do* (Dillon Beach, CA: The Foundation for Critical Thinking, 2003); Diane Halpern, *Thought and Knowledge: An Introduction to Critical Thinking,* 4th Edition (Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 2002), 37; Edward M. Glaser, *An Experiment in the Development of Critical Thinking* (New York, NY: AMS Press, 1941), 6; and Alec Fisher, *Critical Thinking: An Introduction* (Cambridge, UK: Cambridge University Press, 2001), 8.

A Disposition to Think Critically

It is not enough merely to know the skills needed for critical thinking. To be successful, analysts as critical thinkers also need "certain attitudes, dispositions, passions, [and] traits of mind."[26] Actively thinking critically hones the skills; practice yields proficiency. But in order to gain mastery, willingness to reason in this manner becomes essential. The importance of this disposition to critically think cannot be over-emphasized. According to Peter A. Facione, Noreen C. Facione, and Carol A. Giancarlo, "Empirical studies…at multiple sites indicate that for all practical purposes" both critical thinking skills and the disposition to critically think are essential.[27]

There are a number of characteristics associated with the disposition to think critically. The Faciones and Giancarlo identify "seven characterological attributes or habits of mind… truth-seeking, open-mindedness, analyticity, systematicity, critical thinking, self confidence, inquisitiveness, and maturity of judgment."[28] According to Richard Paul and Gerald Nosich, the characteristics of critical thinkers include

> thinking independently, exercising fair-mindedness, developing insight into egocentricity and sociocentricity, developing intellectual humility and suspending judgment, developing intellectual courage, developing intellectual good faith and integrity, developing intellectual perseverance,

---

26 Richard W. Paul and Gerald Nosich, *A Model for the National Assessment of Higher Order Thinking*, (Dillon Beach, CA: Foundation for Critical Thinking, n.d.), 20. Cited hereafter as Paul and Nosich, National Assessment.

27 Peter A. Facione, Noreen C. Facione, and Carol A. Giancarlo, "The Disposition Toward Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill," *Informal Logic* 20, no. 1 (2000): 61–84. Reprinted by Insight Assessment, URL: <http://www.insightassessment.com/pdf_files/J_Infrml_Ppr%20_2000%20–%20Disp%20&%20Skls.PDF>, last accessed 31 March 2006. Cited hereafter as Facione, "Disposition."

28 Peter A. Facione, Noreen C. Facione, Carol A. F. Giancarlo, *Professional Judgment and the Disposition Toward Critical Thinking* (Milbrae, CA: California Academic Press, 2002), URL: < http://www.calpress.com/pdf_files/Prof_jmn.pdf>, last accessed 31 March 2006.

developing confidence in reason, exploring thoughts underlying feelings and feelings underlying thoughts, developing intellectual curiosity.[29]

Both sets closely match the characteristics of successful intelligence analysts identified by Lisa Krizan and the author in their work on intelligence analysts' core competencies. Krizan and the author observe that successful intelligence analysts are insatiably curious. Fascinated by puzzles, their high levels of self-motivation lead them to observe and read voraciously, and to take fair-minded and varied perspectives. This helps them to make the creative connections necessary for solving the hardest intelligence problems. Finally, the emotional tensions created by problems, and the cathartic release at their solution, powerfully motivate analysts.[30]

In addition, emotions play a significant part in the process of critical thinking. As adult learning expert Stephen Brookfield observes, "[emotive] aspects – feelings, emotional responses, intuitions, sensing – are central to critical thinking."[31] He argues that the consideration of alternatives "to one's current ways of thinking" characterizes the approach.[32] Indeed, the consideration of these alternatives requires creativity, which he considers a non–rational form of thought.[33] Creative reasoning generates hypotheses; it has contributed significantly to the development of intellectual, scientific, and technological knowledge.

---

29 Paul and Nosich, *National Assessment*.

30 David Moore and Lisa Krizan, "Intelligence Analysis: Does NSA Have What it Takes," reprint NSA Center for Cryptologic History, *Cryptologic Quarterly* 20, nos. 1/2 (Summer/Fall 2001), 8–11. Cited hereafter as Moore and Krizan, "NSA,"

31 Stephen D. Brookfield, *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting* (San Francisco, CA: Jossey–Bass Publishers, 1987), 12. Cited hereafter as Brookfield, Developing Critical Thinkers.

32 Brookfield, *Developing Critical Thinkers,* 12.

33 Brookfield, *Developing Critical Thinkers,* 12.

The Role of Questions

Greg Treverton observes that in intelligence the right questions rarely get asked.[34] Yet, critical thinking offers a means by which at least *appropriate* questions may be raised. The combination of critical thinking skills and the disposition to think critically focuses and directs inductive, deductive, and abductive reasoning to solve problems. This is an interrogative paradigm. Critical thinking involves questioning that forces broader consideration of issues and problems as well as the various means of resolving or answering them. Such questioning happens at both the individual and collective levels as shown in figure 4.

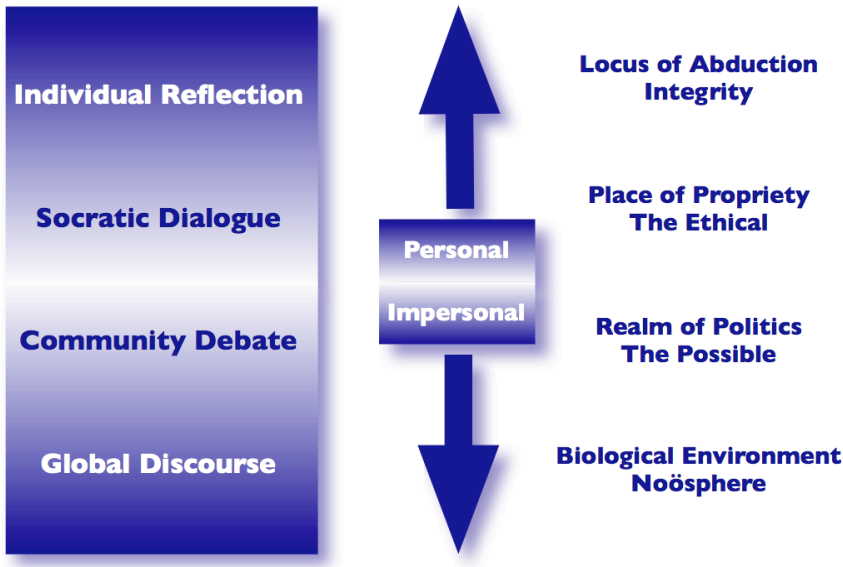


Figure 4: Levels of Questioning: Critical Thinking in a Social Setting

Source: Created by the author with contributions by Russell G. Swenson.

Questioning is either personal or impersonal and ranges from the musings of the individual critical thinker to that of a global discourse. As an individual ponders problems and issues, she abduces the most likely explanations. Moving up a level, questioning becomes a

34 Greg Treverton, conversation with the author, 18 April 2006.

hierarchical dialogue within dyads or larger assemblies. A critically thinking questioner ferrets out answers from others within the group. The process generates new questions that are answered in turn – and in turn, raise further questions. At the level of a community debate, critical thinkers explore what is possible politically and within the community's purview. Ideally, the relationship between thinkers is peer-to-peer. Finally, questions addressed within the context of a global discourse take into account the entire biological landscape (noösphere).[35]

Such questioning produces new and creative thinking, analogous to switching from Newtonian to quantum physics. In this analogy, an atomistic approach to analysis gives way to the associative impulse of synthesis as structured thoughts facilitate a leap to new questions, ideas, and possibilities. This overarching framework of structured reasoning frames questions to help analysts decide the best means or best combination of means that are suited to solving specific intelligence problems. The questions serve to alert an analyst to the notion that she might be deceived, or that she needs to employ some other means of reasoning to determine which of several alternative outcomes is most likely. These questions provide a formal means by which an analyst confronts her biases about likely outcomes. Therefore, in the context of intelligence analysis, critical thinking becomes one of the most – if not *the* most – important skills of the analyst. Facing symmetric and asymmetric threats, analysts have a potent and powerful tool to facilitate their asking the right questions in the process of improving their understanding of the problem at hand as well as their own reasoning about that problem.

Pseudo-Critical Thinking

It is important to understand what critical thinking is *not*. Critical thinking, as has been noted, focuses on both the process and the results of reasoning. However, the term is also used in reference to reasoning that is not reflective. The application of formal logic is sometimes (incorrectly) equated to critical thinking. So too are

35 Wikipedia defines the noösphere as the domain of human thought. Wikipedia, entry under "noösphere," accessed 27 February 2006.

problem solving and structured methods of analysis. Developers of school curricula and other exponents of "sound thinking" often lay claim to the mantel of critical thinking but are really leveraging their coverage of logic or problem solving to capitalize on an uncritical understanding of what critical thinking is. Problem solving, for example, focuses on answers and not on the process by which an answer is obtained. Additionally, logic or problem solving, being goal oriented, offer little means by which a person can improve the process of her thinking. The following problem is a typical example of pseudo–critical thinking:

> Two cyclists race along a straight course. The faster of the pair maintains an average speed of 30 mph. The slower cyclist averages 25 miles per hour. When the race ends, the judges announce that the faster cyclist crossed the finish line one hour before the slower racer. How many miles long was the racing course?[36]

This example (and others like it) focuses on the answer, provides no guidance on the process, and ignores any improvement in reasoning skills. Solvers either figure it out through trial and error or by following a rule-based strategy learned by rote. Therefore it fails to be critical thinking.

Unless the process, and the means, to improve a person's reasoning are emphasized, then at best such examples teach structured problem solving. At worst, they deal merely in criticism; they fail to assist people to learn to reason better. Central to critical thinking are the twin foci on the way in which a person is reasoning and the goal of improving that process. One could easily infer that misconceptions about critical thinking could be associated with what is taught as critical thinking in American educational institutions.[37]

---

36 Michael A. DiSpezio, *Classic Critical Thinking Puzzles* (New York, NY: Main Street, 2005), 85. The answer, by the way, is 150 miles (page 227).

37 Michael R. LeGault reaches this same conclusion in *Think: Why Crucial Decisions Can't Be Made in the Blink of an Eye* (New York, NY: Threshold Editions, 2006), 17. Cited hereafter as LeGault, *Think*.

What Can Be Learned from the Past? Thinking Critically about Cuba

Examining past intelligence successes and failures in light of new developments provides a means to reassess what happened and how outcomes could have been different. The case of the Soviet missiles in Cuba in the summer and fall of 1962 provides a means of examining how critical thinking and structured methodologies could have made a difference.

Deploying the Missiles

During the summer of 1962, CIA analysts received a spate of potentially alarming reports about Russians being seen in Cuba. The reports, however, were only part of a stream of similar, "farfetched tales of African troops with rings in their noses, lurking Mongolians, and even Chinese troops" on the island.[38] Most or all of these reports were discounted by analysts who were inured to spurious reports of Soviet equipment secreted away in caves.[39]

James Hansen – who worked in both the Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA) – posits that the U.S. Intelligence and Policy Communities were the victims of a concerted Soviet campaign of denial and deception that masked the deployment of Soviet forces and missiles into Cuba.[40] The deception campaign even included "accurate information about the deployment [leaked] so as to mask it."[41] As Raymond Garthoff relates, "there were literally thousands of reports of missiles in Cuba in the period *before* any missiles were actually brought there."[42]

---

38 James H. Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence* 46, no. 1 (2002), 56. Cited hereafter as Hansen, "Soviet Deception."

39 Hansen, "Soviet Deception," 56.

40 Hansen, "Soviet Deception," 49–58.

41 Domingo Amuchastegui, "Cuban Intelligence and the October Crisis," in James G. Blight and David A. Welch, Eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 101.

42 Raymond L. Garthoff, "US Intelligence in the Cuban Missile Crisis," in

In fact, the Soviets were able to deploy more than the offensive nuclear missiles that became the centerpiece of the subsequent crisis with the United States. While U.S. analysts and policymakers knew of the conventional weapons, they were blind to the presence of SS-4 Medium Range Ballistic Missiles (MRBM) and SS-5 Intermediate Range Ballistic Missiles prior to the U-2 overflights of 14 October. Additionally, it seems they never discovered the presence of approximately 100 tactical nuclear weapons deployed on the island.[43] There is debate whether U.S. Intelligence also *underestimated* the number of Soviet troops deployed to Cuba. Garthoff reports that one CIA unit concluded there were between 45,000 and 50,000 Soviet troops in Cuba (the actual number was about 42,000) but the official estimate was between 4,500 and 5,000 prior to the crisis.[44]

The Soviets employed an elaborate campaign of denial and deception that took advantage of American points of view about the likelihood of Soviet weapons being located in Cuba. As Robert Jervis makes clear,

> the U.S. did not expect the Russians to put missiles into Cuba or Japan to attack Pearl Harbor because American officials knew that the U.S. would thwart these measures if they were taken. These judgments were correct, but because other countries saw the world and the U.S. less accurately, the American predictions were inaccurate.[45]

It could have been worse. As Gil Merom writes, the Soviets might

---

James G. Blight and David A. Welch, Eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 22. Emphasis in original. Cited hereafter as Garthoff, "US Intelligence."

43 Garthoff, "US Intelligence," 29.

44 Garthoff, "US Intelligence," 28, 58. U.S. Intelligence never did reach a correct conclusion. The closest they got was an estimate of 22,000 troops in early 1963 (Garthoff, "U.S. Intelligence," 28).

45 Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997), 45. Jervis draws on the work of Klaus Knorr. See Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," *World Politics* 16 (April 1964): 455–67.

have *completed* the bases and "threatened major U.S. cities with extinction."[46] The threat is brought home by figure 5.

What caused U.S. analysts to get it wrong? Apparently the U.S. analysts concluded that because some of the HUMINT evidence was ludicrous, all of it was. This inductive conclusion then led them to discount further evidence. For example, having concluded that all the previously considered Cuban HUMINT was false, each new piece, *since it came from Cuba,* also had to be false. Thus, a false inductive conclusion led subsequently to false deductive conclusions.[47] It does not appear that abductive reasoning strategies were ever employed.

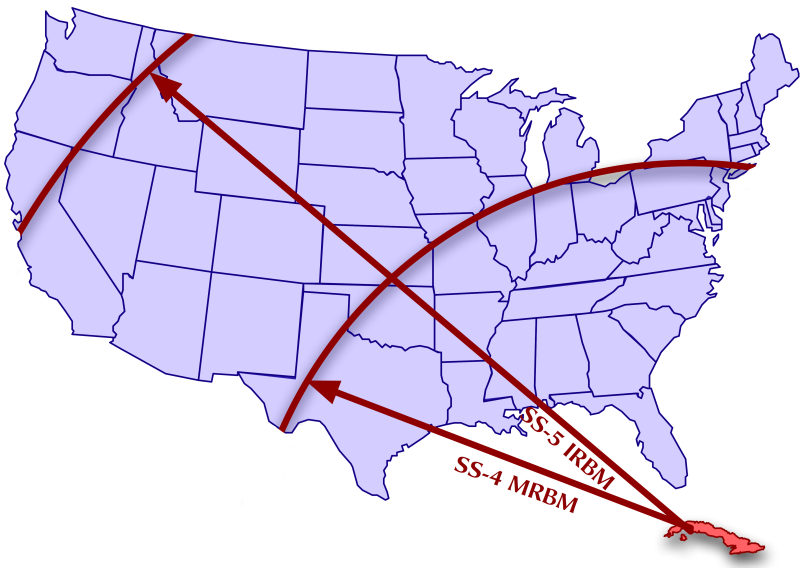


Figure 5: Respective Ranges of Soviet SS-4 MRBM and SS-5 IRBM Missiles

Source: Derived from Hansen, "Soviet Deception," 49.

46 Gil Merom, "The 1962 Cuban Intelligence Estimate: A Methodological Perspective," *Intelligence and National Security* 14, no. 3 (Autumn 1999), 49. Cited hereafter as Merom, "Estimate."

47 Inductive and deductive reasoning were illustrated in figure 1.

It should be noted that the U.S. Intelligence Community was not blind to the possibility that the Soviets might conduct a military buildup in Cuba. In fact, there were two theories being debated: One, that the Soviets would emplace *defensive* weapons, and the other that they would emplace *offensive* weapons. Senior analysts in the Intelligence Community held the former theory while John McCone, then Director of Central Intelligence, favored the latter.

Part of McCone's reasoning had to do with the cost and utility of the installation of SA-2 air defense missiles. McCone apparently reasoned that the purpose of installing such expensive missiles had to be greater than merely denying the United States overflight capabilities (the SA-2 could shoot down – as Francis Gary Powers discovered – a U-2).[48] This led McCone to come "up with an answer that no one wanted to hear: the SA-2s were on the island to deny the United States the capability to see the construction of offensive missile installations."[49]

Unfortunately, McCone was unable to dissuade the majority from their point of view. This may have stemmed, as James Blight and David Welch write, from the realization that while McCone's inference seemed reasonable when viewed in hindsight, in foresight it was faulty because it failed to sufficiently cover the alternatives.[50] Blight and Welch observe that

> the Soviets had also deployed SA-2 missiles to Egypt, Syria, and Indonesia, and in none of those cases had they also deployed strategic nuclear weapons. Indeed, the US intelligence community [sic] expected that the Soviet Union

48 Thomas R. Johnson and David A. Hatch, *NSA and the Cuban Missile Crisis* (Fort Meade, MD: National Security Agency Center for Cryptologic History, 1998), URL: <http://www.nsa.gov/publications/publi00033.cfm>, last accessed 18 April 2006. Cited hereafter as Johnson and Hatch, *NSA*.

49 Johnson and Hatch, *NSA*.

50 James G. Blight and David A. Welch, Eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 5. Cited hereafter as Blight and Welch, Intelligence and the Cuban Missile Crisis.

would deploy SA-2 missiles to Cuba, precisely because it had done so elsewhere.[51]

Even though history proved McCone to be correct (for the wrong reasons), the defensive weapons theory predominated.[52]

The Soviets took advantage of the American beliefs and faulty reasoning. Capitalizing on the idea that it is easier to lead a target astray than to try to change his mind, they successfully placed the nuclear missiles in Cuba.[53] Heuer observes that

> [deceptions] that follow this principle seldom fail, for the odds are then strongly in favor of the deceiver. The human capacity to rationalize contradictory evidence is easily sufficient to outweigh the pernicious effects of security leaks and uncontrolled channels of information that planners of deception…might compromise their efforts.[54]

Assessing the Implications

Exactly what happened in the Cuban case and does it apply to contemporary issues? Roberta Wohlstetter notes in retrospect, "We would like to know not only how we felt, but what we did and what we might have done, and in particular what we knew or what we could have known."[55] Wohlstetter's musings lead to two key questions for analysts: How could this successful deception campaign have been

51 Blight and Welch, *Intelligence and the Cuban Missile Crisis*, 5.

52 Merom, "Estimate," 58.

53 Richards J. Heuer, Jr., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981), 200. Cited hereafter as Heuer, "Strategic Deception." It is interesting to speculate whether the Soviets had a feedback channel that informed them of the predominant theory.

54 Heuer, "Strategic Deception," 200.

55 Roberta Wohlstetter, "Cuba and Pearl Harbor: Hindsight and Foresight," *Foreign Affairs* 46, no. 3 (July 1965), 691. Cited hereafter as Wohlstetter, "Cuba."

thwarted? What can be learned to advise analysts about current adversarial denial and deception?

Simply looking at additional evidence is sometimes promoted as a means of detecting denial and deception by adversaries. In the Cuban case, however, analysts had already processed a superabundance of evidence. Wohlstetter suggests that such riches can be "embarrassing."[56] This is because even as "signals" point

> to the action or to an adversary's intention to undertake it, "noise" or a background of irrelevant or inconsistent signals, [and] signs pointing in the wrong directions…tend always to obscure the signs pointing the right way.[57]

HUMINT assets overwhelmed analysts' abilities to distinguish signals from noise. Heuer and Hansen agree that once "locked in," analysts resist changing their minds. More evidence alone fails to change an analyst's mind because "[new] information is assimilated to existing images."[58] Yet, analysts stand to benefit from changing their opinion in the face of disconfirming evidence.

The limitations of hindsight analysis notwithstanding, if analysts had employed critical reasoning in 1962 they could have detected the Soviet *maskirovka* in Cuba. For example, by applying Paul and Elder's model of critical thinking, analysts would have had a means to question their assumptions and points of view, and subsequently might have questioned the purpose of the apparent "noise" they were discounting as well as their assumptions about the prevalent point of view that the Soviets would not place missiles on the island because we would react. Gil Merom suggests that some appropriate questions would have included: "How aware were the analysts of their own assumptions? Were these assumptions sensible and was it sensible to adhere to them?"[59] Other considerations that critical

56 Wohlstetter, "Cuba," 691.

57 Wohlstetter, "Cuba," 691.

58 Heuer, *Psychology,* 10–11.

59 Merom, "Estimate," 57.

thinking about the crisis might have raised are included in table 2. Applying Paul and Elder's model reveals other considerations that conceivably would have led to an earlier detection of the likelihood of the deployed weapons being *offensive.*

Would this approach have allowed detection of what the Soviets were doing in Cuba before mid-October 1962? One could argue counterfactually that it might have enhanced analysis of collection from other sources.[60] SIGINT assets capable of collecting Russian communications were in place near the island.[61] Imagery assets might have been tasked differently prior to 14 October. Sources less subject to generating noise would have introduced inconsistencies to an analysis of competing hypotheses that was solely HUMINT-based.

Between Dogmatism and Refutation

A systematic approach to directed collection also would have moved analysts toward a disconfirmatory analytic approach. By contrast, a confirmatory approach, often characterized as confirmation bias, leads analysts to accept what they set out to confirm.[62] A disconfirmatory approach aims to refute alternative

---

60 Counterfactual reasoning explores differing outcomes arising from alternative causes. Counterfactuals are commonly used in whenever alternate hypotheses are explored. They are essential for both post-mortem reviews and futures scenario exercises. See Philip E. Tetlock, and Aaron Belkin, *Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives* (Princeton, NJ: Princeton University Press, 1996), 1–38. In the same volume, Richard Ned Lebow and Janice Gross Stein conduct a counterfactual review of the Cuban missile crisis. See Richard Ned Lebow, and Janice Gross Stein, "Back to the Past: Counterfactuals and the Cuban Missile Crisis," in Philip E. Tetlock, and Aaron Belkin, *Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives* (Princeton, NJ: Princeton University Press, 1996), 119–148.

61 Johnson and Hatch, *NSA*. According to the authors, SIGINT played a key role in determining the operational status of the SA-2 air defense missiles. However, SIGINT failed to detect the delivery and installation of the nuclear missiles.

62 Wikipedia defines confirmation bias as "a type of cognitive bias toward confirmation of the hypothesis under study." (Wikipedia, entry under "confirmation bias").

Purpose	· Determine what is going on in Cuba as a part of the U.S. "war" against Castro and the Cuban communists.
Key Questions	· If this really is a Soviet military buildup, what kinds of weapons are being deployed: offensive weapons or defensive weapons? · Why is an expensive missile system like the SA–2 being installed in Cuba? · What is the SA–2 really protecting? · Does a crisis exist?
Evidentiary Considerations	· If defensive weapons are being deployed, what evidence should be observed? · If offensive weapons are being deployed, what evidence should be observed? · What is not being seen?
Inferences	· What is inferred from the observed and collected evidence?
Assumptions	· What is being assumed about the evidence? · What is being assumed about the sources of the evidence? · What is being assumed about why the Soviets would deploy weapons to Cuba?
Concepts	· How does human perception affect the analysis? · How reliable are the sources of evidence? (Could also be an assumption.)
Implications and Consequences	· If conclusions are incorrect about the Soviet build up, what might occur next? · If conclusions are correct about the Soviet build up, what can be expected? · If conclusions are incorrect about offensive weapons being deployed, what happens next? · If conclusions are incorrect about defensive weapons being deployed, what happens next?
Points of View	· What other points of view about what is going on in Cuba exist?

Table 2: Applying Paul and Elder's Critical Thinking Model to the Situation in Cuba, August–September 1962.

Source: Developed by author.

hypotheses. Whatever was left at the end of the process would be the most likely explanation. Would this guarantee a correct "answer"? Ben-Israel concludes that although the answer has to be "no," the approach does allow for narrowing "the margin of error."[63] It does so by moving the analyst away from a "pole of dogmatic tenacity" toward a "pole of refutation" (summarized in figure 6).[64]

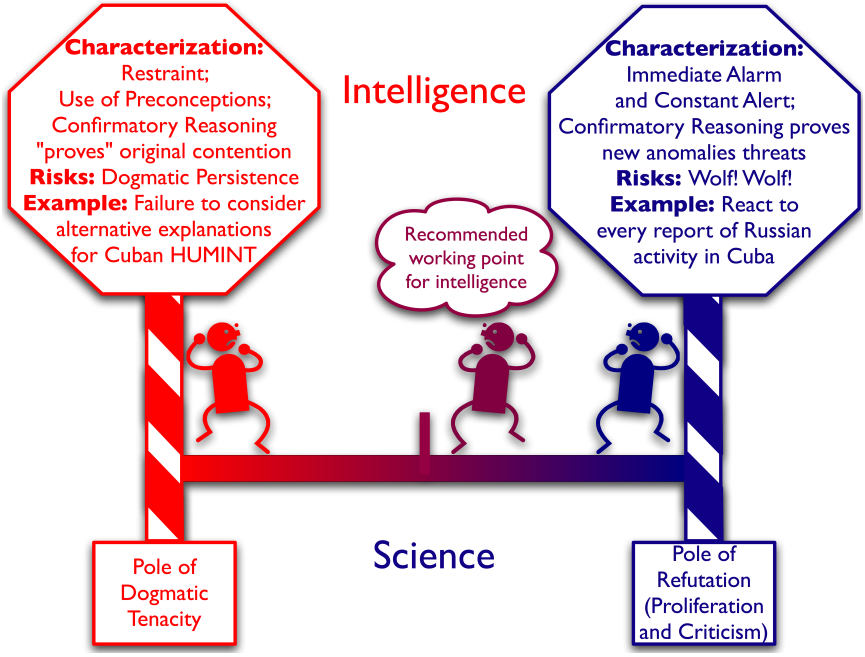


Figure 6: A Place for Analysis between Dogmatism and Criticism

Source: Derived from Ben-Israel, "Methodology of Intelligence," 679.

It should be noted that operating too closely to a pole of refutation can also create problems. For example, analysts might be unable to distinguish between real threats and false positives; they might react to each one regardless of its validity. In the Cuban case, this problem would have manifested itself in goading continual U.S. military reactions to every perceived Soviet and Cuban threat. Here again,

63 Ben-Israel, "Logic of the Estimate Process," 679

64 Ben-Israel, "Logic of the Estimate Process," 691.

critical thinking could moderate this Cassandrian approach.[65] The questioning of assumptions and points of view in critical thinking allows analysts to *discount* certain evidence. Based on his own Israeli intelligence analyst experiences, Ben-Israel asserts that anchoring oneself some distance from a pole of refutation, and not far from the center, is probably best.[66] In other words, enlightened skepticism probably works as a method for distinguishing between real and perceived threats. Critical thinking leads one to assess the processes one is using and the point on the continuum from which to work.

Lacking: Disconfirmation

Merom confirms that a disconfirmatory process did not occur on the Cuban missile problem: "Information that was inconsistent with the prevailing conservative theory was not considered as alarming and necessitating revision, but rather was 'rehabilitated' and rendered 'harmless' on the basis of *ad hoc* statements."[67] Instead, inductive reasoning generally led analysts to "prove" their theory and subsequently to adhere to it "*until it was proven wrong* by conclusive hard evidence" – the U–2 photos, to be exact (of which a detail is reproduced in figure 7).[68]

---

65 Cassandra was the daughter of Priam, King of Troy. She was blessed and cursed by the god Apollo to accurately predict the future yet never be believed. In intelligence, a Cassandrian approach is characterized as one that emphasizes dire outcomes and worst–case scenarios. Analysts who produce such assessments are often discounted and rarely thanked when they are correct. For a real account of how such warnings are perceived (at least at the time they are made), see Charles E. Allen, "Intelligence: Cult, Craft, or Business?" in *Seminar on Intelligence, Command, and Control, Guest Presentations,* Spring 2000 (Cambridge, MA: Harvard University Program on Information Resources Policy, I–01–1, April 2000), URL: <http://www.pirp.harvard.edu/pubs.html>, last accessed 11 January 2006.

66 Ben-Israel, "Logic of the Estimate Process," 679.

67 Merom, "Estimate," 69.

68 Merom, "Estimate," 69. Italics in original.

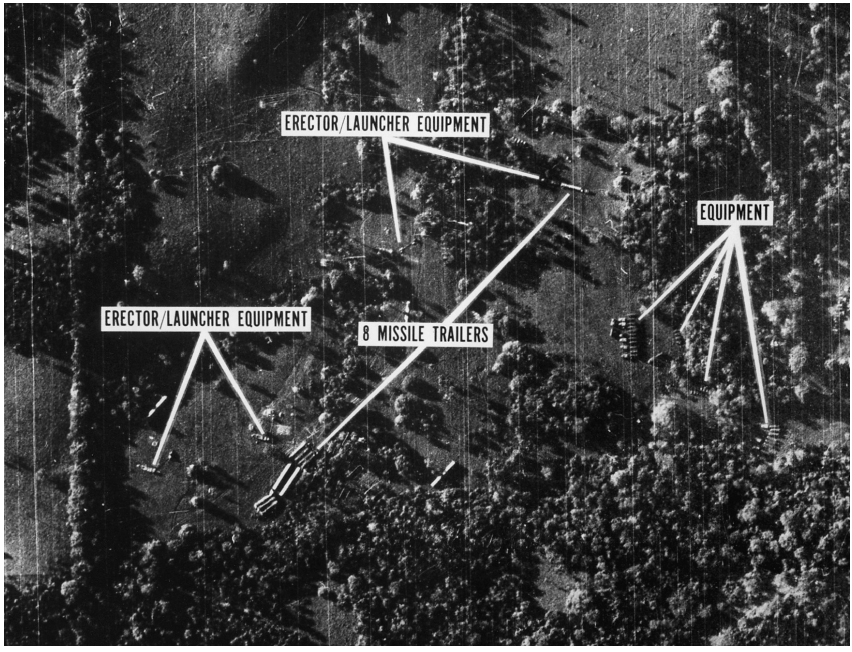


Figure 7: Detail of a U-2 Photograph of an SS-4 MRBM Launch Site, San Cristobal, Cuba, 14 October 1962. This evidence confirmed that Soviet missiles were being installed in Cuba.

Source: U.S. Department of Defense, photograph in the John Fitzgerald Kennedy Library, Boston, MA, PX 66–20:7 14 October 1962.

What tipped off the overhead surveillance were two HUMINT reports of "a Soviet truck convoy that appeared to be towing ballistic missiles toward the San Cristobal area."[69] That these reports were taken seriously is one of the curious serendipities that occur from time to time in intelligence analysis (and other research-based domains). What prompted the CIA and DIA analysts to take these reports seriously while earlier accounts had been dismissed remains a mystery. Garthoff asserts that it was new information taken in context with the observed "pattern of SA-2 surface-to-air missile sites in Western

69 Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis,* 2nd Edition (New York, NY: Longman, 1999), 220. Cited hereafter as Allison and Zelikow, *Essence of Decision.* Raymond Garthoff also notes this to be the case. See Garthoff, "US Intelligence," 23.

Cuba" that led to the tasking of the U-2 flight on 14 October (the track of which is shown in figure 8).[70]

Also contributing to the determination that the deployed missiles were SS-4 MRBMs was information transmitted to the British and American intelligence services by Oleg Penkovsky. While Penkovsky's espionage apparently did not warn the Americans that the Soviets were about to deploy offensive missiles in Cuba, he is credited with – among other things – providing technical information about the missiles.[71] Len Scott observes that Penkovsky provided the technical information that allowed the determination that the missiles were SS-4s instead of SS-3s, as well as information that allowed accurate assessment by the Americans of their readiness. Scott writes that this was important because

> the SS-3 had a range which US intelligence estimated at 630 nautical miles (nm), enabling coverage of seven Strategic Air Command (SAC) bomber/tanker bases; the 1020nm SS-4 could target 18 bomber/tanker bases (plus one ICBM complex), and some 58 cities with a population of over 100,000, including Washington, accounting for 92 million people.[72]

Shortly thereafter Penkovsky was detected, arrested, tried, and executed by the Soviets for his espionage.

---

70 Garthoff, "US Intelligence," 23.

71 Len Scott, "Espionage and the Cold War: Oleg Penkovsky and the Cuban Missile Crisis," *Intelligence and National Security* 14, no. 3 (Autumn 1999), 33. Cited hereafter as Scott, "Penkovsky."

72 Scott, "Penkovsky," 34. In making this assertion Scott draws on work previously published by Allison and Zelikow in *Essence of Decision* and by Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962* (Washington DC: Central Intelligence Agency, 1992).

Figure 8: U–2 Tracks over Cuba, 4–14 October 1962.

Sources: Map, Central Intelligence Agency. Tracks derived from a map in Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962* (Washington DC: Central Intelligence Agency, 1992), 3. Hereafter McAuliffe. Missile locations derived from Arthur C. Lundahl, "Additional Information – Mission 3102," Memorandum for Director of Central Intelligence and Director, Defense Intelligence Agency, 15 October 1962, in McAuliffe, 181–182; and Arthur C. Lundahl, "Additional Information – Mission 3107," Memorandum for Director of Central Intelligence and Director, Defense Intelligence Agency, 19 October 1962, in McAuliffe, 209. Track and missile locations are approximations. Lundahl was the Director, National Photographic Interpretation Center. The 19 October memo reports that a 5 September U–2 overflight did not detect the latter two missile sites. However, a review of the 5 September track (as presented in McAuliffe) shows the aircraft only came near the Sagua La Grande site. It should also be noted that the track of the U-2 – as flown on 14 October – deviated from the original planned route (which was farther to the west). The track as flown took the aircraft closer to the San Cristobal site. What might have happened had the original track been flown?

Despite their efforts at denial and deception, there was an evident lack of concealment of the missiles by the Soviets prior to their "discovery" on 14 October. General Anatoli Gribkov, a member of the Soviet General Staff in Cuba at the time relates,

> A missile–launching complex is not easily disguised…[Such] an installation…could be hidden from ground-level view. But from above, however, it could and did stick out like a sore thumb.[73]

Allison and Zelikow note that the Soviets only began to camouflage the sites *after* "the U.S. announced the discovery of the missiles and announced the blockade."[74] They conclude that the Soviet forces building the bases lacked personnel and resources to conceal them – a situation that apparently changed only after the missiles had been discovered.[75]

The Roles of Critical Thinking in the Cuban Crisis

Merom's critique of the Intelligence Community's estimate of Soviet intentions vis-à-vis Soviet weapons in Cuba reveals areas that would be well-served by critical thinking. First, when a critical thinking paradigm is in control, intelligence foraging and gathering are efficiently oriented. Questions are raised about the existing evidence – both anomalous and consistent – as well as where new disconfirming and confirming evidence might be discovered. Second, alternative – what in the context of Cuba, Merom calls *revolutionary* – theories are considered.[76] A structured process also speeds up the process of analytic sensemaking: estimates are crafted earlier.[77] Third, a methodological process opens analysis to "guiding principles of

---

73 Anatoli Gribkov, "The View from Moscow and Havana," in Anatoli Gribkov and William Y. Smith, *Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis* (Chicago, IL: Edition Q, 1994), 39. Cited hereafter as Gribkov, "The View."

74 Allison and Zelikow, *Essence of Decision*, 208.

75 Allison and Zelikow, *Essence of Decision,* 214.

76 Merom, "Estimate," 71.

77 Structured processes provide a framework that reduces the flailing around as analysts seek to find a starting point for their analyses. Morgan Jones discusses this at some length. See Jones, *Thinker's Toolkit,* xi–xvi.

research," enriching both the process and the results.[78]

However, there are dangers to such a paradigm, especially as "science" commonly is understood. As Jeffrey Cooper notes, "a 'science of analysis' is a conceit, partly engendered by Sherman Kent's dominating view of intelligence as a counterpart of the scientific method."[79] Mark and Barbara Stefik argue that "the working methods of science and invention leaves [sic] out imagination. This makes it both boring and misleading."[80] Analysts must focus on both evidence and inferences; otherwise they can "get the details right at the cost of ignoring important inferential judgments that need to be conveyed in order to provide a true sense of the uncertainties of both evidence and judgment."[81] Here again, critical thinking, with its emphasis on creative questioning, moderates the process. Such questioning opens the way for imaginative thinking. "[Intuition], curiosity, and a thirst for discovery – all essential elements of good science" could have alerted analysts working in 1962 (or at any other time) to the possibility that they were being denied or deceived.[82]

An interesting intersection exists between critical thinking and analogy, or drawing comparisons to derive new patterns and explanations. This intersection lies at the heart of creativity.[83] According to Keith Holyoak and Paul Thagard, there are commonly four steps to analogical problem solving:

> Often a problem solver will select a source analog by retrieving information about it from memory (*selection*), map the source to the target and thereby generate inferences about the target

78 Merom, "Estimate," 57.

79 Cooper, Pathologies, 26..

80 Mark Stefik, and Barbara Stefik, *Breakthrough: Stories and Strategies of Radical Innovation* (Cambridge, MA: MIT Press, 2004), 110.

81 Cooper, *Pathologies,* 27.

82 Cooper, *Pathologies,* 31.

83 This statement illustrates just how pervasive and powerful the use of analogy is in human reasoning and discourse. Taken literally, creativity has no heart (nor any other organs) since it is a notion or a concept, not a living animal. Yet the analogy to a living being aids understanding.

(*mapping*), evaluate and adapt the inferences to take account of unique aspects of the target (*evaluation*), and finally learn something more general from the success or failure of the analogy (*learning*).[84]

Since analogy is such a powerful element in human reasoning, how can critical thinking outwit or control it? As developed in this paper, it does so by imposing a structure on the thinking. By examining inferences and implications as well as alternative points of view, critical thinking calls into question the appropriateness of the analogies in use. Recent work by Paul and Elder reveals how this works. They request, for example, that reasoners state and restate explanations, add examples, and then include an analogy.[85] While initial statements about a phenomenon *do not* imply understanding, restatement, examples, and analogies *do* and further, provide measures by which comprehension can be fixed and assessed; they make knowledge explicit – something that can be thought about.[86] When knowledge and reasoning are explicit, assumptions are revealed.

According to Richard Neustadt and Ernest May, it is known that analogy is a tool commonly invoked by policymakers.[87] Critically thinking analysts can add substantively to the policymakers' options by constructively challenging the tendency to rely upon analogy as a way of addressing situations. For example, Neustadt and May observe that in coping with the missile crisis in Cuba, President Kennedy and his advisers relied on – among other things – an analogy to Pearl Harbor to justify why a "surprise" bombing of the Soviet missile

84 Keith J. Holyoak and Paul Thagard, *Mental Leaps: Analogy in Creative Thought* (Cambridge, MA: The MIT Press, 1995), 15. Emphasis in original. Cited hereafter as Holyoak and Thagard, *Mental Leaps.*

85 Richard Paul and Linda Elder, "Instructions to Participants," 25th Annual Conference on Critical Thinking, Berkeley, California, 9 July 2005. The first three elements were developed previously; analogy was new in 2005.

86 Holyoak and Thagard, *Mental Leaps, 20–22.*

87 Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York, NY: The Free Press, 1986). Cited hereafter as Neustadt and May, *Thinking in Time.*

bases was *not* a satisfactory option.[88] Kennedy's advisers, acting as analysts of the situation, critically evaluated the appropriateness of the analogy, pointing out its weaknesses and strengths. Kennedy concluded that sneak attacks were not a tactic lying within the U.S. tradition.[89]

In the Cuban case, getting analysts to restate their conclusions, provide examples, and make analogies would have revealed the strengths and weaknesses of their arguments about what they observed from the HUMINT sources. It would have shown their comprehension of what they wanted to conclude, revealed their assumptions and, in so doing, opened an avenue for "alternative" assessments of the issue. It would have done so by causing the analysts to question how it was that they failed to notice or ignore things.[90] The stage would have been set for an earlier, less risky, defusing of the impending crisis.

Another analogy employed in the Cuban missile crisis was the comparison to the Soviet position vis-à-vis the presence of *American* MRBMs in Turkey. A critical review reveals that the Soviet Union had tolerated the presence of these missiles – which had a longer range than those placed in Cuba – since 1957.[91] If the U.S. demanded the removal of the Soviet missiles from Cuba, was not a similar withdrawal of the American missiles from Turkey appropriate? Ultimately, this analogy provided a face-saving solution for the Soviet Union in the negotiations that followed. As a "secret" part of the agreement, the American Jupiter MRBMs were removed from Turkey five months after the Soviet Union removed its missiles from Cuba.[92]

---

88 Neustadt and May, *Thinking in Time,* 6.

89 Neustadt and May, *Thinking in Time,* 7.

90 Margaret A. Boden, *The Creative Mind: Myths and Mechanisms* (New York, NY: Basic Books, 1990), *25.*

91 Neustadt and May, *Thinking in Time,* 9.

92 Neustadt and May, *Thinking in Time,* 15.

Winners and Losers: The Crisis in Context

A Critical Assessment of the Leaders. In any confrontation there are winners and there are losers. Thinking critically about the confrontation over the Soviet missiles also involves determining who actually won as well as what the other outcomes might have been. Each of the three actors, Castro, Khrushchev, and Kennedy, had a number of interests at stake. In a number of circumstances each stood to gain at the expense of the others. What solutions were the most advantageous to each of the three actors? What were the motivating factors? A speculative – and admittedly simplified – critical comparison, again using Paul and Elder's model (summarized in table 3) illustrates how critical thinking also reveals much about who stood to gain and who stood to lose in the crisis.

Castro. Castro found his country under attack from the United States – both directly through economic sanctions and indirectly by Batista loyalists living in Florida.[93] The previous year the United States had launched an invasion attempt at the Bay of Pigs – which was repulsed. However the attempts by the United States to destabilize or overthrow the Cuban government did not end with their defeat. As Raymond Garthoff observes, "by the spring of 1962 the United States had embarked on a concerted campaign of overt and covert political, economic, psychological, and clandestine operations to weaken the Castro regime…including attempts to assassinate Castro."[94] In short, the United States was doing everything *except* conventional warfare to destroy Castro and his regime.

Castro's point of view was that the United States was a real enemy. He could reasonably assume that in light of its other activities and having attempted an invasion once, the United States would repeat its actions and this time *might* succeed (an implication). Another possible outcome that probably was considered was that war, conventional or nuclear, was likely. Castro must have possessed evidence of the military capabilities of the United States and probably inferred that

93 Raymond L. Garthoff, *Reflections on the Cuban Missile Crisis* (Washington, DC: The Brookings Institution, 1989), 7. Cited hereafter as Garthoff, *Reflections.*

94 Garthoff, *Reflections,* 9.

Element of Thinking	Considerations as seen from Castro's Point of View
Purpose	· Preserve Regime
Point of View	· United States threatens regime
Assumptions	· A second invasion will be attempted
Implications	· Invasion might succeed · War: conventional or nuclear
Evidence	· U.S. armed forces formidable
Inferences	· U.S. can overcome unaided Cuban forces.
Concepts	· Military strategy and doctrine, communist and capitalist theories
Key Questions	· How to deter United States from invading island

Table 3: A Comparative Assessment of Rival Motivations

Source: Developed by author.

Considerations	
as seen from Khrushchev's Point of View	as seen from Kennedy's Point of View
· Protect Cuba from United States · Force concessions from United States · Remove U.S. and NATO from Berlin · Spread Communism · Preserve Regime	· Get the missiles out of Cuba · Defend U.S. and allies against Communism · Preserve Regime
· United States a threat to Communism · Cuba threatened with invasion	· Communism threatens United States · Missiles are a threat
· Missiles in Cuba bargaining points · Missiles in Cuba protect Castro · Effort will be successful.	· Small Soviet Force · Strategy of removal is possible
· U.S. concessions ·War: conventional or nuclear	· Successful removal · Escalation of measures ·War: conventional or nuclear
· U.S. armed forces formidable	·Administration politically vulnerable over crisis · Khrushchev is a formidable adversary · Khrushchev is bluffing
· U.S. can overcome unaided Cuban forces. · Missiles provide necessary aid · United States will concede.	· Khrushchev will back down · Military option not required
· Military strategy and doctrine, communist and capitalist theories	· Military strategy and doctrine, communist and capitalist theories · Monroe Doctrine
· How to deter United States from invading Cuba · How to dominate the United States	· How to get the Soviets and their missiles off of Cuba

unaided, his own forces were no match for the U.S. forces. Underlying Castro's considerations were a number of ideas about military strategy and doctrine, as well as communist and capitalist theories. A corollary consideration commonly believed by many Americans (at the time and still today) might have been how Communism could have been spread across the Western Hemisphere, especially the United States. Castro's key question was, "How can I prevent the United States from invading again?"

Khrushchev. What motivated Khrushchev remains controversial. His motives certainly were more complex, as various explanatory hypotheses reflect. First, there is the argument that Khrushchev had an ally "in the faith" to protect. He too believed that the United States would invade Cuba a second time.[95] However, as Allison and Zelikow counsel, the troop buildup itself and *not* the nuclear missiles was what Khrushchev did to offset the perceived threat to Cuba from the United States.[96] The deployment of the nuclear missiles was related to some other issue.

Next, the situation posed an opportunity to force concessions from the United States – perhaps about Berlin, or the United States' own offensive missiles located in Europe and Turkey. Allison and Zelikow find sufficient evidence to lead them to believe that removing the U.S. and NATO troops from Berlin was a key factor motivating Khrushchev to deploy the missiles to Cuba.[97] Securing his borders from the American's Jupiter missiles may have been an additional motivating factor.

Additionally, there was Khrushchev's avowed purpose of spreading Communism across the globe. In this context the deployment of weapons lies within the context of "a great power rivalry… between the U.S. and the values and interests it represented…and

95 James J. Wirtz, "Organizing for Crisis Intelligence: Lessons form the Cuban Missile Crisis," in Blight and Welch, *Intelligence and the Cuban Missile Crisis,* 130. Cited hereafter as Wirtz, "Organizing."

96 Allison and Zelikow, *Essence of Decision*, 87.

97 Allison and Zelikow, *Essence of Decision*, 99–109.

the Soviet Union's communist agenda."[98] At a reception for foreign ambassadors in Moscow in 1956, Khrushchev threatened, "Whether you like it or not, history is on our side. We [the communists] will bury you!"[99] This remark (among others) also reveals an additional purpose: Khrushchev, like all dictators, had to appear stronger than his adversaries – his political survival depended on it.

Khrushchev's point of view was that the United States (and its allies) were a threat to Communism everywhere and needed to be contained. He was presented with a confluence of opportunities and responded with the military buildup in Cuba and the deployment of the missiles. He apparently assumed that if he could get nuclear missiles into Cuba he'd have bargaining points useful in such a containment strategy. Later, Khrushchev believed he could effect a change in the balance of power between the two nations.[100] Possible outcomes included the prospect of further U.S. concessions, protection of Cuba from invasion, and either conventional or nuclear war.

Khrushchev had direct evidence drawn from the Korean War and possibly other evidence from spies operating in the United States about the capability of the U.S. military. Given the nuclear missiles he actually deployed as well as his assignment (temporary) of operational control of those missiles to the Soviet Group of Forces commander, General Issa Pliyev, Khrushchev seems to have inferred the U.S. forces were formidable.[101] He also apparently concluded that the missiles – and the other forces – would be adequate to the task of successfully satisfying his purposes; the United States, faced with

98 Allison and Zelikow, *Essence of Decision*, 88.

99 Nikita Khrushchev, "Speech to Ambassadors at Reception, 17 November 1956," in James Beasley Simpson, compiler, *Simpson's Contemporary Quotations: The most Notable Quotes since 1950* (Boston, MA: Houghton Mifflin Company, 1988), online edition, URL: <http://www.bartleby.com/63/83/183.html>, last accessed 20 April 2006. Ironically, Khrushchev was wrong. History sided with his adversaries.

100 Cited in Garthoff, *Reflections,* 23.

100 Gribkov, "The View," 4. Control reverted back to Moscow in September.

operational missiles in Cuba, would concede.[102] The concepts on which Khrushchev relied probably were the same as those on which Castro relied: military strategy and doctrine as well as communist and capitalist theories. Again, Khrushchev's key question mirrored that of Castro: How to keep the Americans from invading Cuba. Additionally, there could have been a second question on how to dominate, or at least gain concessions from, the United States.

Kennedy. Finally, there was Kennedy. While Kennedy's exact purpose vis-à-vis Cuba *prior* to the discovery of the missiles also remains unclear, it is known that he did not plan to invade the island during the summer and fall of 1962.[103] However, 1962 was an election year and the Kennedy administration was vulnerable with respect to Cuba.[104] Kennedy could not afford to appear soft on Communism. Kennedy also had an interest in keeping the U.S. and NATO forces in Berlin.

All this changed once the missiles were discovered. Kennedy's deliberations revolved around removing the missiles as expeditiously as possible. He no doubt realized that if his administration bungled the crisis they might lose at the polls in November.[105] Therefore, it is reasonable to conclude that Kennedy's goals included retaining control of Congress – he too had a regime to preserve. Kennedy's point of view was clear: the deployed Soviet strategic nuclear missiles were a threat to the United States and must be removed. He assumed that such a strategy could be developed. He apparently also assumed that the Soviets had placed a *small* force on the island. Possible outcomes included successful removal of the missiles and their

---

102 Wirtz, "Organizing," 128. Wirtz argues that the Soviets were not only wrong about the U.S. reaction, they were *surprised!*

103 Wirtz, "Organizing," 130.

104 Fen Osler Hampson, "The Divided Decision-Maker: American Domestic Politics and the Cuban Crises," *International Security* 9, no 3 (Winter 1984/85), 136. Cited hereafter as Hampson, "Divided."

105 Hampson, "Divided," 143.

supporting forces, an escalation of measures to prompt that removal, and the possibility of conventional or nuclear war.[106]

Kennedy had evidence of his political vulnerability He also had evidence – Khrushchev's own actions included – that the Soviet leader was a formidable adversary. But based on Penkovsky's evidence he inferred that Khrushchev might be persuaded to back down. As Scott concludes, "various writers contend that Penkovsky's intelligence…[guided] Kennedy's handling of the crisis from a position of strength."[107] This occurred in part because "the KGB's discovery of Penkovsky's espionage alerted Khrushchev to the fact that Kennedy now knew he was bluffing."[108] As has been noted, Kennedy lacked accurate evidence about what was really on the island. Nevertheless as has been noted, he inferred that military strikes were not – at least at that time – an option. Kennedy probably relied on the same concepts on which Castro and Khrushchev relied. In addition, the concepts embodied in the Monroe Doctrine were also probably a factor. Kennedy's key question was, "How to get the Soviets and their missiles out of Cuba?"

Foresight. Viewed with foresight, there were a number of possible outcomes to the crisis based on the inferrable goals that could be associated with any of the three leaders. A win for one of the leaders was not necessarily a loss for the others as table 4 shows. In some cases, achieving one's goal was a win for the leader, but a failure to achieve it was *not* necessarily a loss. "Winning" the crisis should have involved attaining all or most of one's goals. However, since not all goals were of equal importance, failing to achieve one could mean that one lost in the larger crisis. Similarly, achieving one's goals did not guarantee winning the larger crisis. This becomes evident as the actual winners and losers are considered.

---

106 Neustadt and May, *Thinking in Time*, 6-15. Given the presence of the Soviet tactical nuclear weapons on Cuba it is probable that *any* invasion that began with conventional forces would have escalated to nuclear scenarios.

107 Scott, "Penkovsky," 31.

108 Scott, "Penkovsky," 32.

And the Winner is? Who actually won the Missile Crisis? Critical assessments of the three leaders involved and the attainment of their goals reveals the answers. First, Castro certainly got what he wanted: The United States never again invaded Cuba.

What did Khrushchev get out of the resolution of the crisis? From the standpoint of his first goal, to protect Cuba from the United States, he was successful. The subsequent removal of the Jupiter

Goal	Outcome	Leader		
		Castro	Khrushchev	Kennedy
Prevent U.S. Invasion of Cuba	Achieve	Win	Win	Neutral
	Fail	Lose	Lose	Win
Get the Missiles out of Cuba	Achieve	Neutral	Lose	Win
	Fail	Win	Win	Lose
Spread Communism	Achieve	Win	Win	Lose
	Fail	Neutral	Lose	Win
Get U.S. and Allies out of Berlin	Achieve	Neutral	Win	Lose
	Fail	Neutral	Lose	Win
Force Concessions from United States	Achieve	Win	Win	Lose
	Fail	Lose	Lose	Win
Force Concessions from Soviet Union	Achieve	Neutral	Lose	Win
	Fail	Neutral	Win	Lose
Force Concessions from Cuba	Achieve	Lose	Neutral	Win
	Fail	Win	Win	Neutral
Preserve Regime	Achieve	Win	Win	Win
	Fail	Lose	Lose	Lose

Table 4: Goals and Outcomes in the Cuban Missile Crisis

Source: Developed by author.

missiles in Turkey appeared to increase the security of his borders – an apparent concession from the United States.[109] However, Khrushchev failed to spread Communism further. And Berlin remained partially

109 The issue of the Jupiter missiles is complex. They were not included in the formal agreement but were offered up in a secret unilateral assurance from Kennedy (Garthoff, *Reflections,* 132).

in the hands of the West. If, as Allison and Zelikow postulate, this was the real motivation behind the nuclear deployment then Khrushchev's failure was highly significant. Additionally, his regime was embarrassed by the revelation in the United Nations of the presence of the missiles. Ultimately, he was removed from power two years later and placed under house arrest until his death in 1971. So, Khrushchev, while he won a number of his goals, wound up the overall loser.

Kennedy is the other winner in the crisis. He gets the Soviets missiles removed from Cuba while avoiding war. He is later able to retire an obsolete missile system (the Jupiters). He prevents the Soviet Union from seizing control of Berlin. Finally, his popularity increases and the Democrats retained power in the 1962 elections.

Ten Years Later, They Meet Again

It is worth noting that Soviet denial and deception in support of military deployments and operations in Cuba did not end in the early winter of 1962. In 1970 Henry Kissinger stormed into the office of H. R. Haldeman and demanded to see President Nixon. Aerial reconnaissance had brought news. "The Cubans are building soccer fields," Kissinger said. "Cubans play *baseball*. *Russians* play soccer."[110] The Soviets it seems had been discovered building a submarine base at Cienfuegos. Prior to a particular overflight, that fact had been denied to the United States. The soccer fields were for the recreation of Soviet troops.

---

110 H.R. Haldeman, with Joseph DiMona, *The Ends of Power* (New York, NY: Times Books, 1978), 85–86, in Patrick J. Haney, "Soccer Fields and Submarines in Cuba: The Politics of Problem Definition," *Naval War College Review* L, no 4, sequence 360 (Autumn 1997), URL: <http://www.nwc.navy.mil/press/Review/1997/autumn/art5–a97.htm>, last accessed 6 April 2006. Emphasis in original.

Judgment: Critical Thinking Would Have Made a Difference

As this case study makes clear, there are a number of junctures where critical thinking or structured analytic methods could have made a difference in analyzing the Soviet missile deployment to Cuba. While it is true that Sherman Kent argued for a scientific approach to analysis, it does not seem to have been widely practiced at the time.[111] As of 1962, most studies that we now have in hand on human reasoning in intelligence had not been completed. The champions of structured intelligence analysis methods had not yet developed their techniques.

Nevertheless, a study of the crisis is germane because the same kinds of errors *repeat themselves again and again.* The errors seen in the Cuban case – failure to question assumptions, to take seriously the evidence and the patterns they imply, to counterfactually examine analytic implication and consequences, in short to make reflective judgments – also were cited by the Senate in its critique of the 2002 Iraqi WMD estimate.[112] In both cases, deceptions confounded analysts, leading them to wrong conclusions.[113] In the Cuban case the analysts eventually figured it out. This did not occur in the

---

111 Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, PA: Princeton University Press, 1949), 151–208.

112 In the Cuban situation, the debate between McCone and analysts over the nature of the weapons the Soviets might emplace came close to overcoming these errors. Regarding the Iraqi WMD estimate, the debate between the CIA and the Department of Energy over the use of the aluminum tubes also came close. Unfortunately, the incipient debate focused on the results, not the process. In both cases, the side that was eventually proved right failed to make the now-accepted case.

113 Sherman Kent challenged this assertion in his defense of the original estimate and the process by which it was created. He believed that an earlier revelation of the Soviet actions would have led to an intractable situation. However, an earlier revelation – say in August – would have offered President Kennedy and his advisers more options, particularly more *diplomatic* options. Kent also failed to observe that denial and deception occurred – at least for the record. See Sherman Kent, "A Crucial Estimate Relived," Reprint, *Studies in Intelligence* 36, no. 5 (1992): 111–119.

most recent failure. Critical thinking skills went unused among both generations of analysts.

How Can Intelligence Analysts Employ Critical Thinking?

The Poor Record

Critical thinking is what consumers of intelligence appear to expect when they task producers to examine issues. Corporate consumers require analysts creating intelligence to "[evaluate] a situation, problem, or argument and [choose] a path of investigation that leads to finding the best possible answers."[114] In the national security field, strategic intelligence pioneer Washington Platt notes that "[intelligence] is a meaningful statement derived from information which has been selected, evaluated, interpreted, and finally expressed so that its significance to a current national policy problem is clear."[115] Derived from strategic intelligence, "best answers" should clearly express what is significant to national policy problems. They may also support warfighters with essential operational and tactical intelligence. Critical thinking leads to the best answers for the specific context at hand.

Unfortunately, analysts' biases and mindsets repeatedly obscure best questions and answers. From well before the Japanese surprise attack on Pearl Harbor to the 2002 estimate on Iraqi weapons of mass destruction, a failure to think critically about potential crises contributed to repeated intelligence failures.[116] "Expert analysis"

---

114 Daniel Feldman, *Critical Thinking: Strategies for Decision Making* (Menlo Park, CA: Crisp Publications, Inc, 2002), 4.

115 Washington Platt, *Strategic Intelligence Production: Basic Principles* (New York, NY: Frederick A. Praeger, 1957), 8.

116 George S. Pettee, *The Future of American Secret Intelligence* (Washington, DC: Infantry Journal Press, 1946). Chapter 1 provides a summary of U.S. intelligence failures during the first half of the 20th Century. While hindsight is an imperfect mirror for reviewing the past, one conclusion to be drawn from a review of the evidence is that critical thinking could have minimized many of the ensuing crises.

was not enough.[117] Biases and mindsets too often converted subject-matter confidence into arrogance; false assumptions blinded analysts to their target's true intentions. For example, at least one CIA Iraq analyst acknowledged that the 1990 invasion of Kuwait,

> was an intelligence failure…We were guilty of a kind of mindset…The idea that a country [Iraq] would march up to the border, put 100,000 troops there, go in and do what they've done; I don't think anybody thought they'd do it.[118]

In 2002, Intelligence Community analysts failed to definitively assess whether the Iraqi government still possessed weapons of mass destruction. The Senate noted in its review of the failure that

> [rather] than thinking imaginatively, and considering seemingly unlikely and unpopular possibilities, the Intelligence Community instead found itself wedded to a set of assumptions about Iraq, focusing on intelligence reporting that appeared to confirm those assumptions.[119]

The mistakes of 2002 also occurred in 1990 – and for that matter in 1941. Analysts failed to question assumptions widely held at the time. Instead they chose the first answer that satisfied the situation, a phenomenon known as "satisficing."[120] Other means by which intelligence analysts and policymaking customers reasoned poorly are listed in table 5. According to Ephraim Kam, the problem is so great that the intelligence analysis process is "consistently biased, and…bias

---

117 Anthropologist Rob Johnston explores this paradox. See Dr. Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, 2005), 64–66. Cited hereafter as Johnston, *Analytic Culture.*

118 Anonymous CIA Analyst, 1990, in Don Oberdorfer, "Missed Signals in the Middle East," *Washington Post Magazine*, 17 March 1991, 40.

119 The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States,* March 31, 2005, URL: <http://www.wmd.gov/report/ index.html>, last accessed 28 July 2005, 155. Cited hereafter as WMD Commission, *Report.*

120 Morgan D. Jones, conversation with the author, 15 December 2003.

is the cornerstone of intelligence failures."[121] Paul and Elder claim that much thinking is "biased, distorted, partial, uninformed, or down-right [sic] prejudiced."[122] There are repeated failures to think critically; but could critical thinking about these situations prevent the failures?

Means by Which Decisions are Made
Select first answer that appears "good enough."
Focus on narrow range of alternatives, ignoring need for dramatic change from existing position.
Opt for answer that elicits the greatest agreement and support.
Choose the answer that appears most likely to avoid some previous error or duplicate a previous success.
Rely on a set of principles that distinguish "good" alternatives from "bad" alternatives.

Table 5: How Analysts Decide

Source: Excerpted from Alexander George, *Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice* (Boulder, CO: Westview Press, 1980), Chapter 2.

Critical thinking helps mitigate the effects of mindsets and biases by invoking skillful examination of evidence both for and against an issue, as well as consideration of obvious and less obvious alternative explanations. In the 1990 example, thinking critically would have raised other possible explanations for why Hussein's troops were on the Kuwaiti border and what he intended for them to do.[123] That the Iraqi troops were trained by the former Soviet Union and followed its tactics might have been an indicator of future intentions. In the case of the weapons of mass destruction (WMD), analysts might have

121 Ephraim Kam, Surprise Attack: The Victim's Perspective (Cambridge, MA: Harvard University Press, 1990), 85.

122 Paul and Elder, *Concepts and Tools,* 1.

123 A consideration of who trained Hussein's troops – in this case, the Soviet Union – might have led to an examination of military doctrine. Thus, it quickly would have become clear that troops mobilized on a border were going to cross that border. Analysts would then have known that an invasion of Kuwait was imminent.

asked, as they realized they had no new evidence of the weapons, "How can we prove that the weapons of mass destruction definitely are not there?" or "What would we expect to see if Saddam Hussein had gotten rid of his weapons of mass destruction?"[124]

We must assume that analysts can be encouraged to think in this manner. Modern strategic intelligence pioneer Sherman Kent believed this to be the case when he wrote nearly 60 years ago that intelligence analysts "are supposed to have had more training in the techniques of guarding against their own intellectual frailties" than the larger populace.[125]

Assessing Evidence[126]

Understanding how evidence is assessed is a necessary first step in understanding how analysts can better reason with and about it. The incomplete and ambiguous information and data with which intelligence professionals work compounds their reasoning process.[127] Sources are unreliable and contradictory; adversarial denial and deception increase doubt. When information and data are questionable, derived evidence is even more uncertain, and inferences arising from that evidence may be highly suspect. One way that analysts can reduce this uncertainty is by building defensible inferences

---

124 These analyses are those of the author. The last question was jointly arrived at in a conversation between the author and Mark Lowenthal, 26 July 2005.

125 Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949), 199.

126 This section is based (with additions) on materials developed by Francis J. Hughes and the author for a structured analytic methods course taught at the National Defense Intelligence College. For a deeper examination of evidence assessment see Francis J. Hughes and David A. Schum, *Credibility Assessment: A First Step in Intelligence Analysis,* unpublished tutorial, National Defense Intelligence College, April 2003.

127 Information, data, and evidence are different kinds of knowledge. Pieces of information comprise data, which in turn comprise evidence. Evidence is further distinguished from data by the fact that it contributes to discrimination among alternative end states. Data, while relevant, do not necessarily allow discrimination.

TESTIMONIAL: APPLYING CRITICAL THINKING

This is a true story. All the characters are real and really naive.

As a fresh graduate of NSA's critical thinking and structured analysis class, I attended an Intelligence Community class on counterintelligence. My fellow students included folks from all over the community, including CIA and FBI case officers. During the class, the instructor put forth a case study for students to think about and decide how best to "analyze and investigate" to find the mole. Differing opinions surfaced, but a common thread appeared among the case officers: follow your "gut" feeling and collect evidence to support that assumption, no matter how long it took.

The instructor, enjoying the collective mindset and the opportunity to shatter paradigms, concentrated on how information was collected and analyzed. Again, the case officers agreed the best solution was to continue gathering information until you "proved your case." I, the lone NSA token student, raised my objection, "How long is long enough? Until you've ruined the career of innocent, hardworking persons in the IC, or until you find another answer you like?" Although it did not earn me friends, it did open up a window to inform these case officers and other attendees about the intricacies of analysis.

Critical thinking is not just about putting information together, finding a pattern, then choosing an answer, it is about reducing bias, considering all options available, and presenting options to a decision–maker. And critical thinking is about paying attention to what and how you are doing it. I reasoned that, since the investigators in the case study concentrated on only one

Source: A mid–level intelligence professional at the National Security Agency

from the evidence. At their most basic level, these inferences depend on credibility (can it be believed), relevance (does the evidence bear on the issue), and inferential or probative force (how compelling is it in answering the questions raised by the issue). Unfortunately, no mass or body of evidence – in intelligence or anywhere else – comes with these three properties already established. Establishment of these properties to abet uncertainty reduction through inference occurs only through a process of argument, creative hypothesis generation, and the development of chains of reasoning.

Authenticity, accuracy, and reliability represent criteria for establishing the credibility of tangible evidence.[128] An analyst striving

128 "Tangible evidence" is a technical term describing *things* that bear relevance to an issue under scrutiny. It is contrasted with "testimonial evidence"

person, the analysis was faulty because somewhere along the line they limited their suspects (introduced bias) regardless of reason (access, family connections, angel–like qualities, etc.). Although it would take time, the investigators should conduct quantitative and qualitative analysis, make a decision tree (options open to a mole in a heavy security environment), and then play Devil's Advocate. In addition, analysis never reveals one "solution" or "smoking gun"; it leads to two or three "options" which can be investigated in detail.

The instructor, pleased that someone in the class knew what the "Analysis of Competing Hypotheses" was, revealed the answers of the real–life case study: after three years of investigating, the case officers had the wrong person due to incorrect information in old reports and limiting their suspect list. Instead of going back to the original source information, the officers read old reports that were unfortunately biased by Agency politics and external societal events (1950–60s). The real mole was discovered over a decade later; he was the son of a former Agency chief, well educated and well liked, but did not have access to the information. The individual "borrowed" interesting reports from friends who had access, covered his tracks, and continued spying against the U.S. for several years. Just as the authorities were about to arrest him, he was found dead in a hotel room from a reported suicide, but the cops could not figure out how he had two bullets in his chest and one in the back of his head. Miracle suicide.

What is the moral of the story? Conduct a thorough analysis right the first time and you can catch a mole anytime. I only hope the attending case officers got the message, especially from a non–gun toting NSA analyst.

who wishes to remain anonymous, email to the author, 9 March 2006.

to determine authenticity may ask, "Is the evidence what it seems to be?" In determining accuracy, the key question is whether the piece of evidence or the system that produced it has the resolution to reveal what the analyst believes the event or record should reveal. Assessing reliability involves determining whether different means of collection produce the same results.

If, on the other hand, the evidence is testimonial, different criteria apply. The first thing to be established is whether the source is being truthful. Truthfulness is not absolute. Rather, it is time- and context-dependent. A source may believe he is being truthful about an issue or may have legitimate reasons to be untruthful about that issue. In

– what people say about the issue.

another time and about another issue, these impediments to veracity may not exist for that source. Therefore, establishing the truthfulness of a source can pose a significant challenge to the analyst.

In an ideal situation, a review of evidentiary relevance causes an analyst to examine the likelihood of any potential answer to the problem or question – a hypothesis – with an eye to the modification of existing hypotheses or even the invention of new ones. In other words, an analyst might theorize that a certain bit of evidence will indicate that an individual or a group of individuals will engage in nefarious activity. Yet, if none of the evidence at hand bears on the issue, then the analyst may need to reconsider – or even reject – this evidence based on its lack of relevance. The analyst also should consider that the individual *may not* engage in the activity.

What is true about the future is also true about the present and the past. A lack of evidence relevant to an issue should prompt analysts to reassess their theories about the issue at hand. For example, an unnamed FBI investigator in the 2001 anthrax case noted, "[Reasoning] says that if you think a person is your guy, but you can't find anything to put him in the game, you've got to keep looking at others."[129] The failure of the FBI to implicate its principal suspect forced it to consider other explanations as to who sent the anthrax-laden letters in September 2001 to political leaders and media figures.

The analyst also is concerned with how strongly the evidence

129 Allan Lengel and Guy Gugliotta, "Md. Pond Produces No Anthrax Microbes: FBI Sought Clues In Deadly Attacks," *Washington Post*, 1 August 2003, A03. Cited hereafter as *Washington Post,* "No Anthrax." While this is a law-enforcement example, it illustrates good critical questioning about an apparent lack of evidence. Criminal investigation and intelligence analysis similarly assess events and evidence with the goal of description, explanation, and interpretation. The principal difference is that intelligence analysis endeavors to do so *before* the event occurs – in other words, *to estimate.* It is worth noting that over two years after the pond was drained the case remains unsolved; the individual under suspicion at the time was never charged with the crime. The FBI was unable to link the evidence to the individual. See for example, Allan Lengel, "Little Progress In FBI Probe of Anthrax Attacks: Internal Report Compiled As Agents Hope for a Break," *Washington Post,* 16 September 2005, A01.

undermines or supports the particular hypotheses under examination – the probative force of the evidence. Certain evidence, coming from certain kinds of sources, persuades more strongly than does other evidence drawn from other sources. Tangible evidence might have greater probative force than testimonial evidence. Consider, for example, a hypothetical biological weapons issue. Traces of certain toxic substances found near an alleged biological weapons lab carry greater probative force than the testimonial denials of the government of the country in which the lab and the samples were found.

The "ideal" analyst also assesses the objectivity, observational sensitivity, and competence of sources. One question suitable for this assessment is how biases may have corrupted a source's objectivity. Did the source see or hear the evidence directly, and under what conditions did this occur? A reality check also is made at this point. Does it makes sense that a particular source claims to have been in a position to make the observation or have access to the source of information?

Another consideration involves denial and deception. In assessing the evidence, the analyst should ask, "What is the likelihood that I am being deceived? This question is surprisingly difficult to answer accurately. Given that anchoring biases and confirmation heuristics cause analysts to find what they seek to find, a denial and deception hypothesis is often easily proved.[130] Critical thinking challenges this by forcing an examination of alternative points of view. For intelligence analysts, proactive, focused and surreptitious collection of information about the often minimal disconfirming evidence pays rich dividends.[131] In this case, the question becomes, "What is the likelihood that I am *not* being deceived?" Thus engaged, really good intelligence analysts create valuable knowledge.

---

130 Author's notes, National Defense Intelligence College, Denial and Deception Advanced Studies Program, Spring 2005. The author is a National Intelligence Council-sponsored participant in the Foreign Denial and Deception Committee's Denial and Deception Advanced Study Program at the NDIC.

131 Ben-Israel, "Logic of the Estimate Process," 708–709.

Facilitating Evidentiary Assessment

The questions that need to be asked about each piece of evidence are the same as those employed in critical thinking. In making her evaluation of what constitutes evidence, the analyst repeatedly asks "why": "Why do I believe this information is relevant to the question at hand (either against or for) and therefore exists as evidence?" "Why do I believe the source to be credible?" Additional questions about the analyst's own thinking processes might arise, such as: "What are my biases and why do they lead me to think this way?"

For example, in assessing the intentions of former Iraqi dictator Saddam Hussein in light of the U.S. destruction of his intelligence headquarters in 1993, an analyst might ask whether Hussein's declarations not to retaliate against the United States were credible. A corollary question might be, "What does Saddam Hussein gain by denial and deception?" Based on Hussein's statement, a determination that additional evidence was needed would stimulate collection of similar statements from other episodes. By analyzing what Hussein did in those instances, the analyst might determine that he was usually untruthful. Therefore, this piece of evidence would be deemed to be of low credibility despite its probative force, and relevance to the determination whether Hussein would or would not retaliate.[132] In other words, Hussein's statement might reflect an ongoing deception campaign. To explore this hypothesis further, the analyst might seek to determine whether increases in Iraqi agent communications were relevant to the issue and whether additional collection of such broadcasts was warranted.[133]

In practice, these and similar questions can be answered quickly. Analysts often answer some of them unconsciously as they struggle

132 Heuer develops this scenario and evidence in an example of the analysis of competing hypotheses. See Heuer, *Psychology*, 101–102.

133 Heuer, *Psychology,* 101–102. For a recent detailed look at Saddam Hussein and deception see Kevin Woods, James Lacey, and Williamson Murray, "Saddam's Delusions: The View from the Inside," *Foreign Affairs* 85, no. 3 (May/June 2006). URL: <http://www.foreignaffairs.org/20060501faessay85301/kevin-woods-james-lacey-williamson-murray/sadda-s-delusions-the-view-from-the-inside.html>, last accessed 31 March 2006.

to meet short deadlines. However, as a function of not employing scientific methods or other structured and critical thinking techniques, their thinking is largely intuitive. Analysts choose to ignore how mindsets and assumptions impede their judgments. Conversely, critical thinking ensures that the reasoning process is a self-conscious one. By making the unconscious conscious, analysts reveal where they may be biased, helping ensure that questions they address are thoroughly and fairly considered.

Each method of analysis uniquely interacts with the intelligence question; therefore, the method (or methods) selected can produce profoundly different results – affecting the analyst's arrival at the most accurate answer.

An analyst committed to critical thinking continually asks questions while developing the mass of evidence needed to assess an issue. Evidence arises from questions answered satisfactorily. Information for which the questions cannot satisfactorily be answered is excluded – but only after the analyst reflects on the process of evidence development. Consideration is owed to the question of how biases, and possibly active denial and deception by an adversary, have influenced the selection of both questions and answers. One way of revealing bias is by asking questions such as, "If the opposite outcome is actually true, what other evidence would I expect to see?"

The marshaling of evidence refers to a questioning process by which data and information are assessed and evidence is created. It may be done in solitary fashion, Socratically with a teammate, or collegially among Intelligence Community focus groups. It is a vital ingredient of productively imaginative intelligence analysis. Each question an analyst asks not only becomes a device for attracting existing evidence, but also generates new evidence not yet visible. Identifying new evidence increases the thoroughness by which the issue is evaluated and increases the probability that the correct solution has been discovered.

Embracing a Methodology

Once a relevant mass of evidence is established, the analyst evaluates which method or methods of analysis may best develop

a solution to the issue. Differences among various analytic methodologies, techniques, and tools are not trivial.

In fact, comparing the results of different analysis methods can be a valid means of establishing the accuracy of the answer. If various means of analysis yield multiple results, a review by different analysts makes for the ideal environment for critical thinking to discuss and debate those results.[134]

Therefore, assessment of the available evidence includes redirecting thinking, soliciting feedback from other sources, appraising the quality of possible answers, and comparing initial goals with results. In so doing an analyst employs interpretive and evaluative skills to select the best mass of evidence to analyze.

Creating Better Inferences

Critical thinking aims to ensure that inferences are reasonable and evidence-based. Inference creation begins at the same time that analysis starts. As each piece, or the whole mass of evidence, is considered, inferences are made.[135] Resulting "chains" of inferences linking the evidence to the hypotheses under consideration are known as arguments. Chains of inferences converge – strengthening the argument – or diverge – weakening it. The self-reflective nature of critical thinking places a check on these inferences. The analyst asks, "Do my inferences flow from the evidence?" and, "Are my inferences logical given the evidence and other inferences I have made?"

Inferences lead to a search for additional evidence. In other words, based on inferences drawn from the evidence at hand, an analyst may infer that there are other sources of evidence to consider. For example, such reasoning was cited in the explanation of why

134 For a more detailed discussion of this and other means of countering biases, see Heuer, *Psychology*, 170–184; Irving Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, 2nd Edition (Boston, MA: Houghton Mifflin Company, 1982); and Scott Plous, *The Psychology of Judgment and Decision-making* (New York, NY: McGraw Hill, Inc., 1993).

135 Indeed, the analyst's acceptance – or rejection – of this evidence is a result of inferences: either the evidence is valid, credible, and relevant, or it is not.

the FBI investigated a pond in western Maryland during June 2003, searching for the source of the 2001 anthrax attacks. At the time, the FBI believed their primary suspect lived near the pond in question. In their search for additional evidence, they reasoned that the pond might be something in which evidence had been hidden. Thus, inference led the FBI to drain the pond to search for that evidence.[136]

The analyst self-consciously evaluates the thinking process and the biases that have affected it to reduce unproductive thinking and to consciously develop new ways of understanding the evidence at hand. This self-regulation also plays a role as the available evidence is considered. A means of accomplishing this within a collaborative setting is to seek the assistance of colleagues of diverse backgrounds. The underlying premise is that their biases differ sufficiently to enable productive and thorough analysis to occur.[137]

Producing Intelligence

Analysts who produce intelligence assessments and judgments have the opportunity to employ what Peter Facione considers the core cognitive skills of critical thinking: interpretation, analysis, evaluation, inference, explanation, and self-regulation.[138] Each of these competencies contributes to the integration of available evidence through a clear line of reasoning to the most probable answer.

Facione asserts that good critical thinkers can explain "what they think and how they arrived at that judgment."[139] By documenting the

---

136 *Washington Post,* "No Anthrax."

137 See Robert Callum, "The Case for Cultural Diversity in the Intelligence Community," *International Journal of Intelligence and Counter Intelligence* 14, no. 1, Spring 2001: 25–48.

138 Peter A. Facione, Critical Thinking: What It Is and Why It Counts (Milbrae, CA: California Academic Press, 1998, updated 2004), URL<http://www.insightassessment.com/>, last accessed 22 July 2005, 4. Cited hereafter as Facione, Critical Thinking.

139 Facione, *Critical Thinking,* 5.

reasoning process used to arrive at an answer, analysts move beyond merely "stating results [to] justifying procedures, and presenting arguments."[140] Questioning biases and mindsets encourages consideration of alternative possibilities that overcome what Josh Kerbel refers to as "single–outcome [analytic] trajectories."[141] Most importantly, analysts demonstrate a critical spirit – a reflection of character.[142]

Thus, critical thinking contributes to short-term analysis and assumes an essential role in longer-term analysis. Indeed, building a comprehensive picture of an issue or target requires critical thinking to determine which previous reports are included or excluded. "How do the parts contribute to the whole?" is one question the analyst asks. Another is, "How is the whole greater than the sum of its parts?" When previously published intelligence reports diverge, the critical thinking process helps the analyst ensure that the divergence is considered fairly and that the resulting intelligence does not merely satisfice.

---

140 Facione, *Critical Thinking*, 6.

141 Josh Kerbel, "Thinking Straight: Cognitive Bias in the US Debate about China," *Studies in Intelligence* 48 no. 3 (2004), URL: <http://cia.gov/csi/studies/vol48no3/index.html>, last accessed 22 February 2006.

142 Facione, *Critical Thinking*, 7. See also Moore and Krizan, "Intelligence Analysis," 9–11.

How can Analysts be Taught to Think Critically?

Many people would rather die than think – in fact, they do.

—Bertrand Russell

Critical Thinking Education Outside the Intelligence Community

Critical thinking offers a framework for structured problem solving. Yet, despite a corpus of associated literature, critical thinking remains in its infancy as a discipline. It is still "largely misunderstood…existing more in stereotype than in substance, more in image than in reality."[143] As Bertrand Russell's humorous quip reminds us, critical thinking is not a habit acquired by just being alive.

Ideally, valuable skills and dispositions should be developed among prospective analysts before they join intelligence-producing corporations. Yet, observations by the author of newly hired intelligence analysts suggest this happens rarely if at all. This raises two questions, "What are the opportunities for prospective analysts to become critical thinkers before they are hired?" and often "Why do these opportunities not exist?"

Despite its importance, critical thinking is not widely taught in schools and universities. A mid-1990s California study on the role of critical thinking in the curricula of 38 public and 28 private universities concluded that the skill is "clearly an honorific phrase in the minds of most educators."[144] The study concluded that university

143 Richard W. Paul, "A Draft Statement of Principles," The National Council for Excellence in Critical Thinking, URL: <www.criticalthinking.org/ncect.html>, last accessed March 18, 2003. The reasons why critical thinking remains an undeveloped discipline while important, go beyond the scope of this essay and are not addressed.

144 Richard W. Paul, Linda Elder, and Ted Bartell, "Executive Summary,

faculty members "feel obliged to claim both familiarity with it and commitment to it in their teaching, despite the fact that…most have only a vague understanding of what it is and what is involved in bringing it successfully into instruction."[145] Indeed, the authors of the study found that while 89% of the faculty they interviewed "claimed critical thinking was the primary objective of their instruction," only 19% could define the term and only 9% were evidently using it on a daily basis in their instruction.[146] If the results of the California study are representative of the nation at large, they explain why prospective new hires – themselves college graduates – generally fail to exhibit skill in critical thinking at any level of proficiency.[147]

Informal conversations with recent hires at NSA support this premise. Although slightly fewer than half of these individuals indicate they have been exposed to critical thinking skills in college, most have been exposed only in one class and then only as an approach to learning the materials covered in that class. While not discouraged, respondents apparently were not encouraged to apply the skills to other subjects. Thus, a disposition to think critically is rarely fostered. Further, when asked to define critical thinking, most

Study of 38 Public Universities and 28 Private Universities To Determine Faculty Emphasis on Critical Thinking In Instruction," *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations,* California Commission on Teacher Credentialing, Sacramento California, 1997 (Dillon, CA: Foundation for Critical Thinking, 1997), URL: <criticalthinking.org/schoolstudy.htm>, last accessed March 18, 2003. Cited hereafter as Paul, Elder, and Bartell, *Executive Summary.*

145 Paul, Elder, and Bartell, *Executive Summary.*

146 Richard W. Paul, Linda Elder, and Ted Bartell, *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations California Commission on Teacher Credentialing,* Sacramento California, 1997 (Dillon, CA: Foundation for Critical Thinking, 1997), 18.

147 A recent but unscientific survey of several major eastern American universities' online catalogs shows the term "critical thinking" to be used widely in course descriptions. Further examination of some of those courses suggests that East Coast academics may share a similar lack of understanding about critical thinking. Although beyond the purview of this paper, it appears that there is sufficient evidence to warrant repeating the California survey on a national basis.

young analysts were unable to do so in any comprehensive fashion.[148] Finally, few employ any form of critical thinking in their analytic (or other) reasoning unless they have been trained to do so.

In fairness, it should be noted that critical thinking awareness, attitude, and skills varies from one academic discipline to another. For example, students of the physical sciences who employ the scientific method in a community setting probably have a greater inclination toward a basic form of critical thinking if only through osmosis.[149]

There are also some primary, secondary, and university education programs that have adopted a meta-cognitive critical thinking paradigm. Although the results of the impact of such programs are largely anecdotal, at least one study, conducted by Jennifer Reed as part of her dissertation found that students' critical thinking skills improved *after just one course.*[150] Faculty and administrators of these programs routinely attend the annual critical thinking conference sponsored by the Center for Critical Thinking where their results are shared. However, the approximately 500 people who attend this international event represent a small fraction of the educators in the United States.

The elements of scientific method – the formulation of hypotheses, collection of relevant data, testing and evaluation of hypotheses, and the logical derivation of conclusions – are matched step-by-step by

148 These conversations occur routinely as part of a training course the author teaches to newly hired intelligence and language analysts at NSA. When asked to complete the following statement, "In my opinion, critical thinking involves…" typical answers center on "thinking outside the box."

149 Francis J. Hughes, conversation with the author, Washington, DC: National Defense Intelligence College, 8 May 2003. Mr. Hughes is one of the few proponents and teachers of evidence-based inferential intelligence analysis, a means of analysis requiring critical thinking at every stage in the process.

150 Jennifer H. Reed, *Effect of a Model For Critical Thinking on Student Achievement In Primary Source Document Analysis And Interpretation, Argumentative Reasoning, Critical Thinking Dispositions, And History Content in a Community College History Course,* PhD Dissertation, College of Education, University of South Florida, December 1998, vii. URL: <http://www.criticalthinking.org/resources/JReed-Dissertation.pdf>, last accessed 6 May 2006.

critical thinking.[151] Given that most newly hired intelligence analysts – at least at NSA – are drawn from fields other than the physical sciences, one can expect that new hires lack adequate critical thinking skills. If NSA's newly hired intelligence analysts are representative of those being hired across the Intelligence Community then it is probable that few of the thousands of new hires arrive with adequate critical thinking skills.

Critical Thinking Education Inside the Intelligence Community

That analysts need to develop critical thinking skills is recognized within the Intelligence Community. Heuer wrote in 1999, "[Traditionally], analysts at all levels devote little attention to improving how they think."[152] As a direct response to Heuer's criticism, the CIA's Sherman Kent School includes critical thinking as part of the curricula for training new analysts, and recently initiated a class in critical thinking.[153] New employees are encouraged to develop a disposition to think critically as they are taught the skills of intelligence analysis.

A similar approach is employed in courses on structured analysis methods at the National Defense Intelligence College (NDIC). Critical thinking is claimed as a feature of many NDIC courses. However, the emphasis in most courses is on topical or issue-related material, and only incidentally on the process of thinking. At present, the skill itself is largely not taught. Instead, students are expected to figure

151 Steven D. Schafersman, "An Introduction to Critical Thinking," January 1991, URL: <www.freeinquiry.com/critical-thinking.html>, last accessed 9 March 2006.

152 Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: CIA Center for the Study of Intelligence, 1999), 173. Cited hereafter as Heuer, *Psychology*.

153 For a detailed account of how the faculty of the CIA's Sherman Kent School are working to improve their analysts' knowledge, skills, and abilities, see Stephen D. Marrin, "CIA's Kent School: Improving Training for New Analysts," *International Journal of Intelligence and Counter Intelligence* 16, no. 4 (Winter 2003–2004): 609–637.

it out on their own, encouraged by the thesis writing process. The college is aware of the importance of critical thinking and new core courses may include formal critical thinking instruction.

New NSA analysts are provided with an introduction to the solitary part of the skill (as discussed in figure 4) as part of their orientation. The agency's 40-hour follow-on program is the first Intelligence Community course to focus primarily on enhancing analysts' solitary and communal critical thinking skills. In addition to critical thinking skills, participants learn and apply, and then assess, the appropriateness of fourteen structured methods of analysis. The course has been taught to both U.S. and Allied personnel drawn from intelligence, counterintelligence, information assurance, and law enforcement communities.[154]

Training in critical thinking is offered to Defense Intelligence Agency (DIA) analysts using a variation of the NSA-developed course. Also, in 2005, DIA tested the "critical thinking skills" of a sample of its employees using the *Watson-Glaser Critical Thinking Appraisal*. The instrument claims to "measure abilities involved in critical thinking, including the abilities to define problems, select important information for the solution to problems, recognize stated and unstated assumption, formulate and select relevant and promising hypotheses, [and] draw valid conclusions and judge the validity of inferences."[155] The appraisal appears to confuse abilities with skills, although both do belong within the domain of analysis.[156] Finally, it appears that the test does not evaluate an individual's meta-cognitive skills in assessing and correcting the *process* of reasoning.

The increasing opportunities for enhancing critical thinking skills and dispositions reflect a recognition of the importance of critical

---

154 The syllabus from the course is in the Appendix.

155 Harcourt Assessment, Inc., *Local Norms Report, Watson-Glaser Critical Thinking Assessment*, Report prepared for the Defense Intelligence Agency, 2005, 2. Cited hereafter as Harcourt, *Watson–Glaser.*

156 Abilities and skills are easily differentiated. Individuals are born with certain abilities (and can improve them through training) but they *must* learn a skill. See for example, Moore and Krizan, "NSA."

thinking in intelligence analysis.[157] Evidence becomes intelligence through an "ordered thinking process [involving] careful judgments or judicious evaluations leading to defensible conclusions" – through critical thinking.[158] Former CIA analyst Morgan Jones asserts that methods for critical thinking and problem solving, if applied, can improve the quality of analysis and decisionmaking.[159]

Implications of Teaching Critical Thinking

Although Sherman Kent, Richards J. Heuer, Jr., and others have over the years addressed intelligence analysis and its relationship with critical thinking, recent presidential executive orders and legislative mandates are bringing a new emphasis to how the Intelligence Community can change analytic practices to achieve improved outcomes. Teaching analysts to be better critical thinkers may be seen as an easy way to satisfy these requirements. However, linkages between intelligence analysis and critical thinking remain poorly understood. Considerable confusion remains about what constitutes critical thinking and how it supports intelligence analysis.

A common excuse among analysts to defend their "non-use of such self-conscious processes is a lack of time."[160] Teaching critical thinking skills is of little value if analysts are not inclined to use them.[161] For those who are willing to think critically, various

157 The Director of National Intelligence, John D. Negroponte, in the Foreword of the initial *National Intelligence Strategy of the United States of America* (Washington, DC: Office of the DNI, October 2005), wrote that one of the three principal tasks for the reformed Intelligence Community is to "bring more depth and accuracy to intelligence analysis." See http://www.dni.gov/NISOctober2005.pdf.

158 Moore and Krizan, "Intelligence Analysis," 14.

159 Morgan D. Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving* (New York, NY: Random House, Inc, 1995), xi. Cited hereafter as Jones, *Thinker's Toolkit.*

160 Stephen Marrin, email to the author, December 8, 2003. The author has heard similar complaints from analysts at NSA and DIA.

161 Linda Elder, Alec Fisher, Diane Halpern, Gerald Nosich, Richard Paul, and others develop and publish the materials for – as well as teach – such courses.

instructional models offer complementary means of expanding and enhancing analysts' skills. For example, in an area studies class on Russia, students might be asked to evaluate and comment in depth on what different sources say about the influence of organized crime on the national government. Alternatively, critical thinking can be injected into the course as part of a problem-solving curriculum. Here students focus on *how* they think as they apply different strategies to each assignment, and then, ideally, transfer those enhanced skills to their day-to-day analysis. The use of realistic case studies makes classroom-acquired knowledge actionable. Self-reflective and group-reflective analyses of the process of reasoning keep the classes focused toward the working environment of analysts.

Such transformations involve behavior modification and as such take time. Participants engaged in such instruction cannot be expected to become critical thinkers in a one-day or even a week-long course. The instructors of the NSA course attempt over a period of 10 weeks to transform their students into critical thinkers. Some other Community efforts also provide instruction over an extended period. Even so, students leaving the course are still novices in this practice and can slip back to their old methods of reasoning. Becoming critical thinkers requires a change in behavior that extends long past the end of the formal instruction. There is no substitute for continued practice.

Finally, it serves critically thinking analysts poorly if their management and corporations are indisposed toward the application of the skills. It is well known that "engendering the desire to use [critical thinking] as a favored means of problem solving and decision making prepares the ground for teaching and learning the [critical thinking] skills."[162] Such encouragement can occur in the classroom but its effectiveness is limited unless the corporation encourages and welcomes strategies to employ critical thinking in the workplace.

However, there are few metrics for determining the effectiveness of these materials and courses and so their value remains undetermined. The fact that the books developed for, and used in, such courses remain in print (in successive editions) is an indicator that at least this approach is popular, if not effective.

162 Facione, "Disposition."

The best place for such encouragement is from senior and midlevel management. In order for this to occur, they too must be educated in the methods of, and reasons for, critical thinking.

Evaluating Teaching Models

Removing analysts from their work for education and training disrupts their primary mission of intelligence production. Spreading instruction over time provides a reasonable answer to this dilemma. Since improving critical thinking requires a high level of experiential, hands-on practice, an extended course offers students time to practice and apply what they are learning. This is the model used for the NSA course on critical thinking. Feedback from students indicates that once-a-week instruction works best. Mission is minimally disrupted and there is time to study and practice what is being taught. However, the long duration limits students' work-related travel and leave.

Experiential learning also requires that such classes be relatively small and that instructors be proficient. Without a large teaching staff, training a large workforce takes years. Since senior managers – and their strategic visions – change often, a long-term corporate commitment is crucial to success.[163]

Such a long-term commitment exists at the Sherman Kent School for Intelligence Analysis. The school itself grew out of a month-long course on analytic tradecraft developed by former Deputy Director for Intelligence Douglas J. MacEachin.[164] Beginning in 1996, the course was delivered to the entire analytic workforce. The school itself was established in 2000 and continues to evolve as both a training center and a center of best analytic practices.[165]

---

163 Alternately, a large staff can be created, trained, and assigned to teach an entire workforce. This was accomplished in a knowledge domain at NSA in the 1990s. If inducements and cultural change accompanied such a program, this approach might present certain advantages even if its costs are high. An analytic workforce could be transformed rapidly through such a "boot camp" approach.

164 Marrin, "Kent School," 615.

165 Marrin, "Kent School," 609.

Another means of critical thinking instruction is to create an interactive, computer-based or web-based course. This has the benefit of allowing as many analysts to attend as wish to do so. One or two instructors working full-time can answer students' questions. Exercises allow student self-assessment. However, this is presently an unsatisfactory model for critical thinking instruction. Learning to think critically requires Socratic interaction and the impersonal nature of web-based instruction discourages the practice even for the population of dedicated solitary learners. In the future, multi-player simulations and other games could be used to reinforce the lessons learned. However, these are not yet available.

Although computer- and web-based instruction can be accomplished at the analyst's desk, there are other reasons why this may not be a good idea. Analysts who remain in their offices are subject to interruptions. Further, course work is often relegated to the end of the workday, when analysts are tired and learning is impaired. Little learning occurs when taking a class is a chore. The current limitations of both classroom and computer- or web-based education suggest that experimentation with new means of instruction for critical thinking is needed.

Encouraging Analysts to Think Critically

Incorporating critical thinking into both orientation and basic analyst education and training is one way to help newly hired analysts develop their skills. Subsequently placing those analysts in offices where critical thinking is practiced is another way to encourage an analytic culture that fosters thinking critically. Through direct exposure to successful, experienced analysts, junior analysts' doubts about the employment of critical thinking techniques can be overcome.

"Skills pay" can be an inducement for analysts to learn and then employ critical thinking. Rewarding the acquisition, maintenance, and use of other special skills is common in government and industry. For example, linguists at NSA earn significant bonuses for achieving specific levels of foreign-language proficiency – an effective way

to maintain critical language competencies within one intelligence agency's workforce. Given the high-level concern for the health of the intelligence analysis process, direct monetary incentives should be available for analysts to master new tools and demonstrate constructive analytical behaviors.

On the other hand, if an intelligence enterprise fails to recognize and reward the acquisition and application of analytic skills such as critical thinking, it sends a very clear message: the enterprise does not value those skills. Faced with such a message and a lack of inducements to excel, the best and brightest analysts may leave, especially from the more junior ranks – and midlevel employees with families and mortgages may "retire in place." Either outcome hurts mission-critical functions, and can be avoided. As a previous Director of NSA, Air Force Lieutenant General Kenneth A. Minihan, noted, "If we don't win the talent war, it doesn't matter what we invest in the infrastructure."[166] Recognizing and rewarding critical thinkers is one way to win that talent war – with the assumption that really good analysts are more likely to remain active within their intelligence agency workforces.

If an analyst adopts a congeries of skills that contributes to the mastery of critical thinking, and is compensated monetarily, that mastery needs to be certified. If a curriculum that drives the acquisition of those skills is in place, then an assessment of those skills can be administered in-house. Specific tests exist for the assessment of critical thinking, such as the "Thinking Skills Assessment Test."[167]

Persuading to Improve Analysis

Teaching critical thinking is but a first step toward improving analysis. Because analysts and managers have different needs and

166 LtGen Kenneth A. Minihan, USAF, Director, NSA, in Robert K. Ackerman, "Security Agency Transitions from Backer to Participant," *Signal* 53, no. 2 (October 1998), 23.

167 For more information, see http://tsa.ucles.org.uk/index.html, last accessed 15 March 2006.

time constraints, multiple versions of a course are needed to meet the needs of each group. Analysts and first-line supervisors may take an entire course, midlevel managers an abbreviated course, and senior managers an overview. This strategy already is employed at the CIA's Sherman Kent School where new employees spend 13 weeks learning analysis skills, techniques, and methods while supervisors, depending on their seniority, spend three days or one day becoming familiar with these same skills and methods. The analysts also have opportunities to apply new skills immediately as they perform four-week "internships" in various CIA offices.

Other CIA analysts, already in place, do not have the same opportunities to receive this training. Thus a two-tiered analyst population with more skilled junior analysts and more knowledgeable senior analysts is being created. Ideally, each will transfer skills and knowledge to the others. However, an alternate possibility is that it will generate distrust and animosity between the two groups. Older, more experienced analysts may resent the opportunities given to their newer counterparts. This issue is not trivial. Offering the wrong curriculum to the wrong groups of analysts and managers can destroy its effectiveness. Managers in the CIA and elsewhere can influence how the new analytic methods being taught will be adopted, as agencies respond to new legislative and executive mandates.

Will analysts embrace critical thinking as a means to improve their analysis? There are numerous observations of analysts' reluctance to adopt new paradigms.[168] This is true even when analysts are confronted with the fact that their conclusions were wrong. In referring to her work on the issue of Iraqi WMD, one CIA analyst told Senate investigators, "their 'bottom line' judgments would have remained the same."[169] Rob Johnston also found a similar reluctance to change opinions among the analysts he studied. He noted that

168 Stephen Marrin, "Homeland Security and the Analysis of Foreign Intelligence," Markle Foundation Task Force on National Security in the Information Age, 15 July 2002, URL: <www.markletaskforce.org /documents/ marrin_071502.pdf>, last accessed December 9, 2003, 9. Cited hereafter as Marrin, "Homeland Security."

169 SSCI, *Iraq,* 299.

although "analysts can change an opinion based on new information or by revisiting old information with a new hypothesis," they perceive a loss of trust and respect and a subsequent loss of "social capital, or power, within [their] group."[170]

Yet, a case can be made that analysts, and especially experienced analysts, will benefit the most from enhanced critical thinking skills training. These are the analysts who are in positions of technical leadership, who work the most difficult aspects of complex targets. There may be significant consequences if they fail to notice and make sense of an issue. On the other hand, the fact that many of these senior personnel will soon be eligible for retirement raises an important question: Does the corporation get added value from teaching analysts who will soon retire to think more critically in their analysis if they are predisposed not to do so? Maybe so. Heuer, while the head of CIA's Methods and Forecasting Division found that analysts, once persuaded to use new analytic methods, found them "interesting and well worth doing."[171]

Other intelligence analysts have adopted new analytic methods that add value to their analyses. In one example, NSA personnel involved in research and development adopted a means of matching target characteristics and their vulnerabilities with exploitation capabilities and their costs.[172] Such analyses helped ensure that appropriate resources were dedicated to collection and that such collection was better tailored to production analysts' needs. However, some research analysts initially refused to employ the model, claiming it took too much time even as it reduced the volumes of information

---

170 Johnston, *Analytic Culture,* 22.

171 Richards J. Heuer, Jr., *Adapting Academic Methods and Models to Governmental Needs: The CIA Experience* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 31 July 1978), 5. Referenced in Marrin, "Homeland Security," 9.

172 In this context, a "target" refers to an entity – geographical, individual, or topical – in which the Intelligence Community has an interest.

they were required to examine.[173] Adoption of the analytic paradigm required appropriate persuasion.

One interesting means of self-persuasion may be analysts' frustration with the really hard problem. This frustration may lead analysts to try something new.[174] Such frustration occurs more often among experienced analysts. Years of attempting to make sense of overwhelming masses of information with inadequate analytic paradigms and technologies leaves some experienced analysts willing to grasp at anything that will improve how they work. On the other hand, newly hired analysts who have not yet experienced the frustration of inadequate paradigms for analysis may be resistant to adopting rigorous analytic paradigms such as that afforded by critical thinking.[175]

173 Multiple midlevel NSA analysts, interviews with the author, 1998–2005.

174 LT Robert D. Folker, USAF, email to the author, 9 December 2003. Cited hereafter as Folker, email, 9 December 2003.

175 Folker, email, 9 December 2003.

Transforming Intelligence Corporations

In order for an institution to change, all affected personnel, from the lowest to the highest, must first recognize that change is needed and is advantageous – both corporately and personally. As retired World Bank executive Stephen Denning argues, this is difficult to accomplish. Logically sound arguments do not sway employees. Instead, employees remain convinced that what they are doing is satisfactory.[176] Further, outsiders who attempt to induce change face opposition because employees presume that external consultants are arrogant in suggesting that things are not right, and that change is needed.

One way to effect change is through a "springboard story." This approach contrasts with past conventional – and largely unsuccessful – transformation efforts that relied on fixing the systems involved and were characterized by an overabundance of buzzwords:

> Enhance quality. Streamline procedures. Reform and flatten the organizational structure. Analyze things in terms of grids and charts. Develop plans in which individuals are programmed to operate like so many obedient computers. Hone our interpersonal mechanics and build skill inventories. Bring to our difficulties a fix-it attitude, as though our past errors can be easily corrected with straightforward explanations.[177]

---

176 For a discussion of Denning's philosophy about change, see Jeff de Cagna, "Making Change Happen: Steve Denning Tells the Story of Storytelling," Information Outlook, January 2001, 28–35, and Stephen Denning, *The Springboard: How Storytelling Ignites Action in Knowledge-Era Organizations* (Boston, MA: Butterworth-Heinemann, 2001). Cited hereafter as Denning, Springboard.

177 Denning, *Springboard,* xvii. In 23 years of Intelligence Community work, the author heard all of these phrases as slogans for various programs designed to "fix" analysis or the corporations involved. These associated corporate efforts to bring these goals about often had the opposite effect. In the process of "flattening

As Denning points out, these strategies fail to account for the messy and chaotic reality in which real organizations live and work, especially intelligence agencies which have the charter to engage honestly with "the other," or mission-related targets, outside of the bureaucracy in which they serve.[178]

The springboard story helps employees at all levels envision what is needed for the proposed transformation. Denning asserts that it "invites them to see analogies from their own backgrounds, their own contexts, their own fields of expertise."[179] He cautions that transformational stories are not a panacea – there are situations and circumstances in which they are not effective, such as when the change being proposed is a bad idea.[180] The key is finding the appropriate stories within the corporate culture.

One way to find these stories is to examine the best practices of intelligence analysis successes where critical thinking played a role. Just recounting a success is not enough. Listeners need to be able to identify and empathize with the scenario and its actors. The effective story is "about people who have lived [a] knowledge-sharing idea and how things happen in a real-life situation."[181] For example, conducting a trial or experiment on critical thinking within the intelligence analysis process, if it leads to certifiable, actionable success, *does* effectively persuade.

Learning from Early Adopters

Once a sustained number of early adopters openly apply systematic, critical thinking to hard analytic problems, the stage is set for a "tipping point" in the spread of structured methods across

---

the organization" at one intelligence agency, more hierarchical managerial layers were actually created!

178 Denning, *Springboard,* xvii.

179 Denning, *Springboard,* xix.

180 Denning, *Springboard,* xxi.

181 Denning, *Springboard,* 51.

analytic populations.[182] Stanley Feder recounts how a tipping point began to apply to a political analysis method at the CIA in the 1970s and 1980s. The method involved two estimative tools known as Factions and Policon that were used by the "Intelligence Directorate and the National Intelligence Council's Analysis Group to analyze scores of policy and instability issues in over 30 countries."[183] The reasons for the adoption of these tools remain the same: "Forecasts and analyses…have proved to be significantly more precise and detailed than traditional analyses."[184] Writing about the method in 1987, Feder predicted that its use would continue to expand.[185] The method is still in use 19 years after Feder's article was published. However, expanded use failed – perhaps because the tool was on a computer platform that ceased to be supported by the Agency. The recent transfer of the tool to a new suite of programs corresponds with observations that its use is once again expanding.[186]

Non-intelligence-related transformational stories can be applied in the Intelligence Community to facilitate the spread of new ways

182 Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Boston, MA: Little Brown and Company, 2000), 15–29. Gladwell shows how "social epidemics" can infect a variety of domains.

183 Stanley Feder, "Factions and Policon: New Ways to Analyze Politics," in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955–1992* (New Haven, CT: Yale University Press, 1995), 275. Cited hereafter as Feder, "Factions and Policon."

184 Feder, "Factions and Policon," 292.

185 Feder, "Factions and Policon," 292. Feder was wrong about its sustained popular growth.

186 This story is not an isolated instance. In the author's experience, initial implementation and popularization are often followed by a gradually reduced user-base. Certain organizations find the tools useful and they tend to continue to use them even though any underlying technology may be obsolete. In the case of Factions and Policon, the tools were maintained on an aged Macintosh computer. They were updated in 2006 as part of the work of an intelligence research firm in New Mexico. The Factions tool was rewritten and included in Landscape Decision®, a suite of modeling and simulation tools developed under a research contract with the Department of Defense's Advanced Research and Development Activity (ARDA). The updated technology was reinserted into the tasking organization. Other technology transfers are pending.

of thinking. For example, two video commercial advertisements from the Electronic Data System (EDS) company resonate with the challenge of rebuilding intelligence analysis in the face of skeptics, and what it takes to be an intelligence analyst.[187] The two related commercials depict farcical situations based on two well-known clichés: "You've got to build it before you can fly it!" and "It's like herding cats; it can't be done!" In the former, a group of mechanics is building an airplane in mid-flight; while in the other, a group of cowboys has accomplished the impossible – they are herding cats across the Great Plains. EDS' depiction of its revolutionary design capabilities bears a message about corporate rebuilding and individual transformation. The message encourages managers and analysts to compare themselves and their situation to the people tasked with building an airplane at "60,000 feet," or with herding cats across a river.

Intelligence analysts and managers who have seen the videos have had little trouble drawing analogies with the corporate and personal transformations needed in the Intelligence Community. That the situations are humorous only adds to a viewer's buy-in – they are "hooked" before they realize it. Developing other stories that specifically apply to corporate transformation within the Intelligence Community and its various elements is a logical next step in encouraging analysts and managers to use and support critical thinking in analysis. If these stories can be drawn from recent analytic successes, their value can only increase.

The Costs and Benefits of Thinking Critically

Are intelligence failures inevitable if analysts lack critical thinking skills? Yes. However, critical thinking is not a panacea. Intelligence failures still can be expected. If no measure "will guarantee that accurate conclusions will be drawn from the incomplete and ambiguous information that intelligence analysts

187 See *Building Airplanes in Flight*, television advertisement produced for EDS by Fallon-McElligott, November 2000, videocassette; and *Herding Cats,* television advertisement produced for EDS by Fallon-McElligott, January 2000, videocassette.

typically work with…[and] occasional failures must be expected," why should the Intelligence Community invest in teaching its analytic workforce to think critically?[188] A brief review of the causes of failure clarifies the need for such an investment.

Intelligence failures occur in both systematic and functional domains. Systematic intelligence failures occur when producers fail to notice phenomena and the consumers of intelligence fail to heed warnings or even to notice that they are being warned. It may be that both consumers and producers are focused on other issues at the time. Alternatively, intelligence-based warning is not taken seriously at high official levels. In cases where collaboration among intelligence agencies might be critical, key evidence may not be recognized and shared.

All of these failings are illustrated in the "intelligence failure" to warn of the attacks of 11 September 2001 on the World Trade Center in New York and the Pentagon near Washington, DC. In the first place, the policy issue that was at the forefront – according to press at the time – was a national missile defense system, not the likelihood of a terrorist attack on the United States. Richard Clarke, the Clinton and then Bush administrations' terrorism "czar" observes that Bush administration officials were slow to recognize or consider the threats posed by Osama bin Laden.[189] Evidence passed by an FBI field agent about students learning to fly large aircraft with little regard for landing or takeoffs was not taken seriously at higher levels within the Bureau.[190] The Joint Congressional investigation into the attacks noted in its report that collaboration was lacking between agencies, especially between the law enforcement and strategic

188 Heuer, *Psychology,* 184.

189 "Clarke: Bush Didn't see Terrorism as 'Urgent,'" *CNN.com,* 19 May 2004, URL: <http://www.cnn.com /2004/ALLPOLITICS/03/24/911.commission/index.htm>, last accessed 9 March 2006.

190 Michael Elliott, "How the U.S. Missed the Clues," *CNN.com,* 20 May 2002, URL: < http://archives.cnn.com/2002/ALLPOLITICS/05/20/time.clues/index.html>, last accessed 9 March 2006.

intelligence agencies.[191] This was both a cultural and a physical phenomenon. Airport security breaches during the summer of 2001 may have been related, but based on assessments of the catastrophe, were not connected to the events.[192]

The same kinds of failings were identified by the Senate Select Committee on Intelligence in its assessment of the National Intelligence Estimate on Iraqi WMD. As has already been observed, analysts and their managers were focused on the results and not the process.[193]

Critical thinking can mitigate some common causes of failure and provide means by which they can be avoided in the future. Specifically, an intelligence process based on critical thinking offsets the following failures:

Analysts are Wrong. It is unrealistic to expect that analysts can always be correct. Regardless of the processes they employ, analysts make errors and fail. Anthropologist Rob Johnston defines *errors* as "factual inaccuracies in analysis resulting from poor or missing data." Conversely, intelligence *failures* are "systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses."[194] Critical thinking mitigates these by providing means to assess errors in reasoning as they occur and before they become

191 U.S. Congress, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001,* Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee On Intelligence, Together with Additional Views, Senate Report No. 107–351/House Report. No. 107–792, 107th Congress, 2nd Session, December 2002, xvi.

192 The author recalls that media reports of persons hopping over or otherwise improperly passing airport security checkpoints in and around Boston, New York, and Washington seemed to be higher than usual during the summer of 2001.

193 DNI Negroponte, in the *National Intelligence Strategy of the United States* (October 2005, 2) highlights the notion that the Community appropriately undertakes study of its internal processes, as well as of the quality of its products, by addressing both "enterprise" objectives as well as "mission" objectives.

194 Johnston, *Analytic Culture,* 6.

systemic failures. Such a meta-cognitive approach to the analytic process helps keep it under active review at the highest levels.

Policymakers Ignore Intelligence.[195] A critically thinking analytic population cannot directly affect what a policymaker can or will do – neither in fact, can a *non-critically thinking* analytic population. What critically thinking analysts can do, however, is present more effective assessments, perhaps leading policymakers to question their own assumptions on the issues. Additionally, thinking critically about how analysts interact with policymakers can identify ways to restructure the analysis dissemination process to involve policymakers more effectively. Such a process might also encourage them to adopt some of the attributes of critical thinking leading to (it may be presumed) more effective policy.[196]

Adversary Denies and Deceives. Critical thinking reduces the effects of adversarial denial and deception by leading analysts to consider alternative possibilities, to question biases and assumptions, to examine systematically the validity of evidence being considered, and to take seriously anomalies in the evidence.

Adversary is More Capable. In any adversarial system, there are winners and there are losers. While analysts can do everything possible to ensure their work is correct, they rarely work with all the evidence, and indeed may still be deceived. In such cases, they may come to wrong conclusions. Critical

---

195 There is a "classic" argument as to whether this is or is not an "intelligence" failure. In summary, the two sides condense as follows: On the one hand, intelligence should have been so persuasively presented as to compel the policymaker to pay attention. On the other hand, intelligence should not be telling the policymaker what to do. The argument goes all the way to the roots of the post-World War II strategic intelligence system currently in place. Former CIA analyst Jack Davis summarizes the issue in "The Kent-Kendall Debate of 1949," *Studies in Intelligence* 35, no. 2 (Summer 1991): 37–50.

196 Cooper, email to the author, 31 March 2006. Cited hereafter as Cooper, email, 31 March 2006.

> thinking, however, by providing structure and oversight to their reasoning, provides an audit trail. In this case, the means by which the analytic conclusions were reached can be subsequently reviewed, errors and deceptions revealed, and steps taken to improve the process so that the failure is not repeated**.** Indeed, because of its focus on the process, critical thinking becomes a powerful tool for evaluating and enhancing analytical reasoning.

Investment in critical thinking as part of the analysis process minimizes the likelihood of specific failures. With critical thinking essential to so many parts of the intelligence production process, enhancing it increases the likelihood of intelligence success.[197] With the cost of failure catastrophically high, the Intelligence Community is well advised to improve the likelihood of intelligence success, including improving critical thinking. As diplomat Richard Holbrooke opined in 2003, "intelligence is…indispensable. And its greatest successes are preventative."[198]

There are other reasons why systemic intelligence failures occur. Jeffrey Cooper considers ten pathologies, summarized in table 6, that impede successful analysis at both the individual and corporate levels. Cooper specifically believes that given the

> [emphasis] on the systemic nature of the pathologies that afflict intelligence analysis, structured analytic methods

---

197 One metric for intelligence is decreasing intelligence failures. In this case, fewer failures could be considered as "improving intelligence." But the reasons for the prevention of the failures need to be considered. The reduced number of failures could be due to a critically thinking workforce. Or it could be due to coincidences. Although a pointed discussion of metrics for intelligence is beyond the scope of this paper, recent articles explore the issue of intelligence metrics. See, for example, David T. Moore, Lisa Krizan, and Elizabeth J. Moore, "Evaluating Intelligence: A Competency-Based Model," *International Journal of Intelligence and Counterintelligence* 18, no. 2 (Summer 2005): 204–220.

198 Richard Holbrooke, in Judith Miller, "A Battle of Words Over War Intelligence," *New York Times,* online edition, 22 November 2003, URL: <www.nytimes.com/2003/11/22/arts/22INTE.html>, last accessed November 28, 2003.

Cooper's Analytic Pathology	Description
Inefficient "Account" Structure	Work is subdivided into accounts with ownership; provides basis for accountability; ownership inhibits sharing, cooperation, and collaboration; encourages "stovepiping" in collection disciplines.
Evidence-Based Scientism	Descriptive and explanatory intelligence support current policy and military operations; less support for anticipatory intelligence; analysis needs to be "augmented and leavened with intuition, curiosity, and a thirst for discovery – all essential elements of good science."
Tyranny of Current Intelligence	Response to customers' current concerns; support to current, ongoing military operations; little long-term research.
Over-Emphasis on Production	Databases need filling; scheduled reports and assessments must be produced on time; metrics for success measure data collected and processed; number of reports issued used to determine and justify resources allocated.
Over-Reliance on Previous Judgments	Previous reports presumed to be authoritative; previous reports combined to form new judgments; agreed-upon positions retained despite newer contradictory evidence.

Table 6: Cooper's Analytic Pathologies

Source: Summarized from Cooper, *Pathologies*, 30–39.

> become a first line of defense in preventing the networks of errors from developing – they are like "ripstops" that keep problems from propagating into wider "error-inducing systems," in [Charles] Perrow's terms.[199]

199 Jeffrey Cooper, email to the author, 31 March 2006. Cooper refers to Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton, NJ: Princeton University Press, 1999).

Cooper's Analytic Pathology	Description
Neglect of Research	Short–term taskings prevent longer–term research; reward structure favors current reporting, not longer term work; stunts development of deep target expertise.
Neglect of Anticipatory Intelligence	"Information Revolution" leaves intelligence competing with journalism and Internet for policymakers' attention; lack of predictive intelligence against new emerging threats ensures continuing failures to warn.
Loss of "Keystone Species" and "Intellectual Middleware"	Periodic reductions in force skew analyst demographics; "Keystone Species" (journeymen analysts) lacking; journeymen do bulk of professional maintenance; essential for knowledge retention and transfer to apprentices; maintain "intellectual Middleware" or deep understanding of analytic domains and processes.
Lack of Analytic Tools and Methods of Validation	Available and proposed tools not formally validated for accuracy and usefulness; focus on results, not processes, to determine success.
Hindrances of Security Mindset	Security procedures impede multi–source analysis; protection of sources and methods more important than "effective exploitation and cross–fertilization;" artificial and outdated mission distinctions prevent collaboration.

Critical thinking combats this by enhancing the processes by which decisions are made and by which such processes are reviewed. This paper focuses primarily on *individual experience*, and of course, intelligence corporations are made up of individuals. If a sufficient number of intelligence professionals are thinking critically, it is likely they will transform their corporations, if only through the sheer attrition of non-critically thinking managers and leaders who are

retiring from the work force. It should be observed that an Intelligence Community enterprise-wide emphasis on developing critical thinking skills at all levels would speed the process.

Validation

A critically thinking Intelligence Community remains essential for effective intelligence reform. Steven Rieber and Neil Thomason advance this argument in their recent article. The authors assert that "the opinions of experts regarding which methods [of analysis] work may be misleading or seriously wrong."[200] Unfortunately, as the authors show, past (and present) efforts at intelligence reform rely on expert intuitive judgments. However, "[examples] from a wide range of fields show that expert opinion about which methods work are often [not only] dead wrong…but also are generally not self-correcting."[201] Further support of Rieber's thesis is seen in devil's advocacy – not as theoretically applicable but as practiced. They cite Irving Janis who, quoting a Stanford political scientist, notes that "instead of stirring up much-needed turbulence among the members of a policymaking group, [devil's advocacy] may create 'the comforting feeling that they have considered all sides of the issue.'"[202]

To mitigate this and similar analysis-improvement fallacies, Rieber and Thomason argue that improvements in analysis and any proposed methods of judgment and decision-making require validation through scientific study. They note, for example, that research reveals "[a] certain cognitive style, marked by an open-mindedness and skepticism toward grand theories, is associated with

---

200 Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 71.

201 Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 72.

202 Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, 2nd edition. (Boston, MA: Houghton Mifflin and Company, 1982), 268. Referenced in Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 73.

substantially better judgments about international affairs."[203] As the present paper has argued, such attitudes are found in critical thinkers. Scientific study of this and other methods will determine when and how they are appropriate. Critical thinking also supports Rieber and Thomason's call for a "National Institute for Analytic Methods" by providing an overarching structure to champion open-mindedness and skepticism in the study of which methods are appropriate for intelligence analysis. Only then, they argue, will real intelligence reform and improvement occur.

Rieber and Thomason's proposed institute could determine which strategies are most effective at disposing analysts and their corporations to employ critical thinking. Research evidence indicates that simply teaching critical thinking (or for that matter, structured analytic) skills is insufficient. People will not adopt the strategies unless motivated to do so. As noted here, springboard stories are one means of implanting a positive disposition toward critical thinking. Other means certainly also exist. A desirable objective of research in the proposed National Institute for Analytic Methods would be to discover and assess what might motivate analysts most effectively toward thinking critically.

203 Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 74.

What Other Points of View Exist?

A recent best-selling book advances the comfortable idea that conscious reasoning may not confer advantage to the reasoner.[204] Recent research suggests that whereas simple choices may benefit from conscious thought, complex issues are best left to unconscious thought, or "deliberation-without-attention."[205] The explanation of this finding is that in conscious thinking, people face a severe limit on the number of factors that they can effectively consider simultaneously and, second, that in conscious thought people "inflate the importance of some attributes at the expense of others."[206] The authors base this finding on four experiments with subjects who were asked to indicate their preference for various consumer items. The experiments involved differing levels of complexity in terms of factors to be taken into consideration. They ultimately suggest that:

> [there] is no *a priori* reason to assume that the deliberation-without-attention effect does not generalize to other types of choices – political, managerial or otherwise. In such cases, it should benefit the individual to think consciously about simple matters and to delegate thinking about more complex matters to the unconscious.[207]

It appears true that the human capacity to weigh evidence *consciously* is limited to approximately seven factors.[208] But this seven-

---

204 Malcolm Gladwell, *Blink: The Power of Thinking Without Thinking* (New York, NY: Little Brown and Company, 2005). Gladwell argues that thinking does not require detailed assessment of information. Instead, rapid cognitive responses are adequate for decisionmaking.

205 Ap Dijksterhuis, Martin W. Bos, Loran F. Nordgren, and Rick B. von Baren, "On Making the Right Choice: The Deliberation-Without-Attention Effect," *Science* 311, no. 5763 (17 February 2006), 1005. Cited hereafter as Dijksterhuis, "Deliberation-Without-Attention."

206 Dijksterhuis, "Deliberation-Without-Attention," 1005.

207 Dijksterhuis, "Deliberation-Without-Attention," 1005.

208 George A. Miller. "The Magical Number Seven, Plus or Minus Two," *The Psychological Review* 63 (1956), 87. The paper is available online: URL: < http://psychclassics.yorku.ca/Miller/>, last accessed 14 March 2006.

item limit is easily extended: people can hierarchically consider multiple sets of seven items.[209] Employing structured methods of reasoning also extends this capacity. In this context, critical thinking is at once both a structuring method and a means of assessing and monitoring the processes of selecting and using other structured methods. Additionally, "deliberation-without-attention" as applied to consumer choices in the study noted above was measuring *preferences.* Preferences change from person to person – different people conclude differently about oven mitts and cars – as the variety of these products on the market, in kitchens, or on the roads makes clear.[210]

Intelligence analysis is not about preferences; it is about best answers in ambiguous situations with high-stakes implications and consequences. As recent intelligence failures make clear, without forced consideration of alternatives, results are biased. Structured reasoning methods such as Analysis of Competing Hypotheses (ACH) develop these alternatives, allow for multiple factors to be considered fairly, and extend analyst capacities to assess complex situations as accurately as possible.

Intuition is what both Dijksterhuis and Gladwell consider in their respective works. However, exactly *what is intuition?* Rather than just appearing from nowhere, intuition is "almost always informed by experience and hard knowledge won by reasoning things out."[211] As Michael LeGault notes,

> good decisions [are] a nuanced and interwoven mental process involving bits of emotion, observation, intuition, and critical thinking....The essential background to all this is a solid base of knowledge...The broader the base, the more likely all the parts will fit together.[212]

---

209 William Reynolds, conversation with the author, 14 March 2006.

210 Oven mitts and cars are two of the categories for which Dijksterhuis and his colleagues tested.

211 LeGault, *Think*, 12.

212 LeGault, *Think*, 12.

Uninformed "intuitive thinking" contributes to intelligence failures because it fails to reflect on presuppositions. Such unexamined biases and mindsets contributed to the Cuban missile intelligence failure described above. Heuer's outline of the specific biases and mindsets that impede effective analysis is reinforced by the findings of others.[213] For example, Merom, writing about the Cuban crisis, concludes that intelligence failures occur due to a "lack of commitment to fundamental principles of investigation and analysis."[214] Although intuition or "thin slicing" may be appropriate in some domains, in intelligence analysis it appears to be associated with cognitive impediments that cause costly intelligence failures.[215]

However, as Rieber and Thomason note, testing needs to be conducted to determine which methods do work best in which situations in intelligence analysis.[216] Their work ought to go further, developing and modifying methods to overcome the very limitations they identify. For example, investigators have found that ACH suffers from confirmation bias.[217] The present author notes that this may be because non-confirmatory reasoning is so difficult for people to do.[218]

---

213 See for example, Scott Plous, *The Psychology of Judgment and Decision-making* (New York, NY: McGraw Hill, Inc., 1993); Thomas Gilovich, Dale Griffin, and Daniel Kahneman, Eds. *Heuristics and Biases: The Psychology of Intuitive Judgment* (Cambridge, UK: Cambridge University Press, 2002); and Daniel Kahneman, Paul Slovic, and Amos Tversky, eds. *Judgment under Uncertainty: Heuristics and Biases* (Cambridge, UK: Cambridge University Press, 1982).

214 Merom, "Estimate," 49.

215 Gladwell introduces the notion of "thin slicing" as a reasoning strategy in *Blink*.

216 Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 76.

217 Brant A. Cheikes, Mark J. Brown, Paul E. Lehner, and Leonard Adelman, *Confirmation Bias in Complex Analyses,* Mitre Technical Report MTR 04B0000017 (Bedford, MA: Center for Integrated Intelligence Systems, October 2004).

218 The author teaches Analysis of Competing Hypotheses to both new and experienced analysts at the National Security Agency. He notes that holding a non-confirmatory attitude – which ACH, as developed by Heuer, requires – is

Finally, it may be a fallacy that conscious and unconscious reasoning are truly separate. Instead, Morgan Jones (citing work by Richard Restak) asserts that "the unconscious has a governing role in much that we consciously think and do."[219] This means that analysts commit a variety of "analytic sins," including focusing on the initially favored solution – which is also often the first satisfactory solution considered.[220] Part of the problem seems to arise from confusion about "'discussing/thinking hard' about a problem and 'analyzing' it, when the two activities are not at all the same."[221] Ultimately, the unconscious or instinctive approach to reasoning seems to "remain closed to alternatives."[222] This is an unsatisfactory model for intelligence analysis where alternatives *must* be considered.

---

extremely difficult for people to do. Since the method has value, a means of mitigating this difficulty is worth developing.

219 Jones, *Thinker's Toolkit*, 10. Jones bases his assertions and argument on the work of Richard Restak, *The Brain has a Mind of Its Own* (New York, NY: Harmony Books, 1991).

220 Jones, *Thinker's Toolkit*, 11.

221 Jones, *Thinker's Toolkit*, 11.

222 Jones, *Thinker's Toolkit*, 12.

What Does the Future Hold?

Looking ahead, new paradigms for analysis become necessary in light of the many changes occurring across the globe. Rapidly emerging twenty-first century issues and challenges stress both infrastructures and sensemaking enterprises. The changes needed to maintain an edge against adversaries becomes clear as one considers what it is that analysts do, and how and when, as table 7 illustrates.

Gregory Treverton's observations about the evolution of intelligence sensemaking and the organizations that comprise the national intelligence enterprise suggest that current "reform" efforts are merely the first steps in a much lager – and fundamental – transformation. A careful, considered examination of what intelligence must accomplish and how this can be best achieved may ensure that the goals Treverton identifies as necessary for the future are met – and met sooner rather than later. Here again critical thinking has much to offer. By encouraging discussion of the alternatives and their advantages and disadvantages, and by examining analogous cases, critical thinkers aid the transformation. Questioning of assumptions about the roles of intelligence, its activity, and organization will reveal which long-held beliefs need retirement.

Further, technology efforts in support of analysis, such as those being developed through the efforts of the ARDA – and other – advanced technology efforts presume that analysts think critically. For instance, by focusing "analytic attention on the most critical information found within massive data,"[223] some research projects seek to uncover otherwise unknown information that indicates the potential for strategic surprise.[224] These projects seek to build

223 Critical information is that which is *essential* for analysts to make sense of what their targets are going to do. Often it is buried in massive amounts of "noise."

224 Advanced Research and Development Activity, *Broad Agency Announcement for the Novel Intelligence from Massive Data (NIMD) R&D Program,* NMA401–02–BAA–0004, 7 JUNE 2002, 1.

partnerships between analysts and technology applications.[225] In one case, a research firm has developed technology that enables analysts to generate and validate novel hypotheses, distill complex systems into digestible elements, create effective narratives, and inspire creative thinking.[226] Other examples are illustrated in the adjacent text box. Follow-on research efforts such as the Collaboration and Analyst/System Effectiveness (CASE) effort will develop these efforts further.[227] The intelligence workforce these ARDA-supported efforts presuppose is being hired and trained now.

The future also holds opportunities for further developing models of reasoning in intelligence. Exactly how analogy and critical thinking interact, the roles of creative thinking, the roles of intuition, and specific strategies for bias mitigation are all areas warranting further research. Formal validation of how critical thinking improves intelligence reasoning is another research topic. Rieber and Thomason's proposed National Institute of Analytic Methods is an obvious venue for such research. Additionally, the ARDA advanced questioning and answering research program, AQUAINT, as well as other ARDA programs dealing with predictive analysis, prior and tacit knowledge, and hypothesis generation offer other domains in which such research could occur.[228] Such research is of both intrinsic value and necessary for developing new means

225 The five areas on which the NIMD effort focused were modeling analysts and how they work; analysts' prior and tacit knowledge; creating, representing, and tracking multiple scenarios, hypotheses, and/or strategies; massive data management and analysis; and the means by which analysts interact with technology. The author represented his agency in evaluating and mentoring the efforts of the researchers.

226 The author is a technical mentor of this firm's work.

227 For more information, see "Collaboration and Analyst/System Effectiveness (CASE)," AFRL Directorate: IFED BAA 06–02–IFKA, 28 October 2005, URL: <http://www.rl.af.mil/div/IFK/baa/>, last accessed 11 March 2006.

228 Advanced Research and Development Activity (ARDA), "Preliminary Solicitation Information for Advanced QUestion & Answering for INTelligence (AQUAINT)," URL: <http://www.digitalgovernment.org /library/library/pdf/preliminary_information.pdf>, last accessed 26 March 2006.

Issue	1970s and 1980s
Focus of Analysis	Continuing large, well-defined issues and adversaries
	Space for longer-term thinking
Organization and Workflow	Large, centrally organized and managed
	Hierarchical
	Institutional and operational memory mostly in analysts heads
	Time pressure persistent but low intensity (mostly)
Sources and Methods	Dominated by secret sources
	Analysts are separated from collectors
	Analysts mostly passive recipients of information
	Analysis focuses on previous patterns
	Analysts operate on basis of own experience and biases
Analysts' Characteristics	Many analysts are deep specialists
	Analysts mostly work alone or in small groups
	Key analytic choices with analysts

Table 7: Analysis: Past, Present and Future

Source: Developed by Gregory F. Treverton with input from the author.

1990s and 2000s	Future
Emergence of complex, rapidly shifting issues and adversaries	Complex, rapidly shifting issues and adversaries and large, well-defined issues and adversaries
Bias toward current intelligence	Both immediate question–answering and deeper analysis
Large, centrally organized and managed	Tailored to rapidly adapt to shifting foci
Still hierarchical, though problem-oriented "centers" added	Flat, problem-centric networks
Institutional and operational memory mostly in analysts heads	Technology helps to notice what analysts are watching and asking
Time pressure drives toward premature closure	Technology allows memory even of hypotheses, data rejected by analysts
Broader range of sources, but secrets still primary	Draws on a wide variety of sources, open and secret
Analysts are also their own collectors	Analysts are their own collectors
Limited searching of available data	Much more aggressive searching and reaching for data…both classified and unclassified
Same, though growing interest in new methods and tools for shaping, remembering, and examining hypotheses	Formative pattern recognition and data mining capabilities searches for out of the ordinary
Limited use of formal method and technology	Wide use of method and technology – from aggregating expert views to searching, data mining, pattern recognition
Many, perhaps most, analysts are generalists	Mix of generalists and deep specialists, both technical and political
Analysts mostly work alone or in small groups	Analysts work in larger virtual networks
Key analytic choices with analysts	Key analytic choices with analysts

Email exchanges 17–18 May 2006.

of improving intelligence analysis. Knowing the details of how analysts reason and how they might reason more effectively guides managers to understand where educational and training efforts can be most valuable.

TECHNOLOGICAL ADVANCES IN CRITICAL THINKING

One ARDA research team has created a technological system employing an automated critical thinking-based model that provides an overarching control structure for analytic reasoning. It includes both model generation (for counter–examples) and more traditional argument building. The system's creators assert – based on preliminary testing – that analysts employing the system are faster and more accurate problem solvers.

Suppose an analyst develops an argument in the course of using this system, that confirms that Saddam Hussein has WMD and an argument that confirms that Saddam does not have WMD. Working both sides of this issue, this analyst will make inferences from evidence and link them with other evidence-derived inferences. She will not imagine a situation in which all her evidence is true, but her hypothesis is not. For example, the evidence might include communications from which she infers that those communicating – including Saddam's scientists – believe they have WMD. Using the system, she also would be led to consider that the scientists might have wanted to deceive Saddam into believing that they were further along than they were. The generation of this alternative model can only arise through a mechanism that conducts the analyst away from the comfortable, inductive, confirmation path associated with the initial hypothesis.

Conclusion

> Never before in our peacetime history have the stakes of foreign policy been higher.
>
> —Sherman Kent, 1949

This paper posed the intriguing question: "How can intelligence analysts be 'really good'"? Critical thinking, if conceived and employed by intelligence analysts as suggested here, appears capable of leading analysts to adopt personal habits of thought appropriate to the resolution of hard intelligence problems. The idea that intelligence analysts are expected to bring to the table a capability to draw reasoned and actionable conclusions from scant and conflicting information distinguishes their charge from that of their academic brethren. Thus, intelligence analysts in government or other applied work environments may deserve the lavish budgets and technological capabilities they often enjoy.

To earn their high level of resource support, analysts can take advantage of a capability to redirect unique intelligence collection capabilities. In doing so, they are perfectly positioned to apply critical thinking methods to the hard problems. They can, for example, order up special collection against targets that exhibit even fleeting evidence that convincingly disconfirms one or more alternative hypotheses about an impending threat. This is the nub of Ben-Israel's argument for a "logical" approach to intelligence analysis for national security, and is an approach no doubt under-used by those who do not systematically think about threats in the manner developed in this paper.

Although most of the specific threats have changed since Sherman Kent first wrote in 1949, his epigraph remains as true today as it was then: the survival and prosperity of the United States remain at stake; they depend on effective, informed foreign policy.[229] Critical thinking brings with it an indispensable capability to inform a rational

229 Kent, *Strategic Intelligence,* ix.

foreign policy. "Really good analysts" are those who think critically about the issues they work and the problems they solve; they bring structured thought to the foreign policy realm.

Appendix

NSA's Critical Thinking and Structured Analysis Class Syllabus[230]

Background

Twenty-first Century intelligence issues involve uncertainty, mysteries, and risk. This differs from the 20th Century paradigms of security, secrets, and prevention. Analysis of current complex issues requires of its practitioners novel approaches including a productively imaginative process of inquiry. Questions an analyst asks not only serve as devices for attracting existing evidence, but also as devices for generating new evidence not presently considered. In this way, analysts more thoroughly examine complex issues and, aided by technology, are more likely to create novel intelligence and prevent strategic surprise.

However, such reasoning is at odds with how people – all people, including intelligence analysts – naturally think. Instead, people seek to confirm the first answer to a problem they discover, selectively using evidence to support that position *even when there is compelling evidence that an alternative hypothesis may actually be the correct one.* That people routinely fall prey to such poor thinking is well documented. Indeed, most commercial advertisers strive to take advantage of this. So do adversaries. One element of most intelligence failures includes poor thinking on the part of analysts—poor thinking of which adversaries have taken advantage. So how can analysts avoid such thinking?

One solution is to teach intelligence analysts to think critically.

230 This syllabus has been developed and refined by the author through several years of teaching critical thinking at the National Security Agency's National Cryptologic School. An early version of the course bore similarity to one developed by (then) MSGT Robert D. Folker, while a student at the (now) National Defense Intelligence College. Folker's course focused on the methods of analysis, not on the overarching critical thinking. His course (as written) is not taught at the college.

Critical thinking provides structure to the reasoning process that identifies for analysts where they are likely to go astray. It offers a means for self-reflective reasoning that leads to improved thinking. If such thinking is aided by structured analytic techniques, then analysts will (and do) improve how they resolve issues with which they are confronted. The quality of their work improves.

This critical thinking and analytic problem-solving course offers participants a chance to learn a paradigm for critical thinking and critically explore 14 different structured methods of analysis. Texts by critical thinking experts Richard Paul and Linda Elder, and structured analysis experts Morgan Jones and Richards Heuer, as well as materials developed by the instructor, teach the concepts and techniques. Classroom problems as well as operational examples (introduced and developed by the students from their own work) reinforce and help transfer what is learned into the operational environment. A final project developed by student teams completes the formal requirements.

Learning to think critically and to solve problems in a structured manner requires active participation. The class requires 40 hours of classroom time, consisting of ten sessions of four hours each. The method of instruction is Socratic, demanding active classroom participation. Participants also can expect homework, requiring both office and non-office time. Participants will prepare reading summaries for each class session, and develop one (or more) operational examples of at least one structured analytic method. Finally, participants work together on teams to complete classroom assignments and a final project dealing with an operational issue (employing at least five structured analytic methods).

Administration:

Enrollment: Up to 21 Students.
Class Date/Time/Duration: One 4-hour class per day for 10 weeks.
Class Location: _____.
Homework: Yes, but hopefully not too odious. Operational examples are required. A team project is due at the end of the course.

Texts:

Elder, Linda, and Richard Paul. *The Foundations of Analytic Thinking: How to Take Thinking Apart and What to Look for When You Do* (Dillon Beach, CA: Foundation for Critical Thinking, 2003).

Heuer, Richards J., Jr. *The Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), URL: <http://cia.gov/csi/books/19104/index.html>, last accessed 15 March 2006.

Jones, Morgan D. *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions* in B*usiness and in Life* (New York, NY: Crown Publishing Group, 1997).

Several handouts (TBD)

Objectives:

The overall objective of the class is to enable you to critically think about analysis and what analysts are tasked to analyze. A second objective is to provide you with a set of analytic tools that are useful to your analysis. At the end of the class you will be equipped with a set of analytic skills and will have honed your critical thinking skills, allowing you to better function in the workplace. Specifically, the course objectives are as follows:

Upon completion of this course you will be able to:

- Use critical thinking techniques to provide structure to your analytic reasoning.
- Identify, describe, and employ 14 methods for structured reasoning.
- Demonstrate critical thinking proficiency through lecture, classroom participation, and weekly homework assignments.
- Complete a final class assignment using a minimum of five structured analytic methods presented in this course.
- Apply knowledge of critical thinking by using a set of analytic tools designed to hone your skills as an analyst.

In other words, at the end of this 10-week-long class, you will have

- Learned to critically analyze intelligence-associated data, information, and evidence.
- Honed your critical thinking skills.
- Built a "toolbox" of analytic and problem-solving methods.
- Become better analysts.

For example, when you approach a problem you will be able to

- Discover the true problem by restating and considering alternative outcomes.
- Have a variety of methods by which you can organize and make sense of the relevant evidence.

Formal Requirements:

Written summaries of readings. (No more than one page per chapter assigned.) The summaries should answer ***exactly*** the questions on page five of the syllabus. The summaries should also include answers to the exercises in Morgan Jones' book. The summaries will be typed unless prior arrangements have been made with the instructor. In-class discussions will draw heavily on the readings.

Problems from the work environment (Operational Exemplars). As we study the elements of reasoning and the methods of problem solving, we need operational examples

against which to apply/illustrate what we are learning. You will be responsible for providing at least one of those examples for the class to be presented during the week we discuss the method. The best exemplars may be saved for use in subsequent classes.

Final project. Working in teams of three or four, and using any Problem Restatement and Divergent and Convergent Thinking plus at least three other methods developed in the course – for a total of of at least five methods – you will develop an operational project to be presented at the last class. You will apply the elements of critical thinking to the method chosen as well as the specific problem, apply the appropriate methods to solve of problem, report the results, and evaluate the process. The project will be presented during a 15–20 minute briefing. A list of the specific elements that must be included and the format by which the project is graded is on the last page of this syllabus.

Grading:

- **Written Summaries (25%).** Due weekly. The first summary will be graded. Subsequently, a random number generator will be used to select three (3) additional summaries for grading. Grading will be based on the "Universal Intellectual Standards" in *The Foundations of Analytic Thinking* and on whether instructions are followed. For example, if you are asked to identify what key questions an author is attempting to answer, *it is expected that you will provide those questions in the reading summary.*
- **Class Participation (25%).** Since this is a discussion course, you are expected to engage in the process.
- **Operational Exemplars (25%).** Assigned the first week. No longer than 5 minutes each.
- **Final Project (25%).**

Class Descriptions and Weekly Assignments (complete prior to each class):

Class 1 – How We Don't Think and How We Might

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 1–2 (Part One).
Psychology of Intelligence Analysis, 1–30.
Critical Thinking: Concepts and Tools, entire work.

Written Assignment: *Reading summaries for chapters from Jones and Heuer. Exercises in text.*

Class Objectives: *At the end of Class 1 you will be able to:*

- Define a bias and discuss the implications of biases in our decisions.
- Identify sources of cognitive biases.
- Describe the inherent dangers/benefits of biases and the difficulty of compensating for perceptual biases.
- Describe the characteristics and three principles of perception.
- Describe how analysts fall prey to absence-of-evidence biases.
- Describe how anchoring impacts analytical decision-making.
- Describe how a target can use assimilation biases to deceive.
- Acknowledge how analysts unwittingly use confirmation bias to support early assessments.
- Discuss how hindsight and reliability biases play a part in intelligence failures.
- Describe how oversensitivity to consistency bias can lead to undesirable results.
- Discuss how expert biases and the Pollyanna and Cassandra complexes distort our thinking.
- Describe how cultural, personal, and organizational

mindsets impact analysis.

- Define mindsets, discuss how they are derived, and describe how they influence predictions.
- Identify how we think.
- Describe critical thinking and the standards used for evaluating our thinking.
- Identify the elemental structures of thought.
- Describe the differences between inferences and assumptions in intelligence analysis.

Class 2 – Critical Problem Restatement and Alternative Thinking

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life,* Chapters 3, 5.

Written Assignment*: Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 2 you will be able to:*

- Demonstrate knowledge of the critical thinking process by providing an example that meets the universal intellectual standards.
- Describe the role of questioning in critical thinking.
- Identify the three types of questions used in critical thinking.
- Determine the sample domains involved in complex questions.
- Define problem restatement and apply its use through a practical example.
- Discuss the role that our biases play in problem restatement.
- Demonstrate knowledge of the critical thinking process by providing an example that meets the universal intellectual standards.
- Define divergent thinking and its benefits when performing a problem restatement.
- Discuss the pitfall involved in problem definition and how it relates to problem restatement.
- Describe some effective techniques for problem restatement.
- Identify the types of problems that benefit from problem restatement.
- Discuss how points of view influence the critical thinking process.
- Discuss the logic, benefits, risks, and elements of divergent thinking.
- Identify the four main ideas of divergent thinking.

- Describe what is needed to move from divergence to convergence.
- Identify the types of problems that benefit from divergent thinking.

Class 3 – Pollyanna, Cassandra, and Marshaling

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 4, 6.

Written Assignment*: Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 3 you will be able to:*

- Discuss the pros-cons-fixes approach to critical thinking and the six-step method employed by successful analysts.
- Identify the logic behind the pros-cons-fixes approach and discuss those critical thinking problems best suited to this method.
- Apply the techniques of sorting, chronologies, and timelines to critical thinking and identify those critical thinking problems best suited for this approach.
- Identify the two-step technique used for sorted lists, chronologies, and timelines.

Class 4 – Causes, Squares, and Shrubs

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 7, 8, 9.

Written Assignment: *Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 4 you will be able to:*

- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for causal flow diagramming.
- Identify the major factors and cause-and-effect relationships influencing causal flow diagramming.
- Characterize the differences between direct and inverse relationships and their impact on causal flow diagramming.
- Define a feedback loop and discuss what makes it stable or unstable.
- Apply your knowledge of causal diagramming by participating in a classroom exercise.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for scenario matrices and trees.
- Define and discuss the characteristics and differences between matrices and scenario trees.
- Apply your knowledge of scenario matrices by participating in a classroom exercise.
- Apply your knowledge of scenario trees by participating in a classroom exercise.

Class 5 – Weighing the Likelihood

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 10, 13.

Written Assignment: *Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 5 you will be able to:*

- Discuss how individuals view issues.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for weighted ranking.
- List the 9-step process involved in weighted ranking.
- Demonstrate knowledge of weighted ranking through class and small group exercises.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for probability.
- Define and describe how and why we characterize and assign events, and how this influences intelligence analysis.
- Discuss and explain the differences between mutually exclusive and conditionally dependent events relative to probability.
- Identify the seven steps in creating a probability tree.
- Apply your knowledge of probability by participating in a classroom exercise.

Class 6 – Testing the Devil's and Other's Advocacy

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life,* Chapters 11–12.
The Psychology of Intelligence Analysis, Chapter 8.

Written Assignment: *Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 6 you will be able to:*

- Define intelligence.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for devil's advocacy.
- Define, describe, and characterize situations appropriate to employ methods of devil's advocacy in intelligence analysis
- Demonstrate prowess in devil's advocacy through participation in a practical case study.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for hypothesis testing.
- Discuss the benefits of hypothesis testing.
- Identify the 8-step process of hypothesis testing.
- Demonstrate prowess in hypothesis testing through participation in a practical case study.

Class 7 – Analyzing Apples and Toyotas

Reading Assignment*: The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 14, 15, 16.

Written Assignment: *Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 7 you will be able to:*

- Describe how individual viewpoints influence utility analysis.
- Define utility analysis and discuss the type of problems best suited for this method.
- Identify the logic of utility analysis.
- Employ utility analysis to arrive at the most cost-effective solutions.
- List the steps involved in creating a utility tree and apply this knowledge by participating in classroom exercises.
- List the steps involved in creating a utility matrix and apply this knowledge by participating in classroom exercises.
- Examine the benefits of structuring as it applies to utility and probability analysis.
- Describe the differences between utility and probability analysis.
- Examine multi-perspective utility analysis and its use by participating in classroom exercises.
- List the 13 steps of multi-perspective utility analysis.
- Apply your knowledge of multi-perspective utility analysis by participating in a classroom exercise.

Class 8 – And Now for Something Completely Different

Reading Assignment: *Review all assigned readings.*

Written Assignment: *None.*

Class Objectives: *At the end of Class 8 you will be able to:*

- Describe which structured analysis methods work best in particular situations.
- Demonstrate knowledge of critical thinking and structured analysis through a practicum.
- Demonstrate your knowledge of critical thinking and structured analysis through a small group exercise.

Class 9 – Final Project Preparation

Reading Assignment: *Review all assigned readings.*

Written Assignment: *None.*

Class Objectives: *During Class 9 you will:*

- Learn through experience the pros and cons of research, analysis and reporting in small teams.

Class 10 – Final Project Presentation and Wrap-up

Reading Assignment: *Review all assigned readings.*

Written Assignment: *None.*

Class Objectives: *During Class 10:*

- Your small group will make a multi-media presentation on the analytic problem you chose.

Methods:

- A sample of the problem statement and restatement process.
- A sample of the convergent and divergent thinking applied to the problem.
- Concise demonstrations of the three structured analytic methods used to answer the analytic problem.

Assessment:

- **You are evaluated on how clearly the group presents its project, and on whether the project requirements listed above are met as shown on the last page of the syllabus.**

Reading Summary Questions:[231]

For each chapter/work, answer the following questions (in writing) about the reading.

1. What is the author's purpose? If there is more than one main point, what is the overarching purpose?

2. What are the key questions the author raises/addresses?

3. What evidence does the author provide to support his argument?

4. What inferences does the author make from the evidence?

5. On what underlying concepts does the author rely?

6. What does the author take for granted? What assumptions does the author make?

7. What are the implications of the author's point of view? What are the implications if we adopt/do not adopt what the author recommends?

8. What is the author's point of view? What other points of view are there?

231 Paul and Elder, *Concepts and Tools*, 13.

Final Project Evaluation Worksheet[232]

	Clarity	Accuracy	Precision	Relevance	Depth	Breadth	Logic	Significance	Fairness
Purpose									
Key Questions									
Assumptions									
Evidence									
A: Methods									
B: Analysis									
Concepts									
Inferences									
Implications									
Other Points of View									
Lessons Learned									
Comments									

232 Derived by author from Paul and Elder, *Concepts and Tools, 2–9.*

Bibliography

Ackerman, Robert K. "Information Age Poses New Challenges to Intelligence." *Signal* 53, no. 2 (October 1998): 23–25.

Advanced Research and Development Activity. *Broad Agency Announcement for the Novel Intelligence from Massive Data (NIMD) R&D Program.* NMA-401-02-BAA-0004, 7 June 2002, 1.

_____. "Preliminary Solicitation Information for Advanced QUestion & Answering for INTelligence (AQUAINT)." URL: <http://www.digitalgovernment.org/library/library/pdf/preliminary_information.pdf>. Last accessed 26 March 2006.

Air Force Research Laboratory (AFRL). IFED Directorate. "Collaboration and Analyst/System Effectiveness (CASE)." BAA 06-02-IFKA, 28 October 2005. URL: <http://www.rl.af.mil/div/IFK/baa/>. Last accessed 11 March 2006.

Allen, Charles E. "Intelligence: Cult, Craft, or Business?" In *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2000.* Cambridge, MA: Harvard University Program on Information Resources Policy, I-01-1, April 2000. URL: <http://www.pirp.harvard.edu/pubs.html>. Last accessed 11 January 2006.

Allison, Graham, and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis,* 2nd Edition. New York, NY: Longman, 1999.

Amuchastegui, Domingo "Cuban Intelligence and the October Crisis." In James G. Blight and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis.* London, UK: Frank Cass, 1998: 88–119.

Anderson, Terence J., and William Twining. *Analysis of Evidence: How to Do Things with Facts Based on Wigmore's Science of Judicial Proof.* Chicago, IL: Northwestern University Press, 1991.

Anderson, Terence J., David A. Schum, and William Twining. *Analysis of Evidence.* Cambridge, UK: Cambridge University Press, 2005.

Bathurst, Robert B. *Intelligence and the Mirror: On Creating an Enemy.* Oslo, Norway: International Peace Research Institute, 1993.

Ben-Israel, Isaac. "Philosophy and Methodology of Intelligence: The Logic of the Estimate Process. *Intelligence and National Security* 4, no. 4 (October 1989): 660–718.

Blight, James G., and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis.* London, UK: Frank Cass, 1998.

Boden, Margaret A. *The Creative Mind: Myths and Mechanisms.* New York, NY: Basic Books, 1990.

Brei, William S., CAPT, USAF. *Getting Intelligence Right: The Power of Logical Procedure.* Occasional Paper Number Two. Washington, DC: Joint Military Intelligence College, January 1996.

Brent, Joseph. *Charles Sanders Peirce: A Life.* Bloomington, IN: Indiana University Press, 1998.

Brookfield, Stephen D. *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting.* San Francisco, CA: Jossey-Bass Publishers, 1987.

Callum, Robert. "The Case for Cultural Diversity in the Intelligence Community." *International Journal of Intelligence and CounterIntelligence* 14, no. 1, Spring 2001: 25–48.

Cheikes, Brant A., Mark J. Brown, Paul E. Lehner, and Leonard Adelman. *Confirmation Bias in Complex Analyses,* Mitre Technical Report MTR 04B0000017. Bedford, MA: Center for Integrated Intelligence Systems, October 2004.

Christensen, Clayton M. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail.* Boston, MA: Harvard Business School Press, 1997.

Christensen, Clayton M., and Michael E. Raynor. *The Innovator's Solution: Creating and Sustaining Successful Growth.* Boston, MA: Harvard Business School Press, 2003.

Christensen, Clayton M., Scott D. Anthony, and Erik A. Roth. *Seeing What's Next: Using the Theories of Innovation to Predict Industry Change.* Boston, MA: Harvard Business School Press, 2004.

"Clarke: Bush Didn't See Terrorism as 'Urgent'." *CNN.com, 19* May 2004. URL: <http://www.cnn.com/2004/ALLPOLITICS/03/24/911.commission/index.htm>. Last accessed 9 March 2006.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States.* Washington DC: Government Printing Office, March 31, 2005. URL: <http://www.wmd.gov/report/ index.html>, last accessed 28 July 2005.

Cooper, Jeffrey R. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis.* Washington, DC: Center for the Study of Intelligence, 2005.

_____. Email to the author. 31 March 2006.

Davis, Jack. "The Kent-Kendall Debate of 1949." *Studies in Intelligence* 35, no. 2 (Summer 1991): 37–50.

De Bono, Edward. *de Bono's Thinking Course.* New York, NY: Facts on File Publications, 1982.

De Cagna, Jeff. "Making Change Happen: Steve Denning Tells the Story of Storytelling." *Information Outlook*, January 2001: 28–35.

De Rivera, Joseph. *The Psychological Dimension of Foreign Policy.* Columbus, OH: Charles E. Merrill Publishing Company, 1968.

Denning, Stephen. *The Springboard: How Storytelling Ignites Action in Knowledge-Era Organizations.* Boston, MA: Butterworth-Heinemann, 2001.

Devlin, Keith. *Goodbye Descartes: The End of Logic and the Search for a New Cosmology of the Mind.* New York, NY: John Wiley & Sons, Inc., 1997.

Dewey, John. *How We Think: A Restatement of the Relation of Reflective Thinking to the Educative Process.* New York, NY: D.C. Heath and Company, 1910.

Dijksterhuis, Ap, Martin W. Bos, Loran F. Nordgren, and Rick B. von Baren. "On Making the Right Choice: The Deliberation-Without-Attention Effect." *Science*, 311, no. 5763 (17 February 2006): 1005–1007.

DiSpezio, Michael A. *Classic Critical Thinking Puzzles.* New York, NY: Main Street, 2005.

Durkheim, Emile. *The Rules of Sociological Method.* Glencoe, IL: Free Press, 1938.

Eco, Umberto, and Thomas A. Sebeok. *The Sign of Three: Dupin, Holmes, Pierce.* Bloomington, IN: Indiana University Press, 1988

EDS. *Herding Cats*. Television advertisement produced for EDS by Fallon-McElligott. Videocassette, January 2000.

_____. *Building Airplanes in Flight.* Television advertisement produced for EDS by Fallon-McElligott. Videocassette, November 2000.

Elder, Linda, and Richard Paul. *The Foundations of Analytic Thinking: How to Take Thinking Apart and What to Look for When You Do.* Dillon Beach, CA: The Foundation for Critical Thinking, 2003.

Elliott, Michael. "How the U.S. Missed the Clues." *CNN.com*, 20 May 2002. URL: < http://archives.cnn.com/2002/ALLPOLITICS/05/20/time.clues/index.html>. Last accessed 9 March 2006.

Facione, Peter A. *Critical Thinking: What It Is and Why It Counts*. Milbrae, CA: California Academic Press, 1998, updated 2004. URL<http://www.insightassessment.com/>. Last accessed 22 July 2005.

Facione, Peter A., Noreen C. Facione, and Carol A. Giancarlo. "The Disposition Towards Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill," *Informal Logic* 20, no. 1 (2000): 61–84.

_____. *Professional Judgment and the Disposition Toward Critical Thinking* (Milbrae, CA: California Academic Press, 2002). URL: < http://www.calpress.com/ pdf_files/Prof_jmn.pdf>. Last accessed 31 March 2006.

Feder, Stanley. "Factions and Policon: New Ways to Analyze Politics." In Westerfield, H. Bradford, ed. *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955–1992.* New Haven, CT: Yale University Press, 1995.

Feldman, Daniel. *Critical Thinking: Strategies for Decision Making.* Menlo Park, CA: Crisp Publications, Inc, 2002.

Fisher, Alec. *Critical Thinking: An Introduction.* Cambridge, UK: Cambridge University Press, 2001.

Folker, Robert D., MSGT, USAF. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods.* Occasional Paper Number Seven. Washington, DC: Joint Military Intelligence College, January 2000.

Folker, Robert D., LT, USAF. Email to the author. 9 December 2003.

Fursenko, Aleksandr and Timothy Naftali. *"One Hell of a Gamble:" Khrushchev, Castro, and Kennedy, 1958–1964.* New York, NY: W. W. Norton & Company, 1997.

Garthoff, Raymond L. "US Intelligence in the Cuban Missile Crisis." In James G. Blight and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis.* London, UK: Frank Cass, 1998: 18–63.

George, Alexander. *Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice.* Boulder, CO: Westview Press, 1980.

Gilovich, Thomas. *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life.* New York, NY: The Free Press, 1991.

Gilovich, Thomas, Dale Griffin, and Daniel Kahneman, Eds. *Heuristics and Biases: The Psychology of Intuitive Judgment.* Cambridge, UK: Cambridge University Press, 2002.

Gladwell, Malcolm. *The Tipping Point: How Little Things Can Make a Big Difference*. Boston, MA: Little Brown and Company, 2000.

_____. *Blink: The Power of Thinking without Thinking.* Boston, MA: Little Brown and Company, 2005.

Glaser, Edward M. *An Experiment in the Development of Critical Thinking.* New York, NY: AMS Press, 1941.

Grabo, Cynthia M. *Anticipating Surprise: Analysis for Strategic Warning.* Washington DC: Joint Military Intelligence College, 2002.

Gribkov, Anatoli. "The View from Moscow and Havana." In Gribkov, Anatoli, and William Y. Smith. *Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis.* Chicago, IL: Edition q, 1994: 3–76.

Gribkov, Anatoli, and William Y. Smith. *Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis.* Chicago, IL: Edition q, 1994.

Halpern, Diane. *Thought and Knowledge: An Introduction to Critical Thinking,* 4th Edition. Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 2002.

Hampson, Fen Osler. "The Divided Decision-Maker: American Domestic Politics and the Cuban Crises." *International Security,* 9, no 3 (Winter 1984/85): 130-165.

Harcourt Assessment, Inc. *Local Norms Report, Watson-Glaser Critical Thinking Assessment.* Report prepared for the Defense Intelligence Agency, 2005.

Heuer, Richards J., Jr. "Strategic Deception and Counterdeception: A Cognitive Process Approach." *International Studies Quarterly* 25, no. 2 (June 1981): 294–327.

_____. *Adapting Academic Methods and Models to Governmental Needs: The CIA Experience.* Strategic Studies Institute. U.S. Army War College. July 31, 1978.

_____. *Psychology of Intelligence Analysis.* Washington, DC: CIA Center for the Study of Intelligence, 1999.

Hinsley, F. H., and Alan Stripp, Eds. *Codebreakers: The Inside Story of Bletchley Park*. Oxford, UK: Oxford University Press, 1993.

Holyoak, Keith J., and Paul Thagard. *Mental Leaps: Analogy in Creative Thought.* Cambridge, MA: The MIT Press, 1995.

Hughes, Francis J. Conversation with the author. Washington, DC: Joint Military Intelligence College. 8 May 2003.

Hughes, Francis J., and David A. Schum. *Credibility Assessment: A First Step in Intelligence Analysis.* Unpublished tutorial. Joint Military Intelligence College, April 2003.

Janis, Irving. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes,* 2nd Edition. Boston, MA: Houghton Mifflin Company, 1982.

Jervis, Robert. *System Effects: Complexity in Political and Social Life.* Princeton, NJ: Princeton University Press, 1997.

Johnson Thomas R., and David A. Hatch. *NSA and the Cuban Missile Crisis.* Fort Meade, MD: National Security Agency Center for Cryptologic History, 1998. URL: <http://www.nsa.gov/publications/publi00033.cfm>. Accessed 18 April 2006

Johnston, Rob. *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study.* Washington, DC: Center for the Study of Intelligence, 2005.

Jones, Morgan D. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving.* New York, NY: Random House, Inc, 1995.

_____. Conversation with the author. 15 December 2003.

Kahneman, Daniel, Paul Slovic, and Amos Tversky, eds. *Judgment under Uncertainty: Heuristics and Biases.* Cambridge, UK: Cambridge University Press, 1982.

Kam, Ephraim. *Surprise Attack: The Victim's Perspective*. Cambridge, MA: Harvard University Press, 1990.

Kent, Sherman. *Strategic Intelligence for American World Policy.* Princeton, NJ: Princeton University Press, 1949.

_____. "A Crucial Estimate Relived." *Studies in Intelligence* 36, no. 5 (1992): 111–119.

Kerbel, Josh. "Thinking Straight: Cognitive Bias in the US Debate about China." *Studies in Intelligence* 48, no. 3 (2004), URL: <http://cia.gov/csi/studies/vol48no3/index.html>. Last accessed 22 February 2006.

Klein, Gary. *Intuition at Work: Why Developing Your Gut Instincts Will Make You Better at What You Do.* New York, NY: Doubleday, 2003.

Krizan, Lisa. *Intelligence Essentials for Everyone.* Occasional Paper Number Six. Washington, DC: Joint Military Intelligence College, 1999.

Lebow, Richard Ned, and Janice Gross Stein. "Back to the Past: Counterfactuals and the Cuban Missile Crisis." In Philip E. Tetlock, and Aaron Belkin *Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives*. Princeton, NJ: Princeton University Press, 1996: 119–148.

LeGault, Michael R. *Think: Why Crucial Decisions Can't Be Made in the Blink of an Eye.* New York, NY: Threshold Editions, 2006.

Lengel, Allan. "Little Progress in FBI Probe of Anthrax Attacks: Internal Report Compiled As Agents Hope for a Break." *Washington Post.* 16 September 2005. A01.

Lengel, Allan, and Guy Gugliotta. "Md. Pond Produces No Anthrax Microbes: FBI Sought Clues In Deadly Attacks." *Washington Post.* 1 August 2003. A03.

Lipman, Matthew. *Thinking in Education,* 2nd Edition. Cambridge, UK: Cambridge University Press, 2003.

Lundahl, Arthur C. "Additional Information—Mission 3102." Memorandum for Director of Central Intelligence and Director, Defense Intelligence Agency, 15 October 1962. In Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962.* Washington DC: Central Intelligence Agency, 1992: 181–182.

_____. "Additional Information—Mission 3107." Memorandum for Director of Central Intelligence and Director, Defense Intelligence Agency, 19 October 1962. In Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962*. Washington DC: Central Intelligence Agency, 1992: 209.

McAuliffe, Mary S., ed. *CIA Documents on the Cuban Missile Crisis, 1962* Washington DC: Central Intelligence Agency, 1992.

Marrin, Stephen. "Homeland Security and the Analysis of Foreign Intelligence," Markle Foundation Task Force on National Security in the Information Age, 15 July 2002, URL: <www.markletaskforce.org/documents/marrin_071502.pdf>. Last accessed December 9, 2003.

_____. Email to the author, 8 December 2003.

_____. "CIA's Kent School: Improving Training for New Analysts." *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (Winter 2003–2004): 609–637.

May, Ernest R. *Lessons of the Past: The Use and Misuse of History in American Foreign Policy.* Oxford, UK: Oxford University Press, 1973.

Merom, Gil. "The 1962 Cuban Intelligence Estimate: A Methodological Perspective." *Intelligence and National Security*, 14, no. 3 (Autumn 1999): 48–80.

Mid-Level Intelligence Professional. National Security Agency. Email to the author, 9 March 2006.

Miller, George A. "The Magical Number Seven, Plus or Minus Two." *The Psychological Review* 63 (1956): 81–97.

Miller, Judith. "A Battle of Words over War Intelligence." *New York Times.* Online edition, 22 November 2003. URL: <www.nytimes.com/2003/11/22/arts/22INTE.html>. Last accessed November 28, 2003.

Millward, William. "Life in and out of Hut 3." In Hinsley, F. H., and Alan Stripp, Eds. *Codebreakers: The Inside Story of Bletchley Park.* Oxford, UK: Oxford University Press, 1993: 17–29.

Moore, David T. *Creating Intelligence: Evidence and Inference in the Analysis Process.* MSSI Thesis. Washington, DC: Joint Military Intelligence College, July 2002.

_____. "Species of Competencies for Intelligence Analysis." *Defense Intelligence Journal* 11, no. 2 (Summer 2002): 97–119.

_____. Personal Notes. Joint Military Intelligence College, Denial and Deception Advanced Studies Program, Spring 2005.

Moore David T., and Lisa Krizan. "Intelligence Analysis: Does NSA Have What it Takes." Reprint: NSA Center for Cryptologic History. *Cryptologic Quarterly,* 20, nos 1/2 (Summer/Fall 2001): 1–33.

_____. "Core Competencies for Intelligence Analysis at the National Security Agency." In Swenson, Russell G., ed. *Bringing Intelligence About: Practitioners Reflect on Best Practices.* Washington DC: Joint Intelligence Military College, 2003: 95–132.

Moore, David T., Lisa Krizan, and Elizabeth J. Moore. "Evaluating Intelligence: A Competency-Based Model." *International Journal of Intelligence and Counterintelligence* 18, no. 2 (Summer 2005): 204–220.

Myers, David G. *Intuition: Its Powers and Perils.* New Haven, CT: Yale University Press, 2002.

Negroponte, John D., Director of National Intelligence. *National Intelligence Strategy of the United States of America.* Washington, DC: Office of the Director of National Intelligence, October 2005. URL: <http://www.dni.gov/NISOctober2005.pdf>. Last accessed 12 March 2006.

Neustadt, Richard E., and Ernest R. May. *Thinking in Time: The Uses of History for Decision Makers.* New York, NY: The Free Press, 1986.

Oberdorfer, Don. "Missed Signals in the Middle East." *Washington Post Magazine*, 17 March 1991.

Paul, Richard W. "A Draft Statement of Principles." The National Council for Excellence in Critical Thinking. URL: <www.criticalthinking.org/ncect.html>. Last accessed March 18, 2003.

Paul, Richard W., and Linda Elder. *The Miniature Guide to Critical Thinking Concepts and Tools*, 4th Edition. Dillon Beach, CA: The Foundation for Critical Thinking, 2004.

Paul, Richard W., and Gerald Nosich. *A Model for the National Assessment of Higher Order Thinking.* Dillon Beach, CA: Foundation for Critical Thinking, n.d.

Paul, Richard W., Linda Elder, and Ted Bartell. "Executive Summary, Study of 38 Public Universities and 28 Private Universities To Determine Faculty Emphasis on Critical Thinking In Instruction." *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations.* California Commission on Teacher Credentialing, Sacramento, California, 1997. Dillon, CA: Foundation for Critical Thinking, 1997. URL: <criticalthinking.org/schoolstudy.htm>. Last accessed March 18, 2003.

Paul, Richard W., Linda Elder, and Ted Bartell. *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations.* California Commission on Teacher Credentialing, Sacramento California, 1997. Dillon, CA: Foundation for Critical Thinking, 1997.

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies.* Princeton, NJ: Princeton University Press, 1999.

Pettee, George S. *The Future of American Secret Intelligence.* Washington, DC: Infantry Journal Press, 1946.

Platt, Washington. *Strategic Intelligence Production: Basic Principles.* New York, NY: Frederick A. Praeger, 1957.

Plous, Scott. *The Psychology of Judgment and Decision-Making.* New York, NY: McGraw Hill, Inc., 1993.

Raasa, Paul J. "The Denial and Deception Challenge to Intelligence." In Godson, Roy, and James J. Wirtz, *Strategic Denial and Deception.* New Brunswick, NJ: Transaction Publishers, 2002: 223–228.

Reed, Jennifer H. *Effect of a Model For Critical Thinking on Student Achievement In Primary Source Document Analysis And Interpretation, Argumentative Reasoning, Critical Thinking Dispositions, and History Content in a Community College History Course.* PhD Dissertation. College of Education, University of South Florida, December 1998. URL: <http://www.criticalthinking.org/resources/JReed-Dissertation.pdf>. Last accessed 6 May 2006.

Restak, Richard, M.D. *The Brain Has a Mind of Its Own: Insights from a Practicing Neurologist.* New York, NY: Harmony Books, 1991.

Reynolds, William. Conversation with the author, 14 March 2006.

Rieber, Steven, and Neil Thomason. "Toward Improving Intelligence Analysis: Creation of a National Institute for Analytic Methods." *Studies in Intelligence* 49, no. 4 (Winter 2006): 71–80.

Schafersman, Steven D. "An Introduction to Critical Thinking," January 1991. URL: <www.freeinquiry.com/critical-thinking.html>. Last accessed 9 March 2006.

Schecter Jerrold L., and Peter S. Deriabin. *The Spy Who Saved the World.* New York, NY: Scribner's, 1992.

Schum, David A. *Evidence and Inference for the Intelligence Analyst,* 2 volumes. Lanham, MD: University Press of America, 1987.

_____. *Evidential Foundations of Probabilistic Reasoning.* New York, NY: John Wiley & Sons, Inc., 1994.

_____. "Species of Abductive Reasoning in Fact Investigation in Law" *Cardozo Law Review* 22, nos. 5/6 (July 2001): 1645–1681.

_____. "Evidence Marshaling for Imaginative Fact Investigation." *Artificial Intelligence and Law* 9 (2001): 165–188.

Sebeok, Thomas A. "One, Two, Three Spells UBERTY." In Umberto Eco and Thomas A. Sebeok. *The Sign of Three: Dupin, Holmes, Pierce.* Bloomington, IN: Indiana University Press, 1988: 1–10.

Senate Select Committee On Intelligence. *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq.* United States Senate. 108th Congress, 7 July 2004.

Simon, Herbert A. "Invariants of Human Behavior." *Annual Review of Psychology* 41 (1990):1–19.

Stefik, Mark, and Barbara Stefik. *Breakthrough: Stories and Strategies of Radical Innovation.* Cambridge, MA: MIT Press, 2004.

Swenson, Russell G., ed. *Research: Design and Methods.* Washington, DC: Joint Intelligence Military College, 2000.

_____. *Bringing Intelligence About: Practitioners Reflect on Best Practices.* Washington, DC: Joint Intelligence Military College, 2003.

Tetlock, Philip E. *Expert Political Judgment: How Good Is It? How Can We Know?* Princeton, NJ: Princeton University Press, 2005.

Tetlock, Philip E. and Aaron Belkin. *Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives.* Princeton, NJ: Princeton University Press, 1996.

Thagard, Paul. *Coherence in Thought and Action.* Cambridge, MA: The MIT Press, 2000.

Treverton, Gregory F. Conversation with the author, 18 May 2006.

_____. Email exchanges with the author, 17–18 May 2006.

U.S. Congress. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001.* Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, Together with Additional Views. Senate Report No. 107-351/House Report. No. 107-792. 107th Congress, 2nd Session. December 2002.

U.S. Department of Defense. Photograph in the John Fitzgerald Kennedy Library. Boston, MA. PX 66-20:7 14 October 1962.

White, Mark J. *Missiles in Cuba: Kennedy, Khrushchev, Castro, and the 1962 Crisis.* Chicago, IL: Ivan R. Dee, 1997.

Wikipedia. "The Free Encyclopedia." URL: <www.wkikpedia.org>. Last accessed 12 March 2006.

Wirtz, James J. "Organizing for Crisis Intelligence: Lessons form the Cuban Missile Crisis." In James G. Blight and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis.* London, UK: Frank Cass, 1998: 120–149.

Wohlstetter, Roberta. "Cuba and Pearl Harbor: Hindsight and Foresight." *Foreign Affairs* 46, no. 3 (July 1965): 691–707.

Woods, Kevin, James Lacey, and Williamson Murray. "Saddam's Delusions: The View from the Inside," *Foreign Affairs*, 85, no. 3 (May/June 2006). URL: <http://www.foreignaffairs.org/20060501faessay85301/kevin-woods-james-lacey-williamson-murray/saddam-s-delusions-the-view-from-the-inside.html>. Accessed 31 March 2006.

Woods, Kevin M., Michael R. Pease, Mark E. Stout, Williamson Murray, and James G. Lacey, *Iraqi Perspectives Project: A View of Operation Iraqi Freedom from Saddam's Senior Leadership*. Norfolk, VA: Joint Center for Operational Analysis, 2006. URL: <http://www.foreignaffairs.org/special/iraq/ipp.pdf>. Last accessed 31 March 2006.

Zlotnick, Jack. "Bayes' Theorem for Intelligence Analysis." *Studies in Intelligence* 11, no. 4 (Spring 1972): 1–12. URL: <http://cia.gov/csi/kent_csi/pdf/v08i4a11p.pdf#page=1>. Last accessed 7 April 2006.

About the Author

David T. Moore is a career senior intelligence analyst and technical director at the National Security Agency where he is an advocate for, and mentor of best practices in intelligence analysis. He is an adjunct faculty member of the National Cryptologic School; has taught at the National Defense Intelligence College, Washington, DC; and at Trinity University, Washington, DC. Mr. Moore holds a B.A. in sociology from Washington and Lee University and a Master of Science of Strategic Intelligence from the National Defense Intelligence College (formerly the Joint Military Intelligence College).

Mr. Moore's other publications include:

- "Species of Competencies for Intelligence Analysis," *Defense Intelligence Journal,* 11, no. 2 (Summer 2002): 97-119.
- "Species of Competencies for Intelligence Analysis," *American Intelligence Journal*, 23 (2005): 29–43 (an expanded version of the original article).
- With coauthor Lisa Krizan:
    - "Intelligence Analysis, Does NSA Have What it Takes," *Cryptologic Quarterly,* 20, nos. 1/2 (Summer/Fall 2001): 1-32.
    - "Core Competencies for Intelligence Analysis at the National Security Agency," in *Bringing Intelligence About: Practitioners Reflect on Best Practices,* Russell Swenson, ed. (2004): 95-131.
- With coauthors Lisa Krizan and Elizabeth J. Moore
    - "Evaluating Intelligence: A Competency-Based Approach," in the *International Journal of Intelligence and CounterIntelligence*, 18, no. 2 (Summer 2005): 204-220.
- With coauthor William N. Reynolds:
    - "So Many Ways To Lie: The Complexity of Denial and Deception," *Defense Intelligence Journal,* 15, no. 2 (Fall 2006): 95-116.

Colophon

A colophon records the details of the layout and design of a publication. It acknowledges the craftsmanship and art required in creating a printed work. Whereas the acknowledgements record the textual assistance an author receives, a colophon records the equally important technical assistance received.

This Occasional Paper was set in Baskerville, a transitional typeface created by Birmingham printer John Baskerville around 1752. George Jones redesigned it in 1930 for Linotype-Hell; the International Typeface Corporation licensed it in 1982. The long, elegant serifs and the subtle transfer of stroke weight from thick to very thin give it a delicacy and grace that makes it an excellent text typeface. Titling and primary headings were set in Castellar, a Monotype typeface created by John Peters in 1957. Named after a town in the Alps, Castellar also was designed for refined display work. Tables were set in Gill Sans, designed by artist and type designer Eric Gill in 1931 for Monotype. Unlike many sans serif typefaces it is highly legible and readable in text. The cover was set in Californian, a typeface originally designed by Frederic Goudy in 1938 and adapted by various designers for the Font Bureau.

This publication was composed on an Apple iMac and a Macbook Pro using Adobe Systems InDesign. Masters were created in Adobe Acrobat. Illustrations were prepared in Omni Systems Omni Graffle and Adobe Photoshop.

Baskerville, Californian, Castellar, Gill Sans, iMac, Macbook Pro, Acrobat, InDesign, Omni Graffle, and Photoshop are registered trademarks of their respective companies.

Desktop composition by the author.

The cover was designed by Bridgette White.

Published by the National Defense Intelligence College Press, May 2006; and by the National Defense Intelligence College Foundation, March 2007. Printed at the Defense Intelligence Agency, Washington DC.

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE HANDBOOK 14-133

27 SEPTEMBER 2017

Intelligence

INTELLIGENCE ANALYSIS

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2OA

Certified by: AF/A2O
(Brig Gen Aaron M. Prupas)
Pages: 104

This Air Force Handbook (AFH) is the reference guide for conducting intelligence analysis as prescribed by Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources and Operations* and supports the operational requirements and processes outlined under Air Force Instruction (AFI) 14-133, *Intelligence Analysis* and AFI 14-134, *Intelligence Analysis Production and Requirements Management*. This publication provides the definitions, guidelines, procedures and tools for intelligence analysis operations. It has application and use for Regular Component, Air Force Reserve (AFR), Air National Guard (ANG), and Department of the Air Force (AF) Civilians, except where noted otherwise. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW the Air Force Records Disposition Schedule (RDS) in the Air Force Records Information Management System (AFRIMS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct supplements are routed to the OPR of this publication for coordination prior to certification and approval. Major Commands (MAJCOMs) need to provide a copy to the OPR upon publication. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the AF.

Chapter 1— OVERVIEW **5**

1.1. Purpose 5

1.2. Intelligence Analysis 5

1.3. Operational Viewpoint-1 (OV-1). 7

Figure 1.1. AF Intelligence Analysis OV-1. 7

Chapter 2— AF INTELLIGENCE ANALYSIS ENTERPRISE **9**

2.1. Analyst Airmen. 9

2.2. AF Intelligence Analysis Enterprise (AFIAE) 9

Figure 2.1. AFIAE. 9

2.3. Analysis Spectrum 10

Figure 2.2. AF Spectrum of Intelligence Analysis. 11

2.4. Characteristics 11

Table 2.1. Layers of Analysis. 12

Figure 2.3. Layered, Distributed, and Mutually Supporting Nature of AFIAE. 14

Chapter 3— THE NATIONAL INTELLIGENCE ANALYSIS COMMUNITY AND THE AIR FORCE **15**

3.1. The Intelligence Community. 15

3.2. Intelligence Analysis and the Joint Intelligence Process. 16

Figure 3.1. Joint Intelligence Process. 17

3.3. IC Funding. 18

3.4. Quality Analysis Programs 18

3.5. AF National Tactical Integration (AF NTI) 18

Chapter 4— ANALYSIS FUNDAMENTALS–ACTIVITIES, TENETS, & STANDARDS **20**

4.1. AF ISR Capabilities 20

Figure 4.1. Enduring GIISR Capabilities. 20

4.2. AF Intelligence Analysis Activities 20

Figure 4.2. AF Intelligence Analysis Activities. 21

Figure 4.3. AF Intelligence Analysis Continuum. 22

4.3. AF Intelligence Analysis Tenets. 22

4.4. AF Standards of Intelligence Analysis 23
4.5. Beyond the Checklist 24
4.6. AF Analytic Ombuds 25
Chapter 5— ANALYSIS SKILLS AND TRADECRAFT 26
5.1. Overview 26
Figure 5.1. Transforming Data to Decisions. 26
Figure 5.2. Relationship and Role of Intelligence Analysis Skills and Tradecraft. 27
5.2. Skills and Tradecraft Fundamentals 28
Figure 5.3. Fundamental Skills and Tradecraft of the Analysis Process. 29
Figure 5.4. SATs. 31
5.3. Key Analysis Concepts. 35
Figure 5.5. Data Analytics Framework. 36
Figure 5.6. Traditional Model for Target Discovery. 38
Figure 5.7. ABI/OBP Integrated Model for Target Discovery. 39
5.4. Additional Tradecraft Resources. 39
Chapter 6— REQUIREMENTS AND PRODUCTION 40
6.1. Intelligence Requirements and Analytic Focus. 40
6.2. Intelligence Production 42
Figure 6.1. Requirement–Production Cycle. 42
6.3. Request for Information (RFI) and Analysis/Production Process 43
Figure 6.2. RFI and Analysis/Production Process. 43
Figure 6.3. RFI and Analysis/Production Process across the AFIAE. 44
6.4. Acquisition Intelligence 44

Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 46

Attachment 2— PRODUCT AND SERVICE LINES 58

Attachment 3— COMMON ANALYSIS LESSONS 61

Attachment 4— SAMPLE STANDARDS EVALUATION METHODOLOGY 65

Attachment 5— AF ISR SAT TRADECRAFT GUIDE 69

Attachment 6— IC, DOD, AND MILITARY SERVICE REFERENCES 88

Attachment 7— ONLINE RESOURCES FOR ANALYSIS SKILLS AND TRADECRAFT. 92

Attachment 8— ANNOTATED BIBLIOGRAPHY 94

Chapter 1

OVERVIEW

1.1. Purpose.

1.1.1. The responsibilities of the intelligence analyst have never been more important. The increasingly complex global environment demands analyst Airmen be steeped in tradecraft fundamentals, conversant on the Intelligence Community (IC) and other service capabilities, and prepared to tailor their analysis skills to the operational challenge at hand. The purpose of this non-directive publication is to help guide every analyst Airman in answering this call. It provides reference and instructional material for the analyst Airman working in the air, space, and/or cyber domains—whether junior or seasoned; officer, enlisted, or civilian; regular AF, reserve or guard; and serving AF, joint, national, or combined missions. The content of this publication is intentionally broad in nature, ranging from foundational doctrine and tactics, techniques, and procedures (TTPs) to analysis applications and lessons learned.

1.1.2. The long-term intent for this publication is to have it reside as a series of interactive and up-to-date web pages online, with links to IC and AF directives, templates, checklists, and other references. The online version will serve as a useful tool for the analyst Airman to quickly link to their specific analysis topic of interest. Upon publication of this handbook, the AF intends to initiate steps to transition this document to an online, interactive version.

1.1.3. The publication is organized with foundational information in six main chapters followed by useful lists, lessons learned, criteria, forms, guides, and an annotated bibliography in the attachments to aid analyst Airmen in their day-to-day missions. This document also includes links to appropriate websites with additional support material.

1.2. Intelligence Analysis. Intelligence analysis is a cognitive capability—both art and science—applying tools, judgments, processes, and tradecraft to data and information to create and deliver new intelligence, insights, and knowledge, with the goal of providing decision advantage to commanders, decision makers, and intelligence customers. Analysis is foundational to ISR, a key capability of ISR, a core competency in ISR, and integral to Global Integrated ISR (GIISR).

1.2.1. Intelligence as a Foundation. Analysis is a significant capability that extends across all AF ISR Enterprise activities in support of the full range of military operations and assigned national security missions. According to AF/A2's vision for the future of AF Intelligence, *AF ISR 2023: Delivering Decision Advantage*, a "fundamental job of AF ISR Airmen is to analyze, inform, and provide commanders at every level with the knowledge they need to prevent surprise, make decisions, command forces, and employ weapons." AF intelligence analysis provides unique capabilities to focus on and address AF mission requirements. These same unique capabilities, coupled with an Airman's distinctive air/space/cyber perspective, serve to complement and fully integrate with analysis that supports broader defense and national mission requirements.

1.2.2. Intelligence Analysis as a Capability. Analysis is one of four enduring AF ISR capabilities, the other three being Collection Operations, Targeting, and Operations

Integration. **Note**: Refer to the *AF Future Operating Concept: A View of the AF in 2035*. The AF delivers intelligence analysis capability to meet Combatant Command (CCMD) and service needs. As with any other capability area, intelligence analysis is supported by the full range of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P).

1.2.2.1. Doctrine. Doctrinal considerations include analysis fundamental principles; analysis policy and procedures; common lexicon and terminology; recognized TTPs; and shared best practices and lessons learned.

1.2.2.2. Organization. AF ISR organizations range from the tactical to the strategic level, operating in a layered, distributed, and mutually supporting construct. AF initiatives to develop the intelligence analysis capability additionally impact the presentation of analyst Airmen to joint organizations such as combatant commands, joint task forces, and national analysis entities.

1.2.2.3. Training. Considerations include initial, mission, and continuation training; AF Specialty Code (AFSC) entry-, intermediate-, and advanced-level courses; and associated certification.

1.2.2.4. Materiel. Materiel concerns involve tools, technologies, systems, and architectures necessary to equip, operate, maintain, and support analysis activities.

1.2.2.5. Leadership and Education. The attention and priority of leadership is essential to growing the analysis capability. Additionally, undergraduate- and graduate-level education opportunities inside and outside of the AF play a major role.

1.2.2.6. Personnel. Planning and resourcing for qualified personnel are required to effectively conduct analysis missions.

1.2.2.7. Facilities. Cleared and adequately equipped buildings and other structures are required to conduct analysis.

1.2.2.8. Policy. Codified direction and guidance with clearly defined roles, responsibilities, processes, and terminology are fundamental to unity of effort across the AF ISR enterprise.

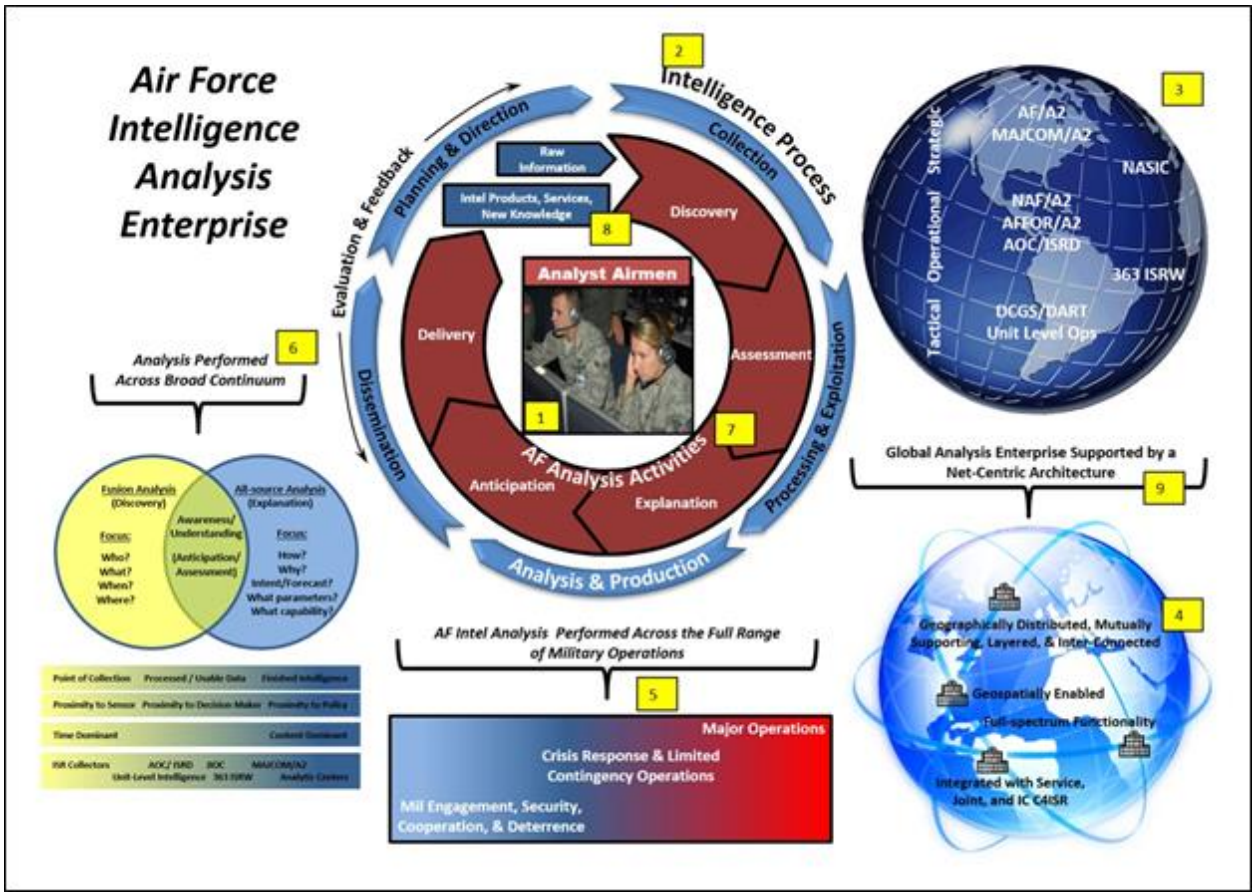
1.2.3. Intelligence Analysis as a Core Competency. ISR core competencies are the primary knowledge, skills, abilities, and behaviors required to perform AF ISR missions and ultimately enable decision advantage. The AF strives to collectively maintain sufficient expertise in its competencies. Because analysis is critical to and a driving factor in the other three enduring capabilities, all AF ISR professionals train in, maintain, and exercise, at a minimum, basic analytical capabilities and critical thinking skills wherever they are assigned. Additional information on this subject can be found in Career Field Education and Training Plan (CFETP) 14NX, Parts I and II, *AFSC 14NX Intelligence Officer Career Field Education and Training Plan* and CFETP 1N0X1, Parts I and II, *AFSC 1N0X1 All Source Intelligence Analyst Career Field Education and Training Plan*.

1.2.4. Intelligence Analysis and Global Integrated ISR (GIISR). As of 2017, GIISR is one of the AF's five enduring core missions as identified in strategic guidance, including the *AF Future Operating Concept* and the *USAF Strategic Master Plan*. A key strategic AF vector is to maintain a robust and flexible GIISR capability, supported by big data analytics. AF

strategic guidance highlights the need for the service to deepen its assessment of potential adversaries, professionalize ISR analysis, and restore analytic competencies. In turn, AF ISR vision and strategic planning establish analysis as one of five priorities for ISR and tie the AF's mandate to deliver decision advantage to its ability to provide world-class, multi- and all-source intelligence across all domains. Accurate, timely, relevant intelligence analysis is not only integral to operations, but in many ways drives military operational decisions.

1.3. Operational Viewpoint-1 (OV-1). Figure 1.1, *AF Intelligence Analysis OV-1*, offers a high-level depiction of AF intelligence analysis. The OV-1 describes analysis operations, capabilities, and activities within the greater AF ISR Enterprise and explains how analysis supports GIISR operations. Together, analyst Airmen and the AF Intelligence Analysis Enterprise (AFIAE) ensure mission success and decision advantage now and into the future. Subsequent chapters of this publication explain in more detail the various elements of the OV-1.

Figure 1.1. AF Intelligence Analysis OV-1.



1.3.1. As indicated by Item 1 in Figure 1.1, at the heart of AF intelligence analysis is the cadre of officer, enlisted, and civilian ISR professionals who are trained in intelligence analysis and production. These analyst Airmen apply critical thinking and advanced analytical skills to turn information and raw data into timely, actionable, and relevant intelligence products and services, leading to improved knowledge.

1.3.2. Analyst Airmen perform their missions within the framework of the overall joint intelligence process of Planning and Direction, Collection, Processing and Exploitation,

Analysis and Production, Dissemination and Integration, and Evaluation and Feedback (PCPAD), as Item 2 of Figure 1.1 illustrates.

1.3.3. Item 3 in Figure 1.1 indicates that AF intelligence analysis is nested within the larger AF ISR Enterprise, a Total Force construct extending from squadron to headquarters level and ranging from tactical to strategic focus.

1.3.4. As depicted in Item 4 of Figure 1.1, analyst Airmen and the AF ISR Enterprise are mutually supporting; unified in policy, authorities, tenets, and strategy; and skilled in employing tools that enable AF, joint, and IC operations.

1.3.5. Analyst Airmen are trained in the art and science of analytical tradecraft and apply common tenets and standards across the full range of military operations, from major theater warfare to humanitarian assistance and disaster relief, as depicted in Item 5 of Figure 1.1.

1.3.6. To support these operations, analyst Airmen engage in various types of analysis, ranging from fusion analysis to all-source analysis (ASA), as shown in Item 6 of Figure 1.1. Fusion analysis entails quickly melding new information with already established baseline knowledge to meet specific operational needs. Comprehensive ASA is often less time sensitive and more focused on studying and understanding long-term trends and maintaining a depth of knowledge on a given subject. Each organization within the AF ISR Enterprise conducts analysis across this continuum - at varying levels based on key intelligence questions and customer requirements - to fill a gap in knowledge, or a need to improve understanding of the threat environment and/or adversary capabilities.

1.3.7. Common analysis activities performed across the AF ISR enterprise include Discovery, Assessment, Explanation, Anticipation, and Delivery, which operate in parallel with the PCPAD process, as depicted in Item 7 of Figure 1.1. Analyst Airmen identify relevant information in support of ongoing operations and requirements, classify and categorize information, and create estimates of capabilities and impacts.

1.3.8. As Item 8 of Figure 1.1 indicates, the derived knowledge is used to create descriptions in greater context to provide indications and warning regarding a specific problem set. Intelligence products and services are developed, tailored, and presented according to key intelligence questions or customer requirements.

1.3.9. As shown in Item 9 of Figure 1.1, the AF intelligence analysis concept and the AF ISR Enterprise are interconnected by both a net-centric architecture and analytic toolsets that ensure critical interface among AF operational elements, Joint, and IC analysts, thereby ensuring access to all relevant data in a geographically-enabled and integrated manner.

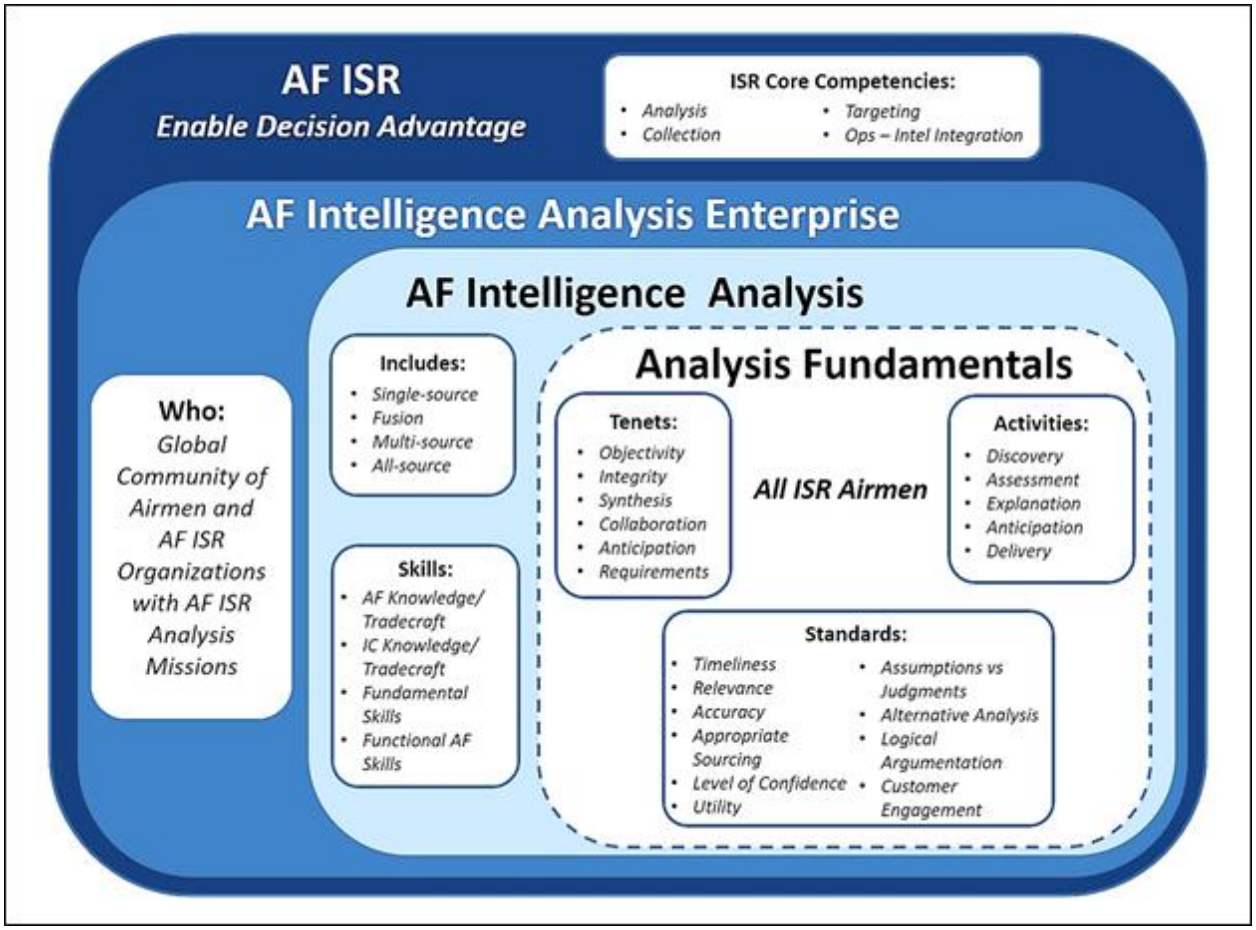
Chapter 2

AF INTELLIGENCE ANALYSIS ENTERPRISE

2.1. Analyst Airmen. An analyst Airman is an AF ISR professional who is skilled and qualified in tradecraft to perform the core competency of intelligence analysis across the air, space, or cyberspace domains. Certification criteria and programs vary based on unit and mission requirements. Analyst Airmen are bound by the professional standards for analysis established by the IC, and supplemented by AF standards and mission qualifications of the assigned ISR unit. Whether ISR professionals are analyst Airmen depends more on what they do than where they sit.

2.2. AF Intelligence Analysis Enterprise (AFIAE) . The enterprise is defined as the global community of analyst Airmen and the AF ISR organizations that employ the core competency of intelligence analysis. Figure 2.1, *AFIAE*, depicts how the AFIAE, intelligence analysis, and analysis fundamentals fit within the larger AF ISR Enterprise. Refer to **Chapter 4** for a detailed explanation of analysis fundamentals. Although not shown in Figure 2.1, the AF ISR Enterprise resides within the IC Enterprise. As a member of the IC, the AF contributes to IC analysis and production and also receives analysis and production support from other IC organizations.

Figure 2.1. AFIAE.



2.3. Analysis Spectrum . Analyst Airmen employ fundamental tenets, standards, and activities to perform analysis across a broad continuum for mission accomplishment. On one end of the analysis continuum are fusion and single-source analysis, with emphasis on timeliness over completeness. On the other end of the spectrum is comprehensive ASA, with less emphasis on rapidity, and greater emphasis on analytic content, depth, trends, technical, and other subject-matter expertise. This spectrum is depicted in Figure 2.2, *AF Spectrum of Intelligence Analysis*.

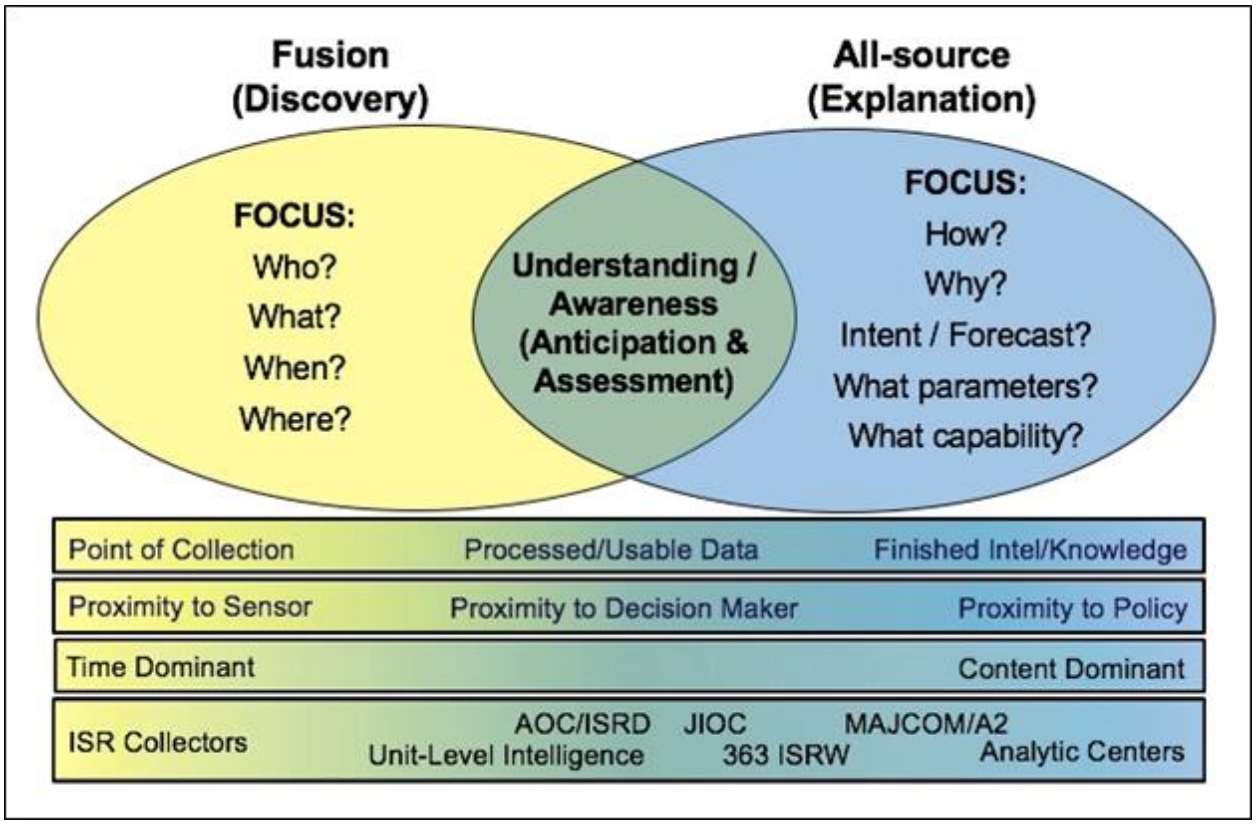
2.3.1. Single-Source Analysis (also called Exploitation). Intelligence analysis that employs a single source or expertise in a functional area to characterize events, people, or things. Such analysis is limited to describing, rather than evaluating, the topic of a particular analysis due to restrictions inherent in single-source intelligence collection, precluding the ability to provide fully contextualized intelligence assessments.

2.3.2. Fusion Analysis. Analysis in a time-sensitive environment in close proximity to the point of collection that entails quickly melding new information with baseline knowledge to meet a specific operational need. **Note:** Proximity does not refer to physical or geographic location but rather functional proximity to the collection step in the intelligence process (for example, a Distributed Common Ground System (DCGS) Analysis and Reporting Team (DART) at Beale AFB may conduct fusion analysis of an operational area on the opposite side of the globe). Emphasis is on the process of managing information and on timeliness over completeness. Fusion analysis generally has three components: 1) it usually includes more than one source; 2) it is time critical; and 3) it is performed to meet a commander's requirements or specific operational need.

2.3.3. Multi-Source Analysis (also called Multi-Intelligence (INT) Analysis). Intelligence analysis that makes use of more than one source when access to additional potential sources is limited by reasons of timeliness, system access, location, or security levels.

2.3.4. All-Source Analysis (ASA). Intelligence analysis that employs all available sources of data and information to enable the creation of new intelligence and knowledge.

Figure 2.2. AF Spectrum of Intelligence Analysis.



2.3.5. At the far left of the graphic, intelligence analysis units, such as AF DARTs, provide near-real-time (NRT), multi-source fusion analysis closest to the point of collection to improve collection, perform dynamic targeting, and support tactical warfighters. Moving to the right across the spectrum, the Air Operations Centers' (AOCs) ISR Divisions (ISRD), Joint Intelligence Operations Centers (JIOCs), and IC organizations provide multi-source and ASA with fewer time constraints and in close proximity to strategic-level commanders and decision-makers to facilitate battlespace awareness, operations planning and sustainment, and policy decisions. Since the late 1990s, changes in technology, operational needs, and CCMD requirements have blurred the once distinct lines of this analysis spectrum. Today AFIAE organizations have evolved to delivery across the spectrum – rather than delivering within any single niche.

2.4. Characteristics of the AF Intelligence Analysis Enterprise (AFIAE).

2.4.1. Layered. Intelligence analysis capabilities reside at multiple levels of command—unit, (squadron, group, wing), Numbered AF (NAF), MAJCOM, and AF-level. Additional levels, including joint and Department of Defense (DoD), exist beyond the AF. Table 2.1, *Layers of Analysis*, identifies the various layers of analysis organizations along with their general analytical focus, typical customers, and timeliness, as modern processes and technologies enable organizations to extend their focus and timelines outside traditional norms. While representative, this table is not a complete listing of all AF analysis organizations.

Table 2.1. Layers of Analysis.

Organization	Focus	Customer	Timeline
CSA (DIA, NSA, NGA, NRO)	Strategic	National leadership, DoD, IC	Days/Months; Mission dependent RT/NRT
CCMD JIOC/JTF	Strategic/Operational	CCMD, Joint forces	Days/Months
Service Intelligence Center (NASIC)	Strategic/Operational/ Tactical	National leadership, CCMD, JTF, DoD, IC, AF all levels, acquisition community	Hours/Days/Months
MAJCOM/A2	Strategic/Operational	MAJCOM staff and supported units	Days/Months
Acquisition Centers	Strategic/Operational	AF/IC leadership, MAJCOMs, acquisition program/project mgrs	Days/Months
NAF/A2, AFFOR/A2, AOC ISR Division	Operational/Tactical	CCMD, JTF/Joint forces, AF NAF and below units	Hours/Days
ISRW	Operational/Tactical	NAF and below units	Hours/Days/Months
DCGS	Operational/Tactical	CFACC, JTF, DoD, IC, AF units	RT/NRT to 72 Hours
Unit Level Intel & RPA SOC	Tactical	AF and other service units	RT/NRT to 72 Hours

AF: Air Force
A2: Director of Intelligence
AFFOR: Air Force Forces
AOC: Air Operations Center
CCMD: Combatant Command
CFACC: Combined Forces Air Component Commander
CSA: Combat Support Agency
DCGS: Distributed Command Ground System
DIA: Defense Intelligence Agency
DoD: Department of Defense
IC: Intelligence Community
ISR: Intelligence, Surveillance & Reconnaissance
ISRW: ISR Wing
JIOC: Joint Intelligence Operations Center
JTF: Joint Task Force
MAJCOM: Major Command
Mgrs: Managers
NAF: Numbered Air Force
NASIC: National Air and Space Intelligence Center
NGA: National Geospatial-Intelligence Agency
NRO: National Reconnaissance Agency
NRT: Near-real-time
NSA: National Security Agency
RPA: Remotely Piloted Aircraft
RT: Real-time
SOC: Squadron Operations Center

2.4.1.1. Starting at the bottom of Table 2.1, unit-level intelligence organizations focus on tactical analysis needs (e.g., location, movement, and readiness of enemy forces) for their tactical-level customers in the AF and other services. Unit-level intelligence organizations typically operate under short timelines from real-time or NRT to several days out.

2.4.1.2. DCGS units are tactically and operationally focused. Within each DCGS unit, the DART conducts analysis for their respective CFACC as well as other IC and DoD customers. DARTs operate in a time sensitive environment but can support the customer up to the operational level of ISR planning. Their main emphasis is fusion analysis.

2.4.1.3. ISR wings provide both operational and tactical level intelligence analysis, with timelines ranging from hours to months. In particular, the 363 ISR Wing (ISRW) is dedicated to providing all-source analysis and targeting intelligence to NAFs and below across the entire AF.

2.4.1.4. NAF/A2s, AF Forces (AFFOR)/A2, and AOC ISRDs are operationally and tactically focused in support of their associated CCMD, their joint task force (JTF), and/or their units. Their typical timelines are hours to days.

2.4.1.5. Intelligence offices within Acquisition Centers, such as the Space and Missile Systems Center (SMC), AF Life Cycle Management Center (AFLCMC) and AF Research Laboratory (AFRL), provide both strategic and operational intelligence for acquisition program managers, project managers, MAJCOMs, and AF/IC leadership, with timelines that range from days to months.

2.4.1.6. MAJCOM/A2s provide strategic and operational analyses for their MAJCOM staff and supported units, usually ranging from days to months. The Air Mobility Command (AMC)/A2 is unique in that its Air Intelligence Squadron (AIS) and the 204th Intelligence Squadron (ANG) provide direct analytic support to 18 AF and subordinate units in the conduct of their rapid global mobility missions. Additionally, U.S. Air Forces in Europe & Air Forces Africa (USAFE-AFAFRICA) and Pacific Air Forces (PACAF) are unique as Component MAJCOMs (C-MAJCOMs) in that they have the responsibility of analytically representing the Joint Force Air Component Commander to the Joint Force Commander.

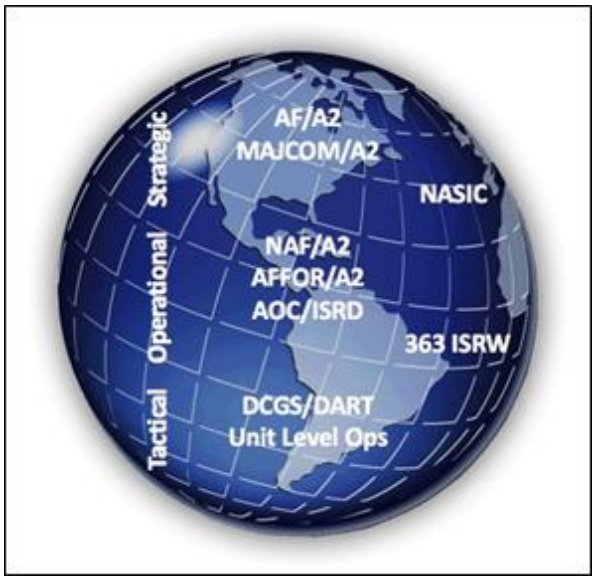
2.4.1.7. The National Air and Space Intelligence Center (NASIC**)** conducts strategic, operational, and tactical analysis for a broad range of customers in the AF, DoD, and IC as well as and including national leadership and the acquisition community. Their timelines extend from short-term to long-term, depending on the customer's needs. Whereas the 363 ISRW is the primary AF organization that conducts tactical intelligence analysis, NASIC is the primary AF organization focused on strategic intelligence. Both the 363 ISRW and NASIC provide significant analysis at the operational level, as well. Further, while other AF layers conduct analysis as part of their mission, analysis is a primary mission of the 363 ISRW and NASIC.

2.4.1.8. Joint intelligence organizations at CCMDs and JTFs conduct strategic and operational analysis in support of their respective regional and functional commands. The timelines of their analysis range from days to months.

2.4.1.9. Combat Support Agencies (CSAs) focus primarily on strategic analysis for national leadership, DoD, and the IC. Although they usually operate on timelines ranging from days to months, they also provide real-time and near-real-time analysis as requirements dictate.

2.4.2. Distributed and Mutually Supporting. In addition to being layered, analysis responsibilities are distributed across geographic regions and functional areas in the AF (see Figure 2.3, *Layered, Distributed, and Mutually Supporting Nature of AFIAE*). Analysis organizations in every layer and every region/function are interconnected and have access to each other. Organizations collaborate and share expertise to ensure the most accurate, timely analysis is provided to answer intelligence requirements. The mutually supporting nature of the AFIAE includes enterprise partners, such as the AF Office of Special Investigations (AFOSI).

Figure 2.3. Layered, Distributed, and Mutually Supporting Nature of AFIAE.



Chapter 3

THE NATIONAL INTELLIGENCE ANALYSIS COMMUNITY AND THE AIR FORCE

3.1. The Intelligence Community. The IC is a coalition of 17 agencies and organizations, including the Office of the Director of National Intelligence (ODNI), within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities. See Attachment 6, Table A6.1, *Members of the IC*, for a complete list of IC organizations.

3.1.1. The Director of National Intelligence (DNI) has overall responsibility for intelligence support to the President and the day-to-day management of the IC. AF analysis falls under the governance and direction of the DNI. The AF is an active participant in governance and oversight forums and follows the analytical priorities, standards, processes, and procedures established by the IC. The DNI issues guidance for analysis and production through IC Directives (ICDs), IC Standards (ICSs), DNI memorandums, and other directive documents. The IC documents that most often impact AF analysis are identified in Attachment 6, Table A6.2, *Common IC and DoD Analysis References*.

3.1.2. DoD Intelligence.

3.1.2.1. The Secretary of Defense (SecDef) is responsible for the DoD portion of the IC. The Under Secretary of Defense for Intelligence (USD(I)) serves as the senior defense intelligence, counterintelligence, and security official below the SecDef and Deputy SecDef. For defense intelligence analysis the USD(I):

3.1.2.1.1. Provides oversight and direction for analysis capabilities to ensure effective support to the DoD mission.

3.1.2.1.2. Ensures analysis is aligned with IC and DoD analytical concepts, methodologies, and priorities.

3.1.2.1.3. Establishes DoD all-source analysis policy and oversees the implementation of DoD all-source analysis plans, programs, and performance.

3.1.2.1.4. Provides strategic guidance to the Defense Intelligence All-Source Analysis Enterprise (DIAAE), the collective set of all DoD organizations that execute all-source analysis activities in production of defense intelligence.

3.1.2.1.5. Develops and maintains the consolidated set of Defense Intelligence priorities that guides DIAAE analysis and reflects the intelligence needs of all Defense Intelligence consumers.

3.1.2.1.6. Establishes the DIAAE Board of Governors (BOG), a body of representatives from the DIAAE organizations that provides a forum for addressing issues, improving transparency, implementing strategies, and making resource recommendations across the DIAAE.

3.1.2.2. The AF participates in the DIAAE BOG and other DoD analysis forums and adheres to DoD analysis-related policies. Within the DoD, the agency with the largest responsibility for promulgating ASA guidance is the Defense Intelligence Agency (DIA).

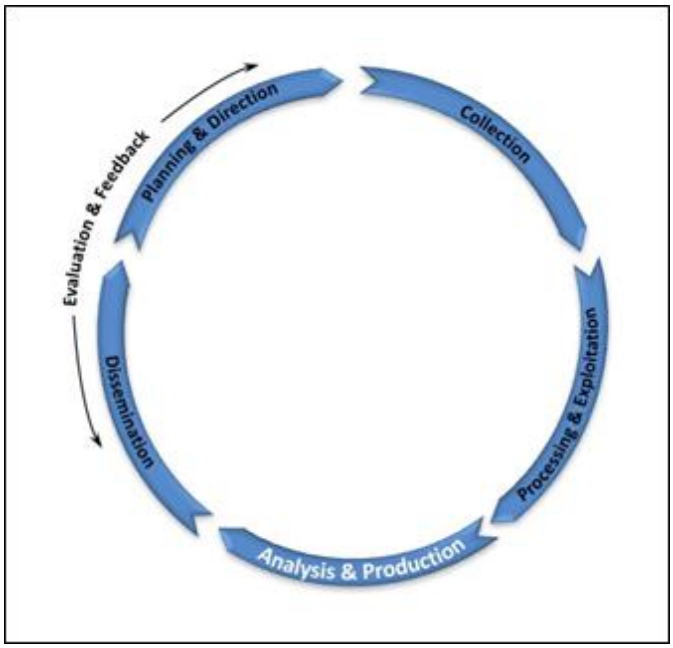
DIA governs ASA responsibilities, policies, priorities, and relationships across the DoD IAW DoD Instruction (DoDI) 3115.17 and as the DoD Functional Manager for ASA. Additionally, DIA manages the Defense Intelligence Analysis Program (DIAP), with the primary goal of maximizing enterprise efficiencies through clearly defined ASA and production responsibilities among DIA, CCMDs, and service intelligence centers.

3.1.2.3. In addition to ASA and production conducted within the DIAP, the AF conducts single-source analysis, e.g., signals intelligence, human intelligence, geospatial intelligence, etc., that is additionally governed by directives established by respective lead DoD agencies. AF production that supports these single-source disciplines adheres to AF guidance as well as standards set forth by the respective DoD lead agencies. Further, the DoD has established overarching policy related to acquisition intelligence, to which the AF adheres. If a conflict arises between the AF and IC agency guidance, IC guidance takes precedence. See Attachment 6, Table A6.2, *Common IC and DoD Analysis References*, for a list of common DoD analysis-related documents.

3.1.3. Military Services. Each military service has a senior intelligence officer (SIO) that oversees intelligence policy, planning, programming, and activities on behalf of the service chief. The AF SIO is the Deputy Chief of Staff (DCS) for ISR, also known as the AF/A2. Each service is authorized one service intelligence center, also called an intelligence analysis center. The AF's service intelligence center is NASIC. The AF has assigned the Air Combat Command (ACC) as its lead MAJCOM for the GIISR capability, which includes intelligence analysis. Similarly, other military services have assigned significant analysis responsibilities to various organizations. All services routinely reach out to each other for service-unique expertise and collaboration in addressing analysis requirements. Refer to Attachment 6, Table A6, *Major Intelligence Analysis Entities of the Military Services*, and Table A6.4, *Common Analysis Organizations*, for a breakdown of the major intelligence analysis entities in each military service and a list of service and other government agencies organized according to the primary analysis they conduct.

3.2. Intelligence Analysis and the Joint Intelligence Process. As highlighted in Joint Publication (JP) 2-0, *Joint Intelligence*, the intelligence process is comprised of six interrelated categories, collectively referred to as PCPAD. Refer to Figure 3.1, *Joint Intelligence Process*, for a graphic depiction of the PCPAD cycle. The PCPAD process is universally recognized throughout the IC and linked to the DoD Joint Capability Area (JCA) of Battlespace Awareness. JCAs provide a common framework for defining needs, analyzing operational gaps, and conducting planning and, by extension, programming for DoD capabilities.

Figure 3.1. Joint Intelligence Process.



3.2.1. Planning and Direction is dependent on the ability to synchronize and integrate the activities of collection, processing, exploitation, analysis and dissemination resources to meet Battlespace Awareness information requirements. Planning and direction activities include, but are not limited to: the identification and prioritization of intelligence requirements; the development of concepts of intelligence operations and architectures required to support the commander's mission; tasking subordinate intelligence elements for the collection of information or the production of finished intelligence; submitting requests for additional capabilities to higher headquarters; and submitting requests for collection, exploitation, or all-source production support to external, supporting intelligence entities. Planning and direction occurs continuously and allows for the prioritization of intelligence support across all ongoing operations and simultaneous planning efforts.

3.2.2. Collection is the ability to gather data and obtain required information to satisfy requirements. Collection is managed by collection managers, whose duties include identifying the most appropriate available assets and then tasking those assets to conduct collection missions. Collection managers also develop and coordinate sensor employment guidance, exercise authoritative control of specific collection operations, revise collection activities as required, monitor the overall satisfaction of requirements, and assess the effectiveness of the collection plan to satisfy the original and evolving intelligence need.

3.2.3. Processing and Exploitation involves the transformation of collected information into formats suitable for further analysis and/or action by man or machine. During processing and exploitation, raw collected data are converted into forms that can be readily used by commanders, decision-makers at all levels, intelligence analysts, and other consumers. Processing and exploitation includes first-phase imagery exploitation, data conversion and correlation, document and media translation, and signal decryption, as well as reporting the results of these actions to analysis and production elements.

3.2.4. Analysis and Production involves the integration, evaluation, and interpretation of information obtained from available sources to develop intelligence and forecast the future state to enable situational awareness and provide new knowledge/actionable information. The AF has identified five activities that occur within this category of the PCPAD process: Discovery, Assessment, Explanation, Anticipation, and Delivery. See **Chapter 4** for a description of each, along with an explanation or how it relates to broader AF ISR activities, and the tenets and standards to which analyst Airmen adhere in order to carry out these five analysis activities.

3.2.5. Dissemination and Integration focuses on the ability to present, distribute, or make available to military and national decision-makers the intelligence, information and environmental content and products that enable understanding of the operational/physical environment. Personal, networked, and database data transfers are all means of dissemination. The diversity of dissemination paths requires a high degree of communications and system interoperability among joint and multinational forces, component commands, DoD organizations, and the interagency community.

3.2.6. Evaluation and Feedback occur continuously throughout the intelligence process. It requires a collaborative dialogue among intelligence planners, collection managers, collectors, analysts, intelligence systems architects, and customers. The intent of evaluation and feedback is to identify potential problems as early as possible to minimize information gaps and mitigate capability shortfalls.

3.2.7. Although “analysis” is specifically identified in the Analysis and Production category of PCPAD, most intelligence analysts agree that analysis takes place in all categories of the joint intelligence process.

3.3. IC Funding. The National Intelligence Program (NIP), administered by the DNI, provides guidance and funding for a broad range of ISR activities within the IC. NIP is divided into sub-programs, including the General Defense Intelligence Program (GDIP) for ASA and other specific intelligence activities, the Consolidated Cryptologic Program (CCP) for signals intelligence activities, and the National Geospatial-Intelligence Program (NGP) for geospatial intelligence activities. Some AF intelligence organizations receive funding through these NIP sources for certain single-source and ASA missions and are required to adhere to the analysis and production guidelines and standards associated with the funding. However, the majority of AF analysis activities, particularly at and below wing level, are funded through the Military Intelligence Program (MIP) for mission execution. For details, refer to ICD 104, *National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation* and DoDD 5205.12, *Military Intelligence Program (MIP).*

3.4. Quality Analysis Programs . The IC and AF offer a variety of analyst enrichment opportunities to broaden and deepen an analyst's experience and expertise. Some examples include the AF Quality of Analysis Program, DNI Quality of Analysis Program, National Intelligence University, DIA's Intelligence Community Advanced Analytical Program, and the AF Institute of Technology.

3.5. AF National Tactical Integration (AF NTI) . The AF NTI program integrates U.S. Signals Intelligence (SIGINT) System resources with theater air and space components to ensure seamless support. The AF NTI team shifts the focus of national SIGINT performance from discovering and reporting data to collaboratively generating actionable intelligence for the Joint

Force Air Component Commander. The AF NTI team capitalizes on data acquisition capabilities, existing databases and datalinks of multiple national SIGINT sources, and access to AF analysts in the AOC, National Cryptologic Centers, and AF intelligence production organizations (e.g., NASIC). While the program remains predominately SIGINT focused, the AF NTI enterprise also has the ability to leverage all AF ISR capabilities. **Note**: Refer to AF ISR Agency Instruction (AFISRAI) 14-153 Volume 3, 480 ISRW Supplement, *Air Force Distributed Common Ground System (AF DCGS) Operations Procedure*s.

Chapter 4

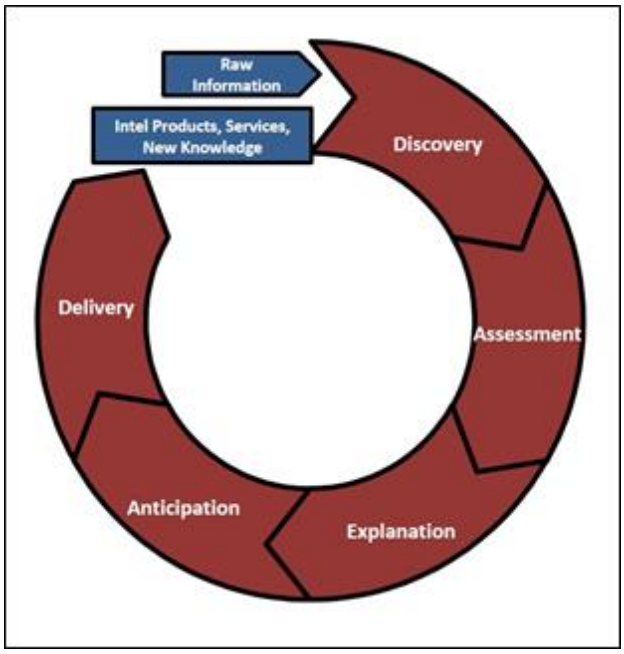
ANALYSIS FUNDAMENTALS–ACTIVITIES, TENETS, & STANDARDS

4.1. AF ISR Capabilities . The AF *GIISR Core Function Concept* highlights five enduring core capabilities (refer to Figure 4.1, *Enduring GIISR Capabilities*) that directly support the JCA of Battlespace Awareness. As previously mentioned, this JCA delineation is key for defining analysis-specific needs, analyzing gaps, and for planning and programming against AF analytic requirements. Similar to the joint PCPAD intelligence process discussed in **Chapter 3**, analysis is an essential and integral component of each of the five enduring GIISR capabilities.

Figure 4.1. Enduring GIISR Capabilities.

4.2. AF Intelligence Analysis Activities . As depicted in Figure 4.2, *AF Intelligence Analysis Activities*, analyst Airmen commonly perform five activities in support of the GIISR enduring capabilities mentioned above.

Figure 4.2. AF Intelligence Analysis Activities.



4.2.1. Discovery is the ability to research, select, manipulate, and correlate data from multiple sources to identify information relevant to ongoing operations and requirements. Discovery is about researching, better organizing, and using the data we already possess; it is also about finding previously hidden patterns and anomalies.

4.2.2. Assessment is the ability to provide focused examination of data and information about an object or an event, to classify and categorize it, and to assess its reliability and credibility in order to create estimates of capabilities and impacts. Assessment is how intelligence determines what our consumers ought to be concerned with.

4.2.3. Explanation is the ability to examine events and derive knowledge and insight from the interrelated data in order to create descriptions and propose significance in greater context. Explanation is how intelligence provides consumers with narrative stories, relates events to broader situations, and identifies the core of "what is going on."

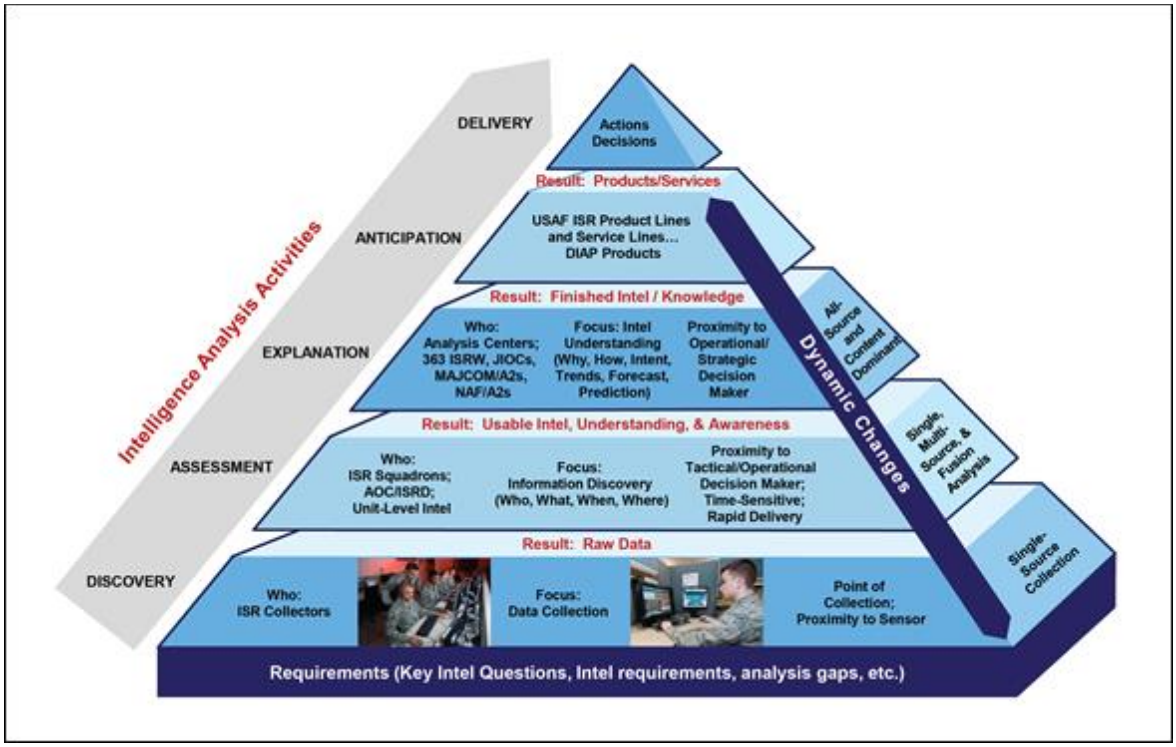
4.2.4. Anticipation is the ability to warn and describe future states of the environment based on the manipulation and synthesis of past and present data. Anticipation includes near-term warning and longer-term forecasting to alert and prepare decision makers for events that could be relevant to their responsibilities.

4.2.5. Delivery is the ability to develop, tailor, and present intelligence products and services according to customer requirements and preferences. Delivery is about classic intelligence products—from tactical reports to in-depth intelligence estimates—and a myriad of intelligence services, ranging from interactive displays and operational pictures, to multimedia crew threat briefings and tablet-embedded, dynamic intelligence assessments, enabling real-time analyst response to requests for information. Delivery is often referred to as production and/or dissemination.

4.2.6. As Figure 4.3, *AF Intelligence Analysis Continuum*, depicts, analysis activities take place across a continuum within the AF, starting with the development of requirements;

progressing through data collection, information discovery, and intelligence understanding; and culminating in services and products that impact commanders' decisions and military actions.

Figure 4.3. AF Intelligence Analysis Continuum.



4.3. AF Intelligence Analysis Tenets. AF tenets of analysis derive from and support IC, joint intelligence, and broader ISR principles, while simultaneously emphasizing analysis attributes of particular interest and priority within the AF. These are the overarching principles held to be true and in common by AF ISR professionals. Collectively, these six tenets cover the most important beliefs about AF intelligence analysis. According to AFI 14-133, while effort should be taken to apply all of these tenets, situations may dictate not all of them being used. The following descriptions are excerpts from AFI 14-133.

4.3.1. Objectivity. Analysis should be based on fact and be clear and truthful about what is *known versus what is judged*. It should *not be distorted by emotion or personal or organizational bias* and shall *be independent of command or political considerations*. Further, it should clearly delineate underlying intelligence, assumptions, and judgments. Analysts should address alternative perspectives and contrary information and avoid being unduly constrained by previous judgments.

4.3.2. Integrity. While closely linked to objectivity, integrity involves a broader focus on all activities, standards, and processes associated with AF intelligence analysis. Integrity calls for *complete honesty* and *reliability in analysis* combined with firm adherence to a code of *professional ethics* and *tradecraft standards* such as *accuracy, timeliness,* and *customer responsiveness*. Integrity includes explaining changes in previous analytic judgments, as well as addressing significant differences in judgment among various U.S. analytic elements.

As stated in JP 2-0, integrity is "the cardinal element in intelligence analysis and reporting, and the foundation on which credibility with the intelligence consumer is built."

4.3.3. Synthesis. AF intelligence analysis requires analysts to *use all available sources of information to maximize completeness*. Analysts should also identify information gaps and, where they exist, they should coordinate with collectors to develop access and collection strategies. Synthesis requires well-honed tradecraft skills, including critical thinking, alternative analysis, and the ability to take the perspective of the adversary. Compatible, service-oriented information technology architectures and tools are also key to facilitating synthesis.

4.3.4. Collaboration. Analysts must *actively solicit opinions and assessments from other analysts and seek to share ideas*. Data, information, and intelligence must be broadly accessed and shared. *Collaboration* should take place internally within the AFIAE, across the IC, and with allies, academia, and other entities outside the IC, when feasible. *Effective collaboration facilitates maximum synthesis*.

4.3.5. Anticipation. Analysis is far more than trend assessment; its true *value resides in warning* and forecasting to be relevant to *decision making, warfighting, operations,* and *acquisition*. Because *information gaps routinely limit our ability to predict with complete accuracy,* it is incumbent on analysts to effectively apply tradecraft standards such as alternative analysis, levels of confidence, assumptions vs. judgments, and appropriate sourcing. Intelligence warning and forecasting are not exact; however, analysts should utilize the most recent data/information for all warning or forecast-related analysis.

4.3.6. Requirements. The AF intelligence analysis mission is motivated by *continuous engagement with customers* to comprehend dynamic needs. Customer requirements can be solicited from a variety of sources such as: understanding their operations; holding working groups or technical exchanges with them; anticipating and listening to their questions; responding to feedback; and addressing documented need statements and derivative data needs. Effectively meeting analysis mission requirements demands an effective balance of customer familiarity, interpreted needs, collaboration, and analytical judgment.

4.4. AF Standards of Intelligence Analysis . The AF has established ten standards by which it measures and assesses analytic excellence and readiness. AF tradecraft standards align with IC standards; however, the AF incorporates two additional attributes: timeliness and customer engagement. AF standards also are in parallel with joint intelligence and GIISR guidance. These standards are used by the AF ISR Enterprise to conduct analysis operations and are integrated into AF Inspection System criteria. Attachment 4 contains a sample methodology and form to evaluate these standards. The following descriptions are excerpts from AFI 14-133. Refer to the AFI for additional details.

4.4.1. Timeliness. Analysis *must be timely* to impact planning, mission objectives, operations and otherwise aid in commanders' decisions. The aim is to deliver information and knowledge at the earliest time and place to enable customers to effectively make decisions and take action.

4.4.2. Appropriate Sourcing. Analysis *cites all sources used,* when feasible, and includes an *objective assessment of the quality, credibility, and reliability of the underlying sources*.

4.4.3. Accuracy. Analysis will *make the most accurate judgments and assessments possible*, based on the intelligence available and in light of known information gaps. A retrospective assessment of the accuracy of a judgment will help identify biases and other potential tradecraft errors for correction in future analysis.

4.4.4. Level of Confidence. To help qualify accuracy and to present analysis in a uniform and consistent manner across the AF, analysts will *indicate the degree of confidence/certainty* associated with analytic judgments and conclusions to the best of their ability, given currently available intelligence. AFI 14-133, Table 3.1, *Confidence Levels in Analytic Judgment*, provides guidance for analysts to use in assigning levels of confidence/certainty.

4.4.5. Assumptions vs. Judgments. Analysis *clearly distinguishes among underlying intelligence, analyst assumptions, and analyst judgments*.

4.4.6. Alternative Analysis. Analysis will *incorporate plausible alternative assessments,* judgments, or hypotheses, *particularly when major judgments contend with significant uncertainties, complexity, or a lack of available intelligence*, or when low probability events could produce high impact results. Whenever possible, analysis should be vetted through at least one other intelligence professional to minimize individual analyst bias.

4.4.7. Relevance. *Analysis is key to decision making*, warfighting, and acquisition efforts. Analysts should make every effort to ensure products and services fulfill the customer's intent and request, while also ensuring products and services are available to others for use beyond the original intent.

4.4.8. Logical Argumentation. Analysis will employ coherent and logical reasoning techniques, be supported by all key relevant information, and be internally consistent.

4.4.9. Utility. AF analytic products and services will *use formats* (written, verbal, visual, etc.) *that best enable understanding by the customer*. Intelligence analysis will be disseminated at the lowest classification and widest releasability levels without jeopardizing its usefulness to the customer.

4.4.10. Customer Engagement. Analysis should fully address customer requirements within time constraints and in a manner most useful. Analyst Airmen will be responsive to customer feedback. While challenging to evaluate, this tradecraft standard is foundational to AF intelligence analysis.

4.5. Beyond the Checklist . The list of analysis activities, tenets, and standards lend themselves to a checklist mentality. This is especially true with the standards, that are the criteria by which the AF evaluates analytical readiness. However, it is vital to remember that intelligence analysis is ***not just a science but also an art***. Following good tradecraft practices aids in developing a sound analytic process and foundation. However, the analyst cannot become paralyzed in making an assessment if all the tradecraft pieces do not fully align. Mistakes will be made – have been made – but we cannot fail to provide decision makers with our best assessment based on what information we had at the time. The analyst Airman learns the fundamentals but then spends many hours of intense effort honing and refining application of the fundamentals in the determined pursuit of excellence. Analysts need to express interest in the analysis activities and be eager to revisit any or all of them for the sake of providing more accurate, mission-relevant analysis for each customer requirement. Analysts need to embrace the

tenets and standards such that they become an intuitive and natural part of all analytical activities. Analysts, supervisors, and commanders also need to hold each other accountable to the tenets and standards.

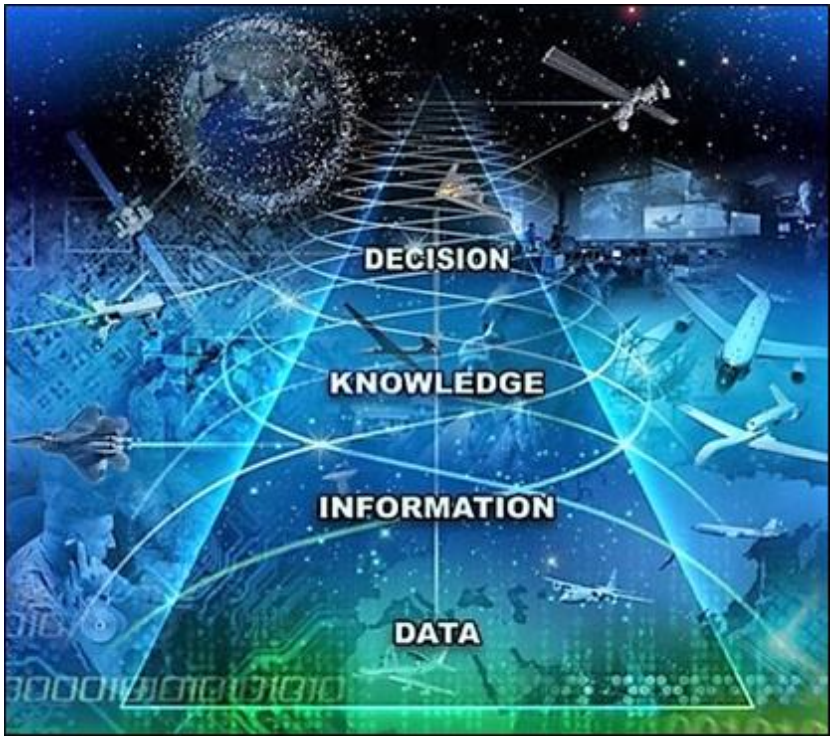
4.6. AF Analytic Ombuds . The AF Analytic Ombuds is the AF representative that responds to concerns raised by intelligence analysts about adherence to AF analysis tenets, standards, and production guidelines. The Ombuds addresses such concerns as lack of objectivity, bias, politicization, or other issues in applying analysis tenets and standards. The AF/A2 appoints the AF Analytic Ombuds in accordance with DNI guidance. In addition, NASIC and each MAJCOM/A2 designate an individual or office to serve as their organization's Analytic Ombuds IAW AFI 14-133.

Chapter 5

ANALYSIS SKILLS AND TRADECRAFT

5.1. Overview. Intelligence analysis is what transforms data into the information and knowledge necessary for warfighters and decision makers to decide and act (refer to Figure 5.1, *Transforming Data to Decisions*). While technology can assist and enable these transformations of data, without human cognition (people "in-the-loop") it is doomed to fail. There are things technology alone is not capable of. The things technology can do depend upon human analysts creating and updating the analytic models, databases, and displays that can be automated or made more efficient. The most basic and necessary unit in intelligence analysis is the analyst. **Note:** Attachment 7 identifies some online resources that contain additional information on analysis skills and tradecraft topics covered in this chapter.

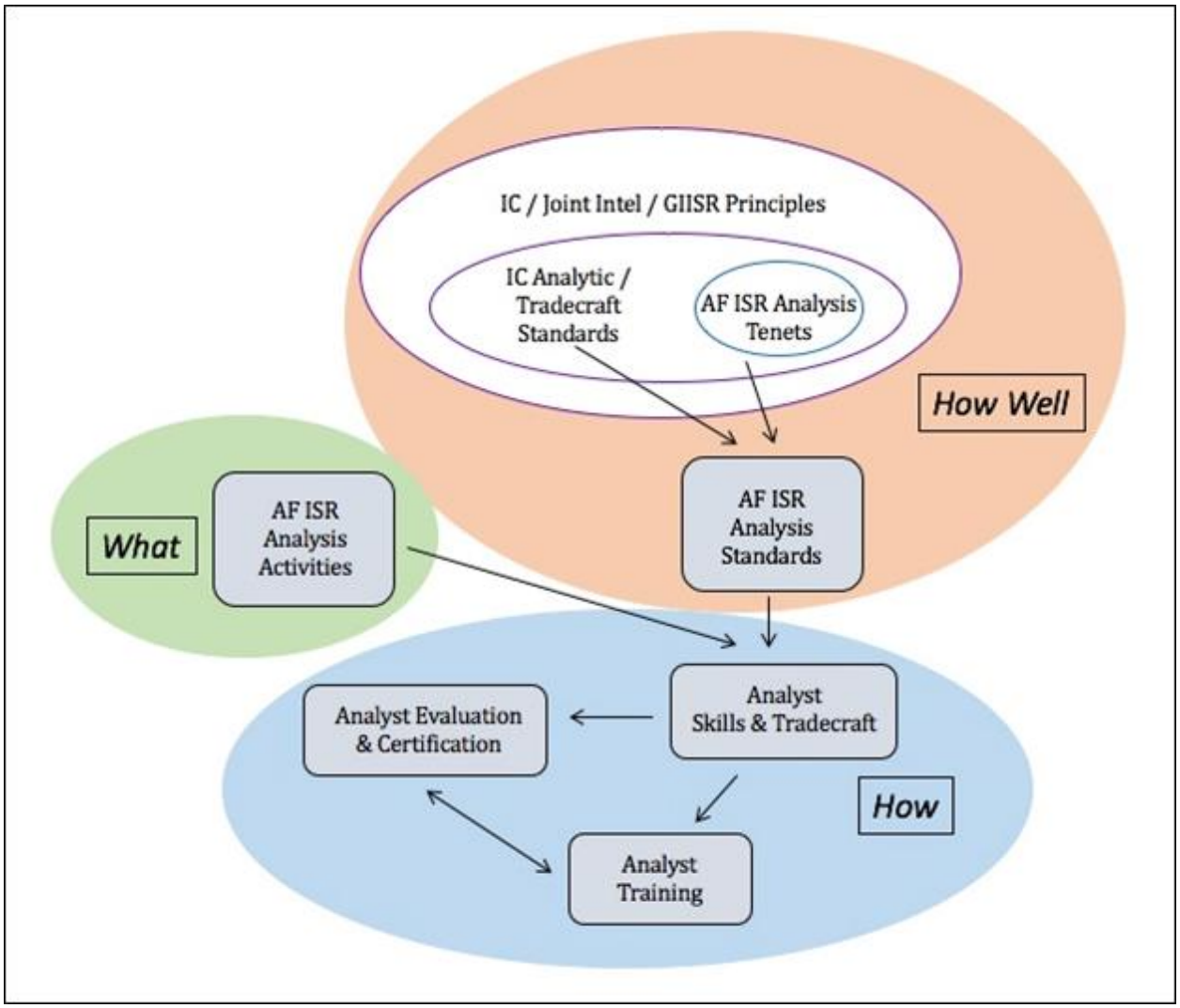
Figure 5.1. Transforming Data to Decisions.



5.1.1. Definitions and Relationships. An analysis skill is a specific ability or collection of capabilities required to competently conduct analysis that is acquired through training and/or experience. Analysis tradecraft is an established or prescribed analysis technique, practice, or systematic process. The relationship and role of intelligence analysis skills and tradecraft is illustrated in Figure 5.2, *Relationship and Role of Intelligence Analysis Skills and Tradecraft*. Whereas the five AF intelligence analysis activities (discovery, assessment, explanation, anticipation, and delivery) comprise "what" analyst Airmen do and analysis tenets/standards establish how well analysis is done, analysis skills and tradecraft are the "how" of analysis. Analysis activities, tenets, and standards drive the skills and tradecraft for which analyst Airmen need to be trained. In turn, analysis skills and tradecraft determine training, evaluation, and certification requirements. Analyst skills and tradecraft highlighted

in this publication are time-tested, repeatable, and proven effective for structured AF intelligence analysis.

Figure 5.2. Relationship and Role of Intelligence Analysis Skills and Tradecraft.



5.1.2. Analysis Transformation.

5.1.2.1. In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA) in response to several commissions and hearings in the aftermath of 9/11. That act is known for establishing the ODNI; however, the act also set forth a number of tasks and objectives for the DNI to accomplish to improve intelligence and prevent or mitigate the failures that led to 9/11. It is worth highlighting that a majority of those tasks and objectives relate to the conduct of intelligence analysis: Congress directed that U.S. intelligence analysis needed to be professionalized, have set standards, and address many shortcomings in skills and tradecraft through increased guidance and training. Thomas Fingar, the first Deputy DNI for Analysis, later reflected that up until IRTPA and the subsequent transformation of analysis in the IC, analysis had largely been a craft in the IC: skills learned only on-the-job, under the tutelage of 'journeymen' and 'masters,'

where the language and processes used could differ from shop to shop, region to region, and advancement was informally recognized and locally derived. **Note:** For more information on this topic, see Thomas Fingar, *Reducing Uncertainty: Intelligence Analysis and National Security*.

5.1.2.2. This is not to say that some agencies or elements in the IC did not have more established vocabulary and tradecraft, and even so-called training and intelligence colleges, such as the CIA and DIA. However, this kind of professional approach was not widespread, and where it was present, organizations were not sharing standards or efforts. IC standards began to promulgate through DNI-approved ICDs and other policy, while shared training and vocabulary were established through collaboration, development, and sharing of IC analysis training. As these directives, policy, and training matured, efforts began to focus on defining the fundamentals of intelligence analysis as a means to true certification of all analysts in the IC. Today, these analytic standards are not only reflected in ICDs, but are standards for AF compliance, as highlighted by AFI 14-133 and associated unit Management Internal Control Toolset (MICT) Self-Assessment Communicators (SACs).

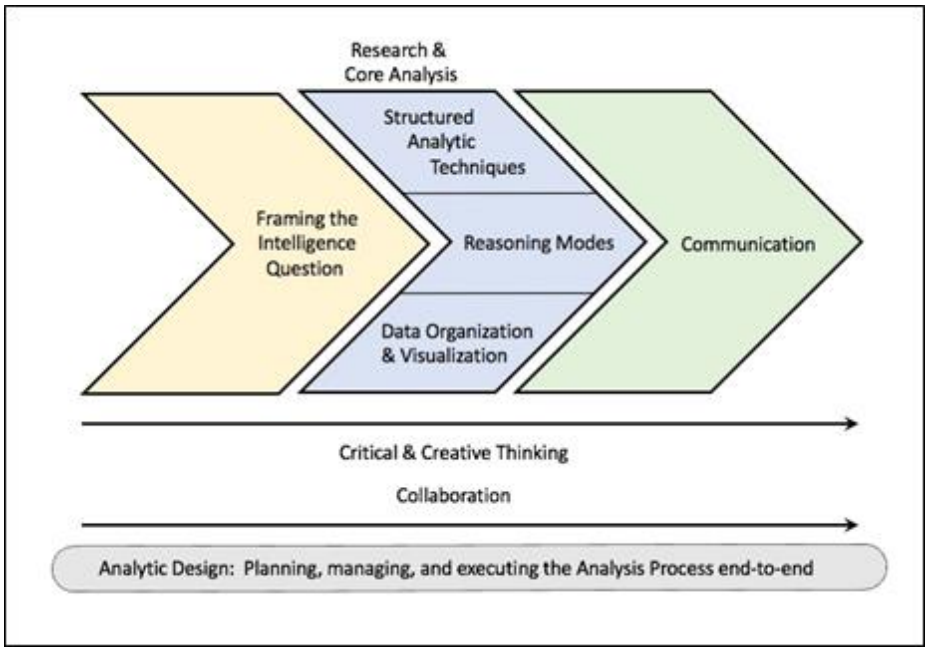
5.1.3. Analysis Certification Programs.

5.1.3.1. All-Source Analysis (ASA) Certification Program. The ASA Certification Program is a USD(I)-approved and DIA-led analysis qualification program for the DoD. The program assesses a candidate's knowledge and performance of ASA skills. The program is in the nascent stages. Initial qualification is focused on the fundamentals of intelligence analysis and open to all military and civilian intelligence analysts. The intent is for the program to expand to follow-on or higher levels of qualification. The AF ISR Force Management Division (AF/A2FD) is the AF OPR for the ASA Certification Program.

5.1.3.2. Other Certification Programs. The IC has also established certification programs for various fields of single-source analysis and activities closely linked with ASA. As one example, the Geospatial Intelligence (GEOINT) Certification Program is part of a broader USD(I) initiative to further professionalize the DoD intelligence workforce. The program applies to all cleared DoD civilian, military, and contractor practitioners in GEOINT-related work roles. Another example is the DoD Collection Management Certification Program, which ensures that collection managers possess the knowledge and skills associated with the competencies necessary to successfully carry out DoD collection management functional tasks.

5.2. Skills and Tradecraft Fundamentals. While analysis skills and tradecraft are taught in varying forms and emphasis across the IC and in AF entry and advanced training for core AF intelligence AFSCs (14N, 1NX, 9SX, 1A8X, and 0132), all AF intelligence analysts require competency in these areas. Figure 5.3, *Fundamental Skills and Tradecraft of the Analysis Process*, portrays the fundamental skills and tradecraft associated with the analysis process. Although the figure suggests an alignment, the order in which the analyst Airman applies the skills and tradecraft techniques varies depending on the requirement and is not as important as ensuring all skills and tradecraft are considered. This section will describe each of these areas.

Figure 5.3. Fundamental Skills and Tradecraft of the Analysis Process.



5.2.1. Critical and Creative Thinking.

5.2.1.1. Critical thinking is considered to be a foundational AF analysis skill. AFI 14-133 defines it as the intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from or generated through observation, experience, reflection, reasoning, or communication, as a guide to belief and action. The concept of critical thinking and its associated improvements to coherent cognition arose from the philosophy departments of schools and universities in the mid-1990s. Many observers feel it was because managers and leaders across the private, commercial, and government worlds began demanding people who could "think better and deeper." **Note:** See Peter A. Facione, *Critical Thinking: What It is and Why it Counts*, p. 3. Critical thinking may be better understood by contrasting it with "normal" thinking. In everyday thinking, people often find themselves with a central thought but are distracted by other thoughts or topics as they occur either physically or mentally. They strive to get to a destination, but may wander and stall before reaching it, with little recognition of where they have been. In contrast, with critical thinking, conscious effort occurs to focus on a particular thought and additionally be "critical" (the origin of the phrase) or reflective and purposeful, using more rigorous reasoning. Reflective reasoning—thinking about how we think, or metacognition—is the key difference between normal and critical thinking.

5.2.1.2. The need for critical thinking in analysis is often paired with another adjective: "creative." Creativity has always been difficult to define, but in the context of intelligence analysis, the 9/11 Commission report abounds with calls for U.S. analysts to have more imagination: to be able to link disparate happenings and facts, to see a "bigger picture," to envision alternatives which are not spelled out. In rigorous thinking, creativity is often associated with "abductive" reasoning: the process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar

explanation. **Note:** See section 5.2.4 for additional information on reasoning. Creativity "characterizes the analyst's ability to come to a conclusion spontaneously, often without a sense of having consciously taken definable steps to get there. While the abduction process may not be easily defined or taught, it may be encouraged by providing analysts with a wide array of research material and experiences, and by supporting the expenditure of time and energy on creative thinking." **Note:** See Lisa Krizan, *Intelligence Essentials for Everyone*, pp. 31-32, and LCDR William G. Schmidlin, *Zen and the Art of Intelligence Analysis.*

5.2.1.3. Both critical and creative thinking are supported in intelligence analysis by the application of methods known as Structured Analytic Techniques (SATs) and an understanding of analytic reasoning and the role of biases, addressed below.

5.2.2. Framing the Intelligence Question. A well-framed intelligence question is the most important factor in assuring the overall quality of intelligence analysis, helping analysts to anticipate emerging trends and developments and focus efforts on addressing issues most relevant to consumers of intelligence. The question drives information discovery, the selection of analytic approaches and methods, and ultimately the analytic message conveyed to intelligence consumers. Successfully framing the intelligence question consists of clearly articulating the key intelligence issues and deconstructing the question to identify the primary factors to be considered in answering the question. A well-framed question also requires the analyst to have an adequate understanding of air/space/cyber power and the missions the analyst directly supports. Framing the question includes identifying intelligence gaps, understanding the information base, and knowing how to drive collection.

5.2.2.1. Intelligence Gaps. An intelligence gap is information that is needed to appropriately conduct intelligence analysis and help answer an intelligence question but is absent from reporting—what we know we don't know. Identifying gaps helps focus the research and collection required to close the gaps. Moreover, awareness of intelligence gaps aids analysts in properly conveying the resulting level of confidence associated with analytic judgments.

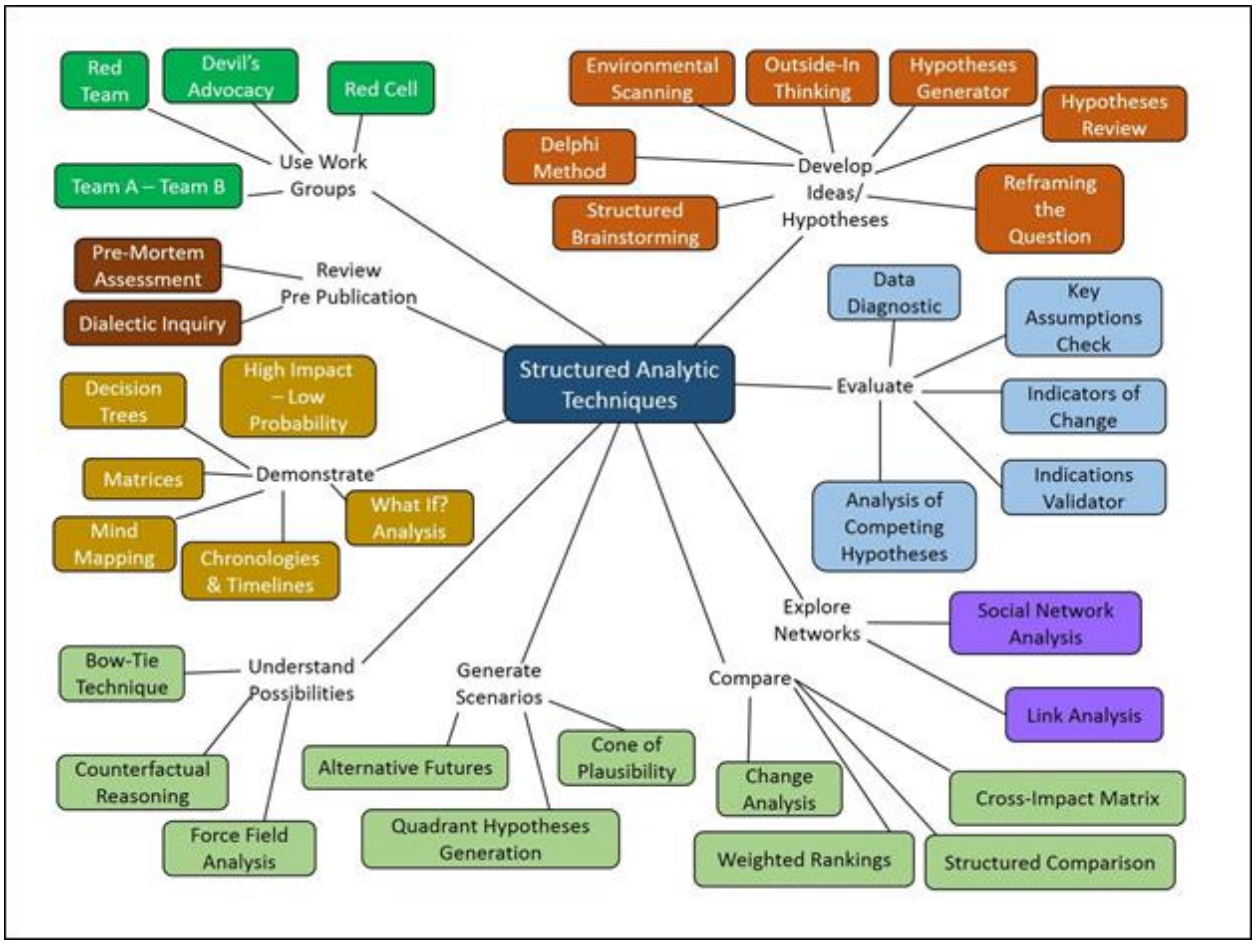
5.2.2.2. Understanding the Information Base. To effectively marshal information needed to answer intelligence questions, analysts require a solid understanding of the available information base. They need to identify what data and information is required, establish whether it is available, and determine where it can be found. In addition, they know the strengths and weaknesses of potential sources of information, are able to assess the quality of that information, in part by knowing where it comes from and how it was processed and disseminated, and understand the role analysis plays in transforming this data and information into knowledge that provides value to intelligence consumers.

5.2.2.3. Driving Collection. Analyst Airmen need to understand how information is collected and processed in the AF and more broadly in the IC to identify which sources of information are most useful in answering their intelligence questions, to assess quality and credibility, and to task collectors to collect information to fill intelligence gaps.

5.2.3. Structured Analytic Techniques (SATs). After properly framing the intelligence question, the analyst dives into the heart of the analysis process. There are several critical skills associated with this core research and analysis phase of the process, one being the application of SATs.

5.2.3.1. In *Structured Analytic Techniques For Intelligence Analysis*, Richards J. Heuer, Jr. and Randolf H. Pherson describe structured analysis as "a step-by-step process that externalizes an individual analyst's thinking in a manner that makes it readily apparent to others, thereby enabling it to be shared, built on, and critiqued by others. When combined with the intuitive judgment of subject matter experts, such a structured and transparent process can significantly reduce the risk of analytic error." **Note**: See Richards J. Heuer, Jr. and Randolf H. Pherson, *Structured Analytic Techniques For Intelligence Analysis*, p. xvi. SATs rose to prominence in intelligence analysis as part of a broad effort to transform the tradecraft following 9/11. Most SATs are not unique to intelligence analysis, but have been developed in other fields that utilize analysis. Many of these techniques, shown in Figure 5.4, *SATs*, broadly fall under the field of operations research, management tools, and general decision-making aids.

Figure 5.4. SATs.



5.2.3.2. Why are SATs important? Their application helps the analyst take a systematic approach to problem solving, mitigate bias and error, and enhance analytic credibility. SATs are useful by both individuals and teams in breaking down problems or "decomposition," generating ideas or "brainstorming," testing ideas or reviewing alternatives, and checking solutions or assessments. Structured techniques offer an effective means of applying scientific methodologies to the operational art of analysis.

Advanced analytic courses, such the AF Critical Thinking and Structured Analysis Course (CTSAC), offer focused training on SATs. Attachment 5 contains a tradecraft guide that details some of the key SATs commonly used by analyst Airmen.

5.2.4. Analytic Reasoning and Bias.

5.2.4.1. The heart of the definition for critical thinking is purposeful, reflective reasoning. Logical reasoning is defined as the process of establishing a justified belief by using premises (rules), evidence (facts), and argument (relationships). Three types of basic reasoning include:

5.2.4.1.1. Deductive reasoning—Sometimes called deductive logic, deduction is reasoning in which a conclusion is a logical consequence of the premise. A deduction moves from general rules and some evidence to particular cases.

5.2.4.1.2. Inductive reasoning—The intellectual process of drawing generalizations on the basis of observations or other evidence. Induction takes place when one learns from experience.

5.2.4.1.3. Abductive reasoning—The process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. Abductive reasoning starts from a set of accepted facts and creatively proposes their best explanation.

5.2.4.2. More recently, social scientists have helped to expand the horizons and suggest there are analytical *modes* of reasoning, most of which are familiar in description yet have significant research behind them. Reasoning is the process of forming conclusions, judgments, facts, opinions, or inferences. Reasoning assists in forming arguments based upon evidence about observed activities. It is the job of an analyst Airmen to make sense of a complicated mass of information—to understand and explain the current situation, to reconstruct the past that led to it, and to use it as the basis of predictions for the future. **Note:** See Barbara Spellman, "Individual Reasoning*"* in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, p. 117. As human beings with developed intellects, we generally may be said to have six modes of reasoning:

5.2.4.2.1. Status Quo—Making immediate judgments and inferences.

5.2.4.2.2. Authoritative—Drawing inferences from expert testimony or strong belief.

5.2.4.2.3. Comparative—Drawing conclusions from examples, cases, or analogies.

5.2.4.2.4. Empirical—Drawing conclusions from personal interaction with real evidence.

5.2.4.2.5. Scientific—Drawing casual inferences using facts, premises, and logic.

5.2.4.2.6. Market—Drawing conclusions from a structured consensus of persons.

5.2.4.3. We use many of these modes of reasoning every day, and there are analytical equivalents used in the process and mission of intelligence. However, bias remains one of the most common detractors in applying the modes of reasoning. Cognitive biases are mental errors caused by our simplified information processing strategies. When people reason, they employ various simplifying strategies and rules of thumb to ease the burden of mentally processing information to make judgments and decisions. "I always get

enchiladas at Mexican restaurants; the interstate is always faster; or I always get my news from an online news source." These simple rules of thumb may be acceptable for surviving the daily grind, but not for performing intelligence analysis. Analysts have to remain detached from normal survival biases and start fresh with each new problem.

5.2.4.4. Common types of cognitive biases include:

5.2.4.4.1. Bandwagon Effect—Tendency to believe something because many others believe it.

5.2.4.4.2. Clustering Illusion—Tendency to overvalue small runs, streaks, or clusters in large sets of data.

5.2.4.4.3. Confirmation Bias—Tendency to overvalue data supporting initial assumptions or expectations, and undervalue that which contradict.

5.2.4.4.4. Framing Effect—Tendency to draw different conclusions from the same data if it is presented differently.

5.2.4.4.5. Illusory Correlation—Belief that two events are related when they might not be.

5.2.4.4.6. Insensitivity to Sample Size—Tendency to underestimate the variation in data from small samples.

5.2.4.4.7. Mirror Imaging— Assumption that others see events and react to them just as we do.

5.2.5. Data Organization, Visualization, and Analytic Modeling.

5.2.5.1. As analyst Airmen begin to acquire information related to their intelligence question, either as part of a focused research effort or routine monitoring within their areas of responsibility, they need to employ a systematic approach to triaging and organizing information to identify trends, patterns, and relationships relevant to their intelligence question. The use of visualization techniques can assist analysts in deriving meaning from large volumes of fragmented information.

5.2.5.2. Visualization and analytic modeling are companion concepts to SATs. Effective visualization helps the analyst Airman analyze and reason about data and evidence. Analytic models can often help capture and expose knowledge, focus collection on the right needs, and apply analytics to the right questions. Visualization and analytic modeling apply to both the analytic process itself, and the delivery of information to consumers. Their importance was a key factor in establishing the analytic tradecraft standards of "effective visual information" by the IC and "utility" by the AF.

5.2.5.3. Like analysis, visualization and analytic modeling are both art and science. The advent of big data and data analytics has begun to emphasize the science and created the field known as data science. Data scientists find, interpret, and merge rich data sources; ensure consistency of data sets; create visualizations to aid in understanding data; build mathematical models using the data; and present and communicate data insights and findings to specialists, scientists and non-technical audiences.

5.2.6. Communication. Effective communication is essential to the craft of intelligence and even the best intelligence analysis falls short if communicated poorly. Consumers often

judge the validity of analysis by the quality of how it is communicated. The importance of communication is underscored by ICDs 203, 206, and 208 and AFI 14-133, which prescribe standards and principles for dissemination and require annual assessments for compliance. Analysts use multiple vehicles and formats to communicate their assessments to consumers.

5.2.6.1. Analytic Writing. Well-written products share a common set of attributes. First and foremost, good intelligence writing is analytic. That means, it does not simply report events; it explains the significance of those events and much more. Intelligence assessments are structured so that busy consumers can quickly grasp the main message and underlying reasoning, and be clear, precise, and convincing. In particular, analysts minimize the chance for misinterpretation of the findings, the certainty behind them, or how they were arrived at. Even the best analysis, if presented poorly, could cause the customer to question its credibility.

5.2.6.2. Visuals. Whereas data visualization during core research and analysis helps the analyst to "discover" the story, visualization for presentation helps "tell" the story. Visual presentation uses graphics—from charts and graphs to maps and complex tables, and both hardcopy and digital—to make relationships between data more easily understood.

5.2.6.3. Briefings. Briefings are a key mechanism for communicating analytic judgments to customers and can foster two-way communications to ensure that customer intelligence questions are addressed. Effective briefings consist of a well-organized, clear message relevant to the target audience; appropriate, tailored visual aids to reinforce the message; and a presentational style that keeps the audience focused on the message. Briefing is a skill that is honed through practice.

5.2.6.4. Multimedia Products. Significant innovations in multimedia tools have emerged that make possible sophisticated products that go beyond static graphical presentations. Multimedia products are generally either interactive or use full-motion video or animated web graphics to display content. Some techniques are particularly useful for depicting changes in data over time or comparing complex or multivariate data by allowing users to choose which variable they want to see. Despite these different ways to communicate analysis, the fundamentals remain the same: analysts need to present their analysis with clarity and sound logic.

5.2.7. Collaboration.

5.2.7.1. Similar to critical and creative thinking, collaboration is a skill that extends across the entire analysis process. Effective intelligence analysis depends on strong interpersonal relationships among analysts within and across intelligence agencies and the way the analysts relate to collectors, customers, and other experts within and outside the IC. Analysts are expected to collaborate and team to tackle complex intelligence questions, coordinate analytic products, and engage in regular discussions with colleagues that explore and challenge analytic judgements and prevailing assumptions. As one of the six AF intelligence analysis tenets, collaboration is considered a fundamental attribute and priority in AF analysis. Further, collaboration is the catalyst to every IC member's responsibility to "provide, discover, and request" as mandated in ICD 501.

5.2.7.2. An important aspect of collaboration and teaming is analytic outreach, which ICD 501 defines as the open, overt, and deliberate act of an IC analyst engaging with an individual outside the IC to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information. Outside experts include those in academics, business, non-governmental organizations, scientists, and others. Various methods of analytic outreach include conferences, seminars, exchanges, sabbaticals, and the building of trusted professional relationships.

5.2.7.3. Skills required for effective collaboration include employing tools to facilitate scheduling, access to data, and the sharing of analysis; effective team management practices; social networking techniques; constructive criticism—both giving and receiving; and interpersonal skills. Analysts need to also be aware of and take measures to avoid impediments to teaming, especially the "What's in it for me?" mindset. A study of the collaboration environment in the IC in 2007 identified six imperatives to help overcome such mindsets: mission criticality, mutual benefit, mutual trust, common understanding through common lexicon and transparent rules of the road, access and agility to identify collaborators and form collaborative communities, and incentives. **Note:** Derived from Integrated Concepts Development Office, *Achieving a Robust Collaborative Environment*.

5.2.8. Analytic Design. Analytic design is the activity of planning, managing, and executing the analysis process end-to-end—from the development of the right intelligence question, research, and core analysis to the crafting of an assessment that captures and communicates analytic insight for customers. Although analytic design is described last in this chapter's list of skills and tradecraft, it takes place up-front and then continues throughout the analysis process. In analytic design, the analyst outlines the plan for framing the question, applying SATs, reasoning and mitigating biases, organizing and visualizing data, communicating the analysis, collaborating with all applicable entities, and employing critical and creative thinking skills. Then, as the plan is put into action, the analyst revisits and revises the plan, as needed, to comprehensively address the requirement. More information on this subject is available at the following site: *ICAT-G/Products Analytic Design Portal*, Joint Worldwide Intelligence Communications System (JWICS) Caution-url: **https://intellipedia.intelink.ic.gov/wiki/Portal:IC_Analytic_Tradecraft_Gateway/Analytic_Design**.

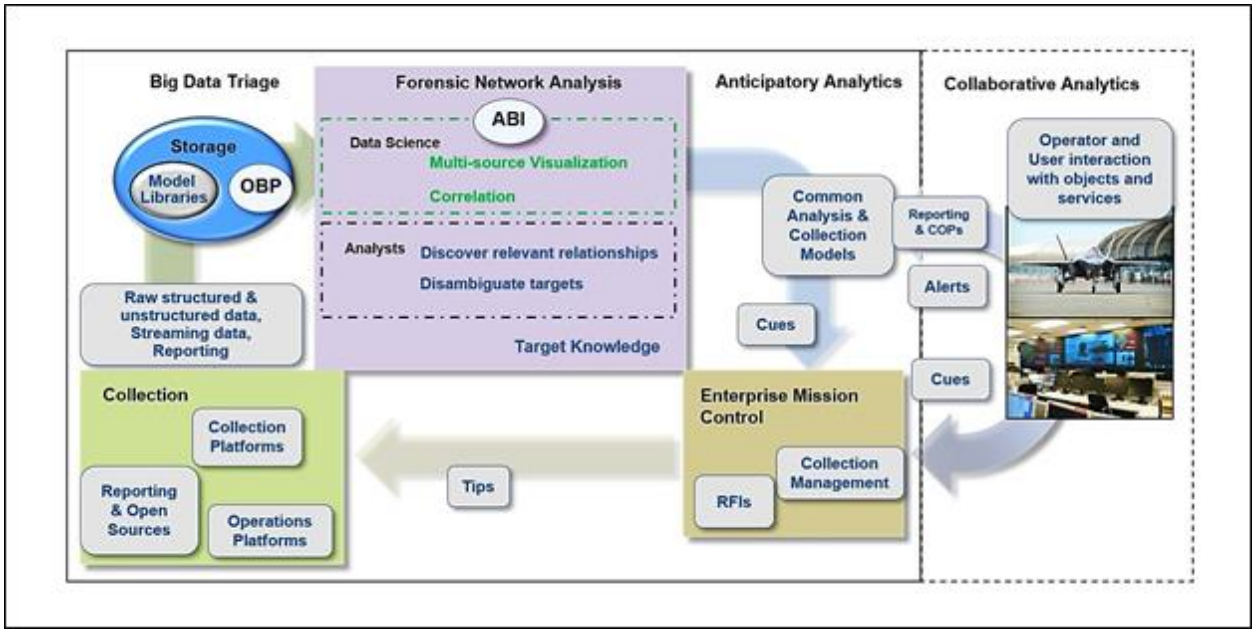
5.3. Key Analysis Concepts.

5.3.1. Big Data, Data Analytics and Data Science.

5.3.1.1. According to the *AF Future Operating Concept: A View of the AF in 2035*, the term big data describes large volumes of high-velocity, complex, variable data that require advanced techniques and technologies to enable the capture, conditioning, reliability, storage, distribution, management, and analysis of the information. The significance of big data extends beyond the sheer volume, complexity, and diversity of data; it is profoundly changing the way we think about data and creates new knowledge and information. **Note**: Paul B. Symon and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data," *Joint Forces Quarterly*, p. 4. Big data is driving us from a perspective of "causation" to one of "correlation." Rather than the traditional perspective of analyzing discrete amounts of data to understand the past cause and effect

(the why) and use that as a predictor of future behavior, data analytics enables analysts to harness the massive amounts of data available to draw correlations and use patterns of life (the what) as a predictor of future behavior, even if we do not understand "the why." **Note**: Kenneth Neil Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think about the World," *Foreign Affairs*. Figure 5.5, *Data Analytics Framework*, depicts a general framework for data analytics.

Figure 5.5. Data Analytics Framework.



5.3.1.2. Data Science is at the heart of adapting the AF ISR Enterprise to the evolving big data environment. It can generally be described as the practice of exploiting and deriving valuable insights from data. This involves extracting knowledge from data sets that may be small, large, structured, multi-modal, multi-lingual, semi-structured or unstructured. Since data science is an inherently technical and specialized field, it is best performed by individuals trained and qualified in the complex and specialized nature of the work. As the DCS for ISR White Paper, *Data Science and the USAF ISR Enterprise* conveys, rather than train analyst Airmen to be data scientists, the AF approach is to develop a force of ISR professionals, operators, and knowledge managers that understand and leverage the capabilities that data scientists bring to the fight. Figure 5.5 highlights the role of data science relative to analysts in the process of data analytics.

5.3.1.3. The implications of big data, data analytics, and data science for intelligence analysis cannot be overstated. In recognition of this, the IC has embarked on a number of analytic modernization initiatives to exploit emergent big data capabilities, improve intelligence integration, and accelerate intelligence decision cycles. Two major initiatives are object-based production (OBP) and activity-based intelligence (ABI).

5.3.2. Object-Based Production (OBP).

5.3.2.1. Traditionally, analysts spend a great deal of time and effort assembling, collating, and parsing diverse data sources that pertain to a given intelligence problem.

As Figure 5.5 illustrates, OBP is a framework for organizing and sharing information. It is defined as the act of organizing intelligence around objects of interest—not by collection or data type—which allows users to aggregate intelligence information from across multiple intelligence domains and associate it with particular objects of interest. All intelligence that relates to something that physically exists in the real world is assembled and made centrally available as an object that all collectors, producers, and consumers can access. Objects include physical things (e.g., ships, buildings, vehicles, persons, and political boundaries), as well as abstract things (e.g., events and issues). The intent of OBP is to provide a consolidated perspective about the behavior of objects and their interaction with one another.

5.3.2.2. Traditionally, the output of each intelligence discipline is assembled by an analyst in order to understand the who/what/where/when of the object. The OBP alternative enables analysis to be directly attached to the object in question to allow delivery of complete find, fix, and track information direct to operational users. Thus, intelligence analysis is not stove-piped or the end result of a linear process. Instead, in this synthetic model, known information is dynamically assembled within the intelligence process. Automatic exploitation systems and manual intelligence analysis work in tandem to dynamically populate a shared community of objects that all analysts have access to. The result is that analysts can better understand intelligence activity by more clearly identifying and managing intelligence gaps and spending less time assembling information.

5.3.3. Activity-Based Intelligence (ABI).

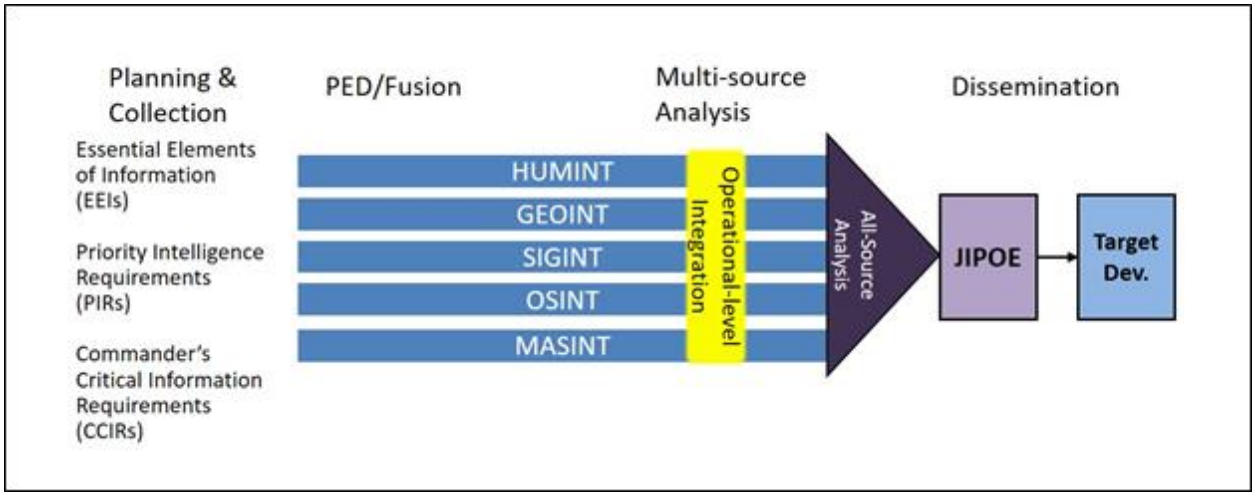
5.3.3.1. ABI emerged from the experiences of analysts working dynamic targets and analytic problems. It centers on the discovery and association of unknown activities. DIA, the National Geospatial-Intelligence Agency (NGA), and the National Security Agency (NSA) describe ABI as an analytic method applied to structured data from all sources, to discover objects (e.g., high-value target location), relationships (e.g., supplier/consumer), or behaviors (e.g., pattern of life) by resolving significant activity.

5.3.3.2. NGA has delineated four ABI tenants that apply to a variety of missions and problem-sets: 1) geo-reference to discover; 2) integration before exploitation; 3) data neutrality; and 4) sequence neutrality. As geo-referenced activity becomes the starting point of discovery, that allows for the rapid integration of multi-INT data and allows for analysis without data-source or sequence biases presented by the traditional linear collection process. Successful ABI analysis relies heavily on geo-referenced data that did not lend itself to an immediate application when it was collected, but eventually enhanced the larger context or provided more accurate characterization and understanding of data collected at a later date.

5.3.3.3. As ABI and OBP have grown to become IC-wide methodologies, NGA has advocated and developed a concept called Structured Observation Management (SOM). SOM is the practice and method of organizing and sharing multi-sensor data that is not focused on objects (e.g., activities or events), in order for the resulting data to be consistent with, and in support of, both ABI and OBP processes. It can be thought of as a 'bridge' between the new analytic processes of OBP and ABI.

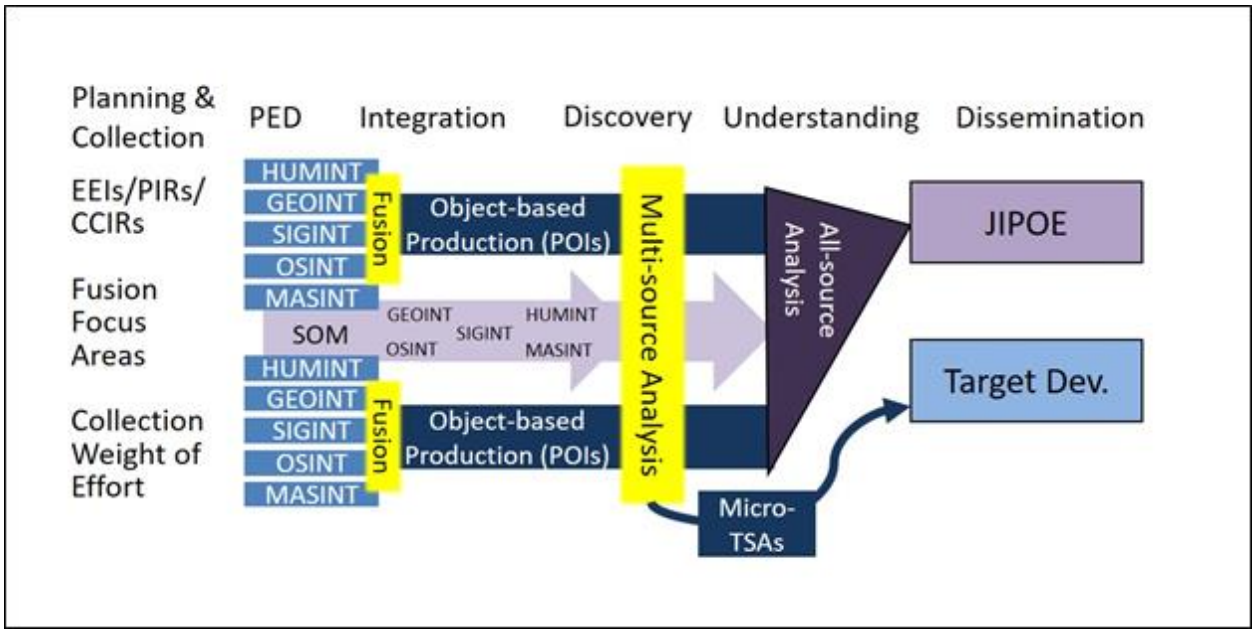
5.3.3.4. AF ISR analysts need to innovate to implement ABI in our mission sets. One such effort is Scoped Activity-based Intelligence for Nodal Targeting (SAINT), an ACC-developed capability that operationalizes ABI, predominantly in support of deliberate targeting. SAINT's strength lies in the rapid fusion of data and information to create multi-source intelligence as early in the intelligence cycle as possible, and close to the point of collection in order to enable collection refinement. Figure 5.6, *Traditional Model for Target Discovery*, depicts the traditional model of a linear production chain that combines to contribute to content-dominant analysis, a time-consuming approach to Joint Intelligence Preparation of the Operational Environment (JIPOE) and ultimately target development. In contrast, Figure 5.7, *ABI/OBP Integrated Model for Target Discovery*, highlights the SAINT construct, in which OBP enables fusion analysis and micro-target system analyses (TSAs) in a time-dominant environment. This model makes possible a symbiotic analysis/collections relationship to support strategic, operational, and tactical objectives simultaneously.

Figure 5.6. Traditional Model for Target Discovery.



Note: Source is Michael Kreuzer and Denis Dallaire, *Targeting the Islamic State: Activity-based Intelligence Empowering Air Force Targeting*.

Figure 5.7. ABI/OBP Integrated Model for Target Discovery.



Note: Source is Michael Kreuzer and Denis Dallaire, *Targeting the Islamic State: Activity-based Intelligence Empowering Air Force Targeting*.

5.4. Additional Tradecraft Resources.

5.4.1. IC Analytic Tradecraft Gateway (ICAT-G). The ICAT-G serves as a repository for the ICs collective knowledge of the analytic process, methods and techniques, and best practices. It is a useful, comprehensive reference aid for analysts and a valuable resource for analytic training. It is located on JWICS at Caution-url: **https://intellipedia/intelink.ic.gov/wiki/ICAT-G**.

5.4.2. Online Critical Thinking and Analysis Environment (OCTANE). OCTANE is a 25 AF online initiative for analysts to find mentors and exchange information through an analyst mentor network, practice tradecraft, compete with peers through IntelTrivia, and download free applications and games for use on mobile devices. The OCTANE site is on the Nonsecure Internet Protocol Router Network (NIPRNet) at **https://www.25afoctane.com**.

5.4.3. Center for Marine Expeditionary Intelligence Knowledge (CMEIK). The CMEIK is dedicated to advancing analytic tradecraft across the Marine Corps intelligence enterprise. The CMEIK offers courses, tradecraft notes, and video podcasts on a variety of analysis topics that are applicable to all military services. Several examples include a writing guide, SAT pocket guide, intelligence preparation of the battlespace template, and a collaboration page. CMEIK information is available on the SECRET Internet Protocol Router Network (SIPRNet) at Caution-url: **www.mcia.usmc.smil.mil/cmeik**.

Chapter 6

REQUIREMENTS AND PRODUCTION

6.1. Intelligence Requirements and Analytic Focus.

6.1.1. Questions, Requirements, and Customers.

6.1.1.1. Intelligence analysis and production are driven by leading questions or requirements for intelligence to fill a gap in knowledge or understanding of the environment, adversary capabilities, centers of gravity, or intentions. Questions may be more formal, such as Key Intelligence Questions (KIQs) from AF and IC Programs of Analysis (PoAs), or more informal, such as those that stem from direct, near-term support to operations. All questions are based on an intelligence organization's relationship with its customer and an understanding of customer needs.

6.1.1.2. Intelligence analysis and production are also driven by priorities at all levels of command, from the President of the United States down to the tactical level of operations. At the national- and IC-level, this primarily manifests itself in the National Intelligence Priorities Framework (NIPF).

6.1.2. National Intelligence Priorities Framework (NIPF**)**. Published annually and reviewed quarterly, the NIPF is the primary mechanism to establish, manage, and communicate national intelligence priorities. Guidance from the President and National Security Advisor determines overall priorities. Secretaries and cabinet-level heads of departments and agencies provide formal input to NIPF development. The DNI is responsible for developing and managing the NIPF. All IC activities, including those of the AF, adhere to the NIPF priorities. **Note:** See ICD 204, *National Intelligence Priorities Framework*, for NIPF policy and responsibilities.

6.1.3. Programs of Analysis (PoAs).

6.1.3.1. Per DNI direction, each IC member publishes an annual PoA to provide comprehensive analysis and production focus for their organization. Collectively, the IC PoAs offer a framework for collaboration with customers, stakeholders, and IC partners. The DNI has directed each IC organization to annually publish a PoA to provide comprehensive intelligence analysis and production focus for their organization.

6.1.3.2. The AF ISR PoA (AFISRPoA) is organized into broad, overarching analytic categories, each with multiple KIQs that represent the most pressing analysis required in each category. AF analysis organizations use these categories and KIQs to guide their analytic focus.

6.1.3.3. All PoAs are to reference NIPF priorities when possible. Additionally, a new DoD Integrated Defense Intelligence Priorities (IDIP) process is being implemented to identify and describe intelligence priorities for the diverse set of DoD customers: policy, operations, and acquisition. The IDIP is the DoD intelligence inject into the NIPF and provides an additional layer of data with traceability to analytic stakeholders. Analysts reference both the NIPF and IDIP for understanding of analysis and production priorities, and reference these priorities, when feasible, in development of respective AF intelligence products and services. Additionally, the IDIP can be used by analysts to help

frame internal resource and planning discussions across the Planning, Programming, Budgeting, and Execution (PPBE) cycle.

6.1.3.4. AFI 14-134 directs development of the AFISRPoA and sub-echelon PoAs for NASIC, and the 363 ISRW via 25 AF and ACC. The intent is for every major AF ISR production element to eventually develop its own PoA to focus on analysis priorities and production. The desired end-state resulting from the AFISRPoA and subordinate level PoAs would be a more unified AF ISR analysis and production enterprise.

6.1.3.5. JWICS Intellipedia lists and provides access to all AF and IC PoAs. A listing of associated AF ISR and IC PoAs resides on JWICS Intellipedia at Caution-url: **https://intellipedia.intelink.ic.gov/wiki/Programs_of_Analysis**. Analysts reference and leverage KIQs that are specific to their analysis mission area, enabling them to work toward common AF and IC goals, improve efficiency through elimination of redundant analytic efforts, and expand their collaboration both within and outside the AF.

6.1.4. Across the AF, DoD, and IC, various terms are used when referring to an intelligence question and/or requirement, including request for information (RFI), request for support (RFS), intelligence need, intelligence requirement, KIQ, and production requirement (PR). Henceforth, this publication will use RFI to refer to all types of intelligence questions and/or requirements. RFIs range from informal to formal and from verbal to formally documented requests. They originate from an intelligence customer (also called an intelligence consumer), which includes but is not limited to, operational units, acquisition organizations, national policy makers, other intelligence elements throughout the AF, DoD, and IC, and counterintelligence units, such as AFOSI. While RFIs may be explicitly stated, analysts anticipate and help shape RFIs, based on known mission needs and a thorough understanding of operations. Supervisors help ensure their analysts are able to engage with the customer, as needed.

6.1.5. Requirements deemed most important to mission accomplishment are identified as priority intelligence requirements (PIRs). By definition, these are the critical requirements that must be satisfied for a commander and staff to understand an adversary and the operational environment in order to successfully plan and conduct a mission. PIRs are general statements of intelligence need, such as, "What is the operational status of the adversary's integrated air defense system?" or "What terrorist groups are active within the area of interest?" PIRs provide the framework for prioritization of all GIISR operations within a CCMD. PIRs, combined with a commander's friendly force information requirements (FFIRs), constitute the commander's critical information requirements (CCIRs).

6.1.6. PIRs drive the development of detailed essential elements of information (EEIs). EEIs further define the commander's PIRs by outlining specific information requirements, such as, "What is the current location of the adversary SA-20 battalion?" The designation of PIRs and EEIs help ensure efforts are focused on critical information needed to support warfighters.

6.1.7. Priority requirements in acquisition intelligence are identified as critical intelligence parameters (CIPs). A CIP is a factor that defines the threshold at which the performance of a foreign system/capability would likely degrade or nullify the effectiveness of an acquisition program or details of a developmental U.S. system, the disclosure of which could allow an

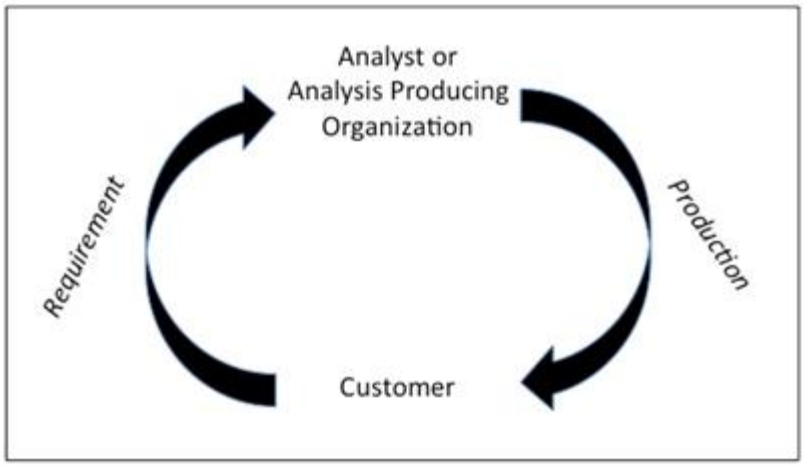
adversary to effect countermeasures to degrade mission effectiveness of the system, if it were to be fielded. CIPs are a key concept for an operational MAJCOM's requirements process/documents, as well as for an acquisition program. They are essentially a PIR for new capabilities going through the requirements and acquisition systems.

6.2. Intelligence Production .

6.2.1. Intelligence production is the development, tailoring, and presentation of intelligence knowledge via products and/or services that meet or address customer requirements. Production is an all-encompassing term that ranges from formal, published products on one end of the spectrum (e.g., a formal intelligence summary) to informal, impromptu updates on the other end (e.g., a location update on a tactical threat as a pilot steps to the aircraft). In some cases, analysts tailor existing intelligence to answer customer requirements. In other cases, analysts perform analysis on existing data, information, and intelligence to create new intelligence and knowledge. Still, in other cases analysts request collection of new data to consider in their analysis.

6.2.2. Ultimately, production culminates in at least one intelligence output for a customer, bringing the cycle full-circle, as depicted in Figure 6.1, *Requirement–Production Cycle*. An output may be an intelligence product or an intelligence service.

Figure 6.1. Requirement–Production Cycle.



6.2.3. An intelligence product is defined as tangible information in written, visual, digital, and/or verbal form that: 1) conveys information of intelligence value (e.g., written assessment, threat map, targeting materials, database, etc.); or 2) facilitates the accomplishment of an intelligence mission (e.g., assessment checklists, training folders, etc.). This definition is sufficiently broad to capture products that both directly and indirectly contribute to mission accomplishment, including those associated with intelligence analysis. The IC has established certain standards that products should meet. See Attachment 4 for a sample methodology and form to evaluate product standards.

6.2.4. An intelligence service is defined as assistance provided to another entity during the performance of ISR support, including: 1) the actual action of delivering or conveying intelligence to a user (e.g., presenting a briefing, tipping and cuing, collaboration, threat modeling, etc.); and 2) the process of enabling an ISR mission (e.g., exercise planning, skill

knowledge training, security clearance indoctrination, etc.). Some intelligence services result in additional intelligence products. Similar to intelligence products, this definition includes services associated with all categories of ISR mission accomplishment, one being intelligence analysis.

6.2.5. AF products and services are grouped into 14 product lines and 14 service lines. See Attachment 2 for descriptions of each product and service line.

6.3. Request for Information (RFI) and Analysis/Production Process . AFI 14-134 establishes and details the AF RFI and analysis/production process. Figure 6.2, *RFI and Analysis/Production Process*, illustrates the basic RFI flow that occurs at each organizational level. Figure 6.3, *RFI and Analysis/Production Process across the AFIAE*, depicts the flow across the whole analysis enterprise. The RFI and analysis/production process operationalizes the layered, distributed, mutually supporting AFIAE. It is the construct through which AF intelligence entities address customer requirements, share analytic findings, tap into analysis expertise across the IC, and collaborate on production. It is the mechanism that enables the AFIAE to achieve decision advantage. Refer to AFI 14-134, **Chapter 3** for specifics on the RFI process, categorization, tracking, and timelines.

Figure 6.2. RFI and Analysis/Production Process.

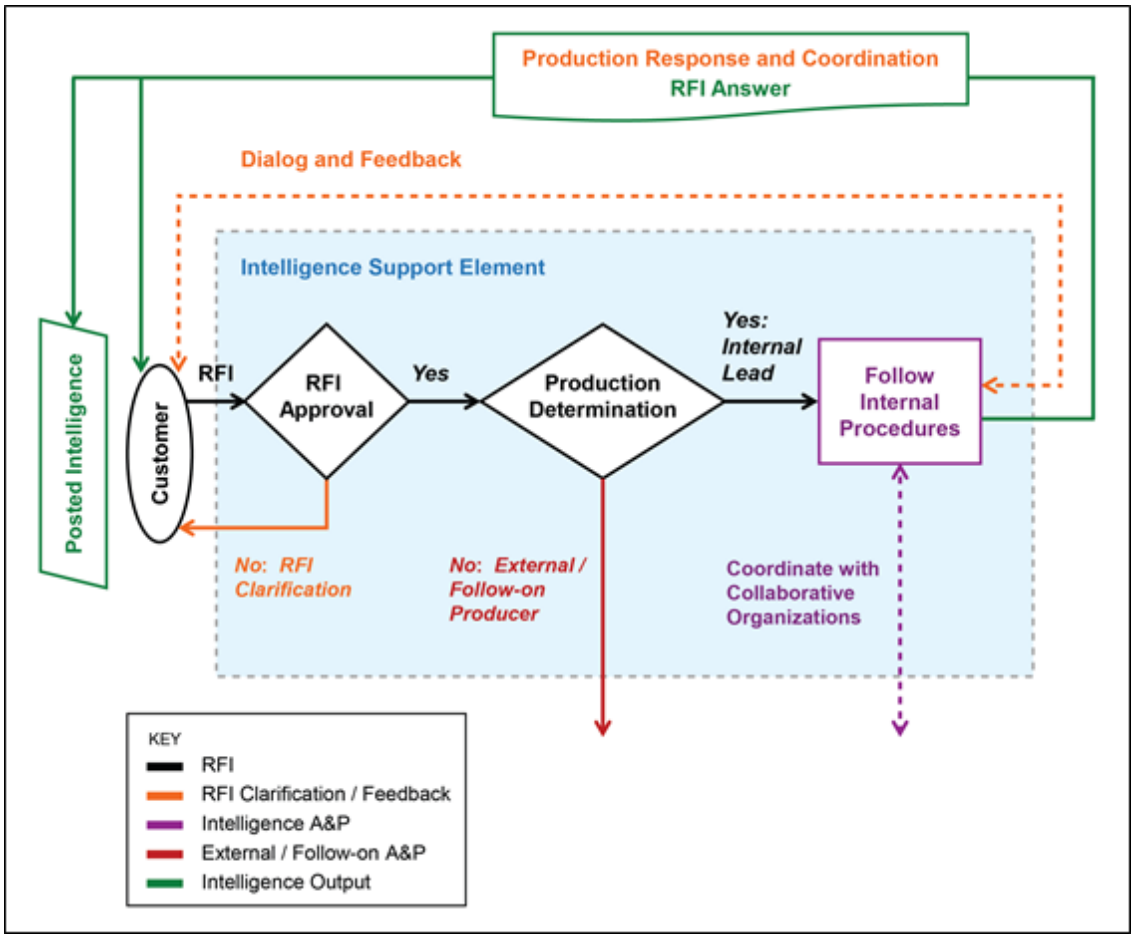
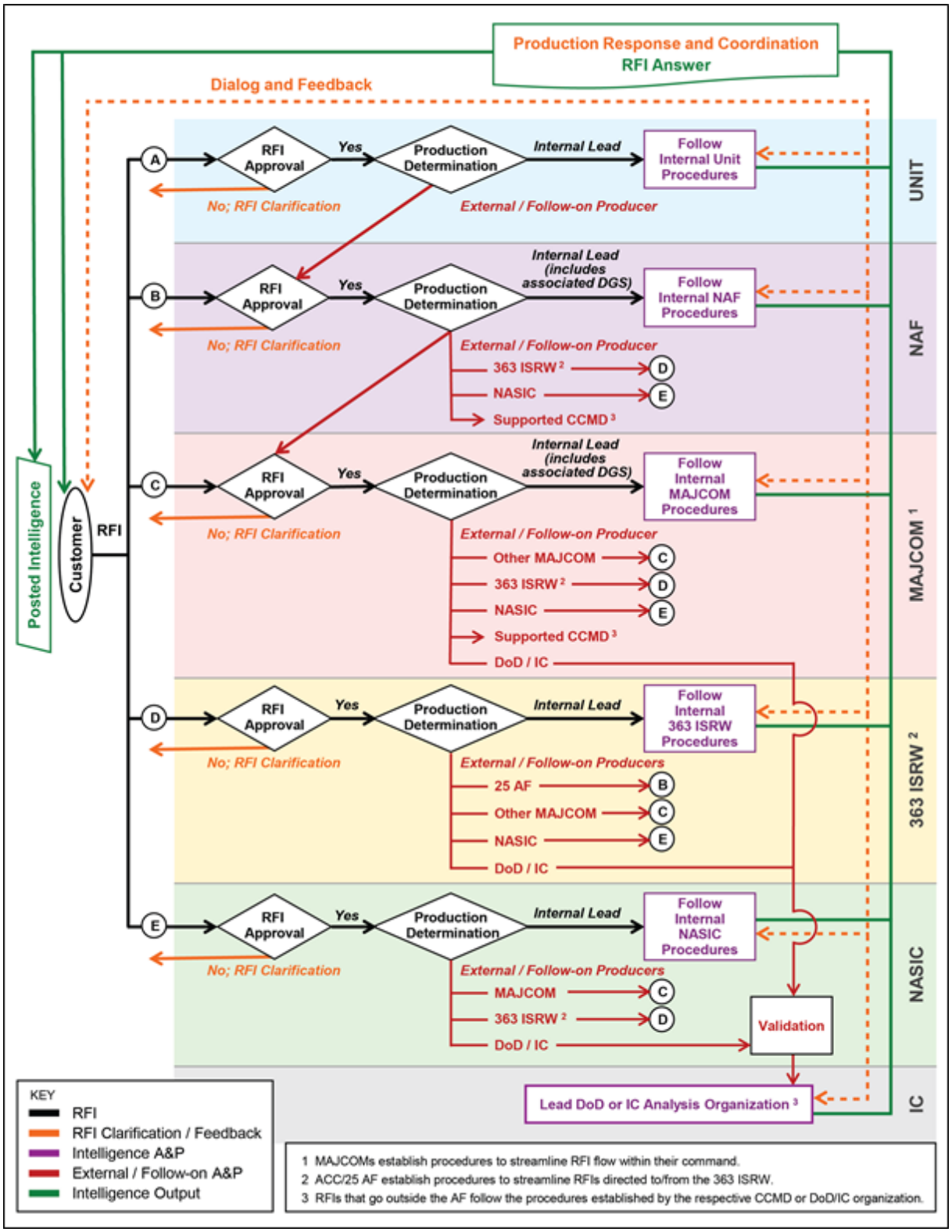


Figure 6.3. RFI and Analysis/Production Process across the AFIAE.



6.4. Acquisition Intelligence Production. Intelligence analysis and production are integral to the entire life cycle process of requirements definition, acquisition, and sustainment of weapon

systems. Acquisition customers require the production of specific threat assessments and potentially unique forms of data to support research, development, test and fielding of warfighting capabilities. Acquisition intelligence analysts support acquisition programs and initiatives by helping to identify and document intelligence dependencies (such as Intelligence Mission Data [IMD], modeling and simulation, etc.) that provide critical input to intelligence production efforts and the development of product/service requirements. As part of threat support to acquisition, NASIC and other service intelligence centers continually monitor and produce intelligence on adversary capabilities deemed critical to operational success for the developing capability. In partnership, acquisition intelligence specialists, operational command intelligence planners, and service intelligence center analysts provide direct support to acquisition decision processes, as defined in the *DIAP Users Guide* and DoD directives and instructions. These documents provide additional guidance for specific requirements and resourcing activities.

VERALINN JAMIESON, Lt Gen, USAF
Deputy Chief of Staff, Intelligence,
Surveillance, and Reconnaissance

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Activity-Based Intelligence: Methods, Origins, Future, RAND, PR-1157-USCA, August 2014

ACWG Charter, 13 February 2015

AF Future Operating Concept: A View of the AF in 2035, September 2015, **http://www.af.mil/Portals/1/images/airpower/AFFOC.pdf**

AFCO-CFA Intellipedia Page, **https://intellipedia.intelink.gov/wiki/Air_Force_Cryptologic_Office_(AFCO)/CFA_Advanced_Analysis_and_Training**

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 90-1601, *Air Force Lessons Learned Program*, 18 December 2013

AFISRAI 14-153 Volume 3, 480 ISRW Supplement, *Air Force Distributed Common Ground System (AF DCGS) Operations Procedure*s, 5 February 2014

AFMAN 33-363, *Management of Records*, 1 March 2008

AFPD 14-1, *ISR Planning, Resources, and Operations*, 2 April 2004

ASA Certification site, JWICS Caution-url: **https://intelshare.intelink.ic.gov/sites/asacertification**

Center for Marine Expeditionary Intelligence Knowledge (CMEIK) site, SIPRNet Caution-url: **www.mcia.usmc.smil.mil/cmeik**

Assistant Director of National Intelligence (A/DNI) for Systems and Resource Analysis, *FY2017-2021 Major Issue Study Final Report Activity-Based Intelligence (ABI) Way Ahead*, May 2015

CFETP 14NX, Parts I and II, *AFSC 14NX Intelligence Officer Career Field Education and Training Plan*, 13 February 2013

CFETP 1N0X1, Parts I and II, *AFSC 1N0X1 All Source Intelligence Analyst Career Field Education and Training Plan*, 26 September 2016

DDII Analytic Integrity and Standards Group, *Applying the Intelligence Community's Analytic Tradecraft Standards: A Guide to Best Practices*, 2nd edition, September 2015

DDII Analytic Integrity and Standards Group, *Multi-INT Collection Source Description Guide: A Tradecraft Working Aid*, July 2005

DIA-01-1309-510, *DIA Style Manual for Intelligence Production 2017*, JWICS Caution-url: **https://intelshare.intelink.ic.gov/sites/ddii/mid/AIS/default.aspx**

DIAD 5000.200, *Intelligence Threat Support for Major Defense Acquisition Programs*, 1 Feb 2013

DIAI 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*, 1 Feb 2013

DIAP Users Guide, January 2016

DNI Memorandum, *All-source Analysis Improvements*, 25 Aug 2015

DNI Memorandum, *Principles of Intelligence Transparency for the Intelligence Community*, 15 Jan 2015

DNI, *Principles of Intelligence Transparency for the Intelligence Community*, January 15, 2015

DoDD 5000.01, *The Defense Acquisition System*, May 12, 2003

DoDD 5105.21, *Defense Intelligence Agency (DIA)*, March 18, 2008

DoDD 5143.01, *Under Secretary of Defense for Intelligence (USD(I))*, October 24, 2014

DoDD 5205.12, *Military Intelligence Program*, November 14, 2008

DoDD 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*, January 22, 2013

DoDI 3115.17, *Management and Oversight of DoD All-Source Analysis*, November 16, 2016

DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015

DoD Manual (DoDM) 3305.02, *DoD Collection Management Accreditation and Certification*, November 21, 2012

GEOINT Professional Certification site, **https://www.nga.mil/Careers/Pages/GEOINT-Professional-Certification.aspx**

IC Analysis Tradecraft Gateway, JWICS Caution-url: **https://intellipedia/intelink.ic.gov/wiki/ICAT-G**

IC Programs of Analysis, JWICS Caution-url: **https://intellipedia.intelink.ic.gov/wiki/Programs_of_Analysis**

ICD 104, *National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation*, 30 April 2013

ICD 191, *Duty to Warn*, 21 July 2015

ICD 205, *Analytic Outreach*, 28 August 2013

ICD 208, *Maximizing the Utility of Analytic Products*, 9 January 2017

ICD 209, *Tearline Production and Dissemination*, 6 September 2012

Integrated Concepts Development Office, *Achieving a Robust Collaborative Environment*, May 2007

JLLIS Database, SIPRNet Caution-url: **https://www.jllis.smil.mil**

Johnston, Cathy, *Modernizing Defense Intelligence: Object Based Production and Activity Based Intelligence*, Briefing for DIA, 27 June 2013

Joint Capability Areas: JCA 2010 Refinement, 8 April 2011

Kreuzer, Michael, and Denis Dallaire, *Targeting the Islamic State: Activity-based Intelligence Empowering Air Force Targeting*, The Mitchell Institute for Aerospace Power, September 2016

National Intelligence Analysis Board, *Integrating the Analytic Enterprise*, October 2015

National Intelligence Priorities Framework, JWICS Caution-url: **https://intellipedia.intelink.ic.gov/wiki/NIPF**

NGA, *Activity-Based Intelligence (ABI) Concept of Operations: A 2015 Strategic Initiative*, Ver. 4.0, August 2015

NGA Briefing, *Object-Based Production (OBP) and Activity Based Intelligence (ABI)*, 19 November 2015

NGA Briefing, *Object Based Production (OBP) Basics*, 1 Nov 2013

ODNI Systems & Resource Analyses, *ABI Way Ahead*, JWICS Caution-url: **https://intelshare.intelink.ic.gov/sites/sramis/abi/default.aspx**

Online Critical Thinking and Analysis Environment (OCTANE), **https://www.25afoctane.com**

Quellfire Documentation, JWICS Caution-url: **https://intelshare.intelink.ic.gov/sites/quellfire/SitePages/ProgramDocumentation.aspx**

QUELLFIRE Object-Based Production Concept of Operations, V1.0, May 2013

QUELLFIRE Program Manager Briefing, *Changing the Way the Intelligence Community Shares Information: Object-based Production*, 20 February 2013

Schmidlin, LCDR William G, *Zen and the Art of Intelligence Analysis*, Joint Military Intelligence College, July 1993

Spellman, Barbara, "Individual Reasoning" in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, Baruch Fischhoff and Cherie Chauvin, Washington D.C., National Academies Press, 2011

Universal GEOINT Certification Program site,**https://usgif.org/certification**

USAF Strategic Master Plan, May 2015, **http://www.af.mil/Portals/1/documents/Force%20Management/Strategic_Master_Plan.pdf**

USD(I) Memorandum, *Strengthening Defense Intelligence Analysis*, May 21, 2016

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

A/DNI—Assistant Director of National Intelligence

A&P—Analysis and Production

A2—Director of Intelligence

A2/AD—Anti-Access/Area Denial

ABI—Activity-Based Intelligence

ACC—Air Combat Command

ACIC—Army Counterintelligence Center

ACWG—Analysis Capability Working Group

AF—Air Force

AF NTI—Air Force National Tactical Integration

AFCO-CFA—Air Force Cryptologic Office Advanced Analysis & Training Branch

AFFOR—Air Force Forces

AFH—Air Force Handbook

AFI—Air Force Instruction

AFIAE—Air Force Intelligence Analysis Enterprise

AFISRAI—Air Force Intelligence, Surveillance, and Reconnaissance Agency Instruction

AFISRPoA—Air Force Intelligence, Surveillance, and Reconnaissance Program of Analysis

AFLCMC—Air Force Life Cycle Management Center

AFLLP—Air Force Lessons Learned Program

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFR—Air Force Reserve

AFRIMS—Air Force Records Information Management System

AFRL—Air Force Research Laboratory

AFSC—Air Force Specialty Code

AGILE—Advanced Global Intelligence Learning Environment

AIS—Air Intelligence Squadron

AMC—Air Mobility Command

AN—Anticipation

ANG—Air National Guard

AOC—Air Operations Center

AOR—Area of Responsibility

AS—Assessment

ASA—All-Source Analysis

BDA—Battle Damage Assessment

BOG—Board of Governors

Btn—Battalion

C-MAJCOM—Component MAJCOM

CAIAC—Civil Aviation Intelligence Analysis Center

CCIR—Commander's Critical Information Requirement

CCMD—Combatant Command

CCP—Consolidated Cryptologic Program

CFACC—Combined Forces Air Component Commander

CFETP—Career Field Education and Training Plan

CFLI—Core Function Lead Integrator

CGCIS—Coast Guard Counterintelligence Service

CGIS—Coast Guard Investigation Service

CIA—Central Intelligence Agency

CID—Criminal Investigation Command

CIP—Critical Intelligence Parameter

CMEIK—Center for Marine Expeditionary Intelligence Knowledge

CSA—Combat Support Agency

CTSAC—Critical Thinking and Structured Analysis Course

CY—Calender Year

CYBERCOM—Cyber Command

DART—Distributed Common Ground System Analysis and Reporting Team

DCGS—Distributed Common Ground System

DCS—Deputy Chief of Staff

DDII—Deputy Director of National Intelligence for Intelligence Integration

DE—Delivery

DEA—Drug Enforcement Agency

DHS—Department of Homeland Security

DI—Discovery

DIA—Defense Intelligence Agency

DIAAE—Defense Intelligence All-Source Analysis Enterprise

DIAD—DIA Directive

DIAI—DIA Instruction

DIAP—Defense Intelligence Analysis Program

DIRINT—Director of Intelligence

DNI—Director of National Intelligence

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DOE—Department of Energy

DOS—Department of State

DOTMLPF-P—Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy

EEI—Essential Element of Information

EVE—Evaluation of Evidence

EX—Explanation

FAC—Framework for Analytic Cognition

FBI—Federal Bureau of Investigation

FFIR—Friendly Force Information Requirements

GDIP—General Defense Intelligence Program

GEOINT—Geospatial Intelligence

GIISR—Global Integrated Intelligence, Surveillance, and Reconnaissance

HPW—Human Performance Wing

HUMINT—Human Intelligence

IAW—In Accordance With

IC—Intelligence Community

ICAT-G—Intelligence Community Analytic Tradecraft Gateway

ICC—Intelligence Coordination Center

ICD—Intelligence Community Directive

ICS—Intelligence Community Standard

ID—Identification

IDIP—Integrated Defense Intelligence Priorities

IMD—Intelligence Mission Data

INSCOM—Intelligence and Security Command

INT—Intelligence

IRTPA—Intelligence Reform and Terrorism Prevention Act

ISR—Intelligence, Surveillance, and Reconnaissance

ISRD—Intelligence, Surveillance, and Reconnaissance Division

ISRW—Intelligence, Surveillance, and Reconnaissance Wing

ISSO—Intelligence Systems Support Office

JCA—Joint Capability Area

JCS—Joint Chiefs of Staff

JIDA—Joint Improvised-Threat Defeat Agency

JIOC—Joint Intelligence Operations Center

JIPOE—Joint Intelligence Preparation of the Operational Environment

JLLIS—Joint Lessons Learned Information System

JLLP—Joint Lessons Learned Program

JP—Joint Publication

JTF—Joint Task Force

JWICS—Joint Worldwide Intelligence Communications System

KIQ—Key Intelligence Question

LL—Lessons Learned

MAJCOM—Major Command

MASINT—Measurement and Signature Intelligence

MCIA—Marine Corps Intelligence Activity

Mgrs—Managers

MICF LANT—Maritime Intelligence Fusion Center Atlantic

MICF PAC—Maritime Intelligence Fusion Center Pacific

MICT—Management Internal Control Toolset

MIP—Military Intelligence Program

MOM—Motive, Opportunity and Means

MOSES—Manipulability of Sources

MQT—Mission Qualification Training

MSIC—Missile and Space Intelligence Center

NAF—Numbered Air Force

NAI2O—National Aviation Intelligence Integration Office

NASIC—National Air and Space Intelligence Center

NCIS—Naval Criminal Investigative Service

NCTC—National Counterterrorism Center

NGA—National Geospatial-Intelligence Agency

NGIC—National Ground Intelligence Center

NGP—National Geospatial-Intelligence Program

NIP—National Intelligence Program

NIPF—National Intelligence Priorities Framework

NIPRNet—Nonsecure Internet Protocol Router Network

NOFORN—Not Releaseable to Foreign Nationals

NRO—National Reconnaissance Office

NRT—Near-real-time

NSA—National Security Agency

NSC—National Security Council

NTI—National Tactical Integration

OBP—Object-Based Production

OCTANE—Online Critical Thinking and Analysis Environment

ODNI—Office of the Director of National Intelligence

ONI—Office of Naval Intelligence

OPR—Office of Primary Responsibility

OSINT—Open-Source Intelligence

OV-1—Operational Viewpoint-1

PACAF—Pacific Air Forces

PCPAD—Planning and Direction, Collection, Processing and Exploitation, Analysis and Production, Dissemination and Integration, Evaluation and Feedback

PED—Processing, Exploitation, and Dissemination

PIR—Priority Intelligence Requirement

PoA—Program of Analysis

POP—Past Opposition Practices

PPBE—Planning, Programming, Budgeting, and Execution

PR—Production Requirement

RDS—Records Disposition Schedule

RDT&E—Research, Development, Test, and Evaluation

RFI—Request for Information

RFS—Request for Support

RPA—Remotely Piloted Aircraft

RT—Real-time

SAC—Self-Assessment Communicator

SAINT—Scoped Activity-based Intelligence for Nodal Targeting

SAT—Structured Analytic Technique

SecDef—Secretary of Defense

SIGINT—Signals Intelligence

SIO—Senior Intelligence Officer

SIPRNet—SECRET Internet Protocol Router Network

SMC—Space and Missile Systems Center

SOC—Squadron Operations Center

SOM—Structured Observation Management

TRANSCOM—Transportation Command

TS/SCI—TOP SECRET/Sensitive Compartmented Information

TSA—Target System Analysis

TTPs—Tactics, Techniques, and Procedures

USA—U.S. Army

USAF—U.S. Air Force

USAFE-AFAFRICA—U.S. Air Forces in Europe & Air Forces Africa

USCG—U.S. Coast Guard

USD(I)—Under Secretary of Defense for Intelligence

USMC—U.S. Marine Corps

USN—U.S. Navy

Terms

Abductive Reasoning—The process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. Abductive reasoning starts from a set of accepted facts and creatively proposes their best explanation.

AF Intelligence Analysis Enterprise (AFIAE)—The global community of analyst Airmen and the AF ISR organizations that employ the core competency of intelligence analysis.

All-Source Analysis—Intelligence analysis that employs all available sources of data and information to enable the creation of new intelligence and knowledge.

Analysis Center—An organization with a predominant mission of all-source analysis. Analysis centers provide timely, accurate, and relevant intelligence analysis to support national and defense policymakers, warfighters, and the acquisition community.

Analysis Skill—A specific ability or collection of capabilities required to competently conduct analysis that is acquired through training and/or experience.

Analysis Tradecraft—An established or prescribed analysis technique, practice, or systematic process.

Analyst Airman—An AF ISR professional who is skilled and certified in tradecraft to perform the core competency of intelligence analysis.

Analytic Ombuds—Representative that is responsible for addressing organizational concerns regarding lack of objectivity, bias, politicization, or other concerns in the application of analysis and production standards.

Analytic Production Steward—Senior AF official designated to represent the analysis and production activities that their respective element is authorized to conduct, and to make determinations regarding the dissemination to or retrieval by authorized personnel of analysis produced by that activity.

Best Practice—A method or technique that has consistently shown results superior to those achieved with other means.

Big Data—A concept used to describe the explosion of available data as a result of the information environment.

Counterintelligence—Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or their agents, or international terrorist organizations or activities.

Counterintelligence Analysis—The process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of a Foreign Intelligence Entity.

Covered Analytic Product—A subset of disseminated analytic products or services that is officially designated by the respective IC element as falling under the authority of ICD 206.

Critical Intelligence Parameter—A factor which clearly defines the threshold at which the performance of a foreign system/capability will likely compromise the program / mission effectiveness of the U.S. system.

Critical Thinking—The intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated through observation, experience, reflection, reasoning, or communication, as a guide to belief and action.

Deductive Reasoning—Reasoning where a conclusion is a logical consequence of the premise. A deduction moves from general rules and some evidence to particular cases.

Defense Intelligence All-Source Analysis Enterprise (DIAAE)—The collective set of all DoD organizations that execute all-source analysis activities in production of defense intelligence.

Defense Intelligence All-Source Analysis Enterprise Board of Governors (DIAAE BOG)—A body comprised of representatives of the organizations of the DIAAE that provides a forum for issue identification and resolution; improving transparency and synchronization across the DIAAE; implementing DIAAE strategies and processes; providing support to the DoD Functional Manager for All-Source Analysis; and making resource recommendations based on changes to priorities and emerging requirements.

Essential Element of Information (EEI)—A specific information requirement that supports a more general Priority Intelligence Requirement (PIR).

Fusion Analysis (also called Time-Dominant Fusion)—Analysis in a time-sensitive environment in close proximity to the point of collection that entails quickly melding new information with baseline knowledge to meet a specific operational need. Emphasis is on the process of managing information and on timeliness over completeness.

Inductive Reasoning—The intellectual process of drawing generalizations on the basis of observations or other evidence. Induction takes place when one learns from experience.

Intelligence Analysis—A cognitive activity–both art and science–applying tools, processes, tradecraft, methods, and judgements to data and information to create and deliver new intelligence, insights, and knowledge, with the goal of providing a decision advantage to commanders and decision makers.

Intelligence Customer (also called Intelligence Consumer)—A requestor or user of intelligence, including an operational unit, an acquisition organization, a national policy maker, or an intelligence organization.

Intelligence Production—The development, tailoring, and presentation of intelligence knowledge via products and/or services that address customer requirements.

Intelligence Requirement—(also called Request for Information, Production Requirement, Request for Support, or Key Intelligence Question)—A need for intelligence to fill a gap in knowledge or understanding of the environment, adversary capabilities, centers of gravity, or intentions.

Intelligence Support Element—An AF intelligence organization at any echelon whose focus is on providing intelligence for AF planning, operation, or decisions.

ISR Activity—A task undertaken by a member of the ISR community that is associated with the accomplishment of an intelligence mission. An ISR Activity could result in one or more intelligence outputs. ISR Activities do not include tasks carried out by ISR personnel that are unrelated to a specific intelligence mission, such as security force augmentation, honor guard duty, professional military education, or physical training.

ISR Output—The result of an ISR Activity. An output is categorized as either an ISR product or an ISR service. Single or multiple outputs may derive from one activity, or one output could be derived from multiple Activities. All outputs relate directly or indirectly to the accomplishment of an intelligence mission.

ISR Product—A specific type of output from an ISR activity that consists of tangible information in written, visual, digital, and/or verbal form that conveys information of intelligence value (e.g., written assessment, threat map, and targeting materials) or facilitates the accomplishment of an intelligence mission (e.g., ISR program element code build, self-assessment checklist, or training folder).

ISR Service—A type of output from an ISR Activity. Assistance provided to another entity during the performance of an ISR mission: (1) the actual action of delivering or conveying intelligence to a user (e.g., presenting a briefing, tipping and cuing, collaboration, or threat modeling), or (2) the process of enabling an ISR mission (e.g., exercise planning, skill

knowledge training, or security clearance indoctrination). Some ISR Services result in additional ISR Products.

Key Intelligence Question—A strategic, high-level question that states the primary unknown, or information need, about an intelligence issue or problem, which subsequently drives intelligence analysis and/or production within an organization.

Lead/Designated Producer—The primary analysis and production organization responsible for integrating collaborative analysis with its own to provide a comprehensive and accurate intelligence product or service to a customer.

Lesson Learned—An observation that, when validated and resolved, results in an improvement in military operations or activities at the strategic, operational, or tactical level and in long-term, internalized change to an individual or an organization.

Multi-Source Analysis (also called Multi—INT Analysis)—Intelligence analysis that makes use of more than one source when access to additional potential sources is limited by reasons of timeliness, system access, location, or security levels.

Priority Intelligence Requirement (PIR)—A critical requirement that a commander and staff need to understand the adversary or operational environment to conduct the mission. A PIR is typically comprised of multiple, specific Essential Elements of Information (EEIs).

Production Response—An agreement between a lead/designated producer and a customer for the production of intelligence, containing sufficient detail to permit customer acceptance, rejection, or modification of the proposed intelligence output.

Service Intelligence Center—The analysis center designated for each military service. The AF has designated NASIC as the service intelligence center for the AF.

Single-Source Analysis (also called Exploitation)—Intelligence analysis that employs a single source or expertise in a functional area to characterize events, people, or things. Such analysis is limited to describing, rather than evaluating, the topic of a particular analysis due to restrictions inherent in single-source intelligence collection, precluding the ability to provide fully contextualized intelligence assessments.

Attachment 2

PRODUCT AND SERVICE LINES

A2.1. As Table A2.1, *Product and Service Line Categories*, illustrates, AF products and services are grouped into 14 product lines and 14 service lines, which can be further classified into four general categories: awareness; mission-specific; representation; and enabling. Sections A2.2 and A2.3 describe each product and service line.

Table A2.1. Product and Service Line Categories.

Category	Product Lines	Service Lines
Awareness	Intelligence Assessment Threat Study Intelligence Summary Intelligence Report Intelligence Alert	Analysis Situational Awareness Collaboration Intelligence Supportability Analysis
Mission Specific	Mission Document Targeting Document Requirement	Mission Operations Targeting Mission Readiness Operational Mission Training Requirements Management
Representation	Database Briefing Display Model	
Enabling	Policy, Plan or Program Mission Support Document	ISR Professional Training Policy, Planning, and Programming Force Management ISR Systems Security

Notes:
1. Some Product and Service Lines have similar labels. A good rule of thumb in distinguishing between them is that a Product Line is focused on a tangible output while a Service Line is focused on the action, process or function that results in the Product Line.
2. Product Lines include sanitized and releasable versions of products.
3. The scope, focus, and window of analysis decrease from Assessments to Alerts.
4. The Enabling category includes those products and services that indirectly contribute to substantive intelligence but, in and of themselves, do not have a primary purpose of

substantive intelligence.

A2.2. ISR Product Lines.

A2.2.1. **Intelligence Assessment** –Strategic, longer-term, analytical publication; focused on future capabilities and intentions; usually broad in military and/or political scope.

A2.2.2. **Threat Study** –Longer-term analysis that is more narrowly scoped than an assessment; usually focused on a threat system or category of threat systems; generally strategic or operational in scope.

A2.2.3. **Intelligence Summary** –Roll-up historical analysis of multiple events or missions; shorter timeframe than an assessment or a study (e.g., daily or weekly summary).

A2.2.4. **Intelligence Report** –Analysis from a single event or mission; includes results from a single-source intelligence collection; often associated with mission results; generally tactical or operational in scope.

A2.2.5. **Intelligence Alert** –High priority intelligence update with potential urgency and/or mission impact; usually focused on a singular threat or data point.

A2.2.6. **Database** –Systematically arranged collection of data, structured for convenient access and manipulation, generally in a computer.

A2.2.7. **Policy, Plan or Program** –Official ISR policy; guidance; plans; TTPs; research, development, test, and evaluation (RDT&E) efforts; agreements; and resourcing data, to include PPBE-related documentation.

A2.2.8. **Mission Document** –Text-based materials associated with conducting an ISR-specific mission or other air/space/cyber operational mission; does not include target materials.

A2.2.9. **Targeting Document** –Text-based analysis, reports, lists, or publications associated with targeting, weaponeering, or battle damage assessment (BDA); includes hard copy and soft copy formats; does not include target briefings or stand-alone target graphics.

A2.2.10. **Requirement** –A need for intelligence information, such as a request for information, a collection need, and essential mission information.

A2.2.11. **Mission Support Document** –Text-based materials that assist in the accomplishment of some enabling activities, such as training, exercises, conferences, security, and continuity.

A2.2.12. **Briefing** –Graphic-based presentation that is usually delivered verbally. Often times, a briefing is developed to visually summarize and verbally present the results of a text-based product (e.g., assessment, study, target document or mission support document). The most common form of a briefing is a Microsoft PowerPoint presentation.

A2.2.13. **Display** –Visual representation of analysis. Formats include maps, charts, videos, graphics, and diagrams. Displays are often incorporated into briefings or text-based products.

A2.2.14. **Model** –Physical representation of a threat or threat system or artificial representation of how a threat system will perform in actual operations.

A2.3. ISR Service Lines.

A2.3.1. **Analysis** –Services associated with the evaluation, interpretation, and often times integration of intelligence from available data sources and types. Includes the conduct of single-source, multi-source, and all-source analysis.

A2.3.2. **Mission Operations** –Services associated with the conduct of air/space/cyber operational missions, including ISR collection and processing, exploitation, and dissemination (PED) missions.

A2.3.3. **Situational Awareness** –Services provided to assist leadership and operators, including other ISR professionals, in comprehensively understanding the threat environment in which they are focused.

A2.3.4. **Intelligence Supportability Analysis** –The process by which intelligence, acquisition, and operations analysts identify, document and plan for requirements, needs, and supporting intelligence infrastructure necessary to successfully acquire and employ AF capabilities.

A2.3.5. **Targeting** –Services associated with the development of target materials, weaponeering, and BDA.

A2.3.6. **Mission Readiness** –Services that support the preparedness or capability of ISR or operational units to carry out their assigned missions.

A2.3.7. **ISR Professional Training** –Services involving the training and education of ISR personnel in ISR-related skills and tradecraft. Includes Mission Qualification Training (MQT) of ISR personnel.

A2.3.8. **Operational Mission Training** –Services associated with *threat-related* training of operational mission crews. Includes threat training for ISR personnel assigned to operational crews, such as cyber defense mission crews.

A2.3.9. **Requirements Management** –Services focused on managing ISR capability needs, requests for intelligence, and requests for assistance, forces, resources, or essential mission information.

A2.3.10. **Policy, Planning, and Programming** –Services involving the development of ISR policy, guidance, plans, TTPs, RDT&E efforts, agreements, and resource management, to include PPBE support.

A2.3.11. **Force Management** –Services associated with governing or guiding ISR manpower and personnel.

A2.3.12. **ISR Systems** –Services involving the establishment, accreditation, maintenance, and employment standards of ISR information technology systems.

A2.3.13. **Security** –Services associated with the protection, sanitization, and disclosure of classified information and with the establishment/maintenance of classified facilities.

A2.3.14. **Collaboration** –Services that explicitly facilitate the sharing of information both within and outside of the ISR community. While all Services involve "sharing information" to a certain extent, the Services in this Service Line are functions whose primary purpose is to share or exchange information.

Attachment 3

COMMON ANALYSIS LESSONS

A3.1. Table A3.1, *Common Analysis Lessons,* captures some of the general considerations broadly accepted across the AF ISR Enterprise and proven effective in improving analysis capabilities throughout time. Key sources for the lessons in this table include subject matter experts with extensive operational and tactical experience, various AF/A2 reviews of intelligence analysis, and a study by RAND Corporation. The table is organized by chapters in this handbook. The identification (ID) column refers to the AFH chapter associated with each lesson along with a unique alpha designator. To the right of the lessons are five columns that correspond to the five analysis activities: Discovery (DI), Assessment (AS), Explanation (EX), Anticipation (AN), and Delivery (DE). Those five columns indicate the primary (large, bold, upper-case X), secondary (standard, upper-case X), and tertiary (lower-case x) analysis activities associated with each lesson.

Table A3.1. Common Analysis Lessons.

ID	LESSON	ANALYSIS ACTIVITIES				
Chp 2	**AF Intelligence Analysis Enterprise (AFIAE)**	**DI**	**AS**	**EX**	**AN**	**DE**
2A	Increase your knowledge of different analytic and PED organizations to best understand AF ISR capabilities, enhance your network, and improve your tradecraft.	**X**	x	x		
2B	Be knowledgeable of air/space/cyber power strategy and theater objectives to help your assessment of developments.		**X**			
2C	Understand the larger context of the theater, problem set, or operation in which you are focused—applies to all analysts.	**X**				
2D	Check with area of responsibility (AOR) analysts to help collaborate your assessment of activities in that theater.		**X**			
2E	Coordinate with theater-specific and 363 ISRW targeteers for full understanding of your target and assessments.		**X**			
2F	Become familiar with different theaters to widen your expertise.			**X**		
2G	Continually balance timely notification to decision makers in support of operations against more in-depth and deliberate analysis/assessments.				**X**	
Chp 3	**IC and other Military Service Capabilities**	**DI**	**AS**	**EX**	**AN**	**DE**
3A	Gain Joint experience at a regional JIOC for improved & integrated analysis.			**X**	X	
3B	Seek out assignments in or deployments to an operational AOR to deepen and broaden your analysis expertise.			**X**	X	

3C	Be aware of U.S. military and theater capabilities and those of coalitions to enhance your analysis.			**X**		
3D	Prepare for future operations in a communications-contested environment; use/build resident capabilities prior to any deployment or operation.	x	x	x	**X**	x
3E	Enhance your Open-Source Intelligence (OSINT) expertise and understanding of IC-wide OSINT capabilities and organizations to leverage during crisis operations and to enhance your analytic prowess.	**X**				
3F	Improve your network with special operations ISR personnel for enhanced interface in-theater.		**X**	x	X	
Chp 5	**Analysis Skills and Tradecraft**	**DI**	**AS**	**EX**	**AN**	**DE**
5A	Leverage IC and joint programs that train, develop, and/or equip analysts to properly use tradecraft and provide better analysis.	x	x	**X**	X	x
5B	Participate in AF and Joint exercises to help sharpen analytic and joint awareness skills prior to an operational deployment.		x	**X**	X	
5C	Expand expertise and analytic skills beyond traditional warfare constructs to also be familiar with irregular warfare and non-traditional enemies.	**X**	x	x		
5D	Develop a network for improved collaboration/Red Teaming in different theaters.		x	**X**	X	
5E	Leverage theater and target-specific linguists as a good source to Red Team analysis, especially given adversary insights.		x	**X**	X	
5F	Leverage expertise and skills from multiple disciplines including scientists, engineers, space and cyber professionals, meteorologists, and the medical community for effective intelligence analysis.	x	x	**X**	X	
5G	Understand knowledge management, data science, and big data analytic concepts and principles for improved data aggregation.			**X**	X	
5H	Don't become influenced/infatuated with a particular sensor or source; cross-reference/check with multiple sources.	**X**				
Chp 6	**Analysis Requirements and Production**	**DI**	**AS**	**EX**	**AN**	**DE**
6A	Educate customers on AF ISR capabilities so they can help provide the best analysis possible to meet existing requirements.					**X**
6B	Understand what products are currently available and who is already working on/analyzing similar requirements to ensure unity of purpose and avoid duplication of effort.	**X**				
6C	Understand basic acquisition-/IMD-related intelligence requirements to help better align assessments in support		**X**			

	of respective customers.					
6D	Prepare now for the operations and warfare of tomorrow; expect contingency operations to occur in your area of analytic expertise and pre-plan against your analytic target with pre-positioned RFIs, target identification, etc.	x			**X**	
6E	Coordinate/interface often with resident collection managers on assessments and proposed collection strategies.	x	**X**		X	
6F	Enhance your ability to assess risks associated with commander estimates and plans (e.g., operational plans, contingency plans, etc.) for improved utility and interface with traditional operations.		**X**			
6G	Always consider the commander's intent, end state, definition of success, and the potential adversary centers of gravity when performing analysis.			x	**X**	
6H	Develop the analysis/assessment then take a final "step back" to review again from a strategic mindset and perspective.		x	**X**		
6I	Strive to produce assessments that are releasable and only make products/services “Not Releaseable to Foreign Nationals (NOFORN)” or caveated when required.					**X**

Notes:
1. The list is not intended to be comprehensive or all inclusive, nor is it intended to serve as a checklist that analyst Airmen are expected to meet. The aim is for analyst Airmen and analysis organizations across the AF to refine and expand the list over time.
2. Key sources for the lessons learned in this table include subject matter experts, various AF/A2 reviews of intelligence analysis, and a study by RAND Corporation: Brien Alkire, et al., *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis*, RR-1330-AF.

A3.2. Some of the intelligence analysis lessons in Table A3.1 have been formally documented in some form or fashion via the AF Lessons Learned (LL) Program (AFLLP). The AFLLP exists to enhance readiness and improve combat capability by capitalizing on the experiences of Airmen and organizations. A lesson learned is an observation that, when validated and resolved, results in an improvement in military operations or activities at the strategic, operational, or tactical level and in long-term, internalized change to an individual or an organization. The AFLLP is part of the larger Joint Lessons Learned Program (JLLP). The Joint LL Information System (JLLIS) is used to track and disseminate LLs throughout the AF, DoD, and IC. JLLIS allows AF personnel to search, submit, and manage all AF Observations, Lessons Identified, After Action Reports, LLs, and other information up to TOP SECRET/Sensitive Compartmented Information (TS/SCI). The JLLIS database is located at SIPRNet Caution-url: **https://www.jllis.smil.mil**. All analyst Airmen are encouraged to register in JLLIS and enter observations that contain potential lessons into JLLIS for coordination through the AFLLP and/or inform their local chain of command as appropriate.

A3.3. In addition, several MAJCOMs actively acquire lessons learned or best practices. For example, HQ ACC/A2OO (Weapons and Tactics) has established a program to capture lessons learned, TTPs, and experience from ISR professionals returning from deployments.

Attachment 4

SAMPLE STANDARDS EVALUATION METHODOLOGY

A4.1. IAW AFI 14-133, MAJCOM/A2s and the NASIC/CC are responsible for developing a means to annually measure and assess AF intelligence analysis standards via SACs for reporting in the MICT. In addition, the DNI requires the AF to annually evaluate specified "covered products" for compliance with IC standards. Table A4.1, *IC Product Evaluation Criteria and Rating Scales*, delineates IC analytic tradecraft standards for use in assessment and "covered product" evaluations. The JWICS Advanced Global Intelligence Learning Environment (AGILE) offers computer-based training on how to conduct product evaluations. It is important to note that while AF tradecraft standards align with IC standards, the AF evaluates two additional standards: timeliness and customer engagement. Table A4.2, *Sample Tradecraft Criteria for Timeliness*, and Table A4.3, *Sample Tradecraft Criteria for Customer Engagement*, offer considerations for self-assessment on these two additional AF standards.

Table A4.1. IC Product Evaluation Criteria and Rating Scales.

Reviewer		Objective	1. Yes	2. No
Date of Review		Independent of political consideration	☐ Yes	☐ No
Product Name		Timely	☐ Yes	☐ No
Product ID Number		Based on all available sources of intelligence	☐ Yes	☐ No

1. Properly describes quality and credibility of underlying sources, data, and methodologies			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Largely lacks sourcing or describes reporting base, data, or methodologies only vaguely; **OR** ☐ Misidentifies or misrepresents cited reporting, data, or methodologies.	☐ Contains basic, generic descriptions of cited reporting, data, or methodologies; **BUT** ☐ Provides little detail on factors that may affect the quality and credibility of underlying sources, data, or methodologies.	☐ Contains at least basic, generic descriptions of cited reporting, data, or methodologies; **AND** ☐ Provides considerable detail on factors that may affect the quality and credibility of underlying sources, data, or methodologies.	☐ Satisfies "good" criteria; **AND** 1. Identifies which sources are most important to major analytic judgments; **OR** ☐ Provides additional detail about sources, data, or methodologies that provides insight into their contribution to the analysis.
Comment:			

2. Properly expresses and explains uncertainties associated with major analytic judgments			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Does not indicate levels of uncertainty associated with major analytic judgments; **OR** ☐ Indicates levels of uncertainty associated with major analytic judgments that are inconsistent with the basis ascribed to them.	☐ Indicates levels of uncertainty associated with major analytic judgments; **BUT** ☐ Does not explain their basis (e.g., by reference to strengths and weaknesses of the information base, contrary reporting, assumptions, or the nature of the judgment).	☐ Indicates levels of uncertainty associated with major analytic judgments; **AND** ☐ Explains their basis (e.g., by reference to strengths and weaknesses of the information base, contrary reporting, assumptions, or the nature of the judgment).	☐ Satisfies "good" criteria; **AND** **1.** Provides especially thorough discussion of nature and sources of uncertainties affecting major analytic judgments; **OR** ☐ Identifies indicators that, if detected, would alter levels of uncertainty associated with major analytic judgments.
Comment:			

3. Properly distinguishes between underlying intelligence information and analysts' assumptions and judgments			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)

☐ Does not distinguish among statements that convey underlying information, assumptions, and judgments.	☐ Sometimes distinguishes among statements that convey underlying information, assumptions, and judgments; **OR** ☐ Does not explicitly state assumptions that serve as linchpins of an argument or bridge key information gaps.	☐ Consistently distinguishes among statements that convey underlying information, assumptions, and judgments; **AND** ☐ Explicitly states assumptions that serve as linchpins of an argument or bridge key information gaps.	☐ Satisfies "good" criteria; **AND** 1. Identifies indicators that, if detected, could validate or refute judgments or assumptions; **OR** ☐ Explains the implications for judgments if assumptions are incorrect.
Comment:			
4. Incorporates alternative analysis			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Does not present alternatives when uncertainties, complexity, or low probability / high impact situations warrant their inclusion.	☐ Presents alternatives when uncertainties, complexity, or low probability / high impact situations warrant their inclusion; **BUT** ☐ Does not explain the evidence and reasoning that underpin them or discuss their likelihood or implications related to U.S. interests.	☐ Presents alternatives when uncertainties, complexity, or low probability / high impact situations warrant their inclusion; **AND** ☐ Explains the evidence and reasoning that underpin them; **AND** ☐ (c) Discusses their likelihood or implications related to U.S. interests.	☐ Satisfies "good" criteria; **AND** ☐ Identifies indicators that, if detected, would affect the likelihood of any identified alternatives.
Comment:			
5. Demonstrates customer relevance and addresses implications			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Provides little or no information or analysis beyond what is generally known; **OR** ☐ Does not respond adequately to a specific tasking.	☐ Provides useful information and analysis but does not address implications; **OR** ☐ Does not address an important issue or question raised by the analysis; **OR** ☐ Satisfies a specific tasking only partially.	☐ Provides useful information and analysis and addresses near-term, direct, or first-order implications; **AND** ☐ Adds value by addressing at least one of the following: trends or prospects, appropriate context, insight gained from synthesizing a large volume of information, warning of threats to U.S. interests, or factors affecting opportunities for U.S. actions (without prescribing U.S. policy); **OR** ☐ Satisfies a specific tasking fully.	☐ Satisfies "good" criteria; **AND** ☐ Assesses longer-term, indirect, or second-order implications; **OR** ☐ Provides exceptionally expert analysis (e.g., by drawing on multiple disciplines or presenting illuminating comparisons); **OR** ☐ Warns of threats in detail (e.g., by discussing specific indicators, likelihood, or imminence); **OR** ☐ Analyzes in detail factors affecting opportunities for U.S. action (e.g., by discussing risks, benefits, or possible reactions to potential U.S. actions).
Comment:			
6. Uses clear and logical argumentation			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Lacks a main analytic message; **OR** ☐ Does not support analytic judgments with relevant evidence or undermines them by using flawed logic; **OR**	☐ Presents a main analytic message; **BUT** ☐ Does not combine evidence, context, and assumptions effectively to support analytic judgments or uses weak logic; **OR**	☐ Presents a prominent and clear main analytic message; **AND** ☐ Presents clear reasoning with no flaws in logic and effectively combines evidence, context, and	☐ Satisfies "good" criteria; **AND** ☐ Addresses any inconsistent or contrary information in a way that reconciles it with analytic judgments; **OR** ☐ Demonstrates notable skill or sophistication in combining evidence, context, and assumptions convincingly to

☐ Often uses unclear language or uses a structure that is not easily understood.	☐ Sometimes uses unclear language or a structure that at times is not easily understood.	assumptions to support analytic judgments; **AND** ☐ Uses clear language and a structure that displays a logical flow appropriate for the argument being presented.	support analytic judgments.
Comment:			

7. Explains change to or consistency of analytic judgments			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Does not note or explain that a major analytic judgment differs from previous production.	☐ Does not note that a major analytic judgment is consistent with previous production; **OR** ☐ Notes how a major analytic judgment compares with previous production but does not explain how new information or reasoning supports changing or maintaining an existing analytic line.	☐ Notes how a major analytic judgment compares with previous production and explains how new information or reasoning supports changing or maintaining an existing analytic line.	☐ Satisfies "good" criteria; **AND** ☐ Highlights and explains how a major analytic judgment compares with judgments on the topic held within the U.S. intelligence community, not just within the same analytic element.
Comment:			

8. Makes accurate judgments and assessments			**Harvest Date:**		
Phase 1			**Phase 2:** Often accuracy cannot be evaluated until a later date. Establish a "harvest" date to revisit the assessment to evaluate Phase 2.		
☐ Unclear	☐ Conditioned	☐ Unconditioned	☐ Accurate	☐ No Accurate	☐ Indeterminate
☐ Judgment or assessment is not expressed clearly.	☐ Judgment or assessment is expressed clearly and is conditioned (e.g., by an "if/then" statement).	☐ Judgment or assessment is expressed clearly and is not conditioned (e.g., by an "if/then" statement).	☐ Judgment or assessment is found to be accurate.	☐ Judgment or assessment is found to be not accurate.	Accuracy could not be determined for any of several reasons: ☐ Nature of judgment or assessment prevented assessment of accuracy. ☐ Data needed to assess accuracy were not found. ☐ Irreconcilable views among evaluators prevented agreement on a final assessment of accuracy.
Comment:					

9. Incorporates effective visual information where appropriate			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Does not use visual information when its use would have substantially complemented or enhanced an analytic product; **OR** ☐ Presents visual information that is inconsistent with or not pertinent to the text of an analytic product, or that confuses or detracts from an analytic product's presentation.	☐ Presents visual information that is pertinent to an analytic product; **BUT** ☐ Does little to clarify (illustrate, summarize, or provide greater detail), complement, or augment data or analytic points in an effective manner that enhances customer understanding of a product's analysis.	☐ Presents visual information that is pertinent to an analytic product; **AND** ☐ Clarifies (illustrates, summarizes, or provides greater detail), complements, or augments data or analytic points in an effective manner that enhances customer understanding of a product's analysis.	☐ Satisfies "good" criteria; **AND** ☐ Takes particularly effective advantage of visual presentational methods to convey data or analytic points in a way that enhances a product's value by making complex issues more understandable, adding insight or perspective, increasing knowledge retention, or highlighting trends, drivers, or indicators.
Comment:			

General Comments:
If an evaluator determines that a standard is **not applicable**, *it should be noted, with a justification, in the comment box.*

Table A4.2. Sample Tradecraft Criteria for Timeliness.

1. Poor (0)	2. Fair (1)	3. Good (2)	4. Excellent (3)
5. ISR element fails to provide analysis products and services in sufficient time to impact planning, operations, and decision-making	6. ISR element timeliness in providing analysis products and services marginally impacts planning, operations and decision-making	7. ISR element provides analysis products and services in sufficient time to impact planning, operations, and decision-making	8. ISR element provides analysis products and services at the earliest time and place to enable decision advantage and create significant mission and capability opportunities
Comment:			
Note: AF intelligence analysis is timely to impact planning, mission objectives, operations and to otherwise aid in commanders' decisions. Analysts are responsible for engaging with customers and end-users of intelligence to understand what they need and when they need it in order to deliver information and knowledge at the earliest time and place to enable customers to effectively make decisions and take action. Timeliness is about ensuring awareness, creating opportunities, and enabling warfighting decision advantage.			

Table A4.3. Sample Tradecraft Criteria for Customer Engagement.

1. Poor (0)	2. Fair (1)	3. Good (2)	4. Excellent (3)
1. ISR element has limited engagement with the customer to understand their requirements or seek feedback on product/service timeliness or utility	2. ISR element requests and responds to customer feedback for some, but not all, products and services	3. ISR element requests and responds to customer feedback for all products and services	4. ISR element satisfies "good" criteria; **AND** 5. Regularly engages with the customer to anticipate their requirements by understanding their operations, listening to their questions and concerns, and identifying intelligence needs to support documented capabilities and concepts; **AND** **6.** Has a formal engagement program established
Comment:			
Note: Analysis fully address customers' requirements within the time constraints and in a manner most useful. Analyst Airmen are responsive to customer feedback. While challenging to evaluate, this tradecraft standard is foundational to AF intelligence analysis.			

Attachment 5

AF ISR SAT TRADECRAFT GUIDE

A5.1. The following 19 figures are excerpts from an AF tradecraft guide on SATs, developed by AFCO-CFA. The figures offer insight into some, but not all, of the key SATs used in intelligence analysis to help improve tradecraft standardization across the AFIAE.

Figure A5.1. Imagination Techniques and Indicators.

IMAGINATION TECHNIQUES AND INDICATORS

Core Techniques	Description	When to Use
Structured Brainstorming	A group process for generating new ideas and concepts	Used to stimulate new thinking and generate a range of hypotheses about an issue
Red Team	A function executed by trained, educated, and practiced team members that provide an independent capability to fully explore alternatives from the perspectives of partners, adversaries, and others	Used to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment
Alternative Futures Analysis	Tool to help analysts explore multiple ways a situation can develop when there is high complexity and uncertainty	Mostly used when a situation is viewed as too complex or the outcomes are too uncertain to trust a single outcome assessment
Outside-In Thinking	Analytical tool used to identify the full range of basic forces, factors and trends that would indirectly shape an issue	Used to identify all the critical, external factors that could influence how a situation will develop

Figure A5.2. Structured Brainstorming.

STRUCTURED BRAINSTORMING

A technique for stimulating new thinking. It can be applied to virtually all of the other structured analytic techniques and allows the analyst to see a wider range of factors that might bear on the topic.

Brainstorming Ground Rules

1. Never criticize an analyst's ideas
2. Allow sufficient time to brainstorm
3. Involve at least one "outsider" in the process

Divergent Thinking Phase

1. "Post-It" note exercise

Convergent Thinking Phase

1. Arrange notes by commonalities to form clusters
2. Some notes may be moved or copied as cluster form
3. Select a word or phrase that characterizes each cluster
4. Identify any notes that do not fit with others and consider them useless noise or the beginning of an idea that deserves further attention (wild cards)
5. Select one or two areas that deserve the most attention
6. Set priorities based on consensus and decide on the next steps for analysis

Figure A5.3. Red Team Analysis.

RED TEAM ANALYSIS

Function executed by trained, educated, and practiced team members to provide commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations, and capabilities in the context of the operational environment and from the perspectives of partners, adversaries, and others.

Red Team Techniques

1. Team puts themselves into the adversary's circumstance and reacts as the adversary would
2. Assessments are not coordinated with anyone outside the team
3. Develop set of "first person" questions
4. Draft policy papers in which the group makes decisions, proposes recommendations, or develops courses of action
5. Present analysis in the first-person format
6. Avoid use of caveats or qualifications
7. Focus on a prediction based on the adversary's world
8. Do not plot out all possible courses of action

Figure A5.4. Alternative Futures Analysis.

ALTERNATIVE FUTURES ANALYSIS

An imaginative technique that systematically explores multiple scenarios. This technique can be used when a situation's uncertainty and complexity require consideration of more than one outcome.

Six-Step Process

1. Develop a focused issue and intelligence question
2. Identify drivers, forces, factors, and variables that can affect the issue
3. Select the two most critical and uncertain drivers
4. Establish plausible endpoints for each driver
5. Form a futures matrix by crossing the two axes. The resulting quadrants are the basis for alternative future scenarios
6. Build narratives that describe these futures and how they might come to be (Signposts or Indicators can then be developed)

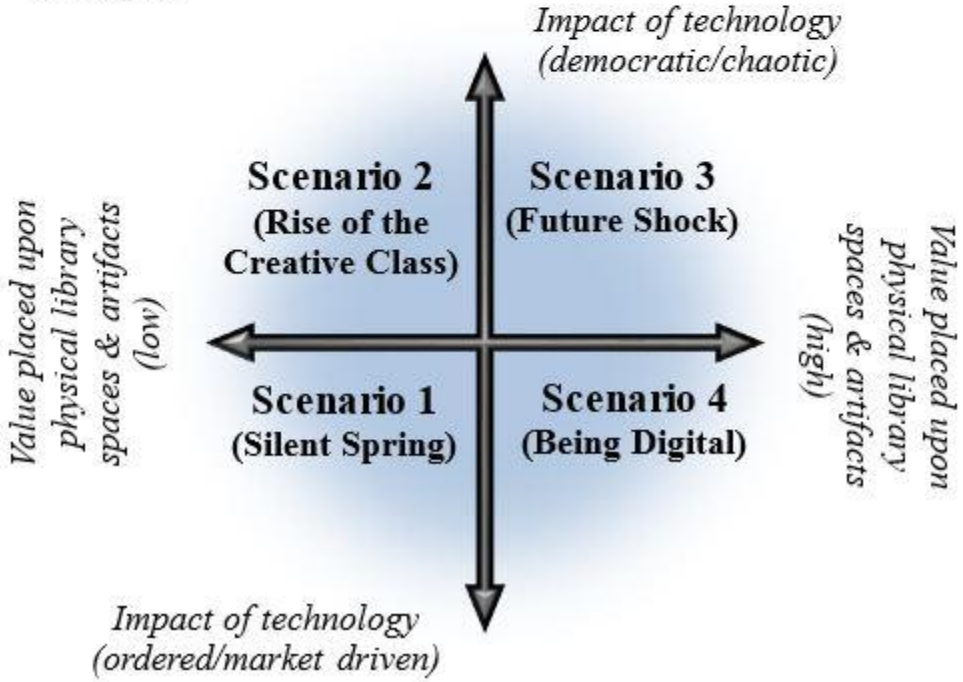


Figure A5.5. Outside-in Thinking.

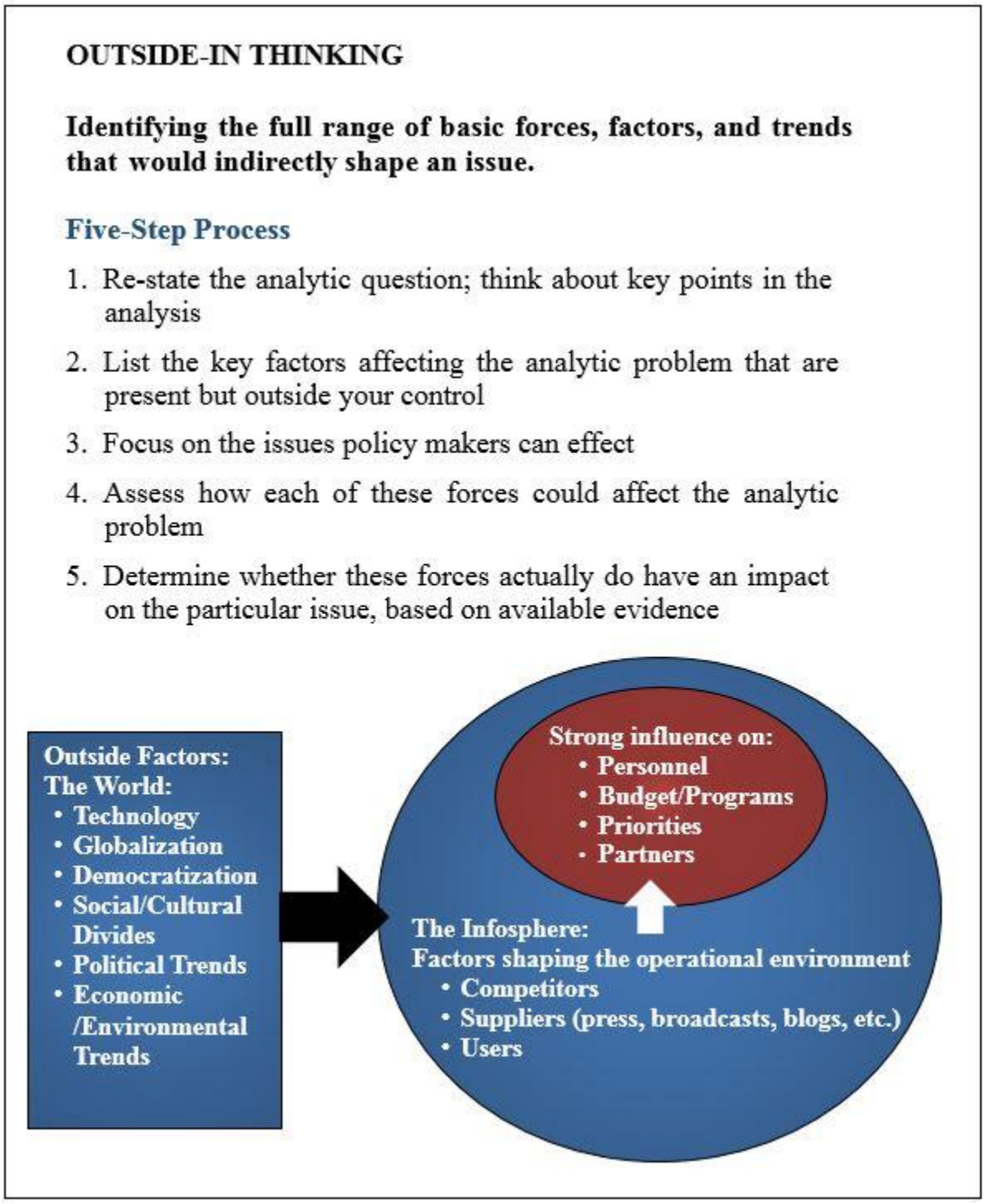


Figure A5.6. Diagnostic Techniques.

DIAGNOSTIC TECHNIQUES

Core Techniques	Description	When to Use
Key Assumptions Check	List and review the key working assumptions on which fundamental judgments rest	Most useful at the beginning of an analytic project
Quality of Information Check	Evaluate completeness and soundness of available information sources	Use to establish confidence level in analytic judgments, & ensure judgments are anchored to strong, relevant sources
Indicators or Signposts of Change	Reviewing observable events and trends to determine if a postulated situation is developing	Used to instill analytic rigor into the analytic process enhancing the credibility of analytic judgments
Deception Detection	Systematic use of checklists to determine when deception may be present and how to avoid being deceived	Used to counter adversary attempts of misinformation, concealment, and misdirection
Analysis of Competing Hypotheses	A systematic and logical approach to generate and evaluate all plausible hypotheses to solve a given problem	Any analysis where there are alternative explanations for what has happened, is happening, or is likely to happen

Figure A5.7. Key Assumptions Check.

KEY ASSUMPTIONS CHECK

A diagnostic technique that identifies hypotheses analysts have accepted to be true and that form the basis of the assumption

Four-Step Process

1. Review the analytic line on the issue; write it down for all to see and defend it orally
2. Articulate all the premises, both stated and unstated in finished intelligence, that are accepted as true for this analytic line to be valid
3. Challenge each assumption, asking why it must be true and whether it remains valid under all conditions
4. Refine the list of key assumptions to contain only those that must be true to sustain your analytic line; consider under what conditions, or in the face of what information, these assumptions might not hold

Questions to Ask

How much confidence exists that this assumption is correct?

What explains the degree of confidence in the assumption?

What circumstances or information might undermine this assumption?

Is a key assumption more likely a key uncertainty or key factor?

Could the assumption have been true in the past but be less so now?

If the assumption proves wrong, would it significantly alter the analytic line? If so, how?

Has this process identified new factors that need further analysis?

Figure A5.8. Quality of Information Check.

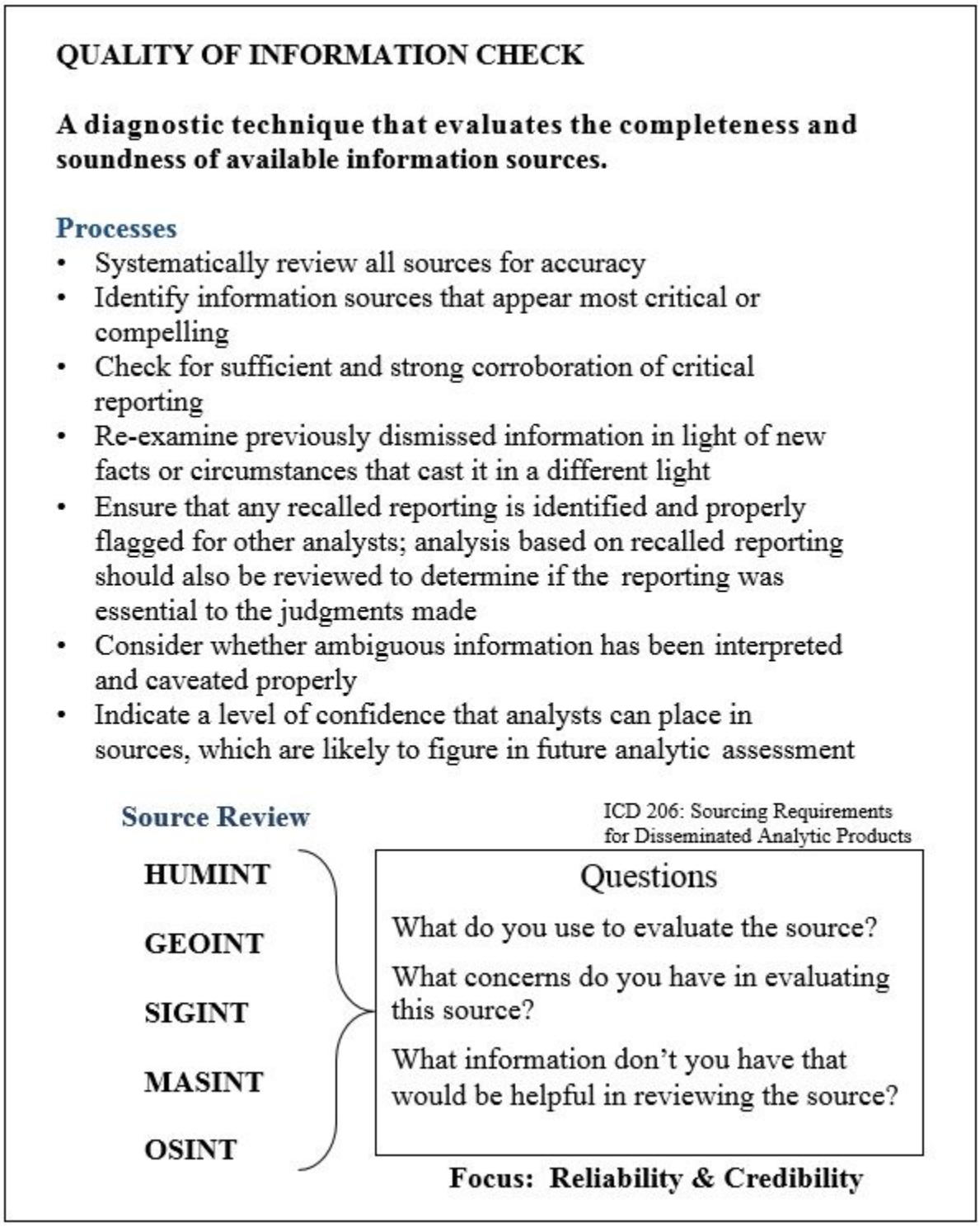


Figure A5.9. Indicators or Signposts of Change.

INDICATORS OR SIGNPOSTS OF CHANGE

Also called Signpost Analysis, this technique involves periodically reviewing a list of observable events or trends to track events, monitor targets, spot emerging trends, and warn of unanticipated change.

Indicator Technique Recommendations	
Analytic Environment	Indicator Technique
Non-Controversial • The issue is non-controversial within the IC or the policy community • Analysts and/or policymakers are uncertain about how the situation will actually evolve	• Simple lists of observables • Two contrasting lists of indicators (that would suggest a leader is growing stronger and a second list that he is growing weaker)
Somewhat Controversial • Some analysts or agencies have preferred positions or established equities to protect • The outcome has major policy or resource implications	• Use simple scales • Provide definitions for each indicator • Portray the information graphically • Revisit on periodic basis
Highly Controversial • Analysts hold strong, contrary views • Major institutional equities are at stake within the IC • The issue is highly charged within the policy community	• Provide a level of confidence for each rating • Provide a narrative description of what one would expect to observe at each level on a rating scale • List the sources of info and how important each was in establishing the rating

Figure A5.10. Deception Detection.

DECEPTION DETECTION

Diagnostic technique where analysts systematically use checklists to determine when deception actually may be present and how to avoid being deceived.

Does a foreign actor have the Motive, Opportunity and Means (MOM) to deceive?

1. Motive (What are the deceiver's goals?)
2. Channels (What means are available?)
3. Risks (What are the risks of discovery?)
4. Costs (Can deception be accomplished?)
5. Feedback (Can the deceiver monitor its use?)

Would this potential deception be consistent with Past Opposition Practices (POP)?

1. Does the deceiver have a history of deception?
2. Does this deception fit past patterns?

Is there cause for concern regarding the Manipulability of Sources (MOSES)?

1. Is the source reliable?
2. Does the source have access?
3. How good are the source's *bona fides*?
4. Is the source vulnerable to control or manipulation by the target?

What can be learned from the Evaluation of Evidence (EVE)?

1. How accurate is the source's reporting?
2. Is the whole chain of evidence available?
3. Does critical evidence check out?
4. Does evidence from one source conflict with others?
5. Do other sources of information provide corroborating evidence?
6. Is the absence of evidence unusual?

Figure A5.11. Analysis of Competing Hypotheses.

ANALYSIS OF COMPETING HYPOTHESES

Provides a systematic and logical approach to generate and evaluate plausible hypotheses to solve a given problem.

Eight-Step Process

1. Generate hypotheses
2. Gather and list evidence
3. Prepare the evidence and hypothesis matrix
4. Refine the matrix
5. Draw tentative conclusions
6. Perform sensitivity analysis
7. Report conclusions
8. Identify milestones

	Cred	Rel	H 1	H 2	H 3
Score			2	4	3
Evidence 1	H	H	C	C	C
Evidence 2	M	M	I	C	C
Evidence 3	M	M	C	C	I
Evidence 4	H	H	I	C	I
Evidence 5	M	M	I	I	C

H – High
M – Medium
L – Low

C – Consistent / Supports
I – Inconsistent / Does Not Support
N/A – Not Applicable

Figure A5.12. Focus Techniques.

FOCUS TECHNIQUES

Core Techniques	Description	When to Use
Issue Development	Used to ensure the central issues and alternative explanations of an issue or problem are identified within the scope and focus of the problem statement to aid in gathering the best answer	Used anytime analysts begin to assess a new issue or problem or begin a new research endeavor to mitigate bias toward the issue
Question Refinement	A simple technique to ensure analysts are answering the right question when responding to an intelligence requirement	Used when a consumer's intelligence requirement is not completely clear or when research begins to lead to ambiguity and confusion

Figure A5.13. Issue Development.

ISSUE DEVELOPMENT

A divergent technique that opens the mind of the analyst to substantive alternatives. Restating a problem opens it up and reveals important perspectives and issues otherwise overlooked.

Start with the initial poorly defined/stated issue

1. Paraphrase: Redefine the issue without losing the original meaning
2. 180 Degrees: Turn the issue on its head. Is the issue the one asked or the opposite of it?
3. Broaden the Focus: Instead of focusing on only one piece of the puzzle, step back and look at several pieces together
4. Narrow the Focus: Can the issue be broken down further? Take the question and ask about the components that make up the problem
5. Redirect the Focus: What outside forces impinge on this issue? Is deception involved?
6. Ask Why: Question the initial issue or question. Develop a new question based on the answer. Then question the second question and develop a new question based on that answer. Repeat this process until you believe the real problem emerges. This process is particularly effective in generating possible alternatives

End with a final refined issue

Figure A5.14. Question Refinement.

QUESTION REFINEMENT

A simple analytical technique used to ensure analysts are answering the right question when responding to a customer's intelligence requirement.

7-Step Process

1. **New Development -** Describe a change to the operating environment or security interests that result in a requirement for intelligence analysis and production.
2. **Raw Question(s) -** In response to the New Development, the immediate questions that come to mind, or that would come to mind for your customer. In relation to an event of interest, the raw questions could be, "Who did it and why?" or "What caused it?"
3. **Key Issue -** A key issue area normally includes an issue area and a geographic area. Issue areas are substantive categories of policy, strategy, or war fighting function. Key issue areas for a military operation can often be found in campaign descriptions of the lines of effort.
4. **National Interests -** The big picture must be considered thoughtfully when refining the intelligence requirement. Analysts should be able to tie assessments to U.S. security interests in general.
5. **Specific Customer Concerns -** This section of the refinery is often used to determine what questions are relevant and required to fulfill the intelligence question versus those specific requirements that might be better answered separately.
6. **Time Frame -** Answering your intelligence requirement should be targeted at a particular time, normally in the future (ex: "in the next 6 months," or "before 1 May 201X").
7. **Refined Question -** The refined intelligence question should be open-ended, requiring more than a yes or no answer, and should meet a specific customer's intelligence needs.

Figure A5.15. Contrarian Techniques.

CONTRARIAN TECHNIQUES

Core Techniques	Description	When to Use
Devil's Advocacy	Technique used to challenge a single, strongly held view or consensus by building the best possible case for an alternative explanation	Used when analysts need to provide further confidence that the current analytic line will hold up to close scrutiny
High Impact / Low Probability	Highlights a seemingly unlikely event that would have major policy consequences if it were to happen	Used when analysts believe an event is unlikely but have not given much thought to the consequences of its occurrence
What If? Analysis	A technique which assumes an event has occurred with potential (negative or positive) impact and explains how it might come about	Used to challenge a strong mindset that an event will not happen or be confidently justified
Team A / Team B Analysis	Separates teams to contrast two or more strongly held views or competing hypotheses	Used when there are two or more equally strong mind-sets held on an issue that need to be clarified (Devil's Advocacy challenges a single dominant mindset)

Contrarian: opposition or rejection of popular opinion

Figure A5.16. Devil's Advocacy.

DEVIL'S ADVOCACY

A contrarian technique for challenging a single, strongly held view or consensus by building the best-possible case for an alternative explanation.

Explicitly challenges key assumptions to see if they will not hold up under some circumstances.

Methodology

1. Outline the mainline judgment and key assumptions and characterize the evidence supporting the current analytic view
2. Select one or more assumptions—stated or not—that appear the most susceptible to challenge
3. Review the information used to determine whether any is of questionable validity, whether deception is possibly indicated, or whether major gaps exist
4. Highlight the evidence that could support an alternative hypothesis or contradicts the current thinking
5. Present to the group the findings that demonstrate there are flawed assumptions, poor quality evidence, or possible deception at work
6. Consider drafting a separate contrarian paper that lays out the arguments from a different analytic conclusion if the review uncovers major analytic flaws
7. Be sure that any products generated clearly lay out the conventional wisdom and are identified as an explicitly "Devil's Advocate" project; otherwise the reader can become confused as to the current official view on the issue

Figure A5.17. High Impact / Low Probability.

HIGH IMPACT / LOW PROBABILITY

A technique used to highlight a seemingly unlikely event that would have major policy consequences if it happened.

If there is a strongly-held view that an event is unlikely, then postulating precisely the opposite should not be difficult.

Perform the following steps to determine the effects of High Impact/Low Probability events:

1. Define the high-impact outcome clearly. This process is what will justify examining what most analysts believe to be a very unlikely development
2. Devise one or more plausible explanations for or "pathways" to the low probability outcome. This should be as precise as possible, as it can help identify possible indicators for later monitoring
3. Insert possible triggers or changes in momentum if appropriate. These can be natural disasters, sudden health problems of key leaders, or new economic or political shocks that might have occurred historically or in other parts of the world
4. Brainstorm with analysts having a broad set of experiences to aid the development of plausible but unpredictable triggers of sudden change
5. Identify for each pathway a set of indicators or "observables" that would help you anticipate that events were beginning to play out this way
6. Identify factors that would deflect a bad outcome or encourage a positive outcome

Figure A5.18. "What If" Analysis.

"WHAT IF" ANALYSIS

That "What If?" Analysis is the technique which assumes an event has occurred with potential (negative or positive) impact and explains how it might come about.

Method

1. Assume the event has happened
2. Select some triggering events that permitted the scenario to unfold to help make the "what if" more plausible; for example, analysts might postulate the death of a leader, a natural disaster, or some economic event that would start a chain of other events
3. Develop a chain of argumentation based as much on logic as evidence to explain how this outcome could have come about
4. "Think backwards" from the event in concrete ways–that is, specifying what must actually occur at each stage of the scenario is often very useful
5. Identify one or more plausible pathways or scenarios to the unlikely event; very often more than one will appear possible
6. Generate a list of indicators or "observables" for each scenario that would help to detect the beginnings of the event
7. Consider the scope of the positive and negative consequences of each scenario and their relative impacts
8. Monitor the indicators developed on a periodic basis

Figure A5.19. Team A / Team B.

TEAM A / TEAM B

Used when there may be competing and possibly equally strong mind sets held on an analytical issue; this approach helps opposing groups see the merit in each other's perspective.

Two Phases

1)Analysis Phase

1. Identify the two or more competing hypotheses or points of view
2. Form teams or designate individuals to develop the best case for each hypothesis
3. Review all pertinent information that supports their respective position
4. Identify missing information that would strengthen their hypotheses
5. Structure each argument, presenting key assumptions, key pieces of evidence, and careful articulation of the logic behind the argument

2)Debate Phase

1. Set aside time for an oral presentation of the alternative team findings; this can be an informal brainstorming session or a more formal debate
2. Have an independent jury of peers to listen to the oral presentation and be prepared to question the teams regarding their assumptions, evidence, or logic
3. Allow each team to present its case, challenge the other team's arguments, and rebut the opponent's critique of its case
4. Let the jury consider the strength of each presentation and recommend possible next steps for further research and collection efforts

Attachment 6

IC, DOD, AND MILITARY SERVICE REFERENCES

A6.1. The IC. As shown in Table A6.1, *Members of the IC*, the IC is a coalition of 17 agencies and organizations, including the ODNI, within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities.

Table A6.1. Members of the IC.

Office of the Director of National Intelligence (ODNI)	
U.S. Air Force (USAF) Intelligence	Department of the Treasury
U.S. Army (USA) Intelligence	Drug Enforcement Agency (DEA)
Central Intelligence Agency (CIA)	Federal Bureau of Investigation (FBI)
U.S. Coast Guard (USCG) Intelligence	U.S. Marine Corps (USMC) Intelligence
Defense Intelligence Agency (DIA)	National Geospatial-Intelligence Agency (NGA)
Department of Energy (DOE)	National Reconnaissance Office (NRO)
Department of Homeland Security (DHS)	National Security Agency (NSA)
Department of State (DOS)	U.S. Navy (USN) Intelligence

A6.2. IC and DoD Reference Documents. Table A6.2, *Common IC and DoD Analysis References*, lists various IC and DoD publications that most often impact AF analysis.

Table A6.2. Common IC and DoD Analysis References.

IC
DNI *Principles of Intelligence Transparency for the Intelligence Community* ICD 191, *Duty to Warn* ICD 203, *Analytic Standards* ICD 204, *National Intelligence Priorities Framework* ICD 205, *Analytic Outreach* ICD 206, *Sourcing Requirements for Disseminated Analytic Products* ICD 208, *Maximizing the Utility of Analytic Products* ICD 209, *Tearline Production and Dissemination*
DoD
DoDI 3115.17, *Management and Oversight of DoD All-Source Analysis* DIA Directive (DIAD) 5000.200, *Intelligence Threat Support for Major Defense Acquisition*

Programs

DIA Instruction (DIAI) 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*

DIAP Users Guide

DoD Directive (DoDD) 5000.01, *The Defense Acquisition System*

DoDD 5105.21, *Defense Intelligence Agency*

DoDD 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*

DoDI 5000.02, *Operation of the Defense Acquisition System*

A6.3. Military Services. As depicted in Table A6.3, *Major Intelligence Analysis Entities of the Military Services*, each military service has a SIO that oversees intelligence policy, planning, programming, and activities on behalf of the service chief. The AF SIO is the DCS for ISR, also known as the AF/A2. Each service is authorized one service intelligence center, also called an intelligence analysis center. The AF's service intelligence center is NASIC. The AF has assigned the ACC as its lead MAJCOM for the GIISR capability, which includes intelligence analysis. Similarly, other military services have assigned significant analysis responsibilities to various organizations. All services routinely reach out to each other for service-unique expertise and collaboration in addressing analysis requirements.

Table A6.3. Major Intelligence Analysis Entities of the Military Services.

	USAF	USA	USN	USMC	USCG
Service Senior Intelligence Officer (SIO)	Deputy Chief of Staff for ISR (USAF/A2)	Deputy Chief of Staff for Intelligence (USA/G2)	Director of Naval Intelligence (USN/N2/6)	Director of Intelligence (USMC/DIRINT)	Assistant Commandant for Intelligence (USCG/CG-2)
Service Intelligence Center	National Air and Space Intelligence Center (NASIC)	National Ground Intelligence Center (NGIC)	Office of Naval Intelligence (ONI)	Marine Corps Intelligence Activity (MCIA)	Intelligence Coordination Center (ICC)
Lead Command	Air Combat Command (ACC) 1. Core Function Lead Integrator (CFLI) for Global Integrated ISR (GIISR) **2.** Chair, Analysis Capability Working Group (ACWG)	Intelligence and Security Command (INSCOM)	N/A	N/A	N/A
Other Major Analysis Organizations	1.Intelligence Systems Support Office (ISSO) 2.363 ISRW 1.Civil Aviation Intelligence Analysis Center (CAIAC)		• Nimitz Operational Intelligence Center • Farragut Technical Analysis Center • Kennedy Irregular Warfare Center Hopper		• Maritime Intelligence Fusion Center Atlantic (MICF LANT) • Maritime Intelligence Fusion Center Pacific (MICF PAC) Coast Guard Investigative Service (CGIS)

			Information Services Center		
Counter-Intelligence Organizations	AF Office of Special Investigations (AFOSI)	Army Counterintelligence Center (ACIC)	Naval Criminal Investigative Service (NCIS)	2nd Intelligence Battalion	Coast Guard Counterintelligence Service (CGCIS)

Notes:
1. The USA service intelligence center (NGIC) falls under INSCOM. The service intelligence center in each of the other military services falls under the service SIO.
2. The AF assigns a CFLI to each of its major capabilities. The ACC Commander is the GIISR CFLI, which includes intelligence analysis. The ACC staff coordinates closely with intelligence analysis stakeholders across the AFIAE to develop, program, and advocate for intelligence analysis capabilities and requirements.
3. The ACWG serves as a cross-MAJCOM entity of analysis stakeholders responsible for supporting the development and advancement of air, space, and cyberspace intelligence analytical capabilities within the AF ISR Enterprise and across the full range of military operations. The ACWG provides a means to coordinate, assess, and synchronize AF intelligence analysis policies, tradecraft, education, training, and tools, as well as to recommend materiel and non-materiel solutions through established AF processes and offices.

A6.4. Common Analysis Organizations. Table A6.4, *Intelligence Analysis Organizations by Mission Type*, identifies IC, DoD, military service, and other government agencies organized according to the primary analysis they conduct. The table is not meant to be exhaustive; rather it provides a sampling of missions and the key analysis organizations that support them.

Table A6.4. Intelligence Analysis Organizations by Mission Type.

Air / Integrated Air Defense Systems	**Short Range Missiles**	**Med / Long Range Missiles**	**Ground**
NASIC	MSIC	NASIC	NGIC
Maritime	**Space**	**Cyber**	**Counter-IED**
ONI MCIA	NASIC NRO 14 AF	CYBERCOM NSA NASIC 24 AF 25 AF AFOSI	JIDA
Counter-terrorism	**Counter-intelligence**	**Threat Finance**	**Criminal**
NCTC DHS FBI CIA CGIS	AFOSI CIA FBI ACIC NCIS 2d Intelligence Btn CGCIS	Treasury FBI	AFOSI FBI NCIS CID CGIS
Rotary Wing	**Unmanned Systems**	**Surface-to-Air Missiles**	**Electronic Warfare Systems**
NGIC	NASIC NGIC ONI	MSIC	NASIC NGIC ONI
Rapid Air Mobility	**Global Commons**		
AMC AIS	CAIAC		

	NAI2O TRANSCOM JIOC AMC AIS MIFC LANT MIFC PAC		

Notes:
1. As the DoD functional manager for analysis, DIA provides overarching all-source analysis and/or guidance for all mission types listed.
2. The Missile and Space Intelligence Center (MSIC) is an equivalent organization to the service intelligence centers. Additionally, MSIC provides support to space analysis.
3. CYBERCOM—Cyber Command; JIDA—Joint Improvised-Threat Defeat Agency; NCTC—National Counterterrorism Center; CGIS—Coast Guard Investigation Service; Btn—Battalion; CID—Criminal Investigation Command; NAI2O—National Aviation Intelligence Integration Office; TRANSCOM—Transportation Command

Attachment 7

ONLINE RESOURCES FOR ANALYSIS SKILLS AND TRADECRAFT.

Table A7.1, *Online Resources for Skills and Tradecraft,* identifies resources that contain additional background, information, and guidance on analysis skills and tradecraft topics discussed in Chapter 5. The list reflects some of the common resources as of 2017 and is not meant to be exhaustive nor all-inclusive.

Table A7.1. Online Resources for Skills and Tradecraft.

Analysis Certification
ASA Certification site, JWICS Caution-url: https://intelshare.intelink.ic.gov/sites/asacertification
Universal GEOINT Certification Program site, https://usgif.org/certification
Critical Thinking and Reasoning
AFCO-CFA Intellipedia Page, https://intellipedia.intelink.gov/wiki/Air_Force_Cryptologic_Office_(AFCO)/CFA_Advanced_Analysis_and_Training
Foundation for Critical Thinking, *The Critical Thinking Community,* http://www.criticalthinking.org
Grimes, Geoffrey, *Scholasticism, Rationalism, and Empiricism: Epistemology and Three Western Systems of Reasoning*, http://www.distancelearningassociates.org/eng2327/BC-ReasoningSystems.htm
SATs
AFCO-CFA Intellipedia Page, https://intellipedia.intelink.gov/wiki/Air_Force_Cryptologic_Office_(AFCO)/CFA_Advanced_Analysis_and_Training
CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*, March 2009, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf
DCS for ISR White Paper, *Data Science and the USAF ISR Enterprise,* February 2016, http://www.defenseinnovationmarketplace.mil/resources/Data_Science_and_the_USAF_ISR_Enterprise%20_White_Paper.PDF
ICAT-G/Research Portal, JWICS Caution-url: https://intellipedia.intelink.ic.gov/wiki/Portal:IC_Analytic_Tradecraft_Gateway
Lengler, Ralph, and Martin J. Eppler, *A Periodic Table of Visualization Methods*,

http://www.visual-literacy.org/periodic_table/periodic_table.html
Collaboration and Communication
AFCO-CFA Intellipedia Page, https://intellipedia.intelink.gov/wiki/Air_Force_Cryptologic_Office_(AFCO)/CFA_Advanced_Analysis_and_Training
DIA-01-1309-510, *DIA Style Manual for Intelligence Production 2017*, JWICS Caution-url: https://intelshare.intelink.ic.gov/sites/ddii/mid/AIS/default.aspx
ICAT-G/Research Portal, JWICS Caution-url: https://intellipedia.intelink.ic.gov/wiki/Portal:IC_Analytic_Tradecraft_Gateway
OPB and ABI
ODNI Systems & Resource Analyses, *ABI Way Ahead*, JWICS Caution-url: https://intelshare.intelink.ic.gov/sites/sramis/abi/default.aspx
Quellfire Documentation, JWICS Caution-url: https://intelshare.intelink.ic.gov/sites/quellfire/SitePages/ProgramDocumentation.aspx

Attachment 8

ANNOTATED BIBLIOGRAPHY

This attachment contains IC and academic resources for analyst Airmen to reference to improve their analysis aptitude. The list reflects some of the common references as of 2017 and is not meant to be exhaustive nor all-inclusive.

A8.1. Analysis Skills, Tradecraft, and Processes in the IC. The following texts focus specifically on IC analysis.

711th Human Performance Wing (HPW), ***The Framework for Analytic Cognition (FAC)***, AFRL, Wright-Patterson Air Force Base, Ohio, April 2014
This report serves as a guide to conducting intelligence analysis thoroughly while remaining sufficiently pliable to adapt to unstructured issues. It focuses on describing methods to foster analyst understanding of human-shaped capabilities and intentions for application in intelligence missions.

CIA, ***A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis,*** March 2009, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf
This guide highlights several structured analytic techniques to outline and assist analysts to think about and work difficult problems associated with intelligence analysis. The primer identifies several hurdles to this process such as biases, expectations, and mental models. Ultimately, the guide aims to inform intelligence analysts about their thinking processes to increase their self-awareness and efficacy in making judgments.

Clark, Robert M., ***Intelligence Analysis: A Target-Centric Approach***, 4th edition, CQ Press, 2012
This book urges analysts to focus on the intelligence problem at hand to drive insight. It provides a thorough overview of how the intelligence analysis process works with ample examples. The book also identifies areas where intelligence analysis could/should work better.

Clark, Robert M., ***The Technical Collection of Intelligence***, CQ Press, 2010
This book examines the technical means by which advanced countries collect intelligence information (acoustic, infrared, etc.). The author describes the collection, processing, and exploitation phases of intelligence technical collection in an understandable language.

Defense Intelligence Reference Document DIA-01-1003-001A, ***Tradecraft Primer: Basic Structured Analytic Techniques***, 4th edition, 3 March 2011
This DIA handbook provides an outline of analytic methods to help intelligence analysts improve their critical thinking skills, producing more thorough, less biased judgments. The techniques provided in this text also function to build a common lexicon in the IC, fostering consistent understanding and thereby efficiency and accuracy.

Folker, Robert D. Jr., ***Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods***, Occasional Paper #7, Joint Military Intelligence College, 2000
This summary of a master's thesis compares the results of those who used a specific structured analytic technique with those who did not in preparing intelligence estimates.

Fingar, Thomas, ***Reducing Uncertainty: Intelligence Analysis and National Security***, Stanford Security Studies, 2011

The goal of this book is to inform readers from outside the IC what analysts in the IC do and how they do it. The book explains the pressures IC analysts are under (political etc.), why they often focus on worst-case scenarios, and the value of National Intelligence Estimates.

Fischhoff, Baruch, and Cherie Chauvin, ***Intelligence Analysis: Behavioral and Social Scientific Foundations***, National Academies Press, 2011

This book focuses on the human aspect of the IC and how to improve judgments made by both individual analysts and groups of analysts. The book provides an overarching perspective on the issues and processes that contribute to tough decision and judgment making.

George, Roger Z., and James B. Bruce, ed., ***Analyzing Intelligence: Origins, Obstacles and Innovation***, Washington D.C.: Georgetown University Press, 2008

This book provides a post-9/11 assessment of the state of intelligence analysis. The text offers insights into the obstacles for intelligence analysis, providing a plan to improve analytical methods, training, and approach. The book highlights adapted tradecraft, predictive analysis, and collaboration as areas needing improvement.

Grabo, Cynthia, ***Anticipating Surprise: Analysis for Strategic Warning***, University Press of America, 2002

This book, originally designed as a CIA analyst training guide, outlines the steps in the anticipatory analysis process, including discussing guidance for assessing the meaning of pieces of intelligence. In the wake of post-9/11 IC critiques, the author provides suggestions on how to improve and clarify warnings to decision makers.

Hackman, Richard J., ***Collaborative Intelligence: Using Teams to Solve Hard Problems***, San Francisco: Berrett-Koehler Publishers Inc., 2011

The book highlights the increased need and prevalence for interdisciplinary collaboration in intelligence analysis and identifies that most teams in the field often break down or prove ineffective. The author outlines six conditions leaders can employ to encourage the development, efficacy, and maintenance of teams working on intelligence analysis tasks.

Hall, Wayne Michael, and Gary Citrenbaum, ***Intelligence Analysis: How to Think in Complex Environments***, Santa Barbara, California: Praeger Security International, 2010

This book discusses the various types of advanced analysis—including anticipatory, semiotics, and link analysis—while laying out the steps of analytical problem solving: decomposition, critical thinking, analysis, recomposition, and synthesis. The book also discusses the systems of thought and how those impact an individual's analytical process and decision/judgment.

Heuer, Richards J., Jr., ***The Psychology of Intelligence Analysis***, Washington, D.C.: Central Intelligence Agency, Center for the Study of Intelligence, 1999

This collection of CIA articles spanning 1978-1986 reviews timeless concepts of cognitive psychology concerning how individuals gather and process information to shape their judgments.

Heuer, Richards J., Jr. and Randolf H. Pherson, ***Structured Analytic Techniques For Intelligence Analysis***, Washington, D.C.: CQ Press, 2014

This text identifies best practices in structured analysis to inform analysts within the intelligence field and across other disciplines.

Kent, Sherman, ***Strategic Intelligence for American World Policy***, Princeton University Press, 2015

This book was originally written and published in 1966 by Sherman Kent, who pioneered many of the methods of intelligence analysis. The book analyzes the varied aspects of what is known as "high-level foreign positive intelligence." Kent asserts that very little of it involves cloaks and

daggers. All of it is important to national survival, and should be understood by the citizens of a democracy.

Kerbel, Josh, and Anthony Olcott, *Synthesizing with Clients, Not Analyzing for Customers*, Studies in Intelligence, Vol. 54, No. 4. December 2010, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-54-no.-4/synthesizing-with-clients-not-analyzing-for.html

This article discusses the challenges, purpose, and shortcomings of the separation between analysts and the policy/decision makers they inform. One purpose is to avoid politicization of analysis and mitigate confirmation biases, but the separation can also lead to unanswered questions from decision-makers or ignored reports created by the analysts but not read.

Lowenthal, Mark M., *Intelligence: From Secrets to Policy*, 6th edition, CQ Press, 2014

This text provides an introduction to the field of intelligence, from both the analyst and policymaker perspectives. This book covers all phases and domains of intelligence analysis, providing current event examples and trends to watch.

Moore, David T., *Critical Thinking and Intelligence Analysis*, 2nd edition, Books Express Publishing, 2010

This book, sponsored by the National Defense Intelligence College, establishes how critical thinking fits into intelligence analysis. The author offers input on how to teach critical thinking to analysts with the goal of integrating into the intelligence analysis process.

Moore, David T., *Sensemaking: A Structure for an Intelligence Revolution*, 2nd edition, CreateSpace Independent Publishing Platform, 2013

The goal of this book is to identify where and how to improve the IC and its processes. The text identifies problem areas, including discussions of 'wicked problems,' complexity theory, and macro-vs-micro cognition. It also proposes possible solutions.

Symon, Paul B., and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data," *Joint Forces Quarterly*, Vol 79, 4th Quarter 2015

This article discusses the emerging challenge of big data analytics for military intelligence communities. The article highlights that, although big data generates knowledge creation, additional tools and methods are needed to absorb, process, and analyze the vast onslaught of information.

White, Jeffrey, *Shakespeare for Analysts: Literature and Intelligence*, CreateSpace Independent Publishing Platform, 2013

This paper, originally sponsored by the Joint Military Intelligence College in 2003, advocates inclusion of Shakespeare in intelligence analysts' bookshelves. The author asserts that since analysts are concerned with human personalities within political and military leadership, analysts should use Shakespeare's work as insight into how people are motivated and pursue power.

Zegart, Amy B., *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford University Press, 2000

Using an institutionalist approach, the author asserts that the CIA, Joint Chiefs of Staff (JCS), and National Security Council (NSC) are hindered from operating effectively by design. Frequent elections, the prominence of elected officials controlling these organizations, and Congressional checks foster competitive, rival organizations fighting amongst themselves to protect their own intelligence assets.

A8.2. Analysis Skills, Tradecraft, and Processes in General . Whereas section A8.1 identifies sources that specifically address IC skills, tradecraft, and processes, the following

sources apply to the discipline of analysis writ large. While the following were written with a broader academia focus, they are also relevant to IC analysis.

Bothamley, Jennifer, *Dictionary of Theories*, Barnes & Noble, 2004
This book is a composite reference that alphabetically arranges theories, laws, hypotheses, etc. from across many disciplines. It serves as a thorough annotated bibliography of well-known theories, and includes short descriptions and comments on the validity of each entry.

Cukier, Kenneth Neil, and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think," *Foreign Affairs*, May - June 2013, https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data
This article discusses the concept of big data, describing the vast and increasing amount of information that can be harnessed, processed and used to support trends and inform new knowledge. The article also cautions that big data should be used to inform but not explain everything.

Dewey, John, *How We Think*, Boston, Massachusetts: D.C. Heath and Co. Publishers, 1910
This book offers an early overview of the importance of self-awareness in thought. The author calls for a focus in "mental training" and "training of thought" to increase one's deliberateness when thinking, solving, and assessing problems.

Elder, Linda, and Richard Paul, *The Thinker's Guide to Analytic Thinking*, 2nd edition, Dillon Beach: Foundation for Critical Thinking Press, 2007
This guide describes the structures and importance of analytic thinking. The authors discuss how we reach our conclusions and judgements–viewing an idea through our biases, point of view, experiences, and assumptions. The book provides a framework for understanding how we think and how that impacts decisions.

Facione, Peter, *Critical Thinking: What It Is and Why It Counts*, Milbrae, California: Measured Reasons and the California Academic Press, 2013
This essay familiarizes readers with the key skills and habits associated with critical thinking and why practicing critical thinking is useful in their personal and social decision-making. The article identifies several of the heuristic strategies individuals are naturally inclined towards and the pros/cons and biases associated therein.

Facione, Peter, and Carol Ann Glittens, *Think Critically*, 3rd edition, Prentice Hall, Pearson Education Inc., 2015
This text introduces and practically describes critical thinking as important for making big decisions in the real-world.

Foundation for Critical Thinking, *The Critical Thinking Community*, http://www.criticalthinking.org
This website is sponsored by the Foundation for Critical Thinking, a non-profit organization that seeks to promote essential change in education and society through the cultivation of fair-minded critical thinking—thinking which embodies intellectual empathy, humility, perseverance integrity, and responsibility.

Gilovich, Thomas, *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life*, The Free Press, 1991
This book addresses the question: When can we trust what we believe, and when are these beliefs suspect? Thomas Gilovich offers a wise and readable guide to the fallacy of the obvious in everyday life. Illustrating his points with vivid examples, he documents the cognitive and social processes that distort our thoughts, beliefs, judgements, and decisions, inevitably altering our impression of reality.

Grimes, Geoffrey, ***Scholasticism, Rationalism, and Empiricism: Epistemology and Three Western Systems of Reasoning***, http://www.distancelearningassociates.org/eng2327/BC-ReasoningSystems.htm
This website discusses the basic concepts of what the author describes as three core systems of reasoning: scholasticism, rationalism, and empiricism. The author asserts all those raised in Western cultures can be binned into one of these three categories.
Jones, Morgan D., ***The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving***, Crown Business, 1998
This handbook provides fourteen tools to help individuals break down problems, enabling more efficient and informed decisions.
Kahneman, Daniel, ***Thinking, Fast and Slow***, New York: Farrar, Straus and Giroux, 2011
In this book author Daniel Kahneman describes the two systems of thinking: the intuitive (fast System 1) and the logical (thorough System 2). The text describes the identifiers of each system and how it impacts our decisions. The author provides methods to identify and prevent mental shortcuts that can cause judgement errors.
Kahneman, Daniel, Andrew Rosenfield, Linnea Gandhi, and Tom Blaser, ***Noise: How to Overcome the High, Hidden Cost of Inconsistent Decision Making***, Harvard Business Review, 2016
This article explains the difference between the concepts of "noise" and bias and provides a prescription of how leaders can test the level of "noise" in their organizations. Further, it describes steps to mitigate noise and promote analytical consistency.
Kahneman, Daniel, Paul Slovic, and Amos Tversky, ***Judgement under uncertainty: Heuristics and biases***, Cambridge University Press, 1982
This book describes the various judgment heuristics and biases. The text discusses how those biases can impact decision-making and judgments and suggests methods for identifying and overcoming these biases.
Kaplan, Abraham, ***The Conduct of Inquiry: Methodology for Behavioral Science***, Transaction Publishers, 1998
In this book the author discusses the various behavioral science disciplines and the methodologies and shortcomings of each. It provides a constructive assessment of the various standards and strategies of social research methods to guide behavioral scientists' research.
Kosko, Bart, ***Fuzzy Thinking: The New Science of Fuzzy Logic***, Hyperion, 1993
This book discusses the concept of fuzzy thinking/fuzzy logic, the principle that nothing is absolute. The author challenges the typical Western thinking that there is black and white—right and wrong, asserting that there are lots of shades of gray, with many perspectives.
Krizan, Lisa, ***Intelligence Essentials for Everyone***, Joint Military Intelligence College, June 1999
This paper provides guidance for the implementation of sound intelligence within and outside government infrastructure. The author describes the methods to employ to reach empirically-supported decisions with fewer flaws.
Laney, Douglas, et al., ***How Data Scientist Skills and Qualifications Differ from those of BI Analysts and Statisticians***, 21 October 2015
This article helps readers understand the distinction between the new data scientist career and associated skill-set and the legacy career of statisticians. Additionally, the authors describe why a statistician is not adequate for data science problems.

Lengler, Ralph, and Martin J. Eppler, ***A Periodic Table of Visualization Methods***,
http://www.visual-literacy.org/periodic_table/periodic_table.html
This online learning tool informs users on the ability to generate, understand, and apply visualizations. The site employs a didactic approach using problem-based learning techniques to foster understanding of visualization methods.
Linden, Alexander, et al., ***Organizational Principles for Placing Advanced Analytics and Data Science Teams***, 4 September 2013
With the onslaught of big data driving the need for teams of advanced analysts and data scientists in organizations of various disciplines, this article discusses where to best place these teams organizationally and the pros and cons of various locations.
Livio, Mario, ***The Equation that Couldn't be Solved: How Mathematical Genius Discovered the Language of Symmetry***, Simon & Schuster, 2006
This book attempts to explain mathematical symmetry through a "quantic" equation to non-mathematically inclined readers. The text discusses how the idea of group theory arose.
Mackay, Charles, ***Extraordinary Popular Delusions and the Madness of Crowds***, CreateSpace Independent Publishing Platform, 2013
This book studies the psychology of crowds and mass mania with historical examples such as the witch hunts. The text offers explanation as to why reasonable, intelligent individuals take on opinions in a crowd environment that they otherwise would not.
Margolis, Howard, ***Patterns, Thinking, and Cognition: A Theory of Judgement***, Chicago, Illinois: University of Chicago Press, 1987
This book discusses how pattern recognition impacts thinking and judgment. The author discusses identification of patterns, sub-patterns and when anomalies are actually part of the pattern.
Mlodinow, Leonard, ***The Drunkard's Walk: How Randomness Rules Our Lives***, Vintage, 2009
This book discusses how much of our lives are lived and guided by randomness. He introduces the concept of chaos theory, and reveals psychological illusions guiding "chance." The text presents several tools to help readers make more informed decisions in their everyday lives.
Pirsig, Robert M., ***Zen and the Art of Motorcycle Maintenance***, Bantam, 1975
In this book the author combines philosophy with the practical, real-world processes of motorcycle mechanics. Despite the title, this book prompts the reader to deep-think about critical thinking methods and more complex philosophical dilemmas, such as good-vs-evil.
Surowiecki, James, ***The Wisdom of Crowds***, Anchor Books, 2008
This book asserts that crowd-sourcing perspectives, or incorporating a range of diverse perspectives, improves problem-solving. The author identifies four necessary conditions that, when met, produce crowds that are smarter together than any one individual.
Tetlock, Philip E., and Dan Gardner, ***Superforecasting: The Art and Science of Prediction***, 1st edition, 2015
In this work, Philip Tetlock and coauthor Dan Gardner offer a masterwork on prediction, drawing on decades of research and the results of a massive, government-funded forecasting tournament. Superforecasting offers the first demonstrably effective way to improve our ability to predict the future.
Tufte, Edward R., ***The Visual Display of Quantitative Information***, 2nd edition, Cheshire, Connecticut: Graphics Press, 2001

This text covers the theory and practice used in the design and use of statistical graphics, charts and tables. It outlines the benefits and potential misrepresentation of empirical visualization methods.

A8.3. Studies and White Papers on Analysis. ***Air Force Intelligence Analysis Roles and Responsibilities Review for 2016***, September 2016

This report is a primary deliverable for the AF Analysis Plan of Action and Milestones. The report details the results of an AF-wide review of roles and responsibilities for analysis and production.

Alkire, Brien, Abbie Tingstad, Dale Benedetti, Amado Cordova, Irina Danescu, Lt Col William Fry, Brig Gen (ret.) D. Scott George, Lawrence M. Hanser, Lance Menthe, Erik Nemeth, David Ochmanek, Julia Pollak, Jessie L. Riposo, Lt Timothy Smith, Alexander Stephenson, ***Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis***, Santa Monica, California: RAND Corporation, RR-1330-AF, 2016, http://www.rand.org/pubs/research_reports/RR1330.html

This RAND report looks to the past for lessons to help inform recommendations in addressing future challenges for the AFIAE. The report identifies challenges regarding future operational pace, contextual and deep knowledge, the integration and understanding of space and cyber missions, and the growing volume of data to be analyzed.

Chang, Welton, Eva Chen, Barbara Mellers, and Philip Tetlock, "Developing Expert Political Judgment: The Impact of Training and Practice on Judgmental Accuracy in Geopolitical Forecasting Tournaments," ***Judgment and Decision Making*** 11, no. 5 (2016): 509-26

This essay tests the power of a cognitive-debiasing training module to improve probability judgments in a four-year series of geopolitical forecasting tournaments sponsored by the U.S. Intelligence Community.

Committee on Improving the Effectiveness and Efficiency of U.S. Air Force Pre-Acquisition Development Planning et al., ***Development Planning: A Strategic Approach to Future Air Force Capabilities***, National Academies Press, 2015

This book provides recommendations, informed by development planning efforts of the past, for leaders to think strategically into upcoming decades concerning where the AF may have capability gaps.

Committee on U.S. Air Force Strategic Deterrence Military Capabilities in the 21st Security Environment et al., ***U.S. Air Force Strategic Deterrence Analytic Capabilities: An Assessment of Tools, Methods, and Approaches for the 21st Century Security Environment***, National Academies Press, 2015

This book describes the analytic skills required in successful nuclear deterrence. The text also discusses how nuclear deterrence works through assurance and posture, how it can fail, and how to mitigate the risk of deterrence failure.

DCS for ISR White Paper, ***Data Science and the USAF ISR Enterprise***, February 2016, http://www.defenseinnovationmarketplace.mil/resources/Data_Science_and_the_USAF_ISR_Enterprise%20_White_Paper.PDF

This paper explores the impact of big data, the transformation of IC information technology, and how each will drive the necessity for an AF ISR strategic approach to data science.

DCS for ISR White Paper, ***Five Examples of Big Data Analytics and the Future of ISR***, November 2014

This paper describes the concept of big data and how it relates to ISR now and in the future through five examples. The paper asserts that big data is the new norm and intelligence professionals must adapt the way they employ data analytics to harness the depth of information now available.

DCS for ISR White Paper, *Revolutionizing AF Intelligence Analysis*, January 2014, http://www.defenseinnovationmarketplace.mil/resources/20140211_IntelligenceAnalysisWhitePaper_PA.pdf

This paper seeks to explain the increasing priority of analysis by identifying motivations, presenting a common lexicon, exploring key issues, and outlining the way ahead. The paper asserts that intelligence analysis is changing and increasing in prominence and therefore our analysis processes and emphasis must also adapt.

ISR Capability Planning and Analysis Process Committee on Examination of the Air Force Intelligence, *Capability Planning and Analysis to Optimize Air Force Intelligence, Surveillance, and Reconnaissance Investments*, National Academies Press, 2012

This report answers a request from the AF to assess the current AF approach to ISR corporate planning and programming. The report identifies best practices and recommends specific improvements to build-out existing tools and processes to ensure AF ISR processes can enable successful satisfaction of customer needs in accomplishing their missions.

Lin-Greenberg, Capt Erik, Krysten Young, and Col Brian Ray, *Improving Intelligence Analysis for the A2/AD Environment*, March 2015

This paper discusses the impact an Anti-Access/Area Denial (A2/AD) environment would have on the AF's ability to collect, analyze, and act on intelligence.

McClung, Lt Col Michael E., *2 Propositions Regarding Intelligence for Airpower*, Air University, 14 February 2013

This research paper provides two propositions concerning AF intelligence: 1) "the nature of intelligence for airpower is driven by the rapid evolution and expanding breadth of airpower itself" and; 2) "Analysis is the essence of intelligence for airpower, and like airpower it is broad, but targeting and threat analysis are central."

Report of USAF ISR Analysis and Production–CY 2014, 19 June 2014

This report is the result of a survey of AF ISR leaders to document AF production, including identifying production goals, focus, and areas for improvement. This survey built upon findings from a 2013 survey and further developed a baseline for comparison of the 2016 survey results.

Survey Report of USAF All-Source Intelligence Analysis, 1 August 2013

This report is the outcome of a survey to gage results and assessments of AF all-source analysis. The report asserts that if the USAF is serious about 'revolutionizing analysis,' it must concur with improved emphasis and investment.

Treverton, Gregory F., and C. Bryan Gabbard, *Assessing the Tradecraft of Intelligence Analysis*, Santa Monica, California: RAND Corporation, 2008, http://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR293.pdf

This RAND report is the result of a survey of the IC and other research to discover what constitutes intelligence analysis and how is it performed. The researchers found that "analysis" covers a range of activities that varies from organization to organization. The report concludes that to foster collaboration and shared understanding, common tools, agendas, and education curriculums should be established and shared across the community.

Treverton, Gregory F., and Jeremy J. Ghez, ***Making Strategic Analysis Matter***, Santa Monica, California: RAND Corporation, 2012, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2012/RAND_CF287.pdf
This RAND report is the result of a workshop that found that though there is not much demand for strategic analysis from policy and decision makers, there is substantial value in conducting this level of analysis.

A8.4. Analysis Scenarios and Historical Applications. Bruce, James B., and Jeffrey Martini, ***Whither Al-Anbar Province? Five Scenarios Through 2011***, Santa Monica, California: RAND Corporation, 2010, **http://www.rand.org/pubs/occasional_papers/OP278.html**

This report produced for the Marines by RAND analyzes the question, 'what does the future hold for Iraq's al-Anbar province?' The researchers play through five scenarios. The report concludes that the U.S. (and specifically the Marines) can influence some of the drivers shaping the scenario outcomes and suggests constant course of action evaluations to identify possible and probable future trajectories.

Ehlers, Robert S., Jr., ***Targeting the Third Reich: Air Intelligence and the Allied Bombing Campaigns***, University Press of Kansas, 2009
This book highlights the cooperative intelligence elements (Royal Air Force) and bombing elements (U.S. Army Air Force) of the allied forces in Europe during World War II. The text discusses the often overlooked value added by the combined intelligence-bomber efforts in crippling the German war-making capabilities.

Fukuyama, Francis, ***Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics***, Baltimore, Maryland: Brookings Institution Press, 2007
This book discusses the value, necessity, and difficulties for foreign policy analysts to anticipate wild card events (such as, the 9/11 attacks, the rapid emergence and spread of diseases like H5NI, and the collapse of communism) in world politics. The author points out that biases and political pressures often influence the prediction and likelihood assessments of these types of events. Additionally, the credibility of some assessments for the probability of these "wild cards" is questionable, with a "boy that cried wolf" tainted view.

Neustadt, Richard E., and Ernest R. May, ***Thinking in Time: The Uses of History for Decision-Makers***, 1st edition, New York: Free Press, 1986
This book provides methods decision-makers and analysts can apply from historical lessons to current decisions.

Taleb, Nassim Nicholas, ***The Black Swan: The Impact of the Highly Improbable***, 2nd edition, Random House Trade Paperbacks, 2010
This book defines and discusses "black swan" events. The author highlights the importance of considering black swans when conducting analysis and making judgments. Although rare, black swan events have occurred and may occur, with far reaching and dramatic consequences.

Vertzberger, Yaacov, ***Risk Taking and Decision Making: Foreign Military Intervention Decisions***, Stanford University Press, 1998
This book discusses the realities of risk and provides analysis of what elements impact risk judgments and preferences in individuals' decision-making. The author uses five case studies to illustrate the calculations and consequences of risks in military interventions.

Walton, Timothy, ***Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present***, Cambridge University Press, 2010

This work provides short, critical analyses of past scenarios that successfully or unsuccessfully employed intelligence analysis.

A8.5. Analysis Education and Training. Center for the Study of Intelligence, *The Future of Higher Education: Implications for Intelligence*, March 2015

This paper argues that because education models in formal education institutions have and continue to change, methods for training in the workplace must also change and adapt for new generations' learning styles.

Chang, Welton, and Philip E. Tetlock, *Rethinking the Training of Intelligence Analysts*, Taylor & Francis, 29 February 2016, http://www.tandfonline.com/doi/pdf/10.1080/02684527.2016.1147164#.V6SgAqpf3xg

This article discusses the continuing challenge of erroneous and/or incomplete intelligence assessments in the IC. The authors advocate for new training approaches for intelligence analysts that adopt a scientifically validated process, which regularly reevaluated against benchmarks.

A8.6. Deception Analysis. Barton Whaley, *Textbook of Political-Military Counterdeception: Basic Principles & Methods*, National Defense Intelligence College, 2007

This is a textbook on counterdeception. It is designed to help users think like a detective in employing analytical skills.

Godson, Roy, and James J. Wirtz, *Strategic Denial and Deception: The Twenty-First Century Challenge*, Transaction Publishers, 2008

This book considers whether globalization, proliferating communication technologies, and the dissemination of vast amounts of information make effective foreign denial and deception more or less likely.

Gooch, John, and Amos Perlmutter, *Military Deception and Strategic Surprise*, Digital Printing, 2007

The six essays in this book deal primarily with the theory of deception and strategic-level deception. They present a picture of the dynamics and potential benefits of deception. Examples of operational-level deception are mentioned in some of the essays to illustrate certain points.

Latimer, Jon, *Deception in War: The Art of the Bluff, the Value of Deceit, and the Most Thrilling Episodes of Cunning in Military History, from the Trojan Horse to the Gulf War*, The Overlook Press, 2001

This work shows how simple some tricks have been, but also how technology has increased the range and subtlety of what is possible—bogus radio traffic, virtual images, even false smells. He draws examples from land, sea, and air to show how great commanders have always had, as Winston Churchill put it, that indispensable "element of legerdemain, an original and sinister touch, which leaves the enemy puzzled as well as beaten."

A8.7. Analysis Policy and Guidance . This list is not intended to be comprehensive but rather to highlight several key resources.

AFI 14-133, *Intelligence Analysis*, 29 March 2016

As the keystone instruction for AF intelligence analysis, this publication codifies how the Air Force conducts and presents analysis capabilities in support of Global Integrated ISR and other service core functions. It establishes the standards for AF intelligence analysis and delineates the associated roles and responsibilities of AF ISR Enterprise organizations.

AFI 14-134, *Intelligence Analysis Production and Requirements Management*, 21 June 2016

This publication provides guidance and procedures on AF intelligence analysis production and requirements management in support of internal AF requirements, as an integral complement to the IC for DIAP-focused production, and in support of the annual AFISRPoA.

Air Force ISR 2023: Delivering Decision Advantage,
http://www.defenseinnovationmarketplace.mil/resources/AF-ISR_2023.pdf
This strategic document approved by AF/A2, discusses emerging and future challenges for the AF ISR Enterprise, and focuses on how the enterprise should posture to addresses these challenges while meeting enduring core missions.

Annex 2-0, ***Global Integrated Intelligence, Surveillance, and Reconnaissance***, 29 January 2015
The annex serves as an AF supplement to JP 2-0 and covers AF specific topics and perspectives on GIISR.

Commander ACC, ***GIISR Core Function Concept***, 23 Jan 2013
This document identifies five enduring core GIISR capabilities that directly support the JCA of Battlespace Awareness. Analysis is an essential and integral component of each of the five enduring capabilities.

DoDI 3115.17, ***Management and Oversight of DoD All-Source Analysis***, November 16, 2016
This instruction establishes DoD policy and assigns responsibilities for the management and oversight of DoD ASA. It also establishes the DIAAE BOG, an intergovernmental committee as the primary forum for DoD-wide analytic synchronization and integration.

ICD 203, ***Analytic Standards***, 2 January 2015
This directive establishes common analytic standards to be used across the IC to ensure clear communication among organizations.

ICD 204, ***National Intelligence Priorities Framework***, 2 January 2015
This directive establishes the NIPF as the mechanism to create, prioritize and share intelligence priorities.

ICD 206, ***Sourcing Requirements for Disseminated Analytic Products***, 22 January 2015
This directive establishes the sourcing information that must be included in covered analytic products so as to increase the credibility and transparency of intelligence analysis.

ICD 501, ***Discovery and Dissemination or Retrieval of Information within the Intelligence Community***, 21 January 2009
In pursuit of a culture of responsible sharing and collaboration across the IC, this directive establishes guidance and policies for the discovery, dissemination or retrieval of intelligence and intelligence-related information collected or analysis produced by the IC.

JP 2-0, ***Joint Intelligence***, 22 October 2013
This publication addresses the nature of intelligence and establishes the principles of joint intelligence. It is one of the base guiding documents for DoD IC organizations.

FM 34-3

INTELLIGENCE ANALYSIS

MARCH 1990

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: **Approved for public release: distribution is unlimited**

FIELD MANUAL
NO 34-3

*FM 34-3
HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 15 March 1990

INTELLIGENCE ANALYSIS

Table of Contents

	Page
Preface	iv
CHAPTER 1 - The Intelligence Mission	1-1
The AirLand Battle	1-1
The Battlefield Area	1-4
The Intelligence Analysis System	1-6
CHAPTER 2 - The Intelligence Cycle	2-1
Directing	2-1
Collecting	2-2
Processing	2-3
Dissemination	2-18
CHAPTER 3 - Order of Battle	3-1
Order of Battle Factors	3-1
Order of Battle References	3-6
Order of Battle Records	3-11
Enemy Combat Effectiveness	3-28
Arbitrary Unit Designators	3-28
CHAPTER 4 - Intelligence Preparation of the Battlefield	4-1
Purpose of Intelligence Preparation of the Battlefield	4-3
Development and Use of Intelligence Preparation of the Battlefield Products	4-5
Weather Analysis	4-21
Threat Evaluation	4-24
Threat Integration	4-26
Intelligence Preparation of the Battlefield During Peacetime	4-34

Distribution restriction: Approved for public release; distribution is unlimited.

*This publication supersedes FM 34-3, 13 January 1986.

	Page
CHAPTER 5 - Analysis in Depth	5-1
Meeting User Requirements	5-1
Determining the Risk Factor	5-3
The Threat Model	5-5
Biases	5-11
CHAPTER 6 - Situation Development	6-1
Enemy Capabilities	6-1
Enemy Courses of Action	6-3
Working Situation Map	6-4
Factors of Analysis	6-7
Techniques of Analysis	6-9
CHAPTER 7 - Target Development	7-1
Decide	7-4
Detect	7-8
Deliver	7-12
CHAPTER 8 - Intelligence Support of Electronic Warfare Operations	8-1
Intelligence Collection to Support Electronic Warfare	8-1
The Effects of Terrain and Weather on Electronic Warfare	8-2
Intelligence Required for Electronic Warfare Support Measures	8-2
Intelligence Required for Electronic Countermeasures	8-2
Intelligence Required for Electronic Counter-Countermeasures	8-3
CHAPTER 9 - Counterintelligence Analysis	9-1
Counter Human Intelligence Collection	9-2
Counter Signals Intelligence Collection	9-3
Counter Imagery Intelligence Collection	9-3
Other Intelligence Support to CI Analysis	9-3
Multidiscipline Counterintelligence	9-13
Intelligence Support to Combatting Terrorism	9-13
CHAPTER 10 Intelligence Support to Counterinsurgency	1o-1
Support of Counterinsurgency Operations	10-2
Intelligence Estimate	10-2
Processing Information	10-3
Dissemination	10-12
Order of Battle	10-12

Page

APPENDIX A - Report Formats A-1

APPENDIX B - Automation Support to Intelligence Analysis B-1

APPENDIX C - Indicators of Enemy Courses of Action C-1

APPENDIX D - Enemy Strength Computations D-1

APPENDIX E - Terrain Analysis in Intelligence Preparation of the Battlefield E-1

GLOSSARY Glossary -1

REFERENCES References -1

INDEX Index -1

PREFACE

This publication describes the processes. procedures. and techniques used to produce all-source intelligence. It focuses on intelligence production at echelons at corps and below and amplifies the doctrine contained in FM 34-1. It provides guidance for intelligence staff officers, warrant officers. NCOs, and intelligence analysts at all skill levels. it is designed for use by the active Army and reserve components (RC).

This publ ication implements international standardization agreement (STANAG) 2077 and quadripartite agreement 511. it is in compliance with STANAGS 1059, 2033, 2044, 2149, 6004, and 6010: quadripartite agreements 170, 295, 354, 492, 523, 528, and 593; and air agreement 101/3D. The proponent of this publication is Headquarters, United States Army Training and Doctrine Command (HQ TRADOC), Submit changes for improving this publication on DA Form 2028 (Recommended Changes to Publications and Blank Forms) and forward it to the Commander, US Army Intelligence Center and School (USAICS), ATTN: ATSI-TD-PAL, Fort Huachuca, Arizona 85613-7000.

CHAPTER 1

THE INTELLIGENCE MISSION

Intelligence is a key element of combined arms operations. It enables commanders to use their combat power effectively to win the decisive battles and it helps them identify and attack high payoff targets (HPTs). Intelligence is an important part of every combat decision.

The dramatic improvements in intelligence collection systems have greatly enhanced the availability of battlefield information from many different sources. Battlefield information, however, is of limited value until it has been analyzed, Through analysis, this information becomes intelligence. The intelligence analyst integrates the seemingly insignificant bits of information from multiple sources to produce an overall picture of the battlefield. This picture reduces the uncertainties about the battlefield and the situation. Analysis generates the intelligence the commander needs to successfully fight on the modern battlefield.

This chapter describes the commander's intelligence requirements. It describes how these requirements are generated and the factors that affect them. It addresses those elements within the intelligence and electronic warfare (IEW) system that plan, coordinate, and execute intelligence analysis operations.

THE AIRLAND BATTLE

Intelligence is a vital part of the AirLand Battle. AirLand Battle is the current US Army doctrine for fighting in a mid- to high-intensity conflict. It is an extended, integrated battle involving the use of all available air and land forces. It is extended because the battle is fought from the forward edge of the area of operation (AO) to the rear boundary as a single, continuous battle (deep, close, and rear operations) . It is integrated in that nuclear and chemical weapons, when released by the national command authority, are merged with electronic and conventional weapons in all operations.

AirLand Battle Doctrine is offensively oriented. Its success depends on the ability of friendly forces to take the initiative from the enemy and to carry the fight into the enemy's rear. The simultaneous attack of forward enemy forces and the deep attack of follow-on echelons is inherent in the battle. Its objectives include the diversion, delay, destruction, or attrition of enemy fol low-on echelon forces before they can take part in the close operation. Figure 1-1 shows a sample deep attack.

The commander orchestrates a combination of offensive and defensive operations to defeat the enemy and gain the initiative. The commander uses defensive and offensive operations to destroy enemy first-echelon forces and deep-attack to simultaneously delay, disrupt, and manipulate enemy follow-on forces. The commander anticipates, creates, and exploits windows of opportunity, using flexible battle planning, to gain the initiative through offensive operations. By effectively employing maneuver and fire support assets, manipulating the enemy, and expertly

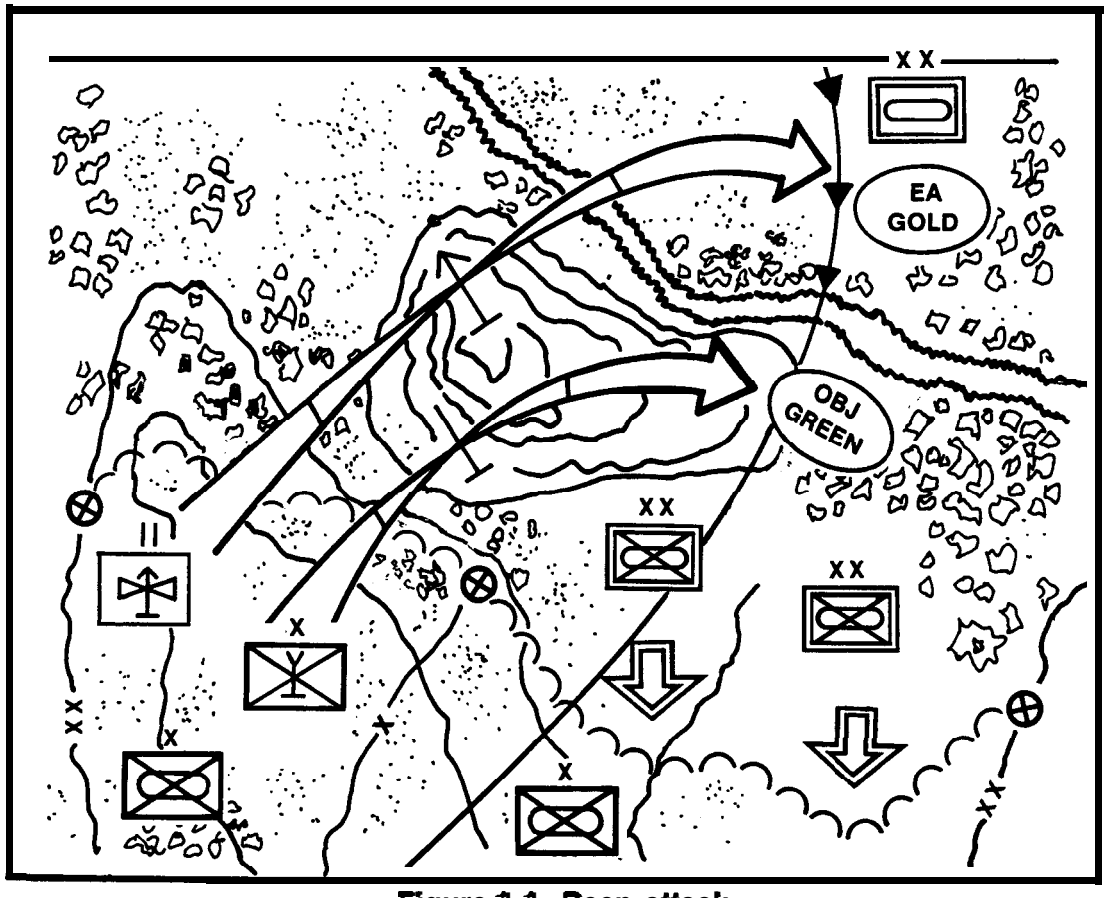


Figure 1-1. Deep attack.

using the weather and the terrain, the friendly commander can successfully defeat a superior enemy force.

To gain the initiative, the commander must--

- See the enemy early and determine the capabilities and intentions of the enemy.
- Find and track enemy follow-on echelons.
- Identify enemy high-value targets (HVTs), targets which if successfully attacked, will contribute to the degradation of important enemy battlefield functions,
- Identify, locate, and develop the required targeting data for the attack of HPTs, which if successfully attacked, will contribute to the success of friendly plans.
- Detect enemy weaknesses and develop the necessary data to support the exploitation of these weaknesses.

- Effectively use electronic warfare (EW) to support the AirLand Battle while protecting friendly use of the electromagnetic spectrum.

- Determine the enemy's capability and guard against that capability.

- Protect friendly forces and operations from enemy intelligence collection operations.

- Use the weather and terrain to friendly advantage.

IEW support is vital to the successful planning and execution of the AirLand Battle at all echelons. Intelligence support at brigade and battalion levels focuses primarily on the close operation, while at division it focuses on both close and deep operations. Corps is the focal point for intelligence operations that support rear and deep operations.

Intelligence support of close operations supports the commander's risk analysis and consideration of mission, enemy, terrain, troops available, and time (METT-T). As such it must be the first step in planning. Intelligence operations reduce risk by identifying the enemy's most likely courses of action, and so al low the commander to concentrate or disDerse forces as appropriate. Intelligence also provides administrative and logistic personnel, engineers, air detense artillery (ADA) staffs, and other planners with guidelines about the expected situations and enemy so they may make the best use of scarce assets.

To conduct deep operations the intelligence system supports the . . commander's need to look deep, find and follow enemy follow-on forces, and detarmine their capabilities, vulnerabilities, and intentions. The commander must designate the HPTs and decide where and when to attack them to achieve the greatest benefit to the operation. The commander conducts deep attacks against designated HPTs to '"shape'" the battlefield by forcing the enemy commander to deviate from established plans and to create favorable conditions for friendly commanders conducting close operations. To facilitate deep operations, corps-level intelligence planning must focus its attention on analyzing and estimating enemy capabilities, intentions, and likely courses of action at least 72 hours in advance. At division-level, intelligence planners must perform this same function at least 24 hours in advance.

Intelligence support of rear operations supports the commander's need to identify enemy capabilities, intentions, and likely courses of action to interdict friendly combat support (CS) and combat service support (CSS) functions, and to inhibit the ability of the friendly commander to flexibly employ the reserves. The intelligence planner must consider all means and measures available to tha enemy, to include sabotage, unconventional warfare, airmobile or airborne assaults, nuclear, chemical, and conventional long-range strikes, deception, and the employment of maneuver forces in deep exploitation or raiding operations.

THE BATTLEFIELD AREA

Commanders consider the battlefield in terms of the time and space necessary to defeat an enemy force or complete an operation before the enemy can reinforce. They view the battlefield as having two distinct areas: the AO and the area of interest (AI).

The AO is that portion of an area of conflict necessary for military operations. The AO is assigned by the next higher commander and designated by lateral and rear boundaries. It carries with it the authority and responsibility to conduct operations therein. The commander must coordinate with adjacent commanders before conducting maneuver and fire support (FS) activities outside the designated AO.

The AI is that area of concern to the commander which includes the AO and areas adjacent thereto. It includes areas forward of, and to the flanks and rear of the AO. It encompasses areas either occupied by enemv forces that could jeopardize friendly mission accomplishment and/or which includes the objectives of friendly current or planned operations.

Each commander determines his own AI. The commander generally relies on higher headquarters and adjacent units to provide information and intelligence about enemy forces in that area. Figure 1-2 shows the battlefield areas of division.

Battlefield areas are important to the intelligence analyst because they help focus the information requirements of commanders concerning the weather, terrain, and enemy forces from battalion to echelons above corps (EAC). Specific information requirements are dependent on the mission and the tactical situation. Usually, in conventional operations, information requirements (IR) on enemv forces are based on the one-up and two-down formula. Commanders require detailed information about enemy forces at their equivalent levels of command as well as at one level above and two levels below their own. For example, brigade commanders need information about enemy regiments (equivalent level), enemy divisions (one-up), and enemy battalions and companies (two-down). Generally, the enemy forces of concern to each commander are found within the command's AO and AI.

The IEW mission includes four major tasks: situation development, target development, EW, and counterintelligence (CI).

Situation development (discussed in Chapter 6) provides commanders with the intelligence they need to make sound tactical decisions. It is a continuing estimate of the situation that projects enemy intentions and the effects of the weather and terrain. Situation development helps cormnanders--

- Find and follow enemv forces.
- Determine enemy capabilities, vulnerabilities, and intentions.
- Identify the enemy main effort.

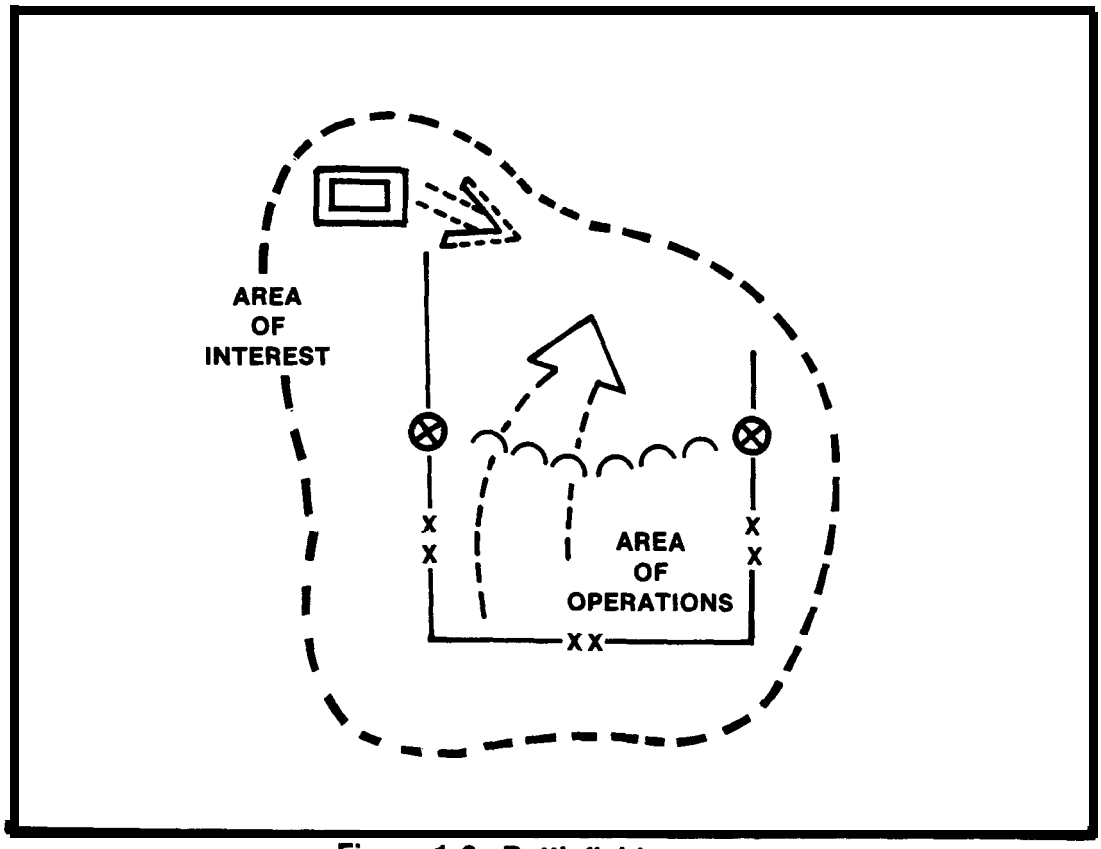


Figure 1-2. Battlefield areas.

- Determine how the weather and terrain will affect friendly and enemy operations.
- Detect opportunities to exploit enemy weaknesses and seize or retain the initiative.
- Assess the relative value of enemy combat systems, which serves as a basis for selecting HVTs.

Target development (discussed in Chapter 7) provides combat information, targeting data, and correlated target information which support the commander's tactical plans. It focuses on HPTs which have been selected, through the targeting efforts of the G2 or S2, the G3 or S3, and the fire support element (FSE), and approved by the commander. Target development identifies, locates, and tracks HPTs until thev are neutralized. Target development operations must provide sufficiently accurate targeting data to attack by fire, maneuver, or electronic means.

Situation and target development provide the intelli gence required to fight the AirLand Battle. Both are distinct tasks, but are interrelated and totally integrated to provide an accurate picture of the battlefield.

EW (discussed in Chapter 8) exploits, disrupts, and deceives the enemy command and control (C^2) system while protecting friendly use of communications and non-communications systems. It is a significant force multiplier when integrated and employed with fire and maneuver. EW consists of the following functions:

- EW support measures (ESM), which provide commanders the capability to intercept, identify, and locate enemy emitters.
- Electronic countermeasures (ECM), which provide commanders the capability to disrupt enemy use of the electromagnetic spectrum.
- Electronic counter-countermeasures (ECCM), which are used to protect friendly command, control, and communications (C^3) systems against enemy radioelectronic combat (REC) activities.

CI (discussed in Chapter 9) includes specific actions which support the protection of the friendly force. Enemy commanders, to succeed against friendly forces, must employ all-source intelligence systems to collect information about friendly forces. Depriving enemy commanders of vital information about friendly forces is crucial to friendly success on the battlefield. CI enhances the operations security (OPSEC) of the command by supporting the following actions:

- Countering the hostile intelligence threat.
- Safeguarding the command from surprise.
- Deceiving the enemy commander.
- Countering enemy sabotage, subversion, and terrorism.
- Developing essential elements of friendly information (EEFI).

THE INTELLIGENCE ANALYSIS SYSTEM

The intelligence analysis system is a single, integrated system that extends from battalion level to national agencies. Figure 1-3 shows the all-source intelligence system.

The system includes the directors, coordinators, producers, and executors. All are linked together both laterally and vertically to ensure a coordinated and effective effort. Figure 1-4 shows the common IEW structure.

Analysis elements are the heart of the intelligence system. They include--

- Intelligence officers and their staff sections.
- Echelons above corps intelligence centers (EACICs).

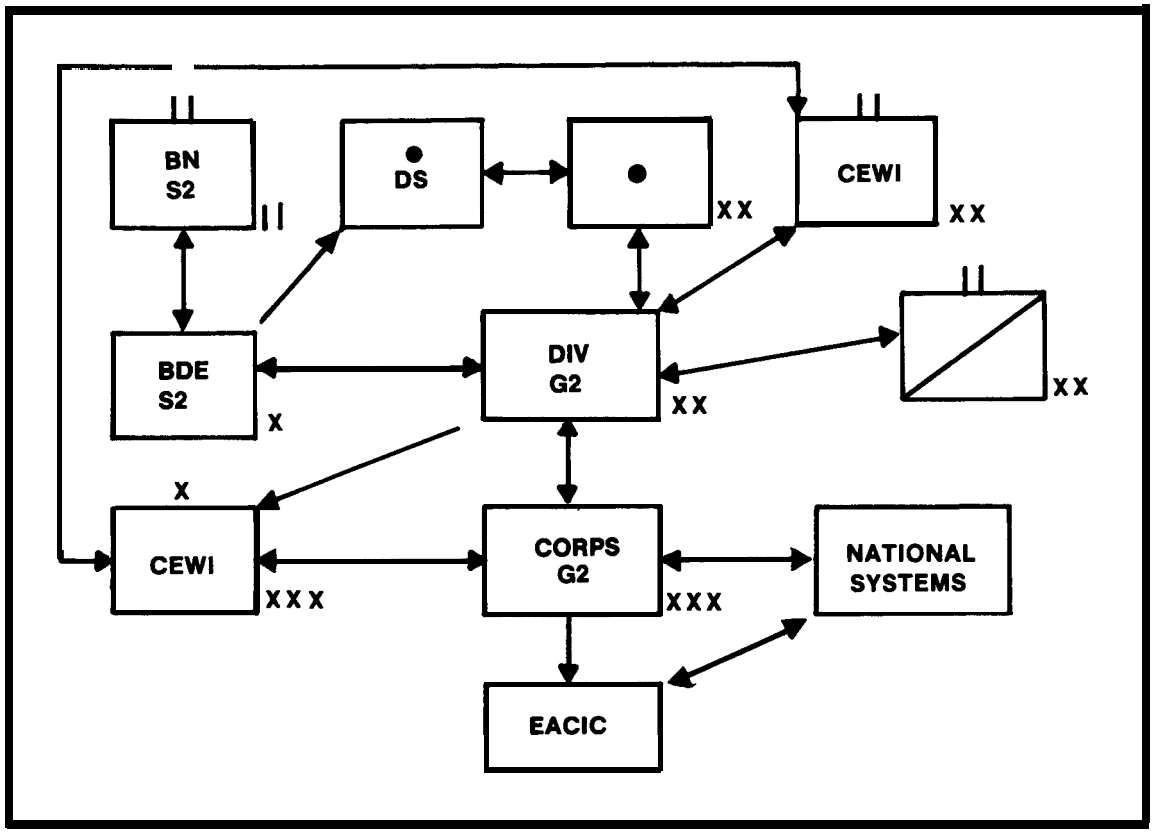


Figure 1-3. All-source intelligence system.

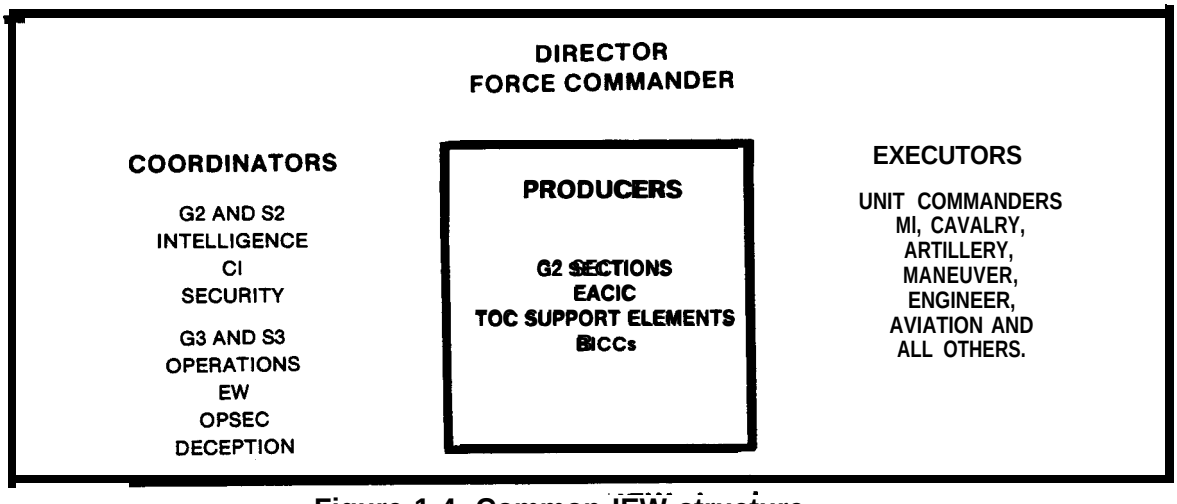


Figure 1-4. Common IEW structure.

- Tactical operations center (TOC) support elements at division and corps levels.

- Technical control and analysis elements (TCAEs) organic to military intelligence (MI) combat electronic warfare and intelligence (CEWI) battalions at division-level and MI CEWI brigades at corps-level.

- Battlefield information coordination centers (BICCs) at maneuver and artillery battalions and brigades.

INTELLIGENCE DIRECTOR, COORDINATORS, AND PRODUCERS

The intelligence director (commander), coordinators (staff), and producers (such as EACICS, TOC support elements, TCAEs, and BICCs) play the major roles in intelligence analysis.

Commander

The commander plays a critical role in intelligence analysis. The commander determines what intelligence is needed to plan and execute an operation. The commander provides guidance to the staff to ensure that the analysis effort is integrated with the other functional systems of the command and that it is focused on critical requirements and priorities. The commander, with the intelligence and operations staffs, accomplishes the planning, directing, guiding, and decision making that generate intelligence analysis and keep it going. The commander approves or modifies the priority intelligence requirements (PIRs) recommended by the G2.

Staffs

While the commander approves the PIR for the command, every staff officer in the command needs intelligence to support the functions under their staff responsibilities. However, the staff officers that are most invoived with intelligence requirements are the G2 or S2, the G3 or S3, and the FS coordinator (FSCOORD).

G2 or S2. The G2 or S2 manages intelligence operations. This officer is responsible for intelligence production and for determining the enemy's intentions. The G2 or S2 recommends PIR, based on the commander's guidance and concept of the operation. The officer manages the collection effort, supervises al i-source analysis, and ensures that combat information and intelligence are disseminated rapidiy. The G2 or S2 deveiops the intelligence estimate. The officer ensures a team effort in planning, supervising, and executing iEW operations within the command.

G3 or S3. Second only to the commander, the G3 or S3 is the primary user of intelligence. As the principal planner and coordinator of unit operations, this officer relies heavily on intelligence support. The operations officer compietes the estimate of the situation and recommends which friendly courses of action are feasible and which should be adopted. These estimates are based on the METT-T, of which a major part

is provided by intelligence. The G3 or S3 IRs are the same as, only more detailed than, those of the commander. The operations officer plays a key role, in conjunction with G2 or S2, in developing and recommending the PIR.

The G3 or S3 also has staff responsibility for EW, OPSEC, and battlefield deception (BAT-D). This officer relies on intelligence to plan and coordinate each of these functions.

Fire Support Coordinator. The FSCOORD plans and coordinates FS. This officer needs intelligence for FS targeting and target development. The FSCOORD, G2 or S2, and G3 or S3 coordinate very closely in selecting HPTs and developing targeting data for attacking HPTs.

Tactical Operations Center Support Elements

The TOC support elements provide dedicated intelligence support to the G2 or S2. TOC support elements, which are assigned to the headquarters and headquarters company (HHC) of the division, or the operations battalion of the corps MI brigade, perform intelligence collection management (CM), analysis, and dissemination functions. The all-source production section (ASPS) or equivalent element within the TOC support element performs intelligence analysis. Other TOC support element sections are collection management and dissemination (CM&D) and CI analysis, which support the G2: and the EW and OPSEC staff elements, which support the G3. There is also an informal targeting team formed in the DTOCSE and CTOCSE to assist in the targeting effort.

The ASPS works under the staff supervision of the G2 or S2. It develops and maintains the intelligence data base. It develops intelligence from unprocessed information and other intelligence products. It performs IPB, assists the G2 or S2 in developing the intelligence estimate, and develops the analysis of the battlefield area. It also develops situation and targeting data to support maneuver, fire, and other battlefield functions. Each ASPS coordinates with other TOC support elements to ensure that all available data is evaluated and to exchange analysis approaches, techniques, and ideas for solving common intelligence problems.

Technical Control and Analysis Element

The TCAE, in addition to managing the signals intelligence (SIGINT) collection and EW assets, performs SIGINT analysis for the command. It maintains the enemy electronic order of battie (EEOB) and technical data bases. It analyzes and correlates ESM and SIGINT data from all sources to update the EEOB and technical data bases needed to produce SIGINT. It passes SIGINT data to the ASPS for correlation with information and intelligence from other sources.

Battlefield Information Coordination Centers

The BICCs are organic to maneuver brigades, battalions, and other support units. They consist of analysts who operate within their unit

TOCS as an integral part of the S2 section. They provide an organic intelligence management, production, and dissemination capability. BICCs vary in the size and type of support they provide, For example, maneuver unit BICCs concentrate on both situation and target development, while artillery unit BICCs are almost exclusively interested in target acquisition (1A) and development.

INTERACTION OF ANALYSIS ELEMENTS

Close coordination and interaction between analysis elements make the system function effectively. Analysis elements at all echelons exchange requirements, information, and intelligence both laterally and vertically throughout the system. At the same time they disseminate combat information and intelligence to maneuver, FS, and other units that need it.

CHAPTER 2

THE INTELLIGENCE CYCLE

Intelligence operations follow a four-phase process known as the intelligence cycle. The intelligence cycle is oriented to the commander's mission. Supervising and planning are inherent in all phases of the cycle. Figure 2-1 shows the intelligence cycle.

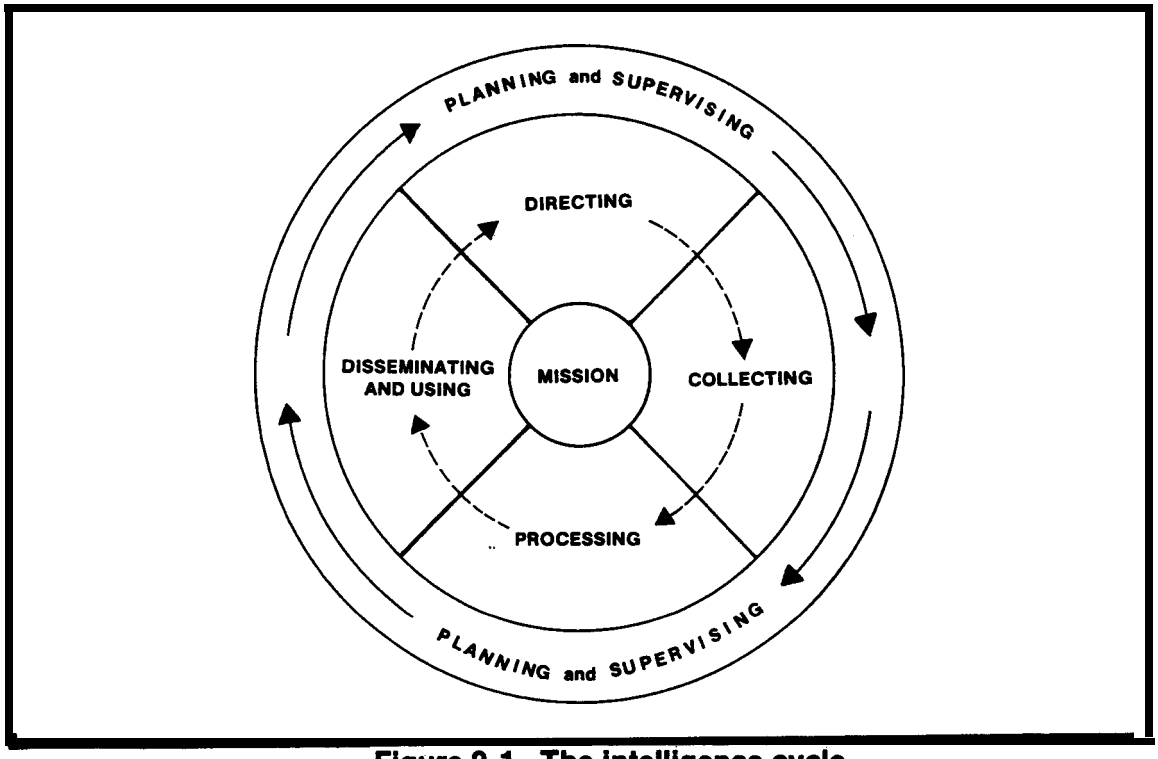


Figure 2-1. The intelligence cycle.

The intelligence cycle is continuous. Even though the four phases are conducted in sequence, all are conducted concurrently. While available information is processed, additional information is collected, and the intelligence staff is planning and directing the collection effort to meat new demands. Previously collected and processed information (intelligence) is disseminated as soon as it is available or needed.

This chapter describes the procedures outlined above and the processing phase of the intelligence cycle.

DIRECTING

The intelligence effort begins by determining requirements, establishing their priorities, and communicating information or intelligence collection orders (to subordinate elements) and requests (to

higher and adjacent units). This is accomplished by the commander and the intelligence and operations staff. Sources of information or intelligence requirements include the following:

- Commander's planning guidance, concept of the operation, and stated requirements.
- METT-T analysis by intelligence and operations staffs.
- Requests for intelligence information (RIIs) from higher, adjacent, allied, and subordinate units and elements, and from other staff elements within the command.

The highest or most important IRs are designated as PIRs. The commander chooses PIRs based in part on the recommendation of the G2 or S2. PIRs are those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision making. However, an excessive number of PIRs degrades efforts to focus relatively scarce intelligence collection resources on the most essential intelligence requirements.

IRs are those items of information regarding the enemy and the environment needing collection and processing to meet the intelligence requirements of the commander. IRs can either support PIRs or be stand-alone requirements of a lesser priority than PIRs. Both PIRs and IRs serve as the basis for collection and intelligence efforts.

Intelligence analysts in the ASPS advise the G2 regarding the PIRs and IRs. They analyze METT-T factors and the commander's guidance and concept of the operation to determine what intelligence and information is needed. The ASPS reviewa the existing data base to identify information that is already available and that which must be acquired. They pass requirements for new information to the CM&D section as additional collection requirements. Figure 2-2 shows the directing phase from the commander's intent to the commander's requirements.

COLLECTING

Based on requirements, the CM&D section manages the collection effort. The CM&D section develops a collection plan that is keyed to the PIRs and IRs. It continuously updates the collection plan as the situation changes.

The ASPS assists the CM&D section in planning and supervising the collection effort. The ASPS helps convart intelligence requirements into specific information requirements (SIR). SIR are keyed to indicators (see Appendix C) which when integrated with other indicators and factors present on the battlefield may provide clues to the enemy's most probable course of action. The ASPS monitors incoming reports, advises the CM&D section when PIR or IR are satisfied, identifies naw requirements, and determines when previously requested information is no longer needed.

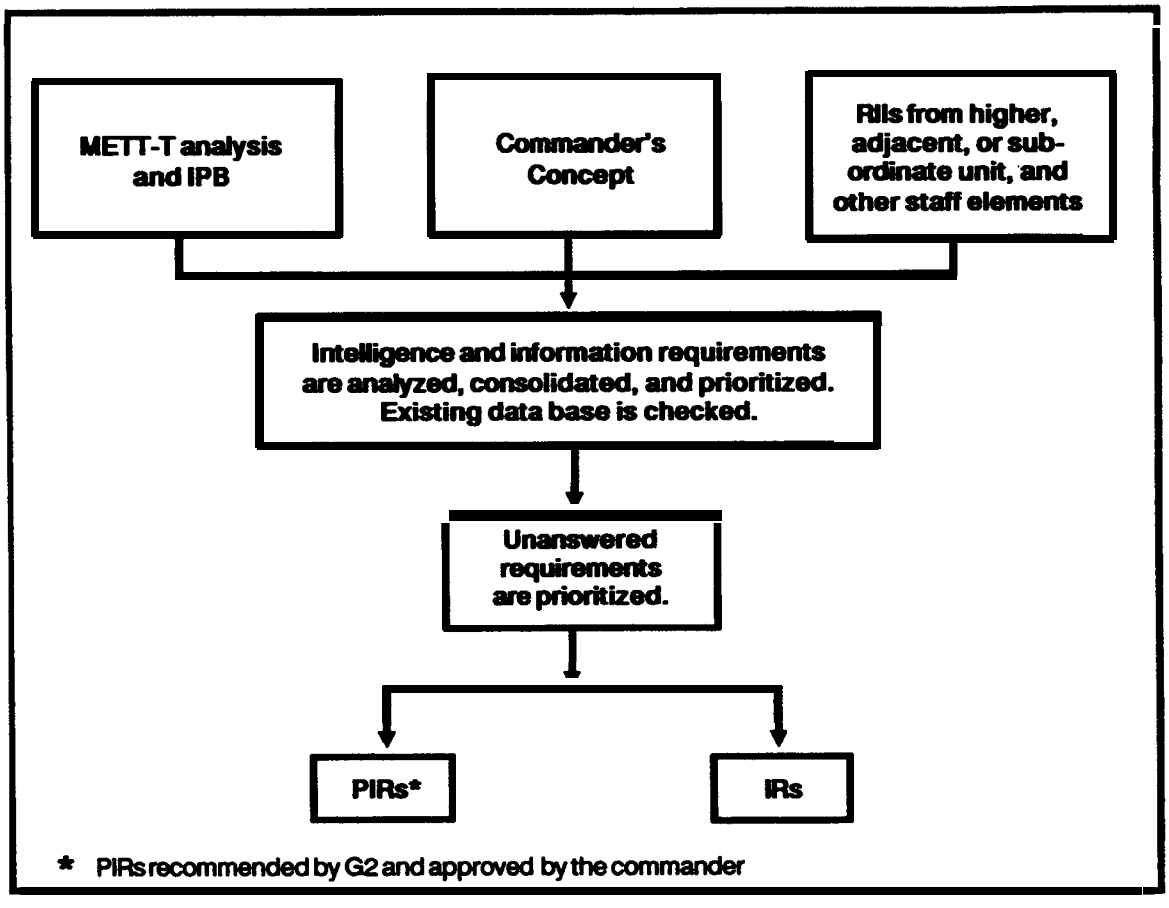


Figure 2-2. Commander's requirements and guidance.

Collection operations generate information from various sources. This information is fed into the ASPS. The ASPS--

- Reports combat information immediately.
- Processes information to develop the intelligence needed for tactical decisions and targeting.

PROCESSING

Processing is the phase in the intelligence cycle in which information becomes intelligence. It consists of three operations:

- Recording. Recording is the reduction of information to writing or some other form of graphical representation and the arranging of this information into groups of related items.

- Evaluation. Evaluation is the determination of the pertinence of information to the operation. reliability of the source or agency, and accuracy of the information.

- Analysis. Analysis is the determination of the significance of the information. relative to information and intelligence already known, and drawing deductions about the probable meaning of the evaluated information.

Processing is a continuous operation. The analyst processes new information as it is received without waiting for additional information. Intelligence derived from fragmentary information is essential, particularly during fast-moving operations or when the information concerns an HPT. Normally there is a time lag between the time an enemy target presents itself and the time the information becomes available to an element that can react to it. Complete information about a target or a situation is seldom available. The analyst continuously identifies information gaps and attempts to acquire information to complete, confirm, or refute fragmentary information. This information must assist the corrmander to generate and apply combat power. It helps the commander to strike critical units or areas, and to achieve and retain the initiative. Figure 2-3 shows information processing.

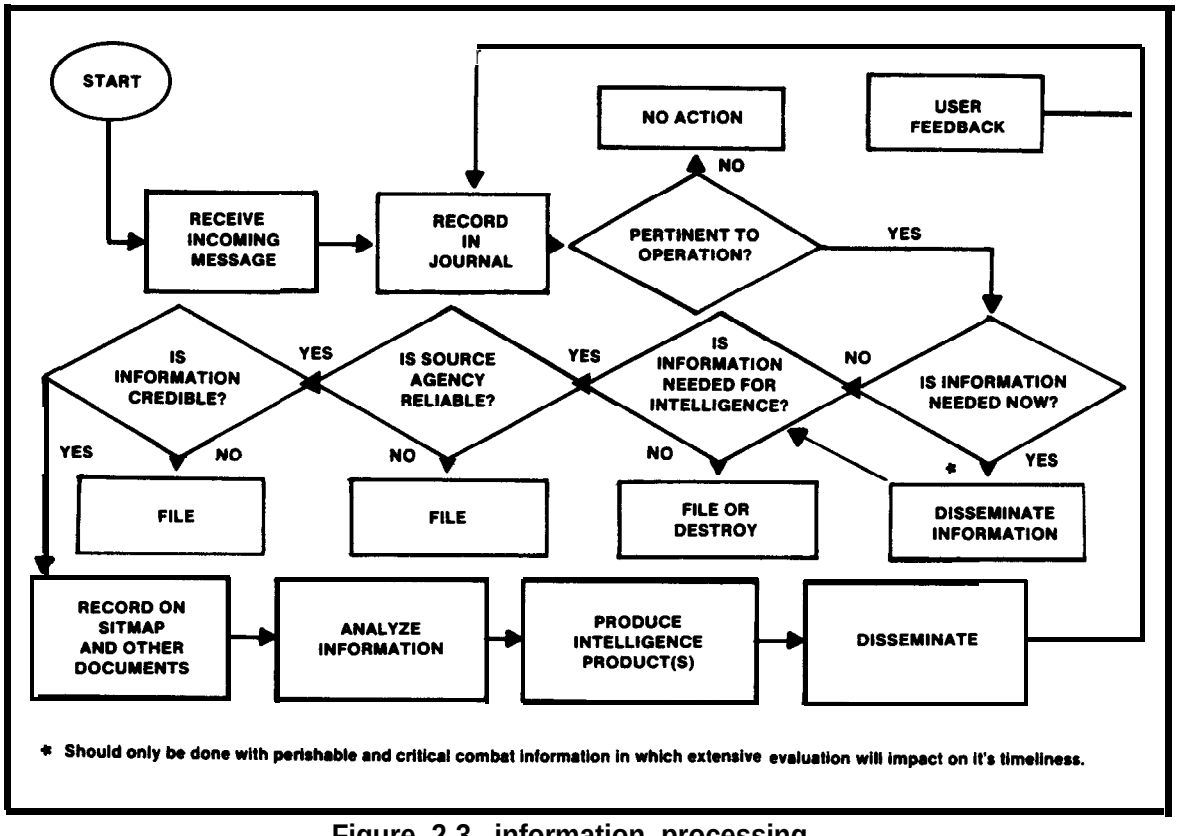


Figure 2-3. information processing.

The sequence for processing varies with the nature and urgency of the information. Information is normally recorded first: however, if it contributes to the development of urgent intelligence, it is recorded simultaneously with or after evaluation and analysis. Combat information or partially developed intelligence that is needed immediately is disseminated before it is completely processed. Information that is not of immediate value is processed before it is disseminated.

Evaluation and analysis may occur simultaneously followed by immediate dissemination. For example, information from a reliable source may indicate that the enemy is about to launch a major attack, In this case, recording is of secondary importance, and the intelligence report that an attack is imminent is disseminated as soon after receipt as possible.

Reporting of information to higher and lower echelons occurs concurrently with processing, For example, to speed target execution time of HPTs, a commander orders lower headquarters to report all information concerning specified enemy units, areas, or activities before the processing cycle is complete. Lower headquarters make similar requests of higher headquarters,

A sound collection program that effectively uses collection assets results in a heavy volume of information. Some information may be of no use to the collecting unit, but of great value to adjacent, higher, or lower units. This includes many reports which may appear insignificant and unrelated to other information. However, when these reports are analyzed along with other available information, definitive and predictable patterns of enemy activity often emerge.

Today, most information is processed manually. Emerging automatic data processing (ADP) systems help the analyst process greater volumes of information faster and mors accurately. Appendix B describes ADP support to intelligence analysis. Developing and maintaining an intelligence data base is essential to processing. The data base is the basis for analyzing new information neaded for situation and target development as well as CM, EW, and CI operations. When possible, intelligence data bases are created for contingency areas during peacetime. Initially, data base information and intelligence are collected by researching available literature published by various agencies and sources, including the following:

- Central Intelligence Agency (CIA).
- Defense Intelligence Agency (DIA).
- National Security Agency (NSA).
- US Army Intelligence Agency (USAIA),
- Unified and specified commands.
- Theater commands.

- Allies.
- Open sources.

The analyst identifies gaps in the data base and passes requirements to the collection manager. As information is received from the various collection agencies, it is correlated with existing information in the data base to assess its significance. Combat information, often highly perishable in nature, is disseminated immediately.

RECORDING

Recording information into the data base makes evaluation and analysis easier and more accurate and facilitates preparation of intelligence reports by conveniently drawing together all available information on a specific subject. The recording means used must be adequate to handle the volume of information and intelligence received and to serve the needs of those who must have access to it. Means and techniques of recording must permit timely dissemination of information and intelligence.

Recording is more complex at higher command echelons. At division level and above, ADP systems assist in the recording function. Some of the more common recording devices are listed below. Others are used when required.

- Intelligence journal.
- Intelligence files.
- Situation map (SITMAP).
- Intelligence workbook.
- Coordinate register.
- Order of battle (OB) records.

Intelligence Journal

The journal is an official, permanent, and chronological record of reports and messages that have been received and transmitted, important events that have occurred, and actions taken in response. Accuracy and completeness are essential , since various elements of the headquarters will refer to it later. It covers a specified time period, usually 24 hours. Journal entries should reflect--

- An accurate and concise statement of the message, report, or event.
- A notation about the sender or individual making the report, to include unit duty position and section: for example, S3 1/60 Infantry Battalion.

- The time of receipt or dispatch and method of transmission.

- Action taken as a result, to include dissemination given to reports, other information received, and other internal G2 recording (workbook, SITMAP),

Journal entries are concise and record the time and essential facts. As a minimum the journal entries include--

- Purpose, subject, and conclusions of conferences.

- Command decisions and summarizations of plans.

- Movements of enemy units, one echelon above and two echelons below your own level,

- Significant messages (radio, radio teletypewriter (RATT), hard-copy, overlays, photos, and any other verbal or written reports) transmitted and received.

- Incidents of enemy activity.

- Friendly patrol activity.

- Liaison activities.

- Changes in personnel within the staff section.

- Summaries of written messages and orders.

- Summaries of action based on enemy and friendly activity.

Figure 2-4 shows a partially completed intelligence journal (DA Form 1594).

Intelligence Files

Intelligence files permit ready access to all available information. The files most commonly maintained are the journal file, reference file, and OB file.

Journal File. The journal file contains all previously recorded journal sheets and supporting materials. Supporting material referenced on the journal sheet is filed in chronological sequence. It includes copies of orders, periodic reports, messages, memoranda, conference notes, map overlays, and other material required to support the journal entries. The journal number is annotated on the supporting document. The unit SOP normally describes procedures for maintaining a journal. One good method is to begin the annotation with the letter "J," followed by the date and an entry number. The fifth entry on June 23d would read "'J-23-05."

DAILY STAFF JOURNAL OR DUTY OFFICER'S LOG
For use of this form, see AR 220-15: the proponent agency is Office of The Deputy Chief of Staff for Operations & Plans.

PAGE NO. 1 | NO. OF PAGES 1

ORGANIZATION OR INSTALLATION: 2D BDE, 52D MECH DIV
LOCATION: BURGEW, GE (LA567275)
PERIOD COVERED: FROM HOUR 0001 DATE 07 DEC 80 — TO HOUR 2400 DATE 07 DEC 80

ITEM NO.	TIME IN	TIME OUT	INCIDENTS, MESSAGES, ORDERS, ETC.	ACTION TAKEN	INL
1	0001		Journal opened 0001		BW
2	0030		1st BTF: Company team A patrol reported		
			enemy supply dump vicinity LA888912.	Map, S3, Cdr	BW
3		0055	ALL UNITS: Execute alternate challenge	Cdr, Staff, Units	DJT
			password. Primary compromised at 0700045.		
4	0200		1st BTF: Follow-up to item 2. Search	Cdr, S3	DJT
			results: 12XAT mines, 30,000 rounds 7.62		
			ammunition, 6 rolls barbed wire, all destroy-		
			ed in place.		
65	2400		Journal closed 2400		
			SUMMARY		
			No enemy contact during period, but one		
			enemy ammunition dump destroyed.		

SAMPLE

TYPED NAME AND GRADE OF OFFICER OR OFFICIAL ON DUTY: SAMUEL A. MORRIS, CPT, MI
SIGNATURE: SAM

DA FORM 1 NOV 62 1594 PREVIOUS EDITION OF THIS FORM IS OBSOLETE. ☆ U.S. Government Printing Office 1984—421-846/17155

Figure 2-4. Intelligence journal sample page.

Reference File. The reference file includes all information that is not of immediate interest but may be of future value. Information is cross-indexed to permit easy retrieval.

OB File. The OB file is discussed in Chapter 3.

Working Situation Map

The working situation map (SITMAP) is the primary analytic tool at all echelons. It is a temporary graphic display of the current dispositions and major activities of the enemy. Information about friendly forces on this map usually is limited to boundaries; locations of command posts (CPs) of higher, lower, and adjacent units; reconnaissance units; the forward edge of the battle area (FEBA), and forward line of own troops (FLOT). The level of detail of the working SITMAP will be proportionate to the echelon at which it is maintained.

Generally, enemy maneuver units are posted which are two echelons below that of the friendly unit. Enemy units, regardless of size, in our rear area are always posted because of the amount of damage they can do to administrative and logistical nodes.

Enemy headquarters (especially regimental and higher levels) and CS and CSS asset locations are also posted. The SITMAP reflects enemy unit identification, disposition, and boundaries; major roads or trails for movement of personnel, weapons, and equipment; and locations of, for example--

- Automatic weapons (battalion SITMAP only).
- Supporting mortars (battalion SITMAP only).
- Antitank guns (battalion SITMAP only).
- Artillery,
- Air defense artillery.
- Minefields.
- Roadblocks.
- Entrenchments.
- Obstacles.
- Defensive positions.
- Logistics and command facilities.
- Aircraft and helicopter staging areas.
- Nuclear, biological, and chemical (NBC) contaminated areas.

- Ground surveillance devices.

- Smoke screens.

When plotting enemy activities and dispositions, indicate the latest time at which the activity was observed or the disposition confirmed. The S2 ensures that the working SITMAP and supporting overlays are maintained as simply as possible and that authorized conventional signs, mil itary symbols and abbreviations are used. See FM 101-5-1 for authorized abbreviations and map symbols. Explain any deviations from these symbols in the marginal data on the map or overlay, Necessary classification markings also must appear in the margins of maps and overlays.

Rather than attempting to plot all entries on a map by means of conventional or Improvised military symbols, the S2 uses a number or letter to plot the area where the activity was observed. A corresponding letter or number then is entered into a space alongside the map and a notation entered as to the activity observed. Use a number or letter that is easily cross-indexed to the journal or message file for a complete report. Ensure that the number or letter indicating an activity in the journal file matches that on the working SITMAP (see "action taken" column in Figure 2-4).

Care must be taken to prevent overcrowding the map, One method of doing this is to group entries by categories on a series of acetate overlays. Use separate overlays to display separate categories of information. A typical separate overlay might show fortifications or potential targets or details of OB. An enlarged sketch map also is prepared to cover overcrowded areas. This allows the presentation of additional details.

The working SITMAP (discussed in this chapter) and the OB SITMAP (discussed in Chapter 3) are two separate items. Although the same types of information are recorded on each, their functions differ. The G2 or S2 uses the working SITMAP for recording and analyzing. The OB SITMAP normally is less cluttered than the working SITMAP.

Maintenance of the OB SITMAP at brigade and battalion levels usually is a joint S2 and S3 action. At higher levels, each section maintains a separate SITMAP. Plotting the friendly situation is the responsibility of the S3, while the enemy situation is the responsibility of the S2. During operations, personnel from either section map or plot friendly or enemy entries on the SITMAP and perform other processing functions.

When the intelligence and operations staffs use separate maps, ensure that acetate overlays are readily interchangeable between these maps. This permits easy comparison of the current enemy situation (G2 or S2 map) with the disposition of friendly forces (G3 or S3 map), and easy comparison of enemy obstacles, barriers, and minefield with planned routes of march.

Examples of separate SITMAP overlays are--

- Enemy fortifications.
- High value targets.
- Obstacles.
- OB data.
- Friendly reconnaissance patrols.
- Surveillance activities (include the ground coverage of each system).

The maintenance of the working SITMAP takes precedence over ail other recording means during combat operations. In a fast-moving situation, particularly at the maneuver battalion level, it is the oniy recording device used.

The working SiTMAP is continually purged of information that is not current or otherwise no longer needed. Purging keeps it neat and uncluttered, making it more useful as an analysis tool. Map overlay tracings or periodic photographs of the SITMAP provide a permanent record of the situation. These records provide a reference to past enemy activity and help determine patterns of enemy movement and dispositions.

Use the working SITMAP to make sound tactical decisions; its primary intelligence uses are to--

- Display the enemy disposition and situation.
- Provide a basis for comparison to determine the significance of newly received data about enemy forces. IPB situation and event templates provide a basis for comparison.
- Provide a background and basis for briefings and other required intelligence reports.
- Provide the basis for overlays which graphically portray the enemy situation.
- Assist in the determination of movement patterns of guerrilla or insurgent forces.
- Show possible intelligence gaps which require redirection of the collection effort. For example, the need to locate and identify enemy units reported for the first time.

For secondary intelligence use, post the following information in the margin of the working SITMAP or on charts or cards nearby:

- Computations of enemy personnel and weapon strengths and weaknesses.

- Organization charts of specified enemv units.
- Summaries of weather and terrain data.
- A listing of PIR and IR.
- Notations about the current patrol plan.
- Movement computations.
- A listing of friendly attachments.
- A listing of unlocated enemy units believed to be in the AO.
- Probable courses of action.
- Battle damage assessment (BDA).

Chapter 6 describes how the SITMAP is used in situation development.

Intelligence Workbook

The intelligence workbook contains information arranged by subject heading. This arrangement helps to sort, evaluate, interpret information, and prepare intelligence reports. It is not a permanent record and it is not distributed to an outside agency. The workbook is kept current with obsolete entries deleted. At higher echelons, analysts maintain separate workbooks on various subjects.

There is no prescribed format for the workbook. At division and lower headquarters, use index tabs to label information in the intelligence summary (INTSUM). At corps and higher levels, use index tabs to label information in the periodic intelligence report (PERINTREP).

Record incoming messages and reports; for example, information concerning a newly identified armor unit could be recorded under index tab 3A, NEW UNITS, as well as index tab 2B, ARMOR. A message that furnishes information on different subjects results in several entries: each entry contains only that subject information. For example, a message containing information on the locations of a reserve armor unit and an artillery unit results in extracts under item 2B, ARMOR and under 2C, ARTILLERY. Base each entry in the workbook on an incoming message and include a reference to the journal serial number of that message. For example, J2, 091200 April, from 20th Engr Cbt Bn: "Bridge at LINDEN AB 910246 destroyed by bombing. Estimated out of action for 30 hours."' The J2 refers to the journal serial number and the date-time group (DTG) entered refers to the time of occurrence of the event. The intelligence officer makes written comments on the evaluation of the information and its possible significance following the appropriate entry.

Figure 2-5 shows a sample intelligence workbook which might be used at corps and higher levels.

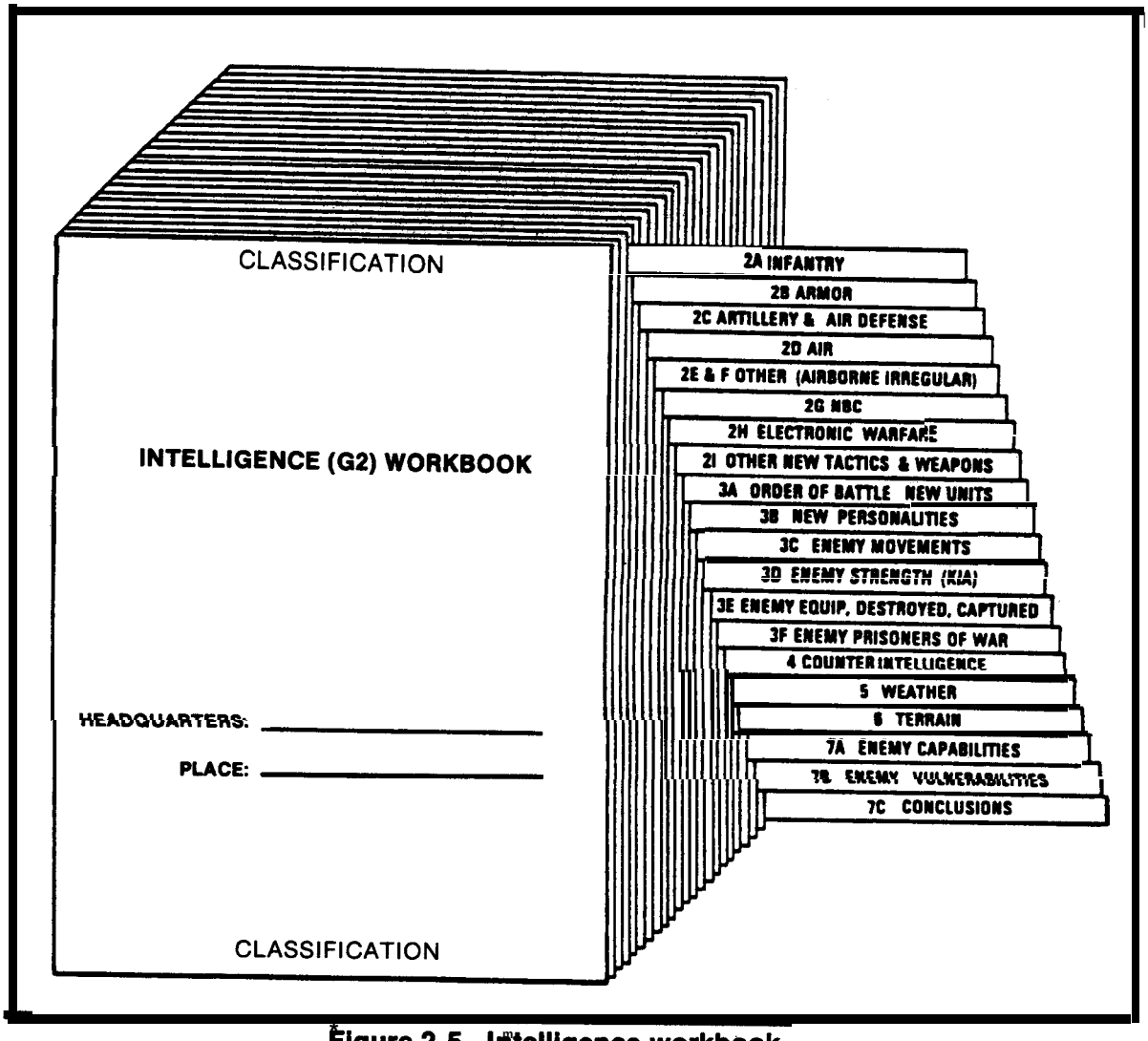


Figure 2-5. Intelligence workbook.

EVALUAT 10N

Evaluation includes determining the pertinence of information, the reliability of the source or agency through which the information was derived, and its credibility. Evaluation of information at the lower echelon is a simple step compared to the procedures employed at higher echelons. From the viewpoint of the brigade or battalion S2, information which relates to the unit's AO and AI is pertinent; information relating to areas outside the area of interest may or may not be pertinent. The brigade or battalion S2 may not be able to judge the reliability of a source because the S2 may not have repetitive contact with that source. This difference between higher and lower echelons is because information received from higher headquarters normally has been processed, evaluated, and interpreted and the information collected by organic agencies at lower

echelons generally is acquired by direct observation or actual contact with the enemy.

Pertinence

Pertinence is the examination of information to determine whether or not the information is-

- Pertinent with regard to the enemy or to the battlefield area. Information that relates to a unit's AO or AI normally is pertinent.
- Needed immediately, and if so, by whom? Of possible present or future value, and if so, to whom?

Reliability

The source of information and the agency by which it was collected are both evaluated for reliability. The principal basis for judging the reliability of a source or an agency, other than troop units, is previous experience with the source. Criteria for evaluating troop units include a knowledge of their training, experience, and past performance.

The headquarters closest to the source or agency is ordinarily the best judge of its reliability. Consequently, a higher headquarters normally accepts the reliability evaluation performed by a reporting headquarters. It does, however, consider the reliability of the reporting headquarters itself.

Credibility

Credibility means the probable truth of the information. Judgment of credibility is based on the answers to the following questions:

- Is it possible for the reported fact or event to have taken place?
- Is the report consistent within itself?
- Is the report confirmed or corroborated by information from different sources or agencies?
- Does the report agree or disagree in any way with other available information?
- If the report does not agree with information from other sources or agencies, which one is more likely to be true?

The most reliable method of judging the accuracy of a report is by comparing it with similar information which already may be available in an intelligence file or workbook. When possible, the intelligence officer obtains confirming or refuting information through different agencies and from other sources.

Marked differences in the evaluation of the accuracy of information may occur between higher and lower echelons. The reason for this difference is because higher echelons, which have more sources of information and intelligence than lower echelons, have a greater opportunity to confirm, corroborate, or refute the accuracy of reported data. Regardless of the source, reevaluate the accuracy of incoming information and intelligence at each echelon. Thus, the role of higher echelons in evaluating the credibility (or probable truth) of information differs somewhat from its role in evaluating the reliability of the source (again, usually done best by the echelon closest to the source),

The evaluation rating of each item of information is indicated by a standard system. Reliability is shown by a letter; accuracy by a numeral . The lowest headquarters possible assigns the evaluation ratings.

Indicate the reliability of the source and agency as follows:

A - completely reliable.

B - usually reliable.

C - fairly reliable.

D - not usually reliable.

E - unreliable.

F - reliability cannot be judged.

A rating of "A" indicates only the most unusual circumstances. For example, this evaluation is given when it is known that the source has long experience and extensive background with the type of information reported. A rating of "B" indicates a source of known integrity. A rating of "'F" indicates there is no basis for estimating the reliability of the source.

Agencies ordinarily are rated A, B, or C. However, when the source and the collecting-reporting agency are evaluated differently, only the lower degree of reliability is indicated.

Indicate the credibility of information as follows:

1 - confirmed by other sources.

2 - probably true.

3 - possibly true.

4 - doubtfully true.

5 - improbable.

6 - truth cannot be judged.

If it can be stated with certainty that the reportsd information originates from a source other than that for already existing information on the same subject, it is classified as "confirmed by other sources" and is rated "'l.'"

If no proof in the above paragraph can be established, and if no reason exists to suspect that the reported information comes from the same source as the information already available, it is classified as "'probably true" and is rated "2.'

If the report is confirmed in essential parts by information already available, it is classified as "probably true"' and is rated "2."

If the investigation reveals that the raported facts, on which no further information is yet available, are compatible with the previously observed behavior of the target, or if the known background of a person leads to the deduction that the person might have acted as reported, the information raceived is classified as "possibly true"' and is rated "3."

Reported but unconfirmed information, which contradicts the estimate of the development or the known behavior of the target, is classified as "doubtful" and is rated "'4'" if this information cannot be disproved by available facts.

Reported information which is not confirmed by available data and contradicts the experience hitherto assumed to be reliable with regard to the development of a target or issue is classified as "improbable" and is rated "5." The same classification is given to reported information that contradicts existing data on a subject originally given the rating "'l" or "2."

If the investigation of a report reveals that a basis for rating 1 to 5 is not given, the reported information is classified as "truth cannot be judged"' and is rated "6."

The statement "truth cannot be judged" is always preferred ovar the inaccurate use of ratings 1 to 5. If there is no sound basis for rating 1 to 5 because of the complete absence of other information on the same target, it must be rated 6.

The scale 1 to 6 does not represent progressive degrees of accuracy. Recognition must be given to the rating represented by the numeric symbol.

Although both letters and numerals are used to indicate the evaluation of an item of information, they are independent of each other. A completely reliable agency may report information obtained from a completely reliable source which, on the basis of other information, is judged to be improbable. In such a case, the evaluation of the information is A-5. A source known to be unreliable may provide raw information that is accepted as accurate information, when confirmed by reliable sources. In this case, a report is evaluated E-1. A report evaluated F-6 may be accurate and should not be arbitrarily discarded.

A report disseminated to higher, lower, and adjacent units should contain the evaluation for each item of information; for example, '"The division artillery of the enemy 46th Tk Div can fire nuclear rounds of 0.5 kt yield (C-3)."

The evaluation and interpretation of information at the brigade and battalion is a simplified mental process: thus, the standard evaluation rating has little if any application. This system assists the G2 or S2 in processing information received from other headquarters and in evaluating information disseminated to other headquarters.

ANALYSIS

The processing of information continues with analysis, which consists of three steps: assessment, integration, and deduction. It is during this phase of the intelligence cycle that information becomes intelligence.

Assessment

Assessment is the sifting and sorting of evaluated information to update significant elements with respect-to the mission and operations of the unit. The first and most important step towards proper assessment is a clear understanding of the unit's mission and the commander's intent. All information gathered is viewed in relation to what the commander wants to accomplish. Assessment also requires judgement and a thorough knowledge of military principles, the characteristics of tha AO, and the enemy situation, to include enemy doctrine and past practices.

Assessment at headquarters above division level often involves detailed research with greater difficulty caused by the increased volume of information. Regardless of the level, individuals who assess information must relate their efforts to the unit's mission to avoid wasted time and effort.

Integration

Integration is the combination of the elements isolated in assessment with other known information to form a logical picture or hypothesis of enemy activities or the influence of operational area characteristics on the mission of the command. In the process, more than one hypothesis may be formulated based upon existing intelligence.

Integration, particularly the development of hypotheses, requires the same good judgment and thorough background knowledge essential to making a good assessment. In formulating hypotheses, the intelligence officer avoids preconceived opinions and hypotheses based solely on personal experience or preference. The officer attempts to adopt the role of the enemy commander in the development of these hypotheses.

After they are formulated, all hypotheses are analyzed and tested. Analysis of an hypothesis includes determining the indications that should exist if the hypothesis is a valid one. Testing includes verifying the

existence or nonexistence of these indications within the limitations of available time and means.

Integration may be a mental process completed in a few moments or it may be a lengthy process involving the collection of a large volume of additional information.

Deduction

The last step in the analysis of information is deduction. Meaning is deduced from the hypotheses developed; these are than tested and considered valid as a result of integration. Deduction answers the question: "What does this information mean in relation to the area of operations, the enemy situation, and the friendly commander's intent?" The answer provides a useful conclusion which can serve as a basis for determining future enemy courses of action and for keeping the intelligence estimate current. Deduction should also answer the question: "What does this information mean in relation to the enemy's use of tactical deception or counterdeception?" 'The resulting answer reduces friendly vulnerability to being deceived and the false belief that battlefield deception operations are being believed by the enemy.

DISSEMINATION

The final step is to disseminate intelligence or information. Dissemination is not limited to regular reports. Critical Pieces of information are passed quickly to those who can use them. The G2 or S2 always is aware of this and prepares to use any form of communication, from RATT to courier, to pass vital reports. Intelligence is of no value on the battlefield when it becomes history.

CHAPTER 3

ORDER OF BATTLE

OB intelligence is an integral part of intelligence analysis at all levels. Intelligence analysts consider OB intelligence. They integrate it with other intelligence pertaining to weather, terrain, and other METT-T factors to determine Threat capabilities, vulnerabilities, and probable courses of action.

This chapter describes the OB analysis process and the tools used to develop and integrate OB.

OB is the identification, strength, command structure, and disposition of the personnel, units, and equipment of any foreign military force. During counterinsurgency operations, or whenever they become militarily significant, include guerilla and insurgent forces, associated agent nets, and the insurgent auxiliary and support structure in the Threat data base,

Data is developed in many fields outeide the scope of 0B, but all intelligence is related ultimately to it. For example, technical intelligence (Tl) produces intelligence on the capabilities of weapons systems, but OB intelligence determines the effect of weapon capabilities and characteristics on enemy tactics, combat effectiveness, and organization.

ORDER OF BATTLE FACTORS

The OB consists of evaluated information on enemy, allied and neutral forces, including--

- Composition.
- Disposition.
- Strength.
- Tactics.
- Training.
- Logistics.
- Combat effectiveness.
- Electronic technical data.
- Miscellaneous data.

COMPOSITION

Composition is the identification and organization of units. It appl ies to specific units or commands as opposed to type units. Unit

identification often is called the key to 0B intelligence because it leads to the answers to many questions concerning the enemy, Unit identification consists of the complete designation of a specific unit by name or number, type, relative size or strength, and (usually) subordination. Through identification, the OB analyst develops a history of the composition, training, tactics, and combat effectiveness of an enemy unit. The identification of a specific unit within an organization alerts the analyst to the possible presence of other unidentified or unlocated units of the sama organization.

Organization is the physical structure of a unit and the relationship of the various elements within the structure. Knowledge of the organization of a unit or military force aids in developing accurate intelligence on current strength, and combat efficiency. Further Threat capabilities as they relate to tactics, training, and logistics are difficult to assess accurately without knowledge of the current organizat ion.

The basic self-sufficient tactical unit (normally a combat division) is considered when developing intelligence concerning composition. In some countries, the field army is considered the basic self-sufficient tactical unit. In others, it is the regiment. The importance of this concept I ies in the term "'self-sufficient.'" Units subordinate to self-sufficient tactical units, although capable of limited independent action, cannot sustain themselves over relatively long periods of time. Subordinate units seldom are employed independently or separately from the basic self-sufficient tactical unit. For example, a new Soviet motorized rifle regiment (MRR) is reported in the AO, Knowing that the division is the Soviets' basic self-sufficient tactical unit and the three MRRs of a motorized rifle division (MRD) seldom are employed independently, the presence not only of a new regiment but of a new MRD is given tentative acceptance. When one of these regiments is located, suspect that the remaining elements of the division also are in the area.

DISPOSITION

Disposition consists of the location of Threat units and the manner in which these units are deployed tactically (or administratively in times of peace) . In addition, disposition includes the recent, current, and projected (or probable) movements of Threat units.

Location refers to a geographical area or position occupied by a unit or units. Knowledge of the strength and location of a Thraat force assists the intelligence officer in determining the capabilities of the force and its effect upon the accomplishment of the friendly mission. Data of this type is collected during peacetime and form the basis for assessing capabilities during the initial period of hostilities.

Tactical deployment is the relative position of units with raspect to one another or to the terrain. Tactical formations are designed for executing the various tactical maneuvers and usually are based upon doctrine. If this deployment is predetermined, it leads to an accurate appraisal of probable Threat courses of action. The knowledge of how

units are arranged in echelon indicates (if the Threat assumes the offensive) which units are used in the initial attack and which units are employed in supporting and reserve roles. Tactical deployment with respect to terrain also is important. A study of disposition with an analysis of the terrain leads to conclusions concerning Threat capabilities, vulnerabilities, and probable courses of action. Accomplish this through the IPB process detailed in FM 34-130.

Movement of units is part of disposition. Movement is the physical relocation of a unit from one geographical point to another. Patrol activity may be an indication of planned movement but, in itself, is not movement. Movement is significant because it automatically changes the tactical deployment of the opposing forces. When a Threat unit has moved, is moving, or possibly will move in the future, it becomes capable of executing a number of actions which affect the conduct of the battle (or the current political situation). Such a unit moves into an attack position, moves to reinforce or to replace a unit, or performs other missions. In view of these possibilities, movement of a unit becomes important. The 06 analyst must continually monitor unit movements in order to provide correct and detailed data on Threat dispositions.

STRENGTH

Strength describes a unit in terms of personnel, weapons, and equipment. Information concerning strength provides the commander with an indication of enemy capabilities and helps determine the probable courses of action or options open to Threat commanders. A lack of strength or a preponderance of strength has the effect of lowering or raising the estimate of the capabilities of an opposing force. Likewise, a marked concentration or buildup of units in an area gives the commander certain indications of enemy objectives and probable courses of action. During peacetime, changes in the strength of potential Threat forces are important factors which may indicate changes in the enemy's intention. Appendix D describes enemy strength computations.

TACT I CS

Tactics in OB intelligence include tactical doctrine as well as tactics employed by specific units. Tactical doctrine refers to the Threat's accepted principles of organization and employment of forces for the conduct of operations. Tactics, on the other hand, describe the manner in which units conduct an operation. From a knowledge of tactical doctrine, the OB analyst knows how the Threat may employ forces under various conditions and in certain type situations or special operations. Units normally are expected to perform according to certain patterns within the framework of their tactical doctrine. Ail Armies establish basic principles and patterns for the employment of infantry, motorized rifle (MR), tank, and artillery units in the offense and defense. Of a more specific nature, special ized tactical doctrine a certain unit employs in given situations during combat or training activities is analyzed, because it indicates possible changes in Threat doctrine. Doctrinal templating, as detailed in FM 34-130, is one method of graphically portraying enemy tactics.

TRAINING

Individual and unit training contribute significantly to the combat effectiveness of any military organization. The thoroughness, degree, and quality of individual training which the recruit, specialist, noncommissioned officer (NCO) , and officer receive are major factors in determining the overall efficiency of an armed force. Unit training, normally conducted in seasonal cycles from small unit exercises to large-scale maneuvers, is an essential part of the training necessary for a unit to operate at its full potential. Each type or phase of training a unit accomplishes adds to its capabilities and effectiveness.

Specialized training that a unit receives may point to its ability to undertake certain missions beyond its normal doctrinal capabilities or responsibilities. Therefore, it is easier to appraise the combat effectiveness of a unit when the degree and quality of its training are known, as well as any specialized training it undertakes.

LOGISTICS

Logistics closely relates to combat effectiveness. The adoption of a course of action depends on the abil ity of the logistical system to support that action. With knowledge of the current capabilities of a unit's logistical support structure, make a more accurate evaluation of its capabilities, strengths, and combat effectiveness. Also, the locations of elements of a unit's logistical support structure indicate the disposition of maneuver formations and CS elements. Categories of logistical information include--

- All classes and types of supply.
- Supply lines of communication.
- Logistical requirements.
- Procurement methods.
- Distribution priorities and procedures.
- Transportation networks and modes.
- Installations and logistical control points.
- Terminals.
- Evacuation and salvage procedures.
- Maintenance.

COMBAT EFFECTIVENESS

Combat effectiveness describes the abilities and fighting quality of a unit. Numerous tangible and intangible factors affect it. Combat effectiveness affects the capabilities of a unit or army and is predicted by analyzing--

- Personnel strength.
- Amount and condition of weapons and equipment.
- Status of training.
- Efficiency of the officer and NCO corps.
- Quality of leadership.
- Length of time a unit has been committed in combat.
- Traditions and past performance.
- Personality traits of the unit commanders.
- Geographical area in which committed.
- Morale, esprit, health, discipline, and political reliability (or belief in the cause for which they fight).
- Status of technical and logistical support of the unit.
- Adequacy of military schooling at all levels.
- National characteristics of the people.

ELECTRONIC ORDER OF BATTLE

Electronic OB information is required to conduct EW. This data includes communications and noncommunications equipment parameters, such as emitter type and nomenclature (including encoding equipment), modulation, multiplex capability, pulse duration, pulse repetition frequency, bandwidth, associated weapons systems, and other technical characteristics of electronic emissions. They also include critical communications nodes such as CPS and logistical control points. They support Threat electronic order of battle (EOB) templating. With electronic technical data, a more accurate evaluation of the enemy's vulnerability to electronic countermeasures (ECM) and deception is made; signals intercept and direction finding (DF) for the production of SIGINT is made easier; and support is given to electronic counter-countermeasures (ECCM) by assessing the threat EW capabilities.

MISCELLANEOUS DATA

Miscellaneous data includes supporting information needed by an analyst to develop other OB elements. Miscellaneous data includes basic intelligence described as "know your enemy."

Personality files contain information on certain characteristics and attributes which describe individual members of a military force. A knowledge of personalities is important in identifying units and, in some cases, predicting the course of action the unit will take. Personality data, therefore, is valuable because the tactics and combat efficiency of particular units are often closely related to key individuals within its command structure.

Unit history includes information and intelligence on the elements of a specific unit; on present and past parent units; personalities who have commanded the unit; and other details like past performance and activities which describe, limit, or clarify the capabilities of the unit concerned. The development of unit history is important in determining the capabilities and limitations of a unit. Military or paramilitary units, like individuals, develop characteristics which distinguish them from other units. Just as they consider the various qualifications and traits of threat personalities, OB personnel also must consider a Threat unit as a personality in analyzing its capabilities and limitations. Information on uniforms and insignias is an important part of "'know your enemy" intelligence. This information assists in establishing unit identification and organization and in determining morale and esprit de corps.

Some foreign armies use systems of code numbers, names or false tactical markings to conceal true designations (or affiliations) of units, field post numbers (FPNs) (unit mailing address), and vehicle identification or side numbers. These systems, when properly analyzed, are valuable sources of information that are related to unit composition and disposition.

The OB analyst is able to recognize and appreciate the capabilities and limitations of foreign weapons and equipment. Although technical intelligence agencies are primarily concerned with the determination of weapons and equipment characteristics and capabilities, the analyst uses this intelligence to analyze the effects of these items on the organization, disposition, tactics, and combat effectiveness of the mil itary force.

ORDER OF BATTLE REFERENCES

THIS SECTION IMPLEMENTS STANAG 2077 1

Standard OB references are published by higher echelons during peacetime. They form the basis for lower echelon OB efforts.

ORDER OF BATTLE BOOK

An OB book is a summary of all basic intelligence concerning the composition, disposition, identification, subordination, and strength of a foreign nation's military forces. It includes all units from the various services that function in a ground or ground support role. It normally is published at EAC by the service departments and by the DIA. Allied nations, particularly the NATO nations, also publish OB books. The level or echelon of units shown depends on the level of command for the intended user. Generally, this is at least one echelon above and two echelons below that of the intended user. During peacetime, units which form only on mobilization are identified as such.

The OB book includes the following information for each unit:

- Identification, to include:
  - -- Numerical designator and type of unit.
  - -- Nationality (if more than one nation's forces are included in the OB).
- FPN.
- Subordination (parent unit) .
- Subordinate units.
- Location, to include:
  - -- Place name (and country if deployed abroad).
  - -- Installation number or name (if applicable).
  - -- Military geographic region (if applicable).
  - -- Universal transverse mercator (UTM) coordinates (supplement with geographic coordinates whenever possible).
- Category and effective strength.

The following data also is included:

- Code name or code number (enemy assigns official name or number).
- Nickname (unofficial popular name).
- Honors or honor titles.
- Unit insignia.
- Latitude and longitude of subject (in addition to UTM coordinates) .

- Commander's name, rank, initials and specialty, and those of other key personnel.

- Combat effectiveness (including any data on special ized training).

- Signature equipment.

- Turret numbers, vehicle registration numbers, or other tactica l identification signs.

- Any other data at the discretion of the originator for example, basic encyclopedia (BE) or target data inventory (TDI) numbers.

The structure of an OB book varies, However, it normally contains three sections:

Section 1. General

Section I contains the table of contents, explanatory notes and glossary of terms, acronyms, and abbreviations used in the document, summary list of major changes since the document was last issued, and sumrnary chart of current dispositions.

Section II. Detailed Order of Battle

Section II contains formations or un ts grouped according to their subordination and echelon. For example, military district, region, front level formations, and units follow immediately after the district, region, and front headquarters to which they are subordinate. While the same methodology is applied at all other levels of command within a district, region, or front formation, the inclusion of units subordinate to regiments is optional. Units of unknown subordination are included at the end of each district, region, or front and are identified clearly as such.

Section III. Sumneries or Supporting Documentation

Section III contains any additional summaries or supporting documentation, such as maps. The use of orientation maps of the nations dealt with in the OB book is an important visual aid, especially when the units being dealt with are superimposed. For a large country like the USSR, include an orientation map for each military district.

Annually issue or emend OB books. While the timing and degree of amendment are left to the discretion of the originators, an amendment normally is published when substantial changes to publ ished OB holdings are detected. The date of information (DOI) for the contents of the OB book is taken to be the information cut-off date. Any amendments to the OB book should indicate their own 001.

ORDER OF BATTLE HANDBOOK

The OB handbook, which is often referred to as a "handbook of military forces,"' is a summary of basic intelligence on a foreign nation's

political or governmental structure and military establishment, including its tactics and doctrine. It includes more technical data, such as the logistical system used and the characteristics of weapons and equipment. Like the OB book, higher US and allied commands publish the handbook.

The OB handbook normally deals with only one country. It deals with two or more countries in separate parts, especially when these countries are closely associated with each other by pact, geographically, or in some other way. As a minimum it contains--

- History, governmental, and political structure. A short history of the nation and a comprehensive description of its governmental and political structure.

- Armed forces organization. A description of the nation's military establishment (including paramilitary and an explanation of how C2 of the ground forces is affected).

- Ground forces organization. A complete explanation of the organization and composition of all the various types of ground force units and formations. The organization and composition of a nonground force unit also is included if that unit is likely to be placed under command or in support of the ground forces in time of war.

- Logistical support organization. An explanation of the logistical system the ground forces employs from ministerial level to the lowest echelon.

- Strategic and tactical doctrine. An explanation of the nation's strategic and tactical military doctrine, especially at combat levels of command.

- Reserve forces or mobilization. A description of reserve forces, the mobilization system and times required for mobilization.

In addition, the OB handbook includes--

- Military education and training. A description of the military education and training system and an explanation of the personnel recruitment and selection process.

- Uniforms and insignia. A full description of all armed forces uniforms, ranks, and insignia.

- Weapons and equipment. A listing and brief description including characteristics of the various types of weapons and equipment found in the ground forces. The list includes weapon and equipment's country of origin, availability of technical expertise, and likelihood of resupply of equipment and spares.

° Allies. A list of likely military and political allies, and type of support each may render.

The contents of the OB handbook are organized in the sequence shown above. When included, organizational and tabular data are presented as follows:

° Armed forces organization, governmental and political structure. Organizational charts are to support the narrative description of these subjects where possible. There is no format for such charts.

° Organizational structure. Depict organizational structure for each type of unit, Within NATO, the-symbols depicted in STANAG 2019 rapresent the various units, formations, or installations. Arrange the organizational diagrams in the following sequence: headquarters, combat units, CS units, service support units.

° Tables of personnel , weapons, and equipment. Produce the tables according to STANAG 2077. Figure 3-1 shows a sample equipment list.

Amend OB handbooks periodically. The timing and degree of amendment are left to the discretion of the originator. They should, however, initiate amendment action whenever you detect a substantial change to intelligence contained in the handbook or whenever you have a number of minor amendments.

INSTALLATION HANDBOOKS

Ideally, installation handbooks contain complete information concerning every military installation in every city in the county or Al. They are useful, particularly during peacetime, for establishing which forces are already in place. During wartime, the usefulness of installation handbooks decreases somewhat. However, they still indicate likely reserve mobilization and training centers. Two particularly useful handbooks are the Automated Installation Intelligence File (AlIF) and the Contingency Planning Facilities List (CPFL).

MISCELLANEOUS REFERENCES

Other publications and periodicals prepared at departmentl and area command levels are of value to the OB analyst. These references may deal specifically with 0B or with any or all phases of tactical, operational, and strategic intelligence. Specialized technical intelligence agencies provide detailed evaluations of equipment. The Soviet Battlefield Development Plan provides current and projected Soviet battlefield capabilities. The CIA produces studies on general mil itary capabilities, and economic factors which impact on military capabilities. Civilian organizations under contract to the Department of Defense (DOD) make special studies on various subjects concerning foreign and enemy military forces. These studies usually are detailed, technical in nature, and provide a wealth of special information not otherwise available.

NATO Serial No	Original or short NATO Title	Description	Remarks

Equipment lists are to conform to the format shown above. The sequence and numbering of equipment are to be established by Supreme Headquarters Allied Powers Europe (SHAPE) according to STANAG 2077.

Figure 3-1. Equipment list.

ORDER OF BATTLE RECORDS

The OB analyst uses various recording aids in organizing and cataloging OB information. The OB analyst creates OB records and files through a compilation of information available in the references discussed above. Subsequently, they are used continuously to produce current intelligence and to update other intelligence records, like the SITMAP and IPB products. OB files facilitate easy reference and comparison of OB information collected at various times from various sources. Each intelligence processing element decides which aids to maintain. The type used depends on the echelon of command and the local situation. Some common recording aids are:

- Unit workbook.
- OB workbook.
- OB SITMAP.
- OB card file.
- Personality file.
- Military installation file.
- Organizational worksheet.
- Strength worksheet.

Other file systems or forms are developed locally for special situations.

UNIT WORKBOOK

The format of the unit workbook depends upon the structure of the foreign army being monitored. Typically, it consists of a collection of OB cards supplemented by supporting documentation and is arranged by type of unit or in numerical sequence. Minimally this documentation includes organization and strength worksheets with the workbook being updated as new information is received. The enemy parent unit listed on the unit worksheet should agree with the analyst's level of command.

The analyst normally maintains records for enemy units one level above and two levels below the command's. In some special purpose units, three levels or more down are followed as well. Review information from units three levels down to develop identities on units two levels down. List personalities on the worksheet as a ready reference to the personalities of the enemy unit. Note and use unit, postal, and vehicle numbers on the worksheet to determine 0B changes or to confirm current data. Note details which may reveal any facet of the enemy unit's 0B or indicate the source of information in the remarks column. Enter reports of branch insignia, number and type of weapons, and statements of local residents in this column in abbreviated form. Include the data and the source of information for each entry. The installation column of the worksheet shows the numerical designation assigned to a particular enemy installation when plotted on a sketch, map sheet, or town plan attached to the workbook. For consistency and to facilitate exchange of information between headquarters, use installation numbers Previously assigned by theater or MACOM, Figure 3-2 shows a sample unit workbook. Figure 3-3 shows a sample page from the unit workbook.

ORDER OF BATTLE WORKBOOK

The OB workbook aids the analyst in sorting, evaluating, and interpreting information and in preparing intelligence reports.

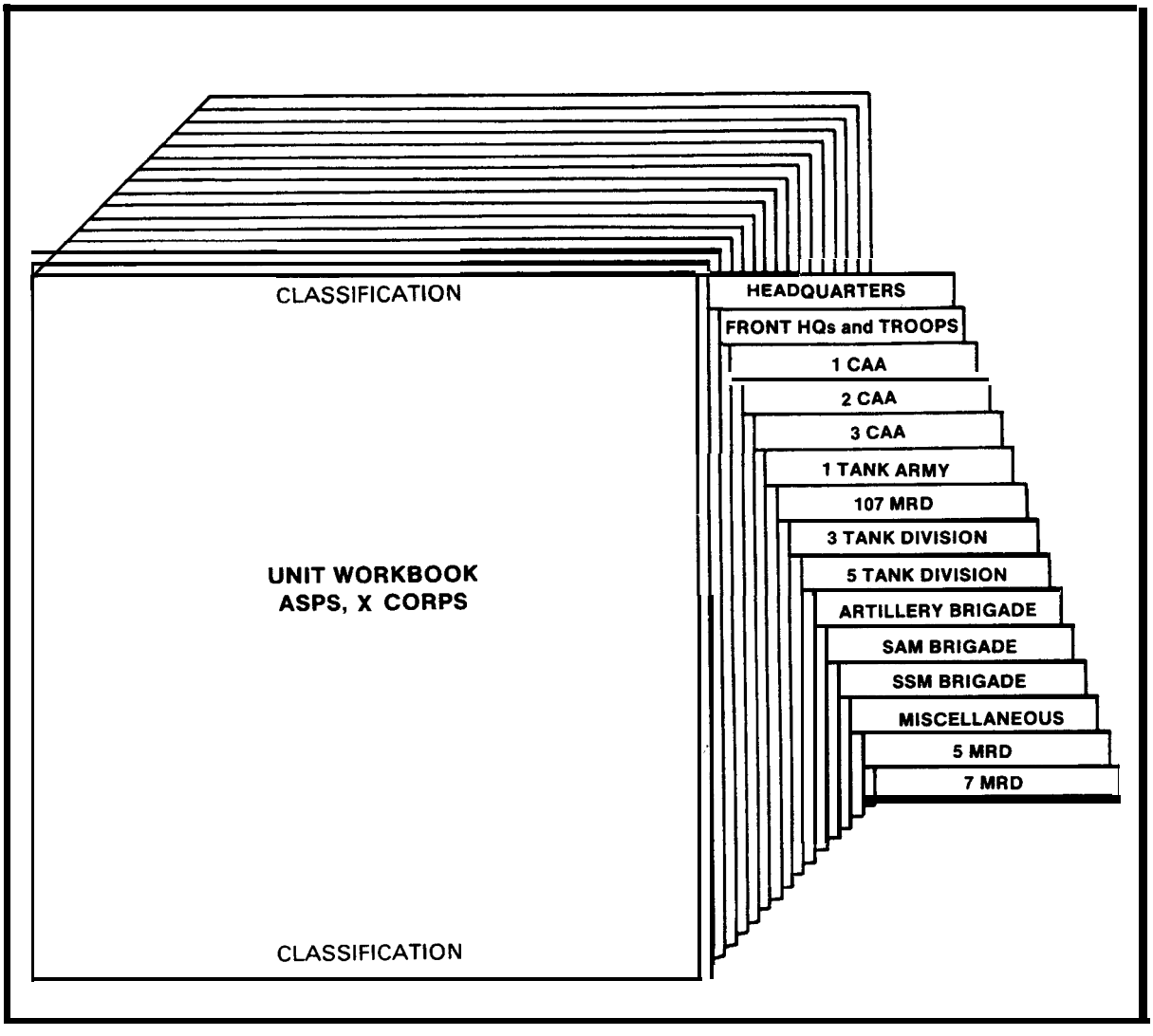


Figure 3-2. Sample unit workbook.

There is no prescribed format for the OB workbook. At corps level and higher, the OB workbook is tabbed to conform with paragraphs of the OB annex of the PERINTREP (see Appendix A). This makes it easier to extract needed information for the production of intelligence reports.

Information is entered under the appropriate haading or headings as either a complete report or a digest of the original report. All entries contain a journal date and number in addition to identification of the source. Comments added after each entry show the significance of tha report when compared with the overall tactical situation. Figure 3-4 showa how information is organized in an OB workbook.

Parent Unit _____

SUBORDINATE UNITS	CITY	COORDINATES	INSTL	PERSONALITIES	ID OR CODE NO	REMARKS
Div Hq	Stein	PV818147	1 and 3	Commander COL Crechin		EPW no 26, Captured 2 Feb 68
96 Mech Rifle Regt	Delitach	PU820934	4	Commander COL Kursheve	16181	Document Captured 19 Mar 68
145 Mech Rifle Regt	Ellenburg	PU852961	2	LTC Shrenko	16182	Deserter 21 Mar 68
3d Bn	Gladbach	PV891024	1			Gladbach residents rpt battalion subordinate to Hqs in Ellenburg, 3 Feb 68
43 Med Tk Regt	Linburg	PV863106	3	Commander COL Reshvic		Agent Report 26 May 68
358 Trans-Bn	Lehrt	PV825158	1		16195	OB Bank

Figure 3-3. Sample page from unit workbook.

ORDER OF BATTLE S I TUAT 10N MAP

The 06 SITMAP is a graphic portrayal of current threat OB, either confirmed or unconfirmed. It shows identification and disposition of the opposing units and any other information which will assist in developing the threat 06.

As a general rule, threat units one echelon above and two echelons below the analyst's own level of command are plotted by using the appropriate symbols in FM 101-5-1. For example, division plots maneuver regiments and battalions; corps plots maneuver divisions and regiments. Plot higher units to tha extent practicable. The foregoing information is only a guide. Analysts at theater level who are responsible for publication of OB books may plot separata battalions. Peculiarities of unit organization, the tactical situation, and time and personnel available within the analysis section determines more precisely what is plotted and what is omitted on OB maps. Enter the time and date of the information to the left of each symbol or plot. During counterinsurgency operations, however, it may be necessary to plot guerilla or insurgent units down to the squad level, since, depending on the situation and the

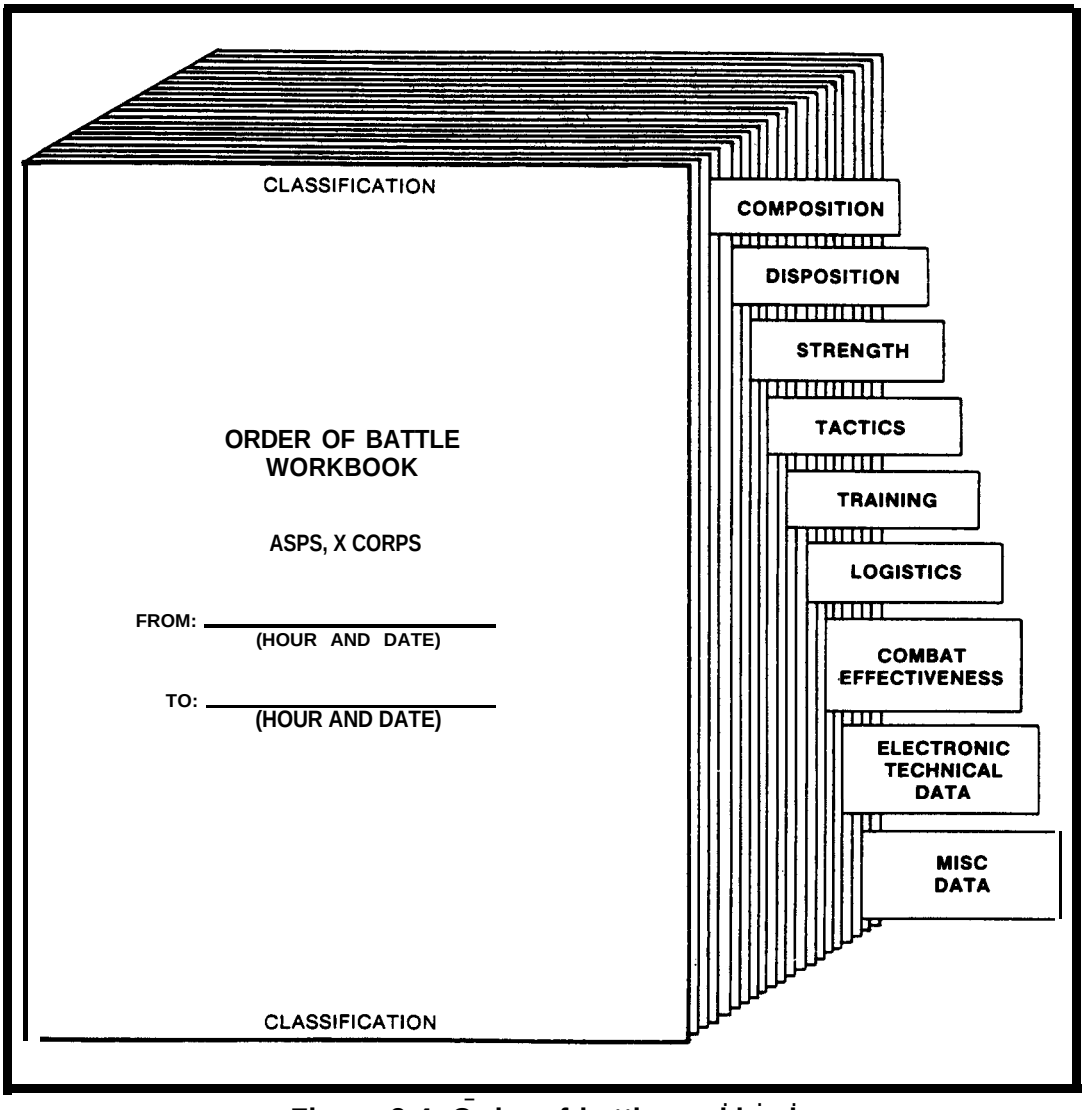
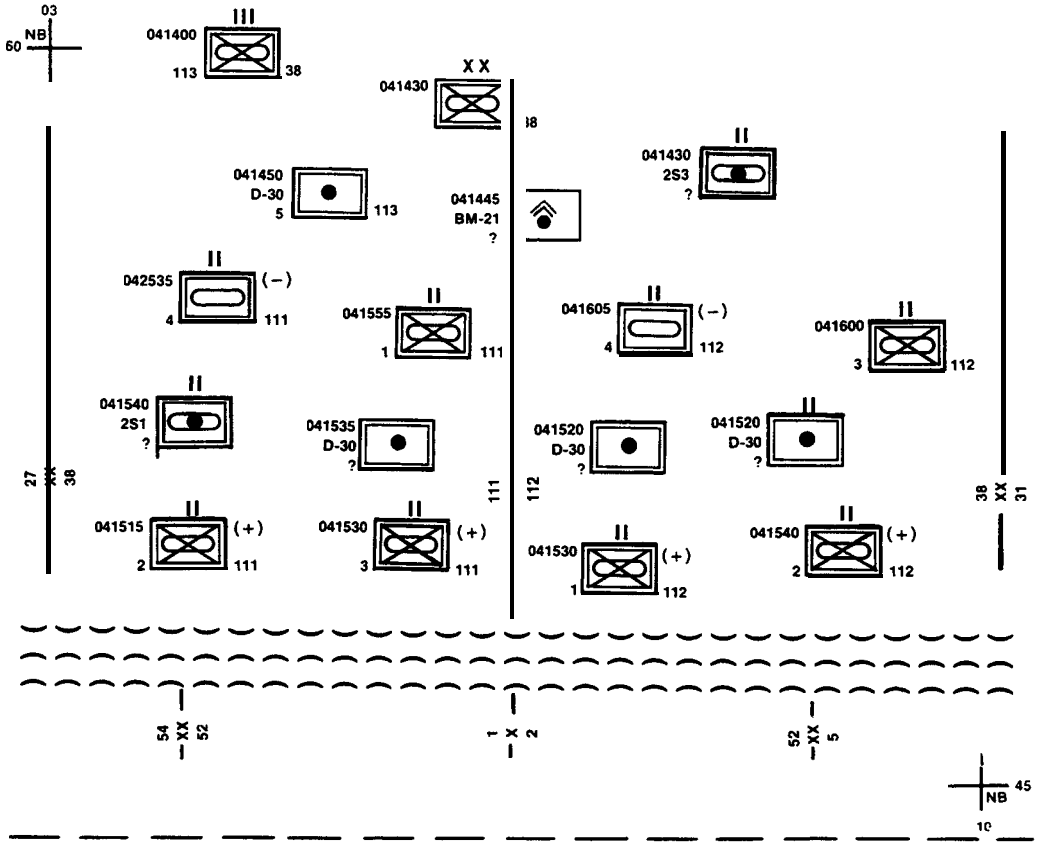


Figure 3-4. Order of battle workbook.

area, there may be no larger units operating against friendly forces. Figure 3-5 shows the OB SITMAP. The OB SITMAP contains the same types of information as the working SITMAP (described in Chapter 2), except it is kept in a less cluttered state so it is better integrated with G3 or S3 operational maps and for briefing purposes. At battalion and brigade levels, S2 and BICC officers often do not keep separate working and briefing OB SITMAPS.

Prepare the OB SITMAP as an overlay. Like other overlays, the OB SITMAP contains titling data. This data includes:

- Overlay title.



Located Units (by type)			Unlocated Units
Committed Forces			
Unit	**No.**	**Wpn**	Recon Bn, 38th GMRD 114th Tk Rqt, 38th GMRD UI Ind Tk Bn, 38th GMRD SSM Bn, 38th GMRD
MRB	6		
TB	2	80 T-64	
Reinforcement			
MMR	1		
TR	1	94 T-64	
ITB	1	51 T-64	
Fire Support			
SSM Bn	1	SS-21	
Arty Bn	8	18xBM-21 MRL 18x152mm SP How 72x122mm How 36x122mm SP How	

Figure 3-5. Order of battle situation map with caption box.

- Map sheet name.
- Map sheet number.
- Map series.
- Map scale.
- Prepared by _____.

A caption box on the OB SITMAP is an annotation containing information which helps to identify and explain the OB situation graphics. Although any number of caption boxes are used, normally three types are necessary: strength, unlocated units, and legend.

The entries in the strength caption box usually consist of strength computations in numbers of personnel, types of units, and weapons and equipment categorized as committed forces, FS, and available reinforcements. Reconnaissance elements which are part of an opposing maneuver unit are considered as reinforcements, if uncommitted. Assumptions like these are made to portray probable enemy capabilities.

The OB analyst must be aware of what is not known about the enemy. The unlocated units caption box lists existing unlocated units. These units pose a threat to the accomplishment of the friendly mission, and maximum effort must be directed toward establishing the disposition of unlocated units in the AO.

When it becomes necessary to improvise symbols for enemy units, include a legend caption box on the OB SITMAP. Within this caption box, explain the exact meaning of each, improvised symbol.

ORDER OF BATTLE CARD

The analyst uses OB cards to maintain complete and accurate data on enemy units. The format of the card is standardized within NATO to facilitate the exchange of information and intelligence among allied forces. The standard recording system (whether manual or automated) is based on a card entitled "'Order of Battle Card."' Such cards are maintained in wartime, at all levels including division and lower when directed by higher headquarters or when desired. Normally, keep one card for each enemy regiment and independent battalion within a friendly unit's AI.

Information on the OB card includes--

- Identification (numerical designation, type of unit, and nationality).
- FPN.
- Subordination (parent unit).

- Subordinate formations or units.
- Location (place name and UTM coordinates).
- Table of major equipment (including war establishment and current effective strength).
- Combat effectiveness and category (where applicable).

The OB card contains the following optional information:

- Code name (offical name assigned by the enemy for convenience or as a cover) .
- Honorific title.
- Nickname (unofficial popular name).
- Insignia.
- Commander.
- Unit history.
- Signature equipment (including significant quantities).
- Turret numbers, vehicle registration numbers or other tactical identification signs.
- Miscellaneous.

Record validity dates and source references on the back of the card. Also record information subject to frequent changes on the back of the card. This includes--

- Unit locations.
- Strength.
- Combat effectiveness.

Figure 3-6 shows the front and back sides of the 08 card.

PERSONALITY FILE

A personality file records personality data on designated categories of individuals. The development of the personality file is probably one of the most difficult analytic functions, particularly for the personnel in Threat units at division level and below.' However, much information is available through open-source I iterature and intelligence information reports (IIRs). This file provides reference material used in the development of other OB intelligence. Information on key military figures

(Front)

BASIC COMPOSITION OVERALL LIST

1. Tactical Symbol	2. Formation or Unit	3. Superior Formation or Unit	4. Nickname	5. Insignia or Personnel Equipment
◇	125 GTR	369 MRD	URAL - KURSK DIVISION	

6. Initial Strength	7. Code Number	8. Code name	9. Location	10. FP Number
85 %				10169

11. Coordinates (UTM)	12. Commander	13. Nationality, Formations or Unit	14. Effective Strength (%)	15. Combat Effectiveness
32 U PB 123456	LTC VASILY YAKOV	UR	80 - 85 %	

Consecutive Number	Subordinate Units	Location	Coordinates (UTM)	Installation	FP Number (Date)	Code Name or Code Number	Commander	Initial Strength	Effective Strength
a.	b.	c.	d.	e.	f.	g.	h.	i.	j.
01	1 GTB		PB 123456				UNK		
02	2 GTB		PB 125498				MAJ ROMANOV		
03	3 GTB		PB 118441				UNK		

History:

Miscellaneous:

Figure 3-6. Order of battle cards.

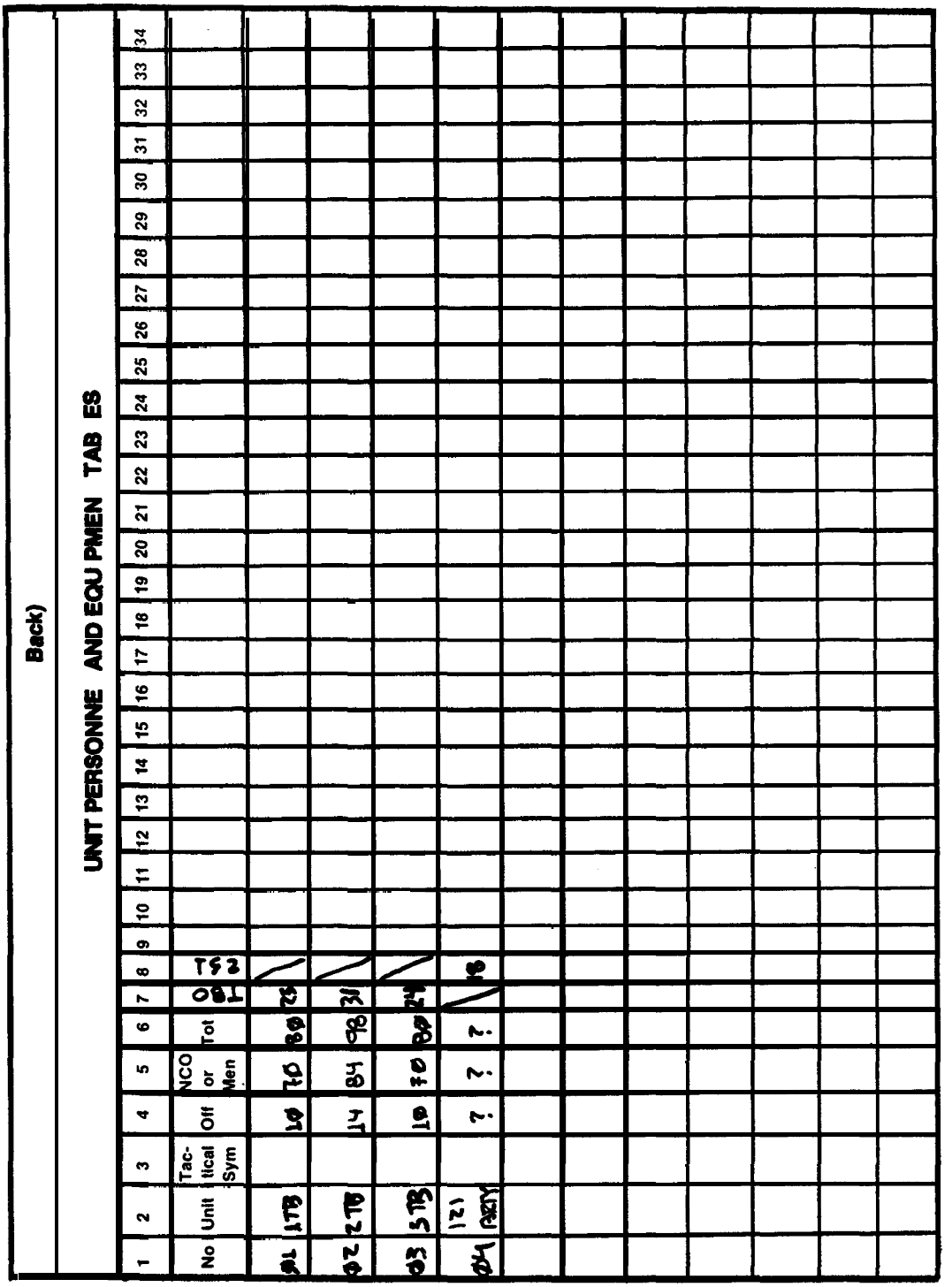


Figure 3-6. Order of baffle cards (continued).

is of significant value in the establishment of unit identification, tactics, and combat effectiveness. Keep the file in alphabetical order.

The card (or sheet) contains information concerning the individual's name, rank, current assignment, date and place of birth, civilian education, political affiliation, nicknames, and physical peculiarities. The file also contains the individual's schools, qualifications, awards, decorations, chronology of assignments, campaigns, engagements, demonstrated performance in leadership assignments, and important activities participated in, as well as character traits I ike morals, reputation, appearance, and mannerisms, published articles (which may identify areas of concentration and expertise), and cliques with which the individual is associated (may indicate influences and upward mobility prospects). Each entry records the source and date of the information.

The personality file also includes information which aids the friendly commander, G2, and G3 in deception planning and operations. This includes habits that make the opposing comrnander and staff vulnerable to deception, the most likely deception targets, the degree of freedom the cormmander allows subordinates, how the commander reacts to new situations, and how the fear of the unknown influences the commander's actions. Figure 3-7 shows a suggested format for biographies used in personality files required by STANAG 2077. Similar files may be maintained for key staff officers and other categories of key personnel.

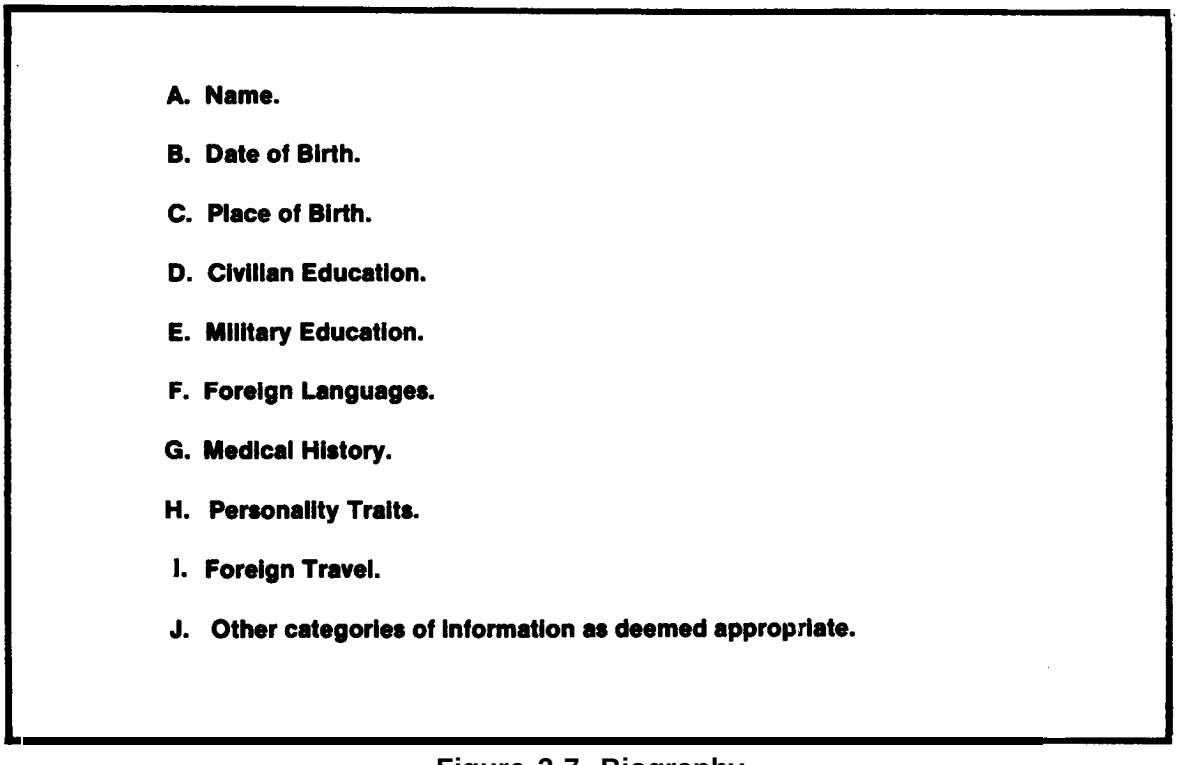


Figure 3-7. Biography.

MILITARY INSTALLATION FILE

During peace time, higher echelons maintain military installation files normally to facilitate publication of installation handbooks. A collation or explanatory sheet contains all information that has bean collected on each installation to include the number and types of buildings and their capacities, personnel uniforms and insignia, and major items of unit equipment. Maps, town plans, or sketches showing the location of each installation within the city supplement this file. Figure 3-8 shows a sample military installation file.

ORGANIZATIONAL WORKSHEET

The organizational worksheet provides a convenient method of showing types of units within an armed force. Organizational worksheets depict the complete breakdown of all units from the highest type headquarters to the lowest unit, including personnel and major wsapon strengths. Since this is rarely possible on a single sheet of paper, prepare a chart showing the general organization of the major unit and individual charts for each of its subordinate units. Prepare principal weapons and equipment charts to supplement organizational charts. Figure 3-9 shows a sample MRR organizational worksheet.

STRENGTH WORKSHEET

Use the strength worksheet to maintain a running numerical tabulation of the enemy's personnel and equipmant strengths. This information is recorded on committed units, FS units, and reinforcements. Figure 3-10 shows a sample strength worksheet.

COORDINATE REGISTER

When personnel and time are available, the brigade and battalion BICCs maintain a coordinate register. The coordinate register provides the lower echelon intelligence officer with a workable counterpart to the extensive intelligence files and workbooks that are maintained at higher echelons. It graphically illustrates the situation over a small geographical area. It is compact enough to be carried with ease for ready access.

The register is usually a looseleaf notebook. Each page represents a single grid square on the operational map which covers the geographical AO and AI. This geographical area should include the enemy area, friendly area, and areas of concern on both flanks.

The coordinate register contains two types of pages. One type is for written entries which describe enemy activities, locations, weapons, and similar items. The DTG and map coordinates precede these entries. The S2 adds personal comments or notations to any entry. Figure 3-11 shows a coordinate register page with written entries.

TOWN HEIMERZHEIM COORD 330LB 5220

INSTL	LOCATION	DESCRIPTION	USE	CAPACITY	STRENGTH	UNIT	TIME LAST INFO	EVAL	REMARKS
	523208 (201-4th St)	5 Story, red brick bldg Flagpole extends from 5th story window	UI HQ	400	Unk	Unk	0758	B-2	Many high ranking officers and official sedans observed.
2	522211 (Hwy 2 between K and L Sts	4 x 2-story, wood barracks Surrounded by 8' board fence	Trps	500	350?	Engr?	0758	C-2	Sentry observed wearing engineer insignia.
3	531215	6 x 4-story, red brick barracks with 2-story bldg	Trps		850	Unidentified Army	0458	B-2	Sentry observed wearing art insignia. Known to local residents as Kaiser Bks.
4	533218 (N of Instl 3)	8 x 1-story garage-type bldg	Gun park				0458	B-2	Probably belongs to unit in Instl 3.9 x 100mm guns observed
5	514231	2 x 3-story, stucco bldg	Trps	Bn	Bn	1st Bn 19th MRR	1257	A-1	
6	535211	Local tng area, obstacle course in NW corner	--- ---	--- ---			0458	B-2	Believe used by trps from both Instl 2 and 3
7	554205	Several underground bunkers enclosed by 8' barbed wire fence. Guard towers. located on each corner.	Ammo dump	10 Tons (est)			1257	F-6	

Figure 3-8. Military installation file.

	PERSONNEL	TANKS	ARTILLERY		ADA			AT		SMALL ARMS	
			122mm SP How	120mm Mort	SA-9	SA-7	ZSU 23-4	ATGM	ATGL	AGS 17	LMG
Regt HQ	65					3					
3XMRB *	1290			18		27			99	18	108
Tk Bn	165	40							2		
SP How Bn	220		18						18		18
AA Missile Artillery Bn	60				4		4				
AT Missile Btry	40							9	9		
Recon Co	55								4		3
Engr Co	60								4		
Sig Co	50										
Cml Def Co	35										
Mtr Transport Co	70										
Maint Co	70								4		
Medical Co	25										
Supply and Service Plt	20										
TOTAL	2225	40	18	18	4	30	4	9	140	18	129

*** Strength and equipment figures are cumulative.**

Figure 3-9. Organization worksheet motorized rifle regiment.

111th Guards Motorized Rifle Equipment

Category	Personnel		Tanks		Artillery						APC or IFVs		Remarks
Type			T-64		122mm How (2S1)		152mm How(2S1)		120mm Mort		BMP-1		
1. Committed Forces	Full Str	Losses	Full Str	Losses	Full Str	Losses	Full Str	Losses	Full Str	Losses			
1st MRB(-)	430	50	13						6				
2nd MRB(-)	430	35	13						6				
2. Reinforcements													
3rd MRB	430	10							6				
4th TB(-)	165	10	14										
3. Fire Support													
Arty Bn or 111 GMRR					18								
							18						
Totals		105	40	11	18	3	18	0	18	3			

Note: Additional columns and rows may be added to encompass additional unit or weapons systems.

Figure 3-10. Strength worksheet (sample).

GRID SQUARE 32U NA2815				
ITEM	LOCAL TIME	COORD	STATEMENT	NOTES
1	092235	28381539	MG fires on recon plt from A Co.	Have next plt check this area.
2	092318	?	Veh noise - Tk? - Heard direct N of A Co OP 2 28321507.	Ask air OP to look
3	100600		Special OB report on wpns and fortifications.	Div wants more info on wpns strength.
		280215323 to 28141527	Trenches and bunkers.	
		281415227 to 28221529	Wire.	
		28611545 to 28781551	Platoon on line has 2 MG's.	Same MG as yesterday? Check this!
		28811551 to 29001599	Extensive trenches and firing PSNS.	
4	102335	28391530 to 28691541	B Co plt rpts wire and AP mines.	New since 081800.
5	110600	28431588	Res unit (co?) in general area.	(From Div PIR).
6	110630	28381557	Med tk spotted by L plane.	How many more?
7	111320	28731584 and 28151564	Active mortars.	
8	120010	28611564	Flash from small cal arty not over 75.	AT? AA? Gun? RR or bazooka? Ask higher HQ.

Figure 3-11. Coordinate register with written entries.

The second type schematically represents a single grid square. Entries are plotted on the square in the same manner used to plot the enemy S I TMAP. This page shows graphically any data applicable to a single grid square. Figure 3-12 shows how an enlarged grid square is drawn and entries are made.

The coordinate register is used to--

- Determine enemy dispositions and routes of movement.
- Predict enemy intentions and main effort.
- Plan reconnaissance and surveillance (R&S) operations.
- Brief and debrief patrols.

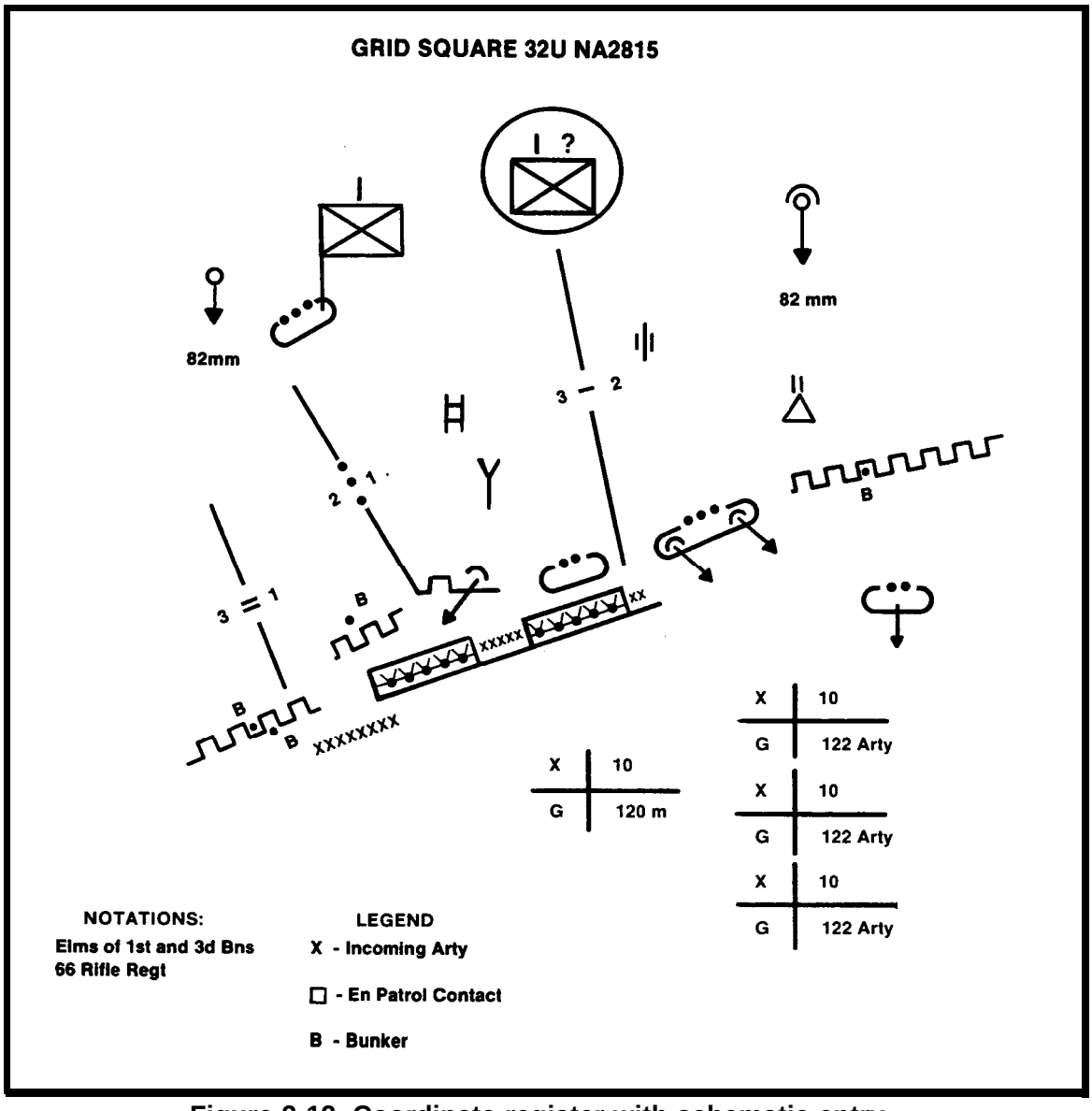


Figure 3-12. Coordinate register with schematic entry.

- Plans FS.
- Brief the commander and staff.
- Assist in IPB.
- Reveal enemy perceptions of how the terrain will support maneuver against them.

Data from the coordinate register is plotted on a vertical aerial photograph that has been annotated with grid lines. A scale of 1:25,000

or larger is desirable. By plotting selected OB information on the photo, an analysis of the terrain is conducted simultaneously with a correlation of information on the enemy. The photo provides an excellent means of briefing commanders down to platoon level on the AO and the enemy situation. Targeting is accomplished in a more precise manner by using a photo instead of the traditional 1:50,000 map. While not common in mid- to high-intentsity conflict these photos are especially useful in LIC.

The coordinate register is reviewed when the unit moves to a new area, when new data is added, and when obsolete data is deleted. Timely maintenance of the coordinate register is not practical in fast-moving high-intensity situations like pursuit, delay, and exploitation. The coordinate register would, however, be very valuable in a relatively static situation or in a low-intensity conflict (LIC).

Whenever possible, maintain the register on strong semitransparent bond paper. The transparency of bond paper is sufficient to allow the use of a grid scale underneath the schematic page. This allows a more accurate and rapid plotting of, or reference to, the entries.

The scale of the schematic page normally is a matter of SOP. Such standardization assists in dissemination of intelligence data from higher to lower echelons. For security reasons, the friendly situation normally is not plotted in the coordinate register.

ENEMY COMBAT EFFECTIVENESS

A number of factors, some tangible, others not, determines the combat effectiveness of enemy units. Of these factors, only the personnel and equipment strength lend themselves to factual analysis, and only major items of equipment, like tanks, armored personnel carriers (APCs), and artillery weapons lend themselves to detailed quantifiable analysis. This is because personnel strength fluctuations are extremely difficult to assess accurately. Appendix D describes procedures for computing personnel and equipment strength. The following states the combat effectiveness of a unit:

> "The 133 MRR is estimated to be at 80 percent effective strength. Evidence of low morale suggests that the unit is less combat effective than the estimated effective strength may indicate."

ARBITRARY UNIT DESIGNATORS

The identification, by title, of a particular unit or formation on the battlefield is difficult during war. Although it is argued that such precise identification is not important and that one enemy division is as much of a threat as another, this ignores the problems of collation, dangers of double counting, and confusion. To deal with this problem, NATO and national formations apply a unique arbitrary unit designator (AUD) to unidentified enemy formations.

There are two types of unidentified enemy formations:

- Formations which are well known except for their actual title.

- Formations seen on the battlefield whose history, background, and title are unknown.

SHAPE allocates the AUDs. They appear in NATO and national OB summaries in peacetime in the columns normally filled by unit title. Use these AUDs in war also.

The AUDS consist of a prefix, a number, and a suffix.

The prefix consists of a three-digit alphanumeric distinguishing code that indicates the number and nationality of the corps that originates the AUD. The following are examples:

- The 1st British Corps uses lUK.

- The 2d German Corps uses 2GE.

- The 7th US Corps uses 7US.

A two-letter distinguishing code indicating the NATO formation and allocating the AUD is an optional method of establishing prefixes. Figure 3-13 shows these AUD prefixes.

Each national corps allocates blocks of numbers between 000 and 999 to their own headquarters and subordinate formations. Similarly, divisions may, if they wish, suballocate numbers to their subordinate formations. All formations of a corps and corps headquarters, however, use the same prefix.

After the prefix and number is a suffix indicating--

- The nationality of the enemy formation.

- The type of formation.

Do not change the actual numbers allocated by a particular national or NATO formation normally unless an unidentified enemy is recognized separately by two formations, each of which allocates its own AUD. Under such circumstances, the relevant superior headquarters, having agreed that an unidentified enemy formation is present, will either--

- Accept one of the already allotted AUDs, but replace the prefix with its own.

- Allocate a new AUD.

In either case, inform both of the originating formations.

As an example of an unidentified enemy with two allotted AUDs, a division of the 2d German Corps and a division of the 1st British Corps separately detect the presence of an unidentified Soviet MRD in the area

SHAPE	SH
AFNORTH	AN
COMNON	NN
COMSONOR	SN
COMBALTAP	BA
COMLANDJUT	JA
COMZEALAND	ZE
AFCENT	AC
NORTHAG	NG
CENTAG	CG
AFSOUTH	AS
LANDSOUTH	LS
LANDSOUTHEAST	SE
AMF(L)	AM

Figure 3-13. Arbitrary unit designator.

of the intercorps boundary and each gives it an AUD using the block of numbers al located to them by their own corps (2GE369 UR MRD and 1UK473 UR MRD, respectively). Each corps adopts the AUD allocated by its division.

The corps HQ knows from which division the AUD originated by the number appl ied. HQ NORTHAG agrees that an UI UR MRD is present and decides to retain the German (GE) number but allocates it a NORTHAG prefix. From then on, until positively identified or changed by Allied Forces, Central Europe (AFCENT), or SHAPE, the unidentified formation is known as NG369 UR MRD. If for some reason it is changed by AFCENT or SHAPE, apply an AFCENT or SHAPE prefix.

CHAPTER 4

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

IPB is a tool to aid the commander and staff in determining where and when to use limited resources to achieve decisive results. IPB applies to all phases of the AirLand Battlefield; close-in, deep, and rear operations synchronization are all supported by the IPB process.

For planning the close-in phase of the operations, IPB provides a guide for the initial allocation and employment of combat power. Through event templating, it is possible to identify where the enemy probably will thrust if attacking, or where the enemy will concentrate forces if defending. Through terrain and weather analysis and templating techniques, it is possible to determine where friendly forces can best move, shoot , and communicate, and where to place friendly strength against enemy weakness. During tactical operations, IPB supports the use of fire and maneuver to achieve a tactical advantage. Event templating facilitates following enemy forces and determining their probable course of action. Decision support templates (DSTs) enable the commander to apply combat power in a timely manner.

IPB is especially useful as a tool for planning and fighting the deep operations. Through threat evaluation, enemy critical nodes and HVTS are identified readily. Event templating determines the optimum time and place to interdict the enemy to achieve maximum delay, disruption, destruction, and when and where to achieve decisive exploitation of identified weakness. it facilitates the identification and location of deep targets in time to strike them at the optimum time and place in a manner which constrains and causes the collapse of close-in enemy actions. AirLand Battle concepts were introduced in Chapter 1 of this manual, and an application of IPB and collection in deep operations and maneuver plans is further explained in FM 34-130.

When planning rear operations, IPB allows the commander to efficiently focus friendly efforts. Capacity and trafficability of supply routes are identified. Avenues for the commitment of reserves become apparent, as do the choke points which the enemy will attempt to target. The analyst studies drop zones (DZs) and landing zones (LZs) and the air approaches to them, and provides the commander information about the rear area threat. The most advantageous locations for support areas can also be found. All of this permits the commander to use friendly forces in the most economical method possible, which frees assets for the close-in and deep operations.

IPB is an essential part of staff planning. Initially, the G2 uses it to develop intelligence about the enemy, weather, and terrain that the commander and staff need to complete their planning. The analysis of the AO and the intelligence estimate primarily embody this intelligence. While IPB does not replace these documents totally, use it as an aid to their development. It aleo converts much of the written material into

graphics which are understood easily, analyzed, and appl ied to the planning process.

The intelligence estimate is a key to the decisionmaking process. Through IPB, the estimate is presented in a graphic format. This enables the commander and staff to see, rather than visualize mentally, where both friendly and enemy forces can move, shoot, and communicate. It provides a graphic data base for comparing friendly and enemy courses of action. Weather and terrain overlays tell us not only where the enemy moves, shoots , and communicates but where friendly units accomplish these functions as well. Just as the G2 uses templating to determine enemy courses of action, the G3 uses templating techniques to compare friendly courses of action.

IPB helps the G2 determine--

- Where to look.
- When to look.
- What to look for.
- What to look with.
- What to expect to see.

IPB helps the G3 determine--

- Where to maneuver, shoot, jam, and communicate.
- When to maneuver, shoot, jam, and communicate.
- What friendly resources to maneuver, shoot, jam, and Communicate with.
- What enemy assets to maneuver, shoot, and jam.
- What results to expect.

IPB is vital to the commander's estimate and tactical decisions regarding the concept of the operation because it produces an accurate comparison of friendly and enemy capabilities and courses of action. It enables the commander to see friendly and enemy vulnerabilities and opportunities and to determine where, when, and how to support forces to ensure success.

Successful preparation and application of IPB products depend on the intelligence analyst's ability. The intel l igence analyst must know both enemy and friendly maneuver doctrine; must understand what a mission statement involves; and must focus efforts to support the mission. To provide the commander with the intelligence required to make a high quality decision, the analyst must also coordinate extensively with other staff sections. These include the G3 or S3, the FSE, AD, engineers,

battlefield deception elements, and USAF weather teams. Other sections, such as the G5 and G4 or S4 become involved in rear area IPB. Each of these sections and others have data which are vital to IPB. Each of these sections also has requirements which are filled by IPB. Use of this manual and FM 34-130 helps the analyst succeed in supporting the commander effectively.

IPB influences every stage of an operation and is continuous. It begins with a staff estimate process, which involves interaction from all the staff sections.. Because battlefield conditions and tactical situations change, IPB must be dynamic. The products which result from IPB are often perishable, and must be updated to remain val id. Figure 4-1 shows how the staff sections interact during the IPB process. Chapter 4 of FM 101-5 describes in detail why IPB is conducted prior to an operation.

Conducting IPB and knowing how to apply its products, are two different processes. This chapter explains how the intelligence analyst utilizes IPB to assist the commander and staff in the successful planning and execution of AirLand Battle. A more detailed description of the IPB process is available in FM 34-130.

PURPOSE OF INTELLIGENCE PREPARATION OF THE BATTLEFIELD

The key to effective IPB application centers around the G2 or S2 staff understanding what can be accomplished with it. Much time and effort is expended without purpose if IPB is conducted in a vacuum.

The analyst's objective when applying the IPB process is to reduce battlefield uncertainties as they relate to terrain, weather, and enemy. During the IPB process, the graphics produced aid the commander and staff in planning and synchronizing more effective operations. IPB focuses the S2's intell igence collection effort where it is most effective. IPB also assists the commander in the decision-making process. For a detailed description of how IPB assists in decision making read Chapter 4, FM 101-5. IPB helps the commander control the battle by describing what the enemy's most likely course of action is, including when and where it will occur and how the enemy's follow-on forces affect the battle.

In situation and target development, the IPB product shows the commander when to most effectively attack enemy forces by fire and maneuver and when to seize the initiative. Using the IPB graphics, the intell igence analyst can identify and prepare the attack of HPTs as they move onto the battlefield. This reduces the effectiveness of the enemy's forces, causing them to be disrupted and delayed, and presenting further targets for maneuver or FS missions. In threat integration of IPB, the analyst uses analysis models to forecast events on the battlefield.

The IPB process, if applied properly and with purpose, contributes immeasurably to mission accomplishment. However, as with any predictive instrument, IPB will never achieve 100 percent accuracy.

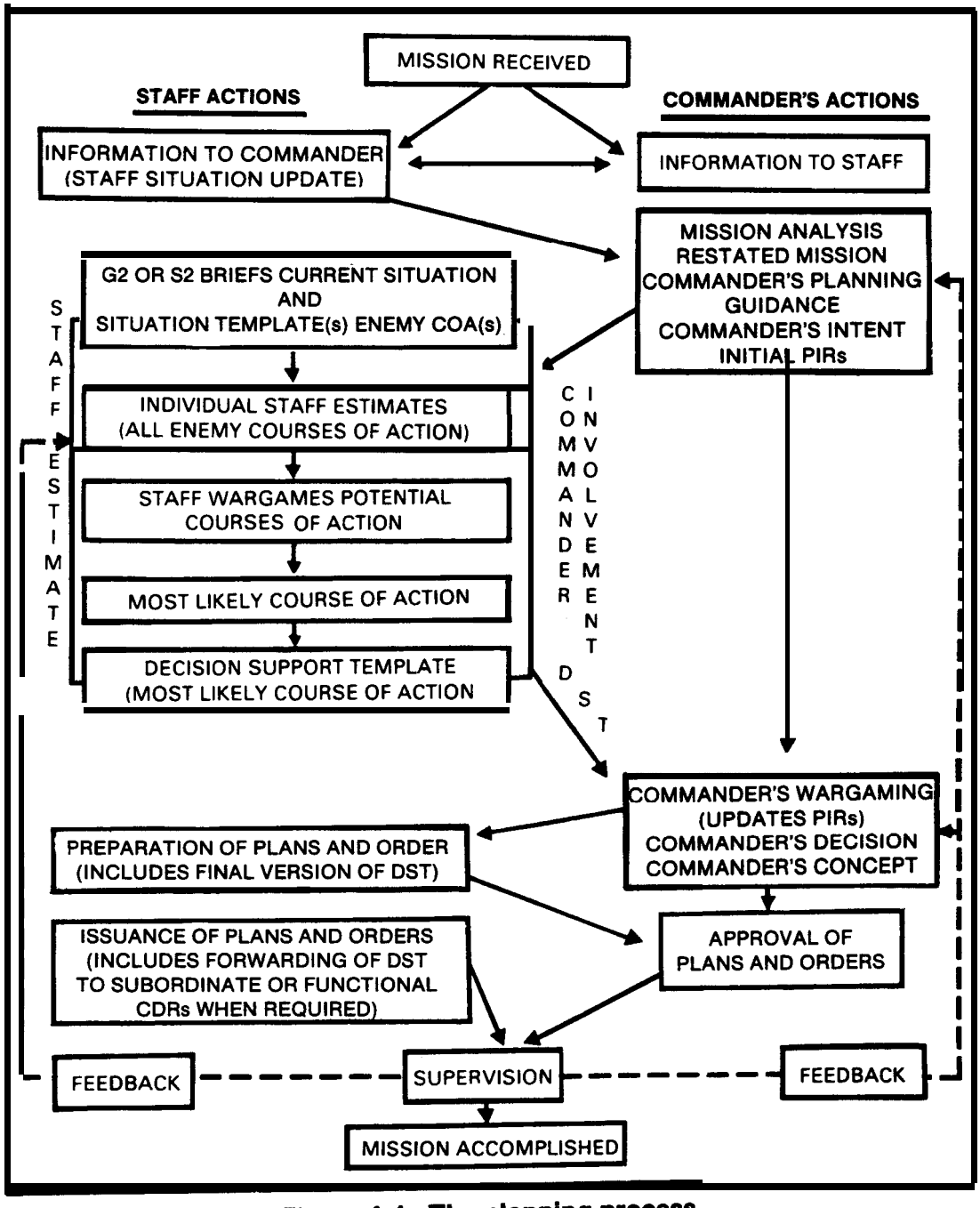


Figure 4-1. The planning process.

DEVELOPMENT AND USE OF INTELLIGENCE PREPARATION OF THE BATTLEFIELD PRODUCTS

Graphics are basic to IPB analysis. Often intelligence is communicated best with pictures. The analysis of the battlefield and the intelligence estimate are not replaced, but merely assisted by graphics. These graphics become the basis for intelligence and operational planning. Currency is maintained through graphic renewal or update. Right now most aspects of IPB analysis are prepared manually. Preparing graphics by hand is slow and time-consuming. Properly prepared, graphics are relatively simple and inexpensive to maintain. The benefits of graphic analysis and display of intelligence are worth the initial investment of time and resources. It is therefore incumbent upon the G2 or S2 to make maximum use of available time and personnel to produce those graphics which are most beneficial to the commander. Particularly at brigade and battalion level, all personnel must be capable of conducting the IPB process. Additionally G2s or S2s at each echelon should provide subordinate unit S2s as many IPB products as possible. This saves time and permits the subordinate level S2 to expand on higher level IPB products or produce others unique to the unit mission.

The graphics produced during the IPB process have numerous purposes and functions. A good analyst knows what to accomplish from each. Terrain and weather factor overlays, for example, help depict the effects of terrain and weather on potential friendly and enemy courses of action.

Further on in the IPB process, analysts produce four templates--doctrinal, situation, event. and decision support. Figure 4-2 gives the description and purpose of each template. These templates help the analyst to deduce and analyze enemy capabilities, predict their most likely courses of action, identify information gaps, and determine TAIs. In other words, the graphics produced during the IPB process help in conducting analysis.

APPLICATION OF INTELLIGENCE PREPARATION OF THE BATTLEFIELD

The IPB process begins with the mission. Upon receipt of a mission, the commander analyzes the situation and has the staff present a situation update. From this initial information, the commander conducts mission analysis and restates the mission. The commander then sets the staff planning process in motion by providing planning guidance and intent. The commander also determines initial PIRs.

Using the commander's guidance, the staff begins to prepare their estimates. The IPB process primarily takes place during the estimate process.

The intelligence analyst considers the amount of available time and the number of soldiers on staff who can conduct IPB. Giving due consideration to resources, the analyst initiates the IPB process with the intent to produce sufficient graphic products to assist the commander and staff in their planning.

As a minimum, the analyst prepares a modified combined obstacle overlay (MCOO), a situation template depicting how the enemy looks at the most critical moment on the battlefield, an event template from which to develop the R&S plan, and a DST.

The G2 or S2 applies IPB to assist the analytical process and accomplish as much of the process as possible to support the commander in what little time is available. Time is the analyst's greatest enemy as there is never enough of it. If there is time for only one situation template, the analyst prepares the one most critical to the commander's mission. This is why it is so important for the G2 or S2 staff to understand the commander's intent. Time spent initially providing guidance and establishing specific tasks for each member of the G2 or S2 staff who conducts IPB, goes a long way towards a more complete IPB product which contributes to the commander's successful mission accomplishment.

TEMPLATE	DESCRIPTION	PURPOSE	WHEN PREPARED
Doctrinal	Enemy doctrinal deployment for various types of operations without constraints imposed by the weather and terrain. Composition, formations, frontages, depths, equipment numbers and ratios, and HVTs are types of information displayed.	Provides the basis for integrating enemy doctrine with terrain and weather data.	Threat Evaluation
Situation	Depicts how the enemy might deploy and operate within the constraints imposed by the weather and terrain.	Used to identify critical enemy activities and locations. Provides a basis for situation and target development and HVT analysis.	Threat Integration
Event	Depicts locations where critical events and activities are expected to occur and where critical targets will appear.	Used to predict time-related events within critical areas. Provides a basis for collection operations, predicting enemy intentions, and locating and tracking HVT.	Threat Integration
Decision Support	Depicts decision points and target areas of interest keyed to significant events and activities. The intelligence estimate in graphic form.	Used to provide a guide as to when tactical decisions are required relative to battlefield event.	Threat Integration

Figure 4-2. Intelligence preparation of the battlefield templates.

BATTLEFIELD AREA EVALUATION

Battlefield area evaluation (BAE) as the first step in the IPB process sets the stage for the rest of the process.

During the conduct of BAE, the intelligence analyst studies the battlefield area to focus the IPB effort. The analyst studies the battlefield to obtain a general feel for how terrain and weather affect operations. The AO has been provided.

Delineation of the AI is done to direct a portion of the collection effort (with support from higher headquarters) against enemy forces which can directly influence the unit's mission. The G2 and G3 or S2 and S3 determine the AI based on how much time the commander needs to react to a threat. For example, if the enemy has the potential to enter the battalion AO via one of the flanks, and the battalion reserve needs two hours to move to most areas on the flanks, then based on an enemy doctrinal advance rate of 6 kilometers per hour (kph), the analyst would probably extend the AI on the flanks to at least 12 kilometers (kms). The analyst must understand the mission, the commander's intent, and both friendly and enemy capabilities.

METT-T and the commander's concept of the operation determine the AI. Once the AI is established, the analyst informs higher command of the area it covers so they can assist in collection.

During the BAE phase the analyst studies the battlefield to determine significant areas and considerations to be studied in more depth during the remaining IPB phases.

Terrain Analysis

The intelligence analyst has one primary objective when conducting terrain analysis -- to reduce the commander's battlefield uncertainties as they relate to terrain. Terrain analysis emphasizes the use of graphics to portray the effects of terrain on operations.

The G2 or S2 depicts via graphic products--

- Terrain which impedes or hinders maneuver and mobility.
- Terrain which does not restrict maneuver and mobility.
- Avenues of approach (AAs) and mobility corridors (MCs).

The lower the level at which the analyst works, the less time the analyst may have to prepare terrain factor overlays. The analyst must prepare those overlays which support the commander's mission and intent. This requires the G2 or S2 to prioritize and set time lines as to what the analyst should accomplish.

Modified Combined Obstacle Overlays

The intelligence analyst prepares a MCOO. This overlay is a combination of various overlays or if done as one overlay, then simply is a graphic representation of what should be highlighted about the terrain. It is based on OCOKA (observation and fields of fire (FofF), concealment and cover, obstacles, key terrain, and AA and MCs).

Terrain analysis at division level and higher benefits from engineer terrain teams or detachments attached to G2 staffs assisting in terrain analysis. Time constraints may not permit receipt of engineer terrain products by brigade and battalion S2s. The intelligence staff must train in the conduct of terrain analysis to be capable of producing their own terrain graphics. Appendix E of this manual, Terrain Analysis in IPB, provides the analyst basic guidelines for conducting terrain analysis. For a detailed description of how to conduct terrain analysis refer to FM 34-130.

Terrain analysis focuses on the military aspects of terrain known as OCOKA. Chapter 4 of FM 34-130 provides a detailed description of OCOKA.

The following guidelines are important to the analyst when applying OCOKA.

Observation and Fields of Fire. Observation involves the type of units (both friendly and enemy) which are on the ground. The analyst asks questions such as:

- To what degree does vegetation or relief obscure tha observation of friendly or enemy units?

- How will the ground unit be observed from the air?

The analyst focuses on the time of attack or expected tima of enemy penetration into the main battle area (MBA). Also the analyst considers what night observation devices both forces possess. These factors impact on the conduct of the battle.

Another important factor is how the friendly force looks from the enemy's perspective. This principal applies to all other OCOKA factors as well. The distinction is made clear to the commander by providing details versus generalities.

Observation also influences the capability for R&S and TA. In the IPB context, this refers to optical and electronic line of sight (LOS). Many battlefield systems require LOS to function effectively. These include radios, radar, intercept and direction finders, jammers, direct fire weapons, human vision, and binoculars.

Air defense (AD) TA and weapons require LOS from their positions to air targets. The analyst considers the anticipated flight altitude relative to the elevation of adjacent terrain.

The effects of terrain and weather on these systems influence the commander's view of the battlefield. What is important for the analyst to consider when studying the terrain is to study it based on the battlefield systems available to the commander and the threat. Again, because time is limited, the analyst prioritizes those battlefield systems most critical to the mission.

LOS overlays graphically illustrate the effects of terrain on friendly and enemy observation and FofF. The horizontal visibility or FofF overlay combines the LOS effects of vegetation and elevation features. The relative capabilities of direct fire weapons, communications, and collection and TA systems become apparent. This overlay assists in identifying key terrain with greater precision. Figure 4-3 shows horizontal LOS FofFs. This is the type of overlay that the engineer terrain team prepares at division or higher. If assigned to brigade or battalion level, the analyst requests this overlay for the AI.

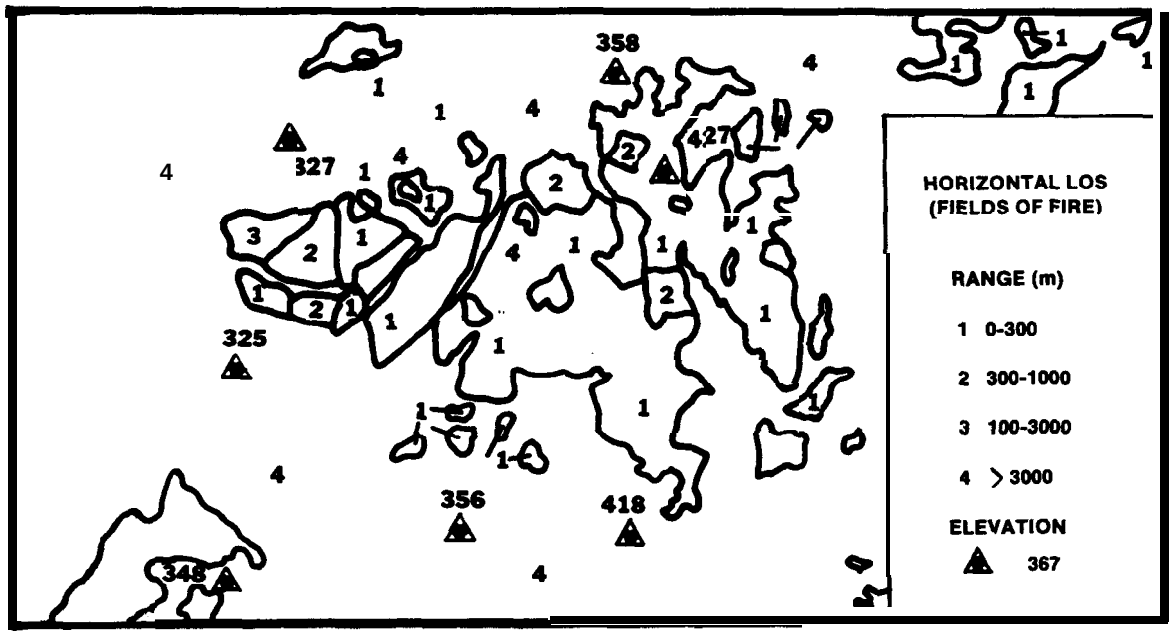


Figure 4-3. Horizontal LOS fields of fire.

Concealment and Cover. Concealment is protection from observation or surveillance. Cover is shelter or protection from fire either natural or artificial. The analyst discerns the difference between concealment and cover . The two are not combined when examining the terrain for their effects. The analyst examines concealment to distinguish it from ground and aerial observation.

The analyst decides the type forces which concealment may or may not impact; for example, concealment may be good for soldiers on foot, yet poor if riding in tracked vehicles.

The analyst addresses cover from direct and indirect fires. The analyst identifies (particularly important at battalion level) points within the AO where concealment and cover are critical to successful mission accomplishment.

Obstacles. Obstacles, whether artificial or natural, are very important considerations in the conduct of terrain analysis. Obstacles significantly impact on a force's ability to maneuver or move rapidly through an area. The analyst should not assume that an obstacle for friendly force units is an obstacle for threat units also. The wise analyst examines obstacles separately from the point of view of both enemy and friendly force units and acknowledges that obstacles are different and impact differently depending on the type of battlefield operating system that is used.

Key Terrain. Key terrain is any point or area on the ground whose control or seizure provides an important tactical advantage. Any terrain which increases a unit's abil ity to apply combat power or decreases the opponent's abil ity to apply theirs is considered key terrain.

Decisive terrain is that terrain which, if not controlled or if controlled by the opponent, significantly degrades the commander's ability to successfully accomplish the mission. For example: The Fulda River in West Germany, and in particular the crossing sites on it, is considered decisive terrain for US forces defending against Threat forces approaching from the east. On the other hand, the Harm River, 6 km east of the Fulda River, while it is considered key terrain for a unit in the defense, probably is not considered decisive terrain because--

- The Harm River hinders enemy movement across it (particularly if covered by fire); but it does not prevent movement because it is narrower and easier to cross than the Fulda.

- It is not an obstacle to movement because it is narrower and much easier to cross.

Avenues of Approach and Mobility Corridors. AAs are routes by which a force reaches key terrain or an objective. AAs are evaluated in the following terms:

- Maneuver support potential .

- Access to key terrain and adjacent AAs.

- Degree of canalization.

- Concealment and cover.

- Observation and FofF.

- Obstacles.

MCS are subsets of AAs. MCS are areas within the AA which permit movement and maneuver. They permit friendly and enemy forces to advance or withdraw in doctrinal configuration, and to capital ize on the principles of mass, momentum, shock, and speed.

The intelligence officer or analyst should not get caught up on whether a piece of terrain is an MC. It is important that the analyst identify, based on knowledge of friendly and enemy assets, routes which either force will most likely use. Later in IPB, the analyst focuses collection resources on them.

When determining AAs and MCs, the analyst uses the one-up, two-down rule. The analyst determines AAs for enemy forces one echelon above and MCS for forces two echelons below the level of command conducting the analysis.

In determining AAs and MCS, the analyst keeps in mind the type force for which they are developed, the unit mission, and the potential enemy force mission. If an air threat exists the analyst develops air AAs. If time is short, the analyst seeks assistance from higher commands. The analyst may even involve the unit air defense artillery (ADA) officer.

The analyst carries the AA through the enemy's immediate and subsequent objectives. When on the offense, the analyst identifies potential enemy counterattack AAs and if possible AAs within the AO for friendly force units. The analyst also identifies MCS for friendly units. In determining friendly AAs and MCS the one-down, two-down rule applies; that is, the analyst identifies potential AAs for subordinate elements one echelon below the command conducting the analysis and MCS for subordinate elements two levels below. The battalion S2, for example, identifies company size AAs and platoon size MCS.

TERRAIN DATA BASE DEVELOPMENT

The analyst compares terrain product requirements with the terrain data base to identify gaps. In addition to standard topographic maps covering the AI, the following sources are helpful:

- Current intelligence estimate and analysis of the AO from higher headquarters.
- Special terrain studies and products prepared by US or host-country agencies, special maps, charts, and geodetic studies.
- Current photography.
- Actual terrain reconnaissance.

TERRAIN FACTOR MATRIX DEVELOPMENT

The terrain factor matrix provides a guide for terrain analysis. The matrix develops from an analysis process whereby terrain factors are

identified and correlated with specific types of combat operations and battlefield functions. The terrain factor matrix assists the intelligence analyst in identifying the types of terrain products needed. Figure 4-4 shows the terrain factor matrix.

COMBINED OBSTACLE OVERLAY DEVELOPMENT

When the terrain factor overlays are stacked and registered, the uncolored portion represents areas in which a force moves unimpeded. Also highlighted are areas which facilitate a maneuver element's ability to shoot and communicate. The overlays show significant terrain features that are further developed in the analysis process. Through graphic terrain factor analysis, the terrain team and the S2 section focus on terrain areas that are significant for further analysis.

	FACTORS							
FUNCTIONS	Surface Configuration (Slope)	Surface Materials (Soils)	Vegetation	Weather Effects On Terrain	Transportation	Obstacle (Linear)	Built-up Areas	Surface Drainage—(Hydrology)
Observation and Fields of Fire	X	X	X	X	X		X	
Concealment and Cover	X		X		X		X	
Assembly Areas	X	X	X	X	X		X	
Key Terrain	X		X	X	X		X	
Ground Avenues Of Approach	X	X	X	X	X	X	X	X
Air Avenues of Approach	X		X	X	X	X	X	X
Weapon Sites	X	X	X	X	X	X	X	X
DZ and LZ	X	X	X	X	X	X	X	X
Maneuver	X	X	X	X	X	X	X	X
LOC and MSR				X	X	X	X	
Barriers and Fortifications	X	X	X	X	X	X	X	X
Line of Sight	X		X		X	X	X	X
Communication Sites	X	X	X	X	X	X	X	
EW Sites	X	X	X	X	X	X	X	

Figure 4-4. Terrain factor matrix.

The combined obstacle overlay incorporates all pertinent terrain factors which assist the analyst in identifying mobility areas and deducing trafficability rates for AA analysis.

Figure 4-5 is an example of a combined obstacle overlay. The overlay is particularly important because it integrates al 1 obstacles into one graphic display. This greatly simplifies further analysis of AAs and MCS. Crosshatching indicates the obstacles and the blank areas indicate freedom of movement.

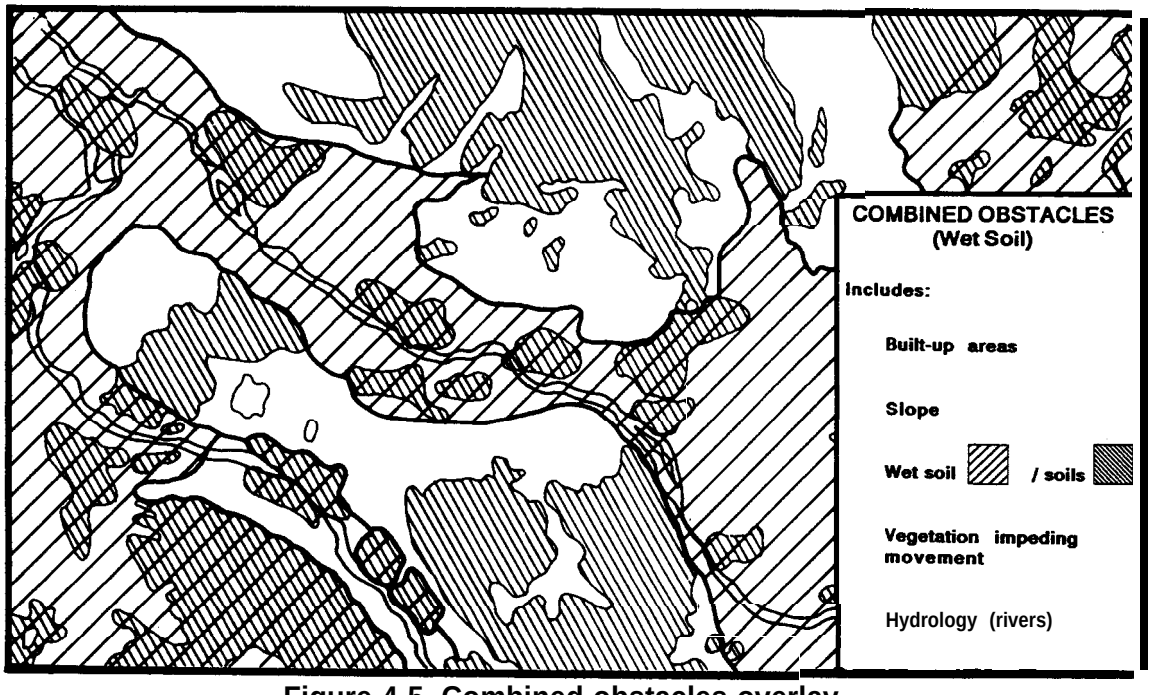


Figure 4-5. Combined obstacles overlay.

The effects of weather on mobility should not be ignored Through the cooperative efforts of terrain and weather teams, weather eff ects are integrated with the terrain analysis. As a result, the comb ned obstacles overlay reflects average weather-induced terrain conditions. Excessive precipitation affects soil density, slope, river stage, and visibility.

Cloud cover (CC) prolongs the drying period. Normal SLOW-GO traffic conditions may convert to NO-GO conditions which impact on both friendly and enemy force movements. The intelligence analyst prepares combined obstacles overlays that reflect at least normal weather effects on mobility. Based on a review of historic weather patterns, the analyst associates specific weather factors with specific time periods.

Figures 4-6 through 4-8 show--

° Obstacles with dry soil.

- Obstacles created by wet soil.
- Combined obstacles w ith wet soil.

The combined obstacles overlay provides a basis for identifying AAs and MCs. Having determined where the enemy cannot move without difficulty, the analyst focuses attention on those areas where the opposing force can move. Figure 4-9 shows normal requirements for identifying AAs and MCS.

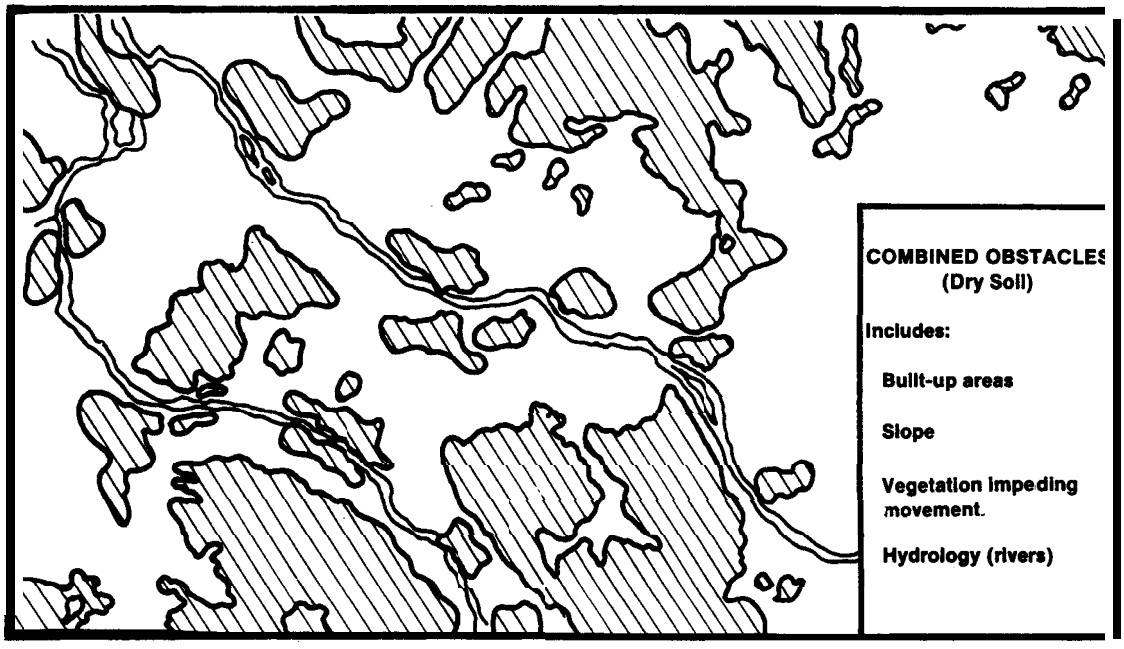


Figure 4-6. Obstacles with dry soil.

The combined obstacles overlay usually reveals one or more MC. Since regiments normally advance along separate MCS, each division AA should contain regimental MCS. The start point of an attack begins at enemy assembly areas and terminates at their objective.

A convenient technique for identifying AAs is to place a doctrinal template over a potential AA and visualize the enemy force moving through. Ask: Is there sufficient maneuver space? How does the enemy look while approaching critical points on the battlefield, such as the FEBA? How does the enemy look when considering attrition? An enemy force fighting through a covering force takes losses. To the attrition add the fact that the enemy has a narrower front when attempting a breakthrough. The analyst uses this information to depict a more realistic AA. When briefing on the AAs, the S2 or analyst must "talk" the commander through a visualization of the enemy force fighting along the AA. Figure 4-10 shows what the commander needs to see.

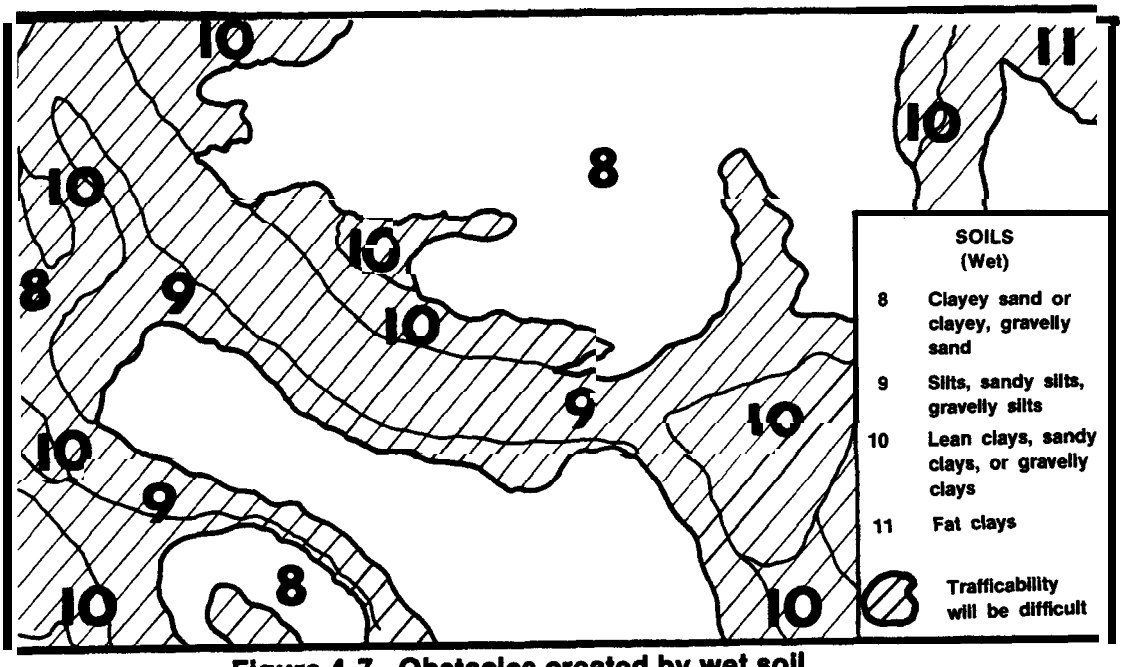


Figure 4-7. Obstacles created by wet soil.

The analyst moves the template along the avenue from projected enemy assembly areas to the objective. An AA is never completely free of obstacles. but it provides for relatively free movament. Obstacles generally parallel the direction of movement.

The analyst selects alternative AAs. If they partially overlap, the analyst should not be concerned. The most direct route to the objective normally is a viable option.

LINE OF SIGHT ANALYSIS

In terrain and weather analysis, the terrain team determines LOS for weapons, communications, TA, intelligence collection, and R&S systems. Direct fire weapon systems like the antitank guided missile (ATGM), the self-propel led antiaircraft gun, and the tank need good FofF to successfully engage the enemy forces at maximum range. FM radio communications, forward observers, TA and surveillance radar systems, and SIGINT need optical or electronic LOS to the target. Terrain and weather factor overlays assist in analyzing LOS limitations. LOS analysis helps determine where ground forces can best shoot and communicate and the most likely low altitude air approaches into the AO. In LOS analysis, the analyst considers the following factors:

- Terrain elevation.

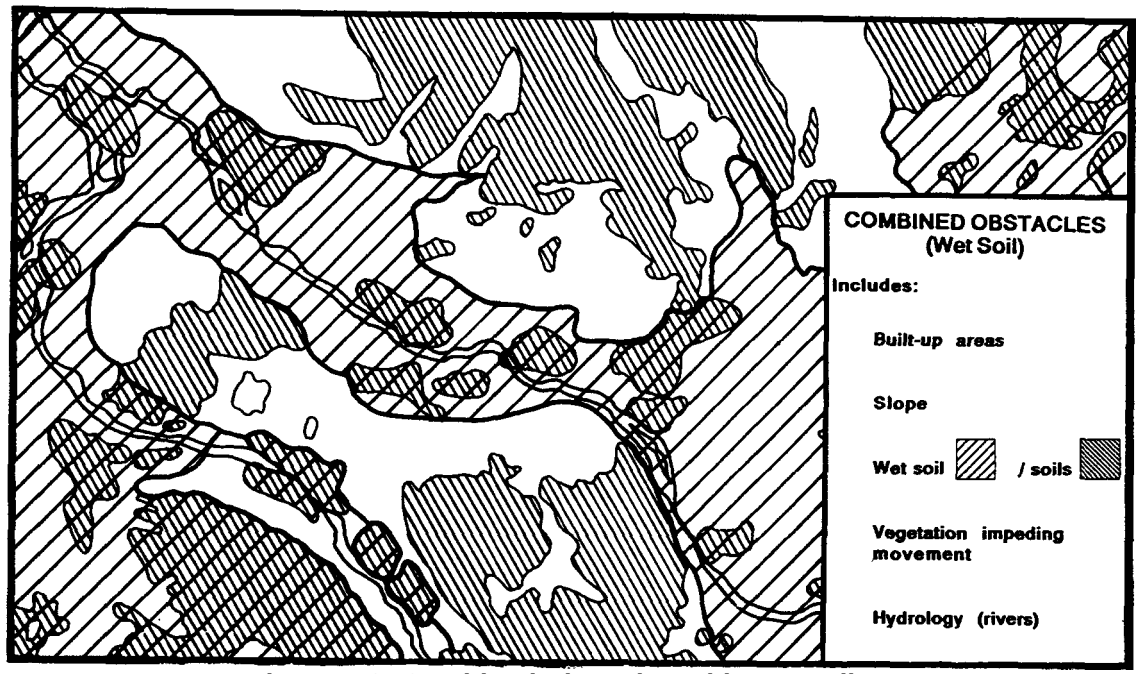


Figure 4-8. Combined obstacles with wet soil.

IF YOU ARE AT	AVENUES OF APPROACH	MOBILITY CORRIDORS
DIVISION	RECEIVE ARMY AA FROM PARENT CORPS DEVELOP DIV AA FOR SUBORDINATE BDE	RECEIVE REGT MC FROM PARENT CORPS DEVELOP BN MC FOR SUBORDINATE BDE
BRIGADE	RECEIVE DIV AA FROM PARENT DIV DEVELOP REGT AA FOR SUBORDINATE BNS	RECEIVE BN MC FROM DIV DEVELOP CO MC FOR SUBORDINATE BN
BATTALION	RECEIVE REGT AA FROM PARENT BDE	RECEIVE CO MC FROM BDE DEVELOP PLT MC

Figure 4-9. Avenues of approach and mobility corridors matrix.

- Tree and vegetation height above elevation.
- Height of built-up areas.
- Density of ground vegetation at full growth.
- Terrain factors, such as defiles, which are not apparent because of contour spacing.

- Effects of weather, such as fog or precipitation that obscure observation.

The effects of seasonal changes on LOS should be readily apparent. Winter vegetation compared to summer full growth alters LOS significantly. The limitations of the standard military map is overcome through imagery analysis (1A) and ground reconnaissance. Imagery analysts and terrain specialists are trained in LOS analysis.

Direct fire weapons systems require horizontal or ground LOS. As a rule, 4,000 meters (m) is considered the maximum range for unaided direct fire weapons. Horizontal LOS overlays also depict friendly LOS.

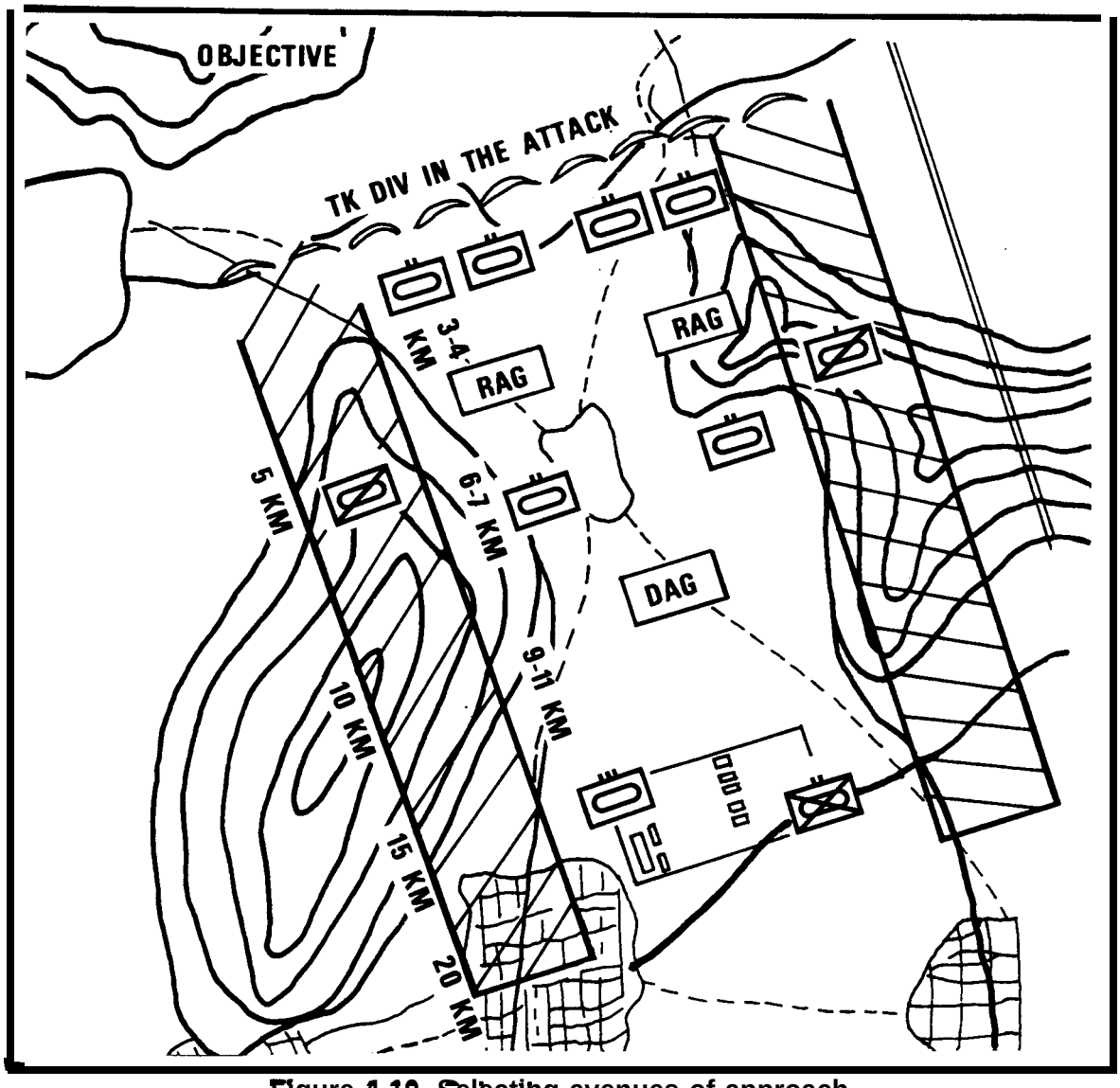


Figure 4-10. Selecting avenues of approach.

Figure 4-11 is a horizontal LOS overlay depicting FofF. Areas of maximum LOS are color-coded to aid analysis. Other range parameters are colored for easy identification. Heavily forested areas would not necessarily obscure LOS. Depending on the density of vegetation, LOS might penetrate 100 m or might penetrate 100 m or more of the forest. The height of ground vegetation and the seasonal density (taller than 1 m) might degrade LOS. This illustrates why an analyst must know the terrain of each battlefield system that is being analyzed.

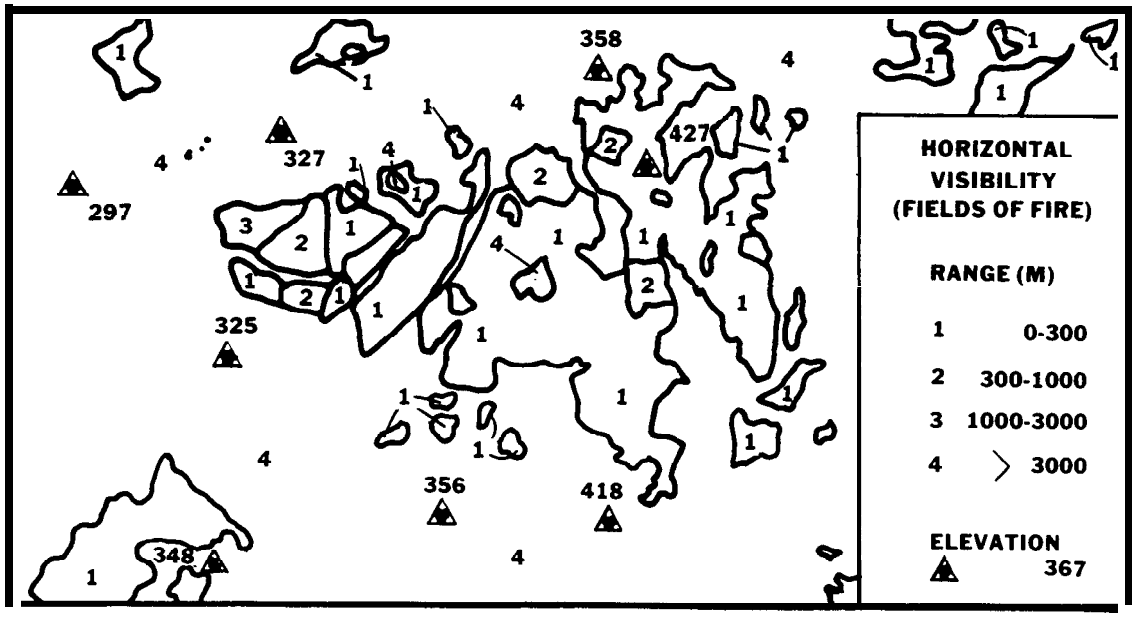


Figure 4-11. Horizontal visibility (fields of fire).

While ground-based systems need horizontal LOS, airborne systems use oblique or vertical LOS. An attack helicopter armed with machine guns and rockets rel ies on LOS from the aircraft to the target. Standoff weapon systems that pop up from behind masking terrain require accurate LOS and positioning data. Airborne R&S systems, such as the side-looking airborne radar (SLAR), have similar needs for LOS data. Analysis of vertical and oblique LOS from an enemy AD and target perspective helps identify the best air avenues of approach (AAAs) into enemy airspace.

Determining how terrain and weather conditions along each AA affects radio and other means of field communications is probably the area least considered by most analysts because of their general lack of knowledge of communications systems. The corps or division signal officer assists in determining the advantages and limitations of each AA to enemy communications systems. The SIGINT analyst also assists in this effort.

Most AAs do not offer unlimited options for the employment of communications and noncommunications systems. The intelligence analyst prepares a communication-noncommunication overlay of potential sites for

each MC. Having done this, the analyst compares each and makes some initial determinations as to which is most favorable. LOS information also is essential to electronic deception since this operation requires knowledge of where friendly signatures are observed. Figure 4-12 shows terrain masking and horizontal LOS.

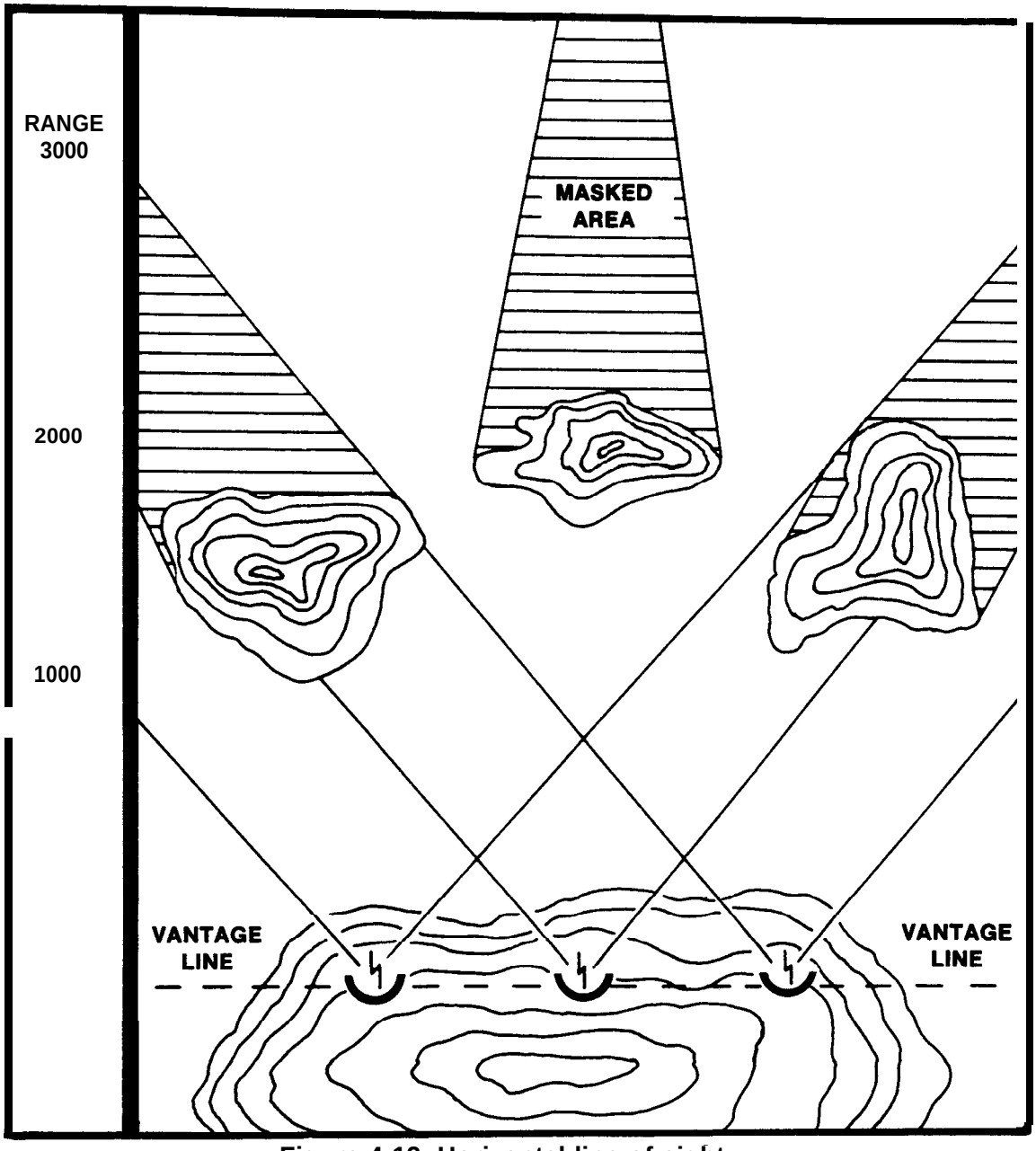


Figure 4-12. Horizontal line of sight.

AVENUES OF APPROACH ANALYSIS

In AA analysis, the intelligence analyst selects the AAs and AAAs that best support the capabilities to move, shoot, and communicate. The analyst considers each avenue in relation to each friendly or enemy capability, and then lists and compares the advantages and disadvantages of each. This is not merely a matter of counting advantages and disadvantages, but requires detai lad analysis and sound judgment.

This analysis is not to determine which AAs the enemy selects, but rather to determine which best supports the capability to move, shoot, and communicate. Figure 4-13 shows how an analyst depicts AAs on an overlay.

Once the most viable AAs are selected, the analyst prepares an overlay depicting each AA and MC. MCS are subsets of AAs and both are shown together. When weather is a consideration, the analyst prepares an overlay for each season.

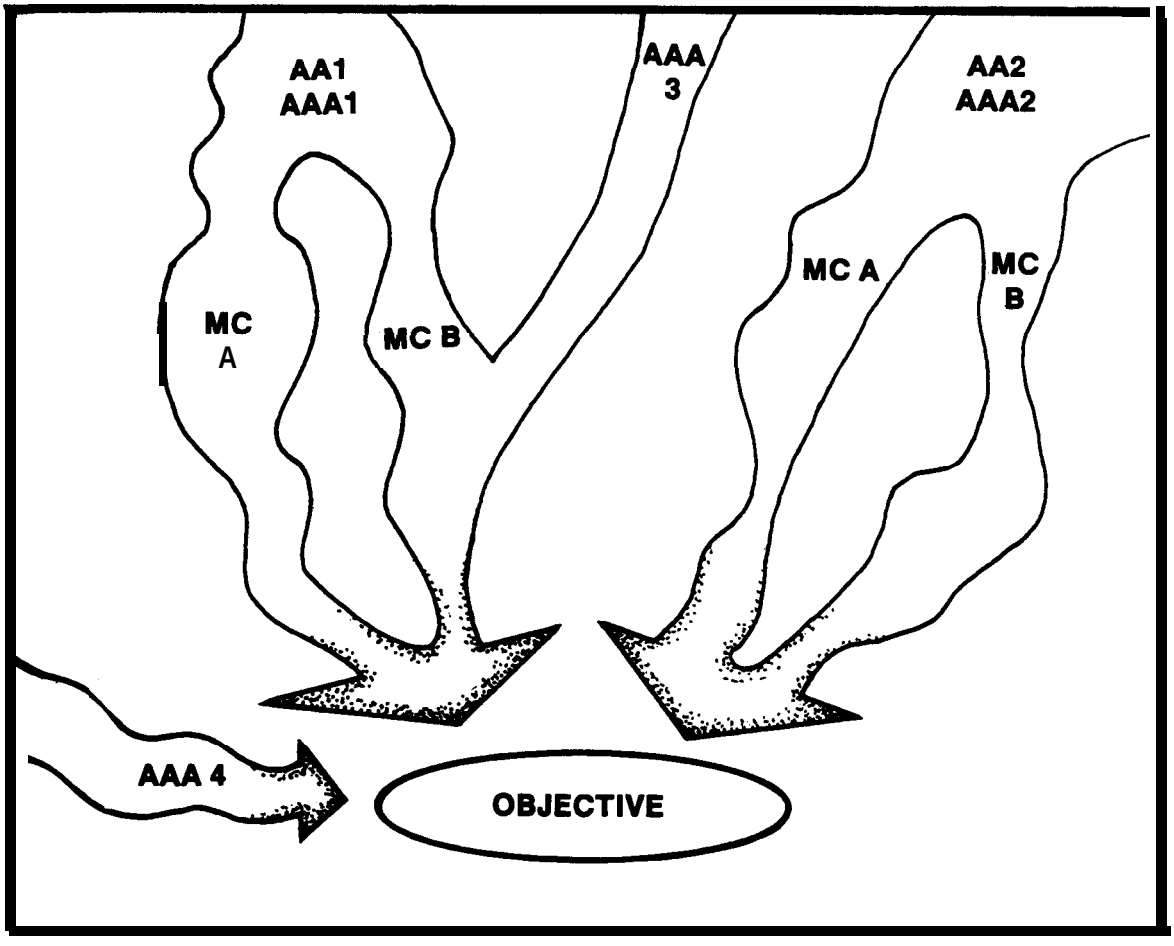


Figure 4-13. Avenues of approach.

APPLICATION OF WEATHER FACTORS OVERLAYS TO ANALYSIS

Similar to terrain analysis, the G2 or S2 produces graphic weather overlays to help facilitate analysis of weather effects on friendly and enemy battlefield operations.

The analyst prioritizes which military effects of weather generally have the greatest impact on the unit and threat force. Time does not allow the analyst to cover all aspects nor to depend solely on the weather teams. Prioritizing becomes critical when operating at battalion or brigade level because there is little time available.

The analyst focuses on each weather factor, examining its effects separately for both friendly and enemy forces. Using weather factor analysis, the analyst identifies specific vulnerabilities and significant benefits which contribute to the command's successful accomplishment of the mission.

The analyst should not generalize weather effects. The analyst should seek details which are useful. The best way to be successful at this is to track weather effects on unit operations during training exercises, catalog these for future reference, and discuss with subordinate commanders what critical weather effects are needed to operate successfully. By doing this, the weather analysis supports operations and the analyst maximizes what little time exists for other IPB requirements.

WEATHER ANALYSIS

Analyzing the climate and weather in the AO helps to determine their effects on friendly and enemy operations. Terrain and weather analysis are inseparable, because the tactical environment requires that climate. weather, and terrain information be considered concurrently. The products of weather analysis are applied in terrain and threat integration.

Weather has a significant impact on both friendly and enemy operations. The weather is analyzed in detail to determine how it affects both friendly and enemy capabilities to move, shoot, and commnunicate. A detailed discussion of weather analysis is found in Chapter 4, FM 34-130.

Weather factor overlays are integrated with the terrain overlays to predict the battlefield araas where friendly and enemy forces can maneuver.

The weather team analyzes climatic data to determine the characteristics of weather in the AO. The terrain team analyzes the effect of weather on tactical operations and, together, the teams integrate weather data and overlays with the terrain analysis and overlays.

The weather analysis team prepares a matrix to define the required analysis and specific weather requirements and determine which overlays are required to support the operation. The matrix isolates militarily significant weather factors and provides the capability to correlate

weather effects with specific combat operations. Examples of weather subfactor overlays produced by the weather analysis team include fog, cloud coverage (summer or winter), rain and snow, and weather effects on slopes. The overlays, along with the combined obstacle overlay, identify where forces maneuver on the battlefield.

At brigade and battalion level the S2 requests those IPB products which address weather effects for their AO from higher headquarters.

Commanders and staffs must understand and consider weather factors in tactical planning. They must recognize the tactical significance of weather effects and the risks or opportunities they present. While considering the effect of weather on all aspects of a mission, the S2 concentrates on weather impact on mobility and LOS. The effects of weather are integrated with the enemy and terrain through IPB; this integration is described in FM 34-81 and FM 34-130. A detailed description of weather effects is in the Weather Effects and Information Handbook (Draft) July 88, USAICS.

Low visibility is beneficial to offensive and retrograde operations and detrimental to defensive operations. In the offense, it conceals the concentration and maneuver of friendly forces, enhancing the possibility of achieving surprise. Low visibility hinders the defense because cohesion and control are difficult to achieve, R&S are impeded, and TA is less accurate. These disadvantages are offset partially by extensive use of illuminants, radar, sound detection, and IR devices. In some instances, using smoke and obscurant aerosols locally reduces visibility. When examining effects of visibility keep in mind friendly and enemy capabilities.

In all operations, restricted visibility prevents or limits the use of aerial systems. The analyst must explain how visibility affects aerial systems.

Wind speed and direction, both on the surface and aloft, usually favor the upwind force. Wind favors the use of either NBC or conventional weapons by the upwind force. Wind of sufficient speed reduces the combat effectiveness of the downwind force by blowing dust, smoke, sand, rain, or snow on personnel and equipment. The upwind force has better visibility and advances easier and faster. Strong winds limit airborne and aviation operations.

Strong surface winds and gusts cause injury to personnel (especially paratroopers in their descent), damage to materiel and structures, false radar returns, and restrictions on visibility by blowing sand, dust, and other materials. Generally, winds above 20 knots create such effects. Smoke operations generally are ineffective at wind speeds greater than 7 knots, As the surface wind increases at low temperatures, either naturally or enhanced by vehicle movement, windchill becomes a critical consideration. The windchill factor adversely affects improperly clothed personnel and impedes activity in unsheltered areas. Wind speed also affects the distance that sound travels. Winds are beneficial because

they improve trafficability by helping dry the soil. A windchill index is available in FM 34-81.

The primary significance of precipitation is its effect on the state of the ground, visibility, personnel effectiveness, and the functioning of some equipment. Ground status affects trafficability; heavy rain makes some unsurfaced roads and off-road areas impassible. Heavy rains make all roads in low-lying areas impassible. Both rain and snow drastically reduce personnel effectiveness by limiting visibility (causing discomfort, increasing fatigue, and creating other physical and psychological problems) and the persistence of chemical weapons thus creating NBC hot spots . Precipitation also adversely degrades the quality of some supplies in storage. Snow accumulation of one inch degrades trafficability and reduces the effectiveness of mines. Generally, more than one inch (2.54 centimeters (cm)) per hour or 2 inches (5.08 cm) in 12 hours of precipitation is considered critical for tactical operations. Snow fall exceeding 2 inches (5.08 cm) in 12 hours, 6 inches (about 15 cm) accumulated on the ground, or drifts of about 2 feet (.6 m) also have a significant effect on operations requiring mobility.

The type and amount of CC, as well as the height of cloud bases and tops, influence both friendly and enemy aviation operations. Extensive CC reduces the effectiveness of air support. This effect becomes more pronounced as CC increases, as cloud bases lower, and as conditions that are frequently associated with clouds, such as icing, turbulence, and poor visibility aloft increase. In relatively unstable air, clouds are associated with strong vertical currents, turbulence, and restricted visibility aloft. Generally, close air support (CAS) and aerial resupply operations require a ceiling of 1,000 feet (305 m) or more.

Clouds affect ground operations by limiting illumination and visibility, They also determine the types, intensities, and amounts of precipitation. Clouds, since they trap incoming heat from the sun and rising heat from the earth, tend to make temperatures near the earth more homogeneous. Temperature and humidity both affect air density. Air density decreases as the temperature or humidity increases; thus, efficiency of aircraft propulsion reduces in areas of high temperature or high humidity. Although temperature and humidity may not directly affect a particular tactical operation, extremes reduce personnel and equipment capabilities, and may necessitate a reduction of aircraft payloads.

Tactics that are effective in one climatic zone may be ineffective if used in another. The high temperatures and humidity found in the tropics are conducive to the growth of dense fol iage, which drastically affects operations. In arctic climates, cold weather periods--

- Create an almost constant need for heated shelters.
- Cause difficulty in constructing fortifications.
- Increase the dependence on logistic support.
- Necessitate special clothing, equipment, and combat skills.

A combination of temperature and wind speed produces a windchill factor . A windchill factor of -26°F (-32°C) is considered the critical value for personnel and equipment operating in cold weather, The opposite extreme, 120°F (49°C), is considered the critical value for personnel and equipment operating in hot weather, Similar restrictions occur in the desert where temperature difference of over 50°F (lO°C) occur between night and day in shelters without air conditioning or heaters.

At division and corps, updating the weather data base is continuous, particularly during periods of increased tension or combat. During these periods, the intelligence analyst compares current and forecasted weather with historic patterns to determine deviations. Updates are forwarded to subordinate commands.

The analyst uses the weather data base as the foundation for analyzing the effects of weather on combat operations. This analysis begins with an evaluation of the mission, threat, Al, and friendly capabilities. While the analyst considers the effects of the weather on personnel and equipment, the primary concern is with their impact on mobility and LOS.

WEATHER FACTOR ANALYSIS MATRIX DEVELOPMENT

The weather factor analysis matrix (see Chapter 4, FM 34-130) assists the analyst in organizing the analysis task, defining Specific weather requirements, and determining what weather factor overlays are required to support mission planning. The matrix isolates those weather factors that are militarily significant and correlates their effects with specific combat operations and supporting functions.

THREAT EVALUATION

During the threat evaluation phase, the intelligence analyst examines enemy forces utilizing the nine OB factors.

The objective for the intelligence analyst during this phase is to determine enemy capabilties, vulnerabilities, and strengths. Also the analyst determines how the enemy would operate doctrinally If not restricted by terrain and weather. The G2 or S2 analyzes the enemy based on known information maintained in the enemy OB file. Information gaps identified are translated into RIIs and sent up the intelligence chain to be answered. Maintaining a detailed enemy OB file is a continuous process. The S2 section maintains one for each of the unit's contingency and normal operating areas. The intelligence analyst uses the enemy OB together with current information and the mission to develop an HVT list.

The S2 and staff develop an HVT list by imagining how the enemy would fight, relative to the friendly force mission. The S2's or analyst's goal is to identify enemy assets an enemy commander would consider valuable or critical for the accomplishment of the mission. In thinking through the enemy plan an analyst considers how the friendly element's mission and intent affects the enemy mission.

For example, if an analyst is thinking through an enemy attack and knows that the friendly force is in prepared positions with extensive obstacles and barriers throughout the perimeter, it is a logical assumption that the enemy commander will want substantial engineer support to breach friendly obstacles. The enemy commander may not be aware of the obstacles, yet engineer assets in fact are critical to the enemy battle plan. Enemy engineer units therefore become HVTS. The G2 or S2 provides this and other HVTS in the form of a HVT list to the G3 or S3 and the FSE so target priorities are established and planned for.

By analyzing probable enemy actions, the analyst enhances the probability of mission success by determining HVTS which can become enemy vulnerabilities if acted on by the G3 or S3 and the FSE.

The analyst develops doctrinal templates during the threat evaluation phase. Before creating doctrinal templates, the analyst determines which enemy echelon is the focal point for analysis. US commanders are interested in enemy echelons one level above their own because that is the enemy echelon that directs a battle against them. Enemy maneuver elements are templated for units two echelons below that of the US commander, because those are the ground force units in direct contact with the unit.

Knowledge of enemy doctrine provides a starting point for doctrinal templates. For example, doctrinal templates may be required to reflect the sequential order of an enemy unit in the attack from its assembly area to the ultimate objective. The sequence may be as follows:

- Tactical march formations.
- River crossing (hasty, deliberate) .
- Breakthrough.
- Envelopment.
- Exploitation.
- Pursuit.

One method of determining which operations and units should be templated is to develop a matrix. The matrix shows which types of operations and units that are expected to be encountered and provides a clear record of what has been determined. Figure 4-14 showa an operations or unit matrix,

It is also important to prepare doctrinal templates of battlefield functional systems. The functional system templates generally expand information that is reflected in the primary doctrinal templates. For example, a template depicting an enemy division in a river crossing is expanded by a subset depicting the deployment of engineer bridging and pontoon equipment.

Again, not every possible enemy action and subset is templated.

Types of Operations / Types of Units	Movement to Contact	Meeting Engagement	River Crossing	Attack Against a Defending Enemy	Pursuit
Motorized Rifle Division	X	X	X	X	X
Motorized Rifle Regiment	X	X	X	X	
Motorized Rifle Battalion		X	X		X
Independent Tank Battalion			X	X	X
Tank Division	X	X	X	X	X
Tank Regiment	X	X	X	X	X
Tank Battalion		X	X		

Figure 4-14. Operations or unit matrix.

A matrix is an easy way to lay out the information to be analyzed and recorded, Using a matrix, the analyst looks for those battlefield functional systems in certain types of operations that tell the most about how the enemy operates in relation to the mission. Figure 4-15 shows the types of operations on a battlefield functional systems matrix.

THREAT INTEGRATION

The objective of threat integration is to integrate enemy doctrine with the terrain and weather analysis done in previous IPB phases. This further reduces uncertainty as to how the enemy fights. Members of the staff analyze potential courses of action during this phase to advise the commander of the best course of action to accomplish the mission.

To assist the staff, the G2 or S2 produces situation, event, and decision support templates. FM 34-130 provides a detailed description on how to prepare these templates. This chapter discusses how the analyst should apply these templates in order to support the staff planning process.

SITUATION TEMPLATE

The situation template depicts how the enemy adjusts doctrine to terrain and weather effects throughout the battlefield. Knowledge of enemy doctrine is critical to developing and using situation templates for analysis.

Types of Operations / Types of Battlefield systems	Tactical March Formations	Meeting Engagement	River Crossing	Attack Against a Defending Enemy	Pursuit
Tactical Rockets and Artillery	X	X	X	X	X
AD	X	X	X	X	X
Communications	X	X	X	X	
REC		X	X	X	X
Missiles				X	X
Reconnaissance	X		X		X
Rear Services			X	X	X
C^3 of MRD	X	X	X	X	X
C^2 of MRR	X	X	X	X	X
Engineers	X		X	X	X

Figure 4-15. Battlefield functional systems matrix.

During this phase the analyst takes doctrinal templates and visualizes where the enemy force will place assets on a particular point on the ground. By doing this, MCS within each AA become apparent.

As enemy forces move along AAs and MCs, they do so sequentially. The analyst follows the enemy by sequentially and situationally templating their movement.

Because of time constraints, apply situation templating initially to critical areas on the battlefield. These are based on the friendly force mission and what the commander feels are critical battlefield points and areas. By applying situation templates the analyst usually depicts expected enemy movements along an AA for the commander and staff. This contributes to the planning process by allowing the commander to get a "visual feel" for the enemy's plan.

PRIORITY INTELLIGENCE REQUIREMENTS

PIRs are the expression of the commander's information needs. When recommending PIRs, the intelligence analyst keeps in mind the commander's intent. The analyst limits the PIR to a few questions. These PIRs must seek answers to questions critical to the successful accomplishment of the unit's mission.

While PIRs are general in nature, they must be specific enough to identify the critical information required. For example if the brigade is preparing defensive positions in anticipation of an attack, then a PIR could be: When will the enemy attack? A more specific PIR would be: When will the enemy attack and where is the main effort? This PIR, if answered, helps the commander prepare a more effective defense particularly if time is short. Knowing where the main effort is helps the commander prioritize defensive preparations.

EVENT TEMPLATE

Situation templating is the basis for event templating. Event templating is the identification and analysis of significant battlefield events which provide indicators of an enemy course of action. It is a projection of what most likely will occur if the enemy adopts a particular course of action. By knowing what the enemy can do and comparing it with what the enemy is doing, it is possible to predict what the enemy will do next. Because there are normally several courses of action which lead to the enemy's objective, each must be identified. Event templates are then developed for each course of action. This is because the enemy course of action which the analyst identifies as the most probable may not be selected for reasons of deception or other factors known only to the enemy. The analyst must be able to shift attention quickly between courses of action during the battle.

The event template is a critical analytical tool for determining the enemy's posture and movement. Knowledge of when and where enemy activity is likely to occur on the battlefield provides indicators of enemy intentions. Indicators may be negative (that is, things that do not happen may be just as critical as what does happen). The projection of battlefield events occurs through situation development during the prehostility or predeployment phase of the IPB process and is verified or refuted during combat operations.

While visualizing the enemy force moving along an AA or MC, critical areas become apparent. These areas are significant because they are where significant events and activities should occur. If the analyst's hypothesis is correct, it is within these areas that targete appear. The intelligence analyst designates these areas as named areas of interest (NAIs) .

An NAI is a point or area, often along an identified MC, where enemy activity (or inactivity) confirms or denies a particular enemy course of action. NAIs also fall outside of a MC. For example, there may be activity on key terrain, such as high ground, in support of movement on an adjacent MC.

The event template and its NAIs are the basis for intelligence collection, R&S, and analysis because they--

- Focus attention on areas where the enemy force must appear if it uses a particular MC.

- Frame militarily significant events by time and location within an NAI.

- Compare events in one NAI with events occurring in the NAI of other MCs to determine enemy intentions.

It is important to develop event templates as quickly as possible. Refine them further as time permits. Early preparation permits quick development of an R&S plan. R&S assets are focused on NAIs to obtain the greatest payoff in relation to limited assets. The primary goal of an analysis is to apply the event template to the collection of information which supports the mission planning effort.

EVENT ANALYSIS MATRIX

The event analysis matrix (EAM) supports the event template. It correlates the expected events and activities within each NAI and adds the dimension of time. Through analysis of enemy doctrinal movement rates and the effects of the terrain and weather on their mobility, estimate the time required for the enemy to move between NAIs.

The analyst prepares an EAM for the primary AA and each MC within it. Figure 4-16 shows a sample EAM. Due to time limitations and staff size, most EAMs are prepared at division level or higher.

Before combat, the EAM and event template illustrate possible enemy courses of action as a basis for comparing friendly courses of action. During combat operations, they focus on enemy probable courses of action.

Event templating enables the G2 to develop precise collection requirements, maximizing the effectiveness of limited resources over extended areas against a vast array of enemy targets. It assists the intelligence analyst in determining where to look, when to look, and what to look for. Situation and event templates enable the collection manager to establish collection priorities based on those courses of action the enemy is most likely to adopt. Framing movers and emitters, the primary indicators of events and activities, in time and location, allows the collection manager to determine the optimum mix of collection sensors.

Event templating also serves the G3 by telling--

- Where and when to shoot, jam, and maneuver.

- What to shoot, jam, and maneuver against.

Event templating is the vital link between the success of the commander's tactical concept and intelligence requirements and the collection, planning, and execution needed to fulfill those requirements.

DECISION SUPPORT TEMPLATE

The DST is a logical extension of event templating; it relates events of the event template to the commander's decision raquirements. The DST

is not the sole responsibility of the G2 or S2. Production of the DST and synchronization matrix is a shared responsibility, involving the entire staff or their representatives. The G2 or S2 provides information about the enemy. The G3 or S3 guides the effort and ensures that it supports the commander's intent.

A properly prepared DST portrays the enemy's most likely course of action and possible target areas of interest (TAIs) along with time phase lines (TPLs). It also depicts decision points (DPs) which relate to the use of fire, maneuver, and CSS.

AVENUE OF APPROACH II				COORDINATES FM: NB 606330-NB 650333 TO: NB 462181-NB 494132	
MOBILITY CORRIDOR A				FM: NB 670300 TO: NB 468158	
NAMED AREA OF INTEREST	**DISTANCE (kms)**	**RATE OF MOV (kph)**	**ESTIMATED TIME**	**EVENT OR ACTIVITY**	**OBSERVED TIME**
NAI NO. 1 NB 649288 RD JUNCTION	30 km		1.5 hrs	A. RECON ELM	
				B. ADV GUARD	
				C.	
NAI NO. 4A NB 647264 CHOKE POINT	30 km		1.5 hrs	A. RECON ELM	
				B. ADV GUARD	
				C.	
NAI NO. 4 NB 601222 RD JUNCTION	9 km		30 min	A. RECON ELM	
				B. ADV GUARD	
				C.	
NAI NO. 3 NB 561220 BRIDGE	40 km		2 hrs	A. RECON ELM	
				B. ADV GUARD	
				C.	
NAI NO. 7 NB 480180 RD JUNCTION				A.	
				B.	
				C.	

Figure 4-16. Event analysis matrix.

Target Areas of Interest

Areas along each AA and MC where the comnander influences the enemy through fire and maneuver are TAIs. The TAIs are normally areas which were earl ier identified as NAI. They are areas where we delay, disrupt, destroy, or manipulate the enemy force. They are also areas suitable for attacking HVTS.

A TAI is an engagement area or point, usually a long an MC, where the interdiction of enemy forces by maneuver, fires, or jamming deprives or reduces a particular enemy capability. It also may cause enemy forces to abandon or require the use of unusual support to continue operations. In the latter option, TAIs are terrain-dependent to inhibit or deny movement.

Sample TAIs include--

- Key bridges.
- Road junctions.
- Choke points.
- DZS and LZS.
- Known fording sites.

The TAIs are significant because they constitute a basis for allocation of attack resources. The identification of TAIs is a joint effort of the intelligence, operations, and FSE staffs. The intelligence staff evaluates enemy forces and the effect of interdiction on their capabilities. The operations staff and FSE consider the availability of interdiction resources, the effects of interdiction on the accomplishment of friendly missions, and priorities for the use of available resources.

Part of determining TAIs involves target value analysis (TVA). TVA is a joint activity of intelligence, operations, and FSE personnel. Through analysis of enemy doctrine, TVA names and provides the basis for locating enemy elements which are key to the enemy's success. These enemy elements are known HVTS.

A second category of targets is the HPT. Destruction of an HPT is advantageous to friendly operations. The commander designates the HPTs. For example, suppose the enemy must cross a wide, deep river in a friendly sector as part of a probable attack. Enemy engineer assets are very important to the enemy commander's success. The engineer units and equipment are HVTs because without them the river crossing is impossible. The friendly commander, briefed on this HVT, designates the enemy engineer assets as HPTs because their destruction is of great value to the friendly defense plan. This particular HPT is prioritized among other HPTs for location by intelligence personnel and subsequent attack by lethal and nonlethal means.

An analyst must have an in-depth knowledge of enemy doctrine to determine potential HVTS, CPS, missile units, and logistics points on situation and event templates. This knowledge helps in cueing collection assets to possible HVT locations designated as TAI for the DST.

Decision Points

Following the selection of TAI, the analyst identifies DPs. The availability and capability of friendly fire and maneuver systems largely influence the location of DPs; therefore, their selection is primarily a G3 or S3 function. However, this task requires the efforts of both the G3 or S3, the G2 or S2, and their respective staffs.

DPs identify those battlefield events which may require tactical decisions and the no-later-than time when these decisions are made for the commander to retain available options. Decisions are made early enough to ensure implementation in time to achieve the desired effects; however, they cannot be made until there are indications that particular battlefield events will occur and their locations determined with a high degree of confidence.

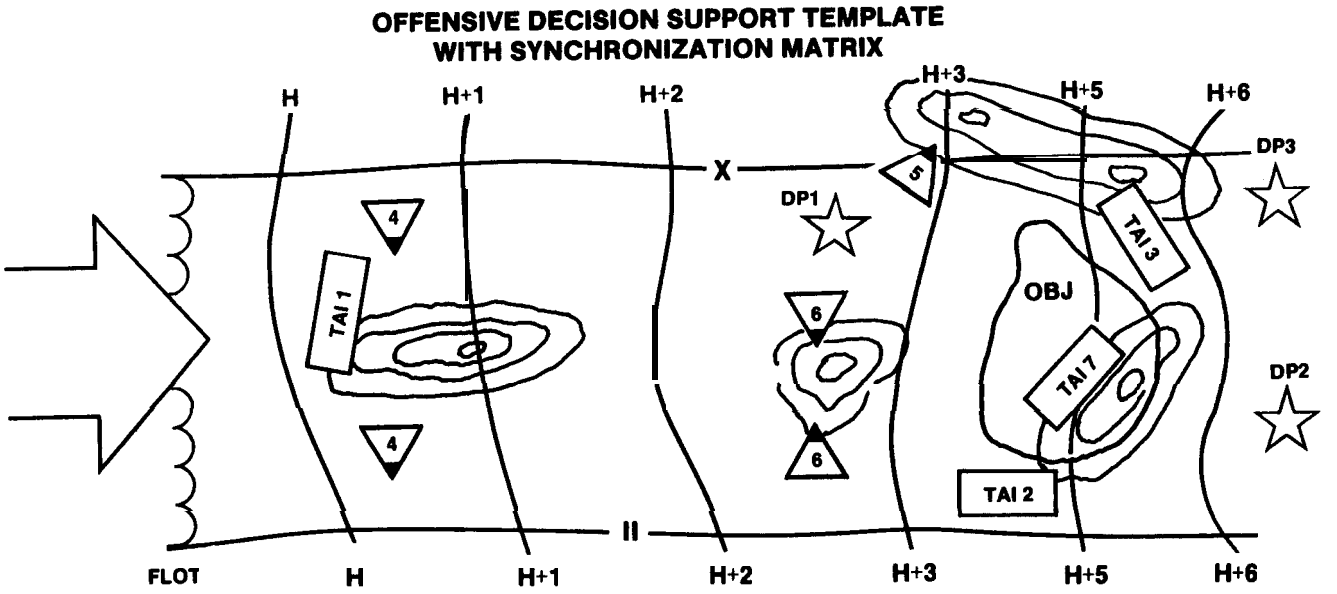
DPs associate projected enemy locations with specific points on the battlefield. Comparing times required to implement decisions, enemy movement rates, and distances determine DPs. For example, if it requires two hours to implement a decision, it must be made while the enemy is at least two hours from the TAI where the event will occur. These decisions include more than fire and maneuver; they also include decisions such as donning mission oriented protective posture (MOPP) gear, and employing smoke. Enemy doctrinal movement rates that the analyst develops are adjusted to compensate for the effects of the terrain, weather, and friendly action on mobility. They provide the basis for computation.

The DST depicts the TAI and DPs. Figure 4-17 shows a sample offensive DST with synchronization matrix.

Decision Support Matrix

A decision support matrix supplements the DST. This matrix relates each DP to the event or associated TAI or NAI requiring a friendly reaction. Decisions are made by the time enemy forces pass DPs or a set of options which were available are negated. Other information from the IPB data base, like enemy composition and probable deployment, supports the DST.

Intelligence provides a basis for tactical planning and execution. Detailed planning is accomplished during the static period, as an 8- to 10-day battlefield scenario does not allow time for detailed planning. Event and decision support templates are the results of detailed intelligence planning that is accomplished during static conditions. They are the basis for all tactical planning. These templates are the filters through which all information and intelligence are directed to the commander. They are relevant to the commander's needs, as expressed in PIR and IR, because they are keyed to important battlefield events and



INTEL	PIR-SCTY	SCOUTS OUT R&S	JAM C² TAI 4 JAM C² TAI 6	PIR-DEF POSN	PIR 2 ECH		
MNVR	A CO MAIN ATK		AH1 TAI 5	C CO MAIN ATK		CONSOL CONTINUE	DP 2 AND 3 COMMIT RESERVES
FS	SMOKE TAI 1 HPT-RECON	PREP FIRES	ARTY TAI 6	CAS TAI 2, 3 HPT-MBA DP1 SMOKE TAI 5	ARTY TAI 7	HPT— 2d ECH	
ADA	YELLOW/FREE			RED/TIGHT		YELLOW/FREE	YELLOW/FREE
MOB/CM	MOB		ENGR FWD			CM-OBSTACLE	
C²	CP NORTH		MOVE TOC		CP SOUTH		
CSS					MOVE TRAINS		

Figure 4-17. Offensive DST with synchronization matrix.

time and space factors known to be of interest to the commander. The DST is the vital link between the conmmander's intelligence needs and the resultant actions the commander and staff require.

The commander is vitally concerned with wresting the initiative from the enemy commander; that is, forcing the enemy commander to choose a less desirable course of action through design rather than chance. The DST frames the commander's opportunities and options and ensures timely and accurate decisions. This provides the means to influence enemy actions rather than just react to them.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD DURING PEACETIME

This chapter has emphasized the vital role that IPB plays in preparing for the next battle. During peacetime, IPB builds an extensive data base for each potential area in which a unit is required to operate. It analyzes this intelligence data base in detail to determine the impact of the enemy, weather, and terrain on operations and presents this information graphically. IPB is initiated any time the commander faces a new enemy or receives a new mission. It is a continuous process which supports planning and execution for all operations.

CHAPTER 5

ANALYSIS IN DEPTH

Analysts do not find intelligence. Analysts develop intelligence through evaluating, assessing, integrating, and interpreting information. This intelligence focuses on the commander's needs. It must support the commander's decision to concentrate or disperse forces on the battlefield. It must provide information to assist the commander in targeting and defeating the enemy. This chapter addresses some of the techniques and tools which the intelligence analyst uses to manage intelligence production.

Analysts face daily problems. These challenges vary from the simple, such as finding information, to the complex, such as predicting specific enemy courses of action. The analyst makes decisions regarding what, how, and when the commander can use information to support the battle. This information often means the difference between winning and losing on the battlefield, so it is vital that analysis be both accurate and timely. This information and analysis influences decision making. Although the analyst does not make decisions for the commander, the commander cannot make qual ity decisions without' the information that analysts provide.

MEETING USER REQUIREMENTS

The ultimate user of intelligence is the commander. The analyst produces intelligence that the user specifically needs. Through stated PIRs and IRs, the commander drives intelligence production and focuses efforts. The commander's IRs often pertain to varied areas on the battlefield. For example, intelligence required to support the rear battle is different from that required for the deep battle. Different staff sections require different information, yet all of this supports the commander's needs on the battlefield.

It follows then, that to satisfy user requirements, the analyst must understand what those needs are. Figure 5-1 lists some of the factors which an analyst should consider in developing an intelligence product. If the analyst and the user do not look at information or problems from the same perspective, the intelligence will not support requirements.

As a simple example, suppose the user asks for a list of locations where a river may be bridged. The analyst considers the enemy's tanks, which weigh about 40 tons, and provides such a list. If the user plans to cross these bridges with American tanks, which weigh about 60 tons, the list of locations is useless. Clearly, the analyst has failed to understand the user's needs.

In the tactical environment, the analyst and the user see the mission as fighting the same enemy in a specific geographic area. From the knowledge each has about the tactical situation, both develop conceptual mode ls, The analyst and the user create some type of theoretical

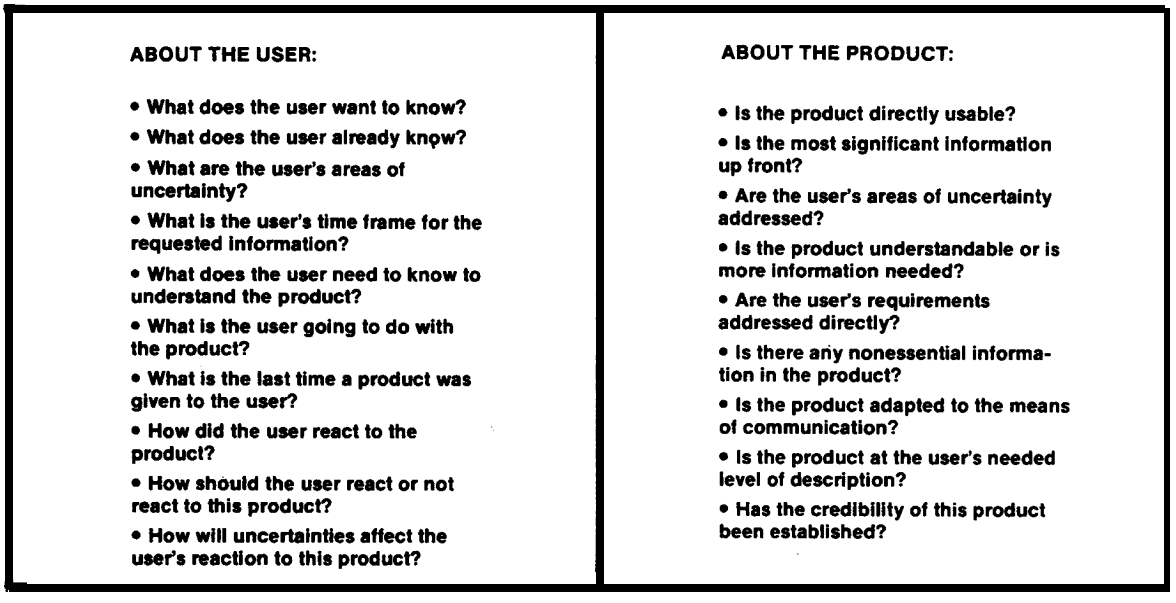


Figure 5-1. Developing an intelligence product.

representation of the tactical situation. These conceptual mode Is have common factors wh ich both anal yst and user share. These common factors are termed "a shared conceptual model ."

Without a shared conceptual model, the user and analyst cannot communicate. Effective communication allows the analyst to understand the user's requirements and to tailor the product to them.

Communication allows analysts to interpret what the user wants and fill in any missing intelligence pieces. This is easily done through feedback.

Feedback greatly improves the quality of any intelligence product. If user and analyst communicate during the development of a product, the shared conceptual model is refined. This allows the analyst to orient on those areas important to the user and to eliminate nonessentials. Refinement of the "model'" sensitizes the analyst to areas of uncertainty and the criticality of time in a given situation. The analyst, in turn, al lows the user to understand the risk inherent in any estimate and the basis for assumptions made.

Face-to-face communication is the best form of feedback. It is also the best way to develop a shared conceptual model. Ambiguous words or ideas can be instantly clarified, pictures or sketches can be drawn, and maps consulted, When face-to-face communication is not possible, the analyst speaks with staff officers or other representatives of the user. If a standard of performance has been established or is described in SOP, the analyst uses this as a measure of current efforts.

DETERMINING THE RISK FACTOR

Uncertainty is what the job of intelligence is all about. To succeed, the analyst handles uncertainty from a number of sources. While objective ground truth is found in the laboratory, it is not part of analysis of the battlefield. The analyst frequently deals with ambiguous or even misleading information.

The analyst's greatest concern is uncertainty, the commander's is risk. Good analysts translate uncertainty into risk. Figure 5-2 shows a graph of risk functions to consider. Risk increases as enemy lethality moves from low to high. When a range of uncertainty is added to the estimate of lethality, the potential danger becomes even greater. The degree of risk a commander will accept governs the amount of uncertainty the analyst reports.

For example, under a very high level of uncertainty, the commander faces between one and three enemy tank divisions. The analyst admits the level of uncertainty involved, while collecting and processing information to reduce the uncertainty. The level of uncertainty that the analyst

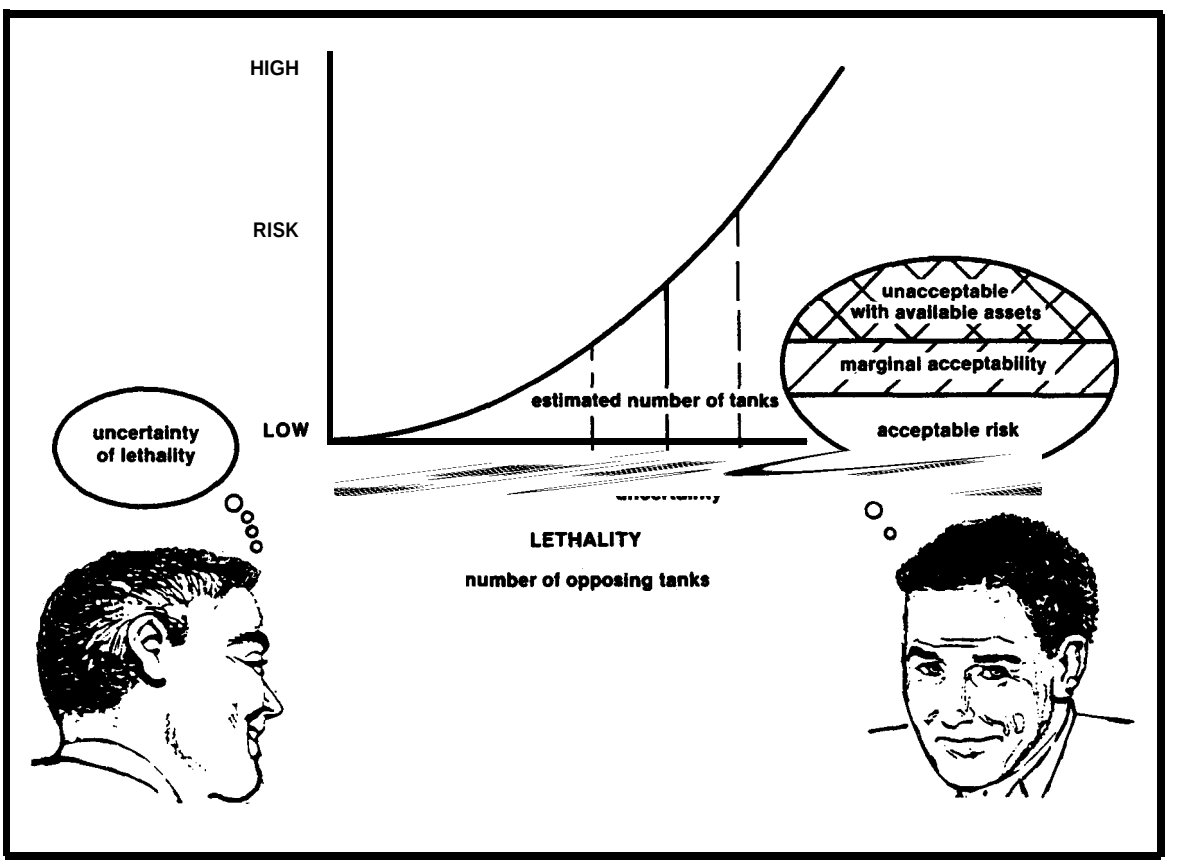


Figure 5-2. Translating uncertainty to risk.

accepts is driven by the degree of risk the commander accepts. The commander is unable to properly plan for battle knowing only that friendly forces face "between one and three enemy tank divisions". The same commander is not concerned about facing 10 or 12 enemy tank battal ions; the commander employs the same plan regardless, in facing 10, 11, or 12 battalions. The analyst does not waste time reducing the level of uncertainty beyond reporting "1O to 12 tank battalions" because the commander is satisfied with the given degree of risk.

Risk is a voluntary exposure to danger, however unavoidable it might be under the circumstances. In combat, there is always risk in not preparing response to a potential enemy action whether or not that action has a high possibility of execution. Risk increases in response to potential danger and decreases when the enemy threat credibility goes down.

Risk increases when--

- Enemy force lethality increases.
- Warning time decreases. (Crises occur when warning time is less than the required preparation time; the worst-case situation is when there is total surprise and no warning.)
- The number of enemy options increases. (If the enemy's plans are ambiguous, then friendly forces might not plan effective responses to all of the enemy opt ions.)
- The number of friendly options decreases. (If fewer options are available for countering the threat, there is a greater chance that the available options will not work.)
- The enemy's knowledge of the battlefield environment, including friendly forces increases.

Risk decreases when--

- The enemy force lethal ity decreases.
- There is greater warning time.
- The enemy has fewer options.
- The number of friendly force options increases.
- The friendly force knowledge of the battlefield environment, including enemy forces, increases. Knowing how the environment affects combat operations allows the commander to exclude unworkable courses of action and to gain maximum effectiveness from others.

The analyst's uncertainty plays a key role in the evaluation of the enemy and the amount of risk accepted. Uncertainty may arise for many

reasons. First, there is uncertainty about the enemy's intent: "What is the enemy's real objective? What are the various means of achieving this objective?"' Second, there is uncertainty in evaluating the capabilities of the enemy force to achieve these objectives. Third, there is uncertainty in other factors (lethal ity, warning time, enemy and friendly options, and environmental conditions). Fourth, there is uncertainty that the method of response will produce the desired outcome.

THE THREAT MODEL

The threat model is a portrayal of the enemy. It allows the analyst to piece together information, identify information gaps, speculate and predict, and do problem solving. Most importantly, the threat model allows some of the risk in a given situation to be quantified. There will always be inaccuracy in a model, and so there will always be uncertainty. Still, based on the model, an analyst can look for changes in a real-world situation to identify patterns, trends, and activity levels. Creating such a model requires a knowledge of--

- Physical objects such as weapons, vehicles, and radar.
- Organizational structures of enemy and friendly forces.
- Battlefield environment, including terrain, hydrology, and weather.

Once developed the model is refined and maintained, or it will lose its validity.

Threat models incorporate white elements (battlefield geography and environment conditions), red elements (the enemy force (or threat), and blue elements (the friendly force). The three elements of white, red, and blue form an organizational structure from which the analyst can mentally picture the battlefield. Figure 5-3 illustrates elements of the threat model.

Thinking white is understanding the elements of the environment as they affect the battle. In threat modeling, development of the white framework comes first. It is the white framework that anchors the threat model to the real world. The white framework is made up of space and time.

Developing the geographic framework of the battlefield is as simple as plotting the battlefield on a map. The dimensions of the battlefield encompass the unit's AO and AI.

The map is a model of the real world. The topographic map contains a wealth of information about the battlefield environment, including descriptions of terrain, roads, and population centers. The highly detailed military map contributes more information to the threat model.

Time in the threat model is a sequence of time-period snapshots (or windows) within which events occur. The analyst compresses threat model

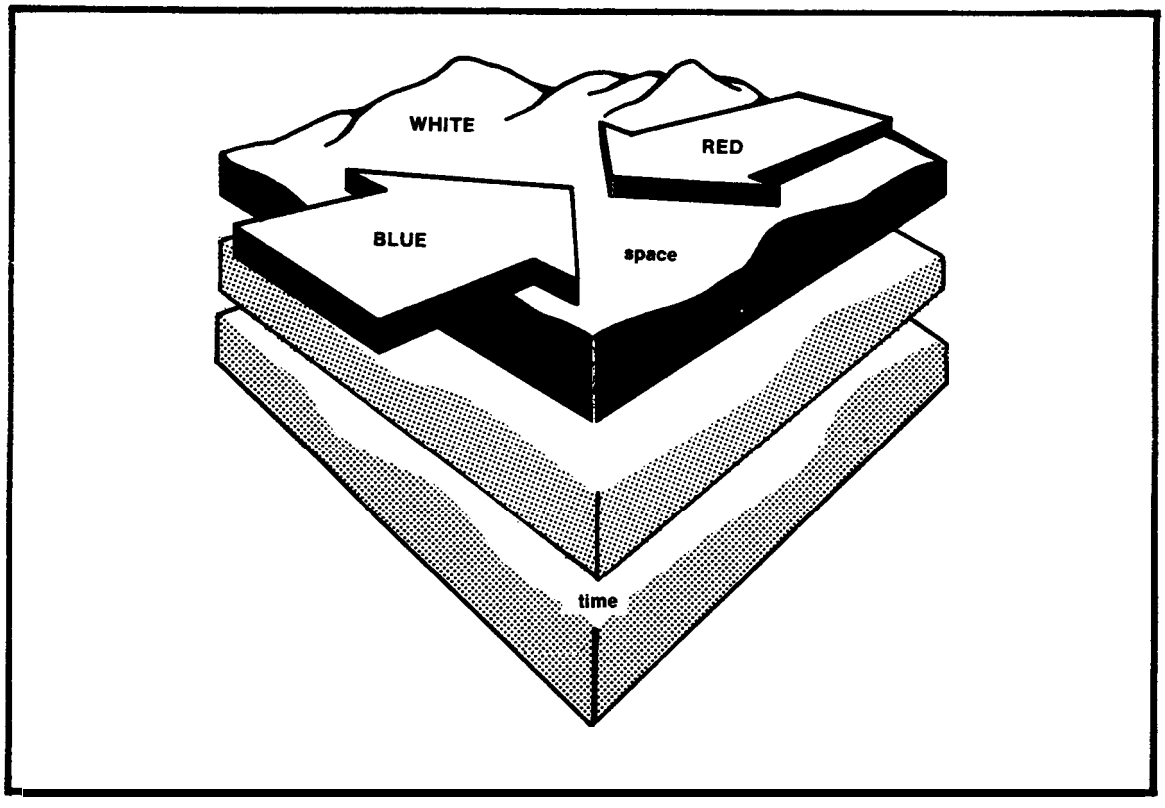


Figure 5-3. Elements of the threat model.

time to bring events closer together or expand it to make individual events more distinguishable. Overlaying time windows helps in seeing patterns of events or distinguishing changes. In the threat model snapshot sequence, one of the snapshots represents the current time frame. A sequence of snapshots al lows the analyst to fol low courses of action from the current time frame to the eventual outcome of the battle. Each snapshot represents an overlay of information on the battlefield geography. Figure 5-4 shows this.

Thinking red is seeing the battle from the enemy's viewpoint. The red element of the threat model is anchored in the real world. Enemy forces use the political and military policies of the foreign nations involved. The enemy combat force is an extension of political policies that are the source of the conflict that creates the battlefield situation.

Next, in threat model ing, plot the red element, including locations and likages of the political, military, and combat organizations on the battlefield. The highest echelon of enemy organization plotted depends on the echelon of interest to the friendly force commander. For example, the strategic-level threat model has all aspects of the civil ian and mil itary

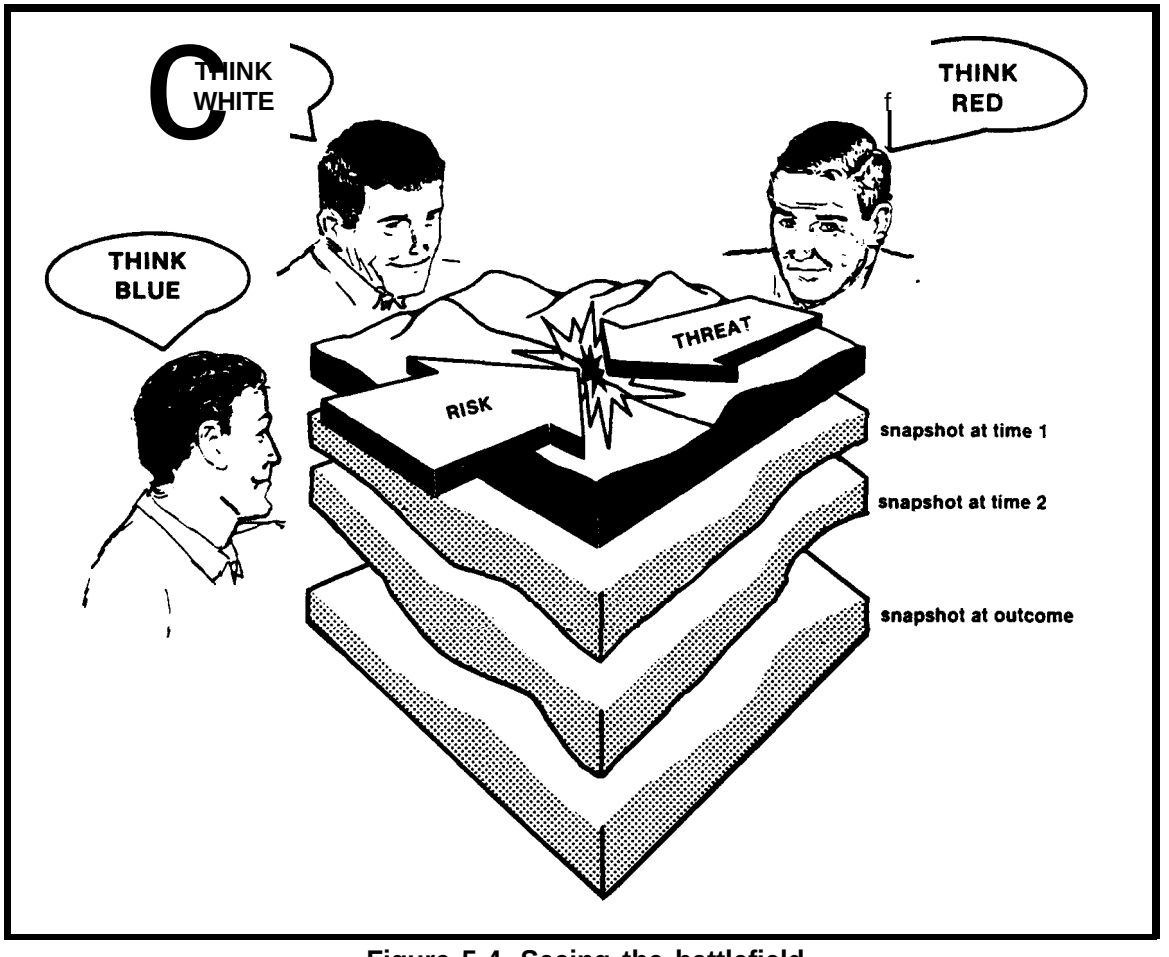


Figure 5-4. Seeing the battlefield.

force structure, whereas a division-level threat model shows only the locations of the red forces up to army level.

The organization of red elements follows some form of hierarchical structure, connected by lines of communication (LOC). The LOC shows the relationships between units for command, control, and coordination. The LOC is overlaid on the geographic structure and relates to physical communication paths like roads, transmission lines, or electromagnetic transmission paths. Figure 5-5 shows the three techniques.

Thinking blue refers to seeing the battle from the friendly commander's point of view. The threat model takes on its full meaning when the blue element is introduced along with white and red. The targets of red threat are blue elements; the components of the friendly force are blue elements.

Fill out the RED War Plan with three techniques:

1. **Start with enemy doctrine to structure the war plan.**
2. **Exploit intelligence sources to fill in details.**
3. **Use analogies to fill in missing information.**

Figure 5-5. Red elements three techniques.

The most common failing of analysts is their inability to "think blue". Analysts become extremely knowledgeable about the enemy, knowing nearly exact numbers of equipment, biographies of commanders, and unit histories, but they cannot see how friendly forces operate. It does little good to understand enemy aviation without understanding some of the characteristics of friendly air defense. While there are staff officers who are experts in friendly systems and tactics, the analyst must still have a familiarity with blue doctrine and tactics. This returns to the need for a shared conceptual model.

In plotting the location of units in the white framework, the analyst is concerned with the location of those combat units that information from the threat model supports. Figure 5-6 lists some information sources for developing the blue element of the threat model.

- **Operations plan for the friendly force.**
- **Friendly force doctrine.**
- **Mission plans.**
- **RED view of friendly forces.**
- **Situation reports from operational elements.**
- **Mirror imaging.**

Figure 5-5. Information sources for developing the blue element.

Figures 5-7, 5-8, and 5-9 show checkl ists of white, red, and blue questions that are asked when creating the threat model.

What is the geography of the battlefield?

What is the culture of the country area?

What is the history of conflicts in this region?

What is the attitude of the local population toward the enemy force? toward the friendly force?

What is the academic, economic, and technological level of the local population?

How is the local population armed?

How is the population distributed in the region?

What local cultural features (airfields, railways) can be exploited for military purposes?

How predictable is the weather in the area?

How does the weather affect operations, personnel, trafficability, equipment, and communications?

During what time frame will hostilities occur?

How much time is available for preparation?

Figure 5-7. Checklist of white questions.

What is the enemy's doctrfne?

What are the enemy's tactics?

How does the enemy prepare war plans?

How does the enemy train?

What are the enemy's objectives?

How is the enemy equipped?

What is the enemy's strategy?

How is the enemy force sustained?

What are the enemy's operational plans?

How is the enemy force structured?

What are the enemy's courses of actions?

Figure 5-8. Checklist of red questions.

What are the BLUE principles of war?	What resources does the have at his disposal?
What are the friendly objectives?	What are the priority information needs of the commander?
What are the friendly force resources?	What are the information needs to execute the mission?
What is the commander's mission?	

Figure 5-9. Checklist of blue questions.

Given a model of how the battlefield should appear in a certain situation, the analyst develops and tests hypotheses of how the enemy may act. An hypothesis is an explanation that accounts for a set of facts and that can be tested by further investigation. It is a set of logically related propositions and an outcome. An hypothesis can be proven false based on evidence, but it can never be proven correct in advance. The best that the analyst can do is rank order several hypotheses or assign rough probabilities to them, Whan seeking evidence to support or reject a hypothesis there are several considerations for the analyst:

- The enemy can be engaged in deception. The course of action selected by the enemy does not have to be the best, but only adequate. Deception efforts then can be mounted which support the most obvious course of action.
- Sensors can collect only in the areas where they look. If targeted at one specific area, they may not collect information in another. This information not collected may have confirmed or denied a particular course of action.
- Indicators may be redundant to several hypotheses,
- Several sensors may collect the same piece of information. This can give undue weight to a hypothesis.
- Some small indicator may be vital to a certain course of action. Large scale river crossings, for example, require engineer support. If that support is conclusively absent, a river crossing cannot occur, no matter what else supports that hypothesis.
- The evidence gathered in one area may not be representative of the whole battlefield. For example, the enemy has 15 battalions of artillery available. Sensors report 4 battalions in the north and 2 in the south. This does not conclusively indicate a total of 10 battalions in the north and 5 in the south. The true disposition may be 4 in the north and 11 well camouflaged battalions in the south .

When selecting an hypothesis as "most likely" or rejecting it out of hand, all of the above issues come into play. These errors in thinking may lead to false alarms or rejecting perfectly good ideas. Other errors also exist which affect analysis. They are called biases.

BIASES

If a single term best describes the factors that interfere with successful analytic thinking, it is bias. A bias is a subjective viewpoint. It indicates a preconceived notion about something or someone. Analysts must recognize biases and be aware of the potential influence they can have on judgment.

Biases can have a positive influence on analysis. With a iack of information, a preconceived notion gives a starting point for thinking about a situation. However, biases are generally bad because they obscure the true nature of the information. The analyst must recognize several categories of biases so as not to be misled or drawn into the wrong conclusions during the analysis process. Biases are cultural, organizational , personal, and cognitive (perception).

CULTURAL BIASES

Cultural biases begin forming at an early age and continue throughout a lifetime. They interfere with the ability to think in the same manner as the enemy (think red). Analysts need considerable background information on culture and social mores to perceive a situation In the same way the enemy perceives it. If analysts do not have this experience or information and decide to depend upon their own values when looking at a situation, the analysis is likely to be wrong. The reason for this is that different cultures tend to view similar situations differently.

ORGANIZATIONAL BIASES

Most organizations have specific policy goals. Any analysis done within these organizations may not be as objective as the same type of analysis done outside the organization. Some of the problems that occur from a subjective internal analysis range from an unconscious altering of judgment because of exposure to selective information and common viewpoints held among individuals, to deliberately altering a judgment to provide what the commander wants to hear. "Best case" analysis is a good example.

"Best case'" is where an analyst preeents the situation in the most optimistic light so as not to anger the commander. This frequently underestimates the enemy's capability while overestimating friendly capability.

PERSONAL BIASES

Personal biases come from past experiences. If a thought pattern previously led to success, analysts may continue to follow this pattern.

Even if the situations have nothing in common, the tendency to follow the methods that were successful in the past is very strong.

COGNITIVE BIASES

The all-source analyst evaluates information from a variety of sources (including HUMINT, SIGINT, IMINT, and open sources). Each source has strengths and weaknesses. The degree of reliability, completeness, and consistency varies from source-to-source and even from message-to-message. This variance often creates doubt about the reliability of some sources.

The cognitive biases that cause analysts the most problems are vividness, absence of evidence, oversensitivity to consistency, persistence of impressions based on discredited evidence, and availability.

Vividness

Clear and concise information has a greater impact on thinking than abstract and vague information. Even if the vague piece of information has more value as evidence, the tendency is to disregard faster than you would eliminate a clear piece of information.

Absence of Evidence

Lack of information is by far the most common problem, especially in a tactical environment. This does not mean that analysts should be content with the information on hand; they always want more. Analysts shouldn't hold back information because it is not conclusive. It rarely is. Instead the analyst should--

- Realize that information sometimes is missing.
- Identify areas where information is lacking and consider alternative hypotheses.
- Adapt and adjust judgments as more information comes in.
- Consider whether a lack of information is normal in those areas or whether the absence of information is itself an indicator.

Oversensitivity to Consistency

Consistent evidence is a major factor for confidence in the analyst's judgment. On the one hand, consistent information is appropriate. On the other hand, information may be consistent because it's redundant, or it may come from a small or biased sample. The analyst considers if the evidence is representative of the total potentially available information. If it is not, or if it is not known, then the confidence level is low, regardless of the consistency. The analyst must be receptive to information that comes in from other sources regardless of whether it supports the hypothesis or not.

Persistence of Impressions Based on Discredited Evidence

Whenever the analyst receives evidence, there is a tendency to think of things that explain the evidence. These connections create impressions. Although the analyst discredits the evidence, the connection remains, and so do the impressions. An example is a clandestine source under hostile control. If the source has a record of passing accurate information, the analyst tends to judge all information that is passed according to previous accuracy. The analyst may doubt the validity of the report claiming that the source is under hostile control or may rationalize the inaccuracy in some other way. Either way, the evidence is based on previous information and not on current indicators. This is one way an enemy could launch a deception operation. This is important. An analyst who "reasons away" information contrary to pet hypotheses does the commander a disservice. Analysts must be professional and capable of saying, "I was wrong," before the situation is lost.

Availability

The ability to recall past events influences judgment concerning future events. Since memory is more readily available, and is more acceptable, it is easy to rely upon memory instead of seeking a proper sample to predict events.

Overcoming bias is a vital step to proper analysis. Any of the above biasas reduces the quality of analysis performed.

CHAPTER 6

SITUATION DEVELOPMENT

Situation development enables commanders to see and understand the battlefield in sufficient time and detail to make sound tactical decisions. It helps locate and identify enemy forces; determine their strength, capabilities, and significant activities; and predict their probable courses of action. Situation development helps the commander to effectively employ available combat resources where and when the decisive battles will be fought. Also, it helps prevent the commander from being surprised.

This chapter describes the analysis phase of situation development. It also describes how information is converted to intelligence to satisfy the commander's PIR. Analysis in support of situation development continues the IPB process and portrays significant aspects of the enemy, weather, and terrain in support of the decision-making process. This portrayal is baeed on the analysis of information from all sources that previously has been recorded, cataloged, and evaluated in a manner to facilitate effective analysis. This intelligence data base is continuously updated to ensure the information in it is current and accurate.

Automation increases the capability to manipulate large volumes of information from many sources and assist in the analysis process. However, analysis continues to be a human function. Information is interpreted by an analyst who adds the element of judgment, which is essential "to effective intelligence analysis.

History provides many examples of intelligence failures that are directly attributable to faulty analysis by people. In some cases, the indicators were present, but were either not recognized or were misinterpreted due to the analyst's preconceptions of the situation. In others, the analysis was correct, but was not presented in such a way that decision makers would accept it.

The primary product of intelligence analysis is the intelligence estimate. The estimate provides the best possible answer to the commander's PIR that is available at the time. The estimate is dynamic, constantly changing with the situation. Thus, analysis is conducted continuously with the information available. The available information almost always is incomplete. The analyst uses what is known about the enemy, weather, and terrain from the IPB to estimate what is not known. In addition, the analyst determines the enemy's capabilities, which are the basis for predicting probable courses of action.

ENEMY CAPABILITIES

Enemy capabilities are courses of action which the enemy can take to influence the accomplishment of the friendly mission. They indicate--

- What the enemy can do.

- When the enemy can do it.
- Where the enemy can do it.
- In what strength the enemy can do it.

The PIR normally are about enemy capabilities. Estimates of enemy capabilities and their probability of adoption impact significantly on the friendly commander's scheme of fire and maneuver for accomplishing the mission. By integrating the enemy's tactical doctrine, characteristics of the AO, and time and space factors as developed through IPB, the analyst estimates enemy capabilities with a reasonable degree of confidence. Enemy actions that would have little effect on friendly operations, would not benefit the enemy, or are not tactically feasible are not considered enemy capabilities. For example, an enemy force normally disengages its troops in an adjacent area to free these for commitment within our sector or zone. However, in some circumstances, this is not a viable enemy option. Therefore, in those circumstances this capability normally is not considered as an option.

Generally, there are four tactical courses of action open to the enemy in conventional operations: attack, defend, reinforce, or conduct a retrograde movement. These are divided into a variety of more specific courses of action. For example, an attack may be a penetration, an envelopment, or other variations of an attack. A retrograde movement may be a delaying action, a withdrawal, or a retirement.

Some enemy capabilities refer specifically to the support of combat forces rather than the capabilities of the combat forces themselves. Support capabilities include--

- Use of NBC weapons.
- EW.

Support capabilities always are considered, especially when enemy implementation of them will significantly affect the accomplishment of the friendly mission.

The analyst considers when the enemy can implement a capability. Time is a critical factor in the Air Land Battle; the friendly commander relies on time to defeat enemy first-echelon forces before follow-on echelon forces are committed to the battle. The friendly commander needs an accurate estimate of when enemy forces are employed to decide how to fight the battle. The analyst considers the following factors in estimating when an enemy force will be employed:

- Mobility capabilities.
- Disposition.
- Doctrinal rates of movement.

- Characteristics of the terrain, LOC, trafficability, and obstacles.

- Time required for displacement, assembly, emplacement, and closing on the battle area.

Integrating information on the enemy and the battlefield environment determines where the enemy implements a capability. The enemy composition, disposition, and weapons and equipment dictate how well the enemy moves, shoots, and communicates--the activities vital to most enemy courses of action. Analysis of existing and forecasted weather conditions and military aspects of the terrain reveals how they affect enemy capabilities in various parts of the AO. AAs and MCS determine where the enemy moves on the ground. LZS and DZS determine where the enemy employs airmobile, air assault, or airborne forces. Suitable beaches determine where the enemy launches an amphibious assault. The location of suitable assembly areas, firing positions, and targets determines where the enemy launches NBC weapons. Also, the location of suitable defensive positions determines where the enemy defends. Terrain factor overlays, which are developed during IPB, identify specified aspects of the terrain. They help the analyst determine where the enemy implements various capabilities.

The strength in which an enemy implements a capability depends primarily on the composition, disposition, and strength of available forces. Chapter 3 describes the 06 files which provide the necessary data for computation. Appendix D describes how to compute enemy strength.

The IPB data base is the key in determining enemy capabilities. Doctrinal and situation templates assist the analyst in estimating enemy capabilities. The avent template and EAM help the analyst determine when and where the enemy can implement a capability. Using the working SITMAP, the analyst continuously monitors the enemy situation. The analyst compares the working SITMAP with IPB templates and adjusts the capabilities accordingly. The analyst also follows the friendly operation to determine which enemy capabilities have the greatest effect on the friendly operation.

ENEMY COURSES OF ACTION

The ultimate objective of intelligence analysis is to answer the PIR with an acceptable degree of confidence. This normally involves a determination of the enemy's most likely courses of action and the probability the enemy adopts those courses of action. Like capabilities, the analyst determines the enemy's probable courses of action in terms of what, when, where, and in what strength. The probable courses of action provide the basis for predicting enemy intentions. By accurately estimating the enemy's intentions, the analyst provides the answers to critical uncertainties which impact on the commander's tactical decisions.

indicators are the basis for situation development. The analyst integrates information from all sources to confirm indicators of enemy

activities. As indicators are detected and confirmed, PIRs are answered. Appendix C lists common indicators.

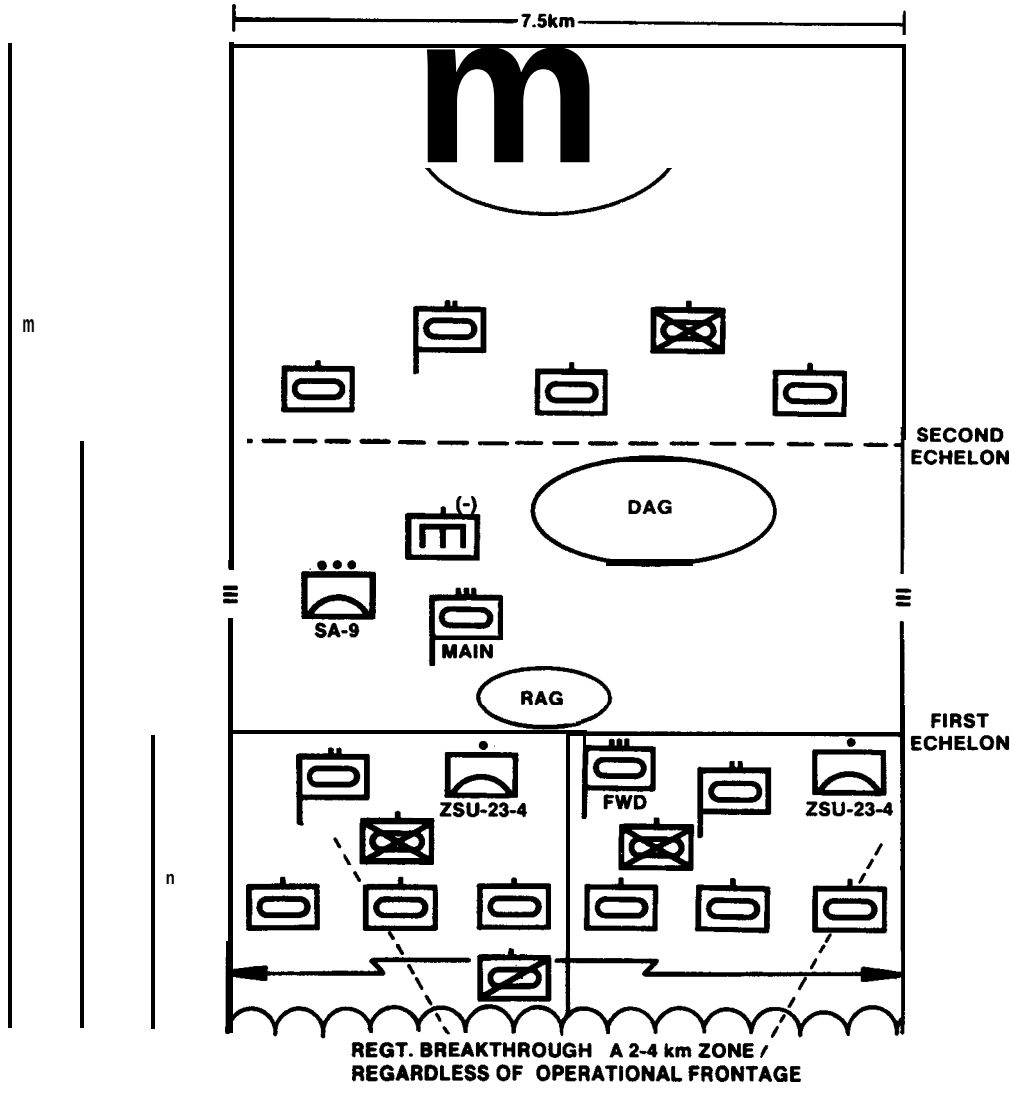
WORKING SITUATION MAP

The working SITMAP is the basic analytical tool at all levels. It provides a graphic presentation of the battlefield for the analyst, commander, and staff. The working SITMAP integrates significant information from all sources in a graphic representation that is easy to comprehend. All intelligence records are used with the working SITMAP to develop the enemy situation and intelligence estimate. The analyst posts all practical information to the working SITMAP. Such information may include strength, activity, or last known location. An "as of" time must always accompany map information. This allows outdated intelligence to be removed and assists in monitoring enemy progress. The analyst maintains separate records of information that cannot be posted and uses them to back up and expand the information on the working SITMAP. Other records normally are more permanent than the working SITMAP. The significant information about the enemy and the terrain becomes apparent when posted. The analyst uses the working SITMAP to--

- Identify critical relationships.
- Evaluate, compare, and integrate information and intelligence from all sources.
- Track enemy forces.
- Identify indicators.
- Wargame opposing courses of action.
- Identify uncertainties.

Critical relationships help to determine the composition of enemy units, assess their capabilities and probable courses of action, and identify exploitable weaknesses. The analyst identifies critical relationships by comparing separate items of information on the working SITMAP and by comparing the working SITMAP with other intelligence records.

By comparing known information about an enemy unit (posted on the working SITMAP) with the appropriate doctrinal template and the OB book, the analyst identifies unknown elements of an enemy unit. For example, if two motorized rifle battal ions (MRBs) of an MRR have been identified, located, and posted on the working SITMAP, the third MRB is most likely deployed nearby. The doctrinal template helps the analyst determine the most likely location of the third MRB. This comparison also helps the analyst identify and locate enemy HVTS I ike CPS and AD weapon sites. Figure 6-1 shows an example of a doctrinal template. Critical relationships become more apparent when the doctrinal templates are compared with known unit locations plotted on the working SITMAP. Further doctrinal templates of Soviet-style forces are available in GTA 30-1-24.



NOTE: For clarity, support units and observation posts are not depicted.

Figure 6-1. Doctrinal template tank regiment main attack (div slice).

The working SITMAP makes it easier to evaluate and compare information from different sources. The analyst compares incoming information with the information previously posted to the working SITMAP for compatibility with existing data. This comparison also helps to integrate new information with existing information and to determine its significance.

The working SITMAP provides a record of the latest location of enemy forces. As new information on enemy locations is received, the analyst compares it with information on the old location. This indicates the direction and rate of enemy movement. It also helps determine the accuracy of reports. For example, if the time a unit is observed in a new location (compared with the location and time the unit was last observed) indicates unusually rapid movement that significantly exceeds the doctrinal rates, the analyst is alerted to a problem. Either the old or the new report is inaccurate, or the two reports may not concern the same unit. It might alert the analyst to the possibility of an enemy deception operation. The analyst uses the IPB event template and EAM to project enemy movement. By comparing these with actual enemy movement as indicated on the working SITMAP, the analyst predicts the enemy's probable course of action and predicts when and where the enemy implements it.

The working SITMAP is vital in recognizing and evaluating indicators. Most indicators are associated with patterns of enemy activity, which become apparent on the working SITMAP. For example, an indicator of attack is the massing of artillery well forward. The working SITMAP reveals the location, density, and movement of enemy artillery. A careful analysis of the working SITMAP helps the analyst identify artillery groups, their composition, disposition, and location in relation to the FLOT. By comparing the working SITMAP with doctrinal and situation templates, the analyst better identifies significant patterns of enemy activity and associates them with specific indicators.

The working SITMAP is well-suited for wargaming opposing courses of action. Wargaming integrates friendly and enemy capabilities and possible courses of action with the weather and terrain. It helps both the operations and the intelligence staffs to analyze opposing courses of action. This is vital to preparing the estimate of the situation and the intelligence estimate. It also helps the analyst predict the enemy reaction to friendly courses of action.

The analyst uses the working SITMAP to clarify uncertainties. For example, if the analyst identifies two MRBs that are subordinate to a particular MRR, further knowledge of the enemy's organization tells the analyst that there is a third MRB that has not been located.

The IPB templates are important analytical tools when used with the working SITMAP. Comparison of templates and the working SITMAP systematizes analysis and increases the accuracy of the estimate. Situation and event templates depict projected enemy activities while the working SITMAP depicts the actual observed enemy activities. By comparing and integrating the two, the analyst predicts future enemy activities with greater accuracy.

FACTORS OF ANALYSIS

The analyst must understand the dynamics of the AirLand Battle to accurately analyze the forces that occupy it and the impact of the environment on those forces.

The analyst understands the enemy's tactical doctrine and the other forces that impact on the execution of that doctrine. The following suggestions are some techniques for developing enemy capabilities and the relative probability of their adoption. These techniques help the analyst use available information effectively to find the right answers to critical uncertainties.

The analyst considers the enemy's use of mass and economy of force. The enemy commander, like the friendly commander, has limited combat resources. The enemy commander uses mass and economy of force at the optimum times and places to accomplish the mission. Rather than dissipate the forces across the entire battlefield, the enemy commander weights the main effort to ensure combat superiority at the decisive time and place. Once the analyst determines how the enemy commander uses mass and economy of force on the battlefield, the enemy's most probable course of action becomes more apparent. The enemy uses follow-on echelons to mass combat power at decisive times and places on the battlefield. In the AirLand Battle, the analyst locates and tracks these enemy follow-on echelons and predicts where and when they will be committed. Situation and event templates used with the working SITMAP help the analyst predict where the enemy will mass.

On a nuclear battlefield, massing presents new opportunities and dangers. Nuclear weapons are substituted for massing of other forms of combat power, yet some concentration of enemy forces is required to successfully exploit strikes.

Analysts identify the composition of enemy force at least one echelon above their own. The mass and economy of force problem is resolved at each enemy echelon. The higher echelon commander's decision on a maneuver scheme and the allocation of combat power and support impacts directly on enemy capabilities within the analyst's unit's zone or sector.

Identifying the enemy composition facilitates construction of a composite picture of the total enemy force structure, including information on identified and unidentified units, located and unlocated units, total reinforcements, types and amounts of CS or CSS, and the availability of special capabilities (river crossing, EW, intelligence collection). In addition, detailed analysis of enemy composition assists in quantifying the degree of uncertainty that still exists. This judgment affects the degree of confidence an analyst has in estimating. Most intelligence judgments are inductive generalizations based on fragmentary evidence. By comparing available information with the composition and organization of the enemy force, the analyst determines what percentage of the total picture of the enemy force is known, and what percentage remains uncertain. For example, agencies report that four enemy artillery batteries have displaced forward. The analyst generalizes that enemy

artillery is displacing forward, an indicator of attack. However, if the composition of the enemy force indicates a total of 40 available batteries, the analyst must recognize that the judgment is based on only 10 percent of the picture. Ninety percent is still uncertain. It is vital that analysts be conscious of the degree of uncertainty remaining in the situation.

Analyze the significance of enemy activity outside your zone or sector . Consider the big picture when assessing the meaning and significance of enemy activity in your AO. Enemy boundaries are not identical to friendly boundaries. Events outside your boundaries may be part of the enemy commander's scheme of maneuver. Analysis of events outside a unit's AO provides indicators or helps focus the collection and analysis efforts within that unit's AO. Events that occur within a friendly unit's AO require correlation with events outside the AO if they are to be correctly interpreted. This is related to and facilitated by the determined composition of the opposing enemy force.

Review enemy tactical doctrine. Enemy commanders are trained to follow their own tactical doctrine. Though some enemy commanders are more or less innovative, most consciously or unconsciously apply doctrine when confronted with a specific mission, threat, and AO.

Enemy tactical doctrine presents many of the indicators of enemy capabilities and probable courses of action. It relates directly to how the enemy uses mass and economy of force in operations.

The enemy's tactical doctrine is depicted on doctrinal templates when possible. Doctrinal templates depict unit formations; frontages and depths for attack, defense, and other operations; characteristic dispositions associated with particular courses of action; allocations of CS and CSS; and information on specialized military operations like river crossings and air assault operations. Event templates depict the doctrinal sequence in which the enemy conducts operations. The IPB templates and the working SITMAP are the basis for comparing the enemy's tactical doctrine with actual events.

Consider how the weather and terrain affect enemy capabilities and the enemy commander's choice of a course of action. Weather and terrain are physical constraints which facilitate or alleviate the adoption of specific courses of action. These constraints have a major impact on how the enemy commander allocates resources. Weather and terrain force enemy commanders to apply special methods of operations. They may require changes in weapons and equipment or in the way they are used. The weather and terrain may give rise to new force structures and organizations.

Paragraph two of the intelligence estimate addresses the effects of the weather and terrain on friendly and enemy operations (see Appendix A). Through continuous IPB and analysis, the analyst relates the enemy force structure and tactical doctrine to the constraints imposed by the weather and terrain, particularly on the AAs.

To relate enemy dispositions and physical constraints of the weather and terrain, there are four specific techniques used to determine how the enemy appl ies mass and economy of force.

The first technique is to determine the enemy unit boundaries and relate them to AAs. Boundaries frequently are identified through the location of enemy reconnaissance and cavalry units (which often have distinctive, easily identified equipment), terrain and doctrinal analysis of enemy prisoner of war (EPW) capture locations, and other techniques. This technique helps determine mass and economy of force and the enemy commander's perceptions of AAs.

The second technique is to compute enemy strength in terms of committed forces, reinforcements, and supporting weapons for the entire AO, then recompute for each AA. Determine whether enemy combat power and support are distributed evenly or whether one option is weighted. Appendix D describes how to compute enemy strength.

The third technique is to analyze enemy allocations of available LOC. Military forces usually allocate roads to tactical units for logistical support and tactical movement. If this allocation is determined through analysis of enemy boundaries and traffic patterns, it indicates the enemy's probable course of action and assists in identifying enemy support priorities.

The final technique is to identify potential enemy objectives and relate them to enemy dispositions and AAs. Determine which avenue is weighted by locating unit boundaries, computing unit strength, identifying allocation of LOC, and identifying the distribution of combat power.

TECHNIQUES OF ANALYSIS

The following techn iques of analysis helps the anal yst identify the presence of indicators.

PATTERN ANALYSIS

Pattern analysis helps the analyst identify indicators of enemy activity. Pattern analysis is based on the premise that the enemy's course of action results in certain characteristic patterns that are identified and correctly interpreted. Ideally, paragraph 3d of the intelligence estimate (Appendix A) should identify the presence of these indicators. The analyst is faced with the problem of organizing and recording incoming information and adding it to existing information so that meaningful relationships are clarified. The working SITMAP and IPB templates are the primary tools used to organize information. Indicators can be ambiguous and incomplete. The analyst identifies the patterns of activity or tip-offs which characterize the operations of specific enemy units.

WEIGHTING INDICATORS

Weighting indicators helps resolve ambiguity. In combat, intelligence analysts usually are confronted with conflicting indicators. Enemy forces may portray patterns associated with attack, defense, and delay simultaneously. Conflicting indicators result from--

- Deliberate deception.
- Bad execution.
- Temporary indecision.
- Transition between missions.
- Random activity.
- Incomplete or inaccurate information.
- Ambiguity of the indicator itself.

When confronted with ambiguous or conflicting indicators, analysts weigh some indicators more heavily than others to determine the enemy's actual intent. This is not a problem of simple mathematics. The enemy's actual course of action may not have the most indicators. Analysts develop a methodology for identifying those indicators which are most highly characteristic of a course of action. There are several techniques which, individually or in combination, assist in this process.

Origin of the Indicator

One technique of determining the enemy's intent is to consider the origin of the indicator; that is, the reason why the enemy force presents a particular pattern or tip-off. In brief, all indicators stem from either military logic, doctrinal training, organizational constraints, bureaucratic constraints, or the personality of the enemy commander.

Military Logic. Military logic implies, and military experts agree, that solutions to many military problems are obvious. For example, all modern armies employ artillery forward for attack and echeloned in-depth for defense. Violation of military logic usually implies the loss of combat power or support at some critical point during an operation.

Doctrinal Training. A nation's tactical doctrine includes military logic and much more. Most doctrine begins where military logic ends. Military experts sometimes disagree on the ideal solution to a specific military problem. For example, US and Soviet doctrine agree on deploying artillery forward in the attack, while they disagree on using artillery in a direct fire role. Just as terrain and weather are physical constraints on the enemy's adoption of a course of action, enemy doctrine and training are mental constraints. Soviet emphasis on detailed, repetitive training is designed to inbreed a sort of reflex action which enhances the value of doctrinal indicators. Though individual commanders display more or less

imagination and creativity in its application, indicators based on doctrine and training are generally reliable.

Organizational Constraints. Organizational structure represents a special case of doctrine. The ideal composition of a division (size, organization, weapons, and organic support) is debatable. The military experts have resolved this issue in radically different ways. Organization influences include a nation's strategic commitments, economic resources, geography, threat perceptions, historical experience, alliances, personnel and equipment resources, and a myriad of other factors. The tactical organization resulting from these factors causes identifiable patterns to develop when employed. A US division generally has three subordinate maneuver headquarters contrasted with four in a Soviet division, and differences in the composition and structure of the division base imposes distinct patterns concerning US and Soviet operations.

Bureaucratic Constraints. Identifying bureaucratic constraints as a source of indicators shows that military units are large organizations and must establish routines and SOPS to function efficiently. This imposes patterns in planning, execution, logistics support, and other activities, though there are general similarities in routines and procedures of comparable units, there are likely to be significant variations which can be identified and exploited locally.

Personality of the Commander. The enemy commander is the final source of indicators. Each commander has a unique history of personal training, experience, success, failure, and idiosyncrasies. Many are creatures of habit, prone to repeat what has worked in the past; others are creative and innovative. All are captives of their experience to some degree. It is the commander who must apply. and mix military logic, doctrine, and organization to accomplish the mission. The commander's personality is one major source of deviation from established doctrinal norms, The importance of personality is recognized in that biographic intelligence is a major component of strategic intelligence. US tactical OB doctrine classifies personality as a subcategory under miscellaneous factors.

In general, indicators are weighed, with the role of the commander being considered a variable. In the case of a strong, innovative, or eccentric commander (Patton or Rommel), personality is more important than doctrine or training; while the personality of a methodical, traditional commander ranks last.

Principle of Mass Indicators

Another technique is to weigh the indicators which reflect or are based on the principle of mass. Military units normally conduct deception operations with the same force constraints in which they accomplish their actual mission. The enemy commander often conducts deception with the least outlay of scarce resources. Indicators based on a major confirmed commitment of combat resources are more likely to reflect the true situation. In a nuclear environment, massing is not required to achieve a favorable combat power ratio; thus, mass is not a reliable indicator.

Analysts identify the enemy's capability to concentrate fires of potential nuclear del ivery systems.

Other Indicators

The last technique is to weight those indicators which are most difficult to fake.

Quantify Probable Relationship. Quantify the probable relationship between the presence of specific indicators and the enemy's adoption of a particular course of action. If the enemy commander intends to adopt a particular course of action, what is the probability that a specific indicator is present? The answer is subjective, but it is based on the analyst's knowledge of and experience with the enemy, the analyst's professional judgment, and to some degree, the mathematical probability of specific indicators associated with enemy courses of action.

Analyze the Time Sequence of Events. It takes time for an enemy force to prepare, move, and execute an operation. Time, mass, and space relationships are a major tool in exposing deception. Since deception is often conducted with the least outlay of combat resources, close analysis of information from different sources which report on the same location, at the same time, or concerning the same enemy unit may reveal significant discrepancies.

Assess the Enemy's Combat Effectiveness. Such assessments are based on an analysis of both tangible and intangible factors. Tangible factors include personnel and equipment strength. Intangible factors include morale, training, political reliability, and other factors. While combat effectiveness bears directly on a unit's capabilities and probable courses of action, there is no scientific method of determining it. It requires the analyst's subjective judgment of the impact of both the tangible and intangible factors.

WARGAMING FRIENDLY AND ENEMY CAPABILITIES

Consider the enemy G2's perception of the friendly force. Though enemy capabilities exist independently of their assessment of friendly forces, the enemy's choice of alternative courses of action does not. Determine the enemy's perception of friendly capabilities through analysis of the collection capabilities, known collection activities, and inadvertent disclosures by friendly forces which might have been monitored by enemy intelligence. Detailed analysis of potential disclosure enables the analyst to partially reconstruct the enemy G2's working SITMAP.

Mentally wargame advantages and disadvantages of identified enemy capabilities from the enemy commander's point of view. This is a valuable analytical technique, but potentially dangerous if it becomes mirror-imaging.

Avoid preconcert ions. The analyst must remember that the objective is not to prove a prior judgment. Experience suggests that preconceptions are the analyst's pr incipal nemesis. Even if the techniques recontnended

above are creatively employed, there is a danger that the analyst who has reached and expressed a preliminary judgment unconsciously begins to seek and weigh evidence which confirms the initial estimate and dismisses or passes over inconsistent or conflicting information. The analyst should not be concerned about the answer, as long as it is the right answer. The analyst reserves judgment, maintains objectivity, remains aware of uncertainties, tolerates dissent, and constantly tests working theory against available evidence. Where practical, the analyst considers establishing a "devil's advocate" system to test, challenge, and think the unthinkable.

CHAPTER 7

TARGET DEVELOPMENT

Targeting is the process of selecting targets and matching the appropriate response to them taking into account operational requirements and capabilities. An efficient, organized targeting effort is critical to the success of AirLand Battle operations. A target is a geographical area, complex, or installation planned for capture or destruction by military forces. Attacking HPTs that are least affordable to lose, strips the enemy of the initiative and forces the enemy to conform to friendly battle plans.

Targeting has always been a complex effort. Large numbars of sensors under the control of different agencies are closely coordinated to be efficient and must rapidly report fleeting or dangerous targets. The wide variety of attack means and munitions are compared to the particular vulnerabilities of many different types of targets. Targeting is a multidisciplined effort, requiring interaction between FS, intelligence, EW, operations, and plans cells.

The object of targeting is to disrupt, delay, or limit those enemy capabilities which could interfere with the achievement of friendly objectives. Do not confuse disrupt, delay, and limit with suppress, neutralize, and destroy. The latter relate to the amount of damage inflicted upon a target. Disrupt, delay, and limit apply to the effect that the damage has upon the target as it pursues a course of action. A further clarification of disrupt, delay, and limit is available in Annex A to FM 6-20-10. The staff recommends how a target is engaged.

Targeting is based on the friendly scheme of maneuver and tactical plans. It includes an assessment of the weather, terrain, and enemy to identify those enemy formations, equipment, facilities, and terrain which are attacked or controlled to ensure success. Targeting is an integral part of the planning process which begins with the receipt of a mission and continues through the development of the approved plan. The targeting process includes the development of a prioritized list specifying what targets are to be attacked, and what is required to defeat the target. Figure 7-1 shows the staff functions during the targeting process.

This process supports the commander's decision on which broad attack option to use to engage the targets: maneuver, EW, FS, or a combination thereof; and the determination of the echelons that engage the target. An assessment of the attack is then conducted to determine the effectiveness of the targeting process. Although the targeting process is more cornnonly associated with high and medium intensity conflicts, it also applies to LIC. While spread sheets and target sheets currently do not exist for LIC, the concept of key personnel meeting together to determine the most important targets to strike in support of the friendly maneuver commander HVTS and to detect and attack those targets still applies. The targeting methodology is characterized by three functions: decide, detect, and deliver. These three functions are inherently intertwined. Figure 7-2 shows the three functions of the targeting process.

Receive guidance on:

Commander's intent.
HPT.
Attack criteria.
Lead time between decision points and TAIs.

Develop:

Future MCOO.
Situation and event templates.

Explain enemy courses of action as part of wargaming. Based on friendly courses of action, refine event template. Assist in development of HPT matrix and target selection standards.

Based on commander's approval or changes of CoA, HPT, attack guidance:

Publish collection plans and SORs.
Brief ASPS, CM&D, TCAE, as appropriate on CoA, HPT, TSS, attack guidance.
Ensure all analysts and collectors understand commander's intent.

Collect information.
Pass HPT related information and intelligence immediately to FS.
Pass other intelligence and target damage assessments per SOP.
Ensure information collection and intelligence production supports any FRAGOs.

Figure 7-1. The targeting process checklist.

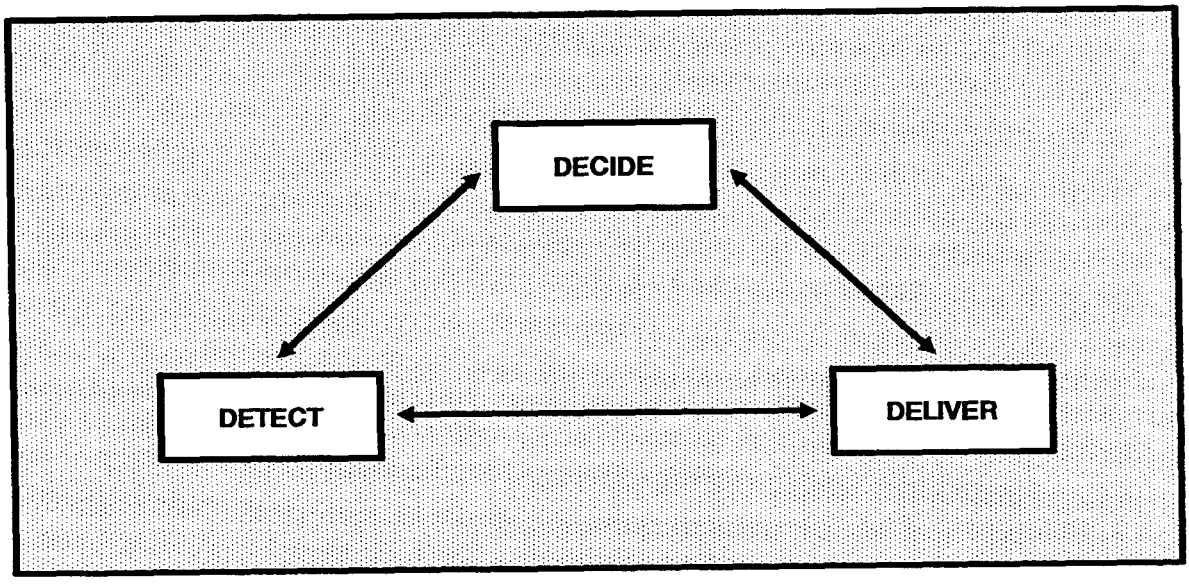


Figure 7-2. Targeting process.

The DECIDE function is the planning associated with a successful targeting effort. It requires close interaction between the commander, intelligence and operating staffs, FS personnel, and various other CS agencies. The staffs must have a clear understanding of the unit's mission, the commander's concept of the operation and intent, and the commander's initial planning guidance with respect to target priorities. With this information, the staff officers prepare their respective estimates. From the standpoint of targeting, the FS, intelligence, and maneuver estimates are interrelated and require close coordination between the respective elements. The DECIDE function provides a clear picture of the targeting priorities applicable to the tasking of TA assets, information processing, the selection of an attack means, and the requirement for post attack assessment. Specifically, the DECIDE function is designed to answer the questions:

- What is it we need to look for?
- Where and when can it be found?
- Who can locate and identify it?
- Which attack option should be used?
- Will target damage assessment (TDA) be required or possible?

In the DETECT function, the priorities developed in the DECIDE function are translated into the TA taskings found in the subordinate unit's portion of the OPORD and in intelligence and FS annexes. All TA assets available to the commander are fully utilized. As the TA assets gather information, they report their findings back to their controlling headquarters which in turn pass pertinent information to the tasking

agency. The information gathered is processed to produce valid targets. Not all the information reported benefits the targeting effort, but it may be valuable to the development of the overall situation. The target priorities developed in the DECIDE function help to expedite the processing of targets. As these targets are developed, appropriate attack systems are tasked in accordance with the commander's guidance and requirements of the attack system managers.

The DELIVER function is the execution portion of the targeting process. It consists of the selection of the appropriate attack means for a given target, the tasking of that attack system, and the execution of the attack by the specified means. If TDA reveals that the commander's guidance has not been met, then the entire targeting process continues focusing on this target.

The targeting effort is continuous. The intelligence, operations, and FS officers comprise the core of the effort at all echelons. Other staff officers that are involved with planning and controlling of firepower and TA also participate. The other staff officers that assist in the process include representatives of the Air Force (AF), the staff weather officer (SWO), the aviation officer, the chemical officer, the Army airspace control officer, the EW staff officers, and the engineer.

The rest of this chapter describes, in detail, the functions required to plan and engage targets successfully using the DECIDE-DETECT-DELIVER methodology.

DECIDE

Decisions are critical to the targeting process. They create the guidelines for the acquisition and engagement of targets. Establishing these guidelines at the beginning of the DECIDE function allows for a unity of effort and efficiency that would otherwise not be achieved.

The decisions that are made are reflected in visual products. The decisions made are what targets should be acquired and attacked, where and when will the targets likely be found and who can locate them, how the targets should be attacked, and is TDA required. The products are the HPT matrix (what targets should be acquired and attacked), target selection standards (TSS) (what assets can produce targets), the collection plan (where and when should targets be found and who can find them), and the attack guidance matrix (how targets should be attacked). The collection plan is a G2 or S2 product that is important to the targeting process but is not discussed in detail in this chapter. See FM 34-2 for discussion of collection plans.

The commander and staff plan for future operations by projecting one or more alternative courses of action based upon a mission analysis, the current and projected battle situation, and anticipated opportunities. IPB is an important process that assists the commander and staff in developing courses of action.

The process begins with the receipt of a mission, which higher headquarters assigns or the commander deduces. The mission statement directs the focus toward a course of action, in a particular area, against a specific enemy. The commander then, either with or without input from the staff, performs mission analysis. This analysis considers tasks that are performed, the purpose behind the tasks, and the constraints on the unit, resulting in a restated mission.

The restated mission provides the basis from which to start the staff estimate process. The intelligence estimate provides key support to target development. Target development is one of the four IEW tasks: situation development, target development, EW, and CI.

IPB AND TARGET DEVELOPMENT

IPB provides most of the information for the intelligence estimate which impacts on the target development process. IPB is a continuous, systematic approach to analyzing the enemy, weather, and terrain in a specific geographical area. This approach evaluates enemy capabilities and predicts enemy courses of action with respect to specific battlefield conditions.

It is important for the analyst to understand the effects of battlefield conditions, especially obscurants, on targeting. Such conditions drive the need for remote sensors and redundant systems to ensure proper coverage. The analyst must "see" the battlefield as it is, and not just as it appears on a map.

The initial IPB effort produces doctrinal templates which convert enemy OB into graphics and aids in the initial identification of potential HVTS. HVTS are those assets that the enemy commander feels are critical to the successful accomplishment of the mission.

Situation templates assist the refinement of HVTS for specific battlefield and courses of action. Concurrent with situation template development is an examination of enemy decision and logic trees associated with each potential course of action. This identifies likely "fail paths" that provide indications of what might happen if the enemy commander's plan fails and what actions comprise the enemy commander's failure options. The "fail path" evaluation leads to an identification of critical enemy functions associated with each enamy course of action and general HVTS associated with each function. Through BAE, terrain evaluation, and weather analysis, the enemy course of action is associated with a specific battlefield. Situation, event, and decision support templates are developed to identify critical enemy activities and any NAIs where specific enemy activities or events or lack therefore wil 1 help to confirm or deny the enemy's adoption of a particular course of action. Additionally, DPs or decision phase lines, TAIs, and HPTs are identified. HPTs are those HVTS that are acquired and successfully attacked to ensure the success of the friendly commander's mission.

TARGET VALUE ANALYSIS

IPB analysis considers terrain, weather, enemy doctrine, and current enemy actions to arrive at conclusions of what the enemy will do; the courses of action. Target value analysis (TVA) is a methodology which identifies potential HVT sets within a given tactical situation. If successfully countered, they provide a tactical opportunity. This methodology provides a relative ranking of worth of target sets. TVA begins when the analyst adopts the place of the enemy commander. The analyst, in coordination with the G3 or S3, FSO, and other staff members, wargames the operation. The purpose of wargaming is to finalize individual staff estimates and to develop a friendly and enemy DST. A by-product of this is the determination of the enemy assets that are critical to the success of the enemy mission--HVTS. Target spread sheets and target sheets are tools used in identifying HVTS. The information found on these documents is produced during the IPB and wargaming process. More information on the development and use of these targeting tools is available in Annex A of FM 6-20-10.

HVTS and HPTs

An HVT is a target whose loss to the enemy can be expected to contribute to substantial degradation of an important battlefield function. HPTs are HVTs which, if successfully attacked, contribute substantially to the success of friendly plans. The G2 or S2 section, together with the FSO and other staff, nominate HVTS to be HPTs. The key to HPTs is that they are based on the friendly concept of the operation and support the friendly force commander's scheme of maneuver. The development of HPTs from HVTS is done during the wargaming process. As the different options are fought by the staff, the G2 or S2 identifies specific HVTS. The staff discusses or wargames different courses of action to develop the HPTs. The HPTs for a specific phase of a battle are recorded on the DST as are the means decided on to deliver the attack. HVTS include enemy C^2 points, air defense artillery (ADA) assets, and engineering equipment. If friendly forces were planning an air attack the enemy C^2 and ADA might be HPTs, while engineers probably would not. Discussion on templating and IPB is available in Chapter 4 and FM 34-130.

The process of designating an HVT as an HPT requires careful staff coordination. The G2 and collection manager evaluate HVTs at different points in the battle to determine if collection assets are capable of detecting them and providing the necessary target resolution, for example, time, location, and so forth, to permit effective action (DELIVER). HPTs, because of their importance, receive priority in the allocation of detection systems. This priority is weighed against the same systems for situation development.

The FSO uses target sheets and the knowledge of friendly weapons systems to determine if there exists a capability to attack the HVT with lethal assets. The EW officer and others assist the FSO with regard to non-lethal systems. Availability of a weapon system should not affect the attack since HPTs have precedence over other targets. Using the capabilities of the systems to attack the targets, the G2 or S2 analyzes

and predicts the enemy's response to each. This analysis determines if the attack of the HVT is necessary to ensure the success of friendly operations. The commander uses it in developing attack guidance. The HVTs that meet the criteria of being acquirable, attachable, and capable of ensuring friendly success are designated HPTs. In most instances, the analyst chooses to target enemy elements that have been designated "critical nodes."' A critical node is an element, position, or corrrnunications entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations. HPTs are formatted for easy reference in an HPT matrix. The G3 or FSO prepares this matrix and gives it to the commander for approval . The selection of HPTs, which also are critical nodes, are facilitated by a number of already existing enemy studies. Selection of these critical nodes, coupled with other TVA efforts, al lows friendly forces to best determine those enemy elements which are HVTS or HPTs.

TARGET SELECTION STANDARDS

TSS are criteria by which personnel determine which systems produce valid targets, and which require some form of confirmation before their targets are considered for attack. The development of TSS is a joint function of the G2 and G3 sections and requires that the capabilities and limitations of collection assets be known. The CM section of the G2 provides the majority of these capabilities and limitations.

TSS do not determine that the information that the sensor receives is, in fact, a target. The analyst determines that. TSS reflect the system's capabilities to produce targets. TSS are dynamic. The effects of weather and terrain on both the Collection assets and enemy equipment are taken into account. TSS are keyed to the tactical situation. Great care is taken to deal with potential enemy deception, and to ensure the reliability of the source or agency that is reporting. TSS are designed to allow targeting personnel in the TOC to readily distinguish between targets and suspect reports. TSS are developed for all TA systems available.

Target location errors (TLEs) are the accuracies to which the assets can locate various targets. The source's TLE and the timeliness of information are considered. It is an inherent responsibility for the FSE to decide which systems have acceptable TLEs for targeting purposes in a specific tactical situation.

ATTACK OPTIONS

Knowing target vulnerabil ities and the effect an attack on them has on an enemy operation al lows a staff to propose the most efficient available attack option. A primary decision here is whether to disrupt, delay, or limit the enemy.

The opportunity to disrupt, delay, or limit is annotated next to the target sets on the target spread sheet. It is emphasized that these are guidelines and each target is attacked based on its own merits.

Once the staff decides whether a target is best disrupted, delayed, or limited, they select attack options. Utilizing the situation template and MCOO, the risk to an asset versus its effectiveness is assessed. The decision on what attack option to use is made at the same time as the decision when to acquire and attack the target. Coordination is required when an attack with two different means, for example, EW and CAS, is decided upon. These decisions are recorded on the DST and are made during the wargaming process. This requires that the proper coordination be performed in a timely manner.

ATTACK GUIDANCE

The commander approves the attack guidance, as recommended by the staff. This guidance details the specific HPTs to attack, when and how they should be attacked, and any attack restrictions, The staff developed and defined all this information during wargaming. Figure 7-3, the attack guidance matrix, shows a format that this information is put in. The matrix consists of a column for target categories, specific HPTs, how targets should be attacked, when they should be attacked, any restrictions. For a detailed explanation on using the attack guidance matrix, refer to FM 6-20-10.

DETECT

DETECT is the next critical function in the targeting process. This function is perhaps the most important area for future planning. The G2 or S2 is the principal figure in directing the CM effort to detect the targets identified in the DECIDE phase. The G2 or S2 works closely with the FAIOs and FSOS to determine requirements for accuracy, identification, and timeliness for collection systems. The intelligence section is responsible for ensuring that the collection system asset managers understand these requirements.

TARGET DETECTION MEANS

The detection of targets is accomplished using all available assets. Key to the detect function is a focus on the HPTs designated during the DECIDE phase of the targeting process. This is accomplished by the CM section of the G2. Every targeting asset is aware of what the commander designates as HPTs.

Field Artillery Target Acquisition Means

Several detection assets are presently organic to the FA at both corps and division.

Field Artillery Battalions. FA battalions in DS of maneuver brigades provide each maneuver battalion headquarters with a FSE to help plan, direct, and coordinate FS operations. The FSE provides fire support teams (FIST) to each of the maneuver battalion companies. Forward observers (FOs) from each FIST are deployed at both company and platoon levels and may accompany reconnaissance patrols or help to man observation posts

CAT		HPT	WHEN	HOW	RESTRICTIONS
(C3)	1	46, 48	I	N EW	COORD ATK WITH EW
(FS)	2	1, 2, 7	A	N	DNE MRL OLDER THAN 10 MIN.
(ADA)	3	58	P	SIG 2	SEAD PROGRAM 120800A
(ENGR)	4		P	N	COUNTERMOBILITY PROGRAM %
(RSTA)	5	85	P	EW	
(REC)	6	103, 105	P	N	
(POL)	7		A	D	ACCY 0-200 M PER TDA REQ
(AMMO)	8		A	D	
(MAINT)	9		P	25%	NOT HIGH VALUE OR PAYOFF
(LIFT)	10		P	N	NOT HIGH VALUE OR PAYOFF
(LOC)	11		P	N G3	NOT HIGH VALUE OR PAYOFF

CAT	=	Target Category (from TVA)
HPT	=	Designated high payoff target; these targets have priority for engagement. Target numbers from TVA target sheets
How	=	How target is attacked
	—S:	Suppress
	—N:	Neutralize
	—D:	Destroy
	—EW:	Jamming or other offensive EW means
	—X%:	Specified percentage of casualties or damage
	—G2:	Coordinate attack with G2 (any other person or element could be indicated)
When	=	When the target should be attacked
	—I:	Immediately. Interrupt other nonimmediate attacks if necessary
	—A:	As acquired. Attack as assets are available
	—P:	Plan. Include target in a program of fires or file for later attack when the situation changes
Restrictions	=	Any constraint on the attack of targets. Such constraints could be accuracy, time since acquisition, required coordination, or munition restrictions by amount or type. Other notes such as "TDA requires" or "Missile target only" could be included.
	DNE:	Do not engage
	—	Other abbreviations could be used as required by unit mission or SOP.

Figure 7-3. Sample attack guidance matrix.

(OPs). They are the grass roots of the FA's TA effort. They observe the battlefield to detect, identify, locate, and laser designate targets for suppression, neutralization, or destruction. They report both target ing data and combat in formation to the maneuver battalion FSO and S2 using either organic or supporting communications means. The capability of the F1ST to provide real time combat information cannot be emphasized enough. The battalion FSO receives in formation from and passes information to the FIST. The FSO continually exchanges targeting data and combat information with the brigade FSO and elements from the DS FA battalion. The FSO coordinates with the battalion S2 and S3 to identify and verify targeting data and combat information derived from the overall collection effort. The FSO is both a producer and a consumer of combat information.

Radar Assets. FA TA assets are the principle means for locating active indirect fire weapons.

Moving target-locating radar (MTLR) detects, locates, and identifies wheeled vehicles (light or heavy), tracked vehicles, and dismounted personnel . MTLR is used for surveillance of critical areas such as AAs. Mortar locating radar detects and locates enemy mortars and artillery quickly and accurately enough for immediate engagement.

The DS FA battalion S2 has staff supervision responsibility for the radar. This officer coordinates with the division artillery (DIVARTY) targeting officer, the DS FA battalion S3, and the FSO at the maneuver brigade to ensure that both FS and maneuver coverage requirements are met. Cueing instructions are required. MI sources provide specific guidance to orient radar assets before the enemy fires.

Combat Observation Laser Teams (COLTS). COLTS organic to each heavy and light division provide a TA capability previously not available on the battlefield. They are equipped to direct the engagement of targets.

Aerial Fire Support Officers. Aerial FSOS and TA aircraft are organic to the division and the corps. These assets are highly mobile and cover a much larger area than ground observers. As such, they are particularly good target detection assets. Targeting data and combat information are reported to the FSO at the maneuver brigade or battalion, the DIVARTY TOC, or the fire direction center of the DS artillery battalion.

Air Defense Artillery TA Assets

The forward area alerting radar (FAAR) of the AD units provides a deep look capability that can detect the location and movement of enemy air assets. The integration of corps and theater AD efforts enable friendly forces to obtain an air picture that can potentially cover the entire area of interest for the echelon in question. Future concepts allow input directly from theater AD assets into division air situation updates. Collation of this AD information with other combat information enables us to locate major enemy air assets, airfields, and refuel ing and rearming points. Many of these become HPTs in support of the friendly scheme of maneuver.

DETECTION PROCEDURES

The collection of combat information is integral to the entire DETECT process. It is essential that all TA assets be used in the most effective and efficient manner possible. Avoid duplication of effort among the various assets unless such duplication is desired to confirm the location or nature of a target. At corps and division, the CM&D section develops and actively manages the collection plan to avoid such duplication. At the same time, the CM&D section ensures that no gaps in planning collection exist. This allows timely combat information to be collected to answer the commander's intelligence and TA requirements. This combat information enables analysts to develop the enemy situation as well as conduct target development.

To detect the desired HPTs in a timely, accurate manner, clear and concise taskings are given to those TA systems capable of detecting a given target. The FS personnel provide the G2 or S2 with the degree of accuracy that the targets must be located with to be eligible for attack. The G2 or S2 matches accuracy requirements to the TLEs of the collection systems. This matching allows the G2 or S2 to develop a more detailed set of TSS based not only on the acquisition system but also upon the HPTs' acceptable TLEs that the G2 or S2 gives. These acceptable TLEs cannot be placed in an SOP as they depend on the situation. Collection efforts focus on those NAI and TAI that the IPB process identifies during the DECIDE phase. Knowledge of the target type and its associated signatures (electronic, visual, thermal) enable friendly forces to direct the most capable collection asset to be tasked for collection against a given target. The asset is positioned in the most advantageous location based on friendly estimates of when and where the enemy target is located.

The decision to limit, disrupt, or delay a given HPT results in a requirement to detect that target. Information needs, to support the detection of the target, are expressed as PIR and IR. Their relative priority is dependent on the importance of the target to the friendly scheme of maneuver coupled with the commander's intent. The PIR and IR that support detection of a target are incorporated into the unit's overall collection plan. The collection manager translates the PIR and IR into SIRS. The collection manager considers the availability and capabilities of all collection assets within their echelon as well as those assets available to subordinate, higher, and adjacent units (to include joint or combined force assets).

As various assets collect the combat information to support target development, this information is forwarded through the IEW system to the intelligence analyst at the G2 or S2 staff. The analyst uses this combat information to perform both situation and target development. When the analyst detects a target, the target is passed immediately to the FS element to determine if the target is an HPT, its priority, and if it meets the TSS. Close coordination among the intelligence staff and the FSCOORD is essential to ensure that these targets are passed to an attack system which engages the target. To ensure that this occurs in a timely manner the FAIO must have access to the ASPS. One technique is for the FAIO to be physically located in the ASPS or CM&D. Procedures are estabI ished for cueing the FAIO as the predesignated HPTs are identified. ASPS personnel are aware of HPT. When an HPT is discovered it is passed without delay to FSE personnel . Usually, a member of the ASPS hand-carries the intelligence. This allows for consultation at a map and for intelligence to be placed into context with the overall situation. The FAIOs coordinate with their respective G2s and FSES to paes the targets directly to the fire control element at the DIVARTY TOC or, if the commander approves, directly to a firing unit. This results in the most efficient and timely engagement of those targets which the FS has designated in advance for engagement.

The passing of targets and suspect targets to the staff is accomplished by a number of means. It is important that essential. Information that is passed for proper analysis and attack takes place. As a minimum, the target report includes:

- Date-time group (DTG) of acquisition by the sensor.
- Description of the target.
- Size of the target.
- Target location.
- TLE.

The specific forms and formats for passing target information are specified in the unit SOP.

The DTG is important as the target's perishability or vulnerability window is analyzed. This impacts on the urgency of the attack or the denial of attack based upon the likelihood of the target having moved.

The target description and target size are required to determine attack means, intensity of attack, number of assets to be corrrnitted, plus other technical considerations. They are used to compare with the attack guidance matrix. The target's location is given as accurately as possible within the confines of timeliness.

DELIVER

The DELIVER portion of the targeting process executes the target attack guidance and supports the commander's battle plan once the HPTs have been located and identified. This portion of the process has two key elements--the attack of targets and the TDA of those targets.

ATTACK OF THE TARGETS

The attack of the targets satisfies the attack guidance that was developed in the DECIDE portion of the targeting process. The attack of targets requires a number of decisions and actions. The decisions are described as a set of tactical and technical decisions. Determining the time for the attack, the attack system, and the required effects on the target are the tactical decisions to make. Based upon these tactical decisions, the technical decisions describe the precise attack means, the unit to conduct the attack, the time of the attack, and in the case of FS assets, the number and type of munition. The actions in the attack of the targets are the actual physical attack of the targets by lethal or non-lethal means. The time of attack of the target is planned or by opportunity.

Planned Targets

Planned targets are evaluated initially to determine if the DF has been reached or a trigger event has occurred. If either of these has

occurred and the resources that were identified to be used against the target are available, the target is attacked. If the decision is to attack now, a check is made to determine if the attack system, that we earlier allocated for the attack of that target, is available. If so, the attack is conducted with that system. If the allocated attack system is not available, a decision is made on which other attack asset to use. If the decision is made to defer the attack, the staff identifies the new DP to the intelligence or acquisition system.

Targets of Opportunity

Targets of opportunity are evaluated initially as to when they should be attacked. This decision is based on a number of factors such as the activity of the target, how long the target can be expected to stay in its current location (target perishability) and the target's payoff, relative to the payoff of the other targets currently being processed for engagement. If the decision is made to attack now, the target is processed further. If required, additional information is requested from the intelligence or acquisition systems. If the decision is made to defer the attack, then a DP is determined and described to intelligence or acquisitions systems. Additionally, an assessment of the availability and capabilities of attack systems to engage the target is made. If the target exceeds either availability or capability of the unit's attack systems, then the target should be nominated to a higher headquarters for attack.

DESIRED EFFECTS

The desired effects on the target are determined. As mentioned earlier, we either delay, disrupt, or limit the target, based either on time or terrain, This determination was made earlier in the case of planned targets. For targets of opportunity, the staff makes the determination. This decision is made based on the payoff of the target and the constraints on availability of attack systems and munitions. The determination of the desired effects is required before selecting an attack system.

TARGET DAMAGE ASSESSMENT

Assessment of the effects of an attack always is desirable and is required for certain important targets. The same assets that acquire targets often provide data on the effectiveness of the attack. The decision on which targets require assessment is made in the DECIDE function of the targeting process. Assessment may take many forms besides the determination of the number of casualties or equipment destroyed. Other information of use includes whether the targets are moving or hardening in response to the attack, changes in deception efforts and techniques, increased communications efforts as the result of jamming, and whether the damage achieved is having the expected effect on the enemy's combat effectiveness.

Assessments also are made passively through the compilation of information regarding a particular target or area. An example is the

cessation of fires from an area. If an assessment is to be made of an attack, the key personnel ensure that the intelligence or acquisition systems must receive adequate warning so the necessary sensors are directed at the target at the appropriate time. The assessment results cause battle plans and earl ier decisions to be changed. If necessary, the decisions made during the DECIDE portion of the process are reexamined. IPB products, the HPT matrix, the TSS, the attack guidance matrix, and the entire battle plan are updated. Assessment allows friendly forces to tune our efforts to achieve the greatest result with the least amount of expenditure or risk.

CHAPTER 8

INTELLIGENCE SUPPORT OF ELECTRONIC WARFARE OPERATIONS

EW is an IEW function that plays a critical role in the AirLand Battle. Intelligence support is essential to maximize the effectiveness of EW operations. This chapter describes how intelligence supports EW operations.

There is a special relationship between EW operations and intel l igence. EW, situation development, target development, and Cl are the four major tasks of the IEW mission. ESM, one of the three EW functions, supports both situation and target development. EW operations are not unique, however, because they require intelligence to be successful and also result in the acquisition of additional intelligence. Both maneuver and FS operations share this characteristic. EW is most effective when integrated and employed with FS and maneuver. Planning this integrated employment requires information that permits a comparison of the courses of action open to the commander. Sources of intelligence that provide support to EW operations and describe the intelligence used for specific EW functions are outlined below.

EW requires careful staff coordination to be effective. This includes coordination within the staff as well as coordination with the Ml unit executing the plan. The interactions involved are very similar to those seen in target development. The G3, in coordination with the G2 and the Ml unit, is responsible for the integration of ECM into the fire and maneuver scheme. The synchronized use of ECM and lethal attack requires the electronic warfare section of the G3 to coordinate closely and constantly with the FSE. To do this, the EWS and the FSO will often be collocated. ESM are also carefully coordinated between the G2 and the Ml battalion. The G2 ensures the ESM efforts are matched to the commander's PIR and targeting requirements. As these requirements change, the G2 coordinates with the Ml unit to update collection efforts.

INTELLIGENCE COLLECTION TO SUPPORT ELECTRONIC WARFARE

The collection of intelligence to support EW is a multidiscipline effort. HUMINT, IMINT, and SIGINT all contribute to the support of EW operations. HUMINT provides invaluable information, such as captured enemy communications-electron ics (C-E) operation instructions or an agent's photograph of an enemy code book contents.

IMINT provides location information important to jamming or intercept attempts and accurate data on the probable frequency ranges of enemy emitters. The size and shape of emitter antennas obtained from imagery provide indications concerning frequency data and other technical characteristics. A picture of an enemy CP or operational weapons site provides information about which types of emitter signals, both communications and noncommunications emissions, are associated with each other and with specific enemy deployments or weapon systems employment.

This information permits complex node analysis and parametric analysis of intercepted signals. This type analysis contributes to SIGINT support of EW.

Since SIGINT deals directly with information obtained from intercepted enemy signals, it provides the greatest volume of intelligence support to EW operations. SIGINT include the same functions as ESM. The primary difference between ESM and SIGINT is how the information is used. Generally, ESM produces combat information that can be used for target development (jamming and FS), maneuver, or threat avoidance with little systematic analysis or processing. SIGINT requires more extensive processing to produce intelligence. ESM and SIGINT are mutually supporting. Information collected through ESM is processed to produce SIGINT, which is essential to support EW. See FM 34-40, Electronic Warfare Operations, for a complete discussion on conducting EW operations.

THE EFFECTS OF TERRAIN AND WEATHER ON ELECTRONIC WARFARE

Signal propagation is affected significantly by terrain and atmospheric conditions. An analysis of these effects is included in any successful EW planning. The IPB techniques described in Chapter 4 of this manual and further discussed in FM 34-130, Annex F, provide a useful tool for evaluating and graphically displaying the effects of the terrain on EW operations. The analyst creates templates to depict possible enemy deployment of electronic systems for C^3, reconnaissance, TA, and REC. The analyst then compares the effects of the terrain on the employment of these assets based on a knowledge of signal propagation principles. Templates depicting locations of friendly ECM and ESM assets and knowledge of their capabilities also are used to help select friendly EW assets for employment against specific targets and indicate potential future deployment sites.

INTELLIGENCE REQUIRED FOR ELECTRONIC WARFARE SUPPORT MEASURES

The requirement to intercept, identify, and locate the sources of Threat electromagnetic emissions demands an extensive Threat electronic OB data base. Intercept operations require detailed intelligence on enemy frequency allocation and signal operating procedures. Identification is assisted by a knowledge of operating procedures; language recognition, to include specialized jargon, dialects, and code words; technical parameters of signals associated with specific functions or echelons; and the collocation of several types of emitters in a recognizable pattern which can be associated with a type of function or deployment. DF provides location data for ESM. As information is collected through ESM and used to support ECM, it also is compared with and integrated into data base information to be used for future ESM collection.

INTELLIGENCE REQUIRED FOR ELECTRONIC COUNTERMEASURES

Jamrning and electronic deception operations depend on current ESM data and all the intelligence required for successful ESM operations. Target receivers are jammed if LOS considerations permit it and the known frequency on which it is operating is capable of being jammed by friendly

ECM assets. However, indiscriminate jamming of target receivers is not the most efficient use of ECM assets. The most effective jamming requires information on the enemy's C^3 system so that the effects of disrupting a particular communications link is anticipated. This expected effect then is integrated into the commander's scheme of fire and maneuver.

Electronic deception operations depend heavily on intelligence. Both manipulative and simulative electronic deception require intelligence on the Threat SIGINT and ESM capabilities and a knowledge of friendly emission patterns and profiles. It would serve no purpose to simulate a friendly C^2 net or radar surveillance system if the opposing force cannot intercept or recognize these transmissions. Even the most simple imitative communications deception attempt, one designed to fool the operator of a clear voice net for only a few minutes, requires some knowledge of the target station's identity and the purpose of the net. A more sophisticated effort, one designed to confuse an enemy decision maker, requires not only detai led knowledge of the enemy communications system but also intelligence concerning the enemy decision-making process. If the deception effort involves intrusion into or imitation of an encrypted signal, the intelligence support may require an extensive multidiscipline effort. See FM 90-2A (C), Electronic Deception, for detailed discussion on electronic deception operations.

INTELLIGENCE REQUIRED ELECTRONIC COUNTER-COUNTERMEASURES

ECCM is divided into those measures designed to counter both ESM and ECM. The anti-ESM effort requires much of the same intelligence support required by manipulative and simulative electronic deception. The primary intelligence required concerns the enemy SIGINT and ESM capability evaluated in terms of the assessed vulnerabilities of friendly systems to such efforts. The counter-SIGINT effort requires technical information on the capabilities of enemy jammers and any intelligence on the capability of opposing forces to accomplish electronic deception. FM 34-60 provides detailed doctrine on counter-SIGINT operations. Threat doctrine on deception and information on the availability of the equipment necessary for Threat forces to implement deception activities is important. Multidiscipline intelligence efforts to obtain information on enemy ECM equipment before it is deployed is necessary if effective counter-countermeasures are to be established.

CHAPTER !3

COUNTERINTELLIGENCE ANALYSIS

Because the hostile intelligence collection threat arraved against US Forces and agencies is multidiscipline, Countering tnat threat aiso must be multidiscipline. Such an approach recognizes the need for a single program which counters all Foreign Intelligence Services collection as well as an analysis capability to bring it all together. The multidiscipline counter intelligence (MDCI) analytical effort is dependent upon information provided by the all-source intelligence system. It is found at various echelons of command. Specifically--

- The CI analysis section (CIAS) at division and corps,
- The CI analysts within EACIC at theater Armv commands.
- The intelligence and threat analysis center (ITAC) at DA.

MDCI analysis is by no means exclusive to Army agencies, but is a crucial activity of DOD. MDCI analysis operates through the DIA, and other federal agencies such as the CIA and the FBI. Highly trained, experienced, and skilled specialists perform MDCI analysis using the latest technology and modern methods of directing, processing, and disseminating.

The CI analyst uses the tools and skills identified in this chapter and Chapter 4, and as described in detail in FM 34-60. The intelligence analyst focuses on "how we see the enemy"; the CI analyst focuses on this and "how the enemy sees us." The CI analyst must also focus on how to counter the enemy's collection efforts. Where the intelligence analyst is a subject matter expert on the enemy, the CI analyst, in addition to having an in-depth understanding and expertise on foreign intelligence collection capabilities, must have a good working knowledge of the friendly force.

The CIAS must be collocated to integrate information fully with the ASPS. It must have access to all-source data that can be screened for CI use.

The CIAS is under the staff supervision of the Assistant Chief of Staff G2 and is found in the table of organization and equipment (TOE) of the EACIC at theater level; the corps tactical operations center support element (CTOCSE) at corps level; and the division tactical operations center support element (DTOCSE) at division level . An all-source mix of special ists is assigned to the CIAS to integrate their various skills and produce the MDCI analytical products required by the commander at each echelon. CIAS products are critical to the function of the G3 OPSEC and deception cells,

The CIAS mission is a diverse and all-encompassing MDCI analytical effort. The CIAS:

- Analyzes the multidiscipline intelligence collection threat targeted against friendly forces.

- Assesses enemy intelligence collection threat vulnerabilities and susceptibility to friendly deception efforts.

- Supports friendly vulnerability assessment.

- Along with the G3 OPSEC staff element, develops, evaluates, and recommends countermeasures to the commander. These countermeasures reduce. eliminate, or take advantage of friendly force vulnerabilties.

- Supports rear operations by identifying collection threats to rear area units and installations, to include low level agents responsible for sabotage and subversion.

- Nominates targets for exploitation, neutralization, or destruction.

- Develops and maintains a comprehensive and current MDCI data base.

- Tasks friendly intelligence collection resources through the CM&D section.

The CIAS focuses on hostile HUMINT, SIGINT, and IMINT collection.

COUNTER HUMAN INTELLIGENCE COLLECTION

Working in a concerted MDCI environment, counter human intelligence (C-HUMINT) analysts incorporate their efforts into the overall CIAS MDCI analysis product. C-HUMINT analysis includes:

- Analyzing and assessing the espionage, terrorism, subversion, treason, sedition, and sabotage threat.

- Analyzing enemy HUMINT collection capabilities and activities, and further analyzing how those collection capabilities can affect the friendly command.

- Analyzing level I (enemy controlled agents or partisan collection) and level II (diversionary and sabotage operations conducted by unconventional forces) threats.

- Recommending countermeasures and deception.

- Nominating targets for exploitation, neutralization, or elimination.

COUNTER SIGNALS INTELLIGENCE COLLECTION

Working in a concerted MDCI environment, counter signals intelligence (C-SIGINT) analysts incorporate their efforts into the overall CIAS MDCI analysis product. C-SIGINT analysis includes:

- Analyzing and assessing enemy SIGINT collection capabilities and activities.
- Comparing enemy collection systems capabilities against friendly targets.
- Identifying, analyzing, and assessing friendly electronic patterns and signatures.
- Analyzing friendly vulnerabilities against enemy SIGINT collection efforts.
- Subsequently recommending countermeasures and deception.
- Nominating enemy SIGINT targets for exploitation, neutralization, or destruction.

COUNTER IMAGERY INTELLIGENCE COLLECTION

Working in a concerted MDCI environment, counter imagery intelligence (C-IMINT) analysts incorporate their efforts into the overall CIAS MDCI product. C-IMINT analysis includes:

- Analyzing and assessing enemy imagery collection capabilities and activities, to include ground, air, and space threat systems. Threat systems include anything from hand-held cameras, to satellite platforms or fixed- or rotary-wing aircraft and unmanned aerial vehicles (UAV).
- Measuring enemy collection systems against friendly targets.
- Identifying, analyzing, and assessing friendly patterns, signatures, and vulnerabilities for subsequent development and recommendation of countermeasures and deception.
- Nominating enemy IMINT systems for exploitation, neutralization, or destruction.

OTHER INTELLIGENCE SUPPORT TO CI ANALYSIS.

MDCI cannot be conducted without the support of all three intelligence disciplines--SIGINT, HUMINT, and IMINT. These disciplines are used to collect critical information on enemy collection, analysis, and dissemination systems. Analysts extract the information from the all-source data base within the CIAS to determine enemy collection capabilities and operations. These systems, coincidentally, collect a great deal of intelligence on friendly forces. This intelligence is vital

in evaluating friendly profiles and thereby determining their vulnerabilities. If the situation warrants, CI analysts can task friendly collection systems to specifically collect intelligence on friendly forces for the CIAS through the CM section.

The CI mission mandates a wide range of functions and tasks that are accomplished in peace and at all intensities of conflict. CI operational activities perform such functions as investigations, operations, and collection. Their products are of great value to the MDCI analyst. To get the CI operational reports, the CIAS closely interfaces with the CM&D section to identify those items of CI interest coming into the CM&D from operational CI personnel. The CIAS must task and receive answers to those taskings through the CM&D section.

ANALYTICAL PRODUCTS

Each of the specialties assigned to the CIAS has individual responsibilities and skills which enable the production of single-discipline analysis products. When these products are combined into a comprehensive product, an MDCI product emerges. The CIAS then uses the MDCI product to nominate targets for exploitation, neutralization, destruction, or elimination. The MDCI products also provide OPSEC or deception planners with critical information required for their operations. Various specialists within the CIAS create the products discussed in the following paragraphs.

Counter Human Intelligence Products

C-HUMINT analysts maintain the C-HUMINT data base. Using this data base, they produce:

- Association matrixes.
- Activities matrixes.
- Time event charting.
- HUMINT communication diagrams.
- Link diagrams.
- HUMINT situation overlays.
- HUMINT-related portions of the threat assessment.
- Black, gray, and white lists.

The analytical techniques used in HUMINT analysis enable the analyst to visualize large amounts of data in graphic form. These analytical techniques, however, are only tools used to arrive at a logical and correct solution to a complex problem; the techniques themselves are not the solution.

There are three basic techniques (tools.) used as aids in analyzing HUMINT-related problems. They are time event charting, matrix manipulation, and link diagraming. Used together, these techniques are critical to the process of transforming diverse and incomplete bits of seemingly unrelated data into an understandable overview of an exceedingly complex situation. See FM 34-60 for detailed discussion on these techniques.

Counter Signals Intelligence Products

C-SIGINT analysts maintain the C-SIGINT data base. Using this data base, they produce:

- Threat fixed-base SIGINT matrixes. These are developed from the enemy collector characteristics data base and the threat fixed station data record.

- Mobile SIGINT matrixes. These are developed from enemy collector characteristics data base and threat OB and location data records.

- A system quick-reference matrix, providing a quick-reference of capabilities and limitations of those SIGINT systems which will most likely threaten that portion of the friendly command for which the analyst is responsible. This matrix is developed through manipulation of the data base to gain quick access to information concerning those systems which are the most likely threats to the corrrnand.

- SIGINT direction charts, portraying areas or targets of threat SIGINT concentrations. This is accomplished through integrating the EEOB overlay with the friendly electromagnetic overlay to determine areas susceptible to collection.

- SIGINT situation overlays. These are a continuous graphic update of the EEOB which depicts known or suspected threat SIGINT or REC positions. These overlays are continuously compared with the friendly electromagnetic overlay to identify susceptibility to collection.

- SIGINT-related portions of the threat assessment.

Counter Imagery Intelligence Products

C-IMINT analysts maintain the C-IMINT data base. Using this data base they produce:

- Threat SATRAN matrixes. (The definition for SATRAN is classified. See FM 34-60A for explanation.) These are designed to identify when and where a system is active and also show the collection characteristics of the system.

- Threat intelligence collection flight matrixes. These are similar to the SATRAN matrix, but are concerned "with other platforms used by the threat. Tracking these collection systems continuously allows the analyst to analyze threat IMINT collection patterns.

- System component quick-reference matrixes, including threat system's capabilities and processing times. This file is a part of the data base which equates to an OB file on threat IMINT systems.

- IMINT situation overlays. These overlays are the paths from the SATRAN and threat intelligence collection flight matrixes depicted on the friendly operations graphics. This identifies areas susceptible to collection.

- IMINT-related portions of the threat assessment.

COLLECTIVE CIAS PRODUCTS

The CIAS collectively prepares MDCI analytical products, ¡nc¡ud¡ng:

- Rear operations IPB (ROIPB) products.

- MDCI graphic summaries (MDCISUM).

- MDCI threat assessments.

- MDCI situation overlays.

- MDCI estimate.

Chapter 3 of FM 34-60 includes a detailed description on how a CIAS functions and details how to prepare single discipline and MDCI products.

The individual products of C-HUMINT, C-SIGINT, and C-IMINT analysts become the analytical tools used to produce the MDCI collective products. A brief description of each collective product follows.

Rear Operations Intelligence Preparation of the Battlefield

IPB is an analytical tool used throughout the MI community. When a greater need for intelligence support to rear operations surfaced, the IPB process evolved into a new dimension and ROIPB surfaced. However, ROIPB is not confined to the geographical boundaries of the rear area alone. In addition to analyzing information of the enemy collection threat located above and beyond the FLOT, it looks at the total friendly AO from the FLOT back. It does not dupl icate the IPB efforts of the ASPS, but rather complements their efforts. To avoid duplication, the CIAS must closely interface with the ASPS.

Like IPB, ROIPB is key in preparing for the next battle. Dur ing peacetime, RO¦PB builds an extensive data base for each potential area in which threat ¡ntelligence collectors or battalion size or smaller units might operate. It analyzes this intelligence base in detail to determine

the impact of enemy, weather, and terrain on operations and presents it in graphic form. It has the added ingredient of assisting in the assessment of friendly courses of action from the enemy's perspective.

Like IPB, ROIPB graphics can assist the commander in identifying targets as they enter the battle area. ROIPB and IPB threat evaluation and integration use the same analytical technique: templating. ROIPB templates are similar to IPB templates in the MBA. ROIPB templates provide a comparative intelligence data base that enables the CI analyst to graphically portray enemy intelligence collection and small unit capabilities; depict probable courses of action before and during the battle; and confirm or refute predictions. Like IPB templates, ROIPB templates are dynamic and require continual review. For additional details concerning RIOPB see FMs 34-130 and 34-60.

Multidiscipline Counterintelligence Summary

The MDCISUM is a graphic portrayal of the current enemy situation from a CI point of view. It graphically displays known enemy collection units, as well as level I and II threats within the friendly area. The MDCISUM ordinarily covers events within a 12-hour period. It portrays friendly targets which have been identified as potential enemy objective during the specified time frame. A clear and concise legend appears on each MDCISUM which contains: time period covered by the MDCISUM, map reference information, and symbols clearly identifying friendly and enemy information. Figure 9-1 shows a sample MDCISUM.

The use of-colors enhances an MDCISUM: but once reproduced, the disseminated product is black and white. Therefore, use dots, dashes, and slashes to ensure consumer understanding; explain these symbols in the legend. Subsequent MDCISUMs will not repeat information contained on previous MDCISUMs unless that information is critical to the current MDCISUM.

Multidiscipline Counterintelligence Threat Assessment

The MDCI threat assessment is a four-paragraph statement which is publ ished as often as necessary and when significantly changed, depending on the situation and the needs of the commander. As a general rule, the MDCI threat assessment is disseminated through CM&D with every third or fourth MDCISUM. The MDCI threat assessment provides justification for MDCI target nominations, a primary goal of MDCI analysis. Figure 9-2 shows an example of the format and substance of an MDCI threat assessment.

Multidiscipline Counterintelligence Situation Overlay

The MDCI situation overlay is a composite of the functional area overlays prepared by the subject matter experts assigned to the CIAS. The MDCI situation overlay incorporates the most important information from each of the other overlays. The functional area overlays serve as "<working" overlays, while the MDCI overlay is the master overlay and serves as the briefing overlay. It should be ready for briefings at all

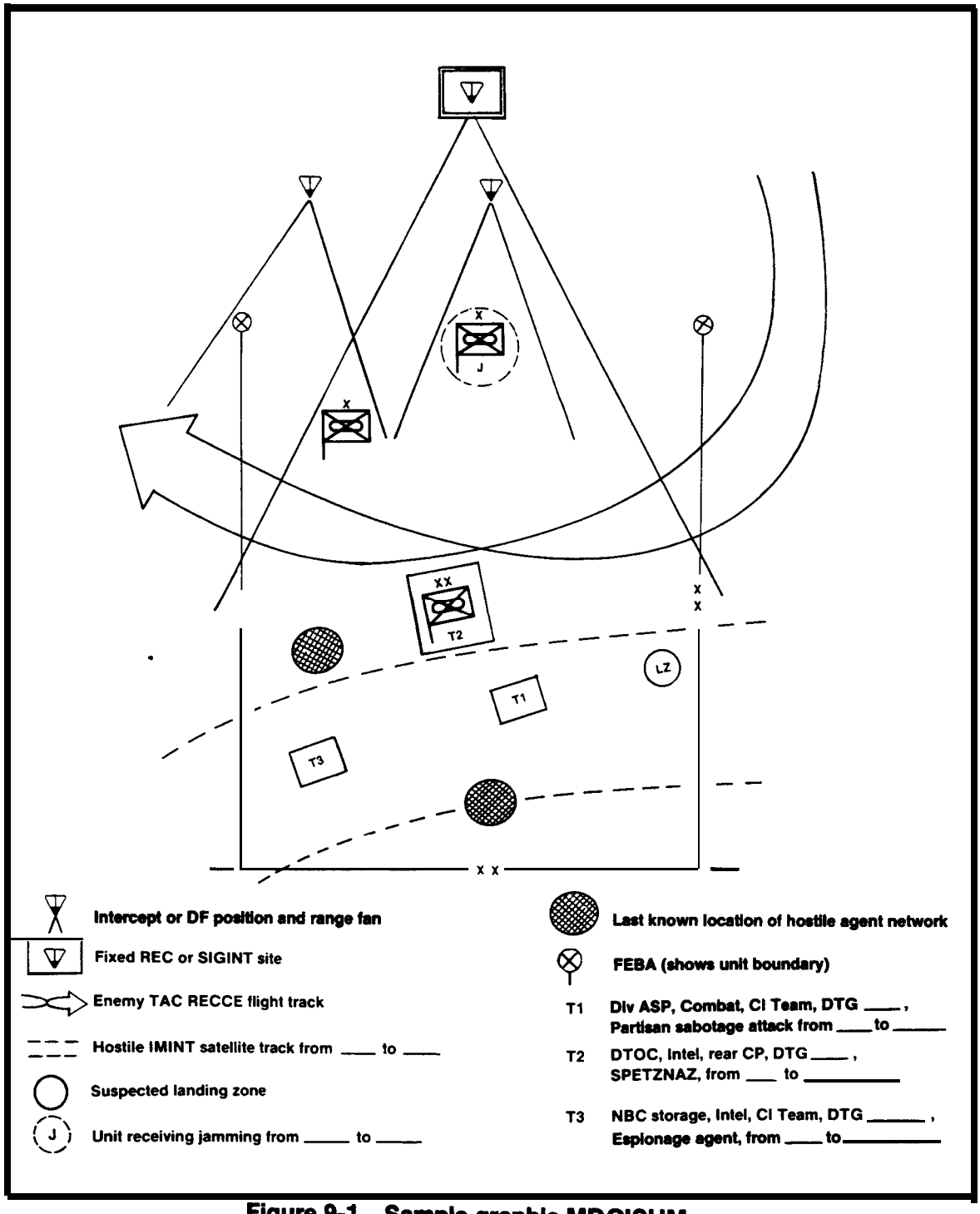


Figure 9-1. Sample graphic MDCISUM.

1. ENEMY ACTIVITY DURING PERIOD _____ TO _____ (LIST DTGs)

A. HUMINT: Summarize all known HUMINT activity during reporting period in one paragraph. Compile data from HUMINT situation overlay, matrixes, link diagrams, and MDCISUMs.

B. IMINT: Summarize all known IMINT activity during the reporting period in one paragraph. Compile data from IMINT situation overlay, matrixes, pattern and analysis charts, and MDCISUMs.

C. SIGINT: Summarize all known SIGINT activity during the reporting period in one paragraph. Compile data from SIGINT situation overlay, matrixes, direction charts, and MDCISUMs.

D. OTHER: Summarize all other enemy activity that is not already addressed using the same analytical tools.

2. INTELLIGENCE DAMAGE ASSESSMENT FOR THE PERIOD _____ TO _____ (LIST DTGs)

Briefly assess the intelligence damage to the friendly units for which the assessment is being prepared. Assessment is based on enemy collection activities that were traced, analyzed, and reported in MDCISUMs and were measured against the friendly force operations profile and countermeasures implemented by the friendly force. Coordination with G3 OPSEC staff element is essential in preparing this paragraph.

3. PROJECTED ENEMY ACTIVITY ASSESSMENT FOR THE PERIOD _____ TO _____ (LIST DTGs)

A. HUMINT: Using the same analytical tools identified in paragraph 1A, above, plus IPB, project or assess enemy HUMINT activity for the next reporting period.

B. IMINT: Using the same analytical tools identified in paragraph 1B, above, plus IPB, project or assess enemy IMINT activity for the next reporting period.

C. SIGINT: Using the same analytical tools identified in paragraph 1C, above, plus IPB, project or assess enemy SIGINT activity for the next reporting period.

D. OTHER: Using the same analytical tools identified in paragraph 1C, above, plus IPB, project or assess all other enemy activity for the next reporting period that is not otherwise addressed in the HUMINT, IMINT, or SIGINT assessments.

4. TARGET NOMINATIONS:

A. EXPLOITATION: Using aforementioned information and all other MDCI analytical tools, identify any targets worthy of exploitation. Provide

Figure 9-2. MDCI threat assessment.

recommended time frames, locations, methods of exploitation, justification, and any other pertinent data.

B. NEUTRALIZATION: Using aforementioned information and all other MDCI analytical tools, identify any targets worthy of neutralization. Provide recommended time frames, methods of neutralization, locations, justification, and any other pertinent data.

C. DESTRUCTION OR EXPLOITATION: Using aforementioned information and all other MDCI analytical tools, identify any targets worthy of destruction or elimination. Provide recommended methods for engagement. time frames, locations, justification, and any other pertinent data.

NOTE: All target nominations must have G2 or G3 approval before dissemination or presentation to the commander or designated representative for decision. Coordination with appropriate elements, consistent with type nomination, is essential.

Figure 9-2. MDCI threat assessment (continued).

CLASSIFICATION

Headquarters
Place
Date, Time, and Zone

MDCI Estimate Number _____.

References: Maps, charts, or other documents.

1. Mission: The restated mission determined by the commander.

2. The Area of operations: Summarizes the analysis of the AO.

a. Weather:

(1) Factors. Include light data and either a weather forecast or climatic information, as appropriate. Use appendixes for graphic representation or weather factors and other detailed information.

(2) Effect on enemy courses of action. Discuss the effects of weather on possible enemy courses of action (for example, sabotage, subversion, raids, air operations) in terms of mobility, concealment, and logistic sustainability. Discuss in terms of level I or II threat, and enemy all-source intelligence collection operations.

b. Terrain:

(1) Existing situation. Use graphic representatives where possible especially in regard to cover, concealment, and logistic

Figure 9-3. MDCI estimate.

sustainability. Use annexes for detailed information. Information covering observation, fields of fire, obstacles, key terrain, and approaches to the probable target aid in determining insurgent terrain. Also, consider graphics for critical facilities and buildings.

(2) Effect on enemy courses of action. Discuss in the same manner as for effects of weather in a(2) above. Discuss in detail those areas favorable and unfavorable to the levels of threat I or II enemy all-source intelligence collection opportunities.

(3) Effect on own courses of action. Discuss in the same manner as for effects of weather in a(2) above. Note the positive or detrimental effects on response forces and defensive measures.

c. Other characteristics. Include in subparagraphs any of the following factors or characteristics which are pertinent to friendly area activity (emphasis on rear area): population, ethnicity, religious makeup, literacy rate, medical considerations, economic stability, transportation, mass media, public services, and current political situation.

3. Enemy situation. Information on the enemy which will permit later development of enemy capabilities and vulnerabilities and refinement of these capabilities into specific course of action and their adoption.

a. Disposition. Reference may be made to overlays, enemy situation maps, or previously published documents. Location of potential threat forces may be difficult to pinpoint, but the greater the detail, the more thorough the analysis. Separate by level and type of threat (that is, combat (level I and II threats) or intelligence).

b. Composition. Summary of the OB of conventional level I and II threats, intelligence collection units and elements, and the structure or organization of paramilitary and/or terrorist groups. Separate by level and type of threat.

c. Strength. The purpose of this listing is to assist in developing enemy capabilities and vulnerabilities. Conventional and intelligence threats are discussed as in a regular intelligence estimate. Terrorist, paramilitary and other threats need to be assessed based on support from populace, monetary base, supplies, armament, personnel, and any other pertinent considerations. Subparagraphs should be used to address the different threats. Separate by level and type of threat.

d. Recent and present significant activities. Items of information are listed to provide bases for analysis to determine relative probability of adoption of specific courses of action and enemy vulnerabilities. Enemy failures to take expected actions are listed as well as positive information. Such a discussion should include recent all-source collection activities, terrorist actions, and other indications.

e. Peculiarities and weaknesses. For conventional and intelligence collection threats, discuss as in an intelligence estimate. For

Figure 9-3. MDCI estimate (continued).

terrorist, paramilitary, or other unconventional threats, discuss such pertinent information as leadership (key personalities), equipment, finances, and relations with the local populace.

4. Enemy capabilities. Based on all the previous information and analysis, develop and list enemy capabilities to conduct operations against the friendly area, with emphasis on the rear area. The listing provides a basis for analyzing the available information to arrive at those capabilities that the enemy can adopt as specific courses of action and their relative probability of adoption. Items should be separated by levels and type of threat.

a. Enumeration. State what, when, where, in what strength, and by what method for each enumerated threat.

b. Analysis and discussion. Each enumerated threat is discussed in terms of indicators of adoption or rejection. The intent is to assess the likelihood of a given threat taking a given action. This paragraph must consider all information previously recorded in the estimate. Some threats may not have any indicators of rejection listed due to insufficient data.

5. Potential enemy targets. Based on all previous information and analysis, develop, to the extent possible, a listing of potential enemy targets. Identify, at a minimum: target identity, capability, location or projected location, and projected intentions. Ascertain if targets can be exploited, neutralized, destroyed, or eliminated. Use subparagraphs and/or annexes as needed.

6. Conclusions.

a. Effects of AO on own courses of action. Indicate weaknesses in ability of response forces to react and in defensive measures.

b. HVT analysis based on the CARVE format (criticality, accessibility, recuperability, vulnerability, and effect). Such targets range from bridges to friendly units, public services, and key facilities. Complete for both friendly and enemy targets.

c. Probable enemy courses of action. Courses of action are listed in order of relative probability of action. However, insufficient data may only permit the probable level of threat for a given target.

d. Enemy vulnerabilities. List the effects of peculiarities and weaknesses that result in vulnerabilities that are exploitable.

Annexes (as required): Annexes may include graphic analysis products which support the estimate such as link diagrams, association matrixes, ROIPB products, or black, white, and gray lists distributed to units requiring them.

CLASSIFICATION

Figure 9-3. MDCI estimate (continued).

times. Ordinarily, the CIAS operations NCO is responsible for maintaining the overlay; however, its preparation is a collective effort of all members of the CIAS.

MULTIDISCIPLINE COUNTERINTELLIGENCE

The CIAS identifies the multitude of intelligence collection capabilities of adversaries on the battlefield. it then narrows the capabilities as accurately as possible to the actual collectors within an area, their targets, and the collectors technical characteristics. The CIAS also provides information to the battlefield deception (BAT-D) staff on the characteristics of friendly equipment so that an "as close as possible"' replication of a friendly force is displayed to enemy collectors. This is done during the development of the deception story in the planning process.

On today's technical battlefield, the friendly force assumes that hostile collectors are analyzing friendly patterns of C^3 to find HVTS. In friendly communications, mostly secure, the enemy must locate the communications externals that identify specific units or nodes. In electronic deception, these communications externals are replicated down to and including specific anomalies in friendly transmissions. Currently, analysis of such signals parameters is extremely difficult. C-SIGINT analysts research technical bulletins, coordinate with C-E staff members and maintenance personnel to collect this information as accurately as possible for the deception staff. As friendly deception equipment evolves into the future and becomes more sophisticated, friendly capability to provide the needed detail of support also must expand.

BAT-D elements become one of the main consumers of the integrated MDCI products. They use the MDCI estimate and graphic summary to determine where best to execute deception based on the collection effort.

Specific needs and requirements for BAT-D are passed through G3 channels to the CM&D at each echelon. The CIAS researches its data base to satisfy these needs with existing intelligence information. If the CIAS cannot satisfy the requirement immediately, it is validated and returned to the CM&D for appropriate tasking and requirements management. When the information is finally collected, it is passed through the CM&D to the CIAS for analysis and product development. It is then passed to deception planners so they can develop deception plans or execute the deception mission.

Since adversaries change the focus of intelligence collection as often as necessary, the CIAS analyzes its efforts continuously and passes the changes to the deception cell rapidly. This enables deception personnel to change focus and evaluate their effectiveness.

INTELLIGENCE SUPPORT TO COMBATTING TERRORISM

Terrorist activities are an ever-increasing threat to Army units. personnel, equipment, and operations, in peacetime and during conflict. CI personnel play a major role in supporting the force protection mission

through investigation, operation, and intelligence collection directed at terrorist groups and activities. The CIAS has an additional analytical role, using C-HUMINT techniques in this manual and fully explained in FM 34-60.

The MDCI threat assessment is an effective product for providing information to support the command force protection mission. The process includes educating the force on the threat, evaluating past activities of terrorists, maintaining a current data base, using pattern analysis, and predicting future activities and incidents. The CIAS also recommends offensive and defensive measures that may be effective in combatting terrorism.

Combatting terrorism is a shared mission among all members of the Army. The relationships between the operations staff, intelligence staff, and military police must be "locked in" completely to be effective. There are many other players who provide information to the process and to the intelligence analysis mission. Using the techniques of C-HUMINT analysis, the friendly goal is to track activities and associations, to predict the next terrorism act, to determine who is performing the act, when and where, and to get the information to decision makers who can do something about it.

CHAPTER 10

INTELLIGENCE SUPPORT TO COUNTERINSURGENCY

Recent history is characterized by the occurrence of numerous insurgences in developing nations. The US government has taken the responsibility to assist, upon request, selected emerging nations in developing political stability, economic strength, and social progress. Thus, the US may become involved in a LIC, either in an advisory and assistance capacity or as a combatant. The analyst plays an important role in all LIC operations including foreign internal defense and peace keeping. The focus in operations such as these is different than in counterinsurgency. Here the analyst is concerned with political questions such as, "How can the people be made to support tha government?" and 'Who is the enemy?"'

This chapter describes how information from all sources is analyzed to produce intelligence to support counterinsurgency. LIC includes counterinsurgency, but also foreign internal defense, peacetime contingence ies, and terrorism counteraction. These last three areas are beyond the scope of this FM.

When the level of US participation with a host nation is sufficient to be considered a combined activity, a combined intelligence operation is carried out. Combined intelligence operations facilitate more effective collection and production capabilities. The host country provides detailed knowledge and access to the populace, while the US Army provides technical expertise, management, and advice. There are often varying degrees of US and host nation cooperation.

The primary responsibility of intelligence personnel engaged in LIC is to produce intelligence to support the prevention or defeat of an insurgency. To defeat an insurgency, information is collected and intelligence produced on virtually all aspects of the internal defense environment. When insurgents are known to be receiving aid from an external power, it is necessary to obtain information on the role of the external power in the insurgency.

The target of the intelligence collection cycle (described in Chapters 1 and 2) for LIC differs from mid- to high-intensity conflicts only in its application to the production of specific intelligence required for counterinsurgency operations. In planning, for example, information is not only needed on the armed insurgents but also on their underground organization and their relations with the populace as well. In collecting information, the local population represents one of the most lucrative sources of information. In processing information into intelligence, sociological, economical, and political requirements have equal or even higher priority than conventional military needs. In addition to military users, US, host nation, and allied governmental, law enforcement, and intelligence agencies are valid users of intelligence products.

SUPPORT OF COUNTERINSURGENCY OPERATIONS

A sound collection program and proper use of the various collection agencies and information sources result in a very heavy volume of information which flows into the intelligence production element. The insurgent environment and its base area system and political and military tactics dictate that intelligence requirements can only be met by reporting minute detai Is on a great variety of subject areas. Each one of these details appear unrelated to others and insignificant by itself; but when mapped and chronologically recorded over long periods of time and analyzed with other details reported, they lead to definitive and predictable patterns of insurgent activity.

For example, as in a conventional conflict, IPB is conducted before and continues throughout a LIC. IPB not only helps identify patterns of insurgent activity, but helps use these patterns to predict future actions. Appendix E, FM 34-130 fully addresses IPB in support of LIC.

Insurgents usually recognize their shortcomings in military posture. The insurgent makes maximum use of the weather, the terrain, and the population, employing secrecy, surprise, and simplicity. Combat plans and orders are usually simple, comprehensive, and repetitive in order to be executed by widely separated forces. Therefore, the insurgent's solution to a problem is composed of a system or systems which together are complex, but apart are independent, having simple, logical, and uniform characteristics. In developing a pattern analysis or IPB products, it is important to chart insurgent and friendly tactical actions. As actions of friendly forces disturb the 'environment and patterns of insurgent activities, it forces the insurgent into unanticipated and unrehearsed situations which can be exploited tactically. Comrnunications intelligence (COMINT) is used to obtain direct insights into insurgent operations and plans. IPB helps the intelligence analyst answer two basic questions:

- Where can we expect to find the enemy?
- Where can we expect not to find the enemy?

The data to be developed and compiled by subject matter varies considerably with the intensity of the insurgent's operations. The types of overlays and categories of subjects plotted, therefore, vary extensively according to the needs. Using a graphic keying system and color schemes on large-scale maps greatly facilitate data analysis when superimposing transparent overlays.

INTELLIGENCE ESTIMATE

IPB provides a basis for the intelligence estimate. As with mid- and high-intensity operations, IPB products are used extensively in the estimate. There are, however, some significant differences from these to estimates that support LIC in general and counterinsurgency specifically:

- Emphasis is placed on different parts of the estimate. The mission statement, for example, may be more difficult to compose because of the wide scope of low-intensity operations and their relationships with the internal defense program.

- Emphasis is accorded nontactical considerations, such as psychological, political, sociological, and economic factors.

- Factors are to be compared during the deliberative process. Advantages and disadvantages of various courses of action may be more complicated than when terrain, weather, and a visible, tangible enemy are the chief factors to be considered.

The intelligence estimate for a LIC operation, as in any situation, is based on all available intelligence and considers everything of operational significance. See Appendix A for an example of a LIC intelligence estimate.

The initial intelligence estimate helps to point out gaps in the intelligence data base. These gaps are a basis for determining requirements.

A basic requirement in low-intensity operations is a thorough understanding of the target area. Knowledge of the target society requires a complete understanding of the internal and external forces at work, those supporting the integrity of the society, and those engaged in subverting it. Only when these factors are thoroughly understood can actions be effected. All available assets are used to provide this intelligence.

Commanders, intelligence staffs, and analysts recognize the impact that political, economic, and sociological factors have on tactical operations of the insurgent and friendly forces. This applies even to a very narrow, confined, and localized situation. Therefore, an intense and continuing study of local history and developments, contemporary personal ities, aspirations, and motivations is made. Because political, sociological, and economic factors are overlapping and interdependent, collation and interpretation of this data are extremely intricate and seldom are reduced to a formula similar to OB for mid- and high-intensity conflicts.

PROCESSING INFORMATION

Processing is the step in the intelligence cycle whereby information becomes intelligence. It consists of recording, evaluating, integrating, and interpreting. Chapter 2 describes information processing. Certain considerations are unique to the internal defense environment. To determine insurgent capabilities and courses of action and to provide the intelligence needed for all facets of LIC, the intelligence analyst is guided by an awareness of these considerations.

RECORDING

As in mid- and high-intensity situations, LIC requires large amounts of information on a continuous basis which are promptly compared with existing information and intelligence to determine their significance. To a large-degree, the extent of the recording effort depends upon the insurgent activity in the area and the analysts available to maintain and analyze the recorded information. All of the recording aids mentioned below, however, serve a unique and useful purpose in the overall intelligence production effort. Chapter 2 provides a detailed description of the journal, journal file, intelligence files, and intelligence workbook. Variations in recording devices which are unique to LIC occur in the use of annotated overlays and working files.

Annotated Maps

Depending on the echelon of responsibility, the state of insurgent activity in the area, and the degree of knowledge of the enemy, the intelligence analyst requires at least two annotated maps: the incident map and the insurgent SITMAP. Each of these recording devices normally is a transparent overlay covering a large-scale topographic map of the area. Unlike the workbook, which is maintained for individual use, the incident and insurgent SITMAPS provide a ready guide for briefing the commander, the civil authorities, or other interested parties. If activity in a particular area is limited, consideration is given to the combination of the two maps. Other annotated maps are valuable aids for recording information, depending on the needs in a particular headquarters' tactical area of responsibility. These special purpose overlays include records of--

- Mining and booby trap incidents.
- Insurgent names or codes for local terrain features, such as villages, areas, and trails.
- Insurgent assassination or resource collection attempts.
- Other significant activity.

It may be necessary to enlarge, with significant detail, certain AIs, either by drawing portions of the map to a larger scale, or by making a mosaic from aerial photos. Past, present, and potential insurgent activity must be visible with a detailed and thorough understanding of the environment. Comparison of the several annotated maps maintained often assist the intelligence officer in estimating the enemy's intentions and capabilities or to establish trends.

Incident Map. The incident map or overlay provides historical cumulative information on trends and patterns of insurgent activity. Properly maintained, the entries enable the intelligence officer to make judgments about the nature and location of insurgent targets, the relative intensity of insurgent interest in specific areas, insurgent control over or support from the population, and potential areas of insurgent operations.

Judgments concerning insurgent operations also require knowledge of terrain factors and insurgent limitations.

insurgent Situation MaQ. The SITMAP or overlay is prepared as part of the IPB process, and is modified as necessary by information from the incident map. It is difficult to pinpoint insurgent installations and dispositions with the same degree of confidence as in a conventional tactical situation. The insurgents can displace on short notice, making a report outdated before it is confirmed. While the SITMAP presents an uncertain and hypothetical picture, composed less of firm information than of reports of fleeting targets, estimates, and abstractions, it graphically substantiates the trends or patterns derived from the incident map. The analyst can then improve the economy and effectiveness of the R&S effort.

Trap Map. The trap map or overlay is used if the insurgent has a capability for sabotage or terrorist action. Data is directly annotated on the map on which the situation overlay is placed, or it can be kept separately. This map portrays particularly attractive target locations for insurgent sabotage or terrorism, such as road and railroad bridges, communications centers, theaters and assembly halls, and places where the terrain favors ambushes and raids. Such areas are identified and analyzed as part of the area study. They are plainly marked on this map with attention directed to possible insurgent access and escape routes. Photographs which are keyed to the map also supplement this effort.

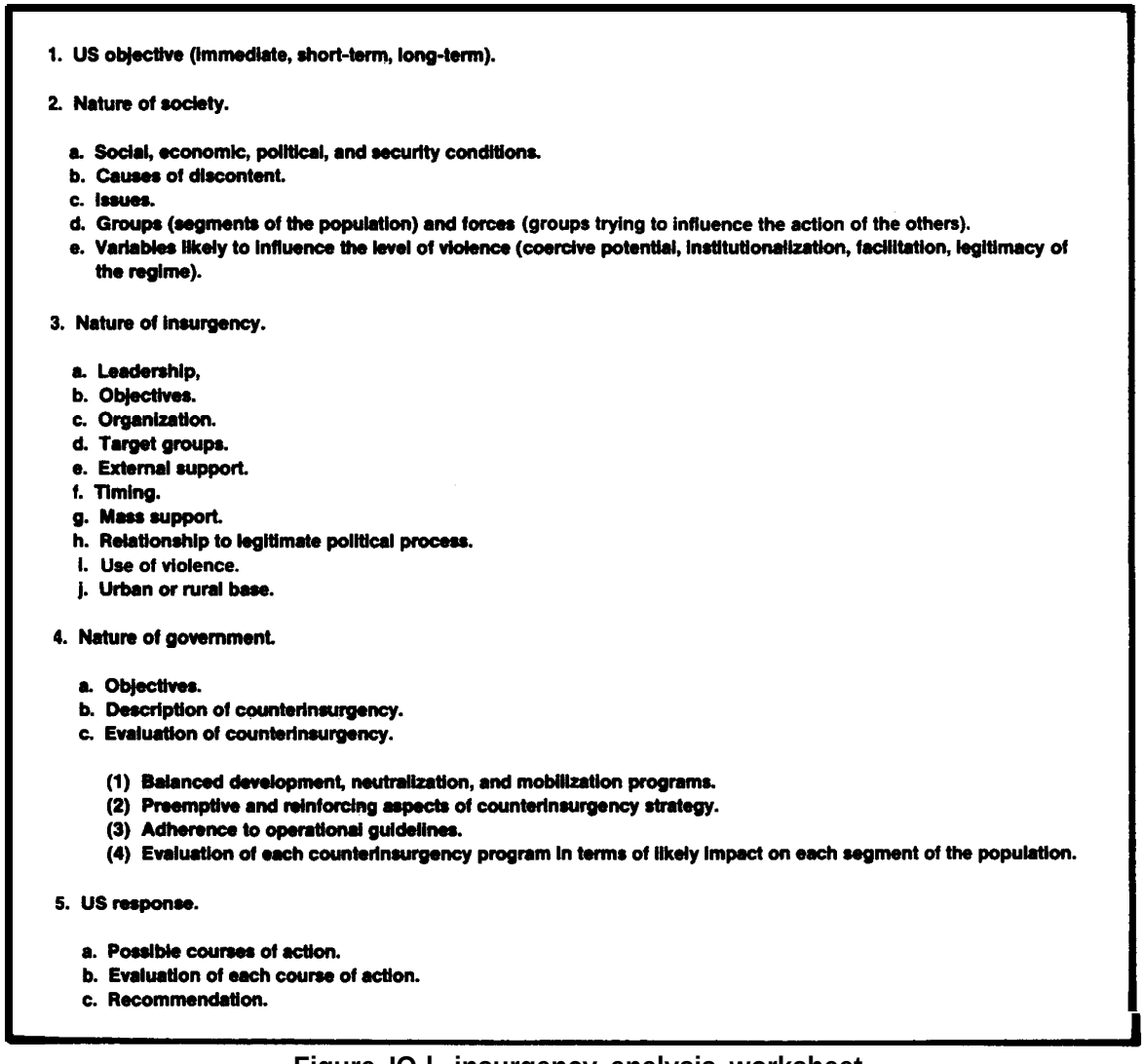
Population Status Map. This consists simply of an overlay to the SITMAP. Essentially, this map portrays the attitudes of the population, whether disaffected, loyal, or doubtful. Colors are used effectively to designate these conditions.

Personalities and Contacts Map. What is known initially about the insurgent situation primarily is information concerning locations and activities of individual agents of espionage, agitation, organization, and liaison. The appearances, movements, meetings, and disappearances of these agents are recorded on a personalities and contacts map or overlay. A large-scale map is required (a city street map or town plan if an urban area is involved). Deviations from regular patterns of movement are detected in this manner. Depending upon the number of personalities under surveillance, the regularity of their habits, and the variety of reports received on them, it is necessary to maintain a separate overlay for each subject. Old overlays are filed for comparison. Each agent's route is portrayed in a different color, and regularly traveled routes distinguished from new routes. Observations are dated and incidents noted by symbol. Depending upon the amount of insurgent activity, this map is combined with the incident map.

Working Files

The intelligence worksheet and the annotated maps serve to isolate problem areas and formulate relationships between items of information and intelligence collected. Extensive research material is required, however, to analyze these problem areas. in the early phase of an insurgency, the insurgent leader is building an organization. The leader's organizational

procedures and tactics, therefore, are unique, and familiarization requires the intelligence officer to study personal ities and incident analysis. Extensive working files, such as the insurgency analysis worksheet, hot files, current propaganda and psychological operations (PSYOP) file, personality and organization files, area study files, civil-military operations file, and resource reference files are established and maintained. Figure 10-1 shows an insurgency analysis worksheet.



1. US objective (immediate, short-term, long-term).

2. Nature of society.

   a. Social, economic, political, and security conditions.
   b. Causes of discontent.
   c. Issues.
   d. Groups (segments of the population) and forces (groups trying to influence the action of the others).
   e. Variables likely to influence the level of violence (coercive potential, institutionalization, facilitation, legitimacy of the regime).

3. Nature of insurgency.

   a. Leadership,
   b. Objectives.
   c. Organization.
   d. Target groups.
   e. External support.
   f. Timing.
   g. Mass support.
   h. Relationship to legitimate political process.
   i. Use of violence.
   j. Urban or rural base.

4. Nature of government.

   a. Objectives.
   b. Description of counterinsurgency.
   c. Evaluation of counterinsurgency.

      (1) Balanced development, neutralization, and mobilization programs.
      (2) Preemptive and reinforcing aspects of counterinsurgency strategy.
      (3) Adherence to operational guidelines.
      (4) Evaluation of each counterinsurgency program in terms of likely impact on each segment of the population.

5. US response.

   a. Possible courses of action.
   b. Evaluation of each course of action.
   c. Recommendation.

Figure IO-I. insurgency analysis worksheet.

Insurgency Analysis Worksheet. The insurgency analysis worksheet helps identify information and intelligence needed to satisfy the PIR and IR. It also provides a guide for analysis of a LIC environment.

Hot File. The hot file is the most important working file. It includes all available material pertaining to an incident or groups of possibly related incidents that are of current interest. This file contains material on persons or places likely to be involved in insurgent activity, together with material on agents or suspects who may be involved. A reported sabotage plot, for example, could initiate a hot file. The hot file remains active until the report is refuted, the incident occurs, the attention of the insurgent is diverted elsewhere, or friendly interest priorities change.

Current Propaganda and PSYOP File. If propaganda constitutes a major part of the insurgent effort in the area, a current propaganda and PSYOP file should contain all pertinent literature, background material, and analyses, to include copies of propaganda speeches and analyses of local grievances being exploited or subject to exploitation by the insurgents.

Personality and Organization Files. A local file is maintained on each insurgent personality. If surveillance is carried out by the local police, basic identifying and biographical information can be transferred from police dossiers to a card file. This card file helps train friendly surveillant to recognize key personalities on sight. The organization section of this file includes information on the history and activities of the insurgent organization's fronts, other subversive or suspected groups, and their officers, overlapping directorates, memberships, and liaison among these organizations. Figure 10-2 shows the format for a personality card file.

Area Study Files. Area study files contain up-to-date and pertinent data in the geographic, political, sociological, economic, and cultural fields. In low-intensity operations, even the lower echelon tactical commander, particularly when operating in the same general operational area over extended periods of time, has a definite requirement for such information. The intelligence staff officer should, therefore, have ready access to such data. The topical breakdown of such files concerns events and activities of continuing significance. Thus, for example, if rice is the basic staple in an economy, the topical breakdown includes files on rice production, distribution and marketing, price levels, and black marketeering and pilferage activities. Since this key economic indicator has continuing influence on friendly military operations as well as on the insurgent forces who depend on this staple for survival, careful analysis of this data over a period of time provides patterns based on which insurgent actions are anticipated and their capabilities predicted.

Resource File. A resource file includes all material which is of importance but are not of immediate value. It includes inactive incident files, inactive personality and organization files, and photography. The latter material is particularly useful. Air or ground photographs of places of interest are arranged chronologically by location and made readily available for use with hot files, incident maps, and trap maps.

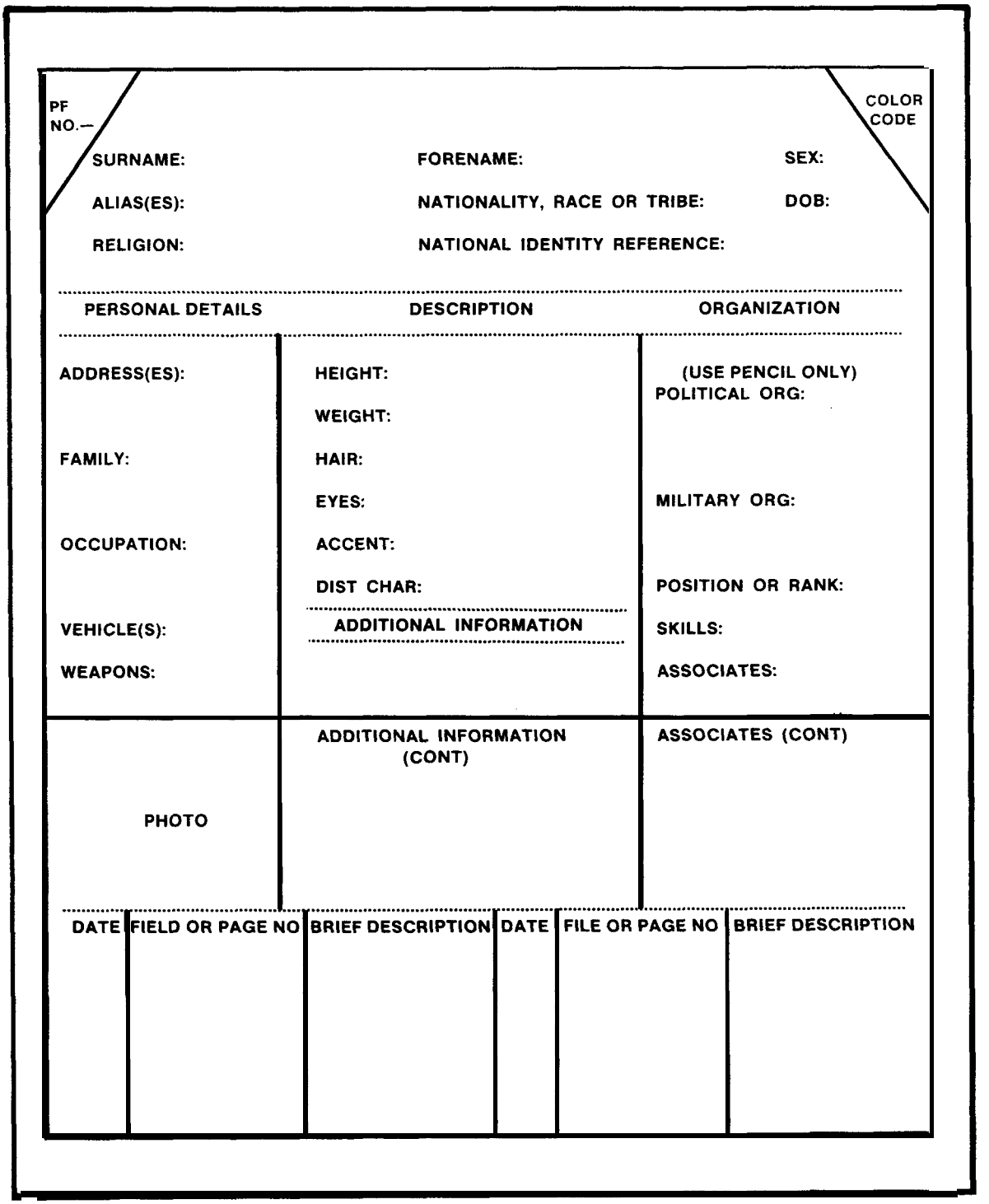


Figure 10-2. Personality card file format.

Reference Material. A library is maintained of reference publications, such as manuals on doctrine, tactics, and methods; books on the area and on the insurgent threat; files of newspaper and magazine clippings; and any other material which is of use. This material is kept at a central library serving the entire staff or located at an area coordination center.

Coordinate Register. The coordinate register is a valuable analytical tool , and method to store information during LIC situations. It illustrates activity in a particular area over a period of time, and is compact enough to be carried with ease. Each page represents a specific geographic area or town that the S2 determined. The coordinate register has two types of pages. One has written entries to record insurgent activity with space for the S2 to add comments. Figure 10-3 shows a sample written-entry coordinate register, applicable to a LIC.

ITEM	TIME	COORDINATE	ACTIVITY	NOTES
1.	150930	XK345678	MG harasses site	position patrol south of site
2.	152230	XK348672	farmer reports 10 guerrillas moving south	
3.	200140	XK348678	individual with binoculars seen observing site	increase friendly surveillance vic. of site

Figure 10-3. Written-entry coordinate register.

The second type of coordinate register is visual. Entries are plotted on the overlay square as they appear on the incident map.

The coordinate register assists in trend and pattern analysis and is a good way to store data, in an easily retrievable manner, for long periods of time. The written register allows easy evaluation of enemy activity by type action while the visual one allows rapid comparisons of activity between several time periods.

Civil-Military Operations File. A civil-military operations file includes all material and information concerning civil-military operations, their results, effectiveness, and any countermeasures the insurgents take.

EVALUATION

Evaluation is the determination of the pertinence of information to the operation, reliability of the source or agency, and accuracy of the information. In evaluating information, the knowledge and judgment of the intelligence analyst plays a major role. In determining the validity of a fact or whether a reported activity is at all possible, it must be realized that certain events are possible despite the fact that they did not previously occur and have been deemed by past analysis as unlikely to occur. Confirmation of information by other sources and agencies is always desirable, but it is not always possible to obtain. Initially, intelligence analysis commences with unconfirmed information which is subsequently supported, confirmed, or denied by the collection of additional and related information. As more information is obtained, the insurgent situation, capabilities, and probable courses of action become increasingly clear. As the body of intelligence expands, information that is not compatible with the current insurgent situation and is not consistent with the recent pattern of insurgent activity is suspect. Chapter 2 describes evaluation in detail. Procedures governing the assignment of evaluation ratings to sources and agencies have equal application in the internal 'defense environment.

INTEGRATION

Evaluated information becomes intelligence only after it has been integrated with other information and interpreted to determine its significance. Integration involves the combining of selected data to form a pattern which will have meaning and establish a basis for interpretation. It is important that the intelligence analyst is sufficiently alert to recognize all the possible patterns that may be formed. The following example illustrates the mental process of integration: The intelligence section of the area coordination center receives information that a prominent labor leader has been murdered. In a search for related information, the intelligence analyst checks the incident file, the friendly and suspect personality files, and the organization file.

The incident file reveals a series of murders that have been linked with the insurgent, with the primary victims being government officials, prosperous merchants, and large landholders who opposed insurgent objectives.

The suspect personality file reveals the labor leader's controlling position within a union that has recently intensified its criticism of the government. The personality file also reveals the labor leader's close association with several government officials and recent extensive travel throughout the nation.

The organization file indicates that the union has recently begun to disseminate antigovernment leaflets and has threatened to call a strike if demands for representation in the current government are not met. The other primary contender for union leadership is a relatively unknown newcomer.

Once all related items of information from the intelligence files are obtained, the intelligence analyst begins to assemble the available information to form as many logical pictures or hypotheses as possible. Alternative methods of assembly are an essential prerequisite to any valid interpretation.

Assembly of information to develop logical hypotheses requires good judgment and considerable background knowledge. In formulating hypotheses, the intelligence analyst avoids the limitations which result from preconceived opinions. In the example of the murdered union leader, the new information is integrated with existing intelligence in several different ways. By combining the murder with one set of facts, the labor leader is pictured as a loyal supporter of the government who became the victim of a campaign of selective terror undertaken by the insurgents. On the other hand, by combining the murder with another set of acts, the labor leader is portrayed as a member of the insurgent organization who was murdered for reasons not connected with the insurgency. As a third possibility, the labor leader may have been a member of the insurgent organization who was eliminated by the insurgents. Finally, there is a fourth possibility that the labor leader and the murder are not connected with the insurgency.

INTERPRETATION

Interpretation is the result of making deductions as to the probable meaning of new information and determining its implications with respect to future insurgent activity. The meaning of the information is determined in relation to the insurgent situation and the insurgents' probable courses of action.

For example, in the case mentioned above, if the labor leader was loyal to the government and was murdered for opposing insurgent control of the union, it reasonably is expected that further consolidation of insurgent control over the union, increased antigovernment agitation by the union, and possibly, an extension of insurgent terrorist activities will take place.

However, if the labor leader was a member of the insurgent organization and was murdered by the insurgents, it is conjectured that the elimination was due to considerable unreliability or slow progression toward the achievement of insurgent objectives. In this case, the prompt emergence of another insurgent union leader who ensures more rapid progress toward insurgent objectives is expected. It also is inferred, however, that the labor leader was murdered as a result of a struggle for power within the insurgent organization. In this case, weaker insurgent control of the union is expected due to the dissension among the insurgents.

Finally, if the labor leader had no connection with the insurgent organization and was murdered for reasons unconnected with the insurgency, this event has no significance from an intelligence standpoint.

DISSEMINATION

One of the more critical aspects of intelligence is the rapid dissemination of the information to personnel and units that nead information. Each information report is looked at immediately to see if it is of immediate concern. If so, it needs to be disseminated to affected units or personnel without delay. Successful intelligence reporting communicates the results of analysis and combat information to the right people, at the right time, and in the right format. It provides the commander with tha information and intelligence needed to raduce risk and uncertainty. The dissemination channel in a LIC varies llttle from the conventional environment but often there are more agencies and individuals to consider: police, potential terrorist targets, and other civilian agencies operating in the AO. Also, intelligence is disseminated to host nation military units.

Local SOP and guidance from higher headquarters dictate the amount and type of information that is given to civilian agencies and host national military forces. This question of releasability is resolved before effective dissemination can exist.

ORDER OF BATTLE

Chapter 3 describes the production of OB intelligence. There are certain OB considerations, however, which are unique to the insurgent enemy. OB intelligence is equally as important in an insurgency as in conventional combat operations. However, some differences in nomenclature and approach must be recognized. The applicability of the various OB factors differs in an insurgency from conventional operations, and there also are differences in applicability between phase I and phase II insurgency situations,

The elements of OB intelligence (OB factors) are not independent of each other; they are closely related and are considered as a whole, Information on one of the elements often leads to a reevaluation or alteration of information previously received on another element. Furthermore, the general rule, whereby OB intelligence is developed and maintained down to and including two echelons below the analyst's own level of command, does not apply to low-intensity operations. Due to the nature of the insurgency and the phased development of the insurgent forces, OB intelligence is produced in much greater detail and pertains to much lower echelons (even down to squad) than in conventional combat operations.

During phase I of an insurgency, subversive activities range from being only a potential threat to frequently occurring activities along an organized pattern. No major outbreak of violence or uncontrolled insurgent activity exists. The insurgent is primarily concerned with organizing infrastructure during this phase, along with conducting PSYOP and terrorist attacks.

Phase II of an insurgency begins when the insurgent has gained sufficient local or external support to initiate organized guerrilla warfare against the government.

A phase III insurgency occurs when the insurgent has transitioned from a guerrilla-oriented force to a primarily conventional-oriented force. FM 100-20 describes, in detail, the goals and activities of insurgent forces during all three phases. An important point to remember is that the insurgent may be operating from areas outside the host country during all three phases. Therefore, geographic boundaries cannot limit intelligence collection and analysis.

A listing of the OB factors follows, together with a brief explanation of their applicability and means in the context of insurgency situations.

COMPOSITION

In some insurgent movements, military force is only one of several instruments through which the insurgent movement seeks power. Development of a military force often has the lowest priority during the early stages of an insurgency. As long as the party core and civil organizations are established and move effectively toward the goal of the insurgency, the military arm either lies dormant or simply exists in cadre form until needed as a supporting force. Even after military organizations are fielded, the infrastructure never loses its importance. A counterinsurgency operation is never over until the infrastructure is neutralized.

Phase I Considerations

Rather than collecting information on the identification and organization of specific enemy units, we are concerned with the internal workings of insurgent activity groups. Knowledge of the composition of insurgent groups is a key to the entire planned course of the insurgency. Details of composition include the appearance of new organizations, the relative amount of enemy effort expended in rural and urban operations, the internal chain of C^2, and the manner in which insurgent groups are organized for operations.

Phase II Considerations

The intelligence analyst is concerned here with determining the composition of insurgent combat units, including their organization and chain of command. The degree of sophistication encountered indicates other factors, such as training, logistics, and strength. Armed platoons or small terrorist cells indicate that the overt military portion of the insurgents' plan is just beginning, and armed battalions and large urban terrorist groups indicate that there is a serious menace to the current government.

POLITICAL STRUCTURE

A tightly disciplined party organization, formally structured to parallel the existing government hierarchy in the country, is found at the center of some insurgent movements. In most instances, this organizational structure consists of comrnitted organizations at the village, district, province, interprovincial, and national levels. Within major divisions and sections of an insurgent military headquarters, totally distinct, but parallel, command channels exist. These are the military chain of command and the political channels of control. Whether it is through a political division of an insurgent military headquarters, a party cell or group in an insurgent military unit, or a unit political officer, the party ensures complete domination over the military structure by use of its own parallel organization. These party organizations fuel mil itary action. Should the military arm be eliminated, and the party left intact, only short-term security is achieved. The party begins construction of a new military organization. The population only is safe when the insurgent's political structure is rendered ineffective.

COMBAT FORCES

The organization of insurgent combat forces is dependent upon the need, the tactics to be employed, and the availability of personnel and equipment. Frequently, subordinate elements of insurgent units are employed independently. The intelligence analyst who receives a confirmed report of a subordinate element of an insurgent unit operating in the area cannot, therefore, assume that the parent unit is also present.

Identification of insurgent units are by--

- Number.
- Commander's name.
- Nickname.
- Code designation.
- Name of the area in which it operates.

Unit designations are frequently changed and multiple designations are often used to confuse friendly intelligence. It follows that the intelligence analyst is not able to determine the size and strength of an insurgent unit merely by obtaining a unit identification.

DISPOSITION

Determination of the disposition of the insurgent involves the location of operational training and supply bases, LOC, and areas of political control. The intelligence analyst arrives at potential dispositions of the insurgent combat forces by developing patterns of activity based upon map study and knowledge of insurgent tactics. Insurgent base areas, for instance, normally are located near areas that

the insurgents politically control, thereby providing an early warning system. By plotting insurgent sightings and combining this information with weather conditions, time factors, detailed investigation of insurgent incidents, and after action reports, the analyst best selects possible enemy dispositions as well as possible areas of tactical deployment. Consideration should also be given to areas where no insurgent activity is reported. These areas, while appearing to be under the control of internal defense forces, may be under the political control of the insurgents.

Phase I Considerations

The location, deployment within this location, and any movements of insurgent organizations or personnel are of concern here. The enemy's strength and tactics are revealed, to some extent, by discovering whether this effort is concentrated in a few places or dispersed throughout the target country and neighboring nations. If the enemy's effort is initially concentrated in one city or in one rural area, then the extent and spread of the insurgent organizations are a key to how long the enemy has been operational and how successful the enemy has been, and is an indication of the enemy's appraisal of friendly strength. In a nation considered a relatively easy conquest, the enemy begins with many operations, rather than a few. By studying the other available elements of 06 intelligence, the intelligence analyst determines such things as whether the movement of an enemy cadre or group is an advance toward new goals or a retreat from an unprofitable operation.

Phase II Considerations

How the insurgent forces are deployed indicates whether the enemy is making a widespread show of strength, with units scattered about the country, or is concentrating forces around a few key targets. It also shows whether the enemy is going to concentrate on such activities as interdicting transportation or actively seeking battle with government forces.

STRENGTH

The strength of the insurgent forces is thought of in terms of the combat forces, political cadres, and popular support. Conventional methods of strength computation are applied in determining insurgent combat forces strength. The analyst should be aware, however, that the insurgent will attempt to have strengths overestimated by low-intensity operations forces. To give this false impression, the insurgent employs rapid unit movement and uses multiple designations for a single element. Reports from the populace concerning the strength of the insurgent forces should be viewed with caution and the importance of actual counts of enemy personnel stressed. Certain insurgent-initiated incidents provide useful indicators of the strength of the insurgents in a particular area. An example of these is an increase in raids with subsequent loss of weapons by friendly forces. The determination of popular support for the insurgents is a more difficult task and is stated best in terms of the

percentage of an area under government control, as opposed to the percentage under insurgent control, with both viewed together in terms of population density. A useful indicator of the extent of insurgent political control is the willingness of the populace to report information concerning the insurgents.

Phase I Considerations

The cadre who organize and activate the movement usually are highly trained, aggressive professionals who exercise an influence disproportionate to their actual numbers. The analyst also is concerned with the number of enemy units in existence, which in phase I means identifying and evaluating new groups and organizations which have either appeared in the host nation or in neighboring countries and any changes in the size of existent groups. Other types of equipment, besides weapons, are of paramount interest. A printing press in phase I is a deadlier weapon than a battalion of artillery in phase III.

Phase II Considerations

The actual number of personnel available to the insurgent now assumes the importance it lacked, to some degree, in phase 1. By knowing also the amount of weapons and equipment available, estimates of capabilities against friendly forces are formulated. The degree of popular support for the insurgent manifests itself in such areas as recruiting for forces, tax or resource collection, and degree of population support for friendly forces.

TACTICS

Tactics include both enemy doctrine and the conduct of operations according to that doctrine. Insurgent forces are more flexible in their application of doctrine than regular military organizations. The doctrine which guides the insurgent must be known and understood by friendly forces if they are to effectively counter insurgent efforts. The careful examination of the tactics, or actual operational techniques, reveals changes in doctrine as well as indications of the personality and competence of the insurgent leader. Again, the choice and application of tactics is a reflection of insurgent appraisal of friendly strength as well as of personnel strength. A continuing estimate of relative strengths is a very basic part of insurgent operational planning and has an immediate effect on tactics. Tactics of the insurgent involve political, military, psychological, and economic considerations, all closely integrated. They vary with the phase of the insurgency. The political goal of the insurgents is to undermine and discredit the established government.

Phase I Considerations

Phase I insurgency is characterized by a relative absence of strictly military operations and an emphasis on subversion and organizational development. Although instances of terrorism begin to occur in the later

stages of phase 1, military activity is usually limited to recruiting and establishment of military cadres.

Phase II Considerations

An increased emphasis on the study and evaluation of insurgent military tactics is required. Tactics during phase II are generally limited to ambushes, raids, sabotage, and terrorism. These activities provide the insurgent with supplies, experience, and self-confidence, while at the same time they erode friendly morale and reduce friendly economic and military capabilities.

TRAINING

Insurgent training is closely related to the tactics being employed and includes vigorous indoctrination in political affairs. Both the combat forces and the people within an area under the political domination of the insurgents receive training. Insurgents carefully plan and train for individual operations and phases of movement. A careful analysis of an area with respect to the type of training taking place provides a useful indicator of the probable courses of action that are employed against friendly forces.

Phase I Considerations

During phase I, the insurgent trains and indoctrinates existing cadre as well as newly accepted or recruited indigenous personnel. Training consists of a great deal of political indoctrination along with techniques of propaganda, communications, and intelligence collection. Training and effectiveness go hand in hand; the type, amount, and val idity of training received by the insurgents is determined, to some degree, by any observed increase in the effectiveness or size of the insurgent movement. Some training normally is conducted in another country and is indicated by a change in number and type of personnel travel ing to that country.

Phase II Considerations

Much attention now is devoted to locating training camps and areas, identifying training cadres, and interdicting the movement of insurgents to and from out-of-country training areas. Some insurgent units are identifiable as having been trained for special missions, such as reconnaissance, demolition, or even suicide attack missions.

LOGISTICS

In an insurgency, as in a conventional warfare situation, the effectiveness of the insurgent is very much dependent on the logistical support. In the early stages of an insurgency, the requirements for military equipment and supplies are less than in the later stages. Accurate intelligence on the insurgent's sources and availab i lity of supplies and equipment is essential to determine the capabil i ty to maintain and expand the insurgency.

Phase I Considerations

Two particular items always are essential to the phase I insurgent--money and a printing press. If highly successful in the establishment and motivation of the power base, the insurgent never really has a requirement for the usual items of military supply. Money is often supplied from abroad, but such occurrences as bank robberies, unusual or excessive fund drives, payroll deduction requests, or sudden affluence among suspect government officials are cause for suspicion. Equipment for the production and dissemination of propaganda, like printing presses and radio sets, is of a special nature, and its acquisition by insurgent forces indicates an increasing level of sophistication in propaganda efforts.

Phase II Considerations

Logistics is now a larger and more elaborate requirement for the insurgent, who must now procure, store, transport, and maintain weapons, ammunition, explosives, signal equipment, and medical supplies. A much larger number of people are required to operate the logistical system. Insurgent supply caches or supply lines become items of critical concern to friendly forces. Borders and coastlines are controlled and aerial surveillance of remote areas or areas known to be used by the insurgents must be instituted to detect or deter the movement of supplies.

EFFECTIVENESS

Effectiveness describes the qualitative ability of the insurgent to achieve political or military purposes.

Phase I Considerations

In phase I, the term "combat effectiveness'" is usually not applicable. While the insurgent uses words like "struggle'" and "front,"' they do not connote the use of armed force. The overall effectiveness of the insurgent effort is sometimes made very obvious by spectacular successes (antigovernment victory in an important election) or failures (collapse of a new factory-worker organization known to have been backed by the insurgent), A continuing decline of governmental influence in a certain area or among a certain group of people may well indicate a corresponding increase in insurgent influence. The leaders forbid overt or easily detectable actions until they feel that their movement is in position to make a serious bid for power. In this case, the insurgent's real effectiveness remains unknown until it is too late for anything but a historical account of it. There usually is overt indication of the effectiveness of the insurgent operation, and information on it is gathered by careful observation of organizations, movements, and elections at all levels. Penetration of these activities by government agents is very desirable and makes a significant contribution to the OB picture.

Phase II Considerations

The factor of effectiveness now expands to include combat efficiency of insurgent military forces. By carefully evaluating the other OB factors, and taking note of actual combat experience, we evaluate the insurgent's combat effectiveness or lack thereof. We determine the insurgent's strengths and weaknesses and, from this, calculate the capability to follow various courses of action.

PERSONALITIES

Personalities are not listed as a separate OB factor in Chapter 3. In an insurgency, personal ities often assume a greater importance than in mid- and high-intensity conflicts.

Phase I Considerations

In phase I, personalities are an extremely important factor. During this phase, when the insurgency is just beginning to organize, function, and attempt to spread its influence, the loss of a comparatively small number of personnel practically destroys it or at least sets back its progress. Unfavorable publicity attached to the movement, as a result of exposure, renders its success less likely. The apprehension, compromise, or exposure of its leaders destroy the insurgency completely. Knowing who the insurgent leaders are also furnishes a valuable indication of how tactics and training are conducted and how effective the overall effort is.

Phase II Considerations

As in phase I, personalities remain a critical concern. Many insurgent units are cat led by their commander's name, rather than having a conventional designation.

ELECTRONIC TECHNICAL DATA

In the early stages, there is often a lack of uniform communications procedures, preventing the development of an extensive enemy electronic order of battle (EEOB) and electronic technical data base. There is very little use of noncommunications equipment, such as radar. The insurgents often use HF shortwave or ham radio sets to serve the initial "Committee of Correspondence'' function. VHF citizen band sets play a role in early terrorist operations. Equipment available to the insurgent ranges from the most primitive to the most modern. Even equipment not generally available in the armed forces of major world powers, I ike spread spectrum and frequency hoppers, is easily obtained.

Phase I Considerations

The propaganda requirements result in insurgent-sponsored medium frequency or commercial radio AM broadcasts. Transmitters are located outside the national boundaries or in remote, inaccessible areas. These broadcasts frequently use code words to control and coordinate insurgent

operations. Later, there is some increased use of VHF transmissions and more organized communications procedures. The standardization of communications practices reflects the level of communications training expertise.

Phase II Considerations

Much more extensive use of communications equipment characterizes this phase. Equipment is captured from government sources, purchased or stolen from commercial sources, provided by external sponsors, or locally manufactured. Communications procedures reflect doctrine and training practices of an external sponsor. Insurgents use repeater transmitters, set to receive and rebroadcast on the same frequency, to degrade VHF DF efforts against them.

MISCELLANEOUS

Any other items which contribute to knowledge of the insurgent, such as goals and methods, are considered here.

Phase I Considerations

This category includes such items as historical studies of people and parties involved in the insurgency, code names or numbers, and any' other information which does not fit under the other eight categories. "This type of information should not be slighted, as seemingly superfluous items may well become useful and important.

Phase II Considerations

Several miscellaneous items now become vital adjuncts to the other factors. Weapons, insignia, code names and numbers, types and colors of uniforms and flags--all these things aid in the identification of insurgent units, the source of outside aid, the source of weapons and equipment smuggled into or purchased in the target nations, and the morale and effectiveness of the insurgent armed forces,

OB FACTORS SUMMARY

There are three points to remember in the application of OB factors to an insurgency:

- The nine OB factors previously discussed are closely interrelated and cannot be analyzed separately.
- When an insurgency escalates from a phase I to a phase II situation, the OB effort is expanded considerably. The enemy combat units must now be considered in addition to the various phase I organizations and activities, which still are active.
- When an insurgency escalates from a phase II to a phase III situation, the application of the OB factors to the insurgent's combat units is the same as for other conventional forces.

APPENDIX A

REPORT FORMATS

The report formats described are standard formats used to report intelligence or information to task assets, or to receive information, intelligence orders, or instructions. These formats are echelon-specific, like the patrol report usually prepared at battalion level, or are general reports used at all echelons, like spot reports.

This appendix provides a brief description of the most common intelligence-related formats, including those formats used to pass information of immediate potential intelligence value from one echelon to another. It also identifies the echelon or echelons where each format is most used and the element or individual responsible for preparing it. An example of each format is also provided. Additional information about report formats is in Chapter 8.

SPOT REPORT

The SALUTE mnemonic requires users to report enemy size, activity, location, unit (or uniform), time, and equipment. Figure A-1 shows a spot report using a SALUTE message format.

```
FROM:  S2, 67TH INF, 3D BDE

TO:  G2 20TH INF DIV

COMBAT OUTPOST NO 26:--A/a/67 PATROL REPORTS SIGHTING FOUR ENEMY
TANKS MOVING WEST ALONG SECONDARY ROAD AT GRID COORD NB613397 AT
241730Z HR.  TANKS TRAVELLING AT APPROX 5 KPH.  HATCHES WERE
OPEN AND VISIBLE ENEMY PERSONNEL WERE WEARING PROTECTIVE MASKS.
UNIT MARKINGS WERE NOT VISIBLE BECAUSE THEY WERE COVERED WITH
MUD AND SANDBAGS.
```

Figure A-l. SALUTE messageformat.

INTELLIGENCE ESTIMATE

The intelligence estimate consists of five paragraphs. The first paragraph is a restatement of the mission. The remaining paragraphs outline an analysis of the battlefield area based on IPB; an estimate of enemy strengths, capabilities, and limitations; and the intelligence officer's conclusions about the total effects of the AO on friendly courses of action, the courses of action meet likely to be adopted by the enemy, and the effects of exploitable enemy vulnerabil ities. The five paragraphs are--

- Mission.
- Area of operations.

- Enemy situation.
- Enemy capabilities.
- Conclusions.

MISSION

Paragraph 1. Describe the mission in a short, clear, and concise restatement of the assigned or assumed mission of the command.

AREA OF OPERATIONS

Paragraph 2. Discuss what influence the AO has on probable enemy courses of action, based on facts and conclusions derived from IPB and an analysis of the AO if one has been prepared. A previously prepared analysis of the AO also is referenced. However, if previously prepared or other reference material is not contained in this paragraph, it must contain enough information to support the conclusions.

Weather and terrain analysis derived from IPB are always included in the characteristics of the AO. Other characteristics are included if they are important to either force in selecting courses of action to carry out their assigned or assumed mission. These other characteristics are of greater importance In AOs which have large civilian populations and to commands with extensive territorial or CSS responsibilities. Detailed or supporting terrain and weather information is included in an appendix to the intelligence estimate.

Weather or terrain effects on the use of nuclear weapons and chemical and biological agents are discussed when either combatant has the capability to use them. Each description of enemy courses of action includes the possible enemy or friendly use of these weapons, including the impact that weather or terrain conditions has on weapons systems and delivery means.

Weather

Weather conditions are those factors that impact on current and planned operations. This includes appropriate light data and either a weather forecast or climatic information. When operations cover a long period or are programed for a future operation, climatic information replaces weather data forecasts. Light data, in tabular form, includes the beginning of morning nautical twilight (BMNT) and beginning of morning civil twilight (BMCT), ending of evening civil twilight (EECT), and the ending of evening nautical twilight (EENT), moonrise, moonset, phases of the moon, and other information as required.

Terrain

The existing terrain situation includes the tactical aspects of the area: observation and fire, concealment and cover, obstacles, key terrain features, and AAs. Each of these aspects is oriented based on its

influence on selected courses of action by either force. For example, in a CSS unit, the discussion of concealment and cover is oriented toward influence on CSS courses of action, including installation locations required to accomplish the CSS mission and on enemy forces which interfere with the accomplishment of the mission. In CSS unit intelligence estimates, key terrain features are omitted unless the enemy has the capability to seize or control terrain features which materially affect the accomplishment of the mission.

Other Considerations

Other characteristics which are considered pertinent are sociology, politics, economics, and psychology, science, materiel, transportation, manpower, and hydrography.

The effects of each characteristic of the AO on possible enemy courses of action normally include consideration of weather, terrain, and NBC capabilities, the effects of these on other possible enemy courses of action, and the possible use of particular weapons, methods, techniques, or forces.

The extent of consideration for the factors is limited by the mission. For example, when the mission is offensive, the discussion does not include defensive courses of action. It does, however, include security considerations.

ENEMY SITUATION

Paragraph 3. Provide information on the enemy which permits later development of enemy capabilities and vulnerabilities. Establish the basis for refining these capabilities into a specific course of action and for determining the probability that the enemy will adopt this course of action.

Paragraph 3 provides the following data on the enemy:

- Disposition,
- Composition.
- Strength.
- Recent and present significant activities.
- Peculiarities and weaknesses.

Disposition

Enemy dispositions are the known or estimated locations and sizes of enemy units. References are made to overlays, enemy SITMAPS, or previously published documents when discussing enemy dispositions. However, if these references are not readily available, they (or a copy of them) are attached as appendixes to the intelligence estimate.

Composition

Composition is 06 data that is used to determine the strength the enemy uses to prevent the accomplishment of the mission. List all the units, including insurgent and guerrilla-type forces that contribute to this. Include such supporting units as air, nuclear delivery, and REC units that also affect the accomplishment of the mission. In determining which enemy units affect mission accomplishment, time and space factors are also considered.

Strength

Strength is all opposing enemy forces which are logically employed against the command in time to affect the accomplishment of the mission. The total forces listed cannot exceed, but is equal to or less than the total forces listed under composition.

Enemy strength includes committed forces, reinforcements, air assets, and NBC operations. Air or NBC operations units are omitted when the enemy lacks such capabilitles.

Committed Forces, Committed forces are those enemy ground maneuver units currently in contact and those ground maneuver units with which imminent contact is expected, regardless of the specific friendly course of action implemented. Designation of enemy forces as committed forces depends on disposition, location, controlling headquarters, and doctrine. For more information on computing enemy strength, see Appendix D.

Reinforcements. Reinforcements are those enemy maneuver units that are not committed in or out of the friendly sector, but react to the friendly course of action in time to influence the accomplishment of the mission. Contact with these units is not expected. Disposition, location, level of control , or other factors are considered in determining which enemy forces are reinforcements.

Enemy Air Capability. The enemy air capability is based upon numbers of enemy aircraft within operational radius, maintenance facilities, expected attrition, ground tactical situation, and other factors. The supporting tactical air force furnishes intelligence on the number of sorties, by type, which the enemy is expected to make within the field army or comparable areas. The estimate is not usually prorated below the field army level. Also, no attempt is made to calculate the number of sorties the enemy can or may make against a subordinate command of the field army or the communications zone (COMMZ). Corps, division, and COMMZ command intelligence officers usually quote the estimate furnished by the higher headquarters in stating enemy air capabilities. For example, a corps or division G2 might state: "30th Army estimates that the enemy can be expected to attack within the army area with as many as 150 fighter, 100 attack, and 75 bomber sorties daily. By massing all aircraft within operational radius, the enemy can make a maximum of 250 fighter, 300 attack, and 250 bomber sorties daily."

Nuclear Weapons and Chemical and Biological Agents. Estimates of enemy NBC capabilities usually are prepared at field army and hlglner headquarters. Units below field army level usually lack the means to gather the information to make such estimates. They use the estimates of the higher headquarters and modify them with available information.

The determination of enemy NBC operation capabilities is based primarily on estimates of numbers and types of weapons and amount and types of agents available, knowledge of enemy doctrine, past experience, and estimates of enemy capabilities involving the employment of ground troops. As with the enemy air capability, it is rarely feasible to estimate what portion of the available enemy NBC effort is used against a division or corps within a field army or a command in the COMMZ. It is also rarely feasible to estimate the number of nuclear weapons the enemy is capable of using within a period as short as one day. The period selected is a month or other period depending on the available information and past experience.

The statement of the enemy's capability to use chemical and biological agents includes the amount, typa, and delivery means of avai lab le chemica l and bio logical agents.

Recent and Present Significant Activities

This is a summary of recent and current enemy activities wh ich serve as indicators of future enemy actions. Significant enemy failures to take action also are listed. For example, if the enemy is apparently defending behind a river obstacle but has failed to destroy certain bridges, the omission is listed as a significant activity. Any basis for a belief that the enemy has specific knowledge of the friendly situation or intentions also is listed. For example, a capture by the enemy of an OPORD or a compromise of current signal operating instructions would be noted. For more information on enemy indicators, see Appendix C.

Peculiarities and Weaknesses

Briefly discuss each enemy peculiarity and weakness, indicating the extent to which it is a vulnerability and how it affects the selection of broad friendly courses of action. For example, if the enemy has an open flank, the fact is stated under operations. Discuss the extent to which the open flank constitutes an exploitable vulnerability. If enemy reserves are small and poorly positioned to extend the flank, the vulnerability may be great. If the enemy reserves are large and in position to extend the flank or counterattack an enveloping force, the vulnerability is probably insignificant. The G2 might state it as: "The enemy north flank is open. Available reserves are adequate to extend this flank a distance of only about 3,000 m. poSit ions to extend the flank have not been prepared. The enemy is vulnerable to a flank attack," Conversely, it might be stated as: "The enemy north flank is open. However, available reserves are adequate either to extend this flank beyond our zone, or to counterattack an enveloping force. Positions suitable to block an attempted envelopment have been prepared as shown on 'the enemy situation map." In the first statement, the enemy's

vulnerability to a flank attack is carried forward to conclusions of the intelligence estimate. In the second statement, the open flank apparently is not a vulnerability and is not carried any further. Another example: If the guerrilla forces are poorly equipped with antitank means of all types, the fact is stated under logistics, and the extent 'to which this is an exploitable vulnerability is discussed briefly. The intelligence officer might state: "The guerrilla forces in our area are poorly equipped with antitank means. They cannot effectively defend against armored vehicles" The inability to defend against armored vehicles is carried forward as a vulnerability to conclusions of the intelligence estimate. Figure A-2 shows some examples of enemy peculiarities and weaknesses.

PERSONNEL

-- Replacement situation (shortages or overages, particularly in specialists) .

-- Morale less than excellent, or exceptionally high.

-- Disproportionate number of very young or very old men.

-- High rate of sickness.

-- Percentage of authorized strength, if less than 80 percent.

INTELLIGENCE

-- Susceptibility to deception or neutralization of certain enemy information collection agencies.

-- Overdependence on one or more categories of information sources.

-- Ineffectiveness of enemy intelligence.

OPERATIONS

-- Habitual repetition of certain schemes of maneuver, or unconventional patterns of operations.

-- Faulty organization of the terrain.

-- Faulty disposition of reserves.

-- Susceptibility to electronic countermeasures.

-- Inadequate troop training, especially in defense against nuclear weapons or chemical agents.

-- Lack of adequate mobility.

Figure A-2. Example sof typical enemy peculiarities and weaknesses.

-- Inadequate air or artillery support, or nuclear weapon del ivery systems.

-- Pronounced failure to disperse and dig in.

-- Habitual failure to attack certain types of targets.

LOGISTICS

-- Shortages or inadequacies of particular supplies and materiel, including nuclear weapons.

-- Status of equipment, if less than 80 percent.

-- Large concentrations of supplies.

-- Location of vulnerable points and bottlenecks in the logistics system or lines of communications.

-- Inability to resupply during action.

-- Failure to equip troops with protective masks or protective clothing.

CIVIL-MILITARY OPERATIONS

-- Hostile attitude toward the civil populace, or of the civil populace toward the enemy.

-- Inadequacies in the control of civil communications, to include movement of civilians.

PERSONALITIES

-- Peculiarities or weaknesses of the enemy commander, major subordinate commanders, or principal staff officers as disclosed by or deduced from their past performance, education, politics, experience, or other basis.

Figure A-2. Examples of typical enemy peculiarities and weaknesses (continued).

ENEMY CAPABILITIES

Paragraph 4. List the enemy courses of action which tha enemy adopts and which influences the accomplishment of the friendly mission, either favorably or unfavorably. A properly stated enemy capability indicates what the enemy can do, when and where the enemy can do it, and in what strength. For example, "Attack (what) now (when) along our front (where) with five motorized battalions supported by all available nuclear weapons, artillery and air (strength). " Another example: "Conduct harassing operations (what) at any time (when) in our area (where) with about 200 guerrillas equipped only with small arms (strength)."'

The evidence considered in the analysis and discussion of enemy capabilities includes characteristics of the AO and positive or negative evidence of enemy activity, listed under recent and present significant activities. A major obstacle across part of the friendly area is evidence that attack elsewhere is more likely. Low ceilings and low visibility are evidence that the enemy is not using all available aircraft. Open, flat areas without any appreciable cover are evidence that the enemy does not use guerrilla or infiltration forces.

In analyzing and discussing each enemy capability or appropriate combination, the intelligence officer judges from the enemy point of view the advantage or disadvantage of adopting the capability. In making this judgment, the G2 or S2 also considers enemy doctrine and practices and the ultimate results of adopting or rejecting the particular capability. For example: "Employment of the unidentified tank division at TNOMYEH deprives the enemy of the reserves needed to counterattack a penetration by either of the two friendly divisions to our south. Commitment of this tank division too early will result in the later defeat of the enemy."

If there is no evidence of the enemy's possible adoption of a particular capability and the capability does not represent a major threat to the accomplishment of the mission, the intelligence officer does not judge it. For example, the enemy usually withdraws beyond our objective. Ordinarily, such withdrawal is not a threat to the accomplishment of the mission. If there is no evidence that the enemy withdraws, a statement of conclusions is omitted. The intelligence officer states: "There is no indication of withdrawal. "

CONCLUSIONS

Paragraph 5. State the intelligence officer's estimate of the--

- Total effects of the AO on friendly courses of action.
- Courses of action most likely to be adopted by the enemy, including their relative probability of adoption.
- Effects of enemy vulnerabil ities that can be exploited.

For a defensive mission, conclusions identify the best defense areas and the best AAs into the defense sector. For an offensive mission, the conclusion describes the best AA to the objectives.

Determine the enemy probable courses of action by the previous analysis and discussion of enemy capabilities. Consider how the enemy views the vulnerabilities as indicated by doctrine, past experiences, and the personality of the enemy commander. Consider previous enemy courses of action selected under similar circumstances. The determination is objective and not an unsubstantiated guess at what the enemy will do.

In determining the relative probability of adoption of enemy courses of action, the intelligence officer avoids conclusions based on friendly doctrine and practices. The officer considers the available evidence, to

include the enemy doctrine and practices, as well as positive or negative enemy activity, If enemy activity is not definitive enough to justify selection of the enemy's most probable course of action, the officer determines the most probable one based on the characteristics of the AO, enemy doctrine, practices, and previous experiences.

In the statement of the courses of action most likely to be adopted by the enemy, several capabilities are combined for brevity and clarity. However, all of the enemy capabilities combined in one statement are capable of being implemented at the same time. For example, the most probable enemy course of action is to: "Attack to envelop our northern flank, reinforced by corps reserve and using all available nuclear weapons, artillery, and air support; and conduct harassing operations in our rear areas with guerrillas and infiltrating forces. "

If more than one enemy course of action is stated, they are listed in the order of their probability of adoption.

An enemy vulnerability is any condition or circumstance of the enemy situation or the AO which makes the enemy especially liable to damage, deception, or defeat. Only those enemy weaknesses which are exploited are considered. In studying the enemy peculiarities and weaknesses to determine such vulnerabilities, the characteristics of the AO, all aspects of the enemy situation, and the enemy's doctrine and practices are considered. Only actual vulnerabilities are presented. An open northern flank which the enemy cannot, with available forces, extend or defend, is a vulnerability. If, however, the enemy has reserves which readily extend the flank to an impassable obstacle or counterattack to pin enveloping troops against that obstacle, the open flank is mentioned as a possible vulnerability, although the vulnerability may be eliminated by commitment of the enemy reserves. However, the commitment of reserves creates another vulnerability.

Each exploitable enemy vulnerability is listed as a brief statement of the effect of the vulnerability rather than a repetition of the peculiarity or weakness. For example: "Shortage of antitank means" is not stated. Instead, the effect of that weakness is given by stating: "Limited capability to oppose armored vehicles. " If the enemy's north flank is vulnerable, it could be stated as: "'Enemy northern flank open to envelopment subject to destruction of enemy reserves at . . . ."

In determining enemy vulnerabilities, the G2 or S2 considers the feasibility of their exploitation and makes appropriate recommendations to the G3 or S3. All enemy vulnerabilities are not exploited at the same time. The exploitation of one vulnerability precludes the exploitation of another vulnerability.

For example, the enemy is vulnerable to both a night penetration and a daytime flank envelopment. The G3 or S3, in coordination with the G2 or S2, recommends to the commander the priority of vulnerabilities to be exploited. Based on the information in this appendix and in Chapter B, Figures A-3 through A-5 show the formats for the annotated intelligence estimate, sample intelligence estimate for a division, and an annotated intelligence estimate for stability operations.

(Classification)

Headquarters
Place
Date, time, and zone
Msg Ref No

INTELLIGENCE ESTIMATE NO_____
References: Maps, charts, or other documents.
Time Zone Used Throughout the Estimate:

(Short title identification)

1. MISSION. The restated mission determined by the commander.

2. AREA OF OPERATIONS. This paragraph discusses influence of the battlefield environment in arriving at conclusions. It is based on the facts and conclusions of IPB and the analysis of the battlefield area, if one has been prepared. It may be a reference to an analysis of the battlefield, if adequate coverage and discussion are contained therein.

a. Weather.

(1) Existing situation. Include light data and either a weather forecast or climatic information, as appropriate. Use appendixes for detailed information.

(2) Effect on enemy courses of action. Describe the effects of weather on each broad course of action (such as attack or defend). Each description concludes with a statement of whether the weather favors the course of action. Among the courses of action, include use of chemical agents, nuclear weapons, and special methods, techniques, equipment, procedures, or forces.

(3) Effect on own courses of action. Describe in the same manner as for (2) above, except that the estimate excludes the use of biological agents.

b. Terrain.

(1) Existing situation. Use graphic representations, such as IPB templates, where possible. Use annexes for detailed material. Include as much information as necessary for an understanding of observation and fire, concealment and cover, obstacles, key terrain features, and AAs. Include effects of nuclear fires, enemy biological and chemical agents, and any other pertinent considerations on each of these factors as appropriate.

(Classification)

Figure A-3. Annotated intelligence estimate.

(Classification)

(Short title identification)

(2) Effect on enemy courses of action. Describe in the same manner as for the effects of weather in a(2) above. For defensive courses of action, state the best defense area and the best AAs leading to it. For attack courses of action, state the best AAs.

(3) Effect on own courses of action. Describe in the same manner as for effects of weather in a(3) above.

c. Other Characteristics. The following additional characteristics considered pertinent are included in separate subparagraphs: sociology, politics, economics, psychology, and other factors. Other factors may include such items as science and technology, materiel, transportation, manpower, and hydrography. These factors are analyzed using the same subheadings as weather and terrain.

3. ENEMY SITUATION. This paragraph gives information on the enemy which will permit later development of enemy capabilities and vulnerabilities and refire ment of these capabilities into a specific c urse of action and its relat ve probability of adoption.

a Disposition. Reference may be made to over ays, enemy situation maps, or previously publ ished documents.

*

b Composition. Summarize enemy OB that can influence accomplishment of the mission. Reference may be made to previously published documents. Special mention is made of units capable of EW, low-intensity operations, and other special operations, as appropriate.

c. Strength. Enemy strength is listed as committed forces, reinforcements, air assets, nuclear weapons, and chemical and biological agents. The purpose of this listing is to assist in developing enemy capabilities and vulnerabilities for use by the commander and staff in selecting courses of action. The unit mission, location of the enemy, enemy doctrine, and the level of command at which the estimate is being prepared are factors to be considered.

(Classification)

Figure A-3. Annotated intelligence estimate (continued).

(Classification)

(Short title identification)

(1) Committed forces. List those enemy ground maneuver units currently in contact and those ground maneuver units with which imminent contact can be expected, regardless of the specific friendly course of action implemented. Designation of enemy forces as committed forces depends on disposition, location, controlling headquarters and doctrine. The intelligence officer usually accounts for committed forces based on the size unit doctrinally used to oppose the friendly unit. Generally, enemy units are counted in terms of units two echelons below the friendly unit's size (for example, a brigade S2 normally considers committed forces in terms of companies; a division G2, in terms of battalions; and a corps G2, in terms of regiments). If there is doubt whether a unit is a committed force or a reinforcement, it is considered a reinforcement.

This attributes to the enemy the maximum capability to reinforce forces to oppose a given friendly course of action.

(2) Reinforcements. Include designation and location. Reinforcements are those enemy maneuver units that may or may not be employed against us, depending on our choice of a specific course of action and enemy plans. Reinforcements are enemy units not committed in or out of the friendly sector, but which can react to the friendly course of action, subject to time and distance considerations, in time to influence the accomplishment of the mission. Imminent contact is not expected. Disposition, location, level of control, or other factors at the time of the estimate are considered in determining which enemy forces are reinforcements.

(3) Air. List the number of enemy aircraft by type within operational radius. Include the number of possible sorties per day by type of aircraft, if known.

(4) Nuclear weapons and chemical and biological agents. Estimate, as appropriate, the number, type, yield, and delivery means of enemy nuclear weapons and chemical and biological munitions or agents available to the enemy.

d. Recent and Present Significant Activities. List selected items of information to provide bases for analyses to determine relative probability of adoption of specific courses of action and enemy vulnerabil ities. Enemy failures to take expected actions are listed, as well as positive information.

(Classification)

Figure A-3. Annotated intelligence estimate (continued).

(Classification)

(Short title identification)

e. Peculiarities and Weaknesses. Based on knowledge of enemy tactical doctrine, practices, the principles of war, the AO, and the enemy situation previously described and discussed, list peculiarities and weaknesses, and briefly describe each, indicating the extent to which they may be vulnerable and how they influence possible friendly courses of action. The items listed are grouped under the headings indicated below. Only pertinent headings are used.

(1) Personnel. An estimate of strength usually is included if less than 80 percent of authorized strength. Status of morale is included, if known.

(2) Intelligence. An estimate of enemy intell igence success, ineffectiveness, and susceptibility to deception and detection is usual ly included.

(3) Operations. An estimate of combat effecti veness is usually included if less than excellent.

(4) Logistics. An estimate of the enemy's capability to support their forces logistically is included if there are apparent weaknesses.

(5) Civil-military operations. An estimate of the attitudes of the enemy and the civilian populace and the status of food supply, medical facilities, communications, and other critical resources is usually included.

(6) Personalities. An estimate of the capabilities and or weaknesses of the enemy commander and principal staff officers usually is included.

4. ENEMY CAPABILITIES. Based on all the previous information and analyses, develop and list enemy capabilities. The listing provides a basis for analyzing the available information to arrive at those capabilities the enemy can adopt as specific courses of action and their relative probability of adoption.

a. Enumeration. State what, when, where, and in what strength for each capability.

(Classification)

Figure A-3. Annotated inteiiigence estimate (continued).

(Classification)

(Short title identification)

b. Analysis and Discussion. To provide a basis for conclusions of enemy capabilities and their relative probability of adoption, each capability, or appropriate combination thereof, is discussed in a separate subparagraph. Consideration of enemy deception measures is included. All the pertinent previous information and conclusions are tabulated as either supporting or rejecting the adoption of the capability. After listing all the evidence, each capability is judged from the enemy point of view of whether the adoption of the capability is advantageous to the enemy. Such judgments need not be made if the conclusion is obvious or if there is no evidence that the enemy will adopt the capability, except when the capability is one that will make the accomplishment of the friendly mission highly doubtful or impossible. This exception is to focus attention on dangerous threats.

5. CONCLUSIONS. Based on all the previous information and analyses, conclusions are stated concerning the total effects of the AO on friendly courses of action; the courses of action most likely to be adopted by the enemy, including their relative probability of adoption; and the effects of enemy vulnerabilities that can be exploited. These conditions assist in the selection of a friendly course of action.

a. Effects of Intelligence Consideration on Operations. Indicate whether the mission set forth in paragraph 1, above, can be supported from the intelligence standpoint. Indicate which courses of action can best be supported.

b. Effects of the AO on Own Courses of Action. For attack courses of action, indicate the best AAs. For defensive courses of action, indicate the best defense areas and the best AAs leading to and into the defense areas. (This subparagraph is omitted if the discussion of the effects of the area on own courses of action in paragraph 2 has been omitted because of the availability of a current analysis of the AO.)

c. Probable Enemy Courses of Action. List courses of action in order of relative probability of adoption. A listed course of action may include several subordinate courses of action that can be executed concurrently. Usually, no more than two or three courses of action, in order of probability of adoption, can be justified by the available evidence.

(Classification)

Figure A-3. Annotated intelligence estimate (continued).

(Classification)

(Short title identification)

d. Enemy Vulnerabil ities. List the effects of peculiarities and weaknesses that result in vulnerabilities that are exploitable at own, higher, or lower levels of command. The order in listing these vulnerabil ities has no significance.

/s/ (Designation of staff officer)

OFFICIAL:
G2's Signature Block

Annexes (as required)
Distribution:

(Classification)

Figure A-3. Annotated intelligence estimate (continued).

(Classification)

Copy --- of --- Copies
G2 Section, 52d Division (Mech)
GLENVILLE (NF3277), EASTLAND
2308302 June 19
Msg Ref No. –

INTELLIGENCE EST MATE NO 20
Reference: Map, series East and, sheets Delta through Kilo, edition 2, 1:50,000 Time Zon e Used Throu ghout the Estimate: Zulu.

1. MISSION. 52d Div defends along Dry Creek and prepares to attack on order.

2. AREA OF OPERATIONS.

a. Weather.

(1) Existing situation. Weather for the period 23 to 28 June #ill be rainy and cool, gradually warming and clearing as a high pressure system moves through the AO from the south. Temperatures from 40 to 65°F . Visibility will range from 16 to 25 kilometers, except during precipitation and in morning fog in low drainage areas. Surface winds from the south at 8 to 10 knots.

Date	BM-NT	BM-CT	EE-CT	EE-NT	Moon-rise	Moon-set
23 June	0331	0419	2029	2130	1746	0125
25 June	0339	0422	2025	2124	1907	0214
27 June	0344	0425	2022	2118	2001	0518
28 June	0349	0428	2018	2112	2022	0820

(2) Effects on enemy courses of action:

(a) Precipitation will not hinder cross country movement except in the low drainage areas of Minertown.

(b) Southerly winds will not affect enemy employment of NBC.

(c) Low visibility during precipitation and morning fog will favor enemy attack.

(3) Effects on friendly courses of action:

(Classification)

Figure A-4. Sample division intelligence estimate.

(Classification)

(a) Precipitation will not hinder cross country movement except in the low drainage areas of Minertown.

(b) Southerly wind direction will not affect friendly use of chemical or nuclear weapons.

(c) Low visibility during precipitation and morning fog will not favor friendly defense.

b. Terrain.

(1) Existing si tuation.

(a) Cover and concealment. Wooded areas around Midway offer good concealment. Numer ous ravines in drainage areas of Minertown offer limited cover and concealment.

(b) Observation and fire. There are good observation points along bluffs above Gringo River. Fields of fire are excellent throughout plains areas north of Mud Creek but limited moderately in populated and vegetated areas near Glenville.

(c) Obstacles.

1 Swift River (fordable 1 km east of Glenville).

2 Bluffs above Gringo River.

3 City of Glenville. Routes around city are passable; routes through city impassable.

(d) Key terrain. Hill mass Jackson and Hill 333.

(e) AAs.

1 Available to the enemy into our sector:

a AA 1 is from Largo through gap around the northeast end of HILL 702, 34 km southwest to Minertown and south to Dry Creek.

b AA 2 is from Largo southeast through Midway to river crossing east of Glenville.

(Classification)

Figure A-4. Sample division intelligence estimate (continued).

(Classification)

2 AA available for US movament into the enemy's area is generally the same as those I isted for enemy into our sector.

(2) Effect on enemy courses of action. Terrain favors the enemy attack using AA 1.

(3) Effect on friendly courses of action. Terrain favors our defense of the srea around Dry Creek.

c. Other Characteristics.

(1) Existing situation. Local nationals throughout the area favor friendly military operations. Large numbers of refugees can be expected to pass through friendly lines.

(2) Effect on enemy courses of action. The enemy can be expected to insert infiltrators as refugees.

(3) Effect on friendly courses of action. Refugees can be expected to provide valuable inteliigence.

3. ENEMY SITUATION.

a. Disposition. Annex A, Situation Overlay.

b. Composition. Enemy forces opposing 52d Div consist of elements of the 4th Combined Arms Army.

(1) Identified units are--

(a) 10th MRD consisting of--

--27th MRR.
--30th MRR.
--31st MRR.
--121st Tk Regt (unlocated).

(b) 19th Mech Div consisting of--

--23d MRR.
--37th Tk Regt.

(2) Unidentified units are: 2 x U/l MRR of 19th MRD.

(Classification)

Figure A-4. Sample division inteiiigence estimate (Continued).

(Classification)

c. Strength.

(1) Committed forces. 52d Div (Mech) is opposed immediately by four mechanized battalions and one tank battalion. These units are supported by normal divisional and regimental artillery groups.

(2) Reinforcements. Reinforcements available to the enemy for commitment in our zone are a total of five MRB and four tank battalions from the 27th MRR, 121st Tk Regt, and the second-echelon battalions of the 30th and 31st MRRs and the 37th Tk Regt. Also, the 23d MRR can totally reinforce within 8 hours from start of movement.

(3) Air. Enemy is supported by the 3d Air Army consisting of unidentified numbers of fighter-bomber aircraft, ground attack aircraft, and reconnaissance aircraft. Air parity currently exists with either force capable of obtaining air superiority for limited periods of time. Up to now enemy has used a maximum of 60 fighter-bomber sorties in a 12-hour period.

(4) Nuclear. No estimate of the enemy's nuclear support for the next 30 days is available. Enemy currently has 152mm Gun-Hows with nuclear rounds and SSMS which can del iver rounds of 10-50 kt yield within range of our division.

d. Recent and Present Significant Activities.

(1) Air reconnaissance and photo reports indicate increased enemy movement along axis Bravo to Limo. Movement indicates reinforcement of forward element of 4th CAA.

(2) Enemy's aerial recon and tactical air flights have increased in the last 36 hours, particularly along the I ine of contact.

(3) For the past 36 hours, volume of vehicular traffic has increased in southerly direction.

(4) Artillery fire from the enemy has become more intensive in the last 24 hours.

(5) Reliable source reports large tracked, amphibious vehicles mov ng into area vicinity Hill 805.

(Classification)

Figure A-4. Sample division intelligence estimate (continued).

(Classification)

(6) Enemy has begun to employ smoke along the forward slope of Hill 702.

e. Peculiarities and Weaknesses.

(1) Personnel. Enemy units are currently estimated to be at 85 to 90 percent authorized strength. Morale is high, although replacements may not be highly trained.

(2) Intelligence. Enemy stresses communications security and subordinate units of the 4th CAA have recently initiated intensive radio security and procedures training.

(3) Operations.

(a) Enemy is susceptible to mine warfare and antitank weapons.

(b) Enemy has trained heavily on attack formations and has been told offensive action is the only way to victory.

(c) Enemy is vulnerable to nuclear weapons due to massed forces and canalization by further advancement.

(4) Logistics. Supplies are adequate for the enemy's conduct of either the offense or defense. The enemy had previously stockpiled supplies wel l forward in division areas.

(5) Personal ities. GD Masonski, CG of the 10th MRD, is an advocate of penetration type offense on a narrow front with subsequent widening of the gaps to split enemy forces.

4. ENEMY CAPABILITIES.

a. Enumeration:

(1) Attack at any time along AA 1 with four MRBs and one tank battalion supported by normal d visional and regimental artillery groups.

(2) Attack at any time along AA 2 with four MRBs and one tank battalion supported by normal divisional and regimental artillery groups.

(Classification)

Figure A-4. Sample division intelligence estimate (continued).

(Classification)

(3) Defend at any time with forces in contact supported by all available divisional and regimental artillery groups.

(4) Reinforce the attack or defense with all or part of the following units at the places and times indicated:

	UNIT	PLACE	TIME
(a)	30th MRR(-)	A A 2	immediately
(b)	31st MRR(-)	AA 1	immediately
(c)	37th Tk Regt (-)	AA 1	immediately
(d)	27th MRR	AA 1 or 2	2 hr after start of movement
(e)	23d MRR	vic Little	8 hr after start of movement
(f)	121st Tk Regt	Unlocated	Unknown
(g)	U/l MRR of 19th MRD	vic Bravo	9 hr after start of movement

(5) Delay in successive positions to the east of Little.

(6) Employ chemical agents within our sector at any time.

(7) Employ nuclear weapons of a 0.5-50 kt yield with delivery by artillery or SSM.

(8) Employ guerrilla forces in our rear area either alone or in communication with the capabilities enumerated below.

(9) The enemy can attack our area with an undetermined number of fighter, ground attack, and bomb sorties daily. The maximum number of daily sorties mounted in our area has been 60.

(Classification)

Figure A-4. Sample division intelligence estimate (continued).

(Classification)

b. Analysis and Discussion.

(1) Attack along AA 1.

(a) The following indicate adoption of this capability:

1 Uses a good AA.

2 The enemy is massing mechanized elements, tanks, artillery and logistic support along this avenue.

3 Forward elements disposed on a relatively narrow front.

4 Extensive artillery preparation along approach.

(b) The scant cover presented along this AA is a limiting factor but does not preclude adoption of this capability.

(2) Attack along AA 2.

(a) The following indicate adoption of this capability:

1 The enemy is massing mechanized elements, tanks, artillery and logistic support along this avenue.

2 Forward elements disposed on a relatively narrow front.

3 Extensive artillery preparation along this avenue.

(b) The following indicate rejection of this capability:

1 This AA accommodates only one deployed regiment and offers limited cover and concealment.

2 The limited obstacle presented by Glenville.

(3) Defend. The following indicate rejection of this capability:

(a) The enemy is massing forces along the line of contact.

(b) Enemy has followed known doctrine for attack.

(Classification)

Figure A-4. Sampie division intelligence estimate (continued).

(Classification)

(c) Terrain favors attack.

(4) Reinforce. The following indicates adoption of this capability:

(a) Movement of additional troops toward the front.

(b) New units identified in the combat zone.

(c) Forward logistical buildup.

(5) Delay. There are no indications of the enemy's adoption of this capability.

(6) Employ chemical agents. There is no indication the enemy will employ chemical agents other than smoke.

(7) Employ nuclear weapons. There is no indication the enemy will employ nuclear weapons.

(8) Employ guerrilla forces. The following indicates adoption of this capability:

(a) Doctrine calls for use of guerrilla force.

(b) Use would enhance enemy advance by creating panic and confusion.

(9) Air attack. Indications are that enemy will continue to employ this capability as referenced in paragraph (9) above.

5. CONCLUSIONS.

a. Intelligence. Available intelligence indicates that the division can accomplish its mission. Intelligence supports adoption of the division course of action.

b. Weather and Terrain. The weather and terrain favors our defense. The beat defensive area is the high ground east of Dry Creek. The best AA into our defensive sector is AA 1.

c. Probable Enemy Courses of Action.

(Classification)

Figure A-4. Sample division intelligence estimate (continued).

(Classification)

(1) Attack with forces in contact supported by air and artillery with the main attack of one mechanized regiment along AA 1. Will reinforce w th elements as indicated in para 4a(4).

(2) Conduct secondary attack with forces in contact supported by air and arti llery with one mechanized regiment along AA 2.

(3) Employ guerrilla or special forces in our rear areas in conjunction with the above courses of action.

d. Enemy Vulnerabilities.

(1) The enemy is vulnerable to counterattack due to slowness to exploit potential penetrations.

(2) Vulnerable to nuclear attack due to massing of troops and concentrated logistics depots.

(3) Mine warfare will be effective against mechanized elements.

KROOK

BG

OFFICIAL:

/s/ Bagger

BAGGER

GS

Annex: A--Situati on Overlay (omitted)
Distribution: A

(Classification)

Figure A-4. Sample division intelligence estimate (continued).

(Classification)

Copy --- of --- Copies
Preparing Staff Element
Organization
Location
Date-Time Group
Msg Ref No

INTELLIGENCE ESTIMATE NO _.
References: maps, charts, or other documents.
Time Zone Used Throughout the Estimate: Zulu

1. MISSION. (States the current or proposed mission of the force designated for stability operations.)

2. THE AREA OF OPERATIONS. (This paragraph discusses characteristics of the host country, the area, and their probable effect upon both insurgent and government courses of act ion.)

a. Geography. (Includes climate and topography.)

(1) Existing situation.

(2) Effect on insurgent courses of action.

(3) Effect on government courses of action.

b. Politics. (Includes governmental organization, political parties, and interest groups.)

(1) Existing situation.

(2) Effect on insurgent courses of action.

(3) Effect on government courses of action.

c. Economy. (Includes private enterprise and publ ic facilities.)

(1) Existing situation.

(2) Effect on insurgent courses of action.

(3) Effect on government courses of action.

(Classification)

Figure A-5. Annotated intelligence estimate for stability operations.

(Classification)

d. Sociology (Includes minority groups and social programs.)

(1) Existing situation.

(2) Effect on insurgent courses of action.

(3) Effect on government courses of action.

e. Psychology. (Includes behavior patterns and motivating factors.)

(1) Existing situation.

(2) Effect on insurgent courses of action.

(3) Effect on government courses of action.

3. THE INSURGENT SITUATION. (This paragraph discusses the insurgent organization and its activities.)

a. Organization and Leadership. (Includes composition.)

(1) Nonmilitary. (Includes the underground.)

(2) Military. (Includes all insurgent armed elements.)

b. Strength and Disposition.

(1) Nonmilitary.

(2) Military.

c. Recent and Present Significant Activities.

(1) Nonviolent action. (Includes political, economic, sociological, and psychological action.)

(2) Terrorist action. (Includes murder, torture, extortion, kidnapping, and sabotage.)

(3) Guerrilla operations. (Includes harassment, destruction, interdiction, and dispersion.)

(Classification)

Figure A-5. Annotated Intelligence estimate for stability operations [continued).

(Classification)

(4) Conventional tactical operations. (Includes attack, defense, clay, and withdrawal.)

d. Strengths and Weaknesses.

(1) Recruitment and retention.

(2) Intelligence and security.

(3) Organization and training.

(4) Finance and logistics.

(5) Communications.

4. INSURGENT CAPABILITIES. (This paragraph lists current insurgent capabilities and discusses them in regard to probability of adoption.)

a. Enumeration. (Includes what, where, when, and how for each capability.)

(1) Basic capabilities.

(a) Nonviolent action.

(b) Terrorist action.

(c) Guerrilla operations.

(d) Conventional tactical operations.

(e) Employment of chemical, biological, or nuclear weapons.

(2 Supporting capabilities.

(a) Intelligence and security.

(b) Recruitment and retention.

(c) Organization and training.

(d) Finance and logistics.

(Classification)

Figure A-5. Annotated intelligence estimate for stability operations (continued).

(Classification)

(e) Reinforcement capabilities.

b. Analysis and Discussion. (Includes all evidence supporting or rejecting the adoption of each capability.)

5. CONCLUSIONS. (This paragraph draws conclusions from the content of :he preceding paragraphs and furnishes a basis for selection of courses of action to accomplish the assigned miss ion.)

a. Effects of the Operational Environment. (States the total effect of the AO upon courses of action.)

b. Probable Insurgent Courses of Action. (Lists probable insurgent courses of action in order of relative probability of adoption.)

c. Insurgent Vulnerabilities, (Lists exploitable insurgent vulnerabilities.)

/s/ _____
G2 or S2
(Commander if distributed outside headquarters)

ANNEXES:
Distribution: (If distributed only.)
Authentication: (G2 or S2 authenticates if commander signs estimate.)

(Classification)

Figure A-5. Annotated intelligence estimate for stability operations (continued).

INTELLIGENCE ANNEX TO THE OPORD OR OPLAN

The intelligence annex disseminates information about enemy forces which is essential to the conduct of the operation and to give any other necessary intelligence orders or guidance for the operation(s) in question. It also serves as a medium for instructing subordinate commanders to acquire information necessary for the conduct of the operation but which can only be obtained immediately before or when the operation itself has begun. The intelligence annex is not a substitute for an intelligence collection plan; rather it is a way to communicate the taskings and requests of the collection plan.

The intelligence annex is a formal intelligence tasking document that accompanies an OPLAN or OPORD. It should be as brief as possible consistent with clarity. Its first paragraph is a summary of the enemy situation required to understand the OPLAN or OPORD and refers to annotated maps, enemy situation overlays, or current intelligence reports. Subsequent paragraphs contain specific collection requirements and instructions. SOP information should not be repeated in the intelligence annex. Figures A-6 and A-7 show a general intelligence annex format and division intelligence annex example.

(Classification)

(Change from oral orders, if any)

Copy no __ of __Copies
Issuing headquarters
Place of issue (may be in code)
Date-time group of signature
Message reference number

ANNEX (INTELLIGENCE) to OPERATION ORDER NO _.
References: Maps, charts, and other relevant documents.
Time Zone Used Throughout the Order: Zulu

1. SUMMARY OF ENEMY SITUATION. Information about enemy forces essential in implementing the operation plan. When the amount of detail makes it appropriate, a brief summary and reference to the appropriate intelligence document, or appendix to the annex, may be used. Reference to documents not included in the annex should not be made when they ara not available to all recipients of the annex.

(Classification)

Figure A-6. Intelligence annex format.

(Classification)

2. INTELLIGENCE REQUIREMENTS. List each PIR in a separate subparagraph. If a priority has been assigned to the PIR list in order, so state. In a final subparagraph, list IRs, if any. If an intelligence annex is not prepared or is distributed separately from the basic order, PIR should be listed in the coordinating instructions subparagraph of the OPORD.

3. INTELLIGENCE ACQUISITION TASKS.

a. Orders to Subordinate and Attached Units. List, by unit, in separate numbered subparagraph, detailed instructions for reports required by the issuing headquarters. Units are listed in the same order as they are I isted in the OPORD.

b. Requests to Higher, Adjacent, and Cooperating Units. List in a separate numbered subparagraph requests for information from units not organic or attached.

4. MEASURES FOR HANDLING PERSONNEL, DOCUMENTS, AND MATERIEL. This paragraph contains instructions about the operation that are not contained in SOP or that modify or amplify SOP for the current operation. Examples include--

a. E P Ws, Deserters, Repatriates, Inhabitants, and Other Persons, Special handling and segregation instructions. Location of EPW collection point as provided by the provost marshal.

b. Captured Documents. Instructions for handling and processing of captured documents from time of capture to receipt by specified intelligence personnel .

c. Captured Materiel. Designation of items or categories of enemy materiel for examination, and specific instructions for their processing and disposition.

5. DOCUMENTS OR EQUIPMENT REQUIRED. This paragraph lists, in each category, the conditions under which certain documents or equipment required by or allocated to units can be obtained or requested. Items may include air photographs and maps.

6. COUNTERINTELLIGENCE.

a. This paragraph is covered largely by SOP. Many special operational instructions having Cl aspects are I isted in the OPORD or in other annexes.

(Classification)

Figure A-6. Intelligence annex format (continued).

(Classification)

b. Certain instructions and procedures on the conduct of special personnel in the operation may require limited dissemination on a need-to-know basis; therefore, a special CI measures appendix may be prepared for a limited and specified number of addresses.

7. REPORTS AND DISTRIBUTION. This paragraph may be covered largely by SOP. It stipulates the conditions (for example, dates, number of copies, issue) regulating the issue of intelligence reports to the originating command for the duration of the operation. Any or all of the following items may be covered in this paragraph:

a. Period to be covered by routine reports and distribution.

b. Routine and special reports that differ from SOP required from subordinate units.

c. Periodic or special conferences of inte lligence officers.

d. Distribution of special intelligence studies, such as defense overprints, photointelligence reports, and OB overlays.

em Special intelligence liaison, when indicated.

8. MISCELLANEOUS INSTRUCTIONS (if required). List here, under separate subparagraphs, necessary items that are not covered above or in SOPS, or which require action different from that detailed in SOPS.

Acknowledge

Last name of commander
Rank

Authentication:
Appendixes:
Distribution:

(Classification)

Figure A-6. Intelligence annex format (continued).

(Classification)

(Change from oral orders, if any)

Copy 4 of 5 Copies
20th Inf Div
Zelle (4671), Buttano
1019OOZ Sep 45
BQ 13

Annex A (Intelligence) to Operations Order 24
Reference: Map, Buttano, Edition 2, 1:50,000 sheets 204 (Zelle-Pagt).
Zulu Time

1. SUMMARY OF ENEMY SITUATION. See INTSUM, this HQ, 1018OOZ September, and Appendix 1, Situation Overlay.

2. INTELLIGENCE REQUIREMENTS.

a. PIR.

(1) Will enemy reinforce the forces along the Flood River before the time of attack? If so, when, where, and with what forces? Special attention to the mechanized regiment and the medium tank regiment in vicinity of Burg.

(2) Will enemy employ nuclear weapons against us? If so, when, where, how many, of what yields, and by what delivery means?

b. IR.

(1) Will enemy continue to defend in the present position? if so, how will forces on the ground be organized, and with what troops? Special attention to locations and activities of reserves and vulnerability to nuclear attack.

(2) Will enemy attack prior to 1105OOZ September? If so, when, where, and in what strength? Special attention to the axis Hill 536--Hill 524--CR9841.

(3) Will enemy use CB agents? If so, what agents, when, how, and where?

(Classification)

Figure A-7. Sample of a division intelligence annex.

(CLASSIFICATION)

'. INTELLIGENCE ACQUISITION TASKS.

a. Orders to Attached and Subordinate Units.

(1) Ist Bale.

(2) 2d Bale.

(a) Report as obtained.

1 Status of construction of defensive positions and minef ields on and to the east of the Flood River.

2 Location and size of ammunition storage sites and l ocat ion. size, and content of engineer equipment parks.

3 Clearing of lanes through obstacles within enemy position n division zone.

4 Number, size, and composition of enemy patrols, and time they were observed.

5 Activity and size of units blocking our patrolling in forward areas.

6 The interception of enemy patrols equipped for CB activity.

7 The presence of enemy troops carrying protective masks or wearing protective clothing.

(b) Report as obtained. Negative reports by 1104OOZ September.

1 Activity in medium tank regiment (-) and tank battalion assembly area in vicinity of Burg.

2 Location and activity of mechanized regiment in vicinity of Burg.

(3) 3d Bale.

(a) Report as obtained--

(Classification)

Figure A-7. Sample of a division intelligence annex (continued)

(Classification)

1 Activity of mechanized battalion north and east of CR9847.

2 Activity of mechanized battalion on Hill 503.

3 Status of construction of defensive positions and ninefields on and to the east of Flood River.

4 Location and size of ammunition storage sites and location, size, and content of engineer equipment parks.

5 Clearing of lanes through obstacles within enemy position in division zone.

6 Number, size, and composition of enemy patrols and ime they were observed or contacted.

7 Activity and size of units blocking our patrolling n forward areas.

8 The interception of enemy patrols equipped for CB activity.

9 The presence of enemy troops carrying protective masks or wearing protective clothing.

(b) Report as obtained--Negative reports by 1104OOZ September.

1 Activity in medium tank regiment (-) and tank battalion assembly area in vicinity of Burg.

2 Location and activity of mechanized regiment in vicinity of Burg.

(4) 1/21 Cav report as obtained--

(a) Activity of mechanized battalion on Hill 503.

(b) Status of construction of defensive positions and minefield on and to the east of the Flood River.

(c) Location and size of ammunition storage sites and location, size, and content of engineer equipment parks.

(Classification)

Figure A-7. Sample of a division intelligence annex (continued).

(Classification)

(d) Clearing of lanes through obstacles within enemy position in division zone.

(e) Number, size, and composition of enemy patrols, and time they were observed.

(f) Activity and size of units blocking our patrolling in forward areas.

(g) The interception of enemy patrols equipped for CB activity.

(h) The presence of enemy troops carrying protective masks or wearing protective clothing.

(5) Div Arty.

(a) Report as obtained--

1 Status of construction of defensive positions and minefield on and to the east of Flood River.

2 Clearing of lanes through obstacles within enemy position in division zone.

3 Number, size, and composition of enemy patrols, and time they were observed or contacted.

4 Activity and size of units blocking our patrolling in forward areas.

5 The interception of enemy patrols equipped for CB activity.

(b) Report as obtained--Negative reports by 110400Z September. Locations of artillery positions, including number of weapons, caliber, and state of preparation of position.

(6) 20 Avn.

(a) Report as obtained--

1 Activity of mechanized battalion north and east of CR9847 .

Classification

Figure A-7. Sample of a division Intelligence annex (continued).

(Classification)

2 Activity of mechanized battalion on Hill 503.

3 Location, size, and type of unit in vicinity of Hill 536 (north of Burg) .

4 Status of construction of defensive positions and ninefields on and to the east of Flood River.

5 Location and size of ammunition sites, location, size, and content of engineer equipment parks.

6 Preparation of emplacements suitable for, and presence of equipment appropriate to, atomic demolition munitions (ADM).

7 The interception of enemy patrols equipped for CB activity.

(b) Report as obtained--Negative reports by 1104OOZ September.

1 Movement on the following roads:

a North on Highway 25.

b West on Highway 2.

c West on Highway 4.

2 Activity in medium tank regiment (-) and tank battalion assembly area in vicinity of Burg.

3 Location and activity of mechanized regiment in vicinity of Burg.

4 Location of artillery positions, including number of weapons, ca iber, and state of preparation of positions.

(7) 20 Engr report as obtained--

(a) Status of construction of defensive positions and minefi elds on and to the east of Flood River.

(b) The interception of enemy patrols equipped for CB activ ty .

(Classification)

Figure A-7. Sample of a division intelligence annex (continued).

(Classification)

b. Requests to Higher, Adjacent, and Cooperating Units.

(1) Ist Corps is requested to provide:

(a) As obtained--

1 Location, size, and type of unit in vicinity of Hill 536 (north of Burg).

2 Number, types, direction of movement, and time of movement of air or surface vehicular traffic within the division zone, with special attention to Highway 2.

3 Troop concentrations, including types of vehicles, east of Highway 25 within the divisional area of interest.

4 Evidence of field fortifications and troop concentrations along the following lines:

a Hill 503--CR9847.

b Hill 518--Hill 536--Hill 499.

5 Location and size of ammunition storage sites and locations, size, and content of engineer equipment parks.

6 Instances of heavily guarded vehicular movement. Special attention to Highway 2 from Zilch to Burg.

7 Areas under unusual security restrictions in the divisional area of interest.

8 Presence of special security troop units in any area east of Highway 25.

9 Any location in the divisional area of interest from which civilians have been evacuated.

10 Launcher sites for guided missiles or rockets within divisional area of interest.

11 Preparation of emplacements suitable for, and presence of equipment appropriate to, ADM.

(Classification)

Figure A-7. Sample of a division intelligence annex (continued).

(Classification)

12 The interception of enemy patrols equipped for CB activity.

13 All CB supply movement and dumping in zone.

14 The presence of enemy troops carrying protective masks or wearing protective clothing.

(b) As obtained--Negative reports by 1104OOZ September.

1 Movement on the following roads:

a North on Highway 25.

b West on Highway 2.

c West on Highway 4.

2 Activity in medium tank regiment (-) and tank battalion assembly area in vicinity of Burg.

3 Location and activity of mechanized regiment in vicinity of Burg.

4, Location and activity of mechanized regiment southwest of CR9944.

5 Locations of artillery positions, including number of weapons, caliber and state of preparation of positions.

6 Command posts, supply points, and medical facilities east of Highway 25.

(2) 18 Inf Div is requested to provide--

(a) As obtained--

1 Troop concentrations, including types of vehicles, east of Highway 25 within the divisional area of interest.

2 Instances of heavily guarded vehicular movement; special attention to Highway 2 from Zilch to Burg.

(Classification)

Figure A-7. Sample of a division intelligence annex (continued).

(Classification)

3 Areas under unusual security restrictions in the divisional area of interest.

4 Presence of special security troop units in any area east of Highway 25.

5 Any location in the divisional area of interest from which civilians have been evacuated.

6 Launcher sites for guided missiles or rockets within divisional area of interest.

7 Locations of heavy artillery positions, including number of weapons, caliber, and state of preparation of positions.

8 Preparation of emplacements suitable for, and presence of equipment appropriate to, atomic demolition munitions (ADM).

9 The interception of enemy patrols equipped for chemical biological (CB) activity.

10 All CB supply movement and dumping in zone.

11 The presence of enemy troops carrying protective masks or wearing protective clothing.

(b) As obtained--Negative reports by 1104OOZ September.

1 Movement on the following roads:

a North on Highway 25.

b West on Highway 2.

c West on Highway 4.

2 Location and activity of mechanized regiment in vicinity of Burg.

(3) 52 Mech Inf Div is requested to provide as obtained--

(a) Troop concentrations, including types of vehicles, east of Highway 25 within the divisional area of interest.

(Classification)

Figure A-7. Sample of a division intelligence annex (continued).

(Classification)

(b) Instances of heavily guarded vehicular movement, special attention to Highway 2 from Zilch to Burg.

(c) Areas under unusual security restrictions in the divisional area of interest.

(d) Presence of special security troop units in any area east of Highway 25.

(e) Any location in the divisional area of interest from which civilians have been evacuated.

(f) Launcher sites for guided missiles or rockets within divisional area of interest.

(g) Locations of heavy artillery positions, including number of weapons, caliber, and state of preparation of positions.

(h) Preparation of emplacements suitable for, and presence of equipment appropriate to, ADM.

(i) The interception of enemy patrols equipped for CB activity.

(j) All CB supply movement and dumping in zone.

(k) The presence of enemy troops carrying protective masks or wearing protective clothing.

(4) Supporting MI units provide information obtainable from SIGINT and ESM and will respond to specific tasking as described in separate instructions.

4. MEASURES FOR HANDLING PERSONNEL, DOCUMENTS, AND MATERIEL (see division SOP).

5. DOCUMENTS AND EQUIPMENT REQUIRED.

a. Maps. SOP distribution of map, Buttano, 1:50,000, Zelle-Pagt.

b. Photographic. Following aerial photographs will be furnished:

(Classification)

Figure A-7. Sample of a division intelligence annex (continued).

(Classification)

(1) Basic cover of division zone (1:10,000 approximate), six copies of each brigade and division artillery; one copy each tank battalion, mechanized infantry battalion, 1/21 Cav, division engineer, aviation battalion or group, and division signal officer.

(2) Annotated air photographs distributed automatically, as available.

6. COUNTERINTELLIGENCE.

a. Appendix 2, Cl.

b. All units coordinate use of Army aircraft through division tactical operations center (DTOC) to minimize number of aircraft in air over division zone prior to attack.

7. REPORTS AND DISTRIBUTION. Effective 1108OOZ September units will submit INTSUM at 0800, 1200, 1600, 2000, 2400, and 0400 hours daily in lieu of times prescribed in division SOP.

8. MISCELLANEOUS INSTRUCTIONS (as required),

None.

Acknowledge.

POWERS
MG

Append xes: 1--Situation Overlay
2--c

Distribution: Same as OPORD

OFFICIAL:

/s/AUSTIN

AUSTIN

G2

NOTE: This format may also be used in Joint Service Operations.

(Classification)

Figure A-7. Sample of a division intelligence annex (continued).

SITUATION REPORT

Preparation and submission of the SITREP is a staff responsibility of the S3; however, the S2 prepares paragraph 1, Enemy, of the SITREP and furnishes it to the S3 in usable form. Figure A-8 shows the prescribed format for preparing a SITREP.

ENEMY .

Committed forces (overlay).

Forces committed against TF 2-80 are--

(1) Four mechanized platoons.
(2) Two medium tank platoons.
(3) Normal regimental artillery.
(4) Six 160mm mortars.
(5) Ten 122mm howitzers.
(6) Four 100mm artillery guns self-propelled (SP).
(7) Two 122mm multiple rocket launchers.
(8) One 152mm gun SP.
(9) Air and nuclear weapons.

Reinforcements (overlay). Reinforcements currently capable of being" employed in sector now total: U/l Medium tk plt vic BD4156, MRC of 281st MRR vic BD4867, MRC of 282d MRR vic BD4873, MRC of 281st MRR vic AB4673, MRB (-) of 281st MRR vic AB4650, MRB of 282d MRR vic CD5060, U/l tk co vic DE5265 .

Enemy Activity During Period IOO6OOZ-1018OOZ.

(1) Occupation of previously unoccupied positions vic BG3531, NT3633, MT3734, DT4239 .
(2) Movement of combat units fwd vic MN4036.
(3) Dispersal of tanks to fwd units vic CG3136.
(4) Movement of assault boats into vic GM3338.
(5) Two 100mm AT guns (SP) vic MT3737, two 120mm AT guns (SP) vic ER3833 .
(6) Six additional 122mm how vic DT3731.
(7) Increased enemy counterbattery fire in bde sector.
(8) Clearing lanes through minefield BC2937.
(9) Mech regimental aid station vic CD3339.
(10) Increased enemy air activity vic FN2836, RB2437.
(11) Suspected jamming of VHF communications (intel net) at 100745Z and 013252.

Concl usions. Enemy's most probable courses of action--

(1) Continue defense now.
(2) Attack along our front within 8 hours.

Figure A-8. Sample situation report.

INTELLIGENCE REPORT

The INTREP is a standardized report which, based on its importance, is disseminated without regard to a specific schedule. It is prepared at all echelons when facts influencing the enemy capabilities have been observed, or when a change in enemy capabilities has taken place. It is passed to higher, lower, and adjacent units at the discretion of the commander producing the report. It is sent as quickly as possible following receipt of the information. Whenever time permits, the INTREP includes the originating office's interpretation of the information or intelligence being reported. The first word of the report is INTREP. Otherwise, there is no prescribed format for this report. It is not used in lieu of the critical INTREP. Figure A-9 shows a message format for INTREPs that has been developed for joint operations.

C110: Message Identification Number.

INTREP: The first word of the report must be "INTREP."

HEADING: Addressee information and meg ctr data.

TEXT: Intelligence or information to be reported. Should answer Who, What, Where, When and How Questions.

CONCLUSIONS: Whenever possible the INTREP should include the originating office's interpretation of the information intelligence being reported.

Figure A-9. Sample INTREP message format.

Figure A-10 shows the Joint Chiefs of Staff (JCS) INTREP format.

MESSAGE HEADING
ORIGINATING AGENCY
ACTION ADDRESSEES
INFORMATION ADDRESSEES
SECURITY CLASSIFICATION AND CODE WORD OR NICKNAME
INTREP (number) AS OF DATE-TIME GROUP (GMT)/MO/YR
BODY Installation, Event, and Sighting Format
Reference to previous message, if any.
Source reliability evaluation.
Concise narrative description.
REMARKS: Any other information not covered in the body of the report.

Figure A-IO. Sample JCS INTREP message format.

INTELLIGENCE SUMMRY

The INTSUM provides a summary of the intelligence situation covering a specific period of time dictated by the commander. Figures A-II and A-12 show INTSUM formats. There is no specified format for the INTSUM, except for joint service operations (see the format in Figure A-12).

Format of an INTSUM NOTE: Omit items not applicable unless otherwise indicated.	IMMEDIATE TO CG 2D CORPS INTSUM NUMBER 144 ENDING 040600Z
1. Issuing unit (always included).	PARA 3 ALFA ENEMY CONTINUED DEFENSE IN ZONE EXCEPT FOR LOCAL ATTACK AT
2. Time and date of issue (always included).	0415 VICINITY RS376759 WITH ESTIMATED 90 MEN CMM 3 MEDIUM TANKS
3. Summary of enemy activity for period.	CMM AND LIGHT ARTILLERY SUPPORT PD
a. Ground activity.	ATTACK REPULSED PD PARA 3 DELTA
b. Trace of forward elements.	ATTACK PRECEDED AT 0410 BY VERY HIGH
c. Potential targets for clear weapons.	AIR BURST NUCLEAR WEAPON CMM GROUND ZERO RS374761 CMM DELIVERY MEANS
d. Nuclear activity.	UNDETERMINED CMM YIELD ESTIMATED AT
e. CB activity.	0 PD 5 KT PD PARA 3 FOXTROT ATTACK
f. Air activity.	SUPPORTED BY 2 JET ATTACK AIRPLANES
g. Other (new tactics, counterintelligence).	BOMBING AND STRAFING VICINITY RS396756 FOR 5 MINUTES STARTING AT
4. Enemy personnel and equipment losses.	0425 PD PARA 4 ALFA CONFIRMED 20 KIA
a. Personnel Killed in Action (KIA).	CMM ESTIMATED 5 KIA PD PARA 4 BRAVO 10 INCLUDING 2 WIA PD PARA 4 CHARLIE
b. EPW.	2 MEDIUM TANKS DESTROYED CMM 1
c. Equipment destroyed or captured.	DAMAGED CMM 1 JET
5. New obstacles and barriers.	ATTACK AIRCRAFT SHOT DOWN PD PARA 6
6. Administrative activities.	PRISONER STATES AMMUNITION SUPPLY IN
7. New identifications.	FORWARD UNITS RUNNING LOW PAREN
a. Units.	CHARLIE DASH 3 PAREN PD PARA 7 ALFA
b. Personalities.	PATROL REPORTS BATTERY 152MM GUN
8. Enemy movements.	HOWITZERS AT RS303292 PD PRISONERS
9. Estimates number and types of vehicles.	CONFIRM LOCATION 2D BATTALION CMM 17F MRR VICINITY RS375758 PAREN
10. Weather and terrain conditions.	BRAVO DASH 1 PAREN PARA 8 AIRBORNE RADAR RECONNAISSANCE DETECTED 10
11. Brief discussion of capabilities and vulnerabilities (always included).	TRUCKS MOVING SOUTH ON ROAD AT RS330280 AT 0345 PD PARA 9 PROBABLY ROUTINE SUPPLY VEHICLES PD PARA 10 SNOW STARTED AT 040545Z AND CONTINUING PD GROUND FROZEN HARD AND SUPPORTS ALL TYPES OF VEHICLES PD

NOTE: In joint service operations, use the format in Figure A-12.

Figure A-11. Format and sample of an intelligence summary.

12. Conclusions (always included).	PARA 11 LOCAL ATTACK REPORTED PROBABLY WAS TO SEIZE HILL 405 PD ENEMY IS CAPABLE OF CONTINUING DEFENSE IN PRESENT POSITION CMM
Examples of a Division INTSUM (full distribution not indicated) FM CG 520 Inf Div (Mech)	MAKING LOCAL ATTACKS TO IMPROVE HIS DEFENSIVE POSITION CMM DELAYING TO STRONGER POSITION ALONG LAURIEX RIVER PD PARA 12 CONTINUED DEFENSE IN PRESENT POSITION MOST PROBABLE.

NOTE: In joint service operations, use the format in Figure A-12.

Figure A-ll. Format and sample of an intelligence summary (continued).

HEAD I NG

PRECEDENCE

ORIGINATING AGENCY

ACTION ADDRESSEES

INFORMATION ADDRESSEES

SECURITY CLASSIFICATION, CODE WORD, OR NICKNAME

INTSUM (Number) FOR PERIOD ENDING DATE-TIME GROUP-MONTH-YEAR

BODY

1. SUMMARY OF ENEMY ACTIVITY FOR THE PERIOD. Is a summary of those that occurred during the period of the report. It contains but not be limited to the following:

a. GROUND ACTIVITY. Summarize major movements and activities of enemy ground forces. Indicate estimated strength, composition, disposition, and any other items of significance.

b. TRACE OF FORWARD ELEMENTS. The most forward location or main location of the enemy force will be shown as a pinpoint position, area boundary, or a series of connected points, as applicable. The following methods for reporting locations is used and stated in the intelligence annex.

Figure A-12. Intelligence summary for joint service operations.

(1) Operations Involving Ground Forces. For unified or joint operations in which ground forces are directly participating, not specifically provided for in the subparagraph below, the UTM system prescribed for the area concerned is used to the maximum extent practicable in communications between ground forces and other forces jointly engaged. When the use of the UTM system is impractical, latitude and longitude is used.

(2) Operations Not Involving Ground Forces, The World Geographic Reference System (GEOREF) is used in joint operations which do not directly involve ground forces.

(3) For Close Air Support of Ground Forces. When air forces (including naval aviation) are acting in close air support of ground forces, the UTM system prescribed for use by ground forces in the area concerned is used.

(4) For Joint Amphibious Operations. The UTM system prescribed for use by landing forces within the amphibious objective area is used for support of landing force operations by all supporting forces.

(5) For Joint Air Defense Operations. GEOREF is used in joint air defense operations. When there is a possibility of confusing which system to use in reporting positions, the reference system should be indicated in the report. GEOREF is not used by air forces (including naval aviation) when reporting positions to ground forces, except in air defense operations. GEOREF is used by ground forces when reporting positions to air forces in air defense operations.

(6) in joint operations not using procedures specified in the above paragraphs, latitude and longitude is used.

c. POTENTIAL TARGETS FOR NUCLEAR WEAPONS. List all potential nuclear targets, such as concentrations of troops or equipment observed during period. Include location, date, and time (Zulu) of observation.

d. NUCLEAR ACTIVITY. Enemy nuclear capability observed during the period is reported. Include any changes to previously reported capabilities. Indicate location, date, and time (Zulu) of observation of artillery, missile, or air nuclear capability.

e. NUCLEAR, BIOLOGICAL, AND CHEMICAL ACTIVITY. Indicate NBC weapons (agents) employed or capability by type, location, date, and time (Zulu) of occurrence.

f. AIR ACTIVITY. All enemy air activity that has occurred during the period (CAS, air interdiction, AD, and reconnaissance affecting the

Figure A-12. Intelligence summary for joint service operations (continued).

operation is summarized, including location, date and time (Zulu), and type of aircraft involved.

g. NAVAL ACTIVITY. Summarize all enemy naval activity that has occurred during the period. include location, date and time (Zulu), and types of ships and craft.

h. OTHER. New tactics observed are summarized. Cl measures of significance, including active and passive measures, are listed. Any item not properly reported in any other paragraph also may be included.

2. ENEMY PERSONNEL AND EQUIPMENT LOSSES.

a. PERSONNEL. List in separate categories confirmed KI A (body count) , estimated KIA, estimated wounded in act on (WIA), and captured.

b. EQUIPMENT AND MATERIEL. List by number and type the enemy equipment and materiel losses during the period. Include damaged enemy equipment separately.

3. NEW OBSTACLES AND BARRIERS. List those identified during the period by type and location.

4. ADMINISTRATIVE ACTIVITIES. Summarize enemy activities pertaining to personnel replacements, supply buildup, or other unusual logistic activity but not information or intelligence reported elsewhere in the INTSUM.

5. NEW IDENTIFICATIONS.

a. UNITS. List new units identified during the period. Include location, date and time (Zulu), and unit making the identification.

b. PERSONALITIES. List significant individuals identified during the period by name, rank or title, and organization.

6. ENEMY MOVEMENTS. Summarize significant enemy movements by type, activity, location, and unit designation, if known.

7. ESTIMATED NUMBER AND TYPES OF VEHICLES, SHIPS, AIRCRAFT. Summarize by type the estimated number of vehicles, ships, and aircraft available to the enemy.

8. WEATHER AND TERRAIN CONDITIONS. A summary of the weather and terrain conditions during the period that would have an effect on subsequent operations.

Figure A-12. Intelligence summary for joint service operations (continued).

9. BRIEF DESCRIPTION OF GAPABILITIES AND VULNERABILITIES. (Always included.) State courses of action which the enemy most probably will adopt.

NOTE: Paragraphs and subparagraphs for which no information has been obtained are omitted in the preparation of the INTSUM. Each topic reported upon retains the numerical (and letter) designation outlined above.

Figure A-12. Intelligence summary for joint service operations (continued).

PERIODIC INTELLIGENCE REPORT

The PERINTREP is a summary of the intelligence situation covering a longer period than the INTSUM. It is a means of disseminating detailed information and intelligence. Other intelligence documents like technical intelligence summaries, EPW interrogation reports, translations of captured documents, and weather and climate summaries are disseminated as appendixes to the PERINTREP. The PERINTREP is concise--but complete--and makes maximum use of sketches, overlays, marked maps, and annexes.

Although not normally prepared by intelligence officers at division and lower levels, PERINTREPs provide detailed information and intelligence. Therefore, intelligence officers at these levels should be familiar with the format and content of PERINTREPs.

The PERINTREP is normally published every 24 hours. The beginning and end of the period is selected to permit dissemination of the PERINTREP in time for its use in daily planning. It is disseminated by the most suitable means consistent with its volume and urgency. Figure A-13 shows the PERINTREP format.

The Supplementary Intelligence Report (SUPINTREP) is a comprehensive analysis of one or more specific subjects. This report is formatted like a PERINTREP and usually contains selected intelligence data collected over an extended period of time. It includes additional details on items contained in other reports. The report is disseminated based on the intelligence contained in the report and the desires of the commander. It is normally produced as the result of a request or in support of a particular operation.

(Classification)

copy No _____
Unit
Location
Date-time group
Message reference number

PERINTREP NO _____
Period Covered: (date and time to date and time).
References: Maps or charts.
Disposal instructions: (if any).

1. GENERAL ENEMY SITUATION. This paragraph contains a brief summary of enemy operations during the period. Amplifying details are furnished in the paragraphs that follow and in appropriate annexes, or both. This paragraph provides brief highlights of the anemy situation and the significance of the enemy's major activities, to include marked changes in morale, strengths, dispositions, tactics, combat effectiveness, and equipment. Data that is langthy or can conveniently be shown graphically are presented in annexes.

2. ENEMY ACTIVITIES. This paragraph, in conjunction with those following, providas the details of the situation summarized in paragraph 1. Detailed intelligence provided in this paragraph covers all operational activities. Information may be presented graphically by overlays, printed maps, sketch maps, and annexes. Subparagraphs are omitted when appropriate intelligence is not available or is adequately covered by othar portions of this report.

a. Ground. (Primarily includes activities of combat arms, raserves, and reinforcements; also includes enemy defensas, minefield, fortifications, barriers, obstacles, and other defensive works.)

b. Air. (Includes Air Force activities, such as bombing, close air support, tactical aerial reconnaissance, air surveillance, and air-supported operations.)

c. Airborne.

d. Irregular.

e. NBC operations.

f. EW.

(Classification)

Figure A-13. Sample format for a periodic intelligence report.

g. Other. (Normally includes other than combat arms; includes appropriate comments not covered in other subparagraphs on reserves, reinforcements, new tactics, weapons and equipment, administrative installations, combat service support, and technical intelligence.)

3. ORDER OF BATTLE, Frequently, this paragraph will consist only of references to the enemy SITMAP (or overlay) and to the OB annex, which is developed using the format shown below. When desired by the commander, particularly significant 06 changes may be summarized in addition to being discussed in detail in the 06 annex.

a. Composition and Disposition.

b. Strength. (Personnel and major weapons and items of equipment.)

(1) Losses.

(2) Current strength.

c. Tactics,

d. Training.

e. Css.

f. Combat Effectiveness.

g. Miscellaneous Data.

4. COUNTERINTELLIGENCE. This paragraph, or parts thereof, should be issued as an annex if a limited distribution is required.

a. General. (A short summary of the CI situation during the period.)

b. Espionage.

c. Sabotage.

d. Subversion.

e. Communication and Noncommunication Security.

f. Miscellaneous.

5. WEATHER. This paragraph gives a summary of the effect of weather on operations during the period.

(Classification)

Figure A-13. Sample format for a period intelligence report (continued).

(Classification)

6. TERRAIN. Use an annex, special maps, and overlays, when possible. Include impact on future operations, if appropriate.

7. ANALYSIS AND DISCUSSION. This paragraph lists and discusses briefly enemy capabilities and vulnerabilities. The conclusions present the commander's assessment of the most probable courses of action available to the enemy, probability of their adoption, and vulnerabilities that are exploitable by own, higher, or lower levels of command.

a. Enemy Capabilities.

b. Enemy Vulnerabilities.

c. Conclusions.

Authentication:

Annexes: (Any intelligence document may be distributed as an annex to a PERINTREP. Although annexes are a means of distributing detailed intelligence and information, care is exercised to avoid unnecessary bulk and duplication.)

DISTRIBUTION:

(Classification)

Figure A-13. Sample format for a periodic intelligence report (continued).

PERIODIC INTELLIGENCE SUMMARY

The periodic intelligence summary (PERINTSUM) is a detailed hard copy summary of the intelligence situation covering a period of time specified by the force commander (normally 24 hours or more). The PERINTSUM is a means of disseminating concise and complete detailed information and intelligence and makes maximum use of sketches, overlays, annotated maps, and annexes. Normally, this report is prepared at corps level and higher. It is disseminated two echelons higher, two echelons lower, and to adjacent units; however, subordinate units also may be tasked to prepare a PERINTSUM. Figure A-14 shows a JCS message format for the PERINTSUM, structured to facilitate updating the intelligence estimate.

HEAD I NG

PRECEDENCE

ORIGINATING AGENCY

ACTION ADDRESSEES

INFORMATION ADDRESSEES

SECURI TY CLASSIFICATION, CODE WORD, OR NICKNAME

PERINT SUM (Number) FOR PERIOD ENDING DATE-TIME GROUP-MONTH-YEAR

BODY

1. AREA OF OPERATIONS. State conditions which exist and indicate the effect of these conditions on enemy capabilities and the assigned mission. The characteristics of the area are based on the facts and conclusions of an analysis of the AO, as follows:

a. TOPOGRAPHY. Include information available on observation and fields of fire, concealment and cover, obstacles, key terrain features, AAs, nuclear fires, biological and chemical agents, and so forth. Graphic representation may be included, if necessary.

b. HYDROGRAPHY. Include general relief of beaches and beach approaches, surf conditions, tides and currents, navigational aids, identifying features, channels, water depths, rocks and shoals, obstacles, anchorages, beach trafficability, coastline, contiguous islands, and compartmentation, as each affects operations.

c. CLIMATE AND WEATHER. Discuss weather during the period which will affect operations.

d. TRANSPORTATION . Include status of beaches, beach airways, pipelines, and inland waterways. The following should be included: capacities, surface conditions, bridges, amount and condition of rolling stock, motor and air transport, barges, freighters, and other inland waterways craft. Vulnerabilities are reported in as much detail as possible.

e. ELECTRONICS AND TELECOMMUNICATIONS, Report existing electronic telecommunications systems and equipment, both military and civil.

f. POLITICS, The extent of civil control of the region, the amenability of the civilian population to political control, the political organizations, and the key political figures.

Figure A-14. Sample periodic intelligence summary.

g. ECONOMICS. Include only that specific economic information which may be necessary for conduct of the current operation.

h. SOCIOLOGY. The sociological factors dealing with customs, characterist its, religions, the minority or dissident groups, and the allegiance of the population.

i. SCIENCE AND TECHNOLOGY. Scientific and technical information on enemy weapons, equipment, and techniques as wel l as the employment of new capabilities during the course of the operations.

2. ENEMY OPERATIONS DURING THE PERIOD.

a. GROUND FORCES.

(1) Strength and Dispositions. (By overlay, if possible.) Summary of enemy units and locations.

(2) Committed Forces. Report those enemy ground units, including guerrillas, together with their supporting ground fire units which are within the AO.

(3) Reinforcements. Include the designation and location of reinforcements which may or may not be employed.

(4) Activity. (Discuss by arm of service.) Include a description of all significant enemy movements which may affect the friendly mission.

(5) Other Order of Battle Factors. Reference may be made to overlays, enemy SITMAPS, or previously published documents.

(6) New Tactics, Weapons, and Equipment. List new tactics and equipment which may affect the mission and enemy capabilities.

(7) Nuclear-Capable Artillery and Launchers. Describe the operational capability to launch missiles by numbers and types of missiles; guidance systems; ranges; types of warheads; type of launching sites (if fixed, whether hardened or not); and for mobile launchers state mobility, rate of fire, and readiness.

(8) Nuclear, Biological, and Nuclear Activity. These weapons should be reported by type, yield, number, method of delivery or application, and enemy doctrine' concerning their use.

b. AIR FORCES.

(1) Strength and Dispositions. Summary of enemy units and locations.

(2) Order of Battle. Summary of opposing forces and other enemy forces that can affect accomplishment of mission.

Figure A-14. Sample periodic intelligence summary (continued).

(3) New Tactics, Weapons, and Equipment. List new tactics, weapons, and equipment which may affect the mission and enemy capabilities.

c. NAVAL FORCES (Including amphibious forces).

(1) Strength and Dispositions. Summary of enemy units and locations.

(2) Order of Battle. Summary of opposing forces and other enemy forces that can affect accomplishment of mission.

(3) New Tactics, Weapons, and Equipment. List new tactics, weapons, and equipment which may affect the mission and enemy capabilities.

d. MISSILE FORCES (Excluding SAMs).

(1) Strength and Dispositions. Summary of enemy units and locations.

(2) Order of Battle. Summary of opposing forces and other enemy forces that can affect accomplishment of mission.

(3) New Tactics, Weapons, and Equipment. List new tactics, weapons, and equipment which may affect the mission and enemy capabilities.

e. ANTIAIRCRAFT DEFENSES (including SAM).

(1) Strength and Dispositions. Summary of enemy units and locations.

(2) Order of Battle. Summary of opposing forces and other enemy forces that can affect accomplishment of mission.

(3) New Tactics, Weapons, and Equipment. List new tactics, weapons, and equipment which may affect the mission and enemy capabilities.

f. AIRBORNE UNITS.

(1) Strength and Dispositions. Summary of enemy units and locations.

(2) Order of Battle. Summary of opposing forces and other enemy forces that can affect accomplishment of mission.

Figure A-14. Sample periodic intelligence summary (continued).

(3) New Tactics Weapons, and Equipment. List new tactics, weapons, and equipment which may affect the mission and enemy capabilities.

3.. ENEMY MILITARY SITUATION.

a. IDENTIFICATION OF COMMITTED GROUND FORCES.

(1) Movement and Locations. Report disposition, location, and echelon of control of enemy ground forces.

(2) Reinforcements. Report disposition, location, and echelon of control of enemy ground force reinforcements.

(3) Logistics. Report the following elements of the enemy's logistic system: transportation, storage distribution, levels of supply, critical shortages.

(4) Equipment. Report weapons systems and equipment used by committed enemy ground forces.

(5) Personalities. Report significant individuals operating for the enemy ground forces.

(6) Morale. Report any significant breakdown or buildup of enemy norale.

(7) Personnel and Materiel Losses.

(a) KIA.

1 Body count.

2 Estimates.

(b) WIA (estimated).

(c) Captured.

(d) Materiel losses.

(8) Analysis of Capabilities. Analyze each capability of enemy-committed ground forces, considering all applicable factors in item 3a above.

Figure A-14. Sample periodic intelligence summary (continued).

b. IDENTIFICATION OF AIR FORCES.

(1) Operational Capability (aircraft and airfields). Report observed aircraft operational capability, including numbers of aircraft, fuel status, weapons, and status of the airfield.

(2) Movements and Locations. Report movements and locations of all observed aircraft and airfields,

(3) Materiel and Personnel Losses,

(a) Aircraft.

1 Confirmed destroyed in the air.

2 Confirmed destroyed on the ground,

3 Confirmed damaged in the air.

4 Confirmed damaged on the ground.

5 Probable destroyed.

6 Probable damaged.

(b) Ground equipment.

1 Destroyed.

2 Damaged.

(c) Personnel.

1 KIA.

a Confirmed.

b Estimated.

2 WIA (estimated).

3 Captured.

(4) Morale. Report any significant breakdown or buildup of enemy morale.

(5) Electronic Warfare Capability. Report enemy ECM, ECCM, and ESM capabilities and activities.

Figure A-14. Sample periodic intelligence summary (continued).

(6) Nuclear Capability. Report nuclear weapons observed, including type, yield, numbers, method of del ivery, and enemy doctrine concerning their use.

(7) Analysis of Capabilities. Analyze each capability of enemy air forces, considering all applicable factors in item 3b above.

c. IDENTIFICATION OF NAVAL FORCES.

(1) Operational Capability. Report observed naval forces' operational capability, including numbers of ships, operational weapons, and problems which could affect their successful employment.

(2) Movements and Locations. Report movement and location of all observed naval forces.

(3) Ships, Materiel, and Personnel Losses.

(a) Ships (identification by name, class, type).

1 Confirmed sunk.

2 Probable sunk.

3 Damaged.

(b) Shore-based equipment and facilities.

1 Destroyed.

2 Damaged.

(c) Personnel .

1 KIA.

a Confirmed.

b Estimated.

2 WIA (estimated).

3 Captured.

(4) Morale. Report any significant breakdown or buildup of enemy morale.

(5) Electronic Warfare Capability. Report enemy ECM, ECCM, and ESM capabilities and activities.

Figure A-14. Sample periodic intelligence summary (continued).

(6) Analysis of Capabilities. Analyze each capability of enemy naval forces, considering all applicable factors in item 3c above,

4. ENEMY UNCONVENTIONAL AND PSYCHOLOGICAL WARFARE.

a. IDENTIFICATION OF GUERRILLA FORCES. Identify guerrilla forces being used in friendly areas or areas newly seized from the enemy.

b. PSYCHOLOGICAL WARFARE. Discuss psychological warfare, including enemy methods and facilities observed for the conduct of propaganda, the susceptibility of the population of the target area, and the major or main focus of the enemy's psychological warfare efforts.

5. COUNTERINTELLIGENCE.

a. SABOTAGE. Report enemy sabotage effects observed, including information concerning his methods, targets, sensitive targets in the AO, and successes or fai lures.

b. ESPIONAGE. Report enemy efforts to collect information by types of espionage: designation (trained agents) or saturation (mass use of citizenry) and include methods of pressure, coercion, and enforcing the saturation-type espionage.

6. CONCLUSIONS. State conclusions derived from item 3 above, and include, when possible, a concise statement of the effects of each enemy capability on the accomplishment of the assigned mission. Cite enemy vulnerabilities, where possible.

Figure A-14. Sample periodic intelligence summary (continued).

RECONNAISSANCE EXPLOITATION REPORT

The RECCEXREP disseminates results obtained from the first rapid interpretation of imagery and debriefing of the aircrew. The report addresses those targets requested in the original tasking with each target addressed separately. The RECCEXREP is submitted as rapidly as possible, but not later than 45 minutes after engine shutdown. If review of the imagery results in information contradictory to that in an earl ier RECCEXREP, the new information is to be reported promptly in another RECCEXREP. Table A-1 shows an annotated format for the RECCEXREP.

Table A-1. Sample reconnassance exploitation report annotated format.

Standard Message Heading	Standard Message Heading
RECCEXREP	RECCEXREP
Air Reconnaissance Mission Number:	2/R/501
A. Location identifier:	A. PB088195
B. Time on target; time of sighting.	B. 24161OZ
C. Results:	C. CAT 06 1. Type: Motor rifle and tank. 2. Status: Moving northwest on road from Rotterode to Asbach. 3. Activity: 24xT-62, 9xBMP. 4. Defenses: 2xZSU-23-4 moving with and defending target.
D. Other information	D. None.
1. TARWI:	1. TARWI 1234X
2. Imagery confirmed:	2. Yes
E. *Type sensor, exposures:	E. Good, large
F. *Percentage of coverage:	F. 100 percent.

* To be completed if significant or requested.

NOTE: Target category codes are found in STANAG 3596. Standard message headings are noted in AR 105-31. The RECCEXREP replaces the hot (high priority) photographic report (HOTPHOTOREP) and mission report (MISREP) (except that the MISREP is used for negative mission results) in USAREUR. It may soon be accepted for use by US forces worldwide.

INITIAL AND SUPPLEMENTAL PROGRAMMED INTERPRETATION REPORT

The initial programed interpretation report (IPIR) and the supplemental programmed interpretation report (SUPIR) are used to report intelligence obtained from imagery which has not been reported through previous reports. The format for both reports is the same and should be used to report data acquired from a systematic review of imagery or to report more detailed information than is provided in other reports. These reports are prepared in either manual or ADP formats.

The IPIR is no t completed on all missions and must be requested. It is disseminated w thin four hours of engine shut-down. The IPIR reports on programed miss on objectives or other vital intelligence information which is readily dentified in reasonable proximity to these objectives and which has not been reported in earlier reports.

The SUPIR reports on all significant targets covered by the mission and not included in other reports or when supplemental information is required. The SUPIR is completed at higher headquarters only if they decide it is necessary.

Table A-2 shows the format used for both the IPIR and the SUPIR. This format also is used for joint service operations.

Table A-2. Initiai and supplemental programmed interpretation reports.

Standard Message Heading IPIR (or SUPIR)	Standard Message Heading IPIR
Air Task or Mission Number:	2/R/501
PART I: Mission highlights:	PART I: One new SA-2 site observed
PART II: Significant results:	PART II:
A. Perishable items:	A. Target 1: CAT 06/PB088195/ 241610Z/LOOII-0113 1. Motorized rifle and tanks 2. Moving northwest on Road Rotterrode-Asbach. 3. 24xT-62, 9xn intelligence annex. 4. Two occupied air warning (AW) positions approx 200m west of site. 5. One FAN SONG E radar in center of site. 6. Six transporters; two van trucks, four cargo trucks.
B. Change and OB items: Target 3: CAT 01/PB4056 241644Z/POO27. 3. Update: AOB: 6 Flagons 21 Fishbed 4 Hook	B. Air order of battle (AOB)
C. Bonus items:	D. (Not used.)
D. Damage assessment:	E. (Not used.)
PART III: Other results:	PART III: (Not used.)
A. Additional items:	A. NTR (nothing to report.)
B. Identification only items:	B. NTR
PART IV: Mission collection results:	PART IV:
A. Collector's objectives satisfied:	A. NTR
B. Collector's objectives not satisfied:	B. CAT 4/PB1437/241653Z/ camera malfunction.

(When issued separately from an OPORD)

INTERROGATION AND TRANSLATION REPORTS

Interrogation reports summarize the results of interrogations of EPW, civil ian detainees, or refugees, and the translations of summaries of enemy documents. Information of immediate value is disseminated in spot reports.

The initial interrogation report serves as a written summary of the initial interrogation of each prisoner. Figure A-15 shows the format of this report. Emphasis is placed on completing as much of the tactical interrogation as possible at the lowest level and supplementing this with further interrogation at higher echelons. The primary purpose of this report is to preclude duplication of effort in subsequent interrogations.

The detailed interrogation report is used to record information obtained in the course of subsequent interrogations of selected interrogees. Figure A-16 shows its format. A more detailed interrogation and screening report format is available in FM 34-52.

During joint service operations, interrogation information of immediate tactical interest (obtained at the brigade or regimental level) is generally reported in the INTREP. Follow-on interrogation reports, the initial interrogation report, and the detailed interrogation report disseminate more complete and comprehensive information. It is essential that these follow-on reports reference the INTREP where the information first appeared to ensure that the information contained in these reports is not used to confirm the preliminary information contained in the INTREP.

Joint services use the document translation report to report information gained through the translation of documents which contain information of tactical value. Figures A-17 and A-18 show the format and sample of a translation report. Full or extract translations are accomplished as the intelligence officer directs. All translations are prepared in triplicate, unless otherwise directed, and each translation is conspicuously annotated with the word "Draft.'"

The original of the translation is appended to the document when it is forwarded to the next higher headquarters. Copies of the original document are provided to the intelligence officers at echelons which contain translation sections to support their journal entries. The document translation report format also is used for joint service operations. Figures A-19 and A-20 show sample screening reports. Figures A-21 and A-22 show sample tactical interrogation reports. These reports are used to record information on interrogees.

(Classification)

REPORT NO _____ C Y N O _ DATE-TIME(Zulu)
(Numbered sequentially)

SOURCE _____ INTG UNIT _____
(last name only) (attached to interrogator)

CATEGORY A B C D MAPS USED _____
(see detailed report) (1 ist sheet name, number, and scale of maps)

LANGUAGE USED _____

PART I INTELLIGENCE POTENTIAL OF ENEMY PRISONERS OF WAR

(rank) (last name, first name) (MI) (service or serial number)

DOB _____ BIRTHPLACE _____
(day, mo, yr) (city, county, or country)

NATIONALITY _____ RACE _____

LANGUAGES _____ UNIT _____
(list and include proficiency) (interrogees' parent unit listed completely to highest headquarters)

CIVILIAN CAREER _____
(summarize prisoner's premilitary career)

MILITARY CAREER _____
(summarize)

ASSESSMENT _____
(intelligence, experience, cooperation, and reliability of the interrogee, NOT the information)

SPECIALIST KNOWLEDGE _____
(knowledge of technical subjects or equipment)

DOCUMENTS _____
(carried at time of capture; include money or valuables)

EQUIPMENT _____
(of intelligence interest) (personal equipment or weapons)

PART II - INFORMATION OBTAINED _____
(sumrnarize)

(Classification)

Figure A-15. Initial interrogation report.

(CLASSIFICATION)

_____ INTG TEAM

UNIT _____
(place and coordinates)

DATE AND TIME _____
(Zulu)

Detailed Interrogation Report No _____
(number reports sequentially)

Maps _____
(list all maps used and indicate sheet name, number, and scale)

PART I

1. RANK _____ NAME _____ SER NO _____
(last name, first name, MI)

_____
(interrogees' parent unit listed completely; for example, 1st Pit, A company, 103 Recon Bn, 3d Rifle Div)

CIRCUMSTANCES OF CAPTURE _____
(summary of details of capture, including date and time, location or coordinates, and capturing unit)

ASSESSMENT _____
(intelligence, experience, reliability) (Concise statement of the interrogator's assessment of the prisoner--not of the information acquired)

CATEGORY: A B C D
(circle one to describe prisoner's intelligence potential, as indicated) :

A High-level prisoner whose broad and specific knowledge of the war effort makes interrogation necessary without delay by specially qualified interrogators at the highest level; that is general officers, scientists, political and intelligence officers, and so forth.

(CLASSIFICATION)

Figure A-16. Detailed interrgation report.

(CLASSIFICATION)

B Prisoner who has enough information about the enemy or any subject of value to intelligence, in addition to information of tactical value, to warrant a second interrogation.

c Prisoner with information of immediate tactical value who will not warrant further interrogation.

D Prisoner of no intelligence value.

DOCU MENTS _____
(list documents of intelligence value taken from the prisoner)

EQUI PMENT _____
(list equipment of intelligence value taken from the prisoner)

PART II

2. ORGAN!ZATI ON, STRENGTH, AND DISPOSITION.

a. Organ ization _____
(summarize the enemy organization as stated by the prisoner, including equipment authorized and on hand)

i). Strength _____
(personnel strength, officer and enlisted, authorized and assigned!

c. Disposition _____
(location of enemy units known to the prisoner)

3. MISSION _____
(statement of enemy missions, beginning with the lowest unit)

4. OTHER ENEMY FORCES _____
(information of enemy forces other than the prisoner's own immediate organization; include and annotate fact and rumor)

5. SUPPLY, LOSSES, REPLACEMENT.

a. supply _____
(information concerning status of SUPPI ies, known shortages and deficiencies)

(CLASSIFICATION)

Figure A-16. Detailed interrogation report (continued).

(CLASSIFICATION)

b. Losses _____
(statement of personnel and equipment losses known to prisoner)

c. Replacements _____
(number and date received, sufficiency, and so forth)

6. PERSONALITIES _____
(list by name, rank, organization, duties, and characteristics)

7. MISCELLANEOUS.

a. Morale _____

b. Tactics _____
(new or unusual tactics)

c. Obstacles _____
(location, coordinates, type)

d. Other Information _____
(other information of intelligence value not covered above)

8. REMARKS

NAME _____
(of Interrogator)

GRADE _____

TRANSLATOR _____
(if used)

_____

Figure A-16 Detailed interrogation report (continued).

(CLASSIFICATION)

DATE :
-0:

'ROM : REPORT NUMBER:

1. CONTROL DATA.

1. DOCUMENT NUMBER,

2. DOCUMENT DESCRIPTION: (type of document, originating headquarters, language, and number of pages),

3. DOCUMENTS ORIGINAL LANGUAGE.

4. DATE AND TIME RECEIVED.

5. DATE AND TIME OF CAPTURE: (date and time (Zulu) and place, including coordinates; if obtained from an individual, identify) .

6, PLACE OF CAPTURE.

7. CAPTURING UNIT: (unit initially obtaining document).

8. CIRCUMSTANCES OF CAPTURE.

9. TRANSLATOR.

10. TYPE OF TRANSLATION: (state whether extract or complete translation) .

J. TEXT OF TRANSLATION (Translation typed in here, using the format of the document. Use continuation sheets as needed).

(CLASSIFICATION)

Figure A-17. Documen translation report.

(CLASSIFICATION)

DATE : 231500ZAug88
TO: G2, X Corps

FROM : Team 1, IPW Section
441st Ml Bn, 23 Div (Armd)
X Corps

REPORT NUMBER: 08-0356

PART 1: CONTROL DATA

1. DOCUMENT NUMBER: US-WAIBVC-03093
2. DOCUMENT DESCRIPTION: Personal letter, 1 page, handwritten, mentions a tank factory disguised as a sugar processing plant, and school teachers and elderly people working in factories.
3. DOCUMENT'S ORIGINAL LANGUAGE: Russ i an
4. DATE AND TIME RECEIVED: 240847ZAug88
5. DATE AND TIME OF CAPTURE: 230923ZAug88
6. PLACE OF CAPTURE: NB640320
7. CAPTURING UNIT: A/1-41/23 AD
8. CIRCUMSTANCES OF CAPTURE: Found in an abandoned enerny CP,
9. TRANSLATOR: SSG Bennett
10. TYPE OF TRANSLATION: Full

PART 2. TEXT OF TRANSLATION

My dear Serzhen'ka:

It has been a long time since I received a letter from you. How are and where are you? The last time you wrote that fighting was going on around you all the time, and this worries me a lot. Take care of yourself. There have been many changes at home. Your mother, despite her age, had to go to work in the factory. They make tanks there, but the sign over the entrance says this is a sugar plant. I don't know why they do this. At the school where I work, we were also told to go and work at the same plant. They are going to close the school. Everyone has either to go to the front or work in the war industry. This is necessary in order to speed up the victory over the enemy of our country. I would be more at ease if I knew that you are alive and well. Please write as soon as you can.

Your KATHY.

(CLASSIFICATION)

Figure A-18. Sample translation report.

(CLASSIFICATION)
WORKING PAPERS

DEPARTMENT OF THE ARMY
1st Brigade IPW Team, 123d MI
APO New York, New York 09166

IPW TEAM REPORT NUMBER: DATE-TIME:

SCREENING REPORT

PART I. INFORMATION CONCERNING CAPTIVE:

A. PREVIOUS SCREENING OR INTERROGATION REPORTS (Unit or Report No!

B. CAPTURE INFORMATION:

1. CAPTIVE TAG NUMBER:

2. CAPTURING UNIT:

3. DATE-TIME OF CAPTURE:

4. PLACE OF CAPTURE:

5. Documents Captured (Disposition): _____

6. Equipment Captured (Disposition): _____

7. Circumstances of Capture: _____

c. BIOGRAPHICAL INFORMATION:

1. Full Name, Rank, Service Number: _____

2. Date, Place of Birth: _____

3. Sex, Marital Status, Religion: _____

4. Full Unit Designation or Unit Code: _____

(CLASSIFICATION)
WORKING PAPERS

Figure A-19. Sample blank screening report.

(CLASSIFICATION;
WORKING PAPERS

5. Duty Position: _____

6. Military Education and Experience: _____

7. Civilian Education and Experience: _____

8. Languages Spoken (Proficiency) : _____

D. OBSERVATIONS

1. Physical Condition of Captive: _____

2. Uniform, Insignia (type and condition): _____

3. Assessment of Attitude and Behavior: _____

4. Assessment of Knowledgeability: _____

PARTII. SCREENING RECOMMENDATIONS

A. SCREENER'S RECOMMENDATIONS:

1 Screener's and Interpreter's Names: _____

2. Place of Screening: _____

3. Screening Code: _____

9. SENIOR INTERROGATOR'S RECOMMENDATIONS:

1. Senior interrogator's Name: _____

2. Interrogate: _____

3. Action: _____

(CLASSIFICATION)
WORKING PAPERS

Figure A-19. Sample blank screening report (continued).

(CLASSIFICATION)
WORKING PAPERS

DEPARTMENT OF THE ARMY
Ist Brigade IPW Team, 123d MI
APO New York, New York 09166

IPW TEAM REPORT NUMBER: 007 DATE-TIME: 181530 AUG 99

SCREENING REPORT

PART I. INFORMATION CONCERNING CAPTIVE:

A. PREVIOUS SCREENING OR INTERROGATION REPORTS (Unit or Report No)

B. CAPTURE INFORMATION:

1. CAPTIVE TAG NUMBER: P-4A

2. CAPTURING UNIT: C Trp, Ist Sqdn, 8 ACR

3. DATE-TIME OF CAPTURE: 181300 AUG 99

4. PLACE OF CAPTURE: NB621108

5. Documents Captured (Disposition): lx ID card no 1350412 (retained by EPW); lx personal letter (evac with EPW); lx map section (evac with EPW).

6. Equipment Captured (Disposition): lx ShM protective mask (retained by EPW); lx standard web gear, lx individual first aid kit (both destroyed in place). lx 5.45rnn AK-74 w/4x mag (129x rds) (evacuated through supply channels).

7. Circumstances of Capture: Surrendered to US Patrol

C. BIOGRAPHICAL INFORMATION:

1. Full Name, Rank, Service Number: Boris Petrovich BARONOV, JrSGT, No 0951046

2. Date, Place of Birth: 16 JAN 78, BRYANSK, BySSR, USSR

3. Sex, Marital Status, Religion: Male, Single, None

(CLASSIFICATION)
WORKING PAPERS

Figure A-20. Sample completed screening report.

(CLASSIFICATION)
WORKING PAPERS

4. Full Unit Designation or Unit Code: Would Not Answer (WNA); QKN-854

5. Duty Position: WNA

6. Military Education and Experience: WNA

7. Civil ian Education and Experience: 10 yrs compulsory civil an education

8. Languages Spoken (Proficiency): Ukrainian (N) , Russian (FL

D. OBSERVATIONS

1. Physical Condition of Captive: Good

2. Uniform, Insignia (type and condition): Standard Soviet uniform, with JrSgt rank tabs and MR insignia, dirty and torn.

3. Assessment of Attitude and Behavior: Calm, cooperative.

4. Assessment of Knowledgeability: UNK

PART II. SCREENING RECOMMENDATIONS

A. SCREENER'S RECOMMENDATIONS:

1. Screener's and Interpreter's Names: SSG BROWN, None

2. Place of Screening: IPW See, 123d Ml Bn Ml, 23d Inf Div (Mech

3. Screening Code: A-2

B. SENIOR INTERROGATOR'S RECOMMENDATIONS:

1. Senior Interrogator's Name: MSG MOSCHETTI

2. Interrogate: YES

3. Action: None

(CLASSIFICATION)
WORKING PAPERS

Figure A-20. Sample completed screening report (continued).

(CLASSIFICATION)
Working Papers Date

TACTICAL
INTERROGATION REPORT

NAME OF PRISONER: LAST NAME SOURCE INTERROGATOR: RANK and LAST NAME

CATEGORY: A B C D UNIT OR FORMATION TO WHICH INTG ATTACHED: _____

INTG SERIAL NO: _____ MAPS USED: _____

DTG OF INTG: _____ LANGUAGE USED: _____

INTG REPORT NO: _____ INTERPRETER: _____

PART I - INTELLIGENCE POTENTIAL OF ENEMY PRISONER OF WAR (EPW)

A. PERSONAL PARTICULARS:

1. Rank, full name, service number, and position:

2. Date and place of birth:

3. Nationality: Ethnic: Religion:

4. Knowledge of languages and proficiency:

5. Unit, formation or organization:

6. Date-time, place or grid references, capturing unit, and circumstances of capture:

B. CAREER:

1. Pre-military:
   Paramilitary Tng:
2. Military:

C. ASSESSMENT OF INTELLIGENCE VALUE:

1. Intelligence, experience, cooperation, reliability:

2. Specialist knowledge:

3. Discussion of approach techniques:

(CLASSIFICATION)
Working Papers

Figure A-21. Sample blank tactical interrogation report.

(CLASSIFICATION)
Working Papers Date

D. DOCUMENTS CARRIED AT TIME OF CAPTUJRE:

1. List of documents:

2. Details of money and valuables:

E. EQUIPMENT OF INTELLIGENCE INTEREST CARRIED AT TIME OF CAPTURE:

1. Personal Equipment:

2. Weapons:

PART II - INFORMATION OBTAINED

A. SUMMARY:

DOI is Time of Capture (TOC) unless otherwise indicated in the body of this report.

B. TEXT:

i. MISSIONS

a. EPW (or) EPW and _____

(i) TOC:

(2) Fut:

(3) Past:

b. Unit:

(1) Pres:

(2) Fut:

(3) Past:

(CLASSIFICATION)
Working Papers

Figure A-21. Sample blank tactical interrogation report (continued).

(CLASSIFICATION)
Working Papers Date

c. Unit:

(1) Pres:

(2) Fut:

(3) Past:

2. COMPOSITION:

a.

b.

c.

d.

e.

3. STRENGTH:

a. Personnel :

(1)

(2)

(3)

b. Weapons and Equipment:

(1) individual Weapons:

(a)

(b)

(2) Crew-served Weapons:

(a)

(b)

(CLASSIFICATION)
Working Papers

Figure A-21. Sample blank tactical interrogation report (continued).

(3) Other Weapons:

(a)

(b)

(4) Armored Vehicles:

(a)

(b)

(5) Other Vehicles:

(a)

(b)

(6) Communications Equipment:

(a)

(b)

(7) NBC Equipment:

(a) Individual:

((1))

((2))

(b) Vehicular:

((1))

((2))

(8) Specialized Equipment:

(a)

(b)

Figure A-21. Sample blank tactical interrogation report (continued).

(CLASSIFICATION)
Working Papers

Date

4. **DISPOSITIONS**

a, Activity, FUD, 6 digit grid coordinate, physical description, collocated units: _____, scty measures: _____: DOI.

b.

5. **TACTICS:**

a. Offensive:

b. Defensive:

c. Special Operations:

6 **TRAINING:**

a. Individual:

b. Unit:

c. Specialized:

7 **COMBAT EFFECTIVENESS:**

a. Losses:

(1) Personnel :

(2) Equipment:

b) Replacements:

(1) Personne!:

(2) Equipment:

c Reinforcements:

(1) Personnel:

(2) Equipment:

(CLASSIFICATION)
Working Papers

Figure A-21. Sample blank tactical interrogation report (continued).

(CLASSIFICATION)
Working Papers Date

d. Combat Experience:

e. Morale:

8. LOGISTICS:

a. Weapons and Ammunition:

(1) Weapons:

(2) Ammunition:

b. Vehicles and POL:

(1) Vehicles:

(2) POL:

c. Food and Water:

(1) Food:

(2) Water :

d. Communications Equipment:

e. Medical:

(1) Individual Equipment:

(2) Vehicular Equipment:

(3) Personnel:

(4) Facilities:

(5) Evacuation Procedures:

f. NBC Equipment:

(1) Individual:

(2) Vehicular:

(CLASSIFICATION)
Working Papers

Figure A-21. Sample blank tactical interrogation report (continued).

g. Specialized Equipment: (NOTE: If para 3.b. (8) was Unk or None, D0 NOT write this sub-para at al!)

3 MISCELLANEOUS:

a. Personal ities:

Last name First name MN/I Rank PSN FUD

b. Code Names and Numbers:

(1) Code Names:

(2) Code Numbers:

c. Radio Frequencies and Call Signs:

(1) Radio Frequencies:

Radio	Primary	Alternate

(2) Call Signs:

Unit	Primary	Alternate

d. Passwords:

Challenge: Countersign:

(NOTE: If more than one password is known, use the following chart.!

Unit	Challenge	Countersign

e. Obstacles:

(1) Enemy:

(2) NATO:

f. PSYOPS:

(1) Enemy:

(2) NATO:

Figure A-21. Sample blank tactical interrogation report (continued).

(CLASSIFICATION)
WORKING PAPERS

TACTICAL
INTERROGATION REPORT

NAME OF PRISONER: BARANOV

INTERROGATOR:

CATEGORY: A (B) C D

UNIT OR FORMATION TO WHICH INTG ATTACHED: IPW See, 123d MI Bn 23d Inf Div (Mech)

INTG SERIAL NO: US-AR-2235-4A

MAPS USED: GERMANY, 1:50,000, EISENACH-HUNFELD, USACGSC 50-242

DTG OF INTG: 181500 AUG 99

LANGUAGE USED: RUSSIAN

INTG REPORT NO: 104

INTERPRETER: NONE

PART I - INTELLIGENCE POTENTIAL OF ENEMY PRISONER OF WAR (EPW)

A. PERSONAL PARTICULARS:

1. Rank, full name, service number, and position: JrSGT Boris Petrovich BARONOV, No, 0951046, driver

2. Date and place of birth: 16 JAN 78, BRYANSK, BySSR, USSR

3. Nationality: Soviet Ethnic: Ukrainian Religion: None

4. Knowledge of languages and proficiency: Ukrainian (N), Russian (FL) .

5. Unit, formation or organization: Regt HQ, 61MRR, 56MRD (HQ, 61MRR, 56MRD)

6. Date-time, place or grid references, capturing unit, and circumstances of capture: 181300 AUG 99; NB621108; C Trp, 1st Sqdn, 8 ACR; surrendered to US Border Patrol .

B. CAREER :

1. Pre-military: Civilian Education: 10 yrs compulsory. No vocational training. No civilian job. Paramilitary training: Standard preinduction training.

(CLASSIFICATION)
WORKING PAPERS

Figure A-22. Sample completed tactical interrogation report.

(CLASSIFICATION)
WORKING PAPERS

2. Military: 21 months conscripted service. Military schools: None. Previous job: None. Previous unit: None.

c. ASSESSMENT OF INTELLIGENCE VALUE:

1. Intelligence, experience, cooperation, reliability: Average, 3 years experience, cooperative, information checked against OB holdings.

2. Specialist knowledge: None.

3. Discussion of approach techniques: Direction approach failed but incentive approach was successful .

D. DOCUMENTS CARRIED AT TIME OF CAPTURE:

1. List of documents: lx ID card no 0951046 (retained by EPW), lx personal letter (returned to EPW), lx map section (evac to G-2)

2. Details of money and valuables: None

E. EQUIPMENT OF INTELLIGENCE INTEREST CARRIED AT TIME OF CAPTURE:

1. Personal Equipment: lx standard web gear, lx indiv first aid kit (both destroyed in.place), lx SHM protective mask (retained by EPW)

2. Weapons: lx 5.45rnn AK-74 assault rifle with 4x full mags (120xrds) (all evac thru supply channels)

PART II - INFORMATION OBTAINED

A. SUMMARY:

DOI is 181300 AUG 99 unless otherwise indicated in the body of this report.

B. TEXT :

1. MISSIONS

a. EPW

(CLASSIFICATION)
WORKING PAPERS

Figure A-22. Sample completed tactical interrogation report (continued).

(CLASSIFICATION)
WORKING PAPERS

(1) TOC: Waiting outside of gasthaus S of Spahl (NB6412) for PO, 61MRR, 56MRD and PO, 1MRB, 61MRR, 56MRD (lMRB, 61MRR, 56MRD) for over an hour.

(2) FUT: At 181330 AUG 99, was to drive PO, 61MRR, 56MRD and PO, 1MRB, 61MRR, 56MRD to a U/l unit 61MRR, 56MRD. (Hearsay: PO, 61MRR, 56MRD. DOI: 181130 AUG 99).

(3) PAST: Left CDP, 61MRR, 56MRD, located SE of Geismar (NB6515) 180800) AUG 99 and drove PO, 61MRR. 56MRD to CP, 1MRB, 61MRR, 56MRD. Waited for PO, 61MRR, 56MRD about 3 hrs and at 181130 AUG 99 drove PO, 61MRR, 56MRD and PO, IMRB, 61, 56MRD to gasthaus S of Spahl (NB6412). At 172330 AUG 99, left assembly area, 61MRR, 56MRD and drove CO, 61MRR, 56MRD to CP, 61MRR, 56MRD arriving at 172345 AUG 99.

b. Unit: 61MRR, 56MRD

(1) PRES: Preparing men and equipment to advance W to Nusttal (NB6010).

(2) FUT: Cross international Border and attack Nusttal (NB6010) NLT 190530 AUG 99. (Hearsay: PO 61MRR to PO 1MRB, 61MRR; DOI: 181130 AUG 99).

(3)- PAST: Moved into assembly area (exact locatlon unk). 61MRR, 16 AUG 99.

c. Unit: 1MRB, 61MRR, 56MRD

(1) ?RES: UNK

(2) FUT: U/l e!ement MRB to secure road junction somewhere N of Nusttal (NB601O) (exac loc unk). Road junction to be secured NLT 190430 AUG 99. (Hearsay: PO 1MRB to PO 61MRR; DOI 181130 AUG 99).

(3) PAST: UNK

2. COMPOSITION: (61MRR, 56MRD)

a. 61MRR had one HQ; three MRBs, dsg 1,2,3; one tk bn; one 122mm how bn; one engr co; one recon co; one supply and svc pit; one med co; one signal co

(Classification)
WORKING PAPERS

Figure A-22. Sample completed tactical interrogation report (continued).

(CLASSIFICATION)
WORKING PAPERS

b. Each MRB, 61MRR had one HQ; three MRC dsg 1,2,3; one mortar btry; one commo pit

3. STRENGTH: (HQ, 61MRR, 56MRD)

a. Personnel : (HQ, 61MRR) - HQ, 61MRR had approx 65 pers (UNK no off and EM)

b. Weapons and Equipment: (HQ, 61MRR)

(1) Individual Weapons: (HQ, 61MRR)

(a) UNK No x 9mm PM pistols (at least one ea off, HQ, 61MRR)

(b) UNK No X 5.45rrrn AK-74 assault rifles (at least one ea UAZ-469 driver, HQ, 61MRR)

(2) Crew-Served Weapons: LINK

(3) Other Weapons: UNK

(4 Armored Vehicles: (HQ, 61MRR) - 2xBTR-70, armament UNK (HQ, 61MRR)

(5 Other Vehicles: (HQ, 61MRR) - 3xUAZ-469 trk (one ea Regt driver, HQ, 61MRR)

(6 Communications Equipment: (HQ, 61MRR)

(a) 3xR-130 transceiver (trans) (one ea UAZ-469 , HQ, 61MRR)

(b) 2xR-123 VHF trans (one ea BTR-70, HQ, 61MRR')

(7) NBC Equipment: (HQ, 61MRR)

(a) Individual: (HQ, 61MRR)

((I)) UNK no.xShM prot masks (lx ea lower EM, HQ, 61MRR)

. ((2) UNK no.xShMK prot masks (lx ea off, lx ea NCO, HQ, 61MRR)

(cLASSIFICATION)
wORKING PAPERS

Figure A-22. Sample completed tactical interrogation report (continued).

((3)) UNK no.xOP-l prot clothing (one ea member, HQ, 61MRR)

((4)) UNK no.xlPP indiv decon kits (one ea member, HQ, 61MRR)

(b) Vehicular: (HQ, 61MRR) - 3xDK-4K portable decontamination sets (one ea UAZ-469 Trk, HQ, 61MRR)

(8) Specialized Equipment: UNK

4. DISPOSITIONS

a. CP, 61MRR, 56MRD loc vic NB665139 at intersection of 2xfarm roads in forest SE of Geismar (NB6515). Collocated units: UNK. Security measures: UNK no.x perimeter guards (FUD UNK). DOI: 180800 AUG 99.

b. Assembly area, 61MRR, 56MRD loc vic NB696163 (center of mass, and measures lkm N to S and E to W) SW of Kranlucken (NB7017). Collocated units: None. Scty measures: UNK No x perimeter guards (FUD UNK). DOI: 172330 AUG 99.

c. CP, 1MRB, 61MRR, F6MRD loc vic NB666156 at intersection of 2x farm roads E of Geismar (NB6515). Collocated units: None. Security measures: UNK. DOI: 181130 AUG 99.

d. DEPL, tk co (FUD UNK) loc vic from NB631104 to NB626104, along farm road S of Reinhards (NB621O). Tanks engines were running and were facing S. Collocate units and security measures: UNK. cot: 181245 AUG 99

5. TACTICS: UNK

6. TRAINING: (61MRR, 56MRD)

a. Individual: (HQ, 61MRR) - The 3x regt drivers have been practicing OPSEC (silence and no lights) while driving.

b. Unit: (61 MRR) - Extensive political training in the 61MRR for the last month. (Hearsay: PO, 61MRR to PO, 1MRB, 61MRR. DOI: 181130 AUG 99.)

c. Specialized: UNK

FIgure A-22 Sample completed tactical interrogation report (continued).

(CLASSIFICATION)
WORKING PAPERS

7. COMBAT EFFECTIVENESS: (61MRR, 56MRD)

a. Losses : (61MRR)

(1) Personnel: (61MRR) - Since arriving in the border area on 16 AUG 99, approx 20 training casualties have been evac to the rear, (Hearsay: PO, 61MRR to PO, 1MRB, 61MRR. Dot: 181130 AUG 99).

(2) Equipment: (61MRR) - None

b. Replacements: (61MRR) None, but there was a replacement center (FUD UNK) in "some large city". (Hearsay: PO, 61MRR to PO, 1MRB, 61MRR. DOI: 181130 AUG 99).

c. Reinforcements: UNK

d. Combat Experience: (HQ, 61MRR) - Most of the officers in HQ, 61MRR have had experience in Afghanistan, but it is always stressed that they were advisors and not fighters.

e. Morale: (HQ, 61MRR) - Officer morale is relatively high as they enjoy field duty and are anxious to show CO, 61MRR that they are proficient. Officers sometimes take their frustrations out on lower EM, causing them to become angry and despondent.

8. LOGISTICS: (HQ, 61MRR, 56MRD)

a. 'Weapons and Ammunit ion: (HQ, 61MRR)

(1) Weapons: (HQ, 61MRR) - All weapons are in good condition due to recondit ioning in JUL 99 by maint unit (FUD UNK). There are miscellaneous spare parts stored in each BTR-70. Hearsay: BTR-70 driver, HQ, 61MRR. DOI: 171400 AUG 99.)

(2 Ammunition: (HQ, 61MRR) - No problems with any ammo. 300xrds were issued for each AK-74 and 2 full mags (16xrds) for PM pistol on 171400 AUG 99 at assembly area, 61 MRR U/l officer, HQ, 61MRR.

b. Vehicles and POL: (HQ, 61MRR)

(CLASSIFICATION)
WORKING PAPERS

Figure A-22. Sample completed tactical Interrogation report (continued).

(CLASSIFICATION)
WORKING PAPERS

(1) Vehicles: (HQ, 61MRR) - All vehicles are in good condition, Drivers are constantly working on vehicles. Spare parts are available from chief of Motor Transport, HQ, 61MRR on an as needed basis, but all drivers steal parts from each other occasionally. Tool kits are stored in each vehicle.

(2 POL: (HQ, 61MRR) - All vehicles were refueled at assembly area, 61MRR 17 AUG 99, Additional fuel will be obtained ' from U/l tanker trucks, 61MRR after reaching Nusttal (NB601O) (Hearsay: chief of Motor Transport, HQ, 61MRR. DOI: 171800 AUG 99.)

c. Food and Water: (HQ, 61MRR)

(1) Food: (HQ, 61MRR) - 9 canned rations were issued to each member, HQ, 61MRR at assembly area, 61MRR 171700 by chief of Food Supply, HQ, 61MRR. After reaching NUSTTAL (NB601O), members will be receiving more canned rations. CO and PO, 61MRR keep their canned rations and eat at gasthauses in Spahl (NB6412).

(2) Water-: (HQ, 61MRR) - U/l Water trailer (FUD UNK) at HQ, 61MRR supplies water as needed.

d. Communications Equipment: (HQ, 61MRR) - All commo equip was in good condition as it was inspected by technical officer, 61MRR 171600 AUG 99 at assembly area, 61MRR.

e. Medical: (HQ, 61MRR)

(1) Individual Equipment: (HQ, 61MRR) - Each member was issued lx U/l indiv first aid kit around the first week of AUG (still sealed).

(2) Vehicular Equipment: (HQ, 61MRR) - Each vehicle had lx U/l first aid kit.

(3) Personnel: UNK

(4) Facilities: UNK

(5) Evacuation Procedures: UNK

f. NBC Equipment: (HQ, 61MRR) - All NBC equip was in good condition due to inspection by technical officer, 61MRR first week of Aug 99.

(CLASSIFICATION)
WORKING PAPERS

Figure A-22. Sample completed tactical Interrogation report (continued).

3. MISCELLANEOUS : (61MRR, 56MRD)

a. Personalities: (61MRR)

LAST NAME	FIRST NAME	MN I	RANK	PSN	FUD
OREKHOV	Nikolai	MNU	COL	CO	61MRR
MILENOVICH	Svetoslav	MNU	LTC	PO	61 MRR
GABOVICH	Vladimir	MNU	MAJ	TO	61 MRR

b. Code Names and Numbers: (61MRR)

(1) Code Name: (61MRR) - NOVY GOD
(2) Code Number: (61MRR) - QKN-854

cm Radio Frequencies and Call Signs: (61MRR)

(1) Radio Frequencies: (61MRR)

RAD 10	PR I MARY	ALTERNATE
R- 130	1.84 MHz	9.01 MHz

Radio frequencies are in effect 18 AUG 99 and are changed daily at 2400 hrs IAW 56MRD CEOI.

(2) Call Signs: (61MRR)

UNIT	PR I MARY	ALTERNATE
Regt HQ, 61MRR	ZHOLTAYA GORA	UNK
PO. 61MRR	ZHOLTAYA GORA-2	UNK

Call signs are in effect 18 AUG 99 and are changed daily at 2400 hrs AW 56MRD CEOI.

d. Passwords (61MRR) - Challenge: ZNAMYA Countersign: VPERYOD Passwords are in effect 18 AUG 99 and are changed daily at 2400 hrs AW 56MRD CEOI.

e. Obstacles UNK

f. PSYOPS : UNK

(CLASSIFICATION)
WORKING PAPERS

Figure A-22. Sample completed tactical interrogation report (continued).

BOMBING. SHELLING. AND MORTARING REPORTS

Bombing reports (BOMREPS), shell reports (SHELREPs), and mortar bombing reports (MORTREPs) supply information on enemy bombing, shelling, or mortaring activity. Submission is the responsibility of the affected unit. Reports are handled as normal messages and are transmitted by the fastest means available. Each transmission is preceded by the code word "SHELREP" in the case of enemy artillery, by the code word "MORTREP" in the case of enemy mortar or rocket fire, and by the code word "BOMREP" in the case of an enemy air attack. The text of the message is transmitted in the clear except for the unit identification and position of the observer. A call sign is used in place of unit identification. The observer's position is encoded if it discloses the location of a headquarters or an important OP. Figure A-23 shows the bombing, shell ing, and mortaring report format.

(CLASSIFICATION)

A. UNIT OF ORIGIN. (use current call sign, address group or code name) .

B. POSITION OF OBSERVER (grid reference preferred--encode if this discloses the location of a headquarters or important OP, or if subparagraph F2, below, is used to give information on location).

c. DIRECT}ON AND ANGLE OF FALL OR DESCENT. (direction and bearing of flash, sound, or groove of shell (state which) is measured clockwise from grld north in mils, unless otherwise specified, The angle of fall or descent may be determined by placing a stick or rod in the fuze tunnel and measuring in roils, Unless otherwise specified, the angle formed by the stick or rod in relation to the horizontal plane).

D. TIME FROM.

E. TIME TO.

F. AREA BOMBED, SHELLED, ROCKETED, OR MORTARED. (may be sent either as--

1. Grid reference (clear reference is to be used).

OR

2. Direction measures clockwise from grid north to impact points (degrees or rnils--state which) and distance in yards or meters (state which) from observer. This information must be encoded. When this method is used, maximum possible accuracy is essential) .

G. NUMBER AND NATURE OF GUNS, MORTARS, ROCKET LAUNCHERS, AIRCRAFT, OR OTHER METHODS OF DELIVERY.

H. NATURE OF FIRE. (adjustment, bombardment, harassing) (may be omitted for aircraft) .

1. NUMBER, TYPE AND CALIBER. (state whether measured or assumed) of shells, rockets (or missi!es) , and bombs.

J. TIME FROM FLASH TO BANG. (omit for aircraft).

F. DAMAGE . (encode if required).

NOTE: JCS Publication 12, page 14, requires an additional message indicator item. This item identifies the report being sent as a shell, bomb, or mortar report. It generally follows the unit of origin item in the message format.

(CLASSIFICATION)

Figure A-23. Format for BOMREP, SHELREP, or MORTREP reports.

NBC ATTACK REPORTS

NBC attack report formats are used according to the provisions of STANAGS 2103 and 2104 and FM 3-3 to report NBC attacks and the resulting NBC hazardous areas. Chemical and radiological hazardous areas resulting from nuclear and chemical attack by friendly forces are also reported using these formats. These reports are--

- NBC-1. Report used by the observing unit to give initial and subsequent data of an enemy chemical, biological, or nuclear attack.
- NBC-2. Report used for passing evaluated data of a chemical, biological, or nuclear attack.
- NBC-3. Report used for immediate warning of expected NBC contamination or hazardous area.
- NBC-4. Report used for radiation dose-rate measurements and detection of chemical or biological contamination.
- NBC-5. Report used to locate the area of NBC contamination or hazard.
- NBC-6. Report used to detail information on chemical or biological attacks.

NBC-1 and -4 reports are prepared by the unit under attack or a unit observing an attack. These reports are submitted through cormmand, intelligence, or FA communications channels to the designated headquarters TOC by the fastest means available. Initial enemy use of NBC weapons is always reported to the theater commander, through the chain of command, by the fastest means with a FLASH message precedence.

The information source for nuclear attack reports is normally the headquarters of an FA or AD unit (other units may also be designated as collection and reporting agencies). These units submit--

- An initial NBC-1 nuclear report to the unit's next higher headquarters with a FLASH message precedence.
- Subsequent NBC-1 nuclear reports, which are transmitted to the unit's next higher headquarters, with an IMMEDIATE message precedence, giving follow-up data.

The information source for chemical and biological attack reports is normally the headquarters of a company or independent platoon. It submits--

- An initial NBC-1 chemical or biological report, to its next higher headquarters, with a FLASH message precedence. The next higher headquarters forwards the initial NBC-1 chemical or biological report through command channels, to the NBC collection center, with the same message precedence.

- Subsequent NBC-1 chemical or biological reports, to the unit's next higher headquarters, with an IMMEDIATE message precedence, giving follow-up data. The next higher headquarters forwards subsequent NBC-1 chemical or biological reports through command channels, to the NBC collection center, with the same message precedence.

NBC COLLECTION CENTER

The NBC collection center is normally the nuclear, biological, and chemical element (NBCE) of the TOC at division. It consolidates NBC-1 nuclear, biological, or chemical reports of the same attack received from its various information sources and transmits an NBC-1 report to the NBC control center, normally the TOC at field army headquarters. It transmits appropriate NBC-2, -3, and -5 reports to subordinate, adjacent, and higher commands. If there is no NBCE, the G3 assumes these responsibilities.

NBC CONTROL CENTER

The NBC control center is normally the NBCE of the tactical operations center at field army. It consolidates and evaluates NBC reports received from subordinate commands and USAF, Marine Corps, and civilian installations and agencies. It directs reconnaissance and survey efforts; transmits evaluated NBC data to subordinate commands and adjacent area commands; and submits appropriate reports to higher headquarters, adjacent commands, and national agencies. If there is no NBCE, the G3 assumes these responsibilities.

NBC-1 REPORTS

NBC-1 reports follow the same format as SHELLREPs, MORTREPS, and BOMBREPs. The words "Type of Report," and the letters "B," "'D," "'H," or either "C or "F" always are reported. Other items are optional. Table A-3 shows the letter explanation for NBC-1 reports. Table A-21 shows the master list of available letters.

Table A-3. Letter explanation for NBC-1 report.

LETTER	MEANING	EXAMPLE NUCLEAR	EXAMPLE CHEMICAL	EXAMPLE BIOLOGICAL
	Precedence date and time (local or Zulu time, state which) Security classification From To Type of Report	NBC 1 (NUCLEAR)	NBC 1 (CHEMICAL)	NBC (BIOLOGICAL)
A.	Strike serial number (if known—as assigned by the NBCE at the operations center responsible for the areas in which the strike occurs).	A. 04	A. 02	
B.	Position of observer (UTM or place).	LB 196400	B. Marvile	

Table A-3. Letter explanation for NBC-1 report (continued).

ETTER	MEANING	EXAMPLE NUCLEAR	EXAMPLE CHEMICAL	EXAMPLE BIOLOGICAL
C.	Direction measured clockwise from or magnetic north (state which) of the attack from observer (degrees or mils, state which).	C. Grid 060 Degrees		
D.	Date and time of denation or date and time attack started (local or Zulu time, state which).	D. 201405 Zulu	D. 201405 (local)	D. 201405 HOTEL
E.	Illumination time (seconds) or time attack ended (local or Zulu, state which).		E. 201412 (local)	
F.	Location of attack (UTM or place) or area attacked (actual or estimated, state which).		F. LB 25300 estimated	F. LB 2030 actual F. LB 2030 actual
G.	Means of delivery, if known.		G. Artillery	G. Aircraft, 100 meters
H.	Type of burst—air, surface or unknown (state which)—including height, if known; type of agent, if known (chemical or biological); or type of attack (chemical or biological).	H. Surface	H. Airburst, nerve	H. Aerial spray
I.	Type and number of munitions or aircraft (state which).			
J.	Flash-to-bang time (seconds).	J. 60		
K.	Crater present or absent and diameter if known (meters).			
L.	Nuclear burst angular cloud width measured at 5 minutes after the detonation (degrees or mils, state which). (Do not report if data is obtained more than 5 minutes after the detonation).	L. 280 mils		
M.	Stabilized cloud-top angle and cloud-bottom angle (state which) or cloud-up and cloud-bottom height (state which) measured at H+10 minutes (degrees, mils, meters, or feet—state which).			
S.	Date-time of reading or date-time contamination initially detected (chemical or biological). State whether local or Zulu time.	S. 201500 (local)		
X.	Located area of contamination (UTM).	X. LB 206303 LB 206306 LB 203303 LB 203306		
	NOTE: When the contaminated area is a complete circle, the first coordinate will be repeated as a last coordinate			

Table A-4. Initial nuclear report example.

(CLASSIFICATION)

FLASH 090910 ROMEO
UNCLASSIFIED
FROM REDDOG TO AMIGO
NBC-1 NUCLEAR
BRAVO SHACKLE DELTA HOTEL BRAVO
UNSHACKLE
CHARLIE GRID 182 MILS
DELTA 090907 ROMEO
HOTEL SURFACE
JULIET 60
END OF MESSAGE

(CLASSIFICATION)

Table A-5. Initial chemical report example.

(CLASSIFICATION)

FLASH
201408 HOTEL
FROM Q7R06
TO E4Z03
NBC-1 CHEMICAL
BRAVO MARVILLE
DELTA 201405 HOTEL
FOXTROT LIMA BRAVO 205305
ESTIMATED
GOLF ARTILLERY
HOTEL AIR

(CLASSIFICATION)

Table A-6. Subsequent NBC-1 nuclear report example.

(CLASSIFICATION)

IMMEDIATE 090913 R0ME0
UNCLASSIFIED
FR0M REDD0G T0 AMIG0
NBC-1 NUCLEAR
BRAV0 SHACKLE DELTA H0TEL BRAV0
UNSHACKLE
CHARLIE GRID 182 MILS
DELTA 090907 R0ME0
H0TEL SURFACE
LIMA 280 MILS
END 0F MESSAGE

(CLASSIFICATION)

Table A-7. Subsequent NBC-l chemical report example.

(CLASSIFICATION)

IMMEDIATE
201438 H0TEL
FR0M Q7R06
T0 E4Z03
NBC-1 CHEMICAL
ALPHA 02
ECH0 201405 H0TEL
H0TEL NERVE

(CLASSIFICATION)

NBC-2 reports are used for passing evaluated data of an NBC attack. They are normally based on two or more NBC-1 reports and include an attack location and in the case of a nuclear detonation, an evaluated yield. Tables A-8 and A-9 show examples of NBC-2 (nuclear) and NBC-2 (chemical) report messages.

Table A-8. NBC-2 nuclear report example.

(CLASSIFICATION)

E4Z03E4Z03
IMMEDIATE NBC-2
FROM Q7J04
ALFA/N001
201405 ZULU
FOXTROT LIMA BRAVO 187486
HOTEL SURFACE
NOVEMBER 50
YANKEE/050/01Z KPH

(CLASSIFICATION)

Table A-9. NBC-2 chemical report example.

(CLASSIFICATION)

E4Z03E4Z03
IMMEDIATE NBC-2
FROM Q7J04
200945Z
FOXTROT LIMA BRAVO 126456Z
HOTEL NERVE

(CLASSIFICATION)

NBC-2 reports include the attack time, location, and, in the case of a nuclear detonation, an evaluated yield. Letters "A,'" "D,"' "F," "H," and "N"" are repeated as often as necessary to produce a summary report. Other letters may be added; however, the letters mentioned must be included in the report. Table A-10 shows the letter explanation for NBC-2 reports.

Table A-10. Letter explanation for NBC-2 report.

LETTER	MEANING	EXAMPLE NUCLEAR	EXAMPLE CHEMICAL AND BIOLOGICAL
	Precedence		
	Date-time (local or Zulu time, state which)		
	Security Classification		
	From		
	To		
	Type of Report	NBC-2 (NUCLEAR)	NBC-2 (CHEMICAL)
A.	Strike serial number	24	i
D.	Date-time of detonation or date-time attack started (local or Zulu time, state which).	201405 Zulu	200945 (local)
F.	Location of attack (UTM or place) or area attacked (actual or estimated, state which) .	LB 187486 actual	LB 126456 actual
G.	Means of delivery, if known.		
H.	Type of burst--air, surface, or unknown (state which)-- including height, if known; type of agent, if known; (chemical or biological); or type of attack (chemical or biological).	Surface	Nerve
N.	Estimated yield (kt).	50	

NBC-3 REPORTS

NBC-3 reports provide irrmediate warning of expected NBC contamination or hazardous areas. Tables A-11 and A-12 show examples of NBC-3 (chemical) and NBC-3 (nuclear) messages.

TableA-II. NBC-3 nuclear report example.

(CLASSIFICATION)

```
A5Z0!E3Z02
IMMEDIATE NBC-3
FR0M R4Q06
DELTA 201402
F0XTR0T LIMA BRAV0 187486
H0TEL SURFACE
PAPA ALPHA-
LIMA BRAV0 199420
LIMA BRAV0 200440
LIMA BRAV0 255410
LIMA BRAV0 257457
YANKEE 0272-0312 DEGREES
ZULU 019-025-05
```

(CLASSIFICATION)

Table A-12. NBC-3 chemical report example.

(CLASSIFICATION)

```
A5Z0!E2Z02
IMMEDIATE NBC-3
FR0M R4Q06
DELTA 201415Z
F0XTR0T LIMA BRAV0 206300Z
H0TEL BC GB
PAPA ALPHA LIMA BRAV0 208320, LIMA BRAV0
210320, LIMA BRAV0 206130, LIMA
BRAV0 204310
```

(CLASSIFICATION)

Table A-13 explains the letters in the NBC-3 nuclear and chemical report examples, Other letters from the master list, are added at the users' discretion.

NOTE: When the effective windspeed is less than 8 kph, the NBC-3 report consists of the letters "D,'" "F,' and "Z." "Z" contains three digits only, (the radial distance of zone l).

Table A-13. Letter explanation for NBC-3 reports.

LETTER	MEANING	EXAMPLE NUCLEAR	EXAMPLE CHEMICAL AND BIOLOGICAL
	Precedence Date-time (local or Zulu time, state which) Security Classification From To Type of Report	NBC 3 (NUCLEAR)	NBC (CHEMICAL AND BIOLOGICAL)
A.	Strike serial number.	A. 24	A. 3
D.	Date-time of detonation or date-time attack started (local or Zulu time, state which).	D. LB 201405 Zulu	D. 201405 (local)
F.	Location of attack (UTM or place) or area attacked (actual or estimated, state which).	F. LB 187486 actual	F. LB 206300 actual
P.	Areas of expected contamination (UTM).		P. LB 208320 LB 206310 LB 210320 LB 204310
Y.	Direction measured clockwise, from grid north, to the left and then to the right radial lines (degrees or mils, state which) (4 digits each).	Y. 0272-0312 degrees	
Z.	Effective windspeed (kph), 3 digits; downwind distance of zone 1 (km); 3 digits; cloud radius (km), 2 digits. (When effective windspeed is less than 8 kph, use 3 digits only for radial distance zone 1).	Z. 019-025-05	

NBC-4 reports are used to transmit radiation dose-rate measurements. Tables A-14 and A-15 show examples of NBC-4 radiation dose-rate messages.

Table A-14. NBC-4 report example 1.

(CLASSIFICATION)

E4Z03 E4Z03
IMMEDIATE NBC-4
FROM Q7R06
201745 HOTEL
QUEBEC LIMA BRAVO 123987
ROMEO 35 INITIAL
SIERRA 201735 HOTEL

(CLASSIFICATION)

Table A-15. NBC-4 report example 2.

(CLASSIFICATION)

REDDOG 3 REDDOG 3
IMMEDIATE NBC-4
FROM ALFA
201745 HOTEL
QUEBEC LIMA BRAVO 123987
ROMEO 1 INITIAL
SIERRA 201735 HOTEL

(CLASSIFICATION)

Table A-16 explains the items in the examples for NBC-4 nuclear and chemical report formats. The letters "Q," "R," and "S" are repeated as often as necessary. Users of NBC-4 reports are not confined solely to the use of the letters shown in the examples; other letters from the master list, (see table A-21), are added at the users' discretion.
NOTE: Radiation dose-rates are measured in the open, one meter above the ground. Other conditions are specified in the message as part of line ROMEO.

Table A-16. Explanation of letters for NBC reports.

LETTER	MEANING	EXAMPLE
	Precedence Date-time (local or Zulu time, state which) Security Classification From To Type of Report	 NBC-4 (NUCLEAR)
Q.	Location of reading (UTM)	Q. LB 123987
R.	Dose-rate (cGy/hr) (this is NOT normalized to H + 1 hour). The words "initial," " increasing, " "peak," or "decreasing," may be added (correlation factor information is included if shielded dose-rate readings are reported).	
s.	Date-time of reading (local or Zulu, state which)	S. 201735 (local) Q. LB 129965 R. 60 S. 201650 (local) Q. LB 146808 R. 27 INCREASING S. 201710 (local)

NBC-5 REPORTS

NBC-5 reports identify the area of contamination or hazard. Tables A-17 and A-18 show examples of an NBC-5 report messages.

Table A-17. NBC-5 nuclear report example.

(CLASSIFICATION)

```
A5Z0!E3Z02
IMMEDIATE NBC-5
090913 G0LF
FR0M REDD0G
T0 AMIG0
NBC-5 NUCLEAR
TANG0 201505Z
VICT0R N0VEMBER DELTA   651455
                        810510
                        821459
                        651455
WHISKEY NOVEMBER DELTA  604718
                        991686
                        114420
                        595007
```

(CLASSIFICATION)

Table A-18. NBC-5 chemical report example.

(CLASSIFICATION)

```
A5Z0!E2Z02
IMMEDLATE NBC-5
SIERRA 20080000Z
TANG0 201045Z
EXRAY CHEM N0VEMBER
DELTA                   206991
                        201575
                         200787
                        206991
```

(CLASSIFICATION)

The NBC-5 report is most useful when sent as a map trace or overlay (if time and distance permit). When the contamination arises from a single threat or unidentified nuclear burst, the dose-rate always refers to H+1 hour, and the letter "'T" is used. When there have been several nuclear detonations at different times or on different days and no single H+1 hour is possible, the dose rates are reported as a specified item using the letter "'O." Letters "O" and "T" are, therefore, alternatives; both cannot be used in the same report. Table A-19 explains the letter designations used in NBC-5 reports.

NOTE: When requested decay rates are to be transmitted, use the letter "R. "

Table A-19. Letter explanation for NBC-5 reports.

LETTER	EXAMPLE NUCLEAR	EXAMPLE CHEMICAL AND BIOLOGICAL
Precedence Date-time (local or Zulu time, state which) Security Classification From To Type of Report	NBC-5 (NUCLEAR)	NBC-5 (CHEMICAL and BIOLOGICAL)
A. Strike serial numbers causing contamination (if known)	A. 24	A. 1
o. Reference date-time for estimated contours (see note (2) above) when not H+1 hour		
s. Date-time contamination initially detected (chemical or biological (local or Zulu time, state which)		S. 200800 (local)

Table A-19. Letter explanation for NBC-5 reports (continued).

T.	H+1 date-time or date-time of latest reconnaissance of contamination in the area (chemical or biological). State whether local or Zulu time.	T. 201505 ZULU	T. 201045 (local)
u.	1,000 cGy/hr contour I ine coordinates		
v.	300 cGy/hr contour line coordinates	V. ND 651455 ND 810510 ND 821459 ND 651455	
w.	100 cGy/hr contour line coordinates	W. ND 604718 ND 991686 ND 114420 ND 595007	
x.	20 cGy/hr contour line coordinates, or located area of contaminant ion (chemical or biological)		X. CHEMICAL ND 206991 ND 201575 ND 200787 ND 206991

Figure A-24 shows a current example of the estimated radiological contamination trace (dose-rate type) format. It is not necessary, or even desirable, to report all four of the contours for different dose rates. Four are given to provide flexibility. (In the example, only two are reported.) When a contour closes to form a complete ring, the first coordinate is reported at the end. The following are colors used for plotting and sending the report as a trace:

- Red for 1 ,000 cGy/hr.
- Green for 300 cGy/hr.
- Blue for 100 cGy/hr.
- Black for 20 cGy/hr,

Yellow is used for chemical and biological contamination or hazardous areas. Additional letters, including those shown in the examples in Table A-19, are used. Letters from the master list in Table A-21 are added at the users' discretion.

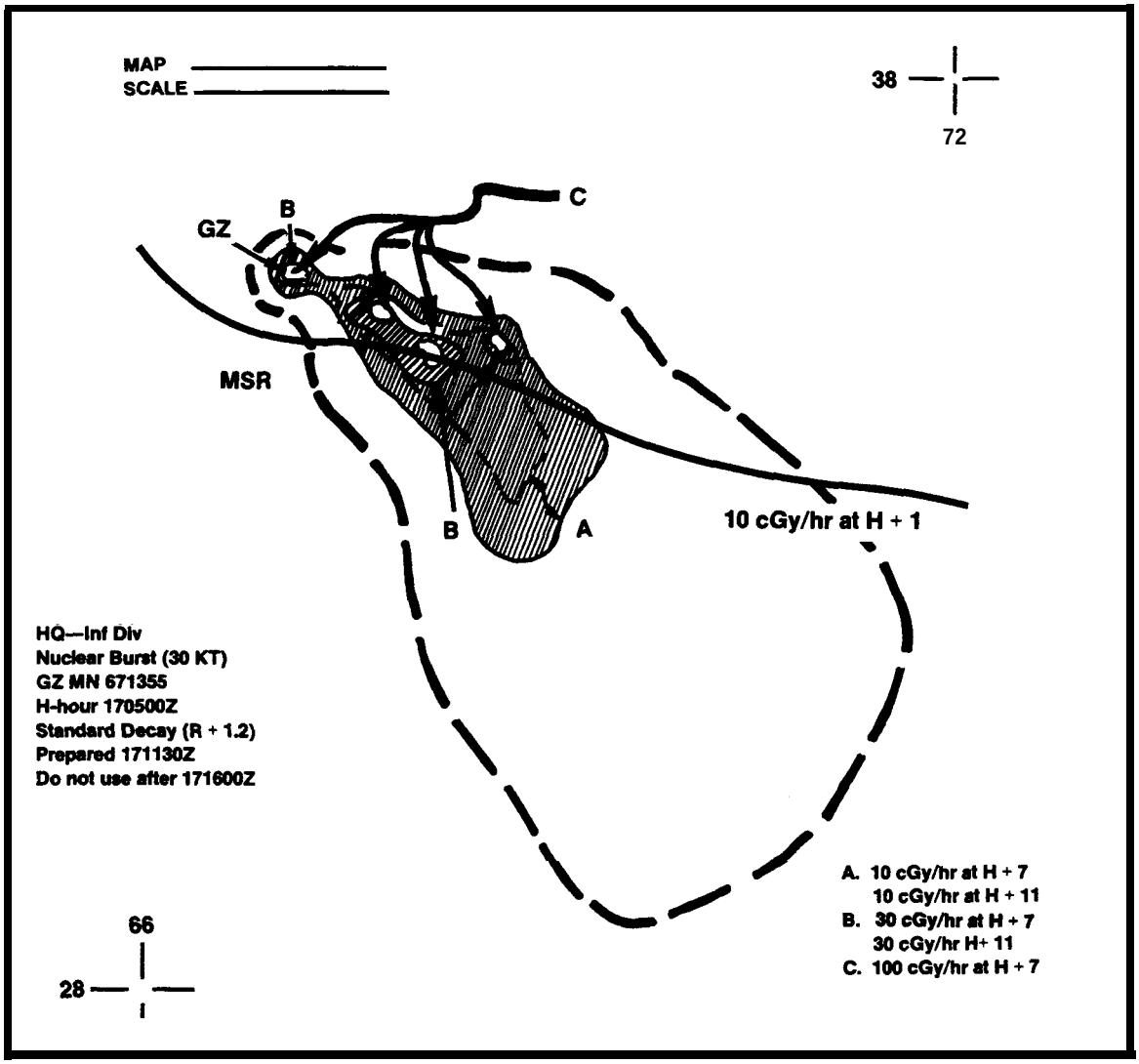


Figure A-24. Radiological contamination trace.

NBC-6 REPORT

NBC-6 reports are used to summarize information concerning a chemical or biolog ical attack. Table A-20 shows an NBC-6 biological report.

Table A-20. NBC-6 biological report.

ALFA	coo l
DELTA	200430Z
ECHO	200435Z
FOXTROT	LBZO0300 to LB208304 Actual
GOLF	Aerial spray
HOTEL	Toxin
INDIA	2 Aircraft
KILO	Rolling hills, mostly open
MIKE	Enemy broke contact just before the attack, then bypassed on right f l ank
QUEBEC	Soil sample taken at LB200300
YANKEE	Downwind direction 270 degrees, wind speed 015 kph
ZULU BRAVO	This is the only biological attack in our area

The NBC-6 report is a narrative description of chemical and biological attacks that have occurred in a unit's AO. It is designed to be developed at battalion level and above. It contains as much information as is known about the attacks. It is submitted only when requested and is usually sent in hard copy.

MASTER LIST

Table A-21 shows the master list of letters that is applicable to all types of NBC reports. Each letter is annotated. Care should be taken to ensure that letters mandatory for each NBC report are incorporated before adding letters to the reports, overlays, or traces.

Table A-21. Master list of letters.

LETTER	MEANING	MEANING
	NUCLEAR REPORTS	CHEMICAL OR BIOLOGICAL REPORTS
A.	Strike serial number(s).	Strike serial number(s).
B.	Position of observer (UTM or place) .	position of observer (UTM) or place) .
c.	Direction measured clockwise from grid or magnetic north (state which) of the attack from observer (degrees or roils, state which).	Direction measured clockwise from grid or magnetic north (state which) of the attack from observer (degrees or roils, state which) .
D.	Date-time of detonation (local or Zulu time, state which) . If local time is used, give the letter of the local time zone, if-known. See FM 101-10-1 for time-zone charts. If the local time is used and the time-zone letter is not known, the word "local" will be transmitted with this item.	Date-time attack started (!ocal or Zulu time, state which). If local time is used, give the letter of the local time zone, if known. See FM 101-10-1 for time-zone charts. If the local time is used and the time-zone letter is not known, the word '"local, " will be transmitted with this item.
E.	Illumination time. (Report only when other data are not available. Report in seconds.)	Time attack ended (local or Zulu, state which).
F.	Location of attack (UTM or place) (actual or estimated, state which).	Area attacked (actual or estimated, state which).
G.	Means of delivery, if known.	Means of delivery, if known.
H.	Type of burst--air, surface, or unknown, state which-- including height, if known.	Type of agent, if known (chemical or biological). Type of attack (chemical or biological).
1.	(This letter item is not used for nuclear report.)	Type and number of munitions or aircraft (state which).
J.	Flash-to-bang time (seconds).	
K.	Crater present or absent and diameter, if known (meters) .	

Table A-21. Master list of letters (continued).

LETTER	MEANING	MEANING
	NUCLEAR REPORTS	CHEMICAL OR BIOLOGICAL REPORTS
L.	Nuclear burst angular cloud width measured at 5 minutes after the detonation (degrees or roils, state which). (Do not report if data is obtained more than 5 minutes after the detonation.)	
M.	Stabilized cloud-top angle and cloud-bottom angle (state which) or cloud-top height and cloud-bottom height (state which) measured at H+1O minutes (degrees, roils, meters, or feet--state which).	
N.	Estimated yield (kt).	
0.	Reference date-time for estimated contours when not H+l hour.	
P.	For radar purposes only:	Area of expected contamination (UTM).
P.A.	UTM coordinates of points to outline external contours of radioactive clouds.	
P.B.	Effective wind direction (direction from which the wind is blowing) in degrees or roils (state which).	
Q.	Location of reading (UTM).	
R.	Dose-rate (cGy/hr). The words "initial," "increasing,"' "peak." or "decreasing" may be added.	
s.	Date-time of reading (local or Zulu time, state which).	Date-time contamination initially detected (local or Zulu time, state which).
T.	H+l date-time (local or Zulu time, state which).	Date-time of latest reconnaissance of contamination in the area (local or Zulu time, state which).
u.	1,000 cGy/hr contour line coordinates (UTM) (red).	
v.	300 cGy/hr contour line coordinates (UTM) (green).	

Table A-21. Master list of letters (continued).

LETTER	MEANING	MEANING
	NUCLEAR REPORTS	CHEMICAL OR BIOLOGICAL REPORTS
W.	100 cGy/hr contour line coordinates (UTM) (blue).	
x.	20 cGy/hr contour line coordinates (UTM) (black).	Located area of contamination (UTM) (yellow).
Y.	Direction measured clockwise from grid north to the left and then to the right radial lines (degrees or roils, state which--4 digits each).	
z.	Effective windspeed (kph), 3 digits; downwind distance of zone I (km), 3 digits; cloud radius (km), 2 digits. (When effective windspeed is less than 8 kph, the NBC-3 report will contain only three significant digits, that is, the radial distance of zone I.)	

ANALYSIS OF AREA OF OPERATIONS

Figure A-25 shows a completed sample and explanation of analysis of the area of operations. The following paragraphs are keyed to paragraphs in the sample.

1. **PURPOSE AND LIMITING CONSIDERATIONS.** State the purpose of the analysis and define the area that is being analyzed. Include a statement of the mission of the command and other considerations that limit the applicability of the analysis. Include the commander's plan of action and enemy capabilities.

2. **GENERAL DESCRIPTION OF THE AREA.**

a. Climatic or Weather Conditions. This paragraph lists items of weather information that have military significance. Throughout the remainder of the analysis, weather information is interpreted as to its operational effects. For example, winds at low temperatures are interpreted in terms of the wind chill factor and the resulting effects on operations, such as attack or defense which must face the prevailing winds, or the use of open or closed storage facilities.

Light data is always reported to assist in selecting courses of action and the conduct of mil itary activities.

The BMNT and the EENT are the beginning and end, respectively, of enough light for limited visibility. The BMCT and the EECT are the beginning and end, respectively, of adequate light for large-scale operations.

Moon phases and other phenomena, like atmospheric conditions and star brilliance, also influence night operations. During full moonlight, conditions of visibility sometimes approach those of daylight. Such conditions need to be anticipated as they influence friendly and enemy courses of action such as attacks, patrolling, and changes in dispositions.

b. Terrain.

(1) Relief and Drainage System, Drainage and ridge lines are basic elements in studying terrain, as they clearly indicate the general shape of the ground. A complete study of relief and drainage includes detailed information about slope, configuration, elevation of ground forms; and depth, width, tide data, and conditions of banks and bottoms of streams and rivers. These items are portrayed graphically on maps.

(2) Vegetation. Vegetation studies are best presented in the form of tinted, or otherwise marked, overlays. Considerations include locations of trees, diameters of trunks, density, ground cover or canopy, undergrowth, and types of natural and cultivated vegetation in nonwooded areas.

(3) Surface Materials. Surface materials are best presented on colored or marked overlays. Soil maps made by the agricultural services of various countries are particularly valuable. The information contained in soil maps frequently is translated into a trafficability map and a map of areas susceptible to high levels of induced radioactivity. A trafficability map based on weather forecasts are colored or marked to indicate degrees of trafficability effectively shows areas suitable for cross-country movement.

(4) Artificial Features, Artificial features of potential military significance include roads, railroads, bridges, tunnels, mines, towns, industrial areas, and fortifications. The features are best represented on maps or marked overlays.

c. Additional Characteristics. Only those characteristics--sociology, politics, economics, transportation, manpower--which influence the choice of a course of action by either force are included. Lengthy data is presented in an annex, preferably in tabular form.

3. MILITARY ASPECTS OF THE AREA. The facts listed in paragraph 2 are analyzed and their influence on tactical and CSS factors that are considered in the selection of a course of action by either force are determined. In the analysis of these factors, the effects of and on nuclear fires, chemical and biological agents, and important devices and equipment used in implementing courses of action are integrated, as appropriate. The tactical aspects of observation and fire, concealment and cover, obstacles, key terrain features, AAs, and the CSS aspects are discussed in the following paragraphs.

a. Tactical Aspects.

(1) Observation and Fire.

(a) Observation depends on conditions of terrain which permit a force to locate the enemy, either visually or through the use of surveillance devices. The highest terrain in an area usually provides the best observation. The increased use of equipment with LOS characteristics requires the availability of suitable terrain features for sighting purposes; while at same time, the capability of employing organic aerial platforms reduces the requirement to use such terrain. Dust clouds caused by nuclear blast reduce electronic LOS. Other limits to observation include darkness and tall vegetation (woods and jungle canopy). The effects of visibility on observation are analyzed along with weather conditions.

(b) Fire, as used in the analysis of the battlefield area, includes the FofFs of all weapons and characteristics of weapons del ivery systems affected by weather and terrain. For example, gusty surface winds affect the use of projectiles. High, irregular terrain features or the absence of overhead mass clearance limit FofFs. A FofF is an area that weapons can cover effectively with fire from given positions. Although observation is essential to effective control of fire, the best observation does not always guarantee the best FofF. An ideal FofF for flat-trajectory weapons is an open area in which the enemy can both be seen and has no protection weapons fire.

(2) Concealment and Cover.

(a) Concealment is protection from observation. It is provided by woods, underbrush, snowdrifts, tall grass, cultivated vegetation, darkness, smoke, dust, fog, ground haze, rain, or falling snow.

(b) Cover is protection from the effects of direct and indirect fires. It is provided by ditches, quarries, caves, riverbanks, folds in the ground, shell craters, buildings, walls, railroad embankments and cuts, sunken roads, and highway fills. Defiladed areas which provide protection against some types of weapons do not necessarily protect against effects of nuclear fires. Unless the forward slopes of a terrain mass are very steep, nuclear blast will affect personnel and material on the reverse slope because the blast wave follows the configuration of all but the most rugged terrain. When a nuclear weapon is fired over a deep val ley, or the valley axis points toward ground zero, the blast effects are canal ized, increasing the damage. Irregular terrain provides some cover from thermal radiation of nuclear fires. Few buildings are sufficiently strong to withstand all effects of blast or, if not damaged or destroyed by blast, to be unaffected by thermal radiation. Foxholes, bunkers, and tunnel-type shelters offer the simplest forms of effective cover.

(c) Concealment and cover are desirable for both the attack and the defense. If troops move forward under the concealment of woods, fog, or a moonless night, the chances of achieving surprise are greater. If troops move protected from the enemy's fire by ditches, embankments, or walls, the attack is more effective. In a defensive situation, friendly forces seek to defend in an area which offers both concealment and cover but does not provide covered approaches for the enemy.

(d) The mobility of the command is considered in determining avai lable concealment and cover. Concealment and cover are desirable during troop movements by any means. Routes which afford good concealment and cover reduce the vulnerability of a moving force to detection and to destruction by fire.

(3) Obstacles.

(a) An obstacle is any natural or artificial terrain feature which stops, impedes, or diverts military movement. Natural obstacles include rivers, streams, canals, lakes, swamps, cliffs, steep slopes, dense woods, jungles, deserts, mountains, cities, and certain types of unstable soil . Artificial obstacles are works of construction and destruction executed to stop or impede military movement. They include minefield, craters, antitank ditches, trenches, abatises, roadblocks, deliberately flooded areas, areas contaminated with chemical and biological agents, extensive rubble, forest fires, trees blown down, and areas contaminated with residual nuclear radiation.

(b) To be fully effective, obstacles are covered by observation and fire. However, even undefended obstacles may canal ize an attacker into concentrations which are easier to detect and which are suitable for nuclear attack. Obstacles perpendicular to a direction of attack favor the defender by slowing the enemy, forcing the enemy into concentrations that tend to occur while crossing obstacles, and holding the attacker for a longer time under the effective fires of the defense. Obstacles parallel to an axis of advance give the attacker flank protection. However, parallel obstacles interfere with lateral movement and coordination.

(c) The mission of the command influences consideration of obstacles. In the defense, the intelligence officer identifies as obstacles those features of the terrain which stop, impede, or divert military movement into, out of, or within the area encompassed by the FEBA, lateral boundaries, and the rear boundary (prescribed or assumed). In the attack, the intelligence officer considers the obstacles from the line of departure to the objective (both inclusive), bounded laterally by the assigned or assumed operational zone.

(4) Key Terrain Features.

(a) A key terrain feature is any locality or area whose seizure or control affords a marked advantage to either opposing force. Key terrain features are selected to indicate areas and localities whose seizure or control are considered in formulating and selecting courses of action. The selection is based on the level of command, type of unit, and mission of the command. Key terrain which would give us a marked advantage in the accomplishment of our mission is selected. If it is seized or controlled by the enemy, it would delay the accomplishment of our mission. For example, a bridge over an unfoldable river gives access to the opposite shore without requiring an assault crossing, Control of a road or rail center reduces the enemy's ability to resist our advance. A level clearing in rough terrain is the only accessible landing field for airmobile operations.

(b) Key terrain varies with the level of command. For example, to an army commander, a large city affords marked advantages as a communications center. To a division commander, the high ground which dominates the city is more important, and the city itself is an obstacle,

(c) Obstacles are rarely key terrain features. The high ground dominating a river, rather than the river itself, is usually the key terrain feature for the lower unit commander. An exception is an obstacle like a built-up area, which is assigned as an objective to a force; the obstacle then becomes key terrain to the force ordered to capture it.

(d) Key terrain, in addition to influencing mission accomplishment, is also highly significant in applying combat power. Control is not ensured only by seizure and occupation. Seizure and physical occupancy of key terrain features by relatively large forces may not be desirable, Destructive fires delivered by long-range means can destroy forces physically occupying key terrain. The commander controls key terrain to avoid destruction of force while keeping the enemy from gaining control. Control includes maneuver, surveillance, security, and use of fires. Terrain which permits or denies maneuver is key terrain. Tactical use of terrain often is directed at increasing the capability for applying combat power and, at the same time, forcing the enemy into areas which result in reduction of the enemy's abil ity to apply combat power. Terrain which permits this also is key terrain. The effects of terrain on maneuver, appl ication of combat power, and preservation of force integrity are considerations in selecting and controlling key terrain and its tactical use.

(e) In the offense, key terrain features are usually forward of the friendly dispositions and are often assigned as objectives. However, terrain features in adjacent sectors are key terrain if their control is necessary for the continuation of the attack or the accomplishment of the mission. If the mission is to destroy enemy forces, terrain is selected whose seizure helps ensure the required destruction. Terrain which gives the enemy effective observation along an axis of advance to be used by the friendly forces is key terrain if the enemy must be denied its possession or control. Key terrain is within friendly territory when its control is essential to the success of an offensive operation. For example, if the enemy attacks before friendly forces attack, the control of this terrain is essential because it affords a marked advantage. Thus, it is a key terrain feature.

In the defense, key terrain is usually within the assigned sector and within or behind the selected defensive area. Some examples of key terrain are--

- Terrain which gives good observation over AAs to and into the defensive position.
- Terrain which permits the defender to cover an obstacle by fire.

- Important communication centers which affect command communications and the use of reserves.

Key terrain also is forward of the defensive area or in adjacent sectors. For example, a terrain feature along the FLOT or in an adjacent sector which gives the enemy good observation over defended localities, corrrnunication routes, or enemy AAs is key terrain when active measures are taken to reduce the enemy advantage. The defender moves positions forward to include the feature or take action to minimize the enemy advantage by the use of fire, chemicals, smoke, concealment, and cover.

(5) Avenues of Approach. An AA is a route for a force of a particular size to reach an objective or key terrain. To be considered an AA, a route provides some ease of movement and enough width for dispersion of a force of a sufficient size to significantly affect the outcome of the operation. The division G2 usually considers AAs adequate for the type brigade of the particular division. The corps and higher G2s usually consider AAs adequate for at least a division. In determining the width of dispersion, consideration is given to the deployment patterns, mobi I ity means, and area required for maneuver to prevent presenting lucrative targets for nuclear fires.

(a) Ground Avenues of Approach. A valley approach gives the advancing force some cover from enemy direct fire and some concealment from enemy observation. A valley approach includes the floor of the valley, the slopes of the ridges, and the military crests. Control of the military crests on each side of the valley is essential. In a valley approach, the best AA is that which offers the best observation, cross-country trafficability, road net, FofF, concealment and cover, and dispersion, In evaluating the use of deep valley approach, the possible intensification of nuclear effects and resulting greater casualties on the valley floor are considered. At times, the best avenue is along the slopes of a ridge below the military crests, rather than along the valley floor.

The use of a ridge approach depends upon the width and shape of the ridge, the size and deployment of the units involved, and the distance to the elevation of adjacent ridges. A ridge approach usually has the advantage of good observation; however, there is little protection from enemy fire on the ridge. The best AA on a ridge is often slightly below the topographical crest, with sufficient force on the crest to control it.

(b) Air Avenues of Approach. An AAA is a route which provides a suitable path for a particular number of aircraft to reach a LZ. The aviation officer or the aviation mission commander assists in evaluating the effect of density altitude, wind, turbulence, and visibility on selected AAAs. In selecting AAAs, the following factors are considered:

- Sufficient air space.

- Concealment from ground observation.

° Eaaily recognized terrain features.

°Length of flight paths.

1 Sufficient air space is required for rapid movement of the aircraft to the LZS. FS requirements involving artillery and tactical air support may restrict the availability of air space. Consideration is given to gun-target lines and to restrictive fire plans that are in effect during the air movement phase. The size of the air assault force involved in the operation also is considered; however, no paramsters are given as to width concerning AAA. Depending on the flight formation, a large number of helicopters are flown over a relatively narrow AAA. Another consideration in relation to adequate air space is the desirability of having multiple flight routes available. Generally, in situations with concentrated enemy forces along the LOC, multiple flight routes from the pickup zone to the objective area and back are desirable.

2 Heavily forested and swamp areas provide good routes and concealment from ground level because ground troops have little opportunity to see and fire on helicopters passing overhead at tree-top level. Low-altitude operations over heavy foliage distort the acoustic wave from aircraft and decrease the distance at which the sound is detected. They also hamper determination of the direction of the noise source by ground observers. AAAs are in defi lade with respect to enemy AD radar and weapon locations. Ridge lines are crossed as infrequently as possible to reduce exposure time to radar detection. Steep defiles or canyons are avoided, especially when there ie an appreciable amount of surface wind that can cause momentary loss of aircraft control because of downdrafts.

3 Navigation at low altitudes is extremely difficult. The presence of easily recognized terrain features, such as rivers or roads, significantly improves the pilot's abil ity to navigate by reference to ground features. Terrain corridors are usually desirable because they afford both ease of navigation and defilade. Linear features that parallel the direction of flight are the most valuable in assisting navigation.

4 In the interest of minimizing the exposure of aircraft enroute to the objective area, the shortest possible flight paths that afford sufficient air space, concealment from ground observation, and easily recognized terrain features are usually preferred. However, longer flight paths are selected for purposes of deception.

(6) Combat Service Support Aspects. The analyses of the facts and subconclusions developed in the preceding parts of the analysis are used as a basis for further studies of the effects of CSS activities on friendly and enemy units. This paragraph determines the effects of the characteristics of the battlefield area on CSS that influence the selection of a course of action by either force.

In studying the influence of the area, consideration is given to effects cm matters such as availability of adequate routes for LOC, facilities for maintenance and storage, construction resources, public health situation, required shelter for administrative facilities, availability of labor, maintenance of discipline, law and order, and control of refugees.

4. EFFECTS OF CHARACTERISTICS OF THE AREA. This paragraph contains the conclusions reached on the basis of the facts and subconclusions previously developed. The effects of the characteristics of the AO on each significant course of action which the enemy is physically oapable of adopting and which, if adopted, could adversely affect the accomplishment of our mission are discussed. Usually, the discussion includes effects on the enemy's ability to defend or attack. It also includes, as appropriate, the effects on the enemy's ability to delay; to use reserves, amphibious or airborne forces, nuclear fires, guerrilla forces, chemical and biological agents, cover and deception, sensor devices; or to conduct special operations and support the enemy's forces administratively. The discussion of the effects on our courses of action is limited to those required for the accomplishment of the mission.

(CLASSIFICATION)

opy no 2 of copies
2d Mech Div
ELLY (8831)
21503S July 19
582

ANALYSIS OF AREA OF OPERATIONS NO 6
eference: Map, series CSM 01, Westland, sheet 1 (Ebel), edition 1974, 1:50,000

. PURPOSE AND LIMITING CONSIDERATIONS

a. Purpose. To analyze and evaluate the area east of Cartersberg (9297) from the general area of verlook Ridge (9406) south to the Erie Canal within the division zone.

b. Mission. Division attacks 140900 July, secures high ground from Hill 322 (1394) to Hill 305 (0490) o deny the enemy a bridgehead, and prepares to cross the Erie Canal and continue the attack to the south.

:. GENERAL DESCRIPTION OF THE AREA

a. Climate or Weather Conditions.

(1) Climate, Annex A (climatic summary).

(2) Weather, Weather forecast, 12-16 July.

(a) Precipitation. None predicted.

(b) Fog. None predicted.

(c) Temperature. Range from 70° to 86°F.

(d) Wind. Surface winds from north, 9 to 17 knots per hour.

(e) Cloudiness. None predicted.

(f) Atmospheric pressure. Average about 980 millibars.

(g) Moon. New moon, 25 July.

(h) Light data.

Date	BMNT	BMCT	EECT	EENT	Moonrise	Moonset
13 July	0232	0440	1933	2138	2024	0608
14 July	0233	0442	1932	2138	2050	0714
15 July	0234	0444	1931	2137	2114	0806
16 July	0235	0446	1930	2137	2137	0901

b. Terrain.

(1) Relief and drainage systems. Annex B (Relief Overlay), Annex C (Drainage Overlay), and Annex D (Slope Overlay). Area is drained by the Maine River on the west and southwest and the South River on the northeast. The northwest to southeast ridge running from Hill 351 (9807) to Albany (3960) generally bisects the area. The major spurs of this ridge run generally east and west. The terrain is generally rolling with a series of sharply, rising table lands. The Maine and South Rivers and the Erie Canal are unfordable. The Maine River south of Cartersberg averages about 30 meters in width and 2 meters in depth. The South River averages about 15 meters in width and about 2 meters in depth. The Erie Canal has steep banks and averages about 3 meters in depth and is about 17 to 21 meters in width at the top of the banks. All other rivers and streams are fordable, varying in width from about 1 to 7 meters, with an average depth of 40 centimeters.

(2) Vegetation. Annex E (Vegetation Overlay) and Annex F (Vegetation Impeding Movement Overlay). Vegetation consists of growing crops, vineyards, pasturelands, orchards, and wooded areas. Hay, wheat, and vegetables are the main crops. Most crops are completely cut by the end of September. Wheat is grown mostly on open-topped tablelands. Vineyards are generally terraced and on the slopes of hills. Most woods in the

(CLASSIFICATION)

Figure A-25. Example and explanation of analysis of the AO.

C I ass if i cat ion is centered at the top and bottom of each page,

Copy number assignad by issuing headquarters. Official designation of unit. Physical I ocat ion of command post by coordinates, state or county.

Date-time roup when the analysis is signed followed by the message reference number (example: SB2) used when the analy sis is distributed outside the adquarters for the purpose of acknowledgment in the clear. All appended material analysis having the suns distribution bears the sane reference number.

The title line identifies the analyses by number (consecutive throughout the calendar year).

Reference I ist maps, charts, or other documents requ i red to understand the analy s is. References to maps inc I ude the map series number (country or geograph ic area, if required), sheet number (and name, if required, edition and scale (if required).

Paragraph 1a states the exact I imi ts of the area being studied.

Paragraph 1b states the mission and any other I imi t ing considerat ions such as t ime limitations, the commander's plan of action, and enemy capabilities.

Paragraph 2 is listing of pertinent facts for use as a basis for the succeeding paragraphs.

Paragraph 2a lists or refers to other docunments containing (for the period under study) meteorlogical conditions to, include precipitation, fog, cloud conditions, temperature, relative humidity, surface winds, effective winds (or winds aloft), atmospheric pressure, I ight data to inc lude moon phases, moonrise and moonset, and other geodetic data as appropriate. When appropriate, include magnetic phenomena.

Paragraph 2a(2) I ists data to be considered by aviation units. It is used in calculating aircraft performance and altimeter setting. Light data are always given, as they are necessary for the set ect ion of courses of action. The BMNT and the EENT are the be inning and end, respectively, of enough I ight for limited visibi I ity. The BMCT and the EECT are the beginning and end, respectively of adequate light for large scale operat ions.

Paragraph 2b(l) describes conf igurat ion of the ground, including slopes, for personnel and vehicles and critical relief for equipmnt dependent on configuration and conditions of streams, including depth, slope, and condition of banks and bottom, and location of crossing sites. Named localities are located by grid coordinates the first time they appear in the anal ysis. Grid coordinates are repeated only if requ i red for ease of reference.

Paragraph 2b(l) also makes maximum use of special colored maps or overlays. Under each characteristic include facts to assist in subsequent determination of the effects of the character ist i c on the use of nuc l ear weapons, chemical agents, and important devices and equipment used implement ing courses of action (do not include here the interpretation of these effect on friendly or enemy possible courses of action).

Paragraph 2b(2) indicates wooded areas, including type, location, size, and shape of trees, diameter of trunks, density, crown cover, and undergrowth include types of natural and cultivated vegatation of norwooded areas.

(CLASSIFICATION)

area are deciduous trees about 25 centimeters in diameter and approximately 10 to 12 meters apart. Underbrush has been cleared throughout the area. Logging operations throughout the forest in vicinity of 9306 have thinned the tree stand to an average density of 90 trees per hectare. Roads and streambanks are generally bordered with trees. Small, scattered patches of trees are found in the lowland plains. Wooded areas restrict, but do not preclude, the employment of armor.

(3) Surface materials. Annex G (Soils Overlays). Surface in most of the area consists of thick clay-like soil on a hard limestone or limey shale base. Above 200 meters elevation, with but few exceptions, the soil is firm and capable of supporting heavy wheeled and tracked vehicles even where under cultivation. The rains do not seriously affect trafficability at this time of year. The soil is generally wet in stream bottoms and in the lowlands below 200 meters elevation. While capable of supporting light tracked or wheeled vehicles, the soil becomes spongy and boggy where the turf has been destroyed.

(4) Artificial features. Annex H (Built-up Areas and LOC Overlay). A double-track railroad crosses the area from Cartersberg to the east. A single-track railroad runs from Nome (9619) to Cartersberg, crossing the Macon saddle (9608). A double-track railroad from the west parallels the south bank of the Erie Canal as far as Dawson (0489). The area is covered with an extensive network of principal and secondary roads. Principal roads radiate from Cartersberg. Roads across Overlook Ridge (9406) from north to south have been improved. National highways are at least 6 meters wide. All bridges on regularly maintained roads are two-way class 50. Villages consist of closely grouped buildings of brick or stone. The enemy has constructed extensive field fortifications and artificial obstacles throughout the area north of Erie Canal. The artificial obstacles consist primarily of minefields and wire and are most extensive in the South River valley and in the general area of Athens (0194) and Auburn (0495).

c. Other Characteristics.

(1) Sociology. The area is generally rural. The farm villages have a present population of from 50 to 100 each. Current population of Cartersberg is estimated at 50,000 and population of Harlow is estimated at 15,000. The population is primarily Caucasian; farming is the principal occupation. Principal crops are wheat, corn, cotton, and grapes.

(2) Economics. Little food and few supplies are available because the enemy has taken food and materials to support the forces. However, some grain crops remain in fields and can be harvested at a later date if protected.

(3) Government. There are civil agencies that are prepared to take over functions of civil government as the country is recaptured.

(4) Psychology. The confiscation of food and supplies and the impressing of civilian labor have made the people extremely hostile toward the enemy. Acts of sabotage occur frequently in the Army's rear area.

3. MILITARY ASPECTS OF THE AREA.

a. Tactical Aspects.

(1) Observation and fire. Annex I (Horizontal Visibility Overlay).

(a) Weather conditions. Annex J (Fog Overlay). Weather permits good air and ground observation. Continued dry weather will increase dust clouds caused by nuclear weapons. Observation will be reduced for a longer period of time in nuclear target areas. Weather favors our, but not enemy's, use of smoke.

(b) Relief. The high ground now held by the enemy affords the enemy excellent observation over approaches into the position. The enemy-held hills west of the Maine River dominate the western part of the area. High ground vicinity Balda's Peak (0004) provides the enemy with excellent observation to the northeast, east, and south. The division objective, with the spur extending north from 1395 to 1004, provides the enemy with excellent observation over all approaches leading directly to it. FofFs within the area for flat-trajectory weapons are generally good but short, except in valley bottoms and from the military crests of open hilltops where they are generally excellent. FofFs on the northern slopes of Overlook Ridge and Hill 351 are excellent and favor enemy defense. FofFs from the northern slopes of the division objective are excellent. Long-range FofFs to the south from Overlook Ridge are good and favor our attack. FofFs for high-angle weapons are good throughout the area.

(CLASSIFICATION)

Figure A-25. Example and explanation of analysis of the AO (continued).

Paragraph *2b(3)* indicates the type and distribution of soils and subsoils in the area and soil trafficability. Include soil content as it affects induced radiation, Use overlay if material is extensive.

Paragraph 2b(4) indicates roads, railroads, bridges, tunnels, mines, towns, industial areas, fortifications, and other features of military significance; include type of construction.

Paragraph 2c (1), (2) consider as pert inent in separate subparagraphs sociology, pol i t ics, economics, psychology, and other character i st ics. Other character i st ics may i nc l ude such items as sc ience, mater iel, transportat i on, manpower, hydrography , etc. Under each of these characteristics considered, list all facts as the pertain to the area of study and which may influence friendly and enemy courses of action. The degree of coverage required of these characteristics varied with the mission and other aspects of the operat ional env iroment. These characteristics influence, to some extent, the decisions of all commanders and become increasingly important as the area of interest of a command increases.

Paragraph 3 anal yzea the facts in the previous paragraph to determine their influence on factors affecting tactical and activities that are considered in the development of specific courses of action. The axtent of the analysis depends on the mission, the means available to accomplish the mission, and the possible means the enemy can use to prevent the accomplishment of the mission. {n considering the factors under each aspect, include the affects, as appropriate, of and on nuclear fires, chemical and enemy biological agents, and important devices and equipment used in implement ing courses of action.

Paragraph 3a considers the effect that the .aerea will have on observation, fire, concealment and obstacles; and deterimines key tarrain features and AAs.

Paragraph 3a(1) indicates graphically or describes the influence of weather, relief, vegetation, surface materials, artifical features, and other pertinent characteristics. Effects of and on nuclear fires, chemical agents, and so forth are included as are any marked effects on surveillance devices equipment based on LOS and fire delivery means. Effects on fire include effects on delivery means, FofFs and effectiveness of fires. Observation and fire are of concern to CSS units as they influence rear area security.

(CLASSIFICATION)

(c) Vegetation. The National Forest from 0306 to 0597 severely restricts observation and FofFs in the eastern part of the area. Within all wooded areas FofFs for flat-trajectory weapons are restricted to forest trails and roads. Fields and tree blowdown in woods, caused by nuclear weapons, may restrict FofFs within woods. Wheat fields severely restrict ground level observation at this time of the year. Forest fire smoke clouds may reduce observation throughout the area.

(d) Artificial features. Church steeples in the numerous villages afford excellent observation points. Villages and farm buildings will limit FofFs for flat-trajectory weapons.

(2) Concealment and cover.

(a) Relief. The rolling nature of the terrain affords some degree of concealment and cover from ground observation. Concealment and cover are poor on the northern slopes of Overlook Ridge and Hill 351. On the southern slopes of Overlook Ridge, concealment and cover are good. The rolling nature of the terrain and numerous folds in the ground will reduce thermal affects of nuclear bursts.

(b) Vegetation. Annex K (Canopy Closure Overlay). National Forest offers excellent concealment and cover for large units. Woods throughout the area afford excellent concealment and protection from thermal effects because of the thick deciduous trees being in full leaf. Wheatfields also afford some degre of concealment.

(c) Artificial features. Buildings in the area offer cover from small arms fire and shell fragments, but do not protect from blast by any significant degree.

(3) Obstacles. Annex L (Combined Obstacles Overlay).

(a) Relief. Terrain favors enemy use of persistent chemicals in the valley forward of the present position. Drainage system consists of the Maine and South Rivers.

(b) Vegetation. Woods, especially the National Forest, will restrict the cross-country mobility of all vehicles, including tracklaying vehicles. They will become severe obstacles in the event of blowdown by blast or if set afire. Cultivated areas will limit wheeled vehicles. Terraced vineyards on the south slopes of Overlook Ridge, Baird's Peak, and the plateau at 9400 northeast of Cartersberg will restrict the movements of tanks and heavy vehicles to road and trails in those areas.

(c) Surface materials. Annex M (Weather Effects on Cross Country Movement Overlay). The soil is generally wet in areas below 299 meters elevation. This will magnify the cratering effects of subsurface nuclear bursts in these locations. While capable of supporting light tracked or wheeled vehicles, the soil becomes spongy and boggy where the turf has been destroyed. Soil composition does not favor the production of high intensities or radio activity.

(d) Artificial features. The enemy has constructed extensive artificial obstacles consisting of minefields and wire, particularly on the east flank and north of Hill 305 (0490). This will hinder movements and limit use of certain AAs in these areas. Buildings and villages do not present significant obstacles even if destroyed by blast, except for the suburbs of Cartersberg on the east bank of the Maine River.

(4) Key Terrain Features.

(a) Hill 351 (9807) and Overlook Ridge west thereof. These terrain features control the AAs in the western and central parts of our zone. The mission will be seriously jeopardized if these areas are not secured.

(b) Hill 359 (0004). This hill mass dominates the central and eastern AAs. Its seizure is essential to the integrity and security of our forces, and will facilitate fire and maneuver to the south.

(c) Hill 334 (9400). This plateau controls the AAs in the western part of the division zone. It is key terrain if our tactical plans call for either a main attack or a supporting attack in the area.

(d) Hill 306 (9997). This hill provides dominant observation over a wide area in this part of the division zone. Its seizure and control will greatly enhance the security, fire, and maneuver of any our forces attacking in this area.

(CLASSIFICATION)

Figure A-25. Example and explanation of analysis of the AO (continued).

Paragraph 3a(2) on concealment and cover, indicates or describes the influence of weather, relief, vegetation, and artifical features. Effects of and on nuclear fires, surveillance devices, chemical and enemy biological agents, and so forth are included as appropriate. The discussion is oriented not only on protection of own and enemy forces, but also on other operations to include use of guerrillas, infiltration and counter infiltration, deception, CI, armor, and artillery. It is also oriented on site requirement for CSS and tactical installations. Include only marked effects that help in selection of friendly and enemy courses of action.

Paragraph 3a(3) on obstacles indicates graphically or describes all natural and artificial obstacles and the influence of relief, weather, vegetation, surface materials, and artifical features. Effects, as appropriate, of and on nuclear fires, chemical and enemy biological agents, and effects on trafficability and accessibility are included. If of significant influence, the effect of each obstacle on possible friendly and enemy courses of action is indicated. Obstacles and trafficability influence site locations for CSS units.

Paragraph 3a(4) describes key terrain features based on the analysis of observations and fire, concealment and cover, obstacles, and mission. Any locality or area the seizure, retention, or control of which affords a marked advantage of either force is considered. The influence of each key terrain feature listed is discussed briefly. The discussion is oriented toward subsequent development of friendly and enemy courses of action. Key terrain features selected are revised as required by the commander's decision and current situation. Key terrain features may be omitted when the enemy has no capability to secure or control terrain features that will materially affect the accomplishment of the mission.

(CLASSIFICATION)

(e) Hill 326 (1199), This hill dominates favorable terrain leading directly to tha eastarn part of the division object ive.

(f) Hi I Is 305 (0490) and 322 (1394). This terrain system constitutes the division objective. 'he mission cannot beaccompl ishad without securing it. Control of this ridge is also necessary to ontinuat ion of the attack to the south,

(5) Avenues of Approach. Annax N (Avenues of Approach Overlay).

(a) Available to enemy into our position.

1. Axis Hill 351 (9607)-Hill 361 (9709),
2. Axis Hill 339 (9206)-Hill 356 (9310).
3. Axis Hill 230 (0010)-Paris (9811)-Hill 364 (9613).

(b) Available to us into the enemy's position.

1. Axis Hill 356 (9310)-Hill 339 (9206)-Hill 334 (9400)-Hill 306 (9997)-Hill 305 (0490)-r idgs east thereof (Avenue A).

2. Axis Hi II 361 (9709)-Hi I I 351 (9607)-Hi I I 359 (0004)-Auburn (0495)-ridge Hi I I 305 (0490) to Hi I I 322 (1394) (Avenue B).

3. Axis Hill 361 (9709)-Hill 351 (9807)-Hill 359 (0004)-Hi I 271 (0702)-Hill 326 [1199)- Hi II 322 (1394)-ridge west thereof (Avenue C).

4. Axis Hill 280 (0010)-Hill 262 (0803)-Hill 326 (1199)-Hill 322 (1394)-ridge west [hereof (Avenue 9).

b. Combat services Support Aspects.

(1) Personnel. Character istics of the society are such that only unskilled civil ian labor will be available at any time. Employment of civi I ian labor to meet short-term objectives must be balanced careful ly aga inat the long-term needs of harvesting rams in ing crops.

(2) Logistics. Lack of civilian food and SUPPI ias may impose added logistic burdens on our forces. Some pi I ferage can be axpected. Few resources beyond basic natural resources ara avai I able formi I i tary use.

(3) Civil-military operationa. Displacement of civil ians through the impressing of civil ian labor by the enemy and lack of food and supplies will create problems which, if not control lad, can impact on mi I i tary operations. The existence of civil agencies capable of assuming the functions of government will help al aviate the problem. However, these agencies will require guidance.

4. EFFECTS OF CHARACTERISTICS OF THE AREA.

a. Ef feet on Enemy Courses of Action.

(1) Effect on enemy defense.

(a) Tarrain now held by the enemy favors defense in depth from present positions to the division objective. The enemy has excel lent observation over al I Ms, and tha enemy's flanks ara protected by the rivers and canal on the west and artificial obstacles on the asst. The enemy's beet defense areas are the enemy-occupied forward PCS i t ions.

(b) The excel lent weather cond it ions favor enemy defense and permi t tha enemy to use supporting firea with maximum effectiveness.

(2) Effects on enemy attack.

(a) The enemy's beat *M is the* axis Hill 260 (0100) -Par is (9811)-Hi I I 364 (9613),

(b) Weather cond it ions are such that the enemy will not be able to maneuver toward our poe it ions without being observed except during tha hours of darkness. Tha lack of precipitat ion favors cross-country mobility.

(CLASSIFICATION)

Figure A-25. Example and explanation of analysis of the AO (continued).

Paragraph 3a(5) describes the AAs that are developed from all the previous analyses of the tactical aspects. Such development does not consider the disposition of the enemy forces. An AA must afford some facility of movement and room for adequate dispersion for a force large enough to have significant effect on the outcome of the operation. When either opposing force has available and adequate number of aircraft that can be used to deploy troops and equipment forward to the battle area and significantly affect the accomplishment of the mission, AAAs are listed. If terrain and weather conditions do not significantly influence choice of flight paths, then AAAs are not listed. Enemy AAs are listed first, followed by a list of AAs into the enemy battle area. When the opposing forces are not in contact, or when only security forces are in contact, AAs to the battle area for both forces are listed. Each listing of an AA is accomplished by a brief discussion to provide a basis for subsequent development of possible courses of action by either force. For CSS units, the discussion of AAs is based on rear area security requirements.

Paragraph 3b analyzes the facts listed in paragraph 2, and the subconclusions developed under tactical aspects. Indicate those facts and subconclusions that significantly affect CSS activities influencing choices of possible courses of action by either force or by requiring special activities to ensure adequate support. Omit any activity that is not significantly influenced.

Paragraph 3b(1) addresses personnel. Personnel management is of particular importance when weather and terrain conditions are severe, when the AO has a significant population and potential labor forces, and when political and economic conditions are unsettled.

Paragraph 3b(2) covers logistics. Logistics is of particular importance when weather and terrain conditions are severe, when the AO imposes additional logistic requirements and has significant resources of military value, and when political and economic conditions are unsettled. Coverage is particularly detailed for those commands accomplishing their mission by logistic support of other units.

Paragraph 3b(3) discusses civil-military operations. Civil-military operations are of particular importance in cold war, limited war, occupation operations, and when extensive civil affairs responsibilities have been assigned to the command. it is particularly important to tactical units when the numbers of civilians in the area present control problems and restrict use of fire power. Coverage is detailed for those commands with extensive civil affairs responsibilities.

Paragraph 4 contains the conclusions developed in the previous paragraphs. The conclusions are stated in terms of effects on the general courses of action available to both forces.

Paragraph 4a(1)(a) lists in turn, each significant possible enemy course of action, such as attack; defense; withdrawal; use of air, armor, nuclear fires, chemical agents, guerrillas, etc. Each listed course of action (using separate subparagraphs) is accomplished by a discussion, to indicate the characteristics of the area favoring the courses of action. For attack courses of action, indicate the best AA . For defense courses of action, indicate the best defense areas and, if appropriate, the best AA leading to the defense areas.

(CLASSIFICATION)

(3) Effect on enemy air,

(a) Weather and terrain favor enemy employment of air in the division AO.

(b) Terrain favors enemy delivery of nuclear weapons by low-level air attack.

(4) Effect on enemy use of nuclear weapons. Weather cond i t ions are favorable for enemy use of nuclear weapons. Ef fect ive winds do not favor use of fallout. Rol l ing terrain, numerous folds in the ground, and foliage will reduce thermal effects. Obstacles will be created by forest and tree blowdown.

(5) Effect on enemy chemical operations. Weather does not favor enemy use of chemicals. Terrain favors use of persistent chemicals in the valley forward of the enemy's present defensive positions.

b. Effect on Own Courses of Action.

(1) The best natural AA into the enemy area is axis Hill 280 (0010)-Hill 232 (0803)-Hill 326 (1199)-Hill 322 (1394)-ridge west thereof (Avenue D). It is blocked by extensive minefields.

(2) The second best AA is axis Hill 361 (97091-Hill 351 (9607)-Hill 359 (0004)-Hill 271 (0702)- Hi l l 326 (1199)-Hi l l 322 (1394)-ridge west thereof (Avenue A).

(3) Weather and terrain do not favor our attack. We will not be able to maneuver toward enemy posit i one without being observed except during the hours of darkness. The lack of precipitation will favor cross-country mobi l ity except below 200 meters elevation. Forest f ires end tree blowdown caused by use of nuclear weapons in Nationel Forest will restrict mobility, observation, and FofFs.

(4) Effect on nuclear weapons. Weather conditions are favorable for the employment of nuclear weapon. The rolling nature of the terrain, numerous folds in the round, and foliage will reduce effects on nuclear bursts. The wooded areas are dry and subject to extensive burning. Soil composition does not favor the production of high intensities of radioactivity. Winds generally favor employment by our forces of radiation effects of fallout from nuclear weapons.

(5) Effect of chemical agents. Weather conditions are favorable for our use of chemicals.

Ackncwledge.

MANN

OFFICIAL:

/s/ Foster
FOSTER
G2

Annex: A-Climatic Summary (omitted)
B-Relief Overlay (omitted)
C-Drainage Overlay (omitted)
D-Slope Overlay (omitted)
E-Vegetation Overlay (omitted)
F-Vegetation Impeding Movement Overlay (omitted)
G-Soils Overlay (omitted
H-Built-up Areas and LOC Overlay (omitted)
I-Horizontal Visibility Overlay (omitted)
J-Fog Overlay (omitted)
K-Canopy Closure Overlay (omitted)
L-Combined Obstacles Overlay (omitted)
M-Weather Effects on Cross Country Movement Overlay (omitted)
N-Avenues of Approach Overlay (omitted)

Distribution: A

(CLASSIFICATION)

Figure A-25. Example and explanation of analysis of the AO (continued).

Paragraph 4b lists, in turn, broad courses of action that will accomplish or facilitate the accomplishment of the mission, such as attack; defense; withdrawal; or use of air, armor, nuclear fires, chemical agents, and guerrillas. Each listed course of action is discussed in the same manner as enemy courses of action.

Acknowledgement instructions included if distributed outside the headquarters. Normally, the word "acknowledge" is sufficient.

The signature block contains the name and rank of the commander and appears on all copies of the analysis if distributed outside the headquarters. If not distributed outside the headquarters, it is signed by the intelligence officer.

Authentication is required only if the analysis has not been signed by the commander and is to be distibuted outside the headquarters.

Annexes are listed by letter and title.

Distribution may refer to a standard distribution list.

PATROL REPORT

A patrol report is a written copy of verbal information reported following a reconnaissance or combat patrol mission. The battalion S2 generally prepares this report. Figure A-26 showa the patrol report format,

(DESIGNATION OF PATROL)

TO: _____

MAPS : _____

A. Size and composition of patrol.

B. Mission.

c. Time of departure.

D. Time of return.

E. Routes out and back.

F. Terrain. (description of the terrain--dry, swampy, jungle, thickly wooded, high brush, rocky, deepness of ravines and draws: condition of bridges as to type, size, and strength; effect on armor and wheeled vehicles).

G. Enemy. (strength, disposition, condition of defense, equipment, weapons, attitude, morale, exact location, movements, and any shift in disposition; time activity was observed, coordinates where activity occurred) .

H. Any map corrections.

1. (Not used.)

J. Miscellaneous information (include aspects of NBC warfare).

K. Results of encounters with enemy (enemy prisoners and disposition; identifications, enemy casualties, captured documents and equipment).

L. Condition of patrol (including disposition of any dead or wounded).

M. Conclusions and recommendations (include to what extent the task was accomplished and recommendations as to patrol equipment and tactics).

Signature Grade or Rank Org Unit of Patrol Leader

Figure A-26. Patrol report format.

N. Additional remarks by interrogator.			
Signature	Grade *or* Rank	Org Unit of Patrol Leader	Time
o. Distribution.			

Figure A-26. Patrol report format (continued).

FRAGMENTARY ORDER

FRAGOs are extracts from more detailed orders or are issued to change previous orders. Like warning orders, these are usually brief oral or written messages. Mission orders are a form of FRAGOs which provide experienced commanders with the essentials of an order (such as a new mission or change to a peavious mission).

FRAGOs do not have a specified format; howaver, to ansure understanding, the OPORD format is useful. A FRAGO is issued orally or in writing. Those elements found in a complete order are omitted when they have not changed, are not essential, or are incomplete at the time of issue. As a general rule, a FRAGO--

- Is addressed to each commandar required to take action.
- Is addressed to higher and adjacent headquarters for information.
- Refers to a previous order. Indicates task organization changes.
- When necessary for clarity, includes a brief outline of the situation that generated the requirement for a FRAGO, to include a statement of the mission, if changed.
- Provides brief and specific instructions without loss of clarity.
- Requests acknowledgment.
- Contains proper classification.

With command approval, FRAGOs are prepared and issued by either coordinating or special staff officers with command approval. Figure A-27 shows an example of a FRAGO.

(CLASSIFICATION)

COPY NO OF COPIES
52d Mech Div
Xrayville (6271), Missouri
141300 5 January 1980

Frag Order YZ55

Reference. OPORD 7
Map, Series V661, Sheet 7061,
Edition 1, Scale 1:50,000

TASK ORGANIZATION. C/52 Avn OPCON 3d Bde
Eff 141400 5 Jan

1. SITUATION. Estimated enemy tank regt delaying advance of 1st Ode
2. MISSION. No change.
3. EXECUTION:
   a. Div continues attack, 3d Bde bypasses 1st Bde in north and attacks in zone to secure division objective. tst Bde becomes reserve, follows 3d Bale. Priority of fires to 3d Bale.
   b. 1-42 FA 0S 3d Bale.
   c. 1-40 FA GSR 1-42 FA.
4. SERVICE SUPPORT. No change.
5. COMMAND AND SIGNAL.
   Tac CP currently at 3067.

ACKNOWLEDGE.

VON STEUBEN
MG

OFFICIAL:

YOUNG
G3

DISTRIBUTION: C

(Classification)

DCOM7308D/FEB83

Figure A-27. Example of a fragmentary order.

MISSION REPORT

The MISREP is used by all air units--strike or attack, reconnaissance or surveillance, airlift, observation, and helicopter--to report the results of all missions and significant sightings along the route of the flight. The MISREP amplifies the inflight report and is normally submitted within 30 minutes after aircraft landing to the tasking agency, the requesting unit or agency, and to other interested organizations. Upon completion of a tactical EW air task or mission, a debriefing is conducted by intelligence personnel, and a MISREP is submitted. Figure A-28 shows the MISREP format.

HEADING

PRECEDENCE

ORIGINATING AGENCY

ACTION ADDRESSEES

INFORMATION ADDRESSEES

SECURITY CLASSIFICATION, CODE WORD, OR NICKNAME

MISREP (Number) DATE-TIME GROUP (GMT)-MONTH-YEAR

BODY

1. AIR TASK OR MISSION NUMBER OR NICKNAME. Reference the request number, FRAGO number, or directive causing initiation of the mission.

2. LOCATION IDENTIFIER. Target number, line number, approved target designator or identifier, or coordinates of the target or sighting being reported.

3. TIME ON TARGET OR TIME OF SIGHTING. Report all times by date-time group, using Zulu time unless otherwise directed.

4. RESULTS AND SIGHTING INFORMATION. This item should contain the pilot or aircrew evaluation of expected results (for example, percent destroyed, number and type destroyed, or percent of coverage) and concise narrative information on significant sightings (for example. unusual or new enemy equipment or concentrations of enemy forces observed to include number, spead, and direction (if applicable)).

5. REMARKS. Includes information not specifically mentioned in above items (for example, enemy defenses encountered, weather data, hostile MIJI attempts, and so forth).

Figure A-28. Mission report format.

ORDER OF BATTLE ANNEX TO THE PERIODIC INTELLIGENCE REPORT

Figure A-29 showa the format for an OB annex to the PERINTREP. Omit items not applicable and renumber the remaining paragraphs.

All remaining entries are completed, and each entry contains an evaluation of the source and information, to include the type of source. Figure A-30 shows a completed sample of the OB annex.

(CLASSIFICATION)

ORDER OF BATTLE

Annex _ (OB) to PERINTREP NO _____ Corps, _____

1. COMPOSITION AND DISPOSITION (see appendix 1, overlay). An overlay is usually attached to present the graphic display of enemy units. The initial subparagraphs always contain information pertaining to organization. Information concerning identification and disposition is listed by mentioning the highest echelons first, followed by subordinate units from left to right or top to bottom, as displayed on the overlay. Related items may be combined and presented in a single entry.

2. STRENGTH. Report information pertaining to enemy personnel, weapons, and equipment losses during the period. Replacement rates and strength figures of individual units may be listed.

3. TACTICS. Report only new tactics and deviations from prescribed tactical doctrine.

4. TRAINING. Report new developments and recent changes in training programs or methods of special training undertaken by the enemy since the initiation of hostilities.

5. LOGISTICS. Report those items which will affect current enemy operations, such as supply status, supply systems, and locations of supply facilities.

6. COMBAT EFFECTIVENESS. Report data on the combat effectiveness of enemy units, either of the entire force or of a major tactical unit., List items indicating morale, esprit, and quality of troops and commanders. Describe the ability of the enemy unit to accomplish its expected mission.

(CLASSIFICATION)

Figure A-29. OB annex to PERINTREP format

(CLASSIFICATION)

7. MISCELLANEOUS DATA. List personalities, unit history, FPO, code numbers and names, 06 changes, and any other item of 06 intelligence that cannot be properly inserted in preceding paragraphs.

Acknowledge.

(SIGNATURE)

Appendixes:
Distribution:
OFFICIAL
(NAME OF G2)

Figure A-29. OB annex to PERINTREP format (continued).

Annex B (OB) to PERINTREP 29, 3 Corps, 201800 August 1985

ORDER OF BATTLE

1. COMPOSITION AND DISPOSITION (see appendix 1 overlay).

a. All EPW captured during period are from the enemy 2d Combined Arms Army. Unit identification include--(C-l)

17 MRD	30 MRD	32 MRD
283 MRR	141 MRR	132d Med Tk Regt
290 MRR	142 MRR	
	130 Tk Regt	
	130 Recon Bn	

COMMENT. 32 MRD accepted as being organic to 2d CAA. 52 Tk Div previously accepted, completing organization of 2d CAA.

b. Two large missile-type weapons mounted on large amphibious armored carriers and several smaller vehicles identified in position vicinity MP 420513. (8-2) .

COMMENT. Probably elements of Free Rocket Regt, 2d CAA, previously unlocated.

c. Captured enemy field order reveals plan to attach 40 Tk Div to 2d CAA effective 22 Aug. (B-l).

COMMENT. EPW previously reported 40th Tk Div moving to reinforce 2d CAA. Enemy main effort probably planned for this area.

2. STRENGTH.

Enemy losses reported during period:

	EPW	KIA	ARTY	ARMOR	AIR	VEH
16 MRD	37	302	2	4	1	21
30 MRD	16	52	8	1	- - -	16
32 MRD	8	12	---	---	---	4
Total 111 US Corps Sector	61	366	10	5	1	41

COMMENT. The marked increase in personnel losses during the period have been sustained primarily by enemy combat patrols. Aircraft loss was HI, observation helicopter, equipped with aeronautics radar. Overall strength of 2d CAA is generally not affected.

(CLASSIFICATION)

Figure A-30. Sample OB annex.

(CLASSIFICATION)

3. TACTICS.

a. EPW from 16 MRD and 30 MRD state they have been instructed, in the event their units are cut off, to continue fighting as guerilla units or in small groups, live off the land, and destroy as much US Army property as possible before gradually infiltrating back to friendly lines. (C-6) .

COMMENT. Intensive guerrilla activity in our rear aress can be expected if elements of these units are cut off.

b. Enemy documents captured 07 Aug included a training pamphlet for battalion, company, and platoon commanders, written by GD Griboyedov entitled "Tanks Out Front,"' (appendix 3). It advocates tactics permitting US patrols and advancing forces to pass through aggressor lines. A coordinated tank-infantry attack is then made on open flanks and rear elements with tanks continuing momentum of attack to destroy remaining US forces. (B-2) .

COMMENT. Considering enemy doctrine that tanks are the decisive arm, the above tactic is possible, particular y in review of reports of probable employment of 40 Tk Div (para 1 .

4. TRAINING.

a. Reference paragraph 3b.

b. Indications of enemy concern for communications security (COMSEC) is noted in document captured from 2d CAA dated 10 Aug, directing all subordinate units to immediately initiate intensive training in radio security and communications procedures. (B-2) .

COMMENT. MI units confirm enemy lack of radio discipline and states that security violations increase during reinforcement and relief operations. Numerous enemy security violations have been noted since 17 Aug, further substantiating reinforcement or relief of 2d CAA units.

5. LOGISTICS.

a. EPW state enemy supply personnel have recently contacted local merchants, farmers, and fishermen for supplies of most class I items. (C-6) .

(CLASSIFICATION)

Figure A-30. Sample OB annex (continued).

(CLASSIFICATION)

COMMENT: Enemy either has critical shortage of class I items or has a bottleneck in the supply system requiring local procurement of these items.

b. Air and ground reconnaissance patrols have reported enemy stockpiling large quantities of supplies and equipment in rear areas of frontline divisions. (B-2) .

COMMENT. Not normal supply procedures. Significance as yet undetermined. Would indicate enemy may be planning major offensive soon.

6. COMBAT EFFECTIVENESS.

a. EPW from 16 MRD and 30 MRD state morale is high but senior officers are disgruntled because their units always receive difficult missions while the 32 MRD and 56 Tk Div have, until recently, been assigned lass hazardous missions. (F-6) .

COMMENT. Analysis of unit history and recent operations of enemy 2d CAA indicates it has usually been highly successful in combat. This, and the fact that 2d CAA has always had fine commanders, would account for high morale in units. This is first indication of dissatisfaction among officer personnel. Report seems cogent, however, since 32 Mech Div has not baen engaged in combat with US Forces in this campaign.

b. EPW reports 30 MRD to be redesignated 30 "Fusilier" Mech Div for superior combat record. (F-6) .

COMMENT. III US Corps rates combat effectiveness of 30 MRD from excellent to outstanding in comparison to other enemy divisions in same sector. 30 MRD casualties have been comparatively small; no deserters have been apprehended and its operations have been executed with determination.

7. MISCELLANEOUS DATA.

a. Personalities identified by EPW: (c-l).

CG, 40th Tk Div	GD GRIBOYEDOV, Semyon P. (Ref 3b)
CO, 282 MRR	Col CARDUCCI, Gherardo S.
CO, 283 MRR	Col UNDSET, Bjornstjerna (Acting CO)
CO, 130 Med Tk Regt	Col STEENWYK, Martin J.
CO, 132 Med Tk Regt	Cot MATTEZ, Mario

(CLASSIFICATION)

Figure A-30. Sample OB annex (continued).

(CLASSIFICATION)

COMMENT. Confirms previously obtained information.

b. Unit history. Officer EPW stated that unit (32 MRR) trained extensively in special tactics for assault of river lines. (F-6) .

COMMENT. Special training received by 32 MRD should increase its overall effectiveness when employed in river-crossing operations. No evidence of other units so trained.

c. Field post numbers: Captured document reveals enemy FPN being used as identification symbols on documents and messages. First two and last three digits are transposed. FPN of 46 MRD will appear as 75031 instead of 31750. (B-1) .

COMMENT. Enemy has employed this system previously as a security measure. Expect this system of transposing digits will occur in different patterns during future operations.

Acknowledge.

LEE
LTG

Appendixes: l--Enemy Disp Overlay
2--Enemy Army Organization Chart
3--Enemy Training Pamphlet

Distribution: Same as PERINTREP 29

OFFICIAL

GRANT
G2

(CLASSIFICATION)

Figure A-30. Sample OB annex (continued).

STANDARD COLLECTION ASSET REQUEST FORMAT

The standard collection asset request format (SCARF) is used for intelligence requirements tasking and for requesting information from higher or adjacent headquarters. At corps and division, intelligence requirements tasking is directed toward Ml commanders and commanders of other elements of the combat force capable of collecting the information.

Intelligence requirements tasking provides the selected unit with a specific requirement, but not with specific instructions for carrying out the mission. The SCARF specifies--

- The information needed.
- Where to look for the movers, shooters, sitters, and emitters.
- When to look.
- When the information is needed.
- What to look with, in some cases.

Figure A-31 showa the SCARF format.

A. Requester number.

B. Originator priority.

C. Activity or target type (area emitter and size (point, area, or unit)).

D. BE number, ELINT notation or case.

E. Location (if known or last known).

F. Ouration--

- Start date-time.
- Frequency.
- Stop date-time.
- Latest acceptable date-time for information utility.

G. Location accuracy--

- Required.
- Acceptable.

H. PIR and information desired.

I. Justification.

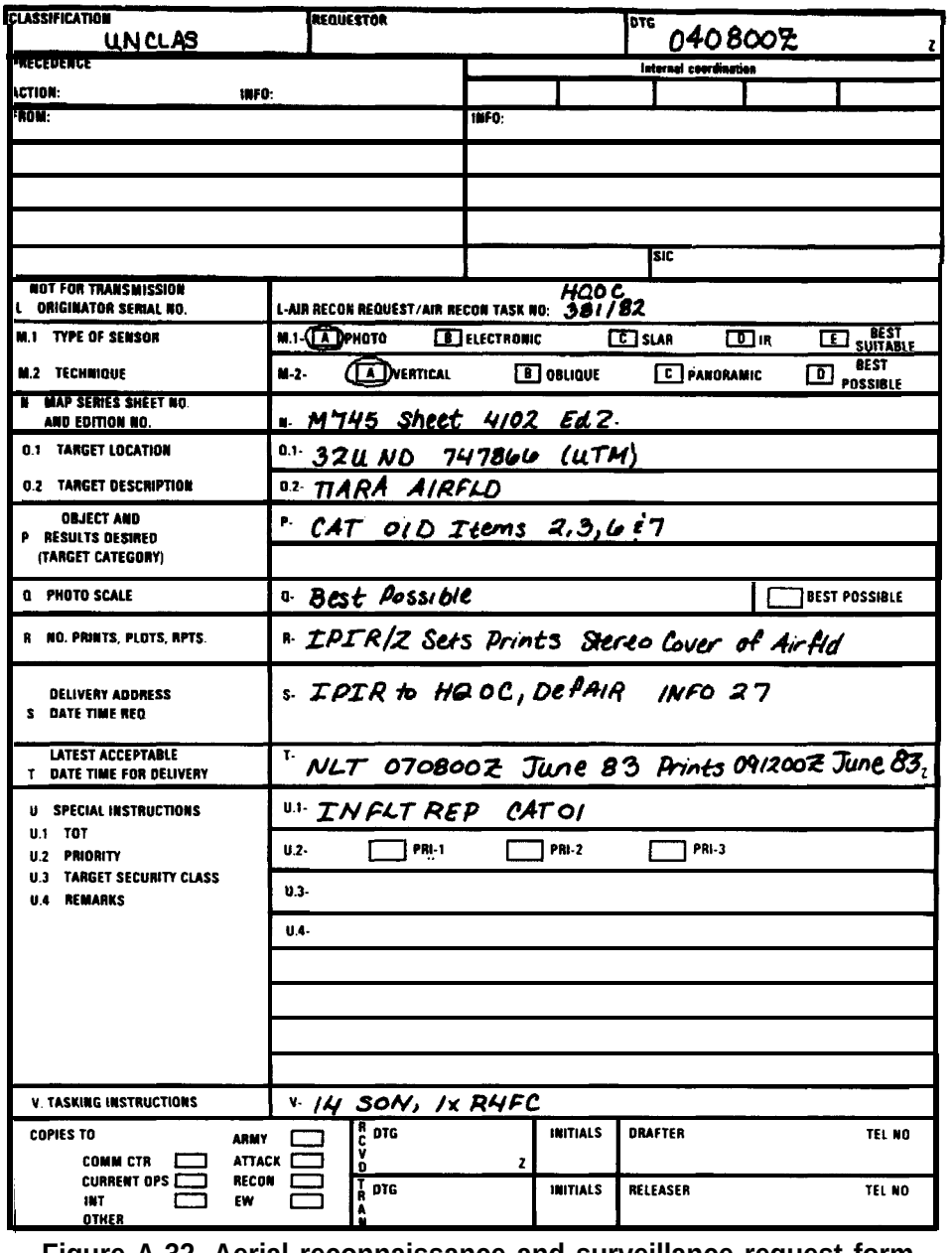
J. Remarks (to include disciplines and collectors recommended).

Figure A-31. SCARF basic format.

AERIAL RECONNAISSANCE AND SURVEILLANCE REQUEST

The aerial R&S request is used to request a tactical air reconnaissance or surveillance mission. The form states requirements, identifies needs, and, occasionally, specifies the actual air asset to perform the mission.

Any echelon initiates the request. It is used for both immediate and preplanned mission requirements. The requester oompletes section I of the request for each specific mission. Normally, these requests are transmitted by electrical means. The headquarters receiving the request adds information required to val idate or complete the request. Figure A-32 shows the aerial R&S request form. This format is the same as the format used for joint service operations.



CLASSIFICATION: UNCLAS	REQUESTOR:	DTG: 040800Z
PRECEDENCE		Internal coordination
ACTION: INFO:		
FROM:	INFO:	
		SIC

NOT FOR TRANSMISSION L ORIGINATOR SERIAL NO.	L-AIR RECON REQUEST/AIR RECON TASK NO: HQOC 381/82
M.1 TYPE OF SENSOR	M.1- (A) PHOTO [B] ELECTRONIC [C] SLAR [D] IR [E] BEST SUITABLE
M.2 TECHNIQUE	M-2- (A) VERTICAL [B] OBLIQUE [C] PANORAMIC [D] BEST POSSIBLE
N MAP SERIES SHEET NO. AND EDITION NO.	N- M745 Sheet 4102 Ed 2.
O.1 TARGET LOCATION	O.1- 32U ND 747866 (UTM)
O.2 TARGET DESCRIPTION	O.2- TIARA AIRFLD
OBJECT AND P RESULTS DESIRED (TARGET CATEGORY)	P- CAT 01D Items 2,3,6 & 7
Q PHOTO SCALE	Q- Best Possible [ ] BEST POSSIBLE
R NO. PRINTS, PLOTS, RPTS.	R- IPIR/Z Sets Prints Stereo Cover of Airfld
DELIVERY ADDRESS S DATE TIME REQ	S- IPIR to HQ OC, DepAIR INFO 27
LATEST ACCEPTABLE T DATE TIME FOR DELIVERY	T- NLT 070800Z June 83 Prints 091200Z June 83
U SPECIAL INSTRUCTIONS U.1 TOT U.2 PRIORITY U.3 TARGET SECURITY CLASS U.4 REMARKS	U.1- INFLT REP CAT 01 U.2- [ ] PRI-1 [ ] PRI-2 [ ] PRI-3 U.3- U.4-
V. TASKING INSTRUCTIONS	V- 14 SON, 1x R4FC

COPIES TO: COMM CTR [ ] CURRENT OPS [ ] INT [ ] OTHER; ARMY [ ] ATTACK [ ] RECON [ ] EW [ ]	RCVD DTG Z	INITIALS	DRAFTER	TEL NO
	TRAN DTG	INITIALS	RELEASER	TEL NO

Figure A-32. Aerial reconnaissance and surveillance request form.

Figure A-33 shows an air reconnaissance request and task format that is keyed to letter designators of message elements. An explanation of each of these letter designators follows in Figure A-34.

Air Reconnaissance Task (Format-not transmitted)		AIR RECON TASK (Example message)	
L.	Originators request and task number.	L.	HQOC 468/82.
M.	Type of recon.	M.	PHOTOGRAPHIC, VERTICAL.
N.	Map series, sheet no and edition.	N.	M745 SHEET 4102 EDITION 2.
o.	Location and description of target.	o.	32U ND 747866 (UTM) TIARA AIRFIELD
P.	Purpose of request and reporting codes.	P.	CAT OID ITEMS 2, 3, 6, 7.
Q.	Photo scale or limits.	Q.	BEST POSSIBLE.
R.	Products required.	R.	IPIR/2SETS PRINTS PROVIDING STEREO COVER OF TIARA AIRFIELD.
s.	Delivery address.	s.	IPIR TO HQOC, DEFAIR INFO 27 SO PRINTS HQOC/TGTS-1, DEFAIR/DAFIS.
T.	Date-time limitation.	T.	TOT NOT BEFORE 0706002 JUN 83 BUT NOT LATER THAN 0708002 JUN 83. PRINTS REQUIRED NOT LATER THAN 0912002 JUN 83.
u.	Special instructions.	u.	INFLIGHTREP CAT 01 ITEMS 3,
v.	Tasking and mission data.	v.	14 SON, 1 X R4FC.

Figure A-33. Alr reconnaissance request and task format.

Explanation of letter designators.

L. ORIGINATOR'S REQUEST NUMBER. The originator's request number usually consists of a unit identifier and a sequential numbering system. Commands may assign blocks of numbers to subordinate units to prevent confusion. if necessary to assist the tasking agency, commands also may establish a system of priorities for reconnaissance tasking and promulgate priority designators to be used in the originator's request number.

M. TYPE OF RECONNAISSANCE. Visual, electronic, weather, photographic, and so forth. Additionally, if the requester requires a specific type of sensor, system, or format to be used for some reason (such as a vertical photograph for briefing purposes), it is specified. Such detail generally should be omitted, however, to allow flexibility in planning and tasking.

N, MAP SERIES Z SHEET NUMBER. AND EDITION. Self-explanatory.

O. LOCATION AND DESCRIPTION OF TARGET. The target location or areas to be searched is indicated by the appropriate coordinate reference. The coordinate reference system used (for example, UTM grid, latitude or longitude) is identified clearly. Predetermined search areas or LOC segments can be nominated by relevant designators. A brief description of the target, its name and BE number (where known) should be included.

P. PURPOSE OF REQUEST AND REPORTING CODES. It is most important that tasking agencies and reconnaissance units understand the exact purpose of the request. Where possible, the code statements in appropriate reference books are used to identify the target category, reconnaissance purpose, and items to be reported. Otherwise, a plain language statement of purpose is provided.

Q. PHOTOGRAPHIC SCALE OR LIMITS. The photographic scale or limits should not be specified unless there is a specific reason for doing so; for example, survey photography or imagery is to be used for a particular task that requires it to be at a nominated scale or physical dimension. If the scale is nominated, care must be taken to differentiate whether the scale appl ies to the original film or to the end product requested (item R).

R. PRODUCTS REQUIRED. Specify the reports (RECCEXREP, IPIR, and any other end product) required. If photographs are required, specify quantities and the size or scale desired. Photographs should be requested only when essential and a report will not suffice. Quantities must be kept to an absolute minimum.

S. DELIVERY ADDRESS. State clearly where the report is to be delivered. For reports, nominate both action and information addressees.

Figure A-34. Explanation of letter designators.

T. DATE AND TIME LIMITATIONS. Specify any time constraints on the mission and follow-up actions. In particular, specify the date and time after which the information will no longer be of value. If the task cannot be accomplished by this date, it will be cancel led automatically.

u. SPECiAL INSTRUCTIONS. Give instructions or information not provided elsewhere that will aid in the planning or accomplishing of the mission. This includes control arrangements, communications, security instructions, details of own forces, or other pertinent entries.

v. TASKING AND MISSION DATA. This is completed by the mission tasking agency. It generally details the unit and number and type of aircraft. The mission number for the task is the originator's request number, abbreviated if necessary.

Figure A-34. Explanation of letter designators (continued).

SIGNALS INTELLIGENCE TACTICAL REPORT

The purpose of the SIGINT TACREP is to transmit combat information to fire and maneuver elements. It also is used to transmit technical data to traffic and analysis teams or to the TCAE. It is normally sent by electrical message or by secure FM voice radio means. it is designed to present highly perishable information in a clear, concise, and easy-to-read format. Distribution is made according to local guidance or as directed by higher commands. An annotated format is available in the classified appendix to FM 34-80.

MEACONING, INTRUSION, JAMMING, AND INTERFERENCE REPORT

The MIJI report is used to pass information from operators to their units about actual or suspected enemy attempts to interfere with, jam, or deceive voice, teletypewriter, or MC signals. The report is submitted by the operator whose communications means is affected, through the net control station (in the case of FM voice), to the unit's C-E officer. The C-E off icer coordinates this report with the EW officer, the intelligence off icer and the supporting MI unit.

MIJI reports are transmitted; however, if they are transmitted over nonsecure equipment, reports are encrypted using the brevity list. See FM 34-40 for additional information about MIJI reports and brevity lists. Figure A-35 shows the MIJI report format.

LINE 1 - Type of report _____

LINE 2 - Affected station _____

LINE 3 - Station's location or. grid coordinates _____

LINE 4 - Frequency or channels affected _____

LINE 5 - Type of equipment affected _____

LINE 6 - Type emission or audio characteristics of interference _____

LINE 7 - Strength of interference _____

LINE 8 - Time interference started _____

LINE 9 - Interference effectiveness _____

LINE 10 - Operator's name and rank _____

LINE 11 - Remarks _____

Figure A-35. Meaconlng, intrusion, jamming, and interference report.

ORAL REPORTS

Briefings are oral reports that present information to commanders, staffs, or other designated audiences. The techniques employed are determined by the purpose of the briefing, the desired response, and the role of the briefer. There are four types of military briefings:

- Information briefing.
- Decision briefing.
- Staff briefing.
- Mission briefing.

The two most important briefing formats to intelligence officers and analysts at the tactical level are the information and decision briefings. An explanation of these two briefings follows.

INFORMATION BRIEFING

The information briefing is intended to inform and gain the listener's understanding. The briefing does not include conclusions or recommendations, or require decisions. The briefing deals primarily with facts. The briefer states that the purpose of the briefing is to provide information and that no decision is required. The briefer provides a short introduction to define the subject and to orient the listener and then presents the information. Figure A-36 shows the information briefing format.

DECISION BRIEFING

Decision briefings are intended to obtain an answer or a decision. They are used to present a staff officer's or intelligence analyst's recommended solution resulting from analysis or study of a problem or problem araa. They vary as to formality and detail depending on the level of command and the-decision maker's knowledge of the problem or problem area. In situations where the person receiving the briefing has" prior knowledge of the problem and some information relating to it, the briefing normally is limited to a statement of the problem, essential background information, and a recommended solution. However, the briefer is prepared to present the assumptions, facts, alternative solutions, or reason(s) for choosing the recommended solution, and any coordination required. If the person who is being briefed is unfamiliar with the problem or the facts surrounding it, then a more detailed briefing is necessary. In this case, the briefing includes any assumptions used in analyzing the problem, facts bearing on the problem, discussion of the alternatives, conclusions, and the coordination involved.

1. **INTRODUCTION.**

a. Greeting. Use military courtesy, address the person(s) being briefed, and identify self.

b. Classification. Announce the classification of your briefing.

c. Purpose. Explain the purpose and scope.

d. Procedure. Explain any special procedures such as demonstrations, displays, or tours.

2. BODY.

a. Arrange main ideas in logical sequence.

b. Use visual aids correctly.

c. Plan for effective transitions.

d. Be prepared to answer questions at any time.

3. CLOSE.

a. Ask for questions.

b. Concluding statement.

c. Announce the next briefer, if any.

Figure A-36. Information briefing format.

In the introduction, it is stated that the briefer is seeking a decision. At the conclusion, if the briefer does not receive a decision, the briefer asks for it. The briefer should understand the decision thoroughly. If there is uncertainty, the briefer asks for clarification. In this regard, a precisely worded recommendation that is used as a decision statement, once approved by the commander, assists in eliminating possible ambiguities. Following the briefing, if the executive officer is not present, the briefer informs the next highest ranking officer or the staff secretary of the decision. Figure A-37 shows the decision briefing format.

1. INTRODUCTION,

a. Greeting. Use military courtesy, address persons being briefed, and identify self.

b. Classification. Announce the classification of the briefing,

c. Purpose. State that the purpose of the briefing is to obtain a dec sion and announce the problem statement.

d. Procedure. Explain any special procedures to be used, such as add itional briefers. Omit if not required.

e. Coordination. Indicate what coordination has been accomplished,

2. BODY.

a. Assumptions. Must be valid, relevant, and essential to a solution to the problem. Omit if there are none.

b. Facts Bearing on the Problem. Must be supportable, relevant, and necessary.

c. Discussion. Analyze courses of action. Use smooth transitions between discussions of each course of action.

d. Conclusions. Degree of acceptance or order-of-merit for each course of action.

e. Recommendations. State actions recommended. Must be specific, not a solicitation of opinion.

3. CLOSE.

a. Ask for Questions.

b. Request a Decision.

Figure A-37. Decision briefing format.

APPENDIX B

AUTOMATION SUPPORT TO INTELLIGENCE ANALYSIS

During the past forty years, the battlefield has evolved from a relatively simple environment to one that is increasingly sophisticated in terms of collection systems and communications capabilities. Current collection systems incorporate state-of-the-art components and advanced technology. Deployed using Army-approved doctrine against known enemy capabilities, they exhibit the ability to collect vast amounts of information from a battlefield environment rich in enemy targets. Parallel advances in communications capabilities complement sensor system advances and provide the ability to transmit information faster and more efficiently than at any other time in history.

As the information flow increases, progressively more time is needed to identify, verify, and organize the information needed to produce intelligence. Yet, intelligence production methods and procedures have not kept pace with the advances made in collection systems and communications. Information collected by technologically advanced sensor systems and sent and received over high-speed communications equipment is still processed individually as it is received by manually sorting, recording, and filing it. Clearly, to produce the intelligence the commander needs, when it's needed, these manual processing functions must be updated and expanded.

This appendix describes how current and emerging automated systems support intelligence analysis. It will--

- Describe general computer system configuration and basic tactical military computer system capabilities and limitations.
- Discuss two current tactical semiautomated systems: MICROFIX and Intelligence Data Processing Set.

INTELLIGENCE ANALYSIS SUPPORT

ADP systems support efficient and timely intelligence production. This support upgrades the ability of analysts to deal with the vast amounts of information produced during the course of a battle. These systems are designed to supplement, not replace, existing manual analysis support systems. They provide expanded capabilities during the storage; access, retrieval , and manipulation; recording and record-keeping; and dissemination portions of the intelligence production process. These capabilities provide the analyst with substantially more time to devote to intelligence analysis.

Using ADP systems, the analyst not only stores more information in less space but the information is consolidated with other information and with previously produced intelligence. With this additional storage capacity, the analyst accesses data bases such as IPB or ground OB data from the same system. Consolidating this data onto one system lets the

analyst quickly and easily retrieve and manipulate the data and information needed to support the intelligence analysis process. With more information to work from, the analyst develops a better picture of the battlefield environment. This reduces risk and uncertainty.

ADP systems also provide the means to access this information quickly and easily. Data is accessed in seconds, rather than minutes or hours. By retrieving various types of information and using the computer capabilities to arrange this information in different patterns, information is manipulated to test previously established hypotheses or to create a new hypotheses based upon new or emerging patterns. Through this process of electronic comparison and contrast, the computer helps the analyst determine unit identifications, strengths, and enemy commanders' intent.

Computer system capabilities is used to facilitate and complement manual methods and procedures. For example, computers are programed to automatically record message header information into a separate file which subsequently is printed and placed in a three-ring binder. This provides a duplicate file that is easy to maintain and keep current and requires a minimum of time and effort. A record of all intelligence messages and products is printed. This establishes a record of all outgoing intel 1 igence products and messages, including a list of all users receiving that message or product. When manual recording is kept to a minimum, it leaves more time for the analyst to develop intelligence.

Another example of a manual system being eased with ADP is recording and storing preprogrammed formats. The computer assists the analyst in preparing a variety of reports, summaries, and other intelligence documents and message formats electronically. Once correctly formatted, previously created lists of addresses and users are selected and automatically printed. If electronic message sending capabilities exist, messages are sent directly from the terminal. This capability significantly reduces the amount of time necessary to prepare, route, and transmit products to users, and the amount of time the intelligence analyst spends preparing and disseminating them.

These tasks are continuous and require time and the ability to assimilate large amounts of data quickly and accurately. The use of ADP enhances the analyst's abil ity to perform these tasks. It is a tool which provides the analyst with the ability to access and use more information and resources than manual processes provide.

COMPUTER SYSTEM CONFIGURATION

Every computer system is composed of hardware and software. Hardware is the actual physical equipment--or components--that make up the total ADP system. Software is a series of commands, recognized by the computer. It tells the computer how to perform a variety of functions.

Typical system hardware consists of a keyboard; central processing unit; storage device (disk drive); display or monitor; and printer. These basic hardware components access files, input new information, manipulate data and information, and display or print data of information which the analyst selects to perform analysis and produce intelligence. Figure B-1 shows the basic computer components.

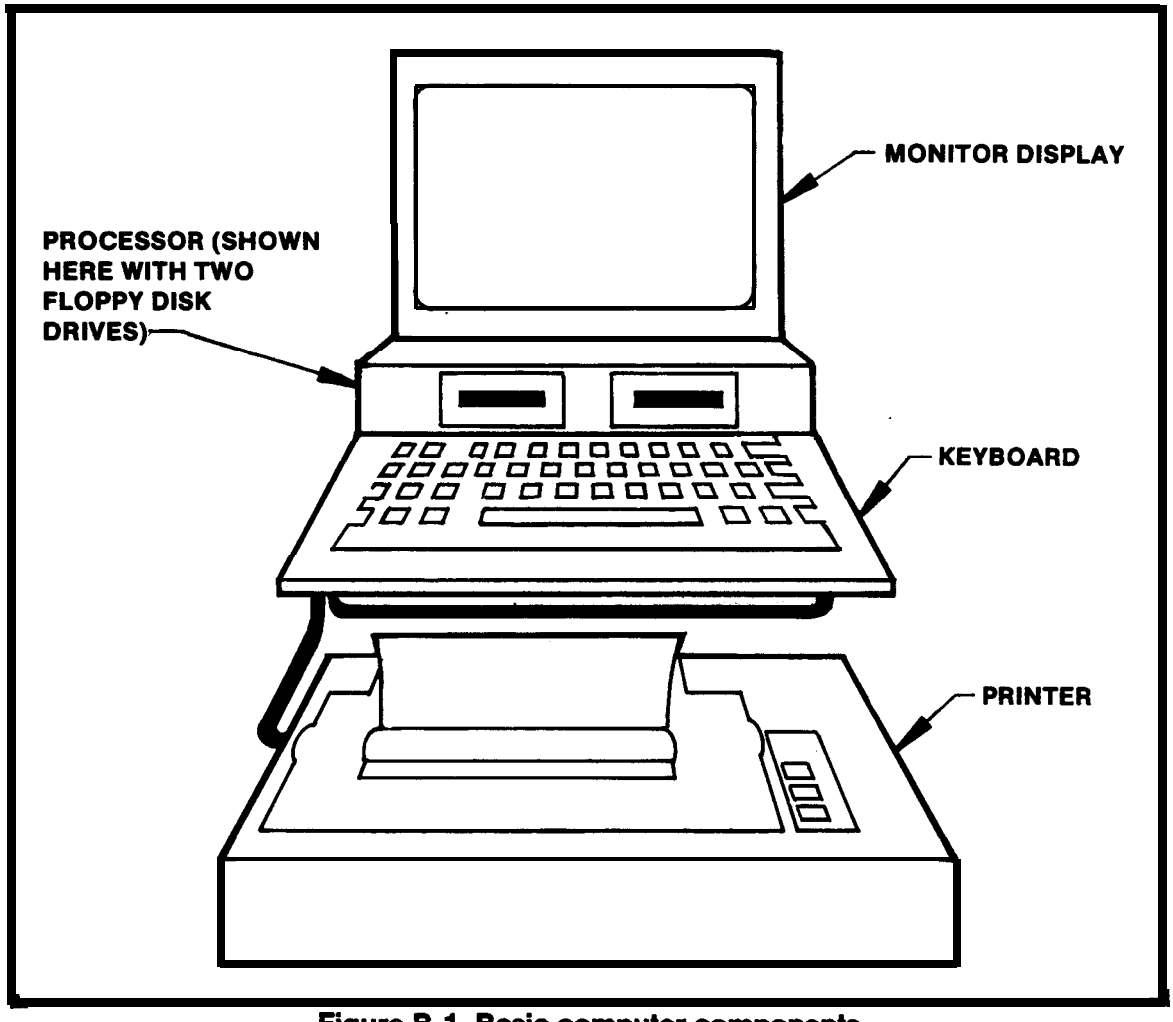


Figure B-1 Basic computer components.

Keyboard. The keyboard serves as the primary input device to the computer. Normally, the keyboard contains the same letters, numbers, and punctuation keys as a standard typewriter. The computer keyboard also contains special function keys which are used to initiate various computer functions.

Processor. The processor is the component that executes the commands from the programs. It controls the flow of information into, within, and out of the computer. It also contains a limited amount of the computer's memory.

Storage Devices. Information is stored inside the processor in special memory locations or in a separate storage device. Examples of storege devices are floppy or removable disks, magnetic tape, large capacity hard cartridge or fixed disks, and cassette tapes, or cartridges. The computer periodically reads these devices during each computing session in order to perform programs selected by the analyst. Conversely at the end of the computing session, data is saved to these devices if it is to be permanently retained. Information solely left displayed on the monitor or in the processor is lost when the system's power is shut off.

Display, The display is a cathode ray tube (CRT) (commonly referred to as a monitor). The monitor displays text, charts, graphs, or maps (depending upon system configuration and capabilities). It is similar to a television screen and is monochromatic or color.

Printer. Printers are similar to high-speed typewriters. Information from the processor is read and the output is printed on computer paper or bond paper. This provides the analyst with a permanent record (hard copy] of the information.

Peripherals

Other components are integrated into the basic ADP system to provide specialized or expanded capabilities. Whether or not components are added to a system depends upon several factors. First, the original system is designed so that it can be expanded. Second, expansion modules, add-on components, or peripherals are compatible with the existing system. Third, software limitations and design constraints are considered. Depending upon these factors, some of the following components are integrated into a tactical ADP system:

- Video disk players (VDPs). VDPS al low map, text, photographs, or any information that can be stored on video disks to be displayed on a monitor.

- Modems and communications networks. This equipment allows information to be passed directly from one computer to another. The modem connects directly to the telephone jack and transmits and receives data through telephone lines. Provides interface between data processing systems over communications lines. Paper tape reader/punch (PTR/P) devices provide the capability to generate and read tactical RATT messages via paper tape.

- Video cassette recorders (VCRs). Identical to VCRs used for home entertainment, some systems have programs that al low a VCR to be connected to the processor for use as a back-up and restore device.

Software

Software provides the instructions, tools, and basic programing required for computer system functions. There are many types of software; however, every system must have an operating system to be able to function.

Operating System Software. This software enables the computer to run applications. This operating system, which also is referred to as a control program, is thought of as a traffic cop. It regulates all actions within the processor and determines when any of the peripherals are activated. Another vital function performed by the operating system is to act as a translator between the users' language (English, German, Spanish) and the computer's language (binary).

Data Base Management Systems (DBMS) Software. DBMS software turns the computer into a high-powered, automated filing cabinet. This data base file is sorted on nearly any variable in the file's structure. The computer also extracts records in the file that match a very exacting criteria, or extract just selected bits of information (fields) about all the records in the file. This allows the analyst to manipulate data in varying ways to get a clearer picture of the battlefield and perhaps identify previously unrecognized patterns.

Word Processing Software. A word processing program turns the computer into a high-powered, automated typewriter. This software gives the analyst the ability to compose briefings, reports, and messages, and to perform editing functions for storage, printing, and display.

Applications Programs. These programs are the actual commands that perform the automated operations the analyst requires. These are written in a DBMS or computer language. Some common languages are BASIC, PASCAL, and FORTRAN.

ADVANTAGES AND DISADVANTAGES

Advantages and disadvantages depend on the system, software, and training. The analyst uses the ADP system to store and manipulate facts or data that, when analyzed, produce intel I igence.

Advantages

In general, for any system, the advantages of automated support to intelligence analysis lie primarily in the areas of information management and dissemination. ADP systems help the analyst disseminate information with speed and increased accuracy.

Speed. ADP support is particularly useful to the analyst because of the speed at which computers can perform calculations and assemble specific data from a large body of information. Given accurate data input, the computer produces a faster, more accurate output than is obtained through human calculation. Stress or pressure do not degrade ADP operations. They carry out prespecified tasks almost indefinitely. A caution about

computers being more accurate than humans working in a purely manual mode. Humans respond almost instantly to questions requiring a judgmental response: "'What are the 10 most significant actions in the last 12 hours?"' The computer cannot make such a response. To a computer, a report about the movement of the independent tank battalion carries the same weight as a report about three wheeled vehicles moving along an unidentified road.

Report Generation. When ADP systems are equipped with word processing capability, the analyst creates reports, messages, summaries, or other intelligence-related documents quickly and easily.

Electronic Communication. If ADP systems are netted, that is, linked together, data is transmitted directly from terminal to terminal. If they are not netted, a messenger sends correctly formatted diskettes, as well as hard copy reports. However, diskettes offer the advantage of being able to be loaded into the receiving person's computer. In any case, copies of the message are produced and then transmitted over established tactical communications channels. In either event, the ability to disseminate intelligence products is substantially improved over more traditional methods of dissemination.

Disadvantages

Understanding the System. Most of the disadvantages of ADP support to intelligence analysis result from a lack of computer literacy or an understanding of specific ADP system limitations and capabilities. Analysts and commanders tend to assign capabilities to the system that it does not possess. This results in an unrealistic view of the support ADP provides to the commander and creates a false reliance on the computer system by the analyst.

Computers perform only those functions they are explicitly told to do. They do not learn from mistakes, nor will they correct improper input. Therefore, the data stored in the computer is only as accurate as the data that is entered. Computers also have a finite capacity to store data. Design parameters establish this capacity. While additional storage capacity is provided by add-on component storage equipment, when maximum storage limits are reached, old data is deleted to make room for new input. Dual record-keeping procedures, both manual and automated, are established and kept in an updated status. If ADP capabilities are interrupted or lost, this ensures that intelligence production continues.

Multi-Processing. Another disadvantage is that some tactical systems cannot input, process, and output data simultaneously. Others only allow access to a shared data base on a one-by-one basis. Therefore, the analyst determines which data is most important and balances input, output, or access functions to best support the mission. This is critical to appropriate and maximum use of the ADP system.

Environment. Computers also are vulnerable to environmental conditions and influences like temperature extremes, weather conditions, power fluctuations, and power outages. Terrain constraints also may affect ADP access, system mobility, or system capabilities.

Temperature extremes, like alternating very hot and very cold weather cause condensation. Condensation inhibits the read and write ability of the system. Extreme temperatures also result in partial or complete loss of previously input data. For example, rain, fog, and high or low humidity cause partial or even complete system failure.

Static electricity also results in partial or complete loss of data. Planned power outages require shutdown of all computer functions immediately before and during the length of the outage. Unplanned power outages or power surges not only shut down computer functions, but also result in varying degrees of hardware or software damage or data loss.

Severe weather conditions, like lightning or dust storms, produce the same effects as unplanned power outages or power surges. Dust in the read and write heads of hard and floppy disk drives result in inaccurate input, output, data loss, or total destruction of disk capability.

Terrain also is a factor in ADP system survivability and use. Each time the system is moved, leveling is required before the system is operational. Crossing rough terrain under highly mobile conditions partially damages or completely destroys the ADP system. Also, while mobile, current systems are inoperative. Data accumulated while the computer system is down or inoperative must be saved and input when circumstances permit. This means that when the system initially returns to an operational status, it does not provide data for irrrnediate analysis until the data base has been updated. If the accumulation of data is such that input requires a substantial amount of time, the analyst finds that manual systems and data bases support the commander's intelligence needs more efficiently.

Many of these disadvantages apply, in whole or in part, to all tactical battlefield electronic and automated systems. When the capabilities and limitations of ADP systems are thoroughly understood, measures are taken to protect the system while making maximum use of ADP support to intelligence analysis. By taking these factors into account, ADP support to intelligence analysis is a viable tool which the analyst uses to give the commander a more complete, accurate, and timely picture of the battlefield.

CURRENT AUTOMATED SUPPORT SYSTEMS

The US Army currently has two systems deployed specifically to support tactical SIGINT and all-source intelligence analysis functions: the MICROFIX and the TCAC. The MICROFIX assists the analyst in fulfilling the commander's need for information and intelligence on the AirLand Battlefield. The TCAC provides a variety of SIGINT and EW asset mission management functions, as well as to assist the analyst. Both of these systems are designed to enhance the analyst's ability to manipulate large quantities of unprocessed or partially processed data. Information is quickly and easily added, deleted, or moved. Historical enemy locations, enemy strengths, equipment, and unit designations, and specific enemy equipment capabilities and limitations are accessed from previously stored data base information. In fact, the analyst accesses data that is limited

only by storage capability, the data bases available for review, and the information or data the analyst elects to input into the system during the course of the battle.

Since the TCAC system is found only in USAREUR and XVIII Airborne Corps, (and is a non-TOE--table of organization and equipment--item) this manual does not address it in detail.

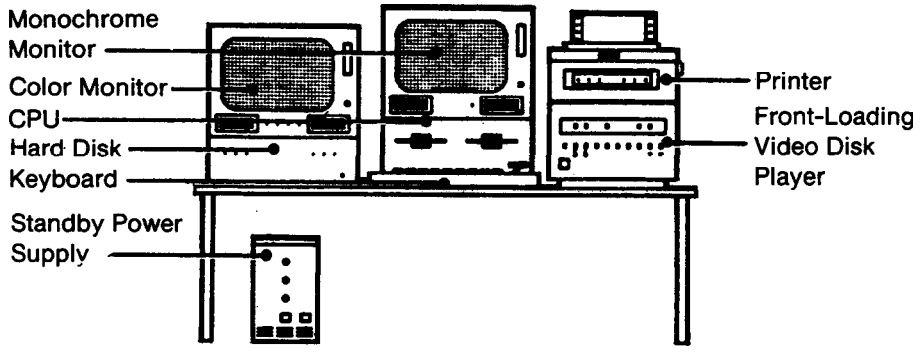
MICROFIX

MICROFIX was introduced into the Army as a training device. The system exists to provide MI soldiers an opportunity to become familiar with computers before future automated systems, such as the all-source analysis system (ASAS), are introduced. The purpose of MICROFIX also is to support the tactical analyst, as OB analyst (96B), SIGINT analyst (98C), counter-SIGINT analyst (97G), CI agent (97B), or a terrain analyst (12 CMF). The MICROFIX gives the analyst the capability to input data into complex data bases. The analyst manipulates this data to provide a source of accurate and frequently updated knowledge about past and present enemy activities. This information assists the analyst in determining enemy courses of action and developing counter-strategy. The MICROFIX system also produces various reports and data files which are generated by the analyst. The system is menu-driven (all the user's options are on the screen at all times) and quite easy to use. Figure B-2 shows the MICROFIX system.

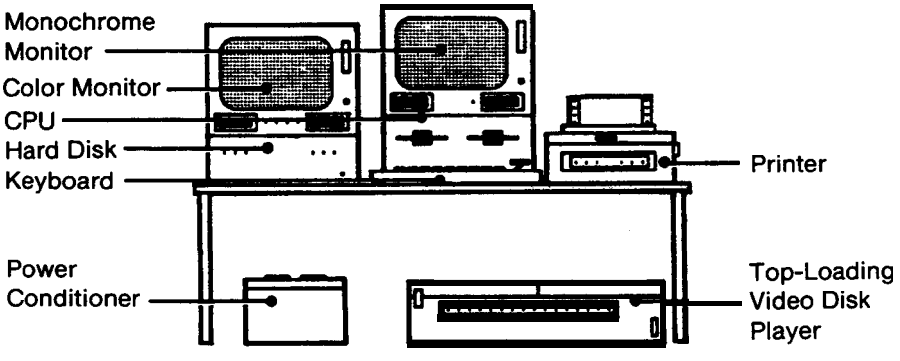
The system is based on the Apple II Pulse Microcomputer and incorporates other off-the-shelf components. TEMPEST engineering provides emission security between components of the system. Expansion cards provide the capability to control a large amount of peripheral equipment in the field environment. Figure B-3 outlines the hardware components of the MICROFIX system.

Figure B-4 shows further details regarding the eight basic components of the MICROFIX system. The MICROFIX is mounted in an AN/TYQ-5 data analysis center or in any shelter, tent, or building the G2 considers appropriate. Since both power boxes, the power conditioner, and the standby power supply, have surge protectors, the system is powered by either commercial power or a filed generator. Both styles of VDP and power box are shown, but only one VDP and one power box comes with each system.

In addition to the eight basic components shown in Figure B-4, two special components are available. The VCR and PTR/P are issued on a 1:3 to 1:4 ratio; one component for every three or four MICROFIX systems. The VCR is used to backup and restore the entire 20 megabyte memory of the hard disk. The PTR/P is used to cut a five or seven band of paper tape. The message is generated in the system's word processor (Wordstar) and, once properly edited, the MICROFIX system cuts the tape. Figure B-5 provides details on these two components.



View with Front-Loading Video Disk Player
and Standby Power Supply



**View with Top-Loading Video Disk Player
and Power Conditioner**

Figure B-2. MICROFIX system.

1. **HARD DISK SYSTEM.** The Corvus 20 megabyte hard disk drive assembly stores and mantains system software and the master data base.

2. **MONOCHROME MONITOR.** The monochrome monitor displays MICROFIX TEXT on a screen in green or black.

3. **COLOR MONITOR.** The amdck color monitor displays color graphic data. This includes video disk maps and military symbology.

4. **PRINTING.** The Apple Dot Matrix Printer operates at 120 characters per second (CPS) and has graphics capability.

5. **VIDEO DISK PLAYER.** The VDP reads photos or map sheets from a laser disk, using the same technology as used on a compact disk player. The photos of the map sheets are displayed on the color monitor.

6. **APPLE II PLUS MICROCOMPUTER.** The microcomputer is capable of controlling a large complement of peripheral equipment while operating in a field environment.

7. **KEYBOARD.** The keyboard assembly uses a full 128 ASCI character set, joystick and enhancer board. This equipment provides upper and lower case letter and number capability, in addition to auto-repeat keying.

8. **POWER BOX.** The older grey power conditioner has eight outlets on its top, assure protector and the capability to work with 110 or 220 volts. The newer green standby power supply has six outlets in the rear panel, a surge protector, a built-in battery pack capable of providing 20-25 minutes of uninterrupted power but works only with 110 volts.

9. **VIDEO CASSETTE RECORDER.** (Not shown in Figure B-2.) The VCR is used to initialize the system (hard disk) and acts as a backup or restore device for the hard disk drive assembly. This expands the potential data base capability of MICRO FIX. The VCR initiatea hard disks and backups which are quicker and easier to use than floppy disks. VCRs are issued with every three to four systems, or one per installation.

10. **PAPER TAPE READER/PUNCH.** (Not shown in Figure B-2.) The paper tape reader/punch (PTR/P) punches a paper tape coPy of messages prepared on the MICROFIX for transmission over tactical RATT systems. It also reads paper tape. PTR/P equipment is issued with every three to four systems, or one per installation.

Figure B-3. MICROFIX hardware components.

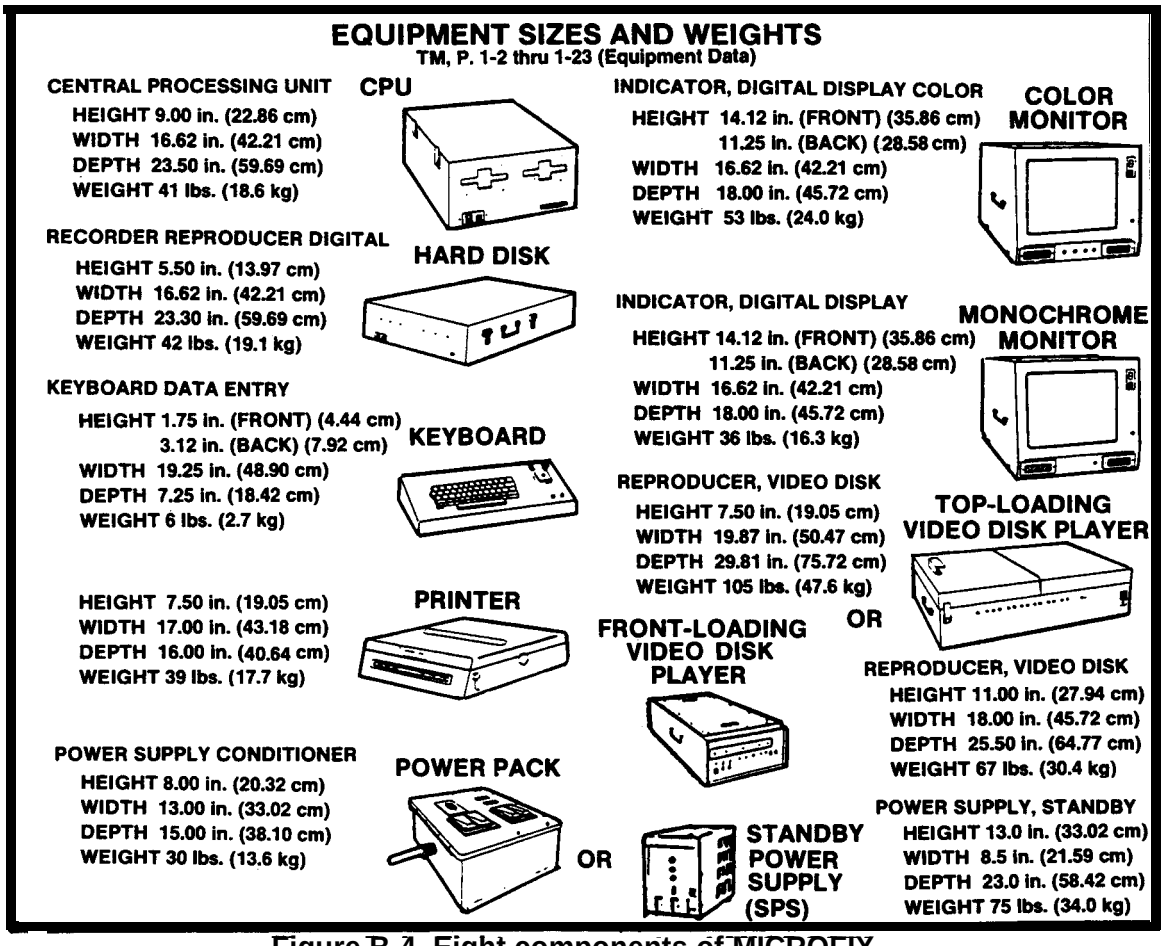


Figure B-4. Eight components of MICROFIX.

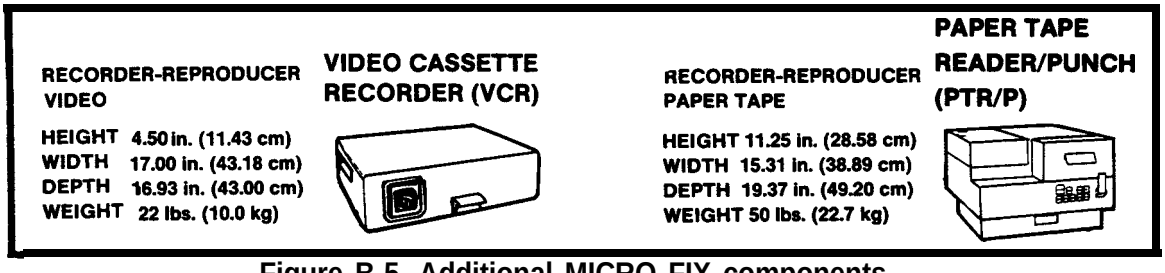


Figure B-5. Additional MICRO FIX components.

MICROFIX SOFTWARE

MICROFIX software provides analysts with the ability to collect, consolidate, and retrieve information in the area of all-source production, SIGINT, counter-SIGINT, OPSEC, and topographic analysis. The analyst uses MICROFIX software to organize information into categories which facilitate rapid and meaningful analysis. The MICROFIX software provides the ability to manipulate records in various data bases, display tactical overlays on the color monitor, cross-correlate data from different data bases, and print reports. Figure B-6 shows the baseline software (those files which are found on all MICROFIX systems).

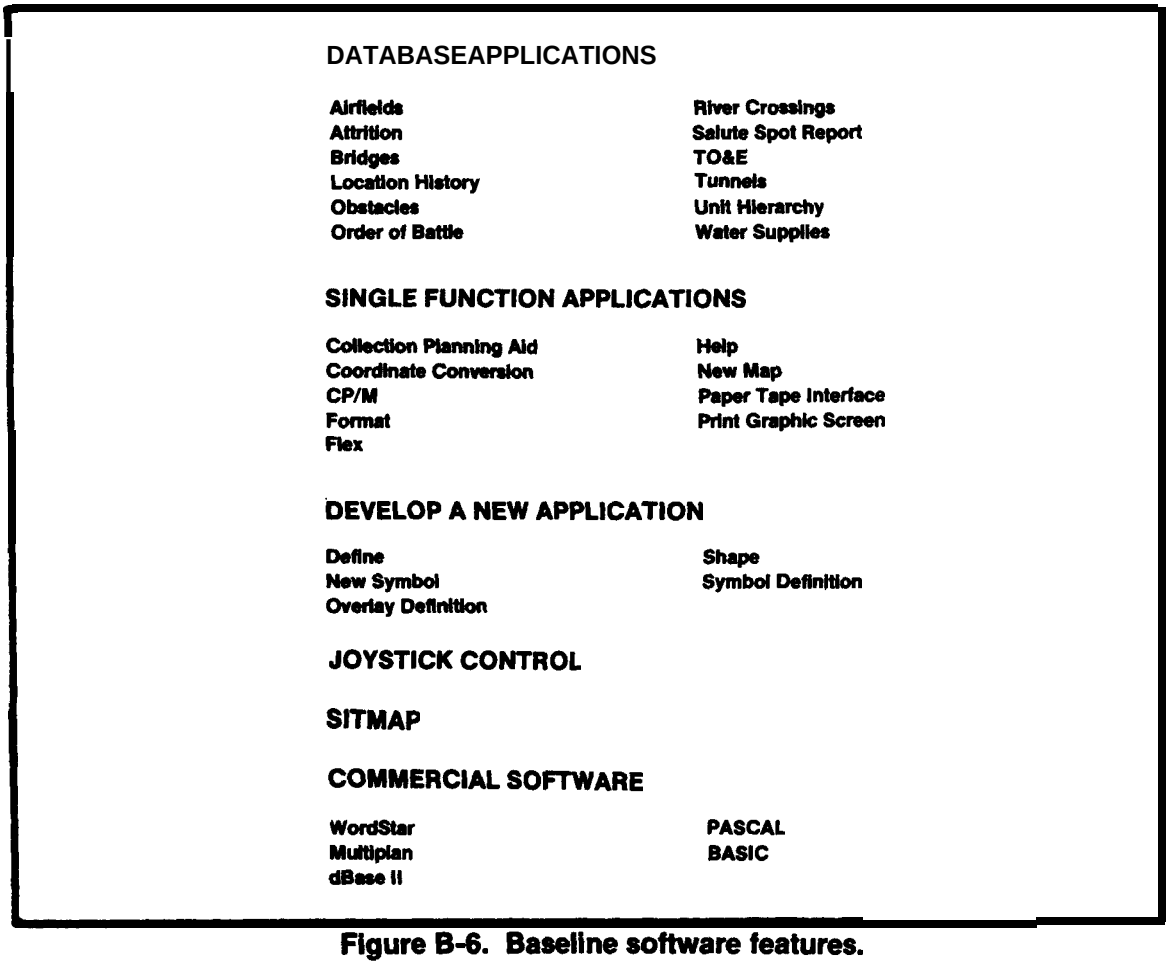


Figure B-6. Baseline software features.

The primary advantage of the MICROFIX system is that it provides the tools to manipulate and retrieve data quickly and accurately. It gives the analyst the ability to access a much larger collection of data with more speed than manual systems provide. New information is added to existing data bases, new data bases are created, and old or inaccurate data are deleted. Graphic overlays allow the analyst to visually test theories and develop or discard hypotheses. Hard-copy printouts of text information, produced at each developmental stage of the analysis process, provide verification of the logic used to develop the final intelligence products and also serve as source documents for historical record-keeping purposes.

Figure B-6 shows all the applications that constitute the software package known as the all-source production system (ASPS). The baseline software package forms the foundation for all the other configurations. The additional software packages are explained in the order in which they were released.

Topographic Workstation

Members of the terrain analysis team use the topographic workstation. The topographic software has all the applications of the baseline plus two topographic-specific applications: Topo and Topows. These applications allow the user to use digital terrain mapping features (tinted elevation, slope, or speed overlays; LOS profile; oblique view; perspective view and visible area plot); weather and environment features (sun rise and set, phases of the moon; NBC and smoke calculations; affect of weather on night vision devices, electro-optic sensors, and density altitude calculations); and a mobility calculator for friendly and enemy wheeled and tracked vehicles.

Technical Control and Analysis Element Workstation

SIGINT analysts use the TCAE workstation. TCAE software has all the applications of baseline software PIUS five SIGINT-specific applications:

- Fix. Allows the user to input and plot lines of bearing and site locations. The program will calculate and plot the ellipse of the intercepts.
- Place. The automated gazetteer.
- COMINT working aid. A collection of four data bases (frequency, call sign, code word, and case notation) that allows correlation across each other.
- ELINT working aid. An automated ELINT parameters list (EPL).
- DATEXT. The data extract (DATEXT) program allows the user to create a subset from a file of messages. DATEXT allows the user to identify several key words, phrases, and numbers to cull the entire file down to a subset of messages which deal with the topic of interest.

Counterintelligence Workstation

The counter-SIGINT analyst uses the CI workstation. The name of the workstation is a misnomer as the CI workstation is appropriate only for the 97G. CI workstation software has all the applications of the baseline software plus 11 counter-SIGINT-specific applications:

- Friend y and enemy antenna systems.
- Friend y and enemy SIGINT and REC unit OB.
- Friend y and enemy SIGINT and REC unit location.
- Friendly and enemy SIGINT and REC organization by doctrine.
- Friendly and enemy emitter and collector's characteristics.
- Enemy fixed station location.

OPSEC Workstation

The OPSEC workstation is designed for use by the intelligence analyst and supporting the OPSEC staff element. Specific characteristics of the OPSEC workstation are uncertain.

DISTRIBUTION OF MICROFIX CONFIGURATIONS

Tables B-1 and B-2 depict the number of systems at each echelon. Also shown is a recommended distribution of the various workstation configurations.

Table B-1. Workstation distribution (mid- to high-intensity conflict).

	TOTAL	ASPS	TCAE	CI	OPSEC	TOPO
Theater	1					1
Corps	13	6	4	1	1	1
Division	7	2	2	1	1	1
SEP BDE or ACR	2	1	1			

Table B-2. Workstation distribution (low- to mid-intensity conflict).

	TOTAL	ASPS	TCAE	cl	OPSEC	TOPO
Theater						
Corps						
Division	7	2	1	1 or 2	2 or 3	1
SEP BDE or ACR	2		O or l	O or l	1	

The G2 determines specifi c al location of workstations for a given exercise or requirement.

UT ILIZATION OF MICROFIX

Methods of using the MICROFIX system are limited only by the user's imagination. Several units are innovators in their use of the system. Some examples are--

- Printing the entire OB file (or selected enemy units) for use as an OB book. Updating the OB book is easier by doing the additions, deletions, or changes on the computer and then printing the updated or added records.

- Printing the unit hierarchy report for the enemy units your unit is facing. This report includes unit name, parent unit name, location, and DTG of last 'siting. Gaps in your intelligence holdings become very evident since the computer prints a blank space for missing data. This report provides guidance to CM&D, provides a quick reference for RIIs from adjacent and higher units and, by posting a copy beside the SITMAP, acts as a quick reference guide for locating enemy units.

- Using the location history function to plot the location histories of key enemy units (that is, independent tank battal ions, RAGs, DAGs, BMP-equipped MRRs) on the color map screen. Plotting the movement history of these units provides an indication or confirmation of enemy commander's intent. Location history also indicates variances to doctrinal rates of march. This alone provides key indications to the enemy commander's intent or the terrain and weather influenced limitations not previously identified in the IPB.

- After doing your IPB in garrison, various options of enemy attack are conjectured. These various options are then templated over the terrain. Each option then is drawn on the color map using the sketch function and saved for immediate recall . When the exercise scenario (or real combat) confirms one of your templated options, considerable time is saved in analyzing the AAs.

APPENDIX C

INDICATORS OF ENEMY COURSES OF ACTION

Indicators are any positive or negative evidence of enemy activity or any characteristic of the AO that points toward enemy capabilities, vulnerabil ities, or intentions. Individual indicators cannot stand alone. Each indicator is integrated with other factors and indicators before patterns are detected and enemy intentions established. Indicators are developed by the ASPS analysts who are assisted by other TOC elements in the G2 or S2 section. All indicators are developed to answer the commander's PIR and IR. The analyst uses indicators to correlate particular events or activities with probable enemy courses of action.

Indicators are also used to determine what events or activities occur for an enemy to follow a particular course of action. The ability to read indicators (including recognition of enemy deception indicators) contributes to the success of friendly operations.

Enemy deception operations provide indicators in an attempt to create false or misleading patterns of enemy intentions. Analysts detect these false indicators and then determine what actual courses of action the enemy is attempting to initiate. Enemy attempts at deception are discovered by comparing indicators, intelligence, and combat information from all sources to arrive at an accurate picture of the battlefield.

INTELLIGENCE INDICATORS

Tables C-1 through C-7 show different types of intelligence indicators. These lists of indicators are by no means complete, nor are they intended to apply to all situations or all types of enemy forces. They give some types of indicators which when incorporated with other indicators, creates patterns or suggests a series of activities which point to typical enemy activities or cour ses of action. Analysts are prepared to develop their own indicator ists for the specific situations which confront them.

TableC-l. Enemy offensive indicators.

ACTIVITY	EXPLANATION
Massing of motorized elements, tanks, artillery, and logistical support.	Areas of secondary importance are often denuded to mass maximum strength for the main effort.
Deployment of combat element (motorized rifle, armor, antitank (AT)) echelons on a relatively narrow frontage.	Normal attack formation provides for the second echelon of the regiment to be located 5-15 km in the rear of the first echelon, on-line; and the division second echelon 15-30 km in the rear of the first echelon.

Table C-1. Enemy offensive Indicators (continued).

ACTIVITY	EXPLANAT10N
Forward units disposed on relatively narrow fronts and depths.	A MRR breakthrough zone is from 2-4 km within an assigned attack frontage, which varies from 3-8 km. MRR headquarters located approximately 4 km from the FLOT during normal attack posture.
Concentration of mass toward e ther or both flanks within f rst echelon defensive area.	Single or double envelopment normally is attempted in the offense. Tanks and motorized units on either or both f anks may indicate single or double envelopment.
Demonstrations and feints.	Local, small-scale attacks or demonstrations involving motorized rifle units, tanks, and artillery frequently precede a general attack.
Establishment and strengthening counterreconna issance screen.	Counterreconnaissance screens are used to cover possible assembly areas, routes of troop movement, or regrouping of forces to be used in the attack.
Forward movement of hostile units.	Before launching an attack, troops may be moved to assembly areas from which they can deploy.
Increased patrolling (ground reconnaissance) .	Patrolling by motorized rifle units usually is more active before an attack.
Forward CPS located close to the FLOT. Other CPS move forward.	Preceding an attack, an auxiliary CP is establ ished, if needed, by Army or front. The division main CP is located 5-15 km from the FLOT; the division forward CP is located 5 km from the FLOT; the regiment main CP is located 2-3 km from the FLOT; and the battalion CP or OP is located 500-1,000 m from the F LOT.
Locating a division-sized operation maneuver group (OMG) at Army; Army-sized OMG at front.	OMGS are formed preceding an offensive operation. They are generally committed before the conclusion of the first echelon battle and operate independently of the main forces. OMGS use a separate axis of advance from the main body.

Table C-1. Enemy offensive Indicators (continued).

ACTIVITY	EXPLANAT 10N
Massing of artillery units.	Large RAGs, DAGs, and Army artillery groups (AAGs) indicate initiation of main attack. Enemy norms are 60-100 tubes per kilometer of frontage against wel l-prepared defenses for main attack; 60-80 tubes per kilometer of frontage against hasty defenses for main attack; and 40 tubes per kilometer frontage for secondary attack. The RAG is usually located 1-4 km from the FLOT; the DAG usually 3-6 km from the FLOT; and the AAG is usually more than 6 km from the FLOT. AAGs are formed only in the offense and only to support the main attack. TMS-65 are within 4 km of the FLOT for smoke operations.
Extensive artillery preparation of up to 50 minutes in duration.	The offense is built around the striking power and shock of massed artillery. Preparations of 1/2 to 1 hour normally precede an offensive.
Dispersal of tanks and self-propelled howitzers to units.	Tanks accompanying leading waves of assault motorized units--with motorized self-propelled howitzers following the tanks closely, by bounds.
Movement of fire and missile forward.	Enemy SAM control radars require time to be set up and oriented. The enemy prefers to establish SAM capability before moving other forces forward. In the event of the arrival of the second echelon, control radars are establ ished to allow for an overlap of coverage as the first echelon moves their SAM radars forward in the offense.
FROG, SS-21, SS-23, and SCUD units located forward.	Enemy offensive operations also occur in-depth. Forward movement of SSMS puts friendly airfields and depots in jeopardy.
2 to 4 ZSU-23-4S located in forward areas.	Medium AD guns are displaced before attack to protect assault forces and to facilitate forward displacement during the attack. ZSU 23-4s protecting the leading battalions are approximately 1.25 km to the rear of the FLOT.

Table C-1. Enemy offensive indicators (continued).

ACTIVITY	EXPLANAT 10N
Increased air reconnaissance,	Air reconnaissance usually is more active before an attack.
Systematic air bombardment.	Before the attack, the enemy may engage in the systematic "softening up" of key positions by bombardment,
Establishment of auxiliary airfields or activation of inactive air fields.	Buildup of logistics and maintenance capability indicates increased capability to support offense.
Clearing lanes through obstacles within own position.	Lanes are cleared and marked through mined areas, and ramps and bridges prepared over ditches and trenches within enemy's own position. This is done before attack to facilitate forward movement and grouping, particularly at night.
Reconnaissance and destruction of obstacles that are part of our defenses.	Usually on the night preceding an attack, enemy patrols reconnoiter friendly obstacles to determine a plan for clearing lanes. The patrol destroys only such obstacles that will not disclose the direction of the main attack.
River assault crossing units located forward (providing there is a water obstacle) .	Amphibious, bridge, and other engineer units with water-crossing capabilities are located near the FLOT and also echeloned to the rear. They are also collocated with other tactical units of the attacking force.
Airborne, airmobile, and air assault attacks on our rear area.	The enemy conducts offensive operations throughout the depth of the defense. Heliborne attacks are also made to facilitate difficult operations, like river crossings.
Increased enemy agent activity in rear area.	The enemy attempts to prevent or disrupt the forward movement of friendly supplies, equipment, maintenance, and reinforcements.
Extensive efforts to destroy nuclear storage areas and delivery systems by air, artillery, and sabotage.	Enemy doctrine calls for the elimination of friendly nuclear weapons by any means. The enemy considers that we are more likely to use nuclear weapons when we are in the defense.

Table C-1. Enemy offensive indicators (continua).

ACTIVITY	EXPLANAT 10N
Movement of noncombatants out of the combat zone.	Noncombatants hinder rapid forward movement of follow-on forces.
Conducting drills and rehearsals in rear areas.	Major attacks may be preceded by drills or rehearsals. This is particularly true of attacks against fortified positions or strongly defended river lines.
Increased activity in rear areas.	Before an attack, supply and administrative activities increase in the rear areas.
Traffic control units marking routes to the FLOT.	Traffic control points are employed throughout the march routes to facilitate march formations. Allied border guards assist by controlling traffic through the barrier areas of the borders.
Forward placement of supply and evacuation installations.	Supply and evacuation installations usually are located well forward for an attack, Technical observation points are established close to the FLOT. Repair and evacuation groups are located at assembly points close to the FLOT to repair or evacuate damaged vehicles. The division supply point (ammunition, petroleum, oil, and lubricants (POL), rations) is located 25-30 km from FLOT. The regimental amrnunition supply point is located 10-15 km from the FLOT; the regimental repair point is located 10-15 km from the FLOT; the regimental POL point is located 10-15 km from the FLOT, and the regimental rations point is located 10-15 km from the FLOT. Battalion ammunition and rations supply points are located 5 km from the FLOT. The division repair point for tanks and weapons is located 2-4 km from the FLOT. The division repair point for wheeled vehicles is located 10-14 km from the FLOT. Rear control points for the front are located 150-200 km from the FLOT; for the Army are 25-40 km from the FLOT; for the division is 20 km from the FLOT; and for the regiment are 20 km from the FLOT.

Table C-1. Enemy offensive indicators (continued).

ACTIVITY	EXPLANAT 10N
Location of maintenance parties on lateral routes.	When the enemy conducts a march, the enemy establishes several maintenance parties on lateral routes to facilitate march operations.
Medical points and stations move forward.	Medical units move forward before an offensive operation to support anticipated medical and evacuation requirements. Division medical points and stations are located 10-14 km from the FLOT; the regimental medical points and station at 10-14 km from the FLOT; and the battalion medical points and station at 1.5-3 km from the FLOT.
Radio sil ence on nets organ c to the d vision.	The enemy attempts to deny us information which can be developed from intercepting radio traffic.
Abnormal logistics traffic on command nets.	To expedite supplies to units about to conduct a main attack, commanders may get personally involved.
Dummy traffic in radio nets to cover unit moves.	The enemy will attempt to deceive us about the location of enemy forces.
Deception operations to cover unit movement.	Same as above.
Extensive smoke operations.	Smoke operations mask the movement of units during the period immediately preceding an attack.
SIGINT and jamming assets located forward.	SIGINT and jamming assets will move well forward to within 2-4 km of the FEBA before attack.
Extensive spot and barrage jamming of our front line units' communications nets, as well as communications systems associated with tactical air control systems.	Extensive jamming will precede an offense to cause the maximum disruption of our C^2 communications. However, jamming will cease when enemy forces reach our main defense area to prevent interference with their own communications systems.

Table C-2. Enemy defensive indicators.

ACTIVITY	EXPLANAT 10N
Preparation of battalion and company defense areas consisting of company and platoon strong points.	Defense is based on holding prepared defensive areas and counterattacks by tank-heavy forces.
Extensive preparation of field fortifications.	The enemy makes extensive use of trenches, prepared positions, and overhead cover in defensive operations.
Formation of AT strongpoints in depth along avenues of logical approach.	AT strongpoints are formed in depth along logical avenues of approach for armor. These are made up of motorized rifle, engineer, and AT gun and missile units with positions strengthened by mines, ditches, and other obstac es.
Attachment of additional AT units to frontline defensive positions.	In areas where there is a serious armored threat, the enemy will concentrate as many as 25 AT guns for every 1,000 m of front.
Preparation of alternate artillery positions.	In normal defensive operations, three positions are prepared for each firing battery.
Employment of roving artillery.	Roving guns and batteries are part of normal defensive operations.
Large tank heavy units located in assembly areas to the rear.	Tank units are held in assembly areas for employment in counterattacks.
Preparation and occupation of defensive positions.	In the defense, a security zone and main defense area are prepared and occupied.
Presence of demolitions, contaminated areas, obstacl es, minefield.	Demolitions, minefield, and other obstacles are placed to cover AA to the position.
Deployment of motorized rif e units on good defensive POSi tions. Preparation of company strongpoints on key terrain	Dominating terrain that has good FofFs and is relatively inaccessible to tanks usually is selected for a defensive position.

Table C-2. Enemy defensive indicators (continued).

ACTIVITY	EXPLANATION
Prestocking ammunition and engineer supplies and equipment and fortification of buildings.	Prestocking ammunition reduces the load on logistics throughout the system once the battle begins, Engineer tools and equipment may be used to dig trenches and to erect obstacles.
Entrenching and erecting bands of wire.	Digging of trenches and the erection of wire indicate preparations to hold the position.
Presence of dummy artillery observation points.	Dummy artillery observation points preserve the effectiveness of the actual artillery positions by deceiving us as to their location.
Presence of dummy CPS.	Same as above.
Increased activity of SIGINT and ESM units but decreased activity of ECM units.	Increased activity is an attempt to gain information about us before the attack.
Early warning sites hardened.	When early warning sites are hardened, it indicates the intention of those forces to remain in place and to protect an important facility.
CPS placed in hardened facili ty.	Same as above.
Additional AT units attached to first eche on maneuver uni ts.	The enemy puts great emphasis on killing tanks early. The enemy believes that if the tanks can be stopped, the attack will fail.
Establishment of a security zone.	A security zone is established to enable fortifications to be constructed away from immediate danger from our artillery and direct-fire weapons.
Forward units disposed on relatively wide fronts and depths compared to offensive posture.	The defense zone of an MRR varies from 10 to 15 km depending upon terrain and the combat availability of forces. MRR depth varies from 7 to 10 km.

Table C-2. Enemy defensive indicators (continued).

ACTIVITY	EXPLANATION
Displacement of logistics and units towards the rear.	Logistics and medical units are displaced to the rear to facilitate combat force defense and counterattack operations.
Displacement of artillery and SSM units towards the rear,	Artillery units are displaced toward the rear to reduce the chance that these units will be lost or destroyed during the preliminary stages of the battle. During the defense, deep fires are not as critical as during the offense.
Presence of large AT reserves with mobile obstacle detachments (MODS).	Large AT reserves are established (with MOD) to provide a quick reaction AT capability.
Decreased communications intercepts (due to increased use of wire).	The enemy places increased reliance on wire in the defense to increase security.
AD systems located in rear areas.	Destruction of logistics, command, and artillery units are high-priority missions for our deep attacks,

Table C-3. Meeting engagement (movement to contact) indicators.

INDICATORS

ACTIVITY	EXPLANATION
Increased air and ground reconnaissance along MCS.	Accurate information about routes speeds the advance.
Road junctions, bridges, and other key features are occupied by either airborne forces or forward detachments.	The enemy wants to control high-speed armor AAs into our key areas.
Increased counterreconnaissance activity.	Counterreconnaissance is an attempt to prevent us from gaining information about enemy dispositions and movements.
Forward movement of columns dispersed laterally in two or more MCS.	The enemy prefers to use march formation when moving to contact.

Table C-4. Reinforcement indicators.

ACTIVITY	EXPLANATION
Movement of additional troops toward the front.	This action increases enemy's present strength.
Increased traffic toward present position.	Increased traffic brings up additional troops, equipment, and supplies.
Identification of new units in in the combat zone.	The presence of new units--in addition to units already present--increases enemy's strength.
Additional CPS and supply and evacuation installations.	Presence of additional units causes an increase in the number of these installations.
Logistical installations moved well forward.	indicates preparation for the resumption of the offensive after reinforcement.

Table C-5. Delaying action indicators.

ACTIVITY	EXPLANATION
Withdrawal from defensive position(s) before becoming heavily engaged.	In delaying actions, units avoid becoming decisively engaged.
Successive local counterattacks with limited objectives.	Counterattacks are employed o assist in disengaging first echelon units, rather than to restore posit on.
Counterattacks broken off before position is restored.	Same as above.
Maximum firepower positioned forward; firing initiated at long ranges.	Long-range fires facilitate the delaying action.
Frontages up to four times that normally assigned to units on the defensive.	Forces conducting a delaying action are normally assigned frontages in excess of that normal for enemy units on the defense.
Prepositioni ng of nuclear weapons.	Prepositioning nuclear weapons facilitates the delaying action.
Discovery of dummy minefield.	Dummy minefield are easier and faster to prepare than active fields but cause approximately the same delay to advancing pursuers.

Table C-6. Withdrawal indicators.

Indications for withdrawal are generally the same as those for delaying action with the addition of the following indicators,

ACTIVITY	EXPLANATION
Systematic destruction of bridges, communication facilities and other assets in enemy-held territory.	Deliberate demolition and scorched earth tactics may be employed in military withdrawals.
Establishment of a covering force and rear guard.	Cover movement or withdrawal of main body. The rear guard fights delaying action, if required,
Increased use of night-driving devices in all areas.	The enemy will attempt to withdraw at night, if possible.
Minimum logistical and medical services.	Nonessential logistics and medical services are withdrawn first.
Marking withdrawal routes.	Movement and location of traffic control units or parties to the rear along the LOCS that are to be used by major units.
Use of contaminated areas to camouflage forces and cover withdrawal .	Contamination hinders reconnaissance and pursuit.
Presence of rear guard and covering force.	Minimizes losses and permits main body more freedom of movement.
Preparation of future defensive lines behind main defensive structure.	If the withdrawal is deliberate, the enemy will want new positions ready before withdrawing.
Jamming or destruction of friendly air and ground battlefield surveillance radars.	Battlefield surveillance radars are capable of detecting withdrawals at night or during conditions of poor visibility.
Engineer reconnaissance and MOD detected along LOCs, tunnels, built-up areas, dams, and dikes.	Withdrawing forces will begin to systematically destroy all crossings and implement obstacles as they withdraw.

Table C-6. Withdrawal Indicators (continued).

ACTIVITY	EXPLANAT 10N
Stockpiling of explosives at central points. Distribution of, and the establishment of, small dumps of explosives and landmines near bridges, possible abatis sites, and other demolition target sites.	Wit hdrawing forces will attempt to de ay pursuit with obstacles,
Preparation of target for systematic or hasty destruction.	Same as above.
Deception operations, such as dummy radio traffic.	Withdrawing units will attempt to portray a normal defense.
Smoke operations to cover withdrawal operations.	Withdrawals must be unobserved to be effective.
Rearward movement of long-range artillery.	Long-range artillery will be moved back to new positions before the withdrawal takes place
Movement of small reconnai ssance parties to the rear.	Withdrawing units need current reconnaissance along w thdrawa routes.
Displacement to the rear of emitters associated with logistics units. Destruction or removal of logistic material from existing depot and dump locations to the rear.	Logistics are withdrawn first to avoid being overrun during a possible pursuit.

Table C-7. Nuclear weapons indicators.

ACTIVITY	EXPLANAT 10N
Heavily guarded movement of supplies, equipment, and material .	Movement of supplies, equipment, and material of nuclear nature requires special security measures.
Heavily guarded installations.	Sites for storage of nuclear supplies and the locations of del ivery units are heavily guarded.
Preparation of heavy artillery positions.	Primary and alternate positions for nuclear del ivery artillery are prepared before movement of the units.
Movement of small, heavily guarded convoys, including closed vans, with a high percentage of automatic weapons.	Nuclear warheads are moved under heavy security, usually in closed vans. Escort vehicles are equipped with machine guns.
Light aircraft circling over moving convoy.	Nuclear warhead convoys often use aerial radio relays to maintain communication.
Movement of small groups of heavily armed hel icopters escorted by tact cat fighters.	Nuclear warheads may be moved by helicopters, with guards and armed helicopters as escort, Tactical aircraft may provide air cover.
Movement of trai ers with rockets or missile bodies.	Trailers are used to resupply missile and rocket units.
Identification of tall, slender objects, like towers, chimneys, or narrow trees, not previously in the area.	Ballistic missiles may be camouflaged as towers, chimneys, or narrow trees, such as poplars.
Large, well-guarded complexes, including tanks, trucks, radars, electronic equipment, generators, and maintenance tents, located wel l to the rear.	SSM units require extensive ground handling equipment.
Evacuation or exclusion of civilians from specific areas suitable for nuclear storage or delivery sites.	Civilians may be evacuated from areas selected for nuclear storage or delivery sites.

Table C-7. Nuclear weapons indicators (continued).

ACTIVITY	EXPLANAT 10N
Presence of meteorological radars.	An END TRAY radar is part of the organic equipment of both the free rocket over ground (FROG) and SS-1c SCUD systems, as wel 1 as other nuclear-capable systems. (END TRAYS also are found with conventional artillery and AF units.)
Construction of FROG, SCUD, or SCALEBOARD, SS-21 or SS-23 launch positions.	All of these systems have confirmed nuclear capabilities. A survey-controlled launch position is constructed for each transporter-erector-launcher (TEL) before occupation.
Movement of SSM TELs to a launch site within 1/3 to 1/2 maximum range from the FLOT.	SSM TELs remain in camouflaged positions until movement to the launch area.
Passage of wind data from mid-range position to a command or technical element.	Enemy SSM accuracy is heavily dependent on wind data.
Passage of a nonsense word over command and selected fire control nets.	May be a code word relative to preparation for or execution of a nuclear fire mission.
Volume of traffic on command nets suddenly increasing then dropping to a low level or standdown.	May reflect passage of strike warnings followed by preparation for electro-magnetic pulse protective measures.
Identification of SSM unit-peculiar equipment.	Presence of nuclear-capable systems.
Limited withdrawal of frontline units without apparent tactical reason.	Frontline units may withdraw for a limited distance to avoid casualties from close-in nuclear explosives.
Sudden and energetic digging in enemy areas.	Prior to use of nuclear weapons, frontline units may be ordered to dig deeper foxholes or take other individual protective measures.

Table C-7. Nuclear weapons indicators (continued).

ACTIVITY	EXPLANAT 10N
Large concentrations of radios, radars, and other electronic equipment located in the vicinity of suitable sites for guided missile launching.	Concentration of equipment is necessary to guide and control guided missiles, which must be located in close proximity of the launching site.
Sudden increase in communications and electronic activity.	Increase may be incident to delivery of nuclear weapons, for example, last minute orders and warnings, and use of electronic guidance and control.
Use of smoke cover on front-line troops.	Smoke may be used to protect troops against thermal effects of weapons used in close support.
Disappearance of known enemy agents from specific areas.	Prior to nuclear attack of an area, agents may be ordered to leave the area.
Increased or unusual air activity.	Delivery of nuclear weapons by air may require a temporary degree of total air superiority, special photo mission, or practice flight pattern runs by the delivery aircraft.
Additional AT elements with first echelon units.	Enemy will expect friendly forces to react to indications of a nuclear strike with an attack of tank-heavy forces. Also, tanks have greater survivability under nuclear conditions.
Movement of small convoys from the warhead storage areas.	Warheads being moved to be mated to missiles.
Removal of antennas and other equipment mounted on the exterior of vehicles.	To prevent blast damage.
Lowering of windshields on vehicles.	See above.
Removal of camouflage nets.	See above.
Movement of vehicles to reverse slopes.	See above.

Table C-7. Nuclear weapons indicators (continued).

ACTIVITY	EXPLANAT 10N
Location of missile and free rocket units within striking distances.	Missile and free rocket units are located within one third of the maximum range from the I ine of contact on the offense, and one half of the maximum range on the defense.
Use of missiles or rockets with high-explosive warheads.	Missiles or free rockets may be used to deliver high-explosive warheads either in a normal support role or in a registration.
Location of very heavy artillery within supporting distance of front lines.	Nuclear delivery artillery is located within one third of its maximum range from the line of contract on the offense, and one half of the maximum range on the defense.
Registration of very heavy artillery.	Registration may be conducted using smoke and low charge or high explosive projectiles prior to firing a nuclear projectile.
Special or unusual activity by frontline troops.	Frontline troops may construct special positions, usually deep or covered foxholes, before enemy use of nuclear weapons.
AD weapons are deployed to cover possible warhead storage areas.	Enemy expects friendly air to attempt to destroy nuclear warheads in storage.
Use of high-explosive warheads from SSMs-or heavy art illery in a normal support role.	Indicates presence of nuclear-capable systems.
Use of missile-associat ed terms on selected radio nets	See above.
Preparation of future launching positions.	See above.
Inability to locate previous γ identified missile units.	May be moving to f iring positions.
Additional administrative, command, fire control, and logistics nets identified in the area of interest.	If these nets can be identified as nuclear-related, they indicate the presence of nuclear-capable units.

Table C-7. Nuclear weapons Indicator (continued).

ACTIVITY	EXPLANATION
Presence of heavy artillery,	203 mm SP gun, 240 mm SP mortar, and towed 203 and 240 have nuclear delivery capabilities, as do 152 mm SP guns.
Deployment of jamming assets.	Jammers are deployed to protect critical targets like nuclear units.

INSURGENT ACTIVITY INDICATORS

Anything that insurgents do to influence and direct a society toward overthrowing its government is reflected by some action or indication, no matter how subtle. These occurrences are referred to as insurgent activity indicators. By recognizing these indicators, it is possible to obtain the first clues to insurgent existence and then evidence of the growth of the insurgent movement. Because there is a great deal of legitimate activity, there is a requirement to determine which of the various sociological, economical, political, and other activities represent insurgent activity.

It is not possible to provide an all-inclusive listing of insurgency indicators because there are too many possibilities existing in the many nations of the world. The following indicators, however, do provide a beginning framework for a detailed analysis of any particular country. The greater the perception of an insurgency situation within a particular country and the greater the knowledge of the insurgent involved, the easier it is to identify the insurgent activity indicators.

These indicators serve as a guide for intelligence officers and analysts in developing appropriate clues to insurgent activity in a particular area. Isolated actions of seemingly little significance in one area show a pattern of an emerging insurgency when coordinated with reports of indicators from other areas. In developing indicators, or using these suggested ones, it is important to remember that insurgent strategy suddenly changes. The insurgent threat unfolds along altogether different lines simultaneously or suddenly switches from use of military force, for example, to a political example, to a political offensive. Such a development is dangerous if it makes the general situation appear to be much less critical than it" really is. The development of appropriate indicators not only indicates that an insurgency or potential insurgent situation exists, but also identifies any problems and dissatisfaction of the people. The elimination or effective control of insurgency is based on coordinated internal defense and development (IDAD) programs which address identified problems or potential problems. Before these programs are developed, the threat is defined. To define the threat, you first establish insurgent activity indicators.

RURAL INSURGENT ACTIVITY

A rural area includes all farming areas, any town or village up to 5,000 people, and any town or village up to 20,000 people with a farm-based economy where the townspeople, if not engaged in farming, earn their livelihood in agricultural service industries. In such areas, where the interests are so interdependent, insurgency indicators would be similar in both the town and countryside. This is not to say that rural insurgency is not directed by urban insurgents and coordinated with urban insurgency; however, some theorists emphasize that the key to success is the countryside and the rural population. In such cases, early insurgency indicaters are found in the rural areas where the subversive insurgents are concentrating their initial efforts.

During the development of a subversive insurgency, some of the first indicators of latent or incipient insurgency appear in the rural areas. While some of these indicators are rather obvious, some are not. For the sake of simplicity, these indicators of insurgency are placed into four categories: population, propaganda, commodity, and environmental.

Population

Population indicators are broken down further into subcategories of general activity, insurgent-promoted activity, and activity directed against the government.

General Activity. This includes--

- Identification of insurgents, their supporters, and sympathizers who suddenly appear in, or move out of, an area.
- New faces in the community.
- Unusual gatherings among the population.
- Disruption of normal social patterns.

Insurgent-Promoted Activities. This includes--

- Refusal of peasants to pay rent, taxes, or loan payments or unusual difficulty in the collection of same.
- Trends of demonstrated hosti l ity on the part of the local population toward government forces.
- Occurrence of actions previously considered taboo by the POPUlace.
- Disappearance of the population from or avoidance by the peeple of certain areas.
- Unexplained disappearance or dislocation of young people.

Activity Directed Against the Government. This includes--

- Strangers attempting to join local security forces.
- Reports of the people being approached for purposes of intelligence recruitment.
- Unusual short absences of government employees.
- Failure of police and informant nets to report properly.
- Growth of general hostility toward the government.

- Unexplained destruction *or* loss of government identification papers or passports and increased forgeries thereof,

- Closing of rural schools.

- Murder and kidnapping of local government officials.

Propaganda

Propaganda indicators are broken down further into subcategories of general activity and activity directed against the established government, national military forces, and the educational system:

General Propaganda Indicators. This includes--

- Dissident propaganda from unidentified sources.

- Increase in the number of entertainers with a political message.

- Increasing religious unrest.

- Increased agitation on issues for which there is no identified movement or organization.

- Renewed activity by insurgent organizations thought to be dormant.

- Circulation of petitions advocating usual insurgent demands.

- Reports from other countries that the country is ready for revolution.

Directed Against the Established Government. This includes--

- Attempts to discredit and ridicule national or public officials.

- Attempts to discredit the judicial system and POI ice organizations.

- Characterization of government leaders as puppets and tools of a foreign government.

- Movement to remove strong anti insurgency leaders.

- Agitation against government projects and plans.

- Rumors designed to gain public acceptance of untruths about the government or governmental leaders.

- Advocacy of popular front government.

Directed Against the National Military Forces. This includes--

- Attacks which embarrass or ridicule military officials.
- Characterization of military leaders as puppets and tools of a foreign government.
- Movement to remove strong anti insurgency leaders from the military.
- Propaganda directed toward youth to refrain them from joining the military service or propaganda directed at soldiers to desert.
- Characterization of the armed forces as the enemy of the people.
- Civilian avoidance of and reluctance to cooperate with the military.

Directed Against the Educational System. This includes--

- Appearance of questionable doctrine in the educational system.
- Charges by students and others that the educational system is not adequate and is only training the youth of the nation to do the government's bidding.

Commodity

Commodity indicators are broken down further into crops, animals, arms and ammunition, clothing, drugs and medicine, and communication activity subcategories.

Crops. This includes--

- Diversion of crops from the market.
- Unexplained decrease in the marketing of a given crop.
- Increased reports of pilfering foodstuffs.
- Strangers attempting to purchase crops or produce.
- Farmers marketing a crop that is smaller than usual, yet showing no signs of subsequent financial difficulty.
- Discovery of caches of staple foodstuffs.
- Increase in crop prices indicating the existence of an insurgent taxing authority in the area.

Animals. This includes--

- Diversion of animals or meat from the market.

- Reports of loss of hides or diversion of hides from the market.

- Disappearance of wild game from an area in which it was previously plentiful.

- Disappearance of pack animals or the appearance of unusual numbers of pack animals in certain areas.

Arms and Ammunition. This includes--

- increased loss of weapons by military and police forces.

- Increased thefts of weapons.

- Discovery of arms caches.

- Attacks on patrols resulting in loss of weapons and ammunition.

The above factors could be applied not only to weapons but also to any similarly essential military goods.

Clothing. This includes--

- Unusual scarcity of any type of material that could be used for footwear. This could include such items as hides of animals and old tires, in addition to manufactured footwear.

- Discovery of caches of clothing or of materials which may be used in the manufacture of clothing or uniforms.

Drugs and Medicine. This includes--

- Scarcity of herbs and plants used in or for drugs and medicine.

- Large-scale purchasing or theft of drugs and medicine and of the herbs used in their manufacture.

Communications. This includes--

- increases in purchase and use of radios.

- Discovery of caches of communications equipment.

- Unusual increase in communications traffic in amateur radio operations.

Environmental

The environmental indicators include--

- Evidence of increased foot traffic in the area.

- Increased travel within and into remote or isolated areas.

- Unexplained trails and cold campsites.

- Establishment of new, unexplained agricultural areas, or recently cleared fields.

- Unusual smoke, possibly indicating the presence of a campsite or a form of communication.

- Concentration of dead foliage in an area, possibly indicating use of camouflage.

- Presence of foot traps, spikes, and the like.

- Presence of obstacles such as those used in roadblocks and canal blocks.

URBAN INSURGENT ACTIVITY

Indicaters of urban insurgent activity also are placed in the four categories of population, propaganda, commodity, and environmental indicators. Many of the same or similar indicators appear for both rural and urban areas.

Population

Population indicators are broken down further into subcategories of general activity, insurgent-promoted activity, and activity directed against the government.

General Activity. This includes--

- Increase in size of embassy or consulate staffs from a country or countries which support insurgent groups.

- Increase in staff and activities in pro insurgency-oriented embassies or consulates in neighboring countries, including unusual patterns in nature and volume of external communications (both in-country and out-of-country).

- Increased travel by suspected subversives to pro insurgency-oriented countries or to countries notably under insurgent influence.

- Influx of insurgent leaders, both foreign and domestic, into the urban area.

- Reports of locals being trained in pro insurgency-oriented countries.

- Increase in visitors from pro insurgency-oriented countries (tourists, technicians, businessmen, and officials).

- Close connections between the diplomatic representatives of pro insurgency-oriented countries and the insurgents.

- Disappearance of known or suspected insurgents and dissident elements.

- Increase in insurgent youth gatherings.

- Hosting of trade fairs or similar activities by pro insurgency-oriented countries.

- Return of nationals from travel or study in pro insurgency-oriented countries.

- Increase in visits to urban centers by rural officials and leaders from areas of unrest.

- Establishment of organizations (even very small) of unexplained origin and of unclear or nebulous aims.

- Establishment of a new organization to replace an existing organizational structure with identical aims.

- Appearance of many new members in established organizations like labor unions,

- Attempts by new groups to obtain control of established organizations.

- Infiltration of student organizations and unions by known agitators.

- Appearance of new organizations with titles stressing patriotism, grievances, or interests of underprivileged or minority groups.

- Reports of large donations to new or revamped organizations.

- Reports of payments to locals for engaging in subversive activities.

- Reports of the formation of subversive paramilitary organizations.

- Use of grenades or other explosives in terrorist acts.

- Reports of insurgent lists of targets for planned terroristic acts.

- Appearance of professional agitators in demonstrations that result in violence.

- Evidence of the participation of paid and armed demonstrators in riots.

Insurgent-Promoted Activities. This includes--

- Reported incidents of attempted recruitment of people to join new movements or underground organizations.
- Unexplained unavailability or disappearance of doctors, printers, and other specialists who may be working with and for the insurgents.
- Habitual criminals and unruly youths who seem to be acting with and for the insurgents.
- Increased unrest and agitation among laborers.
- Inability or refusal of people to pay taxes.
- Reports of extortion and other coercion by the insurgents to obtain financial "donations" from the people.
- Disappearance of young men from the city.

Activity Directed Against the Government. This includes--

- Failure of police and informant nets to report properly, indicating sources are supporting the insurgents or are afraid of them.
- Decreasing success of government agents in infiltrating subversive organizations.
- Assessination or disappearance of government agents.
- Reports of increased attempts by insurgent representatives or suspected subversives to make contact with local leaders or government officials.
- Reports of attempts to bribe or blackmail government and law enforcement employees.
- Reports of attempts to get classified information from government officials or documents from government offices.
- Leakage of classified information to news media.
- Sudden improvement in financial status of certain government and law enforcement employees.
- Failure of government raids on suspected subversive meetings or headquarters apparently because of forewarning.
- Increased activity against the government and its police, minority groups, foreigners, or similar groups.

- Demonstrations against government forces, scapegoat minority groups, or foreigners, designed to goad government forces into acting against crowds.

- More articles or advertisements in newspapers criticizing the government.

- Growth of general hostility toward the government and law enforcement agencies.

- Occurrence of strikes in critical areas casting doubt upon the ability of the government to maintain order and provide for the needs of the people.

- Unusual and unsatisfactorily explained absences of government employees from their offices.

- Sporadic, unexplained destruction, loss, or forgery of government identification cards and passports.

- Unexplained disruptions of public utilities.

- Reports of extortion attempts on local leaders and businessmen.

- Terrorist acts and threats against government and business leaders.

- Murder or kidnapping of government officials.

Propaganda

Propaganda categories are broken down further into categories of general activity, and activity directed against the established government, military and police, and educational systems.

General Activity. This includes--

- Worldwide propaganda by proinsurgency-oriented countries denouncing conditions and blaming the government of the targeted country.

- Appearance in-country of antigovernment slogans and pronouncements by word of mouth, wall scribbling, posters, and leaflets.

- Letter writing campaigns to newspapers and government officials deploring undesirable conditions and blaming individuals in power.

- Increased use of slogans pinpointing specific grievances.

- Increased use of petitions demanding government redress of grievances.

- Circulation of petitions and pamphlets which appear to follow the beliefs and policies of a foreign power.

- More rumors, publications, or leaders from areas occupied by migrants which focus upon lack of official concern about poor conditions.

- More agitation and unrest within the urban population for which there is no logical explanation,

- Appearance of committees and organizations whose leaders do not seem to be from the urban area, yet who purport to speak for the citizens of that area.

- increased appeals directed at intensifying general religious unrest in countries where reiigious competition exists.

- Mass demonstrations where participants voice standard Communist demands.

- Announcements by foreign countries that the concerned country is ripe for "war of national iiteration, " or words to that effect,

- Propaganda linking local ethnic groups with those in neighboring countries.

- Clandestine in-country radio broadcasts worded to appeai to those with special grievances or to underprivileged ethnic groups.

- Use of bullhorns, truck-mounted loudspeakers, and other sophisticated equipment in "spontaneous"' demonstrations.

- Presence of photographers other than newsmen among demonstrators.

- Widespread propaganda which appeals for sympathetic reception or participation in strikes or demonstrations.

- Rallies to honor "martyred" insurgents. Mass demonstrations honoring revolutionary heroes or dates significant to insurgency.

- Nationwide strikes tailed to demonstrate the strength of the insurgent movement.

- Sympathy strikes or demonstrations taking place outside the country concerned.

Activity Directed Against the Established Government. This includes--

- Radio propaganda from foreign countries, aimed at the target country, accusing its government of failure to meet the needs and desires of its people.

- Propaganda from foreign countries, aimed at the target country, denouncing imperialism.

- Demonstrations and violence in foreign countries against embassies, offices, and consulates of the target country or countries which support its government.

- Spreading accusations that the government is corrupt and completely out of touch with the people.

- Agitation against existing or proposed government projects and plans.

- Accusations that the government is a pawn of a foreign government.

- Calls for a popular front government, including new parties.

- Character assassinations of top government officials.

- Movement to remove strong anti insurgency leaders from office.

- Strikes or work stoppages called to protect government actions.

Activity Directed Against the Military and Police. This includes--

- Spreading accusations that the military and police are corrupt and completely out of touch with the people.

- Character assassinations of military and police officials.

- Movement to remove strong anti insurgency military and police leaders from the office.

- Calling on the people to stop cooperating with the military and police.

- Deliberate acts to provoke police reprisals during demonstrations or strikes.

- Accusations of police brutality or ineffectiveness or claims that government forces initiated violence when demonstrations end in riots.

- Publication of photographs purporting to show repressive police practices.

Activity Directed Against the Educational System. This includes--

- Student unrest manifested by new organizations, proclamations, demonstrations, and strikes against authority.

- Charges by students and others that the educational system is not adequate and is only training youth to do the government's bidding.

- Appearance of questionable doctrine in the educational system.

- Clamor for personnel changes in the educational system.

Commodity

Commodity indicators are broken down further into subcategories of foods, arms and ammunition, clothing, and drugs.

Foods. This includes--

- Scarce food supplies when there is no report of natural impediments to agriculture.

- Decline of foodstuffs in a country or province where there is a tolerated black market, which indicates that the food is being diverted.

- Sudden shortages of preserved foods or items of food requiring minimal storage facilities.

- Failure of farmers to transport their products to the city, indicating a fear of travel on the highways.

- Large-scale purchasing of foodstuffs which may be by purchasing agents for an insurgent movement.

Arms and Ammunition. This includes--

- Increase in assaults on police and military personnel which results in thefts of weapons.

- Increase in thefts and purchases of arms, ammunition, and explosives.

- Discovery of arms, ammunition, and explosives being clandestinely manufactured, transported, or cached.

- Increased purchase and theft from salvage yards of metal products like pipe, casings, wire, spikes, snd nails.

- Increased purchase of surplus military goods.

- Increase in demand for small arms and ammunition on the open market.

- Reports of large-scale purchasing of weapons, ammunition, and material used in their manufacture.

- Increase in pilfering of arms and ammunition from the government.

- Increase in the number of armed robberies.

- Reports of theft or sudden shortages of chemicals which could be used in the clandestine manufacture of explosives.

- Appearance of arms manufactured in pro insurgency-oriented countries.

Clothing. This includes--

- Unusual systematic purchase of clothing materials which could be used for the manufacture of insurgent uniforms or footwear.

- Unusual scarcity of clothing or material used in the manufacture of clothing and footwear.

- Distribution of clothing to underprivileged classes by organizations of recent or suspect origin.

- Discovery of caches of uniform clothing.

Drugs. This includes--

- Scarcity of drugs and medical supplies on the market or black market.

- Large-scale purchase or theft of drugs and other medical supplies,

- Diversion of shipments of drugs.

Environmental

The environmental indicators include--

- Apartments and housing being rented, but not lived in as homes.

- Slogans written on walls, bridges, and streets.

- Defacement of government and police information signs.

- Disappearance of electrical lines. Pollution of the urban area's water supply.

- Terror ist acts against physical targets like bridges, dams, airports, or buildings.

- Changes in residence of suspected subversives.

- Discovery of message drops.

- Apartments and houses being used for purchases other than residences.

- Increased smuggling of currency, gold, gems, narcotics, medical supplies, and arms into urban centers.

- Reports that local currency is being bought up in world markets by pro insurgency-oriented countries.
- Appearance of abnormal amounts of counterfeit currency.
- Increase in bank robberies.
- Work stoppages or slowdowns in essential industries.
- Marked decline in product quality in essential industries.
- Marked increases in equipment failures in essential industries.
- Mass strikes and sympathy strikes in essential industries.
- Appearance of known agitators or suspected subversives in picket lines.
- Escalation of peaceful strikes to violence against property and nonstriking personnel.
- Explosions in essential utilities and industries,
- Roadblocks and mines on main lines of communication.
- Malicious damage to industrial products or factory machinery.

APPENDIX D

ENEMY STRENGTH COMPUTATIONS

Enemy strength undergoes a continuous fluctuation between TOE-type strengths and varying levels of force, unit, equipment, and personnel strengths during the course of a battle, campaign, or war. These fluctuations are a result of unit, personnel, and equipment losses and the enemy's ability or inability to provide suitable replacements quickly and consistently.

Enemy strength computations provide a method for estimating the level of combat effectiveness of enemy forces. It is computed in terms of committed forces, reinforcing and supporting units, and the number of nuclear weapons and chemical and biological delivery systems suspected or identified as being deployed within the friendly commandar's AOS or AIs.

Based on the analyst's knowledge of enemy doctrine, OB, and current information and intelligence on enemy dispositions, locations, and capabilities, the numbers of committed, reinforcing, and supporting forces is computed.

Once these enemy forces are determined, individual enemy units can be identified or located and enemy strength computed. Personnel and equipment strengths are described as percentages of known TOE-type strengths, based upon reported enemy personnel and equipment losses and known or estimated rates of replacement.

COMMITTED FORCES AND REINFORCEMENTS

Committed forces are those enemy ground units, currently in contact or with which imminent contact is expected, whose area of employment is not expected to change to counter the specific course of action selected by the friendly commander. Committed forces may change disposition within their area of employment, but no significant delay is involved in their employment. Designation of enemy forces as committed forces depends primarily upon their disposition, location at the time of the estimate, the echelon at which the estimate is being prepared, and enemy doctrine. Committed forces are either located, unlocated, identified, or unidentified units.

Reinforcements are those enemy forces whose area of possible employment against the friendly force depends on the friendly selection of a specific course of action and on enemy capabilities. Reinforcements include all known enemy forces which are neither committed against a friendly force nor committed outside the friendly zone or sector, but which reasonably are considered capable of closing with the friendly force in time to affect the accomplishment of the mission.

Estimates of enemy NBC capabilities usually are prepared at field army and higher headquarters. Units below field army level usually lack the means to gather the information to make such estimates. They use the

estimates of the higher headquarters and modify them with available information.

The determination of enemy NBC operation capabilities is based primarily on estimates of numbers and types of weapons and amount and types of agents available, knowledge of enemy doctrine, past experience, and estimates of enemy capabilities involving the employment of ground troops. It is rarely possible to estimate what portion of the available enemy NBC effort may be used against a division or corps within a field army or a command in the COMMZ. It is also rarely possible to estimate the number of nuclear weapons the enemy is capable of using within a period as short as one day. The period selected is a month or longer, depending on the available information and past experience. The statement of the enemy's capability of using chemical and biological agents includes the amount, type, and delivery means of available agents.

COMPUTING COMMITTED ENEMY UNITS

The commander and the operations officer use the information the G2 or S2 provides on enemy comnitted forces and reinforcements for planning and conducting tactical operations. Accurate information is particularly important during the commander's analysis of opposing courses of action. For example, in planning for an attack, an overestimation of committed enemy forces and an underestimation of enemy reinforcements could cause the friendly commander to attack with a small reserve. The intelligence officer's error in computing committed and reinforcing forces could al low the enemy to counterattack with an unexpectedly strong force, inflicting unacceptable casualties upon the friendly force.

All uncommitted enemy forces are considered as reinforcements if they are committed in time to affect the accomplishment of the mission. If there is doubt as to whether an enemy unit is committed or reinforcing, it is considered as a reinforcement. This reduces the risk of surprise.

Expressing strength in number of units, by type, within an enemy force is stressed because it is a simple, reliable, and readily understood method of computing enemy strength. At the same time, the OB analyst cannot ignore individual unit strength computations. This is particularly important in arriving at a true picture of the enemy's strength.

Strength by type of unit includes the total number of enemy units listed by category and type. Normally, enemy units are counted down to and including two echelons below the friendly force's level of command. Some special purpose units three echelons below may also be counted.

Usually, an intelligence officer accounts for committed enemy forces by the size of the enemy unit which is opposing the friendly elements. At the most basic level, state the actual number of weapons systems. Against an enemy army. a division G2 usually counts committed forces in terms of battalions;a corps G2 in terms of regiments; and field army and higher headquarters, in terms of divisions. At headquarters above field army, a statement of the number of armies and army groups is included. For

example, "The committed forces facing this army group consist of one army group (3 combined arms armies with a total of 11 MRDs and 3 tank divisions). . . ." When committed forces, such as guerrillas, do not have a known organization, their strength is stated in total numbers. All FS weapons systems avai table to the guerrillas, including tanks, infantry fighting vehicles (IFVs), and artillery, also are listed and expressed in terms of total numbers.

The brigade S2 considers as committed forces the first and second echelon companies of enemy MR, tank, or reconnaissance battalions in contact with the brigade. Although the enemy company is the basic sized unit used by the brigade S2 in accounting for committed forces, the S2 also accounts for smaller units which have been located as separately employed.

The battalion S2 considers as committed forces the first and second echelon platoons of the enemy MR, tank, or reconnaissance companies in contact with the battalion. Although the enemy platoon is the basic unit used by the battalion S2 in accounting for committed forces, available intelligence frequently does not enable the individual platoons composing the enemy company to be located. Therefore, the battalion S2 considers that a located enemy company normally consists of three platoons; a company (-) consists of two platoons. Table D-1 shows the process of counting committed forces in the defense and in the offense.

The designation of enemy units as committed forces depends primarily on their disposition and location at the time the estimate is made. Enemy unit identification facilitates determining if a particular unit is the reserve of elements in contact with the brigade or battal ion.

When an enemy unit of the size used in accounting for committed forces is in contact with two adjacent friendly units, the entire enemy unit is considered to be committed by the G2 or S2 of both friendly units. For example, if an enemy battalion is in contact with elements of two adjacent US divisions, both division G2s consider the entire battalion as committed against their respective divisions. This points up the need for correct identification and accurate strength computation at each echelon.

All ground FS weapons organic to the enemy MRB or MRR are usually referred to as normal regimental artillery and are always considered to be in support of committed forces. That is, each committed unit is assumed to have available to it its normal proportion of the available supporting weapons organic to the regiment. These weapons, therefore, need not be enumerated unless desired. FS weapons not organic to enemy motorized battalions or regiments which are identified as within supporting range are enumerated as if in support of committed forces. In the event that the forces committed against the brigade or battalion have no known TOE (that is, volunteer or irregular-type units), all FS weapons which are identified are enumerated.

Table D-1. Counting committed forces in the defense and offense.

When the US is in the defense,

THE	LOOKS AT	LOOKS FOR MR	TK	RECON
Battalion S2	Ist Echelon Bns	Pits	Pits	Pits
Brigade S2	1st Echelon Regts	Cos	Cos	Cos
Division G2	Ist Echelon Divs	Bns	Bns	Cos

When the US is in the offense,

THE	LOOKS	LOOKS FOR MR	TK	RECON
Battalion S2	Between LD, LC and the objective	Pits	Pits	Pits
Brigade S2	Between LD, LC and the objective	Cos	Cos	Cos
Division S2	Between LD, LC and the objective	Bns	Bns	Cos

*Reinforcing units do not need to be expressed in the same units as committed forces; they should be expressed in the simplest possible terms.

*supporting artillery may be expressed as "a RAG (or DAG)" of _____ battalions", battery or battalion equivalents (by type). However, if artillery has been located which is not a normal RAG or DAG asset, the type and size unit must be expressed. For example, "supported by a _____ battalions, RAG or DAG," artillery assets, augmented by one battery of 203 mm guns and one battery of 240 mm mortars.

When enumerating enemy forces in a defensive posture, enemy security elements forward of the combat outpost I ine are normally considered reinforcements of the main defensive position until contact with these security elements is made. The intelligence officer correctly identifies the enemy's main defensive positions and is not deceived by security forces. The security forces normally become reinforcements for the main defense after completing their security mission.

In addition to determining the enemy's ground combat unit strength in terms of committed forces and reinforcements, the G2 or S2 also considers the enemy's air and nuclear weapons strength, However, as estimates of enemy air NBC warfare strength are usually prepared only at field army level and higher, the G2 or S2 simply restates these capabilities in the estimate.

Reinforcements are stated conveniently and meaningfully. For example, if the opposing division has an MRR in reserve, this reinforcement is referred to as a motorized regiment rather than three motorized battalions. When enemy units--either committed forces or reinforcements--are very much understrength, the estimated remaining strength is expressed. Two divisions, each at half strength, are usually more formidable than a single division at full strength because of the added flexibility of employment and the additional CS probably available. A half-strength field artillery battalion is more than half as effective as a full strength battalion,

When only two elements of a unit are located, they are counted as they appear. By templating, it is possible to determine the approximate location of the third element. Although this unit should not be counted, the commander is advised as to its possible location. An exception to this rule occurs, however, in situations where enemy doctrine normally precludes elements of a unit operating independently of each other. For example, if a US brigade S2 detects the presence of one MR company of a Soviet MRB, then the remaining elements of the MRB are counted as committed, albeit unlocated, enemy forces. This is because Soviet doctrine normally precludes the MR companies of an MRB from operating independently of each other.

COMPUTING ENEMY REINFORCEMENTS

Factors derived from analysis of past similar enemy movements determine the time required for an enemy to move troops from one place to another and commit them. The considerations described below are applicable in training and as a point of departure for the development of experience factors in operations against an enemy force.

To determine the time when the enemy employ an uncommitted unit, the travel time from the unit location to a logical point where the unit can be committed is calculated. To the travel time, add the closing time (pass time of a column). Except when observation of enemy units is continuous, it is assumed that any unit could have started to move immediately after its last reported location. Therefore, to determine the earliest time at which the enemy can reinforce, add the travel plus closing time to the time last observed. For example, if an enemy reinforcement was last observed at 0800 hours, and it can deploy to envelop the northern flank in one hour, it is assumed that the attack can be launched as early as 0900 hours (0800 plus one hour). In the exceptional case involving piecemeal commitment of enemy reinforcements, consider only travel time. Forces which are committed piecemeal do not close into an assembly area or attack position.

Because observation of reinforcements is rarely continuous, statements of enemy reinforcing capabilities should include both the earliest time and that time after starting movement when the reinforcement is accomplished. For example, "'the enemy reinforces the attack with the 45th MRR at 0900 hours, or one hour after starting movement. " When the time since the last report is greater than the time after starting movement, only the time after starting movement is given. For example, "the enemy reinforces the attack with the 45th MRR now or one hour after starting movement." When the number of reinforcements is large or the enemy is capable of reinforcing in several areas, reinforcing capabilities are presented in tabular form. Table D-2 is an example of this. It shows the enemy reinforcing the attack or defense with all or part of the following units at the places and times indicated.

Table D-2. Examples of estimating reinforcements.

UNIT	PLACE	MOTOR	FOOT
45th MRR	RJ 6382	Now or 1 hr after starting.	091205 Jun or 4 hr 5 min starting movement.
	RJ 8884	090930 Jun or 1 hr 30 min after starting movement.	091605 Jun or 8 hr 5 min after starting movement.
37th MRR	RJ 6382	091000 Jun or 2 hr after starting movement.	100740 Jun or 23 hr 40 min after starting movement.
	RJ 8884	090920 Jun 1 hr 20 min after starting movement.	091430 Jun or 6 hr 30 min after starting movement.

In selecting a logical point for reinforcement, consider the effects of AO characteristics, such as AAs and logical enemy reactions to friendly courses of action. For reinforcement of an attack capability, select locations for commitment of second echelon and reserve forces for enemy battalions and regiments and forward assembly areas for enemy divisions and larger units. For enemy units moving to reinforce a defense, select defense or counterattack positions. For movements by aircraft, select logical LZS or' DZS from which the enemy forces can materially affect the accomplishment of the mission.

The time required by the enemy to issue extra ammunition, make detailed reconnaissance, issue orders, and deploy to a line of departure is not normally considered because all these actions are completed before starting the operation or simultaneously with movement.

The following guidance is applicable until you develop experience factors against a particular enemy:

- Compute foot marching time for all appropriate reinforcements. Compute motor movement time only for distances greater than 10 kilometers (6 miles). If a unit is observed in trucks, compute only the motor movement time.

- Consider a foot march of more than 32 kilometers (20 miles) as a forced march. Consider a motor movement of more than 280 kilometers (175 miles) as a forced march for motorized units and a movement of more than 224 kilometers (140 miles) as a forced march for tank units.

- Compute closing time at the night rate of march if a column begins to close before the BMNT closing time; if a column begins to close at or shortly after BMNT, use the day rate of march. If a column begins to close before the EENT, use the day rate of march; if a column begins to close at or shortly after EENT, use the night rate of march.

- Move and close the entire unit to move an enemy infantry battalion. To move a unit of regimental or larger size, move and close two-thirds of the combat elements; that is, two battal ions of an infantry regiment, two regiments of an infantry division.

COMPUTING COMBAT STRENGTH

The following three situations illustrate the method for computing combat strength, as discussed in the preceding paragraphs.

SITUATION 1

The 20th Infantry Division is advancing to the south. The advance of the division is stopped by elements of two MRRs (8th and 12th) of the enemy 16th MRD. Each of these MRRs has two MRBs in contact and one MRB in the second echelon. The third MRR (96th) is in contact with the 72d Infantry Division on the flank of the 20th Infantry Division. About 40 kilometers (25 miles) in rear of the 16th MRD and in the area of the 20th Infantry Division objective, two MRRs (43d and 75th) of the enemy 12th MRD are preparing field fortifications.

The four battalions of the 8th and 12th MRRs in contact with the 20th Infantry Division are considered as committed forces by the 20th Infantry Division G2. Regardless of the specific courses of action selected by the commander of the 20th Infantry Division to continue the advance, the area of employment of these four battalions in contact does not change appreciably. The second echelon battalions of the 8th and 12th MRRs are not considered committed since they are not in contact and are employed in other areas. The 96th MRR is considered committed and mentioned in the composition subparagraph of the OPORD, but only its second echelon battalion is listed as a reinforcement by the 20th Division.
The other two battalions are committed against the 72d Division and are not available as reinforcements against the 20th Division. The 43d and 75th MRRs of the 12th MRD are considered as reinforcements because these units are not committed against the friendly force and are committed in

time to affect the mission of the 20th Infantry Division. Although the two MRRs of the 12th MRD are digging field fortifications in the vicinity of the division objective, the enemy commander employs these units against either the 20th Infantry Division or adjacent divisions. Figure D-1 shows this situation in a schematic sketch.

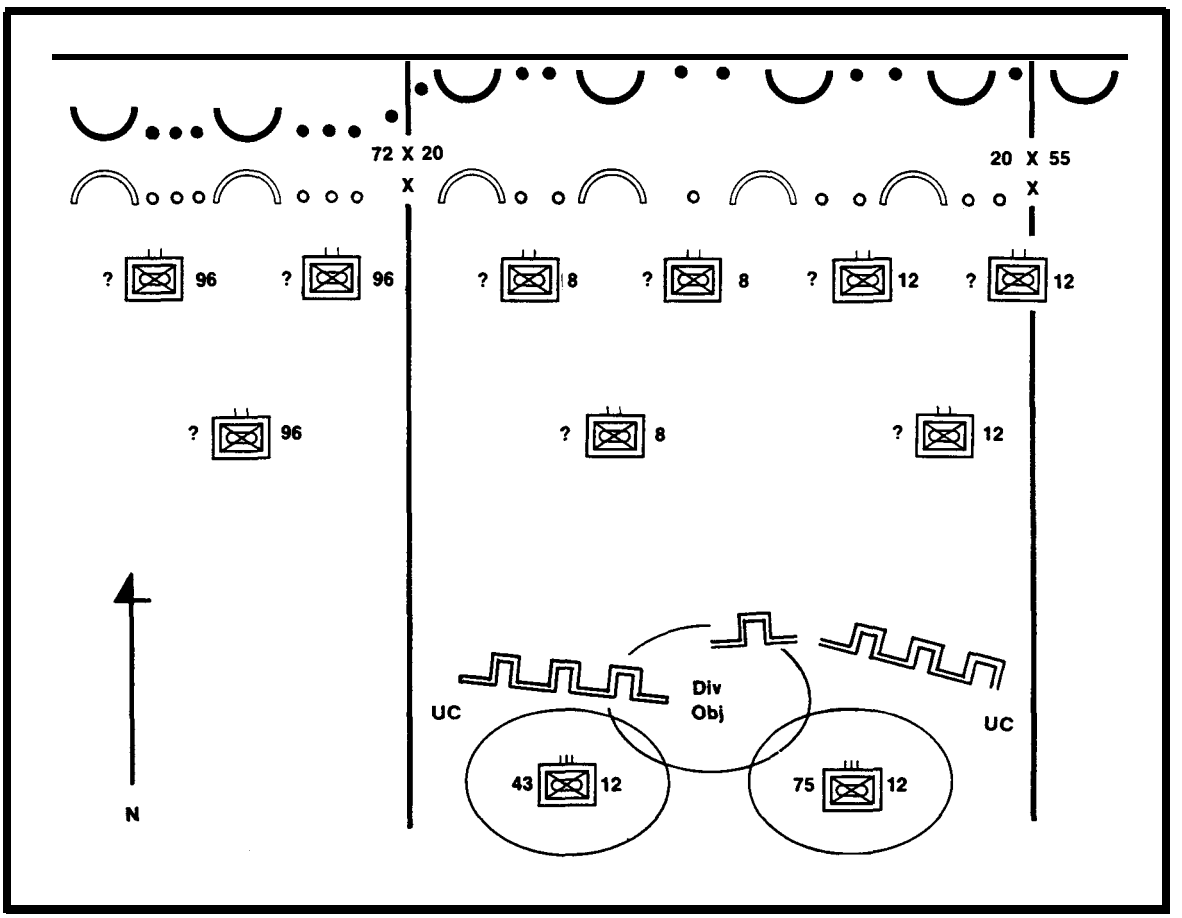


Figura D-1. Schematic sketch, situation 1.

SITUATION 2

The 20th Infantry Division is attacking to the east. Enemy committed forces are the 3d MRB, 3d GMRR, the Ist and 3d battalions of the 5th MRR, and the 1st Battal ion, 7th MRR; the 2d Battalion, 33d GMRR, 2d Battalion, 3d GMRR, and the 3d Battalion, 7th MRR are committed against units on the 20th Infantry Division flanks. The 1st and 2d Battalion, 3d GMRR, 2d Battalion, 5th MRR, and the 2d Battalion, 7th MRR are not in contact and are second-echelon battalions which are employed against the 20th Infantry Division. They are considered as reinforcements. The two enemy regiments in the assembly area astride the 20th Infantry Division north boundary and the enemy MRR south of the south boundary are also possible

reinforcements. From their locations and dispositions, it is apparent that they are the 2d echelon regiments of the divisions committed against the 20th Infantry Division. Depending on the course of action selected by the commander of the 20th Infantry Division and plans of the enemy commander, all or part of these enemy elements are employed against the 20th Infantry Division, at various times and places, in time to affect the accomplishment of the division mission. Figure D-2 depicts this situation.

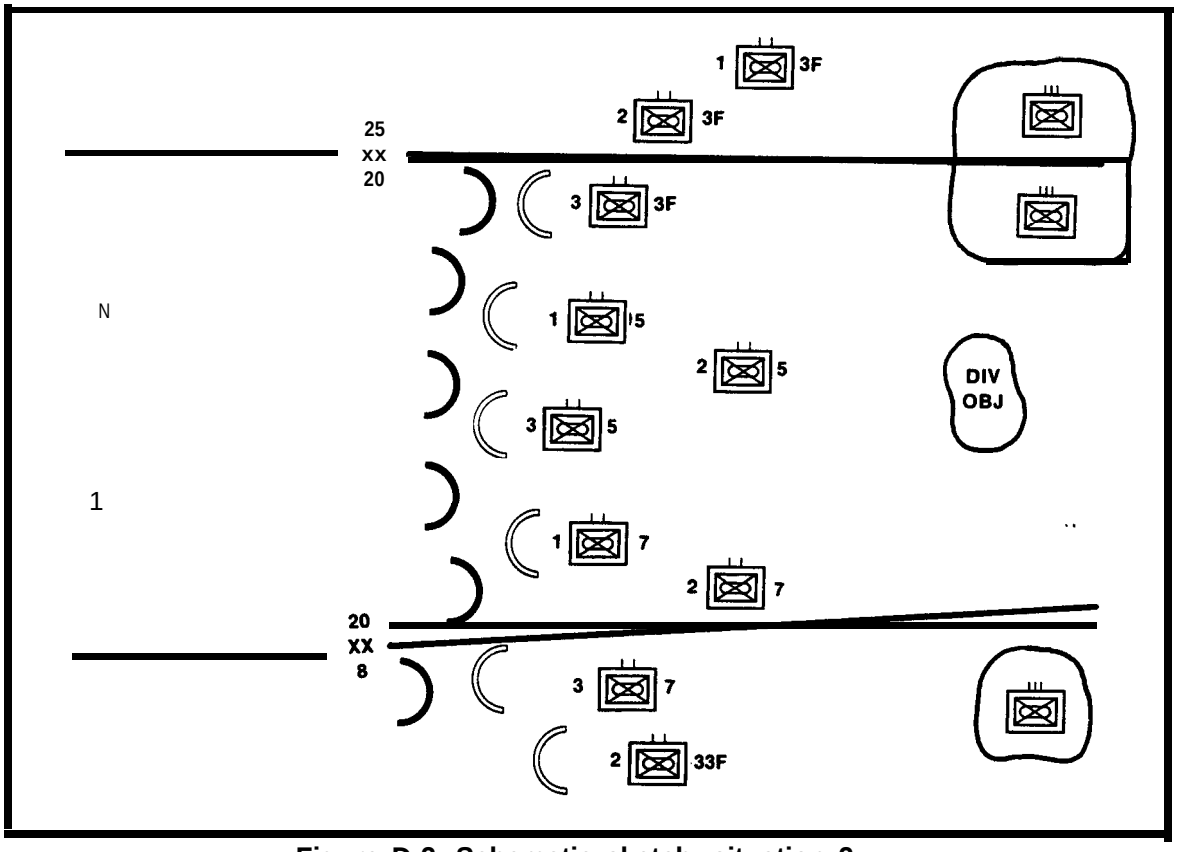


Figure D-2. Schematic sketch, situation 2.

SITUATION 3

This example discusses the determination of enemy strength opposing the Ist Brigade, 21st Infantry Division, and each of its composite units: the 1st Battalion, 69th Infantry; and the 1st Battalion, 70th Infantry.

Figure D-3 shows the Ist Brigade, 21st Infantry Division, with the 1st Battalion, 69th Infantry, and the Ist Battalion, 70th Infantry forward defending positions as indicated in a schematic sketch. Reports from the

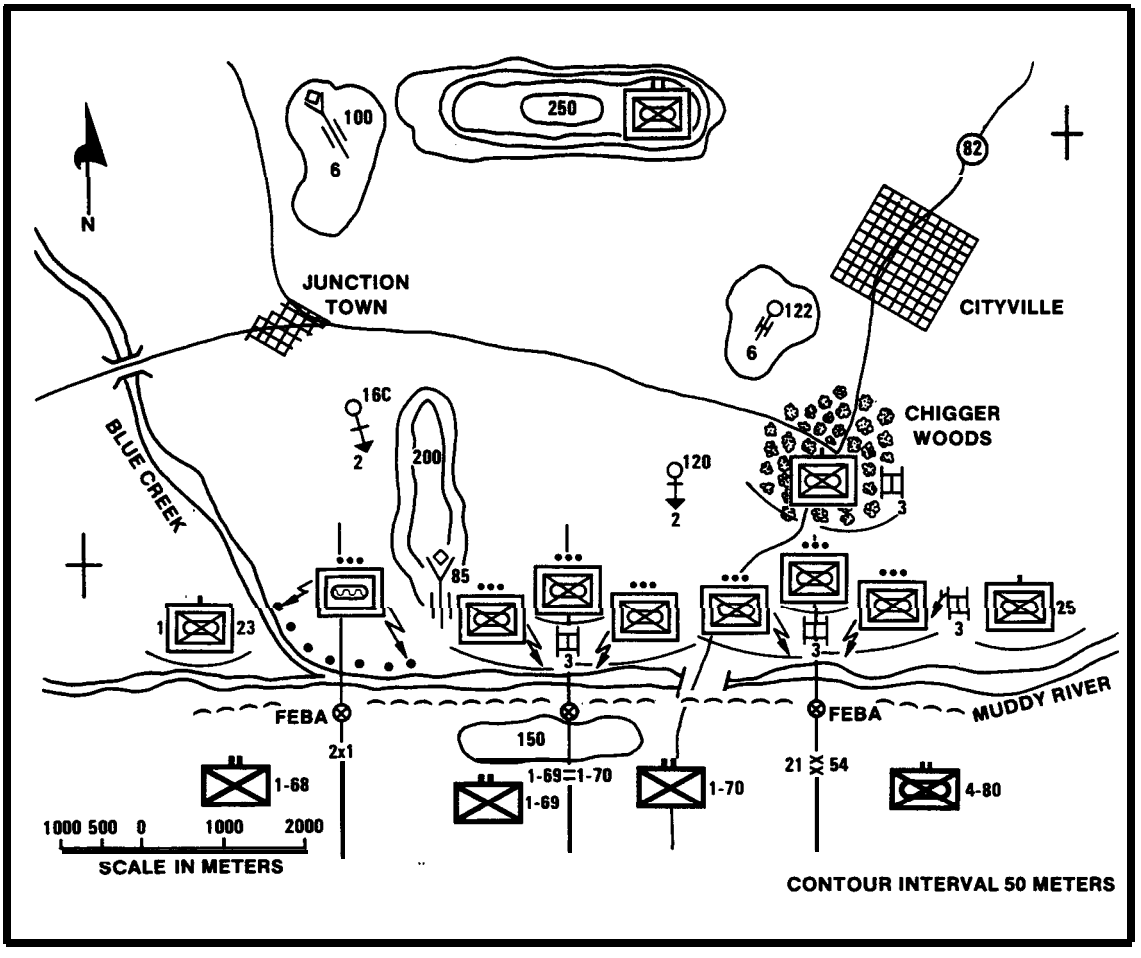


Figure D-3. Schematic sketch, situation 3.

21st **Infantry Division indicate** the enemy has an unknown number of air and nuclear weapons available.

The S2, 1st Brigade, determines enemy strength as follows:

- **Committed Forces:** Ist Brigade is opposed by elements of three MR companies, one reconnaissance platoon, and one medium tank company (13 tanks) supported by normal regimental artillery, plus six 120mm mortars, six 122mm howitzers, six loom AT guns, and all available air and nuclear weapons.

- **Reinforcements:** Enemy reinforcements available for commitment in the sector of 1st Brigade are an unidentified MRB located in the vicinity of Hill 250.

The three MR platoons northwest of the Highway 82 bridge are disposed so that they logically constitute one MR company in contact with, and committed against, the 1st Brigade. The reconnaissance platoon southwest of Hill 200 and the MR company northeast of the Highway 82 Bridge are in

contact with, and committed against, the 1st Brigade and its respective battalions. All three platoons of the company northeast of the Highway 82 bridge are considered as one company committed against 1st Brigade, since brigades account for committed forces in terms of companies. The MR company south of Chigger Woods is located so that it is, logically, the reserve company of an enemy battalion in contact with 1st Brigade and is therefore considered committed. The MR companies of the 25th and 23d Regiments, located to the east and west of the 1st Brigade sector, are totally committed against adjacent brigades and are, therefore, neither committed nor available as reinforcements against 1st Brigade, 21st Infantry Division. Twelve medium tanks are located in the vicinity of the MR companies committed against 1st Brigade and are, therefore, also committed. The S2, 1st Brigade is equally correct to account for these committed medium tanks as three medium tank platoons or one medium tank company. In addition to the 120mm mortars (organic) and the 100mm AT guns and 122mm howitzer battery (both attached), the enemy MRB is supported by the artillery group of its parent regiment. The enemy also has an unknown number of air and nuclear weapons, which are employed in support of committed forces.

The S2, 1-69 Infantry, determines enemy strength now opposing the battalion as follows:

- Committed Forces: 1-69 Infantry is opposed by two MR platoons, one reconnaissance platoon, and one medium tank platoon, supported by normal regimental artillery, plus six 120mm mortars, six 122mm howitzers, six loom AT guns, and all available air and nuclear weapons.

- Reinforcements: Enemy reinforcements available for commitment in the sector of 1-69 Infantry are an unidentified MRB located in the vicinity of Hill 250 and an unidentified MR company and medium tank platoon located in the vicinity of Chigger Woods.

One MR platoon is in sole contact with, and therefore committed against, 1-69 Infantry. The MR platoon north of boundary 1-69 and 1-70 Infantry is counted as committed against both 1-69 Infantry and 1-70 Infantry. The medium tank platoon in the same vicinity is also in contact with and therefore committed against both 1-69 Infantry and 1-70 Infantry. The MR company and tank platoon located in the vicinity of Chigger Woods which are considered as committed by S2, 1st Brigade could logically be employed against 1-69 Infantry in time to affect the accomplishment of the battalion mission and are therefore considered as reinforcements. The discussion above concerning the battalion vicinity Hill 250, the normal regimental artillery and nonorganic weapons in support of committed forces, applies also to the determination by S2, 1-69 Infantry.

The S2, 1-70 Infantry, determines enemy strength now opposing the battalion as follows:

- **Committed Forces: 1-70 Infantry is opposed by four MR platoons and two medium tank platoons supported by normal regimental artillery, plus six 120mm mortars, six 122mm howitzers, six 100mm AT guns and all available air and nuclear weapons.**

- **Reinforcements: Enemy reinforcements available for commitment in the sector of 1-70 Infantry are an unidentified MRB located in the vicinity of Hill 250 and an unidentified MR company and medium tank platoon located vicinity Chigger Woods.**

The S2, 1-70 Infantry, considers the individually located MR platoons vicinity boundary 1-69 Infantry and 1-70 Infantry in the same manner as does S2, 1-69 Infantry. Two platoons of the motorized company northeast of Highway 82 bridge are considered committed against 1-70 Infantry. S2, 4-80 Mechanized, could also consider two platoons of this company committed against the battalion. The discussion concerning reinforcements and supporting fires applies also in the determination by S2, 1-70 Infantry. (See Figure D-3).

APPENDIX E

TERRAIN ANALYSIS IN INTELLIGENCE PREPARATION OF THE BATTLEFIELD

The function of terrain analysis is to reduce the uncertainties regarding the effects of terrain on combat operations. It allows the commander to "see the battlefield" and the effects of weather on the terrain in the AO. In order to accomplish terrain analysis, the intelligence staff receives support from the engineer terrain teams or detachments. To effectively use the terrain information developed by the terrain team, intelligence personnel must understand basic terrain analysis and its applications to the IPB process. In units where terrain analyst assets are not available, the intelligence staff collects, analyzes, and integrates terrain information into the commander's decision-making process.

TERRAIN ANALYSIS PROCESS

The terrain analysis process is paramount in prebattle support. Early in the IPB process planners determine the terrain information required to support the operations at all levels. Terrain analysis emphasizes the use of graphics to depict the effects of the terrain on ground and air operations. It considers the effects of weather on the terrain and how weather influences operations. The Defense Mapping Agency (DMA) prepares much of the data base that terrain analysts use. This DMA data is produced in two standard formats: a planning terrain analysis data base (PTADB) at 1:250,000 scale and a tactical terrain analysis data base (TTADB) at 1:50,000 scale. These scales coincide with the planning and tactical maps used by the US forces. DMA standard factor overlays produced include--

- Surface configuration (slope).
- Surface drainage.
- Vegetation.
- Surface materials (soils).

Overlays produced depicting factors related to military aspects of terrain (OCOKA) are--

- Concealment from aerial detection (summer and winter seasons) .
- Obstacles (microrelief).
- Bui It-up areas.
- Transportation.
- Key terrain.
- Cross-country movement (wet and dry conditions) .

These products have a wide dissemination, but are primarily intended for use by the terrain teams in support of the IPB process.

TERRAIN FACTOR MATRIX AND TERRAIN ANALYSIS SUPPORT GUIDE

The terrain factor matrix and terrain analysis support guide are tools for the analyst. They were developed through an analysis process whereby terrain factors that impact on combat operations are identified and correlated with specific types of combat operations and battlefield functions. Figure E-1 shows a terrain analysis support guide. The terrain factor matrix was introduced in Chapter 4 (see Figure 4-4).

THE TERRAIN DATA BASE

The focus of terrain analysis support in the prebattle is on providing the combat commander with detailed planning graphics of various terrain factors. These graphics are expedient, tailored to the mission, and updated with the changing combat and weather situations. Information concerning the types and sizes of units involved (both friendly and enemy), number and types of vehicles and equipment, and type of operation is needed in this developmental stage.

The process begins with the analyses of the basic terrain factors (surface configuration, surface drainage, vegetation and surface materials, built-up areas, and transportation nets). These products are used to assess the existing situation and further used in combination to develop the factors of OCOKA and other special purpose graphics. The analyst produces overlays depicting terrain factors not found on topographic maps. These factors include, but are not limited to, fording sites, tree height, stem spacing, stem diameter and canopy closure, micro-relief, and the effects of weather on soil . This information is necessary in the development of the OCOKA graphics. The information is gathered through on-site collection, aerial reconnaissance, photographic interpretation and analysis, and other collateral sources.

Surface Configuration

Surface configuration portrays and describes the landforms and the irregularities of the earth's surface. Maneuver commanders need accurate intelligence on the surface configuration of the terrain. The aspects of the various landforms and surface irregularities affect movement of troops, equipment, and materials from one point to another. Therefore, it is necessary that the analyst prepare an accurate surface configuration overlay.

There are three principal landform groups':

- Plains (less than 150 m difference in elevation between the high point and the low point and having more that 50 percent of the area with slope less than 4 percent).

- Hills (150 to 600 m--with low hills of 150 to 300 m and high hills of 300 to 600 m).

MILITARY ASPECTS OF TERRAIN (OCOKA)	ELEMENTS OF TERRAIN INFORMATION	EXAMPLES OF TERRAIN ANALYSIS PRODUCTS
Observation and fields of fire	• Vegetation (summer and winter) • Surfare configuration • Battlefield environmental Effects on the terrain • Urban areas	• Horizontal LOS for DF weapons and radar • Emplacement suitability and performance ratings for ground surveillance
Concealment and cover	• Vegetation (summer and winter) • Surface configuration • Obstacles (micro relief) • Battlefield environmental effects on the terrain • Urban areas	• Cover potential from Direct or indirect fire (good, fair, or poor) • Concealment, potential from horizontal observation (good, fair or poor)
Obstacles	• Vegetation (summer and winter) • Surface configuration • Drainage characteristics • Natural and manmade obstacles • Micro-relief • Surface material (wet and dry) • Urban areas	• Location of exsisting natural and manmade obstacles • Mobility potential on the battlefield expressed in GO, SLOW-GO and NO-GO for both tracked and wheeled vehicles
Key Terrain	• Urban areas • LOCs • Surface configuration • Drainage characteristics	• Location of key terrain features, both natural and manmade. Examples are: bridges, chokepoints, high ground, key military installations
Avenues of approach	• Vegetation (summer and winter) • Urban areas • Surface configuration • Surface materials (wet and dry) • Drainage characteristics • LOCs	• Identification of areas where movement of friendly and enemy forces may occur • Speed prediction • LZs • DZs • Landing beaches • NOE navigation

Figure E-1. Terrain analysis support.

° Mountains (greater than 600 m with low mountains of 600 to 1500 m and h igh mountains greater than 1500 m) .

Major l and forms, naturally and culturally dissected land areas, and micro-relief are depicted. Micro-relief includes escarpments, embankments, cuts and fills, and ditches less than 2 m in height.

Relief is the difference in elevations represented by contour lines, hypsometric tints, shading, or spot elevations. Slope is the inclined surface of a hill, mountain, or any other part of the earth's surface. Slope is shown in three basic categories:

- Map unit A equals 0-30 percent slope, where the distances between contour lines can be as narrow as the lines for 30 percent or wider. Movement and maneuverability are generally unrestricted except in local areas.

- Map unit B equals 30-45 percent slope, where the distances can be as narrow as 30 percent or narrower to 45 percent. Movement for vehicles in these areas is very slow. Maneuverability is difficult for tracks and large-wheeled vehicles.

- Map unit C equals greater than 45 percent slope, where the distances between contour lines are narrower than those for 45 percent. Movement is generally precluded and maneuverability is extremely I imited. These areas are usually designated as NO-GO areas for most vehicles.

Figure E-2 shows the three basic categories of slope on a terrain and weather factor combined overlay. These categories may be further divided to obtain a more descriptive analysis.

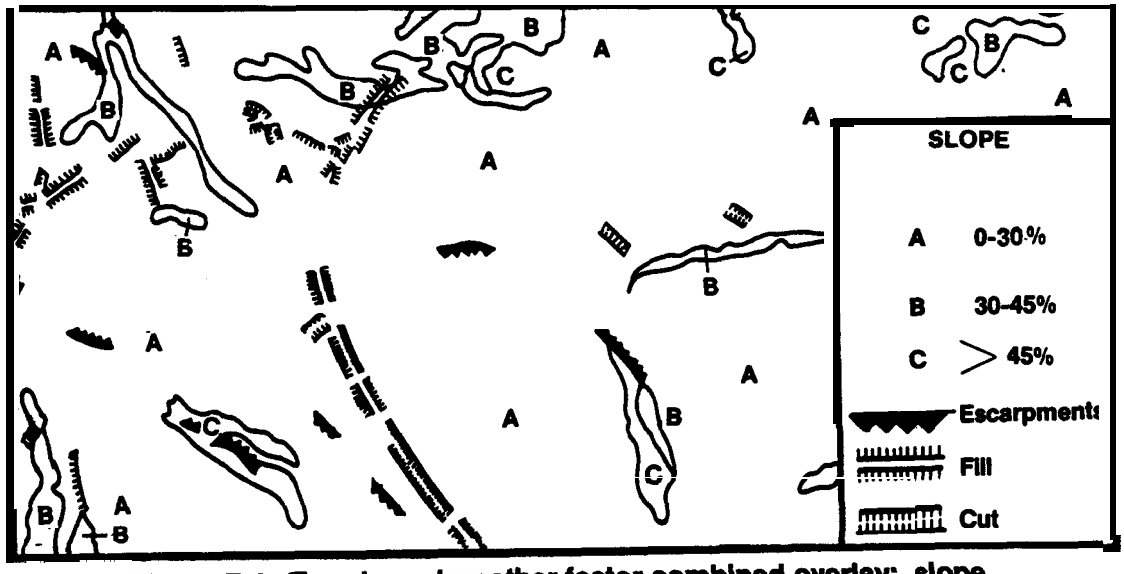
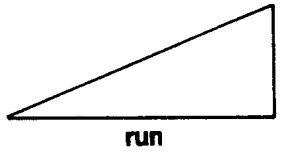
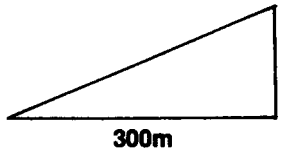


Figure E-2. Terrain and weather factor combined overlay: slope.

Slope can be expressed in three ways: first as a slope ratio (sometimes called gradient) represented as a fraction; second, as a degree of slope labeled in degrees; and third, as percent of slope. The best method of representation is the percent of slope. Figure E-3 shows how to calculate percent of slope.



$\frac{\text{rise}}{\text{run}} \times 100$



$\frac{60m}{300m} \times 100$

.2m x 100 = 20% slope

Construct a slope template of 30 and 45 percent for topographic map with a scale of 1:50,000 and a contour interval of 20m.

EXAMPLE -

1. Calculate horizontal ground distance (HD).

$$HD = \frac{\text{contour interval} \times 100}{\% \text{ slope}}$$

$$HD = \frac{20m \times 100}{30} \qquad HD = \frac{.20m \times 100}{45}$$

$$HD = 66.67m \qquad HD = 44.44m$$

2. Calculate map distance (MD).

$$MD = \frac{HD}{\text{denominator of map scale}}$$

$$MD = \frac{66.67m}{50,000} \qquad MD = \frac{44.44m}{50,000}$$

$$MD = .00133m \text{ or } 1.3mm \qquad MD = .00088m \text{ or } .9mm$$

3. Draw 1.3mm and .9mm on a stable base transparent material. This is the slope template.

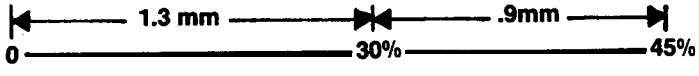


Figure E-3. Percent of slope.

Percent of slope is represented in the three categories described. Use a slope template or slope calculator to assist in determining slope categories.

A slope template or slope calculator is a device used for finding areas within a given class or slope on a topographic map. Many slope calculators have been made by various terrain detachments. These calculators show different contour densities to be used on maps at various scales with various contour intervals. They are usually reproduced by the photo lab on transparent plastic. Figure E-4 shows examples of six different slope calculators combined into one.

There are no significant weather effects on surface configuration. Most changes to surface configuration occur over long periods of time or as a result of a natural or artificial catastrophic event.

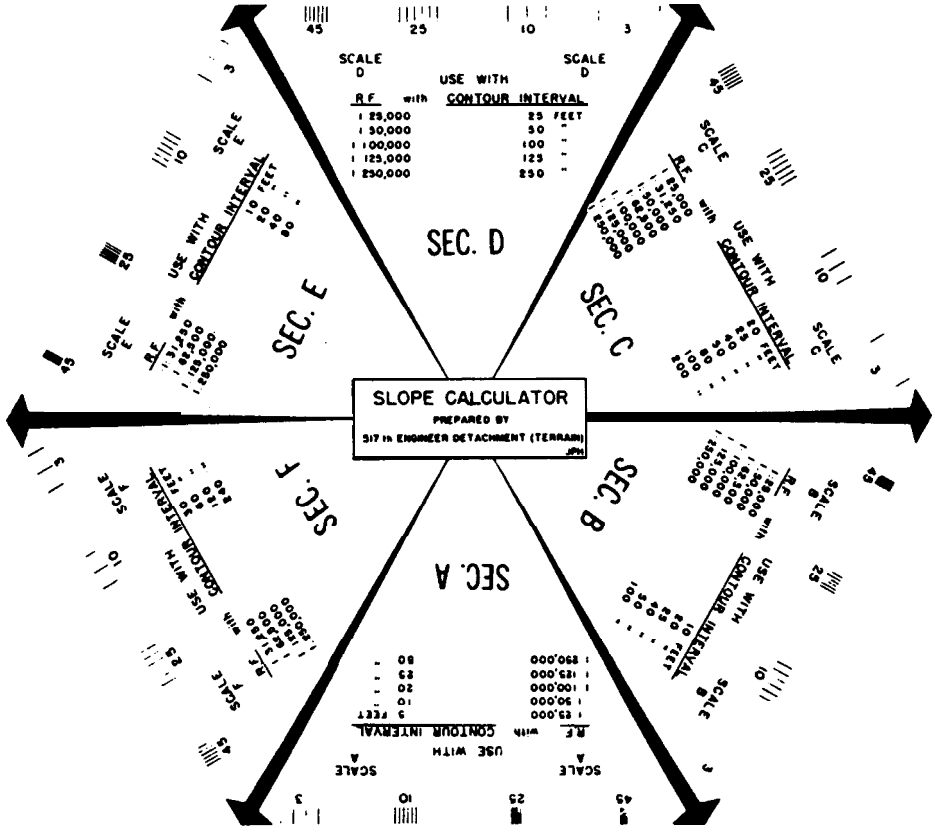
Surface Drainage

With the concept of rapid mobility, it is vital for commanders to know what watercourses exist in their AO. Surface drainage is not just identifying rivers on a map. Military planners need to know types of watercourses, watercourse characteristics, conditions of the surrounding area, and artificial features along the watercourse. Figure E-5 shows a sample watercourse and water body data card. It is essential to military operations that analysts consider seasonal and short-term weather effects.

Watercourses are classified into four types: perennial , intermittent, ephemeral , and tidal . There are also 7 drainage patterns. These are dendr itic, trellis, radial, annular, rectangular, parallel, and pinnate. Drainage patterns provide information on surface materials (soil types and geologic structure) and surface configuration. Figures E-6 through E-12 show the different drainage patterns.

Detailing is important in the preparation of the surface drainage overlay. Include a stream regime in the marginal information. This is a brief descriptive analysis of the prevalent drainage system(s) in the area. Rivers are identified as having a gap width greater than 2.84 mm and a length greater than 20 mm. Streams and canals are classified by type (perennial, intermittent, ephemeral or tidal) and by size. There are three sizes of streams:

- Less than .09 mm gap width.
- Greater than .09 mm-less than .36 mm gap width.
- Greater than .36 mm gap width.



Each section, A through F, is actually a separate calculator. Select one section for an example.

To measure a 45 percent slope-
Use the contour density in section "C," because you are given a map with:
- **an RF of 1:25,000,**
  and
- **a contour interval of 20 ft.**

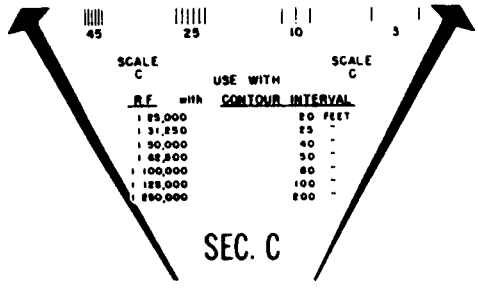
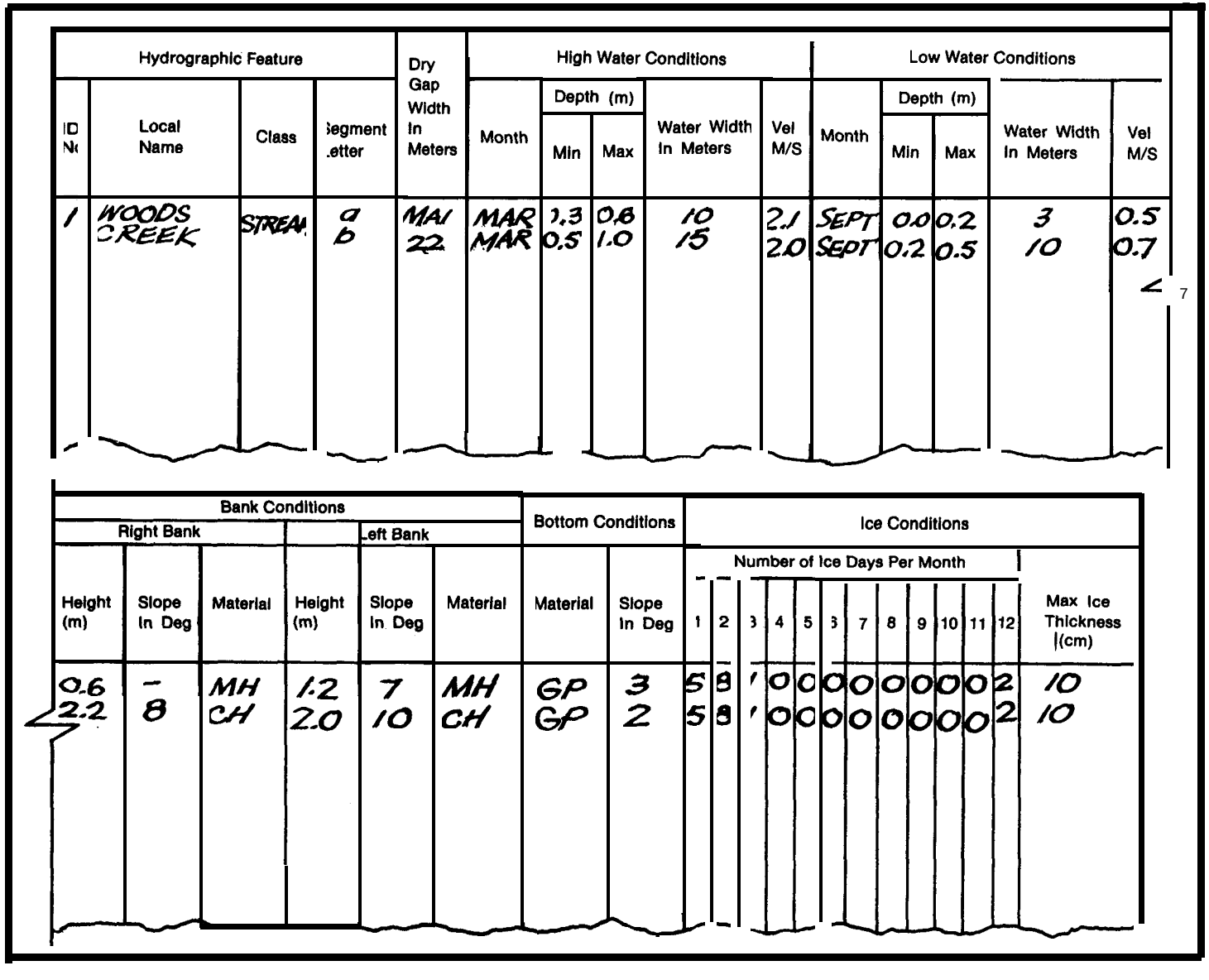


Figure E-4. Slope calculator examples.



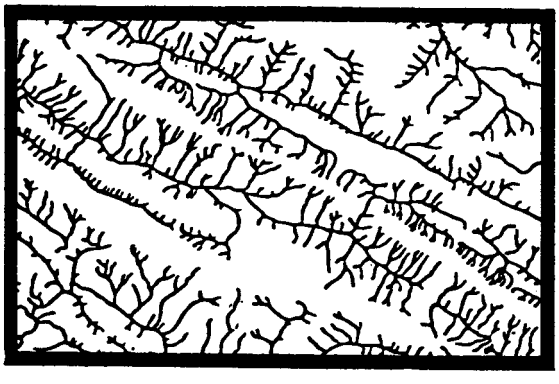
Hydrographic Feature				Dry Gap Width In Meters	High Water Conditions					Low Water Conditions				
ID No	Local Name	Class	Segment Letter		Month	Depth (m) Min	Depth (m) Max	Water Width In Meters	Vel M/S	Month	Depth (m) Min	Depth (m) Max	Water Width In Meters	Vel M/S
1	WOODS CREEK	STREAM	a	MAI	MAR	1.3	0.8	10	2.1	SEPT	0.0	0.2	3	0.5
			b	22	MAR	0.5	1.0	15	2.0	SEPT	0.2	0.5	10	0.7

Bank Conditions						Bottom Conditions		Ice Conditions												
Right Bank			Left Bank					Number of Ice Days Per Month												
Height (m)	Slope In Deg	Material	Height (m)	Slope In Deg	Material	Material	Slope In Deg	1	2	3	4	5	6	7	8	9	10	11	12	Max Ice Thickness (cm)
0.6	-	MH	1.2	7	MH	GP	3	5	8	1	0	0	0	0	0	0	0	0	2	10
2.2	8	CH	2.0	10	CH	GP	2	5	8	1	0	0	0	0	0	0	0	0	2	10

Figure E-5. Watercourses and water bodies data.

A random developed, tree-like pattern composed of branching tributaries to a main stream. It is the most common pattern and is characteristic of essentially flat-lying and relatively homogeneous material.

Figure E-6. Dendritic drainage pattern.

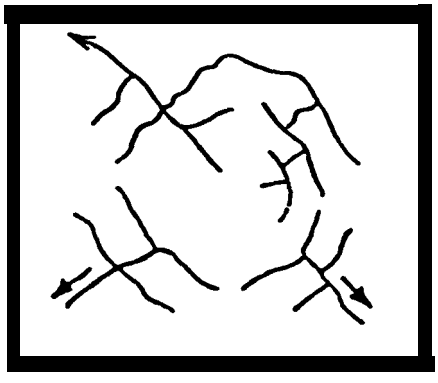


A modified version of the dendritic pattern. Main streams generally flow parallel with the tributaries joining at right angles. This pattern is indicative of bedrock structure where rock strata have been folded and main streams now follow the strike of the rock units.

Figure E-7. Trellis drainage pattern.

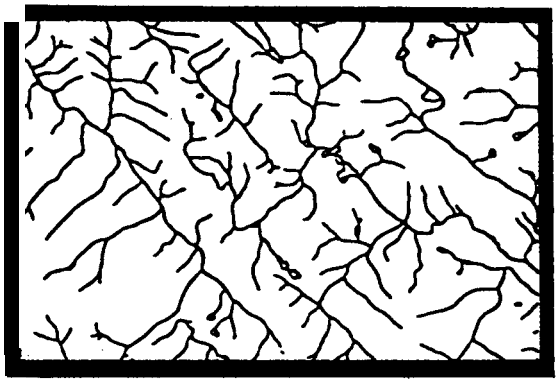
This pattern is characterized by a network of channels, almost parallel, flowing away from a central high point. It is found on dome structures, isolated round hills, or volcanic cones.

Figure E-8. Radial drainage pattern.



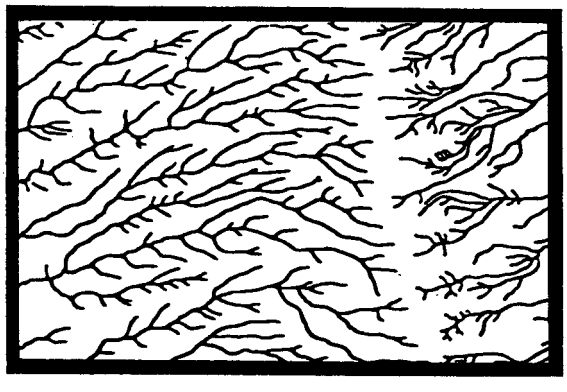
Usually associated with radial drainage, as where sedimentary rocks are upturned by a dome structure. Joints or fractures may control the flow of the tributaries to provide a parallel aspect. Primary drainage will circle around a central high area.

Figure E-9. Annular drainage pattern.



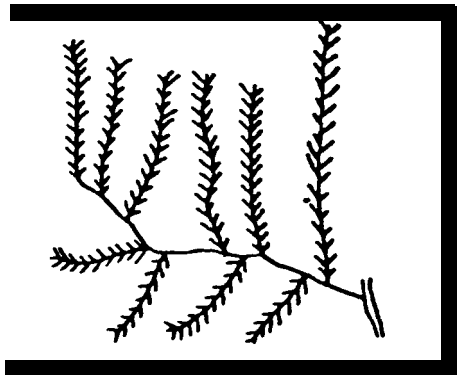
Sometimes called angulate, (rectangular dendritic or angular dendritic) this pattern is also a modified version of the dendritic pattern. It is characterized by abrupt, close to 90 degree, changes in stream directions and distinct obtuse or acute angles of stream juncture. This pattern is generally caused by faulting or jointing of the underlying bedrock. It is usually associated with massive igneous and metamorphic (intrusive) rocks, though it may be found in any rock type.

Figure E-10. Rectangular drainage pattern.



This drainage pattern is characterized by major streams that are trending in the same direction. Parallel streams are indicative of gently dipping beds of uniformly sloping topography. Tributaries characteristically join the mainstream at approximately the same angle. Extensive, uniformly sloping basalt flows and young coastal plains exhibit this drainage pattern. On a smaller scale the slopes of linear ridges may also reflect this pattern.

Figure E-11. Parallel drainage pattern.



This is a hybrid form of a fine dendritic pattern. It strongly resembles a feather structure in appearance. The gullies have steep, nearly vertical walls, profusely rilled with possible pinnacle development. The bottoms are generally flat and broad.

Figure E-12. Pinnate drainage pattern.

An important consideration of streams and rivers are crossing sites for fording, swimming, and bridging, and bank conditions. Most trucks can ford depths up to three feet, most tanks up to four feet. Velocity should be less than five feet per second. Vertical banks greater than one foot stop trucks and greater than four feet stop tanks. Figure E-13 shows a sample surface drainage overlay. See terrain matrix (Figure 4-4) for surface drainage applicability.

Precipitation has a tremendous effect on hydrologic features and adjacent areas. It affects watercourse depths, velocities, and bank slope conditions. Evaluate flood plains and areas subject to inundation. The lack of precipitation also plays an important role in the evaluation of rivers and streams. The absence of water in various channels and flats provides concealed movement routes, however, use caution and give attention to weather forecasting when considering these routes. Wind affects velocity and surface turbulence on the larger watercourses.

Vegetation

Vegetation has a significant effect on many types of military activities and is considered carefully in planning operations. There are many ways vegetation affect military tactics, decisions, and operations. Perhaps the most important is concealment. Concealment is the ability to move troops, vehicles, and equipment without being detected from the ground or air.

Vegetation is defined as the natural plant cover characteristic of an area. There are four types of vegetation:

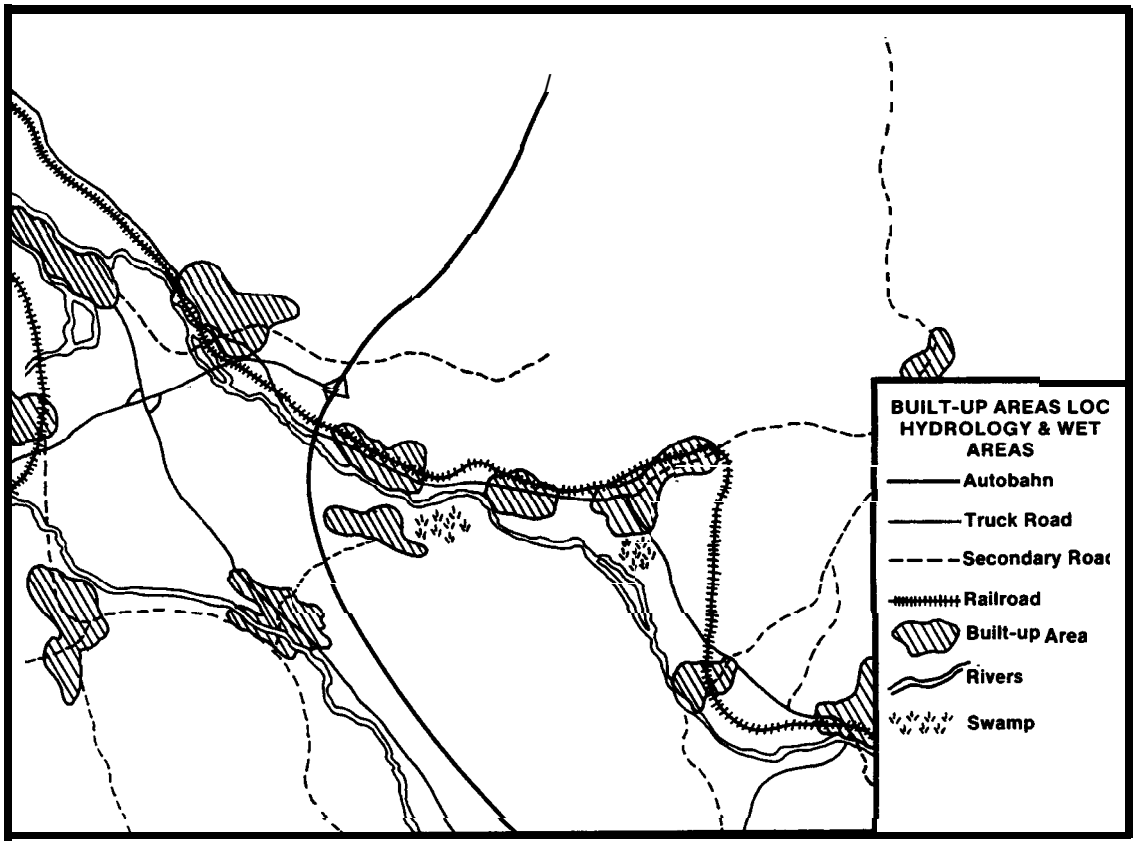


Figure E-13. Built-up areas, LOC and hydrology overlay.

- Trees are greater than 3.05 m tall, perennial wood plants, single sterrrned, with a definite crown shape. They are either of the deciduous or coniferous variety.

- Scrub and shrub. Scrub is vegetation noted by its stunted growth due to poor soil or climatic conditions. Shrub is the undergrowth of the forested areas, normally the dominant vegetation. It is either deciduous or coniferous.

- Grasses are all non-woody plants (grasses and forbs) . hey are classified as tall or short grasses depending on height (less than one meter is short, greater than one meter is tall).

- Crops are defined as cultivated vegetation (vineyards, arms, plantations, orchards, and fields).

Ground reconnaissance of vegetation provides the analyst with the necessary vegetation information to determine concealment possibilities. Reconnaissance allows the analyst to take precise measurements, thus producing a graphic or greater accuracy. Current aerial photography is

essential to accurate analysis of vegetation. The best altitude for photography for this analysis is less than 12,500 feet for accuracy within 10 percent. Altitude should not exceed 16,000 feet.

Areas are at least one square kilometer in size to be depicted on the overlay. It is important to check the surface drainage overlay to ensure the vegetation coincides on both overlays.

Vegetation annotated are those areas marked or those areas greater than 5 mm in size. Stands with more than 60 percent coniferous vegetation are designated as coniferous (C), with more than 60 percent deciduous vegetation are labeled as deciduous (D), and stands with mixed vegetation (C+D)) in 40-60 percent combinations are marked with an E. Use standard symbology for other vegetation types (orchards, vineyards, and swamps). Indicate height and canopy closure for each vegetation type.

Figure E-14 shows mapping capabilities for vegetation data elements in the US, USSR, and Federal Republic of Germany. Figure E-15 shows a sample vegetation overlay. See terrain matrix (Figure 4-4) for vegetation applicability.

Concealment from aerial detection is determined from vegetation type, percent of canopy closure, stem spacing, and vegetation height. Canopy closure is normally computed for forested areas and is defined as the percentage of ground area covered by the tree crown area. Canopy closure has four categories:

- Category 1 - 0-25 percent closure (poorest concealment).
- Category 2 - 25-50 percent closure.
- Category 3 - 50-75 percent closure.
- Category 4 - 75-100 percent closure (best concealment).

In categories two and three, concealment depends on the forest mixture of coniferous and deciduous trees. Tree height and canopy closure hinder visibility, while stem diameter and vegetation density (stem spacing) impede movement and maneuverability. Intervals less than 20 feet in spacing greatly restrict maneuverability. Forested areas with stem diameters greater than 2 inches stop wheeled vehicles (6-8 inches for tracks). The vehicles are able to knock down the trees; however, the brush pileup forms a significant obstacle.

Precipitation and wind affects vegetation by limiting or increasing visibility. Precipitation also impacts on the effects of vegetation on trafficability. Consider the fire potential of extremely high temperatures in conjunction with the lack of precipitation.

Surface Materials

The analysis of soils for military planners has two purposes: first for the engineering and construction uses and second, for military

	UNITED STATES		FEDERAL REPUBLIC GERMANY		USSR	
DATA ELEMENT	1:250,000	1:50.000	1:250,000	1:50,000	1:200,000	1:50,000
1. Map unit identification and vegetation boundaries	Limited to major vegetation boundaries	Limited to major vegetation boundaries	Limited to major vegetation boundaries	Limited to major vegetation boundaries	Limited to major vegetation boundaries	Limited to major vegetation boundaries
2. Mean height to top of canopy	Woodland 3m Scrub 3m	Woodland 3m Scrub 3m	No	No	Yes	Yes
3. Percent canopy closure by season	Limited estimate for major vegetation type	Limited estimate for major vegetation type	Limited	Limited	Limited	Limited
4. Number of stems per hectare	No	No	No	No	No	No
5. Crown diameter	No	No	No	No	No	No
6. Mean stem diameter	No	No	No	No	Yes	Yes
7. Number of trees in each stem diameter class per hectare	No	No	No	No	No	No
8. Stem Spacing	No	No	No	No	Yes	Yes
9. Species identification, seasonality, and distribution	No No No	No No No	Coniferous Deciduous Mixed only	Coniferous Deciduous Mixed only	Coniferous Deciduous Mixed only	Coniferous Deciduous Mixed only
10. Ground cover type, percent of cover, and height	No	No	No	No	No	No
11. Litter type and depth	No	No	Limited	Limited	Limited	Limited
12. Mean height to lowest branches	No	No	No	No	Limited	Limited
13. A representative transect	No	No	No	No	No	No

Figure E-14. Map capabilities for vegetation data elements.

operations, specifically, trafficability. Surface materials are important because of their influence on drainage, vegetation, field fortifications, and trafficability.

Surface materials are broken down into two groups, soils and rocks. Soils are of unconsolidated parent materials and are often called deposits or materials. Rocks are from consolidated parent material.

The Unified Soils Classification System is the system used in determining soil types and characteristics. There are several

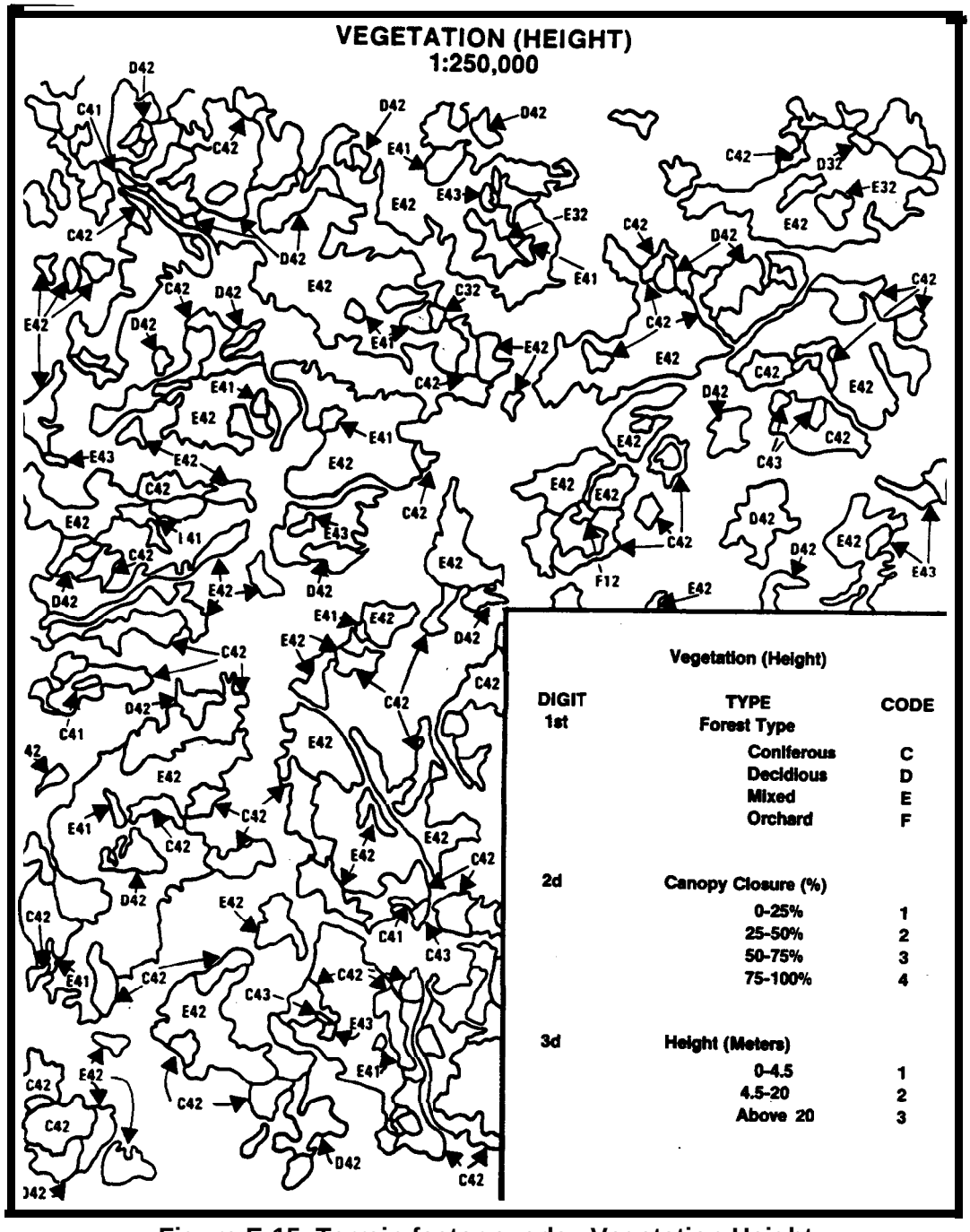


Figure E-15. Terrain factor overlay Vegetation Height.

characteristics needed to produce a surface materials (soils) overlay. The analyst identifies soil composition as either fine-grained, coarse-grained, or organic soils. Figure E-16 shows a sample soil classification chart. Figure E-17 shows a surface material overlay that further explains the classification designations. The first digit is the predominant soil, the second digit is a characteristic description. Surface roughness is depicted in the third digit. The following example further depicts the classification system.

GW1: Well-graded gravels, gravel-sand mixtures with little or no fines. Soil has no roughness effect. This soil is generally free of moisture. Soil depth is less than 5 meters.

Note: The subscript character indicates moisture and soil depth.
. . . indicates soil is normally moist.
_ _ _ indicates soil is normally wet.
_____ indicates soil depth is less than 5 meters.

Other characteristics needed are an analysis of remoldability, soil depth in meters, moisture content, and soil horizonation. Remoldability is the tendency for a soil to change strength with traffic. Soil depth is measured in meters and is classified as--

- Class 1 - 0 - .5 meters deep,
- Class 2 - .5 - 1.5 meters deep.
- Class 3- 1.5- 3.0 meters deep.
- Class 4 - more than 3.0 meters deep.

Soil moisture content (the ability of the soil to retain moisture) must consider daily and seasonal changes. Soil horizonation (or layering) is the natural division of the unconsolidated material into three basic layers. The three layers are: layer A - surface materials; layer B - subsurface materials; and layer C - materials of the consolidated parent material . Other sublayers may be present.

A surface materials overlay breaks down the most probable soil types, characteristics, and distribution. Depicted on a soils overlay (surface configuration) are comrnon soil types along with exposed rock outcrops (R), peat (PT), evaporates (E) and permanent snowfields (PS).

SOIL TRAFFICABILITY

The capability of a soil to withstand traffic is referred to as the soil strength or soil trafficability. Factors affecting soil trafficability are soil type, characteristics and conditions (wet or dry), vehicle type and vehicle cone index, and the soils rating cone index. A rating cone index is the product of the measured cone index and the remolding index. The vehicle cone index is the minimum soil strength that permits a given vehicle to complete 1 pass and 50 passes over a section of terrain. See TM 5-330 for the various vehicles and tables. The analysis

Major Divisions			Group Symbols	Typical Names	Field Identification Procedures (Excluding particles larger than 3 in and basing fractions on estimated weights)		
1	2		3	4	5		
More than half of material is larger than No 200 sieve size.	Gravels More than half of coarse fraction is larger than No. 4 sieve size. (For visual classification, the 1/4-in. Size may be used as an equivalent to the No. 4 sieve size).	Clean Gravels (Little or no fines)	GW	Well-graded gravels, gravel-sand mixtures, little or no fines	Wide range in grain sizes and substantial amounts of all intermediate particle sizes		
			GP	Poorly graded gravels or gravel-sand mixtures, little or no fines	Predominantly one size or a range of sizes with some intermediate sizes missing		
		Gravel With Fines (Appreciable amount of fines)	GM	Silty gravels, gravel-sand-silt mixture	Nonplastic fines or fines with low plasticity (for identification procedures see ML below)		
			GC	Clayey gravels, gravel-sand silt mixtures	Plastic fines (for identification see CL below)		
	Sands More than half of coarse fraction is smaller than No. 4 sieve size.	Clean Sands (Little or no fines	SW	Well-graded sands, gravelly sands, little or no fines	Wide range in grain sizes and substantial amounts of all intermediate particle sizes		
			SP	Poorly graded sands or gravelly sands, little or no fines	Predominantly one size or a range of sizes with some intermediate sizes missing		
		Sands With Fines (Appreciable amount of fines)	SM	Silty sands, sand-silt mixtures	Nonplastic fines or fines with low plasticity (for identification procedures see ML below)		
			SC	Clayey sands, sand-clay mixtures	Plastic fines (for identification procedures see CL below)		
					Identification Procedures on Fraction Smaller than No. 40 Sieve Size		
					Dry Strength (Crushing characteristics)	Dilatancy (Reaction to shaking)	Toughness (Consistency near PL)
More than half of material is smaller No 200 sieve size The No. 200 sieve size is about the smallest particle visible to the naked eye.	Silts and Clays Liquid limit is less than 50		ML	Inorganic silts and very fines sands, rock flour, silty or clayey fine sands or clayey silts with slight plasticity	None to slight	Quick to slow	None
			CL	Inorganic clays of low to medium plasticity, gravelly clays, sandy clays silty clays, clean clays	Medium to high	None to very slow	Medium
			OL	Organic silts and organic silty clays of low plasticity	Slight to medium	Slow	Slight
	Silts and Clays Liquid limit is greater than 50		MH	Inorganic silts, micaceous or diatomaceous	Slight to medium	Slow to none	Slight to medium
			CH	Inorganic clays of high plasticity, fat clays	High to very high	None	High
			OH	Organic clays of medium to high plasticity, organic silts	Medium to high	None to very slow	Slight to medium
Highly Organic Soils			Pt	Peat and other highly organic soils	Readily identified by color, odor spongy feel and frequently by fibrous texture		

Figure E-16. Unified soil classification chart.

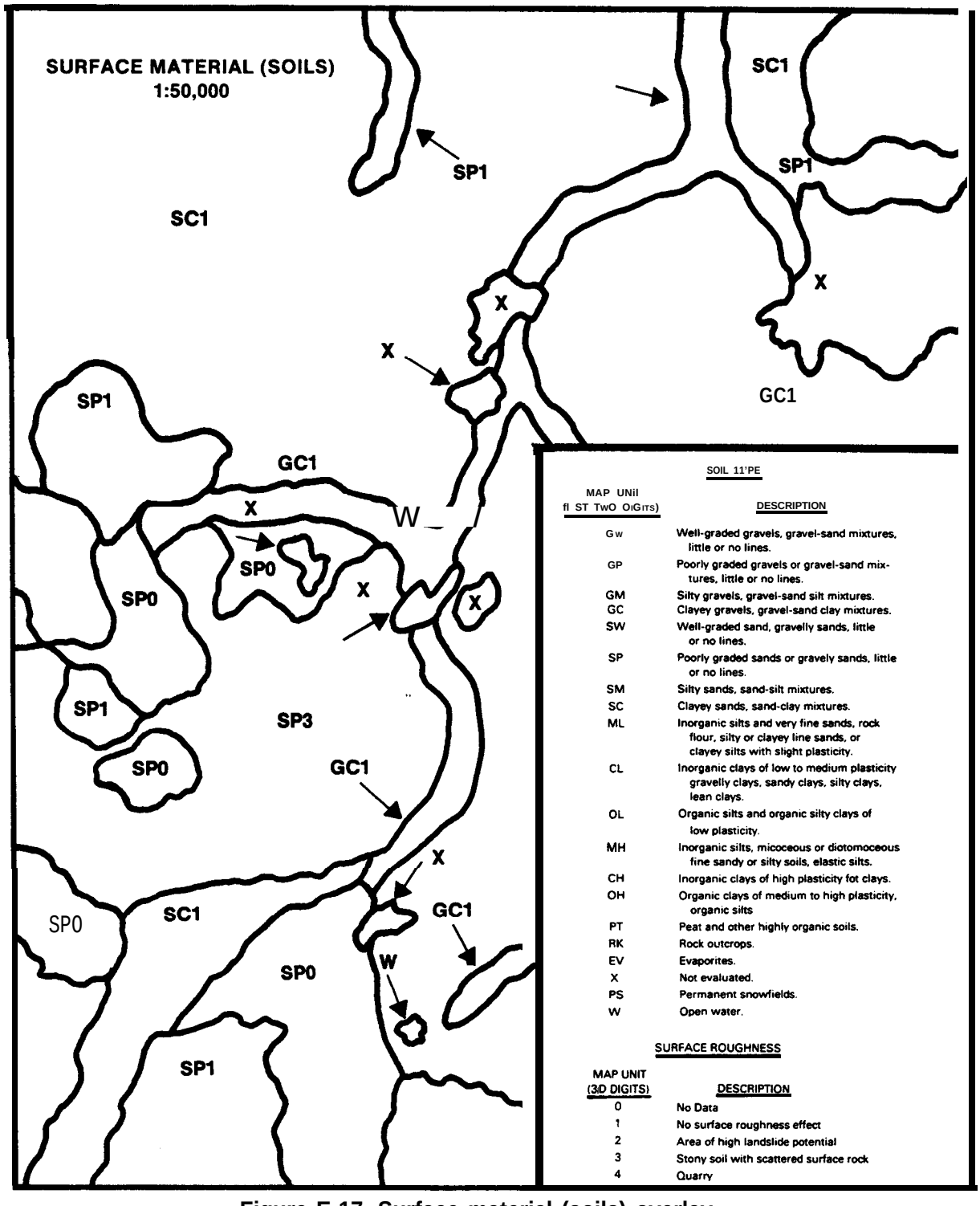


Figure E-17. Surface material (soils) overlay.

of soil trafficability is used in determining cross-country movement and vehicle maneuverability. (See Figures 4-5 and 4-6 for examples of over lays.)

Precipitation affects trafficability by changing the physical properties and characteristics of the soil and the consolidated parent material . Wind also is important because it decreases the drying time of inundated areas. Wind reduces visibility by creating dust plumes in exceptionally dry areas.

MILITARY ASPECTS OF TERRAIN - OCOKA

Terrain analysis focuses on the military aspects of the terrain known collectively as OCOKA. Military aspects of the terrain are observation and fields of fire, concealment and cover, obstacles, key terrain, and avenues of approach and mobility corridors.

Observation and Fields of Fire

Observation involves the influence of the terrain on reconnaissance, surveillance (optical and electronic LOS), and TA. Intervisibility is extremely important. Intervisibility is the unobstructed view from point A to point B. It is the ability to see from one station to another station. Vegetation is particularly effective in limiting observation on plains and plateaus. Prominences that could provide a commanding position are generally lacking. In areas bare of trees, long distance observation is good. The rugged topography of hills and mountains offers variable observation. Terrain masking is the concealment of areas from direct horizontal optical and electronic LOS by terrain features. Masking plays an important role in communications and surveillance techniques and systems emplacement. Consider LOS (intervisibility and masking effects) for various electronic and optical systems. (See Figure 4-12.)

FofF is the effect that the terrain has on weapons and weapons systems effectiveness. LOS is considered for LOS direct fire weapons. Indirect fire should consider surface configuration at the target site. It is important to indicate distance and direction of observation. For FofF indicate direction, trajectory angle for indirect fire to clear vegetation (or other obstructions) from a specific point, and the extent of the firing fan. (See Figure 4-11.)

Concealment and Cover

Concealment is protection from air and ground observation. Cover is protection from the effects of fire, both direct and indirect. Concealment and cover is derived from the surface configuration, vegetation, and built-up area overlays. Slopes greater than 30 percent, dense forested areas, and large bui lt-up areas offer good cover. Fair cover is outl ined by slopes 10-30 percent, medium forest density, and medium built-up areas. A medium built-up area is equal to nine square kilometers. It is important to accurately calculate percent of roof coverage of a built-up area when determining concealment. The best

concealment is described as O-25 percent chance of detection. Concealment is evaluated for summer and winter seasons.

Cover, concealment, or defilade in the plains regions is generally poor. Those areas having low topographic features (micro-relief), such as escarpments, cuts and fills, and embankments afford some protection. The rugged terrain of the hills and mountainous regions provide abundant opportunity for concealment and cover. Above the timberline movement across most slopes or crests is exposed to view in many directions.

Obstacles

Obstacles are natural or artificial features that stop, impede, or divert military movement and maneuverability. Obstacles occur on the ground and in the air. The effects of removing, overcoming, or bypassing the obstacles must be considered in the planning of the overall operation, Hills and mountains usually are considered obstacles to movement and generally favor the defense. History records many cases in which forces inferior in numbers and equipment have held off superior attackers in mountainous areas. There have been many instances in which such obstacles have been effectively achieved by moving over the hilly and mountainous terrain instead of through adjacent corridors where the enemy was prepared. However, factors unfavorable to troop movement must be considered. These conditions include difficulty in movement, lack of maneuvering space, and the vulnerability of the LOC. Consider vegetation, built-up areas, and surface drainage, in addition to the surface configuration and micro-relief features in determining obstacles.

Key Terrain

Key terrain is any feature or area, natural or artificial, that the seizure or control of offers a marked tactical advantage to the occupant over the opposing force. Examples of natural key terrain features include DZS, high ground, route constrictions or choke points, and fording sites. Manmade key terrain features are a little harder to define. These include key bridges, communications and logistics sites, major built-up areas (urban, industrial, or commercial), major transportation centers (airports, rail facilities, ports and harbors, and roadway networks). Significant military, political, or governmental facilities and installations are considered key terrain.

It is important to be selective in determining what features are key. Selective criteria includes the following questions: Will control of this feature provide me with a tactical advantage over the enemy? Is control of this feature crucial to the success of the mission? Is this feature along a major LOC or in a major MC? How will weather affect this feature? What size force can this feature accommodate and are there ready access routes? Additional considerations in selecting key terrain includes concealment and cover and observation and FofFs. It is important to indicate why the selected features are considered key terrain and what effect control has on friendly and enemy forces.

Avenues of Approach and Mobility Corridors

AAs and MCS are routes by which a force may reach key terrain or an objective. AAs and MCs address maneuver support potential, degree of canal ization, concealment and cover, observation and FofFs, obstacles, and the access to key terrain and adjacent avenues or corridors. There are three types of AAs: ground, air, and rear area AAs.

Ground Avenues of Approach. A ground AA is broad enough and contains sufficient MCs to support rapid movement and maneuver of forces along its entire course. It should be free of obstacles. If obstacles are present they should be few in number and require reasonable engineer support to remove them. The avenue also affords good to excellent concealment and cover.

Air Avenues of Approach. These are much the same as ground avenues. They should be free of obstructions or have adjacent corridors to permit bypass of obstructions. It is important to consider avenues and corridors in layers as to reflect different altitudes of approach. This considerate ion would depend on the level and size of the operation.

Rear Area Avenues of Approach. These are avenues that provide the rap id movement of rear threat elements and the additional service support elements to the front l ines.
Note: It is extremely important to indicate the width of the avenues and corridors and what size element can pass through. Note any major choke points that canalize movement along the AA into designated MCs as key terrain. (See Figure 4-13 for examples of AAs and MCs.)

THE MODIFIED COMBINED OBSTACLES OVERLAY

The MCOO is the graphic terrain analysis on which all other IPB products are based. It is one of the two templates (the other being the DST) that is always prepared at all echelons. At echelons where the IPB process is more formal, the terrain analyst produces detailed combined obstacles overlays and AA overlays that may be combined or modified to form the basis of the MCOO. At lower echelons however, the MCOO is normally prepared by the intelligence staff as a single graphic.

A combined obstacles overlay is made up of built-up areas, LOCS, surface drainage, surface configuration (including micro-relief), surface materials, and vegetation. These component factors reflect average weather effects for wet and dry conditions. These features are outlined, highlighted, or marked to show their significance to movement and maneuverability. There are three movement categories: NO-GO, SLOW-GO, and GO.

A MCOO is produced for the IPB process when key terrain features, AAs and MCs for air and ground forces, and a friendly operations graphic are added to the combined obstacles overlay. Detail depends on the level and type of operation. The MCOO contains at a minimum registration marks, classification, titling data, and a legend. As a general rule the following information is depicted:

- NO-GO terrain.
- SLOW-GO terrain.
- Built-up areas.
- LOCs.
- Rivers and water obstacles.
- Obstacles.
- Key terrain.
- AAs and MCs.
- Objectives.

CONCLUSION

Weather and terrain have more impact on the battle than any other physical factor, including weapons, equipment, or supplies. The terrain on which battles are fought presents opportunities to both sides. Most battles are won by the forces that use the terrain and weather to their advantage in both offensive and defensive operations. The resurgence of terrain analysis in today's Army and the recognition of terrain as a potent multiplier of combat power makes each of us responsible for terrain information.

GLOSSARY

Acronyms and Abbreviations

AA	avenue of approach
AAA	air avenue of approach
AAG	Army artillery group
AD	air defense
ADA	air defense artillery
ADM	atomic demolition munitions
ADP	automatic data processing
ADPS	automated data processing system
adv	advance
AE	aerial exploitation
AF	Air Force
AFCENT	Allied Forces Central Europe
AFSCOORD	assistant fire support coordinator
AI	area of interest
AIIF	Automated Installation Intelligence File
AKA	also known as
AMC	Army Materiel Command
ammo	ammunition
AO	area of operations
AOB	air order of battle
AP	antipersonnel
APC	armored personnel carrier
appl	application
approx	approximately
arty	artillery
AS	aerial surveillance
ASAS	all-source analysis system
ASL	authorized stockage list
ASPS	all-source production section
at	antitank
ATGL	antitank guided launcher
ATGM	antitank guided missile
AUD	arbitrary unit designator
Aug	August
AW	air warning
AWS	Air Weather Service
BAT-D	battlefield deception
BDA	battle damage assessment
bde	brigade
BE	basic encyclopedia
BICC	battlefield information coordination center
bks	barracks
bldg	building
BMCT	beginning of morning civil twilight
BMNT	beginning of morning nautical twilight

BMP	designation of a type of Soviet armored personnel carrier
bn	battalion
BOMREP	bombing report
BTF	battalion task force
btrv	battery
C	coniferous
C^2	command and control
C^3	command, control , and communications
C^3CM	command, control , and cormnunications countermeasures
CAA	combined arms army
cal	caliber
CARVE	criticality, accessibility, recuperability, vulnerability, and effect
CAS	close air support
cav	cavalry
CB	chemical biological
cc	cloud cover
CDP	company distributing point
cdr	commander
C-E	Communications-Electron ics
CEWI	combat electronic warfare and intell igence
CFA	covering force area
CG	commanding general
cGy/hr	centiGray hour
C-HUMINT	counter human intelligence
cl	counter inte l ligence
CIA	Central Intelligence Agency
CIAS	counterintelligence analysis section
CID	Criminal Investigation Division
C-IMINT	counter imagery inteligence
cm	centimeter
CM&D	countermeasures
CML	collection management and dissemination
COA	chemical
co	course of action
COL	company
COLT	colonel
comd	combat observation and laser team
COMINT	command
COMMZ	communications intelligence
COMSEC	communications zone
COMZEALAND	communications security
CONUS	Commander, Allied Land Forces, Zealand
coord	Continental United States
COP	coordinate
COSCOM	command observation post
CP	corps support command
CPA	command post
CPFL	collection planning aid
CPS	Contingency Planning Facilities List
	characters per second

CPT	captain
CRT	cathode-ray tube
CRTA	commander rocket troop artillery
CS	combat support
CSA	corps support activity
CSG	corps support group
C-SIGINT	counter signals intelligence
Css	combat service support
CTL	critical task list
CTOC	corps tactical operations center
CTOCSE	corps tactical operations center support element
CTT	commander's tactical terminal
CUBIC	Commnon Users Baseline for the Intelligence Commnunity
CUCV	commercial utility cargo vehicle
CW	continuous wave

D	deciduous
DA	Department of the Army
DAG	division artillery group
DATEXT	data extract
DBMS	data base management system
DCS	Defense Communications System
def	defense
deg	degrees
DF	direction finding
DIA	Defense Intelligence Agency
div	division
D1VARTY	division artillery
DMA	Defense Mapping Agency
DMz	demilitarized zone
DOD	Department of Defense
DOI	date of information
DP	decision points
DS	direct support
DST	decision support template
DTG	date-time group
DTOC	division tactical operations center
DTOCSE	division tactical operations center support element
DZ	drop zone

E	evaporates (soil type)
ea	each
EAC	echelons above corps
EACIC	echelons above corps intelligence center
EAM	event analysis matrix
ECB	echelons corps and below
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
EECT	end of evening civil twilight
EEFI	essential elements of friendly information
EEI	essential element of information

EENT	end of evening nautical twilight
EEOB	enemy electronic order of battle
elm	e l ement
EMCON	emission control orders
en	enemy
engr	engineer
EOB	electronic order of battle
EPL	ELINT parameters list
EPW	enemy prisoner of war
ESM	electronic warfare support measures
est	estimated
EW	electronic warfare
F	Fahrenheit
FA	field artillery
FAC	forward air controller
FAIO	field artillery intelligence officer
FBI	Federal Bureau of Investigation
FEBA	forward edge of the battle area
FIST	fire support team
FLOT	forward line of own troops
FM	field manual
FO	forward observer
Fof F	field of fire
FP	field post
FPN	field post number
FRAGO	fragmentary order
FRG	Federal Republic of Germany
FROG	free rocket over ground
FS	fire support
FSCOORD	fire support coordinator
FSE	fire support element
FSO	fire support officer
ft	feet
FVD	full unit designation
fvdfwd	forward
G1	Assistant Chief of Staff, G1 (Personnel)
G2	Assistant Chief of Staff, G2 (Intelligence)
G3	Assistant Chief of Staff, G3 (Operations and Plans)
G4	Assistant Chief of Staff, G4 (Logistics)
G5	Assistant Chief of Staff, G5 (Civil Affairs)
GE	Germany
GEOREF	Geographic Reference System
GMT	Greenwich Mean Time (Zulu)
GPS	grid producing source
GS	general support or general staff
GSR	ground surveillance radar
GTA	government training aid

HB	high burst
HD	horizontal ground distance
HF	high frequency
HHC	headquarters and headquarters company
HOTPHOTOREP	hot (high priority) photographic report
how	howitzer
HPT	high payoff target
HQ	headquarters
hr	hour
HUMINT	human intelligence
hv	heavy
HVT	high value target
hwy	h i ghway

1A	imagery analysis
ID	identification
I DAD	internal defense and development
I ED	imitative electronic deception
I EW	intelligence and electronic warfare
I FV	infantry fighting vehicles
IIR	intelligence information report
IMINT	imagery intelligence
inf	infantry
I NSCOM	Intelligence and Security Command
i nst I	installation
intg	interrogation
I NTREP	intelligence report
I NTSUM	intelligence summary
I PB	intelligence preparation of the battlefield
IPIR	initial programmad interpretation report
IR	information requirements
I TAC	Intelligence and Threat Analysis Center

JCS	Joint Chiefs of Staff
J2	Intelligence Directorate
J3	Operations Directorate

KIA	killed in action
km	kilometer
kph	kilometers per hour

LIC	low-intensity conflict
LOC	lines of communication
LOS	line of sight
LP	listening post
LTG	lieutenant general
LZ	landing zone

m	meter
maint	maintenance
MAJ	major
MAS [NT	measurement and signature intelligence
ma x	max i mum
MBA	main battle area
MC	mobility corridor
MCOO	modified combined obstacles overlay
MD	map distance
MDC I	multidiscipline counterintelligence
MDC I SUM	multidiscipline counterintelligence summary
mech	mechanized
MED	manipulative electronic deception
METT-T	mission, enemy, terrain, troops, and time available
MG	machinegun; major general
MI	military intelligence
MIJI	meaconing, intrusion, jamming, and interference
MIJIFEEDER	meaconing, intrusion, jamming, and interference report feeder
min	minute or minimum
MISREP	mission report
mm	millimeter
MOD	mobile obstacle detachment
mort	mor tar
MOPP	mission oriented protective posture
MORTREP	mortar bombing report
MOV	military owned vehicle
MP	military police
MR	motorized rifle
MRB	motorized rifle battalion
MRC	motorized rifle company
MRD	motorized rifle division
MRR	motorized rifle regiment
m/s	meters per second
msg	message
msl	missile
MSR	main supply route
MTLR	moving target-locating radar
mtr	motor
mvr	maneuver

NA I	named areas of interest
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NBCE	nuclear, biological, and chemical element
NCO	noncommissioned officer
NLT	no later than
no	number
NSA	National Security Agency
NTR	nothing to report
NW	northwest

06	order of battle
obj	object
OCOKA	observation and fields of fire, concealment and cover, obstacles, key terrain, avenues of approach, and mobility corridors
off	officer
OIC	officer in charge
OMG	operational maneuver group
OP	observation post
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security
org	organization
PERINTREP	periodic intelligence report
PERINTSUM	periodic intelligence summary
PIR	priority intelligence requirement
PL	phase line
PLL	prescribed load list
plt	platoon
PM	provost marshal
POL	petroleum, oils, and lubricants
pos	position
ps	permanent snowfields
Psns	positions
PSYOP	psychological operations
pt	peat
PTADB	planning terrain analysis data base
ptl	patrol
PTR/P	paper tape reader/punch
R	rock outcrops
R&D	research and development
R&S	reconnaissance and surveillance
RAG	regimental artillery group
RATT	radio teletypewriter
RC	reserve component
RD	road
REC	radioelectronic combat (not a US term)
RECCEXREP	reconnaissance exploitation report
recon	reconnaissarnce
regt	regiment
res	reserve
RF	representative fraction
RII	request for intelligence information
ROIPB	rear operations intelligence preparation of the battlefield
rpt	report
RRII	response to request for intelligence information
RSTA	reconnaissance, surveillance, and target acquisition

/s/	signature
S2	Intelligence Officer (US Army)
S3	Operations and Training Officer (US Army)
SA	special agent
SALUTE	size, activity, location, unit, time, equipment (spot report format)
SAM	surface-to-air-missile
SATRAN	definition is classified (see FM34-60A (S-NFD))
SCARF	standard collection asset request format
Sc I	sensitive compartmented information
SCUD	nickname of a missile system
SEAD	suppression of enemy air defenses
SED	simulated electronic deception
SHAPE	Supreme Headquarters Allied Powers Europe
SHELREP	shell report
sig	signal
SIGINT	signals intelligence
S I GSEC	signal security
SIR	specific information requirements
S I TDEV	situation development
S I TMAP	situation map
S I TREP	situation report
SLAR	side-looking airborne radar
SOP	standing operating procedures
SP	self-propel led
SSM	surface-to-surface missile
STANAG	standardization agreement
str	strength
SUPINTREP	supplementary intelligence report
SUPIR	supplemental programed interpretation report
SWO	Staff Weather Officer

TA	target acquisition
TAC-D	tactical deception
TACREP	tactical report
TA I	target areas of interest
TARDEV	target development
TCAC	technical control and analysis center
TCAE	technical control and analysis element
TDA	target damage assessment
TD I	target data inventory
TEL	transporter-erector- launcher
TEMPEST	an unclassified name for studies and investigations of compromising emanations
TF	task force
tgt	target
TI	technical intelligence
tk	tank
TLE	target location error
tng	training
TOC	tactical operations center

TOE	table of organization and equipment
TPL	time phase line
trp	troops
TSS	target selection standards
TTADB	tactical terrain analysis data base
TTY	teletypewriter
TVA	target value analysis
UAV	unmanned air vehicle
UHF	Ultra-high frequency
UI	unidentified
UNCLAS	unclassified
Unk	Unknown
us	United States
USAF	United States Air Force
USAIA	United States Army Intelligence Agency
USAICS	United States Army Intelligence Center and School
USAREUR	United States Army Europe
Uses	Unified Soils Classification System
USSID	United States Signals Intelligence Directive
USSR	Union of Soviet Socialist Republics (Soviet Union)
UTM	universal transverse mercator (grid)
VCR	videocassette recorder
VDP	video disk player
veh	vehicle
VHF	very high frequency
vic	vicinity
WETM	weather team
WIA	wounded in action
WNA	would not answer
wpn	weapon
yr	year

References

REQUIRED PUBLICATIONS

Required publications are sources that users must read in order to understand or to comply with this publication.

Field Manuals (FMs)

FM 34-1	Intelligence and Electronic Warfare Operations
FM 100-5	Operations

RELATED PUBLICATIONS

Rslated publications are sources of additional information. They are not required in order to understand this publication.

Army Regulation (AR)

105-31	Message Preparation and Processing

Field Manuals (FMs)

3-3	NBC Contamination Avoidance
3-12	Operational Aspects of Radiological Defense
3-22	Fallout Prediction
5-26	Employment of Atomic Demolition Munitions
21-26	Map Reading and Land Navigation
34-10	Division Intelligence and Electronic Warfare Operations
34-25	Corps Intelligence and Electronic Warfare Operations
34-37	Echelons Above Corps Intelligence and Electronic Warfare Operations
34-40	(U) Electronic Warfare, Secret
34-60	Counter intelligence
34-60A	(U) Counterintelligence Operations, Secret
34-80	Brigade and Battalion Intelligence and Electronic Warfare Operations.

34-81	Weather Support for Army Tactical Operations
34-130	Intelligence Preparation of the Battlefield
90-2	Battlefield Deception
101-5	Staff Organization and Operations
101-5-1	Operational Terms and Graphics
101-10-1	Staff Officers Field Manual: Organizational , Technical , and Logistical Data
101-31-1	Staff Officers' Field Manual: Nuclear Weapons Employment Doctrine and Procedures

Joint Chiefs of Staff Publications (JCS Pubs)

JCS - Pub 1	Department of Defense Dictionary of Military and Associated Terms
JCS - Pub 25	Title Unavailable, Top Secret.

Training Circulars (TCs)

34-41	Jamming Handbook
34-52	Intelligence interrogation
34-55	Imagery intelligence

Fieid Circular (FC)

1oo-15-1	Corps Deep Battle

Standardization Agreements (STANAGs)

1059	National Distinguishing Letters for Use by NATO Forces
2003	Patrol Reports
2008	Bombing, Shelling, and Mortaring Reports
2014	Operation Orders, Annexes to Operation Orders, and Administration and Logistic Orders
2020	Operational Situation Reports
2022	intelligence Reports
2019	Military Symbols

2029	Method of Describing Ground Locations, Areas and Boundaries
2033	Interrogation of Prisoners of War (PW)
2073	NATO Intelligence Subject Code
2077	Order of Battle (Non-NATO Troops)
2084	Handling and Reporting of Captured Enemy Equipment and Documents
2097	Nomenclature for Soviet Bloc Army Weapons and Equipment
2103	Raporting Nuclear Detonations, Biological and Chemical Attacks, and Predicting and Warning of Associated Hazards and Hazard Areas
2104	Friendly Nuclear Strike Warning
2112	Radiological Survey
2118	Intelligence Estimate
2134	Offensive Air Support Operations
2149	Intelligence Request
3277	Air Reconnaissance Request and Task Form
3377	Air Reconnaissance Intelligence Report Forms
3596	Air Reconnaissance Target Reporting Guide
6004	Meaconing, Intrusion, Jamming, and Interference Report

STANAGs can be obtained from: Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, Pennsylvania 19120.

INDEX

AI. See area of interest
ADP. See automatic data processing
aerial fire support officers (FSO), 7-10
AirLand Battle, 1-1
  area of operation (AO), 1-1
  deep attack, sample of, 1-2
  HVT, 1-2
  IPT, 1-2
  intelligence support to
    close operations, 1-3
    daep operations, 1-3
    rear operations, 1-3
all-source production section (ASPS), 2-2
analysis, 2-4, 2-17
  area of operations, A-108
  pattern, 6-9
annotated jntelljgence estimate, A-10
  for stability operations, 1-4, A-26
applications programs, B-6
arbitrary unit designators, 3-28, 3-30
area of jnterest (AI), 1-4, 4-7
area of operations, 1-1, 1-4, A-108
area study files, 10-7
ASPS. See all-source production section
assessment, 2-17
attack options, 7-7
  delay, 7-7
  disrupt, 7-7
  limit, 7-7
automatic data processing (ADP), B-1
automation support to intelligence analysis, B-1, B-4
  current automated support systems, B-7
    MICROFIX, B-7
    TCAC, B-7
  hardware, B-2
    keyboard, B-3
    modems, B-4
    monitor, B-4
    peripherals, B-4
    printer, B-4
    processor, B-4
    storage device, B-4
    video cassette recorders, B-4
    video disk players, B-4
  software, B-2
    applications program, B-S
    data base management system, B-6
    operating system, B-5
    word processing, B-S
avenues of approach and mobility corridors, 4-10, 4-16, E-22

BAE. See battlefield area evaluation
battlefield area, 1-4
  AI, 1-4
  AO, 1-4
  Cl, 1-4
  Ew, 1-4
    ECCM, 1-6
    ECM, 1-6
    ESM, 1-6
  IEW mission, 1-4
  one-up and two-down formula, 1-4
  situation development, 1-4
    make sound tactical decisions, 1-4
  target development, 1-4
battlefield area evaluation (BAE), 1-4, 4-7, 7-6
battlefield information coordination center (BICC), 1-8, 1-9
biases, S-11
BICC. See battlefield information coordination center
blue element, 5-7
bombing, shelling, and mortaring report, A-87

canopy closure, E-14
capabilities, 6-1
cathode ray tube (CRT), B-4
CC. See cloud cover
checklists of white, red, and blue questions, 5-8
CIAS. See counterintelligence analysis section
civil-military operationa file, 10-9
close operations, 1-3
cloud cover (CC), 4-13, 4-22
CM&D. See collection management and dissemination
COA. See course of action
collecting, 2-2
collection management and dissemination (CM&D), 2-2
COLT. See combat observation and laser team
combat
  effectiveness, 3-1, 3-5, D-1
  forces, 10-14
  observation and laser team (COLT), 7-10
combined
  intelligence operation, 10-1
  obstacle overlay, 4-6, 4-8, 4-12, 4-22, E-22
commander, 1-8
  intent of, 4-6, 4-27, 4-30
committed forces, D-1
composition, 3-1, 10-13
concealment and cover, 4-8, E-20
conceptual model, 6-1
contents of an OB book, 3-9

coordinate register, 3-22, 10-9
counter-human intelligence (C-HUMINT), 9-2
counter-imagery intelligence (C-IMINT), 9-3
counterinsurgency, 10-1
counterintelligence (CI), 1-4
  analysis, 9-1
  analysis section (CIAS), 9-1
    C-HUMINT collection, 9-2
    C-IMINT collection, 9-3
    C-SIGINT collection, 9-2
    EACIC, 9-1
    ITAC, 9-1
    rear operations, 9-2
counter-signals intelligence (C-SIGINT), 9-2
  workstation, B-14
course of action (COA), 6-3
credibility, 2-14
  of information, 2-15
critical nodes, 7-7
CRT. See cathode ray tube
current automated support systems, B-7
current propaganda and PSYOP file, 10-7

data base management system (DBMS) software, B-5
DBMS. See data base management system
decide. See targeting process
decision
  briefing, A-144
  points (DP), 4-30, 4-32, 7-5
  supper t
    matrix, 4-32
    templates (DST), 4-1, 4-5, 4-26, 4-29, 4-32
decisive terrain, 4-10
deduction, 2-17, 2-18
deep attack, 1-1
  sample of, 1-2
delay. See targeting process
deliver. See targeting process
  planned target, 7-12
  target damage assessment, 7-13
  targets of opportunity, 7-13
destroy, 7-1
detect, 7-3, 7-8
  aerial FSO, 7-10
  COLT, 7-10
  FIST, 7-8
  forward area alerting radar, 7-10
  moving target-locating radar, 7-10
  target location errors (TLE), 7-11

target selection standards (TSS), 7-11
directing, 2-1
disposition, 3-1, 3-2, 10-14
dissemination, 2-18, 10-12
disrupt, 1-1, 7-1, 7-7
doctrinal, 4-7, 4-11, 4-24, 4-32
templates, 4-5, 4-14, 4-25, 4-27, 6-4
OP. See decision point

EACIC. See echelons above corps intelligence center
echelons above corps intelligence center (EACIC), 1-6, 9-1
effectiveness, 10-18
effects of weather, E-1
on mobility, 4-13
electronic
counter-countermeasures (ECCM), 1-6
countermeasures (ECM), 1-6
order of battle (EOB), 3-5
technical data, 3-1, 10-19
electronic warfare (EW), 1-4, 6-1
intelligence required for ECCM, 8-3
intelligence required for ECM, 6-2
intelligence required for ESM, 8-2
electronic warfare support measures (ESM), 1-6
enemy
combat effectiveness, 3-28
strength computations, D-1
combat effectiveness, D-1
committed forces, D-1
reinforcements, D-1, D-5
EOB. See electronic order of battle
evaluation, 2-4, 2-13, 10-10
event, 4-3, 4-29
analysis matrix, 4-14
template, 4-1, 4-5, 4-26, 4-28, 4-32
EW. See electronic warfare

factors analysts should consider, 5-1
feedback, 5-2
fire support team (FIST), 7-8
FIST. See fire support team
formats, A-1
analysis of area of operations, A-108
annotated intelligence estimate, A-10
for stability operations, A-25
bombing, shelling, and mortaring reports, A-87
fragmentary order, A-127
initial and supplemental programmed interpretation report, A-59

intelligence annex, A-29
intelligence estimate, A-1
intelligence report, A-43
intelligence summary, A-44
interrogation and translation report, A-61
meaconing, intrusion, jamming, and interference report, A-143
mlsslon report, A-129
NBC attack reports, A-09
oral reports, A-144
decislon briefing, A-144
information briefing, A-144
patrol report, A-126
periodic intelligence report, A-48
periodic intelligence summary, A-51
reconnaissance exploitation report, A-68
SIGINT tactical report, A-142
situation report, A-42
spot report, A-1
standard collection asset request format, A-136
forward area alerting radar, 7-10
fragmentary order, A-127
FSO. See aerial fire support officer

G2/S2, 1-8
G3/S3, 1-8

handbook of military forces, 3-8
hardware, B-2
high payoff target (HPT), 1-2, 4-31, 7-4, 7-6
high value target (HVT), 1-2, 4-24, 4-32, 7-6
historical studies, 10-20
hot file, 10-7
HPT. See high payoff target
WT. See high value target

identify enemy HVTs, 1-2
IEW. See intelligence and electronic warfare
incident map, 10-4
indicators, 6-3
information briefing, A-144
information requirements (IR), 2-2
initial and supplemental programmed interpretation report, A-59
installation handbook, 3-10
insurgency analysis worksheet, 10-7
insurgent situation map (SITMAP), 10-4, 10-5
integration, 2-17, 10-10
intelligence and electronic warfare (IEW) mission, 1-4

intelligence
analysis, B-1
ADP, B-1
automation support to, B-1
CRT, B-4
hardware, B-2
keyboard, B-3
modems, B-4
monitor, B-4
peripherals, B-4
printer, B-4
processor, B-4
software, B-2
applications program, B-5
DBMS, B-6
operating system, B-6
word processing, B-5
storage device, B-4
video cassette recorders, B-4
video disk players, B-4
annex, A-29
director, coordinators, and producers, 1-8
estimate, 10-2
dissemination, 1o-I2
evaluation, 10-10
integration, 1O-10
interpretation, 10-11
recording, 10-4
area study files, 10-7
civil-military operations file, 10-9
coordinate register, 10-9
current propaganda and PSYOP file, 10-7
hot file, 10-7
incident map, 10-4
insurgency analysis worksheet, 10-7
insurgent SITMAP, 10-4
personalities and contracts map, 10-5
personality and organization file, 10-7
population status map, 10-5
resource file, 10-7
trap map, 10-6
file, 2-7
journal, 2-6
report, A-43
required for ECCM, 8-3
required for E(X, 8-2
required for ESM, 8-2
support to
combatting terrorism, 9-14
counterinsurgency, 10-1

summary, *A-44*
workbook, 2-12
intelligence analysis system, !-6
BICC, 1-9
duties of, 1-8
commander, 1-8
coordinator, 1-8
director, 1-8
producers, 1-8
staffs, 1-8
G2/S2, 1-8
G3/S3, 1-8
TCAE, 1-9
TOC support element, 1-9
Intelligence cycle, 2-1
collecting, 2-2
CM&D section, 2-2
directing, 2-1
ASPS, 2-2
IR, 2-2
PIR, 2-2
dissemination, 2-18
processing, 2-3
analysis, 2-4
assessment, 2-17
deduction, 2-18
integration, 2-17
evaluation, 2-4, 2-13
credibility, 2-14, 2-16
pertinence, 2-14
reliability, 2-14
of source and agency, 2-1S
recording, 2-3, 2-6
intelligence journal, 2-6, 2-8
intelligence file, 2-7
intelligence workbook, 2-12
OB SITMAP, 2-10
working SITMAP, 2-9
intelligence preparation of the battlefield (IPB), 4-3, 4-34
application of, 4-5
commander's intent, 4-6, 4-27, 4-30
event template, 4-6, 4-28, 4-32
MCOO, 4-6, 4-8
template, 4-6
battlefield area evaluation (BAE), 4-7
AI, 4-7
METT-T, 4-7
MCOO, 4-6, 4-8
avenues of approach and mobility corridors, 4-16
one-down, two-down rule, 4-11

one-up, two-down rule, 4-11
concealment and cover, 4-8
key terrain, 4-8, 4-28
decisive, 4-10
observation and fields of fire, 4-8
obstacle, 4-6, 4-8, 4-10, 4-22, 4-25
OCOKA, 4-8
combined obstacle overlay, 4-6, 4-8, 4-12, 4-22
effects of weather on mobility, 4-13
in support of LIC, 10-2
line of sight analysis, 4-15
process, 4-1, 4-11, 4-24, 4-26, 4-34
decision support, 4-1, 4-5, 4-26, 4-29
doctrinal template, 4-14, 4-25, 4-27
event, 4-3, 4-29, 4-32
situation, 4-3, 4-5, 4-26, 4-32
products, 4-2, 4-5, 4-7, 4-11, 4-21
templates
decision support, 4-1, 4-26, 4-32
doctrinal, 4-14, 4-25, 4-27
event, 4-6, 4-28, 4-32
situation, 4-6, 4-26
terrain factor matrix, 4-11
threat evaluation, 4-1, 4-24
doctrinal template, 4-25
threat integration, 4-3, 4-21, 4-26
decision support template, 4-1, 4-26, 4-29, 4-32
decision points, 4-30, 4-32
decision support matrix, 4-32
TAI, 4-31
time phase lines, 4-30
event analysis matrix, 4-29
event template, 4-6, 4-28, 4-32
PIR, 4-27, 4-32
situation templates, 4-26
weather analysis, 4-1, 4-15, 4-21, 4-26
cloud cover (CC), 4-13, 4-22
precipitation, 4-13, 4-17, 4-23
visibility, 4-9, 4-13, 4-18
wind speed and direction, 4-22
weather factor analysis matrix, 4-24
intelligence support
of close operations, 1-3
of rear operations, 1-3
to combatting terrorism, 9-14
to deep operations, 1-3
interpretation, 10-11
interrogation and translation report, A-61
ITAC. See intelligence and threat analysis center

keyboard, B-3
Key terrain, 4-8, 4-28, E-21

limit, 7-1, 7-7
line of sight analysis, 4-16
logistics, 3-1, 3-4, 10-17

make sound tactical declsions, 1-4
MCOO. See modified combined obstacle overlay
MOCI. See multidisciplJne counterintelligence
MDCISUM. See multidiscipline counterintelligence summary
meaconing, intrusion, jamming, and interference report, A-143
METT-T. See mission, enemy, terrain, troops, and time available.
MICROFIX, B-7, B-8
CI workstation, B-14
OPSEC workstation, B-14
TCAE workstation, B-13
topographic workstation, B-13
military installation file, 3-22
miscellaneous data, 3-1, 3-6
mission, enemy, terrain, troops, and time available (METT-T), 4-7
mission report, A-129
modems, B-4
modified combined obstacle overlay (MCOO), 4-6, 4-8, E-22
monitor, B-4
moving target-locating radar, 7-10
multidiscipline counterintelligence (MDCI)
estimate, 9-10
situation overlay, 9-7
summary (MODCISUM), 9-7
threat assessment, 9-7, 9-14

named areas of Interest (NAI), 4-32
neutralize, 7-1
nuclear, biological, and chemical (NBC) attack raports, A-89

observation and fields of fire, 4-8, E-20
observation and fields of fire, concealment and cover, obstacles, key terrain, avenues of approach, and mobility corridors (OCOKA), 4-8, E-1
obstacles, 4-8, 4-10, 4-13, 4-25, E-21
one-down, two-down rule, 4-11
one-up and two-down formula, 1-4
one-up, two-down rule, 4-11
operating system software, B-5
operations security (OPSEC) workstation, B-14

oral report, B-144
decision briefing, A-144
information briefing, A-144
order of battle, 10-12
combat forces, 10-14
composition, 10-13
disposition, 10-14
effectiveness, 10-18
electronic technical data, 10-19
factors, 3-1
combat effectiveness, 3-1, 3-6
composition, 3-1, 3-2
disposition, 3-1, 3-2
electronic technical data, 3-1, 3-5
logistics, 3-1, 3-4
miscellaneous data, 3-1, 3-6
personality file, 3-6
unit history, 3-6
strength, 3-1, 3-3
tactics, 3-1, 3-3
training, 3-1, 3-4
historical studies, 10-20
logistics, 10-17
personalities, 10-19
Phase I of an insurgency, 10-12
Phase II of an insurgency, 10-13
Phase III of an insurgency, 10-13
political structure, 10-14
records, 3-11
card, 3-17
coordinate register, 3-22”
military installation file, 3-22
organizational worksheet, 3-22
personality file, 3-18
SITMAP, 2-10, 3-14
strength worksheet, 3-22
unit workbook, 3-12
workbook, 3-12
references, 3-6
book, structure of, 3-7, 3-8
handbook of military forces, 3-8, 3-9
Installation handbooks, 3-10
miscellaneous, 3-10
STANAG 2077, 3-6
strength, 10-15
tactics, 10-16
training, 10-17
patrol report, A-126
pattern analysis, 6-9
patterns and signatures, 9-3

periodic
  intelligence report, A-48
  intelligence summary, A-51
peripherals, B-4
personalities, 10-19
  and contacts map, 10-5
  fries, 3-6, 3-18
pertinence, 2-14
Phase I of an insurgency, 10-12
Phase II of an insurgency, 10-13
Phase III of an insurgency, 10-13
PIR. See priority intelligence requirements
planned targets, 7-12
planning terrain analysis data base, 7-12
population status map, 10-5
precipitation, 4-13, 4-17, 4-23, E-12
printer, B-4
priority intelligence requirements (PIR), 2-2, 4-27, 4-32
processing, 2-3, 10-3
processor, B-4

rear and deep operations, 1-3
rear operations, 9-2
reconnaissance exploitation report, A-58
recording, 2-3, 2-6, 10-4
  area study file, 10-7
  civil-military operations file, 10-9
  coordinate register, 10-9
  current propaganda and PSYOP file, 10-7
  hot file, 10-7
  incident map, 10-4
  insurgency analysis worksheet, 10-7
  insurgent SITMAP, 10-4, 10-5
  personalities and contacts map, 10-5
  population status map, 10-5
  resource file, 10-7
  trap map, 10-5
red element, 5-6
reinforcements, D-1, D-5
reliability, 2-14
  of the source and agency, 2-15
relief, E-4
report formats, A-1
  intelligence estimate, A-1
  spot report, A-1
resource file, 10-7
risk, 5-3

S2/G2, 1-8
S3/G3, 1-8
SIGINT. See signals intelligence
signals intelligence (SIGINT) tactical report, A-142
situation
  development, 1-4, 6-1
    capabilities, 6-1
    courses of action, 6-3
    indicators, 6-3
    pattern analysis, 6-9
    weighting indicators, 6-10
    working SITMAP, 6-4
      doctrinal templata, 6-4
  report, A-42
  template, 4-6, 4-26, 4-32, 7-5
software, B-2
spot report, A-1
staffs, 1-8
STANAG 2077, 3-6
standard collection asset request format, A-136
storage devices, B-4
strength, 3-1, 3-3, 10-15
  computations, D-1
  worksheet, 3-22
structure of an OB book, 3-8
suppress, 7-1
surface materials, E-14

tactical
  operations center (TOC) support elements, 1-8, 1-9
  terrain analysis data base, E-1
tactics, 3-1, 3-3, 10-16
target
  damage assessment, 7-13
  development, 1-4, 1-5, 7-1
    attack options, 7-7
      delay or limit, 7-7
      disrupt, 7-7
    decide function, 7-3
      HPT matrix, 7-4
      target selection standards, 7-4
    detect function, 7-3, 7-8
      aerial fire support officers, 7-10
      combat observation laser teams (COLT), 7-10
      first support teams (FIST), 7-8
      forward area alerting radar (FAAR), 7-10
      moving target locating radar (MTLR), 7-10
      target location errors (TLE), 7-11
      target selection standards (TSS), 7-11

deliver function, 7-4
IPB, 7-5
and BAE, 7-5
decision point, 7-5
situation template, 7-5
TAI, 7-5
terrain evaluation, 7-5
weather analysis, 7-5
location errors (TLE), 7-7
of opportunity, 7-12, 7-13
planned, 7-12
selection standards (TSS), 7-4, 7-7
value analysis, 7-6
critical nodes, 7-7
HPT, 7-6
HVT, 7-6
target areas of interest (TAI), 4-30, 7-5
targeting process, 7-1
functions, 7-1
decide, 7-3
HPT matrix, 7-4
target selection standards (TSS), 7-4
deliver, 7-4
detect, 7-3
objective of, 7-1
delay, 7-1
disrupt, 7-1
limit, 7-1
destroy, 7-1
neutralize, 7-1
suppress, 7-1
target location error (TLE), 7-11
target selection standards (TSS), 7-7, 7-11
TCAC. See technical control and analysis center
TCAE. See technical control and analysis element
technical
control and analysis center (TCAC), B-7
control and analysis element (TCAE), 1-8, 1-9
workstation, B-13
templates, 4-5
decision support, 4-1, 4-26, 4-20, 4-32
doctrinal, 4-14, 4-25, 4-27, 6-4
event, 4-6, 4-28, 4-32
situation, 4-6, 4-26, 7-5
terrain
analysis, E-1
avenues of approach and mobility corridors, E-22
combined obstacles overlay, E-22
concealment and cover, E-20
effects of weather, D-1

key terrain, E-21
modified combined obstacles overlay (MCOO), E-22
observation and fields of fire, E-2o
observation and fields of fire, concealment and cover, obstacles,
key terrain, avenues of approach, and mobility corridors (OCOKA), E-1
obstacles, E-21
planning terrain data basa, E-1
precipitation, E-12
tactical terrain data base, E-1
vegetation, E-12
evaluation, 7-5
factor matrix, 4-11
masking, E-20
military aspects of, E-20
avenues of approach and mobility corridors, E-22
concealment and cover, E-20
key terrain, E-21
observation and fields of fire, E-20
terrain masking, E-20
obstacles, E-21
threat
evaluation, 4-1, 4-24
doctrinal templates, 4-25, 4-27
integration, 4-3, 4-21, 4-26
decision support matrix, 4-32
event analysis matrix, 4-29
PIR, 4-27, 4-32
templates
decision support, 4-1, 4-26, 4-29, 4-32
decision points, 4-30, 4-32
TAI, 4-31
HPT, 4-3, 4-31
HVT, 4-1, 4-24, 4-31
time phase lines, 4-30
event, 4-6, 4-28, 4-32
NAI, 4-28, 4-32
situation, 4-26
model, 5-5
checkist of white, red, and blue questions, 5-8
blue element, 5-7
red element, 5-6
white elements, 5-5
time phase lines, 4-30
TLE. See target location error
TOC. See tactical operations center
topographic workstatlon, B-13
training, 3-1, 3-4, 10-17
trap map, 10-5
TSS. See target selection standard

unit workbook, 3~-12
unit history, 3-6
user of intelligence, 5-1

vegetation, E-12
video cassette recorders, B-4
video disk players, B-4
visibility, 4-9, 4-13, 4-18, 4-22

weather analysis, 4-1, 4-15, 4-21, 4-26, 7-5
  cloud cover, 4-13, 4-22
  precipitation, 4-13, 4-17, 4-23
  visibility, 4-9, 4-13, 4-18, 4-22
  weather factor analysis matrix, 4-24
  wind speed and direction, 4-22
weighting indicators, 6-10
white elements, 5-5
word processing software, B-5
working SITMAP, 2-9, 6-4

BY Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:

WILLIAM J. MEEHAN II
Brigadier General, United States Armv
The Adjutant General

DISTRIBUTION:

Active Army, USAR, and ARNG: To be distributed in accordance with DA Form 12-IIE, requirements for FM 34-3, Intelligence Analysis (Qty rqr block no. 1119).

*U.S.GOVERNMENT PRINTING OFFICE:1996 406-421/62005

ATP 2-01.3
MCRP 2-10B.1
(Formerly MCRP 2-3A)

Intelligence Preparation of the Battlefield/*Battlespace*

November 2014

+DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Headquarters, Department of the Army
Headquarters, United States Marine Corps

144 000141 00

CD&I (C 116)

2 May 2016

ERRATUM

to

MCRP 2-3A

INTELLIGENCE PREPARATION OF THE BATTLEFIELD/BATTLESPACE

1. Change all instances of MCRP 2-3A, *Intelligence Preparation of the Battlefield/Battlespace*, to MCRP 2-10B.1, *Intelligence Preparation of the Battlefield/Battlespace.*

2. File this transmittal sheet in the front of this publication.

PCN 144 000141 80

This publication is available at Army Knowledge Online (https://armypubs.us.army.mil/doctrine/index.html). To receive publishing updates, please subscribe at http://www.apd.army.mil/AdminPubs/new_subscribe.asp.

+*This publication is available at the U.S. Marine Corps Doctrine Web site (https://doctrine.usmc.mil)*

ATP 2-01.3, C1
MCRP 2-3A, C1

Army Techniques Publication
No. 2-01.3
Marine Corps Reference Publication
No. 2-3A

Headquarters
Department of the Army
Washington, DC

Headquarters
United States Marine Corps
Deputy Commandant
Combat Development & Integration
Quantico, Virginia

26 March 2015

Intelligence Preparation of the Battlefield/*Battlespace*

1. This change changes the distribution restriction on this manual, adds the uniform resource locator for the U.S. Marine Corps Doctrine Web Site to the inside cover, and corrects the U.S. Marine Corps address on the title page.

2. A plus sign (+) indicates changed material.

3. ATP 2-01.3/MCRP 2-3A, 10 November 2014, is changed as follows:

Remove Old Pages	Insert New Pages
front cover	front cover
pages i through ii	pages i through ii

4. File this transmittal sheet in the front of the publication for reference purposes.

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Marine Corps PCN: 144 000141 00

ATP 2-01.3, C1
MCRP 2-3A, C1
26 March 2015

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army
1506206

By Direction of the Commandant of the Marine Corps:

K. J. GLUECK, JR.
Lieutenant General, U.S. Marine Corps
Deputy Commandant
Combat Development and Integration

DISTRIBUTION:

Active Army, the Army National Guard, and the United States Army Reserve. Not to be distributed; electronic media only.

Marine Corps PCN: 144 000141 00 **PIN: 104814-001**

ATP 2-01.3, C1
MCRP 2-3A, C1

Army Techniques Publication
No. 2-01.3
Marine Corps Reference Publication
No. 2-3A

Headquarters
Department of the Army
Washington, DC

Headquarters
United States Marine Corps
Deputy Commandant
Combat Development & Integration
Quantico, Virginia

26 March 2015

Intelligence Preparation of the Battlefield/*Battlespace*

Contents

Page

PREFACE ..... **vii**

INTRODUCTION ..... **ix**

PART ONE FUNDAMENTAL PRINCIPLES, PROCESS ACTIVITIES, AND RELATIONSHIPS

Chapter 1 FUNDAMENTALS OF INTELLIGENCE PREPARATION OF THE BATTLEFIELD/*BATTLESPACE* **1-1**
Intelligence Preparation of the Battlefield/*Battlespace* (IPB) 1-1
Process Activities 1-2
Intelligence Estimate 1-4
Staff Integration into IPB 1-4
Relationships 1-6

Chapter 2 IPB SUPPORT TO DECISIONMAKING DURING PLANNING **2-1**
IPB and Decisionmaking 2-1
IPB and Planning 2-1

+DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited

*This publication supersedes FM 2-01.3/*MCRP 2-3A*, 15 October 2009, and FMI 2-01.301, 31 March 2009.

Marine Corps PCN: 144 000141 00

PART TWO FUNDAMENTAL TASK TECHNIQUES

Chapter 3 STEP 1 OF THE IPB PROCESS—DEFINE THE OPERATIONAL ENVIRONMENT 3-1
What Is It? 3-1
Desired End State 3-2
So What? 3-2
How To Do It: (The Process) 3-3
Identify the Limits of the Commander's Area of Operations 3-3
Identify the Limits of the Commander's Area of Interest 3-4
Identify Significant Characteristics Within the Area of Operations and Area of Interest for Further Analysis 3-5
Evaluate Current Operations and Intelligence Holdings to Determine Additional Information Needed to Complete IPB 3-7
Initiate Processes Necessary to Acquire the Information Needed to Complete IPB 3-7

Chapter 4 STEP 2 OF THE IPB PROCESS—DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS/*DESCRIBE THE EFFECTS ON OPERATIONS* 4-1
What Is It? 4-1
Desired End State 4-1
So What? 4-1
How To Do It: (The Process) 4-2
Describe How the Threat/*Adversary* Can Affect Friendly Operations 4-2
Describe How Terrain Can Affect Friendly and Threat/*Adversary* Operations 4-4
Describe How Weather Can Affect Friendly and Threat/*Adversary* Operations 4-18
Describe How Civil Considerations Can Affect Friendly and Threat/*Adversary* Operations 4-29
Civil Considerations Data Files, Overlays, and Assessments 4-35

Chapter 5 STEP 3 OF THE IPB PROCESS—EVALUATE THE THREAT/*ADVERSARY* 5-1
What Is It? 5-1
Desired End State 5-1
So What? 5-1
How To Do It: (The Process) 5-2
Identify Threat Characteristics/*Adversary Order of Battle* 5-3
Create or Refine Threat/*Adversary* Models 5-21

Chapter 6 STEP 4 OF THE IPB PROCESS—DETERMINE THREAT/*ADVERSARY* COURSES OF ACTION 6-1
What Is It? 6-1
Desired End State 6-2
So What? 6-2
How To Do It: (The Process) 6-2
Develop Threat/*Adversary* Courses of Action 6-3
Develop the Event Template and Matrix 6-14

PART THREE CONSIDERATIONS FOR SPECIFIC OPERATIONS, UNIQUE ENVIRONMENTS, AND MISSIONS

Chapter 7 IPB FOR SPECIFIC OPERATIONS 7-1
IPB Considerations for Offensive Tasks/*Operations* 7-1
IPB Considerations for Defensive Tasks/*Operations* 7-4
IPB Considerations for Counterinsurgency Operations and Stability Tasks 7-6
Understanding the Population 7-19

Chapter 8 IPB CONSIDERATIONS FOR UNIQUE ACTIVITIES, TASKS, AND PROCESSES 8-1
IPB Support to Protection/*Force Protection* 8-1
IPB Support to Building Partnership Capacity/*Establishing Genuine Partnerships* 8-4

Chapter 9 IPB CONSIDERATIONS FOR UNIQUE ENVIRONMENTS 9-1
IPB Considerations for an Urban Environment 9-1
IPB Considerations for a Cold Weather or Mountain Environment 9-2
IPB Considerations for a Jungle Environment 9-6
IPB Considerations for a Desert Environment 9-8
IPB Support to Cyber Electromagnetic Activities/*Cyberspace Operations* 9-12

Chapter 10 IPB CONSIDERATIONS FOR UNIQUE MISSIONS 10-1
Conducting IPB in Support of Counterdrug Activities 10-1
IPB Support to Counter-Proliferation 10-3
IPB Support to Counter-Improvised Explosive Device Operations 10-4
IPB Support to Site Exploitation and/or Exploitation of Sensitive Sites 10-4
IPB Support to Peace Operations 10-6
IPB Support to Humanitarian and Disaster Relief and Other Operations 10-9

Appendix A *MARINE CORPS PLANNING PROCESS TOOLS* A-1

Appendix B FUNCTIONAL ANALYSIS B-1

GLOSSARY Glossary-1

REFERENCES References-1

INDEX Index-1

Figures

Figure 2-1. IPB and the MDMP/*MCPP* steps 2-2
Figure 3-1. Sub-steps of step 1 of the IPB process 3-3
Figure 3-2. Example areas of operations 3-4
Figure 4-1. Step 2 of the IPB process 4-2
Figure 4-2. Example threat/*adversary* overlay (irregular forces) 4-3
Figure 4-3. Example of obstacles in natural terrain 4-5
Figure 4-4. Example of obstacles in urban terrain 4-5
Figure 4-5. Avenues of approach with mobility corridors 4-7
Figure 4-6. Mobility corridors (urban terrain) 4-7
Figure 4-7. Key terrain (natural terrain) 4-9

Figure 4-8. Key terrain (urban terrain) 4-9
Figure 4-9. Example of intervisibility lines 4-10
Figure 4-10. Observation and fields of fire (natural terrain) 4-11
Figure 4-11. Observation and fields of fire (urban terrain) 4-12
Figure 4-12. Cover and concealment (natural terrain) and line-of-sight analysis 4-13
Figure 4-13. Example of cover and concealment in urban terrain 4-14
Figure 4-14. Example modified combined obstacle overlay (natural terrain) 4-16
Figure 4-15. Example weather forecast chart 4-21
Figure 4-16. Example light and illumination table 4-22
Figure 4-17. Weather effects matrix/*operational impacts chart* 4-22
Figure 4-18. *Amphibious landing weather example* 4-24
Figure 4-19. *Beach landing site weather example* 4-24
Figure 4-20. *Littoral weather example* 4-25
Figure 4-21. *Tidal weather example* 4-25
Figure 4-22. 96-hour forecast weather example 4-26
Figure 4-23. *Astronomical data weather example* 4-27
Figure 4-24. *Light level weather example* 4-27
Figure 4-25. *Operational impacts weather example* 4-28
Figure 4-26. *Space weather example* 4-28
Figure 4-27. Example of civil considerations data file 4-36
Figure 4-28. Civil considerations data file example (inside view with overlay) 4-37
Figure 4-29. Security organizations and bases example 4-37
Figure 4-30. Voting locations example 4-38
Figure 4-31. Population status example 4-38
Figure 4-32. Ethnic overlay example 4-39
Figure 5-1. Evaluate the threat/*adversary* 5-2
Figure 5-2. Example organizational chart for a regular threat/*adversary* force 5-4
Figure 5-3. Example organizational chart for an irregular threat/*adversary* force 5-5
Figure 5-4. U.S. Army example of a complex battle position for a task-organized guerilla platoon threat model 5-10
Figure 5-5. *Example of a Marine Corps doctrinal template for an irregular adversary* 5-11
Figure 5-6. Example of an integrated attack by task-organized guerilla battalion threat/*adversary* model 5-11
Figure 5-7. Example of a complex battle position: insurgent organization threat/*adversary* model 5-26
Figure 5-8. Example threat/*adversary* template (counterinsurgency) 5-27
Figure 5-9. Event template (IED attack) 5-28
Figure 5-10. Example threat/*adversary* capability statement 5-29
Figure 6-1. Determine threat/*adversary* COAs 6-3
Figure 6-2. Example of a situation template 6-7
Figure 6-3. Example enemy offensive situation overlay 6-9
Figure 6-4. Example enemy reconnaissance attack 6-10

Figure 6-5. Example enemy defensive situation overlay 6-11
Figure 6-6. Example irregular force situation overlay 6-13
Figure 6-7. Example threat/*adversary* COA statement 6-13
Figure 6-8. Example of an event template – 1 6-15
Figure 6-9. Example of an event template – 2 6-16
Figure 6-10. Example event template (regular threat) 6-17
Figure 6-11. Example event template (irregular threat) 6-18
Figure A-1. *Modified combined obstacle overlay* A-3
Figure A-2. *Adversary template* A-4
Figure A-3. *Situation template* A-5
Figure A-4. *Event template* A-6
Figure A-5. *Decision support template* A-7
Figure A-6. *Course of action graphic and narrative* A-9
Figure A-7. *Sample civil considerations* A-12
Figure B-1. Enemy attacking fixed position B-5
Figure B-2. Sniper and riot-enabled insurgency assault B-5

Tables

Introductory table 1. Rescinded Army terms x
Introductory table 2. Modified Army terms x
Table 4-1. Example threat/*adversary* description table (irregular forces) 4-3
Table 4-2. Mobility corridor ranges 4-6
Table 4-3. Example terrain effects matrix 4-17
Table 4-4. PMESII and ASCOPE examples 4-29
Table 5-1. Description of potential irregular forces 5-7
Table 6-1. Constructing an event matrix 6-16
Table 7-1. Example civil security intelligence requirements 7-9
Table 7-2. TTP for evaluating external threat/*adversary o*rganizations 7-10
Table 7-3. TTP for evaluating internal threat/*insurgency* operations 7-12
Table 7-4. TTP for evaluating the general population's role in a conflict 7-13
Table 7-5. Information sources for supporting economic developments 7-17
Table 7-6. Information sources for supporting infrastructure development (*SWEAT-MSO*) 7-18
Table 8-1. Examples of types of non-combat-related injuries 8-4
Table 10-1. IPB products in support of counterdrug activities 10-3
Table A-1. *Marine Corps planning process tools* A-1
Table A-2. *IPB integration throughout the Marine Corps planning process* A-2
Table A-3. *Event matrix* A-6
Table A-4. *Decision support matrix* A-8
Table A-5. *Synchronization matrix* A-10

Table A-6. *Course of action wargame worksheet* A-11
Table A-7. *Comparison and decision matrix with comments* A-12

Preface

ATP 2-01.3/*MCRP 2-3A* is a dual-designated Army and Marine Corps manual that constitutes current doctrine on how to systematically evaluate the effects of significant characteristics of the operational environment for specific missions. It describes how the commander and staff examine mission variables to understand how these variables may affect operations. It discusses intelligence preparation of the battlefield/*intelligence preparation of the battlespace* (IPB) as a critical component of the military decisionmaking process (MDMP)/*Marine Corps Planning Process (MCPP)* and how IPB supports decisionmaking, as well as integrating processes and continuing activities.

This publication supersedes FM 2-01.3/*MCRP 2-3A* and FMI 2-01.301 and expedites delivery of doctrine that the proponent has approved for immediate use in IPB support to operations. It facilitates a common understanding, foundational concepts, and methods of the IPB process.

The principal audience for ATP 2-01.3/*MCRP 2-3A* is Army/*Marine Corps* commanders and staffs. Commanders and staffs of Army/*Marine Corps* headquarters serving as a joint task force or a multinational headquarters also refer to applicable joint or multinational doctrine related to IPB. Trainers and educators throughout the Army/*Marine Corps* also use this publication.

ATP 2-01.3/*MCRP 2-3A* uses joint terms where applicable. Selected joint, Army, and *Marine Corps* terms, and definitions appear in both the glossary and the text. In doctrinal publications, the normal convention for identifying terms is through the use of italics. Since this is a dual-designated Army and *Marine Corps* manual, the following protocol is used to distinguish proponency (authority) for information and terms:

- **Terms and phrasing in italics—Marine Corps.**
- **Terms and definitions in bold—Terms for which ATP 2-01.3/*MCRP 2-3A* is the proponent publication.**
- **Terms in bold and definitions in plain text—Joint terms and Army terms with proponent publication other than ATP 2-01.3, with the proponency publication in parentheses.**

All references to "staffs" in this manual refer to the operations, intelligence, and other coordinating and special staff sections unless indicated otherwise.

This manual applies to intelligence activities conducted outside the United States. Intelligence activities conducted inside the United States, as well as those that target U.S. persons and groups outside the United States, invoke additional requirements and intelligence oversight rules. To the extent any of the activities described in this publication are conducted inside the United States, or target U.S. persons or groups outside the United States, consult your judge advocate for assistance.

ATP 2-01.3/*MCRP 2-3A* applies to the Active Army and Marine Corps, the Army National Guard/Army National Guard of the United States, United States Army Reserve, and the United States Marine Corps Reserve unless otherwise stated.

The proponent of ATP 2-01.3/*MCRP 2-3A* is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Capabilities Development and Integration Division, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Intelligence Center of Excellence, ATTN: ATZS-CDI-D (ATP 2-01.3), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017, by e-mail to usarmy.huachuca.icoe.mbx.doctrine@mail.mil; or submit an electronic DA Form 2028.

United States Marine Corps readers of this publication are encouraged to submit suggestions and changes through the Universal Need Statement (UNS) process. The UNS submission process is delineated in MCO 3900.15B, which can be obtained from the Marine Corps Publications Electronic Library Online.

The UNS recommendation should include the following information:

- *Location of change.*
  - *Publication number and title.*
  - *Current page number.*
  - *Paragraph number (if applicable).*
  - *Line number.*
  - *Figure or table number (if applicable).*
- *Nature of change.*
  - *Addition or deletion of text.*
  - *Proposed new text.*

Introduction

ATP 2-01.3/*MCRP 2-3A* updates and describes the fundamentals of IPB. The following paragraphs summarize the most important updates and changes.

ATP 2-01.3/*MCRP 2-3A* contains 10 chapters and two appendixes.

Chapter 1 makes the following change: Redefines the Army's definition of IPB as "Intelligence Preparation of the Battlefield (IPB) is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations."

Chapter 3 replaces the sub-steps of step 1 with the following:

- **Identify the limits of the commander's area of operations (AO).**
- **Identify the limits of the commander's area of interest.**
- **Identify significant characteristics within the AO and area of interest for further analysis.**
- **Evaluate current operations and intelligence holdings to determine additional information needed to complete IPB.**
- **Initiate processes necessary to acquire information necessary to complete IPB.**

Chapter 4 replaces the sub-steps of step 2 with the following:

- **Describe how the threat/*adversary* can affect friendly operations.**
- **Describe how terrain can affect friendly and threat/*adversary* operations.**
- **Describe how weather can affect friendly and threat/*adversary* operations.**
- **Describe how civil considerations can affect friendly and threat/*adversary* operations.**

Chapter 5 replaces the sub-steps of step 3 with the following:

- **Identify threat characteristics/*adversary order of battle*.**
- **Create or refine threat/*adversary* models.**

Chapter 6 replaces the sub-steps of step 4 with the following:

- **Develop threat/*adversary* courses of action (COAs).**
- **Develop the event template and matrix.**

G-2/S-2 is used in cases when actions are conducted by both U.S. Army and the Marine Corps.

This publication uses "holdings" to annotate many different feeds (for example, biometrics). "Holdings" is used in this publication to refer to information or data, such as data files and/or databases that the command or its higher headquarters has, or information that the command can access. This publication avoids discussing specific disciplines and complementary intelligence capabilities. It describes the IPB process which occurs after this information is collected, processed, and stored.

Based on current doctrinal changes, certain terms for which ATP 2-01.3/*MCRP 2-3A* is proponent have been added, rescinded, or modified for purposes of this manual. The glossary contains acronyms and defined terms. See introductory table 1 and introductory table 2 on the next page for specific term changes.

Introductory table 1. Rescinded Army terms

Term	*Remarks*
event template	Rescinded Army definition. Adopts the joint definition.

Introductory table 2. Modified Army terms

Term	*Remarks*
intelligence preparation of the battlefield/*battlespace*	Modifies the definition.
latest time information is of value	Proponent publication changed to ATP 2-01.

PART ONE

Fundamental Principles, Process Activities, and Relationships

Chapter 1

Fundamentals of Intelligence Preparation of the Battlefield/*Battlespace*

INTELLIGENCE PREPARATION OF THE BATTLEFIELD/ *BATTLESPACE* (IPB)

1-1. Intelligence Preparation of the Battlefield (IPB) is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. ***Intelligence Preparation of the Battlespace (IPB) is the systematic, continuous process of analyzing the threat and environment in a specific geographic area.***

1-2. The G-2/S-2 begins preparing for IPB during the generate intelligence knowledge task/*problem framing step*. (For U.S. Army, see FM 7-15, chapter 2, for the complete list of tasks and their measures of performance. ***For the Marine Corps, see MCWP 5-1 for information on problem framing.*****) The intelligence staff creates data files and/or databases based on the operational environment. Given the limited time available to collect and evaluate information, this information may not be specific enough to support the military decisionmaking process (MDMP)/*Marine Corps Planning Process (MCPP).* However, this information helps create the operational environment frame during the design methodology.**

1-3. IPB results in the creation of intelligence products that are used during the MDMP/*MCPP* to aid in developing friendly courses of action (COAs) and decision points for the commander. Additionally, the conclusions reached and the products created during IPB are critical to planning information collection/*intelligence collection* and targeting operations. (*See MCWP 5-1 for a discussion on the MCPP.)

1-4. The G-2/S-2 leads this staff effort and begins preparing for IPB during the generate intelligence knowledge process associated with force generation and is incorporated into the Army design methodology. During generate intelligence knowledge, the intelligence staff creates data files on specific operational environments based on an evaluation of the information and intelligence related to the operational variables identified in the memory aid PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, time)/*PMESII (political, military, economic, social, information, and infrastructure)*. (*For the Marine Corps, see MCWP 5-1 for more information on intelligence support to planning and problem framing.)*

1-5. Given the limited time available to collect and evaluate information and intelligence on the operational variables, this information may not be specific enough to support the MDMP/*MCPP*. However, it can be used by the commander and the entire staff to aid the Army design methodology. Throughout the operations process, the commander and staff continue to collect information and analyze the operational variables in order to provide increased situational understanding. Upon receipt of a warning order or

mission, they draw relevant information that was categorized by the operational variables and filter it into the mission variables used during mission analysis/*problem framing*. During IPB, the staff focuses on the relevant aspects of the operational environment as it pertains to their warfighting function and the mission variables. The intelligence staff is primarily focused on the mission variables of enemy, terrain, weather, and civil considerations.

1-6. To be effective, IPB must—

- Accurately define the commander's area of interest in order to focus collection and analysis on the relevant aspects of the mission variables of enemy, terrain, weather, and civil considerations. Relevant is defined as having significant effect on friendly operations and threat/*adversary* operations, and population in a unit's area of operations (AO).
- Describe how each of these four mission variables will affect friendly operations and how terrain, weather, and civil considerations will affect the enemy.
- Provide the IPB products necessary to aid each step of the MDMP/*MCPP* in accordance with the planning timelines and guidance provided by the commander.
- Determine how the interactions of friendly forces, enemy forces, and indigenous populations affect each other to continually create outcomes that affect friendly operations. This aspect of IPB is not the sole responsibility of the intelligence staff. This complex analysis involves the commander and the entire staff working together to determine these effects.

1-7. IPB is most effective and best aids the commander's decisionmaking when the intelligence staff integrates the expertise of the other staff and supporting elements, such as civil affairs teams and military information support personnel, into its analysis. This is especially true when operating in environments where the effects of the enemy, terrain, weather, and civil considerations are complex and not easily determined.

1-8. IPB aids commanders in reducing uncertainty by evaluating how the enemy, terrain, weather, and civil considerations may affect operations and decisionmaking. Most intelligence requirements are generated as a result of IPB and its interrelationship with decisionmaking.

1-9. A key aspect of IPB is refinement. The conclusions made and the products developed during IPB are continually refined throughout the operation. This information is incorporated into the running estimate as new information is obtained and further analysis is conducted during situation development. This refinement ensures that the commander's decisions are based on the most current information and intelligence available.

PROCESS ACTIVITIES

1-10. The IPB process consists of the following four steps:

- Define the operational environment.
- Describe environmental effects on operations/d*escribe the effects on operations*.
- Evaluate the threat/*adversary*.
- Determine threat/*adversary* COAs.

STEP 1—DEFINE THE OPERATIONAL ENVIRONMENT

1-11. Defining the operational environment results in the identification of significant characteristics of the operational environment that can affect friendly and enemy operations. This step also results in the identification of gaps in current intelligence holdings. (Step 1 is discussed fully in chapter 3.)

1-12. Step 1 is important because it assists the commander in defining relative aspects of the operational environment in time and space. During step 1, the intelligence staff must identify those significant characteristics related to the mission variables of enemy, terrain, weather, and civil considerations that are relevant to the mission and justify that analysis to the commander. Failure to identify or misidentify the effect these variables may have on operations can hinder decisionmaking and result in the development of an ineffective information collection strategy/*intelligence collection strategy* and targeting effort.

1-13. Understanding friendly and enemy forces is not enough; other factors, such as culture, languages, tribal affiliations, and operational and mission variables, can be equally important. Defining the significant characteristics of the operational environment is essential in identifying the additional information needed to complete IPB. Once approved by the commander, this information becomes the command's initial intelligence requirements. This focuses the command's initial information collection efforts/*intelligence collection efforts* and the remaining steps of the IPB process.

1-14. ***For the Marine Corps, the term "operational environment" is consistent with the need to study and learn as much as possible about a situation. Essentially, commanders analyze the operational environment in order to determine the physical dimensions of their battlespace in the form of areas of interest, influence, and operations. (See MCDP 1-0.)***

STEP 2—DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS/*DESCRIBE THE EFFECTS ON OPERATIONS*

1-15. Once the intelligence staff has identified in step 1of IPB the significant characteristics related to enemy, terrain, weather, and civil considerations of the operational environment, step 2 describes how these characteristics affect friendly operations. The intelligence staff also describes how terrain, weather, civil considerations, and friendly forces affect enemy forces. This evaluation focuses on the general capabilities of each force until threat/*adversary* COAs are developed in step 4 of IPB and friendly COAs are developed later in the MDMP/*MCPP*. Finally, the entire staff determines the impact and effects to the population of friendly and enemy force actions.

1-16. If the intelligence staff does not have the information it needs to form conclusions, it uses assumptions to fill information gaps—always careful to ensure the commander understands when assumptions are used in place of fact to form conclusions. (Step 2 is discussed fully in chapter 4.)

STEP 3—EVALUATE THE THREAT/*ADVERSARY*

1-17. The purpose of evaluating the threat/*adversary* is to understand how a threat/*adversary* can affect friendly operations. Although threat/*adversary* forces may conform to some of the fundamental principles of warfare that guide Army/*Marine Corps* operations, these forces will have obvious, as well as subtle, differences in how they approach situations and problem solving. Understanding these differences is essential in understanding how a threat/*adversary* force will react in a given situation. Threat/*adversary* evaluation does not begin with IPB. The intelligence staff conducts threat/*adversary* evaluation and develops threat/*adversary* models as part of the generate intelligence knowledge task of support to force generation. Using this information, the intelligence staff refines threat/*adversary* models, as necessary, to support IPB. When analyzing a well-known threat/*adversary*, the intelligence staff may be able to rely on previously developed threat/*adversary* models. When analyzing a new or less well-known threat/*adversary*, the intelligence staff may need to evaluate the threat/*adversary* and develop models during the mission analysis step of the MDMP/*problem framing step of MCPP*. When this occurs, the intelligence staff relies heavily on the threat/*adversary* evaluation conducted by higher headquarters and other intelligence agencies.

1-18. In situations where there is no threat/*adversary* force, the intelligence analysis conducted and the products developed relating to terrain, weather, and civil considerations may be sufficient to support planning. An example of this type of situation is a natural disaster. (Step 3 is discussed fully in chapter 5.)

STEP 4—DETERMINE THREAT/*ADVERSARY COURSES OF ACTION*

1-19. During step 4 the intelligence staff identifies and develops possible threat/*adversary* COAs that can affect accomplishing the friendly mission. The staff uses the products associated with determining threat/*adversary* COAs to aid in developing friendly COAs during the COA development and selecting a friendly COA during COA steps of the MDMP/*MCPP*. The identification and development of all valid threat/*adversary* COAs minimize the potential of the commander being surprised by an unanticipated enemy action.

1-20. Failure to fully identify and develop all valid threat/*adversary* COAs may lead to the development of an information collection strategy/*intelligence collection strategy* that does not provide the information necessary to confirm what COA the enemy has taken and may result in the commander being surprised. When needed, the staff should identify all significant civil considerations (this refers to those civil considerations identified as significant characteristics of the operational environment) so that the interrelationship of threat/*adversary*, friendly forces, and population activities is portrayed.

1-21. The staff develops threat/*adversary* COAs in the same manner friendly COAs are developed. Although written specifically as a guide to develop friendly COAs, the COA development discussion in ADRP 5-0/*MCWP 5-1* is an excellent model to use in developing valid threat/*adversary* COAs that are suitable, feasible, acceptable, unique, and consistent with threat/*adversary* doctrine. Although the intelligence staff has the primary responsibility for developing threat/*adversary* COAs, it needs assistance from the rest of the staff to ensure the most accurate and complete analysis is presented to the commander. (Step 4 is discussed fully in chapter 6.)

INTELLIGENCE ESTIMATE

1-22. The intelligence estimate includes all the IPB products necessary to support planning and operations, such as—

- **Enemy situation overlays with associated COA statements and high-value target lists (HVTLs).**
- **Event templates and associated event matrices.**
- **Modified combined obstacle overlays (MCOOs), terrain effects matrices, and terrain assessments.**
- **Weather forecast charts, weather effects matrices/*operational impacts charts*, light and illumination tables, and weather estimates.**
- **Civil considerations overlays and assessments.**

STAFF INTEGRATION INTO IPB

1-23. Staff sections bring their own areas of expertise to IPB. Collaborative analysis among the staff facilitates a greater degree of situational understanding for the commander.

Collaboration Examples

The intelligence staff can provide the personnel staff with information on how the threat/*adversary* may affect personnel replacement or casualty evacuation.

The intelligence staff can provide the sustainment staff with threat/*adversary* information that may have an impact on friendly logistic efforts.

Conversely, the intelligence staff needs to utilize the expertise of the other staff sections.

Collaborating with the staff engineers can provide valuable information on terrain mobility, where the threat/*adversary* is likely to emplace obstacles, and where the threat/*adversary* could employ engineer assets.

Coordinating with the surgeon concerning the health status of threat/*adversary* forces can indicate the willingness of threat/*adversary* forces to engage in long-term operations.

1-24. Staff sections bring their expertise to IPB as follows:

- **The chief of staff, or executive officer—**
  - **Synchronizes staff activities during IPB.**
  - **Using tools, such as the one-third to two-thirds planning rule as a guide, determines—**
    - **How long each step of the MDMP/*MCPP* will take.**
    - **How much time is allocated to mission analysis/*problem framing*.**
- **How much time within mission analysis/*problem framing* can be sub-allocated to IPB. The G-2/S-2 has staff responsibility for the analysis of enemy, terrain, weather, and civil considerations. The G-2/S-2 aids the commander in improving the understanding of how these mission variables can affect operations through the production of an intelligence assessment that supports the MDMP/*MCPP*; the integrating processes of targeting and risk management; and the continuing activities of information collection/*intelligence collection* and security operations. The rest of the staff aids the G-2/S-2 in this effort.**
- **The G-3/S-3 is the staff subject matter expert (SME) on the art and science of military operations and aids the G-2/S-2 by—**
  - **Evaluating threat/*adversary* COAs to ensure they are valid from an operational perspective.**
  - **Evaluating enemy situation overlays, COA statements, HVTLs, and civil considerations overlays and assessments to ensure they contain the information necessary to support friendly COA development and analysis.**
  - **Evaluating the event template and matrix to ensure they contain the information necessary to support friendly COA analysis and the development of the decision support template.**
- **The G-4/S-4 is the staff SME on sustainment operations and aids the G-2/S-2 by—**
  - **Assisting in identifying and evaluating threat/*adversary* and host-nation logistic capabilities.**
  - **Assisting in identifying potential supply routes and resupply points.**
- **The G-6/S-6 is the staff SME on friendly communications systems and aids the G-2/S-2 by assisting in identifying and evaluating friendly communications systems' vulnerabilities to cyber and electronic attack.**
- **For U.S. Army, the Information Operations Office is responsible for integrating information-related capabilities and aids the G-2/S-2 by assisting in identifying and evaluating threat/*adversary* information capabilities and deception and denial capabilities, as well as the means to influence the population. *For the Marine Corps, the G-3/S-3 is responsible for information operations.***
- **For U.S. Army, the G-9/S-9 is the staff SME on civil affairs operations. *For the Marine Corps, the G-3/S-3 is responsible for civil affairs.* This section aids the G-2/S-2 by—**
  - **Assisting in identifying and evaluating civil considerations on military operations and evaluating the effect of military operations on civilian populations in conjunction with the G-3/S-3.**
  - **Assisting, along with the chief of fires or fire support officer/*fire support coordinator or force fires coordinator,* in identifying protected targets.**
  - **Creating and maintaining civil considerations assessments, files, and data files and/or databases.**
- **For U.S. Army, the chief of fires at division and above and the fire support officer at brigade and below is the staff SME on fires. *For the Marine Corps, the fire support coordinator at battalion, the Marine expeditionary unit, regiment, and division and the force fires coordinator at the Marine expeditionary brigade and the Marine expeditionary force is the SME on fires.* The SME on fires (artillery and air defense) aids the G-2/S-2 by—**
  - **Assisting in developing threat/*adversary* high-value targets (HVTs).**
  - **Assisting in evaluating threat/*adversary* fire support operations, including identifying potential friendly high-payoff targets (HPTs) from the threat/*adversary* perspective.**

  - Assisting in positioning threat/*adversary* fire support assets on the situation template.
  - Assisting the staff on protection from threat/*adversary* air and aids the G-2/S-2 by assisting in identifying enemy air avenues of approach (AAs) and in assessing threat/*adversary* fixed-wing, rotary-wing, and air defense capabilities.
- The engineer coordinator is the staff SME on mobility and countermobility and aids the G-2/S-2 by assisting in developing enemy obstacle plans for the threat/*adversary* situation overlay.
- The chemical, biological, radiological, and nuclear (CBRN) officer is the staff SME on CBRN and aids the G-2/S-2 by assisting in determining the locations of CBRN assets and potential areas of employment.
- The surgeon is the staff SME for the analysis and disposition of captured enemy medical materiel and for the analysis of any medications carried by captured or detained threat/*adversary* personnel.

1-25. Deployed units will have additional subject matter expertise that will have input to the IPB process, such as the following groups:

- For U.S. Army, human terrain teams (HTTs), when available, can provide sociocultural research and analysis of the population that supports the intelligence staff's analysis of civil considerations. Units that support corps, divisions, and brigade combat teams without a HTT get this support from the supported headquarters. *For the Marine Corps, when available, foreign area officers, regional affairs officers, other cultural enablers, State Department officers, and other knowledgeable sources can provide sociocultural information, research, and analysis of the population.*
- Red Teams.

RELATIONSHIPS

1-26. As one of the integrating processes, IPB is integral to targeting, risk management, information collection/*intelligence collection*, planning, and decisionmaking. IPB is also related to generate intelligence knowledge and situation development.

TARGETING

1-27. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. During steps 3 and 4 of IPB, the intelligence staff identifies HVTs associated with each threat/*adversary* capability or COA. This aids the fires cell in conducting target-value analysis (TVA). The following techniques may be useful in identifying and evaluating HVTs:

- Identify HVTs from existing intelligence studies, evaluation of the databases, patrol debriefs, and size, activity, location, unit, time, and equipment (SALUTE) reports. A review of threat/*adversary* tactics, techniques, and procedures (TTP) and previous threat/*adversary* operations as well as understanding threat/*adversary* objectives, tasks, purpose, and intent will be useful.
- Identify assets that are key to executing the primary operation or sequels.
- Determine how the threat/*adversary* might react to the loss of each identified HVT. Consider the threat's/*adversary*'s ability to substitute other assets as well as to adopt branches or sequels.

1-28. After identifying the set of HVTs, place them in order of their relative worth to the threat's/*adversary*'s operation and record them as part of the threat/*adversary* model. A HVT's value will vary throughout an operation.

1-29. The high-payoff target list (HPTL) is a prioritized list of HPTs. A high-payoff target is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action (JP 3-60). HPTs are those HVTs that must be acquired and successfully attacked for the success of the friendly commander's mission. HPTs are developed by the staff, and can include various threat/*adversary* considerations that can be detrimental to the success of friendly missions.

1-30. The intelligence staff, aided by other warfighting staffs, also identifies the indicators associated with these targets that assist in determining their location and activities. Chapter 6 discusses the development of HVTs and indicators. Developing HVTs during IPB is essential to developing HPTs during the COA development step of MDMP/*MCPP*, and refining those targets throughout the operations process, particularly during targeting boards and meetings. During targeting meetings, the intelligence officer, along with other staff elements, assesses friendly capabilities, friendly missions, and the effects of friendly actions on the civilian populace. As HPTs are identified, the analysis of enemy, terrain, weather, and civil considerations conducted during IPB aids in developing intelligence target packages on these targets. (See FM 3-60 for more information on targeting.)

RISK MANAGEMENT

1-31. Risk management is a process for identifying hazards and controlling risks. Throughout the operations process commanders and staffs use risk management to mitigate risks associated with all hazards that have the potential to injure or kill friendly and civilian personnel, damage or destroy equipment, or otherwise impact mission effectiveness. (See ATP 5-19 for additional information on risk management.)

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE AND INFORMATION COLLECTION/*INTELLIGENCE COLLECTION*

1-32. Information collection/*intelligence collection* relies on the results of IPB. The staff's completion of IPB provides an analysis of the operational environment and the options it presents to friendly and threat/*adversary* forces. It also provides information required to plan information collection/*intelligence collection* activities, such as—

- **Characteristics of the area of interest that will influence friendly and threat/*adversary* operations (including civil considerations).**
- **Enemy event templates, including decision points and matrices critical to information collection planning.**
- **Information collection assets' sensitivities to weather and the effects of weather on planned or potential operations.**
- **Threat characteristics/*adversary order of battle*, doctrine, tactics, techniques, and behavior.**
- **Possible and likely threat/*adversary* COAs.**
- **HVTs.**

1-33. The Army/*Marine Corps* executes intelligence, surveillance, and reconnaissance through the operations and intelligence processes (with an emphasis on intelligence analysis and leveraging the larger intelligence enterprise) and information collection/*intelligence collection*. The intelligence staff identifies and taps into ongoing or existing information collection activities or joint intelligence, surveillance, and reconnaissance collection that may offer relevant information to fill gaps. These requirements identify the critical pieces of information that the commander must know to successfully plan, prepare, execute, and assess operations.

1-34. There is a relationship between IPB and information collection/*intelligence collection*. All of the IPB products feeding intelligence drive information collection/*intelligence collection* requirements; this means that the IPB process identifies intelligence gaps that are translated into information requirements and priority intelligence requirements (PIRs), which are then answered through collection.

1-35. The staff collaborates on information/*intelligence* considerations and works to integrate available resources into an integrated information collection plan. Developing requirements also supports the commander's decisionmaking regarding targeting. Well-stated information requirements help the commander to accomplish the mission by illustrating those key knowledge gaps and earmarking them for collection.

1-36. To effectively target the threat/*adversary*, the staff develops named areas of interest (NAIs) and target areas of interest. (The staff also develops an HVTL that can include geographic NAIs and TAIs as well as enemy/*adversary* organizations, networks, and individuals identified as key or critical to the

operational environment and are taken into account in branches and sequels.) NAIs should not be tied to a specific terrain; rather, they should be based upon the enemy locations or suspected locations.

> **NAI Example**
>
> Rather than looking at an area surrounding a hilltop named 1631 to see if the enemy has placed an air defense unit there, NAIs should be focused on an enemy unit or functional capability; for example, the suspected locations where the enemy may place his combined arms reserve. In order to refine the locations, analysts should study the enemy's doctrinal or historical use of the combined arms reserve, coupled with the capabilities of the critical combat systems associated with the combined arms reserve, and the known rates of march for the terrain in which the combined arms reserve will be operating.

1-37. Units need to consistently and continuously conduct information collection/*intelligence collection*. In order to be effective, information collection/*intelligence collection* must be based on the results of IPB and adjusted as the results of IPB are refined through the situation development process. Conversely, the results of reconnaissance, surveillance, security operations, and intelligence operations drive the refinement of IPB as appropriate. The staff must understand the roles and relationships of reconnaissance, surveillance, security operations, and intelligence operations and how the commander assesses ongoing operations as the unit develops the situation through action.

1-38. Commanders plan for and the staff controls the execution of all information collection/*intelligence collection* means throughout the operation. The unit must carefully plan for and synchronize reconnaissance, surveillance, security operations, and intelligence operations because the threat/*adversary* will try to use deception and other means to evade friendly collection efforts. Commanders need to know detailed information/*intelligence* about the threat/*adversary* disposition, capabilities, and intentions. Often it is necessary to designate a combined arms unit to develop the situation through close contact with the threat/*adversary* or civilian population.

GENERATE INTELLIGENCE KNOWLEDGE

1-39. Generate intelligence knowledge begins before mission receipt and provides the relevant knowledge required regarding the operational environment for the conduct of operations. As soon as the intelligence officer and other staff sections begin to collect data on the operational environment, they organize the data into databases. The information and intelligence obtained are refined into knowledge for use in mission analysis/*problem framing* through functional analysis. Information is obtained through intelligence reach; research; data-mining; database access; academic studies, products, or materials; intelligence archives; open-source intelligence; reconnaissance and security operations; and other information sources. Generate intelligence knowledge is the foundation for performing IPB and mission analysis/*problem framing*. The primary product of the generate intelligence knowledge task is the creation of initial data files based on the analysis of the operational variables of PMESII-PT/*PMESII* and the intelligence survey. (See ADRP 2-0 for more information on generate intelligence knowledge.)

1-40. ***First published in 1995, the*** **Marine Corps Generic Intelligence Requirements Handbook (GIRH)** ***promulgates frequently used PIRs and information requirements to facilitate crisis planning for Marine expeditionary forces (MEFs). The GIRH details baseline intelligence requirements to allow Marines to efficiently request updated, accurate, and complete information. Intelligence Marines can use a GIRH as a checklist to identify information gaps, a reference when requesting information, or a baseline support tool when providing intelligence to operational units. In addition to the original GIRH, the Marine Corps Intelligence Activity (MCIA) has produced the following specific GIRHs:***

- ***Police forces.***
- ***Cultural.***
- ***Jungle.***

- ***Riverine.***
- ***Urban.***
- ***Information operations.***

1-41. ***All GIRHs are available on MCIA's Joint Worldwide Intelligence Communications System and SECRET Internet Protocol Router Network (SIPRNET) Web sites.***

SITUATION DEVELOPMENT

1-42. Situation development is a process for analyzing information and producing current intelligence concerning the portions of the mission variables of enemy, terrain, weather, and civil considerations within the AO before and during operations. The process helps the intelligence staff recognize and interpret indicators of threat/*adversary* intentions and objectives. Situation development confirms or denies threat/*adversary* COAs, provides threat/*adversary* locations, explains what the threat/*adversary* is doing in relation to the friendly force commander's intent, and provides an estimate of threat/*adversary* combat effectiveness.

1-43. The locations and actions of noncombatant elements and nongovernmental organizations (NGOs) in the AO that may impact operations are also considered. Through situation development, the intelligence officer—

- **Quickly identifies information gaps.**
- **Recommends new information requirements.**
- **Explains threat/*adversary* activities in relation to the unit's operations.**
- **Assists the commander in gaining and maintaining situational understanding.**

1-44. Situation development helps commanders make decisions, including when to execute branches and sequels. The intelligence staff uses the products developed during IPB as a baseline to begin situation development.

This page intentionally left blank.

Chapter 2
IPB Support to Decisionmaking During Planning

IPB AND DECISIONMAKING

2-1. Decisionmaking refers to selecting a COA as the one most favorable to accomplish the mission. Decisionmaking includes knowing whether to decide or not, then when and what to decide, and finally understanding the consequences. (See ADRP 3-0 for further discussion on decisionmaking.) Commanders make decisions in part based on the intelligence developed during initial IPB and on the refinement of that intelligence throughout the operations process. (See ADRP 5-0 for further discussion on the operations process. *See MCWP 5-1 for further discussion on MCPP*.)

2-2. Commanders require accurate and timely intelligence about the operational environment in order to make informed and good decisions. Through IPB, the staff aids the commander's understanding of how the enemy, terrain, weather, and civil considerations influence the operational environment and affect operations. IPB also helps the commander understand how to influence, use, or employ these variables to achieve desired conditions and end state. IPB is essential in helping the commander to understand, visualize, and describe the operational environment, make and articulate decisions, and assess military operations.

- **Understand operations. Understanding involves analyzing the mission variables in a given operational environment. IPB defines and describes the mission variables of enemy, terrain, weather, and civil considerations but, more importantly, concludes how the interrelationships, dynamics, and interactions of these variables cause changes in the operational environment.**
- **Visualize operations. Visualization involves developing situational understanding, determining an end state, and envisioning the sequence of events the force must ensure to achieve the end state. Every product developed during IPB is essential in aiding the commander in visualizing the situation. These products must be produced on time and in accordance with unit standard operating procedures.**
- **Describe operations. After commanders visualize an operation, they communicate their vision to their staffs and subordinate commands using the staff products developed during IPB.**

IPB AND PLANNING

2-3. Commanders conduct planning in order to understand a problem or situation; envision a desired future, and, with the assistance of their staffs, develop COAs that can bring about that future. During planning commanders focus their activities on understanding, visualizing, and describing, while directing and assessing. IPB is one of the processes commanders use to aid in planning. IPB supports the MDMP/*MCPP* and troop leading procedures (TLP).

MILITARY DECISIONMAKING PROCESS/*MARINE CORPS PLANNING PROCESS*

2-4. The MDMP/*MCPP* methodology integrates the activities of the commander, staff, subordinate headquarters, and other partners to—

- **Understand the situation and mission.**
- **Develop and compare COAs.**
- **Decide on a COA that best accomplishes the mission.**
- **Produce an operation plan (OPLAN) or operation order (OPORD) for execution.**

2-5. For the Army, the MDMP is a seven-step planning methodology comprising—

- **Receipt of mission.**
- **Mission analysis.**
- **COA development.**
- **COA analysis (wargaming).**
- **COA comparison.**
- **COA approval.**
- **Orders production, dissemination, and transition.**

2-6. ***For the Marine Corps, the MCPP is a six-step process comprising—***

- ***Problem framing.***
- ***COA development.***
- ***COA wargaming.***
- ***COA comparison and decision.***
- ***Orders development.***
- ***Transition.***

2-7. Figure 2-1 shows the relationship between IPB and the steps of MDMP/*MCPP*. (See ADRP 5-0 for more information on the MDMP.) ***Appendix A and MCWP 5-1 provide more information on MCPP.***

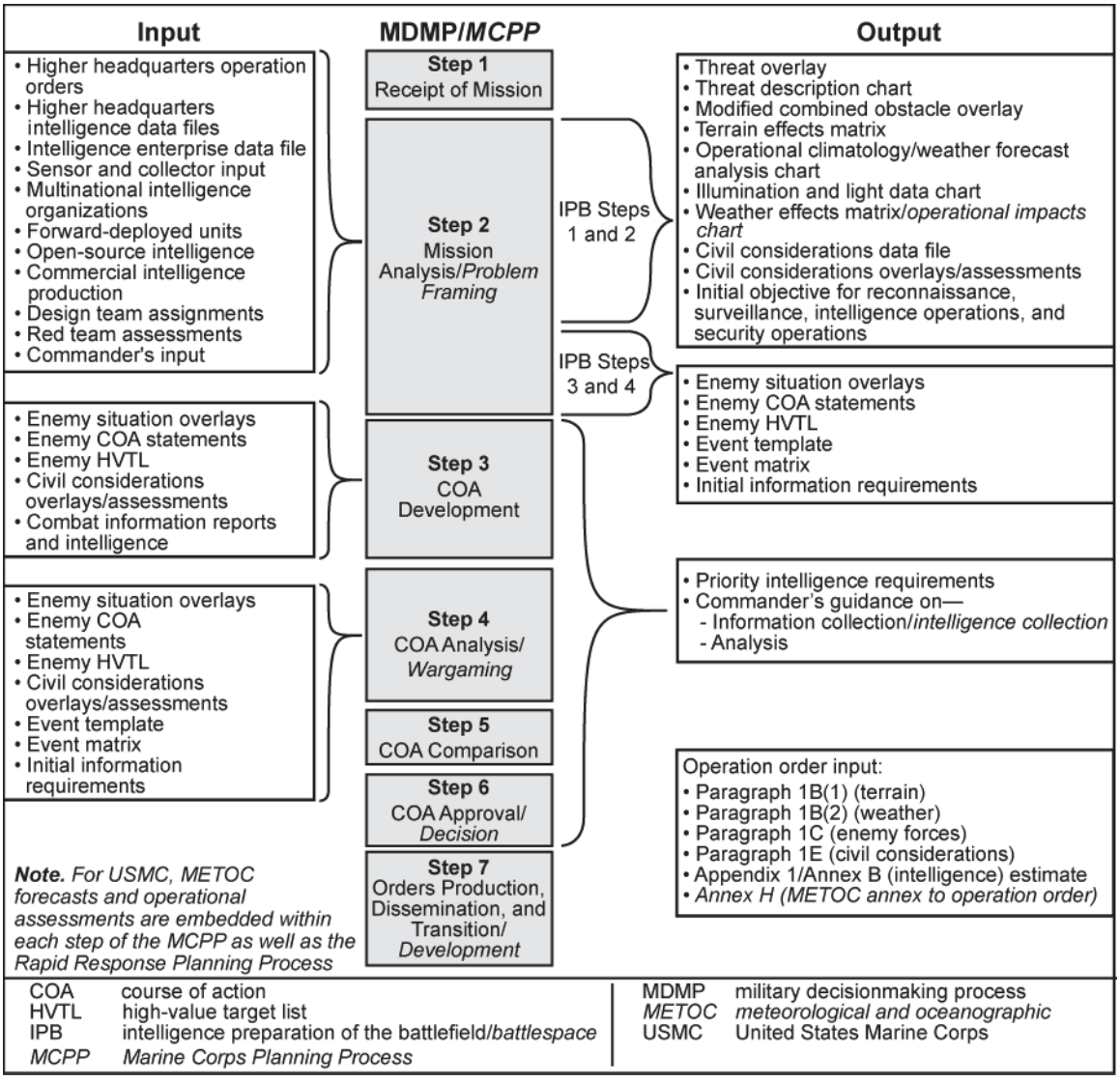


Figure 2-1. IPB and the MDMP/*MCPP* steps

Troop Leading Procedures

2-8. The TLP extend the MDMP to the small-unit level. The MDMP and TLP are similar but not identical. Troop leading procedures are a dynamic process used by small-unit leaders to analyze a mission, develop a plan, and prepare for an operation (ADP 5-0). These procedures enable leaders to maximize available planning time while developing effective plans and preparing their units for an operation.

2-9. The sequence of actions assists leaders to effectively and efficiently use available time to issue orders and execute tactical operations. TLP consist of eight steps. The sequence of the steps is not rigid. Leaders modify the sequence to meet the mission, situation, and available time. The following steps are done concurrently while others may go on continuously throughout the operation.

- **Step 1 – Receive the mission.**
- **Step 2 – Issue a warning order.**
- **Step 3 – Make a tentative plan.**
- **Step 4 – Initiate movement.**
- **Step 5 – Conduct reconnaissance.**
- **Step 6 – Complete the plan.**
- **Step 7 – Issue the order.**
- **Step 8 – Supervise and refine.**

2-10. The intelligence staff at the battalion develops and provides all the IPB products the company commander needs to do TLP. The commanders should not need to do any other refinement of these products.

2-11. The standard IPB products the battalion provides to assist the commander for TLP includes—

- **Enemy situation overlays and COA statements.**
- **Terrain and weather products.**
- **Tactical decision aids (such as the MCOO and the evaluation of terrain effects, weather forecast weather effects, and light data tables).**
- **Civil considerations tools and products.**

Note. **Company commanders coordinate with the battalion intelligence staff for any IPB products or tools they think they will need.**

2-12. However, due to the lack of a staff, resources, and time constraints, the small-unit leader depends on the timely delivery of IPB products developed by higher headquarters tailored to support small-unit planning. Specifically, the components of IPB inform steps 2 through 5 and actions within TLP, as discussed below.

Step 2—Issue a Warning Order

2-13. The battalion intelligence staff provides IPB products to the company commander on what to include in warning orders for areas such as but not limited to—

- **Terrain analysis.**
- **Enemy forces.**
- **AOs and areas of interest.**
- **Commander's critical information requirements (CCIRs) and essential elements of friendly information (EEFIs).**
- **Risk guidance.**
- **Surveillance and reconnaissance to initiate.**
- **Security measures.**

- **Deception guidance.**
- **Mobility and countermobility.**
- **Guidance on rehearsals.**

Step 3—Make a Tentative Plan

2-14. When developing a tentative plan, the company commander relies on the battalion intelligence staff to provide IPB tools as the leader conducts the mission analysis, COA development, COA analysis, and COA comparison and selection (PIRs, friendly force information requirement, and EEFIs).

2-15. The battalion intelligence staff provides IPB tools and products for the leader on mission analysis by evaluating enemy, terrain, weather, and civil considerations. This includes providing information and analysis on the terrain, enemy, and friendly forces that most affect tactical operations.

2-16. In COA development, the battalion intelligence staff provides IPB products to assist the leader in the construct of a solid COA. The purpose of COA development is to determine one or more ways to accomplish the mission that is consistent with the immediate higher commander's intent. A COA describes how the unit might generate the effects of overwhelming combat power against the enemy at the decisive point with the least friendly casualties.

2-17. The battalion intelligence staff provides tools from IPB to leaders during COA analysis. COA analysis begins with both friendly and enemy COAs and, using a method of action-reaction-counteraction wargame, results in a synchronized friendly plan, identified strengths and weaknesses, and updated risk assessment. After developing the COA, the leader analyzes it to determine its strengths and weaknesses and gains insights into actions at the decisive point of the mission. COA analysis (wargaming) brings together friendly and enemy forces on the actual terrain to visualize how the operation will unfold. Wargaming helps the leader synchronize friendly actions while considering the likely reactions of the enemy. The battalion intelligence staff provides IPB tools the leader can use to determine how the enemy will likely react during wargaming.

2-18. During COA comparison and selection, the battalion intelligence staff provides products from IPB to leaders to determine PIRs, friendly force information requirement, and EEFIs. Even though EEFIs are not part of the CCIRs, they still become priorities, and this information must be protected from identification by the enemy.

Step 4—Initiate Movement

2-19. The battalion intelligence staff provides IPB products to leaders on any movement necessary to continue mission preparation or to posture the unit for the start of the mission.

Step 5—Conduct Reconnaissance

2-20. If time permits, leaders verify intelligence from higher headquarters by reconnoitering visually to seek to confirm PIRs that support their tentative plans. These PIRs usually consist of assumptions or critical facts about the enemy (to include strength and location). The PIRs can also include information on the terrain (to verify that a tentative support-by-fire position can suppress the enemy or an AA is useable).

Understand the Situation and Mission

2-21. During the mission analysis step of the MDMP/*problem framing step of MCPP*, the staff conducts IPB in order to understand the situation and mission. The IPB products developed during this step are discussed fully in chapters 3 through 6. The products listed below are critical to developing and comparing COAs, deciding on a COA, and producing an OPORD:

- **Intelligence gaps.**
- **Information requirements.**
- **Enemy situation templates with an associated threat/*adversary* COA statement and HVTL.**
- **Event template with associated event matrix.**
- **Relative combat power matrix for enemy forces.**

- **Geospatial intelligence tactical decision aids required to support continued planning (terrain effects).**
- **Weather tactical decision aids required to support continued planning (operational climatology or weather forecast analysis chart and weather effects matrix).**
- **Civil considerations tactical decision aids required to support continued planning (civil considerations effects).**
- **Estimates on how other significant variables may affect the mission.**
- **Reconnaissance objectives.**
- **The tempo and focus of reconnaissance, surveillance, security operations, and intelligence operations to answer PIRs and meet other requirements.**

Develop and Compare COAs

2-22. In the COA development step of the MDMP/*MCPP*, friendly COAs are broad potential solutions to an identified problem. These solutions are based on the conclusions reached during initial IPB and any refinement of those conclusions that occurs between the conclusion of mission analysis/*problem framing* and the beginning of COA development. The primary IPB product required for COA development is the enemy situation template with an associated enemy COA statement.

Decide on a COA that Best Accomplishes the Mission

2-23. In the COA analysis/*wargaming* step of the MDMP/*MCPP,* deciding on a COA enables commanders and staffs to identify difficulties or coordination problems as well as probable consequences of planned actions for each COA being considered. The primary IPB products required for deciding a COA are—

- **The enemy situation template with an associated enemy COA statement.**
- **The event template with the associated event matrix.**
- **The relative combat power matrix for enemy forces.**

2-24. During counterinsurgency operations and stability tasks, additional products may be required such as civil considerations overlays and assessments. Information collection/*intelligence collection* operations undertaken at the mission analysis/*problem framing* step of the MDMP/*MCPP* will provide pertinent combat information that will inform COA development. This information confirms or denies the enemy situation template and associated enemy COA statement.

Produce an OPLAN or OPORD for Execution

2-25. At the conclusion of the MDMP/*MCPP*, the staff prepares the OPLAN or OPORD by turning the selected COA into a clear, concise concept of operations and required supporting material. The results of IPB are included within the base order and appropriate annexes.

RAPID DECISIONMAKING AND SYNCHRONIZATION PROCESS/*RAPID RESPONSE PLANNING PROCESS*

2-26. The rapid decisionmaking and synchronization process (RDSP)/*rapid response planning process (R2P2)* is a technique that commanders and staff commonly use during execution. Throughout mission execution, continuous information collection is conducted to answer information requirements and to close intelligence gaps. The RDSP/*R2P2* is usually conducted based on an existing OPORD that includes the IPB products and estimates produced during MDMP/*MCPP*. (See ADRP 5-0 for more information on the RDSP. *See MCWP 5-1 for more information on R2P2*.)

2-27. For the U.S. Army, RDSP includes five steps:

- **Compare the current situation to the order. During execution, the staff is continually refining the running estimates based on new information. Part of this process is to compare the current situation to the situation expressed in the OPORD to determine whether adjustments need to be made to the OPLAN and identify any decisions the commander may need to make. During execution, the staff looks for indicators of change variances that may affect the overall operation.**

These change variances must be identified in order for the commander to make necessary modifications to the OPLAN. The event template and event matrix and the decision support template developed during step 4 of IPB are the primary IPB tools the staff uses to identify variances and alert the commander to situations that require a decision. These products are updated as changes occur.

- **Determine that a decision, and what type, is required. When a variance is identified, the staff describes the variance and determines if it provides a significant opportunity to either friendly forces or the threat/*adversary*.**
- **Develop a COA. If the situation warrants the development of a new friendly COA, it may result in the creation of new or modified PIRs and HVTs. It may also require the creation of a new or modified event template and event matrix.**
- **Refine and validate the COA. During this step, the commander and staff conduct a mental wargame of the new COA. At a minimum the enemy situation template and COA statement, along with friendly operations graphics and COA statement, are required to focus the mental wargame.**
- **Implement. The commander normally implements the new COA by issuing a fragmentary order. The following IPB products are issued as part of that fragmentary order:**
  - **IPB products including enemy situation template with COA statement and HPTL, terrain, weather, and civil considerations products.**
  - **Updated PIRs.**

2-28. ***The Marine Corps R2P2, as defined in MCWP 5-1, is a time-constrained six-step process that includes—***

- ***Problem framing*.**
- ***COA development.***
- ***COA wargame.***
- ***COA comparison and decision.***
- ***Orders development.***
- ***Transition.***

PART TWO

Fundamental Task Techniques

Chapter 3

Step 1 of the IPB Process—Define the Operational Environment

WHAT IS IT?

3-1. Step 1 of the IPB process identifies for further analysis the significant characteristics of the operational environment that may influence friendly COAs and command decisions. Within an operational environment, an Army leader may be faced with major combat, military engagements, and humanitarian assistance simultaneously in the same AO. The following examples portray planning scenarios.

Example 1

During planning for a foreign humanitarian task, a brigade/*unit* S-2 identifies five ethnic groups that have armed militias that have attacked each other, as well as indigenous governmental security forces over the past 12 months. In the last month, a helicopter from the nation's Army was shot down by a rocket-propelled grenade. Although these militias have not attacked any of the nongovernmental aid organizations in the area, they have demonstrated the willingness to use violence. Because of this, the S-2 determines each of these groups is a potential threat/*adversary*. There is no information about these groups in the command's intelligence data files or in the data files of their higher headquarters to aid the S-2 in developing valid potential COAs these groups may adopt when U.S. forces enter their AOs.

The S-2 staff conducts a search of various organizations' data files within the intelligence enterprise. The staff determines that while little is known about the threat characteristics/*adversary order of battle* of these militias, there is some information available. Each of these militias is a company-sized element with various types of small-arms and crew-served weapons, mortars, demolitions, and anti-armor rockets. It is not known whether these militias have any air defense artillery.

The S-2 initiates a request for collection on the current location, disposition, strength, and capabilities of each of these militias. Realizing that he will not have this information during IPB, the S-2 determines possible threat/*adversary* COAs based on what he knows and what he assumes, ensuring that the commander and the rest of the staff understand what is known and what is assumed about the threat/*adversary*. As intelligence related to the request for collection arrives, the S-2 updates the threat/*adversary* COAs and informs the commander and the rest of the staff.

Example 2

During planning for an attack, a brigade/*unit* S-2 identifies the enemy has an attack helicopter squadron that could threaten the friendly mission. When developing the enemy situation overlay, the S-2 includes the reported location of the attack helicopter battalion, air attack corridors that could be used to support the enemy defense, and forward arming and refueling points. The S-2 also generates collection requests to locate and track these assets in support of the command's targeting operations.

DESIRED END STATE

3-2. Step 1 of the IPB process focuses the IPB effort on the characteristics of the operational environment that can influence friendly and threat/*adversary* operations. The intelligence staff acquires the intelligence needed to complete IPB in the degree of detail required to support the decisionmaking process. The primary outputs associated with step 1 of the IPB process may include developing the—

- **Determination of the AO and area of interest.**
- **Determination of the area of intelligence responsibility.**
- **Identification of general characteristics of the AO that could influence the unit's mission.**
- **Identification of gaps in current intelligence holdings, translating them into requirements for collection (requests for information, requests for collection) in order to complete IPB.**

SO WHAT?

3-3. The "so what" in this step is clearly defining for the commanders what the relevant characteristics of their areas of interest are.

- **Success results in saving time and effort by focusing only on those characteristics that will influence friendly COAs and command decisions.**
- **Consequences of failure:**
  - **Failure to focus on only the significant characteristics leads to wasted time and effort collecting and evaluating intelligence on characteristics of the operational environment that will not influence the operation.**
  - **Failure to identify all the significant characteristics may lead to the command's surprise and unpreparedness when some overlooked feature of the operational environment has an effect on the operation for which the commander did not plan.**

HOW TO DO IT: (THE PROCESS)

3-4. Defining the operational environment consists of the sub-steps shown in figure 3-1.

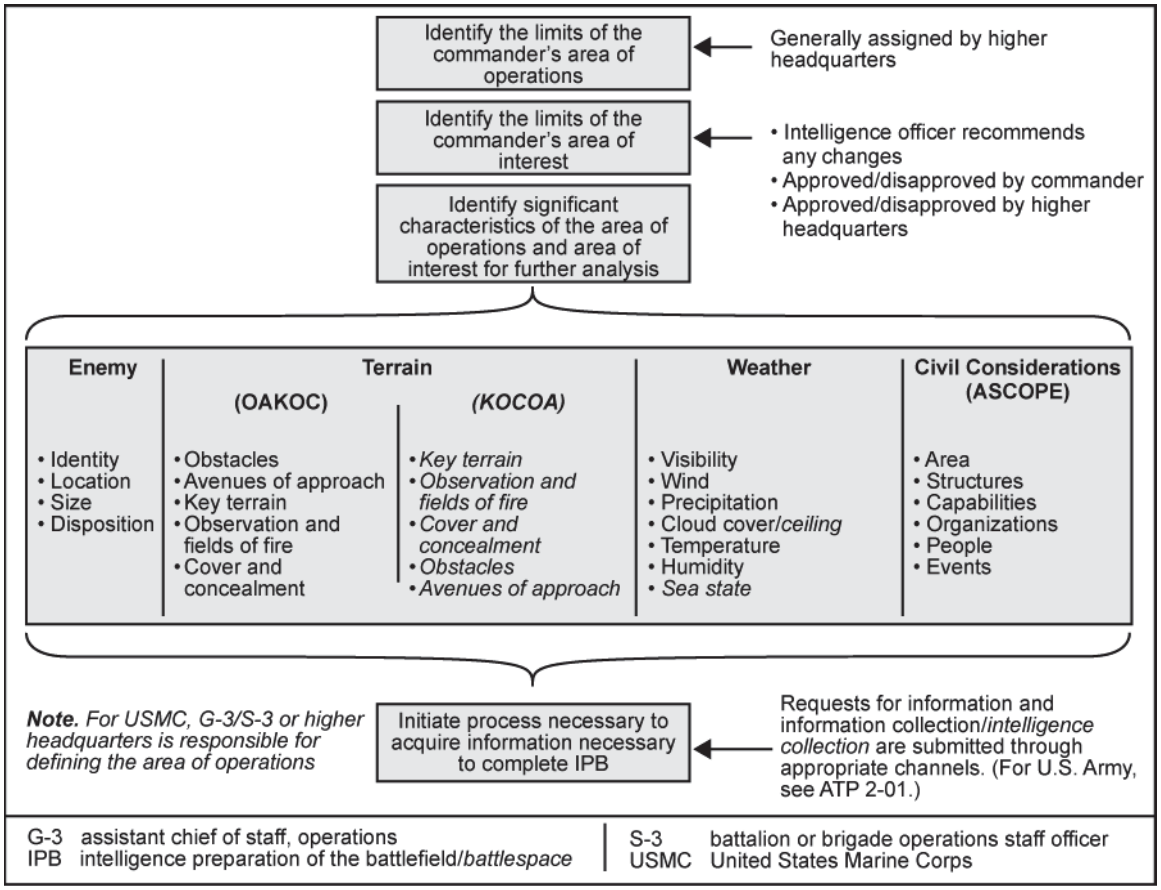


Figure 3-1. Sub-steps of step 1 of the IPB process

IDENTIFY THE LIMITS OF THE COMMANDER'S AREA OF OPERATIONS

3-5. The area of operations is defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces (JP 3-0). The AO is comprised of an external boundary that delineates the AOs of adjacent units and includes subordinate unit AOs. Subordinate unit AOs may be contiguous or noncontiguous. Parts of an AO not assigned to subordinate units are called deep areas. The AO may be impacted due to political boundaries and/or other civil considerations. Once assigned, an AO can be subdivided by that command, as necessary, to support mission requirements. Figure 3-2 on page 3-4 illustrates various AOs.

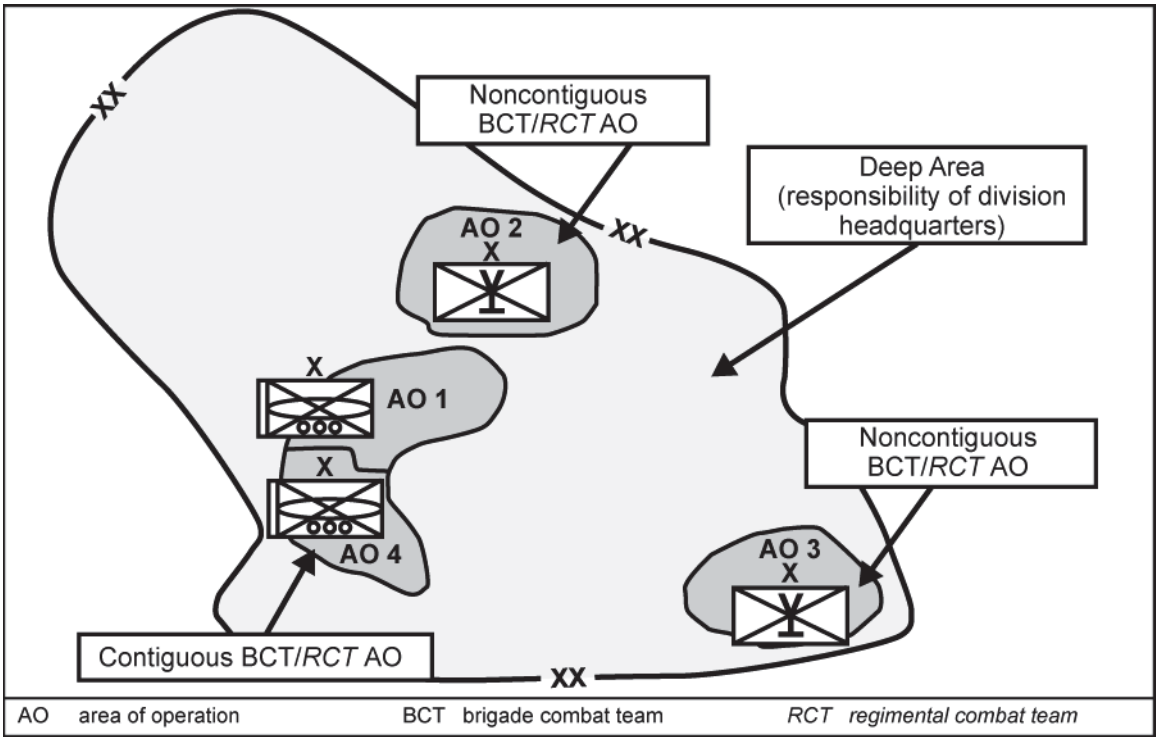


Figure 3-2. Example areas of operations

3-6. An area of influence is a geographical area where a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control (JP 3-0). The area of influence is—

- **An area that includes terrain inside and outside the AO.**
- **An area determined by both the G-2/S-2 and the G-3/S-3.**

IDENTIFY THE LIMITS OF THE COMMANDER'S AREA OF INTEREST

3-7. An area of interest is that area of concern to the commander, including the area of influence, areas adjacent thereto and extending into enemy territory. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission (JP 3-0). The area of interest is—

- **Established by the commander with input from the G-2/S-2 or G-3/S-3. The mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC)/*mission, enemy, terrain and weather, troops and support available, time available (METT-T)* factors must be considered.**
- **An area normally larger than the area of influence and may require more intelligence assets to monitor. It may include staging areas.**

3-8. The area of interest is a geographical area from which information and intelligence are required to execute successful tactical operations and to plan for future operations. It includes any threat/*adversary* forces or characteristics that will significantly influence accomplishing the command's mission. In combat operations/*major operations*, the area of interest extends into enemy territory to the objectives of current or planned friendly operations if those objectives are located outside the assigned AO. In stability operations or defense support of civil authorities operations, the area of interest is typically much larger than that defined for combat operations/*major operations*.

3-9. An additional consideration would be to divide the area of interest into several components; for example, ground area of interest and air area of interest. Such a division accommodates the types of information relevant to each area of interest as well as their usually different geographical limits. At some

point, it will likely become necessary to integrate the various areas of interest into a whole in order to present the commander with a complete, integrated picture.

3-10. An area of interest may be irregular in shape and overlap the areas of adjacent and subordinate unit AOs. The area will change as the situation changes and as commanders determine new information requirements. It is the geographical area from which information is required to facilitate planning and the successful conduct of the command's operation.

Analyzing the Area of Operations

By analyzing a commander's AO in terms of the area of influence and area of interest, a commander determines whether the assigned AO is appropriate. This analysis may include the forces' capabilities to conduct actions across the warfighting functions. Commanders consider the extent of subordinates' areas of influence when defining subordinates' AOs. In identifying an AO, the staff should avoid making it substantially larger than the unit's area of influence. Ideally, the entire AO is encompassed by the area of influence. The area of influence is useful to the commander in focusing information collection operations to shape the battlefield/*battlespace* to facilitate future operations.

3-11. ***For the Marine Corps, battlespace includes the area of interest, area of influence, and operational areas. Operational areas for Marine air-ground task forces (MAGTFs) are usually an AO. The staff may recommend battlespace refinements based on the analysis of the terrain and tasks as well as friendly and adversary centers of gravity, capabilities, and limitations. The size of the area of interest may change based on the commander's understanding of the situation. The area of influence is a geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control (JP 3-0). The extent of the area of influence may change if forces are added or deleted, equipment capability (for example, the range of lethal and nonlethal weapon systems) and availability change, or rules of engagement change. The commander's AO may need to change based on the scope of the mission, the results of operations, operational reach, or to ensure sufficient battlespace to maneuver and protect his force.***

IDENTIFY SIGNIFICANT CHARACTERISTICS WITHIN THE AREA OF OPERATIONS AND AREA OF INTEREST FOR FURTHER ANALYSIS

3-12. In order to focus IPB and what is important to the commander, the staff identifies and defines the aspects of the enemy, terrain, weather, and civil considerations of the operational environment to determine the significance of each in relation to the mission; essentially building an environmental model as the framework to conduct and then present analysis to the commander. This prevents unnecessary analysis and allows the staff to maximize resources on critical areas. The initial analysis that occurs in this sub-step determines the amount of time and resources the intelligence staff commits to the detailed analysis that occurs in step 2 of the IPB process.

ENEMY

3-13. An enemy is a party identified as hostile against which the use of force is authorized (ADRP 3-0). Analysis of the enemy includes not only the known enemy but also other threats/*adversaries* to mission success. Such threats/*adversaries* might include multiple adversaries posing with a wide array of political, economic, religious, and personal motivations. Additionally, threats/*adversaries* may wear uniforms and easily be identifiable. Or, they may not wear uniforms and blend into the population. To understand threat/*adversary* capabilities and vulnerabilities, commanders and staffs require detailed, timely, and accurate intelligence produced as a result of IPB.

TERRAIN AND WEATHER

3-14. Terrain and weather are natural conditions that profoundly influence operations. Terrain and weather favor neither friendly nor enemy forces unless one is more familiar with—or better prepared to operate in—the physical environment. Terrain includes natural features (such as rivers and mountains) and manmade features (such as cities, airfields, and bridges). Terrain directly affects how commanders select objectives and locate, move, and control forces. Terrain also influences protective measures and the effectiveness of weapons and other systems.

3-15. Effective use of terrain reduces the effects of enemy fires, increases the effects of friendly fires, and facilitates surprise. Terrain appreciation—the ability to predict its impact on operations—is an important skill for every leader. For tactical operations, commanders analyze terrain using the five military aspects of terrain, expressed in the Army memory aid OAKOC (obstacles, avenues of approach, key terrain, observation and fields of fire, and cover and concealment) and the Marine Corps memory aid *KOCOA (key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach).*

3-16. The discussion of terrain in chapter 4 covers the broad aspects of terrain analysis essential to all-source intelligence analysts conducting terrain analysis in support of threat/*adversary* analysis. (See ATP 3-34.80 and JP 2-03 for more information on analyzing the military aspects of terrain.)

3-17. Climate refers to the average weather conditions for a location, area, or region for a specific time of the year as recorded for a period of years. Operational climatology is used to assess effects on weapon systems, collection systems, ground forces, tactics and procedures, enemy TTP, and other capabilities based on specific weather sensitivity thresholds when operational planning occurs more than 10 days prior to the execution. Climatological data is important at both the operational and tactical levels. Actual weather forecasts and/or predictions, using weather models and other tools, are used to assess weather effects on weapon systems, collection systems, ground forces, TTP, and other capabilities when operations occur within 10 days of operational planning.

CIVIL CONSIDERATIONS

3-18. Civil considerations reflect the influence of manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within the operational environment on the conduct of military operations. Commanders and staffs analyze civil considerations in terms of the categories expressed in the memory aid ASCOPE (areas, structures, capabilities, organizations, people, and events).

3-19. Civil considerations help commanders understand the social, political, and cultural variables within the AO and their effect on the mission. Understanding the relationship between military operations and civilians, culture, and society is critical to conducting operations and is essential in developing effective plans. Operations often involve stabilizing the situation securing the peace, building host-nation capacity, and transitioning authority to civilian control. Combat operations/m*ajor operations* directly affect the populace, infrastructure, and the force's ability to transition to host-nation authority. The degree to which the populace is expected to support or resist U.S. and friendly forces also affects offensive and defensive operational design.

3-20. Commanders and staffs use personal knowledge and running estimates to assess social, economic, and political factors. Commanders consider how these factors may relate to potential lawlessness, subversion, or insurgency. Their goal is to develop their understanding to the level of cultural awareness. At this level, they can estimate the effects of friendly actions and direct their subordinates with confidence. Cultural awareness improves how Soldiers/*Marines* interact with the populace and deters their false or unrealistic expectations. They have more knowledge of the society's common practices, perceptions, assumptions, customs, and values, giving better insight into the intent of individuals and groups.

***Note.* FM 4-02 has extensive information on the medical aspects of IPB that relate mainly to civil considerations in the AO.**

3-21. To improve the commander's sociocultural understanding, intelligence staffs can use sociocultural databases and repositories as well as HTTs/*foreign area officers, regional affairs officers, and other cultural enablers,* when available, to aid the intelligence analysis conducted as part of assessing civil considerations. Additionally, commanders and staffs continually seek to improve cultural understanding to improve their roles in IPB.

EVALUATE CURRENT OPERATIONS AND INTELLIGENCE HOLDINGS TO DETERMINE ADDITIONAL INFORMATION NEEDED TO COMPLETE IPB

3-22. Not all the information needed to complete IPB will be in the data files and databases of the commands or their higher headquarters. Information gaps should be identified early and prioritized based on the commander's initial guidance and intent for intelligence and information collection/*intelligence collection*. The staff should ensure the commander is aware of any information gaps that cannot be answered within the time allotted for IPB. The staff develops reasonable assumptions to use in place of these answers and explains to the commander how they arrived at these assumptions.

INITIATE PROCESSES NECESSARY TO ACQUIRE THE INFORMATION NEEDED TO COMPLETE IPB

3-23. After determining that information necessary to complete IPB is not contained within local and searchable external data files and databases, staff elements submit requests for information or requests for collection to obtain the information necessary to complete IPB. As information is received, IPB products are updated and intelligence gaps are eliminated. New intelligence gaps and information requirements may be developed as IPB continues. (See FM 3-55/*MCWP 2-2* for more information on information collection/ *intelligence collection*. See ATP 2-01/*MCWP 2-2* for more information on planning requirements and assessing collection.)

This page intentionally left blank.

Chapter 4

Step 2 of the IPB Process—Describe Environmental Effects on Operations/*Describe the Effects on Operations*

WHAT IS IT?

4-1. Step 2 of the IPB process determines how significant characteristics of the operational environment can affect friendly and threat/*adversary* operations. The following example shows how the significant characteristic of the operational environment (specifically the terrain) impacts friendly operations.

> **Example**
> A brigade/*unit* S-2 tells his commander that the terrain the brigade/*unit* must attack through will canalize friendly forces into platoon-sized mobility corridors that will prevent our forces from supporting each other. The S-2 also tells the commander the terrain favors enemy use of obstacles, small antitank ambushes, and indirect fire throughout its security zone.

DESIRED END STATE

4-2. Identify how the operational environment influences friendly and threat/*adversary* COAs. The primary outputs associated with step 2 of the IPB process may include ensuring—

- **Terrain analysis for the AO and area of interest are completed, in particular:**
  - **Ground and air avenues of approach (AAs).**
  - **Key terrain.**
  - **Potential objectives, decision points, NAIs, and TAIs are identified.**
- **The effects of weather and light data are integrated.**
- **Any request for information on requests for collection are refined and updated.**

SO WHAT?

4-3. The "so what" in this step is identifying how relevant characteristics of the area of interest will affect friendly and threat/*adversary* operations:

- **Success results in allowing the commander to quickly choose and exploit terrain, weather, and civil considerations to best support the mission.**
- **Consequences of failure:**
  - **The commander may not have the information needed to exploit the opportunities the operational environment provides.**
  - **The enemy commander may have the information needed to exploit the opportunities the operational environment provides in a way the friendly commander did not anticipate.**

HOW TO DO IT: (THE PROCESS)

4-4. Describing environmental effects on operations consists of the actions illustrated in figure 4-1.

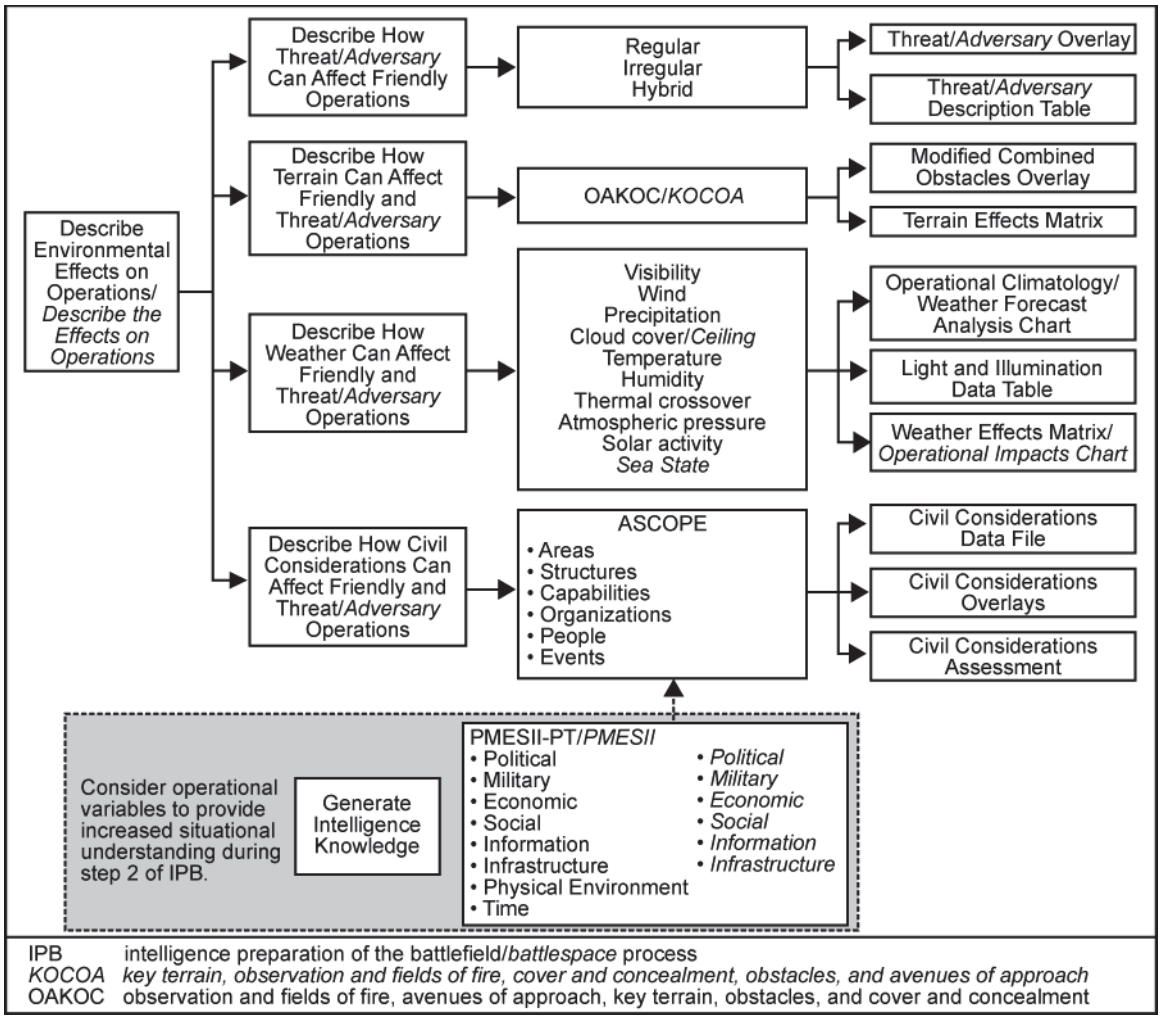


Figure 4-1. Step 2 of the IPB process

DESCRIBE HOW THE THREAT/*ADVERSARY* CAN AFFECT FRIENDLY OPERATIONS

4-5. Threats/*adversaries* are part of the operational environment. Commanders need to understand all the threats/*adversaries* to the operations within the AO and the area of interest. They may face one unified threat/*adversary* force or several disparate threat/*adversary* forces that must be engaged in order to accomplish the mission. Although detailed analysis of enemy forces occurs during steps 3 and 4 of the IPB process, the type of enemy forces and their general capabilities must be defined during step 2. This is done to place the existence of these forces in context with other variables to understand their relative importance as a characteristic of the operational environment. For example:

- **When facing a regular force in major operations regardless of where the engagement occurs, that force is most likely the most important characteristic in that operational environment.**
- **When facing an irregular force conducting operations as part of an insurgency in a failing nation-state, the state of governance and other civil considerations may be more significant than the threat/*adversary* posed by these irregular forces.**

4-6. The threat/*adversary* overlay and threat/*adversary* description table focus the analysis of threat/*adversary* at this point and aid in communicating that analysis to the commander.

THREAT/*ADVERSARY* OVERLAY

4-7. The threat/*adversary* overlay is a depiction of the current physical location of all potential threats/*adversaries* in the AO and the area of interest. This graphic includes the identity, size, location, strength, and AO for each potential threat/*adversary*. Figure 4-2 is an example of a threat/*adversary* overlay for irregular forces.

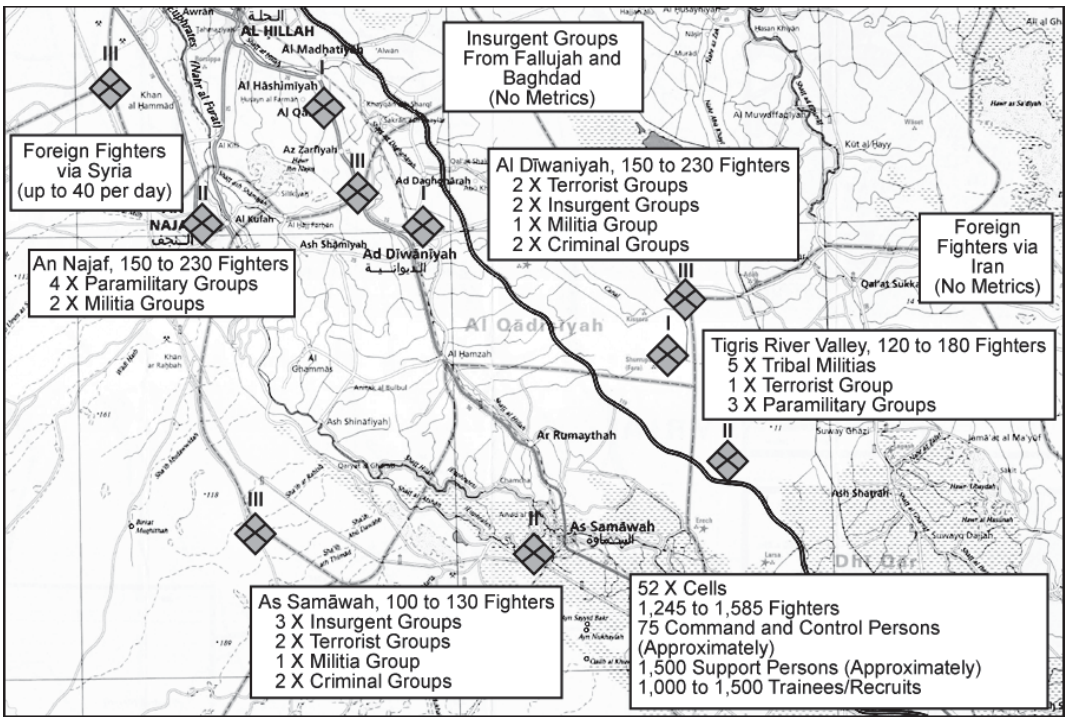


Figure 4-2. Example threat/*adversary* overlay (irregular forces)

THREAT/*ADVERSARY* DESCRIPTION TABLE

4-8. The threat/*adversary* description table supports the threat/*adversary* overlay by classifying the type of threats/*adversaries* identified on the overlay and describing the broad capabilities of each threat/*adversary*. Table 4-1 is an example of a threat/*adversary* description for irregular forces.

Table 4-1. Example threat/*adversary* description table (irregular forces)

Identity	*Location*	*Disposition*	*Description*
26 x separate threat/*adversary* groups	Mosul	Unknown—groups operate from sanctuary locations among the population	Threat/*adversary* groups in Mosul operate independently to disrupt multinational stability tasks
9 x separate threat/*adversary* groups	Tigris River Valley	Unknown—groups operate from sanctuary locations among the population	Facilitate movement of foreign fighters from Syria into Mosul
6 x separate threat/*adversary* groups	Tal Afar	Unknown—groups operate from sanctuary locations among the population	Facilitate movement of foreign fighters from Syria into Mosul
8 x separate threat/*adversary* groups	Sinjar/Biaj	Unknown—groups operate from sanctuary locations among the population	Facilitate movement of foreign fighters from Syria into Mosul

DESCRIBE HOW TERRAIN CAN AFFECT FRIENDLY AND THREAT/*ADVERSARY* OPERATIONS

4-9. Terrain analysis is the evaluation of geographic information on the natural and manmade features of the terrain, combined with other relevant factors, to predict the effect of the terrain on friendly and enemy operations. It involves the study and interpretation of natural and manmade features of an area, their effects on military operations, and the effects of weather and climate on these features. Terrain analysis is a continuous process as changes in the operational environment may alter the analysis of its effect on operations.

4-10. There are two types of terrain in which a command may operate—natural and urban. Both of these terrain types are analyzed based on military aspects using the OAKOC/*KOCOA* considerations. Analysis of natural terrain focuses on surface area, airspace, and subsurface areas. Analysis of urban terrain also focuses on surface area and airspace, but must also consider subsurface as well as internal and external supersurface areas.

ANALYZE THE MILITARY ASPECTS OF TERRAIN

4-11. Generally in the Army, detailed terrain analysis is conducted by geospatial intelligence cells assigned to brigade combat teams, division headquarters, corps headquarters, and theater headquarters based on priorities established by the intelligence officer. These cells have state-of-the-art digital mapping tools and access to national-level support from agencies like the National Geospatial Intelligence Agency. *Generally in the Marine Corps, geospatial intelligence capability resides within the intelligence battalion and the Marine aircraft wing (MAW). During the conduct of operations, this capability can be deployed down to the regimental combat team or Marine aircraft group level.* The result of terrain analysis is the evaluation of the military aspects of terrain on operations.

4-12. Analyzing the military aspects of terrain involves the collection, processing, evaluation, and interpretation of geographic information on natural and manmade features of the terrain, combined with other relevant factors, to determine potential effects of the terrain on military operations. It involves the study and interpretation of natural and manmade features of an area, effects on military operations, and the effects of weather and climate on these features. Terrain analysis is a continuous process as changes in the operational environment may change the analysis of its effect on the operation or threat/*adversary* COAs.

Obstacles

4-13. An obstacle is any natural or man-made obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in personnel, time, and equipment on the opposing force (JP 3-15). Some examples of obstacles to ground mobility are—

- **Buildings.**
- **Mountains.**
- **Steep slopes.**
- **Dense forests.**
- **Rivers.**
- **Lakes.**
- **Urban areas.**
- **Minefields.**
- **Trenches.**
- **Certain religious and cultural sites.**
- **Wire obstacles (concertina wire. barbed wire, and overhead wire).**

4-14. Obstacles affect certain types of movement differently. Obstacles such as rivers, lakes, swamps, dense forested areas, road craters, rubble in the street, or densely populated urban areas may have a greater effect on mounted movement than on dismounted movement. Minefields, concertina wire, or steep slopes may be more effective against dismounted movement.

4-15. Obstacles to air mobility include terrain features that exceed the aircraft's service ceiling; affect nap-of-the-earth flight; impact aircraft lift capabilities; or that force the aircraft to employ a particular flight profile. Examples are tall buildings, cellular telephone towers, power lines, rapidly rising terrain features, mountains, smoke, geologic features, high mountains, and other obscurants. High mountainous regions can impact rotary- and fixed-wing aircraft lift capabilities.

4-16. Obstacles may also decrease the effectiveness of information-related capabilities to influence adversary or enemy operations and activities, friendly populations, and neutral populations. For example, mountains may block terrestrial-based signals used to broadcast surrender appeals and morale-lowering messages to enemy-held territory or messages to populations explaining the intent of U.S. operations. Use of other message delivery platforms may be necessary to compensate for the effects of local terrain.

4-17. Figure 4-3 illustrates examples of obstacles in natural terrain.

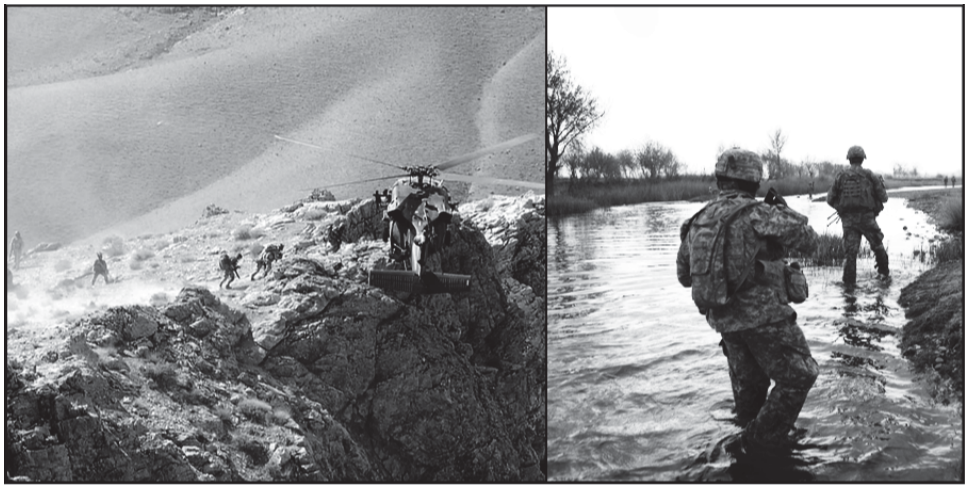


Figure 4-3. Example of obstacles in natural terrain

4-18. Figure 4-4 illustrates examples of obstacles in urban terrain.

Figure 4-4. Example of obstacles in urban terrain

Avenues of Approach

4-19. AAs are air or ground routes used by an attacking force leading to its objective or to key terrain in its path. The identification of AAs is important because all COAs that involve maneuver depend on available AAs. During offensive tasks, the evaluation of AAs leads to a recommendation on the best AAs to a command's objective and identification of avenues available to the enemy for counterattack, withdrawal, or the movement of reinforcements or reserves. In a defense operation, it is important to identify AAs that support enemy offensive capabilities and avenues that support the movement and commitment of friendly reserves. AAs are developed by identifying, categorizing, and grouping mobility corridors and evaluating AAs.

4-20. Mobility corridors are that are relatively free of obstacles where a force will be canalized due to terrain restrictions allowing military forces to capitalize on the principles of mass and speed (JP 2-01.3).

4-21. Identifying mobility corridors requires some knowledge of friendly and enemy forces and their preferred tactics. The best mobility corridors use unrestricted terrain that provided enough space for a force to move in its preferred doctrinal formations while avoiding major obstacles. Mobility corridors can follow, for example, the direction of roads, trails, rivers, streams, ridgelines, subway lines, foot paths, tunnels, and human-sized drainage ditches. Factors other than obstacles and mobility may have to be evaluated when identifying mobility corridors.

4-22. Mobility corridors, like obstacles, are a function of the type and mobility of the force being evaluated. Military forces, such as mechanized infantry or armored units, require large open areas in which to move and maneuver. Irregular forces are less impacted by the presence of obstacles and terrain that would hinder movement of a large formation. The size of a mobility corridor can be determined based on terrain constrictions.

4-23. Mobility corridors are categorized by the size or type of force they can accommodate. Mobility corridors can also be categorized by likely use. For example, a mechanized force requires logistical sustainment; a mobility corridor through unrestricted terrain supported by a road network is generally more desirable. A dismounted force might be able to use more restrictive corridors associated with the arctic tundra, swamps or marshes, jungles, or mountains that may or may not have a road network. Due to their rate of march and lack of fire power, dismounted forces require a more covered and concealed route for survivability to reach their objective.

4-24. AAs consist of a series of mobility corridors through which a maneuvering force must pass to reach its objective. An AA must provide ease of movement and enough width for dispersion of a force large enough to significantly affect the outcome of the operation. Mobility corridors are classed based on the distance between the terrain features that form the corridor. Mobility corridor ranges are not absolute but reflect the relative and approximate distance between terrain features. Table 4-2 identifies these classifications.

Table 4-2. Mobility corridor ranges

Avenue of approach	*Cross-country mobility corridor classification*	*Approximate distance between terrain features (in kilometers)*
Division	Brigade/Regiment	10
Brigade/Regiment	Brigade/Regiment	6
Battalion	Company	2

4-25. Evaluating AAs is a combined effort of the entire staff. Evaluating AAs identifies those that best support threat/*adversary* or friendly capabilities. The AAs should be prioritized based on how well each supports the ability to meet the desired result in a timely and efficient manner. AAs are evaluated for suitability in terms of—

- **Access to key terrain and adjacent avenues.**
- **Degree of canalization and ease of movement.**
- **Sustainability (line of communications [LOC] support).**
- **Access to the objective.**

4-26. Once evaluated, AAs are prioritized on how well each supports maneuver. Figure 4-5 is an example of the identification of AAs with mobility corridors.

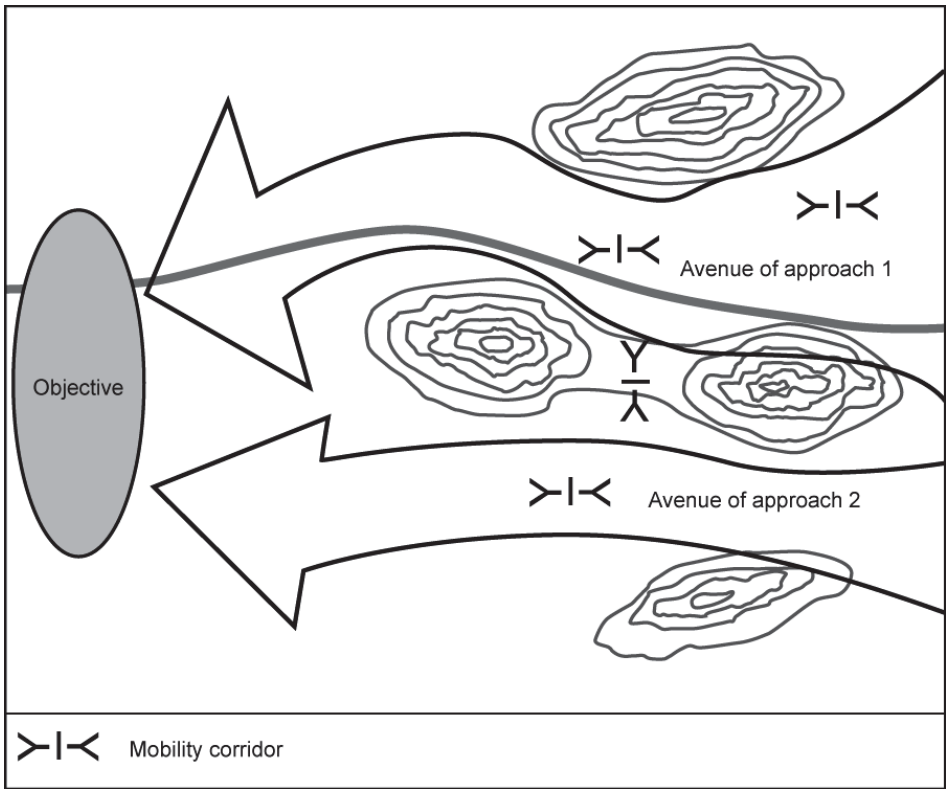


Figure 4-5. Avenues of approach with mobility corridors

4-27. Figure 4-6 is an example of the identification mobility corridors in urban terrain.

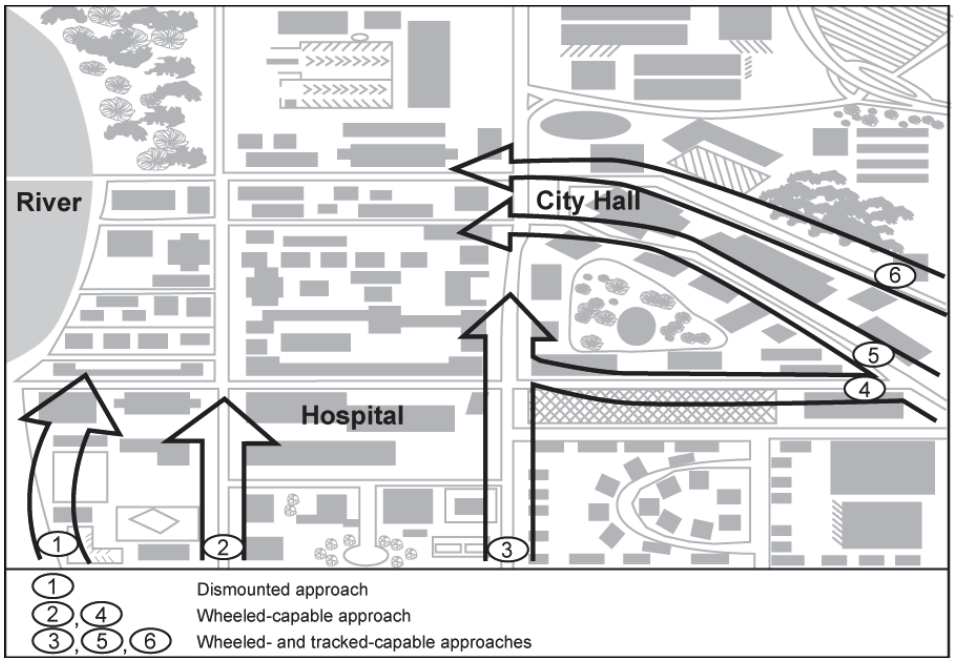


Figure 4-6. Mobility corridors (urban terrain)

Key Terrain

4-28. Key terrain is any locality, or area, the seizure or retention of which affords a marked advantage to either combatant (JP 2-01.3). In natural terrain dominated by restrictive terrain features, high ground can be key terrain because it dominates an area with good observation and fields of fire. In an open or arid environment, a draw or wadi can be key terrain because it offers good cover and concealment.

4-29. In urban environments, infrastructure (such as bridges, medical facilities, choke points, intersections, industrial complexes, and economic, social, and government institutions) can be considered key terrain. *For the Marine Corps, this includes the local population and certain local groups or individuals.* For example, control of a bridge may equate to control over an AA. However, the command needs to consider the operational and strategic impact on the civil dimension when deciding to control a bridge.

Key Terrain Considerations

Control of a bridge may negatively impact commerce, LOC support, military load class of supporting LOCs, and access to the objective. An example of economic or social institution as key terrain is the main bazaar in a town because whoever controls the bazaar or market controls the town. Economic health of the market will be key to the economic health of the area. If the enemy can maneuver through and control the key terrain of the market, the enemy can shut down the town and the economy.

An example for a government institution being key terrain is the local police, who may exert a great deal of influence on the local population (elections, law enforcement, tribal politics, other). Tactical use of terrain is often directed at increasing the capability for applying combat power and at the same time forcing the threat/*adversary* into areas to reduce their ability to apply combat power.

4-30. Key terrain is evaluated by assessing the impact of its control by either force. A technique that aids this assessment is to use the evaluation of the other four aspects of military terrain to assist in determining key terrain.

4-31. In the offense, key terrain features are usually forward of friendly dispositions and are often assigned as objectives. Adjacent terrain features may be key terrain if their control is necessary for the continuation of the attack or the accomplishment of the mission.

4-32. In the defense, key terrain is usually within and/or behind the defensive area, such as terrain that gives good observation over AAs to and through the defensive position; terrain that permits the defender to cover an obstacle by fire; or areas along an LOC that affect the use of reserves or sustainment operations. In counterinsurgency operations, key terrain may include portions of the population, such as political, tribal, and religious groups or leaders; a localized population; infrastructure; or governmental organizations.

4-33. Decisive terrain is key terrain whose seizure and retention is mandatory for successful mission accomplishment. Key terrain is not necessarily decisive terrain. Decisive terrain has an extraordinary impact on the mission. The successful accomplishment of the mission depends on seizing, retaining, or denying the use of the terrain to an enemy force.

4-34. Commanders designate decisive terrain to communicate to the staff and subordinate commanders how important the terrain is to the concept of operations.

4-35. Figure 4-7 illustrates the concept of key terrain in a natural environment.

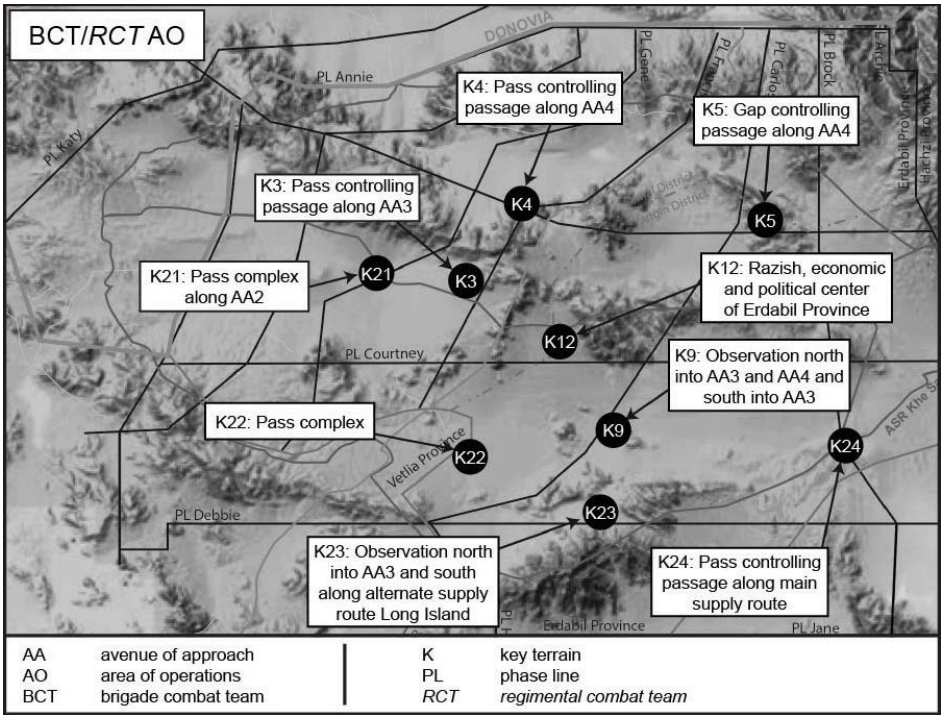


Figure 4-7. Key terrain (natural terrain)

4-36. Figure 4-8 illustrates the concept of key terrain in an urban environment.

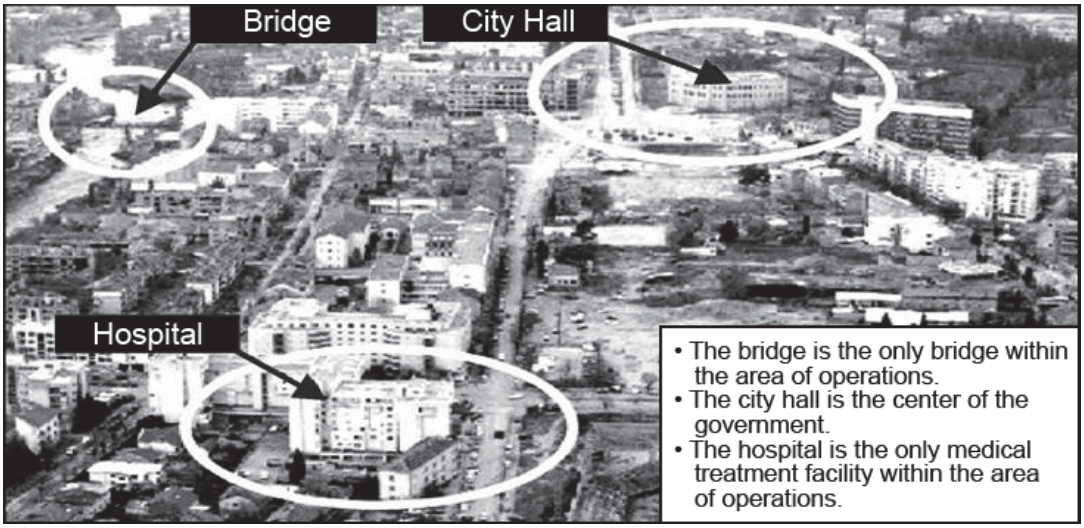


Figure 4-8. Key terrain (urban terrain)

Observation and Fields of Fire

4-37. Observation is the condition of weather and terrain that permits a force to see friendly, enemy, and neutral personnel, systems, and key aspects of the operational environment. Commanders evaluate their observation capabilities for electronic and optical line-of-sight surveillance systems, as well as for unaided visual observation. The highest terrain normally provides the best observation.

4-38. In natural terrain, there are limitations on observation caused by relative, localized, and often subtle variations in terrain elevations. These limitations are known as intervisibility lines (IVLs). Intervisibility is the condition of being able to see one point from the other. Figure 4-9 illustrates IVLs.

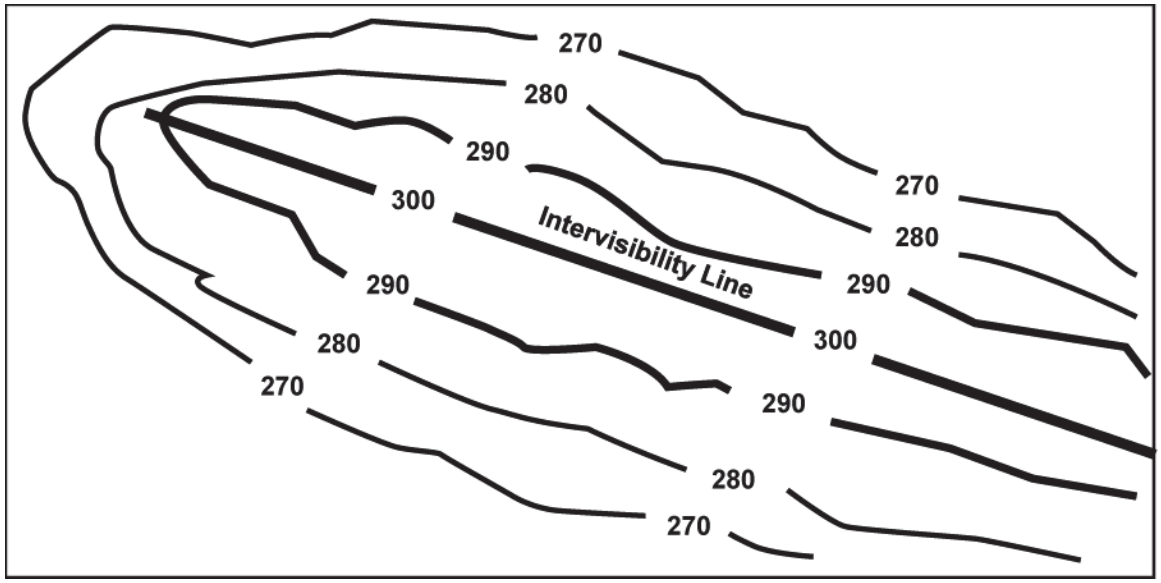


Figure 4-9. Example of intervisibility lines

4-39. Observation can also be limited by adverse weather, dusk, and smoke. In urban terrain, observation is primarily limited by manmade structures, as well as the activity and debris associated with human activity. Analyzing observation and fields of fire in urban terrain is more complicated than it is for natural terrain.

4-40. When evaluating observation and fields of fire for urban terrain, analysts must consider surface, supersurface, subsurface, external, and internal surface areas.

4-41. Fields of fire is observation limited to a specific linear distance based on weapons systems capabilities. A unit's field of fire is directly related to its ability to observe. Evaluation of observation and fields of fire identifies—

- **Potential engagement areas.**
- **Defensible terrain.**
- **Specific equipment or equipment positions.**
- **Areas where forces are most vulnerable to observation and fires.**
- **Identification of visual dead space.**

4-42. Analysis of fields of fire includes an evaluation of all direct and indirect fire weapons systems in a command's inventory. An ideal field of fire for a direct fire weapon is an open area in which the threat/*adversary* can be seen and on which the threat/*adversary* has no protection out to the maximum effective range of that weapon. An ideal field of fire for an indirect fire weapons system is a target area that has no protection from the system's munitions. Terrain that offers good observation and fields of fire generally favors defensive COAs.

4-43. Both observation and fields of fire are based on lines of sight. Line of sight is the unobstructed path from a Soldier's/*Marine's* weapon, weapon site, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another. In other words, a line of sight is a straight line from one point to another. There are two types of lines of sight normally evaluated during terrain analysis—horizontal and oblique.

- **Horizontal line of sight is an unobstructed path from a Soldier's/*Marine's* weapon, weapon sight, laser designator, and electronic sending and receiving antennas.**
- **Oblique or vertical lines of sight aid in planning air defense artillery systems locations, selecting landing zones and drop zones, and selecting forward arming and refueling points.**

4-44. Identifying areas vulnerable to threat/*adversary* aerial intelligence collection systems aids in selecting friendly battle positions. Establishing lines of sight and identifying IVLs are critical parts of analyzing observation and fields of fires because they have a bearing on line-of-sight direct fire weapons, antennas, reconnaissance, and some electro-optical systems.

4-45. An effective technique for analyzing observation and fields of fire is to produce a graphic that displays observation and fields of fire. The use of computer-generated terrain applications can assist in producing observation and fields of fire graphics. An ideal field of fire for direct fire weapons is an open field in which the threat/*adversary* can be seen and has no protection from fires. Analysts identify features of terrain that allow good observation for indirect fire weapons and determine if the terrain has any effect on fire support missions.

4-46. Figure 4-10 shows line-of-sight analysis used to determine observation and fields of fire in natural terrain.

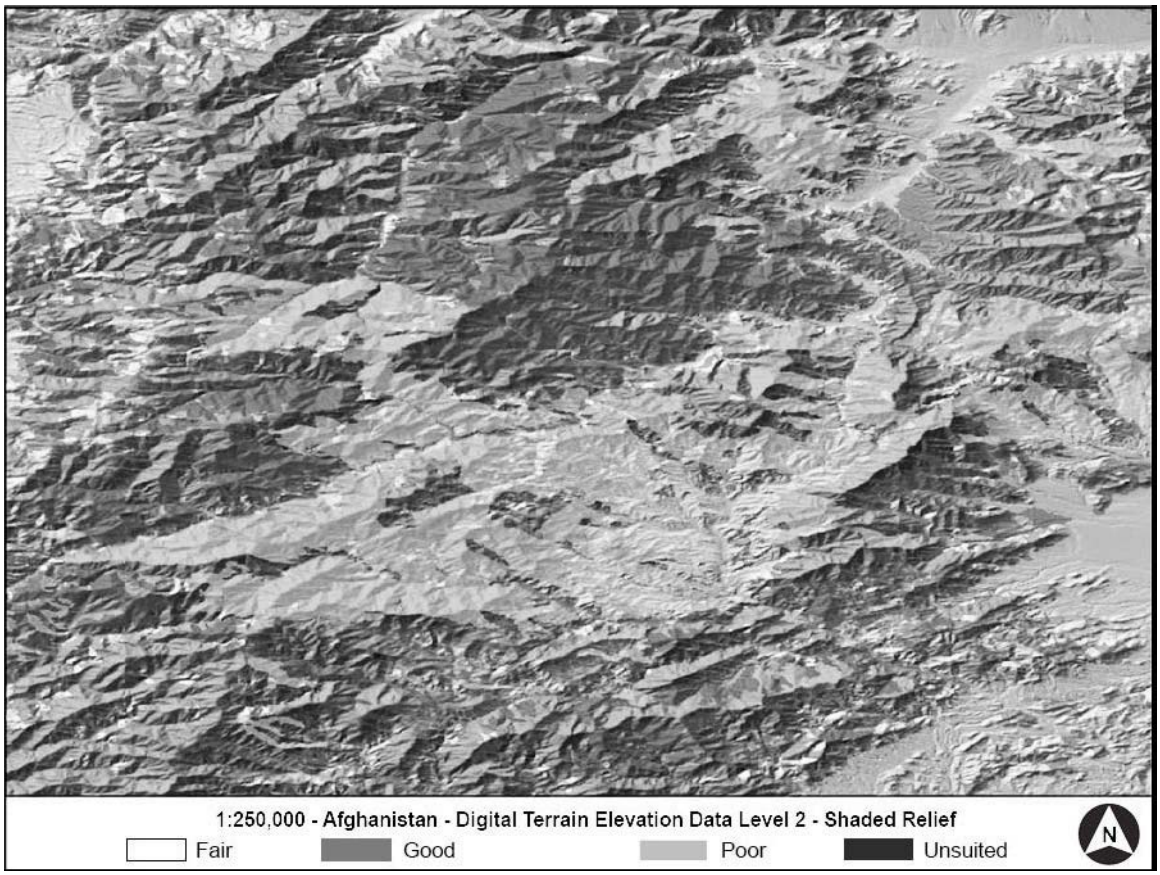


Figure 4-10. Observation and fields of fire (natural terrain)

4-47. Figure 4-11 shows line-of-sight analysis used to determine observation and fields of fire in urban terrain.

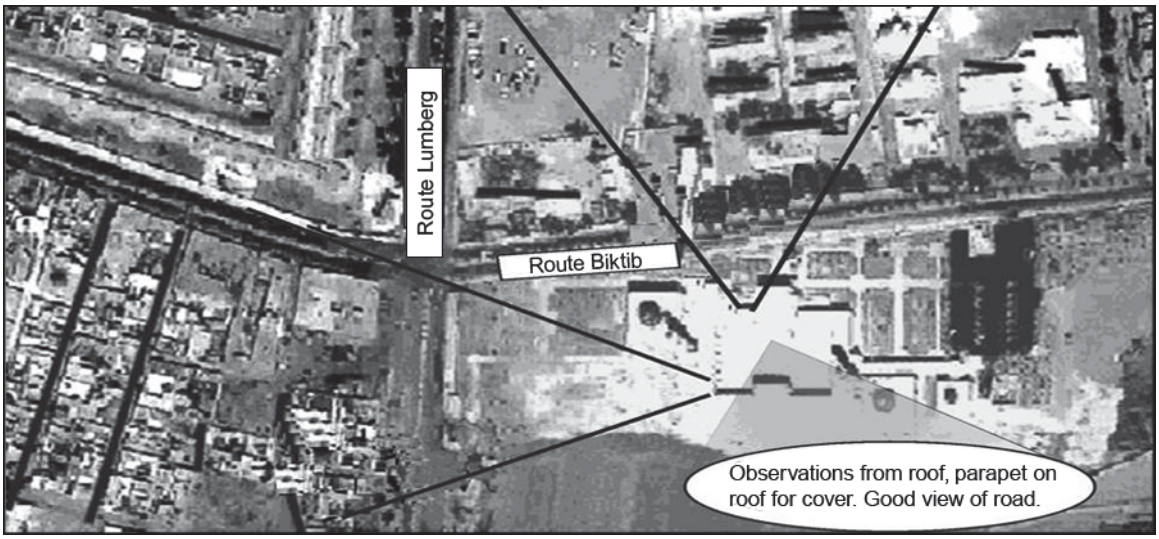


Figure 4-11. Observation and fields of fire (urban terrain)

Cover and Concealment

4-48. In intelligence usage, cover pertains to those measures necessary to give protection to a person, plan, operation, formation, or installation from the enemy intelligence effort and leakage of information (JP 2-01.2). Cover is the physical protection from bullets, fragments of exploding rounds, flame, nuclear effects, and biological and chemical agents. Cover and concealment can be provided by but are not limited to ditches, caves, riverbanks, folds in the ground, shell craters, buildings, walls, and embankments. Cover does not necessarily provide concealment. An example of cover without concealment is a bunker in plain sight that is intended for the protection of personnel.

4-49. Concealment is protection from observation or surveillance (ADRP 1-02). It degrades the threat's/*adversary's* ability to observe forces, equipment, or position. Concealment can be provided by trees, underbrush, tall grass, cultivated vegetation, weather conditions (such as snow, fog, or rain), as well as manmade camouflage. Concealment does not necessarily provide cover.

4-50. Line-of-sight analysis determines the observation, fields of fire, and cover and concealment that the terrain provides to both the friendly and enemy/*adversary* forces. The following example and figure 4-12 illustrate the concept of cover and concealment in natural terrain and line-of-sight analysis.

Line-of-Sight Example

The masked area all lies behind terrain that is level with or higher than the defensive position. One cannot see into the masked area or fire direct weapons into it. One does not have observation or fields of fire behind the masking terrain. The masked area provides the attacker cover from the defender's direct fire and concealment from the defender's observations. If the enemy/*adversary* has done proper analysis, then they would select one or more of the approach routes.

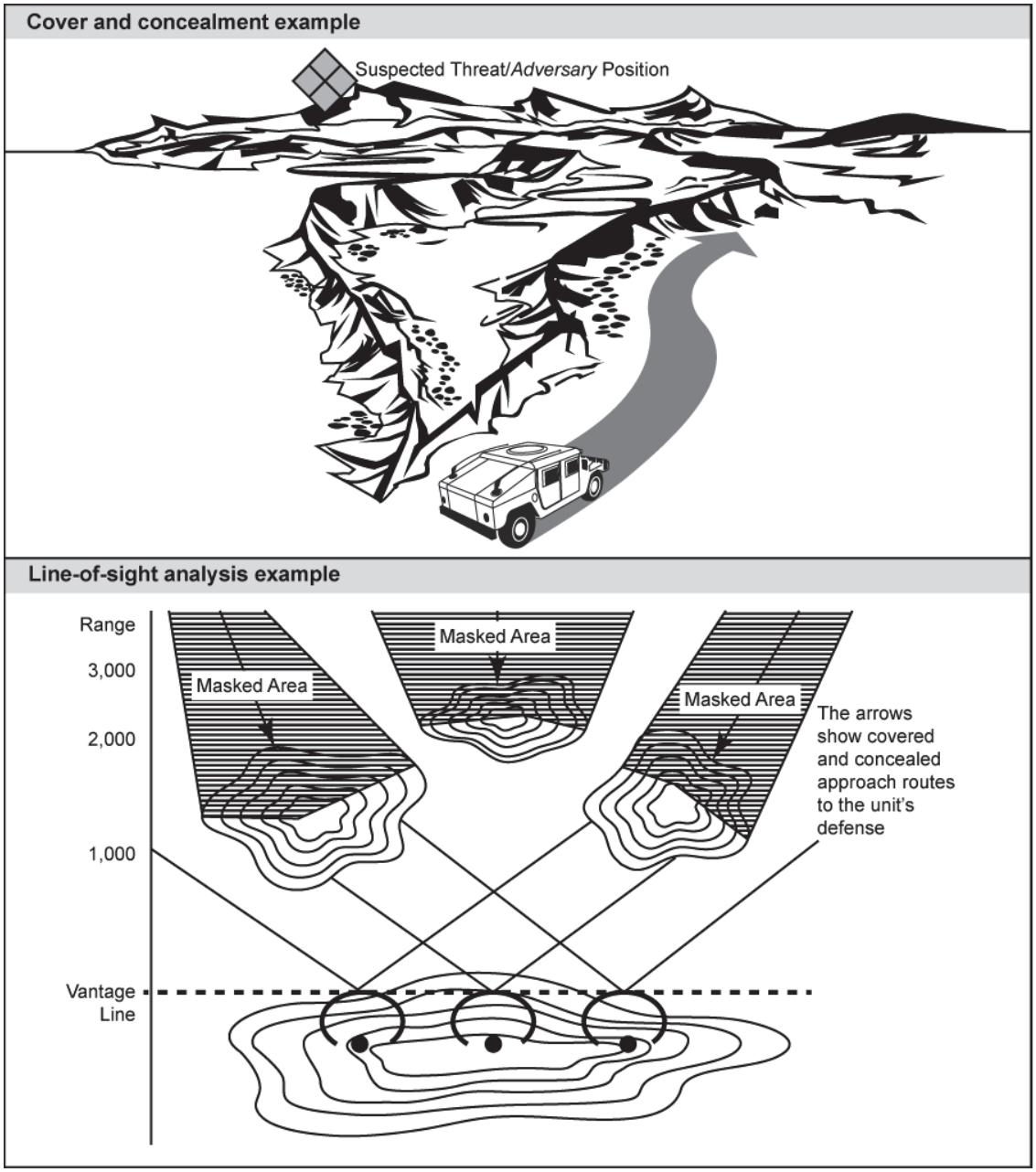


Figure 4-12. Cover and concealment (natural terrain) and line-of-sight analysis

4-51. Figure 4-13 illustrates the concept of cover and concealment in urban terrain.

Figure 4-13. Example of cover and concealment in urban terrain

TERRAIN EFFECTS

4-52. After determining terrain characteristics, the staff must determine the effect that the terrain will have on friendly and threat/*adversary* operations. The primary analytic tools used to aid in determining this effect are the MCOO and the terrain effects matrix.

Modified Combined Obstacle Overlay

4-53. The MCOO is a graphic product that portrays the effects of natural and urban terrain on military operations. The MCOO normally depicts military significant aspects of the terrain and other aspects of the terrain that can affect mobility. Though not all inclusive, some of these aspects are—

- **AAs.**
- **Mobility corridors.**
- **Natural and manmade obstacles.**
- **Terrain mobility classifications.**
- **Key terrain.**

4-54. The combined obstacle overlay provides a basis for identifying ground AAs and mobility corridors. Unlike the cross-country mobility, the combined obstacle overlay integrates all obstacles to vehicular movement, such as built-up areas, slope, soils, vegetation, and hydrology into one overlay. The overlay depicts areas that impede movement (severely restricted and restricted areas) and areas where friendly and enemy forces can move unimpeded (unrestricted areas).

4-55. The MCOO is tailored to the mission and is a collaborative effort involving input from the entire staff. The MCOO depicts the terrain according to mobility classification. These classifications are severely restricted, restricted, and unrestricted:

- **Severely restricted terrain severely hinders or slows movement in combat formations unless some effort is made to enhance mobility. This could take the form of committing engineer assets to improving mobility or deviating from doctrinal tactics, such as moving in columns instead of line formations, or at speeds much lower than those preferred. For example, severely restricted terrain for armored and mechanized forces is typically characterized by steep slopes and large or densely spaced obstacles with little or no supporting roads. A common technique is to depict this type of severely restricted terrain on overlays and sketches by marking the areas with cross-hatched diagonal lines. Another technique is to color code the areas in red.**

- **Restricted terrain hinders movement to some degree. Little effort is needed to enhance mobility, but units may have difficulty maintaining preferred speeds, moving in combat formations, or transitioning from one formation to another. Restricted terrain slows movement by requiring zigzagging or frequent detours. Restricted terrain for armored or mechanized forces typically consists of moderate-to-steep slopes or moderate-to-densely spaced obstacles, such as trees, rocks, or buildings. Swamps or rugged terrain are examples of restricted terrain for dismounted infantry forces. Logistical or sustainment area movement may be supported by poorly developed road systems. A common and useful technique is to depict restricted terrain on overlays and sketches by marking the areas with diagonal lines. Another technique is to color code the areas in yellow.**
- **Unrestricted terrain is free of any restriction to movement. Nothing needs to be done to enhance mobility. Unrestricted terrain for armored or mechanized forces is typically flat to moderately sloping terrain with scattered or widely spaced obstacles such as trees or rocks. Unrestricted terrain allows wide maneuver by the forces under consideration and unlimited travel supported by well-developed road networks. No symbology is needed to show unrestricted terrain on overlays and sketches.**

4-56. Terrain mobility classifications are not absolute but reflect the relative effect of terrain on the different types and sizes of movement formations. They are based on the ability of a force to maneuver in combat formations or to transition from one type of formation to another. The staff should consider the following:

- **Obstacles are only effective if they are covered by observation and fire. However, even undefended obstacles may canalize an attacker into concentrations, which are easier to detect and target or defend against.**
- **When evaluating the terrain's effect on more than one type of organization (for example, mounted or dismounted), the obstacle overlays reflect the mobility of the particular force.**
- **The cumulative effects of individual obstacles in the final evaluation. For example, individually a gentle slope or a moderately dense forest may prove to be an unrestrictive obstacle to vehicular traffic. Taken together, the combination may prove to be restrictive.**
- **Account for the weather's effects on factors that affect mobility.**
- **The classification of terrain into various obstacle types reflects only its relative impact on force mobility. There are many examples of a force achieving surprise by negotiating supposedly "impassable" terrain.**

4-57. Figure 4-14 is an example of a MCOO developed for natural terrain.

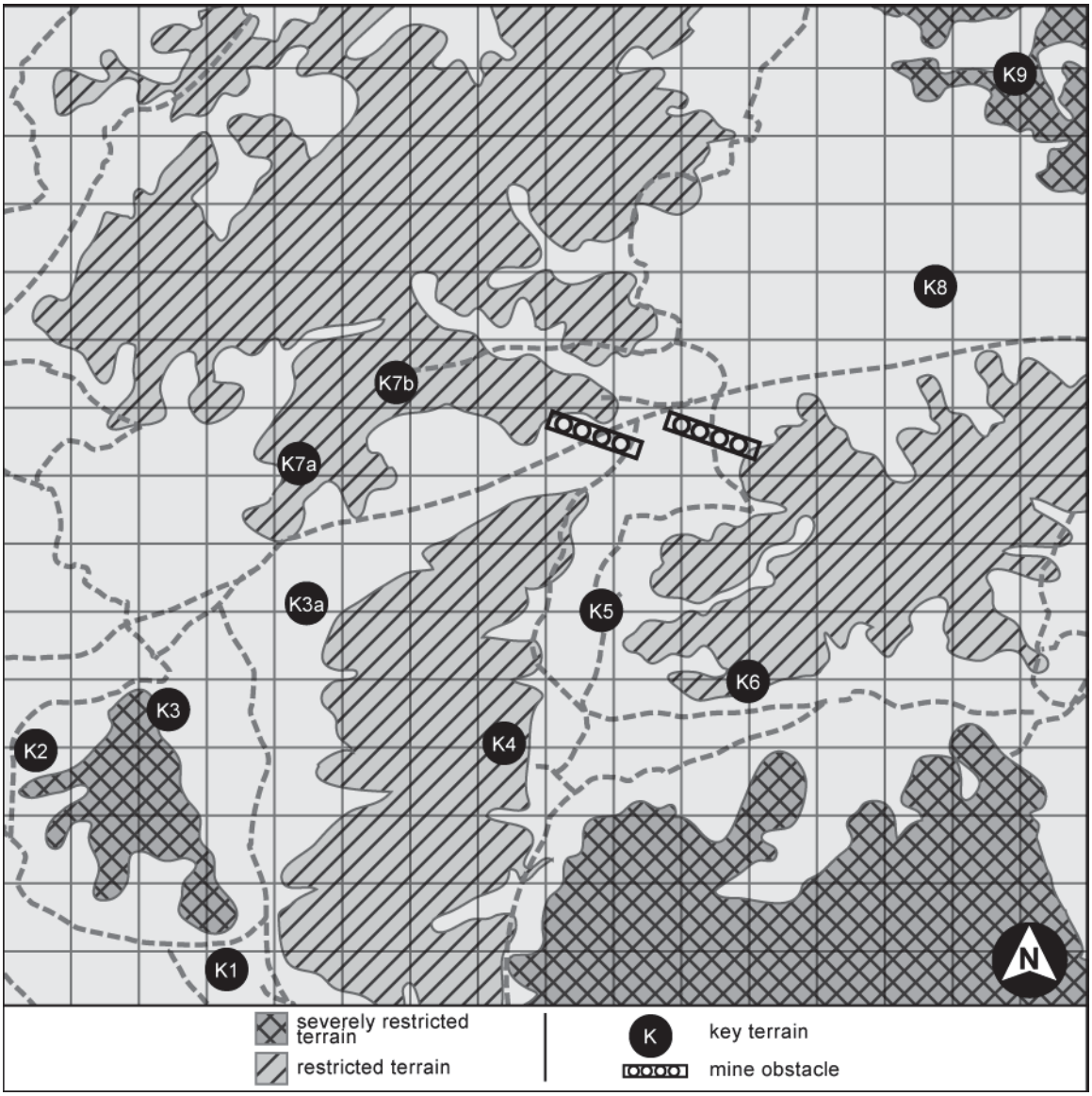


Figure 4-14. Example modified combined obstacle overlay (natural terrain)

4-58. For urban terrain, graphics typically depict population status overlays (population centers, urban areas, political boundaries); logistics sustainability overlays; LOCs; route overlays (street names, patterns, and widths); bridges, underpass and overpass information; potential sniper and ambush locations (likely this data will be a separate overlay); and key navigational landmarks. In developing urban terrain overlays, the following should be depicted:

- **Natural terrain—the underlying natural terrain on which manmade terrain is superimposed, such as rivers, streams, hills, valleys, forests, desert, bogs, swamps.**
- **Manmade terrain—streets, bridges, buildings, railways, canals, traffic control points; building density, construct, dimensions; functional zone disposition; and street construct, materials, disposition, dimensions.**
- **Key facilities, targets and/or terrain—banks, bridges, airports, electric power grids, oil facilities, military facilities, key residences and places of employment, waterways; tall structures (skyscrapers); choke points; intersections; bridges; industrial complexes; other facilities; density of construction or population; street patterns.**

- **Obstacles—rubble and vehicles in the road; fixed barriers; masking of fires; burning of buildings and other fire hazards; rivers and lakes; power lines; cell phone towers; population; trenches; minefields; certain religious or cultural sites; wire obstacles (concertina wire, barb wire).**

Note. **In urban terrain, depict storm and drainage systems as well as public transportation routes, which may present themselves as obstacles to future friendly operations.**

- **In addition to the above factors, also consider—**
  - **The street level necessary to support the smallest enemy or friendly unit size, and the local street names whenever possible (official and unofficial).**
  - **Surface structure composition (cobblestone, concrete, dirt), along with elevation and slope.**
  - **Construction status (building or destroying) if development is underway.**
  - **Time pattern plots as necessary to show local population use in terms of movement.**
  - **Parking areas with weight restrictions, electrification of public transport, local airports, heliports and runways, inland-ports, and any known pipelines (along with their status: active, inactive, dimensions).**

Evaluate Terrain Effects on Operations

4-59. Using the MCOO as a guide, the terrain effects matrix describes the effect each aspect of OAKOC/*KOCOA* has on friendly and threat/*adversary* operations. Table 4-3 is an example of a terrain effects matrix using a table format.

Table 4-3. Example terrain effects matrix

OAKOC aspects	*Terrain effects*
Obstacles	Wadis throughout the area of operations with an average depth of 5 to 10 feet and an average width of 20 feet that runs 6 to 10 kilometers long. Above-ground oil and transport pipeline that runs through the central width of the area of operations.
Avenues of approach	Primary and secondary road systems for high avenues of approach. Generally flat terrain with brigade-sized mobility corridors between small villages. Railroad in the north running east to west.
Key terrain	Airfield used as resupply and troop movements. Dam control waterflow on the river and is the primary objective of the threat/*adversary*.
Observation and fields of fire	Sparse vegetation on generally flat desert terrain with observation of 3 to 5 kilometers. There are 10 kilometers between intervisibility lines. Air support observation is unlimited due to sparse terrain and curve of the earth. Fields of fire for direct fire is 300 to 500 meters for small arms.
Cover and concealment	Cover is provided by intervisibility lines. Concealment is limited by the open terrain and sparse vegetation.

Note. For table 4-3, the Marine Corps* uses *KOCOA (key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach) aspects.

DESCRIBE HOW WEATHER CAN AFFECT FRIENDLY AND THREAT/*ADVERSARY* OPERATIONS

4-60. Weather analysis is the collection, processing, evaluation, and interpretation of relevant military aspects of weather. There are two sub-steps in weather analysis: analyze the military aspects (characteristics) of weather; and evaluate the weather's effects on military operations.

ANALYZE THE MILITARY ASPECTS OF WEATHER

4-61. The following are military aspects of weather:

- **Visibility.**
- **Wind.**
- **Precipitation.**
- **Cloud cover/*ceiling*.**
- **Temperature.**
- **Humidity.**
- **Atmospheric pressure (as required).**
- ***Sea state*.**

Visibility

4-62. Visibility is defined as the greatest distance that prominent objects can be seen and identified by the unaided, normal eye. A major factor in evaluating visibility is the amount of available light based on weather conditions and illumination as determined by the factors discussed below:

- **Begin morning nautical twilight (also called BMNT) is start of that period where, in good conditions and in the absence of other illumination, the sun is 12 degrees below the eastern horizon and enough light is available to identify the general outlines of ground objects and conduct limited military operations (JP 2-01.3). Light intensification devices are still effective and may have enhanced capabilities.**
- **Begin morning civil twilight (also called BMCT) is the period of time at which the sun is halfway between beginning morning and nautical twilight and sunrise, when there is enough light to see objects clearly with the unaided eye (JP 2-01.3). At this time, light intensification devices are no longer effective, and the sun is six degrees below the eastern horizon.**
- **Sunrise is the apparent rising of the sun above the horizon. The rising times are dependent on latitude.**
- **Sunset is the apparent descent of the sun below the horizon. The setting times are dependent on latitude.**
- **End evening civil twilight (also called EECT) is the point in time when the sun has dropped 6 degrees beneath the western horizon, and is the instant at which there is no longer sufficient light to see objects with the unaided eye (JP 2-01.3). Light intensification devices are recommended from this time until begin morning civil twilight.**
- **End of evening nautical twilight (also called EENT) is the point in time when the sun has dropped 12 degrees below the western horizon, and is the instant of last available daylight for the visual control of limited military operations (JP 2-01.3). At end of evening nautical twilight there is no further sunlight available.**
- **Moonrise is the time at which the moon first rises above the horizon. The rising times are dependent on latitude.**
- **Moonset is the time at which the moon sets below the horizon. The setting times are dependent on latitude.**

4-63. Other weather conditions can affect visibility as well. Temperature can affect the use of thermal sights. Cloud cover can negate illumination provided by the moon. Additionally, precipitation and other obscurants can have varying effects as well. Low visibility is beneficial to offensive and retrograde operations because it conceals concentration of maneuver forces, thus enhancing the possibility of surprise.

Low visibility hinders the defense because cohesion and control become difficult to maintain, reconnaissance operations are impeded, and target acquisition is degraded.

Wind

4-64. Wind of sufficient speed from any direction can reduce the combat effectiveness of a force as a result of blowing dust, smoke, sand, or precipitation. Strong winds and wind turbulence limit airborne, air assault, and aviation operations. High winds near the ground can lower visibility due to blowing dust; they also can affect movement or stability of some vehicles. Blowing sand, dust, rain, or snow can reduce the effectiveness or stability of radars, antennas, communications, and other electronic devices. High winds can also affect persistent threat/*adversary* detection systems like an aerostat. Evaluation of weather in support of operations requires information on the wind at the surface as well as at varying altitudes and elevations.

Precipitation

4-65. Precipitation is any moisture falling from a cloud in frozen or liquid form. Rain, snow, hail, drizzle, sleet, and freezing rain are common types. Precipitation affects soil trafficability, visibility, and the functioning of many electro-optical systems. Heavy precipitation can have an effect on sustainment, communications, personnel, military operations, and many civilian activities.

Cloud Cover/*Ceiling*

4-66. Cloud cover affects ground operations by limiting illumination and could affect the thermal signature of targets. Heavy cloud cover can degrade many intelligence sensors and target acquisition systems and general aviation operations. Conversely, low cloud cover may increase the available level of light when there is ground-based light, such as what is available in urban areas. Excessive low cloud cover may restrict visibility and limit safe aviation operations.

4-67. A *ceiling* means the height above the Earth's surface of the lowest layer of clouds or obscuring phenomena that is reported as broken, overcast, or obscuration, and not classified as thin or partial. A ceiling listed as "unlimited" means that the sky is clear or is free of any substantial cloud cover. Cloud cover affects ground operations by limiting illumination and could affect the thermal signature of targets. Heavy cloud cover can degrade many intelligence sensors and target acquisition systems and general aviation operations. Conversely, low cloud cover may increase the available level of light when there is ground-based light, such as what is available in urban areas. Excessive low cloud cover may restrict visibility and limit safe aviation operations.

Temperature

4-68. Temperature extremes can reduce effectiveness of troops and equipment capabilities. They may affect the timing of combat operations/*major operations*. For example, extremely high temperatures in a desert environment may require dismounted troops to operate at night. High temperatures can also affect the lift capability of medium-rotary-lift assets in high altitudes and elevations. For example, during Operation Enduring Freedom, during the summer months in Afghanistan, the UH 60 could not carry its full complement of passengers.

4-69. Thermal crossover is the condition in which the temperature of a ground-based vehicle is close to, if not the same as, the surrounding land. As a result of this condition, thermal optics are unable to detect enemy vehicles until a temperature disparity exists between the land and the vehicles. *Using Target Acquisition Weapons Software, meteorological and oceanographic (METOC) personnel can forecast for thermal crossover and determine specific times that the phenomenon will occur.*

4-70. High temperatures also can increase fuel consumption in vehicles, cause overheating, and affect the muzzle velocity of both direct and indirect fire weapons (155 millimeter howitzers, sniper rifles, tanks, other).

Humidity

4-71. Humidity is the state of the atmosphere with respect to water vapor content. High humidity affects the human body's ability to cool off. Hence, troops in tropical areas may become less effective because of higher humidity levels. Humidity is usually expressed as either relative humidity or absolute humidity.

Atmospheric Pressure (As Required)

4-72. Atmospheric pressure has a significant impact on aviation operations. Based on the elevation of the operational area, atmospheric pressure affects the lift capacity of aircraft, especially rotary-wing and tiltrotor aircraft in mountainous terrain. When combined with extreme temperatures, atmospheric pressure increases the amount of runway an aircraft requires for takeoff. (See JP 3-04 for more information on tiltrotor aircraft operations.)

Sea State

4-73. A *sea state* is the general condition of the surface on a large body of water—with respect to wind waves and swell—at a certain location and moment. A sea state is characterized by statistics, including the wave height, period, and power spectrum. The sea state varies with time, as the wind conditions or swell conditions change. The sea state can either be assessed by an experienced observer, like a trained mariner, or through instruments like weather buoys, wave radar, or remote sensing satellites.

Evaluate the Weather's Effects on Military Operations

4-74. Weather has both direct and indirect effects on military operations. The following are examples of direct and indirect effects on military operations:

- **Temperature inversions might cause some battle positions to be more at risk to the effects of chemical agents as a result of atmospheric ducting, a process that occurs when strong high pressure influences an area and prevents particulates from dispersing into the upper atmosphere.**
- **Local visibility restrictions, such as fog, can have an effect on observation for both friendly and threat/*adversary* forces. Severe restrictions to visibility often restrict aviation operations.**
- **Hot, dry weather might force friendly and threat/*adversary* forces to consider water sources as key terrain.**
- **Dense, humid air limits the range of loudspeaker broadcasts affecting sonic deception, surrender appeals to enemy forces, and the ability to provide instruction to friendly or neutral audiences.**
- **Sandstorms with high silica content may decrease the strength and clarity of radio and television signals.**

4-75. Weather and climate effects have an impact on seasonal outlooks, which have utility for seasonal decisionmaking; for example, giving crop selection and rotation advice in a particular area that boosts plant growth. Knowing that a particular area may be susceptible to locust swarms may enable pesticide application to prevent such a swarm. If a drought is expected, civil affairs personnel may advise planting another crop that raises the benefit to the farmer.

4-76. The following work aids assist in analyzing and describing weather effects on operations. (See *MCWP 3-35.7,* NWP 3-59M/*MCWP 3-35.10*, and JP 3-59 for additional weather-related operational and tactical decision aids.)

4-77. Figure 4-15 is an example of a weather forecast chart. This work aid provides a guide for determining the weather information needed for planning and operations.

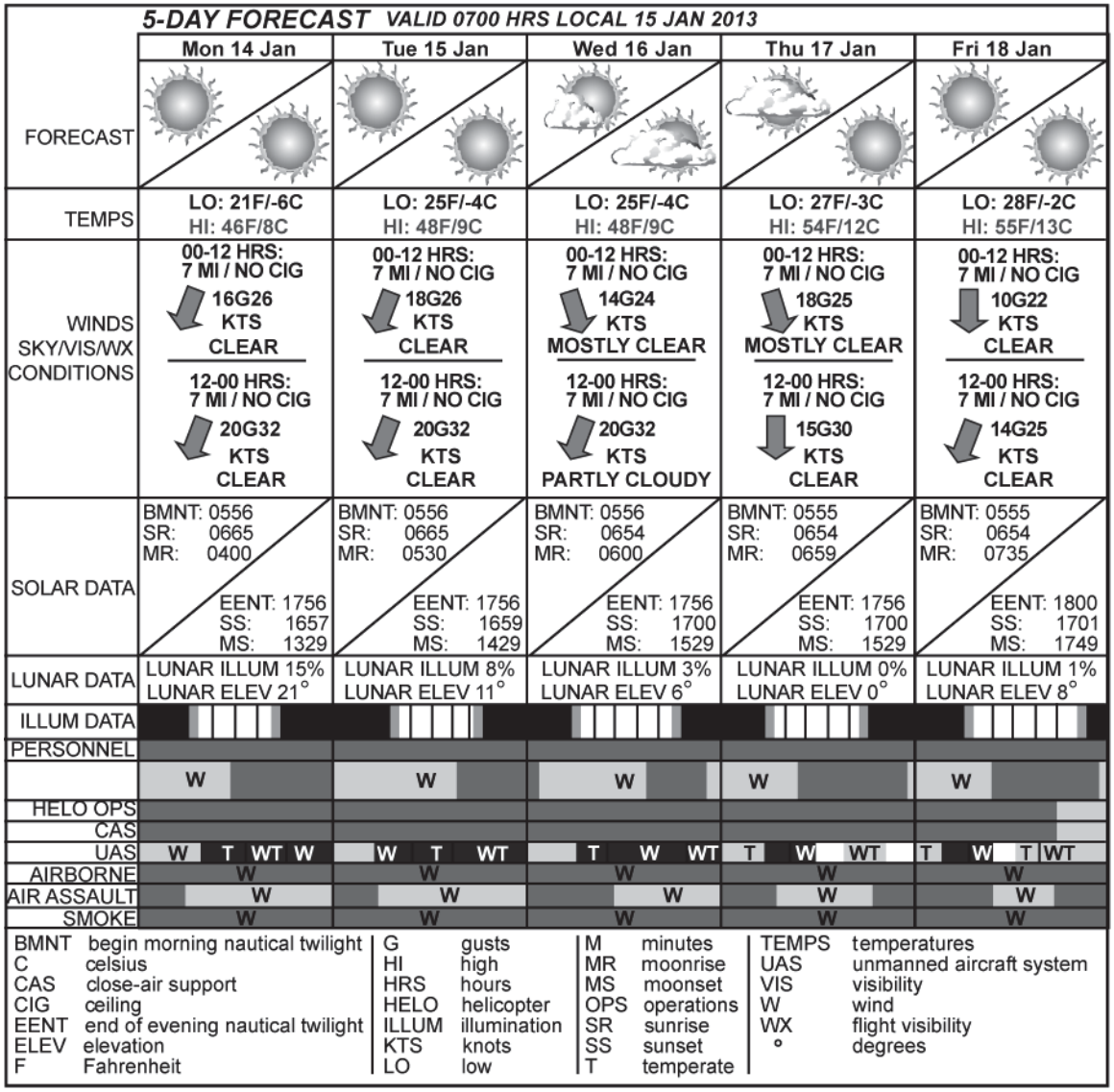


Figure 4-15. Example weather forecast chart

4-78. Figure 4-16 is an example of a light and illumination table. This work aid provides a guide for determining the light and illumination data needed for planning and operations.

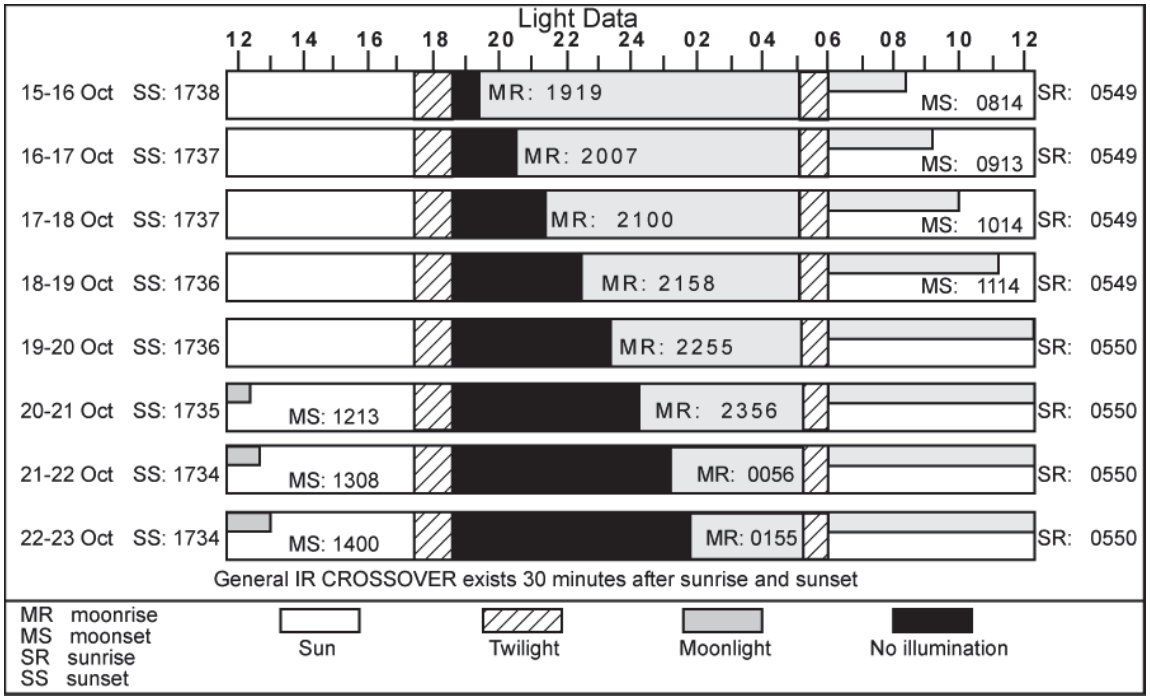


Figure 4-16. Example light and illumination table

4-79. Figure 4-17 is an example of a weather effects matrix/*operational impacts chart* in a table format. This work aid provides a guide for determining the weather effects on personnel, weapons, and equipment needed for planning and operations.

	Operation	06-09	09-12	12-15	15-18	18-21	21-24	00-03	03-06	Comment
INTEL	Dismounted Reconnaissance				C	C	C			
	Mounted Reconnaissance				C	C	C			
	Sensors									
	UAS based on what is assigned								W	
	Maneverability based on unit composition (foot, wheel, track)				P	P				
AVN	Rotary-wing	W								
	Fixed-wing									
	Aircraft Interpect (Radar)									
	Heavy Fixed-wing									
	Airborne Operations									
	Civil Considerations									
	Indirect Fires (Mortars/Artillery)									
	Engineers				P	P				
	Laser or Thermal Operation			P	P	P				
	MOPP IV		T	T	T	T				

Moderate Degradation
Severe Degradation

AVN aviation
HELO helicopter
INTEL intelligence
MOPP mission-oriented protective posture
RECON reconnaissance
UAS unmanned aircraft system

C ceiling
P precipitation
T temperature
V visibility
W wind

Figure 4-17. Weather effects matrix/*operational impacts chart*

4-80. ***In the Marine Corps, METOC Marines are tasked with rendering tactical METOC support to every element of the MAGTF. Throughout the IPB process, METOC considerations are embedded within each step of the planning to ensure a full understanding of environmental impacts across the full range of military operations. As a Service component, the Marine Corps specializes in amphibious landing—forcible entry from the sea. A core competency unique to the Marine Corps, amphibious landings have specific METOC support requirements that must be exercised to ensure mission accomplishment. Current and forecast environmental conditions are applied to the array of vehicles used during amphibious insertions; sea states and surf zone conditions impact all amphibious landing craft in different ways, and a solid forecast is crucial when determining if an amphibious landing is a viable option.***

4-81. ***The main amphibious platforms used by the Marine Corps personnel are the amphibious assault vehicle, landing craft/air cushioned, combat rubber reconnaissance craft, landing craft/utility, and rigid-hull inflatable boat. Forecasting for amphibious landings requires an in-depth knowledge of the platforms used in the operation, as well as environmental parameters that establish Go/No-Go criteria. Each of these platforms has specific operational thresholds while operating over the open ocean as well as within the surf zone at the landing site. Prior to launching any amphibious assets, METOC personnel analyze sea and surf zone conditions, and in concert with topographic and imagery Marines, conduct environmental and geographical analysis on proposed beach landing sites. Key beach landing sites analysis points include but are not limited to—***

- ***Hydrographic surveys (usually accomplished by force reconnaissance Marines or embedded Navy sea, air, and land teams).***
- ***Beach slope (>1/30 favorable, 1/30 to 1/50 marginal, >1/50 unfavorable).***
- ***Soil composition.***
- ***Breaker type (surf observations).***
- ***Sea state.***
- ***Modified surf index at the proposed landing time.***
- ***Bioluminescence.***
- ***Underwater hazards.***
- ***Littoral current speed and direction.***
- ***Immersion survivability time/water temperature.***

4-82. ***Marine METOC personnel work with their Navy METOC counterparts to provide a unified forecast; this coordination usually takes place aboard navy amphibious ships, but also takes place among Marine Corps METOC sections attached to intelligence units.***

Example

During the D-Day invasion at Normandy, surf zone conditions were extremely choppy; however, the date of 6 June 1944 was specifically chosen because that date offered a slight break in sea conditions that were otherwise impassable. Allied forces were able to execute a successful landing, and the German stronghold in France was finally broken.

4-83. ***METOC conditions have historically played a crucial role in operational planning, and are no less important today than they have been in the history of amphibious warfare.***

4-84. ***Figures 4-18 through 4-26 on pages 4-24 through 4-28 are samples of METOC products used during Navy/Marine Corp METOC collaboration while at sea to illustrate Marine Corps METOC support to amphibious operations. (See 3-35.7, NWP 3-59M/MCWP 3-35.10, and JP 3-59 for additional information on Navy/Marine Corp METOC while at sea and during the execution of METOC support.)***

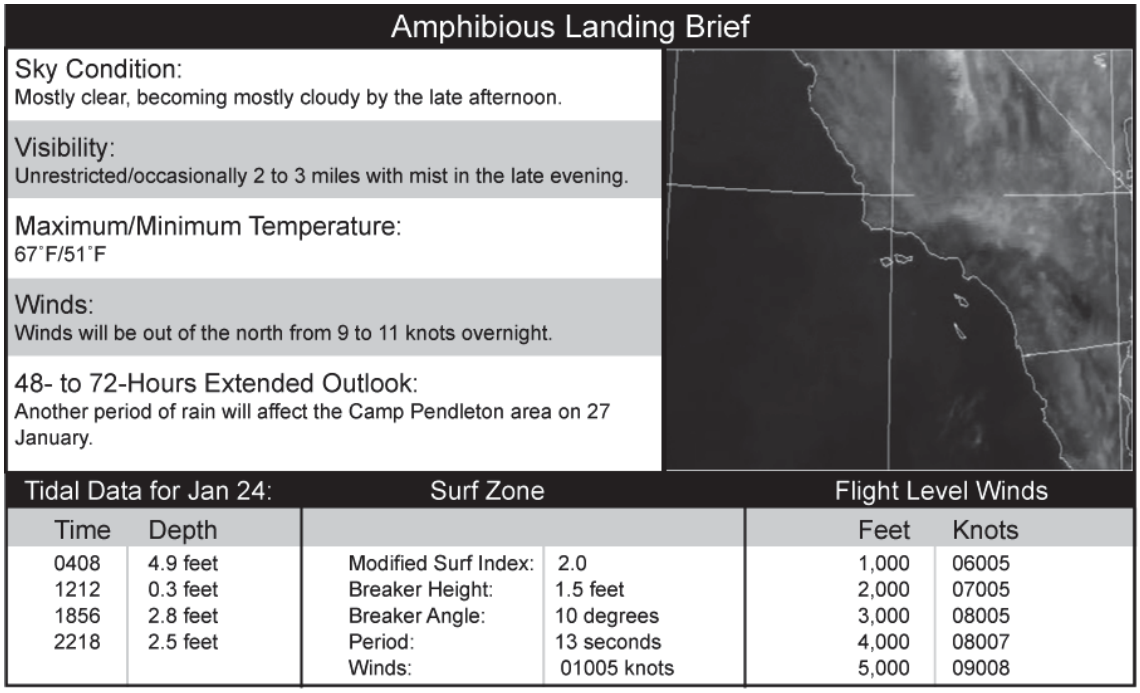


Figure 4-18. ***Amphibious landing weather example***

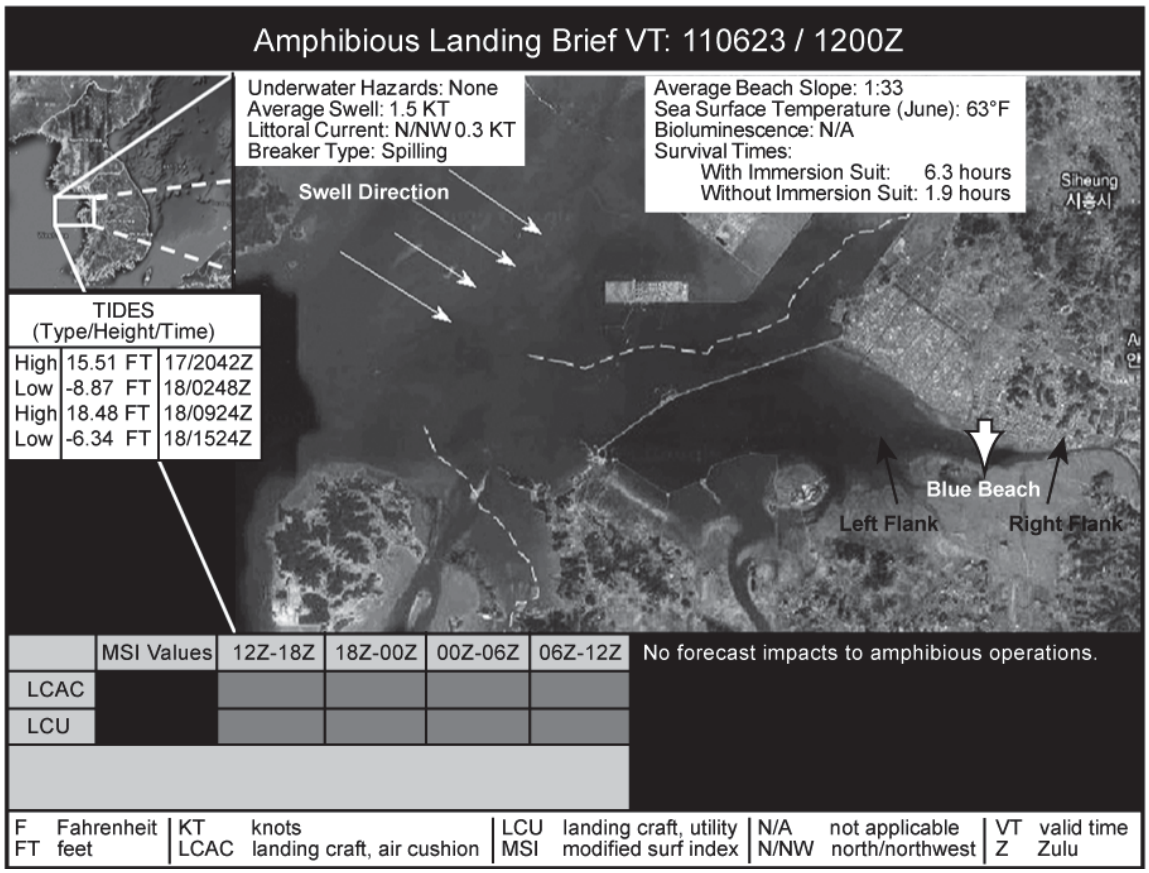


Figure 4-19. ***Beach landing site weather example***

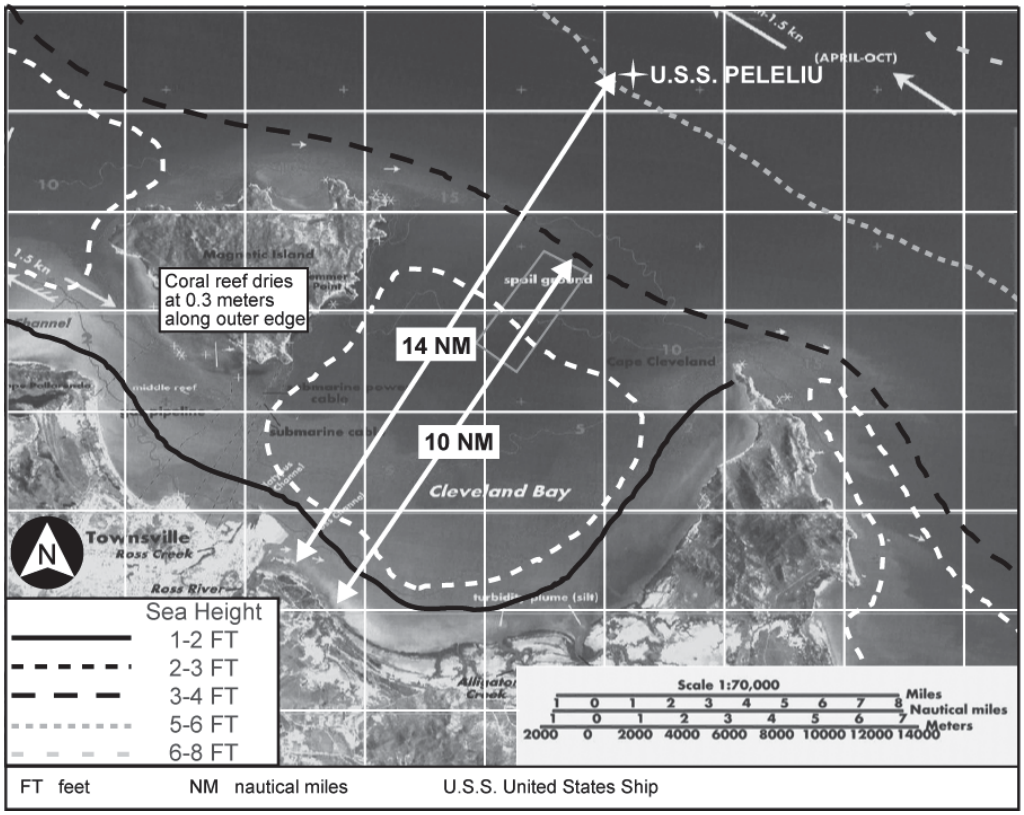


Figure 4-20. ***Littoral weather example***

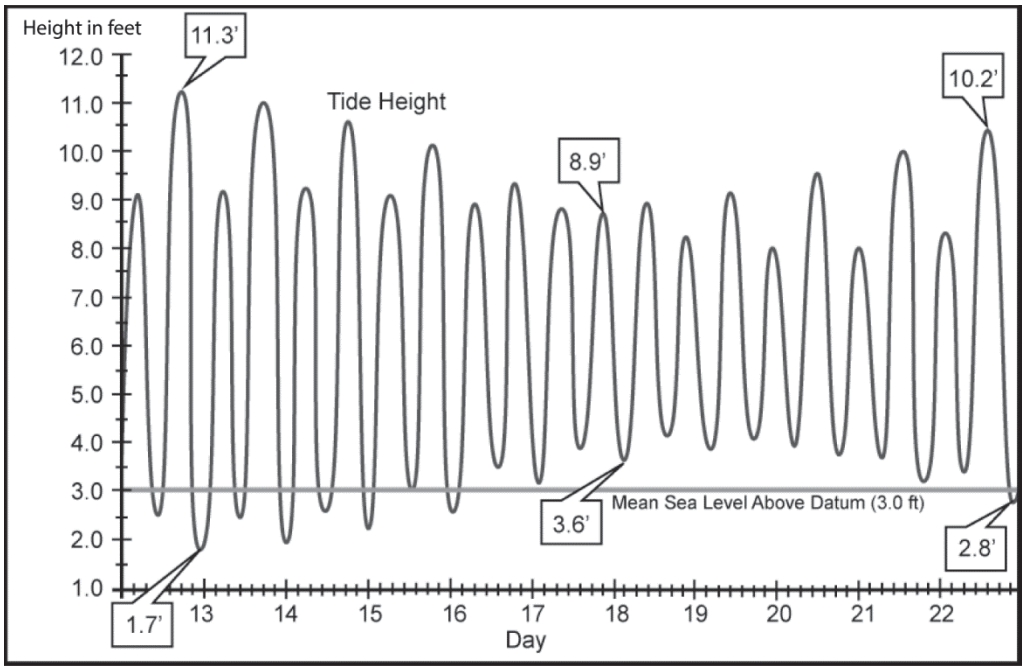


Figure 4-21. ***Tidal weather example***

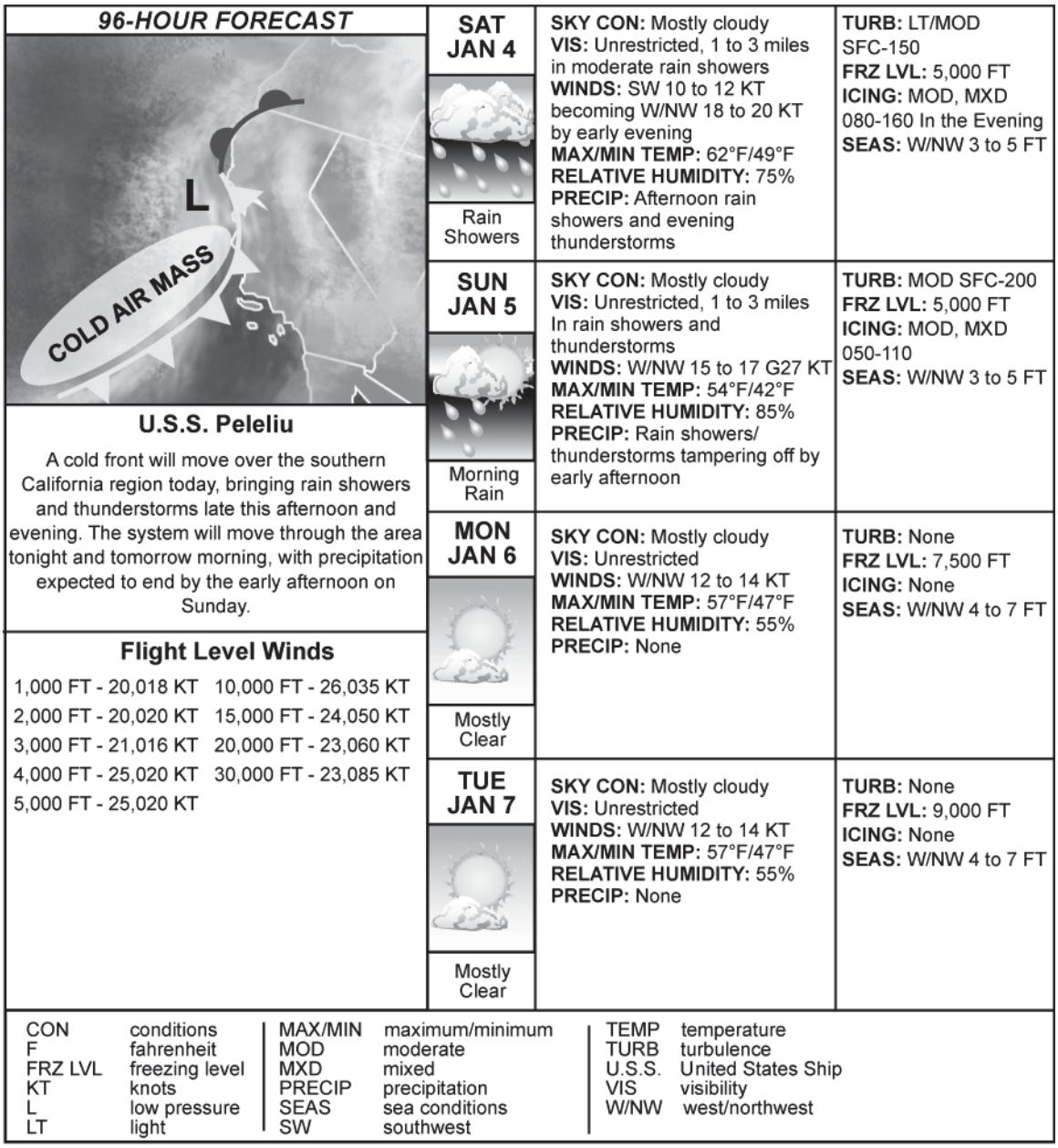


Figure 4-22. 96-hour forecast weather example

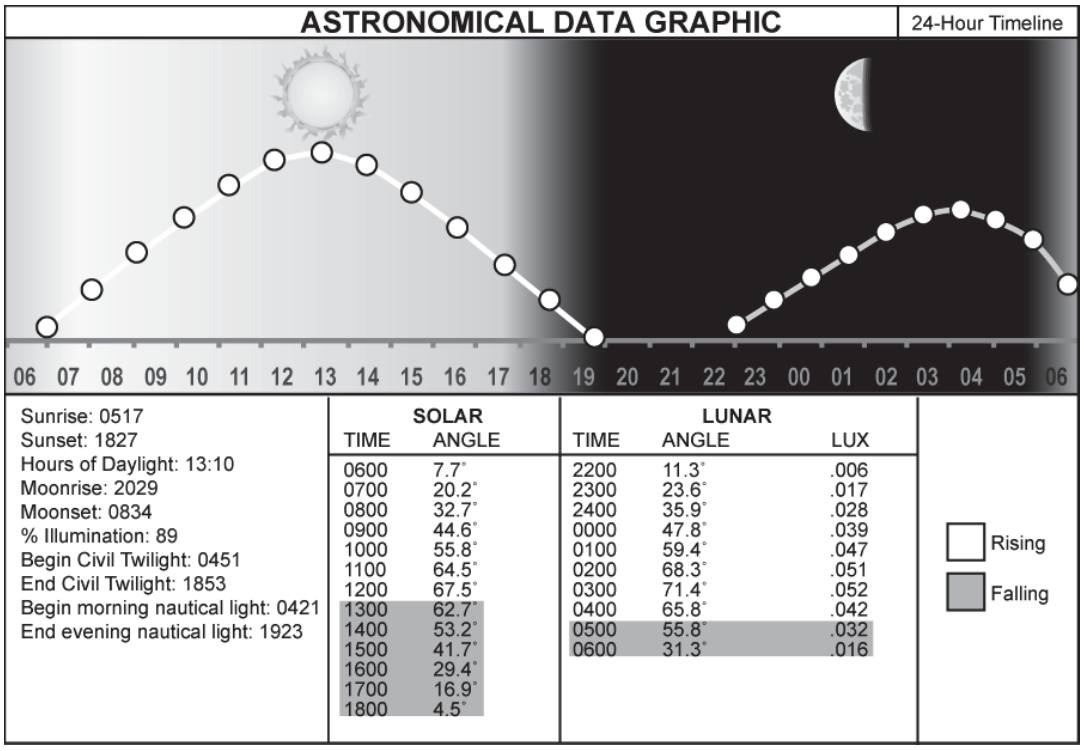


Figure 4-23. ***Astronomical data weather example***

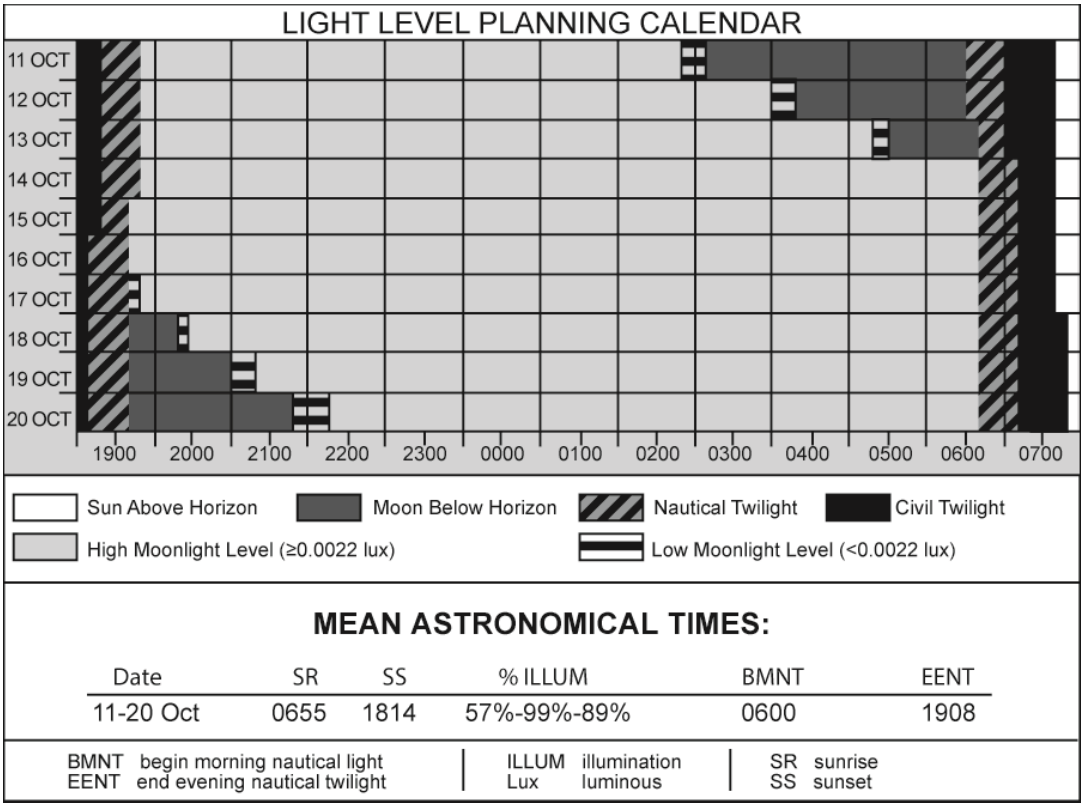


Figure 4-24. ***Light level weather example***

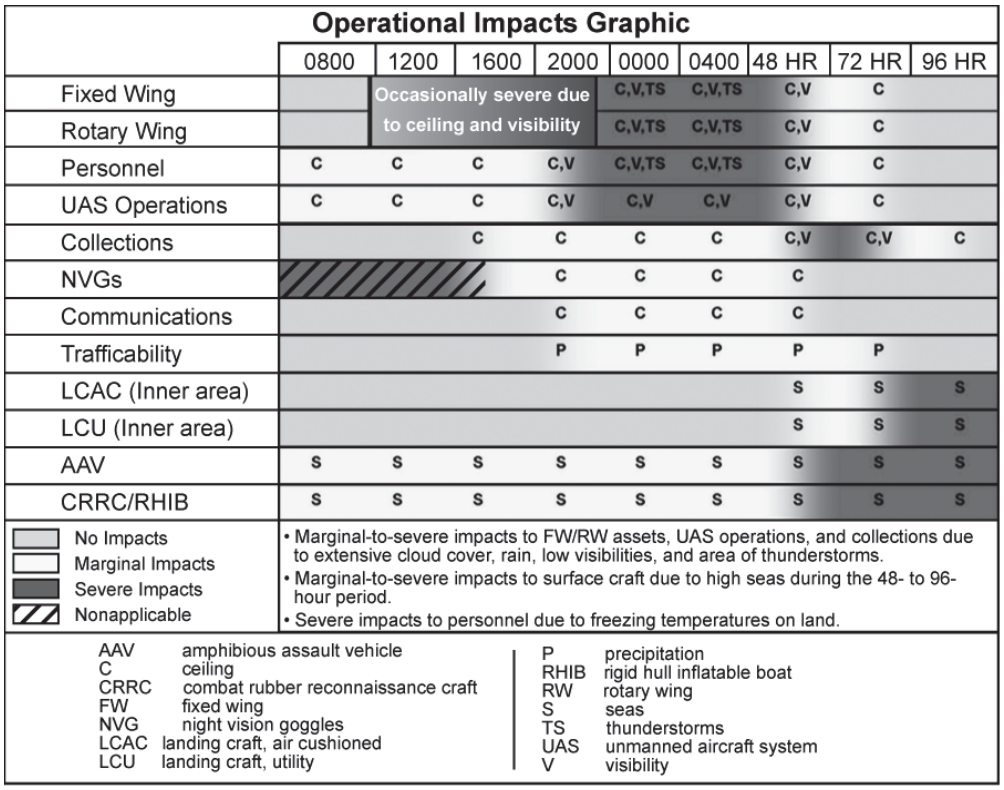


Figure 4-25. ***Operational impacts weather example***

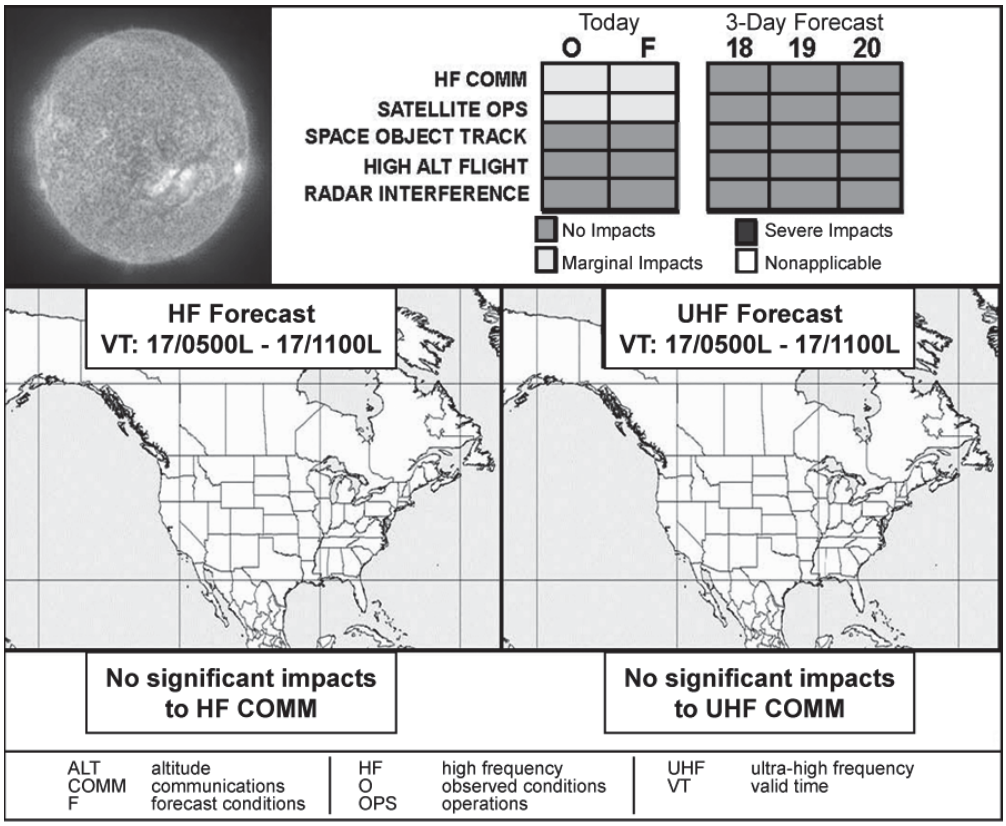


Figure 4-26. ***Space weather example***

DESCRIBE HOW CIVIL CONSIDERATIONS CAN AFFECT FRIENDLY AND THREAT/*ADVERSARY* OPERATIONS

4-85. An understanding of civil considerations—the ability to analyze their impact on operations—enhances several aspects of operations: among them, the selection of objectives; location, movement, and control of forces; use of weapons; and protection measures. The intelligence staff should leverage the rest of the staff, as well as outside agencies, who have expertise in civil considerations to aid the intelligence analysis in this area. Building knowledge during Army force generation is an opportunity to leverage agencies which are not deploying with the unit, but which have relevant regional knowledge.

4-86. Civil considerations comprise six characteristics, expressed in the memory aid ASCOPE. Civil considerations encompass the manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an AO and how these elements influence military operations. Tactical Army/*Marine Corps* staffs use ASCOPE to analyze civil considerations that are essential to support the development of effective plans for operations. Table 4-4 lists one method of cross-walking the operational variables PMESII and some examples for each ASCOPE characteristic.

4-87. ***Sociocultural factors are the social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment (JP 2-01.3) must be closely analyzed during irregular warfare and hybrid conflicts. This cultural information incorporated into the IPB process provides the backdrop against which an analysis of social and political factors will allow for successful operations. The MCIA produced a cultural GIRH and Cultural Intelligence Indicator Guide that will assist Marine forces in understanding foreign cultures. Both documents are available on MCIA's SIPRNET Web site. Used in conjunction with ASCOPE analysis, an appreciation of cultural intelligence enables Marines to understand the environment in which they operate and ultimately lead to mission accomplishment.***

Table 4-4. PMESII and ASCOPE examples

	AREAS	STRUCTURES	CAPABILITIES	ORGANIZATIONS	PEOPLE	EVENTS
POLITICAL	• Enclaves • Municipalities • Provinces • Districts • Political districts • Voting • National boundaries • Party affiliation areas • Shadow government influence areas	• Courts (court houses, mobile courts) • Government centers • Provincial/district centers • Meeting halls • Polling sites	• Public administration: ◦ Civil authority, practices, and rights ◦ Political system ◦ Political stability ◦ Political traditions ◦ Standards and effectiveness • Executive: ◦ Administration ◦ Policies ◦ Powers ◦ Organization • Legislative: ◦ Administration ◦ Policies ◦ Powers ◦ Organization • Judicial/legal: ◦ Administration ◦ Capacity ◦ Policies ◦ Civil and criminal codes ◦ Powers ◦ Organization ◦ Law enforcement • Dispute resolution, grievances • Local leadership • Degrees of legitimacy	• Major political parties: ◦ Formal ◦ Informal • Nongovernment organizations • Host government • Insurgent group affiliations • Court system • Covert political power • Partnerships: foreign	• United Nations representatives • Political leaders • Governors • Councils • Elders • Community leaders • Paramilitary members • Judges • Prosecutors	• Elections • Council meetings • Speeches (significant) • Security and military training sessions • Significant trials • Distribution of power • Political motivation • Treaties • Will
MILITARY	• Area of influence • Area of interest • Area of operation • Safe havens or sanctuary • Multinational/local nation bases • Historic ambush/ improvised explosive device sites/insurgent bases	• Bases • Headquarters (police) • Known leader houses/businesses	• Doctrine • Organization • Training • Materiel • Leadership • Personnel manpower • Facilities • History • Nature of civil-military relationships • Resource constraints • Local security forces • Quick reaction force • Insurgent strength • Enemy recruiting	• Host-nation forces present • Insurgent groups present and networks • Multinational forces • Paramilitary organizations • Terrorists • Multinational forces present • Fraternal organizations • Civic organizations	• Key leaders • Multinational, insurgent, military	• Combat • Historical • Noncombat • Kinetic events • Unit reliefs • Loss of leadership

Table 4-4. PMESII and ASCOPE examples (continued)

	AREAS	STRUCTURES	CAPABILITIES	ORGANIZATIONS	PEOPLE	EVENTS
ECONOMIC	• Commercial • Fishery • Forestry • Industrial • Livestock dealers • Markets • Mining • Movement of goods/ services • Smuggling routes • Trade routes • Black market areas	• Banking • Fuel: ◦ Distribution ◦ Refining ◦ Source • Industrial plants • Manufacturing • Mining • Warehousing • Markets • Silos, granaries, warehouses • Farms/ranches • Auto repair shops	• Fiscal: ◦ Access to banks ◦ Currency ◦ Monetary policy • Ability to withstand drought • Black market • Energy • Imports/exports • External support/aid • Food: ◦ Distributing ◦ Marketing ◦ Production ◦ Processing ◦ Rationing ◦ Security ◦ Storing ◦ Transporting • Inflation • Market prices • Raw materials • Tariffs	• Banks • Business organizations • Cooperatives • Economic nongovernment organizations • Guilds • Labor unions • Major illicit industries • Large landholders • Volunteer groups	• Bankers • Employers/employees • Labor occupations • Consumption patterns • Unemployment rate • Underemployment rate (if this exists) • Job lines • Landholders • Merchants • Money lenders • Black marketers • Gang members • Smuggling chain	• Drought, harvest, yield, domestic animals, livestock (cattle, sheep) and market cycles • Labor migration events • Market days • Payday • Business openings • Loss of business
SOCIAL	• Refugee camps • Enclaves: ◦ Ethnic ◦ Religious ◦ Social ◦ Tribal ◦ Families or clans • Neighborhoods • Boundaries of influence • School districts • Parks • Traditional picnic areas • Markets • Outdoor religious sites	• Clubs • Jails • Historical buildings/ houses • Libraries • Religious • Schools/universities • Stadiums • Cemeteries • Bars and tea shops • Social gathering places (meeting places) • Restaurants	• Medical: ◦ Traditional ◦ Modern • Social networks • Academic • Strength of tribal/village traditional structures • Judicial	• Clan • Community councils and organizations • School councils • Criminal organizations • Familial • Patriotic/service organizations • Religious groups • Tribes	• Community leaders, councils and their members • Education • Ethnicity/racial: ◦ Biases ◦ Dominant group ◦ Percentages ◦ Role in conflict • Key figures: ◦ Criminals ◦ Entertainment ◦ Religious leaders ◦ Chiefs/elders • Language/dialects • Vulnerable populations • Displaced persons • Sports • Influential families • Migration patterns • Culture: ◦ Artifacts ◦ Behaviors ◦ Customs ◦ Shared beliefs/values	• Celebrations • Civil disturbances • National holidays • Religious holidays and observance days • Food line • Weddings • Birthdays • Funerals • Sports events • Market days • Family gatherings • History: Major wars/ conflicts
INFORMATION	• Broadcast coverage area (newspaper, radio, television) • Word of mouth • Gathering points • Graffiti • Posters	• Communications: ◦ Lines ◦ Towers (cell, radio, television) • Internet service: ◦ Satellite ◦ Hard wire ◦ Cafes • Cellular phone • Postal service • Print shops • Telephone • TV stations • Radio stations	• Availability of electronic media • Indigenous communications networks • Internet access • Intelligence services • Printed material: ◦ Journals ◦ Newspapers ◦ Flyers • Propaganda mechanisms • Radio • Television • Social media • Literacy rate • Word of mouth	• Media groups and news organizations • Religious groups • Insurgent inform and influence activities groups • Government groups • Public relations and advertising agencies	• Decisionmakers • Media personalities • Media groups and news organizations • Community leaders • Elders • Heads of families	• Disruption of services • Censorship • Religious observance days • Publishing dates • Inform and influence activities campaigns • Project openings
INFRASTRUCTURE	• Commercial • Industrial • Residential • Rural • Urban • Road systems • Power grids • Irrigation networks • Water tables	• Emergency shelters • Energy: ◦ Distribution system ◦ Electrical lines ◦ Natural gas ◦ Power plants • Medical: ◦ Hospitals ◦ Veterinary • Public buildings • Transportation: ◦ Airfields ◦ Bridges ◦ Bus stations ◦ Ports and harbors ◦ Railroads ◦ Roadways ◦ Subways • Waste distribution, storage, and treatment: ◦ Dams ◦ Sewage ◦ Solid • Construction sites	• Construction • Clean water • Communications systems • Law enforcement • Fire fighting • Medical: ◦ Basic ◦ Intensive ◦ Urgent • Sanitation • Maintain roads, dams, irrigation, sewage systems • Environmental management	• Construction companies: ◦ Government ◦ Contract	• Builders • Road contractors • Local development councils	• Scheduled maintenance (road/bridge construction) • Natural/manmade disasters • Well digging • Community center construction • School construction

4-88. Due to the complexity and volume of data involving civil considerations, there is no simple model for presenting civil considerations analysis. Rather, it comprises a series of intelligence products composed of overlays and assessments. The six characteristics of ASCOPE are discussed in paragraphs 4-89 through 4-116.

AREAS

4-89. Key civilian areas are localities or aspects of the terrain within an AO that often are not militarily significant. This characteristic approaches terrain analysis (OAKOC/*KOCOA*) from a civilian perspective. The intelligence staff analyzes key civilian areas in terms of how they may affect the missions of friendly forces as well as how friendly military operations may affect these areas. Examples of key civilian areas are—

- **Areas defined by political boundaries, such as districts within a city or municipalities within a region.**
- **Locations of government centers.**
- **Social, political, religious, or criminal enclaves.**
- **Ethnic/Sectarian fault lines.**
- **Agricultural and mining regions.**
- **Trade routes.**
- **Possible sites for the temporary settlement of displaced civilians or other civil functions.**

4-90. The intelligence staff maintains this information in the civil considerations data file and constructs an areas overlay to aid in planning. The civil considerations data file and the areas overlay are discussed beginning at paragraph 4-117.

STRUCTURES

4-91. Existing structures can have various degrees of significance. Analyzing structures involves determining how the location, functions, capabilities, and consequences of its use can support or hinder the operation. Using a structure for military purposes often competes with civilian requirements. Commanders must carefully weigh the expected military benefits against costs to the community that have to be addressed in the future. Commanders also need to consider the significance of the structure in providing stability to the AO. Certain structures are critical in providing a state of normalcy back to the community and need to be maintained or restored quickly. The possibility of repaying locals for the use of shared facilities or building more of the same facilities, time and cost permitting, should also be considered. The following are examples of structures:

- **Military bases.**
- **Police stations.**
- **Jails.**
- **Courtrooms.**
- **Political offices.**
- **Electrical power plants and substations.**
- **Petroleum, oils, and lubricants refineries.**
- **Dams.**
- **Water and sewage treatment and distribution facilities.**
- **Communications stations and networks.**
- **Bridges and tunnels.**
- **Warehouses.**
- **Airports and bus terminals.**
- **Universities and schools.**

4-92. Other structures are cultural sites that international law or other agreements generally protect, for example:

- **Religious structures.**
- **National libraries and archives.**
- **Hospitals and medical clinics.**
- **Monuments.**
- **Works of art.**
- **Archaeological sites.**
- **Scientific buildings.**
- **Museums.**
- **Crops, livestock, and irrigation works.**
- **United Nations Educational, Scientific and Cultural Organizations-designated World Heritage Sites.**

4-93. The intelligence staff maintains this information in the civil considerations data file and, due to the amount of information in these categories, constructs multiple overlays for structures to aid in planning.

CAPABILITIES

4-94. Commanders and staffs analyze capabilities from different levels. They view capabilities in terms of those required to save, sustain, or enhance life, in that priority. Capabilities can refer to the ability of local authorities—those of the host nation, aggressor nation, or some other body—to provide a populace with key functions or services, such as—

- **Public administration.**
- **Public safety.**
- **Emergency services.**
- **Technology.**
- **Basic necessities (food, water, medical availability).**

4-95. Capabilities include those areas in which the populace may need help after combat operations/*major operations*, such as public works and utilities, public health, economics, and commerce. Capabilities also refer to resources and services that can be contracted to support the military mission, such as interpreters, laundry services, construction materials, and equipment.

4-96. The intelligence staff maintains this information in the civil considerations data file and constructs a structures overlay to aid in planning.

ORGANIZATION

4-97. IPB considers the organization dimension (such as the nonmilitary groups or institutions) and political influence and their impacts in the AO. Organizations influence and interact with the populace, friendly forces, the threat/*adversary*, and each other. An important aspect of civil considerations is the political dimension of the local population and their expectations relative to threat/*adversary* and friendly operations.

4-98. Political structures and processes enjoy varying degrees of legitimacy with populations from local through international levels. Formally constituted authorities and informal or covert political powers strongly influence events. Political leaders can use ideas, beliefs, violence, and other actions to enhance their power and control over people, territory, and resources. There are many sources of political interest. These may include charismatic leadership; indigenous security institutions; and religious, ethnic, or economic factors. Political opposition groups or parties also affect the situation. Each may cooperate differently with U.S. or multinational forces.

4-99. Understanding the political circumstances helps commanders and staffs recognize key organizations and determine their aims and capabilities. Understanding political implications requires analyzing all relevant partnerships—political, economic, military, religious, and cultural. This analysis captures the presence and significance of external organizations and other groups, including groups united by a common cause. Examples include private security organizations, transnational corporations, and NGOs that provide humanitarian assistance.

4-100. Political analysis must include an assessment of varying political interests and the threat's/*adversaries'* political decisive point/*center of gravity* and will. Will is the primary intangible factor; it motivates participants to sacrifice to persevere against obstacles. Understanding what motivates key groups (for example, political, military, and insurgent) helps commanders understand the groups' goals and willingness to sacrifice to achieve their ends.

4-101. Organizations are nonmilitary groups or institutions in the AO. They influence and interact with the populace, the force, and each other. They generally have a hierarchical structure, defined goals, established operations, fixed facilities or meeting places, and a means of financial or logistic support. Some organizations may be indigenous to the area. These organizations may include—

- **Religious organizations.**
- **Fraternal organizations.**
- **Patriotic or service organizations.**
- **Labor unions.**
- **Criminal organizations.**
- **Community watch groups.**

- **Political groups.**
- **Agencies, boards, committees, commissions (local and regional, councils).**
- **Multinational corporations.**
- **Intergovernmental organizations (IGOs), such as United Nations agencies.**
- **Other host-nation government agencies (foreign version of Department of Education, United States Agency for International Development).**
- **NGOs, such as the International Committee of the Red Cross.**

Note. **The other host-nation government agencies designated above are separate from organizations within the threat/*adversary* capability (military, intelligence, police, paramilitary), such as the Central Intelligence Agency.**

4-102. To enhance their situational awareness, commanders must remain familiar with organizations operating in their AOs, such as local organizations which understand the political dimension of the population. Situational awareness includes having knowledge of how the activities of different organizations may affect military operations and how military operations may affect these organizations' activities. From this, commanders can determine how organizations and military forces can work together toward common goals when necessary.

4-103. In almost every case, military forces have more resources than civilian organizations. However, civilian organizations may possess specialized capabilities that they may be willing to share with military forces. Commanders do not command civilian organizations in their AOs. However, some operations require achieving unity of effort between them and the force. These situations require commanders to influence the leaders of these organizations through persuasion. They produce constructive results by the force of argument and the example of their actions.

4-104. The intelligence staff maintains this information in the civil considerations data file and, due to the amount of information in these categories, constructs multiple overlays for organizations to aid in planning.

PEOPLE

4-105. The use of the general term "people" describes nonmilitary personnel encountered by military forces. The term includes all civilians within an AO as well as those outside the AO whose actions, opinions, or political influence can affect the mission. Individually or collectively, people can affect a military operation positively, negatively, or neutrally. In stability tasks, Army/*Marine Corps* forces work closely with civilians of all types. Understanding the sociocultural factors of the people in the AO is a critical component of understanding the operational environment.

4-106. There can be many different kinds of people living and operating in and around an AO. As with organizations, people may be indigenous or introduced from outside the AO. An analysis of people will identify them by their various capabilities, needs, and intentions. It is useful to separate people into distinct categories such as demographically, social and political groups, and target audiences. (A target audience list can be obtained from the military information support operations element or information operations officer/G-3.) When analyzing people, commanders consider historical, cultural, ethnic, political, economic, religious, and humanitarian factors. They also identify the key communicators and the formal and informal processes used to influence people.

4-107. The languages used in the region will have a huge impact on operations. The staff identifies the languages and dialects used within the AO so language training, communication aids (such as phrase cards and requisitioning of translators) can begin. Translators will be crucial for collecting intelligence, interacting with local citizens and community leaders, and developing products.

4-108. Another aspect of language involves the transliteration guide not written using the English alphabet. This will have an impact on all intelligence operations to include collection, analysis, dissemination, and targeting. In countries that do not use the English alphabet, a theater-wide standard should be set for spelling names. Without a spelling standard, it can be difficult to conduct effective analysis. In addition, insurgents and/or criminals may be released from custody if their names are

misidentified. To overcome these problems, there must be one spelling standard for a theater. Because of the interagency nature of counterinsurgency operations, the standard must be agreed upon by non-Defense agencies. Intelligence staffs should also be aware of family naming conventions in places like the Middle East where various cultures do not use an individual's surname and family name.

4-109. Another major consideration when analyzing people is religion. Religion has shaped almost every conflict of the past, and there are indicators that its influence will only grow. The staff considers the following when incorporating religion in planning. They—

- Know when religious traditions will be affected by the mission and try to determine how religion will affect the mission.
- Know when religious figures have influenced social transformations in a negative or positive way.
- Attempt to understand all parties, no matter how violent or exclusive.

4-110. Religion has the ability to shape the operational environment. Religion can add a higher intensity, severity, brutality, and lethality to conflicts than almost any other factor. Religion can motivate the masses quickly and inexpensively.

4-111. Part of the analysis of people is identifying cultural terms and conditions. Cultural terms and conditions describe both American and foreign ways of thought and behavior. Understanding culture gives insight into motives and intent of nearly every person or group in the operational environment: friend, enemy, or other. This insight in turn allows commanders and staffs to allocate resources, outmaneuver opponents, alleviate friction, and reduce the fog of war. The study of culture for military operations is not an academic exercise and therefore requires specific military guidelines and definition. The analyst sets aside personal bias and judgment and examines the cultural group dispassionately, basing the analysis purely on facts. The military studies broad categories of cultural factors, such as—

- Social structure.
- Behavioral patterns.
- Perceptions.
- Religious beliefs.
- Tribal relationships.
- Behavioral taboos.
- Centers of authority.
- Lifestyles.
- Social history.
- Gender norms and roles.

4-112. Culture is studied in order to give insights into the way people think, the reasons for their beliefs and perceptions, and what kind of behavior they can be expected to display in given situations. Because cultures are constantly shifting, the study of culture is an enduring task that requires historical perspective as well as the collection and analysis of current information.

4-113. The intelligence staff maintains this information in the civil considerations data file and, due to the amount of information in these categories, constructs multiple overlays for people to aid in planning.

EVENTS

4-114. Events are routine, cyclical, planned, or spontaneous activities that significantly affect organizations, people, and military operations. Examples include—

- National and religious holidays.
- Agricultural crop or livestock and market cycles.
- Elections.
- Civil disturbances.
- Celebrations.

- **Natural phenomenon (such as monsoon, seasonal floods and droughts, volcanic and seismic activity, natural disasters).**
- **Manmade disasters.**

4-115. Examples of events precipitated by military forces include combat operations/*major operations*, congested road networks, security restrictions, and economic infrastructure disruption or stimulus. Once significant events are determined, it is important to template the events and to analyze them for their political, economic, psychological, environmental, and legal implications.

4-116. The intelligence staff maintains this information in the civil considerations data file and constructs an events overlay to aid in planning. The civil considerations data file and overlays are discussed below.

CIVIL CONSIDERATIONS DATA FILES, OVERLAYS, AND ASSESSMENTS

4-117. As stated previously, the intelligence staff maintains a civil considerations data file that organizes all the information it has collected and analyzed based on the ASCOPE characteristics. This data file organizes the raw data the intelligence staff uses to assess civil considerations during IPB, as well as to support targeting and civil affairs operations. The data file includes all the information related in the ASCOPE characteristics.

Example

Under the "capabilities" characteristic there may be a section for the sub-characteristic of "oil." This section includes information on the location of all the infrastructure components associated with "oil." It would also include the biographical, contact, and location information for the personnel associated with this capability. Finally, this section includes any intelligence assessments and recommendations associated with "oil."

4-118. One way of maintaining civil considerations data is in a data file and/or database; this contributes to the continuous evaluation of civil considerations as part of the running estimate by organizing the vast amount of information necessary to analyze civil considerations.

4-119. Civil considerations overlays are graphic depictions of the data file and aids planning throughout the MDMP/*MCPP*, as well as aiding situation development during operations. These overlays aid the intelligence staff in describing civil considerations effects, as assessed in the data file, to the commander and rest of the staff.

4-120. The civil considerations data file and associated overlays aids the commander and staff in identifying information and intelligence requirements not normally identified through the event templating process associated with determining threat/*adversary* COAs. In contingency operations, or when conducting stability tasks, these work aids are critical in assisting the intelligence staff in determining and assessing threat/*adversary* COAs.

4-121. The civil consideration assessment is used throughout the MDMP/*MCPP*. Civil consideration assessments utilize both the civil considerations data files and overlays in order to provide the supported commander with a detailed analysis of the civil component of the area of interest in accordance with ASCOPE characteristics. Potential areas of investigation in the civilian consideration assessment could include, but are not limited to, mapping of social and political patterns, including formal and informal leadership as well as identifying key societal friction points. As stated previously, civil considerations help commanders understand the social, political, and cultural variables within the AO and their effect on the mission.

4-122. Understanding the relationship between military operations and civilians, culture, and society is critical to operations and is essential in developing effective plans. The development of civil considerations data files, overlays, and assessments can be augmented by regional civil considerations data repositories maintained at the national and theater levels.

4-123. During predeployment, unit intelligence staffs should become familiar with the information available on assigned or contingency regions in military and other data repositories, Web sites, and portals. During operations, units utilize, update, and add to the body of information available to them and others. During relief in place and/or transfer of authority, it is critical that outgoing units educate incoming units on the information sources available for their areas of operation.

4-124. HTTs/*foreign area officers, regional affairs, and other cultural enablers* can also provide detailed information and analysis pertaining to sociocultural factors as an aspect of civil considerations.

4-125. There is no standard set of sub-characteristics and overlays the intelligence staff produces under this task. The determination of what is needed is based on the intelligence staff's assessment of the situation and complexity of the AO.

4-126. The civil considerations data file is a spreadsheet set up in a workbook format that is tabbed using the categories identified in the ASCOPE characteristics. Figures 4-27 through 4-32 on pages 4-37 through 4-39 are examples of how to construct data files and overlays.

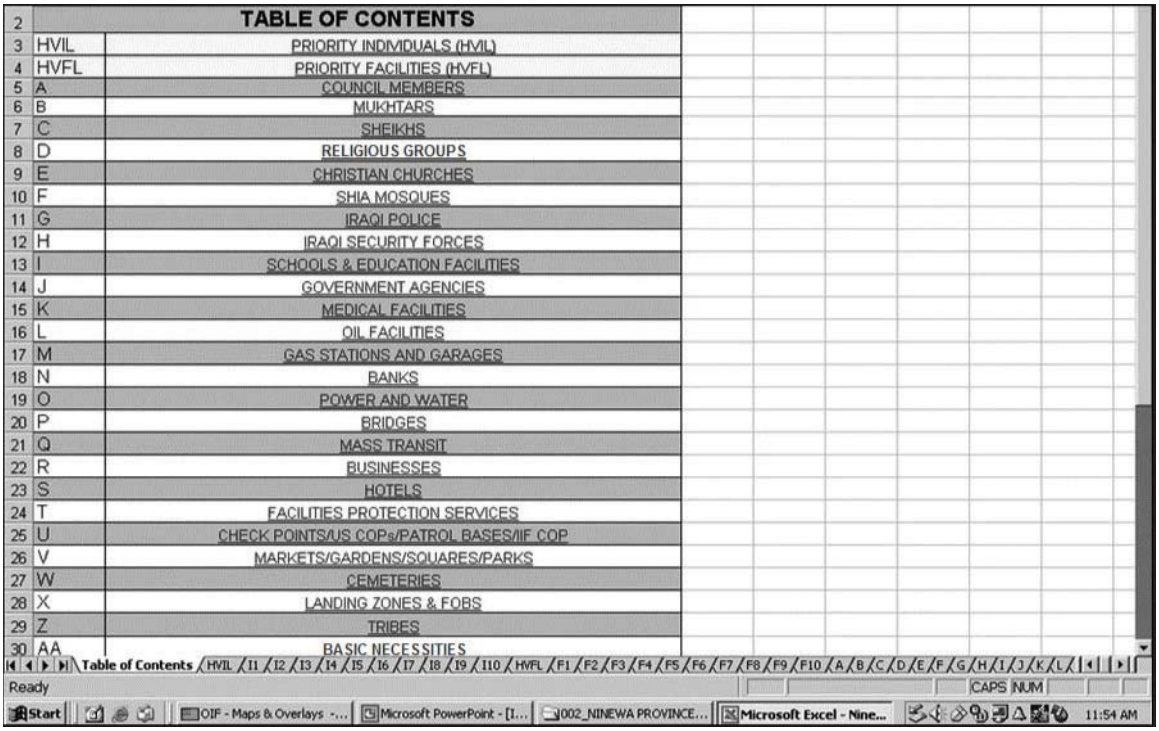


		TABLE OF CONTENTS
3	HVIL	PRIORITY INDIVIDUALS (HVIL)
4	HVFL	PRIORITY FACILITIES (HVFL)
5	A	COUNCIL MEMBERS
6	B	MUKHTARS
7	C	SHEIKHS
8	D	RELIGIOUS GROUPS
9	E	CHRISTIAN CHURCHES
10	F	SHIA MOSQUES
11	G	IRAQI POLICE
12	H	IRAQI SECURITY FORCES
13	I	SCHOOLS & EDUCATION FACILITIES
14	J	GOVERNMENT AGENCIES
15	K	MEDICAL FACILITIES
16	L	OIL FACILITIES
17	M	GAS STATIONS AND GARAGES
18	N	BANKS
19	O	POWER AND WATER
20	P	BRIDGES
21	Q	MASS TRANSIT
22	R	BUSINESSES
23	S	HOTELS
24	T	FACILITIES PROTECTION SERVICES
25	U	CHECK POINTS/US COPs/PATROL BASES/IIF COP
26	V	MARKETS/GARDENS/SQUARES/PARKS
27	W	CEMETERIES
28	X	LANDING ZONES & FOBS
29	Z	TRIBES
30	AA	BASIC NECESSITIES

Figure 4-27. Example of civil considerations data file

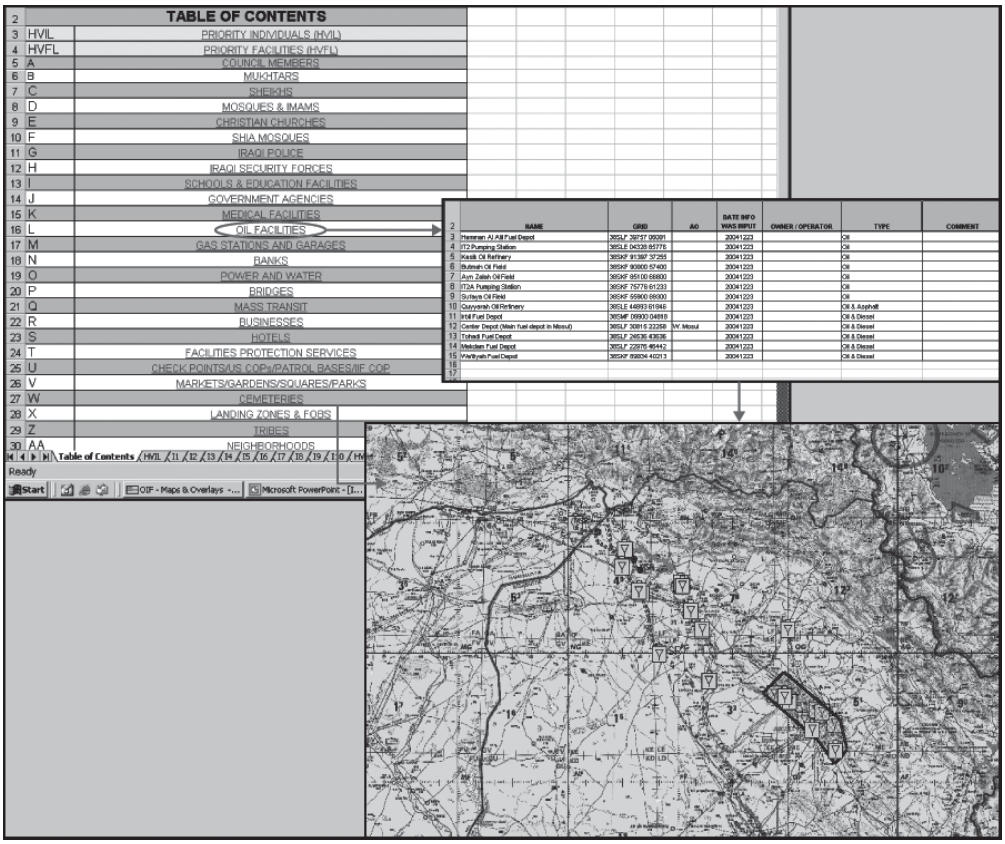


Figure 4-28. Civil considerations data file example (inside view with overlay)

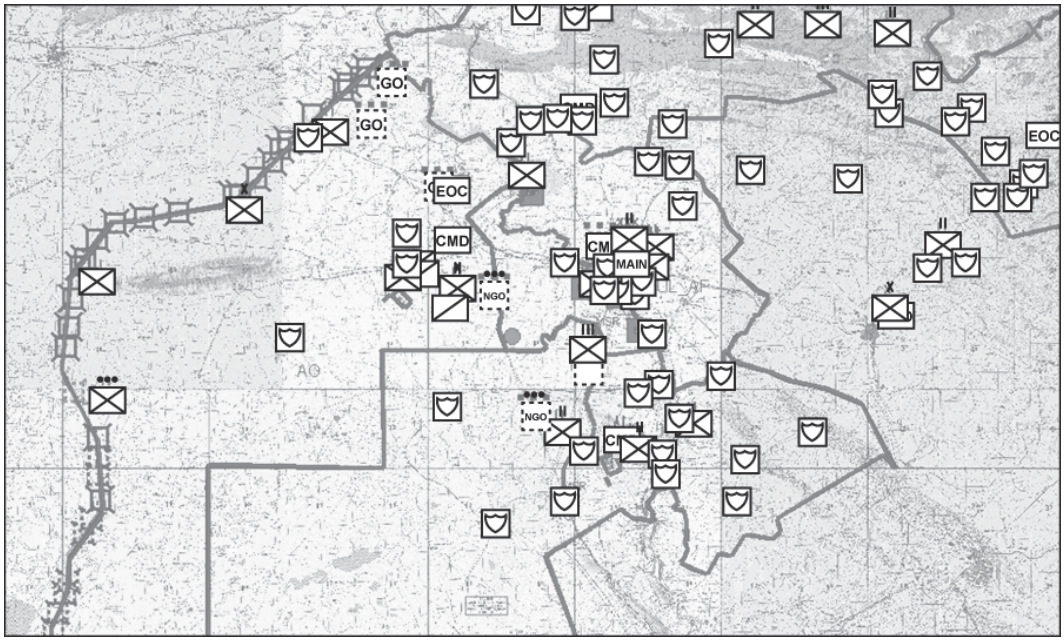


Figure 4-29. Security organizations and bases example

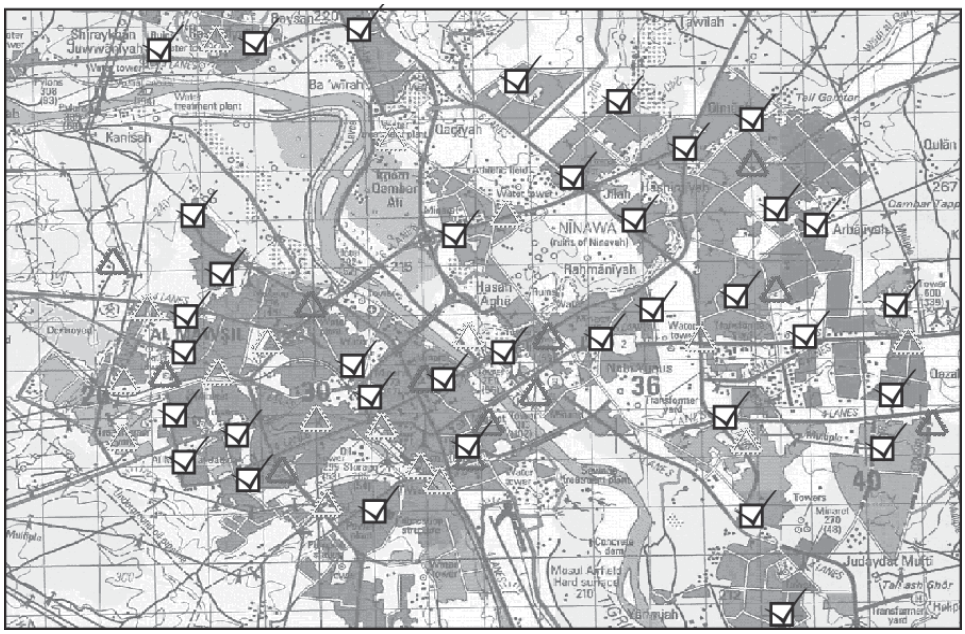


Figure 4-30. Voting locations example

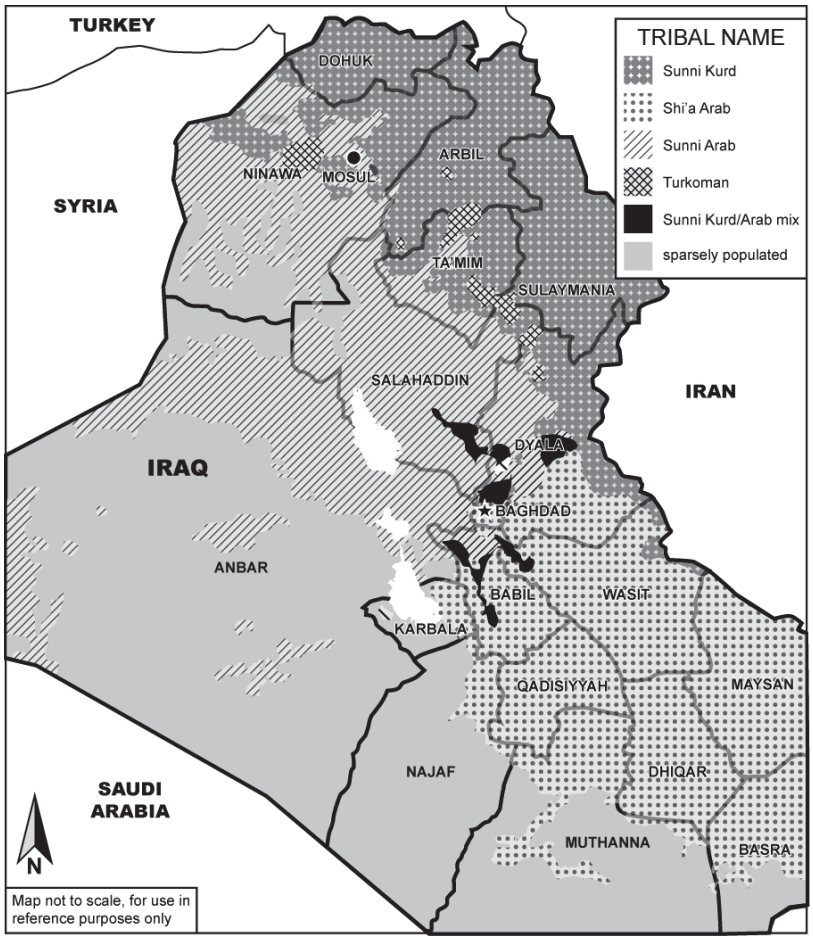


Figure 4-31. Population status example

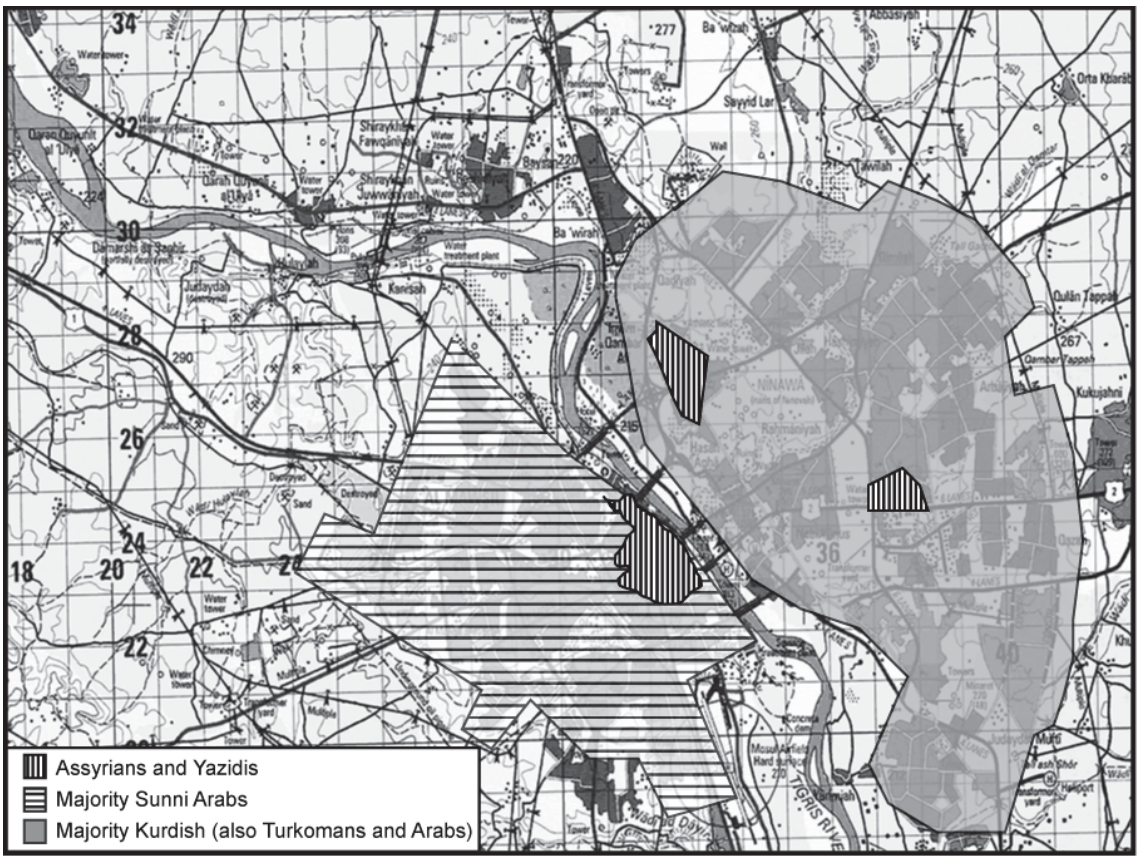


Figure 4-32. Ethnic overlay example

This page intentionally left blank.

Chapter 5

Step 3 of the IPB Process—Evaluate the Threat/*Adversary*

WHAT IS IT?

5-1. Step 3 of the IPB process determines threat/*adversary* force capabilities and the doctrinal principles and TTP threat/*adversary* forces prefer to employ. This may include threats/*adversaries* that create multiple dilemmas for our maneuver forces by simultaneous employment of regular, irregular, terrorist forces, and criminal elements, using an ever-changing variety of traditional and nontraditional tactics.

Example

While planning a contingency show-of-force operation, a G-2 directs the Joint Intelligence Center to study the decisions on record of the targeted country's dictator. As a result of this research, the intelligence center produces a model of how the dictator makes decisions, with special emphasis on the dictator's tendencies during political crises. Meanwhile, the S-2 of the brigade/*unit* that will conduct the operation does an individual evaluation of the threat/*adversary* that includes the S-2's contingency area threat characteristics/*adversary order of battle* files and determines that the two threat/*adversary* brigades within the target area are equipped, organized, and trained well enough to be capable of offensive as well as defensive tasks against the friendly brigade/*unit*. The S-2 prepares threat/*adversary* models depicting the threat/*adversary* normal offensive and defensive tasks in built-up areas (the setting for the show-of-force operation).

DESIRED END STATE

5-2. The G-2/S-2 develops threat/*adversary* models which accurately portray how threat/*adversary* forces normally execute operations and how they have reacted to similar situations in the past for the threats/*adversar*ies specific to the mission and environment. The primary output associated with step 3 of the IPB process is a compilation of threat/*adversary* models for each identified threat/*adversary* in the AO that the intelligence staff uses to guide the development of threat/*adversary* COA. This may include—

- **Creating and updating threat characteristics/*adversary order of battle* files.**
- **Developing the situation template.**
- **Creating threat/*adversary* capabilities statement.**
- **Determining the HVTL.**
- **Updating the intelligence estimate.**
- **Any request for information on requests for collection, which are refined and updated.**

SO WHAT?

5-3. The "so what" in this step is enhancing the commander's understanding of the regular, irregular, catastrophic, or disruptive threat/*adversary* force within the commander's area of interest:

- **Success results in threat/*adversary* COAs developed in the next step of IPB to reflect what the threat/*adversary* is capable of and trained to do in similar situations.**
- **Consequences of failure:**
  - **The staff will lack the intelligence needed for planning.**

- **The threat/*adversary* will surprise the friendly force with capabilities that the G-2/S-2 failed to account for.**
- **The staff may waste time and effort planning against threat/*adversary* capabilities that do not exist.**

HOW TO DO IT: (THE PROCESS)

5-4. Step 3 of the IPB process consists of the following actions, which are shown in figure 5-1.

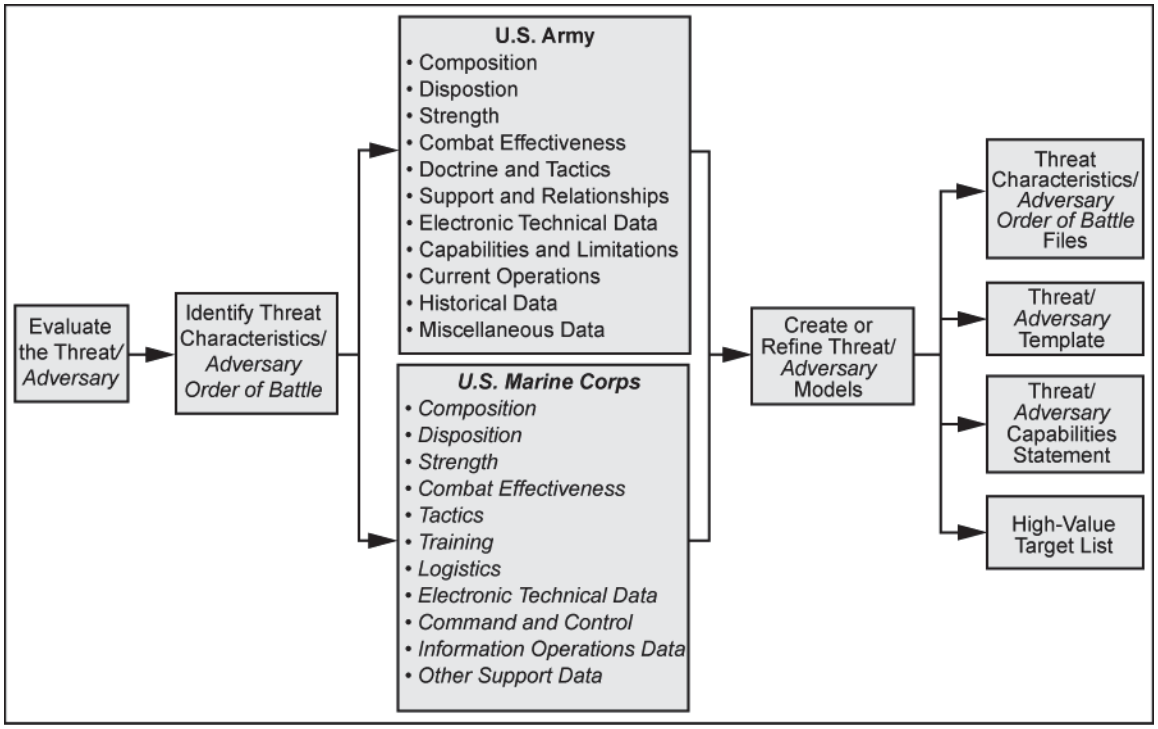


Figure 5-1. Evaluate the threat/*adversary*

5-5. Threats/*adversaries* are a fundamental part of an overall operational environment for any operation but are discussed separately here simply for emphasis. A threat is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADRP 3-0). Threats/*adversaries* may include individuals, groups of individuals (organized or not organized), paramilitary or military forces, nation-states, or national alliances.

5-6. Threats/*adversaries* are generally nation-states, organizations, people, groups, or conditions that can damage or destroy life, vital resources, or institutions. Army/*Marine Corps* doctrine divides these threats/*adversaries* into the following categories: regular, irregular, hybrid, disruptive, catastrophic, and hazards. This publication only discusses the evaluation of regular, irregular, and hybrid threat/*adversary* forces. Evaluating the threat/*adversary* should begin with identifying there is a threat/*adversary*, followed by the analysis of the threat's characteristics/*adversary*'s *order of battle*, and ultimately leading to the identification of the threat/*adversary* model (regular, irregular, or hybrid structure).

- **Regular threats/*adversary* forces are part of nation-states employing recognized military capabilities and forces in understood forms of military competition and conflict. The Islamic Republic of Iran Army and the Peoples Liberation Army of China are examples of regular forces.**
- **Irregular threat/*adversary* forces are an opponent employing unconventional, asymmetric methods and means to counter U.S. advantages. A weaker enemy often uses unconventional methods to exhaust the U.S. collective will through protracted conflict. Unconventional methods include such means as terrorism, insurgency, and guerrilla warfare. Economic, political,**

informational, and cultural initiatives usually accompany and may even be the chief means of irregular attacks on U.S. influence. The Revolutionary Army Forces of Columbia-People's Army and Al Qaeda are examples of irregular forces.

- Hybrid threats/*adversary* forces are the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects.

5-7. The analysis of any enemy force involves understanding that enemy through the de-aggregation of its component parts (threat characteristics/*adversary order of battle*).

5-8. A commander's understanding of the threat/*adversary* is based in part on the intelligence staff's research and analysis on threat/*adversary* characteristics. To ensure this understanding is as complete as possible, the intelligence staff considers the following when assessing these factors:

- Threat characteristics/*adversary order of battle* form a framework for the consistent evaluation of any force.
- The threat characteristics/*adversary order of battle* evaluation framework should be adapted to the mission and a unit's needs.
- Properly maintained files are sources of information on the threat's/*adversary*'s operations, capabilities, and weaknesses.
- Threat characteristics/*adversary order of battle* are analyzed as a whole.

5-9. Although threat/*adversary* forces may conform to some of the fundamental principles of warfare that guide Army/*Marine Corps* operations, these forces all have obvious and subtle differences in how they approach situations and problem solving. Understanding these differences is essential in understanding how a threat/*adversary* force will react in a given situation. (See ADRP 2-0 for additional information on threat capabilities. *See MCWP 2-3 for a discussion on adversary capabilities.*)

IDENTIFY THREAT CHARACTERISTICS/*ADVERSARY ORDER OF BATTLE*

5-10. There are 11 broad areas the intelligence staff considers when analyzing threat characteristics/*adversary order of battle*: composition, disposition, strength, combat effectiveness, doctrine and tactics, support and relationships, electronic technical data, capabilities and limitations, current operations, historical data, and miscellaneous data. (*See MCWP 2-3 for a discussion on adversary order of battle factors such as composition, disposition, strength, tactics, training, logistics, combat effectiveness, electronic technical data, information operations data, and other support data.)*

5-11. During steps 1 and 2 of the IPB process, the intelligence staff identified and defined each individual threat/*adversary* within the commander's area of interest. During step 3, the intelligence staff analyzes the characteristics associated with each of these threats/*adversaries*. The intelligence staff also develops threat/*adversary* models for each of these threats/*adversaries*.

5-12. When operating against a new or emerging threat/*adversary* that is not identified and described in the unit's enemy data files, the intelligence staff has to develop new data files for each of these threats/*adversaries*.

COMPOSITION

5-13. Composition is the identification and organization of a threat/*adversary*. It applies to specific units or commands as opposed to types of units. Regular forces are normally self-identified and organized similar to friendly forces. Irregular forces may follow similar rules but most often are organized based on a cellular structure. Understanding an enemy's composition is—

- Essential in determining its capabilities and limitations.
- Aids in constructing the threat/*adversary* models that help in the development of valid enemy COAs and friendly counteractions.
- Aids in determining an enemy's/*adversary*'s combat effectiveness and in conducting combat assessment.

5-14. Composition describes how an entity is organized and equipped—essentially the number and types of personnel, weapons, and equipment. The staff uses line-and-block chart products to visually see the enemy's composition.

5-15. Composition also refers to how an entity is commanded and controlled. Military forces have distinct and well-defined organizational structures generally built around a linear chain of command. These forces include air and ground forces that, regardless of national origin, generally follow a modern or contemporary military organizational model. Irregular forces also have distinct and well-defined organizational structures generally cellular in nature and directed through a decentralized chain of command usually unique to the area and/or conflict. Regardless of the type of threat/*adversary*, knowing its structure aids in understanding its capabilities and limitations. Figure 5-2 is an example of the organization of a regular threat/*adversary* force. Figure 5-3 is an example of the organization of an irregular threat/*adversary* force.

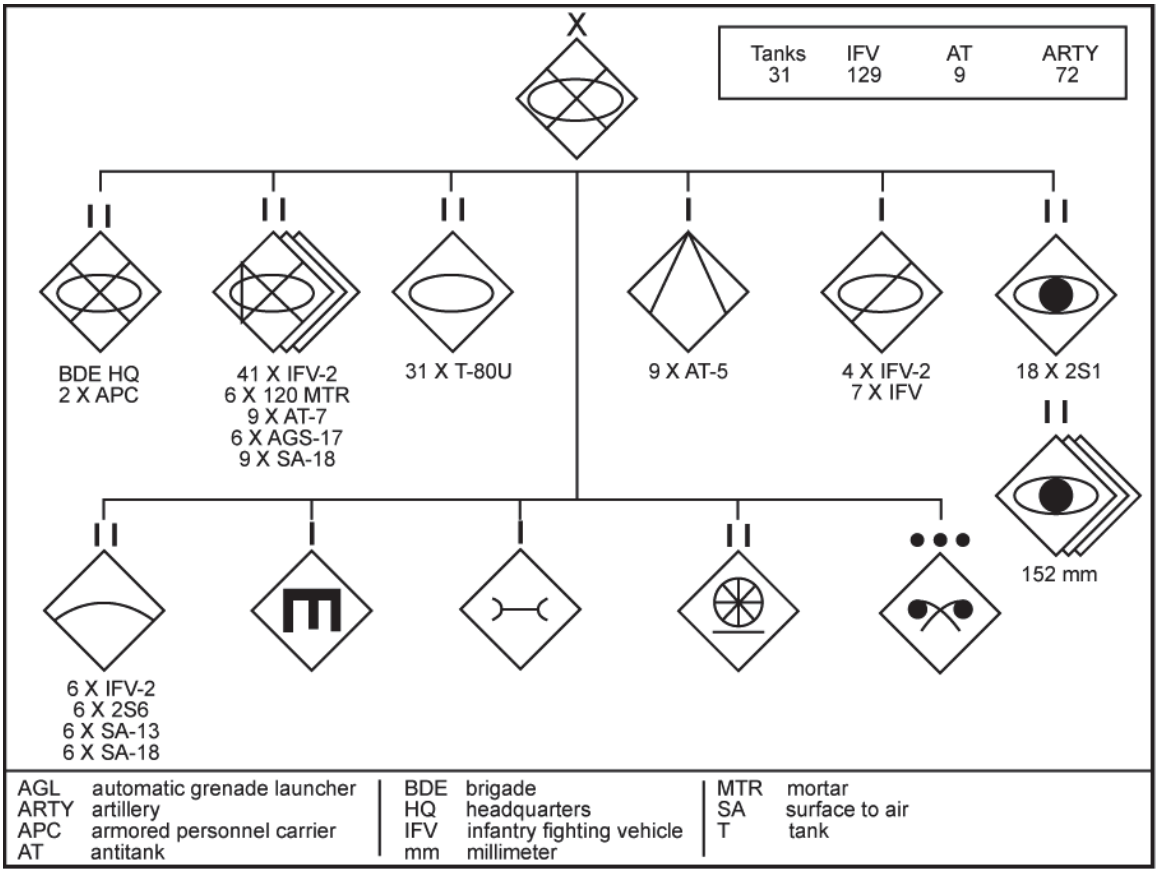


Figure 5-2. Example organizational chart for a regular threat/*adversary* force

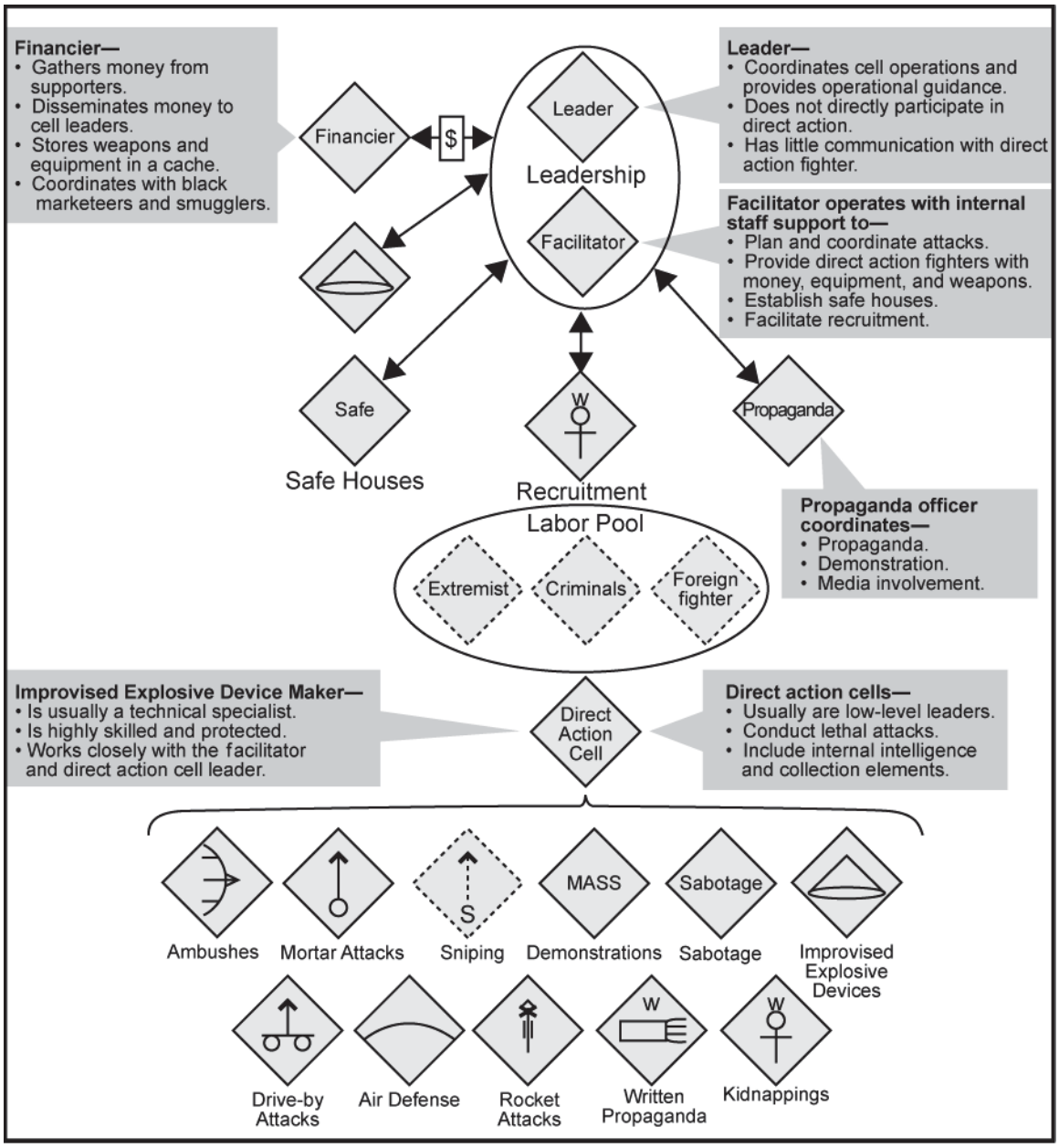


Figure 5-3. Example organizational chart for an irregular threat/*adversary* force

Regular Threat/*Adversary* Forces

5-16. The identity and organization of the regular forces belonging to the world's various nation-states are generally known by the U.S. intelligence community and maintained by the National Ground Intelligence Center. U.S. forces intelligence staffs can access this data as needed to support respective commands. The composition of regular forces is organized around a central command structure. The composition of a regular force is easily communicated though the use of organizational charts that depict the number and types of units in the force as well as the number and types of personnel, weapons systems, and equipment associated with these units.

Irregular Threat/*Adversary* Forces

5-17. Determining composition for irregular threat/*adversary* forces involves the identification of military, political, religious, ethnic, criminal, or terrorist organizations. Unit identification consists of the complete designation of a specific entity by name or number, type, relative size or strength, and subordination. Composition includes—

- **Operational and support cells (similar to sections in a military unit).**
- **Echelons.**
- **Staff elements.**
- **Political, religious, ideological, and military aims.**
- **Internal and external command and control.**
- **Operational organizations.**
- **Internal and external support structure.**
- **External ties.**
- **Assassination squads.**
- **Bomb and demolition squads.**
- **Attack or hit squads.**

5-18. The identity and organization of irregular threat/*adversary* forces is not always known. Irregular threat/*adversary* forces are generally part of an insurgency and are often relatively new organizations. Broadly speaking, there are two kinds of insurgencies: national insurgencies and resistance movements.

- **In a national insurgency, the conflict is between the government and one or more segments of the population. In this type of insurgency, insurgents seek to change the political system, take control of the government, or secede from the country. A national insurgency polarizes the population and is generally a struggle between the government and insurgents for legitimacy and popular support.**
- **In contrast, a resistance movement (sometimes called a liberation insurgency) exists when insurgents seek to expel or overthrow what they consider a foreign or occupation government. The grievance is foreign rule or foreign intervention. Resistance movements tend to unite insurgents with different objectives and motivations. However, such an insurgency can split into competing factions when foreign forces leave and the focus of resistance is gone. That situation may result in a civil war.**

5-19. Irregular forces generally have political objectives and are motivated by an ideology or grievances. These grievances may be real or perceived. Identifying these objectives and motivations can be difficult for a number of reasons:

- **There may be multiple insurgent groups with differing goals and motivations.**
- **Insurgent leaders may change and the movement's goals change with them.**
- **Movement leaders may have different motivations from their followers.**
- **Insurgents may hide their true motivations and make false claims.**
- **The goals of an insurgency may change due to changes in the operational environment.**

5-20. Irregular forces are usually armed military organizations or terrorist groups that have bypassed legitimate political authority and have taken up arms to pursue a common cause. The list at table 5-1, although not all-inclusive, is a description of potential irregular forces.

Table 5-1. Description of potential irregular forces

Type	*Description*
Revolutionary	Organizations involved in a revolution. These forces almost always have a political component that established its goals and objectives.
Guerrilla	Organizations that use unconventional tactics to combat regular forces that have an advantage in size, capability, and support.
Militia	Generally composed of ordinary citizens who have been organized for a specific purpose.
Partisan	General unconventional forces that oppose control of an area by a foreign power or by an Army of occupation by some kind of insurgent activity.
Paramilitary	Usually elements of a regular force using unconventional tactics to combat an occupying regular Army.
Terrorist groups	Organizations that target civilians in order to gain political leverage.
Insurgent organizations	Have no regular table of organization and equipment structure. The mission, environment, geographic factors, and many other variables determine the configuration and composition of each insurgent organization and its subordinate cells. A higher insurgent organization can include organizations at regional, provincial, district, national, or transnational levels. Higher insurgent organizations can contain a mix of local insurgent and guerrilla organizations. Each of these organizations provides differing capabilities.
Mercenaries	Armed individuals who use conflict as a professional trade and service for private gain. Depending on the circumstances, a mercenary may not be a lawful combatant. The term “mercenary” applies to those acting individually and in formed units. Ground forces serving officially in foreign armed forces are not mercenaries. Loan service personnel sent to help train ground forces of other countries as part of an official training agreement between sovereign governments are not mercenaries even if they take a direct part in hostilities.
Criminal organizations	Normally independent of nation-state control. Large-scale criminal organizations often extend beyond national boundaries to operate regionally or worldwide and include a political influence component. Individual criminals or small gangs do not normally have the capability to adversely affect legitimate political, military, and judicial organizations. Large-scale criminal organizations can challenge governmental authority with capabilities and characteristics similar to a paramilitary force. By mutual agreement or when their interests coincide, criminal organizations may become affiliated with other actors, such as insurgents or individuals. They may provide capabilities similar to a primitive Army for hire. Insurgents or guerrillas controlling or operating in the same area as a criminal organization can provide security and protection to the criminal organization’s activities in exchange for financial assistance, intelligence, arms and materiel, or general logistical support.

Hybrid Threat/*Adversary* Forces

5-21. A hybrid threat/*adversary* force is comprised of two or more of the following entities that combine, associate, or affiliate in order to achieve mutually beneficial goals and objectives:

- **A nation-state regular force.**
- **A nation-state irregular force.**
- **Insurgent groups.**
- **Guerilla units.**
- **Criminal organizations.**

5-22. There is no standard organizational structure for a hybrid threat/*adversary* force.

DISPOSITION

5-23. Disposition refers to how threat/*adversary* forces are arrayed on the battlefield/*battlespace*. It includes the recent, current, and projected movements or locations of tactical forces. Regular threat/*adversary* forces are generally conducting some form of offensive or defensive maneuver. Irregular threat/*adversary* forces are generally in some part of the plan, prepare, execute, and assess phases for an operation such as a raid or ambush. Understanding how the threat/*adversary* doctrinally arrays itself on the battlefield/*battlespace* is essential in developing threat/*adversary* models in step 3 of the IPB process and threat/*adversary* situation overlays in step 4 of the IPB process. The intelligence staff familiarizes themselves with graphic training aids that visually depict range fans with weapons' fire limits and direct and indirect weapons capabilities to better understand enemy weapon systems.

Regular Threat/*Adversary* Forces

5-24. When evaluating a regular threat/*adversary* force, disposition refers to geographical location, tactical deployment, and movement of formations. Disposition consists of the location of threat/*adversary* units and the manner in which these units are tactically (or administratively in times of peace) deployed. In addition, disposition includes the recent, current, and proposed (or probable) movements of enemy units.

5-25. Location refers to a geographical area or position occupied by a unit or units. Knowledge of the strength and location of an enemy assists the intelligence staff in determining the capabilities of the force and its effect upon the accomplishment of the friendly mission. Data of this type is collected during peacetime and forms the basis for accessing capabilities during the initial period of hostilities.

5-26. Tactical deployment is the relative position of units with respect to one another or to the terrain. Tactical formations are designed for executing the various tactical maneuvers. If this deployment can be predetermined, it leads to an accurate appraisal of intentions. The knowledge of how enemy units are echeloned may indicate (if the enemy assumes the offensive) which units will be used in the main attack and which units will be used in supporting reserve roles. Tactical deployment with respect to terrain is also important. A study of dispositions and an analysis of the terrain aid the development of conclusions concerning enemy capabilities, vulnerabilities, and intentions.

5-27. Movement of enemy units is also part of disposition. Movement is the physical relocation of a unit from one geographical point to another. Patrol activity may be an indication of planned movement. Movement is significant because it automatically changes the tactical deployment of the enemy forces. When an enemy unit has moved, is moving, or will be moving, there are a number of actions which may affect the situation; for example, a unit may be moving into an attack position, or moving to reinforce or replace a unit, or perform other missions unknown to friendly forces. In view of these possibilities, movement of an enemy unit becomes important and units are monitored at all times in order for the analyst to provide correct and detailed data on enemy dispositions.

5-28. When evaluating a regular enemy force at any point prior to receipt of mission, intelligence staffs will not know the terrain on which either the enemy or friendly force will be operating. Therefore, arraying the enemy on the battlefield/*battlespace* as commonly seen on an enemy situation overlay is not possible. However, it is possible to doctrinally portray how the enemy will array itself on the battlefield/*battlespace* to conduct specific operations. This process is called threat/*adversary* templating, and is part of the threat/*adversary* modeling process. This is an ongoing process that is part of garrison intelligence operations. The threat/*adversary* templates developed here are reexamined and refined during IPB. The development of threat/*adversary* templates is the responsibility of intelligence staffs at any echelon. ***(See figure A-2 on page A-4 for an example of an adversary doctrinal template.)***

Irregular Threat/*Adversary* Forces

5-29. For irregular threat/*adversary* forces, disposition consists of the geographic location of the following elements:

- **Safe houses.**
- **Movement routes.**
- **Training camps.**
- **Base camps.**
- **Logistic bases and resupply points.**

5-30. Additionally, disposition includes the recent, current, and projected movements or locations of tactical forces.

5-31. For the U.S. Army, figure 5-4 on page 5-10 shows an example of a complex battle position for a task-organized guerilla platoon threat model followed by an example scenario. Paragraphs 5-32 through 5-36 apply only to the U.S. Army. ***(For the Marine Corps, see paragraph 5-37 and figure 5-5 on page 5-11.)***

5-32. Complex battle positions typically have the following characteristics that distinguish them from simple battle positions:

- **Limited AAs. (Complex battle positions are not necessarily tied to an AA.)**
- **Any existing AAs are easily observable by the defender.**
- **A 360-degree fire coverage and protection from attack. (This may be due to the nature of surrounding terrain or engineer activity such as tunneling.)**
- **Engineer effort prioritizing camouflage, concealment, cover, and deception measures; limited countermobility effort that might reveal the complex battle position location.**
- **Large logistics caches.**
- **Sanctuary from which to launch local attacks.**

5-33. Leaders of a unit, cell, or organization occupying complex battle positions intend to preserve their combat power until conditions permit offensive action. The threat defending in complex battle positions will use restrictive terrain and engineer countermobility efforts to deny the enemy the ability to approach, seize, and occupy the position. They will also make maximum use of camouflage, concealment, cover, and deception and cultural standoff to deny the enemy the ability to detect and attack the position.

5-34. Complex battle position defenders typically engage only as long as they perceive an ability to defeat the enemy. Should the defending complex battle position leaders evaluate that their forces are about to be decisively engaged, they will attempt a withdrawal or a withdrawal under pressure in order to preserve combat power.

5-35. Depending on the size and capabilities of an irregular force, functions can be allocated to disruption, main defense, support, and a reserve. Reconnaissance and other security measures are a constant activity to observe AAs near a complex battle position in order to provide early warning to the threat leader.

5-36. Information warfare elements of the complex battle position maintain situational awareness and understanding of local conditions with relevant populations as integral to threat reconnaissance, intelligence, surveillance, and target acquisition tasks. Generally, the complex battle position will not have easily detectable information warfare activities.

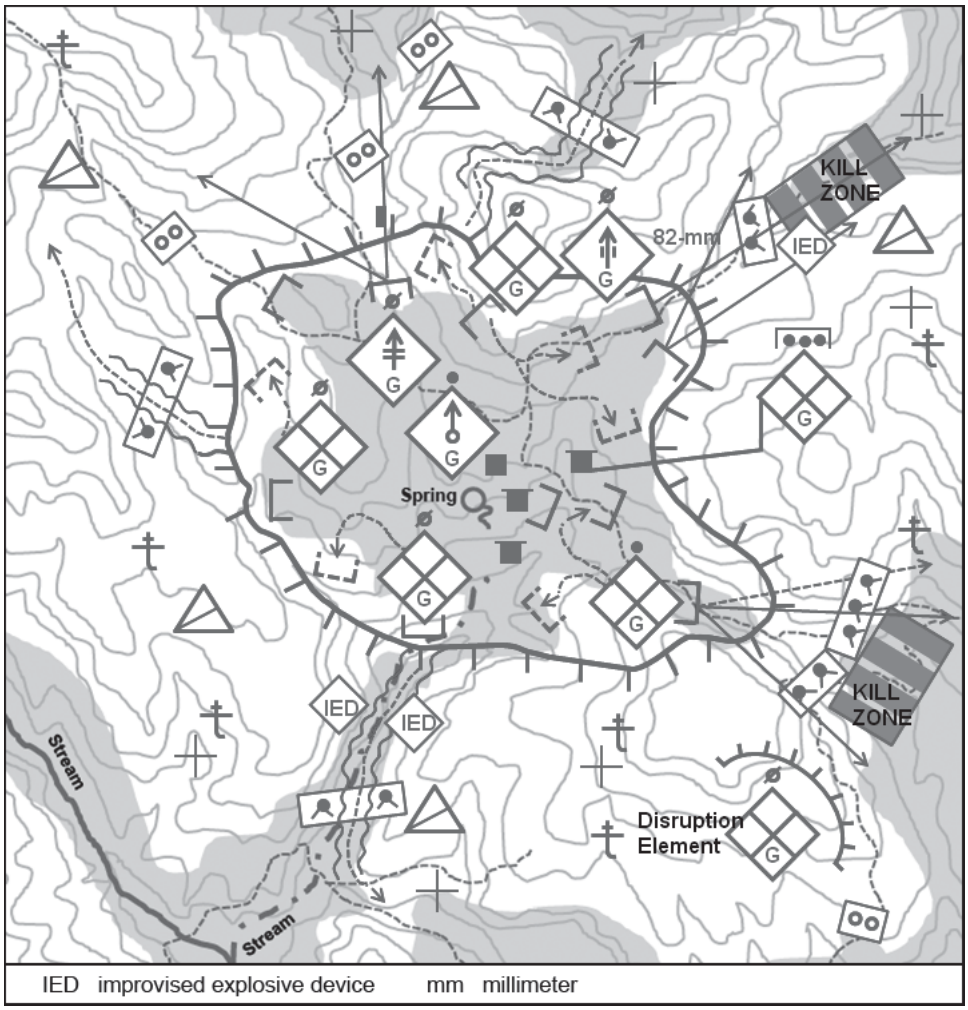


Figure 5-4. U.S. Army example of a complex battle position for a task-organized guerilla platoon threat model

Example

The guerilla platoon occupies a complex battle position as a defensive location designed to employ a combination of complex terrain; camouflage, concealment, cover, and deception; and engineer effort to protect the unit from detection and attack while denying their seizure and occupation by the enemy. A simple battle position differs from a complex battle position in that a simple battle position is a defensive location oriented on the most likely enemy AA and is not necessarily tied to complex terrain. (See TC 7-100.2, paragraphs 4-106, 4-108, and 4-145 to 4-171, for more information on battle positions.)

5-37. ***For the Marine Corps, figure 5-5 shows an example of a Marine Corps doctrinal template for an irregular adversary.***

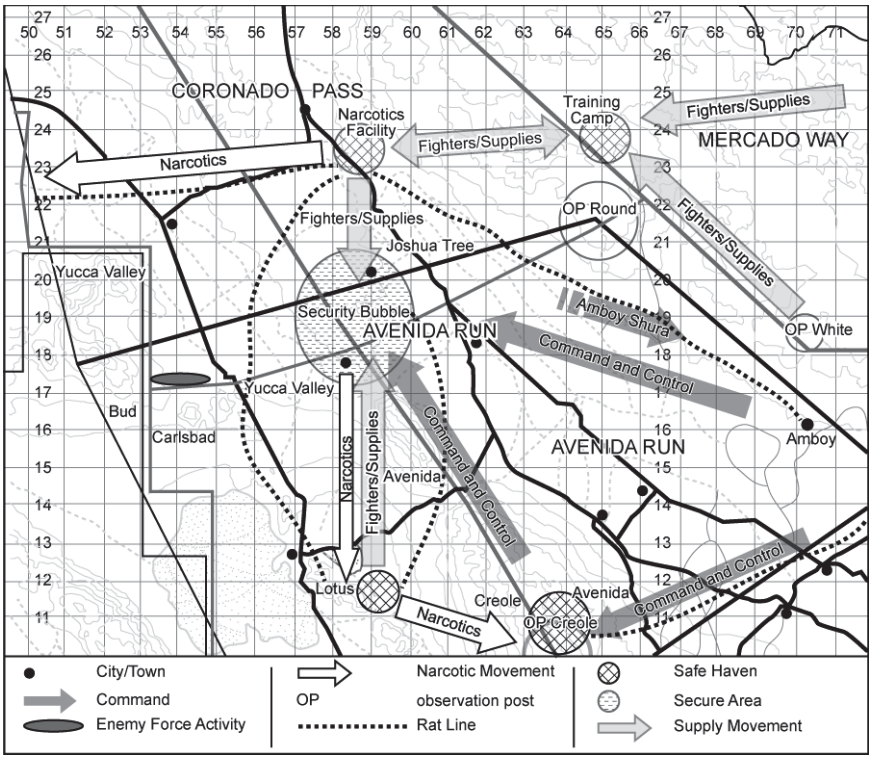


Figure 5-5. ***Example of a Marine Corps doctrinal template for an irregular adversary***

5-38. Figure 5-6 is an example of an integrated attack by a task-organized guerilla battalion threat/*adversary* model.

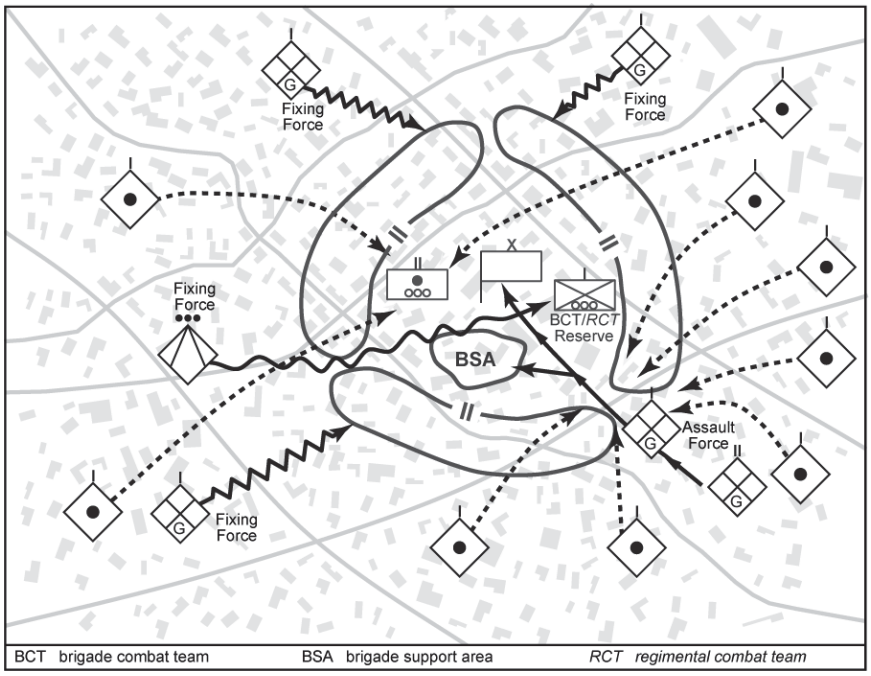


Figure 5-6. Example of an integrated attack by task-organized guerilla battalion threat/*adversary* model

Hybrid Threat/*Adversary* Forces

5-39. There are no threat/*adversary* force models or templates currently developed for specific hybrid threats/*adversary* forces. However, TC 7-100 includes some basic attack and/or defends hybrid force scenarios designed to support exercise design. These scenarios, along with focused research on real-world threat/*adversary* activity, can aid in developing threat/*adversary* templates.

STRENGTH

5-40. Strength describes a unit in terms of personnel, weapons, and equipment. Information concerning strength provides the commander with an indication of enemy capabilities and helps determine the probable COAs or options open to threat/*adversary* commanders. A lack of strength or a preponderance of strength has the effect of lowering or raising the estimate of the capabilities of an enemy force. Likewise, a marked concentration or build-up of units in an area gives the commander certain indications of enemy objectives and probable COAs. During peacetime, changes in the strength of potential threat/*adversary* forces are important factors which may indicate changes in the threat's/*adversary*'s intention. Strength is determined by comparing how a threat/*adversary* organization is doctrinally staffed and equipped with what the organization actually has on hand.

Regular Threat/*Adversary* Forces

5-41. Strength for regular forces is described in terms of personnel, weapons, and equipment. The most important aspect of strength when evaluating a regular force is to determine whether the force has the capability of conducting specific operations. For example, a unit may have adequate weapons systems to conduct an operation, but may not have a sufficient number of trained personnel or crews to man the systems.

Irregular Threat/*Adversary* Forces

5-42. For irregular forces, strength is defined by the capability of direct action teams, political cadre or cells, and, most importantly, popular support. Popular support can range from sympathizers to assistance in conducting operations, storage or moving, logistics, or just withholding information.

Hybrid Threat/*Adversary* Forces

5-43. The strength of a hybrid threat/*adversary* force is determined by understanding the synergy of regular and irregular forces. The hybrid threat/*adversary* force understands that the environment that would produce the most challenges to U.S. forces is one in which conventional military operations occur in concert with unconventional warfare. The hybrid threat/*adversary* force concept is not just one of making do with what is available, but is primarily one of deliberately created complexity.

5-44. Each component of the hybrid threat/*adversary* force brings a capability to bear. The synergy of these capabilities is not to be understated. Operational environments by their very nature provide a myriad of complexities based on their characteristics. The hybrid threat/*adversary* force seeks to introduce additional complexity through the use of an ever-shifting array of forces, technologies, and techniques.

COMBAT EFFECTIVENESS

5-45. Combat effectiveness describes the abilities and fighting quality of a unit. Numerous tangible and intangible factors affect it.

Regular Threats/*Adversary* Forces

5-46. Determining combat effectiveness for regular threat/*adversary* forces is made by assessing the following factors:

- **Personnel strength.**
- **Amount and condition of weapons and equipment.**
- **Status of training.**
- **Efficiency of leadership.**
- **Quality of leadership.**
- **Length of time a unit is committed in combat.**
- **Traditions and past performance.**
- **Personality traits of the unit commanders.**
- **Geographical area in which committed.**
- **Morale, spirit, health, nutrition, discipline, and political reliability (or belief in the cause for which they fight).**
- **Status of technical and logistical support of the unit.**
- **Adequacy of military schooling at all levels.**
- **National characteristics of the people.**

Irregular Threat/*Adversary* Forces

5-47. Combat effectiveness for irregular threat/*adversary* forces is measured differently from combat effectiveness for regular threat/*adversary* forces. The threat/*adversary* is motivated by many factors, which can be, but are not limited to, a goal of independence, equality, religion or ideology, occupation of a foreign nation, or economical. Combat effectiveness is determined by, but not limited to—

- **External support (financial, physical, moral, propaganda). Often threats/*adversaries* are interconnected to other transnational groups, organizations, or governments. Irregular threats/*adversaries* may be dependent on this external support. External support can noticeably increase the significance of irregular threats/*adversaries*. They can establish financial resources (cash, commodities, services of value legally or illegally) to fund operations. The intended use of these resources lends those funds greater significance than their inherent value.**
- **Fear and intimidation. Threats/*adversaries* use attacks on civilians or elements of the civilian population (murder, kidnapping, extortion) and attacks on U.S. forces and host-nation governmental or political organizations, businesses, civil, critical infrastructures, and security organizations. Irregular threats/*adversaries* also use the threat/*adversary* of ambushes, improvised explosive devices (IEDs), raids, sabotage, terror, and violence. Without a stable environment, the power of intimidation on the local population is significant.**
- **Political change. Threats/*adversaries* act as a political entity in a vacuum and claim to be able to fix real or perceived political issues. Irregular threats/*adversaries* use persuasion and coercion to reinforce their political means. They conduct propaganda activities to target the population and international public opinion. These activities may enhance the threat's/*adversary*'s legitimacy and undermine that of the host nation.**
- **Popular support. Threats/*adversaries* use coerced or uncoerced cooperation of the general population. Armed groups involved in insurgent operations directed against the host-nation government draw their strength from the population or at least a segment of the population. These groups establish sanctuary locations among segments of the population and utilize civilian transportation, communications, financial services, and general services to sustain operations. They receive funding by winning the approval of segments of the population or by extorting and utilizing segments of the population to provide indications and warnings of U.S. operations.**

Hybrid Threat/*Adversary* Forces

5-48. Determining the combat effectiveness for hybrid threat/*adversary* forces is made by considering the tangible and intangible factors associated with determining the combat effectiveness for regular and irregular threat/*adversary* forces.

DOCTRINE AND TACTICS

5-49. Doctrine and tactics include tactical doctrine as well as tactics employed by specific units. While tactical doctrine refers to the enemy's accepted organization and employment principles, tactics refer to the threat/*adversary* force's conduct of operations. Based on knowledge of a threat's/*adversary's* tactical doctrine, the intelligence staff can determine how the threat/*adversary* force may employ its forces in the offense and defense under various conditions. Analysts integrate tactics in threat/*adversary* templates and other intelligence products. *Identify the adversary force's possible actions (defend, reinforce, attack, withdraw, delay [DRAW-D]).*

Regular Threat/*Adversary* Forces

5-50. Doctrine and tactics for regular threat/*adversary* force refer to the TTP that guide threat/*adversary* force operations. Understanding how the threat/*adversary* force prefers to operate aids the commander's understanding of potential threat/*adversary* COAs. TTP for regular threat/*adversary* forces can generally be grouped in the following categories:

- **Offensive tasks.**
- **Movement to contact.**
- **Attack.**
- **Exploitation.**
- **Pursuit.**
- **Defensive tasks.**
- **Area defense.**
- **Mobile defense.**
- **Retrograde.**

Irregular Threat/*Adversary* Forces

5-51. Tactics and operations for irregular forces include strategy, methods of procedure, and doctrine. Each refers to the threat/*adversary* force's accepted principles of organization and employment of forces. Tactics also involve political, military, psychological, and economic considerations. Irregular force tactics and operations vary in sophistication according to the level of training the individual or organization has received. Irregular forces carefully plan and train for individual and small-group operations. (See FM 3-24/*MCWP 3-33.5* for more information on potential irregular force tactics and operations.)

Hybrid Threat/*Adversary* Forces

5-52. Threats/*adversaries* to the U.S. and its allies employ hybrid forces as part of a sophisticated, comprehensive, and multidimensional strategy to achieve specific goals and objectives. The doctrine and tactics that guide hybrid forces are similar to Army/*Marine Corps* doctrine and tactics in that strategic, operational, and tactical action are coordinated to achieve objectives and end state.

5-53. Hybrid force doctrine is based on countering a threat's/*adversary*'s capabilities. Hybrid forces often study U.S. and allied military forces and their operations and conduct lessons learned based on their assessments and perceptions.

5-54. Hybrid forces use nations that they see as threats/*adversaries* as baselines for planning adaptive approaches for dealing with the strengths and weaknesses of their forces. These forces use the following principles for applying their various instruments of diplomatic political, informational, economic, and military power:

- **Access limitation.**
- **Control tempo.**
- **Cause politically unacceptable casualties.**
- **Neutralize technological overmatch.**
- ***Conduct information operations aimed at local population, international opinion, and their adversaries' domestic population.***
- **Change the nature of conflict.**
- **Allow no sanctuary.**
- **Employ operational exclusion.**
- **Employ operational shielding.**
- **Avoid defeat.**

SUPPORT AND RELATIONSHIPS

5-55. The threat/*adversary* force's adoption of a COA should depend on the ability of its support system to support that action. However, depending on the threat/*adversary* force's objectives, possible time constraints, and/or willingness to assume risk—especially as dictated by political leaders or dynamics of political-military circumstances—this could substantially alter adoption of a COA. With knowledge of these factors, analysts can better evaluate the threat/*adversary* force capabilities, strength, and combat effectiveness.

Regular Threat/*Adversary* Forces

5-56. The location of a regular threat/*adversary* force's logistical support structure elements aids intelligence staffs in determining the disposition of maneuver formations. Logistic information critical for effective intelligence analysis includes—

- **Classes and types of supply.**
- **LOCs.**
- **Logistical requirements.**
- **Procurement methods.**
- **Distribution priorities and procedures.**
- **Transportation networks and modes.**
- **Installations and terminals.**
- **Damaged equipment evacuation and salvage procedures.**
- **Maintenance.**

Irregular Threat/*Adversary* Forces

5-57. The effectiveness of unconventional warfare depends heavily on support and relationships. This dependency fluctuates horizontally and vertically between the various groups and levels of operation. The intensity of support activity is based on operations. Critical components of support include, but are not limited to—

- **Financing.**
- **Food.**
- **Water.**
- **Weapons and ammunition.**
- **Bombmaking components.**
- **Military information support operations materials (paper, ink, printing press).**
- **Medical.**
- **Transportation.**
- **Support of the population.**

Hybrid Threat/*Adversary* Forces

5-58. Hybrid forces will incorporate the types of support irregular forces use to sustain themselves with the traditional logistical support associated with conventional military operations.

5-59. Because a hybrid force is a composite of many different groups, these groups will often have no standard, readily identifiable organizational relationship. What brings together the capabilities and intent of the components of the hybrid threat/*adversary* is a common purpose, typically opposition to U.S. goals. This unity of purpose can even bring together groups that normally would be fighting among themselves.

5-60. Affiliated organizations are cooperating toward a common goal despite having no formal command or organizational relationship. Affiliated organizations are typically nonmilitary or paramilitary groups, such as criminal cartels, insurgencies, terrorist cells, or mercenaries.

5-61. Affiliated forces are those irregular forces operating in a military unit's AO that the unit may be able to sufficiently influence to act in concert with it for a limited time. No "command relationship" exists between an affiliated organization and the unit in whose AO it operates. In some cases, affiliated forces may receive support from the military unit as part of the agreement under which they cooperate.

ELECTRONIC TECHNICAL DATA

5-62. Electronic technical data derived from targeting and electronic warfare are required to conduct electronic warfare. For U.S. Army, it is also derived from cyber electromagnetic activities. This data includes communications and noncommunications equipment parameters, such as emitter type and nomenclature, modulation, multiplex capability, pulse duration, pulse repetition frequency, bandwidth, associated weapons systems, and other technical characteristics of electronic emissions. This information can be developed into an overlay. In order to produce the overlay, signal intelligence personnel require the assistance and input of the targeting and electronic warfare staff. (For U.S. Army, they also obtain assistance from the cyber electromagnetic activities element.)

Regular Threat/*Adversary* Forces

5-63. For regular threat/*adversary* forces, this data also includes critical threat/*adversary* communications nodes such as command posts and logistical control points. This information supports threat/*adversary* templating. With electronic technical data, a more accurate evaluation of the enemy's vulnerability to electronic countermeasures and deception is made; signals intercept and direction finding for the production of signals intelligence is made easier; and support is given to counter threat electronic warfare by assessing the threat's/*adversary's* electronic warfare capabilities.

Irregular Threat/*Adversary* Forces

5-64. When combating irregular threat/*adversary* forces, the lack of an obvious formal organizational structure or architecture impedes development of an extensive threat/*adversary* communications network diagrams and electronic technical database. The insurgent has communications equipment available ranging from the most modern to the most primitive. Insurgent forces can use high frequency, short-wave, ham radio and Citizen band sets; cellular phones, satellite phones, the Internet, mail, and couriers. While not playing a significant historical role, the insurgent's potential use of radar cannot be ruled out.

Hybrid Threat/*Adversary* Forces

5-65. Hybrid enemy forces will employ a combination of the capabilities used by regular and irregular forces as well as available commercial-off-the-shelf technology and existing civilian communications networks.

CAPABILITIES AND LIMITATIONS

5-66. Capabilities are the broad COAs and supporting operations that the enemy can take to achieve its goals and objectives. The following four tactical COAs are generally open to military forces in conventional operations: attack, defend, reinforce, retrograde/*DRAW-D*.

5-67. Each of these broad COAs can be divided into more specific COAs. An attack may be envelopment, penetration, or other variations of an attack. A retrograde movement may be a delaying action, a withdrawal, or a retirement. Other threat/*adversary* force capabilities include support to broad COAs or specific types of operations, including—

- **Deception operations.**
- **Military information support operations.**
- **Intelligence operations.**
- **CBRN employment.**
- **Espionage, sabotage, subversion, and terrorist operations.**

5-68. Threat/*adversary* capabilities take the form of statements, such as—

- **The threat/*adversary* has the ability to insert up to two infantry battalions in a single lift operation.**
- **The threat/*adversary* can establish a prepared defense by 14 May.**
- **The demonstrators can effectively block traffic at up to seven intersections in the AO.**

5-69. When identifying threat/*adversary* capabilities, intelligence staffs—

- **Start with developed threat/*adversary* models.**
- **Consider the threat/*adversary* ability to conduct each operation based on all factors related to the current situation. (The enemy may be under-strength in equipment or personnel, short of logistic support, lacking air support, or the enemy's troops may be inexperienced or poorly trained.)**

Regular Threat/*Adversary* Forces

5-70. A regular threat/*adversary* force is designed to attack or defend as necessary to accomplish objectives. Determining capabilities and limitations for a regular threat/*adversary* force requires an understanding of the art and science of war, as well as an understanding of the threat/*adversary* force itself.

Irregular Threat/*Adversary* Forces

5-71. The most challenging capability of an irregular threat/*adversary* is its ability to blend in with the population or to hide in complex terrain. This allows the threat/*adversary* to plan and prepare for an operation and attack at a time and place of its own choosing without interference from friendly forces.

Hybrid Theat/*Adversary* Forces

5-72. From a friendly perspective, the most challenging capability of a hybrid force is its ability to adapt and transition. The hybrid force emphasizes speed, agility, versatility, and changeability as the keys to success in a fight against a larger, more powerful opponent.

Adaptation

5-73. Adaptation, broadly defined, is the ability to adjust behaviors based on learning. Adaptation is closely linked to the operational environment and its variables. Threat/a*dversary* forces approach adaptation from two perspectives: natural and directed.

- **Natural adaptation occurs as an actor (nation-state or non-state) acquires or refines its ability to apply its political, economic, military, or informational power. Natural adaptation can be advanced through acquisition of technology, key capabilities, or resources (financial and material), effective organization, effective use of the information environment, or even key regional or global alliances.**
- **Directed adaptation refers to adaptation, based specifically on lessons learned, to counter U.S. power and influence. Counters to U.S. actions will be ever-changing and likely conducted by a hybrid force. Hybrid forces will offer a mix of capabilities along the range of military operations to counter U.S. military actions. Adversaries will learn from U.S. operations what works and what needs refinement. They will be whatever the U.S. force is not. Like natural adaptation, directed adaptation will inform issues of force design, military strategy, and operational designs.**

Transitions

5-74. One of the most dangerous aspects of a hybrid force is the ability of its components to transition in and out of various forms. Military forces, for example, can remove uniforms and insignia and other indicators of status and blend in with the local population. Insurgent forces might abandon weapons and protest innocence of wrongdoing. Criminals might impersonate local police forces in order to gain access to a key facility.

5-75. Hybrid forces will use the difficulties of positive identification of threat/*adversary* actors as threat/*adversary* actors to their advantage. Operational environments will be replete with many actors conducting activities counter to U.S. interests but without a clear visual signature as to their status as threats/*adversaries*. Indeed, often these actors will be providing signatures similar to friendly or neutral actors.

5-76. These concepts of conventional and unconventional warfare and traditional versus adaptive methods are weapons to a hybrid force. These concepts do not have meaning to hybrid forces beyond their ability to be used against their opponents. Hybrid forces see war holistically and do not try to break it up into convenient pieces. Hybrid forces will need to perform certain functions in order for them to succeed. Some functions at some points will best be performed by uniformed military forces. At other times or for other reasons, some functions will be best performed by irregular forces. At some points, both types of forces will be acting together. At others, they will shift between the status of regular and irregular. They may also use deception to shift between combatant and noncombatant status. Hybrid forces will present themselves in many ways but maintain the ability to aggregate at the time and place of their choosing.

CURRENT OPERATIONS

5-77. Current operations are those operations in which an enemy force is currently engaged. This includes operations against U.S. military forces or interests or against the military forces or interests of other nation-states. Analyzing current operations provides up-to-date information on all other threat/*adversary* characteristics.

Regular Threat/*Adversary* Forces

5-78. The Army's/*Marine Corps'* knowledge of regular threat/*adversary* forces is based on its understanding of these forces prior to 11 September 2001 (hereinafter referred to as 9/11). These forces have evolved as the Army/*Marine Corps* has evolved. Intelligence staffs at all echelons continuously study these forces to gain a better understanding of them.

Irregular Threat/*Adversary* Forces

5-79. The Army/*Marine Corps* gained valuable experience in combating irregular forces during Operation Iraqi Freedom and Operation Enduring Freedom. Thus, the Army/*Marine Corps* has learned how diverse and adaptive these threats/*adversaries* can be. It is unlikely that the irregular threats/*adversaries* the Army/*Marine Corps* will face in the future will mirror those it fought in Iraq and Afghanistan. To gain the best understanding of the evolving nature of irregular threats/*adversaries* throughout the world, intelligence staffs analyze these threats/*adversaries* whenever and wherever they appear.

Hybrid Threat/*Adversary* Forces

5-80. Although the Army/*Marine Corps* believes the primary threat/*adversary* it will face in the future will come from hybrid threat/*adversary* forces, little is known about what the character of these threats/*adversaries* will be. Although the Army/*Marine Corps* has developed a hybrid threat/*adversary* force model to use in training combined arms teams, this model provides only limited value in preparing the intelligence staff in understanding this threat/*adversary*. This is because, like the previous contemporary operational environment threat/*adversary* model, it is a generic construct that does not reflect the threat characteristics/*adversary order of battle* of any particular real-world threat/*adversary*. Because of this, it is incumbent upon intelligence staffs at all levels to study these types of threats/*adversaries* wherever they are operating in order to continually increase understanding of this threat/*adversary* category. The intelligence staff also studies historical examples of hybrid threat/*adversary* operations.

HISTORICAL DATA

5-81. Compiling the history of any threat/*adversary* organization involves conducting the research necessary to gather all relevant information regarding the threat/*adversary* and producing the materials needed to communicate that information to the commander and staff. Information briefings and papers are the two most common methods used for this purpose. Both of these methods can be used to support intelligence training, officer professional development, and noncommissioned officer professional development. The history component of the threat/*adversary* data file includes the original sources of information used to compile information briefings and papers. These sources form part of the professional reading required by all of the unit's intelligence personnel.

Regular Threat/*Adversary* Forces

5-82. Regular threat/*adversary* forces develop attributes based on how it has been employed over time and on how it conducted itself during that employment. While not definitive, understanding a unit's lineage can provide insight into the extent a unit will go in order to accomplish its objectives. This also provides insight into what the unit will not do to accomplish its objectives.

Irregular Threat/*Adversary* Forces

5-83. Irregular threat/*adversary* forces also develop attributes based on how it has been employed over time and on how it conducted itself during that employment.

Hybrid Threat/*Adversary* Forces

5-84. The historical record of the operations and activities of hybrid threats/*adversaries* will be one of the results of the analysis of current operations. However, history does provide examples of threat/*adversary* forces using hybrid approaches against a superior force.

Historical Examples of Hybrid Approaches

- 1754 to 1763—Regular British and French forces fought each other amidst irregular Colonialists fighting for the British and American Indians fighting for both sides.
- 1814—Peninsular War ended after the combination of regular and irregular multinational forces from Britain, Portugal, and Spain prevented France from controlling the Iberian Peninsula.
- 1954 to 1976—Viet Cong and People's Army of Vietnam combined irregular and regular forces in fighting the French and U.S. forces. Viet Cong would organize into conventional and unconventional units.
- 2006—Hezbollah mixed conventional capabilities (such as anti-armor weapons, rockets, and command and control networks) with irregular tactics (including information operations, non-uniformed combatants, and civilian shielding). The result was a tactical stalemate and strategic setback for Israel.

MISCELLANEOUS DATA

5-85. Intelligence staffs use supporting information to develop threat/*adversary* force characteristics and to construct comprehensive intelligence estimates. This information includes biographic data, personalities, and biometric data, as well as other information important to mission accomplishment. Biographic data contains information on characteristics and attributes of a threat/*adversary* force's members. Knowledge of personalities is important in identifying units and, in some cases, predicting a unit's COA. Personality data is valuable because the tactics and combat efficiency of particular units are closely tied to the commander's character, schooling, and personality traits. In counterinsurgency operations, supporting data may include tribal, clan, or ethnic group traits and their effects on the combat capabilities or limitations of the threat/*adversary* force, as well as biometric data.

5-86. ***Operations in Iraq and Afghanistan have seen an extensive use of biometric and forensic collection to support counterinsurgency operations. This collection was used to establish the identity, affiliations, and authorizations of an individual, deny anonymity to the adversary, and protect friendly assets, facilities, and forces. Valuable intelligence can and has been gleaned from identity operations. Known as identity intelligence, it is the collection, analysis, protection, exploitation, and management of identity attributes and associated technologies and processes in order to locate, track, and maintain continuity on identities across multiple or disparate instances and/or incidents, or across space and time. Future conflicts will likely involve an adversary who will seek to blend into a civilian populace. Intelligence Marines should seek to deny anonymity to the adversary by directing focused biometric and forensic collections and incorporating identity intelligence into the IPB process.***

Regular Threat/*Adversary* Forces

5-87. When evaluating regular forces, miscellaneous data includes biographic data on the commander's and other key leaders in the organization. When combined with the other threat/*adversary* characteristics, this information may provide insight on how an enemy commander may react in a particular situation or attempt to solve a particular problem.

Irregular Threat/*Adversary* Forces

5-88. When evaluating irregular threat/*adversary* forces, miscellaneous data includes information on personalities, culture, and internal organizational processes.

Personalities

5-89. Personality is an important factor, and sometimes it is critical especially when combating irregular forces. Analysts focus on leaders and other important individuals. Personality files help the analyst conduct this analysis. Personality files include, but are not limited to—

- **Leaders (political, ideological, religious, military, other).**
- **Staff members.**
- **Spokespeople.**
- **Family members (immediate and extended).**
- **Previous experience and skill training in professional disciplines, trades, and specialties.**
- **Media manipulation personnel.**
- **Trainers.**
- **Code names and nicknames.**

5-90. Analysts use these personality files to help conduct link analysis and build organizational diagrams to determine relationships between critical personalities and their associations to various groups or activities. When combating irregular forces, this task is often known as "network analysis." This thorough analysis is critical to help determine the roles and relationships of many different people and organizations and to assess their loyalties, political significance, and interests. It is important to remember that any relationship or organization can span across illegal, terrorist, and other threat/*adversary* as well as legitimate people, money, and activities.

Culture

5-91. Culture is the ideology of a people or region and defines a people's way of life. A people's culture is reflected in daily manners and customs. Culture outlines the existing systems of practical ethics, defines what constitutes good and evil, articulates the structures and disciplines that direct daily life, and provides direction to establish patterns of thinking and behavior. Cultural issues include, but are not limited to, the following:

- **Religion—beliefs, customs, and protocols.**
- **Political and economic beliefs—ideology and work ethic.**
- **Tribe—family allegiances and loyalties; family economic interests; and matriarchies versus patriarchies.**

- **Clan—caste, class, social group, standing, status, hierarchies.**
- **Ethnicity—race, nationality (for example, Arab, Bedouin, and Turkic; Kurd and Armenian; Tibetan, Korean, Mongolian, and Chinese).**
- **Regional affiliations—internal to a nation and those that extend past national borders.**
- **Military attitudes—order, weapons, honor.**
- **Law and justice—one system of law or multiple systems; property rights; and correction versus punishment.**

Internal Organizational Processes

5-92. An organization's flexibility or rigidity is a key determinant as to its strengths and vulnerabilities. This flexibility or rigidity can be accurately estimated by answering several questions:

- **Are achievers viewed as potential competitors, or as important organizational contributors? Is the attitude consistent throughout the organization?**
- **How do organizations replace leader and cadre casualties? What are the primary factors that determine how these replacements are selected?**
- **Rewards and punishments: what are they and are they consistently applied?**
- **Are internal rivalries complex, or does organizational discipline have primacy?**
- **How are policies adjusted and adjudicated: gunfights or dialogue?**
- **What are potential divisions and policy fractures?**
- **Which leaders support specific positions, and why?**
- **Are leader motivations organizational, family, or personal?**

Hybrid Threat/*Adversary* Forces

5-93. The miscellaneous data associated with hybrid threat characteristics/*adversary order of battle* are a combination of that required for regular and irregular forces.

CREATE OR REFINE THREAT/*ADVERSARY* MODELS

5-94. Threat/*adversary* models accurately portray how threat/*adversary* forces normally execute operations and how they have reacted to similar situations in the past. This also includes knowledge of threat/*adversary* capabilities based on the current situation. Threat/*adversary* models are initially created by analyzing information contained in various databases. Some threat/*adversary* models are created and developed by higher agencies and organizations; but in immature operational environments or when a new threat/*adversary* emerges, analysts have to develop threat/*adversary* models.

5-95. A threat/*adversary* model is a three-part analytical work aid designed to assist in the development of situation templates during step 4 of the IPB process. Threat/*adversary* models consist of three parts:

- **Convert threat/*adversary* doctrine or patterns of operation to graphics.**
- **Describe the threat's/*adversary*'s tactics and options.**
- **Identify HVTs.**

CONVERT THREAT/*ADVERSARY* DOCTRINE OR PATTERNS OF OPERATION TO GRAPHICS

5-96. Threat/a*dversary* templates graphically portray how the threat/*adversary* might utilize its capabilities to perform the functions required to accomplish its objectives. Threat/a*dversary* templates are scaled to depict the threat's/*adversary*'s disposition and actions for a particular type of operation (for example, offense, defense, insurgent ambush, or terrorist kidnapping operation). When possible, templates should be depicted graphically as an overlay, on a supporting system or through some other means. Threat/a*dversary* templates are tailored to the needs of the unit or staff creating them. They may depict, but are not limited to, unit frontages, unit depths, boundaries, engagement areas, and obstacles.

5-97. The analyst constructs threat/*adversary* templates through an analysis of the intelligence database and an evaluation of the threat's/*adversary*'s past operations. The analyst also determines how the

threat/*adversary* normally organizes for combat and how threats/*adversaries* deploy and employ their forces and assets. In addition, the analyst looks for patterns in how the threats/*adversaries* organize their forces, timing, distances, relative locations, groupings, or use of the terrain and weather.

5-98. Templating requires continuous refinement to accurately portray threat/*adversary* patterns and practices. For example, while there may be no threat/*adversary* template for emplacement of kidnapping cells or money-laundering activities, evaluating the database can indicate specific patterns of kidnapping and money laundering. Because the implementation time is a consistent planning factor, an analyst can use the implementation time evaluation to determine the likelihood of location or participants.

5-99. Threat/a*dversary* templates are tailored to the needs of the unit or staff section creating them. A G-2 section's threat/*adversary* template will differ in scope from the template created by a brigade/*unit* S-2 section. Some threat/*adversary* templates consider the threat/*adversary* forces as a whole, while others focus on a single warfighting function, such as intelligence or fire support, while other products depict pattern analysis, time event charts, and association matrices.

DESCRIBE THE THREAT'S/*ADVERSARY*'S TACTICS AND OPTIONS

5-100. The threat/*adversary* model includes a description of the threat's/*adversary*'s preferred tactics. A description is still needed even if the threat/*adversary* has preferred tactics are depicted in a graphic form. The description—

- Lists the options available to the threat/*adversary* should the operation fail or succeed.
- Prevents the threat/*adversary* model from becoming more than a "snapshot in time" of the operation being depicted.
- Aids in mentally wargaming the operation over its duration and during the development of threat/*adversary* COAs and situation templates.
- Addresses typical timelines and phases of operation, points where unit's transition from one form of maneuver to the next and how each warfighting function contributes to the success of the operation.

5-101. The analyst describes the actions of the supporting warfighting function in enough detail to allow for identification and development of HVTs. The analyst also examines each phase separately because target values may change from phase to phase.

5-102. The analyst describes and makes a determination of what goal or goals the threat/*adversary* is trying to achieve. Threat/*adversary* objectives are often, but not always, what the unit's mission is trying to prevent; they are often actions taken by the threat/*adversary* to prevent unit mission accomplishment. Threat/*adversary* objectives will be specific to the type of threat/*adversary*, the AO, the unit's composition and mission, and other factors. The analyst also describes the threat/*adversary* objective in terms of purpose and end state. A number of different functions must be executed each time a threat/*adversary* force attempts to accomplish a mission.

IDENTIFY HIGH-VALUE TARGETS

5-103. The following techniques may be useful in identifying and evaluating HVTs:

- Identify HVTs from existing intelligence studies, evaluation of the databases, patrol debriefs, and SALUTE reports. A review of threat/*adversary* TTP and previous threat/*adversary* operations as well as understanding the threat's/*adversary*'s objective, tasks, purpose, and intent will be useful.
- Identify assets that are key to executing the primary operation or sequels.
- Determine how the threat/*adversary* might react to the loss of each identified HVT. Consider the threat's/*adversary*'s ability to substitute other assets as well as adopt branches or sequels.

5-104. After identifying the set of HVTs, place them in order of their relative worth to the threat's/*adversary*'s operation and record them as part of the threat/*adversary* model. A HVTs value will vary over the course of an operation. Staffs should identify and annotate changes in value by phase of operations. The identification of HVTs assists the staff in the creation of HPTs.

5-105. HPTs can include various threat/*adversary* considerations that can be detrimental to the success of friendly missions. HPTs are incorporated into the scheme of fires, and are used in the creation of target selection standards and attack guidance matrices.

IDENTIFY THREAT/*ADVERSARY* CAPABILITIES

5-106. Threat/*adversary* capabilities are options and supporting operations that the threat/*adversary* can take to influence accomplishing friendly missions. The analysts define capabilities with the use of statements. The following are examples of capability statements:

- **"The threat/*adversary* has the capability to attack with up to 8 divisions supported by 150 daily sorties of fixed-wing aircraft."**
- **"The criminal organization has the ability to pay off local law enforcement agencies."**
- **"The terrorists have the capability to send destructive viruses over the Internet, which can destroy computer files and archives."**
- **"The threat/*adversary* can establish a prepared defense by 14 May."**
- **"The terrorists have the capability of using CBRN weapons."**
- **"The drug smugglers have the ability to conduct three drug-smuggling operations at the same time."**
- **"The terrorists have the ability to conduct multiple car bombings simultaneously."**
- **"The threat/*adversary* has the ability to target friendly convoys along main supply routes using remotely detonated IEDs."**

5-107. Other capabilities include support to COAs (attack, defend, reinforce, retrograde/*DRAW-D*) or specific types of operations, as well as operations that would allow the threat/*adversary* force to use a COA that would not normally be available or would be severely hindered if the supporting operation were not conducted. Examples of these types of operations include—

- **Use of CBRN weapons.**
- **Intelligence collection.**
- **Electronic warfare operations.**
- **Use of air assets (fixed- and rotary-wing).**
- **Engineering operations.**
- **Air assault or airborne operations.**
- **Amphibious operations.**
- **River operations.**
- **Propaganda.**
- **Deception operations.**
- **Car bombings, bomb scares, and suicide bombers.**
- **Raids on weapon storage facilities.**
- **Carjacking or hijacking of vehicles used in transporting personnel, weapons, or drugs.**
- **Theft of chemicals related to drug manufacturing.**

5-108. When identifying threat/*adversary* capabilities and COAs, start with a full set of threat/*adversary* models and consider the threat's/*adversary*'s ability to conduct each operation based on the current situation and the threat's/*adversary*'s own METT-TC/*METT-T* conditions. Most situations will not present the threat/*adversary* with ideal conditions envisioned by their doctrine. As a result, the threat/*adversary*'s actual capabilities usually will not mirror the ideal capabilities represented by the complete set of threat/*adversary* models.

5-109. The threat/*adversary* could be under-strength in personnel and equipment, may be short of logistic support, or the personnel may be inexperienced or poorly trained. For example, a terrorist group's normal tactics may call for the use of car bombs as a diversionary tactic in order to conduct other operations elsewhere. The evaluation of the threat's/*adversary*'s logistics might indicate a critical shortage of explosives. Analysts should consider the following:

- **Avoid limiting the threat/*adversary* models and capabilities strictly to the threat/*adversary*'s conventional forces. For example, student rioters during a noncombatant evacuation operation may be or may become a threat/*adversary* during the operation.**
- **Avoid overstating the threat/*adversary* model and threat/*adversary* capabilities. The proper use of findings and recommendations developed from threat/*adversary* assessments will in turn develop realistic threat/*adversary* models.**
- **During any discussion of the threat/*adversary*, cultural awareness is an important factor. By developing an awareness of the culture, friendly units can identify groups or individual members of the population that may be friendly, a threat/*adversary*, somewhere in between, or both.**

THREAT/*ADVERSARY* TEMPLATE

5-110. As operations commence, it is imperative to develop foundationally sound and accurate threat/*adversary* models through careful analysis. The analyst analyzes a threat's/*adversary*'s capability, vulnerabilities, doctrinal principles, and preferred TTP. It is from the threat's/*adversary*'s doctrine, training practices, and observed patterns and activities that analysts construct threat/*adversary* templates.

5-111. A threat/*adversary* template is a graphic that depicts the time and distance of relationships of threat/*adversary* forces conducting a specific operation or activity. Depending on the mission variables, developing templates can be time intensive.

5-112. Threat/*adversary* templates show the deployment pattern and disposition preferred by the threat/*adversary* when not constrained by the effects of the operational environment. These templates are normally scaled depictions of threat/*adversary* dispositions for a particular operation. They include—

- **The location of all enemy units two levels down. For example, an infantry battalion in the defense template would depict platoon and specialty team locations.**
- **The distance and/or time between enemy units.**
- **Graphic control measures associated with the operation (boundaries, routes, other).**

5-113. Threat/*adversary* templates graphically portray how the threat/*adversary* prefers to utilize its capabilities to perform the functions required to accomplish its objectives. Threat/*adversary* templates are scaled to depict the threat's/*adversary*'s disposition and actions for a particular type of operation (for example, offense, defense, insurgent ambush, or terrorist kidnapping operation).

5-114. When possible, templates are depicted graphically as an overlay, on a supporting system, or through some other means. Threat/*adversary* templates are tailored to the needs of the unit or staff creating them. They may depict, but are not limited to—

- **Unit frontages.**
- **Unit depths.**
- **Boundaries.**
- **Engagement areas.**
- **Obstacles.**

5-115. Threat/*adversary* templates allow analysts and the staff to—

- **Fuse all relevant combat information.**
- **Assist in identifying intelligence gaps.**
- **Predict threat/*adversary* activities and adapt COAs.**
- **Synchronize information collection.**

5-116. An integrated attack is an offensive action where the threat/*adversary* seeks a military decision by destroying the enemy's will and/or ability to continue fighting through the application of combined arms effects. An integrated attack is often employed when the threat/*adversary* determines overmatch of the enemy and is able to mass all elements of offensive combat power for mission effects. It may also be employed against a more sophisticated and capable opponent if the appropriate advantage and/or opportunity is created or available. (See TC 7-100-2, paragraphs 3-63 to 3-74, for more information on integrated attacks.)

5-117. Integrated attacks are characterized by—

- **Not being focused solely on destruction of ground combat power but often on enemy command and control and logistics.**
- **Fixing the majority of the enemy's force in place with the minimum force necessary.**
- **Isolating the targeted subcomponents of the enemy's combat system from the enemy's main combat power.**
- **Using complex terrain to force the enemy to fight at a disadvantage.**
- **Using deception to degrade the enemy's situational understanding and ability to target threat/*adversary* formations.**
- **Using flank attack and envelopment, particularly of enemy forces that have been fixed.**

5-118. The threat/*adversary* prefers to conduct integrated attacks when most or all of the following conditions exist. The threat/*adversary*—

- **Recognizes significant overmatch in combat power over enemy forces.**
- **Possesses at least air parity over the critical portions of the battlefield/*battlespace*.**
- **Operates sufficiently free of enemy standoff reconnaissance and attack systems to be able to operate without accepting high levels of risk.**

5-119. An integrated attack employs various types of functional forces. The threat/*adversary*, when task-organized with significant combat capabilities, assigns subordinate units functional designations that correspond to their intended roles in the attack. Two types of forces are enabling forces and action forces.

5-120. The most common type of action force in an integrated attack is the exploitation force. Such a force is capable of penetrating or avoiding enemy defensive forces and attacking and destroying the enemy's support infrastructure. An exploitation force ideally possesses a combination of mobility, protection, and firepower that permits it to reach the target with sufficient combat power to accomplish the mission.

5-121. Enabling forces in an integrated attack are employed typically as fixing, assault, and/or support forces. A disruption force exists but is not created specifically for this type of offensive action.

- **The fixing force in an integrated attack is required to prevent enemy defending forces, reserves, and quick-response forces from interfering with the actions of the assault and exploitation forces. One or more assault forces may be used in an integrated attack.**
- **The assault force in an integrated attack has mission tasks to destroy a particular part of the enemy force or seize key positions.**
- **A support force provides support to the attack with command and control functions, attack by fire effects, and other support/*combat support*, such as smoke; suppressive artillery and rocket fires; air-delivered weapons; combat engineer units; and/or sustainment/*combat service support* capabilities.**

5-122. Figures 5-7 through 5-9 on pages 5-26 through 5-28 are examples of threat/*adversary* models.

5-123. Figure 5-7 is an example of a complex battle position for an insurgent organization threat/*adversary* model.

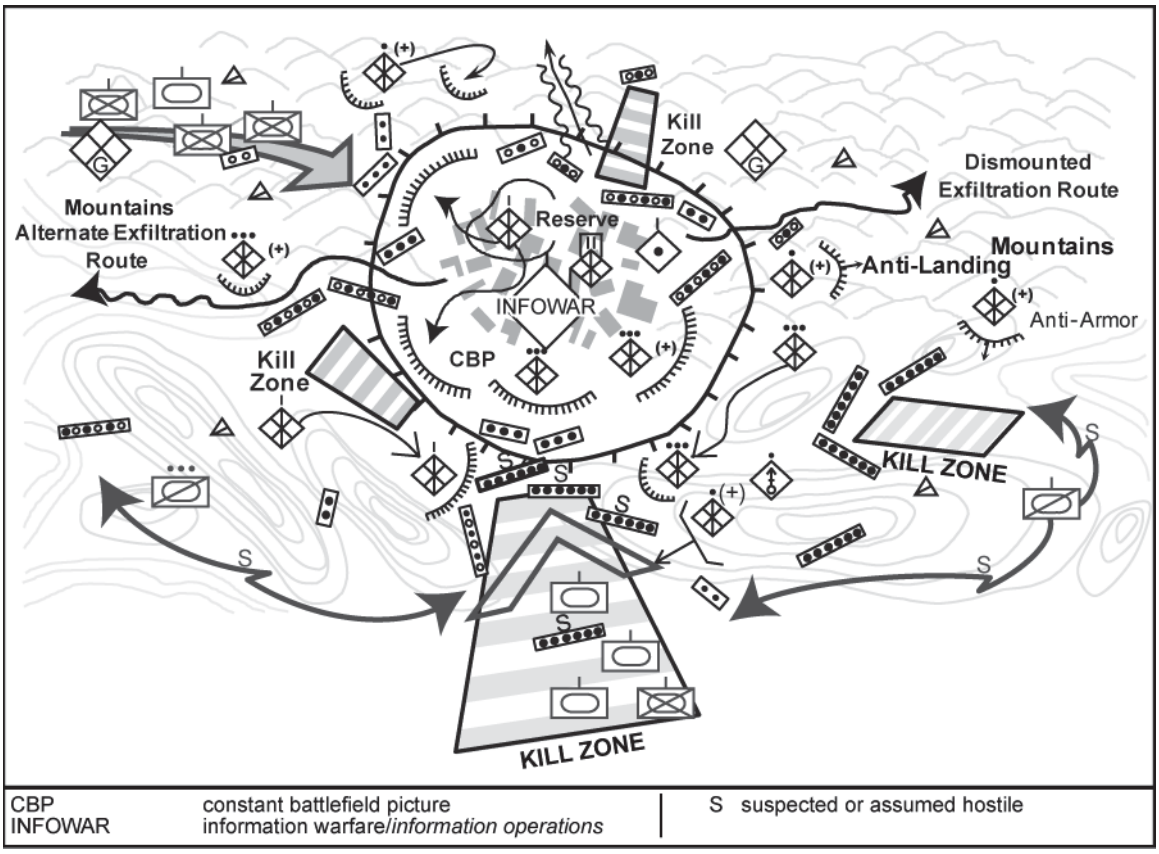


Figure 5-7. Example of a complex battle position: insurgent organization threat/*adversary* model

5-124. Figure 5-8 is an example of a threat/*adversary* template for counterinsurgency operations.

Figure 5-8. Example threat/*adversary* template (counterinsurgency)

5-125. In a threat/*adversary* template, the identification of immediate and subsequent objectives can be terrain-based or force-based. Objectives are more than likely areas deemed as key terrain by the threat/*adversary* commander based on operational timelines.

5-126. The irregular threat/*adversary* opposing friendly forces doctrinally prefers to conduct attacks consisting of—

- **IED attacks (see figure 5-9 on page 5-28).**
- **Convoy ambushes.**
- **Complex attacks against fixed sites.**
- **Urban anti-armor ambushes.**

5-127. Other attacks that the irregular threat/*adversary* opposing the brigade/*unit* may conduct are—

- **Indirect fire attacks.**
- **Murders and kidnappings.**
- **Sniper attacks.**
- **Bombing (vehicle and suicide).**

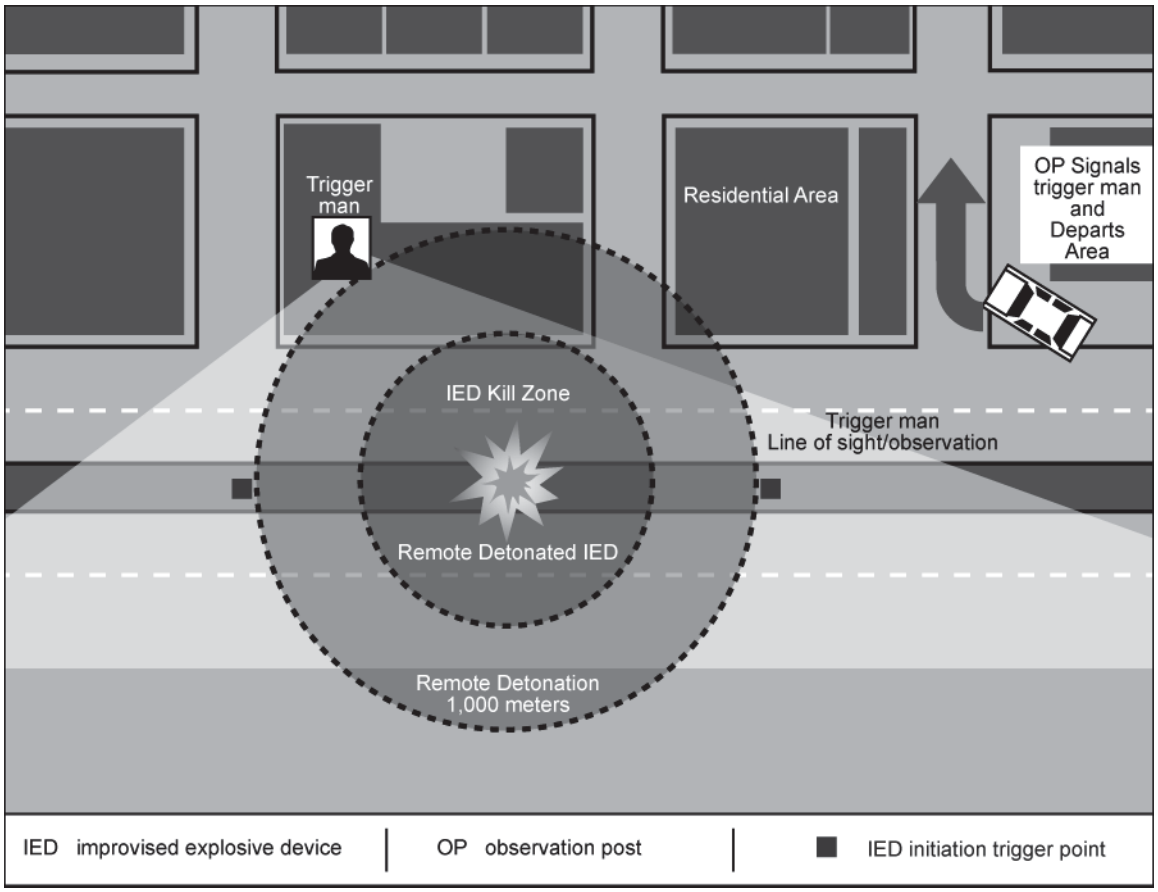


Figure 5-9. Event template (IED attack)

THREAT/*ADVERSARY* CAPABILITIES STATEMENT

5-128. Threat/*adversary* capabilities are the broad options the threat/*adversary* has to counter friendly operations and supporting operations the threat/*adversary* can take based on the conclusions made when determining threat characteristics/*adversary order of battle* at the beginning of step 3 of the IPB process. A threat/*adversary* capabilities statement is a narrative that identifies a particular action for which the threat/*adversary* has the capability to complete and the tactics the threat/*adversary* prefers to use to accomplish its objectives. It addresses operations of major units that will be portrayed on the threat/*adversary* template and the activities of each warfighting function. Figure 5-10 is an example of a threat/*adversary* capability statement that illustrates the capabilities of the 231st Brigade Tactical Group.

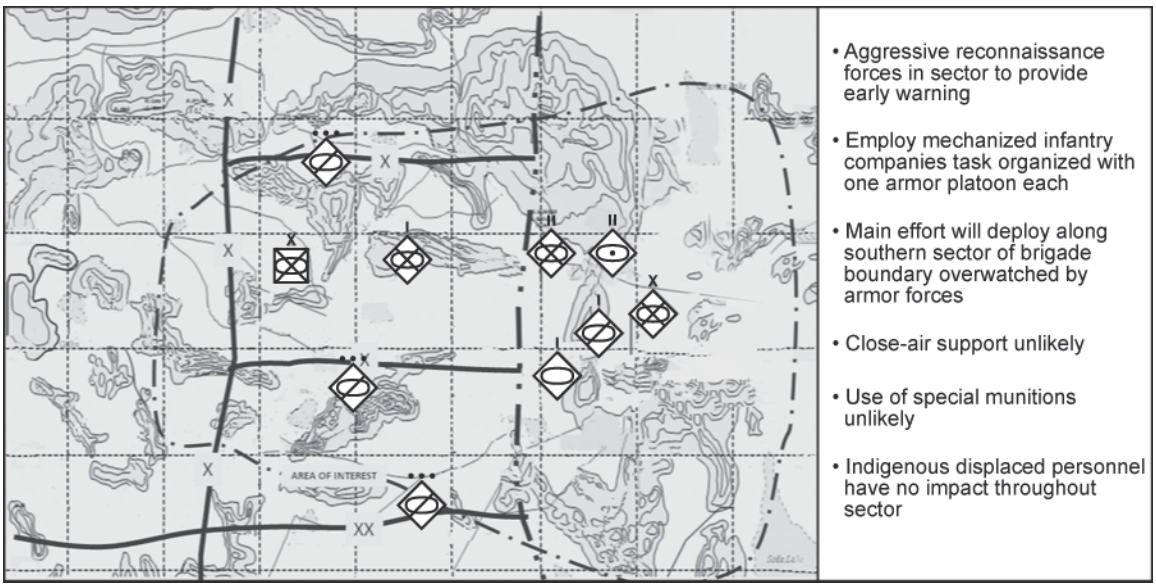


Figure 5-10. Example threat/*adversary* capability statement

HIGH-VALUE TARGET LIST

5-129. The HVTs identified during step 3 of the IPB process are initially refined during step 4 of the IPB process, and are refined again during the COA analysis step of the MDMP/*COA wargaming step of MCPP*. This data is used to develop the HPTL that is continually refined during execution by targeting groups and boards.

5-130. HVTs are determined based on analysis of the threat/*adversary* capabilities statement, an analysis of the threat/*adversary* template, and tactical judgment. Mentally wargaming and thinking through the threat/*adversary* operation is the quickest and most efficient method to determine HVTs at this point. Determining how the threat/*adversary* will employ its assets aids in determining the assets critical to the operation. For example, when mentally wargaming a threat/*adversary* air attack against friendly targets supported by a well-prepared air defense system, it is logical to conclude that the threat/*adversary* will need a substantial air defense suppression package as part of its operation to ensure the success of the attack. In this case, the artillery and air assets that form this suppression package are HVTs.

5-131. In identifying and evaluating HVTs, it may be useful to—

- **Identify HVTs from existing intelligence studies, evaluation of the databases, patrol debriefs, and SALUTE reports. A review of threat/*adversary* TTP and previous threat/*adversary* operations as well as understanding the threat's/*adversary*'s objective, tasks, purpose, and intent will be useful.**
- **Identify assets that are key to executing the primary operation or sequels.**
- **Determine how the threat/*adversary* might react to the loss of each identified HVT. Consider the threat's/*adversary's* ability to substitute other assets as well as to adopt branches or sequels.**

5-132. After identifying the set of HVTs, place them in order of their relative worth to the threat/*adversary* operation and record them as part of the threat/*adversary* model. An HVT's value varies over the course of an operation. The staff should identify and annotate changes in value by the phase of operation. The following are additional considerations:

- **Use all available intelligence sources (for example, patrol debriefs, SALUTE reports) to update and refine the threat/*adversary* models.**
- **Categorize the updates to reach a conclusion concerning the threat's/*adversary*'s operations, capabilities, and vulnerabilities.**

5-133. HPTs can include various threat/*adversary* considerations that can be detrimental to the success of friendly missions. During targeting, HVTs are identified and prioritized during the wargaming phase of

planning. In addition, it identifies the subset of HVTs that must be acquired and attacked for the friendly mission to succeed. HVTs may be nominated as HPTs when these targets can be successfully acquired, vulnerable to attacks, and such an attack supports the commander's scheme of maneuver.

5-134. To ensure all HVTs are identified, the staff determines which assets are critical to the success of the threat's/*adversary*'s main and supporting efforts, as well as those critical to the success of possible threat/*adversary* branches and sequels. Determining how the threat/*adversary* will react to the loss of an asset and its ability to substitute other assets will also aid in this process. HVTs should be prioritized by their relative worth to the threat's/*adversary*'s operation. Target value analysis aids in prioritizing HVTs.

5-135. ***Marine Corps staffs conduct a center of gravity analysis based on the understanding gained through design and task analysis to identify or refine adversary and friendly centers of gravity and to determine which friendly and adversary weaknesses may become critical vulnerabilities. A critical vulnerability is some aspect of the center of gravity that is, or can be made, vulnerable to attack.***

TARGET-VALUE ANALYSIS

5-136. The TVA is a process led by the fires cell as part of targeting that quantifies the relative value of HVTs with each other in relation to a particular enemy operation. (See FM 3-60 and FM 6-20-40 for more discussion on TVA.) This analysis is based in part on the conclusions the intelligence staff reaches as it evaluates threat characteristics/*adversary order of battle* during IPB. The IPB products required to support TVA are the threat/*adversary* template, the threat/*adversary* capabilities statement, and the HVTL. These products aid the fires cell and the rest of the staff in—

- **Providing a focus for the commander's target acquisition effort.**
- **Identifying priorities for the engagement of enemy targets that will facilitate the success of the mission.**
- **Identifying effects criteria.**

Note. **While TVA is conducted initially during IPB, it is a separate process that is repeated throughout the operations process as part of targeting. To be effective, TVA depends on the most current intelligence related to the enemy. Initially based on the threat/*adversary* templates developed during step 3 of the IPB process, TVA should be refined based on the threat/*adversary* COAs developed during step 4 of the IPB process, and refined continually based on changes to the enemy situation overlay during operations. Whenever conducted, the intelligence staff supports TVA with the most up-to-date enemy-related intelligence it has.**

5-137. ***For the Marine Corps, TVA is a method of identifying and ranking potential HVT sets in a COA. The target analyst, in coordination with the G-3/S-3, G-2/S-2, fire support coordinator, and other staff members, wargame the COAs to—***

- ***Finalize individual staff estimates.***
- ***Develop a fire support plan and a scheme of maneuver, as well as friendly and adversary decision support templates.***
- ***Determine critical assets required by the adversary commander to accomplish the commander's mission.***

5-138. See JP 3-60 for more information on TVA.

Chapter 6

Step 4 of the IPB Process—Determine Threat/*Adversary* Courses of Action

WHAT IS IT?

6-1. Step 4 of the IPB process identifies and describes threat/*adversary* COAs that can influence friendly operations. Example 1 is a classic vignette from *The Defence of Duffer's Drift*, by Sir Ernest Swinton, which illustrates the proper use of tactics, IPB, and the practical application of doctrine. Example 2 examines PMESII-PT/*PMESII* and ASCOPE from the threat's perspective.

Example 1

A Boer S-2 tells his commander: "Sir, the enemy platoon leader's likely objective is to retain control of the only crossing point suitable for wheeled traffic over the Silliasvogel River. He can defend the crossing, known as Duffer's Drift, with his 50 Soldiers in any one of the following ways:

- He can leave it undefended until tomorrow (being inexperienced and thinking that we will not arrive until the next day). He can dig his platoon into a small enclosure just on the other side of the drift. A variant of this COA would be for him to establish a trench line astride the main road.
- He can occupy and fortify the Kraal village that overlooks the drift.
- He can occupy the riverbed itself with only a small outpost in the Kraal village. This goes against every canon in British doctrine; however, we must consider this COA because it is so dangerous to the accomplishment of our mission.

The S-2 tells his commander: "Sir, I think the platoon leader will adopt one of these COAs, in order of probability as I gave them. We need to conduct reconnaissance of the riverbed and the Kraal in order to find out which of these COAs he has chosen."

Example 2

While evaluating the threat/*adversary*, another technique is to consider PMESII-PT/*PMESII* and ASCOPE through the perspective of the threat/*adversary* force. As the threat/*adversary* is evaluated, consider how PMESII-PT/*PMESII* and ASCOPE will impact how the enemy will operate. Also, while evaluating the threat/*adversary*, consider how the friendly actions may impact enemy operations and enemy COAs.

DESIRED END STATE

6-2. The desired end state of step 4 of the IPB process is the development of graphic overlays (enemy situation templates) and narratives (enemy COA statements) for each possible enemy COA that has been identified. The staff uses these products during the friendly COA development and friendly COA analysis steps of MDMP/*COA wargaming step of MCPP*:

- **Replicate the set of COAs that the enemy commander and staff are considering.**
- **Identify all COAs that will influence the friendly command's mission.**
- **Identify those areas and activities that, when observed, will discern which COA the enemy commander has chosen. The primary outputs associated with step 4 may include—**
  - **Representing the enemy action or enemy COAs with associated COA statements and HVTLs.**
  - **Developing an event template and associated event matrix.**
  - **Determining the HVTL and providing input to HPTs and the HPTL.**
  - **Providing input into the collection plan.**
  - **Updating the intelligence estimate.**
  - **Providing input into PIRs.**
  - **Providing input into OPORDs and/or OPLANs (annexes and/or appendixes).**

SO WHAT?

6-3. The "so what" in this step is determining the enemy COAs necessary to aid the development of friendly COAs.

- **Success results in the friendly commander will avoid being surprised with an unanticipated enemy action, thus quickly narrowing the set of possible threat/*adversary* COAs to the one the enemy has chosen.**
- **Consequences of failure:**
  - **Failure to identify which of the possible COAs the enemy has chosen, leading to surprise of the friendly command.**
  - **The enemy commander may have the information needed to exploit the opportunities the operational environment provides in a way the friendly commander did not anticipate.**

HOW TO DO IT: (THE PROCESS)

6-4. Determining threat/*adversary* COAs is a two-step process consisting of the actions discussed below and shown in figure 6-1:

- **Develop threat/*adversary* COAs.**
- **Develop the event template and matrix.**

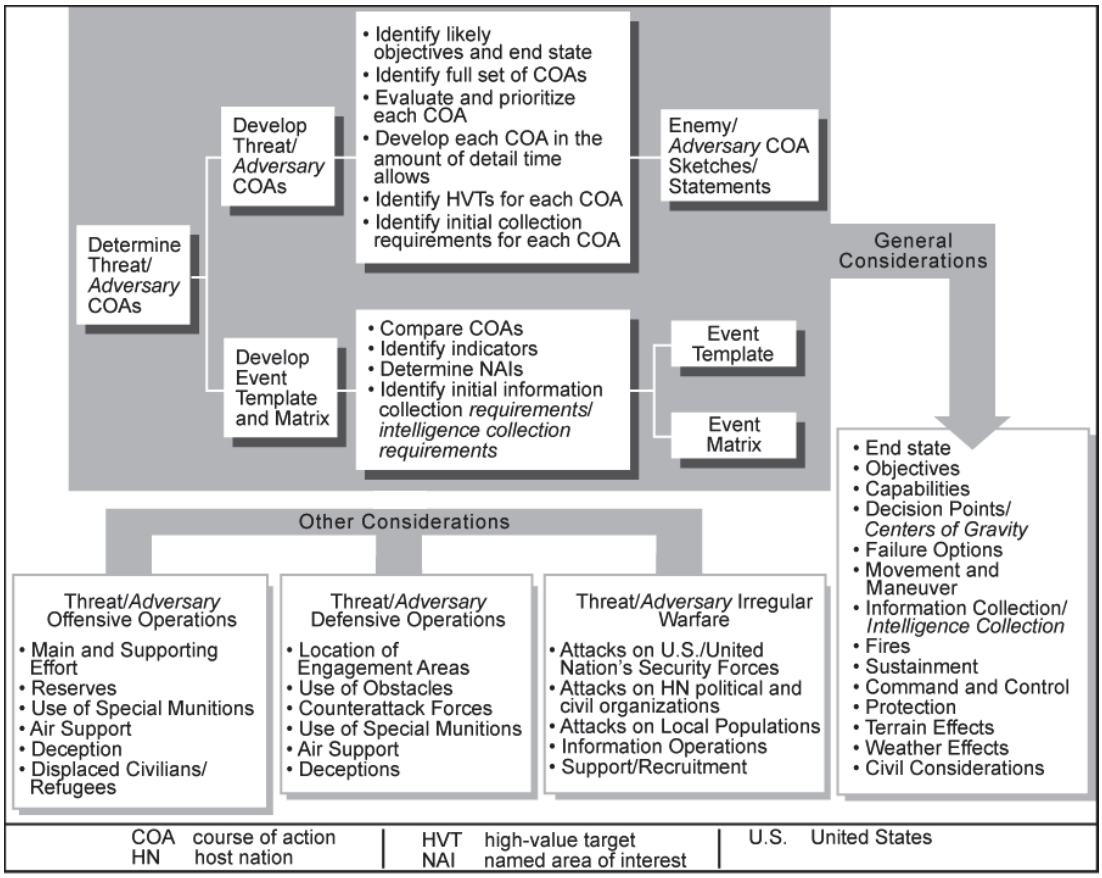


Figure 6-1. Determine threat/*adversary* COAs

DEVELOP THREAT/*ADVERSARY* COURSES OF ACTION

6-5. Threat/*adversary* COA development is a six-step process that requires an understanding of the threat characteristics/*adversary order of battle* discussed in chapter 5, and the effects of terrain, weather, and civil considerations on operations discussed in chapter 4. Population effects to operations will be clearly annotated with full details so that during the wargame the population and the effects and threat/*adversary* actions will be portrayed during the wargame. The most important element in determining enemy COAs is in understanding enemy operational art and tactics. As mentioned in chapter 5, there are three types of threat/*adversary* forces that U.S. forces may encounter: regular, irregular, and hybrid. The process to determine COAs these forces may employ is identical, mirrors friendly COA development, and consists of the following:

- **Identify likely objectives and end state.**
- **Identify the full set of COAs available to the threat/*adversary*.**
- **Evaluate and prioritize each threat/*adversary* COA.**
- **Develop each COA in the amount of detail time allows.**
- **Identify HVTs for each COA.**
- **Identify initial collection requirements for each COA.**

6-6. In order to plan for all possible contingencies, the commander understands all COAs a threat/*adversary* commander can use to accomplish his objectives. To aid in this understanding, the staff determines all valid threat/*adversary* COAs and prioritizes them from most to least likely. The staff also determines which threat/*adversary* COA action is the most dangerous to friendly forces. To be valid, threat/*adversary* COAs should be feasible, acceptable, suitable, distinguishable, and complete—the same criteria used to validate friendly COAs.

6-7. When determining COAs for regular and hybrid threats/*adversaries* where the threat/*adversary* operates under the command and control of a unified command structure, the staff will develop COAs focused on the objectives and end state of that command structure. However, when faced with multiples threats/*adversaries* with varied and competing objectives, such as those encountered during stability tasks, the staff will have to develop COAs for each of these threats/*adversaries*.

6-8. Threat/*adversary* COAs are developed in the same manner as friendly COAs. When developing a threat/*adversary* COA, the intelligence staff accounts for all relevant enemy activity; this includes all possible branches and sequels the threat/*adversary* commander may adopt. (See ADRP 5-0/*MCWP 5-1* for further discussion of the development of friendly COAs.) Intelligence staffs can use this same methodology when developing threat/*adversary* COAs.

IDENTIFY LIKELY OBJECTIVES AND END STATE

6-9. Based on the results of analysis of mission variables conducted earlier in the IPB process, the staff now identifies the enemy's likely immediate and subsequent objectives and desired end state. These elements are included in the threat/*adversary* COA statement developed for each COA.

6-10. An objective is a clearly defined, decisive, and attainable goal toward which every operation is directed. The end state is a set of required conditions that define achievement of the commander's objectives. Enemy objectives are normally terrain or force oriented. For example, an enemy may attack to destroy a friendly force or to seize key terrain; defend to delay a friendly force or retain control of key terrain; or conduct guerrilla operations to disrupt friendly operations.

6-11. The end state is the desired conditions that, if achieved, meet the conditions of policy, orders, guidance, and directives issued by the commander. For example, the end state for an attack to destroy may be the destruction of all friendly forces down to platoon level and friendly forces incapable of conducting a coordinated defense.

6-12. For regular forces, objectives can be either terrain or force oriented, and the end state is usually based on effect and time. For example, the objective of a lead echelon infantry brigade/*unit* performing an attack may be to neutralize defending forces. The brigade's/*unit's* end state may be to prevent defending forces from affecting the movement of second echelon forces. Additionally, the brigade's/*unit's* operations are synchronized in time with higher headquarters operations to ensure combat power is applied where and when needed to ensure success.

6-13. For irregular forces, while the end state remains based on effect, objectives are not always linear or time-based. Often, the objectives for irregular forces are driven by event rather than time. For example, the objective of an extremist group may be to prevent U.S. forces from providing security to the general population by increasing the amount of time spent on resources. The group's end state may be to convince the population to rely on security provided by the extremist group rather than U.S. forces. In this case, the group's operations are synchronized with the operations of U.S. forces attacking patrols, convoys, combat outposts, and security forces.

IDENTIFY THE FULL SET OF COAS AVAILABLE TO THE THREAT/*ADVERSARY*

6-14. A regular force has two primary types of operations it can conduct: attack or defend. Based on its objectives, the enemy must select one of these options. Once selected, the threat/*adversary* generally has multiple options to consider when developing its plan.

6-15. An irregular force can conduct an attack or defend on a small scale, for short periods, or in complex terrain, but it is difficult to sustain these types of operations without degradation to their effectiveness and their operations. The primary types of operations irregular forces can conduct are activities associated with insurgent or guerilla operations, raids, ambushes, sabotage, and acts of terror.

6-16. A hybrid force can combine the capabilities of regular and irregular forces to engage U.S. forces from all points in order to overwhelm U.S. capabilities.

6-17. Regardless of the type of force and the type of operation being conducted, enemy forces may plan operations based on task, purpose, method, and end state. Activities within its operations are planned to support that task and purpose. The staff identifies the tasks, purpose, and end state for each COA developed. By

identifying these for each COA, the intelligence staff will be better able to determine the chosen threat/*adversary* COA during the conduct of operations. Regardless of the type of force, when developing a threat/*adversary* COA, the staff determines—

- **Current enemy situation.**
- **Mission (includes task and purpose).**
- **Enemy/*adversary* objectives, methods, and end state.**
- **Commander's intent, purpose, and end state.**
- **Task organization.**
- **Capabilities.**
- **Vulnerabilities.**
- **HVTs.**
- **Decision points (essential in determining branches and sequels).**
- **Decisive point/*center of gravity* (source of strength, power, and resistance).**
- **Failure options.**
- **Branches and sequels.**
- **Intent for—**
  - **Movement and maneuver.**
  - **Reconnaissance and surveillance.**
  - **Fire support.**
  - **Logistics.**
  - **Threat/*adversary* command and control.**
  - **Protection.**
  - **Information activities.**
  - **Denial and deception.**
- **How terrain and weather will affect threat/*adversary* operations. *For the Marine Corps, this includes a G-2/S-2 red cell analysis. In addition to enemy composition and disposition, METOC parameters are factored in to determine what, if any advantage or disadvantage weather conditions will have on the enemy forces, and how the enemy can use anticipated weather conditions to move against friendly forces.* (*See MCWP 5-1 for more information on red cell analysis*.)**
- **How civil considerations will affect threat/*adversary* operations.**
- **How displaced civilians and displaced persons will affect threat/*adversary* operations.**
- **How the presence and actions of U.S. forces will affect threat/*adversary* operations (reverse IPB).**

6-18. In addition, for enemy offensive tasks, the staff focuses on determining—

- **Main, supporting, and reinforcing efforts.**
- **Use of reserves.**
- **Use of special munitions.**
- **Use of air support.**

6-19. In addition, for enemy defensive tasks, the staff focuses on determining—

- **Location of engagement areas and obstacles.**
- **Location, type, and size of security zone forces.**
- **Location, type, and size of counterattack forces.**
- **Use of special munitions.**
- **Use of air support.**

6-20. In addition, for irregular warfare, the staff generally considers—

- **Guerilla and terror attacks on U.S. forces and host-nation governmental, civil, and security organizations.**
- **Guerilla and terror attacks on local populations.**

6-21. Functional analysis graphically portrays how the threat/*adversary* might utilize its capabilities to perform the functions required to accomplish its objectives. Functional analysis depicts the threat's/*adversary*'s disposition and actions for a particular type of operation. When possible, the results of functional analysis are depicted graphically as an overlay, on a supporting intelligence system, or through some other means. (See appendix B for a discussion on functional analysis.)

6-22. Once the staff has identified all valid threat/*adversary* COAs, it compares each COA to the others and prioritizes them by number. For example, if four COAs have been developed, COA 1 is the enemy's most likely COA and COA 4 is the least likely. Additionally, the staff determines which COA is the most dangerous to U.S. forces. The most likely COA may also be the most dangerous. Additionally, a COA needs to answer six basic questions:

- **Who—the organizational structure of the threat/*adversary* organization, including external organizations providing support.**
- **What—the type of operation: attack, defend, other.**
- **When—the earliest time the action can begin.**
- **Where—the battlefield/*battlespace* geometry that frames the COA (boundaries, objectives, routes, other).**
- **How—the threat/*adversary* will employ its assets to achieve its objectives.**
- **Why—the threat's/*adversary's* objectives.**

EVALUATE AND PRIORITIZE EACH ENEMY/*ADVERSARY* COA

6-23. The commander approves a plan that is optimized to counter the most likely enemy COA, while allowing for contingency options should the threat/*adversary* choose another COA. Therefore, the staff evaluates each enemy COA and prioritizes it according to how likely it is that the threat/*adversary* adopts that option. Generally, threat/*adversary* forces are more likely to use a COA that offers the greatest advantage while minimizing risk. However, based on the situation and its objectives, the threat/*adversary* may choose to accept risk to achieve a desired end state. It is impossible to predict what COA the threat/*adversary* will choose. Therefore, the staff develops and prioritizes as many valid threat/*adversary* COAs as time allows but at a minimum develops the most likely and most dangerous COAs.

DEVELOP EACH COA IN THE AMOUNT OF DETAIL TIME ALLOWS

6-24. A threat/*adversary* COA consists of the following products:

- **Situation template for the threat/*adversary* COA.**
- **Threat/*adversary* COA statement.**
- **HVTs and HVTL for the threat/*adversary* COA.**

Situation Template for the Threat/*Adversary* COA

6-25. When constructing a situation template, the staff uses the threat/*adversary* template developed as part of the threat/*adversary* model during step 3 of the IPB process as a base. That template is modified based on the significant effects the operational environment will have on the threat/*adversary* COA. For example, an enemy may prefer to establish battle positions 1 to 1.5 kilometers apart. The terrain, however, may force the enemy to increase this distance in order to protect its flanks. Another example is, the enemy prefers to attack on high speed AAs but also prefers to avoid complex terrain. Therefore, the location of an urban area along a high speed, optimal AA may force the threat/*adversary* to use a suboptimal approach.

6-26. A threat/*adversary* situation template is a depiction of a potential threat/*adversary* COA as part of a particular threat/*adversary* operation. Situation templates are developed using the threat's/*adversary*'s current

situation, based on threat/*adversary* doctrine and the effects of terrain, weather, and civil considerations. Situation templates can be simple sketches, reserving in-depth development and analysis for later when more time is available.

6-27. A technique is to design a sketch to depict an enemy action or COA which is a graphic representation that will show key outputs or a graphic representation of an enemy action or enemy COA. Each enemy COA has a corresponding situation template. Figure 6-2 is an example of a situation template.

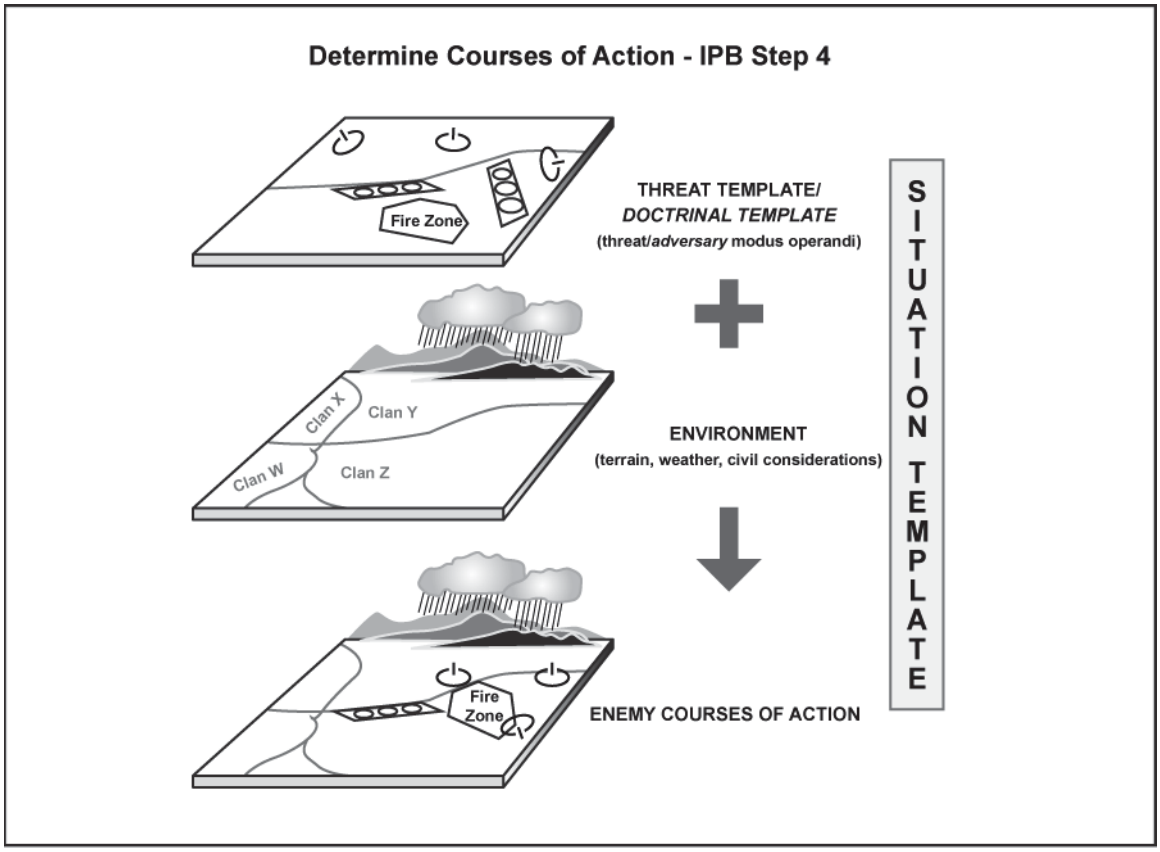


Figure 6-2. Example of a situation template

6-28. A threat/*adversary* situation template is a graphic depiction along with the analysis of expected enemy dispositions related to a specific COA. Situation overlays usually depict the most critical point in the operation as determined by the commander, the operations officer, and the intelligence officer. However, the operation may require several overlays representing different "snapshots in time." This is especially true when developing overlays for enemy offensive tasks where there may be several critical points in the engagement. Chapter 5 contains the figures that show examples of a threat/*adversary* template and situation template.

6-29. Generally, there will not be enough time during the MDMP/*MCPP* to develop enemy situation overlays for all COAs. A good technique is to develop alternate or secondary COAs, write a COA statement, and produce a HVTL to use during the mission analysis briefing and COA development. Once these tools and products are complete, the staff constructs overlays depicting the enemy's most likely and most dangerous COA to use during friendly COA analysis.

6-30. There are three primary types of enemy situation overlays the staff may have to develop: enemy in the offense, enemy in the defense, and irregular forces conducting guerrilla or terror operations. During IPB, these overlays are largely based on assumption and depict enemy locations and activities that are usually templated. This is especially true of overlays depicting enemy offensive tasks or guerilla and/or terror activities. Because the enemy is more static in defensive tasks, the staff may have information related to enemy locations that aids the development of the overlay.

6-31. When developing an overlay depicting regular forces conducting offensive or defensive tasks, the staff should template enemy locations and activities two levels down. For example, a friendly brigade combat team/unit would construct an overlay showing maneuver companies and specialty platoons. One of that brigade's battalions/*an element two levels down from the unit* would refine that overlay for its zone or sector showing maneuver platoons and specialty teams.

6-32. When developing an overlay depicting irregular forces, the staff at every echelon templates enemy locations and activities at the cellular level. For example, whether at corps, division, brigade, or battalion/*regardless of the level of the unit* the staff templates enemy cells where these cells are believed to be operating. Staffs template where they believe the activity associated with each cell can occur. This activity is determined by evaluating enemy activity through predictive and pattern analysis.

6-33. ***For the Marine Corps, once the complete set of adversary COAs has been identified, analysts develop each COA in as much detail as the situation requires and time allows. The order in which each COA is developed is based on its probability of adoption and the commander's guidance. To ensure completeness, each COA must answer the following five questions:***

- ***What (type of operation)?***
- ***When (time the action will begin)?***
- ***Where (sectors, zones, axis of attack)?***
- ***How (method by which the adversary will employ his assets)?***
- ***Why (objective or end state of the adversary)?***

Overlays Depicting the Enemy in Offensive Tasks

6-34. The staff constructs an enemy offensive overlay using an 11-step process that includes the following steps:

- **Step 1—Draw the enemy line of departure. This graphic-control measure is normally placed where the friendly limit of advance is. H-Hour is the time the enemy crosses the enemy line of departure or friendly limit of advance. When the enemy begins movement from assembly areas, to the line of departure or limit of advance, its actions in time and space occur on an H-countdown. Enemy movement that occurs past the line of departure or limit of advance happens on an H+ countdown. This information will be depicted on the enemy attack timeline accompanying the overlay.**
- **Step 2—Draw the enemy's immediate and subsequent objectives as identified in the enemy COA statement. Enemy offensive objectives are normally terrain or force oriented. For example, a force-oriented immediate objective may be to defeat first echelon defending forces and facilitate the passage of second echelon forces. A subsequent objective for this operation may be the destruction of friendly second echelon defending forces. Reverse IPB can aid in determining these objectives. Although the commander has not approved the plan yet, the staff will already have a rough idea of how to construct the defense based on the results of IPB so far.**
- **Step 3—Draw the enemy left and right boundaries. This determination is made on the doctrinal frontage for the enemy attack and the effects of terrain on movement. The MCOO developed during step 2 of the IPB process will show AAs, as well as the optimal and suboptimal movement routes, available to the enemy attacking force.**
- **Step 4—Draw all available attack routes the enemy may use to conduct its attack and secure its immediate and subsequent objectives. The MCOO and weather effects matrix/*operational impacts chart* will aid this analysis also.**
- **Step 5—Template the point of penetration. This area is where the enemy's main effort will attempt to move through the main defensive line. This area will most likely be at the end of a high-speed optimal attack route that allows the enemy to use speed and mass to quickly overwhelm the defense. It may also be at perceived weak points in the defense.**
- **Step 6—Template the locations of enemy ground reconnaissance assets from the line of departure along attack routes to the immediate and subsequent objectives. These locations will normally be associated with the enemy commander's decision points and locations where reconnaissance assets can provide observation in support of targeting.**

- **Step 7—Template the initial and subsequent field artillery firing positions the enemy will use to support the attack. Templating where the range fans for each type of enemy indirect fire system need to be to support actions on each enemy objective aids in this analysis.**
- **Step 8—Template potential locations the enemy may employ special munitions to isolate part of the friendly defense; delaying reorientation of the defense or the use of counterattack forces.**
- **Step 9—Template air AAs that enable the enemy's use of close air support on immediate and subsequent objectives.**
- **Step 10—Template enemy movement formation and attack timeline. There are several ways to do this. One way is to template how the enemy movement formation looks as the advance guard main body enters the defense's engagement area. Another technique is to show how the enemy movement formation looks at different points along attack routes. This technique requires the development of multiple enemy attack formations as it moves through the defense's sector.**
- **Step 11—Label enemy commander's decision points. Indicate on the overlay the areas where the enemy commander has to make a decision regarding the movement of forces to achieve the desired objectives and end state associated with the COA.**

6-35. Figure 6-3 is an example of an enemy situation overlay showing a mechanized infantry brigade in the attack.

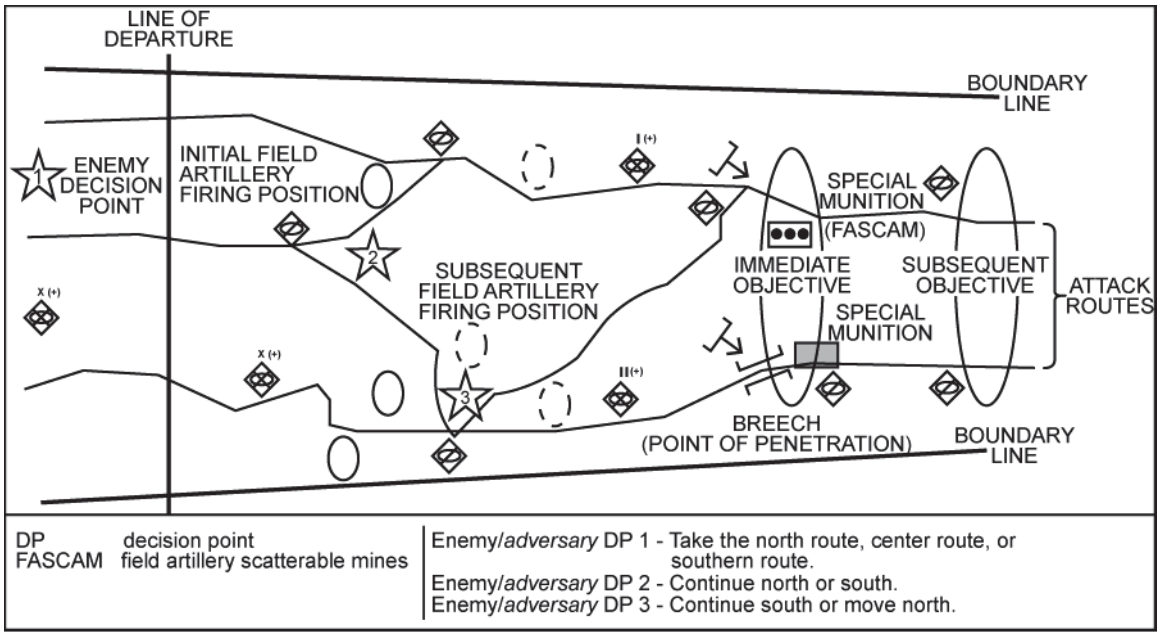


Figure 6-3. Example enemy offensive situation overlay

6-36. Figure 6-4 is an example of an enemy reconnaissance attack.

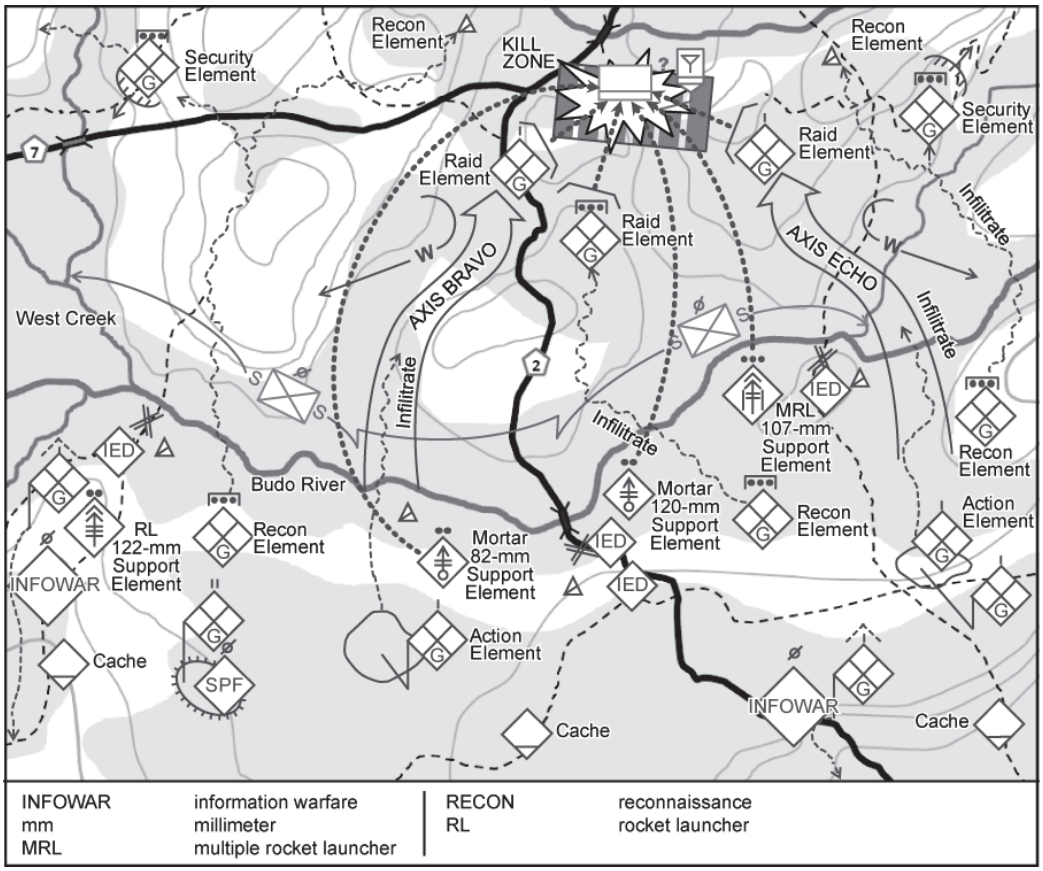


Figure 6-4. Example enemy reconnaissance attack

Overlays Depicting the Enemy in Defensive Tasks

6-37. The staff constructs an enemy defensive overlay using a 10-step process that includes the following steps:

- Step 1—Template the location of enemy battle positions. Enemy battle positions are determined based on the assessed locations of enemy units, what is known about enemy operational art and tactics, and the effects of terrain and weather on the construction of a defense.
- Step 2—Template the location of enemy obstacles. The location of obstacles is determined based on assessed locations of enemy obstacles and unit locations, what is known about enemy operational art and tactics, and the methods available to the enemy to tie its obstacle plan into the terrain.
- Step 3—Template the location of enemy engagement areas. The templated location of enemy battle positions and obstacles aids in determining the location of engagement areas.
- Step 4—Draw the control measures (internal and external boundaries) associated with the defense. The frontage of the enemy defense can be determined by the structure presented by the configuration of battle positions, obstacles, and engagement areas templated in steps 1 through 3.
- Step 5—Template the field artillery firing positions the enemy will use to support the defense. Templating where the range fans for each type of enemy indirect fire system need to be to support enemy forces in the security zone and in the main battle area aids in this analysis.

- **Step 6—Template the locations of enemy observation posts, antitank ambushes, and forward positions located in the security zone. These locations will normally be associated with the enemy commander's decision points, locations where reconnaissance assets can provide observation in support of targeting, and locations where the enemy can disrupt or deceive attacking forces.**
- **Step 7—Template potential locations where the enemy may employ special munitions to channel attacking forces into engagement areas; separate echelons or force attacking forces to adopt a protective posture from CBRN attack.**
- **Step 8—Template air AAs that enable the enemy's use of close air support on the main defensive belt to support the defense.**
- **Step 9—Template the location of enemy counterattack forces and the movement routes these forces can use to support the defense. When templating movement routes, identify the movement times associated with each route.**
- **Step 10—Label enemy commander's decision points. Indicate on the overlay the areas where the enemy commander has to make a decision regarding the movement of forces to achieve the desired objectives and end state associated with the COA.**

6-38. Figure 6-5 is an example of an enemy defensive situation overlay.

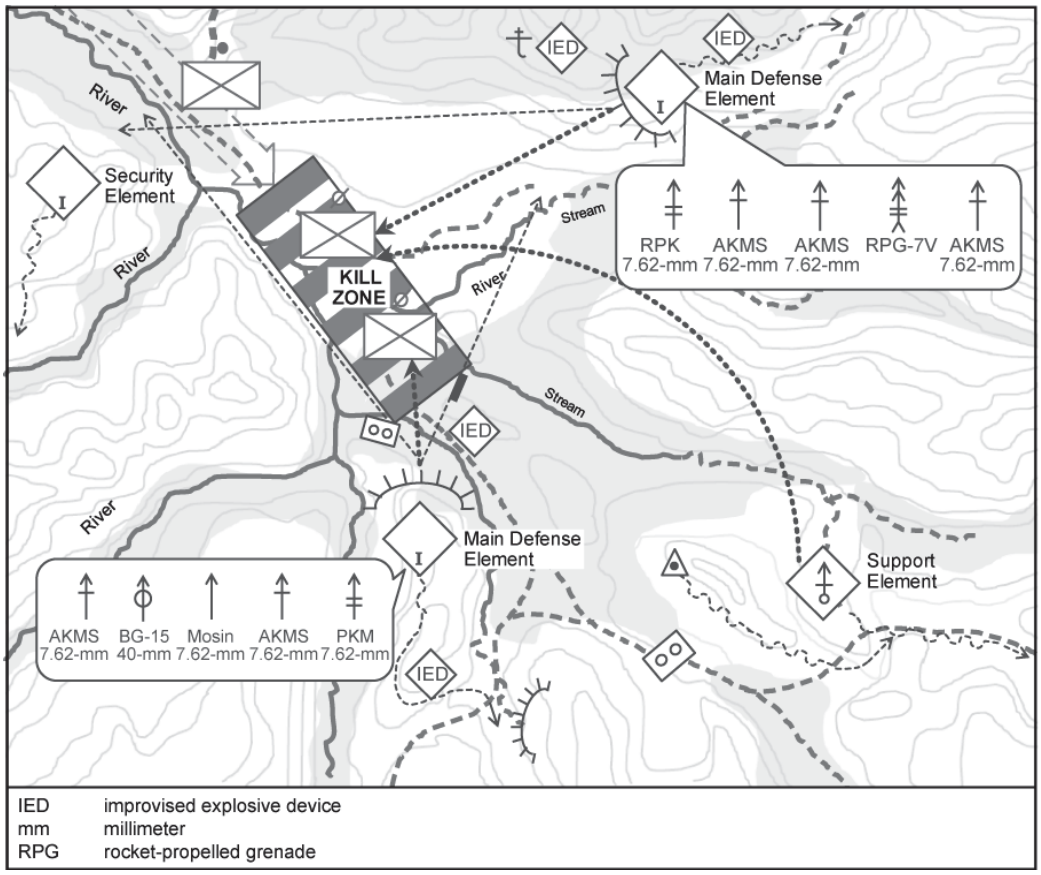


Figure 6-5. Example enemy defensive situation overlay

Overlays Depicting Irregular Forces

6-39. Overlays depicting irregular forces conducting operations typically focus on armed forces in a tactical array. The process and example at figure 6-6 depicts an enemy situation overlay showing an irregular force operating in an urban area.

6-40. Staffs consider whether they need to create overlays that depict the less visible elements of the threat/*adversary* to include auxiliary support networks, and popular support groups as well as the activities they engage in. Additionally, staffs should capture the process they use to template the overlay so that they and subordinate staffs can replicate the process as required.

6-41. The staff constructs an irregular forces overlay using a 10-step process that includes the following steps:

- **Step 1—Template the physical objectives irregular forces may attack. These objectives are typically friendly unit locations and movement routes. These objectives may also be elements or individuals associated with host-nation political, civil, and security organizations; critical infrastructure; or elements of the civilian population.**
- **Step 2—Template ingress and egress routes around objectives. Analysis of these routes includes consideration of nontraditional approaches associated with infiltration and sabotage.**
- **Step 3—Template range fans around objectives. This analysis is based on the ranges of enemy indirect fire and air defense systems.**
- **Step 4—Template potential locations of reconnaissance and surveillance assets. This analysis includes consideration of physical areas of observation around and on the objective. It also focuses on identifying TTP the enemy uses to conduct reconnaissance.**
- **Step 5—Template potential ambush sites along movement routes and near objectives. This analysis is based on pattern and predictive analysis, as well as on analysis of friendly activities and movement.**
- **Step 6—Template potential sniper locations along movement routes and near objectives. This analysis is based on pattern and predictive analysis, as well as on analysis of friendly activities and movement.**
- **Step 7—Template potential IED attack locations along movement routes and near objectives. This analysis is based on pattern and predictive analysis, as well as on analysis of friendly activities and movement.**
- **Step 8—Template potential cache sites. This analysis is based on pattern and predictive analysis, as well as on analysis of TTP.**
- **Step 9—Template the bed-down area for direct action cells and HPTs (individuals). This analysis is based on pattern and predictive analysis.**
- **Step 10—Draw the AO for each direct action cell. This analysis is based on pattern and predictive analysis.**

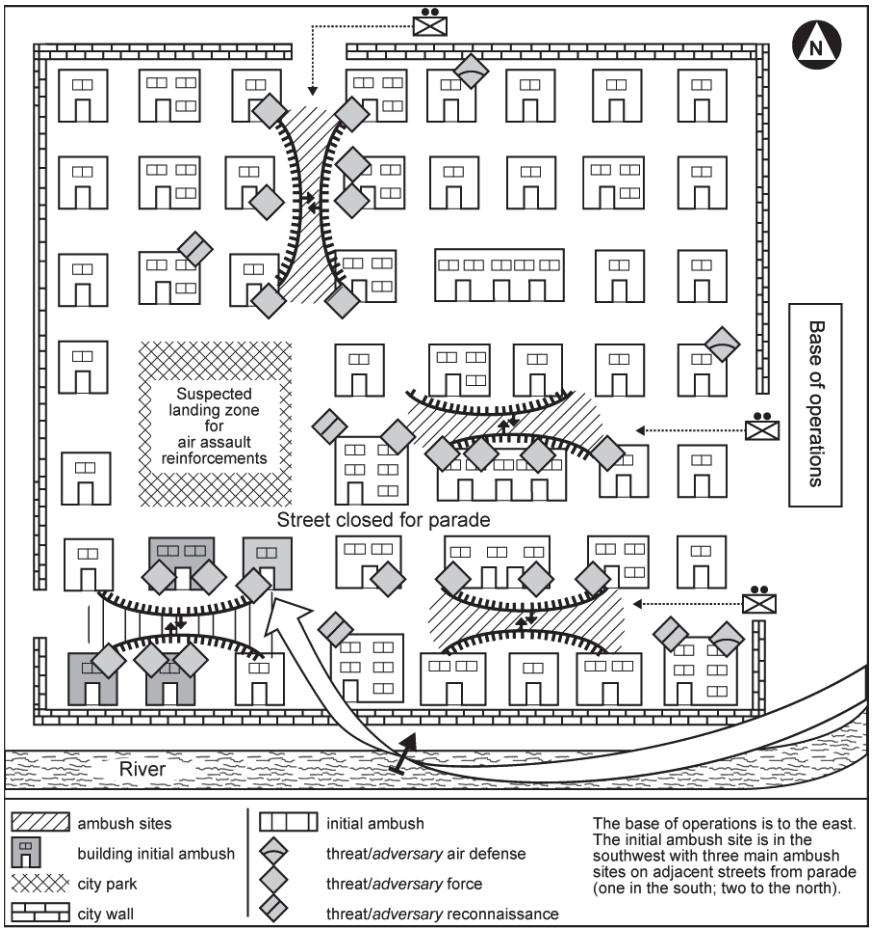


Figure 6-6. Example irregular force situation overlay

Threat/*Adversary* COA Statements

6-42. As stated previously, every threat/*adversary* COA includes a threat/*adversary* COA statement, which is a narrative that describes the situation overlay. Figure 6-7 is an example of a threat/*adversary* COA statement.

Current enemy situation.
Enemy mission.
Enemy objectives and end state.
Enemy task organization.
Capabilities.
Vulnerabilities.
Decision points.
Decisive point/*Center of gravity*.
Failure options.
Commander's intent for—

- Movement and maneuver.
- Information collection/*Intelligence collection*.
- Fires.
- Sustainment.
- Threat/a*dversary* command and control.
- Protection.
- Information activities.
- Denial and deception.

Figure 6-7. Example threat/*adversary* COA statement

HVTs and HVTL for the Threat/*Adversary* COA

6-43. An HVT is an asset an enemy commander requires for the successful completion of a mission. Identifying HVTs involves mentally wargaming an enemy COA to determine what assets are required to complete the mission. This process involves—

- **Using the HVTL developed as part of the threat/*adversary* model in step 3 of the IPB process as a guide.**
- **Determining the effect on the threat/*adversary* COA if each of these targets is lost.**
- **Identifying possible threat/*adversary* responses if the target is lost.**

6-44. Based on the situation, one or more of the targets taken from the threat/*adversary* model may be validated as HVTs. Additionally, targets that were not identified in the threat/*adversary* model may turn out to be HVTs.

6-45. Later on, in planning, the staff will use the HVTLs developed for each threat/*adversary* COA to construct the HPTL. The HPT is an asset that if lost to the enemy will significantly contribute to the success of friendly operations.

IDENTIFY INITIAL COLLECTION REQUIREMENTS FOR EACH COA

6-46. After identifying the full set of potential threat/*adversary* COAs, the staff develops the tools necessary to determine which COA the threat/*adversary* will implement. Because the threat/*adversary* has not acted yet, this determination cannot be made during IPB. However, the staff can develop the information requirements and indicators necessary to support the construction of an information collection plan/*intelligence collection plan* that can provide the information necessary to confirm or deny threat/*adversary* COAs and locate enemy targets. Information requirements are those items of information that need to be collected and processed in order to meet the intelligence requirements of the commander. An indicator is an item of information which reflects the intention or capability of a threat/*adversary* to adopt or reject a COA.

6-47. *For the Marine Corps, after identifying potential adversary COAs, the analyst must determine which one the enemy will adopt. Initial collection requirements are designed to help answer the challenge. The identification of initial intelligence collection requirements revolves around predicting specific areas and activities, which, when observed, will reveal which COAs the adversary has chosen. The areas where the analyst expects key events to occur are designated NAIs. The activities that reveal the selected COA are called indicators.*

6-48. Chapters 7, 8, and 9 discuss the types of information needed to support offensive, defensive, and stability tasks. These requirements are generally related to confirming or denying a threat/*adversary* COA and locating enemy HVTs.

DEVELOP THE EVENT TEMPLATE AND MATRIX

6-49. An event template is a graphic overlay used to confirm or deny enemy COAs. The event template is used as a guide during the COA analysis step of the MDMP/*COA wargaming step of MCPP* to describe enemy actions throughout wargaming. Additionally, the event template is used to develop the information collection overlay/*intelligence collection overlay* and the decision support template during COA analysis. The event template is used during the execution phase of the operations process to aid in determining which COA the enemy has adopted. An event template is always accompanied by an event matrix.

6-50. The event template is comprised of the following elements: time-phase lines, NAIs, and enemy decision points. Time-phase lines are linear geographic areas that depict when enemy activity will occur. NAIs are usually selected to capture indications of enemy COAs, but also may be related to conditions of the operational environment. A decision point is a point in time and space when the enemy commander anticipates making a decision regarding a specific COA.

6-51. An event matrix is a table that associates the NAI and enemy decision points identified on the event template with indicators to aid in determining which COA the enemy commander is implementing. An indicator is an item of information which reflects the intention or capability of an enemy to adopt or reject a COA.

6-52. The initial event template and matrix are normally developed prior to COA analysis, refined during COA analysis, and further refined during execution as the situation changes. In addition to using the event template and matrix to support its own planning, the staff normally disseminates the event template to subordinate units to aid in the development of subordinate unit information collection plans/*intelligence collection plans*.

EVENT TEMPLATE

6-53. Constructing an event template is an analytical process that involves comparing the multiple enemy COAs developed earlier in step 4 of the IPB process to determine the time or event and the place or condition in which the enemy commander must make a decision on a particular COA. Figure 6-8 and figure 6-9 on page 6-16 are examples of how to illustrate the basic mechanics of this process. The figures only display some minimal, but not all-inclusive information, for what is included on the event template.

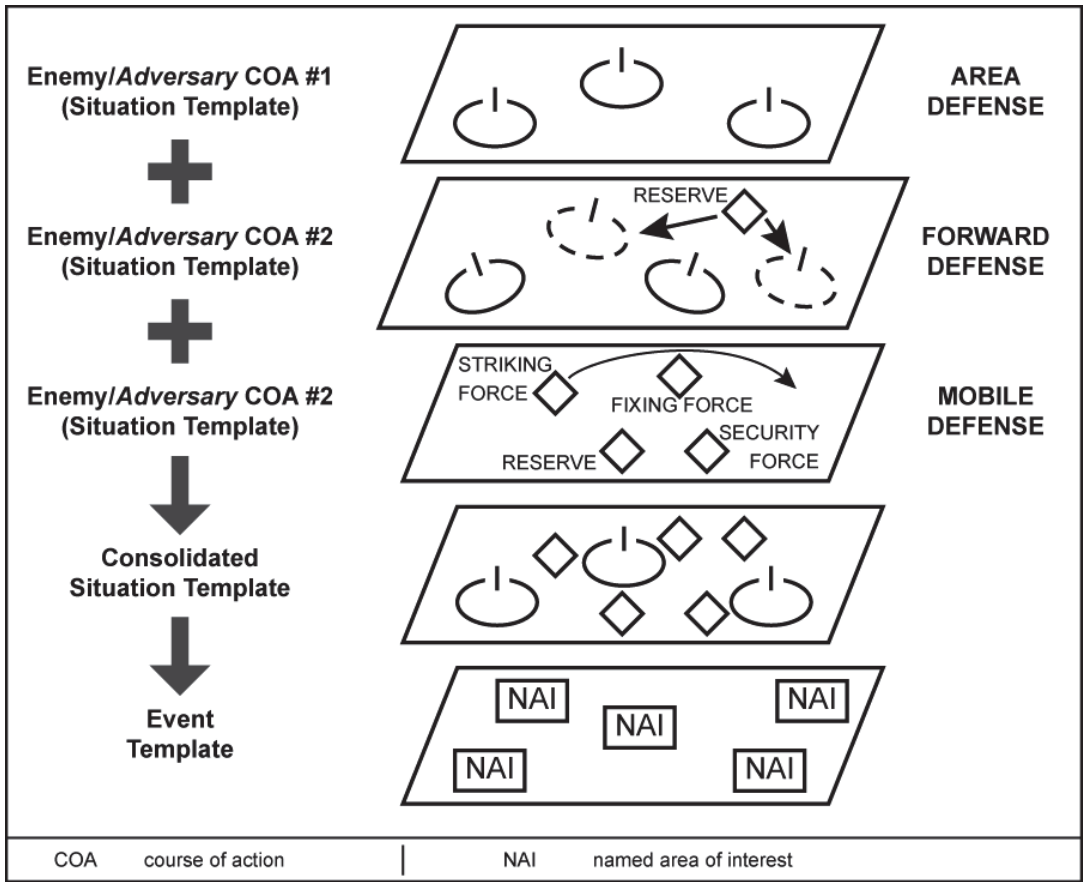


Figure 6-8. Example of an event template – 1

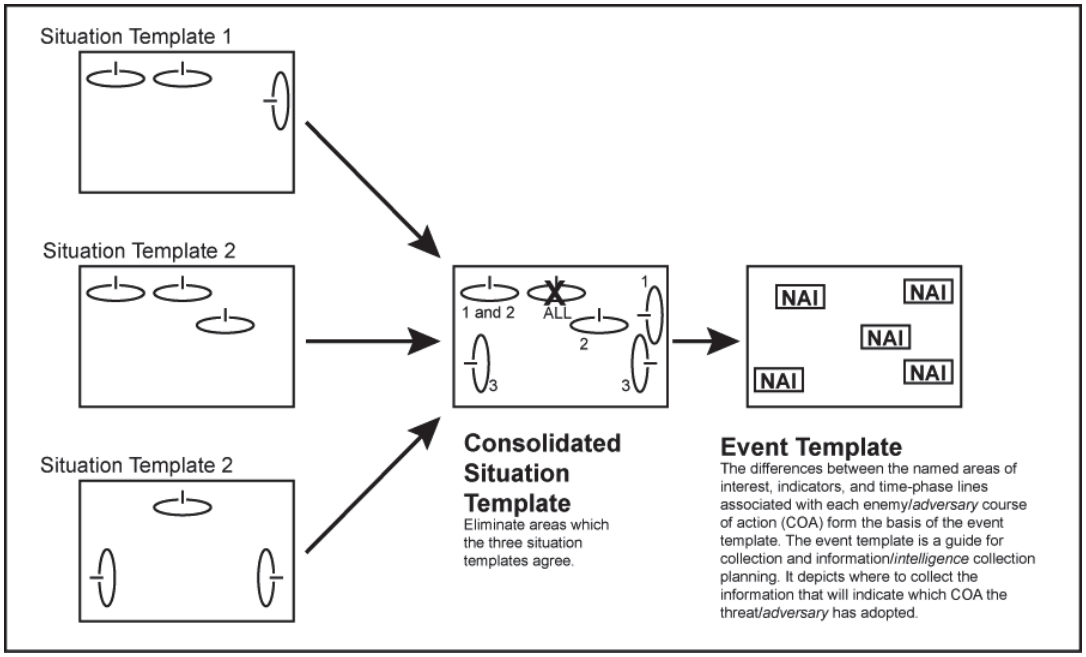


Figure 6-9. Example of an event template – 2

EVENT MATRIX

6-54. Constructing an event matrix is an analytical process that involves determining the indicators of enemy activity that aid in identifying the decisions the enemy commander has made. Table 6-1 illustrates the basic mechanics of this process.

Table 6-1. Constructing an event matrix

Named area of interest	*Indicators*	*Enemy decision point*	*Time (Hour)*	*Enemy course of action (COA) indicated*
1, 2, 3	• Establishment of battle positions and obstacles • Presence of armored vehicles • Presence of engineer assets	1	H–12	COA 1 area defense
1, 3 4	• Establishment of battle positions and obstacles • Presence of armored vehicles • Presence of engineer assets • Identification of company (+) sized reserve	2	H–12	COA 2 forward defense
1, 2, 3 5, 6	• Absence of maneuver and engineer assets • Presence of mobile armored formation	3	H–3	COA 3 mobile defense

6-55. Figure 6-10 is an example of a completed event template for an enemy conducting offensive operations. This figure is for illustrative purposes and is not based on a tactical scenario.

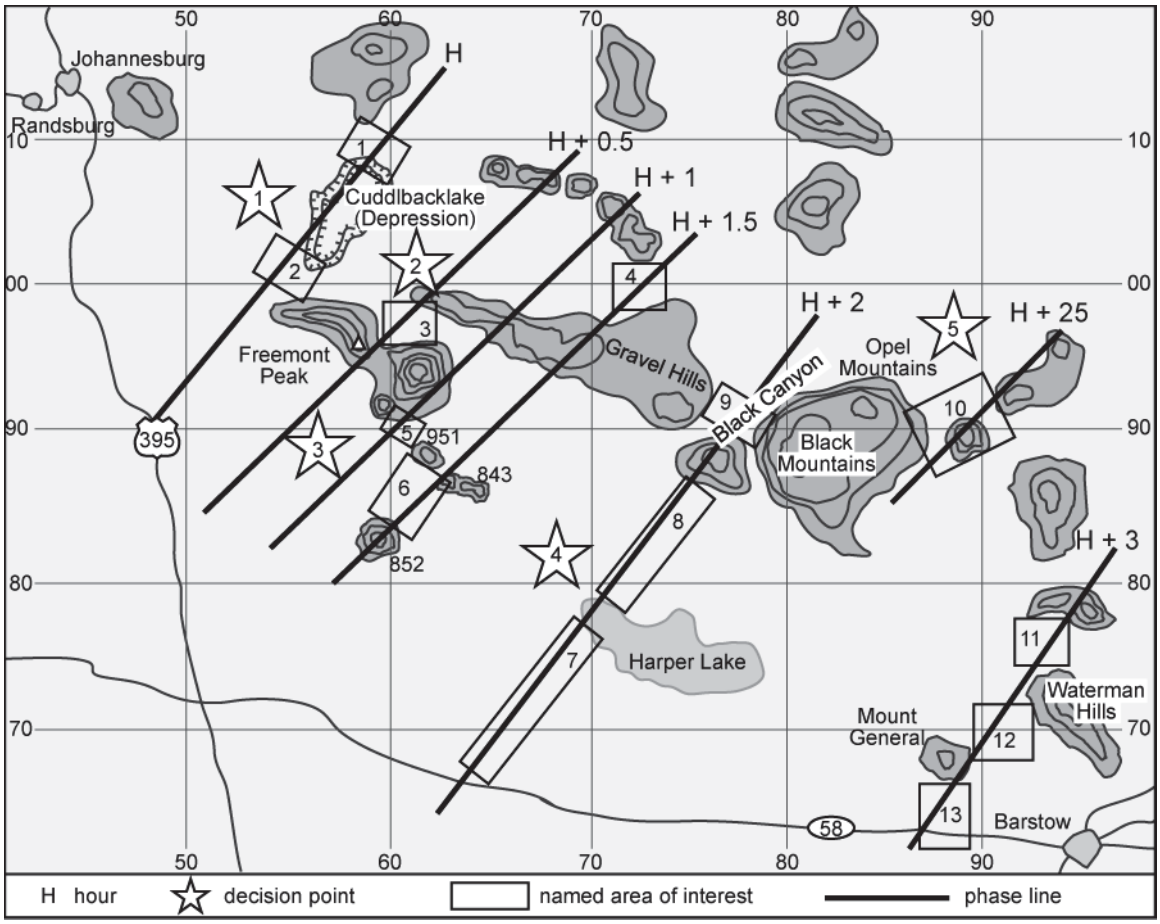


Figure 6-10. Example event template (regular threat)

6-56. Figure 6-11 is an example of a completed event template for an enemy conducting irregular warfare. This figure is for illustrative purposes and is not based on a tactical scenario.

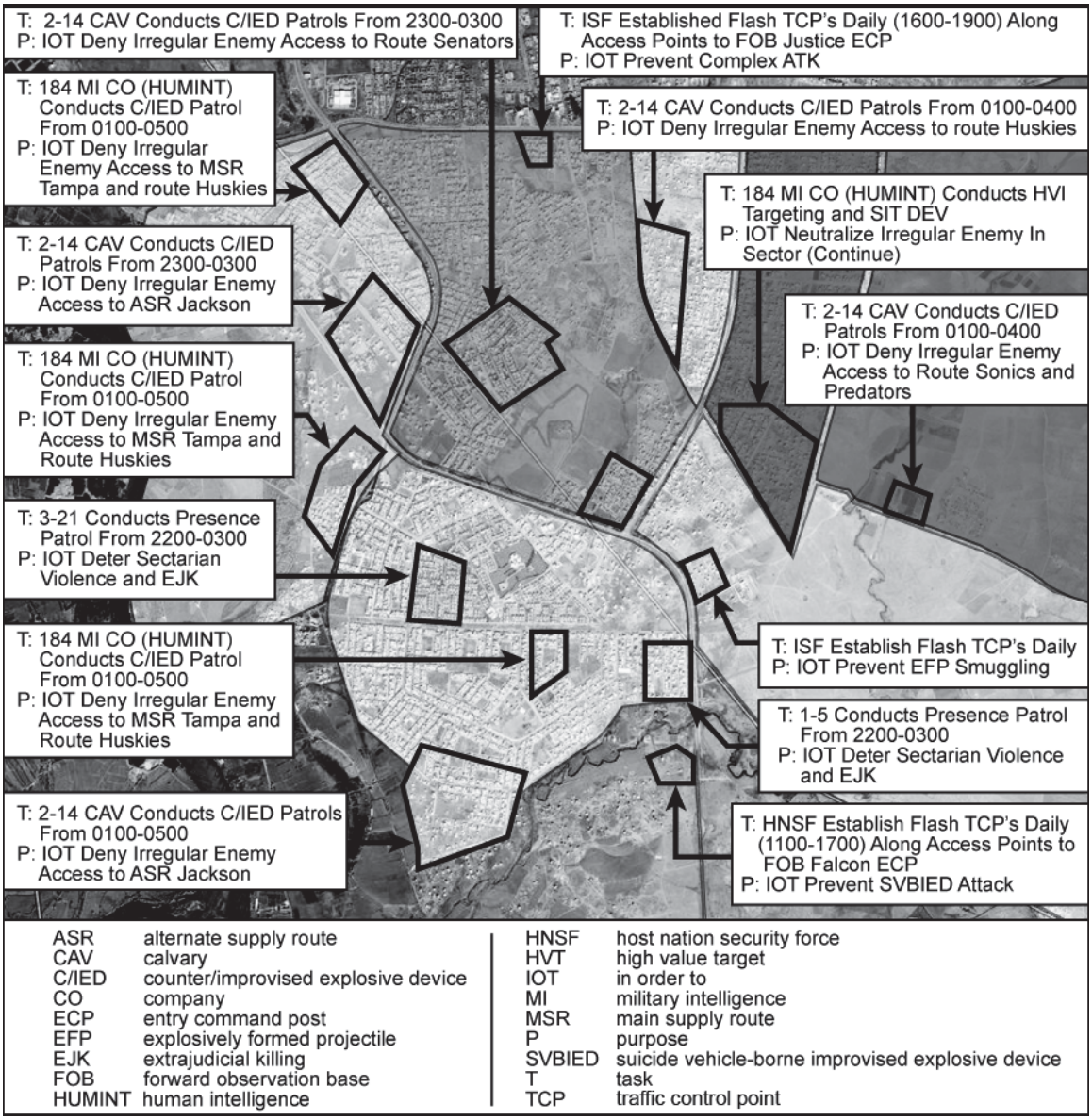


Figure 6-11. Example event template (irregular threat)

Note. **When constructing an event template for an enemy or multiple enemies conducting irregular warfare operations, it is often challenging to discern the tactical enemy decisive point. A way to overcome this is to construct the event template based on conclusions formed based on a pattern and link analysis.**

PART THREE

Considerations for Specific Operations, Unique Environments, and Missions

Chapter 7

IPB for Specific Operations

7-1. Unified action is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1). Under unified action, commanders synchronize military actions with activities of other government agencies, NGOs, IGOs, and the private sector.

7-2. For the Army, the Army's contribution to unified action, as well as its operational concept, is unified land operations. Unified land operations describes how the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution. Chapter 7 discusses specific considerations for IPB conducted in support of unified land operations. (See ADP 3-0 for further discussion of unified land operations.) Army forces conduct decisive and sustainable land operations through the simultaneous combination of offensive, defensive, and stability operations appropriate to the mission and environment.

7-3. ***For the Marine Corps, this chapter discusses specific considerations for IPB in support of specific operations. Intelligence analysts must identify areas that favor each type of MAGTF operation (such as offensive, defensive, force protection, and peace enforcement). They tailor their intelligence analysis and products depending on which type of operation they face. (See MCWP 5-1 for information on planning for specific types of operations.)***

IPB CONSIDERATIONS FOR OFFENSIVE TASKS/*OPERATIONS*

7-4. Offensive tasks are conducted to defeat, destroy, or neutralize an enemy force. A commander may also conduct offensive tasks to secure decisive terrain, to deprive the enemy of resources, to gain information, to deceive and divert the enemy, to hold the enemy in position, to disrupt his attack, and to set the conditions for future successful operations (ADRP 3-90). ***Offensive operations are operations conducted to take the initiative from the enemy, gain freedom of action, and generate effects to achieve objectives. The four types of offensive operations are movement to contact, attack, exploitation, and pursuit (MCRP 5-12C).*** **Intelligence requirements generally associated with offensive operations are as follows:**

- **Determine what type of defense the enemy is employing:**
  - **Area defense.**
  - **Mobile defense.**
  - **Retrograde.**

- **Determine location, disposition, and orientation of enemy defense:**
  - **Main battle area.**
  - **Battle positions.**
  - **Battle handover lines.**
  - **Obstacles.**
  - **Engagement areas.**
  - **Reserves.**
  - **Fire support assets.**
  - **Specialty teams.**
  - **Close air support and other aviation supporting the defense.**
  - **Other assets supporting the defense.**
- **Determine the enemy commander's—**
  - **End state.**
  - **Objectives.**
  - **Decision points.**
  - **Decisive point/*center of gravity*.**
  - **Failure option.**
- **Determine enemy commander's intent for—**
  - **Denial and deception operations.**
  - **Information activities.**
  - **Reconnaissance and surveillance.**
  - **Fires.**
- **Identify terrain and weather effects that support enemy defensive tasks:**
  - **Physical areas that allow the commander to tie in obstacles and battle positions to existing terrain features.**
  - **Air and ground AAs (close air support, reserve, and counterattack forces).**
  - **Terrain that canalizes attacking forces.**
  - **Prevailing winds, temperature inversion, humidity, precipitation, visibility, illumination, and other weather effects.**
- **Identify terrain and weather effects that support friendly movement and maneuver:**
  - **Air and ground AAs.**
  - **Primary and alternate attack routes.**
  - **Landing zones.**
  - **Terrain management (mission command/*command and control*, air defense, signal, and reconnaissance).**
  - **Prevailing winds, temperature inversion, humidity, illumination, and other weather elements.**
- **Determine the impact of civil considerations and displaced civilians on friendly and enemy operations:**
  - **Rural communities.**
  - **Refugee camps.**
  - **Refugee movement.**
  - **Aid organizations located in the AO.**

7-5. In addition to the intelligence requirements listed in paragraph 7-4, each of these operations has its own unique requirements. (See ADRP 3-90/*MCDP 1-0* for additional information on offensive tasks/*operations*.)

MOVEMENT TO CONTACT

7-6. A movement to contact is an offensive task designed to develop the situation and to establish or regain contact. It may also include preliminary diversionary actions and preparation fires. The extent and nature of the movement to contact depends on whether threat/*adversary* forces were previously in contact. If forces are not in contact, then the central feature of the movement-to-contact operations is gaining or reestablishing contact with the enemy. Conducting movement to contact relies heavily on assumptions made during IPB. This is because the relationship of friendly and enemy forces in time and space is an unknown. In addition to the considerations listed in paragraph 7-4, conducting this type of operation includes considering the following intelligence requirements during IPB:

- **Enemy location and intent.**
- **Location and time of potential meeting engagements.**
- **Location of danger areas (enemy defensive locations along routes, engagement areas, observation posts, and obstacles) where friendly forces may encounter enemy forces.**
- **Attack routes that protect friendly forces from ground observation or surprise by the enemy.**
- **Natural and/or manmade obstacles along attack routes that can affect friendly advance.**
- **Location, type, and size of security forces along attack routes.**
- **Location of enemy flanks and other weak points in the enemy's posture.**
- **Threats to friendly force flanks and rear.**
- **Location and extent of CBRN contaminated areas.**

ATTACK

7-7. An attack is a type of offensive task that destroys or defeats enemy forces, seizes and secures terrain, or both. Movement supported by fires characterizes the conduct of an attack. An attack differs from a movement to contact because enemy main body dispositions are at least partially known. In addition to the considerations listed in paragraph 7-4, conducting this type of operation includes considering the following intelligence requirements during IPB:

- **Location of areas where friendly forces could become disoriented, such as rough or restrictive terrain.**
- **The most favorable routes to the objective.**
- **Areas friendly forces can use to support flanking fire and maneuver, such as support by fire and attack by fire positions.**

EXPLOITATION

7-8. An exploitation is a type of offensive task that rapidly follows a successful attack and is designed to disorganize the enemy in depth. The objective of exploitation is to complete the enemy's disintegration. Exploitation takes advantage of previous successes and friendly force continuing activities. In addition to the considerations listed in paragraph 7-4, conducting this type of operation includes considering the following intelligence requirements during IPB:

- **Location of enemy reserves prior to commitment.**
- **Location of enemy countermobility assets prior to their employment on routes friendly forces are using to conduct the exploitation.**
- **Location of enemy forces attempting to reestablish the defense.**
- **Location of enemy logistics and/or resupply operations.**

PURSUIT

7-9. A pursuit is a type of offensive task designed to catch or cut off an enemy force attempting to escape, with the intent to destroy it. A commander often plans for an enemy retrograde operation as either a branch or sequel to an operation. When recommending pursuit, the staff must consider possible enemy deception (whether the enemy is in retreat or attempting to draw friendly forces into a position where they can be destroyed by conventional means or by weapons of mass destruction). In addition to the considerations

listed in paragraph 7-4, conducting this type of operation includes considering the following intelligence requirements during IPB:

- **Possible routes the enemy might use to conduct retrograde operations.**
- **Availability and condition of pursuit routes.**
- **Location and accessibility of blocking points.**
- **Location of critical terrain features that affect enemy and friendly movement.**
- **Location of enemy uncommitted forces.**
- **Identity of fire support and air assets that can affect friendly force movement.**
- **Indications the enemy can no longer maintain defensive positions nor cohesively execute defensive tasks.**
- **Indications the enemy can only conduct limited counterattacks.**
- **Indications the enemy is increasing reconnaissance efforts.**
- **Indications the enemy is destroying weapons and equipment.**
- **Decrease of enemy indirect fire throughout the AO (intensity and effectiveness).**
- **Increase of enemy indirect fire in one or more sectors of the front at a time when the amount of overall defensive fires is decreasing.**
- **Indications of retreating forces.**
- **Location of enemy second echelon defensive lines.**
- **Location, type, strength, and size of bypassed units.**
- **Presence of new forces on the battlefield/*battlespace*.**
- **Indications of increased resistance.**

IPB CONSIDERATIONS FOR DEFENSIVE TASKS/*OPERATIONS*

7-10. For the U.S. Army, a defensive task is a task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks (ADRP 3-90). *For the Marine Corps, defensive operations are operations conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable to offensive and stability operations. The three types of defensive operations are area, mobile, and retrograde (MCRP 5-12C.)* Intelligence requirements generally associated with defensive operations are as follows:

- **Determine, locate, and/or track the enemy's main and supporting efforts.**
- **Locate and/or track enemy reserves.**
- **Locate and/or track enemy reconnaissance assets.**
- **Identify enemy's use of special munitions (CBRN, artillery scatterable mines).**
- **Locate and/or track enemy close air support.**
- **Locate enemy information capabilities.**
- **Identify enemy deception operations.**
- **Determine enemy commander's end state.**
- **Determine enemy commander's objectives.**
- **Determine enemy commander's decision points.**
- **Determine enemy decisive point/*center of gravity*.**
- **Determine enemy's failure option.**

- **Determine enemy commander's intent for—**
  - **Reconnaissance and surveillance.**
  - **Fires.**
  - **Denial and deception.**
  - **Defensible terrain.**
  - **Battle positions.**
  - **Engagement areas.**
  - **Indirect fire assets positions.**
  - **Counterattack routes for reserves plan.**
- **Develop TAIs for indirect fire and close air support.**
- **Determine the impact of civil considerations and displaced civilians on friendly and enemy operations for—**
  - **Rural communities.**
  - **Refugee camps.**
  - **Refugee movement.**
  - **Aid organizations located in the AO.**

7-11. There are three types of defensive operations forces may engage in: area defense, mobile defense, and retrograde. In addition to the intelligence requirements listed in paragraph 7-10, each of these operations has its own unique requirements. (See ADRP 3-90/*MCDP 1-0* for additional information on defensive tasks/*operations*.)

AREA DEFENSE

7-12. Area defense is a type of defensive operation that concentrates on denying enemy forces access to designated terrain for a specific time rather than destroying the enemy outright. The focus of the area defensive task is on retaining terrain where the bulk of the defending force positions itself in mutually supporting, prepared positions. Units maintain their positions and control the terrain between these positions. The decisive operation focuses on fires into engagement areas possibly supplemented by a counterattack. The reserve may or may not take part in the decisive operation. The commanders can use their reserves to reinforce fires; add depth, block, or restore the position by counterattack; seize the initiative; and destroy enemy forces. In addition to the considerations listed in paragraph 7-10, conducting this type of operation includes considering the following intelligence requirements during IPB:

- **The location of natural lines of resistance, well-defined AAs, IVLs, and other terrain features that support defensive tasks.**
- **Whether the terrain better supports a forward defense or a defense in depth.**

MOBILE DEFENSE

7-13. Mobile defense is a type of defensive operation that concentrates on the destruction or defeat of the enemy through a decisive attack by a striking force. A mobile defense focuses on defeating or destroying the enemy by allowing the enemy to advance to a point where he is exposed to a decisive counterattack by the striking force. The decisive operation is a counterattack conducted by the striking force. The striking force is a dedicated counterattack force constituting the bulk of available combat power. A fixing force supplements the striking force. The commanders use their fixing force to hold attacking enemy forces in position, to help channel attacking enemy forces into ambush areas, and to retain areas from which to launch the striking force. In addition to the considerations listed in paragraph 7-10, conducting this type of operation includes considering the following intelligence requirements during IPB:

- **Methods to deceive the enemy regarding the purpose of the defense.**
- **Terrain that will hide the striking force.**

RETROGRADE

7-14. Retrograde is a type of defensive operation that involves organized movement away from the enemy. The enemy may force these operations, or a commander may execute them voluntarily. The higher commander of the force executing the retrograde must approve the retrograde operation before its initiation in either case. A retrograde is a transitional operation; it is not conducted in isolation. It is part of a larger scheme of maneuver designed to regain the initiative and defeat the enemy. In addition to the considerations listed in paragraph 7-10, conducting this type of operation includes considering the following intelligence requirements during IPB:

- **Possible routes friendly forces can use to conduct retrograde operations.**
- **Possible pursuit routes enemy forces may use.**
- **Blocking points enemy forces may use to prevent the retrograde.**
- **Areas enemy movement can be disrupted through the use of obstacles, indirect fire, and close air support.**

7-15. As in supporting planning for offensive operations, the primary intelligence products and work aids necessary to support planning for defensive operations are a MCOO, weather effects matrix/*operational impacts chart*, enemy organizational charts, enemy capabilities statement, enemy situation overlays with COA statements, event template with matrix, relative target value matrix, HVTL, and intelligence requirements specific to the enemy operation.

IPB CONSIDERATIONS FOR COUNTERINSURGENCY OPERATIONS AND STABILITY TASKS

7-16. Counterinsurgency operations are those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency (JP 1-02). Counterinsurgency operations are usually conducted simultaneously with stability tasks.

7-17. Stability operations is an overarching term encompassing various military missions, tasks, and activities conducted outside the Unites States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (JP 3-0).

7-18. The lines of operations in counterinsurgency and stability operations, as discussed in FM 3-24/*MCWP 3-33.5* and FM 3-07, often overlap and can include establishing civil security, establishing civil control, restoring essential services, supporting governance, and supporting economic and infrastructure development.

7-19. The purpose of IPB in counterinsurgency and stability tasks is the same as in offensive and defensive tasks/*operations*. However, the nature of these operations and the intelligence requirements associated with them are unique. The principal difference is the focus and degree of detail of analysis required for the civil aspects of the environment. Unlike major combat/*major operations*, an environment dominated by offensive and defensive tasks/*operations* directed against an enemy force, counterinsurgency, and stability tasks encompass various military missions, tasks, and activities that are not enemy-centric.

7-20. One of the consistent observations from commands involved in Operation Iraqi Freedom and Operation Enduring Freedom is that planning can become too enemy-centric and ignore other lines of operations. The lesson learned is that while enemy analysis needs to be done, so does the analysis related to all the lines of operations the commander has identified as important. This means that the analysis of civil considerations may have equal or greater importance to the analysis of enemy forces.

7-21. FM 3-24/*MCWP 3-33.5* constitutes the Army/*Marine Corps* current doctrine on counterinsurgency and contains the operational discussion that intelligence personnel need to understand to conduct effective IPB in support of counterinsurgency. The primary intelligence requirements associated with counterinsurgency are associated with the following questions:

- **What are the drivers of instability? (Examples include fraudulent elections, rule-of-law issues, sectarian tensions, political and civil government credibility, completion for resources, lack of essential services, and others.)**
- **What is the nature or type of the insurgency? (Who are the insurgents and what do they want?)**
- **What is the insurgent strategy? (How do they intend to achieve what they want?)**
- **What are the insurgents' motivations (strategic goals)?**
- **What are the insurgents' objectives (operational objectives)?**
- **What popular support does the insurgency have (active or passive, tribal, ethnic, other)?**
- **What are the insurgents' capabilities, vulnerabilities (command and control, maneuver, fire support, intelligence, logistics, other)?**

7-22. FM 3-07 constitutes the Army's current doctrine on stability tasks and contains the operational discussion that intelligence personnel need to understand to conduct effective IPB in support of stability tasks. The primary intelligence requirements associated with stability tasks are generally based on lines of operations identified by the commander and are focused on aiding governments in securing the environment, restoring essential services, and promoting infrastructure and economic development.

Note. For the Marine Corps, see MCWP 3-33.5 for additional information on counterinsurgency and the operational discussion that intelligence personnel need to understand to conduct effective IPB in support of counterinsurgency. See also MCDP 1-0 for additional information on stability operations.

7-23. ***Counterinsurgency and stability operations are conducted in support of a host-nation or interim government or as part of an occupation when no government exists. These operations involve both coercive and constructive actions by the military force. They are designed to establish a safe and secure environment; facilitate reconciliation among local or regional adversaries; establish political, legal, social, and economic institutions; and facilitate the transition to legitimate local governance.***

7-24. Counterinsurgency and stability operations promote and protect U.S. national interests by influencing the threat, political, and information aspects of the operational environment through a combination of peacetime developmental, cooperative activities, and coercive actions in response to crises. Regional security is supported by a balanced approach that enhances regional stability and economic prosperity simultaneously. When conducting IPB for stability tasks, a good technique is to balance the analytical effort in the same manner. Commanders and staffs should be wary of becoming too focused on enemy forces and not conducting necessary analysis on civil considerations. In fact, a greater emphasis may need to be placed on civil considerations than on the enemy during counterinsurgency operations and stability tasks. The purpose of counterinsurgency operations and stability tasks is to—

- **Provide a secure environment (isolate insurgents from the local populace).**
- **Gain support for the host-nation government.**
- **Meet the critical needs of the populace.**
- **Build support for host-nation governments and institutions.**
- **Shape the environment for interagency and host-nation success.**

7-25. IPB can help the commander gain the situational understanding needed to accomplish these tasks by—

- **Understanding the root cause or causes of the insurgency.**
- **Identifying external and internal support for the insurgency.**
- **Understanding how the insurgents appeal to the population.**
- **Identifying the targets/audiences on which insurgents focus.**

- **Identifying groups or populations vulnerable to insurgent influence activities and determine why they are vulnerable.**
- **Understanding insurgent motivation and depth of commitment.**
- **Understanding insurgent TTP.**
- **Understanding the conditions the insurgents want to create to achieve their objectives.**
- **Identifying and verifying identities and tracking insurgents, criminals, and known or suspected terrorists.**
- **Identifying demographics for groups supporting, neutral to, or hostile to insurgent organizations and operations.**
- **Identifying the means to gain legitimacy among the population and its leaders (formal and informal).**
- **Accurately assessing the needs and security requirements of the population.**
- **Providing assessments for all lines of operations.**
- **Identifying the themes insurgent organizations use.**
- **Assessing the effects or consequences of friendly operations.**

7-26. There are five lines of operations associated with counterinsurgency and stability tasks that require extensive IPB:

- **Establish civil security.**
- **Establish civil control.**
- **Restore essential services.**
- **Support governance.**
- **Support economic and infrastructure development.**

7-27. In addition to providing intelligence about these lines of operations, IPB provides intelligence about people. U.S. forces must understand the people of the nation in which they are operating in order to accomplish the missions they are given. Commanders and planners require accurate intelligence assessments into the culture, perceptions, values, beliefs, interests, and decisionmaking processes of the individual and groups that comprise the various social networks that comprise the population.

ESTABLISH CIVIL SECURITY

7-28. Establishing civil security is the first responsibility of military forces in counterinsurgency and stability operations and involves providing for the safety of the host nation, including protection from active enemy forces. When dealing with internal and external enemy forces that pose a direct threat to the host nation and its people, there are three basic subtasks associated with civil security that require detailed IPB:

- **Protect external borders.**
- **Combat internal threats/*defeat insurgencies*.**
- **Separate insurgents from the general population.**

7-29. Table 7-1 identifies types of intelligence requirements that may be associated with each of these three subtasks.

Table 7-1. Example civil security intelligence requirements

Protect external borders	*Combat internal threats/defeat insurgencies*	*Separate insurgents from the general population*
• Identify all external state and nonstate actors attempting to influence U.S. operations. • Identify objectives of these groups and individuals. • Identify the tactics, techniques, and procedures these groups and individuals are using to accomplish their objectives. • Identify physical locations these groups and individuals are using to transport weapons, equipment, personnel, money, media, and ideas across the border. • Identify the locations, methods, and operations of organizations within the host nation aiding external state and nonstate actors. • Identify good locations for friendly observation posts, checkpoints, engagement areas, and friendly approach and withdrawal routes.	• Identify all regular and irregular forces that pose a military threat to U.S. and host-nation security forces. • Identify threat characteristics/ *adversary order of battle* for each threat/*adversary* group. • Develop threat/*adversary* templates for each threat/*adversary* group. • Develop an enemy situation overlay for each threat/*adversary* group. • Identify high-value targets. • Identify and verify individuals as insurgents, known or suspected terrorists, and/or criminals. • Identify actors in the civilian population providing support to enemy forces. • Identify external actors providing support to the enemy. • Identify groups and populations that are vulnerable to enemy influence (persuasion, coercion, other).	• Identify the objectives and concerns of stakeholders. • Determine methods to protect the population from insurgents. • Locate sectarian fault lines. • Locate sectarian and ethnic enclaves. • Identify conditions that can promote civilian opposition to insurgents.

7-30. When conducting stability tasks, U.S. forces will generally not have to prepare for an attack by a regional power across an international border. The primary cross-border threats/*adversaries* U.S. forces will encounter are—

- **Foreign nation special forces.**
- **Terrorist organizations.**
- **Regionally based irregular forces.**
- **Criminal organizations.**

7-31. The primary threat/*adversary* activity U.S. forces will have to counter are—

- **Infiltration of foreign operatives and fighters.**
- **Movement of weapons, equipment, money, and other resources needed to support an insurgency.**
- **Criminal smuggling.**

7-32. Commanders need to know what external forces and/or individuals are supporting enemy forces in their AO in order to develop friendly COAs to counter these forces. Failure by the intelligence staff to provide this intelligence can result in the unchecked reinforcement and resupply of these forces. Although commanders may not be able to act directly against these forces, they can request support from the next higher command. Detailed intelligence on these forces provided by the intelligence staff can assist commanders in gaining this support. Table 7-2 on page 7-10 illustrates four steps as a way of presenting this information.

Table 7-2. TTP for evaluating external threat/*adversary o*rganizations

Step	*Requirement*	*Tactics, techniques, and procedures (TTP)*
1	Identify all external state and nonstate actors attempting to influence U.S. operations and their objectives. Include— • Identity. • Location. • Objectives. • Operations. • Methods. • Defeat mechanisms.	• Identify all organizations and their objectives during mission analysis/*problem framing*. • Develop organizational charts for each of these groups during mission analysis/*problem framing*. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain up-to-date data files for each of these organizations.
2	Within the area of operations, identify physical locations these groups or individuals are using to transport weapons, equipment, personnel, money, media, and ideas across the border.	• Develop a situation template (digital overlay) that depicts the border-crossing points, movement routes, safe houses, cache sites, and high-value targets associated with each organization. • Develop a course of action statement describing the operations of each of these organizations during mission analysis/*problem framing*. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain situation template as part of the joint common database.
3	Identify TTP these groups or individuals are using to accomplish their objectives.	• Identify these methods during mission analysis/*problem framing*. • Develop special assessments (text and graphics) that describe TTP in detail. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain up-to-date data files for each of these TTP.
4	Identify good locations for friendly observation posts, checkpoints, engagement areas, and friendly approach and withdrawal routes.	• Develop a digital terrain overlay (geospatial and imagery intelligence) during mission analysis/*problem framing* that describes these locations. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain digital terrain overlays as part of the joint common database.

Combat Internal Threats/*Defeat Insurgencies*

7-33. When engaged in stability operations, U.S. forces can be contested by one or more armed and organized groups that oppose U.S. presence and objectives in the area. These groups will vary in size and capability. Their motivations and objectives may or may not be the same. They may actively oppose each other or they may work together. The one characteristic these groups share is to achieve their goals through violence. Beyond that, these groups can be generally characterized as follows. They—

- **Are generally un-located and not easily detected by U.S. information collection assets/*intelligence collection assets*.**
- **Are often unidentified early in an operation.**
- **Usually operate under a decentralized chain of command.**
- **Are organized under a cellular, militia, or special forces structure.**
- **Operate in complex terrain usually within urban centers or severely restricted natural terrain.**

- **Are a thinking and adaptable enemy that modify TTP, as needed, to operate against conventional forces.**
- **Target four general groups:**
  - **Host-nation political and civil authorities.**
  - **Host-nation military and police forces.**
  - **The general population.**
  - **U.S armed forces and other international military and civilian agencies.**
- **Sustain themselves through external and/or internal support mechanisms.**
- **Establish sanctuary in complex terrain or among civilian populations.**
- **Generally avoid massing forces.**
- **Generally employ—**
  - **Commercial-off-the-shelf communications technology (telephone, cell phone, Internet).**
  - **Tactical radios.**
  - **Nonelectronic methods of command and control.**
  - **Civilian transportation (public transportation, privately owned vehicles).**
  - **Small arms and crew-served weapons.**
  - **IEDs.**
  - **Mortars.**
  - **Shoulder-fired antiaircraft weapons.**
- **Are capable of operations directed against U.S. forces, such as—**
  - **IED attack.**
  - **Mortar attack.**
  - **Complex attack.**
  - **Sniper attack.**
  - **Drive-by shooting.**
  - **Infiltration.**
  - **Ambush.**
  - **Sabotage.**
  - **Suicide bombing.**
  - **Information activities.**
  - **Information for effect.**
  - **Misinformation.**
  - **Disinformation.**
  - **Propaganda.**
  - **Reconnaissance and surveillance.**
- **Can conduct operations directed against host-nation political targets, civil targets, security targets, and the general population (in addition to the above list):**
  - **Assassination and murder.**
  - **Kidnapping.**
  - **Coercion.**
  - **Intimidation.**
  - **Recruitment.**

7-34. The commander needs detailed intelligence on all of the insurgent organizations in the AOs in order to prevent their activity from affecting the command's ability to complete all other assigned stability tasks. Failure by the intelligence staff to provide this intelligence can result in a continual escalation of insurgent activity that may prevent the command from accomplishing the mission. When evaluating this type of enemy, intelligence staffs maintain up-to-date data files relating to the threat characteristics/*adversary order of battle*, historical reporting, and current reporting to produce the predictive assessments the commander needs to plan operation.

7-35. Table 7-3 illustrates a way of evaluating insurgent operations.

Table 7-3. TTP for evaluating internal threat/*insurgency* operations

Step	*Requirement*	*Tactics, techniques, and procedures (TTP)*
1	Identify all regular and irregular forces that pose a military threat to U.S. and host-nation security forces.	• Identify all organizations and their objectives during mission analysis/*problem framing*. • Develop organizational charts for each of these groups during mission analysis. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain up-to-date data files for each of these organizations.
2	Within the area of operations, identify physical locations these groups or individuals are using to transport weapons, equipment, personnel, money, media, and ideas across the border.	• Develop a situation template (digital overlay) that depicts the border-crossing points, movement routes, safe houses, cache sites, and high-value targets associated with each organization. • Develop a course of action statement describing the operations of each of these organizations during mission analysis/*problem framing*. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain a situation template as part of the joint common database.
3	Identify TTP these groups or individuals are using to accomplish their objectives.	• Identify these methods during mission analysis/*problem framing*. • Develop special assessments (text and graphics) that describe TTP in detail. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain up-to-date data files for each of these TTP.
4	Identify good locations for friendly observation posts, checkpoints, engagement areas, and friendly approach and withdrawal routes.	• Develop a digital terrain overlay (geospatial and imagery intelligence) during mission analysis/*problem framing* that describes these locations. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain digital terrain overlays as part of the joint common database.

Separating Insurgents from the General Population

7-36. Paramilitary elements, terrorists, militias, and other insurgent groups of elements conducting irregular warfare depend on the cooperation of the general population. These groups do not have the capability to sustain operations against armed conventional forces without that support. Denying support from the general population to these groups is a critical component of an overall strategy to prevent them from influencing other stability tasks. Armed groups involved in insurgent operations directed against the host-nation government draw their strength from the population. These groups—

- **Establish sanctuary locations among segments of the population.**
- **Utilize civilian transportation, communications, financial services, and general services to sustain operations.**
- **Receive funding by winning the approval of segments of the population or by extortion.**
- **Utilize segments of the population to provide indications and warnings of U.S. operations.**

- **Conduct information activities targeting the population.**
- **Use the threat of violence or specific actions to coerce the population.**

7-37. In order to separate these forces from the population, commanders need to understand how and why the population is supporting these forces. There are many factors that may influence a local population's perspective and sway its support one way or another. Safety from the violence of war and crime, economic viability, religious freedom, view toward government, and view toward U.S. presence are some examples. The intelligence staff continually reevaluates the role the population is playing in the conflict and provides the information the commanders need to conduct operations that can influence the population to support their programs. Steps 1 and 2 in table 7-4 illustrate a way of presenting this information.

Table 7-4. TTP for evaluating the general population's role in a conflict

Step	*Requirement*	*Tactics, techniques, and procedures (TTP)*
1	Conduct an initial assessment of the population during intelligence preparation of the battlefield/*battlespace.*	• This can be a long and difficult process. Begin this assessment during predeployment. • Integrate civil affairs personnel and assessments in the intelligence preparation of the battlefield/*battlespace* process. • Consider how successful insurgent groups have conducted population surveys to determine how these groups view and use the population. • Maintain a civil considerations assessment that accurately describes the civil aspects of the environment, assesses effects of friendly operations on the population, and identifies strategies that can influence the population to aid in combating enemy forces. • Determine how the enemy is using the population as part of its operations. • Determine the positive and negative effects of every type of friendly operation. • When determining intelligence gaps, include those related to the population. This will assist civil reconnaissance as well as information collection operations/*intelligence collection operations* in general.
2	Continually reassess information collected as part of civil and infrastructure reconnaissance.	• Continually update the civil considerations assessment. • Include the civil considerations assessment in all intelligence briefings. • Include the civil considerations/*human environment* assessment in targeting and information collection working groups/*intelligence collection working groups*.

ESTABLISH CIVIL CONTROL

7-38. When mission and conditions warrant, U.S. forces may be required to implement populace and resources control measures to achieve civil control and protect the populace. The military activities associated with establishing civil control generally involve developing interim mechanisms for establishing rule of law and restoring the justice system. Generally, the military role is to—

- **Occupy and assert transitional military authority.**
- **Establish public order and safety.**
- **Establish military government.**
- **Transition to other authority.**
- **Establish interim criminal justice system.**
- **Support—**
  - **Law enforcement and policing reform.**
  - **Judicial reform.**
  - **Property dispute resolution processes.**
  - **Corrections reform.**
  - **War crimes courts and tribunals.**
  - **Public outreach and community rebuilding programs.**
- **Work with the following types of groups to accomplish the task:**
  - **Host-nation political and civil leaders.**
  - **Host-nation military and police forces.**
  - **Leaders of host-nation religious and ethnic groups.**
  - **U.S., host-nation, and international aid organizations.**
  - **Host-nation judicial bodies.**
  - **Local populations.**

7-39. Establishing civil control goes hand-in-hand with establishing civil security and involves developing interim mechanisms for establishing rule of law. When attempting to establish civil control, the commander has two primary intelligence requirements:

- **Identify the appropriate methods necessary to regulate selected behavior and activities of individuals and groups to reduce the overall risk to the general population.**
- **Determine the reliability, capability, and support requirements of the key individuals and organizations assisting with this task.**

7-40. During IPB, the commander and staff assess the indigenous nation's ability to combat crime, as well as identify—

- **All vulnerable elements of the population and assess their needs.**
- **Methods to communicate with the public to promote reconciliation.**
- **Security requirements for humanitarian aid organizations and indigenous security forces.**
- **What civilian police functions need to be performed by U.S. military forces.**
- **Major crime issues.**
- **Critical infrastructure related to criminal justice and security institutions that need to be protected.**

7-41. Civil affairs/*G-3/S-3*, military police, and the staff judge advocate office and other sources of information—including local nationals, local government officials, NGOs, and IGOs—can provide Department of State information on establishing civil control for—

- **Public order and safety.**
- **Criminal justice system reform.**
- **Law enforcement reform.**
- **Judicial system reform.**
- **Corrections system reform.**

- War crimes courts and tribunals.
- Conflict resolution.
- Public outreach and community rebuilding.

RESTORE ESSENTIAL SERVICES

7-42. The military activities associated with restoring essential services generally involve supporting indigenous populations and institutions as well as civilian relief agency operations addressing the effects of humanitarian crises such as famine, dislocated civilians, displaced persons, and human trafficking. Generally, the military role is to provide—

- **An initial response that provides for immediate humanitarian needs (food, water, shelter, and medical support).**
- **A transformational response where military forces build on unified action partner capacity to operate and maintain essential civil services.**

7-43. During IPB, the commander and staff should determine the nature and scope of the humanitarian crisis as well as determine the following:

- **Civilian dislocation/displaced person relief programs:**
  - **Identify the size and location of dislocated civilian populations.**
  - **Identify food, water, shelter, and medical needs.**
  - **Assess the capability of local physical transport, distribution, and storage to deliver relief supplies (including government and relief agencies).**
  - **Determine the command's capability to provide services or augment the efforts of other organizations.**
  - **Identify other threats to the affected population (human rights abuses, minefields, hostile forces, other).**
- **Famine relief programs:**
  - **Assess the effects of conflict on food and availability.**
  - **Determine food and water security requirements.**
  - **Estimate total food and water needs.**
  - **Assess the capability of local physical transport, distribution, and storage to deliver food and water (including government and relief agencies).**
  - **Identify most vulnerable populations.**
  - **Identify security requirements for relief distribution networks.**
  - **Identify other threats to the affected population (human rights abuses, minefields, hostile forces, other).**
- **Nonfood relief programs:**
  - **Identify security requirements for relief distribution networks.**
  - **Identify areas that need emergency nonfood items.**
- **Humanitarian demining:**
  - **Identify mined areas.**
  - **Identify populations and individuals injured by mines.**
  - **Determine medical support required to treat injuries.**
  - **Determine how best to educate the population to recognize and avoid mines.**
- **Human rights initiatives:**
  - **Identify previous human rights violations.**
  - **Identify vulnerable populations.**
  - **Determine how to secure vulnerable populations.**
  - **Determine how best to support IGOs and NGOs.**

- **Public health and education programs:**
  - **Identify public health hazards (malnutrition, water contamination, sewage).**
  - **Identify deficiencies in the existing medical infrastructure.**
  - **Assess the need for additional medical personnel and facilities.**
  - **Identify requirements to open schools.**

7-44. Civil affairs/*G-3/S-3*, military police, and the staff judge advocate office staff proponents and other sources of information including local nationals, local government officials, NGOs, and IGOs can provide Department of State information for restoring essential services, such as—

- **Civilian dislocation programs.**
- **Famine prevention programs.**
- **Nonfood relief programs.**
- **Humanitarian demining programs.**
- **Human rights initiatives.**
- **Public health programs.**
- **Education programs.**

SUPPORT GOVERNANCE

7-45. When a legitimate and functional host-nation government is present, military forces operating in support of a state have a limited role. However, if the host-nation government cannot adequately perform its basic civil functions, some degree of military support to governance may be necessary. Supporting governance is the fourth stability task that may need to be analyzed during IPB. During IPB, the commander and staff assess whether the indigenous government is adequately performing its basic civil functions. If the indigenous government is not adequately performing its basic civil functions, the commander and staff will—

- **Identify founding documents that establish the nature of government of the host nation (for example, United Nations mandate, declaration of independence, constitution or bylaws).**
- **Implement representative facets to government (councils, elections).**
- **Support civil administration and unified action partners by assisting in the development an internal defense and development plan.**
- **Identify critical essential public infrastructure and services that must be restored and maintained.**
- **Establish public information and education programs that support the authority and legitimacy of the host nation.**
- **Promote public health and welfare through foreign humanitarian assistance (FHA) and humanitarian civil assistance programs in support of the internal defense and development plan.**

7-46. The operations office staff proponent and other sources of information including local nationals, local government officials, NGOs, and IGOs can provide Department of State information on supporting governance for—

- **Transitional administrations.**
- **Local governments.**
- **Anti-corruption initiatives.**
- **Elections.**

SUPPORT ECONOMIC AND INFRASTRUCTURE DEVELOPMENT

7-47. The most effective long-term measure of conflict prevention and resolution is the sustainment of a viable government that is actively engaged in meeting the needs of its citizens; including economic development. A nation's economy affects its ability to govern and provide security for its people. The status of a nation's infrastructure affects the sustainment and growth of its economy. Understanding the economy and the state of infrastructure in the AO is critical to a commander's ability to plan and conduct operations that improve economic conditions.

7-48. Support economic and infrastructure development is the fifth and last stability task that may need to be analyzed during IPB. During IPB, the commander and staff—

- **Assess overall economic conditions within the AO.**
- **Assess overall infrastructure conditions within the AO.**

7-49. When assessing economic conditions, while not all-inclusive, the commander and staff consider the following information:

- **Ability of legal border-crossing sites and other ports of entry to assist the legal flow of commerce.**
- **Positive and negative effects of cross-border smuggling of commercial goods.**
- **Positive and negative effects of any existing underground economy.**
- **Status of financial services being provided by the private sector within the AO.**
- **Threats to critical financial institutions, infrastructure, personnel, and transactions.**
- **Corruption within existing financial institutions.**
- **How the various groups of a local population are earning their living (agriculture, trade, industry).**
- **Where the most important items the population consumes come from.**
- **Weather or terrain effects on the availability of commodities.**
- **How conflict has impacted the availability and movement of commerce.**
- **What measures the population has taken to adapt to a disrupted economy.**
- **Current and projected level of job growth without intervention.**
- **Existence of ongoing host-nation and/or international economic recovery programs.**
- **The economic impact of criminal organizations, insurgent groups, and corrupt political and civil elements on the host-nation government, assistance providers, and U.S. military forces.**
- **Availability and distribution of currency.**
- **The best use of the commander's emergency response program.**
- **Status of dislocated civilian population and ongoing relief efforts.**
- **Measures of effectiveness that can be used for assistance programs and civic action programs.**

7-50. The answers to these questions can help the commander avoid actions that might disrupt economic recovery and target efforts that improve local economic conditions through infrastructure development. Table 7-5 shows the intelligence staff where this information is found. Additional sources of information are local nationals, local government officials, NGOs, and IGOs.

Table 7-5. Information sources for supporting economic developments

Economic category	*Staff proponent*	*Information sources*
Economic Generation and Enterprise Creation	Civil Affairs/*G-3/S-3*	Department of Treasury
Monetary Programs	Civil Affairs/*G-3/S-3*	Department of Treasury
National Treasury Operation	Civil Affairs/*G-3/S-3*	Department of Treasury
Public Sector Investment Programs	Civil Affairs/*G-3/S-3*	Department of Commerce
Private Sector Development	Civil Affairs/*G-3/S-3*	Department of Commerce
Natural Resource Protection	Civil Affairs/*G-3/S-3*	Department of Interior
Agricultural Development	Civil Affairs/*G-3/S-3*	Department of Agriculture
Transportation Infrastructure Programs	Civil Affairs/*G-3/S-3*	Department of Commerce
Telecommunications Infrastructure Programs	Civil Affairs/*G-3/S-3*	Department of Commerce
General Infrastructure Programs	Civil Affairs/*G-3/S-3*	Department of Commerce

7-51. When assessing infrastructure conditions, the intelligence staff considers—

- **The condition of existing infrastructure and whether rehabilitation or new infrastructure development is needed.**
- **The organizations and individuals responsible for maintaining infrastructure and providing services.**

- **The capability of responsible organizations and individuals to meet the requirements of the population.**
- **Corruption and favoritism in the delivery of services.**
- **The expectations and perceptions of local communities regarding the provision of services made possible by functional infrastructure.**

7-52. The answers to these questions can help the commander prioritize infrastructure development projects, maximize existing resources, and potentially leverage external resources. Data collected during infrastructure reconnaissance can help answer these questions. Infrastructure reconnaissance as described in FM 3-34-170 results in the collection of the technical information on public systems, services, and facilities necessary to develop the situational understanding of local capability to support the infrastructure requirements of local populace within a specific area. Table 7-6 shows the intelligence staff where to find this information (*memory aid is SWEAT-MSO*.) Additional sources of information are local nationals, local government officials, NGOs, and IGOs.

7-53. When assessing economic and infrastructure conditions, the intelligence staff conducts an analysis of the economic and infrastructure conditions within a targeting area during initial IPB in order to focus the commander and staff on these problem sets during the remainder of planning. This analysis is briefed during the intelligence portion of the mission analysis/*problem framing* briefing and included as part of the intelligence estimate issued with the OPLAN and/or OPORD. Additionally, in order to support continued operations, this analysis is continually updated to ensure planning teams and assessment working groups have the most current data.

Table 7-6. Information sources for supporting infrastructure development (*SWEAT-MSO*)

Infrastructure category	*Staff proponent*	*Information sources*
SEWAGE	Engineer	Engineer reconnaissance teams, infrastructure survey teams, scouts, and combat patrols.
WATER	Engineer	Same as Sewage.
ELECTRICITY	Engineer	Same as Sewage.
ACADEMICS	Civil Affairs/*G-3/S-3*	Civil Affairs teams/*G-3/S-3.*
TRASH	Engineer	Same as Sewage.
MEDICAL	Medical Services	Civil Affairs teams/*G-3/S-3.*
SAFETY	Military Police	Same as Sewage.
OTHER:		
Roads and railroads	Engineer	Same as Sewage.
Bridges and waterways	Engineer	Same as Sewage.
Airports	Engineer	Same as Sewage.
Housing	Engineer	Same as Sewage.
Communications	Engineer	Same as Sewage.
Food supply	Civil Affairs/*G-3/S-3*	Civil Affairs teams/*G-3/S-3.*
Hazardous materials	Engineer	Same as Sewage.
Population concerns related to all above	Civil Affairs/*G-3/S-3*	Civil Affairs teams and human terrain teams/*foreign area officers, regional affairs officers, and other cultural enablers.*

UNDERSTANDING THE POPULATION

7-54. Counterinsurgency and stability tasks are conducted in and around populations. These populations can aid or hinder friendly operations. Understanding these populations aids all aspects of counterinsurgency and stability planning and operations.

7-55. In general, when conducting counterinsurgency operations and stability tasks, people are the decisive point/*center of gravity* and the key terrain for both threat/*adversary* and friendly forces.

7-56. IPB aids the understanding of populations (people) through the analysis of civil considerations as discussed in part one of this publication. Understanding the population aids the commander in developing a plan that can separate the population from the insurgents and gain the support of the population for the host-nation government and its security forces, including U.S. forces. Intelligence requirements associated with understanding the population are as follows:

- **Identify and define the dominant and secondary cultures within the host-nation society.**
- **Determine how the society—groups, institutions, organizations, and networks—functions (social network analysis).**

7-57. Counterinsurgency and stability tasks are conducted in and around populations. These populations can aid or hinder friendly operations. Understanding these populations aids all aspects of counterinsurgency and stability planning and operations.

7-58. In general, when conducting counterinsurgency operations and stability tasks, people are the decisive point/*center of gravity* and the key terrain for both threat/*adversary* and friendly forces.

7-59. IPB aids the understanding of populations (people) through the analysis of civil considerations as discussed in part one of this publication. Understanding the population aids the commander in developing a plan that can separate the population from the insurgents and gain the support of the population for the host-nation government and its security forces, including U.S. forces. Intelligence requirements associated with understanding the population are as follows:

- **Identify and define the dominant and secondary cultures within the host-nation society.**
- **Determine how the society—groups, institutions, organizations, and networks—functions (social network analysis).**
- **Identify language:**
  - **Identify the languages spoken by the host-nation society, the insurgents, and multinational security forces.**
  - **Identify social manners, behaviors, and nonverbal cues that can aid in communicating with the population through interpreters.**
- **Identify power and authority:**
  - **Determine how formal and informal power and authority are apportioned within the society:**
    - **Formal power and authority: central government, local government, government agencies.**
    - **Informal power and authority: political parties; political interest groups; unions; and religious, tribal, and ethnic groups.**
  - **Determine how each formal and informal power holder acquires, maintains, and uses power to attract and maintain followers—**
    - **Through the use of coercive force.**
    - **Through the expenditure of social capital (reciprocity and exchange, patron-client relationships).**
    - **Through the application of economic power.**
  - **Consider the state of the formal economic system (weak or strong, supplanted or supported by an informal economic system).**
  - **Consider the state of any informal economic systems (smuggling, black market, barter and exchange, tribal or clan networks).**
  - **Determine how the primary and secondary cultures in the society perceive their interests.**

- **Determine security:**
  - **Do these cultures believe they are safe from harm?**
  - **Do these cultures have faith in the police, the military, and the judiciary?**
- **Identify basic necessities: Are these groups satisfied with the availability of—**
  - **Food.**
  - **Water.**
  - **Clothing.**
  - **Shelter.**
  - **Medical treatment.**
- **Identify economic well-being: Are these groups optimistic about long-term economic viability for themselves and their children?**
- **Identify political participation: Do these groups believe they are part of, and can affect change, within the political process?**

Chapter 8

IPB Considerations for Unique Activities, Tasks, and Processes

IPB SUPPORT TO PROTECTION/*FORCE PROTECTION*

8-1. Protection relates to those actions taken by commanders to preserve the force so they can apply maximum combat power. Preserving the force includes protecting personnel (combatants and noncombatants), physical assets, and information of the United States and multinational military and civilian partners. The protection warfighting function facilitates the commander's ability to maintain the force's integrity and combat power.

8-2. Intelligence personnel may support command protection/*force protection* programs by identifying, collecting, reporting, analyzing, and disseminating intelligence regarding foreign threats to the Army. Inside the United States, intelligence personnel must limit collection to foreign intelligence and international terrorism threat data. Criminal and domestic terrorism threat information is restricted to law enforcement agencies.

8-3. Protection determines the degree to which potential threats/*adversaries* can disrupt operations and counters or mitigates those threats/*adversaries*. Emphasis on protection increases during preparation and continues throughout execution including in-transit (fort-to-port), redeployment, and home-station operations. Protection is a continuing activity; it integrates all protection capabilities to safeguard bases, secure routes, and protect forces. Supporting tasks that routinely require IPB support include the following:

- **Apply antiterrorism measures.**
- **Implement operations security.**
- **Implement information protection/*information security*.**
- **Conduct operational area security.**
- **Coordinate air and missile defense.**
- **Conduct personnel recovery operations.**
- **Conduct force health protection operations.**

APPLY ANTITERRORISM MEASURES

8-4. For U.S. Army, terrorism is the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (U.S. Code, Title 18, Section 2331). *For the Marine Corps, terrorism is the unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political (JP 3-07.2).* U.S. Code, Title 22, Section 2656f, defines terrorism as premeditated politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents. The Army/*Marine Corps* adds to this definition by recognizing that terrorist groups will target U.S. forces as well as noncombatants.

8-5. Antiterrorism is defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces (JP 3-07.2). It is an element of protection and a consideration during planning and operations. During IPB, the staff identifies potential terrorist threats and other threat activities. Based on this analysis, the staff recommends actions to reduce vulnerabilities to terrorist acts and attacks. Additionally, based on the analysis of terrorist organizations and

capabilities conducted during IPB, the staff develops plans and orders to counter terrorist attacks. Intelligence requirements generally associated with antiterrorism are—

- Identify the individual components (organization) of terrorist networks operating in the AO and area of interest: direct action cells, support cells, intelligence cells, command and control cells, financiers, and others.
- Determine the goals and objectives associated with each network.
- Determine the strengths and weaknesses within each network.
- Identify the HVTs and individuals associated with each network.
- Determine the location of each of the components of the network.
- Identify the targets each network will attack.
- Identify the TTP the networks will employ to conduct their operations.
- Determine the friendly resources and activities that need protection from terrorist attack in order to accomplish the mission.
- Determine what types of actions the force can take to mitigate terrorist attacks on noncombatants.

IMPLEMENT OPERATIONS SECURITY

8-6. JP 3-13.3 defines operations security as a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities that can be observed by *adversary* intelligence systems. Criticality, vulnerability, and threat assessments conducted by counterintelligence personnel contribute to IPB support to operations security. This information should be included into a threat/*adversary* vulnerability assessment. Intelligence requirements associated with operations security are—

- Identify essential elements of friendly information:
  - Locations of headquarters elements.
  - Location and activities of assets critical to operational success.
  - Information collection/*intelligence collection*.
  - Fires.
  - Engineer.
  - Sustainment.
  - Information related to friendly force operations.
  - Information related to friendly strengths and weaknesses.
  - Other information as required based on mission.
- Identify indicators associated with the conduct of friendly operations. The same type of indicators associated with threat/*adversary* operations apply to friendly operations. (See chapter 7 for indicators associated with offensive, defensive, and stability tasks.)
- Identify threats to critical resources, information, and personnel:
  - Identify threat/*adversary* information collection assets/*intelligence collection assets*.
  - Determine threat/*adversary* capability to detect and attack friendly critical resources, assets, and personnel.

IMPLEMENT INFORMATION PROTECTION

8-7. Information protection are those active or passive measures used to safeguard and defend friendly information and information systems. Information protection comprises information assurance, defensive cyberspace operations, and electronic protection. *Marine Corps uses the joint term "information security," which is the security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information that is authorized protection by executive order, statute, or regulation. Information security includes protection of classified, controlled unclassified, and sensitive compartmented information.*

Information Assurance

8-8. Information assurance is the protection and defense of information and information systems on data networks and computer systems. Intelligence requirements associated with information assurance are—

- **Identify the structure of the friendly communications network.**
- **Identify potential threats to the network.**
- **Identify vulnerabilities within the network.**

Defensive Cyberspace Operations

8-9. Computer network defense utilizes defensive cyberspace operations to protect against unauthorized activity. Computer network defense includes monitoring, detection, analysis, response, and restoration activities. Intelligence requirements associated with computer network defense are—

- **Identify threat/*adversary* organization capabilities to disable, corrupt, or compromise friendly information systems.**
- **Identify internal threats/*insurgencies* that can disable, corrupt, or compromise friendly information systems.**

Electronic Protection

8-10. Electronic protection involves actions such as communications avoidance or anti-jamming measures to protect personnel, facilities, and equipment from friendly and enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Intelligence requirements associated with electronic protection are—

- **Identify threat/*adversary* electronic surveillance capabilities.**
- **Identify threat/*adversary* electronic attack capabilities.**

CONDUCT PERSONNEL RECOVERY OPERATIONS/*TACTICAL RECOVERY OF AIRCRAFT AND PERSONNEL*

8-11. The U.S. Army conducts personnel recovery operations that are conducted to recover and return Soldiers, Army civilian personnel, selected Department of Defense contractors, and other personnel as determined by the Secretary of Defense who are isolated, missing, detained, or captured. Intelligence requirements associated with personnel recovery are the same as those for any operation—determining the effects of enemy, terrain, weather, and civil consideration in the area friendly forces are conducting personnel recovery operations. Intelligence requirements also include information on isolated, missing, detained, or captured personnel needing recovery similar to the requirements in a noncombatant evacuation operation and includes—

- **Identifying the location, disposition, capabilities, and possible COAs for all enemy forces.**
- **Anticipating the number of isolated, missing, detained, or captured personnel (total number by area) categorized by medical status.**

8-12. *The U.S. Marine Corps participates and/or supports combat search and rescue. It conducts tactical recovery of aircraft and personnel (TRAP). TRAP includes rescue or extraction, by surface or air, of downed aircraft and/or personnel and equipment; aircraft sanitation; and advanced trauma life support in a benign or hostile environment. (See MCDP 1-0 for more information on TRAP.)*

CONDUCT FORCE HEALTH PROTECTION OPERATIONS

8-13. Throughout history, the number of casualties sustained from disease and nonbattle injuries have far outweighed the number of combat casualties, thereby reducing the operational effectiveness of military forces. Disease and nonbattle injuries may be the result of endemic and epidemic diseases. Table 8-1 on page 8-4 lists some examples of these types of injuries.

Table 8-1. Examples of types of non-combat-related injuries

Disease	*Health threat*	*Stressors*	*Plants*	*Animals*	*Accidents*
• Arthropod • Waste • Waterborne	• Occupational • Environmental • Extreme heat • Extreme cold • Altitude • Toxic industrial materials • Radiation: (ionizing and non-ionizing) • Hazardous noise	• Psychological • Physiological (from traumatic and/or continuous operations)	• Poison ivy • Poison oak	• Insects • Venomous snakes • Spiders	• Self-inflicted wounds • Injuries from accidents • Injuries from recreational activities

8-14. Intelligence requirements associated with force health protection include—

- **Location of facilities that use or manufacture toxic industrial materials (such as research laboratories, gas stations, refineries, or chemical plants).**
- **Location and operational status of sanitation facilities and services (waste disposal facilities, water treatment plants and services, such as trash pickup and landfills).**
- **Types and locations of medical facilities (clinics, hospitals, medical training facilities, research facilities).**
- **Types of transportation available to move patients from point of injury, incident site, or between hospital facilities (dedicated evacuation platforms versus vehicles of opportunity).**
- **Leading causes of death, birth rates, nutrition status, and accessibility to medical care for the local population.**
- **Displaced persons camps to include camp leaders, sanitation facilities, and nutrition status.**

IPB SUPPORT TO BUILDING PARTNERSHIP CAPACITY/ *ESTABLISHING GENUINE PARTNERSHIPS*

8-15. Operations may require inter-organizational efforts to build the capacity of partners to secure populations, protect infrastructure, and strengthen institutions as a means of protecting common security interests. The intelligence requirements associated with building partnership capacity are normally the same as those associated with stability operations.

8-16. ***For the Marine Corps when establishing genuine partnerships, partnership is an arrangement between U.S. and host-nation forces in which they operate together to achieve mission success while building capability and capacity. Partnership requires mutual respect despite the differences in size, skill, training, capability or culture of the partnering forces. (See MCDP 1-0 for more information on establishing genuine partnerships.)***

SMALL-SCALE JOINT OPERATIONS

8-17. Small-scale joint operations are executed to achieve an end state that is clearly defined and limited in scope. They are normally conducted by joint task forces. Examples of small-scale joint operations that Army/*Marine Corps* forces may participate in are noncombatant evacuations, raids, show of force, FHA, sanction enforcement, and elimination of weapons of mass destruction.

8-18. However, the threat of terrorist attack is possible as are attacks from the general population. During these types of operations, the commander is primarily concerned with protection, operations security, and targeting operations. Threat/*adversary* resolution is normally not clear. It usually consists of terrorist, guerilla, paramilitary, political, or religious groups opposing an established government that is being supported by the U.S. Government. These groups are usually not well-defined at the tactical level and are probably un-located. Echelon-above-brigade intelligence organizations/*high-level unit intelligence*

organizations and host-nation agencies generally will not provide the resolution required to satisfy the CCIRs, but they can provide enough information initially to focus information collection operations/*intelligence collection operations.*

PEACE OPERATIONS

8-19. Peace operations is a broad term that encompasses multiagency and multinational crisis response and limited contingency operations. The primary purpose of peace operations is to create a safe and secure environment, deter *adversaries* from overt actions against each other, and provide time for civilian agencies to generate a self-sustaining peace. Peace operations include peacekeeping, peace building, peacemaking, peace enforcement, and conflict prevention. Peace operations normally occur in complex environments and are characterized by irregular forces, a failing government, absence of the rule of law, terrorism, human rights abuses, collapse of civil infrastructure, and the presence of dislocated civilians.

8-20. Attacks by insurgent and terrorist groups are likely, and U.S. forces may have to conduct limited offensive tasks in accordance with rules of engagement against these groups in support of stability tasks. Enemy forces will try to mitigate U.S. information collection/*intelligence collection* capability by adopting command and control; maneuver; fires, intelligence; and logistics TTP that reduce their signature and vulnerability to U.S. collection systems. When conducting IPB and developing a collection plan, the commander considers the enemy's ability to develop low-cost, low-technology counter-information collection solutions/*intelligence collection solutions.*

IRREGULAR WARFARE

8-21. Irregular warfare is a violent struggle among state and non-state actors for legitimacy and influence over a population. It differs from conventional operations in two aspects. First, it is warfare among and within the people. Second, it emphasizes an indirect approach. Irregular warfare avoids direct military confrontation. Instead, it combines irregular forces and indirect unconventional methods to exhaust the opponent.

8-22. Types of operations the unit may be employed in to counter irregular warfare are foreign internal defense, support to insurgency, counterinsurgency, combating terrorism, and irregular warfare. Traditionally, these missions are conducted by Special Forces. However, if Special Forces and host-nation forces cannot defeat irregular threats or *adversaries*, conventional friendly forces can assume the lead role. Operation Iraqi Freedom and Operation Enduring Freedom are good examples of this.

8-23. Just as in limited interventions and peace operations, U.S. forces will generally be opposed by an undefined and un-located enemy that operates within complex terrain. The tactics and operational art employed by these forces will vary from conflict to conflict as will the structure of the threats/*adversaries* themselves. In most cases, current intelligence doctrine will not provide all of the tools the unit needs to counter these threats. When this occurs, commanders will have to modify doctrine and develop methods that work in the moment.

8-24. In addition to operations discussed previously, the Army/*Marine Corps* participates in other operations. Examples include multinational training exercises, security assistance, joint combined exchange training, recovery operations, arms control, and counterdrug operations. Combat is not likely during these operations, but terrorist attacks are always possible; force protection and operations security are two of the commander's primary intelligence concerns. U.S. national and theater intelligence agencies will provide the initial analysis and information collection/*intelligence collection* support to units preparing for these missions. Additionally, these units may receive limited support from host-nation agencies. The commander and staff should consider both of these sources of information when planning for operations.

This page intentionally left blank.

Chapter 9

IPB Considerations for Unique Environments

IPB CONSIDERATIONS FOR AN URBAN ENVIRONMENT

9-1. An urban operation is a military operation where manmade construction and high population density are the dominant features. FM 3-06 constitutes Army doctrine for urban operations and discusses IPB considerations in detail. (*For the Marine Corps, see MCWP 3-35.3 for additional information on military operations on urbanized terrain.)* JP 3-06 also provides extensive discussion on IPB in the urban environment.

9-2. Chapter 4 of this publication discusses terrain analysis conducted for both natural and urban terrain. This section discusses intelligence requirements normally associated with planning considerations for urban operations. The primary terrain effect when operating in an urban environment is the multidimensional nature of the environment. Urban areas are a blend of horizontal, vertical, interior, exterior, and subterranean forms superimposed on the natural relief, drainage, and vegetation. The characteristics of urban environments affect friendly and enemy forces based on their doctrine and tactics. IPB in urban operations evaluates the effect of the characteristics of the urban environment on both.

UNIQUE URBAN CHARACTERISTICS

9-3. Offensive and defensive tasks/*operations* and stability tasks are the three types of operations conducted by the Army/*Marine Corps* in urban environments. Chapter 7 discusses IPB for these three types of operations. In addition to the general intelligence requirements associated with IPB, urban environment in IPB emphasizes the effects of the following characteristics:

- **An urban area is a topographical complex where manmade construction or high population density is the dominant feature. Evaluation of urban areas during IPB is directed on the physical aspects of the area and their effects on operations. This approach is effective when population density is not a factor in the operation. Chapters 3 and 4 discuss how to evaluate the physical aspects of urban terrain and associated civil considerations.**
- **An urban environment includes the physical aspects of the urban area as well as the complex and dynamic interaction and relationships between its key components—the terrain (natural and manmade), the society, and the supporting infrastructure—as an overlapping and interdependent system of systems. This approach is necessary when population density is a factor in the operations. Chapter 7 discusses IPB support to stability tasks.**

EVALUATING THE MILITARY ASPECTS OF THE TERRAIN IN AN URBAN ENVIRONMENT

9-4. Evaluating the effects of terrain in an urban environment differs in many respects from that of open terrain. The analysis of the five military aspects of terrain defined in the OAKOC/*KOCOA* considerations still applies. This analysis, however, must be in the context of urban battlefield/*battlespace* characteristics.

9-5. A standard MCOO developed from a military map will not be of much use to leaders at the company level and below. Standard military maps do not have the detail required to allow a thorough analysis of urban terrain. Many standard military maps are old and do not reflect the more recent buildings, streets, and sometimes significant urban growth. In addition, standard maps do not show the subsurface aspects of the urban environment: sewers, subways, and underground water systems. While these military maps show key public buildings and areas such as hospitals, clinics, stadiums, and parks, they do not clearly identify the water facilities, communication facilities, fuel supply, storage facilities, and temporary conditions (for example, construction sites).

9-6. Terrain analysis software is available to assist in analyzing urban terrain. Familiarization with terrain analysis products and what they can provide assists the G-2/S-2 in explaining and coordinating with geospatial engineers the units' needs in better tailored urban terrain products. A number of sources of information are available such as the U.S. Army Engineer School Reachback Operations Center and National Geospatial-Intelligence Agency, which provide specific types of imagery products, 3-dimensional maps, and types of products to overlay demographics on an urban map.

9-7. The Center for Army Lessons Learned has documented over 10 years of terrain analysis techniques that are available based off products that were developed from urban operations from multiple campaigns such as Operation Iraqi Freedom, Horn of Africa, Philippines, and from hurricane responses. (See FM 3-34.170/*MCWP 3-17.4* for additional information on geospatial engineering and for urban considerations such as sewage, water, electricity, academics, trash, medical, safety, and other *[SWEAT-MSO]* considerations).

9-8. Terrain analysis is done on maps or other imagery that contains this information. Additionally, while conducting terrain analysis for an entire city may be effective for major combat operations/*major operations,* it is not useful for the types of operations associated with stability tasks. In stability tasks, analysis focuses on the requirements of small units (squad, platoon, and company) to move from an operating base to an objective. (Chapter 4 fully discusses the evaluation of terrain effects on operations.)

IPB CONSIDERATIONS FOR A COLD WEATHER OR MOUNTAIN ENVIRONMENT

9-9. In addition to the general requirements associated with IPB, cold weather or mountain environment in IPB emphasizes the effects of cold on personnel and material, the effects of the winter environment on friendly and enemy operations, and planning considerations unique to the winter battlefield/*battlespace* and cold regions. The primary consideration when planning military operations in this type of environment is time. In addition to the increased amount of time consumed in actual movement, allowance must be made for other time-consuming tasks that are not present in temperate zone operations. These include, among others, erecting and striking tents, performing maintenance, constructing roads, starting and warming engines, moving supplies, and hundreds of other small tasks that must be performed while wearing bulky cold weather clothing.

Note. **While not normally considered when conducting IPB, time allowances need to be emphasized in cold weather operations.**

9-10. Mountain terrain is characterized by steep slopes, great variations in relief, natural obstacles, and a lack of accessible routes—all of which can restrict mobility, increase movement times, limit the effectiveness of some weapons and equipment, and complicate sustainment operations. This physically challenging terrain is the primary terrain effect in cold weather or mountain operations and affects operations in greater detail than it does in temperate or desert environments. Like other regions of the world, mountainous terrain has native inhabitants that can be hostile if not treated properly. To prevent conflict, these inhabitants should be treated as friends and have their customs, taboos, privacy, and property respected.

UNIQUE COLD WEATHER OR MOUNTAIN CHARACTERISTICS

9-11. Offensive and defensive tasks/*operations* are the two types of operations conducted by U.S. forces in mountain environments. Chapter 7 discusses IPB for these two types of operations. (See FM 3-97.6/*MCWP 3-35.1* for a detailed discussion on mountain operations.) In addition to the general intelligence requirements associated with IPB, a mountain environment in IPB emphasizes the effects the following characteristics have on operations:

- **Cold**
- **Altitude.**
- **Slope.**
- **Relief.**
- **Natural obstacles.**
- **Movement routes.**
- **Blowing snow and fog.**

Cold

9-12. Temperature is the primary terrain effect in cold weather or mountain operations and has the ability to affect operations to a greater detail than it does in temperate or desert environments. In a cold weather environment the effects of weather are directly tied to the use of clothing. The use of cold weather clothing is affected by two types of weather conditions: wet and dry. These conditions are amplified by humidity, coupled with temperature and wind velocity; high humidity (wet conditions); and low humidity (dry conditions).

9-13. Cold-dry conditions occur when average temperatures are lower than 14 degrees Fahrenheit. The ground is usually frozen and snow is usually dry in the form of fine crystals. Strong winds cause low temperatures to seem colder and increase the need for protection of the entire body (wind chill). During these periods, troops should have available additional insulating layers of clothing. This is particularly true when entering static situations from a period of strenuous exercise. Cold-wet conditions also occur when temperatures are near freezing and variations in day and night temperatures cause alternate freezing and thawing. This freezing and thawing is often accompanied by rain and wet snow, causing the ground to become muddy and slushy. During these periods troops should wear clothing that consists of a water-repellent, wind-resistant outer layer and inner layers with sufficient insulation to provide ample protection in moderately cold weather (above 14 degrees Fahrenheit). (See FM 3-97.6/*MCWP 3-35.1* for a detailed discussion on cold conditions in this unique environment.)

Altitude

9-14. The primary effect of mountainous terrain on personnel is exhaustion caused by altitude. The lack of oxygen at high altitudes negatively affects both the mind and the body. This effect is compounded by the rigorous physical activity necessary to move through the terrain. Additionally, factors such a Soldier's/*Marine's* age, fatigue-level, physical conditioning, previous injury, illness, diet, and use of medications can magnify the effect mountainous terrain can have. As Soldiers/*Marines* ascend in altitude, the proportion of oxygen in the air decreases. Without proper acclimatization, this decrease in oxygen saturation can cause altitude sickness and reduced physical and mental performance.

9-15. Soldiers/*Marines* cannot maintain the same physical performance at high altitude that they can at low altitude, regardless of their fitness level. Exposure to altitudes over 3,000 meters can cause changes in senses, moods, and personality. Altitude also affects the lift capability of certain types of aircraft, reducing the load they can carry and, in some cases, preventing their use altogether. Additionally, decreased molecular density in high elevations results in an increase in fuel consumption necessary to gain and maintain lift.

Slope

9-16. In terrain analysis, slope indicates the steepness, incline, or grade. Mountain slopes generally vary between 15 and 45 degrees. Cliffs and other rocky precipices may be near vertical, or even overhanging. Aside from obvious rock formations and other local vegetation characteristics, actual slope surfaces are usually found as some type of relatively firm earth or grass. Grassy slopes may include grassy clumps known as tussocks, short alpine grasses, or tundra (the latter more common at higher elevations and latitudes).

9-17. Many slopes will be scattered with rocky debris deposited from the higher peaks and ridges. Extensive rock or boulder fields are known as talus. Slopes covered with smaller rocks, usually fist-sized or smaller, are called scree fields. Slopes covered in talus often prove to be a relatively easy ascent route. On the other hand, climbing a scree slope can be extremely difficult, as the small rocks tend to loosen easily and give way. However, this characteristic often makes scree fields excellent descent routes. Before attempting to descend scree slopes, commanders should carefully analyze the potential for creating dangerous rockfalls and take necessary avoidance measures.

9-18. In winter, and at higher elevations throughout the year, snow may blanket slopes, creating an environment with its own distinct effects. Some snow conditions can aid travel by covering rough terrain with a consistent surface. Deep snow, however, greatly impedes movement and requires Soldiers/*Marines* be well-trained in using snowshoes, skis, and over-snow vehicles.

9-19. Steep snow-covered terrain presents the risk of snow avalanches as well. Snow can pose a serious threat to Soldiers/*Marines* not properly trained and equipped for movement under such conditions. Avalanches have taken the lives of more Soldiers/*Marines* engaged in mountain warfare than all other terrain hazards combined. Another hazard is becoming "snowblind" due to the snow's high reflectivity value, or albedo. This condition results when solar radiation reflects off the snow and into the eyes of personnel in a snow-covered area. The effect is identical to a sunburn, and all exposed body parts are susceptible to this hazard.

9-20. Commanders operating in arctic and subarctic mountain regions, as well as the upper elevations of the world's high mountains, may be confronted with vast areas of glaciation. Valleys in these areas are frequently buried under massive glaciers and present additional hazards, such as hidden crevices and ice and snow avalanches. The mountain slopes of these peaks are often glaciated and their surfaces are generally composed of varying combinations of rock, snow, and ice. Although glaciers have their own peculiar hazards requiring special training and equipment, movement over valley glaciers is often the safest route through these areas. (ATTP 3-97.11, FM 3-97.6, and *MCWP 3-35.1* contain more information on avalanches and glaciers and their effects on operations.)

Relief

9-21. Relief is the vertical and horizontal dimension of land surface. Mountains are generally classified according to relief. Mountains are commonly classified as low or high, depending on their local relief and, to some extent, elevation. Low mountains have a local relief of 300 to 900 meters (1,000 to 3,000 feet) with summits usually below the timberline. High mountains have a local relief usually exceeding 900 meters (3,000 feet) and are characterized by barren alpine zones above the timberline.

Natural Obstacles

9-22. Natural obstacles associated with mountain terrain include deep defiles, cliffs, rivers, landslides, avalanches, crevices, scree slopes, and areas of dense vegetation or deadfalls, as well as the physical terrain of the mountain itself.

Movement Routes

9-23. Movement routes associated with mountain terrain include manmade and animal trails, streambeds, and the bottom and top of ravines, as well as exiting LOCs.

Blowing Snow and Fog

9-24. Because of the potential of blowing snow and fog, defensive positions are located on high ground, thus forcing the enemy to attack uphill in deep snow. Each weapon is assigned a field of fire oriented at man-height level on the likely enemy approaches. This increases the likelihood of effective fire during periods of restricted visibility caused by blowing snow and fog. Ice or vapor fogs are common in extreme low temperatures. Such fogs are primarily the result of natural phenomena, but also result from many other causes such as vehicle exhausts, cooking, breathing, and weapons firing. Fogs of this nature hang overhead and could be clear markers of a position. They will also limit visibility.

9-25. The observed fire of automatic and direct fire weapons is handicapped considerably by the fog, smoke, and whirling snow caused by muzzle blast. Placing observers away from the weapons positions may be necessary to control the fire. Placing tarpaulins under the guns, or packing or icing the snow, assists in reducing the effect of muzzle blast. Pauses in firing or change of position may be necessary in order to obtain better fire effect.

EVALUATING THE MILITARY ASPECTS OF THE TERRAIN IN A MOUNTAIN ENVIRONMENT

9-26. Paragraphs 9-27 through 9-33 describe how terrain affects operations in a mountain environment. This discussion follows the outline of the terrain analysis process summarized by the OAKOC/*KOCOA* considerations.

Observation and Fields of Fire

9-27. Although mountainous terrain generally permits excellent long-range observation and fields of fire, steep slopes and rugged terrain affect a Soldier's/*Marine's* ability to accurately estimate range and cause large areas to be hidden from observation. The existence of sharp relief and dead space facilitates unobserved approaches, making surveillance difficult despite long-range observation. Four factors that influence what can be seen and hid in mountainous terrain are—

- **The ability to observe and identify targets in conditions of bright sunlight.**
- **The ability to estimate range in clear air.**
- **The ability to apply wind corrections.**
- **The ability to shoot accurately up and down vertical slopes.**

Avenues of Approach

9-28. In mountainous terrain, there are few easily accessible AAs, and they usually run along valleys, defiles, or the crests and spurs of ridges. This type of geography allows the defender to economize in difficult terrain and to concentrate on dangerous AAs. A typical offensive tactic is to conduct a coordinated assault with the main effort along accessible AAs, and supporting efforts by one or more maneuver elements on difficult and unexpected AAs.

9-29. Normally, high rates of advance and heavy concentration of forces are difficult or impossible to achieve along mountainous AAs. Relief features may create large areas of dead space that facilitate covert movement. Units may use difficult and unlikely AAs to achieve surprise; however, these are extremely high-risk operations and are prone to failure unless forces are well trained and experienced in mountaineering techniques. In mountainous terrain, the analysis of AAs are based on a thorough reconnaissance and evaluated in terms of the following factors:

- **Ability to achieve surprise.**
- **Vulnerability of attack from surrounding heights.**
- **Ability to provide mutual support to forces attacking on other AAs.**
- **Effect on rates of march.**
- **Increase in the number of litter patients and requirements for litter bearers.**
- **Effect on command and control.**
- **Ability to support sustainment operations.**

- Access to secure rest and halt sites.
- Potential to fix enemy forces and reduce the possibility of retreat.

Key Terrain

9-30. Key terrain generally increases in importance with an increase in elevation and a decrease in accessibility. In the mountains, however, terrain that is higher than that held by the enemy force is often key, but only if the force is capable of fighting there. A well-prepared force capable of maneuver in rugged terrain can gain an even greater advantage over an ill-prepared enemy at higher elevation levels.

9-31. The vast majority of operations in the mountains require that the commander designate decisive terrain in his concept of operations to communicate its importance to his staff and subordinate commanders. In operations over mountainous terrain, the analysis of key and decisive terrain is based on the identification of these features at each of the three operational terrain levels. There are few truly impassable areas in the mountains. Commanders recognize that what may be key terrain to one force may be an obstacle to another force. They also recognize that properly trained combatants can use high obstructing terrain as a means to achieve decisive victories with comparatively small-sized combat elements.

Obstacles

9-32. As stated in paragraph 9-17, obstacles associated with mountain terrain include deep defiles, cliffs, rivers, landslides, avalanches, crevices, scree slopes, and areas of dense vegetation or deadfalls, as well as the physical terrain of the mountain itself. Obstacles vary in their effect on different forces. Evaluation of obstacles considers the degree to which obstacles restrict operations, and at the ability of friendly and enemy forces to exploit the tactical opportunities that exist when obstacles are employed. Manmade obstacles used in conjunction with restrictive terrain are extremely effective in the mountains; however, their construction is costly in terms of time, materiel, transportation assets, and labor. Commanders need to know the location, extent, and strength of natural obstacles so they can be incorporated into their scheme of maneuver.

Cover and Concealment

9-33. The identification and proper use of the cover and concealment provided by mountainous terrain is fundamental to all aspects of mountain operations. The ridge systems found in mountainous terrain may provide unobserved approaches through many areas that are hidden from observation by the vegetation and relief. The difficulties a force encounters in finding available cover and concealment along ridges are fewer than those on the peaks, especially above the timberline. Uncovered portions of an approach leave a force exposed to observation and fire for long periods. A defending force can easily detect movement in this region, leaving an attacking force with three primary options to improve cover and concealment:

- Identify and exploit AAs the defender would consider unlikely because of the difficulty of ascent and descent.
- Conduct movement during periods of restricted visibility.
- Employ overwhelming route security.

IPB CONSIDERATIONS FOR A JUNGLE ENVIRONMENT

9-34. FM 90-5 defines a jungle environment as an area where all seasons are nearly alike. FM 90-5/*FMFM 7-28* divides jungle environments into two zones: those areas close to the equator and those areas away from the equator. In areas close to the equator, rains occur throughout the year. In areas away from the equator, jungles have distinct wet and dry seasons. Both zones have high temperatures (averaging 78 to 95+ degrees Fahrenheit), heavy rainfall (400+ inches annually), and high humidity (90 percent) throughout the year.

9-35. Jungle environments are comprised of densely forested areas, grasslands, cultivated areas, and swamps. The vegetation in the jungle diminishes the ability to see. The jungle canopy compounds this issue by preventing ambient light from penetrating. As a result, night observation devices are mostly ineffective under the canopy. Dense vegetation also limits the ability to hear by trapping noise. The potential lack of

road networks and areas that are impassable to vehicles seriously degrade mounted operations. Casualties who would be ambulatory in other types of terrain will become litter patients in the jungle as they are unable to navigate difficult terrain. This will significantly increase evacuation times and will necessitate diverting some troops to become litter bearers.

9-36. High incidences of rust, corrosion, and fungal infestation caused by high humidity and moisture force strict daily maintenance on weapons and equipment. The jungle climate, relief, and foliage combine to reduce the effective range of radio communication and electronic surveillance. Civil considerations are generally not a major factor when planning and conducting jungle operations, although the existence of noncombatants in the area must be considered, consistent with planning offensive and defensive tasks/*operations*. Like other regions of the world, the jungle has native inhabitants that can be hostile if not treated properly. To prevent conflict, these inhabitants should be treated as friends and have their customs, taboos, privacy, and property respected.

UNIQUE JUNGLE ENVIRONMENT CHARACTERISTICS

9-37. Offensive and defensive tasks/*operations* are the two types of operations conducted by U.S. forces in jungle environments. Chapter 7 discusses IPB for these two types of operations. (See FM 90-5/*FMFM 7-28* for details on jungle environment conditions.) In addition to the general intelligence requirements associated with IPB, a jungle environment in IPB emphasizes the effects the following characteristics have on operations:

- Mosquitoes, sandflies, and other insects.
- Leeches.
- Poisonous snakes.
- Crocodiles and caymans.
- Wild animals.
- Poisonous vegetation.
- Waterborne diseases.
- Fungal diseases.

EVALUATING MILITARY ASPECTS OF THE TERRAIN IN A JUNGLE ENVIRONMENT

9-38. Paragraphs 9-39 through 9-43 describe how terrain affects operations in a jungle environment. This discussion follows the outline of the terrain analysis process summarized by the OAKOC/*KOCOA* considerations.

Observation and Field of Fire

9-39. Observation and fields of fire in the jungle are limited because of dense vegetation. Often, observation and fields of fire must be created or improved upon. When this is necessary, Soldiers/*Marines* clear away only what is absolutely necessary in order to retain as much natural concealment as possible. When in properly constructed fighting or observation positions, the Soldier's/*Marine's* eyes and weapon will be at ground level. In this way, the Soldier/*Marine* is concealed from the enemy, is protected by cover, but still can detect any approaching enemy. If a small tree is in a Soldier's/*Marine's* field of fire, only the branches that deny observation should be removed. The cuttings on the tree are darkened with mud. Overly cleared areas or fresh, improperly concealed cuttings are easy to spot. Additionally, restricted lines of sight can prevent visual contact between units, interlocking fires, and the use of tube-launched optically tracked munitions. Adjustment of indirect fire support is difficult due to limited visibility and may have to be accomplished by sound.

Avenues of Approach

9-40. Moving over jungle terrain is difficult because of the lack of clear AAs or routes. There may not be adequate topography survey or map data to identify AAs during planning because of the isolation of jungle environments, the rugged ground, and the presence of a canopy and dense forest. When using aerial photography to identify AAs, these photographs should be less than four months old because trails and

other clearings can be overgrown during that time. In many cases, AAs may need to be created. The use of indigenous people (military and civilian) to identify existing AAs and movement routes is an effective way to quickly identify these terrain features. AAs in the jungle include rivers, streams, valley floors, ridgelines, animal trails, and trails made by man. Because sound in the jungle does not travel far, movement along AAs is generally closer than believed.

Key Terrain

9-41. The aspects of terrain and enemy discussed above result in fewer set-piece battles. Rather than conventional attacks conducted against conventional defenses, jungle battles are more often ambushes, raids, and meeting engagements. Battles are not fought for high ground as frequently as conventional battles. Orientation is on the enemy rather than on the terrain. Hills in the jungle are often too thickly vegetated to permit observation and fire and, therefore, do not always qualify as key terrain. In the jungle, roads, rivers and streams, fording sites, and landing zones are more likely to be key terrain features.

Obstacles

9-42. Rivers and other large bodies of water as well as cliffs are the predominant natural obstacles in a jungle environment. Depending on the type of operation, swamps and heavily forested areas may become obstacles as well.

Cover and Concealment

9-43. Jungle terrain generally provides good concealment from both air and ground observation because of dense vegetation. Natural cover (trees, rocks, logs) provides adequate cover from small arms fire but provides only minimal protection from grenades and indirect fire if not improved upon. When constructing fighting positions, ample natural resources are available to build cover that blends in with the surroundings. Lowland and swamp areas provide good concealment but poor cover because they are generally too wet to permit the digging of fighting positions. Tree limbs can block or deflect mortars, grenades, and small arms fire.

IPB CONSIDERATIONS FOR A DESERT ENVIRONMENT

9-44. FM 90-3/*MCWP 3-35.6* defines a desert environment as an arid, barren region incapable of supporting normal life due to lack of water. Temperatures vary according to latitude and season, from over 136 degrees Fahrenheit in the deserts of Mexico and Libya to the bitter cold of winter in the Gobi (East Asia). In some deserts, day-to-night temperature fluctuation exceeds 70 degrees Fahrenheit. Desert terrain also varies considerably from place to place, the sole common denominator being lack of water with its consequent environmental effects, such as sparse, if any, vegetation.

9-45. The basic land forms are similar to those in other parts of the world, but the topsoil has been eroded due to a combination of lack of water, heat, and wind to give deserts their characteristic barren appearance. The bedrock may be covered by a flat layer of sand or gravel, or may have been exposed by erosion. Other common features are sand dunes, escarpments, wadis, and depressions. Although civil considerations are generally not a major factor when planning and conducting desert operations, consider the impact of noncombatants in the area; consistent with planning offensive and defensive tasks.

UNIQUE DESERT ENVIRONMENT CHARACTERISTICS

9-46. Offensive and defensive tasks/*operations* are the two types of operations conducted by U.S. forces in desert environments. Chapter 7 discusses IPB for these two types of operations. In addition to the general intelligence requirements associated with IPB, a desert environment in IPB emphasizes the effects the following characteristics have on operations:

- Water.
- Terrain.
- Heat and cold.
- Wind.
- Dust and sand.

- **Humidity.**
- **Temperature variations.**
- **Thermal cross-over.**
- **Optical path bending.**
- **Static electricity.**
- **Solar radiation.**

Water

9-47. Although water can be found in the desert, and the location of known and possible water sources is identified during IPB, carrying enough water to accomplish the mission is a primary planning consideration when operating in the desert. This is because even though water is there it may be impossible to find or reach it. If water is accessible, it may not be potable. Also, dependency on local water sources can make movement predictable and expose the force to enemy attack. When planning how much water to carry, consider the following uses:

- **Personnel (drinking only).**
- **Personnel (uses other than drinking).**
- **Medical treatment.**
- **Vehicle and equipment cooling systems.**
- **Decontamination.**
- **Food preparation.**
- **Construction.**
- **Laundry.**

Terrain

9-48. Terrain varies from nearly flat with high trafficability, to lava beds and salt marshes with little or no trafficability. Tracked vehicles are well suited for desert operations. Wheeled vehicles may be acceptable as they can go many places that tracked vehicles can go; however, their lower speed average in poor terrain may be unacceptable during some operations. Vehicles should be equipped with extra fan belts, tires (and other items apt to malfunction), tow ropes (if not equipped with a winch), extra water cans, and desert camouflage nets. Air-recognition panels, signal mirrors, and a tarpaulin for crew sun protection are very useful.

Heat and Cold

9-49. Heat affects personnel as well as weapons and equipment. The extreme heat of the desert can cause heat exhaustion and heatstroke and puts troops at risk of degraded performance. For optimum mental and physical performance, body temperatures must be maintained within narrow limits. Therefore, it is important that the body loses the heat it gains during work. The amount of heat accumulation in the human body depends upon the amount of physical activity, level of hydration, and the state of personal heat acclimatization. Unit leaders must monitor their troops carefully for signs of heat distress and adjust schedules, work rates, rest, and water consumption according to conditions.

9-50. The desert can be dangerously cold, particularly at night. The dry air, wind, and clear sky can combine to produce bone-chilling discomfort and even injury. The ability of the body to maintain body temperature within a narrow range is as important in the cold as in the heat. Loss of body heat to the environment can lead to cold injury; a general lowering of the body temperature can result in hypothermia, and local freezing of body tissues can lead to frostbite. Hypothermia is the major threat from the cold in the desert, but frostbite also occurs. *This effect is mitigated by periods of extensive cloud cover—METOC forecasters will factor this into the planning in a desert environment during bivouac operations.*

Wind

9-51. Desert winds, by their velocity alone, can be very destructive to large and relatively light materiel, such as aircraft, tents, and antenna systems. To minimize the possibility of wind damage, materiel should be sited to benefit from wind protection and be firmly picketed to the ground. Desert winds also move dust and sand from the desert floor into sensitive areas of weapons and equipment, thus causing malfunction and damage.

Dust and Sand

9-52. Dust and sand are the greatest threats to the efficient functioning of weapons and equipment in the desert. It is almost impossible to avoid particles settling on moving parts and acting as an abrasive. Sand mixed with oil forms an abrasive paste that destroys the working of fine parts. The existence of dust and sand requires additional time and resources for maintenance in accordance with applicable maintenance manuals.

Humidity

9-53. Some deserts are humid. Where this is the case, humidity plus heat causes rust on bare metal and mold in enclosed spaces such as optics. Bare metal surfaces on equipment not required for immediate use must be kept clean and very lightly lubricated. Items such as optics should be stored in dry conditions; those in use are kept where air can circulate around them and should be purged at frequent intervals. Aircraft are washed daily, particularly if there is salt in the air, using low-pressure sprays.

Temperature Variations

9-54. Temperature variation is the change in ambient temperature between daytime and nighttime hours. In deserts with relatively high dew levels and high humidity, overnight condensation can occur wherever surfaces (such as metal exposed to air) are cooler than the air temperature. Condensation can affect such items as optics, fuel lines, and air tanks. Draining fuel lines both at night and in the morning (whenever necessary) and cleaning optics and weapons frequently can mitigate the effect of temperature variation.

Thermal Cross-Over

9-55. Thermal cross-over is the natural phenomenon that normally occurs twice daily when temperature conditions are such that there is a loss of contrast between two adjacent objects on infrared imagery. Small arms may be affected by thermal cross-over. Soldiers/*Marines* should modify direct fire control procedures, as needed. Modern U.S. tanks are designed to compensate for thermal cross-over. Enemy tanks may not have this capability.

Optical Path Bending

9-56. Optical path bending, also called refraction, occurs when light passes through one medium to another. This condition can exist when the air is warmer above the desert floor. Heat shimmer is an indication that refraction exists. Refraction can occur during daytime conditions with a clear sky over flat terrain with winds less than 10 miles per hour. Refraction can also occur during nighttime conditions with a clear sky over flat terrain with winds less than 4 miles per hour. Refraction can affect the ability of direct fire weapons systems to engage targets beyond 1,500 meters.

Static Electricity

9-57. Static electricity is the buildup of an electric charge on the surface of objects that remains until the charge is bleed off to a ground or neutralized by discharge. Static electricity is prevalent and poses a danger in the desert. It is caused by atmospheric conditions, coupled with an inability to ground out, due to dryness of the terrain. It is particularly prevalent with aircraft or vehicles having no conductor contact with the soil. The difference of electrical potential between separate materials may cause an electrical discharge between them when contact is made; if flammable gases are present, they may explode and cause a fire.

Solar Radiation

9-58. Solar radiation is generated by the sun's rays. Solar radiation can be detrimental to some plastics, lubricants, pressurized gases, chemicals, and infrared tracking and guidance systems. These materials must be kept out of constant direct sunlight to avoid damage. Over exposure to solar radiation can cause sunburn and damage eyesight. Soldiers/*Marines* need to implement personal protective measures such as applying sun screen and using sunglasses to avoid injury.

EVALUATING MILITARY ASPECTS OF THE TERRAIN IN A DESERT ENVIRONMENT

9-59. Paragraphs 9-60 through 9-64 describe how terrain affects operations in a desert environment. This discussion follows the outline of the terrain analysis process summarized by OAKOC/*KOCOA* considerations.

Observation and Fields of Fire

9-60. Observation and fields of fire are generally excellent in most desert areas. The atmosphere is stable and dry, allowing unrestricted view over vast distances. Flat desert terrain permits direct-fire weapons to be used to their maximum range. Open terrain and a predominantly clear atmosphere generally offer excellent long-range visibility; however, at certain times of the day visibility may be limited or distorted by heat. Additionally, the desert is not absolutely flat, so weapons are sited to provide mutual support. Dead space can also be a problem. Even though the landscape appears flat, upon close inspection it can be undulating with relatively deep wadis and depressions creating IVLs. These areas should be covered by indirect fire.

Avenues of Approach

9-61. AAs are not clearly defined in desert environments. AAs may be wider and of greater availability permitting maneuver from virtually any direction, making wide envelopments possible. Modern sensor technology, limited natural concealment, and improved observation make the element of surprise a challenge. In mountainous and canyon topography avenues are more limited, and the wadis and valleys are likely to be the only possible access routes. Any roads that do exist are probably in valleys.

Key Terrain

9-62. Key terrain in the desert can be manmade features, mountain passes, high ground, and/or valleys. Staff sections provide recommendations of key terrain so that these are analyzed for their benefit to friendly and enemy/*adversary* forces. For example, for the S-6, the only piece of high ground in the AO may be key due to the limitations of frequency modulation communications that require retransmission. Some deserts provide high ground that is crucial for observation. In an open or arid environment, a draw or wadi could be viewed as key terrain. The relative flatness and great distances of some deserts make even large sand dunes dominant features. Flat areas in otherwise rough terrain are vital for airborne operations and aerial resupply. Key terrain in the desert can also include facilities that could provide water or villages.

Obstacles

9-63. There are natural obstacles in the desert. The wadis and steep slopes of escarpments, mountains, hills, and dunes hinder cross-country movement. Sand dunes may stretch for miles and prevent direct movement across their length. Sand dunes are often more than 100 feet in elevation and consist of loose sand with high, steep downwind faces that make vehicular traversing next to impossible. Aerial reconnaissance immediately before any large movement is advisable because sand dunes migrate with shifting winds, and they may not be where maps or even photographs show them. Additionally, dry lake beds and salt marshes may have a crust on the top that can deceive a vehicle driver. A top crust forms on the surface, but below the crust the soil is moist, which is similar to marsh conditions. The surface may appear to have good trafficability, but the crust will collapse with the weight of a vehicle and the vehicle becomes mired. Sandy deserts are ideal for employing minefields. Although windstorms can reveal previously buried mines, these mines can still channel movement and deny access to certain areas.

Cover and Concealment

9-64. Areas in the desert may be wide and provide very limited cover and concealment. Flat sandy terrain provides little, if any, natural cover or concealment, especially from aerial attack or reconnaissance. Ground concealment and protection from fire can be found behind dunes or in wadis. Some arid regions have vegetation that can provide limited concealment from ground observation. In rocky, mountainous deserts, cover and concealment are best found behind boulders and in crevices. Daytime vehicular movement will likely be visible and eliminate the possibility of surprise, as dust trails created by the traffic can be spotted for miles. At night noise and light discipline is critical, as both sound and light travel great distances because of the unobstructed flatness of the terrain and atmospheric stability. Camouflage can be effectively employed to improve on natural cover and concealment.

IPB SUPPORT TO CYBER ELECTROMAGNETIC ACTIVITIES/ *CYBERSPACE OPERATIONS*

9-65. Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12). Cyber capabilities and leveraging cyberspace are critical for the future force to be able to command and control on-the-move while reducing operational risk. Cyberspace can be viewed in three layers (physical, logical, and cyber-persona), all of which can be integrated into the traditional IPB process and aforementioned intelligence disciplines:

- **The physical network layer includes the geographic component and the physical network components. The geographic component is the physical location of elements of the network. The physical network component includes all the hardware and infrastructure (wired, wireless, optical) that support the network and the physical connections (wires, cables, radio frequency, routers, servers, and computers). These items are subject to lethal as well as cyber threats.**
- **The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network. An example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator.**
- **The cyber-persona layer consists of the people actually on the network.**

9-66. The G-2/S-2 will work closely with the G-6/S-6, the defense information agency, and related entities to ascertain enemy cyber TTP, AAs, and enemy COAs. For U.S. Army, the G-2/S-2 will also work closely with the cyber electromagnetic activities elements and the local regional computer incident response team.

9-67. The G-6/S-6 assists the G-2/S-2 in IPB by drawing on intelligence products focused on vulnerabilities and threats in the cyberspace domain and the electromagnetic spectrum. This process provides the commander with an assessment of the operational environment, which includes the cyberspace domain and electromagnetic spectrum within its assigned physical AO. For U.S. Army, the cyber electromagnetic activities element also assists with this assessment.

9-68. The AO, area of influence, and area of interest are defined terms that include the relevant portions of the cyberspace domain and the electromagnetic spectrum. The AO involves a portion of the cyberspace domain as part of its whole. An area of influence may be a geographic area, a portion of the cyberspace domain, or both. The cyberspace domain and electromagnetic spectrum are key terrain considerations.

9-69. The G-6/S-6 assists with the assessment of enemy cyberspace and electromagnetic warfare capabilities, to include an examination of doctrinal principles and TTP, and observed patterns of enemy operations in the cyberspace domain and electromagnetic spectrum leading to a determination of possible enemy COAs. An enemy or adversary COA may involve AAs that reside solely within the cyberspace domain or electromagnetic spectrum themselves. Intelligence in the cyberspace domain involves extensive coordination, and this effort is dependent on the operating environmentand available analytical resources. For U.S. Army, the cyber electromagnetic activities element also provides this assistance to the G-2/S-2.

9-70. See JP 3-12 for more information on IPB considerations for the cyberspace domain and cyberspace operations. For the Army, see FM 3-38 for more information on cyber electromagnetic activities necessary for IPB.

Chapter 10

IPB Considerations for Unique Missions

CONDUCTING IPB IN SUPPORT OF COUNTERDRUG ACTIVITIES

10-1. Unique missions are those operations not routinely conducted by the Army/*Marine Corps*. IPB, with modification, supports the planning for these operations. This chapter discusses IPB tactics and procedures for counterdrug, counter-IED, site exploitation, peace operations, and humanitarian, disaster relief, and noncombatant evacuation operations.

10-2. The purpose of Army/*Marine Corps* support to counterdrug activities is to assist law enforcement agencies in the identification and interdiction of suspected drug trafficking within and along the approaches to the continental United States. Planning for a counterdrug support mission requires the same IPB as any other military operation. To the greatest extent possible, estimates are coordinated with supported law enforcement agencies.

10-3. When conducting intelligence activities inside the United States, or targeted at U.S. persons or groups, additional restrictions and requirements apply. Furthermore, Army intelligence employees may only participate in counterdrug missions inside the United States that have been approved under Procedure 12 of AR 381-10.

10-4. JP 3-07.4 constitutes the current doctrine the Army/*Marine Corps* uses to conduct counterdrug activities. In order to conduct IPB required for this type of operation, commanders and staffs must understand the nature of counterdrug activities and the intelligence requirements associated with them.

10-5. Counterdrug activities are those measures taken to detect, interdict, disrupt, or curtail any activity that is reasonably related to illicit drug trafficking. This includes, but is not limited to, measures taken to detect, interdict, disrupt, or curtail activities related to substances, materiel, weapons, or resources used to finance, support, secure, cultivate, process, or transport illegal drugs (JP 3-07.4). Counterdrug activities conducted by the Army/*Marine Corps* are normally conducted as part of a joint force. Planning for counterdrug activities below the strategic level is conducted using the joint operation planning process (JOPP). Step 2 of the JOPP is mission analysis. IPB begins during step 2 and continues throughout the JOPP.

10-6. IPB support to counterdrug activities is conducted using the IPB process. This is an intellectual process of analysis and evaluation that is modified from traditional military joint intelligence preparation of the operational environment. Using the IPB process identifies likely trafficking routes and the most efficient allocation of scarce resources to locate, track, and apprehend drug traffickers.

10-7. In steps 1 and 2 of the IPB process, in addition to identifying and describing the enemy, terrain, and weather concerns, the staff evaluates the effect the population may have on friendly and drug trafficking operations to—

- **Identify and describe the AOs and areas of interest.**
- **Identify and describe significant threat/*adversary*, terrain and weather, and civil considerations characteristics of the operational environment.**

10-8. Discussion of the threat/*adversary* should be limited to identifying all drug trafficking networks for further analysis and discussion during steps 3 and 4 of the IPB process. Discussion of terrain and weather should be limited to identifying significant effects of these factors. Discussion of civil considerations, however, should discuss in detail how these considerations affect friendly and drug trafficking operations. This analysis focuses on identifying—

- **Whether the local population is supporting drug trafficking and how. (This includes governmental, civil, military, and law enforcement organizations.)**
- **If the local population is supporting drug trafficking organizations, how can friendly forces separate them from these organizations and co-opt them into friendly operations?**

TERRAIN ANALYSIS

10-9. Terrain analysis conducted in support of counterdrug activities is conducted as part of the IPB process and follows the OAKOC/*KOCOA* considerations. Terrain analysis focuses on the effects terrain can have on the operations of friendly forces and on drug traffickers. The standard terrain products and work aids used during traditional IPB can be used as part of IPB support to counterdrug activities without modification, specifically the MCOO and terrain effects matrix. (Refer to chapter 4 for additional details on these products.)

WEATHER ANALYSIS

10-10. Weather analysis conducted in support of counterdrug activities is conducted as part of the traditional IPB process. Weather analysis focuses on the effects weather can have on the operations of friendly forces and on drug traffickers. The standard weather products and work aids used during the traditional IPB process can be used as part of IPB support to counterdrug activities without modification. These products are—

- **Weather forecast and conditions chart.**
- **Weather effects chart/*operational impacts chart*.**
- **Lunar illumination data.**

THREAT EVALUATION

10-11. During step 3 of the IPB process—evaluate the threat/*adversary*—intelligence personnel conducting IPB support to counterdrug activities conduct a functional analysis of drug trafficking networks to develop a database that includes data on—

- **Organizational structure.**
- **Locations (AOs).**
- **Disposition.**
- **TTP.**
- **Command and control structure.**
- **Intelligence-gathering capabilities.**
- **Counterintelligence capabilities.**
- **Logistics operations.**
- **Funding and finance.**
- **Personal data on known smugglers.**
- **Capabilities and limitations.**

10-12. Threat/*adversary* evaluation is critical to threat integration. Without a complete and accurate evaluation of drug trafficking networks, threat/*adversary* integration efforts will be flawed and will result in inaccurate intelligence estimates being used to plan operations.

10-13. In step 4 of the IPB process—determine threat/*adversary* COAs—intelligence personnel conducting IPB analyze what is known about the drug traffickers' modes of operation. The intelligence personnel integrate that analysis with the analysis conducted in the operational area evaluation and terrain

and weather analysis to make a judgment on when, how, and where the drug traffickers will move. The following products are developed during threat integration:

- **Drug trafficking situation overlay that depicts—**
  - **Primary and alternate drug smuggling routes.**
  - **Escape routes.**
  - **Crossing sites (includes official entry points, as well as obstacles that must be navigated, such as rivers, other).**
  - **Locations of drug cultivation, manufacture, and storage.**
  - **Locations and identity of groups and/or individuals—**
    - **Directing drug trafficking operations.**
    - **Funding drug trafficking operations.**
    - **Providing logistics support to drug trafficking operations.**
    - **Providing intelligence and security support to drug trafficking operations.**
    - **Transporting drugs.**
- **Drug trafficking situation statements that describe the battlefield/*battlespace* geometry and activities depicted on the drug trafficking situation overlay.**
- **HVTL identifying the individuals, organizations, and systems associated with the drug trafficking situation overlay.**
- **Drug traffickers' TTP list describing all TTP associated with the drug-smuggling operation.**
- **Indicator list describing the indicators associated with specific types of drug activity.**
- **Drug trafficking event template that identifies the locations where potential activities may occur relating to drug trafficking.**

10-14. The development of all of these products is critical to the development of the decision support template, information collection overlay/*intelligence collection overlay*, and the overall development of a successful interdiction strategy. The format and construct of these products are similar to the threat-related products constructed as part of traditional IPB. Table 10-1 shows this comparison.

Table 10-1. IPB products in support of counterdrug activities

IPB products for counterdrug activities	*Traditional IPB products*
Drug trafficking situation overlay	Enemy situation overlay
Drug trafficking situation statement	Enemy course of action statement
High-value target list	High-value target list
Drug trafficker tactics, techniques, and procedures list	Threat/*adversary* tactics, techniques, and procedures list
Indicator list	Indicator list
Drug trafficking event template	Event template

IPB SUPPORT TO COUNTER-PROLIFERATION

10-15. The proliferation of weapons of mass destruction remains a threat, which adds an even more deadly complication to the environments where U.S. forces potentially have to operate, and may create additional mission requirements. The mission to counter the weapons of mass destruction threat is not limited to defeating ballistic missiles, interceding to prevent weapons of mass destruction proliferation, and ensuring the security of weapons easily smuggled in small quantities. It extends to addressing advanced weapons programs such as nuclear, chemical, and biological munitions that can be protected by a host of defensive and deception techniques. U.S. forces deny threat/*adversary* sanctuaries, destroy critical enemy capabilities, recover personnel or sensitive equipment, safeguard and/or seize weapons of mass destruction or associated materials, and cause the threat/*adversary* to disperse forces.

10-16. Potential proliferation of weapons of mass destruction material, weapons, delivery means, and technology could quickly become a global crisis posing a physical threat. Prevention and countering the

threat/*adversary* is a high priority for U.S. forces. Protection and detection are key elements of countering weapons of mass destruction proliferation.

IPB SUPPORT TO COUNTER-IMPROVISED EXPLOSIVE DEVICE OPERATIONS

10-17. An IED attack is the result of a planned tactical operation with several key elements that work in a coordinated and synchronized manner to attain a desired result. Successful IED defeat operations begin with a thorough understanding of the enemy and the common activities associated with an IED attack. Activities include leadership, planning, financing, materiel procurement, bombmaking, target selection, recruiting, and attack execution. A holistic approach to understanding the requirements of an IED attack assists commanders and planners in identifying vulnerabilities.

10-18. IED defeat operations are unit activities that are planned, prepared for, executed, and assessed to identify, deter, and mitigate the effects of an IED attack. As part of the broader mission of the unit, these activities are conducted to predict, detect, prevent, avoid, neutralize, and protect the force from IED attack. IED defeat operations are not a staff- or function-specific responsibility. IED defeat cuts across the warfighting functions and requires the entire staff to consider all options to eliminate the IED threat. The goal is to identify and defeat enemy leaders, suppliers, trainers, enablers, and executors responsible for the employment of IEDs, while protecting the force from the effects of an IED attack.

10-19. Counter-IED operations are those actions taken by a command to prevent IED attacks on U.S. forces; multinational partners; host-nation governmental, civil, military, law enforcement agencies; and host-nation civilian populations. Counter-IED operations are integrated into any operation where there is an IED threat. The primary components of counter-IED operations are attack the network, defeat the device, and train the force. (See ATP 3-90.37/*MCIP 3-17.02* for more information on counter-IED operations.)

- Attack the network, which aims to find and eliminate bombmakers and their sources of supply—
  - Identifies and locates sources of bombmaking materials.
  - Identifies and locates bombmaking facilities.
  - Determines supply routes used to transport bombmaking material.
  - Determines methods of transport for bombmaking material.
  - Identifies and locates bombmakers.
  - Identifies and locates entities financing IED operations.
  - Locates and identifies enemy forces using IEDs as part of their operations.
  - Identifies enemy current TTP and changes to TTP associated with IEDs.
- Defeat the device, which aims to identify and/or detonate the IED at the point of attack prior to its being used successfully by the enemy—
  - Identifies what types of IEDs are being used.
  - Identifies where IEDs are being used.
  - Identifies the TTP associated with the employment of each IED.
  - Identifies the locations where the enemy will employ IEDs.
- Train the force aims at educating units and personnel on the types of devices being used to attack them; the TTP the enemy is employing; and the TTP friendly forces can use to recognize and protect themselves from IEDs. Train the force incorporates the elements of defeat the device component into IED training.

IPB SUPPORT TO SITE EXPLOITATION AND/OR EXPLOITATION OF SENSITIVE SITES

10-20. The Army/*Marine Corps*, during operations in Iraq and Afghanistan, routinely conducted site exploitation and/or exploitation of sensitive sites against strategically important sites of significant intelligence value. A sensitive site is a geographically limited area with special diplomatic, informational,

military, or economic sensitivity to the United States. Recent examples of sensitive sites include the following:

- **War crimes sites.**
- **Critical hostile government facilities.**
- **Areas suspected of containing persons of high rank or those sought after by the U.S. Government.**
- **Document storage areas containing enemy or terrorist classified files, research, and production facilities involving breakthrough technologies.**
- **Any place containing or suspected to have enemy research, production, storage, employment, or use of CBRN weapons.**

10-21. Exploitation of these types of sites can involve exploiting personnel, documents, electronic files, biometrics, forensics, and other foreign materiel captured at the site for intelligence value, while neutralizing the threat/*adversary* posed by the site or any of its contents.

SITE EXPLOITATION

10-22. A commander conducts site exploitation to—

- **Answer information requirements (usually the CCIRs).**
- **Gather intelligence for future operations (already planned or not yet anticipated).**
- **Gather evidence to support prosecution.**

10-23. Site exploitation is normally an implied task associated with other missions, and planning for site exploitation usually occurs during the planning of those missions. (See ATTP 3-90.15 for more information on site exploitation operations.) Intelligence requirements generally associated with site exploitation are identifying—

- **Characteristics and limits of the AO (search area).**
- **Terrain analysis of military characteristics of the terrain leading to and including the search area (analysis of surface, subsurface, and supersurface areas).**
- **Location, type, size, and interior schematics (floor plan) of buildings in the search area.**
- **Location, size, and capabilities of security forces in and around the search area.**
- **Location and identity of high-value individuals within the search area.**
- **Enemy TTP for concealing information, material, or persons. For example:**
  - **Creating false walls in buildings.**
  - **Burying containers.**
  - **Using women and children as couriers.**
- **Enemy TTP for reacting to the presence of U.S. forces. For example:**
  - **Using security forces to delay, disrupt, or destroy.**
  - **Using reconnaissance assets.**
  - **Using fire support (mortars).**
  - **Using boobytraps and IEDs.**
  - **Using obstacles.**
  - **Destroying material or information media.**
  - **Evacuating information media, material, or persons.**
  - **Using escape routes.**
- **The presence and attitude of noncombatants in and around the search area.**
- **Location of indigenous law enforcement facilities.**
- **Location of indigenous security forces (military and law enforcement).**
- **Objects or entities listed on the no-strike list.**
- **Presence of cultural sites and natural resources in the search area.**
- **Presence of critical infrastructure.**

- Environmental hazards in and around the search area.
- Constraints. For example:
  - Rules of engagement.
  - Search restrictions.
  - Use of force.
- Status and availability of—
  - Weapons technical intelligence collectors.
  - Multifunctional teams.
  - Forensic collection kits.
  - Document and media exploitation assets.
  - Linguists and their associated classifications.
  - Forensic laboratories and facilities.
  - Equipment, such as the biometric identity management tool, remote detection assets, and voice language translation tools.
  - Theater assets that can assist with or conduct exploitation of sensitive sites.

EXPLOITATION OF SENSITIVE SITES

10-24. Exploitation of sensitive sites differs from site exploitation in that the site contains information, materials, or persons that could cause embarrassment, compromise, or threat to U.S. security or national interests. Additionally, sensitive sites can be more dangerous, or present different types of danger, to Army/*Marine Corps* personnel. This is especially true of research and development facilities where the presence and concentration of CBRN material can cause immediate and long-term harm to personnel. Equally as important, exploitation of these sites may be beyond the capability of a tactical unit.

10-25. Some sensitive sites will also be protected sites under international law. Intelligence personnel must take extra care not to cause damage or degradation to a protected site. If exploitation is likely to result in damage, consult the servicing Judge Advocate for further guidance. In addition to intelligence requirements associated with site exploitation, intelligence requirements generally associated with sensitive site exploitation are identifying—

- Possible presence of CBRN.
- Possible CBRN facility.
- Locations containing evidence of war crimes.
- Terrorist training camps.
- Enemy prisoner of war locations.
- Research and production facilities involving breakthrough technologies.
- Government buildings and infrastructure of strategic value.
- Official government residences.
- Sites suspected of harboring high-value individuals or other enemy leaders.

IPB SUPPORT TO PEACE OPERATIONS

10-26. Peace operations include—

- Peacekeeping.
- Peace enforcement.
- Peace building.
- Peacemaking.
- Conflict prevention.

Note. Only the IPB considerations for peacekeeping and peace enforcement are discussed below. (See FM 3-07.31/*MCWP 3-33.8* for multi-Service TTP on peace operations.)

PEACEKEEPING

10-27. The objectives of peace operations include keeping violence from spreading, containing violence that has occurred, and reducing tension among factions. Accomplishing these objectives creates an environment in which other instruments of national power are used to reduce the level of violence to stable peace. Peace operations are usually interagency efforts. They require a balance of military and diplomatic resources. (JP 3-07.3 contains joint TTP for peace operations.)

10-28. Peacekeeping is defined as military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement (JP 3-07.3).

Define the Operational Environment/*Battlespace Environment*

10-29. Consider the following to define the operational environment/*battlespace environment*:

- **Identify and locate all outside influences; for example, political groups, media, and any third-nation support.**
- **Identify significant sociocultural and economic issues. These might include such things as living conditions, religious beliefs, cultural distinctions, allocation of wealth, and political grievances.**
- **Identify the legal mandates, geographical boundaries, rules of engagement, and other limitations that may affect parties involved.**
- **Identify the organization and structure of all players in the AO and area of interest.**
- **Review the history of the AO and area of interest pertinent to the current situation.**
- **Be aware of the media and its influence on the population of both the AO and area of interest.**

Describe Environmental Effects on Operations/*Describe the Battlespace Effects*

10-30. Consider the following to describe the environmental effects on operations/*describe the battlespace effects*:

- **Sociocultural information (for example, root cause of conflict, desire for conflict resolution).**
- **Weather and terrain. Analyze the effects of weather on visibility among all parties, as well as its effect on activities such as demonstrations and on mobility and operations. Identify terrain that allows all threat/*adversary* groups access to the peacekeeper and its effect on mobility and the separation of the various factions. Analyze the terrain to identify likely current disposition of threat/*adversary* groups.**
- **Legal (for example, legal COAs available to all involved parties, the likelihood of belligerents to obey laws and treaty provisions, legal limits on use of force).**
- **Food distribution warehouses or food sources.**
- **Boat docks to unload relief supplies.**
- **Civilian relief agencies.**
- **Nomadic campsites.**
- **Sources of water.**
- **Sites of religious, political, or cultural significance.**
- **Communication structure and capabilities of the parties within the AO.**

Evaluate the Threat/*Adversary*

10-31. Use the following IPB considerations to evaluate the threat/*adversary*:

- **Identify all threat/*adversary* groups. Determine which factions or groups are likely to violate the peace.**
- **Determine any relationships among the groups or factions.**
- **Identify political organizations and their objectives.**
- **Identify political and religious beliefs that directly affect or influence the conduct of the belligerents.**

- **Identify threat/*adversary* military capabilities and key personnel.**
- **Identify local support to all threat/*adversary* parties.**
- **Identify threat/*adversary* tactics for the offense and defense.**

Determine Threat/*Adversary* Courses of Action

10-32. Use the following IPB considerations to determine threat/*adversary* COAs:

- **Template threat/*adversary* actions, to include combat operations/*major operations*, support functions, terrorist acts, and any other actions that would violate the peace.**
- **Template threat/*adversary* responses to violations of the peace.**
- **Template the responses of the threat/*adversary*, the host-nation or foreign-nation government, and local indigenous populations and institutions to friendly force peacekeeping operations.**
- **Template or analyze faction activity as it relates to past events to analyze potential trends.**
- **Wargame terrorist actions and other activities where belligerents could reasonably avoid being held accountable.**

PEACE ENFORCEMENT

10-33. Peace enforcement is the application of military force, or the threat of its use, normally pursuant to international authorization, to compel compliance with resolutions or sanctions designed to maintain or restore peace and order (JP 3-07.3).

Define the Operational Environment/*Battlespace Environment*

10-34. Consider the following to define the operational environment/*battlespace environment*:

- **Identify and locate all outside influences; for example, political groups, media, and any third-nation support.**
- **Identify significant sociocultural and economic issues that may potentially adversely affect the effort to enforce the peace. These might include such things as living conditions, religious beliefs, cultural distinctions, allocation of wealth, and political grievances.**
- **Identify the legal mandates, geographical boundaries, rules of engagement, and other limitations that may affect parties involved. Determine which resolutions are being enforced.**
- **Identify the organization and structure of all players in the AO and area of interest.**
- **Review the history of the AO and area of interest pertinent to the current situation.**
- **Be aware of the media and its influence on the population of both the AO and area of interest.**

Describe Environmental Effects on Operations/*Describe the Battlespace Effects*

10-35. Consider the following to describe environmental effects/*battlespace effects*:

- **Sociocultural information (for example, root cause of conflict, desire for conflict resolution).**
- **Weather and terrain. Analyze the effects of weather on visibility among all parties, as well as its effect on activities such as demonstrations and on mobility and operations. Identify terrain that allows all threat/*adversary* groups access to the peace enforcer and its effect on mobility and the separation of the various factions. Analyze the terrain to identify likely current dispositions of threat/*adversary* groups.**
- **Legal (for example, legal COAs available to all involved parties the likelihood of belligerents to obey laws and treaty provisions, legal limits on use of force). This is critical to peace enforcement operations, as the focus is to get the parties to comply with agreed-to resolutions or sanctions.**
- **Civilian relief agencies.**
- **Sources of water.**
- **Sites of religious, political, or cultural significance.**
- **Communication structure and capabilities of the parties within the AO.**

Evaluate the Threat/*Adversary*

10-36. Use the following considerations to evaluate the threat/*adversary*:

- **Identify all threat/*adversary* groups.**
- **Determine which factions or groups are likely to violate the resolutions.**
- **Determine any relationships among the groups or factions.**
- **Identify political organizations and their objectives.**
- **Determine who wants to violate the resolutions.**
- **Identify political and religious beliefs that directly affect or influence the conduct of the belligerents. Determine whether these beliefs are contrary to the goals of the peace enforcement operation.**
- **Identify threat/*adversary* military capabilities and key personnel.**
- **Determine whether the parties can defeat efforts to enforce the peace.**
- **Determine the tactics the threat/*adversary* will use to affect the will of the peace enforcer.**
- **Identify local support to all threat/*adversary* parties.**
- **Identify threat/*adversary* tactics for the offense and defense.**

Determine Threat/*Adversary* Courses of Action

10-37. Use the following IPB considerations to determine threat/*adversary* COAs:

- **Template threat/*adversary* actions, to include combat operations/*major operations*, support functions, terrorist acts, and any other actions that would violate the peace.**
- **Template threat/*adversary* responses to violations of the peace.**
- **Template the responses of the threat/*adversary*, the host-nation or foreign-nation government, and local indigenous populations and institutions to friendly force peace enforcement operations.**
- **Template or analyze faction activity as it relates to past events to analyze potential trends.**
- **Wargame terrorist actions and other activities where belligerents could reasonably avoid being held accountable.**

IPB SUPPORT TO HUMANITARIAN AND DISASTER RELIEF AND OTHER OPERATIONS

10-38. Humanitarian, disaster relief, and other operations (such as noncombatant evacuation operations) assist governments and security organizations in easing human sufferance caused by manmade or natural disasters.

10-39. Humanitarian and disaster relief provided by U.S. forces is limited in scope and duration. The relief provided is designed to supplement or complement the efforts of the host-nation civil authorities or agencies that may have the primary responsibility for providing relief.

DEFINE THE OPERATIONAL ENVIRONMENT/*BATTLESPACE ENVIRONMENT*

10-40. In defining the operational environment/*battlespace environment* in support of relief, the staff will—

- **Identify areas or activities that might generate displaced civilian movement.**
- **Consider threats to the AO, such as severe weather, gangs; criminal organizations or religious, ethnic, and racial factions.**
- **Identify all military, paramilitary, host-nation, international, IGOs, and NGOs; indigenous populations and institutions; and transnational corporations.**
- **Determine the status of any hostile military or paramilitary forces in the area. Identify the key civilian leaders, community elders, tribal leaders, and their respective supporters.**
- **Assess host-nation infrastructure.**
- **Determine the condition of LOCs, utilities, transportation systems, and government services.**

- **Determine the status of sanitation conditions within the AO.**
- **Identify storage facilities and requirements.**
- **Determine the effects of rules of engagement and other force protection measures on threat/*adversary* operations.**
- **Determine the type and location of all land minefields.**
- **Determine the geography within the AO and its effect on the mission.**

DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS/*BATTLESPACE EFFECTS*

10-41. In describing the environmental effects on operations/*battlespace effects* in support of FHA, the staff will—

- **Consider the effects of terrain on locations of land minefields.**
- **Determine if weather has had an effect on minefield location; for example, has the thawing and freezing of the ground affected known or suspected minefields?**
- **Determine the effect weather and terrain will have on displaced civilian movement, military operations, civil affairs or military information support operations, mass actions, food supplies, and general mobility.**
- **Identify the population sectors. The staff looks at urban or rural areas where real or potential threats/*adversaries* can blend into the population or gain influence over the population.**
- **Focus on demographics. Consider, for example, the effects of—**
  - **Urban and rural population patterns.**
  - **Ethnic, religious, and racial divisions.**
  - **Language divisions.**
  - **Tribe, clan, and sub-clan loyalties.**
  - **Health hazards.**
  - **Political sympathies.**
- **Consider the effects of the infrastructure on—**
  - **Location, activity, and capacity of care distribution points (food, health care).**
  - **Sources of food and water.**
  - **Housing availability.**
  - **Hospital capabilities.**
  - **Utility services.**
  - **Law enforcement agencies and emergency services and their respective capabilities.**
- **Determine the LOCs that can be used by friendly forces and potential threats/*adversaries* to affect movement of FHA.**
- **Locate agricultural areas and other sources of subsistence.**
- **Determine the present and potential effects of severe weather on executing the FHA mission and displaced civilian movement.**
- **Determine if the environment is permissive or hostile to the introduction of friendly forces.**
- **Identify key targets and facilities. The staff should consider that the targets and facilities may also be key terrain.**

Evaluate the Threat/*Adversary*

10-42. In evaluating the threat/*adversary* in support of FHA, the staff will—

- **Consider weather and the environment as potential threats/*adversaries*. Weather will affect the ability to conduct relief operations. For example, if the target of a relief effort is a village isolated by mudslides or another natural disaster, inclement weather may limit or curtail air operations to the site. Consider that the environment may pose threats to the health of both friendly forces and host-nation personnel in the forms of waterborne diseases, spoiled or contaminated foodstuffs, and other environmental hazards.**

- **Identify and evaluate the threat posed by any groups that may oppose friendly force operations.**
- **Consider groups that may clandestinely oppose the operation even though they publicly pledge support.**
- **Consider civilians and local populace (for example, NGOs, indigenous populations, and institutions) that may become hostile as the operation progresses.**
- **Evaluate the threat posed by gangs, paramilitaries, terrorist groups or individuals, insurgents, guerilla forces, or other organized forces.**
- **Identify and evaluate potential trouble spots and contentious issues. Look for riot or similar threat/*adversary* indicators.**

Determine Threat/*Adversary* Courses of Action

10-43. In determining threat/*adversary* COAs in support of FHA, the staff will—

- **Identify threat/*adversary* COAs that seek to embarrass friendly forces during the FHA mission; for example, will the threat/*adversary* use relief workers to embarrass friendly forces?**
- **Identify the possibility of threat/*adversary* military action against civilians (relief workers and host-nation personnel).**
- **Evaluate the threat/*adversary* imposed by a degradation of the capabilities of host-nation law enforcement.**
- **Evaluate the possibility of unknown or new minefields and other obstacles in the AO.**
- **Assess threat/*adversary* propaganda capability.**

10-44. A noncombatant evacuation operation is a small-scale limited operation conducted to assist the Department of State in evacuating U.S. citizens, Department of Defense civilian personnel, and designated host-nation and third-country nationals whose lives are in danger from locations in a foreign nation to an appropriate safe haven. Although normally considered in connection with hostile action, evacuation may also be conducted in anticipation of, or in response to, any natural or manmade disaster. (See JP 3-68 for more information on noncombatant evacuation operations.)

10-45. A noncombatant evacuation operation is a joint operation, and planning is normally conducted by joint task forces using the JOPP. Therefore, commanders and staff use the joint intelligence preparation of the operational environment (JIPOE) process during planning, not IPB. JIPOE begins during step 2 of JOPP—mission analysis—and continues throughout the JOPP. Intelligence requirements generally associated with noncombatant evacuation operations are—

- **Location, disposition, capabilities, and possible COAs for all enemy forces.**
- **Location of evacuation sites (landing zones, ports, beaches).**
- **Anticipated number of evacuees (total number by area) categorized by medical status. Categories include—**
  - **Persons not requiring assistance.**
  - **Persons requiring medical assistance prior to evacuation.**
  - **Persons requiring medical assistance prior to and during evacuation.**
  - **Persons requiring emergency medical evacuation.**
- **Locations of assembly areas and major supply routes.**
- **Location of command posts.**
- **Key personnel (name, location, and methods of contact).**
- **Description of the embassy communications system, transportation fleet, and warden system.**
- **Quantity of Class I (subsistence supplies) on hand at the embassy.**
- **Quantity of Class III (fuel) on hand at the embassy or available elsewhere.**
- **Availability of class VIII (medical supplies) on hand at the embassy.**
- **Standard map products of the local area with annotations identifying critical landmarks.**
- **Rules of engagement.**

10-46. Every U.S. embassy is required to maintain an emergency action plan that includes much of the information the staff needs to support JIPOE. A copy of this action plan is also maintained by the theater headquarters. The joint task force staff should obtain a copy of the emergency action plan prior to beginning JIPOE and coordinate with the theater command and staff and the embassy throughout JIPOE.

10-47. Additionally, the National Geospatial-Intelligence Agency maintains a geospatial intelligence base for contingency operations; this intelligence base contains specific maps, charts, imagery, and other geospatial intelligence products to support noncombatant evacuation operations planning. Other intelligence sources that can aid JIPOE are as follows:

- **The Defense Intelligence Agency maintains various databases that provide details on diplomatic facilities and associated areas for use in evacuation planning.**
- **The *Marine Corps Intelligence Activity* produces joint expeditionary support products containing maps, charts, imagery, points of entry, and route studies for use during expeditionary operations including evacuation planning and execution.**
- **United States Transportation Command maintains the port and airfield collaborative environment Web site, which provides detailed overviews of ports and strategic airfields (capable of C-130s and above) worldwide.**
- **Each Joint Intelligence Operations Center maintains Web sites and databases that provide varying degrees of intelligence support for particular countries.**
- **The Department of State Web site maintains the most current situational information available for the country of interest.**
- **The Central Intelligence Agency maintains basic information and maps for all countries of the world in the factbook data file on its Web site.**
- **Joint task force staffs may also be augmented with a National Intelligence Support Team that provides liaison to national intelligence agencies. (See JP 2-0 for more information on national intelligence support teams.)**

Appendix A

Marine Corps Planning Process Tools

A-1. ***This appendix only applies to the Marine Corps. For the MCPP, commanders and their staffs use MCPP tools to record, track, and analyze critical planning information. These tools help the commander and the staff better understand the environment, facilitate the commander's decisionmaking, assist in the preparation of plans and orders, and increase tempo. The MCPP tools must serve the needs of the commander and the requirements of the situation. Commanders and staffs can tailor these tools to meet their needs and use other tools available that are appropriate for their particular situation.***

A-2. ***Table A-1 identifies commonly used overlays, templates, matrices, worksheets, graphics, and narratives on how each tool supports the MCPP. The examples in this appendix (shown in figures or tables) are at the MEF level, but these tools may be employed at any level of command. The formats and uses of these tools may be modified as required. (See MCWP 5-1 for additional information on the MCPP.)***

Table A-1. ***Marine Corps planning process tools***

Tools	*Problem framing*	*COA development*	*COA wargame*	*Comparison and decision*	*Orders development*	*Transition*
Modified combined obstacle overlay (figure A-1 on page A-3)	*X*	*X*	*X*			
Adversary template (figure A-2 on page A-4)	*X*	*X*	*X*			
Situation template (figure A-3 on page A-5)	*X*	*X*	*X*			
Event template (figure A-4 on page A-6)	*X*	*X*	*X*			
Event matrix (table A-3 on page A-6)	*X*	*X*	*X*			
Decision support template (figure A-5 on page A-7)		*X*	*X*	*X*	*X*	*X*
Decision support matrix (table A-4 on page A-8)		*X*	*X*	*X*	*X*	*X*
COA graphic and narrative (figure A-6 on page A-9)		*X*	*X*	*X*	*X*	
Synchronization matrix (table A-5 on page A-10)		*X*	*X*	*X*	*X*	*X*
COA wargame worksheet (table A-6 on page A-11)			*X*	*X*	*X*	
Comparison and decision matrix with comments (table A-7 on page A-12)				*X*		

INTELLIGENCE PREPARATION OF THE BATTLESPACE PRODUCTS

A-3. ***The IPB is a systematic process of analyzing and visualizing the portions of the mission variables of the enemy, terrain and weather, and, when appropriate, civil considerations in a specific area of interest and for a specific mission. By applying IPB, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space. A continuous planning activity undertaken by the entire staff, IPB builds an extensive database for each potential area in which a unit may be required to operate. The IPB describes the environment in which the command is operating and the effects of that environment on the command's operations. Battlespace and weather evaluations assist in identifying obstacles, mobility corridors, and AAs; predicting weather effects for numerous mobility options; and estimating sea conditions. The IPB process consists of the following steps:***

- ***Define the operational environment.***
- ***Describe the effects on operations.***
- ***Evaluate the adversary.***
- ***Determine the adversary's COAs.***

A-4. ***In conventional military operations, determining adversary COAs will normally include templating with an adversary assessment. Templating continues from planning to execution, both to assess current operations and to support planning for future operations. In irregular warfare, adversary templating will focus on pattern analysis, which involves tracking, analyzing, and identifying specific trends, such as IEDs or population support, over time.***

A-5. ***The IPB products graphically display the results of the IPB process. Table A-2 identifies the major IPB products and shows their integration with the planning process. Note that both the G-2/S-2 and the G-3/S-3 are responsible for specific products. While IPB starts as an intelligence effort, it expands to an operational process and has logistic and communications applications that are not shown in the table. Paragraphs A-6 through A-11 provide a short description of each product.***

Table A-2. *IPB integration throughout the Marine Corps planning process*

Products	Problem Framing	COA Development	COA Wargame	Comparison and Decision	Orders Development	Transition
Modified combined obstacle overlay	G-2/S-2 →					
Adversary template	G-2/S-2 →					continuous[1]
Situation template	G-2/S-2 →					continuous[1]
Pertinent adversary COAs	G-2/S-2 →	→				continuous[1]
Refined and prioritized adversary COAs and event templates and matrices	G-2/S-2 →	→				continuous[1]
Initial decision support template	→	G-2/S-2/OPT →	→			continuous[1]
Decision support template matrix	→	G-2/S-2/OPT →	→	→		continuous[1]

Note[1] . Templates are updated throughout the operation.
COA course of action OPT operational planning team

MODIFIED COMBINED OBSTACLE OVERLAY

A-6. ***The MCOO (see figure A-1) is a graphic of the battlespace's effects on military operations. It is normally based on a product depicting all obstacles to mobility and it is modified as necessary. Modifications can include cross-country mobility classifications, objectives, AAs and mobility corridors, likely obstacles, defensible battlespace, likely engagement areas, key terrain, cultural factors, built-up areas, and civil infrastructure.***

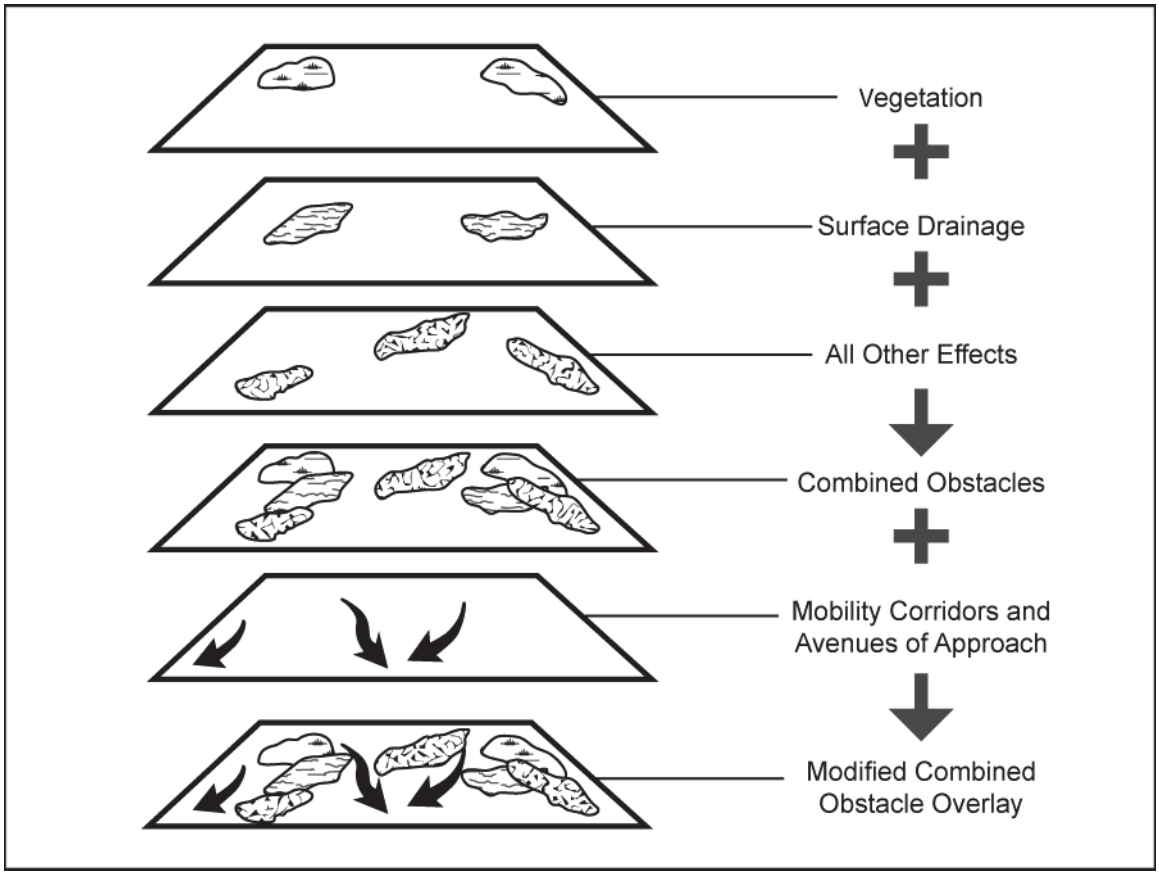


Figure A-1. ***Modified combined obstacle overlay***

ADVERSARY TEMPLATE

A-7. ***Adversary templates (see figure A-2) are models based on postulated adversary doctrine. They illustrate the disposition and activity of adversary forces conducting a particular operation arrayed on ideal terrain. Adversary templates depict the adversary's nominal organization, frontages, depths, boundaries, and control measures for combat. They are usually scaled for use with a map background and are one part of an adversary model. In irregular warfare, adversary templating will focus on pattern analysis, which involves tracking, analyzing, and identifying specific trends, such as IEDs or population support, over time.***

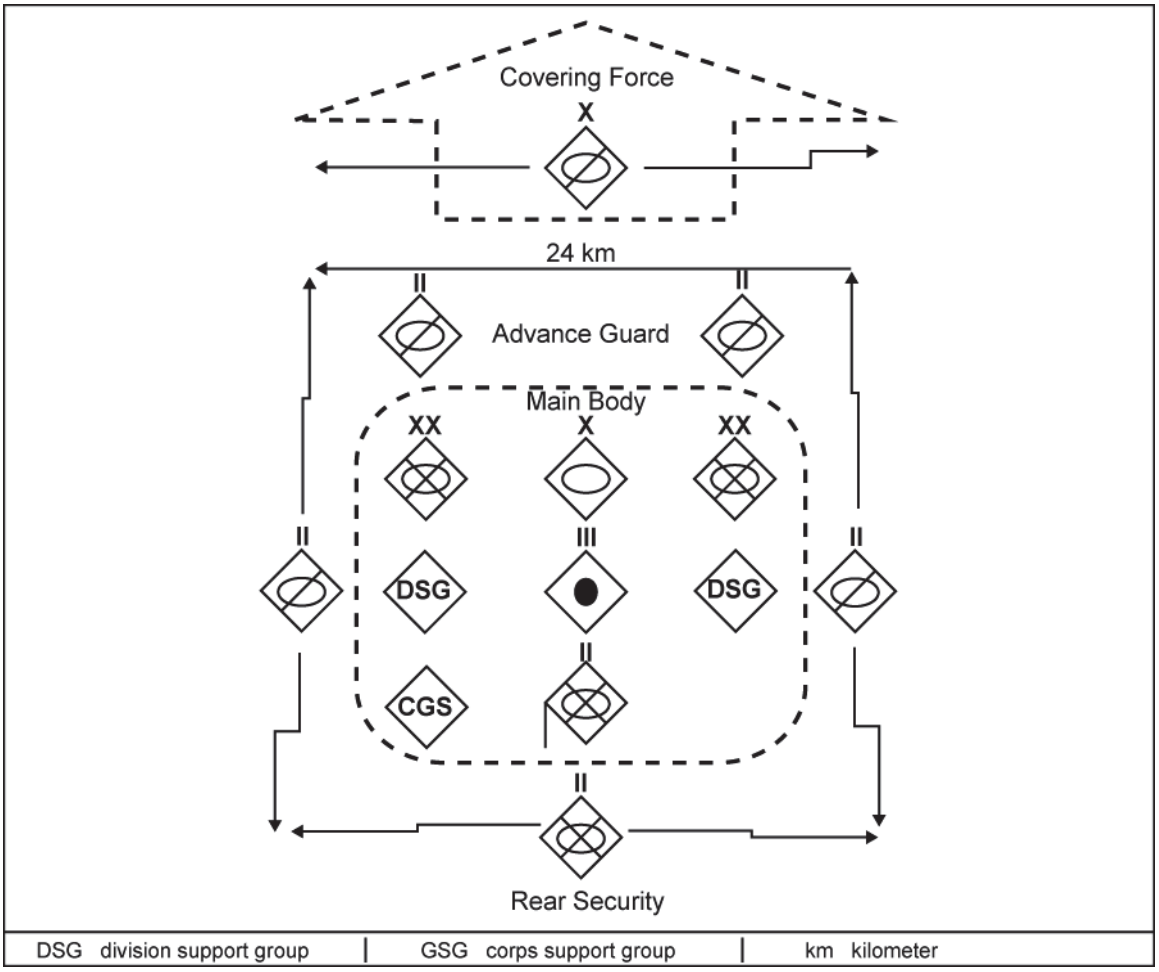


Figure A-2. ***Adversary template***

SITUATION TEMPLATE

A-8. ***A situation template (see figure A-3) is an adversary template that has been modified to depict adversary dispositions based on the effects of the battlespace and the pursuit of a particular COA. This template accounts for the adversary's current situation with respect to the terrain, training and experience levels, logistic status, losses, and dispositions. Normally, the situation template depicts adversary units two levels down and critical points in the COA. Situation templates are one part of an adversary COA model. Models may contain more than one situation template to depict locations and formations at various times.***

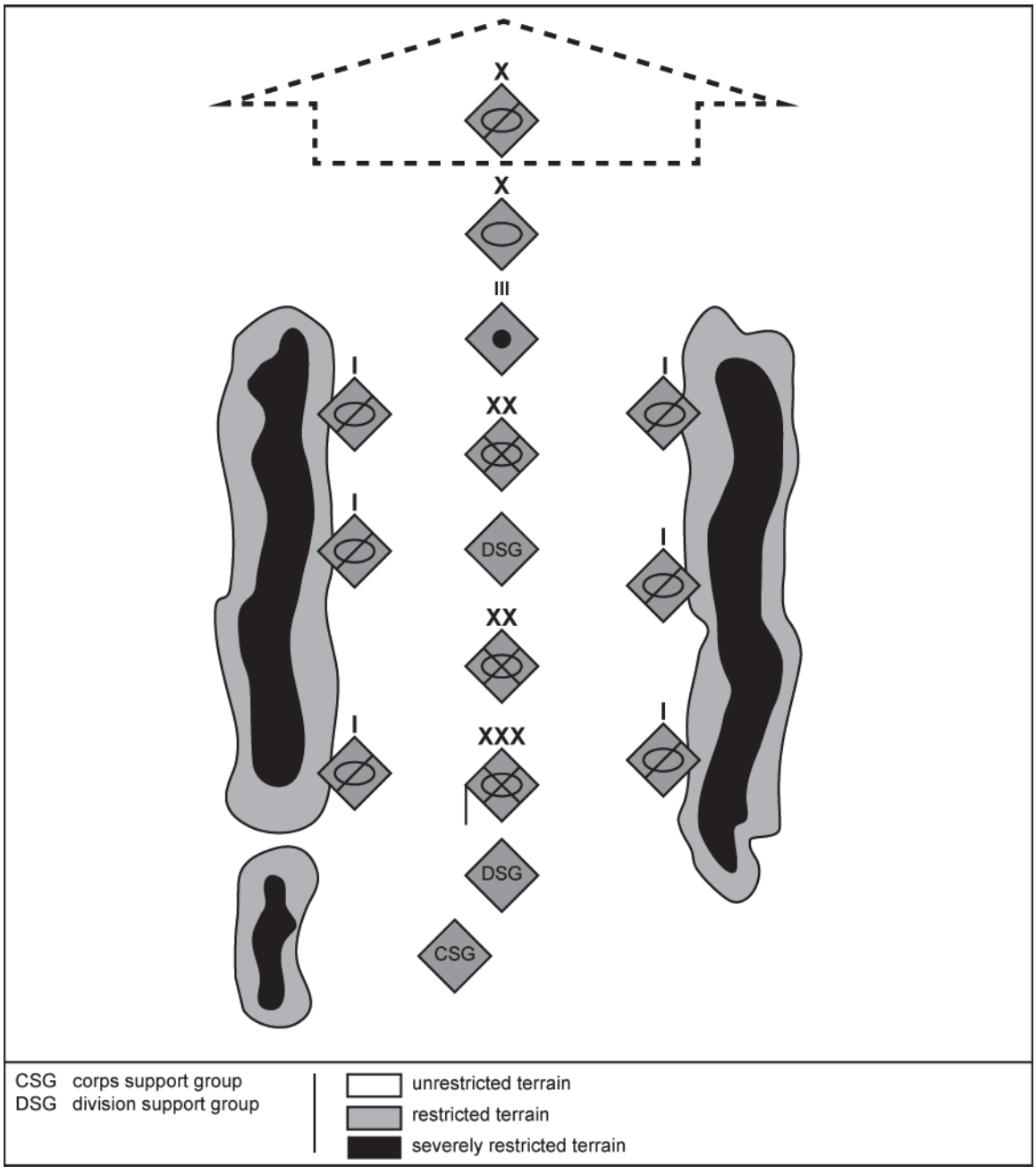


Figure A-3. ***Situation template***

EVENT TEMPLATE AND MATRIX

A-9. ***The event template is derived from the situation template and depicts the NAIs, areas where activity—or lack of activity—will indicate which COA the adversary has adopted. The NAIs are described in paragraphs 1-36, 6-47, 6-50, and 6-51.. Event templates contain time-phase lines that depict movement of forces and the expected flow of the operation. Movement rates depend on the terrain (MCOO) and the adversary COA (DRAW-D). The event template is the IPB starting point for COA wargaming. The event matrix depicts types of activity expected in each NAI, when the NAI is expected to be active, and any additional information to aid in collection planning. (See figure A-4 and table A-3.)***

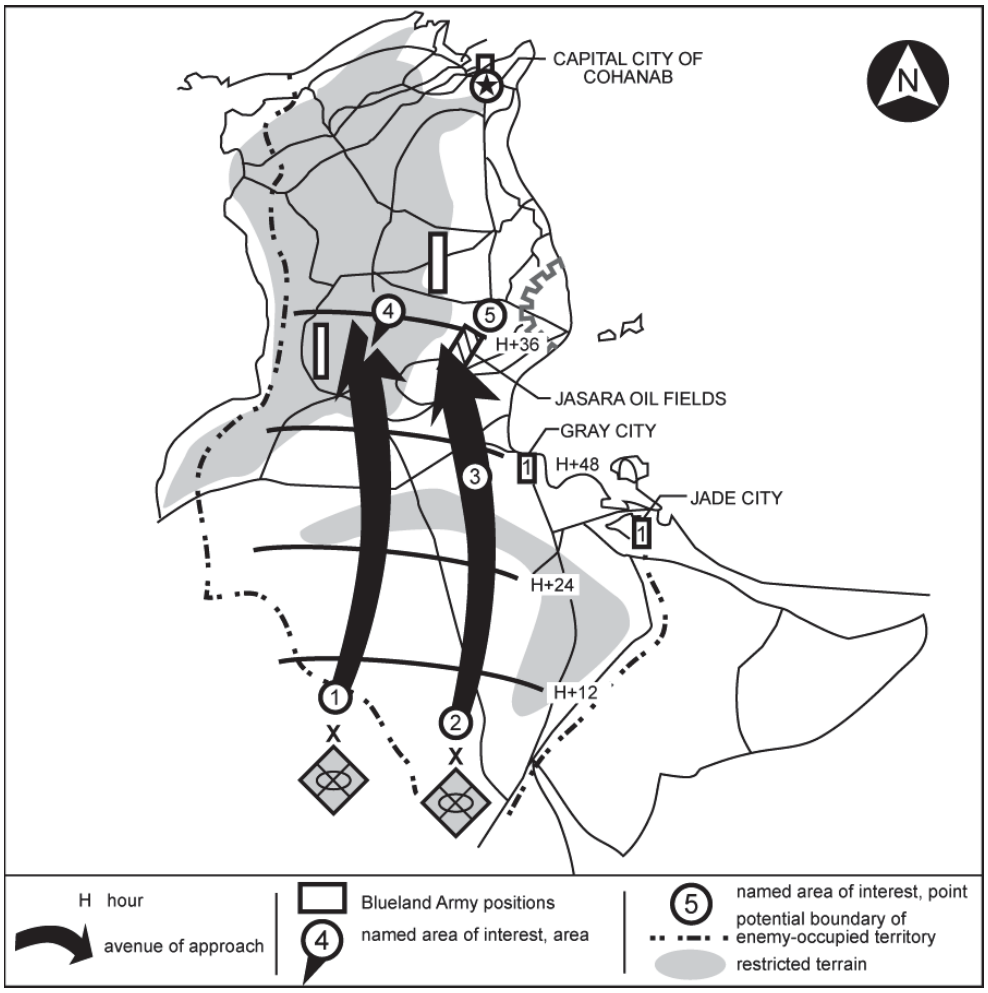


Figure A-4. ***Event template***

Table A-3. ***Event matrix***

Named area of interest	*No earlier than*	*No later than*	*Event or indicator*
1	*H+6*	*H+12*	*Brigade-sized forces moving north.*
2	*H+6*	*H+12*	*Brigade-sized forces moving north.*
3	*H+12*	*H+24*	*Orangeland forces enter Blueland. Northern operational group driving on Jasara oil fields.*
4	*H+14*	*H+24*	*Orangeland forces seize junction of highways 7 and 8. Northern operational group turns northwest toward Jasara.*
5	*H+18*	*H+24*	*Orangeland forces enter Tealton. Northern operational group driving on Jasara.*

DECISION SUPPORT TEMPLATE AND MATRIX

A-10. ***The decision support template is normally developed during COA wargaming. It is derived from adversary, situational, and event templates. The decision support template depicts decision points, time-phase lines associated with movement of adversary and friendly forces, the flow of the operation, and other information required to execute a specific friendly COA.***

A-11. ***The decision support template is a key planning tool for use during transition and execution. The decision support matrix provides a recap of expected events, decision points, and planned friendly actions in a narrative form. It shows where and when a decision must be made if a specific action is to take place. It ties decision points to NAIs, TAIs, CCIRs, collection assets, and potential friendly response options. The decision support template and matrix may be refined as planning progresses after the wargame. (See figure A-5 and table A-4 on page A-8.)***

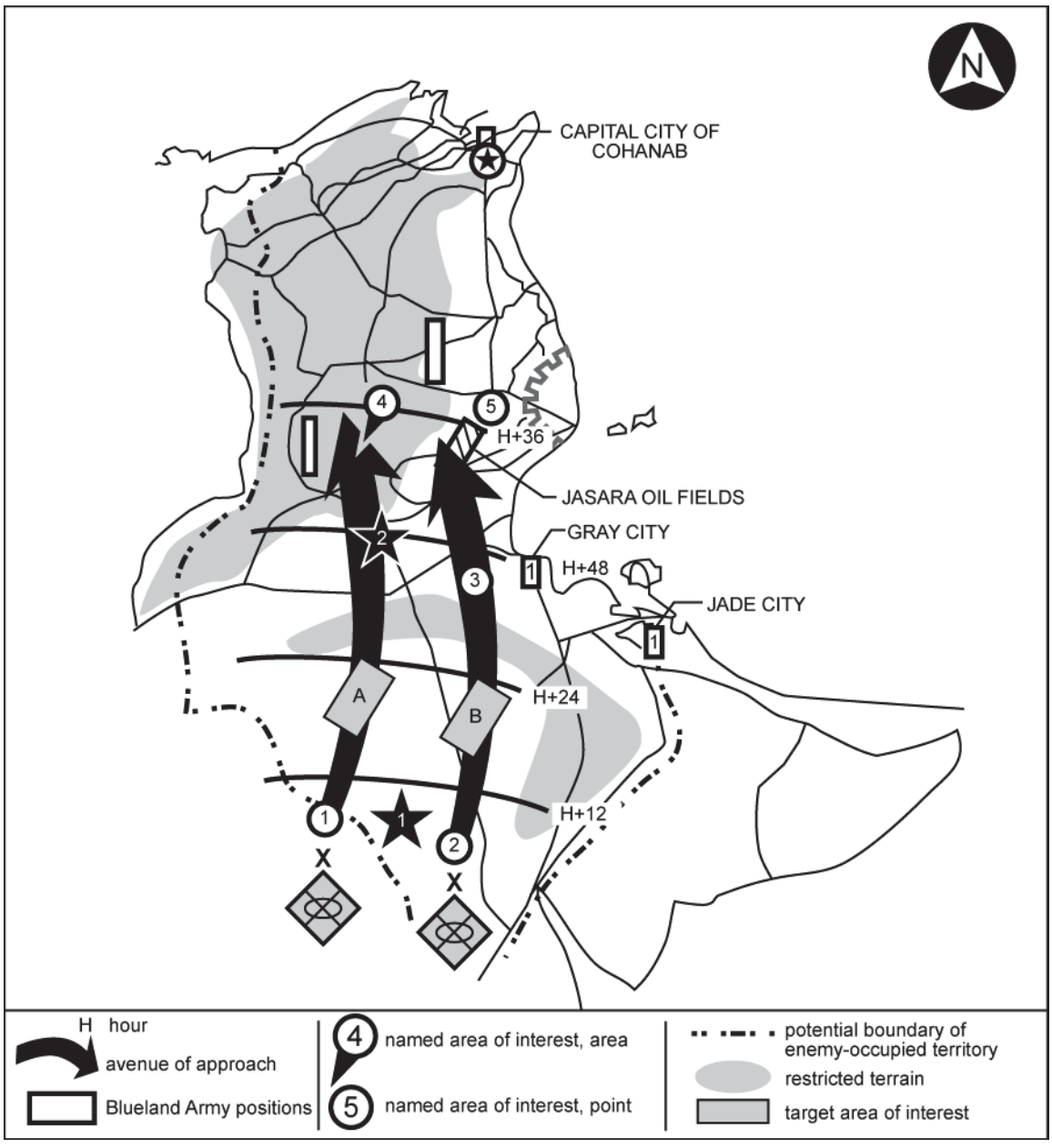


Figure A-5. ***Decision support template***

Table A-4. ***Decision support matrix***

Event Number	Event	No earlier than/no later than	Named area of interest	Target area of interest	Friendly action
1	*Orangeland forces enter Blueland. Northern operational group division driving on Tealton.*	*H+14/H+24*		*A, B*	*Covering force withdraws; Marine aircraft wing conducts interdiction west of phase line Teal (see figure A-6).*
2	*Orangeland forces seize junction of Highways 7 and 8. Northern operational group turns northwest on Jasara.*	*H+18/H+24*	*3, 4*	*C*	*1st and 3d Marine divisions execute branch plan Hawk.*

PLANNING SUPPORT TOOLS

A-12. ***Planning support tools support the commander's and staff's planning effort by recording and displaying critical planning information on the COAs and the commander's decisions and guidance. They aid the commander in decisionmaking by displaying critical information in a useful format. Planning support tools include the COA graphic and narrative, synchronization matrix, COA wargame worksheets, and the comparison and decision matrix.***

COURSE OF ACTION GRAPHIC AND NARRATIVE

A-13. ***The COA graphic and narrative (see figure A-6) is a visual depiction and written description of a COA. It clearly portrays how the organization will accomplish the mission, identifying the who (notional task organization), what (tasks), when, where, how, and why (intent). It should include the tasks and purpose of the main effort, supporting efforts, and reserve. It also includes maneuver control measures, such as boundaries. The COA narrative and graphic, when approved by the commander, forms the basis for the concept of operations and operations overlay in the OPLAN or OPORD.***

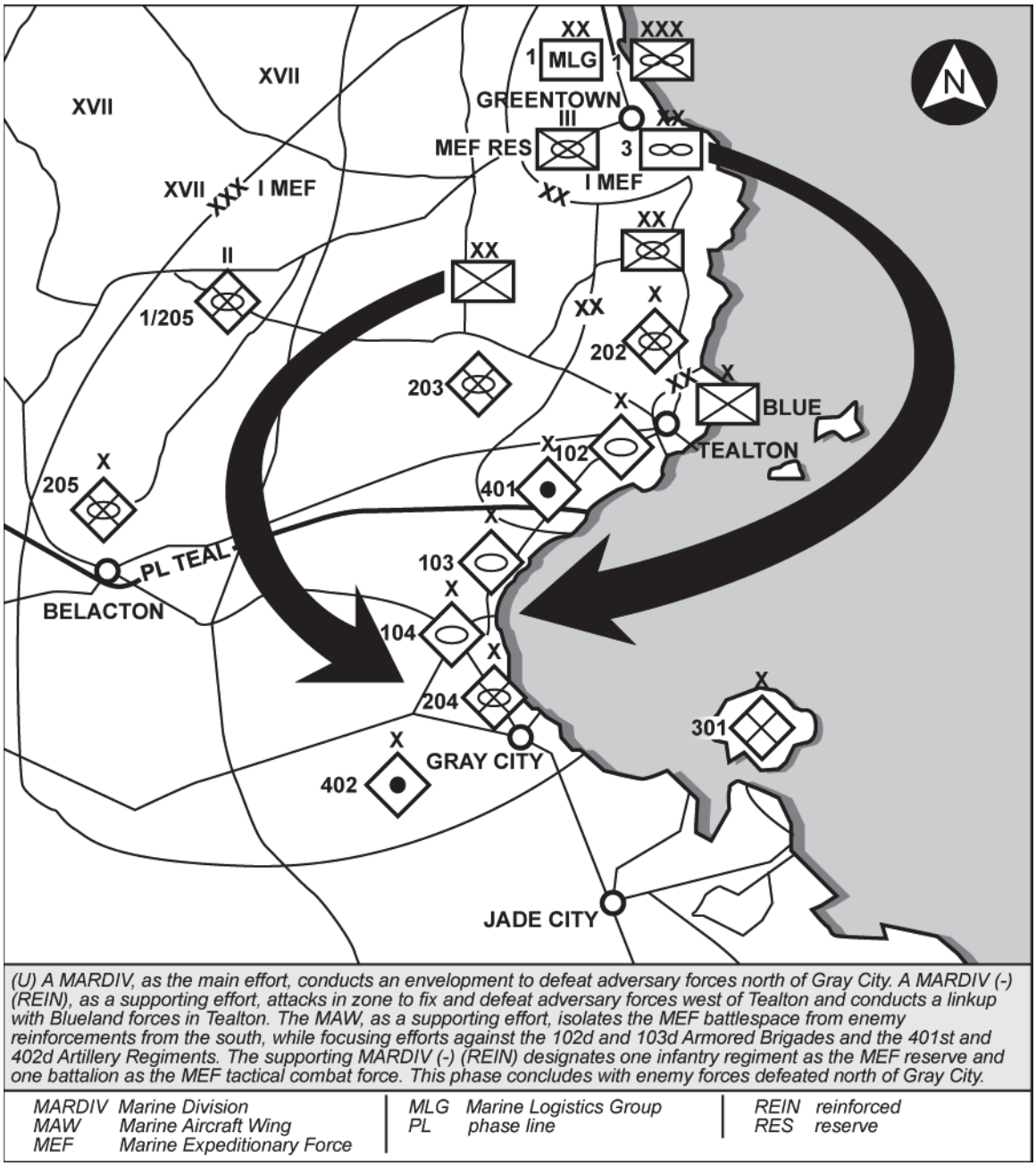


Figure A-6. ***Course of action graphic and narrative***

SYNCHRONIZATION MATRIX

A-14. ***A synchronization matrix (see table A-5) is a planning support tool designed to integrate the efforts of the force. It can be organized across the warfighting functions, lines of operations, or other activities based on the situation. It can also record the results of the COA wargame. It depicts, over time, the diverse actions of the entire force necessary to execute the COA. When completed, it provides the basis for an execution matrix or Annex X (Execution Checklist) to the OPLAN or OPORD.***

Table A-5. ***Synchronization matrix***

Time	Event	Pre-D-day	D-day - D+2	D+3 - D+4	D+5 - D+6
Adversary action					
Decision points				1	2
Intelligence		Marine expeditionary force (MEF) conducts reconnaissance in zone			
	NAI		1, 2	3, 4	5
Force protection	Survivability	Establish combat air patrol over MEF area of operations			
	CBRN		Priority of support to ACE		
Maneuver	Deep		Marine aircraft wing (MAW) attacks northern operational group armor and artillery, C2, and CSS facilities	MAW attacks 102, 103, 401, and 402	
	Security		Covering forces conduct security operations		
	Close		1st and 3d Marine Divisions (MARDIVs) complete rupture of adversary defenses	1st MARDIV attacks adversary forces south of phase line Teal The 2d MARDIV conducts linkup with Blueland forces	
	Reserve	3d MARDIV—one regiment to MEF reserve			
	Rear	3d MARDIV—one battalion to tactical combat force			
	Mobility	Priority of main supply route development in main effort zone			
	Countermobility			Complete execution of barrier plan south	

ACE aviation combat element
C2 command and control
CBRN chemical, biological, radiological, and nuclear
CSS combat service support
NAI named area of interest

COURSE OF ACTION WARGAME WORKSHEET

A-15. ***The COA wargame worksheet (see table A-6) is used during the wargame to record friendly action, adversary reaction, and friendly counteraction involved in each COA. It is also used to capture critical information that may be identified during the wargame, such as potential CCIR, decision points, and NAIs.***

Table A-6. ***Course of action wargame worksheet***

COA 1, Stage A; Box; Most likely							
Action	**Reaction**	**Counteraction**	**Assets**	**Time**	**DP**	**CCIR**	**Remarks**
MARDIV envelops Orangeland forces north of Gray City	*102d and 103d Armored Brigades CATK*	*MAW interdicts moving threat/adversary forces* *MARDIV engages and destroys threat/adversary armor at long range*	*Surge MAW attack assets to interdict threat/adversary armor*	*D+3*	*3*	*Will 102d and 103d Armored Brigades move west to CATK*	*MARDIV has priority of close-air support*
CATK – counterattack *COA – course of action*		*D – day* *DP – decision point*				*MARDIV – Marine division* *MAW – Marine aircraft wing*	

COURSE OF ACTION COMPARISON AND DECISION MATRIX

A-16. ***The COA comparison and decision matrix is a planning support tool designed to assist the commander and staff in recording the advantages and disadvantages of each COA as it is compared against the commander's evaluation criteria. It also provides a venue for further discussion. It may reflect various techniques for weighing the COA against the commander's evaluation criteria (see table A-7 on page A-12). The commander may use the COA comparison and decision matrix to aid his decisionmaking process during the selection of a COA for execution. Commanders and staffs should guard against relying on numerical "rankings" or other simplistic methods that can fail to underscore the complexity involved in the decisionmaking process.***

PLANNING SUPPORT TOOLS FOR STABILITY OPERATIONS

A-17. The following planning support tools have emerged and evolved as a result of lessons learned from Operation Iraqi Freedom and Operation Enduring Freedom.

CIVIL CONSIDERATIONS

A-18. ***Civil considerations are a factor in all types of military operations, but they are of particular significance in stability operations. If the mission is to support civil authorities, civil considerations define the mission. Civil considerations generally focus on the immediate impact of civilians on operations in progress; however, they also include larger, long-term diplomatic, informational, and economic issues at higher levels. At the tactical level, they directly relate to key civil considerations within the AO. The world's increasing urbanization means that the attitudes and activities of the civilian population in the AO often influence the outcome of military operations.***

A-19. ***Civil considerations can either help or hinder friendly or adversary forces and will influence the selection of a COA. An appreciation of civil considerations—the ability to analyze their impact on operations—enhances several aspects of operations, such as the selection of objectives; location, movement, and control of forces; use of weapons; and protection measures. Civil considerations comprise six characteristics— areas, structures, capabilities, organizations, people, and events—expressed in the acronym ASCOPE. (See figure A-7 on page A-12.)***

Table A-7. *Comparison and decision matrix with comments*

Commander's evaluation criteria	COA 1	COA 2	COA 3
Force protection	*Moderate casualties*	*High casualties* *Increased chemical, biological, radiological, and nuclear threat*	*Light casualties*
Tempo, surprise		*Achieving surprise unlikely*	*High change of achieving surprise*
Shapes the battlespace	*ACE interdiction of adversary lines of communications limits adversary's ability to reinforce*		*Deception likely to be effective*
Asymmetrical operations	*ACE operates against second echelon armor forces* *GCE mechanized forces attack adversary dismounted infantry*	*Marine expeditionary forces mechanized forces against adversary mechanized forces*	
Maneuver	*Frontal attack followed by penetration*	*Frontal attack*	*Turning movement*
Decisive actions	*ACE disrupts deployment of second echelon forces through interdiction*		*Isolate first echelon forces. Disrupt lines of communications, logistic facilities, and assembly areas*
Simplicity		*Simplest*	*Demanding command and coordination requirements*
ACE aviation combat element		*GCE ground combat element*	

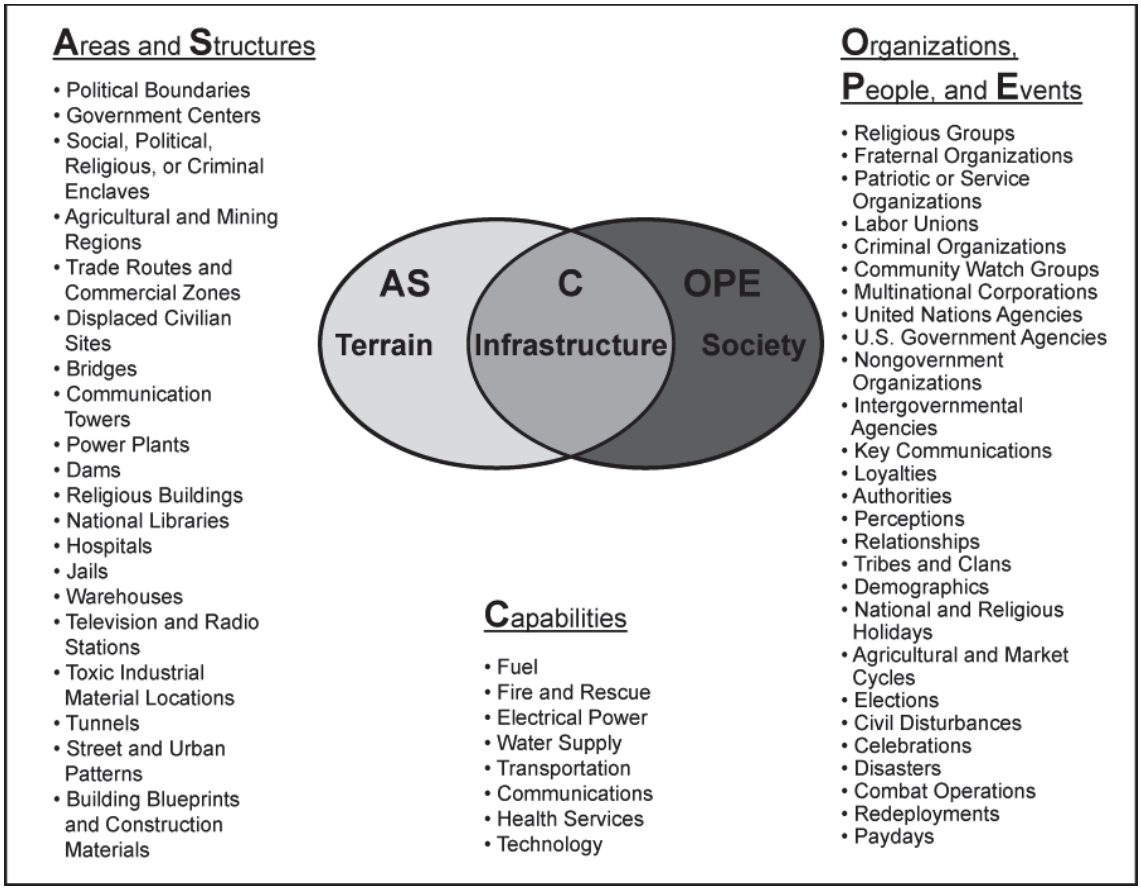


Figure A-7. *Sample civil considerations*

AREAS

A-20. ***Areas are key localities or aspects of the terrain within a commander's operational environment that are not normally thought of as militarily significant. Failure to consider key civil areas, however, can seriously affect the success of any military mission. Civil-military operations planners analyze key civil areas from two perspectives: how do these areas affect the military mission and how do military operations impact civilian activities in these areas? At times, the answers to these questions may dramatically influence major portions of the COAs being considered.***

STRUCTURES

A-21. ***Structures are architectural objects, such as bridges, communications towers, power plants, and dams, and are often identified as traditional HPTs. Other structures, such as churches, mosques, national libraries and hospitals, are cultural sites generally protected by international law or other agreements. Still other structures are facilities with practical applications, such as jails, warehouses, schools, television stations, radio stations, and printing plants, which may be useful for military purposes. Structures analysis involves determining their location, functions, capabilities, and application in support of military operations. It also involves weighing the military, political, economic, religious, social, and informational consequences of removing them from civilian use; the reaction of the populace; and replacement costs.***

CAPABILITIES

A-22. ***Civil capabilities can be viewed from several perspectives. The term "capabilities" may refer to—***

- ***Existing capabilities of the populace to sustain itself, such as through public administration, public safety, emergency services, and food and agriculture systems.***
- ***Capabilities with which the populace needs assistance, such as public works and utilities, public health, public transportation, economics, and commerce.***
- ***Resources and services that can be contracted to support the military mission, such as interpreters, laundry services, construction materials, and equipment. Local vendors, the host nation, or other nations may provide these resources and services. In hostile territory, civil capabilities include resources that may be taken and used by military forces consistent with international law. Analysis of the existing capabilities of the AO is normally conducted based on civil affairs functional specialties. The analysis also identifies the capabilities of partner countries and organizations involved in the operation. In doing so, civil-military operations planners consider how to address shortfalls, as well as how to capitalize on capability strengths.***

ORGANIZATIONS

A-23. ***Civil organizations are groups that may or may not affiliate with government agencies. They can be church groups, fraternal organizations, patriotic or service organizations, or community watch groups. They might be IGOs or NGOs. Organizations can assist the commander in keeping the populace informed of ongoing and future activities in an area of operations and influencing the actions of the populace. They can also form the nucleus of humanitarian assistance programs, interim governing bodies, civil defense efforts, and other activities.***

PEOPLE

A-24. ***People, both individually and collectively, can have a positive, negative, or no impact on military operations. The "people" element of ASCOPE includes civilians or nonmilitary personnel encountered in an AO. The term may also extend to those outside the AO whose actions, opinions, or political influence can affect the military mission. In all military operations, U.S. forces must be prepared to encounter and work closely with civilians of all types. When analyzing people, Marines should consider historical, cultural, ethnic, political, economic, and humanitarian factors. Working with the "people" assists Marines in identifying the key communicators as well as the formal and informal processes used to influence people. Regardless of the nature of the operation, military forces will usually encounter civilians living and operating in and around the supported unit's AO. Major categories of civilians likely to be encountered include—***

- *Local nationals, such as town and city dwellers, farmers, other rural dwellers, and nomads.*
- *Local civil authorities, such as elected and traditional leaders at all levels of government.*
- *Expatriates.*
- *Foreign employees of IGOs or NGOs.*
- *U.S. Government and third-nation government agency representatives.*
- *Contractors, who may be U.S. citizens, local nationals, or third-nation citizens providing contract services.*
- *Department of Defense civilian employees.*
- *The media, including journalists from print, radio, and visual media.*

EVENTS

A-25. *As there are many different categories of civilians, there are many categories of civilian events that may affect the military mission. Some examples are planting and harvest seasons, elections, riots, and voluntary and involuntary evacuations. Likewise, there are military events that impact the lives of civilians in an AO. Some examples are combat operations, including indirect fires, deployments, and redeployments. Civil-military operations planners determine what events are occurring and analyze the events for their political, economic, psychological, environmental, and legal implications.*

Appendix B

Functional Analysis

B-1. Functional analysis shows graphically how the threat/*adversary* might utilize its capabilities to perform the functions required to accomplish its objectives. It depicts the threat's/*adversary*'s disposition and actions for a particular type of operation (for example, offense, defense, movement to contact, insurgent ambush, and/or terrorist kidnapping operation).

B-2. Functional analysis is a method for determining likely threat/*adversary* COAs. This is based on the concept that while every action or battle is unique, certain functions are performed to bring about mission accomplishment. Functional analysis provides a framework for understanding how a specific threat/*adversary* will make use of its capabilities—whatever they are—to accomplish its goals.

B-3. A threat/*adversary* employs functional tactics. It determines the functions it needs to perform as part of an action to bring about its success. Then it allocates appropriate actors to each function and synchronizes the effort.

B-4. A number of different functions are executed each time a threat/*adversary* force attempts to accomplish a mission. The threat/*adversary* commanders identify the specific functions they intend their various subordinate forces or elements to perform. The functions do not change, regardless of where the force or element might happen to be located on the battlefield/*battlespace*. However, the function of a particular force or element may change during the course of the battle.

B-5. Functional analysis may predict likely threat/*adversary* COAs of any type, such as—

- **The methodology and technique an insurgent force will use to emplace and explode an IED along convoy routes.**
- **The methods used by a criminal organization to rob banks.**
- **Convoy procedures a drug trafficking ring will use to transport large amounts of drugs, such as the distance between vehicles, number of vehicles, where security forces are placed, and how many are in the convoy.**
- **How the security force will react to or deploy against a police force.**

B-6. Functional analysis consists of three steps:

- **Determine threat/*adversary* objectives.**
- **Determine threat battlefield/*adversary battlespace* functions.**
- **Determine threat/*adversary* capabilities available to perform each function.**

DETERMINE THREAT/*ADVERSARY* OBJECTIVES

B-7. Functional analysis begins with a determination of what goal or goals the threat/*adversary* is trying to achieve. Threat/*adversary* objectives are often, but not always, what the unit's mission is trying to prevent. These objectives are also often actions taken by the threat to prevent unit mission accomplishment. The objectives are specific to the type of threat, the AO, the unit's composition and mission, and other factors.

B-8. Some examples of these objectives are—

- **Cause friendly unit casualties in order to weaken political resolve in the U.S. and among multinational partners.**
- **Destroy friendly aircraft while on the ground during a refueling operation.**
- **Kidnap and ransom a friendly civil leader.**
- **Prevent friendly security forces from discovering a hidden drug laboratory.**

- Seize an important crossroads to facilitate maneuver of a larger force.
- Describe the objectives in terms of purpose and end state.

DETERMINE THREAT BATTLEFIELD/*ADVERSARY BATTLESPACE* FUNCTIONS

B-9. The threat/*adversary* executes a number of different functions each time a threat force attempts to accomplish a mission. While the various functions required to accomplish any given mission can be quite diverse, they can be divided into four very broad categories: action, enabling, fixing, and security.

ACTION

B-10. The action function (also known as the exploitation, decision, or mission function) is performed by the set of capabilities that actually accomplishes a given mission. If the threat/*adversary* objective is to destroy a city with a weapon of mass destruction, then the weapon of mass destruction is performing the action function. If the threat objective is to seize a friendly capital city and it employs a weapon of mass destruction in another area to force a response by friendly forces that leaves the capital exposed, then the force used to seize the capital is performing the action function and the weapon of mass destruction is performing a different function.

B-11. The action function is performed by the set of capabilities that actually accomplish a given mission. One part of the unit or grouping of units conducting a particular action is normally responsible for performing the primary function or task that accomplishes the goal or objective of that action. In general terms, therefore, that part can be called the action force or action element. In most cases, however, the higher commander will give the action force or element a more specific designation that identifies the specific function it is intended to perform, which equates to achieving the objective of the higher command's mission.

B-12. For example, if the objective of the action is to conduct an assault, the element designated to complete that action is the assault element. In larger offensive actions, an action force that completes the primary offensive mission by exploiting a window of opportunity created by another force is called the exploitation force. In defensive actions, the unit or grouping of units that performs the main defensive mission in the battle zone is called the main defense force or main defense element. However, in a maneuver defense, the main defensive action is executed by a combination of two functional forces: the contact force and the shielding force.

ENABLING

B-13. The enabling function (also known as the assault function) is performed by a set of capabilities that acts to assist those capabilities performing the action function. If the mission is to enter a U.S. base and set off an explosive device, an enabling function would be to penetrate the perimeter defenses of the base or to assist in its infiltration. The enabling function is performed by a set of capabilities that acts to assist those capabilities performing the action function. In relation to the forces or elements conducting the action function, all other parts of the organization or grouping of organizations conducting an action provide enabling functions of various kinds. In general terms, therefore, each of these parts can be called an enabling force or enabling element. However, each subordinate force or element with an enabling function can be more clearly identified by the specific function it performs.

B-14. For example, a force that enables by fixing enemy forces so they cannot interfere with the primary action is a fixing force. Likewise, an element that creates a breach that enables an assault element to assault the enemy forces on the far side of an obstacle is a breach element.

B-15. In larger offensive actions, one force can enable another by conducting an assault that enables another force to exploit the effects of that assault in order to accomplish the primary objective. Thus, that type of enabling force can be called the assault force. In this case, the force that conducts the initial assault is not the one that is actually intended to achieve the objective of the higher command's mission. The role of the assault force is to create an opportunity for another force—the exploitation force—to accomplish the objective. Thus, the assault force, conducting the first part of a two-part offensive action, acts as an

enabling force. In order to create a window of opportunity for the exploitation force to succeed, the assault force may be required to operate at a high degree of risk and may sustain substantial casualties. However, other types of enabling forces or elements may not even need to make contact with the enemy.

B-16. If the mission is to enter an enemy base and set off an explosive device, an enabling function would be to penetrate the perimeter defenses of the base or to assist in the infiltration of the element emplacing the device. In the defense, an enabling function might be to counterattack to restore a portion of the area of responsibility to threat/*adversary* control. There are three specific types of enabling functions common that warrant additional attention: disruption, fixing, and security.

B-17. Disruption forces or elements operate to prevent U.S. forces from executing friendly COAs the way U.S. forces want to and to prevent U.S. forces interfering with the threat's/*adversary*'s COA. U.S. forces can—

- **Disrupt enemy preparations or actions.**
- **Destroy or deceive enemy reconnaissance.**
- **Begin reducing the effectiveness of key components of the enemy's combat system.**

FIXING

B-18. The fixing function is performed by a set of capabilities that acts to prevent opposing capabilities from interfering with mission accomplishment. If the mission is to ambush a convoy moving through an urban area, a fixing function would be to delay arrival of a quick reaction force. If the mission is to destroy a force in a defensive battle position, a fixing function would be to prevent the opposing reserve from maneuvering.

B-19. Fixing is accomplished when a part of the enemy force does not participate in actions that could lead to the failure of the threat/*adversary* COAs. This is accomplished in a variety of ways, including—

- **Suppressing a force with fires.**
- **Deceiving it with information warfare/*information operations*.**
- **Forcing it to conduct disaster relief and humanitarian assistance.**
- **Involving it in a firefight away from the main action.**
- **Restricting its movement with countermobility effects.**
- **Depriving it of logistics resources.**

SECURITY

B-20. The security function is performed by a set of capabilities that acts to protect other capabilities from observation, destruction, or becoming fixed. Security is provided by isolating the battlefield/*battlespace* from enemy elements that could alter the outcome. This can be accomplished by providing early warning and reaction time or actively delaying or destroying arriving enemy forces.

OTHER FUNCTIONS

B-21. The threat/*adversary* commander may designate a subordinate unit or grouping to conduct a deception action (such as a demonstration or feint). This unit or grouping is, therefore, a deception force or deception element. Its function is to lead the enemy to act in ways prejudicial to enemy interests or favoring the success of a threat/*adversary* action force or element.

B-22. A threat/*adversary* commander may also designate some subordinates to perform various support functions. These support elements can provide the following types of support:

- **Perform support by fire (in which case, it can be called more specifically a support by fire element).**
- **Provide support or sustainment/*combat or combat service support*.**
- **Provide command and control functions.**

B-23. At a commander's discretion, some forces or elements may be held out of initial action, in reserve, pending determination of their specific function, so that the commander may influence unforeseen events or

take advantage of developing opportunities. These forces or elements are designated as reserves (reserve force or reserve element). If and when such units are subsequently assigned a mission to perform a specific function, they receive the appropriate functional force or element designation. For example, a reserve force in a defensive operation might become the counterattack force.

DETERMINE THREAT/ADVERSARY CAPABILITIES AVAILABLE TO PERFORM EACH FUNCTION

B-24. Once it is known which functions the threat/*adversary* needs to perform and what goal the threat/*adversary* commander is seeking to accomplish through the performance of those functions, the last step is to identify what capabilities the threat/*adversary* has to execute each function.

B-25. While the functions required to have a high chance of success in achieving a military goal are universal, the means through which they may be accomplished will vary widely depending on the location, threat/*adversary*, and environment. These may even vary from street to street. In one battlefield/*battlespace,* the threat/*adversary* may employ an infantry platoon equipped with infantry-fighting vehicles and sophisticated thermal sensors to execute the security function. In another, the same function may be performed by a civilian in a third-floor apartment window using a cellular phone.

B-26. Both of the examples below are assaults:

- In figure B-1 each of the functions is performed by readily recognized military formations. Air defense and antitank units perform the security function; direct and indirect fire weapons enable the action, while infantry units perform the action function of the assault.
- In figure B-2 the same functions are being performed, but by significantly different actors. The security function is performed individually with communications devices. The enabling function is being performed by sniper teams and a rioting crowd and the assault itself conducted by insurgents initially posing as members of that crowd.

B-27. In both cases, each type of element is performing the same function. The security elements are providing early warning of arriving enemy forces and, if possible, delaying their ability to influence the decisive point. The support elements are providing activities that enable the action element to accomplish its mission. The action elements are executing the task that accomplishes the goal—in this case the enemy's destruction and the seizure of his position.

B-28. Briefly stated, functional analysis is the application of the knowledge of common and necessary military functions to specific threat capabilities. It is a methodology that—

- Forces analysts and the staff to learn and understand tactics and not rote memorizations.
- Reduces the ability of the enemy/*adversary* to deceive analysts and the staff.
- Is transportable between theaters and works all along the range of military operations.

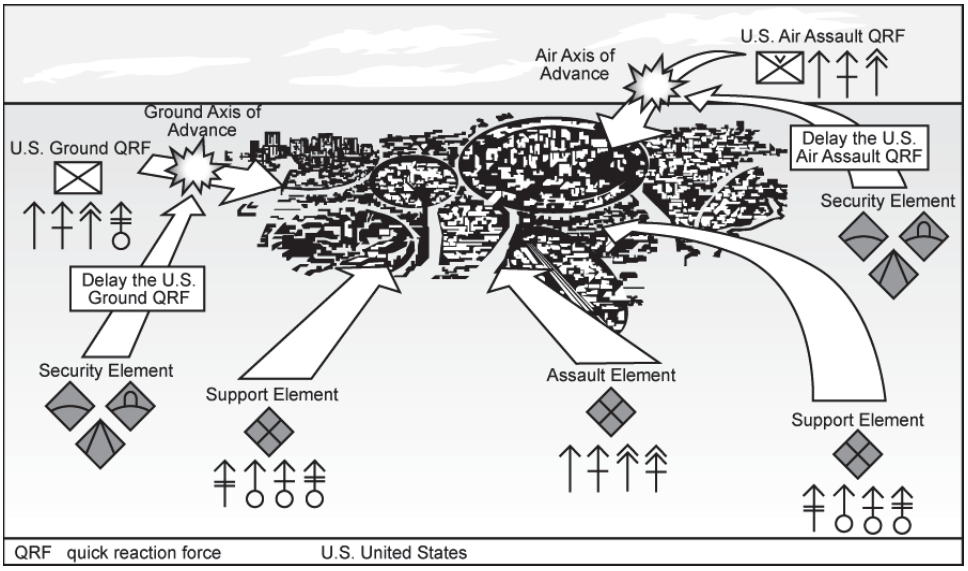


Figure B-1. Enemy attacking fixed position

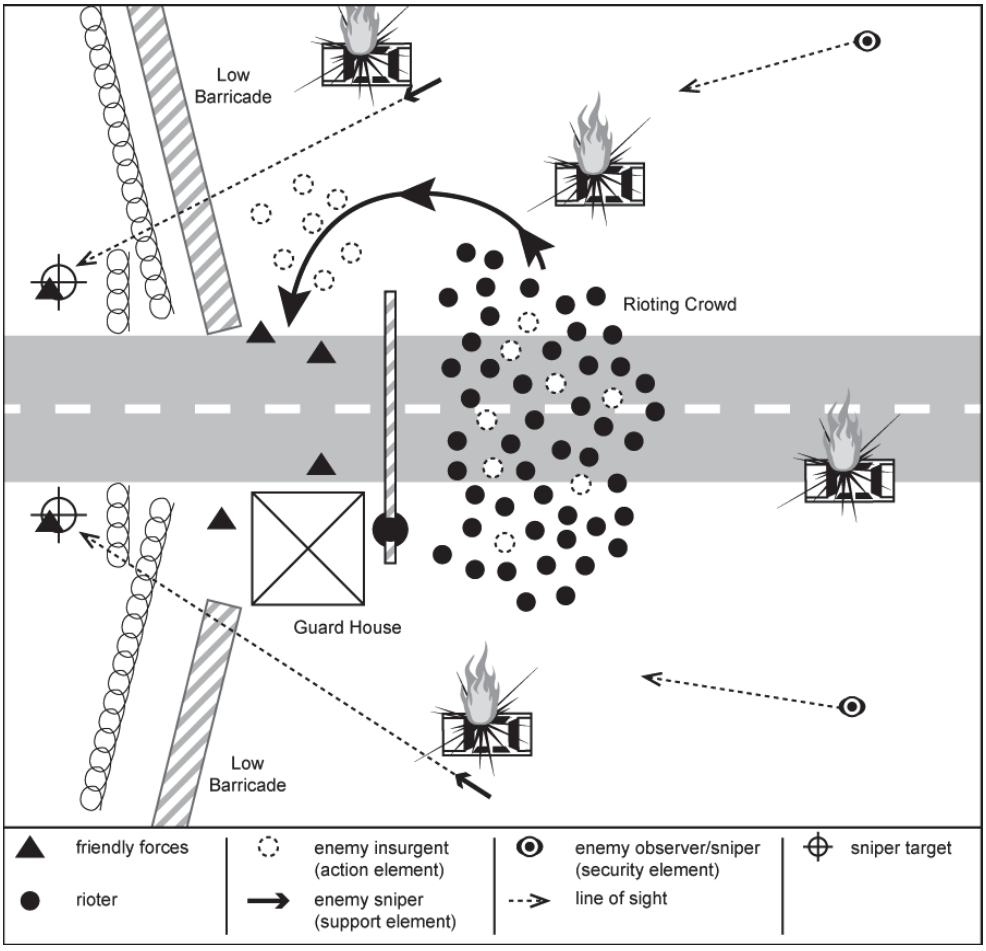


Figure B-2. Sniper and riot-enabled insurgency assault

This page intentionally left blank.

Glossary

For acronyms and terms with Army definitions (Army) precedes the definition. For acronyms and terms with *Marine Corps* definitions (Marine Corps) precedes the definition. The two terms for which ATP 2-01.3/*MCRP 2-3A* is the proponent are marked with an asterisk (*). The proponent publication for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

AA	**avenue of approach**
AO	**area of operations**
ADP	**Army doctrine publication**
ADRP	**Army doctrine reference publication**
AFTTP	**Air Force tactics, techniques, and procedures**
ASCOPE	**areas, structures, capabilities, organizations, people, and events (civil considerations)**
ATP	**Army techniques publication**
ATTP	**Army tactics, techniques, and procedures**
CBRN	**chemical, biological, radiological, and nuclear**
CCIR	**commander's critical information requirement**
COA	**course of action**
DA	**Department of the Army**
DRAW-D	***defend, reinforce, attack, withdraw, delay (Marine Corps)***
EEFI	**essential element of friendly information**
FHA	**foreign humanitarian assistance**
FM	**field manual**
FMFM	***Fleet Marine Force Manual***
G-2	**assistant chief of staff, intelligence**
G-3	**assistant chief of staff, operations**
G-4	**assistant chief of staff, logistics**
G-6	**assistant chief of staff, signal**
G-9	**assistant chief of staff, civil affairs operations**
GIRH	***Generic Intelligence Requirements Handbook (Marine Corps)***
HPT	**high-payoff target**
HPTL	**high-payoff target list**
HTT	**human terrain team (Army)**
HVT	**high-value target**
HVTL	**high-value target list**
IED	**improvised explosive device**
IGO	**intergovernmental organization**

IPB	**intelligence preparation of the battlefield (Army)/*intelligence preparation of the battlespace (Marine Corps)***
IVL	**intervisibility line**
JIPOE	**joint intelligence preparation of the operational environment**
JOPP	**joint operations planning process**
JP	**joint publication**
KOCOA	***key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach (Marine Corps)***
LOC	**line of communications**
MAGTF	***Marine air-ground task force(Marine Corps)***
MAW	***Marine aircraft wing (Marine Corps)***
MCDP	***Marine Corps doctrinal publication (Marine Corps)***
MCIA	***Marine Corps Intelligence Activity (Marine Corps)***
MCIP	***Marine Corps interim publication (Marine Corps)***
MCO	***Marine Corps order***
MCOO	**modified combined obstacle overlay**
MCPP	***Marine Corps Planning Process(Marine Corps)***
MCRP	***Marine Corps reference publication (Marine Corps)***
MCWP	***Marine Corps warfighting publication (Marine Corps)***
MDMP	**military decisionmaking process (Army)**
MEF	***Marine expeditionary force (Marine Corps)***
METOC	***meteorological and oceanographic (Marine Corps)***
METT-T	***mission, enemy, terrain and weather, troops and support available—time available (Marine Corps)***
METT-TC	**mission, enemy, terrain and weather, troops and support available, time available, civil considerations (mission variables) (Army)**
NAI	**named area of interest**
NGO	**nongovernmental organization**
NTTP	**Navy tactics techniques and procedures**
NWP	***Navy warfare publication (Marine Corps)***
OAKOC	**observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (military aspects of terrain) (Army)**
OPLAN	**operation plan**
OPORD	**operation order**
PIR	**priority intelligence requirement**
PMESII	***political, military, economic, social, information, and infrastructure (Marine Corps)***
PMESII-PT	**political, military, economic, social, information, infrastructure, physical environment, time (operational variables) (Army)**
R2P2	***rapid response planning process (Marine Corps)***
RDSP	**rapid decisionmaking and synchronization process (Army)**
S-2	**intelligence staff officer**
S-3	**operations staff officer**

S-4	**logistics staff officer**
S-6	**signal staff officer/*communications staff officer(0602)***
S-9	**civil affairs operations staff officer (Army)**
SALUTE	**size, activity, location, unit, time, and equipment**
SIPRNET	**SECRET Internet Protocol Router Network**
SME	**subject matter expert**
TC	**training circular**
TLP	**troop leading procedures**
TRAP	***tactical recovery of aircraft and personnel (Marine Corps)***
TTP	**tactics, techniques, and procedures**
UNS	***Universal Need Statement (Marine Corps)***
U.S.	**United States**

SECTION II – TERMS

adversary template

(Marine Corps) A model that portrays the adversary's frontage depths, echelon spacing, and force composition as well as the disposition of adversary combat, combat support, and combat service support units for a given operation. It portrays how the adversary would like to fight if he was not constrained.

antiterrorism

(joint) Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. Also called AT. (JP 3-07.2)

area of influence

(joint) A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. (JP 3-0)

area of interest

(joint) That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (JP 3-0)

area of operations

(joint) An operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. Also called AO. (JP 3-0)

avenue of approach

(joint) An air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. Also called AA. (JP 2-01.3)

battlespace

(Marine Corps) The environment, factors, and conditions that must be understood to successfully apply combat power, protect the forces, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrian; the electromagnetic spectrum; and the information environment within the operational areas, areas of interest, and areas of influence. (MCRP 5-12C)

begin morning civil twilight

(joint) The period of time at which the sun is halfway between beginning morning and nautical twilight and sunrise, when there is enough light to see objects clearly with the unaided eye. Also called BMCT. (JP 2-01.3)

begin morning nautical twilight

(joint) The start of that period where, in good conditions and in the absence of other illumination, the sun is 12 degrees below the eastern horizon and enough light is available to identify the general outlines of ground objects and conduct limited military operations. Also called BMNT. (JP 2-01.3)

civil considerations

The influence of manmade infrastructure, civilian institutions, and the attitudes and activities of the civilian leaders, populations, and organizations within an area of operations on the conduct of military operations. (ADRP 5-0)

collection

(Marine Corps) Acquisition of information and the provision of this information to processing. (JP 1-02). The gathering of intelligence data and information to satisfy the identified requirements. (MCRP 5-12C)

commander's critical information requirement

(joint) An information requirement identified by the commander as being critical to facilitating timely decision making. (JP 3-0)

concealment

Protection from observation or surveillance. (ADRP 1-02)

cover

(joint) In intelligence usage, those measures necessary to give protection to a person, plan, operation, formation, or installation from the enemy intelligence effort and leakage of information. (JP 2-01.2)

decision support template

(joint) A combined intelligence and operations graphic based on the results of wargaming that depicts decision points, timelines associated with the movement of forces and the flow of the operation, and other key items of information required to execute a specific friendly course of action. (JP 2-01.3)
(Marine Corps) A staff product initially used in the wargaming process that graphically represents the decision points and projected situations and indicates when, where, and under what conditions a decision is most likely to be required to initiate a specific activity (such as a branch or sequel) or event (such as lifting or shifting of fires). (MCRP 5-12C)

end evening civil twilight

(joint) The point in time when the sun has dropped 6 degrees beneath the western horizon, and is the instant at which there is no longer sufficient light to see objects with the unaided eye. Also called EECT. (JP 2-01.3)

end of evening nautical twilight

(joint) The point in time when the sun has dropped 12 degrees below the western horizon, and is the instant of last available daylight for the visual control of limited military operations. Also called EENT. (JP 2-01.3)

event matrix

(joint) A cross-referenced description of the indicators and activity expected to occur in each named area of interest. (JP 2-01.3)

event template

(joint) A guide for collection planning. The event template depicts the named areas of interest where activity, or its lack of activity, will indicate which course of action the adversary has adopted. See also area of interest. (JP 2-01.3)

high-payoff target list

A prioritized list of high-payoff targets. (FM 3-60)

high-value target

(joint) A target the enemy commander requires for the successful completion of the mission. Also called HVT. (JP 3-60)

hybrid threat

The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects. (ADRP 3-0)

information environment

(joint) The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

intelligence

(joint) 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities.. (JP 2-0) ***(Marine Corps) Knowledge about the enemy or the surrounding environment needed to support decisionmaking. Intelligence is one of the six warfighting functions. (MCRP 5-12C)***

intelligence estimate

(joint) The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy and the order of probability of their adoption. (JP 2-0)

intelligence preparation of the battlefield/*battlespace

(Army) The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. Also called IPB. ***(Marine Corps) The systematic, continuous process of analyzing the threat and environment in a specific geographic area. Also called IPB.***

intelligence requirement*(s)*

(joint) 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. Also called IR. (JP 2-0) ***(Marine Corps) Questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called IRs. (MCRP 5-12C)***

key terrain

(joint) Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant. (JP 2-01.3)

line of communications

(joint) A route, either land, water, and/or air, that connects an operating military force with a base of operations and along which supplies and military forces move. Also called LOC. (JP 2-01.3)

***line of sight**

The unobstructed path from a Soldier's/*Marine's* weapon, weapon site, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another.

mobility corridor

(joint) Areas that are relatively free of obstacles where a force will be canalized due to terrain restrictions allowing military forces to capitalize on the principles of mass and speed. (JP 2-01.3)

modified combined obstacle overlay

(joint) A joint intelligence preparation of the operational environment product used to portray the militarily significant aspects of the operational environment, such as obstacles restricting military movement, key geography, and military objectives. Also called MCOO. (JP 2-01.3)

named area of interest

(Army) The geographical area where information that will satisfy a specific information requirement can be collected. (ADRP 1-02) ***(Marine Corps) A point or area along a particular avenue of approach through which enemy activity is expected to occur. Activity or lack of activity within a named area of***

interest will help to confirm or deny a particular enemy course of action. Also called NAI. (MCRP 5-12C)

obstacle

(joint) Any natural or man-made obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in personnel, time, and equipment on the opposing force. (JP 3-15)

operational environment

(joint) A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Also called OE. (JP 3-0)

priority intelligence requirement

(joint) An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or the operational environment. Also called PIR. (JP 2-0) *(Marine Corps) An intelligence requirement associated with a decision that will critically affect the overall success of the command's misison. (MCRP 5-12C)*

request for information

(joint) 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. Also called RFI. (JP 2-0, part 1 of a 2-part definition)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ADP 5-0)

situation template

(joint) A depiction of assumed adversary dispositions, based on that adversary's preferred method of operations and the impact of the operational environment if the adversary should adopt a particular course of action. (JP 2-01.3)

sociocultural factors

(joint) The social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (JP 2-01.3)

target

(joint) 1. An entity or object that performs a function for the adversary considered for possible engagement or other action. 2. In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. 3. An area designated and numbered for future firing. (JP 3-60, parts 1, 2, and 3 of a 4-part definition)

targeting

(joint) The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

terrain analysis

(joint) The collection, analysis, evaluation, and interpretation of geographic information on the natural and man-made features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. (JP 2-03)

terrorism

(Army) The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (U.S. Code, Title 18, Section 2331) *(Marine Corps) The unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political. (JP 3-07.2)*

References

REQUIRED PUBLICATIONS

These documents must be available to the intended user of this publication.

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/new_pubs/jointpub.htm.

JP 1. *Doctrine for the Armed Forces of the United States.* 25 March 2013.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 8 November 2010.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online at http://www.apd.army.mil.

ADRP 1-02. *Terms and Military Symbols.* 24 September 2013.

RELATED PUBLICATIONS

These documents are cited in this publication.

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/new_pubs/jointpub.htm.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01.2. *Counterintelligence and Human Intelligence in Joint Operations.* 26 August 2011. (This classified publication is available on the SIPRNET. Contact the preparing agency of this manual for access instructions.)

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment.* 21 May 2014.

JP 2-03. *Geospatial Intelligence in Joint Operations.* 31 October 2012.

JP 3-0. *Joint Operations.* 11 August 2011.

JP 3-04. *Joint Shipboard Helicopter and Tiltrotor Aircraft Operations.* 6 December 2012.

JP 3-06. *Joint Urban Operations.* 20 November 2013.

JP 3-07.2. *Antiterrorism.* 14 March 2014.

JP 3-07.3. *Peace Operations.* 1 August 2012.

JP 3-07.4. *Counterdrug Operations.* 14 August 2013.

JP 3-12. *Cyberspace Operations*. 5 February 2013. (This classified publication is available on the SIPRNET. Contact the preparing agency of this manual for access instructions.)

JP 3-13. *Information Operations.* 27 November 2012.

JP 3-13.3. *Operations Security.* 4 January 2012.

JP 3-15. *Barriers, Obstacles, and Mine Warfare for Joint Operations.* 17 June 2011.

JP 3-59. *Meteorological and Oceanographic Operations*. 7 December 2012.

JP 3-60. *Joint Targeting.* 31 January 2013.

JP 3-68. *Noncombatant Evacuation Operations.* 23 December 2010.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://www.apd.army.mil.

ADP 3-0. *Unified Land Operations.* 10 October 2011.

ADP 5-0. ***The Operations Process.*** **17 May 2012.**

ADRP 2-0. ***Intelligence*****. 31 August 2012.**

ADRP 3-0. ***United Land Operations.*** **16 May 2012.**

ADRP 3-90. ***Offense and Defense.*** **31 August 2012.**

ADRP 5-0. ***The Operations Process.*** **17 May 2012.**

AR 380-5. ***Department of the Army Information Security Program.*** **29 September 2000.**

AR 381-10. ***U.S. Army Intelligence Activities.*** **3 May 2007.**

ATP 2-01. ***Plan Requirements and Assess Collection*****. 19 August 2014.**

ATP 3-34.80. ***Geospatial Engineering.*** **23 June 2014.**

ATP 3-90.37. ***Countering Improvised Explosive Devices*****. 29 July 2014.**

ATP 5-19. ***Risk Management.*** **14 April 2014.**

ATTP 3-90.15. ***Site Exploitation Operations.*** **8 July 2010.**

ATTP 3-97.11/*MCRP 3-35.1D***.** ***Cold Region Operations.*** **28 January 2011.**

FM 3-06. ***Urban Operations*****. 26 October 2006.**

FM 3-07. ***Stability*****. 2 June 2014.**

FM 3-07.31/MCWP 3-33.8/AFTTP 3-2.40. ***Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations.*** **26 October 2003.**

FM 3-24/*MCWP 3-33.5***.** ***Insurgencies and Countering Insurgencies.*** **13 May 2014.**

FM 3-34.170/*MCWP 3-17.4***.** ***Engineer Reconnaissance.*** **25 March 2008.**

FM 3-38. ***Cyber Electromagnetic Activities.*****12 February 2014.**

FM 3-55. ***Information Collection.*** **3 May 2013.**

FM 3-60. ***The Targeting Process*****. 26 November 2010.**

FM 3-97.6. ***Mountain Operations*****. 28 November 2000.**

FM 4-02. ***Army Health System.*** **26 August 2013.**

FM 6-20-40. ***Tactics, Techniques, and Procedures for Fire Support for Brigade Operations (Heavy).*** **5 January 1990.**

FM 7-15. ***The Army Universal Task List.*** **27 February 2009.**

FM 90-3/*MCWP 3-35.6***.** ***Desert Operations*****. 24 August 1993.**

FM 90-5/*FMFM 7-28***.** ***Jungle Operations*****. 16 August 1982.**

TC 7-100. ***Hybrid Threat.*** **26 November 2010.**

TC 7-100.2. ***Opposing Force Tactics*****. 9 December 2011.**

NAVY AND MARINE CORPS PUBLICATIONS

Most Marine Corps doctrinal publications are available online at https://www.doctrine.usmc.mil/.

Cultural Intelligence Indicator Guide. Quantico, VA: U.S. Marine Corps Intelligence Activity. October 2009. Available online at https://www.intelink.gov/mcia, accessed on 15 October 2014.

Generic Intelligence Requirements Handbook. Quantico, VA: U.S. Marine Corps Intelligence Activity. June 2003. Available online at https://www.intelink.gov/mcia, accessed on 15 October 2014.

MCDP 1-0. Marine Corps Operations**. 9 August 2011.**

MCIP 3-17.02. Marine Air-Ground Task Force Counter-Improvised Explosive Device Operations**. 24 January 2011.**

MCO 3900.15B. Marine Corps Expeditionary Force Development System (EFDS). **10 March 2008. Available online at http://www.marines.mil/News/Publications/ELECTRONICLIBRARY.aspx, accessed on 15 October 2015.**

MCRP 5-12C. Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms.**16 November 2011.**

MCWP 2-2. MAGTF Intelligence Collection. 30 July 2004.

MCWP 2-3. MAGTF Intelligence Production and Analysis. 27 September 2001.

MCWP 3-35.1. Mountain Warfare Operations. 28 February 2014.

MCWP 3-35.3. Military Operations on Urbanized Terrain (MOUT). 26 April 1998.

MCWP 3-35.7. MAGTF Meteorology and Oceanography Support. 30 June 1998.

MCWP 5-1. Marine Corps Planning Process. 24 August 2010.

NWP 3-59M/MCWP 3-35.10.Operational Level Integration of METOC Capabilities. December 2013.

PUBLIC LAWS AND OTHER PUBLICATIONS

Title 18, United States Code, Section 2331, Chapter 113B, *Terrorism.* Available online at http://uscode.house.gov/, accessed on 19 June 2014.

Title 22, United States Code, Section 2656f, Chapter 38, *Annual Country Reports on Terrorism*. Available online at http://uscode.house.gov/, accessed on 19 June 2014.

Swinton, Ernest Dunlop. *The Defence of Duffer's Drift.* Washington, DC: The United States Infantry Association. Available online at www.gutenberg.org, accessed on 23 October 2014.

RECOMMENDED READINGS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

JP 3-16. *Multinational Operations.* 16 July 2013.

JP 3-24. *Counterinsurgency.* 22 November 2013.

JP 4-0. *Joint Logistics.* 16 October 2013.

JP 4-02. *Health Service Support.* 26 July 2012.

JP 5-0. *Joint Operation Planning.* 11 August 2011.

ARMY PUBLICATIONS

ADP 2-0. *Intelligence.* 31 August 2012.

ADP 3-90. *Offense and Defense.* 31 August 2012.

ADP 6-0. *Mission Command.* 17 May 2012.

ADRP 3-37. *Protection*. 31 August 2012.

ADRP 6-0. *Mission Command.* 17 May 2012.

ATP 1-02.1/*MCRP 3-25B/NTTP 6-02.1/AFTTP3-2.5. Multi-Service Brevity Codes.* 20 September 2012.

ATP 3-37.2. *Antiterrorism*. 3 June 2014.

FM 3-24.2. *Tactics in Counterinsurgency*. 21 April 2009.

FM 3-50. *Army Personnel Recovery*. 2 September 2014.

FM 3-90.1. *Tank and Mechanized Infantry Company Team.* 9 December 2002.

FM 7-100.1. *Opposing Force Operations*. 27 December 2004.

FM 7-100.4. *Opposing Force Organization Guide*. 3 May 2007.

TC 3-97.61. *Military Mountaineering.* 26 July 2012.

NAVY AND MARINE CORPS PUBLICATIONS

MCWP 2-1. Intelligence Operations. 10 September 2003.

MCWP 3-1. Ground Combat Operations. 4 April 1995.

MCWP 3-17. Engineering Operations. 14 February 2000.

PRESCRIBED FORMS

None.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate Web site: www.apd.army.mil.

DA Form 2028. ***Recommended Changes to Publications and Blank Forms*****.**

Index

Entries are by paragraph number unless indicated otherwise.

A

affiliated forces. *See* irregular forces.

antiterrorism
  definition, 8-5

area of influence, 9-68
  Army definition, 3-6
  Marine Corps definition, 3-11

area of interest, 1-6, 1-32, 3-2, 4-121, 5-11, 9-68, A-3
  characteristics, 4-1–4-4
  considerations, 3-8–3-11
  definition, 3-7
  in stabililty operations, 3-8
  intelligence requirements, 8-5
  limits, 3-7

area of operations (AO), 1-6, 3-2, A-23
  analysis of, 3-10, A-22
  and civil considerations, 3-19, 3-21, 4-86
  and site exploitation, 10-23
  definition, 3-5
  economic conditions in, 7-48, 7-49
  FHA support, 1043
  for *MAGTFs*, 3-11
  in cyberspace domain, 9-68
  in operational environment, 3-1
  infrastructure conditions in, 7-48
  relief support, 10-40

ASCOPE. *See also* PMESII-PT/*PMESII* and civil considerations.

ASCOPE characteristics, 4-88, 4-117, 4-121
  areas, 4-89, 4-90
  capabilities, 4-94–4-96
  events, 4-114–4-116
  organization, 4-97–4-104
  people, 4-105–4-113
  structures, 4-91–4-93

avenues of approach (AAs), 1-24
  air and ground routes, 4-19
  and mobility corridors, 4-24
  aspect of terrain, 3-15–3-17
  characteristics of battle positions, 5-32
  development, 4-19
  during offensive tasks, 4-19
  in defense operations, 4-19
  OAKOC/*KOCOA* considerations, 9-28, 9-29

B

battlespace environment, 10-29, 10-34, 10-40

beach landing sites, 4-81

begin morning civil twilight (BMCT)
  definition, 4-62

begin morning nautical twilight (BMNT)
  definition, 4-62

C

civil considerations
  and dispaced civilians, 4-89, 6-17, 7-4, 7-10
  and drug trafficking operations, 10-7–10-14
  and intelligence target packages, 1-30
  and mission variables, 1-5–1-9, 1-12, 2-2
  and state of governance, 4-5
  and the local population, 4-97–4-104
  characteristics, 4-86
  data file, 4-90–4-93, 4-96, 4-104, 4-107, 4-113–4-126
  in an area of interest, 1-1
  in a desert environment, 9-44–9-58
  in a jungle environment, 9-36–9-43
  in the area of operations, 3-5
  in the operational environment, 1-15, 1-20, 10-7
  in urban environment, 9-3
  lessons learned, A-18
  products and tools 2-11, 2-15
  overlays and assessments, 1-22, 1-24, 2-24, 4-88
  samples of ASCOPE, A-19
  tactical decision aids, 2-21

civil considerations categories (ASCOPE), 3-18

civil security subtasks, 7-28, 7-29

COA, 2-21
  analysis/*wargaming*, 2-23
  IPB products, 2-23

COA development, 2-22, 6-2, 6-29
  six-step process, 6-5

combat operations/*major operations,* 3-19, 4-95, 4-115, 10-32
  and terrain analysis, 9-8
  and weather aspects, 4-68
  in the area of interest, 3-8

commander's critical information requirements (CCIRs), 2-13, 2-18, 8-18, 10-22, A-11, A-15

concealment defined, 4-49

counterdrug activities
  definition, 10-5
  IPB support to, 10-6, 10-10–10-14
  law enforcement support, 10-2

counter-IED operations, 10-17–10-19

counterinsurgency
  Marine Corps doctrine, 7-21, 7-22

counterinsurgency operations, 4-32, 4-108, 5-86, 5-125, 7-16, definition, 7-16

counterinsurgency operations and stability tasks, 2-24, 7-16–7-26, 7-54–7-60

counter-proliferation, 10-15

course of action. *See* COA.

cover definition, 4-48

cover and concealment
  in desert terrain, 9-64
  in jungle terrain, 9-43
  in mountainous terrain, 9-33
  in natural terrain, 4-50
  in open or arid environment, 4-28
  in urban terrain, 4-51
  OAKOC/*KOCOA* considerations, 9-33

cultural factors categories, 4-111

cyber electromagnetic activities/*cyberspace operations*, 9-65–9-70

*cyberspace*definition, 9-65

Entries are by paragraph number unless indicated otherwise.

D

decision support template
Marine Corps definition, A-11
decisive point/*center of gravity*, 7-55
decisive terrain, 4-33
defensive cyberspace operations, 8-9
defensive operations
Marine Corps definition, 7-10
defensive operations products
enemy capabilities statement, 7-15
enemy organizational charts, 7-15
enemy situation overlays with COA statements, 7-15
event template with matrix, 7-15
HVTL, 7-15
intelligence requirements, 7-15
MCOO, 7-15
relative target value matrix, 7-15
weather effects matrix/*operational impacts chart*, 7-15
defensive tasks/*operations*
Army and *Marine Corps* definition, 7-10
defensive tasks/*operations* types
area defense, 7-10–7-12
mobile defense, 7-10, 7-13
retrograde, 7-10, 7-11–7-15
desert environment considerations, 9-44–9-64

E

economic and infrastructure development, 7-50–7-53
electronic protection, 8-10
end evening civil twilight (EECT) definition, 4-62
end of evening nautical twilight definition, 4-62
enemy definition, 3-13
enemy defensive overlay steps, 6-37
enemy forces
in the AO, 7-32
enemy offensive overlay steps, 6-34
enemy situation overlay, 1-22
essential elements of friendly information (EEFIs), 2-13
event matrix construction, 6-54
event template
construction, 6-53
example, 6-56
event template and event matrix, 1-22, A-9
exploitation of sensitive sites, 10-24, 10-25

F

FHA, 10-41–10-43
and humanitarian civil assistance, 7-45
in small-scale joint operations, 8-17
fields of fire, 4-42, 4-43
force protection
and rules of engagement, 10-40
force protection and operations security, 8-24
foreign humanitarian assistance. *See* FHA.
functional analysis
capabilities, B-24–B-28
defined, B-1
method, B-21
steps, B-6

G

generate intelligence knowledge process, 1-4

H

high-payoff target (HPT) definition, 1-24, 1-29
high-value target (HVT), 1-24, 5-104
high-value target list (HVTL), 1-22
high-payoff target list (HPTL) definition, 1-29
humanitarian and disaster relief operations, 10-38–10-47
hybrid threat/*adversary*, 5-6
hybrid threat/*adversary* forces
capabilities and limitations, 5-72
combat effectiveness, 5-48
composition, 5-21, 5-22
current operations, 5-80
disposition, 5-39
doctrine and tactics, 5-52–5-54
electronic technical data, 5-65
historical data, 5-84, 5-85
miscellaneous data, 5-94
strength, 5-43, 5-44
support and relationships, 5-58

I

Information assurance, 8-8
information collection strategy/*intelligence collection strategy*, 1-12
intelligence estimate, 1-22
intelligence preparation of the battlefield/*battlespace*. *See* IPB.
intelligence requirements, 1-8, 1-13, 6-46
and civil considerations, 4-120
during IPB, 7-6–7-9
in defensive operations, 7-10–7-15
in offensive operations, 7-4
intelligence target packages, 1-30
intervisibility lines, 4-38
IPB
and decisionmaking, 2-1, 2-2
and generate intelligence knowledge, 1-39–1-41
and ISR and information collection/*intelligence collection*, 1-32–1-38
and planning, 2-3
and risk management, 1-31
and situation development, 1-42–1-44
and targeting, 1-27–1-30
definition (Army and *Marine Corps*), 1-1
function, 1-6
G-2/S-2 role, 1-2, 1-4
refinement, 1-9
IPB process, 1-1, 1-10
Step 1, 1-11–1-14
Step 2, 1-15, 1-16
Step 3, 1-17, 1-18
Step 4, 1-19–1-21
IPB products, 1-22
in support of counterdrug activities, 10-14
IPB relationships, 1-26
IPB support to partnerships, 8-15
in irregular warfare, 8-21–8-24
in peace operations, 8-19, 8-20
in small-scale joint operations, 8-17, 8-18
IPB support to protection/*force protection,* 8-1
tasks, 8-3–8-14
irregular forces, 5-61
overlay steps, 6-39–6-41
irregular threat/*adversary* forces, 5-6
capabilities and limitations, 5-71

Entries are by paragraph number unless indicated otherwise.

irregular threat/*adversary* forces *(continued)*
combat effectiveness, 5-47
composition, 5-17–5-20
current operations, 5-79
disposition, 5-29–5-38
doctrine and tactics, 5-51
electronic technical data, 5-64
historial data, 5-83
miscellaneous data, 5-89
strength, 5-42
support and relationships, 5-57
irregular warfare missions, 8-22

J

joint operations planning process (JOPP) steps, 10-5
jungle environment considerations, 9-34–9-43

K

key terrain
concepts and examples, 4-35
considerations, 4-29
definition, 4-28
in counterinsurgency operations, 7-55
in the defense, 4-32
in the offense, 4-31

L

light and illumination table, 1-22
line of sight
analysis, 4-46–4-50
definition, 4-43

M

Marine Corps Planning Process (MCPP)
six-step process, 2-6, 2-7
tools, Appendix A
military decisionmaking process (MDMP)
seven-step process, 2-4, 2-5, 2-7
MDMP/*problem framing step of MCPP*, 2-21
meteorological and oceanographic (METOC)
and *MAGTF*, 4-80
considerations, 4-80
Navy counterparts, 4-82
parameters and forecastors, 6-17
personnel, 4-69, 4-81, 4-82
products, 4-84
support requirements, 4-80
military aspects of weather
atmospheric pressure, 4-61, 4-72
cloud cover/*ceiling*, 4-61, 4-66, 4-67
humidity, 4-61, 4-71
precipitation, 4-61, 4-65
sea state, 4-61, 4-73
temperature, 4-61, 4-68–4-70, 4-19
visibility, 4-61, 4-63
wind, 4-61, 4-64
mission variables civil considerations, 1-1–1-5, 1-12, 1-42, 2-2, 5-112, 6-9, A-3
enemy, terrain, and weather, 1-6
mobility corridor
definition, 4-20
ranges, 4-24
modified combined obstacle overlay (MCOO), 1-22

N

named area of interest (NAI) example, 1-36
natural terrain
analysis, 4-10
example, 4-17

O

OAKOC/KOCOA
analysis, 4-45
avenues of approach, 9-28, 9-29
considerations, 9-27, 9-30, 9-31
cover and concealment, 9-33
key terrain, 9-30, 9-31
observation and fields of fire, 9-27
obstacles, 9-32
observation and fields of fire, 3-15, 4-28, 4-37, 4-47, 9-27
in desert, 9-60
in jungle, 9-39
in mountainous terrain, 9-27
in natural terrain, 4-28, 4-37–4-47
in urban terrain, 4-47
obstacles definition and examples, 4-13
offensive tasks/*operations*
Army and *Marine Corps* definition, 7-4
offensive tasks/*operations* types
attack, 7-4, 7-7
exploitation, 7-4, 7-8
movement to contact, 7-4, 7-6
pursuit, 7-4, 7-9
operational environment, 1-13, 1-14
adaptation, 5-73
operational environment/*battlespace environment*, 10-29
operational variables, 1-4, 1-5, 1-39, 4-86

P

peace enforcement definition, 10-33
peace operations
peace enforcement, 10-16, 10-33
peacekeeping, 10-16, 10-27
peacekeeping definition, 10-28
PMESII-PT/*PMESII*. *See also* ASCOPE.
and intelligence survey, 1-39
defined, 1-4
examples, 4-86

R

range of military operations, 4-80
hybrid forces capabilities, 5-73
methodology, B-28
rapid decisionmaking and synchronization process/*rapid response planning process (*RDSP/*R2P2)*
Army steps, 2-27
Marine Corps steps, 2-28
regular threat/*adversary* forces, 5-6
capabilities and limitations, 5-70
combat effectiveness, 5-46
composition, 5-16
current operations, 5-78
disposition, 5-24–5-28
doctrine and tactics, 5-50
electronic technical data, 5-63
historical data, 5-82
miscellaneous data, 5-88
strength, 5-41
support and relationships, 5-56
relationships
of intelligence staff, 5-10
relationships and support
of hybrid threat/*adversary* forces, 5-58–5-61
of irregular threat/*adversary* forces, 5-56, 5-57
of regular threat/*adversary* forces, 5-56
running estimate, 1-9, 2-27, 3-20, 4-19

Entries are by paragraph number unless indicated otherwise.

S

site exploitation, 10-22, 10-23

situation template, 1-24, 2-21–2-24, A-8
- example, 6-27, 6-7
- for threat/*adversary* COAs, 6-25–6-33

sociocultural
- and economic issues, 10-29, 10-34
- definition, 4-87
- factors, 4-105, 4-124
- information, 1-25, 10-30, 10-35
- research and analysis, 1-25

stability operations definition, 7-17

staff collaboration examples and roles, 1-23, 1-24

support governance, 7-45

T

tactical decision aids, 2-11, 2-21, 4-76

terrain analysis, 10-9
- and geospatial intelligence cells, 4-11
- defined, 4-9
- in counterdrug activities, 10-9
- in natural and urban terrain, 9-2
- in site exploitation, 10-23
- in the operational environment, 4-12
- in urban operations, 9-6–9-8
- software, 9-6
- types of line of sight, 4-43

terrain and weather
- analysis, 5-98, 10-13
- effects, 6-17, 6-37, 7-4, 10-8
- influences, 3-14–3-17
- products, 2-11

terrain effects tools
- MCOO, 4-52–4-58
- terrain effects matrix, 4-59

terrorism
- Army and *Marine Corps* definition, 8-4

terrorist network components, 8-5

threat definition, 5-5

threat characteristics/*adversary order of battle*
- analysis, 5-6–5-8
- examples, 3-1, 5-1
- files, 5-2, 7-34

threat characteristics/*adversary order of battle* areas
- capabilities and limitations, 5-10, 5-66–5-76
- combat effectiveness, 5-10, 5-45–5-48
- composition, 5-10, 5-13–5-22
- current operations, 5-10, 5-77–5-80
- disposition, 5-10, 5-23–5-39
- doctrine and tactics, 5-10, 5-49–5-54
- electronic technical data, 5-10, 5-62–5-65
- historical data, 5-10, 5-81–5-85
- miscellaneous data, 5-10, 5-86–5-94
- strength, 5-10, 5-40–5-44
- support and relationships, 5-10, 5-55–5-61

threat characteristics/*adversary order of battle* areas, 1-32, 5-10–5-94

threat evaluation, 10-11

threat/*adversary* capabilities and COAs, 5-108, 5-109

threat/*adversary* COA
- process, 6-4, 6-5
- products, 6-24
- statement, 6-42

threat/*adversary*
- forces categories, 5-6, 5-50
- models, 5-2, 5-95–5-106
- templates and purpose, 5-97–5-100, 5-111–5-116

troop leading procedures (TLP)
- definition, 2-8
- steps, 2-9–2-20

U

unified action
- Army contribution, 7-2
- definition, 7-1
- *Marine Corps* considerations, 7-3

unique missions
- counterdrug activities, 10-5
- defined, 10-1

unique urban
- characteristics, 9-3
- operations, 9-3

urbans, 9-3
- operations, 9-3
- terrain example, 4-

W

warning order, 2-13

weather analysis, 10-10

weather effects matrix/*operational impact chart,* 1-22

weather effects on military operations, 4-74

weather estimate, 1-22

weather forecast chart, 1-22

ATP 2-01.3/MCRP 2-3A
10 November 2014

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1430301

By Direction of the Commandant of the Marine Corps:

K. J. GLUECK, JR.
Lieutenant General, U.S.
Marine Corps
Deputy Commandant
Combat Development
and Integration

DISTRIBUTION:

Active Army, the Army National Guard, and the United States Army Reserve. **Not to be distributed; electronic media only.**

USMC

MCTP 2-10B
(Formerly MCWP 2-3)

MAGTF Intelligence Production and Analysis

US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 147 000012 00

USMC

CD&I (C 116)

2 May 2016

ERRATUM

to

MCWP 2-3

MAGTF INTELLIGENCE PRODUCTION AND ANALYSIS

1. Change all instances of MCWP 2-3, *MAGTF Intelligence Production and Analysis***, to MCTP 2-10B,** *MAGTF Intelligence Production and Analysis.*

2. Change PCN 143 000076 00 to PCN 147 000012 00

3. File this transmittal sheet in the front of this publication.

PCN 147 000012 80

To Our Readers

Changes: **Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to morgann@mccdc.usmc.mil. Recommendations should include the following information:**

- **Location of change**
  - **Publication number and title**
  - **Current page number**
  - **Paragraph number (if applicable)**
  - **Line number**
  - **Figure or table number (if applicable)**
- **Nature of change**
  - **Add, delete**
  - **Proposed new text, preferably double-spaced and typewritten**
- **Justification and/or source of change**

Additional copies: **A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status*. An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: http://www.doctrine.usmc.mil.**

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

MCCDC (C 42)
13 Jul 2004

E R R A T U M

to

MCWP 2-3

MAGTF INTELLIGENCE PRODUCTION AND ANALYSIS

1. Change the publication short title to read “MCWP 2-3” (vice MCWP 2-12).

PCN 143 000076 80

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380-1775

27 September 2001

FOREWORD

Marine Corps Doctrinal Publication 2, *Intelligence*, and Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations,* provide the doctrine and higher order tactics, techniques, and procedures for intelligence operations. MCWP 2-12, *MAGTF Intelligence Production and Analysis,* complements and expands upon this information by detailing doctrine, tactics, techniques, and procedures for the conduct of intelligence production and analysis in support of the Marine air-ground task force (MAGTF).

The target audience of this publication is intelligence personnel responsible for the planning and execution of intelligence production and analysis operations.

The MCWP 2-12 provides the information needed by Marines to understand, plan, and execute intelligence production and analysis to support MAGTF operations. It describes intelligence doctrinal fundamentals, the nature of analytical thinking, intelligence preparation of the battlespace, and intelligence support to targeting. This publication also discusses intelligence command and control, communications and information systems support, intelligence products and formats, planning, execution, and training.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

/s/
EDWARD HANLON, JR.
Lieutenant General, U. S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: 143 000076 00

MAGTF INTELLIGENCE PRODUCTION AND ANALYSIS

TABLE OF CONTENTS

Chapter 1 Fundamentals

What is Intelligence Production and Analysis? 1-1
- **Intelligence Functions** 1-1
- **Intelligence Cycle** 1-1

Production Steps 1-3
- **Preparation for Analysis** 1-3
- **Analytical Process** 1-4
- **Product Preparation** 1-5

Operations and Command and Control 1-5
Production and Analysis Company, Intelligence Battalion 1-5

Chapter 2 Organizations and Responsibilities

MAGTF Commander 2-1
- **Focus the Analytical and Production Effort** 2-1
- **Participate in the Analytical Process** 2-1
- **Evaluate the Product** 2-1

Marine Expeditionary Force Command Element Intelligence Officer 2-2
Intelligence Battalion Commander 2-2
- **Responsibilities in Garrison** 2-2
- **Responsibilities During Operations** 2-2

Intelligence Battalion 2-3
Production and Analysis Company 2-3
- **All-Source Fusion Platoon** 2-3
- **Organization for Support** 2-3

Production and Analysis Cell 2-4
- **Tasks** 2-4
- **Organization** 2-4
- **Supporting Organizations** 2-6

Principal Staff Officers 2-7
Unit Intelligence Officer 2-8
Organic Intelligence Sections 2-8
Organization for Employment 2-8
- **Combat Intelligence Center** 2-8
- **Command and Control** 2-9
- **Senior Marine Expeditionary Force Intelligence Staff Officers** 2-10
- **Intelligence Production Support Flow** 2-10
- **Organization for Combat Operations** 2-10

Communications and Information Systems **2-12**
Basic Requirements **2-12**
Information Systems **2-13**

Chapter 3 Filtering, Recording, and Evaluating

Section I Filtering

Filtering Criteria **3-2**
Subject Matter **3-2**
Location **3-2**
Time of Occurrence **3-2**
Redundancy **3-2**
Methodology **3-2**
Manual Filtering **3-2**
Automated Filtering **3-2**

Section II Recording

Methodology **3-3**
Recording Tools **3-3**
Intelligence Journal **3-4**
Enemy Situation Map **3-5**
Intelligence Workbook **3-6**
Order of Battle Files **3-6**
Target Files **3-11**
Tools Automation **3-11**

Section III Evaluation

Relevance **3-12**
Reliability **3-12**
Accuracy **3-12**
Evaluation Rating System **3-12**
Reliability Evaluation Codes **3-13**
Accuracy Evaluation Codes **3-13**

Chapter 4 Analytical Thinking

Section I Analytical Process

Analysis **4-1**
Synthesis **4-2**
Estimation **4-2**

Section II Analytic Problem Solving

Analytical Theories 4-3
Proposition or Premise 4-3
A Priori 4-4
Applied Logic 4-4
Facts 4-4
Opinions 4-4
Inferences 4-4
Reasoning 4-5
Deductive 4-5
Inductive 4-6
Tests of Truth 4-7
Correspondence Test of Truth 4-7
Coherence Test of Truth 4-7
Pragmatic Test of Truth 4-8

Section III Pitfalls of Analysis

Logical Fallacies 4-9
Omission 4-9
Assumption 4-11
Biases 4-12
Cultural 4-12
Organizational 4-13
Personal 4-13
Cognitive 4-13

Section IV Decisionmaking

Analytical 4-15
Intuitive 4-15
Comparison 4-15

Chapter 5 Intelligence Preparation of the Battlespace

Section I Step 1—Define the Battlespace Environment

Identify Significant Characteristics of the Environment 5-2
Identify the Command's Area of Operations and Battlespace Limits 5-2
Area of Influence 5-2
Area of Interest 5-4
Battlespace 5-4
Establish the Area of Interest Limits 5-4
Identify the Detail Required for the Time Available 5-5

Evaluate Existing Intelligence Data Bases and Identify Intelligence Gaps 5-5
Collect the Required Intelligence and Materials. 5-6

Section II Step 2—Describe the Battlespace Effects

Analyze the Battlespace Environment 5-6
Terrain. 5-6
Weather. 5-10
Other Characteristics of the Battlespace. 5-11
Describe the Battlespace Effects on Threat and Friendly Capabilities and Broad Courses of Action. 5-12

Section III Step 3—Evaluate the Threat

Update or Create Threat Models. 5-13
Doctrinal Templates 5-13
Description of Tactics and Options 5-13
Identification of Center(s) of Gravity 5-14
Critical Vulnerabilities 5-14
Identification of Type High-Value Targets 5-14
Identify Threat Capabilities 5-14

Section IV Step 4—Determine Threat Courses of Action

Identify the Threat's Likely Objectives and Desired End State 5-15
Identify the Full Set of Courses of Action Available to the Threat 5-15
Evaluate and Prioritize Each Course of Action 5-17
Develop Each Threat Course of Action in the Amount of Detail Time Allows 5-18
Situation Template 5-18
Description of the Threat's Courses of Action and Options. 5-19
High-Value Targets. 5-21
Identify Initial Intelligence Collection, Production, and Dissemination Requirements 5-22
Event Template 5-23
Event Matrix 5-24

Section V Decision Support Template

Targeted Areas of Interest. 5-25
Decision Points 5-26
Types. 5-26
Considerations 5-26

Section VI Abbreviated Intelligence Preparation of the Battlespace Process

Work Ahead 5-27
Focus on Essentials 5-28
Stay Objective Oriented 5-28
Minimize Essentials 5-28
Output 5-29
Intelligence Estimate 5-29
Target and Objective Studies 5-29

Chapter 6 Analysis of the Battlespace

Section I Responsibilities

Section II Characteristics of the Battlespace

Section III Terrain Analysis

Responsibilities 6-2
Sources of Information 6-3
Geospatial Factors 6-3
Surface Configuration 6-3
Hydrologic Features 6-3
Vegetation Features 6-4
Surface Materials 6-5
Military Aspects of Terrain Evaluation 6-5
Key Terrain 6-5
Observation and Fields of Fire 6-6
Cover and Concealment 6-6
Obstacles 6-7
Avenues of Approach and Mobility Corridors 6-7

Section IV Hydrographic Analysis

Sources of Information 6-9
Hydrographic Conditions 6-9
Seas, Swells, and Surf 6-9
Tides 6-9
Currents 6-9
Beach Selection Considerations 6-10
Size 6-10
Approaches 6-11
Gradient 6-11
Composition 6-11
Trafficability 6-11

Vegetation 6-11
Natural Obstacles 6-11
Manmade Obstacles 6-12
Exits 6-12

Section V Airspace Analysis

Geospatial Analysis Support 6-13
Airspace Evaluation 6-13
Military Aspects of Terrain Evaluation 6-14
Key Terrain 6-14
Observation and Fields of Fire 6-14
Cover and Concealment 6-14
Obstacles 6-14
Avenues of Approach 6-15
Weather 6-15

Section VI Weather Analysis

Responsibilities 6-15
Weather Effects 6-15
Temperature and Humidity 6-16
Precipitation 6-16
Visibility 6-17
Wind Speed and Direction 6-17
Cloud Conditions 6-18
Atmospheric Pressure 6-18
Weather Forecast and Weather Effects Products 6-18

Section VII Infrastructure Analysis

Sources of Information 6-20
Transportation System 6-20
Highway or Road Network 6-20
Railroad Network 6-21
Port and Harbor Facilities 6-21
Airfields 6-22
Structures and Crossings 6-22
Inland Waterways 6-24
Supply Systems 6-24
Power System or Grid 6-24
Petroleum, Oils, and Lubricants Facilities 6-25
Water 6-25
Telecommunications 6-25

Urban Areas 6-25
Characteristics 6-25
Urban Area Classification 6-25
Evaluation Factors 6-26
Construction Resources 6-26

Section VIII Political, Economic, and Sociological Analysis

Political Intelligence 6-26
Basic Governmental Principles 6-27
Governmental Operations 6-27
Foreign Policy 6-27
Political Parties 6-27
Pressure Groups 6-27
Electoral Procedures 6-28
Subversive Movements 6-28
Criminal and Terrorist Organizations 6-28
Economic Intelligence 6-28
Sources of Economic Intelligence 6-29
Evaluation Factors 6-29
Narcotics and Terrorism 6-29
Sociological Analysis 6-29
Population 6-29
Characteristics of the People 6-29
Public Opinion 6-30
Education 6-30
Religion 6-30
Public Welfare 6-30
Narcotics and Terrorism Tolerance 6-30

Chapter 7 Threat Analysis Techniques

Section I Intelligence Preparation of the Battlespace Techniques

Threat Order of Battle 7-1
Order of Battle Factors 7-1
Analytical Considerations 7-5
Threat Model Development 7-5
Doctrinal Templates 7-5
Description of Tactics and Options 7-5
Identification of Type High-Value Targets 7-7
Threat Courses of Action Determination 7-8
Criteria for Testing Threat Courses of Action 7-8
Considerations 7-8
Course of Action Evaluation and Prioritization 7-9

Course of Action Development 7-9
Course of Action Parts 7-10
Considerations 7-10
Course of Action Key Elements 7-10

Section II Specialized Analytical Techniques

Subsystem Threat Analysis 7-11
Air Defense 7-11
Artillery 7-12
Aviation 7-12
Counterintelligence 7-13
Command and Control Warfare 7-13
Engineer 7-14
Combat Service Support 7-15
Pattern Analysis 7-15
Coordinates Register 7-16
Pattern Analysis Plot Sheet 7-16
Matrix Analysis 7-17
Activities Matrix 7-17
Association Matrix 7-19
Link Analysis 7-19
Indicator List 7-20

Chapter 8 Target Development and Combat Assessment

Section I Targeting

Targeting Cycle 8-1
Target Development 8-2
Intelligence Preparation of the Battlespace 8-3
Target Value Analysis 8-3
High-Value and High-Payoff Target Identification 8-3
High-Payoff Target List 8-4
Target Analysis 8-4
Target System Analysis 8-4
Target Complex Analysis 8-6
Target Element Analysis 8-6
Role of the Target Analyst 8-7
Target Analysis Products 8-7
List of Targets 8-7
No-Strike Target List 8-7
Restricted Target List 8-7
Target File 8-8
Collection Requirements 8-8
Target or Objective Studies 8-8

Section II Combat Assessment

Battle Damage Assessment 8-9
Munitions Effects Assessment 8-9
Reattack Recommendations 8-9
Battle Damage Assessment Components 8-10
Physical Damage Assessment 8-10
Functional Damage Assessment 8-11
Target System Assessment 8-12
Responsibilities 8-13
Battle Damage Assessment Methodology 8-14
Battle Damage Assessment Principles 8-14
Objectivity 8-14
Reliability 8-14
Accuracy 8-15
Battle Damage Assessment Reporting 8-15
Reports 8-15
Reporting Methods 8-15

Chapter 9 Intelligence Production

Production Categories 9-1
Deliberate Production 9-1
Immediate Production 9-2
Principles 9-2
Purpose and Use of Intelligence 9-2
Objectivity 9-2
Provision of Integrated and Tailored Products 9-2
Coordination Among Echelons 9-2
Responsibilities 9-2
Management 9-3
Production Cycle 9-3
Define Intelligence Requirements 9-3
Define and Prioritize Intelligence Production Requirements and Tasks 9-3
Develop Intelligence Production Plan and Schedule 9-4
Allocate Resources 9-4
Assign Tasks 9-4
Prepare the Product(s) 9-5
Review and Quality Control 9-5
Approve and Distribute the Product(s) 9-5
Follow Up 9-5
Production Management 9-5
Functions 9-5
Production Managers 9-5
Production Management Elements 9-6

Intelligence Products 9-6
MAGTF Contingency Intelligence Study 9-7
Intelligence Estimate and Supporting Studies 9-7
Target or Objective Study 9-7
Intelligence Summary 9-7
Intelligence Report 9-7
Briefings 9-8
Organic MAGTF Intelligence Production 9-8
Unit Intelligence Sections 9-8
Intelligence Direct Support Teams 9-9
Production and Analysis Company, Intelligence Battalion 9-9
External Production Support 9-9
Department of Defense Support 9-9
National Production Support 9-10
Unified Command Production Support 9-10
Services Production Support 9-11
Non-Department of Defense Intelligence Production Support 9-12
Production Support Requests 9-12
Request Process 9-14
Request Format 9-14
Automated Production Request Procedures 9-14

Chapter 10 Operations

Section I Operational Maneuver From the Sea

Requirements 10-1
Considerations 10-2
Support During Planning 10-2
Support During Execution 10-3

Section II Sustained Operations Ashore

Considerations 10-4
Support During Planning 10-4
Support During Execution 10-4

Section III Military Operations Other Than War

Requirements 10-5
Considerations 10-5
Support During Planning 10-5

MOOTW IPB Requirements 10-6
Define the Battlespace Environment 10-6
Describe the Battlespace Effects 10-6
Evaluate the Threat 10-7
Determine Threat Courses of Action 10-8
MOOTW IPB Products 10-8
Population Status Overlay 10-8
Logistics Sustainability Overlay 10-8
Lines of Communications Overlay 10-8
Key Facilities and Target Overlay 10-10
Coordinates Register and Pattern Analysis Plot Sheet. 10-10

Section IV Joint Operations

Responsibilities 10-11
Marine Corps Component Production and Analysis 10-11
Joint Task Force Headquarters Production and Analysis 10-11
Key Functions 10-11
Support During Planning 10-12
Support During Execution 10-12

Section V Combined Operations

Principles 10-12
Adjustment of National Differences Among Nations 10-12
Unity of Effort Against Common Threat. 10-12
Intelligence Determination and Planning. 10-12
Special Arrangements 10-13
Full Exchange of Intelligence 10-13
Complementary Intelligence Operations 10-13
Combined Intelligence Centers 10-13
Liaison Exchange. 10-13
Foreign Disclosure and Releasability. 10-13
Policies and Procedures 10-13
Security 10-14
Product Format Considerations 10-14
Information Sources. 10-14

Section VI Pre-Crisis Phase

Data Base Management 10-15
Intelligence Reference Library. 10-15
Statement of Intelligence Interest. 10-15
Intelligence Data Bases 10-16

Production 10-16
Contingency Intelligence 10-16
Intelligence Preparation of the Battlespace 10-17
Exercise Intelligence 10-18
Other Intelligence 10-18
Production and Analysis Training 10-18
Individual Training 10-18
Element Training 10-19
Unit Training 10-19
MAGTF Training 10-20

Section VII Warning and Deployment Phase

Initial Production and Analysis 10-20
Determine Initial Requirements 10-20
Assemble and Focus Data Bases 10-20
Develop Initial Estimate and Supporting Studies 10-20
Develop Collection, Production, and Dissemination Requirements 10-21
Production Management 10-21
Standardization of Products 10-21

Section VIII Execution Phase

Production Management 10-21
Support to Current Operations 10-22
Support to Future Operations 10-22
Support to Future Plans 10-23
Support to Targeting 10-23

Appendices

A **Intelligence Estimate Format** A-1
B **Weather Critical Values** B-1
C **Tactical Indicators** C-1
D **Battle Damage Assessment Report Format** D-1
E **MAGTF Intelligence Production Plan Format** E-1
F **Intelligence Summary Format** F-1
G **Intelligence Report Format** G-1
H **Intelligence Information Brief** H-1
I **Production Requirement and Request for Intelligence Format** I-1
J **Glossary** J-1
K **References** K-1

Figures

1-1 Intelligence Cycle. 1-1
1-2 Intelligence Cycle in Support of Commander's Decision 1-2
1-3 Intelligence Support to Planning and Decisionmaking 1-6

2-1 Intelligence Battalion Organization 2-3
2-2 IIP Organization. 2-6
2-3 Topographic Platoon Organization 2-6
2-4 CI/HUMINT Company Organization 2-7
2-5 IOC Organization. 2-10
2-6 C2 and Staff Cognizance of Intelligence Production Support Flow 2-11
2-7 Notional MEF CIS Architecture 2-14

3-1 Example of an Intelligence Journal Page. 3-4
3-2 Example of a Unit Workbook Page 3-8
3-3 Example OOB Overlay 3-9
3-4 Sample OOB Record 3-10

5-1 Battlespace Examination 5-3
5-2 AO and AOI. 5-3
5-3 Battlespace Dimensions and Factors 5-4
5-4 Regimental Ground AA 5-7
5-5 Air AAs Overlay 5-8
5-6 Mobility Corridors Grouped to Form an AA. 5-9
5-7 Lines of Communications and Likely Ambush Sites. 5-9
5-8 Combined Obstacle Overlay 5-10
5-9 Doctrinal Template. 5-13
5-10 Combining Doctrine and Battlespace Effects to Develop Threat COAs 5-16
5-11 Enemy COA 1—Counterattack 5-17
5-12 Enemy COA 2—Withdrawal from the Current Position and Set Up Defense on Eastern Shore of River. 5-17
5-13 Counterattack Situation Template with TPLs and HVTs 5-19
5-14 Threat COA Overlay with Text Description 5-20
5-15 Intelligence Synchronization Matrix 5-20
5-16 Intelligence Synchronization Sheet 5-21
5-17 Templated Locations of HVTs for Enemy COA 1 5-22
5-18 Event Template 5-23
5-19 Event Template Development by Comparing and Contrasting Each COA's NAIs and Indicators. 5-24
5-20 Detailed Event Matrix for a Specific NAI. 5-25
5-21 Decision Support Template 5-26

6-1 Concealment and Cover Overlay 6-6
6-2 Weather Forecast Graphic 6-19
6-3 Weather Effects Matrix 6-19

Figures (Continued)

7-1 Threat Synchronization Matrix 7-6
7-2 Threat Model with Target Value Matrix 7-7
7-3 Coordinates Register 7-16
7-4 Pattern Analysis Plot Sheet 7-17
7-5 Activities Matrix 7-18
7-6 Association Matrix. 7-19
7-7 Link Diagram. 7-19

8-1 Joint Targeting Cycle and D3A 8-2
8-2 Target System, Components, and Elements 8-5
8-3 Combat Assessment Process 8-9
8-4 Phase I BDA or PDA Information Flow 8-10
8-5 Phase II BDA or FDA Information Flow 8-12
8-6 Phase III BDA or TSA Information Flow 8-13

9-1 IPR Flow 9-13

10-1 Population Status Overlay 10-9
10-2 Logistics Sustainability Overlay 10-9
10-3 Sewers and Subterranean Overlay 10-10

Tables

2-1 P&A Company Organization for Support 2-3
2-2 MEF CE's CIC Key Elements 2-9
2-3 Senior Intelligence Staff Officers 2-11

6-1 Landform Elevations 6-3

8-1 Example of Combat Strength Assessment. 8-11

CHAPTER 1. FUNDAMENTALS

Marine air-ground task force (MAGTF) intelligence provides decision-makers with an understanding of the battlespace. This understanding encompasses a sophisticated knowledge of the threat and the physical, political, economic, and cultural environment in the area of operations (AO). That knowledge is developed through intelligence production and analysis (P&A).

What is Intelligence Production and Analysis?

P&A is the filtering, recording, evaluating, and analyzing of information, and product preparation of developed intelligence.

Analysis is a process that involves sifting and sorting evaluated information to isolate significant elements related to the mission of the command, determining the significance of the information relative to information and intelligence already known, and drawing deductions about the probable meaning of the evaluated information. Production is the conversion of evaluated material or information into intelligence. All sources of information are integrated, analyzed, evaluated, and interpreted to prepare intelligence products or all-source intelligence in support of known or anticipated user requirements. Production or the process of analysis and synthesis is the most important action in developing usable intelligence for the commander. Production, the fourth step in the intelligence cycle, helps forecast the effect gathered intelligence will have on the commander's ability to accomplish the mission.

Intelligence Functions

To support the commander, MAGTF intelligence organizations carry out six intelligence functions of which the P&A function is an integral part. In each function, data is synthesized into intelligence that provides a portion of the knowledge from which the commander can reach an acceptable level of understanding before making a decision. Intelligence answers the all-important question: "What effect does all this have on our ability to accomplish the mission?" Intelligence organizations—

- Support the commander's estimate.
- Develop the situation.
- Provide indications and warning.
- Support force protection.
- Support targeting.
- Support combat assessment.

Intelligence Cycle

The intelligence cycle consists of a series of related activities that translate the need for intelligence about a particular aspect of the battlespace or threat into a knowledge-based product that is provided to the commander for use in the decision-making cycle (see fig. 1-1).

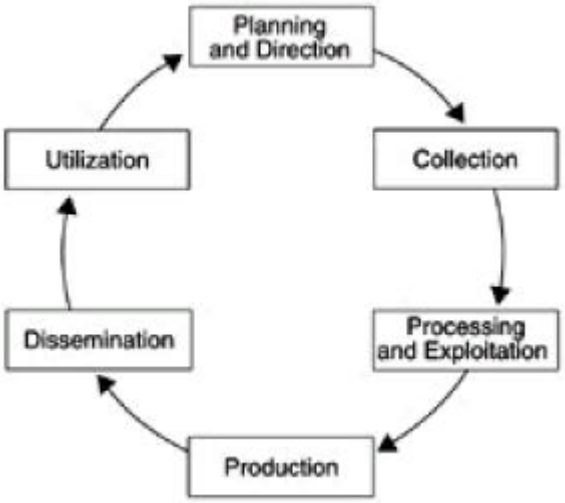


Figure 1-1. Intelligence Cycle.

Planning and Direction

The initial step identifies intelligence needs and develops a plan for satisfying those needs.

Collection

In this step, information used to generate intelligence is drawn from—

- **Intelligence data that is derived from assets primarily dedicated to intelligence collection (e.g., imagery systems, electronic intercept equipment, human intelligence sources).**
- **Sensor data that is derived from sensors whose primary mission is surveillance or target acquisition, air surveillance radar, counterbattery radar, and remote ground sensors.**
- **Combat data that is derived from reporting by operational units.**

Processing and Exploitation

This step converts collected information into an understandable form suitable for the production of intelligence. Processing is accomplished during collection or production. Data collected in a form suitable for analysis is processed automatically during collection. Other types of data require extensive processing, which can affect the timeliness and accuracy of the resulting information. Because processing and production are often accomplished by the same organization, production management generally encompasses processing functions that are required to convert raw data into a usable format. Examples of processing and exploitation include—

- **Film processing.**
- **Document translation.**
- **Signals intercept.**

Production

Production, the fourth step, converts data into intelligence and creates the knowledge (see fig. 1-2) needed for the planning and execution of operations. The intelligence must deliver knowledge, in

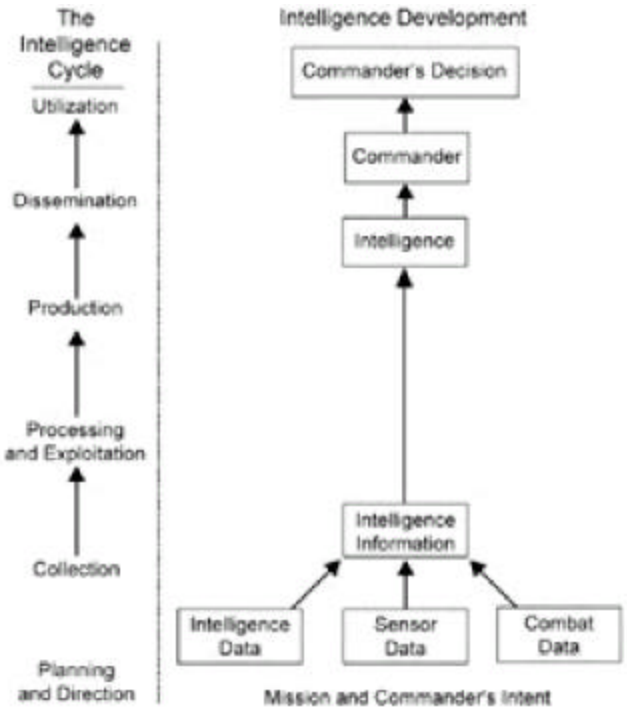


Figure 1-2. Intelligence Cycle in Support of Commander's Decision.

context, in time, and in a form usable in the decisionmaking process. In any situation, providing timely, accurate, and relevant intelligence to commanders and planners is a critical consideration. Production (analysis and synthesis) can be complex, such as comprehensive and detailed intelligence studies required to support the planning of a Marine expeditionary force (MEF) in a major theater war (MTW), or simple, such as direct answers to rapidly changing questions needed to support the ongoing battle at the battalion level. For this reason, production is distinguished as—

- **Deliberate production makes full use of available information to provide a complete and extensive product that satisfies non-time sensitive intelligence requirements (IRs). This type of production normally supports operations planning.**
- **Immediate production identifies information directly applicable to current operations, the information is subjected to a compressed ver-**

sion of the production process, and the resulting product is rapidly disseminated to those affected. This production is associated with mission execution.

Dissemination

This step conveys intelligence to users.

Utilization

During utilization, the processed intelligence is used to influence the conduct of operations.

Production Steps

Production (analysis and synthesis) encompasses the following steps, which begin with the receipt of processed information and end with the completion of an intelligence product that is ready for dissemination:

- Filtering is the discarding of irrelevant or repetitive information prior to its entering the production process.
- Recording is the reduction of information to writing or graphical representation and then the arranging of that information into groups of related items.
- Evaluating is the determining of the pertinence, reliability, and accuracy of information.
- Analyzing is the process in which information is analyzed and synthesized to predict possible outcomes.
- Product preparation is the incorporating of developed intelligence into an appropriate product (e.g., text reports and studies, graphics, overlays, or combinations) for dissemination.

Preparation for Analysis

The first three production steps are tools used to prepare information for analysis. The objective is to discard information not pertinent to the situation, organize and document the information in a manner that facilitates analysis, and assess the quality of the individual elements of information to determine the reliability and importance of each report or piece of information.

In deliberate production, comprehensive procedures are often employed to accomplish filtering, recording, and evaluating. The complexity of these procedures increases with the level of command, scope of the operation, and number of agencies or elements participating in the production process. However, it is important to note that filtering, recording, or evaluation systems are tools to support the analytical effort, not an end unto themselves. Intelligence personnel must be thoroughly familiar with the methodology being employed in preparing information for analysis to ensure that the pertinent information is available to the right analyst when needed.

In immediate production, a central node or individual, normally the intelligence watch in the combat operations center, makes a rapid assessment of each piece of incoming information to determine its pertinence and to evaluate its reliability and accuracy. The intelligence watch personnel's evaluation is based on their knowledge and understanding of the enemy situation, the current intelligence estimate, and ongoing and planned friendly operations and IRs. The watch performs the minimal collating and recording necessary so that an immediate tactical analysis may be completed and judgments made. Simultaneous with or upon completion of immediate production, the information is entered into the formal recording and evaluation system for further use in deliberate production. At lower tactical echelons, the entire process, from receipt of information to dissemination and utilization, can take a matter of seconds or minutes. Organization, established standing operating procedures, and individual and unit training are key components of effective preparation for, and conduct of, P&A.

Analytical Process

Intelligence analysis provides the commander with the battlespace and threat knowledge required for planning and executing combat operations. Intelligence analysts lessen the uncertainty facing a commander, permitting the commander to make decisions and to focus combat power on courses of action (COAs) that maximize the opportunity for success. The analysis framework used by intelligence analysts is described as analysis, synthesis, and estimation. This framework provides a disciplined approach to gathering and understanding information and a means for the analyst to place information in context and relate it to planned or ongoing operations.

Analysis

Effective analysis requires that intelligence analysts—

- **Possess a thorough knowledge of—**
  - **Military operations.**
  - **Characteristics of the battlespace.**
  - **Friendly situation and IRs.**
  - **Threat situation (current situation, doctrine, and past practices).**
- **View collected information in relation to the—**
  - **Unit's mission.**
  - **Commander's intent.**
  - **Commander's IRs.**
- **Divide the battlespace into component parts to isolate and define the individual elements of significant information that include—**
  - **Physical dimensions (i.e., length, depth, width, and altitude).**
  - **Time.**
  - **Threat force structure (e.g., divisions, wings, groups, task forces).**
  - **Battlespace activities (e.g., command and control [C2], air and space defense, fire support).**
  - **Other characteristics that facilitate understanding and satisfy the MAGTF's needs.**
- **Identify key elements of the situation to—**
  - **Formulate hypotheses.**
  - **Make deductions from those hypotheses.**
  - **Reach conclusions.**
- **Compare the existing situation to new pieces of information to determine if they relate to the identified key elements and to assess the impact of the new information on the current intelligence estimate.**

Synthesis

In this step, intelligence analysts—

- **Identify and integrate relationships between individual significant pieces of information with the existing battlespace picture to provide a new image of the situation.**
- **View the battlespace as a coherent whole.**
- **Discern emerging patterns in environmental conditions or enemy activity.**

Estimation

The bottom line of the analytical process, estimation is based on the detailed study of the tactical situation, experience, intelligence successes, the application of specific tools and methods, and the supported commander's intelligence needs. Estimation is not guessing and it is not predicting! Estimation must describe the current conditions and present an image of future possibilities. Well-founded estimates reduce uncertainty and help the commander plan and execute successful MAGTF operations. Building on the image developed during analysis and synthesis, intelligence analysts determine a threat's—

- **Capabilities.**
- **Intent.**
- **Probable COA.**
- **Likely reactions to friendly operations.**

Product Preparation

Products are prepared by translating the results of analysis into usable intelligence formats that are timely, accurate, and tailored to both the unit and its mission. Intelligence analysts must strive to provide knowledge that the decisionmaker can easily and quickly visualize and absorb. A series of standard intelligence products are used to support MAGTF operations. Standard production formats facilitate rapid preparation, mutual support between intelligence sections, ease of dissemination, and, most importantly, familiarity for the user. The baseline production formats provided in this manual can be tailored to meet the requirements of any operational situation. The following standard all-source intelligence products are prepared in MAGTF:

- Intelligence preparation of the battlespace (IPB) graphics, matrices, and charts.
- MAGTF contingency intelligence studies.
- Intelligence estimates.
- Target or objective studies.
- Intelligence summaries.
- Intelligence reports.

Operations and Command and Control

Intelligence drives the planning and execution of operations by providing a menu of factors that the commander considers when making a decision. The analytical and production effort identifies these factors and presents them to decisionmakers in a form that enables them to understand the battlespace, place intelligence in context, and use the product to carry out successful operations. P&A shapes operations by—

- Identifying potential advantages offered by the environment.
- Defining the limitations imposed by the environment.
- Locating and assessing enemy strengths to be avoided.
- Determining enemy vulnerabilities to be exploited.
- Providing an estimate of likely enemy actions and reactions based on reasoned analysis, synthesis, and judgment.

Intelligence and operations must be linked throughout the planning, decision, execution, and assessment (PDE&A) cycle at all command echelons. The PDE&A cycle provides the framework for the implementation of C2, which enhances the commander's ability to make sound and timely decisions. Whether the commander uses the analytical or intuitive decisionmaking approach, intelligence P&A reduces uncertainty.

Deliberate intelligence production shapes the operations plan and provides the knowledge that facilitates execution (see fig. 1-3 on page 1-6). Immediate intelligence production identifies situation changes that modify the plan or trigger decisions during execution of the operation. Intelligence production provides the basis for assessing the effectiveness of current operations, while operations drive the P&A effort. The mission and commander's intent focus the initial IPB, while the potential COAs, the concept of operations, the future planning effort, and IRs determine the scope and content of the production process. Intelligence products must be relevant to the mission and be used to satisfy specific operational and tactical IRs.

Production and Analysis Company, Intelligence Battalion

The P&A company is the MEF's primary all-source P&A element. An organic unit within the intelligence battalion (intel bn), P&A company is composed of an imagery intelligence platoon, a topographic platoon, an all-source fusion platoon, and two direct support teams. The P&A company is in general support of the MAGTF and provides direct support teams to MAGTF

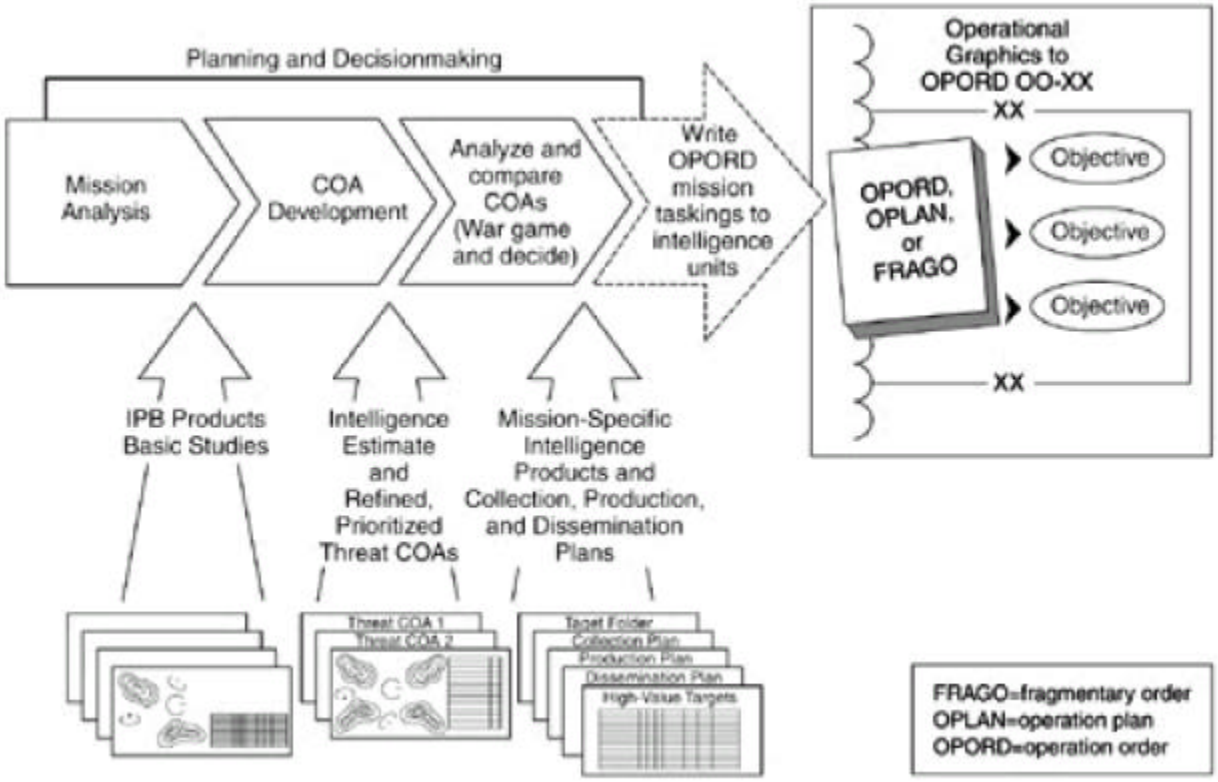


Figure 1-3. Intelligence Support to Planning and Decisionmaking.

subordinate elements, as required. The P&A company performs the following tasks:

- Assists the intel bn commander with planning, developing, and directing the MAGTF intelligence production plan and its integration with the collection and dissemination plans.
- Provides and maintains centralized all-source P&A in support of the MAGTF within the MAGTF P&A cell.
- Maintains an all-source picture of MAGTF AO and area of interest (AOI) threat situation.
- Provides MAGTFs and other commands with geographic intelligence (GEOINT) and geospatial information and services.
- Provides command and control of the topographic platoon.
- Provides imagery analysis and imagery intelligence (IMINT) production support for MAGTFs and other commands.
- Provides command and control of the imagery intelligence platoon.
- Provides task-organized, trained, and equipped detachments or teams to assist MAGTFs or designated commands in the processing, exploitation, evaluation, integration, analysis, interpretation, production, and dissemination of all-source intelligence.

Although the P&A company is a subordinate element of the MEF intel bn and the MAGTF's only dedicated production element, the company responds to the IRs of the entire force. The MAGTF G-2, through the intel bn commander in the role as intelligence support coordinator, establishes the P&A company's analytical and production priorities based on the MAGTF's mission, commander's intent, priority intelligence requirements (PIRs), the current and projected enemy situation, and ongoing planning for future operations. The P&A company focuses primarily on deliberate

production. In garrison or a pre-crisis environment, the P&A company conducts mainly IPB of potential contingency areas to produce MAGTF contingency intelligence studies. During operations and exercises, the P&A company develops intelligence to support future operations, deliberate targeting, and development of the key target or objective area studies. A detailed discussion of the P&A company organization, functions, and employment is provided in chapter 2.

CHAPTER 2. ORGANIZATIONS AND RESPONSIBILITIES

Marine Corps operational forces are organized for combat as MAGTFs. Marine intelligence P&A operations are conducted primarily to facilitate planning and execution of MAGTF operations through the development of tactical intelligence. This chapter discusses responsible officers, organization, supporting organizations, and communications and information systems (CIS) architecture necessary to conduct MAGTF intelligence P&A.

MAGTF Commander

Intelligence is an inherent responsibility of command, and commanders must—

- **Be personally involved in the conduct of intelligence activities.**
- **Specify intelligence requirements and establish PIRs.**
- **Provide guidance to ensure a timely and useful product.**
- **Develop an appreciation for the capabilities and limitations of intelligence.**
- **Make the final synthesis of intelligence.**
- **Supervise the overall intelligence effort to ensure the product is timely, relevant, and useful.**
- **Ensure intelligence activities support subordinate commanders as well as the parent unit.**
- **View intelligence training of all personnel as a command responsibility.**

To ensure the timely development of useful intelligence products, the commander has specific P&A responsibilities.

Focus the Analytical and Production Effort

The commander must—

- **Provide guidance and direction to ensure that the intelligence developed satisfies requirements.**
- **Issue a statement of intent and approval of the command's priority intelligence requirements, focusing the analytical and production effort.**
- **Supervise the process to ensure that it is responding to the intent and intelligence needs.**
- **Provide direction in the scope of the IPB effort, preferred product formats, and priorities among subordinates' production requirements (PRs).**

Participate in the Analytical Process

The commander must understand and participate in the analytical process. Since intelligence analysis is based on incomplete information and involves assumptions and judgments, the commander must scrutinize the process by analyzing intelligence operations and resulting products to determine the operational impact and overall effectiveness.

Evaluate the Product

To provide the basis for continued improvement of the P&A effort, the commander must—

- **Evaluate key areas (e.g., product content, presentation, timeliness).**
- **Identify where the intelligence provided met expectations and where and how it fell short.**

- Provide timely and constructive feedback to the intelligence officer, the supporting intel bn commander or detachment officer in charge, and P&A elements.

Marine Expeditionary Force Command Element Intelligence Officer

The MEF assistant chief of staff (AC/S) G-2 focuses on overall C2 and direction of MEF intelligence, counterintelligence (CI), and reconnaissance operations, to include P&A. The MAGTF commander relies on the AC/S G-2 to provide the necessary information on the weather, terrain, and enemy capabilities, status, and intentions. Through intelligence operation plans (OPLANs) and supporting intelligence and reconnaissance and surveillance plans, the AC/S G-2—

- Plans and coordinates intelligence priorities.
- Integrates collection, production, and dissemination.
- Allocates resources.
- Assigns specific missions to subordinate elements.
- Supervises the overall intelligence and reconnaissance efforts.

Intelligence Battalion Commander

The intel bn commander is responsible for planning and directing, collecting, processing, producing, and disseminating intelligence, and providing CI support to the MEF and MEF major subordinate commands (MSCs).

Responsibilities in Garrison

In garrison, the principal task of the intel bn commander is to organize, train, and equip detachments that support MAGTFs or other designated commands to execute integrated collection, intelligence analysis, production, and product dissemination.

Responsibilities During Operations

During operations the intel bn commander is dual-hatted as the intelligence support coordinator (ISC), serving under the direct staff cognizance of the MEF AC/S G-2. The intel bn S-3 section and the MEF G-2 operations center element form the core of the ISC support effort and conduct planning, directing, and C2 within the intelligence operations center (IOC) support cell. Generally, the IOC is collocated with the main command post of the MEF command element (CE). As ISC, the intel bn commander is responsible to the MEF AC/S G-2 for the overall MEF IR management. During operations, the ISC is responsible for—

- Implementing the concept of intelligence operations developed by the G-2 plans officer and approved by the AC/S G-2.
- Establishing and supervising the MEF IOC, which includes P&A cell, surveillance and reconnaissance cell (SARC), and support cell.
- Developing, consolidating, validating, and prioritizing recommended PIRs and IRs to support MAGTF planning and operations.
- Planning, developing, integrating, and coordinating MEF intelligence collection, production, and dissemination plans.
- Exercising C2 staff cognizance of supporting intelligence and reconnaissance organizations to ensure unity of effort and production of all-source intelligence.
- Developing, in conjunction with the G-2 plans officer and G-2 operations officer, and completing Annex B (Intelligence) to MEF operation order (OPORD), supporting appendices, and intelligence input to other OPORD annexes.
- Providing intelligence support to MEF CE G-2 section and MSCs.

- **Preparing the intelligence and CI estimates to support G-2 plans.**
- **Planning, developing, integrating, and coordinating intelligence and CI support to the commander's estimate, situation development, indications and warning, force protection, targeting, and combat assessment.**

Intelligence Battalion

Within the MEF, the intel bn is organized to conduct intelligence operations for the MEF, MEF MSCs, subordinate MAGTFs, and other commands as directed (see fig. 2-1).

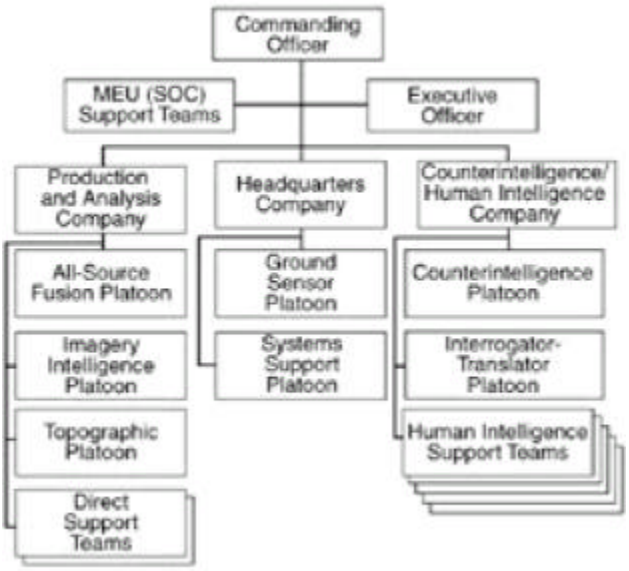


Figure 2-1. Intelligence Battalion Organization.

Production and Analysis Company

The P&A company, intel bn, is the focal point for deliberate intelligence production within the MEF. Although all P&A company elements contribute to the deliberate production process, the focal point for all-source analysis, order of battle (OOB), target intelligence, battle damage assessment (BDA), and deliberate production is the all-source fusion platoon (AFP).

All-Source Fusion Platoon

The AFP, in conjunction with other elements of the intel bn and production elements of radio battalion, force reconnaissance company, Marine tactical electronic warfare squadron (VMAQ), and Marine unmanned aerial vehicle squadron (VMU), provide the capability for all-source intelligence P&A support to the full range of operations conducted by the MEF and other MAGTFs. During operations, AFP forms the core of P&A cell.

Organization for Support

Intel bn's P&A company is organized to provide intelligence support to elements of the MEF CE and MSCs. During operations, P&A company is functionally organized into teams as the P&A cell. The teams support other MAGTF staff organization cells (see table 2-1).

Table 2-1. P&A Company Organization for Support.

Intel Bn, P&A Company Team or Unit	MEF CE Supported Cell
All-source fusion platoon	
• Analysis team	G-3 current and future operations, G-5, and other MEF staff elements*
• OOB team	G-3 current and future operations, G-5, and other MEF staff elements*
• Target analysis and BDA team	G-3 targeting cell and other MEF staff elements*
• IPB team	G-3 current and future operations, G-5, and other MEF staff elements*
Topographic platoon	MEF
Imagery intelligence platoon	MEF
Direct support teams	P&A cell, G-3 current or future operations, G-5, or designated MSC G-2
*The P&A cell supports the G-4, G-1, and other MEF CE staff elements, as appropriate.	

Production and Analysis Cell

The mission of P&A cell is to plan, coordinate, and produce fused all-source tactical intelligence in support of the MEF, its MSCs, and other MAGTFs and commands as directed. A multi-disciplined group of intelligence officers and specialists, the P&A cell provides the intelligence necessary to support contingency planning and current intelligence threat requirements of the MEF, its subordinate MAGTFs, and other commanders as directed.

Tasks

During operations and exercises, the P&A cell provides the intelligence necessary to support current and future operations, future plans, targeting, and development of enemy situation and capabilities. It is responsible for processing information and intelligence from organic and external commands and intelligence organizations. The P&A cell personnel—

- Receive, process and exploit, integrate, analyze, evaluate, interpret, and synthesize intelligence and other information into comprehensive and tailored intelligence products required for the planning and execution of MAGTF operations.
- Provide intelligence support across the conflict spectrum and in support of deliberate and crisis planning, MAGTF deployments, and other operations as directed.
- Provide a dynamic, detailed OOB picture of threats within the MAGTF AO and AOI.
- Provide detailed intelligence P&A support to targeting.
- Maintain a MAGTF-wide summation of damages caused to hostile targets and augment BDA efforts of MAGTF elements as required.
- Provide MAGTF-level BDAs for forwarding to the component, joint task force (JTF), and/or theater commander in chief (CINC) as applicable.
- Provide IPB support to the MAGTF G-3/S-3 and G-5 for battle management and planning efforts and provide IPB-related support to MAGTF elements beyond their organic capabilities.
- Disseminate intelligence products and information to the MAGTF staff and MSCs in a timely, relevant manner.
- Establish and maintain intelligence data bases to support intelligence P&A.
- Coordinate with the collection management and dissemination officer to provide the SARC with collection requirements for MAGTF and external collection units.
- Coordinate with the dissemination manager to disseminate intelligence products throughout the MEF and external organizations.
- Coordinate with the MEF G-2 and intel bn commander/ISC to—
  - Ensure disseminated intelligence and products are understood.
  - Determine whether intelligence products answer commander's PIRs and users' IRs.
  - Identify new intelligence production requirements (IPRs) that result from disseminated intelligence products.
  - Assess the overall effectiveness of intelligence production operations.

Organization

The P&A cell is essentially organized in garrison as it would be organized for operations. Each team has the flexibility to add intelligence and nonintelligence specialists (e.g., G-2 operations red cell members) from other intelligence and reconnaissance organizations as required based on the specific mission and intelligence needs of the MAGTF. For sustained MEF-level operations, global sourcing from other Marine Corps organizations may be required to augment the P&A team structure and to provide sufficient personnel depth for 24-hour operations.

The following P&A cell internal organization and subordinate teams and units provide the P&A functions required to support current and future operations, future planning, targeting, and BDA.

P&A Cell Staff

Members of the staff provide leadership and support functions such as maintenance of the intelligence library. In conjunction with the intel bn's collection management and dissemination officer, P&A cell staff members are responsible for production and IPR management as well as coordination of IPRs with intel bn's overall IR collection and dissemination.

Analysis Teams

The two analysis teams are composed of all-source analysts and specialists from other disciplines (e.g., medical, weather, CI/human intelligence [HUMINT], imagery, terrain, signals intelligence [SIGINT]). With support from other elements of the P&A company, the rest of intel bn, radio battalion, force reconnaissance, VMU, VMAQ, and MSC G-2 intelligence analysts, P&A cell analysis teams produce integrated all-source intelligence products to include—

- **Contingency and other focused intelligence studies.**
- **Intelligence estimates.**
- **Intelligence summaries.**
- **Briefings.**

OOB Teams

The P&A cell has two OOB teams. These teams analyze and maintain a detailed, comprehensive, evolving picture of ground, air, naval, electronic, weapons of mass destruction, and other threats within the MAGTF AO and AOI. The OOB teams perform OOB analysis, and the primary products include—

- **Graphic or electronic situation overlays.**
- **OOB data bases and files.**
- **Threat models for various threat elements.**

Target Analysis and BDA Teams

The two target analysis and BDA teams focus on detailed analysis of MAGTF commander, staff, and MSC-identified targets not destined for the air tasking order (ATO). (The Marine aircraft wing [MAW] G-2 section generally manages target and BDA analysis and intelligence support for ATO-nominated targets.) These teams—

- **Provide target development and analysis to support the MAGTF deliberate and reactive targeting efforts.**
- **Maintain the comprehensive picture of battle damages caused to targets.**
- **Prepare BDA reports and assessments, which support the MEF combat assessment effort.**

IPB Teams

The two IPB teams focus on IPB production support to the MEF G-3 and G-5 in the areas of current battle management and future planning. They also assist subordinate unit intelligence personnel with IPB-related production when requirements are beyond the organic capabilities of that unit.

Direct Support Teams

The two P&A cell direct support teams allow enhanced IR management, intelligence P&A, and dissemination capabilities to be focused down to one or more MSCs. Direct support teams augment the supported unit's intelligence section by—

- **Providing an extension of the intel bn's P&A cell or MSC G-2 intelligence operations element for the receipt, collaborative analysis, production, and dissemination of intelligence to the supported unit.**
- **Tailoring higher and external intelligence products to the needs of the supported unit.**

- Assisting the supported unit's intelligence officer in the formulation and management of external IRs.
- Assisting the supported unit in the production of IPB and other intelligence products to support detailed mission planning and execution.
- Enhancing the intelligence dissemination efforts of the supported unit's intelligence section.

Supporting Organizations

Several organic MAGTF intelligence organizations support the P&A cell P&A effort by contributing specialized MAGTF intelligence expertise and resources. The intel bn commander, serving as the ISC, is directly responsible to MEF AC/S G-2 for exercising C2 staff cognizance of supporting intelligence and reconnaissance organizations to ensure unity of effort and production of all-source intelligence. These supporting organizations contribute to fused, all-source MAGTF intelligence products. The following supporting intelligence and reconnaissance organizations provide significant specialized support to the P&A cell P&A effort.

Imagery Intelligence Platoon

Organized under the intel bn, P&A company, imagery intelligence platoon (IIP) provides imagery interpretation support for MEF requirements and maintains the imagery data base and imagery library for the MAGTF (see fig. 2-2). The IIP is capable of providing IMINT derived from available imagery sources in support of MEF P&A cell products. This includes annotated imagery in support of MEF P&A cell production or in response to separate IRs. A key imagery exploitation resource organic to the IIP is the tactical exploitation group (TEG), which is an element of the broader Joint Services Imagery Processing System (JSIPS). The IIP normally concentrates on the exploitation of imagery and production of IMINT from MEF, JTF, and other tactical resources, such as unmanned aerial vehicles (UAVs) or the F/A-18D (RC) advanced tactical aerial reconnaissance system (ATARS).

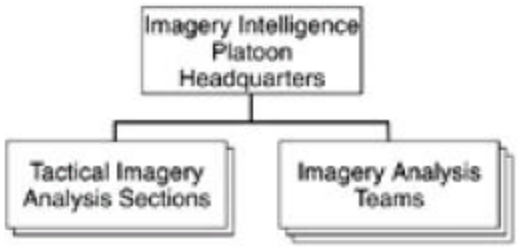


Figure 2-2. IIP Organization.

Topographic Platoon

Organized under the intel bn, P&A company, the topographic platoon provides geospatial information and GEOINT support for all MAGTF requirements (see fig. 2-3). The topographic platoon and IIP work closely as both use many of the same baseline intelligence data and sources for production.

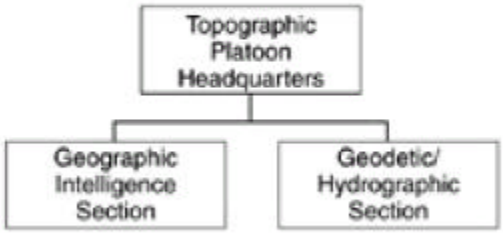


Figure 2-3. Topographic Platoon Organization.

The topographic platoon personnel—

- Integrate, deconflict, analyze, and disseminate theater, Service, and national geospatial data bases for the MAGTF.
- Provide GEOINT and specialized mapping, graphics and other geospatial information and services, and GEOINT products in support of P&A cell all-source intelligence products.
- Provide key support to the IPB process.

- **Produce independent GEOINT studies in response to separate requirements.**

CI/HUMINT Company

Organized under the intel bn, the CI/HUMINT company is responsible for the development and maintenance of the MEF CI estimate and reporting information (see fig. 2-4). The CI/HUMINT company produces—

- **Intelligence derived from human source exploitation, to include—**
  - **Interrogations of enemy prisoners of war, refugees, and displaced persons.**
  - **Counterintelligence operations.**
  - **Human source operations.**
- **Intelligence derived from exploitation of captured documents or materiel.**
- **Specialized CI or force protection assessments in support of P&A cell production or in response to specific IPRs.**

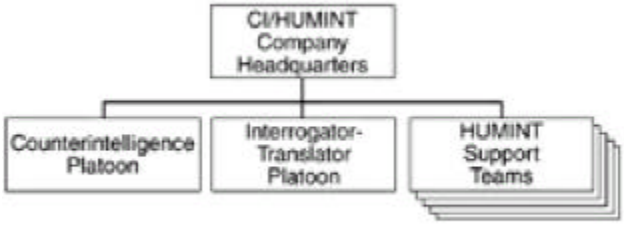


Figure 2-4. CI/HUMINT Company Organization.

Radio Battalion Operational Control and Analysis Center

The radio battalion operational control and analysis center (OCAC) provides the principal MEF SIGINT analytical and production support to MEF IRs. Under staff cognizance of the ISC, the radio battalion is tasked with the responsibility of maintaining the MAGTF electronic OOB and SIGINT data bases and of providing SIGINT analytical and production support to the P&A cell. The OCAC provides MAGTF units with time-sensitive SIGINT and product reporting based on intelligence reporting criteria and the MAGTF intelligence dissemination plan.

VMAQ

In conjunction with the MAW G-2, VMAQ is responsible for the processing, analysis, and production of routine and time-sensitive electronic intelligence reports resulting from EA-6B operations. The resulting information and intelligence is used to help update and maintain the threat electronic OOB, which is used in the planning and execution of aviation and other MAGTF operations. A threat's electronic OOB and the location of electronic emitters in the battlespace are important indicators of threat dispositions, capabilities, and intentions.

Force Reconnaissance Company

The mission of the force reconnaissance company is to conduct amphibious reconnaissance, surveillance, and limited-scale raids in support of the MEF, other MAGTFs, or JTFs as directed.

Under the staff cognizance of the ISC, force reconnaissance company conducts specialized terrain reconnaissance and prepares intelligence products to support hydrographic, beach, road, bridge, route, urban area, helicopter landing zones (HLZs), drop zones (DZs), landing craft air cushion (LCAC) landing zones (LZs), and aircraft forward operating site intelligence studies.

Principal Staff Officers

Like the commander, the other principal staff officers play an important role in intelligence P&A. Through development of focused intelligence requirements, and recommending which should be priority intelligence requirements PIRs, they assist in directing the intelligence P&A effort. They also assist the analytical effort by availing the wide range of skills and backgrounds resident within their staff sections to the intelligence section. A tremendous synergism is achieved when

task-organized teams of intelligence analysts and other occupational specialists form to analyze a specific issue. Likewise, a key component to effective wargaming is a red cell, which has experts in various warfighting functions thinking and fighting like the threat. Principal staff officers must—

- Use the intelligence products.
- Evaluate the worth and effectiveness of those products.
- Provide constructive feedback.
- Develop IRs and recommend their priority.

Unit Intelligence Officer

The intelligence officer manages the intelligence effort for the commander by implementing activities that execute the intelligence P&A function for the command. Understanding the scope and rationale behind the commander's decisionmaking process enables the intelligence officer to anticipate future requirements and properly focus the P&A effort. To execute P&A responsibilities, the intelligence officer must—

- Integrate and focus all-source intelligence on the commander's and sub-ordinate commanders' PIRs to support estimates of the situation, situation development, COA development, planning, and decisionmaking.
- Supervise the development and dissemination of all-source intelligence products that are tailored to the units' needs and concepts of operations and that are provided in time to support planning and decisionmaking.
- Provide the commander and staff with a bottom-line analysis of enemy capabilities, strengths, and vulnerabilities as well as opportunities and limitations presented by the environment.
- Request P&A support for requirements that exceed organic capabilities.
- Ensure the nature of the analytical effort and the content of the intelligence product is understood and properly used in the planning and execution of combat operations.

Organic Intelligence Sections

The unit intelligence section supports the commander, the intelligence officer, and the command through the development of mission-oriented intelligence products. The analytical and production capabilities of organic intelligence sections vary with the size of the section and level or type of command it supports. However, intelligence sections and their supporting intel bn or detachment are capable of performing the following P&A tasks:

- Conducting mission-focused IPB P&A for the unit's AO and AOI.
- Developing and maintaining a comprehensive intelligence estimate.
- Tailoring intelligence products to meet unit requirements.
- Maintaining an accurate all-source picture of the enemy situation in the AO and AOI.
- Preparing target analysis and target intelligence products.
- Providing intelligence operational linkage and communications and information system connectivity with higher, adjacent, supporting, and subordinate analytical elements.

Organization for Employment

When deployed, the P&A cell functions as part of the MEF CE combat intelligence center (CIC), IOC, under C2 of the ISC.

Combat Intelligence Center

The MEF CE CIC is the overarching IOC, which is established within the MEF main command post to conduct the primary functions of MEF intelligence section and intel bn. Key CIC elements (see table 2-2) are designed to

provide tailored, yet flexible, intelligence C2 and functional capabilities to meet MEF and subordinate commander's IRs and supporting intelligence and reconnaissance operations.

Command and Control

The MEF AC/S G-2 focuses on overall C2 and direction of MEF intelligence, CI, and reconnaissance operations by exercising staff cognizance over intel bn, radio battalion, force reconnaissance company, and other MEF intelligence and reconnaissance assets (e.g., UAV squadron). Within this C2 authority, the intel bn commander, serving as the G-2's ISC, performs MEF-wide IR management; develops, integrates, and manages supporting intelligence plans; and supervises plan execution.

These plans encompass the MEF-wide organic efforts for collection, processing, production, and dissemination activities of intelligence and reconnaissance operations. The intel bn commander/ISC is responsible for the establishment and operation of the IOC (see fig. 2-5 on page 2-10).

Table 2-2. MEF CE's CIC Key Elements.

Element	Responsibilities
G-2 Plans	Serves as the G-2 section's main element for coordinating and providing intelligence support to the MEF CE future plans team and leadership and direction of the G-2 section's imagery and mapping, SIGINT, and weather sections.
G-2 Operations	Serves as the G-2 section's main element for coordinating and providing intelligence support to the MEF CE commanding general (CG), battle staff, and current operations center elements; target intelligence support to the force fires and future operations; G-2 section intelligence requirements management activities; red cell support; and MEF intelligence liaison with external commands and organizations.
IOC	Serves as the principal MEF intelligence operations and C2 center that is established by intel bn; performs intelligence requirements management, staff cognizance of ongoing organic and supporting collection operations, intelligence P&A, and intelligence dissemination.
• Support Cell	Serves as primary element for conducting MEF-wide intelligence requirements management, weather support, collections and dissemination planning and direction, and intelligence staff cognizance of MEF organic and supporting intelligence and reconnaissance operations.
• P&A Cell	Serves as the primary P&A element of the MEF; processes and produces all-source intelligence products in response to requirements of the MEF; serves as the principal IMINT and GEOINT production element of the MEF.
• SARC	Serves as the primary element for the supervision of MEF collection operations; directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets.
CI/HUMINT Company Command Post	Serves as the primary element for conducting CI/HUMINT planning and direction, C2, and coordination of MEF CI/HUMINT operations with external CI/HUMINT organizations.
OCAC	Serves as the main node for the C2 of radio battalion SIGINT operations and the overall coordination of MEF SIGINT operations; processes, analyzes, produces, and disseminates SIGINT-derived information; and directs the ground-based electronic warfare activities of the radio battalion.
Reconnaissance Operations Center	Serves as the main node for the C2 of force reconnaissance company's operations and the overall coordination of MEF ground reconnaissance operations; processes, analyzes, produces, and disseminates ground reconnaissance-derived information in support of MEF intelligence requirements.

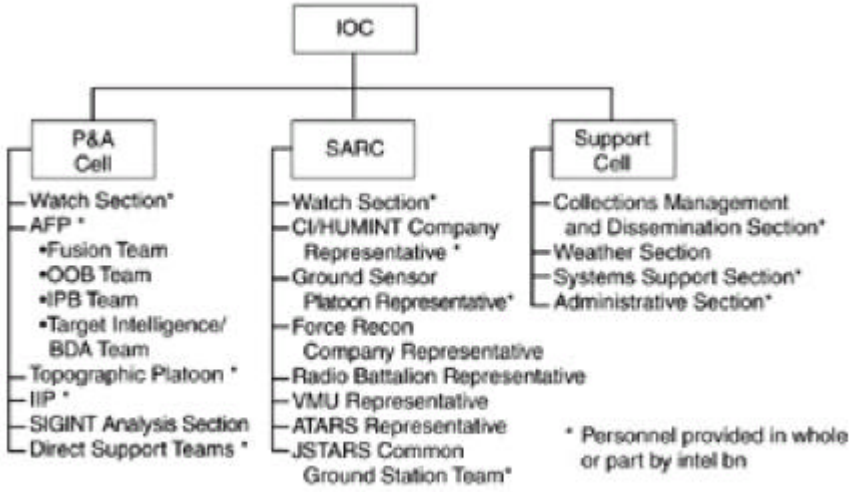


Figure 2-5. IOC Organization.

Senior Marine Expeditionary Force Intelligence Staff Officers

Table 2-3 highlights the key MEF senior intelligence staff officers and their responsibilities, roles, and tasks.

Intelligence Production Support Flow

Requests for intelligence production support from the P&A cell, or other MEF intelligence or reconnaissance elements, must be validated and forwarded via the chain of command to the MEF G-2 for validation, prioritization, and tasking. The intel bn commander, serving as ISC, performs this function for the G-2.

The ISC, upon approval by the AC/S G-2, uses the prioritized intelligence collection requirements (ICRs), IPRs, and intelligence dissemination requirements (IDRs) for planning and direction, follow-on taskings to MEF organic and supporting intelligence and reconnaissance units, C2, and execution. The ISC's overall intelligence production staff cognizance relationships and resulting P&A cell intelligence production support flow are as indicated in figure 2-6.

Organization for Combat Operations

The intel bn and P&A company tailor day-to-day garrison operations to support the IRs of the commander, staff, and MEF subordinate units. With minor adjustments, the P&A company transitions from garrison pre-hostilities organization to P&A cell crisis or combat operations functioning. In practice, the organization of the P&A cell supporting each MEF is based on prospective missions of that MEF and corresponding potential AOs.

During contingency or combat operations, the P&A cell functions as part of the MEF CE's CIC and the intel bn's IOC. The P&A cell may be tasked to provide limited personnel support to an intelligence node or cell with the MEF. In such cases, the intelligence component of these command echelons will contain a limited P&A capability (focused on providing the commander with situational awareness).

Table 2-3. Senior Intelligence Staff Officers.

ISC	G-2 Operations Officer	G-2 Plans Officer
Planning and execution of intelligence operations to support all MEF IRs.	Providing intelligence support to MEF CE battle staff and current operations center agencies.	Providing intelligence support to the plans officer's future planning team for future planning IRs.
Establishing and directing the IOC (P&A cell, SARC, and support cell).	Coordinating intelligence support to higher and adjacent headquarters and agencies.	Recommending IR validation, prioritization, and tasking to AC/S G-2.
Managing IRs (collection, production, and dissemination), validating, prioritizing, and tasking IRs, per AC/S G-2 direction.	Recommending IR validation, prioritization, and tasking to AC/S G-2.	Establishing and directing the G-2 future planning intelligence element.
Exercising C2 of intel bn and staff cognizance over SIGINT, CI, HUMINT, measurement and signature intelligence, IMINT, and air and ground reconnaissance, including staff cognizance of designated G-2 elements.	Establishing and directing intelligence elements and support to the combat operations center, future operations center, target intelligence section, force fires, red cell, and MEF intelligence liaison teams.	Establishing and operating the intelligence section's imagery and mapping, CI, HUMINT, SIGINT, and weather sections (less that under staff cognizance of the ISC).

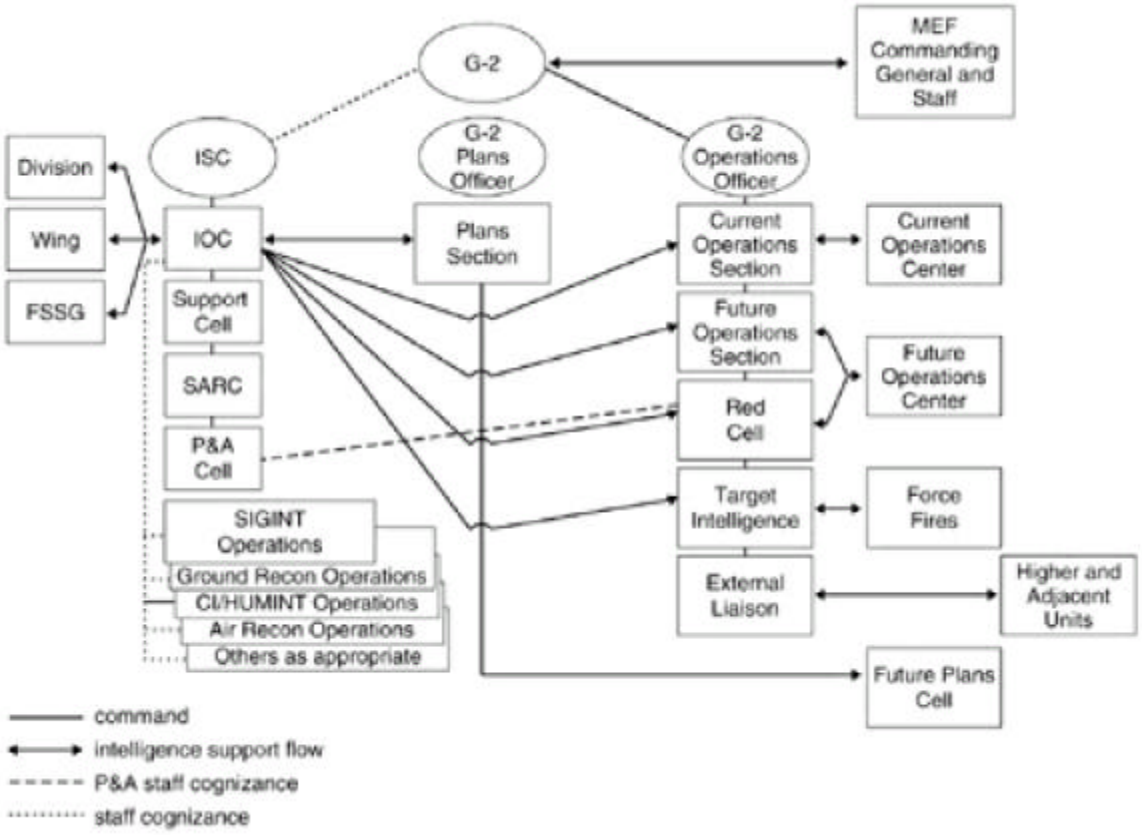


Figure 2-6. C2 and Staff Cognizance of Intelligence Production Support Flow.

The P&A cell may be tasked to provide personnel to support intel bn detachments provided to subordinate commands, MAGTFs, or separate units. Each P&A cell contains within its table of organization (T/O) two direct support teams which can be used to augment the IR management, analysis, production, and dissemination capabilities of the supported unit. Direct support teams can be employed by the MEF AC/S G-2 or ISC to focus intelligence planning, direction, analysis, production, and dissemination support to the main effort or other specified MEF priority. When not so assigned, direct support teams will be integrated within other P&A cell or intel bn operations.

When a MAGTF of less than full MEF size is deployed, the P&A cell may contribute personnel to a task-organized intel bn detachment normally attached to the MAGTF or special-purpose MAGTF (SPMAGTF) command element. A common example would be the detachments provided to Marine expeditionary unit (special operations capable) (MEU[SOC]) CEs. Standing support includes small detachments from the IIP and topographic platoon. The lead and tactical echelons' intelligence nodes and detachments rely heavily on electronic CIS connectivity to allow reach back to the more robust and capable analytical and production resources of the MEF and intel bn.

Communications and Information Systems

The intel bn, P&A cell, subordinate elements, and other key intelligence producers (e.g., radio battalion) must have sufficient communications resources to support internal C2, operations, and IR support. Communications capabilities generally consist of short- and medium-range voice communications equipment. The communications battalion or communications elements provide P&A CIS support beyond the basic requirements.

Basic Requirements

Regardless of the size of the MAGTF, the following standing CIS requirements must be satisfied to facilitate intelligence P&A operations.

Capability to Command and Control Subordinate Units

Intelligence officers and intelligence production element commanders or officers in charge must be capable of positive staff cognizance or C2 of subordinate units and integration of their operations with broader MAGTF and external intelligence and operations C2. Traditionally, single-channel radio and record message traffic have been used to support MAGTF intelligence units' C2, particularly at echelons below the MSC level. At MSC, major subordinate element (MSE), MAGTF CE, and higher command echelons, high capacity communications networks support intelligence production C2, operations, and product dissemination. In semi-static situations, secure electronic mail or telephone provide significant communications capabilities; in highly fluid or mobile scenarios, cellular, satellite communications (SATCOM), and very high frequency (VHF) and high frequency (HF) radios may be used.

Ability to Receive Collected Data, Information, and Intelligence from Organic and External Intelligence Organizations and Production Elements

The CIS architecture must provide connectivity between organic and supporting intelligence units and production elements. Principal and alternate means of CIS are dependent on mission, enemy, terrain and weather, troops and support available-time available (METT-T) factors. The commanders and users' desired product formats also influence the selection of CIS means. The means of communication must include the capability to transmit imagery, GEOINT, and other intelligence products with large data files as well as the capability to

disseminate IMINT and reports digitally via fiber optics, wire, radio, and voice formats.

Ability to Provide Intelligence to Supported Commanders

Supported commanders' intents, concepts of operations and intelligence, command relationships, and standing PIRs and IRs influence intelligence production CIS requirements. The CIS architecture must be capable of integrating production elements' C2 and supporting CIS operations, including general service (GENSER) and sensitive compartmented information (SCI) communications with the primary CIS channels used by supported commanders. The determination of principal and alternate CIS means depends on METT-T. The product format desired by commanders and intelligence users also influences the CIS means. The means of communication must include the capability to transmit imagery, GEOINT, and other intelligence products with large data files as well as the capability to disseminate SCI and GENSER all-source and intelligence discipline-unique reports digitally via fiber optics, wire, radio, and voice formats.

Ability to Share Intelligence Products and Reports with All-Source JTF, Other Components, Theater, National, and Multi-national Intelligence Organizations, Agencies, and Centers

Traditionally, MAGTF GENSER secure record and voice communications provide this capability. While these techniques continue to be used for MAGTF intelligence production, they are now secondary in importance to the use of Joint Worldwide Intelligence Communications System (JWICS), SECRET Internet Protocol Router Network (SIPRNET), and other CIS capabilities which allow participants to access each others' intelligence products and data bases and to immediately pull required data, intelligence, and other products. This CIS requirement includes the capability to disseminate intelligence with designated nongovernmental organizations (NGOs), private volunteer organizations (PVOs), and other U.S. and multinational governmental agencies, particularly during military operations other than war (MOOTW).

Information Systems

Information systems, such as the intelligence analysis system (IAS), and their associated networks are the lifeblood and lifelines of P&A cell and MAGTF intelligence analysis, production, and dissemination operations. Intel bn has sufficient information systems resources to satisfy internal C2, operations, and intelligence needs. Most information systems require access to SIPRNET for GENSER requirements and to JWICS for SCI requirements, which provide intelligence and data base access to MAGTF, JTF, and other components' elements, and theater and national intelligence reporting and data bases.

The nonsecure internet protocol router network (NIPRNET) is also a key resource for intelligence analyst research and access to public domain information, as well as a means to exchange unclassified information. The supporting MEF communications battalions provide the necessary network connectivity for GENSER information networks and communications pathways, and radio battalion provides SCI networks. Figure 2-7 on page 2-14 depicts a notional MEF intelligence processing, analysis, production, and dissemination CIS architecture and resources.

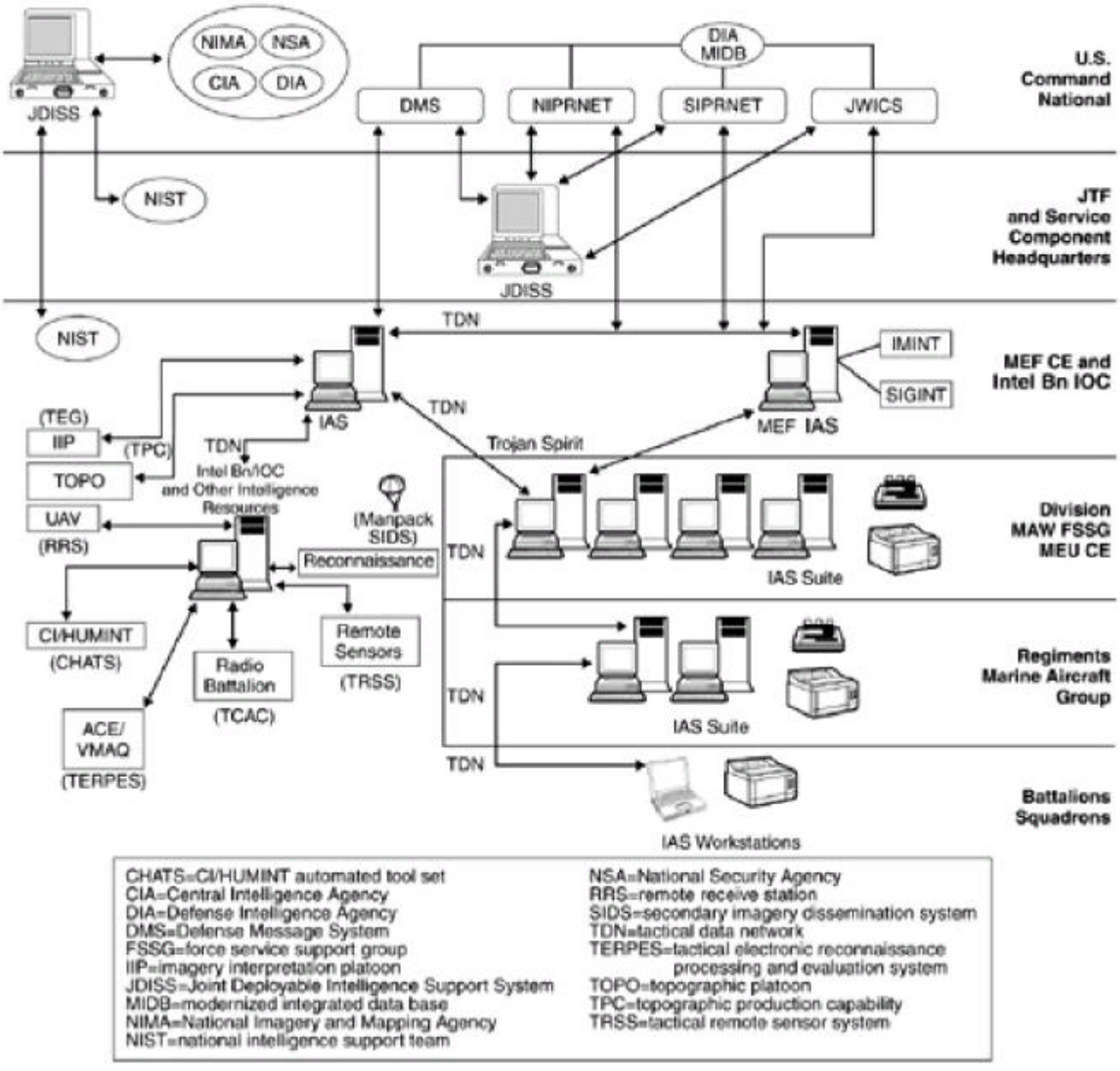


Figure 2-7. Notional MEF CIS Architecture.

CHAPTER 3. FILTERING, RECORDING, AND EVALUATING

When preparing information for analysis, intelligence personnel—

- Identify Information of Immediate Tactical Value. Every piece of data, information, or intelligence received must be assessed to determine its tactical value and its effect on current operations. Particular attention must be paid to possible alarms, triggers, and high-payoff targets (HPTs), which are defined by, and tied to, the PIRs, commander's decision support tools, and targeting priorities. If the information is relevant to ongoing operations, immediate production is initiated. The information is rapidly evaluated, analyzed, and disseminated for use by the commander and staff as well as subordinate and other affected units.
- Eliminate Redundant and Irrelevant Data Early in Processing. Each item received must be scrutinized to determine its pertinence to the unit's intelligence requirements. The incoming flow of data, information, and intelligence must be filtered for redundancy and relevance to the mission, AOI, and timeliness. This ensures intelligence analysts receive information and data that is useful to the analytical process while not being overwhelmed with unnecessary information or repetitive reporting.
- Identify Relevance to Ongoing Production. An important aspect of preparing an item for analysis is determining its impact on the ongoing intelligence production effort. The received data or information is evaluated to identify how it contributes to ongoing production in order to determine who should get the information, how urgent the information is, and in what format the information should be provided.
- Practice Standing Operating Procedures. The employment of information handling standing operating procedures (SOPs) saves time and effort. Standard methods of filtering, collating, recording, and evaluating speed up the preparation of incoming items for analysis, provide consistency in the way information is handled, and enhance comprehension of personnel performing the procedures and of the analysts receiving the incoming items.
- Employ Reliable and Accessible Recording Tools. Effective analysis depends in part on the ability to access, recall, and manipulate the stream of all-source data, information, and intelligence flowing into the command. Recording methods should be simple and flexible without interfering with timely analysis, production, dissemination, and use of intelligence. Analysts must be able to access information when they need it to receive the information in a form that facilitates understanding, and to rapidly integrate the data with other information or intelligence. The widespread use of automated information systems enhances the speed and utility of intelligence recording tools. However, analysts must ensure the necessary reliability and accessibility are built into the automated information systems and that associated backup procedures are established.

SECTION I. FILTERING

Filtering is the discarding of irrelevant or repetitive information prior to its entering the P&A process. Because current and emerging collection, communications, and intelligence automated information systems provide access to a vast quantity of raw data, processed information, and finished intelligence, there is significant potential for information overload of intelligence

sections and personnel. An effective filtering system is essential for managing the flow of data, information, and intelligence into the unit's intelligence processing and production system.

Filtering Criteria

Before information is entered into the production process, each item's relevance to the unit's intelligence requirements is assessed and unrelated material is discarded. The unit intelligence officer establishes basic criteria for filtering. Critical criteria drive the establishment of PIRs and IRs. The filtering criteria must be reviewed on a regular basis and updated to reflect changes in intelligence requirements, the AOI, and timeliness of information needed. Intelligence analysts use the following criteria when making assessments.

Subject Matter

The content of the data or report must be related to the unit's PIRs/IRs. Information that has no bearing on the PIRs/IRs is discarded, unless the information may impact future requirements.

Location

The event detailed in the data or report must have occurred within the unit's AO or AOI.

Time of Occurrence

The report should have continuing significance. For example, reports of future air or missile strikes may be received after the strike has begun; such reports are discarded unless they contain details of analytical importance.

Redundancy

Multiple reports relating to the same data or event are often received. Reports that repeat the initial information without adding significant data or analysis should be discarded, unless the reports provide critical confirmatory information.

Methodology

Filtering should occur as early as possible in the information processing system. Despite the fielding of automated intelligence systems, such as the Marine Corps IAS and the technical control and analysis center (TCAC), filtering is largely a manual process. A human must review voice reports, translated documents, images, and finished intelligence documents from higher echelons.

Manual Filtering

Most intelligence sections establish a central point for the receipt and distribution of incoming intelligence, counterintelligence, and reconnaissance reports. Normally, the intelligence watch within the combat operations center or the surveillance and reconnaissance cell is the receiving and distribution point. The watch examines each piece of data, information, and intelligence received; compares the content to the filtering criteria; and decides whether to discard the report. Filtering personnel must be able to rapidly identify new intelligence information of immediate tactical value and to quickly initiate the necessary actions.

Automated Filtering

For machine-readable formatted messages, automated intelligence systems are significant filtering tools. Systems such as the IAS can automatically filter incoming messages according to specified parameters such as location, time, and type of report. Use of IAS speeds the filtering process by correlating incoming information to existing units' tracks within the data base. However, the unit name or identification and location data fields in the formatted message must be filled out for this automatic function to occur, or the system will hold the message for

manual correlation. Automated systems are a tool to assist the analyst, not replace them. The system operator must continually review the filtering parameters and assess the effectiveness of the information filtering system. As with manual filtering, IAS operators must be familiar with the unit's intelligence requirements, have situational awareness, and exercise sound judgment.

SECTION II. RECORDING

Recording is the reduction of information to written or other graphical representation and the arranging of this information into groups of related items. This step is performed so items of information can be observed as an integrated picture and studied in relation to each other. Recording information makes evaluation and analysis easier and helps prepare intelligence products by drawing together available information on a specific subject. It also provides a record of events for post-operation study of the enemy and AO.

Methodology

Recording performed by intelligence sections at all levels normally involves—

- Registering all incoming information.
- Logging, map or chart marking, filing and indexing, or entering information in the data base of an automated system.
- Maintaining a system designed for rapid and efficient operations.

At lower command echelons, especially during mobile operations, recording may be no more than the maintenance of a log and marked map. At higher command echelons, recording relies heavily on automated information systems, electronic data bases, and visual display units. Both methods should make full use of graphic recording tools (i.e., maps, overlays, graphs, and charts) that make it possible to visualize and absorb the maximum amount of information in the shortest possible time. The indexing and categorizing of subject matter in a recording system must be related to the projected area, scope, and nature of the operations and must be based on the—

- Commander's PIRs.
- Other IRs.
- Anticipated information flow.

The recording means must be able to handle the volume of information and intelligence received and to serve the needs of individuals requiring access to that information. In addition, recording means and techniques must permit timely dissemination of information and intelligence.

In the past, most recording was manually generated either on a map, journal, or status board. Today, the most common recording devices are automated data processing and information systems such as IAS. Office automation software allows the rapid creation of charts and graphs, the annotation and manipulation of images, and the rapid assembly of words and text. Intelligence journals, files, records, and data bases can be updated automatically, and the data can be recalled and displayed in an overlay form.

Recording Tools

Whether operating in a manual or automated environment, the most common types of recording tools used by the intelligence analyst are the intelligence journal, enemy situation map, intelligence workbook, order of battle or analyst files, and target files.

Intelligence Journal

The intelligence journal is an official, permanent, and chronological record of reports and messages that have been received and transmitted, of important events that have occurred, and of response actions taken (see fig. 3-1). Messages are place in the journal file in the numerical order of the journal entry number. The journal, besides providing a brief chronological account of events, serves as an index to the journal file. The journal covers a stated period, normally 24 hours. Each item entered in the journal normally contains—

- **An entry number, which is assigned to an incoming message and is recorded on the message.**
- **The time the information was sent, received, or noted.**
- **The message date-time group.**

INTELLIGENCE SECTION JOURNAL

PAGE NO.	NO. OF PAGES
1	1

ORGANIZATION OR INSTALLATION	LOCATION	PERIOD COVERED			
		FROM		TO	
		HOUR	DATE	HOUR	DATE
1ST MARDIV	BURGEW, GE (LA567275)	0001	02 DEC 00	2400	07 DEC 00

ITEM NO.	TIME IN	TIME OUT	INCIDENTS, MESSAGES, ORDERS, ETC.	ACTION TAKEN	INIT
1	0001		Journal opened 0001		BJP
2	0030		5th MAR: Company team A patrol reported enemy		
			supply dump vicinity LA888912.	Maj, S3, Cdr	BW
3		0055	ALL UNITS: Execute alternate challenge password.	CO, Staff, Units	(55)
			Primary compromised at 0700045.		
4	0200		5th MAR: Follow up to item 2. Search results:	CO, S3	(DJ)
			12XAT mines, 30,000 rounds 7.62 ammunition, 6 rolls		
			barbed wire, all destroyed in place.		
65	2400		Journal closed 2400		
			SUMMARY		
			No enemy contact during period,		
			but one enemy ammunition dump destroyed.		

TYPED NAME AND GRADE OF OFFICER OR OFFICIAL ON DUTY	SIGNATURE
SAMUEL A. MORRIS, CAPT, COC Intel Watch Off	SAM

Figure 3-1. Example of an Intelligence Journal Page.

- The originating agency or addressee.
- A brief description of the item.
- The disposition information.

Enemy Situation Map

The enemy situation map is a temporary graphic display of current enemy dispositions, major enemy activities, and other pertinent intelligence and information. By presenting that information in relation to each other, the enemy situation map also helps with interpretation, analysis, and decisionmaking. In addition, it helps dissemination by permitting the ready transfer of intelligence concerning enemy forces capable of interfering with the mission of the unit concerned. A primary analytical tool, the enemy situation map is often the only recording device used during fast-moving combat operations, particularly at lower command echelons.

Methodology

The enemy situation map should cover enough area to facilitate the conduct of current operations and the planning of future operations. A large MAGTF, such as a MEF, normally requires the following three enemy situation maps:

- Large-scale tactical map (approximately 1:50,000) for current ground operations.
- Medium-scale operational map (approximately 1:250,000) covering the AO and portions of the AOI to record deep enemy installations (e.g., airfields, missile sites) and enemy forces that can affect friendly operations.
- Small-scale strategic map (approximately 1:1,000,000 or smaller) to cover the MAGTF AOI and beyond.

At lower echelons, one map may suffice. The scale depends on the mission and threat. The map scale(s) used should be decided between the G-2/S-2 and the G-3/S-3 when the battlespace is defined (step one of the IPB process). Often, a combined G-2/G-3 map is used to conserve space in the combat operations center or other C2 cells. If separate intelligence and operations maps are maintained, overlays must be readily interchangeable between maps. Information displayed on the situation map must be tailored to the—

- Mission.
- Nature of the threat or enemy.
- Terrain.
- Command echelon being supported.
- Unit's PIRs/IRs.
- Force protection.
- Targeting priorities.

Generally, enemy maneuver units posted on the situation map are two echelons below that of the friendly unit. Enemy units, regardless of size, in friendly rear areas are always posted because of the amount of damage they can inflict on C2 and sustainment. The situation map reflects—

- Enemy unit identification, disposition, and boundaries.
- Significant terrain and infrastructure features.
- Locations of manmade and natural obstacles.

When plotting enemy activities and dispositions, intelligence personnel—

- Indicate the latest time when the activity was observed or the disposition was confirmed.
- Post information using standard military symbols and abbreviations. See Field Manual (FM) 101-5-1/Marine Corps Reference Publication (MCRP) 5-2A, *Operational Terms and Graphics*, for standard symbology.
- Explain any deviations from these symbols in the marginal data on the map or overlay.
- Mark maps and overlays clearly with the appropriate classification.

Information is posted on the situation map as it is received. Information is removed promptly when

no longer current, because omissions or outdated information may result in erroneous evaluations, interpretation, and decisions. On a hard copy situation map, separate flaps of acetate can be used to record different types of information, which reduces overcrowding. Also, to reduce overcrowding, a number or letter system can be used to record significant events or activity. The letter or number is marked at the appropriate location on the map where the activity occurred. On a board or marginal area alongside the map, the same letter or number is recorded with a notation of the activity observed. A numbering system that is easily cross-indexed to the journal or message file should be used.

Automation

Automated functions of the IAS and other intelligence information systems greatly assist the maintenance of an enemy situation map. The IAS enables the operator to—

- Zoom in and out through various maps to quickly change scale views of the battlefield, thereby enhancing the number, size, and types of enemy units displayed.
- Call up information, including last report and location, by clicking on the unit of interest.
- Forward electronic overlays to other IAS users or to systems such as tactical combat operations for display.
- Use large-screen displays to deliver information briefings.
- Share a common picture of the battlespace in near-real time with users at separate locations by using robust communications connectivity. Consideration must be given to developing manual and electronic backups in the event of catastrophic failure of the system.

Intelligence Workbook

Incoming information is recorded by subject in the intelligence workbook for ready reference and comparison. The workbook helps in determining the meaning and significance of related items of information, which facilitates further processing, production, and dissemination (i.e., preparation of intelligence summaries and reports). The workbook can be set up in any format; however, the most common format organizes the book according to topics in the intelligence summary.

As information is received, it is recorded in one or more parts of the workbook based on its content. For example, a report concerning a newly identified enemy armor unit could be recorded under the new units section as well as in the armor section. Each entry should include—

- Journal entry number for the source report.
- Time of the event or observation.
- Location.
- Brief extract of the information applicable to the workbook section.

Maintaining the workbook is a time-intensive, manpower effort, but a properly maintained workbook is a powerful analysis tool. The IAS operator has the ability to simultaneously break down portions of incoming messages into numerous sections of an electronic data base or workbook. Employed properly, this capability can significantly streamline the maintenance of an intelligence workbook.

Order of Battle Files

OOB files include information and intelligence on the identification, strength, command structure, and disposition of personnel, units, and equipment of a military force. Combined with information on the threat, terrain, and weather, OOB information is a key element in the creation of finished intelligence products (e.g., IPB, estimates, BDA).

OOB files maintained on threat, allied, and neutral or third party forces can be subdivided into—

- Ground OOB.
- Air OOB.
- Naval OOB.
- Electronic OOB.
- Weapons of mass destruction.
- Other categories tailored to the unit's needs.

The OOB subdivisions and level of detail maintained in each subdivision depends on the—

- Command level where the analysis takes place.
- Type of threat forces that can influence friendly operations.
- Mission assigned.
- Area of responsibility.

A MEF conducting an amphibious operation needs to maintain information on all types of forces, while a battalion or squadron operating as part of sustained operations ashore focuses on the ground or air OOB that most affect them. The battalion or squadron relies on higher, adjacent, supporting, or Service commands in the theater to provide other OOB (e.g., weapons of mass destruction, electronic OOB, naval OOB). Specific factors are evaluated for each type of OOB (see chapter 7 for a detailed discussion of these factors).

Lower command echelons' OOB analysis is generally more focused, less detailed, immediate in nature, and performed by the unit's intelligence personnel as part of their general duties. At higher levels, particularly at a MEF or MAGTF CE, one or more analysts are assigned to each type of OOB. At these levels, OOB information normally becomes voluminous in a short period of time. In organizing this information, OOB analysts must maintain extensive and systematic compilations and filing systems. Specific items of information and intelligence must be located on short notice and incorporated into comprehensive reports or analyses. Regardless of the level of command, analysts at the tactical intelligence level use several OOB tools.

Unit Workbook

The format for the unit workbook depends on the structure of the enemy force being monitored. It consists of a collection of unit worksheets arranged by type of unit or in numerical sequence. Analysts with OOB baseline documents at their disposal use them as unit workbooks by inserting additional pages as new information is received. Normally, the parent unit listed on the unit worksheet is equivalent in size to the level of command performing the analysis. Records are maintained on units one level above and two levels below the enemy unit being monitored; however, this can be modified based on the situation. The date and the source of information are recorded for each entry (see fig. 3-2 on page 3-8). Unit OOB details noted in the remarks column include—

- Reports of branch insignia.
- Number and types of weapons.
- Local residents' statements in abbreviated form.

OOB Situation Overlay

This is a graphic portrayal of current confirmed or unconfirmed enemy OOB. It shows identification and disposition of enemy units and other information that will assist in developing the enemy OOB. Enemy units, down to and including two echelons below the analyst's own level of command, are plotted using the standard symbols included in FM 101-5/MCRP 5-2A.

Peculiarities of enemy organizations, the tactical situation, and time and personnel available determine what to plot or omit on OOB maps. The information time and date are entered below each plotted symbol.

Parent Unit _____						
Subordinate Units	**City**	**Coordinates**	**Installation**	**Personalities**	**Identification or Code No.**	**Remarks**
Division Headquarters	Stein	PV818147	1 and 3	Commander Col Crechin		EPW no. 26, captured 2 Feb 68
96th Mechanized Rifle Regiment	Delltach	PU820934	4	Commander Col Kurshave	16181	Document captured 19 Mar 68
145th Mechanized Rifle Regiment	Ellenburg	PU852961	2	LtCol Shrenko	16182	Deserter 21 Mar 88
3d Battalion	Gladbach	PV891024	1			Gladbach residents report battalion subordinate to headquarters in Ellenburg, 3 Feb 88
43d Medical Tank Regiment	Linburg	PV863106	3	Commander Col Reshvic		Agent report 26 May 68
358th Transportation Battalion	Lehrt	PV825158	1		16195	OOB Bank

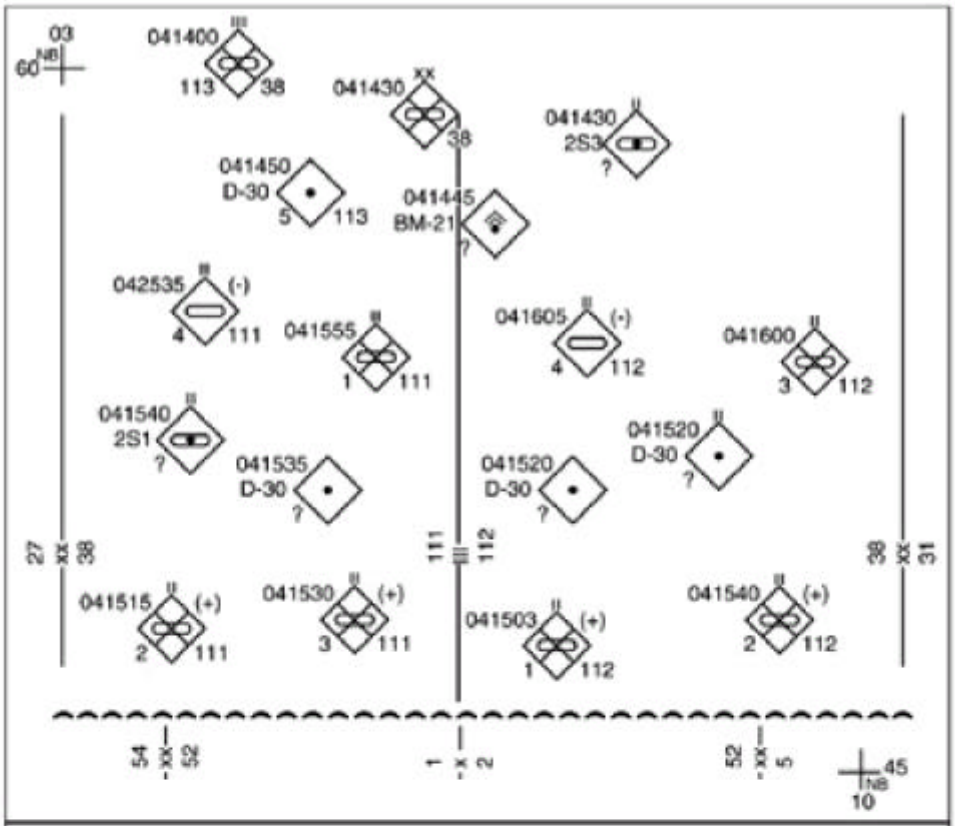
Figure 3-2. Example of a Unit Workbook Page.

An OOB situation map caption box contains annotated information that helps explain the OOB situation. Normally, the three types of caption boxes are: strength, unlocated units, and legend. At lower tactical echelons, the OOB situation overlay and the enemy situation map are combined for simplicity. At higher echelons, applicable analysts maintain separate types of OOB on overlays near their work area. A composite OOB overlay is used for the enemy situation map and for briefings (see fig. 3-3). The IAS allows the rapid generation of tailored electronic overlays based on available data base information.

OOB Record

As referenced in Standardization Agreement (North Atlantic Treaty Organization [NATO]) (STANAG) 2077, *Orders of Battle*, OOB record files are used to maintain accurate and complete data on all units. Normally, one record is maintained on each threat unit in a position to affect current or future operations (see fig. 3-4 on page 3-10). The OOB record contains the following information:

- **Service (branch of armed forces to which the unit belongs, including paramilitary and insurgent).**
- **Formation or unit name (official title).**
- **Alternative name (unofficial name).**
- **Role (principal function of the unit, e.g., command, combat, combat service support [CSS]).**
- **Superior formation (immediate senior formation or unit).**
- **Headquarters location name (nearest identifiable town or village).**
- **Headquarters location coordinates (universal transverse mercator [UTM] and latitude and longitude).**



Located Units (by type)			Unlocated Units
Committed Forces			
Unit	No.	Weapon	Recon Bn, 38th GMR Div
Mech Bn	6		114th Tk Regt, 38th GMR Div
Tk Bn	2	80 T-64	UI Ind Tk Bn, 38th GMR Div
			SSM Bn, 38th GMR Div
Reinforcement			
Tk Regt	1	94 T-64	
Ind Tk Bn	1	51 T-64	
Fire Support			
SSM Bn	1	SS-21	
Arty Bn	8	18xBM-21 MRL	
		18x152mm SP How	
		72x122mm How	
		36x122mm SP How	

Arty=artillery
Bn=battalion
Div=division
GMR=guard motorized
How=howitzer
Ind=Independent
Mech=mechanized
mm=millimeter
MRL=multiple rocket launcher
Recon=reconnassiance
Regt=regiment
SP=self-propelled
SS=surface-to-surface
SSM=surface-to-surface missile
Tk=tank
UI=unidentified

Figure 3-3. Example of OOB Overlay.

PARENT FORMATION									
Service		Formation or Unit Name		Alternative Name		Role		Superior Formation	
HQ Location Name		HQ Location Coordinates		Combat Effectiveness		Allegiance		Commander's Last Name	
SUBORDINATE FORMATIONS/UNITS									
Serial Number	Subordinate Unit or Formation Name	Location Coordinates	Role	Signature Equipment	Equipment Quantity	Commander's Last Name	Personnel Strength	Combat Effectiveness	Record Date/Update
Record Evaluation and Source					Remarks				

SAMPLE

Figure 3-4. Sample OOB Record.

- **Combat effectiveness assessment (ability to perform intended mission or function expressed in a percentage).**
- **Allegiance (entity or country to which unit owes its loyalty).**
- **Commander's last name.**
- **Subordinate formations' and units'—**
  - **Serial number.**
  - **Subordinate unit name.**
  - **Location coordinates (UTM and latitude and longitude).**
  - **Role.**
  - **Signature equipment (equipment that might identify the unit).**
  - **Equipment quantity (number of signature equipment in the unit).**
  - **Commander's last name.**
  - **Personnel strength (assessed strength).**
  - **Combat effectiveness.**
  - **Record date and update (date of information or last time record was updated whichever is later).**
  - **Record evaluation and source (listing of source and reliability as well as validity of the information).**
  - **Remarks (e.g., unit history, insignia).**

Personality File

Personality data on designated categories of individuals are recorded. Information on key figures is valuable in establishing an opponent's intent.

Military Installation File

This file contains collected information on each installation, to include the—

- **Number and types of buildings and their capacities.**
- **Personnel uniforms and insignia.**
- **Major items of equipment.**
- **Maps, town plans, or sketches that show the location of each installation within the city.**

Organizational Chart

This chart depicts the organization of units, from the highest headquarters to the lowest unit. It includes personnel and major weapon strengths. Principal weapon and equipment charts may be prepared to supplement organizational charts.

Strength Worksheet

Used to maintain a running numerical tabulation of the enemy's personnel and equipment strengths, the worksheet contains information recorded on committed units, fire support units, and reinforcements. The strength worksheet may be combined with OOB cards or other unit files. See chapter 8 for a detailed discussion of combat strength assessment.

Target Files

Target files are either standard (full page) or card type files.

Target Intelligence Files

Target intelligence files are developed selectively and aggressively to include the targets which, when attacked, will have an effect on the enemy. These files contain the following information:

- **Location (geographic and UTM coordinates, accurate within 10 meters).**
- **Altitude (target location expressed in meters or feet above sea level).**
- **Description (type, shape, attitude, dispersion, and composition).**
- **Vulnerability (assessed vulnerability of target to ordnance delivery, including construction, degree of protection, and dependence of the target on component parts).**
- **Recovery time (accurate assessment of the time required for the enemy to replace or return the target to active or usable status).**
- **Accessibility (location of a target with respect to other terrain or cultural features that may limit the direction or angle of attack).**
- **Importance (estimate of how the enemy would be affected by damage to that target).**

Target Card Files

These files are comprised of sets of cards; each card contains a target serial number and information concerning a specific target. Target card files are prepared and maintained on current targets and serve as a basis for the preparation of the target list and target bulletins. Cards are also prepared and maintained on potential targets so that a threat unit changing status can quickly be added to the target list. Complete target card files are maintained by commands that will exercise control of the target list during some phase of the operation.

Tools Automation

The IAS provides an automated means to employ the intelligence recording tools. When attached to appropriate communications, the IAS can automatically filter, parse, collate, update, and display threat-related data received from the national and theater level's modernized integrated data base. That data can be manipulated to provide the functionality of an intelligence journal, enemy situation map, workbook, OOB overlays, OOB files, and target files. Desktop application software can be used to generate spread sheets for strength tabulations and other files.

SECTION III. EVALUATION

During evaluation, the intelligence section determines the relevance, the source reliability, and the accuracy of recorded information. Evaluating information in this manner also determines whether immediate or deliberate production and dissemination should be performed.

Relevance

Upon receipt, each item of information is examined for its relevance by area, time, and content. Information relevant to the AO or AOI is processed further. Urgent information is rapidly evaluated and disseminated to those who need it. Information that is not of an urgent nature is usually fully evaluated, interpreted, and disseminated later.

Reliability

The information source and the information collection agency are evaluated for reliability. The principal basis for judging the reliability of a source or agency outside the MAGTF is previous experience with the source. Normally, analysts expect a highly reliable source to provide accurate information. Analysts must consider that even highly reliable human sources have limitations and a reliable electronic source may be subject to enemy interference and deception measures. Information reported from reliable sources should be compared with other facts before being classified as fact.

The headquarters closest to the source or agency is ordinarily the best judge of its reliability. Normally, a higher headquarters accepts the reliability evaluation of the reporting headquarters. Criteria for evaluating MAGTF unit reliability include knowledge of the unit's—

- Training.
- Experience.
- Past performance.

Accuracy

Accuracy involves the probable truth of the information. The most reliable method of judging accuracy is comparison with other information obtained through other collection sources and agencies.

A marked difference in the information accuracy evaluation may occur between higher and lower echelons. Higher echelons have access to more sources of information and intelligence than lower echelons, thus they provide more opportunity to confirm, corroborate, or refute the accuracy of reported data.

Regardless of the source, the accuracy of each report or piece of information is reevaluated at each echelon. Processed, evaluated, and interpreted information received from higher headquarters may be old, or new information that was not available at the time of the higher headquarters assessment may alter the information's accuracy.

Evaluation Rating System

A technique for evaluating the reliability and accuracy of information is determined by using a standard system described in STANAG 2022, *Intelligence Reports*. This system uses code letters to indicate reliability of the source and code numerals to indicate accuracy of the information.

Evaluation ratings are most valuable when information is disseminated to higher, adjacent, or lower units. Each item of information in a report should contain an evaluation to aid the recipient in understanding its significance.

Reliability Evaluation Codes

Agencies are ordinarily rated A, B, or C; however, when the source and the collecting or reporting agency are evaluated differently, the lowest degree of reliability is indicated. Reliability of the source is rated as—

- A—Completely reliable (indicates the source has experience and extensive background with the type of information reported).
- B—Usually reliable (indicates a source of known integrity).
- C—Fairly reliable.
- D—Not usually reliable.
- E—Unreliable.
- F—Reliability cannot be judged (indicates there is no basis for estimating the reliability of the source).

Accuracy Evaluation Codes

Accurate ratings are preferred, but when the truth cannot be judged, the rating of 6 is always favored over the inaccurate of ratings 1 to 5. The accuracy of information is rated as—

- 1—Confirmed by other sources (indicates that the information confirms currently held information and originates from a different source).
- 2—Probably true (indicates that the information confirms all or essential parts of currently held information and does not come from the same source, but cannot be confirmed by other sources).
- 3—Possibly true (indicates that the reported facts, on which no further information is yet available, are compatible with the previously observed target behavior; or that the known background of a person confirms that person's reported actions).
- 4—Doubtfully true (indicates unconfirmed information that contradicts estimates or the known behavior of the target).
- 5—Improbable (indicates information that is not confirmed by available data and that contradicts the experience previously assumed reliable).
- 6—Truth cannot be judged (indicates there is no basis for ratings 1 to 5 because of the complete absence of other information on the same subject).

Although both letters and numerals are used to indicate the evaluation of an item of information, they are independent of each other. A completely reliable agency may report information obtained from a completely reliable source which, on the basis of other information, is judged to be improbable and rated as A-5. A source known to be unreliable may provide raw information that is confirmed by reliable sources, accepted as credible information, and rated as E-1. A report evaluated F-6 may be accurate and should not be arbitrarily discarded.

CHAPTER 4. ANALYTICAL THINKING

Through analysis, information is transformed into knowledge. Understanding is achieved by applying judgment to knowledge, and the future is anticipated by understanding the present. Intelligence analysts enhance the understanding of the commander and staff to reduce uncertainty, limit risk, and support planning and decisionmaking. To enhance understanding for the commander, intelligence analysts must understand how decisionmaking occurs, the forms of reasoning, and the pitfalls often associated with analysis. At a minimum, the analyst must—

- **Know the commander's mission, intent, and guidance.**
- **Understand the battlespace framework, which includes the AO, AOI, battlefield organization, and tangible and intangible factors (e.g., culture, politics, economics, religious, ethnic).**
- **Understand information management.**
- **Understand friendly and threat doctrine and tactics.**
- **Develop PIRs and IRs with the commander, other staff sections, and subordinate units' intelligence officers, who are geared to answer or provide additional information on a threat's capabilities, vulnerabilities, intentions, and COAs.**
- **Understand how to use analytical tools (i.e., IPB, automated intelligence systems, data bases, indications and warning, situation development, targeting, and OOB factors).**
- **Relate information to the six intelligence functions and METT-T.**

SECTION I. ANALYTICAL PROCESS

Intelligence personnel analyze, synthesize, and estimate data gathered on a specific area or subject to support the commander's decisionmaking process.

Analysis

Analysis is a process used by commanders and analysts to establish IRs, to study information and available intelligence, and to determine a threat's capabilities, vulnerabilities, intentions, and COAs against friendly operations and systems. During analysis, a commander's AO and AOI are dissected for pertinent information and intelligence. In its simplest terms, analysis breaks down a geographic region or subject into bits and pieces of information and evaluates that information for its significance. Analysis considers the battlespace and its parts in terms of depth, width, height, time, surface, subsurface, and both friendly and threat commanders' IRs and decision cycles.

The commander starts the analysis process by defining the battlespace and submitting IRs; analysts can then—

- **Focus on the AO and critical aspects of the AOI.**
- **Prioritize all IRs.**
- **Query intelligence data bases.**
- **Determine gaps.**
- **Leverage collection and production assets to estimate the threat's capabilities, vulnerabilities, and intentions.**

Synthesis

Synthesis is the piecing of information into a coherent, meaningful picture. It is based on the ongoing or previous analysis of separate information and events taking place within a given area. More than simply pulling together information, synthesis determines the relationships that exist among that information. It allows commanders and analysts to see the battlespace as a whole and to rapidly discern emerging patterns and indicators. Threat capabilities, vulnerabilities, and intentions are estimated based on the synthesized picture.

Estimation

Estimation is the most challenging element and the last step in the analytical process. It involves a high degree of risk because it addresses future outcomes and probabilities. Intelligence analysts must stretch their intellectual resources to the limit to provide the best estimate possible given the information at hand and the needs of the commander. Employing experience, judgment, intelligence tools, and methodologies, the intelligence analyst must base estimates on solid analysis of identified activity patterns to determine the threat's intentions and probable COAs as well as the effects of those actions on friendly forces. The following example illustrates the analysis, synthesis, and estimation process.

Example: Analysis, Synthesis, and Estimation Process.

Information from aerial reconnaissance indicates the movement of approximately 31 moving target indicators (MTIs). The MTI locations and times are annotated on a mission report. Based on this report, the analyst conducts mental functions (analysis), attempts to fuse this information into what is happening in the battlespace (synthesis), and predicts intentions (estimation). To arrive at a conclusion, the analyst—

- Plots MTI locations on a situation map and annotates the date-time group. Looks for any relationships to previously reported units in the area and—
  - If a relationship is not found, determines what must be done to answer the who, what, where, and why questions.
  - If a relationship is found, determines the type of unit (e.g., tanks, armored personnel carriers), the direction of movement, and the unit's speed as MTIs pass through named AOIs.
- Looks at the big picture to synthesize the information and to answer the following questions:
  - Does the movement indicate where the MTIs will be committed?
  - Is this part of the threat's main effort?
- Prepares to state the threat's intentions through the combination of analysis and synthesis.
  - Provides an estimate, which specifies the type of equipment, the unit designator, the speed of march, and the probable time of attack.

SECTION II. ANALYTIC PROBLEM SOLVING

Intelligence analysis involves the application of reason and logic to solve problems related to the effects of weather, terrain, and threat on current and future friendly operations. During fast-paced, tactical-level operations, the entire analyze-synthesize-estimate process may occur mentally within a matter of seconds. At higher levels, the process may be more involved, with more time available to rigorously apply the analytical techniques. This section discusses

the problem solving analytical theories, terms, and processes most commonly used by military intelligence analysts.

Analytical Theories

Most analytical theories begin with a proposition or premise, which is a statement that may or may not be true.

Proposition or Premise

A proposition or premise is a combination of evidence and assumptions, which, when combined, lay the foundation for an argument, hypothesis, or conclusion. Propositions can be detailed or abstract, observable or inferable, with varying degrees of certainty and fuzziness.

Detailed

In military intelligence, the term for a detailed proposition is a specific information requirement. An example of a detailed proposition is: "An enemy company is defending at named area of interest (NAI) 13." When creating this mental proposition, the analyst is at the "I wonder if stage" of analysis. Because the statement is not known to be true or false, the analyst rephrases the proposition as a question. For example: "Is there an enemy company defending at NAI 13?" The detailed proposition requires verification from a collection asset.

Abstract

The doctrinal term for an abstract proposition is an IR, but commanders designate critical abstract propositions as PIRs. An abstract proposition might be: "Is the enemy's main effort going to be along the landing beaches south of Church Hill?" This proposition is abstract because no one single observation will confirm or deny it. The abstract proposition requires analysis and deduction based on multiple collection asset reports of detailed propositions. These reports would allow the analyst to discern or infer the enemy's main effort.

Observable

A single collection asset can verify a detailed proposition through observation and documentation in a single report.

Inferable

Abstract propositions can only be inferred by the analysis of a set of detailed propositions from multiple reports. The intelligence staff normally generates specific information requirements to subdivide an IR or PIR into more detailed propositions that can be addressed through integrated intelligence operation (i.e., collection, production, and dissemination) planning. The relationship between two propositions allows an intelligence analyst to make inferences and analyze intelligence information or to arrive at analytical conclusions. This relationship is expressed as: "Proposition X causes proposition Y." The same relationship can also be expressed as: "From the observance of proposition Y, we can infer proposition X." The following example illustrates the relationship between two propositions.

Example: Relationship between Two Propositions.

The existence of a regimental artillery group at NAI 14 will cause the existence of certain air defense assets in and around NAI 14. This proposition is restated as: "From the observance of certain air defense assets in and around NAI 14, we can infer the existence of a regimental artillery group at NAI 14."

The probability of each relationship must be taken into account. For example, the types of air defense assets normally associated with the regimental artillery group may also protect a logistic support area or command post. It is more accurate to state: "From the observance of a certain type of air defense near NAI 14, we can infer there is a 50 percent probability of a regimental artillery group in the NAI 14, a 40 percent probability NAI 14 contains a logistic support area, and a 10 percent probability it contains a command post."

Certainty and Fuzziness

Propositions have varying degrees of both certainty and fuzziness. Certainty is the degree of belief in something. An example of certainty is: "I personally saw an enemy company at NAI 13, and we have six corroborating reports." A less certain proposition would be: "HUMINT has a semireliable source that claims there is a company at NAI 13, and we have no other reports on the subject."

Fuzziness is the measure of how well the known information matches the desired information. An example of a certain proposition is: "Our patrol reports the exact number of enemy soldiers and equipment for an enemy company." A fuzzy proposition would be: "Our patrol reports about half the number of men and equipment of an enemy company, so this could be an augmented platoon, two understrength platoons, an extremely weak company or an under-reported enemy company."

A Priori

Probabilities, in the absence of other information, are called *a priori*. In practice, the *a priori* is rarely assessed in isolation of other information; however, more information is possessed than the contents of a single report. This leads to the use of a conditional probability. An example of this situation states *a priori* of the enemy commander choosing to concentrate his main effort along avenue of approach number 1 (AA-1) may be 66 percent. However, the conditional probability of the main effort along AA-1 might be 25 percent given that an unusually large number of combat vehicles on AA-2 were observed.

Applied Logic

Typically, intelligence deals with obscure data, few facts, and severe time constraints, which can limit the analyst's ability to apply formal logic in intelligence analysis. Nevertheless, there are areas of applied logic that are most relevant to intelligence analysis.

In its most basic form, analysis involves drawing reliable conclusions based on facts, opinions, and inferences. As information is received, it is categorized as either fact or opinion. From these facts and opinions, analysts attempt to piece together a picture of the battlefield and the commander's battlespace and to make certain inferences or conclusions. When presenting the resulting conclusions, it is important to distinguish between what is fact and what is opinion.

Facts

A fact is a statement that has been demonstrated to be true. As an example, it is a fact that you are reading this statement. Given a preference, an analyst will always choose to work with facts. Unfortunately, facts are not always available. In the absence of facts, opinions may be used. Combining available facts and expert judgment, analysts attempt to piece together a picture of the battlefield and the commander's battlespace. When presenting the resulting conclusions, it is important to distinguish between what is fact and what is opinion.

Opinions

When facts are unavailable, an analyst might use opinions. An opinion is what someone believes to be true, but it may or may not be true. Sometimes opinions are uttered as statements of fact and often they reflect value judgments. A value judgment is an expression of personal taste, reference, worthiness, merit, quality, excellence, or bias. For example: "Electronic intelligence is a far more reliable source of intelligence than HUMINT." In this case, the speaker's perception is an opinion or generalization. Analysts must use extra caution when basing conclusions on opinions.

Inferences

Inferences are conclusions drawn from facts, opinions, or other inferences. Noting that one area of foliage appeared discolored in contrast

to surrounding foliage, an image interpreter concluded that the area being looked at contained a camouflaged position. Based on expert knowledge of imagery, the analyst inferred the presence of a camouflage position from the fact of discolored foliage. Such inferences may serve as input for subsequent problems; in this case, determining what is camouflaged at that particular location. Inferences are particularly important in determining a threat commander's intent. Unless the threat commander announces it, intent can only be established by inference. Such inferences are based on facts developed through the continual study of an adversary's doctrine, tactics, and capabilities. Whenever possible, inferences should be drawn from facts, or a mixture of facts and opinion. Conclusions drawn from opinions alone are prone to be wrong and should not carry the same weight as those drawn from facts.

Reasoning

Reasoning is the mental process that is brought to bear on facts, opinions, and inferences. Analysts solve problems through deductive and inductive reasoning.

Deductive

The process of reasoning from general cases to specific cases is deductive reasoning. It is the drawing of conclusions from one or more propositions or premises. For example, the statement, "Air strikes and naval bombardment always precede an amphibious landing," is a proposition based on an assumption. Propositions may or may not be true; in the case of the statement above, not all amphibious landings are preceded by preparatory fires. For deduction to be used effectively, intelligence analysts must make certain their propositions are true and their reasoning is correct or valid.

Example 1: Deductive Reasoning.

A Naval intelligence analyst is given a report about an unidentified submarine transiting the polar ice cap. The analyst deduces that—

- The ability to transit under the ice cap requires long submerged endurance.
- The only submarines with adequate endurance are nuclear-powered.
- The unidentified submarine is nuclear-powered.

In this case, the analyst reasoned from a general type (submarines) to a specific type (nuclear-powered).

In the example, the propositions are stated as facts. However, depending on the time of year, the polar ice cap can be transited on the surface. Furthermore, the second proposition, although stated as a fact, assumes that the threat has not developed high-endurance power sources other than nuclear energy. As a result, the conclusion, although valid, is unreliable. In order to be reliable, a conclusion must be drawn from valid and true propositions. If a deductive argument is valid, and if the propositions of that argument are true, then the conclusion of that argument must also be true.

Example 2: Deductive Reasoning.

During a field training exercise, reconnaissance elements are able to photograph opposing force tanks in defilade. The photograph shows a main gun tube with a 125mm bore and three track-return rollers. Four types of threat tanks are equipped with the 125mm gun (T-64, T-72, T-80, and T-90), but only two have three track-return rollers (T-72 and T-90). Since the T-90 was not replicated in this exercise, analysts conclude that friendly forces will be engaging T-72 tanks. In this case, the reasoning went from the general (125mm gun and three track-return rollers) to the specific (T-72, which was the only tank with both characteristics replicated in the exercise). The argument is valid and the propositions forming the argument are true, so the conclusion of the argument must also be true.

Inductive

The process of arriving at conclusions based on evaluating facts or inferences is inductive reasoning.

Example 1: Inductive Reasoning.

The following reports reach an intelligence agency regarding the actions of two adversarial countries—

- Country X is massing armor and artillery along the border of Country Y.
- Country X has also blockaded sea-lanes used by both countries.
- Finally, Country X has imposed wartime restrictions on its civilian population.

From these reports, the analyst uses inductive reasoning by inferring that hostilities between the two countries are imminent.

Induction goes beyond the facts or observations to a statement that has not been or cannot be verified. Since only verified data can be called reliable, conclusions drawn inductively are somewhat unreliable.

Example 2: Inductive Reasoning.

An intelligence analyst is given the following information about a coalition armored vehicle:

- Fact 1—Five road wheels and four return rollers.
- Fact 2—Armament that includes a single 73mm gun, one coaxial- and two hull-mounted 7.62mm machineguns, and a single SAGGER antitank missile mounted on the barrel of the 73mm gun.
- Fact 3—Crew of four with three passengers.
- Inference 1—A maximum speed estimated to be 80 kilometers per hour.

From these characteristics, the analyst inferred that the reported vehicle was a Russian-made BMD. Since a number of separate facts or inferences were used in the reasoning process, the analyst arrived at a conclusion through inductive reasoning.

The strength of an inductive argument depends on how probable the conclusion would be true if the premises or propositions were true. Inductive arguments are characterized as being strong or weak vice valid and invalid. Arguments are made strong by—

- **The number of instances cited in the propositions.**
- **The number of propositions that confirm the conclusion.**
- **The closer in time the occurrences are to the conclusion.**
- **Dissimilarities in the evidence that still support the conclusion.**

Very often propositions used in deduction are arrived at inductively and vice versa.

Example: Deduction and Induction.

Major proposition: The massing of troops along a border is a prelude to war.

Minor proposition: A country is known to have massed troops along the border.

Conclusion: This country is about to initiate war with its neighbor.

At first glance, the deductive argument shown above might seem acceptable. However, a closer look will show that the major proposition is not always true. In certain instances, troops could be massed for internal security, exercises, or a show of force. The major proposition, derived from inductive reasoning, by itself is an ambiguous signal. Assuming the propositions are true, and assuming the analyst reasoned validly, the conclusion the analyst reached is valid. An analyst may reason correctly, but from data that is incorrect, thus arriving at conclusions that are not true.

Tests of Truth

Both inductive and deductive reasoning involve three basic tests of truth that intelligence analysts employ to determine the truth of propositions.

Correspondence Test of Truth

The theory that truth is a statement that corresponds to reality is known as the correspondence test of truth. An analyst, who is studying an information report, notices that the presented information is the result of first-hand observation. Knowing the source to be professionally competent, the analyst assumes that every statement in the report corresponds to reality.

In the example, the statements or other evidence corresponded to reality. To test the degree of correspondence, observations are required. These observations must be tested by additional observations. The chief criterion in observations is objectivity, and using a mix of collection assets can attain greater objectivity.

Analysts naturally place more confidence in one source or system than another. In the case of the UAV report verses the pilot's report, the analyst had more confidence in the UAV's ability to observe the target from multiple aspects. The UAV-derived information had more credibility than the pilot's report, because the pilot may have only had a fleeting glimpse of the target while trying to egress. When a variety of sensors tend to corroborate each other, confidence in the conclusions increases.

The correspondence test of truth requires observations to test whether or not, and to what extent, statements correspond to reality. One problem with this theory is that the threat seldom permits direct observations and often goes to great lengths to prevent direct observations or to deceive those observations.

Example: Correspondence Test of Truth.

Pilots returning from an interdiction mission claim three tanks destroyed. The squadron chief interrogated each pilot separately and they gave substantially the same report.

Assuming the pilots' claims are accurate, then it would reflect reality. By reporting battle damage assessment of three tanks probably destroyed, the squadron chief is adhering to the correspondence test of truth.

Despite the fact that all pilots of one flight claimed three tanks destroyed, the MAGTF commander wants more supporting evidence. To provide confirmation, the MAGTF G-2 plans an UAV mission over the area where the tanks were reportedly hit. Both the commander and the G-2 are placing more credibility in visual evidence, because it is believed to be more objective and less prone to human error. This ignores the fact that video requires interpretation, and this interpretation involves a degree of subjectivity.

Humans must interpret all images. When humans interpret images, they use subjective judgment. One of the weaknesses of the correspondence test of truth is that observations are required to establish the truth. Invariably, these observations must be tested by other observations.

The UAV tape revealed three badly damaged tanks in defilade. The MAGTF battle damage assessment analyst considers the UAV report along with the pilot debriefs. Based on the combined information, the analyst reports three tanks confirmed damaged.

Coherence Test of Truth

This test of truth uses consistency with other ideas or facts to validate statements. Where direct access to the threat is denied, the coherence test of truth becomes necessary. The coherence theory refers to how consistent different pieces of information are in relation to each other. An analyst considering a new piece of information

that corroborates known information would place more credibility in the new information and the conclusions drawn from it.

In the realm of theory, intelligence usually works with some factual basis for most inferences or conclusions. The coherence test of truth supplements the correspondence test of truth.

Example: Coherence Test of Truth.

In the latter part of September, the commander in chief's intelligence staff considered the following information:

- The ACME coalition countries normally conclude a training cycle with a large-scale combined exercise (historical record).
- Visitors to Coyote Land reported being denied access to certain areas in the vicinity of Road Runner in the western Tunnel Province (confirmed report).
- Reports indicate certain infantry, armor, and engineer units from Tasmania, Elmer Land, and Chickenhawk have moved from their garrison locations (unconfirmed reports).
- All commercial air traffic to Road Runner will be restricted for a period of 2 weeks, starting 1 October (confirmed report).

The intelligence staff concluded that this year's ACME exercise will take place in or near Road Runner, Tunnel Province, during the period 1 to 14 October. Although no one piece of information pointed directly to this conclusion, all pieces of information seemed consistent with each other as well as to the conclusion.

Pragmatic Test of Truth

This test proposes that a given statement is true if it works in practice.

A practical tool, the pragmatic test of truth has some weaknesses. First, the results may only appear to justify the means used to achieve them. Second, a successful outcome may be attributed to other factors that could have produced the same outcome. In the Admiral Scott example, the use of radar-controlled guns may have produced the same result no matter what formation was used. Lastly, an unsuccessful outcome does not necessarily imply that the means used were unsound; again, other unknown factors may have contributed to the unsuccessful outcome.

Example: Pragmatic Test of Truth.

Prior to the Battle of Cape Esperance in World War II, Admiral Norman Scott organized a task force into a long, single column. Admiral Scott believed this line-ahead formation would be effective against the Japanese units' night tactics. In the ensuing battle, Scott sank two Japanese destroyers and severely damaged two cruisers. After the battle, Admiral Scott concluded the original line-ahead formation theory was indeed effective. By combining radar-controlled fire control systems with line-ahead formation, Admiral Scott believed any night battle could be mastered.

SECTION III. PITFALLS OF ANALYSIS

The application of logic and reasoning is a mental process that is subject to numerous influences. Intelligence analysts involved in discerning facts, inferences, and conclusions are prone to the influences that shape and mold their view of the world and their ability to reason. These influences are referred to as pitfalls of analysis. To minimize their impact, analysts must be able to recognize these pitfalls in their own analysis and the analysis performed by others. Logical

fallacies and biases are two general categories of analytical pitfalls.

Logical Fallacies

Logical fallacies are errors in the reasoning process caused by the failure to apply sound logic. Though usually committed accidentally, these fallacies are sometimes used deliberately to persuade, convince, or deceive. Omission and assumption are two categories of logical fallacies.

Omission

Fallacies of omission leave out something important. The argument may omit a consideration of many cases; it may omit a consideration of a hypothesis that would account for the same conclusion; or it may omit something unfavorable to the argument. Fallacies of omission can occur in many forms.

Oversimplification

Oversimplification is a generality that fails to adequately account for all the complex conditions bearing on a problem.

Example 1: Oversimplification.

"Air power and the M1A1 tank won the Gulf War." This statement ignores the fact that the attack aircraft and the M1A1 tank were only two of many weapons systems and other capabilities used to provide critical support and ultimate success during the Gulf War.

Oversimplification results when one or more of the complex conditions pertaining to a certain situation are omitted and includes—

- **Ignoring facts.**
- **Using generalities.**
- **Applying an inadequately qualified generalization to a specific case.**

Example 2: Oversimplification.

An ordnance specialist inspecting a captured, hand-carried, surface-to-air missile launcher concludes that the threat has no effective low-level air defense. The assessment is based on the fact that the launcher is equipped with antiquated guidance mechanisms. The ordnance specialist's conclusion omits the following considerations:

- That the launcher was planted by the threat to give a misleading picture of their true capabilities.
- That the threat abandoned the launcher because it was ineffective and more capable systems were available.
- The weapon may have been deliberately doctored to mislead weapons experts.

Other weapons (e.g., antiaircraft artillery, small arms) can be very effective in some situations.

Hasty Generalization

Conclusions drawn from samples that are too few or from samples that are not truly representative are hasty generalizations.

Example: Hasty Generalization.

After interrogating an enemy prisoner of war (EPW), the interrogation officer reports the threat's morale as extremely low and that surrender is imminent.

In this case, the interrogator is making a hasty generalization because the sample population considered (one EPW) is too small.

Composition

The fallacy of composition is erroneously reasoning from the properties of a single entity to properties of a group.

Example: Composition.

During a skirmish with a Viet Cong battalion, a single EPW was captured. This EPW was suffering from malaria, malnutrition, and low morale. It was noted that the EPW was equipped with a semiautomatic weapon of World War II vintage. After a brief interrogation, the intelligence analyst reported the enemy battalion recently engaged was starving, diseased, and poorly armed.

The intelligence analyst failed to consider that—

- Only one prisoner was captured because he was too sick to keep up with the rest of the battalion.
- The weapon of early vintage did not necessarily make it ineffective.
- Few captured prisoners have high morale; in fact, low morale could just as easily result from being captured as it could contribute to being captured.

In this example, besides falling prey to hasty generalization, the analyst also demonstrated the fallacy of composition by applying the properties of a single prisoner to an entire enemy unit.

Division

The fallacy of division erroneously assumes that the characteristics of a group exist in every member of that group.

Example: Division.

Members of the threat guard's brigade had never surrendered in previous combat. After a recent engagement, an EPW stated he was a member of the guard brigade. The interrogator doubted the EPW's statement because personnel from that brigade never surrender.

In this example, the interrogator committed the error of division by assuming that since no guard brigade personnel had ever surrendered, the EPW could not be from that brigade. The analyst took the characteristics of a unit and uniformly applied them to every member of that unit.

Special Pleading

In special pleading, only one side of an argument is presented.

Example: Special Pleading.

At the conclusion of a staff study, the staff members, who are proponents of the proposed COA, are directed to list the pros and cons of the proposal.

Arguments for the proposal:

- Job requires little to no increase in manpower.
- Job can save the Government 2 million dollars.
- Risk to personnel is minimal.
- Equipment is readily available.
- Little special training is required.

Arguments against: None.

By omitting arguments against the COA, the staff committed the fallacy of special pleading. This fallacy also arises when the many interacting forces that give rise to a situation (i.e., cause and effect) are ignored.

Post Hoc

In the fallacy of *post hoc* ergo *propter hoc* (before the event, therefore caused the event), consideration of other factors that might have accounted for the same result are omitted. Post hoc fallacies often occur when trying to establish cause and effect.

Example: Post Hoc.

An aircraft equipped with a new jamming pod was not fired on while flying over threat-controlled territory. It was concluded that, since the aircraft was not intercepted or fired upon, the jamming pod was extremely effective in suppressing threat electronic systems.

The conclusion may or may not account for the aircraft not being attacked. Other considerations include—

- The threat was obtaining electronic intelligence on this new pod.
- The threat recently relocated several surface-to-air missile units and did not want to reveal their new positions.

False Dilemma

The fallacy of the false dilemma omits consideration of more than two alternatives.

Example 1: False Dilemma.

"Either we attack at dawn or the enemy will be too strong."

The two words that generally warn of a potential false dilemma fallacy are "either" and "or." False dilemmas exclude middle alternatives and consider only options of two extreme positions.

Example 2: False Dilemma.

An intelligence staff officer reports to the commanding officer that the enemy has only the capability to either defend in place or retreat. The intelligence officer committed the fallacy of false dilemma by failing to anticipate or ignoring that the enemy could—

- Attack if they were willing to accept high casualties.
- Withdraw to an alternate defensive position.
- Conduct a delaying action.

Assumption

Fallacies of assumption relate to begging the question, stating hypotheses contrary to fact, poisoning the well, and misusing analogies. All of these fallacies implicitly or explicitly involve assumptions, which may or may not be true.

Begging the Question

This fallacy occurs when a speaker gives what is assumed to be a legitimate response to a question but it is merely a rephrase of the question.

Example 1: Begging the Question.

When asked why the enemy was not pinned down by fire, the platoon leader replied: "Our suppressive fire was inadequate."

The fallacy in this response is that by definition suppressive fire pins down the enemy or is intended to pin him down. Since the platoon failed to pin down the enemy, the inadequacy of this fire was self-evident.

Example 2: Begging the Question.

A pilot reporting to a debriefing officer stated: "In response to your questions about whether or not all of my bombs landed on target, I'd like to say that as soon as I completed my pass there were two large secondary explosions."

The pilot begs the question by shifting attention from the primary issue to a secondary one. The response did not address the question that was asked.

Stating Hypotheses Contrary to Fact

This fallacy occurs when someone states decisively what would have happened had circumstances been different. Such fallacies involve assumptions that are either faulty or simply cannot be proven.

Example: Hypotheses Contrary to Fact.

If we had not supported Castro in his revolutionary days, Cuba would be safe for democracy today.

Besides being a gross oversimplification, the assumption made in the statement cannot be verified.

Poisoning the Well

This fallacy seeks to discount evidence before it is presented, most often by discrediting the source.

Example 1: Poisoning the Well.

An ardent spokesman against the value of strategic bombing states: "You can't trust that man's testimony regarding the effectiveness of strategic bombing; he's employed by the Air Force."

The speaker is trying to discredit contrary evidence by creating the specific impression that the testimony is biased because the testifier represents a certain organization.

Example 2: Poisoning the Well.

One intelligence analyst says to another analyst engaged in pilot debriefs: "Be careful with this man; it is his first mission."

This statement intends to discredit evidence before it is presented. It pleads against the subject by assuming that the pilot's lack of experience will result in bad information.

Misusing Analogies

Analogies are strong tools that can impart understanding in a complex issue. In the absence of other evidence, intelligence analysts may reason from analogy. Such reasoning assumes that the characteristics and circumstances of the object or event being looked at are similar to the object or event in the analogy. The strength of a conclusion drawn from analogy is proportional to the degree of similarity between two objects or events. The danger in reasoning from analogy is assuming that because objects, events, or situations are alike in certain aspects, they are alike in all aspects.

Conclusions drawn from analogies are inappropriately used when they are accepted as evidence of proof. Situations may often be similar in certain aspects, but not in others. When one generalizes indiscriminately from analogy to real world, this is misusing analogies. One method for weakening an analogous argument is by citing a counteranalogy. A counteranalogy weakens the original analogy by citing other comparisons that can be made on the same basis.

Biases

A subjective viewpoint, bias indicates a preconceived notion about someone or something. Although biases interfere with successful analytic thinking, they can have a positive influence on analysis. With a lack of information, a preconceived notion can give the analyst a starting point for thinking about a situation. However, biases generally have a detrimental impact because they obscure the true nature of the information. Intelligence analysts must be able to recognize cultural, organizational, personal, and cognitive biases and be aware of the potential influence they can have on judgment.

Cultural

Americans see the world in a certain way. The inability to see things through the eyes of someone from another country or culture is cultural bias. Biases interfere with the analyst's ability to think the way an enemy commander might think or to give policymakers informed advice on the likely reaction of foreign governments to American policy. Also known as mirror imaging, cultural bias attributes someone else's inten-

tions, actions, or reactions to the same kind of logic, cultural values, and thought processes as the individual analyzing the situation. Although cultural bias is difficult to avoid, the following measures can lessen its impact:

- Locate individuals who were born or raised in the analyzed country or culture and—
  - Include them in the analytical process.
  - Ask their opinion about likely responses to friendly actions.
  - Take care when using their opinions, since they may be subject to biases regarding ethnic groups or cultures in the region and their knowledge may be dated or inaccurate.
- Locate regional experts such as foreign area officers and regional area officers who have lived or traveled through the area and are somewhat conversant regarding the culture. Assess the quality of the information provided against the level of knowledge and experience the individual has for that culture or region.

Organizational

Most organizations have specific policy goals or preconceived ideas. Analyses conducted within these organizations may not be as objective as the same type of analysis done outside the organization. Groupthink and best case are organizational biases that can affect subjective internal analysis.

Groupthink

This bias occurs when a judgment is unconsciously altered because of exposure to selective information and common viewpoints held among individuals. Involving people outside the organization in the analysis can combat this bias.

Best Case

This bias occurs when an analyst presents good news or bad news in the most optimistic light. The judgment is deliberately altered to provide only the information the commander wants to hear. Analysts can avoid this bias by having the moral courage to tell the commander the whole story, good and bad.

Personal

Personal biases stem from past experiences. If a thought pattern previously led to success, the analyst tends to follow that pattern. Even if the situations have nothing in common, the tendency to follow past successful methods is very strong.

Cognitive

The all-source intelligence analyst evaluates information from a variety of sources (e.g., HUMINT, SIGINT, IMINT, open source). The degree of reliability, completeness, and consistency varies from source to source and even from report to report. This variance often creates doubt about the reliability of some sources. Cognitive biases that affect the analyst include vividness, absence of evidence, oversensitivity to consistency, persistence of impressions, dependence on memory, and acceptance of new intelligence.

Vividness

Clear and concise or vivid information has a greater impact on analytical thinking than abstract and vague information. A clear piece of information is held in higher regard than a vague piece of information that has more value as evidence. Analysts must consider that an enemy may use deception to portray vivid facts, situations, and capabilities that they want the friendly intelligence effort to believe.

Absence of Evidence

Lack of information is the analyst's most common problem, especially in the tactical environment. Analysts must do their best with limited information and avoid holding back intelligence because it is inconclusive. To avoid this bias, the analyst should—

- **Realize that information will be missing.**
- **Identify areas where information is lacking and consider alternative hypotheses.**
- **Adapt or adjust judgments as more information becomes available.**
- **Consider whether a lack of information is normal in those areas or whether the absence of information itself is an indicator.**

Oversensitivity to Consistency

Consistent evidence is a major factor for confidence in the analyst's judgment. Information may be consistent because it is appropriate, or it may be consistent because it is redundant, is from a small or biased sample, or is the result of the enemy's deception efforts. When making judgments based on consistent evidence, the analyst must—

- **Consider if the evidence represents all available information and intelligence. If it does not, or if it is not known, then the confidence level will be low, regardless of the consistency.**
- **Be receptive to information that comes in from other sources regardless of whether it supports the hypothesis or not.**
- **Be alert against confirmatory circular reporting, which is intelligence already obtained by the unit that is then reformatted by other units and intelligence organizations, modified slightly, and disseminated back to the unit.**
- **Know, to the degree possible, the original source for all intelligence to ensure that a circular report is not used as confirmatory evidence for an intelligence estimate or conclusion.**

Persistence of Impressions

When evidence is received, there is a tendency to think of connections that explain the evidence. Impressions are based on these connections. Though the evidence eventually may be discredited, the connection remains and so do the impressions.

Dependence on Memory

The ability to recall past events influences judgment concerning future events. Since memory is more readily available, it is easy to rely on memory instead of seeking a proper sample to predict events.

Acceptance of New Intelligence

Often newer intelligence reports are valued more than older intelligence reports, which can occur when the intelligence collectors or sources are different.

Example: New versus Old Intelligence.

A ground reconnaissance team reports at 1300 that an enemy mechanized column is moving along a line of communications (LOC) at a given speed and direction. Later, at 1325, an AV-8B in-flight report indicates that the enemy column is moving along a different LOC.

In such cases, the newer intelligence report should be assessed against the full tactical context, and not simply its timeliness, to preclude incorrect intelligence interpretations.

Using the above example, follow-on coordination with the better situated ground reconnaissance team, capable of observing the same LOC and enemy targets for a greater period of time, may lead to a very different intelligence interpretation.

SECTION IV. DECISIONMAKING

One aim of intelligence analysis is to allow the commander to make timely and informed decisions by providing the right elements of available information at the right time and place. Gaining more information can reduce uncertainty, but a decrease in uncertainty occurs at the expense of time. Uncertainty and time always influence the commander's analytical and intuitive decisionmaking ability.

Analytical

In analytical decisionmaking, several options for solving the problem at hand are identified, studied, and compared to arrive at the best solution. Basically, comparing multiple options concurrently produces the optimal solution. This approach to decisionmaking tends to be methodical and time-consuming.

Intuitive

In intuitive decisionmaking, the commander assesses the situation in an effort to recognize a pattern; once a pattern is identified, experience and judgment guide the commander in evaluating the key elements of the problem and rapidly determining a satisfactory solution. The intuitive approach focuses on situation assessment instead of on the comparison of multiple options. Generally much faster than analytical decisionmaking, intuitive decisionmaking aims at finding the first solution that will satisfactorily solve the problem.

Comparison

Each analytical and intuitive decisionmaking approach has strengths and weaknesses. Although conceptually distinct, the two are rarely mutually exclusive. Intelligence supports analytical decisionmaking by helping to identify available options and by providing the estimates and studies for comparisons of those options.

Intelligence supports intuitive decisionmaking by providing the knowledge that helps the commander recognize emerging patterns. The process of intelligence analysis employs both analytical and intuitive decisionmaking to arrive at the conclusions presented to the commander. The IPB process, particularly if the various types of products are prepared in detail, is a distinctly analytical process. The decision support template derived from the IPB process, however, is a tool that facilitates intuitive decisionmaking. Generally, the analytical approach conforms well to the prehostility or contingency planning phase, while the intuitive model is usually more appropriate during execution of tactical operations.

The challenge for the intelligence analyst is knowing how much and what kinds of information the commander requires. Too much information may only confuse an intuitive decisionmaker and information requirements will change continually. Too little information for an analytical decisionmaker may result in procrastination and the continual demand for more information. The key to overcoming these challenges is a solid understanding of the commander, constant interaction through training and exercises, and a well developed process for identifying information requirements.

CHAPTER 5. INTELLIGENCE PREPARATION OF THE BATTLESPACE

An analytical methodology, IPB is employed during operations to identify, assess, and reduce the effects of enemy, environment, and terrain uncertainties on friendly and threat forces. The IPB process analyzes the threat and environment in a specific geographic area to determine and evaluate the threat's capabilities, vulnerabilities, and probable COAs. Designed to support staff estimates, planning, and decisionmaking, IPB results are incorporated into the intelligence estimate, which provides knowledge-based intelligence that can be visualized and absorbed by decisionmakers. See appendix A for a detailed outline of the intelligence estimate format. The formatted graphics and images provided through the IPB process help the commander to rapidly visualize, assimilate, and apply intelligence in the decisionmaking process. This enhances the commander's ability to discern patterns as they emerge and to conduct recognitive or intuitive decisionmaking, thereby increasing operational tempo.

Operations and intelligence must have a common focus to successfully apply the interactive IPB process. See FM 34-130/Fleet Marine Force Reference Publication (FMFRP) 3-23-2, *Intelligence Preparation of the Battlefield*, for a detailed discussion of the IPB process.

The IPB requirements for a humanitarian assistance operation differ significantly from a combat operation against a conventional armed force. In a given situation, a unit or staff section may prepare some or all IPB products. Determining which products to prepare and identifying their relative priority depends on the factors of METT-T and command guidance.

The IPB process develops tailored, mission-focused, knowledge-based intelligence that is incorporated into a variety of intelligence products. Intelligence preparation of the battlespace provides intelligence in graphic and image formats that help the commander rapidly visualize, absorb, and apply the intelligence in the decisionmaking process. Numerous standard overlays and graphics are associated with the IPB process; however, each situation is unique. A modified combined obstacle overlay and threat doctrinal template that support conventional operations may be of limited use in military operations other than war (MOOTW). The type of products generated as a result of IPB vary based on the—

- **Size of the unit.**
- **Time available.**
- **IRs.**
- **Characteristics of the mission and AO.**

The IPB process defines the battlespace environment, describes the battlespace effects, evaluates the threat, and determines threat COAs. These steps are discussed in this chapter and remain constant regardless of the type of mission or size of the staff section; however, the application of the steps varies with each situation. This chapter also goes into detail about the decision support template and discusses the abbreviated IPB process.

SECTION I. STEP 1—DEFINE THE BATTLESPACE ENVIRONMENT

The first step of the IPB process identifies the physical space and specific features of the environment or activities that may influence friendly and enemy COAs and commander's decisions. When defining the battlespace environment, intelligence analysts conduct the following procedures.

Identify Significant Characteristics of the Environment

Characteristics of the battlespace environment that will influence the commander's decisions or affect the COAs available to friendly forces or the threat are of special significance. During a humanitarian assistance operation, for example, the location and activities of civilian relief organizations might be a significant characteristic of the battlespace. During support to counterdrug operations, significant characteristics might include narcotics production or weapons trading. During a conventional war, typical characteristics may include location and activities of enemy reserves, reinforcements, and long-range fire support. When identifying significant characteristics of the battlespace, intelligence personnel consider threat forces and other aspects of the environment that may have an effect on accomplishing the unit's mission. Depending on the situation, these environmental aspects may include—

- **Geography (e.g., area terrain and weather).**
- **Population demographics (e.g., ethnic groups, religious groups, age distribution, income groups).**
- **Political or socioeconomic factors (e.g., the role of clans, tribes, gangs).**
- **Infrastructures (e.g., transportation, telecommunications).**
- **Rules of engagement or legal restrictions (e.g., international treaties, agreements).**
- **Threat forces and their capabilities (e.g., paramilitary and unconventional forces).**

Initially, each environmental characteristic is examined in general terms to identify its significance to the command and its mission. Identifying the significant characteristics of the battlespace environment helps establish the geographical limits of the AOI and directs analytical efforts in steps 2 and 3 of the IPB process. It also helps identify uncertainties or gaps in the type of information and intelligence required to complete the IPB process and answer the PIRs and IRs (see fig. 5-1).

Identify the Command's Area of Operations and Battlespace Limits

The AO represents an area assigned to a commander with authority and responsibility for the conduct of operations (see fig. 5-2). The limits of the AO are normally the boundaries specified in the OPORD or higher headquarters execute order that defines the command's mission.

Area of Influence

This is the geographical area where a commander is able to influence operations through C2 of maneuver or fire support systems. Based on the range of organic or supporting weapon systems, the area of influence may extend beyond the AO.

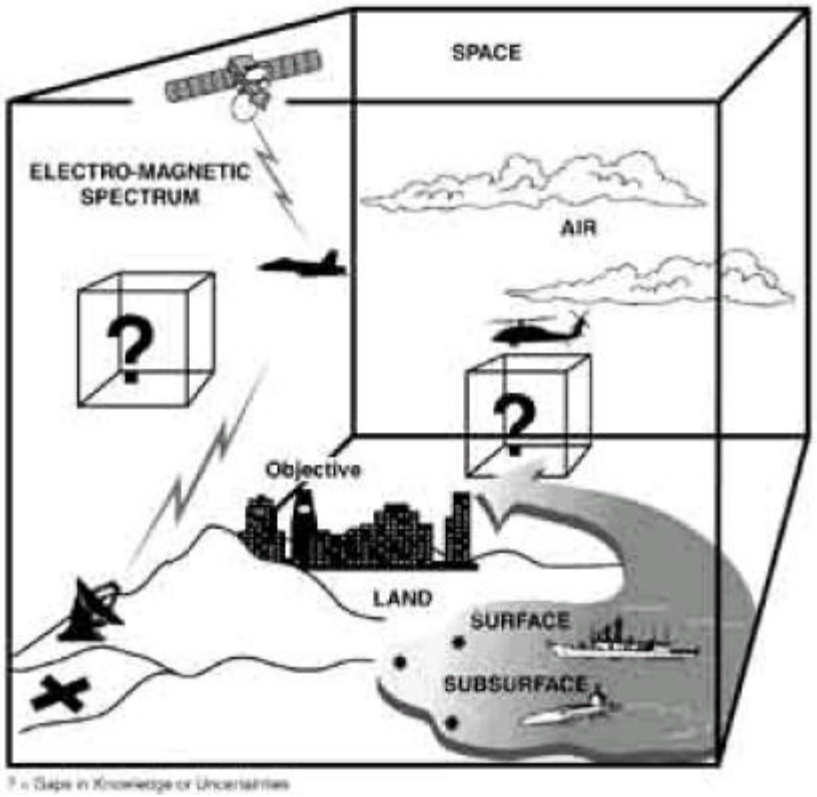


Figure 5-1. Battlespace Examination.

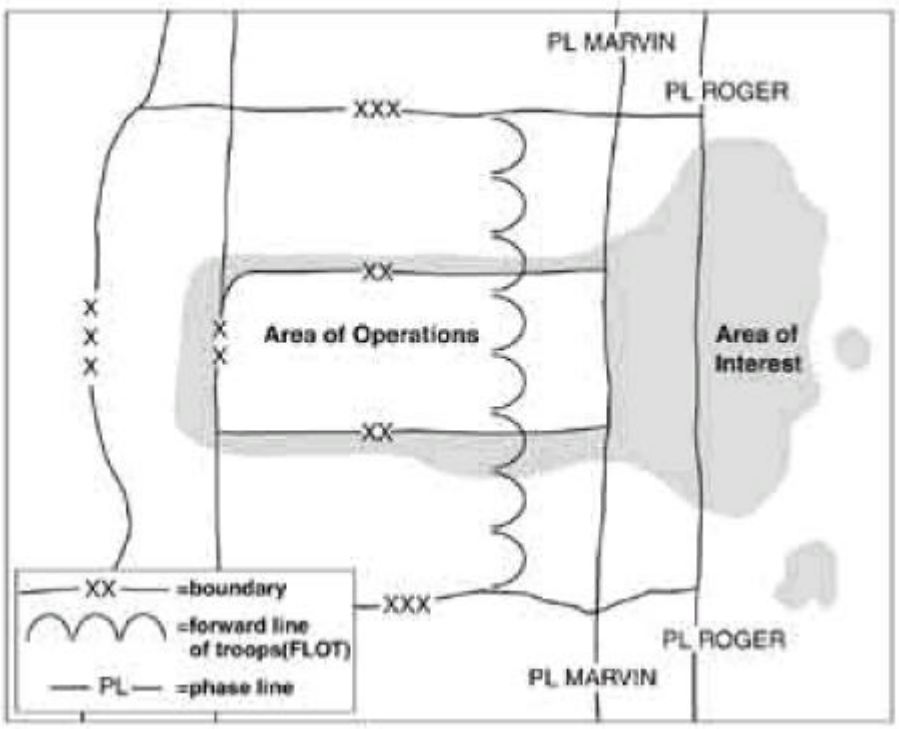


Figure 5-2. AO and AOI.

Area of Interest

The commander selects the AOI based on the estimate of the situation. The dimensions are not constrained by the organic ability to acquire information on that area. The AOI must extend, in as irregular a shape and as far as needed, in all directions to safeguard the command from surprise (see fig. 5-2). The AOI must be viewed in terms of width, depth, height or airspace, and time.

Battlespace

The battlespace is all aspects of air, surface, subsurface, land, and space, as well as the electromagnetic spectrum, the information environment, and other dimensions which encompass the AO, the area of influence, and the AOI. Figure 5-3 depicts many of these battlespace dimensions and factors.

Establish the Area of Interest Limits

The AOI is the geographical area from which information and intelligence are required to permit planning or successful conduct of the command's operation. The command's AOI is generally larger than its AO. The limits of the AOI include each of the characteristics of the battlespace environment identified as exerting an influence on potential COAs or command decisions.

The limits of the AOI are based on the ability of the threat to influence the accomplishment of the command's mission. The geographical locations of other activities or characteristics of the environment that might influence COAs or the commander's decision and the resulting changes in the command's battlespace must be considered when establishing AOI limits.

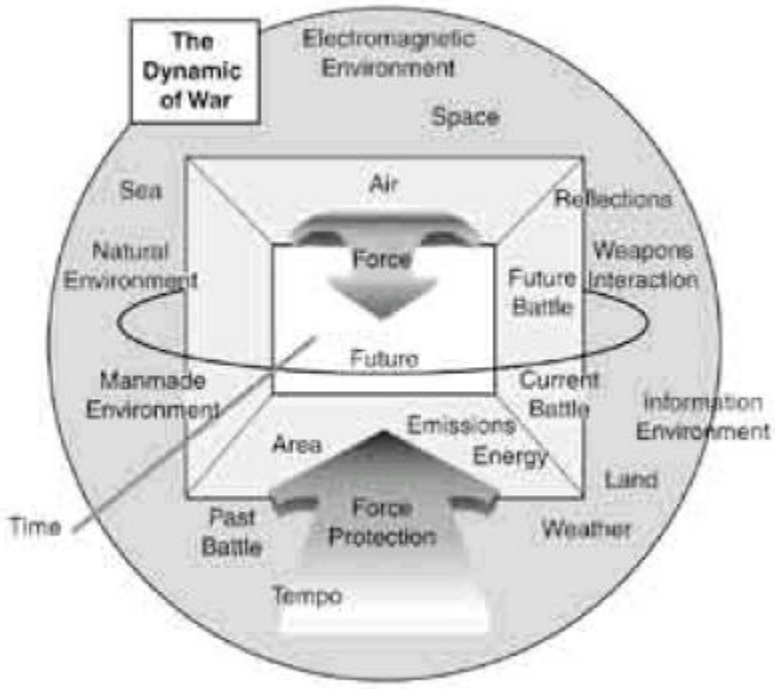


Figure 5-3. Battlespace Dimensions and Factors.

Areas of interest can be divided into several components (e.g., ground, air, political). Altitude must be considered in the air AOI when the projection of air power is of interest. When an air defense-related IPB is conducted, the AOI should extend upwards to the maximum service ceiling of the threat's aircraft. When an aviation-related IPB is conducted, the AOI should extend to the maximum service ceiling of friendly aircraft or the maximum effective altitude of threat air defense systems, whichever is greater. When space-based IPB is conducted, the AOI must extend to the maximum effective altitude of relevant space-based systems. Although AOIs may be developed separately, at some point they must be considered as an integrated whole.

One of the primary considerations in establishing the limits of the AOI is time. The time limit is based on the threat's ground and air mobility and the amount of time needed to accomplish the friendly mission. For missions of relatively short duration, such as the evacuation of noncombatants or raids, the AOI may be relatively small and usually includes only immediate, direct threats to mission accomplishment. A helicopter raid where the MAGTF has air superiority might have an AOI that includes only air defense systems within the range of the engagement area and the air routes. Some long-term missions, such as peacekeeping, will result in an extensive AOI that considers political, economic, and conventional military factors.

Since the limits of the AOI are based on threats to mission accomplishment rather than strictly terrain considerations, the limits may cross into neutral countries. If developments in a neutral country might influence accomplishment of the unit's mission, that country must be included in the AOI.

Identify the Detail Required for the Time Available

The time available for completion of the IPB process may not permit the luxury of conducting each step in detail. The focus must be on the parts of IPB that are most important to the commander in planning and executing the mission. Identifying the amount of detail required avoids wasting time on developing more detail than necessary in each step of the process. For example, the situation may require detailed threat analysis only on selected areas within the command's AO based on the assigned mission or other METT-T factors. Some geographical areas or threat forces within the AO may require only a summary type evaluation of their effects or capabilities.

Evaluate Existing Intelligence Data Bases and Identify Intelligence Gaps

Data bases may only contain some of the intelligence and information required to evaluate the effects of each battlespace characteristic and each threat force. This is especially true of the majority of countries where the MAGTF may conduct operations in the future. Identifying the intelligence gaps early allows the intelligence analysts to initiate action required for collecting intelligence and filling the gaps, to perform the necessary production, and to disseminate the intelligence products in a timely manner. When evaluating existing data bases, intelligence analysts must—

- Identify and prioritize the intelligence gaps in current holdings, using the commander's PIRs and intent to set the priorities.
- Identify any gaps that cannot be filled within the time allowed for IPB.
- Inform the commander and operators of unfilled gaps so that reasonable assumptions can be formulated.

Collect the Required Intelligence and Materials

Ideally, intelligence operations enable the analyst to develop estimates of the battlespace and the threat that match the actual situation. In reality, intelligence will never eliminate the unknown aspects or uncertainties that concern a commander and staff. Intelligence analysts must be prepared to fill in the gaps with reasonable assumptions and estimates. When collecting the required intelligence and materials, intelligence analysts must—

- Initiate collection or requests for intelligence to fill the gaps and to conduct IPB.
- Prioritize collection against all identified significant characteristics of the battlespace.
- Initiate action on identified IPRs and continuously update the IPB products as additional intelligence is received.
- Inform the commander as assumptions are confirmed during the initial mission analysis and IPB process.
- Re-examine the evaluations and decisions on which proven invalid assumptions were based.

SECTION II. STEP 2—DESCRIBE THE BATTLESPACE EFFECTS

The second step in the IPB process is to determine how the battlespace environment affects both threat and friendly operations. This evaluation step begins with an analysis of existing and projected conditions of the battlespace environment and determines how those conditions will affect friendly and threat operations and broad COAs. Intelligence analysts describe the battlespace effects by analyzing the battlespace environment, such as terrain, weather, and other battlespace characteristics, and by describing the battlespace effects on threat and friendly capabilities and broad COAs.

Analyze the Battlespace Environment

The degree of detail in the analysis varies depending on the area of the battlespace environment being evaluated. Generally, the AO is evaluated in more detail than the AOI. Additionally, the focus varies throughout each area. For example, rear areas within the AO may require a different focus than areas near the main battle area. Certain areas or subsectors affect various types of operations to varying degrees. During the evaluation, intelligence analysts must identify areas that favor each type of operation (e.g., offensive, defensive, force protection, peace enforcement). Terrain, weather, and other characteristics of the battlespace are analyzed as part of the IPB process.

Terrain

Terrain analysis is the means to determine which friendly COAs can best exploit the opportunities the terrain provides and how the terrain affects the threat's available COAs. The best terrain analysis is based on a reconnaissance of the AO and AOI. Analysts must identify gaps in knowledge of the terrain that a map analysis cannot satisfy and use the identified gaps to guide reconnaissance planning and to focus on areas most important to the commander and the mission.

The members of intel bn's topographic platoon usually conduct the major portion of the terrain and hydrographic analysis and development of supporting GEOINT products. They also receive

support from Army topographic units operating as part of or in support of the joint force. Topographic personnel work closely with weather personnel and weather analysts to ensure that terrain analysis incorporates the effects of current and projected weather events.

The National Imagery and Mapping Agency (NIMA) produces specialized maps, overlays, and automated data bases for specified areas of the world to aid in map-based evaluations. The tactical terrain analysis data base consists of selected terrain information that is limited to natural and manmade features of tactical military significance, which can be exploited by terrain analysts to satisfy military requirements. Specialized NIMA products address—

- Cross-country mobility.
- Transportation systems (road and bridge information).
- Vegetation type and distribution.
- Surface drainage and configuration.
- Surface materials (soils).
- Ground water.
- Obstacles.

Terrain analysts must ensure that the analysis includes the effects of existing and forecasted weather on the military aspects of the terrain, because changes to the battlespace environment may change the terrain analysis evaluation results. Analysts express the results of evaluating the terrain's effects by identifying areas of the battlespace that favor, disfavor, or do not affect each broad COA. These conclusions are reached through analysis of the military aspects of the terrain and evaluation of the terrain's effects on military operations.

Analyze the Military Aspects of the Terrain

Terrain analysts evaluate the following military aspects of terrain to determine the effects on military capabilities:

- Key Terrain—Any locality or area (natural or manmade) that the seizure, retention, or control of will afford a marked advantage to either combatant.
- Observation and Fields of Fire—Observation is the ability to see the threat either visually or through the use of surveillance devices. Fields of fire are areas that a weapon may effectively cover with fire from a given position.
- Cover and Concealment—Cover is protection from the effects of direct and indirect fires. Concealment is protection from observation. Ditches, caves, river banks, folds in the ground, shell craters, buildings, walls, embankments, woods, underbrush, and other natural or manmade features can provide cover and/or concealment.
- Obstacles—Any natural or manmade feature that stops, impedes, slows, or diverts military movement.
- Avenues of Approach and Mobility Corridors—Avenues of approach (AAs) are air, sea or ground routes of an attacking friendly or threat force of a given size leading to its objectives or to key terrain in its path (see figs. 5-4 below and 5-5 on page 5-8). Mobility corridors are areas where a force will be

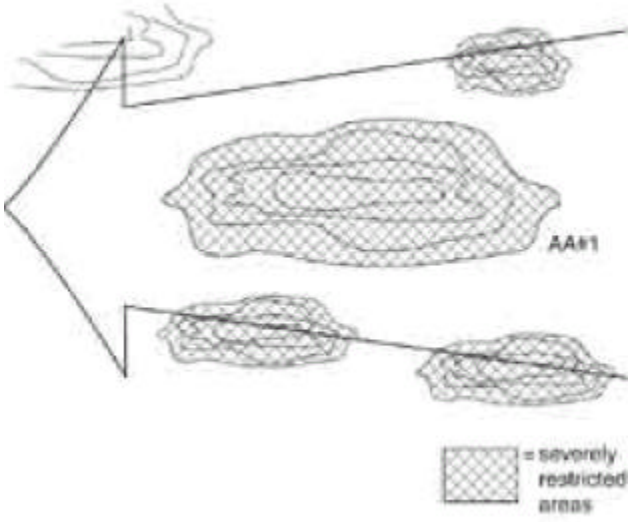


Figure 5-4. Regimental Ground AA.

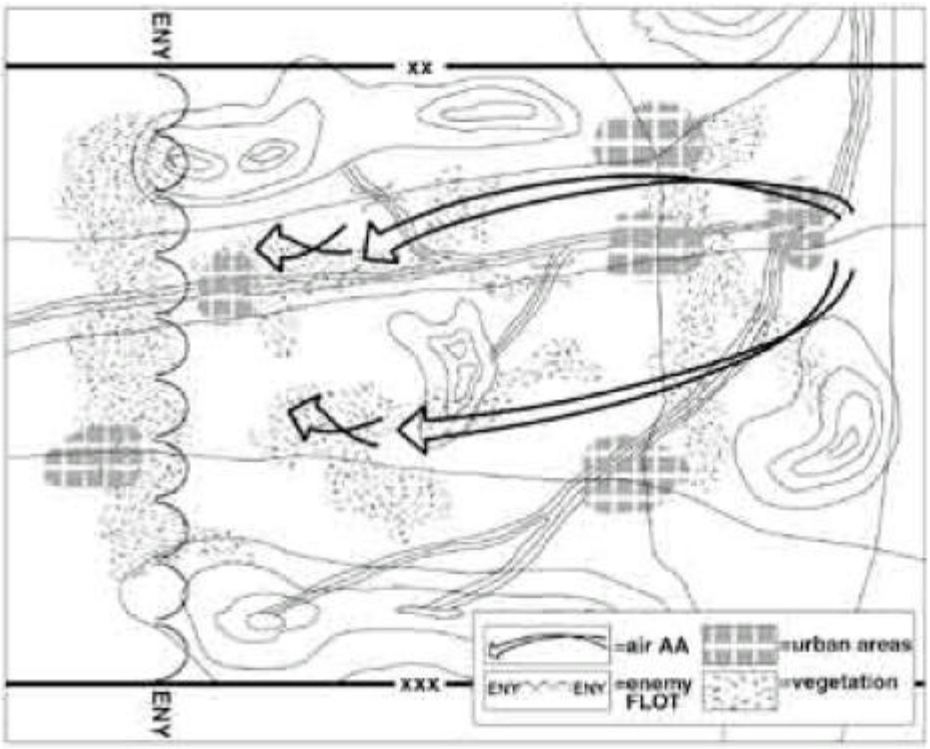


Figure 5-5. Air AAs Overlay.

canalized due to terrain restrictions. A mobility corridor is relatively free of obstacles and wide enough for maneuver of tactical formations, which allows military forces to capitalize on the principles of mass and speed. When grouped together, mobility corridors constitute an AA (see fig. 5-6). Based on previous terrain analyses, the analyst determines how the terrain will allow maneuver to objectives. Analysts must consider littorals/waterways (e.g., beaches, rivers) as possible mobility corridors and AAs.

Evaluate the Terrain's Effects on Military Operations

Terrain analysts evaluate the terrain's effects on friendly and threat offensive and defensive COAs by identifying the areas along each AA best suited for use as potential—

- **Engagement areas and ambush sites—Using results of concealment and cover evaluation, terrain analysts identify areas where maneuvering forces are vulnerable to fires. They consider ranges of weapons, flight times of missiles, and the likely speed of maneuvering forces. If the unit is attacking, analysts identify areas where the unit will be vulnerable to threat fires. If the unit is defending, analysts identify potential engagement areas (see fig. 5-7).**
- **Battle positions—These positions may be used by friendly attacking forces to block enemy counterattacks. Terrain analysts identify concealed and covered positions that offer observation and fields of fire into potential engagement areas. If a command is defending, these positions are potential defensive positions; if a command is attacking, the positions provide a start point for determining possible threat COAs.**

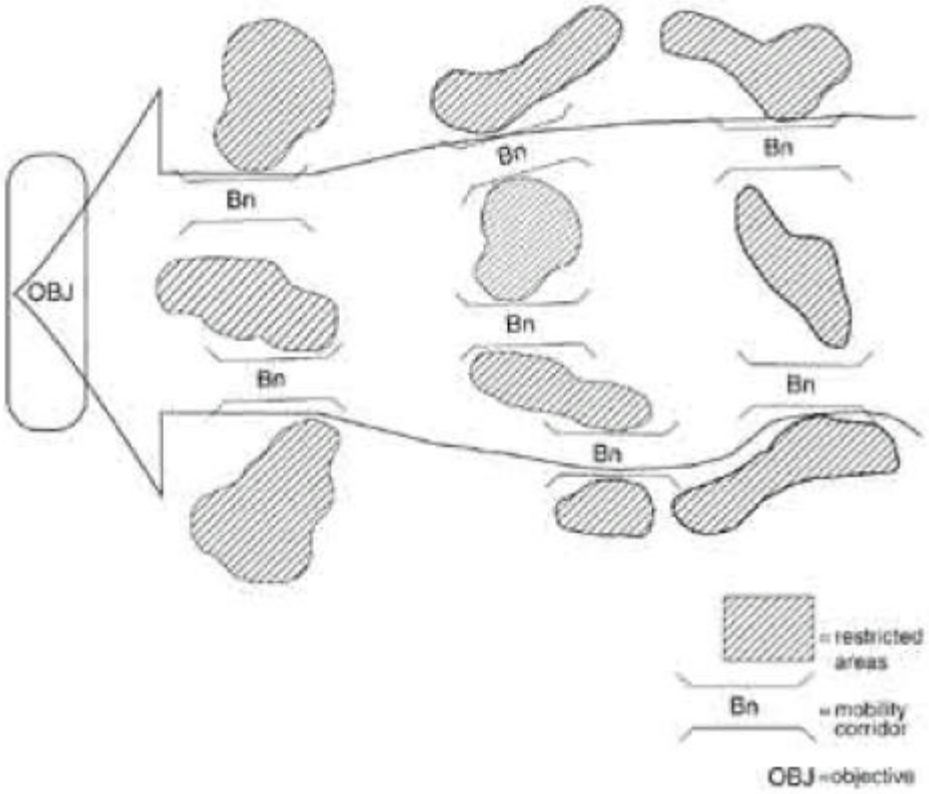


Figure 5-6. Mobility Corridors Grouped to Form an AA.

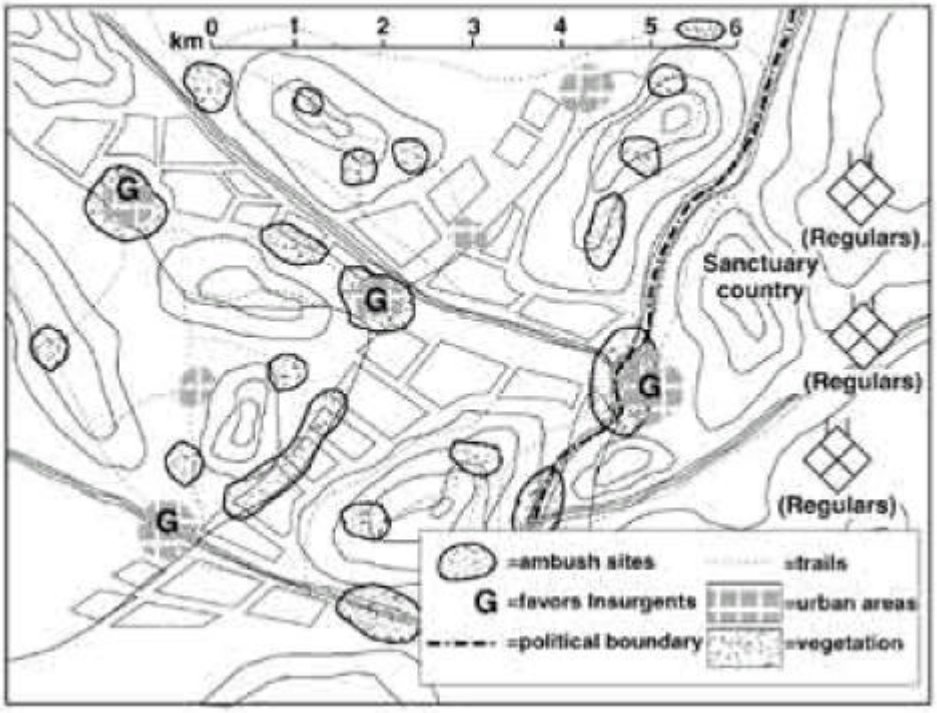


Figure 5-7. Lines of Communications and Likely Ambush Sites.

- Immediate or intermediate objectives—Terrain analysts identify any areas or terrain features that dominate AAs or assigned objective areas. These areas usually correspond to areas already identified as key terrain. As time permits, or situation requires, analysts also identify potential assembly and dispersal areas, observation posts, artillery and air defense positions, LZs, and DZs.

The terrain rarely favors one type of operation throughout the width, depth, and height of the battlespace. Based on the location and nature of the potential engagement areas and battle positions, analysts determine which areas of the battlespace favor attack or defend COAs.

Analysts consider all terrain factors in any order that best supports their analysis, but must focus on the factors most relevant to the specific situation and needs of the commander. To aid the commander's staff in the completion of their estimates and plans, analysts construct a combined obstacle overlay (COO) or a modified combined obstacle overlay (MCOO), which are graphic products that depict battlespace effects on military operations (see fig. 5-8).

Weather

Commanders can take advantage of the weather or minimize its effects through planning based on a weather analysis. During the weather analysis step, weather is studied to determine how it affects friendly and enemy capabilities to move, shoot, and communicate. Terrain and weather are inseparable factors of tactical intelligence and must be integrated. Weather forecasts and assessments contribute to intelligence and must be considered when commanders develop their COAs. The type and amount of weather support needed for a particular mission depends on the mission, the forces, the terrain, and the enemy.

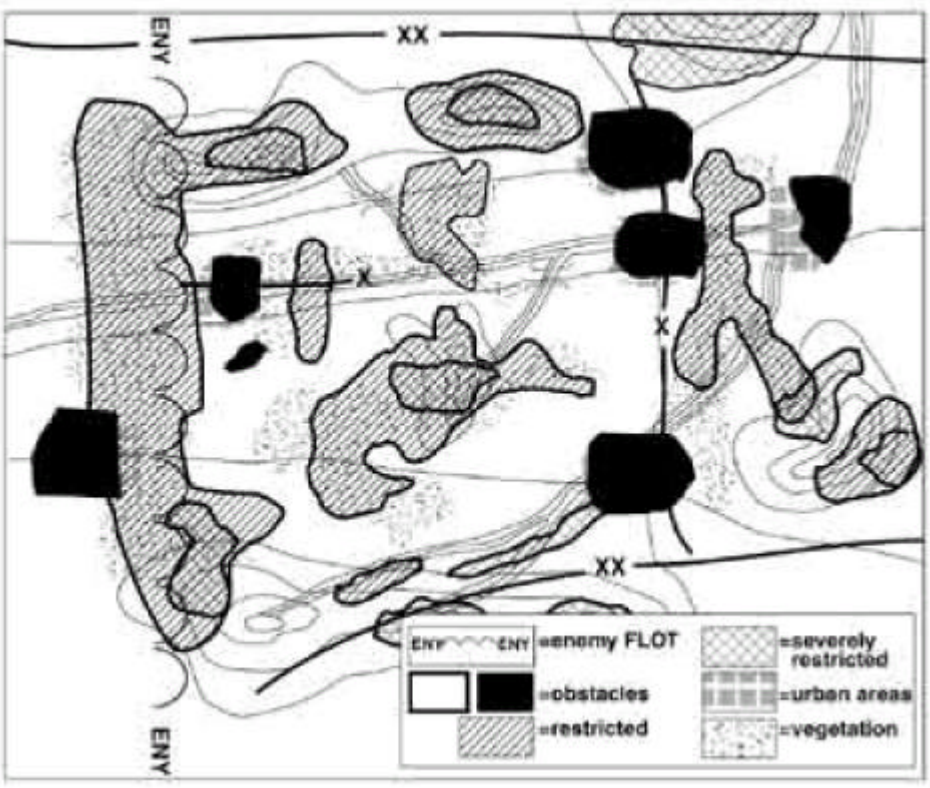


Figure 5-8. Combined Obstacle Overlay.

Evaluation of the direct effects of weather begins by establishing critical values for each aspect of the weather's effects on personnel, equipment (to include all sensors), and military operations the command may be required to perform. Unit intelligence officers and operations personnel develop detailed critical value tables for their units as part of the IPB process. These critical values are used to measure the effects of local weather on both friendly and enemy military operations. See appendix B for an example of a weather critical values table. Weather analysis is covered in more detail in chapter 6 and in Marine Corps Warfighting Publication (MCWP) 3-35.7, *MAGTF Meteorological and Oceanographic Support*. Weather analysis is accomplished by analyzing the military aspects of weather and evaluating the weather's effects on military operations.

Analyze the Military Aspects of Weather

Analysts consider the following five military aspects of weather:

- Temperature and humidity.
- Precipitation.
- Wind.
- Visibility.
- Clouds.

Evaluate the Weather's Effects on Military Operations

Weather has both direct and indirect effects on military operations. Examples of indirect effects include—

- Temperature inversions that might cause some battle positions to be at risk to the effects of chemical warfare.
- Local conditions of visibility, such as fog, that might make some potential engagement areas attractive.
- Hot, dry weather that might force a unit to consider water sources as key terrain.

Other Characteristics of the Battlespace

These characteristics include all aspects of the battlespace environment that affect friendly and threat COAs not incorporated into terrain and weather analysis. For example, an intelligence officer may report that religious considerations will make cordon and search operations on Wednesdays difficult to execute since the local population will be praying at the time of the scheduled search. Examples of other characteristics include—

- Logistic infrastructure (e.g., land use patterns, sources of potable water, bulk fuel storage, natural resources, industries and technologies, chemical and nuclear facilities).
- Population demographics (e.g., living conditions, cultural distinctions, religious beliefs, political grievances, political affiliation, education levels).
- Naval approaches.
- Economics.
- Local, regional, and international politics (e.g., treaties, agreements, legal restrictions, unofficial systems, gangs).

Although effects of other characteristics are usually discussed in text or matrix form, analysts should use graphics wherever possible. Examples of graphic depictions include an overlay showing areas most vulnerable to insurgent activity based on demographic distribution or an overlay showing high-value targets (HVTs) in the logistic infrastructure.

Describe the Battlespace Effects on Threat and Friendly Capabilities and Broad Courses of Action

Intelligence analysts combine the evaluation of the effects of terrain, weather, and other characteristics of the battlespace into one integrated product. They focus on the total environment's effects on COAs available to both friendly and threat forces.

Prior to development of friendly COAs, intelligence analysts provide the operations officer or planning staff with the following IPB products:

- An evaluated and prioritized set of AAs to assist in the designation of axis of advance, direction of attack, or zone of attack for each subordinate unit in offensive operations.
- Sets of defensible terrain along threat AAs to assist in the development of strongpoints, battle positions, or sectors for each subordinate unit in defensive and retrograde operations.
- Periods when weather conditions will optimize the use of friendly target acquisition and aviation operations to help time operations.

After the development of friendly COAs, intelligence analysts provide an evaluation of how each COA does or does not use the opportunities the battlespace provides. When addressing effects on threat COAs, intelligence analysts should view capabilities from the perspective of the enemy. The evaluation of the battlespace effects on the threat must be tailored to include weather and terrain that may affect threat weapon systems, vehicles, and personnel differently than friendly personnel. Operations and planning staffs must understand these battlespace effects on the threat to avoid assumptions that the battlespace will affect both forces equally. Other characteristics may influence threat actions more than weather and terrain, and cultural biases may cause threat personnel to view legal, political, economic, and demographic issues in an entirely different manner than friendly personnel would.

When describing the battlespace effects on threat and friendly capabilities and broad courses of action, intelligence analysts must—

- Evaluate the battlespace from the perspective of the threat.
- Express the evaluation in terms of COAs, not detailed descriptions of the analytical factors that led to the conclusions.
- Focus the commander by relating specific threat activities in both time and space.
- Back their conclusions with the detailed analysis performed.
- Communicate final conclusions in written reports such as the analysis of the AO or intelligence estimate.
- Disseminate graphic products developed during the analysis and evaluation to the staff and other commands for use in their own IPB and planning efforts.

SECTION III. STEP 3—EVALUATE THE THREAT

The third step in the IPB process is to determine the threat force capabilities and the doctrinal principles, tactics, techniques, and procedures it has historically used. This involves a detailed study of the threat's composition, tactical doctrine, procedures, weapons and equipment, and supporting systems. The intelligence section determines threat capabilities and how the threat operates by updating or creating threat models and identifying threat capabilities.

Update or Create Threat Models

Threat models depict how threat forces prefer to conduct operations under ideal conditions. They are based on the threat's normal or doctrinal organization, equipment, tactics, techniques, and procedures. Threat models result from a detailed study of the threat force. Ideally, threat models are constructed prior to deployment. Threat models consist of doctrinal templates, a description of preferred tactics and options, and identification of HVTs.

Doctrinal Templates

Doctrinal templates illustrate the deployment pattern and disposition preferred by the threat's normal tactics when not constrained by the effects of the battlespace environment. They are usually scaled graphic depictions of threat dispositions for a particular type of standard operation, such as a battalion moving to contact or an insurgent ambush (see fig. 5-9).

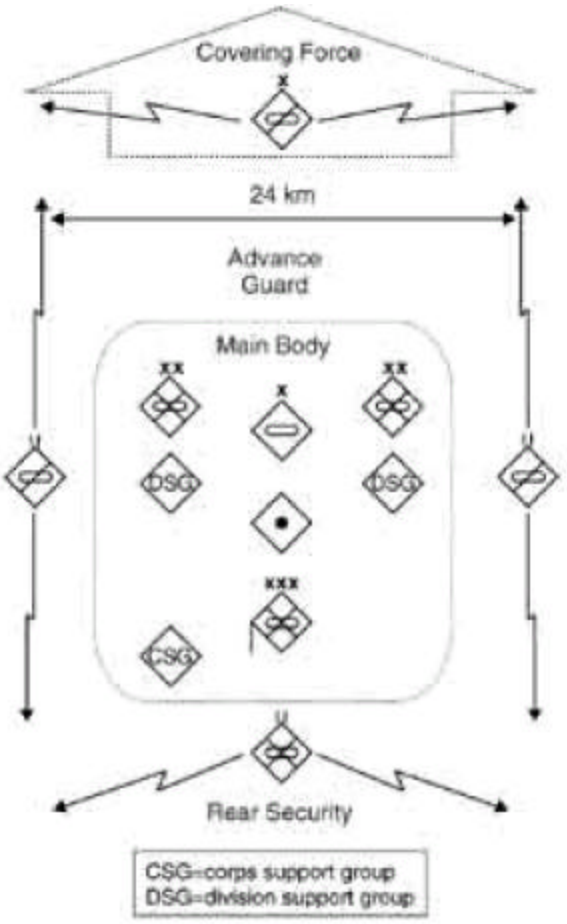


Figure 5-9. Doctrinal Template.

Doctrinal templates must be tailored to the needs of the unit or staff section creating them. Templates are constructed through an analysis of intelligence data bases and an evaluation of the threat's past operations. The analysis should focus on patterns in task organization, timing, distances, relative locations, groupings, and the use of terrain and weather. Some doctrinal templates consider the threat force as a whole, while others focus on a single battlefield function like intelligence or fires.

Description of Tactics and Options

The threat model includes a description of the threat's preferred tactics. It addresses the operations of the major units or elements portrayed on the template and the activities of different battlefield functions. It also contains a listing or description of the options (branches) available to the threat should the operation fail, or subsequent operations (sequels) if it succeeds. Even if the threat's preferred tactics can be depicted graphically, the threat model includes a description.

The description aids in mentally wargaming the operation over its duration during the development of threat COAs and situation templates. It should address typical time lines and phases of the operation, points where units transition from one formation to another, decision criteria, and each battlefield function's contribution to the operation's success. This analysis of the individual role of battlefield functions, related in time and space, will aid in the later identification of HVTs and HPTs.

Identification of Center(s) of Gravity

Marine Corps Doctrinal Publication (MCDP) 1, *Warfighting*, defines a center of gravity (COG) as any important source of strength. It may be mental, moral or physical strength, power or will. COGs may exist at each level of war: strategic, operational, and tactical. It may be tangible or intangible, and there may be multiple COGs. While knowledge of a threat's COGs at all levels is useful, the analyst should focus on the COGs appropriate to the level of operations that concern their friendly force. At this stage of the IPB process, the identification of COGs is an initial assessment.

Critical Vulnerabilities

Aspects of a COG that, if exploited, will do the most significant damage to an adversary's ability to resist are critical vulnerabilities. Vulnerability cannot be critical unless it undermines a key strength. Some vulnerabilities may contribute significantly to the enemy's downfall while others may lead only to minimal gains. Therefore, analysts must focus on a vulnerability that will do the most damage to the enemy's ability to resist.

Identification of Type High-Value Targets

Assets that the threat commander requires for the successful completion of the mission depicted and described on the template are HVTs. Examples of type HVTs include C2, intelligence, fire support, communications and information systems, air defenses, engineers, and logistics and CSS. When evaluating the threat, intelligence analysts must—

- Identify HVTs from an evaluation of the data base, the doctrinal template, the template's supporting narrative, and the use of tactical judgment.
- Develop the initial list of HVTs by mentally wargaming and thinking through the operation to identify assets that are critical to the operation's success, particularly at critical junctures or phases.
- Identify assets, which are key to executing the primary operation, particularly those that are key to satisfying decision criteria.
- Group the identified key assets into one of 13 categories used to develop target sets, thus assisting in the development of targeting strategies.
- Determine how the threat might react to the loss of an HVT; consider his ability to substitute other assets or modify his plan to compensate.
- Rank the identified HVTs with regard to their worth to the threat's operation.
- Identify HVT value changes by phase because that value usually varies over the course of an operation.
- Tailor IPB products to the command's needs by concentrating on HVTs that are important to the mission.

Identify Threat Capabilities

Threat capabilities are the broad COAs and supporting operations that the threat can take to influence the accomplishment of the friendly mission. The following four tactical or broad COAs are generally open to military forces in conventional operations:

- Attack.
- Defend.
- Reinforce.
- Retrograde.

Each of these broad COAs can be divided into more specific COAs. An attack may be envelopment, penetration, or other variations of an attack. A retrograde movement may be a delaying action, a withdrawal, or a retirement. Other threat capabilities include support to

broad COAs or specific types of operations, including—

- Deception operations.
- Riverine operations.
- Psychological operations.
- Intelligence operations.
- Nuclear, biological, and chemical weapons employment.
- Espionage, sabotage, subversive, and terrorist operations.

Threat capabilities take the form of statements, such as—

- The enemy has the ability to insert up to two infantry battalions in a single lift operation.
- The enemy can establish a prepared defense by 14 May.
- The demonstrators can effectively block traffic at up to seven intersections in our zone.

When identifying threat capabilities, intelligence analysts—

- Start with developed threat models.
- Consider other types of operations and broad COAs at other levels of war and during operations other than war.
- Consider the threat's ability to conduct each operation based on all factors related to the current situation. (The threat may be understrength in equipment or personnel, short of logistic support, lacking air support, or his troops may be inexperienced or poorly trained.)

SECTION IV. STEP 4—DETERMINE THREAT COURSES OF ACTION

This step of the IPB process is the identification and development of likely threat COAs that will influence the accomplishment of the friendly mission.

Identify the Threat's Likely Objectives and Desired End State

Depending on METT-T, intelligence analysts generally start identifying threat objectives and desired end state of the threat command at least one level above their own command. Analysts repeat the process for the next subordinate level to at least two levels below their own command, ensuring that each threat level's objective will accomplish the likely objectives and desired end state of its parent command. In operations other than war, analysts may be required to start more than one level above their command (e.g., the government or major clan leadership level). Usually, analysts state the threat's objectives and desired end state as assumptions. The analysts must make sure the assumptions are clearly identified as such and ensure the assumptions are discussed with the commander and staff. During operations other than war, analysts must consider more than the conventional objectives of terrain or friendly forces. This is also true at higher levels of command where the threat's political and economic objectives have a direct influence on his COAs.

Identify the Full Set of Courses of Action Available to the Threat

When identifying the COAs available to the threat, analysts must—

- Consider the COAs that the threat historical doctrine and tactics, techniques, and procedures (TTP) indicate are appropriate to the current situation and the likely objectives identified. This requires an understanding of the threat's decisionmaking process as well as

an appreciation for how he perceives the current situation.

- Consider the threat COAs that could significantly influence the command's mission, even if the threat's doctrine and TTP indicate these as infeasible under current conditions; and consider any indirect COAs that the threat is capable of executing.
- Consider the threat COAs indicated by recent activities and events. To avoid surprise from an unanticipated COA, consider all possible explanations for the threat's activity in terms of possible COAs.
- Consider each COA's subset independently to avoid forming biases that restrict the analysis and evaluation.
- Combine the subsets to eliminate redundancy and minor variations.
- Compare the consolidated list of COAs to threat capabilities identified in step 3 of the IPB process and eliminate any COAs that the threat is incapable of executing.
- Select threat models that will accomplish the threat's likely objectives based on the evaluation of the threat's capabilities.
- Examine how the effects of the battlespace described in step 2 of the IPB process influence the application of COAs (see fig. 5-10).
- Define COAs open to the threat, such as deliberate attack, hasty attack, defend, and delay.
- Define each general COA as a set of specific COAs by integrating the threat models with a description of the battlespace effects.

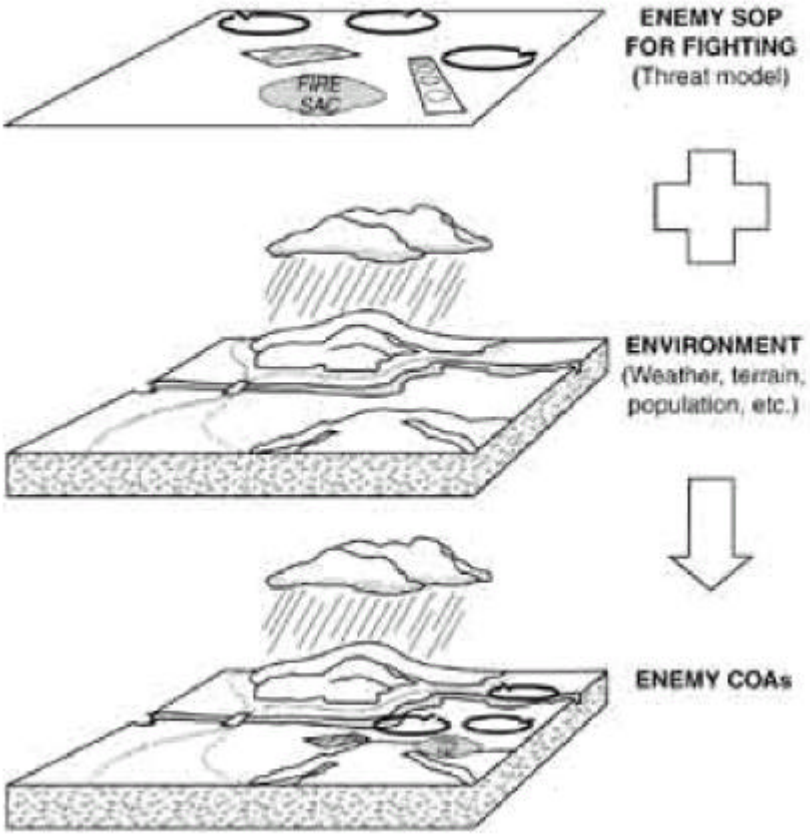


Figure 5-10. Combining Doctrine and Battlespace Effects to Develop Threat COAs.

- **Ensure each COA identified is suitable, feasible, acceptable, unique, and consistent with threat doctrine or TTP and recently observed activities and patterns (see figs. 5-11 and 5-12).**

Evaluate and Prioritize Each Course of Action

Analysts must evaluate each identified threat COA and prioritize it according to an estimate

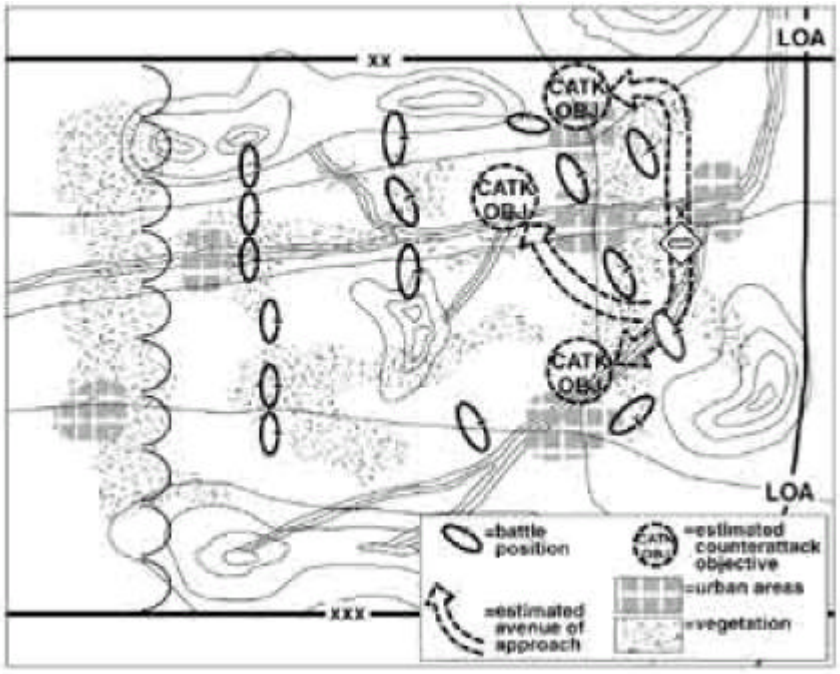


Figure 5-11. Enemy COA 1—Counterattack.

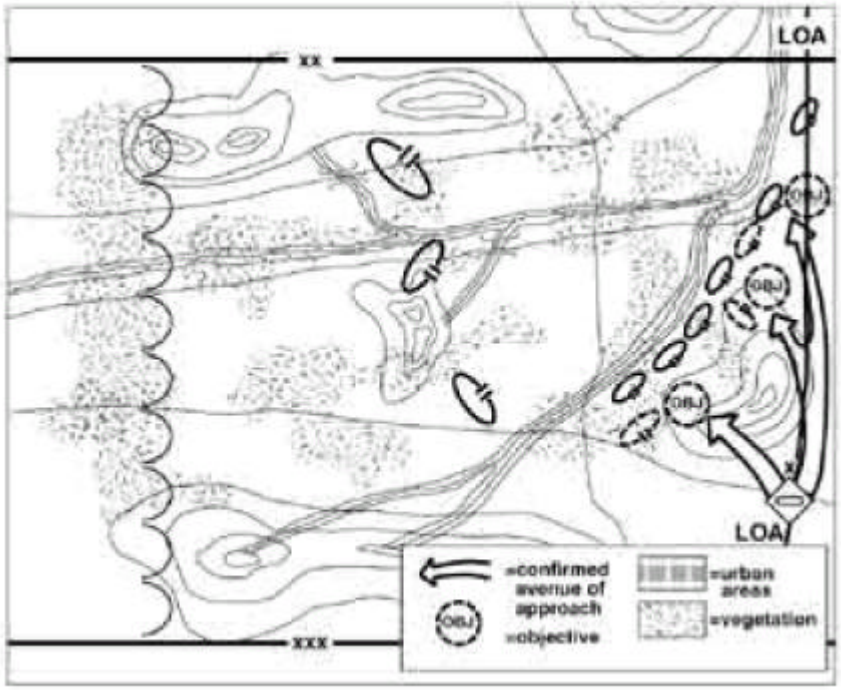


Figure 5-12. Enemy COA 2—Withdrawal from Current

of likely adoption by the threat. The priority list allows the commander and staff to develop a plan for friendly COAs that is based on assumptions about the threat. Once the commander selects a friendly COA, the list may need to be reprioritized to reflect possible reactions to friendly dispositions and activities.

Develop Each Threat Course of Action in the Amount of Detail Time Allows

Once the complete set of threat COAs has been identified, analysts develop each COA in as much detail as the situation requires and time allows. The order in which each COA is developed is based on its probability of adoption and the commander's guidance. To ensure completeness, each COA must answer the following five questions:

- What (type of operation)?
- When (time the action will begin)?
- Where (sectors, zones, axis of attack)?
- How (method by which the threat will employ his assets)?
- Why (objective or end state of the threat)?

When developing each COA, analysts must consider threat forces at least one level above their own command level. For example, a battalion S-2 would consider the COAs available to threat regiments and brigades. This helps account for possible reinforcing forces and the higher threat command's objectives and intent. Generally, analysts consider threat COAs two levels of command below their own command when the MAGTF is in the offense and at least one level below their command when the MAGTF is in the defense. Thus the previously discussed battalion S-2 would depict missions and actions down to the platoon level.

Each developed threat COA has a situation template; a COA description, COGs, critical vulnerabilities, and options; and a listing of HVTs.

Situation Template

Situation templates are graphic depictions of expected threat COAs (see fig. 5-13). Templates usually depict the most critical point in the operation as agreed upon by the G-2/S-2 and G-3/S-3. An analyst may prepare several templates to illustrate different points of time in an operation, starting with the threat's initial array of forces. These templates are useful in depicting points where the threat may adopt branches or sequels to the main COA, places where the threat is especially vulnerable, or other key points in the battle such as initial contact with friendly forces. Situation templates are used to support staff wargaming and to develop event templates. Analysts construct a situation template by—

- Beginning with the threat model representing the operation under consideration.
- Overlaying the doctrinal template on the products (generally, COO or MCOO) that depict the battlespace environment's effects on operations.
- Adjusting the dispositions portrayed on the doctrinal template based on the battlespace environment's effects.
- Viewing the situation from the threat commander's point of view when selecting from among available options.
- Checking the situation template to ensure that all the threat's major assets have been accounted for, particularly the locations and activities of the HVTs listed in the threat model.
- Evaluating time and space factors to develop time phase lines (TPLs) to depict threat movement. The TPLs can be refined during wargaming (see fig. 5-13).

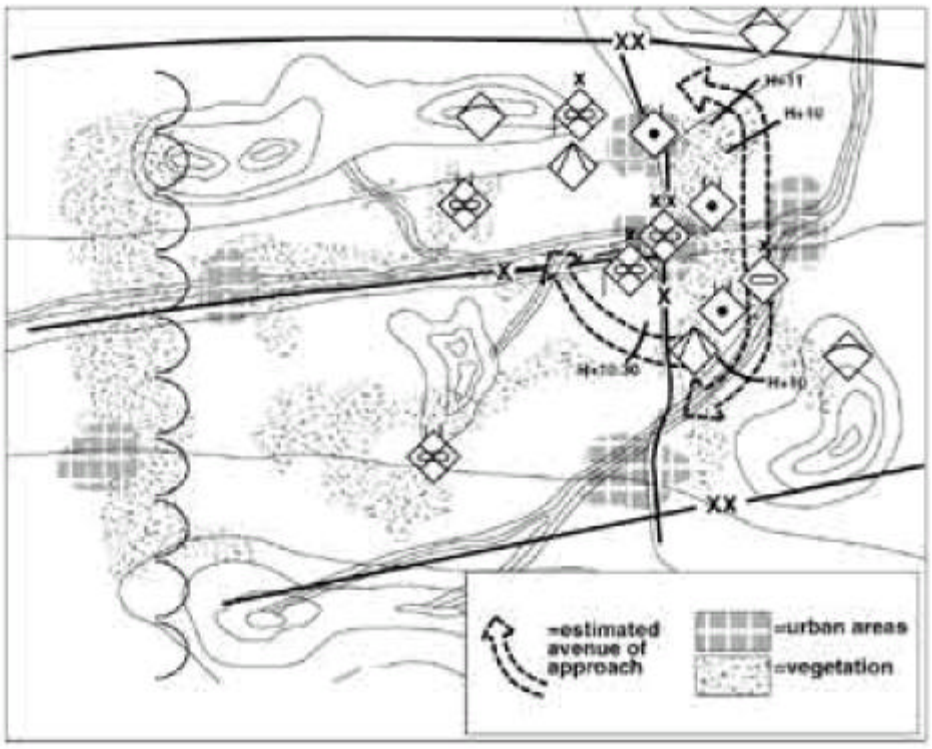


Figure 5-13. Counterattack Situation Template with TPLs and HVTs.

Description of the Threat's Courses of Action and Options

This is a description of the forces' activities depicted on the situation template. It can range from a narrative description or a combined graphics overlay or text matrix (see fig. 5-14 on page 5-20) to a detailed intelligence synchronization matrix depicting the activities of each threat unit and battlespace function in detail (see fig. 5-15 on page 5-20). The COA description supports staff wargaming and the development of the event template and supporting indicators. When preparing the description, analysts mentally war game the COA and attempt to tie threat actions and decisions to both time and space. The description should address the—

- Earliest time the COA can be executed.
- Threat COGs.
- Time lines and phases associated with the COA.
- Decisions the threat commander will make during and after execution of the COA.

Intelligence synchronization is more than simply ensuring that collection systems are operating 24 hours a day. The G-2/S-2 must plan and direct the intelligence system, receive the information it produces, process it, and then produce and disseminate intelligence of value to commanders and planners in time to support their decisions. The coordination of this entire cycle is intelligence synchronization. The IPB process provides the products and tools the G-2/S-2 needs to quickly evaluate incoming information and intelligence as it relates to the command's IPRs and IRs, intelligence synchronization matrix, and the decision support template (DST). These products and tools support the commander's decisions during COA execution and help the commander to quickly confirm or deny the assumptions used during COA wargaming. During operations, the commander and staff track the DST and the intelligence synchronization matrix against incoming intelligence and other tactical reports. As the commander and staff near each decision point, they look to the G-2/S-2 for the intelligence that supports that decision.

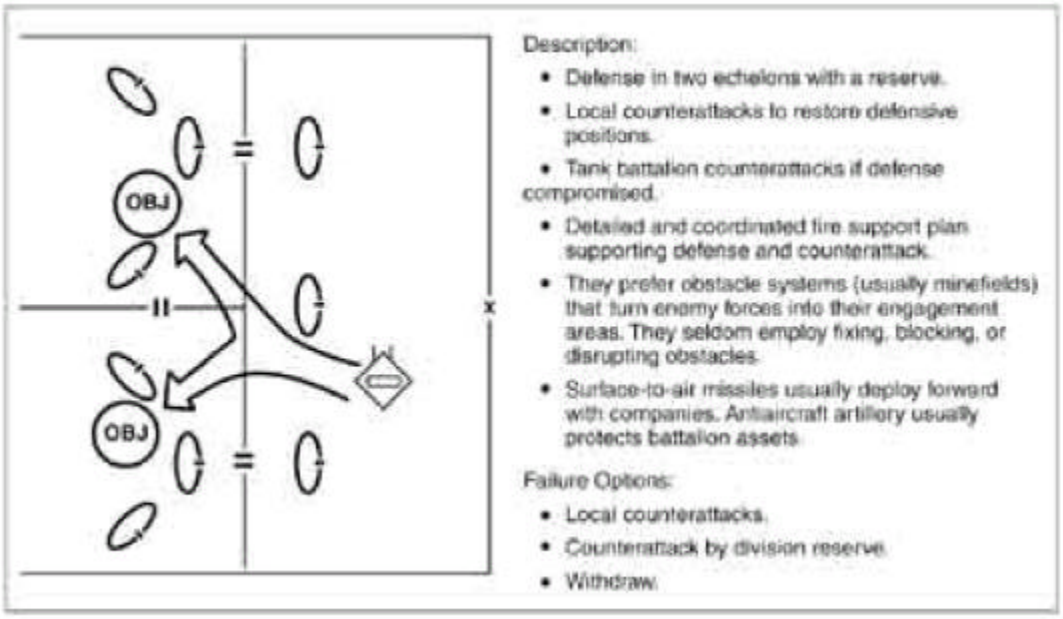


Figure 5-14. Threat COA Overlay with Text Description.

TIME	T + 10	T + 24	T + 36	T + 48
Friendly Event	penetrate 80th Corps	shape 90th Corps	shape 90th Corps	shape reserve
Threat Event		reserve departs assembly areas	reserve deploys combat formation	Corps artillery forward deploys
Decision Points	shift main effort to aviation combat element		shift shaping actions	
Intelligence Event (PIR)	NAI 24-will the reserve reinforce 90th Corps	NAI 1-identify reserve HVT AA	NAI 2-identify reserve HVT locations	NAI 3-identify Corps artillery refueler locations
Intel and Recon Collectors	JSTARS Force Recon Rivet Joint UAV/ATARS Radio Battalion Ground Sensors	JSTARS	Force Recon Senior Scout UAV/ATARS	JSTARS Force Recon

Figure 5-15. Intelligence Synchronization Matrix.

Sometimes a battle progresses in a direction unanticipated during the initial IPB and wargaming, because the enemy follows his own plans and time lines. As the operation unfolds and the enemy's intentions become clearer, key staff members reinitiate the IPB and decision-making processes and conduct a modified war game as needed. During these sessions, the G-2/S-2 reviews and modifies the initial IPB. The battle staff then war games the best friendly response or preemptive action based on the updated set of IPB predictions. New decisions and COAs lead to updating and refining the collection plan, intelligence synchronization, and new decision support tools.

The intelligence synchronization matrix and other intelligence tools are consolidated and displayed within the current operations center to provide all watch leaders and personnel with critical current intelligence operations information. This tool is called the intelligence synchronization sheet, which is tailored to the command echelon or C2 node being supported (see fig. 5-16). Generally, the intelligence synchronization sheet includes lists of—

- Threat objectives and battlespace conditions.
- Current PIRs.
- Anticipated critical threat events, critical intelligence actions, and likely threat activities.
- Targeting priorities.
- Intelligence support priorities.
- Key intelligence collections, production, and dissemination activities.

High-Value Targets

While preparing and mentally wargaming the situation template, the analyst notes how enemy systems provide critical support to the COA. This

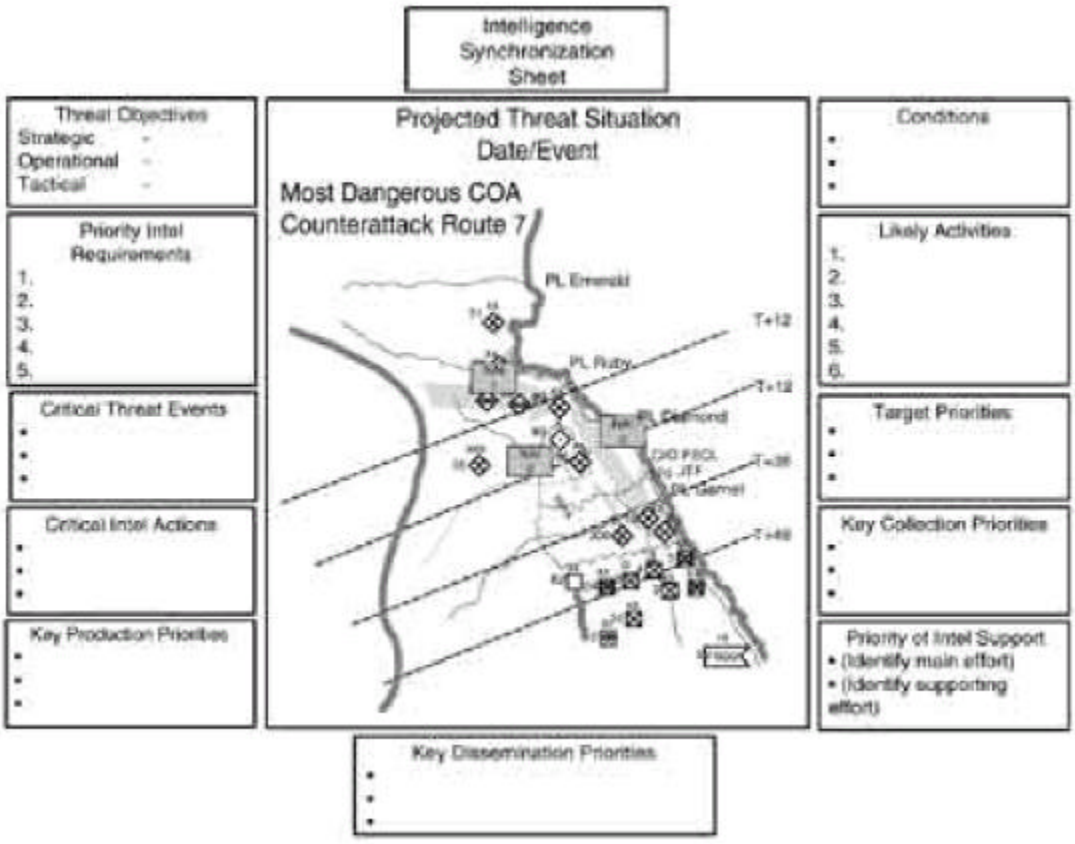


Figure 5-16. Intelligence Synchronization Sheet.

exercise leads to identification of HVTs that may be COGs, critical vulnerabilities, or assets, which if destroyed or neutralized may allow friendly forces to attack a COG or critical vulnerability. Once the HVTs list is compiled, analysts—

- Use the list in the threat model as a guide.
- Determine the effect on the COA of losing each HVT and identify likely threat responses.
- Identify the times or phases in the COA when the target is most valuable to the threat commander and make the appropriate notations on the list of HVTs.
- Transfer the refined and updated list of HVTs to the situation template (see fig. 5-17). The list will support staff wargaming and the targeting process.
- Note on the situation template any areas where HVTs must appear or be employed to make the operation successful.
- Focus on HVT locations at the times they are most valuable or just before. These are potential targeted areas of interest (TAI) and engagement areas that will be refined and used by the G-3/S-3.

Identify Initial Intelligence Collection, Production, and Dissemination Requirements

After identifying potential threat COAs, the analyst must determine which one the enemy will adopt. Initial collection requirements are designed to help answer the challenge. The identification of initial ICRs revolves around predicting specific areas and activities, which, when observed, will reveal which COAs the threat has chosen. The area where the analyst expects key events to occur is designated an NAI. The activities that reveal the selected COA are called indicators. Identified IPRs support prioritization and planning of necessary intelligence products, and identified IDRs support prioritization and planning for the eventual

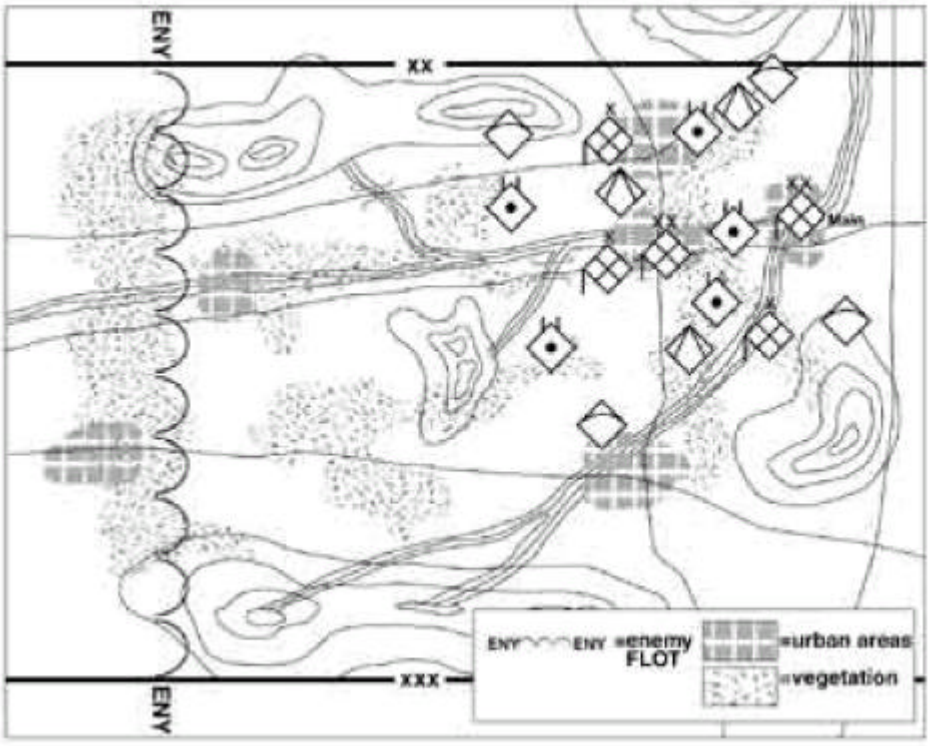


Figure 5-17. Templated Locations of HVTs for Enemy COA 1.

dissemination of intelligence products, such as the event template and event matrix, to commanders and staff sections needing them.

The event template and matrix form the basis for planning integrated collection, production, and dissemination strategies, and synchronize friendly intelligence operations. They enable the G-2/S-2 to develop precise ICRs, IPRs, and IDRs by maximizing the effectiveness of limited resources over extended areas against a vast array of threat targets.

Event Template

The differences between the NAIs, indicators, and TPLs associated with each threat COA form the basis of the event template (see fig. 5-18). The event template is a guide for collection, reconnaissance, and surveillance planning. It depicts where to collect information that will indicate which COA the threat has adopted.

Analysts evaluate each threat COA to identify its associated NAIs. They mentally war game execution of the COA and note places where activity must occur if that COA is adopted. Intelligence analysts must pay particular attention to times and places where the threat's HVTs are employed or areas where HVTs can be easily acquired and engaged. Analysts must also consider places where the threat is expected to take actions or make decisions, such as adoption of a branch plan or execution of a counterattack. These areas will evolve into NAIs in support of targeting.

An NAI can be a specific point, a route, or an area. They can match obvious natural terrain features or arbitrary features, such as TPLs or engagement areas. Analysts must make the NAIs large enough to encompass the activity that serves as the indicator of the threat's COA.

Intelligence analysts compare, contrast, and identify the differences between each COA's NAIs

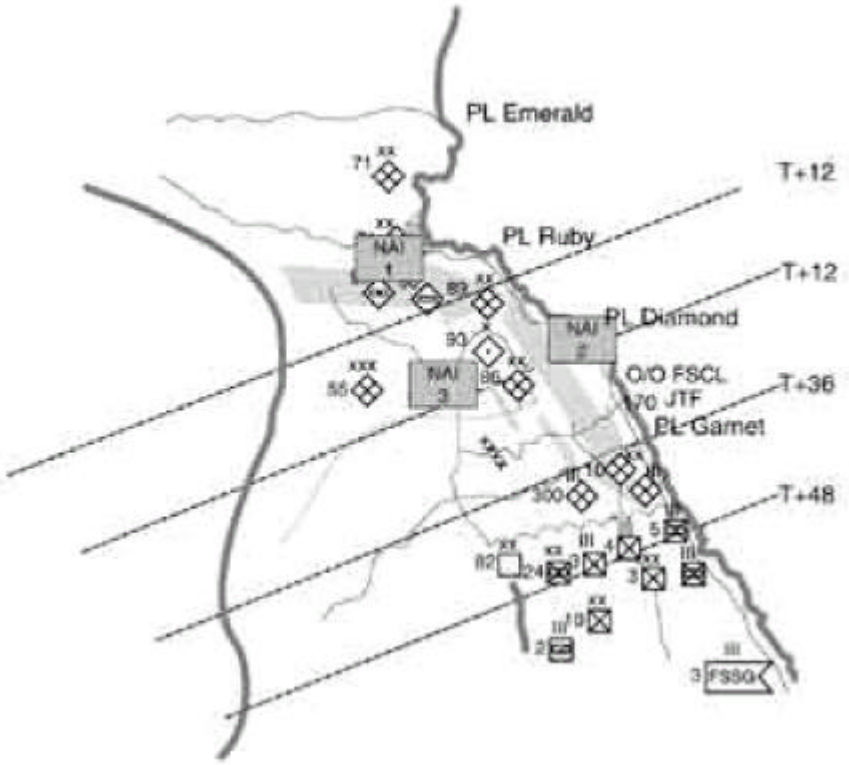


Figure 5-18. Event Template.

and indicators, concentrating on the differences that will provide the reliable indications of COA adoption. Selected NAIs are marked on the event template. The initial event template focuses on identifying which of the predicted COAs the threat has adopted. Analysts update and refine the event template and its supporting matrix to support friendly decisions identified during staff wargaming (see fig. 5-19).

Event Matrix

The event matrix supports the event template by providing details on the type of activity expected in each NAI, the times the NAI is expected to be active, and the relationship of the activity to other events on the battlefield. Primarily used in planning intelligence collection, the event matrix also serves as an aid to situation development (see fig. 5-20).

When preparing the event matrix, intelligence analysts—

- Examine the events associated with each NAI on the event template and restate them in the form of indicators.
- Enter the indicators along with the times the indicators are most likely to occur by using TPLs from the situation template or the description of the COA to establish the expected times.
- Record the latest-time-information-of-value time line, if available, based on the expected flow of events, as a guide for the collection manager.

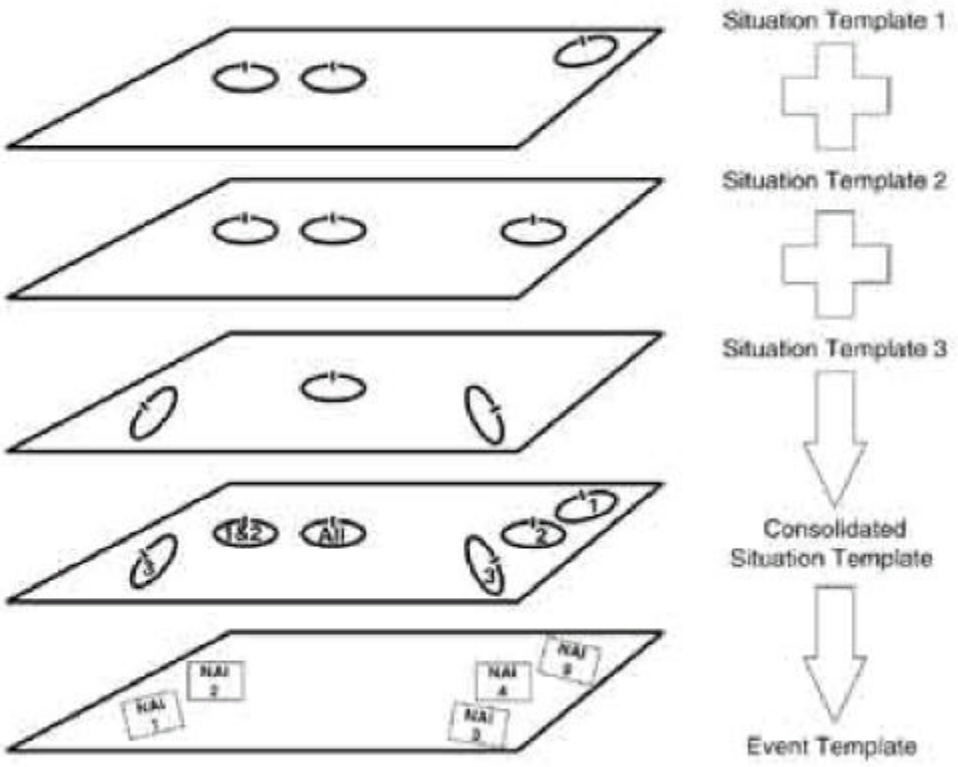


Figure 5-19. Event Template Development by Comparing and Contrasting Each COA's NAIs and Indicators.

NAI	Estimated Time	COA Indicators	COA 2 Indicators	COA 3 Indicators	Other COA Indicators
1	H-15		air assault forces		
2	H-15		air assault forces		
3	H-15	air assault forces		air assault forces	
4	H-15		infiltration of light infantry		
5	H-4		light infantry attack		
6	H-4	light infantry attack NAI 7	light infantry attack		
7	H-4	light infantry attack NAI 8		light infantry attack	
8	H-4	poised to attack		light infantry attack	
9	H-4	poised to attack	poised to attack		tank division attacks
10	H-4		poised to attack	poised to attack abreast	tank division attacks
11	H-6			shifts north	
12	H-18				
13	H-18				1 or 2 brigades attack south

Figure 5-20. Detailed Event Matrix for a Specific NAI.

SECTION V. DECISION SUPPORT TEMPLATE

The DST is the capstone product in the staff planning process and the logical conclusion to IPB, although it is not part of the formal IPB process. The DST relates time, space, and threat actions to assist the commander in determining when decisions need to be made, either to employ fires or maneuver forces (see fig. 5-21 on page 5-26). This template helps the commander think ahead in the battle to reduce uncertainty and aids in recognitive or intuitive decisionmaking.

The DST is normally developed during COA wargaming as threat and friendly actions are compared in time and space. Unlike the previous products, the DST is a staff product prepared under the staff cognizance of the G-3/S-3. It reflects the judgment and expertise of the intelligence, maneuver, fires, CIS, and logistic support staffs. The threat COA models, the event template, and event matrix developed during IPB form the basis for and drive wargaming and development of the DST.

Targeted Areas of Interest

Through event templating, identification is made of those areas on the battlefield where significant events and activities will likely occur and where targets will likely appear. As the wargaming process proceeds, the staff identifies areas where the commander can influence the action through fire and maneuver. These areas are designated TAIs. A TAI is an engagement point or area, usually along a mobility corridor, where the interdiction of threat forces by fires, maneuver, or jamming will deprive or reduce a threat capability. It can also cause the threat commander to abandon a particular COA or require the use of unusual support to continue operations. Times and

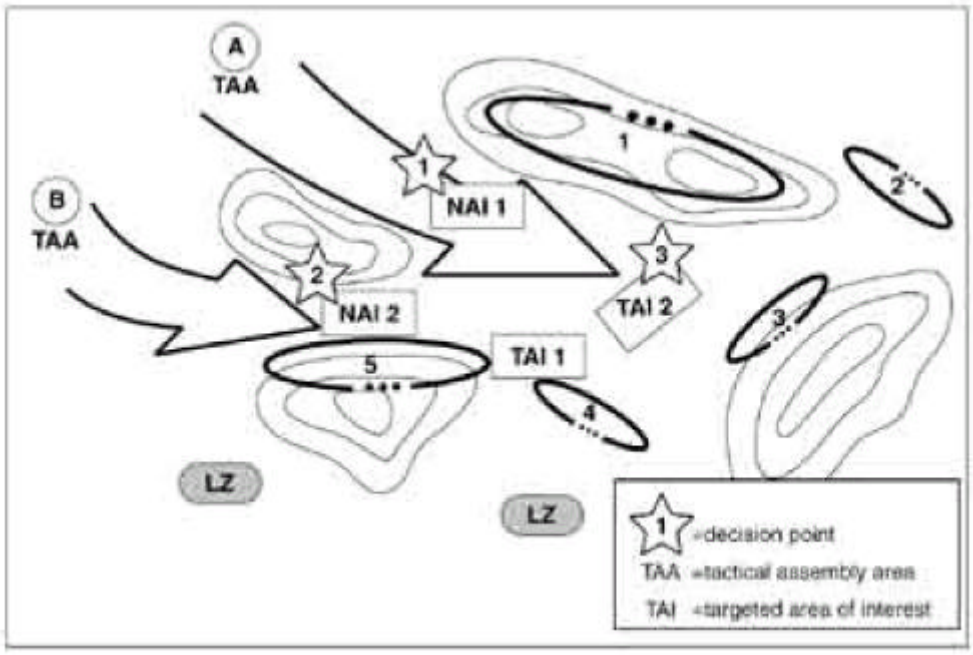


Figure 5-21. Decision Support Template.

locations where HVTs will appear are particularly suited to become TAIs.

The identification of TAIs is a joint effort between the intelligence, operations, and fire support staffs. The intelligence staff identifies the times and places where opportunities present themselves and the effect of interdiction on threat capabilities. The operations and fire support staffs consider the availability of interdiction resources, the effects of interdiction on the accomplishment of the friendly mission, and the priorities for the use of available resources.

Decision Points

Following the selection of TAIs, analysts identify decision points. The location of decision points is largely influenced by the availability and capability of friendly fire and maneuver systems; therefore, decision point selection is primarily a G-3/S-3 function, with support from the fire support coordinator and other key participants in the planning staff.

Types

Decision points identify battlefield events that may require tactical decisions. These points also identify when the tactical decisions must be made for the commander to retain available options. Examples of the types of decisions include—

- Commit the reserve.
- Surge friendly air support.
- Concentrate artillery on TAIs, perhaps in conjunction with electronic attack (EA) operations.
- Deliver scatterable mines.
- Shift the main effort.
- Commence the next phase of an operation.
- Change subordinate unit's overall mission.
- Request assistance from higher headquarters.

Considerations

Decisions must be made early enough to ensure that they can be coordinated across all command echelons and implemented in time to achieve the desired results. The developed NAIs must

provide the required indicators in sufficient time and preciseness to ensure timely decisions.

When identifying decision points, the G-3/S-3 must consider the—

- Time required for intelligence collection, processing, analysis, production, and dissemination to take place.
- Time required to prepare and/or move friendly assets that will execute the mission.
- Activities and movements of the target or threat during the time elapsed between decision and execution.

As the wargaming progresses, a recorder tracks decision points, both by time and location, and develops the synchronization matrix to ensure all battlespace functions are working in harmony toward the same goals. After the commander selects a friendly COA, the intelligence staff develops detailed collection and dissemination plans to support the decision points, NAIs, and TAIs.

SECTION VI. ABBREVIATED INTELLIGENCE PREPARATION OF THE BATTLESPACE PROCESS

Many of the steps involved in IPB are time, labor, and resource intensive, especially at lower tactical echelons where automated systems and personnel support for terrain analysis and other intelligence production functions are usually not available. Those same echelons generally have less time available for the IPB process. Besides the available time, intelligence personnel and resource constraints affect the scope and depth of IPB activities. Consequently, most Marine Corps units use the abbreviated IPB process.

The intelligence product that results from the abbreviated approach is far less than the comprehensive set of previously discussed products. The one-overlay product, when developed to a quality standard and focused on the unit's mission, PIRs, and IRs, has repeatedly proven to be effective on the battlefield. In its most elementary form, the IPB process can be abbreviated by working ahead, focusing on essentials, staying objective oriented, and minimizing essentials.

Work Ahead

When conducting an abbreviated IPB, intelligence personnel should complete as much work ahead of time as possible by—

- Establishing a series of base products, particularly those that deal with the battlespace environment's effects on operations.
- Keeping the products updated by periodic review instead of waiting until receipt of a new mission.
- Updating data bases on potential threats and changing the threat models as intelligence is received that indicates changes or evolution in threat doctrine.
- Conducting periodic reviews to ensure that the base IPB products, such as descriptions of the battlespace environment and the threat, are updated regularly.

- Becoming familiar with the support available from higher headquarters, theater intelligence centers, and Service agencies; knowing how to get needed information and products.
- Submitting PRs for information and intelligence products on areas where the unit is most likely to be employed.
- Developing checklists on how to get support, before, during, and after deployment.
- Maintaining an awareness of plans and priorities for all ICRs, IPRs, and IDRs submitted to higher headquarters.

Focus on Essentials

When starting the IPB effort, intelligence personnel should focus on essentials by—

- Considering the METT-T factors, particularly the factor of time.
- Determining how much time can be devoted to each step of the IPB process, and ensuring that the time line allows for the proper support of the planning and decisionmaking process.
- Deciding which products will be developed and to what degree of detail, and focusing on products most important to the mission.
- Identifying the full range of available threat COAs, rather than fully developing one threat COA at the expense of the others; determining the degree of detail required; and then developing all threat COAs to that level of detail.
- Working in a priority order established by the commander's intent and needs, and developing in detail only those COAs the commander has specified.

Stay Objective Oriented

The objective of IPB is to help the commander and staff make decisions and develop the best possible plans in the time available. This requires models of viable threat COAs that will influence mission accomplishment. Supporting the finished plan with intelligence requires a good event template and matrix.

Minimize Essentials

When minimizing essentials, intelligence personnel can get by with a good set of threat models and a good event template and matrix. They can also save time and materials by—

- Combining threat COA model templates and the event template on a single map overlay or using cartoons and sketches as a map substitute.
- Working directly from the map or sketch of major terrain features if the battlespace environment's effects have not been described.
- Identifying the set of threat COAs and briefly comparing them to determine which is most likely and which is most dangerous based on the current situation and the command's mission; and ranking the remaining threat COAs in order of likely adoption.
- Developing the most dangerous and most likely threat COA, and in the absence of guidance from the commander or G-3/S-3, using judgment in deciding which COA to develop first.
- Constructing an event template that focuses on identifying which of the two COAs the threat adopted, developing the remaining COAs, and working each COA in priority order.
- Incorporating each COA's NAIs in the event template as each threat COA is finished.
- Developing the second most likely or second most dangerous threat COA if the most likely COA is also the most dangerous COA, and ensuring at least two COAs are war gamed.
- Waiting until the staff conducts wargaming before structuring the ICRs.

Output

Throughout the IPB process, various products such as the threat models, threat COA graphics, and the event template are produced to support staff planning. The graphics developed, particularly the weather and terrain effects graphics, the situational templates, and the event template, can be disseminated to assist subordinate units in their own planning. Done correctly, these graphics can provide tremendous volumes of understanding and knowledge in concise and easily usable forms. At other times, however, additional written products can and should be prepared. The two products discussed below are the most commonly used, and both are directly derived from the IPB process.

Intelligence Estimate

In order to facilitate staff planning, the G-2/S-2 prepares the intelligence estimate before the remainder of the staff complete their own estimates. The intelligence estimate is the standard means of conveying key basic and current intelligence and relating it to the operational mission. It is a snapshot in time and forms the basis for the facts and assumptions of the decision-making process, driving the other staff estimates and the remaining steps of the Marine Corps Planning Process.

At higher command levels, the intelligence estimate provides major portions of the commander's written estimate. The products of IPB are the basis for the intelligence estimate. If the G-2/S-2 lacks the time required to prepare a written estimate, usually graphics that depict the results of the IPB evaluations and analysis are used as a substitute. A detailed outline for the intelligence estimate format is provided in appendix A.

Target and Objective Studies

The IPB impacts development through the evaluation of terrain and weather and the association of threat forces at specific times and locations within the battlespace. Situation, event, and decision support templates identify NAIs. Once identified, NAIs can then confirm or deny a threat's activities or adoption of a particular COA. Decision points and TAIs are also identified, requiring key intelligence that supports either fire or maneuver. From the IPB and wargaming processes, HVTs and HPTs are derived. Target and objective studies are focused, detailed intelligence products that aid in the application of fires or the maneuver of forces against a specific target set or area. Small units, such as MEU(SOC)s, can also use these studies for mission preparation and execution. See chapter 8 for a detailed discussion of target development.

CHAPTER 6. ANALYSIS OF THE BATTLESPACE

Analysis of the battlespace is a comprehensive study to determine the characteristics and effects of weather, oceanographic, and terrain environmental factors on enemy and friendly operations throughout the commander's AO and AOI. The battlespace analysis serves as a basis for developing specific friendly COAs and for determining enemy capabilities and COAs. This analysis allows the commander and staff to—

- **See the battlespace in both spatial (width, depth, height or airspace) and temporal (time) dimensions.**
- **Appreciate fully the opportunities and limitations afforded by major terrain and oceanographic features, zones of entry, transportation networks, obstacles, and built-up areas within the AO and AOI.**
- **Fit an operational concept to that battlespace environment.**

The limits of the battlespace are determined for all aspects of air, surface, subsurface, land, space, and the electromagnetic spectrum that can impact friendly forces. Defining the limits of the battlespace is a joint effort between the operations and intelligence staffs based on the commander's guidance.

SECTION I. RESPONSIBILITIES

When time permits, the intelligence officer coordinates the development of a battlespace analysis based on anticipated missions. On receipt of the warning or execute order, the intelligence officer reevaluates the analysis in terms of the commander's assigned AO and potential AOI. Changes in the mission and the commander's AO and AOI, or receipt of additional or more accurate information, necessitate revision of the analysis as the operation progresses. Normally, MEF and higher headquarters staff prepare a detailed written analysis when planning anticipated missions. In MSCs, the G-2s may prepare a written analysis tailored to the unit's specific mission and intelligence needs. However, in most operations, the geospatial information and services officer, the intel bn commander or intelligence support coordinator, and the P&A cell officer in charge use the MEF's analysis supplemented by graphic representations of weather and terrain data covering the MAGTF's AO and AOI.

The intelligence officer is responsible for initiating, coordinating, and ensuring that the analysis of the MAGTF's AO and AOI is completed and disseminated. The final analysis represents a coordinated effort of the intelligence officer, the operations officer, and other staff personnel who contribute within their respective warfighting functional areas. At the MEF or MAGTF level, the following organizations and personnel contribute to the final analysis:

- **Topographic platoon, P&A company, intel bn—**
  - **Provides tailored terrain, littoral, and infrastructure studies and factor overlays.**
  - **Supports integration of weather factors into terrain studies portraying environmental effects.**
  - **Disseminates products such as graphic tactical decision aids to support IPB and COA development.**
- **Staff weather officer, intelligence section, MEF CE provides operational weather forecasts and environmental impact graphics as well as other weather and climatic data (e.g., light and tidal information).**

- All-source fusion platoon, P&A company, intel bn—
  - Develops information on sociological, political, economic, technological, and related conditions covering countries of interest.
  - Provides fused, all-source IPB and other intelligence products to support MEF staff planning and decisionmaking.
- Civil affairs officer provides information on civilian personnel, local labor conditions, and capabilities.
- Engineer officer assists in the analysis of routes, potential obstacles and barriers, and other information related to mobility and countermobility.
- Psychological operations officer assists in the assessment of local conditions for psychological operations.

SECTION II. CHARACTERISTICS OF THE BATTLESPACE

The limits of the battlespace are determined for aspects of air, surface, subsurface, land, space, and the electromagnetic spectrum, which can directly or indirectly impact friendly forces. The battlespace generally includes all or most of the AO as well as the AOI. The AOI encompasses that area beyond the AO from which intelligence and information are required to permit planning, decisionmaking, and the successful conduct of operations. Defining the limits of the AO, the AOI, and the battlespace is a joint effort between the operations and intelligence staffs based on the commander's guidance. The AO and AOI are dynamic in nature and include interrelated factors capable of affecting a unit's operation.

The battlespace is measured in four dimensions: depth, width, height, and time. A battlespace analysis of the AO and AOI evaluates and integrates four environmental dimensions: terrain analysis (land), hydrographic analysis (sea), airspace analysis (air), and climatological analysis (weather). The battlespace analysis study allows the operational commander and staff to fully appreciate the opportunities and limitations afforded by major terrain and oceanographic features, zones of entry, transportation networks, obstacles, and built-up areas within the AO and AOI and fit an operational concept to that environment.

SECTION III. TERRAIN ANALYSIS

Terrain analysis is the evaluation of natural and manmade geographic features. This evaluation provides the planning headquarters with information on AAs (location and trafficability), zones of entry (deep, close, and rear areas), and key or decisive terrain.

Responsibilities

Much of the detailed terrain analysis work is done by P&A company GEOINT support teams attached to or in direct support of the MSCs or by GEOINT teams attached to a MEU(SOC) CE.

The P&A company's topographic platoon and imagery intelligence platoon personnel conduct the major portion of the terrain analysis production by—

- Using data bases as a guide for collection, production, and dissemination planning and operations while focusing on the areas of most importance to the commander and the mission.
- Combining data base information with the results of tactical, aerial, and ground reconnaissance.
- Working closely with staff weather officers to ensure terrain analysis products incorporate the

effects of current and projected weather phenomena.

- Using AO and AOI reconnaissance analysis results to focus on areas of most importance to the commander and the mission.
- Analyzing terrain continuously to evaluate the effects of changes in the battlespace environment.
- Forming conclusions regarding the effects of terrain through analysis of the military aspects of the terrain, and evaluation of the terrain's effects on military operations.

Sources of Information

National Imagery and Mapping Agency produces numerous digital data bases that support the development of geospatial factors and geographic classification. Topographic and geodetic maps, aerial charts, and facility maps are basic sources of information used by terrain analysts. Topographic publications can also be obtained from—

- Geographic societies.
- Engineering and scientific firms.
- Government intelligence agencies.
- Libraries.
- Bookstores.
- Universities.

Geospatial Factors

Terrain analysts need data on the trafficability of soils, the presence of bedrock, as well as the type and density of vegetation when developing cover and concealment, cross-country movement, or other geographic data bases.

Surface Configuration

Surface configuration refers to the shape of the earth's land surface. Terrain analysts study surface features such as mountains, slopes, ravines, embankments, ditches, plowed fields, and rice field dikes, because they can profoundly influence military operations. This factor is limited only by physical shape, size, and arrangement; it is not concerned with whether the feature is manmade or of natural origin.

Analysts categorize surface features or landforms by size and shape. The principal groups of landforms are plains, hills, and mountains; within each of these groups are smaller surface features, such as flat lowlands, and valleys. For geospatial analysis and GEOINT production purposes, major landforms are defined on the basis of local relief. Local relief represents the differences in the elevation of each landform group and subgroup (see table 6-1).

Table 6-1. Landform Elevations.

Landform	Elevation
Plains	less than 150 meters
Flat	less than 15 meters
Undulating	15 to 50 meters
Gently rolling	50 to 100 meters
Rolling	100 to 150 meters
Hills	150 to 600 meters
Low	less than 300 meters
High	300 to 600 meters
Mountains	more than 600 meters
Low	600 to 1500 meters
High	more than 1500 meters

Hydrologic Features

Hydrology is the science of surface and subsurface waters. Terrain analysts are concerned with the shape, size, distribution, and temporal

variance of water bodies. Analysts classify hydrologic features as surface water, subsurface water, and wet areas.

Surface Water

This hydrologic feature encompasses inland waters, which are classified as watercourse (e.g., streams, rivers, canals) and standing bodies of water (e.g., lakes, ponds, glaciers). Terrain analysts evaluate watercourses because drainage conditions vary from place to place and from time to time. Military planners are concerned with the flow and channel characteristics of these watercourses and their effect on military operations. Water bodies affect the characteristics of surface drainage by storing precipitation and runoff and by retarding or augmenting flood flows. These water bodies can obstruct cross-country movement or provide AAs when sufficiently frozen.

Subsurface Water

Groundwater or subsurface water is located beneath the surface of the earth. Groundwater is less susceptible to contamination and may be the only source of water in arid regions.

Wet Areas

These tracts of ground are covered with water seasonally or perennially (e.g., swamps and marshes). These areas are treated separately in the collection of data because information requirements differ from other water bodies, especially in evaluation for cross-country movement.

Vegetation Features

Vegetation includes plant life growing on the surface of the earth or other flora in or on the water. Terrain analysts evaluate area vegetation to determine the potential effect on vehicular and foot movement, concealment, cover, observation, airdrops, and construction. The vegetation present indicates the climatic conditions, soil, drainage, and water supply. Vegetation is grouped by type (e.g., trees, scrub and shrubs, grasses, crops).

Trees

This group of vegetation includes perennial woody plants at least 10 feet in height, with single stems and defined crown shapes. An area extensively covered by trees is classified as a forest. Smaller areas covered by trees are classified as woods, groves, or woodlots. On military maps, any perennial vegetation high enough to conceal troops or thick enough to be a serious obstacle to free passage is classified as woods or brushwood.

Scrub and Shrubs

Either deciduous or coniferous, scrubs include a variety of trees that have had their growth stunted because of soil or climatic conditions. Scrub growth includes cactus, stunted shrubs, sagebrush, mesquite, and similar plants found in arid or semiarid areas.

Shrubs, like trees, are either deciduous or coniferous. Shrubs comprise the undergrowth in open forests; in arid and semiarid areas they are the dominant vegetation. Shrubs normally offer no serious obstacle to movement and provide good concealment from ground observation; however, they may restrict fields of fire.

Grasses

This vegetation group includes nonwoody plants. A grassland is an extensive area where the natural vegetation consists primarily of grasses and herbaceous plants, the dominant type in alpine and certain semidesert areas. In low latitudes, grasslands often are termed savannas; in middle latitudes, they are called prairies (tall grass) and steppes (short grass). Grasslands in wet or poorly drained areas are commonly called meadows. For geospatial analysis purposes, grass more than 1 meter (3 feet) high is considered tall, and below that height, grass is considered short. Grass often improves the trafficability of some

soils; very tall grass may also provide concealment for foot troops.

Field Crops

The predominant class of cultivated vegetation is field crops. Vine crops and orchards are common but not widespread, and tree plantations are found in relatively few areas. Sizes of cultivated areas range from paddy fields covering a quarter of an acre to vast wheat fields extending for thousands of acres. In a densely populated agricultural area where all arable land is used for the crop that brings the highest yield, it may be possible to predict the nature of the soils from information about the predominant crops.

For example, rice requires fine-textured soils. Other crops generally must have firm, well-drained land. An area of orchards or plantations usually consists of rows of evenly spaced trees, which shows evidence of planned planting that can be distinguished on aerial photographs. Usually such an area is free from underbrush and vines. Rice fields are flooded areas surrounded by low dikes or walls. Some crops, such as grain, improve the trafficability of soils, while other crops, such as vineyards, present a tangled maze of poles and wires that are definite obstacles to vehicles and dismounted troops. Wheeled vehicles and some tracked vehicles are unable to cross-flooded paddy fields, although they can negotiate them when the fields are drained or frozen.

Surface Materials

Terrain analysts evaluate the composition and physical properties of the earth's surface materials, which are classified as soil and rock, to determine their effects on military operations and construction.

Soil

This unconsolidated material is an accumulation of disintegrated and decayed rock and vegetation that overlies bedrock. This accumulation can be hundreds of feet thick or it may be absent in given areas. Soils between 15 centimeters (6 inches) and 2 meters (6 feet) in depth are the most important. Next in importance are the soils from 2 to 6 meters (6 to 20 feet). Soil depth can be measured directly from borrow pits, road cuts, building excavations, and stream banks. For field identification, analysts classify soils as gravel, sand, silt, clay, and organic matter.

Rock

Rock is the firm or consolidated mineral matter of the earth's crust. Bedrock is solid undisturbed rock either exposed at the surface or underlying the soil. Terrain analysts evaluate the physical and engineering characteristics of bedrock for use in construction and in locating ground water.

Military Aspects of Terrain Evaluation

Using portions of the IPB process, the intelligence officer evaluates the battlespace in terms of Key terrain, Observation and fields of fire, Cover and concealment, Obstacles, and AAs and mobility corridors (KOCOA). The KOCOA analysis is appropriate at the battalion, squadron, regimental, Marine aircraft group, and CSS detachment levels. At division, Marine aircraft wing, force service support group (FSSG), and higher levels, KOCOA is absorbed into the terrain analysis process. Analysts use KOCOA to determine which friendly COAs can best exploit the opportunities the terrain provides and how the terrain affects the threat's available COAs.

Key Terrain

Key terrain is any location or area that the seizure, retention, or control of affords a marked advantage to either combatant. Terrain analysts depict key terrain on overlays with a large "K" in a circle that encloses and follows the contours of the designated terrain.

Observation and Fields of Fire

Cover and concealment factors can limit or deny observation. Observation analysis is useful in—

- Selecting LZs and DZs.
- Planning helicopter forward arming and refueling point (FARP) locations.
- Identifying areas vulnerable to aerial intelligence collection systems.
- Selecting low-level flight routes and aerial battle positions.

An ideal field of fire for flat trajectory weapons is an open area in which the threat can be seen and on which he has no protection from the fire of those weapons, out to the weapon's maximum effective range.

Geographic factors that offer good observation and fields of fire generally favor defensive COAs. Analysts represent areas of poor observation and fields of fire on an overlay with marked parallel diagonal lines or crosshatching. Observation and fields of fire evaluations identify—

- Potential engagement areas (often referred to as fire sacks or kill zones).
- Defensible terrain and system or equipment positions.
- Locations where maneuvering forces are most vulnerable to observation and fires.

Cover and Concealment

Analysts can combine the cover and concealment evaluation with the overlay developed during the observation and fields of fire evaluation (see fig. 6-1). When preparing the overlay, analysts identify factors that provide cover and concealment. Commanders and staffs use the results of the evaluation to—

- Identify and evaluate AAs.
- Identify defensible terrain and potential battle positions.
- Identify potential assembly and dispersal areas.

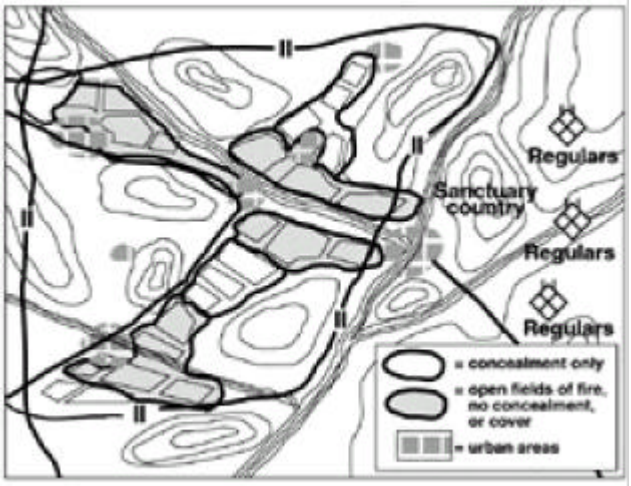


Figure 6-1. Concealment and Cover Overlay.

Cover that provides protection from the effects of direct and indirect fires can be provided by—

- Ditches.
- Caves.
- Riverbanks.
- Folds in the ground.
- Shell craters.
- Buildings.
- Walls.
- Embankments.

Concealment that provides protection from observation can be provided by—

- Woods.
- Underbrush.
- Snowdrifts.
- Tall grass.
- Cultivated vegetation.

Obstacles

Analysts identify natural and manmade obstacles that stop, impede, or divert military movement. Obstacles to air mobility include features that exceed the aircraft's service ceiling, restrict nap-of-the-earth (NOE) flight, or force the aircraft to employ a particular flight profile. An evaluation of obstacles leads to the identification of mobility corridors. This in turn helps identify defensible terrain and AAs.

Evaluation

When evaluating obstacles, analysts—

- Identify pertinent obstacles in the AO by considering—
  - Vegetation.
  - Surface drainage.
  - Surface materials.
  - Surface configuration.
  - Transportation systems (e.g., bridge classifications, road conditions).
  - Weather effects (actual or projected).
- Determine the effect of each obstacle on the mobility of the evaluated force by preparing a separate overlay for each factor, or combine the effects of individual obstacles into an integrated product or COO, which depicts the battlespace effects on mobility.

Classification

Analysts graphically depict and classify the cumulative effects of obstacles as unrestricted, restricted, and severely restricted areas, which are defined below:

- Unrestricted. Indicates terrain free of any restrictions to movement. Nothing needs to be done to enhance mobility. Typically this terrain is flat to moderately sloping terrain with scattered or widely spaced obstacles such as trees or rocks, which allows for armored or mechanized forces and wide maneuvers.
- Restricted. Indicates terrain that hinders movement to some degree. Units may have difficulty maintaining preferred speeds, moving in combat formations, or transitioning from one formation to another. This terrain slows movement by requiring zigzagging or frequent detours. Moderate to steep slopes or moderate to densely spaced obstacles such as trees, rocks, or buildings may restrict armored or mechanized forces. Swamps or rugged terrain may restrict dismounted infantry forces. Poorly developed road systems may restrict logistical and rear area movement. Analysts depict restricted terrain on overlays and sketches by marking the areas with parallel diagonal lines.
- Severely restricted. Indicates terrain that severely hinders or slows movement in combat formations unless some effort is made to enhance mobility. The mobility enhancement efforts could include committing engineer assets to improve mobility, moving in column instead of line formations, or moving at slower than preferred speeds. Steep slopes and large or densely spaced obstacles with little or no supporting roads typically characterize severely restricted terrain for armored and mechanized forces. Analysts depict this type of terrain on overlays and sketches by marking the areas with crosshatched diagonal lines.

Avenues of Approach and Mobility Corridors

To develop the air or ground routes of an attacking force, analysts must identify and categorize mobility corridors. Mobility corridors are areas where a force is channeled around obstacles. The best mobility corridors use unrestricted terrain with enough space for a force to move in its preferred doctrinal formations while avoiding major obstacles. These corridors usually follow the direction of roads and trails.

Considerations

Analysts use the COO to identify mobility corridors wide enough to permit maneuver in tactical formations. If friendly and threat forces require

mobility corridors of different widths as a result of organizational or equipment differences, analysts may conduct two separate evaluations. Identification of mobility corridors requires some knowledge of friendly and threat organizations for combat and preferred tactics. When identifying mobility corridors, analysts must evaluate obstacles and force mobility. The analyst should also consider that—

- Mechanized and armored units generally require large open areas to move.
- Dismounted infantry, most insurgents, and terrorists are less restricted by the presence of obstacles or hindering terrain and prefer areas that provide concealment and cover.
- The mobility corridor used by a jet aircraft with a minimum operating altitude of 1,000 feet is quite different from that considered by a helicopter with a maximum service ceiling of 10,000 feet.

Categories

Once identified, mobility corridors are categorized according to the size or type of force they will accommodate. Mobility corridors are normally identified for forces two echelons below the friendly command. In addition, where terrain is restrictive, the evaluation may need to look several echelons below the friendly command.

Analysts group mobility corridors together to form AAs. Avenues of approach may include areas of severely restricted terrain since they show only the general area through which a force can move. Analysts depict AAs on an overlay using an outline arrow that encompasses the mobility corridors. Threat AAs are generally depicted in red, friendly AAs are depicted in blue.

Evaluation

During offensive operations, analysts evaluate AAs to recommend the best route to the command's objective and to identify avenues available to the enemy for force withdrawal or movement of reserves. During the defense, analysts identify AAs that support the threat's offensive capabilities and avenues that support the movement and commitment of friendly reserves.

An evaluation of AAs identifies those that best support maneuver capabilities. This evaluation should be a combined effort performed by the intelligence section, the imagery and mapping officer or GEOINT support team, and the operations section. These AAs are evaluated for—

- Access to key terrain and adjacent avenues.
- Degree of channelization and ease of movement.
- Use of cover and concealment.
- Use of observation and fields of fire.
- Sustainability.
- Directness to the objective.

SECTION IV. HYDROGRAPHIC ANALYSIS

Sea or hydrographic analysis is the study of areas containing shorelines. Intelligence of coasts and landing beaches is important to military planners because the coast is a country's first line of defense. The hydrographic analysis is subdivided into the offshore, nearshore, and foreshore environments. The land analysis is subdivided into the beach and inland environments. Intelligence personnel conduct hydrographic P&A to evaluate coastal conditions that support amphibious operations. Amphibious operations require detailed oceanography studies that are discussed in Joint Publication (JP) 3-02, *Joint Doctrine for Amphibious Operations,* and FM 34-81, *Weather Support for Army Tactical Operations*.

Sources of Information

The Naval Oceanographic Office (Major Shared Resource Center, John C. Stennis Space Center, National Aeronautics and Space Administration, MS), conducts comprehensive analysis of littoral and hydrographic factors worldwide. Joint Intelligence Center, Pacific; Joint Forces Intelligence Command; and Marine Corps Intelligence Activity (MCIA) produce detailed imagery-based beach studies. Graphic and text-based analysis are available both online via intelligence link (INTELINK) or intelligence link-SECRET (INTELINK-S) and via request for production validated through the operational chain.

Hydrographic Conditions

Analysts evaluating the hydrographic conditions of a coastal region study seas and surf, tides, and currents that can affect amphibious landings.

Seas, Swells, and Surf

Seas are waves that originated in local storms. Swells are waves that have traveled hundreds to several thousands of miles from a distant storm before arriving at the landing site. Breaking waves or surf 4 feet in height normally are considered too high for amphibious assault operations or for logistics over the shore. By identifying the following types of breakers, analysts can determine the trafficability of the nearshore bottom:

- Spilling breakers indicate a gentle sloping bottom. The waves lose energy gradually as they approach shore by breaking only at the crest, and it is common to see a number of such breakers existing simultaneously.
- Plunging breakers indicate an unstable nearshore bottom. These waves break in a rollover, plunging action that causes abrupt changes in the form of a longshore bar or degree of steepness at the shore.
- Surging breakers indicate a steep nearshore gradient and are the least common of all types of breakers. This type of wave peaks near the shoreline, but instead of breaking or spilling, it actually surges up the face of the beach.

Tides

Tides are the alternate rising and falling of the sea caused by the gravitational attraction of the moon and sun. The tidal range is the complicated product of various forces, including local bottom configuration and the size and configuration of oceanic basins that can alter the height and time of the tides. When identifying beach widths, hazards, and depths, analysts must specify the time of day observations were made to permit tidal computations. Tidal information for most places on the coasts of the world can be obtained from tide tables published by the U.S. Department of Commerce.

Currents

Currents in the nearshore zone which influence amphibious landing operations are generally classified as wave-generated, tidal, or river currents.

Wave-Generated Currents

These currents are caused by the angular breaking of waves on the beach slope and the resultant back rush normal to the beach, which results in a littoral current (longshore current) in the nearshore zone, flowing generally parallel with the shoreline. It is found shoreward of the outermost edge of the breaker zone and varies in velocity or force with the force of the waves, their angle of impingement upon the shore, and the steepness of the foreshore. Littoral currents may be insignificant in terms of amphibious operations, or they may be strong enough to cause personnel to lose their footing, to make maneuvering of craft difficult, and to throw landing or assault craft out of control and expose them to broadside attack by the surf. Littoral currents are particularly significant where depths

shoreward of the breaker zone are such as to make wading hazardous.

Tidal Currents

These currents affect amphibious landings in the proximity of tidal inlets, estuaries, river mouths, and similar restricted channels. With large tidal ranges these currents may make the maneuver of landing craft on beaches adjacent to the tidal inlet extremely hazardous.

River Currents

Currents that extend from rivers into the open sea are frequently of such strength that they affect the maneuver of landing craft near the river's mouth.

Beach Selection Considerations

Beaches are the most prevalent natural features of the coastal region. They are accumulations of loose sand, gravel, or boulders that are shaped by waves and currents acting on the shore. Along many lowland coasts, beaches occur as barrier islands that parallel the coast and are separated by a lagoon or bay. Along other stretches of coast, beaches are backed by eroding cliffs, or the beach may be absent with high rocky cliffs facing the waves.

Hydrographic conditions shoreward of the 30-meter depth curve should be thoroughly investigated and surveyed. Shallower depths of the surf zone from 0 to 30 meters are of primary concern in amphibious operations because crafts ground and troops and vehicles disembark in this area. When preparing hydrographic beach surveys, analysts must—

- Record accurate locations of obstructions.
- Determine clear boat passages to the beach.
- Determine trafficability of bottom materials.
- Select suitable beaching locations for amphibious vehicles.
- Determine maneuver areas for crafts.

From a tactical perspective, the ideal sea approaches to the beach should have—

- No obstructions.
- Deep water close inshore.
- Nearshore gradients deep enough for dry-ramp beaching of landing craft and ships.
- Soil composed of firm sand with gentle gradients.
- Small tides.
- No currents or surf.

The ideal beach terrain should be—

- Flat or gently rising.
- Backed by a coastal range high enough to mask the landing area.
- Relatively clear.
- Firm with adequate drainage.

Analysts evaluate the following beach features to determine those areas that come nearest to the optimum landing requirements.

Size

Analysts measure the beach to determine the force size that can be supported. The beach size also defines requirements for follow-on logistical forces and establishment of logistical base sites or dumps. Analysts determine the usable beach length by measuring, in kilometers, the gross length minus unsuitable landing features, such as rivers and rock outcroppings. When preparing the overlay, analysts describe and plot—

- Unsuitable beach sections.
- Features that might affect movement along the beach.
- Beach widths available at the low-water tide stage (maximum width) and at the high-water tide stage (minimum width), noting each stage of the tide.
- Locations of major changes in width.

Approaches

Analysts identify major obstructions and obstacles in the offshore approaches for an area seaward of the 30-meter depth curve. More detailed analysis and information are provided shoreward from the 30-meter depth curve giving distances and azimuths of obstructions and obstacles from the centerline of the beach. When describing general approach conditions, analysts note the presence of—

- Shoals.
- Bars.
- Kelp beds.
- Island groups.
- Exposed rocks.

Gradient

The foreshore gradient may be so steep as to prohibit the landing of vehicles from beached craft without use of matting, or it may be so flat as to cause personnel and vehicles to move great distances from boats over exposed areas to cover. Analysts express the gradient as one unit of vertical rise in relation to horizontal distance (e.g., 1 foot vertical height over 20 feet of horizontal distance = 1:20). Gradient may also be given in percent of slope or degree of angle. Analysts record gradients when—

- High-water zone of the foreshore is much steeper than the foreshore.
- Seasonal gradient changes information is available.
- Backshores are not level.

Composition

A description of the characteristics of the beach material gives a valuable clue to the slope or gradient of a beach when other information is lacking. Analysts can determine the gradient by the size of the beach material and the character of wave action. The depth of beach materials and the nature of subsurface materials are also indications of beach firmness and trafficability.

Trafficability

The beach's ability to sustain troop and vehicle traffic depends on factors such as moisture content, slope, grain size, and compacting. When evaluating beach trafficability, analysts must consider the following general rules:

- Changes in beach firmness may occur in short periods of time.
- Sandy beaches are more firm when damp.
- Beach backshores are frequently dry and therefore soft.
- Pebbles and cobbles are firm for bearing capacity but are loose for vehicle traction.
- Clay is soft when wet, but combinations of clay and sand may be firm.
- Fine to coarse sand mixtures tend to be firm.
- Soft zones are common near the upper level of wave wash at high tide because air pockets are trapped under the wet sand.
- Sand beaches exposed to wave action are generally firmer than beaches of similar material in sheltered locations.

Vegetation

Beach vegetation rarely affects military operations except for mangrove. These tropical trees and shrubs normally grow in sheltered tidal areas that have a soft, fine bottom material, but they may exist on foreshores that do not experience heavy wave action. Analysts identify the mangrove's interlaced roots, which constitute a barrier to movement.

Natural Obstacles

Analysts evaluate cusps, beach ridges, scarp, and berm to identify areas that could impede movement.

Natural Cusps

These are more or less evenly spaced ridges or horns of beach material and intervening crescent shaped troughs. The horns trend at right angles to the shoreline and taper to their point seaward. Cusps present on beaches should be noted. There are several characteristics of this beach feature that may be significant in amphibious landings. Along gravel beaches, the cusps may develop very large proportions, rising several feet above adjacent troughs and becoming a serious hindrance to traffic. Cusps are soft, whereas the troughs are usually of the same firmness as the normal beach face.

Beach Ridges

These continuous mounds or ridges are created by wave action along the upper limits of the beach. They may occur as single ridges or as a series of parallel ridges extending some distance inland. Commonly 3 to 8 feet in height above mean high tide, beach ridges can attain a height of 30 feet on pebble beaches. Ridges may consist of sand, pebbles, or gravel. Gravel or shingle ridges are high and loose and are very difficult to traverse.

Scarp

This near-vertical face cut into beach materials is caused by erosive wave action and may be a formidable barrier to movement across the beach. Scarps cut into the backshore have permanence, but normal wave action will eliminate foreshore scarps.

Beach Berm

A horizontal formation of material deposited by wave action, beach berm begins at the limit of normal-wave up rush and extends landward. Where more than one berm exists, they are separated by beach scarps in various stages of deterioration. The seaward margin of a berm is know as the berm crest. Berms are usually dry and soft but may be firm for a short time when damp.

Manmade Obstacles

Groins, jetties, bulkheads, and sea walls are manmade structures that could hinder beach operations.

Groins

These structures are used to stabilize a beach. They are long, low, narrow structures extending seaward from the backshore that are built to trap water-suspended sand on shore. Because groins are usually built as a system of structures spaced at regular intervals along the beach, analysts identify them as obstacles to the lateral movement of vehicles.

Jetties

Used to improve and stabilize inlets and river mouths, jetties project seaward from the shoreline through the normal surf zone. They are larger and more massive than groins. They prevent sand deposits in the channel, regulate the inflow and outflow of tides and river discharge, and protect vessels entering the inlet or river. Analysts evaluate jetties to determine if they are high enough to protect vessels against storm wave action and to prevent sand movement in the channel.

Bulkheads and Sea Walls

These structures protect areas of the coast against heavy storm wave action. They limit the shoreward movement of destructive waves, but under severe wave action they may cause the removal of sand from the beach. Analysts evaluate bulkheads and sea walls because they are normally strongly built and difficult to break through, which can prevent troop and vehicular movement from the beach to inland areas.

Exits

Uninterrupted movement inland from a beach is necessary to provide direct, rapid support and supply of combat forces and to avoid the creation of lucrative targets of accumulated material

and personnel on beaches. However, movement off a beach inland onto favorable terrain in many localities is one of the most difficult aspects of a landing because of the prevalence of bluffs, dunes, swamp, or lagoons close behind the beach. Existing exits require little or no preparation. They may be manmade or natural, such as roads, ramps, stairs, paths, gullies, dry stream beds, and gaps between dunes. Another characteristic of an exit requiring evaluation is the width. An exit should have a minimum width of 8 feet to permit the passage of vehicles.

SECTION V. AIRSPACE ANALYSIS

The addition of the airplane and helicopter to the arsenal of war requires that the battlespace be viewed in terms of width, depth, and a third dimension, height or airspace (measured in cubic kilometers). Because airspace has no reference points to guide the analyst and evidence of air activity is erased seconds after the activity occurs, it is often difficult to establish NAIs, TAIs, and air operations decision points. Airspace analysts are required to tie air events to time and the ground and to integrate the terrain analysis with analysis of—

- Aircraft maximum service ceilings.
- Minimum operating altitudes for fixed- and rotary-wing aircraft.
- Maximum effective ranges of air defense weapons systems.

Geospatial Analysis Support

The intelligence staff receives support from the terrain team during airspace analysis. However, this support must be augmented by personnel from other functional areas with an understanding of the air threat, air defense systems and operations, and close air support techniques.

Geospatial analysis and GEOINT production in support of air defense, counter air, and air-associated operations deal with an environment that extends several thousand meters above ground level and with forces whose mobility is limited only by the ability of their equipment. Terrain analysis is required because aircraft and air defense elements use the terrain to their best advantage.

Standard military topographic maps are not normally considered suitable for other than the most basic airspace analysis. Standard 1:50,000-scale topographic maps are most useful when analyzing the ability of an aircraft to approach, acquire, and engage a target. The analysis of an aircraft's approach (from air base to target vicinity) or of enemy air corridors should be conducted using standard 1:250,000-scale joint operations graphic-air (JOG-A) specifically designed for this purpose.

Airspace Evaluation

The third dimension of the battlespace includes the air AO and the air AOI. The air AO is the area where the commander is assigned responsibility and authority for military operations. The air AOI includes airspace adjacent to the air AO and extends into enemy airspace upward to the maximum service ceiling of enemy aircraft and the maximum effective altitude of enemy air defense weapons systems. It takes into consideration any space-capable system, i.e., satellites. In addition, the air AOI may extend as far as enemy airfields and to the maximum range of enemy surface-to-surface missile systems. During the airspace evaluation of the battlespace, analysts identify potential locations of LZs, DZs, FARPs,

and forward assembly or expeditionary airfields to pinpoint requirements for further analysis.

Military Aspects of Terrain Evaluation

Terrain analysis for air operations focuses on the same military aspects of terrain as ground operations. However, the analysis of these aspects is directed first at their effects on airspace operations and then on their resultant effects on the overall operation.

Key Terrain

Key terrain in airspace analysis is any terrain feature that allows air defense weapons to engage channeled or constrained air or airborne forces. Analysts should identify—

- Areas that limit aircraft lateral movement.
- Areas that restrict air maneuver.
- Elevations higher than maximum aircraft service ceilings.
- Airfields.
- LZs and DZs.
- Fixed or surveyed air defense weapons and radar sites.
- FARPs.

Observation and Fields of Fire

As with ground operations, observation involves the effects of the terrain on reconnaissance and surveillance as well as target acquisition. Fields of fire involve the effects of terrain on weapon's effectiveness. In air defense, both counterair and other air operations are closely related to line of sight (LOS). Ground operations are concerned primarily with horizontal LOS; air and air-associated operations are primarily concerned with air and ground oblique and vertical LOS.

Attack aircraft and air defense assets want as much protection as possible from enemy observation, and both require direct LOS to the target. It is, therefore, necessary to analyze airspace regarding the routes which provide the best protection for aircraft entering the target area and those which provide the best fields of fire for the aircraft once it reaches the target area. Similarly, the analysts must consider where air defense assets can best be hidden from observation and retain good fields of fire against the primary air AAs and mobility corridors.

Cover and Concealment

Friendly force operations require cover from aerial direct fires and concealment from aerial reconnaissance and surveillance. The enemy also uses terrain to provide cover from direct fires and to conceal their operations from friendly detection. Analysts evaluate airspace routes that provide the best protection for aircraft entering the target area and identify locations where air defense assets can best be hidden from observation.

While not considered as either concealment or cover in the strictest sense, NOE flight enhances both fixed- and rotary-wing aircraft survivability. An NOE flight makes the optimum use of available terrain for concealment and cover and hinders quick countering responses by ground forces and air defense assets.

Obstacles

When evaluating terrain, analysts identify the following types of obstacles, which channel aircraft movement and restrict evasive' actions:

- Obstacles to the effective employment of air defense target acquisition or weapon systems (e.g., terrain that masks LOS, built-up areas, tall buildings, vegetation).
- Obstacles that restrict NOE flights, which are below 22.8 meters or 75 feet in height (e.g., tall trees; radio, television, and microwave relay towers; power transmission lines; support towers; smoke and obscurants; tall buildings).

- Obstacles that force aircraft to employ a particular profile or attack route or to gain excessive altitude that is above 22.8 meters in height (e.g., mountains, large hill masses, built-up areas, excessively tall trees).
- Obstacles that restrict lateral movement within the air AA or mobility corridor. These obstacles have the same effect on aircraft as ground obstacles, that is, channeling movement and restricting evasive action. They often become key terrain for the employment of air defense weapons systems.

Avenues of Approach

A good air AA permits maneuver while providing terrain masking from air defense weapons systems. In addition to the criteria evaluated for ground AAs, analysts consider the following variables when analyzing air AAs:

- Type of aircraft.
- Maximum service ceiling of the aircraft.
- Attack profile being employed.
- Weapon system or expected ordnance.
- Type of target to be attacked.

Weather

Aviation operations are especially susceptible to weather effects, because temperature, humidity, and cloud cover can have a significant impact on an aircraft's ability to use a particular AA. Analysts must evaluate the effects of visibility, wind speed and direction, precipitation, cloud cover, temperature, and humidity when conducting analysis for airspace operations.

SECTION VI. WEATHER ANALYSIS

Commanders and their staffs must acquire weather information about the entire battlespace area and know how to exploit the opportunities the weather offers while minimizing its adverse effects on personnel, equipment, and mission accomplishment.

Responsibilities

The following units and personnel are responsible for determining weather effects on the battlespace environment:

- MEF topographic platoon.
- MSC supporting GEOINT support teams.
- MEU(SOC) CE GEOINT teams.
- Staff engineer officer.
- Staff weather officer.
- Weather team.

Weather Effects

Weather, climate, and terrain are so interrelated they must be considered together when planning MAGTF operations. Weather elements are capable of drastically altering terrain features and trafficability. Conversely, terrain features exert some influence on local weather. This relationship of weather and terrain must be carefully correlated in terrain studies to produce accurate geospatial analysis. Terrain features are affected by such elements as visibility, temperature, humidity, precipitation, winds, clouds, and electrical phenomena. The specific factors described vary with the geographic area, time, and season. Terrain features also influence the climate of an area. The effects of temperature, humidity, precipitation, visibility, wind speed and direction, clouds, and atmospheric pressure can affect the battlespace environment, which can enhance or limit military operations.

Temperature and Humidity

Temperature is the value of heat or cold recorded by a thermometer, which is normally placed 6 feet above the ground. Temperatures are recorded in Fahrenheit and Celsius values.

Humidity is the water vapor content in the atmosphere. It is expressed as relative or absolute humidity.

When evaluating temperature and humidity, analysts must consider the following effects on operations:

- Aircraft efficiency is reduced in areas of high temperature and high humidity, because when temperature and humidity are high, the air is denser.
- Extreme temperature and humidity will reduce personnel capabilities and may necessitate a reduction of aircraft payloads.
- Tactics devised for one climatic zone may require considerable revision if used in another zone.
- High temperature and humidity conditions found in the tropics are conducive to growth of dense foliage and jungles, which affects trafficability and cross-country mobility.
- Cold weather periods—
  - Create a need for heated shelters.
  - Make the construction of fortifications difficult.
  - Increase the amount of dependence upon logistical support.
  - Necessitate special clothing, equipment, and combat skills.
- Periods of freezing temperatures—
  - Increase the trafficability of some soils.
  - Create ice sheets on roads, making movement more difficult.
  - Decrease a projectile's ability to penetrate the earth.
  - Increase the casualty effect of contact-fuzed shells.
- Melting snows may cause floods and avalanches.
- Temperature inversions (air nearest ground is colder than overlying air) cause the air to remain stable and to hold dust and smoke near the ground, which reduces both visibility and air purity.
- The amount of water vapor in the air affects the trajectory of projectiles.
- Humidity affects the distance sounds travel, thus affecting listening posts and sound-ranging operations.

Precipitation

Precipitation is any moisture falling from a cloud in frozen or liquid form. Common types of precipitation are rain, snow, hail, drizzle, sleet, and freezing rain. The intensity of precipitation is described as light, moderate, or heavy.

The primary significance of precipitation is its effect on the state of the ground and trafficability, on the efficiency of personnel, and on visibility. The effects of restricted visibility caused by precipitation are just as important as those caused by airborne particles such as dust or smoke. When evaluating precipitation, analysts must consider the following effects on operations:

- Rain, snow, and fog mask patrol and guerrilla activities by decreasing the enemy's surveillance and detection capability.
- Precipitation severely reduces trafficability by altering the surface condition of different soils to varying extents.
- Heavy rain may make some types of unsurfaced roads impassable.
- Heavy or prolonged precipitation usually aids the protected defense by limiting the mobility of an offensive force.
- Precipitation can drastically reduce the efficiency and effectiveness of exposed personnel.

- Precipitation may aid offensive operations by degrading the surveillance capabilities of radar, electro-optical, and infrared devices.
- Seasonal precipitation may change soil trafficability and affect cross-country movement.
- Seasonal floods or swelling streams may make fording and bridging operations difficult or impossible.
- Snow and sleet hamper movement on roads, often making them impassable in mountainous areas.
- Snow accumulations in mountains afford lower, drier regions with a water supply throughout the year.
- Precipitation usually has an adverse effect on visibility and observation.
- Rain may wash excessive impurities from the air.
- Rain and snow aid concealment, which may facilitate surprise attacks.
- Precipitation often limits operations of listening posts and many electro-optical systems.

Visibility

Weather personnel determine visibility by measuring the horizontal distance that the unaided eye can discern a large object or terrain feature. Visibility is reported in meters or fractions of a mile for the prevailing value of the visibility in all directions. Diminishing visibility measurements are noted in the remarks section of the weather observation report.

When evaluating the weather effects on military operations, analysts must consider that poor visibility—

- Aids ground offense and withdrawal.
- Restricts visual reconnaissance and surveillance.
- Tends to conceal concentrations and maneuver of friendly forces from the enemy, which enhances the possibility of achieving surprise.
- Hinders the defense because defensive cohesion and control are difficult.
- Decreases the ability to place aimed fire on the advancing force, making target acquisition less accurate.
- Enhances patrol activities and guerrilla operations by masking and screening movement.

Wind Speed and Direction

When weather personnel determine wind speed or velocity and direction, they measure the air movement rate past a given point and the direction from which the wind is blowing. A gust is a rapid fluctuation in wind speed with a variation of 10 knots or more between peak and lull.

When evaluating wind speed effects on the environment, analysts must consider the following effects on operations:

- Wind velocity on the surface and aloft favors the upwind force in any type of operation.
- Chemical and biological weapons will saturate the low-level, downwind atmosphere with contaminating aerosols.
- An upwind force, with the wind at its back, has better forward visibility and can advance easier and faster.
- Strong winds in arid or semiarid areas frequently raise large clouds of dust and sand, which greatly reduce observation.
- Blowing snow may reduce visibility over wide areas, which may ground observation aircraft and sensors.
- Winds tend to deflect projectiles from their normal paths, particularly when they are fired at long ranges. The effect that wind will have on a projectile increases with an increase in the wind velocity and the projectile size. The wind direction and velocity must be known to apply compensating corrections to firing data.

- Strong winds hinder amphibious operations by creating high seas, which can prevent landing craft from landing or retracting and restrict helicopterborne operations during the ship-to-shore movement.

Cloud Conditions

Cloud conditions are described by the amount and height of the cloud cover. Weather personnel measure the height of the cloud base from ground level and report that measurement in feet. A cloud base is the height of the lowest broken or overcast layer, while a cloud ceiling is the height of the highest layer of several scattered cloud layers. The types of clouds help determine the intensity and amounts of precipitation.

The type and amount of cloud cover, as well as the height of cloud bases and tops, influence ground tactics because they affect the entire range of both friendly and enemy aviation. Analysts should consider the following effects on operations when evaluating cloud conditions:

- Extensive cloud cover reduces the effectiveness of air support but provides a tactical advantage as cloud cover increases, as cloud bases lower, and as associated conditions increase (e.g., icing, turbulence, poor visibility).
- Clouds affect ground operations because they may limit illumination and visibility.
- As solar radiation interceptors, clouds tend to reduce extremes of surface temperature.
- Daytime cloudiness reduces the amount of heat received from the sun at the earth's surface, slowing down the drying of roads and affecting the trafficability of soils.
- Extensive night cloudiness prevents the loss of heat from the earth's surface, resulting in higher nighttime temperatures.
- Cloudiness affects air operations by limiting aerial observation and reconnaissance.

Atmospheric Pressure

The pressure exerted by the atmosphere at a given point is atmospheric pressure, which is measured by a barometer in millibars or in inches of mercury. The air density is measured at high and low altitudes and is reported as high pressure and low pressure. High pressure is critical to air operations because it affects the lift capability of helicopter and fixed-wing aircraft.

Weather Forecast and Weather Effects Products

While planners cannot control the weather, they should be able to exploit the opportunities offered by weather effects while reducing or minimizing its adverse effects on battlespace operations. Analysts provide planners with weather forecasts that cover the geographical layout of the battlespace and meet or exceed the duration of the planning and execution cycles. Using weather critical values tables created during IPB and weather forecast graphics (see fig. 6-2), analysts can quickly identify and determine the impact of weather effects on personnel, equipment, and planned operations. These impacts are displayed in the weather effects matrix (see fig. 6-3).

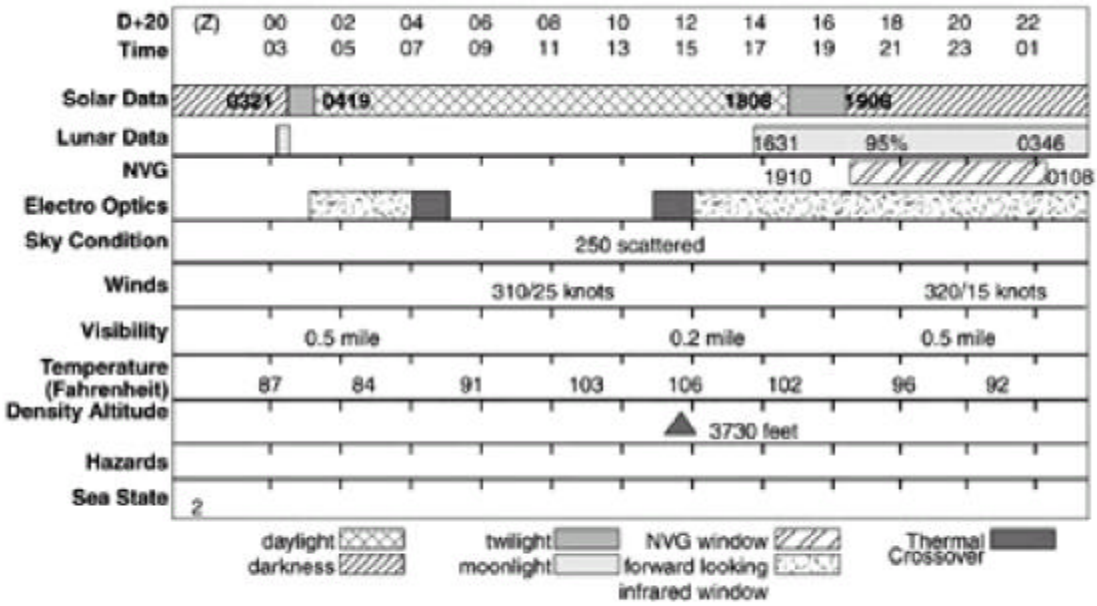


Figure 6-2. Weather Forecast Graphic.

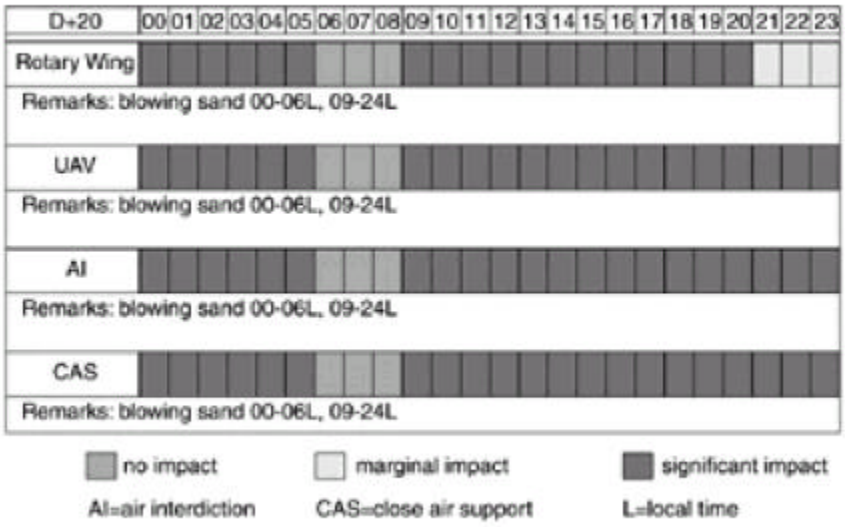


Figure 6-3. Weather Effects Matrix.

SECTION VII. INFRASTRUCTURE ANALYSIS

The infrastructure of a potential AO is a key element of information in an expeditionary environment. Points of entry, transportation systems, economic infrastructure, and social infrastructure, impact how friendly forces enter into, move through, and sustain themselves in the

AO. Infrastructure also impacts a potential threat's ability to conduct operations. The importance of particular facilities depends on the units involved and the type of operations envisioned. The study of a target area's infrastructure must focus on factors that are crucial to mission accomplishment. Most commands, particularly lower level tactical commands, must rely on other organizations and agencies to conduct infrastructure analysis and to provide accessible information.

Sources of Information

Detailed infrastructure analysis can be resource and time intensive, thus identification of analytical requirements prior to conflict or crisis helps ensure the availability of the information when needed. The intelligence staff must be familiar with all sources of infrastructure information that can be rapidly accessed when needed. Infrastructure analyses are performed by—

- Theater joint intelligence centers (JICs).
- U.S. Transportation Command.
- NIMA.
- Defense Intelligence Agency (DIA).
- Service intelligence centers (e.g., National Ground Intelligence Center, MCIA).
- Nonintelligence organizations (e.g., Marine Corps and Army civil affairs units).

Transportation System

In preparing intelligence studies, all transportation facilities must be carefully evaluated to determine their effect on the proposed operations. At higher levels of command, each major facility may be the subject of a detailed study by unit intelligence analysts or by external agencies such as theater JICs, U.S. Transportation Command JIC, or DIA.

Highway or Road Network

For intelligence purposes, a highway means roads, trails, multilane super highways, pack trails, and footpaths. Associated structures and facilities necessary for movement and for protection of routes, such as bridges, ferries, snowsheds, tunnels, and fords are integral parts of the highway system. An adequate highway system is required to conduct a major military operation. Military interest in highways of a given area or country covers physical characteristics of the existing system and various administrative and operational aspects pertaining to construction and maintenance.

Transportation studies should provide information on existing routes, major repair or rehabilitation requirements, and locations of new routes needed to support planned operations. The terrain study should indicate the minimum maintenance and construction requirements that may be anticipated during a planned operation. When evaluating the road network, analysts should consider—

- Routes in the combat zone should meet minimum standards.
- Roads in rear areas near water terminals, airfields, and supply installations must be well surfaced and capable of carrying heavy traffic without excessive maintenance.
- Operations on a wide front require a large number of secondary routes in forward and rear areas. The information presented in a terrain study should indicate the minimum maintenance and construction requirements that may be anticipated during a planned operation.
- Large volumes of heavy traffic severely abuse roads.
- Important bridges, intersections, and narrow passes are primary targets for enemy fires or unconventional operations.

- Maintenance should be conducted only on necessary routes.
- Construction of new routes must be held to a minimum.

Railroad Network

A railway includes fixed property belonging to the line. The fixed property includes land, facilities, bridges, tunnels, snowsheds, galleries, ferries, and other structures necessary for the movement of traffic. Railroad studies cover information pertaining to the development, construction, maintenance, and physical characteristics of the existing system. The network's physical characteristics information is necessary for determining capacities and maintenance requirements. Physical characteristics include the railroad's critical features, component parts (e.g., roadbed, ballast, track, rails/gauge), and horizontal and vertical alignment.

When evaluating railroad networks, analysts must consider the following factors:

- Railways are often the main transportation system in countries without an extensively developed road system.
- Suitability for mass movement and low susceptibility to weather effects make railroads useful for logistic support.
- Secondary and feeder railway lines are important to maneuver warfare with its emphasis on dispersal and the requirement for more and smaller rear installations.
- Railways and their associated facilities are highly vulnerable to enemy attack (e.g., sabotage, guerrilla operations).
- Keeping a railroad operational requires trained security forces and extensive protective measures.

Port and Harbor Facilities

Information and intelligence on ports, naval bases, and shipyard facilities is essential for estimating their capacities, capabilities, vulnerability, and other items of military significance. In wartime, principal and secondary ports and bases are prime targets for destruction. A port normally consists of a harbor plus terminal facilities. When natural, improved, or artificial harbors are developed for transactions between ship and shore, they become part of a port. Analysts classify these harbors as coastal, bay and estuary, and river. When evaluating port and harbor facilities, analysts are interested in harbor works, depths, navigable fairways, and anchorage.

Harbor Works

Structures designed to provide shelter, to control water flow, and to regulate erosion for the improvement of the navigability of a harbor are protective or harbor works. Harbor works do not include port facilities that are designed specifically for the transfer of cargo and the servicing of ships. The principal types of structures are—

- Breakwaters.
- Jetties.
- Groins.
- Sea walls.
- Bulkheads.
- Dikes.
- Locks.
- Moles.

Depths

Analysts compute depths of harbors, entrances, anchorages, wharves, and dry docks in reference planes based on tidal levels. When reporting depth, analysts must clearly indicate the reference plane or chart datum on the hydrographic chart. Datum established for ports is the basis for soundings.

Navigable Fairways

The approach, entrance, and the harbor itself frequently determine the size of ships that can

be accommodated in the port. Analysts must evaluate these fairway dimensions and describe any limitations on a ship's navigation (e.g., draft, length, beam, height above water). In addition, analysts should report ships' experiences entering the fairway.

Anchorage

Analysts show anchorage data on large scale charts and plans. Operational information reported includes—

- Anchorage designations.
- Berth assignments.
- Anchoring practices.
- Ships' experiences.

Airfields

Whether military or civilian, airfields are of vital importance to military combat situations. The size and features of an airfield determine its combat and reconnaissance capabilities.

Types

Installations termed airfields include—

- Air bases.
- Airports.
- Airstrips.
- Landing strips.
- Air depots.
- Heliports.
- Helipads.
- Seaplane stations.

Characteristics

Analysts conduct geographic studies to identify the airfield's—

- Type.
- Physical dimensions.
- Construction materials.
- Field condition.
- Support facilities.

Considerations

When evaluating the airfield, analysts report answers to the following questions:

- Is it serviceable?
- Is it occupied?
- Is it under construction?
- Is it in full or partial operations?

Structures and Crossings

Structures and crossings on highways or railways may reduce or interrupt the flow of traffic on a transportation route. Detailed information on structures and crossings is essential to a battlespace analyst and to an engineer, who may be required to repair or restore a structure. These structures and crossings include bridges, culverts, tunnels, galleries, snowsheds, retaining walls, ferries, fords, cableways, and tramways.

Bridges

Highway and railway bridges are vulnerable points on a LOC. Timely preservation, destruction, or repair of a bridge may be the key to an effective defense or to the successful penetration of an enemy area. A bridge seized intact has great value in offensive operations; even a small bridge facilitates the movement of forces over a river or stream.

Analysts obtain bridge information from reconnaissance or from the NIMA-produced planning terrain tactical data base. Using aerial photographs, analysts can determine bridge length, width, clearance, and height above water. Basic information requirements reported on a bridge include—

- Summary of its structural characteristics.
- Critical dimensions (length, usable width, overhead clearance).

- **Capacity estimation.**
- **General conditions.**

Tunnels, Galleries, and Snowsheds

Features on a transportation route where it would be relatively easy to block traffic or that affect the traffic capacity of the road, are considered to be critical features of the road. Such features include tunnels, snowsheds, galleries, mountain passes, terrain gaps, gorges and defiles, deep cuts, steep grades, and sharp curves. Any obstructions to traffic flow, which limit the physical dimensions of vehicles utilizing a specific route, are important aspects of route studies. Reductions in traveled way widths, such as narrow streets in built-up areas, drainage ditches, embankments, and war damage limit vehicular movement. Underpasses and other covered traveled ways may restrict traffic flow not only as to width but also as to height.

A tunnel is an underground section of the route that has been made by cut-and-cover or bored for the passage of a route. It consists of the bore(s), a liner (optional), and portals. Common shapes of tunnel bores are semicircular, elliptical, horseshoe, and square with arched ceiling. Bores may be unlined or lined with brick, masonry or concrete. Some long tunnels are artificially ventilated by blowers at the portals or in ventilating shafts above the bore. Alignment of tunnels may be straight or curved.

Snowsheds and galleries are protective structures built in rugged mountainous terrain. These are not as common as bridges or tunnels. Snowsheds offer protection against snow accumulations as well as drifts and slides on exposed sections of the permanent way. Galleries offer protection against snow and rock avalanches. They may be cut into the side of a cliff and have a natural overhang, or the cover may be a concrete slab, either of which guides the avalanche across the track or road. One side of a gallery is usually open.

Retaining walls are built to support embankments, either on the uphill or downhill side of the roadway. Retaining walls also are necessary where an embankment requires support against the pressure of water.

Ferries

A ferry site is that place where traffic and cargo are conveyed across a river or other water barriers by a vessel called a ferry or ferryboat. Ferryboats or vessels vary widely in physical appearance and capacity depending on the depth, width, and current of the stream and the characteristics of traffic to be moved. Propulsion of ferries may be by oars, cable and pulleys, poles, stream current (trail and flying ferries), or by steam, gasoline, and diesel engines. Analysts report the capacity of a civil ferryboat in tons and total number of passengers. In addition, it is often assigned a military load classification number. Ferry slips or piers are generally provided on the shore to permit easy loading of passengers, cargo, and vehicles. The slips may vary from simple log piers to elaborate terminal buildings. A distinguishing characteristic of a ferry slip is often the floating or adjustable approach ramp, which accommodates variations in the ferry deck level.

The limiting characteristics of ferry sites includes the width of the water barrier from bank to bank, the distance and time traveled by the ferryboat from one side to the other side, and the depths of the water at each ferry slip. Climatic conditions have a marked effect on ferry operations. Fog and ice substantially reduce the total traffic moving capacity and increase the hazard of the water route. Therefore, data on tide fluctuations, freezing periods, floods, excessive dry spells, and their effects on ferry operation are important considerations. Ferry slips are often optimal places for grounding displacement landing craft or as exit points for amphibious vehicles.

Fords

A ford is a location in a water barrier where the physical characteristics of the current, bottom, and approaches permit the passage of personnel or vehicles and other equipment under their own propulsion. Analysts assess a ford site for use as a bridge bypass.

Ford approaches may be paved with concrete or bituminous surface material but are usually unimproved. The composition of the stream bottom determines its trafficability. In some cases, the natural river bottom of a ford may have been improved to increase load-bearing capacity and to reduce the water depth. Improved fords may have gravel or concrete surfacing, layers of sandbags, metal screening or matting, timber or wooden planking. Bottom conditions are determined by checking the stability and composition of the bed. Known and suspected ford sites are key information when assessing the ability of a bridge to be bypassed.

Basic information requirements reported on a ford include—

- Trafficability.
- Approaches.
- Bottom composition.
- Current.

Cableways and Tramways

Cableways and tramways may be encountered in rugged mountainous regions and beach areas or used as connections between two primary supply routes. Cableways and tramways are considered obstacles to low flying aircraft.

Inland Waterways

The term inland waterways is applied to rivers, streams, canals, lakes, and inland seas which are used as avenues of transport. It also includes the intercoastal waterways, usually running parallel to the coastline of a landmass and sheltered to permit the navigation of small vessels. When evaluating inland waterways, analysts must consider the following factors:

- Inland waterways provide an economical form of transportation for bulk supplies, freeing faster modes for shipments of a higher priority.
- Depths of rivers and streams fluctuate with maximum and minimum rainfall.
- Falls and rapids commonly interrupt streams with fairly direct courses.
- Streams of low and uniform gradients are usually slow moving and their channels shift constantly, creating sandbars, which are a menace to navigation.
- Traffic is halted completely during a freezing period unless ice-breaking operations can be conducted.
- Thaw following a freeze may cause floods.
- Periods of drought may result in insufficient water for the movement of vessels.
- Waterway locks, bridges, cuts, dams, and other fixed facilities are vulnerable to enemy action.

Supply Systems

Utilities, services, facilities, and construction resources comprise the essential internal supply systems and installations used to protect and maintain the life of a region or city. Military interest in this field is primarily logistical, although these facilities take on greater importance during urban operations, particularly operations other than war. Analysts must report the adequacy and quality of the petroleum and natural gas facilities, as well as power, water, and telecommunications systems, to ensure their maximum use by military forces.

Power System or Grid

Electricity is essential to the life of modern regions and cities. Destruction of electrical generation and distribution facilities in most

cities would bring industrial production and most utilities and services to a halt.

Petroleum, Oils, and Lubricants Facilities

Information on a nation's petroleum and natural gas resources provides a means for evaluating the capacity of a nation to produce, process, and supply fluid or gaseous hydrocarbons for military purposes. Analysts also evaluate the petroleum supply system's vulnerability to attack.

Water

Water is the most extensively used commodity in both urban and rural habitats. Water supply systems maintain and control the quality and quantity of water in urban areas. Analysts evaluate an area's water supply system to ensure there is an adequate supply of quality water for military purposes.

Telecommunications

Analysts evaluate an area's civil and military telecommunications systems, services, facilities, and equipment for use by military forces. Governmental and commercial organizations that regulate and operate the area's systems are also evaluated. Telecommunications services evaluated include—

- Telephone.
- Telegraph.
- Teleprinter.
- Facsimile.
- Data transmission.
- Radio broadcast.
- Television broadcast.

Urban Areas

The ever-increasing urbanization of the world's population dictates that urban areas will increasingly be the AO for war and operations other than war. Urban area geospatial studies are important in the planning of operations, targeting, and logistical support for operations.

Characteristics

Knowledge of the characteristics of urban areas is essential to the conduct of civil affairs and counterintelligence operations. Urban areas are significant as military objectives, targets, and bases of operations. Often they will be the focal point for internal ethnic, class, religious, or cultural conflict. Urban areas may be one or a combination of—

- Power centers (e.g., political, economic, military).
- Industrial production centers.
- Population centers.
- Transportation centers.
- Service centers (e.g., distribution points for fuels, power, water, raw materials, food, manufactured goods).
- Cultural and scientific centers (e.g., seats of learning, modern technological developments).

Urban Area Classification

An important aspect in the classification of cities is the determination of construction type. Rarely is a city of one type of construction; instead there will be a mixture of everything from shantytowns to skyscrapers. The analyst should attempt to determine what the predominant construction type is as well as what percentages of the city are composed of varying types. Urban areas or cities are classified according to their—

- Population size and density.
- Position in the country's society, economy, and defense establishment (strategic, secondary, or minor).
- Function.
- Construction type (e.g., shantytowns, skyscrapers).

Evaluation Factors

Line of sight considerations in cities are crucial, thus the urban area must be assessed in ground-level, above-ground, and below-ground dimensions. Since urban operations are manpower intensive and generally conducted at low unit levels, the information required is usually very detailed. The MCIA-1586-005-99, *Urban Generic Information Requirements Handbook*, discusses the components of urban area analysis. The primary factors evaluated in urban area GEOINT studies include—

- Physical characteristics.
- Building construction type.
- Accessibility.
- Utilities.
- Civil facilities.
- Industrial facilities.
- Military and other important installations.
- Underground facilities (e.g., subways, sewers, underground rivers, utility tunnels).

Construction Resources

Analysts conduct construction resource studies to evaluate a foreign area's capability to support friendly military operations. To determine construction capabilities, analysts compare area construction types to the work carried out by the U.S. Army Corps of Engineers. These studies include data on—

- Available construction materials.
- Construction industry organization.
- Major construction firms, including data on the firm's—
  - Size.
  - Capital assets.
  - Organization.
  - Amount of equipment.
  - Personnel skills.
  - Experience.
  - Specialization.

SECTION VIII. POLITICAL, ECONOMIC, AND SOCIOLOGICAL ANALYSIS

The current and historical setting of a country is an important and integral part of intelligence analysis. Most of the analysis effort is expended on armed forces and GEOINT, but the factors that can make a difference in many operations, especially operations other than war, involve political, economic, and sociological aspects of the target area.

Political Intelligence

Political intelligence begins with an assessment of the internal political dynamics of a country to include its leadership, internal political stability, economic position, labor supply, physical resources, and relative military power. The first consideration is the distribution of political power—is it a democracy, an oligarchy, a dictatorship, or has political power devolved to multiple interest groups such as tribes, clans, or gangs?

Consideration must be given to the sources of political power: authority based on a legitimate constitution and the will of the people, political magnetism, skill and competence of the leaders, or brute force. It is particularly important for western-trained analysts to understand nonwestern political institutions. In other countries, institutions that on the surface are western in nature may in fact operate quite differently. For example, civil and military bureaucracies may not be neutral agents of policy but may operate almost entirely in their own self interest. Armies

may function as political parties or administrators rather than as guardians of the national security. Parliaments may have a developmental or honorary role rather than a legislative role.

The analyst must evaluate the political system as it really operates, not the way it is supposed to operate. Political analysis of a foreign country begins with an assessment of the basic principles of government, governmental operations, foreign policy, political parties, pressure groups, electoral procedures, subversive movements, as well as criminal and terrorist organizations.

Basic Governmental Principles

The starting point of political analysis is the formal political structure and procedure of a foreign nation. Analysts must evaluate—

- Constitutional and legal system.
- Legal position of the legislative, judicial, and executive branches.
- Civil and religious rights of the people.
- People's national devotion to constitutional and legal procedures.

Governmental Operations

Governments are evaluated to determine their efficiency, integrity, and stability. Information about how the government actually operates and changes in the method of operation give the intelligence user clues about the probable future of a political system. When assessing governmental operations, analysts should consider the following:

- Marked inefficiency and corruption, which differs from past patterns, may indicate an impending change in government.
- Continued inefficiency and corruption may indicate popular apathy or a populace unable to effect change.
- Increased restrictions on the electoral process and on the basic social and political rights of the people may mean the government is growing less sure of its position and survivability.

Foreign Policy

Analysis of a target country's foreign policy addresses the country's public and private stance toward the United States, foreign policy goals and objectives, regional role, and alliances. Analysts gather foreign policy data from various sources, to include—

- Diplomatic and military personnel.
- Technical collection systems.
- Official foreign government statements.
- Press releases.
- Public opinion polls.
- International businessmen.
- Academic analyses.

Political Parties

Analysts study special interest parties and groups, (e.g., labor, religious, ethnic, industry) to evaluate their—

- Aims.
- Programs.
- Degree of popular support.
- Financial backing.
- Leadership.
- Electoral procedures.

Pressure Groups

With few exceptions, most states have some type of formal or informal pressure groups. Examples include political parties, associations, religious or ethnic organizations, labor unions, even illegal organizations (e.g., banned political party). The analyst must identify these pressure groups and their aims, methods, relative power,

sources of support, and leadership. Pressure groups may have international connections, and in some cases, may be almost entirely controlled from outside the country.

Electoral Procedures

Elections range from stage shows of limited intelligence significance to a means of peaceful, organized, and scheduled revolution. In addition to the parties, personalities, and policies, the intelligence analyst must consider the circumstances surrounding the actual balloting process and changes from the historical norm.

Subversive Movements

In many countries there are clandestine organizations or guerrilla groups whose intention is to overthrow or destroy the existing government. When analysts report on subversive movements, they should include the organization's—

- Size.
- Character of membership.
- Power base within the society.
- Doctrine or beliefs system.
- Affiliated organizations.
- Key figures.
- Funding.
- Methods of operation.

Criminal and Terrorist Organizations

Criminal organizations in some countries are so powerful that they influence or dominate national governments. Analysts must examine the organization's influence or forceful methods of control. Most terrorist organizations are small, short-lived, and not attached to any government. Analysts should determine if external factors or even the area's government assists the terrorist group.

Economic Intelligence

The study of economics involves the production, distribution, and use of wealth. It analyzes the factors of production and how those factors are used to produce the things that people need and want. Economics focuses on production within nations and on relations between nations, especially on the competition for the world's scarce resources. That competition continues to be a major cause of international conflict.

Economic intelligence focuses on the use of natural and human resources, and especially on the functioning of national economies and economic relations between countries. Economic intelligence is vital to estimating the magnitude of military or other threats to ourselves and our allies. A nation can undertake and carry out only those operations, military or economic, that its economy is able to mount or sustain. In the short run, national strength consists of manpower that can be mobilized and weapons and supplies that have been manufactured or purchased.

The extraordinary expense of modern warfare means that anything beyond the briefest of campaigns will require the total economic resources of a nation. Despite the simplicity of the concept, this task is elusive and difficult.

A large nation's economic resources offer a wide range of possible actions. For example, efforts to increase military preparedness do not necessarily foretell military aggression. While it is possible to develop probability estimates based on key indicators, it would be unwise to think that analysis of economic information alone will yield completely dependable results.

Economic intelligence provides indications and warning of potential crisis or conflict. Economic failure often generates social unrest or disputes with neighboring nations. The resulting instability

may require United States or other national force intervention.

Sources of Economic Intelligence

Because nations and businesses often hide information to limit competition or to prevent the discovery of sensitive military-related technologies, the most reliable information may have to be obtained from more traditional intelligence methods such as informed reporting by attaches and officers on the scene. The most comprehensive and reliable sources of economic intelligence are printed and electronic trade and business publications. These open sources should be supplemented with reports from—

- Attaches and officers on the scene.
- Foreign broadcasts.
- Defectors.
- Commercial contacts.
- Clandestine sources.

Evaluation Factors

Analysts gather the following information for economic studies:

- Size of the area's economy.
- Sources of raw materials (e.g., minerals crucial to production of military weaponry).
- Products of the area manufacturers.
- Methods of production (e.g., advanced technologies).
- Profits from narcotics trafficking.
- Funds transfers by terrorist organizations.

Narcotics and Terrorism

Tracking profits from narcotics trafficking has been one of the most useful forms of intelligence activity against these organizations. Drugs enter the United States via a huge number of routes, but the profits exit by a more limited, and potentially traceable, number of routes. In some cases, narcotics are a country's prime resource and export. Terrorist organizations can also be tracked and studied using information on funds transfers, although the amounts tend to be smaller than those of narcotics traffickers.

Sociological Analysis

Analysts must study the way people organize their day-to-day living, including the study of groups within society, their composition, organization, purposes and habits, and the role of the individual in society. For intelligence purposes, analysts study seven sociological factors.

Population

Intelligence data derived from censuses and sample surveys describe the size, distribution, and characteristics of the population, including rate of change. Most countries now conduct censuses and publish detailed data. The U.S. Census Bureau and the United Nations are prime sources for detailed data on foreign populations. Analysts use censuses and surveys to evaluate an area's population in terms of—

- Location.
- Growth rates.
- Age and sex structure.
- Labor force.
- Military manpower.
- Migration.

Characteristics of the People

Analysts study social characteristics to determine their contribution to national cohesion or national disintegration. Social characteristics evaluated by analysts include—

- Social stratification.
- Number and distribution of languages.

- Prejudices.
- Formal and informal organizations.
- Traditions.
- Taboos.
- Nonpolitical or religious groupings and tribal or clan organizations.
- Idiosyncrasies.
- Social mobility.

Public Opinion

Key indicators of a society's goals may be found in the attitudes expressed by significant segments of the population on questions of national interest. Opinions may vary from near unanimity to a nearly uniform scattering of opinion over a wide spectrum. Analysts should sample minority opinions, especially of groups capable of pressuring the government.

Education

Analysts concentrate on the general character of education and on the quality of elementary through graduate and professional schools. Data collected for these studies include—

- Education expenditures.
- Relationship between education and other social and political characteristics.
- Education levels among the various components of society.
- Number of students studying abroad.
- Extent to which foreign languages are taught.
- Subjects taught in schools.

Religion

Religious beliefs may be a potentially dangerous friction factor for deployed U.S. personnel; this was experienced in the Middle East with fundamentalist Islamic sects. Understanding those friction factors is essential to mission accomplishment and the protection of friendly forces. Analysts evaluate data collected on an area's religions, which includes—

- Types.
- Size of denominations.
- Growth or decline rates.
- Cooperative or confrontational relationships between religions, the people they represent, and the government.
- Ways the government deals with religious organizations.
- Roles religious groups play in the national decisionmaking process.
- Religious traditions and taboos.

Public Welfare

To evaluate the general health of a population, analysts must identify—

- Health delivery systems.
- Governmental and informal welfare systems.
- Social services provided.
- Living conditions.
- Social insurance.
- Social problems that affect national strength and stability (e.g., divorce rate, slums, drug use, crime) and methods of coping with these problems.

Narcotics and Terrorism Tolerance

A population's level of tolerance for narcotics and terrorist activities depends on the relations between these organizations and the population as a whole. Analysts should determine if the tolerance is a result of the huge sums of money traffickers pump into the economy or a result of trafficker's use of force. Terrorists may be accepted and even supported by the local populace if they are perceived to be working for the good of the local people. The intelligence analyst must evaluate the way these organizations operate.

CHAPTER 7. THREAT ANALYSIS TECHNIQUES

Intelligence analysts make the greatest impact on plans and operations by conducting threat analysis. Using the IPB threat analysis techniques, analysts provide commanders and planners with paragraphs 3 through 5 of the intelligence estimate (see appendix A). To enhance the intelligence estimate, analysts use specialized analytical techniques. This chapter provides a detailed view of the knowledge essential in conducting threat analysis.

SECTION I. INTELLIGENCE PREPARATION OF THE BATTLESPACE TECHNIQUES

When conducting threat IPB, intelligence analysts evaluate the threat OOB, develop a threat model, and determine, evaluate, prioritize, and develop threat COAs.

Threat Order of Battle

An integral part of intelligence analysis, OOB is the identification, strength, command structure, and disposition of units, personnel, and equipment of foreign military forces, including irregular force units, auxiliary, insurgent, and criminal elements. The analyst must consider and integrate OOB intelligence with other METT-T factors to determine threat capabilities, vulnerabilities, intentions, and COAs.

Order of Battle Factors

The OOB analysis involves evaluating a threat force's composition, disposition, strength, tactics, training, logistics, combat effectiveness, electronic technical data, command and control warfare (C2W) data, and other supporting data.

Composition

The identification and organization of specific threat units or commands are keys to OOB intelligence. Through identification, the analyst develops a history of the threat unit's composition, tactics, training, and combat effectiveness. To determine a unit's composition, analysts identify the threat unit by—

- **Name.**
- **Number.**
- **Type.**
- **Size or strength.**
- **Subordination.**

Organization is the physical structure of a unit and the relationship of the various elements within that structure. The threat unit's identification within an organization alerts the analyst to the possible presence of other units in the same organization. With knowledge of the threat's organization, analysts can develop accurate intelligence on current strength and combat efficiency.

When analyzing composition, intelligence personnel should consider the unit's self-sufficiency. Units subordinate to a self-sufficient tactical unit, although capable of limited independent action, cannot sustain themselves over relatively long periods of time. These subordinate units are seldom employed independently or separately from the basic self-sufficient tactical unit. For example, a new threat battalion is reported to be operating in the AO. Knowing that the threat normally organizes and operates in brigades composed of three

to five battalions and that those battalions are normally not employed independently, analysts determine it is probable that the remaining elements of the threat brigade are in or near the AO.

Disposition

The threat unit's disposition consists of the unit's location and tactical or administrative deployment method. When evaluating a threat unit's disposition, analysts include the unit's current and projected movements to determine the capabilities of the enemy force and its effect on friendly mission accomplishment. A threat that has moved, is moving, or is planning to move may become capable of a number of actions (e.g., attacking, reinforcing, replacing, withdrawing). Analysts must continually monitor threat movements to integrate the threat unit's disposition with terrain analysis into doctrine and situation templates. When assessing a threat unit's disposition, analysts should consider—

- Predetermined doctrinal deployment, which may lead to an accurate appraisal of probable threat COAs.
- Knowledge of the threat's echelon arrangement may indicate which units will be employed in supporting and reserve roles.
- Patrol activity may indicate planned movement (but in itself is not movement).

Strength

A threat unit's strength is described in terms of personnel, weapons, and equipment. Information concerning enemy strength provides the commander with an indication of threat capabilities and helps determine the threat commander's probable COA. When assessing a threat's strength, analysts should consider—

- Lack of strength lowers the threat force's capabilities estimate, while superiority of strength raises the force's capabilities estimate.
- Marked concentration or buildup of units in an area may indicate a probable COA and threat objectives.
- Changes in strength of potential threat forces during peacetime may indicate the threat's intention to wage conflict.

Tactics

In OOB intelligence, tactics include tactical doctrine as well as tactics employed by specific units. While tactical doctrine refers to the threat's accepted organization and employment principles, tactics refer to the threat's conduct of operations. From tactical doctrine knowledge, the analyst can determine how the threat may employ his infantry, mechanized, armor, and artillery units in the offense and defense under various conditions. Analysts integrate tactics in doctrinal templates and other intelligence products.

Training

Individual and unit training can significantly contribute to the combat effectiveness of any military organization. Analysts assess the thoroughness, degree, and quality of individual training received by the threat's recruit, specialist, noncommissioned officer, and officer to determine the overall efficiency of its armed force. When evaluating the threat's training, analysts should consider—

- Small unit exercises to large scale training maneuvers conducted in seasonal cycles are an essential part of the training necessary for a unit to operate at its full potential.
- Each type or phase of training accomplished by a unit adds to its capabilities and effectiveness.
- Crew training for weapons systems (e.g., tanks, artillery, and aircraft) increases weapons systems effectiveness.

Logistics

The threat's adoption of a COA depends on the ability of the logistical system to support that action. With knowledge of the threat's logistic capabilities, analysts can accurately evaluate the threat's capabilities, strength, and combat effectiveness. The location of a threat unit's logistical support structure elements aids analysts in determining the disposition of maneuver formations. Logistic information critical for effective intelligence analysis includes—

- **Classes and types of supply.**
- **Lines of communication.**
- **Logistical requirements.**
- **Procurement methods.**
- **Distribution priorities and procedures.**
- **Transportation networks and modes.**
- **Installations and terminals.**
- **Evacuation and salvage procedures.**
- **Maintenance.**

Combat Effectiveness

The abilities and fighting qualities of a unit are affected by numerous tangible and intangible factors. Analysts are expected to rate threat combat effectiveness by analyzing the following factors:

- **Personnel strength, including estimated losses.**
- **Conditions and amounts of weapons and equipment.**
- **Status of training.**
- **Quality of leadership.**
- **Individuals' combat experience.**
- **Length of time a unit has been exposed to combat.**
- **Efficiency and training of the officer and noncommissioned corps.**
- **Past performance and traditions.**
- **Commander's personality traits.**
- **Morale, esprit, health, discipline, and political reliability (belief in the cause).**
- **Status of technical and logistical support of the unit.**
- **Adequacy of military schooling.**
- **Socioethnic characteristics of the people.**
- **Geographic area in which committed.**

For each unit of interest, analysts must define, evaluate, and assign a color value to each applicable factor. This assessment is highly subjective; the experience and knowledge of the analyst and the scope of available intelligence will determine its validity.

Example: Assessment Values

When evaluating the length of time a unit has been exposed to combat, analysts use the following values:

- *Green*—Sporadic to intermittent limited combat (small arms fire, fire fights).
- *Amber*—Constant limited combat to sporadic intense combat (artillery barrage, heavy weapons).
- *Red*—Sustained intense combat (deliberate attack or defense).

Where a factor has elements, analysts assign a value to each element and then synthesize an overall value for that factor. After assigning a value to each factor, analysts assign an overall combat effectiveness rating to the unit. This process is highly subjective, and allowances can be made for prioritizing or weighting the individual factors. The values assigned to factors and the definitions of the effectiveness rating may be adjusted as the situation dictates.

The values and definitions should be understood by personnel using the information and should be marked on summaries or reports disseminated outside the command.

Example: Combat Effectiveness Values

Threat unit combat effectiveness can be expressed as a color corresponding to the following example definitions. The following associated percentages are not indicators of T/O and table of equipment (T/E) strength, but are shown to indicate a relative range for each definition:

- *Green:* Combat Effective (80-100%)—The unit possesses the required resources to undertake the wartime mission for which it is organized or designed. Few, if any, negative factors exist. The unit does not require any compensation for deficiencies.
- *Amber:* Marginally Combat Effective (60-79%)—The unit possesses the required resources to undertake most of the wartime missions for which it is organized or designed. Some negative factors are present. The unit would require little, if any, compensation for deficiencies.
- *Red:* Limited Combat Effectiveness (40-59%)—The unit possesses the required resources to undertake some, but not all, of the wartime mission for which it is organized or designed. Significant negative factors are present. The unit would require significant compensation for deficiencies.
- *Black:* Combat Ineffective (less than 40%)—The unit is not prepared to undertake its wartime mission. Numerous debilitating negative factors are present.

Electronic OOB and Technical Data

Electronic OOB and other electronic technical data are required to plan and execute SIGINT, electronic warfare, CIS, C2W, and other operations against the threat. This data includes threat communications and noncommunications equipment parameters, modulation, multiplex capability, pulse duration, pulse repetition, frequency, bandwidth, associated weapons systems, and other technical characteristics of electronic emissions. The data also includes critical threat C2 nodes such as command posts, air defense operations centers, and communications relay sites.

With sufficient data, analysts can template threat emitters, which can be used to locate and develop the disposition of forces based on the forces' electronic emission assets. With electronic technical data, a more accurate evaluation of the threat's vulnerabilities to friendly EA and deception can be determined. Additionally, signals intercept and direction finding for SIGINT production are made easier and enhance support to electronic protection.

C2W Data

Analysis of C2W provides the commander with an assessment of the threat's ability to interfere with the friendly force's C2. The C2W data includes threat assets and capabilities to conduct electronic warfare, deception operations, psychological operations, and information warfare. Of increasing importance is the ability of any enemy to penetrate and disrupt friendly C2 and information systems or to deceive or jam friendly position locating devices (e.g., the global positioning system). This requires knowledge of a threat's deception capabilities, EA systems and protection measures, and monitoring capabilities.

Supporting Data

Analysts need supporting information to develop other OOB elements and comprehensive intelligence estimates. Basic intelligence describes the enemy and includes personalities' biographic data, unit history, uniforms and insignia, vehicle numbers, and other information important to mission accomplishment. Biographic data contains information on characteristics and attributes of a threat force's members. Knowledge of personalities is important in identifying units and, in some

cases, predicting a unit's COA. Personality data is valuable because the tactics and combat efficiency of particular units are closely tied to the commander's character, schooling, and personality traits. In MOOTW, supporting data may include tribal, clan, or ethnic group traits and their effects on the combat capabilities or limitations of the threat force.

Analytical Considerations

When assessing OOB factors, analysts should consider that—

- OOB factors must be analyzed as a whole.
- Changes in training status, command personality, strength, or any other OOB factors may affect a unit's tactics.
- The OOB factors form a framework for evaluation of any force.
- Extended family ties of suspected traffickers should be included when evaluating composition during a counternarcotics operation.
- The insurgent political structure and its relationship to the military elements should be included when evaluating an insurgent force.
- Composition analysis of a local terrorist organization would identify the support infrastructure among the local population.
- The OOB evaluation framework should be adapted to the mission and a unit's needs.
- An aviation unit's evaluation of composition would focus more on threat units that contain air defense assets; the equipment evaluation would focus on vulnerabilities of threat targets and technical characteristics of threat air defense systems.
- Properly maintained OOB files are sources of information on the threat's operations, capabilities, and weaknesses. See chapter 2 for a discussion of OOB files.

Threat Model Development

The threat model is a method of synthesizing information into a coherent evaluation of threat intentions and capabilities and predicting COAs. See chapter 5 for a discussion of doctrinal templates, description of preferred tactics and options, and identification of type HVTs.

Doctrinal Templates

When evaluainge doctrinal templates, analysts must—

- Determine how the threat normally organizes for combat and how he deploys and employs his maneuver units and various supporting assets.
- Look for patterns in task organization of forces, timing, distances, relative locations, groupings, or use of terrain and weather.

Doctrinal templates can also portray the threat's normal organization for combat, typical supporting elements available from higher commands, frontages, depths, boundaries, engagement areas, objective depths, and other control measures. The amount of this detail available will vary from situation to situation or may not exist at all. In the latter case, the analyst will need to rely on basic principles of war and tactics to develop an initial doctrinal template. Doctrinal templates are tailored to the needs of the unit creating them.

Description of Tactics and Options

Like the template, the description of the threat's tactics and options is developed from an evaluation of his doctrine and previous and current operations. Analysts include a description of the branches and sequels available to or preferred by the threat should the depicted operation succeed or fail. For example, the threat might prefer to follow successful attacks with pursuit. Should an attack begin to fail, his preferred branches might

include committing reserves, reinforcement, or shifting the main effort. Should the attack fail, his preferred sequel might be a hasty defense.

Analysts include decision criteria revealed in the data base that cause the threat to prefer one option over another. This intelligence will aid in wargaming threat and friendly COAs, targeting, and deception planning. When developing a threat model, analysts use the following techniques to describe tactics and options:

- Start with the scheme of maneuver and examine how each battlespace function provides support.
- Use time-event charts to describe how the threat normally conducts operations. These are particularly useful for describing large-scale air operations, which are difficult to depict graphically. With a time-event chart the time relationship between various echelons and their normal composition can be described easily.
- Make marginal notations on the graphic template and combine words with pictures to enhance understanding. Marginal notes are particularly effective when tagged to key events or positions on the template.
- Use a battlespace or warfighting function synchronization matrix (see fig. 7-1) to dissect threat operations and relate particular actions to time for threats with well-developed tactics and complex combined-arms organizations.

Time	H-10	H-1	H	H+4	H+7	H+8.5	H+10
Friendly Action	Begin move to attack position	Prepare fires	Cross line of departure	Engage 1st echelon	Defeat 1st echelon		
Enemy Decision Point							
Enemy Maneuver				Local counterattack	Close air support and attack helicopters to counterattack objective	Reserves begin move	Reserves pass NAI 9
Enemy Fire Support		Counterbattery	Engage HPTs	Defensive fires	Countermobility fires	Support reserve in engagement areas 7, 8, and 9	
Enemy Intelligence	Locate main effort	Locate artillery, identify main effort	Locate reserve, HPTs				
Enemy C2					Commit reserve to counterattack option 1 or block options 2 and 3		
Enemy Engineers	Continue counter-mobility in main battle area						

Figure 7-1. Threat Synchronization Matrix.

Identification of Type High-Value Targets

Analysts use the following techniques to identify type (e.g., air defense, engineer) HVTs for the threat model:

- Use tactical judgment when evaluating the data base, the doctrinal template, and its supporting narrative to identify HVTs.
- Mentally war game the threat operation under consideration to determine how the threat will use battlespace assets and to identify those assets critical to the operation's success.
- Identify assets necessary to satisfy decision criteria or initial adoption of the branches and sequels listed in the description and option statements.
- Determine the threat's reaction to the loss of each identified HVT. Consider his ability to substitute other assets and to adopt branches to the operation.
- Rank the set of HVTs in order of their relative value to the threat's operation, record sets as part of the threat model, and note value changes by phase of operation.
- Use a target value matrix to annotate identified HVTs in the margins of the doctrinal template. Figure 7-2 is a threat model depicting a doctrinal template, tactics and options description, and target value matrix.

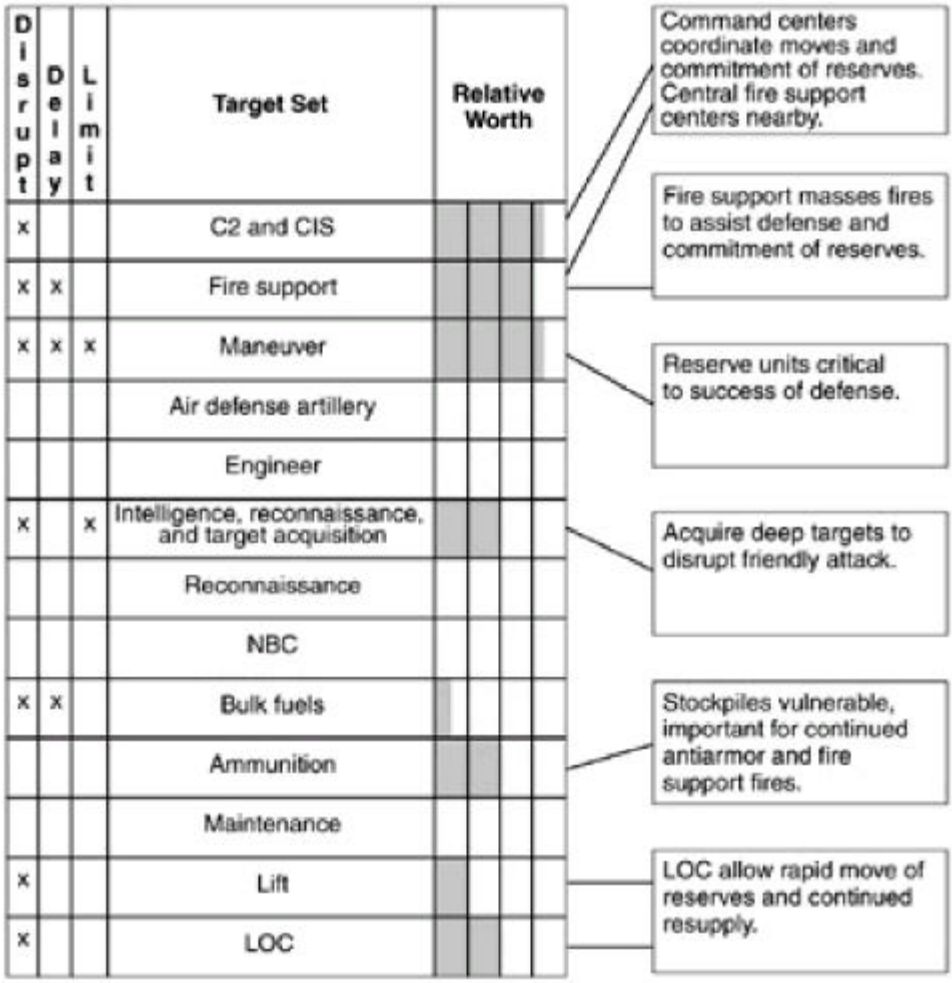


Figure 7-2. Threat Model with Target Value Matrix.

Threat Courses of Action Determination

To determine threat COAs, analysts start with general COAs open to the threat, such as deliberate attack, defend, and delay. They further define each general COA as a set of specific COAs by integrating the threat models developed in IPB process step 3 with the description of the battlespace effects from IPB process step 2.

Criteria for Testing Threat Courses of Action

Analysts must test each enemy COA using the criteria of suitability, feasibility, acceptability, uniqueness, and consistency with doctrine.

Suitability

When determining the suitability of a threat COA, analysts must evaluate the COA's potential for accomplishing the threat's objective.

Feasibility

Analysts evaluating the feasibility of a threat COA must answer the following questions:

- **Are the time and space required to execute the COA available?**
- **Does the threat have the physical means required to make the COA a success?**
- **What radical measures can he take to create the conditions for success?**

Acceptability

In determining the acceptability of a threat COA, analysts must consider the amount of risk involved by answering the following questions:

- **Will threat forces accept the amount of risk entailed in adopting the COA?**
- **Can they afford the expenditure of resources for an uncertain chance at success? (This is a subjective judgment based on knowledge of the threat and his doctrine. In some instances, the threat might undertake otherwise unfavorable COAs, particularly if they are the only means to accomplishing his objective.)**

Uniqueness

To determine the uniqueness of each threat COA, analysts must use their experience and training to answer the following questions:

- **How will the COA affect the friendly mission?**
- **Will the threat use reserves or a second echelon?**
- **Where is the threat's main effort?**
- **What is the threat's scheme of maneuver?**
- **How is the threat task-organized?**

Consistency with Doctrine and Recent Activities

When evaluating a threat COA's consistency with doctrine and recent activities, analysts must answer the following questions to be consistent with the threat's doctrine and recently observed activities, practices, and patterns.

- **Is the COA consistent with the threat's written doctrine and past application of doctrine observation, as revealed in the intelligence data base?**
- **Will the threat achieve surprise by deviating from its known doctrine?**

Considerations

To determine the COAs the threat believes are available, analysts should—

- **Consider the effect of friendly dispositions or the threat's perception of friendly dispositions on the threat's COA.**
- **Conduct reverse IPB or replicate the process the threat is employing to discern friendly COAs.**
- **Consider the intelligence and reconnaissance assets available to the threat, their ability to collect information and produce intelligence, and the picture that intelligence will give threat commanders.**

- **Focus on threat COAs that will affect accomplishment of the friendly mission and include those indications that the threat might adopt a COA that favors accomplishment of the friendly mission. This prepares the commander to take advantage of opportunities that might arise.**

Example: Threat COA That Favors Friendly Mission Accomplishmentp

If the friendly mission is to attack to destroy the threat, interfering threat COAs could be defend (including counterattacks), reinforce, and withdraw. If the friendly mission is to seize a terrain objective, interfering threat COAs could be defend (including counterattacks) and reinforce. Threat withdrawal would favor the accomplishment of this friendly mission and should also be included in the set of COAs if there are indications the threat might actually withdraw.

- **Identify less likely but viable threat COAs by considering the threat's—**
  - **Superior understanding of the political, cultural, or information characteristics of the battlespace.**
  - **Ignorance of the military arts and sciences.**
  - **Immature decisionmaking.**
  - **Uncertainty as to friendly dispositions or intent.**
  - **Unexpected objectives or desired end states.**
  - **Cultural definitions of defeat and victory.**
  - **Willingness to sustain defeat at the tactical or operational level to achieve victory at the strategic or political level.**
  - **Desperation.**
  - **Bureaucratic inefficiency.**
  - **Audacity.**

Course of Action Evaluation and Prioritization

The resulting set of COAs developed should depict the full set of options available to the threat. At this point the analyst should remember that the threat COAs identified are assumptions about the threat, not facts. For this reason, the analyst cannot predict with complete accuracy which of the COAs the threat will employ. However, the commander and staff still need to develop a plan that is optimized to one of the COAs, while allowing for contingency options if the threat chooses another COA. Therefore, the analyst must evaluate, analyze, and form an estimate for each COA and prioritize it according to how likely it is that the threat will adopt that option. The analysts must establish an initial priority list to allow the staff to plan for friendly COAs. Once the commander selects a friendly COA, the analyst may need to reorder the list of threat COAs and consider changes in the threat's perception of friendly forces.

Course of Action Development

Once the complete set of threat COAs has been identified, analysts develop each COA into as much detail as the situation requires and time allows. Analysts base the order in which each COA is developed on its probability of adoption and the commander's guidance. Each COA must answer the following five questions:

- **What—The type of operation (e.g., attack, defend, reinforce, conduct retrograde).**
- **When—The time the action will begin is usually stated in terms of the earliest time that**

the threat can adopt the COA under consideration.

- Where—The sectors, zones, axis of attack, AAs, and objectives that make up the COA.
- How—The method by which the threat will employ his assets (e.g., dispositions, location of main effort, the scheme of maneuver, and support required).
- Why—The objective or end state the threat intends to accomplish.

Course of Action Parts

Analysts consider threat forces available to at least one level of command above their own command when developing each COA. This helps to ensure accountability for possible reinforcing forces and the higher command's own objectives and intent. Each developed threat COA should contain a—

- Situation template.
- Description of the COA and options.
- Listing of HVTs.

Considerations

When considering an attacking threat, less detail is required. For example, depending on the situation, a friendly battalion might need only to work to a level of detail of threat companies. Considering the possible variations in the threat's COA based on the details of employment of individual platoons adds a tremendous amount of effort to the process, perhaps for little gain.

When considering a defending threat, a greater level of detail generally is required. For example, an attacking friendly battalion might be concerned with individual crew-served weapons positions given their relative contribution to the threat's defense.

Operations other than war will generally require a greater level of detail. The situation template may address such things as locations and movements of potential evacuees, displaced persons, or protesters as well as threats such as individual air defense systems and irregular forces. Analysts must focus on what is essential to accomplishing the friendly mission.

Course of Action Key Elements

The key elements of each COA are indicators, NAIs, and HVTs. These key elements will drive the collection and production efforts to determine which COA the threat will actually adopt. The art of identifying initial ICRs and IPRs revolves around—

- Predicting specific areas and activities which, when observed, will reveal the COA the threat has chosen.
- Determining the type intelligence products, formats, and who needs them.

As a threat force is visualized executing a COA during situation templating, analysts identify places where activity must occur if that COA is adopted. The NAIs facilitate intelligence collection, reconnaissance and surveillance, and analysis because—

- Attention is focused on areas where the enemy force must appear if the enemy has selected a particular mobility corridor or AA.
- Military significant events can be framed by time and location within the NAI.
- Events in one NAI can be compared to events occurring in the NAI of other mobility corridors as the basis for determining enemy intentions.
- Events within NAIs can be analyzed for indicators and HVTs against which intelligence and target acquisition resources can be directed.

SECTION II. SPECIALIZED ANALYTICAL TECHNIQUES

While IPB provides the overall framework and techniques for analyzing the threat, situations may dictate the use of more specialized techniques to enhance the overall product. Discussed below are a few of the more common techniques used by intelligence analysts.

Subsystem Threat Analysis

Subsystem analysis plays a major role in determining the overall posture of a threat force. Most of the products prepared during the IPB process will only partially satisfy the requirements of other staff sections and subordinate units. The targeting process may require focus on a particular aspect of the threat force. The intelligence analyst must be aware of the important threat analysis factors that specialized staff sections and units use in their IPB responsibilities. Intelligence analysts serve as the focal point for supplying information and data on a specific subsystem to other staff sections and units. Intelligence personnel assigned to specialized units discussed below will tailor their IPB efforts to the needs of their unit.

Air Defense

Evaluation

When air defense units and staffs evaluate the threat, they focus on threats posed by UAVs, cruise and ballistic missiles, fixed- and rotary-wing aircraft, and airborne and air assault forces. In addition to the broad range of OOB factors and threat capabilities, air defense staffs and units must evaluate—

- **Flight operations tactics.**
- **Ordnance types and availability.**
- **Ordnance delivery techniques (e.g., standoff ranges, release speeds and altitudes, guidance systems).**
- **Technical capabilities of aircraft (e.g., all-weather or night, maximum and minimum speeds, ceilings, range, payloads, aerial refueling).**
- **Target selection priorities for air strikes or attack by air assaults.**
- **Air strike allocation procedures.**
- **C2 and supporting CIS procedures and techniques.**
- **Navigation capabilities.**
- **Threats to friendly air defense artillery (ADA) assets, including threat ground forces and electronic warfare assets.**

COA Determination

The threat's air activities will be a part of his overall operation. Intelligence personnel begin determining the threat's air COAs by acquiring the supported command's basic IPB products, to include situation templates. Analysts evaluate the general COAs that situation templates portray and determine how the threat might support COAs with air power. When determining air COAs, analysts must consider the maneuver forces the COAs support. The employment flexibility of modern aircraft makes the determination of specific threat COAs extremely difficult. When determining the threat's air COAs, analysts should answer the following questions:

- **Where will the threat locate FARPs?**
- **When will the threat's air strikes or air assault operations occur?**
- **What are the threat's targets and objectives?**
- **What are the threat's likely air corridors and air AAs?**
- **What are the threat's strike package composition, flight profiles, and spacing in time and space, including altitudes?**

- **Where do friendly air defense assets fit into the threat COA?**
- **Will the threat ground COAs require movement of friendly ADA assets?**

Artillery

Evaluation

When evaluating the threat, the artillery unit personnel or staff should—

- **Refine standard threat models to focus on HVTs.**
- **Evaluate the threat's ability to fight the counterfire battle by—**
  - **Identifying the threat's target acquisition assets and describing their normal deployment patterns and tactics.**
  - **Describing the accuracy and timeliness of each threat target acquisition system.**
  - **Identifying CIS that moves target acquisition information to decision-makers or weapons systems, and describing the system in terms of efficiency and timeliness.**
- **Describe the threat's ability to locate and destroy friendly target acquisition assets.**
- **Use techniques associated with the rear battle to evaluate rear area threat to artillery units.**

COA Determination

When determining threat COAs, analysts—

- **Refine the threat COA models to reflect—**
  - **HVTs.**
  - **Dispositions and activity of threat fire support.**
  - **Dispositions of threat target acquisition assets.**
  - **Rear area threats to friendly units.**
- **Focus on COAs that primarily deal with counterfire against friendly assets, other aspects of force protection, and threat activities that will require friendly units to displace.**

Aviation

Evaluation

When evaluating the threat, aviation unit personnel identify—

- **Units supported by ADA assets.**
- **Types of ADA systems and their capabilities, such as—**
  - **Ranges.**
  - **Altitudes.**
  - **Engagement times.**
  - **Fusing systems.**
  - **Radars.**
  - **Countermeasures.**
  - **Range capabilities.**
  - **Altitude restrictions.**
- **Other threats such as lasers or artillery fire zones.**
- **Artificial illumination effects on target acquisition and night vision devices.**
- **Target characteristics, such as—**
  - **Normal deployment patterns.**
  - **Capability to detect attacking aircraft.**
  - **Typical reactions.**
  - **HVTs within each formation.**

COA Determination

When refining the higher command's threat COA model, analysts—

- **Include air defense system range fans.**
- **Determine where radars and weapons systems are masked by terrain.**
- **Identify areas with the least amount of air defense coverage.**
- **Identify likely threat air approaches to friendly engagement areas and battle positions.**
- **Develop situation templates for threat actions within the engagement area and include reactions to aviation attack.**

- **Identify threat units along flight paths, consider threat units' reactions, and develop appropriate situation templates.**
- **Consider threat reactions to downed pilots.**

Counterintelligence

Evaluation

When assessing the threat, counterintelligence personnel—

- **Describe the threat decisionmaking process and include descriptions of the threat's—**
  - **IPB process.**
  - **Command estimate and wargaming methods.**
  - **Techniques for selecting intelligence requirements.**
  - **Collection planning and collection management.**
  - **Asset reporting system.**
  - **Intelligence processing architecture.**
  - **Dissemination procedures.**
- **Estimate the standard lengths of the threat decision cycle for both anticipated and unanticipated decisions by answering the following questions:**
  - **How long does it take the threat staff to plan and execute a new mission?**
  - **How long does it take the threat staff to plan and execute changes to the current mission?**
  - **What is the length of time between acquisition of key indicators by collection assets and execution of that decision?**
- **Identify the collection systems available to each threat unit, develop doctrinal templates and descriptions for the standard employment of these systems, and rank each collection system in relative order of importance to standard threat operations.**

COA Determination

When formulating threat COAs, the analyst should—

- **Determine threat intelligence requirements by using the basic maneuver COA model and by answering the following questions:**
  - **What does the threat need to know to make operations successful?**
  - **Where are the decision points?**
  - **When does the threat need to know?**
- **Estimate the threat's intelligence requirements and attempt to recreate his version of the event template, matrix (NAIs and indicators), and collection plan.**
- **Develop products that show the employment of each collection system and the ensuing coverage by—**
  - **Depicting range fans for each system.**
  - **Describing the type of activity that can be collected within each range fan.**
  - **Highlighting the strengths and weaknesses of the threat collection plan.**
- **Develop a friendly event template to support counterintelligence and counterreconnaissance.**
- **Identify locations (NAIs) and activities (indicators) that confirm or deny key elements of the threat collection assumptions.**

Command and Control Warfare

Threat analysis in support of C2W can be divided into areas of threat capabilities to conduct C2W and threat vulnerabilities to C2W.

Evaluation of Capabilities

When evaluating threat C2W capabilities, the analyst should consider the threat's—

- **Ability to locate and intercept our C2 centers and agencies and supporting CIS.**
- **Targeting speed and accuracies of threat intelligence collection systems and capabilities of its production elements.**

- **EA equipment and techniques effectiveness, to include capabilities against space-based systems and computer networks.**
- **Ability to link collection systems to indirect fire systems.**
- **Range capabilities of supporting indirect fire systems.**
- **Ability to conduct deep strikes or special operation forces operations.**
- **Deception doctrine, tactics, techniques, procedures, and effectiveness.**
- **Psychological operation capabilities and effectiveness.**
- **Deployment patterns and tactics of SIGINT collection systems and EA assets, as depicted on the threat model.**
- **Deployment patterns, tactics, and range capabilities of long-range indirect fire systems, as depicted on the threat model.**
- **Techniques of intrusion or electronic deception, as depicted on the threat model.**

Evaluation of Vulnerabilities

When evaluating threat vulnerabilities to C2W, analysts consider the threat's—

- **C2 structure and CIS, with emphasis on locating key C2 nodes.**
- **Decisionmaking process and speed.**
- **Command personalities.**
- **Intelligence, reconnaissance, and target acquisition assets and their vulnerability to jamming or deception.**
- **Communications security procedures and their ability to work through or around EA.**
- **Counterintelligence effectiveness.**
- **Operations security procedures and effectiveness.**
- **Effectiveness of electronic protective measures and computer network protection.**
- **Susceptibility to psychological operations and ability to conduct counterpsychological operations.**

COA Determination

When developing threat COAs, analysts consider threat C2W capabilities and how those capabilities will be used to support specific operations. The threat command, control, and communications posture and associated vulnerabilities are considered during the identification of COGs and HVTs and contribute to development of HPTs and targeting strategies.

Engineer

Evaluation

Analysts conducting threat analysis in support of engineer planning should evaluate the threat's—

- **Engineer units' organization, standard operations, equipment, and employed tactics for conducting mobility, countermobility, survivability, obstacle placement, and breaching operations.**
- **Engineering capabilities required to lay each type of obstacle system, to breach obstacles, to entrench a type unit, and to bridge different size rivers and streams.**
- **Logistical system ability to sustain engineer operations.**
- **Weapons capabilities to penetrate friendly survivability measures and systems.**
- **Survivability techniques (e.g., use of chain-link fence to defeat antitank rounds and missiles).**
- **Engineer capabilities of threat infantry, armor, and other nonengineer units.**

COA Determination

When determining threat COAs, analysts should include engineering factors in threat models and templates. To develop situation templates for engineers, analysts use the maneuver situation

template of the supported unit and develop multiple threat engineer COAs that include—

- An engineer status estimate, which includes the percentage of combat vehicles with entrenched primary, alternate, supplementary, and deception positions and the extent of likely obstacle system measures.
- Likely locations and obstacle systems required to support, disrupt, turn, fix, or block defensive measures.
- A mobility support estimate, which includes the maneuver and supporting engineer detachments' breaching and fording capabilities.

Combat Service Support

Evaluation

When conducting threat analysis in support of CSS staffs and units, analysts should include—

- Regular threat formations, particularly reserves or second echelon units, that might penetrate main defenses or conduct counterattacks through CSS areas.
- Details on air assault, airborne, unconventional warfare, and light infantry forces and their means of infiltration (e.g., air, ground, and sea).
- Insurgent and partisan forces.
- Terrorist organizations.
- Criminal organizations.

COA Determination

When preparing threat models in support of CSS units, analysts include—

- Air assault, airborne, and light infantry techniques for deep attack.
- Unconventional warfare techniques for deep operations.
- Standard procedures for insurgent raids and ambushes.
- Typical procedures for terrorist attacks.
- Targets and methods of operations for criminal organizations.

COA Development

When evaluating threat COAs, the analyst should consider each maneuver COA available to the threat and develop multiple CSS COAs that include—

- Likely areas of penetration for ground forces.
- Likely objectives in the rear area that will facilitate the threat's main attack or defense.
- The HVTs and HPTs (e.g., key terrain, specified CSS activities) that the threat will identify to support their concepts of operations.
- Situation templates for air assault and airborne operations (e.g., air avenues to LZs and DZs, infiltration lanes, exfiltration lanes).
- Insurgent or partisan activities (e.g., assembly and hide areas, infiltration routes, objective actions, exfiltration).
- Terrorist and sabotage activities.

Pattern Analysis

Pattern analysis is the process of careful observation and evaluation of threat activities to deduce the doctrinal principals and techniques, tactics, and procedures that threat forces or groups prefer to employ. When faced by an opponent whose doctrine is unknown or undeveloped, the intelligence analyst must use pattern analysis to create or update threat models and doctrinal templates. This form of analysis is used in operations other than war, such as counterinsurgency, peacekeeping, or even humanitarian assistance operations. The coordinates register and pattern analysis plot sheet are used to develop threat models when it is necessary to determine threat operational patterns.

Coordinates Register

Sometimes referred to as an incident map, a coordinates register illustrates cumulative events that have occurred within the AO (see fig. 7-3). Coordinates registers focus on where an event occurred, but it can contain additional information as the situation dictates. The date and time of the incident are recorded next to the location. As reports of individual events or sightings are recorded, the analyst attempts to identify links between the location and time of those events. What may appear to be random events will often develop into coordinated actions. When time lined and illustrated, these events form patterns that provide the basis for developing threat models and doctrinal templates. Although the time of the event is normally recorded on the coordinates register, it should always be used with the pattern analysis plot sheet and the doctrinal template, if developed.

Pattern Analysis Plot Sheet

The pattern analysis plot sheet focuses on the time and date each incident occurs in the AO. In figure 7-4, the rings depict the days of the month and the radial segments depict the hours of the day. Events are recorded using the same alphanumeric designator as was used on the coordinates register to allow easy cross-referencing. Along the right side of the plot sheet, the events are recorded by the day and date they occurred. By organizing the events in this manner, it is possible to identify the times of the day and days of the

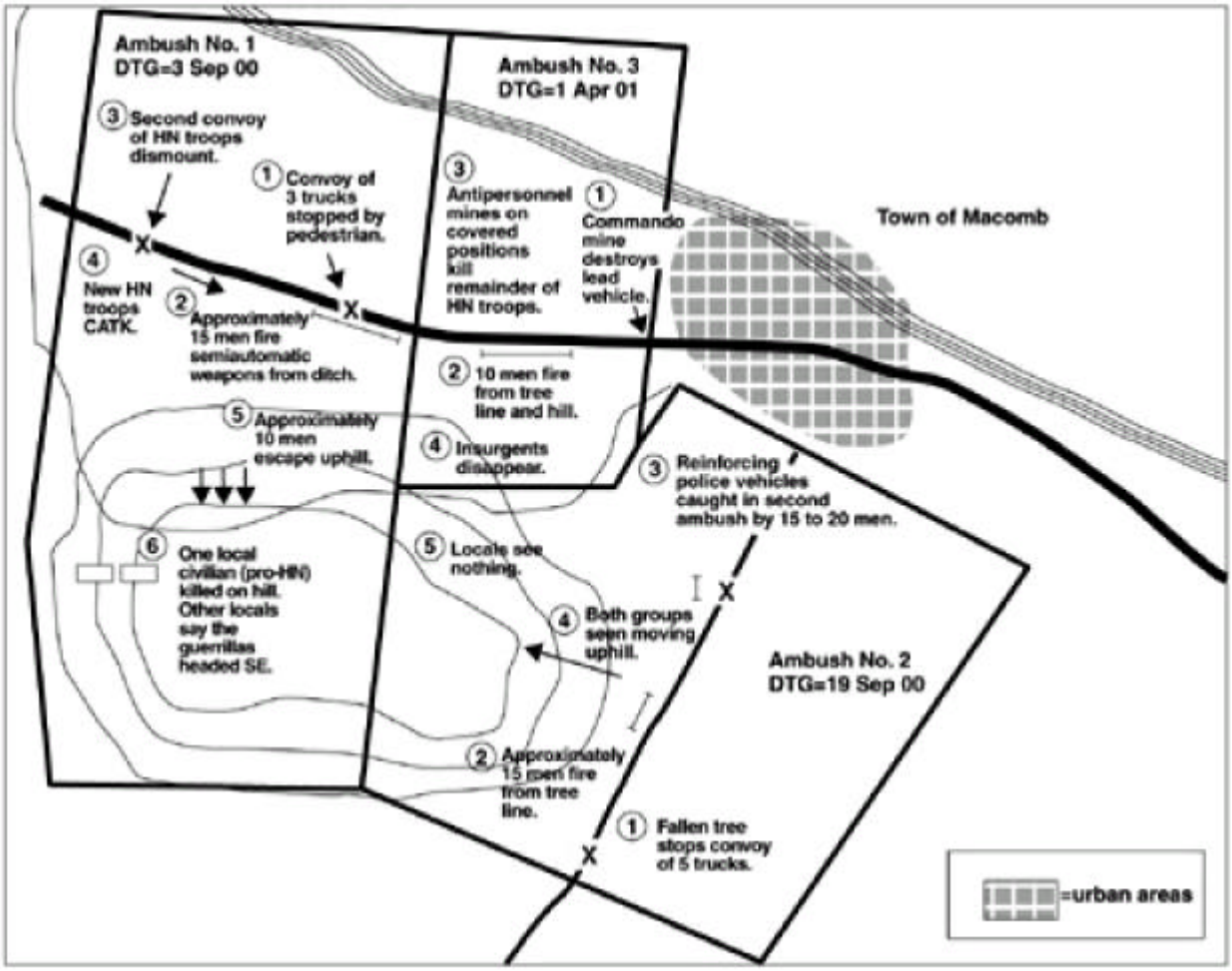


Figure 7-3. Coordinates Register.

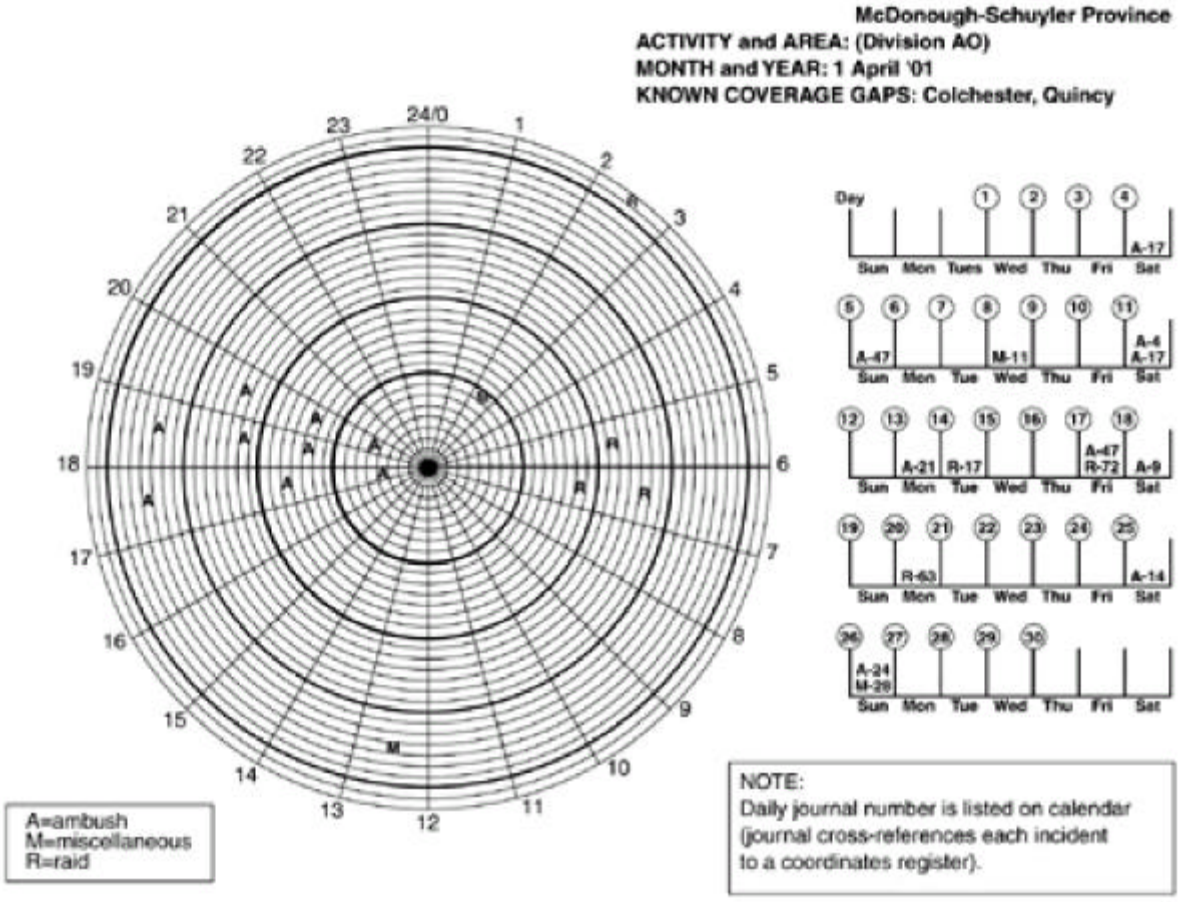


Figure 7-4. Pattern Analysis Plot Sheet.

week or month when threat activities occur. Used in conjunction with the coordinates register, the pattern analysis plot sheet identifies where, when, and how past actions occurred. This allows the analyst to use information derived from the coordinates register and pattern analysis plot sheet, to develop threat models and doctrinal templates, and to predict potential threat activity.

Matrix Analysis

Constructing a matrix is a simple, graphical way to organize a large volume of complex data. Matrices are used to show relationships between numbers of entities, such as people, incidents, organizations, weapons, locations, functions, and actions. Analysts use activities and association matrices to organize a large volume of complex data, particularly in cases where the tracking of individuals and organizations is emphasized. Activities and association matrices are useful in analyzing insurgent, terrorist, criminal or drug trafficking activity.

Activities Matrix

Analysts use the activities matrix to link people to events or organizations. An activities matrix quickly displays which notable personnel within the AO are related to a particular organization or type of activity. This matrix can also link certain activities or incidents within the AO with organizations or units.

In figure 7-5, individuals are listed down one side, with organizations listed across the top. Reported relationships are noted on an individual's row that intersects the appropriate organization's column. This example demonstrates the use of dots to signify the confirmed, possible, or probable certainty of the relationship. The absence of a dot indicates either no relationship or a lack of information. The system used must be explained in a legend. To complete this particular example, the analyst created a remarks column to record significant information regarding each individual.

● – confirmed ◎ – probable
○ – possible

Remarks		Christian Reform Party (good guys)	Society for the Preservation of Order (SPO) (right wingers)	Farmer's Alliance (unknown peasant group)	People's Democratic Society (peaceful moderate)	Insurgent Company	New Liberation Movement (political front for New Metropolitan Edict [NME])	NME	Name of Individual	
Warrant Outstanding	Leader in the insurgent company. Possible platoon commander or company commander.					●	●	●	Johnston, S. D. alias "The Red"	
	Possibly linked to death squad activities.	●	◎						Garra, N. A.	Randolph
	Mayor, ineffective due to war-torn town.	●							Mulvhill, P.	
	Possible platoon leader.	○		●	◎	○	○		Daniels, P.	
	Regional governor.	◎	○	◎	●				Jenkins, T. L.	Malcolm
Warrant Outstanding	Tactical genius, principal trainer of insurgent company.					●	●	◎	Cornier, J.	
				○		◎	◎	◎	Webb, C.	
					◎	○	○		Seipel, B.	
	Leader in the insurgent company. Platoon leader or executive officer.			○		◎	◎	◎	Trollinger, L.	
	Possible head of intelligence.					○	●	●	Ahearn, E.	Beards town
	Probable platoon leader.					◎	○		Timoney, J.	
Warrant						●	●		Thompson, J.	
Warrant	Probable heavy weapons platoon leader.					●	○	●	Bridgeford, R.	
	Possible liaison between insurgent company and the NME			◎	○	○		○	Halbleib, M.	
	"Doctor of Death" leads the SPO.	●	●	○	○				Mueller, H.	Bushnell
Warrant						●	◎	◎	Martinez, E.	

Figure 7-5. Activities Matrix.

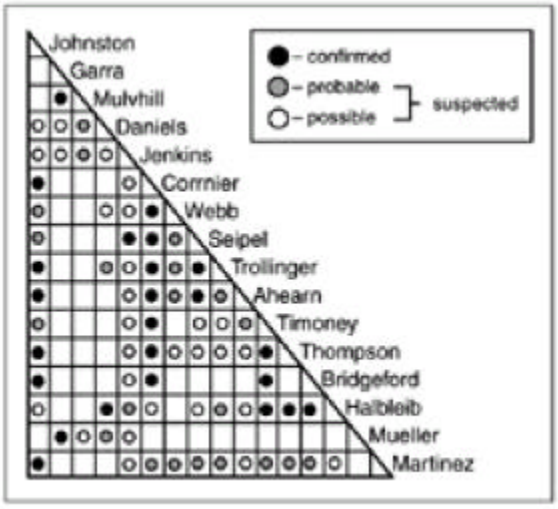


Figure 7-6. Association Matrix.

Association Matrix

The association matrix is used to show relationships between individuals. In figure 7-6, the individual names constitute both a column and a row. A dot indicates that a relationship exists. Through the use of the activities matrix, analysts note individuals that are members of the same organization and indicate the relationship on the association matrix.

Link Analysis

Link analysis is a method of evaluating and displaying relationships and activities information that has been organized into matrices. In link analysis, pictures or symbols are used to display intelligence data that depicts relationships between people or entities. Analysts assess the reliability and validity of the intelligence data and assemble a link diagram to gain greater insight into the construction of a relationship network.

In figure 7-7, the link analysis diagram uses circles to represent people, squares or rectangles to represent organizations, and lines to represent their connections. Solid lines represent confirmed or strong relationships, while dashed lines indicate suspected or weak relationships. When

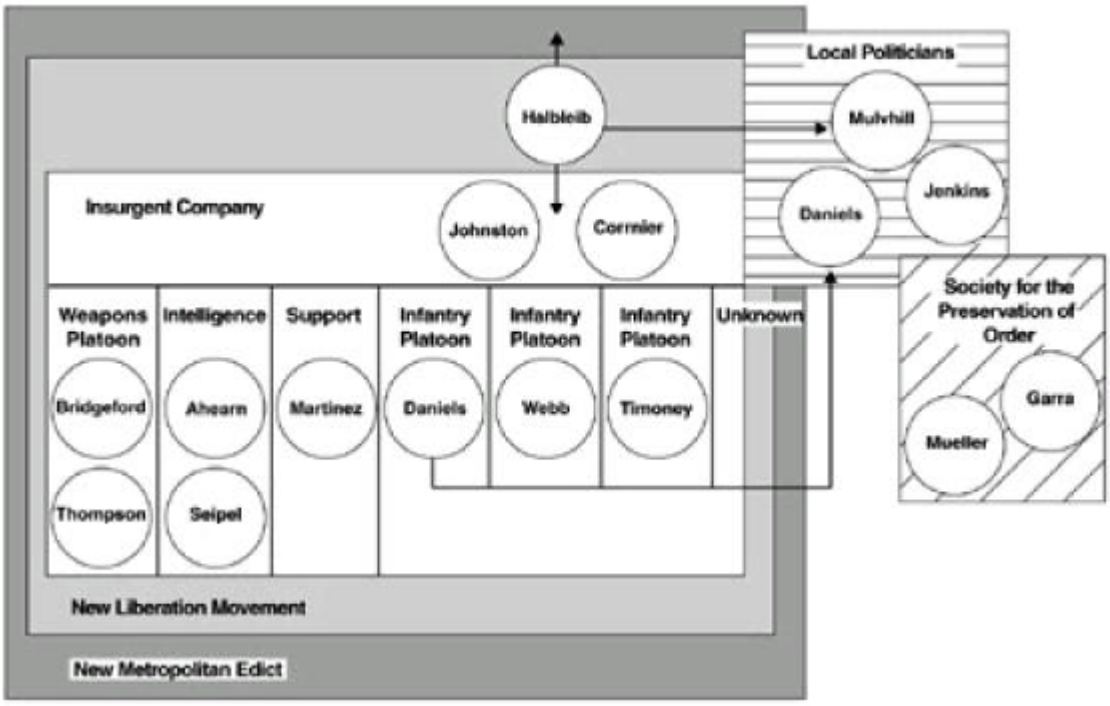


Figure 7-7. Link Diagram.

the analyst suspects that two people are actually the same person, the circles are overlapped. Circles and lines should be arranged so that their relationship lines do not cross. In complex cases, such as large groups, the circles should be arranged to keep the number of relationship-line intersections to a minimum.

The relationship of an individual to an organization can be shown a number of ways. When an individual is confirmed to belong to an organization, that individual's circle is placed within the organization's rectangle. By overlapping organizations, the analyst shows that an individual belongs to more than one organization and that there is a connection between the two organizations.

In cases where an individual is connected to but not a member of an organization, a line is drawn from the individual outside the organization to the rectangle representing the organization. If an individual's contact within the organization has been confirmed, the relationship line would be drawn between the circles representing the individuals.

Indicator List

The activities that reveal a COA are called indicators. Indicators are essential to discerning threat intentions. The analyst uses indicators to cross-reference specific events and activities with probable threat COAs and intentions. When used with other analytical tools (e.g., threat models, event templates, pattern analysis, matrices, and link diagrams), indicators are the key to estimative intelligence. During IPB, indicators are developed for each NAI to focus collection and analysis efforts. This list of indicators is constructed to satisfy the commander and staff's PIRs and IRs.

Indicator lists are formed by asking questions. Intelligence analysts develop a list of threat indicators by focusing on METT-T questions. Using METT-T, analysts determine what the threat must do and define the threat's probable activities (see the example below). These determinations become indications and warning.

Example: Forming an Indicator List Using METT-T

PIR: Will the threat defend objective C using a reverse-slope defense between 230600 to 270800 hours?

Mission: What does the threat commander accomplish by forming a reverse-slope defense?

Enemy: What types of units are available to conduct the defense? What units are necessary to construct and aid in the defense?

Troops and Support: Are threat troops experienced in reverse-slope techniques? What is their SOP for reverse-slope defense?

Terrain and Weather: Is objective C suitable terrain for a reverse-slope defense? If so, where is the most suitable terrain?

Time Available: How long will it take to develop a prepared defense versus a hasty defense? Will threat forces be able to prepare or assume a defense in the specified time period?

To further develop the indicator list, analysts can refine the questions developed using METT-T by breaking them down by battlespace functions. Information based on IPB, OOB factors, and experience aids intelligence analysts in deriving lists of activities that answer the commander's PIRs. These questions serve to narrow and focus on certain activities, equipment, troops, and training which an adversary must possess or do to accomplish their mission. For a representative listing of common tactical level indicators, see appendix C.

CHAPTER 8. TARGET DEVELOPMENT AND COMBAT ASSESSMENT

Successful MAGTF operations depend on an efficient, organized targeting effort to affect those enemy capabilities that could interfere with achievement of the friendly mission and objectives. The targeting process of detecting, selecting, and prioritizing targets requires coordinated interaction between intelligence, maneuver, fires, and planning elements of the MAGTF, joint force commander (JFC), Service components, and supporting agencies. This chapter introduces the targeting cycle, intelligence targeting support, the analyst's role in target development, and combat assessment.

SECTION I. TARGETING

Based on the friendly scheme of maneuver and tactical plans, targeting includes an assessment of the weather, terrain, and enemy to identify those enemy formations, equipment, facilities, and terrain which when attacked or controlled will ensure success. Through the targeting process, analysts develop a prioritized list of targets to be attacked and determine the weapons required to achieve the desired effects.

Targeting Cycle

Defined as deliberate or reactive, targeting is an integral part of the planning process that begins with receipt of the mission and continues through the development of the approved plan. Deliberate targeting is associated with fixed or semi-fixed targets, while reactive targeting is associated with mobile targets. Whether deliberate or reactive, the targeting cycle integrates intelligence, maneuver, fires, and C2 processes to assist the commander in deciding which targets to engage when, where, and to what effect.

Through the targeting cycle, fires planners and targeteers derive nomination lists of forces, installations, or locations that if attacked will promote the commander's warfighting objectives. The higher the command level performing the targeting process, the more formal it becomes and the more the process focuses on events well in the future. At the MAGTF or joint force level, the targeting cycle tends to be deliberate, encompasses greater resources, and involves—

- **Establishment of commander's objectives, guidance, and intent.**
- **Target development, nomination, validation, and prioritization.**
- **Capabilities analysis.**
- **Commander's decision and force assignment.**
- **Mission planning execution.**
- **Combat assessment.**

At lower tactical levels, the same process tends to be reactive, occurs in a shorter time span with less formality, and focuses on events of an immediate nature. The tactical-level targeting cycle is simplified to decide, detect, deliver, and assess

(D3A). Figure 8-1 depicts the joint targeting cycle and its relationship to D3A. Although intelligence is an integral part of each targeting cycle phase, intelligence P&A directly affects target development (decide) and effects assessment (assess).

Target Development

Target development is the analysis of potential enemy military, political, or economic systems to determine their significance and relevance to the commander's objectives, guidance, and intent. The analysis proceeds from broad systems to specific components and finally to individual elements or aim points. Analysts evaluate system components and interrelationships to establish their criticality to the threat's operation and their vulnerability to attack. Through this systematic evaluation, analysts develop targeting strategies to select potential targets and to determine the type of damage that will accomplish the friendly commander's defined objective. Objective definition and target development must comply with the commander's guidance, law of armed conflict, and rules of engagement.

Analysts evaluate each target's lethal and nonlethal capabilities to develop a prioritized list of targets and the intelligence requirements that support target acquisition and combat assessment. The scope, level of detail, and time involved depend on the situation and the level of command conducting targeting. Common processes and procedures employed in target development include IPB, target value analysis, HPT identification, and use of the high-payoff target list (HPTL).

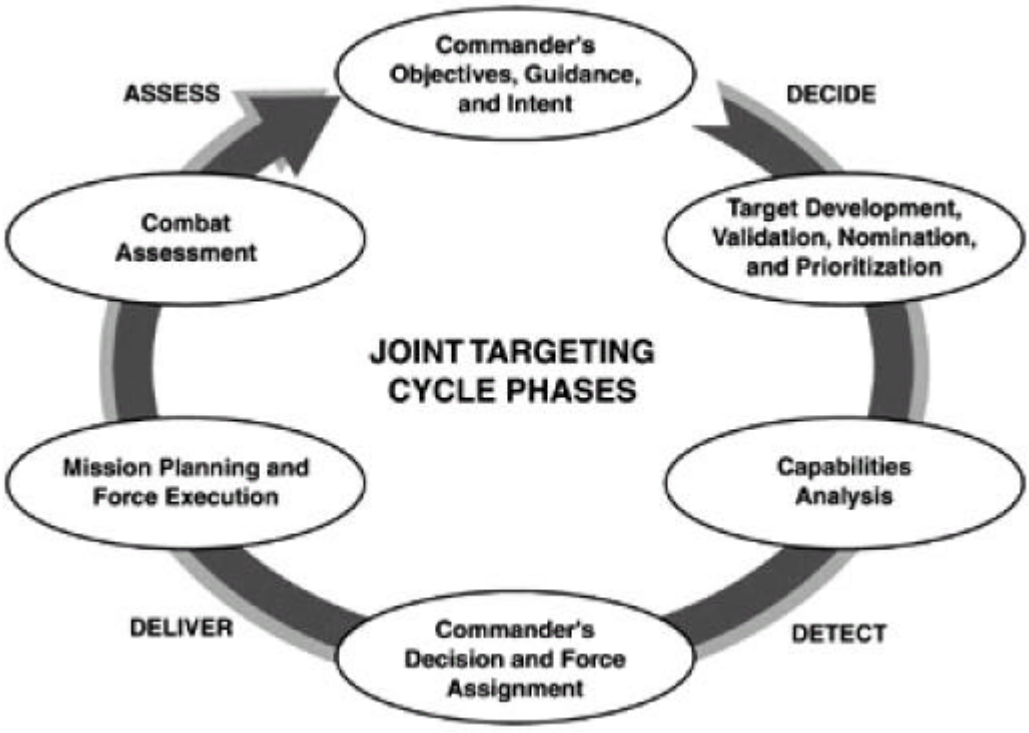


Figure 8-1. Joint Targeting Cycle and D3A.

Intelligence Preparation of the Battlespace

Through the IPB process, intelligence analysts contribute to target development by—

- Determining the threat commander's COAs through systematic analysis of the region, weather, terrain, and doctrine.
- Evaluating doctrinal templates to identify a threat's COGs, critical vulnerabilities, and HVTs.
- Constructing situation templates and examining the threat commander's decision cycle and each potential COA's decision points to refine HVTs.
- Wargaming, mentally, each COA and the threat commander's decisions to identify his key assets as HVTs.
- Developing event and decision support templates to help identify NAIs, decision points, decision phase lines, TAIs, and HPTs.
- Analyzing the threat's target systems, complexes, and components to develop their relevance and importance.

Target Value Analysis

Target value analysis is a method of identifying and ranking potential HVT sets in a COA. The target analyst, in coordination with the G-3/S-3, G-2/S-2, fire support coordinator, and other staff members, war game the COAs to—

- Finalize individual staff estimates.
- Develop a fire support plan, a scheme of maneuver, as well as friendly and threat decision support templates.
- Determine critical assets required by the threat commander to accomplish his mission.

High-Value and High-Payoff Target Identification

An HVT is an asset that the threat commander requires for the successful completion of a mission. Its loss to the threat can be expected to contribute to substantial degradation of an important battlespace function. Contributing to the targeting development process, G-2/S-2 section personnel, the fire support coordinator, and other staff members identify key threat assets that must be dealt with and nominate HVTs to be HPTs. The key to HPTs is that they are based on the friendly commander's scheme of maneuver.

The HPTs are developed during the wargaming process. As the staff fights the different options, the G-2/S-2 identifies specific HVTs. The HPTs for a specific phase of the battle are recorded on the decision support template and synchronization matrix. Those locations where HPTs are expected to appear become TAIs.

The G-2/S-2 and/or collection manager evaluate HVTs at different points in the battle to determine required collection asset capabilities and to provide the necessary target resolution. This evaluation becomes the basis for the collection plan for intelligence support to targeting. Because of their importance, HPTs receive priority in the allocation of detection systems. The G-2/S-2 and the commander must consider the impact the priority will have on maintaining situational awareness, because the same collection assets are used for targeting and battlespace awareness.

The fire support coordinator, air officer, electronic warfare officer, C2W and other representatives use their knowledge of friendly lethal and nonlethal means to determine if a capability exists to attack the HVT and the expected effects of the attack. The G-2/S-2 then assesses the threat response. This effects-based targeting assessment sequence helps determine if attacking the HVT is necessary to ensure the success of the friendly force. If the HVT is acquirable, attackable, and capable of ensuring friendly success, it becomes an HPT. The HPTL identifies prioritized HPTs for a specific battle point.

High-Payoff Target List

The commander-approved HPTL is a tool in determining attack guidance and in developing targeting intelligence collection, production, and dissemination plans.

Collection

Collection efforts focus on NAIs and TAIs that the IPB process identifies during the decide phase. Knowledge of target type and its associated signatures (electronic, visual, thermal) enables friendly forces to direct the most capable collection asset to be tasked against the target. The asset is positioned in the best location based on friendly estimates of when and where the threat target is located.

The decision to destroy, degrade, disrupt, or delay a given HPT results in a requirement to detect that target. Intelligence needs to support the detection of the target are expressed as PIRs and IRs. The PIRs and IRs that support detection of a target are incorporated into the collection plan. The collection manager translates the PIRs and IRs into ICRs and supporting specific IRs. The collection manager considers the availability and capability of MAGTF and external collection assets.

Production

Production efforts focus on developing timely, tailored intelligence products to meet maneuver and fires needs.

Dissemination

Dissemination efforts focus on ensuring CIS readiness to support both routine and time-sensitive intelligence reporting in support of MAGTF targeting needs.

Target Analysis

Target analysis helps to determine the military importance, priority of attack, scale of effort, and weapons required to obtain a desired level of damage or casualties. Other considerations for analysis include target criticality, accessibility, and recognizability. While target analysis helps to determine which targets to hit, operations planning determines how to do it. At strategic and operational levels of war, targeting is more deliberate and focuses on fixed installations or large arrays of targets.

At the tactical level, the MAGTF commander has capabilities to strike deep targets that support threat maneuver or ground forces. These targets are often complex groupings of installations, units, and defenses that may require a methodical approach to ensure success. This methodology is referred to as target system analysis.

Target System Analysis

A target system includes installations, facilities, or forces that are functionally related and situated in the same geographical area. A target system comprised of components and elements can be either fixed installations or mobile target sets. While an individual target may be significant based on its characteristics, its worth is usually derived from its relative importance within the target system. Target system elements are smaller, more intricate parts of the target system than the component and are necessary to the operation of the component. Figure 8-2 depicts the relationship of a target system, its components, and its elements.

Components

A target system's components can also be targets, such as airfields, which are a component of an air defense system. Within industrial or economic systems, a system component belongs to one or more groups of industries or basic utilities

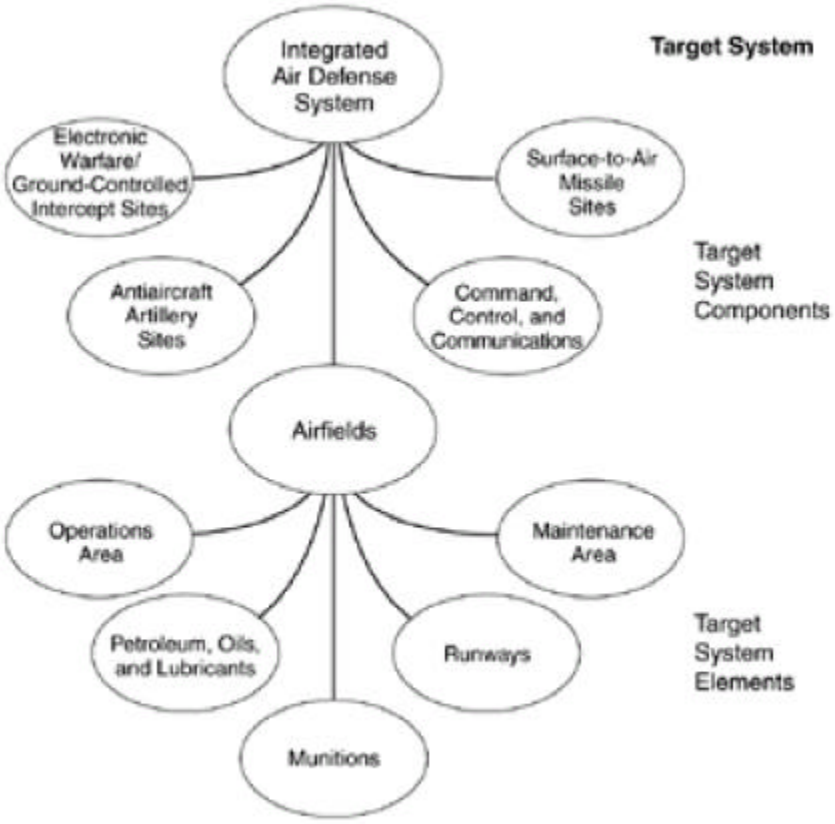


Figure 8-2. Target System, Components, and Elements.

required to produce individual parts of an end product. Target system components can also refer to component services. For example, an air defense system may include C2, early warning and target acquisition radars, antiaircraft artillery and surface-to-air missile batteries, support facilities, and other components that are neither industries nor utilities.

Activity

Target system activities encompass those actions or functions performed by the target system components in pursuit of system goals. By this definition, a combined-arms maneuver division could be viewed as a target system, with components that include air defense units, artillery, armor, mechanized infantry, and engineers. The target development process should focus on the activity of the system or its components. Analysts conduct a comprehensive evaluation of target system components and elements to understand the activities of the total system.

Once analysts have identified the enemy activity that must be affected or defeated, they can determine the key target systems, components, or elements that should be attacked, degraded, or exploited to produce the desired effects. For example, enemy air attacks against friendly ports and LOCs may seriously threaten resupply of friendly forces. To modify or defeat this enemy activity, targeteers analyze the enemy's air force system and identify threat system components and elements. They target the enemy aircraft home bases and identify runways; petroleum, oils, and lubricants storage; and maintenance facilities as potential target elements, which

friendly forces should modify to defeat the enemy's air attack activities.

Linkage

Analysts must understand the linkage or connection between installations performing identical, similar, related, or complementary activities or functions. To develop targets, analysts identify critical nodes or points where target system components and elements are linked and dependent upon each other. These key nodes also exist where target systems interact with other target systems. Matrix and link analysis, as discussed in chapter 7, are highly effective tools for determining linkages and critical nodes.

Target development focuses on identifying the critical nodes within target systems that will satisfy objectives. For example, an enemy's air defense system consists of a number of components, such as surface-to-air missile sites, early warning and ground-controlled intercept sites, antiaircraft artillery sites, and airfields. To function effectively, the elements are linked at a sector headquarters, which exercises responsibility for a specific geographic area. Analysts would target these sector headquarters to sever the critical node within the air defense system.

Target Complex Analysis

A complex is a group of physical elements in close proximity containing multiple target elements that are integrated to contribute to some function of military or civilian value. For example, a system of military airfields distributed throughout the country is made up of individual airfields (e.g., target complexes), containing multiple elements (e.g., individual aircraft, runways, hangars) in close proximity.

After target system analysis identifies a critical target complex, target complex analysis identifies the target environment and defenses associated with the complex. Target complex analysis is used to determine specific targets within the complex as well as supporting actions (e.g., defense, suppression, deception, tactics) that may be necessary to attack the target.

Target Element Analysis

A target element is the smallest identifiable activity of a target component (e.g., sheltered aircraft, control tower, defensive radar site). Based on the targeting objectives, target elements are evaluated as targets for attack. Detailed analysis must be conducted on the individual target element. When conducting target element analysis, the target intelligence officer is responsible for evaluating the element's—

- Location—Exact location expressed in geographic or UTM coordinates.
- Elevation—Altitude above sea level of the element's ground location expressed in feet or meters.
- Identification—Accurate determination of—
  - Type—Brief description of the target's military functions.
  - Size—Length, width, and height dimensions.
  - Shape—Definition of the spatial form.
  - Attitude—Azimuth of the element's long axis expressed in degrees (090-270) or descriptive words (east-west).
  - Dispersion—Pattern of individual elements in the target area expressed as a short word-picture description.
- Vulnerability—Susceptibility to fire.
- Recuperability—Time required for enemy to reactivate the target or reconstitute it in another location.
- Importance—Value within the enemy's operation and degree to which destruction of the potential target would reduce the enemy's capability.

Role of the Target Analyst

Target analysts should complete the following steps when conducting target P&A:

- Collect target information and intelligence.
- Collate data.
- Evaluate potential list of targets.
- Construct flow of threat target component, complex, and system.
- Determine most suitable targets.
- List targets and priorities.
- Present recommendation.
- Refine data and develop required intelligence products.

Target Analysis Products

Analysis products used in target development include a target list, no-strike target list, restricted target list, target files, and collection requirements.

List of Targets

Target intelligence analysts conduct a thorough analysis of targets and coordinate with the other P&A personnel and the G-3/S-3 maneuver and fires targeting team to provide required intelligence supporting the list of targets for the commander's consideration. The fire support coordinator maintains and prioritizes the list of targets in order of relative importance to the commander's objectives. The operations section and ultimately the commander are responsible for validation of targets and formulation of the commander's target list, which is derived from the HPTL developed during IPB and COA wargaming.

No-Strike Target List

During the target validation process that occurs during target development, some potential targets are placed on a no-strike list. Commanders designate no-strike targets, which are prohibited from attack, to avoid—

- Interference with military operations.
- Damage to relations with indigenous personnel or governments.
- Violation of international law, conventions, or agreements.

No-strike lists are nominated by elements of the joint force and approved by the JFC. This list also includes no-strike targets directed by higher authorities. Examples of no-strike targets include—

- Hospitals.
- Schools.
- Places of worship.
- Cultural shrines.

Restricted Target List

This list is composed of targets with specific restrictions. Actions exceeding those restrictions must be coordinated with the establishing headquarters. Restricted targets are nominated by elements of the joint force and approved by the JFC. This list also contains restricted targets directed by higher authorities. The decision to restrict a target centers on the importance of the target to the threat and the plans and intentions of the friendly commander. The following are examples of restricted targets:

- An area in which a friendly reconnaissance team is operating. To avoid fratricide, fires may be placed into the area, but only upon coordination with the establishing headquarters.

- A bridge identified by a commander as critical to future operations. To ensure the bridge is available to friendly forces, this target may be restricted as to the type of ordnance that can be used against it or the level of damage that may be inflicted on it.

Target File

A target file contains pertinent target system, complex, or component information collected during the target development process. Information in the target file is used to build target studies once HPTs are approved or validated. Generally, target files deal with fixed or semi-fixed targets. This information may be in the form of—

- Data bases.
- Selected imagery.
- Graphics.

Collection Requirements

Throughout the target analysis process, analysts identify targeting intelligence gaps and develop ICRs to obtain needed data. The ICRs must be stated early and clearly in the form of PIRs, IRs, and specific IRs. Analysts and planners have to think beyond the traditional picture (i.e., imagery) and use intelligence sources such as SIGINT, HUMINT (i.e., defectors, refugees, prisoners of war, travelers, aircrew debriefs, and special forces), and other sensor data that can provide indications of a target's status. Gaining a familiarity with collection system capabilities is critical. Requesters should recognize the various intelligence sources' strengths and limitations and understand how to best exploit them.

Target or Objective Studies

Once the commander approves a target, intelligence sections develop target or objective studies to support mission planning. These studies are focused, detailed intelligence products that aid in the application of fires or the maneuver of forces against a specific target set or area. Smaller MAGTFs and units use these studies for mission preparation and execution.

Target or objective studies are graphically oriented and may use many of the graphics derived during the IPB process, such as a target folder. Depending on the specific mission, the study may contain the following information:

- Orientation graphic.
- Time-distance graphic.
- Weather forecast.
- Hydrographic forecast and astronomical data.
- Intelligence briefing notes for mission.
- Graphic intelligence summary.
- Objective area graphic enhancements, such as—
  - Orientation graphic (10–20 km around objective).
  - Mission planning graphic (5 km around objective).
- Objective area imagery.
- Imagery and graphics of insertion points.
- Survival, evasion, resistance, escape plan.
- Challenge and reply passwords.
- Mission-specific data as required.

SECTION II. COMBAT ASSESSMENT

The final step of the targeting cycle, combat assessment is the determination of force and weapons system employment effectiveness during military operations. The combat assessment objective is to identify recommendations for the course of military operations. A G-3/S-3 responsibility, combat

assessment is performed as a coordinated effort by the operations, intelligence, and fires staffs. Conducted at strategic, operational, and tactical levels of war and MOOTW, the combat assessment process is used by analysts to—

- Provide the commander with information on the status of an operation.
- Help formulate subsequent battle plans.
- Serve as a benchmark for validating objectives.
- Collect data on weapons and weapons system performance.

The three components of combat assessment are BDA, munitions effects assessment (MEA), and reattack recommendations (RR). Intelligence analysis has a major role in determining BDA, which includes physical damage, functional damage, and target assessment (see fig. 8-3).

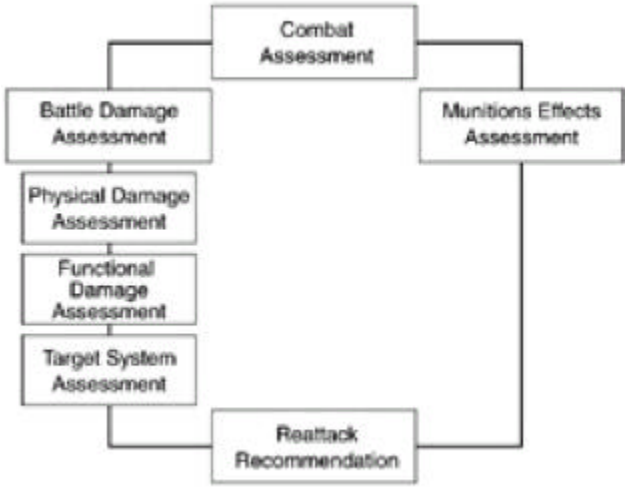


Figure 8-3. Combat Assessment Process.

Battle Damage Assessment

A key component of the combat assessment process, BDA is the timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against an objective or target. Primarily an intelligence responsibility, BDA requires extensive coordination with operations and fires elements. The BDA is munitions-independent (air, ground, naval, and special forces weapon systems) and is target-independent (fixed strategic and mobile or movable tactical targets).

Munitions Effects Assessment

Munitions effects assessment is analysis of the friendly military force in terms of the weapons system, munitions, and weapon delivery parameters to increase force effectiveness. While the operations and fires staffs are responsible for MEA, the MEA is conducted concurrently and interactively with BDA, which is conducted by the intelligence staff.

Reattack Recommendations

Based on results of BDA and MEA, the operations and intelligence team make RRs for the target nomination and development process. The RRs should address operational objectives relative to the target, target critical elements, and enemy combat forces. When making RRs, the operations and intelligence team considers the—

- Current level of achieved operational and tactical objectives.
- Weapons systems and munitions.
- Target and aimpoint selection.
- Attack timing.

Battle Damage Assessment Components

Physical damage assessment (PDA), functional damage assessment (FDA), and target system assessment (TSA) are three subcomponents of BDA.

Physical Damage Assessment

Referred to as Phase I BDA, the PDA is a quantitative estimate of physical damage that occurs to a target through munitions blast, fragmentation, and fires. This assessment is based on observed or interpreted damage.

The unit controlling the weapons system and the intelligence collection observers develop Phase I BDA reports. Figure 8-4 illustrates the flow of Phase I BDA.

For example, visual observation of an enemy artillery battery (the target) verifies four self-propelled howitzers with shattered and dislodged tubes, recoil mechanisms, and turrets. Track damage to one howitzer is noted. Another

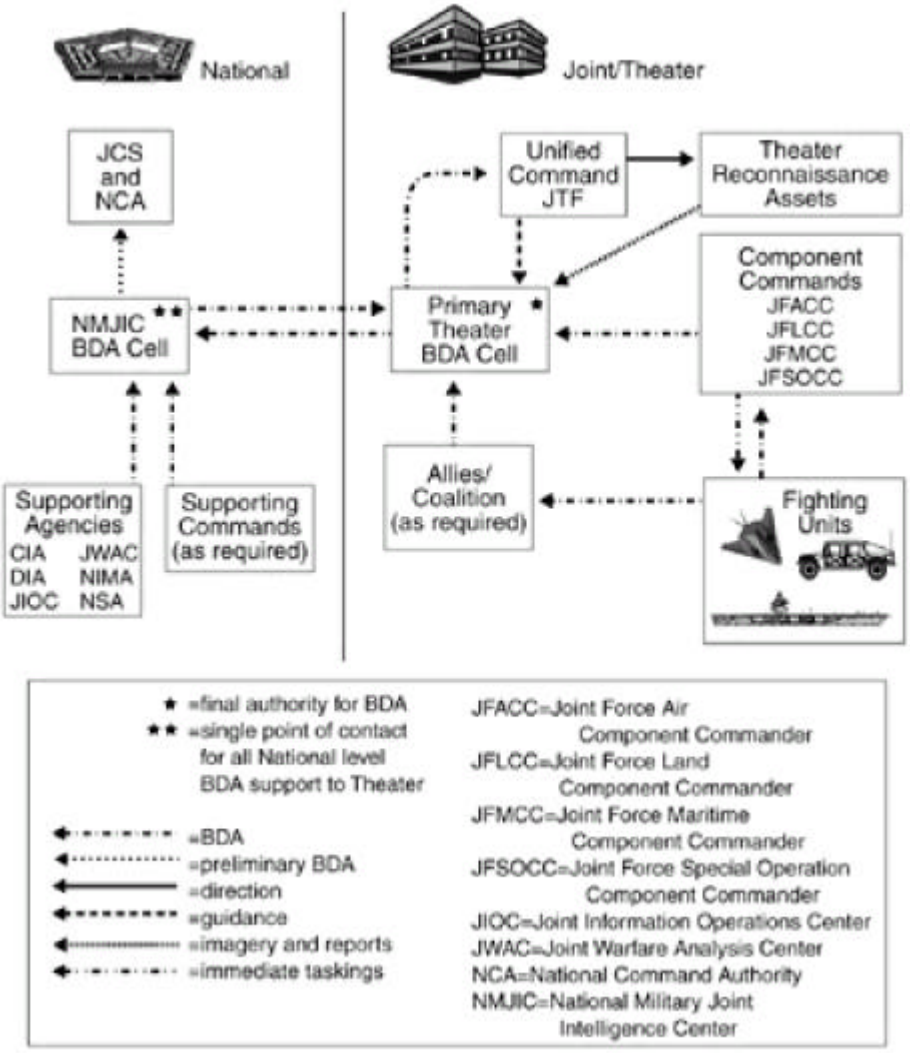


Figure 8-4. Phase I BDA or PDA Information Flow.

howitzer has no visible damage. The PDA of the battery is 65 percent destroyed. The PDA for large, complex targets is keyed to specific aimpoints and critical elements.

Combat Strength Assessment

When dealing with threat ground combat units, the more common term for Phase I BDA or PDA is combat strength assessment. Combat strength is the actual strength on hand of a ground unit in terms of operational tanks, armored vehicles, and artillery. This strength is expressed as either a count of generic type equipment or as a percentage of the T/O and T/E. Threat combat strength is a critical factor to commanders preparing for combat. During operations, commanders rely on combat strength assessment to account for enemy losses and to assess remaining enemy strength.

Combat Strength Baseline

Prior to operations, analysts establish the combat strength baseline of beginning strength numbers. These numbers remain constant for the duration of combat and serve as a benchmark against which losses or gains are measured (see table 8-1). The baseline combat strength represents the maximum amount of equipment possible for a unit, while combat losses represent verified losses.

Table 8-1. Example of Combat Strength Assessment.

105th Mechanized Infantry Division	Tanks	Armored Vehicles	Artillery
T/E	102	135	45
Beginning Strength	98	135	42
Combat Losses	17	22	4
Replacements	6	3	0
Combat Strength	87	116	38
Percent of T/E	85	85	84
Current Combat Strength = 85%			

Combat Strength Computation

Combat strength for each type of equipment is computed by subtracting the confirmed losses from the beginning strength and adding the replacements to that total. The percent of T/O and T/E is calculated by dividing the combat strength by T/O and T/E numbers. The T/O and T/E percentages are totaled and divided by the number of equipment types to determine the current combat strength for the assessed system. Note that while the baseline combat strength represents the maximum amount of equipment possible for a unit, combat losses represent only verifiable losses. Current combat strength can be viewed as a worst-case estimate since it only takes into account confirmed losses. Replacements are included when known. Equipment categories are limited to generic types.

Personnel Losses

Personnel are not normally included in determining combat strength. Acquiring accurate casualty figures and accounting for replacements is extremely difficult, and past experience has shown that body counts are often misleading. A more appropriate and meaningful assessment of the impact of personnel losses can be made as part of combat effectiveness assessment. In MOOTW, however, where personnel may be the threat's principal strength, personnel losses may have to be tracked and combat strength assessed accordingly.

Functional Damage Assessment

The FDA is an estimate of the friendly military force's effect on degrading or destroying the functional or operational capability of the target and an evaluation of the friendly force's operational objective success level. This assessment is based on all-source intelligence and includes an estimate of the time required for reconstitution or replacement of the target function. The FDA is also referred

to as Phase II BDA. Figure 8-5 illustrates the Phase II BDA information flow.

Target System Assessment

The TSA is a broad assessment of the friendly military operations impact and effectiveness against a target system capability. This assessment may be used to measure the threat's combat effectiveness. Based on the commander's operational objectives, a TSA may address significant target system subdivisions. Analysts compile individual target FDAs to produce TSAs, which are applied to the current system analysis or OOB. For example, the threat's fire support system is known to have 21 artillery battalions. Partial destruction of one battery has minor impact on the effectiveness and capability of the threat's overall fire support system. A complex and resource intensive process, TSA is generally performed at the theater level. The TSA is also referred to as Phase III BDA. Figure 8-6 illustrates the Phase III BDA information flow.

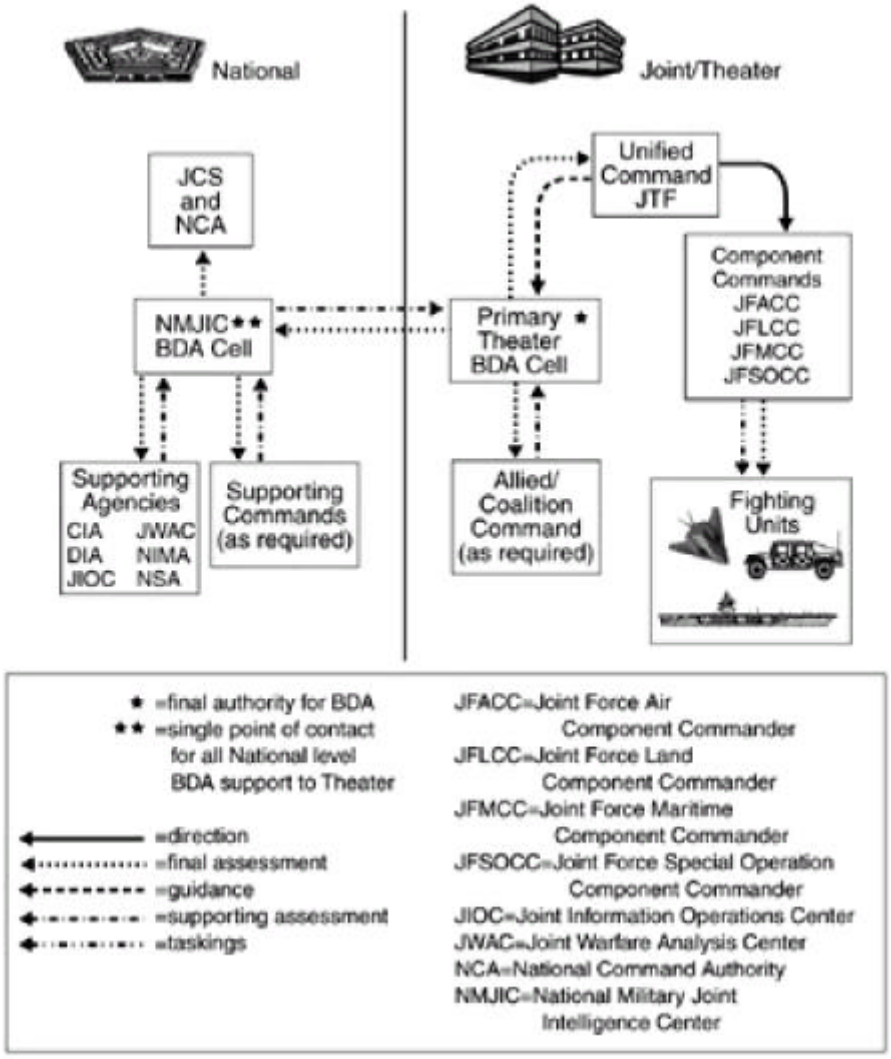


Figure 8-5. Phase II BDA or FDA Information Flow.

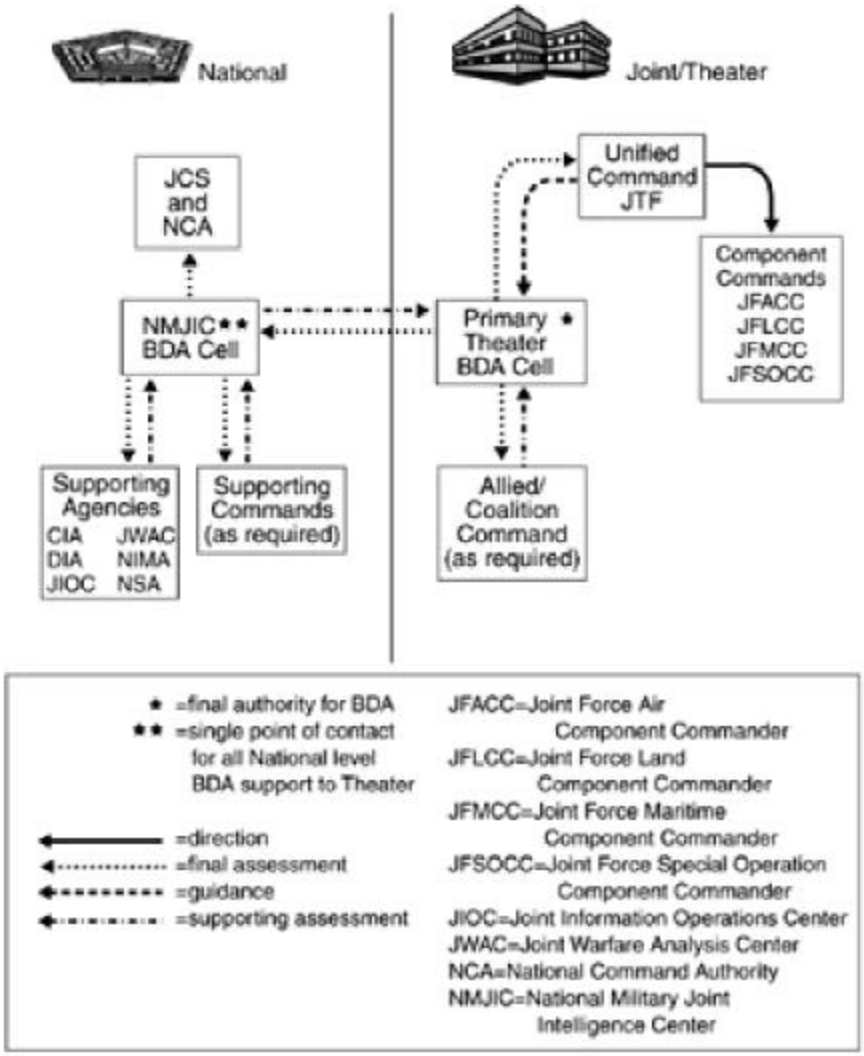


Figure 8-6. Phase III BDA or TSA Information Flow.

Responsibilities

The intelligence officer and the MEF ISC integrate intelligence and operational weapons system and munitions effects data provided by the G-3/S-3 to determine the effects of an executed COA on threat strength and combat effectiveness. In coordination with the G-3/S-3, the intelligence officer or ISC—

- **Recommends HVTs.**
- **Develops and recommends IRs to include those for targeting and BDA.**
- **Coordinates with the G-3/S-3, air officer, and fire support coordinator to develop coordinated targeting, intelligence, BDA, MEA, and RR plans.**
- **Develops integrated collections, production, and dissemination plans to answer the commander's IRs.**
- **Requests collection and production support for intelligence required to satisfy targeting objectives and BDA.**
- **Establishes procedures to ensure observation reports from forward observers, reconnaissance, pilots, etc., are readily available to BDA analysts.**

- Matches BDA against the commanders objectives to determine targeting success and refines intelligence estimates of the threat's situation and capabilities, recommends target reattack, develops and maintains historical BDA data bases, and disseminates hard and soft copy intelligence and BDA products.
- Uses the results of BDA and combat assessment in determining the need to further develop enemy COAs.

Battle Damage Assessment Methodology

After the commander identifies PIRs, IRs, and targeting priorities, the intelligence officer or MEF ISC tasks intelligence collection assets to locate, identify, and track designated targets and directs production assets to plan and prepare needed intelligence products. The ISC, fire support coordinator, and air officer coordinate to identify the appropriate attack system to capture, destroy, degrade, suppress, or neutralize the target.

Based on targets and conditions set by the commander, the ISC refines the commander's BDA-related requirements and integrates them into the intelligence operation plan. These BDA requirements are answered through execution of the intelligence cycle.

As targets are attacked, the ISC coordinates P&A cell's BDA through execution of the intelligence cycle. The commander uses BDA to decide if the target should be reattacked or if the objectives have been met. Once a BDA-related PIR is satisfied, the commander decides if there is a need to establish a new BDA-related PIR or if limited intelligence assets will be used to support another aspect of the mission. The BDA-related PIRs should only address the commander's most critical requirements.

Tactical-level BDA provides a series of timely and accurate snapshots of the effect operations are having on the threat. The BDA helps commanders determine when or if their targeting effort is accomplishing goals and objectives and provides commanders the information needed to quickly allocate or redirect forces.

Battle Damage Assessment Principles

The intelligence officer must work closely with the commander and staff to ensure they know the characteristics and limitations of BDA, which is viewed in terms of objectivity, reliability, and accuracy.

Objectivity

The BDA must be objective and supported by the most reliable data available. Generally, data collected through objective means (imagery) are more reliable than data collected through subjective means (pilot reports). The intelligence officer and ISC should strive to verify conclusions and resolve discrepancies in BDA reporting. It is particularly important to maintain BDA objectivity when BDA becomes the deciding factor for determining and executing a specific COA or decision. When disseminating intelligence, the ISC must make a distinction between facts and estimates.

Reliability

The quantity and quality of available collection and production assets impact BDA reliability. The degree of reliability and credibility of the assessment relies on the resources employed for BDA collection. Collection and production assets must be properly balanced, managed, and supervised to produce reliable reports that are concrete, quantifiable, and precise.

Accuracy

To obtain accurate BDA information, the AO must be frequently and adequately covered by a combination of national, theater, and tactical collection and production assets. Frequent coverage is necessary to accurately determine pre- and post-strike damage.

Battle Damage Assessment Reporting

The intelligence officer or ISC ensures BDA reports conform to the operational plan, reports target damage and destruction, and assesses the degree of mission success. When possible, BDA reporting includes the visual verification of physical damage and an analysis of the damage effects on the threat unit. The MAGTF and subordinate elements are primarily concerned with reporting Phase I BDA or PDA.

Reports

Reports used in BDA include—

- Mission reports and in-flight reports.
- Aircraft cockpit video or weapons system video.
- Imagery and IMINT (e.g., national, theater, and tactical imaging systems, UAVs).
- SIGINT.
- HUMINT.
- Open source intelligence (e.g., television broadcasts, radio broadcasts, newspapers).
- Visual reports from combat units, air controllers, or forward observers.

Reporting Methods

The intelligence officer compiles, refines, and validates the various sources of BDA and develops consolidated PDA or combat strength assessments. The MSCs and major subordinate elements forward consolidated BDA reports to the MEF, usually covering set time periods. See appendix D for an example of a consolidated BDA report format.

At the MEF level, P&A company, intel bn, is responsible for compiling MEF Phase I BDAs or PDAs and for adjusting master OOB data bases to reflect threat combat losses. The BDA cell also prepares and disseminates formal Phase I BDA reports according to theater and national policies and procedures. Defense Intelligence Report, DI-2820-2-99, *Battle Damage Assessment (BDA) Reference Handbook (U)*, provides detailed joint procedures and formats regarding BDA analysis, reporting formats, standard terminology, and resources. This final draft document is available on-line via INTELINK and INTELINK-S.

CHAPTER 9. INTELLIGENCE PRODUCTION

Intelligence production is the conversion of information into intelligence through the integration, analysis, evaluation, interpretation, and synthesis of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. Production involves translating the results of analysis into usable intelligence products that are timely and tailored to the unit, subordinate units, and other supported commands' missions and IRs. The analyst must strive to provide knowledge and understanding that the decisionmaker can visualize and absorb. If possible, that knowledge and understanding should be presented in the form of coherent, meaningful images rather than in the form of accumulated lists, texts, or data fields. During the production phase of the intelligence cycle, information is—

- Evaluated to determine pertinence, reliability, and accuracy.
- Analyzed to isolate significant elements.
- Integrated with other relevant information and previously developed intelligence.
- Interpreted to form logical conclusions, which bear on the situation and support the commander's decisionmaking process.
- Applied to estimate possible outcomes.
- Placed in a product format that will be most useful to the user.

During MAGTF CE deliberate planning, production normally entails the development of detailed, all-source intelligence estimates and studies through the combined efforts of several intelligence and reconnaissance operation elements. During tactical execution, time constraints and ongoing battle demands require rapid processing and production with an emphasis on development of simple, mission-focused intelligence products (e.g., annotated image, target description, overlay depicting current and future threat dispositions). The value of intelligence production is measured in terms of time or resources expended and how well it places information into context, converts it into knowledge and understanding through analysis and synthesis, answers the PIRs and IRs, and applies that knowledge to the decisionmaking process.

There is an inherent friction between the desire to provide as complete and accurate an intelligence product as possible and the continuous requirement to support the time-sensitive urgency of tactical decisionmaking. In practice, these conflicting demands must be balanced by using both stated direction, such as the commander's intent and PIRs, and knowledge of the operational situation to determine when to finish and disseminate a product. To provide a framework to make these determinations, intelligence production is viewed as occurring on deliberate and immediate levels.

Production Categories

In the MAGTF, the primary categories of production are deliberate and immediate.

Deliberate Production

Deliberate production is employed when there is sufficient time to thoroughly evaluate, analyze, and synthesize available information and intelligence. The results of deliberate production efforts are formal, comprehensive intelligence products. Intelligence products that fit into this category include—

- Contingency intelligence studies.
- Detailed, fully developed IPB studies.
- Intelligence estimates.
- Target or objective studies.

Immediate Production

Immediate production is a time-limited, highly focused effort that satisfies an immediate tactical requirement. This type of production involves the rapid processing, analysis, production, and dissemination of intelligence to influence tactical decisionmaking. Often, immediate production is facilitated by, and builds on, a previously completed deliberate production effort.

Elements of data are subjected to a compressed version of the production cycle, and the resulting product is rapidly disseminated to those who are affected. Immediate production is normally conducted during execution and results in simple, mission-specific intelligence products (e.g., situational assessments or answers to specific, individual intelligence requirements).

The nature of the situation and pertinent intelligence requirements dictate the amount of time available to complete each production effort. Intelligence products that fit into this category include—

- Intelligence reports that provide alarm or warning information.
- Reconnaissance and surveillance data related to decision points for branches or sequels.
- Reactive targeting intelligence or hastily prepared intelligence briefings for initiation of small unit action.

Principles

Whether deliberate or immediate, intelligence production is guided by the following principles.

Purpose and Use of Intelligence

To understand the needs of the consumer and to answer the IRs, the producer must know the user's command level, mission, IRs, time sensitivity, responsibilities, and purpose of the intelligence products.

Objectivity

Producers must be objective and unbiased to avoid any tendency toward preconceived ideas. When conflicting information exists, efforts should be made to resolve the difference. If time and resources are inadequate to provide explicit intelligence, the commander must be made aware of the uncertainty. Commanders need pertinent intelligence, including conflicting or contradictory information and opinions.

Provision of Integrated and Tailored Products

Intelligence analysts integrate and tailor information from multiple sources to provide decisionmakers with a clear picture of the battlespace.

Coordination Among Echelons

Intelligence production should be coordinated between national, theater/operational, and tactical-level echelons. The JTF intelligence officer directs and coordinates production activities to ensure they are mutually supporting and not duplicative. Forces at every echelon accomplish joint and combined operations intelligence production, which includes Service-unique products at component commands and operating forces. Higher echelons use organic collection assets and production capabilities to produce intelligence and to refine and compile intelligence received from subordinate units and external organizations. Subordinate units use intelligence products sent to them by the senior command to determine or adjust their mission and operations.

Responsibilities

Higher echelons are responsible for ensuring subordinates are provided the required intelligence exceeding the subordinate's organic capabilities. To provide subordinate commands with required intelligence products and services, higher echelon commanders and intelligence officers identify and task organizations

that can contribute to resolution of subordinate commanders' IRs.

Management

Production management ensures effective and efficient intelligence production in support of operations. Intelligence personnel must receive, review, validate, prioritize, and coordinate production requirements to determine the task, producer, forms, and production schedule.

Production Cycle

The goal of the intelligence cycle is to produce timely, usable intelligence. The production cycle is in essence the intelligence cycle, with the constituent parts of directing, collecting, processing and exploiting, analyzing, and finally producing, disseminating, and using the intelligence. The production cycle spans months or minutes, depending on the level of command conducting production and the nature of the IRs. During the production cycle process, intelligence section personnel must focus on delivering the product in a timely, tailored, complete, and usable manner.

Define Intelligence Requirements

Properly articulated, mission-oriented requirements focus the intelligence effort and define IPRs. The commander, staff, and subordinate commanders play a role in developing the command's IRs. The intelligence officer formulates most of the initial requirements during IPB step 1 by identifying gaps in current intelligence holdings and by defining the scope and detail of production required for IPB support.

As IPB and staff planning progresses, analysts identify additional IRs, which are generally linked to proposed COAs, potential decisions, and targeting. Analysts working to satisfy the command and supported units' IRs also generate new IRs.

Based on the commander's intent and the current phase of the PDE&A cycle, the intelligence officer validates, refines, and prioritizes these additional requirements and converts them into integrated ICRs, IPRs, and IDRs. This is not a one-time effort, but instead a dynamic process of new, existing, and satisfied or no longer relevant requirements. The relative importance of each requirement changes as the PDE&A cycle progresses and as phases of the operation are executed. The intelligence officer must periodically confirm the assignment of priorities with the commander to ensure the intelligence effort is focused on the commander's desires.

Define and Prioritize Intelligence Production Requirements and Tasks

Once IRs have been clearly stated and properly defined, analysts define and prioritize IPRs and tasks by answering the following questions:

- What do I need and where can I obtain the information? The analysts must determine research needs and information sources. The tactical intelligence analyst may have access to a wide range of information and intelligence sources and documents. The product required may have been produced by another source or agency. This requirement may generate ICRs to provide the necessary information.
- When is the product required and in what form? Determination of production assets is based on time and final product requirements (e.g., document, report, supporting study, briefing).
- Who can produce the intelligence product? A small intelligence section does not have the assets to complete a large, detailed study in a short period of time.
- Who will get the product?

- **Is this a product that can or must be shared with multinational allies? The intelligence product's classification and releasability must be considered.**
- **Does this product require supporting work? The analyst must determine the need for supporting requirements (e.g., imagery exploitation, topographic analysis).**

Develop Intelligence Production Plan and Schedule

When dealing with large or complex IRs and IPRs, development of an intelligence production plan and a supporting schedule aids in effectively applying resources to accomplish the task. Production plans and schedules are particularly important at higher echelon commands and intelligence centers where numerous long-term projects are managed and coordinated. At lower echelons, production plans and schedules may consist of the intelligence officer conducting a quick mental assessment of the task and developing a time line for its completion.

Considerations

When developing a production plan and schedule, the first consideration is always priority. The requester's needs drive the due date. Once priority and time available are established, factors to be considered include—

- **Research required.**
- **Time available to collect new information and data.**
- **Coordination needs.**
- **Review and quality control procedures.**
- **User's format requirements.**
- **Graphic preparation.**
- **Reproduction or conversion requirements.**
- **Dissemination requirements.**

Preparation Methods

For large, long-term products, the production schedule is time lined with various milestones, due dates, and completion projections annotated. In large organizations with distinct collection, exploitation, editing, graphics, and dissemination assets, this time line synchronizes those assets to ensure efficient and timely project completion.

Plans and Tools

The principal planning vehicle for a MAGTF is tab B, (Intelligence Production Plan), to appendix 16 (Intelligence Operations Plan), to annex B (Intelligence), to an OPLAN or OPORD. Other tools that may be used by intelligence officers and their production leaders are the intelligence production matrix and the periodic intelligence production status report. Appendix E to this publication provides guidance and suggested formats for use of these plans and tools within a MAGTF. Specific instructions and formats are specified in unit SOPs.

Allocate Resources

The availability of the following organic and external resources required to produce the intelligence product must be determined:

- **Intelligence production personnel.**
- **Time.**
- **Ongoing analysis.**
- **Preprocessed information sources.**
- **Collection assets.**
- **Automated information systems.**
- **CIS.**

Assign Tasks

Specific tasks are assigned to the various collection and production resources that assist in the production process. The priority of tasks is

based on the priority of the IR, the time available, and the production schedule.

Prepare the Product(s)

During this step, existing information, data, and intelligence is researched and integrated with new information derived from collection operations and other all-source intelligence reporting. The resulting information set is analyzed and synthesized to develop conclusions and estimates. A final intelligence product(s) draft is produced based on the analysis performed.

Review and Quality Control

Procedures must be established for product review and quality control before final product approval and dissemination. A balance must be achieved between timely delivery and proper review.

Approve and Distribute the Product(s)

Responsibility for final approval of the intelligence product normally rests with the producing unit intelligence officer. At the MEF level, product approval responsibility is generally delegated to the ISC; however, time and the situation may dictate delegating this authority to lower levels. The intelligence product is only of value if it is distributed to the requester in time for proper use.

Follow Up

The final and most critical step in the production cycle is to follow up with commanders and other intelligence product users to—

- Ensure the product is understood.
- Determine whether PIRs and IRs are satisfied.
- Determine if the intelligence product generated new PIRs or IRs.

Production Management

Efficient management of the production cycle ensures effective military intelligence production in support of MAGTF and joint operations. Production management satisfies established PIRs and IRs in a complete, timely, and efficient manner; helps prioritize competing requirements to ensure timely response; and ensures the most effective use of limited intelligence resources.

Functions

Management of the production cycle encompasses the following functions:

- Determining the scope, content, and format of each product.
- Developing a plan and schedule for the development of each product.
- Assigning priorities among the various IPRs.
- Allocating processing, exploitation, and production resources.
- Integrating production efforts with collection and dissemination.

Production Managers

While intelligence production centers and agencies have separate production managers, management of the production cycle at other command levels is conducted by—

- Intelligence battalion commanding officer, serving as ISC under the staff cognizance of the MEF AC/S G-2, at the MEF CE level.
- Intelligence operations officer or air combat intelligence officer at the MSC level.
- Intelligence staff officer at lower tactical echelons.
- Officer in charge of an intelligence direct support team supporting a lower unit.

Production Management Elements

The following elements are essential for production management:

Production Requirements Development

Each IR must be validated through the chain of command and examined to determine scope, form, and content of the request. These validated and examined IRs are IPRs. A well-developed IPR includes—

- **Point of contact and best way to communicate.**
- **Priority of the requirement.**
- **Date required and latest time the intelligence is of value.**
- **Classification, releasability, and format desired.**
- **Mission background.**
- **Brief description of the desired requirement.**
- **Justification for the requirement.**
- **Sources and documents previously consulted.**
- **Dissemination instructions (e.g., primary and alternate communications means or channels, designated recipients, quantities required).**

Prioritization of Requirements

Production requirements are prioritized for limited intelligence resource use.

Asset Allocation

The intelligence officer and intel bn production manager consider internal or organic and external resources (e.g., JTF, theater, and national) for intelligence production tasking. Although internal resources should be considered first, production managers forward requirements for large, complex products to higher command levels. For example, IPB is an inherent function of staffs at every level; however, the production of detailed terrain analysis products may be more appropriately performed by the MEF intel bn or other supporting agencies.

Scheduling

Production managers must schedule and synchronize task elements in the time allotted to successfully complete intelligence production.

Integration with Collection and Dissemination

Production management starts in the planning and direction phase of the intelligence cycle where IRs are determined. The PIRs and IRs are either answered by intelligence products that are readily available or they become a collection or production requirement. Ultimately, products are disseminated to individuals and organizations that need them. Although collection, production, and dissemination involve their own unique internal procedures and cycles, they must be synchronized to provide a timely, pertinent, and usable intelligence product.

Intelligence Products

Intelligence products may be in graphic, written, or oral form and may be as simple as an answer to a question or as complex as a contingency intelligence study. Although they may be used to produce warnings or to identify opportunities, intelligence products are intended to facilitate planning and decisionmaking.

Graphics are the preferred product form because intelligence products should convey an accurate image of the battlespace or threat to the decisionmaker in a form that facilitates rapid understanding. The use of automated information systems is increasing the capability to develop graphic products that can be disseminated and displayed over web-based systems. Graphics developed by the MEF P&A cell may be pulled via the MAGTF tactical data network from the MEF SIPRNET web site or shared via IAS. Use of these graphics reduces or eliminates MSC production.

In time-sensitive situations, the verbal report or short text message may be the most expeditious and useful intelligence product form. For more complex or precise planning needs, graphics reinforced with detailed supporting text is usually required.

Whether oral, text, or graphic, intelligence products should use standard formats. Baseline formats may be modified to suit unit needs, but format modifications may impact interoperability so they must be thoroughly coordinated with all users. The following intelligence products are the principal intelligence products developed and used in the MAGTF.

MAGTF Contingency Intelligence Study

This baseline intelligence study is prepared in advance for standing OPLANs and likely contingencies. In written form, this study is based on the intelligence estimate format and can be converted to an intelligence estimate when a contingency becomes a reality. Many of the products created in steps 1 through 4 of the IPB process (e.g., MCOO, weather effects charts, threat models, doctrinal templates) can be prepared either as supporting graphics or as standalone products.

Intelligence Estimate and Supporting Studies

The intelligence estimate provides basic and current intelligence and mission-specific IPB results. Normally prepared by echelons of battalion or squadron size and larger during the planning phase, estimates are frequently disseminated to other units to keep them current on intelligence. Supporting studies may cover particular aspects of the enemy situation or the AO. See appendix A for the intelligence estimate format and discussion of the relationship between IPB and the intelligence estimate.

Target or Objective Study

This intelligence product provides mission-specific intelligence in support of small unit execution. There is one basic form, but many variations can be used. The study is used to support attack aviation as well as MEU(SOC) and regular combat operations. See chapter 8 for a discussion of the basic target or objective study.

Intelligence Summary

The intelligence summary (INTSUM) provides a synopsis of the intelligence situation covering a specified period prescribed by the unit intelligence SOP or annex B (Intelligence) to the OPORD. Used to report threat activities, threat capabilities changes, and P&A results, the summary is designed to update original and subsequent intelligence estimates.

At lower tactical echelons, INTSUMs are prepared according to the unit SOP or annex B to the OPORD. At higher commands, a daily INTSUM (DISUM) is published every 24 hours. Using the basic format, units tailor the INTSUM to fit the situation. Automated information systems facilitate graphic production of INTSUMs and DISUMs, which are posted on networks with links to detailed supporting intelligence products, reports, and data bases. See appendix F for the INTSUM format.

Intelligence Report

The intelligence report (INTREP) is a standardized report that is disseminated as rapidly as possible based on its importance to the current situation. This report is the primary means for transmitting new and significant information and intelligence when facts influencing threat capabilities have been observed or when a change in threat capabilities has taken place. Generally, a separate report is prepared for a single item of information by the first intelligence element acquiring the information. When time permits, the INTREP should include the

originator's interpretation of the information or intelligence being reported. See appendix G for the INTREP format.

Briefings

Intelligence briefings should always convey mission-essential intelligence and other pertinent information tailored to the audience and current IRs. Intelligence personnel must be able to prepare and orally convey relevant intelligence in a clear, concise manner to brief commanders, staffs, and subordinate units.

Briefings should be supported with graphics to enhance understanding in the least amount of time. Graphics may be as simple as a sketch or acetate overlay or as complex as a multimedia presentation delivered via video teleconferencing. Intelligence personnel must ensure graphics are clear, legible, simple, visible, and focused on relevant information.

At lower tactical levels, briefings are generally informal and often called on short notice. At higher levels, briefings may be structured and scheduled on a recurring basis. The intelligence brief is usually part of a staff briefing coordinated by the chief of staff, executive officer, or the operations officer. Intelligence briefings can be in the form of an information, decision, or confirmation brief.

Information Brief

This is the most common form of brief intended to enhance situational awareness and understanding. The commander's morning update is an example of an information brief. See appendix H.

Decision Brief

The second type of brief is for the purpose of obtaining a decision from the commander. A briefing conducted to convey wargaming results and to gain the commander's preferred COA is an example of a decision brief.

Confirmation Brief

This brief is a final review of a planned action to ensure participants are certain of the objectives and are synchronized with each other.

Organic MAGTF Intelligence Production

In the MAGTF, deliberate production of detailed, all-source intelligence products supports planning. While deliberate production draws heavily on external national, theater, and Service-level production sources, organic MAGTF intelligence sections tailor products to the MAGTF mission and needs. Small unit intelligence sections, intelligence watches at the regiment or Marine aircraft group and battalion or squadron levels, and intelligence direct support teams conduct primarily immediate production.

Unit Intelligence Sections

The MAGTF CE and MSC intelligence sections primarily conduct deliberate production to satisfy planning requirements. They produce the contingency intelligence studies that lower-level commands tailor to their needs.

Units conduct IPB and prepare estimates and target or objective studies that are tailored and focused on their mission and level of command. The IRs that are beyond a unit's production capability are normally forwarded via the chain of command to the MEF G-2 or intel bn. A well-prepared IPB is the basis for rapid and effective immediate intelligence production.

Small unit intelligence sections (e.g., regiment or battalion and Marine aircraft group or squadron) primarily conduct immediate production to satisfy tactical decisionmaking and operations. Immediate production conducted at higher echelons focuses on alarms or triggers associated with the commander's decision points or reactive targeting against identified HPTs. As units

and sensors collect data related to NAIs, TAIs, decision points, and HPTs, this information is rapidly assessed, placed in context, and disseminated as intelligence to the commander and appropriate agencies for immediate action. Often the product is a verbal report or short INTREP sent via electronic means.

Intelligence Direct Support Teams

Two direct support teams are organic to the P&A company, intel bn, and one each for the division, MAW, and FSSG headquarters. They are designed to allow the MEF or MSC commander and their G-2s to focus intelligence support to designated subordinate units. These teams tailor higher and external intelligence products to the needs of the supported unit and assist the supported unit in the production of IPB and other intelligence products to support detailed mission planning and execution.

Production and Analysis Company, Intelligence Battalion

The P&A company produces and disseminates all-source fused tactical intelligence, IMINT, and GEOINT products in support of the MAGTF, MSCs, and other commands as directed. As the focus of the deliberate production effort, P&A company satisfies IPRs for the entire MAGTF. The P&A company has the personnel and equipment resources and CIS connectivity to national, theater, and Service-level organizations' intelligence products and production resources for augmenting organic capabilities. See chapter 9 for additional information.

External Production Support

Marine Corps intelligence assets are optimized for the production of tactical intelligence in support of MAGTF operations. While organic assets are generally sufficient to meet MAGTF requirements, national, theater, and Service intelligence agencies and centers provide unique intelligence production capabilities. The MAGTF has the ability to exploit external intelligence assets to enhance its organic capabilities. The following key external capabilities are employed to support MAGTF operations:

- National, theater, and Service-level intelligence P&A.
- Geospatial information and services.
- P&A of target intelligence and target materials.
- National imagery collection, exploitation, and production.
- Collection and production support from the U.S. SIGINT System.
- National and theater-level CI and HUMINT collection and production.
- Liaison elements from national and theater intelligence agencies.

To exploit external intelligence support resources, the MAGTF must have—

- Trained personnel experienced with external intelligence assets.
- Sufficient, reliable, CIS connectivity and interoperability with national, theater, and Service intelligence architectures to receive, process, and disseminate information.
- Integration of Marine intelligence specialists into national, theater, and Service intelligence organizations to articulate Marine Corps capabilities and requirements, to influence decisions, and to optimize intelligence support to expeditionary forces.
- Established liaison between the MAGTF and supporting intelligence agencies through dedicated communications and exchange of officers.

Department of Defense Support

Within the Department of Defense (DOD) intelligence production community, the DOD Intelligence Production Program (DODIPP) provides the analytical and production resources to support

operational forces. The DODIPP incorporates basic principles that minimize duplication of effort and make the specialized expertise of its analytical personnel available to support DOD customers. The DOD intelligence production community is comprised of the following agencies, centers, and activities:

- DIA.
- Service production centers (e.g., MCIA).
- Unified command JICs or joint analysis centers, components, and Reserves.
- Allied production activities participating in the shared production program (SPP) or during crisis surge situations.
- National Security Agency, which produces SIGINT.
- National Imagery and Mapping Agency, which produces geospatial information and GEOINT.

National Production Support

The DIA and its supporting agencies (Armed Forces Medical Intelligence Center and Missile and Space Intelligence Center) are responsible for intelligence production in the following areas:

- Foreign national military policy, doctrine, strategy, and planning, including—
  - National military leadership.
  - Mobilization process and potential.
  - Strategic or large scale military operations.
  - Integrated, combined, or joint forces on military net assessments and assessments or estimates focusing on military issues at the national, regional, and global levels.
- Current indications and warning intelligence and strategic targeting and planning by the joint staff.
- Integrated force trends and projection assessments.
- Nuclear weapon programs and doctrine.
- Intelligence on proliferation and technology transfer.
- Technological capabilities of antitank guided missiles, surface-to-air missiles, short-range ballistic missiles, and antiballistic and antitactical ballistic missiles.
- Medical and biological warfare intelligence.
- Global topics, such as military geography, industrial resources, transportation systems, demographics, military industrial and resource bases, and military economics.
- Intelligence production programs on counterterrorism, counterdrug intelligence support to law enforcement agencies, foreign intelligence and security forces, and deception analysis.
- Intelligence programs fulfilling DOD-wide responsibilities of common concern, such as targeting and foreign materiel.
- OOBs and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of those forces.

Unified Command Production Support

A unified command's intelligence production is performed by a production center or JIC, which is assigned to the unified command in support of theater or specialized forces. The JICs fulfill intelligence requirements of unified command CINCs and subordinate commanders by providing tailored, finished intelligence products to support theater mission planning and execution. Regional and functional unified command JICs' production responsibilities vary.

Centers

Unified command intelligence production JICs include—

- U.S. Joint Forces Command's Joint Forces Intelligence Command.
- U.S. Central Command's JIC.

- **U.S. European Command's Joint Analysis Center (JAC).**
- **U.S. Pacific Command's JIC.**
- **U.S. Special Operations Command's JIC.**
- **U.S. Southern Command's JIC.**
- **U.S. Space Command's Combined Intelligence Center.**
- **U.S. Strategic Command's JIC.**
- **U.S. Transportation Command's JIC.**

Responsibilities

The JICs' intelligence production responsibilities include—

- **Operational intelligence, current intelligence, and indications and warning for forces deployed within the command's area of responsibility.**
- **OOBs and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of those forces.**
- **Foreign military forces unit-level training and/or operational readiness.**
- **Physical environment of deployed or committed forces, including terrain analysis and IPB.**
- **Targeting support, including target materials, bomb damage assessments, tactical BDAs, and special operations forces targeting support.**
- **Support to command-sponsored joint planning and exercises.**
- **Tailored and focused intelligence produced elsewhere to meet the specific requirements of command customers.**
- **Background and tactical intelligence to customers within the theater, including operational and allied forces.**

Services Production Support

The Service production centers are responsible for Service-specific intelligence production and for production relative to U.S. Military Forces assigned for the SPP.

Centers

The Service production centers are—

- **Army—National Ground Intelligence Center (NGIC).**
- **Navy—National Maritime Intelligence Center (NMIC).**
- **Marine Corps—Marine Corps Intelligence Activity (MCIA).**
- **Air Force—National Air Intelligence Center (NAIC).**

Responsibilities

The centers' intelligence production responsibilities include—

- **Weapon system technical data, characteristics, performance, system vulnerabilities, and capabilities to support Service and defense acquisition activities and force developers and to support Service operational training and preparation for contingencies or conflicts.**
- **Basic ground, naval, and aerospace intelligence and foreign intentions and capabilities.**
- **Service-unique doctrine, force structure, force modernization, training and education, and acquisition.**
- **Support to Service schools and commands relative to training, exercises, predeployment, or crisis responsibilities or activities.**
- **OOB and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of Services.**

Service-Unique Responsibilities

The following Service production centers have unique intelligence production responsibilities:

- **NGIC produces ground-related systems and develops intelligence on—**
  - **Armor.**
  - **Infantry.**
  - **Field artillery.**
  - **Air defense guns.**
  - **Landmines.**
  - **Chemical warfare.**
  - **Helicopters.**
  - **Munitions.**
  - **Engineering and transport or logistic equipment.**
  - **Associated technologies.**
- **NMIC, Office of Naval Intelligence, produces naval-related systems and develops intelligence on—**
  - **Surface and subsurface combatants.**
  - **Antisubmarine or surface auxiliary and support naval ships and programs.**
  - **Weapons, merchant shipping, and ocean science information.**
  - **Associated technologies.**
- **NAIC produces aerospace-related systems and develops intelligence on—**
  - **Intercontinental ballistic missiles.**
  - **Intermediate-range ballistic missiles.**
  - **Medium-range ballistic missiles.**
  - **Bombers.**
  - **Fighters.**
  - **Special mission aircraft.**
  - **Munitions.**
  - **Space launch systems and satellites.**
  - **Associated technologies.**
- **MCIA produces amphibious and expeditionary warfare intelligence on—**
  - **Shallow water mines.**
  - **Coastal artillery.**
  - **Foreign marine and naval infantry forces.**
  - **Antilanding capabilities.**
  - **Expeditionary studies.**

Non-Department of Defense Intelligence Production Support

Intelligence production in support of military forces is available from agencies outside DOD (e.g., Central Intelligence Agency). Generally, DIA serves as the focal point for tasking these agencies; however, theater and JTF intelligence staffs can access support through their national agency's liaison office or an assigned national intelligence support team (NIST).

A NIST is a nationally sourced, task-organized team composed of intelligence and communications experts from DIA, Central Intelligence Agency, National Security Agency, NIMA, or any combination of these. A NIST provides the supported command with increased IR management, production and dissemination capabilities, and a direct conduit to national agencies. The size and composition of the NIST varies according to the size and nature of the crisis and the mission and intelligence needs of the supported command.

Production Support Requests

A PR begins as an IR levied on the unit intelligence section. Before requesting production support, the unit intelligence officer must determine if the—

- **Intelligence request or request for intelligence (RFI) is most appropriately answered by intelligence resources.**
- **Information or intelligence is already available in unit intelligence files, data bases, or information resources.**
- **Intelligence can be obtained by organic collection assets and developed into intelligence by its production assets.**
- **Intelligence request can be answered from other unit or component intelligence elements.**

Once the unit intelligence officer determines that the requirement cannot be met with local resources, the requirement is forwarded up the chain of command for satisfaction. The intelligence officer determines whether to submit the requirement as RFIs, ICRs, IPRs, or PRs. (The acronym IPR is currently unique to the Marine Corps, while the acronym PR, established in joint doctrine, is chiefly applicable to intelligence operations at the MEF CE level and above.)

Generally, an RFI is submitted if the requirement is a fairly straightforward question. In a noncombatant evacuation operation, a RFI may be, "How many personnel require evacuation?" In this case, no extensive collection or production is required because the intelligence is generally available.

A PR is more appropriate when the IR is complex or substantial, for example, "What is the capability of country X to defend its coastline against an amphibious assault?" This requirement may result in an IPR for the MEF CE or a PR to the JTF headquarters because the answer will require the collection and analysis of a large amount of information ranging from hydrographic conditions to available threat weapon systems. Such analysis may be beyond the capabilities of a small unit intelligence section and more appropriately performed at the theater or Service level where access to information and ability to task collection resources are greater.

A PR is also appropriate to satisfy a requirement that may be recurring in nature or in a denied area, for example, "How many aircraft are maintained on alert status at airfield Y?" The unit intelligence officer submits a request for theater and national production assets, because the airfield will need to be monitored for a period of time to determine the answer and the requesting unit probably does not have the collection resources to monitor the airfield.

As an RFI travels up the chain of command, it is satisfied (from available information or intelligence or by collecting new data), converted into a PR, or forwarded to the next higher level for satisfaction. Each unit in the chain of command validates the PR and either satisfies it from within or passes the requirement to the next higher authority for action. Figure 9-1 illustrates the generic flow of PRs.

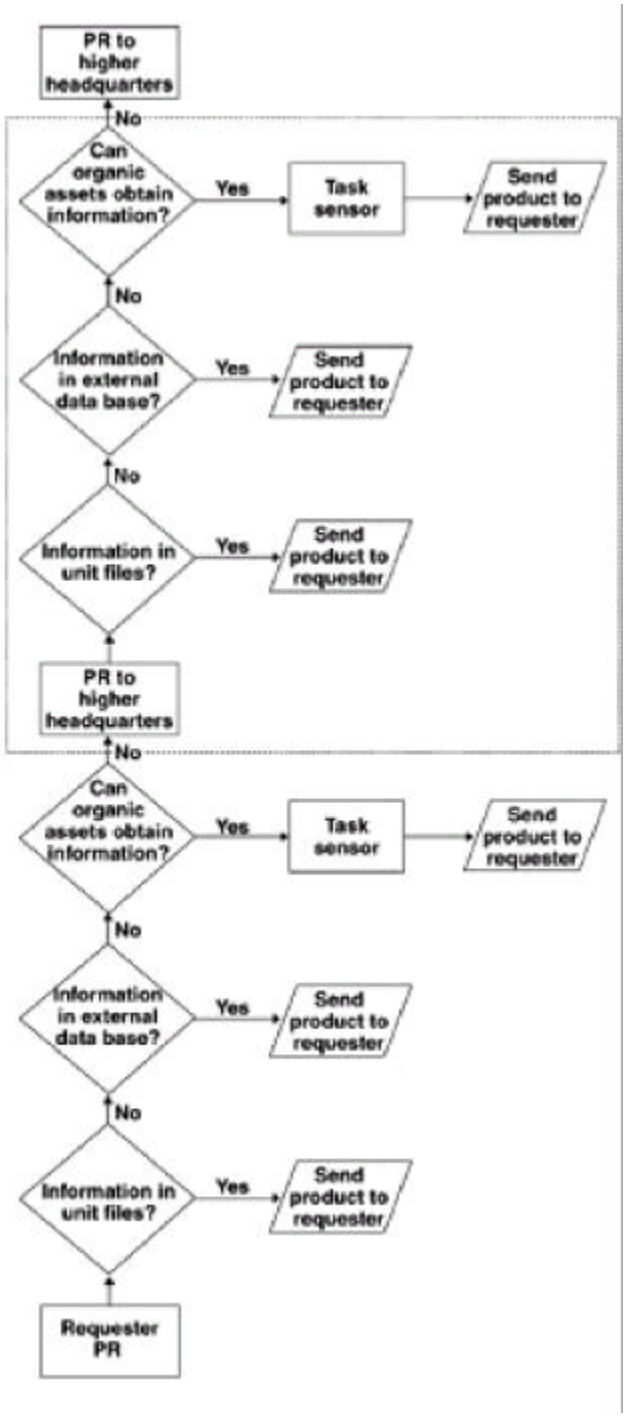


Figure 9-1. IPR Flow.

Request Process

Most IPRs are levied on the intel bn, P&A company's P&A cell, which is the MAGTF's principal deliberate production asset. Based on the commander's guidance and the G-2/S-2's direction, the intel bn commander or ISC—

- Plans, manages, and conducts MAGTF IPR management.
- Exercises staff cognizance over MEF collection and production elements to fulfill PRs.
- Determines which PRs are produced locally and which PRs are forwarded to the appropriate theater, Service, or national DODIPP production center validation office (VO).

The VO reviews the PR, determining whether to accept and satisfy the PR, forward the PR to another production center, or invalidate the PR. The combatant commander, the JFC, or the MAGTF commander directs PR and RFI procedures, which vary from theater to theater. For example, a MAGTF preparing to deploy submits PRs through the normal Service chain of command to the MCIA VO. However, a MAGTF operationally assigned to a combatant commander submits PRs through the established operational chain of command to the VO supporting that theater. A theater intelligence directorate (J-2) may delegate validation authority to a JTF J-2 during a crisis, providing the JTF J-2 a streamlined path for JIC production support and priority over other non-crisis production requirements. For most crises and contingencies, annex B to the joint force commander's OPLAN or OPORD specifies policies and procedures for requesting intelligence production support.

Request Format

The same basic format is generally used for RFIs and PRs. This facilitates conversion of an RFI into a PR at a later time. A basic level production request must include—

- Organization(s) and specific office(s) or individual(s) requesting the product.
- Statement describing the—
  - Required information and intelligence.
  - Sources consulted by the requester and source shortcomings relative to the request.
- Latest time information of value.
- Product form (e.g., hard copy text, electronic file on disk) and total quantity of each.
- Requirements prioritization for multiple elements.

The basic format provided above is sufficient at lower tactical levels; however, at higher levels the format becomes more structured. Defense Intelligence Management Document 0000-151C-95, *Department of Defense Intelligence Production Program (DODIPP): Production Procedures (U),* stipulates the format for PRs, which ultimately will be forwarded to a DODIPP VO and production center. See appendix I for PR format. Each combatant command defines formats and procedures in their applicable intelligence TTP documents. The MEF CE and MSC headquarters SOPs defines formats for their headquarters subordinate elements.

Automated Production Request Procedures

Community On-line Intelligence System for End Users and Managers (COLISEUM) provides an automated capability for the preparation, submission, validation, and assignment of PRs within the DOD intelligence production community. With this system, the requester researches existing requirements and responses to reduce the submission of duplicate requirements. Commands and production centers with access to COLISEUM have immediate visibility of existing and new requirements validation and production status and product completion notification.

Designed to function as an application under the Joint Deployable Intelligence Support System (JDISS) program, COLISEUM is currently available on JDISS 1.01 and JDISS 2.0. The IAS also provides access through JDISS. In addition, the COLISEUM is available on INTELINK sensitive compartmented information (SCI) under

DIA, Directorate of Intelligence Production. The principal inject sites for Marine Corps operating forces PRs are the MEF and Marine Corps forces (MARFOR) G-2s. The MEF, MARFOR, CINC, and DOD policy documents govern procedures for submitting PRs via COLISEUM.

CHAPTER 10. OPERATIONS

Intelligence enables the planning and execution of successful operations. Unity of effort, high tempo, timely decisionmaking, rapid execution, and the relentless exploitation of decisive opportunities characterize MAGTF operations. Intelligence P&A must have the flexibility, agility, and sustainability to support MAGTF operations. This chapter discusses intelligence P&A planning and execution considerations for various MAGTF operations and phases.

Expeditionary in nature, MAGTF operations are conducted according to the following Marine Corps maneuver warfare and emerging operational concepts, which present unique challenges and considerations for intelligence support:

- **Operational Maneuver From The Sea—The maneuver of operational-level naval forces projects sea-based power ashore to deal a decisive blow at a place and time of our choosing. Operational maneuver from the sea (OMFTS) focuses on operational objectives and embodies the application of the principles of maneuver warfare to a maritime campaign.**
- **Sustained Operations Ashore—Those campaigns in which MAGTFs fight as sea-based operational maneuver elements. Embracing the tenets of OMFTS, sustained operations ashore (SOA) envisions a series of operational-level missions designed to enhance the joint force campaign and exploit weaknesses exposed in the opposing force. Normally, SOA involve a MEF assigned to a larger joint or combined force.**
- **Military Operations Other Than War—The conduct of Marine and naval expeditionary operations across the range of military operations short of war. MOOTW encompass a wide variety of activities intended to deter war, resolve conflict, promote peace, and support civil authorities.**

SECTION I. OPERATIONAL MANEUVER FROM THE SEA

Success in OMFTS depends on the ability to seize fleeting opportunities and quickly take advantage of enemy vulnerabilities. Emphasis is placed on deception, surprise, speed, and battlespace preparation to create delay, uncertainty, and ineffectiveness in enemy actions. Intelligence provides the knowledge and understanding that enables the effective conduct of OMFTS. Operational maneuver from the sea relies on intelligence to drive planning, COA development, wargaming and selection, and execution by—

- **Identifying the enemy's COG(s), strengths, and weaknesses.**
- **Exposing critical vulnerabilities to be exploited by naval forces operating from the sea.**
- **Assessing the potential for maneuver offered by the battlespace, to include identifying entry points where the force can establish ashore.**
- **Providing the foundation for effective force protection and C2W efforts, which facilitate the preservation of surprise and the employment of deception to disrupt and disorient the enemy during OMFTS.**

Requirements

Key OMFTS intelligence P&A support requirements include—

- **IPB and situation development covering a broad air, sea, and land maneuver space.**

- Threat analysis focused on determining COGs and critical vulnerabilities.
- Detailed terrain and hydrographic analysis, which identify suitable entry points and support maneuver of widely dispersed combat and CSS elements.
- Responsive processing, analysis, and production capabilities that can rapidly develop the critical intelligence required to shape operational and tactical decisionmaking and to provide the intelligence segment of the common operational or tactical picture.
- Indepth intelligence support of force protection and C2W activities.
- Detailed information regarding local resources (e.g., petroleum, oils, lubricants, water) to reduce MAGTF ashore sustainment requirements.

Considerations

Although the requirements appear similar to the traditional amphibious operations intelligence support requirements, OMFTS presents the following unique considerations:

- The large potential AO may extend 200 nautical miles or more from the sea base.
- Points of entry may be widely dispersed instead of being grouped into a single force beachhead.
- The sea space becomes a maneuver area for LCACs and advanced amphibious assault vehicles transiting to the shore from over the horizon, requiring extensive and detailed hydrographic analysis over a larger area.
- The OMFTS forces rely on rapid maneuver for maximum effectiveness and survivability, necessitating detailed and accurate terrain analysis.
- The vision of dynamic, precision fires at maximum engagement ranges requires precise targeting data and BDA.
- Analysis must occur in real or near-real time and must be available simultaneously to every MAGTF unit and element.
- Intelligence products must be in a format that can be rapidly updated and displayed in graphic form on automated information systems to be used by units, staffs, and decisionmakers.

Support During Planning

Initial production efforts are directed at providing an extensive description of the battlespace and threat required to focus the planning effort. Under the direction of senior Navy and Marine intelligence officers, the MAGTF, MSC, naval expeditionary force, amphibious staff, and ship's intelligence sections engage in a collaborative effort to plan and execute intelligence and reconnaissance operations necessary to support development of intelligence products that support the force.

Individual intelligence sections normally concentrate on their particular areas of expertise, satisfying their units' requirements while contributing a broad-scope product to the general production effort. The MAGTF G-2 CIC or P&A cell may focus on describing the battlespace and enemy C2, logistics, and reserves; while the ground combat element's intelligence section studies the enemy ground forces. The amphibious force and the aviation combat element's intelligence sections both look at air and air defense threats, and the amphibious task force (ATF) intelligence staffs concentrate on the naval, sea mine, and coastal defense threat.

Intelligence personnel access national, theater, and adjacent component resources via reach back to augment organic resources of the force. The integrated Navy and Marine amphibious force intelligence center provides a comprehensive IPB analysis, intelligence estimate, HVT list, and supporting intelligence studies by coordinating amphibious force efforts. As the

planning phase continues, production efforts are concentrated on identifying enemy vulnerabilities to be exploited, providing IPB products, HPTs, and intelligence estimates to support specific COAs under consideration.

In the final stages of the planning process, the production effort shifts to development of mission-specific intelligence products focused on the selected COA(s). These products include IPB graphics, point of entry studies, and target or objective studies. In addition, an extensive all-source intelligence effort supports deception, operations security, psychological operations, and electronic warfare planning according to the commander's information operations or C2W strategy. The production effort becomes increasingly decentralized as MSC and subordinate element intelligence sections focus on their units' specific requirements. The MAGTF CE intelligence section continues to provide products to support the entire force, concentrating on elements designated as the main effort.

Support During Execution

During the execution phase, emphasis is placed on rapid processing and production of intelligence that supports timely decisionmaking, enhanced situational awareness, and engagement of HPTs. Because OMFTS depends on decisive action and operational tempo to break the enemy's cohesion and ability to resist, intelligence personnel must be able to—

- Demonstrate flexibility, agility, and responsiveness to recognize threat vulnerabilities and identify opportunities as they develop during battle.
- Demonstrate an awareness of ongoing operational and tactical activities and potential threat actions or reactions.
- Integrate rapidly all-source intelligence information with sensor data and combat reporting to develop a coherent, timely, and tailored picture of enemy dispositions and an assessment of its intentions and capabilities.
- Convey rapidly the developed picture and assessment to commanders in time to exploit identified opportunities.
- Engage fully in planning for future operations by continuing IPB analysis, delivering BDA results, satisfying new intelligence requirements, and participating in the decisionmaking process.

SECTION II. SUSTAINED OPERATIONS ASHORE

Sustained operations ashore require broad-based intelligence support that bridges the operational and tactical levels. Tactical plans are based on operational-level intelligence assessments, which identify the enemy's COG(s) and critical vulnerabilities across the entire theater.

In SOA, MAGTF intelligence operations contribute to the operational level assessments while translating the conclusions from those assessments into relevant tactical intelligence.

While OMFTS focuses on operations from a sea base, SOA entails large-scale, potentially long-term, land operations supported from the sea. Critical aspects of SOA include a large AO and rapid operational tempo. While P&A in OMFTS is heavily tasked with identifying points of entry, SOA focus on infrastructure related to sustaining a large force. Analysis of threat COGs and vulnerabilities, detailed terrain studies, precise targeting data, and BDA remain requirements under SOA.

Considerations

Considerations for the development of intelligence in support of SOA are similar to those for OMFTS. Intelligence support during the execution of SOA requires the same agility and responsiveness as in OMFTS, with the focus on providing critical intelligence to support tactical decisionmaking. However, SOA are normally conducted over a greater area and with a larger size force than in OMFTS, creating the requirement for a larger and more widely distributed intelligence operation support structure. The potential for integration with theater, allied, and other Service intelligence assets are also greater than in OMFTS.

Support During Planning

P&A efforts in support of SOA parallel those for OMFTS. Initial production is broad in scope, with the focus narrowing as particular COAs are selected and a concept of operations is developed. In SOA, GEOINT production takes on added importance; opportunities for ground and air maneuver as well as LOS profiles for observation, weapons employment, and communications-electronic equipment operations are major considerations. Mapping enhancements, LOC studies, and IPB graphics (e.g., cross-country mobility, weather effects, and COOs) are key products.

Threat analysis must be comprehensive and generally deals with large ground and air formations. This analysis covers reserves as well as committed forces and must take into account factors that impact the enemy's ability to fight at the operational and tactical levels (e.g., leadership, doctrine, training, readiness, and sustainability).

An extensive production effort is devoted to supporting logistic operations. The main components of this effort are studies of the local climate, infrastructure, and resources as well as the rear area threat. Products from national, theater, and joint force intelligence agencies contribute to the production effort, but many of these products will be tailored by the intel bn's P&A company, other intelligence producers, and the MSCs' intelligence sections to satisfy particular MAGTF requirements.

Support During Execution

During execution, emphasis is placed on rapid processing and production of tactical intelligence to support operational decisionmaking in the current battle, while at the same time providing detailed intelligence to shape plans for future operations.

SECTION III. MILITARY OPERATIONS OTHER THAN WAR

Military operations other than war include the following missions and tasks, which present unique intelligence requirements:

- Humanitarian assistance and disaster relief.
- Noncombatant evacuation operations.
- Maritime intercept operations.
- Show of force.
- Strikes and raids.
- Peace operations, including peace enforcement and peacekeeping.
- Support to counternarcotics operations.
- Recovery operations.

Requirements

Intelligence shapes operations during MOOTW as it does during other types of MAGTF operations. However, in addition to understanding the physical environment and the threat, the commander must have intelligence on political, economic, and sociological conditions to develop sound military plans that will accomplish the assigned mission. To support MOOTW, MAGTF intelligence personnel must be able to—

- **Focus on areas with the greatest potential for the execution of contingency operations.**
- **Respond with minimal warning and preparation.**
- **Adapt to a wide variety of potential missions and possess expertise and specialized capabilities to provide MOOTW intelligence.**

Considerations

Intelligence P&A activities in MOOTW are generally characterized by—

- **The initial lack of detailed data bases on the AO and threat forces.**
- **An extensive list of nonstandard intelligence requirements that must be satisfied to support planning and execution (e.g., uncertain force protection requirements).**
- **Analysis of nonmilitary related data.**
- **A rapidly changing situation resulting from crisis conditions in the AO.**
- **Compressed timeframe for intelligence development.**
- **Restrictions on collection operations and the dissemination of intelligence, particularly with multinational military forces, NGOs, and PVOs.**
- **Increased likelihood of participation by coalition partners.**

Support During Planning

Intelligence P&A requirements in MOOTW are normally focused on nontraditional subject areas and IRs. For example, more detailed knowledge of the host nation's economic, transportation, medical, and public works infrastructure will be required to develop plans for humanitarian assistance operations. A threat study to support a peacekeeping mission must encompass an extensive treatment of political, cultural, and sociological factors related to various insurgent or paramilitary factions in addition to the conventional military capabilities of the opposing sides.

Collaboration and coordination with area specialists and expertise from external intelligence organizations, non-DOD agencies (e.g., State Department, Office of Foreign Disaster Assistance, U.S. Agency for International Development) and NGOs or PVOs are crucial to satisfying MOOTW requirements. In turn, the requirement to share information and intelligence with those same agencies, as well as host-nation and allied forces, has a significant impact on analysis, production, and dissemination. While the goal is to provide necessary information and intelligence to participants in the operation, some information must remain releasable only to U.S. forces or allies with long-standing intelligence exchange agreements.

Production formats generally must be adapted to the requirements of a particular situation (e.g., normal IPB products must be modified to highlight factors critical to the specific MOOTW mission). In addition, P&A in MOOTW must be responsive to the unique needs of a large number of small elements conducting independent activities throughout the AO. Production in support of these elements must be tailored to specific mission requirements and provide details pertinent to the small unit level. Intelligence that increases the situational awareness of individual Marines (e.g., information on local customs,

language, health and sanitation) is an important part of this effort.

MOOTW IPB Requirements

The principal difference between IPB for conventional war and MOOTW activities is the focus and the degree of detail required to support the commander's decisionmaking process. Another major difference is the enormous demand for demographic analysis, since the population often is the focus in MOOTW. Typically force protection IRs take on greater priority. The four steps of the IPB process and sample aspects and considerations for various MOOTW activities, are discussed below. (See FM 34-130/FMFRP 3-23.2 for a discussion of each type of operation.)

Define the Battlespace Environment

Intelligence personnel define the MOOTW battlespace environment by expanding the AOI, assembling data on terrain and infrastructure, and compiling data on the host nation.

Expand the AOI

To expand the MOOTW AOI, intelligence personnel must—

- Identify potential sources of assistance to friendly force operations from outside the country or AO.
- Identify military, paramilitary, governmental, nongovernmental, and private volunteer organizations that may interact with the friendly force.
- Identify and locate external influences on the operation.
- Consider media, political, and third nation support or interference.
- Identify the geographic boundaries of the operation, applicable legal mandates or terms of reference, and other limitations or constraints that may impact on the operation.

Assemble Data on Terrain and Infrastructure

To assemble data on MOOTW terrain and infrastructure, analysts must—

- Identify existing infrastructures that have the potential for use by either threat or friendly forces in the operational area.
- Include sources of basic sustenance and energy, as well as transportation and communication networks.
- Identify facilities in adjacent or intermediate countries that could support the introduction of friendly forces or the delivery of necessary materials.
- Compile data on the geography and climate of the area, to include unusual or violent weather patterns or natural disturbances.

Assemble Data on the Host Nation

To assemble data on a MOOTW host nation, intelligence personnel must—

- Identify the existing government and military infrastructure.
- Pay particular attention to their capabilities and limitations with regard to support for or interference in the operation.
- Begin compiling demographic data on the population, to include age, education, religious beliefs, cultural distinctions, ethnic makeup, allocation of wealth, political affiliations and grievances, languages, values, and practices.

Describe the Battlespace Effects

Intelligence personnel describe MOOTW battlespace effects by identifying legal aspects, conducting terrain and weather analysis, evaluating the threat, and determining threat COAs.

Identify Legal Aspects

The MAGTF staff judge advocate should fully explain the impact of legal mandates, terms of references, or other diplomatic agreements. Intelligence personnel should include legal mandates in place that will have a major effect on friendly COAs, particularly rules of engagement and use of force.

Conduct Terrain Analysis

To conduct terrain analysis for MOOTW, intelligence personnel must—

- **Use military aspects of terrain or KOCOA.**
- **Pay attention to routes and areas that offer good observation for friendly security forces.**
- **Depict potential obstacles, choke points, and ambush sites.**
- **Ensure that air and ground AAs are included.**
- **Include analysis of the urban terrain.**

Conduct Weather Analysis

To conduct a standard weather analysis for the MOOTW AO, intelligence personnel must consider the effects of weather on—

- **Displaced persons or refugees.**
- **Hostile groups.**
- **Trafficability.**
- **Air operations.**
- **Seaborne operations.**
- **Night operations.**
- **Communications.**
- **Threat tactics and civil disturbances (e.g., rallies and demonstrations).**

Evaluate the Threat

Doctrinal templates for typical types of threats faced in the MOOTW environment are rare because there are many threats. Intelligence personnel must evaluate the threat according to the specific mission.

Weather

In missions involving humanitarian assistance and disaster relief, where the environment is the threat, intelligence personnel should—

- **Evaluate the environmental impact on the population and friendly operations by determining, for example, if continued rains and flooding could trigger mudslides isolating portions of the population and inhibiting relief operations.**
- **Prepare climatic studies showing historical paths and frequencies of destructive weather (e.g., hurricanes or typhoons), which can serve as a sort of doctrinal template to determine if earthquake aftershocks could collapse fragile water and sewage treatment facilities leading to an increase in waterborne diseases and environmental hazards.**

Competing Factions

In missions involving competing factions, some critical information and intelligence may exist in coalition, host nation, or U.S. data bases, which could be used to begin building a threat model for the operation. Intelligence personnel should recognize differences in threats, strategy, procedures and tactics, as well as weapons, equipment, material, and personnel.

Environment

When evaluating the threat, intelligence personnel must—

- **Determine if the environment is permissive, uncertain, or hostile to U.S. forces entering with or without host nation approval.**
- **Determine if the population supports U.S. forces and if that support is contingent on some type or form of material compensation from U.S. forces (e.g., food, water, shelter, weapons).**
- **Determine if the population is organized to oppose U.S. forces and if the people are**

armed and at what level (e.g., weapons, mines, vehicles).

- Identify dissident groups among the population that may publicly support but clandestinely oppose U.S. forces.
- Identify which terrorist groups are present, thought to be present, or have access to the AO, and if they are supported or directed.
- Identify leaders, trainers, and key staff members and develop psychological profiles on key personnel.

Determine Threat Courses of Action

This step in the IPB process is the culmination of battlespace environment analysis and threat evaluation. The success of U.S. operations in MOOTW depends on the combined efforts of state department officials, numerous government agencies, a unified command and its component Services, special operations forces, and the National Security Council. These organizations work together to accomplish foreign policy objectives of the United States and foreign allies. To determine threat COAs, intelligence personnel must—

- Template or describe the actions of the threat that would interfere with friendly operations (e.g., in peacekeeping operations any violations of the existing legal mandates by either belligerent could adversely effect friendly operations and security).
- Develop COA models depicting the reactions of the threat to friendly operations within the AO and AOI.
- War game each COA.
- Analyze reactions of local populace, multinational partners, NGOs, PVOs, and other key third or neutral parties to friendly COAs.
- War game terrorist and sabotage actions and other activities where the threat could reasonably avoid claiming responsibility, which could jeopardize friendly operations or security.

MOOTW IPB Products

The IPB products that may be useful in the MOOTW environment include (but are not limited to) population status, logistics sustainability, LOC, and key facilities and target overlays, as well as coordinates registers and pattern analysis plot sheets.

Population Status Overlay

To construct a population status overlay encompassing areas in the operation, intelligence personnel should, at a minimum, depict the population by political affinity or regional majority sentiment (e.g., progovernment, anti-American, neutral). If unable to ascertain some root causes of regional unrest (e.g., religious, ethnic, racial, or economic differences), intelligence personnel may display the population in terms of demographic differences. Points where demographic differences intersect often pose the greatest potential for conflict and possible disruption of friendly operations. See figure 10-1.

Logistics Sustainability Overlay

To construct a MOOTW logistics sustainability overlay, intelligence personnel should identify sources of food, potable water, fuel, etc. that could be used by the population, threat, or friendly forces. See figure 10-2.

Lines of Communications Overlay

To construct a MOOTW LOC overlay, intelligence personnel should—

- Identify routes into and out of the operational area.
- Include major streets, highways, railways, subways, waterways, etc.
- Analyze and depict the communication systems in place that could be used to support the operation (e.g., telephones, radio, television, satellite, and microwave systems). See figure 10-3 on page 10-10.

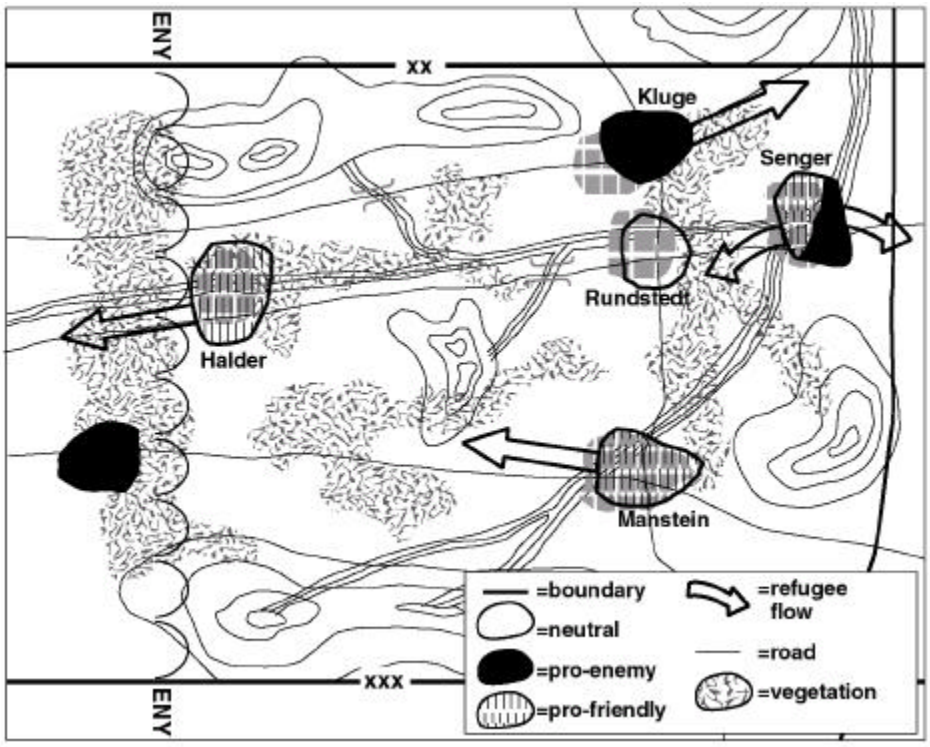


Figure 10-1. Population Status Overlay.

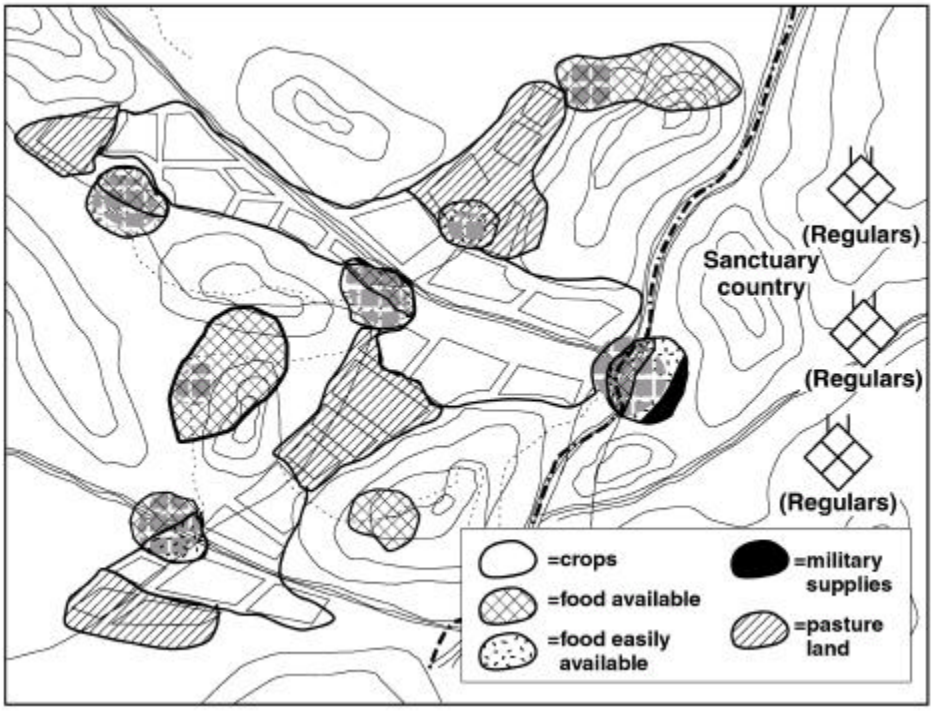


Figure 10-2. Logistics Sustainability Overlay.

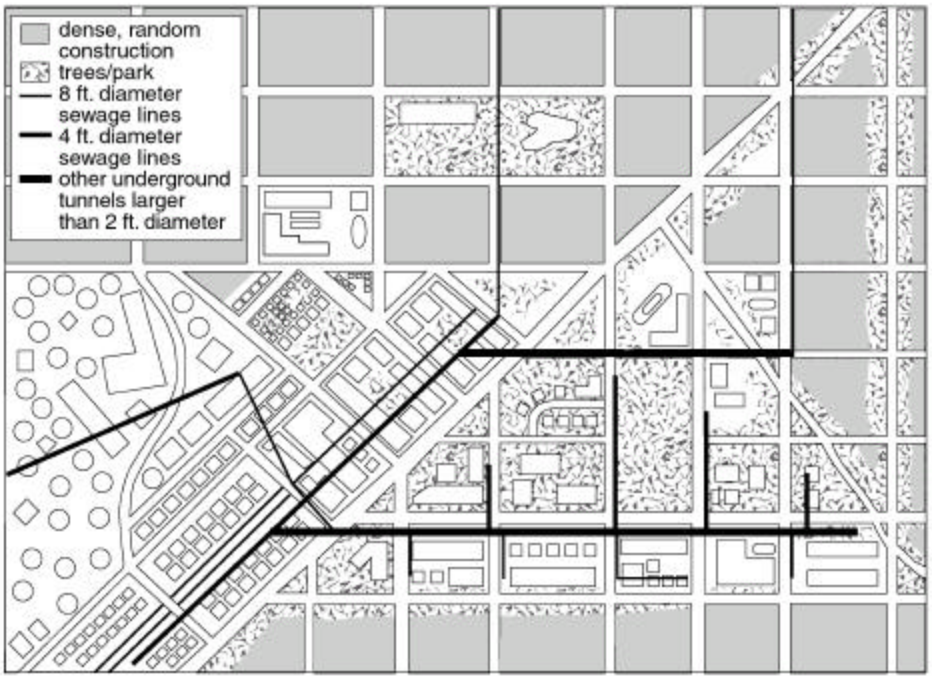


Figure 10-3. Sewers and Subterranean Overlay.

Key Facilities and Target Overlay

Intelligence personnel construct a key facilities and target overlay to depict mission-essential facilities and potential threat targets (e.g., embassies, religious or cultural facilities, military installations, television and radio facilities, government buildings, airports, port facilities, medical facilities, public utilities).

In a noncombatant evacuation operation, the U.S. embassy or the evacuation control center would be considered a mission-essential facility, but it would also be considered a potential target for belligerents.

Coordinates Register and Pattern Analysis Plot Sheet

Because intelligence data bases and doctrinal templates are often limited for many MOOTW situations, intelligence personnel use tools such as the coordinates register and times pattern analysis plot sheets (discussed in chapter 7) to conduct pattern analysis and to rapidly gain an understanding of threat TTP and methodologies.

SECTION IV. JOINT OPERATIONS

Marine Corps forces participate in full partnership with other Services in joint operations, either as a component or as the nucleus of a joint force. A coordinated intelligence effort makes a critical contribution to the success of joint operations. During joint operations, Marine intelligence P&A must be fully integrated with joint intelligence activities to ensure unity of effort, mutual support, and effective employment of limited intelligence resources. Effective intelligence support in joint operations depends on—

- **Agreement on policies and procedures.**
- **Mutual intelligence support.**
- **Sharing of intelligence capabilities and assets.**

- Full interoperability and connectivity among participants.
- Robust liaison.

Responsibilities

The JFC is responsible for intelligence support within the joint command and has responsibility and authority to determine, direct, and coordinate mission-related collection, production, and dissemination activities through centralized or apportioned intelligence requirements management efforts. Component commanders remain responsible for the intelligence function within their commands and employ organic intelligence capabilities to support their assigned missions. The JFC makes national, theater, and joint force intelligence assets available to support the efforts of component commanders. At the same time, component capabilities must be available to assist the joint intelligence effort.

Marine Corps Component Production and Analysis

When assigned as a joint force component, Marine Corps intelligence personnel at each level of command perform the P&A required to support their planning and decisionmaking based on prioritized information requirements; requirements unsatisfied with organic resources are forwarded up the chain of command. Each level of command also disseminates intelligence products to subordinate and adjacent units. Because these higher, adjacent, supporting, and subordinate units may be from a different Service, Marine Corps intelligence sections and units participating in joint operations must—

- Operate according to joint intelligence doctrine, theater TTP, and individual joint force procedures.
- All-source intelligence P&A to satisfy JFC and component IRs.
- Participate in joint intelligence mechanisms for the coordination of IR management (i.e., collection, production, and dissemination requirements).
- Provide P&A support to the joint force headquarters and other component commanders, as required.
- Employ joint or component P&A assets in support of Marine component operations.
- Ensure complete and reliable CIS connectivity within the joint intelligence architecture.
- Exchange liaison elements with the JTF intelligence directorate (J-2), joint intelligence support element (JISE), and/or other joint force component P&A entities as required.

Joint Task Force Headquarters Production and Analysis

A MAGTF may be designated as a JTF with the MAGTF CE forming the nucleus of the JTF headquarters. In this case, the G-2/S-2 must be prepared to function as the JTF J-2 with the MEF CE's intelligence section serving as the base for the establishment of a J-2 section and JISE. The JISE provides intelligence support to the JFC and the entire JTF.

Key Functions

When serving as a JTF J-2, MAGTF intelligence sections must operate according to joint doctrine and theater TTPs. The MAGTF G-2/S-2 must ensure that the P&A portion of the JISE is appropriately augmented or supported by specialists from national agencies, the theater JIC, and other Services possessing the necessary skills to satisfy the force requirements. Key functions performed in the JISE include—

- Centralized collection, production, and dissemination management for joint force and supporting intelligence and reconnaissance assets.

- Development and maintenance of intelligence data bases which support planning, operations, and targeting.
- Production of target studies and materials and intelligence support to force protection.
- Access to supporting national and theater intelligence assets.

Support During Planning

Intelligence product formats, standards, and dissemination means must be defined early to ensure JTF elements can exchange and use intelligence products. When possible, these definitions and standards should be planned for in advance and published in an SOP or TTP that is available to other Service units that may be assigned as part of a Marine-led JTF. The TTP or SOP should be exercised whenever possible to refine procedures and ensure unity of effort.

Support During Execution

The JFC, through the J-2, exercises complete coordination and some specified control over the P&A efforts of the joint force. Often, the J-2 is delegated direct IR validation, prioritization, and tasking authority for intelligence production by the supporting theater JIC. Incumbent with that authority, the J-2 is responsible for managing the force IRs and associated PRs.

SECTION V. COMBINED OPERATIONS

Marine Corps forces may participate in a variety of combined operations, ranging from routine bilateral exercises to coalition warfare in major regional contingencies. Instances of unilateral U.S. military operations are becoming less frequent, particularly in MOOTW. Joint doctrine serves as the doctrinal basis for combined or multinational operations. Each coalition or alliance must develop its own TTP for each operation. The coalition commander determines standardized procedures for coalition forces. NATO STANAGs and quadripartite standing agreements between U.S., British, Canadian, and Australian forces provide standards and guidance for the conduct of military operations by forces in these alliances. See STANAG 2936, *Intelligence Doctrine-AIntP-1(A)*, which governs intelligence operations.

Principles

Successful combined intelligence operations are based on the following principles and considerations.

Adjustment of National Differences Among Nations

Effective combined operations require minimizing the differences in national concepts and TTP for intelligence support. Commanders and their intelligence officers must be prepared to make adjustments to U.S. TTP to facilitate the sharing of intelligence and the integration and interoperability of intelligence and reconnaissance operations.

Unity of Effort Against Common Threat

Intelligence operations must be directed at the common threat. A threat to one alliance member must be considered a threat to all.

Intelligence Determination and Planning

Combined force's IRs and procedures should be identified, planned for, coordinated, and exercised prior to execution of operations.

Special Arrangements

Special arrangements should be considered for developing, communicating, and using intelligence where there are differences in nations' language, culture, doctrine, terminology, organization, as well as intelligence and CIS equipment.

Full Exchange of Intelligence

Each coalition member should share intelligence that supports planning and execution of coalition operations. Intelligence personnel should obtain authorization for foreign disclosure and outline procedures for disclosure and release of intelligence as part of the planning process. During execution, intelligence personnel should monitor the exchange of intelligence and adapt requirements to ensure coalition partners' needs are satisfied.

Complementary Intelligence Operations

Intelligence personnel should integrate and employ each nation's intelligence assets to capitalize on their strengths and offset their weaknesses, providing the coalition with the most effective blend of intelligence and reconnaissance capabilities.

Combined Intelligence Centers

A combined command headquarters should be supported by a combined intelligence center. The center should be manned by personnel from each nation and include appropriate linguist and translator support. This center—

- Develops coalition IRs.
- Validates and establishes priorities.
- Develops integrated intelligence plans.
- Commands and controls intelligence operations.
- Fuses intelligence received from alliance members.
- Disseminates this intelligence to the combined force.

Liaison Exchange

Exchange of intelligence liaison personnel between alliance partners bridges national differences and facilitates the exchange of intelligence and intelligence support.

Foreign Disclosure and Releasability

An important consideration for intelligence P&A in combined operations is the ability to release or disclose intelligence to non-U.S. members of the combined force in a timely manner.

Releasability involves the conveyance of information in documentary form to a foreign national. The document may be a publication, map overlay, imagery, computer disk, or any media that is physically provided to the foreign national.

Disclosure is the conveyance of classified information to a foreign national through either oral or visual means. Disclosure covers classified information that is retained by the United States but is discussed, briefed, or viewed by a foreign national. Often, regardless of whether information and intelligence is released or disclosed, the source(s) of that information and intelligence must not be revealed. Although the members of a coalition are united toward a common goal, it must be assumed that members' intelligence services will attempt to gather information on U.S. capabilities.

Policies and Procedures

The Director of Central Intelligence, DOD, Service, and theater policies and procedures govern foreign disclosure and releasability. The theater CINC is ultimately responsible for establishing policy regarding disclosure and releasability. During crises or contingencies, the CINC may choose to delegate authority to subordinate U.S. joint, combined, or component commanders. When so delegated, each recipient of that authority is responsible for publishing releasability and

disclosure guidance and procedures for their subordinate elements.

During combined operations, MAGTF CEs may be required to act as either a functional or Service component headquarters or as a combined task force headquarters, performing foreign disclosure oversight and guidance. Even when operating as an element of a combined force, every unit and individual Marine must be aware of foreign releasability and disclosure guidance.

Based on the established guidance and procedures, intelligence analysts must pay particular attention to the sources of information and the releasability of the information and intelligence derived from each of those sources. Often one version of an intelligence product must be produced for U.S. forces (and some standing alliance or quadripartite partners), and one version must be releasable to the multinational force.

Security

A balance must be struck between safeguarding classified information and intelligence and ensuring coalition partners are adequately informed and protected. One method for enhancing dissemination while providing necessary security of threat intelligence is to use the tear-line technique in the production process. This process ensures that intelligence and other information below the tear line is releasable to the combined force while simultaneously providing for the protection of U.S. collection intelligence sources and methods. Ultimately, the commander has the final authority to authorize foreign disclosure of information and intelligence directly related to a threat to any coalition partner.

Product Format Considerations

In combined operations, the form in which intelligence is conveyed is critical. Many potential coalition partners lack the technological and functional sophistication to collect, produce, and disseminate intelligence and exercise C2 over intelligence operations. Access to networks using SIPRNET or JWICS is generally not possible due to the inability to restrict the user from accessing unauthorized intelligence and friendly information. Language barriers may affect less sophisticated forms of intelligence dissemination such as text documents or briefings. The ability to exchange and use intelligence may vary from partner to partner.

Solutions for these challenges must be addressed early in planning. Generally, production requirements increase as a result of the need to tailor intelligence for multiple recipients. Increased IRs should be matched with increased analysis, production, and dissemination resources to ensure the timely provision of intelligence throughout the force. Where possible, coalition intelligence personnel should assist in the production of intelligence tailored to support their forces.

Information Sources

The intelligence analyst in a combined operation has the increased burden of assessing the reliability and credibility of non-U.S. information and intelligence sources. While foreign militaries may lack the sophisticated technical means available to the United States, they often enjoy superior capabilities in HUMINT, particularly if they are ethnically or linguistically related to the population of the AO. The analyst may need time to establish the reliability of the source or the accuracy of the information. In addition, the analyst must be aware that foreign forces may withhold, filter, or distort the information provided to the United States to safeguard their intelligence sources and methods. The analyst should apply the techniques and procedures for assessing reliability and accuracy and be conscious of biases that may develop due to preconceived notions regarding the source.

SECTION VI. PRE-CRISIS PHASE

The MAGTF pre-crisis intelligence P&A efforts center on data base management, ongoing production activities, and training.

Data Base Management

The key to effective intelligence and CI P&A is the identification and maintenance of hard copy and electronic intelligence sources and data bases. Intelligence personnel should attempt to develop and maintain relevant data bases during day-to-day operations in garrison. Without the necessary pre-crisis P&A, the ability to provide needed support in a crisis will be diminished. Key sources of intelligence data include the intelligence reference library, statement of intelligence interest, and intelligence data bases.

Intelligence Reference Library

Although intelligence is produced and disseminated increasingly in electronic form, each intelligence section is required to maintain a basic intelligence library in support of command and intelligence functioning. The library should include publications which are tailored to the unit's mission and echelon and are necessary to support day-to-day intelligence planning, operations, and contingency operations. Publications should include maps, charts, imagery, graphics, pertinent finished intelligence, and key supporting documents. Intelligence library publications are categorized as required and nonrequired.

Required Publications

As higher headquarters-directed holdings, these publications represent the minimum required material needed to support intelligence and command functioning. The intelligence officer is responsible for reviewing and validating the command and subordinate command's required holdings to ensure that they meet the minimum intelligence operation support requirements. Requests for additions or deletions of publications will be submitted via the chain of command according to the guidance contained in current directives.

Nonrequired Publications

Intelligence sections maintain nonrequired publications to supplement minimum required holdings, to conduct planning and training, or to use as reference material. The intelligence officer is responsible for ensuring nonrequired publications are available to support intelligence requirements.

National, Service, and unified commands produce intelligence publications that provide intelligence and guidance for intelligence functioning. Procurement procedures are contained in current directives and local SOPs. The manpower or personnel staff officer (G-1/S-1) is responsible for the procurement of doctrinal and tactical publications (e.g., JPs, MCDPs, MCWPs, MCRPs, FMs); however, the intelligence officer is responsible for identifying requirements for these publications.

Statement of Intelligence Interest

The statement of intelligence interest (SII) is the vehicle by which commands register requirements for all-source finished intelligence. Each command must establish an SII with DIA to receive automatic distribution of intelligence publications in support of command requirements. The intelligence officer is responsible for coordinating with the appropriate Dissemination Program Manger (DPM) to ensure the commands's SII is up to date. Statements of intelligence interest are requested through DIA's online Joint Dissemination System (JDS) via INTELINK/INTELINK-S under the Director of Information Systems and Services.

Accounts can be applied for online and are forwarded to the appropriate DPM, which is

Marine Forces, Atlantic, Marine Forces, Pacific, or MCIA, respectively. Once the account is established, it may be modified online. The appropriate MARFOR headquarters or MEF CE intelligence officer determines specific policies governing echelons that may apply for JDS accounts. The Defense Intelligence Production Schedules list DOD planned general intelligence production. Most intelligence producers maintain some type of production forecast on their INTELINK and INTELINK-S web sites.

Intelligence Data Bases

The establishment of intelligence data bases allows the intelligence section to manage and use the large volume of available information and intelligence. Intelligence agencies have established various data bases suited to their needs, resulting in different systems available to support intelligence operations at various levels. The intelligence officer at each command echelon must be aware of relevant intelligence agencies' data bases and plan for their use to support operations. In addition, the intelligence officer should maintain access to appropriate national, theater, and Service data bases.

Data bases are available to Marine Corps commands equipped with the JDISS and the IAS, either as applications or through access to INTELINK and INTELINK-S. As modern information systems technologies mature, the structure and titles of the data bases change frequently. The MCIA 1586-001-96, *MAGTF Contingency Reference Guide*, is a compendium of agencies, products, data bases, and INTELINK sites of potential interest. This publication is available in hard copy, disk, and on-line via both INTELINK and INTELINK-S. In addition, national, theater, and Service producers have created electronic links from their INTELINK web sites to other pertinent sites.

Each intelligence section should create local data bases to support their contingency planning and the development of contingency intelligence support products. Most current intelligence files can be maintained on automated data base systems. Finished intelligence products, imagery, maps, and graphics are available on-line to facilitate data search, access, and retrieval. When assembled, a pre-crisis data base should consist of—

- Current target country intelligence and CI estimates.
- Intelligence reference publications (e.g., intelligence TTP for combatant commands the unit may support, intelligence TTPs or SOPs for other Services with which the unit may operate).
- Standard intelligence data base segments (i.e., modernized integrated data base).
- Mapping, charting, geodetic, and other geospatial holdings.
- Imagery library and related holdings.
- Current intelligence files.
- Open source publications.

Production

Pre-crisis intelligence production includes contingency intelligence production, IPB, exercise intelligence, and other intelligence requirements.

Contingency Intelligence

The main pre-crisis P&A effort of MAGTF and MSC intelligence sections is contingency intelligence production in support of potential missions. The intelligence section must review standing contingency plans and tasking in conjunction with staff operations and plans sections. Intelligence personnel should coordinate with operations and plans personnel to define the mission, scope, and tasks using the following methodology.

Define the Intelligence Requirements

The IRs should be well defined after coordination with commanders and their staffs. Properly focused IRs save time and valuable intelligence assets.

Research Data Bases

Available intelligence data bases should be reviewed before submitting RFIs, ICRs, IPRs, IDRs, or PRs.

Analyze and Synthesize Data

Intelligence personnel must consider data, information, and intelligence from all available sources for analysis and synthesis.

Prepare the Products

Products must be prepared in user-friendly formats and delivered in a timely manner.

Intelligence Preparation of the Battlespace

Pre-crisis IPB is conducted to develop basic and current intelligence needed to support the planning and execution of contingency operations. The extensive and detailed nature of intelligence required to support expeditionary operations demands that a comprehensive research, analytical, and production effort be undertaken far in advance of the initiation of such operations. This demands that commanders and staff principals conduct detailed contingency planning across functional areas and command echelons to identify specific detailed IRs. The pre-crisis period offers the opportunity to carry out a thorough, measured study of potential areas of MAGTF employment. Driving contingency planning efforts, the pre-crisis IPB is the principal contribution of intelligence to combat readiness.

Pre-Crisis Products

The IPB products that can be generated in pre-crisis analysis and production include—

- **Battlespace characteristics analysis.**
- **Terrain and weather analyses and templates.**
- **Weather effects matrices for various seasons and conditions.**
- **Threat models.**
- **Threat capabilities assessments.**
- **Threat COAs, when possible.**

Results

The completed pre-crisis IPB process provides the following products for each potential contingency area:

- **Tailored intelligence data base(s).**
- **Contingency intelligence study.**
- **Intelligence and counterintelligence estimates.**
- **Validated intelligence collection, production, and dissemination requirements.**
- **Integrated intelligence operations plan (collection, production and dissemination).**
- **Tentative tasks for supporting intelligence and reconnaissance units.**

Additional Purposes

In addition to the primary purpose of supporting contingency planning and execution, pre-crisis IPB—

- **Develops an intelligence data base for selected areas.**
- **Educates personnel on potential missions and AOs.**
- **Identifies intelligence collection, production, and dissemination shortfalls (e.g., IRs, key personnel, and equipment).**
- **Trains intelligence personnel in the IPB process and the development of intelligence in support of actual contingency missions.**

Exercise Intelligence

Exercise intelligence production should follow the same procedures as contingency intelligence production and should result in products that mirror image what will be used in an actual operation. The intelligence section should use real-world data bases, IPB, and scenarios whenever possible to enable realistic training of intelligence personnel and staff and to provide solid area and threat familiarization training for unit Marines and Sailors.

When conducting field training exercises, the intelligence section must provide the same quality of GEOINT, IMINT, SIGINT, CI or HUMINT, and other intelligence support as would be provided in an actual operation. Weather conditions and terrain will factor heavily into the success and safety of an exercise involving the actual maneuver and movement of air, land, and seaborne forces.

Other Intelligence

In garrison, the intelligence section is expected to provide indications and warning information and promote threat awareness. The intelligence section must keep the commander and staff, as well as those of subordinate units, informed on items of interest in the unit's assigned or potential contingency areas. This can be accomplished by providing periodic current intelligence briefings, affording access to intelligence publications, and/or preparing current intelligence read boards for commanders and staff members. With increased access to web technologies, the commander, staff, and subordinate units can review daily pertinent information posted on a web site. The intelligence section should always be prepared to field impromptu requirements as directed by the commander or staff.

Production and Analysis Training

While in garrison, intelligence P&A training is accomplished through individual training, element training, unit training, and MAGTF training.

Individual Training

The intelligence analyst receives an introduction to P&A topics at formal intelligence military occupational specialty training courses. However, to develop P&A proficiency, the intelligence section must have a continuing training program to enhance P&A skills.

Skills Development

The Marine intelligence analyst must train to further develop—

- **Comprehensive study and understanding of threat forces' doctrine, operational and functional methodologies, and TTP.**
- **Familiarity with potential operating areas' cultural, ethnic, sociological, and religious orientations, organization, perspectives, values, and issues.**
- **IPB skills, which cover analysis of contingency AOs, threat COGs, critical vulnerabilities, tactical practices, capabilities, and COAs.**
- **Intelligence research methods (e.g., information and intelligence sources, agencies, functions, capabilities, limitations, automated information systems, data base availability and procedures).**
- **Methods of collecting and reporting information.**
- **Processing, recording, and filing information methods (e.g., manually and electronically preparing overlays and posting situation maps).**

- Integration, analysis, evaluation, interpretation, and information synthesis skills to rapidly produce tailored intelligence products.
- Skills in the use of automated information systems to manage data, analyze information, and produce and disseminate GENSER and SCI intelligence products, using all means of presentation (e.g., briefings, text reports, graphics, overlays).

Exercises

Wargaming and command post exercises (CPXs) are the best vehicles for analytical training and must be done independently of major exercises to enhance analytical skills before they are needed. Normally, the majority of training comes as a result of practical application (i.e., preparation of IPB and other products in response to exercise or contingency requirements). Each product must be evaluated and critiqued with the analyst who developed it to improve their skills. The intelligence officer's wargaming goals should include—

- Providing participants with a thorough area and situation orientation.
- Validating the scope and area coverage of the initial IPB.
- Determining gaps in existing intelligence.
- Identifying areas for additional study.
- Developing new collection, production, and dissemination requirements.
- Developing an initial intelligence concept of operations and supporting contingency collection, production, and dissemination plans.

Element Training

Intelligence sections and elements must have an integrated training program to develop the individual, team, and unit skills and capabilities necessary to execute intelligence and reconnaissance operations during MAGTF operations. Section training should first emphasize building specialized individual production skills. Once individual skills are mastered, cross-training and development of depth should be emphasized. A building block approach is used, starting with small group or team training (e.g., watch section, country team, or production element) and working up to exercises employing the entire G-2/S-2 section and those of subordinate commands.

While a command staff exercise, CPX, or field exercise normally provides the best environment for the conduct of intelligence section training, independent G-2/S-2 section training should be conducted in advance of a major command training event. This allows the section to develop and test SOPs, cross train personnel in a variety of functions, and conduct indepth instruction in intelligence P&A. Each production requirement or exercise is a training opportunity and should have specific training objectives associated with it.

Unit Training

Intelligence units conduct training according to their unit's specific mission and functions. As intelligence specialty units are often employed as small, independent subelements, the majority of their training should be targeted at the team, subteam, or detachment level. Intelligence unit training should also emphasize the planning and execution of operations in response to the supported unit's requirements.

Each unit training evolution is an opportunity to enhance P&A training by requiring the development of objectives for each exercise. In addition, unit training must encompass specific, detailed intelligence objectives for commanders and other staff section personnel. Unit training for P&A should—

- Train intelligence sections in meeting tactical requirements by exercising deliberate and immediate tactical production.
- Exercise the IR management process and intelligence cycle between consumers and producers.
- Test and improve standard product formats and content.

- Critique and provide P&A effort feedback.
- Evaluate the effectiveness of integrating intelligence production operations with those of collection and dissemination.

MAGTF Training

This training combines MAGTF units and trains on a larger scale, which provides intelligence personnel the opportunity to exercise the production management function as well as integrate collections and dissemination with P&A. The MAGTF training provides the opportunity to—

- Test requirement priorities and procedures.
- Test the integrated production between the MEF CE CIC, other intelligence and reconnaissance units, and MSCs.
- Determine if the resulting test products meet the commander and staff's needs.

SECTION VII. WARNING AND DEPLOYMENT PHASE

Warning and deployment sets the intelligence foundation for the entire operation. During this phase, intelligence is expected to produce a high volume of critical planning and decision-making support in a short period of time. This phase is further complicated by the need to prepare P&A elements for deployment within the MAGTF. The IPB and contingency intelligence study prepared in the pre-crisis period and the knowledge and skills gained by intelligence personnel, commanders, and other staff personnel during training exercises is the key to the ability to deliver intelligence support and products early in the warning or deployment phase. Initial P&A efforts, production management, and standardization of products frame the warning and deployment intelligence phase of operations.

Initial Production and Analysis

Determine Initial Requirements

Key to the success in determining initial IRs is a clear understanding of the command's mission, assigned tasks, commander's intent and guidance, and a defined AO. Command and staff element requirements should be integrated so that comprehensive products can be developed to meet as many needs as possible.

The P&A goal should be to produce a product only once to avoid duplicating effort and wasting time and assets. Time is the driving factor in determining the amount of detail that can be put into the P&A effort in the warning and deployment phase.

Assemble and Focus Data Bases

With an understanding of the mission and AO, intelligence personnel can refine data bases and other intelligence holdings. Units should agree on standardization of products and data bases early on in this process. Product and data base standardization should be a minor effort if SOPs or TTPs exist and units have worked and coordinated together previously in IPB contingency intelligence study preparation and training. This effort is more complicated in a joint or combined force.

Develop Initial Estimate and Supporting Studies

Preparing the intelligence estimate is easier if the contingency intelligence study is prepared and IPB is in progress. The initial IPB provides the baseline descriptive intelligence to initiate planning and, when paired with the contingency

intelligence study, supports the preparation of an initial estimate and supporting studies.

Develop Collection, Production, and Dissemination Requirements

Shortfalls identified during preparation of the initial intelligence and CI estimates become the basis for development of new collection, production, and dissemination requirements beyond organic capabilities. New requirements must be turned into collection, production, and dissemination plans, necessitating support requests to component, JTF, and/or theater commands for action. The MAGTF intelligence section is responsible for developing these requirements and for coordinating with the planning section to ensure requirements are focused on operations.

Production Management

Production management validates and prioritizes IPRs among competing requirements to determine which ones have the most impact on the mission's outcome. Production must be managed ruthlessly during this phase to ensure that limited assets are properly focused. The commander must be actively involved in—

- Directing intelligence operation efforts.
- Setting priorities.
- Providing the intelligence officer with guidance on where to focus the effort and what requirements are most important.
- Evaluating the effectiveness of operations.

Continuous interaction with staff planners and subordinate commanders and intelligence officers is required to ensure ongoing production supports the development of friendly COAs. Requirements typically change frequently during this phase as COAs are identified, refined, or rejected. Production management must ensure flexibility and responsiveness. Time is the critical element in production during this phase, because requirements must be met on time, even at the expense of detail.

Standardization of Products

The use of standard products simplifies production and dissemination. To provide a cut-and-paste or fill-in-the-blank capability, products should be standardized and automated. Establishing standard products and a regular update schedule is an effective way of managing production and dissemination during this phase. Product standardization can head off constant requests for updates by organizations, which can drain production and dissemination resources and detract the focus from essential requirements. A system of standard products should be developed during training and carried over with only minor modifications.

SECTION VIII. EXECUTION PHASE

In addition to production management, MAGTF intelligence P&A during the execution phase of operations involves support to current operations, future operations, future plans, and targeting.

Production Management

Production management remains critical during the execution phase, as requirements tend to change rapidly. P&A resources must be focused on the main effort according to the commander's guidance and intent, the PIRs, and the unit's operations and intelligence concepts. The commander must balance the production effort between support to current operations and future operations planning. Usually, the higher the echelon, the greater the focus is on future operations and planning; the lower the echelon the greater the focus is on current operations. Normally, at

higher command echelons, commanders and intelligence personnel must remain responsive to their own and lower echelon commanders' tactical needs. During execution, the time element is even more critical, because execution often depends on timely receipt of intelligence required for decisionmaking.

Support to Current Operations

Support to current operations consists primarily of immediate tactical production that is keyed to the commander's decision points, PIRs, and location of HPTs. Each piece of data, information, or intelligence received undergoes immediate tactical processing and assessment to determine if it is pertinent to the ongoing operation. If deemed pertinent, the information is quickly analyzed, impacts are determined, intelligence estimates are prepared, and results are disseminated. Intelligence personnel must maintain situational awareness and understand the operational situation, current PIRs and IRs, and likely enemy reactions to anticipate and meet the needs for immediate tactical production.

Support to current operations must include P&A in support of deep and rear operations and resist focusing on the close battle. Intelligence support to current operations must be balanced against the need to support future operations and plans. Assets cannot be devoted to current operations at the expense of supporting planning for future operations. In addition to short, tailored, mission-focused products in response to an immediate tactical need, production includes regularly scheduled update briefs and intelligence summaries that help maintain a common picture of the battlespace supporting situation development.

Support to Future Operations

Depending on the timeframe of the operation, scope of the operation, and level of command, support to future operations consists of a mix of immediate and deliberate production. Future operations focus on the deep battle, which is defined either by distance or time. Intelligence products in support of future operations must focus on that same planning window and seek to provide the future operations team with a coherent projection of the battlespace and threat within that window.

The future operations cell focuses on a rolling or near-continuous IPB process by generating new COAs, ICRs, IPRs, IDRs and targeting priorities, DSTs, and synchronization matrixes as the battle or operation unfolds. Intelligence production supporting the future operations cell is focused on products generated during IPB, which have been constantly modified by the results of friendly and threat actions. Daily situation update briefings are necessary to ensure the future operations team remains aware of current actions that may impact future operations.

The primary intelligence P&A contributions are the BDA results and the estimate of the situation focused on the appropriate planning horizon. The BDA provides input into combat assessment, which in turn helps determine the nature of future operations. Derived from the continuous IPB effort, the situation estimate provides the basis for planning.

During future operations planning, IPB and estimates draw on and extend previous work rather than generating new production. The intelligence P&A effort requires continuous interaction with the future operations cell. As decisions are made concerning future operations, integrated collection, production, and dissemination requirements are developed and prioritized, missions are assigned, and mission-specific products are prepared. Management of the time element is critical to ensure that products reach the future operations cell, mission planners, and executers in a timely manner.

Support to Future Plans

The MEF CEs, components, and JTF headquarters often require an additional planning cell focused on the next campaign or major phase change within the CINC's campaign plan. This cell, or operational planning team, in the MEF CE looks into the future and deals more in assumption than fact. Production in support of future planning tends to be deliberate and generalized but still encompasses the basic elements of IPB.

Often, the future plans cell is located out of the immediate operations area and may locate in close proximity to the CINC headquarters to facilitate communication and collaboration. Given the timeframe and location of potential future operations, the supporting theater intelligence center may be more suited to produce required intelligence products, with MAGTF intelligence personnel tailoring these products to support the needs of the future plans cell.

Support to Targeting

Intelligence support to targeting requires a continuous, integrating support effort to current and future operations. This support consists of target development (generated through IPB), immediate tactical production of new intelligence related to particular targets, and BDA of the mission execution results. At higher command echelons, the targeting cycle can span days, while at lower echelons it may span hours or minutes. In MAGTFs with organic fixed-wing aviation, the intelligence support to targeting is driven by the ATO cycle. An important goal is the synchronization of the collection and production phases with the appropriate phases of the PDE&A and ATO cycles to ensure the provision of relevant and timely target intelligence.

APPENDIX A. INTELLIGENCE ESTIMATE FORMAT

An intelligence estimate can be prepared at any level, from the battalion or squadron through the Marine expeditionary force command element and Marine Corps forces headquarters levels. The intelligence estimate should be succinct, yet provide the commander and staff the necessary information for decisionmaking. The scope and detail of an intelligence estimate are governed by the—

- **Level of command preparing it.**
- **Nature of the operation it is intended to support.**
- **Current availability of intelligence.**
- **Prior contingency planning.**
- **Time and resources available.**

Whenever possible, the intelligence estimate should clearly present the analysis and conclusions developed during intelligence preparation of the battlespace (IPB). The finished estimate may be in written, graphic, or verbal form, but should always follow the general five-paragraph structure presented in the following pages. Subparagraphs and tabs may be added and omitted based on their relevance to the stated mission. For topics that require a large amount of data, information, and intelligence (i.e., beaches, weapons capabilities, technical characteristics), the salient facts and conclusions should be summarized in the body of the estimate and the detailed data included as a tab.

For a discussion of IPB and the intelligence estimate, see chapter 4. Chapter 5 provides a discussion of the various factors that constitute paragraph 2 of the estimate. Chapter 6 provides a discussion of the factors that constitute paragraph 3.

The sample on page A-2 is the format for an intelligence estimate in support of conventional combat operations. The sample on page A-10 is the format for an intelligence estimate in support of military operations other than war (MOOTW).

SAMPLE FORMAT OF AN INTELLIGENCE ESTIMATE IN SUPPORT OF CONVENTIONAL COMBAT OPERATIONS

(Local variations and modifications may be made as necessary to meet requirements.)

CLASSIFICATION

Copy no.__of__copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time of issue
Message reference number

INTELLIGENCE ESTIMATE (NUMBER) (U)

(U) REFERENCES
- **(a) Maps and charts**
- **(b) Other pertinent intelligence documents and online data bases**

Intelligence and Information Cutoff Time Used for this Estimate: (Provide date-time group)

1. (U) Mission. (The command's restated mission as developed during the mission analysis phase of the planning process.)

2. (U) Characteristics of the Area of Operations. (State conditions that exist and indicate the effect of these conditions on enemy capabilities and the assigned mission. Assess the estimated effects of these conditions on both enemy and friendly capabilities and operations.)

a. (U) Military Geography

(1) (U) Topography

(2) (U) Drainage

(3) (U) Vegetation

(4) (U) Surface Materials

(5) (U) Military Aspects of Terrain

(6) (U) Effects of Terrain on Enemy and Friendly Capabilities and Operations

b. (U) Hydrography

(1) (U) Coastline Description

CLASSIFICATION

(2) (U) Hydrographic Conditions

(a) (U) Surf

(b) (U) Tides

(c) (U) Currents

(3) (U) Beaches

(4) (U) Effects of Hydrography on Enemy and Friendly Capabilities and Operations

c. (U) Climate and Weather

(1) (U) Type and Characteristics

(2) (U) Temperature

(3) (U) Precipitation

(4) (U) Visibility

(5) (U) Winds

(6) (U) Light Data

(7) (U) Flight Conditions

(8) (U) Effects of Weather on Enemy and Friendly Capabilities and Operations

d. (U) Transportation

(1) (U) Airfields

(2) (U) Helicopter Landing Zones

(3) (U) Port Facilities

(4) (U) Roads

(5) (U) Railroads

(6) (U) Inland Waterways

(7) (U) Effects of Transporation on Enemy and Friendly Capabilities and Operations

Page number

CLASSIFICATION

CLASSIFICATION

e. (U) Civilian Telecommunications and Media

(1) (U) International

(2) (U) Domestic

(3) (U) Mass Communications. (Types, capabilities, and key facilities.)

(4) (U) Radio

(a) (U) Television

(b) (U) Print Media

(5) (U) Effects of Telecommunications and Media on Enemy and Friendly Capabilities and Operations

f. (U) Economics and Infrastructure

(1) (U) General Economic Activity and Conditions. (Industry, public works and utilities, finance, banking, agriculture, trades and professions, labor force, etc.)

(2) (U) Monetary System

(3) (U) Power and Utilities

(4) (U) Petroleum, Oils, and Lubricants Facilities

(5) (U) Effects of Economics and Infrastructure on Enemy and Friendly Capabilities and Operations

g. (U) Politics

(1) (U) Political System and Climate

(2) (U) Local Political Conditions

(3) (U) Local Political Leaders

(4) (U) Policy and Attitudes Towards the U.S. and the U.S. Military

(5) (U) Effects of Political Situation on Enemy and Friendly Capabilities and Operations

CLASSIFICATION

h. (U) Sociology

(1) (U) Cities and Towns

(2) (U) Population and Distribution of Area and of Key Cities and Towns

(3) (U) Ethnic Composition

(4) (U) Languages

(5) (U) Religions

(6) (U) Customs and Norms

(7) (U) Social Institutions and Attitudes

(8) (U) Effects of Sociological Situation on Enemy and Friendly Capabilities and Operations

i. (U) Health and Medical

(1) (U) Food Supply

(2) (U) Water Supply

(3) (U) Diseases and Other Medical Problems

(4) (U) Plant and Animal Hazards

(5) (U) Sanitation

(6) (U) Medical Facilities

(7) (U) Effects of Health and Medical Situation on Enemy and Friendly Capabilities and Operations

3. (U) Enemy Military Situation

a. (U) Ground Forces

(1) (U) Composition, Organization, and Strengths. (Describe the structure of enemy forces [i.e., order of battle] and describe unusual organizational features, identity, etc. State the number and size of enemy units in and others available for use in the area of operations. Provide estimated combat effectiveness of enemy forces.)

CLASSIFICATION

(2) (U) Disposition, Locations, Movements, and Activities. (Describe the geographic location and latest known activities of enemy forces, including command and control facilities; fire support elements; and other key combat support forces.)

(a) (U) Committed Forces. (For ground forces, include units currently in contact or with which contact is imminent within the unit's area of operations, regardless of the specific friendly course of action. For amphibious or forcible entry operations, committed forces would be those that could immediately engage friendly units at their point of insertion. All fire support assets within range are normally considered committed, regardless of subordination. Conventional military forces are referred to by numbers of unit types [e.g., armor, infantry] two echelons below the friendly unit. Guerrilla or insurgent forces are expressed in terms of total numbers of personnel and fire support weapons.)

(b) (U) Reinforcements. (Describe the enemy's reinforcement capabilities in terms of possible forces and weapons that can react in time to affect the accomplishment of the mission. Factors to be considered include time available to react, terrain, weather, road and rail nets, transportation, replacements, and possible aid from sympathetic or participating neighbors.)

(3) (U) Weapons and Equipment. (Describe the operational capabilities and technical characteristics of major items of equipment in the enemy's inventory.)

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics. (Describe levels of supply, resupply ability, and capacity of beaches, ports, roads, railways, airfields, and other facilities to support supply and resupply. Consider transportation, hospitalization and evacuation, military construction, labor resources, and maintenance of combat equipment, etc.)

(6) (U) Training, Tactics, Operating Patterns

(7) (U) Capabilities and Effectiveness

Page number

CLASSIFICATION

CLASSIFICATION

b. (U) Naval Forces

(1) (U) Composition, Organization, and Strengths

(2) (U) Disposition, Locations, Movements, and Activities

(3) (U) Weapons and Equipment

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics

(6) (U) Training; Operational and Tactical Doctrine and Tactics, Techniques, and Procedures; Methods of Operations; and Operating Patterns

(7) (U) Capabilities and Effectiveness

c. (U) Air Forces

(1) (U) Composition, Organization, and Strengths

(2) (U) Disposition, Locations, Movements and Activities

(3) (U) Weapons and Equipment

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics

(6) (U) Training; Operational and Tactical Doctrine and Tactics, Techniques, and Procedures; Methods of Operations; and Operating Patterns

(7) (U) Capabilities and Effectiveness

Page number

CLASSIFICATION

CLASSIFICATION

d. (U) Air Defense Forces

(1) (U) Composition, Organization, and Strengths

(2) (U) Disposition, Locations, Movements, and Activities

(3) (U) Weapons and Equipment

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics

(6) (U) Training; Operational and Tactical Doctrine and Tactics, Techniques, and Procedures; Methods of Operations; and Operating Patterns

(7) (U) Capabilities and Effectiveness

e. (U) Paramilitary and Security Forces

(1) (U) Composition, Organization, and Strengths

(2) (U) Disposition, Locations, Movements, and Activities

(3) (U) Weapons and Equipment

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics

(6) (U) Training; Operational and Tactical Doctrine and Tactics, Techniques, and Procedures; Methods of Operations and Operating Patterns

(7) (U) Capabilities and Effectiveness

f. (U) Command and Control Warfare Capability

Page number

CLASSIFICATION

CLASSIFICATION

(1) (U) Intelligence, Counterintelligence, and Reconnaissance Capabilities

(2) (U) Electronic Warfare Capabilities

(3) (U) Psychological Warfare Capabilities

(4) (U) Deception Capabilities

(5) (U) Operational Security Capabilities

g. (U) Nuclear, Biological and Chemical Capabilities

h. (U) Night Combat Capabilities

i. (U) Unconventional Warfare Capabilities (e.g., guerrilla, subversion, sabotage, terrorism)

4. (U) Capabilities and Analysis. (List separately each enemy capability that can affect the accomplishment of the assigned mission. Each enemy capability should contain information on what the enemy can do, where they can do it, when they can start it and get it done, and what strength they can devote to the task. Analyze each capability in light of the assigned mission, considering applicable factors from paragraphs 2 and 3, and attempt to determine and give reasons for the estimated probability of adoption by the enemy. Examine the enemy's capabilities by discussing the factors that favor or militate against its adoption by the enemy. The analysis of each capability should also include a discussion of enemy strengths and vulnerabilities associated with that capability. Also, the analysis should include a discussion of any indications that point to possible adoption of the capability. Finally, state the estimated effect the enemy's adoption of each capability will have on the accomplishment of the friendly mission. The term "capabilities" includes not only the general courses of action open to the enemy (e.g., attack, defend, withdraw), but also the particular courses of action possible under each general course of action. These courses of action should correspond exactly to enemy course of action models developed during step 4 of IPB.)

CLASSIFICATION

5. (U) Conclusions and Vulnerabilities. (State conclusions resulting from discussion in paragraph 4 to include: enemy centers of gravity, critical and other vulnerabilities and estimated exploitability of these by friendly forces, enemy courses of action beginning with the most probable and continuing down the list in the estimated order of probability, and the estimated effects adoption of each capability would have on the friendly mission.)

/s/ _____
_____

TABS: (omit or add other tabs as required)
A - Tactical Study of Terrain
B - Beach Studies
C - Climatology Study
D - Airfield Studies
E - Helicopter Landing Zone and Drop Zone Studies
F - Port Studies
G - Lines of Communications Study
H - Order of Battle Study

SAMPLE FORMAT OF AN INTELLIGENCE ESTIMATE IN SUPPORT OF MILITARY OPERATIONS OTHER THAN WAR

CLASSIFICATION

Copy no.__of__copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time of issue
Message reference number

INTELLIGENCE ESTIMATE (NUMBER) (U)

(U) REFERENCES
- **(a) Maps and charts**
- **(b) Other pertinent intelligence documents and online data bases**

Intelligence and Information Cutoff Time Used for this Estimate: (Provide date-time group)

1. (U) Mission. (The command's restated mission as developed during the mission analysis phase of the planning process.)

2. (U) Characteristics of the Area of Operations. (Discuss characteristics of the host nation [HN], the area, and their probable effects upon the threat, the mission force, and the host government.)

a. (U) Geography

(1) (U) Strategic Location

(a) (U) Neighboring Countries and Boundaries

(b) (U) Natural Defenses, Including Frontiers

(c) (U) Points of Entry and Strategic Routes

(2) (U) Size and Dimensions

(3) (U) Relief

(4) (U) Beach Data

(5) (U) Hydrography

(a) (U) Coastal

CLASSIFICATION

(b) (U) Lakes

(c) (U) Rivers

(6) (U) Land Use

(7) (U) Geological Basics

(8) (U) Vegetation

(9) (U) Water Sources

(10) (U) Natural Foods

(11) (U) Population Centers

(12) (U) Wildlife

b. (U) Climate and Weather

(1) (U) Type and Characteristics

(2) (U) Temperature

(3) (U) Precipitation

(4) (U) Visibility

(5) (U) Winds

(6) (U) Light Data

(7) (U) Flight Conditions

(8) (U) Seasonal Effects of Weather on Terrain and Visibility

c. (U) Demographics

(1) (U) History

(2) (U) Ethnic Composition

(3) (U) Languages

(4) (U) Social System

(5) (U) Education

Page number

CLASSIFICATION

CLASSIFICATION

(6) (U) Living Conditions

(7) (U) Cultural Customs

(8) (U) Religions

(9) (U) Taboos

(10) (U) Grievances

(11) (U) Psychology. (Behavior patterns and motivating factors.)

d. (U) Transportation

(1) (U) Airfields

(2) (U) Helicopter Landing Zones

(3) (U) Port Facilities

(4) (U) Roads

(5) (U) Railroads

(6) (U) Inland Waterways

e. (U) Civilian Telecommunications and Media

(1) (U) International

(2) (U) Domestic

(3) (U) Mass Communications Types, Capabilities, and Key Facilities

(a) (U) Radio

(b) (U) Television

(c) (U) Print Media

f. (U) Politics. (Address existing situation, effects on threat, HN, and military force.)

(1) (U) National Government

(a) (U) Structure

CLASSIFICATION

(b) (U) Regional and/or International Role

(c) (U) Degree of Popular Support

(2) (U) Political Parties. (Both sanctioned and unsanctioned.)

(3) (U) Foreign Dependence or Alliances

(4) (U) Controls and Restrictions

(5) (U) Legal System. (Civil and religious.)

(6) (U) Grievances

g. (U) Economics. (Address existing situation, effects on threat, HN, and mission force.)

(1) (U) Current Value of Currency and Wage Scales

(2) (U) Financial Structure to Include National and International

(3) (U) Foreign Dependence

(a) (U) Assistance Programs

(b) (U) Foreign-Owned Businesses and Enterprises in Country

(c) (U) Trade Agreements

(4) (U) Agriculture and Domestic Food Supply

(5) (U) Natural Resources and Degree of Self-Sufficiency

(6) (U) Industry

(a) (U) Types

(b) (U) Production Levels

(c) (U) Consumer Demands

(d) (U) Unions

(7) (U) Black Market and Illicit Trades. (Drugs, weapons, etc.)

(8) (U) Technology

(a) (U) Capabilities

CLASSIFICATION

(b) (U) Expertise

h. (U) Health and Medical

(1) (U) Food Supply

(2) (U) Water Supply

(3) (U) Diseases and Other Medical Problems

(4) (U) Plant and Animal Hazards

(5) (U) Sanitation

(6) (U) Medical Facilities

3. (U) Threats. (For each category of threat, except medical/environmental and natural disasters, discuss organization and leadership, to include composition; strength and dispositions; recent and present significant activities, strengths and weaknesses; and relationships with other threat categories.)

a. (U) Conventional

b. (U) Insurgent

c. (U) Clans, Tribes, or Factions

d. (U) Terrorist

e. (U) Drug Producers or Traffickers

f. (U) Criminal Organizations

g. (U) Third-Party Nation and External

h. (U) Civil Unrest

i. (U) Medical and Environmental

j. (U) Natural Disasters

4. (U) Capabilities and Analysis. (List current threat capabilities and discuss in regard to probability of adoption.)

a. (U) Enumeration. (Includes what, where, when, and how, for each category of threat.)

CLASSIFICATION

(1) (U) Basic Capabilities

(a) (U) Conventional

(b) (U) Insurgent

(c) (U) Clans, Tribes, or Factions

(d) (U) Terrorist

(e) (U) Drug Producers or Traffickers

(f) (U) Criminal Organizations

(g) (U) Third-Party Nation and External

(h) (U) Civil Unrest

(i) (U) Medical and Environmental

(j) (U) Natural Disasters

(2) (U) Supporting Capabilities. (Includes intelligence, security, recruitment, organization, training, finance, and logistics.)

(a) (U) Conventional

(b) (U) Insurgent

(c) (U) Clans, Tribes, or Factions

(d) (U) Terrorist

(e) (U) Drug Producers or Traffickers

(f) (U) Criminal Organizations

(g) (U) Third-Party Nation and External

(h) (U) Civil Unrest

(i) (U) Medical and Environmental

(j) (U) Natural Disasters

b. (U) Analysis and Discussion. (Includes evidence supporting or rejecting the adoption of each capability.)

Page number

CLASSIFICATION

CLASSIFICATION

5. (U) HN Security

a. (U) Situation. (For each subparagraph, describe organization and leadership; strength and disposition; recent and present significant activities; and strengths and weaknesses.)

(1) (U) Public Order or Internal Security Forces

(2) (U) Armed Forces

(3) (U) External Support Forces and Dependency. (Regional peacekeeping, foreign forces, mercenaries, etc.)

b. (U) Capabilities. (What, where, when, how for basic capabilities and supporting capabilities.)

(1) (U) Public Order or Internal Security Forces

(2) (U) Armed Forces

(3) (U) External Support Forces and Dependency

c. (U) Analysis and Discussion

6. (U) Friendly and Neutral Third-Party

a. (U) Situation. (For each subparagraph, as defined in paragraph 5.a.)

(1) (U) Embassies and Consulates

(2) (U) Military

(3) (U) Business Interests

(4) (U) Nongovernmental Organizations (NGO) and/or Private Voluntary Organizations (PVO)

b. (U) Capabilities. (As defined in paragraph 5.b.)

(1) (U) Embassies and Consulates

(2) (U) Military

(3) (U) Business Interests

CLASSIFICATION

(4) (U) NGO/PVO

c. (U) Analysis and Discussion

7. (U) Conclusions and Vulnerabilities

a. (U) Effects of the Operational Environment. (State total effect of the area of operations upon courses of action.)

b. (U) Probable Threat Courses of Action. (Listed in order of relative probability of adoption.)

c. (U) Threat Vulnerabilities. (List exploitable threat vulnerabilities.)

/s/ _____
_____

TABS: (as necessary)

APPENDIX B. WEATHER CRITICAL VALUES

Establishing weather critical values is essential to weather effects analysis on threat and friendly operations. Critical values provide the parameters for assessing the exact impact of particular weather conditions. Critical values can be established for personnel, specific types of equipment, and types of military operations and tailored to the echelon of command, the composition of the force, and the likely operations the force will be expected to conduct. For example, a MEF may be concerned with general categories such as amphibious operations, fixed-wing aviation operations, and visual reconnaissance operations. A battalion may be concerned with foot mobility, line-of-sight restrictions, and effects on indirect fire support, while an unmanned aerial vehicle unit might be more concerned with visibility, cloud cover, precipitation, and temperatures aloft. Each level of command should focus on the unit mission-essential functions and specific equipment categories.

For each category or function, only weather elements that may have an impact are listed. For example, troops operating in a desert environment (depending on the desert and time of year) are generally not affected by snowfall. Similarly, windchill is not a critical factor when assessing fixed-wing aviation operations, but windchill may affect ground crews.

For each weather element selected, critical values are established that define impact levels. In table B-1, the levels of impact are defined as favorable, marginal, and unfavorable or as unrestricted, restricted, and severely restricted. An effective technique is to assign each level a color-code, such as green, yellow, or red, that can be transferred easily to a graphic weather effects matrix.

The companion weather effects matrix lists the same functions. If a weather element falls within the unfavorable or severely restricted range, the weather effects matrix is color-coded red for that function during the period of time the unfavorable element is forecast to occur. Weather elements that result in a marginal or unfavorable assessment are noted on the weather effects matrix (see chapter 6, figure 6-3).

The MEF command element intelligence section personnel, assisted by the G-2 section's staff weather officer, the intelligence support coordinator, and intelligence battalion personnel, usually compile the weather critical values chart. The commander, operations staff, and friendly force's functional elements define selected functions, weather elements, and critical values. Within a MAGTF, for example, the air officer and aviation combat element should establish weather elements that may impact aviation operations and platforms and define the values that constitute impact levels. Within an infantry battalion, the artillery liaison officer is the best source for effects on supporting fires and artillery delivered munitions.

Regardless of who compiles the list, the commander defines weather intelligence elements that are critical to decisionmaking. The identified weather elements and their established critical values are tracked closely and serve as the basis for weather effects graphics and updates. Like other intelligence requirements, the weather elements and their critical values must be reevaluated as the mission or season changes.

Unit intelligence section personnel develop mission, type unit, and equipment-focused critical values lists during peacetime operations, to include those equipment types and units which will normally be attached or in direct support during operations. Upon receipt of an alert or execute order, these critical values lists can then be refined and tailored to the forces, mission,

and environment assigned. See MCWP 3-35.7, *MAGTF Meteorological and Oceanographic Support,* and FM 34-81-1, *Battlefield Weather Effects*, for additional doctrine and tactics, techniques, and procedures guidance.

Weather critical values are established for threat as well as friendly forces. Due to differences in weapons and personnel characteristics, the same weather may have differing effects on the threat. For example, threat tanks without thermal sights will be severely restricted during periods of reduced visibility, while friendly tanks may be only marginally affected. Comparing the varying effects of weather on friendly and threat forces helps to identify advantages and vulnerabilities that may be exploited by either side.

Table B-1. Weather Critical Values Chart.

Function	Weather Element	Favorable (Unrestricted)	Marginal (Restricted)	Unfavorable (Severely Restricted)
Maneuver: Mobility (track vehicles, day)	visibility rainfall snow depth	> 1.5 km < 0.1 in/hr < 12 in	0.8 to 1.5 km > 0.5 in/hr > 12 to 20 in	< 0.8 km > 0.5 in/hr > 20 in
Maneuver: Mobility (track vehicles, night)	visibility rainfall snow depth	> 0.2 km < 0.1 in/hr < 12 in	0.1 to 0.2 km 0.1 to 0.5 in/hr 12 to 20 in	<0.1 km > 0.5 in/hr > 20 in
Maneuver: Mobility (dismounted infantry)	visibility rainfall snow depth temperature windchill	> 0.3 km < 0.1 in/hr < 3 in < 89.6 °F/32 °C > 32 °F/0 °C	0.1 to 0.3 km 0.1 to 0.5 in/hr 3 to 6 in > 89.6 °F/32 °C 32° F/0 °C to -22° F/-30° C	< 0.1 km > 0.5 in/hr > 6 in ---------- < -22 °F/-30 °C
Fire Support (155mm)	visibility ceiling surface wind snow depth	> 5.0 km > 800 ft < 35 knots < 4.0 in	1.5 to 5.0 km 500 to 800 ft 35 to 50 knots 4.0 to 6.0 in	< 1.5 km < 500 ft > 50 knots > 6 in
Fire Support (close air support)	visibility ceiling	> 8.0 km > 3000 ft	5.0 to 8.0 km 500 to 3000 ft	< 5.0 km < 500 ft
Aviation (rotary wing)	visibility ceiling surface wind precipitation	> 1.5 km > 500 ft < 20 knots none	0.4 to 1.5 km 300 to 500 ft 20 to 30 knots light	< 0.4 km < 300 ft > 30 knots freezing rain or hail
Aviation (air defense)	visibility ceiling rainfall	> 5.0 km > 5000 ft < 0.5 in/hr	3.0 to 5.0 km 3000 to 5000 ft 0.5 to 1.0 in/hr	< 3.0 km < 3000 ft > 1.0 in/hr

°C=degree Celsius °F=degree Fahrenheit ft=feet in/hr=inches per hour km=kilometer

APPENDIX C. TACTICAL INDICATORS

Indicators are any positive or negative evidence of threat activity or any characteristic of the operations area that points toward threat capabilities, vulnerabilities, or intentions. Each indicator is integrated with other factors, indicators, information, and intelligence before patterns are detected and threat intentions are established. Intelligence analysts develop indicators to—

- Assist in discerning answers to a commander's priority intelligence requirements and intelligence requirements.
- Correlate particular events or activities with probable threat courses of action.
- Determine what events or activities must occur for a threat to follow a particular course of action (COA).

As named areas of interest and the event template are developed during intelligence preparation of the battlespace (IPB), analysts develop corresponding indicators which, when detected, will assist in rapidly identifying the particular COA the threat may adopt. While some indicators may apply to most or all of the possible threat courses of action, other indicators may be unique to a particular COA. Well-developed indicator lists also aid in detecting threat deception operations. By comparing indicators, intelligence, and operations reporting, the analyst arrives at an accurate picture of the battlespace and intelligence estimates.

Indicators may be present for more than one COA in the same threat force. For example, a threat division forced to withdraw (and providing indicators accordingly) may employ a subordinate unit (brigade, regiment, or battalion) in a delaying action to cover the withdrawal. Units in contact with the delaying force may characterize the indicators as delaying in nature, but the threat force overall is withdrawing. Indicators from all sources must be analyzed to assess the threat's true intentions.

The tables on the following pages provide some intelligence indicators commonly associated with operations. These lists are intended to provide a basis from which intelligence personnel can develop indicators specific to the threat and environment they are faced with. No one indicator can stand alone; indicators must be examined within the context of the doctrine, tactics, and structure of the specific threat force.

OFFENSIVE INDICATORS

Activity	Explanation
Massing of maneuver elements, armor, artillery, and logistical support.	May strengthen the main effort by weakening areas of secondary importance.
Deployment of combat elements on a relatively narrow frontage (not forced by terrain).	May provide maximum combat power at the point of attack by reducing frontages.
Massing of indirect fire support assets.	May indicate initiation of a main attack.
Extensive artillery preparation of up to 50 minutes in duration or longer.	Indicates preparation preceding an attack.
Dispersal of tanks and self-propelled or towed artillery to forward units.	Can indicate formation of combined arms assault formations with tanks accompanying the leading maneuver elements and artillery following in bounds.
Surface-to-surface missile units located forward.	Provides depth to threat offensive operations; places friendly support and rear areas in range. May also indicate, when employed alone, harassing or special weapons delivery.
Antiaircraft artillery and mobile surface-to-air missiles located well forward with maneuver elements.	Provides increased protection to massed forces prior to attack; extends air defense umbrella forward as units advance.
Demonstrations and feints.	May precede an attack; may deceive actual point of attack.
Establishment and strengthening of counter-reconnaissance screen.	Covers assembly and preparation of forces for attack.
Concentration of mass toward one or both flanks within the forward area.	May indicate intent for single or double envelopment, particularly if massing units are armor-heavy.
Increased patrolling (ground reconnaissance).	May indicate efforts to gather detailed information regarding friendly dispositions prior to attack.
Command posts located well forward; mobile command posts identified.	Enhances command and control during offensive operations.
Movement of noncombatants out of the combat zone.	Removes noncombatants, which hinder rapid forward movement of follow-on forces.
Extensive conduct of drills and rehearsals in rear areas.	Often indicates major attacks, particularly against fortified positions or strongly defended natural or man-made barriers, which require rehearsal of specialized tactics and skills.
Increased activity in supply, maintenance, and motor transport areas.	May indicate movement of additional forces to the front to sustain major attack.
Increased aerial reconnaissance (including unmanned aerial vehicles).	Refines threat's intelligence picture prior to operations.
Establishment of forward arming and refueling points, auxiliary airfields, or activation of inactive airfields.	Increases sortie rate and turnaround time by forward basing aircraft and aviation sustainment.
Clearing lanes through own obstacles.	Facilitates forward movement and grouping of assault units, particularly at night, usually immediately precedes an attack.
Reconnaissance, marking, and destruction of opponent's obstacles.	Facilitates movement of assault echelons through opposing obstacles.
Gap-crossing equipment (e.g., swimming vehicles, bridging, ferries, boats) located in forward areas (provided there is a water or large gap obstacle).	Maintains tempo of the assault echelons when faced with significant gap obstacles, normally concentrated with main effort.
Staging of airborne, air assault, or special forces with modes of transportation/insertion.	Such elements are used to provide depth to the assault and target friendly centers of gravity.
Increased signals traffic or radio silence.	May indicate intent to conduct offensive operations. (Increased traffic may be an attempt to deceive. Radio silence denies information derived from opponent's signals intelligence.
Signals intelligence and electronic warfare assets located forward.	Provides enhanced electronic attack and electronic warfare support for assault forces.

DEFENSIVE INDICATORS

Activity	Explanation
Preparation of battalion and company defensive areas consisting of company and platoon strong points.	Indicates intent for holding terrain with defense in depth, normally supported by armored counterattack forces.
Extensive preparation of field fortifications, obstacles, and minefields.	Indicates strong positional defense.
Attachment of additional antitank assets to frontline defensive positions.	Indicates intent to contest friendly armor in forward positions, and attempts to attrite and channel friendly armor into engagement areas for armor counterattack forces.
Formation of antitank strong points in depth along avenues of approach.	May allow penetration of friendly armor into rear engagement areas.
Preparation of alternate artillery positions.	Increases survivability of artillery in the defense.
Concentration of armor units in rear area assembly areas.	Indicates holding armor units in reserve for possible counterattack or counteroffensive.
Presence of concentrated antitank reserves.	Provides quick reaction capability against armor penetrations.
Displacement of logistics and medical units towards the rear.	Facilitates maneuver defense and counterattack.
Prestocking of ammunition, supplies, and engineer or pioneer equipment in forward positions.	Reduces the burden on logistics during the battle, reduces vulnerability of interdiction of supplies, and ensures strong points can survive for reasonable periods if bypassed or cut off.
Increased depth from the forward line of troops of artillery and surface-to-surface missile units.	Allows continued employment of artillery during maneuver defense without significant rearward displacement.
Increased use of land line communications.	Implies intent to remain in position because landlines are less vulnerable to electronic warfare.
Presence of dummy positions, command posts, and weapons.	Complicates friendly targeting and analysis of actual threat locations and strengths.
Air defense more concentrated in rear areas.	Indicates location of numerous high-value targets (e.g., armor, logistics, artillery, command posts) that dictates strong air defenses in rear areas.

DELAYING INDICATORS

Activity	Explanation
Withdrawal from defensive position(s) before becoming heavily engaged.	Indicates units' delaying actions to avoid decisive engagements.
Numerous local counterattacks with limited objectives; counterattacks broken off before position is restored.	Assists in disengaging units in contact, rather than restoring positions.
Units leapfrogging to new defensive positions.	Indicates units engaging then conducting local withdrawals to new positions while another force takes up the engagement
Maximum firepower located forward; firing initiated at long ranges.	Intends to inflict casualties, slow advance, and provide sufficient combat power to avoid decisive engagement.
Extremely large unit frontages as compared to normal defense.	Indicates delaying actions to economize force, allowing larger formations to withdraw.
Chemical or biological agent weapons in forward areas.	Causes significant delays to the advancing force when employed as barriers or in minefields.
Identification of dummy positions and minefields.	Causes delays by forcing the advancing force to determine whether minefields are active or inert.

WITHDRAWAL INDICATORS

Indications of threat intent to withdraw are often the same as those for delaying actions, with the addition of the following indicators.

Activity	Explanation
Systematic destruction of bridges, communications facilities, and other assets.	Denies the advancing force the use of infrastructure and installations in withdrawal areas.
Establishment of a covering force or rear guard.	Covers the withdrawal of the main body; usually consists of a sub-element of the main force; and usually engages only the rear guard element.
Increased rearward movement noted at night, particularly during inclement weather.	Attempts to withdraw units under the concealment of darkness and weather.
Minimal presence of logistic and medical units. Destruction of dumps and depots.	Indicates withdrawal of nonessential logistic and medical elements and the inability to move depots and dumps.
Establishing and marking withdrawal routes and traffic control points.	Facilitates the rapid movement of forces rearward.
Preparation of new defensive positions beyond supporting range of present positions.	Indicates attempt to establish new positions along suitable terrain prior to the arrival of deliberately withdrawn forces.
Increased engineer activity and stockpiling of explosives in the threat rear area near bridges, tunnels, built-up areas, etc.	Facilitates maintenance of lines of communications for own forces; indicates demolition of infrastructure in front of opposing force.
Rearward movement of long-range artillery.	Positions long-range artillery before withdrawal takes place.
Activation of command posts well removed (beyond doctrinal norms) from the present battle area.	Creates command and control nodes in the new position or assembly area to command and control arriving forces.

MILITARY OPERATIONS OTHER THAN WAR INDICATORS

Given the wide range of military operations other than war (MOOTW), the possible indicators of various activities can be enormous. However, most MOOTW evolutions still involve the requirement to identify risks to friendly forces. By their nature, MOOTW are generally concerned with indigenous populations, regardless of the nature of the mission. The following indicators focus on those indicators associated with possible threats emerging from indigenous populations. These lists provide the analyst with a point of departure for developing case specific indicators.

THREAT POPULATION INDICATORS

General Activities
Identification of agitators, insurgents, militias or criminal organizations, their supporters, and sympathizers who suddenly appear in, or move out of, an area.
New faces in a rural community.
Unusual gatherings among the population.
Disruption of normal social patterns.
Mass urban rural migration or vice versa.
Massing of combatants of competing power groups.
Increase in the size of embassy or consulate staffs from a country or countries which support indigenous disaffected groups, particularly those hostile to the United States and/or the current intervention.
Increase in neighboring countries of staff and activities at embassies or consulates of countries associated with supporting indigenous disaffected groups.
Increased travel by suspected subversives or leaders of competing power bases to countries hostile to the United States or opposed to the current intervention.
Influx of opposition resident and expatriate leaders into the operations area.
Reports of opposition or disaffected indigenous population receiving military training in foreign countries.
Increase of visitors (e.g., tourists, technicians, businessmen, religious leaders, officials) from groups or countries hostile to the United States or opposed to the current intervention.
Close connections between diplomatic personnel of hostile countries and local opposition groups.
Communications between opposition groups and external supporters.
Increase of disaffected youth gatherings.
Establishment of organizations of unexplained origin and with unclear or nebulous aims.
Establishment of a new organization to replace an existing organizational structure with identical aims.
Appearance of many new members in existing organizations such as labor unions.
Infiltration of student organizations by known agitators.
Appearance of new organizations stressing grievances or interests of repressed or minority groups.
Reports of large donations to new or revamped organizations.
Reports of payment to locals for engaging in subversive of hostile activities.
Reports of the formation of opposition paramilitary or militia organizations.
Reports of lists of targets for planned opposition attacks.
Appearance of “professional” agitators in gatherings or demonstrations that result in violence.
Evidence of paid and armed demonstrators’ participation in riots.
Significant increase in thefts, armed robberies, and violent crime in rural areas; increase in bank robberies in urban areas.

Opposition-Directed Activities
Refusal of population to pay or unusual difficulty to collect rent, taxes, or loan payments.
Trends of demonstrated hostility toward government forces and/or mission force.
Unexplained population disappearance from or avoidance of certain areas.
Unexplained disappearance or dislocation of young people.
Reported incidents of attempted recruitment to join new movements or underground organizations.
Criminals and disaffected youth who appear to be acting with and for the opposition.
Reports of extortion and other coercion by opposition elements to obtain financial support from the population.
Use of fear tactics to coerce, control, or influence the local population.
Reports of host nation government and/or mission force facilities and personnel surveillance.
Activities Directed Against the Government/Mission Force
Failure of police and informer nets to report accurate information, which may indicate sources are actively supporting opposition elements or are intimidated.
Decreasing success of government law enforcement or military infiltration of opposition or disaffected organizations.
Assassination or disappearance of government sources.
Reports of attempts to bribe or blackmail government officials, law enforcement employees, or mission personnel.
Reports of attempts to obtain classified information from government officials, government offices, or mission personnel.
Classified information leaked to the media.
Sudden affluence of certain government and law enforcement personnel.
Recurring failure of government or mission force raids on suspected opposition organizations or illegal activities apparently due to forewarning.
Increased hostile or illegal activity against the government, its law enforcement and military organizations, foreigners, minority groups, and/or competing political, ethnic, linguistic, or religious groups.
Demonstrations against government forces, minority groups, or foreigners designed to instigate violent confrontations with government or mission forces.
Increased antigovernment or mission force rhetoric in local media.
Occurrence of strikes in critical areas intended to cast doubt on the government's ability to maintain order and provide for the people.
Unexplained loss, destruction, or forgery of government identification cards and passports.
Recurring unexplained disruption of public utilities.
Reports of terrorist acts or extortion attempts against local government leaders and businessmen.
Murder or kidnapping of government, military, and law enforcement officials or mission force personnel.
Closing of schools.

PROPAGANDA INDICATORS

General Propaganda Activities
Dissident propaganda from unidentified sources.
Increase in the number of entertainers with a political message.
Increase of political themes in religious services.
Increase in appeals directed at intensifying general ethnic or religious unrest in countries where ethnic or religious competition exists.
Increase of agitation on issues for which there is no identified movement or organization.
Renewed activity by dissident or opposition organizations thought to be defunct or dormant.
Circulation of petitions advocating opposition or dissident demands.
Appearance of opposition slogans and pronouncements by word-of-mouth, graffiti, posters, leaflets, etc.
Propaganda linking local ethnic groups with those in neighboring countries or regions.
Clandestine radio broadcasts intended to appeal to those with special grievances or to underprivileged ethnic groups.
Use of bullhorns, truck-mounted loudspeakers, and other public address equipment in "spontaneous" demonstrations.
Presence of nonmedia photographers among demonstrators.
Rallies to honor "martyred" opposition personnel. Mass demonstrations honoring local dissident heroes or dates significant to the opposition.
Nationwide strikes called to demonstrate the strength of the opposition movement(s).
Propaganda Activities Directed Against the Established Government
Attempts to discredit or ridicule national or public officials.
Attempts to discredit the judicial and law enforcement system.
Characterization of government leaders as puppets and tools of foreign intervention forces.
Agitation against government projects and plans.
Radio propaganda from foreign countries that is aimed at the target country's population and accuses the target country's government of failure to meet the people's needs.
Propaganda Activities Directed Against the Mission Force and Host Nation Military and Law Enforcement
Spreading accusations that the host nation military and police are corrupt and out of touch with the people.
Spreading accusations that mission force personnel will introduce customs or attitudes that are in opposition to local cultural or religious beliefs.
Character assassinations of mission, military, and law enforcement officials.
Demands to remove strong anti-opposition or anticrime military and law enforcement leaders from office.
Calls for the population to cease cooperating with the mission force and/or host nation military and law enforcement.
Deliberate incidents to provoke mission, military, or police reprisals during demonstrations or strikes.
Widespread hostile media coverage of even minor criminal violations or incidents involving mission force personnel.
Accusations of brutality or ineffectiveness or claims that mission or government forces initiated violence following confrontations.
Publication of photographs portraying repressive and violent acts by mission force or government forces.
Refusal of businessmen and shop owners to conduct business with mission force personnel.

Propaganda Activities Directed Against the Education System
Appearance of questionable doctrine and teachings in the educational system.
Creation of ethnic, tribal, religious, or other interest group schools outside the government educational system, which propagate opposition themes and teachings.
Charges that the educational system is only training youth to do the government's bidding.
Student unrest manifested by new organizations, proclamations, demonstrations, and strikes against authority.

COMMODITIES INDICATORS

Food-Related Activities
Diversion of crops or meat from markets.
Unexplained shortages of food supplies when there are no reports of natural causes.
Increased reports of foodstuffs pilfering.
Sudden increase in food prices, possibly indicating an opposition-levied tax.
Unwillingness of farmers to transport food to population centers, indicating a fear of traveling highways.
Spot shortages of foodstuffs in regions or neighborhoods associated with a minority group or weaker competing interest group, while food supplies are generally plentiful in other areas. Conversely, sudden local shortages of foodstuffs in rural areas may indicate the existence of an armed opposition group operating in that region.
Sudden increase of meat in markets, possibly indicating slaughtered livestock because of a lack of fodder to sustain them.
Appearance of emergency relief supplies for sale in black markets, possibly indicating diversion from starving population.
Appearance of relief supplies for sale in normal markets in a country or region recently suffering from large-scale hunger, which may indicate the severity of the food crisis is diminishing.
Arms and Ammunition-Related Activities
Increased loss or theft of weapons from military and police forces.
Discovery of arms, ammunition, and explosives being clandestinely manufactured, transported, or cached.
Attacks on patrols resulting in the loss of weapons and ammunition.
Increased purchase of surplus military goods.
Sudden increase in prices for arms and ammunition on the open market.
Reports of large arms shipments destined for neighboring countries, but not intended for that government.
Reports of known arms traffickers establishing contacts with opposition elements.
Increase in armed robberies.
Reports of thefts or sudden shortages of chemicals, which could be used in the clandestine manufacture of explosives.
Reports of large open-market purchases of explosives-related chemicals without an identifiable industrial user.
Appearance of manufactured or smuggled arms from noncontiguous foreign countries.
Clothing-Related Activities
Unusual, systematic purchase or theft of clothing materials, which could be used for the manufacture of uniforms or footwear.
Unusual scarcity of clothing or material used in the manufacture of clothing or footwear.
Distribution of clothing to underprivileged or minority classes by organizations of recent or suspect origin.
Discovery of caches of uniforms and footwear or the materials which could be used to manufacture uniforms and footwear.
Increase of males in the streets wearing military style clothing or distinctive markings.

Medicine-Related Activities
Large-scale purchasing or theft of drugs and medicines or the herbs used to manufacture local remedies.
Scarcity of drugs and medical supplies on the open or black markets.
Diversion of medical aid donations.
Discovery of caches of medical supplies.
Communications-Related Activities
Increase in the purchase and use of radios.
Discovery of caches of communications equipment.
Unusual increase in amateur radio or cellular telephone communications traffic.

ENVIRONMENT-RELATED INDICATORS

Rural Activities
Evidence of increased foot traffic in the area.
Increased travel within and into remote or isolated areas.
Unexplained trails and cold campsites.
Establishment of new, unexplained agricultural areas, or recently cleared fields.
Unusual smoke, possibly indicating the presence of a campsite or a form of communication.
Concentration of dead foliage in an area, possibly indicating use of camouflage.
Presence of foot traps, spikes, boobytraps, or improvised mines along routes and trails.
Urban Activities
Apartments, houses, or buildings being rented, but not lived in as homes.
Slogans written on walls, bridges, and streets.
Defacement of government and mission force information signs.
Sabotage of electrical power network; pollution of urban area's water supply.
Terrorist acts against physical targets such as bridges, dams, airfields, or buildings.
Change of residence of suspected agitators or opposition leaders.
Discovery of message dead-drops.
Increased smuggling of currency, gold, gems, narcotics, medical supplies, and arms into urban centers.
Appearance of abnormal amounts of counterfeit currency.
Increase in bank robberies.
Work stoppages or slowdowns in essential industries.
Marked decline in product quality in essential industries.
Marked increase in equipment failures in essential industries.
Unexplained explosions in essential utilities and industries.
Establishment of roadblocks or barricades around neighborhoods associated with opposition elements.
Attempts to disrupt public transport through sabotage.
Malicious damage to industrial products or factory machinery.

APPENDIX D. BATTLE DAMAGE ASSESSMENT REPORT FORMAT

The periodic summary battle damage assessment (BDA) report on page D-2 is an example format that may be used by MEF major subordinate command intelligence personnel to provide consolidated Phase I BDA, physical damage assessment, to the intelligence battalion's production and analysis cell. The report is a compilation of BDA reporting from subordinate elements as well as BDA obtained at the MSC level during the designated time period. The theater intelligence tactics, techniques, and procedures or the joint task force commander establishes BDA reporting formats for the joint task force, theater, and national level.

Normally, the aviation combat element is responsible for providing BDA on any air tasking order-related missions, while the ground combat element focuses on their subordinate elements' engagement results, to include observed close air support effects.

The target intelligence and BDA team, production and analysis company, intelligence battalion, is responsible for—

- **Consolidating, deconflicting, and refining BDA reports.**
- **Introducing additional information and intelligence obtained from other sources.**
- **Preparing the Phase I BDA, physical damage assessment, for the MEF commander.**
- **Preparing Phase II BDA, functional damage assessment, based on the consolidated reporting from subordinate, higher, and adjacent commands.**
- **Adjusting the MEF order of battle data bases to reflect combat losses.**
- **Developing the combat strength assessment for each unit.**

BATTLE DAMAGE ASSESSMENT REPORT FORMAT EXAMPLE

SUBJECT: 6 HR BDA REPORT (SUBMIT TO INTELLIGENCE BATTALION'S TARGET INTELLIGENCE/ BDA TEAM, P&A CELL, AT SPECIFIED TIMES.)

REPORTING UNIT:

REPORTING PERIOD: (FROM/TO)

ENEMY UNIT OR FACILITY #1: (DOWN TO BDE NAME FOR MANEUVER, BN FOR FIRE SUPPORT, OR AS DIRECTED IN UNIT SOP OR OPORD. REPEAT THIS SECTION FOR EACH UNIT OR FACILITY.)

UIC OR BE#: DHGKNXXXXX

DAMAGED/DESTROYED:

	LOC	TYPE	#DEST	#DMGD/EXTENT
1. ARMOR:				
2. FIRE SUPPORT:				
3. TRUCKS:				
4. AIR DEFENSE:				
5. C2 SYSTEMS:				
6. MOB/CNTRMOB: (ENGINEERS ASSETS, BRIDGES, LINES OF COMMUNICATIONS, MINES, ETC.)				

7. CSS:

	LOC	WIA	KIA
8. PERSONNEL:			

REMARKS:

IF UNIT NAME IS UNKNOWN, INCLUDE TIME OF REPORT (TOR), UNDER HEADING "ENEMY UNIT: UNKNOWN". DO NOT SUMMARIZE; LIST EACH REPORT. FOR EXAMPLE:

ENEMY UNIT: UNKNOWN

UIC: UNKNOWN

DAMAGED/DESTROYED: LIST ALL UNKNOWN UNIT BDA REPORTS BY TIME

	TOR*	LOC	TYPE	#DEST	#DMGD/EXTENT
1. ARMOR:					
2. FIRE SUPPORT:					
3. TRUCKS:					
4. AIR DEFENSE:					
5. C2 SYSTEMS:					
6. MOB/CNTRMOB: (ENGINEERS ASSETS, BRIDGES, LINES OF COMMUNICATIONS, MINES, ETC.)					

7. CSS:

	TOR*	LOC	WIA	KIA	EPW
8. PERSONNEL:					

REMARKS: *TOR: TIME OF REPORT. (NOTE: REMARKS ARE A MEANS OF REPORTING INFORMATION THAT DOES NOT FIT INTO THE TABLES DESCRIBED ABOVE. SPELL IT OUT IN A REMARKS SECTION, FOR EACH UNIT IF NECESSARY OR IF YOUR ASSESSMENT GOES BEYOND NUMBER COUNTS.)

APPENDIX E. MAGTF INTELLIGENCE PRODUCTION PLAN FORMAT

Tab B (Intelligence Production Plan) to Appendix 16 (Intelligence Operations Plan) to Annex B (Intelligence) should explain how intelligence production elements under the command or supporting the MAGTF would be used to support this plan. Additionally, it provides basic guidance and direction to subordinate commanders and intelligence officers for the conduct of MAGTF intelligence production operations and the support of intelligence elements and personnel identified to fulfill the intelligence requirements (IRs) in support of this plan.

CLASSIFICATION

Copy no. __ of __ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time group
Message reference number

TAB B TO APPENDIX 16 (INTELLIGENCE OPERATIONS PLAN) TO ANNEX B (INTELLIGENCE) TO OPERATION ORDER (Number) (Operation CODEWORD) (U)
INTELLIGENCE PRODUCTION PLAN (U)

(U) REFERENCES: (The annex B originator must ensure that all receiving units and executing units have cited references.)
(a) Unit standing operating procedures (SOP) for intelligence, counterintelligence, reconnaissance, and others as appropriate.
(b) Joint task force, naval task force, other components, theater and national intelligence plans, orders and tactics, techniques, and procedures; and multinational agreements pertinent to intelligence operations.
(c) Documents, products, and online intelligence data bases that provide intelligence required for planning.
(d) Appropriate Marine Corps, naval, joint, and other doctrine publications.
(e) Others as appropriate.

(U) Time Zone: Zulu

1. (U) Situation. (May refer to Appendix 11 [Intelligence Estimate] as appropriate.)

a. (U) Definition of the Area of Operations and Area of Interest. (Describe the limits of the area of operations [AO] and area of interest [AOI]. Summarize pertinent

CLASSIFICATION

weather, terrain, and other area characteristics and conditions that may influence MAGTF production operations.)

b. (U) Enemy. (Refer to annex B and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and order of battle pertinent to intelligence production operations.)

c. (U) Assigned MAGTF Organic and Supporting Production Assets. (Identify organic and supporting forces available to perform intelligence production and related functions.)

d. (U) Facts and Assumptions. (State facts and assumptions derived during the mission analysis step of the Marine Corps Planning Process.)

e. (U) MAGTF Intelligence Production Considerations. (List key production and intelligence or other considerations, which impact this operation plan [OPLAN] or contingency plan [CONPLAN].)

(1) (U) Current Priority Intelligence Requirements (PIRs), Unit Concept of Operations, Unit Main Effort's PIRs, and Other Commander's Guidance

(2) (U) Availability of Intelligence

(3) (U) Intelligence Production Support to and from Joint Task Force (JTF) and Other Component Headquarters

(4) (U) Subordinate Units' Production Capabilities and Needs. (Include necessary establishment and manning of forward production elements.)

2. (U) Mission. (State concisely the MAGTF intelligence production mission as it relates to the command's planned operation.)

3. (U) Execution

a. (U) Concept of Operations. (Reference the unit's intelligence SOP and the basic Appendix 16 to Annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall concept of operations as they relate to production operations. Outline the purpose and concept of MAGTF production operations and specified priorities. Summarize the means and agencies to be employed in planning and directing, collection, processing and exploiting, analyzing and producing, disseminating, and using intelligence during execution of the operation order [OPORD]. Address the integration of JTF, other components, theater, national, and allied forces' production operations.)

CLASSIFICATION

b. (U) Tasks for Production and Related Units and Organizations, Subordinate Units, and Task Force Commanders or Officers in Charge (OICs)

(1) (U) Orders to Subordinate, Attached, and Supporting Units. (Use separate numbered subparagraphs to list detailed instructions for each unit conducting production operations, including the originating headquarters, subordinate commands, and separate intelligence support units with critical support to production roles. Some or all of the below units and sections may be addressed here; specific major subordinate commands [MSCs] and other intelligence producers will be tasked according to the unit SOP and mission, enemy, terrain and weather, troops and support available, and time available [METT-T].)

(a) (U) Major Subordinate Commanders

(b) (U) Commanding Officer, Intelligence Battalion

1 (U) OIC, Support Cell

2 (U) OIC, Production and Analysis (P&A) Cell

a (U) Analysis Teams

b (U) Order of Battle Teams

c (U) Target Analysis and Battle Damage Assessment Teams

d (U) Intelligence Preparation of the Battlespace Teams

e (U) Platoon Commander, Imagery Intelligence Platoon

f (U) Platoon Commander, Topographic Platoon

g (U) Staff Noncommissioned OICs, Direct Support Teams

h (U) Weather Analysis Element (if assigned)

3 (U) OIC, Surveillance and Reconnaissance Cell

4 (U) Commanding Officer, Counterintelligence (CI)/Human Intelligence (HUMINT) Company

(c) (U) Commanding Officer, Radio Battalion

(d) (U) Commanding Officer, Force Reconnaissance Company

(e) (U) Commanding Officer, Marine Unmanned Aerial Vehicle Squadron (VMU)

CLASSIFICATION

(f) (U) Commanding Officer, Marine Tactical Electronic Warfare Squadron (VMAQ)

(g) (U) Commander, Marine Corps Imagery Support Unit (if tasked to provide support to the MAGTF)

(h) (U) Others (as appropriate)

(2) (U) Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached, or supporting from which production support is requested, including other components, JTF headquarters, allied or coalition forces, as well as theater and national operational and intelligence elements.

c. (U) Coordinating Instructions. (Reference Appendix 16, and command and other pertinent forces and organizations intelligence SOPs. Detail here or in supporting enclosures, key changes to SOPs. Include or emphasize additional topics [e.g., requesting production support; intelligence production requirement [IPR] numbering and other management issues; direct liaison among subordinate commanders and production elements' leaders, staff officers, and pertinent external organizations and agencies; routine and time-sensitive reporting procedures and formats; releasability to non-U.S. military organizations; security guidance].)

4. (U) Administration and Logistics

a. (U) Logistics. Reference Annex D (Logistics). (Identify production-unique logistic requirements and concerns [e.g., unique combat service support requirements, procedures, and other guidance to support MAGTF production units and operations; or procedures for specialized technical logistic support necessary from external organizations].)

b. (U) Personnel. (Identify unique production personnel requirements and concerns [e.g., critical personnel shortages, global sourcing requirements, security clearance issues, contractor support].)

5. (U) Command and Control

a. (U) Command Relationships. Reference Annex J (Command Relationships). (Provide necessary instructions regarding MAGTF command relationships that will influence production operations.)

CLASSIFICATION

b. (U) Information Management. Reference Annex U (Information Management), Annex C (Operations), Appendix 16, and Tab C (Intelligence Dissemination Plan) to Appendix 16. (Provide any instructions necessary regarding information management [e.g., time-sensitive and routine reporting criteria, intelligence data base administration and authorities, periodic production status reporting from production elements, reports formats and changes] that will influence MAGTF production operations.

c. (U) Communications and Information Systems. Reference Appendix 16 and Annex K (Communications and Information Systems). (Provide any instructions necessary regarding communications and information systems [CIS] that will influence MAGTF production operations and its effective integration with MAGTF collection and dissemination operations.

d. (U) Intelligence Command and Control Nodes and Facilities. Reference the unit's intelligence SOP and Appendix 16. Provide necessary guidance and instructions regarding the establishment, relationships, and operations of MAGTF intelligence production nodes and facilities (e.g., P&A cell, the radio battalion operations control and analysis center, CI/HUMINT company command post).

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

ENCLOSURES:

1–Intelligence Production Matrix
2–Periodic Intelligence Production Status Report Instructions and Format

OFFICIAL:

//s//
NAME
Rank and Service
Title

INTELLIGENCE PRODUCTION MATRIX
INSTRUCTIONS AND FORMAT

The intelligence production matrix is a tool used by MAGTF intelligence officers, the intelligence support coordinator (ISC), and production leaders to effectively plan, direct, and manage intelligence production operations. Making the matrix accessible to subordinate units' intelligence officers and intelligence producers will improve overall collaborative intelligence planning and execution.

The sample below is one format for the intelligence production matrix. The unit specifies the particular format for a given operation. The complexity of the operation and other METT-T factors will determine which format is used.

PIR, IR, or IPR Number	Date Requested	Production Requirement	Event/ Operation/ Exercise	Requesting Unit/POC	Tasked Unit(s)	Tasked Unit(s) POC	Due Date or DTG	First Review Date or DTG	First Review Remarks	Second Review Date or DTG	Second Review Remarks

Third Review Date or DTG	Third Review Remarks	Status	Feedback	Estimated Man-Hours	Actual Man-Hours*	Estimated Cost*	Actual Cost*	Quality and Distribution	Distribution Follow-ups & New IRs/ IPRs	Additional Remarks
*Garrison use only										

PERIODIC INTELLIGENCE PRODUCTION STATUS REPORT INSTRUCTIONS AND FORMAT

The periodic intelligence production status report is used by designated MAGTF units with all-source or other significant intelligence production capabilities to keep commanders, intelligence officers and sections, and other staff elements apprised of the status of current and future intelligence production operations. For the effective management of unit production activities, intelligence officers or their production leaders may require that this report be used by designated production elements under their staff cognizance to report their production status.

The example report on page E-8 is only one format (refer to the unit's SOP for specific format and direction). Normally, variations of the SOP format will be established for text, voice, and record message traffic purposes. Changes for a particular operation will be clearly identified in Annex B.

The unit SOP or Annex B also establishes the timeframe covered by each report and identifies routine and nonroutine recipients. The report may be disseminated by various methods. Interim reports, when required, generally will be disseminated via either briefings or via the tactical data network (TDN). Principal dissemination methods for the production status report include—

- **Intelligence section's homepage on the MAGTF SECRET-TDN (S-TDN), with necessary sensitive compartmented information (SCI) production status posted on the SCI-TDN intelligence section homepage.**
- **Stand-alone record message.**
- **Production data bases accessible via the S-TDN or SCI-TDN (or SECRET Internet Protocol Router Network [SIPRNET] and Joint Worldwide Intelligence Communications System [JWICS] for external commands).**
- **Separate paragraph within the daily intelligence summary.**

CLASSIFICATION

Copy no. ___ of ___ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time group
Message reference number

ENCLOSURE 2 TO TAB B TO APPENDIX 16 TO ANNEX B TO OPERATION ORDER (NUMBER) (OPERATION CODEWORD) (U)
PERIODIC INTELLIGENCE PRODUCTION STATUS REPORT INSTRUCTIONS AND FORMAT (U)

Subj: MEF PERIODIC INTELLIGENCE PRODUCTION STATUS REPORT FOR THE PERIOD 180001Z–182359Z NOV 99

1. (U) Production Operations Status. (Provide essential details to ensure supported commanders, intelligence officers, and other planners are apprised of the current status of key intelligence production operations. At a minimum, PIRs and IPR priorities should be included.)

a. (U) PIR/IR MEF 01-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 01-99	intelligence estimate	III MEF CG and staff; copies to MSCs	031457Z NOV 99	2100001Z NOV 99

(1) (U) Task Production Element(s). P&A cell and assistance from radio battalion operations control and analysis center, CI/HUMINT company and Marine Corps Imagery Support Unit (MCISU) as directed by ISC.

(2) (U) Remarks. Production in support of contingency planning. Final product is the initial Appendix 11 (Intelligence Estimate) with supporting CI estimate. Product is 95 percent complete.

CLASSIFICATION

b. (U) PIR/IR MEF 002-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 002-99; Division 002-99, MAW 003-99, and FSSG 002-99 relate	OPLAN Support	III MEF G-2/3/5; copies to MSCs	031645Z NOV 99	230700Z NOV 99

(1) (U) Task Production Element(s). MEF lead P&A cell developing, in coordination with JFT joint intelligence support element (JISE) and the joint force land component commander intelligence section.

(2) (U) Remarks. Production in support of contingency planning. (Provide template locations and dispositions of estimated enemy command and control [C2] headquarters, maneuver, and logistic elements down to the brigade and regiment level, and fires elements down to battalion level, in support of the five locations specified to support MEF course of action development.) Product is currently in work. Current intelligence is available on the MEF G-2 SCI-TDN homepage. Spreadsheet will be forwarded to staff sections and MSCs upon completion.

c. (U) MEF 003-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 003-99	expeditionary support product (phase 1)	Originator, III MEF G-2/3/4/5/6; copies to Division, FSSG, MAW	062207Z NOV 99	240700Z NOV 99

(1) (U) Task Production Element(s). P&A cell; imagery intelligence platoon (IIP), topographic platoon, and MCISU assist as directed.

(2) (U) Remarks. Expeditionary support product in support of phase 1 scheme of maneuver and course of action analysis. Product is 75 percent complete. Completed helicopter landing zone study, which is posted on MEF G-2 S-TDN homepage. Targets within G-2 designated priority areas are 95 percent scanned.

CLASSIFICATION

d. (U) PIR/IR Division 005-00

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
Division 005-99	map update and reproduction	Division; copy to FSSG	080423Z NOV 99	Initial 10, 140100Z NOV 99; remainder, 270001Z NOV 99

(1) (U) Task Production Element(s). Topographic platoon lead; IIP assist as required.

(2) (U) Remarks. Production in support of division planning and C2. Integrating current geographic intelligence (GEOINT) products with current external imagery in order to update 1993 edition maps. Initial distribution requirement made; remainder 85 percent complete. Anticipate full IR satisfaction by 230001Z NOV 99.

e. (U) PIR/IR MAW 003-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MAW 003-99	CIB graphics	1st MAW G-2; Division, MEF G-5 and FFC	101457Z NOV 99	011000Z DEC 99

(1) (U) Task Production Element(s). IIP assisted by P&A cell, red team, and force fires cell (FFC) future operations personnel as required.

(2) (U) Remarks. Production to support MAW target development and planning. Produce kill boxes using controlled image base (CIB) imagery. Product will be a 5-meter CIB overview of indicated areas, including a graphic reference grid with kill boxes annotated. Product is 80 percent completed.

f. (U) PIR/IR Division 007-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
Division 007-99; FSSG 004-99	LOC study	Division G-2; III MEF G2, FSSG	120937Z NOV 99	140200Z DEC 99

CLASSIFICATION

(1) (U) Task Production Element. Topographic platoon assisted by IIP and P&A cell.

(2) (U) Remarks. Production in support of wargaming and planning. Produce a detailed lines of communications (LOC) intelligence study. Product must maintain a classification level of unclassified. The bridge portion of this product can only be completed 45 percent due to lack of data sets and imagery.

g. (U) PIR/IR MEF 010-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 010-99; Division 009-99	target area/objective studies	MEF G-3 and FFC; Division and MAW	072103Z DEC 99	100400Z DEC 99

(1) (U) Task Production Element(s). P&A cell; IIP and topographic platoon support as required.

(2) (U) Remarks. Production of imagery products and supporting all-source intelligence reports for six specified areas within the division's area of operations. Production is completed; final dissemination ongoing and will be completed by 191000Z Nov 99. Follow-up conference call between MEF G-3/G-2 (P&A cell lead), division G-3/G-2 and MAW G-3/G-2 to verify fully satisfied IR and new IRs scheduled for 191600Z Nov 99.

h. (U) PIR/IR FSSG 016-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
FSSG 016-99	elevation/slope tint	FSSG; Division	130303Z NOV 99	050600Z DEC 99

(1) (U) Task Production Element. Topographic platoon.

CLASSIFICATION

(2) (U) Remarks. Production in support of FSSG site locations assessments and rear area security planning. Produce elevation and slope tint at 1:50,000 scale for defined areas. Slope tint will be provided in place of comprehensive cross-country movement study for two areas because there is no terrain data; possible new information from yesterday's JTF imagery collection missions. Product is 80 percent complete.

i. (U) PIR/IR MEF 012-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 012-99	enemy C2 and CIS template	MEF G-5/G-3; MAW and Division	071457Z DEC 99	140100Z DEC 99

(1) (U) Task Production Element(s). Radio battalion operations control and analysis center; P&A cell, MAW G-2, and VMAQ tactical electronic reconnaissance processing and evaluation system assist as required.

(2) (U) Remarks. Production in support of MEF C2 warfare and targeting planning. Provide template locations and dispositions of estimated enemy C2 headquarters, maneuver, and logistic elements down to the brigade and regiment level, and fires elements down to battalion level, with estimated key CIS emitters in support of the five locations specified to support MEF COA development and wargaming. IR modified 071800Z DEC 99 to incorporate specified enemy radars and other noncommunications emitters to support MAW suppression of enemy air defenses planning. Product is 75 percent complete. Final product dissemination will be restricted to U.S. and designated multinational intelligence and operations elements.

2. (U) Production Problems. (Identify and describe significant production problems [e.g., anticipated delays meeting the latest times information of value for validated PIRs and higher priority IRs; CIS difficulties; releasability issues].)

CLASSIFICATION

3. (U) Production Detachments. (In initial report, identify intelligence detachments in support of MAGTF subordinate units that have a production capability. In subsequent reports, identify detachment name and annotate "NO CHANGE," if applicable, and new detachments deployed since the last status report. Other supporting information will be according to unit SOP and may include: period of support; detachment's intelligence support purpose; personnel and military occupational specialty information; anticipated near-term detachments support.)

Who	Dates/Period	Supported Unit	Purpose
Intelligence Battalion 1-99 (P&A cell)	01 Nov 00–(to be determined)	JTF J-2/ JISE	one 0202, two 0231s, and one 0241 for liaison and targeting support
Intelligence Battalion 2-99 (P&A Company, Direct Support Team #1)	10 Nov 99–(to be determined)	Division G-2	MEF main effort support
Intelligence Battalion 3-99 (P&A Company, Direct Support Team #2)	15 Nov 00–(to be determined)	FSSG G-2	rear area security support
Intelligence Battalion 4-99 (HUMINT Support Team #1)	19 Nov 99–(to be determined)	Division G-2	CI force protection support
Intelligence Battalion 5-99 (HUMINT Support Team #2)	22 Nov 99–(to be determined)	FSSG G-2	CI force protection support
Intelligence Battalion 6-99 (HUMINT Support Team #3)	22 Nov 99–(to be determined)	MAW G-2	CI force protection support
Intelligence Battalion 7-99 (Topographic Platoon, Geographic Intelligence Support Team #1)	19 Nov 99–(to be determined)	Division G-2	GEOINT support
Intelligence Battalion 8-99 (Topographic Platoon, Geographic Intelligence Support Team #2)	1 Dec 99–(to be determined)	FSSG G-2	GEOINT support
Radio Company Command Element (Signals Support Unit lead echelon element)	1 Dec 99–(to be determined)	Division G-2	Signals Intelligence support
Intelligence Battalion 9-99 (Topographic Platoon, Geographic Intelligence Support Team #3)	5 Dec 99–(to be determined)	MAW G-2	GEOINT support

CLASSIFICATION

4. (U) Miscellaneous. (Detail other information pertinent to ongoing collaborative intelligence production planning, direction, and operations. This may include items such as anticipated CIS problems, intelligence data base changes, nonscheduled cells or other intelligence briefings, critical intelligence collection and production issues, key external intelligence production items, security, and dissemination issues.)

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

OFFICIAL:
//s//
NAME
Rank and Service
Title

CLASSIFICATION

APPENDIX F. INTELLIGENCE SUMMARY FORMAT

The intelligence summary (INTSUM) provides a synopsis of the reporting unit's intelligence situation covering a specified period of time. It is used to report threat activities, changes to threat capabilities, and results of further collections, analysis, and production to higher, adjacent, and subordinate forces. The INTSUM updates the current intelligence estimate and provides a continual intelligence assessment of threat actions and estimated capabilities and courses of action.

The theater intelligence directorate (J-2) provides guidance on INTSUM reporting periods and submission deadlines. Theater tactics, techniques, and procedures (TTP) and the specific operations plan or operation order (OPORD) designate INTSUM reporting requirements for subordinate joint task forces (JTFs) or Service and functional components. Based on those requirements, MAGTF intelligence officers (G-2/S-2) establish INTSUM reporting requirements for their major subordinate commands (MSCs) or elements; at the MEF CE level, the intelligence support coordinator establishes reporting requirements.

Established deadlines allow the intelligence battalion's production and analysis cell sufficient time to incorporate subordinate INTSUMs into intelligence products. The MAGTF MSCs and elements' G-2/S-2s determine INTSUM requirements for their headquarters and subordinate elements. The MEF TTP and standing operating procedures (SOP), which reflect anticipated theaters of operations TTP, should establish standard INTSUM reporting requirements.

Although any unit can produce INTSUMs, normally they are generated by major subordinate or higher level commands. An abbreviated INTSUM format focused on significant threat actions and anticipated future actions may be more appropriate for lower tactical echelons.

Higher command levels, particularly JTFs and unified commands, usually publish a daily intelligence summary (DISUM) every 24 hours. While INTSUMs generally provide a fine-grained tactical perspective, the DISUM encompasses more aspects of a threat country's elements of national power and focuses on operational-level intelligence analysis and estimates. Generally, MAGTF command elements tasked as JTF headquarters are required to submit DISUMs to the combatant command's commander in chief. The combatant command's TTP provides for the DISUM format, which may vary from theater to theater.

Generally based on the intelligence estimate format, the INTSUM should be tailored and focused on the mission, type of unit, and information and intelligence needs of the commander. Formats for INTSUMs can be in written or graphic and text formats.

WRITTEN INTELLIGENCE SUMMARY FORMAT

The sample below provides a written INTSUM format that may be posted on a website. This format is representative of an INTSUM format used at the MAGTF or MSC level for conventional military operations. Generally, this format is modified to meet the unique needs of military operations other than war (MOOTW).

Note: Paragraphs not applicable to the reporting unit are annotated "NA" or the paragraph may be skipped (paragraph numbering should remain the same). If no significant information or intelligence is available for a particular paragraph, the notation "NSTR" (nothing significant to report) may be used. The annotation "( )" reflects classification of that information line.

CLASSIFICATION/RELEASABILTY
INTSUM #: (Sequentially numbered such, as "DD-001-97")
DTG: DDHHMM (time zone) (month) YY
INFO cutoff DTG
PERIOD: DDHHMM TO DDHHMM (month) YY

I. (U) Highlights:

A. (U) Ground: Highlights of the current ground situation, usually divided by area or sector.

B. (U) Air: Highlights of the current air situation.

II. (U) Summary of Enemy Situation: (Each category should use the commander's related priority intelligence requirements [PIRs] as the basis for the analysis and assessment. For MOOTW operations, separate paragraphs for each category of threat or significant power group may be created to supplement or replace the below categories.)

A. (U) Ground: Detailed analysis of the battlefield by area or sector with comments on projected activity in the next 12 hours.

B. (U) Air: Detailed analysis of the air and air defense situation with comments on projected activity in the next 12 hours.

C. (U) Naval: Detailed analysis of the naval situation with comments on projected activity in the next 12 hours.

D. (U) Surface-to-Surface Missile and Weapons of Mass Destruction: Detailed analysis of the surface-to-surface missile and weapons of mass destruction situation with comments on projected activity in the next 12 hours.

E. (U) Special Operations Forces: Detailed analysis of the special operations forces, force protection, and rear area security situation with comments on projected activity in the next 12 hours.

F. (U) Other: May be used for detailed analysis of paramilitary, insurgent, terrorist, or other significant threat categories not discussed elsewhere.

III. (U) MEF or MSC Assessment:

A. (U) Most Likely Course of Action:

B. (U) Most Dangerous Course of Action:

C. (U) Others: (as necessary)

IV. (U) Enemy Movement During the Reporting Period: Major enemy units (to include at least two levels below that of the reporting command) and universal transverse mercator [UTM] coordinates of the new position.

V. (U) PIRs: The commander's PIRs and current satisfaction level (i.e., partially satisfied, satisfied, not satisfied) assessment for each requirement.

VI. (U) Intelligence Plans, Missions, and Systems Status: Key intelligence collection, production, and dissemination plan updates; information on planned intelligence and reconnaissance missions; and intelligence systems status (generally only those systems that are less than fully operational). (The unit SOP or annex B to the OPORD prescribes the period covered by this paragraph.)

GRAPHIC INTELLIGENCE SUMMARY INSTRUCTIONS

In an effort to enhance the understanding of the INTSUM and to save dissemination time, the INTSUM is graphically portrayed as a single or set of map overlays. Intelligence summaries can be posted in graphic and text formats on web-based automated information systems, which provides MAGTF intelligence users with access to the web site the option of pulling intelligence and products.

There are limitations to electronically generated graphic INTSUMs. Graphics can require large bandwidth and processing power to be pulled over a web-based system, with possible degradation of the overall MAGTF tactical data network. Lower-level tactical units and allied nation forces may not possess the means to access and use the information, which generally requires graphic and text INTSUMs to be disseminated using other electronic transmission methods and hard copy delivery.

Graphic INTSUMs must convey essential intelligence and other information in a clear, concise, and easy to understand visual format. Because of the volume of detail to be presented, most graphic INTSUMs, particularly at higher commands, have evolved into digital slide shows. The unit SOP or Annex B to the OPORD establishes graphic INTSUM formats, which are tailored to the level of command, type of operation, and the commander's intelligence requirements. Generally graphic INTSUMs contain the same elements. The following are examples of common graphic INTSUM elements:

- **Weather Graphics—Composite graphics, based on satellite imaging, showing area weather fronts, cloud coverage, high and low pressure areas, etc. May include forecast graphics for specified future periods.**
- **5-Day Forecast—Similar to television weather forecasts, showing forecast weather conditions (e.g., cloudy, partly cloudy, rainy), high and low temperatures, winds, normal temperatures based on climatology, and any other elements that may be of interest to the commander; should also include light data for the same period.**
- **Weather Impacts Graphics—Normally presented in green, yellow, and red colored chart format; should include those forces, types of operations, or critical items of equipment that are essential to friendly and enemy unit mission performance.**
- **PIRs—Current and new PIRs, and may include a satisfaction level (i.e., not answered, partially answered, answered) assessment for each requirement.**
- **Activities and Assessments—Consists of a graphical situation map denoting locations of threat forces of interest and, if possible, graphically indicating status or combat effectiveness using color coding or other symbology. Depending on the level of command and information needs, separate graphics for categories of threat forces (i.e., ground, air, air defense) may be created to increase clarity. Each graphic should—**
  - **Note significant threat activity over the reporting period with text comment boxes tied to locations or an event numbering system with marginal text comments.**
  - **Provide an assessment based on the commander's PIRs.**
  - **Use supporting graphics to examine items in detail, such as aircraft sortie analysis or the location and status of a particular category of force or equipment (e.g., heavy equipment transporter systems, specialized units).**

- **Collection, Production, and Dissemination Plans and Status of Planned Missions and Tasks—Graphically presents locations of organic collection assets (e.g., reconnaissance teams, radio battalion assets, unmanned aerial vehicle tracks, sensor strings) and/or provides a time line showing daily projected availability windows and mission tracks (as applicable) of nonorganic supporting assets (e.g., Airborne Warning and Control System, RC-135, U2); also identifies changes to previous production and dissemination plans and any new plans.**
- **Outlook or Assessment—Provides an overall assessment of estimated threat courses of action (at a minimum, the threat's most likely and most dangerous courses of action). The assessment may be broken into estimate time periods, such as 24-48 hours, 48-96 hours, or whatever periods of time are applicable to the commands requirements to plan future actions. Courses of action should be graphically portrayed. In prehostilities or MOOTW, these graphics may be used to address anticipated political or societal actions or events that may impact the force.**

APPENDIX G. INTELLIGENCE REPORT FORMAT

An intelligence report (INTREP) is a standardized report that is used to disseminate important intelligence without regard to a specific schedule. The first intelligence element acquiring the information prepares and disseminates the INTREP as rapidly as possible to units requiring the information. Generally, each report will concern only a single item.

An INTREP is generally required whenever an event occurs that is likely to result in a change in the friendly plan or when a change to the current or future analytical assessment is made. The intelligence element generally initiates an INTREP when facts influencing threat capabilities have been observed or when a change in threat capabilities has taken place. The commander's priority intelligence requirements serve as the basis for determining what information warrants an INTREP.

Whenever possible, the INTREP should include the originator's significant intelligence assessment as well as a source reliability and accuracy evaluation. The format below is a sample INTREP that would be posted on a web site or forwarded via SECRET internet protocol router network (SIPRNET) or MAGTF tactical data network (TDN) electronic mail.

CLASSIFICATION/RELEASABILITY

INTREP#: DD-001-97 (Sequentially numbered by originating unit)

DTG: DDHHMM(Time Zone) (Month) YY

I. ( ) Significant Event(s): Summarize the significant event(s) or developments that initiated the INTREP. Answer either the 5Ws (i.e., who, what, where, when, and why) or the SALUTE (i.e., size, activity, location, unit, time, equipment) formats.

II. ( ) Assessment: Describe the effect of the current activity on threat capabilities or courses of action.

III.( ) Evaluation of Source: State the original information source and evaluate the accuracy and reliability of that source.

Note: ( ) Reflects classification of that information line.

APPENDIX H. INTELLIGENCE INFORMATION BRIEF

The intent of the intelligence information brief is to enhance situational awareness and impart understanding. Intelligence information briefings may be as simple as a quick verbal update to a commander in front of a situation map or as complex as a Marine expeditionary force or joint task force level daily update to the commanding general and staff. At lower tactical levels, briefings are generally less formal and often short-notice. Higher commands generally employ regularly scheduled daily update briefings, which include intelligence. Regardless of the degree of formality or the level of command, a standard briefing format or outline can help intelligence personnel to rapidly and effectively organize for the brief.

To develop and deliver an effective intelligence information brief, intelligence personnel should—

- Know the audience. Is the audience the commander, the staff, or subordinate commanders? Who is the focus of the brief? What is audience's level of knowledge concerning the subject? Does the commander have any briefing preferences?
- Know the purpose and intent of the briefing. Is the brief a critical events update, or is it intended to describe in detail the threat and area of operations prior to crisis action planning?
- Concentrate on essential information and intelligence; prepare to provide details or expand intelligence should questions arise.
- Use clear, concise, readable graphics; ensure graphics can be seen from the rear of the room.
- Know the information; anticipate questions on unfamiliar subjects and arrange to have a subject matter expert present or take questions for follow-up research; never make up an answer.
- Distinguish between known facts and gaps or estimates.

The most common type of intelligence information briefing is the boardwalk. The boardwalk is an informal, on-demand brief conducted using the combat operations center map boards or screen displays from automated systems. Generally, the brief only presents significant changes to threat capabilities or courses of action. This brief also provides the commander an opportunity to ask direct questions.

At higher command echelons, the most common type of intelligence information brief is the commander's morning or evening update brief. Usually more formal and detailed, these briefs are scheduled for set times either once or twice per day. The planning, decision execution, and assessment cycle or unit standing operating procedure determines the schedule. In addition to briefing the current situation and significant events, this brief may address the commander's priority intelligence requirements (PIRs); collection, production, dissemination plans and status; weather; and estimates of future threat actions. Often briefings are presented using graphics software.

By focusing on intelligence and events that correspond to the commander's PIRs, the briefer can quickly organize information and intelligence as well as ensure that the commander is given the most essential information in the shortest amount of time. The brief is also used to present significant occurrences affecting current or future plans.

The following are examples of update briefing elements:

- Weather Forecast.
- Weather Effects Assessment.
- PIRs and Intelligence Requirements (IRs).
- Situation (e.g., ground, air, air defense) Keyed to PIRs.

- **Collection, Production, and Dissemination Plan Status.**
- **Intelligence Estimate (at a minimum, the most likely and most dangerous enemy courses of action).**

These elements closely follow the elements of the web-based intelligence summary (INTSUM) graphic. See appendix F. Because the INTSUM and the update provide the same intelligence and other information, using the same format and graphics can save time and resources. To save more time, elements that have not changed since the last briefing can be briefed as "no change." However, the weather forecast, PIRs, plans status, and intelligence estimate should always be briefed.

APPENDIX I. PRODUCTION REQUIREMENT AND REQUEST FOR INTELLIGENCE FORMAT

An intelligence production requirement (IPR), production requirement (PR), or request for intelligence (RFI) begins as an intelligence requirement (IR) levied on a unit's intelligence section. If the unit cannot satisfy the requirement with the available resources, the requirement must be forwarded up the chain of command for satisfaction. The requirement then becomes either an intelligence collection requirement (ICR), an RFI, or an IPR. Single or multiple requests for information may be combined into one PR.

A requirement must contain the following four basic elements:

- **Who—Organization and specific office or individual that submitted the original requirement.**
- **What—Statement describing the intelligence required.**
- **When—Latest time information of value.**
- **How—Requested product format (e.g., hard copy, soft copy, verbal report), quantities, all receiving units.**

Most theater tactics, techniques, and procedures (TTP) combine the three forms of requirements into one basic PR or RFI format. The joint task force headquarters intelligence directorate or combatant command joint intelligence center receiving the requirement determines whether collection or product development is necessary.

Defense Intelligence Agency also has an established basic PR or RFI format. This format is used in the Community On-Line Intelligence System for End Users and Managers (COLISEUM), which has become the standard medium for requirements submission throughout the Department of Defense intelligence production community. The following COLISEUM format is from Defense Intelligence Management Document (DIMD) 0000-151C-95, *Department of Defense Intelligence Production Program (DODIPP): Production Procedures*. Although theater TTP formats generally follow the same elements, they are modified according to the specific theater needs. Marine air-ground task forces and Marine Corps forces headquarters must follow the procedures established in their theater of operation.

Item 1. PR Number—A 12-space number with 10 alphanumeric characters and 2 separation dashes (e.g., C610-94-0001). The unit intelligence section requesting the information or production enters this number, which is unique to the unit. The first four characters are the customer's statement of intelligence interest (SII) account number or in a crisis, the customer's unit identification code (UIC). The second two numbers are the fiscal year. The last four numbers are the customer's sequence number for PRs or RFIs submitted in the fiscal year.

Item 2. Subject—A short descriptive, unclassified (if possible) title. Clarity is more important than keeping the subject unclassified.

Item 3. Customer's Organization—This line should include the end user's name, organization, mailing address, electronic-mail address (clearly identify Joint Worldwide Intelligence Communications Systems [JWICS] or Secret internet protocol router network [SIPRNET]), naval message address, and if possible, the customer's commercial and DSN phone numbers.

Item 4. Date of Request—Entered by the supporting intelligence office in YYMMDD format.

Item 5. Date Product Required—The latest date the product or information will be of value to the customer. Also referred to as latest time information of value (LTIOV).

Item 6. Form and Frequency of Response—This item is key to getting the desired response to the requirement. Sub items should be narrative with an emphasis on clarity:

- **Media—Identify the preferred product form and second and third alternatives. Examples are message, floppy disk, CD-ROM, on-line data base, data base printout, bound hard copy report, study, or handbook. In addition to the media requested, the production element often disseminates intelligence and pertinent information in other media to increase access to a wider number of potential users.**
- **Frequency—Specify request for scheduled, non-crisis-related production as one-time, as required, or recurring. Crisis or immediate production requests are normally handled as one-time requests unless otherwise specified.**
- **Revision or New Product—Specify the existing product requiring update as completely as possible, or specify as a new PR.**
- **Classification and Releasability—Provide the desired classification and the highest classification that can be used by the customer. If the product needs to be releasable to foreign forces, specify which forces, if known, and justify the release.**

Item 7. Statement of Requirement—The first paragraph should provide a summary of the requirement in 50 words or less. If the requirement supports an operation plan or contingency plan, the first sentence should identify which plan. Subsequent paragraphs should provide greater detail, specific intelligence and information elements, and a justification. The justification should specify what intelligence and other information sources have been consulted and why they were not sufficient to answer the requirement. If the requirement addresses separate questions, or multiple countries or topics, they must be prioritized. If all requests carry the same priority, list them by time urgency.

Item 8. Comments—Additional comments as necessary.

Item 9. Security Classification—The highest classification of the question and information contained in the requirement. The lower the classification, the easier it will be to process and use; however, clarity should not be sacrificed for lower classification. Codeword or special access program requirements will be submitted through appropriate channels and may require additional time to transmit and process.

APPENDIX J. GLOSSARY

SECTION I. ACRONYMS AND ABBREVIATIONS

AA . . . . . avenue of approach
ACE . . . . . aviation combat element
AC/S . . . . . assistant chief of staff
ADA . . . . . air defense artillery
AFP . . . . . all-source fusion platoon
AI . . . . . air interdiction
AIntP . . . . . allied intelligence publication
AO . . . . . area of operations
AOA . . . . . amphibious objective area
AOI . . . . . area of interest
ATARS . . . . . advanced tactical airborne reconnaissance system
ATF . . . . . amphibious task force
ATO . . . . . air tasking order
AWACS . . . . . Airborne Warning and Control System

BDA . . . . . battle damage assessment
BDE . . . . . brigade
BE . . . . . basic encyclopedia
BP . . . . . battle position

C2 . . . . . command and control
C2W . . . . . command and control warfare
CA . . . . . combat assessment
CAS . . . . . close air support
CATF . . . . . commander, amphibious task force
CATK . . . . . counterattack
CCIR . . . . . commander's critical information requirements
CD-ROM . . . . compact disc read only memory
CE . . . . . command element
CG . . . . . commanding general
CHATS . . . . . CI/HUMINT automated tool set
CI . . . . . counterintelligence
CIA . . . . . Central Intelligence Agency
CIB . . . . . controlled image base
CIC . . . . . combat intelligence center
CINC . . . . . commander in chief
CIS . . . . . communications and information systems
CNTRMOB . . . . . countermobility
COA . . . . . course of action
COC . . . . . combat operations center
COG . . . . . center of gravity
COLISEUM . . . . . Community On-Line Intelligence System for End Users and Managers
CONPLAN . . . . . contingency plan
COO . . . . . combined obstacle overlay
CP . . . . . command post
CPX . . . . . command post exercise
CSS . . . . . combat service support

D3A . . . . . decide, detect, deliver, assess
DDHHMM . . . . . day, hour, minute
DEST . . . . . destination
DIA . . . . . Defense Intelligence Agency
DIMD . . . . . defense intelligence management document
DISUM . . . . . daily intelligence summary
DMGD . . . . . damaged
DMS . . . . . Defense Message System
DOD . . . . . Department of Defense
DODIPP . . . . . Department of Defense Intelligence Production Program
DON . . . . . Department of the Navy
DP . . . . . decision point
DPM . . . . . Dissemination Program Manager
DSN . . . . . Defense Switched Network
DST . . . . . decision support template
DTG . . . . . date-time group
DZ . . . . . drop zone

EA . . . . . electronic attack
e.g. . . . . . for example
EPW . . . . . enemy prisoner of war

FARP . . . . . forward arming and refueling point
FDA . . . . . functional damage assessment
FFC . . . . . force fires cell
FFIR . . . . . friendly force information requirements
FLIR . . . . . forward-looking infrared
FM . . . . . field manual (Army)
FMFRP . . . . . Fleet Marine Force reference publication
FSSG . . . . . force service support group

G-1 . . . . . manpower or personnel staff officer/organization

G-2 . . . . . intelligence staff officer/organization
G-3 . . . . . operations staff officer/organization
G-4 . . . . . logistics staff officer/organization
G-5 . . . . . plans officer/organization
GCE . . . . . ground combat element
GENSER. . . . . general service
GEOINT . . . . . geographic intelligence

HF . . . . . high frequency
HLZ. . . . . helicopter landing zone
HN. . . . . host nation
HPT. . . . . .high-payoff target
HPTL . . . . . .high-payoff target list
HQ. . . . . .headquarters
HUMINT . . . . . .human intelligence
HVT . . . . . high-value target

i.e. . . . . that is
I&W . . . . . .indications and warning
IAS . . . . . .intelligence analysis system
ICR . . . . . intelligence collection requirement
IDR . . . . intelligence dissemination requirement
IIP . . . . . imagery intelligence platoon
IMINT. . . . . .imagery intelligence
IMO. . . . . .imagery and mapping officer
intel bn . . . . . intelligence battalion
INTELINK . . . . . intelligence link
INTELINK-S . . . . . intelligence link-SECRET
INTREP . . . . . intelligence report
INTSUM. . . . . .intelligence summary
IOC . . . . . intelligence operations center
IPB . . . . . .intelligence preparation of the battlespace
IPR . . . . . intelligence production requirement
IR . . . . . .intelligence requirement
ISC . . . . . intelligence support coordinator
ISM . . . . . .intelligence synchronization matrix
ISS. . . . . .intelligence synchronization sheet

J-2 . . . . . .intelligence directorate
JAC . . . . . joint analysis center
JCS . . . . . .Joint Chiefs of Staff
JDISS . . . . . Joint Deployable Intelligence Support System
JDS . . . . . .Joint Dissemination System
JFC . . . . . .joint force commander
JFIC. . . . . .Joint Forces Intelligence Command
JIC . . . . . joint intelligence center
JISE. . . . . joint intelligence support element
JOG-A. . . . . joint operations graphic-air
JP. . . . . .joint publication
JSIPS. . . . . .Joint Services Imagery Processing System
JSTARS . . . . . joint surveillance, target attack radar system
JTF . . . . . joint task force
JWICS. . . . . .Joint Worldwide Intelligence Communications System

KIA . . . . . killed in action
km . . . . . kilometer
KOCOA . . . .key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach, and mobility corridors

LCAC . . . . . .landing craft air cushion
LOA . . . . . limit of advance
LOC . . . . . line of communications
LOS. . . . . line of sight
LTIOV . . . . . .latest time information of value
LZ . . . . . .landing zone

MAGTF . . . . . Marine air-ground task force
MARFOR . . . . . .Marine Corps forces
MAW . . . . . .Marine aircraft wing
MCDP. . . . . Marine Corps doctrinal publication
MCIA . . . . . Marine Corps Intelligence Activity
MCISU . . . Marine Corps Imagery Support Unit
MCOO . . . modified combined obstacle overlay
MCRP. . . . .Marine Corps reference publication
MCWP . . . . . Marine Corps warfighting publication
MEA . . . . . mission effectiveness assessment
MEF . . . . . Marine expeditionary force
METT-T . . . . . mission, enemy, terrain and weather, troops and support available-time available
MEU(SOC) . . . . . Marine expeditionary unit (special operations capable)
MIDB . . . . . .modernized integrated database
mm . . . . . millimeters
MOB . . . . . mobility
MOOTW. . . . military operations other than war
MOS . . . . . military occupational specialty
MSC . . . . . major subordinate command
MSE . . . . . .major subordinate element
MTI. . . . . moving target indicator
MTW. . . . . major theater war

NA. . . . . .not applicable

NAI . . . . . named area of interest
NAIC. . . . . National Air Intelligence Center
NATO . . . . . North Atlantic Treaty Organization
NBC . . . . . nuclear, biological, and chemical
NEF. . . . . naval expeditionary force
NEO . . . . . noncombatant evacuation operation
NGIC. . . . . National Ground Intelligence Center
NGO . . . . . nongovernmental organization
NIMA . . . . . National Imagery and Mapping Agency
NIPRNET . . . . . nonsecure internet protocol router network
NIS . . . . . national input segment
NIST . . . . . national intelligence support team
NMIC . . National Maritime Intelligence Center
NOE . . . . . nap of the earth
NSA . . . . . National Security Agency
NSTR . . . . . nothing significant to report
NVG . . . . . night vision goggles

obj . . . . . objective
OCAC . . . . . operations control and analysis center
OIC . . . . . officer in charge
OMFTS . . . operational maneuver from the sea
OOB . . . . . order of battle
OPCON . . . . . operational control
OPLAN . . . . . operation plan
OPORD . . . . . operation order

P&A . . . . . production and analysis
PDA . . . . . physical damage assessment
PDE&A . . . . . planning, decision, execution, and assessment
PIR . . . . . priority intelligence requirement
POC. . . . . point of contact
POL. . . . . petroleum, oils, and lubricants
PR . . . . . production requirement
PVO . . . . . private voluntary organization

RAG . . . . . regimental artillery group
RC. . . . . reconnaissance capable
recon . . . . . reconnaissance
rep . . . . . representative
RFI . . . . . request for intelligence
RR. . . . . reattack recommendation
RRS. . . . . remote receive station

S-1. . . . . manpower or personnel staff officer/organization
S-2. . . . . intelligence staff officer/organization
S-3. . . . . operations staff officer/organization
SALUTE. . . . . size, activity, location, unit, time, equipment
SAM . . . . . surface-to-air missile
SARC . . . . surveillance and reconnaissance cell
SATCOM . . . . . satellite communications
SCI . . . . . sensitive compartmented information
SCR. . . . . single channel radio
SIDS . . . . . secondary imagery dissemination system
SIGINT . . . . . signals intelligence
SII . . . . . statement of intelligence interest
SIPRNET . . . . . SECRET Internet Protocol Router Network
SOA . . . . . sustained operations ashore
SOP. . . . . standing operating procedure
SPMAGTF . . . . . special-purpose Marine air-ground task force
SPP . . . . . shared production program
STANAG . . . . . standardization agreement (NATO)

TAA . . . . . tactical assembly area
TAI . . . . . targeted area of interest
TCAC . . . . technical control and analysis center
TDN . . . . . tactical data network
T/E . . . . . table of equipment
TEG. . . . . tactical exploitation group
TERPES . . . . tactical electronic reconnaissance processing and evaluation system
T/O . . . . . table of organization
topo . . . . . topographic
TOR . . . . . time of report
TPC. . . . . topographic production capability
TPL. . . . . time phase lines
TRSS. . . . . tactical remote sensor system
TSA. . . . . target system assessment
TTP . . . . . tactics, techniques, and procedures

UAV . . . . . unmanned aerial vehicle
UIC . . . . . unit identification code
U.S. . . . . United States
UTM . . . . . universal transverse mercator

VHF . . . . . very high frequency
VMAQ . . . . . Marine tactical electronic warfare squadron
VMU . . . . . Marine unmanned aerial vehicle squadron
VO. . . . . validation office

WIA . . . . . wounded in action
YYMMDD . . . . . year, month, day

SECTION II. DEFINITIONS

a priori—Probabilities, in the absence of other information; presupposed by experience.

all-source intelligence—Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. (JP 1-02)

amphibious force—An amphibious task force and a landing force together with other forces that are trained, organized, and equipped for amphibious operations. (Proposed by JP 3-02 for inclusion in JP 1-02)

amphibious objective area—A geographical area, delineated in the initiating directive, for purposes of command and control within which is located the objective(s) to be secured by the amphibious task force. This area must be of sufficient size to ensure accomplishment of the amphibious task force's mission and must provide sufficient area for conducting necessary sea, air, and land operations. Also called AOA. (JP 1-02)

amphibious task force—A Navy task organization formed to conduct amphibious operations. The amphibious task force, together with the landing force and other forces, constitutes the amphibious force. Also called ATF. (Proposed by JP 3-02 for inclusion in JP 1-02)

analysis—In intelligence usage, a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation. See also intelligence cycle. (JP 1-02) The sifting and sorting of evaluated information to isolate significant elements with respect to the mission and operations of the command. (MCWP 2-1)

area of interest—That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (JP 1-02)

area of operations—An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. Also called AO. (JP 1-02)

aviation combat element—The core element of a Marine air-ground task force that is task-organized to conduct aviation operations. The aviation combat element provides all or a portion of the six functions of Marine aviation necessary to accomplish the Marine air-ground task force's mission. These functions are anti-air warfare, offensive air support, assault support, electronic warfare, air reconnaissance, and control of aircraft and missiles. The aviation combat element is usually composed of an aviation unit headquarters and various other aviation units or their detachments. It can vary in size from a small aviation detachment of specifically required aircraft to one or more Marine aircraft wings. The aviation combat element may contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. The aviation combat element itself is not a formal command. Also called ACE. (Approved for inclusion in next version of MCRP 5-12C)

basic intelligence—Fundamental intelligence concern-ing the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (JP 1-02)

battle damage assessment—1. The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (JP 1-02) 2. In Marine Corps usage, the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCWP 5-12C)

battlespace—All aspects of air, surface, subsurface, land, space, and electromagnetic spectrum which encompass the area of influence and area of interest. (MCRP 5-12C)

battlespace dominance—The degree of control over the dimensions of the battlespace which enhances friendly freedom of action and denies enemy freedom of action. It permits force sustainment and application of power projection to accomplish the full range of potential operational and tactical missions. It includes all actions conducted against enemy capabilities to influence future operations. (MCRP 5-12C)

branch(es)—A contingency plan or course of action (an option built into the basic plan or course of action) for changing the mission, disposition, orientation, or direction of movement of the force to aid success of the operation based on anticipated events, opportunities, or disruptions caused by enemy actions. See also sequel(s). (MCRP 5-12C)

centers of gravity—1. Those characteristics, capa-bilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. Also called COG. (JP 1-02) 2. A key source of strength without which an enemy cannot function. (MCDP 1-2)

centralized control—In military operations, a mode of battlespace management in which one echelon of command exercises total authority and direction of all aspects of one or more warfighting functions. It is a method of control where detailed orders are issued and total unity of action is the overriding consideration. (MCRP 5-12C)

collate—1. The grouping together of related items to provide a record of events and facilitate further processing. 2. To compare critically two or more items or documents concerning the same general subject; normally accomplished in the processing phase in the intelligence cycle. (JP 1-02)

collection—Acquisition of information and the provision of this information to processing and/or production elements. (JP 1-02) In Marine Corps usage, the gathering of intelligence data and information to satisfy the identified requirements. (MCWP 5-12C)

collection agency—Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (JP 1-02)

collection asset—A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02)

collection management—The process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 1-02)

collection manager—An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. (JP 1-02)

collection plan—A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02)

combat assessment—The determination of the overall effectiveness of tactical force employment during military operations. Combat assessment is composed of three major components, (a) battle damage assessment (BDA), (b) munitions effects assessment, and (c) future course-of-action (COA) or reattack recommendation. Also called CA. (Proposed by JP 3-60 for inclusion in JP 1-02.)

combat data—Data derived from reporting by opera-tional units. (MCWP 5-12C)

combatant command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

combined operation—An operation conducted by forces of two or more allied nations acting together for the accomplishment of a single mission. (JP 1-02)

command and control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1-02) Also in Marine Corps usage, the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCRP 5-12C)

command and control warfare—The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Also called C2W. (Excerpt from JP 1-02)

command element—The core element of a Marine air-ground task force that is the headquarters. The command element is composed of the commander, general or executive and special staff sections, headquarters section, and requisite communications support, intelligence and reconnaissance forces, necessary to accomplish the MAGTF's mission. The command element provides command and control, intelligence, and other support essential for effective planning and execution of operations by the other elements of the Marine air-ground task force. The command element varies in size and composition and may contain other Service or foreign military forces assigned or attached to the MAGTF. Also called CE. (Approved for inclusion in next version of MCRP 5-12C)

commander's critical information requirements—Information regarding the enemy and friendly activities and the environment identi-

fied by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR. NOTE: CCIRs are normally divided into three primary subcategories: priority intelligence requirements; friendly force information requirements; and essential elements of friendly information. (MCRP 5-12C)

commander's intent—A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

commander's planning guidance—Directions and/or instructions which focus the staff's course of action de-velopment during the planning process. (MCRP 5-12C)

communications intelligence—Technical and intel-ligence information derived from foreign communi-cations by other than the intended recipients. (JP 1-02)

communications security—The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (Excerpt from JP 1-02)

coordination—The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (MCRP 5-12C)

counterintelligence—1. Information gathered and ac-tivities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02) 2. Within the Marine Corps, counterintelligence constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. Also called CI. (MCRP 5-12C)

crisis action planning—The time-sensitive planning for the deployment, employment, and sustainment of assigned and allocated forces and resources that occurs in response to a situation that may result in actual military operations. Crisis action planners base their plan on the circumstances that exist at the time planning occurs. (JP 1-02)

critical information—Specific facts about friendly in-tentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02)

critical intelligence—Intelligence which is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential/actual enemy. It includes but is not limited to the following: a. strong indications of the imminent outbreak of hostilities of any type (warning of attack); b. aggression of any nature against a friendly country; c. indications or use of nuclear-biological-chemical weapons (targets); d. significant events within potential enemy countries that may lead to modification of nuclear strike plans. (JP 1-02)

critical node—An element, position, or communica-tions entity whose disruption or destruction immediately degrades the ability of

a force to command, control, or effectively conduct combat operations. (JP 1-02)

critical vulnerability—An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. (MCRP 5-12C)

daily intelligence summary—A report prepared in message form at the joint force headquarters that provides higher, lateral, and subordinate headquarters with a summary of all significant intelligence produced during the previous 24-hour period. The "as of" time for information, content, and submission time for the report will be as specified by the joint force commander. Also called DISUM. (JP 1-02)

data—Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (JP 1-02)

data base—Information that is normally structured and indexed for user access and review. Data bases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (JP 1-02)

database replication—Process by which like databases reflect commonality in information and timeliness of that information. (MCRP 5-12C)

debriefing—Interviewing of an individual who has completed an intelligence or reconnaissance assignment or who has knowledge, whether through observation, participation, or otherwise, of operational or intelligence significance. (MCRP 5-12C)

decentralized control—In military operations, a mode of battlespace management in which a command echelon may delegate some or all authority and direction for warfighting functions to subordinates. It requires careful and clear articulation of mission, intent, and main effort to unify efforts of subordinate leaders. (MCRP 5-12C)

deception operation—A military operation conducted to mislead the enemy. A unit conducting a deception operation may or may not make contact with the enemy. Deception operations include demonstrations, diversions, displays, feints, ruses, actions, events, means, and objectives. (MCRP 5-12C)

decision point—An event, area, or point in the battlespace where and when the friendly commander will make a critical decision. Also called DP. (MCRP 5-12C)

deliberate planning—A planning process for the deployment and employment of apportioned forces and resources that occurs in response to a hypothetical situation. Deliberate planners rely heavily on assumptions regarding the circumstances that will exist when the plan is executed. (JP 1-02)

deliberate targeting—The methodical identification, compilation, and analysis of potential fixed or semifixed targets followed by the decision of which potential targets will be attacked, when, and/or by what weapon and ordnance. It is practiced primarily during the planning phase of an operation, when planning for an attack, or when the tempo of combat is slow. (MCRP 5-12C)

descriptive intelligence—Class of intelligence which describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: *basic intelligence*, which is general background knowledge about established and relatively constant conditions; and *current intelligence*, which is concerned with describing the existing situation. (MCRP 5-12C)

detachment—1. A part of a unit separated from its main organization for duty elsewhere. 2. A temporary military or naval unit formed from other units or parts of units. (JP 1-02)

direction finding—A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. (JP 1-02)

direct support—A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance. (JP 1-02)

dissemination—Conveyance of intelligence to users in a suitable form. (JP 1-02)

dissemination management—Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12C)

effective damage—That damage necessary to render a target element inoperative, unserviceable, nonproductive, or uninhabitable. (JP 1-02)

effectiveness—The measurement of the results of military action against a target by lethal or nonlethal means. (Proposed by JP 3-60 for inclusion in JP 1-02.)

effects—The result of military action against a target by lethal or nonlethal means. (Proposed by JP 3-60 for inclusion in JP 1-02.)

effects assessment—A determination of the overall effectiveness of force or weapon system employment during military operations and recommends future courses of action. Effects assessment is conducted at the strategic, operational, and tactical levels-of war or MOOTW. Effects assessment is the assessment of all execution effects, and includes steps commonly associated with combat assessment. (Proposed by JP 3-60 for inclusion in JP 1-02.)

electromagnetic spectrum—The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02)

electronic attack—That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. (JP 1-02)

electronic intelligence—Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 1-02)

electronic protection—That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment or electronic warfare that degrade, neutralize, or destroy friendly combat capability. (JP 1-02)

electronic reconnaissance—The detection, identifica-tion, evaluation, and location of foreign electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 1-02)

electronic warfare—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three

major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support. Also called EW. (Excerpt from JP 1-02)

electronic warfare support—That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence (SIGINT), communications intelligence (COMINT), and electronic intelligence (ELINT). (JP 1-02)

essential elements of friendly information—1. Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. Also called EEFI. (JP 1-02) 2. Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. (MCRP 5-12C)

estimative intelligence—Class of intelligence which attempts to anticipate future possibilities and probabilities based on an analysis of descriptive intelligence in the context of planned friendly and assessed enemy operations. See also descriptive intelligence. (MCRP 5-12C)

evaluation—In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. Appraisal is accomplished at several stages within the intelligence cycle with progressively different contexts. Initial evaluations, made by case officers and report officers, are focused upon the reliability of the source and the accuracy of the information as judged by data available at or close to their operational levels. Later evaluations by intelligence analysts, are primarily concerned with verifying accuracy of information and may, in effect, convert information into intelligence. Appraisal or evaluation of items of information or intelligence is indicated by a standard letter-number system. The evaluation of the reliability of sources is designated by a letter from A through F, and the accuracy of the information is designated by numeral 1 through 6. These are two entirely independent appraisals, and these separate appraisals are indicated in accordance with the system indicated below. Thus, information adjudged to be "probably true" received from a "usually reliable source" is designated "B-2" or "B2," while information of which the "truth cannot be judged" received from a "usually reliable source" is designated "B-6" or "B6."

Reliability of Source

A - Completely reliable
B - Usually reliable
C - Fairly reliable
D - Not usually reliable
E - Unreliable
F - Reliability cannot be judged

Accuracy of Information

1 - Confirmed by other sources
2 - Probably true
3 - Possibly true
4 - Doubtful
5 - Improbable
6 - Truth cannot be judged (JP 1-02)

fires—The effects of lethal or nonlethal weapons. (JP 1-02)

force protection—Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combatting terrorism, physical security, operations

security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (JP 1-02)

force reconnaissance company—A unit whose mission is to conduct preassault and deep postassault reconnaissance operations in support of a landing force and its subordinate elements. (MCRP 5-12C)

friendly force information requirements—Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition, readiness, personnel status, and logistics status could become a friendly force information requirement. Also called FFIR. (MCRP 5-12C)

functional damage assessment—The estimate of the effect of military force to degrade/destroy the functional or operational capability of the target to perform its intended mission and on the level of success in achieving operational objectives established against the target. This assessment is based upon all-source information, and includes an estimation of the time required for recuperation or replacement of the target function. (Upon approval of JP 3-60, this term and its definition will be included in JP 1-02.)

fusion—In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 1-02)

fusion center—In intelligence usage, a physical location to accomplish fusion. It normally has sufficient intelligence automated data processing capability to assist in the process. (JP 1-02)

future operations section—1. In MAGTF operations, a section normally under the staff cognizance of the G-3 which focuses on planning/producing new fragmentary orders or the next change of major subordinate command mission; this section forms and leads the integrated planning effort with a planning horizon of 72-120 hours out. It develops branch plans and sequels. 2. In Marine aviation, that portion of the tactical air command center and aviation combat element commander's battlestaff responsible for the detailed planning and coordination of all future air operations conducted by the aviation combat element in support of the Marine air-ground task force. The future operations section plans for and publishes the next air tasking order(s) (normally a 48/72-hour period). (MCRP 5-12C)

general military intelligence—Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or allied military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries,; military and civilian C4 systems; military economics, including foreign military assistance; insurgency and terrorism; military-political-sociological intelligence; location, identification, and description of military-related installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence.) (JP 1-02)

general support—That support which is given to the supported force as a whole and not to any particular subdivision thereof. (JP 1-02)

geographic coordinates—The quantities of latitude and longitude which define the position of a point on the surface of the earth with respect to the reference spheroid. (JP 1-02)

geographic intelligence—The process of collecting, organizing, analyzing, synthesizing, disseminating and utilizing geospatial information and services (GI&S) with regards to the military aspects of the terrain. Also called GEOINT. GEOINT is the integration and analysis of all-source geospatial information in support of specific Marine Corps operations. The analysis is focused on a specific mission and includes intensification of information detail and resolution to meet tactical requirements. GEOINT analysis is focused on the intelligence preparation of the battlespace (IPB) process and addresses key terrain, observation & fields of fire, cover & concealment, obstacles, avenues of approach & mobility corridors. This analysis is commonly referred to as KOCOA for easy reference.

geospatial information and services—The concept for collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. These data are used for military planning, training, and operations including navigation, mission planning, mission rehearsal, modeling, simulation and precise targeting. Geospatial information provides the basic framework for battlespace visualization. It is information produced by multiple sources to common interoperable data standards. It may be presented in the form of printed maps, charts, and publications; in digital simulation and modeling data bases; in photographic form; or in the form of digitized maps and charts or attributed centerline data. Geospatial services include tools that enable users to access and manipulate data, and also includes instruction, training, laboratory support, and guidance for the use of geospatial data. (JP 1-02)

global sourcing—A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

ground combat element—The core element of a Marine air-ground task force that is task-organized to conduct ground operations. It is usually constructed around an infantry organization but can vary in size from a small ground unit of any type, to one or more Marine divisions that can be independently maneuvered under the direction of the MAGTF commander. It includes appropriate ground combat and combat support forces and may contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. The ground combat element itself is not a formal command. Also called GCE. (Approved for inclusion in next version of MCRP 5-12C)

helicopter landing zone—A specified ground area for landing assault helicopters to embark or disembark troops and/or cargo. A landing zone may contain one or more landing sites. Also called HLZ. (JP 1-02)

high-payoff target—A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through wargaming, which must be acquired and successfully attacked for the success of the friendly commander's mission. Also called HPT. (JP 1-02)

high-value target—A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. Also called HVT. (JP 1-02)

human intelligence—1. A category of intelligence derived from information collected and provided by human sources. (JP 1-02) 2. In Marine Corps usage, human intelligence operations cover a wide range of activities encompassing reconnaissance patrols, aircrew debriefs,

debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations. Also called HUMINT. (JP 1-02)

humanitarian assistance—Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Humanitarian assistance provided by US forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing humanitarian assistance. (JP 1-02)

hydrography—The science which deals with the measurements and description of the physical features of the oceans, seas, lakes, rivers, and their adjoining coastal areas, with particular reference to their use for navigational purposes. (JP 1-02)

imagery exploitation—The cycle of processing and printing imagery to the positive or negative state, assembly into imagery packs, identification, interpretation, mensuration, information extraction, the preparation of reports, and the dissemination of information. (JP 1-02)

imagery intelligence—Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called IMINT. (JP 1-02)

imagery interpretation—The process of location, recognition, identification, and description of objects, activities, and terrain represented on imagery. (JP 1-02)

immediate targets—Targets upon which are detected too late to be included in the normal targeting process, therefore, effects have not been scheduled. Immediate targets have three subcategories: unplanned, unanticipated, and time-sensitive. (Upon approval of JP 3-60, this term and its definition will be included in JP 1-02.)

indications and warning—Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (JP 1-02)

indirect effects—Result created through an inter-mediate effect or mechanism to produce the final outcome, which may be physical or psychological in nature. Indirect effects tend to be delayed, and may be difficult to recognize. (Proposed by JP 3-60 for inclusion in JP 1-02.)

information—1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

information exchange requirement—The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom, as well as why the information is necessary and how that information will be used. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included

in the information exchange requirement. (MCRP 5-12C)

information report—Report used to forward raw information collected to fulfill intelligence requirements. (JP 1-02)

information requirements—Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 1-02)

integration—A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. (JP 1-02)

intelligence—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02) Also in Marine Corps usage, intelligence is knowledge about the enemy or the surrounding environment needed to support decision-making. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence annex—A supporting document of an operation plan or order that provides detailed information on the enemy situation, assignment of intelligence tasks, and intelligence administrative procedures. (JP 1-02)

intelligence cycle—The steps by which information is converted into intelligence and made available to users. (Excerpt from JP 1-02)

intelligence data—Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline—A well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), and open-source intelligence. (JP 1-02)

intelligence estimate—The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (JP 1-02)

intelligence journal—A chronological log of intelligence activities covering a stated period, usually 24 hours. It is an index of reports and messages that have been received and transmitted, and of important events that have occurred, and actions taken. The journal is a permanent and official record. (JP 1-02)

intelligence operations—The variety of intelligence tasks that are carried out by various intelligence organizations and activities. (Excerpt from JP 1-02)

intelligence preparation of the battlespace—1. An analytical methodology employed to reduce un-certainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, en-vironment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (JP 1-02) 2. In Marine Corps usage, the

systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCRP 5-12C)

intelligence report—A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP. (JP 1-02)

intelligence requirement—1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (JP 1-02) 2. In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called IR. (MCRP 5-12C)

intuitive decisionmaking—The act of reaching a conclusion which emphasizes pattern recognition based on knowledge, judgment, experience, education, intelligence, boldness, perception, and character. This approach focuses on assessment of the situation vice comparison of multiple options. (MCRP 5-12C)

joint deployable intelligence support system—A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called JDISS. (JP 1-02)

joint force—A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (JP 1-02)

joint intelligence center—The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (JP 1-02)

joint intelligence support element—A subordinate joint force forms a joint intelligence support element as the focus for intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called JISE. (JP 1-02)

joint operations—A general term to describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces. (JP 1- 02)

joint targeting coordination board—A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance and priorities, and preparing and/or refining joint target lists. The board is normally comprised of representatives from the joint force staff, all components, and if required, component subordinate units. (JP 1-02)

joint task force—A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. Also called JTF. (JP 1-02)

Joint Worldwide Intelligence Communications System—The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (JP 1-02)

large-scale map—A map having a scale of 1:75,000 or larger. (JP 1-02)

line of communications—A route, either land, water, and/or air, which connects an operating military force with a base of operations and along which supplies and military forces move. (JP 1-02)

list of targets—A tabulation of confirmed or suspect targets maintained by any echelon for informational and fire support planning purposes. (JP 1-02)

main effort—The designated subordinate unit whose mission at a given point in time is most critical to overall mission success. It is usually weighted with the preponderance of combat power and is directed against a center of gravity through a critical vulnerability. (MCRP 5-12C)

maneuver warfare—A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. (MCRP 5-12C)

mapping, charting, and geodesy—Maps, charts, and other data used for military planning, operations, and training. These products and data support air, land, and sea navigation; weapon system guidance; target positioning; and other military activities. These data are presented in the forms of topographic, planimetric, imaged, or thematic maps and graphics; nautical and aeronautical charts and publications; and, in digital and textual formats, gazetteers, which contain geophysical and geodetic data and coordinate lists. (JP 1-02)

Marine air-ground task force—The Marine Corps principal organization for all missions across the range of military operations, composed of forces task-organized under a single commander capable of responding rapidly to a contingency anywhere in the world. The types of forces in the MAGTF are functionally grouped into four core elements: a command element, an aviation combat element, a ground combat element, and a combat service support element. The four core elements are categories of forces, not formal commands. The basic structure of the Marine air-ground task force never varies, though the number, size, and type of Marine Corps units comprising each of its four elements will always be mission dependent. The flexibility of the organizational structure allows for one or more subordinate MAGTFs, other Service and/or foreign military forces, to be assigned or attached. Also called MAGTF. (Approved for inclusion in next version of MCRP 5-12C)

Marine Corps Planning Process—A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of mission analysis, course of action development, course of action analysis, comparison/decision, orders development, and transition. Also called MCPP. NOTE: Tenets of the MCPP include top down planning, single battle concept, and integrated planning. (MCRP 5-12C)

Marine expeditionary force—The largest Marine air-ground task force and the Marine Corps principal warfighting organization, particularly for larger crises or contingencies. It is task-organized around a permanent command element and normally contains one or more Marine divisions, Marine aircraft wings, and Marine force service support groups. The Marine expeditionary force is capable of missions across the range of military operations, including amphibious assault and sustained operations ashore in any environment. It can operate from a sea base, a land base, or both. It may also contain other Service or foreign military forces assigned or attached to the MAGTF. Also called MEF. (Approved for inclusion in next version of MCRP 5-12C)

Marine expeditionary unit—A Marine air-ground task force that is constructed around an infantry battalion reinforced, a helicopter squadron reinforced, and a task-organized combat service support element. It normally fulfills Marine Corps forward sea-based deployment requirements. The Marine expeditionary unit provides an immediate reaction capability for crisis response and is capable of limited combat operations. It may contain other Service or foreign military forces assigned or attached. Also called MEU. (Approved for inclusion in next version of MCRP 5-12C)

Marine expeditionary unit (special operations capable)—The Marine Corps standard, forward-deployed, sea-based expeditionary organization. The MEU(SOC) is a MEU, augmented with selected personnel and equipment, that is trained and equipped with an enhanced capability to conduct amphibious operations and a variety of specialized missions, of limited scope and duration. These capabilities include specialized demolition, clandestine reconnaissance and surveillance, raids, in-extremis hostage recovery, and enabling operations for follow-on forces. The Marine expeditionary unit (special operations capable) is not a special operations force but, when directed by the National Command Authorities, the combatant commander in chief, and/or other operational commander, may conduct limited special operations in extremis, when other forces are inappropriate or unavailable. It may also contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. Also called MEU (SOC). (Approved for inclusion in next version of MCRP 5-12C)

measurement and signature intelligence—Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. (JP 1-02)

medium-scale map—A map having a scale larger than 1:600,000 and smaller than 1:75,000. (JP 1-02)

meteorological data—Meteorological facts pertaining to the atmosphere, such as wind, temperature, air density, and other phenomena which affect military operations. (JP 1-02)

military operations other than war—Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and occur before, during, and after war. Also called MOOTW. (JP 1-02)

modified combined obstacle overlay—A product used to depict the battlespace's effects on military operations. It is normally based on a product depicting all obstacles to mobility, modified to also depict the following, which are not prescriptive nor inclusive: cross-country mobility classifications (such as RESTRICTED); objectives; avenues of approach and mobility corridors; likely locations of countermobility obstacle systems; likely engagement areas; and key terrain. Also called MCOO. (MCRP 5-12C)

multinational operations—A collective term to describe military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance. (JP 1-02)

multi-spectral imagery—The image of an object obtained simultaneously in a number of discrete spectral bands. (JP 1-02)

munitions effects assessment. Conducted concurrently and interactively with battle damage assessment, the assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and

recommend any required changes to the methodology, tactics, weapon system, munitions, fusing and/or weapon delivery parameters to increase force effectiveness. Munitions effects assessment is primarily the responsibility of operations with required inputs and coordination from the intelligence community. Also called MEA. (Proposed by JP 3-60 for inclusion in JP 1-02.)

named area of interest—A point or area along a particular avenue of approach through which enemy activity is expected to occur. Activity or lack of activity within a named area of interest will help to confirm or deny a particular enemy course of action. Also called NAI. (MCRP 5-12C)

national intelligence support team—A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. Also called NIST. (JP 1-02)

near real time—Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP 1-02)

noncombatant evacuation operations—Operations directed by the Department of State, the Department of Defense, or other appropriate authority whereby noncombatants are evacuated from foreign countries when their lives are endangered by war, civil unrest, or natural disaster to safe havens or to the United States. Also called NEO. (JP 1-02)

no-strike target list—A list designated by a commander containing targets not to be destroyed. Destruction of targets on the list would interfere with or unduly hamper projected friendly military operations, or friendly relations with indigenous personnel or governments. (JP 1-02)

open-source intelligence—Information of potential intelligence value that is available to the general public. (JP 1-02)

operational architecture—A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges. (MCRP 5-12C)

operational control—Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. (JP 1-02)

operations control and analysis center—Main node for the command and control of radio battalion signals intelligence operations and the overall coordination of MAGTF signals intelli-

gence operations. Processes, analyzes, produces, and disseminates signals intelligence-derived information and directs the ground-based electronic warfare activities of the radio battalion. Also called OCAC. (MCRP 5-12C)

operational level of war—The level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics; they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives. (JP 1-02)

order of battle—The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called OOB. (JP 1-02)

paramilitary forces—Forces or groups which are distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission. (JP 1-02)

physical damage assessment—The estimate of the quantitative extent of physical damage (through munitions blast, fragmentation, and/or fire damage effects) to a target resulting from the application of military force. This assessment is based upon observed or interpreted damage. (Proposed by JP 3-60 for inclusion in JP 1-02.)

planned targets—Targets that are known to exist in an operational area and which effects are scheduled in advance or are on-call. Examples range from targets on joint target lists (JTLs) in applicable campaign plans, to targets detected in sufficient time to list in the air tasking order (ATO), mission-type orders, or fire support plans. Planned targets have two subcategories: *scheduled* or *on call.* (Proposed by JP 3-60 for inclusion in JP 1-02.)

priority intelligence requirements—1. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called PIR. (JP 1-02) 2. In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCRP 5-12C)

production—The conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. Production is a process of synthesis—the most important action in developing usable intelligence for the commander. (MCWP 2-1)

production management—Encompasses determining the scope, content, and format of each intelligence product, developing a plan and schedule for the development of each product, assigning priorities among the various production requirements, allocating processing, exploitation, and production resources, and integrating production efforts with intelligence collection and dissemination. (MCRP 5-12C)

reach back—The ability to exploit resources, capabilities, expertise, etc., not physically located in the theater or a joint operations area, when established. (MCRP 5-12C)

reactive target—The method used for targeting targets of opportunity. It is used when time and situation do not allow for targeting; i.e., during deliberate targeting, during an attack, when defending against an attack, or upon discovery of the location of a target such as a

radio jammer, tank, or antiaircraft weapon. (MCRP 5-12C)

reattack recommendation—An assessment, derived from the results of battle damage assessment and munitions effects assessment, providing the commander systematic advice on reattack of targets and further target selection to achieve objectives. The reattack recommendation considers objective achievement, target, and aimpoint selection, attack timing, tactics, weapon system and munitions selection. The reattack recommendation is a combined operations and intelligence function. (Proposed by JP 3-60 for inclusion in JP 1-02.)

request for information—Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures. (JP 1-02)

scheduled targets—Planned targets that are known to exist in an operational area and are located in sufficient time for deliberate planning to meet specific campaign objectives. (Proposed by JP 3-60 for inclusion in JP 1-02.)

scientific and technical intelligence—The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the research and development related thereto, and the production methods employed for their manufacture. (JP 1-02)

SECRET internet protocol router network—Worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called SIPRNET. (JP 1-02)

sensitive compartmented information—All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. Also called SCI. (JP 1-02)

sensitive compartmented information facility—An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. (JP 1-02)

sensor data—Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radars, counterbattery radars, and remote ground sensors. (MCRP 5-12C)

sequel(s)—Major operations that follow the current major operations. Plans for these are based on the possible outcomes (success, stalemate, or defeat) associated with the current operation. (MCRP 5-12C)

signals intelligence—1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. (JP 1-02)

situational awareness—Knowledge and understanding of the current situation which promotes timely, relevant, and accurate assessment of

friendly, enemy, and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. (MCRP 5-12C)

special purpose Marine air-ground task force—A Marine air-ground task force organized, trained and equipped with narrowly focused capabilities. It is designed to accomplish a specific mission, often of limited scope and duration. It may be any size, but normally it is a relatively small force--the size of a Marine expeditionary unit or smaller. It may contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. Also called SPMAGTF. (Approved for inclusion in next version of MCRP 5-12C)

staff cognizance—The broad responsibility and authority over designated staff functions assigned to a general or executive staff officer (or their subordinate staff officers) in his area of primary interest. These responsibilities and authorities can range from coordination within the staff to the assignment or delegation to the staff officer by the commander to exercise his authority for a specified warfighting function or sub-function. Staff cognizance includes the responsibility for effective use of available resources and may include the authority for planning the employment of, organizing, assigning tasks, coordinating, and controlling forces for the accomplishment of assigned missions. Marine Corps orders and doctrine provide the notional staff cognizance for general or executive staff officers, which may be modified by the commander to meet his requirements. (Draft MCWP 6-2)

surveillance and reconnaissance cell—Primary element responsible for the supervision of MAGTF intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called SARC. (Change approved for inclusion in next version of MCRP 5-12C)

sustained operations ashore—The employment of Marine Corps forces on land for an extended duration. It can occur with or without sustainment from the sea. Also called SOA. (MCRP 5-12C)

synthesis—In intelligence usage, the examining and combining of processed information with other information and intelligence for final interpretation. (JP 1-02) Note: The piecing of information into a coherent, meaningful picture of the battlespace based on the ongoing or previous analysis of information and events taking place in the area of operations.

tactical intelligence—Intelligence that is required for planning and conducting tactical operations. (JP 1-02) In Marine Corps usage, tactical intelligence is concerned primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather within the battlespace. (MCRP 5-12C)

tactical effect—Result of action(s) at the individual unit, mission, or engagement level. Can be either direct or indirect, and typically acts in concert with other tactical effects to produce results at higher levels of war. (Proposed by JP 3-60 for inclusion in JP 1-02.)

target—A geographical area, complex, or installation planned for capture or destruction by military forces. (JP 1-02)

target analysis—An examination of potential targets to determine military importance, priority of attack, and weapons required to obtain a desired level of damage or casualties. (JP 1-02)

targeted area of interest—The geographical area or point along a mobility corridor where successful interdiction will cause the enemy to either abandon a particular course of action or

require him to use specialized engineer support to continue, where he can be acquired and engaged by friendly forces. Not all targeted areas of interest will form part of the friendly course of action; only targeted areas of interest associated with high-payoff targets are of interest to the staff. These are identified during staff planning and war-gaming. Target areas of interest differ from engagement areas in degree. Engagement areas plan for the use of all available weapons. Targeted areas of interest might be engaged by a single weapon. Also called TAI. (MCRP 5-12C)

target complex—A geographically integrated series of target concentrations. (JP 1-02)

target component—A major element of a target complex or target. It is any machinery, structure, personnel, or other productive asset that contributes to the operation or output of the target complex or target. (JP 1-02)

target concentration—A grouping of geographically proximate targets. (JP 1-02)

target critical damage point—The part of a target component that is most vital. Also called critical node. (JP 1-02)

target dossier—A file of assembled target intelligence about a specific geographic area. (JP 1-02)

target folder—A folder containing target intelligence and related materials prepared for planning and executing action against a specific target. (JP 1-02)

targeting—The process to detect, select, and prioritize targets, match the appropriate action, and assess the resulting effects based on the commander's objective, guidance, and intent. (Proposed by JP 3-60 for inclusion in JP 1-02.)

target intelligence—Intelligence which portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (JP 1-02)

target materials—Graphic, textual, tabular, digital, video, or other presentations of target intelligence, primarily designed to support operations against designated targets by one or more weapon(s) systems. Target materials are suitable for training, planning, executing, and evaluating military operations. (JP 1-02)

target of opportunity—A target visible to a surface or air sensor or observer, which is within range of available weapons and against which fire has not been scheduled or requested. (JP 1-02)

target priority—A grouping of targets with the indicated sequence of attack. (JP 1-02)

target signature—The characteristic pattern of a target displayed by detection and identification equipment. (JP 1-02)

target stress point—The weakest point (most vulnerable to damage) on the critical damage point. Also called vulnerable node. (JP 1-02)

target system—1. All the targets situated in a particular geographic area and functionally related. (DOD) 2. A group of targets which are so related that their destruction will produce some particular effect desired by the attacker. (JP 1-02)

target system assessment—The broad assessment of the overall impact and effectiveness of the full spectrum of military force applied against the operation of an enemy target system or total combat effectiveness (including significant subdivisions of the system) relative to the operational objectives established. (Proposed by JP 3-60 for inclusion in JP 1-02.)

target system component—A set of targets belonging to one or more groups of industries and basic utilities required to produce compo-

nent parts of an end product such as periscopes, or one type of a series of interrelated commodities, such as aviation gasoline. (JP 1-02)

technical control—The performance of specialized or professional service, or the exercise of professional guidance or direction through the establishment of policies and procedures. (Proposed USMC definition per MCWP 6-2 and the next revision of MCRP 5-12C.)

tempo—The relative speed and rhythm of military operations over time. (MCRP 5-12C)

terrain analysis—The collection, analysis, evaluation, and interpretation of geographic information on the natural and manmade features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. (JP 1-02)

terrain study—An analysis and interpretation of natural and manmade features of an area, their effects on military operations, and the effect of weather and climate on these features. (JP 1-02)

time-sensitive targets—Those targets requiring immediate response because they pose (or will soon pose) a clear and present danger to friendly forces or are highly lucrative, fleeting targets of opportunity. (JP 1-02)

validation—A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. (JP 1-02)

vulnerability—1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02)

warfighting functions—The six mutually supporting military activities integrated in the conduct of all military operations are:

1. command and control—The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.

2. maneuver—The movement of forces for the purpose of gaining an advantage over the enemy.

3. fires—Those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight.

4. intelligence—Knowledge about the enemy or the sur-rounding environment needed to support decision-making.

5. logistics—All activities required to move and sustain military forces.

6. force protection—Actions or efforts used to safe-guard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. (MCRP 5-12C)

weaponeering—The process of determining the quantity of a specific type of lethal or nonlethal weapons required to achieve a specific level of damage to a given target, considering target vulnerability, weapon effect, munitions delivery accuracy, damage criteria, probability of kill, and weapon reliability. (JP 1-02)

APPENDIX K. REFERENCES

North Atlantic Treaty Organization Standardization Agreements (STANAGs)

2022	**Intelligence Reports**
2077	**Orders of Battle**
2936	**Intelligence Doctrine-AIntP-1(A)**

Defense Intelligence Management Documents (DIMDs)

0000-151-94	**Department of Defense Intelligence Production Program (DODIPP)**
0000-151C-95	**Department of Defense Intelligence Production Program (DODIPP): Production Procedures**

Defense Intelligence Report

DI-2820-2-99	**Battle Damage Assessment (BDA) Reference Handbook (final draft)**

Joint Publications (JPs)

1-02	**Department of Defense Dictionary of Military and Associated Terms**
2-0	**Doctrine for Intelligence Support to Joint Operations**
2-01	**Joint Intelligence Support to Military Operations**
2-01.3	**Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace**
2-02	**National Intelligence Support to Joint Operations**
2-03	**Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations**
3-02	**Joint Doctrine for Amphibious Operations**
3-02.1	**Joint Doctrine for Landing Force Operations**
3-07	**Joint Doctrine for Military Operations Other Than War**
3-09	**Doctrine for Joint Fire Support**
3-13	**Joint Doctrine for Information Operations**
3-13.1	**Joint Doctrine for Command and Control Warfare**
3-50.3	**Joint Doctrine for Evasion and Recovery**
3-55	**Doctrine for Reconnaissance, Surveillance, and Target Acquisition Support for Joint Operations**
3-60	**Doctrine for Joint Targeting (Draft)**
5-00.2	**Joint Task Force (JTF) Planning Guidance and Procedures**

Marine Corps Intelligence Activity Publications

1586-001-96	MAGTF Contingency Reference Guide
1586-005-99	Urban Generic Information Requirements Handbook

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-2	Campaigning
2	Intelligence
3	Expeditionary Operations
5	Planning
6	Command and Control

Marine Corps Warfighting Publications (MCWPs)

0-1.1	Componency
2-1	Intelligence Operations
2-12.1	Geographic Intelligence
2-14	Counterintelligence
2-15.2	Signals Intelligence
3-2	Aviation Operations
3-16	Fire Support Coordination in the Ground Combat Element
3-35.3	Military Operations on Urbanized Terrain (MOUT)
3-35.7	MAGTF Meteorological and Oceanographic Support
4-1	Logistics Operations
5-1	Marine Corps Planning Process
6-22	Communications and Information Systems

Marine Corps Reference Publications (MCRPs)

5-12C	Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms
5-12D	Organization of Marine Corps Forces

Fleet Marine Force Manual (FMFM)

6	Ground Combat Operations (under revision as MCWP 3-1)

Army Field Manuals (FMs)

34-8-2	Intelligence Officer's Handbook
34-81	Weather Support for Army Tactical Operations
34-81-1	Battlefield Weather Effects
34-130/FMFRP 3-23.2	Intelligence Preparation of the Battlefield (under revision as MCRP 2-12A)
101-5-1/MCRP 5-2A	Operational Terms and Graphics

Directorate of Intelligence

A Compendium of Analytic Tradecraft Notes

Volume I
(Notes 1-10)

Reprinted with a new Foreword by the Deputy Director for Intelligence

February 1997

Directorate of Intelligence

A Compendium of Analytic Tradecraft Notes

Volume I
(Notes 1-10)

Reprinted with a new Foreword by the Deputy Director for Intelligence

February 1997

Reverse Blank

Contents

		Page
Foreword		v
Summary		vii
Note 1	Addressing US Interests in DI Assessments	1
Note 2	Access and Credibility	5
Note 3	Articulation of Assumptions	9
Note 4	Outlook	13
Note 5	Facts and Sourcing	17
Note 6	Analytic Expertise	25
Note 7	Effective Summary	29
Note 8	Implementation Analysis	33
Note 9	Conclusions	37
Note 10	Tradecraft and Counterintelligence	41

A Compendium of Analytic Tradecraft Notes

Foreword by the Deputy Director for Intelligence

The core mission of the CIA's Directorate of Intelligence, which I head, has remained the same despite a decade rocked by profound changes in the world. As the analytical arm of the CIA, we seek to provide the most useful, high-quality analysis to US policymakers, lawmakers, warfighters, law enforcement officers, negotiators, and other officials responsible for protecting US national interests. Our analysis continues to draw from a wide range of sources—from newspapers to the most sensitive technical collection systems.

How we fulfill our mission, however, has changed dramatically. Intelligence analysts are challenged as never before to be creative and proactive in meeting intelligence needs. Long analytic papers largely focused on the Soviet threat worldwide that were the norm 10 years ago have given way to a combination of briefings and short but insightful written and multimedia products covering a broad range of regional and transnational issues.

Now more than ever, new products are tailored to the individual intelligence consumer's concerns. Our analysts put the highest premium on knowing what their consumers need.

The revolution in information technologies has improved our access to sources and our ability to quickly deliver intelligence. But it has also made our work more challenging as we are bombarded with information of varying quality, relevance, and depth.

To meet the challenge of political change and technological advances and take advantage of the opportunities they present, the Directorate of Intelligence has reexamined its core analytic "tradecraft" skills, updating them to reflect how we do our business. The word "tradecraft" comes from our colleagues in the clandestine service, who use it to embody the special skills and methods required to do their business. We have borrowed it to capture our special skills and methods.

We are making the *Compendium of Analytic Tradecraft Notes* available to scholars to shed light on how we support intelligence consumers. This release, although unusual for an intelligence agency, reflects our renewed commitment to reach out to academia and the public, as defined in the Directorate's new Strategic Plan.

Pursuit of expertise in analytic tradecraft is a central element of this plan. Our tradecraft enables analysts to provide "value-added" to consumers of intelligence by ensuring:

- Dedication to objectivity—tough-minded evaluation of information and explicit defense of judgments—which enhances our credibility with consumers dealing with complex and sensitive policy issues.

- Delivery of our products to the right people in time to be useful in their decisionmaking, and using feedback and tasking from them to drive the collection of the basic intelligence that we need to produce our analysis.

Analytic tradecraft skills also serve as "force multipliers," helping us provide top-quality analysis:

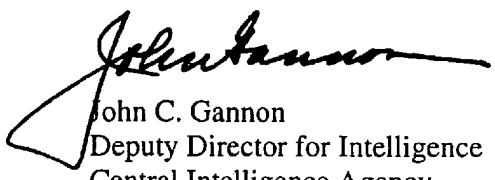
- The feedback our customers give us on our customized analysis clarifies for the analyst what questions most need answering.

- Employing rules for evaluating information and making judgments helps analysts manage the deluge of information, discern trends, and identify attempts at deception.

- Tradecraft standards can be used to iron out differences among experts who have complementary substantive specialties. Their interaction enhances teamwork, which allows the DI to be more productive.

The author of the *Tradecraft Notes* is Jack Davis, a retired CIA officer who has spent 40 years as practitioner, teacher, and critic of intelligence analysis. The *Notes* benefited from the foresight and sharp editorial pen of F. Douglas Whitehouse, Chief of the Directorate's Product Evaluation Staff, during 1994-96. Above all, they reflect the strong commitment to raising analytic standards begun by my predecessor, Douglas E. MacEachin, who served during 1993-95.

Requests for additional copies of *Tradecraft Notes* or copies of the Strategic Plan should be addressed to my Communications Chief, Jon Nowick, on (703) 874-3882. I also welcome your comments on this volume as my colleagues and I work to enhance the way we serve our nation.



John C. Gannon
Deputy Director for Intelligence
Central Intelligence Agency

Summary

Below is a brief characterization of each of the 10 Tradecraft Notes presented in this volume.

Note 1. Addressing US Interests in DI Assessments
PES launched the tradecraft series with a note on the various ways analysts can assure value added for their important clients in the world of policymakers, warfighters, and law enforcement officials:

- One tradecraft tip recommends converting general substantive issues into specific questions that key officials might raise in their preparations to decide on policy action.

- Analysts are encouraged either to organize their assessment around these questions or to make sure in some other way that the operational concerns of policy officials are well covered.

Note 2. Access and Credibility
Demonstrates how the nine evaluation criteria used by PES work together to enhance access to and credibility with the US officials who count most on the analyst's substantive agenda:

- The first challenge is to convince key consumers that the DI assessment is targeted to their concerns. Thus, the importance, for example, of *Addressing US Interests*, providing an *Effective Summary*, and assuring *Effective Use of Unique Intelligence*.

- The second challenge is to maintain credibility in an environment of uncertainty overseas and policy competition in Washington. Thus, the importance of rigorous attention to *Facts and Sourcing* and explicit *Articulation of Assumptions*.

Note 3. Articulation of Assumptions
US officials who must make their policy decisions amidst uncertainty about developments abroad are more likely to rely on DI assessments when the assumptions supporting the analysts' estimative judgments are made clear.

Tradecraft tips cover techniques for:

- Identification, challenge, and defense of *drivers* (key variables) and *linchpins* (assumption about the drivers) before analysts start to draft an assessment.

- Presenting the argumentation in textboxes, for example, when it is not appropriate to belabor the text with details that explicate the critical thinking underlying key judgments.

Note 4. Outlook
The outlook sections of DI assessments must address not only what analysts believe to be the most likely course of developments but also important alternative outcomes that could confront US officials:

- On issues vital to US security such as the military intentions of adversaries, analysts must help policymakers and warfighters engage in contingency planning by addressing alternative courses of developments, including plausible challenges that analysts believe are remote possibilities.

Note 5. Facts and Sourcing
What the analysts know and *how they know it* are central to their credibility not only with policy officials asked to rely on DI assessments for designing and taking action, but also with the managers who are asked to place the Directorate's authority behind the memorandum or briefing.

The two evaluation standards at play here—the handling of facts and of sourcing—were combined in one note that sets out guidelines for analysts and illustrates "best practices" for explicit and tough-minded depiction of information derived from reporting and research. For example:

- Be precise about what is known.

- Distinguish between reported information and analyst judgment.

- Take account of the possibility of deception.

Note 6. Analytic Expertise
Analytic expertise establishes the DI's authority to speak to an issue on which US national security interests are at stake. This note addresses the several facets of analytic expertise and provides tradecraft tips for effectively conveying authority in DI assessments.

The aspects covered include:

- In-depth substantive knowledge that clarifies complex issues.

- Skill in interpreting unique intelligence information.

- Deft organization of data in support of findings and judgments.

- Insight into the decisionmaking processes of US officials.

Note 7. Effective Summary
An effective summary makes the distinctive DI value added stand out for the intended consumers within constricted space limitations. For example:

- When the clients for a DI assessment are few in number and their priority interests regarding the issue at hand are well known, the analyst's job is to craft a summary that presents in a couple of lines of text the *what's new* and the *so what.*

- When an assessment is broadcast to a larger and more diffuse audience, to assure requisite attention, the summary has to convey evidence of the DI's distinctive expertise as well as key findings and judgments.

Note 8. Implementation Analysis
Implementation Analysis is one of the techniques for extending customized intelligence support to policymakers and action takers outlined in Note 1, *Addressing US Interests.* When the DI provides an assessment of tactical alternatives available to the United States for pursuing opportunities and averting dangers, the role of the analyst complements but is distinctive from the role of the policymaker:

Analysts—calling upon their expertise on foreign cultures—identify and evaluate alternatives for implementing objectives.

Policy officials first set the objectives and then make decisions about which tactics to adopt.

Note 9. Conclusions
Analysts must be precise in conveying their level of confidence in the conclusions of a DI assessment; that is, their findings based on organizing, evaluating, and interpreting all-source information:

- When analysts believe they have made their case after a careful scrubbing of ample information, they should state their conclusions boldly (regarding, for example, what has *increased, decreased,* or *taken on a pattern*).

- In contrast, when available information is susceptible to foreign deception operations and other sources of ambiguity, the analysts' reasonable doubts (for example, about *cause-and-effect relationships*) must be shared with the officials who may rely on DI assessments in taking policy action.

Note 10. Tradecraft and Counterintelligence
Guidelines for countering deception efforts to distort analysts' understanding of what is going on abroad build on the advice for rigorous evaluation of information contained in Notes 5 (*Facts and Sourcing*) and 9 (*Conclusions*).

For issues where analysts suspect the presence of deception and for all assessments on which policy officials may directly rely in making decisions on whether to take military or other action to defend US interests, we recommend a structured effort to validate the integrity of key information.

On these *suspect and sensitive issues*, we urge analysts to answer a blunt question:

- *How do you know you are not being deceived?*

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

March 1995

Note 1

Addressing US Interests in DI Assessments

This is the first of a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

The DI professional ethic requires that analysts provide direct support to policymakers' efforts to define and defend US national security interests. The standard is for DI products to convey distinctive value added that promotes feedback, tasking, and access generally. In many cases, this standard requires going beyond general relevance to US interests to customized assistance for identified policy officials who have the "action" on designing, implementing, or monitoring US policy on an individual issue.

The ultimate judges of the utility of DI products for the policymaking process are the officials who choose whether or not to rely on them. The opportunities for adding distinctive intelligence values are usually clear to DI analysts when policy officials ask for a study, memorandum, or briefing. These officials indicate what they expect to gain from their request: for example, specialized information, research findings, cause-and-effect analysis; cost-benefit assessment of tactical alternatives.

The challenge to address effectively US interests is greater when the initiative for launching a DI product comes largely from the intelligence side of the relationship. It is here that Agency monitors (such as the staffs of the congressional oversight committees) are most likely to raise questions about the policymaking utility of individual DI products.

How to proceed? Each analytic assignment represents a distinctive opportunity for providing support to policy officials and the policymaking process. That said, veteran analysts and managers have garnered from direct experience and feedback from policy officials that DI products are usually best directed to meet the needs of the user when they are either organized around or specifically highlight one or more of the following values:

- Opportunities and dangers for US interests, especially unexpected developments that may require a US reaction.
- Motives, objectives, strengths, and vulnerabilities of adversaries, allies, and other actors.
- Direct and indirect sources of US leverage on foreign players and issues.
- Tactical alternatives for advancing stated US policy goals.

Veteran analysts and managers also recommend the following *Tradecraft Tips* for increasing the utility of DI assessments for policymakers.

Getting Started

- *Think of the analyst's role as that of the objective or tough-minded expert for a policymaking team.* Much of the time, hands-on policy officials know the "story" or general pattern of events overseas regarding their priority accounts. What they need most from the intelligence analyst is organized information, including specialized intelligence, that clarifies the goals and motives as well as the strengths and weaknesses of adversaries, allies, and other foreign players.
- *Recognize that research and reporting are inputs or means to an end.* The output is customized support to help policy officials get their jobs done—usually planning for, taking, or monitoring an action. The goal is to convert substantive expertise into action-support analysis before conveying it to consumers.
- *Put a face as well as a name on the five to 10 policy officials who are the core customers on a country or functional account.* Analysts should study what these officials have written or said on important substantive issues and debrief policy staffers who work for core consumers, as well as anyone on the intelligence side of the river who knows their professional habits. The goal is to learn how key officials absorb information and reach judgments, as well as their current priority interests.

- *Target the policymakers' specific interest in a substantive issue.* To identify lines of analysis that provide value added, analysts should think through what they would want to know *if they were policymakers charged with leveraging an issue.* That done, in drafting an assessment or outlining a briefing, the analysts bring to bear the DI's collective substantive expertise, distinctive collection resources, and rigorous analytic tradecraft.

- *Be aware that consumers' needs may change as the policymaking process evolves.* Policy officials often are receptive to broad analytic treatments when an issue first emerges and they are in their long-range planning or goal-setting phase. But once the lines of US policy are set, their focus shifts to specifics about vulnerabilities, leverage, and other facets of policy implementation.

Special Tradecraft Challenges

- *Support the policymaking process without engaging in policymaking per se.* The "if, then" approach can facilitate close policy support without crossing the line to policy prescription. *If* the US policy goal is to get from A to B, *then* the analysts' research findings, all-source collection, and general expertise indicate the following opportunities for moving forward and dangers to be avoided.

- *Long-shot threats and opportunities.* Policy officials often have a strong interest in low-probability, high-impact dangers and objectives. DI analysis in support of policymaking in these circumstances should provide expert, tough-minded assessments that concentrate, not on *whether* an event is likely, but on *how* and *why* it might come about, including the leverage the United States has for constricting dangers and enhancing opportunities.

- *Pointing is not choosing.* Policy-support analysis at times requires the analyst to identify and clarify the vulnerabilities of adversaries and the sources of US leverage over allies and third parties as well as enemies. The responsibility and risk of choosing what actions to take remains with the policymaker.

- *The timeliness challenge.* When policy officials are engaged in managing day-to-day crises, they will use whatever information is available to them when a decision point comes. Rarely will they wait for intelligence analysis. To provide utility, intelligence updates and other analytic support must be delivered in time to meet decision and action deadlines.

Drafting and Self Review

- *Convert issues into questions.* One way to assure utility for policymakers is to organize an analytic effort around the known or presumed questions of key officials on the account. Whenever appropriate, use the questions as section headings, or otherwise make sure that the sections address the identified operational concerns of hands-on policy officials.

- *Use the "so-what" test.* In reviewing a first draft, analysts should evaluate the sections of the paper from the intended customers' point of view and ask—*so what?* Does the draft address specifically and effectively what key policymakers need to know to get *their* jobs done?

- *Or use the "action-support" test.* As an alternative test of the policy utility of a draft, analysts can list the five or so matters they personally would like to see clarified if they were directly responsible for managing US policy action. Next to each entry, list the paragraphs of the draft that provide *actionable* information or insight. Adjust the draft if key identified concerns are not addressed or if too many of the paragraphs are not directly related to specific concerns.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

April 1995

Note 2

Access and Credibility

This is the second in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

The goal of enhancing the policy utility and analytic quality of DI papers and briefings is centered on efforts to promote analysts' access to and credibility with the US officials who count most in policymaking, warfighting, and law enforcement:

- The quest for access—and with it guidance, tasking, and feedback—is driven by the DI's determination to produce analysis for people, not publications.

- Commitment to credibility reflects the core professional value of presenting objective analysis to officials who often have a range of conflicting information and views on complex issues.

The two standards are complementary. Without credibility, analysts will lose their access to the hands-on policy and operational officials who need sound and reliable intelligence analysis to succeed in their professional missions. Without access, even unquestionably objective assessments do little to promote the effective use of intelligence by consumers.

As indicated below, the nine standards the Product Evaluation Staff uses to evaluate DI analytic performance reflect the importance of increasing access and protecting credibility:

- The first challenge for analysts is to make clear to key officials *what's in it for them* when asked to commit their most precious commodity—their time—to read or listen to a DI assessment. Thus, the need for analysts to address US interests effectively, provide value added via substantive expertise and special information, and summarize key points efficiently.

- The second challenge is to help key officials succeed in promoting US objectives by producing assessments that can be relied on for sound treatment of evidence, inference, and judgment.

Increasing Access

Addressing US Interests. The most important and demanding charge given to DI analysts is to assist US officials to fulfill their obligation to design, implement, and monitor national security policy. The highest standard is to structure DI assessments to underscore what officials need to know to get their jobs done (for example, about vulnerabilities and strengths of adversaries). When this is not practical, DI deliverables should contain a carefully crafted section that addresses implications, dangers, and opportunities with the role of US policymakers, warfighters, and law enforcement officials as *action officers* clearly in mind.

Sophistication of the Analysis/Depth of Research. Especially in broadly distributed and fully developed assessments, analysts have to convey their distinctive expertise on an issue. This demonstration of authority to speak to the issue should be based on some combination of research methodology, firsthand knowledge of country or subject, all-source data bases, closeness to collectors, and clear articulation of facts and assumptions—attributes that make a busy policymaker want to come back to the analyst for additional information and analysis.

Unique Intelligence Information. Especially in quick turnaround deliverables for small numbers of key officials, the analyst should make appropriate use of unique, at times highly classified, information that provides insights not otherwise available to well-informed officials. Policymakers and warfighters who have the action on key issues almost always have the clearances as well. At times they need assistance, however, in understanding the context and character of intelligence from clandestine collection and other special sources.

Effective Summary. The analyst's charge is to convey the distinctive values of the paper in the prescribed space. To maximize service to heavily engaged officials, the most important findings and judgments should be highlighted within a bare-bones depiction of the general context. Even more than in the main text, the summary should be made "actionable" via emphasis on US policy implications.

Maintaining Credibility

The Facts—Or What We Know. With emphasis on what is new, different, attention-worthy, a DI assessment should set out what the Directorate knows with sufficient confidence to warrant reliance by policymakers and warfighters in planning and executing US courses of action. When relevant, DI deliverables should also address what analysts do not know that could have significant consequences for the issue under consideration. If the paper notes intelligence gaps, it should, when appropriate, suggest collection strategies to fill the gaps.

Sources of the Facts—How We Know It. DI assessments have to depict the sources of information on which consumers are asked to rely within the general rules for using evidence. Direct evidence (for example, imagery and most intercepts) should be distinguished from testimonial evidence (for example, most clandestine and embassy reporting). On complex matters (for example, the attitudes and plans of foreign leaders) analysts should make explicit their levels of confidence in the evidence.

Conclusions. Assessments should enunciate the conclusory findings from the hard evidence (for example, well-documented events) in terms of trends, patterns, and precedents that underscore dangers or opportunities for US policymakers, warfighters, and law enforcement officials. When appropriate, the calculus that leads to the extension of the factual base to an actionable finding should be spelled out (for example, rules used to establish degrees of risk in dual-purpose technological transfers).

Clear Articulation of Assumptions. When analysts address uncertainty—matters that require interpretations and estimates that go well beyond the hard evidence—their argumentation must clarify the premises, suppositions, and other elements of critical thinking that underlie the judgments. For example, effective argumentation for consumers, who will often have their own strong opinions, requires the analyst to clarify not only degree of confidence in key assumptions but also the criticality of the latter to bottom-line judgments.

Outlook. The outlook sections of estimative assessments (for example, the likely course and impact of political, economic, and military developments in foreign countries) should identify the dynamics that will have the greatest impact on subsequent developments. In other words, what are the drivers that will determine the outcome, or what drivers would have to change to alter the outcome?

- The analyst's judgment on the most likely outcomes must follow clearly from the marshaling of evidence and articulation of assumptions.

- When the US stake is high and plausible alternative outcomes are judged to be in the range of, say, 20 percent or greater, outlook sections should also identify the factors at play that could lead to unexpected developments, signposts of change, and events that could trigger a major shift in direction (for example, assassination of a leader).

- On issues vital to US security (for example, military intentions of adversaries), analysts must help policymakers and warfighters engage in contingency planning by (1) addressing all factors at play that could influence subsequent events, (2) ranking their relative importance, and (3) relating them to a range of plausible outcomes, including alternatives analysts deem to be remote possibilities.

Reverse Blank

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

May 1995

Note 3

Articulation of Assumptions

This is the third in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

DI analysts are regularly tasked to assist policymakers, warfighters, and law enforcement officers in *managing the uncertainty* that complicates US efforts to deal with national security threats and opportunities. Many issues cannot be addressed with certainty—by analysts, by policy officials, or even by the foreign players involved. The pattern of political and economic developments in, say, a newly democratic country can depend on so many actors, institutional variables, and contingencies that the outlook cannot be predicted with high confidence. Estimating over an extended timeline or during a period of political or economic crisis increases the burden of uncertainty.

As a rule, the greater the degree of uncertainty attending an issue:

- The greater the analysts' reliance on judgment rather than evidence; thus the greater the likelihood of estimative error.
- The larger the prospect for divergent views about the outlook among analysts and concerned policy officials.
- The greater the need for sound reasoning and precise argumentation to align facts, assumptions, and judgments.

This tradecraft note on *Articulation of Assumptions* and the next note on *Outlook* will address the DI tradecraft for argumentation that sets the standard for helping consumers deal effectively with the uncertainty they face in planning for, taking, and monitoring US action.

By "argumentation" we mean the communication in an intelligence assessment of the structure of the analysts' critical thinking in support of the bottom-line judgments. Under the DI tradecraft standard, when policymakers, warfighters, and law enforcement officials are asked to rely on DI analysis, the reasoning that ties evidence, to assumption, to judgments must be:

- *Logical*—soundly reasoned.

- *Precise*—clearly stated.

- *Realistic*—attuned to the hazards of forecasting error.

Drivers and Linchpins

The DI tradecraft for the articulation of assumptions places emphasis on identifying the *drivers* or key variables—the uncertain factors that analysts judge most likely to determine the outcome of a complex situation. At times the economy is the key uncertain factor; at times the loyalty of the security forces; at times the leadership skills of a president or dictator. At times all three are judged to carry equal weight in driving future developments.

The analysts' working assumptions about the drivers are sometimes referred to as *linchpin assumptions* because these are the premises that hold the argument together and warrant the validity of the conclusion.

The following are hypothetical examples to illustrate the relationships of drivers, linchpin assumptions, and conclusions:

- The loyalty of the military is the key factor in determining Egyptian stability in the short term. The military probably will continue supporting the government. Therefore, the government is unlikely to be seriously threatened by opposition forces over the next year.

- Castro's skill in handling recurring antiregime incidents will largely determine the Cuban regime's staying power over the next several months. He probably will continue to diffuse antiregime pressures with a mix of carrots and sticks. Thus, a serious threat to regime stability is unlikely.

Linchpin assumptions are by definition debatable and subject to error. Thus, analysts must defend their judgments by marshaling supporting evidence and reasoning. For instance, in the Egyptian example, the analysts should offer convincing evidence for the assumption that "the military probably will continue supporting the government."

Moreover, on an important issue such as this, the inherent uncertainty has to be accounted for by addressing plausible alternative courses of development, a topic that will be covered in the Tradecraft Note on "Outlook." Here we present recommendations for refining and articulating the assumptions that support the analysts' bottom-line conclusions.

Tradecraft Tips

1. Each assessment represents a distinctive challenge in terms of how to set out the argumentation. As a rule of thumb, the more complex and controversial the issue, the more the analysts should make clear the sinews of the reasoning:

- For some papers, the assumptions can be adequately articulated in the course of the text.
- For others, a textbox may be needed to clarify the causal relationships.
- At times, the entire assessment should be organized to march step-by-step through the critical thinking.

2. Before starting to draft an assessment, analysts should open up the search for drivers, and not rely solely on what was determined to be the key factors in the last exercise. That is, they should put aside their previous conclusions and focus initially on the range and alignment of assumptions:

- For example, generate a list of all the important variables—factors that cannot be known with certainty that are palpably affecting the issue under study.
- Assess the relationships among these variables—search for hierarchies of importance and other linkages.
- At times, with the help of colleagues acting as *devil's advocates*, construct competing cases for selecting the drivers from among the host of variables.
- A useful question to ask to isolate the key variables is: *What factors would have to change to change your mind about the expected outcome?*

3. Also, analysts should open up the process of determining assumptions about the drivers:

- Before settling on the linchpin assumptions that will serve to underwrite the conclusions, assess the quality of the evidence. One test: How likely is new information to change your judgment of what is probable?
- Again with the help of colleagues, test the soundness of the supporting line of reasoning (the articulation of subordinate assumptions) that leads to the linchpin assumptions:

  —In the Egyptian example, the subordinate assumptions to the linchpin assumption that the military probably will continue to support the government could include judgments about the military's stake in secular government and antagonism toward the Islamic extremists.

- Also test key assumptions against any contrary judgments held by other informed observers. What hard evidence and inferential reasoning, for example, lead them to alternative interpretations?

4. Analysts should review their first draft against a tough standard:

- Could a consumer who was not reading all the traffic quickly identify and summarize the essential elements of the assessment's reasoning?

5. Some specific questions analysts should ask about the draft:

- Does the depicted hard evidence adequately explain the linchpin assumptions?

- Do the assumptions in turn adequately defend the bottom-line conclusions?

In Sum

DI analysts can speak with authority on substantively complex and politically controversial issues only through sound and precise argumentation. The more effectively drivers and assumptions are identified and defended, the greater the credibility of the bottom-line conclusions.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

June 1995

Note 4

Outlook

This is the fourth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

This Note on *Outlook* continues coverage of DI standards for helping policymakers, warfighters, and law enforcers manage uncertainty regarding threats to and opportunities for US security interests. (Please see Note 3, *Articulation of Assumptions.)*

The outlook sections of DI assessments must address not only what analysts believe to be the most likely course of development but also important alternative outcomes that could confront US officials. *This concern for the unlikely or unexpected* reflects an experience-based appreciation of (1) the fallibility of analytic judgment, (2) the special analytic requirements of US officials for addressing long-shot threats and opportunities, and (3) the adversarial character of the policymaking process.

The perils of analytic judgment include:

- Limitations in the evidence and in the analysts' understanding of complex issues that can lead to judgments structured around either the wrong drivers (key variables) or incorrect linchpin assumptions.

- The impact of essentially unpredictable events on sound analytic judgments; for example, changes in political stability caused by assassination of a president or the sudden advent of a charismatic opposition leader.

Policymakers and other consumers who carry the burden of executing US policy often have a different attitude than analysts toward unlikely events.

- Officials who are charged with advancing a long-shot objective may probably see a 20 percent likelihood of success as promising opening odds for arranging a negotiated settlement of a longstanding civil war or diverting an entrenched nuclear weapons program.

- Officials also require an understanding of unlikely developments to prepare contingency plans against low-probability, high-impact dangers (such as protecting Persian Gulf oil suppliers from another Iraqi military attack on Kuwait or an Iranian blockade of the Straits of Hormuz).

Finally, the outlook on important issues can be subject to deep-seated disagreements—among and between analysts, Administration officials, and congressmen—that generate suspicions about the objectivity of DI memoranda and briefings.

- At such times, DI credibility can depend more on explanation of why the outlook—for example, for Cuba after Castro or for Russia after the next election—cannot be predicted with high confidence than in an attempt to trivialize uncertainty by "just making the call."

General Rules

As indicated in previous Tradecraft Notes, each DI assessment represents a distinctive challenge to analysts on how to assure credibility with the consumers who count most in planning and executing US policy. The general rules that follow should weigh heavily as analysts choose the most appropriate approach.

1. In all cases, the analysts' judgment on the most likely outcomes must follow clearly from the marshaling of evidence and articulation of assumptions.

- The more complex and controversial the issue, the more analytic effort is required to ensure that drivers and linchpin assumptions are precisely stated and well defended.

2. When the US stake is high (for example, political stability of an important ally or adversary) and plausible alternative outcomes are judged to be in the range of for instance, 20 percent or greater, the outlook section should also structure these potentially important outcomes. Policymakers and other consumers should get enough understanding of these alternatives to decide whether to review contingency plans, ask for more evidence, or levy additional tasks on analysts.

Analysts should identify:

- *The factors at play that could lead to unexpected developments.* What alternative key variables could *drive* the outcome in a different direction (perhaps the economy, or growing corruption)? Or what plausible reversal of linchpin assumptions about correctly defined drivers could turn things around (perhaps the Egyptian military *will not* remain loyal to the Mubarak government)?

- *Signposts or indicators of change.* What intermediate developments would indicate that events may not be working out as originally expected? For example, such negative signposts for regime stability as the advent of coup plotting or capital flight.

- *Events that could trigger a major shift in direction.* What essentially unpredictable events could precipitate the unexpected outcome? For example, a crop failure, or a mishandled natural disaster, or anti-government demonstrations that get out of control.

3. On issues vital to US security (for example, military intentions of adversaries), analysts must help policymakers and warfighters engage in contingency planning by:

- Addressing all important factors at play that could influence subsequent events.

- Ranking their relative importance.

- Relating them to a range of plausible outcomes, including alternatives analysts deem to be remote possibilities against which policy planners may nonetheless decide to deploy resources.

Tradecraft Tips

1. Analysts should avoid unrealistic precision in citing odds. Weather forecasters may have sufficient data to determine that the chances of rain *are slightly better than even.* Analysts rarely have such luxury in assessing the political or economic outlook.

2. Also avoid phrases that compound unavoidable uncertainty with unnecessary confusion: for example, *real possibility, good chance.*

3. As a rule, use constructions that tie the outcome to the driver and linchpin assumptions, rather than flat predictions.

- *Castro is unlikely to be forced out of office over the next six months unless his security forces mishandle disturbances and trigger prolonged violent riots.*

4. To minimize misinterpretation when making important judgments, combine probabilistic phrases and rough numerical odds.

- *On balance, Castro is unlikely to be forced from office in the next six months (less than a one-in-five chance).*

5. To understand the often intense concern of hands-on policy officials about a 20 percent likelihood of a disastrous turn of events happening on their watch, analysts should consider whether they would voluntarily get on an airplane that had a one-in-five chance of crashing.

6. To deal rigorously with unlikely developments, analysts should switch their focus from *whether* something will happen to *how* it could happen. Some techniques for generating credible alternative scenarios by structuring the available evidence differently:

- *Who and What Counts.* Generate lists of the key individual and group players that can determine the outcome of an issue (for example, whether Egyptian politics will continue to simmer or will explode), and critically examine the factors most likely to determine their behavior (such as institutional loyalties, personal rivalries, family interests).

- *Thinking Backwards.* Start with the assumption that the targeted danger or opportunity has occurred. For example, revolutionary violence undermines the Castro government! Then generate one or more plausible "how-it-could-happen" scenarios, by postulating who would have to do what, when, how, and why.

- *Judgments Discarded.* List assumptions that fell by the wayside in reaching the bottom line. Regarding the judgment that the military will continue supporting the Egyptian government, for example, revisit any available data or supportive reasoning indicating such support may be weakening, for example, among junior officers.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

July 1995

Note 5

Facts and Sourcing

This is the fifth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

> *The present note is longer than those previously published because it addresses two closely related evaluation standards.*

The credibility of DI assessments with key consumers starts with the analyst's skill in organizing and evaluating the information presented in support of policymaking, warfighting, and law enforcement. Estimative judgments are also important, and at times essential for addressing complex and uncertain issues. But extensive feedback makes clear that US officials with hands-on responsibility for planning and executing policy take their first measure of DI analysts in terms of the judgment they exercise in providing actionable and reliable information:

- As a rule, then, the consumer's confidence in the analyst's estimative judgment comes only after he or she has established credentials for expert command over all-source information.

- Thus, while taking account of space limitations, analysts should err on the side of providing more rather than less relevant information.

This tradecraft note, on *Facts and Sourcing,* presents DI guidelines for depiction in memorandums and briefings of what the DI knows—that is, the character and source of its information. The guidelines will be illustrated by hypothetical examples of "best practices" for handling recurring challenges in characterizing information—for example, addressing the reported attitudes and intentions of foreign actors.

Definitions

DI analysts have a good track record in conveying what they know clearly and credibly to consumers of intelligence. What is undertaken here is codification of rules of thumb into general guidelines.

The following definitions are an attempt to promote standardized use of common terms and concepts relating to intelligence information.

Fact: Verified information; something known to exist or to have happened.

Information: The content of reports, research, and analytic reflection on an intelligence issue that helps analysts and their consumers evaluate the likelihood that something is factual and thereby reduces uncertainty.

Direct Information: Information relating to an intelligence issue under scrutiny the *details* of which can, as a rule, be considered factual, because of the nature of the source, the source's direct access to the information, and the concrete and readily verifiable character of the contents. For example:

- Special intelligence quoting what a foreign official said.
- Imagery providing a count of the number of ships at a pier.
- An event observed by a US Embassy officer.

Indirect Information: Information relating to an intelligence issue the details of which may or may not be factual, the doubt reflecting some combination of the source's questionable reliability, the source's lack of direct access, and the complex character of the contents. For example:

- What a third party told a reliable clandestine source a foreign official said.
- The count of ships at a pier as reported in a foreign government document.
- A US Embassy officer's report of an event based on local media accounts.
- Special intelligence citing what a foreign official believes.

Sourcing: Depiction of the manner in which information was obtained, in order to assist in evaluating the likelihood that the content is factual. A single report from a source or collection platform can contain both direct and indirect information.

Data: Organized information that provides context for evaluating the likelihood that a matter

under scrutiny is factual. The information can be either direct (a chronology of events based on observation by US Embassy officers) or indirect (a chronology based on reports provided by a liaison intelligence service.

These terms are illustrated by the following hypothetical example.

We believe country X has begun a major crackdown on the "Extremist Movement," which the government holds responsible for the campaign of terrorism over the past two years.

The Army has been ordered to support the police in cleaning out *Extremist* strongholds (*direct information*), according to special intelligence (*sourcing*). The President of X reportedly is using last week's attack on a shopping center in a working-class neighborhood to justify calling upon the Army to close down the terrorist campaign (*indirect information*), according to a reliable clandestine source (*sourcing*). The progovernment press reports (*sourcing*) the *Extremists* cannot match Army firepower and are taking high casualties (*indirect information*). A US Embassy observer reports (*sourcing*) seeing Army trucks deliver more than 100 prisoners, some badly wounded, to the Central Prison (*direct information*). According to country X police officials (*sourcing*), these were part of the 1,000 *Extremists* rounded up so far in the crackdown (*indirect information*). CIA's "Country X Terrorism Chronology" indicates this is the first time the Army has been used against the *Extremists* since the terrorism campaign began in 1993 (*data*).

Guidelines

Rule 1. Be precise about what is known.

With US interests, and at times lives, on the line, policymakers, warfighters, and law enforcement officials need to be informed precisely *what the all-source analysts know and how they know it*. In making decisions on whether and how to take action, it is important for them to know if the information is direct or indirect, and if and why the analysts have concluded it is factual.

Most key consumers of intelligence have learned to respect the complexity of the national security issues they are charged with managing and the frequent uncertainty about what is taking place and what lies ahead. DI analysts should write to their standard and not to that of the occasional consumer who *wants answers* no matter what the circumstances.

Thus, in the name of reliability, analysts should never exaggerate what is known. They should report any important gaps in information bearing on US decisionmaking and potential courses of action, as well as relevant information that seems to contradict the main flow of information.

Best Practices

- According to special intelligence, President X has canceled his planned trip to country Y. Imagery indicates no signs of the airport security procedures that usually are undertaken for a Presidential flight. The media in both countries, however, continue to report plans for the scheduled peace talks between the two countries.

- We have no direct information on President X's involvement in narcotics trade, despite persistent charges in the media by his political opponents that his reelection campaign is being financed with funds he obtained from his engagement in trafficking.

Analysts should be precise as well in sourcing information. The phrase, *According to the US Embassy*, for example, does not inform the reader whether the information is direct or indirect.

Best Practices

- US Embassy officers observed sparse crowds at several political rallies.

- In the opinion of a US Embassy official, political support for President X has increased in recent weeks.

Rule 2. Distinguish carefully between information and fact.

Analysts may have direct information on what a foreign leader said, for example, and responsibly conclude this as factual. But what that foreign leader believes, intends to do, and will do cannot be known to be true on the basis of a report on what he or she said.

Best Practices

- According to special intelligence, President X is telling confidants he will fire Prime Minister Y next week.

- President X is reported to be ready to fire Prime Minister Y, according to a reliable clandestine source.

Rule 3. Distinguish carefully between information and estimative judgment.

Analysts' estimative judgments, as indicated, are an important element in the process of supporting policymakers, warfighters, and law enforcement officials. As a rule, these judgments cannot rely solely on reported opinions of foreign players or clandestine sources.

They must be amply argued in terms of the entire body of available information and sound inferential reasoning.

Best Practices

- We believe recovery is under way in Country X. CIA's "Country X Economic Database" shows sustained improvement over the past three months in expanding production and exports and in containing inflation. According to a reliable clandestine source, the Finance Minister has stated that the economy has turned the corner toward recovery.

Also, care should be taken to avoid confusion over whether the DI analyst is making an estimative judgment or a source is expressing an opinion. Thus, the following formulation should be avoided: "Country X has turned the corner toward recovery, as indicated by a reliable clandestine source with access to the Finance Minister."

Best Practices

- According to a reliable clandestine source, the Finance Minister has stated that country X has turned the corner toward recovery.

Rule 4. Take account of substantive complexity.

The more complicated an issue (that is, the more inherently difficult it is to be certain on a matter), the greater the informational demands to establish that the matter under consideration is factual. The burden of proof for determining what foreign leaders or groups believe or intend to do, for example, is much greater than that required for determining what they have done or said. Again, analysts may properly make a conditional judgment about what a foreign leader intends to do. (*We believe country X is preparing to invade country Y.)* But only rarely can this be stated as verified or factual information. (*Country X will invade country Y.)*

Best Practices

- We believe country X is preparing to invade country Y. The deployment of military forces of country X along the border of country Y is consistent both with routine annual military exercises and with preparations for an invasion. Special intelligence, however, indicates two key generals have been called back from an important arms purchase mission abroad. A reliable clandestine source reports that two generals who oppose an invasion have been placed under house arrest. US Embassy officers report extensive civil defense drills and the closing of the national airport to civilian flights. According to a CIA database, these actions have not been undertaken in previous military exercises.

The mindsets of foreign leaders—their attitudes, for example—are also extremely difficult to verify, even with direct or firsthand information, and should rarely be stated as factual. When appropriate, mindset can be a subject for the analyst's estimative judgment.

Best Practices

- Multiple reliable clandestine sources report President X is optimistic about economic prospects.

- President X probably is optimistic about economic prospects. Multiple reliable clandestine sources report his recent upbeat statements. Moreover, recently released IMF statistics indicate a marked improvement in exports and worker productivity.

Rule 5. Take account of policy sensitivity.

As with substantively complex matters, the burden of proof is high on matters that are controversial among policymakers or politically sensitive between the administration and Congress. Directly stated, a solid informational base is needed to present as factual (rather than as the analysts' conditional judgment) something that will be seen by key consumers as *bad news.* As a rule, then, on controversial matters analysts should place emphasis on the relevant information, and not on estimative conclusions.

Best Practices

- Six international observers have described the large-scale election irregularities they monitored in country X, according to press reports. Special intelligence indicates progovernment activists introduced hundreds of bogus ballots into the vote count in three outlying districts. The usually cautious press in country X is reporting alleged eyewitness accounts of progovernment activists denying opposition supporters entry into voting places in several precincts. The legitimacy of the election is coming under increasing question on the part of foreign embassies, according to reliable clandestine sources and press reports.

Similarily, when addressing the behavior of a given country regarding treaties and agreements with the United States, DI analysts should place emphasis on reporting rather than interpretation. As a rule in these matters, *analysts monitor* (report relevant information), and *policymakers verify* (decide whether a violation of a treaty or an agreement has taken place).

Best Practices

- The following information relates to the recent behavior of country X regarding its pledge, under the US economic assistance agreement, to cease support of antigovernment guerrilla forces in country Y:

  —The President of country X told the US Ambassador that all official assistance had been terminated, although small-scale shipments of weapons by private groups that sympathize with the guerrillas' cause might still be taking place.

  —According to a reliable clandestine source, a senior assistant to the President of X has ordered the military to hide small shipments of weapons for the guerrillas in trucks engaged in normal cross-border trade.

  —Special intelligence indicates that a military mission from country X is to await further orders before purchasing abroad communications equipment requested by the guerrillas.

Rule 6. Take account of the possibility of deception.

Deception can be defined as the manipulation of information by a foreign government, group, or individual to get US intelligence analysts to reach an erroneous conclusion. Deception often works because it gives busy analysts what they are seeking—seemingly reliable information on which to base a conclusion.

Here is where the strength of the all-source analyst comes into play. One test for detecting and countering deception is to determine whether all the sources and collection platforms that should be reporting on a matter have indeed done so.

Databases, or organized information, also help. *Is the reported or observed information consistent, in all important details, with past patterns? Do intelligence services with an interest in the matter have a record of perpetrating deceptions?*

So does critical thinking. *Is the information consistent with the analysts' best judgments on the subject's interests, capabilities, and methods of operation?*

Best Practices

- President X assured the US Ambassador on Tuesday that all missile sites in his country had been dismantled, but imagery from last week shows no dismantling activity at the 29 missile sites listed in CIA's database.

- We have no direct information to support reports by a clandestine source with access to Colonel X that antigovernment military forces loyal to him are about to undertake a military coup. No other clandestine sources with military contacts are reporting advanced

coup planning or unusual movements of troops. Opposition political groups abroad report that they are unaware of any serious coup activity, according to multiple reliable clandestine sources. The government, therefore, could be running a deception operation involving Colonel X, to smoke out "disloyal" officers.

Rule 7. Use the term "evidence" sparingly.

This tradecraft note uses the term *information* as synonymous with the term *evidence* as it usually is employed in DI assessments. That is, both are used to refer to the content of reports and research that helps reduce the uncertainty surrounding a specific matter.

The US legal system, however, uses *evidence* in a more specialized manner—to refer to matters introduced in a court case and subject to proof and refutation by contending parties. Because the DI is increasingly providing assessments to support law enforcement officials and because even other kinds of assessments can be subpoenaed for possible use in a court case, analysts should avoid using the term *evidence* when *information* serves their purposes just as well. At times, characterization of the information is sufficient to make the analysts' point for the benefit of consumers.

Best Practices

- Information from special intelligence and clandestine reporting indicates that Justice Minister X has been involved in the narcotics trade.
- Special intelligence and clandestine reporting indicate that Justice Minister X has been involved in the narcotics trade.

Special Circumstances

This note has concentrated on general guidelines for depicting the character and source of the DI's information. The DI serves a broad range of audiences with varied needs and entitlements for intelligence support on a multiplicity of substantive issues. Thus, the special character of the subject matter, the delivery vehicle, or the audience can require exceptions to the rules posited above.

For example, either the limited clearances of the recipients of an assessment or a customer's request for an unclassified memorandum can require the analyst *to avoid precision* in depicting information and sources.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

August 1995

Note 6

Analytic Expertise

This is the sixth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

Analytic expertise establishes the DI's authority to speak to an issue on which US national security interests are at stake. Demonstration of expertise in DI assessments is thus needed to gain access to and credibility with the policymakers, warfighters, and law enforcement officials who carry the heaviest burden for US decision and action on national security issues.

As with all evaluation criteria addressed in these tradecraft notes, analysts have to tailor their demonstration of expertise in individual memorandums and briefings to the circumstances of each assignment. These include the degree of substantive complexity, the analytic requirements and timeline of the policymaking process, and whether the DI production unit already has established close ties to its key clients.

As a rule though, no DI product should be delivered without deliberate effort to make it stand out from the formidable competition including other intelligence providers, journalists, scholars, lobbyists, and various additional purveyors of information and judgment:

- Demonstration of in-depth substantive knowledge is usually the most important element in establishing the credentials for a DI product. To a large extent, the Directorate *is* what it knows and can bring to bear to reduce uncertainty on complex issues.

- Analytic expertise is also conveyed by (1) skill in accessing and interpreting clandestine and technically collected information, (2) deft organization of data in support of findings and judgments, (3) dealing effectively with longshot contingencies and with uncertainty generally, and (4) demonstrating insight into the decisionmaking processes of intelligence customers.

How much expertise needs to be demonstrated? Taking space and time limitations into account, the more the better. The DI not only has to stand out regarding the breadth and depth of its analytic expertise, it also has to convince its key customers that it can put this expertise to use for their benefit.

Again, the appropriate means through which to convey expertise varies with each analytic assignment. As a general test, we recommend that analysts read their first draft critically, to answer the following questions *as if they were posed by a policy official deciding whether to rely on the DI to meet the challenges on his or her agenda.*

- Do the analysts show in-depth knowledge of their subject—the history, civil culture, and other general contexts of the issue, as well as the latest reporting?
- Is there evidence that the analysts have "been there" or represent an analytic and operational team with members who have experience-based insights?
- Have the analysts brought to bear all the dimensions or disciplines that define the issue—political, economic, military, S&T?
- Have the analysts brought to bear all-source information and made a special effort to help the busy intelligence user grasp the key patterns revealed by the information?
- Do the timing and format reflect the analysts' sensitivity to the timeline, decision points, and underlying tensions (areas under debate) of the policymaking process?
- Do the analysts have an effective method or structure for arraying information and reducing uncertainty?
- Further on uncertainty, do the analysts help me think through complex challenges by making their key assumptions clear and dealing rigorously with alternative interpretations and outcomes?
- In sum, would I want to rely on DI analysts and pose followup tasking, to deal with the threats to, and opportunities for, US interests on my policy agenda?

Tradecraft Tips

Research papers are natural vehicles for effective display of analytic expertise. DI veterans, over the years, have devised an armory of measures for demonstrating hard-earned individual and collective expertise even in quick turnaround papers and within the space limitations for most DI deliverables. We list below some of these measures:

- *Evidence of previous research.* In a preface, footnote, textbox, or annex, list related finished intelligence on the subject at hand. Be sure to take a Directorate or team approach by citing the works of other production units.

- *Evidence of scholarship.* Often one footnote or textbox that indicates the breadth of the analysts' grasp helps to establish credentials. For example, citing a historical incident with either common or contrasting elements to the issue at hand.

- *Evidence of data bases.* Expertise can be demonstrated by a paragraph or textbox that presents a chronology, a series of quotes over time by a foreign leader, or a schematic representation of trends (terrorist incidents, inflation or economic growth rates, growth in military inventories, S&T milestones).

- *Evidence of ground truth.* At times it takes only a sentence or two to demonstrate special insight into key personalities, groups, and forces at work. Use your own feel for the ground truth or rely on your analytic teammates to work in some experience-based references. Examples could include references to local political humor, to the household commodities on which short supplies would be most likely to cause popular disgruntlement, or to the modus operandi of local intelligence and security forces.

- *Evidence of teamwork.* Put your professional support colleagues to work on your behalf to clarify a key point or to organize and display the information supporting a point—via annotated maps, imagery, and other graphics. Interviews with customers indicate that those who are heavily engaged on an issue particularly appreciate visual aids that help in keeping up with the fire hose of information.

- *Leadership analysis.* US leaders, naturally enough, tend to be interested in foreign leaders, especially their approach to making decisions, negotiating, and dealing with conflict. Addressing these matters in the text, a textbox, or an annex demonstrates both the breadth and depth of the DI's collective expertise.

- *Secrets.* Excessive classification should be avoided in assessments intended for a broad and general audience. But when a DI assessment is intended for the handful of officials fully engaged (and fully cleared) on an issue, contextual explanation of information from clandestine and technical sources conveys a sense of special expertise.

- *Mysteries.* Demonstrating skill in dealing with uncertainty is appreciated by the hands-on policy officials who have to decide which risks to cover. This includes making explicit the assumptions that drive the argumentation and taking account of low-probability, high-impact contingencies. Here, too, the coverage can be set aside in a textbox or annex, if the goal is to keep the main text lean.

- *The only game in town.* Understandably, policy officials believe that policymaking and implementation is the reason why intelligence exists, and not vice versa. Analysts should demonstrate—in a cover note, preface, or footnote, if not in the main text—that they are informed on the policy timeline and the key matters under debate. Indeed, few things call the DI's reputation into question more than an assessment that arrives after a decision has been made or that addresses in a conventional manner issues on which there already is both broad knowledge and consensus among policy officials.

- *Customized support.* When writing for a small number of officials, analysts can demonstrate by the issues they highlight that they know where their consumers are on their learning curve as well as their decision cycle.

Expertise in Support of the Intelligence Consumer

We end with an obvious caution. When the analysts know their clients' specific needs, demonstration of expertise is readily projected as a tool or means for providing value added. With larger assessments prepared for a broader audience, more care has to be taken to avoid excessive display of knowledge—that is, substantive expertise as an end in itself. Here is where investment in knowing the timelines of the policymaking process and the specific dangers and opportunities policy officials are dealing with comes into play.

September 1995

Note 7

Effective Summary

This is the seventh in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

The summary plays a key role in determining the kind of impact a DI report or memorandum will have on the policymaking process. Thus, within the allotted space, the summary has to make the distinctive DI value added stand out—whether consisting of special intelligence with immediate bearing on US security interests, important findings from the sifting of all-source information, or actionable judgments about pending threats and opportunities.

As with other criteria covered in this series of tradecraft notes, analysts have to tailor each summary to the circumstances of the individual assignment. One way or another, though, the analyst has to crystallize the DI expertise presented in the text in a manner that will seize the attention of the intended audience.

When the clients for the assessment are few in number and their priority interests regarding US policy and action agendas are well known to the DI, the analysts' job is to craft a summary that crisply presents the *what's new* and the *so what:*

- For example, in a Special Intelligence Report, the allotted "hook" of a couple of lines of text must be designed to assure the intelligence consumer that his or her time will be well spent in digesting the rest of the report.

When an assessment is broadcast to a larger and more diffuse audience, the analysts' challenge in determining the structure and content of the summary is greater. Usually, the two most important goals are:

- *To highlight the value added of the paper* against the contingency that busy readers will not get into the main text, especially the implications regarding threats to and opportunities for US interests.

- *To support these values with distinctive expertise* in order to motivate the "gatekeepers" to read the text and recommend that their principals survey sections targeted to help them advance their policy and action agendas.

To account for the diversity of the potential audience for broadcast assessments, other introductory sections can be put to use in flagging the full range of value added and DI expertise. In particular, an *introductory textbox*, placed immediately after the summary, can be used to meet the needs of specialized segments of the audience:

- For example, a depiction of the background or general context that would try the patience of the officials already directly engaged on a policy issue can be provided in a textbox to serve the needs of peripherally engaged intelligence consumers.

- Similarly, technical findings needed to meet the threshold of value added for a small, highly specialized portion of the intended audience can be placed in a textbox.

- And when depiction of policy implications on a controversial issue requires more space for balanced presentation than a summary can accommodate (for example, cost-benefit analysis of alternative courses of action), a textbox is an effective solution.

A *preface* is also a useful instrument, in longer and broadly distributed assessments, for supplementing the summary:

- Use it to explain to peripherally engaged readers the precise policy challenges the assessment seeks to clarify.

- Use it to augment DI credibility; for example, by listing prior publications on the issue at hand.

Tradecraft Tips

DI veterans offer the following experience-based tips for enhancing the effectiveness of summaries:

- *Conform the summary to the text and vice versa.* Often the process of squeezing all the values of the text into a summary paragraph or page sharpens the analyst's depiction of key variables (drivers), cause-and-effect relationships, and argumentation generally. Retrofit any new insights and values into the text.

- *Break up the typography.* Many readers interpret summaries with paragraph blocks that run solidly from margin to margin as a signal that the memorandum or report is "user unfriendly":

  —Use short paragraphs, bullets and subbullets, **bold face**, and *italics* to break up the space and to help the busy decisionmaker latch on quickly to the key information, relationships, and judgments.

- *Fit the writing style to audience and purpose.* When writing for a broad audience, including many policy officials with whom the production unit has only limited contact, top-quality exposition can help attract the readers' attention to the main text. When working in support of a single consumer, however, consider using a more informal style to speed his or her grasp of the value added:

  —One official reported that he did not have time for "whole sentences"—just for what it was the analyst wanted him to know.

- *Concentrate on the new and important.* Historical background and other setting of the context can be presented tersely or dispensed with altogether. Use the allotted space to concentrate on content that will make a difference to well-informed policymakers, warfighters, and law enforcement officers as they contend with their daily challenges:

  —This usually means policy implications. In effect, the summary is a vehicle for explaining why a busy policy official should spend time on a DI product.

  —Strive to make the summary *actionable*; that is, structure it to help a policy official get something started, stopped, or otherwise sorted out.

- *Role-play key members of the targeted audience.* Regarding what belongs in and what can be omitted from the summary: If you were a time-challenged policy official, what would you want to gain from spending five minutes or so with your assessment?

- *Make fewer points, but make them well.* If you have to choose between the quantity and quality of the points made in the summary, opt for the latter. This is particularly important when writing for a well-informed audience which has no need for a "tutorial" on the issue:

  —If the assessment makes a bottom-line predictive judgment, refer to the key assumptions and other essential elements of the argumentation.

  —If the assessment conveys important new findings, cover the reliability of the sourcing and the essence of the methodology.

Reverse Blank

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

October 1995

Note 8

Implementation Analysis

This is the eighth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

This note discusses *Implementation Analysis*, one of the techniques for extending customized intelligence support to policymakers, law enforcement officials, and warfighters outlined in Note 1, *Addressing US Interests in DI Assessments.*

Implementation Analysis provides decisionmakers and action takers with an assessment of tactical alternatives for pursuing opportunities and averting dangers regarding established US policy goals. The role of the analyst complements but is distinctive from the role of the policymaker:

> *Analysts identify and evaluate alternatives for implementing objectives; policy officials first set the objective and then make the decisions about which tactics to adopt.*

Illustrative hypothetical cases of Implementation Analysis include:

- Identifying the major supply routes available to a military adversary and evaluating their logistic importance and vulnerability to US attack.
- Identifying the money-laundering techniques used by a major drug trafficker and evaluating their vulnerability to disruption and curtailment.
- Identifying and evaluating the economic vulnerabilities that could be exploited to leverage a foreign government to terminate development of a nuclear weapons capability.
- Identifying diplomatic, political, and economic initiatives that could be taken to shore up an unstable government the United States wishes to keep in office.
- Identifying and evaluating confidence-building measures either to draw military adversaries into negotiations or to restart stalled talks.

Why and When

Policy implementation regularly involves attempting to advance US interests under uncertain and often risky conditions. In these circumstances, policy officials recognize that US objectives can be difficult to achieve. Deterring rogue states from developing weapons of mass destruction and promoting democratic practice in polities with entrenched authoritarian traditions, for example, require overcoming deeply imbedded obstacles. Policy officials need support from intelligence analysts in identifying and assessing opportunities and dangers.

Intelligence analysts, through Implementation Analysis, can bring important value added to the policymakers' table:

- Expertise in understanding foreign cultures, including the risk analysis and negotiating styles of adversaries and allies.

- Findings on strengths and vulnerabilities of target countries and organizations, based on evaluation of all-source information.

- Detachment from departmental bureaucratic pressures and a commitment to objectivity in examining tactical alternatives.

Even when the analysts' inventory of alternatives largely mirrors that of policy officials, the latter benefit from exposure to the organized information and rigorous argumentation of the former.

In addition to its intrinsic value added, Implementation Analysis can also help the DI maintain effective policy ties on politically charged issues. When pursuit of US goals entails coping with multiple difficult challenges, heavily engaged policy officials do not appreciate a steady stream of DI assessments that reminds them (as well as congressional critics, for example) that they are working against long odds. Implementation Analysis sends the message that the intelligence team, although professionally committed to objectivity, is not indifferent to the challenges the policy team faces and will lend its expertise to help advance and protect US interests even under difficult circumstances.

In any case, analysts should place a premium on close lines of communication in delivering Implementation Analysis:

- As a rule, policy officials should *request* such customized support.

- Intelligence managers who are well connected to the officials doing the heavy lifting can, at times, advertise the capability and solicit a request.

The initial DI delivery of Implementation Analysis usually consists of a briefing or memorandum for one or a handful of principal policy officials. In recognition of the value added, the latter have in the past subsequently asked for:

- Regularly scheduled repeat briefings or memorandums.
- An increase in the circle of recipients.
- Incorporation of the analysis into policy planning documents.

Tradecraft Tips

Veteran analysts offer the following tradecraft tips for putting Implementation Analysis into practice:

- Redefining an intelligence issue in the policymakers' terms can be a useful first step for providing value added through Implementation Analysis. In other words, analysts shift focus from their normal quest for understanding *what's going on in country X* to the policymakers' quest for *doing something about what's going on in country X.* This requires:

  —Recognition of the policymakers' role as "action officers"—charged with getting things started or stopped among adversaries and allies overseas.

  —Recognition of the policy officials' propensity at times to take risk for gain. For example, policymakers may see a one-in-five chance of turning an unsatisfactory situation around as a sound investment of US prestige and their professional energies.

- Analysts also gain insight for adding value by concentrating on what it takes to achieve the operational goal (*think like a policy professional)* before turning to an objective survey of the ground truth (*execute like an intelligence professional*):

  —For example, if the objective of US policy is to leverage a foreign government or organization to reverse its course, analysts can first think of what developments could lead to that outcome and then make an inventory of the forces at play that could trigger such developments.

- The *If, Then* structure often can be used to relate US tactics to US goals, while reserving the DI's tough-minded analytic posture toward both—that is, without crossing the line between professional analytic support of the policymaking process and poliey prescription. For example:

  —*If* US policy calls for getting from point A to point B, *then* here are some gateways to consider and some cul-de-sacs to avoid.

  —*If* the US policy objective is to strengthen the forces for moderation in country X, *then* the following factors should be examined as potential catalysts for the desired development.

- Implementation Analysis often requires *divergent thinking*—the setting aside of attention to mainstream interpretations and the most likely outcome and focusing instead on the full range of plausible alternative interpretations and outcomes. Analytic techniques such as brainstorming, role playing, and "thinking backward" (examining the paths by which a low-probability event could occur) can help identify little-known forces at play that could effect a change in momentum:

  —When analysts are pessimistic about prospects for advancing US objectives, they can employ a variation of the Sherlock Holmes methodology for moving forward when there is no promising suspect in a murder case. *Provide policymakers with an assessment of the least unpromising tactical alternatives.*

  —DI analysts, in effect, are the scouts that provide information and insights to help the policymaker-coach develop the most sensible game plan, win or lose.

- In addition to knowledge of the ground truth, the value added of Implementation Analysis can depend on analysts' knowledge of US instruments for leveraging a situation (that is, the available *carrots and sticks*). Analysts are well advised to make an inventory of US means for executing foreign policy based on the study of policy documents and discussions with intelligence managers and contacts in policy agencies.

- The final step for Implementation Analysis is presentation of the results of the analytic process in ways that make it clear that professional analysts have been at work. Often the responsible policy officials will be more interested in *how analysts reached their evaluations of alternatives* than in the evaluations per se:

  —Presentation and ranking of alternatives via a matrix containing a rough cost-benefit analysis is a useful way to convey the analysts' underlying all-source findings and linchpin assumptions. At the same time, such a matrix focuses the DI effort on *analyzing alternatives*, while leaving the actual choosing to the policymakers.

- Because Implementation Analysis calls on distinctive and challenging tradecraft techniques, analysts should engage colleagues and managers early on in the process of defining the issue and selecting promising tactical alternatives to assess. This team approach will help tap into corporate expertise, as well as smooth the coordination and review processes.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

December 1995

Note 9

Conclusions

This is the ninth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

Conclusions—the analysts' findings based on organizing, evaluating, and interpreting the all-source information available on the issue at hand usually are the most important value added for key consumers of DI assessments. Because policymakers and action takers rely on DI assessments as they define and defend US interests, analysts must be precise in conveying the level of confidence in their conclusions, taking appropriate account of the prospect of deception and other sources of uncertainty.

Heavily engaged policy officials often receive directly much of the open-source and intelligence information available to DI analysts. But the policy officials need DI assistance in keeping track of the facts, fictions, and trivia. The important event has to be identified from among the ordinary, the underlying patterns have to be cobbled together from seemingly unrelated pieces of information, and the reliable sources have to be distinguished from the self-serving.

On complex national security issues the information available to the analysts rarely speaks for itself. Gaps and inconsistencies are the rule. This is where the DI analysts' expertise comes into play. When seasoned and skeptical DI analysts believe they have made their case by a careful scrubbing of ample all-source information, they should lean forward in making their conclusions precise and clear to the policy officials responsible for management of the issue. Analysts who have organized and evaluated their information are able to *conclude* with authority, for example:

- The latest information shows country "X's" expenditures on weapons-related technology *increased sharply* in 1995 after several years of little or no growth.

- DI data demonstrate that incidents of human rights violations in country "Y," as reported by international monitors and reliable clandestine sources, are *decreasing for the first time* since the military government took power in 1989.

- The DI database shows that terrorist incidents in country "Z" *are taking on a pattern* of attempting to intimidate the foreign business community.

- Examination of DI chronologies of the seven national elections since the restoration of civilian government in country "A" indicates that recent government use of armed thugs to break up opposition political rallies *is without precedent.*

- The *cause-and-effect relationship* between Premier "B's" political difficulties and his calling for military exercises to turn public attention to the "foreign threat" is by now well established.

DI assessments are particularly valuable to policy officials when the analytic findings are derived from the collective databases of a multidisciplinary team. Depiction of the political context for a foreign country's lax policy on narcotics controls, for example, or its financial and technological potential for pursuing a nuclear weapons program enables users of DI analysis to take a better measure of the potential risks and benefits of contemplated US policy initiatives.

In contrast, when available information is incomplete or susceptible to foreign deception operations and other sources of ambiguity, the analysts' reasonable doubts about, say, cause-and-effect relationships should be shared with the officials who may rely on DI assessments in taking policy actions.

Many of the issues that the DI tackles are inherently complex and thus shrouded by uncertainties. The analysts have a professional obligation—where warranted—to conclude that *they do not know*. In such instances, presentation of two or more plausible interpretations of the available information makes a more useful conclusion than a single unreliable one masked in vague language (for example, *a real possibility*).

Analysts should be particularly wary about projecting thin information as a DI conclusion. When, for example, analysts do not have a solid informational base and are relying on a small number of reports depicting an event as unprecedented or a pattern as well-established, they should attribute such conclusions to the source. Clandestine agents, foreign officials, and the local media may jump to conclusions. DI analysts should not.

In sum, the value added to policymakers, negotiators, warfighters, and law enforcement officials of conclusions in DI memorandums and briefings rests on:

- The solidity of the individual and collective DI expertise brought to bear through analysis of databases and other information.

- The precision analysts use in stating levels of confidence in their findings.

Tradecraft Tips

DI veterans offer the following recommendations for conveying conclusions effectively:

1. When analysts have reached firm conclusions on complex and especially controversial issues, take the time to present the data, to point to the relationships and other implications, and to state the conclusions forcefully. For example:

- The latest technically collected information, when combined with previous all-source reporting, indicates that country "X" has the means to conduct a weapons test within months, if not weeks.

2. Again, when an issue is complex and controversial, describe the credentials that lie behind the findings—in a textbox or footnote, if not in the main text. For example: depict the reliability of the sources of the information and other specific characteristics of a database; spell out the indicators used to determine diversion to military use of dual-purpose technology imports.

3. To minimize confusion when conveying a necessarily qualified conclusion, think of supplementing adverbial descriptors with a statement of rough numerical odds:

- On the basis of the well-documented effectiveness of "X's" intelligence service in penetrating previous plots and the poor security exhibited by the present conspirators, the President almost certainly knows about the impending coup attempt (roughly a 90-percent likelihood).

4. When the quality of available information requires either reserving judgment about conclusions or presenting multiple plausible interpretations, consider including a textbox or annex on information gaps and collection requirements.

5. When the text must be kept brief because of space limitations of a DI art form, the findings can be laid out in some detail in a textbox. This coverage can be useful both for those consumers who need a quick study into the issue and those with direct responsibility for decision and action who have an interest in taking precise account of what the DI knows.

6. Also use a textbox to explain any major shift in a DI conclusion from previous assessments or the basis for a contrasting conclusion held by other Intelligence Community analysts.

7. When appropriate, use chronologies, matrices, and other graphics to supplement the text in conveying complex trends and relationships. Even the best informed policy officials appreciate graphics that help them evaluate important information.

8. Conclusions are the bedrock foundation for estimative judgments in DI assessments that address future patterns of development. In papers that are divided between sections that set out the findings and those that make predictive judgments, analysts may find it useful to summarize the findings in a textbox immediately preceding the estimative portion. This helps clarify the argument for the critical reader. It can also help analysts audit their own logic trail.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

December 1995

Note 10

Tradecraft and Counterintelligence

This is the 10th in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting standards into practice.

This tradecraft note addresses the aspect of counterintelligence (CI) on which the DI is most directly responsible for improved Agency performance: *Countering deception operations by foreign governments and organizations aimed at distorting the conclusions and judgments of analysts' assessments.*

A subsequent note will address related CI aspects on which DI substantive expertise and analytic skill can make important contributions, including (1) countering espionage by helping to identify the US secrets foreign intelligence services are most interested in obtaining and (2) analytic support of efforts to manipulate foreign intelligence operations to US advantage.

Deception is here defined as all efforts by a foreign intelligence service or adversarial group to distort and otherwise manipulate the perceptions of analysts in order to place analysts and their policy clients at a disadvantage in understanding and dealing with the perpetrating country or group. Deception operations can be divided into two closely related subsets:

- *Denial*—measures taken to protect secrets through concealment, camouflage, and other activities that degrade collection systems, including the information analysts receive from open sources, diplomatic channels, clandestine assets, and technical collection.

- *Disinformation*—operations to feed analysts false or partly false information through the use of double agents and manipulation of diplomatic and media as well as intelligence channels.

Countering Deception

For DI analysts, the first step in improving CI performance is to show increased respect for the deceiver's ability to manipulate perceptions and judgments by compromising collection systems and planting disinformation. Next, analysts must adjust the balance between *speed* and *care* in producing DI assessments. There is no "free lunch" here. The analysts' major

defense for countering deception—exercising increased care in evaluating information and in testing working assumptions—places pressures on the DI commitment to timeliness in servicing consumer demand for tailored products.

The key to holding down the opportunity costs of countering deception is to tie the effort as closely as possible to the normal processes analysts use to expand expertise and to ensure quality and policy utility in their memorandums and briefings:

- As analysts become more accomplished in countering deception they also become better qualified to provide value added to decisionmakers and action takers who need customized support based on *reliable* all-source information.

Warning Signs

Through an investment in understanding the warning signs that a deception operation may be under way, analysts become more expert about their subjects as well as about when and how to apply their main weapons for protecting the integrity of DI assessments:

- Skepticism about the reliability of *all information*, whether from human or technical collection, whether open source or classified, and no matter what the level of classification.

- Readiness to challenge and test even well-established assumptions about trends, patterns, and cause-and-effect relationships.

The first set of warning signs addresses the likelihood that a country or organization is engaged in an attempt to distort the analysts' perceptions:

1. ***Means***. The country or entity (for example, terrorist group) being assessed has the experience and means to undertake sophisticated deception operations. Nearly all countries and entities given priority attention under PDD 35 have well-practiced means to deceive, often in third countries as well as at home.

- Becoming more expert on foreign intelligence practices will also provide analysts with greater understanding of the political dynamics of the country or entity under study, especially when intelligence services are a vital part of the power equation.

2. ***Opportunity***. The foreign country or entity is known to have countered the collection systems or platforms on which the DI analyst is particularly dependent. For example, when a target country has knowledge of the periodicity and acuity of technical collection vehicles that pass over an area it wishes to protect, analysts have to be aware that the resultant information may be incomplete if not also deliberately distorted.

Enhanced knowledge of both the reach and the vulnerabilities of collection systems will also help analysts in dealing with the everyday challenges of evaluating incomplete and ambiguous information.

3. ***Motive***. A motive to deceive is believed to be present. Accomplished intelligence services—for example, in Russia, China, or Cuba—have the ability to mount elaborate denial and disinformation operations virtually across the board. Would they see a high payoff from distorting analyst and policymaker perceptions about the issue at hand?

- Knowledge of which secrets an adversary most seeks to protect adds a distinctive perspective to the analysts' understanding of the country's military, political, and economic priorities.

The second set of warning signs focuses on anomalies in the information available to the analyst. Investment in addressing these warning signs reinforces core skills regarding what the analysts know, how they know it, and what they do not know that could affect the outcomes in ways important to policy officials, warfighters, and law enforcement officials. See, for example, Tradecraft Note No. 5, *Facts and Sourcing* (July 1995).

These warning signs include:

4. ***Suspicious gaps in collection***. For example, when information central to the analysts' conclusions and judgments received through one collection channel is not supported to the extent expected from the take of other collection systems. In other words, the analysts are not receiving the range and volume of information they would expect if there was no deliberate tampering with sources and collection platforms.

5. ***Contradictions to carefully researched patterns.*** Does new information undercut the trends and relationships honed through past research? While analysts must be openminded about the possibility of unexpected change, they should examine critically information that signals an inexplicable change, for example, in an adversary's priorities and practices.

6. ***Suspicious confirmations***. For example, when a new stream of information from clandestine sources or technical collection seems to reinforce the rationale for or against a US policy initiative. In these circumstances, receiving the same "story" from more than one DO or diplomatic source does not in itself speak to the authenticity of the information.

Tradecraft Tips

The effort needed to meet the DI standard of ensuring appropriate protection against deception at the lowest net cost to timeliness will vary from case to case. For each assignment, analysts and managers will have to weigh the costs to credibility of being deceived against the opportunity costs of increased care. Below are general schemes for proceeding efficiently against two distinct levels of risk for DI assessments on complex issues.

Regular Issues. We recommend a two-step defense against deception for assessments on which there is no specific reason to suspect deception is at play and on which the primary value added to consumers is a general increase in understanding (as contrasted with tailored support for decision and action):

Step One. Organize the key information by setting it out, for example, on a yellow pad or blackboard, and examine it critically with warning signs of deception in mind. Are all the expected collection systems kicking in? Is the information appropriately consistent? Are the pieces of information on which conclusions and judgments are most heavily based from a *reliable* clandestine source or *uncompromised* collection platform?

- This investment of, say, one hour in questioning the authenticity of sources will occasionally turn up something suspicious. Even when it does not, analysts, as a result of the effort, will be better able to refine and defend their conclusions and judgments.

Step Two. Play Devil's Advocate and develop a hypothetical argument for the case that deception is taking place; that is, a foreign entity *is* attempting to manipulate perceptions through some combination of denial and disinformation. Then determine to what extent the information organized in Step One lends support to the case for the existence of a deception operation. Look for "hits and misses" between the information and the hypothetical case that substantially raise or diminish the likelihood of the presence of an elaborate deception effort.

- This investment of an additional hour or so will also at times raise suspicions that require more deliberate attention. The investment also enhances skill in structuring plausible low-probability, high-impact scenarios, a key to meeting the demands of policy officials for more help in contingency planning.

Suspect and Sensitive Issues. Where there is reason to suspect the presence of deception (based on general warning signs and the exercises outlined above), analysts should undertake a more elaborate defense of the integrity of their assessments. With or without cause for suspicion, an extended defense should also be employed on sensitive issues—those on which the policy officials may directly rely in making decisions on whether to take military, diplomatic, or economic actions to defend US interests.

On suspect and sensitive issues, we recommend that analysts prepare a textbox or annex that addresses the possibility that a deception operation is distorting the assessment's conclusions and estimative judgments. Managers should consider preparation and defense of the textbox

as an essential element of the analyst's effort, even in instances when they determine it is unnecessary to publish it.

The content of the recommended assessment of the integrity of information will vary with circumstances. But at a minimum it should convey that (1) the possibility of the presence of deception has been taken seriously, (2) analytic tests to determine the likelihood of deception have been executed, and (3) any reasonable doubts are forthrightly reported.

Specific questions that analysts can address with profit include:

1. What is known of the ability of the country or group under examination to engage in deception? About incentives to do so?

2. What is known about the reliability and integrity of the sources and collection platforms most heavily depended upon?

3. What can be said about the availability and consistency of information from all relevant sources and platforms?

4. What tradecraft tests were used to evaluate the authenticity of the information relied upon to reach key conclusions?

In sum, such a textbox provides the analysts with an answer to a question likely to be posed with greater frequency by Agency leaders and policy officials in the wake of the Ames case: *How do you know you are not being deceived?*

01-OSS 21 PRIMER Essential Elements of Information Joint Planning, Operations Other Than War and Open Source Intelligence - Link Page

Previous INTELLIGENCE ANALYSIS IN A NEW CENTURY: A CUMUDGEON'S VIEW

Return to Electronic Index Page

Psychology of Intelligence Analysis

by
Richards J. Heuer, Jr.

CENTER *for the* STUDY *of* INTELLIGENCE

Psychology of Intelligence Analysis

by
Richards J. Heuer, Jr.

CENTER *for the* STUDY *of* INTELLIGENCE
Central Intelligence Agency
1999

This book was prepared primarily for the use of US Government officials, and the format, coverage, and content were designed to meet their specific requirements.

Because this book is now out of print, this Portable Document File (PDF) is formatted for two-sided printing to facilitate desktop publishing. It may be used by US Government agencies to make copies for government purposes and by non-governmental organizations to make copies for educational purposes. Because this book may be subject to copyright restriction, copies may not be made for any commercial purpose.

This book will be available at www.odci.gov/csi.

All statements of fact, opinion, or analysis expressed in the main text of this book are those of the author. Similarly, all such statements in the Forward and the Introduction are those of the respective authors of those sections. Such statements of fact, opinion, or analysis do not necessarily reflect the official positions or views of the Central Intelligence Agency or any other component of the US Intelligence Community. Nothing in the contents of this book should be construed as asserting or implying US Government endorsement of factual statements or interpretations.

ISBN 1 929667-00-0

Originally published in 1999.

Psychology of Intelligence Analysis

by Richards J. Heuer, Jr.

Author's Preface vi

Foreword.....ix

Introduction xiii

PART I—OUR MENTAL MACHINERY.....1

Chapter 1: Thinking About Thinking 1

Chapter 2: Perception: Why Can't We See What Is There To Be Seen?.....7

Chapter 3: Memory: How Do We Remember What We Know?.....17

PART II—TOOLS FOR THINKING.....31

Chapter 4: Strategies for Analytical Judgment: Transcending the Limits of Incomplete Information ...31

Chapter 5: Do You Really Need More Information? ...51

Chapter 6: Keeping an Open Mind 65

Chapter 7: Structuring Analytical Problems 85

Chapter 8: Analysis of Competing Hypotheses 95

PART III—COGNITIVE BIASES.....111

Chapter 9: What Are Cognitive Biases?.....111

Chapter 10: Biases in Evaluation of Evidence.....115

Chapter 11: Biases in Perception of Cause and Effect 127

Chapter 12: Biases in Estimating Probabilities 147

Chapter 13: Hindsight Biases in Evaluation of Intelligence Reporting..... 161

PART IV—CONCLUSIONS 173

Chapter 14: Improving Intelligence Analysis..... 173

Author's Preface

This volume pulls together and republishes, with some editing, updating, and additions, articles written during 1978–86 for internal use within the CIA Directorate of Intelligence. Four of the articles also appeared in the Intelligence Community journal *Studies in Intelligence* during that time frame. The information is relatively timeless and still relevant to the never-ending quest for better analysis.

The articles are based on reviewing cognitive psychology literature concerning how people process information to make judgments on incomplete and ambiguous information. I selected the experiments and findings that seem most relevant to intelligence analysis and most in need of communication to intelligence analysts. I then translated the technical reports into language that intelligence analysts can understand and interpreted the relevance of these findings to the problems intelligence analysts face.

The result is a compromise that may not be wholly satisfactory to either research psychologists or intelligence analysts. Cognitive psychologists and decision analysts may complain of oversimplification, while the non-psychologist reader may have to absorb some new terminology. Unfortunately, mental processes are so complex that discussion of them does require some specialized vocabulary. Intelligence analysts who have read and thought seriously about the nature of their craft should have no difficulty with this book. Those who are plowing virgin ground may require serious effort.

I wish to thank all those who contributed comments and suggestions on the draft of this book: Jack Davis (who also wrote the Introduction); four former Directorate of Intelligence (DI) analysts whose names cannot be cited here; my current colleague, Prof. Theodore Sarbin; and my editor at the CIA's Center for the Study of Intelligence, Hank Appelbaum. All made many substantive and editorial suggestions that helped greatly to make this a better book.

—Richards J. Heuer, Jr.

Foreword

By Douglas MacEachin[1]

My first exposure to Dick Heuer's work was about 18 years ago, and I have never forgotten the strong impression it made on me then. That was at about the midpoint in my own career as an intelligence analyst. After another decade and a half of experience, and the opportunity during the last few years to study many historical cases with the benefit of archival materials from the former USSR and Warsaw Pact regimes, reading Heuer's latest presentation has had even more resonance.

I know from first-hand encounters that many CIA officers tend to react skeptically to treatises on analytic epistemology. This is understandable. Too often, such treatises end up prescribing models as answers to the problem. These models seem to have little practical value to intelligence analysis, which takes place not in a seminar but rather in a fast-breaking world of policy. But that is not the main problem Heuer is addressing.

What Heuer examines so clearly and effectively is how the human thought process builds its own models through which we process information. This is not a phenomenon unique to intelligence; as Heuer's research demonstrates, it is part of the natural functioning of the human cognitive process, and it has been demonstrated across a broad range of fields ranging from medicine to stock market analysis.

The process of analysis itself reinforces this natural function of the human brain. Analysis usually involves creating models, even though they may not be labeled as such. We set forth certain understandings and expectations about cause-and-effect relationships and then process and interpret information through these models or filters.

The discussion in Chapter 5 on the limits to the value of additional information deserves special attention, in my view—particularly for an

1. Douglas MacEachin is a former CIA Deputy Director of Intelligence. After 32 years with the Agency, he retired in 1997 and became a Senior Fellow at Harvard University's John F. Kennedy School of Government.

intelligence organization. What it illustrates is that too often, newly acquired information is evaluated and processed through the existing analytic model, rather than being used to reassess the premises of the model itself. The detrimental effects of this natural human tendency stem from the raison d'etre of an organization created to acquire special, critical information available only through covert means, and to produce analysis integrating this special information with the total knowledge base.

I doubt that any veteran intelligence officer will be able to read this book without recalling cases in which the mental processes described by Heuer have had an adverse impact on the quality of analysis. How many times have we encountered situations in which completely plausible premises, based on solid expertise, have been used to construct a logically valid forecast—with virtually unanimous agreement—that turned out to be dead wrong? In how many of these instances have we determined, with hindsight, that the problem was not in the logic but in the fact that one of the premises—however plausible it seemed at the time—was incorrect? In how many of these instances have we been forced to admit that the erroneous premise was not empirically based but rather a conclusion developed from its own model (sometimes called an assumption)? And in how many cases was it determined after the fact that information had been available which should have provided a basis for questioning one or more premises, and that a change of the relevant premise(s) would have changed the analytic model and pointed to a different outcome?

The commonly prescribed remedy for shortcomings in intelligence analysis and estimates—most vociferously after intelligence "failures"—is a major increase in expertise. Heuer's research and the studies he cites pose a serious challenge to that conventional wisdom. The data show that expertise itself is no protection from the common analytic pitfalls that are endemic to the human thought process. This point has been demonstrated in many fields beside intelligence analysis.

A review of notorious intelligence failures demonstrates that the analytic traps caught the experts as much as anybody. Indeed, the data show that when experts fall victim to these traps, the effects can be aggravated by the confidence that attaches to expertise—both in their own view and in the perception of others.

These observations should in no way be construed as a denigration of the value of expertise. On the contrary, my own 30-plus years in the business of intelligence analysis biased me in favor of the view that, end-

less warnings of information overload notwithstanding, there is no such thing as too much information or expertise. And my own observations of CIA analysts sitting at the same table with publicly renowned experts have given me great confidence that attacks on the expertise issue are grossly misplaced. The main difference is that one group gets to promote its reputations in journals, while the other works in a closed environment in which the main readers are members of the intelligence world's most challenging audience—the policymaking community.

The message that comes through in Heuer's presentation is that information and expertise are a necessary but not sufficient means of making intelligence analysis the special product that it needs to be. A comparable effort has to be devoted to the science of analysis. This effort has to start with a clear understanding of the inherent strengths and weaknesses of the primary analytic mechanism—the human mind—and the way it processes information.

I believe there is a significant cultural element in how intelligence analysts define themselves: Are we substantive experts employed by CIA, or are we professional analysts and intelligence officers whose expertise lies in our ability to adapt quickly to diverse issues and problems and analyze them effectively? In the world at large, substantive expertise is far more abundant than expertise on analytic science and the human mental processing of information. *Dick Heuer makes clear that the pitfalls the human mental process sets for analysts cannot be eliminated; they are part of us. What can be done is to train people how to look for and recognize these mental obstacles, and how to develop procedures designed to offset them.*

Given the centrality of analytic science for the intelligence mission, a key question that Heuer's book poses is: Compared with other areas of our business, have we committed a commensurate effort to the study of analytic science as a professional requirement? How do the effort and resource commitments in this area compare to, for example, the effort and commitment to the development of analysts' writing skills?

Heuer's book does not pretend to be the last word on this issue. Hopefully, it will be a stimulant for much more work.

Introduction

Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis

by Jack Davis[2]

I applaud CIA's Center for the Study of Intelligence for making the work of Richards J. Heuer, Jr. on the psychology of intelligence analysis available to a new generation of intelligence practitioners and scholars.

Dick Heuer's ideas on how to improve analysis focus on helping analysts compensate for the human mind's limitations in dealing with complex problems that typically involve ambiguous information, multiple players, and fluid circumstances. Such multi-faceted estimative challenges have proliferated in the turbulent post-Cold War world.

Heuer's message to analysts can be encapsulated by quoting two sentences from Chapter 4 of this book:

> Intelligence analysts should be self-conscious about their reasoning processes. They should think about *how* they make judgments and reach conclusions, not just about the judgments and conclusions themselves.

Heuer's ideas are applicable to any analytical endeavor. In this Introduction, I have concentrated on his impact—and that of other pioneer thinkers in the intelligence analysis field—at CIA, because that is the institution that Heuer and his predecessors, and I myself, know best, having spent the bulk of our intelligence careers there.

2. Jack Davis served with the Directorate of Intelligence (DI), the National Intelligence Council, and the Office of Training during his CIA career. He is now an independent contractor who specializes in developing and teaching analytic tradecraft. Among his publications is *Uncertainty, Surprise, and Warning* (1996).

Leading Contributors to Quality of Analysis

Intelligence analysts, in seeking to make sound judgments, are always under challenge from the complexities of the issues they address and from the demands made on them for timeliness and volume of production. Four Agency individuals over the decades stand out for having made major contributions on how to deal with these challenges to the quality of analysis.

My short list of the people who have had the greatest positive impact on CIA analysis consists of Sherman Kent, Robert Gates, Douglas MacEachin, and Richards Heuer. My selection methodology was simple. I asked myself: Whose insights have influenced me the most during my four decades of practicing, teaching, and writing about analysis?

Sherman Kent

Sherman Kent's pathbreaking contributions to analysis cannot be done justice in a couple of paragraphs, and I refer readers to fuller treatments elsewhere.[3] Here I address his general legacy to the analytical profession.

Kent, a professor of European history at Yale, worked in the Research and Analysis branch of the Office of Strategic Services during World War II. He wrote an influential book, *Strategic Intelligence for American World Power,* while at the National War College in the late 1940s. He served as Vice Chairman and then as Chairman of the DCI's Board of National Estimates from 1950 to 1967.

Kent's greatest contribution to the quality of analysis was to define an honorable place for the analyst—the thoughtful individual "applying the instruments of reason and the scientific method"—in an intelligence world then as now dominated by collectors and operators. In a second (1965) edition of *Strategic Intelligence,* Kent took account of the coming computer age as well as human and technical collectors in proclaiming the centrality of the analyst:

> Whatever the complexities of the puzzles we strive to solve and whatever the sophisticated techniques we may use to collect

3. See, in particular, the editor's unclassified introductory essay and "Tribute" by Harold P. Ford in Donald P. Steury, *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA, Center for the Study of Intelligence, 1994). Hereinafter cited as Steury, *Kent*.

> the pieces and store them, there can never be a time when the thoughtful man can be supplanted as the intelligence device supreme.

More specifically, Kent advocated application of the techniques of "scientific" study of the past to analysis of complex ongoing situations and estimates of likely future events. Just as rigorous "impartial" analysis could cut through the gaps and ambiguities of information on events long past and point to the most probable explanation, he contended, the powers of the critical mind could turn to events that had not yet transpired to determine the most probable developments.[4]

To this end, Kent developed the concept of the analytic pyramid, featuring a wide base of factual information and sides comprised of sound assumptions, which pointed to the most likely future scenario at the apex.[5]

In his proselytizing and in practice, Kent battled against bureaucratic and ideological biases, which he recognized as impediments to sound analysis, and against imprecise estimative terms that he saw as obstacles to conveying clear messages to readers. Although he was aware of what is now called cognitive bias, his writings urge analysts to "make the call" without much discussion of how limitations of the human mind were to be overcome.

Not many Agency analysts read Kent nowadays. But he had a profound impact on earlier generations of analysts and managers, and his work continues to exert an indirect influence among practitioners of the analytic profession.

Robert Gates

Bob Gates served as Deputy Director of Central Intelligence (1986–1989) and as DCI (1991–1993). But his greatest impact on the quality of CIA analysis came during his 1982–1986 stint as Deputy Director for Intelligence (DDI).

4. Sherman Kent, *Writing History*, second edition (1967). The first edition was published in 1941, when Kent was an assistant professor of history at Yale. In the first chapter, "Why History," he presented ideas and recommendations that he later adapted for intelligence analysis.
5. Kent, "Estimates and Influence" (1968), in Steury, *Kent*.

Initially schooled as a political scientist, Gates earned a Ph.D. in Soviet studies at Georgetown while working as an analyst at CIA. As a member of the National Security Council staff during the 1970s, he gained invaluable insight into how policymakers use intelligence analysis. Highly intelligent, exceptionally hard-working, and skilled in the bureaucratic arts, Gates was appointed DDI by DCI William Casey in good part because he was one of the few insiders Casey found who shared the DCI's views on what Casey saw as glaring deficiencies of Agency analysts.[6] Few analysts and managers who heard it have forgotten Gates' blistering criticism of analytic performance in his 1982 "inaugural" speech as DDI.

Most of the public commentary on Gates and Agency analysis concerned charges of politicization levied against him, and his defense against such charges, during Senate hearings for his 1991 confirmation as DCI. The heat of this debate was slow to dissipate among CIA analysts, as reflected in the pages of *Studies in Intelligence,* the Agency journal founded by Sherman Kent in the 1950s.[7]

I know of no written retrospective on Gates' contribution to Agency analysis. My insights into his ideas about analysis came mostly through an arms-length collaboration in setting up and running an Agency training course entitled "Seminar on Intelligence Successes and Failures."[8] During his tenure as DDI, only rarely could you hold a conversation with analysts or managers without picking up additional viewpoints, thoughtful and otherwise, on what Gates was doing to change CIA analysis.

Gates's ideas for overcoming what he saw as insular, flabby, and incoherent argumentation featured the importance of distinguishing between what analysts know and what they believe—that is, to make clear what is "fact" (or reliably reported information) and what is the analyst's opinion (which had to be persuasively supported with evidence). Among his other tenets were the need to seek the views of non-CIA experts, in-

6. Casey, very early in his tenure as DCI (1981-1987), opined to me that the trouble with Agency analysts is that they went from sitting on their rear ends at universities to sitting on their rear ends at CIA, without seeing the real world.

7. "The Gates Hearings: Politicization and Soviet Analysis at CIA", *Studies in Intelligence* (Spring 1994). "Communication to the Editor: The Gates Hearings: A Biased Account," *Studies in Intelligence* (Fall 1994).

8. DCI Casey requested that the Agency's training office provide this seminar so that, at the least, analysts could learn from their own mistakes. DDI Gates carefully reviewed the statement of goals for the seminar, the outline of course units, and the required reading list.

cluding academic specialists and policy officials, and to present alternate future scenarios.

Gates's main impact, though, came from practice—from his direct involvement in implementing his ideas. Using his authority as DDI, he reviewed critically almost all in-depth assessments and current intelligence articles *prior to publication.* With help from his deputy and two rotating assistants from the ranks of rising junior managers, Gates raised the standards for DDI review dramatically—in essence, from "looks good to me" to "show me your evidence."

As the many drafts Gates rejected were sent back to managers who had approved them—accompanied by the DDI's comments about inconsistency, lack of clarity, substantive bias, and poorly supported judgments—the whole chain of review became much more rigorous. Analysts and their managers raised their standards to avoid the pain of DDI rejection. Both career advancement and ego were at stake.

The rapid and sharp increase in attention paid by analysts and managers to the underpinnings for their substantive judgments probably was without precedent in the Agency's history. The longer term benefits of the intensified review process were more limited, however, because insufficient attention was given to clarifying *tradecraft* practices that would promote analytic soundness. More than one participant in the process observed that a lack of guidelines for meeting Gates's standards led to a large amount of "wheel-spinning."

Gates's impact, like Kent's, has to be seen on two planes. On the one hand, little that Gates wrote on the craft of analysis is read these days. But even though his pre-publication review process was discontinued under his successors, an enduring awareness of his standards still gives pause at jumping to conclusions to many managers and analysts who experienced his criticism first-hand.

Douglas MacEachin

Doug MacEachin, DDI from 1993 to 1996, sought to provide an essential ingredient for ensuring implementation of sound analytic standards: *corporate tradecraft* standards for analysts. This new tradecraft was aimed in particular at ensuring that sufficient attention would be paid to cognitive challenges in assessing complex issues.

MacEachin set out his views on Agency analytical faults and correctives in *The Tradecraft of Analysis: Challenge and Change in the CIA.*[9] My commentary on his contributions to sound analysis is also informed by a series of exchanges with him in 1994 and 1995.

MacEachin's university major was economics, but he also showed great interest in philosophy. His Agency career—like Gates'—included an extended assignment to a policymaking office. He came away from this experience with new insights on what constitutes "value-added" intelligence usable by policymakers. Subsequently, as CIA's senior manager on arms control issues, he dealt regularly with a cadre of tough-minded policy officials who let him know in blunt terms what worked as effective policy support and what did not.

By the time MacEachin became DDI in 1993, Gates's policy of DDI front-office pre-publication review of nearly all DI analytical studies had been discontinued. MacEachin took a different approach; he read—mostly on weekends—and reflected on numerous already-published DI analytical papers. He did not like what he found. In his words, roughly a third of the papers meant to assist the policymaking process had no discernible argumentation to bolster the credibility of intelligence judgments, and another third suffered from flawed argumentation. This experience, along with pressures on CIA for better analytic performance in the wake of alleged "intelligence failures" concerning Iraq's invasion of Kuwait, prompted his decision to launch a major new effort to raise analytical standards.[10]

MacEachin advocated an approach to structured argumentation called "linchpin analysis," to which he contributed muscular terms designed to overcome many CIA professionals' distaste for academic nomenclature. The standard academic term "key variables" became *drivers.* "Hypotheses" concerning drivers became *linchpins*—assumptions underlying the argument—and these had to be explicitly spelled out. MacEachin also urged that greater attention be paid to analytical processes for alerting policymakers to changes in circumstances that would increase the likelihood of alternative scenarios.

9. Unclassified paper published in 1994 by the Working Group on Intelligence Reform, which had been created in 1992 by the Consortium for the Study of Intelligence, Washington, DC.
10. Discussion between MacEachin and the author of this Introduction, 1994.

MacEachin thus worked to put in place systematic and transparent standards for determining whether analysts had met their responsibilities for critical thinking. To spread understanding and application of the standards, he mandated creation of workshops on linchpin analysis for managers and production of a series of notes on analytical tradecraft. He also directed that the DI's performance on tradecraft standards be tracked and that recognition be given to exemplary assessments. Perhaps most ambitious, he saw to it that instruction on standards for analysis was incorporated into a new training course, "Tradecraft 2000." Nearly all DI managers and analysts attended this course during 1996–97.

As of this writing (early 1999), the long-term staying power of MacEachin's tradecraft initiatives is not yet clear. But much of what he advocated has endured so far. Many DI analysts use variations on his linchpin concept to produce soundly argued forecasts. In the training realm, "Tradecraft 2000" has been supplanted by a new course that teaches the same concepts to newer analysts. But examples of what MacEachin would label as poorly substantiated analysis are still seen. Clearly, ongoing vigilance is needed to keep such analysis from finding its way into DI products.

Richards Heuer

Dick Heuer was—and is—much less well known within the CIA than Kent, Gates, and MacEachin. He has not received the wide acclaim that Kent enjoyed as the father of professional analysis, and he has lacked the bureaucratic powers that Gates and MacEachin could wield as DDIs. But his impact on the quality of Agency analysis arguably has been at least as important as theirs.

Heuer received a degree in philosophy in 1950 from Williams College, where, he notes, he became fascinated with the fundamental epistemological question, "What is truth and how can we know it?" In 1951, while a graduate student at the University of California's Berkeley campus, he was recruited as part of the CIA's buildup during the Korean War. The recruiter was Richard Helms, OSS veteran and rising player in the Agency's clandestine service. Future DCI Helms, according to Heuer, was looking for candidates for CIA employment among recent graduates of Williams College, his own alma mater. Heuer had an added advantage

as a former editor of the college's newspaper, a position Helms had held some 15 years earlier.[11]

In 1975, after 24 years in the Directorate of Operations, Heuer moved to the DI. His earlier academic interest in how we know the truth was rekindled by two experiences. One was his involvement in the controversial case of Soviet KGB defector Yuriy Nosenko. The other was learning new approaches to social science methodology while earning a Master's degree in international relations at the University of Southern California's European campus.

At the time he retired in 1979, Heuer headed the methodology unit in the DI's political analysis office. He originally prepared most of the chapters in this book as individual articles between 1978 and 1986; many of them were written for the DI after his retirement. He has updated the articles and prepared some new material for inclusion in this book.

Heuer's Central Ideas

Dick Heuer's writings make three fundamental points about the cognitive challenges intelligence analysts face:

- The mind is poorly "wired" to deal effectively with both inherent uncertainty (the natural fog surrounding complex, indeterminate intelligence issues) and induced uncertainty (the man-made fog fabricated by denial and deception operations).

- Even increased awareness of cognitive and other "unmotivated" biases, such as the tendency to see information confirming an already-held judgment more vividly than one sees "disconfirming" information, does little by itself to help analysts deal effectively with uncertainty.

- Tools and techniques that gear the analyst's mind to apply higher levels of critical thinking can substantially improve analysis on complex issues on which information is incomplete, ambiguous, and often deliberately distorted. Key examples of such intellectu-

11. Letter to the author of this Introduction, 1998.

al devices include techniques for structuring information, challenging assumptions, and exploring alternative interpretations.

The following passage from Heuer's 1980 article entitled "Perception: Why Can't We See What Is There to be Seen?" shows that his ideas were similar to or compatible with MacEachin's concepts of linchpin analysis.

> Given the difficulties inherent in the human processing of complex information, a prudent management system should:
>
> - Encourage products that (a) clearly delineate their assumptions and chains of inference and (b) specify the degree and source of the uncertainty involved in the conclusions.
>
> - Emphasize procedures that expose and elaborate alternative points of view—analytic debates, devil's advocates, interdisciplinary brainstorming, competitive analysis, intra-office peer review of production, and elicitation of outside expertise.

Heuer emphasizes both the value and the dangers of *mental models,* or *mind-sets.* In the book's opening chapter, entitled "Thinking About Thinking," he notes that:

> [Analysts] construct their own version of "reality" on the basis of information provided by the senses, but this sensory input is mediated by complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it. What people perceive, how readily they perceive it, and how they process this information after receiving it are all strongly influenced by past experience, education, cultural values, role requirements, and organizational norms, as well as by the specifics of the information received.
>
> This process may be visualized as perceiving the world through a lens or screen that channels and focuses and thereby may distort the images that are seen. To achieve the clearest possible image . . . analysts need more than information . . . They also

> need to understand the lenses through which this information passes. These lenses are known by many terms—mental models, mind-sets, biases, or analytic assumptions.

In essence, Heuer sees reliance on mental models to simplify and interpret reality as an unavoidable conceptual mechanism for intelligence analysts—often useful, but at times hazardous. What is required of analysts, in his view, is a commitment to *challenge, refine, and challenge again* their own working mental models, precisely because these steps are central to sound interpretation of complex and ambiguous issues.

Throughout the book, Heuer is critical of the orthodox prescription of "more and better information" to remedy unsatisfactory analytic performance. He urges that greater attention be paid instead to more intensive exploitation of information already on hand, and that in so doing, analysts continuously challenge and revise their mental models.

Heuer sees *mirror-imaging* as an example of an unavoidable cognitive trap. No matter how much expertise an analyst applies to interpreting the value systems of foreign entities, when the hard evidence runs out the tendency to project the analyst's own mind-set takes over. In Chapter 4, Heuer observes:

> To see the options faced by foreign leaders as these leaders see them, one must understand their values and assumptions and even their misperceptions and misunderstandings. Without such insight, interpreting foreign leaders' decisions or forecasting future decisions is often nothing more than partially informed speculation. Too frequently, foreign behavior appears "irrational" or "not in their own best interest." Such conclusions often indicate analysts have projected American values and conceptual frameworks onto the foreign leaders and societies, rather than understanding the logic of the situation as it appears to them.

Competing Hypotheses

To offset the risks accompanying analysts' inevitable recourse to mirror-imaging, Heuer suggests looking upon analysts' calculations about

foreign beliefs and behavior as hypotheses to be challenged. Alternative hypotheses need to be carefully considered—especially those that cannot be *disproved* on the basis of available information.

Heuer's concept of "Analysis of Competing Hypotheses" (ACH) is among his most important contributions to the development of an intelligence analysis methodology. At the core of ACH is the notion of competition among a series of plausible hypotheses to see which ones survive a gauntlet of testing for compatibility with available information. The surviving hypotheses—those that have not been disproved—are subjected to further testing. ACH, Heuer concedes, will not always yield the right answer. But it can help analysts overcome the cognitive limitations discussed in his book.

Some analysts who use ACH follow Heuer's full eight-step methodology. More often, they employ some elements of ACH—especially the use of available information to challenge the hypotheses that the analyst favors the most.

Denial and Deception

Heuer's path-breaking work on countering denial and deception (D&D) was not included as a separate chapter in this volume. But his brief references here are persuasive.

He notes, for example, that analysts often reject the possibility of deception because they see no evidence of it. He then argues that rejection is not justified under these circumstances. If deception is well planned and properly executed, one should not expect to see evidence of it readily at hand. Rejecting a plausible but unproven hypothesis too early tends to bias the subsequent analysis, because one does not then look for the evidence that might support it. The possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found.

Heuer's Impact

Heuer's influence on analytic tradecraft began with his first articles. CIA officials who set up training courses in the 1980s as part of then-DDI Gates's quest for improved analysis shaped their lesson plans partly on the basis of Heuer's findings. Among these courses were a seminar on intelligence successes and failures and another on intelligence analysis.

The courses influenced scores of DI analysts, many of whom are now in the managerial ranks. The designers and teachers of Tradecraft 2000 clearly were also influenced by Heuer, as reflected in reading selections, case studies, and class exercises.

Heuer's work has remained on reading lists and in lesson plans for DI training courses offered to all new analysts, as well as courses on warning analysis and on countering denial and deception. Senior analysts and managers who have been directly exposed to Heuer's thinking through his articles, or through training courses, continue to pass his insights on to newer analysts.

Recommendations

Heuer's advice to Agency leaders, managers, and analysts is pointed: To ensure sustained improvement in assessing complex issues, analysis must be treated as more than a substantive and organizational process. Attention also must be paid to techniques and tools for coping with the inherent limitations on analysts' mental machinery. He urges that Agency leaders take steps to:

- *Establish an organizational environment* that promotes and rewards the kind of critical thinking he advocates—or example, analysis on difficult issues that considers in depth a series of plausible hypotheses rather than allowing the first credible hypothesis to suffice.

- *Expand funding for research* on the role such mental processes play in shaping analytical judgments. An Agency that relies on sharp cognitive performance by its analysts must stay abreast of studies on how the mind works—i.e., on *how* analysts reach judgments.

- *Foster development of tools* to assist analysts in assessing information. On tough issues, they need help in improving their mental models and in deriving incisive findings from information they already have; they need such help at least as much as they need more information.

I offer some concluding observations and recommendations, rooted in Heuer's findings and taking into account the tough tradeoffs facing intelligence professionals:

- *Commit to a uniform set of tradecraft standards based on the insights in this book.* Leaders need to know if analysts have done their cognitive homework before taking corporate responsibility for their judgments. Although every analytical issue can be seen as one of a kind, I suspect that nearly all such topics fit into about a dozen recurring patterns of challenge based largely on variations in substantive uncertainty and policy sensitivity. Corporate standards need to be established for each such category. And the burden should be put on managers to explain why a given analytical assignment requires deviation from the standards. I am convinced that if tradecraft standards are made uniform and transparent, the time saved by curtailing personalistic review of quick-turnaround analysis (e.g., "It reads better to me this way") could be "re-invested" in doing battle more effectively against cognitive pitfalls. ("Regarding point 3, let's talk about your assumptions.")

- *Pay more honor to "doubt."* Intelligence leaders and policymakers should, in recognition of the cognitive impediments to sound analysis, establish ground rules that enable analysts, after doing their best to clarify an issue, to express doubts more openly. They should be encouraged to list gaps in information and other obstacles to confident judgment. Such conclusions as "We do not know" or "There are several potentially valid ways to assess this issue" should be regarded as badges of sound analysis, not as dereliction of analytic duty.

- *Find a couple of successors to Dick Heuer. Fund their research. Heed their findings.*

PART I—OUR MENTAL MACHINERY

Chapter 1

Thinking About Thinking

Of the diverse problems that impede accurate intelligence analysis, those inherent in human mental processes are surely among the most important and most difficult to deal with. Intelligence analysis is fundamentally a mental process, but understanding this process is hindered by the lack of conscious awareness of the workings of our own minds.

A basic finding of cognitive psychology is that people have no conscious experience of most of what happens in the human mind. Many functions associated with perception, memory, and information processing are conducted prior to and independently of any conscious direction. What appears spontaneously in consciousness is the result of thinking, not the process of thinking.

Weaknesses and biases inherent in human thinking processes can be demonstrated through carefully designed experiments. They can be alleviated by conscious application of tools and techniques that should be in the analytical tradecraft toolkit of all intelligence analysts.

* * * * * * * * * * * * * * * * * * * *

"When we speak of improving the mind we are usually referring to the acquisition of information or knowledge, or to the type of thoughts one should have, and not to the actual functioning of the mind. We spend little time monitoring our own thinking and comparing it with a more sophisticated ideal."[12]

When we speak of improving intelligence analysis, we are usually referring to the quality of writing, types of analytical products, relations between intelligence analysts and intelligence consumers, or organization

12. James L. Adams, *Conceptual Blockbusting: A Guide to Better Ideas* (New York: W.W. Norton, second edition, 1980), p. 3.

of the analytical process. Little attention is devoted to improving how analysts think.

Thinking analytically is a skill like carpentry or driving a car. It can be taught, it can be learned, and it can improve with practice. But like many other skills, such as riding a bike, it is not learned by sitting in a classroom and being told how to do it. Analysts learn by doing. Most people achieve at least a minimally acceptable level of analytical performance with little conscious effort beyond completing their education. With much effort and hard work, however, analysts can achieve a level of excellence beyond what comes naturally.

Regular running enhances endurance but does not improve technique without expert guidance. Similarly, expert guidance may be required to modify long-established analytical habits to achieve an optimal level of analytical excellence. An analytical coaching staff to help young analysts hone their analytical tradecraft would be a valuable supplement to classroom instruction.

One key to successful learning is motivation. Some of CIA's best analysts developed their skills as a consequence of experiencing analytical failure early in their careers. Failure motivated them to be more self-conscious about how they do analysis and to sharpen their thinking process.

This book aims to help intelligence analysts achieve a higher level of performance. It shows how people make judgments based on incomplete and ambiguous information, and it offers simple tools and concepts for improving analytical skills.

Part I identifies some limitations inherent in human mental processes. Part II discusses analytical tradecraft—simple tools and approaches for overcoming these limitations and thinking more systematically. Chapter 8, "Analysis of Competing Hypotheses," is arguably the most important single chapter. Part III presents information about cognitive biases—the technical term for predictable mental errors caused by simplified information processing strategies. A final chapter presents a checklist for analysts and recommendations for how managers of intelligence analysis can help create an environment in which analytical excellence flourishes.

Herbert Simon first advanced the concept of "bounded" or limited rationality.[13] Because of limits in human mental capacity, he argued, the

13. Herbert Simon, *Models of Man*, 1957.

mind cannot cope directly with the complexity of the world. Rather, we construct a simplified mental model of reality and then work with this model. We behave rationally within the confines of our mental model, but this model is not always well adapted to the requirements of the real world. The concept of bounded rationality has come to be recognized widely, though not universally, both as an accurate portrayal of human judgment and choice and as a sensible adjustment to the limitations inherent in how the human mind functions.[14]

Much psychological research on perception, memory, attention span, and reasoning capacity documents the limitations in our "mental machinery" identified by Simon. Many scholars have applied these psychological insights to the study of international political behavior.[15] A similar psychological perspective underlies some writings on intelligence failure and strategic surprise.[16]

This book differs from those works in two respects. It analyzes problems from the perspective of intelligence analysts rather than policymakers. And it documents the impact of mental processes largely through

14. James G. March., "Bounded Rationality, Ambiguity, and the Engineering of Choice," in David E. Bell, Howard Raiffa, and Amos Tversky, eds., *Decision Making: Descriptive, Normative, and Prescriptive Interactions* (Cambridge University Press, 1988).

15. Among the early scholars who wrote on this subject were Joseph De Rivera, *The Psychological Dimension of Foreign Policy* (Columbus, OH: Merrill, 1968), Alexander George and Richard Smoke, *Deterrence in American Foreign Policy* (New York: Columbia University Press, 1974), and Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).

16. Christopher Brady, "Intelligence Failures: Plus Ca Change. . ." Intelligence and National Security, Vol. 8, No. 4 (October 1993). N. Cigar, "Iraq's Strategic Mindset and the Gulf War: Blueprint for Defeat," *The Journal of Strategic Studies*, Vol. 15, No. 1 (March 1992). J. J. Wirtz, *The Tet Offensive: Intelligence Failure in War* (New York, 1991). Ephraim Kam, *Surprise Attack* (Harvard University Press, 1988). Richard Betts, *Surprise Attack: Lessons for Defense Planning* (Brookings, 1982). Abraham Ben-Zvi, "The Study of Surprise Attacks," *British Journal of International Studies*, Vol. 5 (1979). *Iran: Evaluation of Intelligence Performance Prior to November 1978* (Staff Report, Subcommittee on Evaluation, Permanent Select Committee on Intelligence, US House of Representatives, January 1979). Richard Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, Vol. 31, No. 1 (October 1978). Richard W. Shryock, "The Intelligence Community Post-Mortem Program, 1973-1975," *Studies in Intelligence*, Vol. 21, No. 1 (Fall 1977). Avi Schlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," *World Politics*, Vol. 28 (April 1976). Michael Handel, *Perception, Deception, and Surprise: The Case of the Yom Kippur War* (Jerusalem: Leonard Davis Institute of International Relations, Jerusalem Paper No. 19, 1976). Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," *World Politics*, Vol. 16 (1964).

experiments in cognitive psychology rather than through examples from diplomatic and military history.

A central focus of this book is to illuminate the role of the observer in determining what is observed and how it is interpreted. People construct their own version of "reality" on the basis of information provided by the senses, but this sensory input is mediated by complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it. What people perceive, how readily they perceive it, and how they process this information after receiving it are all strongly influenced by past experience, education, cultural values, role requirements, and organizational norms, as well as by the specifics of the information received.

This process may be visualized as perceiving the world through a lens or screen that channels and focuses and thereby may distort the images that are seen. To achieve the clearest possible image of China, for example, analysts need more than information on China. They also need to understand their own lenses through which this information passes. These lenses are known by many terms—mental models, mind-sets, biases, or analytical assumptions.

In this book, the terms mental model and mind-set are used more or less interchangeably, although a mental model is likely to be better developed and articulated than a mind-set. An analytical assumption is one part of a mental model or mind-set. The biases discussed in this book result from how the mind works and are independent of any substantive mental model or mind-set.

Before obtaining a license to practice, psychoanalysts are required to undergo psychoanalysis themselves in order to become more aware of how their own personality interacts with and conditions their observations of others. The practice of psychoanalysis has not been so successful that its procedures should be emulated by the intelligence and foreign policy community. But the analogy highlights an interesting point: Intelligence analysts must understand themselves before they can understand others. Training is needed to (a) increase self-awareness concerning generic problems in how people perceive and make analytical judgments concerning foreign events, and (b) provide guidance and practice in overcoming these problems.

Not enough training is focused in this direction—that is, inward toward the analyst's own thought processes. Training of intelligence ana-

lysts generally means instruction in organizational procedures, methodological techniques, or substantive topics. More training time should be devoted to the mental act of thinking or analyzing. It is simply assumed, incorrectly, that analysts know how to analyze. This book is intended to support training that examines the thinking and reasoning processes involved in intelligence analysis.

As discussed in the next chapter, mind-sets and mental models are inescapable. They are, in essence, a distillation of all that we think we know about a subject. The problem is how to ensure that the mind remains open to alternative interpretations in a rapidly changing world.

The disadvantage of a mind-set is that it can color and control our perception to the extent that an experienced specialist may be among the last to see what is really happening when events take a new and unexpected turn. When faced with a major paradigm shift, analysts who know the most about a subject have the most to unlearn. This seems to have happened before the reunification of Germany, for example. Some German specialists had to be prodded by their more generalist supervisors to accept the significance of the dramatic changes in progress toward reunification of East and West Germany.

The advantage of mind-sets is that they help analysts get the production out on time and keep things going effectively between those watershed events that become chapter headings in the history books.[17]

A generation ago, few intelligence analysts were self-conscious and introspective about the process by which they did analysis. The accepted wisdom was the "common sense" theory of knowledge—that to perceive events accurately it was necessary only to open one's eyes, look at the facts, and purge oneself of all preconceptions and prejudices in order to make an objective judgment.

Today, there is greatly increased understanding that intelligence analysts do not approach their tasks with empty minds. They start with a set of assumptions about how events normally transpire in the area for which they are responsible. Although this changed view is becoming conventional wisdom, the Intelligence Community has only begun to scratch the surface of its implications.

If analysts' understanding of events is greatly influenced by the mind-set or mental model through which they perceive those events,

17. This wording is from a discussion with veteran CIA analyst, author, and teacher Jack Davis.

should there not be more research to explore and document the impact of different mental models?[18]

The reaction of the Intelligence Community to many problems is to collect more information, even though analysts in many cases already have more information than they can digest. What analysts need is more truly useful information—mostly reliable HUMINT from knowledgeable insiders—to help them make good decisions. Or they need a more accurate mental model and better analytical tools to help them sort through, make sense of, and get the most out of the available ambiguous and conflicting information.

Psychological research also offers to intelligence analysts additional insights that are beyond the scope of this book. Problems are not limited to how analysts perceive and process information. Intelligence analysts often work in small groups and always within the context of a large, bureaucratic organization. Problems are inherent in the processes that occur at all three levels—individual, small group, and organization. This book focuses on problems inherent in analysts' mental processes, inasmuch as these are probably the most insidious. Analysts can observe and get a feel for these problems in small-group and organizational processes, but it is very difficult, at best, to be self-conscious about the workings of one's own mind.

18. Graham Allison's work on the Cuban missile crisis (*Essence of Decision*, Little, Brown & Co., 1971) is an example of what I have in mind. Allison identified three alternative assumptions about how governments work--a rational actor model, an organizational process model, and a bureaucratic politics model. He then showed how an analyst's implicit assumptions about the most appropriate model for analyzing a foreign government's behavior can cause him or her to focus on different evidence and arrive at different conclusions. Another example is my own analysis of five alternative paths for making counterintelligence judgments in the controversial case of KGB defector Yuriy Nosenko: Richards J. Heuer, Jr., "Nosenko: Five Paths to Judgment," *Studies in Intelligence*, Vol. 31, No. 3 (Fall 1987), originally classified Secret but declassified and published in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal 1955-1992* (New Haven: Yale University Press, 1995).

Chapter 2

Perception: Why Can't We See What Is There To Be Seen?

The process of perception links people to their environment and is critical to accurate understanding of the world about us. Accurate intelligence analysis obviously requires accurate perception. Yet research into human perception demonstrates that the process is beset by many pitfalls. Moreover, the circumstances under which intelligence analysis is conducted are precisely the circumstances in which accurate perception tends to be most difficult. This chapter discusses perception in general, then applies this information to illuminate some of the difficulties of intelligence analysis.[19]

* * * * * * * * * * * * * * * * * * * *

People tend to think of perception as a passive process. We see, hear, smell, taste or feel stimuli that impinge upon our senses. We think that if we are at all objective, we record what is actually there. Yet perception is demonstrably an active rather than a passive process; it constructs rather than records "reality." Perception implies understanding as well as awareness. It is a process of inference in which people construct their own version of reality on the basis of information provided through the five senses.

As already noted, what people in general and analysts in particular perceive, and how readily they perceive it, are strongly influenced by their past experience, education, cultural values, and role requirements, as well as by the stimuli recorded by their receptor organs.

Many experiments have been conducted to show the extraordinary extent to which the information obtained by an observer depends upon the observer's own assumptions and preconceptions. For example, when

19. An earlier version of this article was published as part of "Cognitive Factors in Deception and Counterdeception," in Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception* (Pergamon Press, 1982).

Figure 1

you looked at Figure 1 above, what did you see? Now refer to the footnote for a description of what is actually there.[20] Did you perceive Figure 1 correctly? If so, you have exceptional powers of observation, were lucky, or have seen the figure before. This simple experiment demonstrates one of the most fundamental principles concerning perception:

We tend to perceive what we expect to perceive.

A corollary of this principle is that it takes more information, and more unambiguous information, to recognize an unexpected phenomenon than an expected one.

One classic experiment to demonstrate the influence of expectations on perception used playing cards, some of which were gimmicked so the spades were red and the hearts black. Pictures of the cards were flashed briefly on a screen and, needless to say, the test subjects identified the normal cards more quickly and accurately than the anomalous ones. After test subjects became aware of the existence of red spades and black hearts, their performance with the gimmicked cards improved but still did not approach the speed or accuracy with which normal cards could be identified.[21]

20. The article is written twice in each of the three phrases. This is commonly overlooked because perception is influenced by our expectations about how these familiar phrases are normally written.

21. Jerome S. Bruner and Leo Postman, "On the Perception of Incongruity: A Paradigm," in Jerome S. Bruner and David Kraut, eds., *Perception and Personality: A Symposium* (New York: Greenwood Press, 1968).

This experiment shows that patterns of expectation become so deeply embedded that they continue to influence perceptions even when people are alerted to and try to take account of the existence of data that do not fit their preconceptions. Trying to be objective does not ensure accurate perception.

The position of the test subject identifying playing cards is analogous to that of the intelligence analyst or government leader trying to make sense of the paper flow that crosses his or her desk. What is actually perceived in that paper flow, as well as how it is interpreted, depends in part, at least, on the analyst's patterns of expectation. Analysts do not just have expectations about the color of hearts and spades. They have a set of assumptions and expectations about the motivations of people and the processes of government in foreign countries. Events consistent with these expectations are perceived and processed easily, while events that contradict prevailing expectations tend to be ignored or distorted in perception. Of course, this distortion is a subconscious or pre-conscious process, as illustrated by how you presumably ignored the extra words in the triangles in Figure 1.

This tendency of people to perceive what they *expect* to perceive is more important than any tendency to perceive what they *want* to perceive. In fact, there may be no real tendency toward wishful thinking. The commonly cited evidence supporting the claim that people tend to perceive what they want to perceive can generally be explained equally well by the expectancy thesis.[22]

Expectations have many diverse sources, including past experience, professional training, and cultural and organizational norms. All these influences predispose analysts to pay particular attention to certain kinds of information and to organize and interpret this information in certain ways. Perception is also influenced by the context in which it occurs. Different circumstances evoke different sets of expectations. People are more attuned to hearing footsteps behind them when walking in an alley at night than along a city street in daytime, and the meaning attributed to the sound of footsteps will vary under these differing circumstances. A military intelligence analyst may be similarly tuned to perceive indicators of potential conflict.

22. For discussion of the ambiguous evidence concerning the impact of desires and fears on judgment, see Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), Chapter 10.

Patterns of expectations tell analysts, subconsciously, what to look for, what is important, and how to interpret what is seen. These patterns form a mind-set that predisposes analysts to think in certain ways. A mind-set is akin to a screen or lens through which one perceives the world.

There is a tendency to think of a mind-set as something bad, to be avoided. According to this line of argument, one should have an open mind and be influenced only by the facts rather than by preconceived notions! That is an unreachable ideal. There is no such thing as "the facts of the case." There is only a very selective subset of the overall mass of data to which one has been subjected that one takes as facts and judges to be relevant to the question at issue.

Actually, mind-sets are neither good nor bad; they are unavoidable. People have no conceivable way of coping with the volume of stimuli that impinge upon their senses, or with the volume and complexity of the data they have to analyze, without some kind of simplifying preconceptions about what to expect, what is important, and what is related to what. "There is a grain of truth in the otherwise pernicious maxim that an open mind is an empty mind."[23] Analysts do not achieve objective analysis by avoiding preconceptions; that would be ignorance or self-delusion. Objectivity is achieved by making basic assumptions and reasoning as explicit as possible so that they can be challenged by others and analysts can, themselves, examine their validity.

One of the most important characteristics of mind-sets is:

Mind-sets tend to be quick to form but resistant to change.

Figure 2 illustrates this principle by showing part of a longer series of progressively modified drawings that change almost imperceptibly from a man into a woman.[24] The right-hand drawing in the top row, when viewed alone, has equal chances of being perceived as a man or a woman. When test subjects are shown the entire series of drawings one by one, their perception of this intermediate drawing is biased according to which end of the series they started from. Test subjects who start by viewing a picture that is clearly a man are biased in favor of continuing

23. Richard Betts, "Analysis, War and Decision: Why Intelligence Failures are Inevitable", *World Politics*, Vol. XXXI (October 1978), p. 84.
24. Drawings devised by Gerald Fisher in 1967.

Figure 2

Impressions resist change.

to see a man long after an "objective observer" (for example, an observer who has seen only a single picture) recognizes that the man is now a woman. Similarly, test subjects who start at the woman end of the series are biased in favor of continuing to see a woman. Once an observer has formed an image—that is, once he or she has developed a mind-set or expectation concerning the phenomenon being observed—this conditions future perceptions of that phenomenon.

This is the basis for another general principle of perception:

New information is assimilated to existing images.

This principle explains why gradual, evolutionary change often goes unnoticed. It also explains the phenomenon that an intelligence analyst assigned to work on a topic or country for the first time may generate accurate insights that have been overlooked by experienced analysts who have worked on the same problem for 10 years. A fresh perspective is sometimes useful; past experience can handicap as well as aid analysis. This tendency to assimilate new data into pre-existing images is greater "the more ambiguous the information, the more confident the actor is of

Figure 3

It is difficult to look at the same information from different perspectives.

the validity of his image, and the greater his commitment to the established view."[25]

The drawing in Figure 3 provides the reader an opportunity to test for him or herself the persistence of established images.[26] Look at Figure 3. What do you see—an old woman or a young woman? Now look again to see if you can visually and mentally reorganize the data to form a different image—that of a young woman if your original perception was of an old woman, or of the old woman if you first perceived the young one. If necessary, look at the footnote for clues to help you identify the other

25. Jervis, p. 195.
26. This picture was originally published in *Puck* magazine in 1915 as a cartoon entitled "My Wife and My Mother-in-Law."

image.[27] Again, this exercise illustrates the principle that mind-sets are quick to form but resistant to change.

When you have seen Figure 3 from *both* perspectives, try shifting back and forth from one perspective to the other. Do you notice some initial difficulty in making this switch? One of the more difficult mental feats is to take a familiar body of data and reorganize it visually or mentally to perceive it from a different perspective. Yet this is what intelligence analysts are constantly required to do. In order to understand international interactions, analysts must understand the situation as it appears to each of the opposing forces, and constantly shift back and forth from one perspective to the other as they try to fathom how each side interprets an ongoing series of interactions. Trying to perceive an adversary's interpretations of international events, as well as US interpretations of those same events, is comparable to seeing both the old and young woman in Figure 3. Once events have been perceived one way, there is a natural resistance to other perspectives.

A related point concerns the impact of substandard conditions of perception. The basic principle is:

> **Initial exposure to blurred or ambiguous stimuli interferes with accurate perception even after more and better information becomes available.**

This effect has been demonstrated experimentally by projecting onto a screen pictures of common, everyday subjects such as a dog standing on grass, a fire hydrant, and an aerial view of a highway cloverleaf intersection.[28] The initial projection was blurred in varying degrees, and the pictures were then brought into focus slowly to determine at what point test subjects could identify them correctly.

This experiment showed two things. First, those who started viewing the pictures when they were most out of focus had more difficulty identifying them when they became clearer than those who started view-

27. The old woman's nose, mouth, and eye are, respectively, the young woman's chin, necklace, and ear. The old woman is seen in profile looking left. The young woman is also looking left, but we see her mainly from behind so most facial features are not visible. Her eyelash, nose, and the curve of her cheek may be seen just above the old woman's nose.
28. Jerome S. Bruner and Mary C. Potter, "Interference in Visual Recognition," *Science*, Vol. 144 (1964), pp. 424-25.

ing at a less blurred stage. In other words, the greater the initial blur, the clearer the picture had to be before people could recognize it. Second, the longer people were exposed to a blurred picture, the clearer the picture had to be before they could recognize it.

What happened in this experiment is what presumably happens in real life; despite ambiguous stimuli, people form some sort of tentative hypothesis about what they see. The longer they are exposed to this blurred image, the greater confidence they develop in this initial and perhaps erroneous impression, so the greater the impact this initial impression has on subsequent perceptions. For a time, as the picture becomes clearer, there is no *obvious* contradiction; the new data are assimilated into the previous image, and the initial interpretation is maintained until the contradiction becomes so obvious that it forces itself upon our consciousness.

The early but incorrect impression tends to persist because the amount of information necessary to invalidate a hypothesis is considerably greater than the amount of information required to make an initial interpretation. The problem is not that there is any inherent difficulty in grasping new perceptions or new ideas, but that established perceptions are so difficult to change. People form impressions on the basis of very little information, but once formed, they do not reject or change them unless they obtain rather solid evidence. Analysts might seek to limit the adverse impact of this tendency by suspending judgment for as long as possible as new information is being received.

Implications for Intelligence Analysis

Comprehending the nature of perception has significant implications for understanding the nature and limitations of intelligence analysis. The circumstances under which accurate perception is most difficult are exactly the circumstances under which intelligence analysis is generally conducted—dealing with highly ambiguous situations on the basis of information that is processed incrementally under pressure for early judgment. This is a recipe for inaccurate perception.

Intelligence seeks to illuminate the unknown. Almost by definition, intelligence analysis deals with highly ambiguous situations. As previously noted, the greater the ambiguity of the stimuli, the greater the impact of expectations and pre-existing images on the perception of that

stimuli. Thus, despite maximum striving for objectivity, the intelligence analyst's own preconceptions are likely to exert a greater impact on the analytical product than in other fields where an analyst is working with less ambiguous and less discordant information.

Moreover, the intelligence analyst is among the first to look at new problems at an early stage when the evidence is very fuzzy indeed. The analyst then follows a problem as additional increments of evidence are received and the picture gradually clarifies—as happened with test subjects in the experiment demonstrating that initial exposure to blurred stimuli interferes with accurate perception even after more and better information becomes available. If the results of this experiment can be generalized to apply to intelligence analysts, the experiment suggests that an analyst who starts observing a potential problem situation at an early and unclear stage is at a disadvantage as compared with others, such as policymakers, whose first exposure may come at a later stage when more and better information is available.

The receipt of information in small increments over time also facilitates assimilation of this information into the analyst's existing views. No one item of information may be sufficient to prompt the analyst to change a previous view. The cumulative message inherent in many pieces of information may be significant but is attenuated when this information is not examined as a whole. The Intelligence Community's review of its performance before the 1973 Arab-Israeli War noted:

> The problem of incremental analysis—especially as it applies to the current intelligence process—was also at work in the period preceding hostilities. Analysts, according to their own accounts, were often proceeding on the basis of the day's take, hastily comparing it with material received the previous day. They then produced in 'assembly line fashion' items which may have reflected perceptive intuition but which [did not] accrue from a systematic consideration of an accumulated body of integrated evidence.[29]

And finally, the intelligence analyst operates in an environment that exerts strong pressures for what psychologists call premature closure.

29. *The Performance of the Intelligence Community Before the Arab-Israeli War of October 1973: A Preliminary Post-Mortem Report,* December 1973. The one-paragraph excerpt from this post-mortem, as quoted in the text above, has been approved for public release, as was the title of the post-mortem, although that document as a whole remains classified.

Customer demand for interpretive analysis is greatest within two or three days after an event occurs. The system requires the intelligence analyst to come up with an almost instant diagnosis before sufficient hard information, and the broader background information that may be needed to gain perspective, become available to make possible a well-grounded judgment. This diagnosis can only be based upon the analyst's preconceptions concerning how and why events normally transpire in a given society.

As time passes and more information is received, a fresh look at all the evidence might suggest a different explanation. Yet, the perception experiments indicate that an early judgment adversely affects the formation of future perceptions. Once an observer thinks he or she knows what is happening, this perception tends to resist change. New data received incrementally can be fit easily into an analyst's previous image. This perceptual bias is reinforced by organizational pressures favoring consistent interpretation; once the analyst is committed in writing, both the analyst and the organization have a vested interest in maintaining the original assessment.

That intelligence analysts perform as well as they do is testimony to their generally sound judgment, training, and dedication in performing a dauntingly difficult task.

The problems outlined here have implications for the management as well as the conduct of analysis. Given the difficulties inherent in the human processing of complex information, a prudent management system should:

- Encourage products that clearly delineate their assumptions and chains of inference and that specify the degree and source of uncertainty involved in the conclusions.
- Support analyses that periodically re-examine key problems from the ground up in order to avoid the pitfalls of the incremental approach.
- Emphasize procedures that expose and elaborate alternative points of view.
- Educate consumers about the limitations as well as the capabilities of intelligence analysis; define a set of realistic expectations as a standard against which to judge analytical performance.

Chapter 3

Memory: How Do We Remember What We Know?

Differences between stronger and weaker analytical performance are attributable in large measure to differences in the organization of data and experience in analysts' long-term memory. The contents of memory form a continuous input into the analytical process, and anything that influences what information is remembered or retrieved from memory also influences the outcome of analysis.

This chapter discusses the capabilities and limitations of several components of the memory system. Sensory information storage and short-term memory are beset by severe limitations of capacity, while long-term memory, for all practical purposes, has a virtually infinite capacity. With long-term memory, the problems concern getting information into it and retrieving information once it is there, not physical limits on the amount of information that may be stored. Understanding how memory works provides insight into several analytical strengths and weaknesses.

* * * * * * * * * * * * * * * * * * * *

Components of the Memory System

What is commonly called memory is not a single, simple function. It is an extraordinarily complex system of diverse components and processes. There are at least three, and very likely more, distinct memory processes. The most important from the standpoint of this discussion and best documented by scientific research are sensory information stor-

age (SIS), short-term memory (STM), and long-term memory (LTM).[30] Each differs with respect to function, the form of information held, the length of time information is retained, and the amount of information-handling capacity. Memory researchers also posit the existence of an interpretive mechanism and an overall memory monitor or control mechanism that guides interaction among various elements of the memory system.

Sensory Information Storage

Sensory information storage holds sensory images for several tenths of a second after they are received by the sensory organs. The functioning of SIS may be observed if you close your eyes, then open and close them again as rapidly as possible. As your eyes close, notice how the visual image is maintained for a fraction of a second before fading. Sensory information storage explains why a movie film shot at 16 separate frames per second appears as continuous movement rather than a series of still pictures. A visual trace is generally retained in SIS for about one-quarter of a second. It is not possible to consciously extend the time that sensory information is held in SIS. The function of SIS is to make it possible for the brain to work on processing a sensory event for longer than the duration of the event itself.

Short-Term Memory

Information passes from SIS into short-term memory, where again it is held for only a short period of time—a few seconds or minutes. Whereas SIS holds the complete image, STM stores only the interpretation of the image. If a sentence is spoken, SIS retains the sounds, while STM holds the words formed by these sounds.

Like SIS, short-term memory holds information temporarily, pending further processing. This processing includes judgments concerning meaning, relevance, and significance, as well as the mental actions necessary to integrate selected portions of the information into long-term

30. Memory researchers do not employ uniform terminology. Sensory information storage is also known as sensory register, sensory store, and eidetic and echoic memory. Short- and long-term memory are also referred to as primary and secondary memory. A variety of other terms are in use as well. I have adopted the terminology used by Peter H. Lindsay and Donald A. Norman in their text on *Human Information Processing* (New York: Academic Press, 1977). This entire chapter draws heavily from Chapters 8 through 11 of the Lindsay and Norman book.

memory. When a person forgets immediately the name of someone to whom he or she has just been introduced, it is because the name was not transferred from short-term to long-term memory.

A central characteristic of STM is the severe limitation on its capacity. A person who is asked to listen to and repeat a series of 10 or 20 names or numbers normally retains only five or six items. Commonly it is the last five or six. If one focuses instead on the first items, STM becomes saturated by this effort, and the person cannot concentrate on and recall the last items. People make a choice where to focus their attention. They can concentrate on remembering or interpreting or taking notes on information received moments ago, or pay attention to information currently being received. Limitations on the capacity of short-term memory often preclude doing both.

Retrieval of information from STM is direct and immediate because the information has never left the conscious mind. Information can be maintained in STM indefinitely by a process of "rehearsal"—repeating it over and over again. But while rehearsing some items to retain them in STM, people cannot simultaneously add new items. The severe limitation on the amount of information retainable in STM at any one time is physiological, and there is no way to overcome it. This is an important point that will be discussed below in connection with working memory and the utility of external memory aids.

Long-Term Memory

Some information retained in STM is processed into long-term memory. This information on past experiences is filed away in the recesses of the mind and must be retrieved before it can be used. In contrast to the immediate recall of current experience from STM, retrieval of information from LTM is indirect and sometimes laborious.

Loss of detail as sensory stimuli are interpreted and passed from SIS into STM and then into LTM is the basis for the phenomenon of selective perception discussed in the previous chapter. It imposes limits on subsequent stages of analysis, inasmuch as the lost data can never be retrieved. People can never take their mind back to what was *actually there* in sensory information storage or short-term memory. They can only retrieve their interpretation of what they *thought* was there as stored in LTM.

There are no practical limits to the amount of information that may be stored in LTM. The limitations of LTM are the difficulty of processing information into it and retrieving information from it. These subjects are discussed below.

The three memory processes comprise the storehouse of information or database that we call memory, but the total memory system must include other features as well. Some mental process must determine what information is passed from SIS into STM and from STM into LTM; decide how to search the LTM data base and judge whether further memory search is likely to be productive; assess the relevance of retrieved information; and evaluate potentially contradictory data.

To explain the operation of the total memory system, psychologists posit the existence of an interpretive mechanism that operates on the data base and a monitor or central control mechanism that guides and oversees the operation of the whole system. Little is known of these mechanisms and how they relate to other mental processes.

Despite much research on memory, little agreement exists on many critical points. What is presented here is probably the lowest common denominator on which most researchers would agree.

Organization of Information in Long-Term Memory. Physically, the brain consists of roughly 10 billion neurons, each analogous to a computer chip capable of storing information. Each neuron has octopus-like arms called axons and dendrites. Electrical impulses flow through these arms and are ferried by neurotransmitting chemicals across what is called the synaptic gap between neurons. Memories are stored as patterns of connections between neurons. When two neurons are activated, the connections or "synapses" between them are strengthened.

As you read this chapter, the experience actually causes physical changes in your brain. "In a matter of seconds, new circuits are formed that can change forever the way you think about the world."[31]

Memory records a lifetime of experience and thoughts. Such a massive data retrieval mechanism, like a library or computer system, must have an organizational structure; otherwise information that enters the system could never be retrieved. Imagine the Library of Congress if there were no indexing system.

31. George Johnson, *In the Palaces of Memory: How We Build the Worlds Inside Our Heads.* Vintage Books, 1992, p. xi.

There has been considerable research on how information is organized and represented in memory, but the findings remain speculative. Current research focuses on which sections of the brain process various types of information. This is determined by testing patients who have suffered brain damage from strokes and trauma or by using functional magnetic resonance imaging (fMRI) that "lights up" the active portion of the brain as a person speaks, reads, writes, or listens.

None of the current theories seems to encompass the full range or complexity of memory processes, which include memory for sights and sounds, for feelings, and for belief systems that integrate information on a large number of concepts. However useful the research has been for other purposes, analysts' needs are best served by a very simple image of the structure of memory.

Imagine memory as a massive, multidimensional spider web. This image captures what is, for the purposes of this book, perhaps the most important property of information stored in memory—its interconnectedness. One thought leads to another. It is possible to start at any one point in memory and follow a perhaps labyrinthine path to reach any other point. Information is retrieved by tracing through the network of interconnections to the place where it is stored.

Retrievability is influenced by the number of locations in which information is stored and the number and strength of pathways from this information to other concepts that might be activated by incoming information. The more frequently a path is followed, the stronger that path becomes and the more readily available the information located along that path. If one has not thought of a subject for some time, it may be difficult to recall details. After thinking our way back into the appropriate context and finding the general location in our memory, the interconnections become more readily available. We begin to remember names, places, and events that had seemed to be forgotten.

Once people have started thinking about a problem one way, the same mental circuits or pathways get activated and strengthened each time they think about it. This facilitates the retrieval of information. These same pathways, however, also become the mental ruts that make it difficult to reorganize the information mentally so as to see it from a different perspective. That explains why, in the previous chapter, once you saw the picture of the old woman it was difficult to see the young

woman, or vice versa. A subsequent chapter will consider ways of breaking out of mental ruts.

One useful concept of memory organization is what some cognitive psychologists call a "schema." A schema is *any pattern of relationships* among data stored in memory. It is any set of nodes and links between them in the spider web of memory that hang together so strongly that they can be retrieved and used more or less as a single unit.

For example, a person may have a schema for a bar that when activated immediately makes available in memory knowledge of the properties of a bar and what distinguishes a bar, say, from a tavern. It brings back memories of specific bars that may in turn stimulate memories of thirst, guilt, or other feelings or circumstances. People also have schemata (plural for schema) for abstract concepts such as a socialist economic system and what distinguishes it from a capitalist or communist system. Schemata for phenomena such as success or failure in making an accurate intelligence estimate will include links to those elements of memory that explain typical causes and implications of success or failure. There must also be schemata for processes that link memories of the various steps involved in long division, regression analysis, or simply making inferences from evidence and writing an intelligence report.

Any given point in memory may be connected to many different overlapping schemata. This system is highly complex and not well understood.

This conception of a schema is so general that it begs many important questions of interest to memory researchers, but it is the best that can be done given the current state of knowledge. It serves the purpose of emphasizing that memory does have structure. It also shows that how knowledge is connected in memory is critically important in determining what information is retrieved in response to any stimulus and how that information is used in reasoning.

Concepts and schemata stored in memory exercise a powerful influence on the formation of perceptions from sensory data. Recall the experiment discussed in the previous chapter in which test subjects were exposed very briefly to playing cards that had been doctored so that some hearts were black and spades red. When retained in SIS for a fraction of a second, the spades were indeed red. In the course of interpreting the sensory impression and transferring it to STM, however, the spades became black because the memory system has no readily available schema for a

red spade to be matched against the sensory impression. If information does not fit into what people know, or think they know, they have great difficulty processing it.

The content of schemata in memory is a principal factor distinguishing stronger from weaker analytical ability. This is aptly illustrated by an experiment with chess players. When chess grandmasters and masters and ordinary chess players were given five to 10 seconds to note the position of 20 to 25 chess pieces placed randomly on a chess board, the masters and ordinary players were alike in being able to remember the places of only about six pieces. If the positions of the pieces were taken from an actual game (unknown to the test subjects), however, the grandmasters and masters were usually able to reproduce almost all the positions without error, while the ordinary players were still able to place correctly only a half-dozen pieces.[32]

That the unique ability of the chess masters did not result from a pure feat of memory is indicated by the masters' inability to perform better than ordinary players in remembering randomly placed positions. Their exceptional performance in remembering positions from actual games stems from their ability to immediately perceive patterns that enable them to process many bits of information together as a single chunk or schema. The chess master has available in long-term memory many schemata that connect individual positions together in coherent patterns. When the position of chess pieces on the board corresponds to a recognized schema, it is very easy for the master to remember not only the positions of the pieces, but the outcomes of previous games in which the pieces were in these positions. Similarly, the unique abilities of the master analyst are attributable to the schemata in long-term memory that enable the analyst to perceive patterns in data that pass undetected by the average observer.

Getting Information Into and Out of Long-Term Memory. It used to be that how well a person learned something was thought to depend upon how long it was kept in short-term memory or the number of times they repeated it to themselves. Research evidence now suggests that neither of these factors plays the critical role. Continuous repetition does not necessarily guarantee that something will be remembered. The key

32. A. D. deGroot, *Thought and Choice in Chess* (The Hague: Mouton, 1965) cited by Herbert A. Simon, "How Big Is a Chunk?" *Science*, Vol. 183 (1974), p. 487.

factor in transferring information from short-term to long-term memory is the development of associations between the new information and schemata already available in memory. This, in turn, depends upon two variables: the extent to which the information to be learned relates to an already existing schema, and the level of processing given to the new information.

Take one minute to try to memorize the following items from a shopping list: bread, eggs, butter, salami, corn, lettuce, soap, jelly, chicken, and coffee. Chances are, you will try to burn the words into your mind by repeating them over and over. Such repetition, or maintenance rehearsal, is effective for maintaining the information in STM, but is an inefficient and often ineffective means of transferring it to LTM. The list is difficult to memorize because it does not correspond with any schema already in memory.

The words are familiar, but you do not have available in memory a schema that connects the words in this particular group to each other. If the list were changed to juice, cereal, milk, sugar, bacon, eggs, toast, butter, jelly, and coffee, the task would be much easier because the data would then correspond with an existing schema—items commonly eaten for breakfast. Such a list can be assimilated to your existing store of knowledge with little difficulty, just as the chess master rapidly assimilates the positions of many chessmen.

Depth of processing is the second important variable in determining how well information is retained. Depth of processing refers to the amount of effort and cognitive capacity employed to process information, and the number and strength of associations that are thereby forged between the data to be learned and knowledge already in memory. In experiments to test how well people remember a list of words, test subjects might be asked to perform different tasks that reflect different levels of processing. The following illustrative tasks are listed in order of the depth of mental processing required: say how many letters there are in each word on the list, give a word that rhymes with each word, make a mental image of each word, make up a story that incorporates each word.

It turns out that the greater the depth of processing, the greater the ability to recall words on a list. This result holds true regardless of whether the test subjects are informed in advance that the purpose of the experiment is to test them on their memory. Advising test subjects to expect a test makes almost no difference in their performance, presum-

ably because it only leads them to rehearse the information in short-term memory, which is ineffective as compared with other forms of processing.

There are three ways in which information may be learned or committed to memory: by rote, assimilation, or use of a mnemonic device. Each of these procedures is discussed below.[33]

By Rote. Material to be learned is repeated verbally with sufficient frequency that it can later be repeated from memory without use of any memory aids. When information is learned by rote, it forms a separate schema not closely interwoven with previously held knowledge. That is, the mental processing adds little by way of elaboration to the new information, and the new information adds little to the elaboration of existing schemata. Learning by rote is a brute force technique. It seems to be the least efficient way of remembering.

By Assimilation. Information is learned by assimilation when the structure or substance of the information fits into some memory schema already possessed by the learner. The new information is assimilated to or linked to the existing schema and can be retrieved readily by first accessing the existing schema and then reconstructing the new information. Assimilation involves learning by comprehension and is, therefore, a desirable method, but it can only be used to learn information that is somehow related to our previous experience.

By Using A Mnemonic Device. A mnemonic device is any means of organizing or encoding information for the purpose of making it easier to remember. A high school student cramming for a geography test might use the acronym "HOMES" as a device for remembering the first letter of each of the Great Lakes—Huron, Ontario, etc.

To learn the first grocery list of disconnected words, you would create some structure for linking the words to each other and/or to information already in LTM. You might imagine yourself shopping or putting the items away and mentally picture where they are located on the shelves at the market or in the kitchen. Or you might imagine a story concerning one or more meals that include all these items. Any form of processing information in this manner is a more effective aid to retention than rote repetition. Even more effective systems for quickly memorizing lists of

33. This discussion draws on Francis S. Bellezza, "Mnemonic Devices: Classification, Characteristics, and Criteria" (Athens, Ohio: Ohio University, pre-publication manuscript, January 1980).

names or words have been devised by various memory experts, but these require some study and practice in their use.

Mnemonic devices are useful for remembering information that does not fit any appropriate conceptual structure or schema already in memory. They work by providing a simple, artificial structure to which the information to be learned is then linked. The mnemonic device supplies the mental "file categories" that ensure retrievability of information. To remember, first recall the mnemonic device, then access the desired information.

Memory and Intelligence Analysis

An analyst's memory provides continuous input into the analytical process. This input is of two types—additional factual information on historical background and context, and schemata the analyst uses to determine the meaning of newly acquired information. Information from memory may force itself on the analyst's awareness without any deliberate effort by the analyst to remember; or, recall of the information may require considerable time and strain. In either case, anything that influences what information is remembered or retrieved from memory also influences intelligence analysis.

Judgment is the joint product of the available information and what the analyst brings to the analysis of this information. An experiment documenting differences between chess masters and ordinary chess players was noted earlier. Similar research with medical doctors diagnosing illness indicates that differences between stronger and weaker performers are to be found in the organization of information and experience in long-term memory.[34] The same presumably holds true for intelligence analysts. Substantive knowledge and analytical experience determine the store of memories and schemata the analyst draws upon to generate and evaluate hypotheses. The key is not a simple ability to recall facts, but the ability to recall patterns that relate facts to each other and to broader concepts—and to employ procedures that facilitate this process.

34. Arthur S. Elstein, Lee S. Shulman & Sarah A. Sprafka, *Medical Problem Solving: An Analysis of Clinical Reasoning* (Cambridge, MA: Harvard University Press, 1978), p. 276.

Stretching the Limits of Working Memory

Limited information is available on what is commonly thought of as "working memory"—the collection of information that an analyst holds in the forefront of the mind as he or she does analysis. The general concept of working memory seems clear from personal introspection. In writing this chapter, I am very conscious of the constraints on my ability to keep many pieces of information in mind while experimenting with ways to organize this information and seeking words to express my thoughts. To help offset these limits on my working memory, I have accumulated a large number of written notes containing ideas and half-written paragraphs. Only by using such external memory aids am I able to cope with the volume and complexity of the information I want to use.

A well-known article written over 40 years ago, titled "The Magic Number Seven—Plus or Minus Two," contends that seven—plus or minus two—is the number of things people can keep in their head all at once.[35] That limitation on working memory is the source of many problems. People have difficulty grasping a problem in all its complexity. This is why we sometimes have trouble making up our minds. For example, we think first about the arguments in favor, and then about the arguments against, and we can't keep all those pros and cons in our head at the same time to get an overview of how they balance off against each other.

The recommended technique for coping with this limitation of working memory is called externalizing the problem—getting it out of one's head and down on paper in some simplified form that shows the main elements of the problem and how they relate to each other. Chapter 7, "Structuring Analytical Problems," discusses ways of doing this. They all involve breaking down a problem into its component parts and then preparing a simple "model" that shows how the parts relate to the whole. When working on a small part of the problem, the model keeps one from losing sight of the whole.

A simple model of an analytical problem facilitates the assimilation of new information into long-term memory; it provides a structure to which bits and pieces of information can be related. The model defines the categories for filing information in memory and retrieving it on

35. George A. Miller, "The Magical Number Seven--Plus or Minus Two: Some Limits on our Capacity for Processing Information." *The Psychological Review*, Vol. 63, No. 2 (March 1956).

demand. In other words, it serves as a mnemonic device that provides the hooks on which to hang information so that it can be found when needed.

The model is initially an artificial construct, like the previously noted acronym "HOMES." With usage, however, it rapidly becomes an integral part of one's conceptual structure—the set of schemata used in processing information. At this point, remembering new information occurs by assimilation rather than by mnemonics. This enhances the ability to recall and make inferences from a larger volume of information in a greater variety of ways than would otherwise be possible.

"Hardening of the Categories". Memory processes tend to work with generalized categories. If people do not have an appropriate category for something, they are unlikely to perceive it, store it in memory, or be able to retrieve it from memory later. If categories are drawn incorrectly, people are likely to perceive and remember things inaccurately. When information about phenomena that are different in important respects nonetheless gets stored in memory under a single concept, errors of analysis may result. For example, many observers of international affairs had the impression that Communism was a monolithic movement, that it was the same everywhere and controlled from Moscow. All Communist countries were grouped together in a single, undifferentiated category called "international Communism" or "the Communist bloc." In 1948, this led many in the United States to downplay the importance of the Stalin-Tito split. According to one authority, it "may help explain why many Western minds, including scholars, remained relatively blind to the existence and significance of Sino-Soviet differences long after they had been made manifest in the realm of ideological formulae."[36]

"Hardening of the categories" is a common analytical weakness. Fine distinctions among categories and tolerance for ambiguity contribute to more effective analysis.

Things That Influence What Is Remembered. Factors that influence how information is stored in memory and that affect future retrievability include: being the first-stored information on a given topic, the amount of attention focused on the information, the credibility of the information, and the importance attributed to the information at the

36. Robert Tucker, "Communist Revolutions, National Cultures, and the Divided Nations," *Studies in Comparative Communism* (Autumn 1974), 235-245.

moment of storage. By influencing the content of memory, all of these factors also influence the outcome of intelligence analysis.

Chapter 12 on "Biases in Estimating Probabilities" describes how availability in memory influences judgments of probability. The more instances a person can recall of a phenomenon, the more probable that phenomenon seems to be. This is true even though ability to recall past examples is influenced by vividness of the information, how recently something occurred, its impact upon one's personal welfare, and many other factors unrelated to the actual probability of the phenomenon.

Memory Rarely Changes Retroactively. Analysts often receive new information that should, logically, cause them to reevaluate the credibility or significance of previous information. Ideally, the earlier information should then become either more salient and readily available in memory, or less so. But it does not work that way. Unfortunately, memories are seldom reassessed or reorganized retroactively in response to new information. For example, information that is dismissed as unimportant or irrelevant because it did not fit an analyst's expectations does not become more memorable even if the analyst changes his or her thinking to the point where the same information, received today, would be recognized as very significant.

Memory Can Handicap as Well as Help

Understanding how memory works provides some insight into the nature of creativity, openness to new information, and breaking mind-sets. All involve spinning new links in the spider web of memory—links among facts, concepts, and schemata that previously were not connected or only weakly connected.

Training courses for intelligence analysts sometimes focus on trying to open up an analyst's established mind-set, to get him or her to see problems from different perspectives in order to give a fairer shake to alternative explanations. More often than not, the reaction of experienced analysts is that they have devoted 20 years to developing their present mind-set, that it has served them well, and that they see no need to change it. Such analysts view themselves, often accurately, as comparable to the chess masters. They believe the information embedded in their long-term memory permits them to perceive patterns and make inferences that are beyond the reach of other observers. In one sense, they are quite correct in not wanting to change; it is, indeed, their existing

schemata or mind-set that enables them to achieve whatever success they enjoy in making analytical judgments.

There is, however, a crucial difference between the chess master and the master intelligence analyst. Although the chess master faces a different opponent in each match, the environment in which each contest takes place remains stable and unchanging: the permissible moves of the diverse pieces are rigidly determined, and the rules cannot be changed without the master's knowledge. Once the chess master develops an accurate schema, there is no need to change it. The intelligence analyst, however, must cope with a rapidly changing world. Many countries that previously were US adversaries are now our formal or de facto allies. The American and Russian governments and societies are not the same today as they were 20 or even 10 or five years ago. Schemata that were valid yesterday may no longer be functional tomorrow.

Learning new schemata often requires the unlearning of existing ones, and this is exceedingly difficult. It is always easier to learn a new habit than to unlearn an old one. Schemata in long-term memory that are so essential to effective analysis are also the principal source of inertia in recognizing and adapting to a changing environment. Chapter 6, "Keeping an Open Mind," identifies tools for dealing with this problem.

PART II—TOOLS FOR THINKING

Chapter 4

Strategies for Analytical Judgment: Transcending the Limits of Incomplete Information

When intelligence analysts make thoughtful analytical judgments, how do they do it? In seeking answers to this question, this chapter discusses the strengths and limitations of situational logic, theory, comparison, and simple immersion in the data as strategies for the generation and evaluation of hypotheses. The final section discusses alternative strategies for choosing among hypotheses. One strategy too often used by intelligence analysts is described as "satisficing"—choosing the first hypothesis that appears good enough rather than carefully identifying all possible hypotheses and determining which is most consistent with the evidence.[37]

* * * * * * * * * * * * * * * * * * * *

Intelligence analysts should be self-conscious about their reasoning process. They should think about *how* they make judgments and reach conclusions, not just about the judgments and conclusions themselves. Webster's dictionary defines judgment as arriving at a "decision or conclusion on the basis of indications and probabilities when the facts are not clearly ascertained." [38] Judgment is what analysts use to fill gaps in their knowledge. It entails going beyond the available information and is the principal means of coping with uncertainty. It always involves an analytical leap, from the known into the uncertain.

37. An earlier version of this chapter was published as an unclassified article in *Studies in Intelligence* in 1981, under the title "Strategies for Analytical Judgment."
38. Webster's *New International Dictionary*, unabridged, 1954.

Judgment is an integral part of all intelligence analysis. While the optimal goal of intelligence collection is complete knowledge, this goal is seldom reached in practice. Almost by definition of the intelligence mission, intelligence issues involve considerable uncertainty. Thus, the analyst is commonly working with incomplete, ambiguous, and often contradictory data. The intelligence analyst's function might be described as transcending the limits of incomplete information through the exercise of analytical judgment.

The ultimate nature of judgment remains a mystery. It is possible, however, to identify diverse strategies that analysts employ to process information as they prepare to pass judgment. Analytical strategies are important because they influence the data one attends to. They determine where the analyst shines his or her searchlight, and this inevitably affects the outcome of the analytical process.

Strategies for Generating and Evaluating Hypotheses

This book uses the term hypothesis in its broadest sense as a potential explanation or conclusion that is to be tested by collecting and presenting evidence. Examination of how analysts generate and evaluate hypotheses identifies three principal strategies—the application of theory, situational logic, and comparison—each of which is discussed at some length below. A "non-strategy," immersion in the data and letting the data speak for themselves, is also discussed. This list of analytical strategies is not exhaustive. Other strategies might include, for example, projecting one's own psychological needs onto the data at hand, but this discussion is not concerned with the pathology of erroneous judgment. Rather, the goal is to understand the several kinds of careful, conscientious analysis one would hope and expect to find among a cadre of intelligence analysts dealing with highly complex issues.

Situational Logic

This is the most common operating mode for intelligence analysts. Generation and analysis of hypotheses start with consideration of concrete elements of the current situation, rather than with broad generalizations that encompass many similar cases. The situation is regarded as one-of-a-kind, so that it must be understood in terms of its own unique logic, rather than as one example of a broad class of comparable events.

Starting with the known facts of the current situation and an understanding of the unique forces at work at that particular time and place, the analyst seeks to identify the logical antecedents or consequences of this situation. A scenario is developed that hangs together as a plausible narrative. The analyst may work backwards to explain the origins or causes of the current situation or forward to estimate the future outcome.

Situational logic commonly focuses on tracing cause-effect relationships or, when dealing with purposive behavior, means-ends relationships. The analyst identifies the goals being pursued and explains why the foreign actor(s) believe certain means will achieve those goals.

Particular strengths of situational logic are its wide applicability and ability to integrate a large volume of relevant detail. Any situation, however unique, may be analyzed in this manner.

Situational logic as an analytical strategy also has two principal weaknesses. One is that it is so difficult to understand the mental and bureaucratic processes of foreign leaders and governments. To see the options faced by foreign leaders as these leaders see them, one must understand their values and assumptions and even their misperceptions and misunderstandings. Without such insight, interpreting foreign leaders' decisions or forecasting future decisions is often little more than partially informed speculation. Too frequently, foreign behavior appears "irrational" or "not in their own best interest." Such conclusions often indicate analysts have projected American values and conceptual frameworks onto the foreign leaders and societies, rather than understanding the logic of the situation as it appears to them.

The second weakness is that situational logic fails to exploit the theoretical knowledge derived from study of similar phenomena in other countries and other time periods. The subject of national separatist movements illustrates the point. Nationalism is a centuries-old problem, but most Western industrial democracies have been considered well-integrated national communities. Even so, recent years have seen an increase in pressures from minority ethnic groups seeking independence or autonomy. Why has this phenomenon occurred recently in Scotland, southern France and Corsica, Quebec, parts of Belgium, and Spain—as well as in less stable Third World countries where it might be expected?

Dealing with this topic in a logic-of-the-situation mode, a country analyst would examine the diverse political, economic, and social groups whose interests are at stake in the country. Based on the relative power

positions of these groups, the dynamic interactions among them, and anticipated trends or developments that might affect the future positions of the interested parties, the analyst would seek to identify the driving forces that will determine the eventual outcome.

It is quite possible to write in this manner a detailed and seemingly well-informed study of a separatist movement in a single country while ignoring the fact that ethnic conflict as a generic phenomenon has been the subject of considerable theoretical study. By studying similar phenomena in many countries, one can generate and evaluate hypotheses concerning root causes that may not even be considered by an analyst who is dealing only with the logic of a single situation. For example, to what extent does the resurgence of long-dormant ethnic sentiments stem from a reaction against the cultural homogenization that accompanies modern mass communications systems?

Analyzing many examples of a similar phenomenon, as discussed below, enables one to probe more fundamental causes than those normally considered in logic-of-the-situation analysis. The proximate causes identified by situational logic appear, from the broader perspective of theoretical analysis, to be but symptoms indicating the presence of more fundamental causal factors. A better understanding of these fundamental causes is critical to effective forecasting, especially over the longer range. While situational logic may be the best approach to estimating short-term developments, a more theoretical approach is required as the analytical perspective moves further into the future.

Applying Theory

Theory is an academic term not much in vogue in the Intelligence Community, but it is unavoidable in any discussion of analytical judgment. In one popular meaning of the term, "theoretical" is associated with the terms "impractical" and "unrealistic". Needless to say, it is used here in a quite different sense.

A theory is a generalization based on the study of many examples of some phenomenon. It specifies that when a given set of conditions arises, certain other conditions will follow either with certainty or with some degree of probability. In other words, conclusions are judged to follow from a set of conditions and a finding that these conditions apply in the specific case being analyzed. For example, Turkey is a developing country in a precarious strategic position. This defines a set of conditions that

imply conclusions concerning the role of the military and the nature of political processes in that country, because analysts have an implicit if not explicit understanding of how these factors normally relate.

What academics refer to as theory is really only a more explicit version of what intelligence analysts think of as their basic understanding of how individuals, institutions, and political systems normally behave.

There are both advantages and drawbacks to applying theory in intelligence analysis. One advantage is that "theory economizes thought." By identifying the key elements of a problem, theory enables an analyst to sort through a mass of less significant detail. Theory enables the analyst to see beyond today's transient developments, to recognize which trends are superficial and which are significant, and to foresee future developments for which there is today little concrete evidence.

Consider, for example, the theoretical proposition that economic development and massive infusion of foreign ideas in a feudal society lead to political instability. This proposition seems well established. When applied to Saudi Arabia, it suggests that the days of the Saudi monarchy are numbered, although analysts of the Saudi scene using situational logic find little or no current evidence of a meaningful threat to the power and position of the royal family. Thus, the application of a generally accepted theoretical proposition enables the analyst to forecast an outcome for which the "hard evidence" has not yet begun to develop. This is an important strength of theoretical analysis when applied to real-world problems.

Yet this same example also illustrates a common weakness in applying theory to analysis of political phenomena. Theoretical propositions frequently fail to specify the time frame within which developments might be anticipated to occur. The analytical problem with respect to Saudi Arabia is not so much whether the monarchy will *eventually* be replaced, as when or under what conditions this might happen. Further elaboration of the theory relating economic development and foreign ideas to political instability in feudal societies would identify early warning indicators that analysts might look for. Such indicators would guide both intelligence collection and analysis of sociopolitical and socioeconomic data and lead to hypotheses concerning when or under what circumstances such an event might occur.

But if theory enables the analyst to transcend the limits of available data, it may also provide the basis for ignoring evidence that is truly

indicative of future events. Consider the following theoretical propositions in the light of popular agitation against the Shah of Iran in the late 1970s: (1) When the position of an authoritarian ruler is threatened, he will defend his position with force if necessary. (2) An authoritarian ruler enjoying complete support of effective military and security forces cannot be overthrown by popular opinion and agitation. Few would challenge these propositions, yet when applied to Iran in the late 1970s, they led Iran specialists to misjudge the Shah's chances for retaining the peacock throne. Many if not most such specialists seemed convinced that the Shah remained strong and that he would crack down on dissent when it threatened to get out of control. Many persisted in this assessment for several months after the accumulation of what in retrospect appears to have been strong evidence to the contrary.

Persistence of these assumptions is easily understood in psychological terms. When evidence is lacking or ambiguous, the analyst evaluates hypotheses by applying his or her general background knowledge concerning the nature of political systems and behavior. The evidence on the strength of the Shah and his intention to crack down on dissidents was ambiguous, but the Iranian monarch was an authoritarian ruler, and authoritarian regimes were assumed to have certain characteristics, as noted in the previously cited propositions. Thus beliefs about the Shah were embedded in broad and persuasive assumptions about the nature of authoritarian regimes *per se.* For an analyst who believed in the two aforementioned propositions, it would have taken far more evidence, including more unambiguous evidence, to infer that the Shah would be overthrown than to justify continued confidence in his future.[39]

Figure 4 below illustrates graphically the difference between theory and situational logic. Situational logic looks at the evidence within a single country on multiple interrelated issues, as shown by the column

39. Even in retrospect these two propositions still seem valid, which is why some aspects of the Shah's fall remain incredible. There are, in principle, three possible reasons why these seemingly valid theoretical assumptions failed to generate an accurate estimate on Iran: (1) One or more of the initial conditions posited by the theory did not in fact apply--for example, the Shah was not really an authoritarian ruler. (2) The theory is only partially valid, in that there are certain circumstances under which it does and does not apply. These limiting conditions need to be specified. (3) The theory is basically valid, but one cannot expect 100-percent accuracy from social science theories. Social science, as distinct from natural science, deals with a probabilistic environment. One cannot foresee all the circumstances that might cause an exception to the general rules, so the best that can be expected is that the given conditions will lead to the specified outcome most of the time.

Figure 4

	Country	Country	Country	Country
Issue	Evidence	Evidence	Evidence	Evidence
Issue	Evidence	Evidence	Evidence	Evidence
Issue	Evidence	Evidence	Evidence	Evidence
Issue	Evidence	Evidence	Evidence	Evidence

Situational Logic Vs. Theory

highlighted in gray. This is a typical area studies approach. Theoretical analysis looks at the evidence related to a single issue in multiple countries, as shown by the row highlighted in gray. This is a typical social science approach.

The distinction between theory and situational logic is not as clear as it may seem from this graphic, however. Logic-of-the-situation analysis also draws heavily on theoretical assumptions. How does the analyst select the most significant elements to describe the current situation, or identify the causes or consequences of these elements, without some implicit theory that relates the likelihood of certain outcomes to certain antecedent conditions?

For example, if the analyst estimating the outcome of an impending election does not have current polling data, it is necessary to look back at past elections, study the campaigns, and then judge how voters are likely to react to the current campaigns and to events that influence voter attitudes. In doing so, the analyst operates from a set of assumptions about human nature and what drives people and groups. These assumptions form part of a theory of political behavior, but it is a different sort of theory than was discussed under theoretical analysis. It does not illuminate the entire situation, but only a small increment of the situation, and it may not apply beyond the specific country of concern. Further, it is

much more likely to remain implicit, rather than be a focal point of the analysis.

Comparison with Historical Situations

A third approach for going beyond the available information is comparison. An analyst seeks understanding of current events by comparing them with historical precedents in the same country, or with similar events in other countries. Analogy is one form of comparison. When an historical situation is deemed comparable to current circumstances, analysts use their understanding of the historical precedent to fill gaps in their understanding of the current situation. Unknown elements of the present are assumed to be the same as known elements of the historical precedent. Thus, analysts reason that the same forces are at work, that the outcome of the present situation is likely to be similar to the outcome of the historical situation, or that a certain policy is required in order to avoid the same outcome as in the past.

Comparison differs from situational logic in that the present situation is interpreted in the light of a more or less explicit conceptual model that is created by looking at similar situations in other times or places. It differs from theoretical analysis in that this conceptual model is based on a single case or only a few cases, rather than on many similar cases. Comparison may also be used to generate theory, but this is a more narrow kind of theorizing that cannot be validated nearly as well as generalizations inferred from many comparable cases.

Reasoning by comparison is a convenient shortcut, one chosen when neither data nor theory are available for the other analytical strategies, or simply because it is easier and less time-consuming than a more detailed analysis. A careful comparative analysis starts by specifying key elements of the present situation. The analyst then seeks out one or more historical precedents that may shed light on the present. Frequently, however, a historical precedent may be so vivid and powerful that it imposes itself upon a person's thinking from the outset, conditioning them to perceive the present primarily in terms of its similarity to the past. This is reasoning by analogy. As Robert Jervis noted, "historical analogies often precede, rather than follow, a careful analysis of a situation."[40]

40. Robert Jervis, "Hypotheses on Misperception," *World Politics* 20 (April 1968), p. 471.

The tendency to relate contemporary events to earlier events as a guide to understanding is a powerful one. Comparison helps achieve understanding by reducing the unfamiliar to the familiar. In the absence of data required for a full understanding of the current situation, reasoning by comparison may be the only alternative. Anyone taking this approach, however, should be aware of the significant potential for error. This course is an implicit admission of the lack of sufficient information to understand the present situation in its own right, and lack of relevant theory to relate the present situation to many other comparable situations

The difficulty, of course, is in being certain that two situations are truly comparable. Because they are equivalent in some respects, there is a tendency to reason as though they were equivalent in all respects, and to assume that the current situation will have the same or similar outcome as the historical situation. This is a valid assumption only when based on in-depth analysis of both the current situation *and* the historical precedent to ensure that they are actually comparable in all relevant respects.

In a short book that ought to be familiar to all intelligence analysts, Ernest May traced the impact of historical analogy on US foreign policy.[41] He found that because of reasoning by analogy, US policymakers tend to be one generation behind, determined to avoid the mistakes of the previous generation. They pursue the policies that would have been most appropriate in the historical situation but are not necessarily well adapted to the current one.

Policymakers in the 1930s, for instance, viewed the international situation as analogous to that before World War I. Consequently, they followed a policy of isolation that would have been appropriate for preventing American involvement in the first World War but failed to prevent the second. Communist aggression after World War II was seen as analogous to Nazi aggression, leading to a policy of containment that could have prevented World War II.

More recently, the Vietnam analogy has been used repeatedly over many years to argue against an activist US foreign policy. For example, some used the Vietnam analogy to argue against US participation in the Gulf War—a flawed analogy because the operating terrain over which

41. Ernest May, *`Lessons' of the Past: The Use and Misuse of History in American Foreign Policy* (New York: Oxford University Press, 1973).

battles were fought was completely different in Kuwait/Iraq and much more in our favor there as compared with Vietnam.

May argues that policymakers often perceive problems in terms of analogies with the past, but that they ordinarily use history badly:

> When resorting to an analogy, they tend to seize upon the first that comes to mind. They do not research more widely. Nor do they pause to analyze the case, test its fitness, or even ask in what ways it might be misleading.[42]

As compared with policymakers, intelligence analysts have more time available to "analyze rather than analogize." Intelligence analysts tend to be good historians, with a large number of historical precedents available for recall. The greater the number of potential analogues an analyst has at his or her disposal, the greater the likelihood of selecting an appropriate one. The greater the depth of an analyst's knowledge, the greater the chances the analyst will perceive the differences as well as the similarities between two situations. Even under the best of circumstances, however, inferences based on comparison with a single analogous situation probably are more prone to error than most other forms of inference.

The most productive uses of comparative analysis are to suggest hypotheses and to highlight differences, not to draw conclusions. Comparison can suggest the presence or the influence of variables that are not readily apparent in the current situation, or stimulate the imagination to conceive explanations or possible outcomes that might not otherwise occur to the analyst. In short, comparison can generate hypotheses that then guide the search for additional information to confirm or refute these hypotheses. It should not, however, form the basis for conclusions unless thorough analysis of both situations has confirmed they are indeed comparable.

Data Immersion

Analysts sometimes describe their work procedure as immersing themselves in the data without fitting the data into any preconceived pattern. At some point an apparent pattern (or answer or explanation) emerges spontaneously, and the analyst then goes back to the data to check how well the data support this judgment. According to this view,

42. Ibid., p. xi.

objectivity requires the analyst to suppress any personal opinions or preconceptions, so as to be guided only by the "facts" of the case.

To think of analysis in this way overlooks the fact that information cannot speak for itself. The significance of information is always a joint function of the nature of the information and the context in which it is interpreted. The context is provided by the analyst in the form of a set of assumptions and expectations concerning human and organizational behavior. These preconceptions are critical determinants of which information is considered relevant and how it is interpreted.

Of course there are many circumstances in which the analyst has no option but to immerse himself or herself in the data. Obviously, an analyst must have a base of knowledge to work with before starting analysis. When dealing with a new and unfamiliar subject, the uncritical and relatively non-selective accumulation and review of information is an appropriate first step. But this is a process of absorbing information, not analyzing it.

Analysis begins when the analyst consciously inserts himself or herself into the process to select, sort, and organize information. This selection and organization can only be accomplished according to conscious or subconscious assumptions and preconceptions.

The question is not whether one's prior assumptions and expectations influence analysis, but only whether this influence is made explicit or remains implicit. The distinction appears to be important. In research to determine how physicians make medical diagnoses, the doctors who comprised the test subjects were asked to describe their analytical strategies. Those who stressed thorough collection of data as their principal analytical method were significantly less accurate in their diagnoses than those who described themselves as following other analytical strategies such as identifying and testing hypotheses.[43] Moreover, the collection of additional data through greater thoroughness in the medical history and physical examination did not lead to increased diagnostic accuracy.[44]

One might speculate that the analyst who seeks greater objectivity by suppressing recognition of his or her own subjective input actually has less valid input to make. Objectivity is gained by making assumptions

43. Arthur S. Elstein, Lee S. Shulman, and Sarah A. Sprafka, *Medical Problem Solving: An Analysis of Clinical Reasoning* (Cambridge, MA: Harvard University Press, 1978), p. 270.
44. Ibid., p. 281. For more extensive discussion of the value of additional information, see Chapter 5, "Do You Really Need More Information?"

explicit so that they may be examined and challenged, not by vain efforts to eliminate them from analysis.

Relationships Among Strategies

No one strategy is necessarily better than the others. In order to generate all relevant hypotheses and make maximum use of all potentially relevant information, it would be desirable to employ all three strategies at the early hypothesis generation phase of a research project. Unfortunately, analysts commonly lack the inclination or time to do so.

Different analysts have different analytical habits and preferences for analytical strategy. As a broad generalization that admits numerous exceptions, analysts trained in area studies or history tend to prefer situational logic, while those with a strong social science background are more likely to bring theoretical and comparative insights to bear on their work. The Intelligence Community as a whole is far stronger in situational logic than in theory. In my judgment, intelligence analysts do not generalize enough, as opposed to many academic scholars who generalize too much. This is especially true in political analysis, and it is not entirely due to unavailability of applicable political theory. Theoretical insights that are available are often unknown to or at least not used by political intelligence analysts.

Differences in analytical strategy may cause fundamental differences in perspective between intelligence analysts and some of the policymakers for whom they write. Higher level officials who are not experts on the subject at issue use far more theory and comparison and less situational logic than intelligence analysts. Any policymaker or other senior manager who lacks the knowledge base of the specialist and does not have time for detail must, of necessity, deal with broad generalizations. Many decisions must be made, with much less time to consider each of them than is available to the intelligence analyst. This requires the policymaker to take a more conceptual approach, to think in terms of theories, models, or analogies that summarize large amounts of detail. Whether this represents sophistication or oversimplification depends upon the individual case and, perhaps, whether one agrees or disagrees with the judgments made. In any event, intelligence analysts would do well to take this phenomenon into account when writing for their consumers.

Strategies for Choice Among Hypotheses

A systematic analytical process requires selection among alternative hypotheses, and it is here that analytical practice often diverges significantly from the ideal and from the canons of scientific method. The ideal is to generate a full set of hypotheses, systematically evaluate each hypothesis, and then identify the hypothesis that provides the best fit to the data. Scientific method, for its part, requires that one seek to disprove hypotheses rather than confirm them.

In practice, other strategies are commonly employed. Alexander George has identified a number of less-than-optimal strategies for making decisions in the face of incomplete information and multiple, competing values and goals. While George conceived of these strategies as applicable to how decisionmakers choose among alternative policies, most also apply to how intelligence analysts might decide among alternative analytical hypotheses.

The relevant strategies George identified are:

- "Satisficing"—selecting the first identified alternative that appears "good enough" rather than examining all alternatives to determine which is "best."

- Incrementalism—focusing on a narrow range of alternatives representing marginal change, without considering the need for dramatic change from an existing position.

- Consensus—opting for the alternative that will elicit the greatest agreement and support. Simply telling the boss what he or she wants to hear is one version of this.

- Reasoning by analogy—choosing the alternative that appears most likely to avoid some previous error or to duplicate a previous success.

- Relying on a set of principles or maxims that distinguish a "good" from a "bad" alternative.[45]

45. Alexander George, *Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice* (Boulder, CO: Westview Press, 1980), Chapter 2.

The intelligence analyst has another tempting option not available to the policymaker: to avoid judgment by simply describing the current situation, identifying alternatives, and letting the intelligence consumer make the judgment about which alternative is most likely. Most of these strategies are not discussed here. The following paragraphs focus only on the one that seems most prevalent in intelligence analysis.

"Satisficing"

I would suggest, based on personal experience and discussions with analysts, that most analysis is conducted in a manner very similar to the satisficing mode (selecting the first identified alternative that appears "good enough").[46] The analyst identifies what appears to be the most likely hypothesis—that is, the tentative estimate, explanation, or description of the situation that appears most accurate. Data are collected and organized according to whether they support this tentative judgment, and the hypothesis is accepted if it seems to provide a reasonable fit to the data. The careful analyst will then make a quick review of other possible hypotheses and of evidence not accounted for by the preferred judgment to ensure that he or she has not overlooked some important consideration.

This approach has three weaknesses: the selective perception that results from focus on a single hypothesis, failure to generate a complete set of competing hypotheses, and a focus on evidence that confirms rather than disconfirms hypotheses. Each of these is discussed below.

Selective Perception. Tentative hypotheses serve a useful function in helping analysts select, organize, and manage information. They narrow the scope of the problem so that the analyst can focus efficiently on data that are most relevant and important. The hypotheses serve as organizing frameworks in working memory and thus facilitate retrieval of information from memory. In short, they are essential elements of the analytical process. But their functional utility also entails some cost, because a hypothesis functions as a perceptual filter. Analysts, like people in general, tend to see what they are looking for and to overlook that which is not specifically included in their search strategy. They tend to limit the processed information to that which is relevant to the current hypothesis.

46. The concept of "satisficing," of seeking a satisfactory rather than an optimal solution, was developed by Herbert A. Simon and is widely used in the literature on decision analysis.

If the hypothesis is incorrect, information may be lost that would suggest a new or modified hypothesis.

This difficulty can be overcome by the simultaneous consideration of multiple hypotheses. This approach is discussed in detail in Chapter 8. It has the advantage of focusing attention on those few items of evidence that have the greatest diagnostic value in distinguishing among the validity of competing hypotheses. Most evidence is consistent with several different hypotheses, and this fact is easily overlooked when analysts focus on only one hypothesis at a time—especially if their focus is on seeking to confirm rather than disprove what appears to be the most likely answer.

Failure To Generate Appropriate Hypotheses. If tentative hypotheses determine the criteria for searching for information and judging its relevance, it follows that one may overlook the proper answer if it is not encompassed within the several hypotheses being considered. Research on hypothesis generation suggests that performance on this task is woefully inadequate.[47] When faced with an analytical problem, people are either unable or simply do not take the time to identify the full range of potential answers. Analytical performance might be significantly enhanced by more deliberate attention to this stage of the analytical process. Analysts need to take more time to develop a full set of competing hypotheses, using all three of the previously discussed strategies—theory, situational logic, and comparison.

Failure To Consider Diagnosticity of Evidence. In the absence of a complete set of alternative hypotheses, it is not possible to evaluate the "diagnosticity" of evidence. Unfortunately, many analysts are unfamiliar with the concept of diagnosticity of evidence. It refers to the extent to which any item of evidence helps the analyst determine the relative likelihood of alternative hypotheses.

To illustrate, a high temperature may have great value in telling a doctor that a patient is sick, but relatively little value in determining which illness the patient is suffering from. Because a high temperature is consistent with so many possible hypotheses about a patient's illness, it has limited diagnostic value in determining which illness (hypothesis) is the more likely one.

47. Charles Gettys et al., *Hypothesis Generation: A Final Report on Three Years of Research.* Technical Report 15-10-80. University of Oklahoma, Decision Processes Laboratory, 1980.

Evidence is diagnostic when it influences an analyst's judgment on the *relative* likelihood of the various hypotheses. If an item of evidence seems consistent with all the hypotheses, it may have no diagnostic value at all. It is a common experience to discover that most available evidence really is not very helpful, as it can be reconciled with all the hypotheses.

Failure To Reject Hypotheses

Scientific method is based on the principle of rejecting hypotheses, while tentatively accepting only those hypotheses that cannot be refuted. Intuitive analysis, by comparison, generally concentrates on confirming a hypothesis and commonly accords more weight to evidence supporting a hypothesis than to evidence that weakens it. Ideally, the reverse would be true. While analysts usually cannot apply the statistical procedures of scientific methodology to test their hypotheses, they can and should adopt the conceptual strategy of seeking to refute rather than confirm hypotheses.

There are two aspects to this problem: people do not naturally seek disconfirming evidence, and when such evidence is received it tends to be discounted. If there is any question about the former, consider how often people test their political and religious beliefs by reading newspapers and books representing an opposing viewpoint. Concerning the latter, we have noted in Chapter 2, "Perception: Why Can't We See What Is There to Be Seen?" the tendency to accommodate new information to existing images. This is easy to do if information supporting a hypothesis is accepted as valid, while information that weakens it is judged to be of questionable reliability or an unimportant anomaly. When information is processed in this manner, it is easy to "confirm" almost any hypothesis that one already believes to be true.

Apart from the psychological pitfalls involved in seeking confirmatory evidence, an important logical point also needs to be considered. The logical reasoning underlying the scientific method of rejecting hypotheses is that ". . . no confirming instance of a law is a verifying instance, but that any disconfirming instance is a falsifying instance."[48] In other words, a hypothesis can never be proved by the enumeration of even a large body of evidence consistent with that hypothesis, because

48. P. C. Wason, "On the Failure to Eliminate Hypotheses in a Conceptual Task," *The Quarterly Journal of Experimental Psychology*, Vol. XII, Part 3 (1960).

the same body of evidence may also be consistent with other hypotheses. A hypothesis may be disproved, however, by citing a single item of evidence that is incompatible with it.

P. C. Wason conducted a series of experiments to test the view that people generally seek confirming rather than disconfirming evidence.[49] The experimental design was based on the above point that the validity of a hypothesis can only be tested by seeking to disprove it rather than confirm it. Test subjects were given the three-number sequence, 2 - 4 - 6, and asked to discover the rule employed to generate this sequence. In order to do so, they were permitted to generate three-number sequences of their own and to ask the experimenter whether these conform to the rule. They were encouraged to generate and ask about as many sequences as they wished and were instructed to stop only when they believed they had discovered the rule.

There are, of course, many possible rules that might account for the sequence 2 - 4 - 6. The test subjects formulated tentative hypotheses such as any ascending sequence of even numbers, or any sequence separated by two digits. As expected, the test subjects generally took the incorrect approach of trying to confirm rather than eliminate such hypotheses. To test the hypothesis that the rule was any ascending sequence of even numbers, for example, they might ask if the sequence 8 - 10 - 14 conforms to the rule.

Readers who have followed the reasoning to this point will recognize that this hypothesis can never be proved by enumerating examples of ascending sequences of even numbers that are found to conform to the sought-for rule. One can only disprove the hypothesis by citing an ascending sequence of odd numbers and learning that this, too, conforms to the rule.

The correct rule was any three ascending numbers, either odd or even. Because of their strategy of seeking confirming evidence, only six of the 29 test subjects in Wason's experiment were correct the first time they thought they had discovered the rule. When this same experiment was repeated by a different researcher for a somewhat different purpose, none

49. Wason, ibid.

of the 51 test subjects had the right answer the first time they thought they had discovered the rule.[50]

In the Wason experiment, the strategy of seeking confirming rather than disconfirming evidence was particularly misleading because the 2 - 4 - 6 sequence is consistent with such a large number of hypotheses. It was easy for test subjects to obtain confirmatory evidence for almost any hypothesis they tried to confirm. It is important to recognize that comparable situations, when evidence is consistent with several different hypotheses, are extremely common in intelligence analysis.

Consider lists of early warning indicators, for example. They are designed to be indicative of an impending attack. Very many of them, however, are also consistent with the hypothesis that military movements are a bluff to exert diplomatic pressure and that no military action will be forthcoming. When analysts seize upon only one of these hypotheses and seek evidence to confirm it, they will often be led astray.

The evidence available to the intelligence analyst is in one important sense different from the evidence available to test subjects asked to infer the number sequence rule. The intelligence analyst commonly deals with problems in which the evidence has only a probabilistic relationship to the hypotheses being considered. Thus it is seldom possible to eliminate any hypothesis entirely, because the most one can say is that a given hypothesis is unlikely given the nature of the evidence, not that it is impossible.

This weakens the conclusions that can be drawn from a strategy aimed at eliminating hypotheses, but it does not in any way justify a strategy aimed at confirming them.

Circumstances and insufficient data often preclude the application of rigorous scientific procedures in intelligence analysis—including, in particular, statistical methods for testing hypotheses. There is, however, certainly no reason why the basic conceptual strategy of looking for contrary evidence cannot be employed. An optimal analytical strategy requires that analysts search for information to disconfirm their favorite theories, not employ a satisficing strategy that permits acceptance of the first hypothesis that seems consistent with the evidence.

50. Harold M. Weiss and Patrick A. Knight, "The Utility of Humility: Self-Esteem, Information Search, and Problem-Solving Efficiency," *Organizational Behavior and Human Performance*, Vol. 25, No. 2 (April 1980), 216-223.

Conclusion

There are many detailed assessments of intelligence failures, but few comparable descriptions of intelligence successes. In reviewing the literature on intelligence successes, Frank Stech found many examples of success but only three accounts that provide sufficient methodological details to shed light on the intellectual processes and methods that contributed to the successes. These dealt with successful American and British intelligence efforts during World War II to analyze German propaganda, predict German submarine movements, and estimate future capabilities and intentions of the German Air Force.[51]

Stech notes that in each of these highly successful efforts, the analysts employed procedures that ". . . facilitated the formulation and testing against each other of alternative hypothetical estimates of enemy intentions. Each of the three accounts stressed this pitting of competing hypotheses against the evidence."[52]

The simultaneous evaluation of multiple, competing hypotheses permits a more systematic and objective analysis than is possible when an analyst focuses on a single, most-likely explanation or estimate. The simultaneous evaluation of multiple, competing hypotheses entails far greater cognitive strain than examining a single, most-likely hypothesis. Retaining multiple hypotheses in working memory and noting how each item of evidence fits into each hypothesis add up to a formidable cognitive task. That is why this approach is seldom employed in intuitive analysis of complex issues. It can be accomplished, however, with the help of simple procedures described in Chapter 8, "Analysis of Competing Hypotheses."

51. Alexander George, *Propaganda Analysis: A Study of Inferences Made From Nazi Propaganda in World War II* (Evanston, IL: Row, Peterson, 1959); Patrick Beesly, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945* (London: Hamish Hamilton, 1977); and R. V. Jones, *Wizard War: British Scientific Intelligence 1939-1945* (New York: Coward, McCann & Geoghegan, 1978).

52. Frank J. Stech, Political and Military Intention Estimation: A Taxonometric Analysis, Final Report for Office of Naval Research (Bethesda, MD: MATHTECH, Inc., November 1979), p. 283.

Chapter 5

Do You Really Need More Information?

The difficulties associated with intelligence analysis are often attributed to the inadequacy of available information. Thus the US Intelligence Community invests heavily in improved intelligence collection systems while managers of analysis lament the comparatively small sums devoted to enhancing analytical resources, improving analytical methods, or gaining better understanding of the cognitive processes involved in making analytical judgments. This chapter questions the often-implicit assumption that lack of information is the principal obstacle to accurate intelligence judgments.[53]

* * * * * * * * * * * * * * * * * * * *

Using experts in a variety of fields as test subjects, experimental psychologists have examined the relationship between the amount of information available to the experts, the accuracy of judgments they make based on this information, and the experts' confidence in the accuracy of these judgments. The word "information," as used in this context, refers to the totality of material an analyst has available to work with in making a judgment.

Using experts in a variety of fields as test subjects, experimental psychologists have examined the relationship between the amount of information available to the experts, the accuracy of judgments they make based on this information, and the experts' confidence in the accuracy of these judgments. The word "information," as used in this context, refers

53. This is an edited version of an article that appeared in *Studies in Intelligence*, Vol. 23, No. 1 (Spring 1979). That *Studies in Intelligence* article was later reprinted in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal*, 1955-1992 (New Haven: Yale University Press, 1995). A slightly different version was published in *The Bureaucrat*, Vol. 8, 1979, under the title "Improving Intelligence Analysis: Some Insights on Data, Concepts, and Management in the Intelligence Community." For this book, portions of the original article dealing with improving intelligence analysis have been moved to Chapter 14 on "Improving Intelligence Analysis."

to the totality of material an analyst has available to work with in making a judgment.

Key findings from this research are:

- Once an experienced analyst has the minimum information necessary to make an informed judgment, obtaining additional information generally does not improve the accuracy of his or her estimates. Additional information does, however, lead the analyst to become more confident in the judgment, to the point of overconfidence.

- Experienced analysts have an imperfect understanding of what information they actually use in making judgments. They are unaware of the extent to which their judgments are determined by a few dominant factors, rather than by the systematic integration of all available information. Analysts actually use much less of the available information than they think they do.

As will be noted below, these experimental findings should not necessarily be accepted at face value. For example, circumstances exist in which additional information does contribute to more accurate analysis. However, there also are circumstances in which additional information—particularly contradictory information—decreases rather than increases an analyst's confidence.

To interpret the disturbing but not surprising findings from these experiments, it is necessary to consider four different types of information and discuss their relative value in contributing to the accuracy of analytical judgments. It is also helpful to distinguish analysis in which results are driven by the data from analysis that is driven by the conceptual framework employed to interpret the data.

Understanding the complex relationship between amount of information and accuracy of judgment has implications for both the management and conduct of intelligence analysis. Such an understanding suggests analytical procedures and management initiatives that may indeed contribute to more accurate analytical judgments. It also suggests that resources needed to attain a better understanding of the entire analytical process might profitably be diverted from some of the more costly intelligence collection programs.

These findings have broad relevance beyond the Intelligence Community. Analysis of information to gain a better understanding of current developments and to estimate future outcomes is an essential component of decisionmaking in any field. In fact, the psychological experiments that are most relevant have been conducted with experts in such diverse fields as medical and psychological diagnosis, stock market analysis, weather forecasting, and horserace handicapping. The experiments reflect basic human processes that affect analysis of any subject.

One may conduct experiments to demonstrate these phenomena in any field in which experts analyze a finite number of identifiable and classifiable kinds of information to make judgments or estimates that can subsequently be checked for accuracy. The stock market analyst, for example, commonly works with information concerning price-earnings ratios, profit margins, earnings per share, market volume, and resistance and support levels, and it is relatively easy to measure quantitatively the accuracy of the resulting predictions. By controlling the information made available to a group of experts and then checking the accuracy of judgments based on this information, it is possible to investigate how people use information to arrive at analytical judgments.

An Experiment: Betting on the Horses

A description of one such experiment serves to illustrate the procedure.[54] Eight experienced horserace handicappers were shown a list of 88 variables found on a typical past-performance chart—for example, the weight to be carried; the percentage of races in which horse finished first, second, or third during the previous year; the jockey's record; and the number of days since the horse's last race. Each handicapper was asked to identify, first, what he considered to be the five most important items of information—those he would wish to use to handicap a race if he were limited to only five items of information per horse. Each was then asked to select the 10, 20, and 40 most important variables he would use if limited to those levels of information.

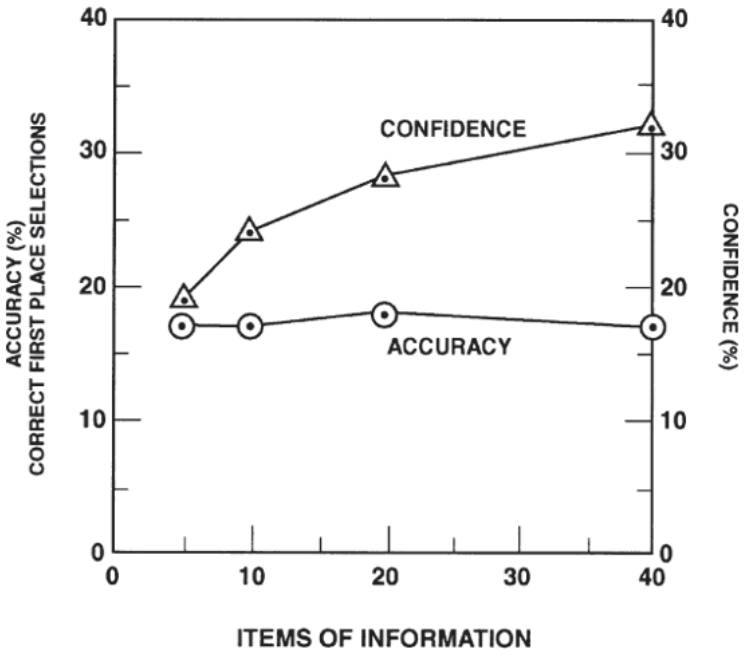
At this point, the handicappers were given true data (sterilized so that horses and actual races could not be identified) for 40 past races and

54. Paul Slovic, "Behavioral Problems of Adhering to a Decision Policy," unpublished manuscript, 1973.

were asked to rank the top five horses in each race in order of expected finish. Each handicapper was given the data in increments of the 5, 10, 20 and 40 variables he had judged to be most useful. Thus, he predicted each race four times—once with each of the four different levels of information. For each prediction, each handicapper assigned a value from 0 to 100 percent to indicate degree of confidence in the accuracy of his prediction.

When the handicappers' predictions were compared with the actual outcomes of these 40 races, it was clear that average accuracy of predictions remained the same regardless of how much information the handicappers had available. Three of the handicappers actually showed less accuracy as the amount of information increased, two improved their accuracy, and three were unchanged. All, however, expressed steadily increasing confidence in their judgments as more information was received. This relationship between amount of information, accuracy of the handi-

Figure 5



cappers' prediction of the first place winners, and the handicappers' confidence in their predictions is shown in Figure 5.

With only five items of information, the handicappers' confidence was well calibrated with their accuracy, but they became overconfident as additional information was received.

The same relationships among amount of information, accuracy, and analyst confidence have been confirmed by similar experiments in other fields.[55] In one experiment with clinical psychologists, a psychological case file was divided into four sections representing successive chronological periods in the life of a relatively normal individual. Thirty-two psychologists with varying levels of experience were asked to make judgments on the basis of this information. After reading each section of the case file, the psychologists answered 25 questions (for which there were known answers) about the personality of the subject of the file. As in other experiments, increasing information resulted in a strong rise in confidence but a negligible increase in accuracy.[56]

A series of experiments to examine the mental processes of medical doctors diagnosing illness found little relationship between thoroughness of data collection and accuracy of diagnosis. Medical students whose self-described research strategy stressed thorough collection of information (as opposed to formation and testing of hypotheses) were significantly below average in the accuracy of their diagnoses. It seems that the explicit formulation of hypotheses directs a more efficient and effective search for information.[57]

Modeling Expert Judgment

Another significant question concerns the extent to which analysts possess an accurate understanding of their own mental processes. How good is their insight into how they actually weight evidence in making judgments? For each situation to be analyzed, they have an implicit "mental model" consisting of beliefs and assumptions as to which vari-

55. For a list of references, see Lewis R. Goldberg, "Simple Models or Simple Processes? Some Research on Clinical Judgments," *American Psychologist*, 23 (1968), pp. 261-265.
56. Stuart Oskamp, "Overconfidence in Case-Study Judgments," *Journal of Consulting Psychology*, 29 (1965), pp. 261-265.
57. Arthur S. Elstein *et al., Medical Problem Solving: An Analysis of Clinical Reasoning* (Cambridge, MA and London: Harvard University Press, 1978), pp. 270 and 295.

ables are most important and how they are related to each other. If analysts have good insight into their own mental model, they should be able to identify and describe the variables they have considered most important in making judgments.

There is strong experimental evidence, however, that such self-insight is usually faulty. The expert perceives his or her own judgmental process, including the number of different kinds of information taken into account, as being considerably more complex than is in fact the case. Experts overestimate the importance of factors that have only a minor impact on their judgment and underestimate the extent to which their decisions are based on a few major variables. In short, people's mental models are simpler than they think, and the analyst is typically unaware not only of which variables *should* have the greatest influence, but also which variables *actually* are having the greatest influence.

All this has been demonstrated by experiments in which analysts were asked to make quantitative estimates concerning a relatively large number of cases in their area of expertise, with each case defined by a number of quantifiable factors. In one experiment, for example, stock market analysts were asked to predict long-term price appreciation for 50 securities, with each security being described in such terms as price/earnings ratio, corporate earnings growth trend, and dividend yield.[58] After completing this task, the analysts were asked to explain how they reached their conclusions, including how much weight they attached to each of the variables. They were instructed to be sufficiently explicit that another person going through the same information could apply the same judgmental rules and arrive at the same conclusions.

In order to compare this verbal rationalization with the judgmental policy reflected in the stock market analysts' actual decisions, multiple regression analysis or other similar statistical procedures can be used to develop a mathematical model of how each analyst actually weighed and combined information on the relevant variables.[59] There have been at least eight studies of this type in diverse fields,[60] including one involving

58. Paul Slovic, Dan Fleissner, and W. Scott Bauman, "Analyzing the Use of Information in Investment Decision Making: A Methodological Proposal," *The Journal of Business*, 45 (1972), pp. 283-301.

59. For a discussion of the methodology, see Slovic, Fleissner, and Bauman, op. cit.

60. For a list of references, see Paul Slovic and Sarah Lichtenstein, "Comparison of Bayesian and Regression Approaches to the Study of Information Processing in Judgment," *Organizational Behavior and Human Performance*, 6 (1971), p. 684.

prediction of future socioeconomic growth of underdeveloped nations.[61] The mathematical model based on the analyst's actual decisions is invariably a more accurate description of that analyst's decisionmaking than the analyst's own verbal description of how the judgments were made.

Although the existence of this phenomenon has been amply demonstrated, its causes are not well understood. The literature on these experiments contains only the following speculative explanation:

Possibly our feeling that we can take into account a host of different factors comes about because, although we remember that at some time or other we have attended to each of the different factors, we fail to notice that it is seldom more than one or two that we consider at any one time.[62]

When Does New Information Affect Our Judgment?

To evaluate the relevance and significance of these experimental findings in the context of intelligence analysts' experiences, it is necessary to distinguish four types of additional information that an analyst might receive:

- **Additional detail about variables already included in the analysis:** Much raw intelligence reporting falls into this category. One would not expect such supplementary information to affect the overall accuracy of the analyst's judgment, and it is readily understandable that further detail that is consistent with previous information increases the analyst's confidence. Analyses for which considerable depth of detail is available to support the conclusions tend to be more persuasive to their authors as well as to their readers.

- **Identification of additional variables:** Information on additional variables permits the analyst to take into account other factors that may affect the situation. This is the kind of additional information used in the horserace handicapper experi-

61. David A. Summers, J. Dale Taliaferro, and Donna J. Fletcher, "Subjective vs. Objective Description of Judgment Policy," *Psychonomic Science*, 18 (1970) pp. 249-250.
62. R. N. Shepard, "On Subjectively Optimum Selection Among Multiattribute Alternatives," in M. W. Shelly, II and G. L. Bryan, eds., *Human Judgments and Optimality* (New York: Wiley, 1964), p. 166.

ment. Other experiments have employed some combination of additional variables and additional detail on the same variables. The finding that judgments are based on a few critical variables rather than on the entire spectrum of evidence helps to explain why information on additional variables does not normally improve predictive accuracy. Occasionally, in situations when there are known gaps in an analyst's understanding, a single report concerning some new and previously unconsidered factor—for example, an authoritative report on a policy decision or planned coup d'etat—will have a major impact on the analyst's judgment. Such a report would fall into one of the next two categories of new information.

- **Information concerning the value attributed to variables already included in the analysis:** An example of such information would be the horserace handicapper learning that a horse he thought would carry 110 pounds will actually carry only 106. Current intelligence reporting tends to deal with this kind of information; for example, an analyst may learn that a dissident group is stronger than had been anticipated. New facts affect the accuracy of judgments when they deal with changes in variables that are critical to the estimates. Analysts' confidence in judgments based on such information is influenced by their confidence in the accuracy of the information as well as by the amount of information.

- **Information concerning which variables are most important and how they relate to each other:** Knowledge and assumptions as to which variables are most important and how they are interrelated comprise the mental model that tells the analyst how to analyze the data received. Explicit investigation of such relationships is one factor that distinguishes systematic research from current intelligence reporting and raw intelligence. In the context of the horserace handicapper experiment, for example, handicappers had to select which variables to include in their analysis. Is weight carried by a horse more, or less, important than several other variables that affect a horse's performance? Any information that affects this judgment influences how the handi-

capper analyzes the available data; that is, it affects his mental model.

The accuracy of an analyst's judgment depends upon both the accuracy of our mental model (the fourth type of information discussed above) and the accuracy of the values attributed to the key variables in the model (the third type of information discussed above). Additional detail on variables already in the analyst's mental model and information on other variables that do not in fact have a significant influence on our judgment (the first and second types of information) have a negligible impact on accuracy, but form the bulk of the raw material analysts work with. These kinds of information increase confidence because the conclusions seem to be supported by such a large body of data.

This discussion of types of new information is the basis for distinguishing two types of analysis- data-driven analysis and conceptually-driven analysis.

Data-Driven Analysis

In this type of analysis, accuracy depends primarily upon the accuracy and completeness of the available data. If one makes the reasonable assumption that the analytical model is correct and the further assumption that the analyst properly applies this model to the data, then the accuracy of the analytical judgment depends entirely upon the accuracy and completeness of the data.

Analyzing the combat readiness of a military division is an example of data-driven analysis. In analyzing combat readiness, the rules and procedures to be followed are relatively well established. The totality of these procedures comprises a mental model that influences perception of the intelligence collected on the unit and guides judgment concerning what information is important and how this information should be analyzed to arrive at judgments concerning readiness.

Most elements of the mental model can be made explicit so that other analysts may be taught to understand and follow the same analytical procedures and arrive at the same or similar results. There is broad, though not necessarily universal, agreement on what the appropriate model is. There are relatively objective standards for judging the quality

of analysis, inasmuch as the conclusions follow logically from the application of the agreed-upon model to the available data.

Conceptually Driven Analysis

Conceptually driven analysis is at the opposite end of the spectrum from data-driven analysis. The questions to be answered do not have neat boundaries, and there are many unknowns. The number of potentially relevant variables and the diverse and imperfectly understood relationships among these variables involve the analyst in enormous complexity and uncertainty. There is little tested theory to inform the analyst concerning which of the myriad pieces of information are most important and how they should be combined to arrive at probabilistic judgments.

In the absence of any agreed-upon analytical schema, analysts are left to their own devices. They interpret information with the aid of mental models that are largely implicit rather than explicit. Assumptions concerning political forces and processes in the subject country may not be apparent even to the analyst. Such models are not representative of an analytical consensus. Other analysts examining the same data may well reach different conclusions, or reach the same conclusions but for different reasons. This analysis is conceptually driven, because the outcome depends at least as much upon the conceptual framework employed to analyze the data as it does upon the data itself.

To illustrate further the distinction between data-driven and conceptually driven analysis, it is useful to consider the function of the analyst responsible for current intelligence, especially current political intelligence as distinct from longer term research. The daily routine is driven by the incoming wire service news, embassy cables, and clandestine-source reporting from overseas that must be interpreted for dissemination to consumers throughout the Intelligence Community. Although current intelligence reporting is driven by incoming information, this is not what is meant by data-driven analysis. On the contrary, the current intelligence analyst's task is often extremely concept-driven. The analyst must provide immediate interpretation of the latest, often unexpected events. Apart from his or her store of background information, the analyst may have no data other than the initial, usually incomplete report. Under these circumstances, interpretation is based upon an implicit mental model of how and why events normally transpire in the country for which the analyst is responsible. Accuracy of judgment depends almost exclusively

upon accuracy of the mental model, for there is little other basis for judgment.

It is necessary to consider how this mental model gets tested against reality, and how it can be changed to improve the accuracy of analytical judgment. Two things make it hard to change one's mental model. The first is the nature of human perception and information-processing. The second is the difficulty, in many fields, of learning what truly is an accurate model.

Partly because of the nature of human perception and information-processing, beliefs of all types tend to resist change. This is especially true of the implicit assumptions and supposedly self-evident truths that play an important role in forming mental models. Analysts are often surprised to learn that what are to them self-evident truths are by no means self-evident to others, or that self-evident truth at one point in time may be commonly regarded as uninformed assumption 10 years later.

Information that is consistent with an existing mind-set is perceived and processed easily and reinforces existing beliefs. Because the mind strives instinctively for consistency, information that is inconsistent with an existing mental image tends to be overlooked, perceived in a distorted manner, or rationalized to fit existing assumptions and beliefs.[63]

Learning to make better judgments through experience assumes systematic feedback on the accuracy of previous judgments and an ability to link the accuracy of a judgment with the particular configuration of variables that prompted an analyst to make that judgment. In practice, intelligence analysts get little systematic feedback, and even when they learn that an event they had foreseen has actually occurred or failed to occur, they typically do not know for certain whether this happened for the reasons they had foreseen. Thus, an analyst's personal experience may be a poor guide to revision of his or her mental mode.[64]

63. This refers, of course, to subconscious processes. No analyst will consciously distort information that does not fit his or her preconceived beliefs. Important aspects of the perception and processing of new information occur prior to and independently of any conscious direction, and the tendencies described here are largely the result of these subconscious or preconscious processes.

64. A similar point has been made in rebutting the belief in the accumulated wisdom of the classroom teacher. "It is actually very difficult for teachers to profit from experience. They almost never learn about their long-term successes or failures, and their short-term effects are not easily traced to the practices from which they presumably arose." B. F. Skinner, *The Technology of Teaching* (New York: Appleton-Century Crofts, 1968), pp. 112-113.

Mosaic Theory of Analysis

Understanding of the analytic process has been distorted by the mosaic metaphor commonly used to describe it. According to the mosaic theory of intelligence, small pieces of information are collected that, when put together like a mosaic or jigsaw puzzle, eventually enable analysts to perceive a clear picture of reality. The analogy suggests that accurate estimates depend primarily upon having all the pieces, that is, upon accurate and relatively complete information. It is important to collect and store the small pieces of information, as these are the raw material from which the picture is made; one never knows when it will be possible for an astute analyst to fit a piece into the puzzle. Part of the rationale for large technical intelligence collection systems is rooted in this mosaic theory.

Insights from cognitive psychology suggest that intelligence analysts do not work this way and that the most difficult analytical tasks cannot be approached in this manner. Analysts commonly find pieces that appear to fit many different pictures. Instead of a picture emerging from putting all the pieces together, analysts typically form a picture first and then select the pieces to fit. Accurate estimates depend at least as much upon the mental model used in forming the picture as upon the number of pieces of the puzzle that have been collected.

A more accurate analogy for describing how intelligence analysis should work is medical diagnosis. The doctor observes indicators (symptoms) of what is happening, uses his or her specialized knowledge of how the body works to develop hypotheses that might explain these observations, conducts tests to collect additional information to evaluate the hypotheses, then makes a diagnosis. This medical analogy focuses attention on the ability to identify and evaluate all plausible hypotheses. Collection is focused narrowly on information that will help to discriminate the relative probability of alternate hypothesis.

To the extent that this medical analogy is the more appropriate guide to understanding the analytical process, there are implications for the allocation of limited intelligence resources. While analysis and collection are both important, the medical analogy attributes more value to analysis and less to collection than the mosaic metaphor.

Conclusions

To the leaders and managers of intelligence who seek an improved intelligence product, these findings offer a reminder that this goal can be achieved by improving analysis as well as collection. There appear to be inherent practical limits on how much can be gained by efforts to improve collection. By contrast, an open and fertile field exists for imaginative efforts to improve analysis.

These efforts should focus on improving the mental models employed by analysts to interpret information and the analytical processes used to evaluate it. While this will be difficult to achieve, it is so critical to effective intelligence analysis that even small improvements could have large benefits. Specific recommendations are included the next three chapters and in Chapter 14, "Improving Intelligence Analysis."

Chapter 6

Keeping an Open Mind

Minds are like parachutes. They only function when they are open. After reviewing how and why thinking gets channeled into mental ruts, this chapter looks at mental tools to help analysts keep an open mind, question assumptions, see different perspectives, develop new ideas, and recognize when it is time to change their minds.

A new idea is the beginning, not the end, of the creative process. It must jump over many hurdles before being embraced as an organizational product or solution. The organizational climate plays a crucial role in determining whether new ideas bubble to the surface or are suppressed.

* * * * * * * * * * * * * * * * * * * *

Major intelligence failures are usually caused by failures of analysis, not failures of collection. Relevant information is discounted, misinterpreted, ignored, rejected, or overlooked because it fails to fit a prevailing mental model or mind-set.[65] The "signals" are lost in the "noise."[66] How can we ensure that analysts remain open to new experience and recognize

65. Christopher Brady, "Intelligence Failures: Plus Ca Change. . ." *Intelligence and National Security*, Vol. 8, No. 4 (October 1993). N. Cigar, "Iraq's Strategic Mindset and the Gulf War: Blueprint for Defeat," *The Journal of Strategic Studies*, Vol. 15, No. 1 (March 1992). J. J. Wirtz, *The Tet Offensive: Intelligence Failure in War* (New York, 1991). Ephraim Kam, *Surprise Attack* (Harvard University Press, 1988). Richard Betts, *Surprise Attack: Lessons for Defense Planning* (Brookings, 1982). Abraham Ben-Zvi, "The Study of Surprise Attacks," *British Journal of International Studies*, Vol. 5 (1979). *Iran: Evaluation of Intelligence Performance Prior to November 1978* (Staff Report, Subcommittee on Evaluation, Permanent Select Committee on Intelligence, US House of Representatives, January 1979). Richard Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, Vol. 31, No. 1 (October 1978). Richard W. Shryock, "The Intelligence Community Post-Mortem Program, 1973-1975," *Studies in Intelligence*, Vol. 21, No. 1 (Fall 1977). Avi Schlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," *World Politics*, Vol. 28 (April 1976). Michael Handel, *Perception, Deception, and Surprise: The Case of the Yom Kippur War* (Jerusalem: Leonard Davis Institute of International Relations, Jerusalem Paper No. 19, 1976). Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," World Politics, Vol. 16 (1964).

66. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford University Press, 1962). Roberta Wohlstetter, "Cuba and Pearl Harbor: Hindsight and Foresight," *Foreign Affairs*, Vol. 43, No. 4 (July 1965).

when long-held views or conventional wisdom need to be revised in response to a changing world?

Beliefs, assumptions, concepts, and information retrieved from memory form a mind-set or mental model that guides perception and processing of new information. The nature of the intelligence business forces us to deal with issues at an early stage when hard information is incomplete. If there were no gaps in the information on an issue or situation, and no ambiguity, it would not be an interesting intelligence problem. When information is lacking, analysts often have no choice but to lean heavily on prior beliefs and assumptions about how and why events normally transpire in a given country.

A mind-set is neither good nor bad. It is unavoidable. It is, in essence, a distillation of all that analysts think they know about a subject. It forms a lens through which they perceive the world, and once formed, it resists change.

Understanding Mental Ruts

Chapter 3 on memory suggested thinking of information in memory as somehow interconnected like a massive, multidimensional spider web. It is possible to connect any point within this web to any other point. When analysts connect the same points frequently, they form a path that makes it easier to take that route in the future. Once they start thinking along certain channels, they tend to continue thinking the same way and the path may become a rut. The path seems like the obvious and natural way to go. Information and concepts located near that path are readily available, so the same images keep coming up. Information not located near that path is less likely to come to mind.

Talking about breaking mind-sets, or creativity, or even just openness to new information is really talking about spinning new links and new paths through the web of memory. These are links among facts and concepts, or between schemata for organizing facts or concepts, that were not directly connected or only weakly connected before.

New ideas result from the association of old elements in new combinations. Previously remote elements of thought suddenly become as-

sociated in a new and useful combination.[67] When the linkage is made, the light dawns. This ability to bring previously unrelated information and ideas together in meaningful ways is what marks the open-minded, imaginative, creative analyst.

To illustrate how the mind works, consider my personal experience with a kind of mental block familiar to all analysts—writer's block. I often need to break a mental block when writing. Everything is going along fine until I come to one paragraph and get stuck. I write something down, know it is not quite right, but just cannot think of a better way to say it. However I try to change the paragraph, it still comes out basically the same way. My thinking has become channeled, and I cannot break out of that particular thought pattern to write it differently.

A common response to this problem is to take a break, work on something different for a while, and come back to the difficult portion later. With the passage of time, the path becomes less pronounced and it becomes easier to make other connections.

I have found another solution. I force myself to talk about it out loud. I close the door to my office—I am embarrassed to have anyone hear me talking to myself—and then stand up and walk around and talk. I say, okay, "What is the point of this paragraph? What are you trying to communicate?" I answer myself out loud as though talking to someone else. "The point I am trying to get across is that . . . ," and then it just comes. Saying it out loud breaks the block, and words start coming together in different ways.

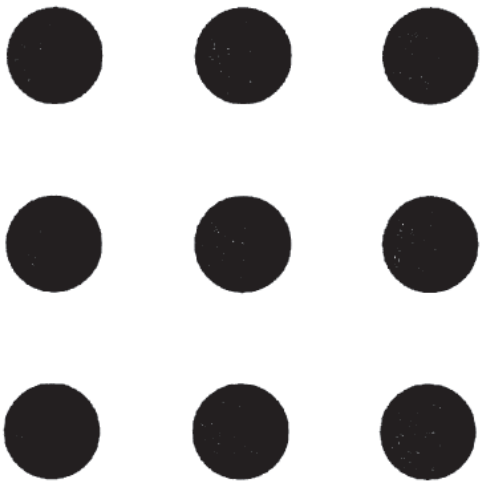
Recent research explains why this happens. Scientists have learned that written language and spoken language are processed in different parts of the brain.[68] They activate different neurons.

Problem-Solving Exercise

Before discussing how analysts can keep their minds open to new information, let us warm up to this topic with a brief exercise. Without lifting pencil from paper, draw no more than four straight lines that will cross through all nine dots in Figure 6.[69]

67. S. A. Mednick, "The Associative Basis of the Creative Process," *Psychological Review*, Vol. 69 (1962), p. 221.
68. Jerry E. Bishop, "Stroke Patients Yield Clues to Brain's Ability to Create Language," *Wall Street Journal*, Oct. 12, 1993, p.A1.
69. The puzzle is from James L. Adams, *Conceptual Blockbusting: A Guide to Better Ideas*. Second Edition (New York: W. W. Norton, 1980), p. 23.

Figure 6



After trying to solve the puzzle on your own, refer to the end of this chapter for answers and further discussion. Then consider that intelligence analysis is too often limited by similar, unconscious, self-imposed constraints or "cages of the mind."

You do not need to be constrained by conventional wisdom. It is often wrong. You do not *necessarily* need to be constrained by existing policies. They can sometimes be changed if you show a good reason for doing so. You do not *necessarily* need to be constrained by the specific analytical requirement you were given. The policymaker who originated the requirement may not have thought through his or her needs or the requirement may be somewhat garbled as it passes down through several echelons to you to do the work. You may have a better understanding than the policymaker of what he or she needs, or should have, or what is possible to do. You should not hesitate to go back up the chain of command with a suggestion for doing something a little different than what was asked for.

Mental Tools

People use various physical tools such as a hammer and saw to enhance their capacity to perform various physical tasks. People can also use simple mental tools to enhance their ability to perform mental tasks. These tools help overcome limitations in human mental machinery for perception, memory, and inference. The next few sections of this chapter discuss mental tools for opening analysts' minds to new ideas, while the next one (Chapter 7) deals with mental tools for structuring complex analytical problems.

Questioning Assumptions

It is a truism that analysts need to question their assumptions. Experience tells us that when analytical judgments turn out to be wrong, it usually was not because the information was wrong. It was because an analyst made one or more faulty assumptions that went unchallenged. The problem is that analysts cannot question everything, so where do they focus their attention?

Sensitivity Analysis. One approach is to do an informal sensitivity analysis. How sensitive is the ultimate judgment to changes in any of the major variables or driving forces in the analysis? Those linchpin assumptions that drive the analysis are the ones that need to be questioned. Analysts should ask themselves what could happen to make any of these assumptions out of date, and how they can know this has not already happened. They should try to disprove their assumptions rather than confirm them. If an analyst cannot think of anything that would cause a change of mind, his or her mind-set may be so deeply entrenched that the analyst cannot see the conflicting evidence. One advantage of the competing hypotheses approach discussed in Chapter 8 is that it helps identify the linchpin assumptions that swing a conclusion in one direction or another.

Identify Alternative Models. Analysts should try to identify alternative models, conceptual frameworks, or interpretations of the data by seeking out individuals who disagree with them rather than those who agree. Most people do not do that very often. It is much more comfortable to talk with people in one's own office who share the same basic mind-set. There are a few things that can be done as a matter of policy,

and that have been done in some offices in the past, to help overcome this tendency.

At least one Directorate of Intelligence component, for example, has had a peer review process in which none of the reviewers was from the branch that produced the report. The rationale for this was that an analyst's immediate colleagues and supervisor(s) are likely to share a common mind-set. Hence these are the individuals least likely to raise fundamental issues challenging the validity of the analysis. To avoid this mind-set problem, each research report was reviewed by a committee of three analysts from other branches handling other countries or issues. None of them had specialized knowledge of the subject. They were, however, highly accomplished analysts. Precisely because they had not been immersed in the issue in question, they were better able to identify hidden assumptions and other alternatives, and to judge whether the analysis adequately supported the conclusions.

Be Wary of Mirror Images. One kind of assumption an analyst should always recognize and question is mirror-imaging—filling gaps in the analyst's own knowledge by assuming that the other side is likely to act in a certain way because that is how the US would act under similar circumstances. To say, "if I were a Russian intelligence officer . . ." or "if I were running the Indian Government . . ." is mirror-imaging. Analysts may have to do that when they do not know how the Russian intelligence officer or the Indian Government is really thinking. But mirror-imaging leads to dangerous assumptions, because people in other cultures *do not* think the way we do. The frequent assumption that they do is what Adm. David Jeremiah, after reviewing the Intelligence Community failure to predict India's nuclear weapons testing, termed the "everybody-thinks-like-us mind-set."[70]

Failure to understand that others perceive their national interests differently from the way we perceive those interests is a constant source of problems in intelligence analysis. In 1977, for example, the Intelligence Community was faced with evidence of what appeared to be a South African nuclear weapons test site. Many in the Intelligence Community, especially those least knowledgeable about South Africa, tended to dismiss this evidence on the grounds that "Pretoria would not want a nucle-

70. Jim Wolf, "CIA Inquest Finds US Missed Indian `Mindset'," UPI wire service, June 3, 1998.

ar weapon, because there is no enemy they could effectively use it on."[71] The US perspective on what is in another country's national interest is usually irrelevant in intelligence analysis. Judgment must be based on how the other country perceives its national interest. If the analyst cannot gain insight into what the other country is thinking, mirror-imaging may be the only alternative, but analysts should never get caught putting much confidence in that kind of judgment.

Seeing Different Perspectives

Another problem area is looking at familiar data from a different perspective. If you play chess, you know you can see your own options pretty well. It is much more difficult to see all the pieces on the board as your opponent sees them, and to anticipate how your opponent will react to your move. That is the situation analysts are in when they try to see how the US Government's actions look from another country's perspective. Analysts constantly have to move back and forth, first seeing the situation from the US perspective and then from the other country's perspective. This is difficult to do, as you experienced with the picture of the old woman/young woman in Chapter 2 on perception.

Several techniques for seeing alternative perspectives exploit the general principle of coming at the problem from a different direction and asking different questions. These techniques break your existing mind-set by causing you to play a different and unaccustomed role.

Thinking Backwards. One technique for exploring new ground is thinking backwards. As an intellectual exercise, start with an assumption that some event you did not expect has actually occurred. Then, put yourself into the future, looking back to explain how this could have happened. Think what must have happened six months or a year earlier to set the stage for that outcome, what must have happened six months or a year before that to prepare the way, and so on back to the present.

Thinking backwards changes the focus from whether something might happen to how it might happen. Putting yourself into the future creates a different perspective that keeps you from getting anchored in the present. Analysts will often find, to their surprise, that they can construct a quite plausible scenario for an event they had previously thought unlikely. Thinking backwards is particularly helpful for events that have

71. Discussion with Robert Jaster, former National Intelligence Officer for Southern Africa.

a low probability but very serious consequences should they occur, such as a collapse or overthrow of the Saudi monarchy.

Crystal Ball. The crystal ball approach works in much the same way as thinking backwards.[72] Imagine that a "perfect" intelligence source (such as a crystal ball) has told you a certain assumption is wrong. You must then develop a scenario to explain how this could be true. If you can develop a plausible scenario, this suggests your assumption is open to some question.

Role playing. Role playing is commonly used to overcome constraints and inhibitions that limit the range of one's thinking. Playing a role changes "where you sit." It also gives one license to think and act differently. Simply trying to imagine how another leader or country will think and react, which analysts do frequently, is not role playing. One must actually act out the role and become, in a sense, the person whose role is assumed. It is only "living" the role that breaks an analyst's normal mental set and permits him or her to relate facts and ideas to each other in ways that differ from habitual patterns. An analyst cannot be expected to do this alone; some group interaction is required, with different analysts playing different roles, usually in the context of an organized simulation or game.

Most of the gaming done in the Defense Department and in the academic world is rather elaborate and requires substantial preparatory work. It does not have to be that way. The preparatory work can be avoided by starting the game with the current situation already known to analysts, rather than with a notional scenario that participants have to learn. Just one notional intelligence report is sufficient to start the action in the game. In my experience, it is possible to have a useful political game in just one day with almost no investment in preparatory work.

Gaming gives no "right" answer, but it usually causes the players to see some things in a new light. Players become very conscious that "where you stand depends on where you sit." By changing roles, the participants see the problem in a different context. This frees the mind to think differently.

Devil's Advocate. A devil's advocate is someone who defends a minority point of view. He or she may not necessarily agree with that view,

72. Jon Fallesen, Rex Michel, James Lussier, and Julia Pounds, "Practical Thinking: Innovation in Battle Command Instruction" *(Technical Report 1037, US Army Research Institute for the Behavioral and Social Sciences*, January 1996).

but may choose or be assigned to represent it as strenuously as possible. The goal is to expose conflicting interpretations and show how alternative assumptions and images make the world look different. It often requires time, energy, and commitment to see how the world looks from a different perspective.[73]

Imagine that you are the boss at a US facility overseas and are worried about the possibility of a terrorist attack. A standard staff response would be to review existing measures and judge their adequacy. There might well be pressure—subtle or otherwise—from those responsible for such arrangements to find them satisfactory. An alternative or supplementary approach would be to name an individual or small group as a devil's advocate assigned to develop actual plans for launching such an attack. The assignment to think like a terrorist liberates the designated person(s) to think unconventionally and be less inhibited about finding weaknesses in the system that might embarrass colleagues, because uncovering any such weaknesses is the assigned task.

Devil's advocacy has a controversial history in the Intelligence Community. Suffice it to say that some competition between conflicting views is healthy and must be encouraged; all-out political battle is counterproductive.

Recognizing When To Change Your Mind

As a general rule, people are too slow to change an established view, as opposed to being too willing to change. The human mind is conservative. It resists change. Assumptions that worked well in the past continue to be applied to new situations long after they have become outmoded.

Learning from Surprise. A study of senior managers in industry identified how some successful managers counteract this conservative bent. They do it, according to the study,

> By paying attention to their feelings of surprise when a particular fact does not fit their prior understanding, and then by highlighting rather than denying the novelty. Although surprise made them feel uncomfortable, it made them take the cause [of the surprise] seriously and inquire into it. . . . Rather than

73. For an interesting discussion of the strengths and potential weaknesses of the "devil's advocate" approach, see Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), pp. 415-418.

> deny, downplay, or ignore disconfirmation [of their prior view], successful senior managers often treat it as friendly and in a way cherish the discomfort surprise creates. As a result, these managers often perceive novel situations early on and in a frame of mind relatively undistorted by hidebound notions.[74]

Analysts should keep a record of unexpected events and think hard about what they might mean, not disregard them or explain them away. It is important to consider whether these surprises, however small, are consistent with some alternative hypothesis. One unexpected event may be easy to disregard, but a pattern of surprises may be the first clue that your understanding of what is happening requires some adjustment, is at best incomplete, and may be quite wrong.

Strategic Assumptions vs. Tactical Indicators. Abraham Ben-Zvi analyzed five cases of intelligence failure to foresee a surprise attack.[75] He made a useful distinction between estimates based on strategic assumptions and estimates based on tactical indications. Examples of strategic assumptions include the US belief in 1941 that Japan wished to avoid war at all costs because it recognized US military superiority, and the Israeli belief in 1973 that the Arabs would not attack Israel until they obtained sufficient air power to secure control of the skies. A more recent instance was the 1998 Indian nuclear test, which was widely viewed as a surprise and, at least in part, as a failure by the experts to warn of an impending test. The incorrect strategic assumption was that the new Indian Government would be dissuaded from testing nuclear weapons for fear of US economic sanctions.[76]

Tactical indicators are specific reports of preparations or intent to initiate hostile action or, in the recent Indian case, reports of preparations for a nuclear test. Ben-Zvi found that whenever strategic assumptions and tactical indicators of impending attack converged, an immediate threat was perceived and appropriate precautionary measures were taken.

74. Daniel J. Isenberg, "How Senior Managers Think," in David Bell, Howard Raiffa, and Amos Tversky, *Decision Making: Descriptive, Normative, and Prescriptive Interactions* (Cambridge University Press, 1988), p. 535.
75. Abraham Ben Zvi, "Hindsight and Foresight: A Conceptual Framework for the Analysis of Surprise Attacks," *World Politics*, April 1976.
76. Transcript of Admiral David Jeremiah's news conference on the Intelligence Community's performance concerning the Indian nuclear test, fourth and fifth paragraphs and first Q and A, 2 June 1998.

When discrepancies existed between tactical indicators and strategic assumptions in the five cases Ben-Zvi analyzed, the strategic assumptions always prevailed, and they were never reevaluated in the light of the increasing flow of contradictory information. Ben-Zvi concludes that tactical indicators should be given increased weight in the decisionmaking process. At a minimum, the emergence of tactical indicators that contradict our strategic assumption should trigger a higher level of intelligence alert. It may indicate that a bigger surprise is on the way.

Chapter 8, "Analysis of Competing Hypotheses," provides a framework for identifying surprises and weighing tactical indicators and other forms of current evidence against longstanding assumptions and beliefs.

Stimulating Creative Thinking

Imagination and creativity play important roles in intelligence analysis as in most other human endeavors. Intelligence judgments require the ability to imagine possible causes and outcomes of a current situation. All possible outcomes are not given. The analyst must think of them by imagining scenarios that explicate how they might come about. Similarly, imagination as well as knowledge is required to reconstruct how a problem appears from the viewpoint of a foreign government. Creativity is required to question things that have long been taken for granted. The fact that apples fall from trees was well known to everyone. Newton's creative genius was to ask "why?" Intelligence analysts, too, are expected to raise new questions that lead to the identification of previously unrecognized relationships or to possible outcomes that had not previously been foreseen.

A creative analytical product shows a flair for devising imaginative or innovative—but also accurate and effective—ways to fulfill any of the major requirements of analysis: gathering information, analyzing information, documenting evidence, and/or presenting conclusions. Tapping unusual sources of data, asking new questions, applying unusual analytic methods, and developing new types of products or new ways of fitting analysis to the needs of consumers are all examples of creative activity.

A person's intelligence, as measured by IQ tests, has little to do with creativity, but the organizational environment exercises a major influence. New but appropriate ideas are most likely to arise in an organizational climate that nurtures their development and communication.

The old view that creativity is something one is born with, and that it cannot be taught or developed, is largely untrue. While native talent, per se, is important and may be immutable, it is possible to learn to employ one's innate talents more productively. With understanding, practice, and conscious effort, analysts can learn to produce more imaginative, innovative, creative work.

There is a large body of literature on creativity and how to stimulate it. At least a half-dozen different methods have been developed for teaching, facilitating, or liberating creative thinking. All the methods for teaching or facilitating creativity are based on the assumption that the *process* of thinking can be separated from the *content* of thought. One learns mental strategies that can be applied to any subject.

It is not our purpose here to review commercially available programs for enhancing creativity. Such programmatic approaches can be applied more meaningfully to problems of new product development, advertising, or management than to intelligence analysis. It is relevant, however, to discuss several key principles and techniques that these programs have in common, and that individual intelligence analysts or groups of analysts can apply in their work.

Intelligence analysts must generate ideas concerning potential causes or explanations of events, policies that might be pursued or actions taken by a foreign government, possible outcomes of an existing situation, and variables that will influence which outcome actually comes to pass. Analysts also need help to jog them out of mental ruts, to stimulate their memories and imaginations, and to perceive familiar events from a new perspective.

Here are some of the principles and techniques of creative thinking that can be applied to intelligence analysis.

Deferred Judgment. The principle of deferred judgment is undoubtedly the most important. The idea-generation phase of analysis should be separated from the idea-evaluation phase, with evaluation deferred until all possible ideas have been brought out. This approach runs contrary to the normal procedure of thinking of ideas and evaluating them concurrently. Stimulating the imagination and critical thinking are both important, but they do not mix well. A judgmental attitude dampens the imagination, whether it manifests itself as self-censorship of one's own ideas or fear of critical evaluation by colleagues or supervisors. Idea generation should be a freewheeling, unconstrained, uncritical process.

New ideas are, by definition, unconventional, and therefore likely to be suppressed, either consciously or unconsciously, unless they are born in a secure and protected environment. Critical judgment should be suspended until after the idea-generation stage of analysis has been completed. A series of ideas should be written down and then evaluated later. This applies to idea searching by individuals as well as brainstorming in a group. Get all the ideas out on the table before evaluating any of them.

Quantity Leads to Quality. A second principle is that quantity of ideas eventually leads to quality. This is based on the assumption that the first ideas that come to mind will be those that are most common or usual. It is necessary to run through these conventional ideas before arriving at original or different ones. People have habitual ways of thinking, ways that they continue to use because they have seemed successful in the past. It may well be that these habitual responses, the ones that come first to mind, are the best responses and that further search is unnecessary. In looking for usable new ideas, however, one should seek to generate as many ideas as possible before evaluating any of them.

No Self-Imposed Constraints. A third principle is that thinking should be allowed—indeed encouraged—to range as freely as possible. It is necessary to free oneself from self-imposed constraints, whether they stem from analytical habit, limited perspective, social norms, emotional blocks, or whatever.

Cross-Fertilization of Ideas. A fourth principle of creative problem-solving is that cross-fertilization of ideas is important and necessary. Ideas should be combined with each other to form more and even better ideas. If creative thinking involves forging new links between previously unrelated or weakly related concepts, then creativity will be stimulated by any activity that brings more concepts into juxtaposition with each other in fresh ways. Interaction with other analysts is one basic mechanism for this. As a general rule, people generate more creative ideas when teamed up with others; they help to build and develop each other's ideas. Personal interaction stimulates new associations between ideas. It also induces greater effort and helps maintain concentration on the task.

These favorable comments on group processes are not meant to encompass standard committee meetings or coordination processes that force consensus based on the lowest common denominator of agreement. My positive words about group interaction apply primarily to

brainstorming sessions aimed at generating new ideas and in which, according to the first principle discussed above, all criticism and evaluation are deferred until after the idea generation stage is completed.

Thinking things out alone also has its advantages: individual thought tends to be more structured and systematic than interaction within a group. Optimal results come from alternating between individual thinking and team effort, using group interaction to generate ideas that supplement individual thought. A diverse group is clearly preferable to a homogeneous one. Some group participants should be analysts who are not close to the problem, inasmuch as their ideas are more likely to reflect different insights.

Idea Evaluation. All creativity techniques are concerned with stimulating the flow of ideas. There are no comparable techniques for determining which ideas are best. The procedures are, therefore, aimed at idea generation rather than idea evaluation. The same procedures do aid in evaluation, however, in the sense that ability to generate more alternatives helps one see more potential consequences, repercussions, and effects that any single idea or action might entail.

Organizational Environment

A new idea is not the end product of the creative process. Rather, it is the beginning of what is sometimes a long and tortuous process of translating an idea into an innovative product. The idea must be developed, evaluated, and communicated to others, and this process is influenced by the organizational setting in which it transpires. The potentially useful new idea must pass over a number of hurdles before it is embraced as an organizational product.

The following paragraphs describe in some detail research conducted by Frank Andrews to investigate the relationship among creative ability, organizational setting, and innovative research products.[77] The subjects of this research were 115 scientists, each of whom had directed a research project dealing with social-psychological aspects of disease. These scientists were given standardized tests that measure creative ability and intelligence. They were also asked to fill out an extensive questionnaire

77. Frank M. Andrews, "Social and Psychological Factors Which Influence the Creative Process," in Irving A. Taylor and Jacob W. Getzels, eds., *Perspectives in Creativity* (Chicago, Aldine Publishing, 1975).

concerning the environment in which their research was conducted. A panel of judges composed of the leading scientists in the field of medical sociology was asked to evaluate the principal published results from each of the 115 research projects.

Judges evaluated the research results on the basis of productivity and innovation. Productivity was defined as the "extent to which the research represents an addition to knowledge along established lines of research or as extensions of previous theory." Innovativeness was defined as "additions to knowledge through new lines of research or the development of new theoretical statements of findings that were not explicit in previous theory.[78] Innovation, in other words, involved raising new questions and developing new approaches to the acquisition of knowledge, as distinct from working productively within an already established framework. This same definition applies to innovation in intelligence analysis.

Andrews found virtually no relationship between the scientists' creative ability and the innovativeness of their research. (There was also no relationship between level of intelligence and innovativeness.) Those who scored high on tests of creative ability did not necessarily receive high ratings from the judges evaluating the innovativeness of their work. A possible explanation is that either creative ability or innovation, or both, were not measured accurately, but Andrews argues persuasively for another view. Various social and psychological factors have so great an effect on the steps needed to translate creative ability into an innovative research product that there is no measurable effect traceable to creative ability alone. In order to document this conclusion, Andrews analyzed data from the questionnaires in which the scientists described their work environment.

Andrews found that scientists possessing more creative ability produced more innovative work only under the following favorable conditions:

- When the scientist perceived himself or herself as responsible for initiating new activities. The opportunity for innovation, and the encouragement of it, are—not surprisingly—important variables.

78. Ibid., p. 122.

- When the scientist had considerable control over decisionmaking concerning his or her research program—in other words, the freedom to set goals, hire research assistants, and expend funds. Under these circumstances, a new idea is less likely to be snuffed out before it can be developed into a creative and useful product.

- When the scientist felt secure and comfortable in his or her professional role. New ideas are often disruptive, and pursuing them carries the risk of failure. People are more likely to advance new ideas if they feel secure in their positions.

- When the scientist's administrative superior "stayed out of the way." Research is likely to be more innovative when the superior limits himself or herself to support and facilitation rather than direct involvement.

- When the project was relatively small with respect to the number of people involved, budget, and duration. Small size promotes flexibility, and this in turn is more conducive to creativity.

- When the scientist engaged in other activities, such as teaching or administration, in addition to the research project. Other work may provide useful stimulation or help one identify opportunities for developing or implementing new ideas. Some time away from the task, or an incubation period, is generally recognized as part of the creative process."

The importance of any one of these factors was not very great, but their impact was cumulative. The presence of all or most of these conditions exerted a strongly favorable influence on the creative process. Conversely, the absence of these conditions made it quite unlikely that even highly creative scientists could develop their new ideas into innovative research results. Under unfavorable conditions, the most creatively inclined scientists produced even less innovative work than their less imaginative colleagues, presumably because they experienced greater frustration with their work environment.

In summary, some degree of innate creative talent may be a necessary precondition for innovative work, but it is unlikely to be of much value unless the organizational environment in which that work is done nurtures the development and communication of new ideas. Under unfavorable circumstances, an individual's creative impulses probably will find expression outside the organization.

There are, of course, exceptions to the rule. Some creativity occurs even in the face of intense opposition. A hostile environment can be stimulating, enlivening, and challenging. Some people gain satisfaction from viewing themselves as lonely fighters in the wilderness, but when it comes to conflict between a large organization and a creative individual within it, the organization generally wins.

Recognizing the role of organizational environment in stimulating or suppressing creativity points the way to one obvious set of measures to enhance creative organizational performance. Managers of analysis, from first-echelon supervisors to the Director of Central Intelligence, should take steps to strengthen and broaden the perception among analysts that new ideas are welcome. This is not easy; creativity implies criticism of that which already exists. It is, therefore, inherently disruptive of established ideas and organizational practices.

Particularly within his or her own office, an analyst needs to enjoy a sense of security, so that partially developed ideas may be expressed and bounced off others as sounding boards with minimal fear of criticism or ridicule for deviating from established orthodoxy. At its inception, a new idea is frail and vulnerable. It needs to be nurtured, developed, and tested in a protected environment before being exposed to the harsh reality of public criticism. It is the responsibility of an analyst's immediate supervisor and office colleagues to provide this sheltered environment.

Conclusions

Creativity, in the sense of new and useful ideas, is at least as important in intelligence analysis as in any other human endeavor. Procedures to enhance innovative thinking are not new. Creative thinkers have employed them successfully for centuries. The only new elements—and even they may not be new anymore—are the grounding of these procedures in psychological theory to explain how and why they work, and their formalization in systematic creativity programs.

Learning creative problem-solving techniques does not change an analyst's native-born talents but helps an analyst achieve his or her full potential. Most people have the ability to be more innovative than they themselves realize. The effectiveness of these procedures depends, in large measure, upon the analyst's motivation, drive, and perseverance in taking the time required for thoughtful analysis despite the pressures of day-to-day duties, mail, and current intelligence reporting.

A questioning attitude is a prerequisite to a successful search for new ideas. Any analyst who is confident that he or she already knows the answer, and that this answer has not changed recently, is unlikely to produce innovative or imaginative work. Another prerequisite to creativity is sufficient strength of character to suggest new ideas to others, possibly at the expense of being rejected or even ridiculed on occasion. "The ideas of creative people often lead them into direct conflict with the trends of their time, and they need the courage to be able to stand alone."[79]

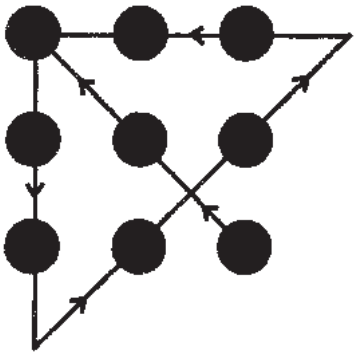
79. Robin Hogarth, *Judgment and Choice* (New York: Wiley, 1980), p. 117.

SOLUTIONS TO PUZZLE PRESENTED IN FIGURE 6

Figure 6

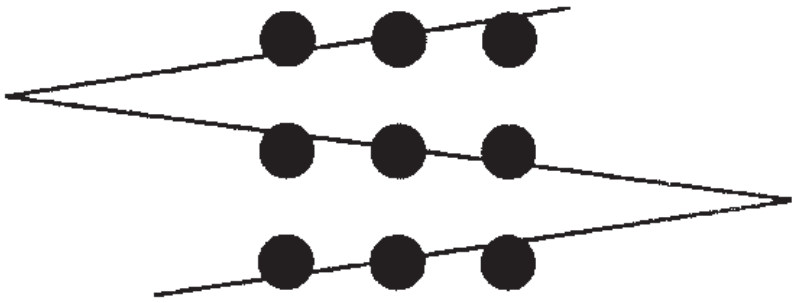
The nine-dots puzzle illustrated in Figure 6 above and earlier in this chapter is difficult to solve only if one defines the problem to narrowly. A surprising number of people assume they are not supposed to let the pencil go outside an imaginary square drawn around the nine dots.

Figure 7



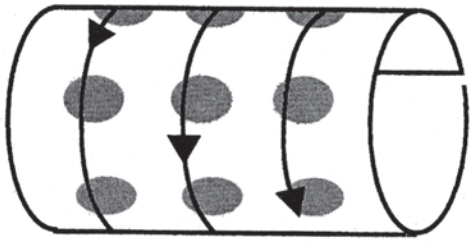
This unconscious constraint exists only in the mind of the problem-solver; it is not specified in the definition of the problem. With no limit on the length of lines, it should be relatively easy to come up with the answer shown in Figure 7.

Figure 8



Another common, unconscious constraint is the assumption that the lines must pass through the center of the dots. This constraint, too, exists only in the mind of the problem solver. Without it, the three-line solution in Figure 8 becomes rather obvious.

Figure 9



A more subtle and certainly more pervasive mental block is the assumption that such problems must be solved within a two-dimensional-plane. By rolling the paper to form a cylinder, it becomes possible to draw a single straight line that spirals through all nine dots, as in Figure 9.

Chapter 7

Structuring Analytical Problems

This chapter discusses various structures for decomposing and externalizing complex analytical problems when we cannot keep all the relevant factors in the forefront of our consciousness at the same time.

Decomposition means breaking a problem down into its component parts. Externalization means getting the problem out of our heads and into some visible form that we can work with.

* * * * * * * * * * * * * * * * * * * *

The discussion of working memory in Chapter 3 indicated that "The Magic Number Seven—Plus or Minus Two"[80] is the number of things most people can keep in working memory at one time. To experience firsthand this limitation on working memory while doing a mental task, try multiplying in your head any pair of two-digit numbers- for example, 46 times 78. On paper, this is a simple problem, but most people cannot keep track of that many numbers in their head.

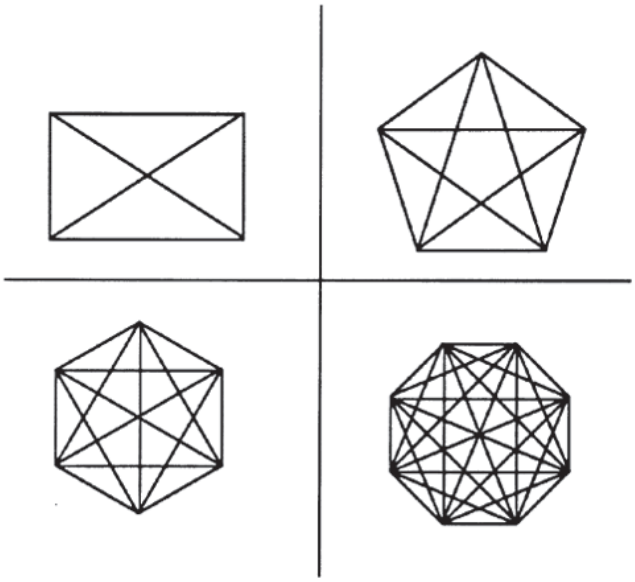
The limited capacity of working memory is the source of many problems in doing intelligence analysis. It is useful to consider just how complicated analysis can get, and how complexity might outstrip your working memory and impede your ability to make accurate judgments. Figure 10 illustrates how complexity increases geometrically as the number of variables in an analytical problem increases. The four-sided square shows that when a problem has just four variables, there are six possible interrelationships between those variables. With the pentagon, the five variables have 10 possible interrelationships. With six and eight variables, respectively, there are 15 and 28 possible interrelationships between variables.

The number of possible relationships between variables grows geometrically as the number of variables increases.

There are two basic tools for dealing with complexity in analysis—decomposition and externalization.

80. George A. Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information." *The Psychological Review*, Vol. 63, No. 2 (March 1956).

Figure 10



The number of possible relationships between variables grows geometrically as the number of variables increases.

Decomposition means breaking a problem down into its component parts. That is, indeed, the essence of analysis. Webster's Dictionary defines analysis as division of a complex whole into its parts or elements.[81]

The spirit of decision analysis is to divide and conquer: Decompose a complex problem into simpler problems, get one's thinking straight in these simpler problems, paste these analyses together with a logical glue . . .[82]

Externalization means getting the decomposed problem out of one's head and down on paper or on a computer screen in some simplified form that shows the main variables, parameters, or elements of the problem and how they relate to each other. Writing down the multiplication problem, 46 times 78, is a very simple example of externalizing an ana-

81. *Webster's Ninth New Collegiate Dictionary*, 1988.
82. Howard Raiffa, *Decision Analysis* (Reading, MA: Addison-Wesley, 1968).

lytical problem. When it is down on paper, one can easily manipulate one part of the problem at a time and often be more accurate than when trying to multiply the numbers in one's head.

I call this drawing a picture of your problem. Others call it making a model of your problem. It can be as simple as just making lists pro and con.

This recommendation to compensate for limitations of working memory by decomposing and externalizing analytical problems is not new. The following quote is from a letter Benjamin Franklin wrote in 1772 to the great British scientist Joseph Priestley, the discoverer of oxygen:

> In the affair of so much importance to you, wherein you ask my advice, I cannot for want of sufficient premises, advise you what to determine, but if you please I will tell you how. When those difficult cases occur, they are difficult, chiefly because while we have them under consideration, all the reasons pro and con are not present to the mind at the same time, but sometimes one set present themselves, and at other times another, the first being out of sight. Hence the various purposes or inclinations that alternatively prevail, and the uncertainty that perplexes us.
>
> To get over this, my way is to divide half a sheet of paper by a line into two columns; writing over the one Pro, and over the other Con. Then, during three or four days of consideration, I put down under the different heads short hints of the different motives, that at different times occur to me, for or against the measure.
>
> When I have thus got them all together in one view, I endeavor to estimate their respective weights; and where I find two, one on each side, that seem equal, I strike them both out. If I find a reason pro equal to some two reasons con, I strike out the three . . . and thus proceeding I find at length where the balance lies; and if, after a day or two of further consideration, nothing new that is of importance occurs on either side, I come to a determination accordingly.

> And, though the weight of reasons cannot be taken with the precision of algebraic quantities, yet when each is thus considered, separately and comparatively, and the whole lies before me, I think I can judge better, and am less liable to make a rash step, and in fact I have found great advantage from this kind of equation. . . . [83]

It is noteworthy that Franklin over 200 years ago ident2ified the problem of limited working memory and how it affects one's ability to make judgments. As Franklin noted, decision problems are difficult because people cannot keep all the pros and cons in mind at the same time. We focus first on one set of arguments and then on another, ". . . hence the various purposes and inclinations that alternatively prevail, and the uncertainty that perplexes us."

Franklin also identified the solution—getting all the pros and cons out of his head and onto paper in some visible, shorthand form. The fact that this topic was part of the dialogue between such illustrious individuals reflects the type of people who use such analytical tools. These are not aids to be used by weak analysts but unneeded by the strong. Basic limitations of working memory affect everyone. It is the more astute and careful analysts who are most conscious of this and most likely to recognize the value gained by applying these very simple tools.

Putting ideas into visible form ensures that they will last. They will lie around for days goading you into having further thoughts. Lists are effective because they exploit people's tendency to be a bit compulsive—we want to keep adding to them. They let us get the obvious and habitual answers out of the way, so that we can add to the list by thinking of other ideas beyond those that came first to mind. One specialist in creativity has observed that "for the purpose of moving our minds, pencils can serve as crowbars"[84]—just by writing things down and making lists that stimulate new associations.

With the key elements of a problem written down in some abbreviated form, it is far easier to work with each of the parts while still keeping the problem as a whole in view. Analysts can generally take account of more factors than when making a global judgment. They can manipulate

83. J. Bigelow, ed., *The Complete Works of Benjamin Franklin* (New York: Putnam, 1887), p. 522.
84. Alex Osborn, *Applied Imagination*, Revised Edition (New York: Scribner's, 1979), p. 202.

individual elements of the problem to examine the many alternatives available through rearranging, combining, or modifying them. Variables may be given more weight or deleted, causal relationships reconceptualized, or conceptual categories redefined. Such thoughts may arise spontaneously, but they are more likely to occur when an analyst looks at each element, one by one, and asks questions designed to encourage and facilitate consideration of alternative interpretations.

Problem Structure

Anything that has parts also has a structure that relates these parts to each other. One of the first steps in doing analysis is to determine an appropriate structure for the analytical problem, so that one can then identify the various parts and begin assembling information on them. Because there are many different kinds of analytical problems, there are also many different ways to structure analysis.

Lists such as Franklin made are one of the simplest structures. An intelligence analyst might make lists of relevant variables, early warning indicators, alternative explanations, possible outcomes, factors a foreign leader will need to take into account when making a decision, or arguments for and against a given explanation or outcome.

Other tools for structuring a problem include outlines, tables, diagrams, trees, and matrices, with many sub-species of each. For example, trees include decision trees and fault trees. Diagrams includes causal diagrams, influence diagrams, flow charts, and cognitive maps.

Consideration of all those tools is beyond the scope of this book, but several such tools are discussed. Chapter 11, "Biases in Perception of Cause and Effect," has a section on Illusory Correlation that uses a (2x2) contingency table to structure analysis of the question: Is deception most likely when the stakes are very high? Chapter 8, "Analysis of Competing Hypotheses," is arguably the most useful chapter in this book. It recommends using a matrix to array evidence for and against competing hypotheses to explain what is happening now or estimate what may happen in the future.

The discussion below also uses a matrix to illustrate decomposition and externalization and is intended to prepare you for the next chapter on "Analysis of Competing Hypotheses." It demonstrates how to apply

these tools to a type of decision commonly encountered in our personal lives.

Car Purchase Matrix

In choosing among alternative purchases, such as when buying a car, a new computer, or a house, people often want to maximize their satisfaction on a number of sometimes-conflicting dimensions. They want a car at the lowest possible price, with the lowest maintenance cost, highest resale value, slickest styling, best handling, best gas mileage, largest trunk space, and so forth. They can't have it all, so they must decide what is most important and make tradeoffs. As Ben Franklin said, the choice is sometimes difficult. We vacillate between one choice and another, because we cannot keep in working memory at the same time all the characteristics of all the choices. We think first of one and then the other.

To handle this problem analytically, follow the divide-and-conquer principle and "draw a picture" of the problem as a whole that helps you identify and make the tradeoffs. The component parts of the car purchase problem are the cars you are considering buying and the attributes or dimensions you want to maximize. After identifying the desirable attributes that will influence your decision, weigh how each car stacks up on each attribute. A matrix is the appropriate tool for keeping track of your judgments about each car and each attribute, and then putting all the parts back together to make a decision.

Start by listing the important attributes you want to maximize, as shown for example in Figure 11.

Figure 11

Price

Maintenance Cost

Styling

Gas Mileage

Comfort

Handling

Next, quantify the relative importance of each attribute by dividing 100 percent among them. In other words, ask yourself what percentage of the decision should be based on price, on styling, etc. This forces you to ask relevant questions and make decisions you might have glossed over if you had not broken the problem down in this manner. How important is price versus styling, really? Do you really care what it looks like from the outside, or are you mainly looking for comfort on the inside and how

Figure 12

Price	**30%**
Operating Cost	**10%**
Styling	**20%**
Comfort	**20%**
Handling	**15%**
Safety	**5%**
Total	**100%**

it drives? Should safety be included in your list of important attributes? Because poor gas mileage can be offset by lower maintenance cost for repairs, perhaps both should be combined into a single attribute called operating cost.

This step might produce a result similar to Figure 12, depending on your personal preferences. If you do this together with your spouse, the exact basis of any difference of opinion will become immediately apparent and can be quantified.

Figure 13

	% Value	Car 1	Car 2	Car 3
Price	30%	3.5%	3.0%	3.5%
Operating Cost	10%	3.5%	2.0%	4.5%
Styling	20%	2.5%	4.5%	3.0%
Comfort	20%	4.0%	2.5%	3.5%
Handling	15%	3.0%	4.0%	3.0%
Safety	5%	3.5%	2.5%	4%

Next, identify the cars you are considering and judge how each one ranks on each of the six attributes shown in Figure 12. Set up a matrix as shown in Figure 13 and work across the rows of the matrix. For each attribute, take 10 points and divide it among the three cars based on how well they meet the requirements of that attribute. (This is the same as taking 100 percent and dividing it among the cars, but it keeps the numbers lower when you get to the next step.)

You now have a picture of your analytical problem—the comparative value you attribute to each of the principal attributes of a new car and a comparison of how various cars satisfy those desired attributes. If you have narrowed it down to three alternatives, your matrix will look something like Figure 13:

When all the cells of the matrix have been filled in, you can then calculate which car best suits your preferences. Multiply the percentage value you assigned to each attribute by the value you assigned to that attribute for each car, which produces the result in Figure 14. If the percentage values you assigned to each attribute accurately reflect your preferences, and if each car has been analyzed accurately, the analysis shows you will gain more satisfaction from the purchase of Car 3 than either of the alternatives.

Figure 14

	% Value	Car 1	Car 2	Car 3
Price	30%	105	90	105
Operating Cost	10%	35	20	45
Styling	20%	50	90	60
Comfort	20%	80	50	70
Handling	15%	45	60	45
Safety	5%	17.5	12.5	20
Totals		332.5	322.5	345

At this point, you do a sensitivity analysis to determine whether plausible changes in some values in the matrix would swing the decision to a different car. Assume, for example, that your spouse places different values than you on the relative importance of price versus styling. You can insert your spouse's percentage values for those two attributes and see if that makes a difference in the decision. (For example, one could reduce the importance of price to 20 percent and increase styling to 30 percent. That is still not quite enough to switch the choice to Car 2, which rates highest on styling.)

There is a technical name for this type of analysis. It is called Multiattribute Utility Analysis, and there are complex computer programs for doing it. In simplified form, however, it requires only pencil and paper and high school arithmetic. It is an appropriate structure for any purchase decision in which you must make tradeoffs between multiple competing preferences.

Conclusions

The car purchase example was a warmup for the following chapter. It illustrates the difference between just sitting down and thinking about a problem and really *analyzing* a problem. The essence of analysis is breaking down a problem into its component parts, assessing each part separately, then putting the parts back together to make a decision. The matrix in this example forms a "picture" of a complex problem by getting it out of our head and onto paper in a logical form that enables you to consider each of the parts individually.

You certainly would not want to do this type of analysis for all your everyday personal decisions or for every intelligence judgment. You may wish to do it, however, for an especially important, difficult, or controversial judgment, or when you need to leave an audit trail showing how you arrived at a judgment. The next chapter applies decomposition, externalization, and the matrix structure to a common type of intelligence problem.

Chapter 8

Analysis of Competing Hypotheses

Analysis of competing hypotheses, sometimes abbreviated ACH, is a tool to aid judgment on important issues requiring careful weighing of alternative explanations or conclusions. It helps an analyst overcome, or at least minimize, some of the cognitive limitations that make prescient intelligence analysis so difficult to achieve.

ACH is an eight-step procedure grounded in basic insights from cognitive psychology, decision analysis, and the scientific method. It is a surprisingly effective, proven process that helps analysts avoid common analytic pitfalls. Because of its thoroughness, it is particularly appropriate for controversial issues when analysts want to leave an audit trail to show what they considered and how they arrived at their judgment.[85]

* * * * * * * * * * * * * * * * * * * *

When working on difficult intelligence issues, analysts are, in effect, choosing among several alternative hypotheses. Which of several possible explanations is the correct one? Which of several possible outcomes is the most likely one? As previously noted, this book uses the term "hypothesis" in its broadest sense as a potential explanation or conclusion that is to be tested by collecting and presenting evidence.

Analysis of competing hypotheses (ACH) requires an analyst to explicitly identify all the reasonable alternatives and have them compete against each other for the analyst's favor, rather than evaluating their plausibility one at a time.

The way most analysts go about their business is to pick out what they suspect intuitively is the most likely answer, then look at the available information from the point of view of whether or not it supports this answer. If the evidence seems to support the favorite hypothesis,

85. The analysis of competing hypotheses procedure was developed by the author for use by intelligence analysts dealing with a set of particularly difficult problems.

analysts pat themselves on the back ("See, I knew it all along!") and look no further. If it does not, they either reject the evidence as misleading or develop another hypothesis and go through the same procedure again. Decision analysts call this a satisficing strategy. (See Chapter 4, Strategies for Analytical Judgment.) Satisficing means picking the first solution that seems satisfactory, rather than going through all the possibilities to identify the very best solution. There may be several seemingly satisfactory solutions, but there is only one best solution.

Chapter 4 discussed the weaknesses in this approach. The principal concern is that if analysts focus mainly on trying to confirm one hypothesis they think is probably true, they can easily be led astray by the fact that there is so much evidence to support their point of view. They fail to recognize that most of this evidence is also consistent with other explanations or conclusions, and that these other alternatives have not been refuted.

Simultaneous evaluation of multiple, competing hypotheses is very difficult to do. To retain three to five or even seven hypotheses in working memory and note how each item of information fits into each hypothesis is beyond the mental capabilities of most people. It takes far greater mental agility than listing evidence supporting a single hypothesis that was pre-judged as the most likely answer. It can be accomplished, though, with the help of the simple procedures discussed here. The box below contains a step-by-step outline of the ACH process.

Step 1

Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.

Psychological research into how people go about generating hypotheses shows that people are actually rather poor at thinking of all the possibilities.[86] If a person does not even generate the correct hypothesis for consideration, obviously he or she will not get the correct answer.

86. Charles Gettys et al., *Hypothesis Generation: A Final Report on Three Years of Research*, Technical Report 15-10-80 (University of Oklahoma, Decision Processes Laboratory, 1980).

Step-by-Step Outline of Analysis of Competing Hypotheses

1. Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.

2. Make a list of significant evidence and arguments for and against each hypothesis.

3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence and arguments—that is, identify which items are most helpful in judging the relative likelihood of the hypotheses.

4. Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.

5. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.

6. Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.

7. Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.

8. Identify milestones for future observation that may indicate events are taking a different course than expected.

It is useful to make a clear distinction between the hypothesis generation and hypothesis evaluation stages of analysis. Step 1 of the recommended analytical process is to identify all hypotheses that merit detailed examination. At this early hypothesis generation stage, it is very useful to bring together a group of analysts with different backgrounds and perspectives. Brainstorming in a group stimulates the imagination and

may bring out possibilities that individual members of the group had not thought of. Initial discussion in the group should elicit every possibility, no matter how remote, before judging likelihood or feasibility. Only when all the possibilities are on the table should you then focus on judging them and selecting the hypotheses to be examined in greater detail in subsequent analysis.

When screening out the seemingly improbable hypotheses that you do not want to waste time on, it is necessary to distinguish hypotheses that appear to be *disproved* from those that are simply *unproven*. For an unproven hypothesis, there is no evidence that it is correct. For a disproved hypothesis, there is positive evidence that it is wrong. As discussed in Chapter 4, "Strategies for Analytical Judgment," and under Step 5 below, you should seek evidence that *disproves* hypotheses. Early rejection of unproven, but not disproved, hypotheses biases the subsequent analysis, because one does not then look for the evidence that might support them. Unproven hypotheses should be kept alive until they can be disproved.

One example of a hypothesis that often falls into this unproven but not disproved category is the hypothesis that an opponent is trying to deceive us. You may reject the possibility of denial and deception because you see no evidence of it, but rejection is not justified under these circumstances. If deception is planned well and properly implemented, one should not expect to find evidence of it readily at hand. The possibility should not be rejected until it is disproved, or, at least, until after a systematic search for evidence has been made and none has been found.

There is no "correct" number of hypotheses to be considered. The number depends upon the nature of the analytical problem and how advanced you are in the analysis of it. As a general rule, the greater your level of uncertainty, or the greater the policy impact of your conclusion, the more alternatives you may wish to consider. More than seven hypotheses may be unmanageable; if there are this many alternatives, it may be advisable to group several of them together for your initial cut at the analysis.

Step 2

Make a list of significant evidence and arguments for and against each hypothesis.

In assembling the list of relevant evidence and arguments, these terms should be interpreted very broadly. They refer to all the factors that have an impact on your judgments about the hypotheses. Do not limit yourself to concrete evidence in the current intelligence reporting. Also include your own assumptions or logical deductions about another person's or group's or country's intentions, goals, or standard procedures. These assumptions may generate strong preconceptions as to which hypothesis is most likely. Such assumptions often drive your final judgment, so it is important to include them in the list of "evidence."

First, list the general evidence that applies to all the hypotheses. Then consider each hypothesis individually, listing factors that tend to support or contradict each one. You will commonly find that each hypothesis leads you to ask different questions and, therefore, to seek out somewhat different evidence.

For each hypothesis, ask yourself this question: If this hypothesis is true, what should I expect to be seeing or not seeing? What are all the things that must have happened, or may still be happening, and that one should expect to see evidence of? If you are not seeing this evidence, why not? Is it because it has not happened, it is not normally observable, it is being concealed from you, or because you or the intelligence collectors have not looked for it?

Note the absence of evidence as well as its presence. For example, when weighing the possibility of military attack by an adversary, the steps the adversary has not taken to ready his forces for attack may be more significant than the observable steps that have been taken. This recalls the Sherlock Holmes story in which the vital clue was that the dog did *not* bark in the night. One's attention tends to focus on what is reported rather than what is not reported. It requires a conscious effort to think about what is missing but should be present if a given hypothesis were true.

Step 3

Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence and arguments- that is, identify which items are most helpful in judging the relative likelihood of alternative hypotheses.

Step 3 is perhaps the most important element of this analytical procedure. It is also the step that differs most from the natural, intuitive approach to analysis, and, therefore, the step you are most likely to overlook or misunderstand.

The procedure for Step 3 is to take the hypotheses from Step 1 and the evidence and arguments from Step 2 and put this information into a matrix format, with the hypotheses across the top and evidence and arguments down the side. This gives an overview of all the significant components of your analytical problem.

Then analyze how each piece of evidence relates to each hypothesis. This differs from the normal procedure, which is to look at one hypothesis at a time in order to consider how well the evidence supports that hypothesis. That will be done later, in Step 5. At this point, in Step 3, take one item of evidence at a time, then consider how consistent that evidence is with each of the hypotheses. Here is how to remember this distinction. In Step 3, you work *across* the rows of the matrix, examining one item of evidence at a time to see how consistent that item of evidence is with each of the hypotheses. In Step 5, you work *down* the columns of the matrix, examining one hypothesis at a time, to see how consistent that hypothesis is with all the evidence.

To fill in the matrix, take the first item of evidence and ask whether it is consistent with, inconsistent with, or irrelevant to each hypothesis. Then make a notation accordingly in the appropriate cell under each hypothesis in the matrix. The form of these notations in the matrix is a matter of personal preference. It may be pluses, minuses, and question marks. It may be C, I, and N/A standing for consistent, inconsistent, or not applicable. Or it may be some textual notation. In any event, it will be a simplification, a shorthand representation of the complex reasoning that went on as you thought about how the evidence relates to each hypothesis.

After doing this for the first item of evidence, then go on to the next item of evidence and repeat the process until all cells in the ma-

trix are filled. Figure 15 shows an example of how such a matrix might look. It uses as an example the intelligence question that arose after the US bombing of Iraqi intelligence headquarters in 1993: Will Iraq retaliate? The evidence in the matrix and how it is evaluated are hypothetical, fabricated for the purpose of providing a plausible example of the procedure. The matrix does not reflect actual evidence or judgments available at that time to the US Intelligence Community.

Figure 15

Question: Will Iraq Retaliate for US Bombing of Its Intelligence Headquarters?

Hypotheses:
H1 - Iraq will not retaliate.
H2 - It will sponsor some minor terrorist actions.
H3 - Iraq is planning a major terrorist attack, perhaps against one or more CIA installations.

	H1	H2	H3
E1. Saddam public statement of intent not to retaliate.	+	+	+
E2. Absence of terrorist offensive during the 1991 Gulf War.	+	+	−
E3. Assumption that Iraq would not want to provoke another US attack.	+	+	−
E4. Increase in frequency/length of monitored Iraqi agent radio broadcasts.	−	+	+
E5. Iraqi embassies instructed to take increased security precautions.	−	+	+
E6. Assumption that failure to retaliate would be unacceptable loss of face for Saddam.	−−	+	+

The matrix format helps you weigh the *diagnosticity* of each item of evidence, which is a key difference between analysis of competing hypotheses and traditional analysis. Diagnosticity of evidence is an important concept that is, unfortunately, unfamiliar to many analysts. It was introduced in Chapter 4, and that discussion is repeated here for your convenience.

Diagnosticity may be illustrated by a medical analogy. A high-temperature reading may have great value in telling a doctor that a patient is sick, but relatively little value in determining which illness a person is suffering from. Because a high temperature is consistent with so many possible hypotheses about a patient's illness, this evidence has limited diagnostic value in determining which illness (hypothesis) is the more likely one.

Evidence is diagnostic when it influences your judgment on the *relative* likelihood of the various hypotheses identified in Step 1. If an item of evidence seems consistent with all the hypotheses, it may have no diagnostic value. A common experience is to discover that most of the evidence supporting what you believe is the most likely hypothesis really is not very helpful, because that same evidence is also consistent with other hypotheses. When you do identify items that are highly diagnostic, these should drive your judgment. These are also the items for which you should re-check accuracy and consider alternative interpretations, as discussed in Step 6.

In the hypothetical matrix dealing with Iraqi intentions, note that evidence designated "E1" is assessed as consistent with all of the hypotheses. In other words, it has no diagnostic value. This is because we did not give any credence to Saddam's public statement on this question. He might say he will not retaliate but then do so, or state that he will retaliate and then not do it. On the other hand, E4 is diagnostic: increased frequency or length of Iraqi agent radio broadcasts is more likely to be observed if the Iraqis are planning retaliation than if they are not. The double minus for E6 indicates this is considered a very strong argument against H1. It is a linchpin assumption that drives the conclusion in favor of either H2 or H3. Several of the judgments reflected in this matrix will be questioned at a later stage in this analysis.

In some cases it may be useful to refine this procedure by using a numerical probability, rather than a general notation such as plus or minus, to describe how the evidence relates to each hypothesis. To do this, ask the following question for each cell in the matrix: If this hypothesis is true, what is the probability that I would be seeing this item of evidence? You may also make one or more additional notations in each cell of the matrix, such as:

- Adding a scale to show the intrinsic importance of each item of evidence.

- Adding a scale to show the ease with which items of evidence could be concealed, manipulated, or faked, or the extent to which one party might have an incentive to do so. This may be appropriate when the possibility of denial and deception is a serious issue.

Step 4

Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.

The exact wording of the hypotheses is obviously critical to the conclusions one can draw from the analysis. By this point, you will have seen how the evidence breaks out under each hypothesis, and it will often be appropriate to reconsider and reword the hypotheses. Are there hypotheses that need to be added, or finer distinctions that need to be made in order to consider all the significant alternatives? If there is little orno evidence that helps distinguish between two hypotheses, should they be combined into one?

Also reconsider the evidence. Is your thinking about which hypotheses are most likely and least likely influenced by factors that are not included in the listing of evidence? If so, put them in. Delete from the matrix items of evidence or assumptions that now seem unimportant or have no diagnostic value. Save these items in a separate list as a record of information that was considered.

Step 5

Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove hypotheses rather than prove them.

In Step 3, you worked across the matrix, focusing on a single item of evidence or argument and examining how it relates to each hypothesis. Now, work down the matrix, looking at each hypothesis as a whole. The matrix format gives an overview of all the evidence for and against all the hypotheses, so that you can examine all the hypotheses together and have them compete against each other for your favor.

In evaluating the relative likelihood of alternative hypotheses, start by looking for evidence or logical deductions that enable you to reject hypotheses, or at least to determine that they are unlikely. A fundamental precept of the scientific method is to proceed by rejecting or eliminating hypotheses, while tentatively accepting only those hypotheses that cannot be refuted. The scientific method obviously cannot be applied *in toto* to intuitive judgment, but the principle of seeking to disprove hypotheses, rather than confirm them, is useful.

No matter how much information is consistent with a given hypothesis, one cannot prove that hypothesis is true, because the same information may also be consistent with one or more other hypotheses. On the other hand, a single item of evidence that is inconsistent with a hypothesis may be sufficient grounds for rejecting that hypothesis. This was discussed in detail in Chapter 4, "Strategies for Analytical Judgment."

People have a natural tendency to concentrate on confirming hypotheses they already believe to be true, and they commonly give more weight to information that supports a hypothesis than to information that weakens it. This is wrong; we should do just the opposite. Step 5 again requires doing the *opposite* of what comes naturally.

In examining the matrix, look at the minuses, or whatever other notation you used to indicate evidence that may be inconsistent with a hypothesis. The hypotheses with the fewest minuses is probably the most likely one. The hypothesis with the most minuses is probably the least likely one. The fact that a hypothesis is inconsistent with the evidence is certainly a sound basis for rejecting it. The pluses, indicating evidence that is consistent with a hypothesis, are far less significant. It does not follow that the hypothesis with the most pluses is the most likely one, because a long list of evidence that is consistent with almost any reasonable hypothesis can be easily made. What is difficult to find, and is most significant when found, is hard evidence that is clearly inconsistent with a reasonable hypothesis.

This initial ranking by number of minuses is only a rough ranking, however, as some evidence obviously is more important than other evidence, and degrees of inconsistency cannot be captured by a single notation such as a plus or minus. By reconsidering the exact nature of the relationship between the evidence and the hypotheses, you will be able to judge how much weight to give it.

Analysts who follow this procedure often realize that their judgments are actually based on very few factors rather than on the large mass of information they thought was influencing their views. Chapter 5, "Do You Really Need More Information?," makes this same point based on experimental evidence.

The matrix should *not* dictate the conclusion to you. Rather, it should accurately reflect your judgment of what is important and how these important factors relate to the probability of each hypothesis. You, not the matrix, must make the decision. The matrix serves only as an aid to thinking and analysis, to ensure consideration of all the possible interrelationships between evidence and hypotheses and identification of those few items that really swing your judgment on the issue.

When the matrix shows that a given hypothesis is probable or unlikely, you may disagree. If so, it is because you omitted from the matrix one or more factors that have an important influence on your thinking. Go back and put them in, so that the analysis reflects your best judgment. If following this procedure has caused you to consider things you might otherwise have overlooked, or has caused you to revise your earlier estimate of the relative probabilities of the hypotheses, then the procedure has served a useful purpose. When you are done, the matrix serves as a shorthand record of your thinking and as an audit trail showing how you arrived at your conclusion.

This procedure forces you to spend more analytical time than you otherwise would on what you had thought were the less likely hypotheses. This is desirable. The seemingly less likely hypotheses usually involve plowing new ground and, therefore, require more work. What you started out thinking was the most likely hypothesis tends to be based on a continuation of your own past thinking. A principal advantage of the analysis of competing hypotheses is that it forces you to give a fairer shake to all the alternatives.

Step 6

Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.

In Step 3 you identified the evidence and arguments that were most diagnostic, and in Step 5 you used these findings to make tentative judgments about the hypotheses. Now, go back and question the few linchpin assumptions or items of evidence that really drive the outcome of your analysis in one direction or the other. Are there questionable assumptions that underlie your understanding and interpretation? Are there alternative explanations or interpretations? Could the evidence be incomplete and, therefore, misleading?

If there is any concern at all about denial and deception, this is an appropriate place to consider that possibility. Look at the sources of your key evidence. Are any of the sources known to the authorities in the foreign country? Could the information have been manipulated? Put yourself in the shoes of a foreign deception planner to evaluate motive, opportunity, means, costs, and benefits of deception as they might appear to the foreign country.

When analysis turns out to be wrong, it is often because of key assumptions that went unchallenged and proved invalid. It is a truism that analysts should identify and question assumptions, but this is much easier said than done. The problem is to determine which assumptions merit questioning. One advantage of the ACH procedure is that it tells you what needs to be rechecked.

In Step 6 you may decide that additional research is needed to check key judgments. For example, it may be appropriate to go back to check original source materials rather than relying on someone else's interpretation. In writing your report, it is desirable to identify critical assumptions that went into your interpretation and to note that your conclusion is dependent upon the validity of these assumptions.

Step 7

Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.

If your report is to be used as the basis for decisionmaking, it will be helpful for the decisionmaker to know the relative likelihood of all the alternative possibilities. Analytical judgments are never certain. There is always a good possibility of their being wrong. Decisionmakers need to make decisions on the basis of a full set of alternative possibilities, not

just the single most likely alternative. Contingency or fallback plans may be needed in case one of the less likely alternatives turns out to be true.

If you say that a certain hypothesis is probably true, that could mean anywhere from a 55-percent to an 85-percent chance that future events will prove it correct. That leaves anywhere from a 15-percent to 45 percent possibility that a decision based on your judgment will be based on faulty assumptions and will turn out wrong. Can you be more specific about how confident you are in your judgment? Chapter 12, "Biases in Estimating Probabilities," discusses the difference between such "subjective probability" judgments and statistical probabilities based on data on relative frequencies.

When one recognizes the importance of proceeding by eliminating rather than confirming hypotheses, it becomes apparent that any written argument for a certain judgment is incomplete unless it also discusses alternative judgments that were considered and why they were rejected. In the past, at least, this was seldom done.

The narrative essay, which is the dominant art form for the presentation of intelligence judgments, does not lend itself to comparative evaluation of competing hypotheses. Consideration of alternatives adds to the length of reports and is perceived by many analysts as detracting from the persuasiveness of argument for the judgment chosen. Analysts may fear that the reader could fasten on one of the rejected alternatives as a good idea. Discussion of alternative hypotheses is nonetheless an important part of any intelligence appraisal, and ways can and should be found to include it.

Step 8

Identify milestones for future observation that may indicate events are taking a different course than expected.

Analytical conclusions should always be regarded as tentative. The situation may change, or it may remain unchanged while you receive new information that alters your appraisal. It is always helpful to specify in advance things one should look for or be alert to that, if observed, would suggest a significant change in the probabilities. This is useful for

intelligence consumers who are following the situation on a continuing basis. Specifying in advance what would cause you to change your mind will also make it more difficult for you to rationalize such developments, if they occur, as not really requiring any modification of your judgment.

Summary and Conclusion

Three key elements distinguish analysis of competing hypotheses from conventional intuitive analysis.

- Analysis starts with a full set of alternative possibilities, rather than with a most likely alternative for which the analyst seeks confirmation. This ensures that alternative hypotheses receive equal treatment and a fair shake.

- Analysis identifies and emphasizes the few items of evidence or assumptions that have the greatest diagnostic value in judging the relative likelihood of the alternative hypotheses. In conventional intuitive analysis, the fact that key evidence may also be consistent with alternative hypotheses is rarely considered explicitly and often ignored.

- Analysis of competing hypotheses involves seeking evidence to refute hypotheses. The most probable hypothesis is usually the one with the least evidence against it, not the one with the most evidence for it. Conventional analysis generally entails looking for evidence to confirm a favored hypothesis.

The analytical effectiveness of this procedure becomes apparent when considering the Indian nuclear weapons testing in 1998. According to Admiral Jeremiah, the Intelligence Community had reported that " there was no indication the Indians would test in the near term."[87] Such a conclusion by the Community would fail to distinguish an unproven hypothesis from a disproved hypothesis. An absence of evidence does not necessarily disprove the hypothesis that India will indeed test nuclear weapons.

87. Transcript of Adm. Jeremiah's news conference, last sentence of third paragraph, 2 June 1998.

If the ACH procedure had been used, one of the hypotheses would certainly have been that India is planning to test in the near term but will conceal preparations for the testing to forestall international pressure to halt such preparations.

Careful consideration of this alternative hypothesis would have required evaluating India's motive, opportunity, and means for concealing its intention until it was too late for the US and others to intervene. It would also have required assessing the ability of US intelligence to see through Indian denial and deception if it were being employed. It is hard to imagine that this would not have elevated awareness of the possibility of successful Indian deception.

A principal lesson is this. Whenever an intelligence analyst is tempted to write the phrase "there is no evidence that . . . ," the analyst should ask this question: If this hypothesis is true, can I realistically expect to see evidence of it? In other words, if India were planning nuclear tests while deliberately concealing its intentions, could the analyst realistically expect to see evidence of test planning? The ACH procedure leads the analyst to identify and face these kinds of questions.

Once you have gained practice in applying analysis of competing hypotheses, it is quite possible to integrate the basic concepts of this procedure into your normal analytical thought process. In that case, the entire eight-step procedure may be unnecessary, except on highly controversial issues.

There is no guarantee that ACH or any other procedure will produce a correct answer. The result, after all, still depends on fallible intuitive judgment applied to incomplete and ambiguous information. **Analysis of competing hypotheses does, however, guarantee an appropriate *process of analysis. This procedure leads you through a rational, systematic process that avoids some common analytical pitfalls. It increases the odds of getting the right answer, and it leaves an audit trail showing the evidence used in your analysis and how this evidence was interpreted. If others disagree with your judgment, the matrix can be used to highlight the precise area of disagreement. Subsequent discussion can then focus productively on the ultimate source of the differences.***

A common experience is that analysis of competing hypotheses attributes greater likelihood to alternative hypotheses than would conventional analysis. One becomes less confident of what one thought one

knew. In focusing more attention on alternative explanations, the procedure brings out the full uncertainty inherent in any situation that is poor in data but rich in possibilities. Although such uncertainty is frustrating, it may be an accurate reflection of the true situation. As Voltaire said, "Doubt is not a pleasant state, but certainty is a ridiculous one."[88]

The ACH procedure has the offsetting advantage of focusing attention on the few items of critical evidence that cause the uncertainty or which, if they were available, would alleviate it. This can guide future collection, research, and analysis to resolve the uncertainty and produce a more accurate judgment.

88. M. Rogers, ed., *Contradictory Quotations* (England: Longman Group, Ltd., 1983).

PART III—COGNITIVE BIASES

Chapter 9

What Are Cognitive Biases?

This mini-chapter discusses the nature of cognitive biases in general. The four chapters that follow it describe specific cognitive biases in the evaluation of evidence, perception of cause and effect, estimation of probabilities, and evaluation of intelligence reporting.

* * * * * * * * * * * * * * * * * * * *

Fundamental limitations in human mental processes were identified in Chapters 2 and 3. A substantial body of research in cognitive psychology and decisionmaking is based on the premise that these cognitive limitations cause people to employ various simplifying strategies and rules of thumb to ease the burden of mentally processing information to make judgments and decisions.[89] These simple rules of thumb are often useful in helping us deal with complexity and ambiguity. Under many circumstances, however, they lead to predictably faulty judgments known as cognitive biases.

Cognitive biases are mental errors caused by our simplified information processing strategies. It is important to distinguish cognitive biases from other forms of bias, such as cultural bias, organizational bias, or bias that results from one's own self-interest. In other words, a cognitive bias does not result from any emotional or intellectual predisposition toward a certain judgment, but rather from subconscious mental procedures for processing information. A cognitive bias is a mental error that is consistent and predictable. For example:

89. Much of this research was stimulated by the seminal work of Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, 27 September 1974, Vol. 185, pp. 1124-1131. It has been summarized by Robin Hogarth, *Judgement and Choice* (New York: John Wiley & Sons, 1980), Richard Nisbett and Lee Ross, *Human Inference: Strategies and Shortcomings of Human Judgment* (Englewood Cliffs, NJ: Prentice-Hall, 1980), and Robyn Dawes, *Rational Choice in an Uncertain World* (New York: Harcourt Brace Jovanovich College Publishers, 1988). The Hogarth book contains an excellent bibliography of research in this field, organized by subject.

> The apparent distance of an object is determined in part by its clarity. The more sharply the object is seen, the closer it appears to be. This rule has some validity, because in any given scene the more distant objects are seen less sharply than nearer objects. However, the reliance on this rule leads to systematic errors in estimation of distance. Specifically, distances are often overestimated when visibility is poor because the contours of objects are blurred. On the other hand, distances are often underestimated when visibility is good because the objects are seen sharply. Thus the reliance on clarity as an indication of distance leads to common biases.[90]

This rule of thumb about judging distance is very useful. It usually works and helps us deal with the ambiguity and complexity of life around us. Under certain predictable circumstances, however, it will lead to biased judgment.

Cognitive biases are similar to optical illusions in that the error remains compelling even when one is fully aware of its nature. Awareness of the bias, by itself, does not produce a more accurate perception. Cognitive biases, therefore, are, exceedingly difficult to overcome.

Psychologists have conducted many experiments to identify the simplifying rules of thumb that people use to make judgments on incomplete or ambiguous information, and to show—at least in laboratory situations—how these rules of thumb prejudice judgments and decisions. The following four chapters discuss cognitive biases that are particularly pertinent to intelligence analysis because they affect the evaluation of evidence, perception of cause and effect, estimation of probabilities, and retrospective evaluation of intelligence reports.

Before discussing the specific biases, it is appropriate to consider the nature of such experimental evidence and the extent to which one can generalize from these experiments to conclude that the same biases are prevalent in the Intelligence Community.

When psychological experiments reveal the existence of a bias, this does not mean that every judgment by every individual person will be biased. It means that in any group of people, the bias will exist to a greater or lesser degree in most judgments made by most of the group. On the basis of this kind of experimental evidence, one can only generalize about

90. Tversky and Kahneman, ibid.

the tendencies of groups of people, not make statements about how any specific individual will think.

I believe that conclusions based on these laboratory experiments can be generalized to apply to intelligence analysts. In most, although not all cases, the test subjects were experts in their field. They were physicians, stock market analysts, horserace handicappers, chess masters, research directors, and professional psychologists, not undergraduate students as in so many psychological experiments. In most cases, the mental tasks performed in these experiments were realistic; that is, they were comparable to the judgments that specialists in these fields are normally required to make.

Some margin for error always exists when extrapolating from experimental laboratory to real-world experience, but classes of CIA analysts to whom these ideas were presented found them relevant and enlightening. I replicated a number of the simpler experiments with military officers in the National Security Affairs Department of the Naval Postgraduate School.

Chapter 10

Biases in Evaluation of Evidence

Evaluation of evidence is a crucial step in analysis, but what evidence people rely on and how they interpret it are influenced by a variety of extraneous factors. Information presented in vivid and concrete detail often has unwarranted impact, and people tend to disregard abstract or statistical information that may have greater evidential value. We seldom take the absence of evidence into account. The human mind is also oversensitive to the consistency of the evidence, and insufficiently sensitive to the reliability of the evidence. Finally, impressions often remain even after the evidence on which they are based has been totally discredited.[91]

* * * * * * * * * * * * * * * * * * * *

The intelligence analyst works in a somewhat unique informational environment. Evidence comes from an unusually diverse set of sources: newspapers and wire services, observations by American Embassy officers, reports from controlled agents and casual informants, information exchanges with foreign governments, photo reconnaissance, and communications intelligence. Each source has its own unique strengths, weaknesses, potential or actual biases, and vulnerability to manipulation and deception. The most salient characteristic of the information environment is its diversity—multiple sources, each with varying degrees of reliability, and each commonly reporting information which by itself is incomplete and sometimes inconsistent or even incompatible with reporting from other sources. Conflicting information of uncertain reliability is endemic to intelligence analysis, as is the need to make rapid judgments on current events even before all the evidence is in.

The analyst has only limited control over the stream of information. Tasking of sources to report on specific subjects is often a cumbersome and time-consuming process. Evidence on some important topics is sporadic or nonexistent. Most human-source information is second hand at best.

91. An earlier version of this chapter was published as an unclassified article in *Studies in Intelligence* in summer 1981, under the same title.

Recognizing and avoiding biases under such circumstances is particularly difficult. Most of the biases discussed in this chapter are unrelated to each other and are grouped together here only because they all concern some aspect of the evaluation of evidence.

The Vividness Criterion

The impact of information on the human mind is only imperfectly related to its true value as evidence.[92] Specifically, information that is vivid, concrete, and personal has a greater impact on our thinking than pallid, abstract information that may actually have substantially greater value as evidence. For example:

- Information that people perceive directly, that they hear with their own ears or see with their own eyes, is likely to have greater impact than information received secondhand that may have greater evidential value.

- Case histories and anecdotes will have greater impact than more informative but abstract aggregate or statistical data.

Events that people experience personally are more memorable than those they only read about. Concrete words are easier to remember than abstract words,[93] and words of all types are easier to recall than numbers. In short, information having the qualities cited in the preceding paragraph is more likely to attract and hold our attention. It is more likely to be stored and remembered than abstract reasoning or statistical summaries, and therefore can be expected to have a greater immediate effect as well as a continuing impact on our thinking in the future.

Intelligence analysts generally work with secondhand information. The information that analysts receive is mediated by the written words of others rather than perceived directly with their own eyes and ears. Partly because of limitations imposed by their open CIA employment, many intelligence analysts have spent less time in the country they are

92. Most of the ideas and examples in this section are from Richard Nisbett and Lee Ross, *Human Inference: Strategies and Shortcomings of Social Judgment* (Englewood Cliffs, NJ: Prentice-Hall, 1980), Chapter 3.
93. A. Paivio, *Imagery and Verbal Processes* (New York: Holt, Rinehart & Winston, 1971).

analyzing and had fewer contacts with nationals of that country than their academic and other government colleagues. Occasions when an analyst does visit the country whose affairs he or she is analyzing, or speaks directly with a national from that country, are memorable experiences. Such experiences are often a source of new insights, but they can also be deceptive.

That concrete, sensory data do and should enjoy a certain priority when weighing evidence is well established. When an abstract theory or secondhand report is contradicted by personal observation, the latter properly prevails under most circumstances. There are a number of popular adages that advise mistrust of secondhand data: "Don't believe everything you read," "You can prove anything with statistics," "Seeing is believing," "I'm from Missouri. . ."

It is curious that there are no comparable maxims to warn against being misled by our own observations. Seeing should not always be believing.

Personal observations by intelligence analysts and agents can be as deceptive as secondhand accounts. Most individuals visiting foreign countries become familiar with only a small sample of people representing a narrow segment of the total society. Incomplete and distorted perceptions are a common result.

A familiar form of this error is the single, vivid case that outweighs a much larger body of statistical evidence or conclusions reached by abstract reasoning. When a potential car buyer overhears a stranger complaining about how his Volvo turned out to be a lemon, this may have as much impact on the potential buyer's thinking as statistics in *Consumer Reports* on the average annual repair costs for foreign-made cars. If the personal testimony comes from the potential buyer's brother or close friend, it will probably be given even more weight. Yet the logical status of this new information is to increase by one the sample on which the *Consumer Reports* statistics were based; the personal experience of a single Volvo owner has little evidential value.

Nisbett and Ross label this the "man-who" syndrome and provide the following illustrations:[94]

- "But I know a *man who* smoked three packs of cigarettes a day and lived to be ninety-nine."

- "I've never been to Turkey but just last month I met a *man who* had, and he found it . . ."

Needless to say, a "man-who" example seldom merits the evidential weight intended by the person citing the example, or the weight often accorded to it by the recipient.

The most serious implication of vividness as a criterion that determines the impact of evidence is that certain kinds of very valuable evidence will have little influence simply because they are abstract. Statistical data, in particular, lack the rich and concrete detail to evoke vivid images, and they are often overlooked, ignored, or minimized.

For example, the Surgeon General's report linking cigarette smoking to cancer should have, logically, caused a decline in per-capita cigarette consumption. No such decline occurred for more than 20 years. The reaction of physicians was particularly informative. All doctors were aware of the statistical evidence and were more exposed than the general population to the health problems caused by smoking. How they reacted to this evidence depended upon their medical specialty. Twenty years after the Surgeon General's report, radiologists who examine lung x-rays every day had the lowest rate of smoking. Physicians who diagnosed and treated lung cancer victims were also quite unlikely to smoke. Many other types of physicians continued to smoke. The probability that a physician continued to smoke was directly related to the distance of the physician's specialty from the lungs. In other words, even physicians, who were well qualified to understand and appreciate the statistical data, were more influenced by their vivid personal experiences than by valid statistical data.[95]

Personal anecdotes, actual accounts of people's responsiveness or indifference to information sources, and controlled experiments can all be cited *ad infinitum* "to illustrate the proposition that data summaries, de-

94. Nisbett and Ross, p. 56.
95. Ibid.

spite their logically compelling implications, have less impact than does inferior but more vivid evidence."[96] It seems likely that intelligence analysts, too, assign insufficient weight to statistical information.

Analysts should give little weight to anecdotes and personal case histories unless they are known to be typical, and perhaps no weight at all if aggregate data based on a more valid sample can be obtained.

Absence of Evidence

A principal characteristic of intelligence analysis is that key information is often lacking. Analytical problems are selected on the basis of their importance and the perceived needs of the consumers, without much regard for availability of information. Analysts have to do the best they can with what they have, somehow taking into account the fact that much relevant information is known to be missing.

Ideally, intelligence analysts should be able to recognize what relevant evidence is lacking and factor this into their calculations. They should also be able to estimate the potential impact of the missing data and to adjust confidence in their judgment accordingly. Unfortunately, this ideal does not appear to be the norm. Experiments suggest that "out of sight, out of mind" is a better description of the impact of gaps in the evidence.

This problem has been demonstrated using fault trees, which are schematic drawings showing all the things that might go wrong with any endeavor. Fault trees are often used to study the fallibility of complex systems such as a nuclear reactor or space capsule.

A fault tree showing all the reasons why a car might not start was shown to several groups of experienced mechanics.[97] The tree had seven major branches—insufficient battery charge, defective starting system, defective ignition system, defective fuel system, other engine problems, mischievous acts or vandalism, and all other problems—and a number of subcategories under each branch. One group was shown the full tree and asked to imagine 100 cases in which a car won't start. Members of this group were then asked to estimate how many of the 100 cases were

96. Nisbett and Ross, p. 57.
97. Baruch Fischhoff, Paul Slovic, and Sarah Lichtenstein, *Fault Trees: Sensitivity of Estimated Failure Probabilities to Problem Representation*, Technical Report PTR- 1 042-77-8 (Eugene, OR: Decision Research, 1977).

attributable to each of the seven major branches of the tree. A second group of mechanics was shown only an incomplete version of the tree: three major branches were omitted in order to test how sensitive the test subjects were to what was left out.

If the mechanics' judgment had been fully sensitive to the missing information, then the number of cases of failure that would normally be attributed to the omitted branches should have been added to the "Other Problems" category. In practice, however, the "Other Problems" category was increased only half as much as it should have been. This indicated that the mechanics shown the incomplete tree were unable to fully recognize and incorporate into their judgments the fact that some of the causes for a car not starting were missing. When the same experiment was run with non-mechanics, the effect of the missing branches was much greater.

As compared with most questions of intelligence analysis, the "car won't start" experiment involved rather simple analytical judgments based on information that was presented in a well-organized manner. That the presentation of relevant variables in the abbreviated fault tree was incomplete could and should have been recognized by the experienced mechanics selected as test subjects. Intelligence analysts often have similar problems. Missing data is normal in intelligence problems, but it is probably more difficult to recognize that important information is absent and to incorporate this fact into judgments on intelligence questions than in the more concrete "car won't start" experiment.

As an antidote for this problem, analysts should identify explicitly those relevant variables on which information is lacking, consider alternative hypotheses concerning the status of these variables, and then modify their judgment and especially confidence in their judgment accordingly. They should also consider whether the absence of information is normal or is itself an indicator of unusual activity or inactivity.

Oversensitivity to Consistency

The internal consistency in a pattern of evidence helps determine our confidence in judgments based on that evidence.[98] In one sense, consistency is clearly an appropriate guideline for evaluating evidence.

98. Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, Vol. 185 (27 September 1974), 1126.

People formulate alternative explanations or estimates and select the one that encompasses the greatest amount of evidence within a logically consistent scenario. Under some circumstances, however, consistency can be deceptive. Information may be consistent only because it is highly correlated or redundant, in which case many related reports may be no more informative than a single report. Or it may be consistent only because information is drawn from a very small sample or a biased sample.

Such problems are most likely to arise in intelligence analysis when analysts have little information, say on political attitudes of Russian military officers or among certain African ethnic groups. If the available evidence is consistent, analysts will often overlook the fact that it represents a very small and hence unreliable sample taken from a large and heterogeneous group. This is not simply a matter of necessity—of having to work with the information on hand, however imperfect it may be. Rather, there is an illusion of validity caused by the consistency of the information.

The tendency to place too much reliance on small samples has been dubbed the "law of small numbers."[99] This is a parody on the law of large numbers, the basic statistical principle that says very large samples will be highly representative of the population from which they are drawn. This is the principle that underlies opinion polling, but most people are not good intuitive statisticians. People do not have much intuitive feel for how large a sample has to be before they can draw valid conclusions from it. The so-called law of small numbers means that, intuitively, we make the mistake of treating small samples as though they were large ones.

This has been shown to be true even for mathematical psychologists with extensive training in statistics. Psychologists designing experiments have seriously incorrect notions about the amount of error and unreliability inherent in small samples of data, unwarranted confidence in the early trends from the first few data points, and unreasonably high expectations of being able to repeat the same experiment and get the same results with a different set of test subjects.

Are intelligence analysts also overly confident of conclusions drawn from very little data—especially if the data seem to be consistent? When working with a small but consistent body of evidence, analysts need to consider how representative that evidence is of the total body of poten-

99. Tversky and Kahneman (1974), p. 1125-1126.

tially available information. If more reporting were available, how likely is it that this information, too, would be consistent with the already available evidence? If an analyst is stuck with only a small amount of evidence and cannot determine how representative this evidence is, confidence in judgments based on this evidence should be low regardless of the consistency of the information.

Coping with Evidence of Uncertain Accuracy

There are many reasons why information often is less than perfectly accurate: misunderstanding, misperception, or having only part of the story; bias on the part of the ultimate source; distortion in the reporting chain from subsource through source, case officer, reports officer, to analyst; or misunderstanding and misperception by the analyst. Further, much of the evidence analysts bring to bear in conducting analysis is retrieved from memory, but analysts often cannot remember even the source of information they have in memory let alone the degree of certainty they attributed to the accuracy of that information when it was first received.

The human mind has difficulty coping with complicated probabilistic relationships, so people tend to employ simple rules of thumb that reduce the burden of processing such information. In processing information of uncertain accuracy or reliability, analysts tend to make a simple yes or no decision. If they reject the evidence, they tend to reject it fully, so it plays no further role in their mental calculations. If they accept the evidence, they tend to accept it wholly, ignoring the probabilistic nature of the accuracy or reliability judgment. This is called a "best guess" strategy.[100] Such a strategy simplifies the integration of probabilistic information, but at the expense of ignoring some of the uncertainty. If analysts have information about which they are 70- or 80-percent certain but treat this information as though it were 100-percent certain, judgments based on that information will be overconfident.

A more sophisticated strategy is to make a judgment based on an assumption that the available evidence is perfectly accurate and reliable,

100. See Charles F. Gettys, Clinton W. Kelly III, and Cameron Peterson, "The Best Guess Hypothesis in Multistage Inference," *Organizational Behavior and Human Performance, 10*, 3 (1973), 365-373; and David A. Schum and Wesley M. DuCharme, "Comments on the Relationship Between the Impact and the Reliability of Evidence," *Organizational Behavior and Human Performance, 6* (1971), 111-131.

then reduce the confidence in this judgment by a factor determined by the assessed validity of the information. For example, available evidence may indicate that an event probably (75 percent) will occur, but the analyst cannot be certain that the evidence on which this judgment is based is wholly accurate or reliable. Therefore, the analyst reduces the assessed probability of the event (say, down to 60 percent) to take into account the uncertainty concerning the evidence. This is an improvement over the best-guess strategy but generally still results in judgments that are overconfident when compared with the mathematical formula for calculating probabilities.[101]

In mathematical terms, the joint probability of two events is equal to the product of their individual probabilities. Imagine a situation in which you receive a report on event X that is probably (75 percent) true. *If the report on event X is true,* you judge that event Y will probably (75 percent) happen. The actual probability of Y is only 56 percent, which is derived by multiplying 75 percent times 75 percent.

In practice, life is not nearly so simple. Analysts must consider many items of evidence with different degrees of accuracy and reliability that are related in complex ways with varying degrees of probability to several potential outcomes. Clearly, one cannot make neat mathematical calculations that take all of these probabilistic relationships into account. In making intuitive judgments, we unconsciously seek shortcuts for sorting through this maze, and these shortcuts involve some degree of ignoring the uncertainty inherent in less-than-perfectly-reliable information. There seems to be little an analyst can do about this, short of breaking the analytical problem down in a way that permits assigning probabilities to individual items of information, and then using a mathematical formula to integrate these separate probability judgments.

The same processes may also affect our reaction to information that is plausible but known from the beginning to be of questionable authenticity. Ostensibly private statements by foreign officials are often reported though intelligence channels. In many instances it is not clear whether such a private statement by a foreign ambassador, cabinet member, or other official is an actual statement of private views, an indiscretion, part of a deliberate attempt to deceive the US Government, or part of an ap-

101. Edgar M. Johnson, "The Effect of Data Source Reliability on Intuitive Inference," Technical Paper 251 (Arlington, VA: US Army Research Institute for the Behavioral and Social Sciences, 1974).

proved plan to convey a truthful message that the foreign government believes is best transmitted through informal channels.

The analyst who receives such a report often has little basis for judging the source's motivation, so the information must be judged on its own merits. In making such an assessment, the analyst is influenced by plausible causal linkages. If these are linkages of which the analyst was already aware, the report has little impact inasmuch as it simply supports existing views. If there are plausible new linkages, however, thinking is restructured to take these into account. It seems likely that the impact on the analyst's thinking is determined solely by the substance of the information, and that the caveat concerning the source does not attenuate the impact of the information at all. Knowing that the information comes from an uncontrolled source who may be trying to manipulate us does not necessarily reduce the impact of the information.

Persistence of Impressions Based on Discredited Evidence

Impressions tend to persist even after the evidence that created those impressions has been fully discredited. Psychologists have become interested in this phenomenon because many of their experiments require that the test subjects be deceived. For example, test subjects may be made to believe they were successful or unsuccessful in performing some task, or that they possess certain abilities or personality traits, when this is not in fact the case. Professional ethics require that test subjects be disabused of these false impressions at the end of the experiment, but this has proved surprisingly difficult to achieve.

Test subjects' erroneous impressions concerning their logical problem-solving abilities persevered even after they were informed that manipulation of good or poor teaching performance had virtually guaranteed their success or failure.[102] Similarly, test subjects asked to distinguish true from fictitious suicide notes were given feedback that had no relationship to actual performance. The test subjects had been randomly divided into two groups, with members of one group being given the impression of above-average success and the other of relative failure at this task. The subjects' erroneous impressions of the difficulty of the task

102. R. R. Lau, M. R. Lepper, and L. Ross, "Persistence of Inaccurate and Discredited Personal Impressions: A Field Demonstration of Attributional Perseverance," paper presented at 56th Annual Meeting of the Western Psychological Association (Los Angeles, April 1976).

and of their own performance persisted even after they were informed of the deception—that is, informed that their alleged performance had been preordained by their assignment to one or the other test group. Moreover, the same phenomenon was found among observers of the experiment as well as the immediate participants.[103]

There are several cognitive processes that might account for this phenomenon. The tendency to interpret new information in the context of pre-existing impressions is relevant but probably not sufficient to explain why the pre-existing impression cannot be eradicated even when new information authoritatively discredits the evidence on which it is based.

An interesting but speculative explanation is based on the strong tendency to seek causal explanations, as discussed in the next chapter. When evidence is first received, people postulate a set of causal connections that explains this evidence. In the experiment with suicide notes, for example, one test subject attributed her apparent success in distinguishing real from fictitious notes to her empathetic personality and the insights she gained from the writings of a novelist who committed suicide. Another ascribed her apparent failure to lack of familiarity with people who might contemplate suicide. The stronger the perceived causal linkage, the stronger the impression created by the evidence.

Even after learning that the feedback concerning their performance was invalid, these subjects retained this plausible basis for inferring that they were either well or poorly qualified for the task. The previously perceived causal explanation of their ability or lack of ability still came easily to mind, independently of the now-discredited evidence that first brought it to mind.[104] Colloquially, one might say that once information rings a bell, the bell cannot be unrung.

The ambiguity of most real-world situations contributes to the operation of this perseverance phenomenon. Rarely in the real world is evidence so thoroughly discredited as is possible in the experimental laboratory. Imagine, for example, that you are told that a clandestine source who has been providing information for some time is actually under hostile control. Imagine further that you have formed a number

103. Lee Ross, Mark R. Lepper, and Michael Hubbard, "Perseverance in Self-Perception and Social Perception: Biased Attributional Processes in the Debriefing Paradigm," *Journal of Personality and Social Psychology, 32*, 5, (1975), 880-892.
104. Lee Ross, Mark R. Lepper, Fritz Strack, and Julia Steinmetz, "Social Explanation and Social Expectation: Effects of Real and Hypothetical Explanations on Subjective Likelihood," *Journal of Personality and Social Psychology, 33*, 11 (1977), 818.

of impressions on the basis of reporting from this source. It is easy to rationalize maintaining these impressions by arguing that the information was true despite the source being under control, or by doubting the validity of the report claiming the source to be under control. In the latter case, the perseverance of the impression may itself affect evaluation of the evidence that supposedly discredits the impression.

Chapter 11

Biases in Perception of Cause and Effect

Judgments about cause and effect are necessary to explain the past, understand the present, and estimate the future. These judgments are often biased by factors over which people exercise little conscious control, and this can influence many types of judgments made by intelligence analysts. Because of a need to impose order on our environment, we seek and often believe we find causes for what are actually accidental or random phenomena. People overestimate the extent to which other countries are pursuing a coherent, coordinated, rational plan, and thus also overestimate their own ability to predict future events in those nations. People also tend to assume that causes are similar to their effects, in the sense that important or large effects must have large causes.

When inferring the causes of behavior, too much weight is accorded to personal qualities and dispositions of the actor and not enough to situational determinants of the actor's behavior. People also overestimate their own importance as both a cause and a target of the behavior of others. Finally, people often perceive relationships that do not in fact exist, because they do not have an intuitive understanding of the kinds and amount of information needed to prove a relationship.

* * * * * * * * * * * * * * * * * * * *

We cannot see cause and effect in the same sense that we see a desk or a tree. Even when we observe one billiard ball striking another and then watch the previously stationary ball begin to move, we are not perceiving cause and effect. The conclusion that one ball *caused* the other to move results only from a complex process of inference, not from direct sensory perception. That inference is based on the juxtaposition of events in time and space plus some theory or logical explanation as to why this happens.

There are several modes of analysis by which one might infer cause and effect. In more formal analysis, inferences are made through procedures that collectively comprise the scientific method. The scientist advances a hypothesis, then tests this hypothesis by the collection and statistical analysis of data on many instances of the phenomenon in question. Even then, causality cannot be proved beyond all possible doubt.

The scientist seeks to disprove a hypothesis, not to confirm it. A hypothesis is accepted only when it cannot be rejected.

Collection of data on many comparable cases to test hypotheses about cause and effect is not feasible for most questions of interest to the Intelligence Community, especially questions of broad political or strategic import relating to another country's intentions. To be sure, it is feasible more often than it is done, and increased use of scientific procedures in political, economic, and strategic research is much to be encouraged. But the fact remains that the dominant approach to intelligence analysis is necessarily quite different. It is the approach of the historian rather than the scientist, and this approach presents obstacles to accurate inferences about causality.

The procedures and criteria most historians use to attribute causality are less well defined than the scientist's.

> The historian's aim [is] to make a coherent whole out of the events he studies. His way of doing that, I suggest, is to look for certain dominant concepts or leading ideas by which to illuminate his facts, to trace the connections between those ideas themselves, and then to show how the detailed facts became intelligible in the light of them by constructing a "significant" narrative of the events of the period in question.[105]

The key ideas here are coherence and narrative. These are the principles that guide the organization of observations into meaningful structures and patterns. The historian commonly observes only a single case, not a pattern of covariation (when two things are related so that change in one is associated with change in the other) in many comparable cases. Moreover, the historian observes simultaneous changes in so many variables that the principle of covariation generally is not helpful in sorting out the complex relationships among them. The narrative story, on the other hand, offers a means of organizing the rich complexity of the historian's observations. The historian uses imagination to construct a coherent story out of fragments of data.

The intelligence analyst employing the historical mode of analysis is essentially a storyteller. He or she constructs a plot from the previous

105. W. H. Walsh, *Philosophy of History: An Introduction* (Revised Edition: New York: Harper and Row, 1967), p. 61.

events, and this plot then dictates the possible endings of the incomplete story. The plot is formed of the "dominant concepts or leading ideas" that the analyst uses to postulate patterns of relationships among the available data. The analyst is not, of course, preparing a work of fiction. There are constraints on the analyst's imagination, but imagination is nonetheless involved because there is an almost unlimited variety of ways in which the available data might be organized to tell a meaningful story. The constraints are the available evidence and the principle of coherence. The story must form a logical and coherent whole and be internally consistent as well as consistent with the available evidence.

Recognizing that the historical or narrative mode of analysis involves telling a coherent story helps explain the many disagreements among analysts, inasmuch as coherence is a subjective concept. It assumes some prior beliefs or mental model about what goes with what. More relevant to this discussion, the use of coherence rather than scientific observation as the criterion for judging truth leads to biases that presumably influence all analysts to some degree. Judgments of coherence may be influenced by many extraneous factors, and if analysts tend to favor certain types of explanations as more coherent than others, they will be biased in favor of those explanations.

Bias in Favor of Causal Explanations

One bias attributable to the search for coherence is a tendency to favor causal explanations. Coherence implies order, so people naturally arrange observations into regular patterns and relationships. If no pattern is apparent, our first thought is that we lack understanding, not that we are dealing with random phenomena that have no purpose or reason. As a last resort, many people attribute happenings that they cannot understand to God's will or to fate, which is somehow preordained; they resist the thought that outcomes may be determined by forces that interact in random, unpredictable ways. People generally do not accept the notion of chance or randomness. Even dice players behave as though they exert some control over the outcome of a throw of dice.[106] The prevalence of the word "because" in everyday language reflects the human tendency to seek to identify causes.

106. Ellen J. Langer, "The Psychology of Chance," *Journal for the Theory of Social Behavior,* 7 (1977), 185-208.

People expect patterned events to look patterned, and random events to look random, but this is not the case. Random events often look patterned. The random process of flipping a coin six times may result in six consecutive heads. Of the 32 possible sequences resulting from six coin flips, few actually look "random."[107] This is because randomness is a property of the process that generates the data that are produced. Randomness may in some cases be demonstrated by scientific (statistical) analysis. However, events will almost never be perceived intuitively as being random; one can find an apparent pattern in almost any set of data or create a coherent narrative from any set of events.

Because of a need to impose order on their environment, people seek and often believe they find causes for what are actually random phenomena. During World War II, Londoners advanced a variety of causal explanations for the pattern of German bombing. Such explanations frequently guided their decisions about where to live and when to take refuge in air raid shelters. Postwar examination, however, determined that the clustering of bomb hits was close to a random distribution.[108]

The Germans presumably intended a purposeful pattern, but purposes changed over time and they were not always achieved, so the net result was an almost random pattern of bomb hits. Londoners focused their attention on the few clusters of hits that supported their hypotheses concerning German intentions—not on the many cases that did not.

Some research in paleobiology seems to illustrate the same tendency. A group of paleobiologists has developed a computer program to simulate evolutionary changes in animal species over time. But the transitions from one time period to the next are not determined by natural selection or any other regular process: they are determined by computer-generated random numbers. The patterns produced by this program are similar to the patterns in nature that paleobiologists have been trying to understand. Hypothetical evolutionary events that seem, intuitively, to have a strong pattern were, in fact, generated by random processes.[109]

Yet another example of imposing causal explanations on random events is taken from a study dealing with the research practices of psy-

107. Daniel Kahneman and Amos Tversky, "Subjective Probability: A Judgment of Representativeness," *Cognitive Psychology*, 3 (1972), 430-54.
108. W. Feller, *An Introduction to Probability Theory and Its Applications* (3rd Edition; New York: Wiley, 1968), p. 160.
109. Gina Bari Kolata, "Paleobiology: Random Events over Geological Time," *Science*, 189 (1975), 625-626.

chologists. When experimental results deviated from expectations, these scientists rarely attributed the deviation to variance in the sample. They were always able to come up with a more persuasive causal explanation for the discrepancy.[110]

B. F. Skinner even noted a similar phenomenon in the course of experiments with the behavioral conditioning of pigeons. The normal pattern of these experiments was that the pigeons were given positive reinforcement, in the form of food, whenever they pecked on the proper lever at the proper time. To obtain the food regularly, they had to learn to peck in a certain sequence. Skinner demonstrated that the pigeons "learned" and followed a pattern (which Skinner termed a superstition) even when the food was actually dispensed randomly.[111]

These examples suggest that in military and foreign affairs, where the patterns are at best difficult to fathom, there may be many events for which there are no valid causal explanations. This certainly affects the predictability of events and suggests limitations on what might logically be expected of intelligence analysts.

Bias Favoring Perception of Centralized Direction

Very similar to the bias toward causal explanations is a tendency to see the actions of other governments (or groups of any type) as the intentional result of centralized direction and planning. ". . .most people are slow to perceive accidents, unintended consequences, coincidences, and small causes leading to large effects. Instead, coordinated actions, plans and conspiracies are seen."[112] Analysts overestimate the extent to which other countries are pursuing coherent, rational, goal-maximizing policies, because this makes for more coherent, logical, rational explanations. This bias also leads analysts and policymakers alike to overestimate the predictability of future events in other countries.

Analysts know that outcomes are often caused by accident, blunder, coincidence, the unintended consequence of well-intentioned policy, improperly executed orders, bargaining among semi-independent bu-

110. Amos Tversky and Daniel Kahneman, "Belief in the Law of Small Numbers," *Psychological Bulletin*, 72, 2 (1971), 105-110.
111. B. F. Skinner, "Superstition in the Pigeon," *Journal of Experimental Psychology*, 38 (1948), 168-172.
112. Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), p. 320.

reaucratic entities, or following standard operating procedures under inappropriate circumstances.[113] But a focus on such causes implies a disorderly world in which outcomes are determined more by chance than purpose. It is especially difficult to incorporate these random and usually unpredictable elements into a coherent narrative, because evidence is seldom available to document them on a timely basis. It is only in historical perspective, after memoirs are written and government documents released, that the full story becomes available.

This bias has important consequences. Assuming that a foreign government's actions result from a logical and centrally directed plan leads an analyst to:

- Have expectations regarding that governmentÍs actions that may not be fulfilled if the behavior is actually the product of shifting or inconsistent values, bureaucratic bargaining, or sheer confusion and blunder.

- Draw far-reaching but possibly unwarranted inferences from isolated statements or actions by government officials who may be acting on their own rather than on central direction.

- Overestimate the United States' ability to influence the other government's actions.

- Perceive inconsistent policies as the result of duplicity and Machiavellian maneuvers, rather than as the product of weak leadership, vacillation, or bargaining among diverse bureaucratic or political interests.

Similarity of Cause and Effect

When systematic analysis of covariation is not feasible and several alternative causal explanations seem possible, one rule of thumb people use to make judgments of cause and effect is to consider the similarity between attributes of the cause and attributes of the effect. Properties of the cause are ". . .inferred on the basis of being correspondent with or

113. For many historical examples, see Jervis, ibid., p. 321-23.

similar to properties of the effect."[114] Heavy things make heavy noises; dainty things move daintily; large animals leave large tracks. When dealing with physical properties, such inferences are generally correct.

People tend, however, to reason in the same way under circumstances when this inference is not valid. Thus, analysts tend to assume that economic events have primarily economic causes, that big events have important consequences, and that little events cannot affect the course of history. Such correspondence between cause and effect makes a more logical and persuasive—a more coherent—narrative, but there is little basis for expecting such inferences to correspond to historical fact.

Fischer labels the assumption that a cause must somehow resemble its effect the "fallacy of identity,"[115] and he cites as an example the historiography of the Spanish Armada. Over a period of several centuries, historians have written of the important consequences of the English defeat of the Spanish Armada in 1588. After refuting each of these arguments, Fischer notes:

> In short, it appears that the defeat of the Armada, mighty and melodramatic as it was, may have been remarkably barren of result. Its defeat may have caused very little, except the disruption of the Spanish strategy that sent it on its way. That judgment is sure to violate the patriotic instincts of every Englishman and the aesthetic sensibilities of us all. A big event *must* have big results, we think.[116]

The tendency to reason according to similarity of cause and effect is frequently found in conjunction with the previously noted bias toward inferring centralized direction. Together, they explain the persuasiveness of conspiracy theories. Such theories are invoked to explain large effects for which there do not otherwise appear to be correspondingly large causes. For example, it seems ". . .outrageous that a single, pathetic, weak figure like Lee Harvey Oswald should alter world history."[117] Because the purported motive for the assassination of John Kennedy is so dissimilar

114. Harold H. Kelley, "The Processes of Causal Attribution," *American Psychologist* (February 1973), p. 121.
115. David Hackett Fischer, *Historian's Fallacies* (New York: Harper Torchbooks, 1970), p. 177.
116. Ibid, p. 167.
117. Richard E. Nisbett and Timothy DeC. Wilson, "Telling More Than We Can Know: Verbal Reports on Mental Processes," *Psychological Review* (May 1977), p. 252.

from the effect it is alleged to explain, in the minds of many it fails to meet the criterion of a coherent narrative explanation. If such "little" causes as mistakes, accidents, or the aberrant behavior of a single individual have big effects, then the implication follows that major events happen for reasons that are senseless and random rather than by purposeful direction.

Intelligence analysts are more exposed than most people to hard evidence of real plots, coups, and conspiracies in the international arena. Despite this—or perhaps because of it—most intelligence analysts are not especially prone to what are generally regarded as conspiracy theories. Although analysts may not exhibit this bias in such extreme form, the bias presumably does influence analytical judgments in myriad little ways. In examining causal relationships, analysts generally construct causal explanations that are somehow commensurate with the magnitude of their effects and that attribute events to human purposes or predictable forces rather than to human weakness, confusion, or unintended consequences.

Internal vs. External Causes of Behavior

Much research into how people assess the causes of behavior employs a basic dichotomy between internal determinants and external determinants of human actions. Internal causes of behavior include a person's attitudes, beliefs, and personality. External causes include incentives and constraints, role requirements, social pressures, or other forces over which the individual has little control. The research examines the circumstances under which people attribute behavior either to stable dispositions of the actor or to characteristics of the situation to which the actor responds.

Differences in judgments about what causes another person's or government's behavior affect how people respond to that behavior. How people respond to friendly or unfriendly actions by others may be quite different if they attribute the behavior to the nature of the person or government than if they see the behavior as resulting from situational constraints over which the person or government has little control.

A fundamental error made in judging the causes of behavior is to overestimate the role of internal factors and underestimate the role of external factors. When observing another's behavior, people are too in-

clined to infer that the behavior was caused by broad personal qualities or dispositions of the other person and to expect that these same inherent qualities will determine the actor's behavior under other circumstances. Not enough weight is assigned to external circumstances that may have influenced the other person's choice of behavior. This pervasive tendency has been demonstrated in many experiments under quite diverse circumstances[118] and has often been observed in diplomatic and military interactions.[119]

Susceptibility to this biased attribution of causality depends upon whether people are examining their own behavior or observing that of others. It is the behavior of others that people tend to attribute to the nature of the actor, whereas they see their own behavior as conditioned almost entirely by the situation in which they find themselves. This difference is explained largely by differences in information available to actors and observers. People know a lot more about themselves.

The actor has a detailed awareness of the history of his or her own actions under similar circumstances. In assessing the causes of our own behavior, we are likely to consider our previous behavior and focus on how it has been influenced by different situations. Thus situational variables become the basis for explaining our own behavior. This contrasts with the observer, who typically lacks this detailed knowledge of the other person's past behavior. The observer is inclined to focus on how the other person's behavior compares with the behavior of others under similar circumstances.[120] This difference in the type and amount of information available to actors and observers applies to governments as well as people.

An actor's personal involvement with the actions being observed enhances the likelihood of bias. "Where the observer is also an actor, he is likely to exaggerate the uniqueness and emphasize the dispositional origins of the responses of others to his own actions."[121] This is because the observer assumes his or her own actions are unprovocative, clearly

118. Lee Ross, "The Intuitive Psychologist and his Shortcomings: Distortions in the Attribution Process," in Leonard Berkowitz, ed., *Advances in Experimental Social Psychology*, Volume 10 (New York: Academic Press, 1977), p. 184.
119. Jervis, ibid., Chapter 2.
120. Edward E. Jones, "How Do People Perceive the Causes of Behavior?" *American Scientist*, 64 (1976), p. 301.
121. Daniel Heradstveit, *The Arab-Israeli Conflict: Psychological Obstacles to Peace* (Oslo: Universitetsforlaget, 1979), p. 25.

understood by other actors, and well designed to elicit a desired response. Indeed, an observer interacting with another actor sees himself as determining the situation to which the other actor responds. When the actor does not respond as expected, the logical inference is that the response was caused by the nature of the actor rather than by the nature of the situation.

Intelligence analysts are familiar with the problem of weighing internal versus external causes of behavior in a number of contexts. When a new leader assumes control of a foreign government, analysts assess the likely impact of changed leadership on government policy. For example, will the former Defense Minister who becomes Prime Minister continue to push for increases in the defense budget? Analysts weigh the known predispositions of the new Prime Minister, based on performance in previous positions, against the requirements of the situation that constrain the available options. If relatively complete information is available on the situational constraints, analysts may make an accurate judgment on such questions. Lacking such information, they tend to err on the side of assuming that the individual's personal predispositions will prompt continuation of past behavior.

Consider the Soviet invasion of Afghanistan. The Soviets' perception of their own behavior was undoubtedly very different from the American perception. Causal attribution theory suggests that Soviet leaders would see the invasion as a reaction to the imperatives of the situation in South Asia at that time, such as the threat of Islamic nationalism spreading from Iran and Afghanistan into the Soviet Union. Further, they would perceive US failure to understand their "legitimate" national interests as caused by fundamental US hostility.[122]

122. See Richards J. Heuer, Jr., "Analyzing the Soviet Invasion of Afghanistan: Hypotheses from Causal Attribution Theory," *Studies in Comparative Communism*, Winter 1980. These comments concerning the Soviet invasion of Afghanistan are based solely on the results of psychological research, not on information concerning Soviet actions in Afghanistan or the US reaction thereto. The nature of generalizations concerning how people normally process information is that they apply "more or less" to many cases but may not offer a perfect fit to any single instance. There were obviously many other factors that influenced analysis of Soviet actions, including preconceptions concerning the driving forces behind Soviet policy. The intent is to illustrate the relevance of psychological research on the analytical process, not to debate the merits of alternative interpretations of Soviet policy. Thus I leave to the reader to judge how much his or her own interpretation of the Soviet invasion of Afghanistan may be influenced by these attributional tendencies.

Conversely, observers of the Soviet invasion would be inclined to attribute it to the aggressive and expansionist nature of the Soviet regime. Dislike of the Soviet Union and lack of information on the situational constraints as perceived by the Soviets themselves would be likely to exacerbate the attributional bias.[123] Further, to the extent that this bias stemmed from insufficient knowledge of situational pressures and constraints, one might expect policymakers who were not Soviet experts to have had a stronger bias than analysts specializing in the Soviet Union. With their greater base of information on the situational variables, the specialists may be better able to take these variables into account.

Specialists on occasion become so deeply immersed in the affairs of the country they are analyzing that they begin to assume the perspective—and the biases—of that country's leaders. During the Cold War, there was a persistent difference between CIA specialists in Soviet affairs and specialists in Chinese affairs when dealing with Sino-Soviet relations. During border clashes in 1969, for example, specialists on the USSR argued that the Chinese were being "provocative." These specialists tended to accept the Soviet regime's versions as to the history and alignment of the border. Specialists in Chinese affairs tended to take the opposite view—that is, that the arrogant Russians were behaving like Russians often do, while the Chinese were simply reacting to the Soviet high-handedness.[124] In other words, the analysts assumed the same biased perspective as the leaders of the country about which they were most knowledgeable. An objective account of causal relationships might have been somewhere between these two positions.

The Egypt-Israel peace negotiations in 1978–1979 offered another example of apparent bias in causal attribution. In the words of one observer at the time:

> Egyptians attribute their willingness to sign a treaty with Israel as due to their inherent disposition for peace; Israelis explain Egyptian willingness to make peace as resulting from a deteriorating economy and a growing awareness of Israel's military superiority. On the other hand, Israelis attribute their own orientation for accommodation as being due to their ever-present

123. Edward Jones and Richard Nisbett, "The Actor and the Observer: Divergent Perceptions of Their Behavior," in Edward Jones *et al., Attribution: Perceiving the Causes of Behavior* (New Jersey: General Learning Press, 1971), p. 93.
124. Based on personal discussion with CIA analysts.

> preference for peace. Egypt, however, explains Israel's compromises regarding, for example, Sinai, as resulting from external pressures such as positive inducements and threats of negative sanctions by the United States. In addition, some Egyptians attribute Israel's undesirable behavior, such as establishment of Jewish settlements on the West Bank of the Jordan River, as stemming from Zionist expansionism. If Israel should not place settlements in that territory, Egyptians might account for such desirable behavior as being due to external constraints, such as Western condemnation of settlements. Israelis, on the other hand explain undesirable behavior, such as Egypt's past tendency to issue threats to drive them into the sea, as resulting from Egypt's inherent opposition to a Jewish state in the Middle East. When Egyptians ceased to make such threats, Israelis attributed this desirable behavior as emanating from external circumstances, such as Israel's relative military superiority.[125]

The persistent tendency to attribute cause and effect in this manner is not simply the consequence of self-interest or propaganda by the opposing sides. Rather, it is the readily understandable and predictable result of how people normally attribute causality under many different circumstances.

As a general rule, biased attribution of causality helps sow the seeds of mistrust and misunderstanding between people and between governments. We tend to have quite different perceptions of the causes of each other's behavior.

Overestimating Our Own Importance

Individuals and governments tend to overestimate the extent to which they successfully influence the behavior of others.[126] This is an exception to the previously noted generalization that observers attribute the behavior of others to the nature of the actor. It occurs largely because a person is so familiar with his or her own efforts to influence another, but much less well informed about other factors that may have influenced the other's decision.

125. Raymond Tanter, "Bounded Rationality and Decision Aids," essay prepared for the Strategies of Conflict seminar, Mont Pelerin, Switzerland, 11-16 May 1980.
126. This section draws heavily upon Jervis, Chapter 9.

In estimating the influence of US policy on the actions of another government, analysts more often than not will be knowledgeable of US actions and what they are intended to achieve, but in many instances they will be less well informed concerning the internal processes, political pressures, policy conflicts, and other influences on the decision of the target government.

This bias may have played a role in the recent US failure to anticipate Indian nuclear weapons testing even though the new Indian Government was elected partly on promises it would add nuclear weapons to India's military arsenal. Most US intelligence analysts apparently discounted the promises as campaign rhetoric, believing that India would be dissuaded from joining the nuclear club by economic sanctions and diplomatic pressure. Analysts overestimated the ability of US policy to influence Indian decisions.

When another country's actions are consistent with US desires, the most obvious explanation, in the absence of strong evidence to the contrary, is that US policy effectively influenced the decision.[127] Conversely, when another country behaves in an undesired manner, this is normally attributed to factors beyond US control. People and governments seldom consider the possibility that their own actions have had unintended consequences. They assume that their intentions have been correctly perceived and that actions will have the desired effect unless frustrated by external causes.

Many surveys and laboratory experiments have shown that people generally perceive their own actions as the cause of their successes but not of their failures. When children or students or workers perform well, their parents, teachers, or supervisors take at least part of the credit; when they do poorly, their mentors seldom assume any blame. Successful candidates for Congress generally believe their own behavior contributed strongly to their victory, while unsuccessful candidates blame defeat on factors beyond their control.

Another example is the chest thumping that some Americans engaged in after the fall of the Soviet Union. According to some, the demise of the USSR was caused by strong US policies, such as increased defense expenditures and the Strategic Defense Initiative, which caused Soviet leaders to realize they could no longer compete with the United

127. It follows from the same reasoning that we may underestimate the consequences of our actions on nations that are not the *intended* target of our influence.

States. The US news media played this story for several weeks, interviewing many people—some experts, some not—on why the Soviet Union collapsed. Most serious students understood that there were many reasons for the Soviet collapse, the most important of which were internal problems caused by the nature of the Soviet system.

People and governments also tend to overestimate their own importance as the target of others' actions. They are sensitive to the impact that others' actions have on them, and they generally assume that people and governments intend to do what they do and intend it to have the effect that it has. They are much less aware of, and consequently tend to downgrade the importance of, other causes or results of the action.

In analyzing the reasons why others act the way they do, it is common to ask, "What goals are the person or government pursuing?" But goals are generally inferred from the effects of behavior, and the effects that are best known and often seem most important are the effects upon ourselves. Thus actions that hurt us are commonly interpreted as intentional expressions of hostility directed at ourselves. Of course, this will often be an accurate interpretation, but people sometimes fail to recognize that actions that seem directed at them are actually the unintended consequence of decisions made for other reasons.

Illusory Correlation

At the start of this chapter, covariation was cited as one basis for inferring causality. It was noted that covariation may either be observed intuitively or measured statistically. This section examines the extent to which the intuitive perception of covariation deviates from the statistical measurement of covariation.

Statistical measurement of covariation is known as correlation. Two events are correlated when the existence of one event implies the existence of the other. Variables are correlated when a change in one variable implies a similar degree of change in another. Correlation alone does not necessarily imply causation. For example, two events might co-occur because they have a common cause, rather than because one causes the other. But when two events or changes do co-occur, and the time sequence is such that one always follows the other, people often infer that the first caused the second. Thus, inaccurate perception of correlation leads to inaccurate perception of cause and effect.

Judgments about correlation are fundamental to all intelligence analysis. For example, assumptions that worsening economic conditions lead to increased political support for an opposition party, that domestic problems may lead to foreign adventurism, that military government leads to unraveling of democratic institutions, or that negotiations are more successful when conducted from a position of strength are all based on intuitive judgments of correlation between these variables. In many cases these assumptions are correct, but they are seldom tested by systematic observation and statistical analysis.

Much intelligence analysis is based on common-sense assumptions about how people and governments normally behave. The problem is that people possess a great facility for invoking contradictory "laws" of behavior to explain, predict, or justify different actions occurring under similar circumstances. "Haste makes waste" and "He who hesitates is lost" are examples of inconsistent explanations and admonitions. They make great sense when used alone and leave us looking foolish when presented together. "Appeasement invites aggression" and "agreement is based upon compromise" are similarly contradictory expressions.

When confronted with such apparent contradictions, the natural defense is that "it all depends on. . . ." Recognizing the need for such qualifying statements is one of the differences between subconscious information processing and systematic, self-conscious analysis. Knowledgeable analysis might be identified by the ability to fill in the qualification; careful analysis by the frequency with which one remembers to do so.[128]

Illusory correlation occurs when people perceive a relationship that does not in fact exist. In looking at a series of cases, it seems that people often focus on instances that support the existence of a relationship but ignore those cases that fail to support it. Several experiments have demonstrated that people do not have an intuitive understanding of what information is really needed to assess the relationship between two events or two variables. There appears to be nothing in people's intuitive understanding that corresponds with the statistical concept of correlation.

Nurses were tested on their ability to learn through experience to judge the relationship, or correlation, between a symptom and the di-

128. This paragraph draws heavily from the ideas and phraseology of Baruch Fischhoff, "For Those Condemned to Study the Past: Reflections on Historical Judgment," in R. A. Shweder and D. W. Fiske, eds., *New Directions for Methodology of Behavioral Science: Fallible Judgment in Behavioral Research* (San Francisco: Jossey-Bass, 1980).

agnosis of illness.[129] The nurses were each shown 100 cards; every card ostensibly represented one patient. The cards had a row of four letters at the top representing various symptoms and another row of four letters at the bottom representing diagnoses. The nurses were instructed to focus on just one letter (A) representing one symptom and one letter (F) representing one diagnosis, and then to judge whether the symptom A was related to the diagnosis F. In other words, on the basis of experience with these 100 "patients," does the presence of symptom A help to diagnose the presence of illness F? The experiment was run a number of times using different degrees of relationship between A and F.

Put yourself briefly in the position of a test subject. You have gone through the cards and noticed that on about 25 of them, or a quarter of the cases, the symptom and the disease, A and F, are both present. Would you say there is a relationship? Why? Is it appropriate to make a judgment solely on the basis of the frequency of cases which support the hypothesis of a relationship between A and F? What else do you need to know? Would it be helpful to have the number of cases in which the symptom (A) was present without the disease (F)? Let us say this was also true on 25 cards, so that out of the 100 cards, 50 had A and 25 of those cards with A also had F. In other words, the disease was present in half the cases in which the symptom was observed. Is this sufficient to establish a relationship, or is it also necessary to know the number of times the disease was present without the symptom?

Actually, to determine the existence of such a relationship, one needs information to fill all four cells of a 2 x 2 contingency table. Figure 16 shows such a table for one test run of this experiment. The table shows the number of cases of patients having each of four possible combinations of symptom and disease.

Eighteen of 19 test subjects given the 100 cards representing this particular combination of A and F thought there was at least a weak relationship, and several thought there was a strong relationship, when in fact, there is no correlation at all. More than half the test subjects based their judgment solely on the frequency of cases in which both A and F were present. This is the upper left cell of the table. These subjects were trying to determine if there was a relationship between A and F. When looking through the cards, 25 percent of the cases they looked at were

129. Jan Smedslund, "The Concept of Correlation in Adults," *Scandinavian Journal of Psychology*, Vol. 4 (1963), 165-73.

Figure 16

	A	Not A
F	25	25
Not F	25	25

consistent with the belief that symptom and diagnosis were perfectly correlated; this appears to be a lot of evidence to support the hypothesized relationship. Another smaller group of test subjects used somewhat more sophisticated reasoning. They looked at the total number of A cases and then asked in how many of these cases F was also present. This is the left side of the table in Figure 16. A third group resisted the basic concept of making a statistical generalization. When asked to describe their reasoning, they said that sometimes a relationship was present while in other cases it was not.

Of the 86 test subjects involved in several runnings of this experiment, not a single one showed any intuitive understanding of the concept of correlation. That is, no one understood that to make a proper judgment about the existence of a relationship, one must have information on all four cells of the table. Statistical correlation in its most elementary form is based on the ratio of the sums of the frequencies in the diagonal cells of a 2 x 2 table. In other words, a predominance of entries along either diagonal represents a strong statistical relationship between the two variables.

Let us now consider a similar question of correlation on a topic of interest to intelligence analysts. What are the characteristics of strategic deception and how can analysts detect it? In studying deception, one of the important questions is: what are the correlates of deception? Historically, when analysts study instances of deception, what else do they see that goes along with it, that is somehow related to deception, and that might be interpret as an indicator of deception? Are there certain practices relating to deception, or circumstances under which deception is most likely to occur, that permit one to say, that, because we have seen x or y or z, this most likely means a deception plan is under way? This would be comparable to a doctor observing certain symptoms and

concluding that a given disease may be present. This is essentially a problem of correlation. If one could identify several correlates of deception, this would significantly aid efforts to detect it.

The hypothesis has been advanced that deception is most likely when the stakes are exceptionally high.[130] If this hypothesis is correct, analysts should be especially alert for deception in such instances. One can cite prominent examples to support the hypothesis, such as Pearl Harbor, the Normandy landings, and the German invasion of the Soviet Union. It seems as though the hypothesis has considerable support, given that it is so easy to recall examples of high stakes situations in which deception was employed. But consider what it would take to prove, empirically, that such a relationship actually exists. Figure 17 sets up the problem as a 2 x 2 contingency table.

Figure 17

	High Stakes	Not High Stakes
Deception	68	?
No Deception	35	?

Barton Whaley researched 68 cases in which surprise or deception was present in strategic military operations between 1914 and 1968.[131] Let us assume that some form of deception, as well as surprise, was present in all 68 cases and put this number in the upper left cell of the table. How many cases are there with high stakes when deception was not used? That is a lot harder to think about and to find out about; researchers seldom devote much effort to documenting negative cases, when something did not occur. Fortunately, Whaley did make a rough estimate that both deception and surprise were absent in one-third to one-half of the cases of "grand strategy" during this period, which is the basis for putting the number 35 in the lower left cell of Figure 17.

130. Robert Axelrod, "The Rational Timing of Surprise," *World Politics*, XXXI (January 1979), pp. 228-246.
131. Barton Whaley, *Stratagem: Deception and Surprise in War*, (Cambridge, MA: Massachusetts Institute of Technology, unpublished manuscript, 1969), p. 247.

How common is deception when the stakes are not high? This is the upper right cell of Figure 17. Entries for this cell and the lower right cell are difficult to estimate; they require defining a universe of cases that includes low-stakes situations. What is a low-stakes situation in this context? High-stakes situations are definable, but there is an almost infinite number and variety of low-stakes situations. Because of this difficulty, it may not be feasible to use the full 2 x 2 table to analyze the relationship between deception and high stakes.

Perhaps it is necessary to be content with only the left side of the Figure 17 table. But then we cannot demonstrate empirically that one should be more alert to deception in high-stakes situations, because there is no basis for comparing high-stakes and low-stakes cases. If deception is even more common in tactical situations than it is in high stakes strategic situations, then analysts should not be more inclined to suspect deception when the stakes are high.

It is not really clear whether there is a relationship between deception and high-stakes situations, because there are not enough data. Intuitively, your gut feeling may tell you there is, and this feeling may well be correct. But you may have this feeling mainly because you are inclined to focus only on those cases in the upper left cell that do suggest such a relationship. People tend to overlook cases where the relationship does not exist, inasmuch as these are much less salient.

The lesson to be learned is not that analysts should do a statistical analysis of every relationship. They usually will not have the data, time, or interest for that. But analysts should have a general understanding of what it takes to know whether a relationship exists. This understanding is definitely not a part of people's intuitive knowledge. It does not come naturally. It has to be learned. When dealing with such issues, analysts have to force themselves to think about all four cells of the table and the data that would be required to fill each cell.

Even if analysts follow these admonitions, there are several factors that distort judgment when one does not follow rigorous scientific procedures in making and recording observations. These are factors that influence a person's ability to recall examples that fit into the four cells. For example, people remember occurrences more readily than non-occurrences. "History is, by and large, a record of what people did, not what they failed to do."[132]

132. E. H. Carr, *What is History?* (London: Macmillan, 1961), p. 126, cited by Fischhoff, *op. cit*.

Thus, instances in which deception occurred are easier to recall than instances in which it did not. Analysts remember occurrences that support the relationship they are examining better than those that do not. To the extent that perception is influenced by expectations, analysts may have missed or discounted the contrary instances. People also have a better memory for recent events, events in which they were personally involved, events that had important consequences, and so forth. These factors have a significant influence on perceptions of correlation when analysts make a gut judgment without consciously trying to think of all four cells of the table.

Many erroneous theories are perpetuated because they seem plausible and because people record their experience in a way that supports rather than refutes them. Ross describes this process as follows:

> . . .the intuitive observer selectively codes those data potentially relevant to the relationship between X and Y. Data points that fit his hypotheses and predictions are accepted as reliable, valid, representative, and free of error or "third-variable influences." Such data points are seen as reflective of the "real". . .relationship between X and Y. By contrast, data points that deviate markedly from the intuitive . . . expectations or theory are unlikely to be given great weight and tend to be dismissed as unreliable, erroneous, unrepresentative, or the product of contaminating third-variable influences. Thus the intuitive scientist who believes that fat men are jolly, or more specifically that fatness causes jolliness, will see particular fat and jolly men as strong evidence for this theory; he will not entertain the hypothesis that an individual's jollity is mere pretense or the product of a particularly happy home life rather than obesity. By contrast, fat and morose individuals will be examined very carefully before gaining admission to that scientist's store of relevant data. He might, for instance, seek to determine whether the individual's moroseness on the day in question is atypical, or the result of a nagging cold or a disappointing day, rather than the reflection of some stable attribute. It need hardly be emphasized that even a randomly generated [set of data] can yield a relatively high correlation if coded in the manner just outlined.[133]

133. Ross, *op. cit.*, pp. 208-209.

Chapter 12

Biases in Estimating Probabilities

In making rough probability judgments, people commonly depend upon one of several simplified rules of thumb that greatly ease the burden of decision. Using the "availability" rule, people judge the probability of an event by the ease with which they can imagine relevant instances of similar events or the number of such events that they can easily remember. With the "anchoring" strategy, people pick some natural starting point for a first approximation and then adjust this figure based on the results of additional information or analysis. Typically, they do not adjust the initial judgment enough.

Expressions of probability, such as possible and probable, are a common source of ambiguity that make it easier for a reader to interpret a report as consistent with the reader's own preconceptions. The probability of a scenario is often miscalculated. Data on "prior probabilities" are commonly ignored unless they illuminate causal relationships.

* * * * * * * * * * * * * * * * * * * *

Availability Rule

One simplified rule of thumb commonly used in making probability estimates is known as the availability rule. In this context, "availability" refers to imaginability or retrievability from memory. Psychologists have shown that two cues people use unconsciously in judging the probability of an event are the ease with which they can imagine relevant instances of the event and the number or frequency of such events that they can easily remember.[134] People are using the availability rule of thumb whenever they estimate frequency or probability on the basis of how easily they can recall or imagine instances of whatever it is they are trying to estimate.

134. Amos Tversky and Daniel Kahneman, "Availability: A Heuristic for Judging Frequency and Probability," *Cognitive Psychology*, 5 (1973), pp. 207-232.

Normally this works quite well. If one thing actually occurs more frequently than another and is therefore more probable, we probably can recall more instances of it. Events that are likely to occur usually are easier to imagine than unlikely events. People are constantly making inferences based on these assumptions. For example, we estimate our chances for promotion by recalling instances of promotion among our colleagues in similar positions and with similar experience. We estimate the probability that a politician will lose an election by imagining ways in which he may lose popular support.

Although this often works well, people are frequently led astray when the ease with which things come to mind is influenced by factors unrelated to their probability. The ability to recall instances of an event is influenced by how recently the event occurred, whether we were personally involved, whether there were vivid and memorable details associated with the event, and how important it seemed at the time. These and other factors that influence judgment are unrelated to the true probability of an event.

Consider two people who are smokers. One had a father who died of lung cancer, whereas the other does not know anyone who ever had lung cancer. The one whose father died of lung cancer will normally perceive a greater probability of adverse health consequences associated with smoking, even though one more case of lung cancer is statistically insignificant when weighing such risk. How about two CIA officers, one of whom knew Aldrich Ames and the other who did not personally know anyone who had ever turned out to be a traitor? Which one is likely to perceive the greatest risk of insider betrayal?

It was difficult to imagine the breakup of the Soviet Union because such an event was so foreign to our experience of the previous 50 years. How difficult is it now to imagine a return to a Communist regime in Russia? Not so difficult, in part because we still have vivid memories of the old Soviet Union. But is that a sound basis for estimating the likelihood of its happening? When analysts make quick, gut judgments without really analyzing the situation, they are likely to be influenced by the availability bias. The more a prospective scenario accords with one's experience, the easier it is to imagine and the more likely it seems.

Intelligence analysts may be less influenced than others by the availability bias. Analysts are evaluating all available information, not making quick and easy inferences. On the other hand, policymakers and journal-

ists who lack the time or access to evidence to go into details must necessarily take shortcuts. The obvious shortcut is to use the availability rule of thumb for making inferences about probability.

Many events of concern to intelligence analysts

> . . .are perceived as so unique that past history does not seem relevant to the evaluation of their likelihood. In thinking of such events we often construct scenarios, i.e., stories that lead from the present situation to the target event. The plausibility of the scenarios that come to mind, or the difficulty of producing them, serve as clues to the likelihood of the event. If no reasonable scenario comes to mind, the event is deemed impossible or highly unlikely. If several scenarios come easily to mind, or if one scenario is particularly compelling, the event in question appears probable.[135]

US policymakers in the early years of our involvement in Vietnam had to imagine scenarios for what might happen if they did or did not commit US troops to the defense of South Vietnam. In judging the probability of alternative outcomes, our senior leaders were strongly influenced by the ready availability of two seemingly comparable scenarios—the failure of appeasement prior to World War II and the successful intervention in Korea.

Many extraneous factors influence the imaginability of scenarios for future events, just as they influence the retrievability of events from memory. Curiously, one of these is the act of analysis itself. The act of constructing a detailed scenario for a possible future event makes that event more readily imaginable and, therefore, increases its perceived probability. This is the experience of CIA analysts who have used various tradecraft tools that require, or are especially suited to, the analysis of unlikely but nonetheless possible and important hypotheses. (Such techniques were discussed in Chapter 6, "Keeping an Open Mind" and Chapter 8, "Analysis of Competing Hypotheses.") The analysis usually results in the "unlikely" scenario being taken a little more seriously. This phenomenon has also been demonstrated in psychological experiments.[136]

135. Ibid., p. 229.
136. John S. Carroll, "The Effect of Imagining an Event on Expectations for the Event: An Interpretation in Terms of the Availability Heuristic", *Journal of Experimental Social Psychology*, 14 (1978), pp. 88-96.

In sum, the availability rule of thumb is often used to make judgments about likelihood or frequency. People would be hard put to do otherwise, inasmuch as it is such a timesaver in the many instances when more detailed analysis is not warranted or not feasible. Intelligence analysts, however, need to be aware when they are taking shortcuts. They must know the strengths and weaknesses of these procedures, and be able to identify when they are most likely to be led astray. For intelligence analysts, recognition that they are employing the availability rule should raise a caution flag. Serious analysis of probability requires identification and assessment of the strength and interaction of the many variables that will determine the outcome of a situation.

Anchoring

Another strategy people seem to use intuitively and unconsciously to simplify the task of making judgments is called anchoring. Some natural starting point, perhaps from a previous analysis of the same subject or from some partial calculation, is used as a first approximation to the desired judgment. This starting point is then adjusted, based on the results of additional information or analysis. Typically, however, the starting point serves as an anchor or drag that reduces the amount of adjustment, so the final estimate remains closer to the starting point than it ought to be.

Anchoring can be demonstrated very simply in a classroom exercise by asking a group of students to estimate one or more known quantities, such as the percentage of member countries in the United Nations that are located in Africa. Give half the students a low-percentage number and half a high-percentage number. Ask them to start with this number as an estimated answer, then, as they think about the problem, to adjust this number until they get as close as possible to what they believe is the correct answer. When this was done in one experiment that used this question, those starting with an anchor of 10 percent produced adjusted estimates that averaged 25 percent. Those who started with an anchor of 65 percent produced adjusted estimates that averaged 45 percent.[137]

Because of insufficient adjustment, those who started out with an estimate that was too high ended with significantly higher estimates than

137. Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, Vol. 185, Sept. 27, 1974, pp. 1124-1131.

those who began with an estimate that was too low. Even the totally arbitrary starting points acted as anchors, causing drag or inertia that inhibited fulladjustment of estimates.

Whenever analysts move into a new analytical area and take over responsibility for updating a series of judgments or estimates made by their predecessors, the previous judgments may have such an anchoring effect. Even when analysts make their own initial judgment, and then attempt to revise this judgment on the basis of new information or further analysis, there is much evidence to suggest that they usually do not change the judgment enough.

Anchoring provides a partial explanation of experiments showing that analysts tend to be overly sure of themselves in setting confidence ranges. A military analyst who estimates future missile or tank production is often unable to give a specific figure as a point estimate. The analyst may, therefore, set a range from high to low, and estimate that there is, say, a 75-percent chance that the actual production figure will fall within this range. If a number of such estimates are made that reflect an appropriate degree of confidence, the true figure should fall within the estimated range 75 percent of the time and outside this range 25 percent of the time. In experimental situations, however, most participants are overconfident. The true figure falls outside the estimated range a much larger percentage of the time.[138]

If the estimated range is based on relatively hard information concerning the upper and lower limits, the estimate is likely to be accurate. If, however, the range is determined by starting with a single best estimate that is simply adjusted up and down to arrive at estimated maximum and minimum values, then anchoring comes into play, and the adjustment is likely to be insufficient.

Reasons for the anchoring phenomenon are not well understood. The initial estimate serves as a hook on which people hang their first impressions or the results of earlier calculations. In recalculating, they take this as a starting point rather than starting over from scratch, but why this should limit the range of subsequent reasoning is not clear.

138. Experiments using a 98-percent confidence range found that the true value fell outside the estimated range 40 to 50 percent of the time. Amos Tversky and Daniel Kahneman, "Anchoring and Calibration in the Assessment of Uncertain Quantities," (Oregon Research Institute Research Bulletin, 1972, Nov. 12, No. 5), and M. Alpert and H. Raiffa, "A Progress Report on The Training of Probability Assessors," Unpublished manuscript, Harvard University, 1968.

There is some evidence that awareness of the anchoring problem is not an adequate antidote.[139] This is a common finding in experiments dealing with cognitive biases. The biases persist even after test subjects are informed of them and instructed to try to avoid them or compensate for them.

One technique for avoiding the anchoring bias, to weigh anchor so to speak, may be to ignore one's own or others' earlier judgments and rethink a problem from scratch. In other words, consciously avoid any prior judgment as a starting point. There is no experimental evidence to show that this is possible or that it will work, but it seems worth trying. Alternatively, it is sometimes possible to avoid human error by employing formal statistical procedures. Bayesian statistical analysis, for example, can be used to revise prior judgments on the basis of new information in a way that avoids anchoring bias.[140]

Expression of Uncertainty

Probabilities may be expressed in two ways. Statistical probabilities are based on empirical evidence concerning relative frequencies. Most intelligence judgments deal with one-of-a-kind situations for which it is impossible to assign a statistical probability. Another approach commonly used in intelligence analysis is to make a "subjective probability" or "personal probability" judgment. Such a judgment is an expression of the analyst's personal belief that a certain explanation or estimate is correct. It is comparable to a judgment that a horse has a three-to-one chance of winning a race.

Verbal expressions of uncertainty—such as "possible," "probable," "unlikely," "may," and "could"—are a form of subjective probability judgment, but they have long been recognized as sources of ambiguity and misunderstanding. To say that something could happen or is possible

139. Alpert and Raiffa, ibid.

140. Nicholas Schweitzer, "Bayesian Analysis: Estimating the Probability of Middle East Conflict," in Richards J. Heuer, Jr., ed., *Quantitative Approaches to Political Intelligence: The CIA Experience* (Boulder, CO: Westview Press, 1979). Jack Zlotnick, "Bayes' Theorem for Intelligence Analysis," *Studies in Intelligence*, Vol. 16, No. 2 (Spring 1972). Charles E. Fisk, "The Sino-Soviet Border Dispute: A Comparison of the Conventional and Bayesian Methods for Intelligence Warning", *Studies in Intelligence*, vol. 16, no. 2 (Spring 1972), originally classified Secret, now declassified. Both the Zlotnick and Fisk articles were republished in H. Bradford Westerfield, *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, (New Haven: Yale University Press, 1995).

may refer to anything from a 1-percent to a 99-percent probability. To express themselves clearly, analysts must learn to routinely communicate uncertainty using the language of numerical probability or odds ratios.

As explained in Chapter 2 on "Perception," people tend to see what they expect to see, and new information is typically assimilated to existing beliefs. This is especially true when dealing with verbal expressions of uncertainty. By themselves, these expressions have no clear meaning. They are empty shells. The reader or listener fills them with meaning through the context in which they are used and what is already in the reader's or listener's mind about that context.

When intelligence conclusions are couched in ambiguous terms, a reader's interpretation of the conclusions will be biased in favor of consistency with what the reader already believes. This may be one reason why many intelligence consumers say they do not learn much from intelligence reports.[141]

It is easy to demonstrate this phenomenon in training courses for analysts. Give students a short intelligence report, have them underline all expressions of uncertainty, then have them express their understanding of the report by writing above each expression of uncertainty the numerical probability they believe was intended by the writer of the report. This is an excellent learning experience, as the differences among students in how they understand the report are typically so great as to be quite memorable.

In one experiment, an intelligence analyst was asked to substitute numerical probability estimates for the verbal qualifiers in one of his own earlier articles. The first statement was: "The cease-fire is holding but could be broken within a week." The analyst said he meant there was about a 30-percent chance the cease-fire would be broken within a week. Another analyst who had helped this analyst prepare the article said she thought there was about an 80-percent chance that the cease-fire would be broken. Yet, when working together on the report, both analysts had believed they were in agreement about what could happen.[142] Obviously, the analysts had not even communicated effectively with each other, let alone with the readers of their report.

141. For another interpretation of this phenomenon, see Chapter 13, "Hindsight Biases in Evaluation of Intelligence Reporting."
142. Scott Barclay et al, *Handbook for Decision Analysis*. (McLean, VA: Decisions and Designs, Inc. 1977), p. 66.

Sherman Kent, the first director of CIA's Office of National Estimates, was one of the first to recognize problems of communication caused by imprecise statements of uncertainty. Unfortunately, several decades after Kent was first jolted by how policymakers interpreted the term "serious possibility" in a national estimate, this miscommunication between analysts and policymakers, and between analysts, is still a common occurrence.[143]

I personally recall an ongoing debate with a colleague over the bona fides of a very important source. I argued he was probably bona fide. My colleague contended that the source was probably under hostile control. After several months of periodic disagreement, I finally asked my colleague to put a number on it. He said there was at least a 51-percent chance of the source being under hostile control. I said there was at least a 51-percent chance of his being bona fide. Obviously, we agreed that there was a great deal of uncertainty. That stopped our disagreement. The problem was not a major difference of opinion, but the ambiguity of the term probable.

The table in Figure 18 shows the results of an experiment with 23 NATO military officers accustomed to reading intelligence reports. They were given a number of sentences such as: "It is highly unlikely that. . . ." All the sentences were the same except that the verbal expressions of probability changed. The officers were asked what percentage probability they would attribute to each statement if they read it in an intelligence report. Each dot in the table represents one officer's probability assignment.[144] While there was broad consensus about the meaning of "better than even," there was a wide disparity in interpretation of other probability expressions. The shaded areas in the table show the ranges proposed by Kent.[145]

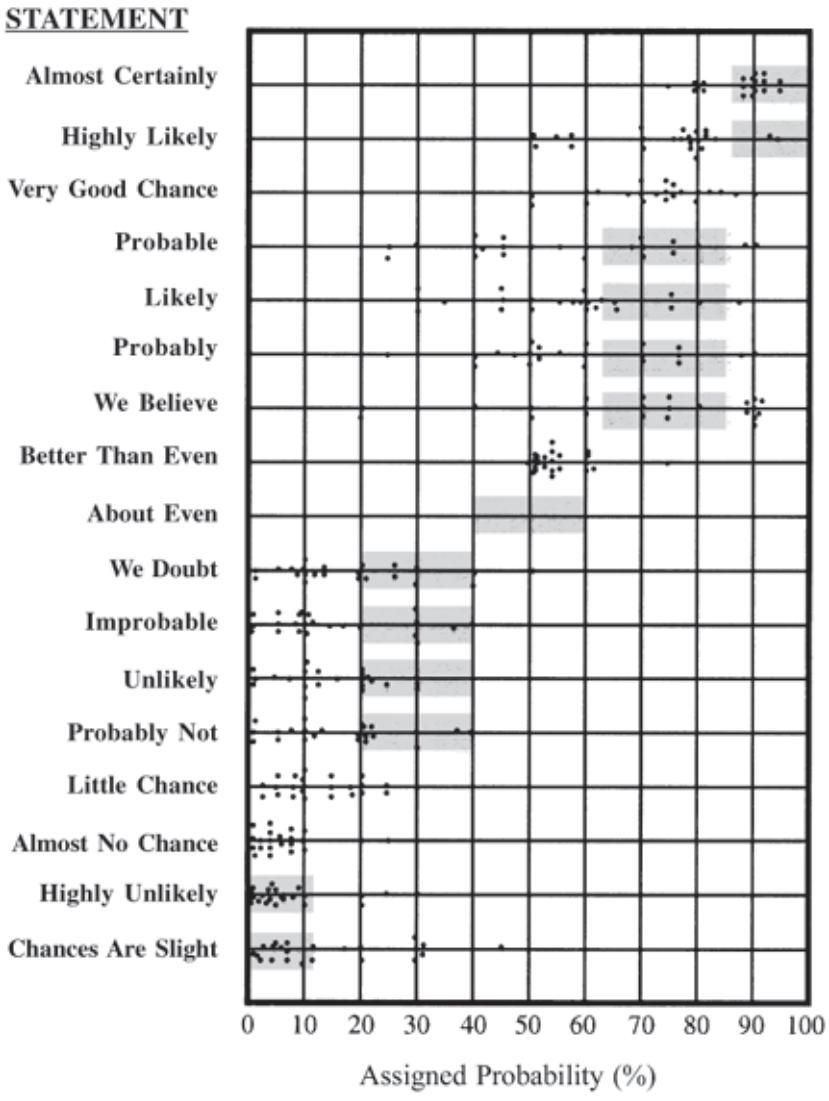
The main point is that an intelligence report may have no impact on the reader if it is couched in such ambiguous language that the reader can easily interpret it as consistent with his or her own preconceptions. This

143. Sherman Kent, "Words of Estimated Probability," in Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA, Center for the Study of Intelligence, 1994).

144. Scott Barclay et al, p. 76-68.

145. Probability ranges attributed to Kent in this table are slightly different from those in Sherman Kent, "Words of Estimated Probability," in Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA, Center for the Study of Intelligence, 1994).

Figure 18: Measuring Perceptions of Uncertainty



ambiguity can be especially troubling when dealing with low-probability, high-impact dangers against which policymakers may wish to make contingency plans.

Consider, for example, a report that there is little chance of a terrorist attack against the American Embassy in Cairo at this time. If the Ambassador's preconception is that there is no more than a one-in-a-hundred chance, he may elect to not do very much. If the Ambassador's preconception is that there may be as much as a one-in-four chance of an attack, he may decide to do quite a bit. The term "little chance" is consistent with either of those interpretations, and there is no way to know what the report writer meant.

Another potential ambiguity is the phrase "at this time." Shortening the time frame for prediction lowers the probability, but may not decrease the need for preventive measures or contingency planning. An event for which the timing is unpredictable may "at this time" have only a 5-percent probability of occurring during the coming month, but a 60-percent probability if the time frame is extended to one year (5 percent per month for 12 months).

How can analysts express uncertainty without being unclear about how certain they are? Putting a numerical qualifier in parentheses after the phrase expressing degree of uncertainty is an appropriate means of avoiding misinterpretation. This may be an odds ratio (less than a one-in-four chance) or a percentage range (5 to 20 percent) or (less than 20 percent). Odds ratios are often preferable, as most people have a better intuitive understanding of odds than of percentages.

Assessing Probability of a Scenario

Intelligence analysts sometimes present judgments in the form of a scenario—a series of events leading to an anticipated outcome. There is evidence that judgments concerning the probability of a scenario are influenced by amount and nature of detail in the scenario in a way that is unrelated to actual likelihood of the scenario.

A scenario consists of several events linked together in a narrative description. To calculate mathematically the probability of a scenario, the proper procedure is to multiply the probabilities of each individual event. Thus, for a scenario with three events, each of which will probably (70 percent certainty) occur, the probability of the scenario is .70 x .70

x .70 or slightly over 34 percent. Adding a fourth probable (70 percent) event to the scenario would reduce its probability to 24 percent.

Most people do not have a good intuitive grasp of probabilistic reasoning. One approach to simplifying such problems is to assume (or think as though) one or more probable events have already occurred. This eliminates some of the uncertainty from the judgment. Another way to simplify the problem is to base judgment on a rough average of the probabilities of each event. In the above example, the averaging procedure gives an estimated probability of 70 percent for the entire scenario. Thus, the scenario appears far more likely than is in fact the case.

When the averaging strategy is employed, highly probable events in the scenario tend to offset less probable events. This violates the principle that a chain cannot be stronger than its weakest link. Mathematically, the least probable event in a scenario sets the upper limit on the probability of the scenario as a whole. If the averaging strategy is employed, additional details may be added to the scenario that are so plausible they increase the perceived probability of the scenario, while, mathematically, additional events must necessarily reduce its probability.[146]

Base-Rate Fallacy

In assessing a situation, an analyst sometimes has two kinds of evidence available—specific evidence about the individual case at hand, and numerical data that summarize information about many similar cases. This type of numerical information is called a base rate or prior probability. The base-rate fallacy is that the numerical data are commonly ignored unless they illuminate a causal relationship. This is illustrated by the following experiment.[147]

During the Vietnam War, a fighter plane made a non-fatal strafing attack on a US aerial reconnaissance mission at twilight. Both Cambodian and Vietnamese jets operate in the area. You know the following facts:

(a) Specific case information: The US pilot identified the fighter as Cambodian. The pilot's aircraft recognition capabilities were tested under appropriate visibility and flight conditions. When presented

146. Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein, "Cognitive Processes and Societal Risk Taking," in J. S. Carroll and J.W. Payne, eds., *Cognition and Social Behavior* (Potomac, MD: Lawrence Erlbaum Associates, 1976), pp. 177-78.

147. This is a modified version, developed by Frank J. Stech, of the blue and green taxicab question used by Kahneman and Tversky, "On Prediction and Judgment," Oregon Research Institute Research Bulletin, 12, 14, 1972.

with a sample of fighters (half with Vietnamese markings and half with Cambodian) the pilot made correct identifications 80 percent of the time and erred 20 percent of the time.

(b) Base rate data: 85 percent of the jet fighters in that area are Vietnamese; 15 percent are Cambodian.

Question: What is the probability that the fighter was Cambodian rather than Vietnamese?

A common procedure in answering this question is to reason as follows: We know the pilot identified the aircraft as Cambodian. We also know the pilot's identifications are correct 80 percent of the time; therefore, there is an 80 percent probability the fighter was Cambodian. This reasoning appears plausible but is incorrect. It ignores the base rate—that 85 percent of the fighters in that area are Vietnamese. The base rate, or prior probability, is what you can say about any hostile fighter in that area before you learn anything about the specific sighting.

It is actually more likely that the plane was Vietnamese than Cambodian despite the pilot's "probably correct" identification. Readers who are unfamiliar with probabilistic reasoning and do not grasp this point should imagine 100 cases in which the pilot has a similar encounter. Based on paragraph (a), we know that 80 percent or 68 of the 85 Vietnamese aircraft will be correctly identified as Vietnamese, while 20 percent or 17 will be incorrectly identified as Cambodian. Based on paragraph (b), we know that 85 of these encounters will be with Vietnamese aircraft, 15 with Cambodian.

Similarly, 80 percent or 12 of the 15 Cambodian aircraft will be correctly identified as Cambodian, while 20 percent or three will be incorrectly identified as Vietnamese. This makes a total of 71 Vietnamese and 29 Cambodian sightings, of which only 12 of the 29 Cambodian sightings are correct; the other 17 are incorrect sightings of Vietnamese aircraft. Therefore, when the pilot claims the attack was by a Cambodian fighter, the probability that the craft was actually Cambodian is only 12/29ths or 41 percent, despite the fact that the pilot's identifications are correct 80 percent of the time.

This may seem like a mathematical trick, but it is not. The difference stems from the strong prior probability of the pilot observing a Vietnamese aircraft. The difficulty in understanding this arises because untrained intuitive judgment does not incorporate some of the basic statistical principles of probabilistic reasoning. Most people do not incor-

porate the prior probability into their reasoning because it does not seem relevant. It does not seem relevant because there is no causal relationship between the background information on the percentages of jet fighters in the area and the pilot's observation.[148] The fact that 85 percent of the fighters in the area were Vietnamese and 15 percent Cambodian did not *cause* the attack to be made by a Cambodian rather than a Vietnamese.

To appreciate the different impact made by causally relevant background information, consider this alternative formulation of the same problem. In paragraph (b) of the problem, substitute the following:

(b) Although the fighter forces of the two countries are roughly equal in number in this area, 85 percent of all harassment incidents involve Vietnamese fighters, while 15 percent involve Cambodian fighters.

The problem remains mathematically and structurally the same. Experiments with many test subjects, however, show it is quite different psychologically because it readily elicits a causal explanation relating the prior probabilities to the pilot's observation. If the Vietnamese have a propensity to harass and the Cambodians do not, the prior probability that Vietnamese harassment is more likely than Cambodian is no longer ignored. Linking the prior probability to a cause and effect relationship immediately raises the possibility that the pilot's observation was in error.

With this revised formulation of the problem, most people are likely to reason as follows: We know from past experience in cases such as this that the harassment is usually done by Vietnamese aircraft. Yet, we have a fairly reliable report from our pilot that it was a Cambodian fighter. These two conflicting pieces of evidence cancel each other out. Therefore, we do not know—it is roughly 50-50 whether it was Cambodian or Vietnamese. In employing this reasoning, we use the prior probability information, integrate it with the case-specific information, and arrive at a conclusion that is about as close to the optimal answer (still 41 percent) as one is going to get without doing a mathematical calculation.

There are, of course, few problems in which base rates are given as explicitly as in the Vietnamese/Cambodian aircraft example. When base

148. Maya Bar-Hillel, "The Base-Rate Fallacy in Probability Judgments," *Acta Psychologica*, 1980.

rates are not well known but must be inferred or researched, they are even less likely to be used.[149]

The so-called planning fallacy, to which I personally plead guilty, is an example of a problem in which base rates are not given in numerical terms but must be abstracted from experience. In planning a research project, I may estimate being able to complete it in four weeks. This estimate is based on relevant case-specific evidence: desired length of report, availability of source materials, difficulty of the subject matter, allowance for both predictable and unforeseeable interruptions, and so on. I also possess a body of experience with similar estimates I have made in the past. Like many others, I almost never complete a research project within the initially estimated time frame! But I am seduced by the immediacy and persuasiveness of the case-specific evidence. All the causally relevant evidence about the project indicates I should be able to complete the work in the time allotted for it. Even though I know from experience that this never happens, I do not learn from this experience. I continue to ignore the non-causal, probabilistic evidence based on many similar projects in the past, and to estimate completion dates that I hardly ever meet. (Preparation of this book took twice as long as I had anticipated. These biases are, indeed, difficult to avoid!)

149. Many examples from everyday life are cited in Robyn M. Dawes, *Rational Choice in an Uncertain World* (Harcourt Brace Jovanovich College Publishers, 1988), Chapter 5.

Chapter 13

Hindsight Biases in Evaluation of Intelligence Reporting

Evaluations of intelligence analysis—analysts' own evaluations of their judgments as well as others' evaluations of intelligence products—are distorted by systematic biases. As a result, analysts overestimate the quality of their analytical performance, and others underestimate the value and quality of their efforts. These biases are not simply the product of self-interest and lack of objectivity. They stem from the nature of human mental processes and are difficult and perhaps impossible to overcome.[150]

* * * * * * * * * * * * * * * * * * * *

Hindsight biases influence the evaluation of intelligence reporting in three ways:

- Analysts normally overestimate the accuracy of their past judgments.
- Intelligence consumers normally underestimate how much they learned from intelligence reports.
- Overseers of intelligence production who conduct postmortem analyses of an intelligence failure normally judge that events were more readily foreseeable than was in fact the case.

None of the biases is surprising. Analysts have observed these tendencies in others, although probably not in themselves. What may be

150. This chapter was first published as an unclassified article in *Studies in Intelligence*, Vol. 22, No. 2 (Summer 1978), under the title "Cognitive Biases: Problems in Hindsight Analysis." It was later published in H. Bradford Westerfield, editor, *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992* (New Haven: Yale University Press, 1995.)

unexpected is that these biases are not only the product of self-interest and lack of objectivity. They are examples of a broader phenomenon that is built into human mental processes and that cannot be overcome by the simple admonition to be more objective.

Psychologists who conducted the experiments described below tried to teach test subjects to overcome these biases. Experimental subjects with no vested interest in the results were briefed on the biases and encouraged to avoid them or compensate for them, but could not do so. Like optical illusions, cognitive biases remain compelling even after we become aware of them.

The analyst, consumer, and overseer evaluating analytical performance all have one thing in common. They are exercising hindsight. They take their current state of knowledge and compare it with what they or others did or could or should have known before the current knowledge was received. This is in sharp contrast with intelligence estimation, which is an exercise in foresight, and it is the difference between these two modes of thought—hindsight and foresight—that seems to be a source of bias.

The amount of good information that is available obviously is greater in hindsight than in foresight. There are several possible explanations of how this affects mental processes. One is that the additional information available for hindsight changes perceptions of a situation so naturally and so immediately that people are largely unaware of the change. When new information is received, it is immediately and unconsciously assimilated into our pre-existing knowledge. If this new information adds significantly to our knowledge—that is, if it tells the outcome of a situation or the answer to a question about which we were previously uncertain—our mental images are restructured to take the new information into account. With the benefit of hindsight, for example, factors previously considered relevant may become irrelevant, and factors previously thought to have little relevance may be seen as determinative.

After a view has been restructured to assimilate the new information, there is virtually no way to accurately reconstruct the pre-existing mental set. Once the bell has rung, it cannot be unrung. A person may *remember* his or her previous judgments if not much time has elapsed and the judgments were precisely articulated, but apparently people cannot accurately *reconstruct* their previous thinking. The effort to reconstruct what we previously thought about a given situation, or what we would

have thought about it, is inevitably influenced by our current thought patterns. Knowing the outcome of a situation makes it harder to imagine other outcomes that might have been considered. Unfortunately, simply understanding that the mind works in this fashion does little to help overcome the limitation.

The overall message to be learned from an understanding of these biases, as shown in the experiments described below, is that an analyst's intelligence judgments are not as good as analysts think they are, or as bad as others seem to believe. Because the biases generally cannot be overcome, they would appear to be facts of life that analysts need to take into account in evaluating their own performance and in determining what evaluations to expect from others. This suggests the need for a more systematic effort to:

- Define what should be expected from intelligence analysts.
- Develop an institutionalized procedure for comparing intelligence judgments and estimates with actual outcomes.
- Measure how well analysts live up to the defined expectations.

The discussion now turns to the experimental evidence demonstrating these biases from the perspective of the analyst, consumer, and overseer of intelligence.

The Analyst's Perspective

Analysts interested in improving their own performance need to evaluate their past estimates in the light of subsequent developments. To do this, analysts must either remember (or be able to refer to) their past estimates or must reconstruct their past estimates on the basis of what they remember having known about the situation at the time the estimates were made. The effectiveness of the evaluation process, and of the learning process to which it gives impetus, depends in part upon the accuracy of these remembered or reconstructed estimates.

Experimental evidence suggests a systematic tendency toward faulty memory of past estimates.[151] That is, when events occur, people tend to overestimate the extent to which they had previously expected them to occur. And conversely, when events do not occur, people tend to underestimate the probability they had previously assigned to their occurrence. In short, events generally seem less surprising than they should on the basis of past estimates. This experimental evidence accords with analysts' intuitive experience. Analysts rarely appear—or allow themselves to appear—very surprised by the course of events they are following.

In experiments to test the bias in memory of past estimates, 119 subjects were asked to estimate the probability that a number of events would or would not occur during President Nixon's trips to Peking and Moscow in 1972. Fifteen possible outcomes were identified for each trip, and each subject assigned a probability to each of these outcomes. The outcomes were selected to cover the range of possible developments and to elicit a wide range of probability values.

At varying time periods after the trips, the same subjects were asked to remember or reconstruct their own predictions as accurately as possible. (No mention was made of the memory task at the time of the original prediction.) Then the subjects were asked to indicate whether they thought each event had or had not occurred during these trips.

When three to six months were allowed to elapse between the subjects' estimates and their recollection of these estimates, 84 percent of the subjects exhibited the bias when dealing with events they believed actually did happen. That is, the probabilities they remembered having estimated were higher than their actual estimates of events they believed actually did occur. Similarly, for events they believed did not occur, the probabilities they remembered having estimated were lower than their actual estimates, although here the bias was not as great. For both kinds of events, the bias was more pronounced after three to six months had elapsed than when subjects were asked to recall estimates they had given only two weeks earlier.

In summary, knowledge of the outcomes somehow affected most test subjects' memory of their previous estimates of these outcomes, and the more time that was allowed for memories to fade, the greater the

151. This section is based on research reported by Baruch Fischoff and Ruth Beyth in "I Knew It Would Happen: Remembered Probabilities of Once-Future Things," *Organizational Behavior and Human Performance*, 13 (1975), pp. 1-16.

effect of the bias. The developments during the President's trips were perceived as less surprising than they would have been if actual estimates were compared with actual outcomes. For the 84 percent of subjects who showed the anticipated bias, their retrospective evaluation of their estimative performance was clearly more favorable than warranted by the facts.

The Consumer's Perspective

When consumers of intelligence reports evaluate the quality of the intelligence product, they ask themselves the question: "How much did I learn from these reports that I did not already know?" In answering this question, there is a consistent tendency for most people to underestimate the contribution made by new information. This "I knew it all along" bias causes consumers to undervalue the intelligence product.[152]

That people do in fact commonly react to new information in this manner was tested in a series of experiments involving some 320 people, each of whom answered the same set of 75 factual questions taken from almanacs and encyclopedias. As a measure of their confidence in their answers, the subjects assigned to each question a number ranging from 50 percent to 100 percent, indicating their estimate of the probability that they had chosen the correct answer.

As a second step in the experiment, subjects were divided into three groups. The first group was given 25 of the previously asked questions and instructed to respond to them exactly as they had previously. This simply tested the subjects' ability to remember their previous answers. The second group was given the same set of 25 questions but with the correct answers circled "for your [the subjects'] general information." They, too, were asked to respond by reproducing their previous answers. This tested the extent to which learning the correct answers distorted the subjects' memories of their own previous answers, thus measuring the same bias in recollection of previous estimates that was discussed above from the analyst's perspective.

The third group was given a different set of 25 questions they had not previously seen, but which were of similar difficulty so that results

152. Experiments described in this section are reported in Baruch Fischhoff, *The Perceived Informativeness of Factual Information*, Technical Report DDI- I (Eugene, OR: Oregon Research Institute, 1976).

would be comparable with the other two groups. The correct answers were marked on the questionnaire, and the subjects were asked to respond to the questions as they would have responded had they not been told the answer. This tested their ability to recall accurately how much they had known before they learned the correct answer. The situation is comparable to that of intelligence consumers who are asked to evaluate how much they learned from a report, and who can do this only by trying to recollect the extent of their knowledge before they read the report.

The most significant results came from this third group of subjects. The group clearly overestimated what they had known originally and underestimated how much they learned from having been told the answer. For 19 of 25 items in one running of the experiment and 20 of 25 items in another running, this group assigned higher probabilities to the correct alternatives than it is reasonable to expect they would have assigned had they not already known the correct answers.

In summary, the experiment confirmed the results of the previous experiment showing that people exposed to an answer tend to remember having known more than they actually did. It also demonstrates that people have an even greater tendency to exaggerate the likelihood that they would have known the correct answer if they had not been informed of it. In other words, people tend to underestimate both how much they learn from new information and the extent to which new information permits them to make correct judgments with greater confidence. To the extent that intelligence consumers manifest these same biases, they will tend to underrate the value to them of intelligence reporting.

The Overseer's Perspective

An overseer, as the term is used here, is one who investigates intelligence performance by conducting apostmortemexamination of a high-profile intelligence failure. Such investigations are carried out by Congress, the Intelligence Community staff, and CIA or DI management. For those outside the executive branch who do not regularly read the intelligence product, this sort of retrospective evaluation of known intelligence failures is a principal basis for judgments about the quality of intelligence analysis.

A fundamental question posed in anypostmorteminvestigation of intelligence failure is this: Given the information that was available at the

time, should analysts have been able to foresee what was going to happen? Unbiased evaluation of intelligence performance depends upon the ability to provide an unbiased answer to this question.[153]

Unfortunately, once an event has occurred, it is impossible to erase from our mind the knowledge of that event and reconstruct what our thought processes would have been at an earlier point in time. In reconstructing the past, there is a tendency toward determinism, toward thinking that what occurred was inevitable under the circumstances and therefore predictable. In short, there is a tendency to believe analysts should have foreseen events that were, in fact, unforeseeable on the basis of the information available at the time.

The experiments reported in the following paragraphs tested the hypotheses that knowledge of an outcome increases the perceived inevitability of that outcome, and that people who are informed of the outcome are largely unaware that this information has changed their perceptions in this manner.

A series of sub-experiments used brief (150-word) summaries of several events for which four possible outcomes were identified. One of these events was the struggle between the British and the Gurkhas in India in 1814. The four possible outcomes for this event were 1) British victory, 2) Gurkha victory, 3) military stalemate with no peace settlement, and 4) military stalemate with a peace settlement. Five groups of 20 subjects each participated in each sub-experiment. One group received the 150-word description of the struggle between the British and the Gurkhas with no indication of the outcome. The other four groups received the identical description but with one sentence added to indicate the outcome of the struggle—a different outcome for each group.

The subjects in all five groups were asked to estimate the likelihood of each of the four possible outcomes and to evaluate the relevance to their judgment of each datum in the event description. Those subjects who were informed of an outcome were placed in the same position as an overseer of intelligence analysis preparing a postmortem analysis of an intelligence failure. This person tries to assess the probability of an outcome

153. Experiments described in this section are reported in Baruch Fischhoff, "Hindsight does not equal Foresight: The Effect of Outcome Knowledge on Judgment Under Uncertainty," *Journal of Experimental Psychology: Human Perception and Performance*, 1, 3 (1975), pp. 288-299.

Figure 19

Experimental Groups	Average Probabilities Assigned to Outcomes			
	1	2	3	4
Not Told Outcome	33.8	21.3	32.3	12.3
Told Outcome 1	57.2	14.3	15.3	13.4
Told Outcome 2	30.3	38.4	20.4	10.5
Told Outcome 3	25.7	17.0	48.4	9.9
Told Outcome 4	33.0	15.8	24.3	27.0

based only on the information available before the outcome was known. The results are shown in Figure 18.

The group not informed of any outcome judged the probability of Outcome 1 as 33.8 percent, while the group told that Outcome 1 was the actual outcome perceived the probability of this outcome as 57.2 percent. The estimated probability was clearly influenced by knowledge of the outcome. Similarly, the control group with no outcome knowledge estimated the probability of Outcome 2 as 21.3 percent, while those informed that Outcome 2 was the actual outcome perceived it as having a 38.4 percent probability.

An average of all estimated outcomes in six sub-experiments (a total of 2,188 estimates by 547 subjects) indicates that the knowledge or belief that one of four possible outcomes has occurred approximately doubles the perceived probability of that outcome as judged with hindsight as compared with foresight.

The relevance that subjects attributed to any datum was also strongly influenced by which outcome, if any, they had been told was true. As Roberta Wohlstetter has written, "It is much easier after the fact to sort the relevant from the irrelevant signals. After the event, of course, a signal is always crystal clear. We can now see what disaster it was signaling since

the disaster has occurred, but before the event it is obscure and pregnant with conflicting meanings."[154] The fact that outcome knowledge automatically restructures a person's judgments about the relevance of available data is probably one reason it is so difficult to reconstruct how our thought processes were or would have been without this outcome knowledge.

In several variations of this experiment, subjects were asked to respond as though they did not know the outcome, or as others would respond if they did not know the outcome. The results were little different, indicating that subjects were largely unaware of how knowledge of the outcome affected their own perceptions. The experiment showed that subjects were unable to empathize with how others would judge these situations. Estimates of how others would interpret the data without knowing the outcome were virtually the same as the test subjects' own retrospective interpretations.

These results indicate that overseers conducting postmortemevaluations of what analysts should have been able to foresee, given the available information, will tend to perceive the outcome of that situation as having been more predictable than was, in fact, the case. Because they are unable to reconstruct a state of mind that views the situation only with foresight, not hindsight, overseers will tend to be more critical of intelligence performance than is warranted.

Discussion of Experiments

Experiments that demonstrated these biases and their resistance to corrective action were conducted as part of a research program in decision analysis funded by the Defense Advanced Research Projects Agency. Unfortunately, the experimental subjects were students, not members of the Intelligence Community. There is, nonetheless, reason to believe the results can be generalized to apply to the Intelligence Community. The experiments deal with basic human mental processes, and the results do seem consistent with personal experience in the Intelligence Community. In similar kinds of psychological tests, in which experts, including intelligence analysts, were used as test subjects, the experts showed the same pattern of responses as students.

154. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), p. 387. Cited by Fischhoff.

My own imperfect effort to replicate one of these experiments using intelligence analysts also supports the validity of the previous findings. To test the assertion that intelligence analysts normally overestimate the accuracy of their past judgments, there are two necessary preconditions. First, analysts must make a series of estimates in quantitative terms—that is, they must say not just that a given occurrence is probable, but that there is, for example, a 75-percent chance of its occurrence. Second, it must be possible to make an unambiguous determination whether the estimated event did or did not occur. When these two preconditions are present, one can go back and check the analysts' recollections of their earlier estimates. Because CIA estimates are rarely stated in terms of quantitative probabilities, and because the occurrence of an estimated event within a specified time period often cannot be determined unambiguously, these preconditions are seldom met.

I did, however, identify several analysts who, on two widely differing subjects, had made quantitative estimates of the likelihood of events for which the subsequent outcome was clearly known. I went to these analysts and asked them to recall their earlier estimates. The conditions for this mini-experiment were far from ideal and the results were not clear-cut, but they did tend to support the conclusions drawn from the more extensive and systematic experiments described above.

All this leads to the conclusion that the three biases are found in Intelligence Community personnel as well as in the specific test subjects. In fact, one would expect the biases to be even greater in foreign affairs professionals whose careers and self-esteem depend upon the presumed accuracy of their judgments.

Can We Overcome These Biases?

Analysts tend to blame biased evaluations of intelligence performance at best on ignorance and at worst on self-interest and lack of objectivity. Both these factors may also be at work, but the experiments suggest the nature of human mental processes is also a principal culprit. This is a more intractable cause than either ignorance or lack of objectivity.

The self-interest of the experimental subjects was not at stake, yet they showed the same kinds of bias with which analysts are familiar. Moreover, in these experimental situations the biases were highly resis-

tant to efforts to overcome them. Subjects were instructed to make estimates as if they did not already know the answer, but they were unable to do so. One set of test subjects was briefed specifically on the bias, citing the results of previous experiments. This group was instructed to try to compensate for the bias, but it was unable to do so. Despite maximum information and the best of intentions, the bias persisted.

This intractability suggests the bias does indeed have its roots in the nature of our mental processes. Analysts who try to recall a previous estimate after learning the actual outcome of events, consumers who think about how much a report has added to their knowledge, and overseers who judge whether analysts should have been able to avoid an intelligence failure, all have one thing in common. They are engaged in a mental process involving hindsight. They are trying to erase the impact of knowledge, so as to remember, reconstruct, or imagine the uncertainties they had or would have had about a subject prior to receipt of more or less definitive information.

It appears, however, that the receipt of what is accepted as definitive or authoritative information causes an immediate but unconscious restructuring of a person's mental images to make them consistent with the new information. Once past perceptions have been restructured, it seems very difficult, if not impossible, to reconstruct accurately what one's thought processes were or would have been before this restructuring.

There is one procedure that may help to overcome these biases. It is to pose such questions as the following: Analysts should ask themselves, "If the opposite outcome had occurred, would I have been surprised?" Consumers should ask, "If this report had told me the opposite, would I have believed it?" And overseers should ask, "If the opposite outcome had occurred, would it have been predictable given the information that was available?" These questions may help one recall or reconstruct the uncertainty that existed prior to learning the content of a report or the outcome of a situation.

This method of overcoming the bias can be tested by readers of this chapter, especially those who believe it failed to tell them much they had not already known. If this chapter had reported that psychological experiments show no consistent pattern of analysts overestimating the accuracy of their estimates, or of consumers underestimating the value of our product, would you have believed it? (Answer: Probably not.) If it had reported that psychological experiments show these biases to be

caused only by self-interest and lack of objectivity, would you have believed this? (Answer: Probably yes.) And would you have believed it if this chapter had reported these biases can be overcome by a conscientious effort at objective evaluation? (Answer: Probably yes.)

These questions may lead you, the reader, to recall the state of your knowledge or beliefs before reading this chapter. If so, the questions will highlight what you learned here—namely, that significant biases in the evaluation of intelligence estimates are attributable to the nature of human mental processes, not just to self-interest and lack of objectivity, and that they are, therefore, exceedingly difficult to overcome.

PART IV—CONCLUSIONS

Chapter 14

Improving Intelligence Analysis

This chapter offers a checklist for analysts—a summary of tips on how to navigate the minefield of problems identified in previous chapters. It also identifies steps that managers of intelligence analysis can take to help create an environment in which analytical excellence can flourish.

* * * * * * * * * * * * * * * * * * * *

How can intelligence analysis be improved? That is the challenge. A variety of traditional approaches are used in pursuing this goal: collecting more and better information for analysts to work with, changing the management of the analytical process, increasing the number of analysts, providing language and area studies to improve analysts' substantive expertise, revising employee selection and retention criteria, improving report-writing skills, fine-tuning the relationship between intelligence analysts and intelligence consumers, and modifying the types of analytical products.

Any of these measures may play an important role, but analysis is, above all, a mental process. Traditionally, analysts at all levels devote little attention to improving how they think. To penetrate the heart and soul of the problem of improving analysis, it is necessary to better understand, influence, and guide the mental processes of analysts themselves.

Checklist for Analysts

This checklist for analysts summarizes guidelines for maneuvering through the minefields encountered while proceeding through the analytical process. Following the guidelines will help analysts protect themselves from avoidable error and improve their chances of making the right calls. The discussion is organized around six key steps in the analytical process: defining the problem, generating hypotheses, collecting information, evaluating hypotheses, selecting the most likely hypothesis, and the ongoing monitoring of new information.

Defining the Problem

Start out by making certain you are asking—or being asked—the right questions. Do not hesitate to go back up the chain of command with a suggestion for doing something a little different from what was asked for. The policymaker who originated the requirement may not have thought through his or her needs, or the requirement may be somewhat garbled as it passes down through several echelons of management. You may have a better understanding than the policymaker of what he or she needs, or should have, or what is possible to do. At the outset, also be sure your supervisor is aware of any tradeoff between quality of analysis and what you can accomplish within a specified time deadline.

Generating Hypotheses

Identify all the plausible hypotheses that need to be considered. Make a list of as many ideas as possible by consulting colleagues and outside experts. Do this in a brainstorming mode, suspending judgment for as long as possible until all the ideas are out on the table.

Then whittle the list down to a workable number of hypotheses for more detailed analysis. Frequently, one of these will be a deception hypothesis—that another country or group is engaging in denial and deception to influence US perceptions or actions.

At this stage, do not screen out reasonable hypotheses only because there is no evidence to support them. This applies in particular to the deception hypothesis. If another country is concealing its intent through denial and deception, you should probably not expect to see evidence of it without completing a very careful analysis of this possibility. The deception hypothesis and other plausible hypotheses for which there may be no immediate evidence should be carried forward to the next stage of analysis until they can be carefully considered and, if appropriate, rejected with good cause.

Collecting Information

Relying only on information that is automatically delivered to you will probably not solve all your analytical problems. To do the job right, it will probably be necessary to look elsewhere and dig for more information. Contact with the collectors, other Directorate of Operations personnel, or first-cut analysts often yields additional information. Also check academic specialists, foreign newspapers, and specialized journals.

Collect information to evaluate all the reasonable hypotheses, not just the one that seems most likely. Exploring alternative hypotheses that have not been seriously considered before often leads an analyst into unexpected and unfamiliar territory. For example, evaluating the possibility of deception requires evaluating another country's or group's motives, opportunities, and means for denial and deception. This, in turn, may require understanding the strengths and weaknesses of US human and technical collection capabilities.

It is important to suspend judgment while information is being assembled on each of the hypotheses. It is easy to form impressions about a hypothesis on the basis of very little information, but hard to change an impression once it has taken root. If you find yourself thinking you already know the answer, ask yourself what would cause you to change your mind; then look for that information.

Try to develop alternative hypotheses in order to determine if some alternative—when given a fair chance—might not be as compelling as your own preconceived view. Systematic development of an alternative hypothesis usually increases the perceived likelihood of that hypothesis. "A willingness to play with material from different angles and in the context of unpopular as well as popular hypotheses is an essential ingredient of a good detective, whether the end is the solution of a crime or an intelligence estimate."[155]

Evaluating Hypotheses

Do not be misled by the fact that so much evidence supports your preconceived idea of which is the most likely hypothesis. That same evidence may be consistent with several different hypotheses. Focus on developing arguments *against* each hypothesis rather than trying to confirm hypotheses. In other words, pay particular attention to evidence or assumptions that suggest one or more hypotheses are *less* likely than the others.

Recognize that your conclusions may be driven by assumptions that determine how you interpret the evidence rather than by the evidence itself. Especially critical are assumptions about what is in another country's national interest and how things are usually done in that country. Assumptions are fine as long as they are made explicit in your analysis

155. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962), p. 302.

and you analyze the sensitivity of your conclusions to those assumptions. Ask yourself, would different assumptions lead to a different interpretation of the evidence and different conclusions?

Consider using the matrix format discussed in Chapter 8, "Analysis of Competing Hypotheses," to keep track of the evidence and how it relates to the various hypotheses.

Guard against the various cognitive biases. Especially dangerous are those biases that occur when you lack sufficient understanding of how a situation appears from another country's point of view. Do not fill gaps in your knowledge by assuming that the other side is likely to act in a certain way because that is how the US Government would act, or other Americans would act, under similar circumstances.

Recognize that the US perception of another country's national interest and decisionmaking processes often differs from how that country perceives its own interests and how decisions are actually made in that country. In 1989–90, for example, many analysts of Middle Eastern affairs clearly assumed that Iraq would demobilize part of its armed forces after the lengthy Iran-Iraq war so as to help rehabilitate the Iraqi economy. They also believed Baghdad would see that attacking a neighboring Arab country would not be in Iraq's best interest. We now know they were wrong.

When making a judgment about what another country is likely to do, invest whatever time and effort are needed to consult with whichever experts have the best understanding of what that country's government is actually thinking and how the decision is likely to be made.

Do not assume that every foreign government action is based on a rational decision in pursuit of identified goals. Recognize that government actions are sometimes best explained as a product of bargaining among semi-independent bureaucratic entities, following standard operating procedures under inappropriate circumstances, unintended consequences, failure to follow orders, confusion, accident, or coincidence.

Selecting the Most Likely Hypothesis

Proceed by trying to reject hypotheses rather than confirm them. The most likely hypothesis is usually the one with the least evidence against it, not the one with the most evidence for it.

In presenting your conclusions, note all the reasonable hypotheses that were considered. Cite the arguments and evidence supporting your

judgment, but also justify briefly why other alternatives were rejected or considered less likely. To avoid ambiguity, insert an odds ratio or probability range in parentheses after expressions of uncertainty in key judgments.

Ongoing Monitoring

In a rapidly changing, probabilistic world, analytical conclusions are always tentative. The situation may change, or it may remain unchanged while you receive new information that alters your understanding of it. Specify things to look for that, if observed, would suggest a significant change in the probabilities.

Pay particular attention to any feeling of surprise when new information does not fit your prior understanding. Consider whether this surprising information is consistent with an alternative hypothesis. A surprise or two, however small, may be the first clue that your understanding of what is happening requires some adjustment, is at best incomplete, or may be quite wrong.

Management of Analysis

The cognitive problems described in this book have implications for the management as well as the conduct of intelligence analysis. This concluding section looks at what managers of intelligence analysis can do to help create an organizational environment in which analytical excellence flourishes. These measures fall into four general categories: research, training, exposure to alternative mind-sets, and guiding analytical products.

Support for Research

Management should support research to gain a better understanding of the cognitive processes involved in making intelligence judgments. There is a need for better understanding of the thinking skills involved in intelligence analysis, how to test job applicants for these skills, and how to train analysts to improve these skills. Analysts also need a fuller understanding of how cognitive limitations affect intelligence analysis and how to minimize their impact. They need simple tools and techniques to help protect themselves from avoidable error. There is so much research to be done that it is difficult to know where to start.

Scholars selected for tours of duty in the Intelligence Community should include cognitive psychologists or other scholars of various backgrounds who are interested in studying the thinking processes of intelligence analysts. There should also be post-doctoral fellowships for promising scholars who could be encouraged to make a career of research in this field. Over time, this would contribute to building a better base of knowledge about how analysts do and/or should make analytical judgments and what tools or techniques can help them.

Management should also support research on the mind-sets and implicit mental models of intelligence analysts. Because these mind-sets or models serve as a "screen" or "lens" through which analysts perceive foreign developments, research to determine the nature of this "lens" may contribute as much to accurate judgments as does research focused more directly on the foreign areas themselves.[156]

Training

Most training of intelligence analysts is focused on organizational procedures, writing style, and methodological techniques. Analysts who write clearly are assumed to be thinking clearly. Yet it is quite possible to follow a faulty analytical process and write a clear and persuasive argument in support of an erroneous judgment.

More training time should be devoted to the thinking and reasoning processes involved in making intelligence judgments, and to the tools of the trade that are available to alleviate or compensate for the known cognitive problems encountered in analysis. This book is intended to support such training.

Training will be more effective if supplemented with ongoing advice and assistance. An experienced coach who can monitor and guide ongoing performance is a valuable supplement to classroom instruction

156. Graham Allison's work on the Cuban missile crisis (Essence of Decision, Little, Brown & Co., 1971) is an example of what I have in mind. Allison identified three alternative assumptions about how governments work--the rational actor model, organizational process model, and bureaucratic politics model. He then showed how an analystÍs implicit assumptions about the most appropriate model for analyzing a foreign government's behavior cause him or her to focus on different evidence and arrive at different conclusions. Another example is my own analysis of five alternative paths for making counterintelligence judgments in the controversial case of KGB defector Yuriy Nosenko. Richards J. Heuer, Jr., "Nosenko: Five Paths to Judgment," *Studies in Intelligence*, Vol. 31, No. 3 (Fall 1987), originally classified Secret but declassified and published in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency Internal Journal 1955-1992* (New Haven: Yale University Press, 1995).

in many fields, probably including intelligence analysis. This is supposed to be the job of the branch chief or senior analyst, but these officers are often too busy responding to other pressing demands on their time.

It would be worthwhile to consider how an analytical coaching staff might be formed to mentor new analysts or consult with analysts working particularly difficult issues. One possible model is the SCORE organization that exists in many communities. SCORE stands for Senior Corps of Retired Executives. It is a national organization of retired executives who volunteer their time to counsel young entrepreneurs starting their own businesses. It should be possible to form a small group of retired analysts who possess the skills and values that should be imparted to new analysts, and who would be willing to volunteer (or be hired) to come in several days a week to counsel junior analysts.

New analysts could be required to read a specified set of books or articles relating to analysis, and to attend a half-day meeting once a month to discuss the reading and other experiences related to their development as analysts. A comparable voluntary program could be conducted for experienced analysts. This would help make analysts more conscious of the procedures they use in doing analysis. In addition to their educational value, the required readings and discussion would give analysts a common experience and vocabulary for communicating with each other, and with management, about the problems of doing analysis.

My suggestions for writings that would qualify for a mandatory reading program include: Robert Jervis' *Perception and Misperception in International Politics* (Princeton University Press, 1977); Graham Allison's *Essence of Decision: Explaining the Cuban Missile Crisis* (Little, Brown, 1971); Ernest May's "*Lessons" of the Past: The Use and Misuse of History in American Foreign Policy* (Oxford University Press, 1973); Ephraim Kam's, *Surprise Attack* (Harvard University Press, 1988); Richard Betts' "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics,* Vol. 31, No. 1 (October 1978); Thomas Kuhn's *The Structure of Scientific Revolutions* (University of Chicago Press, 1970); and Robin Hogarth's *Judgement and Choice* (John Wiley, 1980). Although these were all written many years ago, they are classics of permanent value. Current analysts will doubtless have other works to recommend. CIA and Intelligence Community postmortem analyses of intelligence failure should also be part of the reading program.

To facilitate institutional memory and learning, thorough postmortem analyses should be conducted on all significant intelligence failures. Analytical (as distinct from collection) successes should also be studied. These analyses should be collated and maintained in a central location, available for review to identify the common characteristics of analytical failure and success. A meta-analysis of the causes and consequences of analytical success and failure should be widely distributed and used in training programs to heighten awareness of analytical problems.

To encourage learning from experience, even in the absence of a high-profile failure, management should require more frequent and systematic retrospective evaluation of analytical performance. One ought not generalize from any single instance of a correct or incorrect judgment, but a series of related judgments that are, or are not, borne out by subsequent events can reveal the accuracy or inaccuracy of the analyst's mental model. Obtaining systematic feedback on the accuracy of past judgments is frequently difficult or impossible, especially in the political intelligence field. Political judgments are normally couched in imprecise terms and are generally conditional upon other developments. Even in retrospect, there are no objective criteria for evaluating the accuracy of most political intelligence judgments as they are presently written.

In the economic and military fields, however, where estimates are frequently concerned with numerical quantities, systematic feedback on analytical performance is feasible. Retrospective evaluation should be standard procedure in those fields in which estimates are routinely updated at periodic intervals. The goal of learning from retrospective evaluation is achieved, however, only if it is accomplished as part of an objective search for improved understanding, not to identify scapegoats or assess blame. This requirement suggests that retrospective evaluation should be done routinely within the organizational unit that prepared the report, even at the cost of some loss of objectivity.

Exposure to Alternative Mind-Sets

The realities of bureaucratic life produce strong pressures for conformity. Management needs to make conscious efforts to ensure that well-reasoned competing views have the opportunity to surface within the Intelligence Community. Analysts need to enjoy a sense of security, so that partially developed new ideas may be expressed and bounced off

others as sounding boards with minimal fear of criticism for deviating from established orthodoxy.

Much of this book has dealt with ways of helping analysts remain more open to alternative views. Management can help by promoting the kinds of activities that confront analysts with alternative perspectives—consultation with outside experts, analytical debates, competitive analysis, devil's advocates, gaming, and interdisciplinary brainstorming.

Consultation with outside experts is especially important as a means of avoiding what Adm. David Jeremiah called the "everybody-thinks-like-us mindset" when making significant judgments that depend upon knowledge of a foreign culture. Intelligence analysts have often spent less time living in and absorbing the culture of the countries they are working on than outside experts on those countries. If analysts fail to understand the foreign culture, they will not see issues as the foreign government sees them. Instead, they may be inclined to mirror-image—that is, to assume that the other country's leaders think like we do. The analyst assumes that the other country will do what we would do if we were in their shoes.

Mirror-imaging is a common source of analytical error, and one that reportedly played a role in the Intelligence Community failure to warn of imminent Indian nuclear weapons testing in 1998. After leading a US Government team that analyzed this episode, Adm. Jeremiah recommended more systematic use of outside expertise whenever there is a major transition that may lead to policy changes, such as the Hindu nationalists' 1998 election victory and ascension to power in India.[157]

Pre-publication review of analytical reports offers another opportunity to bring alternative perspectives to bear on an issue. Review procedures should explicitly question the mental model employed by the analyst in searching for and examining evidence. What assumptions has the analyst made that are not discussed in the draft itself, but that underlie the principal judgments? What alternative hypotheses have been considered but rejected, and for what reason? What could cause the analyst to change his or her mind?

Ideally, the review process should include analysts from other areas who are not specialists in the subject matter of the report. Analysts within the same branch or division often share a similar mind-set. Past experience with review by analysts from other divisions or offices indi-

157. Transcript of Adm. David Jeremiah's news conference at CIA, 2 June 1998.

cates that critical thinkers whose expertise is in other areas make a significant contribution. They often see things or ask questions that the author has not seen or asked. Because they are not so absorbed in the substance, they are better able to identify the assumptions and assess the argumentation, internal consistency, logic, and relationship of the evidence to the conclusion. The reviewers also profit from the experience by learning standards for good analysis that are independent of the subject matter of the analysis.

Guiding Analytical Products

On key issues, management should reject most single-outcome analysis—that is, the single-minded focus on what the analyst believes is probably happening or most likely will happen. When we cannot afford to get it wrong, or when deception is a serious possibility, management should consider mandating a systematic analytical process such as the one described in Chapter 8, "Analysis of Competing Hypotheses." Analysts should be required to identify alternatives that were considered, justify why the alternatives are deemed less likely, and clearly express the degree of likelihood that events may not turn out as expected.

Even if the analyst firmly believes the odds are, say, three-to-one against something happening, that leaves a 25-percent chance that it will occur. Making this explicit helps to better define the problem for the policymaker. Does that 25-percent chance merit some form of contingency planning?

If the less likely hypothesis happens to be, for example, that a new Indian Government will actually follow through on its election campaign promise to conduct nuclear weapons testing, as recently occurred, even a 25-percent chance might be sufficient to put technical collection systems on increased alert.

Verbal expressions of uncertainty—such as possible, probable, unlikely, may, and could—have long been recognized as sources of ambiguity and misunderstanding. By themselves, most verbal expressions of uncertainty are empty shells. The reader or listener fills them with meaning through the context in which they are used and what is already in the reader's or listener's mind about that subject. An intelligence consumer's interpretation of imprecise probability judgments will always be biased in favor of consistency with what the reader already believes. That means the intelligence reports will be undervalued and have little impact on the

consumer's judgment. This ambiguity can be especially troubling when dealing with low-probability, high-impact dangers against which policymakers may wish to make contingency plans.

Managers of intelligence analysis need to convey to analysts that it is okay to be uncertain, as long as they clearly inform readers of the degree of uncertainty, sources of uncertainty, and what milestones to watch for that might clarify the situation. Inserting odds ratios or numerical probability ranges in parentheses to clarify key points of an analysis should be standard practice.

The likelihood of future surprises can be reduced if management assigns more resources to monitoring and analyzing seemingly low-probability events that will have a significant impact on US policy if they do occur. Analysts are often reluctant, on their own initiative, to devote time to studying things they do not believe will happen. This usually does not further an analyst's career, although it can ruin a career when the unexpected does happen. Given the day-to-day pressures of current events, it is necessary for managers and analysts to clearly identify which unlikely but high-impact events need to be analyzed and to allocate the resources to cover them.

One guideline for identifying unlikely events that merit the specific allocation of resources is to ask the following question: Are the chances of this happening, however small, sufficient that if policymakers fully understood the risks, they might want to make contingency plans or take some form of preventive or preemptive action? If the answer is yes, resources should be committed to analyze even what appears to be an unlikely outcome.

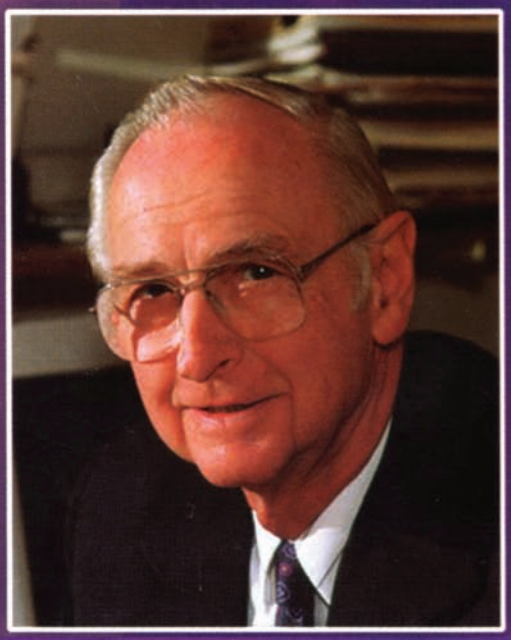
Managers of intelligence should support analyses that periodically re-examine key problems from the ground up in order to avoid the pitfalls of the incremental approach. Receipt of information in small increments over time facilitates assimilation of this information to the analyst's existing views. No one item of information may be sufficient to prompt the analyst to change a previous view. The cumulative message inherent in many pieces of information may be significant but is attenuated when this information is not examined as a whole.

Finally, management should educate consumers concerning the limitations as well as the capabilities of intelligence analysis and should define a set of realistic expectations as a standard against which to judge analytical performance.

The Bottom Line

Analysis can be improved! None of the measures discussed in this book will guarantee that accurate conclusions will be drawn from the incomplete and ambiguous information that intelligence analysts typically work with. Occasional intelligence failures must be expected. Collectively, however, the measures discussed here can certainly improve the odds in the analysts' favor.

The Author



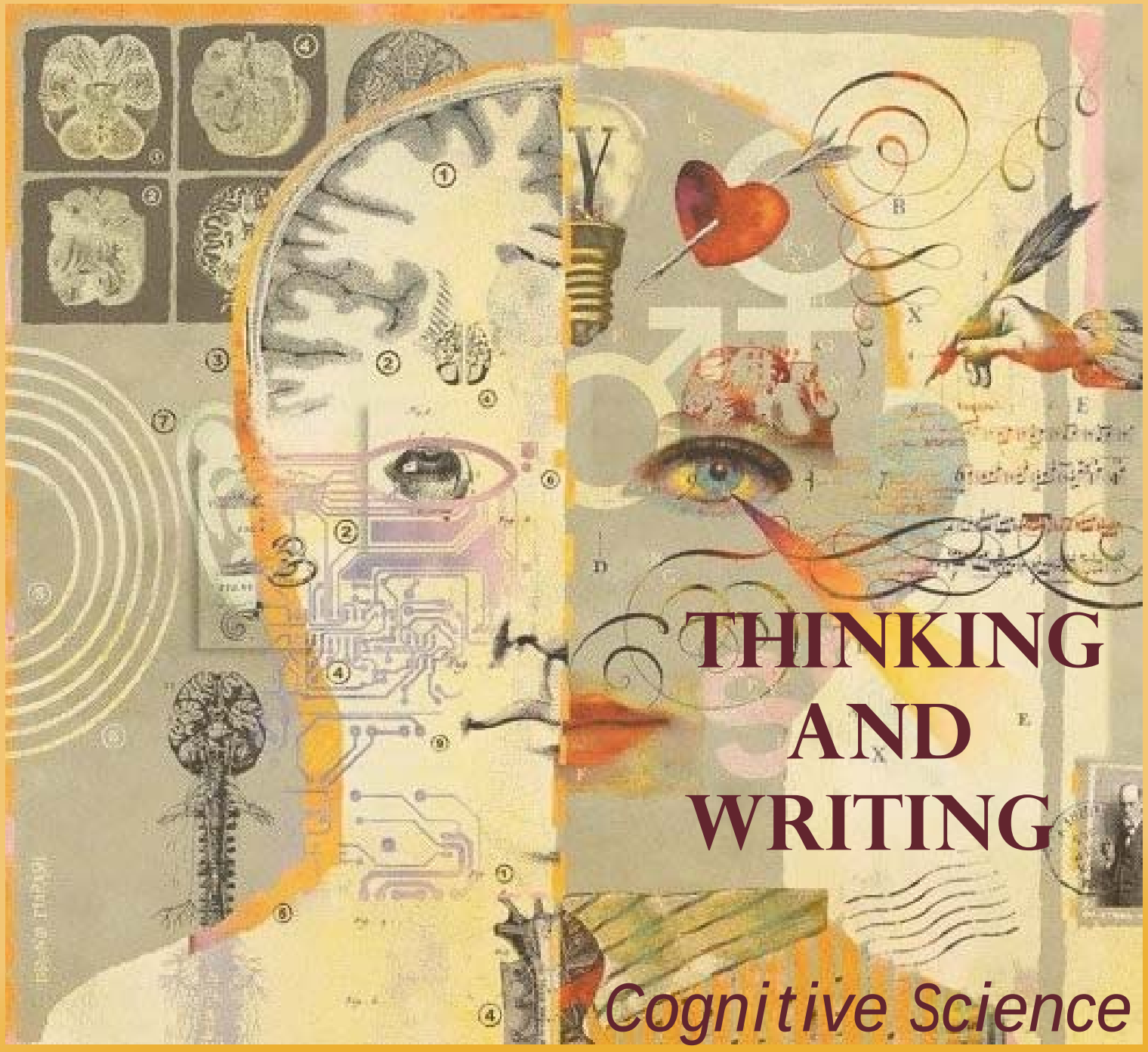
Richards J. Heuer, Jr. worked for the CIA for nearly 45 years—first as a staff officer from 1951 until his retirement in 1979 and then as a contractor on a variety of projects until 1995. He began his career in the Directorate of Operations and later transferred to the Directorate of Intelligence, where he headed the unit working on analytic methods in the Office of Political Analysis. He is now a consultant for the Defense Security Service's Security Research Center in Monterey, California.

Mr. Heuer was awarded the Agency Seal Medallion in 1987 for developing and teaching an innovative methodology for addressing complex and challenging problems facing the Intelligence Community. He was recognized in 1988 for his "outstanding contribution to the literature of intelligence," and again in 1996 for "superior accomplishment." In addition to his work on the psychology of intelligence analysis, Mr. Heuer is a published author on counterintelligence, deception, analytical methodology, and personnel security issues.

Many of the chapters in this book were originally written for the Directorate of Intelligence in the 1980s. They were recently edited and assembled, along with additional material that Mr. Heuer prepared specifically for this book, under the auspices of the CIA's Center for the Study of Intelligence.

I have been a fan of Richards Heuer ever since I met him and read some of his material 20 years ago. This book combines Dick's many years of experience with his extensive knowledge of psychological research. He examines impediments to good intelligence analysis and points the way to how to overcome them. The volume should be of real assistance to people faced with the need to draw sound estimates from changing and ambiguous information.

Robert Jervis
Professor, Institute of
War and Peace Studies
Columbia University



THINKING AND WRITING

Cognitive Science and Intelligence Analysis

By Robert S. Sinclair

CENTER *for the* STUDY *of* INTELLIGENCE

Revised edition of a monograph originally published by CSI in January 1984.

All statements of fact, opinion, or analysis expressed in this study are those of the author. They do not necessarily reflect official positions or views of the Central Intelligence Agency or any other US Government entity, past or present. Nothing in the contents should be construed as asserting or implying US Government endorsement of the study's factual statements and interpretations.

Cover image creator, Bruno Mallart.
© Images.com/Corbis.

Thinking and Writing:

Cognitive Science and Intelligence Analysis

Robert S. Sinclair

Center *for the* Study *of* Intelligence
Washington, DC
February 2010
Originally published in January 1984

This study was originally prepared by Robert Sinclair during a fellowship with the Center for the Study of Intelligence. It has been updated with a new introduction and slightly edited.

Robert Sinclair was a CIA intelligence analysts for 37 years. He is now a consultant on analytical issues.

The Center for the Study of Intelligence (CSI) was founded in 1974 in response to Director of Central Intelligence James Schlesinger's desire to create within CIA an organization that could "think through the functions of intelligence and bring the best intellects available to bear on intelligence problems." The Center, comprising professional historians and experienced practitioners, attempts to document lessons from past operations, explore the needs and expectations of intelligence consumers, and stimulate serious debate on current and future intelligence challenges.

To support these activities, CSI publishes *Studies in Intelligence*, as well as books and monographs addressing historical, operational, doctrinal, and theoretical aspects of the intelligence profession. It also administers the CIA Museum and maintains the Agency's Historical Intelligence Collection.

Readers wishing to have copies of this monograph or other CSI publications may call 703-613-1753 or secure 31753. Requests may also be sent via Lotus Notes to CSI-PubReq.

Contents

Introduction and Update v

A Quick Summary vi

Suggestion: Develop Collaborative Analysis vii

Suggestion: Increase Cognitive Diversity ix

Thinking and Writing: Cognitive Science and Intelligence Analysis

Summary 1

Recommendations 3

Preface 4

Introduction 4

I. A Quick Survey 6

II. Heuristics and the Incredible Chunk 8

III. Speaking and Writing, News and Knowledge 14

IV. Writing Schemes and Cognitive Overload 19

V. Creativity and the Conceptual Front End 21

VI. What Next? 26

1. Recruitment. 26

2. Training. 26

3. Analytic Writing. 26

4. Organization. 26

5. Presentational Methods. 27

6. Further Exploration. 27

Afterword 28

Introduction and Update

When this monograph was published a quarter-century ago, it sank virtually without a trace. It is clear to me now that the paper lacked what today would be called "curb appeal"; moreover, cognitive science was a new and unproven discipline. Then, few inside or outside the intelligence world were aware of it, and even fewer had thought about its relevance to intelligence analysis.[a]

The field has opened up to a stunning degree since then. Not only have we seen a flood of studies documenting the myriad cognitive activities our brains engage in, but electronic imaging allows us to observe what happens in the brain as it goes about its business. Authors like Malcolm Gladwell have mined the literature to show the insights these processes can produce, as well as the times they leave us stuck in unproductive ways of thinking. In *Blink: The Power of Thinking Without Thinking*, Gladwell reports that when experts were asked to assess the provenance of an allegedly ancient sculpture, they could agree that it was a fake but could not put into words how they had reached that conclusion. This and other examples, he says, illustrate how the things we learn through experience often are not readily available to our conscious minds.[b]

Economists these days speak of "behavioral economics," which uses research based partly on cognitive-science protocols to suggest the limits to rational-actor models. Behavioral economics has reinstalled John Maynard Keynes on his pedestal.

> *In economics, the crucial Keynesian concept is uncertainty. Where it prevails, the simple rules of classical economics don't apply. That's because the classical economics that both predated Keynes and superseded him relies on rational actors making rational assessments. In order to make such assessments you have to have reliable knowledge, usually derived from past experience. Buyers of oranges or newspapers or legal services can be said to possess such knowledge. Buyers of specula-*

a. One exception was Richards J. Heuer, whose articles, published in *Studies in Intelligence* beginning in 1978, helped trigger my own interest in the field. The CIA Center for the Study of Intelligence published an updated version of Heuer's articles in a book, *Psychology of Intelligence Analysis*, in 1999. Since reprinted by CIA and available commercially, the book is now a staple in many analytic training courses.

b. See Malcolm Gladwell, *Blink: The Power of Thinking Without Thinking* (New York: Little Brown and Company, 2005), 3-8. More recently, Gladwell told a story with a different outcome: In 2007 and 2008 the head of the investment firm Bear Stearns could not recognize, even in retrospect, the role his skills—the very skills that lay behind his earlier successes—played in his company's collapse. See Gladwell, "Cocksure: Banks, Battles, and the Psychology of Overconfidence," *New Yorker*, 27 July 2009.

Acknowledgements

I would be remiss if I failed to thank those who made this odd project possible, both now and 25 years ago: Mary-Ann Rozbicki, Paul Corscadden (both of whom have since passed away), and Carla Scopelitis—the first time around; and Carmen Medina, until December 2009, the director of the Center for the Study of Intelligence (CSI), which originally published this monograph, and CSI's Andy Vaart for its return. I would be doubly remiss if I failed to mention my gratitude to Jack Davis, the Directorate of Intelligence's long-time stealth subversive. Jack is one of the few people inside the Central Intelligence Agency who has sought to develop a genuine doctrine of intelligence analysis. His roller-coaster career—for a while in the 1970s and 1980s, it seemed that Jack was about to be fired at one moment, and at the next he was getting a medal for outstanding work—is in part a reflection of how difficult such a quest can be.

For me, Jack's early work with electronic mail (years before any of us had heard of the Internet) sensitized me to the medium's possibilities, including its culture-changing potential. He had kind words about my monograph from the outset, and he and I have had countless fruitful exchanges over the years. Finally, it was Jack who put the idea of reissuing the monograph into my head. He thus can claim a big share of the credit for the publication of this strange hybrid document; any shortcomings, of course, are my responsibility alone.

tive securities cannot. They're always looking into an uncertain future, "anticipating what average opinion expects the average opinion to be," as Keynes put it.[a]

And for its part, the Intelligence Community has taken a long list of initiatives ranging from structured analytic techniques to on-line blogs and social networking sites.

So why reissue this monograph? What could anyone gain from a 25-year-old piece on a subject that gets such broad coverage in today's popular literature? For me, the most telling answer came from a couple of talks based on the monograph that I gave in the spring of 2009. I spoke to conference-room-sized groups of analysts from CIA's Directorate of Intelligence (DI), and each time I had the impression that the talk was a revelation for most of the audience. Even after allowing as best I could for my own bias, I came away wondering whether information about cognitive science had percolated as widely as I had thought. In addition, in my regular interactions as a tutor of analysts and managers of analysts, I have similarly sensed that we have not absorbed the science into the way we think about our analytic jobs. Thus, one further attempt at consciousness-raising might not be out of place, especially since we have so many more ways to present this paper than we did 25 years ago.[b]

Moreover, while acknowledging that we have learned a great deal since 1984, I would argue that the elements of cognitive science highlighted in the monograph are still the ones of first-order relevance for the DI. I do not think an intelligence analyst will gain much professionally from knowing how neurons fire or which parts of the brain participate in which mental operations. I do consider it essential, however, that we be aware of how our brains ration what they make available to our conscious minds as they cope with the fact that our "ability to deal with knowledge is hugely exceeded by the potential knowledge contained in man's environment."[c] Not only do they select among outside stimuli, they also edit what they let us know about their own activities.[d] This is the focus of the monograph.

A Quick Summary

The monograph has two parts: first, a survey of cognitive science as we understood it in 1984; second, suggestions for changing the way we do intelligence analysis in light of what the discipline was telling us. As I have indicated, I think the survey section holds up pretty well. While I would like to think the reader will learn something useful from immersion in all the detail (notably the diagram on page 10, which makes graphic the many elements that interactively shape our conscious mental activity), the basic concept is quite simple. The conscious mind cannot track more than about seven cognitive elements at the same time (cognitive-science jargon often refers to these elements as *chunks*); and to cope with this constraint, our brains constantly manipulate those elements, always at top speed and usually outside our conscious awareness.

The second section is more of a mixed bag, but I believe the following concepts remain relevant:

- The importance of bringing to light what might be called, with a bow to former Defense Secretary Rumsfeld, the "unknown knowns"—the factors in our analysis that we are unaware of.

a. Justin Fox, review of two books about Keynes, *New York Times Book Review*, 1 November 2009, 13.

b. In 1984 CSI had no Web presence internally or externally, and the only way of delivering the findings of its fellows was through printed products advertised in internal notices or generated from searches conducted by library researchers.

c. Jerome Bruner, *On Knowing: Essays for the Left Hand* (Cambridge, MA: Harvard University Press, 1962), 240.

d. A recent book by two neuroscientists puts it this way:

Your brain lies to you a lot. . . . [It] doesn't intend to lie to you, of course. For the most part, it's doing a great job, working hard to help you survive and accomplish your goals in a complicated world. But because you often have to react quickly to emergencies and opportunities alike, your brain usually aims to get a half-assed answer in a hurry rather than a perfect answer that takes a while to figure out. Combined with the world's complexity, this means that your brain has to take shortcuts and make a lot of assumptions. Your brain's lies are in your best interest—most of the time—but they also lead to predictable mistakes.

See Sandra Aamodt and Sam Wang, *Welcome to Your Brain* (New York: Bloomsbury, 2008), 2.

- The conservative bias of our default analytic approach: we tend to work from what we already "know"—even though, in fact, a host of "unknown knowns" affect the "known."

- The solitary nature of the writing process and the difference between the way intelligence analysts typically do their work (linear, cerebral, mostly written) and the way policymakers do theirs (nonlinear, transactional, mostly oral and interactive).

- The importance of constructing our prose with the reader in mind; the monograph, summarizing the work of cognitive-science investigators, states, "A striking aspect of the approach of skilled writers is the frequency with which they think about how they are affecting the reader."

- The importance of the work done at the beginning of an analytic project—what the monograph calls the "conceptual front end."

- The time needed to gain real skill at a craft; the monograph cites data suggesting that people are unlikely to get good at what they do for at least a decade.

- The use that can be made of information technology to improve the quality of analysis.

Suggestion: Develop Collaborative Analysis

The Intelligence Community has not been blind to the potential in any of these areas. One has only to think of the emphasis on structured analysis and customer relevance; the attention we devote to scope notes; and the many blogs, the broader platforms such as A-Space and Intellipedia, and the coordination tools such as CIA's POINT.

Since I wrote the monograph, however, I have nurtured an idea that I think would move our analysis well beyond these accomplishments. The monograph is not terribly clear on this point since I still was laboring to articulate the idea; but as far back as 1984, I was sure that electronic interaction was the wave of the future for DI analysis. More specifically, I thought the time was at hand when we would be producing finished intelligence not just online but collaboratively.

The vision was reinforced later on when I read the introduction to *Thinking in Time,* by Harvard professors Richard Neustadt and Ernest May. The authors say they collaborated so closely that sometimes they lost track of who had written which part of the text.

> *In every sense of the word the book is coauthored. We taught together, class by class, and have written together, chapter by chapter. It has been a long process. We each wrote half the chapters in our first draft, then swapped them for redrafting with the rule that anything could be changed. Almost everything was. We had a further rule that any changes could be argued. Some were, some not. We carried on the argument by means of successive drafts, with new material subject to the same rules. There were so many swaps that each of us would change something only to be surprised by the other's "OK with me, you wrote it." We debated sources and argued out interpretations. Not only can we no longer remember who first wrote what, we cannot now remember who first thought what—or even who first found what when we jointly researched something. We are of one mind and (we hope) one voice."* [a]

I kept wondering, wouldn't this sort of approach benefit our work?

I am sure that some collaboration of this sort is occurring today, but I have seen little sign, a quarter-century after the monograph came out, of any impact on the way the community as a whole operates. I have given a good deal of thought to the reasons my vision was so wrong:

- First, the idea required orders of magnitude more bandwidth and much more sophisticated software than we had in 1984. This constraint no longer holds, of course. We have plenty of

a. Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: The Free Press, 1986), xii.

bandwidth, and programs to aid collaborative work are now widely available.

- Second, as I noted, the act of writing remains in essence a private process. To most writers, the idea of working interactively will seem like an intrusion into a space where they have always been alone.

- Third, the proposition faces serious cultural and organizational barriers. Hierarchy is at the core of any bureaucracy, including the DI's. The core of an analyst's performance evaluation is his or her publication record as an individual, and the serial review process is firmly ensconced as the way we generate our analytic product. A collaborative process would challenge the traditional approach in both areas. Managing it would require a healthy dollop of faith that something so messy and free-form can produce worthwhile results.[a] Furthermore, the obstacles loom larger in government bureaucracies than in the private sector. The risk/reward relationship is clearer in the latter, the budgetary process is more flexible and more under the control of management, and market competition and the bottom line will often prod managers toward innovation.[b]

- Fourth, interactive forums, whether Facebook and YouTube outside the community or Intellipedia and A-Space within it, may be enlightening for the participants, but nothing about them presses participants toward consensus or closure. Their mode is conversational; their strength lies in information-sharing and an ongoing batting-around of ideas. A participant might take insights reached online and use them elsewhere, but the idea of a discrete *product* coming out of such mediums seems almost a contradiction in terms.[c] The incentive to generate such a product would have to originate somewhere else.

- Finally, managers may have special difficulty adjusting to the interactive world. Lee Rainie of the Pew Internet and American Life Project distinguishes "nine tribes of the Internet." These, he says, can be divided into two groups: those "motivated by mobility" and the "stationary media majority." One component of the latter group is the "desktop veterans," who by themselves comprise 13 percent of the user population. Desktop veterans have been Internet users for 10.5 years on average; they are heavy users at home and work; 77 percent have cell phones. They are "content to use a high-speed connection and a desktop computer . . . [and] happy to be connected while they are stationary and sitting. So, they place their cell phone and mobile connections in the background. And their 2004 cell phone still serves its primary purpose for them—making phone calls. Online hit its zenith about 3-5 years ago when they first got broadband connections."[d] I myself am a charter member of this cohort.

I would guess that the older and more senior the manager, the more closely he or she will fit the "desktop veteran" profile. Such a manager will use electronic mail, word-processing software, spreadsheets, and presentational tools like PowerPoint. But he or she will have only second-hand familiarity

a. In the late 1970s the DI tried something analogous to this model (minus the IT element) in one of the offices responsible for political analysis. The branch-chief level of supervision was abolished, and analysts were encouraged to work on projects of their own choosing. A periodical called *Contra* was established to air alternative views. But over the next three or four years a sort of bureaucratic regression to the mean took place, and hierarchy and the review process reestablished themselves. *Contra* withered on the vine. The pendulum had swung far in the other direction by 1982, when Robert Gates (now the Secretary of Defense) took charge of the directorate. Gates undertook to review every draft himself and he pretty much did so.

b. The following is taken from Marc Ambinder, "Shutdown of Intelligence Community E-mail Network Sparks E-Rebellion," Blog: TheAtlantic.com, 6 October 2009:

> *A former chief technology officer at the Defense Intelligence Agency . . . [stated,] "in some cases we are seeing IT departments cancel everything associated with innovation—which would be a sign of a dying organization in the private sector."*

c. Whether a policymaker might find the online interchange useful is another question, one that is not addressed here but might be worth experimenting with.

d. Lee Ramie, "The Nine Tribes of the Internet." Presentation at the Washington Web Managers Roundtable, 10 June 2009.

with the interactive resources underlying any effort at online collaboration. (These will be more familiar to those in the lower ranks who are "motivated by mobility.") And if it is correct, as noted above, that (1) interactive media exchanges are unlikely to reach closure without outside encouragement, and (2) managers, the obvious source of such encouragement, are not familiar enough with interactive media to provide it, the odds are against the full exploitation of this resource.

Perhaps we need not worry about this. Or perhaps the requisite organizational and (even more important) cultural changes seem too costly and the benefits too uncertain. I would only point out that cognitive-science literature makes clear the shortcomings of the process now in use, which amounts to an end-to-end series of solo efforts to get a piece drafted and then to coordinate and review it.

For every analyst and every reviewer in this serial process, the analysis starts from a body of analogies and heuristics that are unique to that individual and grow out of his or her past experience—afterimages of ideas and events that resonate when we examine a current problem, practical rules of thumb that have proven useful over time.

The power of this approach is incontestable, but we are all too easily blinded to its weaknesses. The evidence is clear: analysis is likely to improve when we look beyond what is going on in our own heads—when we use any of several techniques designed to make explicit the underlying structure of our argument and when we encourage others to challenge our analogies and heuristics with their own. Little about the current process fosters such activities, it seems to me; they would be almost unavoidable in a collaborative environment.

Suggestion: Increase Cognitive Diversity

One final thought, which is based on little more than observations about myself and those around me: I call it "cognitive diversity." I believe the DI has always been populated very largely by serial thinkers like me, who analyze a problem by deconstructing it and laying out the result in writing, a quintessentially serial medium. I would of course be the last to decry this approach, but sometimes I am aware of getting so transfixed by my discoveries in the weeds that I have trouble getting back to the whole picture, much less the "so-what" that is the real purpose of the analysis. On the other hand, I have a good friend (he doesn't work in intelligence) who as far as I can tell has not a serial bone in his body. Sometimes, however, he can see the entirety of an issue when I am still back in the weeds, and sometimes he runs circles around me when it comes to the "so-what." In short, the analytic route taken by his mind differs from mine but is not necessarily less "analytic" in its own way, and sometimes he winds up in a more useful place than I do.

Might the DI do a better job if it were more cognitively diverse—if it took in more people with different cognitive "furniture"? I have opinions but no real answer to this question. I do believe diversifying the workforce in this way would require a cultural shift at least comparable to that involved in a shift to online substantive collaboration. Without such a shift, the directorate, like any organism under threat, would identify people who failed to fit the dominant pattern as foreign bodies and extrude them.

Thinking and Writing: Cognitive Science and Intelligence Analysis

By Robert S. Sinclair

Summary

The pages that follow describe some of the powerful metaphors about the workings of our minds that have developed over the past two decades, and attempt to apply those metaphors to the work of CIA's Directorate of Intelligence.[a] I believe the DI can thereby gain insights into such issues as the following:

- What is the best way to reconcile the bureaucratic imperatives of accountability, centralization, and structure with the fact that analytic work is essentially an individual effort?
- Can the directorate do a better job of pitching its analysis to catch the attention of its audience without sacrificing essential analytic detail?

I am not claiming that cognitive science offers definitive answers to such questions, but I do think it has something important to contribute to our understanding.

The term "cognitive science" embraces several disciplines, notably computer science, linguistics, and neurophysiology, as well as psychology. A cognitive scientist seeks to understand what the mind does when it searches for patterns, when it makes a value judgment, when it must choose between pattern-finding and judgment-making, when it engages in the myriad other activities that occupy it. Some fragmentary answers to questions such as this have become possible in the last 20 years.

Before they are six years old, nearly all humans learn to generalize, to impute continuity, to discern relationships, and to determine cause-and-effect. Moreover, we can store the conclusions drawn from such processes in a way that gives us access to them without burdening our working memory. We also learn a language, that uniquely human capacity which sits at the center of conscious cognitive activity. Language opens the way to abstraction and generalization, and permits each normal human to develop a rich network of concepts.

All of us are aware of the limitations of these processes. For example, we all are obtuse in dealing with logic and probability; we are comfortable with imprecision; and our minds are conservative in their approach to new information—quicker to recognize the familiar than the unfamiliar, reluctant to change concepts once we have accepted them. Finally, there are innumerable processes that influence our mental activity but are not accessible to the conscious part of the mind.

Some of the attributes that look like limitations, however, are actually the main sources of the mind's power; sloppiness is not just the bane but the strength of our mental activity. This is because of the role played by heuristics. The heuristic approach is a form of intelligent trial and error, in which we use experience and inference to refine a problem and render it workable. Few would give the process high marks for elegance, but it is quick, it gets the job done, and it keeps us from getting paralyzed by the range of choices confronting us. There are many disadvantages: the approach is inherently conservative, it tends to be imprecise, and it is not particularly congenial to logic, probability, and the scientific method. Nonetheless, heuristics are likely to remain the way we go about our busi-

a. The original monograph and this edition's introduction focus on CIA's Directorate of Intelligence because it is the analytic component of the Intelligence Community I am most familiar with. I hope, however, that the points I raise have relevance elsewhere in the IC's analytic world.

ness most of the time, particularly when we are deeply engaged in an issue.

The heuristic approach is based in part on deeply set mental patterns. “Working memory,” the part of the mind that does our conscious mental work, can handle about seven items at a time. In compensation, it can manipulate those items with extraordinary speed. Cognitive scientists refer to this manipulative capability as the mind’s *chunking* capacity—our ability to develop conceptual entities or *chunks*, to build hierarchies of those entities, to alter them, and to bring wildly differing entities together. We form chunks about any information that interests us, and we tend to believe our chunks are valid until the evidence that they are not is overwhelming. Each new bit of data is evaluated in light of the chunks already on hand; it is much harder to evaluate existing chunks on the basis of new evidence.

When we need to get through large quantities of data, when we do not have to move too far from an experiential reference point, and when a “best possible” solution suffices, heuristics and chunking can be amazingly effective, as Herbert Simon proved in his studies of first-class chess players. Such players are distinguished by the large number of board patterns (50,000, say) they keep in their long-term memories. Talent obviously is important as well, but Simon concluded that no one can become an expert player without such a store of chunks. Developing such a store in any field of mental activity is laborious, and there apparently are no shortcuts: the investment may not pay off for a decade.

All this information quickly takes on operational significance for the Directorate of Intelligence when we turn to writing, an activity that is simultaneously at the heart of the DI’s work and at the frontier of cognitive science. When cognitive scientists refer to the means used by humans to communicate with one another, they tend to use the term “language,” and unless they state otherwise, the word means speech rather than writing; few of them have focused on writing as a subject of research. Yet there are many ways in which the cognitive processes involved in writing differ from those involved in speech. Among other things, writing is capable of far more breadth and precision; neither complex ideas nor complex organizations would be possible without it. On the other hand, because everyone works with speech, whereas not everyone works very much with writing, speech is a far more general medium of exchange. I would argue that speech is the medium to which all of us, even the compulsive writers among us, turn when an issue engages our emotions; and above all, I think, speech is the medium of decisionmaking.

I find it impossible to avoid the conclusion that our work will do its job better if it includes an element of speech—if we aim for prose that has a conversational ring. Such prose would often differ from that now produced in the directorate, and I think it would strain the organization to turn in this direction. I do believe, however, that to do so would help us get our message across.

Conversational prose must be produced by the original writer; it cannot be edited in later. This implies there will be an additional burden on the writer, but it is easy to overstate the burden and misstate the way it would be felt. Cognitive science makes it clear that, although the writing process is extraordinarily convoluted, good writers represent the writing problem as a “complex speech act.” With them, the conversational element is already present to some degree.

In the words of one expert, “a writer in the act is a thinker on a full-time cognitive overload.” One principal source of the overload is that the writer creates a datum—a malleable entity outside the mind that grows out of the mind’s internal workings. The datum acts as an extension of working memory, but working memory itself cannot keep track of all aspects of the datum unless it shifts constantly from one aspect to another. Skilled writers have various ways of reducing the overload. For example, like the chess master with his 50,000 patterns, they use chunks stored in long-term memory. Or they satisfice—an ungainly bit of jargon referring to the mind’s ability to accept a “best-possible” solution, at least temporarily. One of the most effective techniques is to develop and monitor a variety of heuristic strategies. Typically there are three sorts of strategies:

- A scheme *To Do*, the overall rhetorical problem as posed by the person solving it.
- Subordinate to this scheme, a scheme *To Say*—the substantive points to be made.
- Finally, in coordination with the scheme *To Say*, a scheme *To Compose*, the interaction between ideas and the developing text.

Good writers, it has been found, spend much of their time considering schemes *To Do* and *To Compose*; unskilled writers concentrate on schemes *To Say*. A striking aspect of the skilled writer's approach is the frequency with which he or she thinks about the audience. The cognitive-science literature indicates that developing a vivid image of the audience tends to enhance substantive content as well. Thus, being clear about the overall strategy and refining one's concept of the audience offer a way to bridge the gap between speech and writing.

Cognitive science also sheds light on the tension between creativity and the demands of a structured organization like the DI. The problems can be reduced if we recognize the overriding importance of what we do right at the outset of the analytic process. It is here that the writer makes assumptions about the overall rhetorical problem—the strategy *To Do*. I suspect this strategy is not well articulated for much of the DI's work, and I think it is problems at this level that cause the real headaches. There is, moreover, a built-in potential for conflict between what happens at the "conceptual front end" and the demands of a necessarily serial review process: plans *To Do* may have to be articulated over and over as the process goes forward.

Plans *To Do* typically get articulated incrementally and heuristically in any case, and thus it takes time to find out what is going on. Not all analysts find such inquiries congenial, and managers at all levels begrudge the time. But to the extent that all concerned can work early and often at narrowing the gaps between various concepts of the scheme *To Do*, the chance of a bumpy review process will diminish, whatever creativity there is may be preserved, and a sense of collegiality will be enhanced.

Recommendations

These findings have obvious implications for the way the directorate recruits and trains its people. They suggest that more emphasis should be given to effectiveness at the *To-Do* level, and perhaps that skills of the *To-Say* variety are somewhat less important. Moreover, if it is true that around 10 years are needed to acquire a first-class network of chunks, training probably should figure far more heavily in the DI's thinking than it does now.

The trends already under way in the DI should encourage conversational prose, and the notion of bringing the audience into focus should help writers and reviewers establish common ground to work out the nonsubstantive aspects of a paper. It still will take repeated effort, however, to bridge the conceptual gaps that are bound to appear.

The conflict between organizational imperatives and the way analysts do their cognitive work might be reduced by divorcing substance from hierarchy as often as possible; through hierarchy-jumping in contacts with consumers; and by enfolding SAFE—which has the potential to bring significant changes in the way the directorate does its work—in the culture of the directorate. Concept papers could be made to bring out the *To Do* schemes of the various participants more clearly.

The directorate might explore the possibilities of non-written media, such as television, more extensively.

Finally, the ideas contained in this essay do not exhaust the possibilities offered by cognitive science. Suggestions for further work include a cognitive task analysis of the analytic process and an exploration of the extent to which the directorate's concentration on the written word limits its analytic flexibility.

Preface

This essay has its origins in the controversies over CIA's analytic work that arose after Vietnam and Watergate, the criticisms levied against the Agency by its principal consumers, and the Agency's efforts to respond to those criticisms. For much of this period it seemed that producer and consumer were talking past each other, and I sometimes thought that the resultant organizational tinkering was proceeding with little reference to the analytic work going on around me. The producer-consumer gap has since been greatly narrowed, and our analytic work seems more on target now than in the past. I have a sense, however, that we still do not understand the way we do our analysis, or the intricacies of the producer-consumer relationship, as well as we might. These are the questions addressed in the following pages. The essay is a layman's view of a body of knowledge that did not exist two decades ago, together with an attempt to lay out some operational implications of that knowledge.

The concerns that stimulated my inquiries still were pretty inchoate when I submitted my request for a sabbatical (in this sense the genesis of the essay exemplifies the cognitive processes it discusses). I think it is a tribute to those who approved the request—perhaps to their faith, perhaps to their gullibility—that I have been allowed to spend six months finding out what my questions were and then trying to answer them.

Introduction

Two quotations sum up what this essay is about:

Our insights into mental functioning are too often fashioned from observations of the sick and the handicapped. It is difficult to catch and record, let alone understand, the swift flight of a mind operating at its best.[a]

A writer in the act is a thinker on a full-time cognitive overload.[b]

The pages that follow will be concerned with the "mind operating at its best"—and in the Directorate of Intelligence, which operates mainly in the written mode, that usually means a mind "on a full-time cognitive overload." In brief, I hope to describe some of the powerful metaphors about the workings of our minds that have developed over the past couple of decades. I think these metaphors can help provide better answers to such questions as the following:

- What is the best way to reconcile the bureaucratic imperatives of accountability, centralization, and structure with the fact that analytic work is essentially an individual effort?
- Can the directorate do a better job of pitching its analysis to catch the attention of its audience without sacrificing essential analytic detail?

The hardest part of the essay to get right comes at the outset. Few readers are likely to know much about the territory I am asking them to explore, and much of the terminology—"cognitive science," "psycholinguistics," "neurophysiology"—is abstruse and off-putting. I believe, however, that the new territory is likely to prove surprisingly accessible. One of the virtues of cognitive science, in fact, is the way it gives insights into what we have been doing all along. Unlike Moliere's *bourgeois gentilhomme*, who was surprised to learn he had been speaking prose all his life, I think most of us will recognize ourselves in what follows.

But how relevant are these findings to the Directorate of Intelligence? Many might argue, for instance, that introspection of this sort will gain noth-

a. Bruner, *On Knowing,* 15.

b. Linda Flower and John R. Hayes, "The Dynamics of Composing: Making Plans and Juggling Constraints" (article provided by the authors).

ing at best and paralysis at worst. The point is just to do the analysis, and doing it is learned on the job, in consultation with our consumers. Those who hold this view probably would applaud the thought behind the following bit of doggerel:

A centipede was happy quite
Until a frog in fun
said, "Pray, which leg comes after which?"
This raised its mind to such a pitch
It lay distracted in a ditch
Considering how to run.

This is not an easy argument to dispose of, and the centipede will reappear from time to time in the pages that follow. The argument is based on the proposition, which seems correct to me, that the DI is essentially a craft shop, and I agree that most of the learning of a craft does take place on the job. But look again at the quotation from Flower and Hayes that I began with. If the very act of writing puts a writer—any writer at all—into "full-time cognitive overload," then perhaps we would benefit from a better understanding of what contributes to the overload.

The novelist and poet Walker Percy offers a concept that may be even more fruitful. In a series of essays dealing with human communication, Percy asserts that a radical distinction must be made between what he calls "knowledge" and what he calls "news."[a] Percy's notion takes on added significance in light of the findings of cognitive science (of which he seems largely unaware), and I will be discussing it at greater length in due course. For the present I would simply assert that the nature of our work forces us to swing constantly back and forth between knowledge and news, and I believe cognitive science has something to contribute to our understanding of the problem. I am not claiming it offers a panacea; I do think that in ways such as this it sheds powerful light on important practical issues.

A few clarifications are in order at the outset. First, although this essay talks a lot about writing, it is not designed to deal with the how-to-write issue. As the title indicates, its topic is thinking and writing—the complex mental patterns out of which writing comes, their strengths and limitations, and the challenges they create, not just for writers but for managers. I hope my suggestions are relevant to the never-ending struggle toward better writing, but I am trying to cast my net more broadly than that.

Second, it should be obvious that cognitive science is only one of many ways to approach human mental activity. Factors other than the cognitive activities discussed in this essay play major roles in the way we do our mental work—for example, the attitudinal predilections that can be measured by psychological testing, or the emotional factors discussed in the psychoanalytic literature. To my mind, however, the findings of cognitive science have special relevance for the way the directorate does its business because they illuminate the process itself as well as the equipment we bring to the procedure.

Third, I am not claiming to speak as an across-the-board expert in cognitive science. What follows is the result of very rapid chunking (a useful bit of cognitive-science jargon, as we shall see), and it tends to emphasize the work of Herbert Simon and his colleagues at Carnegie-Mellon University. I think there is good reason for such an emphasis since I believe their work has particular relevance for the DI's writing-based culture. I would be the last, however, to assert that what follows is a definitive treatment. That is why many of the suggestions in the last section are put as questions rather than assertions. My main goal is to start a discussion; any progress will need the help of real experts.

a. Walker Percy, *The Message in the Bottle* (New York; Farrar, Straus, and Giroux, 1982).

I. A Quick Survey

First we need to get some notion of what is involved in cognitive science. The term embraces several disciplines, notably computer science, linguistics, and neurophysiology, as well as psychology. Very broadly there are three main areas of inquiry: how the various parts of the brain (and the nervous system as a whole) interact, in both a neurological and a functional sense; how the human capacity for language is turned into specific linguistic skill; and how people analyze and solve problems, both simple and complex. To pick a starting point, we might say the field began to open up in 1959, when the linguist, and all-round radical thinker, Noam Chomsky published a scathing review of a book by B.F. Skinner, whose behavioral-science approach had dominated research into the workings of the mind up to that point.

Viewing the Interstate

To get some flavor of what this activity has produced, imagine that you are sharing my aerie on the 10th floor of a building that overlooks Interstate 66, just outside Washington, DC. Every afternoon we can watch a game involving the Virginia State Police and that rugged individualist, the Washington commuter. No car is supposed to use the westbound lanes of the interstate after 3:30 p.m. unless there are two or more people in it, but some commuters tempt fate every afternoon, and many afternoons the police are waiting for them as they come over the rise on the access ramp.

From our vantage point we can view this game in different ways. We can guess whether a specific car is going to be stopped. We can see if we can discern any patterns in the frequency with which the police appear. Or we can ponder the values that come into play when a government limits the use of a road and individuals decide to ignore the rules. In the latter case we can look at the conflict more or less dispassionately—guessing, perhaps, about the likelihood that the government will stick to its position—or we can join the fray, siding with either the government or the commuter. I would argue that all these activities are analogous to the sort of work DI analysts do at one time or another.

Now imagine that there is a third person, a cognitive scientist, in the room with us. To this person the interesting question is not the judgments you and I make about what is happening on the interstate, but the processes our minds use to make those judgments. He or she wants to know what the mind does when it searches for patterns, when it makes a value judgment, when it is forced to choose between pattern-finding and judgment-making, when it engages in the myriad other activities that occupy it. And the amazing thing— amazing given the physical complexity of the brain, where the neocortex alone contains something like 10 billion nerve cells, each capable of firing several times a second—is that some fragmentary answers are possible.

To illuminate the answers to the scientist's questions, we need to operate at a more elemental level. As you imagine yourself looking at the interstate, consider not the little drama that is going to begin when the next car gets to the top of the rise, but your perception of the car itself. A crucial point is that perception itself involves analytic work of a very basic sort. You constantly check out the characteristics of the car and match this information with information already in your memory. You then predict what the car is going to do next, and you check that prediction against what happens. You are not aware of these processes because long ago you learned them thoroughly (cognitive scientists would use the term "overlearned") and no longer have to waste the limited capacity of your working memory on them.

But it is worth pausing to reflect on what we all learn without apparent difficulty before the age of six. In the context of the I-66 example, any of us would know that the car that just emerged from behind the building across the way is the same one that disappeared behind the other side a few moments ago; that the term "car" can be applied to both the Continental and the Honda, however different they may appear, but not to the GMC pickup;

that the shiny metal and glass, glimpsed momentarily through a gap in the fence, is another passing car; and that the styrofoam cup in the road is being blown about because a car has just passed. In more formal terms, we all learned to generalize, to impute continuity, to discern relationships, and to determine cause-and-effect. And we can store the conclusions drawn from such processes in a way that gives us access to them without burdening our working memory. This is a formidable array of skills (they obviously are the basis for the skills used in the DI), and they all developed with such ease that the childhood process seems almost automatic.

But this is not all. We also learned to give names both to the things we see and to the relationships among those things. In short, we learned a language, the uniquely human capacity that sits at the center of all our conscious cognitive activity. Obviously it is language that permits us to communicate information of any complexity to each other, but in addition, language is a prerequisite for the steadily increasing complexity of which our own minds are capable as they develop. Naming a thing and naming its relationship with other things are themselves acts of abstraction and generalization, and once we have taken this step we can name relationships among relationships, thereby building a dense conceptual network.

All of us know, however, that if we did nothing but marvel at the achievements of our minds we would be leaving a lot unsaid. I am not referring to the times our mental processes prove inadequate to a task; I want to focus on the limitations these processes encounter even when they are working well—limitations, we often see more easily in others than in ourselves. For example, we all are determinedly obtuse when we attempt to deal with logic and probability. We are much readier to use them to buttress arguments we have already worked out than to discipline those arguments.

We also are surprisingly comfortable with imprecision. Douglas Hofstadter, in his brilliant and infuriatingly self-indulgent book, *Gödel, Escher, Bach*, states the situation well:

> *The amazing thing about language is how imprecisely we use it and still manage to get away with it. SHRDLU* [an artificial-intelligence computer program] *uses words in a "metallic" way, while people use them in a "spongy" or "rubbery" or even "Nutty-Puttyish" way. If words were nuts and bolts, people could make any bolt fit into any nut; they'd just squish the one into the other, as in some surrealistic painting where everything goes soft. Language, in human hands, becomes almost like a fluid, despite the coarse grain of its components.*[a]

A small example from close to home: a group of DI analysts, asked what numerical odds they would associate with the word "probable," gave answers ranging from 50 to 95 percent. Part of the tendency toward imprecision derives from the way humans surround every explicit statement with a cloud of assumptions. Our cognitive activity would be cumbersome indeed if we had to articulate all these assumptions, even though in not doing so we may discover afterwards that we were not talking about the same thing as someone else. Another factor making for imprecision is the element of abstraction that is built into language, since with abstractions it is difficult to be clear exactly what we are referring to. Indeed people deal in hierarchies of abstractions, and the DI generally operates toward the more abstract rather than the more concrete end of the hierarchies.

Moreover, our minds are conservative in the way they select information for processing by working memory. The capacity of working memory is tiny: It can only deal with about seven items of information at once. Yet the mind must sort through a welter of sensory data (held in very short-term buffers and all clamoring for attention) and must also make effective use of the information in long-term memory. Faced with this cacophony, our minds generally are quicker to recognize the familiar than the unfamiliar, and data already in our memories heavily influence the processing of new data. We rarely are fully conscious of the choices that are made. To put it more

a. Douglas Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid* (New York: Vintage Books, 1980), 674–75.

concisely, within broad limits, we see what we want to see and make what we want of what we see.

Complex though they are, moreover, these aspects of the mind's activities, which are at least partly conscious and volitional, are far from the whole story. The literature is full of information on processes of which we cannot be aware, processes that constantly affect our conscious mental operations.[a]

But given all this uncertainty, all these aspects of our minds that are in principle unknowable or beyond our control, what can introspection gain us? Don't you wind up in the ditch with the centipede if you start asking what goes on in our minds? In fact, however, it is by looking at some of these very attributes that we gain useful insights into the way we go about our work. Some things that up to now have looked like weaknesses are actually the main sources of the mind's power. It turns out that sloppiness is not just the bane but the strength of our mental activity.

a. These processes have been discovered through neurological investigations; they are distinct from the unconscious activities investigated by psychoanalysts. For further information, see Erich Harth, *Windows on the Mind* (New York; Morrow, 1982) and Gazzaniga and Ledoux, *The Integrated Mind* (New York: Plenum, 1978). Among other things, the latter book provides a useful corrective to the popular literature's treatment of the right brain/left brain phenomenon.

II. Heuristics and the Incredible Chunk

Some readers may remember the following episode from Jacques Tati's classic film comedy, *Mr. Hulot's Holiday*. The scene is a French railroad station. The camera takes in three platforms, and a little knot of travelers is waiting expectantly on the platform in the center. Suddenly the loudspeaker overhead begins to bleat a long and utterly unintelligible announcement; and just then a train slowly approaches the platform on the left. After a few moments of growing agitation the travelers, goaded by more bleats from the loudspeaker, disappear down the platform steps. They emerge on the left platform just as it becomes obvious that the train is going through without stopping. *Their* train is at that moment pulling in at the platform to the right.

The heuristic approach is a form of intelligent trial and error in which we use experience and inference…

This episode can serve as a model for the way our minds work in a much larger sphere. It is not hard to reconstruct the cognitive work being done—done at a furious pace—by the travelers. First, with the trains, they are following the overlearned patterns that we followed with the cars on the interstate: matching what their senses tell them with information already in their memories, they recognize the train and make some predictions for their senses to check out. But they then apply a similar process of perception/prediction/verification to information that for the most part is generated internally. What emerges is a collection of unspoken hypotheses, which might perhaps be put into words as follows: "My train is the next one scheduled; the loudspeaker almost certainly is announcing my train; that train over there seems to be the only one coming in; all trains must stop at the station; so the train over there must be mine." They easily reach a consensus; perhaps they even perceive that the train is slowing a bit (it's easy to let one's presuppositions affect one's perceptions). And, of course, they wind up looking silly.

But—and this is a critical part of the model—they do *not* miss their train. Further, I think anyone watching the movie would assume that even if the travelers make some mistakes, they still can catch the train if they scramble. In other words we and the travelers start from the idea that the system is built to accommodate a certain amount of trial and error.[a]

a. In New York City that is the case, according to the *New York Times*, which on 16 October 2009 reported that commuter trains almost always leave their platforms a minute after their scheduled departure times.

The jargon for the approach of the travelers is *heuristics*. A cognitive scientist might call their struggles a heuristic exploration of a poorly defined problem space; he or she would argue that heuristics offer a more satisfactory account of the way humans learn than the stimulus-response approach of the behavioral scientists. The heuristic approach is a form of intelligent trial-and-error, in which we use experience and inference to clarify, narrow, or otherwise refine a problem to make it workable. Logic has a role, but a subordinate one. The essence of the process is a non-random barging around. If we decide one tactic is not working, we back up and try another, but we are reluctant to do so. We tend to assume our theories are right until they are firmly disproven. Much of the time we end our search for solutions before we achieve the optimal outcome. We accept a "best-possible" solution and move on to something else, or to use the ungainly word invented (I think) by Herbert Simon, we satisfice.[a]

Few would give the process high marks for elegance, but it does deserve high marks for success. In other words, it works. Heuristics seem to have played a major role in the rapidity of human evolution, and they are equally prominent in the development of each individual. This is true of both cognitive and physical skills. The way children learn their native language is a particularly clear example. Preschool children do not learn a language by memorizing rules or parroting the sentences they hear. The essence of their approach from the very beginning is to experiment with linguistic patterns of their own. Using this approach they can learn rules of extraordinary complexity with little apparent trouble. Moreover, from the beginning, their linguistic activity has both a creative component and an element of satisficing. Logic and the scientific method—what Piaget called formal procedures—come late, are almost never fully assimilated, and seem to be used less systematically by nearly everyone after the age of 20 or so.[b]

What is it about heuristics that makes them so useful? First, they are quick and they get the job done, assuming the experiential base is sufficient and a certain amount of satisficing is not objectionable. Second, what cognitive scientists call the problem-space remains manageable. Theoretically that space becomes unmanageably large as soon as you start to generalize and explore: any event may be important now, any action on your part is possible, and you could get paralyzed by possibilities as the centipede did. But humans constantly narrow the problem-space on the basis of their own experience. And most of the time the results are acceptable: what more efficient way is there to narrow an indefinitely large problem-space?

But there are obvious limitations to the approach, and the limitations become more apparent when one faces issues like those confronting the DI:

- Heuristics are inherently conservative; they follow the tried-and-true method of building on what has already happened. When the approach is confronted with the oddball situation or when someone asks what is out there in the rest of the problem-space, heuristics begin to flounder. Yet we resist using other approaches, partly because we simply find them much less congenial, partly because the record allows plausible argument about their effectiveness when dealing with an indefinitely large set of possibilities.

- As most people use them, heuristics are imprecise and sloppy. Some of the reasons why cognitive activity is imprecise were noted earlier; another reason is the tendency to satisfice, which encourages us to go wherever experience dictates and stop when we have an adequate answer. With perseverance and sufficient information one can achieve considerable precision, but there is nothing in the heuristic approach itself that compels us to do so and little sign that humans have much of an urge to use it in this way. Most of the time,

a. The last syllable of the word rhymes with "dice." Herbert Simon, a Nobel laureate in economics, began delving into cognitive theory partly out of dissatisfaction with the benefits-maximizing "rational man" of classical economic theory. His "thinking man" is a satisficer. See Simon, *Models of Thought* (New Haven: Yale University Press, 1979), 3.

b. See Carol Gilligan and J.M. Murphy, "Development from "Adolescence to Adulthood: The Philosopher and the Dilemma of the Fact" in *Intellectual Development Beyond Childhood*, No. 5 in the series *New Directions for Child Development* (San Francisco, CA: Jossey-Bass, 1979).

moreover, the information is not terribly good. We then may find ourselves trying to get more precision out of the process than it can provide.

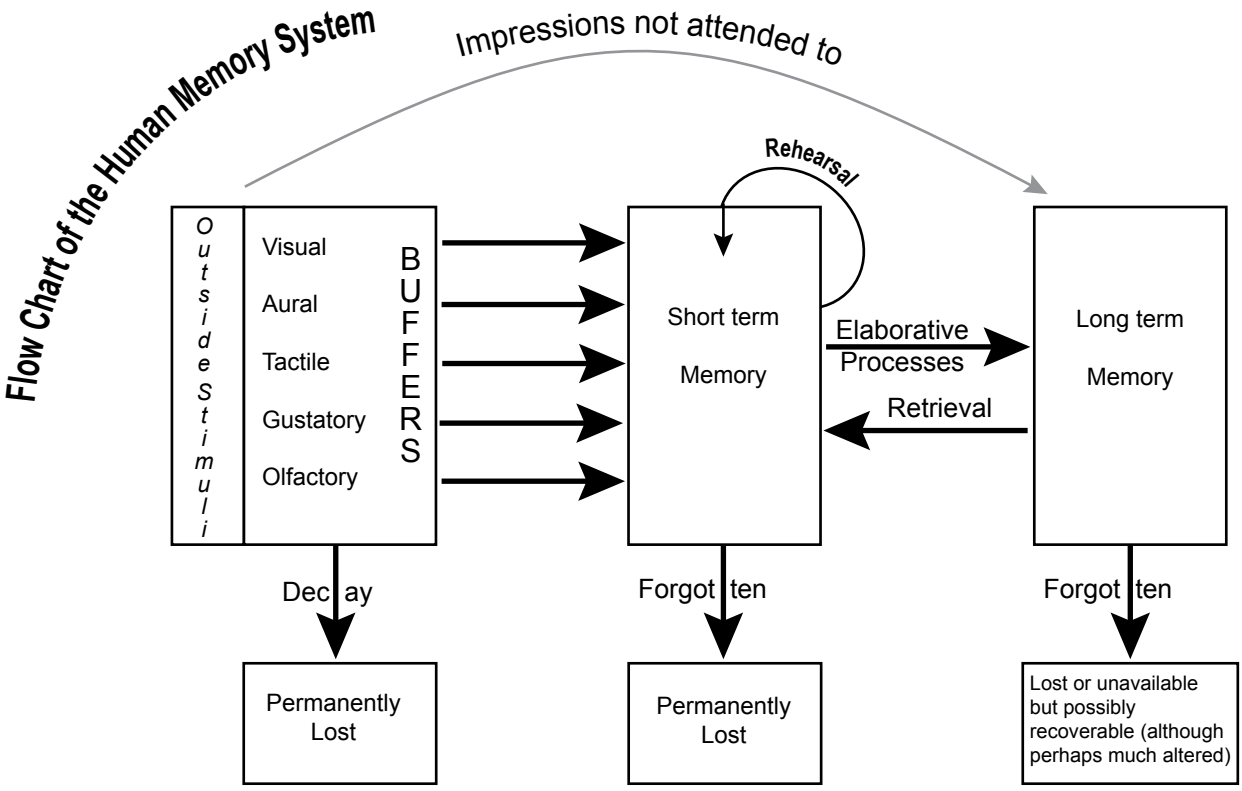
- In everyday use, heuristics are not congenial to formal procedures such as logic, probability, and the scientific method. This fact helps explain why we rarely use logic rigorously, why we tend to be more interested in confirming than in disconfirming a hypothesis, and why we are so poor at assessing odds.

Warts and all, however, heuristics are likely to remain the way we all go about our business most of the time. And it seems to me that the more deeply engaged we are, the likelier we are to operate this way. Perhaps it is an obvious proposition that humans use the approaches they are most comfortable with when an issue is important to them, and heuristics, whatever its drawbacks, are what we all are comfortable with.

One reason the heuristic approach is so deep-set is that it uses even more deeply set mental patterns. Once again at this level we find capabilities with great power (they let us run circles around computers in many respects) but with significant limitations as well—limitations we probably would be well advised to learn to work with rather than try to change.

The below diagram is typical of the way cognitive scientists represent the mind's operations.[a] We all have a system of buffers that enables us to organize incoming stimuli, a long-term memory of essentially infinite capacity, and a short-term or working memory that does our conscious mental work. At the level of generality at which we are operating, the roles of the buffers and long-term memory are fairly obvious. It is working memory that needs further discussion.

a.This particular diagram is taken from Morton Hunt, *The Universe Within* (New York: Simon and Schuster, 1982), l03.



The two salient features of working memory are its speed and its limited capacity. In one of P.G. Wodehouse's novels a particularly dunderheaded character is said to be capable of only "one thought at a time—if that," and the rest of us are closer to this standard than we might like to admit. As I noted earlier, working memory can handle perhaps seven items at a time. This number has to include not just substantive information but also any processing cues. If we have something we want to say in a complex sentence, for example, we must use one or more of the seven slots to keep track of where we are—which is one reason our spoken discourse rarely uses complex sentences.

It should be apparent the heuristic approach is critical to the effectiveness of our conscious mental activity, since short-term memory needs procedures like heuristics that narrow its field of view. On the other hand, the drawbacks are equally apparent. The ability to process large quantities of information is always an advantage and sometimes a necessity. How can we operate effectively if we can consider so little at a time? The answer to this question lies in the speed and flexibility with which we can manipulate the information in short-term memory; to use the terminology, in our *chunking* prowess.

In Morton Hunt's formulation, a *chunk* is

> *any coherent group of items of information that we can remember as if it were a single item; a word is a chunk of letters, remembered as easily as a single letter (but carrying much more information); a well-known date—say, 1776—is remembered as if it were one digit; and even a sentence, if familiar ("A stitch in time saves nine.") is remembered almost as effortlessly as a much smaller unit of information.*[a]

A chunk, it should be clear, equates to one of the roughly seven entities that short-term memory can deal with at one time. Hunt's formulation notwithstanding, it need not be tied to words or discrete symbols. Any conceptual entity—from a single letter to the notion of Kant's categorical imperative—can be a chunk. And not only do we work with chunks that come to us from the outside world, we create and remember chunks of our own. Anything in long-term memory probably has been put there by the chunking process. We build hierarchies of chunks, combining a group of them under a single conceptual heading (a new chunk), "filing" the subordinate ideas in long-term memory, and using the overall heading to gain access to them. We can manipulate any chunk or bring wildly differing chunks together, and we can do these things with great speed and flexibility.

Consider just two examples. First, the use you make of this essay. You are not likely to recall a single sentence of it when you finish; but you will (I hope) have stored ideas derived from it in your long-term memory. You will, in fact, have developed your own chunks on the basis of what you have read. If I have done my job there will be a great many such chunks, they will bear at least a familial resemblance to the ideas I am trying to explicate, you will have formulated them quickly and easily, and you will manipulate them on your own.

The second example is very different. Simon and his colleagues at Carnegie-Mellon University have specialized in the oral protocol, in which individuals are asked to articulate as much as possible of their thought-processes as they solve a problem or engage in some other kind of mental activity. Here is an excerpt from one such protocol, in which the subject has been asked to turn a simple story problem into an algebraic equation. The aspect that sheds light on the chunking process is the use of "it" at the two points where I have underlined the word.

> *We'll call the number n. It says that if we multiply <u>it</u> by 6 and add 44 to <u>it</u>, "the result is 68."* [b]

You will notice that superficially the meaning of "it" changes between the first and the second use; the word refers to *n* the first time and to *6n* the second. But there is an underlying sense in which "it" remains constant. One might articulate this sense as "the idea (or chunk) I am currently manipulat-

a. Morton Hunt, *The Universe Within*, 88.

b. Simon, *Models of Thought*, 209.

ing, whatever its specific content at the moment." Furthermore, this sense is clear enough for us to have little doubt what the person doing the protocol is trying to say. In this brief excerpt the subject of the experiment has been caught in the act of rapid chunking, and we have been caught in the act of comprehending the process without noticing it. The process was as quick for us as it was for the subject.[a]

In some ways "chunk" is a misleading term for the phenomenon. The word calls to mind something discrete and hard-edged, whereas the very essence of the phenomenon is the way we can give it new shapes and new characteristics, and the way conceptual fragments interpenetrate each other in long-term memory. A chunk might better be conceived of, metaphorically, as a pointer to information in long-term memory, and the information it retrieves as a cloud with a dense core and ill-defined edges. The mind can store an enormous number of such clouds, each overlapping many others.

This "cloudiness"—the way any one concept evokes a series of others—is a source of great efficiency in human communication; it is what lets us get the drift of a person's remarks without having all the implications spelled out. But it can also be a source of confusion. Consider the following examples, some showing efficiency, some opening the way for confusion.

- My teenage daughter, nervously trying to pour conditioner into a narrow-necked bottle, says, "This isn't going to work." But she doesn't hesitate in her pouring, and the job is completed without mishap. Her words, her inflections, and her actions have communicated a whole web of concepts to me (and perhaps to herself) which are far indeed from what she actually said.

- A boss comes out of an inner office, puts a small stack of typewritten pages on the secretary's desk, says, "There aren't enough copies," and goes back into the office. The secretary might tell you the boss had said to make more copies. The boss might agree. Both are working from assumptions that go unarticulated but not from what the boss actually said. (In addition you, the reader, may have thought of the boss as being male and the secretary as being female—another unarticulated assumption.)

- In a cognitive science lecture a speaker reads aloud the following sentences: "Mary heard the ice cream truck coming down the street. She remembered her birthday money and ran into the house." Those in the audience conclude that the sentences are about a little girl who is going to buy some ice cream; the speaker notes that this conclusion is based on inference, not on anything explicitly stated.

Cognitive scientists apply a variety of terms—"networks," "schemata," "scripts"—to the unspoken contexts into which we set pieces of information. The last example in particular makes clear how eager we are to build such contexts. Neither we nor the lecturer's audience had any obvious need to construct any story at all from those two sentences about Mary, yet nearly everyone does. We form chunks about any information that interests us, and (heuristics again) we tend to believe our chunks are valid until the evidence that they are not is overwhelming. And we form our chunks right away, as the information is coming in: there is no nonsense about waiting for a sufficiency of evidence. Each new bit of data is evaluated in light of the chunks already on hand, all of which are treated as at least arguably valid. We find it far more difficult to evaluate existing chunks on the basis of a new piece of data.

When we need to get through large quantities of data, when we do not have to move too far from an experiential reference point, when a "best possible" answer is sufficient (and these criteria are met most of the time), chunking can be amazingly effective. The approach works in contexts far more complicated than might be expected, as is indicated by the experiments with chess players conducted by Simon and others.

a. Another point this little excerpt brings to light is the degree of linguistic imprecision we can tolerate, particularly when we are dealing with spoken language

What are the hallmarks of a first-class chess player? Not, it seems, the ability to look further ahead in the game or to evaluate a larger number of possible moves; the master's approach is not much more extensive in these respects than the beginner's. What distinguishes the master and the grandmaster is the store of chess patterns built up in long-term memory over years of competition and study. Simon estimates that a first-class player will have 50,000 of these patterns to call on—by no means a small number, but orders of magnitude less than the theoretical possibilities that flow from any given position. The expert can use them to drastically reduce the number of choices he must consider at any point in a game, with the result that he often hits on an effective move with such speed that the observer attributes it to pure intuition.

So formidable is this ability (which is little more than heuristics and chunking) that humans were able to keep ahead of chess-playing computers for longer than most experts in the field predicted. When a computer that could beat nearly every human was developed, it did not duplicate the chunking approach but instead performed a brute-force search of all possible moves. Computers still are far inferior to humans in their ability to narrow the field heuristically, but they can now explore the whole field of chess moves in the time normally allowed between moves.

None of this emphasis on the importance of a' store of chunks is to deny the importance of individual talent in chess or any other field of mental activity. There is nothing that says you will automatically become a grandmaster if you simply lodge 50,000 or more chess patterns in your long-term memory. But you apparently cannot become a grandmaster *without* such a store of chunks, and cognitive scientists argue that a network of similar size and complexity is essential for effective work in most fields. Developing an adequate network is laborious and time-consuming, and there apparently are no shortcuts. Edison's aphorism about genius being two percent inspiration and 98 percent perspiration is buttressed by J.R. Hayes's discovery that almost without exception, classical composers did not start producing first-rate work until they were at least 10 years into their careers.[a]

By now we can speak in some detail about how the centipede runs—i.e., how humans do mental work. We still are speaking in highly schematic terms, the picture that emerges is exceedingly complex, and there is a great deal that cannot be addressed intelligently at all. But I think we can draw some illuminating conclusions, often humbling and heartening at the same time:

- Heuristics—non-random exploration that uses experience and inference to narrow the field of possibilities—loom large in the development of each individual and are deeply ingrained in all of us (particularly when we are doing something we consider important). Combined with the chunking speed of short-term memory, the heuristic approach is a powerful way to deal with large amounts of information and a poorly defined problem space.

- But there is always a tradeoff between range and precision. The more of the problem space you try to explore—and the "space," being conceptual rather than truly spatial, can have any number of dimensions—the harder it is to achieve a useful degree of specificity. Talent and experience can often reduce the conflict between the need for range and the need for precision, but they cannot eliminate it. We almost always end up satisficing.

- We are compulsive, in our need to chunk, to put information into a context. The context we start with heavily conditions the way we receive a new piece of information. We chunk so rapidly that "the problem," whatever it is, often

a. Mozart, who springs to mind as the obvious exception, turns out to have been a late bloomer by this standard. Hayes used a criterion for "first-rate work" that seems terribly unscientific at first: he decided that a composition qualified if five or more recordings of it were listed in the Schwann catalogue. The idea looks a bit more sensible at second glance, and in any case the consistency of Hayes's findings is striking. He obtained data for 76 composers and found only three—Satie, Shostakovich, and Paganini—who produced even one such piece within 10 years of the time they began studying music intensively.

has been sharply delimited by the time we begin manipulating it in working memory.

- Skill in a given area of mental activity involves both talent and time, the latter to build the extensive network of chunks that appears to be a prerequisite for really first-class work. The effort typically extends over several years; the investment may not pay off for a decade.

- Although the conceptual network formed through years of experience may make an individual a more skillful problem-solver, it can also make him or her less open to unusual ideas or information—a phenomenon sometimes termed "hardening of the categories." The conservative bias of the heuristic approach—the tendency we all share of looking to past experience for guidance—makes it easy for an old hand to argue an anomaly out of the way. In fact the old hand is likely to be right nearly all the time; experience usually does work as a model. But what about the situation when "nearly all the time" isn't good enough? Morton Hunt recounts an instance of a computer proving better than the staff of a mental hospital at predicting which patients were going to attempt suicide.

- Finally, the mental processes outlined in this section seem certain to remain the processes of choice for all of us. With all their drawbacks, heuristics remain arguably the most efficient way to narrow a large field of possibilities; and efficient or not, we like it.

So far, however, the findings we have discussed are little more than abstractions; they lack an operational context for the DI. And for good reason: the directorate is basically a writing organization, and cognitive science can hardly be relevant to our work until it addresses the main thing we do. As the section that follows makes clear, the focus quickly becomes operational as soon as the ideas accumulated so far are applied to the issue of writing.

III. Speaking and Writing, News and Knowledge

When people who deal with cognitive activity discuss the means we use to communicate with each other, they tend to refer to something they call "language." Unless they specify otherwise they generally mean spoken language, not writing. They discuss written language much less frequently, and when they do there sometimes is even a hint that they consider it less important than speech. Few have focused on it as a subject of research. This seems strange, since not only do these people make their living by the written word, they would have little hope of fully articulating their thoughts unless they had writing available as a tool.

Speech is the natural medium of decisionmaking....The essence of the decision process is oral.

What accounts for this phenomenon? First, it simply may not have occurred to them that there is a useful distinction to be made between speech and writing. Second, writing is a much more opaque process than speech and thus is harder to analyze. A speaker literally is making up what he says as he goes along, and it is relatively easy to gain insights into his cognitive activity by observing what he says and how he says it. The writing process is more convoluted and internal, and it is harder to get even a general notion of what is happening.

But I think there is a third reason, one that has great import for the way the directorate goes about its cognitive work. In some ways those who treat writing as less important than speech are right. The spoken word is the dominant (usually the only) linguistic medium in those preschool years when our basic conceptual furniture is being established, and I would argue that it is the medium to which we all, even the compulsive writers among us, naturally turn when an issue engages our emotions. Above all, I think, speech is the natural medium of decisionmaking. In my own family, when we are doing something hard like

picking a college for a high-schooler, we will write some transactional letters, and we will do some reading to gain information. But the essence of the decision process is oral. If this is true for someone like me—someone whose whole career has been involved with writing—how much truer must it be for those who do not see writing as a way of life. This latter group obviously includes most of humanity; it specifically includes nearly all of those for whom our written products are intended. I do not conclude from this that the directorate should get out of the writing business. I do not think we can do our work in any other medium. But if it can be shown that the cognitive processes involved in writing and speech differ in important respects, then I think it follows that the relationship between our writing-based work and our speech-oriented consumers deserves close attention.

Here are some of the ways in which writing and speech differ:

- With speech, much of the communication takes place in ways that do *not* involve words: in gesture, in tone of voice, in the larger context surrounding the exchange. Speech is a complex audio-visual event, and the implications we draw—the chunks we form—are derived from a whole network of signals. With writing there is nothing but the words on the paper. The result may be as rich as with speech—nobody would accuse a Shakespeare sonnet of lacking richness—but the resources used are far narrower.

- Writing calls for a sharper focus of attention on the part of both producer and receiver. When you and I are conversing, we both can attend to several other things—watching the passing crowd, worrying about some aspect of work, waving away a passing insect—and still keep the thread of our discourse. If I am writing or reading I must concentrate on the text; these other activities are likely to register as distractions.

- The pace and pattern of chunking is very different in the two modes. With speech, one word or phrase quickly supersedes the last, and the listener cannot stop to ponder any of them. What he ponders is the chunk he forms from his perception of everything the speaker is saying, and he is not likely to ponder even that very intensively. He does have the opportunity to ask the speaker about what he has heard (an opportunity almost never available to a reader), but he rarely does so; the spoken medium has enormous forward momentum. In compensation, speech uses a much narrower set of verbal formulae than writing. It relies heavily on extralinguistic cues, and by and large it is more closely tied to a larger context that helps keep the participants from straying too far from a common understanding. In the written medium, by contrast, the reader can chunk more or less at his own pace. He can always recheck his conclusion against the text, but he has little recourse beyond that. All the signals a writer can hope to send must be in the written words.

- A reader is dealing with a finished product: the production process has been essentially private. A listener is participating in a transaction that is still in progress, a transaction that is quintessentially social.

- Partly because of the factors listed so far, writing is capable of more breadth and more precision than speech. Neither complex ideas nor complex organizations would be possible without writing. My own impression is that even in this television-dominated era, people attach more solidity and permanence to something written than to something spoken. Perhaps we have an ingrained sense that the products of speech are more ephemeral than the products of writing. But to achieve this aura of permanence writing sacrifices a sense of immediacy. A writer tends to speak with the voice of an observer, not a participant.

Thus it appears that a person working with speech is doing markedly different things than a person working with writing. This is true whether the person is acting as a producer or a consumer. Further, because everyone works at times with speech—whereas not everyone works in any

comprehensive sense with writing—speech is a far more general medium of exchange. I suspect that most people tend to transfer what they have learned from writing into the spoken mode: usually that is where information gets used.

The transfer from writing to speech is made easier because the chunks I form after reading your text are most unlikely to take in all the detail you have laid out. The only way to work back toward your degree of detail is to reread your text, and I will not take in everything even if I do so (much of what you want to say is not even set down explicitly). If I do not go back I will operate with the chunks as they currently exist in my mind (and as they combine with other chunks, at least equally powerful, that my mind was working with before). This does not necessarily mean that my new set of chunks will be either less complex or less valid than yours; it does suggest that what I glean from your prose will be altered and simplified. Because of the simplification, what I have gleaned will be easily available for me to use in the speech mode. I will be all the more inclined to use it in this way if I am oriented toward decision and action, either generally or in this particular situation. If such is my inclination, I probably will do just what I did when the issue of sending children to college arose: view the text mainly in terms of what seems useful and ignore the rest.

The distinction I am making between writing-based and speech-based cognitive processes is illumined by Walker Percy's distinction between news and knowledge. To introduce his thesis Percy asks us to imagine an isolated island inhabited by people with a well-developed culture. On the shores of this island arrive thousands of sealed bottles, each bottle containing a single assertion like the following:

- E=MC2.
- A war party is approaching from Bora Bora.
- The dream symbol, house and balcony, usually represents a woman.
- Being comprises essence and existence.
- In 1943 the Russians murdered 10,000 Polish officers in the Katyn Forest.
- Tears, idle tears, I know not what they mean.
- There is fresh water in the next cove.
- Chicago is on the Hudson River or Chicago is not on the Hudson River.

An islander, Percy avers, might experiment with various ways of organizing these messages, but in the end would put each of them into one of two categories. The first category would include all the scientific and formal statements, all the generalizations, and also all the poetry and art. Producers of such statements are alike in their

> *withdrawal from the ordinary affairs of life to university, laboratory, studio, mountain eyrie, where they write sentences to which other men assent (or refuse to assent), saying, "Yes, this is indeed how things are."*

The second category would include statements that are significant

> *precisely insofar as the reader is caught up in the affairs and in the life of the island and insofar as he has not withdrawn into laboratory or seminar room.*

The statements about the Bora Bora war party and the water in the next cove would be obvious candidates for this category. The categories are neither hermetic nor unchanging. The statement about the Katyn massacre might be in either. The first category Percy calls knowledge; the second, news.[a]

Percy continues that not only are there two categories of information, they are read from two different postures, there are two different kinds of verifying procedures, and there are two different kinds of response:

- *Nature of the sentence*. Knowledge can in theory be arrived at "anywhere by anyone and

a. Percy, *The Message in the Bottle*, 119–39.

at any time"; news involves a nonrecurring event or state of affairs which bears on the life of the recipient.

- *Posture of the reader*. The reader of a piece of knowledge stands "outside and over against the world;" the reader of a piece of news is receiving information relevant to his specific situation.

- *Scale of Evaluation*. We judge knowledge according to the degree it achieves generality; we judge news according to its relevance to our own predicament.

- *Canons of acceptance*. We verify knowledge either experimentally or in light of past experience. News is "neither deducible, repeatable, nor otherwise confirmable *at the point of hearing*." We react to it on the basis of its relevance to our predicament, the credentials of the newsbearer (according to Percy, "a piece of news requires that there be a newsbearer"), and its plausibility.

- *Response of the reader*. A person receiving a piece of knowledge will assent to it or reject it; a person receiving a piece of news will take action in line with his evaluation of the news. (And, I would add, the receiver of a piece of news is more immediately concerned than the reader of a piece of knowledge with the correctness of the information.)

Obviously, I am building toward an assertion that the DI tends to deal in knowledge and our customers are interested mainly in news; and furthermore that there are correlations between news and the cognitive processes involved in speech on the one hand, and between knowledge and the cognitive processes involved in writing on the other. Equally obviously, the reality is not that simple, and the correlations are not exact. Not only does it demean our consumers to imply that they have little interest in knowledge as Percy defines it, but the distinction between news and knowledge, never airtight, has become increasingly problematic over time. With the information explosion and the widespread acceptance of the notion that knowledge is power (or to be more consistent with Percy's terminology, the notion that control over news is a source of power), speech- and action-oriented people have become ever more eager to scan knowledge-purveying documents for their news value. Moreover, the scope and depth of what such individuals are expected to know has expanded greatly. In both senses the potential domain of news has grown and has come to include regions that might in the past have been left to knowledge.

The boundaries get fuzzed in other ways. If I have discovered a new way to look at a problem, the discovery is likely to have the feel of news for me. But I may decide I have to use a knowledge-based mode to explain it. Perhaps, if I come from a scholarly environment, I believe knowledge has higher status than news. Or perhaps I do not think I can do justice to my discovery in a news-based mode—and if news, like speech, has a limited capacity to cope with complexity and my discovery is complex, my belief may have some validity. The recipient probably will duly register the resulting product as knowledge and may miss the sense of discovery altogether.

Finally, the material the DI deals with usually can fit under either heading, as was the case with the sentence about the Katyn massacre. A statement about the boiling point of water clearly is knowledge, and a statement about a fire that has just broken out in my office clearly is news; a statement about a balance-of-payments problem or a festering insurgency or a restive legislature could be either and is probably both. None of the latter statements is likely to have a high level of generality, none is likely to be easily verifiable under the canons of acceptance applicable to knowledge, and all are likely to involve the news-type question, "What (if anything) should the United States do?"

I still would argue, however, that when all is said and done the analytic work of the directorate fits more naturally on the knowledge side of the line and is inseparable from writing; whereas our consumers tend to look for news and to be more

comfortable with speech. I think this is one way of stating a basic challenge facing the directorate.[a]

I find it impossible to avoid the conclusion that we will do our work better if we include elements of speech and news. I also think that if we produce something that sounds like speech, it will tend to sound like news as well. I am not saying we should make our writing read like spoken English; the canons of speech and writing differ too greatly for that. But I do think we should aim for prose that has a conversational ring. How one does this is largely a matter of individual style, but some suggestions may be possible. Speech specializes in short sentences, it shies away from complex constructions, it uses short words (especially Anglo-Saxon ones), and it is peppered with verbs. Modelling prose around these characteristics—not inflexibly, not burdened by the specious claim that the result will inevitably be Dick-and-Jane (or perhaps Hemingway) prose—will, I think, help writing sound a little more like speech.

But don't you thereby rob yourself of conceptual complexity? Is it possible to lay out difficult ideas in conversational prose? All I can say is, it's been done. Whatever one thinks of Robert Pirsig's *Zen and the Art of Motorcycle Maintenance* in terms of substance, it does present some tough philosophical concepts in a palatable enough way to make the best-seller lists. The same is true of Hofstader's *Godel, Escher, Bach*. There is, in fact, a tradition of heavyweight conversational prose dating back as far as St. Paul and Plato. So at least in theory the idea is feasible. I would also urge all writers to ask themselves the following question: the idea may have been hard to clothe in words and get down on the page properly, but now that it is there, does it seem quite so complicated? Perhaps so; on the other hand, perhaps not. If the latter, perhaps putting it into more conversational language would not be too difficult.

This approach would nonetheless pose several problems. What I have called heavyweight conversational prose differs markedly in style from that usually produced by the directorate, and I think the differences arise from factors other than the DI's stylistic conventions and variations in individual writing skill. The most notable difference is that all the writers I cited as examples make extensive use of the first and second persons. This is a natural tendency when one is being conversational; one almost inevitably tries to personify the newsbearer and the recipient. I found in writing this essay that giving in to the tendency has a liberating effect.

A writer can forgo the first person singular and still be conversational— fortunately for the directorate, since the message-bearer for the news we write is a collective labeled "CIA," which can call itself "we" but never "I." The tendency to personify would persist, however. Even without the first person singular, I suspect the directorate's prose would take on a more individualistic cast. Moreover, a person writing in this mode is likely to assume a more actively persuasive tone and to risk crossing the line between persuasion and argumentativeness. These considerations lead me to believe that a turn toward conversational prose would add to the stress of the review and (perhaps even more) the coordination processes. I also think it is worth asking whether the structure would really be willing to tolerate a higher individuality quotient in the papers it produces.

I do not believe any substantial move would be made toward a greater news/speech content without tradeoffs such as these. They probably could be managed, if only because such changes in institutional style would have to come gradually, with large amounts of satisficing at every stage. But I do think such issues would have to be anticipated.

a. I also believe it is one factor making for turbulence in the flow of the review process. A reviewer, alive to the desires of the consumer, is likely to be looking for something resembling news/speech, whereas the writer will worry that the nuances and precision that can be conveyed only through knowledge/writing will be lost. What is pedestrian or convoluted to one is detailed and circumstantial to the other.

IV. Writing Schemes and Cognitive Overload

Only the original writer can impart a conversational tone to a draft, of course; it cannot be edited in later. Yet this essay has suggested that a writer is not likely to get his ideas articulated with the precision they require unless he works in a knowledge/writing mode, and that knowledge/writing is not inherently conversational. This implies that the writer would have to rework his prose even after the ideas had been articulated—a prospect few writers would relish. But putting the issue in these terms overstates the added burden and misstates the way it would be felt. The writing process is extraordinarily convoluted, and all writers constantly shift from one aspect of the problem to another. In this juggling act there is no question of deciding what you are going to say and then deciding how you are going to say it; writers—good writers in particular—work on all aspects of their problem virtually from beginning to end. If Flower and Hayes are correct, moreover, good writers represent this problem to themselves as a "complex speech act"; the conversational element is already present to some degree.

The writer does not decide what his ideas are and then decide how to communicate them; internal and external communication are of a piece.

Looking at the writing process as a whole will illuminate these notions. A writer is trying to accomplish two quite different things: to define what his ideas are by clothing them in words, and to communicate those ideas to others. Such is the nature of writing that the two goals are inextricably intertwined. To repeat, the writer does not decide what his ideas are and then decide how to communicate them; internal and external communication are of a piece. The complexity of this operation is one source of "cognitive overload." Another source is that as he writes, the writer is creating a datum—a malleable entity outside the mind that grows out of the mind's internal workings. The datum acts as an extension of working memory; the writer now has available a dependable array of chunks that is not limited by what working memory can attend to. Yet working memory itself is as tiny as ever, and it cannot keep track of all aspects of the datum unless it shifts constantly from one aspect to another.

Skilled writers use a variety of means to reduce the overload. For example, they satisfice. "Not the right word but what the hell," said one subject of an oral-protocol experiment at Carnegie-Mellon. The context indicates he was implying that the word was good enough for now and could be polished when working memory had been cleared of other demands. Or they draw on patterns stored in long-term memory, just as the skilled chess player does. (The patterns must be appropriate, of course. A new arrival in the DI is likely to discover that many patterns learned earlier no longer work, and building a store of, say, 50,000 patterns that do work takes time.) According to Flower and Hayes, perhaps the most effective technique of all is what they call "planning"—but the term takes on a different meaning in this context. It does not simply equate with outlining. In fact, Flower and Hayes found in their analysis of oral protocols that few people made use of outlines or other structured techniques. "Planning" might better be thought of as developing heuristic strategies and monitoring those strategies.

Flower and Hayes suggest that there are three different sorts of strategies:

- At the highest level, a strategy *To Do*. This is the rhetorical problem the writer sets out for himself: "Write a current intelligence article shooting down this coup report"; "Turn out something that will get through the review process without too much hassle"; "Write a paper that shows how stupid the conventional wisdom is"; "Set down this new idea."

- Next, a strategy *To Say*. This is essentially a content plan—the points to be gotten across to the reader. One can jot down informal notes or work up a detailed outline. "A plan *To Say* is

essentially a scale model of the final product. Perhaps that is why it has been so widely and vigorously taught, often to the exclusion of any other kind of planning." The plan *To Say* is subordinate to the plan *To Do*.

- Finally, and coordinate with the strategy *To Say*, a strategy *To Compose*. This category includes the interaction between ideas and the developing text. It includes short-range mental notes like "I'll write down a bunch of ideas and connect them later." or "A point I will want to make someplace is that…"

Failure to go beyond a plan *To Say* is a good route to ineffective prose. Skilled writers are adept at using all three strategies in conjunction with each other, checking and rechecking one against another and monitoring how each is working. They spend less time considering plans *To Say* than do novices, and more time considering the overall assignment (plans *To Do*) and the rhetorical challenges involved (plans *To Compose*). Flower and Hayes add: "Moreover, as they write, they continue to develop their image of the reader, the situation, and their own goals with increasing detail and specificity."

A striking aspect of the approach of skilled writers is the frequency with which they think about how they are affecting the reader. A comparison between two writers of different skill levels is shown in the table below. The expert spoke of the way he represented the audience and the assignment more than twice as often as the novice did, and he spoke of goals vis-a-vis the audience 11 times, whereas the novice did not consider this aspect of the problem at all. By contrast, the two were quite similar in the frequency with which they addressed questions of text and meaning. Hayes and Flower go on to assert that being alive to the audience and other aspects of the rhetorical context enriches substantive content as well. With a good writer three fifths of the new ideas grew out of thoughts about the assignment, the audience, or the writer's own goals; whereas with poor writers 70 percent of the new ideas flowed from the topic itself. "All of this suggests that setting up goals to affect a reader is not only a reasonable act, but a powerful strategy for generating new ideas and exploring…a topic."

Here we have, I think, a way of closing the gap between news/speech and knowledge/writing. Perhaps, in setting up the dichotomy between news and knowledge, Percy underestimated the wiliness of the skilled writer. Perhaps the body of information that he calls knowledge is roughly equivalent to what a writer would work with under a plan *To Say*—the substantive points to be made. But Flower and Hayes say the mark of a good writer is the resources devoted to the aspects of the problem other than the substantive points, especially the strategy *To Do*. Attention to these areas—and in particular, treating the audience as a vivid entity—is what distinguishes those who can turn the process of creating text into a "complex speech act." For such writers, conversational prose not only is possible, it is what they tend to produce.[a] Thus to move writing back toward speech and knowledge back toward news, a writer should be urged to treat the nonsubstantive aspects of the assignment with the importance they deserve. It usually will not be possible to retain all the density of argumentation that knowledge/writing can achieve, but a surprising percentage can be preserved, and what does get set out has a much better chance of actually being transferred.

a. This notion is buttressed by the examples of "good writing" included in my favorite how-to-write book, Jacques Barzun's *Simple and Direct*. The writers whom Barzun singled out range from Dorothy Sayers to Eric Hoffer to a man writing about how to use a saw. Nearly all of them, and Barzun himself for that matter, produced what I have been calling conversational prose.

	Analysis of rhetorical situation: Audience and Assignment		Analysis of goals			
		Audience	Self	Text	Meaning	Total
Novice	7	0	0	3	7	17
Expert	18	11	1	3	9	42
Number of times writer explicitly represented each aspect of the rhetorical problem in first 60 lines of protocol						

V. Creativity and the Conceptual Front End

One of the enduring concerns of DI analysts is the creativity issue. What role is there for creativity in a structured, basically hierarchical organization—an organization, moreover, that operates more or less according to craft-work standards? Doesn't such an organization run the risk of stunting creativity, making do with run-of-the-mill analysis, and perhaps missing important trends? On the other hand, some might argue that creativity is not even particularly relevant to what we do. The important goal is to meet the needs (stated and implicit) of our consumers in a timely and accurate way, and tons of creativity will not help if this goal is not met. An organization has both the ability and the obligation to impose norms, these people might argue; constraints of some sort are bound to turn up sooner or later, and they almost certainly will seem arbitrary when they do. So why not impose the constraints of the craft, which at least have the virtue of some consistency and continuity?

What role is there for creativity in a structured, basically hierarchical organization ?

This argument is clouded by a definitional problem which needs to be disposed of before we can address the issue constructively. Creativity usually is treated as a rare phenomenon, and so it is under the usual definition. But the whole cognitive process actually has a creative component, and in this specific sense creativity is all around us. I believe many of the problems confronting an organization like the DI, whose raison d'etre is the intellectual activity of the people who comprise it, flow from the conflict between these two sorts of creativity.

Herbert Simon provides a useful list of the criteria by which the creative aspect of a piece of work is judged:

- The work has novelty and value (either for the originator or for his culture).
- It is unconventional in the sense that it requires modification or rejection of previously accepted ideas.
- It requires high motivation and persistence, taking place either over a considerable span of time (continuously or intermittently) or at high intensity.
- The problem as initially posed was vague and ill-defined, so that part of the task was to formulate the problem itself.[a]

Simon notes that not all the criteria need be satisfied before a work is considered creative. I would go further and assert that for the individual producing the work, one criterion suffices by itself: that the work have "novelty and value…for the originator." Furthermore, the nature of the cognitive process is such that almost everything produced will meet this criterion. I noted early in this essay that a child's approach to the learning of a language has a creative as well as a satisficing element. A child discovers how language works by constructing original sentences, sentences that did not exist until he formed them. I suspect that pleasure at having produced something new is a powerful force for further linguistic exploration and that an overlearned (and thus unconscious) sense of satisfaction accounts for part of the conversational dynamic in adults.

The creative component in this narrow, individualistic sense is if anything even more apparent with written work. With speech, the words are ephemeral and part of a social process. The individual producing them cannot get too closely identified with them; they are tossed into the conversational stream and soon are lost to consciousness, leaving nothing behind but an assortment of conceptual chunks in the memories of those participating

a. Simon, *Models of Thought*, 139.

in the exchange. (People do, of course, identify themselves closely with the chunks.) By contrast, a person producing a written sentence is bringing something discrete and durable into existence, and I would suppose that the sense of having created something is all the stronger for that reason. The private nature of the writing process reinforces this sense. Moreover, the imbalance in emotional investment between producer and consumer—the one closely involved with the specific words, the other much less so—is likely to be more apparent with writing.

The writer must circulate his text to others; this is part of his unspoken contract with the rest of the world. The criteria at this point, however, are the other items on Simon's list, which are all essentially social rather than individual, and society discerns creativity less often than the individual does in himself. An organization, moreover, is necessarily concerned with standards of some sort, and it has a right to require a degree of conformity from the journeyman.

Acceptance of such norms does not always hobble creativity. Until the last couple of centuries much of the great art was produced by people whose outlook was that of craftsmen. Consider the following comment by Jerome Bruner:

> *One cannot help but compare the autobiographic fragment left by Ghiberti, discussing the long period during which he worked on the famous doors of the Baptistery at Florence, with the personal writing, say, of a modern sculptor like Henry Moore. Ghiberti talks of the material that was "needed" to do the designs that were "required." It is as if it were all "out there." Moore is concerned with the creating of illusions and symbols, and self-awareness for him is as important as a stone chisel.*[a]

Yet it does seem to me that creativity is important for an organization like the DI, and that such an organization constantly runs the risk of inhibiting the creative component in the work of its people. Few, I suspect, would dispute the proposition that satisfying consumer needs is aided by a certain degree of creativity, and to me it is equally obvious that some sort of creativity is essential if the directorate is to satisfy the predictive aspect of its mission as well as possible. I would also suppose that work deemed creative under Simon's broader, socially determined criteria must have creativity in the narrow sense as a precondition. It is here that the risks arise for an organization like the DI. The following examples cited by Morton Hunt support this argument.

> *In one of Torrance's many studies of creativity in school children, children were given pencils, crayons, and simple collage materials and told to make a picture that no one else would be likely to come up with. A variety of kinds of comment and appraisal were given to different groups of the children, and some got no evaluation at all. The upshot: those who worked without evaluation turned out pictures that were more creative than those produced by children receiving the most constructive commentary. In a study by another researcher, a group of students were told they would earn a reward for thinking up the largest number of plot titles and stories; their output was less imaginative and original than that of another group who expected no reward. Merely, knowing that one's work will be critically appraised by experts after it is finished has a negative influence. Teresa Amabile, in her collage studies, told one group of college women that their efforts would be judged by artists, while another group was told nothing; the latter group did significantly more creative work.*[b]

One can easily criticize research such as this. For example, how is it possible to judge something as subjective as creativity? Might not the researchers have gone into their studies with biases that skewed the results? Perhaps a more telling point is that the subjects of the experiments seem not to have had much skill or experience in the activities they were engaged in, and thus may have been particularly sensitive to the notion of being judged. One might expect a more complex situation, for

a. Bruner, *On Knowing*, 54.

b. Morton Hunt, *The Universe Within*, 313.

instance, if an experienced artist was faced with the possibility of being judged by other artists. But even taking such objections into account, the notion of creativity being inhibited by the mere prospect of outside comment—even positive comment—is thought-provoking. Even a skilled artist might be inhibited if he was required to keep in the front of his mind the evaluation to which his work was to be submitted. Yet this is a requirement which a structured organization can hardly avoid imposing.

Or consider the comment by Jacob Bronowski in his Silliman lectures at Yale in 1967:

> *The society of scientists, the community of scientists, has this advantage, that from the moment we enter it, we all know that fifty years from now, most of the things we learned here will turn out not to have been quite right. And yet that will have been achieved without enormous personal dramas. It will be achieved by giving due honor to the people who take the steps, the steps that turn out to be wrong as well as the steps that turn out to be right.*[a]

Again one can quibble: surely it is only the "steps that turn out to be right" which win Nobel prizes. But the essence of Bronowski's argument is hard to dispute. Science does reserve a place of honor for those who explore blind alleys, not least because discovery is as likely to proceed from an earlier error or ambiguity as from an earlier truth. The place of error in a structured organization, on the other hand, is much less certain, particularly if accountability is one of the driving forces in that organization. Even with the best will in the world such an organization is likely to put a premium on being right. As a result tentative ideas may have a harder time surviving, and there may be a tendency to equate "being right" with "not being wrong." If so, caution and the school solution will have an easier time of it than they might otherwise have.

a. Jacob Bronowski, *The Origins of Knowledge and Imagination* (New Haven: Yale University Press, 1978), 133.

And yet the Directorate of Intelligence cannot devote many of its resources to nurturing creativity, at least under any very expansive definition of the term. Like any craft organization, the DI has jobs to do, and worrying about creativity would often get in the way. Moreover, much of the activity we report and analyze is actually pretty ordinary or closely tied to a narrow set of events, and with work of such an ephemeral nature the scope for creativity is limited. Finally, there is no guarantee that you will get more creativity if you do nurture it. I know of no approach that has proven more capable than others of producing results which are simultaneously creative, valid, relevant, and efficient.

Yet, the DI cannot devote many resources to nurturing creativity... it has jobs to do and worrying about creativity would often get in the way.

The concepts discussed in this essay do, however, offer some hints about reducing the tension between structure and creativity—reducing rather than eliminating, since the sources of tension will not go away and we are certain to wind up satisficing. The key is the importance of the work we do right at the outset of the process. Simon notes at one point, "Much of the skilled processing in chess occurs at the perceptual front end." This proposition holds for all cognitive activity, although in the DI's case it may be more accurate to talk about a conceptual rather than a perceptual front end. Being clear what is going on at the beginning takes on overwhelming importance in light of cognitive scientists' findings; moreover, there is a built-in potential for conflict between what happens at the conceptual front end and what happens during a necessarily serial review process.

The importance, as well as the difficulty, of defining what is happening at the start is put into clearer relief by an obvious point made by Flower and Hayes: "People only solve the problems they give themselves." I cannot give you a problem to solve; I can try to interest you in a problem; I can talk it through it with you; if I am your boss, I can order you to take it on. But the problem you solve still will be the one you pose to yourself, not the one I have given you. The two will rarely be congruent, and if we are not clear with each other they may diverge

drastically. Each of us will have sharply narrowed our concept of the problem by the time we begin to talk about it, and neither my concept nor yours will be confined to the substance of the issue. We both will have a complex set of assumptions as well as an assortment of goals, usually unspoken, that we hope to achieve. If I am your boss one of my goals might be, "Try once more to get some worthwhile prose out of this analyst." You, the subordinate, might have "Get this guy off my back" as one of yours. Both goals will affect the product—your goals more than mine, in fact, since as the one in charge of the keyboard you have the biggest role in deciding how the problem will actually be solved.[a]

The problem you give yourself to solve is roughly equivalent to your strategy *To Do*—the rhetorical challenge in all its complexity, as it is posed by the person meeting it. This is easily the most important part of the "conceptual front end" to articulate, particularly if the topic is difficult or controversial or if it is breaking new analytic ground. I suspect it is the part that is least well articulated for much of the DI's work. Most of the time we focus on the areas of *To Say* and *To Compose*—the points we are going to make and the way we are going to express them. But problems in these areas are often easy to fix. It is the unspoken divergences at the level of plans *To Do*, I believe, that cause the real headaches. This is particularly true if such divergences do not come to light until a paper makes its way up through the hierarchy.

It is terribly hard to articulate one's strategies at this level. In the ivory-tower setting of this paper I can make the obvious point that everyone benefits when a goal like "Show those turkeys downtown how stupid they are" is brought into the open, or when a reviewer-to-be makes explicit a line of attack that looks promising. In a real-life situation, however, it is in the nature of assumptions that they do not even get noticed, much less articulated. And articulated in the context of the specific situation: if an assumption is not so articulated, you can never be sure it is common property, given the idiosyncratic way each of us chunks the information at our disposal. The post-facto "any-fool-should-have-known" argument is always an unsatisfactory substitute.

A sure way not to illumine a strategy *To Do* is to develop nothing but an outline, since outlines are necessarily concerned mainly with plans *To Say*. Concept papers will shed more light, but in my experience they rarely are fully satisfactory. This is at least partly because strategies *To Do* typically get articulated bit by bit (once again we meet the proposition that learning and insight are achieved heuristically and incrementally). Thus the actual process of finding out what has happened at the beginning of the conceptual process takes time. It involves a series of exchanges, not just at the formal inception of a project but even before it takes shape and also as it progresses.

Not all analysts find such exchanges congenial, managers at all levels begrudge the time, and divergences among various strategies *To Do* are not always resolved amicably. And indeed not all projects are worth spending too much time on. But to the degree that all concerned—higher level reviewers as well as those actually involved in the writing—can work early and often at narrowing the gaps among various conceptions of the rhetorical problem, the chances of a bumpy review process will diminish. Perhaps more important, the chances of preserving whatever creativity there is will be enhanced. And finally, hammering out differences at the level of strategies *To Do* might make a virtue of necessity: it might give a more collegial cast to a process whose hierarchical aspects are built-in and inescapable.[b]

a. Many analysts may cavil at the last statement, arguing that the review process has left them no longer in charge of their own prose. Perhaps analysts do have less control than in earlier eras, but I would argue that because they are the ones constructing the prose, for better or for worse they remain by far the most influential factors in what gets produced.

b. Looking at the problem in this way exposes an anomaly in a related area. As we have seen, the value of experience—experience extending over a decade or more—is well documented in the cognitive-science literature. Such experience generally makes itself felt at higher levels of problem solving; a first-class composer or a chess grandmaster stands out because of his skill at a level analogous to Flower and Hayes's strategy *To Do*. In the DI the people in upper levels of management have a high concentration of experience of this sort, yet the serial nature of the review process and the other demands of their job make it hard for them to bring it to bear at the point where

(Editor's note: At the time of this monograph's original appearance there were developments on the horizon that promised profound effects on the way DI analysts did business in just these areas. Project SAFE and the concurrent development of AIM appeared with recurrent troubles that tended to buttress the negative mindsets of many in the directorate at the time. Their potential attractiveness became apparent before long. The attractiveness in this context arose not from the information-retrieval aspect of SAFE, but from the interactive capabilities of the partner development, AIM, which was designed to permit frequent written exchanges between analysts–December 2009.)

If the history of such systems is any guide, DI analysts are likely to find interaction of this sort a congenial way to work. If they perceive the initial capability to be inferior to what is available elsewhere, they are likely to press for greater speed, comprehensiveness, and flexibility.

AIM's interactive capacity will be a boon in many ways, but it will also pose new managerial challenges:

- It will encourage collegiality among analysts concerned with various aspects of the same problem—an important advantage in the expanded directorate. It will not magically eliminate parochialism and dog-in-the-manger attitudes, but to the extent it is used, it will help analysts establish communication and get around competitive barriers.

- Exchanges via AIM will be informal and basically conversational, and there is every reason to expect some of the conversational flavor to carry over into more formal products. Thus AIM seems likely to foster the sort of prose called for earlier in this essay. If it does, of course, it will also raise the sort of managerial questions discussed there.

- AIM seems well suited to the incremental articulation of strategies *To Do*. Those involved in the exchanges are likely to develop clearer notions—and a higher degree of consensus—about what their purposes are.

There never will be dependable correlation between the intensity of the interaction and the quality of the product.

- But those who do not participate will have a harder time catching up. This means, among other things, that potential reviewers may find it even more difficult to make contact with the problem-defining process unless they keep current as it progresses—unless they participate in the written as well as the spoken interplay. The potential for heavier demands on managers' time is obvious.

- At the same time, collegiality could work at cross purposes with hierarchy. What would it do for a division or branch chief's authority, for example, if the office director used AIM to get deeply involved in helping an analyst define a rhetorical problem?

- Nor will the system be uniformly beneficial on the substantive side. Writing still will be essentially a private process, and some analysts will not function at their best if they have to work in a sort of electronic marketplace of ideas. Others may find the exchanges so much fun that they forgo analytic digging. There never will be dependable correlation between the intensity of the interaction and the quality of the product.

strategies *To Do* are evolving.

VI. What Next?

Out of this discussion grow numerous questions about the way the directorate goes about its business. They include the following subject areas.

1. Recruitment.

Is there any way in pre-employment interviews to focus more sharply on the way a prospective employee deals with strategies *To Do* (and perhaps *To Compose*)? More pointedly, in hiring decisions should more weight be given to these attributes and less to skills of the *To-Say* variety? Should we look harder for writers and reporters and less hard for scholars? Should we count more on internal training and put less reliance on what an individual has learned before coming aboard? Should there be sharper distinctions in approach between disciplines—would it be reasonable, just for example, to require advanced degrees for economists but to emphasize BAs among political analysts? There never will be absolute answers to questions like these, but the ideas laid out in this essay make affirmative answers plausible in many cases. It also would be worthwhile seeing if there are any tests that get at skills of the *To-Do* variety.

2. Training.

If it is correct that around 10 years are needed to acquire the conceptual network necessary for first-class work, what are the implications for the way the directorate goes about its training effort? Presumably an analyst is well into the notional 10 years on his or her arrival, but it still might be prudent at that point to anticipate another 5 years of development. If so, it seems to me, more careful attention needs to be given to how the analyst learns the trade, and training should figure far more heavily in the DI's thinking than it does now. I would suggest that if what is involved is, in fact, craftwork, nearly all the training should be on the job. It even might make sense to make training one of the specific functions discussed on a branch chief's performance appraisal report (PAR). The question would then shift to how branch chiefs should be trained. (An exercise of this sort might also produce a broader examination of the branch chief's functions—an examination I think the directorate would find illuminating.)

3. Analytic Writing.

The suggestions in this essay about conversational prose mesh with some of the trends already underway in the DI. If the best route to that sort of writing is to build a vivid image of one's audience, then frequent contact with the audience is likely to prove a useful tool for sharpening the writer's effectiveness. Moreover, the notion of bringing the audience into focus should help writer and reviewers establish common ground to work out the nonsubstantive aspects of a paper.[a] Beyond that, I would suggest that the vocabulary of cognitive science (and the concepts behind it) will be useful to those involved in teaching analytic writing, both on the job and elsewhere.

4. Organization.

I have suggested that there is an unavoidable conflict between the way an organization operates and the way the individuals in the organization do their cognitive work. Estimating the costs imposed on the organization by this conflict is impossible, since to do so one would have to guess what might have been produced but wasn't. It seems safe to say, however, that although the costs probably are lower than analysts believe, they probably are higher than many managers would admit. If so, some effort to ameliorate the conflict might prove worthwhile. Four lines of approach come to mind.

a. To an analyst, of course, the audience includes the chain of review; this may actually be the most important audience of all from his or her perspective. In addition, it should be obvious that an analyst will get a different sort of audience-image from working-level colleagues than from exposure to their bosses, and that secondhand information about the interests of the latter will have a tough time competing with the first-person experience. This is one of many conceptual gaps it will take repeated effort to bridge.

- *First, divorcing substance from hierarchy as often as possible.* This means exchanges between managers and analysts at times when a paper is neither under review nor in prospect—at conferences, for example, or simply as part of everyday chitchat. The greater the hierarchical gap, the harder such exchanges are to arrange, but the more valuable they might prove to be. To the extent that nonhierarchical channels for feedback can be developed, I believe the chances of operating at cross purposes when something is on the line will be reduced.

- *Second, hierarchy-jumping in contacts with consumers.* The desk analyst, in my opinion, would benefit enormously from learning firsthand what is on the minds of high-ranking officials.

- *Third, enfolding AIM's interactive function into the culture of the directorate.* Interactive systems are basically democratic, and I believe that properly used, they can reduce the height of organizational barriers.

- *Fourth, giving more articulation to assumptions at the level of strategies* To Do. One way this might be done is to modify the format of concept papers. Putting such papers in the first person, and replacing impersonal constructions ("This paper will examine…") with straightforward questions ("What will happen if…?") would help to make the rhetorical scheme more visible. AIM and extrahierarchical exchanges will have a similar effect.

- If a videotape were to be produced in which an analyst discussed the findings of a freshly produced paper, those findings would almost certainly make it across the gap between knowledge and news. Many in the DI's potential audience would probably find an extemporaneous discussion much more vivid than words on paper. The list of objections to the idea, of course, is formidable—the loss of precision as the analyst speaks extemporaneously, the time involved in producing even an informal discussion, the problem of defining the audience, the dilution of the sense that the paper is a product of the directorate as an institutional entity. But the benefits, if the tape was done right, might be equally impressive.

- Television might offer a better way of laying out alternative hypotheses. I have trouble believing that the present method, in which heated disagreements are set forth in determinedly flat prose, captures enough of the flavor to be much help. Taping a live discussion among experts might do a better job.

- In fast-breaking situations of prime importance, it might be useful to supplement other forms of current intelligence with televised analytic commentary. These days, current intelligence at its best almost exactly fulfills Walker Percy's criteria for news: it produces information bearing on the reader's predicament and it is carried by a newsbearer. Videotape would let a knowledgeable analyst be called into service as a specialized newsbearer on matters of great moment.

5. Presentational Methods.

Conversational prose is one way to bridge the gap between speech and writing, but are there others? Can more extensive use be made, for example, of television, whose effectiveness as an intelligence medium has already been proven in a limited way? I am thinking of something less formal, more ephemeral, and more personalized than what has been produced so far. Three possibilities spring to mind.

6. Further Exploration.

The DI might benefit from using cognitive-science techniques to analyze the production process. After reading an earlier draft of this essay, for example, Professor J.R. Hayes of Carnegie-Mellon University suggested a "cognitive task analysis of what analysts do. This information could aid the design of systems such as SAFE [and AIM]." Hayes has also suggested that we could do our own oral protocols of an analyst—or a reviewer—at work; he adds that

observing the reviewer might give particularly illuminating insights into the process.

Moreover, the notions in this essay exploit only a part of the expertise in cognitive science. For example, there is considerable disagreement in the field over the role of language in the cognitive process. Many would argue against the emphasis I have placed on the written word. They would say that such concentration significantly limits the directorate's analytic flexibility. Others might assert that I have understated the degree to which computers can supplement our mental processes. Exploration of either field (they are not mutually exclusive) might bring further benefits to the DI's analytic effort. At this point, however, we leave the area in which I can even pretend to competence.

Afterword

This list of suggestions points up once again the difficulty of the cognitive activities in which the DI is engaged. The difficulties arise because, as this essay has tried to show, the directorate must mediate a series of irreconcilable demands:

- Between the individual, private nature of the analytic effort and the social and hierarchical constraints imposed by bureaucratic imperatives.
- Between the cognitive patterns that are necessary to develop complex ideas (patterns that can only operate through writing) and the patterns our speech- and news-oriented customers are comfortable with.
- Between the early point at which critical analytic decisions are made and the serial nature of the review process.
- Between the need to search for new insights—to explore the murkier reaches of a problem space—and the need to avoid mistakes.

These conflicts have always been present, and we probably have always been aware of them, more or less. But as the DI grows and works out the implications of the trend toward centralization, as it spreads its analytic net more broadly and uses a finer mesh, they are likely to become more acute.

It would be easy to find a catalogue of conflicts like this depressing—to feel a bit like the centipede after its mind was set churning by the frog. But unlike centipedes (even sentient ones), humans can also treat such conflicts as a challenge. Indeed it seems to be part of our nature to see a situation as a problem to be solved. Morton Hunt notes:

> *We* perceive *situations as problems, and therefore undertake to solve them. An ape, coming to a broad river, would see it merely as an end to further travel in that direction; a human being might see it as a body of water to be crossed, and thereupon invent a raft. Innate neural impulses and early learning provide each species of animal with the specific procedures it needs to obtain food, avoid enemies, mate, care for its young, and so on; human beings, too, acquire procedures for dealing with these basic problems, but they also solve countless others that did not exist until their own minds saw them as problems. Art and arithmetic, music and money, detergents and democracy are all solutions to problems created not by Nature but by the human mind.*
>
> *Problem solving is virtually species-specific, but what is absolutely species-specific and ultimately human is* problem generating. *The problem is in the eye of the beholder, and we are beholders.*[a]

We are, in fact, better at generating problems than at solving them. Rarely can we say unequivocally that we have solved a problem, particularly if it is a hard one. Rather we keep plugging away

a. Hunt, *The Universe Within*, 240.

at it heuristically. Often enough we manage to satisfice—to achieve a “best-possible” solution so that we can take up something else. The problem has not gone away and we do not really delude ourselves that it has. But being realists (i.e., heuristic individuals to the core), we accept the results and live with them—recognizing that sometime we may find ourselves returning to the problem once more. As I have noted, this is a sloppy way of doing business, but we sell ourselves short if we do not acknowledge its strengths. It deals as well as anything yet developed with the fact, to use Jerome Bruner’s words, that our “ability to deal with knowledge is hugely exceeded by the potential knowledge contained in man’s environment.”

The gross imbalance between what humans can know and what is available to be known is nowhere more apparent than in the Directorate of Intelligence. Indeed this is the central dilemma the DI faces. We have always coped with the dilemma in a typically heuristic, satisficing way, and there is no reason to suppose this approach will change. My own impression, however, is that the directorate has never articulated the nature of the dilemma very clearly—a fine example of how hard it is to talk about the “conceptual front end.” A clearer notion of what the pressures are, and of what there is in our own makeup that makes them so powerful, should enable us to make better use of the power inherent in the heuristic approach. We never will get away from the need to satisfice—in other words, we always will be able to look at a given solution to a problem and see ways to make it better—but with greater understanding of what we are about, we may be able to attain a level of satisficing that we are more content with.

A Tradecraft Primer:
Structured Analytic Techniques
for Improving Intelligence Analysis

Prepared by the US Government

March 2009

This primer highlights structured analytic techniques—some widely used in the private sector and academia, some unique to the intelligence profession. It is not a comprehensive overview of how intelligence officers conduct analysis. Rather, the primer highlights how structured analytic techniques can help one challenge judgments, identify mental mindsets, stimulate creativity, and manage uncertainty. In short, incorporating regular use of techniques such as these can enable one to structure thinking for wrestling with difficult questions.

TABLE OF CONTENTS

Introduction 1

How To Use These Techniques 5

Diagnostic Techniques 7
- Key Assumptions Check 7
- Quality of Information Check 10
- Indicators or Signposts of Change 12
- Analysis of Competing Hypotheses (ACH) 14

Contrarian Techniques 17
- Devil's Advocacy 17
- Team A/Team B 19
- High-Impact/Low-Probability Analysis 22
- "What If?" Analysis 24

Imaginative Thinking Techniques 27
- Brainstorming 27
- Outside-In Thinking 30
- Red Team Analysis 31
- Alternative Futures Analysis 34

Strategies for Using Structured Analytic Techniques 38

Selective Bibliography 40

THE "MIND-SET" CHALLENGE

Using the analytic techniques contained in this primer will assist analysts in dealing with the perennial problems of intelligence: the complexity of international developments, incomplete and ambiguous information, and the inherent limitations of the human mind. Understanding the intentions and capabilities of adversaries and other foreign actors is challenging, especially when either or both are concealed. Moreover, transnational threats today pose even greater complexity, in that they involve multiple actors—including nonstate entities—that can adapt and transform themselves faster than those who seek to monitor and contain them. Finally, globalization has increased the diversity of outcomes when complex, interactive systems such as financial flows, regional economies or the international system as a whole are in flux.[2]

The first hurdle for analysts is identifying the relevant and diagnostic information from the increasing volume of ambiguous and contradictory data that is acquired through open source and clandestine means. Analysts must also pierce the shroud of secrecy—and sometimes deception—that state and nonstate actors use to mislead. A systematic approach that considers a range of alternative explanations and outcomes offers one way to ensure that analysts do not dismiss potentially relevant hypotheses and supporting information resulting in missed opportunities to warn.

Cognitive and perceptual biases in human perception and judgment are another important reason for analysts to consider alternatives. As Richards Heuer and others have argued, all individuals assimilate and evaluate information through the medium of "mental models" (sometimes also called "frames" or "mind-sets"). These are experience-based constructs of assumptions and expectations both about the world in general and more specific domains. These constructs strongly influence what information analysts will accept—that is, data that are in accordance with analysts' unconscious mental models are more likely to be perceived and remembered than information that is at odds with them.

Mental models are critical to allowing individuals to process what otherwise would be an incomprehensible volume of information. Yet, they can cause analysts to overlook, reject, or forget important incoming or missing information that is not in accord with their assumptions and expectations. Seasoned analysts may be more susceptible to these mind-set problems as a result of their expertise and past success in using time-tested mental models. The key risks of mind-sets are that: analysts perceive what they expect to perceive; once formed, they are resistant to change; new information is assimilated, sometimes erroneously, into existing mental models; and conflicting information is often dismissed or ignored.

> *"Intelligence analysts should be self-conscious about their reasoning processes. They should think about how they make judgments and reach conclusions, not just about the judgments and conclusions themselves."*
>
> —Richards Heuer, *The Psychology of Intelligence Analysis*[1]

[1] Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis* (Washington: Center for the Study of Intelligence, 1999).

[2] These observations were drawn from a lengthier treatment of cognitive bias found in the Sherman Kent Center's Occasional Paper, *Making Sense of Transnational Threats*, Vol. 3, No. 1, October 2004.

Common Perceptual and Cognitive Biases

Perceptual Biases

Expectations. We tend to perceive what we expect to perceive. More (unambiguous) information is needed to recognize an unexpected phenomenon.

Resistance. Perceptions resist change even in the face of new evidence.

Ambiguities. Initial exposure to ambiguous or blurred stimuli interferes with accurate perception, even after more and better information becomes available.

Biases in Evaluating Evidence

Consistency. Conclusions drawn from a small body of consistent data engender more confidence than ones drawn from a larger body of less consistent data.

Missing Information. It is difficult to judge well the potential impact of missing evidence, even if the information gap is known.

Discredited Evidence. Even though evidence supporting a perception may be proved wrong, the perception may not quickly change.

Biases in Estimating Probabilities

Availability. Probability estimates are influenced by how easily one can imagine an event or recall similar instances.

Anchoring. Probability estimates are adjusted only incrementally in response to new information or further analysis.

Overconfidence. In translating feelings of certainty into a probability estimate, people are often overconfident, especially if they have considerable expertise.

Biases in Perceiving Causality

Rationality. Events are seen as part of an orderly, causal pattern. Randomness, accident and error tend to be rejected as explanations for observed events. For example, the extent to which other people or countries pursue a coherent, rational, goal-maximizing policy is overestimated.

Attribution. Behavior of others is attributed to some fixed nature of the person or country, while our own behavior is attributed to the situation in which we find ourselves.

Intelligence analysts must actively review the accuracy of their mind-sets by applying structured analytic techniques that will make those mental models more explicit and expose their key assumptions. The techniques found in this primer are designed to assist in this regard by:

- Instilling more structure into the intelligence analysis.
- Making analytic arguments more transparent by articulating them and challenging key assumptions.
- Stimulating more creative, "out-of-the-box" thinking and examining alternative outcomes, even those with low probability, to see if available data might support these outcomes.
- Identifying indicators of change (or signposts) that can reduce the chances of surprise.

Incorporating findings derived from these techniques into our intelligence products also serves the policymaker by:

- Highlighting potential changes that would alter key assessments or predictions.
- Identifying key assumptions, uncertainties, intelligence gaps and disagreements that might illuminate risks and costs associated with policy choices.
- Exploring alternative outcomes for which policy actions might be necessary.

Strategic Assumptions That Were Not Challenged

1941 World War II

Japan would avoid all-out war because it recognized US military superiority.

Given that US superiority would only increase, Japan might view a first strike as the only way to knock America out of the war.

1950s Korean War

China would not cross the Yalu River in support of the North Korean government.

Red China could make good on its threats to counter "US aggression" against the North.

1962 Cuban Missile Crisis

The Soviet Union would not introduce offensive nuclear weapons into Cuba.

The Kremlin could miscalculate and believe it could create a fait accompli that a young US President would not be prepared to reverse.

1973 Yom Kippur War

Arabs knew they could not win because they had failed to cooperate in the past and still lacked sufficient air defenses to counter Israeli airpower.

A surprise Arab attack, even if repelled, could wound Israel psychologically and prompt international calls for cease-fires and diplomatic negotiations.

1989 German Unification

East Germany could not unify with the West Germany against the wishes of the Soviet Union.

The Soviet Union—under Gorbachev—might not be prepared to intervene militarily in Eastern Europe as it had in the past.

1998 Indian Nuclear Test

Conducting a nuclear test risked international condemnation and US sanctions and would threaten a newly elected coalition government.

A successful and surprise nuclear test could boost Indian nationalist pride and solidify public support for a shaky coalition government.

2003 Iraq's WMD Programs

Saddam failed to cooperate with UN inspectors because he was continuing to develop weapons of mass destruction.

If Iraqi authorities had destroyed their WMD stocks and abandoned their programs, they might refuse to fully acknowledge this to the UN to maintain Iraq's regional status, deterrence, and internal regime stability.

HOW TO USE THESE TECHNIQUES

The analytic techniques in this primer are designed to help individual analysts, as well as teams, explore and challenge their analytical arguments and mind-sets. Some techniques are fairly simple to understand and employ—such as Brainstorming and Devil's Advocacy. Others are more complex and demand a greater degree of analytical sophistication, resource commitment, and time. All the techniques are included because they have helped other analysts avoid rigid ways of thinking or assisted them in exploring new outcomes or implications of an intelligence problem.

The techniques are grouped by their purpose: **diagnostic** techniques are primarily aimed at making analytic arguments, assumptions, or intelligence gaps more transparent; **contrarian** techniques explicitly challenge current thinking; and **imaginative thinking** techniques aim at developing new insights, different perspectives and/or develop alternative outcomes. In fact, many of the techniques will do some combination of these functions. However, analysts will want to select the tool that best accomplishes the specific task they set out for themselves. Although application of these techniques alone is no guarantee of analytic precision or accuracy of judgments, it does improve the sophistication and credibility of intelligence assessments as well as their usefulness to policymakers. As Richards Heuer notes in his own work on cognitive bias, "analysis can be improved."[3]

[3] Heuer, *Psychology of Intelligence Analysis*, p. 184.

KEY ASSUMPTIONS CHECK

List and review the key working assumptions on which fundamental judgments rest.

WHEN TO USE

A Key Assumptions Check is most useful at the beginning of an analytic project. An individual analyst or a team can spend an hour or two articulating and reviewing the key assumptions. Rechecking assumptions also can be valuable at any time prior to finalizing judgments, to insure that the assessment does not rest on flawed premises. Identifying hidden assumptions can be one of the most difficult challenges an analyst faces, as they are ideas held—often unconsciously—to be true and, therefore, are seldom examined and almost never challenged.

A key assumption is any hypothesis that analysts have accepted to be true and which forms the basis of the assessment. For example, military analysis may focus exclusively on analyzing key technical and military variables (sometimes called factors) of a military force and "assume" that these forces will be operated in a particular environment (desert, open plains, arctic conditions, etc.). Postulating other conditions or assumptions, however, could dramatically impact the assessment. Historically, US analysis of Soviet-Warsaw Pact operations against NATO had to "assume" a level of non-Soviet Warsaw Pact reliability (e.g., would these forces actually fight?). In this case, there was high uncertainty and depending on what level of reliability one assumed, the analyst could arrive at very different conclusions about a potential Soviet offensive operation. Or when economists assess the prospects for foreign economic reforms, they may consciously, or not, assume a degree of political stability in those countries or the region that may or may not exist in the future. Likewise, political analysts reviewing a developing country's domestic stability might unconsciously assume stable oil prices, when this key determinant of economic performance and underlying social peace might fluctuate. All of these examples highlight the fact that analysts often rely on stated and unstated assumptions to conduct their analysis. The goal is not to undermine or abandon key assumptions; rather, it is to make them explicit and identify what information or developments would demand rethinking them.

VALUE ADDED

Explicitly identifying working assumptions during an analytic project helps:

- Explain the logic of the analytic argument and expose faulty logic.
- Understand the key factors that shape an issue.
- Stimulate thinking about an issue.
- Uncover hidden relationships and links between key factors.
- Identify developments that would cause you to abandon an assumption.
- Prepare analysts for changed circumstances that could surprise them.

Key Assumptions Check: The 2002 DC Sniper Case

The outbreak of sniper shootings in the Washington, DC area in the fall of 2002 provides a good example of how this technique could have been applied. After the initial flurry of shootings, the operating assumption that quickly emerged was that the shootings were the work of a single, white male who had some military training and was driving a white van. If law enforcement officials had conducted a Key Assumptions Check, they could have broken this statement into its key components and assessed the validity of each statement as follows:

Key Assumption	Assessment
The sniper is a male.	Highly likely (but not certain) given past precedent with serial killers. We are taking little risk by not looking for a female.
The sniper is acting alone.	Highly likely (but not certain) given past precedents.
The sniper is white.	Likely, but not as certain, given past precedents. We would be taking some risk if we rule out nonwhites as suspects.
The sniper has military training/experience.	Possible, but not sufficient reason to exclude from consideration potential suspects who have not had any military training.
The sniper is driving a white van.	Possible because you have a credible eyewitness account but worthy of continuing scrutiny given the number of white vans in the area (more than 70,000 registered in the Maryland suburbs of Metropolitan Washington, DC) and that different kinds of vehicles are being described.

A Key Assumptions Check could have allowed law enforcement officials to:

- Avoid jumping to conclusions (the sniper is white, has military training, and is driving a white van) that did not hold up under closer scrutiny. By explicitly examining each assumption, officials could have avoided prematurely narrowing down the potential pool of suspects to a group that did not include the actual perpetrator. Similarly, they might have been more cautious about accepting that the sniper was driving a white van.
- Be receptive to new leads and citizen tips, such as eyewitness reports that the sniper fled the scene driving a specific model Chevrolet.
- More seriously consider evidence that subsequently became available, which contradicted a key assumption. If officials had stated explicitly that they were assuming the sniper was acting alone, they might have been sensitive to new information that contradicted that key assumption. Often this type of information gets “lost in the noise” if the analyst has not already thought about what key assumptions he or she is making.

THE METHOD

Checking for key assumptions requires analysts to consider how their analysis depends on the validity of certain premises, which they do not routinely question or believe to be in doubt. A four-step process will help analysts:

1. Review what the current analytic line on this issue appears to be; write it down for all to see.

2. Articulate all the premises, both stated and unstated in finished intelligence, which are accepted as true for this analytic line to be valid.

3. Challenge each assumption, asking why it "must" be true and whether it remains valid under all conditions.

4. Refine the list of key assumptions to contain only those that "must be true" to sustain your analytic line; consider under what conditions or in the face of what information these assumptions might not hold.

QUESTIONS TO ASK DURING THIS PROCESS INCLUDE:

- How much confidence exists that this assumption is correct?
- What explains the degree of confidence in the assumption?
- What circumstances or information might undermine this assumption?
- Is a key assumption more likely a key uncertainty or key factor?
- Could the assumption have been true in the past but less so now?
- If the assumption proves to be wrong, would it significantly alter the analytic line? How?
- Has this process identified new factors that need further analysis?

QUALITY OF INFORMATION CHECK

Evaluates completeness and soundness of available information sources.

WHEN TO USE

Weighing the validity of sources is a key feature of any critical thinking. Moreover, establishing how much confidence one puts in analytic judgments should ultimately rest on how accurate and reliable the information base is. Hence, checking the quality of information used in intelligence analysis is an ongoing, continuous process. Having multiple sources on an issue is not a substitute for having good information that has been thoroughly examined. Analysts should perform periodic checks of the information base for their analytic judgments. Otherwise, important analytic judgments can become anchored to weak information, and any "caveats" attached to those judgments in the past can be forgotten or ignored over time.

If a major analytic assessment is planned, analysts should individually or collectively review the quality of their information and refresh their understanding of the strengths and weaknesses of past reporting on which an analytic line rests. Without understanding the context and conditions under which critical information has been provided, it will be difficult for analysts to assess the information's validity and establish a confidence level in an intelligence assessment.

VALUE ADDED

A thorough review of information sources provides analysts—as well as policymakers—with an accurate assessment of "what we know" and "what we do not know." It is also an opportunity to confirm that sources have been cited accurately. In the case of HUMINT, this will require extensive review of the sources' background information and access as well as his or her motivation for providing the information. Similarly, reviewing technical sourcing can sometimes reveal inadvertent errors in processing, translation, or interpretation that otherwise might have gone unnoticed.

In addition, a quality of information check can be valuable to both collectors and policymakers:

- It can help to detect possible deception and denial strategies by an adversary.
- It can identify key intelligence gaps and new requirements for collectors.
- It can assist policymakers in understanding how much confidence analysts are placing on analytic judgments.

THE METHOD

An analyst or a team might begin a quality of information check by developing a database in which information is stored according to source type and date, with additional notations indicating strengths or weaknesses in those sources.[4] Ideally, analysts would have a retrieval and search capability on the database, so that periodic reviews are less labor intensive and result in a more complete review of all sources used in past analysis. For the information review to be fully effective, analysts will need as much background information on sources as is feasible. Knowing the circumstances in which reporting was obtained is often critical to understanding its validity. With the data in hand, analysts can then:

- Review systematically all sources for accuracy.
- Identify information sources that appear most critical or compelling.
- Check for sufficient and strong corroboration of critical reporting.
- Reexamine previously dismissed information in light of new facts or circumstances that cast it in a different light.
- Ensure that any recalled reporting is identified and properly flagged for other analysts; analysis based on recalled reporting should also be reviewed to determine if the reporting was essential to the judgments made.
- Consider whether ambiguous information has been interpreted and caveated properly.
- Indicate a level of confidence that analysts can place in sources, which are likely to figure in future analytic assessments.

[4] Analysis of Competing Hypotheses (ACH), discussed later in the primer, is a useful technique for exploring the possibility that deception could explain the absence of evidence.

Quality of Information Problem on Iraq

". . . Analysts community wide are unable to make fully informed judgments on the information they received, relying instead on nonspecific source lines to reach their assessments. Moreover, relevant operational data is nearly always withheld from analysts, putting them at a further analytical disadvantage . . ."

—*Senate Select Committee on Intelligence, Report on the US Intelligence Community's Prewar Intelligence Assessments on Iraq*

"Analytic errors included over-reliance on a single, ambiguous source, [and, in addition to collection shortfalls] failure of analysts to understand fully the limitations of technical collection . . ."

"The Intelligence Community relied too heavily on ambiguous imagery indicators . . ."

—*Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.*

INDICATORS OR SIGNPOSTS OF CHANGE

Periodically review a list of observable events or trends to track events, monitor targets, spot emerging trends, and warn of unanticipated change.

WHEN TO USE

An analyst or team can create an indicators or signposts list of observable events that one would expect to see if a postulated situation is developing; e.g., economic reform, military modernization, political instability, or democratization. Constructing the list might require only a few hours or as much as several days to identify the critical variables associated with the targeted issue. The technique can be used whenever an analyst needs to track an event over time to monitor and evaluate changes. However, it can also be a very powerful aid in supporting other structured methods explained later in this primer. In those instances, analysts would be watching for mounting evidence to support a particular hypothesis, low-probability event, or scenario.

When there are sharply divided views on an issue, an indicators or signposts list can also "depersonalize" the argument by shifting analytic attention to a more objective set of criteria. Using an indicators list can clarify substantive disagreements, once all sides agree on the set of objective criteria used to measure the topic under study.

VALUE ADDED

By providing an objective baseline for tracking events or targets, indicators instill rigor into the analytic process and enhance the credibility of analytic judgments. An indicators list included in a finished product also allows the policymaker to track developments and builds a more concrete case for the analytic judgments. By laying out a list of critical variables, analysts also will be generating hypotheses regarding why they expect to see the presence of such factors. In so doing, analysts make the analytic line much more transparent and available for scrutiny by others.

THE METHOD

Whether used alone, or in combination with other structured analysis, the process is the same:

- Identify a set of competing hypotheses or scenarios.
- Create separate lists of potential activities, statements, or events expected for each hypothesis or scenario.
- Regularly review and update the indicators lists to see which are changing.
- Identify the most likely or most correct hypotheses or scenarios, based on the number of changed indicators that are observed.

Developing two lists of indicators for each hypothesis or scenario may prove useful to distinguish between indicators that a development is or is not emerging. This is particularly useful in a "What If?" Analysis, when it is important to make a case that a certain event is unlikely to happen.

Tracking the Potential for Political Instability in a Foreign Country

Topics	Indicators	1999				2000		
		I	*II*	*III*	*IV*	*I*	*II*	*III*
Government Capacity	Quality of leadership/organizational capabilities	●	●	●	■	●	●	●
	Responsiveness to popular demands	●	●	●	●	●	●	●
	Ability to deliver basic goods and services							
	Internal Security Capabilities							
	Effectiveness of civil/criminal justice systems							
Legitimacy of Regime	Breadth and depth of political participation	●	●	●	●	●	●	●
	Perceived level of corruption	●	●	●	●	●	●	●
	Human rights violations	●	●	●	●	●	●	●
	Weakness of civil society							
	Pervasiveness of transnational criminal organizations							
	External support for government							
Opposition Activity	Ethnic/religious discontent	●	●	●	●	●	●	●
	Military discontent with civilian government	●	●	●	●	●	●	●
	Popular demonstrations/strikes/riots							
	Insurgent/separatist/terrorist group activity							
	External support for opposition							
	Threat of conflict with or in neighboring state							
Economic Factors	Weakness of domestic economy/unemployment/ inflation							
	Degree of income disparity							
	Capital flight							
	Decreased access to foreign funds							
	Reduced trade openness							
Environmental Issues	Extent of environmental degradation							
	Food/energy shortages							
	Ability to respond to natural disasters							

Presence of Trigger Mechanisms (▶ if present)							
Contested elections				▶			
Unpopular changes in food/energy prices			▶				
Sudden imposition of unpopular policies							
Coup plotting				▶			
Government mismanagement of natural disaster or national emergency							
Death of key figure							

■ Serious concern
● Substantial concern
● Moderate concern
● Low concern
● Negligible concern

Tracking the Potential for Political Instability in an Indicators Matrix. Analysts tracked the potential for regime change in 2000 and identified a list of indicators, to which they posed the question, "is this occurring or not? Analysts also went further and developed a list of "trigger mechanisms" that might bring about a political shift.

ANALYSIS OF COMPETING HYPOTHESES (ACH)

Identification of alternative explanations (hypotheses) and evaluation of all evidence that will disconfirm rather than confirm hypotheses.

WHEN TO USE

Analysis of Competing Hypotheses (ACH) has proved to be a highly effective technique when there is a large amount of data to absorb and evaluate. While a single analyst can use ACH, it is most effective with a small team that can challenge each other's evaluation of the evidence. Developing a matrix of hypotheses and loading already collected information into the matrix can be accomplished in a day or less. If the data must be reassembled, the initial phases of the ACH process may require additional time. Sometimes a facilitator or someone familiar with the technique can lead new analysts through this process for the first time.

ACH is particularly appropriate for controversial issues when analysts want to develop a clear record that shows what theories they have considered and how they arrived at their judgments. Developing the ACH matrix allows other analysts (or even policymakers) to review their analysis and identify areas of agreement and disagreement. Evidence can also be examined more systematically, and analysts have found that this makes the technique ideal for considering the possibility of deception and denial.

VALUE ADDED

ACH helps analysts overcome three common mistakes that can lead to inaccurate forecasts:

- Analysts often are susceptible to being unduly influenced by a first impression, based on incomplete data, an existing analytic line, or a single explanation that seems to fit well enough.
- Analysts seldom generate a full set of explanations or hypotheses at the outset of a project.
- Analysts often rely on evidence to support their preferred hypothesis, but which also is consistent with other explanations.

In essence, ACH helps analysts to avoid picking the first solution that seems satisfactory instead of going through all the possibilities to arrive at the very best solution.

THE METHOD

ACH demands that analysts explicitly identify all the reasonable alternative hypotheses, then array the evidence against each hypothesis—rather than evaluating the plausibility of each hypothesis one at a time. To create a level playing field, the process must:

- Ensure that all the information and argumentation is evaluated and given equal treatment or weight when considering each hypothesis.
- Prevent the analyst from premature closure on a particular explanation or hypothesis.
- Protect the analyst against innate tendencies to ignore or discount information that does not fit comfortably with the preferred explanation at the time.

To accomplish this, the process should follow these steps:

- Brainstorm among analysts with different perspectives to identify all possible hypotheses.
- List all significant evidence and arguments relevant to all the hypotheses.

- Prepare a matrix with hypotheses across the top and each piece of evidence on the side. Determine whether each piece of evidence is consistent, inconsistent, or not applicable to each hypothesis.[5]
- Refine the matrix and reconsider the hypotheses—in some cases, analysts will need to add new hypotheses and re-examine the information available.
- Focus on disproving hypotheses rather than proving one. Talley the pieces of evidence that are inconsistent and consistent with each hypothesis to see which explanations are the weakest and strongest.

[5] The "diagnostic value" of the evidence will emerge as analysts determine whether a piece of evidence is found to be consistent with only one hypothesis, or could support more than one or indeed all hypotheses. In the latter case, the evidence can be judged as unimportant to determining which hypothesis is more likely correct.

- Analyze how sensitive the ACH results are to a few critical items of evidence; should those pieces prove to be wrong, misleading, or subject to deception, how would it impact an explanation's validity?
- Ask what evidence is not being seen but would be expected for a given hypothesis to be true. Is denial and deception a possibility?
- Report all the conclusions, including the weaker hypotheses that should still be monitored as new information becomes available.
- Establish the relative likelihood for the hypotheses and report all the conclusions, including the weaker hypotheses that should still be monitored as new information becomes available.
- Identify and monitor indicators that would be both consistent and inconsistent with the full set of hypotheses. In the latter case, explore what could account for inconsistent data.

Terrorism in Tokyo From Aum Shinrikyo

		Weight	H: 1	H: 4	H: 2	H: 3
			Kooky Cult	Terrorist Group	Political Movement	Criminal Group
	Inconsistency Score ⇨		-1.0	-1.0	-2.0	-3.0
E3	Attacks on Journalists	MEDIUM	I	N	I	I
E2	Religious Affiliation	MEDIUM	C	I	I	I
E4	Established Party	MEDIUM	N	N	C	I
E1	Blind Leader Mastsumoto	MEDIUM	C	C	C	C

ACH Matrix of Terrorism in Tokyo. In March 1995, a largely unknown group attacked the Tokyo subways by using a highly lethal nerve agent known as sarin. ACH provides a mechanism to carefully examine all the evidence and possible explanations for understanding what type of group could have been responsible. In simplified form, the above matrix arrays each piece of evidence on the vertical axis and then evaluates each in terms of the item's consistency with four possible explanations for the terrorist attack in Tokyo (horizontal axis). Analysts rate a piece of evidence as consistent (C); inconsistent (I); or neutral (N). This process allows analysts to see that some evidence will be consistent with more than one hypothesis and be less valuable in disproving hypotheses.

DEVIL'S ADVOCACY

Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.

WHEN TO USE

Devil's Advocacy is most effective when used to challenge an analytic consensus or a key assumption regarding a critically important intelligence question. On those issues that one cannot afford to get wrong, Devil's Advocacy can provide further confidence that the current analytic line will hold up to close scrutiny. An individual analyst can often assume the role of the Devil's Advocate if he or she has some doubts about a widely held view, or a manager might designate a courageous analyst to challenge the prevailing wisdom in order to reaffirm the group's confidence in those judgments. In some cases, the analyst or a team can review a key assumption of a critical judgment in the course of their work, or more likely, a separate analytic product can be generated that arrays all the arguments and data that support a contrary hypothesis. While this can involve some analytic time and effort, when a group of analysts have worked on an issue for a long period of time, it is probably wise to assume that a strong mind-set exists that deserves the closer scrutiny provided by Devil's Advocacy.

VALUE ADDED

Analysts have an obligation to policymakers to understand where their own analytic judgments might be weak and open to future challenge. Hence, the Devil's Advocacy process can highlight weaknesses in a current analytic judgment or alternatively help to reaffirm one's confidence in the prevailing judgments by:

- Explicitly challenging key assumptions to see if they will not hold up under some circumstances.
- Identifying any faulty logic or information that would undermine the key analytic judgments.
- Presenting alternative hypotheses that would explain the current body of information available to analysts.

Its primary value is to serve as a check on a dominant mind-set that can develop over time among even the best analysts who have followed an issue and formed strong consensus that there is only one way of looking at their issue. This mind-set phenomenon makes it more likely that contradictory evidence is dismissed or not given proper weight or consideration. An exercise aimed at highlighting such evidence and proposing another way of thinking about an issue can expose hidden assumptions and compel analysts to review their information with greater skepticism about their findings. The analyst could come away from the exercise more certain that: 1) the current analytic line was sound; 2) the argument is still the strongest, but that there are areas where further analysis is needed; or 3) some serious flaws in logic or supporting evidence suggest that the analytic line needs to be changed or at least caveated more heavily.

THE METHOD

To challenge the prevailing analytic line, the Devil's Advocate must:

- Outline the mainline judgment and key assumptions and characterize the evidence supporting that current analytic view.
- Select one or more assumptions—stated or not—that appear the most susceptible to challenge.
- Review the information used to determine whether any is of questionable validity, whether deception is possibly indicated, or whether major gaps exist.

- Highlight the evidence that could support an alternative hypothesis or contradicts the current thinking.

- Present to the group the findings that demonstrate there are flawed assumptions, poor quality evidence, or possible deception at work.

- Consider drafting a separate contrarian paper that lays out the arguments for a different analytic conclusion if the review uncovers major analytic flaws.

- Be sure that any products generated clearly lay out the conventional wisdom and are identified as an explicitly "Devil's Advocate" project; otherwise, the reader can become confused as to the current official view on the issue.

TEAM A/TEAM B

Use of separate analytic teams that contrast two (or more) strongly held views or competing hypotheses.

WHEN TO USE

A Team A/Team B approach is different from Devil's Advocacy, where the purpose is to challenge a single dominant mind-set. Instead, Team A/Team B recognizes that there may be competing and possibly equally strong mind-sets held on an issue that need to be clarified. Sometimes analysts confuse the two techniques by drafting a Team B exercise that is really a Devil's Advocacy exercise.

If there are at least two competing views within an analytic office or perhaps competing opinions within the policymaking community on a key issue, then Team A/Team B analysis can be the appropriate technique to use. Developing a full-blown Team A/Team B exercise requires a significant commitment of analytic time and resources, so it is worthwhile considering if the analytic issue merits this kind of attention.

A longstanding policy issue, a critical decision that has far-reaching implications, or a dispute within the analytic community that has obstructed effective cross-agency cooperation would be grounds for using Team A/Team B. If those circumstances exist, then analysts will need to review all of the data to develop alternative papers that can capture the essential differences between the two viewpoints.

VALUE ADDED

Managers have found that when there are office tensions among competing factions of analysts, a Team A/Team B approach can help opposing experts see the merit in the other group's perspective. The process of conducting such an exercise can reduce the friction and even narrow the differences. At a minimum, it allows those holding opposing views to feel that their views have been given equal attention.

For the policymaker, this technique helps to surface and explain important analytic differences within the expert community. Often senior officials can learn more by weighing well-argued conflicting views than from reading an assessment that masks substantive differences or drives analysis to the lowest common denominator. By making the key assumptions and information used for each argument more transparent, a policymaker can judge the merits of each case, pose questions back to the analysts, and reach an independent judgment on which argument is the strongest. Moreover, highlighting alternative views puts collectors on notice that they need to be searching for new information that can confirm or disconfirm a range of hypotheses.

If opposing positions are well established, it can be useful to place analysts on teams that will advocate positions they normally do not support; forcing analysts to argue "the other side" can often make them more aware of their own mind-set.

A Team A/Team B View: China's Military

A: *China's Hollow Military* by Bates Gill and Michael O'Hanlon	B: *China's Military: A Second Opinion* by James Lilley and Carl Ford
". . . We believe that the recent clamor over China's strategic ambitions is greatly overblown. Most of the Chinese aims that run counter to US interests are in fact not global or ideological but territorial in nature and confined primarily to the islands and waterways to China's south and southeast . . . An enormous gap separates China's military capabilities from its aspirations. The PRC's armed forces are not very good and not getting better very fast. Whatever China's concerns and intentions, its capacity to act upon them in ways inimical to US interests is severely limited, and will remain so for many years . . . The PRC's power projection capabilities, too, are constrained by huge weaknesses–especially in areas such as aerial refueling, electronic warfare, command and control and amphibious and air assault assets. China owns considerably less top-level equipment than medium powers like Japan and Britain; it owns even less than smaller powers such as Italy, South Korea or The Netherlands . . . The resources it devotes to acquiring modern weaponry are akin to those of countries spending $10-20 billion a year on defense . . ."	". . . We think they got it half right. China is no military superpower and will not acquire that status for some years to come. But measured in terms of its capacity to challenge key US allies in East Asia, China's capabilities have grown exponentially . . . By emphasizing direct comparisons between the defense capabilities of the United States and the PRC, the authors create an artificial and misleading construct . . . What the regime gives every indication of striving for is sufficient military clout to achieve its aims in Asia. In the short term, it wishes to intimidate Taiwan sufficiently to bring about unification on Beijing's terms . . . . . . Investments of the sort Beijing is making can mean only one thing: China is determined to improve the PLA's fighting capability. While most nations are reducing defense expenditures in the post–Cold War era, China is one of the few doing the opposite . . . Across the board, the PLA is engaged in a major spending effort to upgrade weapons and equipment and improve its operational capability. According to the Pentagon, these efforts have already enhanced China's ability to project military power . . ."

—Excerpted from journal articles found in The National Interest, Fall and Winter 2000/2001.

THE METHOD

Analysis Phase. A Team A/Team B exercise can be conducted on an important issue to:

- Identify the two (or more) competing hypotheses or points of view.
- Form teams or designate individuals to develop the best case that can be made for each hypothesis.
- Review all pertinent information that supports their respective positions.
- Identify missing information that would buttress their hypotheses.
- Structure each argument with an explicit presentation of key assumptions, key pieces of evidence, and careful articulation of the logic behind the argument.

Debate Phase. An oral presentation of the alternative arguments and rebuttals in parallel fashion can then be organized for the benefit of other analysts:

- Set aside time for an oral presentation of the alternative team findings; this can an informal brainstorming session or a more formal "debate."
- Have an independent "jury of peers" listen to the oral presentation and be prepared to question the teams regarding their assumptions, evidence, or logic.
- Allow each team to present their case, challenge the other team's arguments, and rebut the opponent's critique of its case.
- Let the jury consider the strength of each presentation and recommend possible next steps for further research and collection efforts.

HIGH-IMPACT/LOW-PROBABILITY ANALYSIS

Highlights a seemingly unlikely event that would have major policy consequences if it happened.

WHEN TO USE

High-Impact/Low-Probability Analysis is a contrarian technique that sensitizes analysts to the potential impact of seemingly low probability events that would have major repercussions on US interests. Using this technique is advisable when analysts and policymakers are convinced that an event is unlikely but have not given much thought to the consequences of its occurrence. In essence, this can be a warning that the intelligence and policy communities must be alert to an unexpected but not impossible event. For example, the fall of the Shah, the collapse of the Soviet Union, and the reunification of Germany were all considered low probability events at one time; however, analysts might have benefited from considering the consequences of such events and how they might plausibly have come about.

VALUE ADDED

Mapping out the course of an unlikely, yet plausible, event can uncover hidden relationships between key factors and assumptions; it also can alert analysts to oversights in the mainstream analytic line. In addition, an examination of the "unthinkable" allows analysts to develop signposts that may provide early warning of a shift in the situation. By periodically reviewing these indicators an analyst is more likely to counter any prevailing mind-set that such a development is highly unlikely.

THE METHOD

If there is a strongly held view that an event is unlikely, then postulating precisely the opposite should not be difficult.

- Define the high-impact outcome clearly. This process is what will justify examining what most analysts believe to be a very unlikely development.
- Devise one or more plausible explanations for or "pathways" to the low probability outcome. This should be as precise as possible, as it can help identify possible indicators for later monitoring.
- Insert possible triggers or changes in momentum if appropriate. These can be natural disasters, sudden health problems of key leaders, or new economic or political shocks that might have occurred historically or in other parts of the world.
- Brainstorm with analysts having a broad set of experiences to aid the development of plausible but unpredictable triggers of sudden change.
- Identify for each pathway a set of indicators or "observables" that would help you anticipate that events were beginning to play out this way.
- Identify factors that would deflect a bad outcome or encourage a positive outcome.

High Impact of a Low-Probability Event: Pearl Harbor

". . . So far as relations directly between the United States and Japan are concerned, there is less reason today than there was a week ago for the United States to be apprehensive lest Japan make "war" on this country.

Were it a matter of placing bets, the undersigned would give odds of five to one that the United States and Japan will not be at "war" on or before December 15; would wager three to one that the United States and Japan will not be at 'war' on or before the 15th of January (i.e, seven weeks from now); would wager even money that the United States and Japan will not be at "war" on or before March 1 (a date more than 90 days from now) . . ."

—State Department Special Assessment, 27 November 1941

High-Impact/Low-Probability Analysis on 9/11

The 9/11 Commission report includes examination of speculative analysis that was provided to senior policymakers highlighting what were thought to be highly unlikely scenarios that would have a very high impact. One of those items was the 6 August 2001 President's Daily Brief, which stated:

Al-Qai'da members—including some who are US citizens—have resided in or traveled to the US for years, and the group apparently maintains a support structure that could aid attacks. Two al-Qai'da members found guilty in the conspiracy to bomb our embassies in East Africa were US citizens, and a senior EIJ [Egyptian Islamic Jihad] member lived in California in the mid-1990s.

- A clandestine source said in 1998 that a Bin Ladin cell in New York was recruiting Muslim-American youth for attacks.

We have not been able to corroborate some of the more sensational threat reporting, such as that from a service in 1998 saying that Bin Ladin wanted to hijack a US aircraft to gain the release of "Blind Shaykh" 'Umar Abd al-Rahman and other US-held extremists.

—9/11 Commission Report, declassified and approved for release 10 April 2004.

"WHAT IF?" ANALYSIS

Assumes that an event has occurred with potential (negative or positive) impact and explains how it might come about.

WHEN TO USE

"What If?" analysis is another contrarian technique for challenging a strong mind-set that an event will not happen or that a confidently made forecast may not be entirely justified. It is similar to a High-Impact/Low-Probability analysis, but it does not dwell on the consequences of the event as much as it accepts the significance and moves directly to explaining how it might come about.

VALUE ADDED

By shifting the focus from whether an event could occur to how it may happen, analysts allow themselves to suspend judgment about the likelihood of the event and focus more on what developments—even unlikely ones—might enable such an outcome. An individual analyst or a team might employ this technique and repeat the exercise whenever a critical analytic judgment is made.

Using this technique is particularly important when a judgment rests on limited information or unproven assumptions. Moreover, it can free analysts from arguing about the probability of an event to considering its consequences and developing some indicators or signposts for its possible emergence. It will help analysts address the impact of an event, the factors that could cause—or alter—it, and likely signposts that an event is imminent.

A "What If?" analysis can complement a difficult judgment reached and provide the policymaker a thoughtful caution to accepting the conventional wisdom without considering the costs and risks of being wrong. This can help decision-makers consider ways to hedge their bets, even if they accept the analytic judgment that an event remains unlikely.

THE METHOD

Like other contrarian methods, "What If?" analysis must begin by stating clearly the conventional analytic line and then stepping back to consider what alternative outcomes are too important to dismiss, even if unlikely. Brainstorming over a few days or weeks can develop one or more plausible scenarios by which the unlikely event occurs:

- Assume the event has happened.
- Select some triggering events that permitted the scenario to unfold to help make the "what if" more plausible; for example, analysts might postulate the death of a leader, a natural disaster, or some economic event that would start a chain of other events.
- Develop a chain of argumentation based as much on logic as evidence to explain how this outcome could have come about.
- "Think backwards" from the event in concrete ways–that is, specifying what must actually occur at each stage of the scenario is often very useful.
- Identify one or more plausible pathways or scenarios to the unlikely event; very often more than one will appear possible.
- Generate a list of indicators or "observables" for each scenario that would help to detect the beginnings of the event.
- Consider the scope of the positive and negative consequences of each scenario and their relative impacts.
- Monitor the indicators developed on a periodic basis.

"What If?" Analysis: An Unlikely Outcome in Yugoslavia, 1990.

The possibility of muddling through is very low. In the unlikely event that it happens, this is what it would look like.

Memories of the internecine civil war during World War II and fear of another destructive conflict would lead the two most numerous South Slav people—Serbs and Croats—to reach some political accommodation. A compromise that preserves Yugoslavia would include:

- Basic principles:
  - -No change in existing Republic borders.
  - -No change in Yugoslavia's existing international status.
  - -Mutually recognized sovereignty of each republic

- Confederal institutions:
  - -A single foreign ministry, to which diplomatic representatives would be accredited.
  - -A central military organization with a joint General Staff responsible for planning.
  - -A central bank, determining macroeconomic policy, a common currency,

- Powers reserved to republics.
  - -Veto over actions of the Confederal Authority.
  - -Control of internal security, including guarantee of minority rights.
  - -Operational control over some or all military units stationed on the republic's territory.
  - -Raising taxes and allocating funds to discharge mutually agreed confederal responsibilities.

Only the Serbs can open the door to a confederal Yugoslavia, and Serbia's leader, Slobodan Milosevic, holds the key. Some observers felt there are pressures on him to try. If he does not, he would give his opponents the leverage to remove him. The potential penalties of failure to compromise would be too great, in this view, for the peoples and leaders of Yugoslavia to forgo every effort to find a compromise.

—*Excerpts from the declassified* NIE: Prospects for Yugoslavia*, October 1990.*

BRAINSTORMING

An unconstrained group process designed to generate new ideas and concepts.

WHEN TO USE

Brainstorming is a widely used technique for stimulating new thinking and it can be applied to virtually all of the other structured analysis techniques as an aid to thinking. Typically, analytic will brainstorm when they begin a project to help generate a range of hypotheses about their issue.

Brainstorming, almost by definition, involves a group of analysts meeting to discuss a common challenge; a modest investment of time at the beginning or critical points of a project can take advantage of their different perspectives to help structure a problem. This group process allows others to build on an initial idea suggested by a member of the brainstorming session.

An individual analyst also can brainstorm to produce a wider range of ideas than a group might generate, without regard for other analysts' egos, opinions, or objections. However, an individual will not have the benefit of others' perspectives to help develop the ideas as fully. Moreover, an individual may have difficulty breaking free of his or her cognitive biases without the benefit of a diverse group.

VALUE ADDED

This technique can maximize creativity in the thinking process, force analysts to step outside their normal analytic mind-sets, and suspend their typical "good judgment" about the practicality of ideas or approaches. More generally, brainstorming allows analysts to see a wider range of factors that might bear on the topic than they would otherwise consider. Analysts typically censor out ideas that seem farfetched, poorly sourced, or seemingly irrelevant to the question at hand. Brainstorming gives permission to think more radically or "outside the box." In particular, it can spark new ideas, ensure a comprehensive look at a problem or issues, raise unknowns, and prevent premature consensus around a single hypothesis.

THE METHOD

Paradoxically, brainstorming should be a very structured process to be most productive. An unconstrained, informal discussion might produce some interesting ideas, but usually a more systematic process is the most effective way to break down mind-sets and produce new insights. In particular, the process involves a divergent thinking phase to generate and collect new ideas and insights, followed by a convergent phase in which ideas are grouped and organized around key concepts. Some of the simple rules to be followed include:

- Never censor an analyst's ideas no matter how unconventional they might sound.
- Rather find out what prompted the thought, as it might contain the seeds of an important connection between the topic and an unstated assumption.
- Give yourself enough time to do brainstorming correctly. It usually takes one hour to set the "rules" of the game, get the group comfortable, and exhaust the conventional wisdom on the topic. Only then will the truly creative ideas begin to emerge.
- Involve at least one "outsider" in the process—that is, someone who does not share the same educational background, culture, technical knowledge or mind-set as the core group but has some familiarity with the topic.

A two-phase, twelve-step, structured process is often used to get the most out of the brainstorming sessions:

Brainstorming and Divergent Thinking: Perspectives of an Experienced Practitioner

". . . First, leave rank at the door and focus on "a democracy of ideas." Thoughts from experts, senior officers, and supervisors are of course, valuable and welcome, but such experts are not permitted to cut off debate by citing their seniority. In fact, it pays to invite junior officers as well as senior ones who are not involved directly in working the issue under discussion. Some of the most creative ideas at brainstorming sessions frequently come from relatively junior people who can look at a problem with fresh perspective, or from senior ones who are not experts on the issue.

Second, make sure there is no official analytic line. One of the most significant blocks to new thinking is the presence of a long held analytic line that analysts—and even more so managers—are reluctant to change. Rather than trying to fit ideas into the framework of "what we've said before," analysts need to feel free to go wherever bits of the evidence and informed supposition take them. They must feel free to throw out seemingly strange but plausible ideas that might be based on historical precedent and instinct rather than on concrete information. Facilitators can stimulate this process by deliberately posing an alternative outcome to a problem that differs starkly from the accepted analysis or by proposing a contrary way to think about an issue.

Third, don't permit killer phrases like "that would not work" or "that could not happen" to be voiced out loud. Effective brainstorming starts with ideas and possibilities, not with practicalities and self-imposed obstacles to fresh perspectives. Force the group to get as wide a range of ideas out for discussion as possible. At some point, a set of ideas might be winnowed down and subject to tests of workability, but that comes later—not during brainstorming.

Fourth, keep the brainstorming session to no more than 90 minutes. There is no hard and fast rule, but somewhere between 60 and 90 minutes, the idea stream starts to dry up, people repeat themselves, and jokes replace creative ideas.

Fifth, record ideas in a visible way. Lots of people take notes at brainstorming sessions for their own use, and that is good. We have found it valuable to have someone jot down the ideas presented on large paste-a-note sheets that we put on the walls. This allows participants in brainstorming sessions to react to ideas generated earlier. Moreover, analysts are encouraged to participate in such exercises if they see their own ideas put down in writing. Having a notional record of brainstorming also helps the analyst who ends up writing a report based on the discussion. Ideas that may not be used in one report are invariably put to use later, so it is good to have a record of them . . ."

Divergent Thinking Phase:

- Distribute “Post-It” notes and pens or markers to all participants. Typically, 10-12 people works best.
- Pose the problem in terms of a “focal question.” Display it in one sentence on a large easel or whiteboard.
- Ask the group to write down responses to the question, using key words that will fit on the small “Post-It” note.
- Stick all the notes on a wall for all to see—treat all ideas the same.
- When a pause follows the initial flow of ideas, the group is reaching the end of their conventional thinking and the new divergent ideas are then likely to emerge.
- End the “collection stage” of the brainstorming after two or three pauses.

Convergent Thinking Phase:

- Ask the participants as a group to rearrange the notes on the wall according to their commonalities or similar concepts. No talking is permitted. Some notes may be moved several times as notes begin to cluster. Copying some notes is permitted to allow ideas to be included in more than one group.
- Select a word or phrase that characterizes each grouping or cluster once all the notes have been arranged.
- Identify any notes that do not easily fit with others and consider them either useless noise or the beginning of an idea that deserves further attention.
- Assess what the group has accomplished in terms of new ideas or concepts identified or new areas that need more work or further brainstorming.
- Instruct each participant to select one or two areas that deserve the most attention. Tabulate the votes.
- Set the brainstorming group’s priorities based on the voting and decide on the next steps for analysis.

OUTSIDE-IN THINKING

Used to identify the full range of basic forces, factors, and trends that would indirectly shape an issue.

WHEN TO USE

Analysts find this technique most useful at the conceptualization of an analytic project, when the goal is to identify all the critical, external factors that could influence how a particular situation will develop. It would work well for a group of analysts responsible for a range of functional and/or regional issues. When assembling a large database that must identify a number of information categories or database fields, this technique can aid in visualizing the entire set of categories that might be needed in a research effort. Often analysts realize only too late that some additional information categories will be needed and then must go back and review all previous files and recode the data. With a modest amount of effort, "Outside-in Thinking" can reduce the risk of missing important variables early in the analytic process.

VALUE ADDED

Most analysts spend their time concentrating on familiar factors within their field or analytic issue. That is, they think from the "inside"—namely, what they control—out to the broader world. Conversely, "thinking from the outside-in" begins by considering the external changes that might, over time, profoundly affect the analysts' own field or issue. This technique encourages analysts to get away from their immediate analytic tasks (the so-called "inbox") and think about their issues in a wider conceptual and contextual framework. By recasting the problem in much broader and fundamental terms, analysts are more likely to uncover additional factors, an important dynamic, or a relevant alternative hypothesis.

THE METHOD

The process begins by developing a generic description of the problem or the phenomenon under study. Then, analysts should:

- List all the key forces (social, technological, economic, environmental, and political) that could have an impact on the topic, but over which one can exert little influence (e.g., globalization, social stress, the Internet, or the global economy).
- Focus next on key factors over which an actor or policymaker can exert some influence. In the business world this might be the market size, customers, the competition, suppliers or partners; in the government domain it might include the policy actions or the behavior of allies or adversaries.
- Assess how each of these forces could affect the analytic problem.
- Determine whether these forces actually do have an impact on the particular issue based on the available evidence.

RED TEAM ANALYSIS

Models the behavior of an individual or group by trying to replicate how an adversary would think about an issue.

WHEN TO USE

Frequently, analysts face the challenge of forecasting how a foreign leader or decisionmaking group may behave when it is clear that there is a risk of falling into a "mirror-image" problem. That is, analysts can sometimes impute to a foreign actor the same motives, values, or understanding of an issue that they hold. Traditional analysis sometimes assumes that foreign leaders or groups will behave "rationally" and act as the analysts would if faced with the same threats or opportunities. History has shown that foreign leaders often respond differently to events because of different cultural, organizational, or personal experiences.

Red Team analysis tries to consciously place analysts in the same cultural, organizational, and personal setting ("putting them in their shoes") in which the target individual or group operates. Whereas analysts normally work from the position of the "blue" (friendly forces), a "red" team of analysts attempts to work in the environment of the hostile forces.

VALUE ADDED

Like Devil's Advocacy and Team A/Team B techniques, Red Team analysis is aimed at freeing the analyst from the prison of a well-developed mind-set; in this case, the analyst's own sense of rationality, cultural norms, and personal values. Whereas analysts usually operate as "observers" of a foreign adversary, the Red Team technique transforms the analyst into an "actor" operating within the adversary's culture and political milieu. This form of "role playing" is useful when trying to replicate the mind-set of authoritarian leaders, terrorist cells, or other non-Western groups that operate under very different codes of behavior or motivations. Often this technique can introduce new or different stimuli that might not have been factored into traditional analysis—such as the target's familial ties or the international political, economic, and military pressures felt by the individual. For example, Red Team participants might ask themselves: "What would my peers, family, or tribe expect me to do? Alternatively, a Red Team analyst might pose the question to his colleagues: "How do we perceive the external threats and opportunities?" Finally, the Red Team technique can factor into its analysis the way in which personal power and status might influence a target's behavior.

THE METHOD

On issues that lend themselves to Red Team analysis, a manager needs to build a team of experts with in-depth knowledge of the operating environment, the target's personality, and the style of thinking used. The team should be populated not just with those who understand the language, but also with people who might have experienced the culture, share the ethnic background, or have worked in a similar operational environment. Once established and separated from traditional analysis, the team members should:

- Put themselves in the adversary's circumstances and react to foreign stimuli as the target would.
- Develop a set of "first-person" questions that the adversary would ask, such as: "How would I perceive incoming information; what would be my personal concerns; or to whom would I look for an opinion?"
- Draft a set of policy papers in which the leader or group makes specific decisions, proposes recommendations, or lays out courses of actions. The more these papers reflect the cultural and personal norms of the target, the more they can offer a different perspective on the analytic problem.

A Red Team Perspective
Iran's Military Strategy Vis-a-vis the United States

". . . The United States and Israel may be contemplating military operations against Iran, as per recent media reports . . . A week-long combined air and ground maneuver has just concluded in five of the southern and western provinces of Iran, mesmerizing foreign observers, who have described as 'spectacular' the massive display of high-tech, mobile operations, including rapid-deployment forces relying on squadrons of helicopters, air lifts, missiles, as well as hundreds of tanks and tens of thousands of well-coordinated personnel using live munitions.

Learning from both the 2003 Iraq war and Iran's own previous experiences of the 1980-88 war with Iraq and the 1987-88 confrontation with US forces in the Persian Gulf, Iranians have focused on the merits of a fluid and complex defensive strategy that seeks to take advantage of certain weaknesses in the US military superpower while maximizing the precious few areas where they may have the upper hand, e.g.; numerical superiority in ground forces, guerrilla tactics, terrain, etc.

Any US attack on Iran will likely be met first and foremost by missile counter-attacks engulfing the southern Persian Gulf states playing host to US forces, as well as any other country—e.g., Azerbaijan, Iraq, or Turkey allowing their territory or airspace to be used against Iran. The rationale for this strategy is precisely to pre-warn Iran's neighbors of the dire consequences, with potential debilitating impacts on their economies for a long time, should they become accomplices of foreign invaders of Iran.

Another key element of Iran's strategy is to "increase the arch of crisis" in places such as Afghanistan and Iraq, where it has considerable influence, to undermine the United States' foothold in the region, hoping to create a counter-domino effect wherein instead of gaining inside Iran, the US would actually lose territory partly as a result of thinning its forces and military 'overreach.'

Iran's counter-psychological warfare, on the other hand, seeks to take advantage of the 'death-fearing' American soldiers who typically lack a strong motivation to fight wars not necessarily in defense of the homeland. A war with Iran would definitely require establishing the draft in the US, without which it could not possibly protect its flanks in Afghanistan and Iraq.

There is a sense of national-security siege in Iran these days, in light of a tightening "security belt" by the US benefiting from military bases in Iraq, Turkey, Azerbaijan, Uzbekistan, Tajikistan, Kyrgyzstan, as well as Kuwait, Saudi Arabia, Qatar, Bahrain, Oman, and the island-turned garrison of Diego Garcia. From Iran's vantage point, the US, having won the Cold War, has turned into a 'leviathan unhinged' capable of manipulating and subverting the rule of international law and the United Nations with impunity, thus requiring a sophisticated Iranian strategy of deterrence, that, in the words of certain Iranian media pundits, would even include the use of nuclear weapons . . ."

—Excerpts from Kaveh L. Afrasiabi (Tehran University), "How Iran Will Fight Back," cited in Asia Times Online Ltd., 2004.

Red Team analysis is not easy to conduct. It requires significant time to develop a team of qualified experts who can think like the adversary. The team has to distance itself from the normal analysis and work as though living in the target's world. Without a sophisticated understanding of the culture, operational environment, and personal histories of the foreign group, analysts will not be able to behave or think like the enemy. Analysts can never truly escape their own experiences and mind-sets, but this technique can at least prevent them from falling into "mirror-imaging" unconsciously.

The most novel feature of Red Team analysis is its presentation.

- The analysis is often in a "first person" format—that is, drafted as memos to or from a leader or group.
- Red Team analysis avoids the use of caveats or qualifications and assumes that the recipient understands that the paper is aimed more at provoking thought or challenging the conventional understanding of how an adversary thinks.
- Such papers are rarely coordinated among other experts and do not purport to represent the consensus view on an issue.

Red Team papers do not plot out all possible courses of action but seek to give a prediction based on the target's special personal, organizational, or cultural experiences.

ALTERNATIVE FUTURES ANALYSIS

Systematically explores multiple ways a situation can develop when there is high complexity and uncertainty.

WHEN TO USE

Alternative futures analysis (often referred to as "scenarios") is most useful when a situation is viewed as too complex or the outcomes as too uncertain to trust a single outcome assessment. First, analysts must recognize that there is high uncertainty surrounding the topic in question. Second, they, and often their customers, recognize that they need to consider a wide range of factors that might bear on the question. And third, they are prepared to explore a range of outcomes and are not wedded to any preconceived result. Depending on how elaborate the futures project, the effort can amount to considerable investment in time, analytic resources, and money. A team of analysts can spend several hours or days organizing, brainstorming, and developing multiple futures; alternatively, a larger-scale effort can require preparing a multi-day workshop that brings together participants (including outside experts). Such an undertaking often demands the special skills of trained scenario-development facilitators and conferencing facilities.

This technique is a sharp contrast to contrarian techniques, which try to challenge the analysts' high confidence and relative certitude about an event or trend. Instead, multiple futures development is a divergent thinking technique that tries to use the complexity and uncertainty of a situation to describe multiple outcomes or futures that the analyst and policymaker should consider, rather than to predict one outcome.

VALUE ADDED

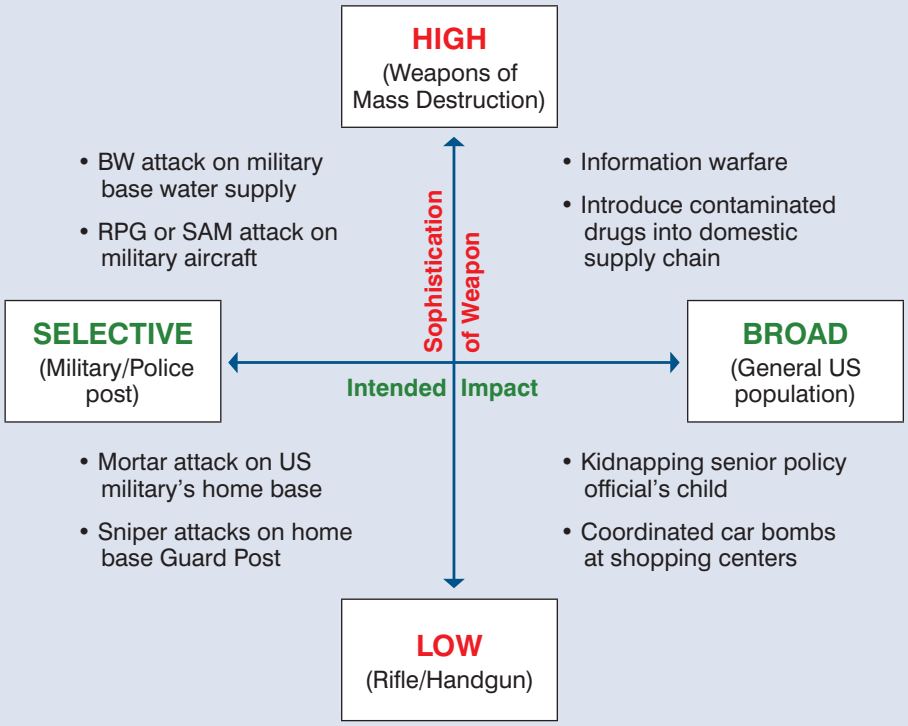
Alternative futures analysis is extremely useful in highly ambiguous situations, when analysts confront not only a lot of "known unknowns" but also "unknown unknowns." What this means is that analysts recognize that there are factors, forces, and dynamics among key actors that are difficult to identify without the use of some structured technique that can model how they would interact or behave. As the outcomes are not known prior to the futures exercise, analysts must be prepared for the unexpected and willing to engage in a more free-wheeling exchange of views than typically occurs in order to "imagine the future." Given the time and resources involved, scenario analysis is best reserved for situations that could potentially pose grave threats or otherwise have significant consequences.

From past experience, analysts have found that involving policymakers in the alternative futures exercise is the most effective way to communicate the results of this exploration of alternative outcomes and sensitize them to key uncertainties. Most participants find the process of developing such scenarios as useful as any finished product that attempts to capture the results of the exercise. Analysts and policymakers can benefit from this technique in several ways:

- It provides an effective means of weighing multiple unknown or unknowable factors and presenting a set of plausible outcomes.
- It can help to bound a problem by identifying plausible combinations of uncertain factors.
- It provides a broader analytic framework for calculating the costs, risks, and opportunities presented to policymakers by different outcomes.

> *"The future is plural."*
>
> —Peter Schwartz, author of *The Art of the Long View* and a widely acclaimed scenario developer.

Hypothetical Threats to the Homeland: Using Spectrums to Define Potential Targets



A Futures Exercise. The graphic captures four potential futures to understand how foreign insurgents might carry out an attack on the United States. A brainstorming exercise helped analysts identify two key uncertainties (the sophistication of weapons used by the insurgents and the intended impact of the attack) and arrayed these factors on a graph as the "x" and "y" axes. The four resulting quadrants in the 2 x 2 matrix allowed analysts to visualize potential targets from the various combinations (low to high sophistication of weapons and selective to broad intended impact of an attack). For example, if a group possessed highly sophisticated weapons and intended a broad attack on the United States, potential targets could include computer networks and domestic drug supplies. Having filled in a quadrant, analysts can then turn to devising likely indicators or signposts of such a future.

- It aids analysts and policymakers in anticipating what otherwise would be surprising developments by forcing them to challenge assumptions and consider possible "wild cards" or discontinuous events.

- It generates indicators to monitor for signs that a particular future is becoming more or less likely, so that policies can be reassessed.

THE METHOD

Although there are a variety of ways to develop alternative futures, the most common approach used in both the public and private sectors involves the following steps:

- Develop the "focal issue" by systematically interviewing experts and officials who are examining the general topic.

- Convene a group of experts (both internal and external) to brainstorm about the forces and factors that could affect the focal issue.

- Select by consensus the two most critical and uncertain forces and convert these into axes or continua with the most relevant endpoints assigned.

- Establish the most relevant endpoints for each factor; e.g., if economic growth were the most critical, uncertain force, the endpoints could be "fast" and "slow" or "transformative" and "stabilizing" depending on the type of issue addressed.

- Form a futures matrix by crossing the two chosen axes. The four resulting quadrants provide the basis for characterizing alternative future worlds.

- Generate colorful stories that describe these futures and how they could plausibly come about. Signposts or indicators can then be developed.

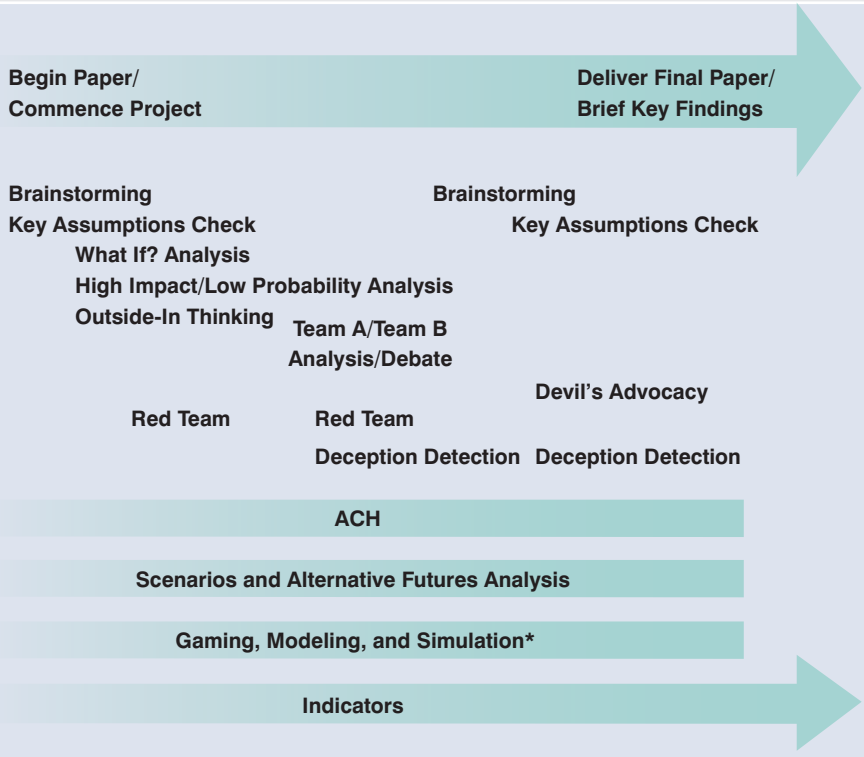
Participants, especially policymakers, can then consider how current decisions or strategies would fare in each of the four worlds and identify alternative policies that might work better either across all the futures or in specific ones. By anticipating alternative outcomes, policymakers have a better chance of either devising strategies flexible enough to accommodate multiple outcomes or of being prepared and agile in the face of change.

These structured analytic techniques can be used in a variety of ways when analysts begin a new assessment. Some can be used equally effectively at multiple points in the process and can promote an analyst's ability to keep an open mind, to consider multiple—including highly unlikely—hypotheses, to challenge conventional wisdom, and to assess the impact of important information gaps or deception on analytic judgments and confidence levels. The Timeline for Using Analytic Techniques provides some thoughts on when to use one or more of them during the course of an analyst's research and writing.

Starting Out

At the beginning of an analytic project, analysts are always wise to consider brainstorming and assumptions checks to insure that important factors are not being missed or taken for granted. Similarly, outside-in-thinking can sometimes put an analytic project into a broader international context, in which factors outside the lead analyst's area of responsibility might impact on his or her analytic judgments. For instance, economic assumptions about the price of oil might be key to a regional political analyst's understanding the prospects for political stability in an oil-exporting

A Timeline for Using Analytic Techniques Throughout an Analytic Project



*Gaming, Modeling, and Simulation are among the more sophisticated techniques taught in a more advanced analytic methods course and usually require substantial commitments of analyst time and corporate resources.

country or a underdeveloped country entirely dependent on expensive energy imports. A High Impact/Low Probability assessment can also sensitize analysts early on to the significance of dramatic events that might affect their analytic lines.

Some techniques like Indicators and Signposts or Analysis of Competing Hypotheses (ACH) can be useful throughout a project and revisited periodically as new information is absorbed and analyzed. ACH, in particular, is a good tool to use throughout a project to prevent premature closure and to highlight evidence that is most "discriminating" in making an analytic argument. Alternative Futures analysis is similarly useful at the beginning of a project, but can amount to the structure for the entire project.

Hypothesis Testing

As an analytic project takes shape, and hypotheses are being formed about the key intelligence question, it can be appropriate to use one or another contrarian technique to challenge the conventional analytic line that is being developed. If the assessment contains strong judgments about an adversary's behavior, then challenging this view with a "Red Team" effort might be a good corrective to too much of a rational actor approach. Also, a review of intelligence gaps at this juncture can also help give the analysts a better degree of confidence in the information base and judgments reached in the assessment.

A Final Check

As the assessment is being finalized, it can still be useful to review key assumptions as a sanity check on the underlying logic of the analysis. A brainstorming session also may be helpful to insure that no plausible hypothesis has been dismissed or left unaddressed. If a firm consensus has formed around an analytic line and has not been seriously questioned in some time, then a Devil's Advocacy exercise could be useful. Analysts might also use a final review to decide if they have identified a list of key indicators for future developments. This can be an important guide to include in the assessment as a way to track future developments and monitor whether the analytic judgments reached are being realized or in need of revision.

Graham Allison, *Essence of Decision*: *Explaining the Cuban Missile Crisis*: Examines the Kennedy Administration's decisionmaking style from alternative perspectives of the "rational actor," "organizational actor," and "bureaucratic politics" models.

Max Bazerman and Michael D. Watkins, *Predictable Surprises: The Disasters You Should Have Seen Coming and How To Prevent Them*. Examines the cognitive, organizational and political causes of some predictable surprises and outlines steps to overcome them.

Richard Betts, *Surprise Attack: Lessons for Defense Planning*. Explains why surprise attacks historically have succeeded and argues that the US needs strategies for avoiding surprise or at least reducing their consequences. Uses examples from World War II, Korea, and the Middle East.

Josh Epstein and Rob Axtell, *Sugarscape: Creating Artificial Societies from the Ground Up*. Develops a very simple agent-based model of a silicon-based society and then does simulations of various social, economic and political phenomena, including conflict.

Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference*. Examines how social trends, ideas, and products emerge from nowhere and take hold.

Cynthia M. Grabo, *Anticipating Surprises: Analysis for Strategic Warning.* Examines distinctive ingredients of the analytical method of intelligence and suggests ways of improving warning assessments.

Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis*. Examines the impediments to good analysis and provides techniques for overcoming mind-sets and cognitive biases.

Barry Hughes, *International Futures*. Develops scenarios for international relations using a simulation tool contained in a CD ROM in the back jacket.

Robert Jervis, *Perception and Misperception in International Politics*. Examines how policymakers learn from history, perceive complexity, and form and change their beliefs.

Gary Klein, *Intuition At Work*. Shows how developing one's intuition can improve your analytic skills and that it is a "learnable" technique.

Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decisionmakers*. Uses case study methods to identify the perils of historical analogies and recommends identifying what is "known, unclear and presumed."

Peter Schwartz, *The Art of the Long View: Planning for the Future in an Uncertain World*. Explains the "scenaric" approach pioneered at Royal Dutch Shell and argues for making strategic decisions that will be sound for "all plausible futures."

James Surowiecki, *The Wisdom of Crowds*. Argues that diversity and independence of even non-expert individuals in groups, properly organized, can reach more accurate forecasts than individual experts.

M. Mitchell Waldrop, *Complexity: The Emerging Science at the Edge of Disorder and Chaos*. Introduces the literature of complex systems and suggests why forecasting anything complicated is so difficult.

Joint Military Intelligence College

June 1999

INTELLIGENCE ESSENTIALS FOR EVERYONE

Occasional Paper Number Six

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 1999		**00-00-1999 to 00-00-1999**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intelligence Essentials for Everyone	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Military Intelligence College,200 MacDill Blvd,Washington,DC,20340-5100**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**89**	

The Joint Military Intelligence College supports and encourages research on intelligence issues that distills lessons and improves support to policy-level and operational consumers.

This series of Occasional Papers presents the work of faculty, students and others whose research on intelligence issues is supported or otherwise encouraged by the Joint Military Intelligence College through its Office of Applied Research. Occasional Papers are distributed to Department of Defense schools and to the Intelligence Community, and unclassified papers are available to the public through the National Technical Information Service (www.ntis.gov).

Proposed manuscripts for these papers are submitted for consideration to the Applied Research Editorial Board. Papers undergo review by senior officials in Defense, Intelligence, and occasionally civilian academic or business communities. Manuscripts or requests for additional copies of Occasional Papers should be addressed to Defense Intelligence Agency, Joint Military Intelligence College, Office of Applied Research, MCE, Bolling AFB, Washington, DC 20340-5100.

Occasional Paper Number Six

INTELLIGENCE ESSENTIALS FOR EVERYONE

By Lisa Krizan

JOINT MILITARY INTELLIGENCE COLLEGE
WASHINGTON, DC
June 1999

The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government

This paper has been approved for unrestricted public release by the Office of the Secretary of Defense (Public Affairs)

CONTENTS

Preface v

Foreword vii

Prologue: Intelligence Sharing in a New Light. 1

Part

I Intelligence Process 7

II Converting Customer Needs into Intelligence Requirements 13

III Collection 21

IV Processing Collected Information 25

V Analysis 29

VI Production 39

VII Managing the Intelligence Process 49

VIII Portrait of an Intelligence Analyst. 55

IX Defensive Measures for Intelligence 61

Epilogue 71

Glossary 72

Bibliography 75

About the Author 81

INTELLIGENCE ESSENTIALS FOR EVERYONE

Preface

The "importance of understanding" has become almost an obsession with significant portions of American business. There remain, however, many companies that attempt to operate as they traditionally have in the past — placing great faith in the owner's or manager's judgment as to what is required to remain competitive.

In this paper, the author has articulated clearly the fundamentals of sound intelligence practice and has identified some guidelines that can lead toward creation of a solid intelligence infrastructure. These signposts apply both to government intelligence and to business. Good intelligence should always be based on validated requirements, but it may be derived from a wide variety of sources, not all of which are reliable.

Understanding the needs of the consumer and the sources available enable an analyst to choose the correct methodology to arrive at useful answers. The author has laid out in clear, concise language a logical approach to creating an infrastructure for government and business. Every system will have flaws but this discussion should help the reader minimize those weaknesses. It is an important contribution to the education of government and business intelligence professionals.

James A. Williams, LTG, U.S. Army (Ret.)
Former Director, Defense Intelligence Agency

INTELLIGENCE ESSENTIALS FOR EVERYONE

Foreword

Decades of government intelligence experience and reflection on that experience are captured in this primer. Ms. Krizan combines her own findings on best practices in the intelligence profession with the discoveries and ruminations of other practitioners, including several Joint Military Intelligence College instructors and students who preceded her. Many of the selections she refers to are from documents that are out of print or have wrongly been assigned to a dustbin.

This primer reviews and reassesses Intelligence Community best practices with special emphasis on how they may be adopted by the private sector. The government convention of referring to intelligence users as "customers" suggests by itself the demonstrable similarities between government intelligence and business information support functions.

The genesis for this study was the author's discovery of a need to codify for the Intelligence Community certain basic principles missing from the formal training of intelligence analysts. At the same time, she learned of requests from the private sector for the same type of codified, government best practices for adaptation to the business world. As no formal mechanism existed for an exchange of these insights between the public and private sectors, Ms. Krizan developed this paper as an adjunct to her Master's thesis, *Benchmarking the Intelligence Process for the Private Sector.* Her thesis explores the rationale and mechanisms for benchmarking the intelligence process in government, and for sharing the resultant findings with the private sector.

The author and editor wish to acknowledge the constructive comments of two reviewers from the business community, representing the Amoco Corporation and DeGenaro and Associates, Inc. of Sarasota, Florida.

Comments on this paper are welcome, and should be directed to the Office of Applied Research, MCE-2, Joint Military Intelligence College, DIAC, Bolling AFB, Washington, DC 20340-5100. Telephone (202) 231-4193; DSN 428-4193; e-mail *AFswerg@dia.osis.gov.*

Dr. Russell G. Swenson, Editor and Director, Office of Applied Research

PROLOGUE: INTELLIGENCE SHARING IN A NEW LIGHT

Education is the cheapest defense of a nation.
— Edmund Burke, 18th-century British philosopher

National Intelligence Meets Business Intelligence

This intelligence primer reflects the author's examination of dozens of unclassified government documents on the practice of intelligence over a period of nearly seven years. For the national security Intelligence Community (IC), it represents a concise distillation and clarification of the national intelligence function. To the private sector, it offers an unprecedented translation into lay terms of national intelligence principles and their application within and potentially outside of government.[1] Whereas "intelligence sharing" has traditionally been a government-to-government transaction, the environment is now receptive to government-private sector interaction.

The widespread trend toward incorporating government intelligence methodology into commerce and education was a primary impetus for publishing this document. As economic competition accelerates around the world, private businesses are initiating their own "business intelligence" (BI) or "competitive intelligence" services to advise their decisionmakers. Educators in business and academia are following suit, inserting BI concepts into professional training and college curricula.[2]

Whereas businesses in the past have concentrated on knowing the market and making the best product, they are shifting their focus to include knowing, and staying ahead of, competitors. This emphasis on competitiveness requires the sophisticated production and use of carefully analyzed information tailored to specific users; in other words, intelligence. But the use of intelligence as a strategic planning tool, common in government, is a skill that few companies have perfected.[3]

Although BI practitioners refer to the national security model of intelligence, they do not seek to conduct secret intelligence operations, which are limited by law to government

---

[1] For the purpose of this study, the author includes in national security intelligence those analogous activities conducted by law enforcement personnel at the federal, state, and local levels. Readers seeking further information on law enforcement applications of intelligence may wish to read Marilyn Peterson, *Applications in Criminal Analysis* (Westport, Connecticut: Greenwood Press, 1994). An additional resource is the International Association of Law Enforcement Intelligence Analysts. Local IALEIA chapters are listed on the Association's web site: http://www.ialeia.org.

[2] An authoritative guide to business intelligence practices is found in Larry Kahaner, *Competitive Intelligence: From Black Ops to Boardrooms — How Businesses Gather, Analyze and Use Information to Succeed in the Global Marketplace* (New York, NY: Simon and Schuster, 1996).

[3] Richard D'Aveni, "Hypercompetition," briefing to SCIP Conference, Alexandria, VA, 28 March 1996.

authorities. The Society of Competitive Intelligence Professionals (SCIP), headquartered in the Washington, DC area, is an international organization founded in 1986 to "assist members in enhancing their firms' competitiveness through a greater... understanding of competitor behaviors and future strategies as well as the market dynamics in which they do business."[4] SCIP's code of conduct specifically promotes ethical and legal BI practices.[5] The main focus of "collection" is on exploiting on-line and open-source information services, and the theme of "analysis" is to go beyond mere numerical and factual information, to interpretation of events for strategic decisionmaking.[6]

Large corporations are creating their own intelligence units, and a few are successful at performing analysis in support of strategic decisionmaking. Others are hiring BI contractors, or "out-sourcing" this function. However, the majority of businesses having some familiarity with BI are not able to conduct rigorous research and analysis for value-added reporting. According to University of Pittsburgh professor of Business Administration John Prescott, no theoretical framework exists for BI. He believes that most studies done lack the rigor that would come with following sound research-design principles. By his estimate, only one percent of companies have a research-design capability exploitable for BI applications.[7] At the same time, companies are increasingly opting to establish their own intelligence units rather than purchasing services from BI specialists. The implication of this trend is that BI professionals should be skilled in both intelligence and in a business discipline of value to the company.[8]

On the other hand, as businesses come to appreciate the value of intelligence about their competitors, they are increasingly realizing their own vulnerability to similar scrutiny. The private sector can therefore benefit from IC expertise in disciplines complementary to active intelligence production, namely defensive measures. The whole concept of openness regarding intelligence practices may hinge upon the counter-balancing effect of self-defense, particularly as practiced through information systems security (INFOSEC) and operations security (OPSEC).[9] Because the IC seeks to be a world leader in INFOSEC and OPSEC as well as intelligence production, defensive measures are an appropriate topic for dialogue between the public and private sectors.

The U.S. government INFOSEC Manual sums up the relationship between offense and defense in a comprehensive intelligence strategy in this way:

> In today's information age environment, control of information and information technology is vital. As the nation daily becomes more dependent on

---

4 SCIP, *Competitive Intelligence Review*, 8, No. 3 (Fall 1997), unnumbered 8th page.

5 SCIP, *1995 SCIP Membership Directory* (Alexandria, VA: SCIP, 1995), xxvii.

6 Leila Kight, "Elements of CI Success," briefing to SCIP Conference, Alexandria, VA, 28 March, 1996.

7 John Prescott, Professor of Business Administration, University of Pittsburgh, "Research," briefing to SCIP conference, Alexandria, VA, 28 March 1996.

8 Jan Herring, "Strides in Institutionalizing BI in Businesses," briefing to SCIP Conference, Alexandria, VA, 28 March 1996.

9 These concepts are addressed in Part IX.

> networked information systems to conduct essential business, including military operations, government functions, and national and international economic enterprises, information infrastructures are assuming increased strategic importance. This has, in turn, given rise to the concept of information warfare (INFOWAR) — a new form of warfare directed toward attacking (offensive) or defending (defensive) such infrastructures.[10]

Giving citizens the tools they need to survive INFOWAR is one of the IC's explicit missions. This intelligence primer can assist that mission by offering a conceptual and practical "common operating environment" for business and government alike.[11]

Assessing and Exchanging Best Practices

In documenting the essentials of intelligence, this primer is an example of *benchmarking*, a widely used process for achieving quality in organizations, the use of which is a criterion for the business world's Malcolm Baldrige National Quality Award.[12] Benchmarking normally assesses best professional practices, developed and refined through experience, for carrying out an organization's core tasks.[13] An additional aim of benchmarking is to establish reciprocal relationships among best-in-class parties for the exchange of mutually beneficial information.[14] Because the IC is the *de facto* functional leader in the intelligence profession, and is publicly funded, it is obligated to lead both the government and private sector toward a greater understanding of the intelligence discipline.

In the mid-1990s, as national intelligence agencies began to participate in international benchmarking forums, individuals from the private sector began to request practical information on the intelligence process from IC representatives. The requestors were often participants in the growing BI movement and apparently sought to adapt IC methods to their own purposes. Their circumspect counterparts in the government were not prepared to respond to these requests, preferring instead to limit benchmarking relationships to common business topics, such as resource management.[15] Concurrently, the annual SCIP international conference highlighted the needs and capabilities of intelligence departments in the private sector.

---

[10] National Security Agency, *1995 INFOSEC Manual* (Ft. Meade, MD: NSA, 1995), para. C.1.

[11] Readers in doubt of the need for INFOSEC in the private sector may wish to study the real-world examples of INFOWAR battles and their implications for economic and personal security that author Winn Schwartau reveals in *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994).

[12] A useful reference to benchmarking within the U.S. government is Jerry Frankenfield and Melissie Rumizen, *A Guide to Benchmarking* (Fort Meade, MD: National Security Agency (NSA), 12 July 1995). An overview of benchmarking in the private sector can be found in Dean Elmuti, Hanus Kathawaia, and Scott J. Lloyed, "The Benchmarking Process: Assessing Its Value and Limitations," *Industrial Management*, 39, No. 4 (July/August 1997): 12-19.

[13] Elmuti, Kathawaia and Lloyed, 12.

[14] Elmuti, Kathawaia and Lloyed, 13.

[15] Melissie C. Rumizen, Ph.D., Benchmarking Manager, National Security Agency, interview with the author, 2 April 1996.

Demand in the private sector for intelligence skills can be met through the application of validated intelligence practices presented in this document. Conversely, the business-oriented perspective on intelligence can be highly useful to government intelligence professionals. As a BI practitioner explains, every activity in the intelligence process must be related to a requirement, otherwise it is irrelevant.[16] Government personnel would benefit from this practical reminder in every training course and every work center. In the private sector, straying from this principle means wasting money and losing a competitive edge. The consequences of inefficient national intelligence can be costly on an even larger scale.

The basis for an IC benchmarking exchange with the private sector continues to grow. The Society of Competitive Intelligence Professionals is a clearinghouse for the review of private business intelligence practices, and therefore a champion of information sharing. Leading colleges and universities are beginning to offer coursework in intelligence methods, and in many cases intend to expand their offerings. Curriculum exchanges between private sector educators and the IC are encouraged by legislation and by Congressional Commission recommendations,[17] yet little such formal exchange has taken place.

Whereas government practitioners are the acknowledged subject-matter experts in intelligence methodology, the private sector offers a wealth of expertise in particular areas such as business management, technology, the global marketplace, and skills training. Each has valuable knowledge to share with the other, and experience gaps to fill. On the basis of these unique needs and capabilities, the public and private sectors can forge a new partnership in understanding their common responsibilities, and this primer may make a modest contribution toward the exchange of ideas.

The following chapters outline validated steps to operating an intelligence service for both the government and the private sector. In either setting, this document should prove useful as a basic curriculum for students, an on-the-job working aid for practitioners, and a reference tool for experienced professionals, especially those teaching or mentoring others. Although the primer does not exhaustively describe procedures for quality intelligence production or defensive measures, it does offer the business community fundamental concepts that can transfer readily from national intelligence to commercial applications, including competitive analysis, strategic planning and the protection of proprietary information. Universities may incorporate these ideas into their business, political science, and intelligence studies curricula to encourage and prepare students to become intelligence practitioners in commerce or government. For anyone outside of the

---

[16] David Harkleroad, “Actionable CI,” briefing to SCIP Conference, Alexandria, VA, 28 March 1996.

[17] For example, the 1991 National Security Education Act (P.L. 102-183), the 1993 Government Performance and Results Act (P.L. 103-62), and the Congressional Report of the Commission on the Roles and Capabilities of the U.S. Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Washington, DC: GPO, 1 March 1996), 87.

national security apparatus, this intelligence primer will shed light on why and how the government spends federal tax dollars on national intelligence.

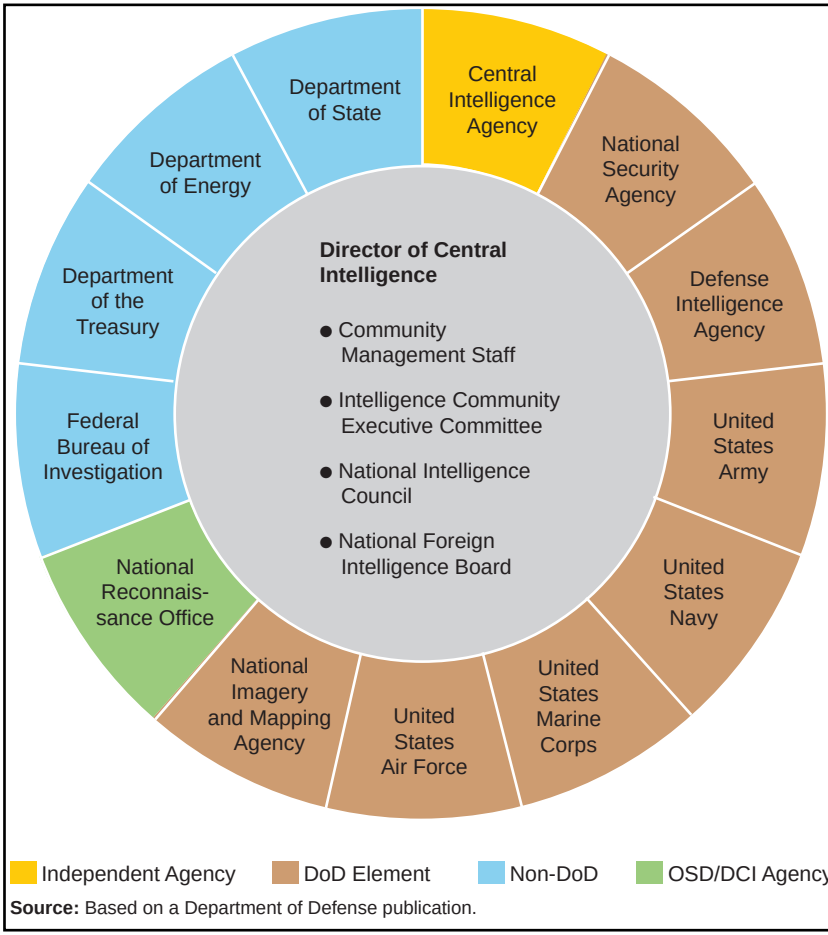


Figure 1: The National Intelligence Community.

PART I
INTELLIGENCE PROCESS

> [I]ntelligence is more than information. It is knowledge that has been specially prepared for a customer's unique circumstances. The word *knowledge* highlights the need for human involvement. Intelligence collection systems produce... data, not intelligence; only the human mind can provide that special touch that makes sense of data for different customers' requirements. The special processing that partially defines intelligence is the continual collection, verification, and analysis of information that allows us to understand the problem or situation in actionable terms and then tailor a product in the context of the customer's circumstances. If any of these essential attributes is missing, then the product remains information rather than intelligence.[18]

The intelligence profession, already well established within government, is growing in the private sector. Intelligence is traditionally a function of government organizations serving the decisionmaking needs of national security authorities. But innovative private firms are increasingly adapting the national security intelligence model to the business world to aid their own strategic planning. Although business professionals may prefer the term "information" over "intelligence," the author will use the latter term to highlight the importance of adding value to information. According to government convention, the author will use the term "customer" to refer to the intended recipient of an intelligence product — either a fellow intelligence service member, or a policy official or decisionmaker. The process of converting raw information into actionable intelligence can serve government and business equally well in their respective domains.

The Intelligence Process in Government and Business

Production of intelligence follows a cyclical *process*, a series of repeated and interrelated steps that add value to original inputs and create a substantially transformed product. That transformation is what distinguishes intelligence from a simple cyclical activity.[19] In government and private sector alike, analysis is the catalyst that converts information into intelligence for planners and decisionmakers.

Although the intelligence process is complex and dynamic, several component functions may be distinguished from the whole. In this primer, components are identified as Intelligence Needs, Collection Activities, Processing of Collected Information, Analysis and Production. To highlight the components, each is accorded a separate Part in this study. These

---

[18] Captain William S. Brei, *Getting Intelligence Right: The Power of Logical Procedure*, Occasional Paper Number Two (Washington, DC: Joint Military Intelligence College, January 1996), 4.

[19] Melissie C. Rumizen, Benchmarking Manager at the National Security Agency, interview by author, 4 January 1996.

labels, and the illustration below, should not be interpreted to mean that intelligence is a unidimensional and unidirectional process. "[I]n fact, the [process] is multidimensional, multidirectional, and — most importantly — interactive and iterative."[20]

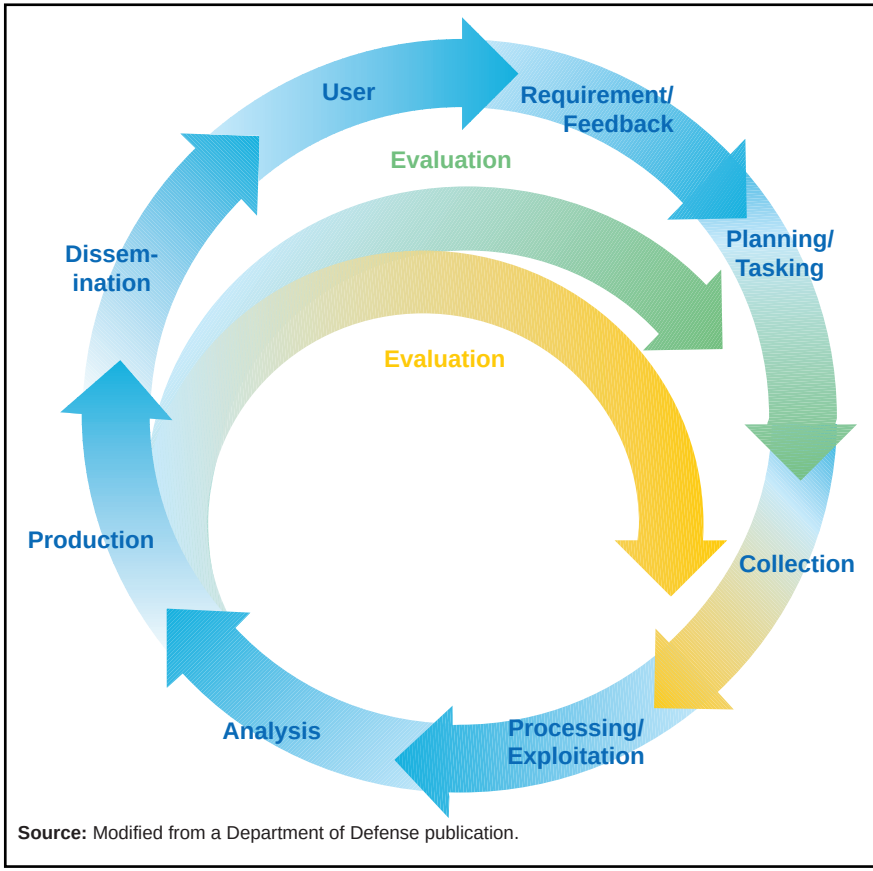


Figure 2: Process of Intelligence Creation and Use.

[20] Douglas H. Dearth, "National Intelligence: Profession and Process," in *Strategic Intelligence: Theory and Application*, eds. Douglas H. Dearth and R. Thomas Goodden, 2d ed. (Washington, DC: Joint Military Intelligence Training Center, 1995), 17.

The purpose of this process is for the intelligence service to provide decisionmakers with tools, or "products" that assist them in identifying key decision factors. Such intelligence products may be described both in terms of their subject content and their intended use.[21]

Table 1: Types of Intelligence Product Categories
Source: adapted from Garst, "Components of Intelligence"

By Subject	By Use
Biographic	Research
Economic	Current
Geographic	Estimative
Military	Operational
Political	Scientific and Technical
Sociological	Warning
Scientific and Technical	
Transportation and Communications	

Any or all of these categories may be relevant to the private sector, depending upon the particular firm's product line and objectives in a given industry, market environment, and geographic area.

A nation's power or a firm's success results from a combination of factors, so intelligence producers and customers should examine potential adversaries and competitive situations from as many relevant viewpoints as possible. A competitor's economic resources, political alignments, the number, education and health of its people, and apparent objectives are all important in determining the ability of a country or a business to exert influence on others. The eight subject categories of intelligence are exhaustive, but they are not mutually exclusive. Although dividing intelligence into subject areas is useful for analyzing information and administering production, it should not become a rigid formula. Some intelligence services structure production into geographic subject areas when their responsibilities warrant a broader perspective than topical divisions would allow.[22]

---

[21] Ronald D. Garst, "Components of Intelligence," in *A Handbook of Intelligence Analysis*, ed. Ronald D. Garst, 2d ed. (Washington, DC: Defense Intelligence College, January 1989), 1; Central Intelligence Agency, *A Consumer's Guide to Intelligence* (Washington, DC: Public Affairs Staff, July 1995), 5-7.

[22] Garst, *Components of Intelligence*, 2,3.

Similarly, characterization of intelligence by intended use applies to both government and enterprise, and the categories again are exhaustive, but not mutually exclusive. The production of basic research intelligence yields structured summaries of topics such as geographic, demographic, and political studies, presented in handbooks, charts, maps, and the like. Current intelligence addresses day-to-day events to apprise decisionmakers of new developments and assess their significance. Estimative intelligence deals with what might be or what might happen; it may help policymakers fill in gaps between available facts, or assess the range and likelihood of possible outcomes in a threat or "opportunity" scenario. Operational support intelligence incorporates all types of intelligence by use, but is produced in a tailored, focused, and timely manner for planners and operators of the supported activity. Scientific and Technical intelligence typically comes to life in in-depth, focused assessments stemming from detailed physical or functional examination of objects, events, or processes, such as equipment manufacturing techniques.[23] Warning intelligence sounds an alarm, connoting urgency, and implies the potential need for policy action in response.

How government and business leaders define their needs for these types of intelligence affects the intelligence service's organization and operating procedures. Managers of this intricate process, whether in government or business, need to decide whether to make one intelligence unit responsible for all the component parts of the process or to create several specialized organizations for particular sub-processes. This question is explored briefly below, and more fully in Part VII.

Functional Organization of Intelligence

The national Intelligence Community comprises Executive Branch agencies that produce classified and unclassified studies on selected foreign developments as a prelude to decisions and actions by the president, military leaders, and other senior authorities. Some of this intelligence is developed from special sources to which few individuals have access except on a strictly controlled "need-to-know" basis.[24] The four categories of special intelligence are Human Resources (HUMINT), Signals (SIGINT), Imagery (IMINT) and Measurement and Signatures (MASINT). The four corresponding national authorities for these categories are the Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Imagery and Mapping Agency (NIMA) and the Defense Intelligence Agency (DIA). DIA shares authority for HUMINT, being responsible for Department of Defense HUMINT management. Along with these four agencies, other members of the Intelligence Community use and produce intelligence by integrating all available and relevant collected information into reports tailored to the needs of individual customers.

Private sector organizations use open-source information to produce intelligence in a fashion similar to national authorities. By mimicking the government process of translating customer needs into production requirements, and particularly by performing rigorous analysis on gathered information, private organizations can produce assessments that aid their leaders in

---

[23] CIA, *Consumer's Guide*, 5-7.
[24] CIA, *Consumer's Guide*, vii.

planning and carrying out decisions to increase their competitiveness in the global economy. This primer will point out why private entities may desire to transfer into their domain some well-honed proficiencies developed in the national Intelligence Community. At the same time, the Intelligence Community self-examination conducted in these pages may allow government managers to reflect on any unique capabilities worthy of further development and protection.

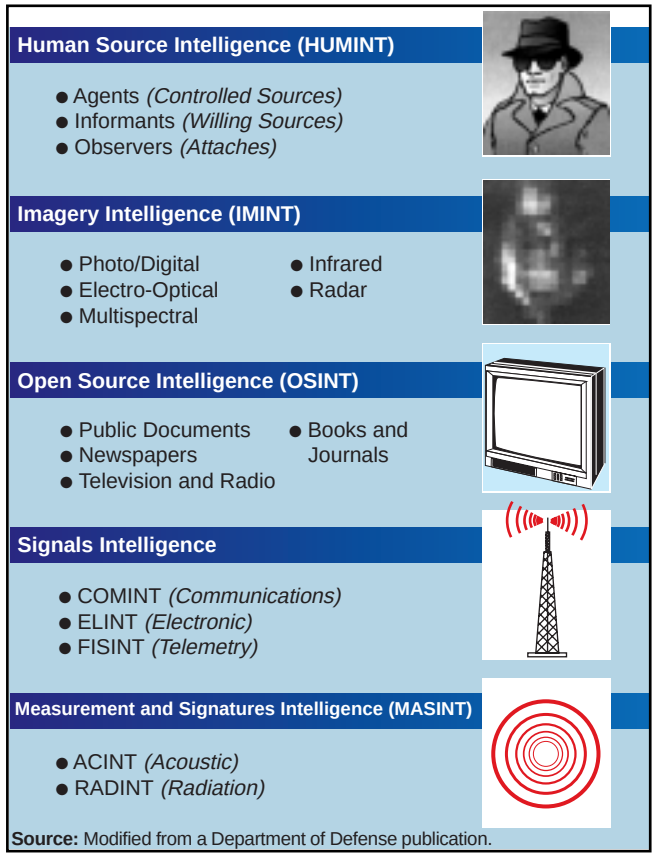


Figure 3: National Intelligence Production Resources.

PART II
CONVERTING CUSTOMER NEEDS INTO INTELLIGENCE REQUIREMENTS

> The articulation of the requirement is the most important part of the process, and it seldom is as simple as it might seem. There should be a dialogue concerning the requirement, rather than a simple assertion of need. Perhaps the customer knows precisely what is needed and what the product should look like. Perhaps... not. Interaction is required: discussion between ultimate user and principal producer. This is often difficult due to time, distance, and bureaucratic impediments, not to mention disparities of rank, personality, perspectives, and functions.[25]

Defining the Intelligence Problem

Customer demands, or "needs," particularly if they are complex and time-sensitive, require interpretation or analysis by the intelligence service before being expressed as intelligence requirements that drive the production process.[26] This dialog between intelligence producer and customer may begin with a simple set of questions, and if appropriate, progress to a more sophisticated analysis of the intelligence problem being addressed.

The "Five Ws" — *Who*, *What*, *When*, *Where*, and *Why* — are a good starting point for translating intelligence needs into requirements. A sixth related question, *How*, may also be considered. In both government and business, these questions form the basic framework for decisionmakers and intelligence practitioners to follow in formulating intelligence requirements and devising a strategy to satisfy them. Typically, government intelligence requirements are expressed in terms of foreign threats to national or international security. In business, requirements may be expressed in terms of the competitor's standing in the marketplace in comparison to one's own posture. Representative examples from each sector follow:

[25] Dearth, "National Intelligence," 17-18.
[26] Dearth, "National Intelligence," 18.

Table 2: Illustrative Definitions of Intelligence Problems and Customer Needs

Source: Author

A Government Scenario

The Intelligence Problem					
Who	***What***	***When***	***Where***	***Why***	***How***
A foreign president	Refusing to allow weapons sites to be inspected	Now; for several months	Country X	Unknown, possibly to hide illegal weapons	Barring access, destroying monitoring equipment
The Intelligence Need					
Who	***What***	***When***	***Where***	***Why***	***How***
U.S. President	Wants info on Country X President	Now, and update	White House	Determine power base and intent	All-source collection & analysis

A Business Scenario

The Intelligence Problem					
Who	***What***	***When***	***Where***	***Why***	***How***
Company X	Reorganizes production department	Sudden	Saturated market	Unknown	Unknown
The Intelligence Need					
Who	***What***	***When***	***Where***	***Why***	***How***
CEO of similar Company Y	Wants to know why and how Company X changed	ASAP	CEO's office	Determine if new structure gives advantage	Open source analysis; tailored, confidential report

Examination of these basic scenarios should inspire further development of the concept of determining customer needs in specific situations. The thoughtful researcher may propose, for example, ways to gather information on additional aspects of the problem (Who, What) and on customers (Who), as well as on the attendant motivations (Why) and strategies (How) of the target and the customer. Defining the intelligence problem in this manner paves the way for the next step in the intelligence process — the development of intelligence collection, analysis, and production *requirements*, explained later in this chapter.

Another, more complex model for defining intelligence scenarios employs the Taxonomy of Problem Types.[27] The table below illustrates the factors that customers and producers may take into account in articulating the nature of the intelligence problem and selecting a strategy for resolving it.

Table 3: Taxonomy of Problem Types

Source: Analysis course material, Joint Military Intelligence College, 1991

Characteristics	Problem Types				
	Simplistic	**Deterministic**	**Moderately Random**	**Severely Random**	**Indeterminate**
What is the question?	Obtain information	How much? How many	Identify and rank all outcomes	Identify outcomes in unbounded situation	Predict future events/ situations
Role of facts	Highest	High	Moderate	Low	Lowest
Role of judgment	Lowest	Low	Moderate	High	Highest
Analytical task	Find information	Find/create formula	Generate all outcomes	Define potential outcomes	Define futures factors
Analytical method	Search sources	Match data to formula	Decision theory; utility analysis	Role playing and gaming	Analyze models and scenarios
Analytical instrument	Matching	Mathematical formula	Influence diagram, utility, probability	Subjective evaluation of outcomes	Use of experts
Analytic output	Fact	Specific value or number	Weighted alternative outcomes	Plausible outcomes	Elaboration on expected future
Probability of error	Lowest	Very low	Dependent on data quality	High to very high	Highest
Follow-up task	None	None	Monitor for change	Repeated testing to determine true state	Exhaustive learning

[27] Morgan D. Jones, *The Thinker's Toolkit* (New York: Random House, 1995), 44-46, as elaborated by Thomas H. Murray, Sequoia Associates, Inc., Arlington, VA., in coursework at the Joint Military Intelligence College.

As with the "Five Ws," this model enables decisionmakers and analysts to assess their needs and capabilities in relation to a particular intelligence scenario. This ability to establish a baseline and set in motion a collection and production strategy is crucial to conducting a successful intelligence effort. Too often, both producers and customers waste valuable time and effort struggling to characterize for themselves a given situation, or perhaps worse, they hastily embark upon an action plan without determining its appropriateness to the problem. Employing a structured approach as outlined in the Taxonomy of Problem Types can help the players avoid these inefficiencies and take the first step toward generating clear intelligence requirements by defining both the intelligence problem and the requisite components to its solution. Following are example scenarios. The reader is encouraged to follow the scenarios down the columns of the taxonomy table, then generate new scenarios in similar fashion.

Intelligence Problem Definition

A Government Scenario

The Severely Random problem type is one frequently encountered by the military in planning an operational strategy. This is the realm of wargaming. The initial intelligence problem is to identify all possible outcomes in an unbounded situation, so that commanders can generate plans for every contingency. The role of valid data is relatively minor, while the role of judgment is great, as history and current statistics may shed little light on how the adversary will behave in a hypothetical situation, and the progress and outcome of an operation against that adversary cannot be predicted with absolute accuracy. Therefore, the analytical task is to define and prepare for all potential outcomes. The analytical method is role playing and wargaming: placing oneself mentally in the imagined situation, and experiencing it in advance, even to the point of acting it out in a realistic setting. After experiencing the various scenarios, the players subjectively evaluate the outcomes of the games, assessing which ones may be plausible or expected to occur in the real world. The probability of error in judgment here is inherently high, as no one can be certain that the future will occur exactly as events unfolded in the game. However, repeated exercises can help to establish a measure of confidence, for practice in living out these scenarios may enable the players to more quickly identify and execute desired behaviors, and avoid mistakes in a similar real situation.

A Business Scenario

The Indeterminate problem type is one facing the entrepreneur in the modern telecommunications market. Predicting the future for a given proposed new technology or product is an extremely imprecise task fraught with potentially dire, or rewarding, consequences. The role of valid data is extremely minor here, whereas analytical judgments about the buying public's future — and changing — needs and desires are crucial. Defining the key factors influencing the future market is the analytical task, to be approached via the analytical method of setting up models and scenarios: the if/then/else process. Experts in the proposed technology or market are then employed to analyze these possibilities. Their output is a synthesized assessment of how the future will look under various conditions with regard to the

proposed new product. The probability of error in judgment is extremely high, as the decision is based entirely on mental models rather than experience; after all, neither the new product nor the future environment exists yet. Continual reassessment of the changing factors influencing the future can help the analysts adjust their conclusions and better advise decisionmakers on whether, and how, to proceed with the new product.

Generating Intelligence Requirements

Once they have agreed upon the nature of the intelligence problem at hand, the intelligence service and the customer together can next generate intelligence *requirements* to drive the production process. The intelligence requirement translates customer needs into an intelligence action plan. A good working relationship between the two parties at this stage will determine whether the intelligence produced in subsequent stages actually meets customer needs. However, the differing perspectives that each side brings to the negotiation process can make cooperation between them a difficult feat.[28]

Customers want intelligence to guide them clearly in making policy and operational decisions. They may have little understanding of the intelligence process, and little patience for the subjectivity and conditionality of intelligence judgments. For customers, intelligence can be just one of many influences on their decisionmaking, and may be given little weight in comparison to other, more readily digested, familiar, or policy-oriented inputs. However, intelligence is neither designed nor equipped to meet these customer expectations.[29]

As a discipline, intelligence seeks to remain an independent, objective advisor to the decisionmaker. The realm of intelligence is that of "fact," considered judgment, and probability, but not prescription. It does not tell the customer what to do to meet an agenda, but rather, identifies the factors at play, and how various actions may affect outcomes. Intelligence tends to be packaged in standard formats and, because of its methodical approach, may not be delivered within the user's ideal timeframe. For all these reasons, the customer may not see intelligence as a useful service.[30]

Yet, somehow the intelligence producer and customer must reconcile their differing perspectives in order to agree on intelligence requirements and make the production process work. Understanding each other's views on intelligence is the first step toward improving the relationship between them. The next step is communication. Free interaction among the players will foster agreement on intelligence priorities and result in products that decisionmakers recognize as meaningful to their agendas, yet balanced by rigorous analysis.[31] In addition, as discussed below, customer feedback on production quality will lead to better definition of future intelligence problems and requirements.

---

[28] Arthur S. Hulnick, "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach," *Intelligence and National Security*, 1, No. 2, (May 1986): 214-216.

[29] Hulnick, "Producer-Policy Consumer Linkage," 215-216.

[30] Hulnick, "Producer-Policy Consumer Linkage," 216.

[31] Adapted from Michael A. Turner, "Setting Analytical Priorities in U.S. Intelligence," *International Journal of Intelligence and CounterIntelligence*, 9, No. 3, (Fall 1996): 320-322.

Types of Intelligence Requirements

Having thus developed an understanding of customer needs, the intelligence service may proactively and continuously generate intelligence collection and production requirements to maintain customer-focused operations. Examples of such internally generated specifications include analyst-driven, events-driven, and scheduled requirements. The table below briefly describes them.[32]

Table 4: Types of Producer-Generated Intelligence Collection and Production Requirements

Source: Hulnick

Analyst-driven	Based on knowledge of customer and issues
Events-driven	In response to time-sensitive relevant events
Scheduled	Periodic activities to document and update target status

Further distinctions among intelligence requirements include timeliness and scope, or level, of intended use. Timeliness of requirements is established to meet standing (long-term) and *ad hoc* (short-term) needs. When the customer and intelligence service agree to define certain topics as long-term intelligence issues, they generate a standing requirement to ensure that a regular production effort can, and will, be maintained against that target. The customer will initiate an *ad hoc* requirement upon realizing a sudden short-term need for a specific type of intelligence, and will specify the target of interest, the coverage timeframe, and the type of output desired.

The scope or level of intended use of the intelligence may be characterized as strategic or tactical. Strategic intelligence is geared to a policymaker dealing with big-picture issues affecting the mission and future of an organization: the U.S. President, corporate executives, high-level diplomats, or military commanders of major commands or fleets. Tactical intelligence serves players and decisionmakers "on the ground" engaged in current operations: trade negotiators, marketing and sales representatives, deployed military units, or product developers.

Table 5: Types of Customer-Defined Intelligence Requirements

Source: Author

Timeliness	Short-term *(ad hoc)*	Long-term (standing)
Scope	Broad (strategic)	Narrow (tactical)

[32] Adapted from Arthur S. Hulnick, "Managing Intelligence Analysis: Strategies for Playing the End Game," *International Journal of Intelligence and CounterIntelligence* 2, No. 3 (Fall 1988): 327.

Ensuring that Requirements Meet Customer Needs

Even when they follow this method of formulating intelligence requirements together, decisionmakers and their intelligence units in the public and private sectors may still have an incomplete grasp of how to define their needs and capabilities — until they have evaluated the resultant products. Thus, customer feedback, production planning and tasking, as well as any internal product evaluation, all become part of the process of defining needs and creating intelligence requirements. However, when intelligence producers and users are not in nearly direct, daily contact, this process can consume a good deal of time. This is why the national Intelligence Community is experimenting with compressing both the accustomed time and spatial dimensions of the intelligence process through remote electronic collaboration and production methods.[33]

Whether in business or government, six fundamental values or attributes underlie the core principles from which all the essential intelligence functions are derived. The corollary is that intelligence customers' needs may be defined and engaged by intelligence professionals using these same values. Table 6 offers a brief explanation of how both intelligence customers and producers may use these values to evaluate how well they have translated needs into requirements that will result in useful products.[34]

Interpretation of these values turns a customer's need into a collection and production requirement that the intelligence service understands in the context of its own functions. However, illustrating the complexity of the intelligence process, once this is done, the next step is not necessarily collection.

Rather, the next stage is analysis. Perhaps the requirement is simply and readily answered — by an existing product, by ready extrapolation from files or data bases, or by a simple phone call or short desk note based on an analyst's or manager's knowledge. On the other hand, the requirement might necessitate laborious effort — extrapolation, collation, analysis, integration, and production — but still the product can be constructed and sent directly to the requester. Case closed; next problem.... Preliminary analysis might well show, however, that while much data exists, because the issue at hand is not a new one, gaps in information must be filled... Obviously, this calls for collection. This brings up an essential point: consumers do not drive collection *per se*; analysts do — or should.[35] Part III explores this next step in the intelligence process.

---

[33] The U.S. military has pioneered the concept of an electronic intelligence operating environment that transcends organizational boundaries. Congress has recommended that the IC adopt this *Joint Intelligence Virtual Architecture* model to take advantage of technological developments, reduce bureaucratic barriers, and thereby provide policymakers with timely, objective, and useful intelligence. See U.S. Congress Staff Study, House Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century,* (April 1996): Section III, "Intelligence Requirements Process."

[34] The six values are adapted by Brei from an earlier version of U.S. Department of Defense, Joint Chiefs of Staff, Joint Pub 2-0, *Joint Doctrine for Intelligence Support to Operations* (Washington, DC: GPO, 5 May 1995), IV-15.

[35] Dearth, "National Intelligence," 18-19.

Table 6: Intelligence Values

Source: Brei

Accuracy: All sources and data must be evaluated for the possibility of technical error, misperception, and hostile efforts to mislead.
Objectivity: All judgments must be evaluated for the possibility of deliberate distortions and manipulations due to self-interest.
Usability: All intelligence communications must be in a form that facilitates ready comprehension and immediate application. Intelligence products must be compatible with a customer's capabilities for receiving, manipulating, protecting, and storing the product.
Relevance: Information must be selected and organized for its applicability to a customer's requirements, with potential consequences and significance of the information made explicit to the customer's circumstances.
Readiness: Intelligence systems must be responsive to the existing and contingent intelligence requirements of customers at all levels of command.
Timeliness: Intelligence must be delivered while the content is still actionable under the customer's circumstances.

PART III
COLLECTION

The collection function rests on research — on matching validated intelligence objectives to available sources of information, with the results to be transformed into usable intelligence. Just as within needs-definition, analysis is an integral function of collection.

Collection Requirements

The collection *requirement* specifies exactly how the intelligence service will go about acquiring the intelligence information the customer needs. Any one, or any of several, players in the intelligence system may be involved in formulating collection requirements: the intelligence analyst, a dedicated staff officer, or a specialized collection unit.

In large intelligence services, collection requirements may be managed by a group of specialists acting as liaisons between customers and collectors (people who actually obtain the needed information, either directly or by use of technical means). Within that requirements staff, individual requirements officers may be dedicated to a particular set of customers, a type of collection resource, or a specific intelligence issue. This use of collection requirements officers is prevalent in the government. Smaller services, especially in the private sector, may assign collection requirements management to one person or team within a multidisciplinary intelligence unit that serves a particular customer or that is arrayed against a particular topic area.

Regardless of how it is organized, the requirements management function entails much more than simple administrative duties. It requires analytic skill to evaluate how well the customer has expressed the intelligence need; whether, how and when the intelligence unit is able to obtain the required information through its available collection sources; and in what form to deliver the collected information to the intelligence analyst.

Collection Planning and Operations

One method for selecting a collection strategy is to first prepare a list of expected target evidence. The collection requirements officer and the intelligence analyst for the target may collaborate in identifying the most revealing evidence of target activity, which may include physical features of terrain or objects, human behavior, or natural and man-made phenomena. The issue that can be resolved through this analysis is “What am I looking for, and how will I know it if I see it”?

Successful analysis of expected target evidence in light of the customer’s needs can determine what collection source and method will permit detection and capture of that evidence. Increasingly sophisticated identification of evidence types may reveal what collectible data are essential for drawing key conclusions, and therefore should be given priority; whether the evidence is distinguishable from innocuous information; and whether the intelligence service has the skills, time, money and authorization to collect the data

needed to exploit a particular target. Furthermore, the collection must yield information in a format that is either usable in raw form by the intelligence analyst, or that can be converted practicably into usable form.

For example, in the case of the first business scenario presented in Part II, the CEO needs intelligence on why and how the similar, competitor company suddenly reorganized its production department. The collection requirement might specify that the intelligence unit give first priority to this new issue; it will focus on collecting information about the competitor's reorganization. A list of relevant evidence might include the following: changes in personnel assignments, changes in supply of production components, budget deficit or surplus, age of infrastructure, breakthroughs in research and development, and changes in the cultural or natural environment. To exploit this evidence, the intelligence service would thus need direct or indirect access to information on the company's employees, its previous production methods, its financial status, its physical plant, its overall functional structure and operations, and the consumer market. The collection unit would choose from among the sources listed in Table 7 below those most likely to provide timely access to this information in usable form.

Finally, upon defining the collection requirement and selecting a collection strategy, the intelligence unit should implement that strategy by tasking personnel and resources to exploit selected sources, perform the collection, re-format the results if necessary to make them usable in the next stages, and forward the information to the intelligence production unit. This aspect of the collection phase may be called collection operations management. As with requirements management, it is often done by specialists, particularly in the large intelligence service. In smaller operations, the same person or team may perform some or all of the collection-related functions.

The small, multidisciplinary intelligence unit may experience certain benefits and disadvantages in managing multiple phases of the intelligence process at the same time. In comparison to the large, compartmentalized service, the smaller unit will likely experience greater overall efficiency of operations and fewer bureaucratic barriers to customer service. The same few people may act as requirements officers, operations managers and intelligence analysts/producers, decreasing the likelihood of communication and scheduling problems among them. This approach may be less expensive in terms of infrastructure and logistics than a functionally divided operation. On the other hand, the financial and time investment in training each individual in every facet of the intelligence process may be substantial. Furthermore, careful selection and assignment of personnel who thrive in a multidisciplinary environment will be vital to the unit's success, to help ward off potential worker stress and overload. An additional pitfall that the small unit should strive to avoid is the tendency to be self-limiting: overreliance on the same customer contacts, collection sources and methods, analytic approaches, and production formulas can lead to stagnation and irrelevance. The small intelligence unit should be careful to invest in new initiatives that keep pace with changing times and customer needs.

Collection Sources

The range of sources available to all intelligence analysts, including those outside of government, is of course much broader than the set of restricted, special sources available only for government use. U.S. government collection of information for intelligence purposes is channelled through the recognized intelligence collection disciplines described in Part I. From a different perspective, four general categories serve to identify the types of information sources available to the intelligence analyst: people, objects, emanations, and records. Strictly speaking, the information offered by these sources may not be called intelligence if the information has not yet been converted into a value-added product. In the government or private sector, collection may be performed by the reporting analyst or by a specialist in one or more of the collection disciplines. The following table, derived from Clauser and Weir, illustrates the distinct attributes offered by the four sources of intelligence.[36]

Table 7: Categories of Intelligence Sources by Analytic Use

Source: Adapted from Clauser and Weir

Source	Related Collection Discipline(s) and Source Attributes	Analytic Use
People	HUMINT; subject-matter experts, professional researchers, information specialists, eyewitnesses or participants	Transfer of first-hand knowledge, referral to other sources
Objects	IMINT; physical characteristics of equipment, materials, or products, such as texture, shape, size, and distinctive markings	Basis for emotive but objective reporting on composition, condition, origin, or human purpose
Emanations	MASINT, SIGINT; detectable phenomena given off by natural or man-made objects; electromagnetic energy, heat, sound, footprints, fingerprints, and chemical and material residues	Scientific and technical analysis
Records	IMINT, SIGINT, symbolic (written and oral reports, numerical tabulations) or non-symbolic (images, electro-magnetic recordings of data)	Research, background information, translation, conversion to usable form

[36] Jerome K. Clauser and Sandra M. Weir, *Intelligence Research Methodology: An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence* (Washington, DC: Defense Intelligence School, 1975), 111-117.

The following table offers examples from government and business of each source type.

Table 8: Comparison of Illustrative Intelligence Sources from Government and Business

Source: Author

Source	Information Provided	Government	Business
People	Inadvertent or intentional revelation by a person in a casual encounter, official meeting, or informant relationship	A foreign diplomat	A fellow exhibitor at a trade show
Objects	Physical and functional characteristics of the item, discerned through physical or visual examination	Military equipment	Products or components
Emanations	Clues about the identity and activities of the originator	Intercepted communications	Trace chemicals in factory effluent
Records	Evidence of existence and characteristics of target entities	Imagery, telemetry, documents	Product literature

The collection phase of the intelligence process thus involves several steps: translation of the intelligence need into a collection requirement, definition of a collection strategy, selection of collection sources, and information collection. The resultant collected information must often undergo a further conversion before it can yield intelligence in the analysis stage. Processing of collected information into intelligence information is addressed in the following Part of this primer.

PART IV
PROCESSING COLLECTED INFORMATION

From Raw Data to Intelligence Information

No matter what the setting or type of collection, gathered information must be packaged meaningfully before it can be used in the production of intelligence. Processing methods will vary depending on the form of the collected information and its intended use, but they include everything done to make the results of collection efforts usable by intelligence producers. Typically, "processing" applies to the techniques used by government intelligence services to transform raw data from special-source technical collection into intelligence *information*.[37]

> While collectors collect "raw" information, certain [collection] disciplines involve a sort of *pre-analysis* in order to make the information "readable" to the average all-source analyst. For instance: imagery analysts "read-out" the basic information on the image; foreign language broadcasts must be literally translated by linguists and analyzed for linguistic "context"; electronic signals require sorting out to be intelligible to the uninitiated in that arcane art; agent reports also need literal translations and perhaps comments as to access, context, assumed or proven past veracity.[38]

In the private sector, some processing activities are analogous to those of the government. Interpreting and annotating open-source information for a business intelligence service may include: marking locations of interest on a map or photograph, "translating" press releases or technical reports, transcribing the words of a speaker from video or audiotape into text, or drafting a detailed commentary from a personal interview.

Another term for processing, *collation*, encompasses many of the different operations that must be performed on collected information or data before further analysis and intelligence production can occur. More than merely physically manipulating information, collation organizes the information into a usable form, adding meaning where it was not evident in the original. Collation includes gathering, arranging, and annotating related information; drawing tentative conclusions about the relationship of "facts" to each other and their significance; evaluating the accuracy and reliability of each item; grouping items into logical categories; critically examining the information source; and assessing the meaning and usefulness of the content for further analysis. Collation reveals information

---

[37] The Department of Defense defines intelligence information as "unprocessed data of every description which may be used in the production of intelligence." (Department of Defense, Joint Chiefs of Staff, Joint Pub 1-02, *Dictionary of Military and Associated Terms* (Washington, DC: 23 March 1994), 184.)

[38] Dearth, "National Intelligence," 19.

gaps, guides further collection and analysis, and provides a framework for selecting and organizing additional information.[39]

Examples of collation include filing documents, condensing information by categories or relationships, and employing electronic database programs to store, sort, and arrange large quantities of information or data in preconceived or self-generating patterns. Regardless of its form or setting, an effective collation method will have the following attributes:

1. Be impersonal. It should not depend on the memory of one analyst; another person knowledgeable in the subject should be able to carry out the operation.

2. Not become the "master" of the analyst or an end in itself.

3. Be free of bias in integrating the information.

4. Be receptive to new data without extensive alteration of the collating criterion.[40]

Evaluating and Selecting Evidence

To prepare collected information for further use, one must evaluate its relevance and value to the specific problem at hand. An examination of the information's *source* and *applicability* to the intelligence issue can determine whether that information will be further employed in the intelligence production process. Three aspects to consider in evaluating the relevance of information sources are reliability, proximity, and appropriateness.

Reliability of a source is determined through an evaluation of its past performance; if the source proved accurate in the past, then a reasonable estimate of its likely accuracy in a given case can be made. A human source's own testimony of reliability may also be taken into account; qualifiers such as "certain," "believe," and "guess" indicate how sure the source is of the information being conveyed. However, if the source is completely untested, then evaluation of the information must be done solely on its own merits, independent of its origin.[41]

Proximity refers to the source's closeness to the information. The direct observer or participant in an event may gather and present evidence directly, but in the absence of such firsthand information, the analyst must rely on sources with varying degrees of proximity to

---

[39] R.H. Mathams, "The Intelligence Analyst's Notebook," in *Strategic Intelligence: Theory and Application*, eds. Douglas H. Dearth and R. Thomas Goodden, 2d ed. (Washington, DC: Joint Military Intelligence Training Center, 1995), 85-86.

[40] Mathams, 86.

[41] adapted from Gary Harris, "Evaluating Intelligence Evidence," in *A Handbook of Intelligence Analysis*, ed. Ronald D. Garst, 2d ed. (Washington, DC: Defense Intelligence College, January 1989), 34-35. For an in-depth treatment of evidence evaluation techniques and factors, see David A. Schum, *Evidence and Inference for the Intelligence Analyst*, Vols. I and II (Lanham, MD: University Press of America, 1987).

the situation. A primary source passes direct knowledge of an event on to the analyst. A secondary source provides information twice removed from the original event; one observer informs another, who then relays the account to the analyst. Such regression of source proximity may continue indefinitely, and naturally, the more numerous the steps between the information and the source, the greater the opportunity for error or distortion.[42]

Appropriateness of the source rests upon whether the source speaks from a position of authority on the specific issue in question. As no one person or institution is an expert on all matters, the source's individual capabilities and shortcomings affect the level of validity or reliability assigned to the information it provides regarding a given topic.[43]

The following examples illustrate the use of reliability, proximity, and appropriateness to evaluate a source.

> The mail clerk at 3rd Army Headquarters told me that, according to the 1st Armored Division Supply Officer, the Division is being deployed to Site Y in three days.

The reliability of the mail clerk as a source (questionable), his proximity to the information (secondary), and the appropriateness of the Supply Officer as a source on the fact of deployment (uncertain), make this information of little value to the intelligence production process.

> A major national newspaper published an interview with the CEO of Big Company, quoting the CEO's announcement of a merger the company had just secretly concluded with Large Company.

The reliability of a major national newspaper as a source (good), its proximity to the information (secondary), and the appropriateness of the CEO as the source of the merger announcement (high) make this information of high value to intelligence production.

Three aspects of the information itself have a bearing on its applicability to intelligence issues: plausibility, expectability, and support. *Plausibility* refers to whether the information is true under any circumstances or only under certain conditions, either known or possible. *Expectability* is assessed in the context of the analyst's prior knowledge of the subject. *Support* for information exists when another piece of evidence corroborates it — either the same information from a different source, or different information that points to the same conclusion.[44]

For example, a source contends that the President of Country X recently died, but the death is being kept secret from all but a few members of his regime. Although unusual, this information is plausible, and even has precedent in history. The scenario may meet the expectability criterion, if the country or this particular regime is known to be

---

[42] Harris, 35.
[43] adapted from Harris, 36.
[44] adapted from Harris, 36-38.

extremely secretive and paranoid about being vulnerable to hostile internal or external takeover movements. Support for this information may come from the same source providing details on the President's secret burial ceremony, or a different source, such as an actor who was hired to play the part of the President in a false Presidential address televised to the nation.

All these factors of source and content contribute to an initial assessment of the value of a particular piece of information to the intelligence production process. Those pieces that are judged to be useful may then undergo further scrutiny in light of customer needs, while items of questionable value may be rejected or set aside for further processing and comparison with other information. This initial selection of intelligence information sets the stage for intelligence analysis and production, as explained in the following Parts of the primer.

PART V
ANALYSIS

> Analysis is the breaking down of a large problem into a number of smaller problems and performing mental operations on the data in order to arrive at a conclusion or a generalization. It involves close examination of related items of information to determine the extent to which they confirm, supplement, or contradict each other and thus to establish probabilities and relationships.
>
> — *Mathams, 88.*

Analysis is not merely reorganizing data and information into a new format. At the very least, analysis should fully *describe* the phenomenon under study, accounting for as many relevant variables as possible. At the next higher level of analysis, a thorough *explanation* of the phenomenon is obtained, through interpreting the significance and effects of its elements on the whole. Ideally, analysis can reach successfully beyond the descriptive and explanatory levels to synthesis and effective persuasion, often referred to as *estimation*.

The *purpose* of intelligence analysis is to reveal to a specific decisionmaker the underlying significance of selected target information. Frequently intelligence analysis involves estimating the likelihood of one possible outcome, given the many possibilities in a particular scenario. This function is not to be confused with prediction, as no one can honestly be credited with predicting the future. However, intelligence analysis does appropriately involve forecasting, "which requires the explicit statement by the analyst of the degree of confidence held in a certain set of judgments, based upon a certain set of explicit facts or assumptions."[45] Different levels of analysis result in corresponding levels of conclusions that may be traced along an "Intelligence Food Chain."[46] This concept, illustrated in the following table, is equally applicable in government and business intelligence.

Table 9: The Intelligence Food Chain

Source: adapted from Davis, Analytic Tradecraft

Facts	verified information related to an intelligence issue (for example: events, measured characteristics).
Findings	expert knowledge based on organized information that indicates, for example, what is increasing, decreasing, changing, taking on a pattern.
Forecasts	judgments based on facts and findings and defended by sound and clear argumentation.
Fortunetelling	inadequately explained and defended judgments.

[45] Dearth, "National Intelligence," 25.

[46] Adapted from Jack Davis, *Intelligence Changes in Analytic Tradecraft in CIA's Directorate of Intelligence*, (Washington, DC: CIA Directorate of Intelligence, April 1995), 6.

Intelligence analysts may use this Food Chain model to measure their adherence to rigorous analytic thought — how far to go with their analytic judgments, and where to draw the line. The mnemonic "Four Fs Minus One" may serve as a reminder of how to apply this criterion. Whenever the intelligence information allows, and the customer's validated needs demand it, the intelligence analyst will extend the thought process as far along the Food Chain as possible, to the third "F" but not beyond to the fourth.

Types of Reasoning

Objectivity is the intelligence analyst's primary asset in creating intelligence that meets the Four Fs Minus One criterion. More than simply a conscientious attitude, objectivity is "a professional ethic that celebrates tough-mindedness and clarity in applying rules of evidence, inference, and judgment."[47] To produce intelligence objectively, the analyst must employ a process tailored to the nature of the problem. Four basic types of reasoning apply to intelligence analysis: induction, deduction, abduction and the scientific method.

Induction. The induction process is one of discovering relationships among the phenomena under study. For example, an analyst might discover from systematic examination of media reports that Country "X" had been issuing aggressive statements prior to formally announcing an arms agreement with Country "Y." Or an analyst may notice that a characteristic sequence of events always precedes Country "Z's" nuclear weapons tests.[48] In the words of Clauser and Weir:

> Induction is the intellectual process of drawing generalizations on the basis of observations or other evidence. Induction takes place when one learns from experience. For example, induction is the process by which a person learns to associate the color red with heat and heat with pain, and to generalize these associations to new situations.
>
> Induction occurs when one is able to postulate causal relationships. Intelligence estimates are largely the result of inductive processes, and, of course, induction takes place in the formulation of every hypothesis. Unlike other types of intellectual activities such as deductive logic and mathematics, there are no established rules for induction.[49]

Deduction. "Deduction is the process of reasoning from general rules to particular cases. Deduction may also involve drawing out or analyzing premises to form a conclusion."[50] In the case of Country "Z" above, the analyst noted a pattern of events related to testing of nuclear weapons. Later, after noticing this series of events occurring in Country "Z," the analyst may conclude that another nuclear weapons test is about to take place in that coun-

---

[47] Davis, *Analytical Tradecraft,* 5.
[48] Clauser and Weir, 81.
[49] Clauser and Weir, 81.
[50] clauser and Weir, 81.

try. The first premise, that certain events were related to weapons testing, was derived inductively — from specific observations to a conclusion. The second premise, that another test was imminent, was derived deductively — from a generalization to a specific case.[51]

Deduction works best in closed systems such as mathematics, formal logic, or certain kinds of games in which all the rules are clearly spelled out. For example, the validity and truthfulness of the following conclusion is apparent to anyone with a knowledge of geometry: "This is a triangle, therefore the sum of the interior angles will equal 180 degrees." In closed systems, properly drawn deductive conclusions are always valid.[52]

However, intelligence analysis rarely deals with closed systems, so premises assumed to be true may in fact be false, and lead to false conclusions. For example, in the weapons testing case above, Country "Z" may have deliberately deceived potential observers by falsely staging activities similar to those usually taken before a real weapons test. A conclusion that observed activities signalled a real test would be false in this case. Thus, as human activities rarely involve closed systems, deduction must be used carefully in intelligence analysis.[53]

Readers interested in further study into the use of deductive logic in estimative intelligence may wish to read the work of Israeli intelligence analyst Isaac Ben-Israel on this subject.[54] At the Joint Military Intelligence College, one student, Navy Lieutenant Donald Carney, explored the application of deductive logic to intelligence collection and analysis decisions in estimating the disintegration of Yugoslavia. Carney showed that Ben-Israel's "critical method" of inquiry could be applied prospectively to the collection of information to refute specific hypotheses, allowing for an unusually definitive estimate of the likelihood of each outcome.[55]

Abduction. Abduction is the process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. This process differs from induction in that it adds to the set of hypotheses available to the analyst. In inductive reasoning, the hypothesized relationship among pieces of evidence is considered to be already existing, needing only to be perceived and articulated by the analyst. In abduction, the analyst creatively generates an hypothesis, then sets about examining whether the available evidence unequivocally leads to the new conclusion. The latter step, testing the evidence, is a deductive inference.[56]

---

[51] Clauser and Weir, 82-83.

[52] Clauser and Weir, 83.

[53] Clauser and Weir, 83-84.

[54] Isaac Ben-Israel, "Philosophy and Methodology of Intelligence: The Logic of Estimative Process," *Intelligence and National Security 4*, no. 4 (October 1989): 660-718.

[55] LT Donald J. Carney, USN, *Estimating the Dissolution of Yugoslavia*, Seminar Paper (Washington, DC: Joint Military Intelligence College, September 1991).

[56] David A. Schum, *Evidence and Inference for the Intelligence Analyst*, Volume I (Lanham, MD: University Press of America, 1987): 20.

Abductive reasoning may also be called intuition, inspiration, or the "Ah-ha!" experience. It characterizes the analyst's occasional ability to come to a conclusion spontaneously, often without a sense of having consciously taken definable steps to get there. While the abduction process may not be easily defined or taught, it may be encouraged by providing analysts with a wide array of research material and experiences, and by supporting the expenditure of time and energy on creative thinking.[57]

Examples of abductive reasoning in intelligence analysis include situations in which the analyst has a nagging suspicion that something of intelligence value has happened or is about to happen, but has no immediate explanation for this conclusion. The government intelligence analyst may conclude that an obscure rebel faction in a target country is about to stage a political coup, although no overt preparations for the takeover are evident. The business analyst may determine that a competitor company is on the brink of a dramatic shift from its traditional product line into a new market, even though its balance sheet and status in the industry are secure. In each case, the analyst, trusting this sense that the time is right for a significant event, will set out to gather and evaluate evidence in light of the new, improbable, yet tantalizing hypothesis.

Scientific Method. The scientific method combines deductive and inductive reasoning: Induction is used to develop the hypothesis, and deduction is used to test it. In science, the analyst obtains data through direct observation of the subject and formulates an hypothesis to explain conclusions suggested by the evidence. Experiments on the subject are devised and conducted to test the validity of the hypothesis. If the experimental results match the expected outcome, then the hypothesis is validated; if not, then the analyst must develop a new hypothesis and appropriate experimental methods.[58]

In intelligence analysis, the analyst typically does not have direct access to the observable subject, but gathers information indirectly. From these gathered data, the intelligence analyst may proceed with the scientific method by generating tentative explanations for a subject event or phenomenon. Next, each hypothesis is examined for plausibility and compared against newly acquired information, in a continual process toward reaching a conclusion. Often the intelligence analyst tests several hypotheses at the same time, whereas the scientist usually focuses on one at a time. Furthermore, intelligence analysts cannot usually experiment directly upon the subject matter as in science, but must generate fictional scenarios and rigorously test them through mental processes such as those suggested below.[59]

---

[57] The relationship of this type of reasoning to Eastern philosophy is addressed in LCDR William G. Schmidlin, USN, *Zen and the Art of Intelligence Analysis*, MSSI Thesis (Washington, DC: Joint Military Intelligence College, July 1993).

[58] Mathams, 91. A seminal contribution to understanding scientific method is Abraham Kaplan's *The Conduct of Inquiry* (San Francisco, CA: Chandler, 1964). The applicability of this method in social science, and therefore, in intelligence, is developed in Earl Babbie's *The Practice of Social Research* (Belmont, CA: Wadsworth Publishing Co, 1992).

[59] Mathams, 91.

Methods of Analysis

Opportunity Analysis. Opportunity analysis identifies for policy officials opportunities or vulnerabilities that the customer's organization can exploit to advance a policy, as well as dangers that could undermine a policy.[60] It identifies institutions, interest groups, and key leaders in a target country or organization that support the intelligence customer's objective; the means of enhancing supportive elements; challenges to positive elements (which could be diminished or eliminated); logistic, financial, and other vulnerabilities of adversaries; and activities that could be employed to rally resources and support to the objective.[61] Jack Davis notes that in the conduct of opportunity analysis,

> [T]he analyst should start with the assumption that every policy concern can be transformed into a legitimate intelligence concern. What follows from this is that analysts and their managers should learn to think like a policymaker in order to identify the issues on which they can provide utility, but they should always [behave like intelligence producers]. ... The first step in producing effective opportunity analysis is to redefine an intelligence issue in the policymaker's terms. This requires close attention to the policymaker's role as "action officer" - reflecting a preoccupation with getting things started or stopped among adversaries and allies.... It also requires that analysts recognize a policy official's propensity to take risk for gain....[P]olicymakers often see, say, a one-in-five chance of turning a situation around as a sound investment of [organizational] prestige and their professional energies....[A]nalysts have to search for appropriate ways to help the policymaker inch the odds upward - not by distorting their bottom line when required to make a predictive judgment, or by cheerleading, but by pointing to opportunities as well as obstacles. Indeed, on politically sensitive issues, analysts would be well advised to utilize a matrix that first lists and then assesses both the promising and discouraging signs they, as objective observers, see for... policy goals.... [P]roperly executed opportunity analysis stresses information and possibilities rather than [explicit] predictions.[62]

Linchpin Analysis. Linchpin analysis is one way of showing intelligence managers and policy officials alike that all the bases have been touched. Linchpin analysis, a colorful term for structured forecasting, is an *anchoring* tool that seeks to reduce the hazard of self-inflicted intelligence error as well as policymaker misinterpretation. At a minimum, linchpin tradecraft promotes rigor through a series of predrafting checkpoints, outlined below. Analysts can also use it to organize and evaluate their text when addressing issues

---

[60] Jack Davis, *The Challenge of Opportunity Analysis* (Washington, DC: Center for the Study of Intelligence, July 1992), v.

[61] Davis, *Opportunity Analysis*, 7.

[62] Davis, *Opportunity Analysis*, 12-13.

of high uncertainty. Reviewing managers can use — and have used — linchpin standards to ensure that the argument in such assessments is sound and clear.[63]

Table 10: Steps in Linchpin Analysis

Source: Davis, *Analytic Tradecraft*

1. Identify the main uncertain factors or key variables judged likely to drive the outcome of the issue, forcing systematic attention to the range of and relationships among factors at play.
2. Determine the *linchpin* premises or working assumptions about the drivers. This encourages testing of the key subordinate judgments that hold the estimative conclusion together.
3. Marshal findings and reasoning in defense of the linchpins, as the premises that warrant the conclusion are subject to debate as well as error.
4. Address the circumstances under which unexpected developments could occur. What *indicators* or patterns of development could emerge to signal that the linchpins were unreliable? And what *triggers* or dramatic internal and external events could reverse the expected momentum?

Analogy. Analogies depend on the real or presumed similarities between two things. For example, analysts might reason that because two aircraft have many features in common, they may have been designed to perform similar missions. The strength of any such analogy depends upon the strength of the connection between a given condition and a specified result. In addition, the analyst must consider the characteristics that are dissimilar between the phenomena under study. The dissimilarities may be so great that they render the few similarities irrelevant.

> One of the most widely used tools in intelligence analysis is the analogy. Analogies serve as the basis for most hypotheses, and rightly or wrongly, underlie many generalizations about what the other side will do and how they will go about doing it.[64]

Thus, drawing well-considered generalizations is the key to using analogy effectively. When postulating human behavior, the analyst may effectively use analogy by applying it to a specific person acting in a situation similar to one in which his actions are well documented: an election campaign or a treaty negotiation, for example. However, an assumption that a different individual running for the same office or negotiating a similar treaty would behave the same way as his predecessor may be erroneous. The key condition in this analogy is the personality of the individual, not the similar situations. This principle of appropriate comparison applies equally to government and business intelligence analysis.

---

[63] Davis, *Analytic Tradecraft*, 8-9.
[64] Clauser and Weir, 246-248.

> Analogies are used in many different kinds of intelligence analyses from military and political to industrial intelligence. For example, major U.S. auto makers purchase their competitors' models as soon as they appear in the showrooms. The new cars are taken to laboratories where they are completely and methodically disassembled. Reasoning by analogy, that is, assuming that it would cost one producer the same amount to produce or purchase the same components used by another, the major auto producers can estimate their competitors' per-unit production costs, any cost-saving measures taken, and how much profit is likely to be earned by the sale of a single unit.[65]

Customer Focus

As with the previous stages of the intelligence process, effective analysis depends upon a good working relationship between the intelligence customer and producer. A significant difference exists between the public and private sectors with regard to this customer-producer relationship. Government analysts typically benefit from close interaction with policymakers by virtue of their well understood institutional position. The same is not often true in the business world, where the intelligence analyst's role is not yet well institutionalized.

The government intelligence analyst is generally considered a legitimate and necessary policymaking resource, and even fairly junior employees may be accepted as national experts by virtue of the knowledge and analytic talent they offer to high level customers. Conversely, in the private sector, the intelligence analyst's corporate rank is generally orders of magnitude lower than that of a company vice-president or CEO. The individual analyst may have little access to the ultimate customer, and the intelligence service as a whole may receive little favor from a senior echelon that makes little distinction between so-called intelligence and the myriad of other decisionmaking inputs. When private sector practitioners apply validated methods of analysis geared to meet specific customer needs, they can win the same kind of customer appreciation and support as that enjoyed by government practitioners.

Statistical Tools

Additional decisionmaking tools derived from parametric or non-parametric statistical techniques, such as Bayesian analysis, are sometime used in intelligence. An exploration of them is beyond the scope of this study. Many of the statistically oriented tools continue to rely fundamentally on human judgment to assign values to variables, so that close attention to the types of reasoning and methods of analysis presented herein remain the fundamental analytical precondition to their use.[66]

---

[65] Clauser and Weir, 248-250.

[66] Editor's note: A former JMIC faculty member, Douglas E. Hunter, explores the intelligence applications of Bayesian Analysis in *Political/Military Applications of Bayesian Analysis: Methodological Issues* (Boulder, CO: Westview, 1984).

Analytic Mindset

Customer needs and collected information and data are not the only factors that influence the analytic process; the analyst brings his or her own unique thought patterns as well. This personal approach to problem-solving is "the distillation of the intelligence analyst's cumulative factual and conceptual knowledge into a framework for making estimative judgments on a complex subject."[67] Mindset helps intelligence analysts to put a situation into context, providing a frame of reference for examining the subject. Analysis could not take place if thinking were not bounded by such constructs. However, mindset can also lead analysts to apply certain viewpoints inappropriately or exclusively while neglecting other potentially enlightening perspectives on an issue. While no one can truly step outside his or her own mindset, becoming aware of potential analytic pitfalls can enable intelligence analysts to maximize the positive effects of mindset while minimizing the negatives.[68] Analysts can use the accompanying list of analytical pitfalls to determine which, if any, they may be applying in their work, and whether the relevant ones are accounted for in their analytic tasks.

Categories of Misperception and Bias[69]

Evoked-Set Reasoning: That information and concern which dominates one's thinking based on prior experience. One tends to uncritically relate new information to past or current dominant concerns.

Prematurely Formed Views: These spring from a desire for simplicity and stability, and lead to premature closure in the consideration of a problem.

Presumption that Support for One Hypothesis Disconfirms Others: Evidence that is consistent with one's preexisting beliefs is allowed to disconfirm other views. Rapid closure in the consideration of an issue is a problem.

Inappropriate Analogies: Perception that an event is analogous to past events, based on inadequate consideration of concepts or facts, or irrelevant criteria. Bias of "Representativeness."

Superficial Lessons From History: Uncritical analysis of concepts or events, superficial causality, over-generalization of obvious factors, inappropriate extrapolation from past success or failure.

Presumption of Unitary Action by Organizations: Perception that behavior of others is more planned, centralized, and coordinated than it really is. Dismisses accident and chaos. Ignores misperceptions of others. Fundamental attribution error, possibly caused by cultural bias.

---

[67] Jack Davis, "Combatting Mindset," *Studies in Intelligenc*e 35, no. 4 (Winter 1991): 13-18.
[68] Davis, "Combatting Mindset," 13-15.
[69] Excerpted from Dearth, "The Politics of Intelligence," 106-107.

Organizational Parochialism: Selective focus or rigid adherence to prior judgments based on organizational norms or loyalties. Can result from functional specialization. Group-think or stereotypical thinking.

Excessive Secrecy (Compartmentation): Over-narrow reliance on selected evidence. Based on concern for operational security. Narrows consideration of alternative views. Can result from or cause organizational parochialism.

Ethnocentrism: Projection of one's own culture, ideological beliefs, doctrine, or expectations on others. Exaggeration of the causal significance of one's own action. Can lead to mirror-imaging and wishful thinking. Parochialism.

Lack of Empathy: Undeveloped capacity to understand others' perception of their world, their conception of their role in that world, and their definition of their interests. Difference in cognitive contexts.

Mirror-Imaging: Perceiving others as one perceives oneself. Basis is ethnocentrism. Facilitated by closed systems and parochialism.

Ignorance: Lack of knowledge. Can result from prior-limited priorities or lack of curiosity, perhaps based on ethnocentrism, parochialism, denial of reality, rational-actor hypothesis (see next entry).

Rational-Actor Hypothesis: Assumption that others will act in a "rational" manner, based on one's own rational reference. Results from ethnocentrism, mirror-imaging, or ignorance.

Denial of Rationality: Attribution of irrationality to others who are perceived to act outside the bounds of one's own standards of behavior or decisionmaking. Opposite of rational-actor hypothesis. Can result from ignorance, mirror-imaging, parochialism, or ethnocentrism.

Proportionality Bias: Expectation that the adversary will expend efforts proportionate to the ends he seeks. Inference about the intentions of others from costs and consequences of actions they initiate.

Willful Disregard of New Evidence: Rejection of information that conflicts with already-held beliefs. Results from prior policy commitments, and/or excessive pursuit of consistency.

Image and Self-Image: Perception of what has been, is, will be, or should be (image as subset of belief system). Both inward-directed (self-image) and outward-directed (image). Both often influenced by self-absorption and ethnocentrism.

Defensive Avoidance: Refusal to perceive and understand extremely threatening stimuli. Need to avoid painful choices. Leads to wishful thinking.

Overconfidence in Subjective Estimates: Optimistic bias in assessment. Can result from premature or rapid closure of consideration, or ignorance.

Wishful Thinking (Pollyanna Complex): Hyper-credulity. Excessive optimism born of smugness and overconfidence.

Best-Case Analysis: Optimistic assessment based on cognitive predisposition and general beliefs of how others are likely to behave, or in support of personal or organizational interests or policy preferences.

Conservatism in Probability Estimation: In a desire to avoid risk, tendency to avoid estimating extremely high or extremely low probabilities. Routine thinking. Inclination to judge new phenomena in light of past experience, to miss essentially novel situational elements, or failure to reexamine established tenets. Tendency to seek confirmation of prior-held beliefs.

Worst-Case Analysis (Cassandra Complex): Excessive skepticism. Reflects pessimism and extreme caution, based on predilection (cognitive predisposition), adverse past experience, or on support of personal or organizational interests or policy preferences.

Because the biases and misperceptions outlined above can influence analysis, they may also affect the resultant analytic products. As explained in the following Part, analysis does not cease when intelligence production begins; indeed, the two are interdependent. The foregoing overview of analytic pitfalls should caution intelligence managers and analysts that intelligence products should remain as free as possible from such errors of omission and commission, yet still be tailored to the specific needs of customers. Consistently reminding intelligence producers of the dangers and benefits of mindset may help them avoid errors and polish their analytic skills. In addition, managers may conduct post-production evaluation of intelligence products, using the biases and misperceptions listed above to identify strengths and weaknesses in individual analysts' work, and to counsel them accordingly.

PART VI
PRODUCTION

Creating Intelligence

The previously-described steps of the intelligence process are necessary precursors to production, but it is only in this final step that functionality of the whole process is achieved. *Production* results in the creation of intelligence, that is, value-added actionable information tailored to a specific customer. In practical terms, production refers to the creation, in any medium, of either interim or *finished* briefings or reports for other analysts, or for decisionmakers or policy officials. As with elements of analysis developed in Part V, production principles described and explained here may apply to both government and private sector intelligence operations.

In government parlance, the term "finished" intelligence is reserved for products issued by analysts responsible for synthesizing all available sources of intelligence, resulting in a comprehensive assessment of an issue or situation, for use by senior analysts or decisionmakers. Creating finished intelligence for national and military customers is the role of CIA and DIA analysts, respectively. Analysts within an intelligence sub-discipline may also speak of a "finished" product from their point of view, meaning that intelligence from a single source, such as SIGINT, was interpreted as fully as possible in light of all other available intelligence from that source, plus any relevant published intelligence from other sources, and open source information. Analysts within the single-source intelligence agencies consider any information or intelligence not issued by their own organization to be "collateral."

Similar designations for finished intelligence products may apply in the business world. Particularly in large corporations with multidisciplinary intelligence units, or in business intelligence consulting firms, some production personnel may specialize in the creation of intelligence from a single source, while others specialize in finished reporting. For example, there may be specialists in library and on-line research, "HUMINT" experts who conduct interviews and attend conferences and trade shows, or scientists who perform experiments on products or materials. The reports generated by such personnel may be considered finished intelligence by their intended customers within subdivisions of the larger company. The marketing, product development, or public relations department of a corporation may consume single-source intelligence products designed to meet their individual needs. Such a large corporation may also have an intelligence synthesis unit that merges the reports from the specialized units into finished intelligence for use in strategic planning by senior decisionmakers. Similarly, in the intelligence consulting firm, each of the specialized production units may contribute their reports to a centralized finished intelligence unit which generates a synthesized product for the client.

Emphasizing the Customer's Bottom Line

The intelligence report or presentation must focus on the *results* of the analysis and make evident their significance through sound arguments geared to the customer's interests. In short, intelligence producers must BLUF their way through the presentation — that is, they must keep the "Bottom Line Up Front." This axiom applies not only to written expression, but also to oral briefings, or any other medium of expression used in the intelligence environment of government or business.

> It is often difficult for... intelligence [producers] to avoid the temptation to succumb to the Agatha Christie Syndrome. Like the great mystery writer, we want to keep our readers in suspense until we can deliver that "punch line." After we have worked hard on this analysis... we want the reader to know all the wonderful facts and analytical methods that have gone into our conclusions.... Most readers really will not care about all those bells and whistles that went into the analysis. ***They want the bottom line***, and that is what intelligence professionals are paid to deliver.[70]

Knowing the customer enables the producer to generate intelligence that highlights the bottom line. Some customers are "big picture" thinkers, seeking a general overview of the issue, and guidance on the implications for their own position and responsibilities. An appropriate intelligence product for such a customer will be clear, concise, conclusive, and free of jargon or distracting detail.[71] Conversely, some customers are detail-oriented, seeing themselves as the ultimate expert on the subject area. This type of customer needs highly detailed and specialized intelligence to supplement and amplify known information. The broad-brush approach to intelligence will not only miss the mark with this customer, but may actually be perceived as an insult, lessening the chances that future products by the offending producer will be accepted or used.[72] Producers should therefore tailor both the content and delivery of the intelligence to the customer. The following section provides guidelines for creating intelligence products that meet customer needs.[73]

Anatomy of an Intelligence Product

Whether it is produced within the government, or in the business setting, the basic nature of the intelligence product remains the same. The analyst creates a product to document ongoing research, give the customer an update on a current issue or situation, or

---

[70] James S. Major, *The Style Guide: Research and Writing at the Joint Military Intelligence College*, (Washington DC: Joint Military Intelligence College, August 1994): 345.

[71] Mathams, 88.

[72] Davis, *Analytic Tradecraft*, 7.

[73] The Central Intelligence Agency has published an unclassified collection of essays on techniques for producing finished national security intelligence. The purpose of the collection is to document best practices, and to reach out to academia and the public. Its title emphasizes the instrumentality of analysis to production. See Central Intelligence Agency, *A Compendium of Analytic Tradecraft Notes*, (Washington, DC, Directorate of Intelligence: February 1997).

provide an estimate of expected target activity. In general terms, the product's function is to cover one or more subject areas, or to be used by the customer for a particular application. Along with these aspects, additional dimensions of the intelligence product are summarized in the table below. They are more fully described in the following paragraphs.

Table 11: Dimensions of an Intelligence Product

Source: Author

Dimension Category	Dimension	Examples
Content	Subject	Biographical, economic, geographic, military, political, science and technology, sociology, transportation and communications
	Intended Use	Research, current, estimative, operational, science and technology, warning
Features	Timeliness	Short-/long-term, opportune, routine/priority
	Periodicity	Ad hoc/scheduled; analyst/customer-initiated
	Scope	Narrow/broad; detailed/summary; basic/exhaustive
Packaging	Medium	Hard/softcopy, written/oral, video
	Format	Formal/informal, textual/graphical
Customer	Relationship to producer	Intended/incidental recipient; internal/external; novice/expert
	Distribution method	Internal/external; direct/indirect; focused/broad

Content

Determination of product content is done in close cooperation with the customer, sometimes at the initiative of one or the other, often in a cycle of give-and-take of ideas. Formal intelligence requirements, agreed upon by both producer and customer in advance, do drive the production process, but the converse is also true. The intelligence unit's own self-concept and procedures influence its choice of which topics to cover, and which aspects to emphasize. As a result, the customer comes to expect a certain type of product from that unit, and adjusts requirement statements accordingly. In addition, the intelligence process may bring to light aspects of the target that neither the producer nor customer anticipated. When the parties involved have a close working relationship, either

one may receive inspiration from interim products, and take the lead in pursuing new ways to exploit the target.[74]

Often, this dialogue centers around the pursuit of new sources associated with known lucrative sources. Examples from government include HUMINT targeting of persons identified in SIGINT as having access to foreign leaders, and SIGINT targeting of communications equipment revealed in IMINT of a foreign military installation. Parallel business examples might include intelligence personnel following leads to new sources revealed in original research or a published report: A pharmaceutical industry analyst who reads a business intelligence report about current breast cancer treatments may then investigate how to access human and documentary sources mentioned in the report, for further information on new drug therapy options for the disease.

The basic orientation of the intelligence product toward a particular subject or application is also determined by the producer-customer relationship. Frequently, the intelligence service will organize the production process and its output to mirror the customer organization. Government production by the single-source intelligence agencies is largely organized geographically or topically, to meet the needs of all-source country, region, or topic analysts in the finished-intelligence producing agencies, such as DIA or the National Counterintelligence Center. In the private sector, some intelligence consultant firms are specializing in one subject area, and gearing all production to one customer set, such as the petroleum industry.

In terms of intended use by the customer, both business and government producers may generate intelligence to be applied in the current, estimative, operational, research, science and technology, or warning context. Serendipity plays a role here, because the collected and analyzed information may meet any or all of these criteria. A good example is warning intelligence. Military and political analysts are always alert for target indications that an emergency, such as outbreak of war, or a political coup, is imminent. Standing procedures dictate that routine operations switch to warning mode in this case, so that time-sensitive intelligence on the situation can be issued to all relevant customers. Business intelligence analysts may also find themselves in the warning role unexpectedly, when they make discoveries that have significant time-sensitive implications for customer decisions and actions.

Features

Three key features of the intelligence product are timeliness, scope, and periodicity. Timeliness includes not only the amount of time required to deliver the product, but also the usefulness of the product to the customer at a given moment. Scope involves the level of detail or comprehensiveness of the material contained in the product. Periodicity describes the schedule of product initiation and generation.

---

[74] Turner, 314-320.

In intelligence production, the adage "timing is everything" is particularly apt. When a customer requests specific support, and when actionable information is discovered through collection and analysis, the resultant intelligence product is irrelevant unless the customer receives it in time to take action — by adapting to or influencing the target entity. Timeliness therefore encompasses the short-term or long-term duration of the production process, and the degree to which the intelligence itself proves opportune for the customer. In addition, the relative priority of the intelligence contained in the product affects the timeliness calculus. For example, a business intelligence analyst conducting research for a consumer electronics corporation may produce short-term routine reports as new information becomes available. A long-term routine summary report may be the final output from this project. However, a short-term priority report may result at any time, if time-sensitive information on competitor capabilities or intentions comes to light.

The scope of an intelligence product describes both the amount of material it contains and the depth of coverage it provides on the topic. Its focus may be narrow or broad, and the content may be detailed or in summary form. The level of coverage may be basic or exhaustive. All of these aspects are determined by the customer's needs, and by the amount and extent of the source material available.

> The amount of detail distributed will depend on the circumstances and the requirements of the user. Time constraints often will determine how much detail is given. There may be such a wealth of detail on a particular subject that an analyst might spend a month or more making a detailed analysis, but the urgency of the need for the intelligence may be such as to make a brief survey, produced in two days, much more valuable. It is important to remember that many users of intelligence have neither the time nor the patience to read through a voluminous study, however excellent it may be, and would much prefer to have the essential elements of the analysis set down in a few succinct paragraphs. Some users, however, do require detail, and when that is the case it should be provided in a usable form.[75]

Periodicity is also linked to validated customer requirements. Intelligence products correspond to requirements that specify responsiveness criteria, thus production may occur on an *ad hoc* basis or on a schedule. Analysts may proactively generate products to meet known needs of specific customers, or they may respond to spontaneous customer requests for tailored intelligence. Furthermore, "analysts, as experts in their fields, are expected to initiate studies that address questions yet unformulated by [customers]."[76] By selecting from available source material, and determining when to issue an intelligence product, analysts have the potential to influence how their customers use intelligence to make policy decisions.[77] In the government, topic experts may become close advisors to National Intelligence Officers or directly to senior policymakers. In

[75] Mathams, 92.
[76] Turner, 319.
[77] Turner, 320.

the business world, a sharp intelligence analyst might be responsible for a dramatic change in a retail company's focus, by identifying emerging consumer trends and sensitizing management for the need to reorient the company. To effect this change, the company would become dependent on intelligence about competitors in the same industry. For example, an analyst's assessment of consumer interest in buying natural pet foods might stimulate requirements for further studies, and might lead a manufacturer to change its products to meet consumer demand, before another company captures that market.

Packaging

Government intelligence products are typically packaged as highly structured written and oral presentations, including electrical messages, hardcopy reports, and briefings.[78] Many organizations also generate video intelligence products, especially in the form of live daily "newscasts," or canned documentary presentations. However, the production landscape is being transformed by technology, and today, a wide range of options is available to both business and government. Modern telecommunications and software make possible a whole new world of intelligence production, in which all the players, including customers, are in constant interaction. The Department of Defense, for example, has devised the Joint Intelligence Virtual Architecture (JIVA) concept to accelerate and streamline the entire intelligence process. Under JIVA, intelligence personnel will use advanced communication and analysis tools to electronically collaborate with each other and their customers, resulting in improved timeliness and customization of Defense intelligence products.[79] Part of the JIVA concept is the use of on-line product modules that can stand alone as finished intelligence, or be synergistically combined with other modules for use by interim or ultimate customers.[80] Similar collaborative production techniques may be successful in large business intelligence units with geographically dispersed personnel and customers. However, the benefits offered by modern intelligence practices such as JIVA also present significant challenges, including the financial and political investment in new infrastructure, and the legal implications of the required cooperation between the government and technology firms.[81]

The format of the intelligence product, regardless of the medium used to convey it, affects how well it is received by the customer. Even in a multimedia presentation, the personal touch can make a positive difference. Therefore, the degree of formality, and the mix of textual and graphical material should match the customer's preferences. Some cus-

---

[78] A guide to orally presenting intelligence is found in James S. Major, *Briefing with Intelligence*, (Washington DC: Joint Military Intelligence College, August 1997).

[79] Defense Intelligence Agency, *Vector 21, A Strategic Plan for the Defense Intelligence Agency* (Washington, DC: Programs and Operations Staff, undated), 20.

[80] Louis E. Andre, "Intelligence Production: Towards a Knowledge-Based Future," *Defense Intelligence Journal* 6, no. 2 (Fall 1997): 41.

[81] William O. Studeman, "Leading Intelligence Along the Byways of Our Future: Acquiring C^4ISR Architectures for the 21st Century," *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 52.

tomers want formal briefings, while others enjoy conversational give and take; some want a scheduled meeting, others want the analyst to be available at any time for impromptu consultation. Often, verbally oriented customers request one-on-one exchanges during official travel in automobiles or in airplanes. Conversely, the visually oriented customer may prefer video clips, graphs, charts, and photographs, accompanied by brief amplifying text. Many customers prefer written analyses, often in the form of concise executive summaries or point papers; some will ask for an in-depth study after consuming the initial or periodic assessment. However, producers should be aware of the potential pitfalls of relying on the executive summary to reach key customers. If the product does not appeal to the executive's staff members who read it first, it may never reach the intended recipient.[82]

Customer

In addition to understanding the customer's intelligence requirements, the producer may benefit from an awareness of the relationship between the customer organization and the intelligence service itself. Status issues between the two parties may influence the tone of the intelligence product. Aspects of the producer-customer relationship include whether the recipient is the intended or incidental customer, whether the customer is internal or external to the intelligence service, and whether the parties differ in their level of subject matter knowledge.

The intelligence producer selects the product content and format to suit a specific individual or customer set. However, the producer should beware of selecting material or phraseology that is too esoteric or personal for a potential wide audience. Intelligence products are official publications that become official records for use by all authorized personnel within the producer and customer organizations. They should focus on the primary customer's needs, yet address the interests of other legitimate players. Sometimes, when the producer is struggling with how to meet the needs of both internal and external customers, the solution is to create two different types of products, one for each type of customer. Internal products contain details about the sources and methods used to generate the intelligence, while external products emphasize actionable target information. Similarly, the producer adjusts the product content and tone to the customer's level of expertise. For example, a SIGINT producer may issue a highly technical and detailed product for fellow SIGINT service members, but for intelligence producers in a different agency, a less technical but still producer-oriented product may be appropriate. Similarly, the business intelligence producer within a marketing department may generate a highly specialized report for the head of the department, but may issue an executive summary for the company president.

Selection of the distribution method for the product is also closely tied to the relationship between producer and customer. The ability to deliver specific types of products to internal and external customers depends upon available infrastructure and

---

[82] Loch K. Johnson, *America's Secret Power, The CIA in a Democratic Society,* (New York: Oxford University Press, 1989): 98.

resources (telecommunications lines, transportation, media equipment). Politics affect whether intelligence can be delivered by the individual analyst directly to the customer, or only through a chain of command. Finally, the number of designated recipients is often determined by the sensitivity of the intelligence issue covered in the product. If the intelligence is highly sensitive, such as a report on threats to the president's life, then only the few involved persons (the president and a few key security personnel) will receive the report. A routine report may be broadly distributed to a large customer set. Thus, the choice of distribution method is more a marketing decision than a mechanical exercise.[83] Successful delivery of a truly useful intelligence product to a receptive customer is the result of communication and cooperation among all the players.

Customer Feedback and Production Evaluation

The production phase of the intelligence process does not end with delivering the product to the customer. Rather, it continues in the same manner in which it began: with dialogue between producer and customer.

> If the product is really to be useful for policy-making and command, dissemination involves feedback, which is part of the marketing function.... Ideally, the "marketer" who delivers the product is the same individual who accepts and helps to refine the initial requirement.[84]

Intelligence producers need feedback from end-users. If producers do not learn what is useful and not useful to customers, they cannot create genuine intelligence. Internal review procedures that focus on the format and style of intelligence products are not sufficient for producers to judge their performance; they must hear from customers on the intelligence value of their work. Then producers can modify their practices to further develop those activities that served the customer well, and improve or eliminate those that did not.

Feedback procedures between producers and customers should include key questions, such as: Is the product usable? Is it timely? Was it in fact used? Did the product meet expectations? If not, why not? What next? The answers to these questions will lead to refined production, greater use of intelligence by decisionmakers, and further feedback sessions. Thus, production of intelligence actually generates more requirements in this iterative process.[85] Producers and managers may use the framework developed by Brei and summarized below as an initial checklist for evaluating their own work, and as a basis for formal customer surveys to obtain constructive feedback.

Producers also need performance feedback from their own managers. Useful aspects of such an internal evaluation may include whether the output met the conditions set down by customers and producers in formal intelligence requirements, whether the intel-

---

[83] Johnson, 97.
[84] Dearth, "National Intelligence," 20.
[85] Dearth, "National Intelligence," 20.

ligence was indeed used by customers, and whether the product resulted from a high standard of analytic quality.[86] To establish a formal internal review process for monitoring the quality of analysis in intelligence products, managers could select experienced analysts to serve on a rotating basis as "mindset coaches" — reviewing assessments for issues of mindset, uncertainty, and policy utility, or consider pairing with another production division to swap personnel for this activity. As a rule, the less the critical reader knows about the substance of the paper the more he or she will concentrate on the quality of the argumentation. A reward for the best "mindset coaches" would be to make them branch chiefs.[87]

Table 12: A Framework for Intelligence Product Evaluation and Customer Feedback

Source: adapted from Brei

Accuracy: Were all sources and data free of technical error, misperception, and hostile efforts to mislead?

Objectivity: Were all judgments free of deliberate distortions and manipulations due to self-interest?

Usability: Was all production issued in a form that facilitated ready comprehension and immediate application? Were products compatible with the customer's capabilities for receiving, manipulating, protecting, and storing the product?

Relevance: Was information selected and organized for its applicability to a customer's requirements, with potential consequences and significance of the information made explicit to the customer's circumstances?

Readiness: Are intelligence systems responsive to the existing and contingent intelligence requirements of customers at all levels of command?

Timeliness: Was intelligence delivered while the content was still actionable under the customer's circumstances?

Management's role extends beyond fostering quality production, to bearing responsibility for organizing and administering the complete intelligence process. Managers make key decisions that mirror the intelligence process and make production possible. In conjunction with customers, managers determine what customer set the intelligence unit will serve; what sources it will exploit; what types of intelligence it will produce; and what methods of collection, processing, analysis, production, customer feedback, and self-evaluation it will use. The following Part of this primer explores best practices in managing the intelligence process.

[86] Arthur S. Hulnick, "Managing Intelligence Analysis," 338.
[87] Davis, "Mindset," 17.

PART VII
MANAGING THE INTELLIGENCE PROCESS

The Role of Management

> Another discipline integral to the intelligence profession — but worthy of special consideration in this context — is that of management. The effective administration and direction of intelligence activities can be regarded as the epitome of intelligence professionalism. Just as an untutored civilian cannot be expected competently to command [a military unit], so an untrained or inexperienced layperson cannot be expected effectively to direct [an intelligence operation]. But mastery of professional intelligence skills does not, in itself, ensure that a person is able to direct intelligence functions competently; expertise in administrative techniques and behavioral skills is also essential to managerial effectiveness. Some facility in these areas can be acquired through experience, but a professional level of competence requires familiarity with the principles and theories of management, and leadership.[88]

Moreover, supervisors and managers have a particular responsibility for ensuring the professional development of their subordinates. When all the members of the intelligence unit are competent, then the effectiveness of the group increases. Enabling subordinates also frees managers to thoroughly plan and administer the intelligence operation, instead of redoing the work of production personnel. Meanwhile, managers may continue to broaden their own knowledge of the intelligence process and its customer-service mission.[89]

Organizing the Intelligence Service

In the national Intelligence Community, federal laws form the basis for a centrally coordinated but functionally organized system. The Director of Central Intelligence (DCI) leads the community with the aid of the National Intelligence Council (NIC). Members of the NIC come from all the intelligence agencies plus academia and the private sector. The

---

[88] George Allen, "The Professionalization of Intelligence," in Dearth and Goodden, 1995, 37. Informed debate on the realities of analysts' and managers' intelligence responsibilities toward customers is ongoing in the *International Journal of Intelligence and CounterIntelligence.* Examples of this literature are: Michael A. Turner, "Setting Analytical Priorities in U.S. Intelligence," 9, no. 3 (Fall 1996): 313-327; H. Bradford Westerfield, "Inside Ivory Bunkers: CIA Analysts Resist Managers' "Pandering" Part I, 9, no. 4 (Winter 1996/97): 407-424; and H. Bradford Westerfield, "Inside Ivory Bunkers: CIA Analysts Resist Managers' "Pandering" Part II, 10, no. 1 (Spring 1997): 19-54.

[89] Russell G. Swenson, *An Office Manager's Guide to Intelligence Readiness,* Occasional Paper Number Three (Washington, DC: JMIC, December 1996), 3-5.

NIC manages the national Intelligence Needs Process and supervises the production of National Intelligence Estimates for senior policymakers. Other senior bodies advise or assist the DCI in matters of policy, resource management, performance review, coordination of elements, customer relations, and intra-community relations.[90] Four topical intelligence centers staffed by multiple agencies coordinate intelligence production for policymakers in the key areas of Counterterrorism, Counterintelligence, Counternarcotics, and Nonproliferation.[91] Crisis situations may spark the formation of a temporary special task force, integrating intelligence functions that are usually separate. Although the national Intelligence Community is centrally coordinated, each member organization develops some self-determined policies and procedures, and engages in competitive analysis with respect to the other organizations.

The unifying principle across government intelligence missions is the basic charter to monitor and manage threats to national interests and to the intelligence service itself. In both the national Intelligence Community and the business community, managers may make a distinction between self-protective intelligence activities and competitive intelligence activities. Self-protection involves gathering and analyzing data about threats to public, personal, or multinational mission members' security, whereas competitive activities involve gathering and analyzing data about adversary organizations or countries. In business, the two functions are sometimes undertaken by entirely different companies or groups within the same company.[92] Government subordinates both functions within the intelligence infrastructure.

Table 13: Three Contexts for Government and Business Intelligence Tasks

Source: Author and Editor

Contexts:	**Individual**	**Corporate**	**Global**
Government Tasks:	Diplomatic Security/ Force Protection	Foreign Capabilities Assessment	Strategic Warning from Intelligence
Business Tasks:	Threat Analysis, Personal Risk Analysis	Business/Competitive Intelligence	Business Scenario Planning

Threat analysis in the business environment depends on the open exchange of information between companies, as it is widely recognized that no one benefits from other companies encountering unnecessary risk or danger to their personnel. On the other hand, at the corporate level, competitive business intelligence relies on the protection or discovery of important corporate data. In the public security environment, diplomatic security and

[90] CIA, *Consumer's Guide*, 2-3.

[91] Davis, *Opportunity Analysis*, 8.

[92] Jonathan Tetzlaff, Area Director, Security Research and Analysis, Amoco Corporation, personal correspondence with editor, 24 October 1997.

force protection for a government's own citizens, and for personnel in multilateral operations, is in the best interests of all. Conversely, foreign capabilities assessment operates in the context of a zero-sum game among countries, with potential winners and losers of the tactical advantage.

When the very survival of a corporation or country is at stake vis-a-vis other players in their respective environments, a global or strategic model applies. At this level, strategic warning intelligence takes center stage in the government security setting, and its counterpart — strategic scenario planning — achieves value in the private sector. Scenario planning has been used advantageously by some companies. The Shell Oil Company, for example, used scenario planning to justify disinvestment in oil exploitation infrastructure prior to the worldwide fall in oil demand in the 1980s. The company rose from 14th to 2nd place among oil multinationals, as overinvested companies lost billions.[93] The alternative to taking global or strategic intelligence action is to allow threats to emerge and to bring company or government officials to the realm of crisis management. There, fundamental government or business interests are at stake, and the outcome is more likely to be left to the vagaries of impulse and chance than to the considered judgment and actions of corporate or government leaders.

Private sector intelligence services can consider which elements of the national intelligence model may apply in their own domain. Will the organization require central coordination of diverse elements as the national system does, or might the intelligence unit more closely resemble a single collector or producer agency with a simpler management structure? Will an advisory group mediate between intelligence producers and customers, and does the intelligence service require its own staff to coordinate operations? Will the service be organized functionally into collection and production elements, or perhaps topically? Is

---

[93] Robbie E. Davis-Floyd, "Storytelling Corporate Futures: The Shell Scenarios," *International Journal of Futures Studies* 1 (1995-1997), on-line at http://www.systems.org/HTML/journals.htm, accessed 3 December 1997. The purpose of scenario planning is to force business managers and executives to face future uncertainties squarely by elaborating and evaluating the likelihood and impact of alternative hypothetical business environments. Dissenters are valued, rather than avoided, and, as in government intelligence channels, information is proactively developed to champion and refute the various scenarios as "controllable" pathways to the future. Recent reviews of business scenario planning include Kathy Moyer, "Scenario Planning at British Airways — A Case Study," *Long Range Planning* 29, No. 2 (April 1996): 172-181; Francoise Hecht, "The Aha! Factor," *Director* 50, No. 12 (July 1997): 59; and Ian Smith, "Avoiding Future Shock," *Director* 50, No. 12 (July 1997): 56-59.

A seminal work on the analytical environment for strategic warning in government intelligence is Ephraim Kam, *Surprise Attack* (Cambridge, MA: Harvard University Press, 1988). Although Kam focuses on military attack scenarios, the arena for strategic warning in government intelligence work has expanded as international security concerns shift toward economic competition and away from military confrontation. The convergence of economics and security signals a need for benchmarking the intelligence process, and could presage an era of greater collaboration between cells of intelligence analysts and policymakers at the highest levels, not unlike the give and take that characterizes successful business scenario planning.

the intelligence service an independent organization with external customers, or does it operate within a parent organization? If the latter, does each department, such as Marketing, Planning, or Research require its own tailored intelligence support? Does the chief executive require a centralized intelligence service, by whatever name, to assist in corporate policy-making? Should the service develop contingency plans for providing time-sensitive support in a crisis situation? On a larger scale, should intelligence services within an industry pool their resources for mutual benefit in a crisis environment, or to proactively adapt to a changing environment, as does the national Intelligence Community? The answers to these questions may help private sector intelligence organizations determine how closely to pattern their structure after that of the national intelligence system.

Managing Analysis and Production

Intelligence managers in government and industry need to decide how to organize the production process just as they need to determine the structure of the intelligence service as a whole. Typical methods of assigning analysts are by target function, geographical region, technical subject, or policy issue. The intelligence service may task analysts to concentrate on one type of source information, or to merge all available sources to produce "finished" intelligence or estimates. Some industries will need analysts to specialize in certain technical subject areas or complex issues, while large corporations may assign intelligence analysts to each of several departments such as Research or Product Development. Small independent intelligence services may require personnel to perform all the functions of the intelligence process from needs assessment to production and performance evaluation. In that case, analysts might be assigned to a particular customer account rather than a specific topic area. Part VIII of this primer presents findings on the attributes of intelligence analysts that may prove useful in determining how to allocate human resources in the intelligence production process.

> Some characterizations of the analytic mission...seem to emphasize serving the policymaking process as an abstraction: to tell it like it is, to level the playing field, to keep the policymakers honest, to be right on the record.... But excessive adherence to these attributes can cause overproduction of assessments that feature what analysts think policy officials should want to know, and underproduction of assessments featuring what officials think they need from...analytic specialists.... To provide the requisite benefits for policymakers, the analytic assessments of the intelligence production unit have to deliver a high order of understanding and insight that can support sound decisionmaking. One should avoid a definition of effective analysis that emphasizes accurate prediction...or one that centers on whether or not a policy worked.[94]

> Furthermore, managers can take the initiative in transforming intelligence into a proactive service. Managers who are isolated from the intelligence customer tend to monitor the quantity of reports produced and level of polish in intelligence products, but not the utility of the intelligence itself.[95]

---

[94] Davis, *Opportunity Analysis*, 2-3.
[95] Davis, *Opportunity Analysis*, 10.

> But policy officials will seek information and judgment from the source that provides it at the lowest personal cost, including the mass media, no matter how much money the intelligence organization is spending to fund analysis on their behalf. Thus, managers need to learn to ask for and accept opportunity analysis included in intelligence products, not remove it as inappropriate during the review process. One way to ensure that analysts produce truly useful intelligence is for managers to take an inventory, say twice per year, of the specific professional interests of their key [customers]. Policy officials are more comfortable thinking in terms of outputs than of inputs. Thus, the inventory should be couched in terms of the policymakers' objectives — their hopes and fears — and not in terms of their "intelligence priorities."... The intelligence manager should then take responsibility for converting the inventory into signals for the restructuring of collection, research, and analytic production.[96]

Evaluating the Intelligence Process

Beyond organizing and monitoring intelligence production, an additional management responsibility is to evaluate the intelligence service's overall mission performance. From the manager's perspective, intelligence products are not the only output from the intelligence process; therefore, products are not the only focus of rigorous self-evaluation. In the course of its operations, the intelligence unit expends and generates significant amounts of financial and political capital. Careful examination of this commodity flow may yield key insights into process improvement. Internal review procedures may thus include measures of how well the intelligence service and its components organize their work, use funds, allocate materiel and human resources, and coordinate with parent and customer organizations, all from the self-interested perspective of the intelligence service itself. To assist them in this effort, managers may evaluate the sub-processes and interim products of the Needs Definition, Collection, Processing, Analysis, and Production phases of the intelligence process in terms of Brei's Intelligence Values: Accuracy, Objectivity, Usability, Relevance, Readiness, and Timeliness.

Furthermore, to put a human face on intelligence process, conscientious managers may wish to include in their internal review a frank analysis of their own personnel management record. Perhaps a new definition of "customer" is in order for carrying out this aspect of intelligence evaluation. Seeing the members of the intelligence service as customers of management, and of each other, can enable managers to create a work culture in which each person's needs and talents are respected and incorporated into the organization's mission. By subscribing to the philosophy that a happy workforce is a productive workforce, managers may also achieve the organizational goal of satisfying external customer requirements. With this purpose in mind, principles for matching intelligence personnel to appropriate job assignments are discussed in the next Part of this primer.

---

[96] Davis, *Opportunity Analysis*, 6.

PART VIII
PORTRAIT OF AN INTELLIGENCE ANALYST

The efficacy of the intelligence process described in the foregoing chapters depends upon personnel who are both able and willing to do the specialized work required. Through the findings of several government studies, this section presents the ideal characteristics of the central figure in value-added production — the intelligence analyst. According to these studies, the successful intelligence analyst brings to the discipline certain requisite knowledges and abilities, or has a high aptitude for acquiring them through specialized training; is able to perform the specific tasks associated with the job; and exhibits personality traits compatible with intelligence analysis work. This profile will remain valid in any setting modeled after the national security intelligence system.

The cognitive, performance and personality attributes of the intelligence analyst are explained below. Readers are encouraged to apply this information in accordance with their own particular circumstances. For example:

> Incumbents and individuals considering employment in intelligence analysis may deepen their self-awareness and assess their potential for success and satisfaction in this profession.
>
> Educators and recruiters may identify and prepare candidates for employment in intelligence analysis.
>
> Managers and supervisors may make enlightened decisions about selection, placement, tasking and evaluation of intelligence analysis personnel.

Cognitive Attributes

An individual's analytic skill results from a combination of innate qualities, acquired experience, and relevant education. Psychologists call these mental faculties cognitive attributes, and further divide them into two types: abilities (behavioral traits, being able to perform a task) and knowledges (learned information about a specific subject).[97] Whereas an individual's cognitive abilities are relatively fixed by the time he or she enters the job market, knowledges are situation-specific and can be acquired through training.[98]

According to a recent formal job analysis of selected intelligence analysts conducted by the NSA Office of Human Resources Services, important cognitive abilities for intelligence analysis include written expression, reading comprehension, inductive reasoning, deductive reasoning, pattern recognition, oral comprehension, and information

---

[97] Mark H. Haucke, Industrial Psychologist, NSA, interview with the author, 25 May 1995.
[98] Melissie C. Rumizen, Benchmarking Manager, NSA, interview with the author, 5 July 1996.

ordering.[99] Furthermore, both junior analysts and experienced analysts or supervisors agree that high levels of these abilities are necessary for performing the intelligence analysis job. The abilities are defined in the box below.

Cognitive Abilities Required of Intelligence Analysts[100]

Written Expression: The ability to use words and sentences in writing so others will understand. Involves knowledge of the meanings and distinctions among words, knowledge of grammar, and the ability to organize sentences and paragraphs.

Reading Comprehension: The ability to read and understand written sentences and paragraphs.

Inductive Reasoning: The ability to combine separate pieces of information, or specific answers to problems, to form general rules or conclusions. Involves the ability to think of possible reasons why things go together. Also includes coming up with a logical explanation for a series of events that seem unrelated.

Deductive Reasoning: The ability to apply general rules to specific problems to come up with a logical resolution. Involves deciding if the resolution makes sense.

Pattern Recognition: The ability to identify or detect a known pattern (a figure, word, or object) that is hidden in other material.

Oral Comprehension: The ability to listen and understand spoken words and sentences.

Information Ordering: The ability to follow a rule or set of rules in order to arrange things or actions in a meaningful order. The rule or set of rules to be used must already be given. The things or actions to be put in order can include numbers, letters, words, pictures, procedures, sentences, and mathematical or logical operations.

One set of junior analysts and another of supervisors were separately asked to judge the importance of each of these abilities in performing the intelligence analysis job (see Table 14). Junior analysts assign greater importance to two abilities (written expression and inductive reasoning), but significantly less importance to pattern recognition, than do their supervisors. These results have implications for staffing the intelligence analysis job in both the government and private sector. For example, if junior analysts place greater importance on written expression than their supervisors do, they may be frustrated to receive less training, tasking and recognition than needed for this aspect of their job. The discrepancies in the rankings among the five abilities judged most important by the two groups can be addressed individually by managers. However, the rankings provide some useful generalizations for identifying cognitive attributes applicable to any intelligence environment. In the case of the National Security Agency, the results presented here led

[99] Data were generated by Mark H. Haucke, Industrial Psychologist, using a Management Research Institute (MRI) survey instrument presented in *Ability and Knowledge Requirements* (Bethesda, MD: MRI, 1994).

[100] Adapted from MRI, *Ability and Knowledge Requirements.*

psychologists to design a job-relevant pre-employment aptitude exam for intelligence analysts.

Table 14: Comparative Ranking of Cognitive Abilities Thought to Be Required for Intelligence Analysis

(The lower the number on the 1 to 5 scale, the higher the perceived importance of the ability)

Source: Author and Haucke Study

Cognitive Ability	GROUP 1 (23 Junior Analysts - less than 7 years experience)	GROUP 2 (18 Supervisors — older generation; Ave. Years experience: 19)
Written Expression	1	3
Reading Comprehension	2	1
Inductive Reasoning	2	3
Deductive Reasoning	3	2
Pattern Recognition	3	1
Oral Comprehension	4	4
Information Ordering	5	4

Unlike the abilities categories, areas of knowledge for government intelligence specialists do not necessarily apply to their private sector counterparts. The formal job study of government intelligence analysts revealed that knowledge of military-related and technical subjects, not surprisingly, was prevalent among the individuals in the research group.[101] However, in either public or private sectors, managers can hire and train personnel to apply the requisite knowledges in a given job. A next logical step is to define the components of the intelligence analysis job, to be able to plan and assess individual job performance.

Performance Factors

Even as the analysis described above examined cognitive inputs to the job, a related performance review project, also at NSA, described intelligence analysts' output on the job. As part of this review, supervisors of intelligence analysts placed their subordinates' mission-essential job tasks into seven categories. Next, they evaluated the job performance of

[101] Data courtesy of Dr. Mark Haucke.

intelligence analysts according to those criteria. Researchers found a strong positive correlation between aptitude for intelligence analysis (as measured in the knowledges and abilities survey) and successful job performance (as rated by supervisors).[102] Following is a brief description of the seven intelligence analysis performance categories:[103]

Data Collection - Research and gather data from all available sources.

Data Monitoring - Review flow of scheduled incoming data.

Data Organizing - Organize, format, and maintain data for analysis and technical report generation.

Data Analysis - Analyze gathered data to identify patterns, relationships, or anomalies.

Data Interpretation/Communication - Assign meaning to analyzed data and communicate it to appropriate parties.

Computer Utilization - Use computer applications to assist in analysis.

Coordination - Coordinate with internal and external organizations.

This concise inventory echoes the intelligence process and illustrates the complexity of the intelligence analyst's job. It also serves as a blueprint for managers as they design intelligence organizations and individual personnel assignments. In particular, the analyst's job description should reflect these expected behaviors for purposes of recruitment, selection, placement, training, and performance evaluation. The intelligence organization should also be structured physically and logically to enable these functions to occur. Managers should consider how all these factors combine to determine the effectiveness of individual analysts, intelligence units, and even national agencies or private firms that produce and use intelligence.

Personality Traits

The third component of the intelligence analyst profile, personality traits, addresses the individual's preferences for behaving in certain ways under specific conditions. Adults tend to exhibit the same set of behavior preferences consistently in familiar situations. This behavior pattern may be identified as a personality type. One well-known instrument for identifying an individual's personality type is the Myers-Briggs Type Indicator (MBTI).[104] The following discussion of the intelligence analyst's personality is based upon MBTI research.

---

[102] Haucke interview, 13 June 1996.

[103] Standardized categories are presented in an MRI performance evaluation booklet, *Job Dimension Ratings* (Bethesda, MD: MRI, 1995).

[104] See Isabel Briggs Myers, *Introduction to Type*. (Palo Alto, CA: Consulting Psychologists Press, 1980), and Ronald D. Garst, *Intelligence Types: The Role of Personality in the Intelligence Profession*. 2d printing, (Washington, DC: Joint Military Intelligence College, August 1995).

> Personality types are associated with more or less predictable patterns of behavior — meaning that people of different personality types approach tasks differently and have different tastes, interests, likes and dislikes. For example, some people would rather work alone while others prefer to work with other people. Some enjoy working with concrete information, others with abstract information. Some decide on the basis of personal reasons, some on cold, hard logic. And finally, some people enjoy making decisions while others are reluctant to decide because of perceived information inadequacy.[105]

Research at the Joint Military Intelligence College (JMIC) demonstrates that intelligence professionals exhibit a pattern of personality traits that sets them apart from the U.S. population as a whole. In this regard, intelligence professionals are no different from many others, for every profession has its own distinct pattern of personality traits. A significant percentage (21 percent) of those who choose to pursue employment in national security intelligence tend to express the following behavior preferences: orientation to the inner world of ideas rather than the outer world of things and people, tendency to gather factual information through the senses rather than inspiration, proclivity to make decisions on the basis of logic rather than emotion, and an eagerness to seek closure proactively instead of leaving possibilities open. In contrast, researchers found that people who exhibit the opposite set of personality traits are almost non-existent among intelligence professionals. The chart below summarizes the terminology by which the MBTI describes personality traits. Note that the most frequently occurring type among the respondents to the JMIC survey exhibit the traits I, S, T and J.[106]

The JMIC data are based on a large sample of government intelligence students and practitioners. Persons engaged in the study or practice of other forms of intelligence, particularly in the private sector, should not expect their personality type to match the JMIC profile. However, intelligence practitioners who choose and successfully apply the intelligence methodology presented in this primer are likely to exhibit the same personality traits as those identified in government practitioners. Because people tend to be satisfied and productive in their work if their own personalities match the corresponding behaviors suitable to their jobs, this research tying personality traits to the intelligence profession can help individuals consider their general suitability for certain types of intelligence work.

---

[105] Garst, *Intelligence Types*, 1.
[106] Garst, *Intelligence Types*, 9.

Personality Aspects Measured by the MBTI[107]

Orientation to the world

E=Extraversion	**I=Introversion**
Orientation to the outer world of things and people, interacting with and affecting them	Orientation to the inner world of ideas and concepts, solitude and self-awareness

Perception: non-rational processes; awareness of things, people, events or ideas, selection of stimuli to attend to

S=Sensing	**N=Intuitive**
Gather information by physical sensation; oriented to facts, detail and the present	Gather information by inspiration, unconscious processes; oriented to possibilities, relationships, and the future

Judgment: ways of deciding, evaluating, choosing, selecting

T=Thinking	**F=Feeling**
Decide on basis of logic, impersonal objective criteria, cause and effect, laws and justice	Decide on basis of subjective, personal criteria and values, and how decisions affect other people and relationships.

Preference for Closure as manifested through behavior using S/N or T/F Functions

J=Judging	**P=Perceiving**
Want to have an issue or project completed so they can move on; work takes precedence over play; proactive	Leave decisions open to modify response in accordance with new information; use play to make work more enjoyable; reactive

[107] Compiled from Garst, *Intelligence Types*, 4-9.

PART IX
DEFENSIVE MEASURES FOR INTELLIGENCE

> [A]s information becomes more and more a factor of production, of tangible worth for its own sake, the value of the special knowledge that is the essence of intelligence will command a higher price in the global information age marketplace than will the generally available knowledge. Therein lies the most ancient and, at the same time, the most modern challenge to the future of intelligence — protecting it.
>
> *— Goodden, in Dearth and Goodden, 415.*

Beyond Intelligence Process: Protecting the Means and the Results

An intelligence organization's openness about its validated intelligence methods is of course tempered by self-defense considerations. Two arenas that are complementary to intelligence production, Operations Security (OPSEC) and Information Systems Security (INFOSEC), focus on how practitioners can avoid revealing proprietary or classified information. OPSEC measures protect the specific actions taken to produce intelligence, whereas INFOSEC protects from disclosure the intelligence information used in production, as well as the resulting intelligence products.

In government circles, standard procedures guide the implementation of OPSEC and INFOSEC measures. In the private sector, trial and error may predominate. Companies that emphasize methods for exploiting publicly available information about their competitors may show little regard for protecting themselves from being targeted by the same means they have employed to target others. Furthermore, the trend toward greater computerization of the workplace, including on-line information systems and networked services, makes both government and commercial organizations vulnerable to being exploited themselves.[108]

For example, the Boeing Corporation discovered in 1992 that amateur computer hackers had found their way into the company's computer network, and used stolen passwords to open pathways to proprietary information stored in other computers in industry, government, and education organizations.[109] Prosecuting this case cost Boeing, the FBI, and other law-enforcement authorities considerable time and money.[110] This case was trivial

---

[108] Keen insights into such vulnerabilities are presented in Ira Winkler, *Corporate Espionage: What It Is, Why It Is Happening in Your Company, What You Must Do about It,* (Rocklin, CA: Prima Publishing, 1997).

[109] Rhonda E. MacLean, Senior Manager, Boeing Computing and Communications Security, "The Boeing Hacker Incident," *DODSI Security Awareness Bulletin* Number 1-94 (Richmond, VA: Department of Defense Security Institute, August 1994), 19.

[110] MacLean, 20-21

compared to other well publicized security breaches in government and industry.[111] Yet, at the March 1996 international SCIP conference, of 72 presentations held during four days, only three specifically addressed counterintelligence or security.[112] One reason for this is that businesses may be reluctant to admit their own vulnerabilities in the presence of competitor firms. However, as a Boeing computer security officer has noted, corporations are beginning to realize that admitting flaws in information system defenses is the first step toward preventing future violations, and business and government should work together toward this goal.[113]

In light of the tendency to overlook OPSEC and INFOSEC implementation, the remainder of this section develops an instructional overview of the basic information that government and business personnel should know to protect their activities from unauthorized exploitation. Indeed, for the health of U.S. commerce and national security activities, everyone needs user-friendly information on how to protect proprietary information. Even the most sophisticated corporations have difficulty keeping up with the hazards of the information age; it was not until 1992 that Boeing mandated that all company computer users attend a security awareness briefing, and this was after the firm suffered a major breach of information security. Now Boeing sees "...the importance of information security to our company's long-term competitiveness..." and considers awareness activity as the cornerstone to a good security program.[114]

Operations Security

OPSEC is essential to the intelligence function in both the national security and business environments. OPSEC denies adversaries information about one's own operational capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conduct of those operations and other related activities. An adversary is not necessarily a belligerent enemy: In OPSEC terms, an adversary is any entity that acts against one's own interest or actively opposes one's own goals.[115]

To protect an intelligence operation, practitioners can adopt an adversary's perspective. For example, factors at risk in one's own environment can be categorized into critical information, indicators, and vulnerabilities, described briefly below.

---

[111] Examples include those cited in Clifford Stoll, *The Cuckoo's Egg*, (New York: Pocket Books, 1990) and Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994).

[112] SCIP, *Conference Proceedings.* Annual International Conference & Exhibit, March 27-30, 1996, (Alexandria, VA: SCIP, March 1996).

[113] MacLean, 22.

[114] MacLean, 22.

[115] National Cryptologic School, Information Security Department, *Operations Security Fundamentals*, (Fort Meade, MD: 1994), 2.

Factors at Risk in Intelligence Operations	
Critical Information	Details of capabilities and operations directed against an adversary
Indicator	Detectable actions and publicly available information revealing critical information
Vulnerability	Conditions making exploitable information available to the adversary

Countermeasure options to prevent an adversary from exploiting these factors include: eliminating the indicators altogether, concealing indicator activities, disguising indicator activities, and staging deceptive (false) activities.[116]

The practice of OPSEC is so important to national security that a federal organization has been established as its advocate. As a result of the 1988 Presidential Directive on national operations security, the Interagency OPSEC Support Staff (IOSS) was formed, with the National Security Agency as its director. The core membership of the IOSS includes the Department of Defense, Department of Energy, Central Intelligence Agency, Federal Bureau of Investigation, and General Services Administration.[117] Other executive and national security bodies, including the military services, have representation on the National Operations Security Advisory Committee, which advises the Executive Branch on the practice of OPSEC.[118] The IOSS may be contacted for assistance at:

Interagency OPSEC Support Staff, 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770-1405 Telephone (301) 982-2313/0323.

Information Systems Security

Information Systems Security (INFOSEC) refers to the protection of information that an organization uses and produces in the course of its operations. Today, this means protecting complex electronic networks. Government and business depend upon computerized systems for everything from banking, communications, and data processing to physical security and travel reservations. To the casual observer, INFOSEC may seem the domain of a few technical specialists, or the exclusive concern of the military or intelligence agencies. But INFOSEC is the responsibility of everyone who has ever used a telephone, computer, or automatic bank teller machine.[119]

---

[116] National Cryptologic School, 9.

[117] National Security Agency, Introduction.

[118] National Operations Security Advisory Committee, *National Operations Security Doctrine*, (Greenbelt, MD: Interagency OPSEC Support Staff, January 1993): unnumbered back of first and second physical pages from beginning.

[119] A basic reference on INFOSEC is the National Research Council book *Computers at Risk: Safe Computing in the Information Age*, (Washington, DC: National Academy Press, 1991).

> INFOSEC today [involves] significantly more than the traditional security offered by encryption. Network vulnerability to adversarial intercept, tampering, or destruction of data mandates INFOSEC solutions that ensure the authentication, integrity, and availability of classified and unclassified information created, stored, and processed on [information] systems. ... Such solutions must enable the interconnection of Command and Control, intelligence, and support systems and must allow for the commingling of critical information of different classification levels on a common transport backbone. INFOSEC solutions must be flexible, configurable, and result from a risk management scenario that balances the costs and availability of countermeasures against actual threats to, and vulnerabilities of, networks and systems. Finally, INFOSEC must accomplish all of this in an environment in which networks are neither owned nor controlled by [the government] and resources are severely constrained.[120]

Each intelligence organization and activity must tailor its INFOSEC measures to its particular technologies and operational practices, weighing the costs of such measures against their value in safeguarding the mission. A three-dimensional model of INFOSEC, illustrated below, may guide the intelligence service in implementing protective measures and assessing their adequacy. The first dimension addresses the need to understand the vulnerability of information as it passes through different stages of use. The second dimension includes the key characteristics of information that must be preserved for it to remain useful and secure. The third dimension covers the general categories of INFOSEC tools that the intelligence service may employ. Each element of the model is dependent on the others.[121] Together, these interlocking pieces make up a comprehensive INFOSEC strategy appropriate to the public or private sector.

Dimensions of INFOSEC[122]

Information States:	Transmission, Storage, Processing
Critical Information Characteristics:	Confidentiality, Integrity, Availability to Legitimate Users
Countermeasures:	Technology, Policy/Practice, Education

Role of the Federal Government

Federal agencies, including Intelligence Community members, play key roles in helping both government and businesses learn and practice INFOSEC. The two primary authorities for INFOSEC are the Department of Commerce and the Department of

[120] National Security Agency, Introduction, para. D.2.

[121] Lynn F. Fisher, "Defining the Threat to Information Systems," *DODSI Security Awareness Bulletin* 2-94, (August 1994), 4.

[122] Fisher.

Defense. Organizations within these departments provide INFOSEC services to their respective constituencies within the framework of national information policies established by the Executive Branch. The following overview begins with a summary of Executive Branch policy.

National Information Policy

> The vision of the National Information Infrastructure — or NII — is [as] a vast accessible network of networks that supports communications and information processing to create jobs, increase productivity, improve access to government services, and encourage community networking. The NII is also the wide array of information of all kinds within the networks, whether it is stored, processed, or communicated. Finally, it includes the people... who are today creating and using the NII.[123]

The federal government's role in the NII is to provide a sound legal and policy framework, in conjunction with state, local and Native American governments. Current initiatives include assuring universal service on the NII, thereby enabling open access to government information; protecting intellectual property rights; protecting the privacy of individual information; and stimulating the development of advanced information technologies, including security technologies.[124] The Office of Management and Budget's (OMB) national information security authority covers the development, promotion, implementation and evaluation of government policies and practices for information resource management.[125]

A multi-agency group, the national Information Infrastructure Task Force (IITF), coordinates the federal role in the NII through three committees: the Committee on Applications and Technology, the Telecommunications Policy Committee, and the Information Policy Committee. The OMB's Office of Information and Regulatory Affairs chairs the IITF's Information Policy Committee. As noted below, elements of the Commerce Department chair the other two IITF committees. In addition, the NII Security Issues Forum coordinates NII security activities throughout the IITF and the federal government.[126]

Commerce Department

The Commerce Department's Assistant Secretary for Communications and Information heads the National Telecommunications and Information Administration (NTIA).

---

[123] Sally Katzen, Administrator, Office of Information and Regulatory Affairs, U.S. Office of Management and Budget, Remarks prepared for delivery at the National Computer Security Conference, Baltimore, MD, 11 October 1994.

[124] Katzen.

[125] U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments* (Washington, DC: GPO, September 1994), 137.

[126] Katzen.

The NTIA's information security responsibilities include: serving as the principal executive adviser to the President on telecommunications and information policy; serving as the principal federal telecommunications research and engineering laboratory, through the Institute for Telecommunication Sciences in Boulder, Colorado; and providing grants to programs that promote the development and provision of advanced telecommunications technologies for the public. The NTIA chairs the IITF's Telecommunications Policy Committee.[127]

The Commerce Department's Technology Administration includes two components involved in information security, the Office of Technology Policy (OTP) and the National Institute for Standards and Technology (NIST).

> The primary role of the OTP is to offer assistance to private sector and government communities in advocating and pursuing policies that maximize the impact of technology on economic growth, and by exercising leadership to define the role of government in supporting U.S. industrial competitiveness in the post-cold war environment. ... NIST's primary mission is to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards.[128]

NIST is the national authority for developing government-wide standards and guidelines for protecting unclassified but sensitive information, and for developing government-wide training programs.[129] NIST also chairs the IITF's Committee on Applications and Technology.[130] Finally, NIST maintains the Computer Security Resource Clearinghouse (CSRC) as a resource for anyone with an interest in computer security. It is available on-line 24 hours a day, seven days a week at no charge. The CSRC provides access to crisis response information on security-related threats, vulnerabilities, and solutions, and is a general index to computer security topics such as general risks, privacy, legal issues, viruses, assurance, policy, and training.[131]

Defense Department

The Secretary of Defense is the Executive Agent for National Security Telecommunications and Information Systems Security.[132] As a whole, Department of Defense (DoD) information and communications systems are termed the Defense Information Infrastructure (DII). Under the direction of the Secretary of Defense, three DoD agencies form the

---

[127] Katzen.

[128] Office of the Federal Register, National Archives and Records Administration, *The United States Government Manual 1995/96* (Washington, DC: GPO, 1 July 1995), 167-168.

[129] U.S. Congress, Office of Technology Assessment, 13.

[130] Katzen.

[131] Defense Information Systems Agency (DISA), "The NIST Computer Security Resource Clearinghouse," *DISSPatch* 4, no. 1 (3rd Quarter 1996): 6. See CSRC home page at: http://www.csrc.nist.gov.

[132] National Security Agency, Chapter 3, B.d.

core DII INFOSEC team: the Defense Intelligence Agency (DIA), the Defense Information Systems Agency (DISA), and the National Security Agency (NSA). Although notionally the DII is a dedicated system for proprietary and classified national defense information, in fact over 95 percent of its communications are carried on the public switched networks of the NII.[133] Thus, DoD expertise in information security doctrine and technology makes the organizations explained below key resources for other government organizations and for the private sector.

The Defense Intelligence Agency, as the central authority for military intelligence, provides INFOSEC threat analysis and support to the DII.[134] Another agency, DISA, is responsible for planning, developing, and supporting command, control, communications, and information systems that serve the needs of the National Command Authorities under all conditions of peace and war; it further ensures the interoperability of all DII systems and those national and/or international commercial systems that affect the DISA mission.[135] NSA acts as the National Manager for National Security Telecommunications and Information Systems Security in the name of the Secretary of Defense. In this capacity, NSA is the focal point for U.S. government cryptography and for the security of national security telecommunications and information systems.[136] NSA provides DISA with the tools, techniques, products, services, and security management structures to protect the DII, through its "V" Group, the customer service and engineering organization for information systems security.[137] Within NSA, the National Computer Security Center (NCSC) conducts technical evaluation of the protection capabilities of commercially produced and supported systems.[138] Through its Information Systems Security Research Joint Technology Office (ISSR-JTO), NSA coordinates with DISA and the DoD's Advanced Research Projects Agency on engineering INFOSEC technologies. The ISSR-JTO provides a first line of defense for defensive information warfare, and permits electronic commerce between DoD and its contractors. It also maintains research and technology interfaces with the military departments, national labs, universities, and industry.[139] NSA coordinates with the National Institute for Standards and Technology (NIST) in matters of common concern.[140] Together, DIA, DISA, and NSA operate the DoD Center for Information Systems Security.[141]

---

[133] LtGen Kenneth A. Minihan, "Intelligence and Information System Security," *Defense Intelligence Journal* 5, no. 1 (Spring 1996): 20.

[134] Defense Information Systems Agency, "INFOSEC and the DII," *DISSPatch* 4, No. 1, (3rd Quarter, CY 1996): 7.

[135] Office of the Federal Register, 234.

[136] NSA, Chapter 3, B.e.(2).

[137] DISA, "Introducing NSA's New and Improved V Group," *DISSPatch* 4, no. 3 (3rd Quarter 1996): 2.

[138] NSA, Chapter 6, para. 1.

[139] DISA, "V Group," 5.

[140] INFOSEC Program Management Office (IPMO), *DISSPatch*, May 97, 14.

[141] DISA, "INFOSEC and the DII," *DISSPatch* 4, No. 1 (3rd Quarter 1996): 7.

The Department of Defense's INFOSEC Program Management Office (IPMO) is a joint DoD/DISA/NSA organization charged with executing centrally managed INFOSEC functions within the DoD.[142] The IPMO provides operational protection and detection capability for the DII against information exploitation, manipulation, or destruction. It administers DoD-wide INFOSEC training and manages the DoD INFOSEC Technical Services Contract. The IPMO conducts vulnerability, threat, and operational analyses of the DII, provides security policy guidance and oversight to DISA programs, and certifies DISA and non-DISA systems that connect to the DII.[143] The IPMO also provides support to the Assistant Secretary of Defense for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (ASD/C4ISR).[144] Another DoD body, chaired by the ASD/C4ISR, also has a role in INFOSEC. Under the purview of the National Security Council, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) advises Executive Branch agencies and Departments on the status of national security systems. Its two subcommittees focus on telecommunications security and information systems security, respectively. NSA provides the NSTISSC secretariat.[145]

In addition, the DoD Security Institute (DODSI) promotes security awareness and compliance with security procedures in DoD by offering training courses to security personnel in DoD and DoD-related industry, publishing security awareness bulletins, and disseminating information to security trainers on security and counterintelligence.[146]

INFOSEC for Everyone

The national authorities for INFOSEC described above evolved out of the need to protect the fundamental role of information in a democratic society and market economy. They help strike the balance between free exchange of information and privacy, and between free enterprise and regulation. Government-sponsored information policy and technology set the standards upon which nearly every facet of public and private life is based. Citizens receive basic services through government-created or -regulated information infrastructure, including automatic payroll deposit to employee bank accounts, cellular telephone service, electronic commerce via the Internet, air and rail traffic control, emergency medical services, and electrical power supply.

Such services contribute not only to the citizen's quality of life, but to the very functioning of the nation. Information is the lifeblood of society and the economy. Imagine the chaos that would reign if the government, the military, banks, businesses, schools, and hospitals could not communicate reliably. Life would come to a halt.

---

[142] IPMO, 14.
[143] DISA, "INFOSEC," 7.
[144] U.S. Department of Defense Security Institute (DODSI), *DODSI Security Awareness Bulletin* 2-94 (August 1994): 25.
[145] NSA, Chapter 3, B.a, B.b, and B.c.
[146] DODSI, front cover, 12, 18.

INFOSEC is designed to protect society from inadvertent or intentional harm to these key functions. The same free access to information that makes society flourish also makes it vulnerable to damage, attack or exploitation. For example, passive threats such as shoddy equipment, faulty software, or negligent personnel can disrupt service and destroy information. Hostile threats include thrill-seeking computer hackers and belligerent foreign adversaries who deliberately target sensitive government and public information networks with the aim of disrupting or destroying key operations, such as military projects or power grids.[147] Comparable scenarios within the business sector, to include information sabotage and deception actions against competitors, are at least plausible. Therefore, basic knowledge of INFOSEC may benefit citizens in all walks of life. Addresses and phone numbers for the INFOSEC agencies that can assist the public are listed at the end of this chapter.[148]

Government expertise in information technology and policy has made it the authority specifically on protecting intelligence operations. The private sector may also benefit from this expertise by applying INFOSEC measures in business intelligence. In brief, successful intelligence operations rely on secure transmission, storage, and processing of the information used. The information itself must be exchanged only among legitimate users, and it must retain its intended meaning and be available to users upon demand. Finally, intelligence information and products can be protected through technology (access control, encryption), through security policies and practices, and through educating the workforce, as with this document.

Points of contact:

Commerce Department:

NIST, Public Inquiries Unit, 100 Bureau Drive, Gaithersburg, MD 20899-0001; 301-975-6478 (voice); email: inquiries@*nist.gov*; Website: *http://www.nist.gov/*.

DoD:

IPMO, 5111 Leesburg Pike, Suite 100, Falls Church, VA 22014-3206; 703-681-7944/DSN761-7944 (voice); 703-681-1386/DSN 703-761-1386 (fax); e-mail: *cissa@ncr.disa.mil*, Website: *http://www.disa.mil/ciss*.

DISA, Public Affairs Office, 701 South Courthouse Road, Arlington, VA 22204-2199; 703-607-6900 (voice); Website: *http://www.disa.mil*.

DODSI, 8000 Jefferson Davis Highway, Building 33E, Richmond, VA 23297-5091; 804-279-5314/DSN 695-5314 (voice); 804-279-5239/DSN 695-5239 (fax).

---

[147] Gregory L. Vistica and Evan Thomas, "The Secret Hacker Wars, Behind the spreading battle over cyberterrorism," *Newsweek* (1 June 1998): 60.

[148] In addition, the National Counterintelligence Center provides support to the private sector regarding economic espionage, economic intelligence collection, and threat awareness. The NACIC website is *http://www.nacis.gov.*

NCSC, Suite 6765, 9800 Savage Road, Fort George G. Meade, MD 20755-6765; 20 410-859-4371 (voice); 410-859-4375 (fax).

NSA, Fort George G. Meade, MD 20755-6000, Attn: V1, Office of Customer Support Services; 410-859-4384/DSN 644-0111; 800-688-6115 (voice); Website: *http://www.nsa.gov:8080/*.

EPILOGUE

This primer has reviewed government intelligence production practices in building-block fashion. It has also explored the defensive measures comprising information security and operations security, which are integral to all the building blocks, and are equally applicable to private businesses and government organizations. Finally, the primer has drawn a cognitive, behavioral and personality profile of the central figure in intelligence production — the intelligence analyst. In the spirit of benchmarking, this document invites a reciprocal examination of best practices that may have been developed by private businesses, and of principles that may have been derived from other academic studies of intelligence-related processes.

Although this effort reflects a government initiative, in fact the government Intelligence Community may receive the greater share of rewards from benchmarking its own process. Potential benefits to the Community include an improved public image, increased self-awareness, more efficient recruitment through more informed self-selection by candidates for employment, as well as any resultant acquisition of specialized information from subject matter experts in the business and academic communities.

Primary advantages for the government's partners in the exchange of information on best practices could be greater understanding of how tax dollars are spent, and the opportunity to transfer an appreciation of government professional intelligence production, security, and staffing methods into academic curricula and business operations.

For all participants in benchmarking, releasing information is actually a way of controlling it, a way of depicting and fostering an accurate organizational image rather than allowing others to draw and disseminate erroneous characterizations. For the U.S. Intelligence Community in particular, any initiative in benchmarking the intelligence process fulfills a charge of the recently completed Report on the Community's Roles and Capabilities: to improve its performance through closer relationships with customers, including the private sector.

GLOSSARY

ASD/C4ISR	Assistant Secretary of Defense for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
BI	Business Intelligence
CIA	Central Intelligence Agency
CISS	Center for Information Systems Security
CSRC	Computer Security Resource Center
DCI	Director of Central Intelligence
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DoD	Department of Defense
DODSI	Department of Defense Security Institute
FISINT	Foreign Instrumentation and Signature Intelligence
GPO	U.S. Government Printing Office
HUMINT	Human Intelligence
IC	Intelligence Community
IITF	Information Infrastructure Task Force
IMINT	Imagery Intelligence
INFOSEC	Information Systems Security
INFOWAR	Information Warfare
IOSS	Interagency OPSEC Support Staff
IPMO	INFOSEC Program Management Office
ISSR-JTO	Information Systems Security Research Joint Technology Office
JIVA	Joint Intelligence Virtual Architecture

JMIC	Joint Military Intelligence College
MASINT	Measurement and Signature Intelligence
MBTI	Myers-Briggs Type Indicator
MRI	Management Research Institute
NACIC	National Counterintelligence Center
NCSC	National Computer Security Center
NIC	National Intelligence Council
NII	National Information Infrastructure
NIMA	National Imagery and Mapping Agency
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OTP	Office of Technology Policy
SCIP	Society of Competitive Intelligence Professionals
SIGINT	Signals Intelligence

BIBLIOGRAPHY

Allen, George. "The Professionalization of Intelligence." In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 33-40. Washington, DC: Joint Military Intelligence Training Center (JMITC), 1995.

Andre, Louis E. "Intelligence Production: Towards a Knowledge-Based Future." *Defense Intelligence Journal* 6, no. 2 (Fall 1997): 35-45.

Babbie, Earl. *The Practice of Social Research.* Belmont, CA: Wadsworth Publishing Co, 1992.

Ben-Israel, Isaac. "Philosophy and Methodology of Intelligence: The Logic of Estimative Process." *Intelligence and National Security* 4, no. 4 (October 1989): 660-718.

Brei, Captain William S. *Getting Intelligence Right: The Power of Logical Procedure*. Occasional Paper Number Two. Washington, DC: Joint Military Intelligence College (JMIC), January 1996.

Carney, LT Donald J., USN. *Estimating the Dissolution of Yugoslavia*. Seminar Paper. Washington, DC: Joint Military Intelligence College, September 1991.

Central Intelligence Agency. *A Compendium of Analytic Tradecraft Notes*. Washington, DC, Directorate of Intelligence, February 1997.

_____. *A Consumer's Guide to Intelligence*. Washington, DC: Public Affairs Staff, July 1995. PAS 95-00010.

Clauser, Jerome K. and Sandra M. Weir. *Intelligence Research Methodology, An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence*. Washington, DC: Defense Intelligence School, 1975.

D'Aveni, Richard. "Hypercompetition." Briefing to SCIP Conference. Alexandria, VA, 28 March 1996.

Davis, Jack. "Combatting Mindset." *Studies in Intelligence* 35, no. 4 (Winter 1991): 13-18.

_____. *Intelligence Changes in Analytic Tradecraft in CIA's Directorate of Intelligence*. Washington, DC: CIA Directorate of Intelligence, April 1995.

_____. *The Challenge of Opportunity Analysis*. Intelligence Monograph. Washington, DC: Center for the Study of Intelligence, July 1992. CSI 92-003U.

Davis-Floyd, Robbie E. "Storytelling Corporate Futures: The Shell Scenarios." *International Journal of Futures Studies* 1 (1995-1997), on-line at http://www.systems.org/HTML/journals.htm, accessed 3 December 1997.

Dearth, Douglas H. “National Intelligence: Profession and Process.” In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 15-31. Washington, DC: JMITC, 1995.

_____. “The Politics of Intelligence.” In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 97-121. Washington, DC: JMITC, 1995.

Defense Information Systems Agency. “INFOSEC and the DII.” *DISSPatch* 4, no. 1 (3rd Quarter 1996): 7.

_____. “Introducing NSA’s New and Improved V Group.” *DISSPatch* 4, no. 1 (3rd Quarter 1996): 2, 5.

_____. “The NIST Computer Security Resource Clearinghouse.” *DISSPatch* 4, no. 1 (3rd Quarter 1996): 6.

Defense Intelligence Agency. *Vector 21, A Strategic Plan for the Defense Intelligence Agency.* Washington, DC: Programs and Operations Staff, undated.

Elmuti, Dean, and Hanus Kathawaia and Scott J. Lloyed. “The Benchmarking Process: Assessing Its Value and Limitations.” *Industrial Management*, 39, No. 4 (July/August 1997): 12-19.

Fisher, Lynn F. “Defining the Threat to Information Systems.” *DODSI Security Awareness Bulletin* 2-94 (August 1994): 3-10.

Frankenfield, Jerry and Melissie Rumizen. *A Guide to Benchmarking*. Fort Meade, MD: NSA, 12 July 1995.

Garst, Ronald D. “Components of Intelligence.” In *A Handbook of Intelligence Analysis*, 2d ed. Ed. Ronald D. Garst, 1-32. Washington, DC: Defense Intelligence College, January 1989.

_____. *Intelligence Types: The Role of Personality in the Intelligence Profession*. Washington, DC: Joint Military Intelligence College, August 1995.

Goodden, Royal Thomas. “Intelligence in the Information Age.” In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 409-416. Washington, DC: JMITC, 1995.

Harkleroad, David. “Actionable CI.” Briefing to SCIP Conference. Alexandria, VA, 28 March 1996.

Harris, Gary. “Evaluating Intelligence Evidence.” In *A Handbook of Intelligence Analysis*, 2d ed. Ed. Ronald D. Garst, 33-48. Washington, DC: Defense Intelligence College, January 1989.

Haucke, Mark H. Industrial Psychologist, National Security Agency. Interview with the author, 25 May 1995.

Hecht, Francoise. "The Aha! Factor." *Director* 50, No. 12 (July 1997): 59.

Herring, Jan. "Strides in Institutionalizing BI in Businesses." Briefing to SCIP Conference. Alexandria, VA, 28 March 1996.

Hulnick, Arthur S. "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach." *Intelligence and National Security*, 1, No. 2, (May 1986): 212-233.

_____. "Managing Intelligence Analysis: Strategies for Playing the End Game." *International Journal of Intelligence and CounterIntelligence*, 2, No. 3, (Fall 1988): 321-343.

Hunter, Douglas E. *Political/Military Applications of Bayesian Analysis: Methodological Issues.* Boulder, CO: Westview, 1984.

Johnson, Loch K. *America's Secret Power, The CIA in a Democratic Society.* New York: Oxford University Press, 1989.

Jones, Morgan D. *The Thinker's Toolkit.* New York: Random House, 1995: 44-46.

Kahaner, Larry. *Competitive Intelligence: From Black Ops to Boardrooms*. New York: Simon and Schuster, 1996.

Kam, Ephraim. *Surprise Attack*. Cambridge, MA: Harvard University Press, 1988.

Kaplan, Abraham. *The Conduct of Inquiry.* San Francisco, CA: Chandler, 1964.

Katzen, Sally. Administrator, Office of Information and Regulatory Affairs, U.S. Office of Management and Budget. Remarks prepared for delivery at the National Computer Security Conference, Baltimore, Maryland, 11 October 1994.

Keesing, Hugo A. Instructor, Joint Military Intelligence College. Remarks to a meeting of the Communications Analysis Association, Fort Meade, MD, 6 November 1995.

Keirsey, David. *Portraits of Temperament*. Amherst, NY: Prometheus, 1987.

Kight, Leila. "Elements of CI Success." Briefing to SCIP Conference. Alexandria, VA, 28 March, 1996.

Macdaid, Gerald P., Mary H. McCaulley and Richard I. Kainz. *Myers-Briggs Type Indicator: Atlas of Type Tables*. Gainesville, FL: Center for Applications of Psychological Type, 1986.

MacLean, Rhonda E. "The Boeing Hacker Incident." *DODSI Security Awareness Bulletin* 2-94 (August 1994): 19-22.

Major, James S. *Briefing with Intelligence*. Washington DC: Joint Military Intelligence College, August 1997.

_____. *The Style Guide: Research and Writing at the Joint Military Intelligence College*. Washington DC: Joint Military Intelligence College, August 1994.

Management Research Institute (MRI). *Ability and Knowledge Requirements*. Bethesda, MD: MRI, 1994.

_____. *Job Dimension Ratings*. Performance evaluation booklet. Bethesda, MD: Management Research Institute, 1995.

Mathams, R. H. "The Intelligence Analyst's Notebook." In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 77-96. Washington, DC: JMITC, 1995.

Minihan, Lt. Gen. Kenneth A. Director, National Security Agency. "DIR Addresses the Future of NSA." *Communicator* 4, no. 20 (14 May 1996): 1-3.

_____. "Intelligence and Information System Security." *Defense Intelligence Journal* 5, no. 1 (Spring 1996): 13-23.

_____. "Winning the Information Game: NSA's Role in the 21st Century." *NSA Newsletter*, May 1996, 3.

Moyer, Kathy. "Scenario Planning at British Airways — A Case Study." *Long Range Planning* 29, No. 2 (April 1996): 172-181.

Murray, Thomas H. "Taxonomy of Problem Types." Analytic coursework material for the Joint Military Intelligence College, based upon Morgan D. Jones, *The Thinker's Toolkit.* New York: Random House, 1995: 44-46.

Myers, Isabel Briggs. *Introduction to Type*. Palo Alto, CA: Consulting Psychologists Press, 1980.

_____. and Mary H. McCaulley. *Manual: A Guide to the Development and Use of the Myers-Briggs Type Indicator.* Palo Alto, CA: Consulting Psychologists Press, 1985.

_____. with Peter Myers. *Gifts Differing*. Palo Alto, CA: Consulting Psychologists Press, 1980.

National Cryptologic School (NCS). Information Security Department, *Operations Security Fundamentals*. Fort Meade, MD: NCS, 1993.

National Operations Security (OPSEC) Advisory Committee. *National Operations Security Doctrine*. Greenbelt, MD: Interagency OPSEC Support Staff, January 1993.

National Research Council. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press, 1991.

National Security Agency. *1995 INFOSEC Manual*. Fort Meade, MD: NSA, 1995.

Office of the Federal Register. National Archives and Records Administration. *The United States Government Manual 1995/96*. Washington, DC: GPO, 1 July 1995.

P.L. 102-183. "David L. Boren National Security Education Act of 1991." Title VIII, Sections 801-802, 4 December 1991.

P.L. 103-62. "Government Performance and Results Act of 1993."

Peterson, Marilyn. *Applications in Criminal Analysis.* Westport, Connecticut: Greenwood Press, 1994.

Prescott, John. Professor of Business Administration, University of Pittsburgh. "Research." Briefing to SCIP Conference, 28 March 1996

Rumizen, Melissie C. Benchmarking Manager, National Security Agency. Interviews with the author, 4 January 1996 and 5 July 1996.

Schmidlin, LCDR William G., USN. *Zen and the Art of Intelligence Analysis*. MSSI Thesis. Washington, DC: Joint Military Intelligence College, July 1993.

Schum, David A. *Evidence and Inference for the Intelligence Analyst*. Volume I. Lanham, MD: University Press of America, 1987.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway.* New York: Thunder's Mouth Press, 1994.

SCIP. *1995 SCIP Membership Directory.* Alexandria, VA: SCIP, 1995.

_____. *Competitive Intelligence Review* 8, No. 3 (Fall 1997): unnumbered 8th page.

_____. *Conference Proceedings.* Annual International Conference & Exhibit, March 27-30, 1996. Alexandria, VA: SCIP, March 1996.

Smith, Ian. "Avoiding Future Shock." *Director* 50, No. 12 (July 1997): 56-59.

Stoll, Clifford. *The Cuckoo's Egg*. New York: Pocket Books, 1990.

Studeman, William O. "Leading Intelligence Along the Byways of Our Future: Acquiring C^4ISR Architectures for the 21st Century." *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 47-65.

Swenson, Russell G. *An Office Manager's Guide to Intelligence Readiness*. Occasional Paper Number Three. Washington, DC: JMIC, December 1996.

Tetzlaff, Jonathan. Area Director, Security Research and Analysis, Amoco Corporation. Personal correspondence with editor, 24 October 1997.

Turner, Michael A. "Setting Analytical Priorities in U.S. Intelligence." *International Journal of Intelligence and CounterIntelligence* 9, no. 3 (Fall 1996): 313-327.

U.S. Congress, House Permanent Select Committee on Intelligence. *IC21: The Intelligence Community in the 21st Century.* Staff Study, April 1996: Section III, "Intelligence Requirements Process."

_____. Office of Technology Assessment. *Information Security and Privacy in Network Environments*. Washington, DC: GPO, September 1994. OTA-TCT-60

_____. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. Report of the Commission on the Roles and Capabilities of the U.S. Intelligence Community. Washington, DC: GPO, 1 March 1996.

U.S. Department of Defense. DoD Security Institute (DODSI). *DODSI Security Awareness Bulletin* 2-94 (August 1994).

_____. Joint Chiefs of Staff. Joint Pub 1-02. *Dictionary of Military and Associated Terms*. Washington, DC: 23 March 1994: 184.

_____. Joint Chiefs of Staff. Joint Pub 2-0. *Joint Doctrine for Intelligence Support to Operations*. Washington, DC: GPO, 5 May 1995.

Vistica, Gregory L. and Evan Thomas, "The Secret Hacker Wars, Behind the Spreading Battle Over Cyberterrorism." *Newsweek* (1 June 1998): 60.

Westerfield, H. Bradford. "Inside Ivory Bunkers: CIA Analysts Resist Managers" Pandering' — Part I." *International Journal of Intelligence and CounterIntelligence* 9, no. 4 (Winter 1996/97): 407-424.

_____. "Inside Ivory Bunkers: CIA Analysts Resist Managers' "Pandering' — Part II." *International Journal of Intelligence and CounterIntelligence* 10, no. 1 (Spring 1997): 19-54.

White House. *National Operations Security Program*. Fact Sheet. Washington, DC: January 1988.

Winkler, Ira. *Corporate Espionage: What It Is, Why It Is Happening in Your Company, What You Must Do about It*. Rocklin, CA: Prima Publishing, 1997.

ABOUT THE AUTHOR

Lisa Krizan has been a researcher with the Department of Defense since 1987. She received a master's degree from the Joint Military Intelligence College in 1996 and developed many of the ideas for this paper as part of her thesis on benchmaking the intelligence process. A second-generation intelligence scholar, she follows the example set by her father, 1972 Defense Intelligence College graduate Allen J. Montecino, Jr., Colonel, USAF (Ret).

Joint Military Intelligence College
Occasional Papers

1. Classified paper.

2. *Getting Intelligence Right: The Power of Logical Procedure*, Capt (USAF) William S. Brei, 1996.

3. *An Office Manager's Guide to Intelligence Readiness*, Russell G. Swenson, 1996.

4. Classified paper.

5. *A Flourishing Craft: Teaching Intelligence Studies*, Papers Prepared for the 18 June 1999 JMIC Conference on Teaching Intelligence Studies at Colleges and Universities, 1999.

6. *Intelligence Essentials for Everyone*, Lisa Krizan, 1999.

MCWP 2-22
(formerly MCWP 2-15.2)

Signals Intelligence

U.S. Marine Corps

DISTRIBUTION STATEMENT A: approved for public release; distribution is unlimited

PCN 14300006300

MCCDC (C 42)
13 Jul 2004

E R R A T U M

to

MCWP 2-22

SIGNALS INTELLIGENCE

1. Change the publication short title to read "MCWP 2-22" (vice MCWP 2-15.2).

PCN 143 000063 80

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380-1775

22 February 1999

FOREWORD

Marine Corps Warfighting Publication (MCWP) 2-22, *Signals Intelligence*, serves as a basic reference for understanding concepts, operations, and procedures for the conduct of signals intelligence (SIGINT) operations in support of the Marine air-ground task force. This publication complements and expands on Marine Corps Doctrinal Publication 2, *Intelligence*, and MCWP 2-1, *Intelligence Operations,* which provide doctrine and higher order tactics, techniques, and procedures for intelligence operations.

The primary target audience of this publication is intelligence personnel responsible for planning and executing SIGINT operations. Personnel who provide support to SIGINT or who use the results from these operations should also read this publication.

MCWP 2-22 describes aspects of SIGINT operations, including doctrinal fundamentals, equipment, command and control, communications and information systems support, planning, execution, security, and training. Detailed information on SIGINT operations and tactics, techniques, and procedures is classified and beyond the scope of this publication.

MCWP 2-22 supersedes Fleet Marine Force Manual 3-23, (C) *Signals Intelligence/Electronic Warfare Operations* (U), dated 21 September 1990.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

J. E. RHODES
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: 143 000063 00

To Our Readers

Changes: **Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to smb@doctrine div@mccdc. Recommendations should include the following information:**

- **Location of change**
  - **Publication number and title**
  - **Current page number**
  - **Paragraph number (if applicable)**
  - **Line number**
  - **Figure or table number (if applicable)**
- **Nature of change**
  - **Add, delete**
  - **Proposed new text, preferably double-spaced and typewritten**
- **Justification and/or source of change**

Additional copies: **A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status*. An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: http://www.doctrine.quantico.usmc.mil.**

Unless otherwise stated, whenever the masculine or feminine gender is used, both men and women are included.

Signals Intelligence

Table of Contents

		Page
Chapter 1.	**Fundamentals**	
1001	What is Signals Intelligence?	1-1
1002	Concept of Employment	1-1
1003	SIGINT and Electronic Warfare	1-2
1004	Threats	1-3
1005	All-Source Intelligence and Operations Command Support	1-3
1006	Capabilities	1-4
1007	Limitations	1-5
1008	Organization	1-5
1009	Command and Control	1-6
1010	Operations	1-6
1011	Commanders' Responsibilities	1-8
Chapter 2.	**SIGINT Responsibilities in the Supporting Establishment**	
2001	Marine Corps SIGINT Organization	2-1
2002	SIGINT Organizations in Other Military Services	2-2
2003	National SIGINT Organizations	2-3
Chapter 3.	**SIGINT Responsibilities in the MAGTF**	
3001	Commanders, Marine Corps Forces	3-1
3002	MAGTF Staff Sections	3-1
3003	MAGTF Intelligence Section Elements	3-2
3004	Marine Divisions and Aircraft Wings	3-5
3005	Radio Battalions	3-5
3006	VMAQs	3-5
Chapter 4.	**Radio Battalion**	
4001	Tasks	4-1
4002	Organization	4-1
4003	Task Organization for MAGTF Operations SIGINT Support Unit	4-3
4004	Command and Control	4-5
4005	Notional Concepts of Employment and Task Organizations	4-5

Chapter 5. Marine Tactical Electronic Warfare Squadrons

5001	Mission and Tasks	5-1
5002	Organization and Concept of Employment	5-1
5003	EA-6B Prowler	5-2
5004	Tactical EA-6B Mission Planning System	5-4
5005	TERPES	5-4

Chapter 6. Communications and Information Systems

6001	Basic MAGTF SIGINT CIS Requirements	6-1
6002	Notional MAGTF SIGINT Operational Architectures	6-2
6003	Planning Consideration	6-7
6004	SIGINT Communications	6-7

Chapter 7. Planning and Operations

Section I	SIGINT Functional Planning	7-1
7101	SIGINT Concept of Operations	7-1
7102	Enemy Characteristics	7-1
7103	Topography	7-2
7104	Planning Responsibilities	7-3
7105	Coordination of SIGINT Operations	7-3
Section II	SIGINT Operational Planning	7-5
7201	Planning and Direction	7-5
7202	Collection	7-6
7203	Processing and Exploitation	7-7
7204	Production	7-8
7205	Dissemination	7-8
7206	Utilization	7-10
Section III	SIGINT Plans and Orders	7-11
Section IV	Execution	7-12

Chapter 8. Security of Sensitive Compartmented Information

8001	Special Security Officer	8-2
8002	Personnel Security Program	8-2
8003	Physical Security	8-3
8004	Information Systems Security	8-5

Chapter 9. Training

9001	Military Occupational Specialty Training	9-1
9002	Functional Training	9-2
9003	Exercises	9-2
9004	Operational Training Objectives	9-3

Appendices

A	Radio Battalion SIGINT Support Unit Checklist	A-1
B	Marine Corps SIGINT Equipment	B-1
C	SIGINT and SCI Security Management Operations Flowchart	C-1
D	SIGINT Appendix Format	D-1
E	TSCIF Checklist	E-1
F	Glossary	F-1
G	References and Related Publications	G-1

List of Figures

1-1	The Intelligence Cycle	1-7
4-1	Radio Battalion Organization	4-2
4-2	SIGINT Support Unit Elements	4-3
4-3	Notional SSU Fly-In Echelon Configuration	4-6
5-1	EA-6B Prowler	5-2
5-2	VMAQ Organization	5-2
5-3	VMAQ and TERPES Operations	5-3
6-1	Notional MEF SIGINT Operational Architecture	6-3
6-2	Notional MEF Lead Echelon SIGINT Operational Architecture	6-4
6-3	MEU(SOC) CE Afloat SIGINT Operational Architecture	6-5
6-4	MEU(SOC) CE Ashore SIGINT Operational Architecture	6-6
6-5	MEF CE CIC Communications and Information Systems Architecture	6-9
6-6	RadBn SSU Operations Control and Analysis Center Communications and Information Systems	6-10
6-7	VMAQ Operations Center and TERPES Communications and Information Systems	6-11
7-1	MAGTF and Supporting SIGINT Operations	7-13
B-1	AN/ULQ-19(V2)	B-1
B-2	AN/MLQ-36	B-2
B-3	AN/MLQ-36A	B-3
B-4	AN/PRD-12	B-4
B-5	AN/MSC-63A	B-5
B-6	AN/MSC-63A (interior view)	B-5
B-7	Technical Control and Analysis Center Concept of Employment	B-6
B-8	Team Portable Collection System Upgrade	B-8

B-9 Team Portable Collection System COMINT Collection Subsystem B-8
B-10 Team Portable Collection System Analysis Subsystem B-9
B-11 Trojan Spirit II B-10
B-12 RREP SS-1 B-11
B-13 RREP SS-2 B-11
B-14 Rifle-Mounted HIDRAH B-12
B-15 EA-6B Prowler B-14
B-16 AN/TSQ-90D/E(V), TERPES Portable Unit B-14

List of Tables

2-1 Marine Support Battalion Companies 2-2
4-1 Notional MEU(SOC) SSU T/O 4-7
4-2 Notional Fly-In Echelon T/O 4-7
7-1 Emitter Technical Data 7-2

Chapter 1

Fundamentals

All military forces use the electromagnetic spectrum to command and control operating forces acquire targets, guide weapons, and direct supporting arms. These military forces also use the electromagnetic spectrum to collect, process, and report intelligence and to support other administrative and logistics operations. Most facets o military operations involve the use of some device or system that radiates or receives electromagnetic energy via air waves, metallic cable, or fiber optics. Radios, radars, sensors, smart munitions, telephone systems, and computer networks use electromagnetic radiation. Both complex and unsophisticated military organizations depend on these systems and their inherent use of the electromagnetic spectrum. Signals intelligence operations are the principal way to exploit an adversary's use of the electromagnetic spectrum.

1001. What Is Signals Intelligence?

Signals intelligence (SIGINT) is "a category o intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted" (Joint Pub 1-02). Simply, SIGINT is intelligence gained by exploiting an adversary's use of the electromagnetic spectrum with the aim of gaining undetected firsthand intelligence on the adversary's intentions, dispositions, capabilities, and limitations.

a. Communications Intelligence

Communications intelligence (COMINT) is the technical and intelligence information derived from foreign communications by anyone othe than the intended recipient.

b. Electronics Intelligence

Electronics intelligence (ELINT) is the technical and intelligence information derived from foreign noncommunication electromagnetic radiation emanating from anywhere other than nuclear detonations or radioactive sources.

c. Foreign Instrumentation Signals Intelligence

Foreign instrumentation signals intelligence (FISINT) is the technical and intelligence information derived from the intercept of foreign instrumentation signals by anyone other than the intended recipients. (FISINT is primarily strategic in nature and will not be addressed further in this manual.)

1002. Concept of Employment

SIGINT can be employed in tactical situation when the enemy uses electromagnetic spectru communications and/or systems. Optimal employment is against enemy forces that depend on tactical communications and noncommunications for command and control of their operations. SIGINT operations are more difficult against enemy forces that have established more permanent emplacements using land lines or other cabled communications systems.

SIGINT is one of several intelligence disciplines. The other key intelligence disciplines are imagery intelligence (IMINT), human resources intelligence (HUMINT), and measurement and signature intelligence (MASINT).

1003. SIGINT and Electronic Warfare

Electronic warfare (EW) is "any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy" (Joint Pub 1-02). EW denies the enemy use of the electromagnetic spectru for command and control and protects it for friendly command and control. There are three divisions of EW.

a. Electronic Warfare Support

Electronic warfare support (ES) includes actions tasked by or under the direct control of an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated enemy electromagnetic signals for the purpose of *immediate* threat recognition. ES provides information required for immediate tactical decisions and operations such as the identification of imminent hostile actions, threat avoidance, targeting, or electronic attack.

Both SIGINT and ES involve searching for, intercepting, identifying, and locating electronic emitters. The primary differences between the two are the information's intended use, the degree of analytical effort expended, the detail of information provided, and the timeliness required.

SIGINT is used to gain information concerning the enemy, usually in response to a priority intelligence requirement (PIR), an intelligence requirement (IR), or other means. As described in chapter 6, SIGINT support is usually provided to the Marine air-ground task force (MAGTF) as a whole, but may also be provided directly to subordinate elements.

SIGINT information is normally provided to the MAGTF all-source fusion center (AFC) for inclusion into all-source intelligence products and for further dissemination throughout the MAGTF and to external organizations. See Marine Corps Warfighting Publication [MCWP] 2-1, *Intelligence Operations*. SIGINT-derived information of immediate tactical importance that does not require further processing, correlation, or analysi may be passed directly to subordinate commanders or to the operations section or supporting arms element of supported commands, in accordance with United States Signals Intelligence Directive (USSID) 316, *Non-Codeword Reporting Program*, and USSID 240, *ELINT Processing, Analysis, Reporting, and Forwarding Procedures*.

b. Electronic Attack

Electronic attack (EA) is action taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum.

The objectives of SIGINT may conflict with those of EA. For example, EA may be conducted to interfere with the adversary's use of an emitter a the same time as SIGINT operations are designed to exploit the adversary's use of the same emitter. Furthermore, EA operations against one target may disrupt or otherwise interfere with friendly SIGINT collection against the same or differen targets.

SIGINT operations, EA operations, and the MAGTF's overall use of the electromagnetic spectrum for command and control (C2) operations must be carefully coordinated within the MAGTF and with pertinent external organizations. Depending on operational requirements, SIGINT and EA operations coordination and deconfliction may occur within the radio battalion operations control and analysis center (OCAC) within the electronic warfare coordination center (EWCC), or within the MAGTF command element (CE) current operations center (COC).

c. Electronic Protection

Electronic protection (EP) involves the action taken to ensure effective, friendly use of the electromagnetic spectrum despite the enemy's use of EW. Within the MAGTF, SIGINT elements may be tasked to employ similar techniques agains friendly force electronic emitters in order to identify and help eliminate signals security vulnerabilities that could be exploited by an enemy's SIGINT operations.

1004. Threats

a. Enemy Capabilities

The more a combat unit relies on the electromagnetic spectrum, the more vulnerable it is to the enemy's signals intelligence and electronic warfare actions. The enemy can—

- Detect a unit's devices which radiate electromagnetic energy to reveal its identity and location.
- Monitor a unit's communications to reveal its intentions, combat capabilities, logistics and personnel status, and other critical operational and tactical information.
- Inject false information into communications and information systems (CIS) to confuse and mislead a unit.
- Interrupt a unit's use of the electromagnetic spectrum, thereby degrading its ability to receive and process intelligence, plan operations, and execute C2 functions.

b. Countermeasures

To counter threats listed and to enhance effectiveness, Marines must be able to—

- Protect, to the maximum extent possible, the free use of the electromagnetic spectrum and ensure the reliable performance of ou CIS.
- Exploit the enemy's use of the electromagnetic spectrum for intelligence and targeting and intrude into the enemy's CIS and networks.
- Attack the enemy's CIS to adversely affect their decisionmaking process and operations.

1005. All-Source Intelligence and Operations Command Support

Generally, SIGINT is more useful to the commander and the decisionmaking process when has been correlated and fused with information from other intelligence sources and disseminated in easily usable, tailored, all-source intelligence products. Tactical SIGINT operations within the MAGTF, along with other services, theater, and national SIGINT support, make SIGINT a valuable source of information within the overall intelligence effort. SIGINT supports the following six functions of intelligence.

a. Commander's Estimate

SIGINT helps formulate and modify the commander's estimate of the situation by providing information needed to analyze the enemy's C2 operations, identify the current parameters of operating emitters, give insight into enemy intentions, and assess the enemy's intelligence, EW and other military capabilities.

b. Development of the Situation

SIGINT's ability to track enemy emitters and associated units and to obtain indicators of intentions can confirm or refute potential enemy courses of action. SIGINT also helps commanders to better understand the enemy and the battlespace, thereby reducing uncertainty by acquiring information regarding enemy structure, dispositions, locations, movements, and operational activities and patterns.

c. Indications and Warning

SIGINT is often the principal provider of indications and warning (I&W) because adversaries often reveal their intentions, locations, and movements in their communications and other electronic emissions.

d. Force Protection

SIGINT supports force protection by revealing critical intelligence about enemy intelligence, sabotage, subversion, and terrorism and by assessing the vulnerability of friendly C2 and CI operations.

e. Targeting

SIGINT supports targeting by providing key operational and locational intelligence on enemy C2 operations and facilities, weapons systems, force compositions, and dispositions. Information provided through SIGINT can identify high value and high payoff targets and help develop options for attacking these targets. SIGINT also supports all-source intelligence gain and loss assessments of potential enemy targets.

f. Combat Assessment

SIGINT can aid in all-source intelligence support of battle damage assessments by exploiting enemy reports of sustained battle damages and by detecting changes in enemy operations subsequen to friendly attacks.

1006. Capabilities

a. Remote Intelligence

SIGINT operations provide extended-range intelligence without the need for physical presence within or near the surveillance area. The standoff range for SIGINT operations is directly dependent on the characteristics of the terrain in which SIGINT collection is being conducted and the type, operating characteristics, and methods of employment of the enemy's electromagnetic systems. Some enemy electromagnetic systems may require that SIGINT operations be close to the transmission origin, path, or medium. Conversely, other electromagnetic systems may be exploitable from positions farther away from the transmission origin, path, or medium.

(1) Ground SIGINT Elements. Locating ground SIGINT operational elements with friendly combat forces provides the friendly commander with the capability to collect a wide range of intelligence information. Locating SIGINT element with the ground combat element (GCE) forces provides the MAGTF commander with intelligence support for decisionmaking as well as I&W and force protection intelligence reporting to the local unit.

(2) Air-Platform SIGINT Elements. Airborn SIGINT elements can provide direct support to both air and ground operations and significantly enhance collection operations by exploiting enemy targets masked or otherwise unattainable by ground-based elements. These SIGINT elements also support friendly air operations by identifying, locating, and determining the status of enemy surveillance, targeting, and weapons systems and by providing intelligence support to friendly EA operations targeting these enemy systems.

(3) Ship-Based SIGINT Elements. SIGINT elements may operate from ship-based SIGIN operations facilities in support of amphibious operations. Marine and Navy elements operating from ship-based SIGINT facilities may support amphibious operations as a part of the assault force, airborne SIGINT operations, or ship-based SIGINT operations. Within an amphibious task force (ATF), the principal SIGINT facilities are found with ship's signals exploitation spaces (SSESs) located within the intelligence centers of many ships.

b. Target Detection and Identification

SIGINT can detect enemy activity in designated areas and provide a general indication of its type and volume. Analysis of SIGINT information can provide the identity and location of specific enemy units, indications of enemy plans and future operations, and the type, function, and location of specific enemy units and systems.

c. Near-Real-Time Reporting

SIGINT operations can immediately report enemy actions or events critical to the operations of friendly units. Time-sensitive SIGINT reporting to combat units may be via standard MAGTF

intelligence communications channels or any available direct communications means.

d. Continuous Operations

SIGINT operations are conducted on a 24-hou basis. The size and composition of SIGINT forces along with the supported commander(s)'s concept of operations will influence the scope, services and capabilities of SIGINT operations.

e. Stealth

SIGINT operations are a passive intelligence technique and can usually be conducted withou the enemy's knowledge or detection. EW operations include both active and passive techniques and, depending on implementation, may or may not be recognized by the enemy.

f. Flexibility

Marine SIGINT operations may be employed in a variety of means to support the MAGTF concept of operations and supporting intelligence operations. SIGINT elements may be deployed with advance forces or forward ground units; they may be aboard air platforms or ship-based. Additionally, Marine SIGINT elements routinely operate with joint and other service elements. These elements are effective at leveraging their capabilities in support of MAGTF requirements.

1007. Limitations

a. Enemy System

The primary value of SIGINT operations is against enemy systems using electromagnetic spectrum system transmissions. SIGINT operations are ineffective against systems that do no use radio frequency (RF) transmissions (e.g., fiber optics, land-line telephone systems, or other cabled systems). If the enemy conducts operations under enemy emission control (EMCON) conditions (e.g., radio silence), SIGINT operations will not be effective.

b. Terrain Masking

Heavily wooded and urban areas reduce the susceptibility of enemy transmissions to SIGINT collection. In these areas, generally, SIGINT elements must be closer to the enemy's transmission origin or medium. Mountainous or very hilly terrain also inhibits SIGINT operations (particularly ground-based operations) by effectively blocking enemy signals from detection.

c. Complex Signals

Enemy signals that are complex or encrypted reduce the intelligence information available from the transmission. Complex signals (i.e., frequency hoppers) require special equipment for intercep and signals analysis. Encrypted signals require deciphering to reveal intelligence information. Deciphering simple encryption methods may be possible, but an enemy's use of complex encryption methods is currently beyond the scope of tactical SIGINT elements.

d. SIGINT versus Electronic Attack

SIGINT operations may be affected when enemy signals are being jammed. Prior to initiating EA jamming operations, consideration must be given to the intelligence value of the enemy's signal and the effects of its loss.

1008. Organization

Within the Marine Corps, the units responsible for the conduct of tactical SIGINT are the two radio battalions and the four Marine tactical electronic warfare squadrons.

a. Radio Battalion

The radio battalion (RadBn) provides tactical SIGINT, electronic warfare, communications security monitoring and analysis, and special communications operations in support of the MAGTF. A variety of employment concepts may be used depending upon the situation. Refer to chapter 4 for a detailed description of RadBns.

b. Marine Tactical Electronic Warfare Squadron

The Marine tactical electronic warfare squadron (VMAQ) conducts tactical electronic reconnaissance and ELINT operations in support of the MAGTF.

The VMAQ provides—

- ELINT collection operations to maintain the electronic order of battle, including identification of selected emitters and location o nonfriendly emitters.
- Threat warnings for friendly aircraft, ships, and ground units.
- Intelligence support to prevent, delay, or interrupt detection and tracking by enemy early warning, acquisition, and fire or missile control radars of aviation combat elemen (ACE) operations and Marine EA-6B tacti cal jamming aircraft in support of strike aircraft.

Refer to chapter 5 for a detailed description of the VMAQ.

1009. Command and Control

a. Radio Battalion

The RadBn (or RadBn detachment) is generally a subordinate command of, or attached to, the MAGTF CE. The MAGTF commander has operational control (OPCON) of the RadBn (or RadBn detachment).

(1) Staff Cognizance. The MAGTF commander exercises C2 over the RadBn or its detachments via the MAGTF intelligence officer. Such a relationship allows for the centralized direction and effective integration of SIGINT operations within the MAGTF's broader all-source intelligence concept of operations. RadBn's EW operations fa under the staff cognizance of the MAGTF operations officer, requiring close coordination and integration among the intelligence staff officer (G-2/S-2), operations staff officer (G-3/S-3), and communications and information systems officer (G-6/S-6) to achieve optimum employment of RadBn.

(2) Support Relationships The RadBn most typically operates in general support of the MAGTF. However, RadBn or its elements may be employed in direct support of any of the MAGTF's major support elements, i.e., GCE and ACE. In such cases, the scope of the supported commander's control over assigned RadBn elements usually is specified to ensure effective support of operations while allowing the MAGTF commander to maintain effective control of broader intelligence and SIGINT operations.

b. Marine Tactical Electronic Warfare Squadron

VMAQ or its detachments are subordinate to the ACE and under the OPCON of the ACE commander.

(1) Staff Cognizance. The ACE commander will usually exercise C2 over VMAQ via the ACE operations officer or tactical air command center (TACC). The ACE intelligence officer will exercise staff cognizance over VMAQ ELINT activities beyond that required to support EA missions.

(2) Support Relationships. VMAQ elements principally operate in direct support of ACE operations or other designated commanders (e.g., the joint force air component commander). However, ELINT acquired during VMAQ operations is capable of being used in general support of MAGTF elements and supporting intelligence operations.

1010. Operations

RadBn and VMAQ conduct both COMINT and ELINT operations to varying degrees. RadBns conduct predominantly COMINT operations; they also ensure rapid dissemination of fused ELIN and COMINT from organic or external sources to the G-2/S-2 and subordinate commanders. The VMAQ's main focus is ELINT and ES.

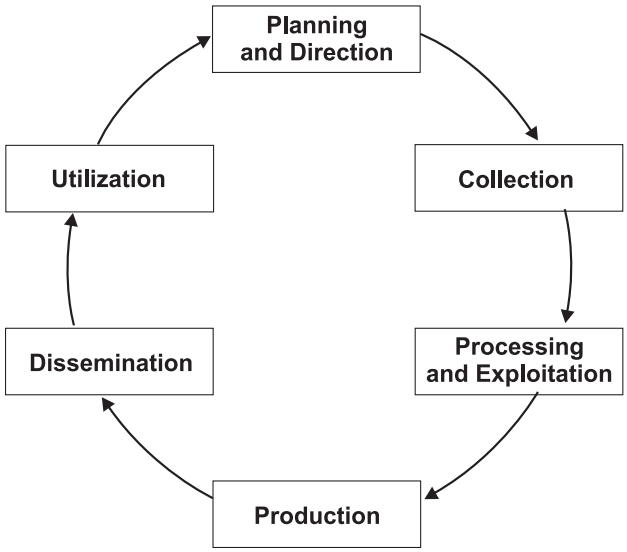


Figure 1-1. The Intelligence Cycle.

To complete intelligence tasks, RadBn an VMAQ incorporate the six intelligence cycle phases into their SIGINT methodology (see figure 1-1). Products of the SIGINT cycle are disseminated to commanders and others through the MAGTF intelligence officer. RadBn and VMAQ also provide SIGINT products to other Service and agencies as directed.

a. Planning and Direction

SIGINT direction is a continuous process that encompasses the tactical and technical employment of SIGINT assets. It begins on receipt of a warning order, initiating directive, or establishment of a planning objective and continues until termination of the mission. SIGINT unit commanders closely coordinate their operations with the MAGTF intelligence officer and pertinent external intelligence and SIGINT elements.

Planning and direction involves—

- Determining PIR and IR and SIGINT requirements to support them.
- Preparing supporting SIGINT collection, production, and dissemination plans.
- Issuing orders and requests to SIGINT units.
- Checking continuously on the productivity and effectiveness of SIGINT collectors, producers, disseminators, and other SIGINT elements and agencies.

b. Collection

During collection, organic, attached, and supporting SIGINT elements detect, collect, and record COMINT and ELINT data. The collected COMINT and ELINT data is then delivered to the appropriate SIGINT processing or production element. The OCAC is the processing and production element for RadBn, while the Tactical Electronic Reconnaissance Processing and Evaluation System (TERPES) is VMAQ's processing and production element. In some instances, such as immediate threat information, PIRs and supporting reporting criteria may direct the SIGINT collector to disseminate SIGINT reports directly to the local commander (e.g., an infantry maneuver element) for immediate support to operations.

c. Processing and Exploitation

SIGINT processing consists of converting and formatting raw signals data to a form that is usable in follow-on SIGINT and all-source intelligence analysis. The processing and exploitation phase is usually not a discrete function, but rather one that is accomplished during collection. Once the collected information has been processed, analysis must determine its significance. Other intelligence information may also be fused together with the processed SIGINT to give a comprehensive picture and to show how the information can be used by the commander to gain an advantage.

d. Production

The production stage involves converting the SIGINT analysis into appropriately tailored SIGINT reports and all-source intelligence product that can be easily understood by the commander and other users. Specifically formatted standardized messages, graphics, and other intelligence products are required to familiarize these user with layout and content and to ensure rapid usage and automated processing of finished reports. Within the MAGTF, the RadBn OCAC and the VMAQ TERPES produce SIGINT reports and products, and the MAGTF AFC incorporates

SIGINT products and information into all-source intelligence products.

e. Dissemination

Dissemination is the process through which SIGINT products are delivered to MAGTF users: the MAGTF commander, subordinate commanders and their staffs, and others as appropriate (e.g. joint force commander, joint components, and various theater and national organizations and intelligence agencies). SIGINT products are disseminated via dedicated SIGINT or general purpose CIS channels according to available CIS resources, the classification of the product, and the intelligence dissemination plan. These products include time-sensitive voice reports, text reports, data base updates, and web-based resources (e.g., via the MAGTF sensitive compartmented information local area network).

f. Utilization

SIGINT must be exploited to have value. Commanders, G-2/S-2s, G-3/S-3s, and other principal staff officers must continuously evaluate SIGINT products for timeliness, usefulness, and overa quality and provide feedback to the intelligence officer and SIGINT elements.

1011. Commanders' Responsibilities

MAGTF commanders are responsible for the planning and direction, collection, processing production, dissemination, utilization, and security of all SIGINT information by units under their command. The Director, National Security Agency (DIRNSA), delegates SIGINT operational tasking authority (SOTA) to MAGTF commanders by name for the duration of an operation o other specified period of time. SOTA allows the designated commander to task and direct the operations of organic or attached SIGINT units. Additional information regarding SOTA may be found in USSID 4, *Concept of SIGINT Support to Military Commanders*.

Commanders are also responsible for planning integrating, and using SIGINT support, if available, from other United States or allied nationa and military SIGINT organizations. The commander's primary responsibilities fall into the following areas.

a. Tasking and Directing

The commander possessing SOTA is responsible for the effective tasking and operation of assigned SIGINT assets. Generally, once a commander determines the intelligence requirements, the G-2 S-2, with the advice and assistance of the intelligence operations officer and SIGINT officer (SIO), decides which requirements can be satisfied via organic SIGINT operations. SIGINT unit commanders or officers in charge (OICs) will also coordinate operations with other key staff officers within the intelligence section (i.e., the collections manager, the AFC OIC, the surveillance and reconnaissance center OIC, and the dissemination manager). The G-2/S-2 passes these IRs as taskings to the commanding officer (CO) or OIC o the organic or attached SIGINT unit (e.g., a RadBn unit). These requirements will be in the form of either PIRs or IRs. PIRs and IRs are further managed within the intelligence effor through the use of intelligence collection requirements (ICRs), intelligence production requirements (IPRs), and intelligence dissemination requirements (IDRs) in order to achieve effective, mutually supporting all-source intelligence operations (see MCWP 2-1, chapter 3, for detailed information on IR management). The SIGINT unit commander is then responsible for commanding and controlling resources to accomplish the assigned mission. This process is discussed further in chapter 7.

b. Reporting

The ultimate goal of tactical SIGINT operations is the timely and usable production of SIGINT information which answers the MAGTF commander's PIRs and other MAGTF IRs. SIGINT reports are discussed in detail in chapter 7.

c. Protecting

The MAGTF commander is responsible for safeguarding SIGINT personnel, facilities, and information used or produced by units within the command. Loss of SIGINT units and capabilities by destruction or capture and unintended disclosures of SIGINT operations may result in severe losses of MAGTF capabilities. The effectiveness of SIGINT depends on the ability to maintain security and conceal SIGINT techniques and success from the adversary. Accordingly, the commander must provide adequate protection to prevent the capture of SIGINT facilities and personnel. In addition, special intelligence courier must be adequately protected, and positive measures must be taken to conceal courier runs and routes. To meet this responsibility, the MAGT commander must satisfy the following four basi security requirements.

(1) A special security officer (SSO) must be appointed in all units authorized to receive and use SCI. The SSO is under the staff cognizance of the unit intelligence officer and is responsible for the operation of the SCIF and the security, control, and use of SCI within the SCIF. Marine expeditionary force (MEF) CEs, Marine divisions, Marine aircraft wings, force service support groups, and other designated organizations have SSOs. Other SSOs may also be appointed as needed during tactical operations or whenever a TSCIF is established.

(2) Sensitive compartmented information (SCI generally must be handled, processed, or stored only in a SCI facility (SCIF). This may be either a mobile tactical SCIF (TSCIF) or a permanent facility. SCI security requirements are discussed in greater detail in chapter 8.

(3) Persons who handle or use SIGINT information must have proper security clearances and be indoctrinated for access to SCI and any additional required accesses. Access to SCI will be governed by need-to-know requirements. Unit commanders are responsible for determining who requires SCI access. At a minimum, all unit staff principals and key functional planners should have SCI access.

(4) SCI-secure CIS means for handling and transmitting special intelligence and SIGINT-related information must be available. These include SCI voice circuits, SCI record communications, SC local area networks (LANs), and Joint Worldwide Intelligence Communications System (JWICS).

d. Training

The MAGTF commander is responsible for ensuring that staff and operating forces are trained to effectively use SIGINT and to protect themselves against enemy SIGINT efforts.

(reverse blank)

Chapter 2

SIGINT Responsibilities in the Supporting Establishment

RadBns and VMAQs are the principal SIGINT units within the operating forces. These units are addressed further in chapters 4 and 5. To effectively execute their missions, MAGTFs, RadBns, and VMAQs draw on a wide range of external organizations to provide personnel and equipmen resources, training opportunities, and unique SIGINT support. To understand how MAGTF SIGINT operations can be supported externally, it is necessary to understand the missions and functions of external SIGINT organizations and how they provide operational support to the MAGTF.

2001. Marine Corps SIGINT Organization

a. Headquarters Marine Corps

Headquarters Marine Corps (HQMC) is responsible for the internal organization, training, equipping, and readiness of the Marine Corps; for the operation of its material support system; and for the total performance of the Marine Corps. The Assistant Chief of Staff, Command, Control, Communications, Computers, and Intelligence Department (C4I), has the following SIGINT responsibilities:

- Formulates Marine Corps SIGINT plans and policies and participates in the formulation of joint and combined plans, policies, and related command relationships.
- Determines present and future SIGINT active and reserve personnel requirements, both quantitative and qualitative.
- Provides final authority on validation and approval of all personnel augmentation from non-Fleet Marine Force (FMF) resources to support MAGTF operations.
- Reviews the internal organization, training requirements, and readiness of all SIGIN elements of the Marine Corps. The internal organization of Marine Corps SIGINT elements is constantly reviewed, with particular emphasis on occupational field (OccFld) military occupational specialty (MOS) skill requirements, to ensure requisite skills and training are available to meet MAGTF operational needs.

b. Marine Support Battalion

The Marine support battalion (MarSptBn) is a special supporting activity that provides for Marine Corps participation in national and Department of the Navy (DON) cryptologic activities. (SIGINT operations within the Navy are generally referred to as *cryptologic* operations This term may generally be used synonymously with the term *SIGINT*.) Marines in MarSptBn are assigned to national and theater organizations that support both deployed and in-garrison MAGTFs with routine and time-sensitive, mission-critica SIGINT support. Additionally, these Marines learn national-level SIGINT collection, production, and dissemination systems and benefit from SIGINT skills training available only at these sites.

(1) Commanding Officer. The principal functions and tasks assigned to the CO, MarSptBn, include the following:

- Coordinate the withdrawal of MarSptBn Marines to augment MAGTFs in response to global-sourcing requests.
- Support Marine Corps SIGINT requirements through interface at the National Security Operations Center (NSOC) and regional security operations centers

(RSOCs). (Refer to paragraph 2003 for a detailed discussion of these organizations.)

- Manage and administer the reserve SIGINT program to provide augmentation to active duty SIGINT forces.
- Provide for entry-level skills qualification and skills progression training of Marine SIGINT personnel.

(2) Battalion Headquarters. The battalion headquarters, collocated with Commander, Naval Security Group (CNSG), Fort Meade, Maryland, provides command, administrative, and Marine Corps-unique logistics support for the battalion and Marine Corps personnel in various Naval Security Group (NSG). It is under the military command and management control of the Commandant of the Marine Corps (CMC) and under the staff cognizance of the Assistant Chief of Staff, C4I, HQMC.

(3) Letter Companies. MarSptBn's letter companies support the naval mission of the Naval Security Group Activity (NSGA) to which they are assigned as well as provide for the unique service support of assigned Marines (see table 2-1). The letter companies are under the military command and administrative control of the CO, MarSptBn, while under the OPCON and technical direction of the CO of the NSGA site each supports.

(4) Company K. Company K, MarSptBn, provides administration for Marine students and staff assigned to the Naval Technological Training Center (NTTC), Pensacola, Florida, and provides liaison and instructors in conjunction with SIGINT training.

2002. SIGINT Organizations in Other Military Services

Services man, train, and equip organic SIGIN forces to support their operational commander and to prepare to participate in joint, theater, national, and combined operations. Each Service has a service cryptologic element (SCE) headquarters that provides SIGINT management, guidance, and oversight. The National Security Agency (NSA) maintains SIGINT operational control of each SCE.

Table 2-1. Marine Support Battalion Companies.

Company	Site/Host	Location
Headquarters Company	NSG	Ft. Meade, Maryland
Company A	NSGA Denver	Buckley Air National Guard Base, Aurora, Colorad
Company B	NSG	Ft. Meade, Maryland
Company D	NSGA Ft. Gordon	Ft. Gordon, Georgia
Company E	NSGA Misawa	Misawa Air Force Base (AFB), Japan
Company F[1]	NSGA Rota	Rota, Spain
Company G	NSGA Menwith Hill	Royal Air Force Menwith Hill, England
Company H	NSGA San Antonio	Kelly AFB, San Antonio, Texas
Company I	NSGA Kunia	Kunia, Hawaii
Company K	NTTC Corry Station	Pensacola, Florida
Company L	NSGA Guantanamo	Guantanamo Bay, Cuba
[1]Company F is scheduled for deactivation 30 June 1999.		

a. Naval Security Group

NSG is the DON's SCE. It directly supports deployed MAGTFs by providing access to—

- SSES use with MAGTF SIGINT personnel while embarked.
- Direct support to MAGTF operations with NSG elements operating aboard Navy ships or aircraft.
- Direct service support to MAGTF operations from ashore NSG facilities in the theater of operations.
- Hardware, software, specialized equipment, and training to the RadBns.
- SIGINT technical support kits from regionally focused cryptologic shore support activities.

b. United States Army Intelligence and Security Command

United States Army Intelligence and Security Command (INSCOM) is the Army's SCE. It provides support to deployed MAGTFs when—

- Marines are part of a joint force that includes Army SIGINT units.
- Marines are serving as part of a larger force that includes adjacent Army units.
- Army theater fixed-site activity or mobile SIGINT asset can provide support.

c. Air Intelligence Agency

Air Force Intelligence Agency (AIA) is the Ai Force's SCE. Its elements support deployed MAGTFs by collecting and producing air intelligence or by providing SIGINT support for air and air defense operations.

2003. National SIGINT Organizations

a. National Security Agency

In order to provide timely, effective SIGINT support to military commanders, NSA established several tailored support mechanisms.

(1) National Security Operations Center.

The NSOC supports JTF and MAGTF operations by providing SIGINT reporting derived from national assets. The NSOC functions as the current operations and crisis management center of the NSA to ensure that time-sensitive SIGINT needs of commanders are satisfied. The NSOC works closely with the National Military Command Center (NMCC) and other Department of Defense (DOD) I&W watch centers.

(2) Regional Security Operations Centers.

NSA established three RSOCs to enhance SIGINT support to combatant commanders at all echelons. RSOCs are regionally focused and receive inputs from multiple sources. The RSOCs are located at Fort Gordon, Georgia; San Antonio, Texas; and Kunia, Hawaii.

The following organizations are established at each RSOC:

- NSG established a cryptologic shore support activity (CSSA) staffed with Marine and Navy personnel at each RSOC. CSSAs provide direct support to naval tactical operations through interface with the RSOC. This interface allows greater tailoring of RSOC operations supporting the intelligence requirements of MAGTF operations. Principal communications connectivity to CSSAs i provided by Navy communications systems within SSES.
- INSCOM established a technical control and analysis element (TCAE) at each of the RSOC locations. CSSA Marine personne interface with TCAE personnel to provide ground-oriented intelligence information in support of the MAGTF. Communication connectivity with the TCAEs is provided generally via the Trojan Spirit II communications system organic to the RadBns or communications battalions.

b. National Reconnaissance Office

The National Reconnaissance Office (NRO) provides critical support to United States SIGINT operations. NRO's mission is to enable United States global information superiority during peace

and war. NRO is responsible for unique and innovative technology, large-scale systems engineering, development and acquisition, and operation of space reconnaissance systems and related intelligence activities to support global information superiority. NRO's capabilities include supporting I&W, monitoring arms control agreements and supporting military operations. The NRO accomplishes its mission through ongoing research and development, acquisition, and operation o spaceborne and airborne intelligence data collection systems. NRO assets and capabilities may be requested to support MAGTF operations unde procedures described in the *Joint Tactical Exploitation of National Systems (J-TENS) Manual*.

Chapter 3

SIGINT Responsibilities in the MAGTF

The MAGTF commander is ultimately responsible for the conduct of MAGTF SIGINT operations. The MAGTF commander's staff, major subordinate commands (MSCs), specialized units, and theater or national level organizations assist the commander in execution of SIGINT responsibilities. This chapter focuses on the roles and responsibilities of Marine operating forces' staffs, MSCs, and specialized units.

3001. Commanders, Marine Corps Forces

Commanders, Marine Corps forces (COMMARFORs), are responsible for using their organic SIGINT assets effectively and for ensuring responsive national and theater support to subordinate commands. COMMARFORs—

- **Review and validate SIGINT support requests from subordinate commands and ensure they receive the tailored support they require.**
- **Review and comment on cryptologic support plans (CSPs) prepared by NSA and theater combatant commanders for MAGTF operation plans (OPLANs).**
- **Coordinate SIGINT issues and requirements with the theater and national agencies in support of Marine Corps forces (MARFOR).**
- **Coordinate with theater and national SIGINT and all-source intelligence agencies and organizations to support MARFORs.**
- **Review, exercise, and if necessary, develop, interoperable CIS architectures to support the SIGINT effort.**
- **Coordinate between MARFOR and their subordinate commands to improve SIGINT interoperability, standardization, preparedness, and performance.**

3002. MAGTF Staff Sections

a. G-2/S-2

All MAGTF intelligence and counterintelligence activities, to include SIGINT, are under the staff cognizance of the unit G-2/S-2. Within the bounds of the commander's SOTA, the G-2/S-2 is responsible for planning, directing, managing, and supervising the tasking and operations of SIGINT units organic to and supporting the MAGTF. The G-2/S-2—

- **Develops and satisfies outstanding PIRs and IRs by planning, directing, integrating, and supervising organic SIGINT operations and other MAGTF all-source intelligence operations.**
- **Prepares MAGTF SIGINT plans and orders.**
- **Coordinates SIGINT collection (to include SIGINT amplifications and SIGINT time sensitive requirements), production, and dissemination requirements that are beyond the capability of the MAGTF and submits them to higher headquarters for JTF, theater, o national SIGINT support.**
- **Ensures routine and time-sensitive SIGINT information is rapidly processed, analyzed, and incorporated in all-source intelligence products, and rapidly disseminates this information to MAGTF and external units.**
- **Evaluates JTF, theater, and national SIGINT support to the MAGTF and adjusts stated requirements if necessary.**
- **Identifies, validates, and assists with resolution of SIGINT personnel and equipment resources deficiencies (e.g., insufficient linguists and special signal analysts expertise).**
- **Incorporates SIGINT in training exercises to improve MAGTF individual, collective, and unit readiness.**

b. G-1/S-1

The manpower or personnel staff officer (G-1/S-1) is responsible for all SIGINT personnel requirements. Often it is necessary to augment organic SIGINT units with specially-trained personnel from outside the command. The G-1 S-1 either internally sources or forwards personnel augmentation requests developed by the G-2/S-2 to higher headquarters for action.

c. G-3/S-3

The G-3/S-3 is responsible for planning, coordinating, and supervising the tactical employmen of units. The G-3/S-3 coordinates the movement and operations of SIGINT units with the G-2/S-2 for integration in current and future operations planning. Because SIGINT units also provide certain EW capabilities, the G-3/S-3, normally via the electronic warfare officer (EWO), coordinates SIGINT units' tactical positioning to provide tactical EW and command and control warfare (C2W) support. Normally, as the principal staf SIGINT user, the G-3/S-3 has the primary responsibility for planning maneuver operations and fire support, which requires close coordination throughout the planning process to ensure effective SIGINT support.

d. G-4/S-4

The logistics staff officer (G-4/S-4) is responsible for the combat service support (CSS) of MAGTF SIGINT units. To ensure the required support i available, the G-4/S-4 develops CSS arrangements to meet the needs of the deployed SIGINT units (particularly SIGINT units' unique equipment logistics requirements).

e. G-6/S-6

The G-6/S-6 is responsible for providing and protecting internal and external MAGTF CIS connectivity and operations. The G-6/S-6—

- Coordinates or provides communication paths, network accesses, and frequencies for SIGINT organizations attached to and/or supporting the command.
- Provides representation for CIS matters within the EWCC, when it is established.
- Assists the unit security manager and G-3/S-3 in promoting personnel awareness o enemy SIGINT threat capabilities, signals security training, and unit signals security preparedness.

3003. MAGTF Intelligence Section Elements

The MAGTF intelligence section, resident in the MAGTF CE, is the focal point for MAGTF SIGINT planning and direction and is supported by the combat intelligence center (CIC). Depending on the size of the MAGTF, operational requirements or other factors, the CIC may consist of a number of subordinate elements.

a. Combat Intelligence Center

The CIC is established within the MAGTF CE. Performing the primary functions of the MAGTF intelligence section, the CIC includes the following subelements.

(1) All-Source Fusion Center The AFC is the primary MAGTF analysis and production element. It processes and produces all-source intelligence products in response to MAGTF requirements.

(2) Surveillance and Reconnaissance Center. The surveillance and reconnaissance cente (SARC) is the primary element for the supervision of MAGTF collection operations. It directs, coordinates, and monitors intelligence collections operations conducted by organic, attached, and direct support collection assets.

(3) Operations Control and Analysis Center. The OCAC is the main node for the command and control of RadBn SIGINT operation and the overall coordination of MAGTF SIGINT operations. It processes, analyzes, produces, and disseminates SIGINT-derived information and directs the ground-based EW activities of the RadBn.

b. Intelligence Section and SIGINT Unit Commanders and Officers in Charge

(1) Intelligence Operations Officer. The intelligence operations officer is responsible to the G-2/S-2 for the overall planning and execution of MAGTF all-source intelligence operations. The intelligence operations officer—

- Plans and implements a concept of intelligence operations based upon the mission threat, commander's intent, and concept of operations.
- Develops, consolidates, validates, and prioritizes recommended PIRs and IRs to support MAGTF planning and operations.
- Plans, develops, and directs MAGTF intelligence collections, production, and dissemination plans, to include the effective employment and integration of MAGTF multidiscipline intelligence and reconnaissance operations.
- Coordinates and integrates MAGTF intelligence operations with other components, JTF, theater, and national intelligence operations.
- Evaluates and improves MAGTF intelligence operations.

(2) SIGINT Officer. The SIO is responsible to the MAGTF G-2/S-2 for the planning, direction, and execution of MAGTF SIGINT operations. The SIO—

- Coordinates with other intelligence section staff officers, the RadBn CO or OIC, and the ACE G-2/S-2 (for VMAQ TERPES operations) to prepare SIGINT plans and order for the MAGTF.
- Coordinates with the collection management officer and RadBn and VMAQ TERPES planners to coordinate, plan, supervise, and assist SIGINT collection requirement and taskings for MAGTF operations.
- Coordinates with the SARC OIC, RadBn CO or OIC, VMAQ TERPES OIC, and G-3/S-3 to coordinate the movement, operation, and reporting of SIGINT units.
- Coordinates with MAGTF AFC OIC, RadBn CO or OIC, and VMAQ TERPES OIC to coordinate MAGTF AFC analyst exchanges with RadBn TERPES COMINT and ELINT analysts and to coordinate the integration of SIGINT with all-source intelligence production.
- Coordinates with the dissemination officer to plan for the timely reporting of SIGINT-derived intelligence to MAGTF and external elements and the rapid handling of perishable SIGINT information.
- Coordinates with the G-6/S-6, Marine division (MARDIV) OICs, Marine aircraft wing (MAW) special security communications teams (SSCTs), and SIGINT unit OICs to plan and coordinate special intelligence communications paths and operations.
- Assists the intelligence operations officer with preparing and presenting special intelligence briefings and reports as required.

(3) Special Security Officer. The SSO is responsible to the commander for ensuring the command's adherence to SCI regulations and policies, security clearance procedures, and SCI materia handling. Generally, the SSO is the unit's senior intelligence officer. The SSO—

- Establishes and/or maintains a SCIF or TSCIFs to support SIGINT and other compartmented operations.
- Ensures that the command and all subordinate organizations have sufficient SCI billets to meet all potential operational requirements, to include the administration and management of unit SCI billets and SCI security investigations.
- Provides oversight, training, and supporting procedures for the conduct of SCI sanitization and dissemination within the MAGTF. This includes the determination of applicable authority for sanitization and authorized recipients of the sanitized material.

(4) Collections Management Officer. The collections management officer (CMO) is responsible for formulating detailed ICRs and tasking and coordinating internal and external collection operations to satisfy the requirements. The CMO receives PIRs and IRs from the intelligence operations officer and develops an integrated collection plan using organic and supporting resources.

In coordination with the SIO and SIGINT unit COs or OICs, the CMO—

- Determines and coordinates ICRs that may be tasked to organic or supporting SIGINT elements.
- Identifies ICRs and prepares requests for intelligence that are beyond organic capabilities and that must be submitted to higher headquarters and external agencies for satisfaction.

(5) MAGTF All-Source Fusion Center Officer in Charge. The MAGTF AFC OIC is primarily responsibile for managing and supervising the MAGTF's all-source intelligence production and processing effort. The MAGTF AFC OIC—

- Determines and coordinates MAGTF IPRs, to include SIGINT element products as well as all-source intelligence products.
- Maintains all-source automated intelligence data bases, files, workbooks, country studies, planning imagery, mapping and topographic resources, and other references.
- Administers, operates, and maintains intelligence processing and production systems both general service (GENSER) and SCI, e.g., joint deployable intelligence support system (JDISS) and intelligence analysis system (IAS).
- Analyzes and fuses all-source intelligence into tailored products in response to stated or anticipated PIRs and IRs, to include sanitized SCI products.
- Develops and maintains current and future intelligence situational, threat and environmental assessments, and target intelligence based upon all-source analysis, interpretation, and integration.

(6) Surveillance and Reconnaissance Center Officer in Charge. The SARC OIC is responsible for coordinating and supervising the execution of the integrated organic, attached and direct support intelligence collection, and reconnaissance operations. The SARC OIC—

- Maintains the status of the following ongoing intelligence collection operations, to include deployed RadBn collection and direction finding teams:
  - Mission of all teams.
  - Locations and times of all restricted fire areas and reconnaissance areas of operations.
  - Time and method of radio reconnaissance team (RRT) insertion and extraction.
  - Primary and alternate communications plans.
  - Time of last contact.
  - Time of next contact.
- Coordinates and monitors the insertion and extraction of SIGINT and other intelligence elements.
- Coordinates RadBn and VMAQ TERPES elements' collection and reporting activities under the overall intelligence operations plan. Ensures SIGINT elements understand the collection plan and are able to carry out their responsibilities under the plan.
- Ensures other MAGTF C2 nodes (e.g., the current operations center, the fire support coordination center) are apprised of ongoing intelligence and reconnaissance operations.
- Receives routine and time-sensitive intelligence reports from deployed SIGINT collection teams; cross-cues or exchanges intelligence reports with other intelligence collectors, as appropriate; and rapidly disseminates intelligence to MAGTF C2 nodes and others in accordance with intelligence reporting criteria and dissemination plans.

(7) Dissemination Officer. The dissemination officer is responsible for the effective conduct of

intelligence dissemination within the MAGTF. The dissemination officer—

- Determines and coordinates MAGTF IDRs, to include all-source IDRs as well as intelligence discipline-unique requirements.
- Recommends dissemination priorities.
- Advises on and selects dissemination means.
- Develops intelligence dissemination plans and coordinates with the G-6/S-6 supporting CIS architectures for both voice and data networked communications. Coordinates and integrates these plans and architectures with theater, joint force, and MAGTF CIS and intelligence plans and architectures.
- Monitors the flow and ensures timely delivery of intelligence throughout the MAGTF.

(8) SIGINT Unit Commanding Officer or Officer in Charge. The SIGINT unit CO or OIC is responsible for the effective conduct o SIGINT operations in support of the commander's intent and the operational and intelligence concept of operations. The SIGINT unit CO or OIC—

- Plans and employs SIGINT resources in response to the commander's intent, threat situation, MAGTF G-2/S-2's guidance a direction, and intelligence operations plan.
- Effects technical direction and control of MAGTF organic SIGINT collection, processing and exploitation, production, and dissemination operations. Also helps coordinate MAGTF SIGINT operations with JTF, theater, national, and other Service SIGINT agencies.
- Coordinates movement and operations of SIGINT units with MAGTF staff element and subordinate units' commanders. Ensures that all element movements are coordinated with the COC, fire support coordination center (FSCC), and SARC.
- Advises the G-2/S-2, SIO, intelligence operations officer, MAGTF AFC OIC, CMO, and dissemination officer on SIGINT employment and its integration with JTF, theater, and national SIGINT operations.

3004. Marine Divisions and Aircraft Wings

SIGINT activities of the MARDIVs and MAWs come under the staff cognizance of the respective G-2s. This includes the integration of SIGINT operations and products in support of unit operations and the operations of their organic SSCT. SSCTs provide special intelligence (SI) communications support to their commanders and designated subordinate elements.

3005. Radio Battalions

The 1st and 2d RadBns are the Marine Corps' principal organic, tactical, SIGINT direct support elements. The primary mission of the RadBn and its detachments is to provide tactical SIGINT support to MAGTFs. RadBns are discussed further in chapter 4.

3006. VMAQs

VMAQs of Marine aircraft group (MAG)-14 perform airborne electronic reconnaissance and, through the use of TERPES, produce ELINT reports and electronic order of battle (EOB) intelligence. Due to the unique capabilities of TERPES, the ACE will often be tasked with producing and maintaining the EOB to be used by all MAGT elements. VMAQs are discussed in chapter 5.

(reverse blank)

CHAPTER 4

Radio Battalion

The mission of radio battalions is to provide communications security (COMSEC) monitoring, tactical SIGINT, EW, and SI communication support to the MAGTF.

4001. Tasks

The radio battalion—

- **Conducts interception, radio direction finding (DF), recording, and analysis of communications and noncommunications signals and SIGINT processing, analysis, production, and reporting.**
- **Conducts EW against enemy or other hostile communications.**
- **Assists in the protection of MAGTF communications from enemy exploitation by conducting COMSEC monitoring, analysis, and reporting on friendly force communications.**
- **Provides SI communications support and cryptographic guard (personnel and terminal equipment) in support of MAGTF command elements and RadBn operations. (Normally, communications connectivity for SI communications is provided by the communications unit supporting the MAGTF CE.)**
- **Provides task-organized detachments to MAGTFs with designated SIGINT, EW, SI communications, and other required capabilities.**
- **Exercises technical control and direction over MAGTF RadBn SIGINT and EW operations.**
- **Provides RRT with specialized insertion and extraction capabilities (e.g., combat rubber raiding craft, fast rope, rappel, helocast, static line parachute) to provide specified SIGINT and EA support during advance force, preassault, or deep postassault operations.**
- **Coordinates technical SIGINT requirements and exchanges SIGINT technical information and material with national, theater, joint, and other SIGINT units.**
- **Provides intermediate, third- and fourth-echelon maintenance of RadBn SIGINT and EW equipment.**

4002. Organization

The 1st RadBn, Marine Corps Base (MCB), Kaneohe Bay, Hawaii, is subordinate to Commander, Marine Corps Forces, Pacific (COMMARFORPAC), and supports both I and III MEFs. The 2d RadBn, Camp Lejeune, North Carolina, is subordinate to II MEF. Both battalions are organized and equipped along functional lines to provide administrative control of subordinate elements, to facilitate training, and to permit rapid structuring and operational deployment o task-organized units or detachments.

The 1st RadBn is organized into a headquarter and service (H&S) company and three line companies (A, B, and C). The 2d RadBn is comprised of an H&S company and two line companies (A and B). See figure 4-1 on page 4-2. RadBns' line companies are not tactical organizations, but instead they serve as training and administrative units providing the basic unit structure around which task-organized SIGINT support units o detachments are trained, equipped, and formed Even if the entire RadBn were to deploy, it would task-organize for the mission assigned.

a. Headquarters and Service Company

The H&S company provides personnel and facilities with which the RadBn commander commands and controls battalion operations. It also provides service support for other battalion

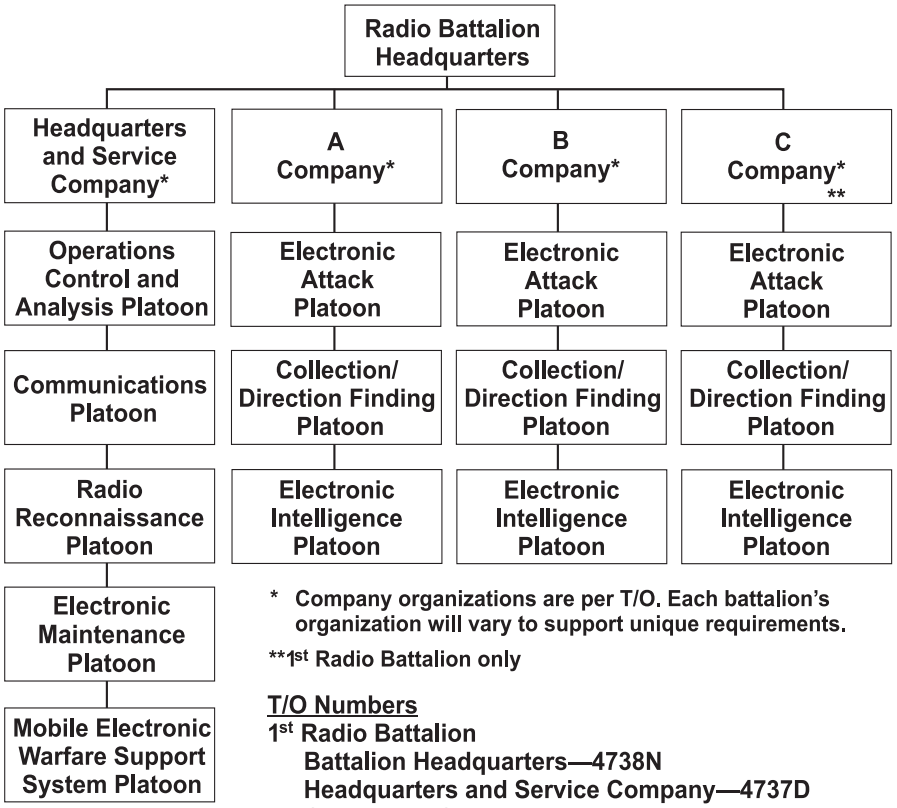


Figure 4-1. Radio Battalion Organization.

elements. Those tasks are accomplished by H&S staff sections (i.e., S-1, S-2, S-3, S-4, and S-6) and the following specialized platoons.

(1) Operations Control and Analysis Platoon. The operations control and analysis (OCA) platoon provides the Marines and equipment to perform RadBn operational planning and direction and SIGINT production, analysis, and reporting operations. Additionally, it is the nucleus for the RadBn OCAC during tactical operations.

(2) Communications Platoon. The communications platoon provides Marines and equipment to conduct special security communications operations in support of RadBn and, when deployed, MAGTF CE operations. Additionally, the platoon is equipped to support RadBn's internal communications requirements.

(3) Radio Reconnaissance Platoon. The radio reconnaissance platoon (RRP) provides trained RRTs for operations during advance force, preassault, or other operations where the employment of conventional RadBn teams may be inappropriate or unfeasible.

(4) Electronic Maintenance Platoon. The electronic maintenance platoon provides up to fourth-echelon maintenance support on RadBn unique equipment and second-echelon support on Marine Corps common communications and electronics equipment.

(5) Mobile Electronic Warfare Support System Platoon. Using a light armored vehicle (LAV) variant platform, the mobile electronic warfare support system (MEWSS) platoon provides Marines and equipment capable of SIGINT

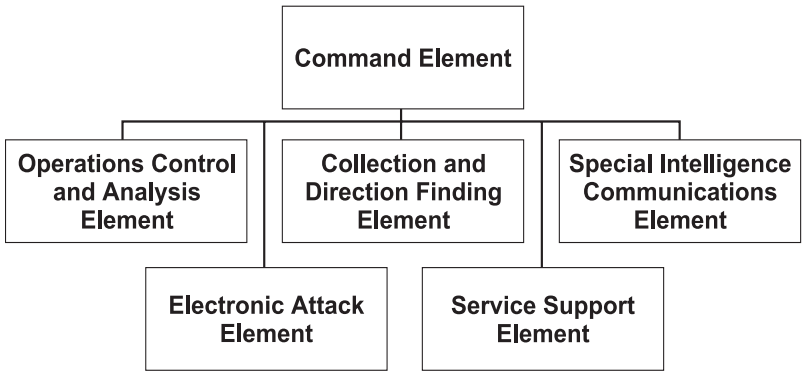


Figure 4-2. SIGINT Support Unit Elements.

collection, DF, reporting, and communication jamming operations.

b. Operational Companies

Each RadBn operational company has a table of organization (T/O) of 5 officers and 100 enlisted Marines organized into a company headquarters, EA platoon, voice collection and DF platoon, and nonvoice or ELINT collection platoon. During tactical operations, the company will be task-organized or reinforced with battalion assets consistent with the threat, mission, commander's intent, and intelligence concept of operations.

4003. Task Organization for MAGTF Operations SIGINT Support Unit

An entire RadBn will support a MEF operation To support smaller MAGTFs, the RadBn's tactical organization is the task-organized SIGINT support unit (SSU). The SSU may be as large as an operational company (minus or reinforced) or as small as a four-Marine team. The RadBn organization enables the rapid structuring and operational deployment of task-organized SSUs.

a. SIGINT Support Unit Structure

A fully structured SSU containing all the capabilities found in the RadBn is comprised of six basic elements (see figure 4-2). The nature of the threat, specific mission tasking, and intelligence and operational requirements determine the composition and equipment of each element.

(1) Command Element. The RadBn CO w designate an OIC and/or a staff noncommissioned officer in charge (SNCOIC) for each SSU. The command element is comprised of the personnel and facilities to command and control the SSU For smaller SSUs, the command element may be integrated within the operations control and analysis element with an OIC or an operations officer, noncommissioned officer in charge or an operations chief, and sufficient resources for command and control of the SSU operations. When the majority of the battalion deploys, the command element consists of the battalion commander, executive officer, sergeant major, and sufficien personnel for command and administrative support.

(2) Operations Control and Analysis Element. The SSU's command and control, analysis, production, and dissemination functions are executed within the OCAC. The OCAC performs the SIGINT processing, analysis, exploitation, production, and reporting of signals intelligence products and information. Additionally, it is the principle element that coordinates with other intelligence nodes to plan, direct, and integrate SIGINT operations with other intelligence and reconnaissance operations. Marines assigned to this element include the operations watch officers or operations watch chiefs, COMINT and ELIN analysts, translators or transcribers, and SIGINT report writers.

(3) Collection and Direction Finding Element. The collection and DF element is comprised of SIGINT support teams (SSTs) and other collection elements consisting of Marines and equipment for conducting SSU SIGINT collection and DF operations. Personnel assigned to this element include SIGINT linguists (or voice intercept operators), manual-Morse, non-Morse, and ELINT collection and DF operators, and supervisory personnel. Additionally, this element may contain MEWSS- or RRT-capable SSTs if the mission or situation warrants.

(4) Electronic Attack Element. The EA element is comprised of the Marines and equipment to conduct EA operations. Personnel assigned to this element include EA supervisors or controllers and EA operators.

(5) Special Intelligence Communications Element. The SI communications element installs and operates the SI or special security communications terminals for the SSU and the MAGTF CE. In addition, the SI communications element will install and operate SCI-level LAN systems to support SSU operations. The systems installed will depend on the mission, intelligence and CIS operations concepts, connectivity requirements, and terminal equipment availability. Personnel assigned to this element include communications supervisory personnel, information systems security and system administrators, and communications operators.

(6) Service Support Element. The service support element provides limited supply, engineers, electronic maintenance, and medical support to the SSU. The SSU depends on the MAGTF combat service support element (CSSE) for most of its combat service support. Marine assigned to the service support element may include medical, electronic maintenance, motor transport, engineer, supply, and administrative personnel.

b. SIGINT Support Unit Task-Organizational Considerations

SSUs are task-organized from resources available throughout the RadBn and are tailored to the requirements of the supported commander. The SSU's specific size and composition will also be influenced by threat and environmental factors known or expected to be encountered in the intended area of operations. The following factors must be considered when task-organizing an SSU.

(1) Enemy Signals Environment. The prime factor in determining the size, composition, and capabilities of an SSU is the known or anticipated enemy signals environment. Enemy factors to consider are—

- Target power output and frequency range.
- Digital or analog signals.
- Modulation techniques.
- Target signal operating instructions (i.e., sophisticated or complex).
- Target emitters (i.e., number, type, and density).

(2) Physical Environment. Terrain, climate, vegetation, and the operations area size influence the size and composition of the SSU.

(3) Operational Environment. Among factors that must be considered are—

- The military and political situation.
- The adversary's—
  - Size.
  - Composition.
  - Disposition.
  - C2 and CIS operations.
  - Doctrine, tactics, techniques, and procedures.
- The friendly force's—
  - Composition.
  - Commander's intent.
  - Operational and intelligence concepts.
  - Task organization.
  - Mobility.

c. SIGINT Support Unit Operations Watch Structure

The SSU must be capable of sustained, 24-hou operations. SSU elements, excepting the service

support element, are normally employed in two or three watch sections. In large SSUs, each watch section may have an officer and/or a staff noncommissioned officer (SNCO) assigned as an operations watch officer (OWO) or operations watch chief (OWC). In smaller SSUs, this function may be performed by a noncommissioned officer (NCO).

4004. Command and Control

a. Command Relationships

(1) Operational Control. The MAGTF commander with SOTA has OPCON of RadBn, which is exercised by the MAGTF G-2/S-2 and executed by the RadBn OIC.

(2) Administrative Control. Administrative control (ADCON) of RadBn SSUs is exercised by the unit to which the SSU is attached (in most cases the MAGTF CE).

(3) SIGINT Technical Control. SIGINT technical control (TECHCON) of United States SIGINT system assets, to include RadBn SSUs, is always retained by DIRNSA who delegates SOTA to MAGTF commanders. This means that within the MAGTF, the MAGTF commander with SOTA generally retains, coordinates, and exercises SIGINT TECHCON regardless of any other C2 relationships established for the operation (e.g., RadBn elements attached to or placed in direct support of MAGTF subordinate elements).

b. Support Relationships

The MAGTF commander may establish variou support relationships between the SSU and MAGTF subordinate elements when one organization should aid, protect, complement, or sustain another unit. The nature of the support relationship will be specified by a directive (e.g., annex B of the operations order) which should detail—

- Forces and other resources allocated to the subordinate element of the SSU.
- Time, place, level, and duration of the SSU support effort.
- Priority of the SSU supporting effort.
- Command relationships and degree of authority granted to the supported commander.

The two most common support relationships fo SSUs are general and direct support.

(1) General Support General support (GS) is action given to the MAGTF as a whole rather than to a particular subordinate element. Given the nature of SIGINT operations, GS is the most com mon support relationship used for SSU operations.

(2) Direct Support. Direct support (DS) is a mission requiring a force to support another specific force and authorizing it to answer directly the supported force's requests for assistance. When required by the mission and situation, elements of a SSU may be placed in DS of MAGTF subordinate elements (e.g., elements of the SSU in DS of the GCE).

4005. Notional Concepts of Employment and Task Organizations

The mission, enemy or other potentially hostile elements, and operational environment will always influence the composition and employment of SIGINT assets, as will logistics concerns such as footprint or airlift availability. To serve as a planning departure point, RadBns have developed notional SSU packages and concepts of employment which will be refined as mission and adversary details become known. (Appendix A, Radio Battalion SIGINT Support Unit Checklist, is provided as an SSU operations planning guide.) The levels of RadBn support can range from electronic collocation with the supported unit to an entire RadBn (minus or reinforced) deploying with a MEF as indicated by the following examples. It is important to note that no specific RadBn SSU may ever match exactly the following notional descriptions due to task organization, personnel or

equipment availability, and mission and threat considerations.

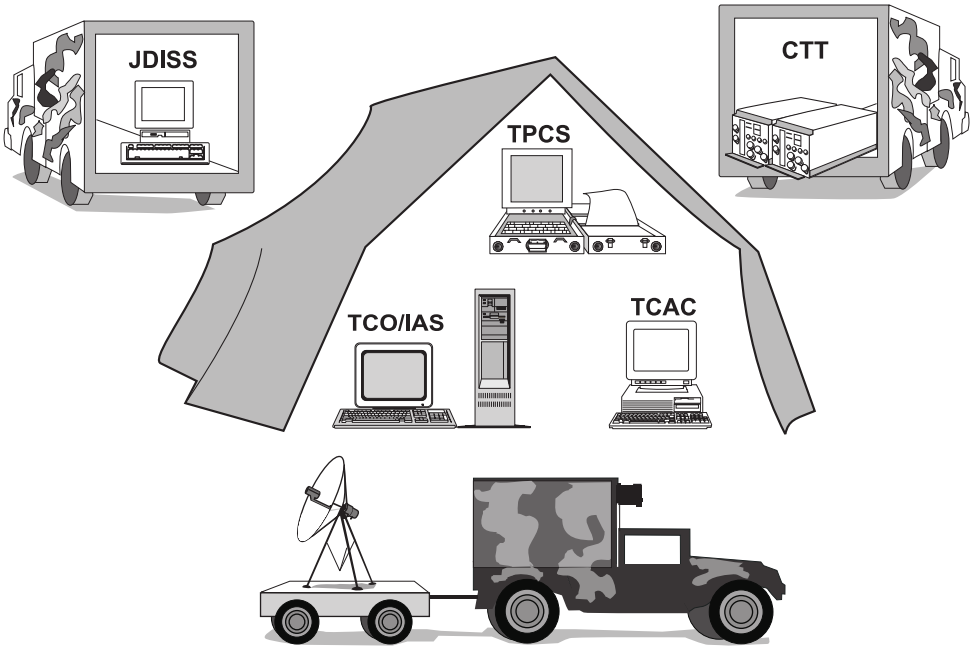
a. Marine Expeditionary Unit (Special Operations Capable) SIGINT Support Unit

The SSU concept of employment is dependent on the Marine expeditionary unit's (MEU) mission, threat, and planned concept of operations. The SSU is attached to the CE and almost always is employed in general support of the MEU (special operations capable [SOC]).

Generally, MEU(SOC) SSUs consist of 1 officer as the OIC, possibly another officer as the assistant OIC, and 20 or more enlisted Marines (to normally include at least one RRT). Table 4-1 provides a notional MEU(SOC) SSU T/O.

b. Fly-In Echelon

The fly-in echelon (FIE) is integrated and task organized to provide immediate SIGINT, EW, and SI communications in support of lead elements of a MAGTF or to reinforce MEU(SOC SSU capabilities. The FIE serves as the foundation for the buildup of SIGINT assets as required. Figure 4-3 illustrates a notional FIE configuration. The FIE generally consists of 2 officers and 18 to 30 enlisted Marines. Table 4-2 provides a typical FIE T/O. The FIE is under the operational control of the MAGTF commander who exercises SOTA. Initial operations will be in general support of MAGTF requirements. As the situation matures and the mission and associated tasks become clearer, the task organization and command relationships of the FIE or SSU elements may be modified to provide direct support to designated major subordinate elements (MSEs).



Legend	
CTT=Commander's Tactical Terminal	TCO=Tactical Combat Operations
TCAC=Technical Control and Analysis Center	TPCS=Team Portable Collection System

Figure 4-3. Notional SSU Fly-In Echelon Configuration.

Table 4-1. Notional MEU(SOC) SSU T/O.

Billet	Rank	MOS
H&S Support Elemen		
OIC	Capt	0202/0206
Assistant OIC	Lt	0206
SNCOIC	GySgt	2621/2629
Electronic maintenance technicia	Cpl	2841
SI CIS chief	Sgt	2651
LAV mechanic	LCpl-Sgt	2147
OCA Element		
Processing and reporting chief	SSgt	2621/2629
ELINT analyst	Sgt	2631
Signals analyst	Sgt	2621/2629
Collection/DF Team #1 (MEWSS capable)		
Team leader	SSgt	2621/2629
Linguist or voice intercept operator	Sgt	267X
Linguist or voice intercept operator	Cpl	267X
Manual morse or DF operator	LCpl	2621
EA operator	LCpl	2621
Collection/DF Team #2 (Helo capable)		
Team leader	Sgt	2621/2629
Linguist or voice intercept operator	Cpl	267X
Linguist or voice intercept operator	LCpl	267X
Collection or DF operator	LCpl	2621
Collection/DF Team #3 (RRT capable		
Team leader	SSgt	2621/2629
Assistant team leader	Sgt	267X
Linguist or voice intercept operator	Cpl	267X
Linguist or voice intercept operator	LCpl	267X
Collection or DF operator	Cpl	2621
Collection or DF operator	LCpl	2621

Table 4-2. Notional Fly-In Echelon T/O.

Billet	Rank	MOS
H&S Support Elemen		
OIC	Capt	0202/0206
SNCOIC	MSgt	2691
Electronic maintenance technicia	Sgt	2841
SI Communications Element		
Communications chief	SSgt	2651
Trojan Spirit operator[1]	Sgt	2651
Trojan Spirit operator	LCpl	2651
Communications operator	Cpl	2651
Communications operator	LCpl	2651
OCA Elemen		
Operations officer	Lt	0206
Senior analyst	GySgt	267X/2629
Analyst	SSgt	2621/2629
Analyst	Sgt	2621/2629
Signals chief	SSgt	2621/2629
Signals analyst	Sgt	2621
Signals analyst	Cpl	2621
ELINT analyst	Sgt	2631
ELINT analyst	LCpl	2631
Collection/DF Element		
Team leader	SSgt	2621/2629
Linguist or voice intercept operator	Sgt	267X
Linguist or voice intercept operator	Cpl	267X
Collection or DF operator	Cpl	2621
[1]2nd RadBn does not have Trojan Spirit		

c. Marine Expeditionary Force Support

For detailed SIGINT support information regarding a specific MEF operation, refer to the CSP and annex B of the OPLAN for that operation The following is a discussion of RadBn support of a notional MEF operation.

(1) Concept of Operations A MEF-level operation is supported by the RadBn (minus or reinforced. It could be minus because prior committed RadBn assets, such as MEU SSUs, were unavailable. It could be reinforced because some level of personnel or equipment augmentation from the other RadBn, MarSptBn, and/or Marine Corps units might be required.

(2) Concept of Employment. The RadBn task-organizes and employs its companies and teams to best support the MEF by—

- Deploying collection or DF teams for improved target signals access and operational support to forward MAGTF units.
- Collocating RadBn's C2 node with the MAGTF G-2/S-2's CIC and operating within the integrated intelligence concept of operations in GS of the MAGTF.
- Focusing on tasked PIRs and IRs and providing required support to all six intelligence functions.
- Disseminating time-sensitive SIGINT products to subordinate MAGTF units when required by the tactical situation.
- Providing OCAC liaison teams (OLTs) to the lead elements of the MEF, its MSEs and adjacent units as required; and providing SIGINT support elements (SSEs) and SSTs with mobile MAGTF units.
- Providing security and CIS for all internal RadBn requirements and for specified MAGTF CE support.
- Integrating operations with other MAGTF intelligence units to support cueing of other intelligence and reconnaissance collection elements, all-source intelligence production, and other mutual support.

(3) Company Command Element. One of the keys to effective MEF support is the placemen and use of the company command elements (CCEs). The CCEs are normally collocated with the GCE or MAGTF-subordinate task force headquarters depending on the mission and threat. The CCE—

- Provides I&W support to the supported commanders.
- Coordinates location, operations, and support of SSTs with supported units and other forward-deployed intelligence and reconnaissance units.
- Serves as the C2, communications, and SIGINT-tasking channel between the OCAC and forward-deployed SST as required.
- Provides company liaison teams (CLTs) to adjacent and subordinate units as required.
- Provides or arranges for SST administration, logistic, and physical security support.
- Provides SIGINT tasking and direction of SSTs when the OCAC is unable to provide tasking and direction.

d. Radio Reconnaissance Teams

RRTs are six-Marine teams trained in special insert or extract means and basic amphibious reconnaissance capabilities. This additional training makes the RRT capable of advance force, preassault, deep postassault, and maritime special purpose force (MSPF) SIGINT missions as assigned. RRTs support the six intelligence functions. Additionally, they may be tasked to conduct SIGINT signals search and data base development in order to enhance understanding of threat operations prior to the arrival of other SSU forces. In an advance force role, RRTs may be employed to—

- Provide SIGINT-derived I&W intelligence support to advance forces.
- Provide SIGINT collection and reporting in areas not accessible to conventional SSTs.
- Provide SIGINT collection and reporting in support of assault and landing forces.
- Provide collection of unique signals. Unique signals are signals expected to have intelligence value that cannot be collected by other reasonable means (e.g., low-powered UHF communications).
- Conduct threat signals search and data base development.

e. Mobile Electronic Warfare Support System SIGINT Support Team

The principal advantage of a MEWSS SST is its high mobility, light armored protection, allowing it to maintain operations and provide direct support of similarly equipped ground combat element units. The employment of MEWSS vehicles requires close coordination with both the G-2/S-2 and G-3/S-3 as the MEWSS provides the only ground-based ELINT collection and the major ground-based communications EA capabilities organic to the MAGTF. The COMINT capabilities of the MEWSS are similar to that of any SST.

f. Aviation SIGINT Support Team

The aviation SSTs capabilities are similar to those of other SSTs. Its principal advantage is the ability to operate aboard Marine aviation platforms (e.g., helicopters). Aviation SSTs can provide SIGINT support to air and airborne units during missions such as deep raids and tactical recovery of aircraft and personnel operations or when the MAGTF commander needs immediate I&W accessible only by airborne SIGINT collection elements. The use of airborne SIGINT operation provides supporting SSTs with the ability to collect and exploit threat signals from extended ranges. The basic aviation SST is task-organized consistent with the mission and supported force's requirements. Generally, an aviation SST consists of RadBn Marines with a COMINT receiver, intelligence broadcast receiver, communications jammer, and UHF satellite communications radio.

g. Operations Control and Analysis Center Liaison Team

An OLT supports the intelligence effort of MAGTF subordinate elements (e.g., ACE or CSSE headquarters or rear area operations center). OLTs collocate with the G-2/S-2 of the supported unit operating from within its TSCIF. The OLT is task-organized out of available SSU assets in tactical support of the organization to which it is assigned. This assignment could be for a specific operation, phase, or for the duration of a conflict. Primarily, OLTs provide additional SIGINT C2 support and CIS connectivity for tactical SIGINT planning, production, and reporting with the MAGTF G-2/S-2 and RadBn OCAC. OLTs expedite, simplify, and coordinate the sharing of SIGINT I&W, technical data, taskings, and products. Normally, the OLT monitors RadBn collection teams and theater SIGINT reporting communications to provide the supported unit access to tactical and operational-level SIGINT and I&W intelligence. In most cases, an OLT will consists of at least one officer and three enlisted Marines with supporting CIS equipment.

h. Company Liaison Team

A CLT is task-organized with available assets to best satisfy the requirements of the organization or unit to which it is assigned (e.g., an infantry battalion). This assignment is normally for a specific duration or operational phase. In most cases, a CLT will consist of one SNCO and one to three additional enlisted Marines. Like the OLT, the CLT expedites SIGINT I&W to local decision-makers and assists with SST employment, tasking, and support.

i. Augmentation and Composition

Due to the low density of many SIGINT skills and equipment and the high tempo of operations, the RadBns may lack sufficient personnel with the requisite skills or SIGINT equipment with the necessary capabilities for a particular operation RadBns are reinforced with personnel and SIGINT equipment by augmenting and compositing.

For a small number of personnel requirements, individual augmentation often works best. With concurrence from the supported organization, the RadBn will forward a request for SIGINT personnel augmentation to CMC (C4I or CIS) via the COMMARFOR (G-1/G-2). Once the request is received at CMC, it will be validated and forwarded to CNSG and MarSptBn. MarSptBn will attempt to satisfy the request with active and/o reserve Marines from the battalion. Any portion of the request that MarSptBn can not satisfy will be returned to CMC (C4I/CIS) for sourcing from other Marine Corps units or other sources.

For significant numbers of personnel and equipment in support of a large operation or major regional contingency, elements may be composited from one RadBn with the other RadBn. Coordination between the RadBns should be continuous in the development of contingency plans (CONPLANs), OPLANs, and CSPs to ensure mutual understanding and validation of requirements and information (e.g., time-phased force deployment data).

Chapter 5

Marine Tactical Electronic Warfare Squadrons

Marine aviation performs six functions: offensive air support (OAS), antiair warfare (AAW), assault support, aerial reconnaissance, EW, and C2 of aircraft and missiles. VMAQs provide the MAGTF and other designated forces with EW support. The VMAQ also has an inherent capability to perform visual and electronic air reconnaissance. Electronic reconnaissance is the detection, identification, evaluation, and location of foreign electromagnetic radiation to provide EOB information. This chapter will focus on the VMAQ electronic reconnaissance and ELINT capabilities.

5001. Mission and Tasks

VMAQs provide EW (principally EA) and ELINT support to the MAGTF and other designated forces. When deployed, the VMAQ is under the operational and administrative control of the ACE commander. To support the MAGTF, the VMAQ conducts tactical jamming to prevent, delay, or interrupt detection and tracking by enemy early warning, acquisition, fire or missile control, counterbattery, and battlefield surveillance radars. Tactical jamming also denies and/or degrades enemy communications capabilities.

In addition, the VMAQ conducts electronic reconnaissance and ELINT operations to maintain EOB, to include both selected emitter parameters and location of nonfriendly emitters. VMAQs also provide threat warnings for friendly aircraft, ships, and ground units.

Key VMAQ tasks include—

- Providing aerial EA and ES support to ACE and other designated operations.
- Processing, analyzing, and producing routine and time-sensitive ELINT reports fo updating and maintaining enemy EOB. This is accomplished through the intelligence and electronic warfare division, TERPES, and the tactical EA-6B mission planning system (TEAMS) sections to support premission planning and postmission processing of collected data and production of pertinent intelligence reports. Working in concert with the intelligence section, TERPES and TEAMS sections provide required ELINT and EOB intelligence products to the ACE and MAGTF.
- Providing liaison personnel to ACE and MAGTF CE staffs to assist in VMAQ employment planning. Inherent in this task i the requirement to provide an air EW liaison officer to the MAGTF EWCC.
- Conducting EA operations for EP training of MAGTF units.
- Intercepting, recording, and jamming threat communications and noncommunication emitters.

5002. Organization and Concept of Employment

There are four VMAQs (designated VMAQ-1 through VMAQ-4) assigned to MAG-14, 2d MAW, Cherry Point, North Carolina. Each squadron has five EA-6B Prowler aircraft and is organized into administrative, intelligence and electronic warfare, operations, logistics, safety and standardization, and maintenance divisions See figures 5-1 and 5-2 on page 5-2.

EA-6B aircraft conduct EA, ELINT, and electronic reconnaissance operations in support of ACE and other MAGTF missions. The TERPES section functions as a key element of the MAGTF's intelligence operations. TERPES is an

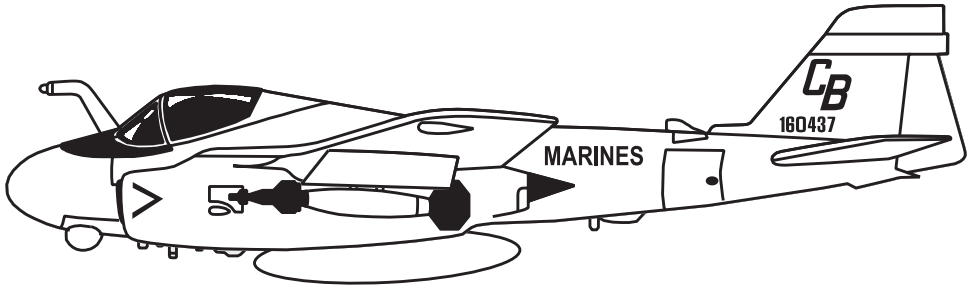


Figure 5-1. EA-6B Prowler

air-transportable, land-mobile intelligence processing and production system organic to VMAQ and is used to develop, maintain, and distribute tactical EOB and ELINT reports. TERPES functions as an automated tactical data system capable of producing current and future intelligence through information storage and retrieval, data recording, data base management, and data comparison. TERPES has a stand-alone capability but is utilized by VMAQs to optimize signals analysi and reporting to support MAGTF operations. Figure 5-3 provides an overview of VMAQ and TERPES operations.

5003. EA-6B Prowler

The EA-6B Prowler is a subsonic, all-weather, carrier-capable aircraft. The crew is composed of one pilot and three electronic countermeasure officers. The Prowler's primary missions include collecting and processing designated threat SO for jamming and subsequent processing, analysis, and intelligence reporting; and employing the AGM-88 high-speed antiradiation missile (HARM) against designated targets. The AN/ALQ-99 Tactical Jamming System effectively

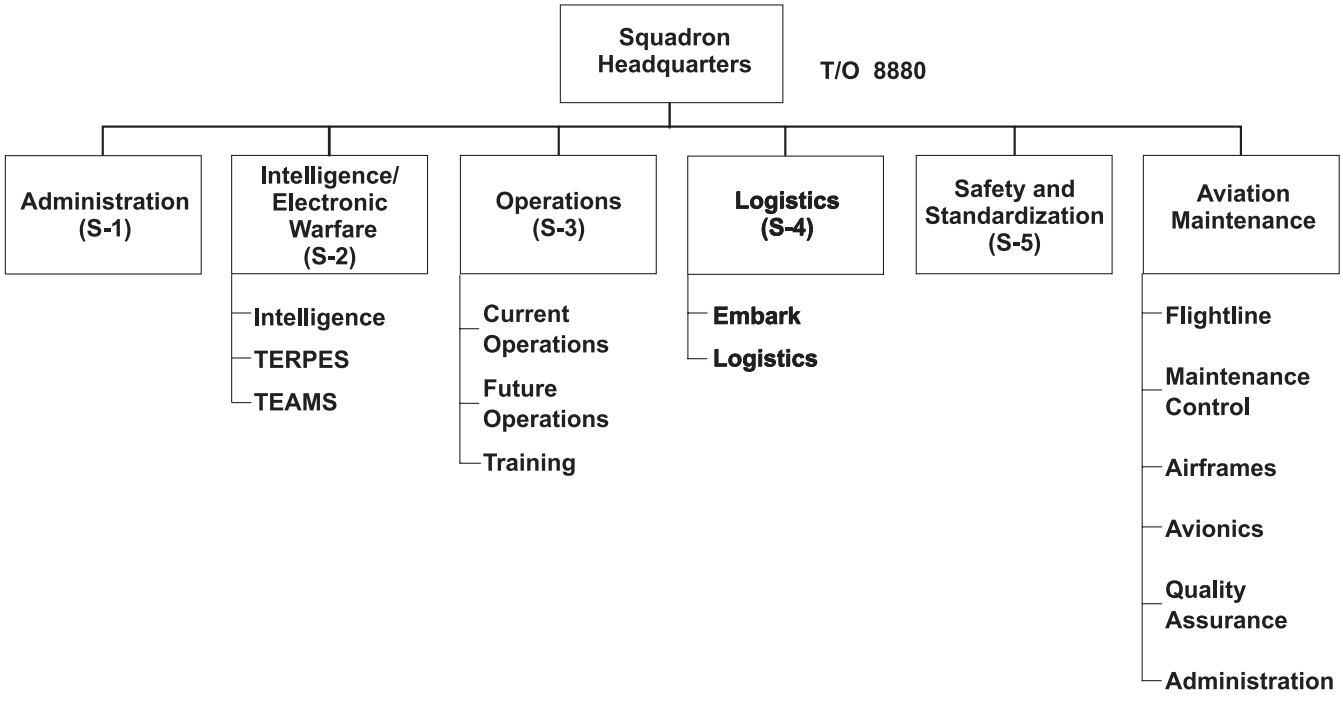


Figure 5-2. VMAQ Organization.

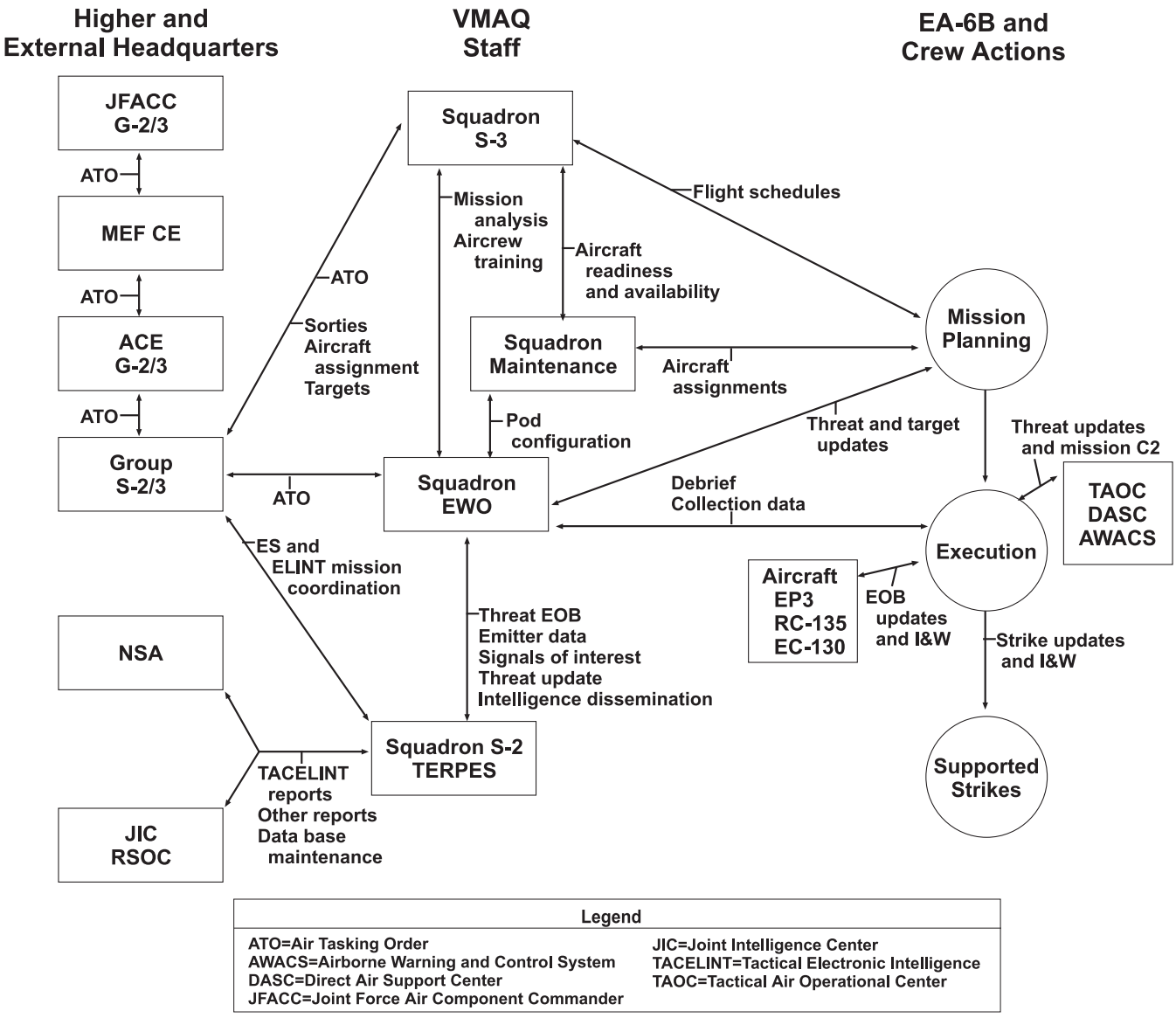


Figure 5-3. VMAQ and TERPES Operations.

incorporates receivers and external pods for signals reception and transmission of jamming signals (principally those associated with threat air defense radars and associated C2).

In addition to the AN/ALQ-99, the EA-6B also employs the USQ-113 Communications Suite which provides the ability to collect, record, and disrupt threat communications in either of the following two modes of operation:

- EA which scans the electromagnetic environment to intercept and jam targeted signals of interest (SOIs).
- ES which scans the electromagnetic environment to intercept and digitally record SOIs.

5004. Tactical EA-6B Mission Planning System

TEAMS is designed to assist EA-6B aircrew with planning allocation and optimization of receivers, jammers, HARM, and other integrated weapon systems into a comprehensive C2W package. Basic intelligence data is provided by various MAGTF theater and other intelligence and analysis centers. Parametric data for friendly and adversary platforms, weapons systems, and emitters is provided by the electronic warfare data base system (EWDS) on a quarterly basis and near-real-time updates may be provided through tactical receive equipment (TRE) integrated by the TERPES section into the TEAMS workstation. World maps, terrain data, and digitized navigation charts are provided by the National Imagery and Mapping Agency (NIMA) on a quarterly basis.

TEAMS allows the operator to—

- Maintain area of operations emitter listings.
- Edit emitter parameters.
- Develop mission-specific geographic data and EOB.
- Perform postflight mission analysis to—
  - Identify electronic emitters using various electronic parameter data bases and ELINT analytical techniques.
  - Locate emitters by coordinates with a certain circular error of probability for each site.
  - Correlate new information with existing data.
- Accomplish mission planning in support of coordinated strikes and EA-6B optimization.

5005. TERPES

TERPES (AN/TSQ-90) is an air- and land-transportable, single-shelter ELINT processing and correlation system. The TERPES team is composed of Marines, equipment, software, and supporting procedures integrated to—

- Identify and locate enemy radar emitters from data collected by EA-6B aircraft o those received from other intelligence sources.
- Process and disseminate EW data rapidly to MAGTF intelligence centers.
- Provide mission planning and briefing support to VMAQ EA and ES operations.

The standard TERPES configuration consists o one 8- by 8- by 20-foot shelter and two skid-mounted environmental control units (ECUs). Positioned on and around the shelters are a TRE antenna, an HF antenna, and two mast-mounted UHF antennas. These modules can be tailored to specific mission requirements. Electrical powe support for TERPES must be obtained from the Marine wing support squadron.

The TERPES is operated by one MOS 2602 SIGINT/EW warrant officer and six MOS 2631 TERPES operators/analysts. Maintenance support i provided by one MOS 9966 TSQ-90 maintenance officer and four MOS 2821 TSQ-90 technicians.

a. Operational Capabilities

The TERPES will—

- Translate rapidly the machine-readable, airborne-collected digital data into man- and machine-readable reports (i.e., paper, magnetic tape, secure voice, plots, and overlays).
- Receive and process EA-6B mission tapes.
- Accept, correlate, and identify electronic emitters data from semiautomatic or automatic collection systems using various electronic parameter data bases and ELINT analytical techniques.
- Locate emitters by coordinates with a certain circular error of probability for each site.

- Provide EA-6B EWOs with tactical intelligence briefings to support EA and ES missions. (The official title for EWO is electronic countermeasures officer [ECMO]. EWO is used to accurately reflect the scope of MOS 7588 activities and EW terminology changes.)
- Provide tactical jamming analysis.
- Ensure tactical intelligence data base maintenance for the VMAQ and the EOB for the MAGTF.

b. Mapping Package

The TERPES mapping and overlay package is based on NIMA products which have been integrated into a software program called the Delorme mapping system. This system allows TERPES operators to display mapping data that is loaded to the TERPES system at scales ranging from worldwide scale down to the 1:5,000 scale. A wide range of tools such as zoom, projection magnification, perspective, linear, and spatial analysis allow operators to manipulate mapping data to enhance understanding of the overlaid threat information.

c. Intelligence Analysis

The TERPES Intelligence Analysis Application (IAA) enables the operator to analyze ELINT data combined with additional modernized integrated data base (MIDB) intelligence data to—

- Respond to requests for intelligence (RFIs).
- Prepare intelligence data base updates.
- Analyze threat and tactical situations.
- Estimate changes in the threat's tactical situation.

d. Data Fusion

MIDB is the primary intelligence data base for IAA operator queries. In addition to EA-6B aircraft mission tapes, other inputs required to maximize the support provided to tactical intelligence operations include the following:

- Naval intelligence data base (NID) contains characteristics and performance data for weapons, sensors, and platforms.
- EWDS is similar to the NID and provides EA-6B tailored data.
- ELINT parameters list (EPL) is NSA's observed radar parametric data.
- Electronic warfare integrated reprogramming (EWIR) is produced by the United States Air Force Foreign Technology Division. EWIR combines assessed technical radar parameters from the United States Air Force EW Science and Technology data base with the observed parameters of the NSA data base.
- Joint spectrum center (JSC) is used to derive friendly EOB and radar parametric data.

e. TERPES Fusion Processor

The TERPES fusion processor (TFP) processe intelligence data from tactical ELINT (TACELINT) reports, tactical reports (TACREPs), and IMINT reports. The TFP provides filtering, characteristic and performance identification, order of battle (OOB) identification, technical analysis, multisource correlation, and candidate updates. The TFP presents the information in various forms for analysis. One TFP integrated information source is the TRE and Related Applications (TRAP) broadcast. This broadcast is accessed using the TRE and provides near-real-time (NRT), national-level reports to the TERPES. The TRAP broadcast also assists the TFP in maintaining an ELINT parameter data base to track airborne, shipboard, and land-based targets as a tool to develop EOBs and as an instrument to perform comparative studies on radar parameters.

f. TERPES ELINT Preprocessor

The TERPES ELINT preprocessor (TEPP) processes all EA-6B SOI collected from recorder o reproducer set tape or disk files. Specifically, the application allows for the NRT analysis of technical ELINT data. Position reports and specific unit identification and location information are used to

update the TERPES data base and to prepare TACELINT reports. TERPES also provides tactical jamming system (TJS) analysis for the EA-6B aircrew and maintenance personnel.

TJS analysis consists of recovering recorded data for verifying jammer calibration, on- and off-jammer times, and frequency and azimuth coverage. TERPES will use mission data in the generation of EW mission summary reports.

g. Intelligence Reporting

The primary intelligence output from TERPES operations is mission reports. Mission reports are available in many forms and are provided primarily to MAGTF intelligence elements in response to established intelligence requirements. The most commonly used reporting form is the TACELINT (refer to USSID 340, *Tactical ELINT Reporting*, for format and content).

Other report forms include the following:

- TACREP provides information on immediate threat activity.
- ELINT summary report provides a summary of ELINT activity over established periods (normally 24 hours). Refer to USSID 200 *Technical SIGINT Reporting,* for format and content.
- ELINT technical report provides for analyst exchange of information of parametric data. Refer to USSID 341, *Technical ELINT Reporting*, for format and content.
- Over the horizon (OTH) "GOLD" report provides information derived from contac reports of ELINT parametrics.
- Order of battle report (OBREP) provides order of battle information such as basic encyclopedia (BE) number, equipment, and location.

Chapter 6

Communications and Information Systems

The area of SIGINT operations currently undergoing substantial change is SIGINT CIS technological advances and architectures development. SIGINT architectures are changing from the use of separate, secure, 24-hour manned communications centers with dedicated, bulk-encrypted links to the use of multilevel information system security initiative (MISSI) capabilities over unsecured commercial or DOD networks via the Defens Message System (DMS). Adding the proliferation of SIGINT collection, processing, and production systems and centers along with other intelligence and operations systems and centers that must disseminate and share SIGINT and communicate digitally creates a very dynamic situation.

The SIGINT effort depends heavily on a secure, reliable, and fast CIS architecture to receive SIGINT and all-source intelligence products and to pass collected data and SIGINT products and technical reports to the MAGTF and other users. Communications and information systems are also required for the C2 of SIGINT units and their integration with multidiscipline intelligence operations. Every mission and situation is unique, requiring some modifications to the CIS architecture supporting MAGTF SIGINT operations. Detailed planning and close coordination among the SIGINT units' CO or OICs, the MAGTF G-2/S-2 and G-6/S-6, and pertinent operational and intelligence organizations is critical to establishing reliable and effective SIGINT architecture.

See appendix B, Marine Corps SIGINT Equipment, of this publication for additional information on select communications and information systems resources pertinent to MAGTF SIGIN operations. Also, see MCWP 6-22, *Communications and Information Systems*, for a detailed review of MAGTF CIS and supporting tactics, techniques, and procedures.

6001. Basic MAGTF SIGINT CIS Requirements

a. Capability to Command and Control Subordinate Units

MAGTF SIGINT units must be capable of positive C2 of subordinate units and integration of its operations with broader MAGTF and external intelligence and operations C2. Traditionally, single-channel radio (SCR) and record message traffic have been used to support C2 of SIGIN units. In semistatic situations, secure electronic mail or the telephone may be the method of choice, while in highly fluid or mobile scenarios, cellular telephones, satellite communications (SATCOM), VHF, or HF radio may be used.

b. Ability to Receive and Transmit Collected Data and Information from Collection and DF Elements

The SIGINT architecture must provide connectivity among organic and supporting SIGINT collection or DF teams, SIGINT analysis and production centers, and supported MAGTF operations and intelligence centers. Requirements include the capability to receive and transmit collection files and reports digitally via fiber, wire, or radio (voice and data) in formats that are

readily usable by the SIGINT and all-source intelligence analysts.

c. Ability to Provide Intelligence to the Supported Commander

The required SIGINT architecture must support the commander's intent, concepts of operation and intelligence, command relationships, and standing PIRs and IRs. The SIGINT CIS architecture must be capable of integrating SSU SCI-secure channels and C2 operations with the primary GENSER channels used by supported commanders throughout the MAGTF.

d. Ability to Share SIGINT Products and Technical Reports

The SIGINT architecture must provide the means to share products and reports with MAGTF all-source intelligence centers and with SIGINT and all-source JTF, other components, theater, and national intelligence centers. The traditional means for providing this capability are the SCI secure defense special security communication system (DSSCS) for record communications and operator's communications (OPSCOM) circuit for SIGINT analyst-to-analyst exchanges and coordination. These means are rapidly being replaced by—

- JWICS which provides interoperability of intelligence systems, access to intelligence data bases, and direct analyst-to-analyst exchange.
- National Security Agency Network (NSANET) which provides access to national-level SIGINT reports and data bases and electronic mail connectivity for SIGINT analyst-to-analyst exchanges and intelligence requests.

e. Ability to Receive and Disseminate SIGINT Indications and Warnings

A significant strength of SIGINT is its ability t provide time-sensitive I&W of the adversary's actions and intentions. This I&W intelligence is disseminated by a variety of means to include voice, record messages, tactical reports, electronic mail, and intelligence broadcasts. Having the capability to receive the information, recognizing the I&W intelligence as such, and possessing a method to disseminate this I&W intelligence to the affected units and decisionmakers are key to satisfying this requirement.

f. Ability to Receive SIGINT Broadcasts

For several years MAGTFs have possessed intelligence broadcast receivers capable of accessing select SIGINT broadcasts. The broadcast receivers currently being fielded and under development will allow MAGTFs to receive multiple channels of JTF, fleet, theater, and national intelligence broadcast data. This data includes all-source intelligence and SIGINT on enemy operations as well as friendly positional and other information. Effective planning, design, and integration of SCI and GENSER CIS and proper information management filtering, correlating, and tailoring prior to dissemination or display provide timely SIGINT reporting to supported commanders while preventing information overload.

6002. Notional MAGTF SIGINT Operational Architectures

a. MEF

Figure 6-1 depicts a notional SIGINT operational architecture for a fully deployed MEF. It shows a full complement of organic and supporting JTF other service components, theater, and nationa SIGINT capabilities.

Key architectural concepts include the following:

- SIGINT operations planning and management are centralized within the MAGTF G-2/S-2.

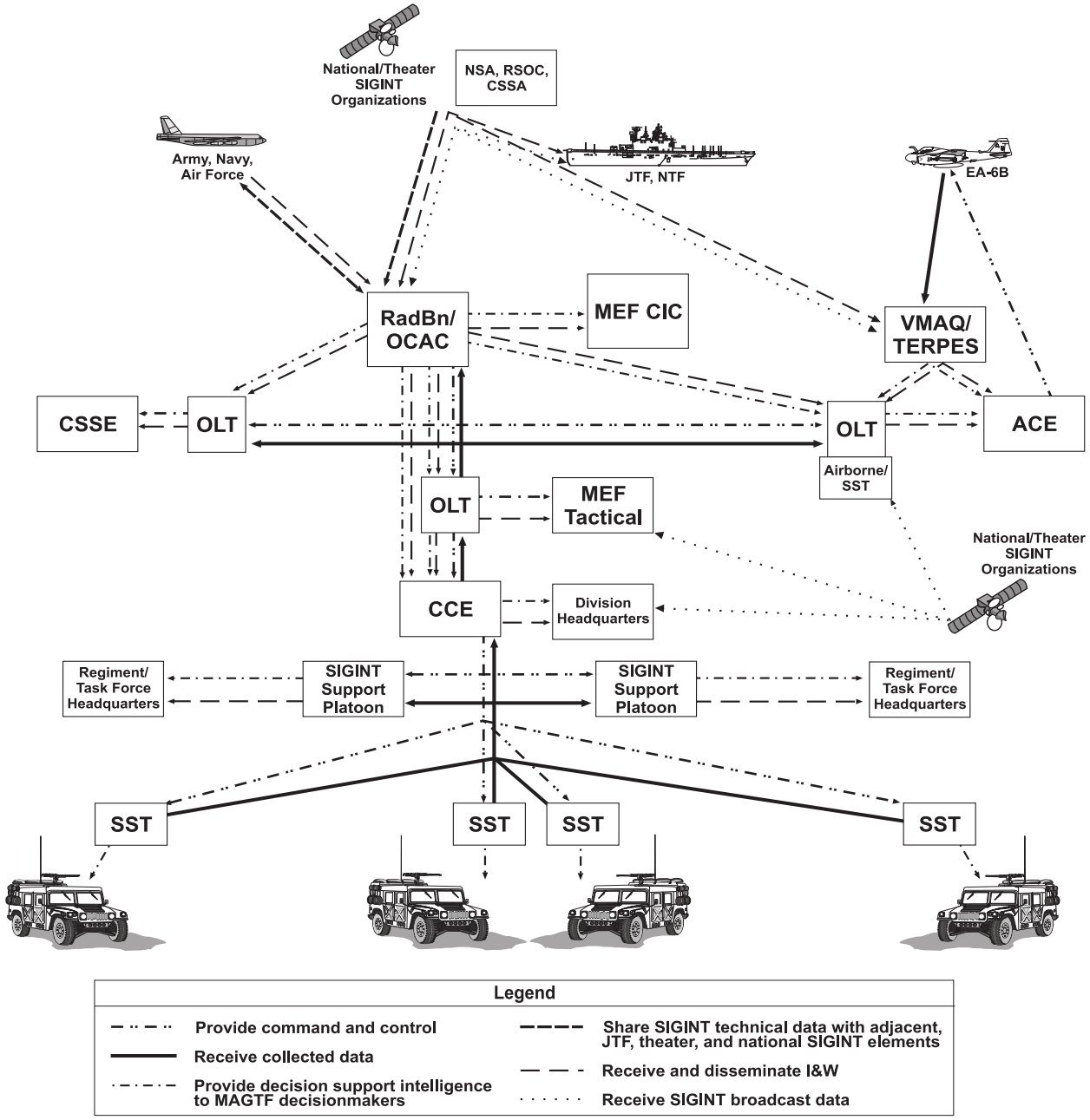


Figure 6-1. Notional MEF SIGINT Operational Architecture.

- **RadBn OCAC is collocated with the G-2/ S-2 CIC and operates in general support of the MAGTF, with collection or DF teams collocated with forward-deployed MAGTF units.**
- **VMAQ TERPES is collocated with ACE headquarters and principally supports ACE operations.**
- **MAGTF CIC, RadBn OCAC, and TERPES maintain connectivity with appropriate**

external intelligence and SIGINT organizations.

b. MEF Lead Echelon

Figure 6-2 shows a notional operational architecture in support of the MEF lead echelon during its initial deployment and employment phases. SIGINT operations focus on the MEF as it deploys into the area of operations and builds its combat power.

Key architectural concepts include the following:

- SIGINT operations planning and management remain centralized within the MAGTF G-2/S-2, which is not yet within the area of operations.
- RadBn fly-in echelon is collocated with lead elements of the MAGTF G-2, with organi teams operating in GS of deployed elements. RadBn OCAC is collocated with the G-2/S-2 CIC.
- VMAQ TERPES is collocated with ACE headquarters and principally supports ACE operations.

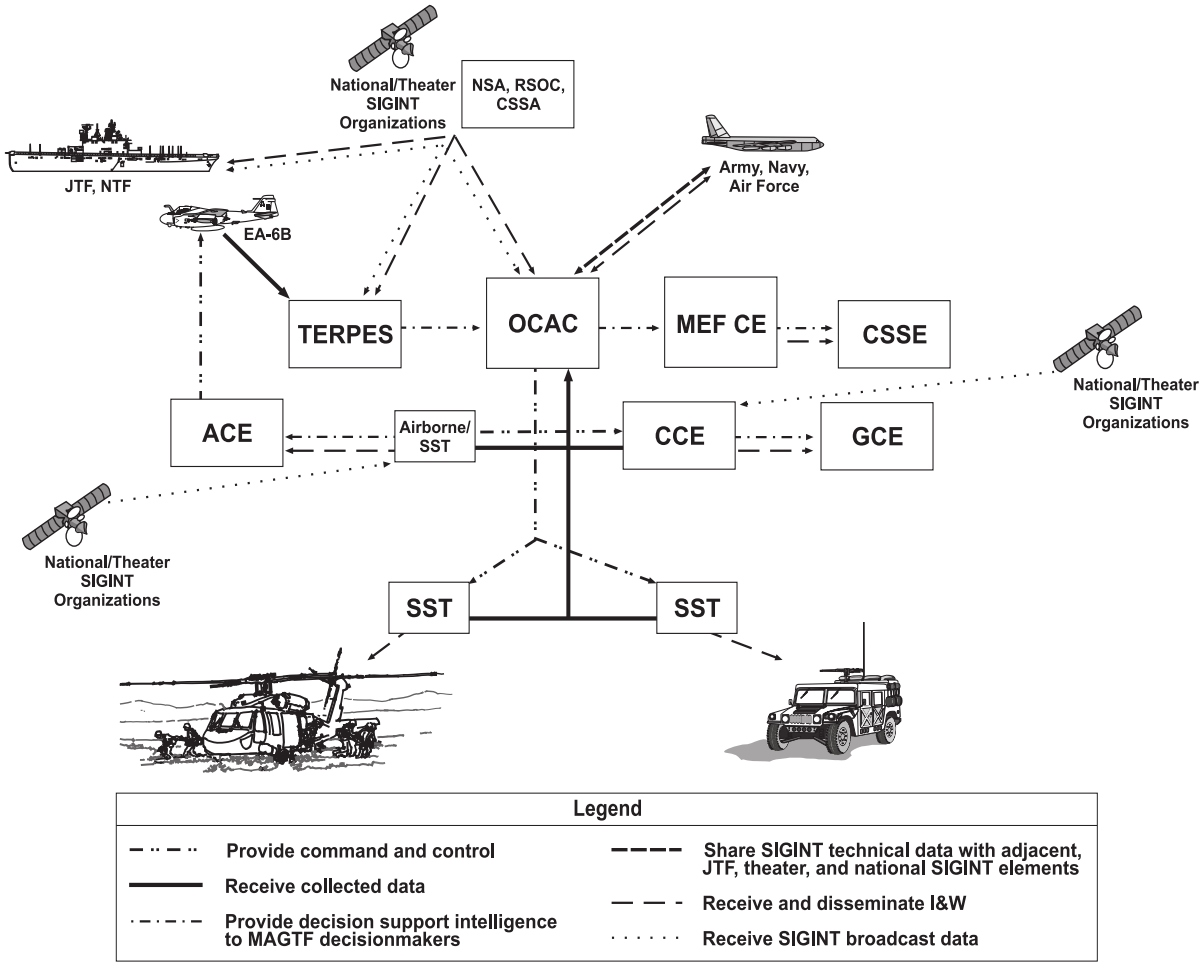


Figure 6-2. Notional MEF Lead Echelon SIGINT Operational Architecture.

- **MAGTF CIC, RadBn OCAC, and TERPES maintain connectivity with appropriate external intelligence and SIGINT organizations.**

c. MEU(SOC) CE Afloat

Figure 6-3 shows a notional operational architecture in support of a MEU(SOC) afloat. During such operations, MEU and ATF SIGINT capabilities and organizations generally collocate within the same afloat facilities (e.g., SSESs) integrate and share some systems operations. A critical component of this architecture is satisfactor voice and data ship-to-shore SCI communications between the MEU(SOC) command element and ashore SIGINT elements.

Key architectural concepts include the following:

- **SIGINT operations planning and management are centralized in the MEU(SOC) S-2.**
- **RadBn SSU OCAC operates out of the SSES collocated with the S-2 CIC within the amphibious task force intelligence center (ATFIC). RadBn operates in general support of the MAGTF. Depending on the mission, RadBn collection and DF elements may operate in either general support of the MAGTF or direct support of elements operating ashore.**
- **MAGTF CIC and RadBn OCAC maintain connectivity with appropriate external intelligence and SIGINT organizations.**

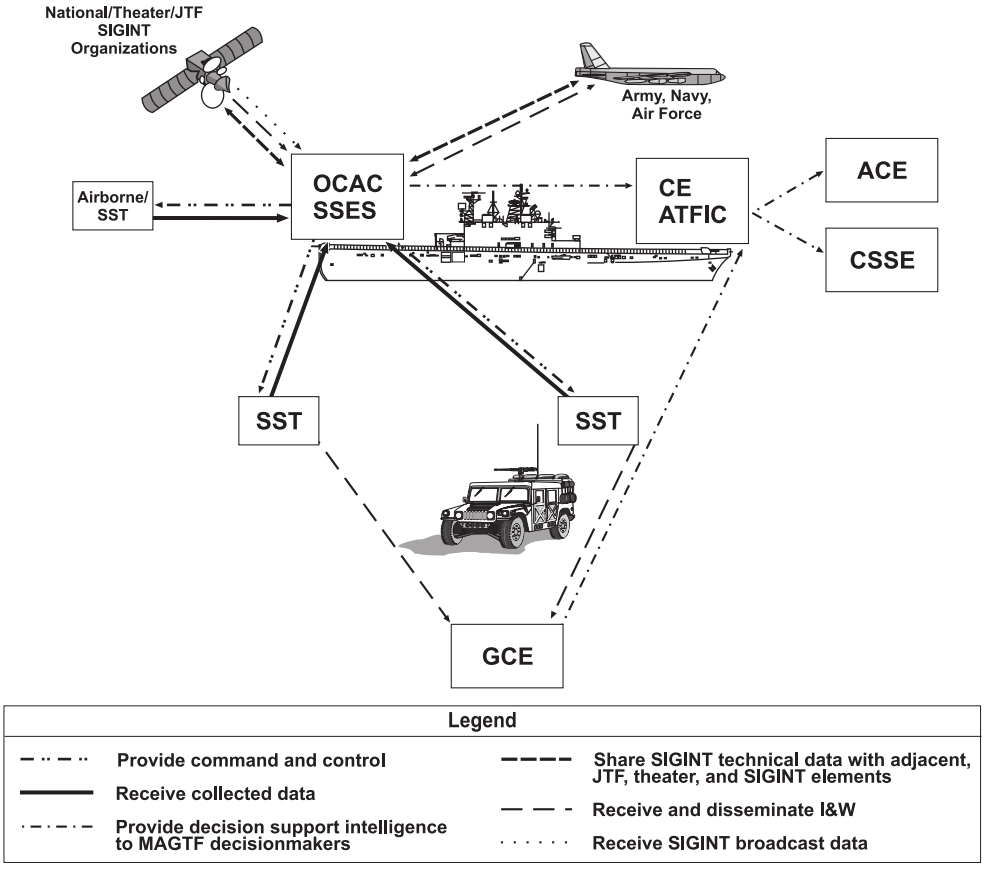


Figure 6-3. MEU(SOC) CE Afloat SIGINT Operational Architecture.

d. MEU(SOC) CE Ashore

Figure 6-4 depicts a notional operational architecture in support of a shore-based MEU(SOC) CE. The MEU(SOC) requires ship-to-shore SCI communications connectivity to continue exploiting external SIGINT capabilities and resources while minimizing the CIS and logistic footprints ashore.

Key architectural concepts include the following:

- **SIGINT operations planning and C2 remain centralized within the MEU(SOC) S-2.**
- **The MAGTF RadBn SSU OCAC is collocated ashore with the S-2 CIC. Other SSU elements provide continued support from the amphibious task force intelligence center SSES.**
- **RadBn SSU normally will operate in GS of the MAGTF.**
- **MAGTF CIC and RadBn OCAC principal connectivity with appropriate external intelligence and SIGINT organizations is via the amphibious task force intelligence center SSES.**

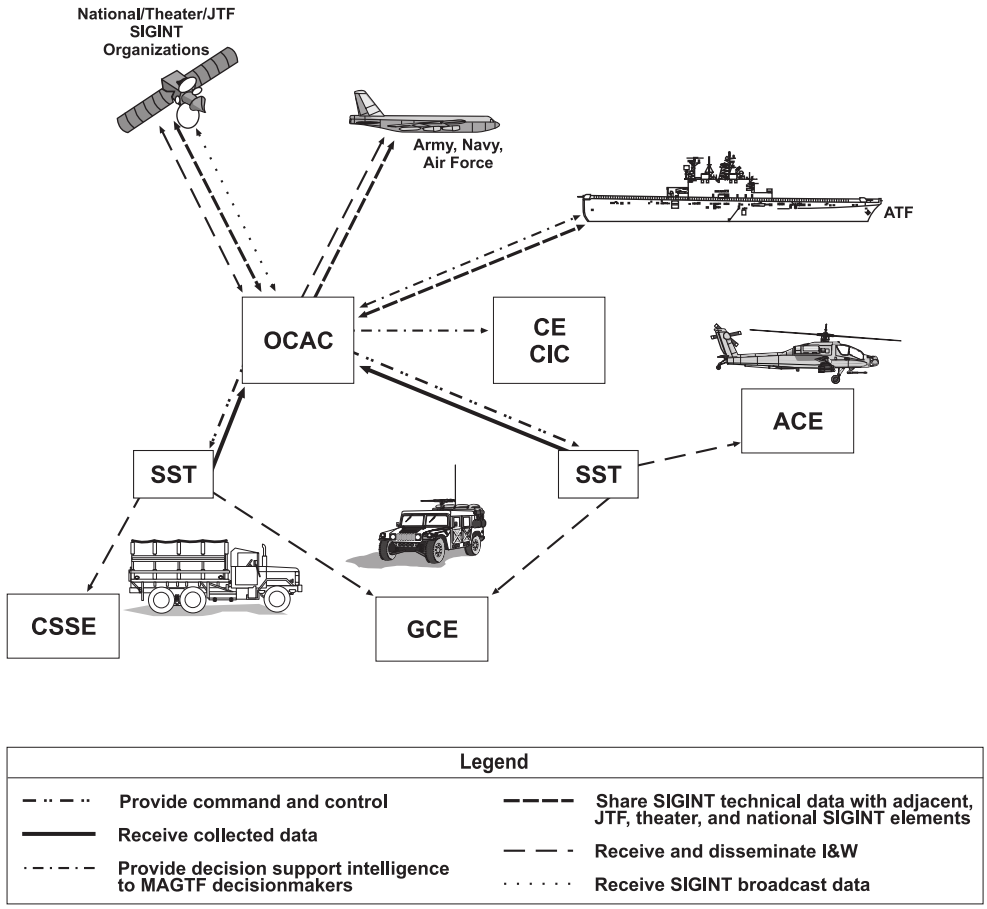


Figure 6-4. MEU(SOC) CE Ashore SIGINT Operational Architecture.

6003. Planning Consideration

The following are key CIS requirements and planning considerations in support of MAGTF SIGINT operations.

- Add the MAGTF CE, RadBn SSU, VMAQ TERPES, and other MAGTF elements to appropriate addressee indicator groups (AIGs) to receive pertinent JTF, theater, and national intelligence and SIGINT products.
- Obtain and activate SCI plain language addresses for MAGTF CE, RadBn SSU, and other MAGTF elements as appropriate.
- Determine and coordinate radio nets, supporting frequencies, and procedures for—
  - MAGTF external SIGINT operations.
  - MAGTF internal SIGINT operations.
  - Intelligence broadcasts.
  - Retransmission sites.
  - Routine and time-sensitive operations.
- Obtain authority and establish procedures for the sanitization of SIGINT products, reports, and other information.
- Determine and coordinate wire communications, to include telephones.
- Determine and coordinate SCI and GENSER LANs and WANs and unique intelligence networks information systems requirements (e.g., hardware, software, internet protocol addresses).
- Determine and coordinate SCI-courier requirements and operations.
- Integrate RadBn SSU and VMAQ CIS operations with those of other MAGTF and pertinent JTF and other components intelligence and reconnaissance units (e.g., mutual support, cueing).
- Integrate RadBn SSU, SSE, and SST, and VMAQ TERPES communications with collocated GCE, ACE, CSSE, and other MAGTF elements to—
  - Provide time-sensitive I&W and noncodeword (NCW) SIGINT reporting.
  - Coordinate with maneuver forces.
  - Support targeting.
  - Support force protection.
- Coordinate SIGINT CIS and dissemination operations and procedures with allied and coalition forces.
- Coordinate SCI and SIGINT CIS activation and restoration priorities and procedures.
- Determine unique COMSEC material system (CMS) requirements for SIGINT and SCI communications.
- Determine communications requirements between TSCIFs and mobile SCIFs and supporting security forces.

6004. SIGINT Communications

The SIGINT CIS architecture for any given operation is dynamic. Specific theater, JTF, or MAGTF reference documents include—

- CSPs developed for various OPLANs.
- Combatant commanders intelligence, CIS, and SIGINT tactics, techniques, and procedures (TTPs).
- Annexes B (intelligence), C (operations), and K (communications) of an OPORD.
- Appendix 2 (SIGINT) to annex B of an OPORD.

The MAGTF mission, threat signals environment, friendly concepts of operations and intelligence, and supporting task organization and command relationships influence which communications nets are established.

The following information addresses importan aspects of systems and technical architectures in support of MAGTF SIGINT operations.

a. MAGTF Command Element SIGINT Communications Nets

Figure 6-5 shows aspects of a notional CIS architecture for the MEF CIC. The following key SIGINT communications nets terminate within the MAGTF CE CIC or RadBn SSU.

(1) MAGTF DSSCS or Special Intelligence Communications Net External (HF). The DSSCS provides the MAGTF commander with a secure data communications channel for the exchange of SCI information and the receipt of record communications. The path is provided by the supported commander, and the terminal equipment and personnel are provided by the RadBn SSU. Key net participants include—

- The MAGTF CE via the RadBn SSU's special security communications element.
- Commander, joint task force (CJTF).
- Commander, amphibious task force (CATF).
- Other theater and national organizations.

(2) MAGTF Critical Communications Net (UHF-SATCOM/VHF). The critical communications (CRITICOMM) net provides the MAGTF commander communications with adjacent service cryptologic and other SIGINT and JTF elements and theater cryptologic support groups The path is provided by the supported commander, and the terminal equipment and personnel are provided by the RadBn SSCT. Key net participants include—

- MAGTF CE via the RadBn or SSU special security communications element.
- JTF.
- Adjacent headquarters.
- Theater and national intelligence or SIGINT agencies.

(3) Theater Cryptologic Support Net (HF/UHF-SATCOM). Theater cryptologic support net provides for rapid exchange of cryptologic information with the SIGINT elements of other organizations. The path is provided by the supported commander, and the terminal equipment is provided by the RadBn/SSU. Key participants include—

- RadBn OCAC.
- Adjacent service cryptologic elements.
- JTF or ATF SIGINT agencies.
- Theater and national SIGINT agencies.

(4) Tactical Receive Equipment and Related Applications Program Data Dissemination System. The TRE and related applications program data dissemination system (TDDS) broadcast provides I&W and global surveillance information in time for sensor cueing. Data is forwarded from sensor to communications gateways or relays for dissemination to worldwide military users via geosynchronous UHF satellite links. TDDS data sources include national and tactical sensor systems. Participants include the MAGTF CE CIC or SSU OCAC and other JTF, theater, and national intelligence centers and agencies.

(5) Tactical Information Broadcast Service. The tactical information broadcast service (TIBS) provides near-real-time intelligence from an open network of interactive participants using multiple sensors and sources. The TIBS broadcast uses UHF SATCOM assets for network operation and for the relay of out-of-theater specific information into the tactical users' areas of operation. TIBS participants include a wide variety of national and Service airborne, surface, and subsurface intelligence platforms. The broadcast will terminate in the MAGTF CE CIC or SSU OCAC.

(6) Tactical Intelligence Net. Tactical intelligence (TACINTEL) net is an automated, high speed data link for transmission and reception of SCI (data and voice) among SIGINT collection and production units during amphibious operations. Key participants include naval expeditionary force (NEF) and ATF SIGINT centers (within the SSES) and the RadBn and SSU OCAC.

(7) MAGTF-Internal Special Intelligence Communications Net (VHF/UHF/SHF). Special intelligence communications (SPINTCOMM) net provides the MAGTF commander with secure SCI communications with subordinate division or wing commanders through their organic SSCT.

The path is provided by the supported commander, and the terminal equipment and personnel are provided by the RadBn SSU or SSCT.

(8) TROJAN SPIRIT II Net. The Trojan Spirit II net (C and Ku band SATCOM) receives and disseminates intelligence information over a special-purpose satellite system. Key participants include the MAGTF CE CIC, RadBn SSU OCAC, amphibious task force intelligence center SSES and various external intelligence agencies and organizations.

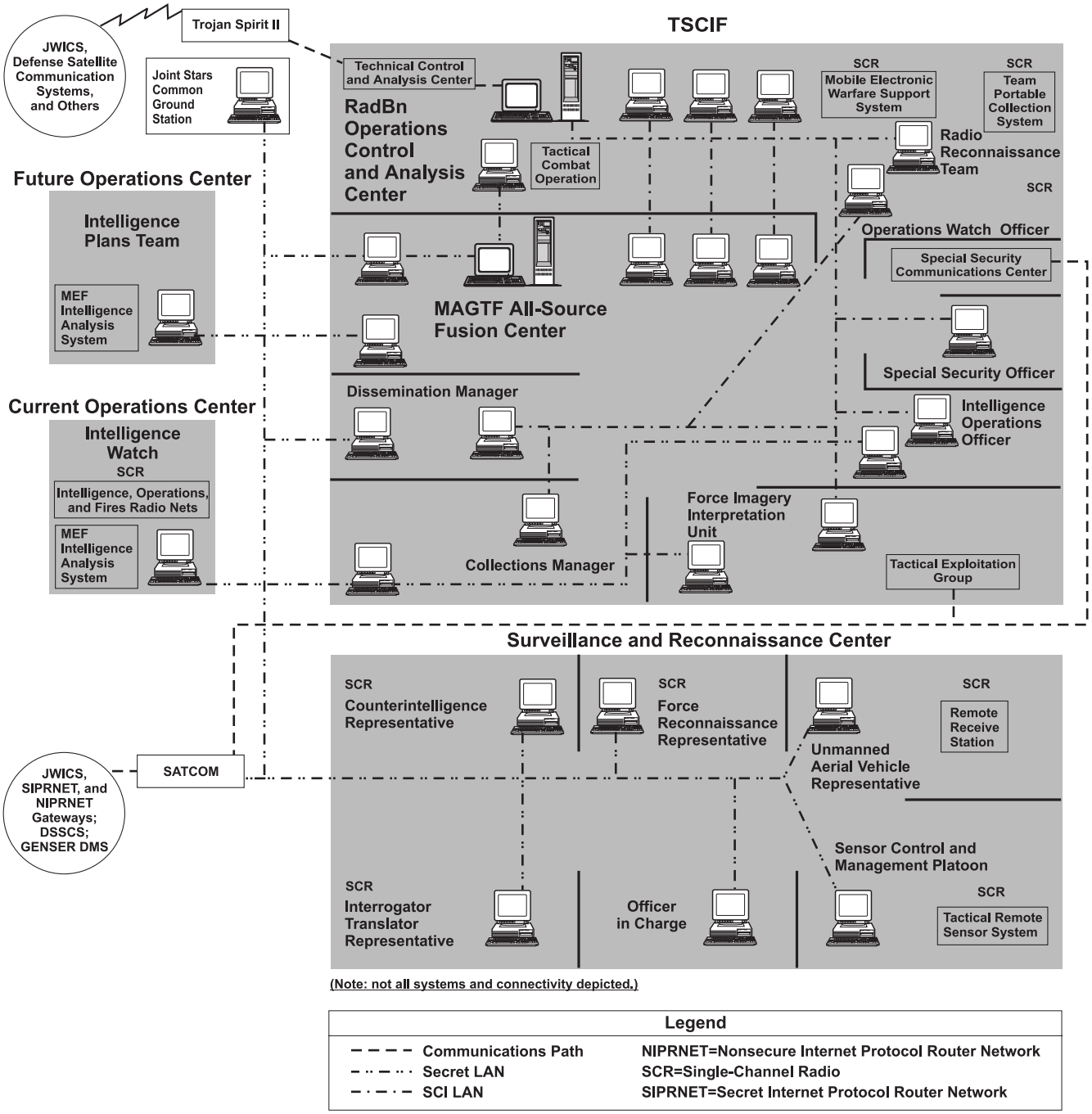


Figure 6-5. MEF CE CIC Communications and Information Systems Architecture.

b. Radio Battalion SIGINT Support Unit Internal Communications Nets

Figure 6-6 shows key aspects of the CIS architecture for the internal operations of the RadBn SSU. The following key communications nets terminate within the RadBn SSU OCAC.

(1) Command and Control Net (HF/VHF). The RadBn SSU C2 net provides the battalion commander or detachment OIC with C2 of subordinate elements. The path, equipment, and personnel are provided by the RadBn. Key net participants include the RadBn SSU OCAC and deployed collection and DF, EA, and RRT teams.

(2) Collection and Reporting Net (UHF-SATCOM/HF/VHF). The collection and reporting net provides C2 and SIGINT reporting net for RadBn SSU collection operations. Key participants include the OCAC and deployed collection and DF teams.

(3) Electronic Attack Control Net (VHF). The EA control net provides direction and control of RadBn EA teams and assets. The path, equipment, and personnel are provided by the RadBn SSU. Key participants include the OCAC and deployed MEWSS and EA teams.

(4) Direction Finding Flash Net (VHF). The DF flash net provides the DF control station with a means of broadcasting DF flashes to DF teams. The path, equipment, and personnel are provided by the RadBn. Key participants include the OCAC's DF control and deployed collection and DF teams.

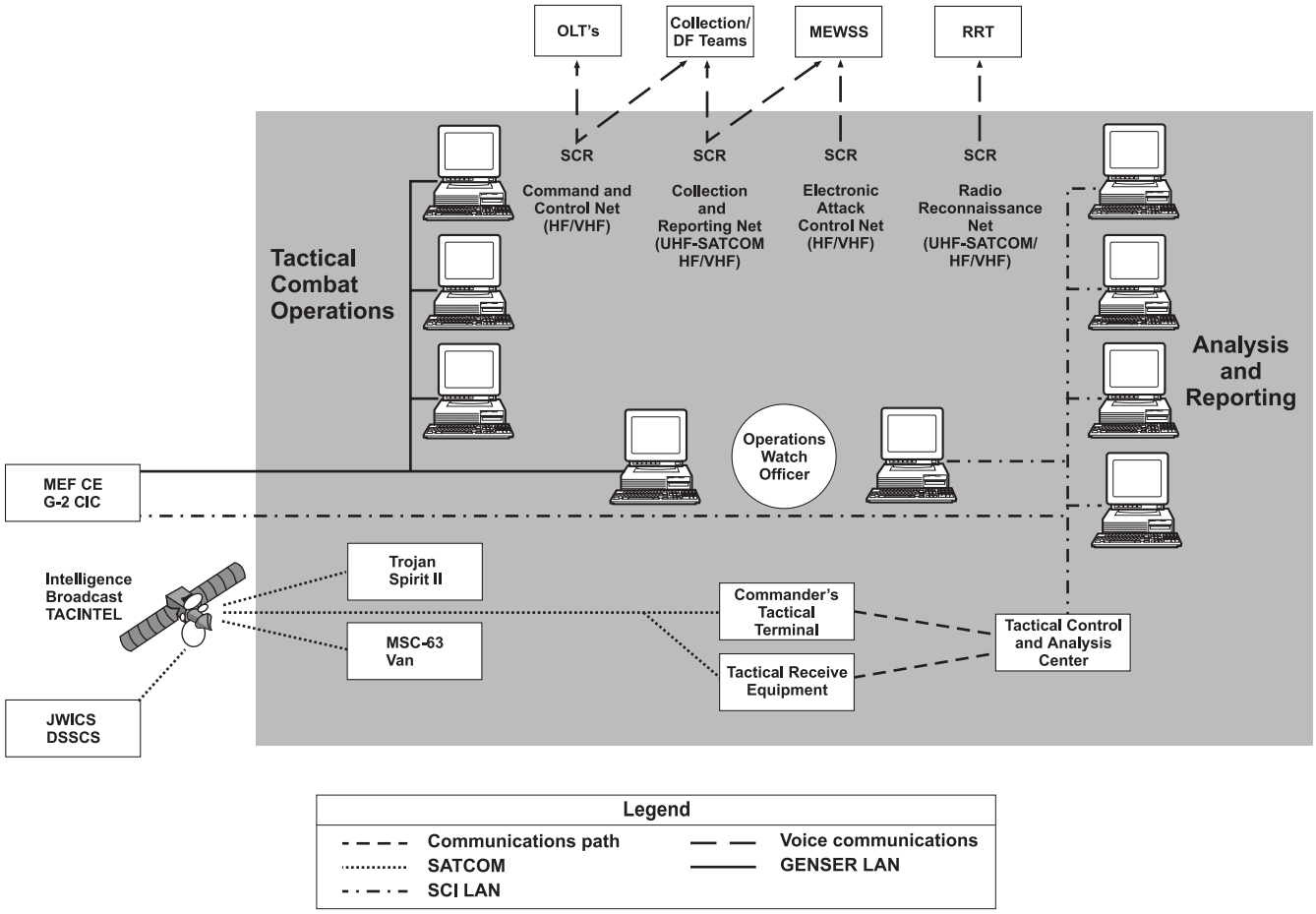


Figure 6-6. RadBn SSU Operations Control and Analysis Center Communications and Information Systems.

(5) Direction Finding Report Net (VHF). The DF report net provides reporting from DF outstations to the OCAC DF control. Path, equipment, and personnel are provided by the RadBn SSU.

(6) Direction Finding Data Net (VHF). The DF data net exchanges DF information between the deployed collection and DF team and the OCAC DF control. The path, equipment, and personnel are provided by the RadBn.

(7) Mission Equipment Control Data Link Net (UHF). The mission equipment control dat link (MECDL) net provides the means to control, coordinate, and monitor the mission equipment of MEWSS teams. This net is used for internal MEWSS operations and for interface and coordination with the Army intelligence and EW common sensor systems.

(8) Tasking and Reporting Net (VHF) The tasking and reporting net provides a means for the RadBn to task deployed collection teams and to report SIGINT information.

(9) Radio Reconnaissance Command Net (UHF-Tactical Satellite/HF) The radio reconnaissance command net provides the means to command and control deployed RRTs and their reporting of SIGINT collection and DF reports to the RadBn SSU OCAC.

c. Marine Tactical Electronic Warfare Squadron Communications Nets

Figure 6-7 shows key aspects of the CIS architecture for VMAQ TERPES operations. The following key SIGINT communications nets terminate within VMAQ operations or TERPES elements.

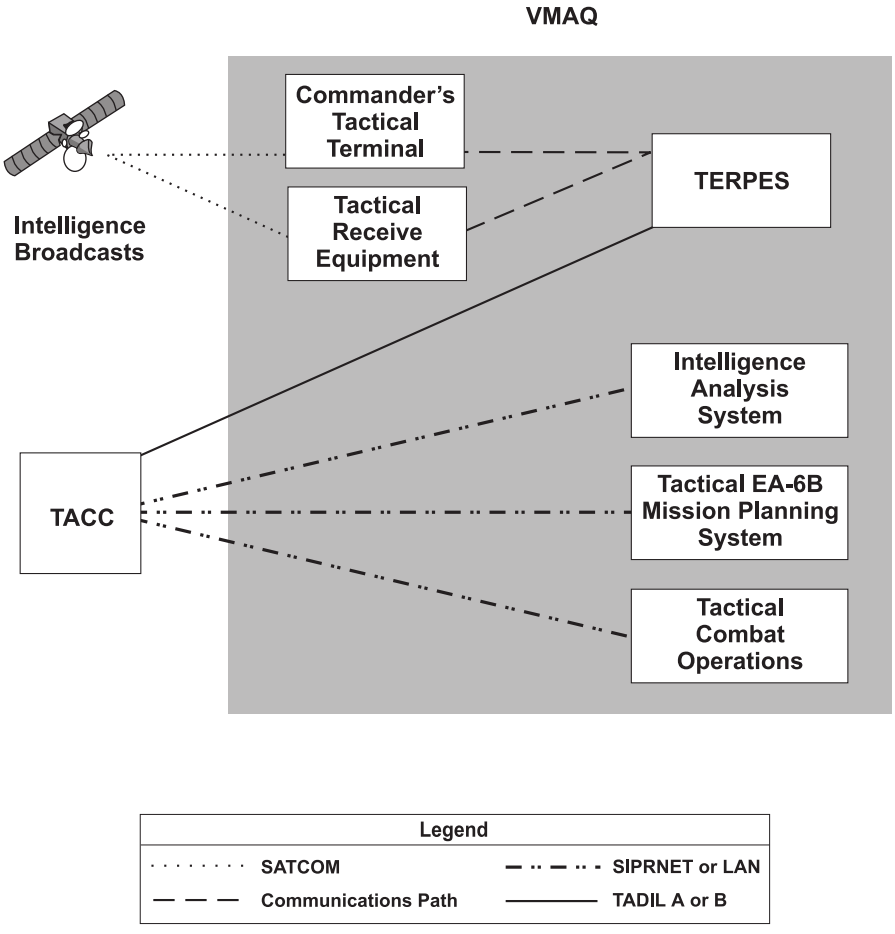


Figure 6-7. VMAQ Operations Center and TERPES Communications and Information Systems.

(1) Aviation Combat Element Command Net (HF). The ACE command net provides a means for the ACE commander to exercise command and coordinate subordinate units' administrative and logistic functions. Composition includes ACE headquarters, MAG detachments Marine air control group or detachment, and independent squadrons or battalions.

(2) Aviation Combat Element Intelligence Net (VHF/HF/UHF). The ACE intelligence ne provides a means for rapid collection and dissemination of intelligence between the ACE headquarters and subordinate units. Composition includes the ACE headquarters, the TACC, MAGs or squadrons headquarters, the tactical air operations center (TAOC), direct air support center (DASC), TERPES, and others as appropriate.

(3) Tactical Digital Information Link A (HF/UHF). Tactical digital information link A (TADIL-A), also called Link-11, is used to exchange tactical data in real time among ships, aircraft, and shore sites. TADIL-A messages provide navigational data, surface and subsurface tracks, and operational orders. TADIL-A is an encrypted half-duplex system. It can be used on either H single- or dual-sideband or UHF frequencies.

There are two data rates:

- Fast, at 2250 bits per second (bps) which is the most used data rate.
- Slow, at 1364 bps.

TADIL-A is available within the United State Navy, Air Force, Marine Corps, and Army. The MAGTF's C2 nodes that can use TADIL-A are the TAOC and the TACC. The exchange of digital information by TADIL-A is accomplished by net-configured participating units (PUs) under the control of a net control station (NCS). A net can be composed of as few as two PUs (e.g., TERPES, via the TACC, and the TAOC).

(4) Tactical Digital Information Link B (Multichannel Radio). TADIL-B, multichannel radio (MUX), (also known as Link-11B) is a full-duplex, point-to-point, encrypted system that simultaneously exchanges tactical data between two units capable of TADIL-B at a rate of 600 1200, and 2400 bps. TADIL-B messages provide navigational data, surface and subsurface tracks, and operational orders. It may use VHF, UHF, SHF, and ground mobile force-SATCOM MUX systems. Additionally, TADIL-B can also be exchanged over wire. TADIL-B is used by the United States Air Force, Army, and Marine Corps. MAGTF C2 nodes with TADIL-B capability are the TACC, TAOC, and Marine air traffic control detachment (MATCD). Participants on a TADIL-B network, such as TERPES, are called reporting units (RUs). Some RUs are capable of simultaneously linking with several other RUs. Those units that can redistribute the information re ceived from one RU to another RU are called forwarding reporting units (e.g., TACC and TAOC).

(5) Tactical Digital Information Link C (UHF). TADIL-C, also called Link-4A, is used by the North Atlantic Treaty Organization (NATO) and the United States Armed Forces. TADIL-C is an unencrypted, computer-to-computer digital information link that operates in the UHF frequency range at 5000 bps. The TADIL-C link is between a controlling unit and a controlled tactical aircraft. TADIL-C is a valuable means for providing radar track correlated symbology both up to the aircraft and, in the case of two-way transmissions, back down to the controlling agency. The MAGTF TAOC uses the TADIL-C for one-way and two-way links to control F-14, F/A-18, EA-6B, and S-3 aircraft.

(6) Voice Product Net (UHF). The voice product net (VPN) provides a communications means for forwarding nondigital intelligence information to other intelligence and operations elements. Key MAGTF participants include the TACC, TAOC, EA-6B, and TERPES, as well as other MAGT external platforms (e.g., Rivet Joint, Compass Call, EP-3).

Chapter 7

Planning and Operations

The purpose of SIGINT operations is to develop intelligence on the enemy's capabilities, intent, and operations by exploiting the enemy's use of communication, radars, and electronic systems.

Section I. SIGINT Functional Planning

Detailed planning must precede actual SIGINT operations to take advantage of the wealth of information available on the adversary's signals emanations and operations.

7101. SIGINT Concept of Operations

SIGINT operations must support the commander's intent, concept of operations, and the supporting concept of intelligence operations.

Questions that must be answered to develop the SIGINT concept of operations include the following:

- What is the MAGTF area of operations (AO) and area of interest (AI)?
- What is the MAGTF concept of operations, task organization, and main and supporting efforts? Does the friendly concept of operations allow for fixed-site SIGINT collection and DF operations, mobile collection and DF operations, or both?
- What are the standing PIRs and IRs? Which have been tasked to SIGINT units? What specific information is the commander most interested in (e.g., enemy air operations, enemy ground operations, friendly force protection, target battle damage assessment [BDA], or enemy future intentions)?
- What is the MAGTF force protection concept of operations?
- What is the MAGTF concept of fire support? How will MAGTF target development and target intelligence be conducted?
- What are the SIGINT and intelligence concepts of operations of other JTF components, the JTF, and theater resources? What are the task organization and command or support relationships for all other MAGTF intelligence and reconnaissance units?
- How can shipboard SIGINT assets and other JTF, theater, and national SIGINT assets be integrated and employed to support MAGTF operations?

7102. Enemy Characteristics

Intelligence operations focus on the enemy. Prior to commencing SIGINT operations, MAGTF intelligence personnel must learn as much as they can about the following enemy C2 CIS practices.

a. Size and Composition of Enemy Forces

- What threat forces are within the MAGTF AO and AI?
- What are the enemy's centers of gravity and critical vulnerabilities?
- Is this a large enemy force organized along conventional military lines or a small, loosely knit guerrilla or unconventional military force?

b. Enemy Command and Control and Supporting Communications and Information Systems

- What and where are the enemy's critical C2 nodes and what are their vulnerabilities?
- What types and categories of communications nets and networks are used by the enemy?
- What echelons of command do the communications nets and networks serve?
- What are the associated communications and noncommunications electronic emitters?
- What are the tactics, techniques, and procedures used for enemy CIS operations? How do they relate to various threat functional activities?
- How is information transferred among the enemy's units and command echelons?
- Does the enemy employ communications emitters at all levels of command or does it rely on communications means less exploitable by SIGINT (e.g., fiber, wire, and messenger)?

c. Emitter Technical Data

Effective SIGINT operations require extensive technical information on the enemy's CIS resources and operations. See table 7-1 for key threat emitter technical data requirements.

Table 7-1. Emitter Technical Data.

Aspect	Technical and Operational Characteristics
Communications Operations and Emitters	
Frequency range and use	HF, VHF, UHF, etc.
Call sign use	Rota, random, etc.
Transmitter power	Hearability, SIGINT collection, and DF location requirements
Emission type	Single, multichannel, spread spectrum, frequency hopping, burst, etc.
Signal type	Analog or digital
Modulation	AM, FM, PCM, etc.
Cryptologic system	Public, private key, none
System type	Voice, data, teletype, facsimile, video, combinations of some or all
Language use	Dialect, written, or voice
Miscellaneous	Communication procedures, emissions control practices, use of deception, security systems, etc.
Noncommunications Operations and Emitters	
Location	Fixed, mobile
Platform	Air, ship, vehicle, fixed-installation
Associated C2 node or weapon system	Command post, type of weapon system
Frequency range	Band of operation
Modulation characteristics	Pulse duration, pulse repetition frequency, etc.
Transmitter power	Effective radiated power, effective range
Purpose of function	Jamming, surveillance, targeting, C2, fire control, etc.

7103. Topography

Terrain, physical obstructions, and vegetation in the area of operations have a major effect on the employment of SIGINT resources and their ability to exploit enemy signals. Proper placement of SIGINT collection and DF assets is essential for effective reception of adversary emanations. Several factors affect reception quality.

a. Target Frequencies

Many of the frequency ranges and power levels in use by the world's military and paramilitary forces require line-of-sight (LOS) or near-LOS paths from transmitter to receiver. Generally, the higher the frequency used, the greater the LOS influence and the more critical the accurate placement of SIGINT collection and DF equipment. Lower

frequencies (particularly those below 30 MHz) generally do not require LOS paths. Consequently, the placement of SIGINT collection and DF sites to exploit these frequencies may be located at greater distances from the target transmitters.

b. Power Output

The power output of a transmitter is an important factor in receiving the signal. To intercept some low-powered signals, SIGINT collection and DF assets must be located closer to the adversary's transmitter, often requiring SIGINT collection and DF teams to either collocate with or closely follow forward MAGTF combat units.

c. Antennas

If the targeted adversary's system uses highly directional antennas, as do many multichannel systems, the SIGINT collection and DF site must be placed within the adversary's antenna radiating pattern.

7104. Planning Responsibilities

Primary staff responsibility for SIGINT operations planning lies with the G-2/S-2. The G-2/S-2 responsibilities are—

- Preparing integrated, multidiscipline intelligence and reconnaissance operations, to include supporting SIGINT plans, orders, annexes, and appendices.
- Coordinating with the G-3/S-3 to ensure—
  - Planned SIGINT effort will support the concept of operations and scheme of maneuver.
  - SIGINT and EW operations are effectively prioritized and integrated.
  - Adequate site placement and security for SIGINT collection elements is provided.
- Coordinating with the G-6/S-6 officer for CIS support to the SIGINT elements, including circuits and networks access, frequency assignment, equipment, and call signs.
- Acting as liaison with SIGINT agencies and units external to the MAGTF.
- Coordinating with the G-4/S-4 to ensure adequate logistics support of SIGINT elements (e.g., transportation and maintenance of SIGINT units' unique equipment).

7105. Coordination of SIGINT Operations

a. Internal Coordination

Internal MAGTF SIGINT requirements must be coordinated with maneuver, fires, electronic warfare, force protection, and CIS requirements. This coordination may occur within the EWCC under G-3/S-3 staff cognizance, within the CIC, or within the OCAC, depending upon the task organization and C2 and support relationships in effect. Additionally, collection and DF team movements and locations must be coordinated with the MAGTF's tactical movements to ensure continuous support without interference.

These efforts are accomplished through planning and close coordination among the following MAGTF staff officers:

- MAGTF G-2/S-2, the intelligence operations officer, and the intelligence battalion commander.
- SIO, MAGTF AFC OIC, collections officer, SARC OIC, and the dissemination manager.
- MAGTF G-3/S-3 future and current operations officers, C2W officer, and EWO.
- MAGTF G-6/S-6.
- GCE, ACE, and CSSE staff officers.
- RadBn SSU and VMAQ TERPES COs and OICs.

b. External Coordination

(1) Higher Headquarters and External Organizations. The MAGTF G-2/S-2 and all SIGINT planners must coordinate SIGINT operations, activities, and requirements with DIRNSA. Accordingly, a continuous exchange of

data and information is required. This requires JWICS access and special security communications circuits for the exchange of SIGINT technical data and intelligence information.

(2) Adjacent and Area SIGINT Activities. MAGTF SIGINT activities must be coordinated with other SIGINT activities within the joint operations area and theater to reduce duplication and to ensure maximum use of available assets and mutual support. For example, an NSG-fixed site outside the MAGTF tactical operations area could be conducting SIGINT collection and DF against targets within the MAGTF area of responsibility. With proper planning and coordination, external SIGINT assets of the combatant commander, JTF, and other components can provide SIGINT support to the MAGTF (e.g., product reporting, exchanges of technical information), allowing organic MAGTF SIGINT resources to focus on critical targets.

Section II. SIGINT Operational Planning

This section provides a general description of the SIGINT planning cycle and activities to enable an understanding and appreciation for the SIGINT effort as a whole. No attempt is made to provide technical details for SIGINT processing. The SIGINT cycle is in concert with the following six phases of the intelligence cycle (see MCWP 2-1 for additional information on the intelligence cycle and intelligence planning).

7201. Planning and Direction

The planning and direction phase of the intelligence cycle consists of those activities which identify and prioritize pertinent IRs and provide the means for satisfying them. Intelligence planning and direction is a continuous function and a command responsibility. The commander directs the intelligence effort; the intelligence officer manages this effort based upon the commander's intent, designation of PIRs, and specific guidance provided during the planning process. The intelligence planning and direction functions are—

- Requirements development.
- Requirements management.
- Collections management.
- Production management.
- Dissemination management.
- Intelligence support structure.
- Supervision of the intelligence effort.

SIGINT planning is performed in concert with overall intelligence planning. It consists of those activities that identify pertinent IRs which have been tasked to SIGINT units and then provides the means for satisfying those IRs. SIGINT planning and direction is a continuous function that requires close interaction between the G-2/S-2 and SIGINT unit planners.

SIGINT planning and direction objectives include—

- Identifying intelligence requirements tasked to SIGINT elements.
- Preparing a SIGINT operations plan, to include integral SIGINT collection, production, and dissemination plans.
- Planning and establishing the SIGINT support system (e.g., CIS, logistics).
- Issuing orders and tasking to SIGINT units.
- Supervising and coordinating the SIGINT operations.

The selection of a particular source of information or intelligence discipline to fulfill a given intelligence requirement is an important decision. SIGINT is a valuable source of information, and an effective, dynamic SIGINT operations plan must be developed to maximize the effectiveness of the SIGINT effort. With the multitude of threat signals being transmitted, the collection plan must be carefully constructed to collect and exploit enemy signals that are most likely to provide the necessary intelligence data. Additionally, the SIGINT production and dissemination plans must effectively support unique SIGINT and all-source intelligence operations requirements and operations.

a. Mission Planning

Based on the commander's PIRs and IRs, the G-2/S-2 determines those ICRs which are applicable to and have the potential to be satisfied by the organic SIGINT collection effort. The G-2/S-2 incorporates these ICRs into the overall intelligence collection plan and issues mission tasking and guidance to the RadBn OIC, ACE G-2/S-2, and other attached or supporting SIGINT units. Additionally, SIGINT taskings from the joint force commander (JFC) and supplemental taskings from DIRNSA will need to be assessed by the G-2/S-2 and incorporated if possible into MAGTF SIGINT operations (refer to USSID 4 for additional information regarding DIRNSA supplemental tasking).

b. Mission Management

SIGINT mission management is the unit commander's supervision of collection, processing, production, and dissemination efforts. Proper mission management requires centralized control of SIGINT assets at the MAGTF command element level. The OCAC (for RadBn SSUs) and the TERPES section (for VMAQ) provide this centralized control for the their respective SIGINT efforts. Collection and DF elements are usually positioned throughout the MAGTF's operations area based on the MAGTF's focus of effort, scheme of maneuver, hearability of enemy signals, and security of SIGINT units. Air SIGINT operations in support of both ACE and MAGTF requirements will be planned and incorporated in the supporting air tasking order (ATO). SIGINT unit commanders and planners must ensure that coverage is complete, that assets are gainfully employed or redirected, and that SIGINT reporting (and supporting CIS support) is effective. Collection tasks must be analyzed to determine if they can be met or if new collection or analysis efforts are required. The collection, direction finding, and analysis and production efforts must be supervised, integrated with all-source intelligence operations, and evaluated to ensure mission effectiveness.

7202. Collection

During collection, organic, attached, and supporting SIGINT elements collect and deliver information to the appropriate processing or production element (e.g., OCAC or TERPES). In some instances (e.g., immediate threat) the information will be delivered directly to the local commander for immediate action.

a. COMINT Collection

COMINT collection is performed using equipment that intercepts adversary communications signals. Simple signals (e.g., unencrypted single-channel voice) can be received by ordinary receivers. More complicated signals or those that are encrypted require more sophisticated equipment to fully exploit the signals for their intelligence value (i.e., external SIGINT processing and production centers such as the RSOCs or NSA).

Initially, a concentrated intercept search, signals analysis, and target development program is carried out to catalog the electromagnetic environment and identify the desired threat SOIs. In many cases, prior knowledge of some technical characteristics, such as in RSOC or CSSA data bases, will enhance and streamline the MAGTF's COMINT search effort. When SOIs are acquired that are readily exploitable, SIGINT collection operators prepare a gist of the transmission. Recording of the entire intercepted signal using tape recorders may also occur.

Multichannel transmissions are first divided by SIGINT operators into their component parts or separate channels and then processed channel by channel. The acquired data (e.g., logs, gists, data files, page-prints, tapes) are rapidly assessed against standing PIRs for items of immediate tactical intelligence value and reported in accordance with reporting and dissemination criteria to—

- Designated commanders.
- OCAC or TERPES production elements for detailed analysis and reporting.
- MAGTF AFC for all-source analysis and production.

b. Direction Finding

Radio DF uses electronic equipment to obtain the locations of adversary emitters by determining the direction of arrival or the time difference of arrival of the radio waves. In ideal conditions, direction finders are arrayed in a network along a predetermined baseline consisting of at least three collection and DF stations, one of which acts as net control. The DF sites must be placed carefully so that all stations can hear the target SOI and mutually support the mission.

Close coordination between collection and DF sites and the OCAC is required for a responsive DF effort. RadBn SSU DF results are then reported, either manually or via automated means, to

the OCAC for follow-on intelligence exploitation and reporting.

c. ELINT Collection and Direction Finding

Although few in numbers, the RadBn MEWSS product improvement program (PIP) (AN/MLQ-36A) provides for the automated search, acquisition, identification, and a single DF line of bearing of radars and other noncommunications emitters. Mission management, reporting, and dissemination are handled similarly to COMINT DF operations.

Additionally, in support of its strike escort mission, VMAQ elements collect ELINT information that can be used by MAGTF intelligence producers such as the MAGTF AFC and OCAC. Technical capabilities within the EA-6B's ELINT collection system allow for DF operations to occur from a single aircraft. Acquired signals are recorded and then provided to the TERPES section for postmission analysis, production, and reporting.

7203. Processing and Exploitation

The following processing and exploitation functions are used to convert collected raw information into a form suitable for SIGINT production.

a. Traffic Analysis

Traffic analysis is the study of all characteristics of communications except encrypted texts. Call signs, frequencies, times of transmission, cryptographic indicators, precedence, and message lengths are examples of these characteristics. These characteristics are called externals and are compiled and sorted primarily for the purpose of reconstructing the adversary's communication structure and organization. This information yields valuable electronic order of battle data and other information. With on-line communication encryption systems becoming widely used by potential adversaries, traffic analysis becomes an increasingly difficult function.

b. Cryptanalysis

Cryptanalysis is the study of encrypted signals, data, and texts to determine their plain language equivalents. The capability to read the adversary's encrypted communications is obviously valuable. The RadBns' limited cryptanalysis capability depends on the sophistication of the target's encryption system and the availability of specialized equipment and software resources from NSA.

c. Linguistic Analysis

Linguistic analysis is the transcription and translation of foreign language intercepts into English. This analysis starts at the collection site upon interception. Messages of considerable length require more time and are usually transcribed and translated in the OCAC. Marines are trained in a wide variety of languages for this task, but augmentation by external sources (e.g., native and/or contract linguists) may be required in order to satisfy all requirements.

d. Signal Analysis

Signal analysis consists of working with all types of signals (e.g., COMINT, ELINT, pro forma) to identify, isolate, reduce to pure form, and exploit acquired SOIs. The signal analyst must be well trained and possess the proper electronic and software support tools to be effective.

e. ELINT Analysis

The location of early warning, surveillance, and fire control radars can provide a general trace of the adversary's forward battle positions and locations of key C2 and fire control nodes and weapons systems. Medium-range and counterweapons radar identification provides order of battle information since these systems are organic to specific adversary units.

Identification and location of air defense radars provide information on the disposition of the adversary's air defense systems and their threat to strike, close air support, and assault support aircraft. Following the reporting of any I&W information to tactical decisionmakers, technical data and detailed ELINT information is forwarded to

the OCAC or to the TERPES section for further analysis, production, and reporting.

7204. Production

Production is the conversion of raw information into SIGINT product reports through the evaluation, integration, and interpretation of the information derived during the processing and exploitation effort. The results of the analysis are correlated by SIGINT analysts and reporters to form the basis for SIGINT reports. These reports are provided directly to tactical commanders when appropriate, to the G-2/S-2 for the further analysis and production of all-source intelligence, and to the staff sections for future operations planning.

SIGINT production planning and management are closely coordinated with all-source intelligence production planning and management to—

- Determine the scope, content, and format for each product.
- Develop a plan and schedule for the development of products.
- Assign priorities among the various SIGINT product requirements.
- Allocate SIGINT processing, exploitation, and production resources.
- Integrate production efforts with all-source collection and dissemination activities.

The production goal is the effective and efficient use of limited resources while focusing on established SIGINT priorities.

a. Evaluation

SIGINT analysts evaluate the raw SIGINT information to determine its pertinence to intelligence requirements. Further evaluation is made to judge the reliability and accuracy of the information and to isolate significant elements.

b. Integration

The information derived from traffic analysis, cryptanalysis, linguistic analysis, signal analysis, ELINT analysis, and radio DF must be fully integrated into a fused SIGINT product to develop a complete SIGINT picture. Concurrently, integration of SIGINT processing and production with ongoing MAGTF G-2/S-2 all-source intelligence processing and production is essential to achieve a complete, effective, and current intelligence estimate while using the strengths and results from the other intelligence disciplines to improve SIGINT operations.

c. Interpretation

The information derived from SIGINT collection is interpreted to form logical conclusions and estimates of enemy capabilities, intentions, and future actions. This step completes the translation of the raw SIGINT information into usable intelligence.

7205. Dissemination

Dissemination is the provision of SIGINT information in a timely manner and in a usable form to commanders, other decisionmakers, or all-source intelligence analysts. Because of security requirements, dissemination of COMINT information is made primarily to SIGINT and all-source intelligence production elements such as the MAGTF AFC. Proper SIGINT C2 and supporting CIS architectures that provide accurate situational awareness, along with effective IRs and tactical requirements management, enable proper dissemination.

SIGINT dissemination planning and management involves establishing dissemination priorities, stipulating dissemination and reporting criteria, selecting dissemination means, and monitoring the flow of SIGINT reporting. The ultimate dissemination goal is to deliver SIGINT products to the appropriate user in the proper form and at the right time, while concurrently preventing the dissemination of irrelevant products and avoiding information overload.

Reporting consists of providing the SIGINT products in standardized, easily usable formats needed to satisfy tasked requirements in a timely manner. The nature of the SIGINT effort requires timely reporting to effectively exploit its intelligence value. SIGINT reports generally fall into two categories, product reports and technical reports. Standardized formats are used in the preparation and transmission of these reports for speed and compatibility. As most of these formats are classified, readers should refer to USSID 300, S***IGINT Reporting***, for specific information and examples.

a. Product Reports

Product reports are prepared by all SIGINT producers for commanders, planners, and all-source intelligence analysts. A product report contains timely, accurate, thorough, relevant, and useful SIGINT information about the adversary in response to the supported commander's PIRs and IRs. Reports may be sent periodically or may be sent whenever highly perishable data is acquired in accordance with specified intelligence reporting criteria. Generally, SIGINT product reports will fall into one of three categories:

(1) SIGINT Report. In SIGINT reports, the source of information is clearly SIGINT by the content and classification markings. Such reports generally contain the SIGINT assessment along with pertinent SIGINT technical information. These reports are handled within SCI-controlled facilities and communications channels. Within a MEF, the CE, GCE, and ACE may be included in distribution for SIGINT products. Within a MEU(SOC) or special-purpose Marine air-ground task force (SPMAGTF), the CE is generally the sole recipient of these reports. When pertinent, either these reports will be fused within all-source intelligence products for further dissemination within the MAGTF or dissemination will occur via SCI courier or briefings.

(2) Non-Codeword Report. NCW reporting procedures may be used only when authorized by DIRNSA. The principal value of NCW reporting is to allow time-sensitive dissemination of critical SIGINT information to a broader audience during high tempo operations. In NCW reports, the source of information is clearly SIGINT. However, unlike standard SIGINT product reports, the NCW report is passed directly to commanders without SIGINT markings or SI security controls to allow immediate tactical use (e.g., I&W, support to targeting, support to force protection). For example, NCW reports may be passed directly from the SSU collector to other MAGTF units (e.g., an infantry battalion) via GENSER communications (usually voice message). Typically, the format for these is the standard size, activity, location, unit, time, and equipment (SALUTE) report. Specific procedures regarding NCW reporting during operations should be contained within the SIGINT appendix to annex B of the operations order.

(3) Sanitized Report. Sanitized SIGINT reports contain SIGINT information that is reported via GENSER communications means in a manner that does not reveal SIGINT as the source of the information. The level of sanitization authority allowed the MAGTF commander is established by DOD Directive TS-5105.21-M-2, ***Sensitive Compartmented Information (SCI) Security Manual, Communications Intelligence (COMINT) Policy***. Within the MAGTF, actual sanitization of SIGINT reports is generally performed by designated intelligence personnel under the guidance and supervision of the MAGTF SSO or AFC OIC. The reports are disseminated via all-source products or other GENSER intelligence reports.

b. Technical Reports

Technical reports consist of the SIGINT technical elements required by SIGINT collectors, analysts, and technical support and production agencies external to the MAGTF (e.g., call signs, frequencies, operating schedules). SIGINT technical reporting requires SCI-secure connectivity with pertinent organizations (e.g., NSA, theater RSOC, supporting CSSA) via JWICS, NSANET, or some alternate SCI communications means. Within the MAGTF, all SIGINT technical reporting is conducted by either RadBn or VMAQ's TERPES section.

7206. Utilization

SIGINT, as all intelligence, has no inherent value. Its value is realized only through its effective support of the commander's intelligence requirements or other operational requirements. Commanders, G-2/S-2s, and G-3/S-3s must continuously evaluate SIGINT operations, products, and reports for timeliness, usefulness, and overall quality and responsiveness to stated IRs. They must provide feedback to the MAGTF G-2/S-2 and SIGINT unit leaders to improve future SIGINT operations. Ultimately, SIGINT utilization provides guidance for future intelligence and SIGINT operations and management.

See appendix C, SIGINT and SCI Security Management Operations Flowchart, that summarizes the principal SIGINT planning considerations, activities, and products discussed in this chapter.

Section III. SIGINT Plans and Orders

Guidance for the conduct of SIGINT operations comes from many sources. The DIRNSA-developed USSID series are the principal SIGINT operations directives that contain policy, direction, guidance, instruction, and procedures on performing SIGINT functions in compliance with national directives and security requirements. Additionally, since MAGTFs will normally be part of a JTF or NEF, reference to joint and naval orders, guidance, and SIGINT TTPs is necessary to identify unique operating concepts and methodologies and support procedures and formats.

The MAGTF G-2/S-2 prepares SIGINT plans and orders. The intelligence operations officer coordinates the overall effort with the assistance of the SIO, other intelligence section staff officers, and the CO or OICs of organic and supporting SIGINT units. SIGINT plans and orders focus on internal MAGTF SIGINT requirements, operations, and TTP.

The SIGINT appendix will appear as appendix 2 (signals intelligence) to annex B (intelligence) in all MAGTF operations plans and orders. (See appendix D, SIGINT Appendix Format, of this manual for a recommended format for the SIGINT appendix.) It should include the following:

- Friendly forces to be utilized include—
  - Personnel augmentation requirements.
  - SIGINT units of adjacent or other theater forces and the support expected.
  - Joint force maritime component commander (JFMCC) and ATF DS SIGINT elements and CSSA available to support the landing force during amphibious operations.
  - RSOC, joint force land component commander (JFLCC), joint force air component commander (JFACC), and other component commanders or task forces capable of providing SIGINT support during JTF operations.
- Planned arrangement, employment, and use of external SIGINT support, to include any special collection, production, dissemination and CIS arrangements.
- Establishment of coordinating instructions for SIGINT operations planning and control, to include technical support expected from higher headquarters.
- MAGTF SIGINT element taskings.
- Communication and information SIGINT support.

Section IV. Execution

MAGTF SIGINT operations generally are centrally managed by the MAGTF G-2/S-2 and decentrally executed to—

- Integrate RadBn SSU and ACE VMAQ TERPES SIGINT effectively with other MAGTF and external intelligence and reconnaissance operations.
- Provide the most effective MAGTF intelligence requirements support.

The integration of RadBn SSU and VMAQ TERPES SIGINT collection, production, and dissemination plans and activities with those of other MAGTF and supporting intelligence organizations uses these limited resources and their mutual support more effectively (e.g., cueing). The MAGTF mission, commander's intent, threat operations and signals usage, concept of operations, and environmental considerations all influence the ultimate task organization, command relationship, concepts of employment, and tasks of SIGINT units. For example, they determine a decision to task-organize elements of the SSU in direct support of the GCE or rear area operations commanders. Such information is specified within annexes B, C, and K of the operations order or in a subsequent fragmentary order.

Figure 7-1 notionally depicts the following seven key aspects of these interrelated SIGINT operations.

- Task organization and command or support relationships of MAGTF SIGINT units with other MAGTF elements. RadBn SSU OCAC is collocated with the MAGTF G-2/S-2 and operates in general support of the MAGTF. VMAQ and TERPES are organic and OPCON to the ACE.
- External SIGINT units that typically support a MAGTF.
- Principal SIGINT systems employed within and in support of the MAGTF.
- Relationship of other MAGTF intelligence and reconnaissance units with SIGINT units.
- Principal communications pathways, means, and level of classification.
- Key intelligence information systems that interoperate with SIGINT systems.
- Principal SIGINT reports disseminated via the communications pathways shown.

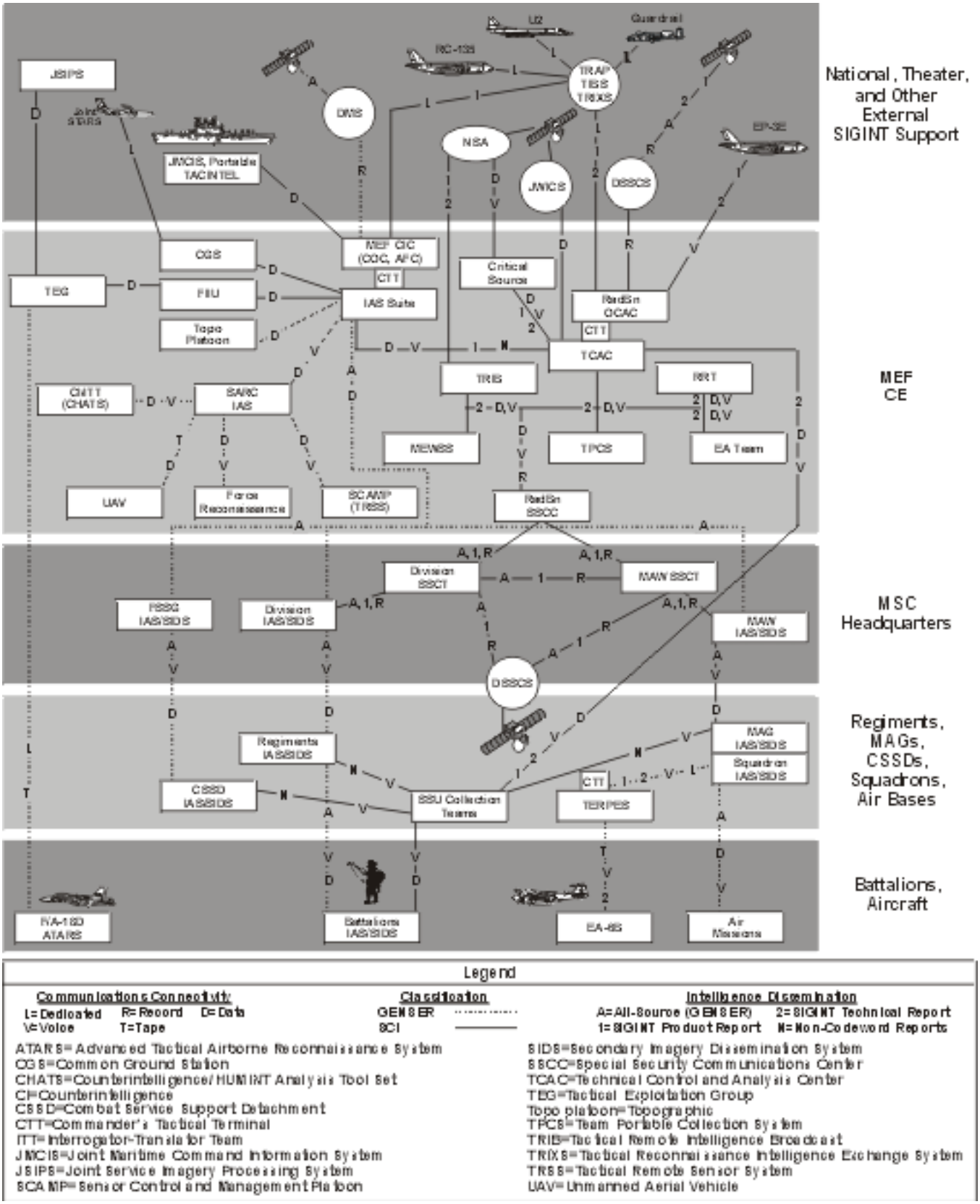


Figure 7-1. MAGTF and Supporting SIGINT Operations.

(reverse blank)

Chapter 8

Security of Sensitive Compartmented Information

SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI). Only intelligence and information that clearly warrant extraordinary security measures will be restricted to SCI control.

When dealing with issues involving SCI security, refer to the following publications for policy and instructions:

- **Director, Central Intelligence Directive (DCID) 1/14, *Personnel Security Standards and Procedures Governing Eligibility fo Access to Sensitive Compartmented Information.***
- **DCID 1/16, *Security Manual for Uniform Protection of Intelligence Processed in AISs and Networks*.**
- **DCID 1/21, *Physical Security Standards for Sensitive Compartmented Information Facilities*.**
- **Defense Intelligence Agency Manual (DIAM) 50-4, *Department of Defense Intelligence Information Systems (DODIIS) Information Security (INFOSEC) Program.***
- **Department of Defense Directive (DODD) 5105.21-M-1, *Sensitive Compartmented Information (SCI) Security Manual, Administrative Security*.**
- **Department of the Navy Supplement (NAVSUP) to DODD 5105.21-M-1, *SCI Administrative Security Manual*.**

These documents provide policy and guidance on—

- **SCI personnel and information security clearance procedures.**
- **SCIF and TSCIF requirements.**
- **Classification levels.**
- **Compartmentation.**
- **Decompartmentation.**
- **Sanitization.**
- **Release to foreign governments.**
- **Emergency use.**
- **Security policy and procedures for the protection of information controlled in SCI compartments.**

Safeguarding SCI is critical. Security of SCI is important as it protects not only a piece of intelligence but also its source. For these reasons, dissemination and access to SCI information and materials are restricted. However, to be worthwhile, SCI must be accessible to commanders for use in decisionmaking. SCI must be classified only to the degree necessary in the interests of security. SCI security must be applied within the context of the mission, with security needs constantly assessed and balanced against operational mission needs.

SCI security is the responsibility of the commander, who exercises this responsibility through the unit G-2/S-2. The SSO serves as the primary staff officer for day-to-day SCI security administration and management. The commander must ensure SCI is accessed only by those persons with an appropriate clearance, access approval, identified need-to-know, and appropriate SCI indoctrination. This is accomplished by carefully managing those units and persons with SCI access and the equipment and facilities used to process, disseminate, and store SCI. (Appendix C, SIGINT and SCI Security Management Operations Flowchart, summarizes the principal SCI security planning considerations, activities, and products discussed in this chapter.)

8001. Special Security Officer

The SSO serves as the command's focal point for the receipt, control, and accountability of SCI materials and the supervision of the SCI security functions of subordinate SCIFs. The SSO will be a military commissioned officer, warrant officer, or civilian (GS-9 or above). The SSO—

- Supervises the operation of the special security office and administers the SCI security program. This includes oversight of other local SCIFs under the SSO's cognizance.
- Maintains required SCI directives, regulations, manuals, and guidelines to adequately discharge SSO duties and responsibilities.
- Ensures all SCI is properly accounted for, controlled, marked, transmitted, transported, packaged, and safeguarded. Ensures all SCI is destroyed in authorized destruction facilities and in accordance with current regulations.
- Ensures SCI is disseminated only to persons authorized access with an established need-to-know.
- Provides guidance and assistance for processing SCI access and eligibility requests.
- Serves as the official channel for passing SCI access certifications.
- Conducts or otherwise manages SCI personnel, information, physical, and technical security (i.e., TEMPEST, technical surveil lance countermeasures [TSCM]) actions and procedures according to current regulations.
- Conducts SCI security briefings, indoctrinations, and debriefings; administers and maintains signed nondisclosure agreements; and performs other related personnel security actions.
- Investigates SCI security infractions, makes recommendations, prepares required reports, and initiates and supervises any necessary corrective actions.
- Conducts a continuing training and awareness program to ensure that all SCI-indoctrinated individuals are apprised of new requirements and guidelines.
- Ensures that appropriate accreditation documentation is available for each SCIF, TSCIF, and SCI system under the SSO's cognizance.

8002. Personnel Security Program

The protection of SCI is directly related to the effectiveness of the personnel security program. DCID 1/14 establishes the personnel security standards for the United States intelligence community. A mutually supporting series of program elements (e.g., need-to-know, investigation, binding contractual obligations on those granted access, security education and awareness, and individual responsibility) provides reasonable assurances against compromise of SCI by those authorized access to it.

a. Access Approval Authority

In accordance with DCID 1/14, the Director o Naval Intelligence is authorized to grant, deny, or revoke SCI access to Marines and Sailors. This responsibility is carried out through the Department of the Navy Central Adjudication Facility (DONCAF).

b. Requirements for SCI Access

DONCAF may grant an individual SCI access when the following requirements have been met.

(1) Need-to-Know is Determined. Even when approved for a specific access, the holder is expected to acquire or disseminate only that SCI essential to effectively carry out an assignment No person will have a need-to-know solely by virtue of rank, title, or position.

(2) Eligibility is Determined. DCID 1/14 provides eligibility standards for investigation and evaluation for an individual's access to SCI. A

single-scope background investigation (SSBI) conducted within the last 5 years serves as the basis for determining access approval.

(3) SCI Billet is Identified. DCI does not require the Navy to maintain an SCI billet structure. However, SSO Navy and CNSG have decided to retain the current SCI billet numbering system for accountability within the DON. SCI billets are administered by the local command SSO and reported annually to SSO Navy or CNSG as appropriate.

(4) Security Indoctrination is Completed SCI indoctrination is the instruction an individual receives prior to receiving access to an SCI systems, programs, and materials. The instruction convey the unique nature, sensitivity, and special security safeguards and practices for SCI handling, particularly the necessity to protect sensitive sources and methods.

(5) Nondisclosure Agreement is Signed. As a condition of access to SCI, individuals authorized SCI access must sign a DCI-authorized nondisclosure agreement (NDA). The NDA establishes explicit obligations on both the Government and the individual for the protection of SCI. An NDA is binding for life and cannot be revoked or waived. Failure to sign an NDA is cause for denial of SCI access.

8003. Physical Security

All SCI must be processed, used, and stored within an accredited SCIF. Accreditation is granted when the proposed facility meets the physical security standards stipulated in DCID 1/21. The SSO, DIA, is the accrediting authority for all DOD SCIFs, while NSA is the accreditation authority for all service cryptologic element SCIFs. Organizations are responsible for ensuring that SCIFs are established only when operationally required and when existing SCIFs are not adequate to support the unit's mission.

a. Sensitive Compartmented Information Facility

A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed. Access to SCIFs will be controlled to preclude entry by unauthorized personnel. Non SCI-indoctrinated personnel entering a SCIF must be continuously escorted by an indoctrinated individual who is familiar with the security procedures of that SCIF. The physical security protection for a SCIF is intended to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons.

b. Emergency Action Plans

Each accredited SCIF will establish an emergency action plan. This plan will be approved by the appropriate G-2/S-2 or SSO. The essential concern of the plan must be safety of personnel over a other factors. The plan will address—

- Physical protection of personnel working in the SCIF.
- Adequacy of fire fighting equipment and life-support equipment (e.g., oxygen and masks).
- Entrance of emergency personnel (e.g. police, medical technicians, and firemen) into a SCIF.
- Evacuation plans for persons.
- Emergency destruction and transfer procedures of classified material and equipmen in the event of—
  - Fire.
  - Loss of essential utilities.
  - Sabotage.
  - Riots.
  - Civil disorders.
  - Hostile or terrorist attack or capture.
  - Natural disasters.

c. Tactical Sensitive Compartmented Information Facility

Recognizing the need for SCIFs to support tactical operations, the DCI requires the following minimum physical security standards for a TSCIF. If the situation and time permit, these minimum standards will be improved on by using the security considerations and requirements for permanent secure facilities. (Appendix E, TSCIF Checklist, is provided as a guide when activating or deactivating a TSCIF.)

- Locate the TSCIF within the supported headquarter's defensive perimeter, preferably within its main command echelon.
- Use permanent-type facilities, if available.
- Maintain 24-hour operation under field or combat conditions.
- Establish a physical barrier around the TSCIF. Where practical, the physical barrier should be triple-strand concertina o general-purpose barbed-tape obstacle. The TSCIF approval authority determines whether proposed security measures provide adequate protection based on local threat conditions.
- Guard the TSCIF perimeter by stationing walking or fixed guards to observe the controlled area. Guards will be armed with weapons and ammunition in accordance with Marine Corps Order (MCO) 5500.6F, *Arming of Security and Law Enforcemen (LE) Personnel and the Use of Force*.
- Restrict access to the controlled area with a single gate or entrance that is guarded continuously.
- Maintain an access list. Only those people whose names appear on the list will be allowed access to the TSCIF.
- Staff the TSCIF with sufficient personnel as determined by the on-site SSO or G-2/S-2 based on the local threat conditions.
- Keep emergency destruction and evacuation plans current.
- Store SCI material in lockable containers when not in use.
- Establish and maintain communications with local security or emergency reaction forces, if possible.
- Conduct an inspection of the vacated TSCIF area. The SSO or G-2/S-2 ensures SCI materials are not inadvertently left behind when the TSCIF displaces.
- Coordinate planning with the unit's headquarters commandant, who is responsible for providing TSCIF guard personnel, communication with command post guard forces, emergency personnel reaction forces, and internal reaction forces.

d. Mobile Tactical Sensitive Compartmented Information Facility

Mobile TSCIF requirements are as follows:

- Maintain a 24-hour operation and staff the TSCIF with sufficient personnel as determined by the on-site SSO or G-2/S-2 based on the local threat conditions.
- Incorporate external physical security measures into the perimeter defense plans for the immediate area in which the mobile TSCIF is located. (A physical barrier is not required as a prerequisite to establish a mobile TSCIF.)
- Use Marines performing the day-to-day operations of the TSCIF to control external physical security.
- Establish and maintain communication with backup guard forces, if possible.
- Incorporate incendiary methods in emergency destruction plans to ensure total destruction of SCI material during emergency situations.
- Adhere to the following restrictions when using a rigid-sided shelter or portable van.
  - Mount the shelter to a vehicle so that the shelter can move on short notice.
  - Affix a General Services Administration (GSA)-approved security container permanently within the shelter. Protect the lock combination to the level of security of the material stored therein.

- Control the entrance to the mobile TSCIF with SCI-indoctrinated Marines on duty within the shelter.
- Limit entrance to the mobile TSCIF to SCI-indoctrinated personnel.
- Store classified material within the locked GSA container and secure the shelter' exterior entrance during redeployment.

- Adhere to the following restrictions when using a mobile TSCIF for a soft-sided vehicle or man-portable system.
  - Protect SCI material in an opaque container (i.e., leather pouch, metal storage box, or other suitable container that prevents unauthorized viewing).
  - Keep this container in the physical possession of an SCI-indoctrinated person.

- Limit the quantity of SCI material permitted within the mobile TSCIF to that which is absolutely essential to sustain the mission. Employ stringent security arrangements to ensure that the quantity of SCI material is not allowed to accumulate more than is absolutely necessary.

e. Tactical Sensitive Compartmented Information Facility Accreditation

The accreditation process consists of three steps, each requiring a message to be sent to the cognizant approval authority (see NAVSUP to DODD 5105.21-M-1). Approval authorities vary with respect to information and formats required. When requesting TSCIF authorization and accreditation, use the current reference from the cognizant authority. The following reports and messages are prepared by the unit SSO or G-2/S-2.

(1) Concept of Operations. A message that outlines the who, what, when, where, and why for the TSCIF and identifies supporting security, administrative, and point of contact information.

(2) TSCIF Activation Report. A report sent to the approval authority upon commencement o TSCIF operations.

(3) TSCIF Deactivation Report. A report sent to the approval authority when the TSCIF has ceased operations and has been certified to be free of SCI material.

8004. Information Systems Security

All SCIF intelligence and information systems used for processing, storing, and conveying intelligence and/or SIGINT information must be accredited prior to operating. The DON approving authority for SCIF intelligence systems is the Office of Naval Intelligence (ONI-54) in accordance with DIAM 50-4. The cognizant DON approving authority for SCIF resident cryptologic systems is CNSG (N1).

The SSO is responsible to the G-2/S-2 for overall management and administration of the unit's SCI security program and for SCIF security. The unit's information system security manager (ISSM) and the information system security officer (ISSO) complement the SSO and are accountable for the SCIF-resident information systems The ISSM or ISSO will help ensure new and changed information systems meet all security requirements. These individuals coordinate the approval of new or changed systems with the appropriate DON approving authority. Normally, the ISSM and ISSO are the principal interface between the approving authority and the local command.

Chapter 9

Training

The policies, standards, and procedures for the conduct of SIGINT training as well as the assignment of responsibilities to ensure adequate and responsive training are spelled out in DODD 5210.70, *DOD Cryptologic Training.* Additionally, MCO 1510.50A, *Individual Training Standards (ITS) System for the Signals Intelligence Ground Electronic Warfare Occupational Field (OccFld)*, provides a detailed description (by rank and MOS) of tasks SIGINT Marines must be capable of performing.

9001. Military Occupational Speciality Training

Training for the SIGINT Marine focuses on building, maintaining, and enhancing the technical skills required to be MOS proficient.

a. Entry-Level Training

The foundation for all SIGINT Marine training is the entry-level training. Due to its highly technical nature, this OccFld possesses some of the longest MOS entry-level training pipelines. The following paragraphs briefly describe these pipelines.

(1) 0206 Basic SIGINT. Following The Basic School, all SIGINT-designated lieutenants are sent to the Cryptologic Division Officers Course (CDOC), Corry Field, Pensacola, Florida. Following CDOC, all 0206 lieutenants are ordered to one of the two RadBns to develop and enhance their SIGINT skills.

(2) 7588 Electronic Warfare Officer. The initial, formal EW training for air EW lieutenants is the Joint Electronic Warfare School, Pensacola Florida. The course focuses on basic radar theory, friendly and threat integrated air defense system (IADS), naval forces organization and capabilities, and the application of EW.

Following the Joint Electronic Warfare School, 7588 lieutenants receive specialized training with the Fleet Replacement Squadron (VAQ-129), Whidbey Island, Washington. This 9-month course provides instruction and training on the EA-6B aircraft operations and systems and on threat IADS aircraft and shipping. Additionally all 7588 electronic warfare officers obtain Naval Air Training and Operating Procedures Standardization (NATOPS) program qualification in the EA-6B.

(3) 2621 Manual Morse Intercept Operator. Manual Morse training begins with Morse code training at Ft. Huachuca, Arizona. Upon graduation, the new manual Morse intercept operator reports to Corry Field, Pensacola, Florida, for the Communication Signals Collection and Processing (450) Course.

(4) 2631 ELINT Intercept Operator or Analyst. Basic ELINT training is provided by the Cryptologic Technician Course, Corry Field, Pensacola, Florida. Marines assigned to the VMAQ TERPES section also attend the TERPES Operator Course, Navy and Marine Corps Intelligence Training Center, Dam Neck, Virginia.

(5) 2651 Special Intelligence Communicator. Training in SI communications, data communications, networks, and system security is provided in the Cryptologic Technician "O" Course, Corry Field, Pensacola, Florida.

(6) 267X Cryptologic Linguist. The cryptologic linguist has the longest initial training track of any ground MOS. Training begins with basic language training at the Defense Language Institute (DLI), Monterey, California, for a period of 47 to 63 weeks, depending on the language and

student's ability. Following graduation from DLI, the basic linguist will report to Goodfellow AFB, Texas, for cryptologic linguist specialist training.

(7) 2629 SIGINT Analyst. Upon completion of their initial tour, many 2621's, and some 2631's, and 267X's will attend the Fleet Analysis and Reporting Course, Goodfellow AFB, Texas, for additional training to qualify for MOS 2629, SIGINT analyst.

b. SIGINT Skill Progression Training

SIGINT Marines have a wealth of resident and nonresident training opportunities to refine, maintain, or enhance their skills. These programs are announced by HQMC and include—

- NSA Director's Fellowship Program for field grade officers.
- Junior Officer Cryptologic Career Program for company grade officers.
- Middle Enlisted Cryptologic Career Advancement Program for SNCOs.
- Military Intern SIGINT Analyst Program for SNCOs and NCOs.
- Military ELINT Signals Analyst Program for SNCOs and NCOs.
- Marine Corps Cryptologic Computer Administration Program for enlisted Marines.
- Various military linguist programs.

9002. Functional Training

Functional SIGINT training focuses on ensuring Marines in all elements of the MAGTF are aware of SIGINT contributions and the corresponding SIGINT or EW threat from our adversaries.

a. SIGINT Marines

Functional training educates SIGINT Marines on all-source intelligence operations within the MAGTF, naval forces, and JTFs. SIGINT Marines participate in exercises to learn operational intelligence requirements; the interaction between commanders and staffs and MAGTF units and intelligence sections; and the capabilities, limitations, and operational support methodologies within MAGTF and other units. During exercises, SIGINT Marines interact with the G-3/S-3 and G-6/S-6 to refine coordination requirements and improve intelligence flow during actual operations.

b. SIGINT Training of Non-SIGINT Marines

Non-SIGINT Marines are trained in the capabilities and limitations of Marine, Navy, JTF, theater, and national SIGINT systems that support MAGTF operations. Equal time should be spen training these Marines on the capabilities and limitations of the adversary's SIGINT or EW systems and on individual and force protection tactics and techniques. To improve mutual understanding and eliminate misconceptions, the unique security restrictions required when dealing with SIGINT information should also be explained to and practiced by non-SIGINT Marines.

9003. Exercises

SIGINT operations in exercises are closely controlled. The same security precautions and controls are required for both the real world and exercises. USSID 56, *Exercise SIGINT*, provides guidance on obtaining and using SIGINT during exercises.

Exercise SIGINT provides commanders, staffs and units with experience in SIGINT operations, information, rules, communications, and personnel. Exercise SIGINT operations may be conducted with or without an opposition force. Care should be taken during exercises to present a realistic picture of what SIGINT systems can provide to avoid creating false expectations.

If an opposition force does not participate, exercise SIGINT may be scripted or preplanned (e.g., staff exercise [STAFFEX] or a command post exercise [CPX]). Use of scripted SIGINT in an exercise must be requested and approved by the appropriate agency well in advance of the exercise. This will allow time to script the exercise

SIGINT necessary to realistically support the scenario. Exercise planners and exercise SIGINT scripters must coordinate to ensure the SIGIN information flow is realistic. All security requirements must be maintained throughout the exercise (e.g., TSCIF activation and SCI-handling procedures).

Exercise SIGINT operations may be conducted against an opposition force (e.g., during a MAGTF field exercise). This provides more realistic training for the SIGINT element and SIGINT users. Depending on the level of the exercise, the use of simulators and national systems may be requested to add realism and enhance training These assets must be requested well in advance of the exercise and approved by the appropriate agency described in the J-TENS manual.

9004. Operational Training Objectives

The major objective for SIGINT operations training is exercising SIGINT operations in a realistic tactical environment with all elements of the MAGTF.

a. SIGINT Organizations

RadBns and VMAQs should—

- Train unit leaders, planners, and supervisory personnel to—
  - Plan and direct, process and exploit, produce, disseminate, and use unique SIGINT and integrated all-source intelligence.
  - Plan and integrate SIGINT operations with multifunctional staff operations.
  - Conduct SIGINT operations.
- Train SIGINT operators in SIGINT—
  - Operations.
  - Systems.
  - Equipment.
  - TTP.
  - Supporting operations (i.e., CIS, logistics, and intelligence).

b. G-2/S-2 and Intelligence Personnel

Intelligence personnel must be able to—

- Understand the capabilities and limitations of SIGINT collection operations and the planning, integration, coordination, and execution of SIGINT collection with multidiscipline intelligence and reconnaissance collection operations.
- Understand the capabilities and limitations of SIGINT production operations and the planning, integration, coordination, and execution of SIGINT production with all-source intelligence production operations.
- Understand the capabilities and limitations of SIGINT dissemination operations (e.g. planning, integration, coordination, and execution of routine and time-sensitive SIGINT dissemination) and the requirements, establishment, and integration of unique SIGINT and multiuse CIS architectures.

c. G-3/S-3 and Maneuver and Fires Personnel

Operations, maneuver, and fires personnel should be able to—

- Plan, coordinate, and conduct effective MAGTF SIGINT, EW, and CIS operations.
- Plan, coordinate, and conduct insertion and extraction methods.
- Site and coordinate SIGINT collection and DF teams with supporting SIGINT elements, G-2/S-2, and subordinate commanders.
- Coordinate SIGINT operations with MAGTF and subordinate units' future and current operations centers and fire support coordination centers.
- Disseminate and use SIGINT and other SCI information.

d. G-4/S-4 and Combat Service Support Personnel

Logistics and CSS personnel should understand SIGINT units' unique CSS requirements (particularly electronic maintenance and unique consumables such as batteries).

e. G-6/S-6 and Communications and Information Systems Personnel

CIS personnel must be able to plan, coordinate and integrate SIGINT CIS requirements within MAGTF and supporting CIS plans and operations.

f. Headquarters Commandant

Headquarters commandant personnel must be able to understand, plan, and provide for the SIGINT units' security requirements (particularly those associated with TSCIFs and mobile SIGINT SCIFs).

Appendix A

Radio Battalion SIGINT Support Unit Checklist

The following checklist is provided as a guide to assist the radio battalion (RadBn) SIGINT support unit (SSU) officer in charge (OIC) conduc operations. Depending on the mission, location and duration of an operation, some items may not be applicable.

Planning Stage

- ❑ **Coordinate with the RadBn S-3 to—**
  - ❍ **Determine exact mission and tasking of the detachment and the authority and command relationship.**
  - ❍ **Review all messages related to deployment and composition of the detachment.**
  - ❍ **Ensure S-3 tasks companies or sections to provide required personnel to fill detachment table of organization (T/O) line numbers.**
  - ❍ **Request assignment of RadBn SIGINT address and producer designator digraph, if necessary.**
  - ❍ **Verify formats and instructions for required reports.**
  - ❍ **Determine if area clearances and clearance certifications are necessary and request special security officer (SSO) take appropriate action.**
  - ❍ **Review pertinent orders and instructions of the supported unit.**
  - ❍ **Identify and arrange for special training and operational requirements.**
- ❑ **Coordinate with the following supported command—**
  - ❍ **G-2/S-2 intelligence operations officer to determine initial intelligence collection, production, and dissemination requirements and current intelligence estimate.**
  - ❍ **G-2/S-2 intelligence operations officer to determine time constraints for submission of input to appendix 2 to annex B of the operations order.**
  - ❍ **G-2/S-2 all-source fusion center OIC to determine plans and integration of intelligence and SIGINT production activities.**
  - ❍ **G-2/S-2 dissemination officer for a list of SIGINT products recipients, appropriate report formats, and routine and time-sensitive communications and information systems (CIS) plans.**
  - ❍ **G-2/S-2 intelligence operations officer and G-4/S-4 for supply and logistics requirements to be provided by supported command (e.g., electronic maintenance and consumables such as batteries; meals, ready to eat; maps; and fuel).**
  - ❍ **G-3/S-3 electronic warfare officer for electronic attack (EA) requirements and capabilities and input to appendix 3 to annex C of the operations order.**
  - ❍ **G-2/S-2 operations officer and G-6/S-6 to address requirements for communications support (e.g., secure and unclassified local area network [LAN] access, equipment).**
  - ❍ **G-3/S-3 to establish liaison teams with supported unit's subordinate elements if necessary.**
  - ❍ **Command security manager, G-2/S-2, and G-3/S-3 for force protection and communications security monitoring requirements and plans.**
- ❑ **Develop and publish a training schedule in coordination with the RadBn S-3 and supported unit's intelligence officer.**

- ❑ Request courier cards from RadBn SSO for appropriate detachment personnel.
- ❑ Coordinate collection and analytical and production requirements with the operations control and analysis (OCA) element to—
  - ○ Ensure the detachment analytical and production team knows the technical aspects of the operations area.
  - ○ Ensure the analytical and production team has a current technical support package; request an update if required (i.e., hardcopy, electronic copy).
  - ○ Ensure SIGINT position designators for equipment are current; prepare and issue required SIGINT resource status report (RSR).
  - ○ Ensure the National Security Agency (NSA) or the pertinent regional security operations center or cryptologic shore support activity provides a current technical briefing on targets in the area of operations.
- ❑ Coordinate transportation requirements with RadBn S-3, S-4, and supported unit.
- ❑ Coordinate embarkation requirements with RadBn S-4 and supported unit to—
  - ○ Review current embarkation orders.
  - ○ Complete embarkation forms (e.g., Tactical Cargo Manifest Declaration, 1387-2, 1348-1).
  - ○ Review current inbound and outbound agricultural restrictions on vehicles.
  - ○ Assemble complete embarkation kit with guidelines for use upon departure.
  - ○ Request table of equipment (T/E) items for detachment.
- ❑ Coordinate communications and information requirements with RadBn S-6 and supported unit intelligence officer and CIS officer to—
  - ○ Determine circuit request requirement.
  - ○ Determine telecommunications service request (TSR) requirement.
  - ○ Determine frequency and call sign requirements and request communications-electronics operating instructions.
  - ○ Request special intelligence (SI) routing indicator and plain language address assignments.
  - ○ Determine communications security materials system (CMS) requirements and request that the CMS custodian have material available for issue.
  - ○ Designate an SSO CMS custodian.
  - ○ Determine TEMPEST inspections and automated information systems accreditation requirements.
  - ○ Determine cryptographic hardware and keying material requirements and procedures with all communication elements.
- ❑ Ensure all personnel are qualified with T/O weapons and arrange for battlesight zero (BZO) firing as necessary.

Predeployment Stage

- ❑ Audit health records to—
  - ○ Determine inoculations required and arrange for required shots with the corpsman.
  - ○ Determine if detachment members or members of their families are undergoing extensive outpatient care, with an indefinite prognosis.
  - ○ Confirm and record blood types.
  - ○ Ensure all personnel requiring eyeglasses have two pair. Also ensure they have optical inserts for gas masks.
  - ○ Ensure detachment members meet class I or II dental readiness.
  - ○ Arrange for block pickup of health and dental records.

- ❑ Coordinate legal affairs to—
  - ○ Inform personnel of advisability of wills and procedures for obtaining them.
  - ○ Inform personnel of powers of attorney and procedures for obtaining them.
- ❑ Arrange for storage of privately owned vehicles and personal effects.
- ❑ Arrange for mail handling.
- ❑ Coordinate pay matters to—
  - ○ Conduct personal financial record audit.
  - ○ Prepare savings and other allotments.
- ❑ Coordinate administrative matters to—
  - ○ Verify accuracy of record of emergency data.
  - ○ Ensure identification cards are current and have proper Geneva Convention category information.
  - ○ Ensure personnel have current identification (ID) tags.
  - ○ Audit and update officer qualification records and enlisted service record books.
  - ○ Complete change of reporting senior fitness reports, fitness report roughs, and proficiency and conduct marks.
- ❑ Coordinate clothing inspection and requirements to—
  - ○ Ensure personnel have appropriate serviceable uniforms for all destinations.
  - ○ Ensure personnel have appropriate civilian attire in accordance with local military customs of country(ies) to be visited.
  - ○ Ensure temporary issue requirements draw includes the proper sizes and is coordinated through the RadBn S-4 and supported unit.
- ❑ Ensure baggage is appropriate and of sturdy construction.
- ❑ Ensure personnel know customs requirements of locations to be visited.
- ❑ Prepare government transportation request.
- ❑ Prepare military transportation authorization.
- ❑ Conduct the following:
  - ○ Family services deployment briefing for all SSU and family members.
  - ○ Red Cross brief.
  - ○ Navy and Marine Corps Relief brief (to include preauthorized emergency loan applications).
  - ○ Religious services brief.
  - ○ Family services brief.
  - ○ Key spouses brief.
- ❑ Assemble assigned T/E equipment required for deployment to—
  - ○ Perform operational check of equipment.
  - ○ Complete limited technical inspection (LTI) on all equipment.
  - ○ Perform acceptance inspections on all temp-loan equipment.
  - ○ Check the date of last calibration, if applicable.
- ❑ Arrange for draw or transfer of CMS material.
- ❑ Receive CMS custodial briefing from CMS custodian.
- ❑ Receive security requirements and emergency destruction briefing from SSO.
- ❑ Conduct training in accordance with established detachment training schedule.
- ❑ Coordinate with the RadBn SSO and classified materials control officer to—
  - ○ Designate a detachment classified material secondary control point and custodian.

- ○ Ensure required single-scope background investigation periodic reviews are initiated on those detachment personnel identified as needing updates.
- ○ Request sensitive compartmented information (SCI) clearance certification on all detachment personnel be forwarded to cognizant units and other organizations as necessary.

❑ Coordinate with the RadBn adjutant or S-1 to—

- ○ Draw record books.
- ○ Pick up orders.
- ○ Establish report criteria.
- ○ Arrange for administrative and legal briefs.
- ○ Arrange for detachment Uniform Code of Military Justice and code of conduct briefings.

❑ Coordinate with RadBn SSO to—

- ○ Confirm security requirements.
- ○ Pick up courier cards for specified personnel.
- ○ Receive area intelligence briefs to include customs, politics, religion, and standards of personal conduct.
- ○ Receive counterintelligence area threat briefs.
- ○ Ensure all required personnel receive appropriate special access indoctrination(s).
- ○ Transfer necessary technical material from SSO and OCA classified material control center accounts.

❑ Coordinate with RadBn S-3 to—

- ○ Establish SIGINT operations report criteria.
- ○ Determine topographic and map requirements and request allowance from OCA or the supported unit.
- ○ Request preparation of appropriate cryptologic technical kits from NSA or the supporting cryptologic shore support activity.

❑ Coordinate with RadBn S-4 supply to establish fiscal account job order numbers and sign the consolidated memorandum receipt.

❑ Coordinate with RadBn S-4 electronic maintenance to—

- ○ Establish equipment maintenance procedures.
- ○ Establish electronic maintenance support and prepare pre-expend bin support block.
- ○ Ensure that all equipment receives a predeployment LTI.
- ○ Ensure skeleton record jackets are prepared for all equipment.

❑ Coordinate with RadBn S-4 motor transport and engineer to—

- ○ Establish equipment maintenance procedures.
- ○ Establish motor transport and engineer support.
- ○ Ensure skeleton record jackets are prepared for all vehicles.

❑ Coordinate with RadBn S-4 ordnance officer to—

- ○ Determine weapon requirements and other ordnance needs.
- ○ Obtain proper storage boxes for the transport of weapons.
- ○ Draw weapons.
- ○ Conduct necessary inspections.
- ○ Conduct daily sight counts.

- ○ Determine ammunition and pyrotechnic training requirements during deployment.

- ❑ Coordinate with RadBn S-4 embarkation officer to—
  - ○ Receive embarkation package.
  - ○ Determine dunnage requirements.
- ❑ Draw equipment and sign for gear assigned to detachment.
- ❑ Receive medical brief from battalion medical personnel.
- ❑ Contact special services officer for recreation items.
- ❑ Publish the final—
  - ○ Detachment T/O and T/E.
  - ○ Roster of personnel.
  - ○ Dependent point-of-contact roster.
  - ○ Equipment and uniforms required.
  - ○ Detachment training schedule.
  - ○ Detachment operations order.
- ❑ Palletize or combat load supplies and equipment.
- ❑ Coordinate embarkation of personnel and equipment with S-4 of supported unit.
- ❑ Stage for embarkation.

Deployment

- ❑ Coordinate with G-2/3 and S-2/3 for initial location of combat operations center, combat intelligence center, and collection direction finding (DF) and EA teams.
- ❑ Continue coordination of collection and DF team and radio reconnaissance team locations with G-2/S-2 collections officer and G-3/S-3. Include updates for inserts, extract times, and methods.
- ❑ Coordinate with G-2/S-2 intelligence operations officer for inputs and presentation for intelligence estimate, concept of operations, and intelligence operations plans briefings.
- ❑ Submit the following required reports and messages:
  - ○ Activation report and deactivation report to RadBn S-3 and supported unit G-2/S-2.
  - ○ Circuit activation report to RadBn S-6 and supported unit G-6/S-6.
  - ○ Administrative reports to RadBn S-1.
  - ○ CMS destruction reports to SSO or CMS.
  - ○ Circuit deactivation report to RadBn S-6 and supported unit G-6/S-6.
  - ○ Transportation request to RadBn and supported unit G-4/S-4.
  - ○ Required analysis and technical reports to OCA and supported unit G-2/S-2. (RSR to NSA upon activation and deactivation.)
  - ○ Tactical SCI facility activation and deactivation reports to Commander, Naval Security Group, supported unit SSO, and others as appropriate.
- ❑ Prepare and distribute required reports to the supported commander.
- ❑ Send deactivation message.

Postdeployment

- ❑ Turn in weapons and classified material immediately upon return.
- ❑ Participate in supported unit operations debriefings as required. Debrief with RadBn commanding officer and S-3 on the first working day after return.
- ❑ Coordinate with RadBn adjutant, S-1, S-3, and S-4 to—
  - ○ Return record books to S-1.
  - ○ Return medical and dental records.

- ❍ Terminate temporary additional duty (TAD) orders.
- ❍ Prepare and submit performance evaluation reports and proficiency and conduct marks as required for the TAD period.
- ❍ Notify mail clerk to stop forwarding mail.
- ❍ Return technical material to the OCA platoon.

❑ Return CMS material to CMS custodian within 48 hours of return.

❑ Return courier cards to SSO.

❑ Prepare equipment for postdeployment LTI.

❑ Ensure proper maintenance is conducted on equipment prior to returning to respective companies or sections.

❑ Turn in equipment on equipment repair orders and note any equipment damage or problems.

❑ Settle fiscal account.

❑ Submit an after action report within 20 days of return (or as directed) to the supported unit G-2/S-2, G-3/S-3, and RadBn S-3.

❑ Disband detachment.

❑ Prepare award recommendations on deserving personnel.

❑ Recommend necessary changes to unit SOPs and coordinate with the RadBn and supported unit staff.

Appendix B

Marine Corps SIGINT Equipment

Radio battalions (RadBns) and Marine tactical electronic warfare squadrons (VMAQs) use unique specialized equipment for the search, detection, identification, processing and exploitation of enemy signals of interest (SOIs), and the subsequent production and dissemination of SIGINT products. The following sections describe the primary SIGINT equipment in the inventory of the RadBns and VMAQs.

Section I. Radio Battalion SIGINT Equipment

AN/ULQ-19(V)2 Electronic Attack Set

The AN/ULQ-19(V)2 electronic attack (EA) set (figure B-1) provides the capability to conduct spot or sweep jamming of single-channel, encrypted or unencrypted, voice or data signals operating in the standard military frequency range of 20-79.975 MHz from selected mobile platforms (e.g., high mobility, multipurpose wheeled vehicles [HMMWVs], mobile electronic warfare support system [MEWSS], helicopters). In addition, it can provide up to four channels of high-power VHF voice and/or data communications when not being used as a jamming system. When employed as a tactical, general-purpose, low-VHF jamming system, it has a 250-watt radio frequency linear amplifier that produces a nominal 200 watts of effective radiated power (ERP) using a standard omnidirectional whip antenna. To provide required jamming, the system must be employed and operated from a location with an unobstructed signal line of sight to the target enemy's communications transceiver.

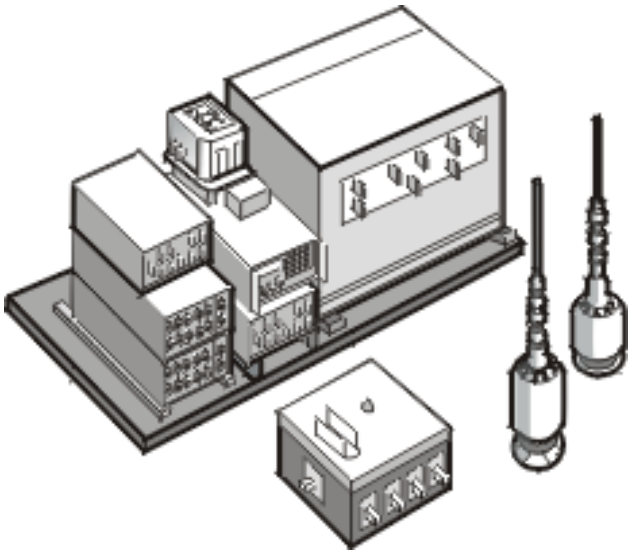


Figure B-1. AN/ULQ-19(V)2.

AN/MLQ-36 Mobile Electronic Warfare Support System

The AN/MLQ-36 MEWSS provides a multifunctional capability that gives SIGINT electronic warfare (EW) operators limited armor protection (figure B-2). This equipment is ideally suited to provide SIGINT EW support for highly mobile mechanized and military operations in urban terrain where maneuver and/or armor protection is critical. MEWSS comprises a signals intercept system, a radio direction finding (DF) system, an EA system, a secure communications system, and an intercom system installed in a logistics variant of the light armored vehicle (LAV)-25. Electronic warfare support (ES) activities are accomplished through the use of two WJ-8618B(S1) acquisition receivers and the WJ-32850 MANTIS DF system. EA activities are conducted with the AN/ULQ-l9(V) electronic attack set.

Figure B-2. AN/MLQ-36.

AN/MLQ-36A Mobile Electronic Warfare Support System Product Improvement Program

The mobile electronic warfare support system product improvement program (MEWSS-PIP) is an advanced SIGINT/EW system integrated into an LAV (figure B-3). The MEWSS-PIP provides a total replacement of the EW mission equipment now fielded in the AN/MLQ-36 MEWSS. It provides the ground commander with a mobile SIGINT/EW system capable of operating in a variety of tactical situations. The primary mission of the MEWSS-PIP is to provide intercept, collection, automated DF, and EA against threat modern communications and noncommunications emitters across a broad frequency range. It is a multiservice, open-systems architecture developed by the Marine Corps and the Army that incorporates elements of the Army's intelligence and electronic warfare common sensor (IEWCS) system. This system enhances interoperability through cooperative engagement, data sharing, and precision location. Initial operational capability is scheduled for fourth quarter, fiscal year 1999.

Figure B-3. AN/MLQ-36A.

AN/PRD-12 Direction Finder Set

The AN/PRD-12 is a tactical, man-transportable system that provides search, intercept, and DF on communications signals in the HF/VHF/UHF bands (figure B-4). Up to four PRD-12 stations can be networked, providing DF data to a mission control station via radio link with single-channel ground and airborne radio system (SINCGARS) equipment. Each station has the ability to function as the net control station. When stations are networked, they provide target emitter position data to mission control via voice link. A complete station can be relocated rapidly, optimizing its use in forward areas with combat units.

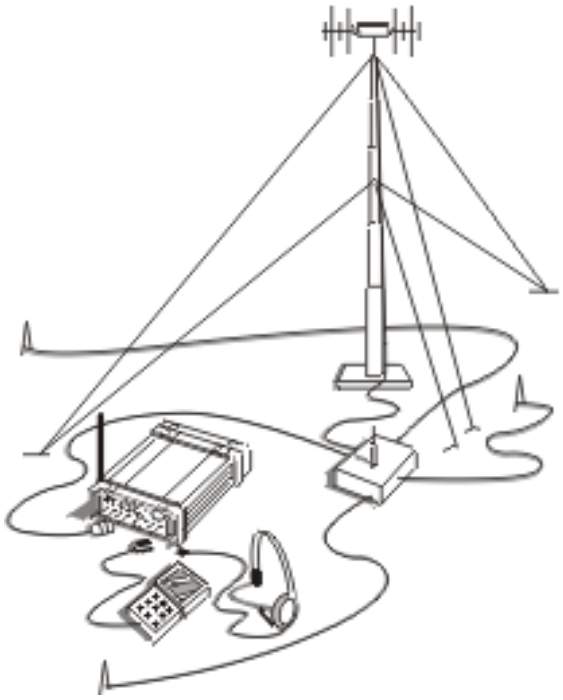


Figure B-4. AN/PRD-12.

AN/MSC-63A Communications Central

The AN/MSC-63A is a shelterized communications switch that provides a secure semiautomated data communications switch and terminals for the processing of general service (GENSER) or defense special security communications system (DSSCS) sensitive compartmented information (SCI) record message traffic. See figure B-5. There is one AN/MSC-63A with each Marine division and Marine aircraft wing special security communications team, and three AN/MSC-63A's with each RadBn. The system consists of three functional subsystems: shelter and auxiliary support subsystem, the communications subsystem, and the data processing subsystem. See figure B-6. The AN/MSC-63A is fully compatible with the Army's AN/TYC-39.

Figure B-5. AN/MSC-63A.

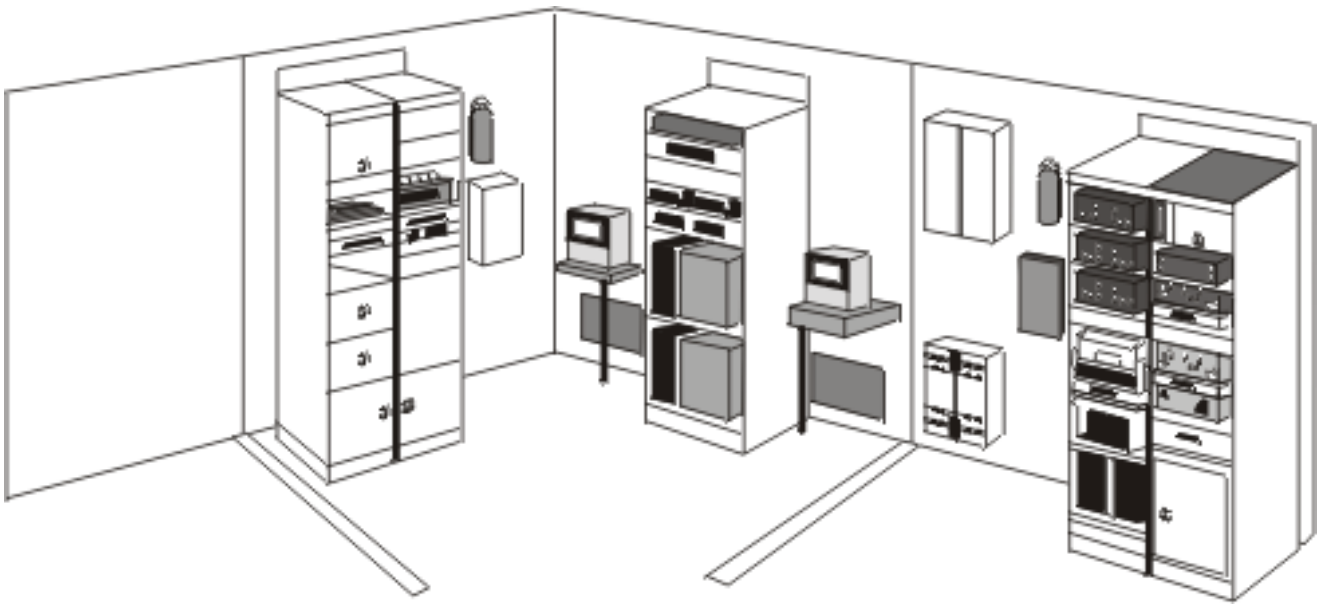


Figure B-6. AN/MSC-63A (interior view).

AN/TSQ-130(V)2/(V)5 Technical Control and Analysis Center

The AN/TSQ-130(V)2/(V)5 technical control and analysis center (TCAC) is an all-weather, tactical, transportable, SIGINT-processing, analysis and reporting system installed in a large, self-contained, modified S-280G shelter. TCAC is the primary system used by the RadBn SIGINT support unit. It is capable of performing semiautomated-SIGINT collection management, data base maintenance, analysis, technical and tactical reporting, and SIGINT technical control of forward deployed RadBn elements or teams. The (V)2 is the baseline system, while the (V)5 has upgraded communications capabilities. See figure B-7 for a notional TCAC concept of employment.

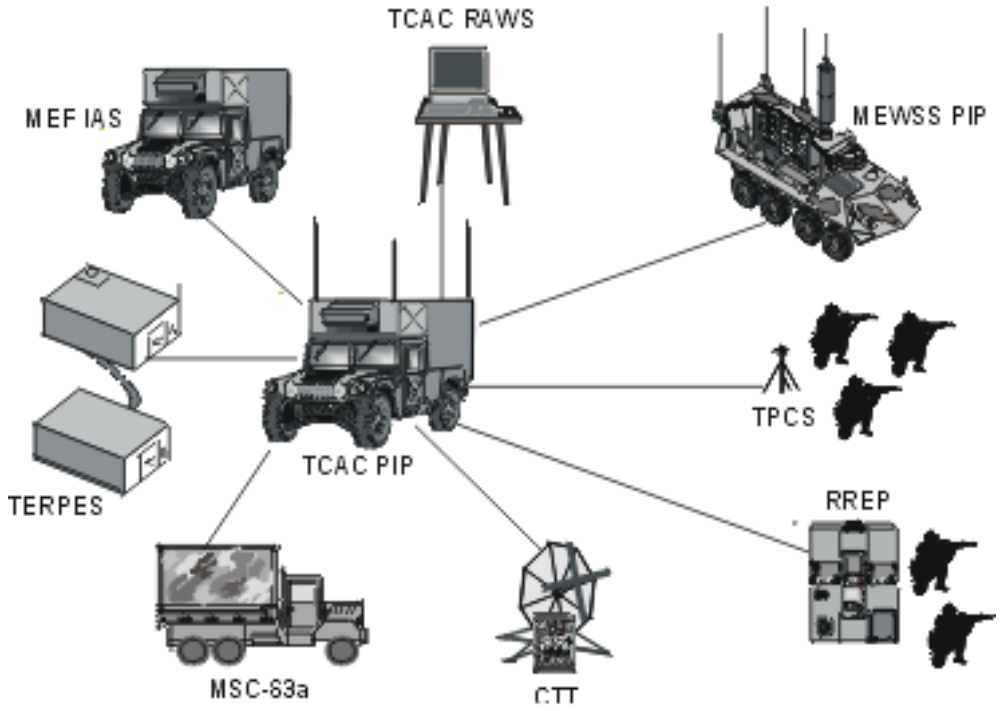


Figure B-7. Technical Control and Analysis Center Concept of Employment.

AN/MYQ-8 TCAC-PIP

The AN/MYQ-8 TCAC-PIP will replace the TCAC. It will consist of three remoteable analysis workstations (RAWSs), one communications interface module (CIM), and one supervisor control module (SCM). Each workstation will consist of modularly designed component equipment fully integrated to perform their intended functions.

Remoteable Analysis Workstation

RAWS provides the capability to perform necessary analysis and reporting functions at a central location or a more forward deployed site, remoted from the TCAC shelter. During shelter operations, a RAWS will be electrically interconnected to the other terminals in the shelter. During remote operations, a RAWS will be connected to the shelter via local area network (LAN) or radio link. It could operate in a stand-alone mode.

Communications Interface Module

CIM provides man-machine interface to communication subroutines that support the interface between the TCAC PIP and other RadBn systems (e.g., team portable collection system, mobile electronic warfare support system) or external intelligence agencies.

Supervisor Control Module

SCM provides a man-machine interface to file server and supervisor subroutines to support system control and overall supervision of the TCAC PIP workstations.

AN/USC-55 Commander's Tactical Terminal

The AN/USC-55 commander's tactical terminal (CTT) is a multiservice-developed, special application, UHF satellite communications receiver that can be dedicated to receive critical, time-sensitive intelligence by commanders and intelligence centers at all echelons, in near-real-time, at GENSER or SCI levels. The receiver provides one full-duplex and two receive-only channels. Planned concept of employment for CTT is similar to that of the tactical receive equipment (TRE) fielded widely within the MAGTF to allow access to intelligence broadcasts and intelligence collectors and producers. Full operational capability for CTT is expected during fiscal year 1999.

Team Portable Collection System Upgrade

The team portable collection system (TPCS) upgrade (figure B-8) is a semiautomated, man-transportable communications intelligence (COMINT) system. It provides intercept, collection, radio direction finding, analysis, reporting, and collection management support. The system provides significant SIGINT capabilities in a modular configuration that can be deployed by component as a stand-alone COMINT system or as part of the integrated RadBn SIGINT and MAGTF intelligence efforts. TPCS uses state-of-the-art equipment that consolidates information and expedites the delivery of critical COMINT to MAGTF and external commanders and agencies. The upgrade will extend the frequency range of the system and provide capabilities against modern signals.

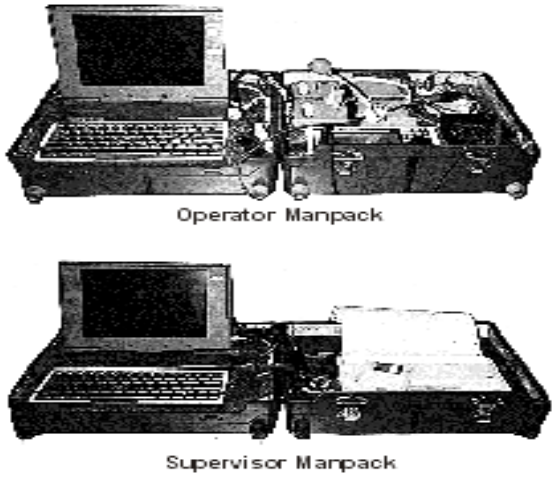


Figure B-8. Team Portable Collection System Upgrade.

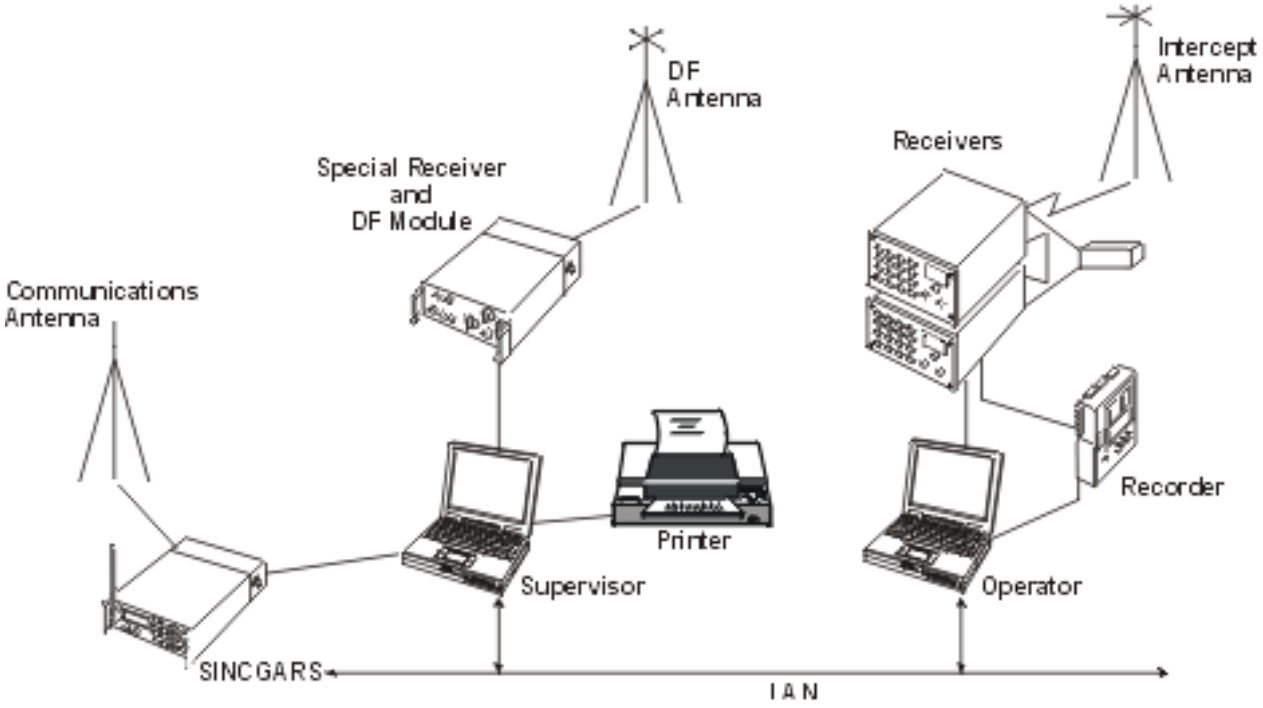


Figure B-9. Team Portable Collection System COMINT Collection Subsystem.

TPCS upgrade is comprised of three subsystems: a COMINT collection subsystem (CCS), including the AN/PRD-12 direction finding set (to be replace by TOPMAKER) and collection receivers (see figure B-9 on the facing page); an analysis subsystem (AS) (figure B-10); and a communications subsystem (CS). Modern single-channel radio nets are used to link TPCS upgrade outstations with the RadBn TCAC to allow automated processing and dissemination of collected information and ultimate dissemination to the MAGTF G-2/S-2 and other organizations. Full operational capability for TPCS upgrade is expected by the second quarter of fiscal year 2001.

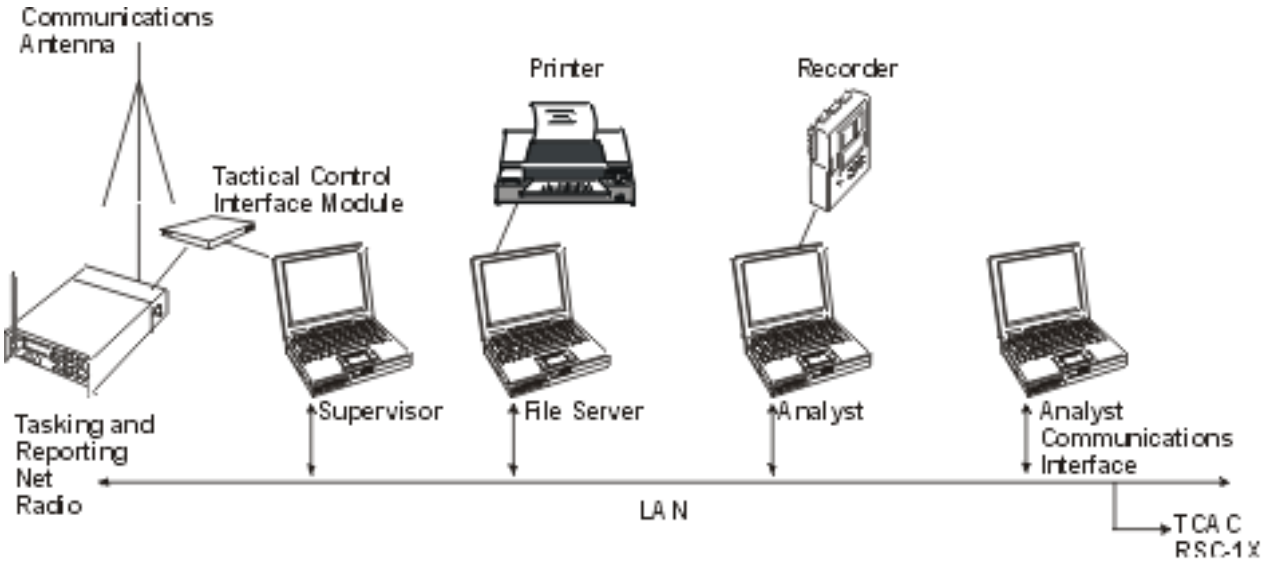


Figure B-10. Team Portable Collection System Analysis Subsystem.

Trojan Spirit II

Trojan Spirit II (TS II) is a mobile SHF satellite communications (SATCOM) system that uses commercial or military satellites to receive, transmit, and process secure, voice, data, video teleconferencing (VTC), and facsimile communications. See figure B-11. TS II provides 14 channels of digital voice or data (SCI or GENSER) with a maximum aggregate data rate of 1.544 megabytes per second (Mbps). LAN communications are supported by SCI and GENSER ethernets. Routers provide access to the secret internet protocol router network, the Joint Worldwide Intelligence Communications System, National Security Agency platform, and the defense SATCOM system. These capabilities provide the necessary dedicated communications for coordinating MAGTF SIGINT and other intelligence operations. The system consists of three HMMWVs with mounted standard integrated command post lightweight multipurpose shelters, tunnel-mounted power generation units, a towed 2.4 meter (C, Ku-band), and a 6.1 meter (C, Ku, X-band) antenna.

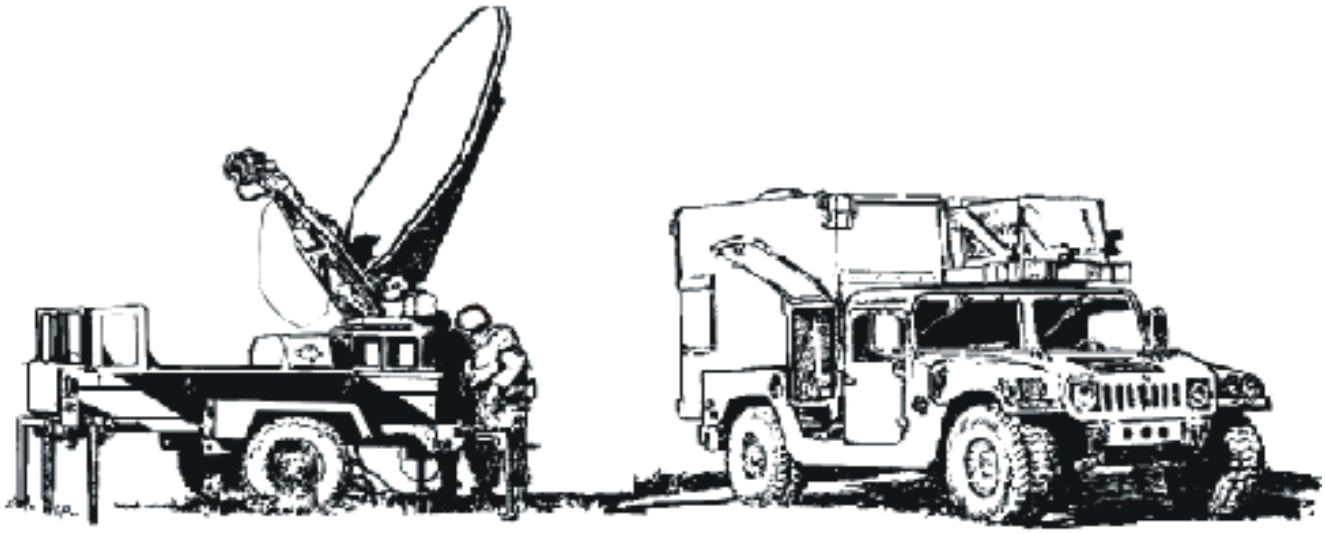


Figure B-11. Trojan Spirit II.

Radio Reconnaissance Equipment Program

The radio reconnaissance equipment program (RREP) SIGINT suite (SS)-1 is a semiautomated, integrated radio intercept and DF system composed of a ruggedized computer and six functional modules that plug together. See figure B-12. RREP SS-1 modules may operate independently or semi-independently through the use of the ruggedized, handheld computer system. It is designed to enable preplanned product improvements and future technology upgrades. The selected equipment will enable the radio reconnaissance teams (RRTs) to target the majority of low-level, single-channel, unencrypted tactical signals of interest used by military, police, insurgents, and other potential hostile forces throughout the world. RREP SS-1 will be employed by RRTs during advance force, preassault and deep postassault conventional, and special operations, under any environmental, climatic, or weather conditions. The system is designed to lighten the individual RRT Marine's combat load as well as to enhance the RRT's operational signal search and technical data base development collection operations.

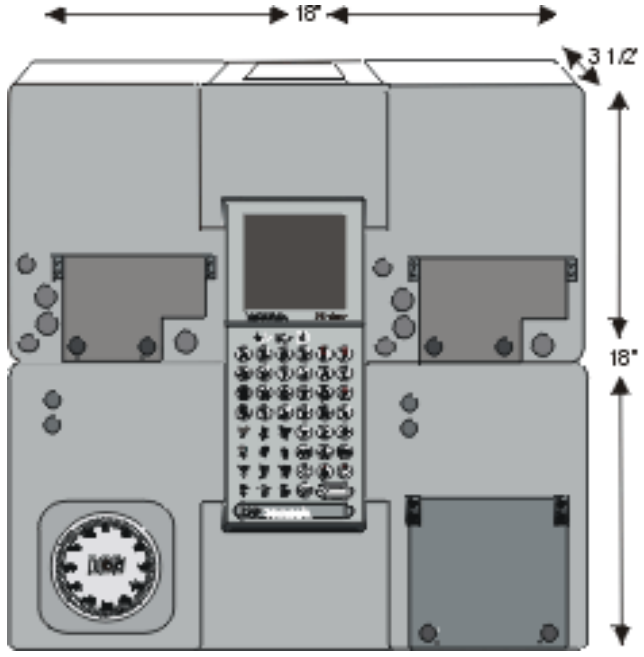


Figure B-12. RREP SS-1.

The RREP SS-2 will provide a highly deployable, man-transportable, signals intercept and DF system employed by RRTs in support of the entire spectrum of MAGTF operations. See figure B-13. RREP SS-2 employs advanced receiver capabilities, cellular phone and other digital communications collection and DF technology, global positioning system map navigation software, a more modular design, and electronic attack capabilities. As with RREP SS-1, the SS-2 operates at the modular level and at the integrated system level. The system can be controlled manually or via subcompact personal computer.

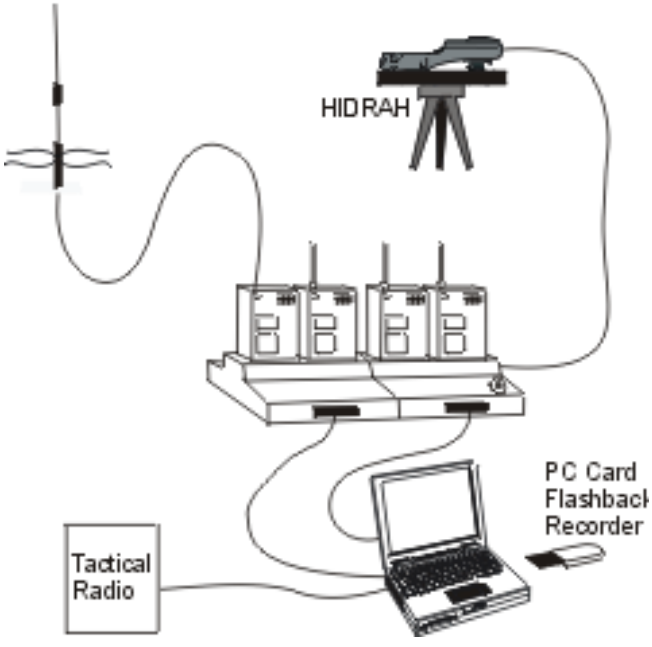


Figure B-13. RREP SS-2.

The handheld integrated directional receiver and homing (HIDRAH) system is a man-transportable, tactical, cordless, radio intercept and signal line-of-bearing (LOB) DF system consisting of several commercial off-the-shelf items of equipment fully integrated in a single, ruggedized and weather-resistant housing. HIDRAH provides RRTs with a threat I&W capability during radio reconnaissance foot-mobile patrols and signal homing support for tactical recovery of aircraft and personnel operations. The HIDRAH system has a unique design that may be employed independently in a handheld manner or by mounting it to an M16 rifle (figure B-14).

Figure B-14. Rifle-Mounted HIDRAH.

Section II. Radio Battalion SIGINT Equipment Technical Characteristics

Designator	Description	Frequency Coverage	Modulation
AN/MLQ-36	MEWSS; COMINT collect/process/ analysis; EA	20-80 MHz (collection and DF expandable to 500 MHz)	AM, FM, ICW, SSB, FSK
AN/MLQ-36A	MEWSS-PIP; COMINT/ELINT collect/process/geolocation; EA	0.5 MHz - 40 GHz	conventional, low probability of intercept
AN/PRD-12	direction finder set, man packable	.5 - 500 MHz	AM, FM, ICW, SSB, FSK
AN/ULQ-19(V)2	electronic attack set; EA	20 - 79.975 MHz	FM
AR-2002	commercial VHF/UHF frequency scanner; COMINT	25 - 550 MHz, 800 - 1300 MHz	AM, FM
AR-2500	commercial HF/VHF/ UHF frequency scanner; COMINT	1 - 1500 MHz	AM, FM, CW, SSB
AR-2515	commercial HF/VHF/ UHF frequency scanner; COMINT	5 - 1500 MHz	AM, FM
AR-3000	commercial HF/VHF/ UHF frequency scanner; COMINT	0.1 - 2036 MHz	AM, FM, CW, SSB
EB-100	receiver, miniport VHF/UHF; DF	20 - 1000 MHz intercept and DF	AM or FM
HEXJAMS	hand-emplaced, expendable jammers	barrage jam 20 - 80 MHz	NA
HIDRAH	COMINT collection, DF	.1 - 1900 MHz intercept 25 - 1000 MHz DF	AM, FM, USB, LSB, CW
IC-R71A	general coverage HF receiver; COMINT	0.1 - 30 MHz	AM, FM, CW
IC-R7000	general coverage VHF/UHF receiver; COMINT	25 - 1300 MHz	AM, FM, SSB
IC-R9000	general coverage HF/VHF/UHF receiver; COMINT	0.1 - 1999.80 MHz	AM, FM, CW, SSB
ICF-PR080	commercial HF/VHF handheld frequency scanner; COMINT	.15 - 108 MHz & 115.15 - 223 MHz	AM, FM, SSB
MPR-88	receiver, miniport VHF/UHF, ruggedized; COMINT	20 - 1000 MHz intercept	AM or FM
R-2174(P)/URR	radio receiver, general purpose, HF; COMINT	0.5 - 29.999 MHz	AM, FM, CW, SSB
RREP SS-1	COMINT collection, DF	1 - 2000 MHz intercept 25 - 1000 MHz DF	AM, FM, USB, LSB, CW
RREP SS-2	COMINT collection, DF	.1 - 1900 MHz intercept 25 - 1000 MHz DF	AM, FM, USB, LSB, CW
WJ-8616	radio receiver, general purpose, HF; COMINT	0.5 - 29.999 MHz	AM, FM, CW, SSB
WJ-8618	radio receiver, general purpose, VHF/UHF; COMINT	20 - 500 MHz	AM, FM, CW, pulse
WJ-8654	radio receiver, general purpose, COMINT	.5 MHz - 1.0 GHz	AM, FM, CW, pulse

Section III. VMAQ SIGINT and EW Equipment

EA-6B Prowler

The EA-6B Prowler (figure B-15) is a subsonic advanced warfare carrier capable aircraft, powered by twin turbojet engines. The crew is composed of one pilot and three electronic countermeasure officers. The AN/ALQ-99 tactical jamming system effectively incorporates receivers and external pods for power and transmission of jamming signals. The Prowler receives and processes designated signals of interest (SOIs) for jamming selected SOIs for subsequent processing and analysis and employs the AGM-88 high-speed antiradiation missile (HARM).

Figure B-15. EA-6B Prowler.

AN/TSQ-90D/E(V) TERPES

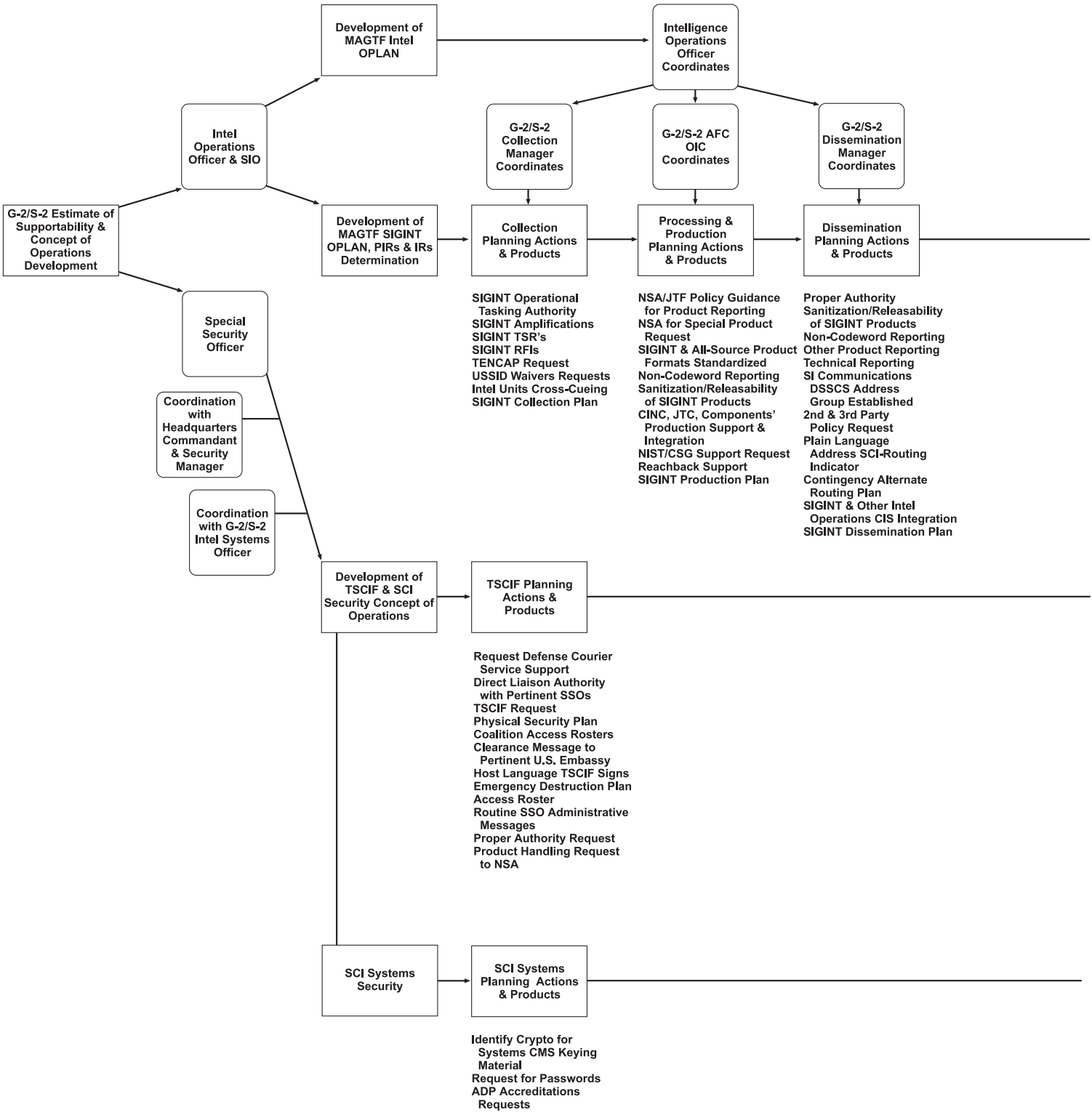
The AN/TSQ-90D/E(V) tactical electronic reconnaissance processing and evaluation system (TERPES) receives, processes, evaluates, and displays electronic reconnaissance and EA mission information received from the EA-6B aircraft and other theater and national electronic intelligence (ELINT) assets (figure B-16). TERPES also assists the MAGTF aviation combat element's (ACE) air strike mission planning and intelligence requirements. It is a multisource, integrated, tactical ELINT data processing, correlation, and fusion system installed in a S-280-size transportable shelter. TERPES supports the ELINT and EA/ES mission and VMAQ and MAGTF ACE commander's intelligence requirements. TERPES may be transported by aircraft, shock-mounted air-ride commercial or tactical ground vehicle, or attachable mobilizer for short distances.

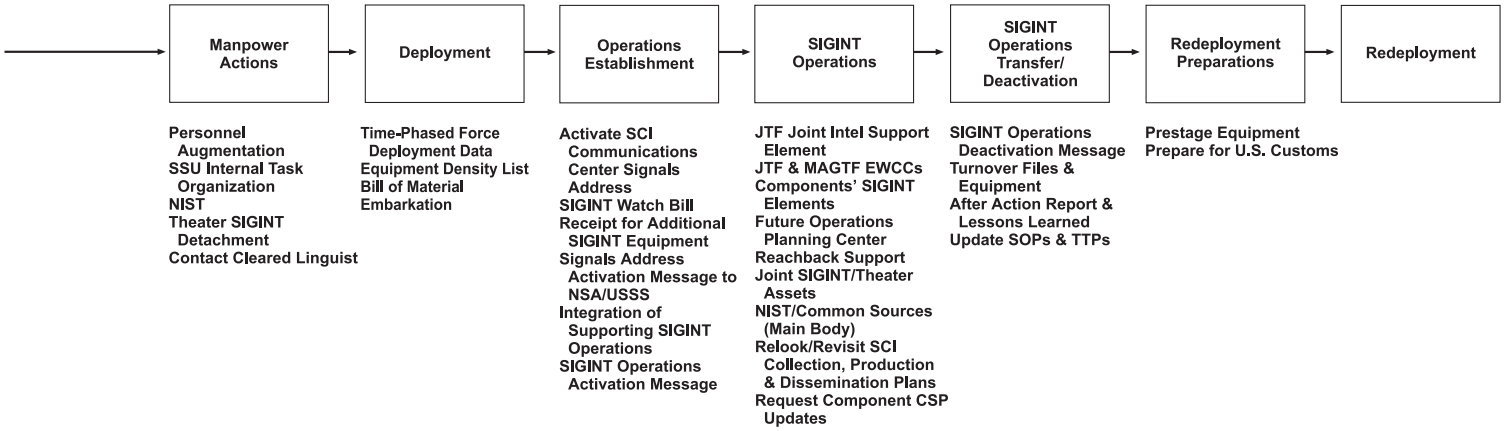
Figure B-16. AN/TSQ-90D/E(V), TERPES Portable Unit.

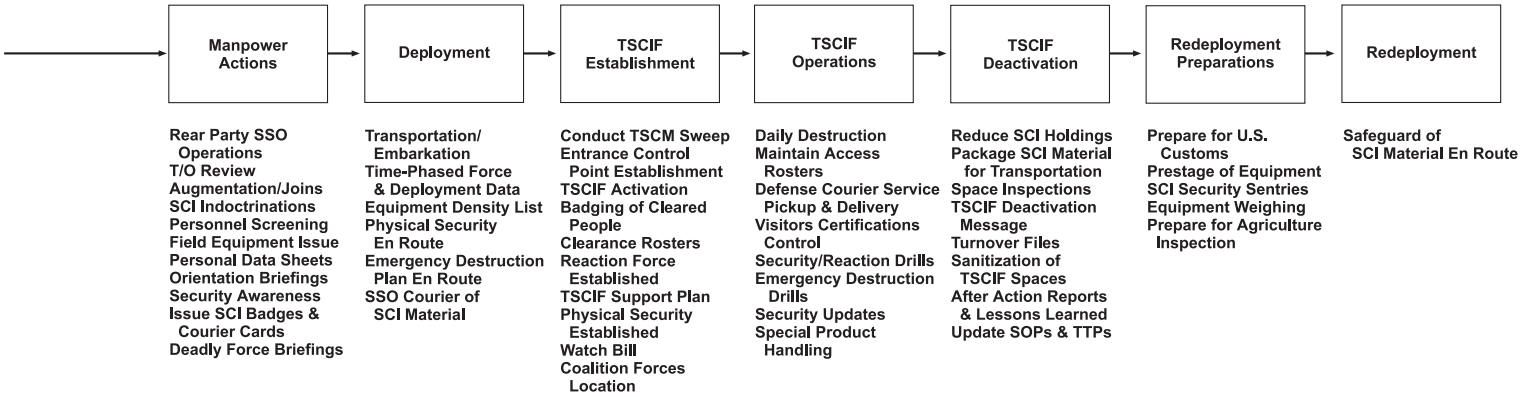
Appendix C

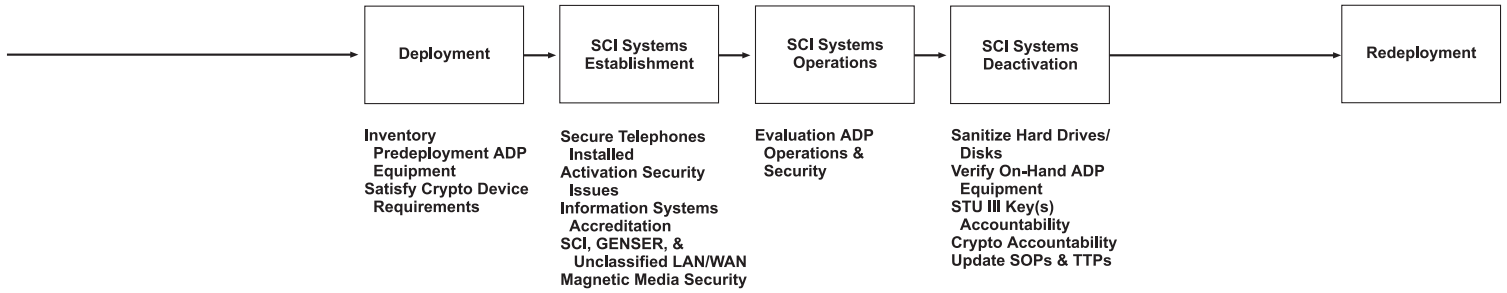
SIGINT and SCI Security Management Operations Flowchart

The flowchart on the following pages summarizes the principal SIGINT and SCI security planning considerations, activities, and products discussed in this publication.


Development of MAGTF Intel OPLAN
Intelligence Operations Officer Coordinates
Intel Operations Officer & SIO
G-2/S-2 Collection Manager Coordinates
G-2/S-2 AFC OIC Coordinates
G-2/S-2 Dissemination Manager Coordinates
G-2/S-2 Estimate of Supportability & Concept of Operations Development
Development of MAGTF SIGINT OPLAN, PIRs & IRs Determination
Collection Planning Actions & Products
Processing & Production Planning Actions & Products
Dissemination Planning Actions & Products
SIGINT Operational Tasking Authority
SIGINT Amplifications
SIGINT TSR's
SIGINT RFIs
TENCAP Request
USSID Waivers Requests
Intel Units Cross-Cueing
SIGINT Collection Plan
NSA/JTF Policy Guidance for Product Reporting
NSA for Special Product Request
SIGINT & All-Source Product Formats Standardized
Non-Codeword Reporting
Sanitization/Releasability of SIGINT Products
CINC, JTC, Components' Production Support & Integration
NIST/CSG Support Request
Reachback Support
SIGINT Production Plan
Proper Authority
Sanitization/Releasability of SIGINT Products
Non-Codeword Reporting
Other Product Reporting
Technical Reporting
SI Communications
DSSCS Address Group Established
2nd & 3rd Party Policy Request
Plain Language Address SCI-Routing Indicator
Contingency Alternate Routing Plan
SIGINT & Other Intel Operations CIS Integration
SIGINT Dissemination Plan
Special Security Officer
Coordination with Headquarters Commandant & Security Manager
Coordination with G-2/S-2 Intel Systems Officer
Development of TSCIF & SCI Security Concept of Operations
TSCIF Planning Actions & Products
Request Defense Courier Service Support
Direct Liaison Authority with Pertinent SSOs
TSCIF Request
Physical Security Plan
Coalition Access Rosters
Clearance Message to Pertinent U.S. Embassy
Host Language TSCIF Signs
Emergency Destruction Plan
Access Roster
Routine SSO Administrative Messages
Proper Authority Request
Product Handling Request to NSA
SCI Systems Security
SCI Systems Planning Actions & Products
Identify Crypto for Systems CMS Keying Material
Request for Passwords
ADP Accreditations Requests







(reverse blank)

Appendix D

SIGINT Appendix Format

This appendix should explain how SIGINT elements supporting or under the operational control of the MAGTF will be used to support this plan. It should also provide guidance to subordinate commanders for the conduct of SIGINT operations and the support of SIGINT elements and personnel identified to fulfill the SIGINT requirements in this plan.

CLASSIFICATION

Copy no.___ of ___ copies
Issuing Unit
PLACE OF ISSUE
Date/time group
Message reference number

APPENDIX 2 (Signals Intelligence) to ANNEX B (Intelligence) to Operation Order _____ ( )

Ref: (a) Unit standing operating procedures (SOPs) for intelligence and counterintelligence

(b) Combatant commander, joint task force, or other higher authorities' operation orders (OPORDs) and tactics, techniques, and procedures directives

(c) (List other documents that provide guidance required for SIGINT and supporting operations planning functions.)

1. ( ) <u>SITUATION</u>

a. ( ) <u>Enemy Situation</u>. (Reference Appendix 8 [Intelligence Estimate] to Annex B. Describe the threat and potential threat, the basic situation and the SIGINT operations perspective. Identify the enemy's command and contro tactical and electronic orders of battle; and estimates of the enemy's centers of gravity, critical vulnerabilities, intentions, capabilities, and possible courses of action pertinent to SIGINT operations. When possible, identify finished intelligence products supporting these findings. Reference Annex B and current intelligence estimates for threat capabilities, limitations, vulnerabilities, order o battle, and assessed courses of action.)

CLASSIFICATION

b. ( ) Friendly Situation. (Reference Annex C [Operations] and other pertinent sources.)

c. ( ) SIGINT Support Available. (Reference Annex A [Task Organization], Annex B, and other pertinent sources. Identify organic, attached, and supporting SIGINT elements available to support MAGTF intelligence operations. Specify elements attached to or in direct support of any subordinate unit.)

2. ( ) MISSION

(State concisely the SIGINT mission as it relates to the command's planned operation.)

3. ( ) EXECUTION

a. ( ) Concept of Operations. (Summarize pertinent command relationships, task organization, main and supporting efforts, and the scope of MAGTF and supporting SIGINT and relevant all-source intelligence operations.)

b. ( ) Tasks for SIGINT and Subordinate Units and Task Force Commanders and Officers in Charge (OICs).

(1) ( ) Radio battalion (RadBn) SIGINT support unit (SSU) commanding officer or OIC

(2) ( ) Aviation combat element commander (special attention to VMAQ tasks)

(3) ( ) Ground combat element (GCE) commander

(4) ( ) Rear area operations center (RAOC) commander

(5) ( ) (Others as appropriate)

(This section may include direction, requirements, authority, and other guidance regarding SIGINT elements placed in direct support of MAGTF subordinate element. Also it may include tactical sensitive compartmented [SCI] facilities, special security offices, physical security, and personnel supporting SIGINT and SCI operations, etc.)

CLASSIFICATION

c. ( ) Coordinating Instructions. (Restatement of MAGTF priority intelligence requirements; detailed procedures for intelligence requirements management; SIGINT support requests; direct liaison among subordinate commanders, MAGTF SIGINT units, staff officers, and pertinent external organizations and agencies; routine and time-sensitive reporting and formats; etc.)

4. ( ) ADMINISTRATION AND LOGISTICS

a. ( ) Logistics. (Reference Annex D [Logistics]. Identify unique combat service support requirements, procedures, and guidance to support MAGTF SIGINT units and operations. Specify procedures for specialized technical logistics support necessary from external organizations [e.g., from Director, National Security Agency, or via service cryptologic element channels].)

b. ( ) Personnel. (Reference Annex E [Personnel]. Identify SIGINT-unique personnel requirements and concerns, including global sourcing support and contracted linguist requirements.)

c. ( ) Consolidated Listing and Impact Assessment of Shortfalls and Limiting Factors. (Provide a consolidated listing and impact assessment of personnel and equipment shortfalls and other limiting factors that significantly affect unit SIGINT operations and support. Identify resource problems and specify key tasks that might not be accomplished adequately.)

5. ( ) COMMAND AND CONTROL

(Reference the MAGTF's and SIGINT units' SOPs and Appendix 10 [Intelligence Operations Plan]. Provide guidance as appropriate on the following, including internal unit and external organizations' command and control [C2])

a. ( ) Command Relationships. (Reference Annex J [Command Relationships]. Provide any instructions necessary regarding command relationships arrangements that will influence MAGTF SIGINT operations, with special attention to C2 relationship concerning SIGINT elements attached to or in direct support of MAGTF subordinate units.)

b. ( ) Information Management. (Reference Annex U [Information Management], Annex C [Operations], and Appendix 10 to Annex B. Provide any instructions necessary regarding information management [e.g., time-sensitive and routine SIGINT reporting criteria, SIGINT data bases, administration and access, reports] that will influence MAGTF SIGINT operations.)

CLASSIFICATION

c. ( ) Communications and Information Systems (CIS) . (Reference Appendix 10 to Annex B and Annex K [Communications and Information Systems]. Provide any instructions necessary regarding CIS that will influence MAGTF SIGINT operations.)

d. ( ) SIGINT C2 Nodes and Facilities. (Reference the MAGTF's and SIGINT units' SOPs and Appendix 10 to Annex B. Provide any guidance and instructions necessary regarding the establishment and operations of SIGIN C2 nodes and facilities [e.g., the operations control and analysis center, amphibious task force ship's signals exploitation spaces] and their integration with other MAGTF C2 nodes [e.g., the MAGTF all-source fusion center, the surveillance and reconnaissance center, the reconnaissance operations center, the amphibious task force intelligence center, electronic warfare coordination center].)

/s/ _____
_____

OFFICIAL

/s/ _____
_____

TABS:

A - Communications Intelligence Operations Requirements

B - Electronic Intelligence Operations Requirements

C - (Others as appropriate: routine and time-sensitive reporting formats, SIGINT CIS plan, etc.)

CLASSIFICATION

Copy no.___ of ___ copies
Issuing Unit
PLACE OF ISSUE
Date/time group
Message reference number

TAB A (Communications Intelligence Operations Requirements) to APPENDIX 2 (Signals Intelligence) to ANNEX B (Intelligence) to Operation Order _____( )

1. ( ) GENERAL

(The purpose of this tab is to identify operations requirements for communications intelligence [COMINT] support to the planned MAGTF operation.)

NOTE: SCI controls may require this tab to be published separately from the basic OPORD, Annex B and/or Appendix 2.

a. ( ) (Orient COMINT collection, processing and exploitation, production, and dissemination efforts to answer the questions listed in paragraphs 2 and 3 below.)

b. ( ) (These requirements should address both organic and external direct support SIGINT resources tasked to support the MAGTF.)

c. ( ) (Reference other pertinent portions of Annex B and current intelligence estimates.)

2. ( ) COMINT OPERATIONS REQUIREMENTS AND MANAGEMENT

a. ( ) Classification. (Designate the overall classification of the information included. Assign the lowest classification possible consistent with established security guidelines.)

b. ( ) Statement of Requirement. (Describe in detail COMINT information need, priority, specification of timeliness, location accuracy, and periodicity using the following format:

(1) ( ) Requirement. A detailed narrative statement of the requirement.

CLASSIFICATION

(2) ( ) Priority. The priority of each requirement specification, using the following criteria for assigning priority:

(a) ( ) Priority 1. Intelligence vital to successful plan implementation (forms the basis for the most crucial operational decisions).

(b) ( ) Priority 2. Intelligence of critical importance to plan implementation, required for making operational decisions and planning future operations.

(c) ( ) Priority 3. Intelligence of major importance to plan implementation, including intelligence required for the security of significant numbers of United States (and allied) forces.

(d) ( ) Priority 4. Intelligence of considerable importance to plan implementation (makes important contribution to operational decisionmaking and planning).

(e) ( ) Priority 5. Intelligence of moderate importance to plan implementation (makes moderate contribution to operational decisionmaking and planning).

(f) ( ) Priority 6. Intelligence of some importance to plan implementation (contributes in a measurable way to operational decisionmaking and planning).

(g) ( ) Priority 7. Intelligence of interest to plan implementation.

(3) ( ) Time. (Identify the maximum delay acceptable for receipt of information by the intended user [e.g., within 10 minutes after recognition].)

(4) ( ) Location Accuracy. (Identify the minimum locational accuracy for which the information is needed [e.g., 95-percent confidence, within 1 kilometer of center mass, within 25 kilometers of emitter location].)

(5) ( ) Periodicity. (Identify the maximum amount of time that should pass before the target is covered again [i.e., once every 24 hours or once every 8 hours].)

CLASSIFICATION

c. ( ) User Echelon(s). (Identify the primary echelon needing the information [e.g., GCE, RAOC]. List multiple users only if all data elements o subparagraph 2c above are the same for all listed echelons; otherwise, restate the requirement.)

d. ( ) Geographic Area. (Specify the geographic area for which the requirement specification applies, defined precisely [i.e., Country X, 0 to 50 km from western border; or Country Y, 50 to 75 km from southeastern border].)

e. ( ) Justification. (For each requirement specification, indicate the operational function(s) or purpose(s) [i.e., artillery targeting or air reconnaissance planning].)

3. ( ) UPON IMPLEMENTATION OF THE OPORD. (List, in the manner described above, the COMINT operational requirements that become relevant upon implementation of the plan. Use subsequent paragraphs to reflect additional support requirements for planned phases of combat operations.)

Appendix E

TSCIF Checklist

The following checklist is provided as a guide when activating and deactivating a tactical sensitive compartmented information facility (TSCIF). The security measures identified should be improved upon as the situation permits. Refer to Director of Central Intelligence Directive (DCID) 1/21, *Physical Security Standards for Sensitive Compartmented Information Facilities*, and Department of Defense Directive (DODD) 5105.21-M-1, *Sensitive Compartmented Information (SCI) Security Manual*, *Administrative Security*, for detailed TSCIF operations policy and procedures.

TSCIF Activation

- ❑ **Obtain site location from advance party personnel.**
- ❑ **Submit request to establish TSCIF to cognizant special security officer (SSO).**
- ❑ **Assign vehicle and/or shelter locations to site personnel.**
- ❑ **Move vehicles into site position. Ensure SCI containers remain locked and guarded unt site is accredited.**
- ❑ **Configure site for operation needs and ease of future movement.**
- ❑ **Erect shelters, antennas, and camouflage.**
- ❑ **Establish internal communications (SSO to access control point and emergency reaction force).**
- ❑ **Review and implement guard procedures.**
- ❑ **Emplace barrier material and restriction signs.**
- ❑ **Establish a 24-hour, single-gate access point (shelter with lights). Provide guards with access roster of authorized personnel.**
- ❑ **Determine location of destruction site (burn barrel, etc.).**
- ❑ **Conduct briefings (i.e., operations security, emergency destruction, emergency evacuation, shift schedule, reaction force, perimeter defense, badge system).**
- ❑ **Doublecheck physical security of site.**
- ❑ **Accredit site; declare site secure.**
- ❑ **Inventory SCI documents and materials as they are unpacked.**
- ❑ **Inform G-2/S-2 of commencement of TSCIF operations.**
- ❑ **Begin SCI operations and communications.**
- ❑ **Send TSCIF activation message.**

TSCIF Deactivation

- ❑ **Receive the order to terminate operations.**
- ❑ **Coordinate deactivation time with the G-2/S-2.**
- ❑ **Zeroize communications security (COMSEC) equipment; ensure message queues are emptied.**
- ❑ **Establish guards for SCI materials; inventory and pack SCI into locked containers.**
- ❑ **Debrief all one-time access personnel.**
- ❑ **Ensure all magnetic media is degaussed a minimum of three times each and all tele type, printers, and/or typewriter ribbons are destroyed or secured with SCI material.**
- ❑ **Sweep all SCI work areas for SCI and other classified materials, including telephone directories, newspapers, magazines, notepads, trash bags, etc. Check desk drawers, underneath desks and boxes, equipment containers, bulletin boards, acetate overlays, etc.**

- ❑ **Ensure all SCI is either packed in proper containers for redeployment or destroyed using established procedures.**
- ❑ **Account for all TSCIF badges and access rosters.**
- ❑ **Make a final inspection of the TSCIF and declare it officially deactivated.**
- ❑ **Send TSCIF deactivation message.**
- ❑ **Ensure all personnel are briefed on movement time and location and SCI is properly controlled.**
- ❑ **Upon termination of operations, return to garrison SCIF, reinventory and account fo all SCI material, reset all combination locks, clear all hand receipts, and clean equipment.**
- ❑ **Update standing operating procedure and files with lessons learned during the operation.**

Appendix F

Glossary

Section I

Acronyms and Abbreviations

AAW ..... antiair warfare
ACE ..... aviation combat element
ADCON ..... administrative control
ADP ..... automatic data processing
AFB ..... Air Force base
AFC ..... all-source fusion center
AI ..... area of interest
AIA ..... Air Force Intelligence Agency
AIG ..... addressee indicator group
AM ..... amplitude modulation
AMP ..... amplifier
AO ..... area of operations
AS ..... analysis subsystem
ATARS ..... advanced tactical airborne reconnaissance system
ATF ..... amphibious task force
ATFIC ..... amphibious task force intelligence center
ATO ..... air tasking order
AWACS ..... airborne warning and control system

BDA ..... battle damage assessment
BE ..... basic encyclopedia
Bn Hq ..... battalion headquarters
bps ..... bits per second
BZO ..... battlesight zero

C2 ..... command and control
C2W ..... command and control warfare
C4I ..... command, control, communications, computers, and intelligence
Capt ..... captain
CATF ..... commander, amphibious task force
CCE ..... company command element
CCIR ..... commander's critical information requirements
CCS ..... COMINT collection subsystem
CDOC ..... cryptologic division officers course
Cdr ..... commander
CE ..... command element
CGS ..... common ground station
CHATS ..... counterintelligence/HUMINT analysis tool set
CI ..... counterintelligence
CIC ..... combat intelligence center
CIM ..... communications interface module
CINC ..... commander in chief
CIS ..... communications and information systems
CJTF ..... commander, joint task force
CLF ..... commander, landing force
CLT ..... company liaison team
CMC ..... Commandant of the Marine Corps
CMO ..... collections management officer
CMS ..... COMSEC materials system
CNSG ..... Commander, Naval Security Group
CO ..... commanding officer
COC ..... current operations center
COMINT ..... communications intelligence
comm ..... communications
COMMARFOR ..... commander, Marine Corps forces
COMMARFORLANT ..... Commander, Marine Corps Forces, Atlantic
COMMARFORPAC ..... Commander, Marine Corps Forces, Pacific
COMSEC ..... communications security
CONPLAN ..... contingency plan
Cpl ..... corporal
CPX ..... command post exercise
CRITICOMM ..... critical communications
CS ..... communications subsystem
CSG ..... cryptologic support group
CSP ..... cryptologic support plan
CSS ..... combat service support
CSSA ..... cryptologic shore support activity

CSSD ..... combat service support detachment
CSSE ..... combat service support element
CTT ..... commander's tactical terminal
CW ..... continuous wave

DASC ..... direct air support center
DCI ..... Director of Central Intelligence
DCID ..... Director of Central Intelligence Directive
DCS ..... Defense Courier Service
DF ..... direction finding
DIA ..... Defense Intelligence Agency
DIAM ..... Defense Intelligence Agency manual
DIRNSA ..... Director, National Security Agency
DLI ..... Defense Language Institute
DMS ..... Defense Message System
DOD ..... Department of Defense
DODD ..... Department of Defense directive
DON ..... Department of the Navy
DONCAF ..... Department of the Navy Central Adjudication Facility
DS ..... direct support
DSSCS ..... defense special security communications system

EA ..... electronic attack
EA-6B ..... all weather electronic attack aircraft (Prowler)
ECAC ..... Electromagnetic Compatibility Analysis Center
ECMO ..... electronic countermeasures officer
ECU ..... environmental control unit
e.g. ..... for example
EHF ..... extremely high frequency
ELINT ..... electronics intelligence
EM ..... electromagnetic
EMCON ..... emission control
EOB ..... electronic order of battle
EP ..... electronic protection
EPL ..... ELINT parameters list
ERP ..... effective radiated power
ES ..... electronic warfare support
EW ..... electronic warfare
EWCC ..... electronic warfare coordination center
EWDS ..... electronic warfare data base system
EWIR ..... electronic warfare integrated reprogramming
EWMSNSUM ..... EW mission summary report
EWO ..... electronic warfare officer

FDM ..... frequency division multiplexing
FIE ..... fly-in echelon
FIIU ..... force imagery interpretation unit
FISINT ..... foreign instrumentation signals intelligence
FM ..... frequency modulation
FMF ..... Fleet Marine Force
FMFM ..... Fleet Marine Force manual
FSCC ..... fire support coordination center
FSK ..... frequency shift key
FSSG ..... force service support group

G-1 ..... manpower or personnel staff officer
G-2 ..... intelligence staff officer
G-3 ..... operations staff officer
G-4 ..... logistics staff officer
G-6 ..... communications and information systems officer
GCE ..... ground combat element
GENSER ..... general service
GHz ..... gigahertz
GS ..... general support; general schedule
GSA ..... General Services Administration
GySgt ..... gunnery sergeant

H&S ..... headquarters and service
HARM ..... high-speed antiradiation missile
HF ..... high frequency
HIDRAH ..... handheld integrated directional receiver and homing
HMMWV ..... high mobility, multipurpose wheeled vehicle
HQMC ..... Headquarters, Marine Corps
HUMINT ..... human resources intelligence

I&W ..... indications and warning
IAA ..... Intelligence Analysis Application
IADS ..... integrated air defense system
IAS ..... intelligence analysis system
ICR ..... intelligence collection requirement
ICW ..... interrupted continuous wave
ID ..... identification
IDR ..... intelligence dissemination requirement
i.e. ..... that is
IEWCS ..... intelligence and electronic warfare common sensor
IMINT ..... imagery intelligence

INSCOM..... U.S. Army Intelligence and Security Command
intel .....intelligence
IPR ..... intelligence production requirement
IR .....intelligence requirement
ISSM ..... information system security manager
ISSO..... information system security officer
ITS .....individual training standards
ITT ..... interrogator-translator team

JC2WC..... Joint Command and Control Warfare Center
JCS ..... Joint Chiefs of Staff
JDISS .....joint deployable intelligence support system
JFACC ..... joint force air component commander
JFC ....joint force commander
JFLCC..... joint force land component commander
JFMCC.....joint force maritime component commander
JIC .....joint intelligence center
JISE..... joint intelligence support element
JMCIS ..... joint maritime command information system
JSC.....joint spectrum center
JSIPS ..... Joint Service Imagery Processing System
J-TENS..... Joint Tactical Exploitation of National Systems
JTF .....joint task force
JWICS.....Joint Worldwide Intelligence Communications System

LAN .....local area network
LAV ..... light armored vehicle
LCpl .....lance corporal
LE.....law enforcement
LOB ..... line of bearing
LOS ..... line of sight
LSB ..... lower sideband
Lt.....lieutenant
LTI ..... limited technical inspection

MAG ..... Marine aircraft group
MAGTF ..... Marine air-ground task force
MARDIV ..... Marine division
MARFOR .....Marine Corps forces
MarSptBn ..... Marine support battalion
MASINT .....measurement and signature intelligence
MATCD ..... Marine air traffic control detachment
MAW .....Marine aircraft wing
Mbps ..... megabytes per second
MCB..... Marine Corps base
MCO ..... Marine Corps Order
MCW .....modulated continuous wave
MCWP .....Marine Corps warfighting publication
MECDL ..... mission equipment control data link
MEF .....Marine expeditionary force
MEU .....Marine expeditionary unit
MEU(SOC) .....Marine expeditionary unit (special operations capable)
MEWSS .....mobile electronic warfare support system
MEWSS PIP .....mobile electronic warfare support system product improvement program
MHz .....megahertz
MIDB ..... modernized integrated data base
MISSI..... multilevel information system security initiative
MOS ..... military occupational specialty
MSC.....major subordinate command
MSE .....major subordinate element
MSgt.....master sergeant
MSPF ..... maritime special purpose force
MUX ..... multichannel radio

NATO ..... North Atlantic Treaty Organization
NATOPS..... Naval Air Training and Operating Procedures Standardization
NAVSUP ..... Navy supplement
NCA ..... National Command Authorities
NCO.....noncommissioned officer
NCOIC ..... noncommissioned officer in charge
NCS.....net control station
NCW ..... non-codeword
NDA.....nondisclosure agreement
NEF.....naval expeditionary force
NID .....naval intelligence data base
NIMA ..... National Imagery and Mapping Agency
NIPRNET..... nonsecure internet protocol router network
NIST..... national intelligence support team
NMCC..... National Military Command Center

NRO ..... National Reconnaissance Office
NRT ..... near-real-time
NSA ..... National Security Agency
NSANET ..... National Security Agency Network
NSG ..... Naval Security Group
NSGA ..... Naval Security Group Activity
NSOC ..... National Security Operations Center
NTF ..... naval task force
NTTC ..... Naval Technological Training Center

OAS ..... offensive air support
OBREP ..... order of battle report
OCA ..... operations control and analysis
OCAC ..... operations control and analysis center
OccFld ..... occupational field
OIC ..... officer in charge
OLT ..... OCAC liaison team
ONI ..... Office of Naval Intelligence
OOB ..... order of battle
OPCON ..... operational control
OPLAN ..... operation plan
OPNAV ..... Office of the Chief of Naval Operations
OPORD ..... operation order
OTH ..... over the horizon
OWO ..... operations watch officer

PCM ..... pulse code modulation
PIP ..... product improvement program
PIR ..... priority intelligence requirement
PU ..... participating unit

RadBn ..... radio battalion
RAOC ..... rear area operations center
RAWS ..... remoteable analysis workstation
recon ..... reconnaissance
RF ..... radio frequency
RFI ..... request for intelligence
RREP ..... radio reconnaissance equipment program
RRP ..... radio reconnaissance platoon
RRT ..... radio reconnaissance team
RSOC ..... regional security operations center
RSR ..... resource status report
RU ..... reporting unit

S-1 ..... manpower or personnel staff officer
S-2 ..... intelligence staff officer
S-3 ..... operations staff officer
S-4 ..... logistics staff officer
S-6 ..... communications and information systems staff officer
SALUTE ..... size, activity, location, unit, time, and equipment
SARC ..... surveillance and reconnaissance center
SATCOM ..... satellite communications
SCAMP ..... sensor control and management platoon
SCE ..... service cryptologic element
SCI ..... sensitive compartmented information
SCIF ..... sensitive compartmented information facility
SCM ..... supervisor control module
SCR ..... single-channel radio
Sgt ..... sergeant
SHF ..... super high frequency
SI ..... special intelligence
SIDS ..... secondary imagery dissemination system
SIGINT ..... signals intelligence
SINCGARS ..... single-channel ground and airborne radio system
SIO ..... signals intelligence officer
SIPRNET ..... secret internet protocol router network
SNCO ..... staff noncommissioned officer
SNCOIC ..... staff noncommissioned officer in charge
SOC ..... special operations capable
SOI ..... signal of interest
SOP ..... standing operating procedure
SOTA ..... SIGINT operational tasking authority
SPINTCOMM ..... special intelligence communications
SPMAGTF ..... special-purpose Marine air-ground task force
SS ..... SIGINT suite
SSB ..... single sideband
SSBI ..... single-scope background investigation
SSCC ..... special security communications center
SSCT ..... special security communications team
SSE ..... SIGINT support element
SSES ..... ship's signals exploitation space
SSgt ..... staff sergeant
SSO ..... special security officer
SSOC ..... special security operations center
SST ..... SIGINT support team
SSU ..... SIGINT support unit

STAFFEX ..... staff exercise
STU III..... secure telephone unit-type III

TACC..... tactical air command center (USMC) tactical air control center (USN)
TACELINT..... tactical ELINT
TACINTEL..... tactical intelligence
TACREP ..... tactical report
TACSAT.....tactical satellite
TAD ..... temporary additional duty
TADIL ..... tactical digital information links
TAMPS ..... Tactical Aircraft Mission Planning System
TAOC ..... tactical air operations center
TCAC ..... technical control and analysis center
TCAE..... technical control and analysis element
TCIM .....tactical control interface module
TCO .....tactical combat operations
TDDS.....tactical receive equipment and related applications program data dissemination system
TDN ..... tactical data network
T/E .....table of equipment
TEAMS ..... tactical EA-6B mission planning system
TECHCON.....technical control
TEG.....tactical exploitation group
TENCAP .....tactical exploitation of national capabilities program
TEPP..... TERPES ELINT preprocessor
TERPES.....Tactical Electronic Reconnaissance Processing and Evaluation System
TFP.....TERPES fusion processor
TIBS.....tactical information broadcast system
TJS .....tactical jamming system
T/O ..... table of organization
topo ..... topographic
TPCS .....team portable collection system
TPFDD.....time-phased force and deployment data
TPU.....TERPES portable unit
TRAP.....TRE and Related Applications
TRE .....tactical receive equipment
TRIB ..... tactical remote intelligence broadcast
TRIXS ..... Tactical Reconnaissance Intelligence Exchange System
TRSS.....tactical remote sensor system
TS II..... Trojan Spirit II
TSCIF..... tactical sensitive compartmented information facility
TSCM ..... technical surveillance countermeasures
TSR.....telecommunications service request
TTP..... tactics, techniques, and procedures

UAV.....unmanned aerial vehicle
UHF ..... ultra high frequency
USAF.....United States Air Force
USB ..... upper sideband
USMC..... United States Marine Corps
USSID ..... United States Signals Intelligence Directive
USSS ..... United States SIGINT System

VHF ..... very high frequency
VMAQ .....Marine tactical electronic warfare squadron
VPN .....voice product net
VTC ..... video teleconferencing

WAN..... wide area network

Section II

Definitions

A

all-source intelligence Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. (Join Pub 1-02)

amphibious objective area—A geographical area, delineated in the initiating directive, for purposes of command and control (C2) within which is located the objective(s) to be secured by the amphibious task force (ATF). This area must be of sufficient size to ensure accomplishment of the ATF's mission and must provide sufficient area for conducting necessary sea, air, and land operations. Also called AOA. (Joint Pub 1-02)

area of interest—That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (Joint Pub 1-02)

area of operations—An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. Also called AO. (Joint Pub 1-02)

B

basic intelligence—Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (Joint Pub 1-02)

battle damage assessment—The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (Joint Pub 1-02) In Marine Corps usage, the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCRP 5-12C)

battlespace—All aspects of air, surface, subsurface, land, space, and electromagnetic spectru which encompass the area of influence and area of interest. (MCRP 5-12C)

battlespace dominance—The degree of control over the dimensions of the battlespace which enhances friendly freedom of action and denies enemy freedom of action. It permits force sustainment and application of power projection to accomplish the full range of potential operational and tactical missions. It includes all actions conducted against enemy capabilities to influence future operations. (MCRP 5-12C)

C

centralized control—In military operations, a mode of battlespace management in which one echelon of command exercises total authority and

direction of all aspects of one or more warfighting functions. It is a method of control where detailed orders are issued and total unity of action is the overriding consideration. (MCRP 5-12C)

collection—In Marine Corps usage, the gathering of intelligence data and information to satisfy the identified requirements. (MCRP 5-12C)

collection management—The process of converting intelligence requirements into collection requirements, establishing priorities, tasking o coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required. (Joint Pub 1-02) Its purpose is to conduct an effective effort to collect all necessary data while ensuring the efficient use of limited and valuable collection assets. (MCRP 2-1)

combat data—Data derived from reporting by operational units. (MCRP 5-12C)

combatant command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President through the Secretary of Defense and with the advice and assistance of Chairman of the Joint Chiefs of Staff. Combatant command typically have geographic or functional responsibilities. (Joint Pub 1-02)

command and control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (Joint Pub 1-02) The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCRP 5-12C)

command and control warfare—The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Also called C2W. (Joint Pub 2-0)

commander's critical information requirements—Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR. Note: CCIRs are normally divided into three primary subcategories: priority intelligence requirements, friendly force information requirements, and essential elements of friendly information. (MCRP 5-12C)

commander's intent—A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

communications intelligence—Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (Joint Pub 1-02)

communications security—The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results o such possession and study. Also called COMSEC. (Joint Pub 1-02 extract)

coordination—The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence and other situations in which coordination is considered necessary. (MCRP 5-12C)

critical information—Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and

act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (Joint Pub 1-02)

critical intelligence—Intelligence which is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential/ actual enemy. It includes but is not limited to the following: a. strong indications of the imminent outbreak of hostilities of any type (warning of attack); b. aggression of any nature against a friendly country; c. indications or use of nuclear-biological-chemical weapons (target); and d. significant events within potential enemy countries that may lead to modification of nuclear strike plans. (Joint Pub 1-02)

critical vulnerability—An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. Also called CV. (MCRP 5-12C)

D

decentralized control—In military operations, a mode of battlespace management in which a command echelon may delegate some or all authority and direction for warfighting functions to subordinates. It requires careful and clear articulation of mission, intent, and main effort to unify efforts of subordinate leaders. (MCRP 5-12C)

descriptive intelligence Class of intelligence which describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: *basic intelligen* , which is general background knowledge about established and relatively constant conditions; and *current intelligence*, which is concerned with describing the existing situation. (MCRP 5-12C)

detachment—1. A part of a unit separated from its main organization for duty elsewhere. 2. A temporary military or naval unit formed from other units or parts of units. (Joint Pub 1-02)

direction finding—A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receive or ancillary equipment. (Joint Pub 1-02)

dissemination—Conveyance of intelligence to users in a suitable form. (Joint Pub 1-02)

E

electronic attack—That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. (Joint Pub 1-02)

electronic protection—That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. (Joint Pub 1-02)

electronic reconnaissance—The detection, identification, evaluation, and location of foreign electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (Joint Pub 1-02)

electronic warfare—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support. (Joint Pub 1-02)

electronic warfare support—That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations

and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT), and electronic intelligence (ELINT). (Joint Pub 1-02)

electronic intelligence—Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (Joint Pub 1-02)

essential elements of friendly information—Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. Also called EEFI. (Joint Pub 1-02) Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. (MCRP 5-12C)

estimative intelligence Class of intelligence which attempts to anticipate future possibilitie and probabilities based on an analysis of descriptive intelligence in the context of planned friendly and assessed enemy operations. (MCRP 5-12C)

F

friendly force information requirements—Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition readiness, personnel status, and logistics statu could become a friendly force information requirement. Also called FFIR. (MCRP 5-12C)

fusion—In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (Joint Pub 1-02)

G

global sourcing—A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

I

indications and warning—Those intelligenc activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the Unite States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (Joint Pub 2-01)

intelligence—The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of evaluated information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, o understanding. (Joint Pub 1-02) Also in Marine Corps usage, intelligence is knowledge about the enemy or the surrounding environment needed to support decisionmaking. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence cycle—The process by which information is converted into intelligence and made available to users. (Joint Pub 2-01)

intelligence data—Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline—A well-defined area o intelligence collection, processing, exploitation and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), and open source intelligence. (Joint Pub 1-02)

intelligence operations—The variety of intelligence tasks that are carried out by various intelligence organizations and activities. (Joint Pub 1-02 extract)

intelligence preparation of the battlespace—An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operation and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (Joint Pub 1-02) In Marine Corps usage, the systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCRP 5-12C)

intelligence requirement—1. Any subject, general or specific, upon which there is a need for the collection of information or the production of intelligence. (Joint Pub 1-02 2. In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called IR. (MCRP 5-12C)

J

joint deployable intelligence support system—A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called JDISS. (Joint Pub 1-02)

joint force—A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (Joint Pub 1-02)

joint intelligence center—The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (Joint Pub 1-02)

Joint Worldwide Intelligence Communications System—The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-poin or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (Joint Pub 1-02)

M

main effort—The designated subordinate unit whose mission at a given point in time is mos critical to overall mission success. It is usually weighted with the preponderance of combat power and is directed against a center of gravity through a critical vulnerability. (MCRP 5-12C)

maneuver warfare—A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. (MCRP 5-12C)

Marine Corps Planning Process—A six-step methodology which helps organize the though processes of the commander and staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance o tempo. The six steps consist of mission analysis, course of action development, course of action analysis, comparison/decision, orders development, and transition. Also called MCPP. Note: Tenets of the MCPP include top down planning, single battle concept, and integrated planning (MCRP 5-12C)

N

named area of interest—A point or area along a particular avenue of approach through which enemy activity is expected to occur. Activity or lack of activity within a named area of interest will

help to confirm or deny a particular enemy course of action. Also called NAI. (MCRP 5-12C)

national intelligence support team—A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. Also called NIST. (Joint Pub 2-01)

O

operational architecture—A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges. Also called OA. (MCRP 5-12C)

operational control—Transferable command authority that may be exercised by commanders a any echelon at or below the level of combatan command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish mission assigned to the command. Operational control should be exercised through the commanders o subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or un training. Also called OPCON. (Joint Pub 1-02)

operations control and analysis center—Main node for the command and control of radio battalion signals intelligence operations and the overall coordination of MAGTF signals intelligence operations. Processes, analyzes, produces, and disseminates signals intelligence-derived information and directs the ground-based electronic warfare activities of the radio battalion. Also called OCAC. (MCRP 5-12C)

order of battle—The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force Also called OOB. (Joint Pub 1-02)

P

priority intelligence requirements—1. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called PIR. (Joint Pub 1-02) 2. In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCRP 5-12C)

production management—Encompasses determining the scope, content, and format of each intelligence product, developing a plan and schedule for the development of each product, assigning priorities among the various production requirements, allocating processing, exploitation, and production resources, and integrating production efforts with intelligence collection and dissemination. (MCRP 5-12C)

R

reach back—The ability to exploit resources, capabilities, expertise, etc., not physically located in the theater or a joint operations area, when established. (MCRP 5-12C)

S

sensitive compartmented information All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which

community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DOD 52001R, Information Security Program Regulation.) Also called SCI. (Joint Pub 1-02)

sensitive compartmented information facility—An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. Also called SCIF. See also sensitive compartmented information. (Joint Pub 1-02)

sensor data—Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radars, counterbattery radars, and remote ground sensors. (MCR 5-12C)

Service component command—A command consisting of the Service component commander and all those Service forces such as individuals units, detachments, organizations, and installations under the command, including the support forces that have been assigned to a combatant command, or further assigned to a subordinate unified command or joint task force. (Joint Pub 1-02)

signals intelligence—A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. Also called SIGINT. (Joint Pub 1-02)

SIGINT operational tasking authority—A military commanders's authority, delegated by DIRNSA/CHCSS, to operationally direct and levy SIGINT requirements on designated SIGINT resources. This includes authority to deploy and redeploy all or part of the SIGINT resources for which SOTA has been delegated. Also called SOTA. (USSID 1, *SIGINT Operating Policy*)

situational awareness—Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, enemy, and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. (MCRP 5-12C)

split base—Two or more portions of the same force conducting or supporting operations fro separate physical locations. (MCRP 5-12C)

surveillance and reconnaissance center—Primary element responsible for the supervision o MAGTF intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called SARC. (MCRP 5-12C)

sustained operations ashore—The employment of Marine Corps forces on land for an extended duration. It can occur with or without sustainment from the sea. Also called SOA. (MCRP 5-12C)

systems architecture—Defines the physical connection, location, and identification of key nodes, circuits, networks, warfighting platforms, etc and specific system and component performance parameters. The systems architecture is constructed to satisfy operational architecture requirements per standards defined in the technical architecture. The systems architecture shows how multiple systems within a subject area link and interoperate and may describe the internal construction or operations of particular systems within the architecture. Also called SA. (MCRP 5-12C)

T

tactical intelligence—Intelligence that is required for planning and conducting tactical operations. (Joint Pub 1-02) In Marine Corps usage, tactical intelligence is concerned primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather within the battlespace. (MCRP 5-12C)

technical architecture—The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technica guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product line are developed. Also called TA. (MCRP 5-12C)

technical control—The performance of specialized or professional service, or the exercise o professional guidance or direction through the establishment of policies and procedures.

tempo—The relative speed and rhythm of military operations over time. (MCRP 5-12C)

W

warfighting functions—The six mutually supporting military activities integrated in the conduct of all military operations are:

1. command and control—The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.
2. maneuver—The movement of forces for the purpose of gaining an advantage over the enemy.
3. fires—Those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight.
4. intelligence—Knowledge about the enemy or the surrounding environment needed to support decisionmaking.
5. logistics—All activities required to move and sustain military forces.
6. force protection—Actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities.
Also called WF. (MCRP 5-12C)

Appendix G

References and Related Publications

Department of Defense Directives (DODDs)

S-3115.7	Signals Intelligence
5105.21-M-1	Sensitive Compartmented Information (SCI) Security Manual, Administrative Security
TS-5105.21-M-2	Sensitive Compartmented Information (SCI) Security Manual, Communications Intelligence (COMINT) Policy
TS- 5105.21-M-3	Sensitive Compartmented Information (SCI) Security Manual, TK Policy
5200.1	DOD Information Security Program
5210.70	DOD Cryptologic Training

Director of Central Intelligence Directives (DCIDs)

1/14	Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information
1/16	Security Manual for Uniform Protection of Intelligence Processed in AISs and Networks
1/21	Physical Security Standards for Sensitive Compartmented Information Facilities

United States Signals Intelligence Directive (USSIDs)

1	SIGINT Operating Policy
4	Concept of SIGINT Support to Military Commanders
56	Exercise SIGINT
200	Technical SIGINT Reporting
240	ELINT Processing, Analysis, Reporting, and Forwarding Procedures
300	SIGINT Reporting
316	Non-Codeword Reporting Program
340	Tactical ELINT Reporting
341	Technical ELINT Reporting
510	Information for SIGINT Users

Defense Intelligence Agency Manual (DIAM)

50-4	Department of Defense Intelligence Information Systems (DODIIS) Information Security (INFOSEC) Program

Department of the Navy Supplement (NAVSUP) to DODD

5105.21-M-1	SCI Administrative Security Manual

Joint Publications (Joint Pubs)

1-02	Department of Defense Dictionary of Military and Associated Terms
2-0	Doctrine for Intelligence Support to Joint Operations
2-01	Joint Intelligence Support to Military Operations
2-02	National Intelligence Support to Joint Operations
3-02	Joint Doctrine for Amphibious Operations
3-13.1	Joint Doctrine for Command and Control Warfare
3-54	Joint Doctrine for Operations Security
5-0	Doctrine for Planning Joint Operations
6-0	Doctrine for C4 Systems Support to Joint Operations

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
2	Intelligence
3	Expeditionary Operations
4	Logistics
5	Planning
6	Command and Control

Marine Corps Warfighting Publications (MCWPs)

2-1	Intelligence Operations
6-22	Communications and Information Systems

Marine Corps Reference Publication (MCRP)

5-12C	Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms
5-12D	Organization of Marine Corps Forces

Marine Corps Orders (MCOs)

1510.50A	Individual Training Standard (ITS) System for the Signals Intelligence/Ground Electronic Warfare Occupational Field (OccFld) 26
5500.6F	Arming of Security and Law Enforcement (LE) Personnel and the Use of Force

Army Field Manuals (FMs)

34-2	**Collection Management and Synchronization Planning**
34-130	**Intelligence Preparation of the Battlefield**

Related Publication

Joint Tactical Exploitation of National Systems (J-TENS) Manual

REF ID:A58489

~~RESTRICTED~~

DEPARTMENT OF THE ARMY TECHNICAL MANUAL TM 32-250

DEPARTMENT OF THE AIR FORCE MANUAL AFM 100-80

FUNDAMENTALS OF TRAFFIC ANALYSIS (RADIO-TELEGRAPH)

RESTRICTED. DISSEMINATION OF RESTRICTED MATTER.—No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also AR 380–5.)

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
OCTOBER 1948

~~RESTRICTED~~

Declassified and approved for release by NSA on 12-24-2013 pursuant to E.O. 13526

REF ID:A58489

WARNING

Authority for release of this document to a foreign government must be secured from the Assistant Chief of Staff, G–2.

When this document is released to a foreign government, it is released subject to the following conditions: This information is furnished with the understanding that it will not be released to another nation without specific approval of the United States of America, Department of the Army; that it will not be used for other than military purposes; that individual or corporation rights originating in the information whether patented or not will be respected; and that the information will be afforded substantially the same degree of security as afforded by the United States of America, Department of the Army.

REF ID:A58489

TM 32–250—AFM 100–80

FUNDAMENTALS OF TRAFFIC ANALYSIS (RADIO-TELEGRAPH)

RESTRICTED. ***DISSEMINATION OF RESTRICTED MATTER.***—**No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also AR 380–5.)**

United States Government Printing Office
Washington; 1948

REF ID:A58489

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
Washington 25, D C, 1 October 1948

TM 32-250—AFM 100-80, Fundamentals of Traffic Analysis (Radio Telegraph) is published for the information and guidance of all concerned

[AG 300.7 (9 Jun 48)]

BY ORDER OF THE SECRETARIES OF THE ARMY AND THE AIR FORCE

OFFICIAL
EDWARD F WITSELL
Major General
The Adjutant General

OMAR N BRADLEY
Chief of Staff, United States Army

OFFICIAL
L L JUDGE
Colonel, USAF
Air Adjutant General

HOYT S VANDENBERG
Chief of Staff, United States Air Force

DISTRIBUTION

Army

GSUSA (1), Arm & Sv Bd (2), AFF (15), OS Maj Comd (5), Base Comd (2), MDW (16), A (ZI) (30), (Overseas) (15), CHQ (5), D (3), USMA (20), Sch (10) except Ground Gen and 11 (25), ROTC (1), T/O & E 32-952 (20), 32-1027 (20)

Air Force

USAF (10), USAF Maj Comds (5), USAF Sub Comds (3), Div (Air) (2)

For explanation of distribution formula, see TM 38-405

REF ID:A58489

CONTENTS

		Paragraphs	Page
CHAPTER 1.	**INTRODUCTION.**		
Section I	General	1–5	1
II	General Approach	6–7	4
CHAPTER 2.	**RADIO OPERATIONS.**		
Section I	Introduction	8–9	6
II	Operating Data	10–15	7
III	Elements of Radio Procedure	16–20	28
IV	The Message Externals	21–29	34
V	Textual Features	30–36	40
VI	Collateral Material	37–40	42
CHAPTER 3.	**RECONSTRUCTION OF THE RADIO NETWORK.**		
Section I	Introduction	41–43	45
II	Analysis of Radio Operations	44–52	45
III	Net Reconstruction	53–59	73
IV	Methodology of Analysis	60–62	86
CHAPTER 4.	**APPLICATIONS OF TRAFFIC ANALYSIS.**		
Section I	Intercept Operations	63–69	90
II	Applications to Cryptanalysis	70–74	94
III	Applications to Intelligence	75–79	98
APPENDIX.	**REFERENCES**		102

REF ID:A58489

CHAPTER 1

INTRODUCTION

Section I. GENERAL

1. Purpose

The purpose of this manual is to present a standard approach to traffic analysis problems of the military type in order to furnish signal intelligence personnel with a knowledge of traffic analysis techniques, capabilities, and applications. It is to be recognized that no text on analytic techniques can be definitive because techniques are subject to continual improvement and change in order to meet changing problems. This text is intended merely as a guide. Specific application is dependent on the ability and ingenuity of the analyst.

2. Scope

This manual is concerned only with traffic analysis of military radio communications, but the techniques covered will also be found of value in the analysis of other kinds of communication networks. Discussion of other means of communication, such as wire or cable, has not been included; in the reconstruction of the radio communication system it should be remembered that often these other means will account for missing portions of the system. Further, the scope is limited to the study of Morse transmissions. Non-Morse transmissions, such as radio-teletype and radio-telephone, are not discussed. The differences, however, are largely technical and procedural and involve the material transmitted only to a limited extent. It is thought, therefore, that this text will serve as a basis for all traffic analysis and that, with some minor modification, the methodology described will be found applicable to all types of transmission.

REF ID:A58489

3. References

A general knowledge of radio theory, Morse code, and radio procedure is assumed. For reference purposes the field and technical manuals listed in the appendix will be found useful.

4. Definition of Traffic Analysis

Traffic analysis is that branch of signal intelligence analysis which deals with the study of the external characteristics of signal communications and related materials for the purpose of obtaining information concerning the organization and operation of a communication system. This information is used (1) as a guide to efficient intercept operation, (2) as an aid to cryptanalysis, and (3) as a basis for drawing deductions and inferences of value as intelligence even in the absence of specific knowledge of the contents of the message.

5. Objectives

To achieve planned and coordinated action, it is necessary for the components of a military force to communicate with each other from the highest headquarters through all intermediary channels to the individual man in the field or the airplane in the air. Much of this communication, for reason of speed and efficiency, is conducted by radio, and radio is vulnerable to intercept. Therefore, disguises are devised to conceal both the traffic passed and the structure of the communication network. Traffic is disguised through the employment of codes and ciphers, and it is the task of cryptanalysis to solve these codes and ciphers. The communications net work is disguised through the use of a number of techniques which relate, for example, to the use of call signs and frequencies, the method of routing messages, and the use of secret procedure signs. These techniques, the means for attacking them, and the resulting reconstruction of the network are the study of traffic analysis. The responsibility of the traffic analyst, however, does not stop with the reconstruction of the communication network. It is also part of his mission to discover practical applications for his knowledge in the associated fields of intercept, cryptanalysis, intelligence, and security. The objectives of traffic analysis, then, fall into two main groups:

a. The acquisition of a detailed knowledge and a complete understanding of a communications network. This involves the reconstruction of the nets, the determination of the features of their operation, the solution of call sign and routing systems, analysis of the components of the message externals, the interpretation of radio procedure, and the use of the various cryptographic systems passed; in

REF ID:A58489

other words, everything about communications except the actual cryptanalysis of the text.

b. The application of this knowledge to—

(1) *Intercept operations.* Traffic analysis contributes to three aspects of the intercept problem. First, by providing the intercept station with certain necessary information, such as call sign and frequency lists, target locations, schedules, etc., it assists the station in the accomplishment of its mission and encourages the best possible results. Second, in coordination with cryptanalytic and intelligence interests, it determines the priorities governing the interception of individual circuits. Third, through a study of intercept, it checks the performance of the station in relation to its mission.

(2) *Cryptanalysis.* Aid to cryptanalysis is furnished in a great variety of ways, largely dependent on the cryptanalytic and traffic analytic peculiarities of the communications under study. *In most instances, traffic analysis and cryptanalysis become so interrelated that it is impossible to determine where one begins and the other leaves off, and it is necessary to set an arbitrary dividing line.* In general, however, assistance takes the following forms: the solution of the routing systems, where disguised, and the placing of the routings in the clear on traffic; the study of the uses of the various cryptographic systems; the reading of chatter for items of cryptanalytic interest; the discovery of crib, or stereotype, texts from message externals; the location of isolog messages; and the application of other traffic analysis data, such as message serial numbers, which may be of value in specific cryptanalytic problems.

(3) *Intelligence.* Military communications, including both the organization of the nets and the traffic passed, reflect the disposition of troops and the intentions for movements and operations. A careful analysis, therefore, of net structure, traffic contacts and patterns, traffic volumes, and similar signals features, assists in the building of the final intelligence picture. The exact techniques to be used are, again, dependent on the individual problem and involve the recruitment, training, organization, and order of battle of the military forces under study as well as characteristics of communications.

(4) *Security.* Because the traffic analyst becomes skilled in probing the weaknesses of communication systems, he is in an ideal position to assist in maintaining high standards of security within our own communication networks. This function of traffic analysis is mentioned merely in passing. It will not be discussed further in this text.

REF ID:A58489

Section II. GENERAL APPROACH

6. The Raw Material

The traffic analyst begins his study of a communications network with three types of raw (basic) data:

a. INTERCEPT DATA. This is the information supplied by the intercept operator. It consists of the frequencies to which he is listening, the times during which he hears signals, and occasional comments such as notes on the quality of the signal or the characteristics of the radio operator.

b. THE TRANSMISSION. The transmission is the sum total of everything sent by the radio operators. It includes the initial call-up, the exchange of call signs, the traffic, servicing, miscellaneous chatter, and signing off. Traffic may be divided into two parts: the message externals (preamble and postamble) and the text. The externals generally contain radio station and message center numbers of a variety of types, routing instructions, addresses, precedence indicators, and file times, all of value in traffic analysis. The text usually exhibits a number of cryptographic features in the clear which are likewise of use.

c. COLLATERAL INFORMATION. Besides the above material, there is a large amount of data which is available or which can be made available for traffic analysis purposes. Some of these are directly related to intercept, such as goniometric bearings. Other items are message decodes, captured documents, and intelligence reports.

7. The Analytic Approach

a. Traffic analysis is partly analytic, partly synthetic. Analysis is performed on each feature of the communications network and then, through exploiting the relationships between these features or within them, traffic analysis synthesizes them into a unified whole. In other words, the types of raw data noted in paragraph 6 are first analyzed until everything possible is known about each item independently, after which, though often seemingly unrelated, they can be pieced together to produce a complete picture of the radio nets. This means that the analyst must pay particular attention to detail and must carry much of this detail in his mind so that he can readily perceive the relationships between discrete items and integrate them to form the whole.

b. The actual approach to a traffic analysis problem is broadly determined by the stage of development of the problem. These stages of development are threefold, but it should be understood that what is represented are not clear-cut divisions in operation, but rather, gradual shiftings of emphasis as the problem matures.

REF ID:A58489

(1) *Initial attack.* (*a*) In the initial period, little is known about the problem and it may first be necessary to identify the radio nets and traffic involved so that they can be distinguished from all other types. When this has been accomplished, the characteristics are furnished to the intercept station which embarks on a large-scale search mission, scanning the entire range of frequencies for transmissions of the desired nature. During this time, it is the task of the traffic analyst to give direction to this mission and to evolve from it a definite assignment. It should be noted here that the search mission, in reduced scale, should always continue until the problem has ceased to exist, in order to cover new net developments.

(*b*) As soon as material begins to accumulate, an elementary study may be conducted on the elements of the transmission, particularly the message externals. The functions of the various preamble components should be observed, the method of routing noted, and in general, the significance of each component determined.

(2) *Development.* During the second period, emphasis is placed on the study of the communications system with a view to learning all its details of organization, operation, and procedure. There are usually two phases to this: the research phase, which involves thorough analysis of every item, such as call signs, procedure signs, message numbers, routing codes, and cryptographic features; and the actual net reconstruction, consisting of the building of the entire radio net complete with call signs, frequencies, schedules, and station locations.

(3) *Application.* When this knowledge has been gained, and even while it is being gained, it can be put to use in the three related fields of control, cryptanalysis, and intelligence. From the very first moment that traffic analysis is performed, it begins contributing to these phases of communications intelligence, but it is not until a substantial amount of information has been gathered that these applications receive full emphasis. The final goal of traffic analysis operations is the reconstruction of the complete radio network against its cryptographic and order of battle background, and the production on a day-to-day basis of items of cryptanalytic application and intelligence importance.

REF ID:A58489

CHAPTER 2

RADIO OPERATIONS

Section I. INTRODUCTION

8. Radio Operations

a. The operation of a radio network requires a set of fixed rules and regulations which define the manner and form of communications. These rules are in part subject to the laws of nature, in part to the necessities of communication itself, and in part to the whim and ingenuity of the personnel formulating them. The first two factors impose some degree of uniformity on radio networks, no matter what the type or nationality. This makes it possible to set down the basic features of communications, e.g., call signs, frequencies, message numbers, and routing instructions. However, the third factor acts to vary those features by determining the way that they are used. This chapter outlines what these basic features are and some of the ways in which they may be manipulated. It is, of course, not possible to include all the types which may be encountered, but it is hoped that what is given will serve to indicate the general patterns the traffic analyst is likely to meet in studying radio operations and will serve to set up general lines of traffic analysis thinking.

9. Phases of Radio Operations

Radio operations for purposes of study may be divided into four main phases:

a. Operating Data. The first considerations in the creation of a communication net relate to the structure or form of the net, the use of frequencies and call signs, and the system of schedules. These are the basic operating data of the net and involve its mechanical functioning. In the case of some nets, the military for instance, attempts are made to conceal these data; in other cases, such as commercial, they can be determined with little effort.

b. The Radio Transmission. Once the operating data have been determined, the next step is to devise the form and language of radio transmission. There must be regulations governing the Morse code to be used (largely dependent on the alphabet concerned), the pro-

REF ID:A58489

cedure signals which make for brevity and speed and which may be encoded for reasons of security, the order of elements in the transmission, the plain-language chatter of the radio operators, and the plain-language and simple cipher messages usually considered part of the traffic analysis task.

c. THE MESSAGE EXTERNALS. The message externals are actually a part of the radio transmission and belong under *b* above, but because of their importance a separate section (sec. IV, this ch.) is devoted to them. They include the preamble and postamble and generally contain serial numbers of various types, group check, file date and time, precedence indicators, and routing instructions.

d. TEXTUAL FEATURES. Some of the cryptographic aspects of the text are in the clear to make possible proper handling of the traffic by message center personnel and to permit decrypting. These features in the clear are often of great assistance to the traffic analyst. They may merely involve whether the text is in letters or numbers, or the length of the code groups, or they may be somewhat more complex as discriminants, indicators, or pad numbers.

Section II. OPERATING DATA

10. General

The operating data enable the network to function. They consist of the frequencies, call signs, and schedules used in communication. Traffic analysis is interested not only in the operating data as used by the network, but also in the general system on which the allocation of operating data to specific nets and radio stations is based. This section is devoted to a discussion of radio nets and of the ways in which the operating data are used and assigned.

11. Definitions

a. A radio network is composed of radio stations organized for the purpose of intercommunication. This organization is not haphazard but follows very definite and detailed patterns. These patterns are based on the order of battle since the lines of communication themselves must coincide with the echelon of command and the military requirements. Before it is possible to enter into a discussion of these patterns, however, it is necessary to define some of the terminology to be used.

(1) *Link:* Any system of telecommunication between two points.

(2) *Group:* One or more links whose stations work together as a communication entity under a common operating control.

REF ID:A58489

(3) *Net:* One group or a number of groups assembled on the basis of common operating characteristics, presumably under the administrative direction of an immediate common superior headquarters.

(4) *Network:* The radio system of a service of a nationality, as United States Army network, United States Naval network, United States Air Force network.

b. These definitions may appear somewhat obscure to the student for the moment, but it should be kept in mind that they are formulated from a traffic analysis point of view, that is, from the outside looking in. These terms must be so categorized in order to be of value analytically and, therefore, they represent the situation as it appears rather than as it actually is. Figure 1 will help to clarify these terms, and it is suggested that the student study the diagram from time to time as its understanding is essential to the proper approach to net reconstruction.

c. Figure 1 illustrates the general organization of the military network, proceeding from Department of the Army Headquarters through theater, army group, army, corps, and division. The equivalent Department of the Air Force organizations are shown in figure 2. (The following pertains equally to the Department of the Air Force.) Each line or connection represents a radio link within the terms of the definition in *a*(1) above—any telecommunication system between two points. It is to be emphasized that only *two* stations are involved in a link, never any more. Thus, the line from Department of the Army HQ to Theater "A" is a link; the line from Department of the Army HQ to Theater "B" is another; the line from 2d Corps to 1st Division is one; as is the connection from 1st Division to 2d Division. The links which form the triangle, 2d Corps, 1st Division, 2d Division, constitute a group; those forming the triangle, 2d Corps, 3d Division, 4th Division, constitute another. These links are placed in groups because they work together as a communication entity under a common operating control (the group control being at the highest headquarters of the group, here the 2d corps), yet do not, in themselves, comprise the complete net. The net is made up of the two groups together and is, in this instance, the 2d Corps net with the 2d Corps headquarters as net control. It should be observed that very often the link and the group may be the same thing, or the link, group, and net may be the same. Each definition of the larger unit enfolds the lesser. For example, the line from Department of the Army HQ to Theater "A" may be termed a link, for it is composed of only two stations, or a group because its stations work as a communication entity under the control of the Department of the Army station; the three links, or groups, however, running out from Department of the Army HQ form the Department of the Army net.

REF ID:A58489

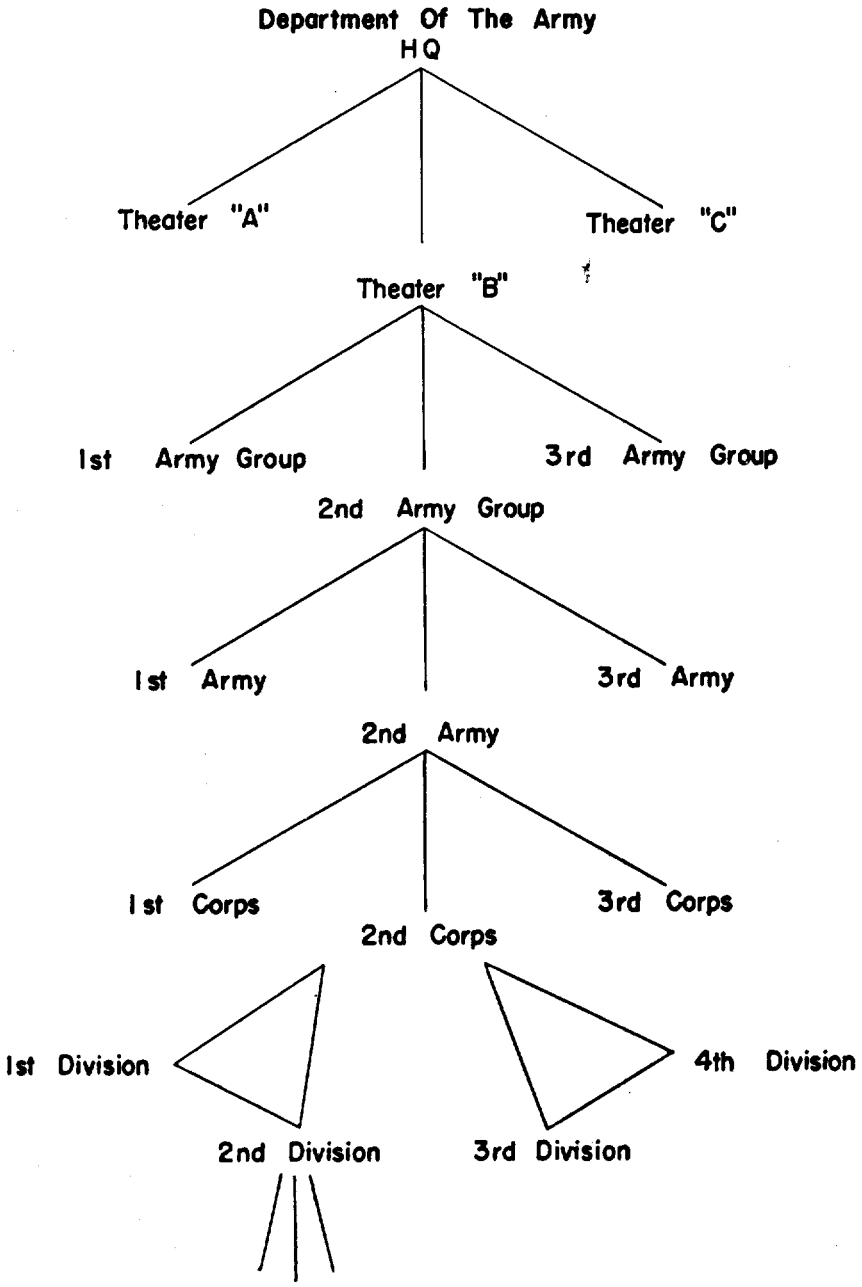


Figure 1. General organization of military network—United States Army.

REF ID:A58489

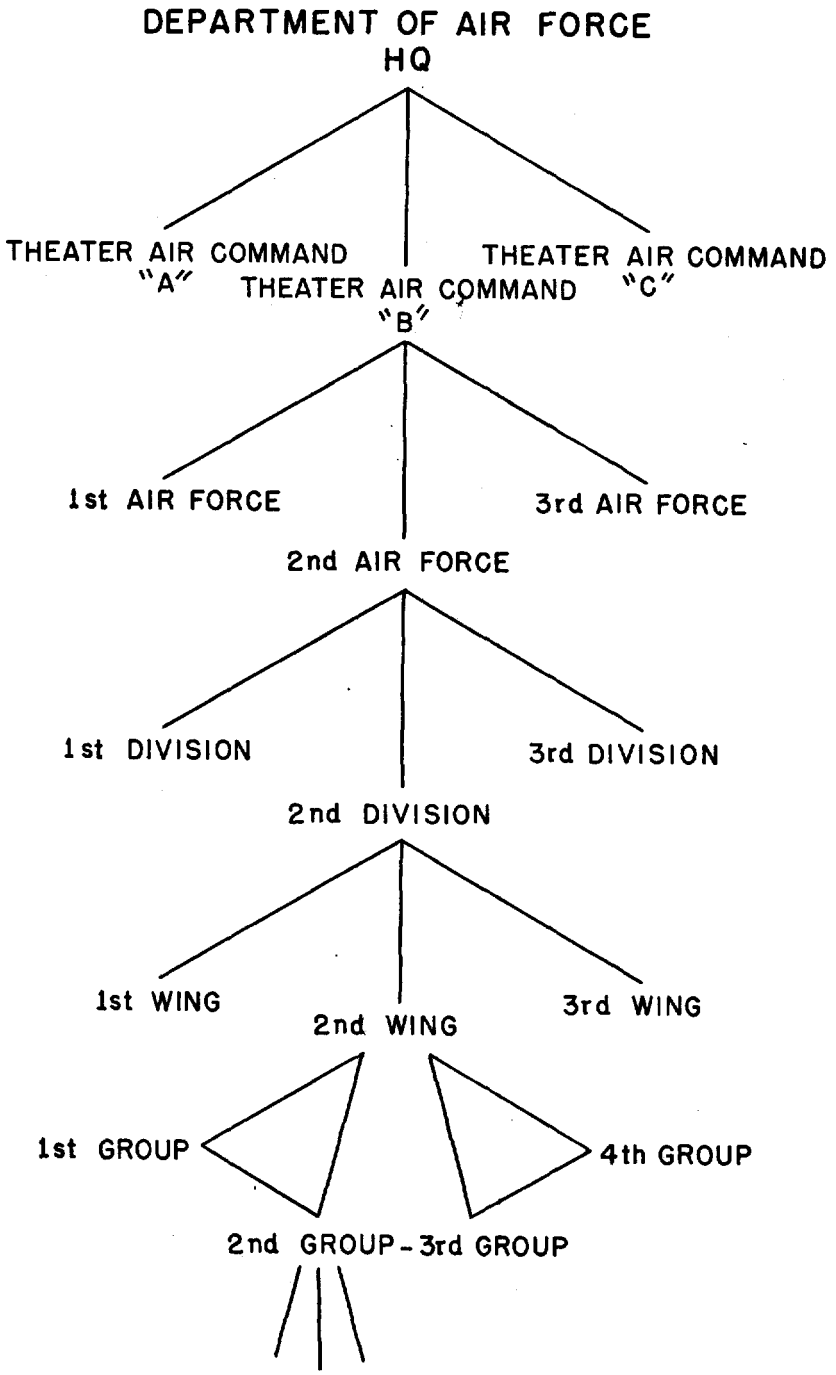


Figure 2. General organization of military network—United States Air Force.

REF ID:A58489

d. It will be recalled that, in discussing these definitions in *b* above, it was stated that they were formulated from an analytic point of view. This is particularly true of the definition of the net. In the reconstruction of the radio network, one of the first problems is the organizing of a number of radio links into groups and nets. In the case of the group, this is fairly simple to accomplish for the group is a communication entity, that is, all of its stations either work each other or have contact with a central operating control. The net, on the other hand, often does not exhibit such cohesive characteristics. A number of groups, apparently unrelated, may eventually fall into a single net when the order of battle is finally derived. There are two touchstones for the association of groups into nets:

(1) *Common operating characteristics.* Since the links and groups of the net all have a common superior headquarters, it may be assumed that certain rules of procedure and operation will be promulgated by this superior and that, therefore, all links and groups of the net will exhibit these in common.

(2) *Administrative direction of an immediate superior headquarters.* When the order of battle is known, it is often possible to associate groups and links through the knowledge that they are controlled by the same unit.

e. The net, the group, and the link, then, are merely units of organization in the radio network, just as armies are broken down into corps, divisions, regiments, companies, and platoons. Likewise, air forces are broken down into divisions, wings, groups, squadrons, and flights. And these nets, groups, and links may be characterized by the unit served and the function performed. For instance, figure 1 represents command channels so that there is a Department of the Army command net, a Theater "B" command net, a 2d Army Group command net, and so on. Radio, however, serves many other military functions than that of command. Military nets, for example, may be organized to contain an antiaircraft artillery group, an artillery air-ground group, an artillery observation group, a reconnaissance group, an air warning group, and others beside the command group.

12. Examples of Radio Nets

Figures 3 through 9 illustrate some of the type nets which may be encountered. These types will vary in individual instances; they serve, however, to indicate some of the possibilities.

REF ID:A58489

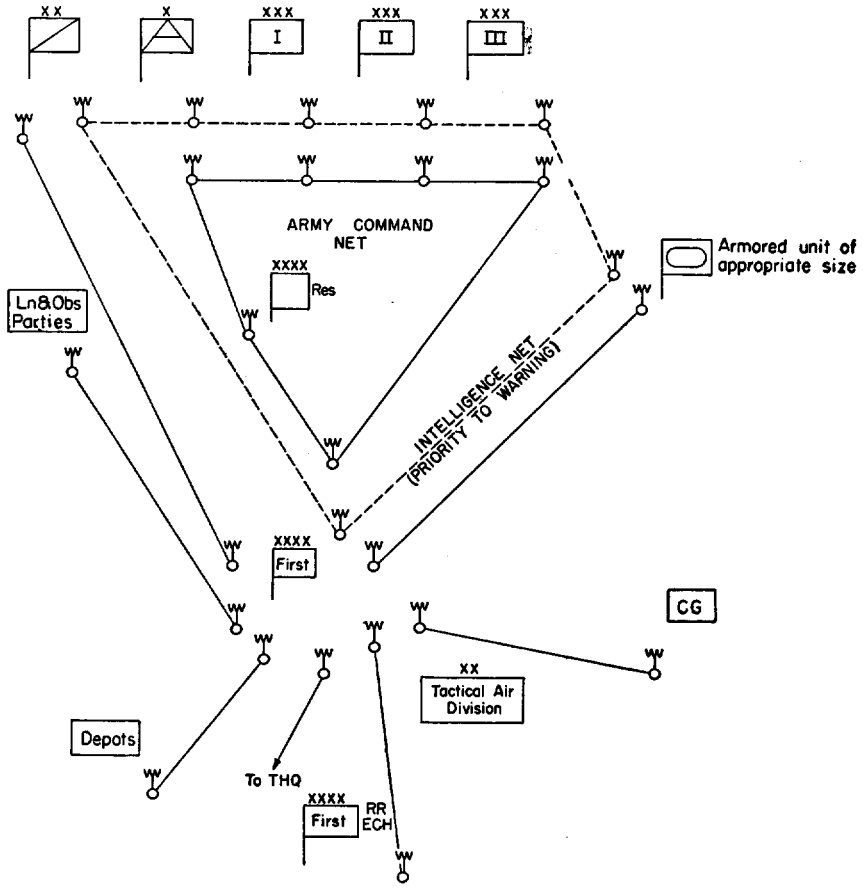


Figure 3. Type radio nets, Army.

REF ID:A58489

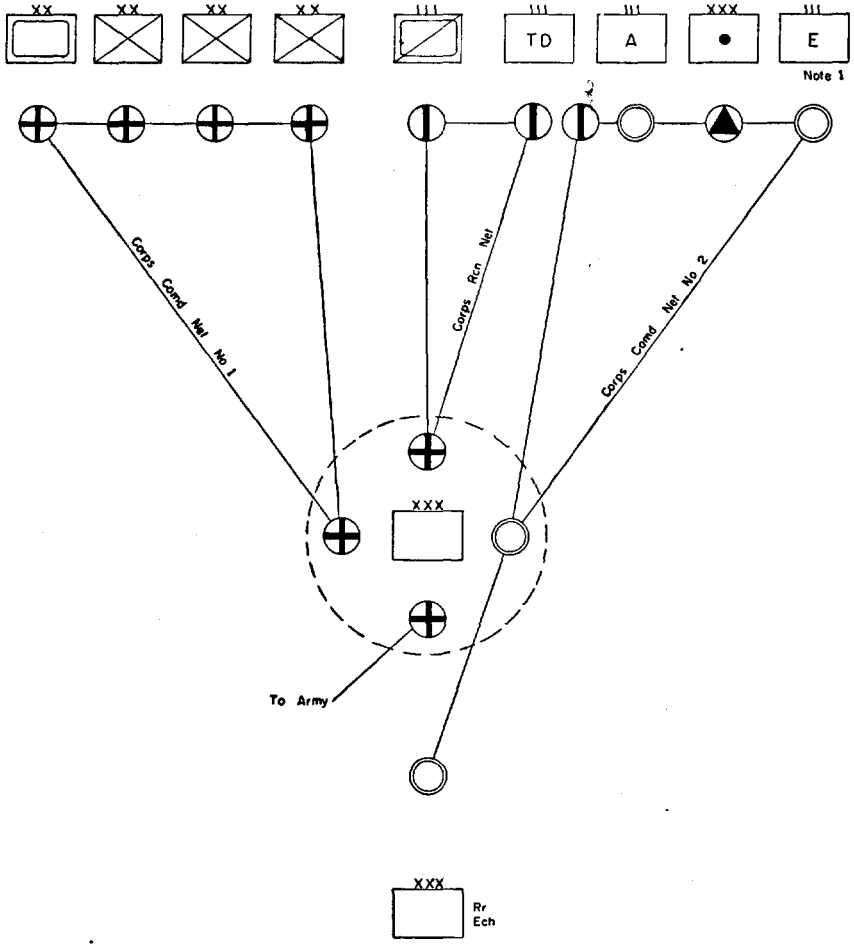


Figure 4. Type radio nets, corps.

REF ID: A684682

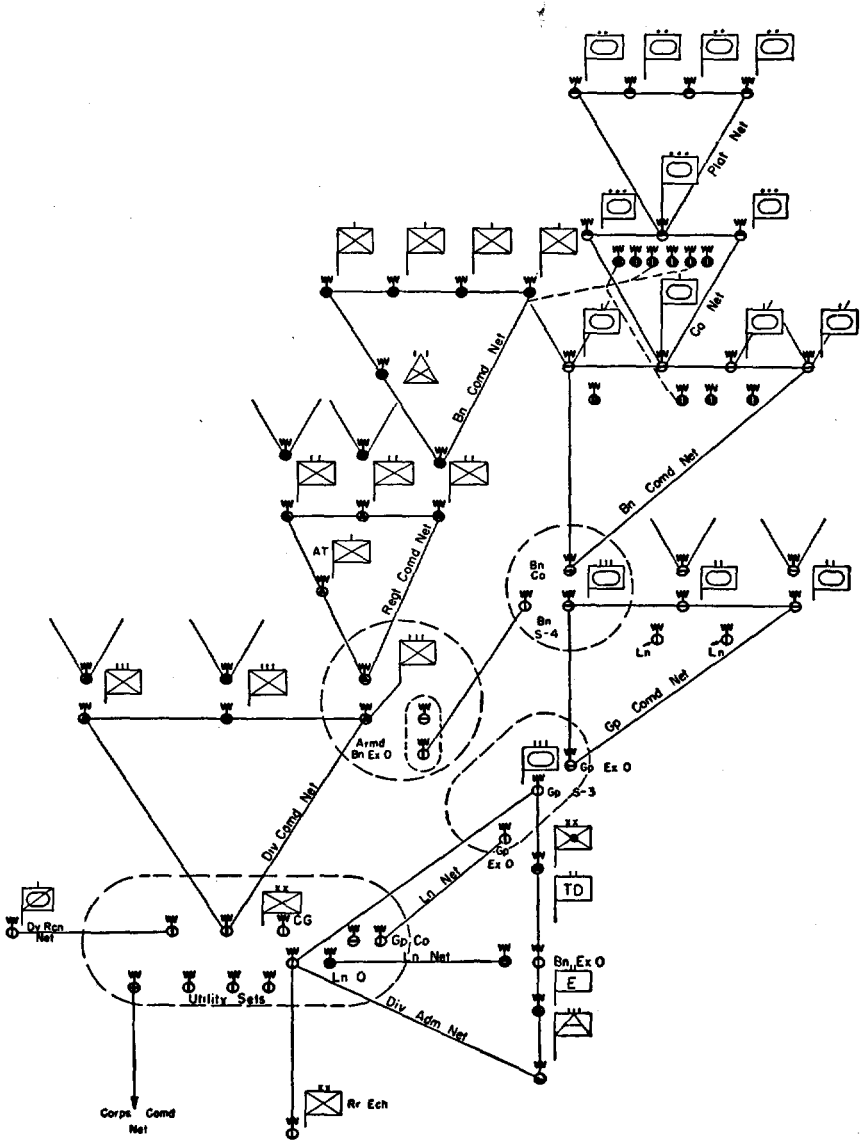


Figure 5. Type radio nets, infantry division, with attached units.

REF ID: A684682

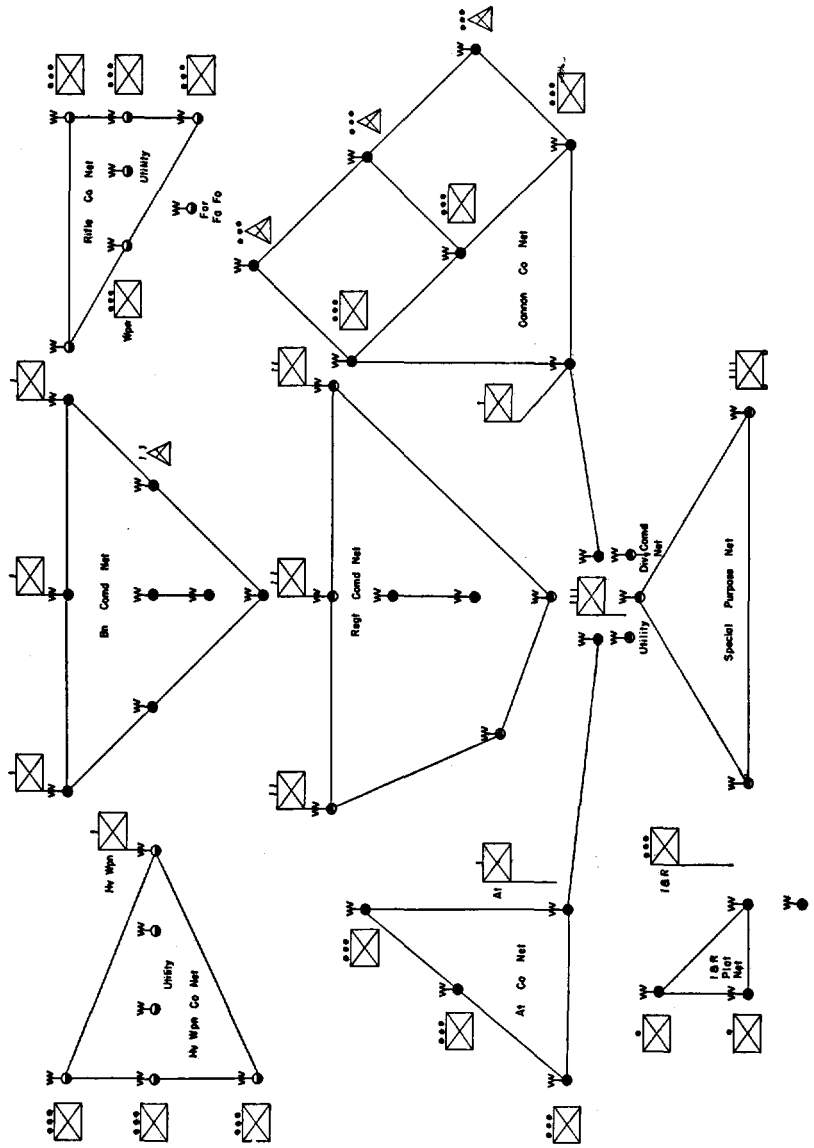


Figure 6. Various radio nets in an infantry regiment.

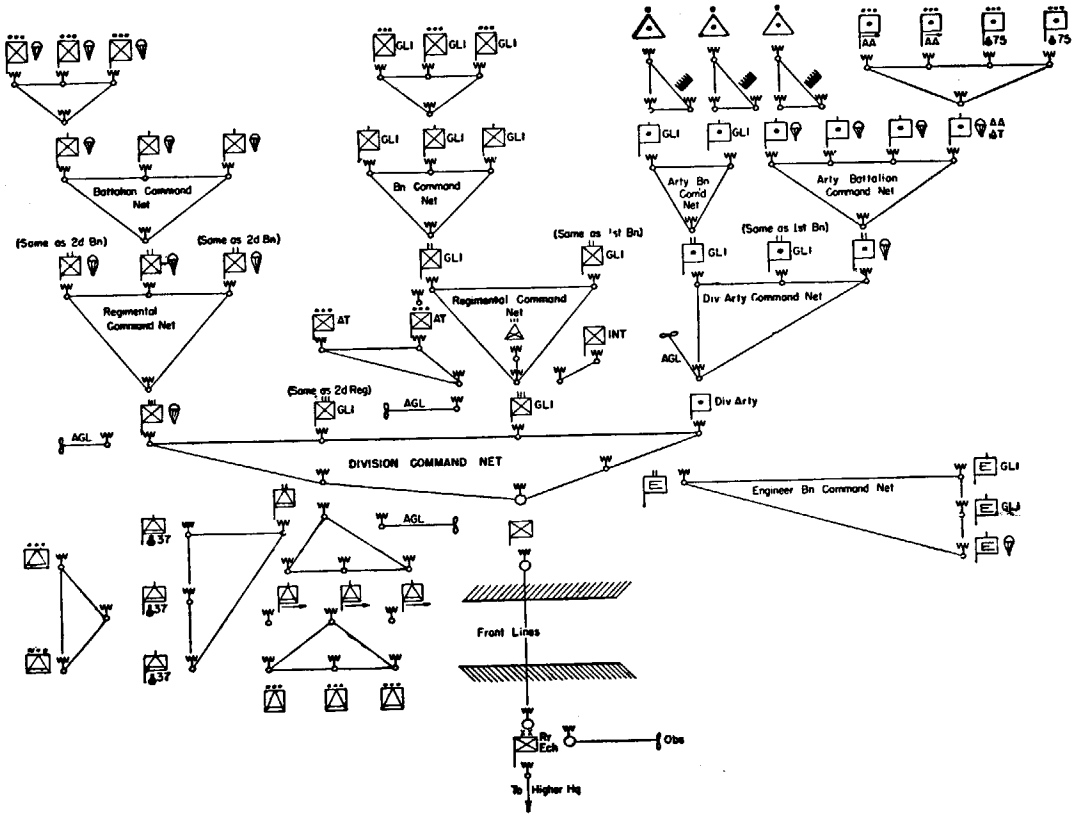


Figure 7. Type radio nets, airborne division.

REF ID:A584489

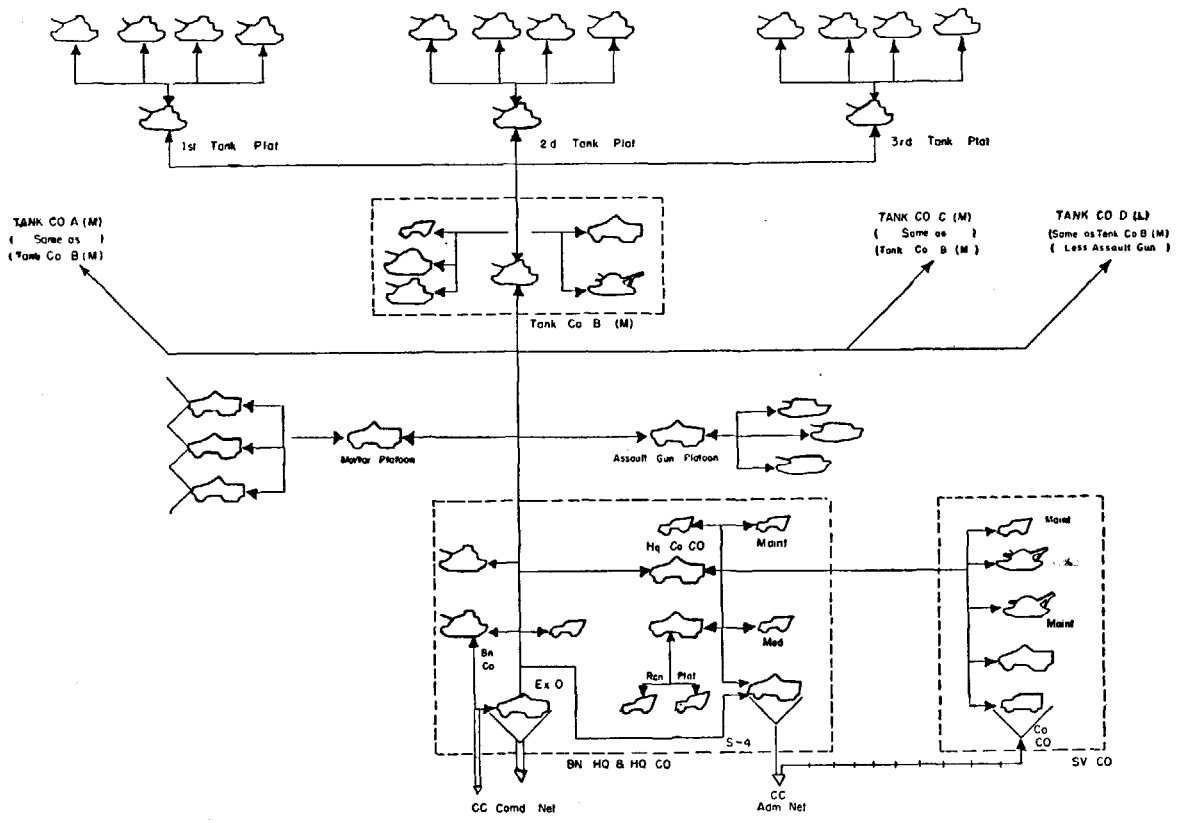


Figure 8. Type radio nets, tank battalion.

REF ID:A58489

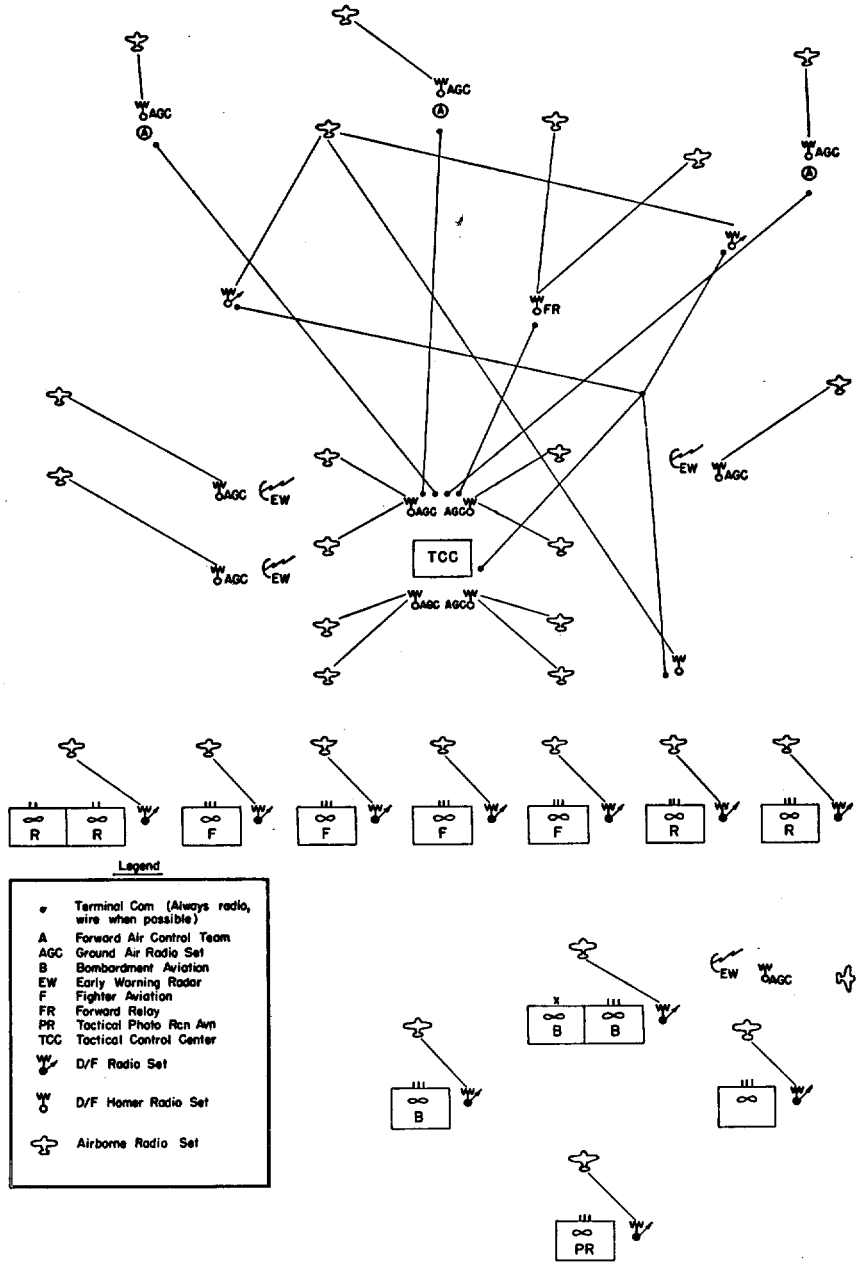


Figure 9. Tactical Air Force control channels.

REF ID:A58489

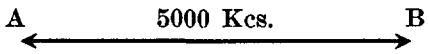
13. Frequencies

a. GENERAL. The analysis of the use of frequencies on a network may be divided into two parts:

(1) *Systems of use.* The system of use is concerned with the manner in which frequencies are employed on the net, i.e., whether the entire net uses one frequency, whether each station sends on an individual frequency, etc.

(2) *Systems of allocation.* The system of allocation is the method used to assign specific frequencies for communications so that different stations will not interfere with each other. It also involves the rotation of frequencies for security purposes.

b. SYSTEMS OF USE. (1) *Simplex:* Two stations intercommunicating on the same frequency.



(*a*) A sends to B on 5,000 Kcs.

(*b*) B sends to A on 5,000 Kcs.

(2) *Complex sending* (fig. 10): Two or more stations on different sending frequencies. A different frequency is assigned to each radio transmitter in the net, and each transmitter uses its assigned frequency to contact the other stations.

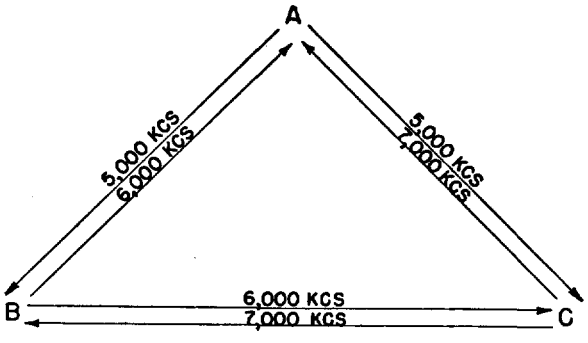


Figure 10.

(*a*) A sends to B and C on 5,000 Kcs.

(*b*) B sends to A and C on 6,000 Kcs.

(*c*) C sends to A and B on 7,000 Kcs.

(3) *Complex receiving* (fig. 11): Two or more stations on different receiving frequencies. A frequency is assigned to each station for receiving transmissions. All stations in the net when sending to a particular station will use the frequency assigned to the receiving station.

REF ID:A58489

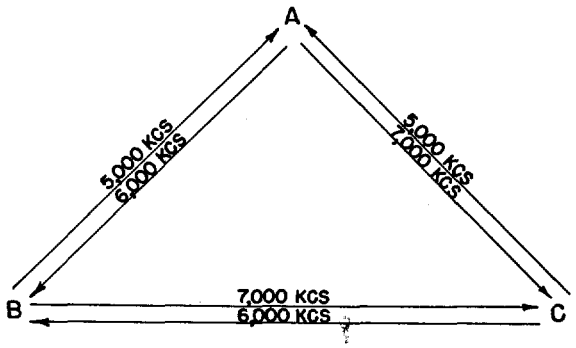


Figure 11.

(*a*) B and C send to A on 5,000 Kcs.

(*b*) A and C send to B on 6,000 Kcs.

(*c*) A and B send to C on 7,000 Kcs.

(4) *Star* (fig. 12): A number of stations on the same frequency with no normal lateral working. This is an extension of the simplex system, as the latter involves only two stations on the same frequency. In the star form, if one outstation wishes to contact another, it must obtain permission from control.

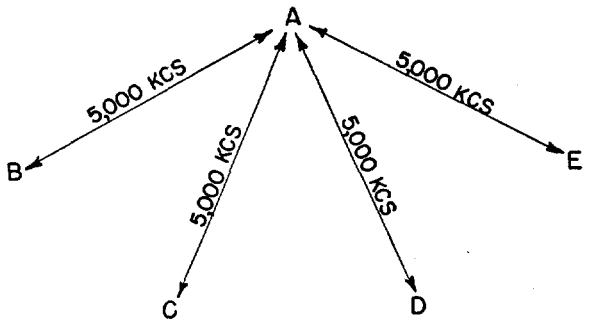


Figure 12.

(*a*) A sends to B, C, D, and E on 5,000 Kcs.

(*b*) B, C, D, and E send to A on 5,000 Kcs. B, C, D, and E may not intercommunicate without express authorization from A. Normally, messages between outstations will be relayed through A (control).

(5) *Star with lateral* (fig. 13): Number of stations on the same frequency with some lateral working. In many of the star nets, lateral working will be a regular procedure between some, but not all, of the outstations.

REF ID:A58489

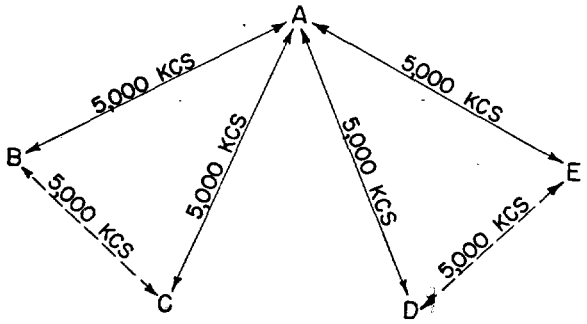


Figure 13.

(*a*) A sends to B, C, D, and E on 5,000 Kcs.
(*b*) B, C, D, and E send to A on 5,000 Kcs.
(*c*) B sends to C on 5,000 Kcs. and C to B on 5,000 Kcs.
(*d*) D sends to E on 5,000 Kcs. and E to D on 5,000 Kcs.

(6) *Free star* (fig. 14): Number of stations on the same frequency with free operation. One frequency is assigned to the entire net and any station in the net may contact any other on the assigned frequency.

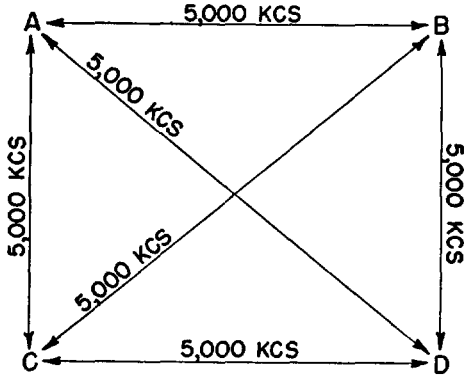


Figure 14.

(*a*) A sends to B, C, and D on 5,000 Kcs.
(*b*) B sends to A, C, and D on 5,000 Kcs.
(*c*) C sends to A, B, and D on 5,000 Kcs.
(*d*) D sends to A, B, and C on 5,000 Kcs.

(7) *Complex star* (fig. 15): Number of stations with control on one frequency, outstations on others. This is similar to the star in its form, but it uses several frequencies instead of only one. Often, a number of the outstations will operate on one frequency, others on another.

REF ID:A58489

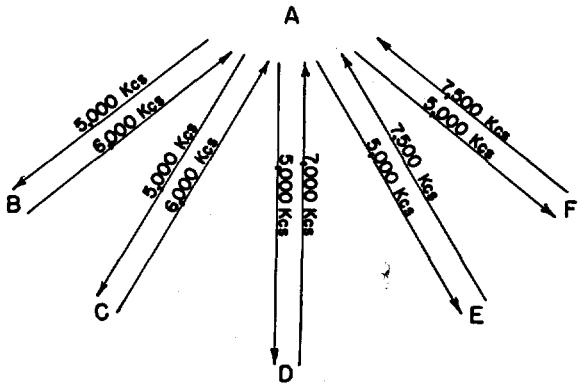


Figure 15.

(*a*) A sends to B, C, D, E, and F on 5,000 Kcs.
(*b*) B and C send to A on 6,000 Kcs.
(*c*) D sends to A on 7,000 Kcs.
(*d*) E and F send to A on 7,500 Kcs.

(8) *Broadcast* (fig. 16): A frequency is assigned to the broadcasting station. Usually no frequency is assigned to the outstations for reply.

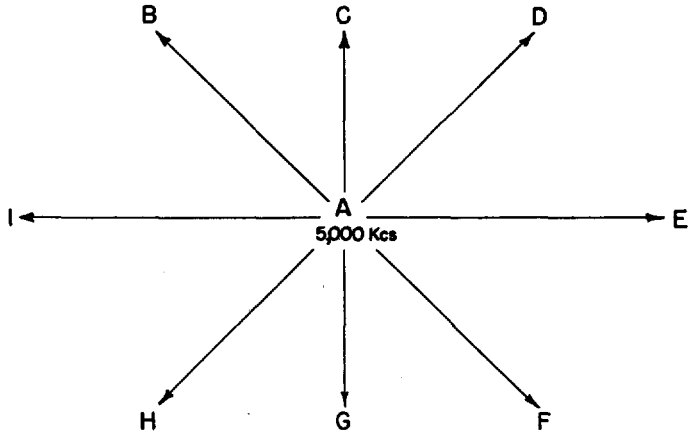


Figure 16.

(*a*) A sends to all stations simultaneously on 5,000 Kcs.

(*b*) Because a broadcast must be heard at so many scattered places, care must be taken in the selection of a frequency in order to choose one that will be heard by all stations. Sometimes, where this has not proved possible, double-keying is resorted to, i.e., the broadcasting station sends on two or more different frequencies at the

REF ID:A58489

same time. Outstations may receipt for traffic on regularly assigned frequencies in the net. In many such nets, however, no receipt is given.

c. SYSTEMS OF ALLOCATION. (1) *General.* Several factors enter into the selection of specific frequencies for use. These involve two basic considerations: readability (the ability of the receiving station to hear) and security. A number of miscellaneous factors, such as the type of power supply available, the nature of the transmitting and receiving equipment, and military and operational requirements, also affect the choice.

(2) *Readability.* The readability of a frequency is dependent on certain factors of wave propagation. These factors involve consideration of the distances between stations, ionospheric conditions, including night and day effects which usually make it necessary to allocate several frequencies to each radio station or net for night and day use, seasonal changes, and the type of terrain, e.g., water, high mountains, and jungle. Furthermore, the possibility of interference between transmitters on approximately the same frequency in the same area must be borne in mind and care taken to avoid such conflict. In any allotment of frequencies, therefore, central control must be established and an over-all plan of allocation devised.

(3) *Security.* One of the methods of attaining security against communications analysis is to hinder the act of intercept. This may be accomplished by changing frequency so that the intercept operator will be forced to "search" the entire frequency range for the desired transmissions. A second effect achieved by these changes is to increase the difficulty of identifying stations or units with frequencies. Maximum effectiveness is obtained by changing call signs along with the frequency. Plans for changes of frequency may operate in a patterned or random fashion, but in any event, such plans must take into consideration the factors noted under (2) above; thus these plans are usually rather detailed and complex.

(4) *Range of frequencies.* Frequencies may range from very low to ultra-high. The latter are not usable for long distance operation and find their chief applications in low echelon, air-ground, and plane to plane communication. Many of the applications of ultra-high frequency transmissions are still in the experimental stage. Low frequencies, such as 300 or 400 kilocycles, may be used for close field contact or air-ground and plane to plane nets. However, the major portion of military transmissions presently falls between 1,500 and 20,000 kcs. In passing, mention should also be made of the use of frequency modulation. FM has found its main application in tank, air, and small combat units where distances are not great and a minimum of noise level is desired for reception.

(5) *Secret frequencies.* As a countermeasure to possible jamming

RET ID: A584489

operations, some nets are provided with secret reserve frequencies These frequencies are not employed except in the case of jamming of the usual frequencies and circumstances demand that communication be kept open The secret frequency, of course, only remains secret for as long as it takes intercept to scan the bands and pick it up, but this interval may be sufficient to complete the transmission

(6) *Example of allocation of frequencies* The following chart illustrates a system which might be used for the allocation and rotation of frequencies

	Jan	*Feb*	*Mar*	*Apr*	*May*	*Jun*	*Jul*	*Aug*		*Dec*
A	1955	2035	2150	1910						
	2035	2150	1910	2305						
	2150	1910	2305	2070						
B	1910	2305	2070	2190						
	2305	2070	2190	2210						
	2070	2190	2210	1940						
C	2190	2210	1940	2350						
	2210	1940	2350	1925						
	1940	2350	1925	2240						
D	2350	1925	2240	1955						
	1925	2240	1955	2035						
	2240	1955	2035							

The months are listed across the top of the chart The squares are divided into three portions representing ten day periods within each month, 1–10, 11–20, 21–31 Each station of the net is assigned a letter and finds its frequency for each period in the square opposite the letter The frequencies which have been selected on the basis of their operational characteristics can be inscribed in the squares at random, in this instance, they are moved up one each month For example, on 1–10 January, A uses 1955 kilocycles, B, 1910 kilocycles, C, 2190 kilocycles On 11–20 January, A uses 2035 kilocycles, B, 2305 kilocycles, C, 2210 kilocycles

14. Call Signs

a General Call signs are actually names for the correspondents in a radio net They are usually composed of letters, numbers, or combinations of both and serve as a convenient means of identification The analysis of call signs falls into the same categories as does the study of frequencies systems of use, and systems of allocation

b Systems of Use (1) *Single station call* One call only is nor-

REF ID:A58489

mally used by the calling station This call may be either the sending station's or the receiving station's call

1 (ABC) _____ 2 (DEF)

Call up	1 to 2	DEF DEF DEF
	2 to 1	DEF DEF DEF
	or	
	1 to 2	DEF DEF DEF
	2 to 1	ABC ABC ABC

Note in this last instance that only one call was used by the calling station This makes the procedure single call even though the reply used a second call

(2) *Double-station call* Both the sending station s and the receiving station's calls are normally used by the calling station

1 (ABC) _____ 2 (DEF)

Call-up	1 to 2	DEF DEF DEF de ABC ABC ABC
	2 to 1	ABC ABC ABC de DEF DEF DEF

(3) *Link call* (fig 17) A common call sign is used for intercommunications between two stations Unlike the previous two types, here the call sign does not belong to an individual station but to a link

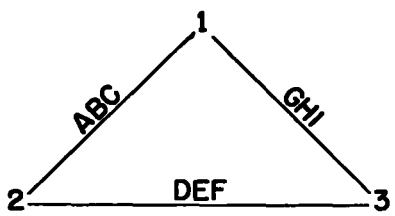


Figure 17

Call up	1 to 2	ABC ABC ABC
	2 to 1	ABC ABC ABC
	1 to 3	GHI GHI GHI
	3 to 1	GHI GHI GHI

(4) *Collective call* In addition to one of the above assignments, a collective call may also be allocated This call is used to alert all stations in the net preparatory to the transmission of broadcast traffic There are also some nets which are maintained only for broadcast purposes and this type of call is usually assigned to such groups The use of "CQ" may be classified under this heading

(5) *Split call working* Usually a single call is assigned to a transmitter or receiver position or to a link However, the use of separate calls for each frequency, one for day, one for night, is also valid This variation may be applied to any of the systems enumer-

REF ID: A684682

ated above and is known as split call working. It has the advantage of dissociating the night and day frequencies, but requires the use of twice as many calls.

(6) *Secondary calls.* In some systems of communication a secondary call is employed in conjunction with link call procedure. These secondary calls are of the station call type and serve as a more definite identification of each station than is supplied by the link call.

(7) *Authenticators.* In order to prevent outside stations from entering a net and confusing its operations, authenticators are sometimes used. They generally consist of a word or a combination of letters and/or digits to which there is a secret, prearranged reply.

c. SYSTEMS OF ALLOCATION. (1) *Composition.* Call signs may be composed of any combination of letters and/or numbers. Usually they are kept as brief as possible and the general range is from 2 to 5 characters. Calls may be composed at random or in some methodical fashion, such as the use of sliding alphabets. An example is included in *d* (2) below.

(2) *Methods of assignment.* Since calls are used as identifying marks, it is necessary to assign them so that two stations operating in proximity or in the same net do not have the same call. Otherwise, confusion would result on call-ups and the passage of traffic hindered. This necessitates some form of over-all control of call sign allocation. This control may be of a very tight nature in which every call is allotted from headquarters down to the smallest unit, or it may be rather loose with considerable discretion left to major subordinate groups whose commands are sufficiently separated geographically to prevent the possibility of confusion. A second consideration in the assignment of calls involves the problem of security since calls are identifications and thereby, if unchanged, furnish continuities for intercept and analysis. Most systems, therefore, cover not only the allotment of calls, but also provisions for change or rotation. These changes may be made daily, weekly, monthly, or at any other interval thought desirable. Calls which change frequently are called "changing calls", those which remain constant for some length of time, are called "fixed".

d. In general, call-sign systems may be divided into two basic groups:

(1) *Book systems.* These systems are founded on a call-sign book from which all calls are taken. These books will usually contain thousands of call signs and some method is provided for the allocation of calls from the book to individual radio stations. The recovery of these books often requires traffic intercept for a period of a year or more.

(2) *Cipher systems.* Call signs may be generated by the use of simple cipher devices such as sliding alphabets and square tables.

REF ID:A58489

The number of call signs available through such systems is usually limited and the method of assigning the call signs to individual radio stations is often bound up with the method for generating the calls. Figure 18 illustrates the use of a cipher system for the allocation and rotation of calls.

1	B	M	A	K	D
2	R	W	C	T	I
3	Z	G	N	O	U
4	H	L	S	X	E
5	V	J	P	F	Y

Figure 18.

The square is filled in random fashion. Station 1 begins with the letter "B" and takes off its calls in diagonal fashion, moving over one diagonal each day. At the end of each line, it drops down one line. Station 2 begins with "R", 3 with "Z", etc. Every 25 days, the calls repeat.

	Station No. ( )				
Date	1	2	3	4	5
1	BWN	RGS	ZLP	HJA	VMC
2	MCO	WNX	GSF	LPK	JAT
3	ATU	COE	NXY	SFD	PKI
4	KIZ	TUH	OEV	XYB	FDR
5	DRG	IZL	UHJ	EVM	YBW
6	RGS	ZLP	HJA	VMC	BWN
7	WNX	GSF	LPK	JAT	MCO
to					
25					

15. Times of Communication

a. GENERAL. An integral part of the operating data of the net is the setting of the times for communication. There are two main systems for accomplishing this: Unrestricted signaling and restricted signaling.

b. UNRESTRICTED SIGNALING. Under the system of unrestricted signaling, the stations of a net are free to contact each other at any time they choose. This method may be implemented either by the stations setting the time for the next schedule at the close of the

REF ID:A58489

previous one or by "alert" operating. In alert operating, which finds its greatest use in tactical and warning nets, all stations are always tuned to receive on certain assigned frequencies.

c. RESTRICTED SIGNALING. Restricted signaling limits the time at which contacts may be made between two radio stations. It is divided into two types: period signaling and priority signaling.

(1) *Period signaling.* The times of communication are assigned by definite schedule and contacts are made only at those specific times.

(2) *Priority signaling.* Priority signaling sets down a definite order in which the stations of a net will send traffic. It differs from unrestricted signaling in that one station may not call another at any time; and from period signaling in that no particular time is set aside for one station to call another. An example of priority signaling is shown in figure 19.

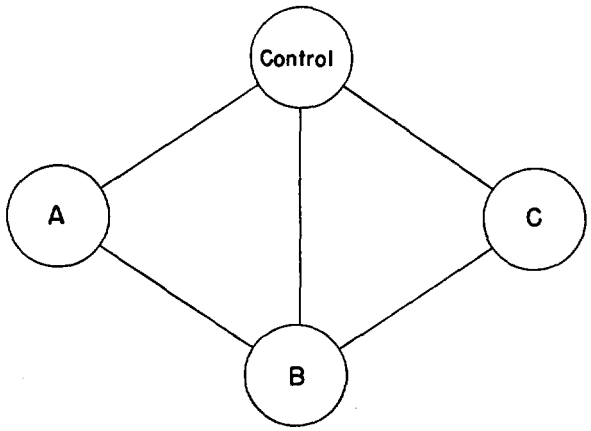


Figure 19.

In this net, "control" is permitted to send first, then stations A, B, and C in order. Schedules may be set up for the hours at which "control" comes on the air.

Section III. ELEMENTS OF RADIO PROCEDURE

16. Morse Code

Morse code is a system of dots and dashes used to transmit letters and numbers by electrical means. In the case of the English alphabet the Morse code is standardized by international convention, is used the world over, and is known as International Morse. In the instance of some nations whose alphabets differ from the English, however, special combinations of dots and dashes have been devised. For

REF ID:A58489

example, in German Morse, the German letters which correspond to the English follow the International, but the umlauted letters and "ch", for which there are no equivalents, are designated by new combinations:

A .—.—
O ———.
U ..——
CH ————

Morse code may be transmitted automatically or manually. In lower-echelon communications, the latter is usually employed, in the higher echelons sending is often automatic. Automatic transmission permits of speeds as high as 400 or 500 words per minute, though generally it averages somewhere between 75 and 200. Manual sending of coded traffic rarely rises above 35 words per minute. Atmospheric conditions, operator abilities, equipment, and similar items are, of course, limiting factors.

17. Procedure Signals

a. In order to facilitate conversation between radio operators, certain signals and signs have been composed. The most common sets of such signals used internationally, are made up of three-letter combinations beginning with "Q" or "Z", and are called "Q Signals" and "Z Signals". The use of these signals saves considerable time and simplifies transmission. Examples are—

QSV Send V's.
QRN I am troubled by atmospherics.
QSA? What is my signal strength?
QSA 4 Your signal strength is 4.

b. Beside these signals, there are a number of standard signs called prosigns which are likewise considered part of international procedure. Some of these are—

AA all after
R received
K go ahead

c. Another type of standard signal is the International Service Code. These signals are made up of five letters in pronounceable form:

UPBAG—for your information

d. Since much information may be derived from a study of chatter, military nets often make up sets of secret procedure signals and, in some cases, may encipher these signals on a periodic basis. For instance, the standard Q signal list may be used, but the last two letters of the signal enciphered by means of a daily changing alphabet.

899152 O - 50 - 5

REF ID:A58489

18. Elements of the Transmission

a. GENERAL. Just as a definite procedure is followed in making a telephone call, so in the normal radio transmission there is also a more or less fixed procedure which covers the basic elements involved. These elements are—

(1) *The call-up.* This embodies the rules of procedure by which one station makes contact with another and prepares for the transmissions of traffic.

(2) *The order of traffic.* After contact has been established, it is necessary to determine which station is to send traffic first.

(3) *Transmission of traffic.* The traffic is transmitted according to a prescribed form.

(4) *Receipting for traffic.* The receiving station acknowledges receipt of the message.

(5) *Corrections and services.* Messages are frequently garbled because of reception difficulties or operators' errors. Thus methods are provided for the efficient and speedy correction of these garbles.

(6) *Signing off.* At the conclusion of the schedule, the two stations follow certain procedures in signing off.

b. If allowance is made for differences in language and procedure signs and signals, it will be found that the above elements are generally standard for most communication systems. The detail, however, may vary somewhat between countries and also within the military of any one country. For instance, different units may observe different rules relative to the transmission of the call or the method of servicing. This often stems from individual requirements arising from strategic or tactical situations, e.g., an air unit as against an infantry unit. Furthermore, the echelon will also alter procedures. The lower echelons will usually abbreviate their procedures as much as possible because of the necessities of time and because they do not require all the data and detail that higher echelons do. Similarly, transmissions on low-echelon nets are liable to be confusing since a number of stations are often on the air at the same time and on approximately the same frequency.

c. THE CALL-UP. The calling station usually comes on the air with a series of V's sent for tuning purposes and the appropriate calls. The calls are generally sent three times, though this number may vary. The called station replies with a series of V's and calls. If the contact between the two stations is quickly made, readability reports are exchanged. Should these reports be unsatisfactory, transmitters and receivers will be adjusted, frequencies changed, etc., until signals are readable. If contact cannot be made, the calling station may hold its traffic for a later schedule, relay it through a third station, or send it blind. In sending blind, messages are generally

REF ID:A58489

transmitted twice and at a slow speed in the hope that the called station can hear although it cannot be heard.

d. THE ORDER OF TRAFFIC. Once contact has been successfully established, it becomes necessary to determine who will send traffic first. Various methods are employed. It may be ordered, for example, that the station of higher echelon send first, or that the calling station have this privilege, or that the highest priority traffic be cleared before all else regardless of which station is involved. One-for-one procedure may be used; i.e., the calling station is permitted one message, then the called station sends one, thus alternating back and forth until one of the stations has cleared all its traffic. Duplex working may be employed when the stations have the available operators and equipment and there is a large amount of traffic to be passed by both. Four operators are required in this type of working. For example, in figure 20, Operator No. 1 at station A sends

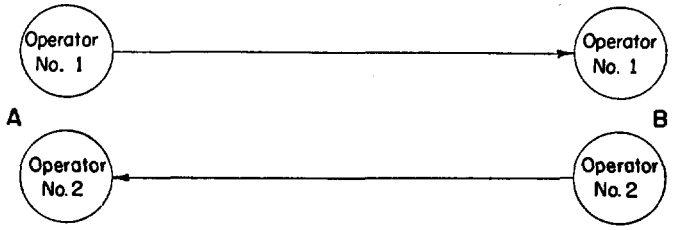


Figure 20

to Operator No. 1 at station B, at the same time that Operator No. 2 at B is sending to No. 2 at A. The chief difficulty with this sort of sending arises when No. 1 at B requires a service on a message from A. Since No. 1 at B is then using the frequency channel of the station, No. 2 at B must stop his transmission.

e. THE TRANSMISSION OF TRAFFIC. Traffic is usually preceded by a commence signal indicating that a message is about to be sent. The traffic itself is composed of the message externals and the text. The message externals contain such items as message numbers, file date and time, group count, addresses, routing instructions, precedences, and similar data. These externals may either precede or follow the text (preamble and postamble) or may be split between the two locations. Most commonly, however, these data appear in the preamble position. The text may be transmitted in code groups of letters, numbers, or both, or in plain text. In the case of coded traffic there are often signals indicating the end of a line and page of text as a check for the receiving operator. Signals usually appear preceding and following the text, the former separating the preamble from the text, the latter indicating the end of the message.

f. RECEIPTING FOR TRAFFIC. After the transmission of a message,

REF ID:A58489

the sending operator waits for a receipt from the receiving operator. This is generally rendered as simply "R". There are also procedures for provisional receipts and other special forms. In some cases, time of receipt may be given following the receipt sign.

g. Corrections and Services. A variety of methods are employed for the servicing of traffic depending on the nature and magnitude of the difficulty. A missed digit, for instance, may be serviced immediately; on the other hand, if a group were omitted this would not be known until the conclusion of the message and might be serviced at that time or might be held until all traffic has been sent. This latter procedure is fairly common, since it is convenient to transmit all traffic without interruption and then to take care of all necessary servicing. Some methods of servicing follow:

(1) *Break-in procedure.* When reception between two stations is good, "break-in" procedure may be used for quick servicing. It is useful only for minor corrections such as garbles caused by a moment of static, is very fast, and calls for alert operating.

A.	6403	3661	9626 - - -	
B.	2			B sends "2" as it is the last number he received correctly.
A.	26	8139	5560	A picks it up from 2.
or:				
A.	6403	3661	9826 - - -	
B.	(Merely depresses his key)			
A.	9826	8139	5560	A re-sends the last group and continues.

(2) *Correction of error (U. S. Army procedure).*

A.	QXTU SRV SRWP TSTL	EEEEEEEE	Actually eight or more dots indicating that "V" is in error.

(3) *Repetitions (U. S. Army procedure):*

A.	IMI	3–6 to 8 K	Repeat groups 3 and 6 to 8 of last message.
B.	3–LAJY–6 to 8– MUCU KAWC GUXO K		

(4) *Verifications and corrections (U. S. Army procedure).*

A.	J 271545 Z	3–6 to 8 K	Verify and repeat groups 3 and 6 to 8 of message filed at 271545 Z.
B.	C 271545 Z 3–LAJY– 6 to 8–MUCU KAWC GUXO K		

(5) *RQ's and BQ's.* Services which are more complex than the types noted above are usually sent as short messages. A request for

REF ID:A58489

service in international procedure is preceded by the sign "RQ", the reply by "BQ". Services which relate to cryptographic features, however, are generally sent as regular encrypted messages.

h. SIGNING OFF. When there is no further traffic to be transmitted, or at the end of the schedule time, the two stations will sign off. Usually, each station sends the "I have no more traffic" signal and then the "sign-off" signal. In many nets, the time of the next schedule is included just prior to the sign-off. These times may be enciphered for security purposes. Stations in lower-echelon nets will often sign off in order. An example from U. S. Army procedure follows:

A.	2SN	V	6F2	QNW	K	"2SN" is net call. QNW is the "close down" signal.
B.	6F2	V	G94	R	AR	
C.	6F2	V	KFR	R	AR	

19. Chatter

Radio operators, particularly the lesser-trained and on the lower echelons, exhibit a disposition to chatter amongst themselves. This chatter is the source of much information of value. It does not fall into the categories discussed above as it may relate to anything from discussions of personal problems to mentions of units or cryptographic features. This sort of talk is forbidden since it represents not only idling but a serious breach of security. Nevertheless, depending on the degree of discipline, it will occur in some volume in almost every radio net.

20. Plain-language and Low-grade Cipher Messages

Very often the error is made of transmitting, in plain language or low-grade cipher, messages which are apparently of no analysis value, yet when properly used prove of enormous assistance in the traffic analysis processes. Such messages may involve personal items or routine affairs which serve to reveal such important data as personalities, units, and locations. This type of traffic is particularly prevalent in the lower units where speed may be of the essence and where it is cumbersome to use complex cryptographic devices. Radio station personnel also indulge in this practice for exchange of technical data. They often find it necessary to ask, or reply to, questions of a semi-secret nature relative to their own operations. For this purpose, they may not use a standard system which would involve the delay of the code room and message center, but instead devise their own relatively simple ciphers.

REF ID:A58489

Section IV. THE MESSAGE EXTERNALS

21. Usual Components

a. In order to insure the proper handling of messages in both the message center and the radio station, some information must be sent in the clear or in simple code relative to message routing and accounting. This information is usually embodied in the preamble or postamble although, in some instances, it may be buried in the text. It may include any or all of the following items:

(1) Serial numbers, such as radio station numbers, message center numbers, etc.

(2) Group count.

(3) File date and time.

(4) Routing systems which serve to indicate message centers or units of origin, destination, and sometimes relay points of traffic. Distinction is also often made as to action and informational destinations. Routings may be in plain language, code, and/or cipher.

(5) Addresses and signatures, either in clear or cryptographed.

(6) Priorities, indicating the transmission and delivery precedence of traffic.

(7) Special instructions, as "time of receipt requested," "personal," "service," "repeated message," "relay message."

b. As a general rule, high-echelon traffic will contain most of these items, low-echelon traffic will cut them to a minimum. Their uses, positions, and surrounding procedure vary considerably according to communication system.

22. Serial Numbers

a. Serial numbers appearing on traffic may be enciphered or unenciphered and may represent any of the various stages through which the message passes before it is actually transmitted. The serial number acts as a reference to the message, and generally there are as many numbers in the externals as are necessary for convenient reference. The points at which such numbers may be attached to the message are—

(1) *The writer.* The writer of the message may have a personal series of numbers allotted for his use. Usually, however, numbers of this type, if present, will be included in the text.

(2) *Message center.* The message center of the unit in which the message originates generally assigns it a number. A number of this nature, if used, will usually remain constant through various relays of the traffic as it is the basic reference.

(3) *Signal center.* At large locations, several unit message centers often forward their traffic to a central signal center. The signal

REF ID:A58489

center also gives a number to the message. This number may appear in place of the message center number, along with it (though this is rare), or it may not be included at all. It is often difficult, where only one number is transmitted, to determine whether it is a message center or a signal center number.

(4) *Code room.* The code room, whether located in the message or signal center, may add a number to the traffic. Again this number may replace, or be used along with, the other types.

(5) *Radio station in-desk.* Each radio station maintains some form of in-desk for the handling of incoming messages and their routing to the proper radio positions for transmission. Here, too, a number may be put on the message. There may be several such desks for the forwarding of different types of traffic and this may result in several different series of numbers. In relayed traffic, these numbers (as well as the type included in (6), (7), and (8), below) may accumulate on the message, or a new one may be substituted for the old on each retransmission so that only the latest number appears.

(6) *Transmitter.* A number is often put directly on traffic by the radio operator as his reference. This number may be assigned in different ways. One method is to allot a series of numbers to a transmitter position and regardless of the receiving station this series is continued.

(7) *Link.* A second method is the employment of a link number, i.e., separate series are allocated for each station worked.

(8) *Operator.* A third system is the allocation of a personal series of numbers to each operator. A diagram of the above possibilities is given in figure 21.

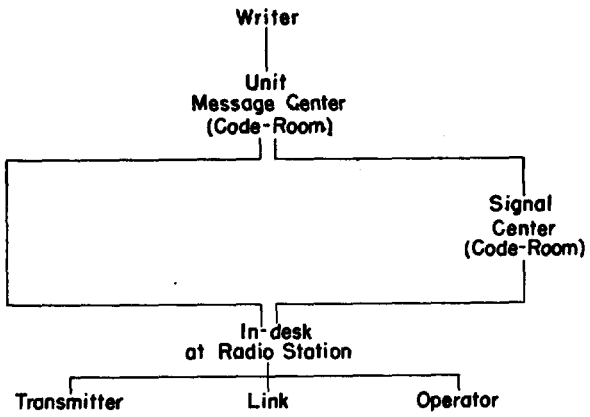


Figure 21

b. As a general rule, not more than two numbers will appear in the message externals, one representing some stage of the message or signal center phase, the other the radio station phase. In the lower

REF ID:A684682

echelons often only one number is used since the whole operation is usually so small that these fine distinctions lose much of their significance.

c. Series of numbers are allotted in some organized fashion, though this fashion may differ from net to net and from unit to unit. The series may be allocated in block form, e.g., 1 to 100 or 501 to 1000, etc. The blocks may be used until completed and then started over again; or the series may begin over on a periodic, such as a daily, basis, but if the prescribed limit is reached within the period, it is likewise recommenced. The series, on the other hand, may be open-end and repeat only at the close of a fixed period as a week, a month, or a year. In some types of series, the date or similar feature may be incorporated in the number.

d. These numbers may be enciphered in order to conceal the volume of traffic passed. It is not likely that this would be done with any of the radio station numbers because of the complexity of the operation, but it may be done at message center or signal center level. In this procedure, the plain text numbers run in serial order and messages are filed in the sending center by it. Another center referring to a specific message would do so by the enciphered number, the sending unit would then decipher same and locate the traffic. Thus, it is not necessary for the receiving center to know the system of encipherment and this permits considerable latitude in the employment of enciphering methods between the various centers.

23. Group Count

The group count may cover only the text of the message or it may include both externals and text. In some types of preamble separate counts are given for each. The group count may represent either the number of cryptographic groups, number of plain language words, or the number of individual letters and/or digits according to the method used.

24. Date Time Group

The date time group appears in the message externals and is expressed in six digits followed by a time zone suffix. It is intended to indicate the time the message was authorized for transmission, but may be used to indicate the time the message was filed at the message center, signal center, or at the radio station for transmission. Time is expressed in terms of the 24-hour clock and may be based on Greenwich Mean Time or on some local time zone. Whatever the base, it is generally kept standard for the entire net, if not for the entire communication system, regardless of the geographical area covered.

RECD 10 : AD684682

25. Routing Systems

a. GENERAL. Some method is required on radio traffic to indicate points of origin and destination and, in many cases, relay points. These methods must be relatively simple as they are designed chiefly as an aid to radio station personnel in the routing of messages. In this respect, it is necessary to understand the distinction between the routing designations and the addresses when both appear. The routing designations usually refer to message or signal centers, the addresses to specific units or persons. (There is nothing to bar the use of routing designations for specific persons but this is not generally the case.) It may be compared with the address on a letter, the routing designation representing the city of address, the address representing the company or person. On high-echelon traffic this difference is generally made, but in low-echelon traffic the routing designation often suffices for both purposes since message centers are small and traffic is almost always intended for the commanding officer. Thus, addresses as such do not usually appear on messages at this level. This distinction similarly holds true for routing designations used to indicate origin and signature.

b. The discussion of routing systems has been divided into two portions, the first dealing with the composition of routing systems, the second with their use.

(1) *Composition of routing systems.* Routing systems may be divided into three main types, plain text, call sign, and code. Plain text is seldom used on military nets because of its insecurity. Thus, generally, either the call signs of the stations are used for routing or a separate code is set up for this purpose. A routing code usually consists of two parts: code and syllabary. The code is composed of short number and/or letter combinations which may represent a location, message center, or unit. The syllabary provides code equivalents for the spelling out of place names or units not provided for in the regular code. These codes are usually rather simple, often being one-part in nature so as to be convenient for application. In some cases they are not used for security reasons, but rather for brevity. Generally, however, they serve both purposes and an encipherment of the code may be a feature of a few of these systems.

(2) *Use of routing systems.* Methods of using routing designations and the placement of these designations on traffic vary to a considerable extent. It may be set forth as a cardinal principle, however, that in most systems routing designations are used only when absolutely necessary. This increases their security and also makes it more difficult for the traffic analyst to determine the origin and destination of a message. On traffic which is point-to-point in nature, therefore, there are usually no routings at all. For example, in figure 22, A has a message for B. This message will be transmitted over

REQ: DD: AD684639

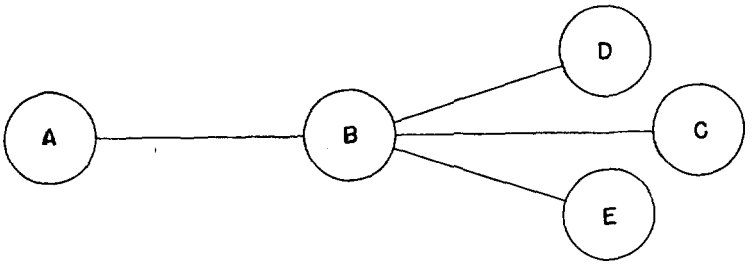


Figure 22

the A-B link and since it has originated with A and is destined for B, routing designations are not required. On the other hand, if A has a message for C, this is generally indicated in the externals so that B knows that it is to be forwarded. (It should be remembered that it is always possible to bury routing instructions in the text, but this is, as a rule, not done since it would necessitate the decoding of the message at each stage of the transmission.) This may be handled in two ways. The message may carry the routing "A to C," or it may only carry "to C" with the originator omitted. When the message is relayed from B to C, it may state "A to C," "from A," or have no routing at all. In some systems the relay point is noted, as "A to C through B."

c. Messages to several addressees can be indicated in several ways. For instance, in figure 22, A may originate a message for B, C, D, and E. All of these destinations could be incorporated in one preamble, "A to B, C, D, and E," or a separate preamble could be added at the end of the message for each location. Thus, the preamble preceding the message may carry no routing since it is being forwarded direct from A to B, but each of the preambles following the text would note "A to C," "A to D," "A to E." When this message reached B, B would transmit a copy with the proper preamble to each of the stations indicated. In this manner each copy would be numbered separately; in the single preamble method, only one message number would appear for all the recipients. It is further to be observed that if various specific addresses at one location, or routing designation, were involved, it would be possible to handle it in either of these ways or to indicate the addresses internally.

d. Distinction also may be made externally as to information and action destinations by the use of appropriate procedure. For example, in U. S. Army procedure, "W" is used to separate action from information addresses, e.g., "ABC W XQR" where ABC is the action addressee, XQR the information.

REF ID:A58489

26. Addresses and Signatures

Addresses and signatures may or may not appear externally on messages. Very often it is standard procedure to conceal them as part of the text. When they do appear externally, however, they are usually encoded and/or enciphered by means of complex cryptographic systems since they contain the specific names of units and persons and thereby are of high intelligence value. The address, unless it is in simple cipher or plain text, is usually considered a cryptanalytic, rather than a traffic analytic problem. Nevertheless, there are some features of the address and signature, such as length and manner of encipherment, which are of interest and use to traffic analysis.

27. Precedence Indicators

a. In order to insure the most expeditious handling of important traffic in both message center and radio station, some means of designating such traffic through the use of precedence indicators is usually devised. The precedences may be in the form of plain text, abbreviations of plain-text words, or number or letter code groups. Furthermore, in some military systems, these code groups may be enciphered.

b. The number of precedences used varies considerably from one nation to another and may range through several classifications of high priority to routine and deferred. There is, very often, no precedence designated "routine" and messages in this category, which are generally the most numerous, carry no marking at all.

28. Special Items

There are a great number of special items which are often included in the message externals. Some of the more common follow.

a. Part Messages. Long messages are usually broken up into several parts for ease of handling or for reasons of cryptographic security. Indications of this may be transmitted in the preamble.

b. Message Type. Indicators may be included to designate the type of message, for example, service, air warning, personal, weather, practice, repeated message, etc.

c. Miscellaneous Items. Procedures may also be provided for the transmission of miscellaneous items such as, "Time of receipt requested," "Each group sent twice," "Message sent blind," "Text in five (5) digit groups," "Relay message."

29. Message Examples

The elements discussed in the preceding paragraphs appear in message preambles and postambles in fixed positions according to the

REF ID: A5384682

procedure prescribed. These procedures differ from country to country and also often from one branch of service to another and from one echelon to another. Examples taken from U. S. Army procedures follow:

a. AB9 V PT3 291155Z GR12
BT Text
BT 291155Z K
AB9—Receiving call and destination.
PT3—Transmitting call and origin.
291155Z—File date and time, repeated as postamble.
GR12—Group count.
BT—Break before and after text.
K—"Go ahead" sign sent after message.

b. 3XF B79 V FR8–O–P B79–T–RST–A–FR8
152312Z 3XF RST B79 GR 19
BT TEXT.
BT 152312Z K
3XF B79—Multiple call-up; receiving calls.
FR8—Transmitting call.
O–P—Operational priority. (Precedence designation.)
B79–T–RST—B79 to transmit message to RST.
A–RF8—Denotes origin.
152312Z—File date and time.
3XF RST B79—Action destinations.
GR 19—Group count.

c. A45 BR6 B STX P–A45 BR6–T–N–A45
A–79K 011046Z A45–W–F2P SLW BR6
GR 28
BT TEXT.
BT 011046Z K
A45 BR6—Multiple call-up; receiving calls.
STX—Transmitting call.
P–A45—Message is priority to A45 only; to others routine.
BR6–T–N–A45—BR6 is to relay to all destinations except A45.
A–79K—Originator of message.
011046Z—File date and time.
A45—Action destination.
W–F2P SLW BR6—Denotes information destinations.
GR 28—Group count.

Section V. TEXTUAL FEATURES

30. General

While textual features and cryptographic systems are chiefly the field of the cryptanalyst, the traffic analyst should also understand

REF ID:A58489

certain aspects, both for the purpose of assisting in his study of communication nets and in the accomplishment of his responsibility to the cryptanalyst. These aspects relate to the distribution, use, and identification of systems, and to the use of indicators.

31. Distribution of Systems

Many cryptographic systems are limited in distribution; this limitation constitutes a cryptonet. For example, a system may be distributed only to the corps headquarters of a theater. These corps then are a cryptonet. Or it may be given only to units along a line of communications. There may be several reasons for the delineation of these nets but the chief ones are security, the nature of the system involved, and the physical problems of distribution. Forward units, for instance, are generally furnished different systems than the rear echelons because first, they are more liable to capture; second, they cannot handle the more complex methods of encipherment; and third, their traffic does not require the same degree of security. Within the higher echelons, divisions are made to prevent the overuse of any one system and thus deny depth. Such divisions also arise from the major break-down in command which allows some latitude in the composition of codes and ciphers to individual services or units. Furthermore, special systems may be prepared for use in particular operations where a high degree of security is desired. The important point, however, for the traffic analyst is to think of cryptonets not in terms of locations, but in terms of order of battle units, and to recognize the exact relationship existing between a system and a unit or group of units. It should also be observed that the existence of cryptonets necessitates the re-encrypting of traffic which passes from one net to another.

32. Use of Systems

Many times cryptonets will exhibit another distinguishing feature. This feature concerns the use of the system. For example, a system may be used only for confidential material, or only for secret material; or it may carry only information about supply, or shipping, or personnel, or operations. Again, this distinction is of high traffic analysis value and provides, as well, assistance to the cryptanalyst.

33. Identification of Systems

Some external feature usually appears in the text of a message to designate the system used. Where only one system of a given external appearance (as 4-letter, 5-digit) is used between two correspondents, this is not necessary, but in most instances, this designation is required and it can be accomplished in two main ways. The first is

REF ID:A5384682

the use of the form of the message itself. For example, the last group of the message may contain a repeat of the group count or the indicators may be peculiar in their formation, or they may be placed in a unique position. Any distinction of this sort will serve. The second method is the addition of a discriminant to the message, generally as a part of the text, most often as the first group. This discriminant is usually composed in a distinctive manner, as five like letters, repeated digraphs, ascending or descending numbers. It may be enciphered. Where a discriminant is lacking, it is often the task of the traffic analyst to determine means of identifying systems and to isolate homogeneous traffic.

34. Use of Indicators

The difference between the discriminant and the indicator should be understood. The discriminant identifies the general system used, while the indicator provides the specific key for decipherment. These indicators are often in the clear and, if they display any peculiarities of use, they become a valuable traffic analysis weapon. The pages of a one-time pad, for example, may be applied in order and the page indicators will thus reflect the number of messages enciphered. The pad numbers themselves will also be of value since each pad will be limited as to its users.

35. Practice Traffic

When new nets are being established, or operators are being trained, practice traffic is often devised for exercise purposes. Sometimes special nets are set up to this end, and they carry nothing but practice material. On the other hand, certain schedules may be set aside on regular links.

36. Control Traffic

In order to mislead enemy traffic analysts, control traffic may be used. Such operations may range from the formation of dummy nets to the passing of dummy traffic over the usual links. Control traffic can be employed merely to hide an operation through maintaining a volume level on all nets, or it can be used deliberately to deceive by creating high volumes at points of slight military activity.

Section VI. COLLATERAL MATERIAL

37. General

Aside from the usual intercept material discussed in the preceding sections, there are many other sources of raw data which are of value to traffic analysis. They may be divided into two groups, the first

REF ID:A58489

directly related to intercept, the second more or less miscellaneous in nature. The first group includes direction finding. The second is concerned with the study of nets other than military, the use of decode material, intelligence reports, prisoner-of-war reports, and captured documents. With reference to this second group, it should be observed that traffic analysis, in both its analytic and applied phases, often involves the fusing of information and material of all types and from all sources toward the production of a complete communication picture. In this respect, traffic analysis touches to some degree upon almost every phase of intelligence, and to a great degree upon every phase of signal intelligence.

38. Direction Finding

a. Direction finding (D/F) is a method of locating radio stations through use of specially constructed receiving antennae. These antennae register the direction along which a radio signal is travelling as it passes on a great-circle path through the D/F location. When the direction of a radio signal is determined at more than one D/F site, the location of the transmitter may be plotted by noting the point at which the bearing lines intersect (fig. 23). A location determined in this manner is called a "fix."

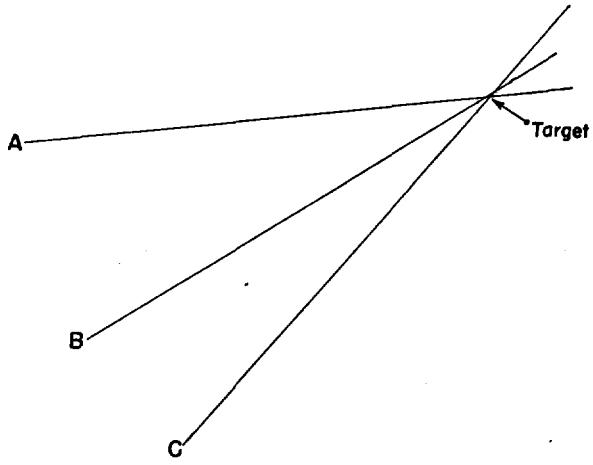


Figure 23

b. Usually, bearings will not yield a perfect fix, but will, depending on a number of factors, give a more or less restricted area. These factors include (1) the distance from the D/F station to the target, (2) the number of D/F stations involved in locating a target and the number of bearings taken, (3) the amount of the signal's deflection as encountered (for example, when the radio wave passes over mountains or shore lines), and (4) the quality of the D/F equipment.

RECD: 10 Jun 1946

Despite these and other limitations, D/F bearings seldom are misleading because the D/F operator is able to recognize whether or not a bearing is reliable and furnishes an evaluation of each bearing as it is forwarded to the plotting unit. The plotting unit also is in a position to make an accurate judgment on the reliability of a fix. An adequate arrangement for accurate direction finding requires a number of D/F stations (at least 3) located along a rather broad base (relative to the distance from the target) and so connected that they can all listen to the same signal and take their bearings simultaneously. It should be noted that D/F is particularly useful in low-echelon traffic analysis, but that over distances running into the thousands of miles it loses much of its effectiveness.

39. Information Derived from Cryptanalytic Results

Cryptanalytic solutions of traffic furnish, very often, the relationship between nets and order of battle. Since this is one of the ultimate goals of traffic analysis, detailed study of all solved messages, against the background of the nets, is a necessity. Study of solved messages should also be carried on for the purpose of relating internal information to external characteristics. This has an application to cryptanalysis for the identification of crib messages and to intelligence for the determination of the significance of traffic contacts and patterns. Message plain texts also yield a certain amount of signal information, as station locations and data concerning calls, frequencies, and schedules.

40. Intelligence Reports

Intelligence reports may vary from predigested order of battle lists to raw materials, such as captured documents or prisoner of war reports. Order of battle is the basis for the entire radio network and for the traffic passed over it. As such, an understanding of the order of battle is the necessary foundation for traffic analysis and its cryptanalytic and intelligence applications. The relationship is a circular one—intelligence added to traffic analysis yields additional intelligence. Aside from the broad phase of relating nets and battle order, this integration has specific applications in the analysis of traffic contacts and patterns and in the study of the uses of cryptographic systems and the transmission of routine messages.

REF ID:A58489

CHAPTER 3

RECONSTRUCTION OF THE RADIO NETWORK

Section I. INTRODUCTION

41. General

This chapter is concerned with the first objective of the traffic analyst, that of the reconstruction of the radio network. There are two phases to this objective, analysis of radio operations and net reconstruction.

42. Analysis of Radio Operations

This phase involves the identification and study of the elements discussed in the preceding chapter. It includes the identification of all components of the transmission, the analysis of their use, and the determination of their operating data.

43. Net Reconstruction

The nets are reconstructed coincidently with the study of radio operations. Each task helps the other; the distinction made here is only for academic purposes. In actual practice, attack must be carried out on all elements simultaneously, so far as possible, because analysis depends on the perception of relationships. Net reconstruction is concerned with the grouping of stations into nets, the determination of the links operating between those stations, and the identification of the stations with geographic locations, culminating in the production of the net diagram. The pertinent features of radio operations, such as calls, frequencies, and serial number blocks, may then be added to this diagram to complete the "pure" traffic analysis picture. The superimposition of the cryptonets and order of battle on the diagram is discussed in later chapters.

Section II. ANALYSIS OF RADIO OPERATIONS

44. Frequency Analysis

The main objectives of frequency study are (1) the determination of the system of use and (2) the solution of the system of allocation,

899152 O - 50 - 7

REF ID: A684682

including the method of original assignment, the pattern of rotation, and the reconstruction of the basic charts involved.

a. ANALYSIS OF THE SYSTEM OF USE. (1) The chief problem in the study of the system of use is the determination of accurate basic data. Once these data have been properly recorded the conclusion will usually be apparent. The basic data consist of who sends to whom and on what frequencies. To simplify study, a rough circuit diagram may be prepared. Two examples of these data and the conclusion to be drawn are given below.

(*a*) In the following example the net is a free star (fig. 24):

A to B on 5,000 KCS.
A to C on 5,000 KCS.
B to A on 5,000 KCS.
B to C on 5,000 KCS.
C to A on 5,000 KCS.
C to B on 5,000 KCS.

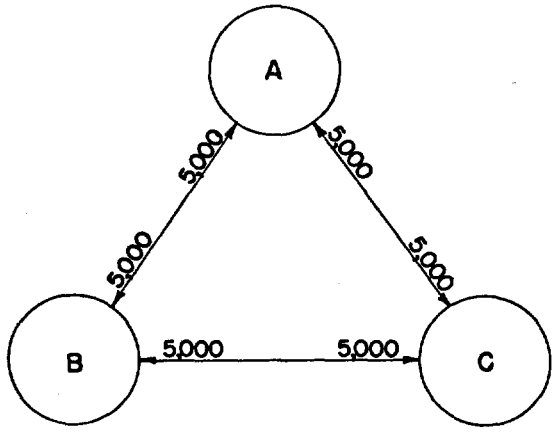


Figure 24. The net is a free star.

(*b*) In the following example the net uses the complex-sending system (fig. 25):

A to B on 5,000 KCS and 10,500 KCS.
A to C on 5,000 KCS and 10,500 KCS.
B to A on 4,000 KCS and 7,500 KCS.
B to C on 4,000 KCS and 7,500 KCS.
C to A on 3,000 KCS and 6,000 KCS.
C to B on 3,000 KCS and 6,000 KCS.

REF ID:A58489

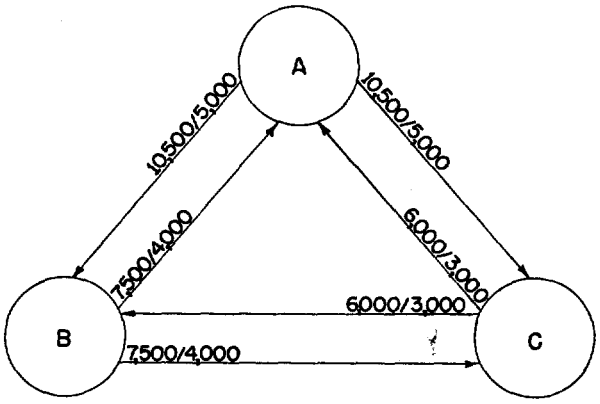


Figure 25. The net uses the complex-sending system.

(2) Arriving at accurate data, however, is often a fairly difficult task. It requires a detailed study of chatter for at least a week's period and usually somewhat longer, depending on the completeness of coverage during the period and the complications involved in the use of the frequencies. It is well to mention that, for the analysis of many features of radio operations, it is often desirable to have complete cover on a net for a limited period, such as a day, than to have spotty cover over a longer time. Generally, however, cover will be incomplete, that being one of the reasons why careful study of chatter is necessary before a decision is reached. A second difficulty arises where the enemy stations drift from the assigned channel. For example, a station allocated 4,650 kcs may vary all the way from 4,600 to 4,700 kcs. In the case of simplex and star working, much of this variation is intentional so that the one station can reply a little off the correspondent's frequency. A third problem is created by the assignment, as sometimes happens, of four or five or more wave lengths to a station. These wave lengths are not restricted to fixed times of day, but the station is at liberty to use whichever one can best be heard. It should be pointed out that there will often be exceptional uses of frequencies which cause the net to vary from its basic form of working. These exceptional uses should be carefully studied and explained, but they should not be considered as changing the net type.

(3) To illustrate some of these problems, assume that a cursory examination of a week's transmissions reveals the following:

A to B on 5,000 KCS, 11,600 KCS.
B to A on 5,000 KCS, 7,000 KCS, 11,590 KCS.
A to C on 5,000 KCS, 5,500 KCS, 11,625 KCS.
C to A on 5,010 KCS, 5,025 KCS, 6,995 KCS.

REF ID: A584682

B to C not heard.
C to B not heard.

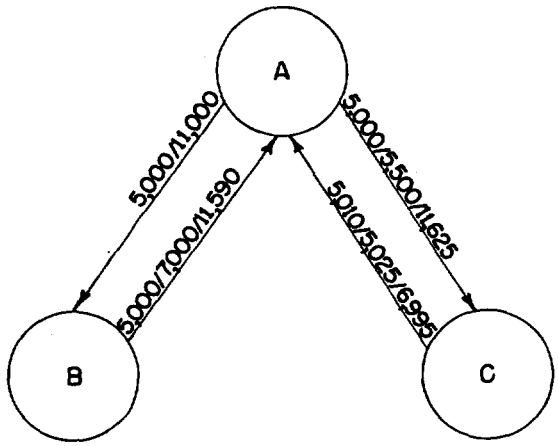


Figure 26.

The net, at first glance, appears to be a star (fig. 26) though there are several discrepancies to be explained. It may be assumed that C's 5,010 and 5,025 kcs are drifts of the base frequency 5,000 kcs, that A's 11,600 and 11,625 and B's 11,590 should all be 11,600 and that B's 7,000 and C's 6,995 are both 7,000. However, A uses 5,500 kcs to C, but neither B nor C have been heard on this frequency. This runs counter to the principle of the star. A check is made of the appearance of 5,500 kcs and it is found to have been used twice during the period under study, both times under the same circumstances. A came up on 5,000 kcs, C reported interference on this frequency, and A switched to 5,500 kcs. It is likely, then, that 5,500 kcs is an extra wave length assigned to the net for emergency purposes and that, in time, the other stations will also make use of it. In this instance the net is not working star since 5,500 kcs at A is corresponding with 5,010 kcs at C, but it is known that A did try to make contact under the established procedure first, so that this becomes the exceptional case and does not contradict the theory as to the star form. The 7,000 kcs at B and C also create a problem since A has never used this frequency. Again reference is made to the chatter logs where it is discovered that this frequency is used during the evening hours and has been heard once from B, twice from C. However, on all three occasions the A end of the circuit was not heard at all. It is possible that A was up on this approximate wave length but, because of some propagation or reception peculiarity, the intercept station was unable to hear it, or that the intercept station, for one reason or another, may only have been

REF ID:A58489

able to cover one end. Whatever the reason, imperfect coverage is apparent and, until A has been monitored on this schedule, nothing can be determined which would affect the star hypothesis. The net picture, as mentioned above, indicates that the star is controlled rather than free since B and C have not been observed in contact. Study of chatter, however, casts some doubt. At one point, A has asked B for a special schedule at 1500. B replies he cannot make it then since he has a schedule at that hour with C. On another occasion, A sends two messages to C for relay to B, A stating he has not been able to contact B. This chatter suggests that B and C work each other and that the net is a free, rather than a controlled, star. The evidence is slim since the schedules mentioned in the chat may only have been emergency ones, but it is sufficient to justify reserving decision and waiting for further developments.

b. Solution of the System of Allocation. Solution of systems of allocation requires at least several months of observation and, if some complex method of rotation is involved, may run into much longer periods. The problem is twofold: (1) the method of basic allocation and (2) the method of rotation, if present.

(1) It should be stated at the outset that usually a method of basic allocation will not be used except as it is tied into a system of rotation. Where frequencies are fixed, they have generally been assigned because they can be heard between two points and because there is no interference from other frequencies. This is particularly true on high-eschelon nets. It is always worthwhile, however, to check the frequencies of the various nets of a radio network for characteristics, if only to be sure. Some pattern may appear, for example, air-ground nets, wherever located, may be restricted to a definite set of frequencies, or divisional nets may be limited to a certain band. Anything in the way of a pattern, naturally, is possible. A tabulation of frequencies against net and the seeking of relationships in frequencies between related nets should serve to reveal most such patterns. Related nets may be so determined on the basis of function, such as air, shipping, line of communications, divisional artillery, by echelon, or by command.

(2) Whether a frequency system is fixed or changing, and if changing what the period of change is, can be discovered merely by observation. If a changing system is used, the first step in analysis is to determine some method of maintaining continuity so that if station A transmits on 4,300 kcs one day and 3,750 kcs the next day, there is some way of knowing that 4,300 and 3,750 are both the same station. Continuities may be established in two main ways:

(*a*) *Characteristics of radio operations.* Almost any item of radio operations may serve the purpose:

RECD 10 : AD684682

1.

Calls. If frequencies change and calls do not, identification is a relatively simple matter.

2.

Schedules. Taken in conjunction with other data, schedules may provide a clue to continuities. They are likely to be characteristic for the stations of a net, but care must be exercised in the use of this technique and supporting evidence should always be present. Also of value is any mention of future schedules at the time of the sign off, for example, "QRX 0100" (next schedule at 0100). It is then possible to relate stations heard at 0100 on the following day back to the stations involved in the chatter.

3.

Serial numbers. If serial numbers do not begin over at the time of each frequency change, they may be utilized. In the case of message center serials, care must be exercised to avoid the use of relayed traffic. For example, in figure 27, A, on the 15th, may

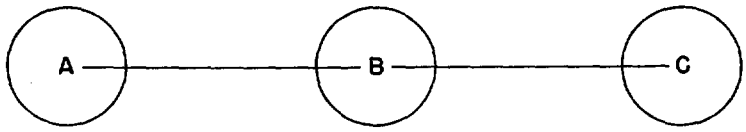


Figure 27.

send a series of messages over the A–B circuit with the message center serial range 1544–1573. On the 16th, the entire net changes frequency, and several messages are intercepted with the routing instructions A to C and the serials 1578–1581. It cannot be assumed that the new frequency heard on this transmission is at A since the traffic might have been passing on the B–C link. If some of the traffic, however, was routed A to B or else carried no routing indicating a local message, then the continuity might tentatively be established. Of far greater value in this respect are the radio station members, and, except in the case of the in-desk number where it is possible for several different circuits to be transmitting the same series, these ranges are reliable. Where serial ranges are fairly distinctive they may also be used in reverse. For example, station A may receive traffic in only a certain message center serial range from a correspondent. This may be caused by the fundamental assignment of the range to a definite service, for example, supply. Station A is at a quartermaster depot; consequently all the traffic to A from the correspondent will be in the one series.

REF ID:A58489

4.

Routings. Routing codes can also be of value when used by nets. It may be assumed that, as a general rule, a radio station will originate and receive more of its own traffic than it will handle on relay for other stations. For example, station A is at Gettysburg. If A changed frequency daily, it could probably still be spotted because of the large amount of Gettysburg correspondence transmitted and taken.

5.

Routines. Because of the requirements of military operations, it is necessary for units to make routine periodic reports. Very often these reports can be identified because of the stereotyped nature of the message externals. For example, a situation report, or a strength report, may be sent from station A to B, C, and D each day at approximately 2000. It would be a relatively easy matter to watch for this report to pass and to identify it purely by these external characteristics. Such routines furnish a trade-mark for the originating station and can be discovered and utilized without any knowledge of the text.

6.

Cryptographic systems. Cryptographic systems which are unique to certain correspondents can likewise be used as identifications. This also holds for some of the cryptographic features such as pad numbers of one-time pad systems. The 10th Division, for example, which sends through station A, is enciphering its traffic in pad number 1234. Usually, only one originator is permitted to encipher messages in a given pad because of its one-time nature. There may be one or several holders who can receive. Thus, until completely used, the pad will identify the originating station and, in some cases, also the recipient. Caution must again be exercised, however, with regard to relay messages and to the possi-

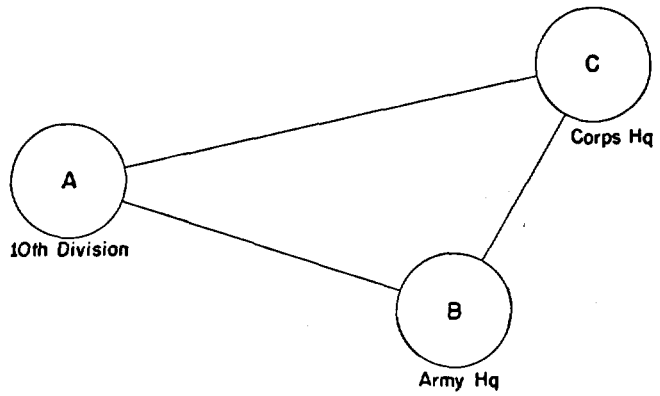


Figure 28.

REF ID:A5384682

bility of this traffic being transmitted over a different circuit of station A. If, for instance, the pad is used between the division and headquarters for some special purpose it could pass by several different paths (fig. 28). According to which route is available or readable, 10th Division's traffic may go directly to Corps or be relayed through Army.

7.

Services. Messages transmitted on one day may be serviced at some later date. If the date span bridges the frequency change, it may be possible to determine continuity.

8.

Chatter. Items of chatter often serve continuity purposes. Names of radio operators, for instance, may be observed in chatter, and, on recurring after a change, act as an identification.

9.

Procedural peculiarities. Some stations and operators develop unique habitual procedures which mark them. A station might, for example, regularly misspell a place name, or transpose the digits of a routing code number because of an error in the chart; an operator might send his call signs four times instead of the three used by others on the net, or send a separator between the hours and minutes of the file time though no one else does. Such peculiarities, which often arise from personal quirks, are usually rather difficult to discover because they involve painstaking attention to detail, but they are well worth the trouble. It is one of the phases to which the intercept operator, through his knowledge of the usual, can make an important contribution.

(*b*) *Use of direction finding.* This identification technique, described in paragraph 38, is a valuable means of providing continuities where efforts to use procedural characteristics have proved inconclusive. It is to be pointed out that, in general, procedural characteristics furnish a faster, less expensive, and more accurate method if they can be so utilized.

(3) Some of the techniques outlined above can stand by themselves, but it will always be found wise to apply several of them in combination so that one checks the other and reinforcing evidence is supplied. For example, the message center serials may indicate a continuity, and a routine message or the use of a restricted cryptographic system serves to confirm it. Incidentally, these methods of determining continuities are applicable to any sort of frequency change, whether periodic or irregular, and will also serve to tie together night and day frequencies and variant frequencies of the same station.

(4) When continuities have been established, the next task is the

REF ID:A58489

listing of the frequencies against the date breaks and the search for patterns of change or rotation. Once the general system has been solved, it will usually not be too difficult to keep abreast of changes. No attempt will be made in this manual to describe actual methods of solution further than to say that the problem, at this point, becomes one of cryptanalytic attack.

45. Call-sign Analysis

The main objectives of call-sign analysis correspond with those of frequency analysis, that is, (1) the determination of the system of use, and (2) the solution of the system of allocation.

a. Analysis of the System of Use. This analysis is conducted through a study of call signs as they are reported in the chatter. The period of call-up furnishes the most fruitful material, but all allusions to calls must be noted. A listing of the call-ups will generally provide sufficient information to identify the system.

(1) *Net using double-station call procedure* (fig. 29):

A calls B	DEF de ABC
B replies	ABC de DEF
A calls C	GHI de ABC
C replies	ABC de GHI
B calls C	GHI de DEF
C replies	DEF de GHI
B calls A	ABC de DEF
A replies	DEF de ABC
C calls A	ABC de GHI
A replies	GHI de ABC
C calls B	DEF de GHI
B replies	GHI de DEF

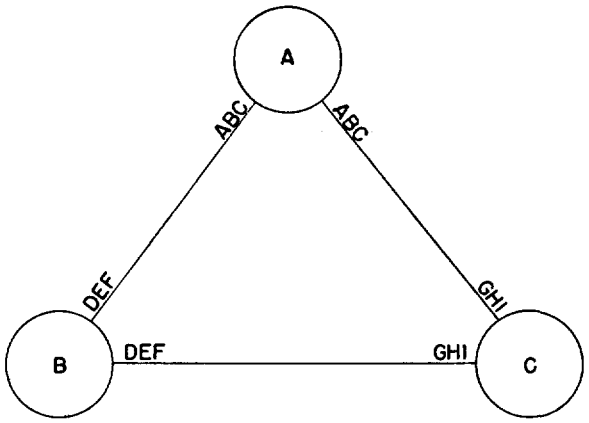


Figure 29.

REF ID:A58489

(2) *Net using link call system* (fig 30)

A calls B	ABC
B replies	ABC
A calls C	DEF
C replies	DEF
B calls C	GHI
C replies	GHI
B calls A	ABC
A replies	ABC
C calls A	DEF
A replies	DEF
C calls B	GHI
B replies	GHI

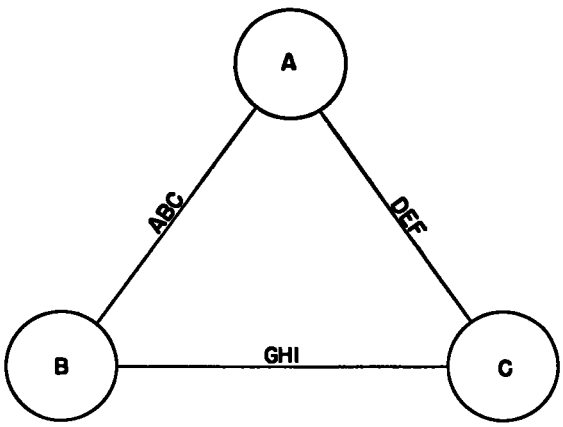


Figure 30

(3) *Net using single station call* (fig 31)

A calls B	DEF
B replies	DEF
A calls C	GHI
C replies	GHI
B calls C	GHI
C replies	GHI
B calls A	ABC
A replies	ABC
C calls A	ABC
A replies	ABC
C calls B	DEF
B replies	DEF

REF ID:A58489

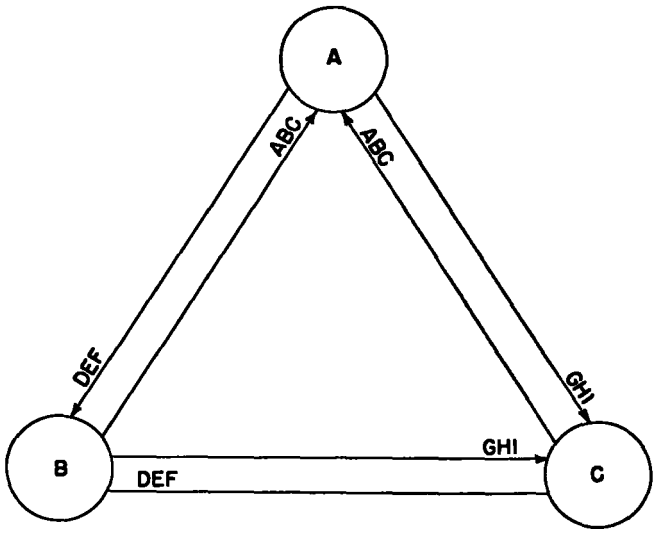


Figure 21

b Solution of the System of Allocation Like the study of frequency systems, the analysis of call sign systems may require anywhere from several months to several years Again like the frequency systems, the problem is twofold (1) the method of basic allocation and (2) the method of rotation, if present

(1) Calls must first be classified as to composition, for example, 3 digit, digit-letter-digit, etc, then these break-downs checked for pattern The allocation of calls may or may not be centralized. In the former instance, there will generally not be more than two or three systems to be solved, e g, Army and Air Force In the latter, however, depending upon the amount of decentralization, there may be a great many small systems Thus, in the initial analysis, calls should be listed by net, and the composition of the calls on each individual net observed If, for example, of all the nets under study, only two nets use 4 letter calls, it may be assumed, for the moment, that these nets employ a common call allocation After nets have been grouped by composition of calls, a search is made on each net for pattern For instance, the calls on three of the nets may carry "T" as a middle letter, indicating a possible grouping for study If a number of other nets also display similar characteristics, one using "R", another "V", etc, it is likely that all of the calls on these nets originate in the same general system The following lists of calls by net will serve to illustrate the general procedure

REF ID: A684682

Net I	*Net II*	*Net III*	*Net IV*
ABD	CDF	V7K	BCE
EFH	GHJ	V8J	KLN
FGI	LMO	X3M	OPR
JKM	MNP	Y4T	
		Y6S	

Net V	*Net VI*	*Net VII*	*NET VIII*
BAO	IJL	DEA	FQR
HIU	NOQ	HOA	JLT
KOE	PQS	JIE	SRM
MEA	STV		VTR
PAE			XOM
			XOA

(*a*) In the first quick grouping, the following division could be made:

Nets I, II, IV, V, VI, VII, VIII—3-letter.
Net III—letter-digit-letter.

(*b*) The first group then splits into three:
Nets V, VII—consonant-vowel-vowel.
Nets I, II, IV, VI—1st and 2d letters are in alphabetic order, 3d letter skips one from 2d.
Net VIII—apparently random.

(*c*) Thus, there are at least four systems of call distribution involved. On the other hand, studies of the calls on a number of nets may reveal no pattern at all. This is usually indicative of a large, general system in which control is highly centralized and the randomization carefully planned.

(2) Other features may also be employed to assist in the establishment of homogeneous call-sign systems for relationships between any of the elements of different nets that indicate possible relationships in other elements. For example, there may be some question as to whether or not the calls appearing on two separate nets can be grouped together. A cryptographic system, found nowhere else, is discovered on circuits of both nets. This suggests that there is some connection between the two nets and increases the possibility of a common call system. Procedural peculiarities of any type may likewise be used to associate nets. Order of battle, if known, furnishes another valuable method. All the nets of a given Army, for instance, will probably use the same call allocation. It may be that, in a highly centralized organization, a dichotomy can be established simply between Army and Air Force.

(3) Once the various systems have been segregated, it becomes possible to attack each separately. If a pattern exists within the call itself (as in Nets I, II, IV, and VI in (1) above), all possible

REF ID:A58489

calls can be listed and this used as a basis for the reconstruction of the allocation chart. If no pattern can be found, however, (as in Net VIII), it becomes infinitely more difficult to reconstruct these charts, and if the system is a large one it may be necessary to collect data over a period of years before a solution can be effected.

(4) Often these allocation charts serve as a base for the change or rotation of calls or for the choice of alternate calls at the same station. In analysis of the system of rotation, the first step is to determine the periodicity, which can usually be done simply by observation, and the second to establish continuities so that the calls related to each station or link and the order of their use are known. The techniques outlined in paragraph 44*b* (2) for the determination of continuities when frequencies change also apply to call signs with one exception (par. 44*b* (2) (*a*)*1*) and need not be further discussed here. In this one exception the reverse is true—if calls change and frequencies remain constant, the frequencies furnish the continuities to the calls. When continuities have been established, the calls may be listed in order for each station, and through the application of cryptanalytic techniques, the system attacked.

(5) In the practical aspects of call-sign system solution, it will be found that garbled and missed calls account for much of the difficulty in the initial stages of attack. Where there is a pattern to the call composition, garbles can be resolved with relative simplicity. In random composition, however, the problem is more complex and care must be taken to eliminate all spurious calls before beginning analysis. Garbles occur with some frequency in calls partly because the enemy makes an attempt to restrict their use, and partly because his operators become so familiar with them that they tend to send them in a quick, sloppy manner. In general, a call should be intercepted several times, preferably at different schedules, before it is accepted as genuine. Garbles can often be corrected by reference to the actual Morse equivalents. For example, if the call "AHV" has been established and the call "ASV" appears once on the same net, the Morse will indicate the possibility of error:

AHV .— ....—
ASV .— ... ...—

the difference being only a dot. Other link characteristics such as frequency, serial numbers, etc., will assist in confirming or disproving the identity of the two calls.

(6) Missed calls also present a problem to the analyst. They arise from imperfect coverage, and there is no remedy except to give more complete coverage and schedule information to the monitoring stations. Since calls are often sent only at the start of each schedule, this time is most important.

REF ID:A584489

(7) The following example, based on the call composition used in Nets I, II, IV, and VI in (1) above, will illustrate the general approach (since these calls have a definite pattern, all possible calls can be listed):

ABD
BCE
CDF
DEG
EFH
FGI
GHJ
HIK
IJL
JKM
KLN
LMO
MNP
NOQ
OPR
PQS
QRT
RSU
STV
TUW
UVX
VWY
WXZ
XYA
YZB
ZAC

(*a*) It is noted that calls change daily on the four nets involved; after the completion of one week, a tabulation by net and station can be made. (Garbled calls have been corrected.)

	1	2	3	4	5	6	7
Net I							
Station A	ABD	PQS	TUW	KLN	BCE	RSU	....
Station B	....	WXZ	BCE	EFH	HIK	....	UVX
Station C	MNP	JKM	MNP	WXZ	NOQ	XYA	CDF
Net II							
Station A	CDF	....	IJL	YZB	....	ABD	JKM
Station B	UVX	LMO	VWY	STV	JKM	GHJ	....
Station C	IJL	STV	OPR	ABD	DEG	MNP	WXZ

REF ID:A58489

Net IV

Station A	TUW	RSU	....	RSU	UVX	FGI	IJL
Station B	....	EFH	....	FGI	IJL	LMO	....
Station C	NOQ	KLN	....	XYA	OPR	YZB	VWY
Station D	HIK	XYA	....	LMO	CDF	STV	DEG

Net VI

Station A	....	ABD	DEG	MNP	PQS	BCE	....
Station B	VWY	....	PQS	TUW	....	HIK	....
Station C	DEG	YZB	JKM	GHJ	EFH	TUW	....

(*b*) Observation of the calls indicates that they are being rotated in a simple manner, and a check against the list of all possible calls shows that the difference of six between calls on the same net is fairly common. For example, on the 1st, MNP is 12 calls away from ABD; IJL is 6 away from CDF; NOQ is 6 away from HIK. It is also noted that the calls QRT and ZAC do not appear, probably to prevent confusion with Q and Z signals. This leaves 24 possible calls, and the periodicity of 6 suggests that the basic table is arranged as follows:

ABD	GHJ	MNP	TUW
BCE	HIK	NOQ	UVX
CDF	IJL	OPR	VWY
DEG	JKM	PQS	WXZ
EFH	KLN	RSU	XYA
FGI	LMO	STV	YZB

and that the calls are taken off across the chart and allotted to Net I, Net IV, Net II, and Net VI in that order. Within each net the calls are assigned to individual stations in what appears to be a random order.

46. Schedule Analysis

Schedule analysis is designed to discover what system is in use, whether the signalling is restricted or unrestricted and, if the former, what the time of each schedule is.

a. Analysis of the System. Analysis involves a tabulation of times of communication together with a study of chatter. Time is correlated with circuit and, if a definite pattern shows up several weeks running, it may be assumed that period signalling is in use. In the preparation of the data, record should be made of such chatter items as, "I have a schedule at 2200 with XYZ." Such information helps to fill in the gaps in cover. Also note must be taken of the very brief schedules where the stations have no traffic and merely call up, say, "I have no traffic," and sign off; or where a station is running over his schedule time and calls his regular correspondent

REF ID: A684682

to say, "I am busy," and then goes back to the first correspondent. If no pattern appears, however, it is then likely that either unrestricted signalling or priority signalling is in use. This can be determined by a check of the tabulation, since in priority signalling the control station will usually come up at regular schedule times. Chatter will also prove characteristic for this type of operating since the order of transmitting is fixed and usually only one message is sent at a time by each station. The type of unrestricted signaling can likewise be identified from chatter. Where arbitrary schedules are used, the stations will arrange for the next schedule at the time of sign-off. Incidentally, in period signaling, the stations also sometimes mention the time of their next schedule so care should be exercised not to confuse the two. The regular pattern of times over a long period will usually distinguish period signaling. In alert operating, no arrangements are made, all stations standing by for transmissions at any time.

b. Determination of Schedules. The tabulations made for the above purpose will also serve to determine the times of regular schedules. Each circuit may be plotted on cross-section paper with hours down the side and days across the top. This will give a month's picture at a glance (fig. 32). The letters in each square indicate

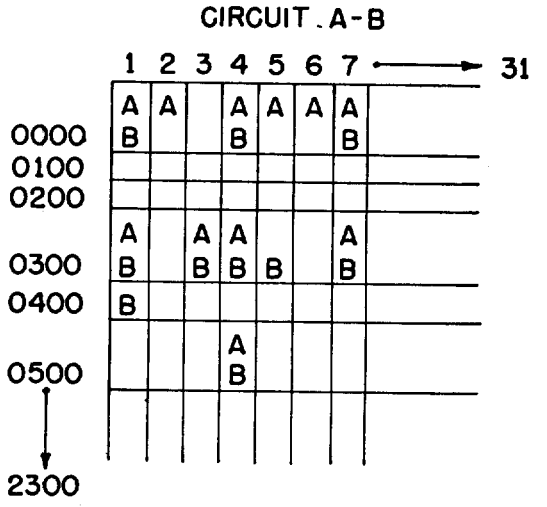


Figure 32.

the end of the circuit that was heard. On the 2d at 0000, for instance, only A was intercepted. Other items may be added to this tabulation if desired. These might include number of messages passed, indication as to which of the alternate frequencies was being used, and special notes from chatter relating to schedules. Two irregulari-

REF ID:A586489

ties will be noted in the pattern in figure 32. On the 1st at 0400 B ran over the regular 0300 schedule. Reference to chatter discloses that B asked A for additional time. On the 4th at 0500, A-B worked a special schedule. A check of chatter on other A circuits shows that A arranged for this schedule through a third station, which could contact both A and B, for the purpose of passing urgent traffic.

47. Procedure Analysis

Analysis of procedure is undertaken (1) to discover characteristics which will assist in identifications and continuities, and (2) to solve any encipherments employed.

a. Study of Characteristics. The normal characteristics of the procedure under study should first be established. This includes the call-up, exchange of readability, order of traffic, message externals, servicing methods, and sign off. In many communication systems, several normal procedures may be apparent, each representing a major division of nets. When this task has been completed, variations from the normal as applied to individual nets, groups, links, and stations must be identified. These variations may be of any sort. For example, one net may use break-in procedure for servicing, or may place the priority of the message in a different preamble position, or may tune up with a letter other than "V"; or a station may regularly place an NR before the link serial number while others do not, or fail to use an RQ before its request for services. These variations arise in several ways. They may be due to an oversight on the part of personnel, such as failing to change to a new method of procedure because of habit or because the station was not included in the distribution of the new instructions. Such situations will usually be corrected in time, or, if distribution is impossible, continue to serve as an important identifying feature. Or they may arise from the latitude permitted nets or stations in compiling their own rules. The only approach to this analysis is through the detailed study of chatter and the recording of the normal and the unusual.

b. Solution of Enciphered Procedures. The solution of enciphered procedures depends on the ability to determine the meaning of procedure signs and signals in context and, where a periodic change is involved, the equating of the same procedure in terms of different encipherments. For example, in the opening minutes of a schedule, procedures such as "Send V's," "How is my readability," "I cannot hear you," "Readability is poor," "Adjust your transmitter," etc., will be common. By study of the context over a period of time, it should be possible to identify the appropriate meaning.

RECD 100 : 2684682

48. Serial Number Analysis

The analysis of serial numbers is directed toward the determination of the type of number, the manner of assignment, the solution of any encipherments, and the identification of the series with units.

a. ANALYSIS OF TYPE. The type of the serial number, that is, indesk, message center, signal center, etc., is determined through a correlation of the numbers with other signal features. The numbers should be tabulated for a period of a week or more as necessary against call signs, file times, intercept times, cryptographic systems, routings, and similar items. The following discussion is not intended to be complete since there are so many possibilities involved in these manifold relationships, but it is hoped to give some general indications on how to think about them.

(1) Serials which run in order by cryptographic systems may be a code room number, a message center number, or a signal center number. It will rarely be a radio station number. The caution to be observed is that the cryptographic system may not be the basic factor and the serial the result, but rather the system, like the serial, may be the effect of something more basic. For example, a series is found which agrees with the cryptographic system and every message in that system is always in that series. It is noted, however, that the system is the only one held by the unit involved. Thus, both the system and the series are representative of the unit, and the number only accidentally follows the system.

(2) Serials which correlate with routings are also usually in the message/signal center phase. Sometimes several series which do not match with other features are observed originating at the same routing. These are often the expressions of several units operating through a single signal center. Such numbers may be put on at the unit message center or they may be added at the signal center, the latter maintaining several series, one for each of the units involved.

(3) Serials which run in order by file time may represent either the message/signal center or radio station stage. Usually, file times are put on at the radio station, but, since the traffic comes to the station direct from the message or signal center, its order is seldom disturbed, so that it could be numbered in one place and time-stamped in another and still demonstrate a relationship. In the case of radio station numbers, it will usually be found that several call signs, used at the same station, will run in a common series.

(4) Transmitter numbers will, as a rule, correlate with the sending call signs and the intercept time. Link serials will be evidenced by the further distinction of a separate series for each station called. Operator numbers are indicated by several series originating at one call, regardless of reply, unless the station works to only one correspondent.

REF ID:A58489

(5) It is just as important in the study of serials to have negative evidence as positive, so note should also be taken of what does not fit the series. If several routings fall in the same series, for instance, the number was not assigned at the message center if that is what the routing represents. Such a series is more likely to relate to the radio station which handles traffic for several different routings.

(6) Many times series will appear which bear a relationship to several items. It is then necessary to determine what is the basic consideration. For example, a tabulation of serial numbers reveals:

Serial	*Crypt. System*	*Routing*		*Call sign*		*File date and time*	*Intercept date and time*
		From	*To*	*From*	*To*		
326	A	A	B	PQR	XYZ	08 1040	08 1215
327	A	A	B	PQR	XYZ	.....	08 1217
328	B	A	C	PQR	XYZ	08 1040	08 1220
335	A	A	B	....	....	09 1230	09 1530
339	C	A	C	PQR	XYZ	09 1210	09 1532
340	A	A	B	PQR	XYZ	09 1235	09 1535
343	B	A	C	PQR	....	09 1300	09 1538
344	C	A	C	PQR	XYZ	09 1300	09 1600
345	C	A	C	PQR	XYZ	09 1250	09 1615
346	A	A	D	PQR	XYZ	09 1310	09 1619
362	C	A	C	PQR	XYZ	11 1240	11 1525
367	C	A	C	PQR	....	11 1500	11 1801
368	C	A	C	PQR	XYZ	.....	11 1820
429	B	A	C	PQR	XYZ	08 1100	08 1223
437	B	A	C	PQR	XYZ	09 1315	09 1623

Except for the last two numbers which are garbled, the serials correlate with origin, calls from and to, and intercept time. File time is slightly off in several places. Since intercept time fits so well, it may be assumed that this is a radio station number. Reference is now made to the circuit diagram and it is noted that PQR is on the edge of the net and that it is connected to it by the single circuit to XYZ. Thus the routing "A" is probably the only message center routing through PQR and, therefore, the relation between "A" and the serials is forced and not the true one. If it were the true one, it is likely that the intercept times would be somewhat out of order because of the routine of processing traffic and the passing of priority messages. But since there is only one link out of the station, the type of radio station number used cannot be defined. It may be an in-desk, a transmitter, or a link number. If the picture is expanded, however, to include an additional link with numbers, it will appear as follows:

REF ID: A584682

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
372	B	A	C	PQR	STN	08 0900	08 1025
733	A	A	B	PQR	STN	08 0910	08 1030
734	A	A	B	PQR	STN	08 0910	08 1033
759	B	A	C	PQR	STN	11 1535	11 1911
765	C	A	C	PQR	STN	11 1820	11 1914

The serial is a link number since the numbers run in a separate series for the PQR–STN channel.

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
603	B	A	C	PQR	MNO	171441	172010
604	A	A	C	PQR	MNO	171411	172013
605	B	A	C	PQR	MNO	171411	172016
606	B	A	C	PQR	MNO	171415	172021
610	B	B	D	GHI	STN	171430	171810
612	C	B	D	GHI	STN	171430	171812
612	C	B	D	CHI	STN	171430	171812
613	A	B	C	PQR	MNO	171440	172005
634	A	A	C	PQR	MNO	181120	181523
636	A	A	E	GHI	STN	181135	181803
639	A	A	D	GHI	STN	181150	181809
640	B	A	C	PQR	MNO	181155	181520
641	A	A	C	PQR	MNO	181155	181535

Note the correlation with file date and time and the interlocking of the call signs. This is an instance where file date and time are entered at the radio station.

(7) The following tabulation is that of a signal center number:

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
020	A	A	C	GHI	PQR	230910	231233
023	A	A	C	GHI	PQR	230910	231230
024	A	A	C	GHI	PQR	230925	231225
026	B	B	D	JKL	STN	230910	231413
029	C	B	D	JKL	STN	230915	231416
153	A	A	C	GHI	PQR	241120	241236
155	A	A	E	MNO	XYZ	241125	241228
156	D	A	E	MNO	XYZ	241130	241231
164	A	A	E	MNO	XYZ	241130	241238
166	B	B	D	JKL	STN	241145	241411
167	B	B	D	JKL	STN	241130	241402
170	C	B	D	JKL	STN	241145	241409
171	C	B	D	JKL	STN	241150	241421
172	D	A	C	GHI	PQR	241145	241250

REF ID:A58489

Both A and B route through the signal center where a common series is applied to the traffic of both. The possibility of this being an in-desk number is largely ruled out by the failure to correlate with file time.

b. Analysis of Assignment. Study of the manner of assignment of serial numbers is concerned with three phases: (1) composition of the numbers, (2) range of the series, and (3) over-all pattern of assignment.

(1) *Composition.* The numbers may consistently be two-digit, or three, or four, etc. They may incorporate such features as the date. Composition, if sufficiently distinctive, often furnishes a means of quick recognition.

(2) *Range.* The range of the series may be readily determined, or it may take several years. It can be established by observation of the reversion to the lowest number of the range, which will fix its limits in terms of either time or numbers, or both.

(3) *Over-all assignment.* Serial ranges of the same type of number should be checked for pattern of assignment against each other. In the case of message center numbers, for example, it may be found that each division of an army has been given separate blocks, 1–100, 101–200, 201–300, 301–400, etc. Similar patterns may appear with regard to signal center or radio station numbers. These patterns can be analyzed through a comparison of ranges representing groups which bear an order of battle or a net relationship to each other.

c. Solution of Encipherments. The solution of enciphered serial numbers is a matter of cryptanalytic approach. The initial break, however, can often be made by gathering a group of messages on which it is thought that the serials run in order. If, for instance, an in-desk number is involved, messages arranged by file time should assist in attacking the system. It also may be helpful to select the first message of the day, if possible, and use it as No. 1. It will serve as a base even though that may not be its actual number. If the numbers are thought to repeat daily a selection of this message each day may yield different encipherments of the same number. As a rule, these systems should not prove too difficult to solve unless the method is one of complete randomization.

d. Identification of Series. Once the type of series is known, the next step is to determine the actual unit behind each series. In the case of a message center number, for example, what message center is it? Or if there are three series of in-desk numbers out of the same station, what do each of these series represent? These identifications are established by "pure" traffic analysis plus the use of collateral material on the basis of the axiom that things equal to the same thing are equal to each other. For instance, a range of in-desk numbers appears only with codes A and B. Codes A and B are known to be

REF ID: A5384682

transportation systems. Therefore, the serial range represents the transportation unit at the signal center. Care must always be taken, in chaining data of this sort, that the basic assumptions are valid (in this case, that A and B are transportation codes) and that the things compared demonstrate an exact relationship (if A and B were also used on another range of numbers out of the same station, then it is unlikely that the first range represents transportation, but rather that it represents some other type of unit or else a specific transportation unit, these possibly being two at the station). Decode and order of battle material are invaluable in the study of these series. If some of the traffic related to a series can be read, solid evidence for conclusions is provided and often a definite unit can be identified. Order of battle will do much the same. For example, where only one air unit is carried at a given location and a series, tied to the air cryptographic systems, is observed out of that location, it may be assumed that the series represents the air unit.

49. Analysis of Priorities

The analysis of priorities is directed toward determining their order and the solution of any encipherments. The order is determined by comparing file times with intercept times. In general, the shorter the average time lapse, the higher the priority. However, time lapses should be compared within stations not between them since the size of the station and the volume of traffic handled will cause individual differences. Relayed traffic, of course, should not be included in the comparisons. The cryptanalysis of encipherments is naturally dependent on the system used, but it is of assistance to group messages according to expected priority, thus providing isologs.

50. Analysis of Routing Systems

The main objectives of routing system analysis are to discover the manner of use and to solve the routing codes.

a. Analysis of Use. When routings appear on traffic, it is first necessary to determine what they represent in terms of origin and destination. This is done by observation. If necessary a tabulation can be made against call signs which will readily reveal which routing is the originator and which the addressee. The difference where present between information and action addressees may be a little more difficult, but checks, for example against priorities, should assist. Further observation will indicate the manner of handling local and relay traffic and the nature of the routings in these instances. Any peculiar use of routings, as in the readdressing of traffic, can also be determined. Following these routings against the net diagram is often helpful.

REF ID: A584682

b. Solution of Routing Codes. The initial step in the solution of routing codes is to check the code groups for characteristics in composition and range. Once these patterns, if present, have been recovered, the next step is the specific identification of code and syllabary groups. Identifications are chiefly based on cribs from known systems to unknown, on net diagrams, on breaches of security, on decode and order of battle material, and on a number of variations of these. As identifications are produced, it may be possible to ascertain the structure of the code and syllabary, such as alphabetical, geographic, order of battle, etc., and this, in turn, assists in future recoveries. In order to suggest methods of attacking this problem, some of the possibilities are discussed below:

(1) *Tying the code group to a known radio station.* Where the station locations are known, several methods present themselves according to the use of the routing codes. The predominant originator out of a station may ordinarily be assumed to be located there. This also applies to the predominant destination, unless destinations are dropped on local traffic. But, because the identification is made with a location, this identification is a true one only if the routing numbers represent locations. If they represent units, then it is necessary to seek further, and the recovery of the location can only be considered tentative in lieu of something more exact. Along with the use of this technique, the lapse between file and intercept times should be averaged for each originator. Messages originating locally will show a shorter time lapse than those previously relayed. If destinations are habitually dropped on the last, or local, leg of a relay, they may be related to the receiving station. For instance, a message from A to C carries the routing "123–567" on the A–B link (fig. 33), but when B relays to C, it only carries "123", thus matching 567 with C.

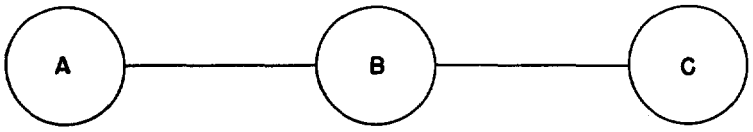


Figure 33.

When the same message is sent to several locations, the local copies may not carry routings while the relayed ones do, making possible the identification of the origin with the sending station. For example, in figure 34, A sends the same message to C and D. The message to C on the A–B channel is marked "123–567", that to D has no routings, thus identifying 123 with A.

(2) *Cribs.* The availability of cribs is chiefly based on the existence of several different routing systems. This may involve checking into networks other than military, such as Naval or domestic, for

REF ID: A684682

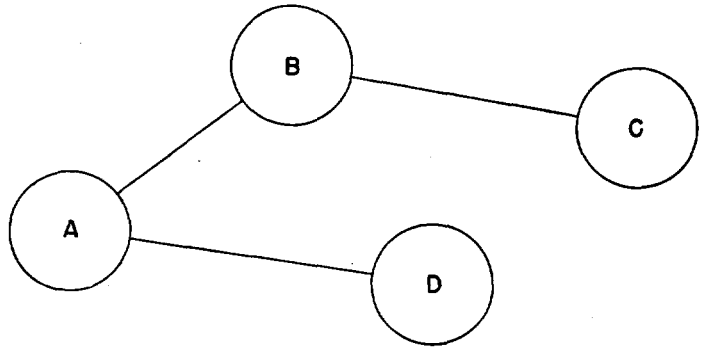


Figure 34.

such data. No possibility should be overlooked. Some of the crib techniques follow.

(*a*) *Relay crib.* If it is necessary for a message to pass over different nets with different routing systems, origins, and destinations can be correlated, and if one system is known, the other can be identified. For example, the message on Net I carries "123–567", on Net II "ABC–JKL", then 123 equals ABC and 567, JKL. One caution here relates to the destination. If this is a book message going to several addressees, there may be a direct correspondence between the originators, but not the destinations, since 567 may be one receiver and JKL another. Sometimes, this can be verified by checking the address and serial numbers.

(*b*) *Book message crib.* Where the same message goes to a number of destinations over different nets employing different routing codes, it is possible to crib originators. This often happens with large centers who work in several nets and may use several routing codes. It also occurs where traffic is relayed out of the net. Naturally, this would also yield a relay crib, but if the first transmission has been missed, the later relay can be used as a book message crib.

(*c*) *Serial number crib.* Serial numbers may be used to crib originators if the serial is a message or signal center number. For example, if a tabulation of serials reveals the following:

Serial	*Routing*	*File date and time*
53	123	092005
54	123	092005
55	123	092005
58	ABC	092005
59	123	092005
60	123	092015
65	ABC	092020
67	ABC	092020

then 123 may be cribbed with ABC.

REF ID:A684682

(*d*) *Error crib.* Where several routing systems are available to a station which works in a number of nets, it may occasionally happen that the wrong system is used. Such errors will generally be corrected yielding a crib between the two codes.

(*e*) *Address and signature cribs.* A unit or person addressed at one routing group in a known system will yield a crib against the same unit addressed at an unknown group. For instance, the 37th Division may be addressed at ABC, known to be Mannheim, on one message, and to 123 on another on the same day; 123 may then be identified with Mannheim. The possibility of unit movement, however, must be considered, and also that of detachments being addressed. The new recovery should be checked against the pattern, if present, of the routing system. In address systems where solution is only partial, but unenciphered code is available, the same address code groups may be used to crib the routing groups. Address code groups, for example, 1234, 5678, may appear with destination group ABC and also with 135. It is not necessary to know the value of 1234 5678 to crib ABC with 135. These same techniques are applicable to signatures and points of origin.

(3) *Operator chatter.* Operator chatter may give away the identity of a code group through the mention of a place name or a unit.

(4) *Address information.* Where addresses are separate from routing codes, use may be made of the address when readable. A unit, whose location is known from other order of battle sources, may be addressed at an unknown routing group thus identifying this group. Consideration must be given in such an instance to the possibility of the unit having moved. If there is some pattern to the composition of the code, the new value should be checked for fit. The recency of the date of the unit's identification and the trustworthiness of the source should also be noted.

(5) *Solved message information.* Solved messages may contain outright assignments of routing code values; more usual, however, is the traffic which permits correlation of internal originators, addressees, or subject matter with externals. All solved messages should be read for clues to routing code identities.

(6) *Miscellaneous sources.* These involve prisoner-of-war reports, captured documents, and similar materials.

(7) *Syllabary solution.* The syllabary to the routing code may be solved by using any of the above methods, but also available is the use of word patterns. If, for example, the routings consist of place names, a list may be constructed of all likely places which will show patterns of repeated or doubled letters, digraphs, etc., within each location, and this may be applied against similar patterns in the encipherments.

REF ID: A5384682

(8) *System change.* If the routing system changes, the continuity techniques discussed in paragraph 44 *b* (2) may be applied. For example, the continuation of a series of serial numbers may serve to identify a new routing designation with an old. Also of value are the contact patterns or associations in which a routing designation may be involved. If, for instance, routing number 123 sends traffic daily to three particular locations, and after the change of system, ABC is discovered following the same pattern, then 123 and ABC may be equated.

c. The above listing of methods of identification is only partial and specific application is dependent on the nature of the communication system under study and on the structure of the routing codes. Identifications, as made, should be evaluated and some sort of validity indicator attached to them as a guide to the reliability of the value. These validities are the result of personal judgment and the peculiarities of evidence and no rules can be laid down for their use on a general basis though in any specific problem definite standards can be set up. Where identifications are based on a crib, however, it should be remembered that the validity of the cribbed value can be no higher than that of the base value.

51. Analysis of Textual Features

The analysis of cryptographic features is concerned with the recognition, use, and distribution of systems, the use of indicators, and the identification of practice and dummy traffic.

a. Recognition. The recognition of cryptographic systems is the first step in their analysis either for traffic analysis or cryptanalytic purposes. Where a discriminant in the clear is present, this becomes a simple matter; encipherment somewhat complicates the problem. But, if there is no discriminant, it is necessary to make use of other features. In the attack, traffic should be sorted down by net and then studied for individual peculiarities. For instance, the following differences may appear as to the type of text:

Net	Type of text	No. of messages
I	4-letter	65
	4-digit	40
	3-digit	29
II	4-letter	48
	5-digit	73
	4-digit	51

Since the net usually represents an order of battle entity it also often represents a crypto-entity. Therefore, all 4-letter traffic passing on Net I (barring the discovery of any further distinction) may be assumed to belong and may be considered for the moment a hemo-

REF ID:A58489

geneous system in itself. Further study is then necessary on the relationships of the two possible systems. Some elemental difference as to form may be apparent which will distinguish them as separate systems, such as the presence of a digit indicator in one. On the other hand, no distinction may be noted and it will be up to the cryptanalyst to determine if the same or different systems are involved. Routings should also be checked in this respect, a relationship between routings (as to echelon, for example) evidencing the likelihood of the same system though passed on different nets. Other factors, beside type of text, are of course also valuable. These include priorities, characteristic serial number ranges, or features of the text such as the nature of the indicators.

c. Analysis of Use. Tabulations of the nets and routings of traffic will often indicate the use of a system. A system, for example, passing only over a water transport net may be identified tentatively as a water transport system, or one used only between intelligence units may be considered a special intelligence system. Caution should always be exercised in making such assumptions because of the ever present possibility that the transmitting of certain traffic over specific nets may result from communications necessity. Peculiarities as to priorities, serial number ranges, and miscellaneous preamble classifications may also assist.

d. Analysis of Distribution. Directly related to the study of use is the analysis of distribution which can be accomplished on the basis of the same tabulation. For instance, a given system may be identified as Air Force and, furthermore, it may be discovered that its distribution is limited to a certain type of Air unit. The tabulation may be as follows:

Net	*Routings*	*Volumes*	*Other characteristics*
I	A–B	354	All traffic uses 5-digit message center numbers.
	A–D	251	
	B–A	240	
	B–D	223	
	C–A	112	
II	A–E	232	5-digit message center numbers.
	A–F	227	
	E–F	116	
	F–E	34	
III	A–G	249	5-digit message center numbers.
	B–G	245	
	G–C	121	
	G–H	112	
	H–G	78	

REF ID: A5384682

Nets I, II, and III are known to be high-echelon Air Force administrative nets. The system under study appears only on these nets and a further check reveals that it composes the bulk of the traffic passed, indicating that it is probably the high-echelon administrative Air system. The 5-digit message center numbers are of interest because numbers of this size appear only on traffic of Air division or higher. Furthermore, most of the routings involved are known to be locations of Air divisions and higher headquarters. Thus, the limits of the distribution of the system are established and now the reasoning may be reversed: any routing appearing with this system may be assumed to be an Air division or above. One-time pads lend themselves to this type of analysis because of their highly restricted distribution. Tabulation of the pad numbers against other features will generally define the users, and since these pads are usually used in only one direction, fix the originator and the one or more recipients.

e. Analysis of Indicators. Where indicators appear in the clear they may be of traffic analysis value. Observation will reveal any peculiarities of the indicators and, if present, they can be correlated with other features.

f. Analysis of Practice Traffic. Practice traffic can often be identified through a study of the text. Messages may be made up at random which generally leads to a patterning and repetition of combinations of letters or digits. Also since there is usually no desire to disguise practice traffic, it may carry a designation in the heading. On the other hand, skillfully designed practice traffic, particularly if an effort is made to conceal it, may be undetectable except for security breaches in operator chatter.

g. Analysis of Control Traffic. Control traffic, if properly handled, may prove very difficult to identify. The usual means of analysis, such as operator chatter, distinctive serial number ranges, etc., are always open. For example, very fast receipting for traffic and few services may indicate that the operators know that the traffic is dummy and are not particularly concerned about it. On the other hand, in an efficient control operation, the operators will not know that they are dealing with dummy traffic and hence will furnish no clues. Another method open to the analyst, however, is the study of traffic volumes and proportions. A level traffic volume on a number of circuits may indicate an attempt to conceal the natural peaks and troughs of a military operation. Moreover, high volumes in areas which other intelligence sources reveal as inactive should be viewed with suspicion. Abnormal rises of certain types of priorities of traffic should be carefully checked for evidences of spuriousness. Control operations carefully planned will take into account the

REF ID:A584489

proper proportions between the various types, but, because of their complexity, breaches of security will often occur.

52. Miscellaneous Items

Every communication system has its own peculiarities in its procedure and traffic. No rules can be given for their analysis except to observe the manner of use and to seek out the relationships between them and other features. It is hoped that the foregoing discussion of certain specific components will not only serve to set the pattern for research on these miscellaneous items, but, more than that, will encourage the traffic analyst to use his ingenuity in the development of new techniques.

Section III. NET RECONSTRUCTION

53. Introduction

The reconstruction of the radio net proceeds simultaneously with the analysis of radio operations. (Furthermore, it is a continuing task since net formations and operating data are seldom static factors.) As noted before, it involves the grouping of stations into nets, the building of the net structure, and the identification of the stations with geographic locations and military units. The resulting net diagram may be drawn in either a schematic or geographic design, according to purpose, and signal features added. This involves, in effect, the reproduction of the radio communications section of the enemy "Signal Operation Instructions" (SOI). These instructions are the orders issued setting up the required signal nets for each military operation and include the assignment of frequencies, call signs, schedules, and miscellaneous data. For a more complete description of the "Signal Operation Instructions," and for United States Army examples of same, see chapter 4, FM 24–16.

54. Grouping of Stations

a. The initial step in analysis is to list all stations and their correspondents. This will yield a rudimentary grouping. For example, the study of a day's chatter reveals—

ABC works DEF
ABC works GHI
ABC works JKL
DEF works MNO
DEF works PQR
MNO works PQR
XYZ works STU
XYZ works ?

REF ID: A384682

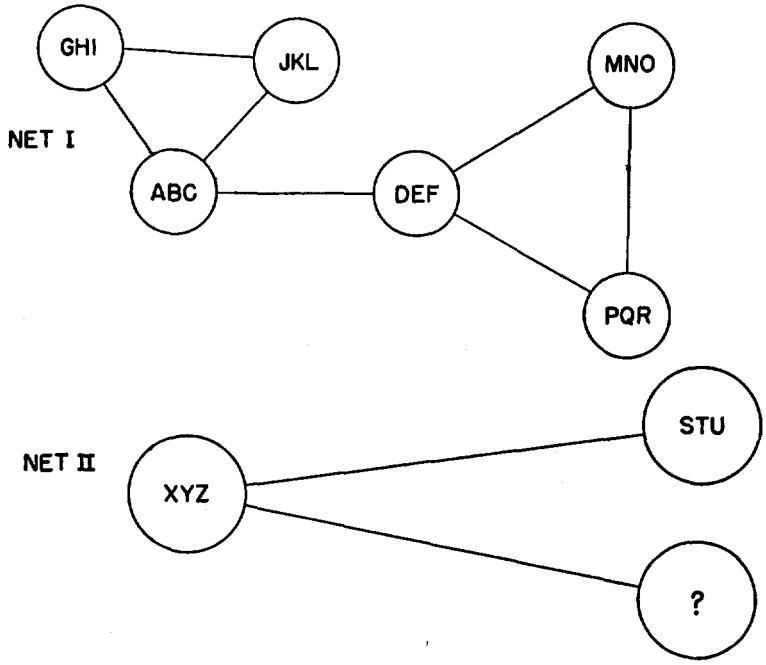


Figure 35.

Thus there are, for the moment, two separate groupings of stations with Net I apparently divided into two groups (fig. 35). It should be remembered that one day's intercept will rarely result in anything as complete as this, and that where daily changing calls are employed, the continuity techniques covered in paragraph 44 must be used. Missed calls present a similar problem. The next task is to study the characteristics of these stations as far as radio operation and procedure is concerned in order to refine the above groupings. It may be found, for example, on the one hand, that the ABC group and Net II exhibit such like characteristics that they appear to belong to the same net and that the connecting link between them has not yet been monitored; and, on the other hand, that the DEF group displays such different characteristics that it must be considered separate and that the DEF call must serve two groups (DEF–MNO–PQR and DEF–ABC).

b. The characteristics to be compared relate to all the features of radio operations:

(1) *Frequencies:*
(*a*) System of use.
(*b*) System of allocation.
(2) *Call signs:*
(*a*) System of use.
(*b*) System of allocation.

REF ID: A584682

(3) *Schedules:*
(4) *Procedure:*
(*a*) Call up.
(*b*) Order of traffic.

(c) Message externals (form and composition of preamble and postamble).

(*d*) Receipting.
(*e*) Corrections and services.
(*f*) Signing off.
(5) *Cryptographic systems.*

c. These items may be used as a check list. Stations, or circuits, do not have to agree in every particular to be grouped, but they should on the major features and, often, on the more characteristic of the minor. What constitutes this latter depends on the net itself. If, for example, strict instructions are issued by the net relative to the order of the preamble components, any deviation, however slight, may be taken as evidence of a separate net. On the other hand, if instructions are rather lax, deviations may not hold any significance. The traffic analyst seldom knows about the nature of the orders on operating procedure, but he can, through careful observance of the net, gain a general impression of how closely it is controlled and how well it is disciplined.

d. The following example illustrates the use of these techniques:

ABC works DEF
ABC works GHI
ABC works ?
XYZ works MNO
XYZ works PQR
STU works ?
? works ?

(1) *The diagrams* (see fig. 36).

(2) *The characteristics:*

(*a*) *Frequencies:*

Net I: Complex-sending Frequency Fixed.
Net II: Star Frequency Fixed.
Net III: Complex-sending Frequency Fixed.
Net IV: Complex-sending Frequency Fixed.

(*b*) *Call signs:*

Net I: Double-station Calls Monthly Changing.
Net II: Double-station Calls Monthly Changing.
Net III: Double-station Calls Daily Changing.
Net IV: Double-station Calls Monthly Changing.

REF ID:A584482

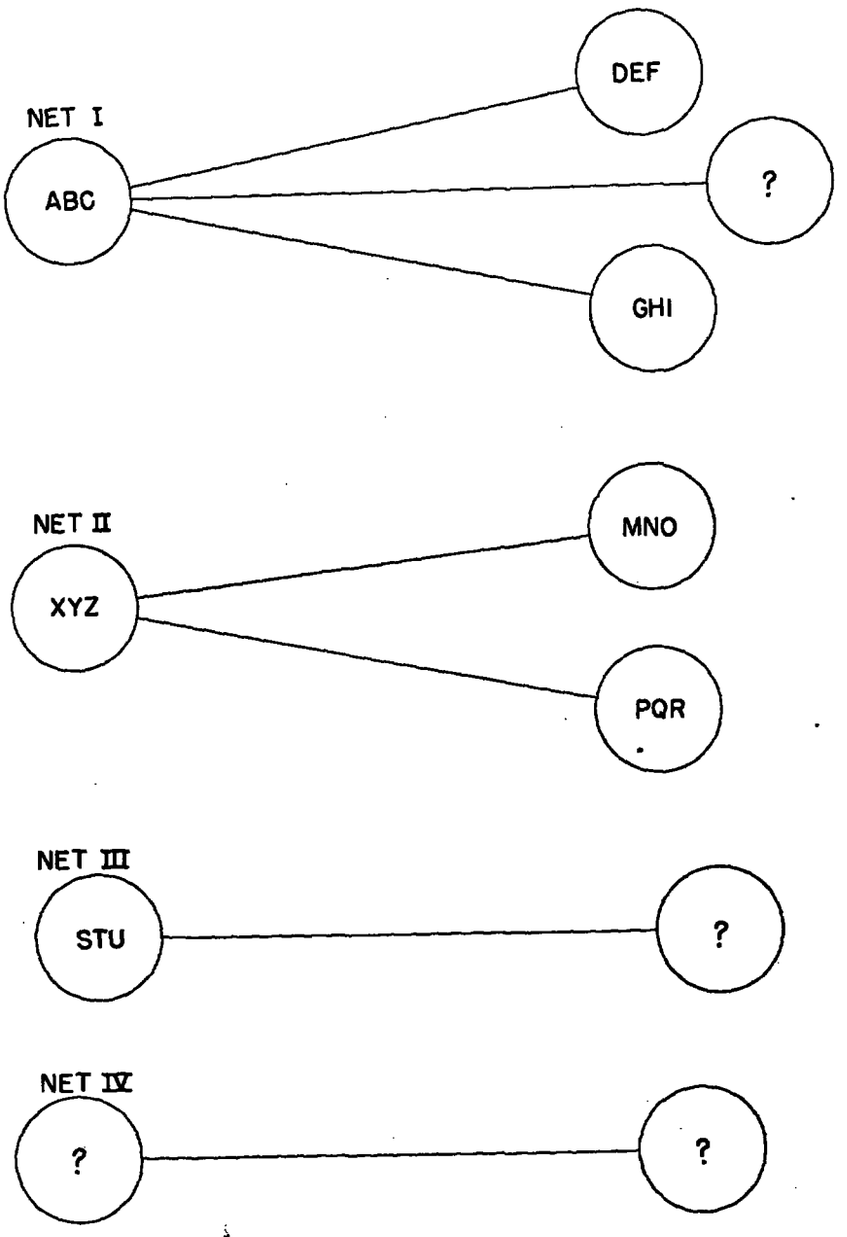


Figure 36.

REF ID:A58489

(*c*) *Schedules:*

Net I: Period.
Net II: Period.
Net III: Unrestricted.
Net IV: Period.

(*d*) *Procedure:*

All Nets: Q signals; International.

1. Call up:

All Nets: Usual.

2. Order of traffic:

All Nets: Precedence traffic first.

3. Message externals:

Net I:
Preamble: Circuit No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Net II:
Preamble: Circuit No.; Message Center No.; Group Count; File Date and Time; Routings.

Net III:
Preamble: In-desk No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Net IV:
Preamble: Circuit No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Separators: Same for all nets.

4. Receipting:

All Nets: Usual.

5. Corrections and services:

All Nets: Usual.

6. Signing off:

Net I: Usual.
Net II: Usual.
Net III: Makes next schedule.
Net IV: Usual.

(*e*) *Cryptographic systems:*

Net I: A, B, C, D.
Net II: A, E, F.
Net III: A, G, H, I, J.
Net IV: A, B, D.

e. It will be observed from the above that Nets I and IV have similar characteristics, and that II and III differ in certain important respects. Net II uses a net frequency. This alone would be insuffi-

REQ# 109:AS84819

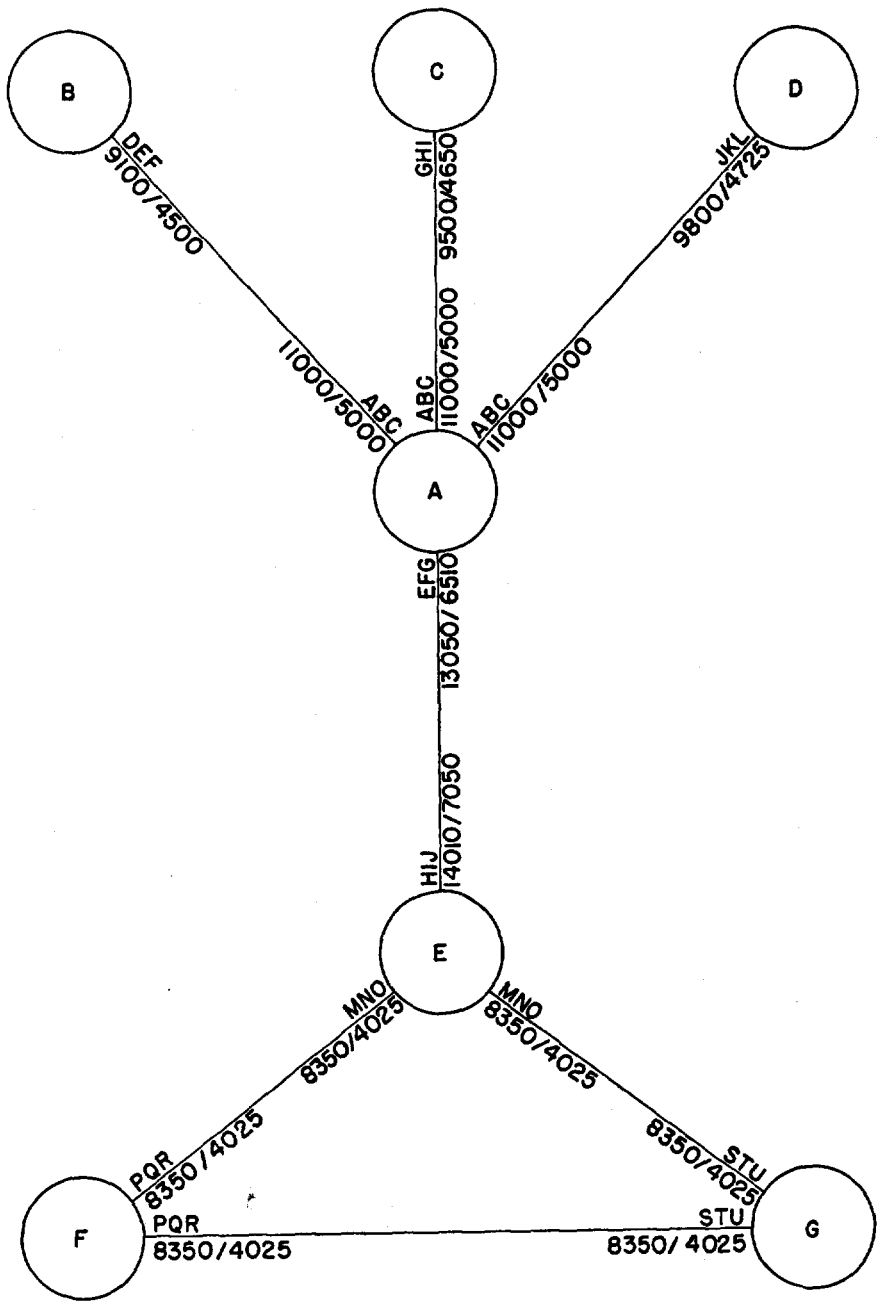


Figure 87.

REF ID: A58489

cient grounds for isolating it, but the position of the precedence in the preamble, and the use of different cryptographic systems furnishes enough additional evidence. Net III employs daily changing calls, usually adequate premise for setting a net apart. In this instance, added weight is given by the use of unrestricted signaling, the in-desk number, and the distinctive cryptographic systems.

55. Building the Net Structure

a. An elementary amount of net building is accomplished in the process of grouping the stations into nets. A number of additional techniques are now brought into play to complete the task. The crux of the problem involves the identification of different frequencies and calls with a station, in other words, that call ABC is at the same station as DEF, or that 11,000 kcs is at the same station as 9,050 kcs. When this has been done, the links and groups will fall into place and the net reconstruction be completed. It is difficult to set down definite methods to be pursued because much depends on the individual characteristics of the network. The following paragraphs discuss some of the principles involved and are suggestive of the general approach. Examples used are based on the diagram in figure 37.

b. Frequencies, Calls, Schedules. As a general rule, like calls or like frequencies may be assumed to be at the same station. Thus, in figure 37, the call ABC on frequencies 11000/5000 kcs was always considered the same regardless of station called. But caution should be exercised in arriving at this decision because it is always possible that no relationship may exist. A check of schedules is helpful. If ABC is heard working two different stations at the same time, it is likely that the two ABC's are separate stations. Other checks are traffic routings, cryptographic systems, etc.

c. Interlocking Serials. Where a radio station in-desk number is used, the serials out of different calls can be interlocked. When the serial is a message or signal center number, the interlocking technique may also be used, but account must be taken of the relay possibility. For instance, in figure 38 A and C are under analysis in an attempt to tie them together. Message center numbers on traffic out of ABC run:

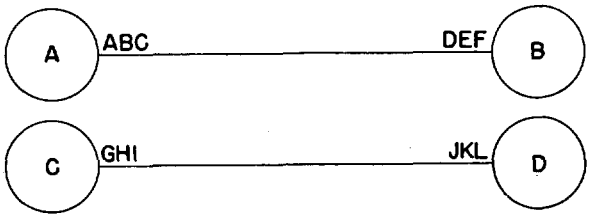


Figure 38.

RHQR 109:AD684682

1578	1607
1579	1608
1585	1609
1586	1610
1587	1629
1588	1630
1589	1631
1603	1641
1605	1642
1606	1643

Message center numbers on traffic out of GHI run:

1581
1582
1583
1584

But, if the latter traffic shows evidence of being relayed and, if there are no other grounds for identification, a conclusion cannot be reached. On the other hand, if it is found that nonrelay traffic on this net carries no routings, but that relay traffic does, and that all the messages listed above under both ABC and GHI have no routings, it may be assumed that ABC and GHI are co-located. Other types of serials, such as link numbers, generally cannot be used for this purpose.

d. Traffic Routings. On the theory that the predominant originator out of a call or frequency and the predominant destination into a call or frequency represent the location of the call or frequency, a tabulation of traffic routings may be used for net-building. For example, tabulations of routings relative to ABC and GHI reveal:

Call	*Routing*	*Volume*
Out of ABC	1234	75
	2345	43
	3456	10
	4567	3
Into ABC	1234	58
	2345	12
	4567	1
Out of GHI	1234	158
	2345	79
Into GHI	1234	101
	2345	39

The similarities in routings suggest their co-location though further proof is necessary for positive identification.

(1) Also useful is the system of omitting routings on local traffic. Calls of the same station will demonstrate similar relay routing lists

REF ID:A584482

with the station's own routing rather low in the tabulation. Book messages can be used as explained in paragraph 50*b* (2) (*b*).

(2) A somewhat different use of routings is in the inferring of links which have not been heard. For example, the routing 1234–6789 is noted on a message from A to B. 1234 has been located at C, but no link from C to A has been observed. Nevertheless, there must be some connection either through another station or directly. It is difficult to determine which is the case; a check of file time against intercept time will sometimes serve to indicate whether, considering the precedence of the message and the usual time lapses on the net, how many prior relays are likely. A tentative diagram could be drawn as shown in figure 39.

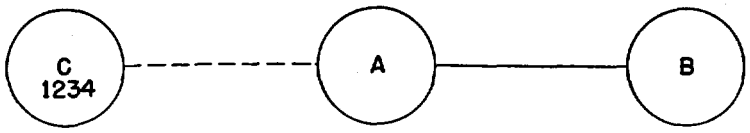


Figure 39.

e. Cryptographic Systems. On locally originated traffic, distinctive cryptographic systems, such as one-time pads, may be used to tie calls or frequencies together. As in the application of all message center features to radio stations, care must be taken to avoid relayed traffic.

f. Chatter. Items of chatter furnish important clues to net-building. In many instances, outright statements are made which relate one link to another. For example, ABC tells DEF, "At 1100 I have schedule with GHI." At 1100, JKL is heard calling GHI, indicating the identity of JKL and ABC. Mention of operators names or other local personalities also assist by the appearance of the same personality on different links.

g. Relayed Traffic. The study of relayed traffic presents one of the most important techniques in net-building. As messages pass from station to station, the net automatically reconstructs itself since it is only necessary to trace the messages' path to determine the structure. The chief caution to be observed is the possibility of having missed a relay, but this can generally be checked by differencing the intercept times. For example, a message is transmitted from ABC to DEF and an hour later from GHI to JKL. The diagram in figure 40 may then be drawn.

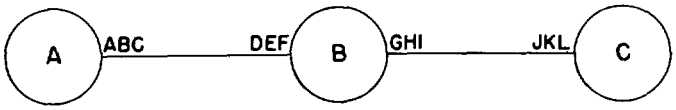


Figure 40.

REF ID:A684682

The possibility of the picture being as shown in figure 41, however,

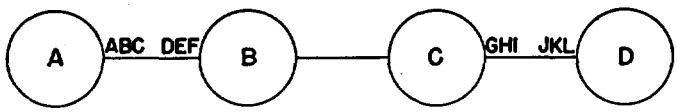


Figure 41.

does exist, but the short time lapse of one hour makes it unlikely that the extra relay took place. Of course, what constitutes a short time lapse is dependent on the habitual lapses and on the precedence of the messages under study.

h. COLLATERAL INFORMATION. Direction-finding is an important technique and, when the radio system is highly secure, may furnish the chief method of net building. Decode material, captured documents, prisoner-of-war reports, when available, should also be used to the fullest extent.

56. Location of Stations

The geographic location of stations is the third step to be performed in the reconstruction of the radio system.

a. IDENTIFICATION WITH A KNOWN ELEMENT. Identification with a known element is one of the chief means of locating the station. For instance, the tying-in of a station to an identified routing number will place the station. Similarly, calls, frequencies, serial ranges, and cryptographic systems which have been matched to locations may serve this purpose. The techniques involved can be derived from those discussed in this section and in section II. A validity should be attached to each station identification dependent on the weight of the identifying evidence.

b. CHATTER. Chatter often furnishes identifications through operator carelessness. Clues to locations, such as mentions of weather, local conditions, and similar items, should be carefully appraised.

c. DIRECTION-FINDING. Direction-finding is here listed separately because of its importance in the locating of stations. Often it is the only means available. This is particularly true in low-echelon nets where movement is liable to be frequent and where message externals are held to a minimum. It may sometimes be necessary to utilize a knowledge of order of battle, geography, and military strategy in connection with direction-finding. Bearings will usually give a general area, larger or smaller according to the distance from the target and the accuracy of the bearings, but seldom will pin-point a location. However, inference as to the most likely location within narrow limits is permissible provided it is backed with sound reasoning.

d. COLLATERAL MATERIAL. Order of battle information, decode

REF ID:A58489

material, captured documents, and similar items are often of great value in placing stations. For example, a division headquarters, whose radio station has been identified, moves to a new location. This new location is revealed by other sources. It may then be assumed that the headquarters radio station is also at this point.

57. Unit Identifications

a. The last step in the reconstruction of the radio system is the imposition of the order of battle. The order of battle underlies the entire net organization and each radio station must be identified with the units which it serves. In the high echelons, the nets are usually composed of large fixed installations which serve a number of units in the vicinity. Generally, however, there will be one major unit which the station represents. In the lower echelons, on the other hand, there will be a close correlation between unit and station. This is partially the result of the customary policy of manning large installations with an independent signal organization, while in the lower echelons the signal sections operate as an integral part of the unit.

b. The techniques of matching units with stations are only outlined below since it is felt that the preceding discussion sets the pattern of reasoning.

(1) *Identification with a known element.* This involves such items as call sign or frequency patterns which may be distinctive for certain commands or echelons, serial number ranges, routing systems, cryptographic systems, and procedural characteristics.

(2) *Chatter.*

(3) *Order of battle.* Beside the usual method of identifying a unit with a location and a location with a station, it is sometimes possible to force identification. For example, the order of battle information given in figure 42 is known, and a net is reconstructed as illustrated in figure 43.

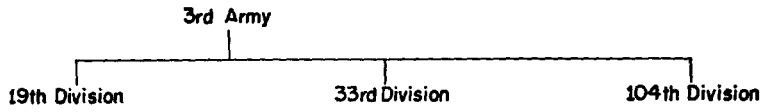


Figure 42.

It becomes apparent that station D is probably the 104th Division. In many cases, the echelon of command can be determined from the structure of the network and this may later lead to the identification with specific units. For example, the network shown in figure 44 is built.

REF ID: A384682

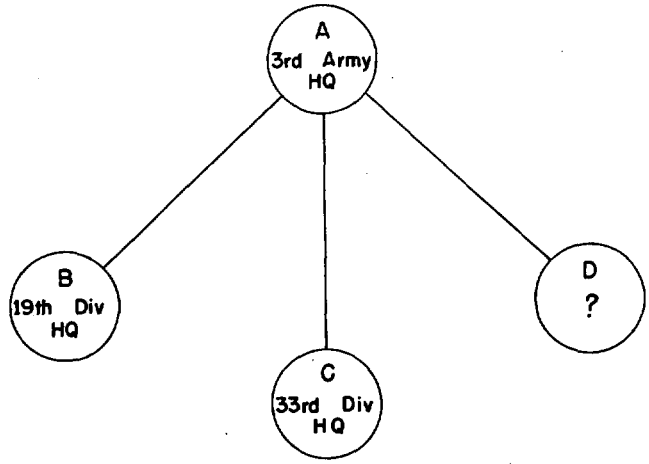


Figure 43.

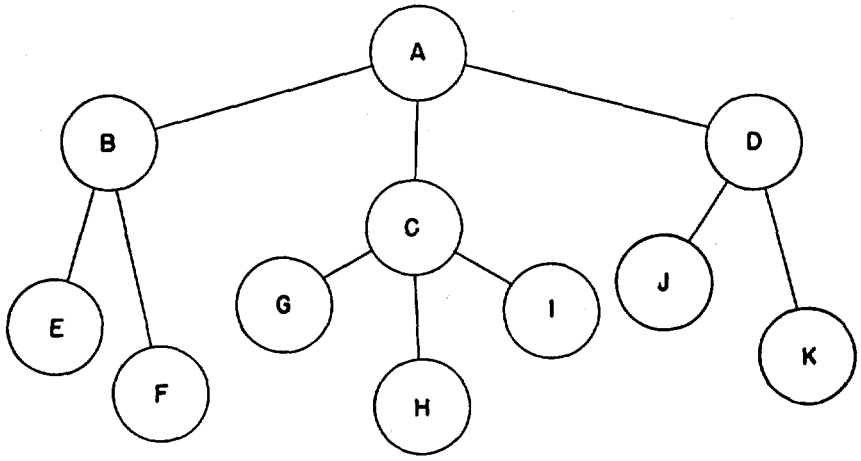


Figure 44.

It will be observed that A is probably the top headquarters, that B, C, and D are lower equivalent units, and that their out-stations are still further down the line. If anything is known of the order of battle in this area, it may be possible to match it with the net diagram.

(4) *Collateral material.*

58. Dummy Nets

Dummy nets and stations may be set up for the same purpose as that served by control traffic. Often when a headquarters is moved, a radio station is left operating at the former location to conceal the redeployment. Similarly, when it is desired to misdirect the

REF ID:A58489

enemy's attention, entire spurious nets may be employed to create the appearance of activity in an inactive area. The detection of such nets and stations may be difficult to accomplish and is largely dependent on the ability to uncover breaches of security resulting from careless chatter or ineptitude.

59. The Integrated Diagram

The immediate objective of the reconstruction of the nets is the production of the integrated network diagram which will serve as a

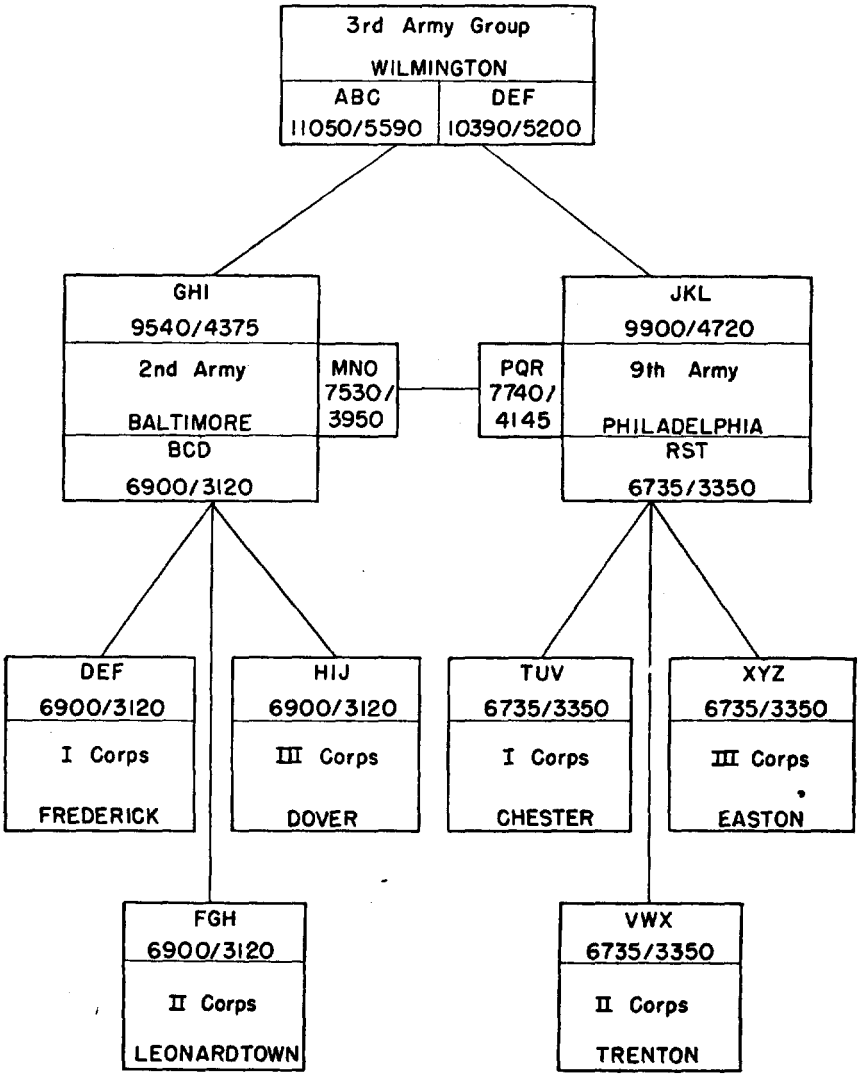


Figure 45.

REF ID: A5384682

backdrop for future study of the nets and for the production of intelligence and cryptanalytic aids. Because of the limitations of space and the complexities of some of the data, however, it is often not possible to include all the information necessary to a complete network picture in diagrammatic form. Therefore, certain basic diagrams may be produced either in schematic or geographic arrangement, and the omitted data supplied in accompanying charts. An example of such a basic diagram is given in figure 45. It will be noted that it contains order of battle units, locations, frequencies, and call signs, and is drawn schematically. Other data, which could be appended in chart form, might include range of serial numbers at each location or on each link, cryptographic systems used, and routings which appear or are identified with units or locations.

Section IV. METHODOLOGY OF ANALYSIS

60. Introduction

The preceding sections of this chapter dealt with the techniques of traffic analysis in regard to the study of radio operations and the reconstruction of the nets. In order to perform this analysis and achieve these ends, the proper machinery for processing raw material must be employed. This section is concerned with this machinery, and includes the processing of the chatter logs and the maintenance of appropriate files. The methods and forms outlined are only suggestive of the possibilities and changes should be made as necessary to meet individual situations.

61. Intercept Operator's Log

a. The raw material of traffic analysis is the chatter log. This is a complete record of the transmission as it is copied by the intercept operator and includes both traffic and chatter. An example of a portion of such a log follows (procedure is Q signals and international):

ABC	(2765 kcs) VVVVVVVVVV	
	DEF DEF DEF de ABC ABC ABC VVV QSV K	2133Z
DEF	(3152 kcs) VVVVVVVVVV	
	VVVVVVVVVVV ABC ABC ABC de DEF DEF	
	DEF VVVVV K	2135Z
ABC	V's QSA ? QSA ? K	2138Z
DEF	QSA4 QSA4 QSA? K	2139Z
ABC	QSA4 QTC 2 OP	
	QTC2 OP K	2140Z
DEF	QRV QRV K	2141Z

REF ID:A58489

ABC	QTC QTC	
	NR695 OP GR14 121541 BT	
	1904 2391 6025 8034 1709	
	6123 8051 6843 2967 1035	
	4114 EEEEEEEEE 4104 5281 7399	2144Z
DEF	3? 3?	
ABC	7399 1211 BT QSL? QSL? K	2145Z
DEF	R	2145Z
ABC	AS5 AS5 K	2146Z
DEF	OK OK OK	
	SAW TOM IN TOWN LAST NITE	2148Z
ABC	WHERE WAS HE GNG?	2149Z
DEF	31 Div They lost 2 ops in raid	2151Z
ABC	TOO BD AS AS	2151Z
ABC	QTC QTC QRV? K	2155Z
DEF	QRV QRV QRV K	2156Z

b. The important items of this chatter log must be extracted and recorded. The usual method to accomplish this is the use of the intercept operator's log on which is entered the significant features of the transmission as they occur. A sample log based on the above chatter is shown in figure 46.

c. The log is the basic analysis recording. Once it has been completed it should not be necessary, except in rare instances, to go back to the chatter logs. Consequently, considerable care should go into its preparation. It should contain all the data required for analysis and for the compilation of files.

62. Files

The contents of files are largely determined by the particular problem. It will generally be found advantageous, however, to maintain files based on the following:

a. Frequency. A master-frequency file containing a record of all frequencies, the time and date when first heard, associated frequencies, location, calls if reasonably fixed, net, etc.

b. Call Signs. A master call-sign file containing a record of all calls, date when first heard, associated calls, location, frequencies, net, etc. The information on the card here or in the frequency file may be kept to a minimum if one is adequately cross-indexed to the other.

c. Serial Numbers. Where practicable, files should be maintained on the various serial number ranges together with related features.

d. Routing System. A file of routing code groups with proofs of identifications.

e. Cryptographic Systems. A file of all cryptographic systems, how they can be identified, by whom used, for what purpose, and net.

REF ID: A584682

Date_____

GMT	Freq.	C/S	No.	Serial	Origin	Dest.	Remarks
2133	3152	ABC					V's DEF de ABC
2135	2765	DEF					V's ABC de DEF
2138		ABC					QSA?
2139		DEF					QSA4
2140		ABC					QSA4
2144		ABC	695				OP GR14 121541 1904 . . . . 7399 1211
2148		DEF					SAW TOM IN TOWN LAST NITE
2149		ABC					WHERE WAS HE GNG?
2151		DEF					31 DIV. THEY LOST 2 OPs IN RAID

Figure 46. Sample intercept operator's log.

In the case of distinctive features, such as one-time pads, files should also be maintained for each pad together with other pertinent data.

f. PROCEDURE. A file on the meanings of noninternational procedure signs and signals.

g. PERSONALITIES. All personalities appearing in traffic or chatter together with the connection in which they were mentioned. Personalities derived from other sources can be added to this file but they should be so marked.

h. ORDER OF BATTLE. All order of battle identifications originating with traffic analysis plus that available from other sources.

i. NET, GROUP, AND LINK. A running record should be kept on each net or, where necessary, group or link which will act as a history and also include the basic data for station identifications as to location and order of battle.

REF ID:A58489

j. Collateral Materials. Appropriate files should be maintained for all collateral materials. In the case of direction-finding, information must be organized to suit the particular problem. Files, as required, should also be maintained on solved messages, captured documents, and similar items.

REF ID: A5384682

CHAPTER 4

APPLICATIONS OF TRAFFIC ANALYSIS

Section I. INTERCEPT OPERATIONS

63. Introduction

Traffic analysis plays an important role in the direction of intercept. It furnishes the basic information necessary to the intercept station for the performance of its mission; its requirements are coordinated with those of intelligence and cryptanalysis for the purpose of prescribing cover and fixing priorities; and it checks certain phases of station performance. Depending on the nature of the organization, traffic analysis may also be responsible for the specific determination of missions for the intercept stations.

64. Intercept Information

a. The elementary function of traffic analysis in intercept control is the providing of basic net data to the stations. This includes chiefly frequencies, calls, schedules, and station locations. Other information may be added as required. A sample listing follows:

Locations	*Frequencies*	*Call signs*	*Schedules*
Hoboken	10500/5030	ABC	0100; 0300;
Zanesville	11350/6125	DEF	0500; 0700;
			1700; 2100
Hoboken	10500/5030	ABC	even hours
Overton	16400/7625	GHI	
Overton	16400/7625	GHI	0900; 1100;
Zanesville	11350/6125	DEF	1300; 1900; 2300
Star Lake	8430/4175	MNO	0700; 0900;
Ticonderoga	8600/4235	PQR	1800; 2200;
Star Lake	8430/4175	MNO	0400; 0600;
Buffalo	7550/3965	STU	1900

b. Technical reports may also be furnished to the intercept station. Certain items are fundamental. For instance, in the case of a changing-call system, the elements of the system are necessary for con-

REF ID:A58489

tinuity in cover; the same is true of frequency systems, procedure signs and signals, etc. In the determination of the type of materials to be forwarded, a balance must be struck between the requirements of security and those of intercept. All information is of use to the station, but some is more essential. Thus, it should be the policy to furnish everything that is available, consonant with security. Even much data which appear irrelevant may be of value if only to indicate to the intercept station the importance placed upon its product.

65. Types of Coverage

If it were possible to cover all desired nets or links twenty-four hours a day, there would be few problems to intercept control. Because of limited facilities and operators, however, such is not the case, and it becomes necessary to draw a number of fine distinctions with regard to types of cover and the order of priorities. Thus, cover may be divided into several types according to the purpose it serves.

a. FULL TIME. This is the highest of all intercept priorities (except in special instances) and consists of complete daily monitoring of each assigned net or link on all known schedules. The number of missions included in the full time classification should be sufficiently small to permit the monitoring station to cover all of them with ease so that, unless something entirely unforeseen intervenes, intercept is assured. Full time cover should never tax the maximum facilities and personnel of the station except under unusual circumstances, since positions should be reversed for other types of cover. These positions may, of course, be switched to full time if absolutely necessary.

b. SAMPLING. Nets or links which cannot be covered on full time may be put on sampling. The net is checked at regular intervals, the intercept station listening to several missions each day and rotating them until all have been monitored when the list repeats. This method yields some traffic on a variety of nets and enables the traffic analyst to keep abreast of current developments.

c. SEARCH. This mission consists of a search through a frequency band or bands for new transmitters and for changes of wave lengths. In the early stages of traffic analysis, this mission is of first importance since it serves to outline what is on the air.

d. PRELIMINARY CHECK. New frequencies discovered on search must be followed up to ascertain their genuineness and desirability. To accomplish this, they are placed on preliminary check, actually an extension of the search mission. If proved valuable, these links are then transferred to either full time or sampling.

e. SPECIAL CHECK. Special check is the complete cover of a net or link for a limited period of time. The check may serve a variety of

REF ID: A584682

purposes such as whether the link is still active, or what its schedules are, or whether it can be heard at the monitoring station.

66. Factors in Assignment

The main considerations in the assignment of missions to specific intercept stations are:

a. The ability of the station to hear at the times desired.

b. The availability of positions and personnel for coverage at the station.

c. The most economic use of the station's time. This involves the problem of the common transmitter which makes it desirable to assign an entire net, where possible, to one station. For example, in the net shown in figure 47 both the A–B and A–C link should be assigned

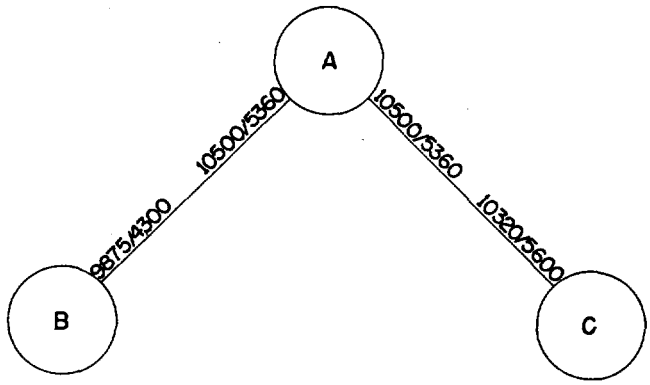


Figure 47.

to the same station, for by covering A throughout the day the activities of the net can be followed. On the other hand, if the intercept unit can hear A and B, but not C, it would become necessary to split the assignment. A second consideration in following this procedure is that the common transmitter arrangements tend to spread out until they include more links than can be handled at a single station. For example, C works another station on 10320/5600, B does likewise on 9875/4300, etc. Thus, a compromise assignment must often be devised.

d. The communication facilities between the station and the central analysis agency. In many instances, it is of prime importance that traffic arrive at a central point for analysis within the shortest possible time. For this reason assignments are sometimes made to the station which, though unable to provide the best cover, can forward the traffic the fastest.

REF ID: A584682

67. Factors in Priorities

The determination of priorities rests on the threefold requirements of intelligence, cryptanalysis, and traffic analysis. The traffic analysis needs are:

a. INTELLIGENCE. Traffic analysis, on its own, contributes to the intelligence picture and consequently is interested in seeing to it that the nets which yield the major portion of traffic analysis intelligence are adequately covered.

b. ANALYSIS OF RADIO OPERATIONS. In the study of certain elements of radio operations, intensive cover may be found valuable for limited periods of time, for example, the defining of schedules on a given net. Special check may be used to this end.

c. NET RECONSTRUCTION. Traffic analysis must maintain an up-to-date picture of all radio nets for the benefit of intercept control personnel regardless of the needs of intelligence and cryptanalysis (because those needs may change from time to time), and information must be available to permit the immediate assumption of coverage. In the reconstruction of nets of little current significance, or where the significance is unknown, special check is useful. Where nets have already been reconstructed and it is merely desired to watch them for changes, sampling cover is satisfactory.

68. Interpretation of Requirements

Besides making its own demands on intercept, traffic analysis frequently interprets the requirements of intelligence and cryptanalysis in terms of links and nets. For example, intelligence expresses interest in a given area; traffic analysis knows what links or nets to monitor in order to blanket the area. Or cryptanalysis wants more traffic in a given system, a certain routine message, or a type of isolog; traffic analysis knows what nets or links carry large portions of this traffic.

69. Station Performance

a. In order to insure proper performance by the intercept station and to check on the fitness of the assignment, coverage results are continually evaluated.

b. If a serial number, relative to the sending station, is available, it may be analyzed for missed traffic. Forms can be devised for the simple maintenance of this data which, in turn, can be obtained from the intercept operator's log. Other features, such as message center serials, may also be employed to check for missed traffic though care must be exercised in making use of them. Incidentally, there is a tendency to place emphasis on the volume of traffic copied at a station as a gauge of its efficiency. This attitude is to be discouraged since

REF ID: A684682

it is often necessary to monitor nets or links which yield little traffic, but do carry cryptographic systems of great cryptanalytic or intelligence value, or possess useful traffic analysis features.

Section II. APPLICATIONS TO CRYPTANALYSIS

70. Introduction

a. The relationship between traffic analysis and cryptanalysis is not easily defined. Often an arbitrary line must be drawn between them when it is desired to keep the functions separate, but it will be found necessary, whatever the distinctions made, for the cryptanalyst to be grounded in traffic analysis and the traffic analyst in cryptanalysis. This arises from the basic concept of traffic analysis and cryptanalysis as closely related processes with traffic analysis furnishing the frame of reference within which cryptanalysis is performed. The material supplied by traffic analysis falls into four main categories:

(1) General background information.
(2) Crib messages.
(3) Isologs.
(4) Chatter.

b. It should be borne in mind by the traffic analyst that the requirements of the cryptanalyst vary according to the stage of solution. At times, for example, an isolog may be of great value, at other times it may be of no use at all, and at still others it may be of potential use pending the development of the problem. Therefore the traffic analyst should gear his production in this field to the needs of cryptanalysis.

71. General Background Information

Traffic analysis furnishes a large amount of routine information relative to communication features which assist the cryptanalyst. Some of the main items are—

a. Routings. The knowledge of the origin and destination of traffic is fundamental.

b. Identification of Systems. Traffic analysis contributes to the identification of cryptographic systems where discriminants do not form an obvious guide and assists in the sorting of traffic into homogeneous groups.

c. Use of Systems. Through discovering the use of systems, and any peculiarities relative to it, traffic analysis aids the cryptanalytic processes. Specific applications, of course, depend on the nature of the system and the externals available.

RECD 10 : 2684682

72. The Crib Message

a. DEFINITION. When it is possible to assume portions of the underlying plain text through the recognition of external characteristics, a message may be termed a crib message. Crib messages may be divided into two main groups.

(1) Messages which display a direct external-internal relationship, as the correlation of an internal signature with the external originator.

(2) Messages which are proforma reports. These arise out of the command function which necessitates the rendering of reports both up and down channel. They are usually formalized to insure completeness and thus present several portions of predictable plain text. Reports are of two types: those periodically filed which are called routines, and those which are forwarded as the situation requires.

b. IDENTIFICATION OF CRIB MESSAGES. (1) *Use of originator or destination.* If traffic contains internal addresses or signatures, they may be assumed by a knowledge of order of battle in relation to the message routings. Thus, messages originating at Dallas, known to be the location of the 14th Division, may contain the "14th Division", its commanding officer, or one of its subordinate units in the signature position. The possibility of several units at a location should not be overlooked.

(2) *Use of serial number range.* The serial number range may be tied to an internal originator, and the signature on all traffic in the series may be predicted.

(3) *Use of other features.* In the study of internal originators and addresses, other features, such as cryptographic system, relationships between preamble originators and destinations, etc., should be correlated with the above. For example, a specific originator may be defined by a combination of routing origin, serial range, and cryptographic system.

(4) *Use of external patterns.* In the case of report messages, these can often be distinguished by the characteristics of the traffic which chiefly include—

(*a*) *Destinations.* Because the report is regularly rendered to specific people, the destinations will furnish one peculiarity of the message. If order of battle is known, the relationship between the originator and the destinations may be explained and it may even be found possible to identify the nature of the report. When the routine pattern has been established, the order of battle must be watched for changes which will result in alterations of the pattern.

Note. Crib messages bear a very direct relationship to the military situation and the order of battle since they are, particularly in the report type, instrument of the command process. Thus, a detailed knowledge of enemy dispositions and movements is essential to the study of crib traffic.

REF ID: A5384682

(*b*) *Cryptographic system.* Reports usually pass in the same system. But, where a change does take place and it can be recognized, the crib may assist in a solution of the new system.

(*c*) *Serial number range.* Because the same unit generally originates the same report, characteristic serial number ranges may be of value.

(*d*) *File date and time.* Reports which are routine in nature often exhibit a periodicity in the file date and time. For example, a ten-day report will be filed every tenth day, or a daily report as of 1700 will usually carry a file time after 1700 of that day.

(*e*) *Message length.* Because of the stereotyped nature of a report, the group count may show some consistency. In many cases, however, the length will be determined by the amount of information to be filled in, so while the message length acts as a guide, lack of regularity in this respect does not rule out the possibility of a genuine crib message existing.

(5) *Use of solved messages.* The reading of messages often produces crib traffic not previously suspected. This traffic should be studied and its characteristics noted to aid in future solution. Furthermore, it may be assumed that, if one unit originates a report, the same report is required of all other similar units. A check with order of battle will reveal the location of these other units and the specific traffic can be studied. For instance, a report may be observed from an oil depot to headquarters. This suggests that other oil depots also originate a similar report. These depots are then located and their traffic examined for the proper external characteristics as indicated on the decode.

73. The Isolog

a. DEFINITION. An isolog exists where the underlying plain text is encrypted in two different systems. There are many types of isologs depending on the nature of the cryptographic system, and it is hardly possible in this text to explore all the likely variations. Isologs arise from the cryptonets which, in turn, bear a close relationship to the order of battle. They are caused in three main ways:

(1) *The relay isolog.* When a message is relayed from one cryptonet to another, an isolog is likely. In figure 48, a message passed from A to C is reenciphered at B who holds both systems I and II. This type of isolog is usually formed by traffic passing up and down channels where reencipherment is necessary into simpler and simpler systems, the more forward the unit.

(2) *The book-message isolog.* Messages which are to be sent to a number of recipients in different cryptonets must be enciphered in different systems. In figure 48, for instance, if B wants to send the same message to A and C, the appropriate system is used for each.

REF ID:A58489

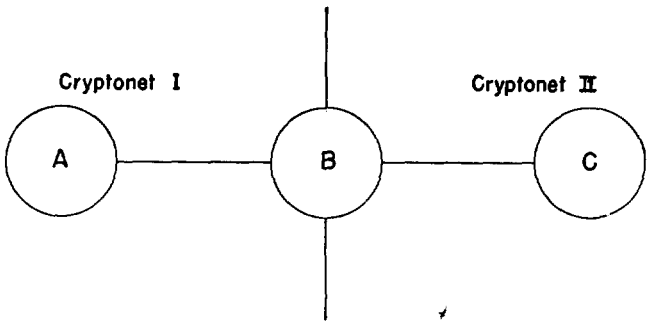


Figure 48.

(3) *Cryptographic error.* At times the code clerk will encipher a message in the wrong system. This will be refused by the receiver and the originator will reencipher in the correct system, yielding an isolog.

b. Identification of Isologs. (1) *Mechanical approach.* Isologs may be found by sorting traffic by originator and then looking for similar group counts and file dates and times. Where the two systems involved are not radically different in makeup, group counts should be close. Likewise, file dates and times, under most circumstances, will be similar.

(2) *Use of cryptonets.* A knowledge of cryptonets often simplifies the search for isologs. Certain locations, because they are in several nets, will be predisposed to the transmitting of this material. For instance, in the group of cryptonets shown in figure 49, the logical

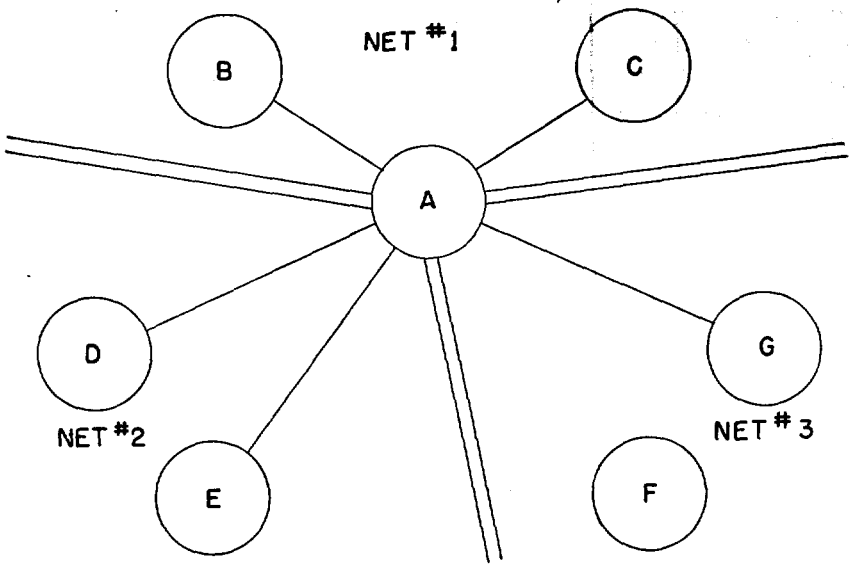


Figure 49.

REF ID:A684682

traffic to study for isologs would be messages received and transmitted by station A. Order of battle changes should be carefully followed for the cryptonets are formed by units, not radio stations, and the movement of a unit often means that a new location must be taken into account.

(3) *Use of refused traffic.* When messages are originally sent in the wrong system they will be refused or serviced, sometimes in the clear. This is a signal to watch for a retransmission of the traffic in its correct version. For this reason alone, it is important for the traffic analyst to be thoroughly familiar with procedure and the methods of servicing both encrypted and plain traffic.

74. Chatter

The study of chatter occasionally produces information of cryptanalytic value. Some of this material may be simply a discussion in the clear of cryptographic features by the radio operators. In other instances, the derivation of information may require some analysis.

Section III. APPLICATIONS TO INTELLIGENCE

75. Introduction

a. It is one of the chief objectives of traffic analysis to produce direct intelligence. Seldom will this be "pure" traffic analysis intelligence, but rather it will represent the fusing of traffic analysis data with material from other sources. In some cases, traffic analysis will furnish the initial indication; in others it will act as confirming evidence. The ability of traffic analysis to contribute to order of battle is based on the necessity for communication between military units and the fact that these communications are expressive of the enemy's dispositions and intentions.

b. The problem breaks down into three parts—

(1) Determination of order of battle relationships.
(2) Determination of movement.
(3) Identification of units.

76. Determination of Order of Battle Relationships

a. NET STRUCTURE. The net structure is one of the chief keys to the study of order of battle relationships. Methods of utilizing this element are covered in paragraph 57.

b. CONTACT RELATIONSHIPS. (1) *Traffic associations.* A study of the traffic contacts of any one point gives some indication of the nature and the echelon of the unit since every message passed implies a relationship between the sender and the recipient. In order to use

REF ID:A58489

this technique, some of the factors must be identified and the general principles of the enemy order of battle known. For example, if the following set of contacts are recorded over a period of time, and B, C, and D are all air transport units, it is likely that A is also—

Location A

To B	43 messages
To C	29 messages
To D	12 messages
From B	38 messages
From C	15 messages
From D	3 messages

Of course, other factors must be considered and these may alter the conclusion. In some orders of battle, for instance, certain of the air transport units may come under the command of an Army unit and A may represent this Hq. Thus, hasty interpretations relative to traffic associations cannot be made, and the use of all available collateral material is necessary. It may be noted, for example, that certain types of traffic associations are characteristic of units at divisional level. These associations may involve heavy traffic with Army Hq., somewhat lighter traffic with Army group, and a little traffic with characteristic points in the homeland. Similar patterns of other locations may indicate the presence of a division. There are so many variations to this type of analysis, and it is so dependent on the order of battle concerned, that it is not possible to develop the problem completely here, but the analyst's ingenuity should suggest the many applications.

(2) *Book messages.* Book messages are of particular interest because it is likely that some relationship exists between the various recipients which causes them to receive the same message. Some inferences can be made if something is known of any of the elements, such as the originator, a few of the recipients, or the use of the cryptographic system. A message, for example, passes from A to B, C, and D. A is an Army Hq., and B and C have been identified as divisional locations. Then it is probable that D is the third division of the Army. On the other hand, if the cryptographic system involved is one used by water transport units, it may be that D is included as a water transport unit which is handling the movement of some men for the two divisions.

c. Cryptographic Systems. If a cryptographic system is associated with a certain type of unit or with a definite unit and its subordinates, it will serve as an identification. For example, a system may be employed only by headquarters of Army or higher. Thus, every location sending in this system is probably Army or higher. Receiving in a system cannot be regarded as good evidence unless

REF ID:A58489

it happens in some volume, because of the possibility of a sender's error. To send in a system it must definitely be held, but receiving in it only implies that it is held. Systems restricted to Air Force, or supply, etc., may similarly be used to infer the nature of the unit at the location under study.

d. PATTERN OF SIGNAL FEATURES. These patterns may be of any type and concern almost any signal item. Three-letter calls, for instance, may only be assigned to Air Force units, or the manner of assignment may reflect the echelon of command. The same holds true for routing codes. Serial numbers which are 5-digit may be used by higher units, while 4-digit are reserved for division or below. Here again the possibilities must be developed to fit the individual case.

e. VOLUME OF TRAFFIC. The volume of traffic originated and received by any one point is indicative of its importance. Consideration, however, must be given to coverage facilities and assignments so that the traffic counts are not unduly weighted.

f. CHATTER. Security breaches involving units or clues to units occur occasionally, and chatter should be carefully scanned for them.

77. Determination of Movement

a. CHANGES IN NET STRUCTURE. It is apparent that most changes in net structure result from a more fundamental change in order of battle. Items to be noted include:

(1) Appearance of new stations on the net which often indicates the addition of a new unit.

(2) Disappearance of old stations which may mean the deactivation or move of an old unit.

(3) Moves of radio stations which usually denote the redeployment of the using unit. In moves of this sort, there is often a period of several days, between the closing of the old station and the opening of the new, when the unit will be off the air.

b. CHANGES IN CONTACT RELATIONSHIPS. (1) *Traffic Associations.* Any change in the traffic associations of a location should be carefully examined as it may indicate a resubordination or the move of a unit. For example, Army HQ at A regularly sends traffic to a division HQ at B. This contact later changes, A to C, indicating the move of Army HQ to C or else the division to a different Army if A continues to show the characteristics of an Army Hq.

(2) *Book messages.* Changes in the pattern of recipients of book messages indicate underlying order of battle changes. This is particularly applicable in the case of routine traffic where a distinguishable message passes regularly to several locations. If, for instance, a routine situation report sent daily from A to B, C, and D, changes to B, C, and E, it may be assumed that the unit at D has shifted to E.

c. CHANGES IN TRAFFIC VOLUMES. Changes in the traffic volumes

REF ID:A58489

handled at a point indicate some sort of activity though other techniques must be employed to determine the nature of the activity. In order to watch for changes, a standard of traffic volume into and out of each location is established as normal. Any rises or drops suggest changes in the situation. For example, a location handling an average of three or four messages per day suddenly jumps to 50. It is apparent that units are moving in the vicinity, that preparations are under way for a move, or that it has assumed a more important role. And the possibility that it may be caused by the use of control traffic for the purpose of deceiving the analyst should not be overlooked. As a corollary to this, changes in the volumes of precedence traffic, or in the usual file times, may also be of significance.

d. Moves of Serial Ranges. A message or signal center serial range, which is sufficiently distinctive, may be used as an indication of unit moves. For instance, an Army located at A is employing message center serials running 563–581 on the 10th. On the 12th, messages with serials 585–593 are observed originating at B, suggesting the Army's move to B.

e. Moves of Cryptographic Systems. Similar to the move of serial ranges, the move of a characteristic cryptographic system often signifies an order of battle change. A one-time pad, for instance, held only by a certain division and appearing on messages out of location A, suddenly is noted out of location B.

78. Identification of Units

The initial identification of units usually does not result from traffic analysis. Rather traffic analysis furnishes the means for following a unit about, once it has been identified. But, through the study of net, contact, and cryptographic associations (and the use of other signals features when applicable) it is often possible to define the nature and the echelon of a unit at a given location, and in some cases to name it. Chatter, also, may furnish the specific designations of units through breaches of security.

79. Conclusion

The traffic analysis techniques discussed in this manual require considerable study. It is difficult to cover a subject of this type, where so many individual bits and pieces must be fitted together, in text form since, in order to convey effectively the concept of traffic analysis, no one part should be presented before the other but rather the whole presented at once. For this reason, the text should be read and re-read. It is further to be noted that this manual is chiefly a theoretical text, that the field is still expanding, and that it is the task of the individual analyst to devise the applications best suited to his specific problems.

REF ID:A58489

APPENDIX

REFERENCES

FM 7–24	Communication in the Infantry Division.
FM 11–22	Signal Operations in the Corps and Army.
FM 17–70	Signal Communications for Armored Units.
FM 24–6	Radio Operators Manual, Army Ground Forces.
FM 24–10	Combined Radiotelegraph (W/T) Procedure.
FM 24–16	Signal Orders, Records and Reports.
FM 24–17	Signal Center and Message Center Procedure.
FM 24–18	Radio Communication.
TM 1–465	Air-Ground Communication.
TM 11–454	The Radio Operator.
TM 11–455	Radio Fundamentals.
TM 11–462	Signal Corps Reference Data.
TM 11–484	Elementary Military Cryptography.
TM 11–485	Advanced Military Cryptography.
JANAP 122	Joint Communication Instructions—Part II—Security.
JANAP 127	Joint Communication Instructions—Part VII—Joint Tape Relay Procedures.
JANAP 143	Communication Security.

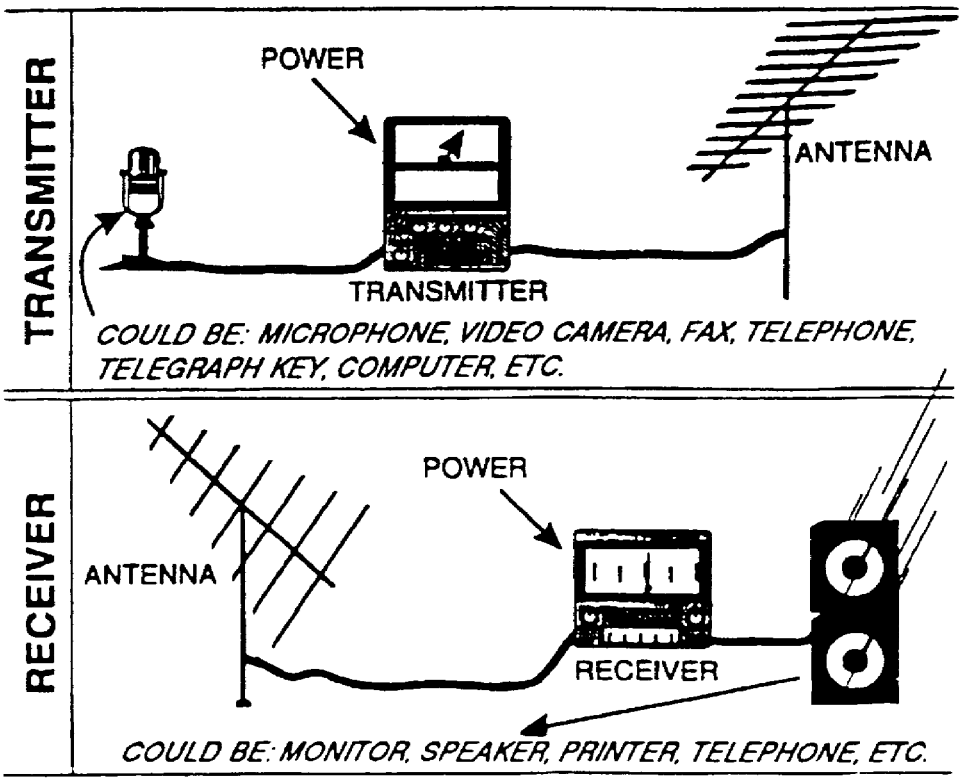
U. S. GOVERNMENT PRINTING OFFICE : 0—1950

SUBCOURSE
IT0302

EDITION
C

US ARMY INTELLIGENCE CENTER

INTRODUCTION TO RADIO DIRECTION FINDING



THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT
ARMY CORRESPONDENCE COURSE PROGRAM

AIPD
READINESS/ PROFESSIONALISM
THRU GROWTH

INTRODUCTION TO RADIO DIRECTION FINDING

Subcourse Number IT0302

EDITION C

US ARMY INTELLIGENCE CENTER
FORT HUACHUCA, AZ 85613-6000

5 CREDIT HOURS

EDITION DATE: AUGUST 1999

SUBCOURSE OVERVIEW

This subcourse is designed to teach you the basic concepts and minimum equipment requirements of radio direction finding (DF) as it is practiced in the Army today. The applications of DF are varied, with each application having its own requirements. You will be introduced to the basic terms and concepts of DF necessary to understand its application to other specialists or to prepare for the complete DF course.

There are no prerequisites for this subcourse.

TERMINAL LEARNING OBJECTIVE

ACTION: You will select the basic terminology/concepts of DF, and select the basic equipment requirements for a radio DF system and certain concepts needed for discussion of DF equipment.

CONDITION: You will use information provided in this subcourse.

STANDARD: To demonstrate competency of this task, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications:

FM 34-40-0(U)	FM 11-666
FM 11-64	FM 30-476
FM 34-86	

TABLE OF CONTENTS

Section	Page
Subcourse Overview	i
Lesson 1: Basic Terminology	1-1
Introduction	1-1
Part A: Radio Wave Propagation	1-2
Part B: Properties	1-13
Part C: Elements	1-18
Practice Exercise	1-23
Answer Key and Feedback	1-26
Lesson 2: Equipment Requirements	2-1
Introduction	2-1
Part A: Components	2-2
Part B: Definitions	2-4
Part C: Requirements	2-7
Practice Exercise	2-19
Answer Key and Feedback	2-22

LESSON 1

BASIC TERMINOLOGY

CRITICAL TASK: None

OVERVIEW

LESSON DESCRIPTION:

Upon completion of this lesson you will be able to show your understanding of the basic terminology and concepts of direction finding by matching terms and concepts with correct explanations.

TERMINAL LEARNING OBJECTIVE:

TASK: Identify with the basic terminology and concepts of direction finding.

CONDITION: Given the information provided in this subcourse.

STANDARD: To demonstrate competency of this task, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications:

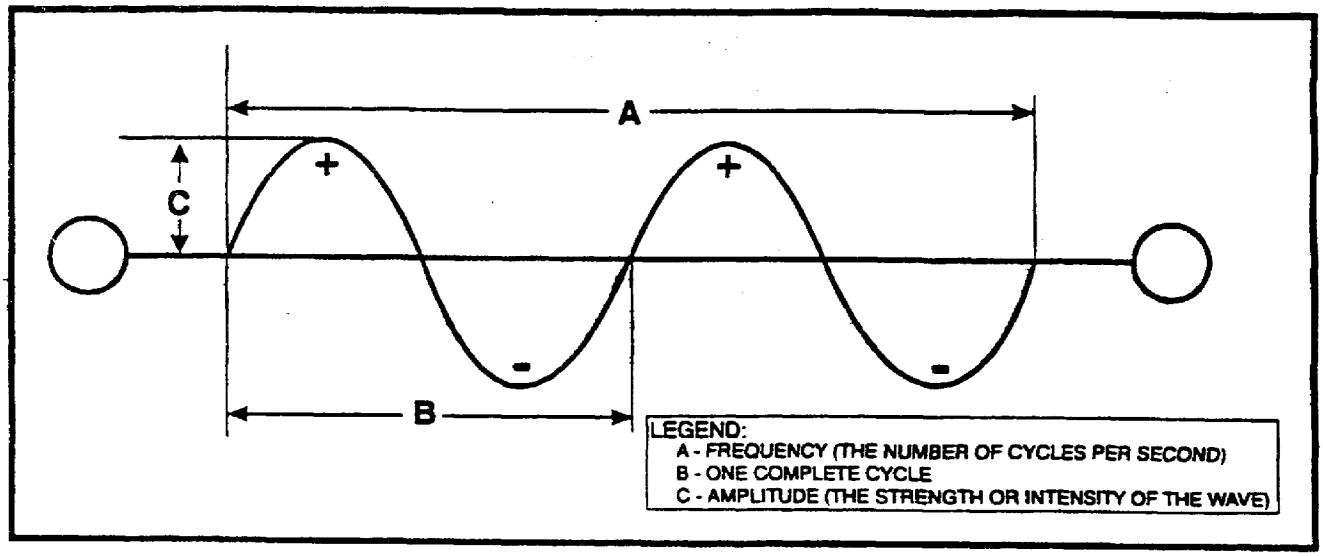
FM 34-40-0(U)
FM 11-666
FM 11-64
FM 30-476
FM 34-86

INTRODUCTION

Radio direction finding deals with the direction of arrival of radio waves. Therefore, it is necessary to understand the basic principles involved in the propagation of radio waves from the transmitting station to the DF equipment.

PART A: RADIO WAVE PROPAGATION

The distance traveled by a radio wave during a single cycle is known as a wavelength. A wavelength can be expressed in any unit of measure. However, it is normally expressed in meters. The number of complete waves that move past a given point in one second is called frequency. A unit of frequency is called Hertz (Hz). One unit is equal to one cycle per second Figure 1-1). The radio wave's strength or intensity is called its amplitude.



The radio wave, which is electromagnetic in nature, consists of an electrical field (E field) and a magnetic field (H field). Each field supports the other, and neither can be propagated by itself. Table 1, lists frequency bands, their designators, and the commonly accepted limits of each band.

The direction of the E field of a radio wave, relative to the ground, determines the polarization of the wave. Polarization can either be horizontal, vertical, or a mutation which adopts portions of vertical and horizontal. The later results in a circular or hybrid form of a wave. If a whip or other vertical type transmitting antenna is used to propagate radio waves, the transmitted wave is considered to be vertically polarized. If the transmitting antenna is horizontal, relative to the earth's surface, the transmitted wave is horizontally polarized.

Table 1. Frequency range and band designator.

FREQUENCY RANGE		BAND DESIGNATOR
3-30	kilohertz (kHz)	very low frequency (VLF)
30-300	kHz	low frequency (LF)
300-3000	kHz	medium frequency (MF)
3-30	megahertz (MHz)	high frequency (HF)
30-300	MHz	very high frequency (VHF)
300-3000	MHz	ultra high frequency (UHF)
3-30	gigahertz (GHz)	super high frequency (SHF)
30-300	GHz	extremely high frequency (EHF)

To illustrate vertical wave polarization, imagine a rope lying reasonably straight on the ground. One end is attached to a tree or other support (Figure 1-2). If the loose end of the rope is raised, tightened, and given a violent up and down motion, a series of undulationing waves will travel along the rope. The movement of the waves will be vertical to the earth and clearly visible.

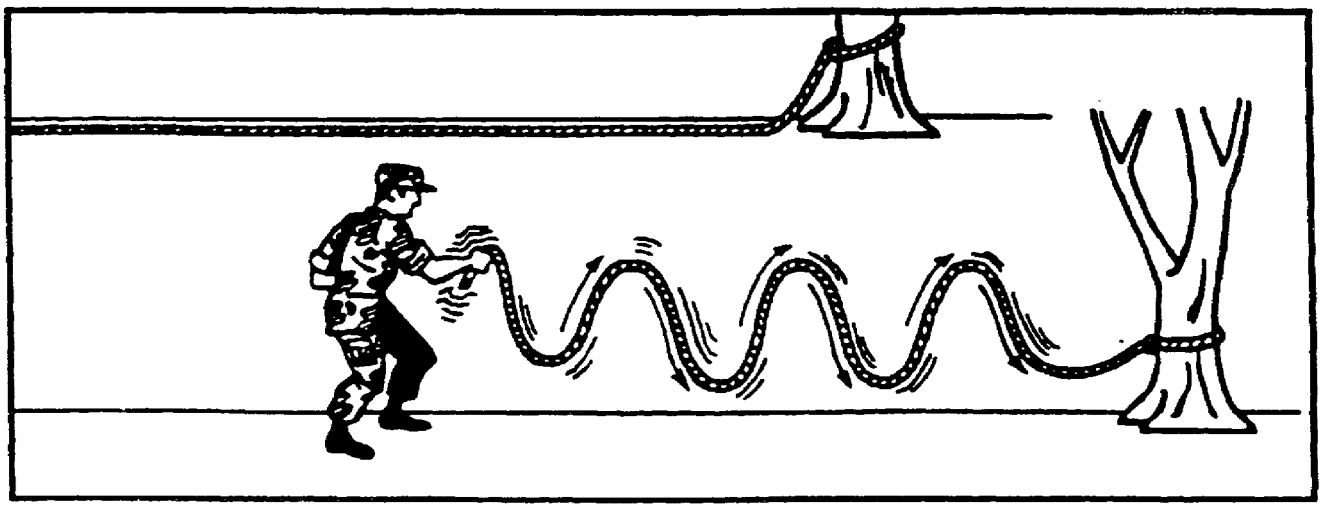


Figure 1-2. Vertical wave polarization.

If the same rope had a similar movement applied in a horizontal manner, the waves would be in a horizontal plane. These waves would be called horizontally polarized (Figure 1-3).

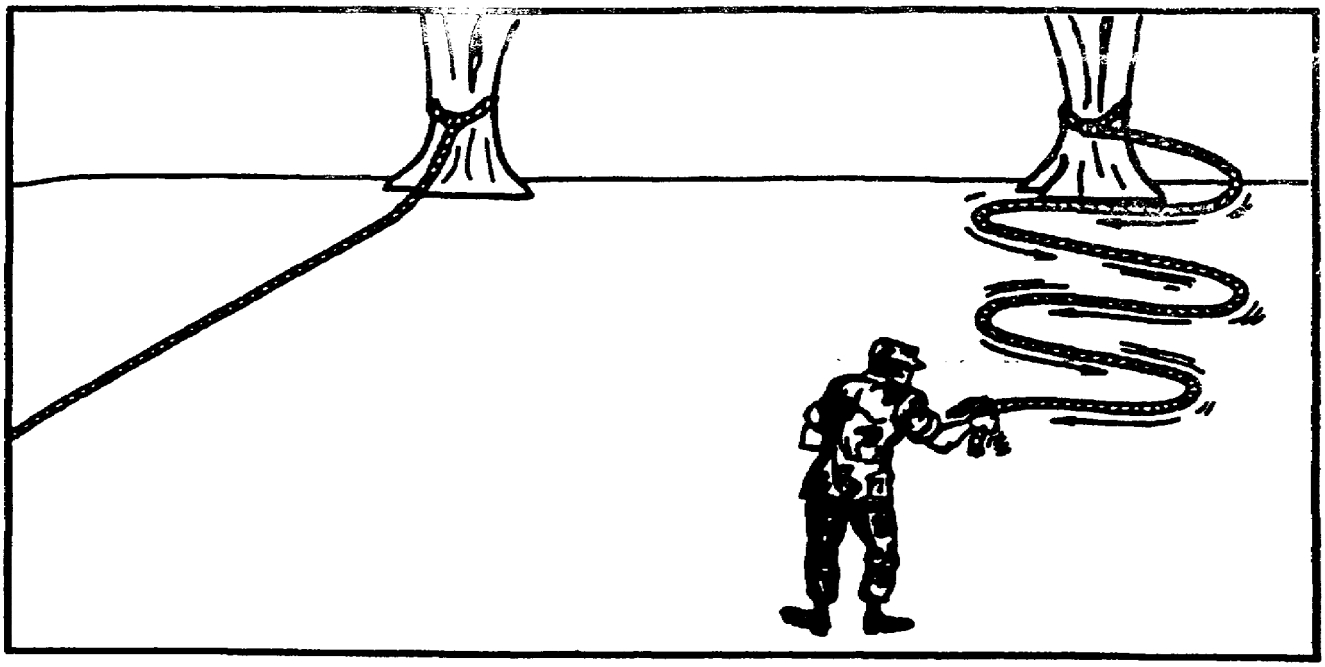


Figure 1-3. Horizontal wave polarization.

Wavelength, frequency, and polarization are all essential elements of the actual wave and are factors which affect the radio wave propagation. The simplest form of propagation is through space. Radio waves tend to travel in straight lines unless they are acted on by some force. They can be reflected off the surface of any sharply defined object such as the earth's surface. The radio waves can also meet other obstructions or objects that will scatter or reflect the signal. They can be reflected, refracted, or diffracted.

Radio waves are reflected similar to light waves traveling at the same speed. Although light waves can be seen, radio waves must be detected by electronic equipment. Figure 1-4 illustrates how radio waves are reflected off the ionosphere.

Refraction can best be illustrated by a pencil held obliquely so that a portion of it is beneath the surface of some water (Figure 1-5). From most viewpoints, the pencil will have the appearance of being bent at the point where it enters the water. This effect is because light waves travel more slowly in water than air.

Diffraction of a radio wave is the phenomena of bending the wave around a solid object. The lower the frequency or the longer the wavelength, the greater the bending of the wave. Therefore, radio waves are more readily diffracted than light waves. Sound waves are more readily diffracted than radio waves. This illustrates why sound waves can be heard around the corner of a large building.

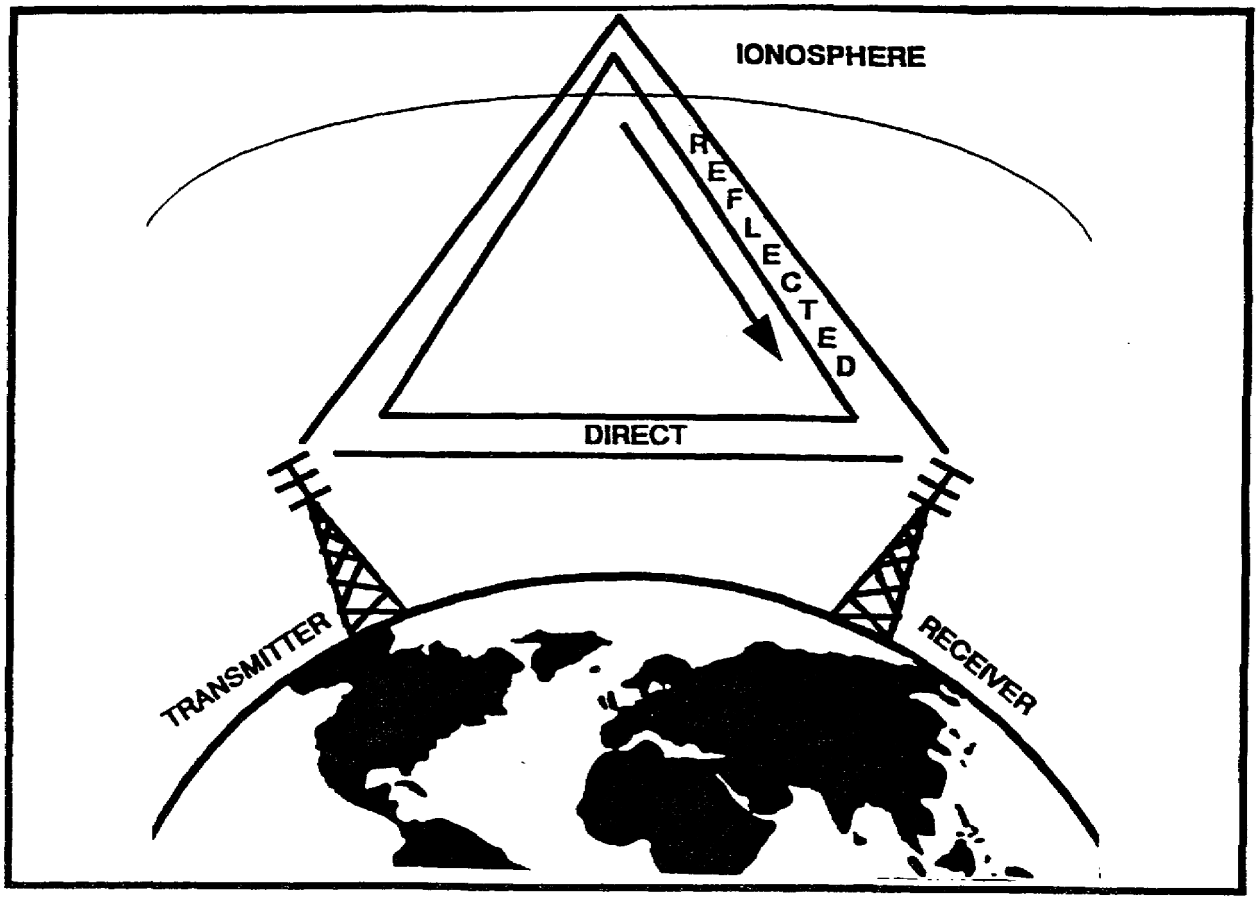


Figure 1-4. Reflected radio waves.

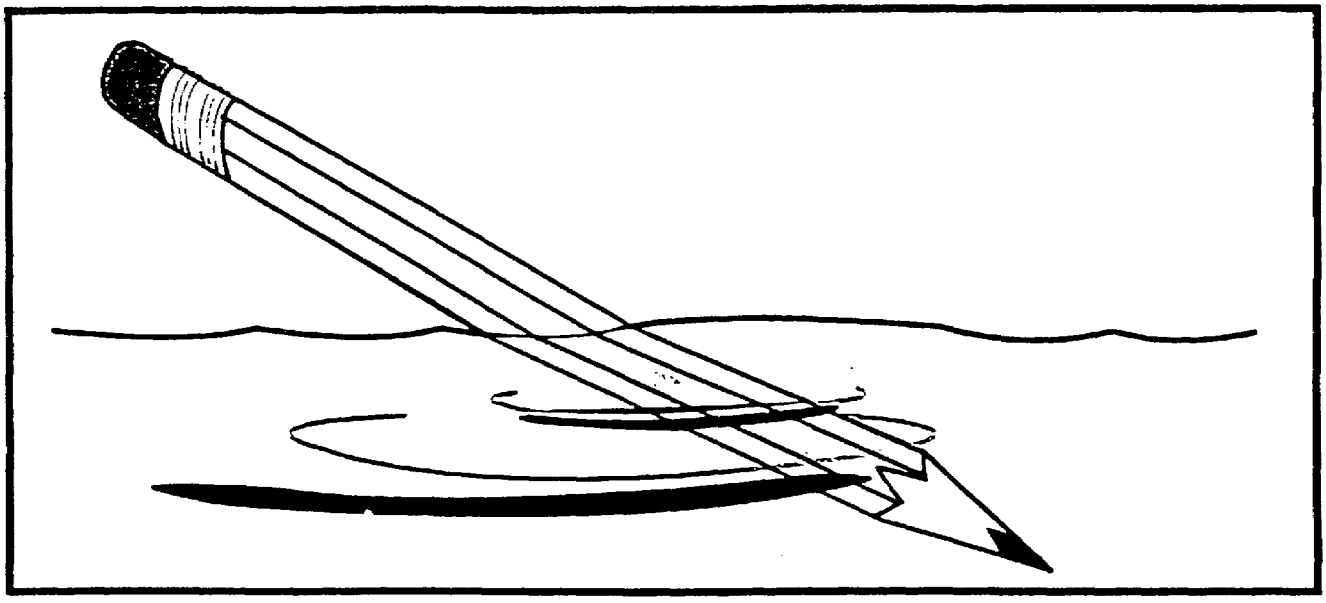


Figure 1-5. Refraction of a pencil.

The earth's atmosphere plays a crucial role in long distance radio communications. Radio waves may be reflected in the atmosphere and returned to earth. This technique is discussed later in this lesson. As shown in Table 2, the atmosphere consists of multiple layers, of which only a few have any discernible effect on radio waves. The ionosphere is the primary layer that is used to return a radio wave back to earth.

Table 2. Characteristics of the atmosphere.

ATMOSPHERIC REGION	LOCATION (Km)	FEATURES	EFFECT ON COMMUNICATIONS (Radio Frequency)
Ionosphere	Extending 50-600 km from the earth's surface.	Electrically charged set of layers, with large amounts of free electrons.	Excellent reflection/refraction of MF and HF signals. Some VHF may be propagated as well. Primary medium for sky wave communications.
Stratosphere	Extending 15-50 km from the earth's surface.	The only isothermal region of the atmosphere.	No effect.
Troposphere	From earth's surface to 10-15 km.	Lowest region of the atmosphere. Sustains life. Temperature decreases with increasing altitude.	Negligible effect. Allows direct, surface, and ground wave communications of all frequencies.

The ionosphere is a region of ionized (electrically charged) gasses located approximately 50-600 kilometers (km) above the earth's surface. As illustrated in Table 3, there are essentially four layers (D, E, F1, and F2) of the ionosphere which affect communications and DF. These layers vary in ionization and height above the earth's surface, depending on the amount of exposure to the sun.

The ionosphere is formed when extreme ultraviolet light from the sun strips the electrons from neutral atoms in the ionosphere. Thus, the electrons become free (unbound), and the remaining atom becomes positively ionized. The free electrons reflect/refract radio waves of a certain frequency. Due to this process, the E and F layers become positively ionized.

However, the free electrons may attach to neutral atoms. When such attachments occur, the atoms become negatively ionized. This process is common in the D layer, making the region of the ionosphere negatively ionized. Factors which influence the ionosphere and its effect on radio waves include--

- The time of day.
- The seasons of the year.
- Solar flares.
- Magnetic storms.
- Certain man-made disturbances such as nuclear detonations.

An important relationship between radio waves and the ionosphere is that the higher the frequency, the less its tendency to bend. Depending upon ionospheric conditions and the angle of the signal's arrival at the ionosphere, the bending may be slight. The radio waves may not be sent back to earth (Figure 1-6).

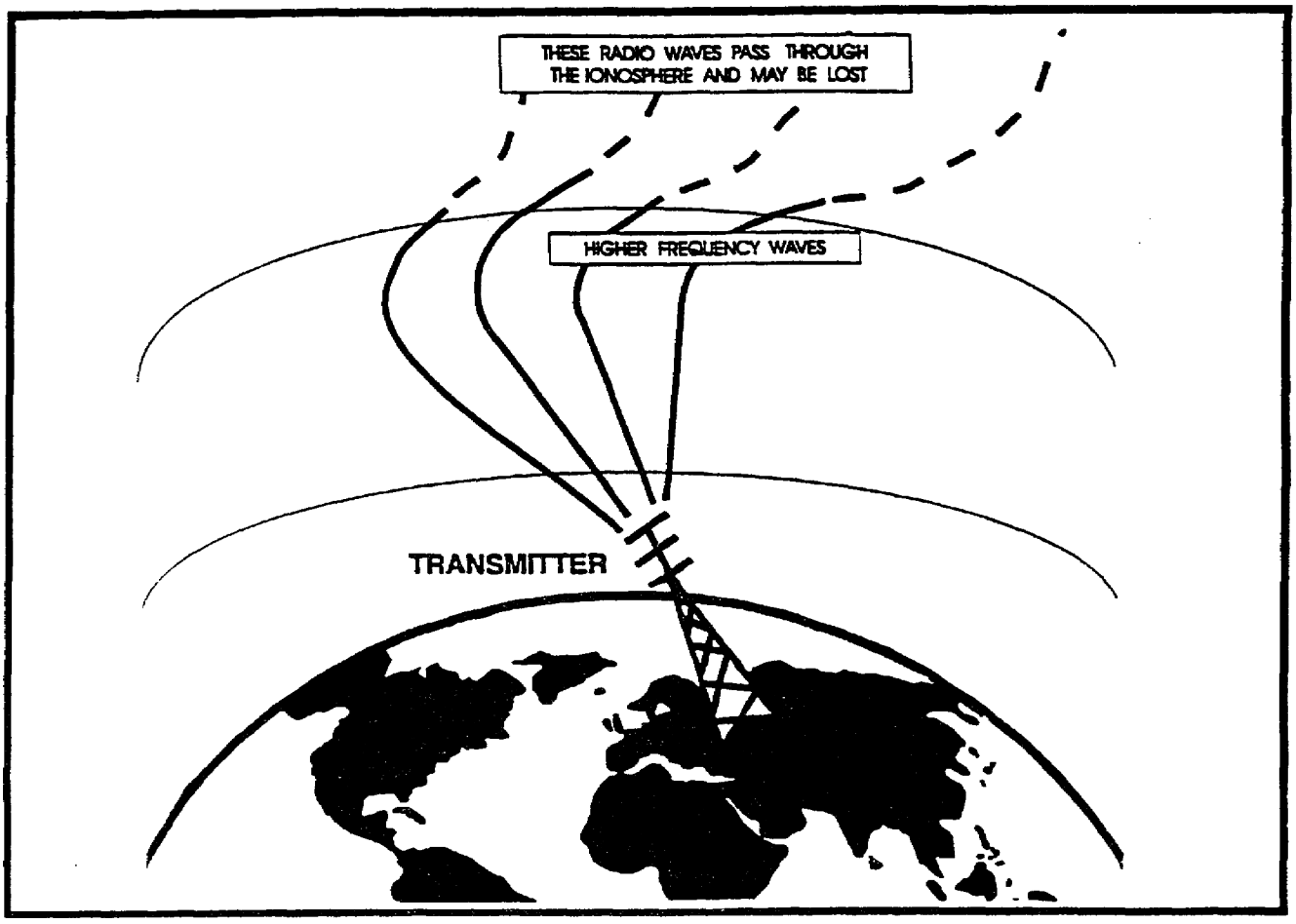


Figure 1-6. High frequency wave penetration.

During daylight hours, the ionosphere is subject to full ultraviolet output from the sun. Therefore, the D, E, F1, and F2 layers reach their full potential. At night, the composition of the layers of the ionosphere changes as the F layers combine. Therefore, higher radio frequencies are more likely to penetrate the ionosphere and be lost. As a general rule, lower communication frequencies are used during the night.

Conversely, during the day when ionization of the atmosphere is more intense, higher communications frequencies can be used without undue loss of the signal. This is because penetration of the ionized layer is at a minimum. Changes in the relative proximity of the sun to the earth will also cause gradual changes in the ionosphere.

Table 3. Characteristics of the ionosphere.

IONOSPHERIC REGION	LOCATION (Km)	FEATURES	EFFECT ON COMMUNICATIONS (Radio Frequency)
D	50-100 km	Layer closest to earth. Negatively ionized layer, with relatively little free electrons. Exists during the day.	Primarily acts to absorb radio waves. Small amounts of refraction are possible, but unpredictable.
E	100-200 km	Positively ionized with varying amounts of free electrons. State changes with temperature, angle of the sun, magnetic fields, and time of day. Exists during the day.	Erratic behavior. Sometimes reflects/refracts radio waves in MF, HF, and lower VHF bands.
F	145-400 km (F1-145-200 km) (F2-240-400 km)	Very positively ionized with large amounts of free electrons. During the day, this region separates into the F1 and F2 layers. The F region decreases in ionization and increases in altitude at night.	Primary means of reflecting/refracting MF and HF signals in sky wave propagation. At night, behavior becomes slightly erratic, but communications distances are much greater.

The longer exposure of the ionosphere to the sun in the summer causes a greater degree of ionization during the night and day. Therefore, higher frequencies may be used for summer operations.

Remember, however, that the actual number of layers, their heights above the earth, and the relative intensity of ionization present will vary. They vary from hour to hour, from day to day, from month to month, and from year to year.

There are three distinct paths that a radio wave may take to reach the receiving antenna. They are--

- Direct.
- Reflected.
- Refracted.

The direct and reflected paths are shown in Figure 1-7. They are purposely exaggerated to enable the reader to clearly grasp the differences.

The direct path goes directly from the transmitting to the receiving antenna. The reflected path bounces off the ionosphere or the surface of the earth at the same angle at which it arrives and continues to the receiving antenna (angle incidence=angle of arrival). The refracted path is the path caused by the bending of the waves in the same manner light waves are bent when seen through water.

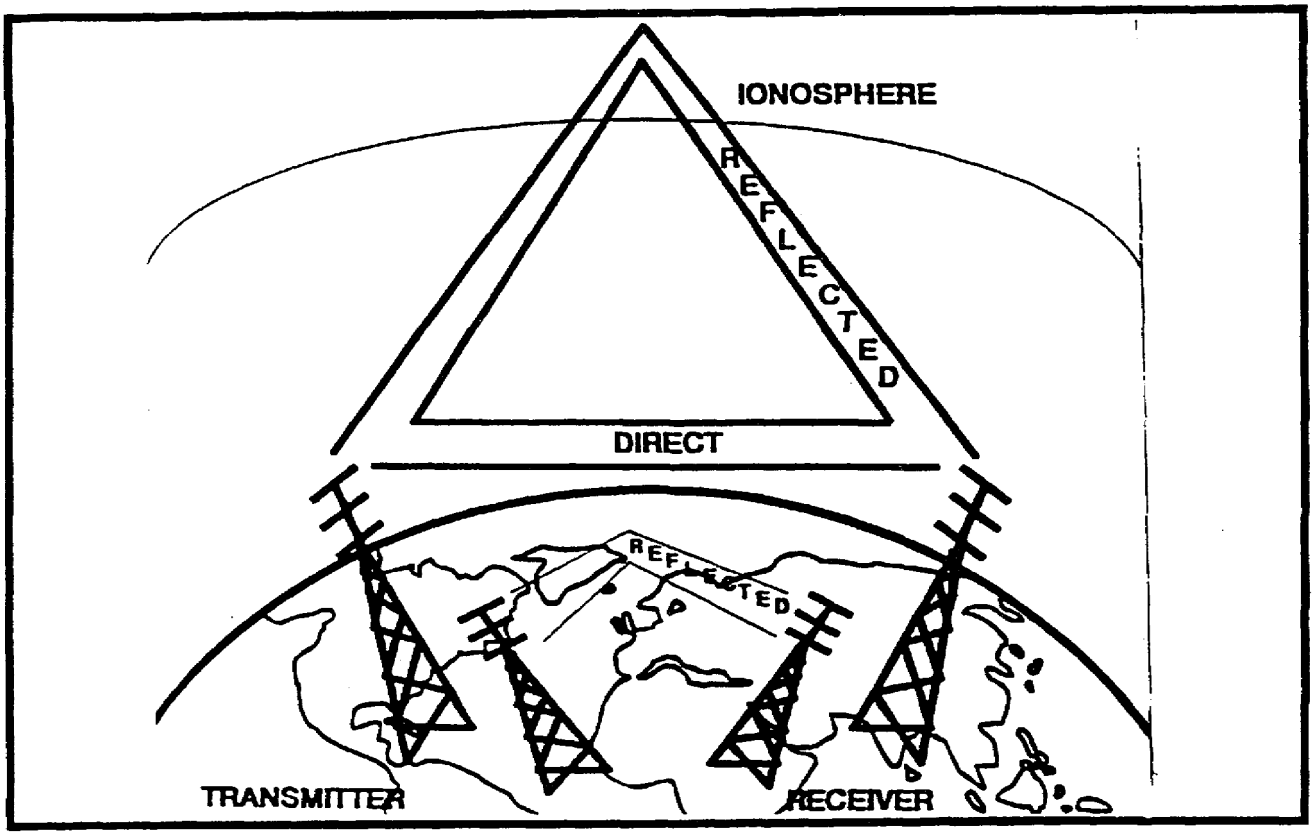


Figure 1-7. Direct and reflected routes for radio waves.

If the waves are refracted by the earth, the distance they travel is severely limited due to large losses of energy in the form of heat dissipated into the earth's crust.

Radio waves may be classified as either ground waves or sky waves (Figure 1-8).

Ground waves are continually in contact with the earth's surface. They do not make use of reflection from the ionosphere. They have a tendency to be refracted and, in some cases, reflected into the lower atmosphere. At frequencies above 1500 kilohertz, a ground wave is affected very little by the time of day or season. The ground wave loses much of its strength and dissipates energy as it travels over the earth's surface. However, less strength is lost when it travels over water.

Sky waves are transmitted upward with respect to the earth's surface. Sky waves would not be useful for communications were it not for the ionosphere. Radio waves approaching the ionosphere at an angle are refracted back to earth. They may be detected and used for communications purposes or for DF exploitation.

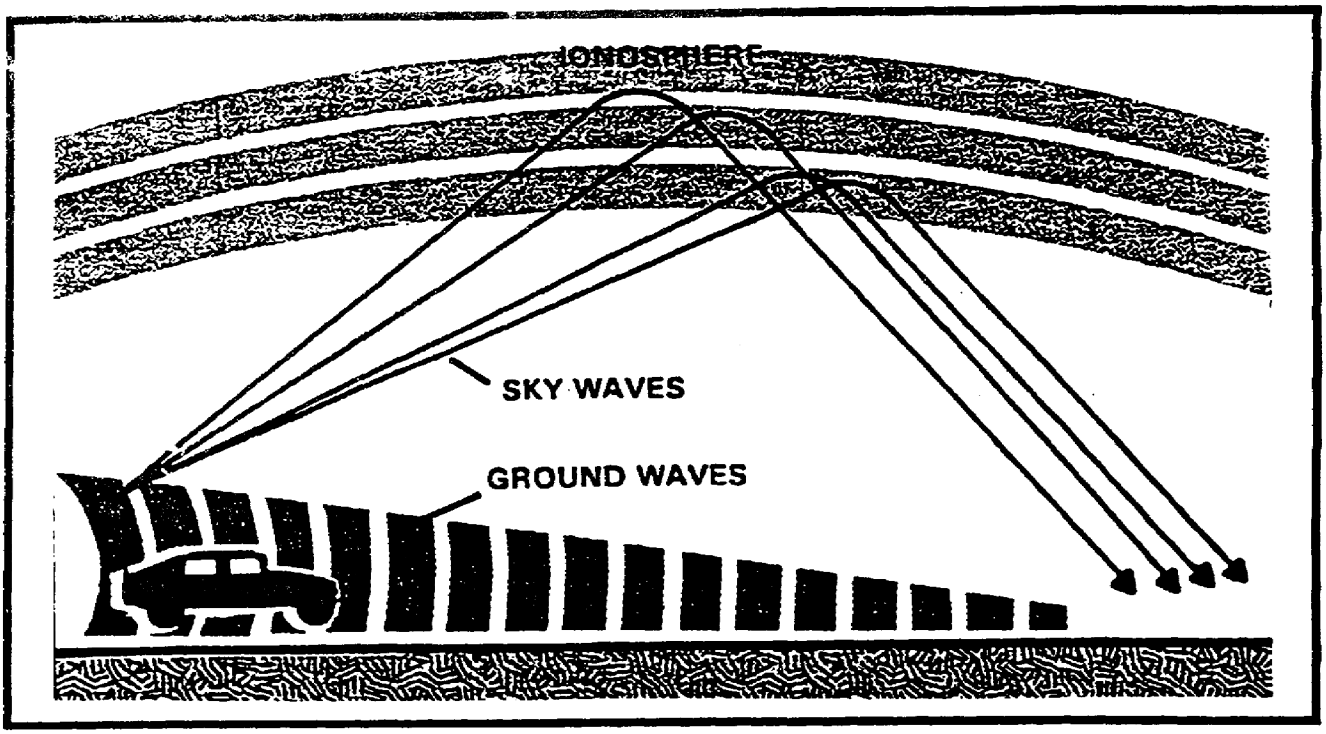


Figure 1-8. Ground waves and sky waves.

The skip zone is the area where the ground wave can no longer be detected (Figure 1-9) and the sky wave has not yet returned to earth after being reflected or refracted off the ionosphere or troposphere. The skip distance is that area where no sky wave reception will be possible. This is because the wave has not returned to earth after its first or subsequent bounce off the reflecting layer.

Depending upon the frequency and the transmitter power, multihop transmissions are routinely used for communications. Figure 1-10 illustrates multihop transmissions. There will be, however, skip zones between the points of the wave's return at each hop. Note, however, skip zones are not static or stable.

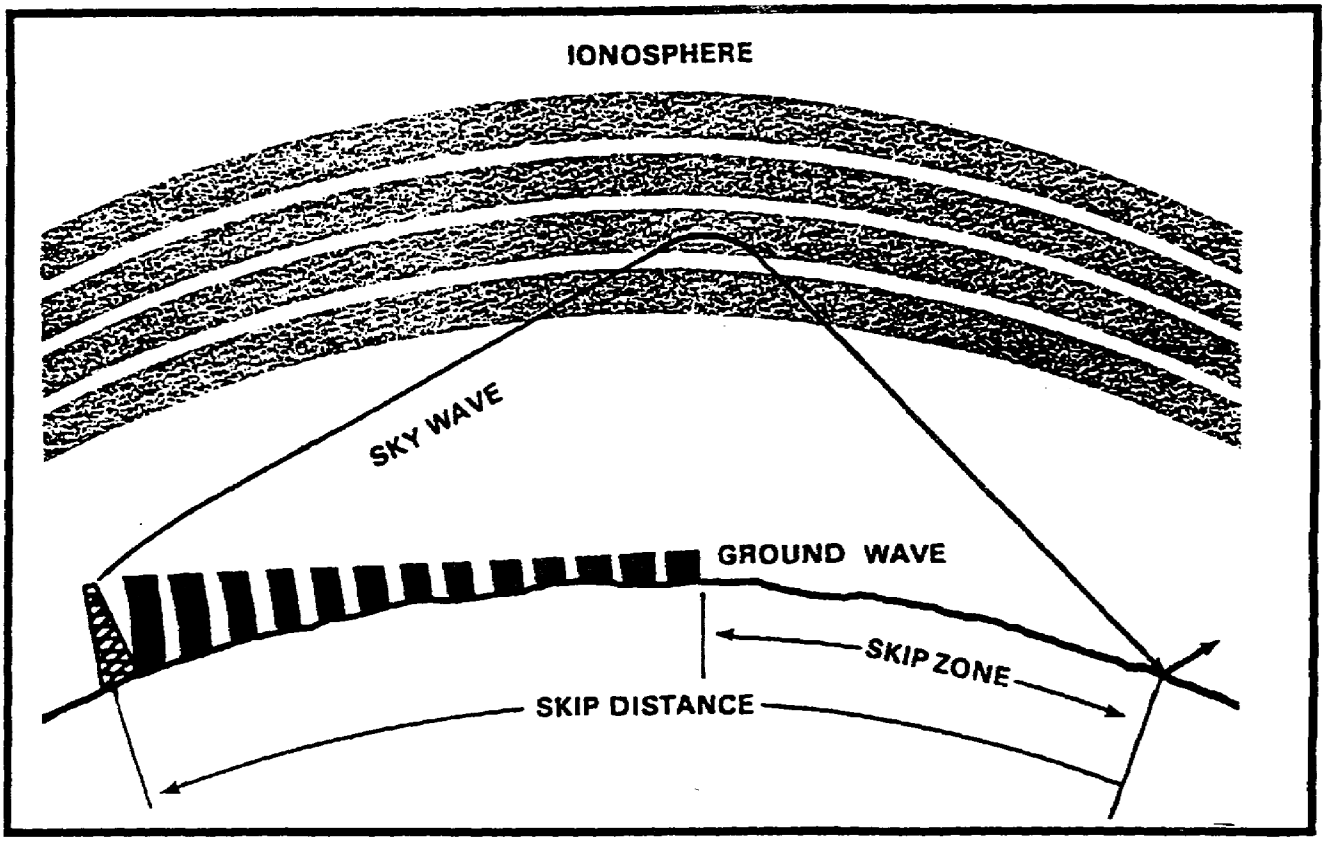


Figure 1-9. Skip zone and distance.

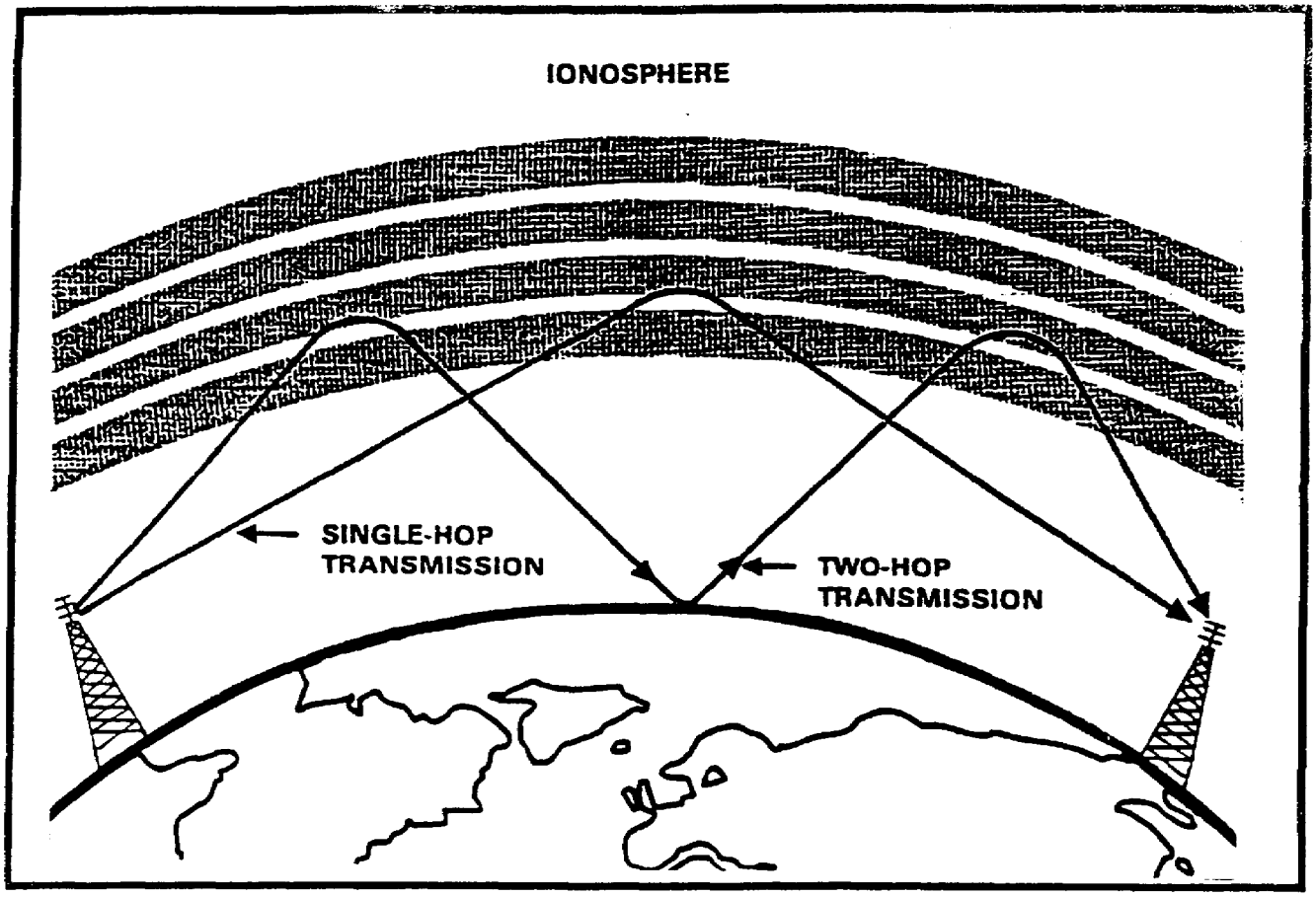


Figure 1-10. Multihop transmission.

PART B: PROPERTIES

Have you ever rotated a portable radio to find the best position to hear the station? If so, you are an experienced radio direction finder. The equipment was not very complex, but it met your requirements to get the results you wanted.

If you had turned the radio on full circle you would have heard two maximum and two minimum volumes. The reason for this is quite simple. The antenna in the portable radio is usually a bar-type antenna which is highly directional.

The pencil can be used to demonstrate the directional properties of the bar antenna. Hold a pencil in front of yourself with the pencil parallel to the ground. (See Figure 1-11).

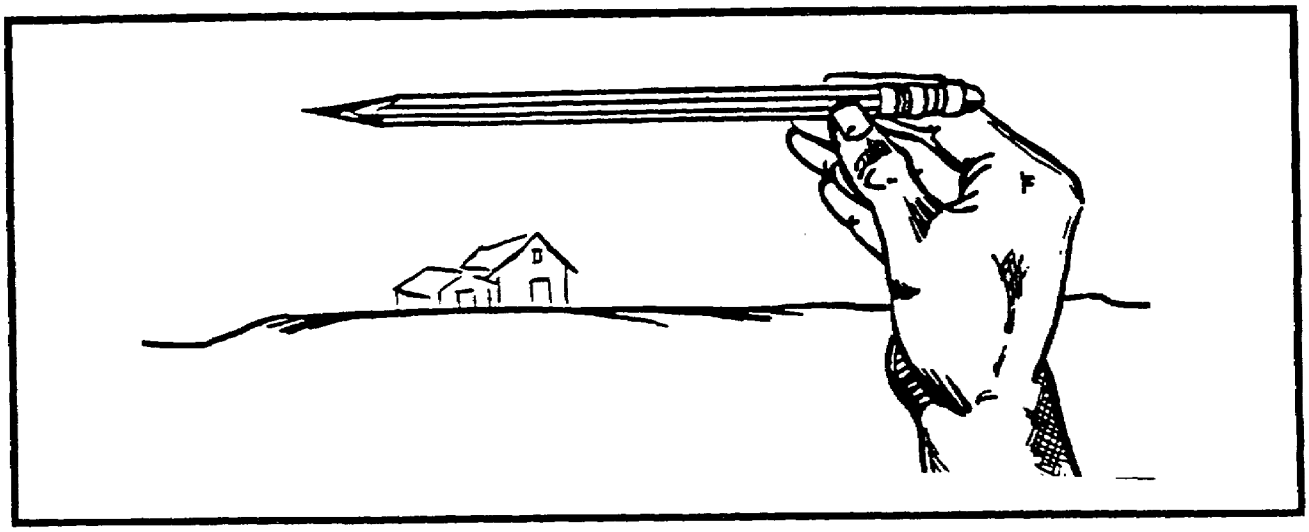


Figure 1-11. Pencil parallel to ground.

Keeping the pencil parallel to the ground, rotate it one full circle. Note that you see each end once and each side once, or put another way, the pencil is sideways to your twice and end on twice. In a bar antenna the sides give maximum reception (signal is loudest) and the ends give minimum reception. The minimum reception points are called NULL points and are important to direction finders because they are easier to hear and locate accurately than are the maximum signals.

The response pattern (a diagram showing the maximum and minimum areas of reception) for a bar antenna is a figure eight. The diagram in figure 1-12 indicates that the end points of the bar receive almost no signal, while the sides receive maximum signal. Since we are using our ears as aural indicators for signal reception, and since a minimum signal or NULL is easier to locate accurately than a maximum signal, we would use aural null indication to locate the transmitter. Of course the problem for a portable radio is locating the best reception rather than the least, but the principle is the same.

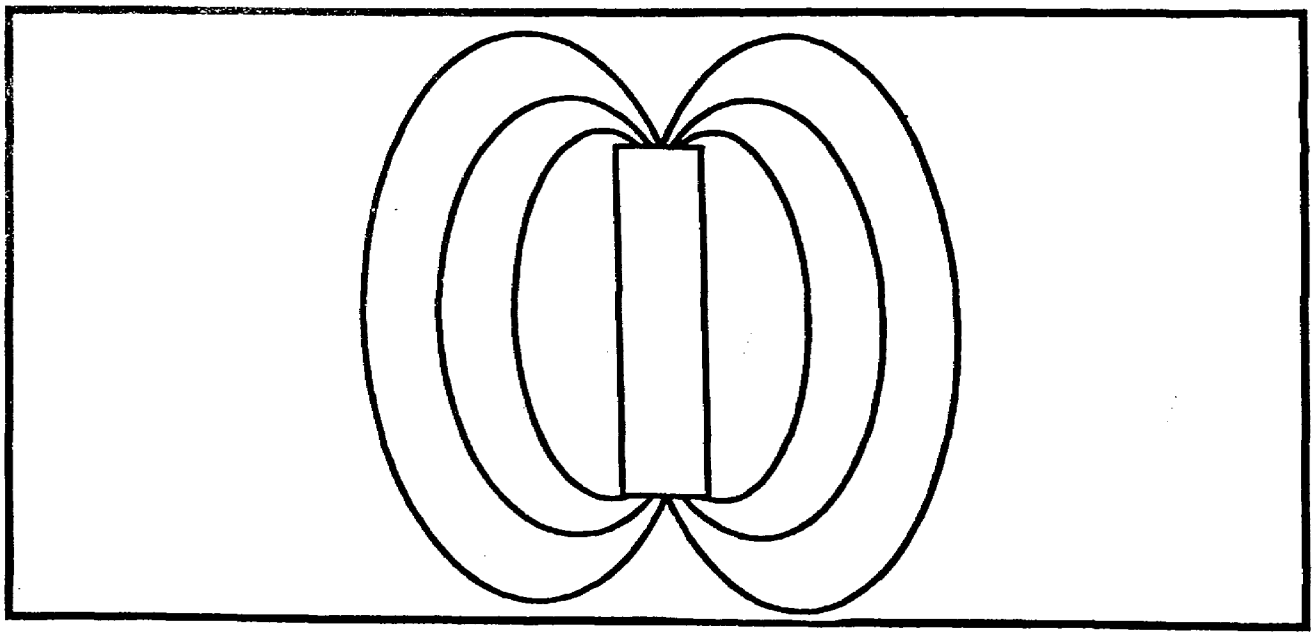


Figure 1-12. Response pattern for a bar antenna.

If we had some sort of compass or direction indicator on the radio we would have a complete direction finder. There is one other factor to be considered. We have two possible directions to choose from. This is the bidirectional ambiguity (the hard way to say it)(See Figure 1-13) which must be resolved (you must make a choice) for accurate direction finding. To do this we must add the signal input of another antenna (sense antenna) to the directional antenna giving us a cardioid (heart-shaped) pattern. This takes away one of the nulls, allowing us to decide which direction to choose. (See Figure 1-14).

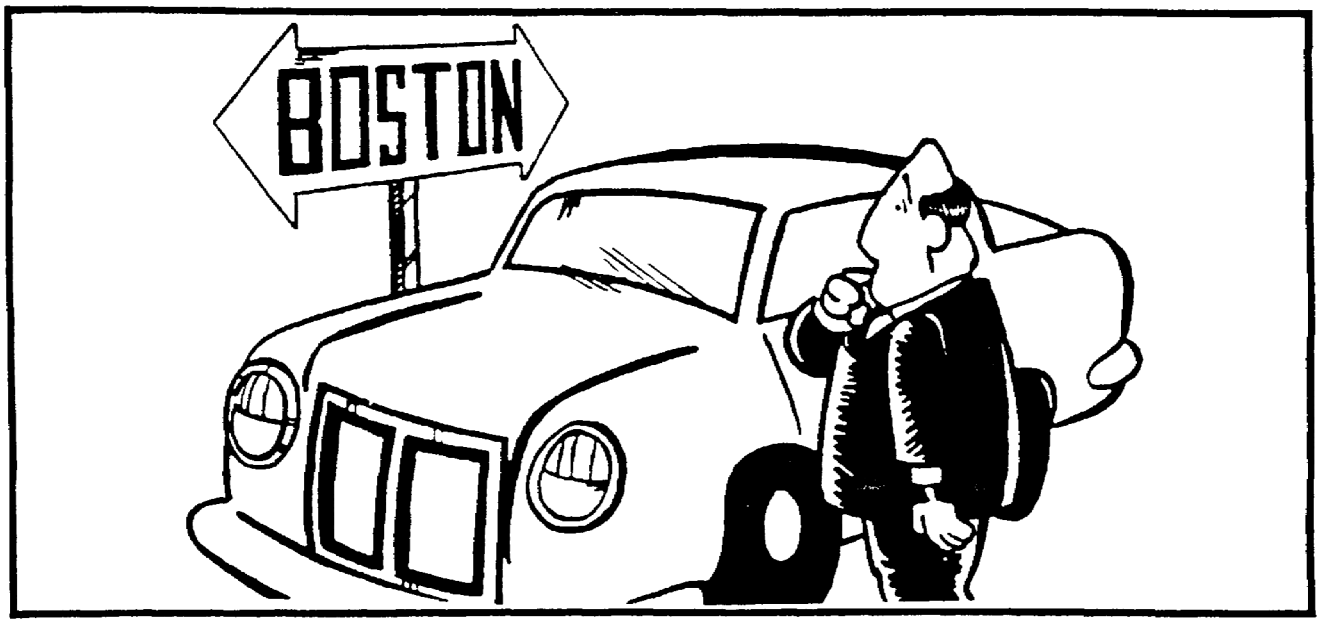


Figure 1-13. Example of bidirectional ambiguity.

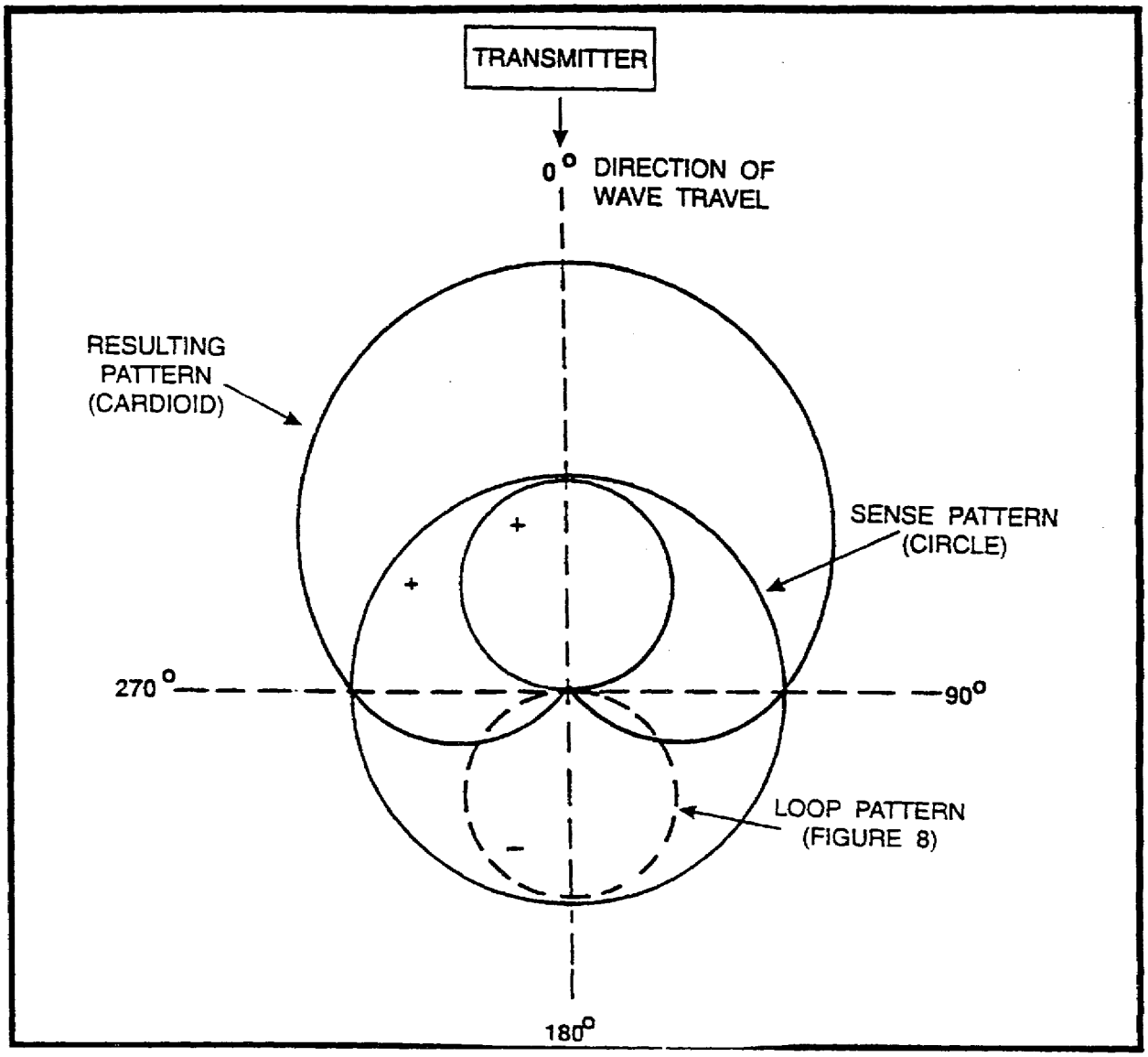


Figure 1-14. Combination of sense and directional antennas.

With the continual development of minicomputers and microprocessors, other methods of direction finding have become feasible. One common method of azimuth determination is Time of Arrival measurements. For this measurement, at least two antennas are used to form an antenna baseline. (See Figure 1-15).

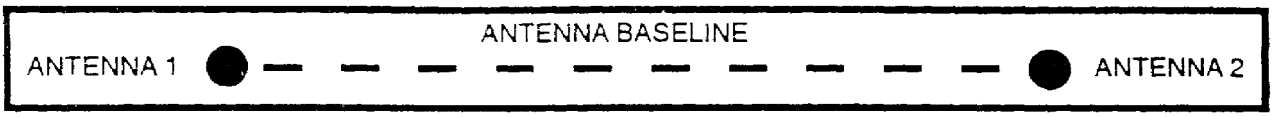


Figure 1-15. Antenna baseline.

As the wavefront strikes each antenna, a microprocessor measures the difference in the time of arrival at each antenna, and the angle of arrival is determined. (See Figure 1-16).

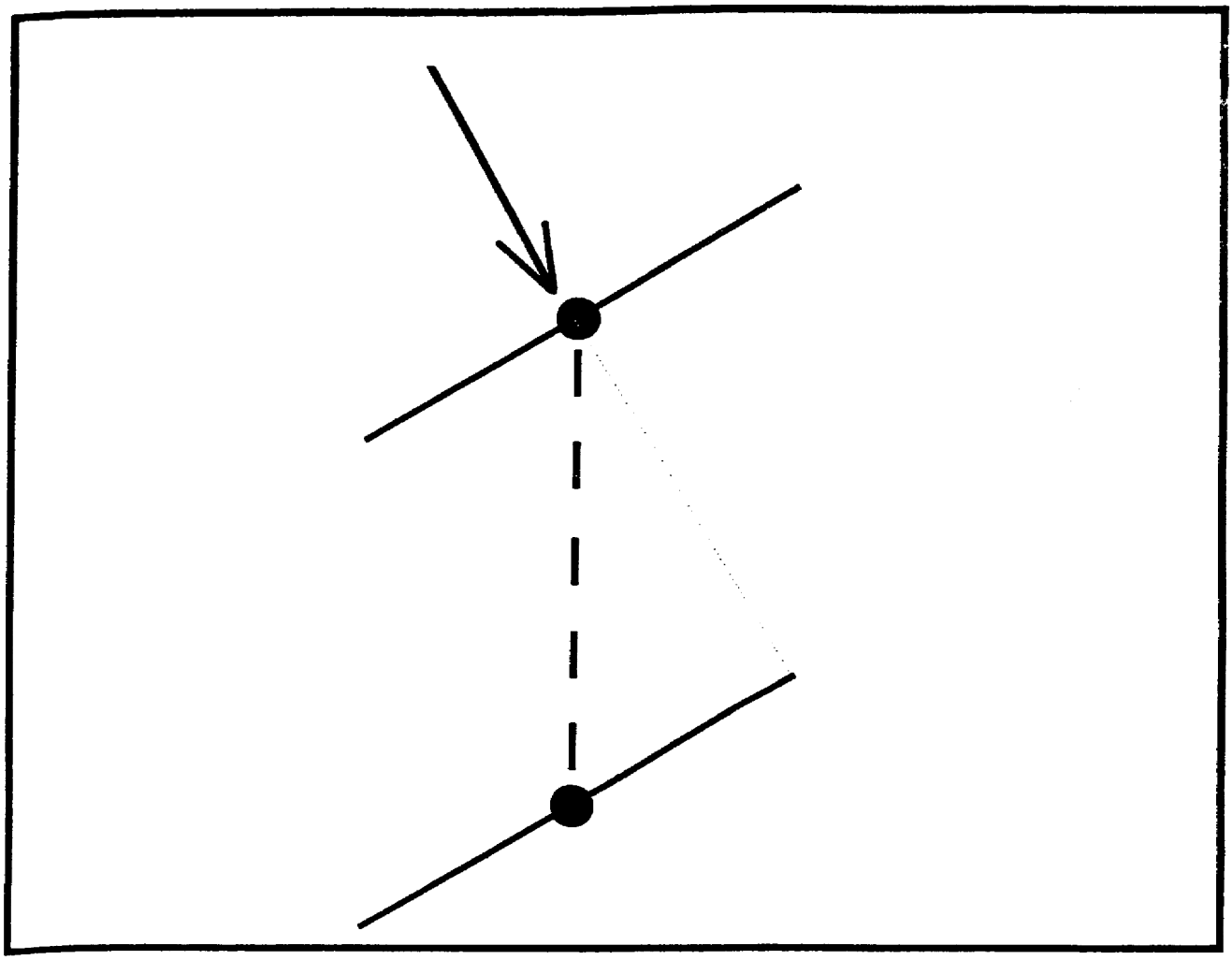


Figure 1-16. Angle of arrival.

As with the bar antenna, however, a possibility of bidirectional ambiguity exists with time of arrival measurements if the wavefront strikes both antennas at the same time. (See Figure 1-17).

To resolve this ambiguity, at least one more antenna is added to form one or more added baselines. (See Figure 1-18).

If a wavefront strikes antennas 1 and 2 at the same time, the ambiguity is resolved by measuring the time difference of arrival of the wavefront at antenna 3.

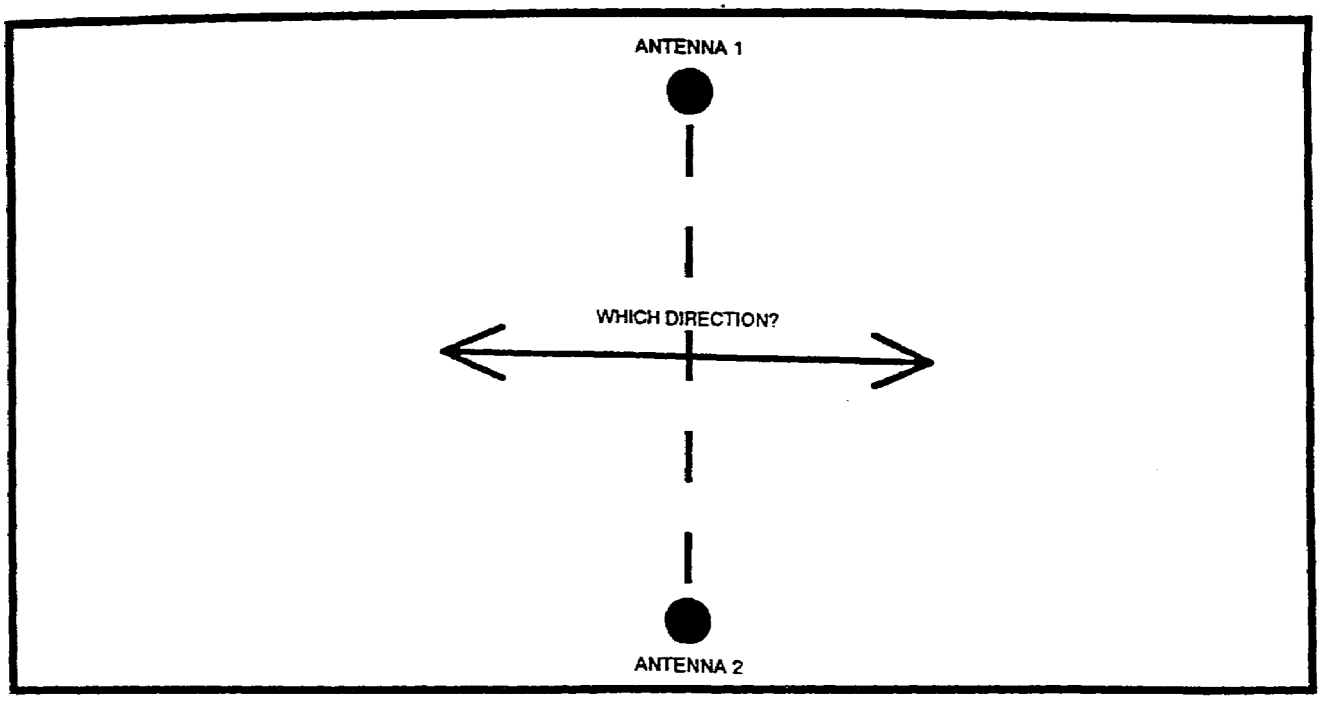


Figure 1-17. Bidirectional ambiguity.

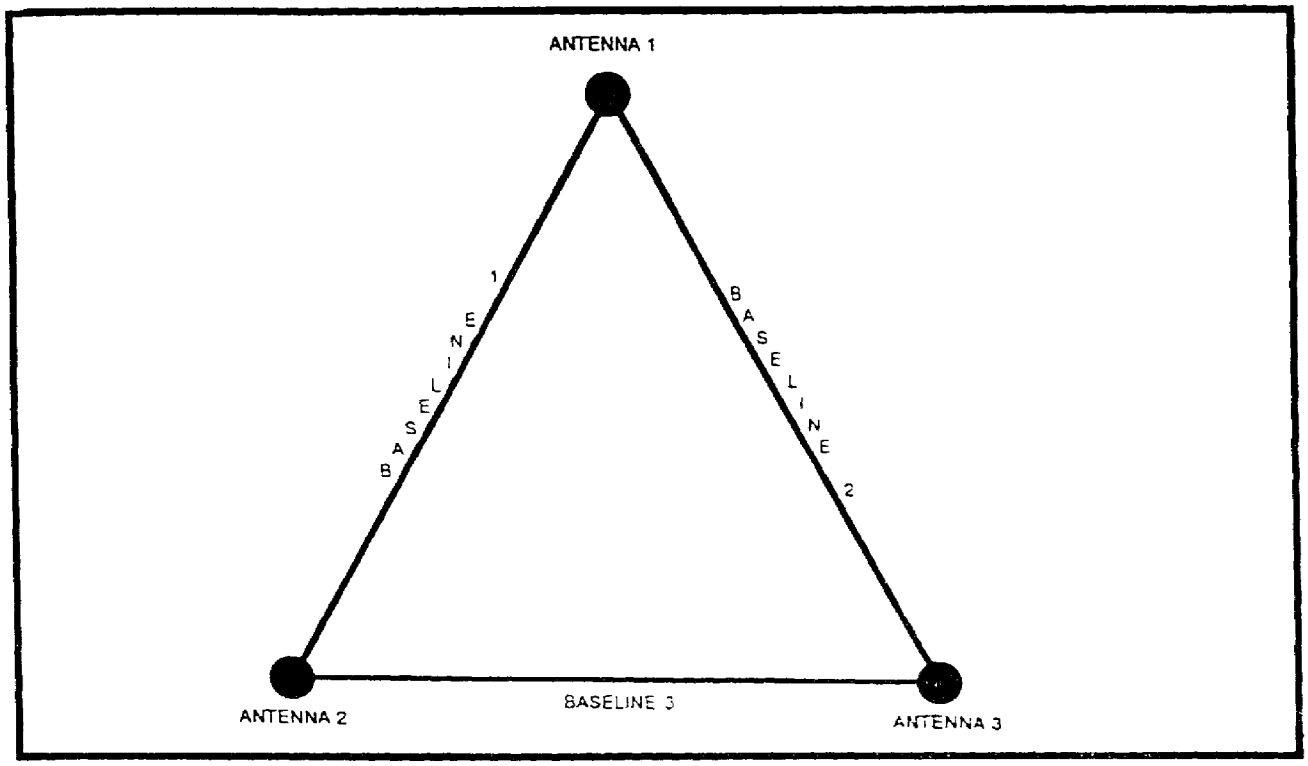


Figure 1-18. Antenna Baseline.

PART C: Elements

This is the basic theory of direction finding and the principle under which most direction finding is "determining the horizontal angle of arrival of a radio wave with respect to a known reference." The known reference is usually True North for strategic systems or Grid North for tactical systems. The horizontal angle is specified because other radio problems involve the vertical angle of arrival (how far to tilt the antenna for best reception) and arrival is specified because we want to know where it is coming from, not where it is going.

The determination of the azimuth is made by determining the angle of arrival, then measuring the angle between the point of arrival and the reference. This is called the azimuth or line of bearing (LOB) and has many applications. It can tell the operator the approximate direction to a transmitting antenna. If the direction finder is placed on a ship or aircraft, the vessel can "home in" on the transmitter. (See Figure 1-19).

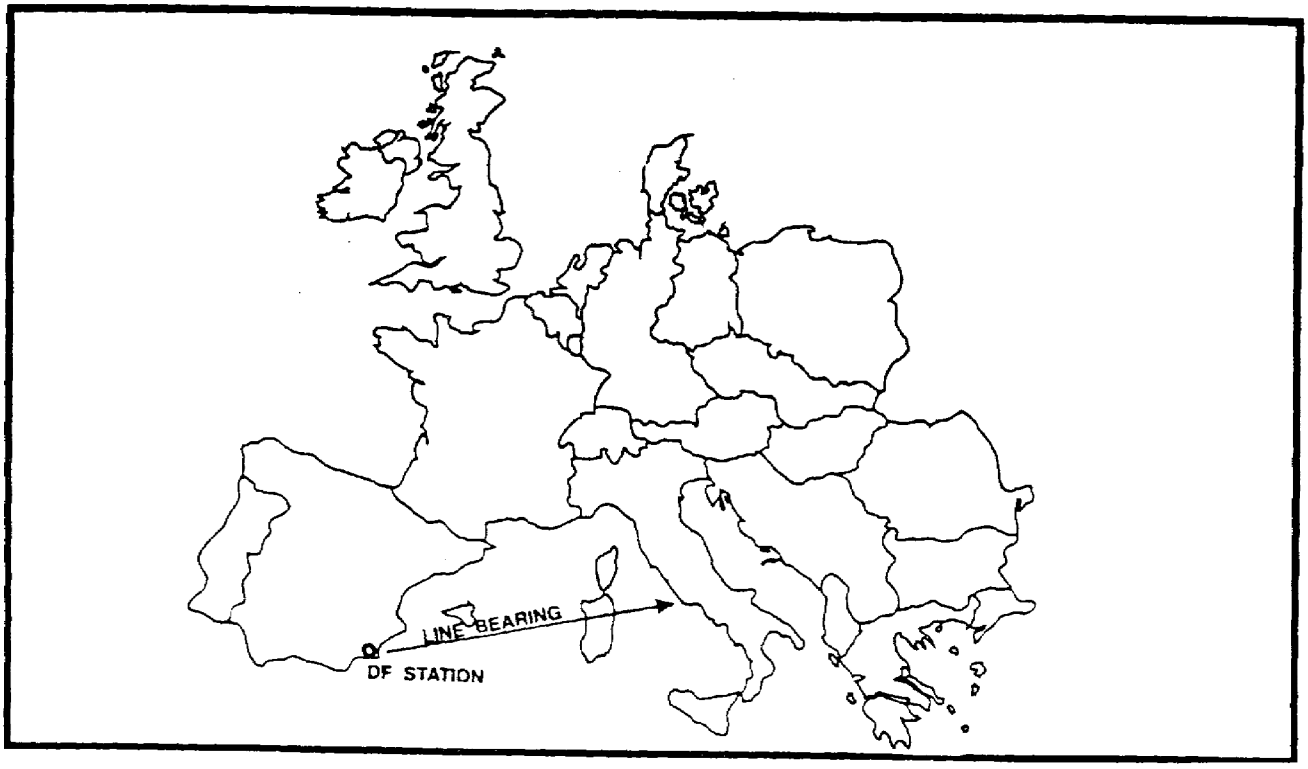


Figure 1-19. DF station line of bearing.

If we use two direction finders and take bearings with both at the same time we can locate a transmitting antenna with limited accuracy. The intersection of two azimuths is called a CUT and will provide the general location of the transmitting antenna. (See Figure 1-20).

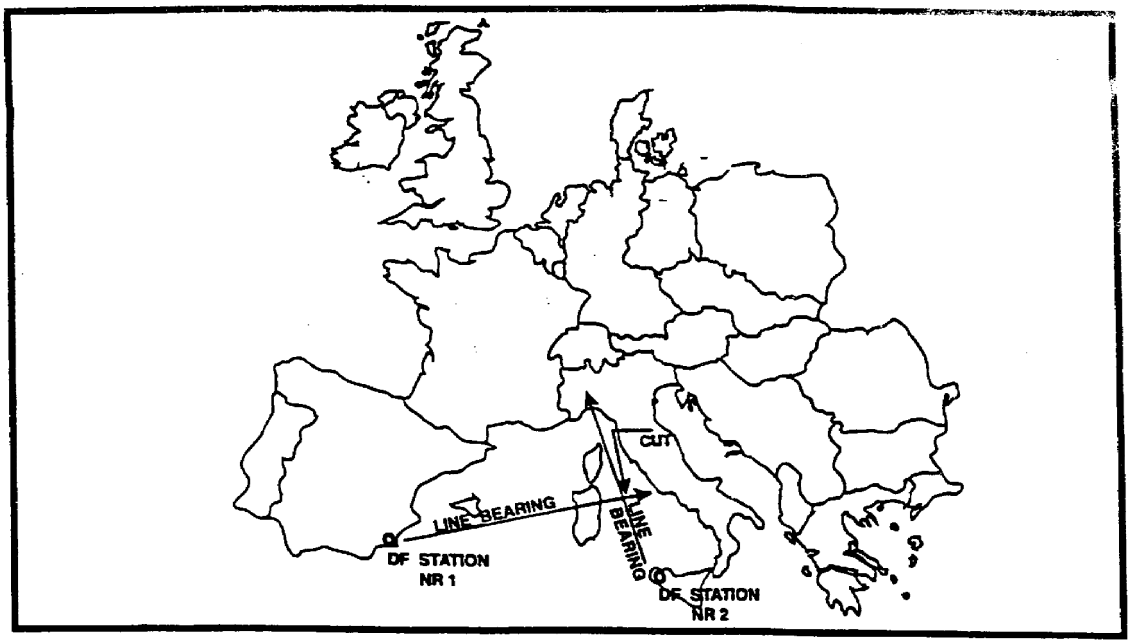


Figure 1-20. Cut of 2 DF stations.

For better accuracy in locating a transmitting antenna we must have three or more direction finders taking simultaneous bearings. This is termed a FIX, or FIX AREA, and will provide the probable location of the transmitting antenna. (See Figure 1-21).

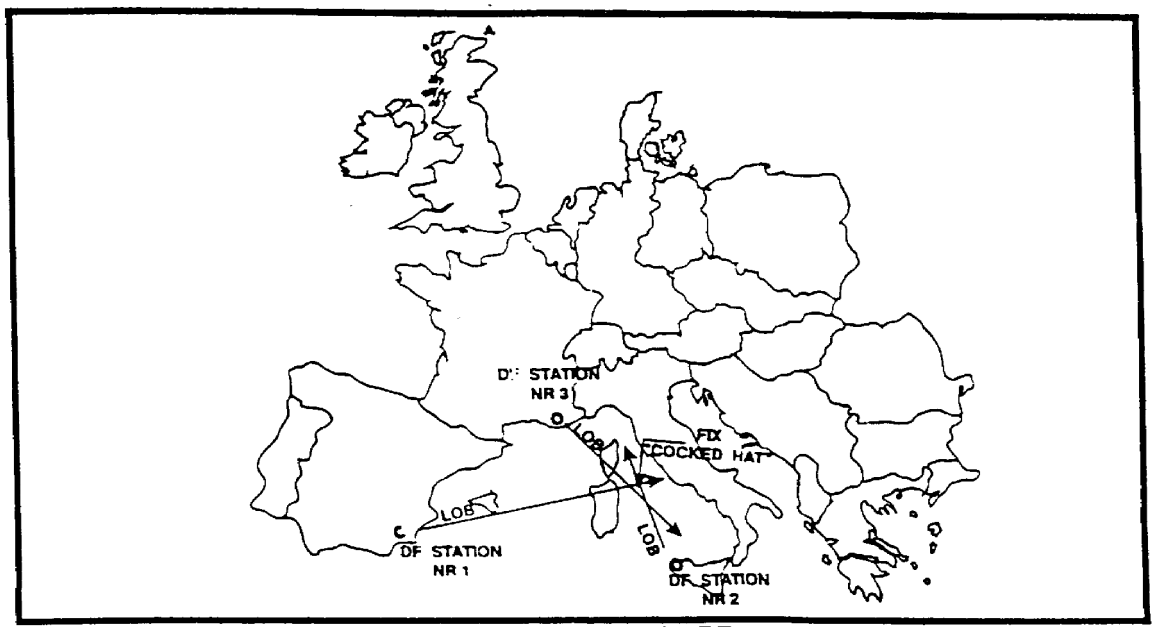


Figure 1-21. Fix area of 3 Led stations.

Note that we use the terms "approximate direction", "general location", and "probable location." This is necessary because of the many variables that affect direction finding. Your studies of radio wave propagation will find many causes of inaccuracies In direction finding. The most

accurate direction-finding equipment in use today has an equipment error of plus (+) or minus (-) 1 degree. This means that if there were no propagation errors to contend with, the equipment itself might cause an error of over 17 miles at a distance of 1000 miles. This problem of errors is taken up more fully in another course.

To be effective, direction finders must have access to listening posts or intercept stations, and must be tied together with a reliable high-speed communications system, and they must be carefully placed in well-planned locations. The spacing of these locations results in a BASELINE, which is important in respect to direction-finding net capabilities. The listening post will monitor several frequencies, and when a transmitter is heard, the direction finders will be notified using the communications system. If the direction finders are placed on a well-planned baseline they will be able to locate the transmitting antenna with a fairly high degree of accuracy. The baseline must be arranged so that the intersection of the bearings for a target located in the approximate center of the area of interest, will be close to 90 degree angles.

The azimuth from each direction finder is plotted on a map, the resultant enclosed area probably includes the location of the transmitting antenna. (See Figure 1-22).

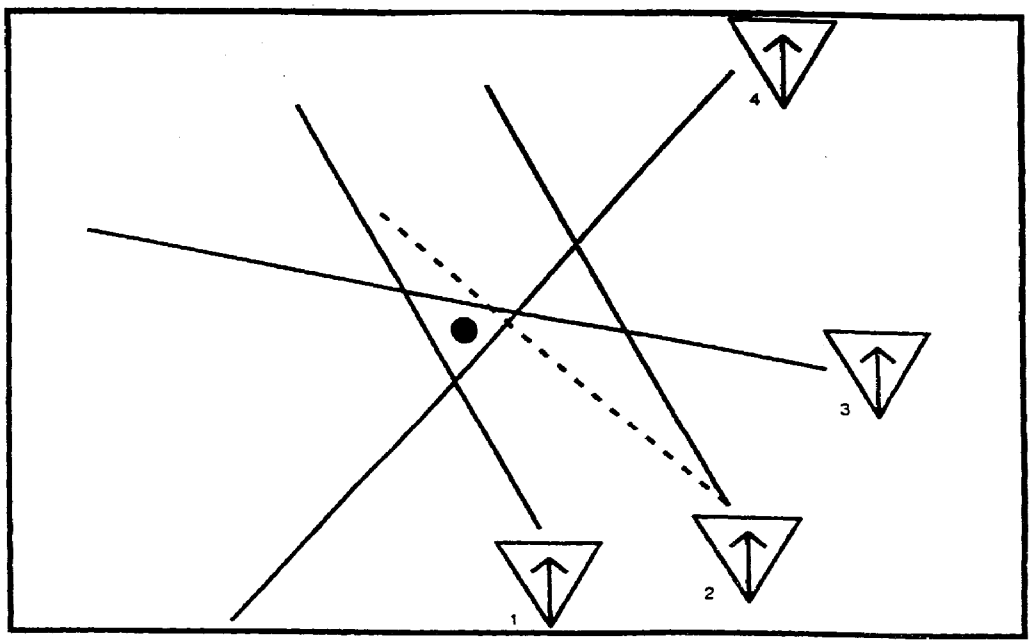


Figure 1-22. Plotted probable location.

The Chiefs of Staff of the Army and Navy have implemented a Joint Air-Sea Rescue Communication Plan (Joint Emergency Rescue Communication Plan JANY-10) which prescribes the procedure to be followed in establishing contact with shore DF stations. The services maintain high frequency DF networks along the various air routes. providing aids "fixes" to aircraft.

An evaluation center is associated with each DF network for the purpose of furnishing fixes and other navigational information to operations offices.

Radio direction-finding devices are used by ground force units for homing or positioning of patrols and reconnaissance units. Airborne troops also use these devices to regroup after landing. In many cases these devices are not complete DF units but simple devices attached to a common field radio receiver. DF is used to locate enemy aircraft in flight, ground control stations, and radio navigational aids. The results of DF correlated with other information comprise one of the most important sources of combat intelligence from which it is possible to determine the enemy order of battle when there is no physical contact. This information is usually more comprehensive than that derived from enemy radio stations. These stations are then monitored by DF for possible movement.

As demonstrated earlier, there are many types of direction finding systems. In some, only the azimuth of the arrival angle can be measured. In others, the azimuth and the elevation angle can be obtained. When only an azimuth is resolved, two or more independent DF stations are needed to determine the location of the transmitting antenna. Systems that measure both azimuth and elevation angles are called **single station locator** (SSL) systems. The SSL was developed because of the problems of audibility with the traditional DF network. Sometimes the signal could only be heard at one DF site.

The SSL system direction finder is a phase measuring interferometer. Location data include an azimuth measure on the target signal and a range estimate based on the measured parameters at the DF site. The combination of azimuth and great circle range to the target produces the location output from the system's computer.

Because the SSL system depends on ionospheric propagations, it is designed for use against the high frequency (HF) spectrum sky wave transmissions. As shown in Figure 1-23, the combination of an azimuth and great circle range to the target produces a location from the system that is expressed in geographic coordinates.

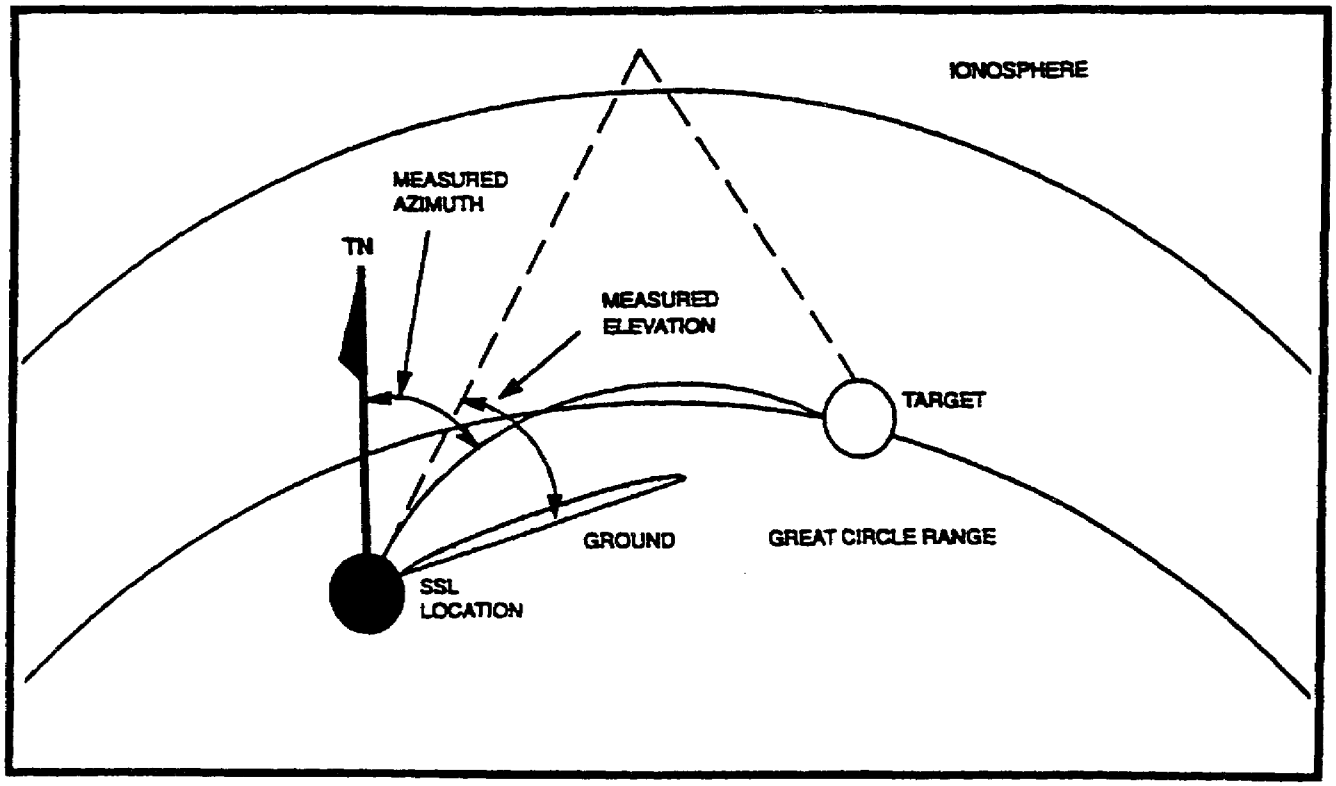


Figure 1-23. Single station locator DF.

LESSON 1

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. What is a radio waves strength or intensity called?

   A. Consecutive Cycles
   B. Complete Wavelength
   C. Its Magnitude
   D. Its Amplitude

2. What does DF determine the direction of?

   A. Artillery Fire
   B. The arrival of a radio wave
   C. The direction a radio should be pointed for the best reception
   D. The distance of a receiver

3. What band designator would the frequency 200 MHz be in?

   A. HF
   B. VHF
   C. UHF
   D. SHF

4. What are the DF results with a range of 1000 miles called?

   A. Approximations
   B. Exact, if enough sites are used
   C. Reliable
   D. An indicator of general direction only

5. Which of the following is NOT used as a military application of DF?

   A. Positioning of ground forces
   B. Determining order of battle
   C. Location of communications systems
   D. Detection of chemical agents

6. What is the most common reference point for DF?

   A. The enemy front
   B. The friendly forces front
   C. Magnetic north
   D. True north or grid north

7. Which frequencies would you use for the best communications at night?

   A. Lower Frequencies
   B. Mid-range Frequencies
   C. Higher Frequencies
   D. Ultra High Frequencies

8. What is the accuracy of the most accurate DF equipment used today?

   A. +1%
   B. + 2%
   C. + 1 degree
   D. + 2 degrees

9. What is the term used for the intersection of two azimuths?

   A. Bidirectional
   B. LOB
   C. Cut
   D. Fix Area

10. Including an azimuth, what is also measured by a SSL system in order to determine the location of a transmitting antenna?

    A. Elevation Angle
    B. Ground Waves
    C. Target Area
    D. Skip-Zone

LESSON 1

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	D. (page 1-2)
2.	B. (page 1-1)
3.	B. (page 1-3)
4.	A. (page 1-19)
5.	D. (page 1-21)
6.	D. (page 1-18)
7.	A. (page 1-7)
8.	C. (page 1-20)
9.	C. (page 1-18)
10.	A. (page 1-21)

LESSON 2

EQUIPMENT REQUIREMENTS

CRITICAL TASK: None

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to identify the basic equipment requirements for a radio direction finding system and certain concepts needed for discussion of direction finding equipment.

TERMINAL LEARNING OBJECTIVE:

TASK: Identify the basic equipment requirements for a radio direction finding system and certain concepts needed for discussion of direction finding equipment.

CONDITION: You will use the information provided in this subcourse.

STANDARD: To demonstrate competency of this task, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications:

FM 11-64
FM 11-666
FM 30-476
FM 34-40-9(U)
FM 34-86

INTRODUCTION

Radio direction finding equipment comes in all sizes and shapes, depending upon the requirements of the users. Some equipment can be hand-held, back-packed, or airborne (Figure 2-1) while other configurations require several acres of land for installations.

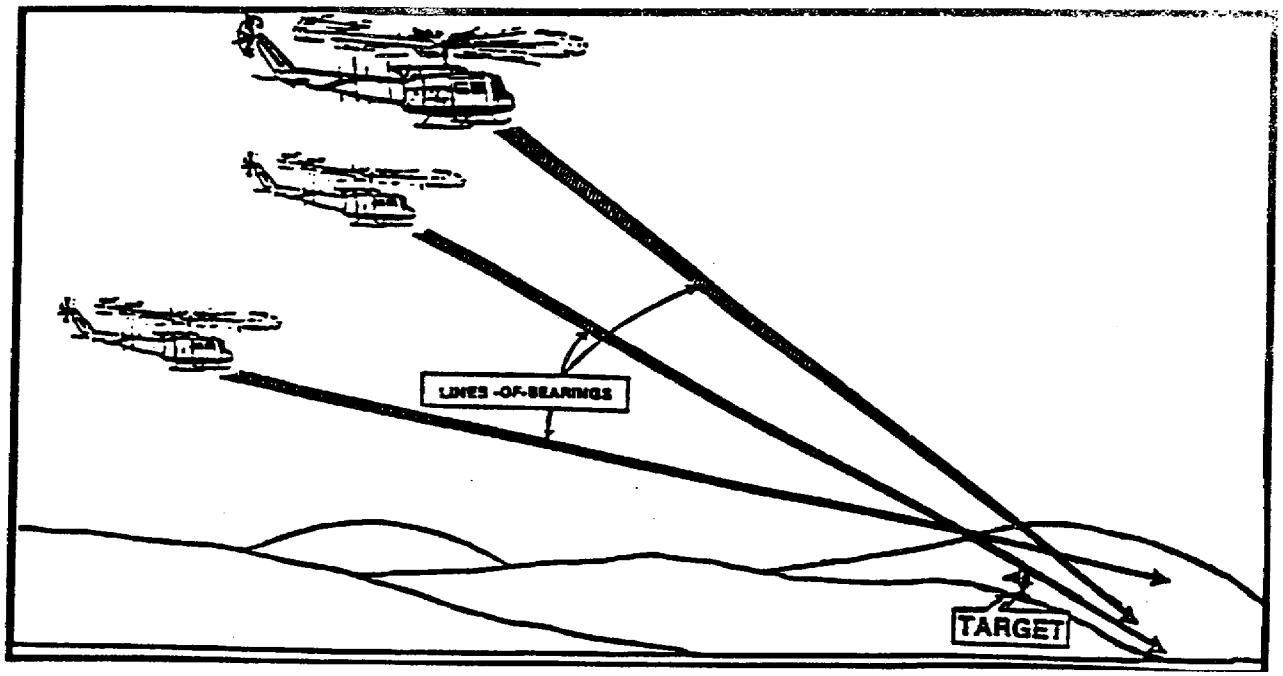


Figure 2-1. Airborne radio direction finding.

PART A: COMPONENTS

Regardless of the requirement, direction finding equipment will have the same basic components. (See Figure 2-2).

a directional antenna
a radio receiver
a coupling system
a method of indication

Suppose we refer to the portable radio mentioned in the first lesson. The directional antenna is the bar antenna. The receiver is the radio itself. The coupling system is the "direct coupling." The indication system is the "aural null." Each is designed for the specific job it is supposed to do, and is the most efficient piece of equipment the manufacturer can use within he parameters (requirements) needed. Probably the first consideration for the manufacturer was cost efficiency, second was size and weight. Third was ease of use. Fourth was neatness of design. There are others but our discussion will stop here.

The Directional Antenna. The bar antenna is the most compact for the frequency range of the receiver. It is highly efficient and relatively inexpensive, consisting of a number of turns of wire wound around a core. The fact that it is bidirectional was of secondary importance to the manufacturer, but it makes a net illustration for the DF student. Of course, the user of the radio is more interested in the peak reception than the null, but still the directivity is there and can be used. As an illustration of the case of use of the null, as compared to the maximum point, try lining yourself with the length of the antenna as compared with centering yourself on the width.

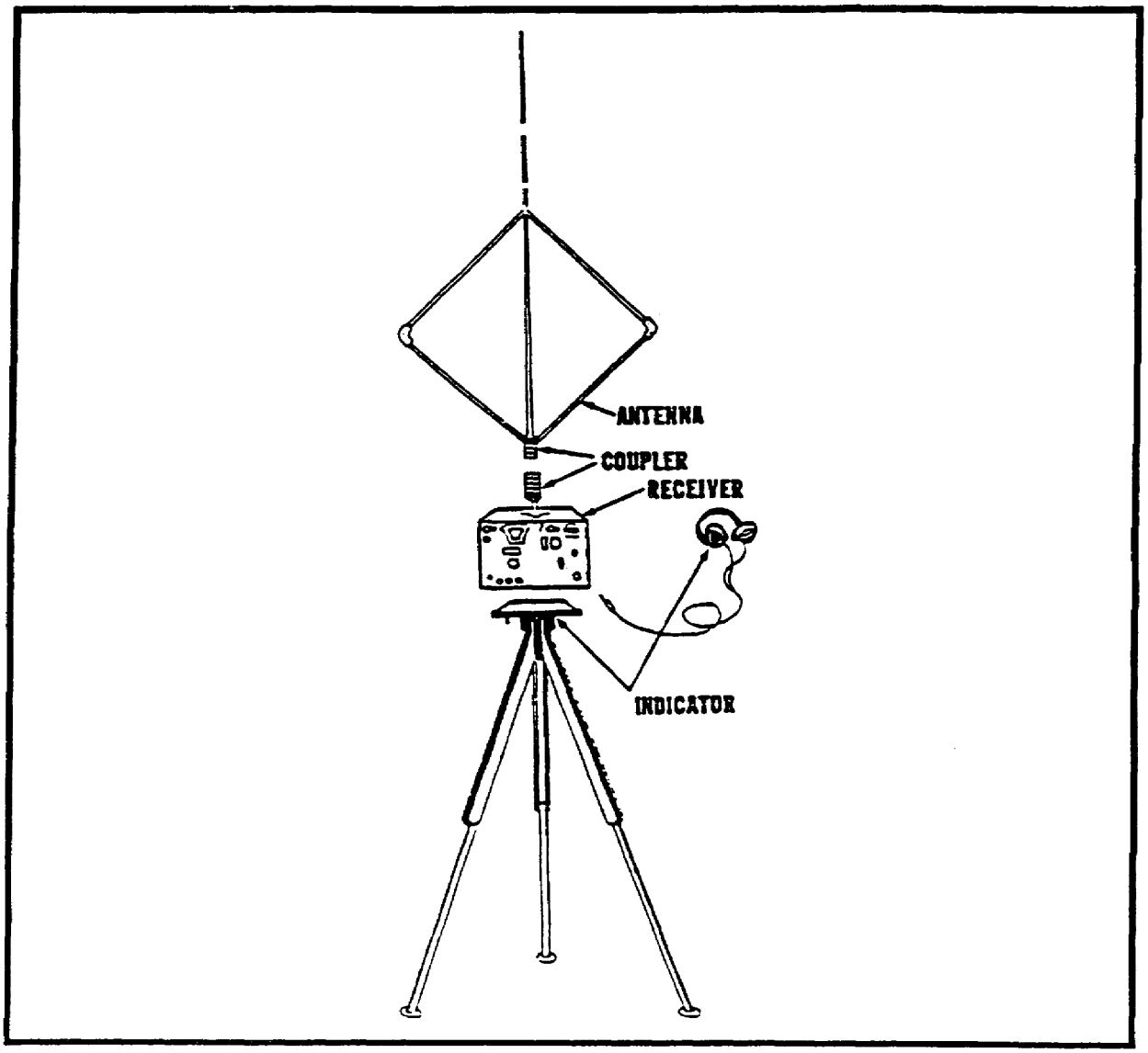


Figure 2-2. Basic components.

Or, put another way, if you hold a pencil you can tell where the point is by looking, but where is the exact middle of either side?

The coupling system. This is the device that connects the antenna to the receiver. The directional antenna must be rotated in a circle to detect the angle of arrival of the radio wave. If we were to use a simple antenna cable, it would soon twist until it broke. Several systems have been devised but all can be identified as either manual or electronic. The simplest system is the direct coupling in your portable radio. The problem is that it requires us to rotate the receiver as well as the antenna to determine the angle of arrival. This would be difficult with our large systems. Another manual coupling is slip ring and brushes. This is an antenna which is rotatable but maintains contact by means of brushes (such as in the generator of your car touching slip rings which allows the signal voltage to pass freely from the antenna to the receiver). For direction finding antennas that are too large to be normally rotated, a device

called a goniometer is used to electrically rotate the antenna. The leads from the antenna are connected to coils in the goniometer, and another coil is rotated in order to sample each portion of the circle in turn. Some of our VHF/UHF DF systems use a microprocessor or minicomputer to electronically measure the time of arrival instead of rotating the antenna.

The Radio Receiver. Your portable radio, whether it be a small Amplitude Modulated (AM) receiver or the larger, and costlier, transoceanic AM, Frequency Modulated (FM) shortwave type, is designed to receive broadcasts within certain wavelength imitations. These limits are called the frequency range of the receiver. Which receiver will be used with your DF system depends upon the frequency range of the transmitter in which you are interested. Another consideration is the desired mobility (how fast it can be moved without damage) and transportability (what does it take to move it) of the DF system. The DF receiver must have good stability (stays on frequency), sensitivity (you can hear and target), selectivity (you can tune out the signals you don't want), and a Beat Frequency Oscillator (BFO) which is used to give a steady tone for ease of direction finding/AM signals.

The input and output circuits of an ordinary communications receiver usually require modification for use with direction finders. The portable radio, for example, has the correct frequency range for the targets desired. It is designed to be hand carried, relatively stable, has selectivity, and is as sensitive as the price allows. It does not have a BFO, therefore, it does not meet our requirements. If we were to use it with our systems we would have to add a BFO.

The Method of Indication. By now you are familiar with aural null indication. The most common system other than aural null is visual indication. This employs a cathode ray tube or some type of meter which indicates the null or maximum signal for your interpretation. The indicator is usually associated with some sort of a measuring device so the operator can record what he/she sees or hears.

A useful direction-finding system must have these four components. The targets, and the tactical situation will indicate what combination and size of equipment can or should be used.

PART B: DEFINITIONS

Many of the terms used in discussing direction finding are unique to direction finding or are used in a different sense. In order to understand how these terms relate to the discussion that follows, you will need to know exactly what is meant by each of them. These terms relate primarily to a discussion of antenna theory.

(a) Loop. Originally a loop antenna was a circle of wire. Modern loops come in a variety of shapes but essentially and electrically they are the same as the original circle. It might be easier to think of the circle as a square, with vertical and horizontal sides, since the action of the radio wave on the antenna is discussed in terms of how it affects the horizontal and vertical members of the loop.

(b) Conductor. The wire or similar material used to pass current from one part of a circuit to another.

(c) Instantaneous voltage. The amount of voltage present at any given instant in an electric circuit. Differences in instantaneous voltages, or the lack of differences, give an antenna its directivity.

(d) Magnitude. How big, or small, strong, or weak, something is. For our purposes magnitude refers to the strength of an electric or magnetic field.

(e) Plane parallel to the wavefront. This concept is the biggest single stumbling block to discussion of wave theory the average uninitiated person finds. With reference to the path of the wave, even though the wave front (first part of the wave) is spherical by the time it has reached a reasonable distance from the transmitting antenna, the portion of the wave we intercept with our antennas is assumed to be a straight flat plane. If the wave is traveling toward us in a straight line the wave front is at right angles to the direction of travel. Look at a wall. The line to the wall (or move exactly from the wall to you) is the wavepath, and the wall is the wave front. If you were an antenna with your plane parallel to the wavefront, you would be turned so that the wave front would hit both arms at the same time, if the wall (wave front) went over you (the antenna).

(f) Plane perpendicular to the wave front (Figure 2-3). The loop antenna has been turned so that the incoming wave strikes one vertical arm before it strikes the other. If the antenna face is at the true perpendicular the voltages in use in the receiver are strongest, because the differences in the voltages in the opposing arms of the loops are greatest. This is because the wave will be at different intensities (strengths) for each arm of the loop.

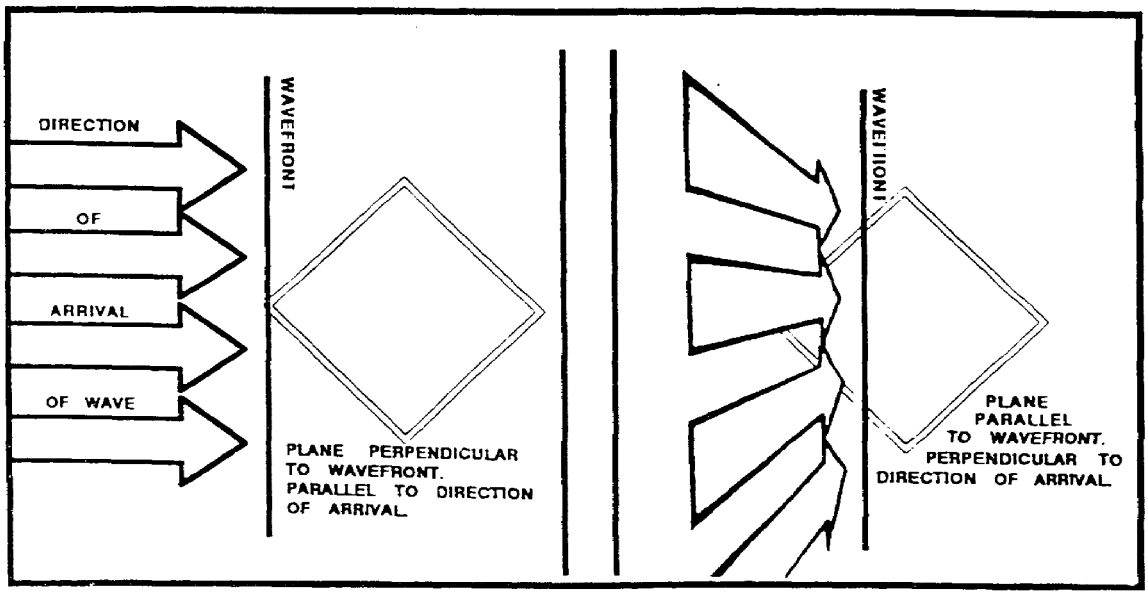


Figure 2-3. Plane perpendicular to the wave front.

(g) Spacing. The physical distance between the antenna elements. Spacing is usually measured in terms of the wavelength, which means that any antenna which is spaced properly for one frequency will not necessarily be spaced properly for another. Spacing is one of the principal limiting factors in determining the frequency range of a directional antenna.

(h) Sense. The addition of an equal voltage from another antenna to the response of a directional antenna. If the voltage added is equal to the original voltage the response pattern is changed to move the nulls to different places in the pattern. Because of this, it is possible to determine from which direction the signal is arriving.

(i) Response pattern. If a target transmitter were physically moved around an antenna, putting out the same amount of signal all the way around a circle at a fixed distance from the center of the antenna, the amount of signal received would vary according to the type of antenna being measured. If this variation is recorded on circular graph paper as so much volume equals so many lines on the graph, with a relationship between direction on the paper and direction in the field, a pattern results which indicates the response of the antennas at any direction. The whip antenna has a circular (omnidirectional) pattern.

(j) Omnidirectional. The response pattern of (for example) the whip antenna. All directions produce an equal response.

(k) Null. The point of weakest response or ideally no response. If the equipment is sensitive enough to allow critical measurement the system is said to have deep nulls. A system with broad nulls does not meet the accuracy requirements of today's direction finding systems (Figure 2-4).

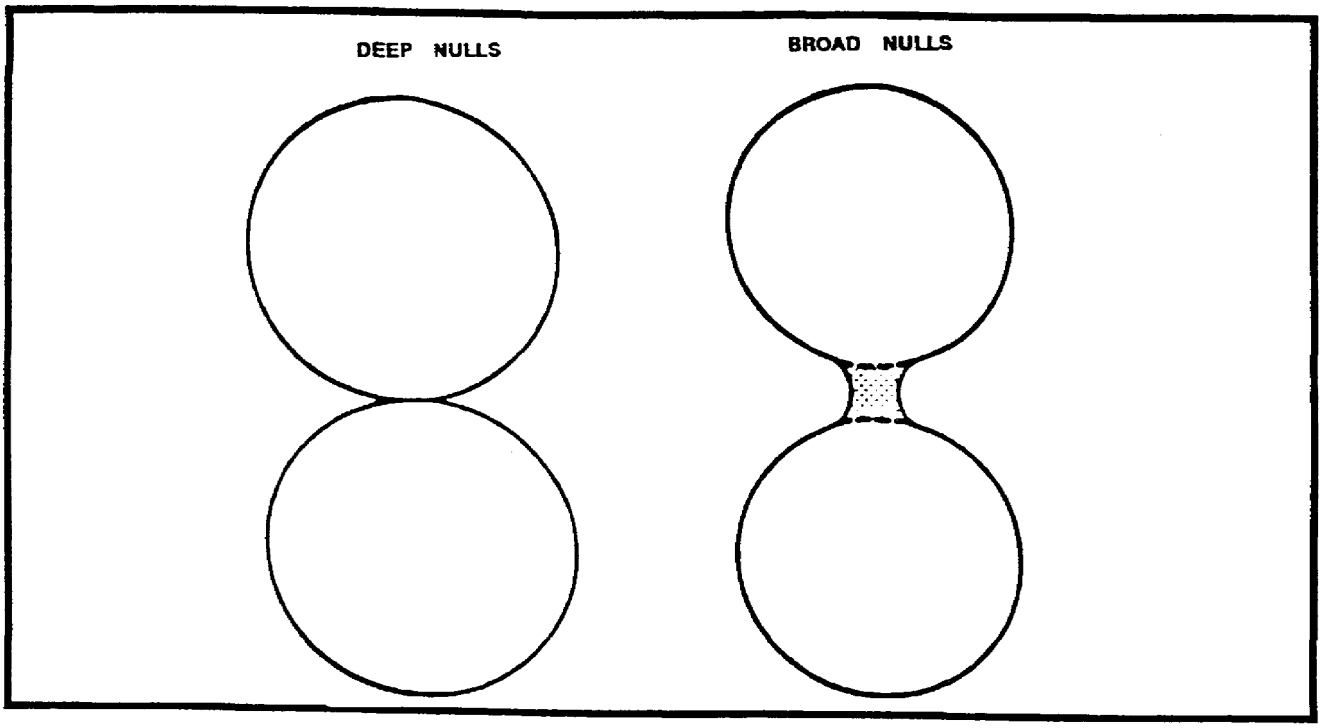


Figure 2-4. Deep nulls and broad nulls.

PART C: REQUIREMENTS

1. The principal antennas used in direction finding are the loop (Figure 2-5), crossed loop (Figure 2-6), Adcock (Figure 2-7), crossed Adcock (Figure 2-8), and circularly disposed antenna arrays (CDAA, Figure 2-9). Each has directional properties, and can be used with direction finding sets to meet specific requirements. Your studies in wave propagation, and definitions of terms used in antenna theory should have given you the terms you will need to understand the following discussion.

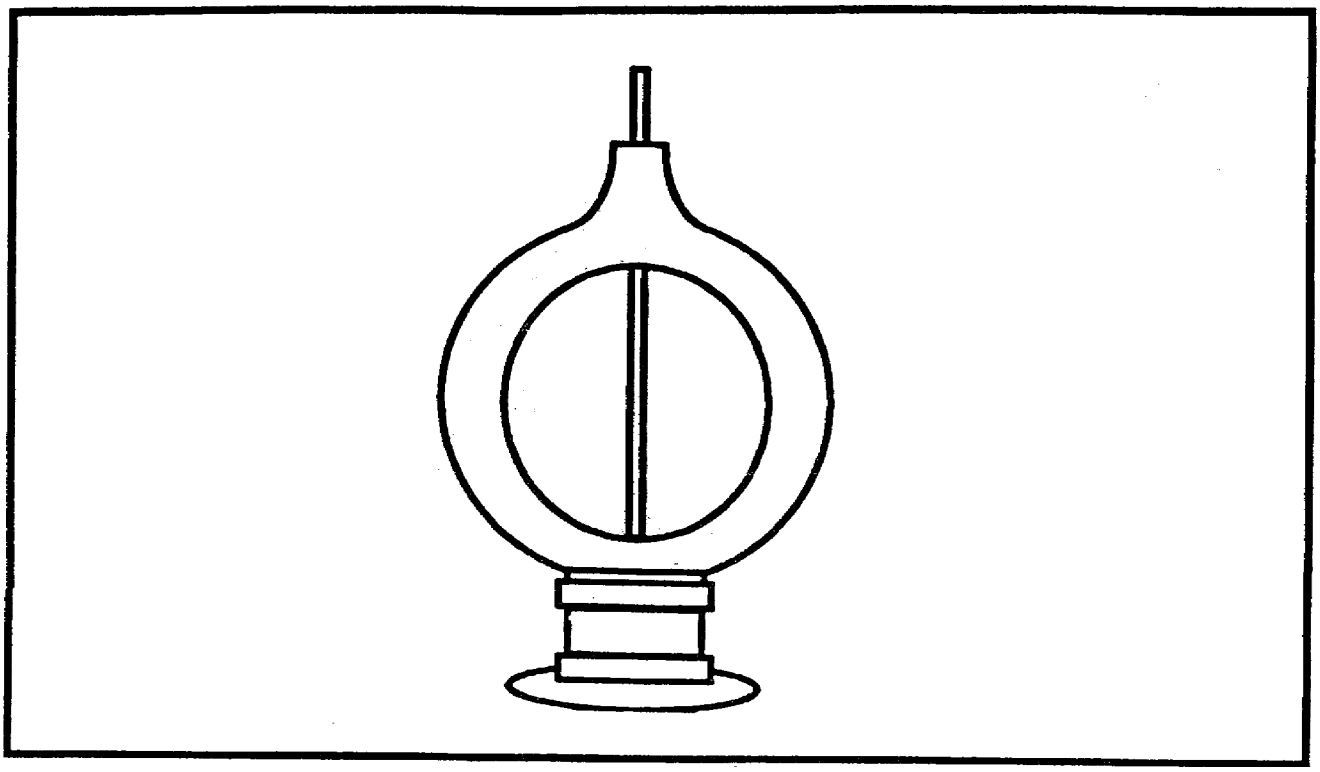


Figure 2-5. Loop Antenna.

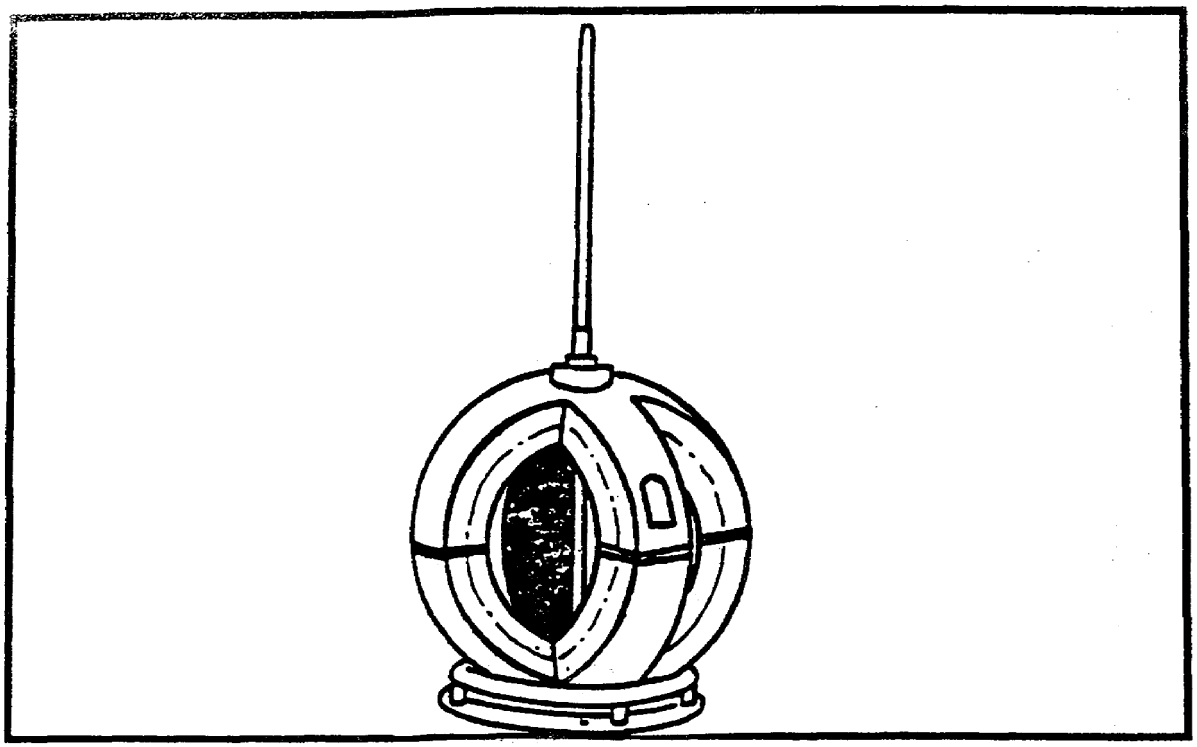


Figure 2-6. Crossed loop antenna.

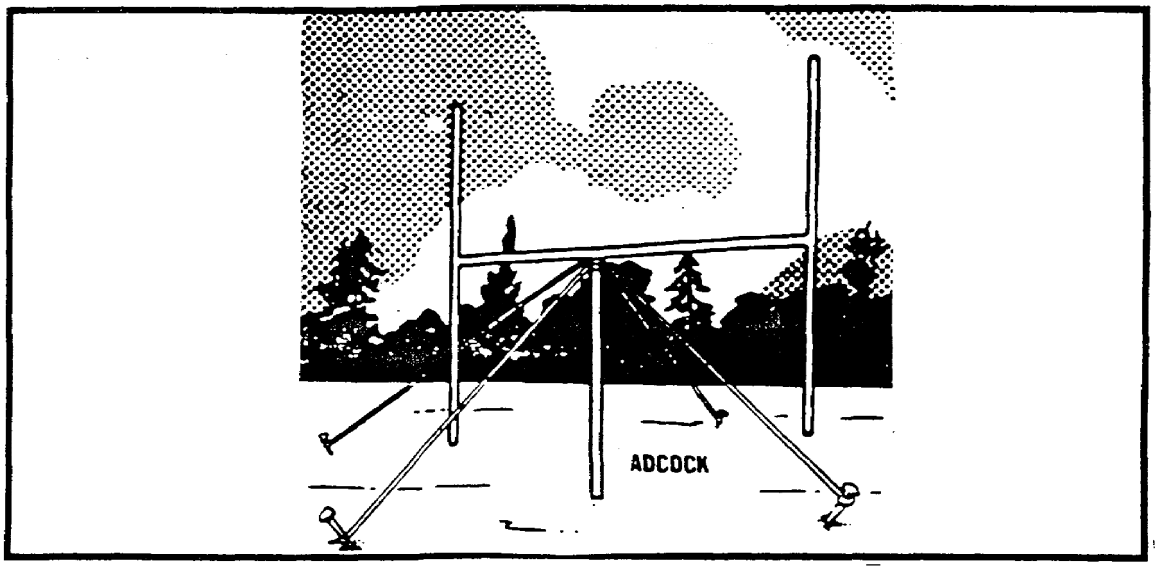


Figure 2-7. Adcock antenna.

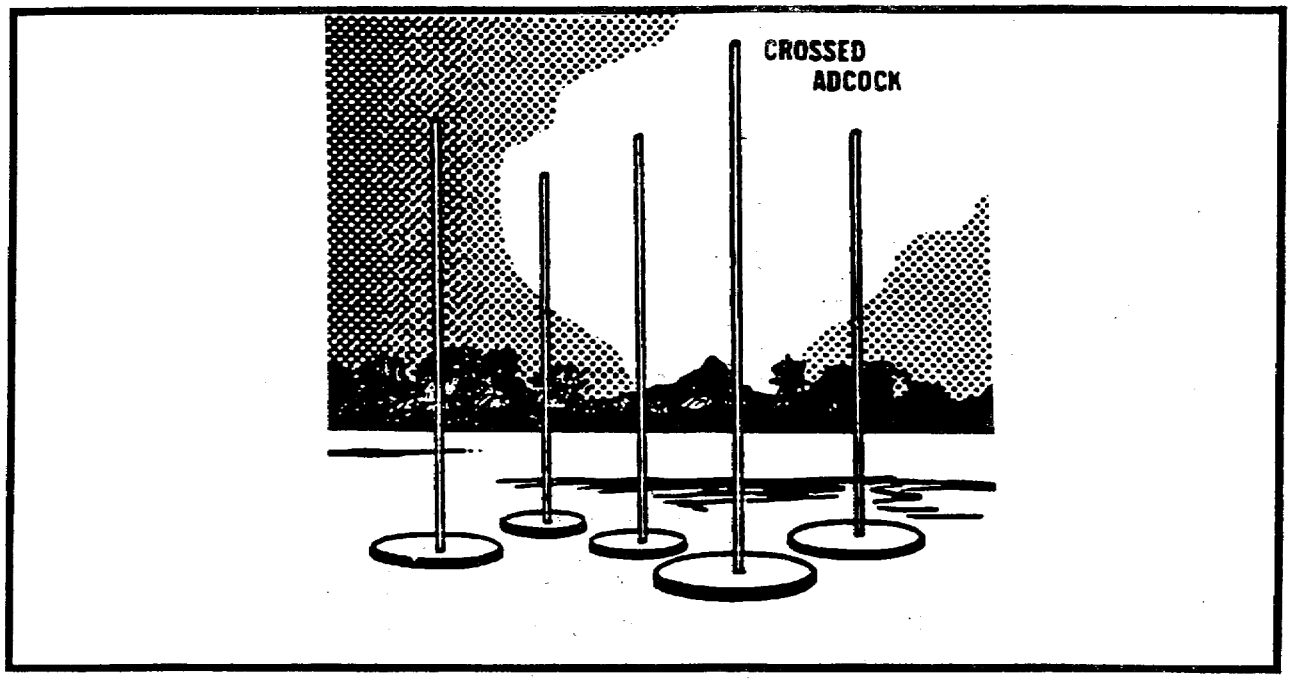


Figure 2-8. Crossed adcock antenna.

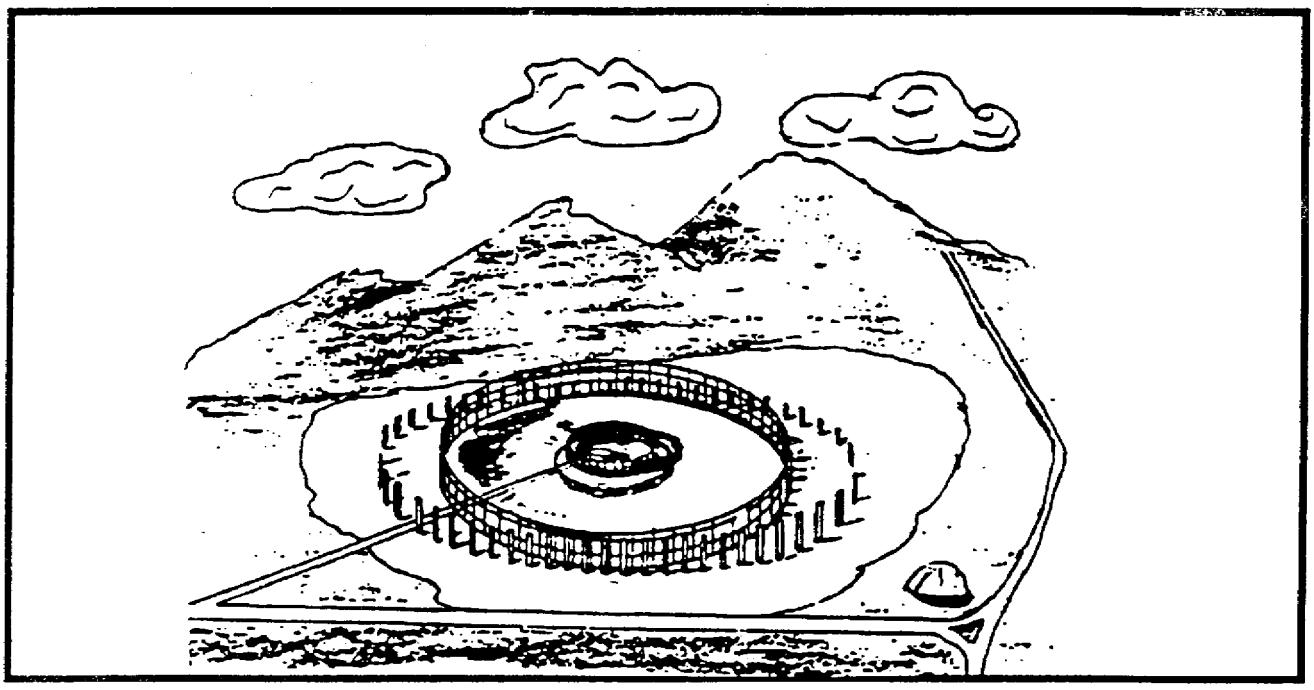


Figure 2-9. Circularly disposed antenna array.

Loop antennas are as old as radio itself. Hertz used them in the original experiments demonstrating transmission and reception, and their directional properties were known long

before there were enough transmitters to make direction finding worthwhile, A loop antenna consists of one or more turns of conductor, either self supporting or wound on a frame. The most common are diamond, square or circular loops (Figure 2-10).

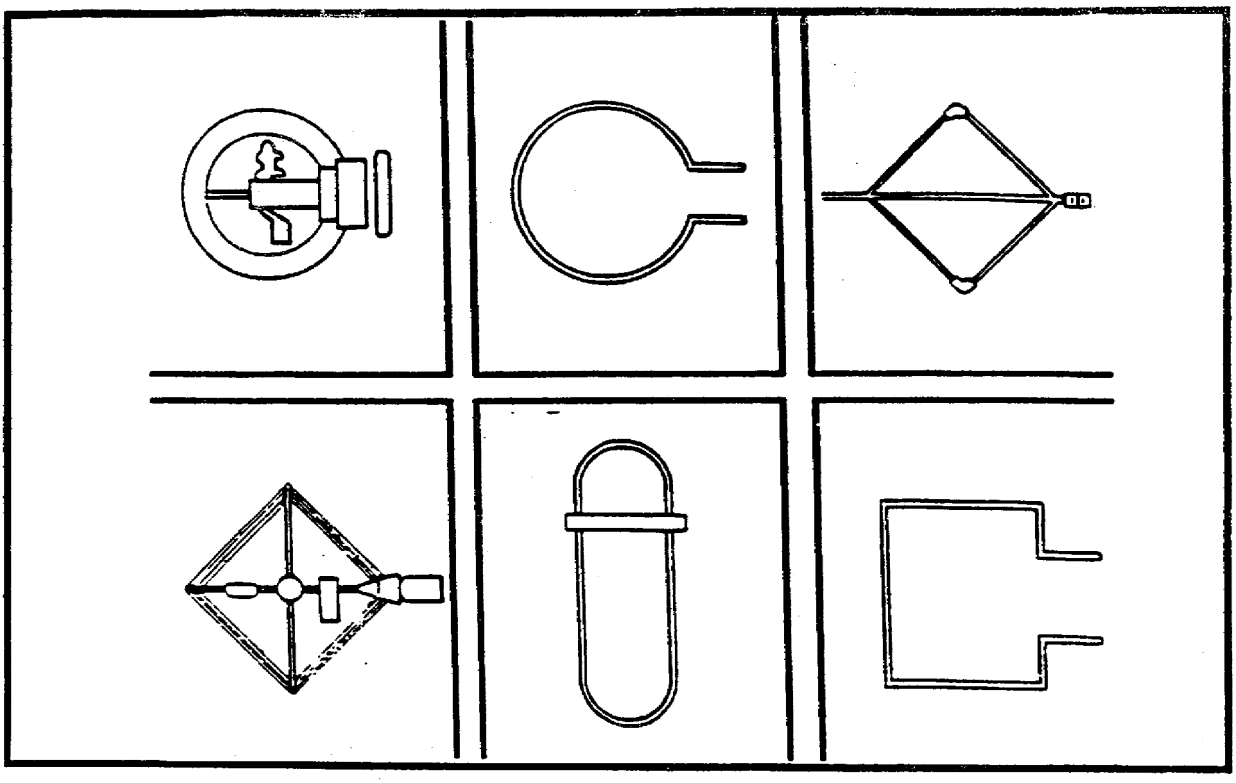


Figure 2-10. Variation of Loop Antennas.

Imagine a loop placed in the path of a vertically polarized wave and turned so that a line from side to side of the loop is parallel (plane perpendicular to the wave front) to the direction of the wave. (Refer to Figure 2-3). Since polarization is discussed in terms of the electric field, the magnetic field of a vertically polarized wave is horizontal. This horizontal magnetic field induces voltage in the loop's vertical arms and in the horizontal arms, since the wave travels parallel to them. The two voltages induced into the vertical arms tend to partially cancel across the antenna, but only partially, since the simultaneous voltages are different. This causes a voltage according to the size of the wave, or put more technically, a voltage is developed which has a magnitude relative to the field intensity of the wave. If the loop is rotated until it is broadside (plane parallel to the wave front) to the oncoming wave the voltages induced in the arms are equal and in phase with each other and cancel across the coupler to give a minimum response, or null. Two null points are present in a loop, 180 degrees apart, giving the antenna a response pattern shaped like a figure eight. (See Figure 2-11).

Unless the general direction of the transmitter is known, a direction finder equipped with a single loop cannot determine whether the transmitter lies forward or to the rear of the direction finder. There is no indication as to which of the two nulls indicates the true direction. From the previous lesson you may remember that this is known as the BIDIRECTIONAL AMBIGUITY, and solving the problem is known as resolving the bidirectional ambiguity. A sense antenna,

usually a whip, is placed at the center axis of the loop, and the two response patterns are electrically combined to produce an unbalanced pattern (cardioid, or heart-shaped) which can be used to resolve the bidirectional ambiguity.

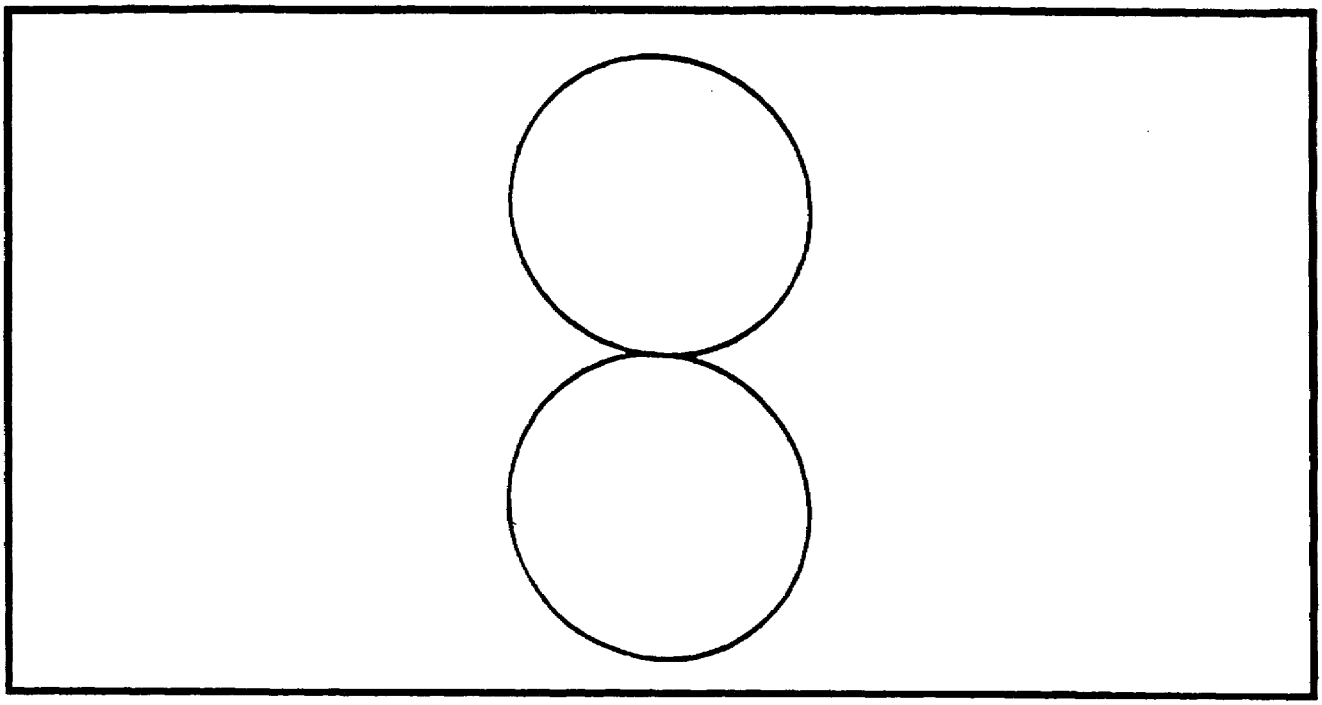


Figure 2-11. Two null points.

The crossed loop antenna consists of two loops with identical characteristics mounted at right angles to each other. Each loop has a figure eight pattern, but the two patterns are displaced 90 degrees in azimuth. As a result, the ratio of the two responses varies with direction. The outputs of the two antennas are connected through a coupler which can be rotated to find the null. This coupler is called a goniometer or a rotary coupler. Since the loops themselves are not rotated they can be made quite large for increased sensitivity. Loop and crossed loop antennas are subject to large polarization errors.

An adcock antenna consists of two spaced vertical antennas connected in opposition (one to each side of a coil). An example of a common type of Adcock is shown in Figure 2-12. In theory it responds only to the vertically polarized wave and, therefore, is not subject to polarization error. In practice there is some polarization error, but usually much less than In a loop receiving the same signal. The Adcock is preferable when medium or high frequency signals must be received at a point beyond ground wave range.

The action of the antenna, as far as vertically polarized waves are concerned, is identical with that of the loop. A resultant current in the output coil is proportional to the difference of the voltages induced in the vertical members, exactly as in the loop. Horizontally polarized components of the incoming signals do not affect the antenna because of the absence of upper and lower horizontal members and because the crossed arrangement of the center

members effectively cancels the voltage induced in them. The response pattern is the same figure eight as the loop antenna.

Both the loop and Adcock antenna have polarization errors when the incoming wave is horizontally polarized, but so long as the vertical polarization is predominant the Adcock is

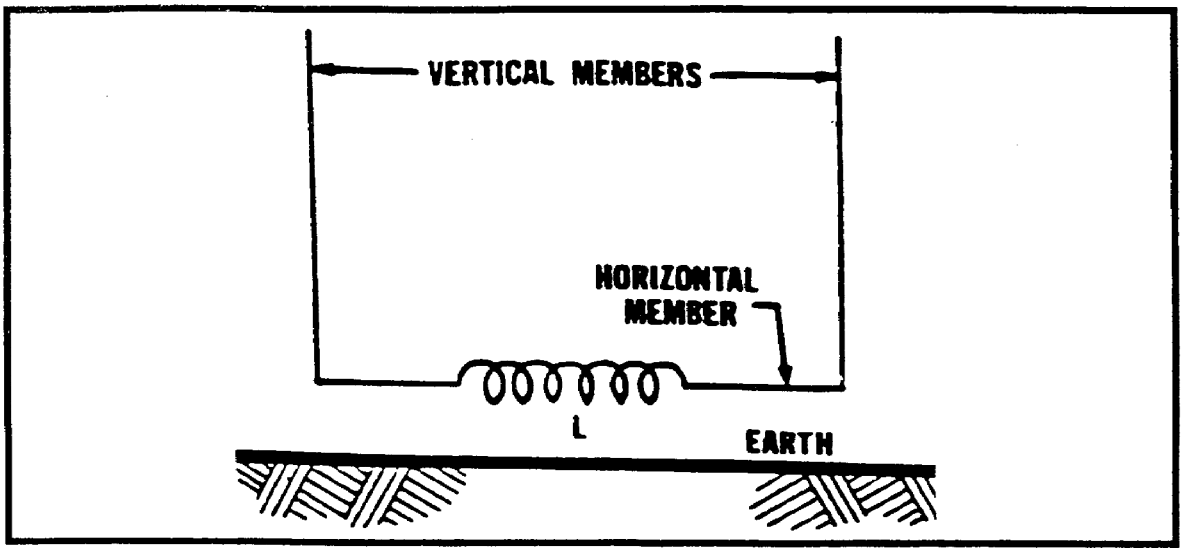


Figure 2-12. Example of adcock antenna.

relatively free from polarization error. The Adcock antenna also requires a sense antenna to resolve the bidirectional ambiguity.

The crossed Adcock antenna consists of two identical Adcock antennas oriented 90 degrees apart in azimuth. At low or medium frequencies crossed Adcock antennas can be made much larger than rotatable Adcocks and are, therefore, much more sensitive. At high frequencies this advantage is small because of the limitations imposed by spacing (OCTANTAL ERROR).

In a crossed Adcock system the maximum spacing is 1/2 wavelength between antennas (.707 wave length between diagonally spaced antennas). Above this limit the same indication may be obtained for signals coming from three different directions. (Six before sensing). Above approximately half this absolute limit the correction of octantal errors is necessary for almost every azimuth reading taken, and the nominal top frequency is usually set at this point.

Circularly disposed antenna arrays (CDAA) are the largest installations sometimes several areas in size requiring special coupling and sensing devices in order to present a directional pattern on a visual display system. (Refer to Figure 2-9) While the systems are both accurate and sensitive, direction finding is not their primary purpose.

Interferometric systems are a completely different class of direction finding systems (as illustrated in Figure 2-13). The azimuth of an incoming wave is not deduced by rotating beams. It is taken from the phase measurements of signals, made on a number of spaced antennas. Unlike the beam-forming type of WADFs, interferometers accept all signals on the

array. Two different approaches are used to process the results. Depending on the type of system, one or both of the following may be used:

- Wavefront analysis (WFA).
- Wavefront testing (WFT).

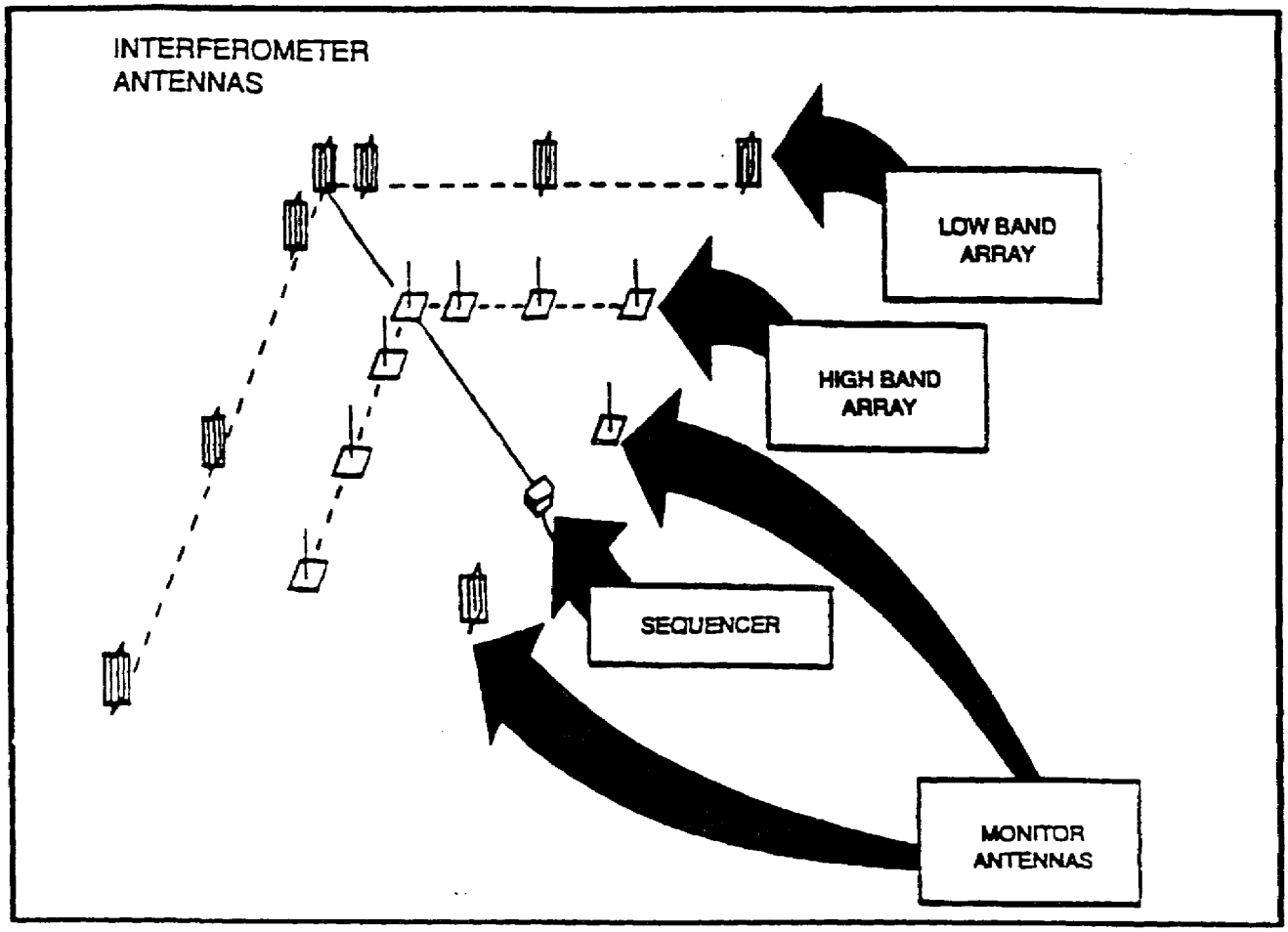


Figure 2-13. Interferometric system.

Wavefront analysis accepts all signals but attempts to recover the major ones. it attempts this by analyzing the complex voltages measured on the elements of the antenna array under wave Interference conditions.

Wavefront testing accepts only signals arriving from one direction or quasi uni-modal propagation (QUMP). QUMP is achieved by detecting a linear phase shift across the array with near equal amplitudes on all the elements. (This process is also called coincidence interferometry.)

The requirements for an efficient coupling system for DF are simple, and there are several types in use, some more complex than others, but all categorized into two groups;

(1) Systems used with fixed antennas.

(2) Systems used with rotatable antennas.

The requirements for coupling systems are:

(1) The system must efficiently conduct the energy picked up by the antenna to the radio. If this requirement is not met the direction finder will lack sensitivity.

(2) It must not pick up or otherwise add additional energy from the wanted signal. Failure to meet this requirement results in bearing errors.

(3) It must not introduce unwanted signals or noise. These effects, if present, produce interference and impair the bearing readability.

With rotatable antennas the two most common types of coupling are DIRECT, and TRANSMISSION LINE.

Direct coupling is the simplest form of coupling, directly coupling the antenna terminals to the receiver input. It is used in those few cases where it is practicable to design a DF system in which the radio receiver is located at the antenna terminals, and the antenna and receiver rotate together as a unit. Some directly coupled DF sets are small, hand-carried, transistorized receiving sets used by counterinsurgency personnel. The loop is generally the carrying handle, and the entire set is rotated to produce line bearings in the direction of the target transmitter.

Transmission line coupling is used in its simplest form when the antenna system is placed some distance above, but is rotatable with, the DF receiver. Because of its length and position the transmission line will, if its shielding or balance are not perfect, introduce unwanted energy, causing bearing errors or impaired readability. Additionally, if the length of the transmission line is an appreciable fraction of a wavelength or more, its characteristic impedance must accurately match the impedance of the receiver and the antenna, or a considerable loss of sensitivity will occur.

The direct and transmission line systems of coupling the antenna to the receiver may be used when it is desired to rotate the antenna without rotating the receiver. This is accomplished by adding a rotatable coupling element. Some of these elements are:

(1) Slip rings. These are insulated metal rings in contact with sliding fingers or brushes, which permit rotation without interrupting the circuit. By mounting the rings on a shaft and providing fixed brushes, it is possible to conduct the antenna current to a stationary receiver while permitting the antenna to turn at will.

(2) Rotating transformer. This rotatable coupling device consists of a transformer whose primary and secondary windings are coaxial. Under this condition one winding may be rotated with respect to the other without changing the coupling which exists between them.

(3) Rotating capacitator. This element makes use of the fact that the capacitance between coaxial rings or discs is independent of their rotation.

Fixed antennas use some form of goniometer. The term goniometer is applied to a device used to couple two or more input circuits (usually connected to antennas) to an output circuit (usually connected to the receiver). This is done in such a manner that the degree of coupling varies with the rotation of a shaft. The coupling between one input circuit and the output circuit decreases while the coupling with the other input circuit increases. When properly connected, a well constructed goniometer provides an output at each position of its shaft identical to that which would be produced by a single figure-eight pattern antenna oriented to the corresponding position. Thus, the goniometer provides an equivalent for the rotation of an antenna, and makes it possible to use large fixed antenna systems (either loop, Adcock, CDAA, or others) which would be too bulky for an operator to rotate.

Goniometers must meet these basic requirements:

(1) The fixed elements must be electrically identical.

(2) There must be a complete absence of coupling between the fixed elements.

(3) Accurate positioning of the fixed elements at the same angle as the antennas (usually 90 degrees) is necessary.

(4) Coupling between the rotating element and the fixed elements must vary with shaft revolution in the same manner as the variation of antenna response with azimuth angle. These requirements are met in practical goniometers to the extent that the maximum error is less than plus or minus one degree.

In applying to the goniometer to a practical direction finder, it is often desirable to locate the goniometer some distance away from the antenna. To accomplish this, it is necessary to provide transmission lines between the antenna and its goniometer. These lines must be well shielded and are usually balanced to ground to avoid stray pick-up. Additionally, the transmission lines connecting the several antennas to the goniometer must be electrically identical, particularly in time delay, over the entire frequency range of the equipment in order to preserve accuracy and provide deep nulls.

The principal types of goniometers are:

(1) Inductive, usually consisting of two fixed windings at right angles to each other and enclosing a third winding which rotates on a shaft.

(2) Capacitive, with two fixed sets of plates enclosing a rotatable set of plates, and

(3) Electronic, which utilizes circuitry instead of physical rotation, and, therefore, allows higher speeds than can be obtained by mechanical rotation.

The use of a goniometer introduces an additional possibility for octantal error above that caused by antenna spacing. This is caused by nonuniformity within the electric fields of the stationary windings of the goniometer. In early days this nonuniformity was considerable, and octanta! error was large. In more modern goniometers, the windings are distributed in such a manner that this cause of octantal error is practically eliminated. The octantal error is

caused by antenna spacing still exists, usually requiring a correction chart for the higher ranges o the equipment.

2. The type of bearing **indicator** used with any particular direction finder depends on the type of DF system in use, the complexity and physical size permitted, and the accuracy desired for a particular DF application. Many types of bearing indicators have been designed and used in DF systems, but those having the greatest application can be grouped into the categories of AURAL indicators and VISUAL indicators. Visual indicators can be further grouped into three subelements, left-right indicators, instantaneous indicators, and automatic bearing seeking indicators. Each type of indicator has certain specific characteristics and applications. Many of these characteristics are closely related to, and cannot be separated from, characteristics of the type of DF system with which a particular indicator is used. Therefore, keep in mind that some of the characteristics credited to a specific indicator are really characteristics of the DF system with which the indicator is used.

Aural Indicators. An aural indicator is a headset or loudspeaker connected to the DF receiver audio circuit. It enables the operator to detect the bearing of a signal by changes in audible receiver output as the antenna is rotated. In DF systems which use aural indicators, the antenna system must be able to be rotated to the bearing position, and this position must be characterized by an abrupt change in the antenna response pattern, and, therefore, in the receiver output.

In most common direction finders which use an aural indication the antenna is a rotatable loop or Adcock, or a fixed crossed-loop or crossed-Adcock effectively rotated by a goniometer. All these antennas have, or result in, a figure-eight response pattern with broad maxima and sharp nulls. Therefore, the nulls of the system are selected as the bearing points. Because of this, these systems are called aural-null indicators. At higher frequencies (several hundred megahertz) directional arrays having response patterns with sharp maxima can be used. Because aural-null systems are more common we will not discuss aural-maxima systems further.

The most important characteristics of an aural-null indicator are:

(1) It is the simplest indicator that can be used with a direction finder for the following reasons;

(a) it adds nothing to the direction finder because a headset or loudspeaker is usually included for monitoring purposes.

(b) it can be used with simple loop or Adcock antenna systems without the addition of complicated couplings.

(c) it reduces to a minimum the size, weight, and maintenance factors of the indicator.

(d) it is simple to use, even by unskilled operators.

(2) Because it does not necessitate the use of complicated and elaborate antenna, coupler, and receiving systems, the sensitivity and instrumental accuracy of the direction finder is high.

(3) The indicator cannot detract from the accuracy inherent in the remainder of the system.

(4) The readability of the indicator is not influenced by the type of signal received, whether it is continuous wave (cw), interrupted continuous wave (icw, or modulated continuous wave (mcw). Readability shows how the indicator can detect relatively small changes.

(5) The readability of the indicator is high on weak signals in the presence of noise or interference signals because the human ear can distinguish between desired and undesired signals.

(6) The readability is poor on fading signals because it cannot discriminate between a fade and a null indication.

(7) The readability of the indicator is poor on swinging signals because the antenna cannot be rotated fast enough to follow the swinging bearing. A swinging signal is one that because of propagation errors seems to move back and forth through several degrees of arc.

(8) An extra operation must be performed to determine which of the two directions indicates the correct azimuth (sensing).

3. Visual indicators. Visual indication has been accomplished through various means. Each has the common characteristic of operation by comparison of antenna voltages. These voltages may originate from any of several antennas. Among the types of visual indication are left-right meter, crossed pointer meter, magic eye, matched line oscilloscopes, and instantaneous oscilloscope indicators. Because the instantaneous indicators are most common this lesson will limit itself to them.

An instantaneous indicator, using a cathode ray tube, continuously and automatically presents on the tube screen a pattern or trace that points toward the azimuth of the arriving signal as read from an azimuth scale situated around the tube face. The presentation of this pattern is accomplished without manually rotating the DF antenna to the bearing point.

The antenna system must be one of the following types:

(a) It may be a fixed oriented, crossed loop or crossed Adcock variety and effectively rotated through 360 degrees at some continuous and constant rate by a spinning mechanical goniometer or electric goniometer method.

(b) The antenna system may be a single-loop or Adcock that is continuously rotated by mechanical means at a constant rate through 360 degrees.

(c) The antenna system may be of the fixed oriented, crossed loop or crossed Adcock variety and the output of each of the antennas must be maintained as separate signals through individual channels in the indicator.

(d) The antenna may be of the CDAA type and employ either antenna switching or goniometers to effectively rotate the antenna through 360 degrees at a constant rate.

Because these special features must be incorporated in a DF system using instantaneous indicator, its size, weight, power consumption, complexity of design, and maintenance are greater than for other systems. When not prohibitive, these disadvantages are more than compensated for by the increased performance obtained when using this type of indicator. Characteristics of instantaneous indicators in comparison with aural-null are as follows:

(a) There is greater speed in obtaining bearings because the antenna is usually not rotated.

(b) Simplicity of operation is increased. Tuning the receiver and reading the bearing are the only operations necessary.

(c) Readability is increased on moderate and weak signals.

(d) There is equal readability on cw, icw, and mcw signals.

(e) Readability on swinging signals is increased because the indication continuously and instantaneously changes with the bearing swing, thus enabling the operator to choose the most likely bearing.

(f) Readability on fading bearings is increased because the indicator has a high degree of discrimination between a change in signal level due to fade, and a change in bearing and signal indication.

(g) There is increased readability on combinations of swining, fading and unfavorably polarized signals, because the indicator exhibits certain features which tell the operator when conditions are most favorable for obtaining a bearing.

(h) Sense indication may be simultaneous with the presentation (continuously sensed) or it may be accomplished by pressing a key (sense switch).

(i) Readability in the presence of interfering signals is fair, although not as good as with aural indication.

4. Bearing seeking indicators. Bearing seeking indicators are normally used on aircraft where an automatic bearing readout is required but size and weight requirements preclude the use of Instantaneous visual indication. In these systems the antenna system is rotated automatically to the true bearing position and a pointer on the indicator comes to rest when it is aligned with the antenna.

LESSON 2

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. Including a receiver, what are the other basic equipment requirements needed for a DF system?

   A. Aural Null, Visual Indicator, and a Coupler
   B. Aural Null, Visual Indicator, and a Directional Antenna
   C. Coupler, Indicator, and a Directional Antenna
   D. Coupler, Indicator, and a Secondary Receiver

2. Besides stability and selectivity, what else must a DF receiver have?

   A. BFO, and Headsets
   B. BFO, and Sensitivity
   C. Sensitivity, and Headsets
   D. Sensitivity, and Frequency Range

3. What device connects the antenna to the receiver?

   A. Coupling
   B. Goniometer
   C. Frequency Modulator
   D. Antenna Modulator

4. What is an example of a visual indicator for the null?

   A. Goniometer
   B. Crossed Pointer
   C. Loudspeaker
   D. Cathode Ray Tube

5. DF equipment comes in several sizes. What are the specific requirements dictated by?

   A. The Mission
   B. The Cost
   C. The Location
   D. Transportation Capabilities

6. What part of the DF receiver is used to give a steady tone for ease of direction finding/AM signals?

   A. Aural Null
   B. BFO
   C. AM Modulator
   D. FM Modulator

7. What device is used to electrically rotate an antenna?

   A. Slip Rings and Brushes
   B. Goniometer
   C. Direct Coupling
   D. Cathode Ray Tube

8. Which is the simplest form of coupling?

   A. Transmission line
   B. Rotating
   C. Direct
   D. Indirect

9. Which antenna requires an additional sense antenna?

   A. Loop
   B. Adcock
   C. Both Loop and Adcock
   D. Neither Loop no Adcock

10. What is the most common type of visual indicator?

    A. Left-Right Meter
    B. Crossed Pointer Meter
    C. Oscilloscope Indicator
    D. Instantaneous Indicator

LESSON 2

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	C. (page 2-2)
2.	B. (page 2-4)
3.	A. (page 2-3)
4.	D. (page 2-4)
5.	A. (page 2-1)
6.	B. (page 2-4)
7.	B. (pages 2-3/2-4 and 2-15)
8.	C. (page 2-14)
9.	B. (page 2-12)
10.	D. (page 2-17)

TC 9-64

COMMUNICATIONS-ELECTRONICS FUNDAMENTALS

Wave Propagation, Transmission Lines, and Antennas

JULY 2004

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

HEADQUARTERS
DEPARTMENT OF THE ARMY

This publication is available at

Army Knowledge Online

www.us.army.mil

Training Circular
No. 9-64

Headquarters
Department of the Army
Washington, DC, 15 July 2004

Communications-Electronics Fundamentals: Wave Propagation, Transmission Lines, and Antennas

Contents

Page

Preface ..... **ix**

Chapter 1 **WAVE PROPAGATION** **1-1**
Learning Objectives 1-1
What is Propagation? 1-2
Principles of Wave Motion 1-2
Sound Waves 1-15
Light Waves 1-23
Electromagnetic Spectrum 1-30
Electromagnetic Waves 1-32
Summary 1-39

Chapter 2 **RADIO WAVE PROPAGATION** **2-1**
Learning Objectives 2-1
Electromagnetic Fields 2-2
Radio Waves 2-6
Summary 2-38

Chapter 3 **PRINCIPLES OF TRANSMISSION LINES** **3-1**
Learning Objectives 3-1
Introduction to Transmission Lines 3-1
Effect of Termination on Standing Waves 3-42
Summary 3-46

Chapter 4 **ANTENNAS** **4-1**
Learning Objectives 4-2
Radio Frequency Safety Precautions 4-2
Principles of Antenna Radiation 4-4
Current and Voltage Distribution on an Antenna 4-6
Radiation of Electromagnetic Energy 4-8
Antenna Characteristics 4-9
Reciprocity of Antennas 4-10
Basic Antennas 4-20
Summary 4-54

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes FM 11-64, 13 June 1985.

Appendix A **A-1**
Glossary **Glossary-1**
References **References-1**
Index **Index-1**

Figures

Figure 1-1. Formation of Waves in Water 1-3
Figure 1-2. How a Falling Stone Creates Wave Motion on Water's Surface 1-4
Figure 1-3. Elements of a Wave 1-4
Figure 1-4. Transverse Wave 1-5
Figure 1-5. Sound Propagation by a Tuning Fork 1-5
Figure 1-6. The Three Elements of Sound 1-6
Figure 1-7. Comparison of Waves with Different Amplitudes 1-7
Figure 1-8. Longitudinal Wave Represented Graphically by a Transverse Wave 1-9
Figure 1-9. Reflection of a Wave 1-12
Figure 1-10. Refraction of a Wave 1-13
Figure 1-11. Analogy of Reflection 1-14
Figure 1-12. No Air, No Sound 1-17
Figure 1-13. Musical Sound Versus Noise 1-18
Figure 1-14. Sound Waves Spread in All Directions 1-19
Figure 1-15. Combination of Tones 1-20
Figure 1-16. Refraction of Sound 1-22
Figure 1-17. Waves and Radii from a Nearby Light Source 1-25
Figure 1-18. Use of a Prism to Split White Light into Different Colors 1-26
Figure 1-19. Light Waves Reflected, Absorbed, and Transmitted 1-27
Figure 1-20. Transparent, Translucent, and Opaque Substances 1-28
Figure 1-21. Diffusion of Light 1-30
Figure 1-22. Electromagnetic Spectrum 1-32
Figure 1-23. Simple Radio Communication System 1-33
Figure 1-24. Antenna 1-34
Figure 1-25. Electric Fields between Plates 1-36
Figure 1-26. Electric Fields between Plates at Different Angles 1-36
Figure 1-27. Electric Fields between Elements 1-37
Figure 1-28. Magnetic Fields around Elements 1-38
Figure 1-29. Left-Hand Rule for Conducting Elements 1-39
Figure 1-30. Relationship of E-Lines and Current Flow 1-40
Figure 1-Sum 1. Formation of Waves in Water 1-41
Figure 1-Sum 2. Elements of a Wave 1-41
Figure 1-Sum 3. The Three Elements of Sound 1-41
Figure 1-Sum 4. Reflection of a Wave 1-42
Figure 1-Sum 5. Refraction of a Wave 1-43
Figure 1-Sum 6. Musical Sound Versus Noise 1-44
Figure 1-Sum 7. Use of a Prism to Split White Light into Different Colors 1-45
Figure 1-Sum 8. Electromagnetic Spectrum 1-46
Figure 2-1. Induction Field about an Antenna 2-3
Figure 2-2. Phase Relationship of Induction Field Components 2-4

Figure 2-3. Radiation from an Antenna 2-5
Figure 2-4. E and H Components of Induction and Radiation Fields 2-6
Figure 2-5. Vertical and Horizontal Polarization 2-10
Figure 2-6. Right-Hand Rule for Propagation 2-11
Figure 2-7. Phase Shift of Reflected Radio Waves 2-12
Figure 2-8. Radio Wave Refraction 2-13
Figure 2-9. Diffraction around an Object 2-14
Figure 2-10. Layers of the Earth's Atmosphere 2-15
Figure 2-11. Ground Waves and Sky Waves 2-16
Figure 2-12. Surface Wave Propagation 2-17
Figure 2-13. Space Wave Propagation 2-18
Figure 2-14. Layers of the Ionosphere 2-21
Figure 2-15. Effects of Ionospheric Density on Radio Waves 2-22
Figure 2-16. Frequency Versus Refraction and Distance 2-23
Figure 2-17. Different Incident Angles of Radio Waves 2-23
Figure 2-18. Effects of Frequency on the Critical Angle 2-24
Figure 2-19. Relationship between Skip Zone, Skip Distance, and Ground Wave 2-25
Figure 2-20. Ray Paths for a Fixed Frequency with Varying Angles of Incidence 2-26
Figure 2-21. Multipath Transmission 2-28
Figure 2-22. Freespace Loss Principle 2-29
Figure 2-23. Refraction of Frequency below the Lowest Usable Frequency (LUF) 2-34
Figure 2-24. RF Energy Losses from Scattering 2-36
Figure 2-25. Duct Effect Caused by Temperature Inversion 2-37
Figure 2-26. Tropospheric Scattering Propagation 2-38
Figure 2-Sum 1. Vertical and Horizontal Polarization 2-40
Figure 2-Sum 2. Phase Shift of Reflected Radio Waves 2-41
Figure 2-Sum 3. Ground and Sky Waves 2-41
Figure 2-Sum 4. Surface Wave Propagation 2-42
Figure 2-Sum 5. Space Wave Propagation 2-42
Figure 2-Sum 6. Layers of the Ionosphere 2-43
Figure 2-Sum 7. Frequency Versus Refraction and Distance 2-43
Figure 2-Sum 8. Effects of Frequency on Critical Angle 2-44
Figure 2-Sum 9. Relationship between Skip Zone, Skip Distance, and Ground Wave 2-44
Figure 2-Sum 10. Multipath Transmission 2-45
Figure 2-Sum 11. Refraction of Frequency below the Lowest Usable Frequency (LUF) 2-45
Figure 2-Sum 12. Duct Effect Caused by Temperature Inversion 2-46
Figure 2-Sum 13. Tropospheric Scattering Propagation 2-46
Figure 3-1. Basic Transmission Line 3-2
Figure 3-2. Parallel Two-Wire Open Line 3-3
Figure 3-3. Two-Wire Ribbon Line 3-3
Figure 3-4. Twisted Pair 3-4
Figure 3-5. Shielded Pair 3-4
Figure 3-6. Rigid (Air) Coaxial Line 3-5

Figure 3-7. Flexible (Solid) Coaxial Line 3-6
Figure 3-8. Waveguides 3-6
Figure 3-9. Equivalent Circuit of a Two-Wire Transmission Line 3-11
Figure 3-10. Distributed Inductance 3-11
Figure 3-11. Distributed Capacitance 3-12
Figure 3-12. Distributed Resistance 3-12
Figure 3-13. Leakage in a Transmission Line 3-13
Figure 3-14. Fields between Conductors 3-13
Figure 3-15. Short Section of Two-Wire Transmission Line and Equivalent Circuit 3-15
Figure 3-16. Characteristic Impedance 3-16
Figure 3-17 Termination of a Line 3-18
Figure 3-18. DC Voltage Applied to a Line 3-20
Figure 3-19. AC Voltage Applied to a Transmission Line 3-20
Figure 3-20. DC Applied to an Equivalent Transmission Line 3-21
Figure 3-21. AC Applied to an Equivalent Transmission Line 3-22
Figure 3-22. Instantaneous Voltages along a Transmission Line 3-23
Figure 3-23. DC Applied to an Equivalent Transmission Line 3-25
Figure 3-24. Reflection from an Open-Ended Line 3-29
Figure 3-25. Reflection from a Short-Circuited Line 3-31
Figure 3-26. Formation of Standing Waves 3-32
Figure 3-27. Instantaneous Values of Incident and Reflected Waves on an Open-Ended Line 3-34
Figure 3-28. Conventional Picture of Standing Waves 3-35
Figure 3-29. Composite Results of Instantaneous Waves 3-36
Figure 3-30. Standing Waves on a Shorted Line 3-37
Figure 3-31. Sending-End Impedance of Various Lengths and Terminations 3-39
Figure 3-32. Voltage, Current, and Impedance on Open Line 3-41
Figure 3-33. Voltage, Current, and Impedance on Shorted Line 3-42
Figure 3-34. Effects of Various Terminations on Standing Waves 3-44
Figure 3-Sum 1. Two-Wire Open Line 3-48
Figure 3-Sum 2. Two-Wire Ribbon Type Line 3-48
Figure 3-Sum 3. Twisted Pair 3-48
Figure 3-Sum 4. Shielded Pair 3-49
Figure 3-Sum 5. Rigid (Air) Coaxial Line 3-49
Figure 3-Sum 6. Flexible (Solid) Coaxial Lines 3-49
Figure 3-Sum 7. Waveguides 3-50
Figure 3-Sum 8. Equivalent Circuit of a Two-Wire Transmission Line 3-50
Figure 3-Sum 9. Distributed Constants 3-51
Figure 3-Sum 10. Leakage in a Transmission Line 3-51
Figure 3-Sum 11. Fields between Conductors 3-52
Figure 3-Sum 12. Characteristic Impedance 3-52
Figure 3-Sum 13. Formation of Standing Wave 3-53
Figure 3-Sum 14. Instantaneous Values of Incident and Reflected Waves 3-53
Figure 3-Sum 15. Voltage, Current, and Impedance on a Shorted Line 3-54

Figure 3-Sum 16. Various Termination Effects on Standing Waves 3-55
Figure 4-1. Satellite/Earth Station Communications System 4-1
Figure 4-2. Warning Signs for Radio Frequency Radiation Hazards 4-3
Figure 4-3. Typical Antenna System 4-5
Figure 4-4. Typical Antennas 4-6
Figure 4-5. Current and Voltage Distribution on a Antenna 4-7
Figure 4-6. Antenna and RF Source 4-8
Figure 4-7. Standing Waves of Voltage and Current on an Antenna 4-9
Figure 4-8. Reciprocity of Antenna 4-11
Figure 4-9. Satellite Transmissions Using Polarized Radiation 4-13
Figure 4-10. Isotropic Radiator 4-15
Figure 4-11. Comparison of Rectangular and Polar-Coordinate Graph for an Isotropic Source 4-16
Figure 4-12. Anisotropic Radiator 4-19
Figure 4-13. Polar-Coordinate Graph for Anisotropic Radiator 4-20
Figure 4-14. Electrically Equal Antenna 4-22
Figure 4-15. Development of Vertical and Horizontal Pattern 4-23
Figure 4-16. Radiation Pattern of a Dipole 4-24
Figure 4-17. Standing Waves of Current and Voltage 4-25
Figure 4-18. Mobile Antennas 4-26
Figure 4-19. Grounded Quarter-Wave Antenna Image 4-26
Figure 4-20. Ground Screen and Counterpoise 4-27
Figure 4-21. Folded-Dipole Antennas 4-28
Figure 4-22. Phasing of Antenna in Free Space 4-31
Figure 4-23. Phasing of Connected Elements 4-32
Figure 4-24. Directivity and Interference 4-33
Figure 4-25. Single Antenna Versus Array 4-34
Figure 4-26. Single Half-Wave Antenna versus Two Half-Wave Antenna in Phase 4-35
Figure 4-27. Typical Broadside Array 4-37
Figure 4-28. Parallel Elements in Phase 4-38
Figure 4-29. Typical End-Fire Array 4-39
Figure 4-30. Parallel Elements 180 Degrees Out of Phase 4-40
Figure 4-31. Unidirectional End-Fire Arrays 4-42
Figure 4-32. Patterns Obtained Using a Reflector with Proper Spacing 4-44
Figure 4-33. Yagi Antenna 4-46
Figure 4-34. Typical Parasitic Array Used for Transmitting and Receiving 4-47
Figure 4-35. Beverage Antenna 4-48
Figure 4-36. Basic V Antenna 4-49
Figure 4-37. Formation of Directional Radiation from a Resonant V Antenna 4-49
Figure 4-38. Basic Rhombic Antenna 4-50
Figure 4-39. Formation of a Rhombic Antenna Beam 4-51
Figure 4-40. Turnstile Antenna Radiation Pattern 4-53
Figure 4-41. Stacked Turnstile Antenna 4-54
Figure 4-42. Ground-Plane Antenna 4-55

Figure 4-43. Corner-Reflector Antenna 4-56
Figure 4-Sum 1. Reciprocity of Antennas 4-57
Figure 4-Sum 2. Radiation Patterns 4-58
Figure 4-Sum 3. Radiating Energy of an Isotropic Radiator 4-59
Figure 4-Sum 4. Directional Radiating Energy of an Anisotropic Radiator 4-60
Figure 4-Sum 5. Null and Lobe Radiation Patterns 4-61
Figure 4-Sum 6. Antenna Loading 4-61
Figure 4-Sum 7. Half-Wave Antenna Pattern 4-62
Figure 4-Sum 8. Quarter-Wave Antenna 4-62
Figure 4-Sum 9. Ground Screen and Counterpoise Antennas 4-63
Figure 4-Sum 10. Folded Dipole 4-63
Figure 4-Sum 11. Broadside Array Elements 4-64
Figure 4-Sum 12. End-Fire Array 4-65
Figure 4-Sum 13. Parasitic Array 4-65
Figure 4-Sum 14. Multi-Element Arrays 4-66
Figure 4-Sum 15. Long-Wire Antenna 4-66
Figure 4-Sum 16. Beverage Antenna Wavelengths 4-66
Figure 4-Sum 17. V Antenna Layout 4-67
Figure 4-Sum 18. Rhombic Antenna Conductors 4-67
Figure 4-Sum 19. Turnstile Antenna 4-68

Tables

Table 1-1. Comparison of Velocity of Sound in Various Mediums 1-21
Table 1-2. Comparison of Light Waves and Sound Waves 1-31
Table 2-1. Radio Frequency Bands 2-7
Table 2-2. Surface Conductivity 2-17

Preface

This manual is a reference text for trainees and other personnel in the communications-electronics field. It provides information about wave propagation, transmission lines, and antennas. This manual also identifies important safety practices to follow when working with electromagnetic radiation.

The proponent of this publication is Headquarters, U.S. Army Training and Doctrine Command (TRADOC). Send comments and recommendations for improving this document on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) directly to: Commander, USACASCOM&FL, Training Directorate, Ordnance Training Division, ATTN: ATCL-AO, 401 First Street, Fort Lee, Virginia 23801.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Chapter 1

Wave Propagation

The methods used to propagate (transmit) waves through space are based on the same physical principles today as they were 70 years ago. In this chapter, we discuss propagation theory on an introductory level, without going into the technical details that concern the engineer. Understanding wave propagation requires you to use your imagination to visualize the associated concepts and how they are used in practical application. To help you in this process, this chapter includes many illustrations and step-by-step descriptions that guide you from simple concepts to more complex ideas. This chapter covers the fundamentals of wave propagation and the physical factors that affect propagation. Many of the principles discussed are observable in common, everyday occurrences with which you are already familiar.

LEARNING OBJECTIVES

1-1. Learning objectives are included at the beginning of each chapter and serve as a preview of the information you are expected to learn. Comprehensive check questions are included at the end of the chapters and are based on the learning objectives. Upon completing this chapter, you should be able to do the following:

- State what wave motion is; define the terms reflection, refraction, and diffraction; and describe the Doppler effect.
- State what sound waves are and define a propagating medium.
- List and define terms as applied to sound waves, such as cycle, frequency, wavelength, and velocity.
- List the three requirements for sound.
- Define pitch, intensity, loudness, and quality and their application to sound waves.
- State the acoustical effects that echoes, reverberation, resonance, and noise have on sound waves.
- Define light waves and list their characteristics.
- List the various colors of light and define the terms reflection, refraction, diffusion, and absorption as applied to light waves.
- State the difference between sound waves and light waves.
- State the electromagnetic wave theory and list the components of the electromagnetic wave.

WHAT IS PROPAGATION?

1-2. Early man was quick to recognize the need to communicate beyond the range of the human voice. To satisfy this need, he developed alternate methods of communication, such as hand gestures, beating on a hollow log, and smoke signals. Although these methods were effective, they were still greatly limited in range. Eventually, the range limitations were overcome by the development of courier and postal systems; but there was then a problem of speed. For centuries the time required to deliver a message depended on the speed of a horse.

1-3. During the latter part of the nineteenth century, both distance and time limitations were largely overcome. The invention of the telegraph made possible instantaneous communication over long wires. Then a short time later, man discovered how to transmit messages in the form of radio waves.

1-4. As you will learn in this chapter, radio waves are propagated. Propagation means "movement through a medium." Light rays most easily illustrate this concept. When a light is turned on in a darkened room, light rays travel from the light bulb throughout the room. When a flashlight is turned on, light rays also radiate from its bulb, but are focused into a narrow beam. You can use these examples to picture how radio waves propagate. Like the light in the room, radio waves may spread out in all directions. They can also be focused (concentrated) like the flashlight, depending upon the need. Radio waves are a form of radiant energy, similar to light and heat. Although they can neither be seen nor felt, their presence can be detected through the use of sensitive measuring devices. The speed at which both forms of waves travel is the same; they both travel at the speed of light.

1-5. You may wonder why you can see light but not radio waves, which consist of the same form of energy as light. The reason is that you can see only what your eyes can detect. Your eyes can detect radiant energy only within a fixed range of frequencies. Because the frequencies of radio waves are below the frequencies your eyes can detect, you cannot see radio waves.

PRINCIPLES OF WAVE MOTION

1-6. All things on the land, or in the water are showered continually with waves of energy. Some of these waves stimulate our senses and can be seen, felt, or heard. For instance, we can see light, hear sound, and feel heat. However, there are some waves that do not stimulate our senses. For example, radio waves, such as those received by our portable radio or television sets, cannot be seen, heard, or felt. A device must be used to convert radio waves into light (TV pictures) and sound (audio) for us to sense them.

1-7. A wave can be defined as a disturbance (e.g., sound, light, radio waves) that moves through a medium (e.g., air, water, vacuum). To help you understand what is meant by "a disturbance that moves through a medium," picture the following illustration. You are standing in the middle of a wheat field. As the wind blows across the field toward you, you can see the wheat stalks bending and rising as the force of the wind moves into and across them. The wheat appears to be moving toward you, but it isn't. Instead, the stalks are actually moving back and forth. We can then say that the

"medium" in this illustration is the wheat and the "disturbance" is the wind moving the stalks of wheat.

1-8. Wave motion can be defined as a recurring disturbance advancing through space with or without the use of a physical medium. Wave motion, therefore, is a means of moving or transferring energy from one point to another point. For example, when sound waves strike a microphone, sound energy is converted into electrical energy. When light waves strike a phototransistor or radio waves strike an antenna, they are likewise converted into electrical energy. Therefore, sound, light, and radio waves are all forms of energy that are moved by wave motion. We discuss sound waves, light waves, and radio waves later in this chapter.

WAVE MOTION IN WATER

1-9. A type of wave motion familiar to almost everyone is the movement of waves in water. We explain these waves first to help you understand wave motion and the terms used to describe it.

1-10. Basic wave motion can be shown by dropping a stone into a pool of water (see figure 1-1). As the stone enters the water, a surface disturbance is created, resulting in an expanding series of circular waves.

Figure 1-1. Formation of Waves in Water

1-11. Figure 1-2 is a diagram of this action. View A shows the falling stone just an instant before it strikes the water. View B shows the action taking place at the instant the stone strikes the surface, pushing the water that is around it upward and outward. In view C, the stone has sunk deeper into the water, which has closed violently over it causing some spray, while the leading wave has moved outward. An instant later, the stone has sunk out of sight, leaving the water disturbed as shown in view D. Here the leading wave has continued to move outward and is followed by a series of waves gradually diminishing in amplitude. Meanwhile, the disturbance at the original point of contact has gradually subsided.

1-12. In this example, the water is not actually being moved outward by the motion of the waves, but up and down as the waves move outward. The up and down motion is transverse, or at right angles, to the outward motion of the waves. This type of wave motion is called transverse wave motion.

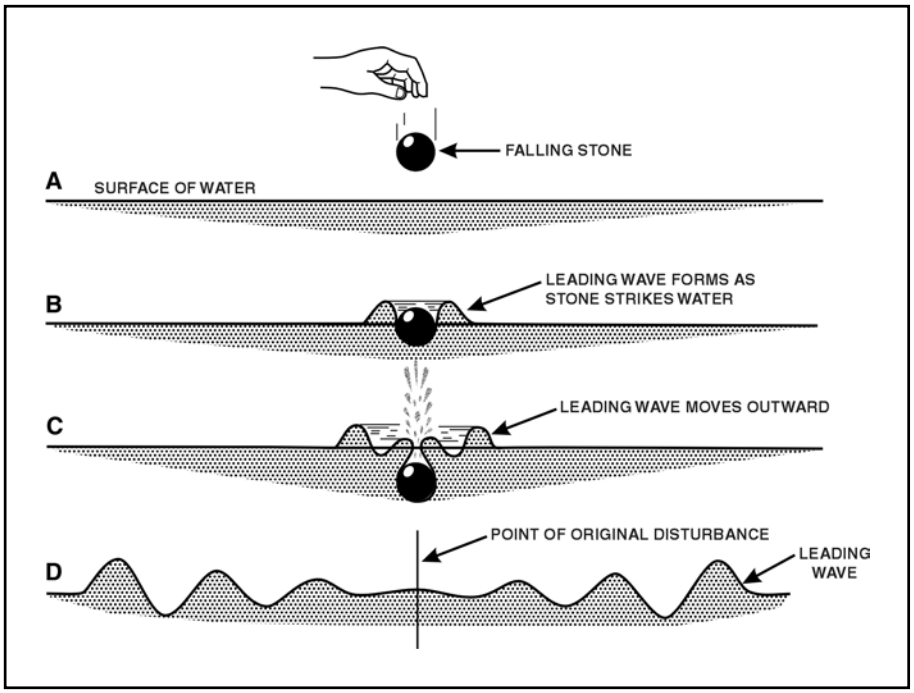


Figure 1-2. How a Falling Stone Creates Wave Motion on Water's Surface

TRANSVERSE WAVES

1-13. To explain transverse waves, we again use our example of water waves. Figure 1-3 is a cross-section diagram of waves viewed from the side. Notice that the waves are a succession of crests and troughs. The wavelength (one 360-degree cycle) is the distance from the crest of one wave to the crest of the next, or between any two similar points on adjacent waves. The amplitude of a transverse wave is half the distance measured vertically from the crest to the trough. Water waves are known as transverse waves because the motion of the water is up and down, or at right angles to the direction in which the waves are traveling. You can see this by observing a cork bobbing up and down on water as the waves pass by; the cork moves very little in a sideways direction.

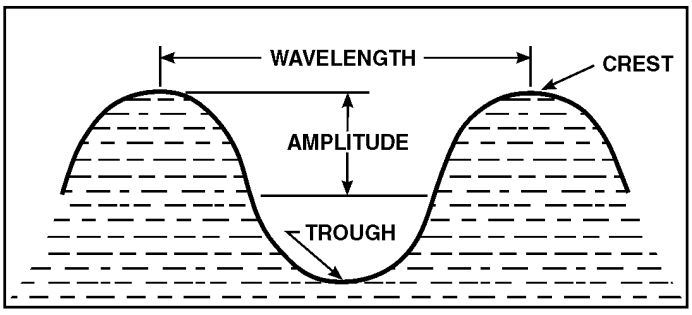


Figure 1-3. Elements of a Wave

1-14. In figure 1-4, the small arrows show the up-and-down direction the cork moves as the transverse wave is set in motion. The large arrow shows the direction the wave travels. Radio waves, light waves, and heat waves are examples of transverse waves.

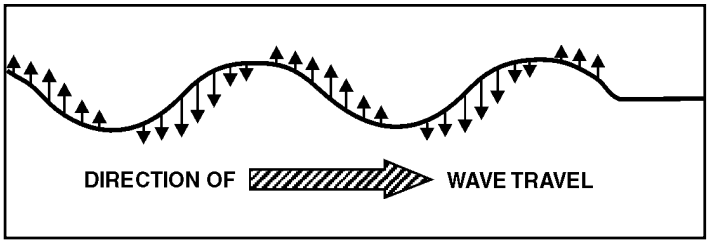


Figure 1-4. Transverse Wave

LONGITUDINAL WAVES

1-15. In the previous discussion, we listed radio waves, light waves, and heat waves as examples of transverse waves, but we did not mention sound waves. Why? Simply because sound waves are longitudinal waves. Unlike transverse waves, which travel at right angles to the direction of propagation, sound waves travel back and forth in the same direction as the wave motion. Therefore, longitudinal waves are waves in which the disturbance takes place in the direction of propagation. Longitudinal waves are sometimes called compression waves.

1-16. Waves that make up sound, such as those set up in the air by a vibrating tuning fork, are longitudinal waves. When struck, the tuning fork in figure 1-5 sets up vibrations. As the tine moves in an outward direction, the air immediately in front of it is compressed (made more dense) so that its momentary pressure is raised above that at other points in the surrounding medium (air). Because air is elastic, the disturbance is transmitted in an outward direction as a compression wave. When the tine returns and moves in the inward direction, the air in front of the tine is rarefied (made less dense or expanded) so that its pressure is lowered below that of the other points in the surrounding air. The rarefied wave is propagated from the tuning fork and follows the compressed wave through the medium (air).

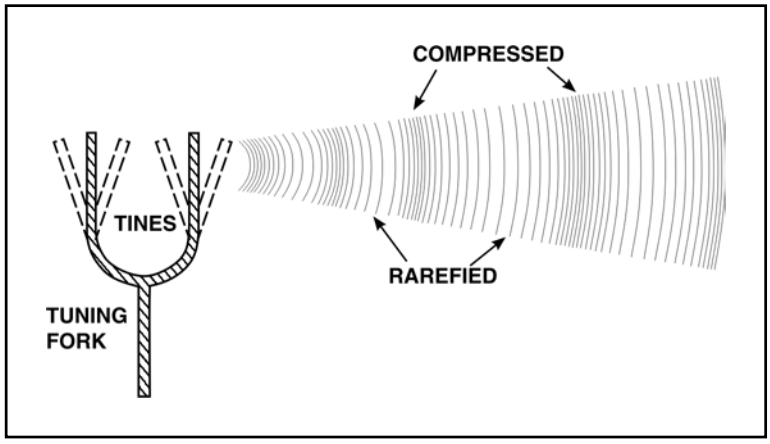


Figure 1-5. Sound Propagation by a Tuning Fork

MEDIUM

1-17. We have used the term medium in describing the motion of waves. Because medium is a term that is used frequently in discussing propagation, it needs to be defined so you will understand what a medium is and its application to propagation.

1-18. A medium is the vehicle through which the wave travels from one point to the next. The vehicle that carries a wave can be just about anything. An example of a medium, already mentioned, is air. Air, as defined by the dictionary, is the mixture of invisible, odorless, tasteless gases that surrounds the earth (the atmosphere). Air is made up of molecules of various gases (and impurities). We will call these molecules of air particles of air or simply particles. Figure 1-6 can help you to understand how waves travel through air. The object producing the waves is called the source—a bell in this illustration. The object responding to the waves is called a detector or receiver; in this case, the human ear. The medium is air, which is the means of conveying the waves from the source to the detector. The source, detector, and medium are all necessary for wave motion and wave propagation (except for electromagnetic waves, which require no medium). The waves shown in figure 1-6 are sound waves. As the bell is rung, the particles of air around the bell are compressed and then expanded. This compression and expansion of particles of air set up a wave motion in the air. As the waves are produced, they carry energy from particle to particle through the medium (air) to the detector (ear).

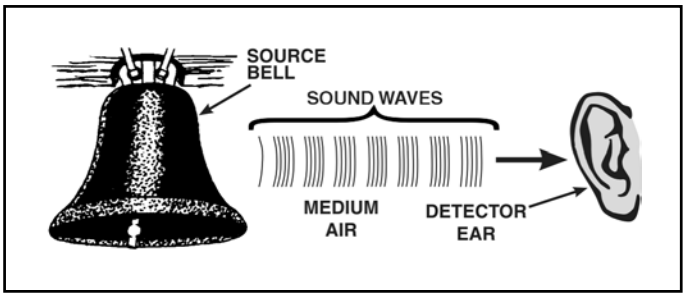


Figure 1-6. The Three Elements of Sound

TERMS USED IN WAVE MOTION

1-19. There are a number of special terms concerning waves that you should know. Many of the terms, such as cycle, wavelength, amplitude, and frequency, were introduced in TC 9-60. We now discuss these terms in detail as they pertain to wave propagation. Before we begin our discussion, however, note that in figure 1-7, wave 1 and wave 2 have equal frequency and wavelength but different amplitudes. The reference line (also known as rest position or point of zero displacement) is the position that a particle of matter would have if it were not disturbed by wave motion. For example, in the case of the water wave, the reference line is the level of the water when no wave motion is present. With this in mind, let us go on to our discussion of the four terms, as shown in figure 1-7.

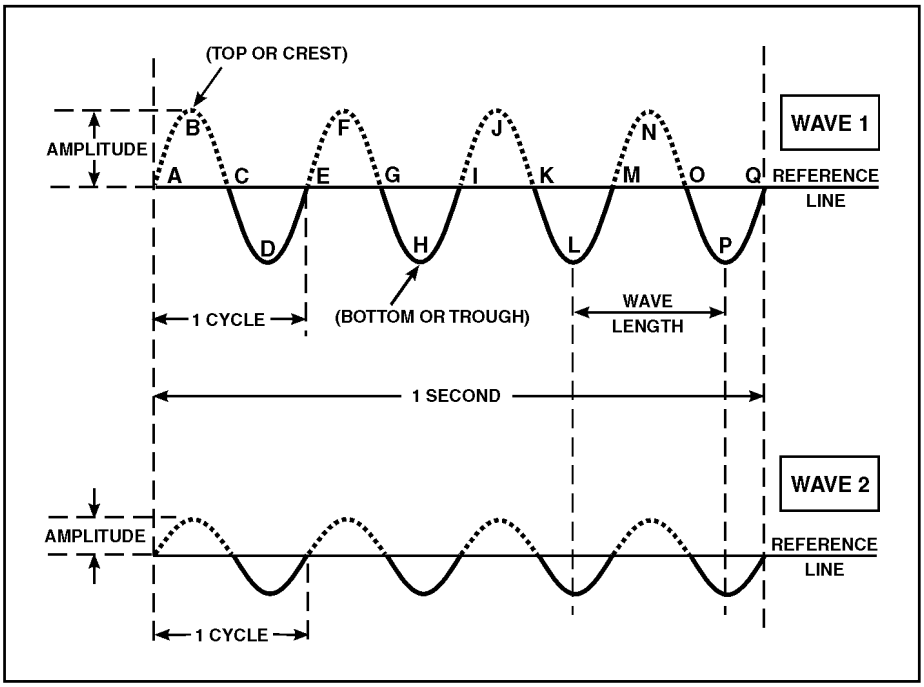


Figure 1-7. Comparison of Waves with Different Amplitudes

Wave Cycles

1-20. Refer to wave 1 in figure 1-7. Notice how similar it is to the sine wave you have already studied. All transverse waves appear as sine waves when viewed from the side. In figure 1-7, wave 1 has four complete wave cycles. Points ABCDE comprise one complete cycle having a maximum value above and a maximum value below the reference line. The portion above the reference line (between points A and C) is called a positive alternation and the portion below the reference line (between points C and E) is known as a negative alternation. The combination of one complete positive and one complete negative alternation represents one cycle of the wave. At point E, the wave begins to repeat itself with a second cycle completed at point I, a third at point M, and so forth. The peak of the positive alternation (maximum value above the line) is sometimes referred to as the top or crest, and the peak of the negative alternation (maximum value below the line) is sometimes called the bottom or trough, as depicted in the figure. Therefore, one cycle has one crest and one trough.

Wavelength

1-21. A wavelength is the distance in space occupied by one cycle of a radio wave at any given instant. If the wave could be frozen in place and measured, the wavelength would be the distance from the leading edge of one cycle to the corresponding point on the next cycle. Wavelengths vary from a few hundredths of an inch at extremely high frequencies to many miles at extremely low frequencies; however, common practice is to express wavelengths in meters. In figure 1-7 (wave 1), the distance between A and E, or B and F, etc., is one wavelength. The Greek letter lambda (λ) is used to signify wavelength. Why lambda and not "l" or "L"? This is because "L" is

used conventionally as the symbol for inductance, and "l" is used for dimensional length; therefore, λ is used to indicate the length of waves.

Amplitude

1-22. Two waves may have the same wavelength, but the crest of one may rise higher above the reference line than the crest of the other. Compare wave 1 and wave 2 of figure 1-7 again. The height of a wave crest above the reference line is called the amplitude of the wave. The amplitude of a wave gives a relative indication of the amount of energy the wave transmits. A continuous series of waves, such as A through Q, having the same amplitude and wavelength, is called a train of waves or wave train.

Frequency and Time

1-23. Time is an important factor in wave studies. When a wave train passes through a medium, a certain number of individual waves pass a given point in a specific unit of time. For example, if a cork on a water wave rises and falls once every second, the wave makes one complete up-and-down vibration every second. The number of vibrations, or cycles, of a wave train in a unit of time is called the frequency of the wave train and is measured in hertz. If 5 waves pass a point in one second, the frequency of the wave train is 5 cycles per second. In figure 1-7, the frequency of both wave 1 and wave 2 is four cycles per second (abbreviated as cps).

1-24. In 1967, in honor of the German physicist Heinrich Hertz, the term hertz was designated for use in lieu of the term "cycle per second" when referring to the frequency of radio waves. It may seem confusing that in one place the term "cycle" is used to designate the positive and negative alternations of a wave, but in another instance the term "hertz" is used to designate what appears to be the same thing. The key is the time factor. The term cycle refers to any sequence of events, such as the positive and negative alternations, comprising one cycle of electrical current. The term hertz refers to the number of occurrences that take place in one second.

CHARACTERISTICS OF WAVE MOTION

1-25. The two types of wave motion, transverse and longitudinal, have many of the same characteristics, such as frequency, amplitude, and wavelength. Another important characteristic that these two types of wave motion share is velocity. Velocity of propagation is the rate at which the disturbance travels through the medium, or the velocity with which the crest of the wave moves along. The velocity of the wave depends both on the type of wave (e.g., light, sound, or radio) and type of medium (e.g., air, water, or metal). If longitudinal waves are plotted as a graph, they appear as transverse waves. This fact is illustrated in figure 1-8. The frequency of a longitudinal wave, like that of a transverse wave, is the number of complete cycles the wave makes during a specific unit of time. The higher the frequency, the greater is the number of compressions and expansions per unit of time.

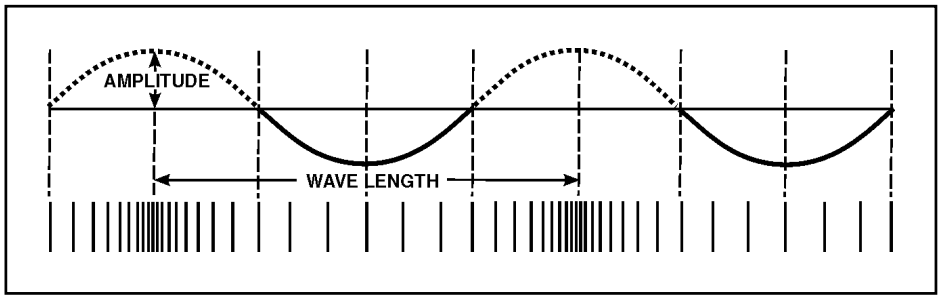


Figure 1-8. Longitudinal Wave Represented Graphically by a Transverse Wave

1-26. In the two types of wave motion described in the preceding discussion, the following quantities are of interest:

- The period, which is the time (T) in which one complete vibratory cycle of events occurs.
- The frequency of vibration (f), which is the number of cycles taking place in one second.
- The wavelength (λ), which is the distance the disturbance travels during one period of vibration.

1-27. Now, consider the following concept. If a vibrating object makes a certain number of vibrations per second, then 1 second divided by the number of vibrations is equal to the period of time of 1 vibration. In other words, the period, or time of 1 vibration is the reciprocal of the frequency. Thus—

$$\text{Time (T) of one vibration} = \frac{1}{\text{frequency (f)}}$$

Or

$$T = \frac{1}{f}$$

1-28. If you know the velocity of a wave, you can determine the wavelength by dividing the velocity by the frequency. As an equation—

$$\lambda = \frac{v}{f}$$

Where:

λ = wavelength
v = velocity of propagation
f = frequency of vibration

1-29. When you use the above equation, be careful to express velocity and wavelength in the proper units of length. For example, in the English system, if the velocity (expressed in feet per second) is divided by the frequency (expressed in cycles per second, or Hz), the wavelength is given in feet per cycle. If the metric system is used and the velocity (expressed in meters per second) is divided by the frequency (expressed in cycles per second), the wavelength is given in meters per cycle. Be sure to express both the wavelength and the frequency in the same units. (Feet per cycle and meters per cycle are normally abbreviated as feet or meters because one wavelength indicates one cycle.) Because this equation holds true for both transverse and

longitudinal waves, it is used in the study of both electromagnetic waves and sound waves.

1-30. Consider the following example:

Two cycles of a wave pass a fixed point every second, and the velocity of the wave train is 4 feet per second. What is the wavelength? The formula for determining wavelength is as follows:

$$\lambda = \frac{v}{f}$$

Where:

λ = wavelength in feet
v = velocity in feet per second
f = frequency in Hz

Given:

v = 4 feet per second
f = 2 Hz

Solution:

$$\lambda = \frac{v}{f}$$

$$\lambda = \frac{4 \text{ feet per second}}{2 \text{ Hz}}$$

$$\lambda = 2 \text{ feet}$$

1-31. In problems of this kind, be sure not to confuse wave velocity with frequency. Frequency is the number of cycles per unit of time (Hz). Wave velocity is the speed with which a wave train passes a fixed point.

1-32. Here is another problem:

If a wave has a velocity of 1,100 feet per second and a wavelength of 30 feet, what is the frequency of the wave?

By transposing the general equation:

$$f = \frac{v}{\lambda}$$

We have the equation:

$$\lambda = \frac{v}{f}$$

Given:

v = 1,100 feet per second
λ = 30 feet

Solution:

$$f = \frac{1{,}100 \text{ feet per second}}{30 \text{ feet}}$$

$$f = 36.67 \text{ Hz}$$

To find the velocity, rewrite the equation as follows:

$$v = \lambda f$$

1-33. Let us work one more problem, this time using the metric system.

Suppose the wavelength is 0.4 meters and the frequency is 12 kHz. What is the velocity? Use the following formula:

velocity = wavelength x frequency ($v = \lambda f$)

Given:

$\lambda =$ 0.4 meters

$f =$ 12 kHz

Solution:

$v = \lambda \times f$

$v =$ 0.4 meters x 12,000 Hz

$v =$ 4,800 meters per second

1-34. Other important characteristics of wave motion are reflection, refraction, diffraction, and the Doppler effect. Big words, but the concept of each is easy to see. For ease of understanding, we explain the first two characteristics using light waves, and the last two characteristics using sound waves. You should keep in mind that all waves react in a similar manner.

1-35. Within mediums, such as air, solids, or gases, a wave travels in a straight line. When the wave leaves the boundary of one medium and enters the boundary of a different medium, the wave changes direction. For our purposes, a boundary is an imaginary line that separates one medium from another.

1-36. When a wave passes through one medium and encounters a medium having different characteristics, three things can occur—

- Some of the energy can be reflected back into the initial medium.
- Some of the energy can be transmitted into the second medium where it may continue at a different velocity.
- Some of the energy can be absorbed by the medium. In some cases, all three processes (reflection, transmission, and absorption) may occur to some degree.

Reflection

1-37. Reflection waves are simply waves that are neither transmitted nor absorbed, but are reflected from the surface of the medium they encounter. If a wave is directed against a reflecting surface, such as a mirror, it will reflect or "bounce" from the mirror. Refer to figure 1-9. A wave directed toward the surface of the mirror is called the incident wave. When the wave bounces off of the mirror, it becomes known as the reflected wave. An imaginary line perpendicular to the mirror at the point at which the incident wave strikes the mirror's surface is called the normal, or perpendicular. The angle between the incident wave and the normal is called the angle of incidence. The angle between the reflected wave and the normal is called the angle of reflection. If the reflecting surface is smooth and polished, the angle between the incident ray and the normal will be the same as the angle between the reflected ray and the normal. This conforms to the law of reflection, which states: *The angle of incidence is equal to the angle of reflection*.

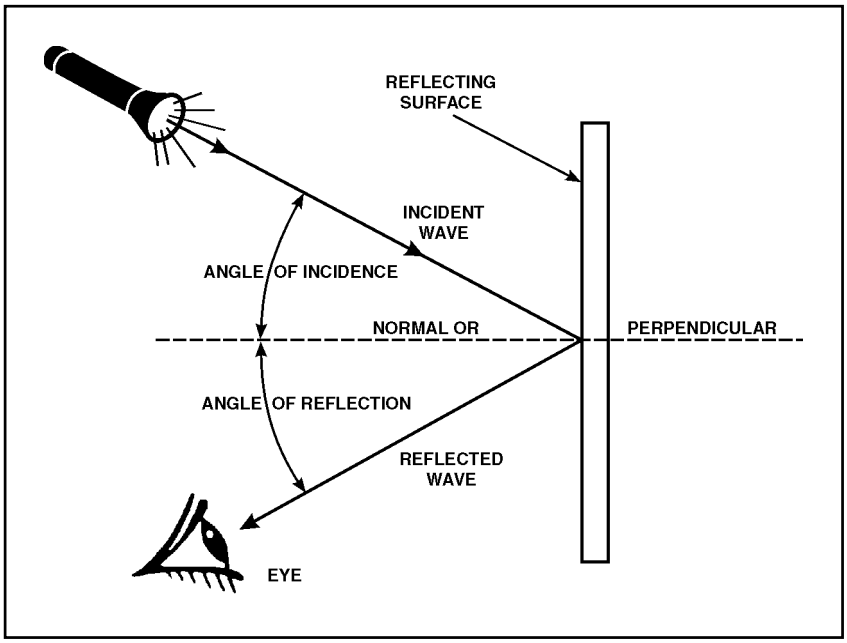


Figure 1-9. Reflection of a Wave

1-38. The amount of incident wave energy reflected from a given surface depends on the nature of the surface and the angle at which the wave strikes the surface. As the angle of incidence increases, the amount of wave energy reflected increases. The reflected energy is the greatest when the wave is nearly parallel to the reflecting surface. When the incident wave is perpendicular to the surface, more of the energy is transmitted into the substance and less is reflected. At any incident angle, a mirror reflects almost all of the wave energy, while a dull, black surface reflects very little.

Refraction

1-39. When a wave passes from one medium into another medium that has a different velocity of propagation, a change in the direction of the wave will occur. This changing of direction as the wave enters the second medium is called refraction. As in the discussion of reflection, the wave striking the boundary (surface) is called the incident wave, and the imaginary line perpendicular to the boundary is called the normal. The angle between the incident wave and the normal is called the angle of incidence. As the wave passes through the boundary, it is bent either toward or away from the normal. The angle between the normal and the path of the wave through the second medium is the angle of refraction.

1-40. A light wave passing through a block of glass is shown in figure 1-10. The wave moves from point A to B at a constant speed. This is the incident wave. As the wave penetrates the glass boundary at point B, the velocity of the wave is slowed down. This causes the wave to bend toward the normal. The wave then takes the path from point B to C through the glass and becomes both the refracted wave from the top surface and the incident wave to the lower surface. As the wave passes from the glass to the air (the second boundary), it is again refracted—this time away from the normal—and takes

the path from point C to D. As the wave passes through the last boundary, its velocity increases to the original velocity. As figure 1-10 shows, refracted waves can bend toward or away from the normal. This bending depends on the velocity of the wave through each medium. The broken line between points B and E is the path that the wave would travel if the two mediums (air and glass) had the same density.

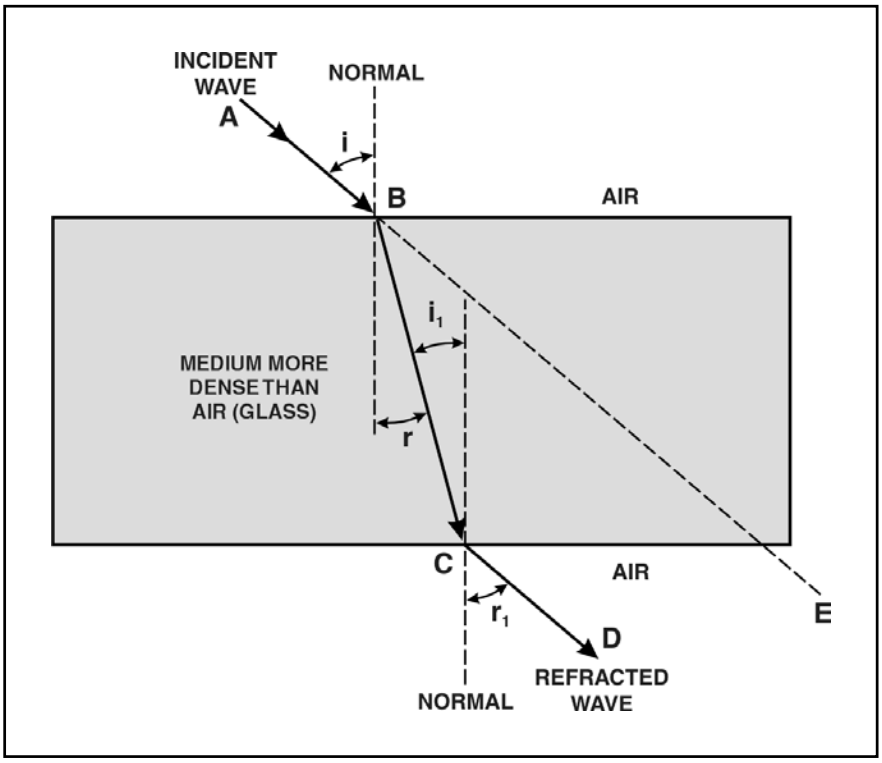


Figure 1-10. Refraction of a Wave

1-41. To summarize what figure 1-10 shows—

- If the wave passes from a less dense medium to a denser medium, it is bent toward the normal, and the angle of refraction (r) is less than the angle of incidence (i).
- If the wave passes from a denser to a less dense medium, it is bent away from the normal, and the angle of refraction (r_1) is greater than the angle of incidence (i_1).

1-42. You can more easily understand refraction by looking at figure 1-11. There is a plowed field in the middle of a parade ground. Think of the incident wave as a company of recruits marching four abreast at an angle across the parade ground to the plowed field, then crossing the plowed field and coming out on the other side onto the parade ground again. As the recruits march diagonally across the parade ground and begin to cross the boundary onto the plowed field, the front line is slowed down. Because the recruits arrive at the boundary at different times, they will begin to slow down at different times (number 1 slows down first and number 4 slows down last in each line). The net effect is a bending action. When the recruits leave the plowed field and reenter the parade ground, the reverse action takes place.

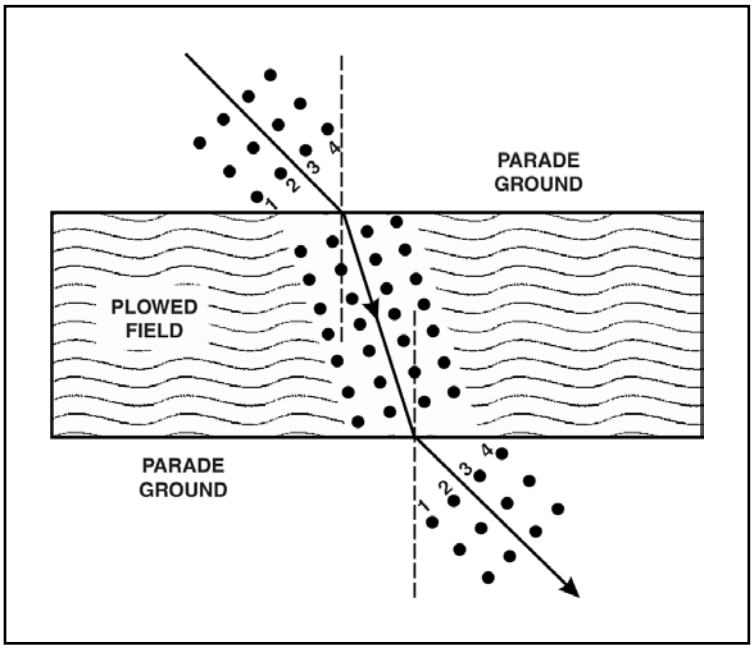


Figure 1-11. Analogy of Reflection

Diffraction

1-43. Diffraction is the bending of the wave path when the waves meet an obstruction. The amount of diffraction depends on the wavelength of the wave. Higher frequency waves are rarely diffracted in the normal world that surrounds us. Because light waves are high frequency waves, you will rarely see light diffracted. You can, however, observe diffraction in sound waves by listening to music. Suppose you are outdoors listening to a band. If you step behind a solid obstruction, such as a brick wall, you will hear mostly low notes. This is because the higher notes, having short wave lengths, undergo little or no diffraction and pass by or over the wall without wrapping around the wall and reaching your ears. The low notes, having longer wavelengths, wrap around the wall and reach your ears. This leads to the general statement that lower frequency waves tend to diffract more than higher frequency waves. Broadcast band (AM band) radio waves (lower frequency waves) often travel over a mountain to the opposite side from their source because of diffraction, while higher frequency TV and FM signals from the same source tend to be stopped by the mountain.

Doppler Effect

1-44. The last, but equally important, characteristic of a wave that we discuss is the Doppler effect. The Doppler effect is the apparent change in frequency or pitch when a sound source moves either toward or away from the listener, or when the listener moves either toward or away from the sound source. This principle, discovered by the Austrian physicist Christian Doppler, applies to all wave motion.

1-45. The apparent change in frequency between the source of a wave and the receiver of the wave is because of relative motion between the source and the receiver. To understand the Doppler effect, first assume that the

frequency of a sound from a source is held constant. The wavelength of the sound will also remain constant. If both the source and the receiver of the sound remain stationary, the receiver will hear the same frequency sound produced by the source. This is because the receiver is receiving the same number of waves per second that the source is producing. Now, if either the source or the receiver or both move toward the other, the receiver will perceive a higher frequency sound. This is because the receiver will receive a greater number of sound waves per second and interpret the greater number of waves as a higher frequency sound. Conversely, if the source and the receiver are moving apart, the receiver will receive a smaller number of sound waves per second and will perceive a lower frequency sound. In both cases, the frequency of the sound produced by the source will have remained constant.

1-46. For example, the frequency of the whistle on a fast-moving train sounds increasingly higher in pitch as the train is approaching than when the train is departing. Although the whistle is generating sound waves of a constant frequency, and though they travel through the air at the same velocity in all directions, the distance between the approaching train and the listener is decreasing. As a result, each wave has less distance to travel to reach the observer than the wave preceding it. Thus, the waves arrive with decreasing intervals of time between them.

1-47. These apparent changes in frequency, called the Doppler effect, affect the operation of equipment used to detect and measure wave energy. In dealing with electromagnetic wave propagation, the Doppler principle is used in equipment such as radar, target detection, weapons control, navigation, and sonar.

SOUND WAVES

1-48. As you know, sound travels through a medium by wave motion. Although sound waves and the electromagnetic waves used in the propagation of radio and radar differ, both types of waves have many of the same characteristics. Studying the principles of sound-wave motion will help you understand the actions of both sound waves and the more complex radio and radar electromagnetic waves. The major differences among sound waves, heat waves, and light waves are as follows:

- Their frequencies.
- Their types.
- The mediums through which they travel.
- The velocities at which they travel.

SOUND—WHAT IS IT?

1-49. The word sound is used in everyday speech to signify a variety of things. One definition of sound is the sensation of hearing. Another definition refers to a stimulus that is capable of producing the sensation of hearing. A third definition limits sound to what is actually heard by the human ear.

1-50. In the study of physics, sound is defined as a range of compression-wave frequencies to which the human ear is sensitive. For the purpose of this chapter, however, we need to broaden the definition of sound to include compression waves that are not always audible to the human ear. To distinguish frequencies in the audible range from those outside that range,

the words sonic, ultrasonic, and infrasonic are used. Sounds capable of being heard by the human ear are called sonics. The normal hearing range extends from about 20 to 20,000 hertz. In the Army to eliminate confusion when referring to different ranges of frequencies, an arbitrary dividing line has been established at 10,000 Hz. Even though the average person can hear sounds above 10,000 hertz, it is standard practice to refer to sounds above that frequency as ultrasonic. Sounds between 15 hertz and 10,000 hertz are called sonic. Sounds below 15 hertz are known as infrasonic (formerly referred to as subsonic) sounds.

REQUIREMENTS FOR SOUND

1-51. Recall that sound waves are compression waves. The existence of compression waves depends on the transfer of energy. To produce vibrations that become sounds, a mechanical device (the source) must first receive an input of energy. Next, the device must be in contact with a medium that will receive the sound energy and carry it to a receiver. If the device is not in contact with a medium, the energy will not be transferred to a receiver, and there will be no sound. Thus, three basic elements for transmission and reception of sound must be present before a sound can be produced. They are as follows:

- The source (or transmitter).
- A medium for carrying the sound (e.g., air, water, metal).
- The detector (or receiver).

1-52. A simple experiment provides convincing evidence that a medium must be present if sound is to be transferred. In figure 1-12, an electric bell is suspended by rubber bands in a bell jar from which the air can be removed. An external switch is connected from a battery to the bell so the bell may be rung intermittently. As the air is pumped out, the sound from the bell becomes weaker and weaker. If a perfect vacuum could be obtained, and if no sound were conducted out of the jar by the rubber bands, the sound from the bell would be completely inaudible. In other words, sound cannot be transmitted through a vacuum. When the air is admitted again, the sound is as loud as it was at the beginning. This experiment shows that when air is in contact with the vibrating bell, it carries energy to the walls of the jar, which in turn are set in vibration. Thus, the energy passes into the air outside of the jar and then on to the ear of the observer. This experiment illustrates that sound cannot exist in empty space (or a vacuum).

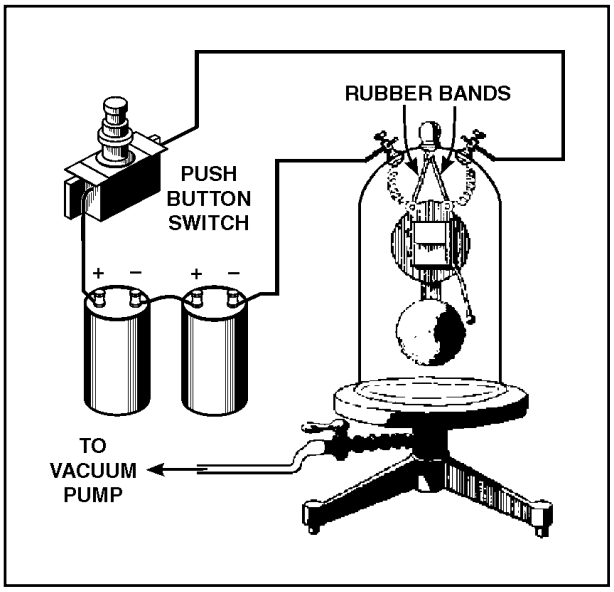


Figure 1-12. No Air, No Sound

1-53. Any object that moves rapidly back and forth, or vibrates, and thus disturbs the medium around it may be considered a source for sound. Bells, speakers, and stringed instruments are familiar sound sources.

1-54. The material through which sound waves travel is called the medium. The density of the medium determines the ease, distance, and speed of sound transmission. The higher the density of the medium, the slower sound travels through it.

1-55. The detector acts as the receiver of the sound wave. Because it does not surround the source of the sound wave, the detector absorbs only part of the energy from the wave and sometimes requires an amplifier to boost the weak signal.

1-56. As an illustration of what happens if one of these three elements is not present, let us refer to our experiment in which a bell was placed in a jar containing a vacuum. You could see the bell being struck, but you could hear no sound because there was no medium to transmit sound from the bell to you. Now let us look at another example in which the third element, the detector, is missing. You see a source (such as an explosion) apparently producing a sound, and you know the medium (air) is present, but you are too far away to hear the noise. Thus, as far as you are concerned, there is no detector and, therefore, no sound. We must assume, then, that sound can exist only when a source transmits sound through a medium, which passes it to a detector. Therefore, in the absence of any one of the basic elements (source, medium, and detector) there can be no sound.

TERMS USED IN SOUND WAVES

1-57. Sound waves vary in length according to their frequency. A sound having a long wavelength is heard at a low pitch (low frequency); one with a short wavelength is heard at a high pitch (high frequency). A complete wavelength is called a cycle. The distance from one point on a wave to the

corresponding point on the next wave is a wavelength. The number of cycles per second (hertz) is the frequency of the sound. The frequency of a sound wave is also the number of vibrations per second produced by the sound source.

CHARACTERISTICS OF SOUND

1-58. Sound waves travel at great distances in a very short time, but as the distance increases the waves tend to spread out. As the sound waves spread out, their energy simultaneously spreads through an increasingly larger area. Thus, the wave energy becomes weaker as the distance from the source is increased.

1-59. Sounds may be broadly classified into two general groups. One group is noise, which includes sounds such as the pounding of a hammer or the slamming of a door. The other group is musical sounds, or tones. The distinction between noise and tone is based on the regularity of the vibrations, the degree of damping, and the ability of the ear to recognize components having a musical sequence. You can best understand the physical difference between these kinds of sound by comparing the waveshape of a musical note, depicted in view A of figure 1-13, and the waveshape of noise, shown in view B. You can see by the comparison of the two waveshapes that noise makes a very irregular and haphazard curve and a musical note makes a uniform and regular curve.

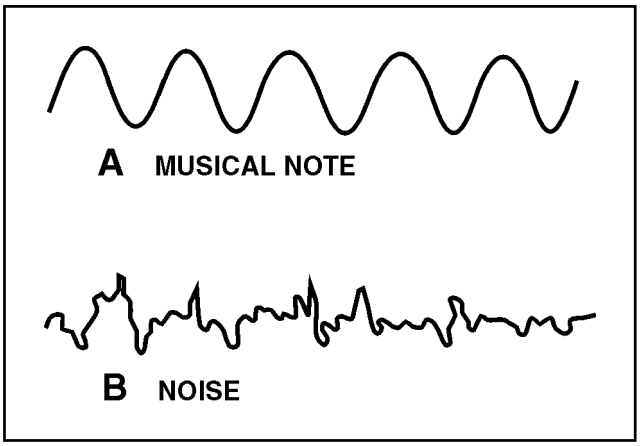


Figure 1-13. Musical Sound Versus Noise

1-60. Sound has three basic characteristics: pitch, intensity, and quality. Each of these three characteristics is associated with one of the properties of the source or the type of waves that it produces. The pitch depends upon the frequency of the waves, the intensity depends upon the amplitude of the waves, and the quality depends upon the form of the waves. With the proper combination of these characteristics, the tone is pleasant to the ear. With the wrong combination, the sound quality turns into noise.

Sound Pitch

1-61. The term pitch is used to describe the frequency of a sound. An object that vibrates many times per second produces a sound with a high pitch, as with a police whistle. The slow vibrations of the heavier strings of a violin

cause a low-pitched sound. Thus, the frequency of the wave determines pitch. When the frequency is low, sound waves are long; when it is high, the waves are short. A sound can be so high in frequency that the waves reaching the ear cannot be heard. Likewise, some frequencies are so low that the eardrums do not convert them into sound. The range of sound that the human ear can detect varies with each individual.

Sound Intensity

1-62. The intensity of sound, at a given distance, depends upon the amplitude of the waves. Thus, a tuning fork gives out more energy in the form of sound when struck hard than when struck gently. You should remember that when a tuning fork is struck, the sound is omnidirectional (heard in all directions), because the sound waves spread out in all directions, as shown in figure 1-14. You can see from the figure that as the distance between the waves and the sound source increases, the energy in each wave spreads over a greater area; hence, the intensity of the sound decreases. The speaking tubes sometimes used aboard a ship prevent the sound waves from spreading in all directions by concentrating them in one desired direction (unidirectional), producing greater intensity. Therefore, the sound is heard almost at its original intensity at the opposite end of the speaking tube. The unidirectional megaphone and the directional loudspeaker also prevent sound waves from spreading in all directions.

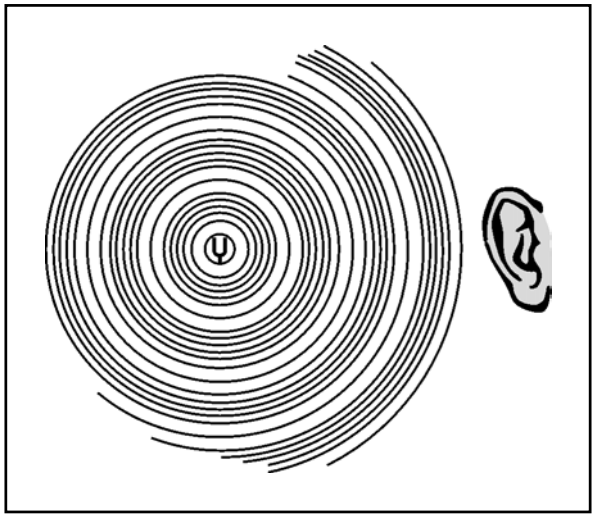


Figure 1-14. Sound Waves Spread in All Directions

1-63. Sound intensity and loudness are often mistakenly interpreted as having the same meaning. Although they are related, they are not the same. Sound intensity is a measure of the sound energy of a wave. Loudness, on the other hand, is the sensation the intensity (and sometimes frequency) the sound wave produces on the ear. Increasing the intensity causes an increase in loudness but not in a direct proportion. For instance, doubling the loudness of a sound requires about a tenfold increase in the intensity of the sound.

Sound Quality

1-64. Most sounds, including musical notes, are not pure tones. They are a mixture of different frequencies (tones). A tuning fork, when struck, produces a pure tone of a specific frequency. This pure tone is produced by regular vibrations of the source (tines of the tuning fork). On the other hand, scraping your fingernails across a blackboard creates only noise, because the vibrations are irregular. Each individual pipe of a pipe organ is similar to a tuning fork, and each pipe produces a tone of a specific frequency. But sounding two or more pipes at the same time produces a complex waveform. A tone that closely imitates any of the vowel sounds can be produced by selecting the proper pipes and sounding them at the same time. Figure 1-15 illustrates the combining of two pure tones to make a complex wave.

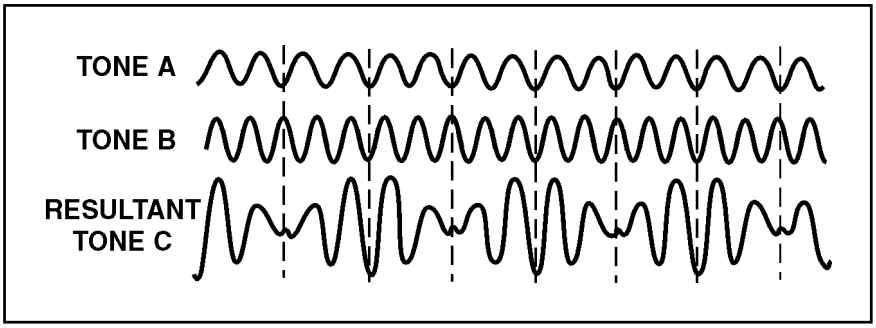


Figure 1-15. Combination of Tones

1-65. The quality of a sound depends on the complexity of its sound waves, such as the waves shown in tone C of figure 1-15. Almost all sounds (musical and vocal included) have complicated (complex) waveforms. Tone A is a simple wave of a specific frequency that can be produced by a tuning fork, piano, organ, or other musical instrument. Tone B is also a simple wave but at a different frequency. When the two tones are sounded together, the complex waveform in tone C is produced. Note that tone C has the same frequency as tone A with an increase in amplitude. The human ear could easily distinguish between tones A and tone C because of the quality. Therefore, we can say that quality distinguishes tones of like pitch and loudness when sounded on different types of musical instruments. It also distinguishes the voices of different persons.

VELOCITY OF TRANSMISSION

1-66. Sound waves travel through any medium to a velocity that is controlled by the medium. Varying the frequency and intensity of the sound waves will not affect the speed of propagation. The elasticity and density of a medium are the two basic physical properties that govern the velocity of sound through the medium.

1-67. Elasticity is the ability of a strained body to recover its shape after deformation, as from a vibration or compression. The measure of elasticity of a body is the force it exerts to return to its original shape.

1-68. The density of a medium or substance is the mass per unit volume of the medium or substance. Raising the temperature of the medium (which

decreases its density) has the effect of increasing the velocity of sound through the medium.

1-69. The velocity of sound in an elastic medium is expressed by the formula:

$$V = \sqrt{\frac{E}{d}}$$

1-70. Even though solids such as steel and glass are far denser than air, their elasticities are so much greater that the velocities of sound in them are 15 times greater than the velocity of sound in air. Using elasticity as a rough indication of the speed of sound in a given medium, we can state as a general rule that sound travels faster in harder materials (such as steel), slower in liquids, and slowest in gases. Density has the opposite effect on the velocity of sound, that is, with other factors constant, a denser material (such as lead) passes sound more slowly.

1-71. At a given temperature and atmospheric pressure, all sound waves travel in air at the same speed. Thus the velocity that sound will travel through air at 32°F (0°C) is 1,087 feet per second. But for practical purposes, the speed of sound in air may be considered as 1,100 feet per second. Table 1-1 gives a comparison of the velocity of sound in various mediums.

Table 1-1. Comparison of Velocity of Sound in Various Mediums

MEDIUM	*TEMPERATURE*		*VELOCITY (Ft/Sec)*
	ºF	*ºC*	
Air	32	0	1,087
Air	68	20	1,127
Aluminum	68	20	16,700
Carbon Dioxide	32	0	856
Fresh Water	32	0	4,629
Fresh Water	68	20	4,805
Hydrogen	32	0	4,219
Lead	32	20	4,030
Salt Water	32	0	4,800
Salt Water	68	20	4,953
Steel	32	0	16,410
Steel	68	20	16,850

ACOUSTICS

1-72. The science of sound is called acoustics. This subject could fill volumes of technical books, but we scratch only the surface in this chapter. We present the important points that you need for a better understanding of sound waves. Acoustics, like sound, relates to the sense of hearing. It also deals with the production, control, transmission, reception, and effects of sound. For the present, we are concerned only with the last relationship—the effects of sound. These same effects will be used throughout your study of wave propagation.

Echo

1-73. An echo is the reflection of the original sound wave as it bounces off a distant surface. Just as a rubber ball bounces back when it is thrown against a hard surface, sound waves also bounce off most surfaces. As you have learned from the study of the law of conservation of energy, a rubber ball never bounces back with as much energy as the initial bounce. Similarly, a reflected sound wave is not as loud as the original sound wave. In both cases, some of the energy is absorbed by the reflecting surface. Only a portion of the original sound is reflected, and only a portion of the reflected sound returns to the listener. For this reason, an echo is never as loud as the original sound. Sound reflections (echoes) have many applications. The most important of these applications can be found in the use of depth-finding equipment (the fathometer) and sonar. The fathometer sends sound-wave pulses from the bottom of a ship and receives echoes from the ocean floor to indicate the depth of the ocean beneath the ship. The sonar transmits a pulse of sound energy and receives the echo to indicate range and bearing of objects or targets in the ocean depths.

Refraction

1-74. When sound waves traveling at different velocities pass obliquely (at an angle) from one medium into another, the waves are refracted; that is, their line of travel is bent. Refraction occurs gradually when one part of a sound wave is traveling faster than the other parts. For example, the wind a few feet above the surface of the earth has a greater velocity than that near the surface because friction retards the lower layers (see figure 1-16). The velocity of the wind is added to the velocity of the sound through the air. The result is that the upper portion of the sound wave moves faster than the lower portion and causes a gradual change in the direction of travel of the wave. Refraction causes sound to travel farther with the wind than against it.

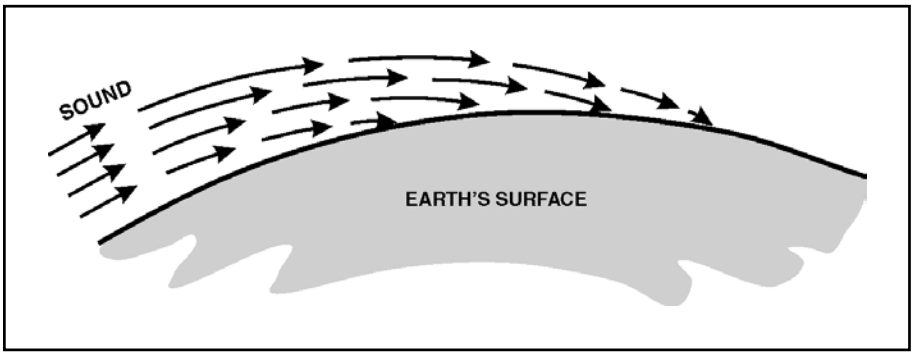


Figure 1-16. Refraction of Sound

Reverberation

1-75. In empty rooms or other confined spaces, sound may be reflected several times to cause what is known as reverberation. Reverberation is the multiple reflections of sound waves. Reverberations seem to prolong the time during which a sound is heard. Examples of this effect often occur in nature. For instance, the discharge of lightning causes a sharp, quick sound. By the time this sound has reached the ears of a distant observer, it is usually drawn out into a prolonged roar by reverberations that we call thunder. A similar case often arises with underwater sound equipment. Reverberations

from nearby points may continue for such a long time that they interfere with the returning echoes from targets.

Interference

1-76. Any disturbance, man-made or natural, that causes an undesirable response or the degradation of a wave is referred to as interference. Two sound waves moving simultaneously through the same medium will advance independently, each producing a disturbance as if the other were not present. If the two waves have the same frequency—are in phase with each other and are moving in the same direction—they are additive and are said to interfere constructively. If the two waves have the same frequency and are moving in the same direction, but out of phase with each other, they are subtractive and are said to interfere destructively. If these two subtractive waves have equal amplitudes, the waves cancel each other. This addition or subtraction of waves is often called interference.

Resonance

1-77. At some time during your life you probably observed someone putting his or her head into an empty barrel or other cavity and making noises varying in pitch. When that person's voice reached a certain pitch, the tone produced seemed much louder than the others. The reason for this phenomenon is that at that a certain pitch the frequency of vibrations of the voice matched the resonant (or natural) frequency of the cavity. The resonant frequency of a cavity is the frequency at which the cavity body will begin to vibrate and create sound waves. When the resonant frequency of the cavity was reached, the sound of the voice was reinforced by the sound waves created by the cavity, resulting in a louder tone. This phenomenon occurs whenever the frequency of vibrations is the same as the natural frequency of a cavity, and is called resonance.

Noise

1-78. The most complex sound wave that can be produced is noise. Noise has no tonal quality. It distracts and distorts the sound quality that was intended to be heard. Noise is generally an unwanted disturbance caused by spurious waves originating from man-made or natural sources, such as a jet breaking the sound barrier, or thunder.

LIGHT WAVES

1-79. The concepts used to describe the behavior of waves—including reflection, refraction, and diffraction—can help you understand the behavior of light and light waves described below. The relationship between light and light waves (rays) is the same as for sound and sound waves.

1-80. Light is a form of electromagnetic energy. It can be produced by various means (e.g., mechanical, electrical, and chemical). We can see objects because the light waves (rays) they give off or reflect reach our eyes.

PROPAGATION OF LIGHT

1-81. The exact nature of light is not fully understood, although scientists have been studying the subject for many centuries. Some experiments seem to show that light is composed of tiny particles, and some suggest that it is made up of waves.

1-82. One theory after another attracted the approval and acceptance of physicists. Today, some scientific phenomena can be explained only by the wave theory and others only by the particle theory. Physicists, constantly searching for some new discovery that would bring these two theories into agreement, gradually have come to accept a theory that combines the principles of the two theories.

1-83. According to the view now generally accepted, light is a form of electromagnetic radiation; that is, light and similar forms of radiation are made up of moving electric and magnetic fields. These two fields are explained thoroughly later in this chapter.

ELECTROMAGNETIC THEORY OF LIGHT

1-84. James Clark Maxwell, a brilliant Scottish scientist of the mid-nineteenth century, constructed an oscillating electrical circuit, which he used to show that electromagnetic waves could move through empty space. Light eventually was proved to be electromagnetic.

1-85. Current light theory says that light is made up of very small packets of electromagnetic energy called photons (the smallest unit of radiant energy). These photons move at a constant speed in the medium through which they travel. Photons move at a faster speed through a vacuum than they do in the atmosphere, and at a slower speed through water than air.

1-86. The electromagnetic energy of light is a form of electromagnetic radiation. Light and similar forms of radiation are made up of moving electric and magnetic forces and move as waves. Electromagnetic waves move in a manner similar to the waves produced by the pebble dropped in the pool of water discussed earlier in this chapter. The transverse waves of light from a light source spread out in expanding circles much like the waves in the pool. However, the waves in the pool are very slow and clumsy in comparison with light, which travels approximately 186,000 miles per second.

1-87. Light radiates from its source in all directions until absorbed or diverted by some substance (figure 1-17). The lines drawn from the light source (a light bulb in the example in figure 1-17) to any point on one of these waves indicate the direction in which the waves are moving. These lines, called radii of the spheres, are formed by the waves and are called light rays. Although single rays of light do not exist, light “rays” are used in illustrations as a convenient method to show the direction in which light is traveling at any point.

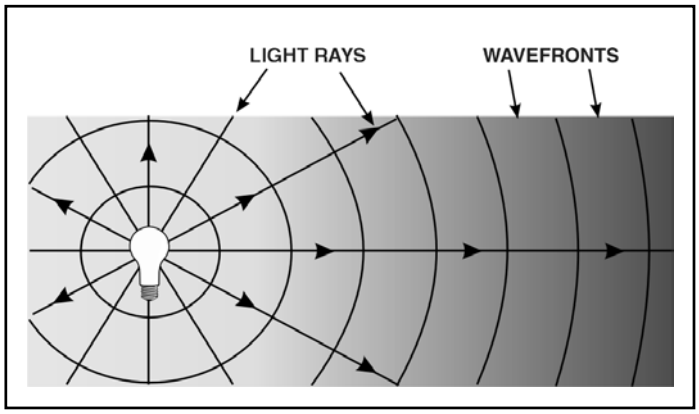


Figure 1-17. Waves and Radii from a Nearby Light Source

1-88. A large volume of light is called a beam; a narrow beam is called a pencil; and the smallest portion of a pencil is called a light ray. A ray of light can be illustrated as a straight line. This straight line drawn from a light source represents an infinite number of rays radiating in all directions from the source.

FREQUENCIES AND WAVELENGTHS

1-89. Compared to sound waves, the frequency of light waves is very high and the wavelength is very short. To measure these wavelengths conveniently, a special unit of measure called an angstrom unit, or more usually, an angstrom (Å), was devised. Another common unit used to measure these waves is the millimicron (mm), which is one millionth of a millimeter. One mF equals ten angstroms. One angstrom equals 10^{-10} meters.

FREQUENCIES AND COLOR

1-90. For our discussion of light wave waves, we use the millimicron measurement. The wavelength of a light determines the color of the light. Figure 1-18 indicates that light with a wavelength of 700 millimicrons is red, and that light with a wavelength of 500 millimicrons is blue-green. This illustration shows approximate wavelengths of the different colors in the visible spectrum. In fact, the color of light depends on its frequency, not its wavelength. However, light is measured in wavelengths. When the wavelength of 700 millimicrons is measured in a medium such as air, it produces the color red, but the same wave measured in a different medium will have a different wavelength. When red light that has been traveling in air enters glass, it loses speed. Its wavelength becomes shorter or compressed, but it continues to be red. This phenomenon indicates that the color of light depends on frequency and not on wavelength. The color scale in figure 1-18 is based on the wavelengths in air.

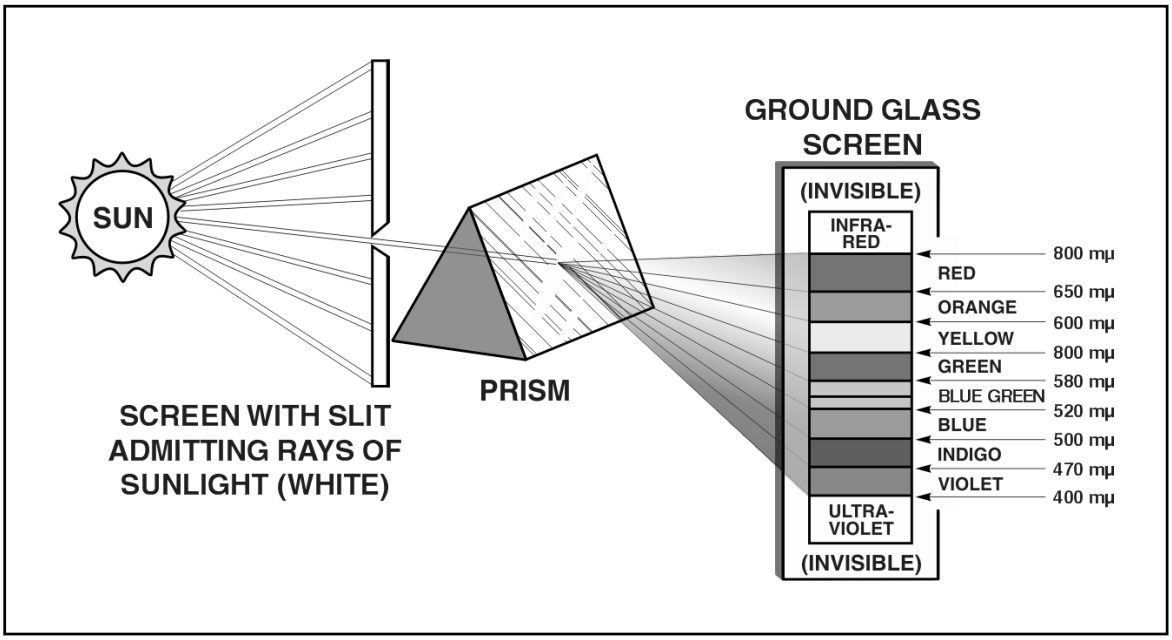


Figure 1-18. Use of a Prism to Split White Light into Different Colors

1-91. When a beam of white light (sunlight) is passed through a prism, as shown in figure 1-18, it is refracted and broken down into its component wavelengths. (This phenomenon of breaking light down into its component wavelengths is known as dispersion.) Each of these wavelengths causes a different reaction of the eye, which sees the various colors that compose the visible spectrum. The visible spectrum is recorded as a mixture of red, orange, yellow, green, blue, indigo, and violet. White light results when the primaries (red, green, and blue) are mixed together in overlapping beams of light. (These are not the primary colors used in mixing pigments, such as in paint.) Furthermore, the complementary or secondary colors (magenta, yellow, and cyan) may be shown with equal ease by mixing any two of the primary colors in overlapping beams of light. Thus, red and green light mixed in equal intensities make yellow light; green and blue produce cyan (blue-green light); and blue and red correctly mixed produce magenta (a purplish red light).

LIGHT AND COLOR

1-92. All objects absorb some of the light that falls on them. An object appears to be a certain color because it absorbs all of the light waves except those whose frequency corresponds to that particular color. Those waves are reflected from the surface, strike your eye, and cause you to see the particular color. The color of an object therefore depends on the frequency of the electromagnetic wave reflected.

LUMINOUS BODIES

1-93. If an object is the source of light energy, it is called luminous. If the object is not the source of light but reflects light, it is called an illuminated body.

1-94. Certain bodies, such as the sun, a gas flame, and an electric light filament are visible because they are light sources. They are called self-luminous bodies. Objects other than self-luminous bodies become visible only when they are in the presence of light from luminous bodies.

1-95. Most nonluminous bodies are visible because they diffuse or reflect the light that falls on them. A good example of a nonluminous diffusing body is the moon, which shines only because the sunlight falling onto its surface is diffused.

1-96. Black objects do not diffuse or reflect light. They are visible only when outlined against a background of light from a luminous or diffusing body.

PROPERTIES OF LIGHT

1-97. When light waves, which travel in straight lines, encounter any substance, they are transmitted, reflected, or absorbed. These effects are illustrated in figure 1-19. When light strikes a substance, some absorption and some reflection always take place. No substance completely transmits, reflects, or absorbs all of the light rays that reach its surface. Substances that transmit almost all the light waves that fall upon them are said to be transparent. A transparent substance is one through which you can see clearly. Clear glass is transparent because it transmits light rays without diffusing them (figure 1-20, view A). There is no known perfectly transparent substance, but many substances are nearly so. Substances through which some light rays can pass but through which objects cannot be seen clearly because the rays are diffused are called translucent (figure 1-20, view B). The frosted glass of a light bulb and a piece of oiled paper are examples of translucent materials. Substances that do not transmit any light rays are called opaque (figure 1-20, view C). Opaque substances can either reflect or absorb virtually all of the light rays that fall upon them.

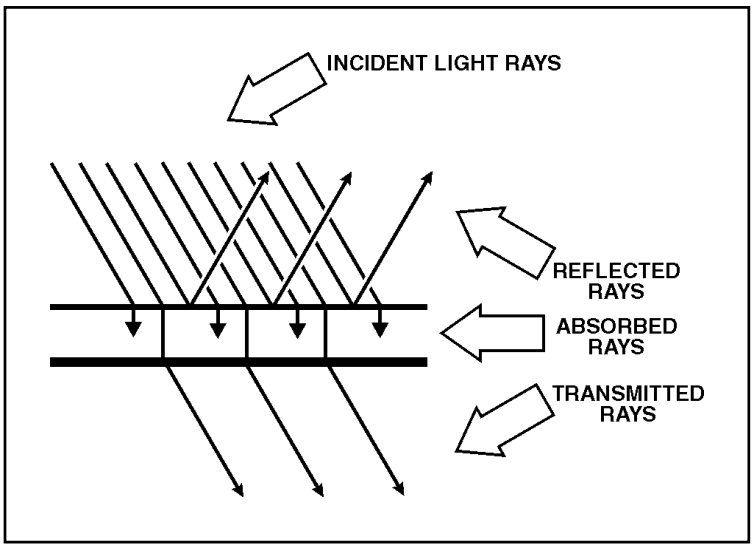


Figure 1-19. Light Waves Reflected, Absorbed, and Transmitted

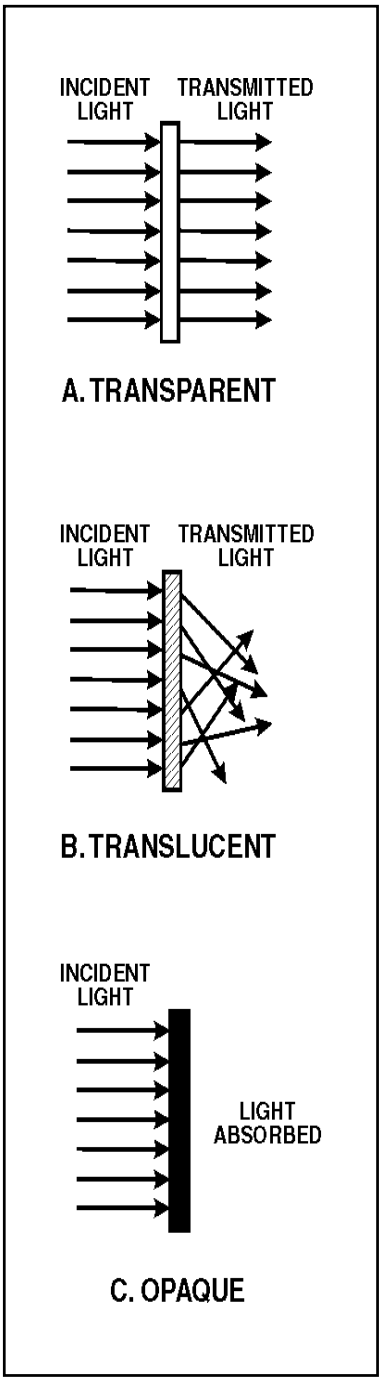


Figure 1-20. Transparent, Translucent, and Opaque Substances

Speed of Light

1-98. You probably have heard people say, "quick as lightning" or "fast as light" to describe rapid motion; nevertheless, it is difficult to realize how fast light actually travels. Not until recent years have scientists been able to measure accurately the speed of light.

1-99. Prior to the mid-seventeenth century, scientists thought that light required no time at all to pass from the source to the observer. Then, in 1675, Ole Roemer, a Danish astronomer, discovered that light travels approximately 186,000 miles per second in space. At this velocity, a light beam can circle the earth 7 1/2 times in one second.

1-100. The speed of light depends on the medium through which the light travels. In empty space, the speed is 186,000 (1.86×10^5) miles per second. It is almost the same in air. In water, it slows down to approximately 140,000 (1.4×10^5) miles per second. In glass, the speed of light is 124,000 (1.24×10^5) miles per second. In other words, the speed of light decreases as the density of the substance through which the light passes increases.

1-101. The velocity of light, which is the same as the velocity of other electromagnetic waves, is considered to be constant, at 186,000 miles per second. If expressed in meters, the velocity of light is 300,000,000 meters per second.

Reflection of Light

1-102. Light waves obey the law of reflection in the same manner as other types of waves. Consider the straight path of a light ray admitted through a narrow slit into a darkened room. The straight path of the beam is made visible by illuminated dust particles suspended in the air. If the light beam is made to fall onto the surface of a mirror or other reflecting surface, however, the direction of the beam changes sharply. The light can be reflected in almost any direction, depending on the angle at which the mirror is held.

1-103. As shown earlier in figure 1-9, if a light beam strikes a mirror, the angle at which the beam is reflected depends on the angle at which it strikes the mirror. The beam approaching the mirror is the incident or striking beam, and the beam leaving the mirror is the reflected beam.

1-104. The term "reflected light" simply refers to light waves that are neither transmitted nor absorbed, but are thrown back from the surface of the medium they encounter. This phenomenon is described more fully in the discussions of radio waves (chapter 2) and antennas (chapter 4).

Refraction of Light

1-105. The change of direction that occurs when a ray of light passes from one transparent substance into another of different density is called refraction. Refraction is due to the fact that light travels at various speeds in different transparent substances. For example, water never appears as deep as it really is, and objects under water appear to be closer to the surface than they really are. A bending of the light rays causes these impressions.

1-106. Another example of refraction is the apparent bending of a spoon when it is immersed in a cup of water. The bending seems to take place at the surface of the water, or exactly at the point where there is a change of density. Obviously, the spoon does not bend from the pressure of the water. The light forming the image of the spoon is bent as it passes from the water (a medium of high density) to the air (a medium of comparatively low density).

1-107. Without refraction, light waves would pass in straight lines through transparent substances without any change of direction. Refer back to figure 1-10, which shows refraction of a wave. As you can see, all rays striking the glass at any angle other than perpendicular are refracted. However, the perpendicular ray, which enters the glass normal to the surface, continues through the glass and into the air in a straight line—no refraction takes place.

Diffusion of Light

1-108. When light is reflected from a mirror, the angle of reflection of each ray equals the angle of incidence. When light is reflected from a piece of plain white paper, however, the reflected beam is scattered, or diffused, as shown in figure 1-21. Because the surface of the paper is not smooth, the reflected light is broken up into many light beams that are reflected in all directions.

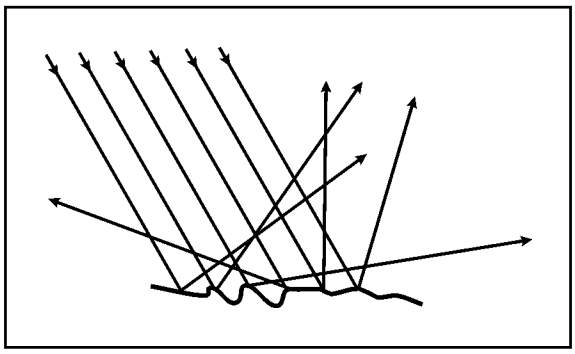


Figure 1-21. Diffusion of Light

Absorption of Light

1-109. As illustrated in figure 1-21, a light beam is reflected and diffused when it falls onto a piece of white paper. If a light beam falls onto a piece of black paper, the black paper absorbs most of the light rays and very little light is reflected from the paper. If the surface on which the light beam falls is perfectly black, there is no reflection; that is, the light is totally absorbed. No matter what kind of surface light falls on, however, some of the light is absorbed.

COMPARISON OF LIGHT WAVES WITH SOUND WAVES

1-110. There are two main differences between sound waves and light waves. The first difference is in velocity. Sound waves travel through air at the speed of approximately 1,100 feet per second; light waves travel through air and empty space at a speed of approximately 186,000 miles per second (300,000,000 meters per second). The second difference is that sound is composed of longitudinal waves (alternate compressions and expansions of matter) and light is composed of transverse waves in an electromagnetic field.

1-111. Although both are forms of wave motion, sound requires a solid, liquid, or gaseous medium, whereas light can travel through empty space. The denser the medium, the greater the speed of sound. The opposite is true of light. Light travels approximately one-third slower in water than in air. Sound travels through all substances, but light cannot pass through opaque materials.

1-112. Frequency affects both sound and light. A certain range of sound frequencies produces sensations that you can hear. A slow vibration (low frequency) in sound gives the sensation of a low note. A more rapid sound vibration (higher frequency) produces a higher note. Likewise, a certain range of light frequencies produces sensations that you can see. Violet light is produced at the high-frequency end of the light spectrum, while red light is produced at the low-frequency end of the light spectrum. A change in frequency of sound waves causes an audible sensation—a difference in pitch. A change in the frequency of a light wave causes a visual sensation—a difference in color. For a comparison of light waves with sound waves, see Table 1-2.

Table 1-2. Comparison of Light Waves and Sound Waves

	SOUND WAVES	***LIGHT WAVES***
Velocity in air	Approximately 1,100 feet per second.	Approximately 186,000 miles per second (300,000,000 meters per second).
Form	A form of wave motion.	A form of wave motion.
Wave composition	Longitudinal.	Transverse.
Transmitting medium	All substances.	Empty space and all substances except opaque materials.
Relation of transmitting medium velocity to velocity	The denser the medium, the greater the speed.	The denser the medium, the slower the speed.
Sensations produced	Hearing.	Seeing.
Variations in sensations produced	A low frequency causes a low note; a high frequency causes a high note.	A low frequency causes red light; a high frequency causes violet light.

ELECTROMAGNETIC SPECTRUM

1-113. Light is one kind of electromagnetic energy. There are many other types of electromagnetic energy, including heat energy and radio energy. The only difference between the various types of electromagnetic energy is the frequency of their waves (rate of vibration). The term spectrum is used to designate the entire range of electromagnetic waves arranged in order of their frequencies. The visible spectrum contains only those waves that stimulate the sense of sight. As a technician, you might be expected to maintain equipment that uses electromagnetic waves within, above, and below the visible spectrum.

1-114. There are neither sharp dividing lines nor gaps in the electromagnetic spectrum. Figure 1-22 illustrates how portions of the electromagnetic spectrum overlap. Notice that only a small portion of the electromagnetic spectrum contains visible waves, or light, that can be seen by the human eye.

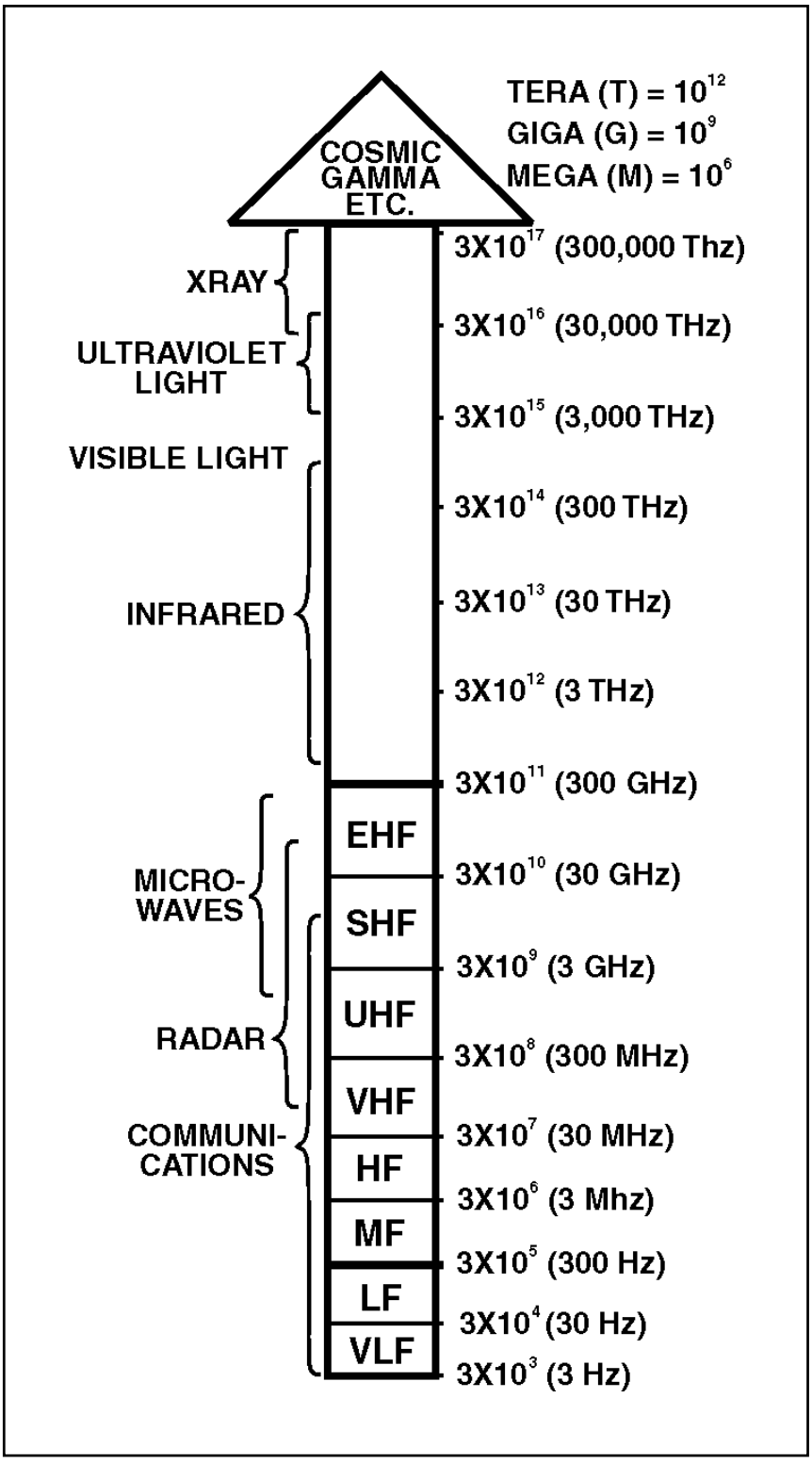


Figure 1-22. Electromagnetic Spectrum

ELECTROMAGNETIC WAVES

1-115. In general, the same principles and properties of light waves apply to the communications electromagnetic waves you are about to study. The electromagnetic field is used to transfer energy (as communications) from point to point. The basic antenna is a propagation source of these electromagnetic waves.

THE BASIC ANTENNA

1-116. The study of antennas and electromagnetic wave propagation is essential to a complete understanding of radio communication, radar, loran, and other electronic systems. Figure 1-23 shows a simple radio communication system. In the illustration, the transmitter is an electronic device that generates radio-frequency energy. The energy travels through a transmission line (discussed in chapter 3) to an antenna. The antenna converts the energy into radio waves that radiate into space from the antenna at the speed of light. The radio waves travel through the atmosphere or space until they are either reflected by an object or absorbed. If another antenna is placed in the path of the radio waves, it absorbs part of the waves and converts them to energy. This energy travels through another transmission line and is fed to a receiver. From this example, you can see that the requirements for a simple communications system are as follows:

- Transmitting equipment.
- Transmission line.
- Transmitting antenna.
- Medium.
- Receiving antenna.
- Receiving equipment.

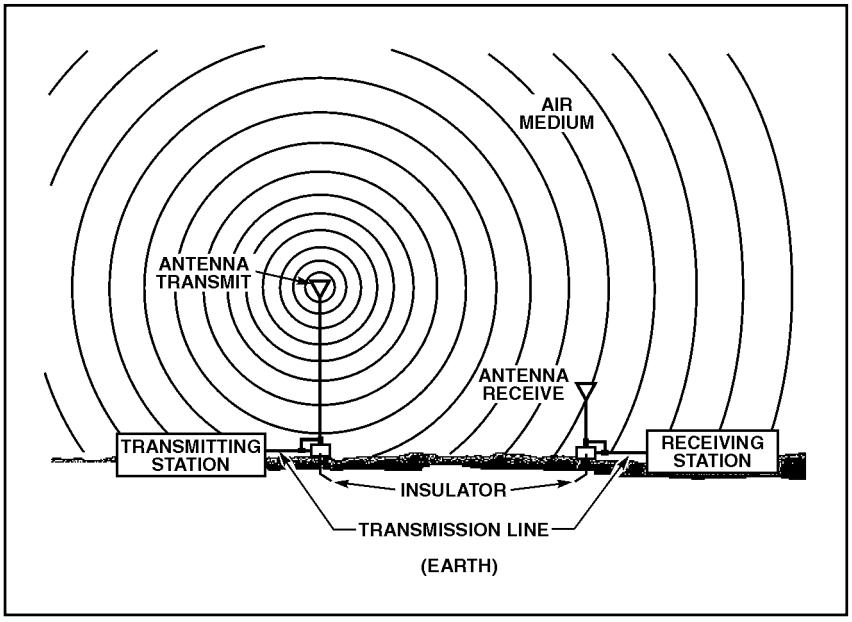


Figure 1-23. Simple Radio Communication System

1-117. An antenna is a conductor or a set of conductors used either to radiate electromagnetic energy into space or to collect this energy from space. Figure 1-24 shows an antenna. View A is a drawing of an actual antenna; view B is a cut-away view of the antenna; and view C is a simplified diagram of the antenna.

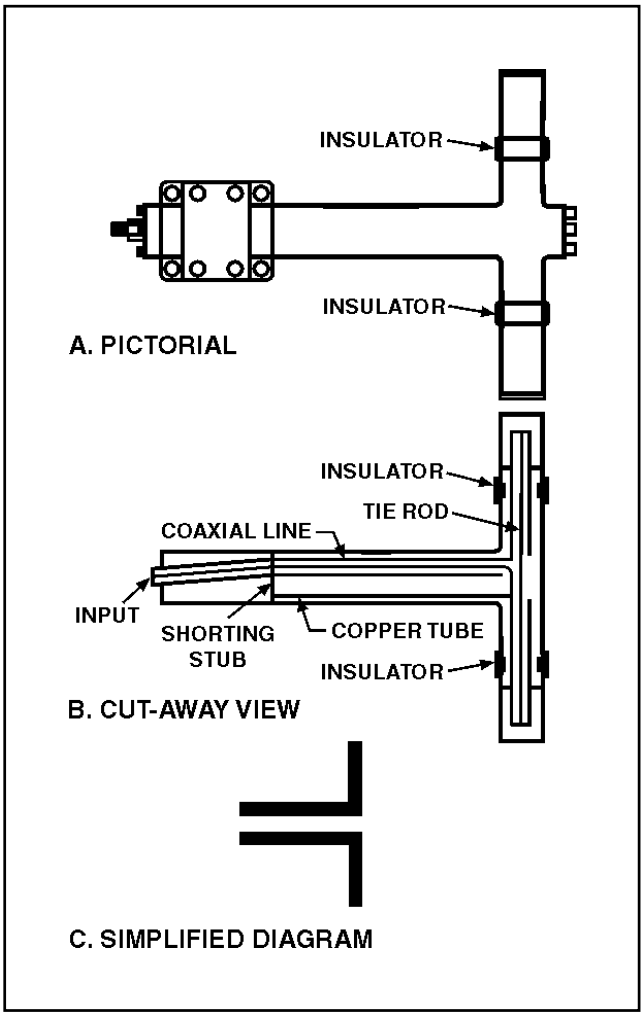


Figure 1-24. Antenna

COMPONENTS OF THE ELECTROMAGNETIC WAVE

1-118. An electromagnetic wave consists of two primary components—an electric field and a magnetic field. The electric field results from the force of voltage, and the magnetic field results from the flow of current.

1-119. Although electromagnetic fields that are radiated are commonly considered to be waves, under certain circumstances their behavior makes them appear to have some of the properties of particles. In general, however, it is easier to picture electromagnetic radiation in space as horizontal and vertical lines of force oriented at right angles to each other. These lines of force are made up of an electric field (E) and a magnetic field (H), which together make up the electromagnetic field in space.

1-120. The electric and magnetic fields radiated from an antenna form the electromagnetic field. This field is responsible for the transmission and reception of electromagnetic energy through free space. An antenna, however, is also part of the electrical circuit of a transmitter or a receiver and is equivalent to a circuit containing inductance, capacitance, and resistance. Therefore, the antenna can be expected to display definite voltage and current relationships with respect to a given input. A current through the antenna produces a magnetic field, and a charge on the antenna produces an electric field. These two fields combine to form the induction field. To help you gain a better understanding of antenna theory, the following subsections review some basic electrical concepts, including voltage and its electric field, current and its magnetic field, and their relationship to the propagation of electrical energy.

Electric Field

1-121. Around every electrically charged object is a force field that can be detected and measured. This force field can cause electric charges to move in the field. When an object is charged electrically, there is either a greater or a smaller concentration of electrons than normal. Thus, a difference of potential exists between a charged object and an uncharged object. An electric field is, therefore, associated with a difference of potential, or a voltage.

1-122. Lines that are drawn to show the paths along which the force acts commonly represent this invisible field of force. The lines representing the electric field are drawn in the direction that a single positive charge would normally move under the influence of that field. A large electric force is shown by a large concentration of lines; a few lines indicate a weak force.

1-123. When a capacitor is connected across a source of voltage, such as a battery, it is charged by a particular amount, depending on the voltage and the value of capacitance (see figure 1-25). Because of the EMF (electromotive force) of the battery, negative charges flow to the lower plate, leaving the upper plate positively charged. Along with the growth of charge, the electric field is also building up. The flux lines are directed from the positive to the negative charges and at right angles to the plates. When the capacitor is fully charged, the voltage of the capacitor is equal to the voltage of the source and opposite in polarity. The charged capacitor stores the energy in the form of an electric field. It can be said, therefore, that an electric field indicates voltage.

1-124. If the two plates of the capacitor are spread farther apart, the electric field must curve to meet the plates at right angles (figure 1-26). The straight lines in view A of figure 1-26 become arcs in view B, and approximately semicircles in view C, where the plates are in a straight line. Instead of flat metal plates, as in the capacitor, the two elements can take the form of metal rods or wires and form the basic antenna.

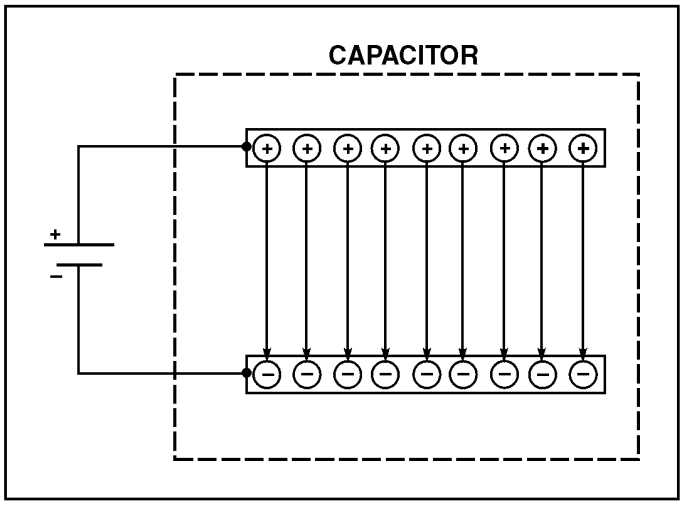


Figure 1-25. Electric Fields between Plates

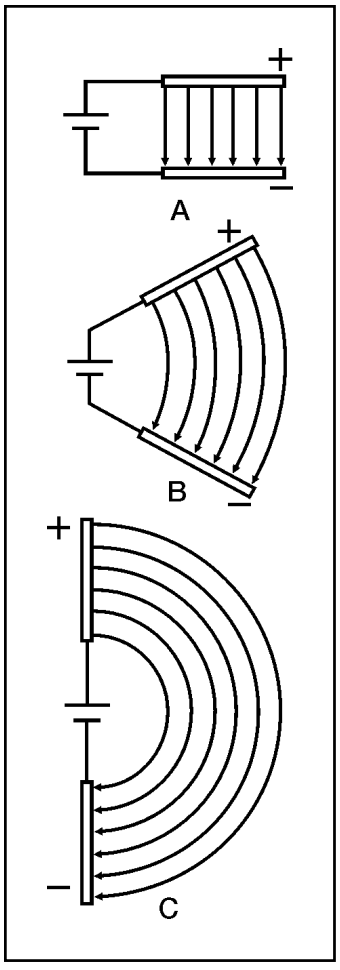


Figure 1-26. Electric Fields between Plates at Different Angles

1-125. In figure 1-27, two rods replace the plates of the capacitor, and the battery is replaced by an AC source generating a 60-hertz signal. On the positive alternation of the 60-hertz generator, the electric field extends from the positively charged rod to the negatively charged rod, as shown. On the negative alternation, the charge is reversed. The previous explanation of electrons moving from one plate to the other of the capacitor in figure 1-25 can also be applied to the rods in figure 1-27.

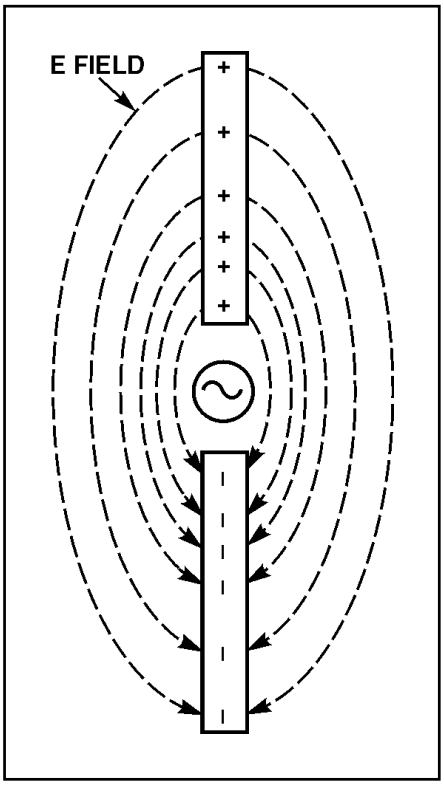


Figure 1-27. Electric Fields between Elements

1-126. The polarity of charges and the direction of the electric fields will reverse polarity and direction periodically at the frequency of the voltage source. The electric field will build up from zero to maximum in one direction and then collapse back to zero. Next, the field will build up to maximum in the opposite direction and then collapse back to zero. This complete reversal occurs during a single cycle of the source voltage. The half-wave dipole antenna (two separate rods in line as illustrated in figure 1-27) is the fundamental element normally used as a starting point of reference in any discussion concerning the radiation of electromagnetic energy into space. If RF energy from the AC generator (or transmitter) is supplied to the element of an antenna, the voltage across the antenna lags the current by 90 degrees. The antenna acts as if it were a capacitor.

Magnetic Field

1-127. When current flows through a conductor, a magnetic field is set up in the area surrounding the conductor. In fact, any moving electrical charge will create a magnetic field. The magnetic field is a region in space where a

magnetic force can be detected and measured. There are two other fields involved—an induction field, which exists close to the conductor carrying the current, and the radiation field, which becomes detached from the current-carrying rod and travels through space.

1-128. To represent the magnetic field, lines of force are again used to illustrate the energy. Magnetic lines are not drawn between the rods, nor between high- and low-potential points, as the E lines that were discussed earlier. The flow of current rather than the force of voltage creates magnetic lines. The magnetic lines of force, therefore, are drawn at right angles to the direction of current flow.

1-129. The magnetic fields that are set up around two parallel rods, as shown in figure 1-28 view A, are in maximum opposition. Rod 1 contains a current flowing from the generator, while rod 2 contains a current flowing toward the generator. As a result, the direction of the magnetic field surrounding rod 1 is opposite the direction of the magnetic field surrounding rod 2. This will cause cancellation of part or all of both magnetic fields with a resultant decrease in radiation of the electromagnetic energy. View B illustrates that if the far ends of rods 1 and 2 are separated from each other while the rods are still connected to the generator at the near ends, more space—and consequently less opposition—will occur between the magnetic fields of the two rods. View C illustrates that placing the rods in line makes the currents through both rods flow in the same direction. Therefore, the two magnetic fields are in the same direction; thus, maximum electromagnetic radiation into space can be obtained.

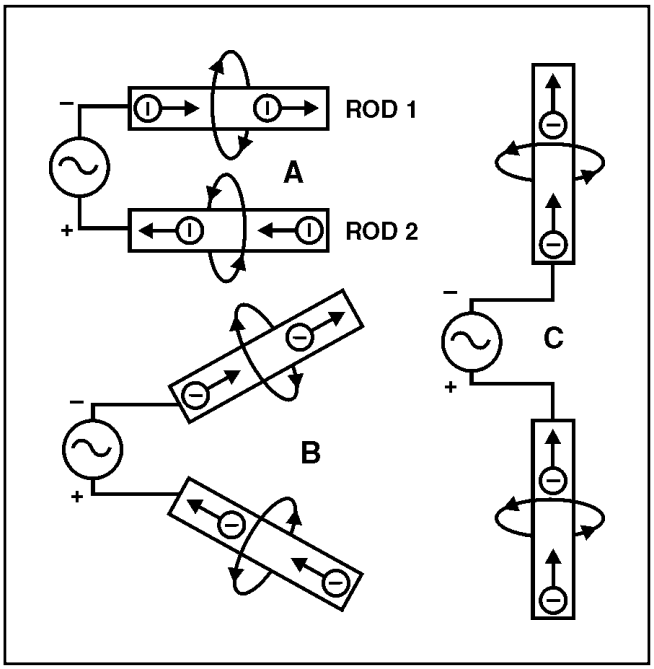


Figure 1-28. Magnetic Fields around Elements

1-130. Magnetic lines of force are indicated by the letter H and are called H lines. The direction of the magnetic lines may be determined by use of the left-hand rule for a conductor: If you grasp the conductor in your left hand

with the thumb extended in the direction of the current flow, your fingers will point in the direction of the magnetic lines of force. In view C of figure 1-28, the direction of current flow is upward along both halves of the elements (conductors). The lines of magnetic force (flux) form concentric loops that are perpendicular to the direction of current flow. The arrowheads on the loops indicate the direction of the field. The left-hand rule, illustrated in figure 1-29, is used to determine the direction of the magnetic field. The direction of the magnetic lines may be determined as follows: If you grasp the conductor in your left hand with the thumb extended in the direction of the current flow, then the rough circles formed by the fingers indicate the direction of the magnetic field.

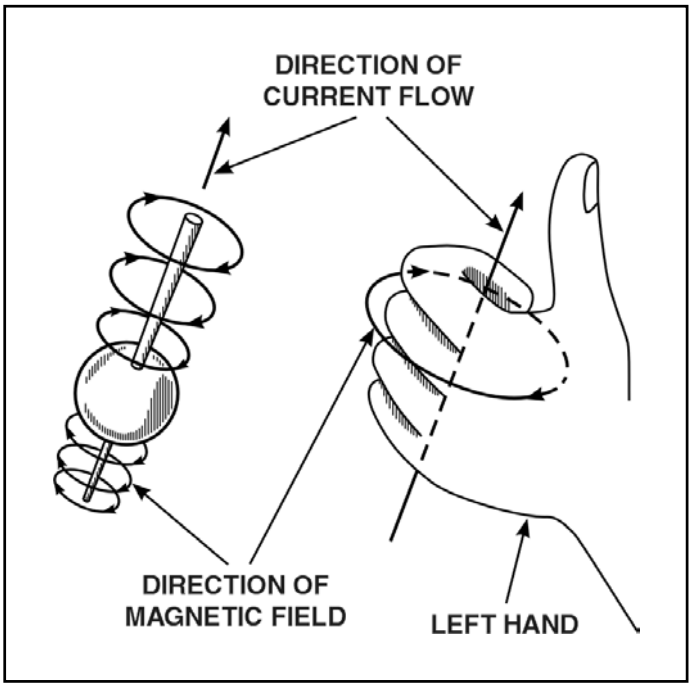


Figure 1-29. Left-Hand Rule for Conducting Elements

Combined Electric and Magnetic Fields

1-131. The generator, shown in figure 1-30, provides the voltage, which creates an electric field, and current, which creates a magnetic field. This source voltage and current build up to maximum values in one direction during one half-cycle, and then build up to maximum values in the other direction during the next half-cycle. Both the electric and magnetic fields alternate from minimum through maximum values in synchronization with the changing voltage and current. The electric and magnetic fields reach their maximum intensity one quarter-cycle apart. These fields form the induction field. Because the current and voltage that produce these E and H fields are 90 degrees out of phase, the fields will also be 90 degrees out of phase.

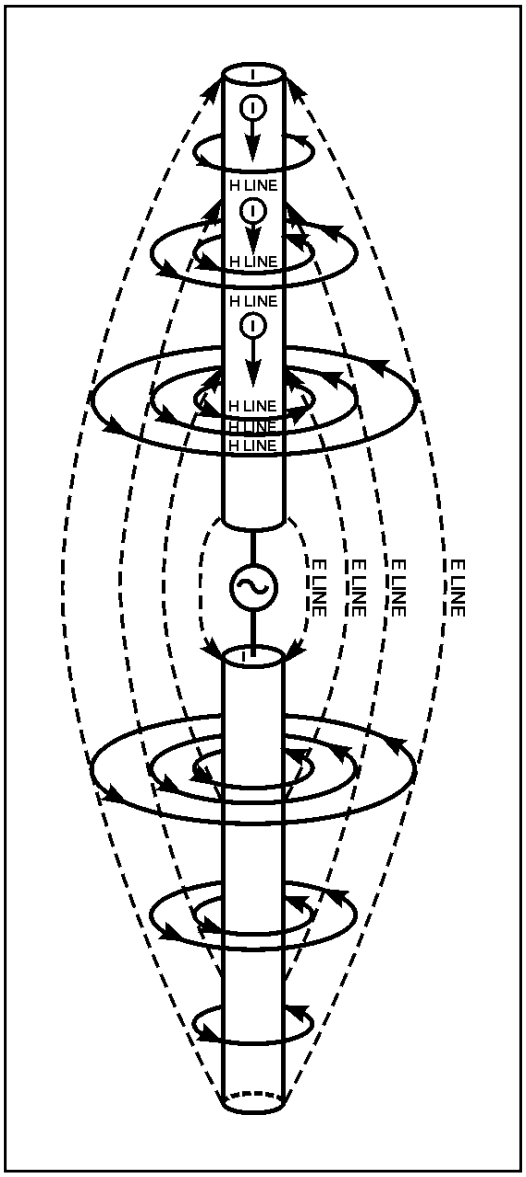


Figure 1-30. Relationship of E-Lines and Current Flow

SUMMARY

Now that you have completed this chapter, let us review some of the new terms, concepts, and ideas you have learned. You should have a thorough understanding of these principles before moving on to chapter 2.

Wave propagation is an invisible force that enables man to communicate over long distances. Wave transmission can take many forms, such as light, sound, and radio.

Light is a form of wave motion that can be seen. Heat cannot normally be seen, but can be felt. Radio waves cannot be seen or felt.

Wave motion can be seen in action by throwing a pebble into a pool of still water. The ripples that move toward the edge of the pool demonstrate the propagation theory.

Figure 1-Sum 1. Formation of Waves in Water

The transverse wave is a type of wave motion. Radio, light, and heat waves are examples of transverse waves.

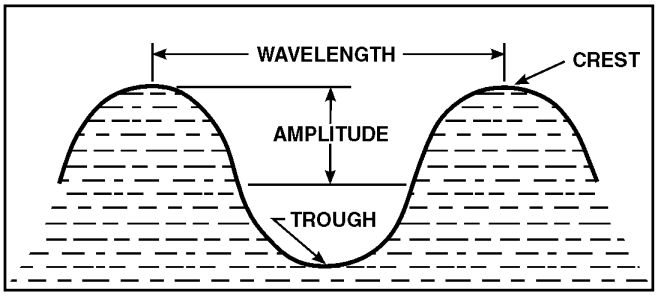


Figure 1-Sum 2. Elements of a Wave

The longitudinal wave is another type of wave motion. The sound wave is the only example of a longitudinal wave given in this text.

Source, medium, and detector (receiver) are the three requirements for all wave motion.

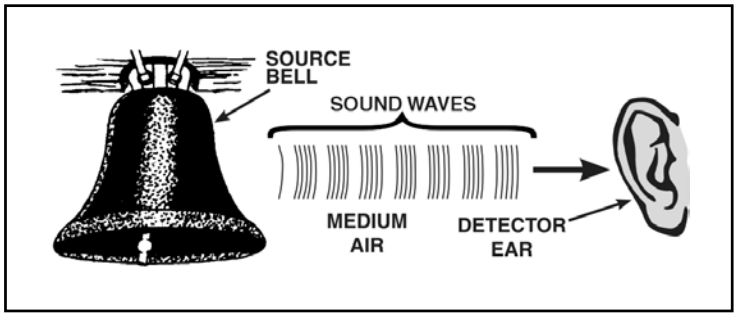


Figure 1-Sum 3. The Three Elements of Sound

A source can be anything that emits or expends energy (waves).

The medium is the vehicle for carrying waves from one point to another. Water, air, metal, and empty space are examples of mediums. Empty space can serve as a medium for electromagnetic waves but not for sound waves.

The sound detector absorbs the waves emitted by the source. The human ear is an example of a detector.

Hertz, which is abbreviated Hz, is used in lieu of "cycle per second" when referring to radio frequencies.

Velocity of propagation is the speed (or rate) at which the crest of a wave moves through a medium. Velocity can be calculated by using the formula:

$$v = \lambda f$$

Where v is velocity of propagation and is expressed in feet (meters) per second, λ is the wavelength in feet (meters), and f is the frequency in hertz.

Reflection occurs when a wave strikes an object and bounces back (toward the source). The wave that moves from the source to the object is called the incident wave, and the wave that moves away from the object is called the reflected wave.

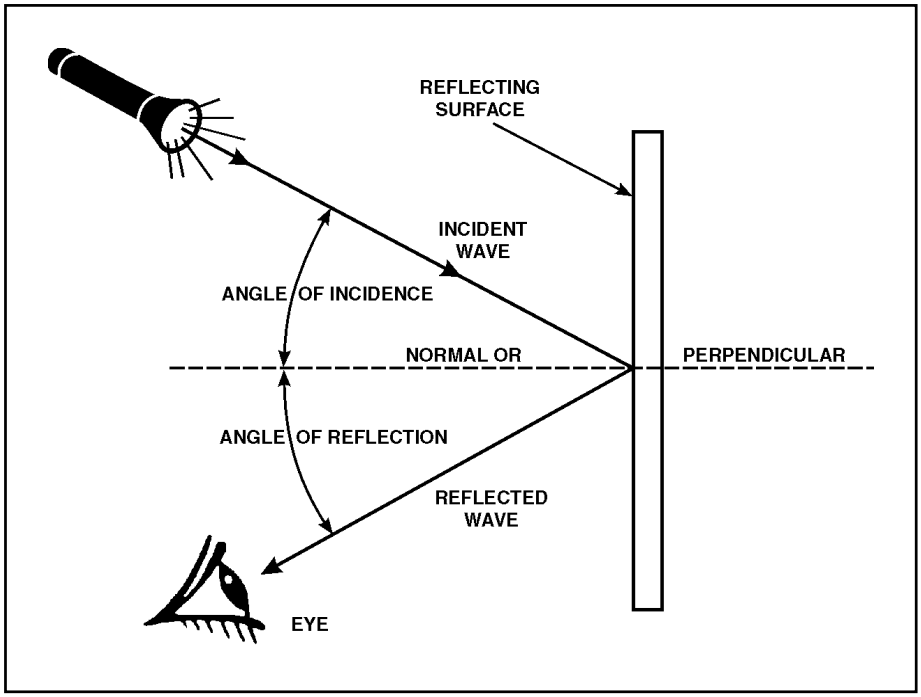


Figure 1-Sum 4. Reflection of a Wave

The law of reflection states that *the angle of incidence is equal to the angle of reflection*.

Refraction occurs when a wave traveling through two different mediums passes through the boundary of the mediums and bends toward or away from the normal.

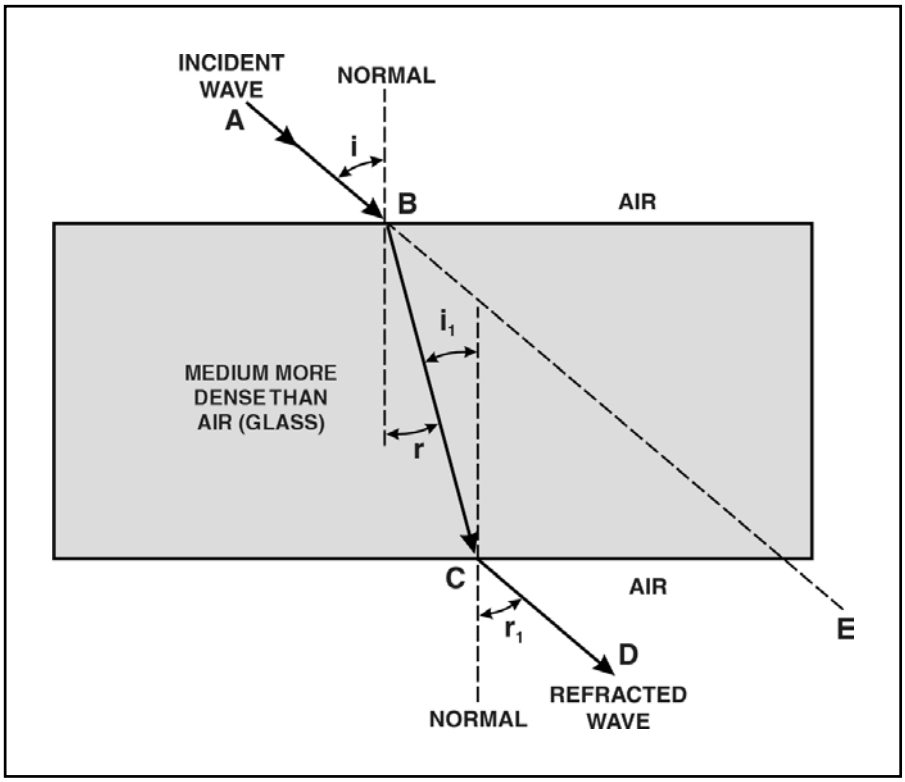


Figure 1-Sum 5. Refraction of a Wave

Diffraction can account for the ability of the AM radio waves (due to their low frequency) to travel over a mountain, while FM and TV signals (due to their higher frequencies) are blocked.

The Doppler effect is the apparent change in frequency of a source as it moves toward or away from a detector. It can affect the operation of equipment used to detect and measure wave energy.

Characteristics of sound can be audible to the human ear or it can be outside the hearing range.

Noise and tones are the two general groups that broadly classify all sounds.

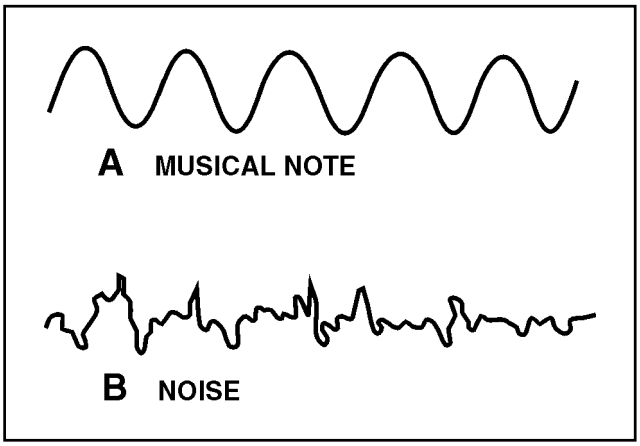


Figure 1-Sum 6. Musical Sound Versus Noise

Pitch, intensity, and quality are the three basic characteristics of sound. Pitch describes the frequency of sound. Intensity describes how much energy is transmitted. Quality enables us to distinguish one sound from another.

The density of a medium, temperature, and atmospheric pressure affect the velocity of sound. If temperature, density, or pressure increases, the velocity of sound increases and vice versa.

Acoustics is the science of sound and relates to the sense of hearing.

Echo is an example of reflection. Sound echoes are used in sonar and depth finders to determine or measure the range of an object or the depth of the ocean bottom.

Reverberation is the multiple reflections of sound waves. The prolonged roar of thunder is caused by reverberations. With underwater sound equipment, reverberations of nearby objects may interfere with returning echoes from actual targets.

Interference occurs when two waves move simultaneously through a medium. They can interfere constructively, destructively, or produce a resultant of zero.

Resonance occurs when an objects vibrates (or resonates) at its natural frequency. When different frequencies are produced inside a cavity, the sound from the cavity sounds louder at its resonant frequency than at all other frequencies.

Noise is any disturbance that distracts from or distorts the quality of sound.

A photon is the smallest unit of radiant energy that makes up light waves and radio waves.

Angstrom (Å) units are used for measuring the wavelength of light. One angstrom = 10^{-10} meters .

The visible spectrum contains all the colors between infrared and ultraviolet. Infrared and ultraviolet are invisible to the human eye.

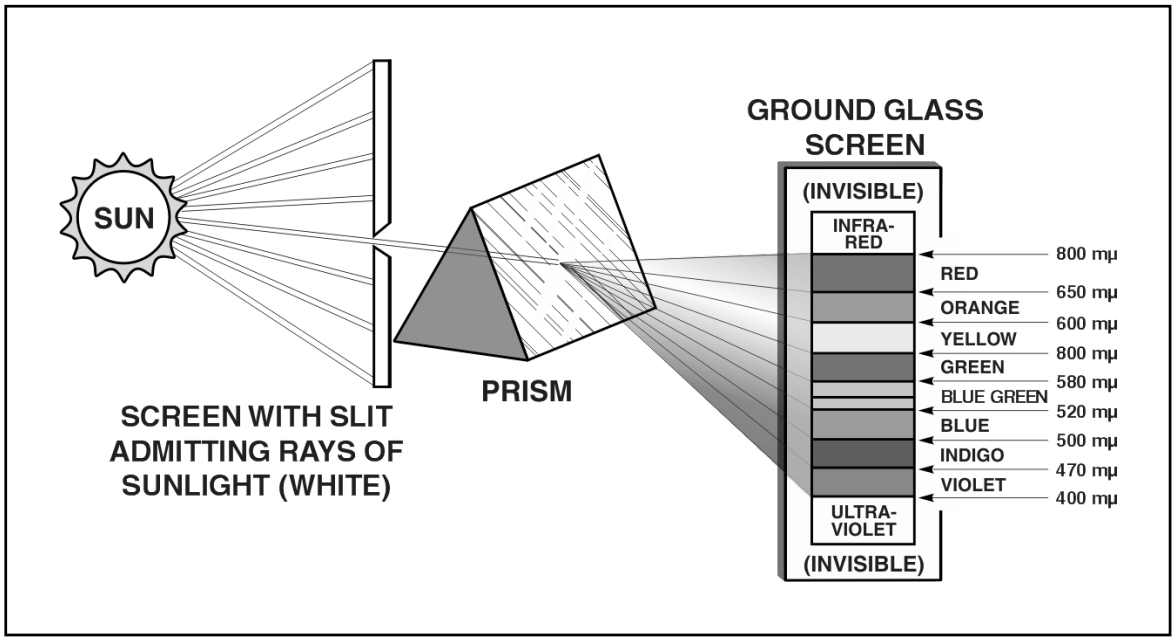


Figure 1-Sum 7. Use of a Prism to Split White Light into Different Colors

The primary colors of light are red, green, and blue. These primaries can be mixed to make any color between red and violet. If the three colors are mixed equally, they produce white light.

The complementary colors of light are magenta, yellow, and cyan. Mixing any two of the primary colors together in overlapping beams produces them.

The speed of light in empty space is considered to be 186,000 miles per second (or 300,000,000 meters per second). This speed varies in different mediums, but the constant of 186,000 miles per second is always used as the speed of light.

The electromagnetic spectrum is the complete range of electromagnetic frequencies from 3 kHz to beyond 300,000 THz. Audio frequencies (15 Hz to 20 kHz) are not electromagnetic energy and are not included in the electromagnetic spectrum. The electromagnetic field consists of an electric field and a magnetic field. These fields are responsible for the transmission and reception of electromagnetic energy through free space.

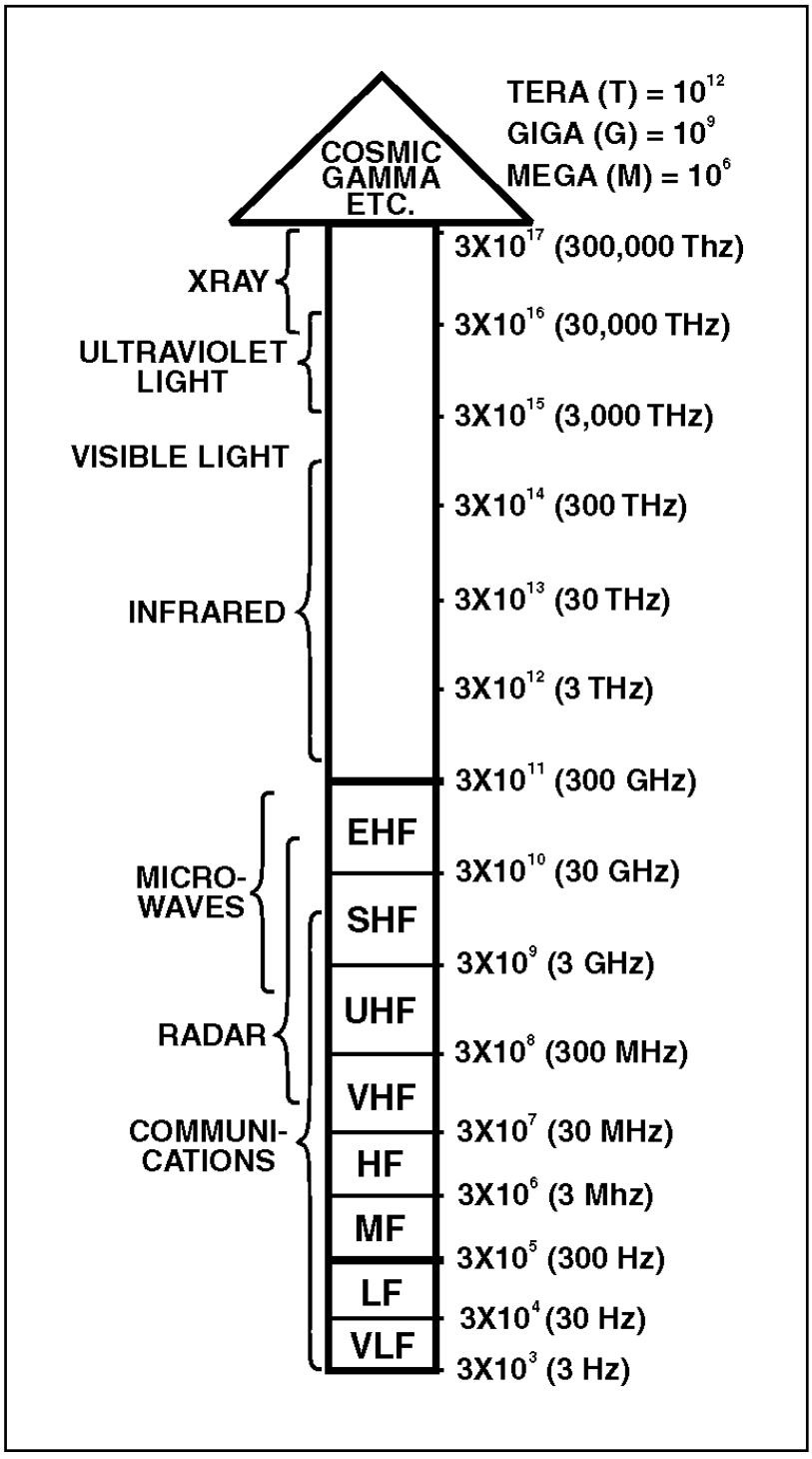


Figure 1-Sum 8. Electromagnetic Spectrum

Check-on-Learning Questions

Wave Propagation

When you are satisfied that you have answered every question to the best of your ability, check your answers using appendix A. If you missed eight or more questions, you should review the chapter, paying particular attention to the areas in which your answers were incorrect.

1. What is propagation?
2. How is a wave defined as it applies to wave propagation?
3. What is wave motion?
4. What are some examples of wave motion?
5. What type of wave motion is represented by the motion of water?
6. What are some examples of transverse waves?
7. What example of a longitudinal wave was given in the text?
8. What are the three requirements for a wave to be propagated?
9. What is a cycle?
10. What is wavelength (λ)?
11. What is the law of reflection?
12. When a wave is reflected from a surface, energy is transferred. When is the transfer of energy greatest?
13. When is the transfer of energy minimum?
14. A refracted wave occurs when a wave passes from one medium into another medium. What determines the angle of refraction?
15. The apparent change in frequency or pitch because of motion is explained by what effect?
16. What term describes sounds capable of being heard by the human ear?
17. Are all sounds audible to the human ear? Why?
18. Sound waves transmitted from a source are sometimes weak when they reach the detector. What instrument is needed to boost the weak signal?
19. What are the three basic requirements for sound?
20. What are the two general groups of sound?
21. What are the three basic characteristics of sound?
22. What is the normal audible range of the human ear?
23. What is intensity as it pertains to sound?
24. What characteristic of sound enables a person to distinguish one musical instrument from another, if they are all playing the same note?
25. How do density and temperature affect the velocity of sound?
26. What term is used to mean the science of sound?

27. A sound wave that is reflected back toward the source is known as what type of sound?
28. What is the term for multiple reflections of sound waves?
29. A cavity that vibrates at its natural frequency produces a louder sound than at other frequencies. What term is used to describe this phenomenon?
30. What do we call a disturbance that distracts or distorts the quality of sound?
31. What are three means of producing light?
32. What is the smallest unit of radiant energy?
33. What unit is used to measure the different wavelengths of light?
34. What are the three primary colors of light?
35. What are the three secondary colors of light?
36. White light falls upon a dull, rough, dark-brown object. Will the light primarily be reflected, diffused, or absorbed by the object?
37. What color will be emitted by a dull, rough, black object when white light falls upon it?
38. A substance that transmits light but through which an object cannot be seen clearly is known as what kind of substance?
39. At what speed does light travel?
40. A light wave enters a sheet of glass at a perfect right angle to the surface. Is the majority of the wave reflected, refracted, transmitted, or absorbed?
41. When light strikes a piece of white paper, the light is reflected in all directions. What do we call this scattering of light?
42. What three examples of electromagnetic energy are mentioned in the text?
43. What is the main difference between the bulk of the electromagnetic spectrum and the visible spectrum?
44. What are the two components (fields) that make up the electromagnetic wave?
45. What do we call a conductor (or set of conductors) that radiates electromagnetic energy into space?
46. What do we call the field that is created between two rods when a voltage is applied to them?
47. When current flows through a conductor, a field is created around the conductor. What do we call this field?
48. An induction field is created around a conductor when current flows through it. What do we call the field that detaches itself from the conductor and travels through space?

Chapter 2

Radio Wave Propagation

LEARNING OBJECTIVES

2-1. Upon completing this chapter, you should be able to do the following:

- State what the electromagnetic field is and what components make up the electromagnetic field.
- State the difference between the induction field and the radiation field.
- State what radio waves are.
- List the components of a radio wave and define the terms cycle, frequency, harmonics, period, wavelength, and velocity as applied to radio wave propagation.
- Compute the wavelength of radio waves.
- State how radio waves are polarized, vertically and horizontally.
- State what reflection, refraction, and diffraction are as applied to radio waves.
- State what influence the earth's atmosphere has on radio waves and list the different layers of the earth's atmosphere.
- Identify a ground wave and a sky wave, and describe the effects of the ionosphere on the sky wave.
- Identify the structure of the ionosphere.
- Define density of layer, frequency, angle of incidence, skip distance, and skip zone.
- Describe propagation paths.
- Describe fading, multipath fading, and selective fading. Describe propagation paths.
- State how transmission losses affect radio wave propagation.
- State how electromagnetic interference, man-made/natural interference, and ionospheric disturbances affect radio wave propagation. State how transmission losses affect radio wave propagation.
- Identify variations in the ionosphere.
- Identify the maximum, optimum, and lowest usable frequencies of radio waves.
- State what temperature inversion is, how frequency predictions are made, and how weather affects frequency.
- State what tropospheric scatter is and how it affects radio wave propagation.

ELECTROMAGNETIC FIELDS

2-2. The way energy is propagated into free space is a source of great dispute among people concerned with it. Although many theories have been proposed, the following theory adequately explains the phenomena and has been widely accepted. There are two basic fields associated with every antenna; an induction field and a radiation field. The field associated with the energy stored in the antenna is the induction field. This field is said to provide no part in the transmission of electromagnetic energy through free space. However, without the presence of the induction field, there would be no energy radiated.

INDUCTION FIELD

2-3. Figure 2-1, which illustrates a low-frequency generator connected to an antenna, will help you understand how the induction field is produced. Let us follow the generator through one cycle of operation.

2-4. Initially, you can consider that the generator output is zero and that no fields exist about the antenna, as shown in figure 2-1, view A. Now assume that the generator produces a slight potential and has the instantaneous polarity shown in view B. Because of this slight potential, the antenna capacitance acts as a short, allowing a large flow of current (I) through the antenna in the direction shown. This current flow, in turn, produces a large magnetic field about the antenna. Because the flow of current at each end of the antenna is minimum, the corresponding magnetic fields at each end of the antenna are also minimum. As time passes, charges—which oppose antenna current and produce an electrostatic field (E field)—collect at each end of the antenna. Eventually, the antenna capacitance becomes fully charged and stops current flow through the antenna. Under this condition, the electrostatic field is maximum, and the magnetic field (H field) is fully collapsed, as shown in view C.

2-5. As the generator potential decreases back to zero, the potential of the antenna begins to discharge. During the discharging process, the electrostatic field collapses and the direction of current flow reverses, as shown in figure 2-1, view D. When the current again begins to flow, an associated magnetic field is generated. Eventually, the electrostatic field completely collapses, the generator potential reverses, and current is maximum, as shown in view E. As charges collect at each end of the antenna, an electrostatic field is produced and current flow decreases. This causes the magnetic field to begin collapsing. The collapsing magnetic field produces more current flow, a greater accumulation of charge, and a greater electrostatic field. The antenna gradually reaches the condition shown in view F, where current is zero and the collected charges are maximum.

2-6. As the generator potential again decreases toward zero, the antenna begins to discharge and the electrostatic field begins to collapse. When the generator potential reaches zero, discharge current is maximum and the associated magnetic field is maximum. A brief time later, generator potential reverses, and the condition shown in view B recurs.

Note: The electric field (E field) and the electrostatic field (E field) are the same. The terms are used interchangeably throughout this text.

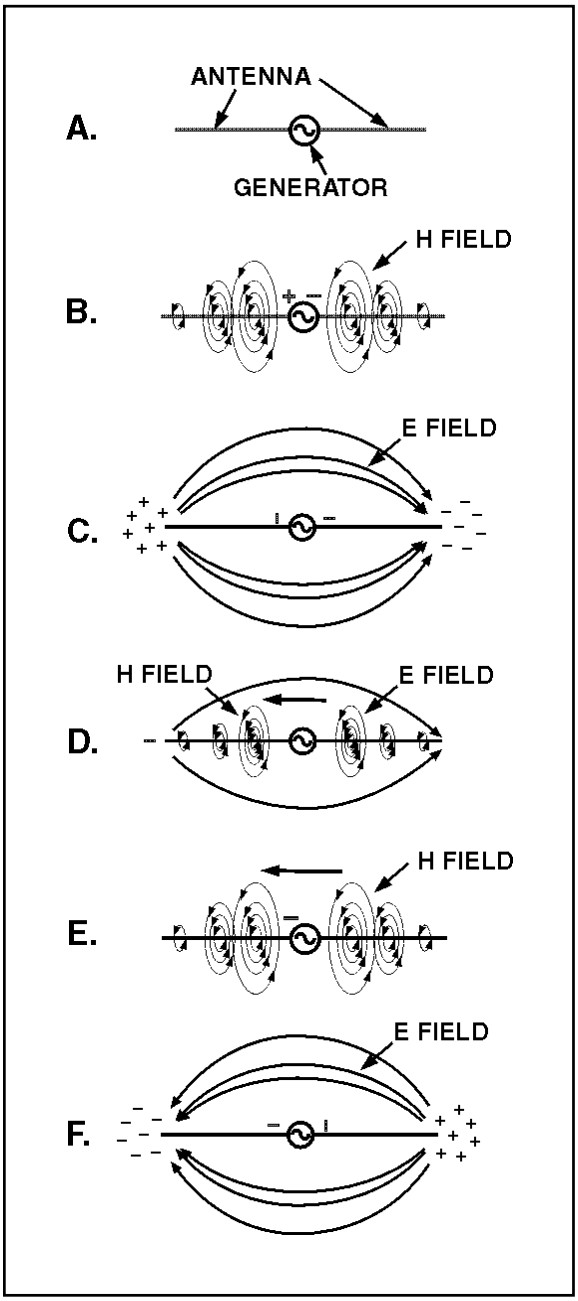


Figure 2-1. Induction Field about an Antenna

2-7. The graph shown in figure 2-2 shows the relationship between the magnetic (H) field and the electric (E) field plotted against time. Note that the two fields are 90 degrees out of phase with each other. If you compare the graph in figure 2-2 with figure 2-1, you will notice that the two fields around the antenna are displaced 90 degrees from each other in space. (The H field exists in a plane perpendicular to the antenna. The E field exists in a plane parallel with the antenna, as shown in figure 2-1.)

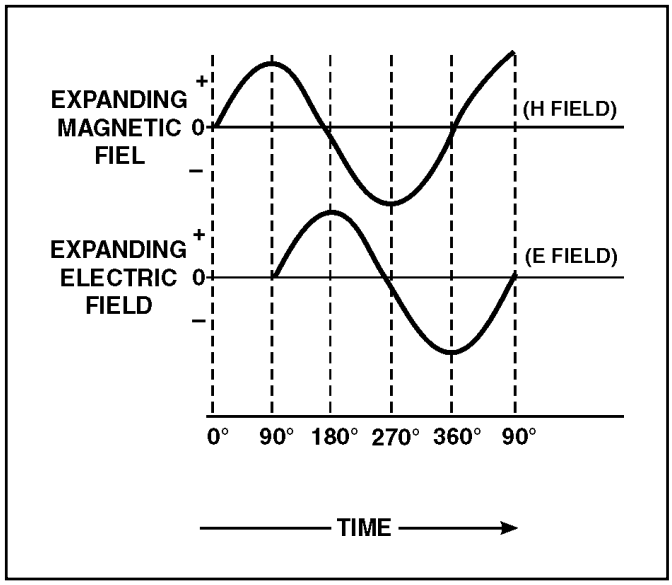


Figure 2-2. Phase Relationship of Induction Field Components

2-8. All the energy supplied to the induction field is returned to the antenna by the collapsing E and H fields. No energy from the induction field is radiated from the antenna. Therefore, the induction field is considered a local field and plays no part in the transmission of electromagnetic energy. The induction field represents only the stored energy in the antenna and is responsible only for the resonant effects that the antenna reflects to the generator.

RADIATION FIELD

2-9. The E and H fields that are set up in the transfer of energy through space are known collectively as the radiation field. This radiation field is responsible for electromagnetic radiation from the antenna. The radiation field decreases as the distance from the antenna is increased. Because the decrease is linear, the radiation field reaches great distances from the antenna.

2-10. Let us look at a half-wave antenna to illustrate how this radiation actually takes place. Simply stated, a half-wave antenna is one that has an electrical length equal to half the wavelength of the signal being transmitted. Assume, for example, that a transmitter is operating at 30 megahertz. If a half-wave antenna is used with the transmitter, the antenna's electrical length would have to be at least 16 feet long. (The formula used to compute the electrical length of an antenna is explained in chapter 4.) When power is delivered to the half-wave antenna, both an induction field and a radiation field are set up by the fluctuating energy. At the antenna, the intensities of these fields are proportional to the amount of power delivered to the antenna from a source such as a transmitter. At a short distance from the antenna and beyond, only the radiation field exists. This radiation field is made up of an electric component and a magnetic component at right angles to each other in space and varying together in intensity.

2-11. With a high-frequency generator (a transmitter) connected to the antenna, the induction field is produced as described in the previous section. However, the generator potential reverses before the electrostatic field has had time to collapse completely. The reversed generator potential neutralizes the remaining antenna charges, leaving a resultant E field in space.

2-12. Figure 2-3 is a simple picture of an E field detaching itself from an antenna. (The H field is not considered in this example, although it is present.) In view A, the voltage is maximum and the electric field has maximum intensity. The lines of force begin at the end of the antenna that is positively charged and extend to the end of the antenna that is negatively charged. Note that the outer E lines are stretched away from the inner lines. This is because of the repelling force that takes place between lines of force in the same direction. As the voltage drops (view B), the separated charges come together, and the ends of the lines move toward the center of the antenna. However, because lines of force in the same direction repel each other, the centers of the lines are still being held out.

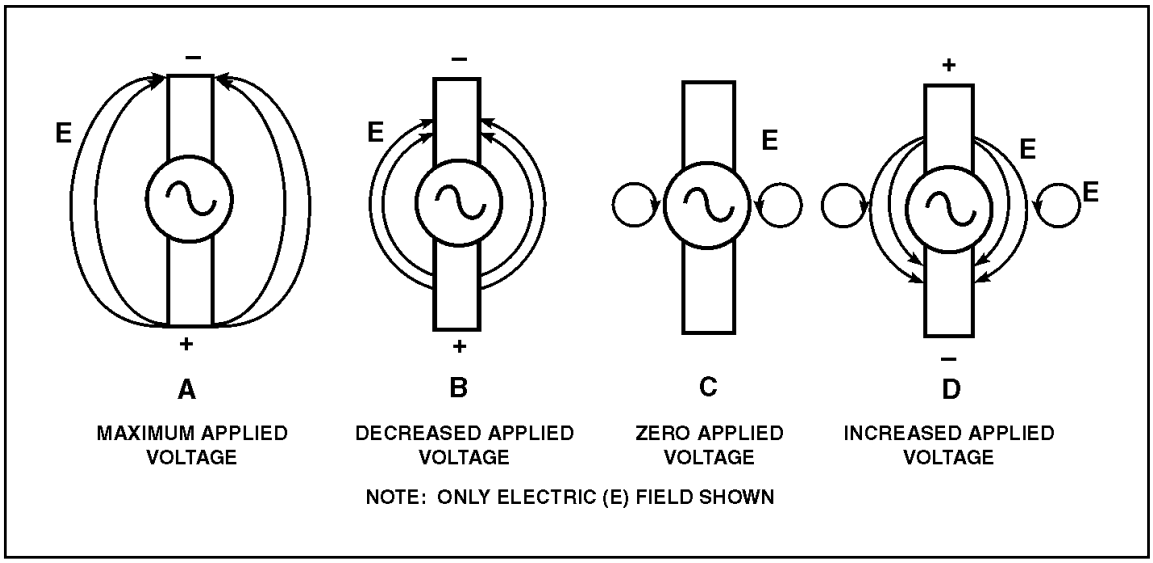


Figure 2-3. Radiation from an Antenna

2-13. As the voltage approaches zero (view B), some of the lines collapse back into the antenna. At the same time, the ends of other lines begin to come together to form a complete loop. Notice the direction of these lines of force next to the antenna in view C. At this point the voltage on the antenna is zero. As the charge starts to build up in the opposite direction (view D), electric lines of force again begin at the positive end of the antenna and stretch to the negative end of the antenna. These lines of force, being in the same direction as the sides of the closed loops next to the antenna, repel the closed loops and force them out into space at the speed of light. As these loops travel through space, they generate a magnetic field in phase with them.

2-14. Because each successive E field is generated with a polarity that is opposite the preceding E field (that is, the lines of force are opposite), an oscillating electric field is produced along the path of travel. When an electric field oscillates, a magnetic field having an intensity that varies directly with

that of the E field is produced. The variations in magnetic field intensity, in turn, produce another E field. Thus, the two varying fields sustain each other, resulting in electromagnetic wave propagation.

2-15. During this radiation process, the E and H fields are in phase in time but physically displaced 90 degrees in space. Thus, the varying magnetic field produces a varying electric field; and the varying electric field, in turn, sustains the varying magnetic field. Each field supports the other, and neither can be propagated by itself. Figure 2-4 shows a comparison between the induction field and the radiation field.

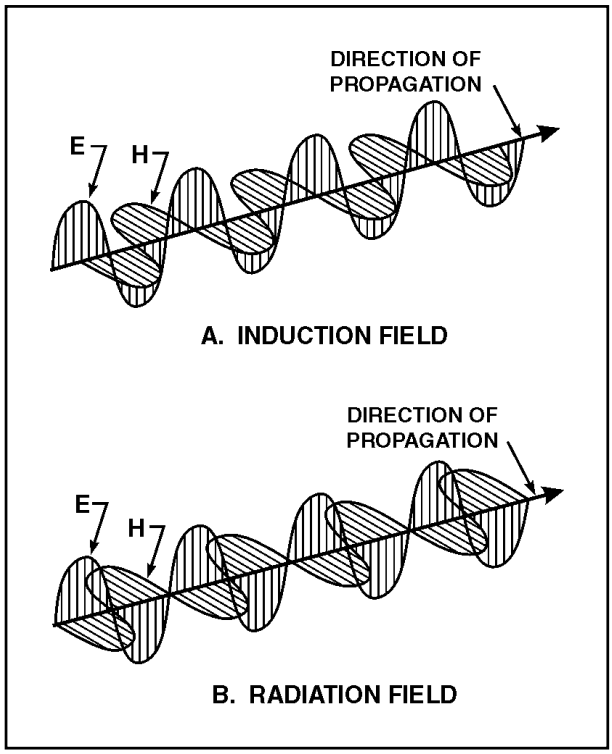


Figure 2-4. E and H Components of Induction and Radiation Fields

RADIO WAVES

2-16. An energy wave generated by a transmitter is called a radio wave. The radio wave radiated into space by the transmitting antenna is a very complex form of energy containing both electric and magnetic fields. Because of this combination of fields, radio waves are also referred to as electromagnetic radiation. The discussion that follows explains the earth's atmosphere and its effect on radio waves. All the principles of wave motion that were discussed in chapter 1 also apply to radio waves.

Note. The term radio wave is not limited to communications equipment alone. The term applies to all equipment that generates signals in the form of electromagnetic energy.

CHARACTERISTICS OF RADIO WAVES

2-17. **Shape**. The basic shape of the wave generated by a transmitter is that of a sine wave. The wave radiated out into space, however, may or may not retain the characteristics of the sine wave.

2-18. A sine wave can be one cycle or many cycles. Recall from chapter 1 that the number of cycles of a sine wave that are completed in 1 second is known as the frequency of the sine wave. For example, 60 cycles of ordinary house current occur each second, so house current is said to have a frequency of 60 cycles per second or 60 hertz.

2-19. **Frequency**. The frequencies falling between 3000 hertz (3 kHz) and 300,000,000,000 hertz (300 GHz) are called radio frequencies (abbreviated RF) because they are commonly used in radio communications. This part of the radio frequency spectrum is divided into bands, each band being 10 times higher in frequency than the one immediately below it. This arrangement serves as a convenient way to remember the range of each band. The RF bands are shown in Table 2-1. The usable radio-frequency range is roughly 10 kilohertz to 100 gigahertz.

Table 2-1. Radio Frequency Bands

DESCRIPTION	*ABBREVIATION*	*FREQUENCY*
Very low	VLF	3 to 30 kHz
Low	LF	30 to 300 kHz
Medium	MF	300 to 3000 kHz
High	HF	3 to 30 MHz
Very high	VHF	30 to 300 MHz
Ultrahigh	UHF	300 to 3000 MHz
Superhigh	SHF	3 to 30 GHz
Extremely high	EHF	30 to 300 GHz

2-20. **Harmonics**. Any frequency that is a whole number multiple of a smaller basic frequency is known as a harmonic of that basic frequency. The basic frequency itself is called the first harmonic or, more commonly, the fundamental frequency. A frequency that is twice as great as the fundamental frequency is called the second harmonic; a frequency three times as great is the third harmonic; and so on. For example:

- First harmonic (fundamental frequency) 3000 kHz
- Second harmonic 6000 kHz
- Third harmonic 9000 kHz

2-21. **Period**. The period of a radio wave is simply the amount of time required to complete one full cycle. If a sine wave has a frequency of 2 hertz, each cycle has a duration, or period, of one-half second. If the frequency is 10 hertz, the period of each cycle is one-tenth of a second. Because the frequency of a radio wave is the number of cycles that are completed in one second, you should be able to see that as the frequency of a radio wave increases, its period decreases.

2-22. **Wavelength**. A wavelength is the space occupied by one full cycle of a radio wave at any given instant. Wavelengths are expressed in meters (1 meter is equal to 3.28 feet). You need to have a good understanding of frequency and wavelength to be able to select the proper antenna(s) to use for successful communications. The relationship between frequency, wavelength, and antennas are discussed in chapter 4.

2-23. **Velocity**. The velocity (or speed) of a radio wave radiated into free space by a transmitting antenna is equal to the speed of light, which is 186,000 miles per second or 300,000,000 meters per second. Because of various factors, such as barometric pressure, humidity, and molecular content, radio waves travel inside the earth's atmosphere at a speed slightly less than the speed of light. Normally, in discussions of the velocity of radio waves, the velocity referred to is the speed at which radio waves travel in free space.

2-24. The frequency of a radio wave has nothing to do with its velocity. A 5-megahertz wave travels through space at the same velocity as a 10-megahertz wave. However, the velocity of radio waves is an important factor in making wavelength-to-frequency conversions, the subject of our next discussion.

WAVELENGTH-TO-FREQUENCY CONVERSIONS

2-25. Radio waves are often referred to by their wavelength in meters rather than by frequency. For example, most people have heard commercial radio stations make announcements similar to the following: "Station WXYZ operating on 240 meters." To tune receiving equipment that is calibrated by frequency to such a station, you must first convert the designated wavelength to its equivalent frequency.

2-26. As discussed earlier, a radio wave travels 300,000,000 meters per second (speed of light); therefore, a radio wave of 1 hertz would have traveled a distance (or wavelength) of 300,000,000 meters. Obviously then, if the frequency of the wave is increased to 2 hertz, the wavelength will be cut in half to 150,000,000 meters. This illustrates the principle that the higher the frequency, the shorter the wavelength.

2-27. Wavelength-to-frequency conversions of radio waves are really quite simple because wavelength and frequency are reciprocals: Either one divided into the velocity of a radio wave yields the other. Remember, the formula for wavelength is:

$$\lambda = \frac{v}{f} \quad \text{or} \quad f = \frac{v}{\lambda}$$

Where:

λ = wavelength in meters

v = velocity of radio of radio wave (in Hz, kHz, or MHz)

f = frequency of radio wave (in Hz, kHz, or MHz)

2-28. The wavelength in meters divided into 300,000,000 yields the frequency of a radio wave in hertz. Likewise, the wavelength divided into 300,000 yields the frequency of a radio wave in kilohertz, and the wavelength divided into 300 yields the frequency in megahertz.

2-29. Now, let us apply the formula to determine the frequency to which the receiving equipment must be tuned to receive station WXYZ operating on 240 meters. Radio wave frequencies are normally expressed in kilohertz or megahertz.

2-30. To find the frequency in hertz, use the formula:

$$f = \frac{v}{\lambda}$$

Given:

$v = 300{,}000{,}000$ meters per second

$\lambda = 240$ meters

Solution:

$$f = \frac{300{,}000{,}000 \text{ meters per second}}{240 \text{ meters}}$$

$f = 1{,}250{,}000$ Hz

2-31. To find the frequency in kilohertz, use the formula:

$$f\,(\text{kHz}) = \frac{300{,}000}{\lambda}$$

Given:

$\lambda = 240$ meters

Solution:

$$f\,(\text{kHz}) = \frac{300{,}000}{240 \text{ meters}}$$

$f = 1{,}250$ kHz

2-32. To find the frequency in megahertz, use the formula:

$$f\,(\text{MHz}) = \frac{300}{\lambda}$$

Given:

$\lambda = 240$ meters

Solution:

$$f\,(\text{MHz}) = \frac{300}{240 \text{ meters}}$$

$f = 1.25$ MHz

POLARIZATION

2-33. For maximum absorption of energy from the electromagnetic fields, the receiving antenna must be located in the plane of polarization. This places the conductor of the antenna at right angles to the magnetic lines of force moving through the antenna and parallel to the electric lines, causing maximum induction.

2-34. Normally, the plane of polarization of a radio wave is the plane in which the E field propagates with respect to the earth. If the E field component of the radiated wave travels in a plane perpendicular to the earth's surface (vertical), the radiation is said to be vertically polarized, as shown in figure 2-5, view A. If the E field propagates in a plane parallel to the earth's surface (horizontal), the radiation is said to be horizontally polarized, as shown in view B.

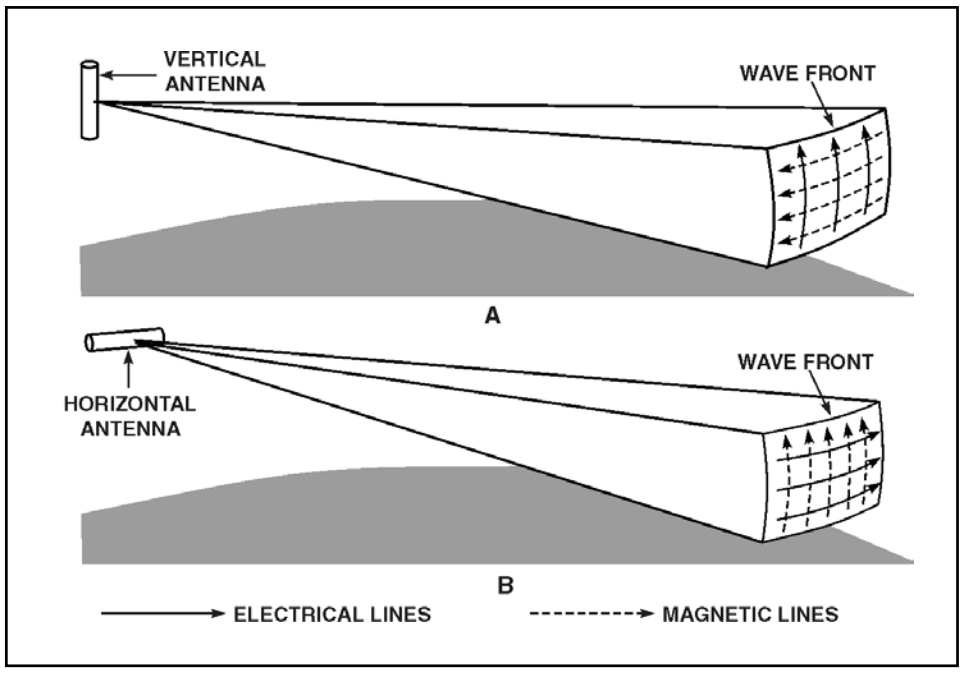


Figure 2-5. Vertical and Horizontal Polarization

2-35. The position of the antenna in space is important because it affects the polarization of the electromagnetic wave. When the transmitting antenna is close to the ground, vertically polarized waves cause greater signal strength along the earth's surface. On the other hand, antennas high above the ground should be horizontally polarized to get the greatest possible signal strength to the earth's surface. Vertically and horizontally polarized antennas are discussed in more detail in chapter 4.

2-36. The radiated energy from an antenna is in the form of an expanding sphere. Any small section of this sphere is perpendicular to the direction the energy travels and is called a wavefront. All energy on a wavefront is in phase. Usually all points on the wavefront are at equal distances from the antenna. The farther the wavefront is from the antenna, the less spherical

the wave appears. At a considerable distance the wavefront can be considered as a plane surface at a right angle to the direction of propagation.

2-37. If you know the directions of the E and H components, you can use the "right-hand rule" to determine the direction of wave propagation (see figure 2-6). This rule states that if the thumb, forefinger, and middle finger of the right hand are extended so they are mutually perpendicular, the middle finger will point in the direction of wave propagation if the thumb points in the direction of the E field and the forefinger points in the direction of the H field. Because both the E and H fields reverse directions simultaneously, propagation of a particular wavefront is always in the same direction (away from the antenna).

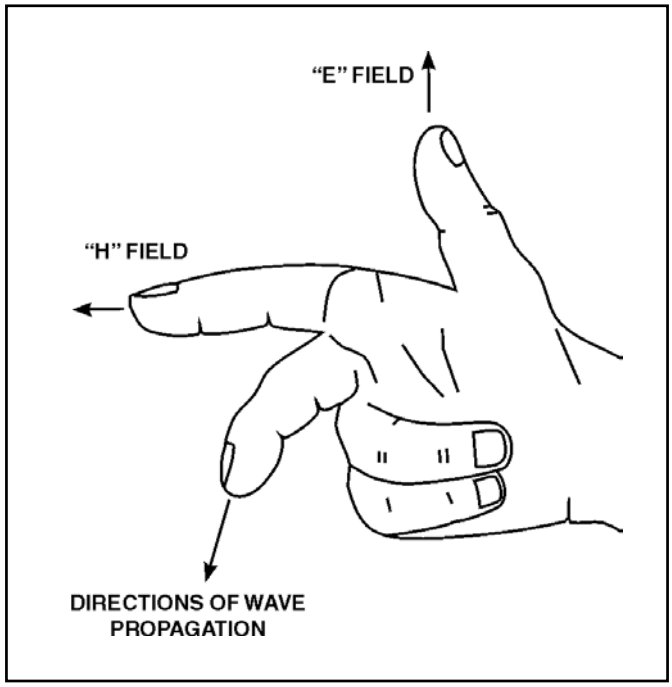


Figure 2-6. Right-Hand Rule for Propagation

ATMOSPHERIC PROPAGATION

2-38. Within the atmosphere, radio waves can be reflected, refracted, and diffracted in the same manner as light and heat waves.

Reflection

2-39. Radio waves may be reflected from various substances or objects they meet during travel between the transmitting and receiving sites. The amount of reflection depends on the reflecting material. Smooth metal surfaces of good electrical conductivity are efficient reflectors of radio waves. The surface of the earth itself is a fairly good reflector. The radio wave is not reflected from a single point on the reflector but rather from an area on its surface. The size of the area required for reflection to take place depends on the wavelength of the radio wave and the angle at which the wave strikes the reflecting substance.

2-40. When radio waves are reflected from flat surfaces, a phase shift in the alternations of the wave occurs. Figure 2-7 shows two radio waves being reflected from the earth's surface. Notice that the positive and negative alternations of radio waves (A) and (B) are in phase with each other in their paths toward the earth's surface. After reflection takes place, however, the waves are approximately 180 degrees out of phase. The amount of phase shift that occurs is not constant. It depends on the polarization of the wave and the angle at which the wave strikes the reflecting surface. Radio waves that keep their phase relationships after reflection normally produce a stronger signal at the receiving site. Those that are received out of phase produce a weak or fading signal. The shifting in the phase relationships of reflected radio waves is one of the major reasons for fading. Fading is discussed in more detail later in this chapter.

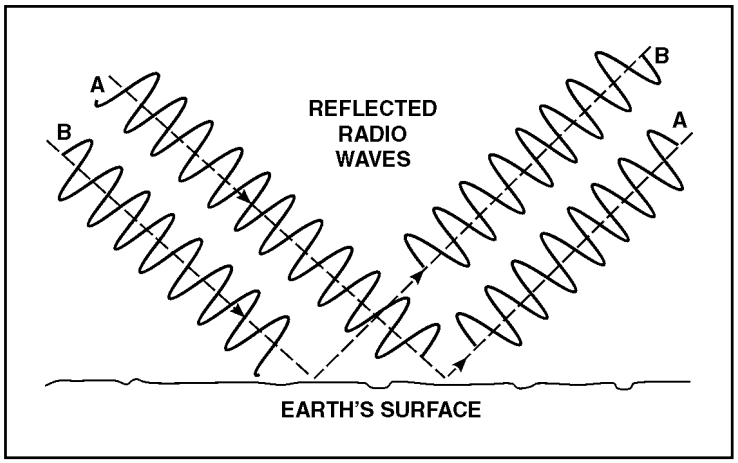


Figure 2-7. Phase Shift of Reflected Radio Waves

Refraction

2-41. Another phenomenon common to most radio waves is the bending of the waves as they move from one medium into another in which the velocity of propagation is different. This bending of the waves is called refraction. For example, suppose you are driving down a smoothly paved road at a constant speed and suddenly one wheel goes off onto the soft shoulder. The car tends to veer off to one side. The change of medium, from hard surface to soft shoulder, causes a change in speed or velocity. The tendency is for the car to change direction. This same principle applies to radio waves as changes occur in the medium through which they are passing. As an example, the radio wave shown in figure 2-8 is traveling through the earth's atmosphere at a constant speed. As the wave enters the dense layer of electrically charged ions, the part of the wave that enters the new medium first travels faster than the parts of the wave that have not yet entered the new medium. This abrupt increase in velocity of the upper part of the wave causes the wave to bend back toward the earth. This bending, or change of direction, is always toward the medium that has the lower velocity of propagation.

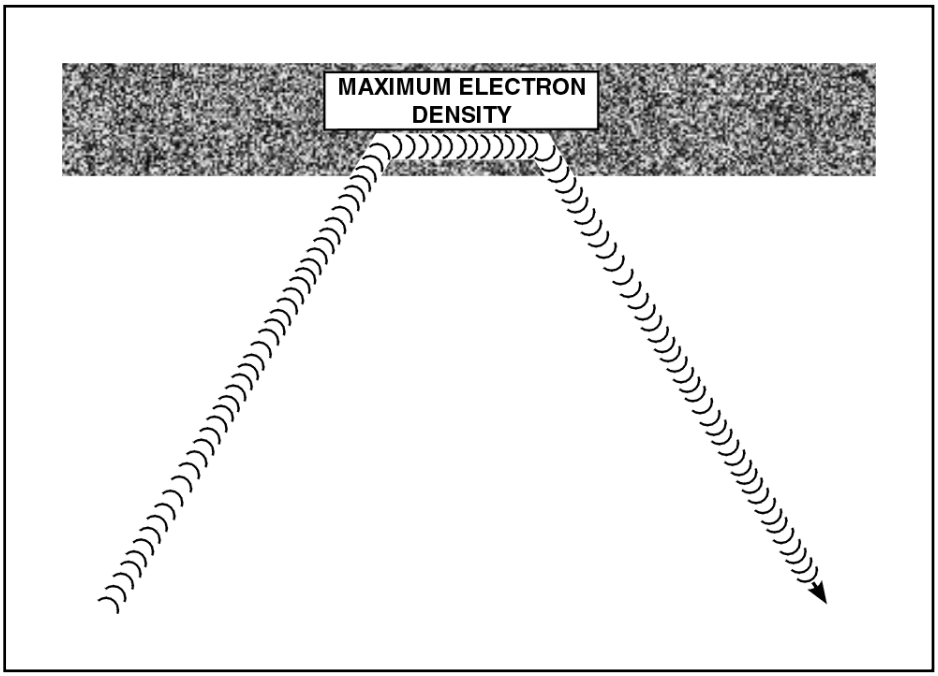


Figure 2-8. Radio Wave Refraction

2-42. Radio waves passing through the atmosphere are affected by certain factors, such as temperature, pressure, humidity, and density. These factors can cause the radio waves to be refracted. This effect is discussed in greater detail later in this chapter.

Diffraction

2-43. A radio wave that meets an obstacle has a natural tendency to bend around the obstacle, as illustrated in figure 2-9. The bending, called diffraction, results in a change of direction of part of the wave energy from the normal line-of-sight path. This change makes it possible to receive energy around the edges of an obstacle as shown in figure 2-9, view A or at some distances below the highest point of an obstruction, as shown in view B. Although diffracted RF energy usually is weak, it can still be detected by a suitable receiver. The principal effect of diffraction extends the radio range beyond the visible horizon. In certain cases, by using high power and very low frequencies, radio waves can be made to encircle the earth by diffraction.

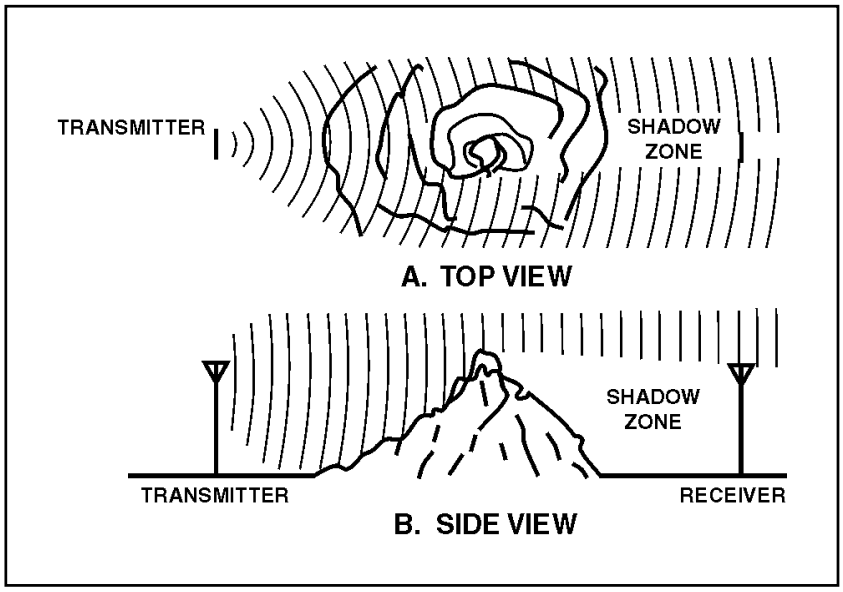


Figure 2-9. Diffraction around an Object

EFFECT OF THE EARTH'S ATMOSPHERE ON RADIO WAVES

2-44. The discussion of electromagnetic wave propagation is concerned mainly with the properties and effects of the medium located between the transmitting antenna and the receiving antenna. While radio waves traveling in free space have little outside influence affecting them, radio waves traveling within the earth's atmosphere are affected by varying conditions. The influence exerted on radio waves by the earth's atmosphere adds many new factors to complicate what at first seems to be a relatively simple problem. These complications are because of a lack of uniformity within the earth's atmosphere. Atmospheric conditions vary with changes in height, geographical location, and even with changes in time (day, night, season, and year). Knowledge of the composition of the earth's atmosphere is extremely important for understanding wave propagation.

2-45. The earth's atmosphere is divided into three separate regions, or layers. They are the troposphere, the stratosphere, and the ionosphere. The layers of the atmosphere are illustrated in figure 2-10.

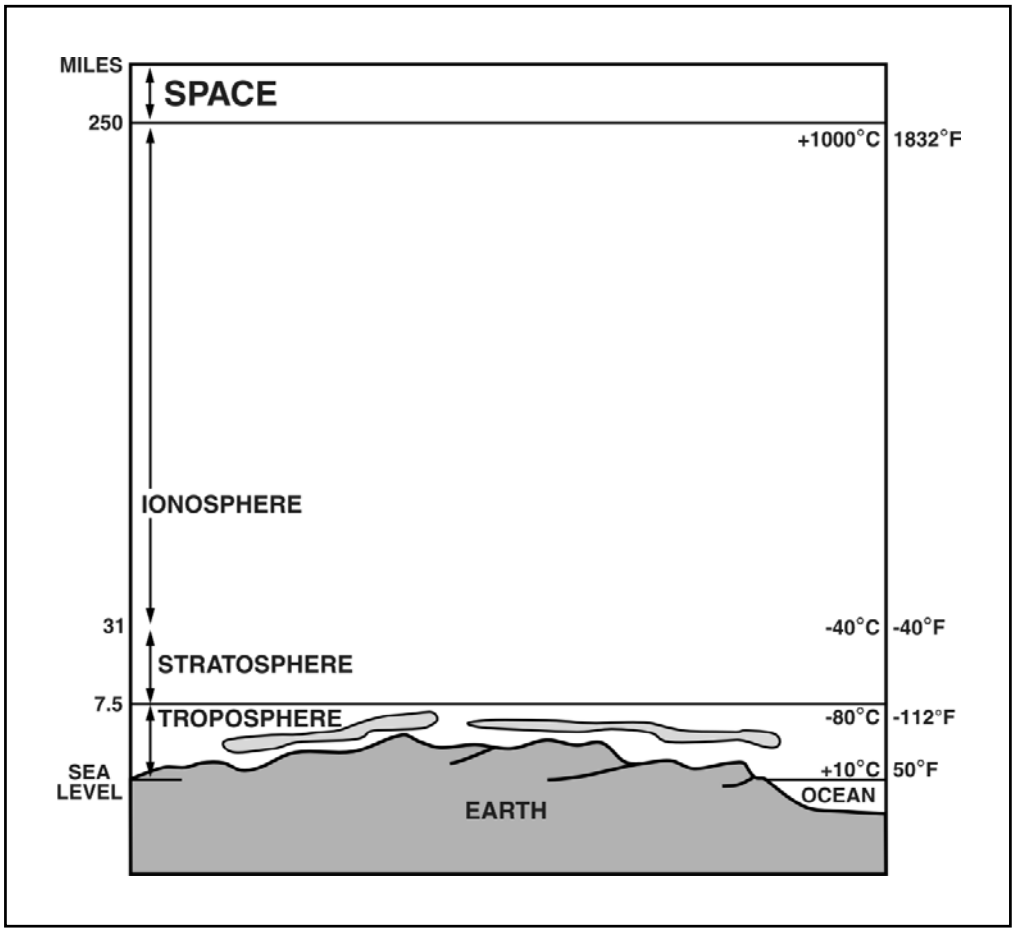


Figure 2-10. Layers of the Earth's Atmosphere

Troposphere

2-46. The troposphere is the portion of the earth's atmosphere that extends from the surface of the earth to a height of about 3.7 miles (6 km) at the North Pole or the South Pole, and 11.2 miles (18 km) at the equator. Virtually all weather phenomena take place in the troposphere. The temperature in this region decreases rapidly with altitude, clouds form, and there may be much turbulence because of variations in temperature, density, and pressure. These conditions have a great effect on the propagation of radio waves, as explained later in this chapter.

Stratosphere

2-47. The stratosphere is located between the troposphere and the ionosphere. The temperature throughout this region is considered to be almost constant and there is little water vapor present. The stratosphere has relatively little effect on radio waves because it is a relatively calm region with little or no temperature changes.

Ionosphere

2-48. The ionosphere extends upward from about 31.1 miles (50 km) to a height of about 250 miles (402 km). It contains four cloud-like layers of electrically charged ions, which enable radio waves to be propagated to great distances around the earth. This is the most important region of the atmosphere for long distance point-to-point communications. This region is discussed in detail later in this chapter.

RADIO WAVE TRANSMISSION PATHS

2-49. There are two principal ways in which electromagnetic (radio) energy travels from a transmitting antenna to a receiving antenna. One way is by ground waves and the other is by sky waves. Ground waves are radio waves that travel near the surface of the earth (surface and space waves). Sky waves are radio waves that are reflected back to Earth from the ionosphere (see figure 2-11).

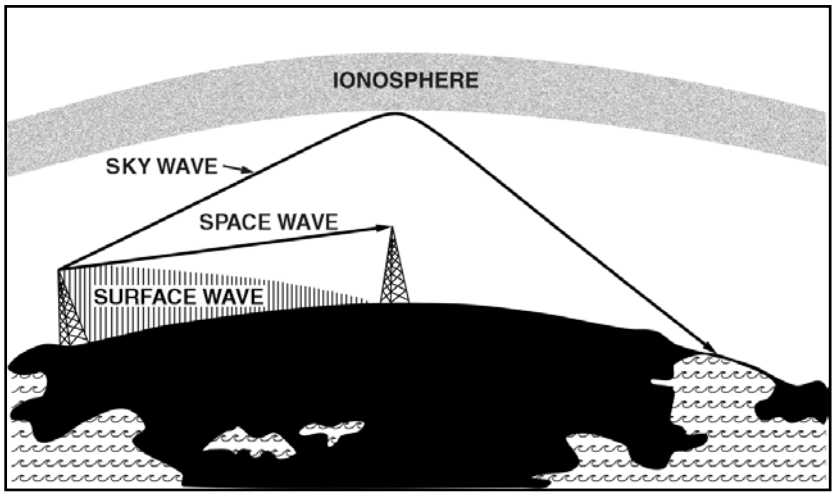


Figure 2-11. Ground Waves and Sky Waves

Ground Waves

2-50. The ground wave is actually composed of two separate component waves. These are known as the surface wave and the space wave (figure 2-11). The determining factor in whether a ground wave component is classified as a space wave or a surface wave is simple. A surface wave travels along the surface of the earth. A space wave travels over the surface.

2-51. **Surface wave**. The surface wave reaches the receiving site by traveling along the surface of the ground as shown in figure 2-12. A surface wave can follow the contours of the earth because of the process of diffraction. When a surface wave meets an object and the dimensions of the object do not exceed its wavelength, the wave tends to curve or bend around the object. The smaller the object, the more pronounced the diffractive action will be.

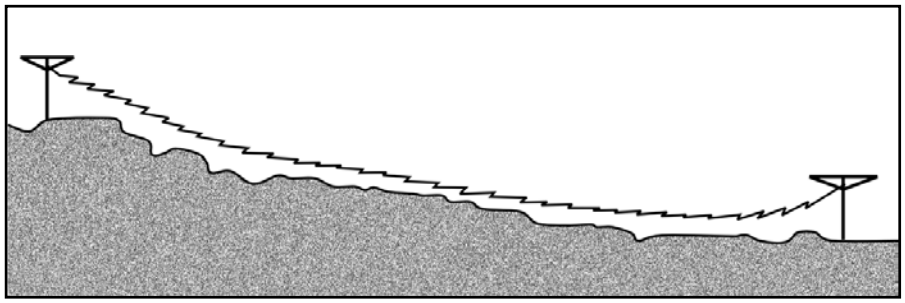


Figure 2-12. Surface Wave Propagation

2-52. As a surface wave passes over the ground, the wave induces a voltage in the earth. The induced voltage takes energy away from the surface wave, thereby weakening, or attenuating, the wave as it moves away from the transmitting antenna. To reduce the attenuation, the amount of induced voltage must be reduced. This is done by using vertically polarized waves that minimize the extent to which the electric field of the wave is in contact with the earth. When a surface wave is horizontally polarized, the electric field of the wave is parallel with the surface of the earth and, therefore, is constantly in contact with it. The wave is then completely attenuated within a short distance from the transmitting site. On the other hand, when the surface wave is vertically polarized, the electric field is perpendicular to the earth and merely dips into and out of the earth's surface. For this reason, vertical polarization is vastly superior to horizontal polarization for surface wave propagation.

2-53. The attenuation that a surface wave undergoes because of induced voltage also depends on the electrical properties of the terrain over which the wave travels. The best type of surface is one that has good electrical conductivity. The better the conductivity, the less the attenuation. Table 2-2 gives the relative conductivity of various Earth surfaces.

Table 2-2. Surface Conductivity

SURFACE	*RELATIVE CONDUCTIVITY*
Sea water	Good
Flat, loamy soil	Fair
Large bodies of fresh water	Fair
Rocky terrain	Poor
Desert	Poor
Jungle	Unusable

2-54. Another major factor in the attenuation of surface waves is frequency. Recall from earlier discussions on wavelength that the higher the frequency of a radio wave, the shorter its wavelength will be. These high frequencies, with their shorter wavelengths, are not normally diffracted but are absorbed by the earth at points relatively close to the transmitting site. You can assume, therefore, that as the frequency of a surface wave is increased, the more rapidly the surface wave will be absorbed, or attenuated, by the earth.

Because of this loss by attenuation, the surface wave is impractical for long-distance transmissions at frequencies above 2 megahertz. On the other hand, when the frequency of a surface wave is low enough to have a very long wavelength, the earth appears to be very small, and diffraction is sufficient for propagation well beyond the horizon. In fact, by lowering the transmitting frequency into the very low frequency (VLF) range and using very high-powered transmitters, the surface wave can be propagated great distances.

2-55. **Space wave**. The space wave follows two distinct paths from the transmitting antenna to the receiving antenna—one through the air directly to the receiving antenna, the other reflected from the ground to the receiving antenna. These paths are illustrated in figure 2-13. The primary or direct path of the space wave is directly from the transmitting antenna to the receiving antenna. So, the receiving antenna must be located within the radio horizon of the transmitting antenna. Because space waves are refracted slightly, even when propagated through the troposphere, the radio horizon is actually about one-third farther than the line-of-sight or natural horizon.

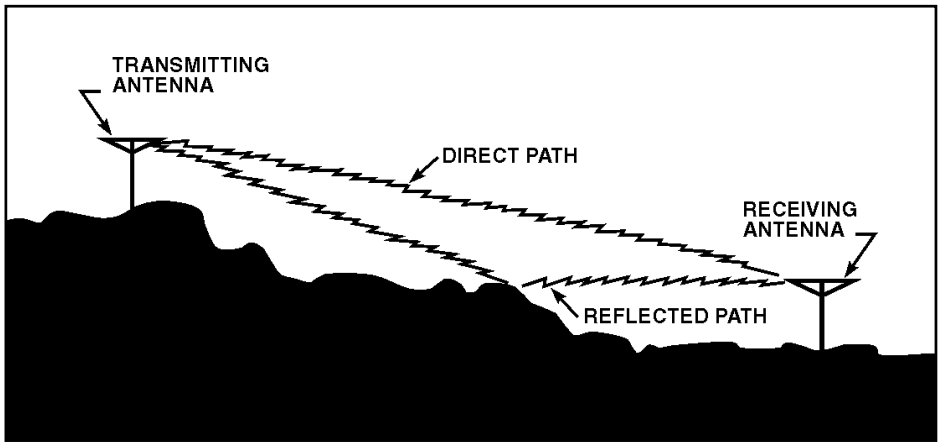


Figure 2-13. Space Wave Propagation

2-56. Although space waves suffer little ground attenuation, they nevertheless are susceptible to fading. This is because space waves actually follow two paths of different lengths (direct path and ground reflected path) to the receiving site and, therefore, may arrive in or out of phase. If these two component waves are received in phase, the result is a reinforced or stronger signal. Likewise, if they are received out of phase, they tend to cancel one another, which results in a weak or fading signal.

Sky Wave

2-57. The sky wave, often called the ionospheric wave, is radiated in an upward direction and returned to Earth at some distant location because of refraction from the ionosphere. This form of propagation is relatively unaffected by the earth's surface and can propagate signals over great distances. Usually the high frequency (HF) band is used for sky wave propagation. The following study of the ionosphere and its effect on sky waves will help you understand the nature of sky wave propagation.

STRUCTURE OF THE IONOSPHERE

2-58. As stated previously, the ionosphere is the region of the atmosphere that extends from about 31.1 miles (50 km) above the surface of the earth to about 250 miles (402 km) above the surface. It is appropriately named the ionosphere because it consists of several layers of electrically charged gas atoms called ions. A process called ionization forms the ions.

Ionization

2-59. Ionization occurs when high-energy ultraviolet light waves from the sun enter the ionospheric region of the atmosphere, strike a gas atom, and literally knock an electron free from its parent atom. A normal atom is electrically neutral because it contains equal numbers of positively charged protons in its nucleus and negatively charged electrons that orbit the nucleus. When an electron is knocked free from the atom, the atom becomes positively charged (called a positive ion) and remains in space along with the free electron, which is negatively charged. This process of upsetting electrical neutrality is known as ionization.

2-60. The free negative electrons subsequently absorb part of the ultraviolet energy, which initially freed them from their atoms. As the ultraviolet light wave continues to produce positive ions and negative electrons, its intensity decreases because of the absorption of energy by the free electrons, and an ionized layer is formed. The rate at which ionization occurs depends on the density of atoms in the atmosphere and the intensity of the ultraviolet light wave, which varies with the activity of the sun.

2-61. Because the atmosphere is bombarded by ultraviolet light waves of different frequencies, several ionized layers are formed at different altitudes. Lower frequency ultraviolet waves penetrate the atmosphere the least; therefore, they produce ionized layers at the higher altitudes. Conversely, ultraviolet waves of higher frequencies penetrate deeper and produce layers at the lower altitudes. An important factor in determining the density of ionized layers is the elevation angle of the sun, which changes frequently. For this reason, the height and thickness of the ionized layers vary, depending on the time of day and even the season of the year.

Recombination

2-62. Recall that the process of ionization involves ultraviolet light waves knocking electrons free from their atoms. A reverse process called recombination occurs when the free electrons and positive ions collide with each other. Because these collisions are inevitable, the positive ions return to their original neutral atom state.

2-63. The recombination process also depends on the time of day. Between the hours of early morning and late afternoon, the rate of ionization exceeds the rate of recombination. During this period, the ionized layers reach their greatest density and exert maximum influence on radio waves. During the late afternoon and early evening hours, however, the rate of recombination exceeds the rate of ionization, and the density of the ionized layers begins to decrease. Throughout the night, density continues to decrease, reaching a low point just before sunrise.

Four Distinct Layers

2-64. The ionosphere is composed of three layers designated D, E, and F, from lowest level to highest level as shown in figure 2-14. The F layer is further divided into two layers designated F1 (the lower layer) and F2 (the higher layer). The presence or absence of these layers in the ionosphere and their height above the earth varies with the position of the sun. At high noon, radiation in the ionosphere directly above a given point is greatest. At night it is minimum. When the radiation is removed, many of the particles that were ionized recombine. The time interval between these conditions finds the position and number of the ionized layers within the ionosphere changing. Because the position of the sun varies daily, monthly, and yearly, with respect to a specified point on the earth, the exact position and number of layers present are extremely difficult to determine. However, the following general statements can be made:

- The D layer ranges from about 30 to 55 miles. Ionization in the D layer is low because it is the lowest region of the ionosphere. This layer has the ability to refract signals of low frequencies. High frequencies pass right through it and are attenuated. After sunset, the D layer disappears because of the rapid recombination of ions.
- The E layer limits are from about 55 to 90 miles. This layer is also known as the Kennelly-Heaviside layer, because these two men were the first to propose its existence. The rate of ionic recombination in this layer is rather rapid after sunset and the layer is almost gone by midnight. This layer has the ability to refract signals as high as 20 megahertz. For this reason, it is valuable for communications in ranges up to about 1500 miles.
- The F layer exists from about 90 to 240 miles. During the daylight hours, the F layer separates into two layers, the F1 and F2 layers. The ionization level in these layers is quite high and varies widely during the day. At noon, this portion of the atmosphere is closest to the sun and the degree of ionization is maximum. Because the atmosphere is rarefied at these heights, recombination occurs slowly after sunset. Therefore, a fairly constant ionized layer is always present. The F layers are responsible for high frequency, long distance transmission.

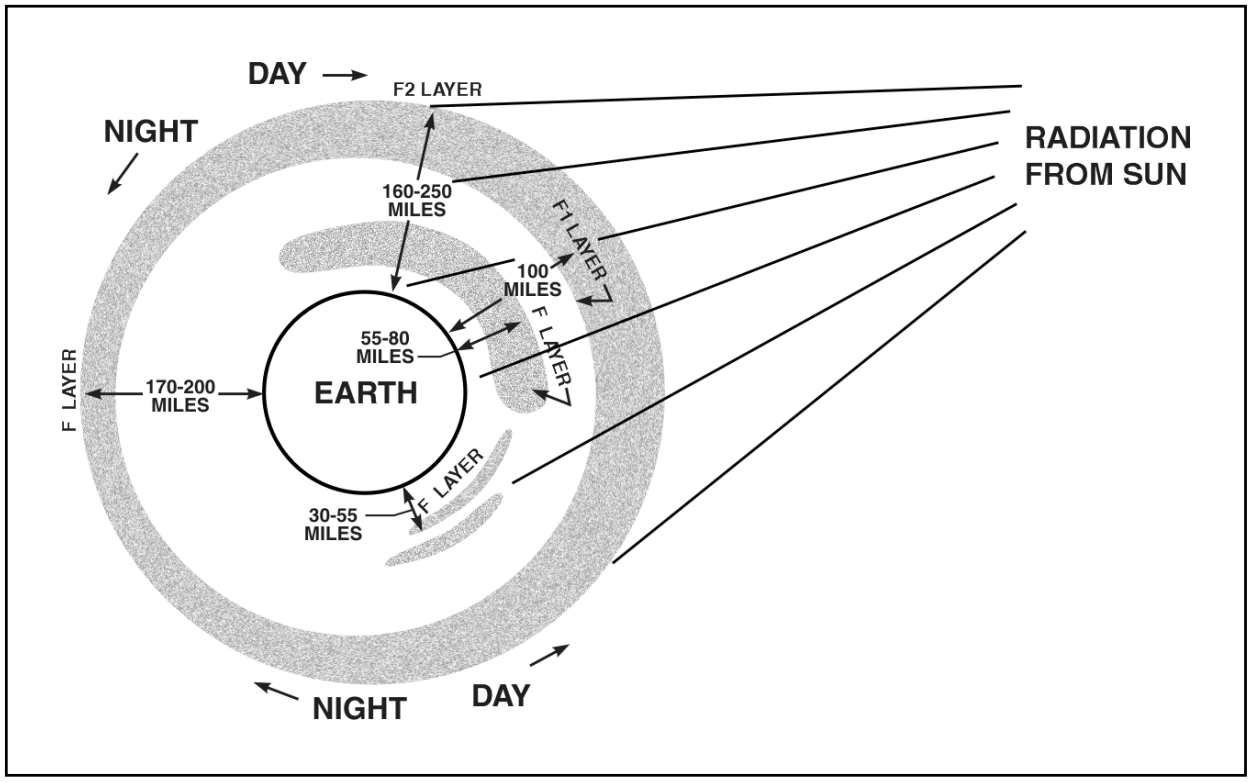


Figure 2-14. Layers of the Ionosphere

REFRACTION IN THE IONOSPHERE

2-65. When a radio wave is transmitted into an ionized layer, refraction, or bending of the wave, occurs. As we discussed earlier, refraction is caused by an abrupt change in the velocity of the upper part of a radio wave as it strikes or enters a new medium. The amount of refraction that occurs depends on three main factors: (1) the density of ionization of the layer, (2) the frequency of the radio wave, and (3) the angle at which the wave enters the layer.

Density of Layer

2-66. Figure 2-15 illustrates the relationship between radio waves and ionization density. Each ionized layer has a central region of relatively dense ionization, which tapers off in intensity both above and below the maximum region. As a radio wave enters a region of increasing ionization, the increase in velocity of the upper part of the wave causes it to be bent back toward the earth. While the wave is in the highly dense center portion of the layer, however, refraction occurs more slowly because the density of ionization is almost uniform. As the wave enters into the upper part of the layer of decreasing ionization, the velocity of the upper part of the wave decreases, and the wave is bent away from the earth. If a wave strikes a thin, very highly ionized layer, the wave may be bent back so rapidly that it appears to have been reflected instead of refracted back to Earth. To reflect a radio wave, the highly ionized layer must be approximately no thicker than one wavelength of the radio wave. Because the ionized layers are often several miles thick, ionospheric reflection is more likely to occur at long wavelengths (low frequencies).

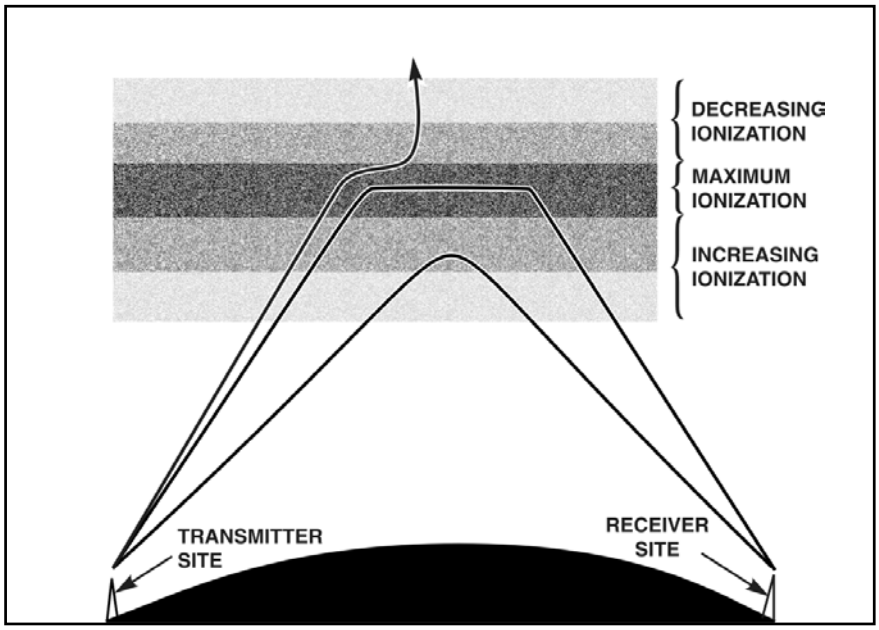


Figure 2-15. Effects of Ionospheric Density on Radio Waves

Frequency

2-67. For any given time, each ionospheric layer has a maximum frequency at which radio waves can be transmitted vertically and refracted back to Earth. This frequency is known as the critical frequency. It is a term that you will hear frequently in any discussion of radio wave propagation. Radio waves transmitted at frequencies higher than the critical frequency of a given layer will pass through the layer and be lost in space; but if these same waves enter an upper layer with a higher critical frequency, they will be refracted back to Earth. Radio waves of frequencies lower than the critical frequency will also be refracted back to Earth unless they are absorbed or have been refracted from a lower layer. The lower the frequency of a radio wave, the more rapidly the wave is refracted by a given degree of ionization. Figure 2-16 shows three separate waves of different frequencies entering an ionospheric layer at the same angle. Notice that the 5-megahertz wave is refracted quite sharply. The 20-megahertz wave is refracted less sharply and returned to Earth at a greater distance. The 100-megahertz wave is obviously greater than the critical frequency for that ionized layer and, therefore, is not refracted but is passed into space.

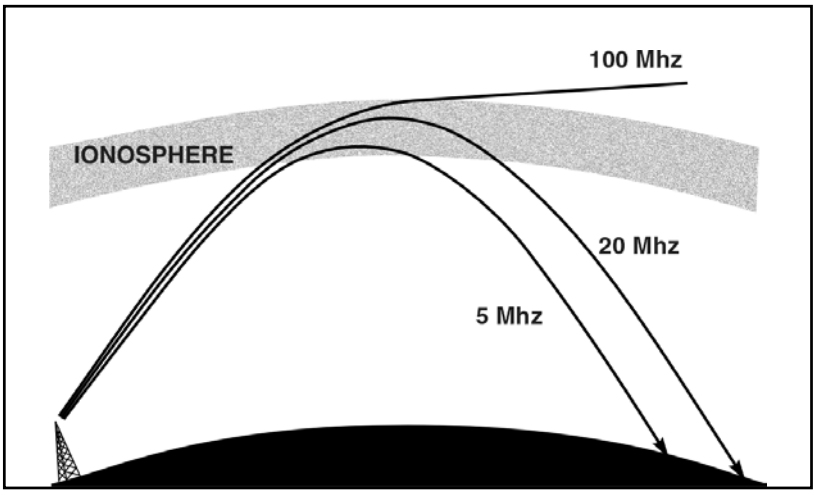


Figure 2-16. Frequency Versus Refraction and Distance

Angle of Incidence

2-68. The rate at which a wave of a given frequency is refracted by an ionized layer depends on the angle at which the wave enters the layer. Figure 2-17 shows three radio waves of the same frequency entering a layer at different angles. The angle at which wave A strikes the layer is too nearly vertical for the wave to be refracted to Earth. As the wave enters the layer, it is bent slightly but passes through the layer and is lost. When the wave is reduced to an angle that is less than vertical (wave B), it strikes the layer and is refracted back to Earth. The angle made by wave B is called the critical angle for that particular frequency. Any wave that leaves the antenna at an angle greater than the critical angle will penetrate the ionospheric layer for that frequency and then be lost in space. Wave C strikes the ionosphere at the smallest angle at which the wave can be refracted and still return to Earth. At any smaller angle, the wave will be refracted but will not return to Earth.

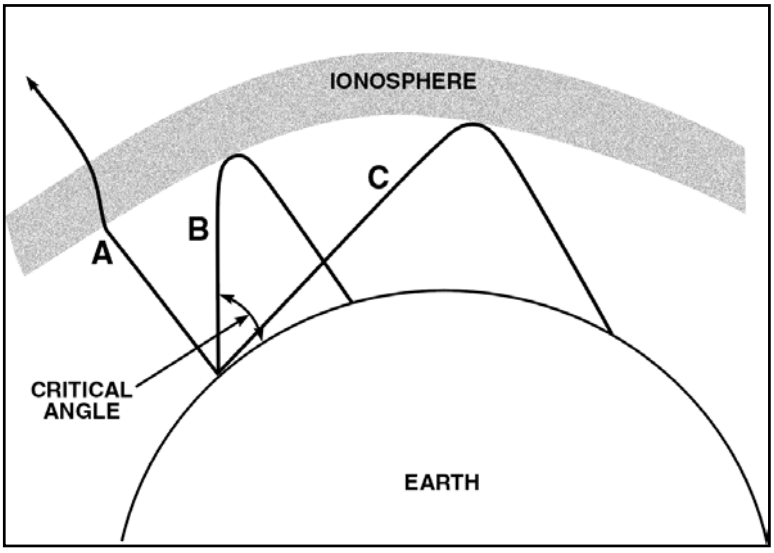


Figure 2-17. Different Incident Angles of Radio Waves

2-69. As the frequency of the radio wave is increased, the critical angle must be reduced for refraction to occur. This point is illustrated in figure 2-18. The 2-megahertz wave strikes the layer at the critical angle for that frequency and is refracted back to Earth. Although the 5-megahertz wave (broken line) strikes the ionosphere at a lesser angle, it nevertheless penetrates the layer and is lost. As the angle is lowered from the vertical, however, a critical angle for the 5-megahertz wave is reached, and the wave is then refracted to Earth.

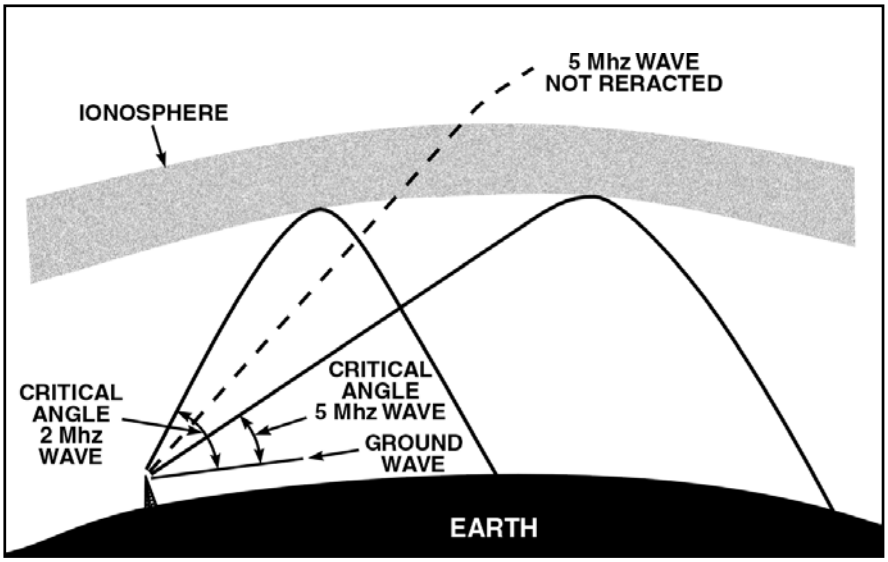


Figure 2-18. Effects of Frequency on the Critical Angle

Skip Distance/Skip Zone

2-70. In figure 2-19, note the relationship between the sky wave skip distance, the skip zone, and the ground wave coverage. The skip distance is the distance from the transmitter to the point where the sky wave is first returned to Earth. The size of the skip distance depends on the frequency of the wave, the angle of incidence, and the degree of ionization present.

2-71. The skip zone is a zone of silence between the point where the ground wave becomes too weak for reception and the point at which the sky wave is first returned to Earth. The size of the skip zone depends on the extent of the ground wave coverage and the skip distance. When the ground wave coverage is great enough or the skip distance is short enough that no zone of silence occurs, there is no skip zone.

2-72. Occasionally, the first sky wave will return to Earth within the range of the ground wave. If the sky wave and ground wave are nearly of equal intensity, the sky wave alternately reinforces and cancels the ground wave, causing severe fading. This fading is caused by the phase difference between the two waves, a result of the longer path traveled by the sky wave.

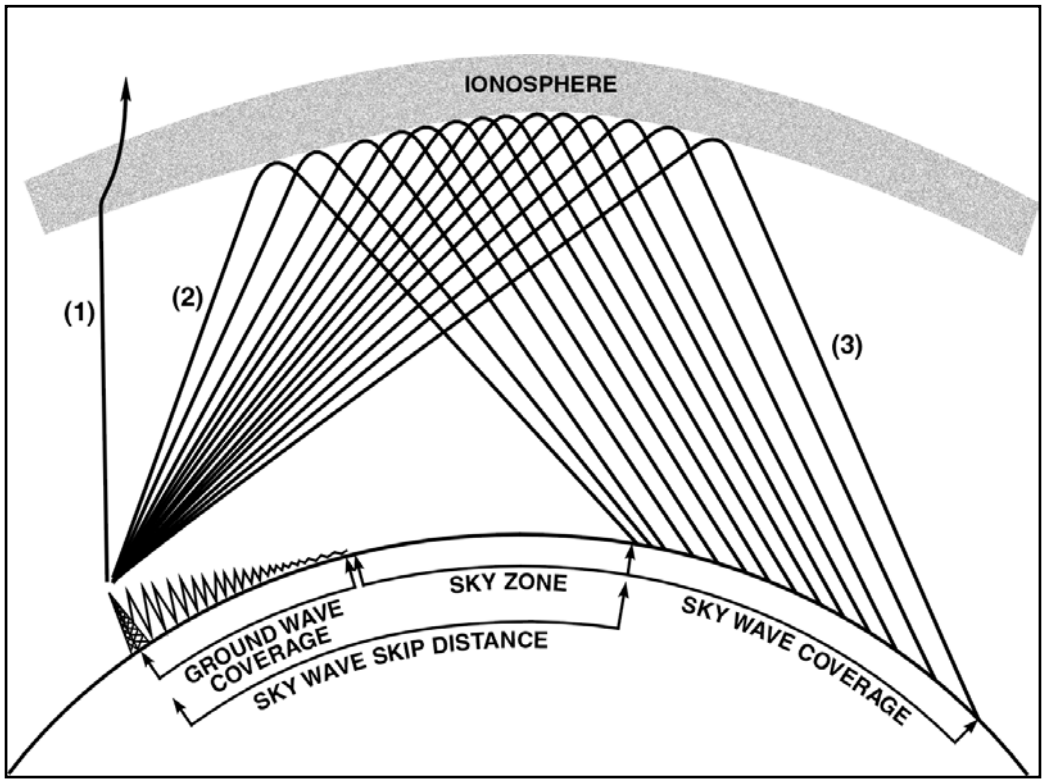


Figure 2-19. Relationship between Skip Zone, Skip Distance, and Ground Wave

Propagation Paths

2-73. The path that a refracted wave follows to the receiver depends on the angle at which the wave strikes the ionosphere. You should remember, however, that the RF energy radiated by a transmitting antenna spreads out with distance. The energy therefore strikes the ionosphere at many different angles rather than a single angle.

2-74. After the RF energy of a given frequency enters an ionospheric region, the paths that this energy might follow are many. It may reach the receiving antenna via two or more paths through a single layer. It may also, reach the receiving antenna over a path involving more than one layer, by multiple hops between the ionosphere and Earth, or by any combination of these paths.

2-75. Figure 2-20 shows how radio waves may reach a receiver via several paths through one layer. The various angles at which RF energy strikes the layer are represented by dark lines and designated as rays 1 through 6.

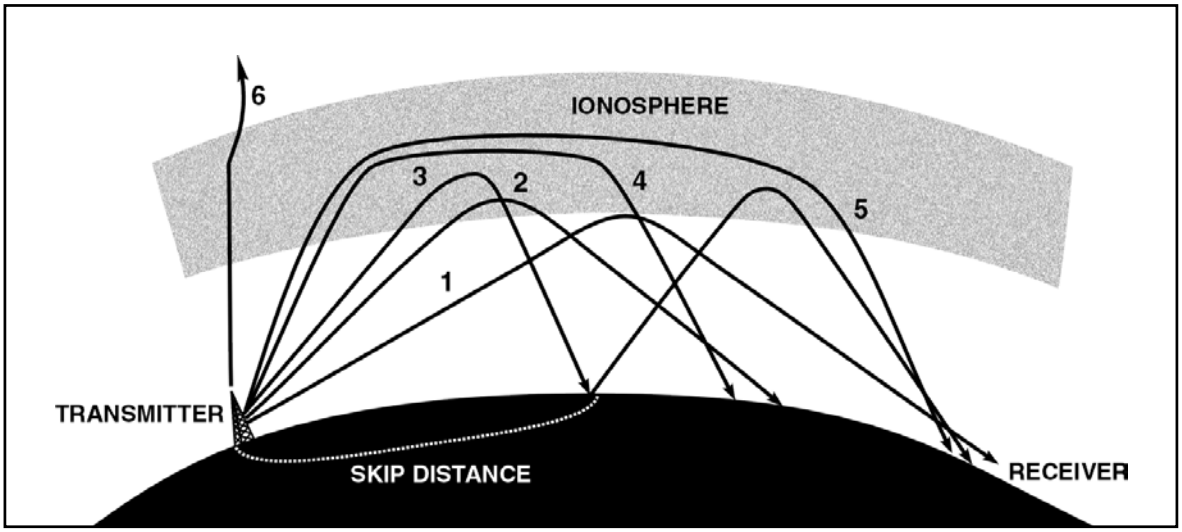


Figure 2-20. Ray Paths for a Fixed Frequency with Varying Angles of Incidence

2-76. When the angle is relatively low with respect to the horizon (ray 1), there is only slight penetration of the layer and the propagation path is long. When the angle of incidence is increased (rays 2 and 3), the rays penetrate deeper into the layer but the range of these rays decreases. When a certain angle is reached (ray 3), the penetration of the layer and rate of refraction are such that the ray is first returned to Earth at a minimal distance from the transmitter. Notice, however, that ray 3 still manages to reach the receiving site on its second refraction (called a hop) from the ionospheric layer.

2-77. As the angle is increased still more (rays 4 and 5), the RF energy penetrates the central area of maximum ionization of the layer. These rays are refracted rather slowly and are eventually returned to Earth at great distances. As the angle approaches vertical incidence (ray 6), the ray is not returned at all, but passes on through the layer.

ABSORPTION IN THE IONOSPHERE

2-78. Many factors affect a radio wave in its path between the transmitting and receiving sites. The factor that has the greatest adverse effect on radio waves is absorption. Absorption results in the loss of energy of a radio wave and has a pronounced effect on both the strength of received signals and the ability to communicate over long distances.

2-79. As discussed previously in the section on ground waves, surface waves suffer most of their absorption losses because of ground-induced voltage. Sky waves, on the other hand, suffer most of their absorption losses because of conditions in the ionosphere. Note that some absorption of sky waves may also occur at lower atmospheric levels because of the presence of water and water vapor. However, this becomes important only at frequencies above 10,000 megahertz.

2-80. Most ionospheric absorption occurs in the lower regions of the ionosphere where ionization density is greatest. As a radio wave passes into the ionosphere, it loses some of its energy to the free electrons and ions. If these high-energy free electrons and ions do not collide with gas molecules of

low energy, most of the energy lost by the radio wave is reconverted into electromagnetic energy, and the wave continues to be propagated with little change in intensity. However, if the high-energy free electrons and ions do collide with other particles, much of this energy is lost, resulting in absorption of the energy from the wave. Because absorption of energy depends on collision of the particles, the greater the density of the ionized layer, the greater the probability of collisions; therefore, the greater the absorption. The highly dense D and E layers provide the greatest absorption of radio waves.

2-81. Because the amount of absorption of the sky wave depends on the density of the ionosphere, which varies with seasonal and daily conditions, it is impossible to express a fixed relationship between distance and signal strength for ionospheric propagation. Under certain conditions, the absorption of energy is so great that communicating over any distance beyond the line of sight is difficult.

FADING

2-82. The most troublesome and frustrating problem in receiving radio signals is variations in signal strength, most commonly known as fading. There are several conditions that can produce fading. When a radio wave is refracted by the ionosphere or reflected from the earth's surface, random changes in the polarization of the wave may occur. Vertically and horizontally mounted receiving antennas are designed to receive vertically and horizontally polarized waves, respectively. Therefore, changes in polarization cause changes in the received signal level because of the inability of the antenna to adjust to the polarization changes.

2-83. Fading also results from absorption of the RF energy in the ionosphere. Absorption fading occurs for a longer period than other types of fading, because absorption takes place slowly. Usually, however, fading on ionospheric circuits is mainly a result of multipath propagation.

Multipath Fading

2-84. Multipath is simply a term used to describe the multiple paths a radio wave may follow between transmitter and receiver. Such propagation paths include the ground wave, ionospheric refraction, reradiation by the ionospheric layers, reflection from the earth's surface or from more than one ionospheric layer, and others. Figure 2-21 shows a few of the paths that a signal can travel between two sites in a typical circuit. One path, XYZ, is the basic ground wave. Another path, XEA, refracts the wave at the E layer and passes it on to the receiver at A. Still another path, XFZFA, results from a greater angle of incidence and two refractions from the F layer. At point Z, the received signal is a combination of the ground wave and the sky wave. These two signals having traveled different paths arrive at point Z at different times. Thus, the arriving waves may or may not be in phase with each other. Radio waves that are received in phase reinforce each other and produce a stronger signal at the receiving site. Conversely, those that are received out of phase produce a weak or fading signal. Small alternations in the transmission path may change the phase relationship of the two signals, causing periodic fading. This condition occurs at point A. At this point, the double-hop F layer signal may be in or out of phase with the signal arriving from the E layer.

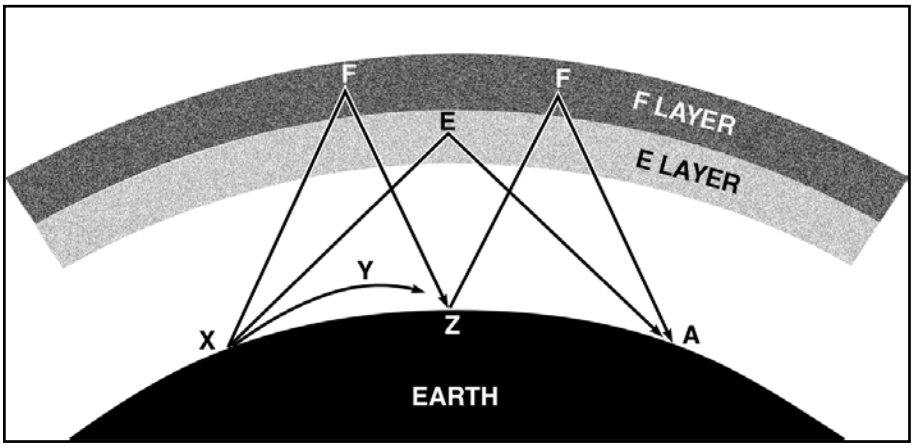


Figure 2-21. Multipath Transmission

2-85. Multipath fading may be minimized by practices called space diversity and frequency diversity. In space diversity, two or more receiving antennas are spaced some distance apart. Fading does not occur simultaneously at both antennas; therefore, enough output is almost always available from one of the antennas to provide a useful signal. In frequency diversity, two transmitters and two receivers are used, each pair tuned to a different frequency, with the same information being transmitted simultaneously over both frequencies. One of the two receivers will almost always provide a useful signal.

Selective Fading

2-86. Fading resulting from multipath propagation varies by frequency because each frequency arrives at the receiving point via a different radio path. When a wide band of frequencies is transmitted simultaneously, each frequency will vary in the amount of fading. This variation is called selective fading. When selective fading occurs, all frequencies of the transmitted signal do not retain their original phases and relative amplitudes. This fading causes severe distortion of the signal and limits the total signal transmitted.

TRANSMISSION LOSSES

2-87. All radio waves propagated over ionospheric paths undergo energy losses before arriving at the receiving site. As discussed earlier, absorption in the ionosphere and lower atmospheric levels account for a large part of these energy losses. There are two other types of losses that also significantly affect the ionospheric propagation of radio waves. These losses are known as ground reflection loss and freespace loss. The combined effects of absorption, ground reflection loss, and freespace loss account for most of the energy losses of radio transmissions propagated by the ionosphere.

Ground Reflection Loss

2-88. When propagation is accomplished via multihop refraction, RF energy is lost each time the radio wave is reflected from the earth's surface. The amount of energy lost depends on the frequency of the wave, the angle of incidence, ground irregularities, and the electrical conductivity of the point of reflection.

Freespace Loss

2-89. Normally, the major loss of energy is because of the spreading out of the wavefront as it travels away from the transmitter. As the distance increases, the area of the wavefront spreads out, much like the beam of a flashlight. This means the amount of energy contained within any unit of area on the wavefront decreases as distance increases. By the time the energy arrives at the receiving antenna, the wavefront is so spread out that the receiving antenna extends into only a very small fraction of the wavefront, as illustrated in figure 2-22.

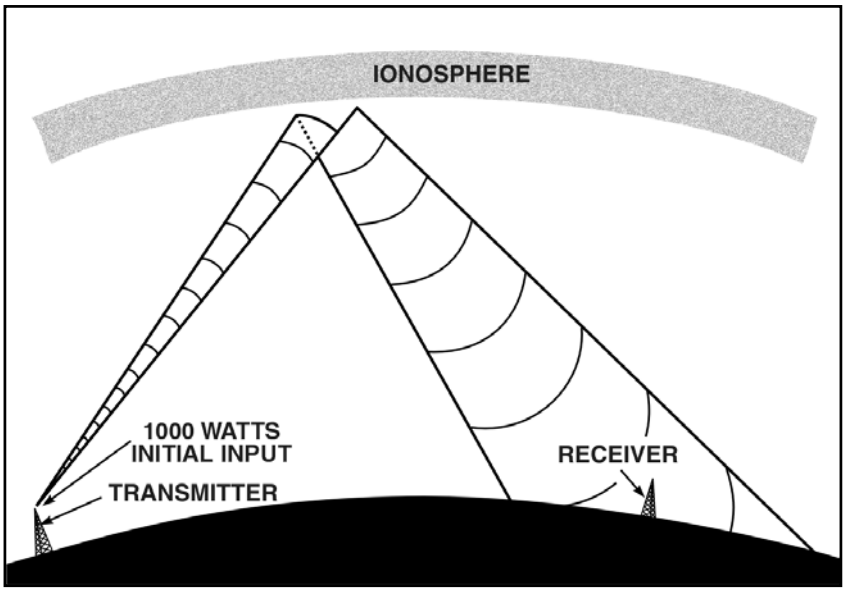


Figure 2-22. Freespace Loss Principle

ELECTROMAGNETIC INTERFERENCE (EMI)

2-90. The transmission losses just discussed are not the only factors that interfere with communications. An additional factor that can interfere with radio communications is the presence of electromagnetic interference (EMI). This interference can result in annoying or impossible operating conditions. Sources of EMI are both man-made and natural.

Man-Made Interference

2-91. Man-made interference may come from several sources. Some of these sources, such as oscillators, communications transmitters, and radio transmitters, may be specifically designed to generate radio frequency energy. Some electrical devices also generate radio frequency energy, although they are not specifically designed for this purpose. Examples are ignition systems, generators, motors, switches, relays, and voltage regulators. The intensity of man-made interference may vary throughout the day and drop off to a low level at night when many of these sources are not being used. Man-made interference may be a critical limiting factor at radio receiving sites located near industrial areas.

Natural Interference

2-92. Natural interference refers to the static that you often hear when listening to a radio. This interference is generated by natural phenomena, such as thunderstorms, snowstorms, cosmic sources, and the sun. The energy released by these sources is transmitted to the receiving site in roughly the same manner as radio waves. As a result, when ionospheric conditions are favorable for the long distance propagation of radio waves, they are likewise favorable for the propagation of natural interference. Natural interference is very erratic, particularly in the HF band, but generally decreases as the operating frequency is increased and wider bandwidths are used. There is little natural interference above 30 megahertz.

Control of EMI

2-93. Electromagnetic interference can be reduced or eliminated by using various suppression techniques. The amount of EMI that is produced by a radio transmitter can be controlled by cutting transmitting antennas to the correct frequency, limiting bandwidth, and using electronic filtering networks and metallic shielding.

2-94. Radiated EMI during transmission can be controlled by the physical separation of the transmitting and receiving antennas, the use of directional antennas, and limiting antenna bandwidth.

VARIATIONS IN THE IONOSPHERE

2-95. Because the existence of the ionosphere is directly related to radiations emitted from the sun, the movement of the earth about the sun or changes in the sun's activity will result in variations in the ionosphere. These variations are of two general types:

- Those that are more or less regular and occur in cycles and, therefore, can be predicted in advance with reasonable accuracy.
- Those that are irregular as a result of abnormal behavior of the sun and, therefore, cannot be predicted in advance. Both regular and irregular variations have important effects on radio wave propagation.

Regular Variations

2-96. The regular variations that affect the extent of ionization in the ionosphere can be divided into four main classes: daily, seasonal, 11-year, and 27-day variations.

2-97. **Daily**. Daily variations in the ionosphere are a result of the 24-hour rotation of the earth about its axis. Daily variations of the different layers (figure 2-14) are summarized as follows:

- The D layer reflects VLF waves, is important for long range VLF communications, refracts LF and MF waves for short-range communications, absorbs HF waves, has little effect on VHF and above, and disappears at night.
- In the E layer, ionization depends on the angle of the sun. The E layer refracts HF waves during the day up to 20 megahertz to distances of about 1200 miles. Ionization is greatly reduced at night.

- The structure and density of the F region depend on the time of day and the angle of the sun. This region consists of one layer during the night and splits into two layers during daylight hours.
- Ionization density of the F1 layer depends on the angle of the sun. Its main effect is to absorb HF waves passing through to the F2 layer.
- The F2 layer is the most important layer for long distance HF communications. It is a particularly variable layer and its height and density change with time of day, season, and sunspot activity.

2-98. **Seasonal**. Seasonal variations are the result of the earth revolving around the sun; the relative position of the sun moves from one hemisphere to the other with changes in seasons. Seasonal variations of the D, E, and F1 layers correspond to the highest angle of the sun; thus the ionization density of these layers is greatest during the summer. The F2 layer, however, does not follow this pattern; its ionization is greatest in winter and least in summer, the reverse of what might be expected. As a result, operating frequencies for F2 layer propagation are higher in the winter than in the summer.

2-99. **Eleven-year sunspot cycle**. One of the most notable phenomena on the surface of the sun is the appearance and disappearance of dark, irregularly shaped areas known as sunspots. The exact nature of sunspots is not known, but scientists believe they are caused by violent eruptions on the sun and are characterized by unusually strong magnetic fields. These sunspots are responsible for variations in the ionization level of the ionosphere. Sunspots can, of course, occur unexpectedly, and the life span of individual sunspots is variable; however, a regular cycle of sunspot activity has also been observed. This cycle has both a minimum and maximum level of sunspot activity that occurs approximately every 11 years.

2-100. During periods of maximum sunspot activity, the ionization density of all layers increases. Because of this, absorption in the D layer increases and the critical frequencies for the E, F1, and F2 layers are higher. At these times, higher operating frequencies must be used for long distance communications.

2-101. **27-Day sunspot cycle**. The number of sunspots in existence at any one time is continually subject to change as some disappear and new ones emerge. As the sun rotates on its own axis, these sunspots are visible at 27-day intervals, the approximate period required for the sun to make one complete rotation.

2-102. The 27-day sunspot cycle causes variations in the ionization density of the layers on a day-to-day basis. The fluctuations in the F2 layer are greater than for any other layer. For this reason, precise predictions on a day-to-day basis of the critical frequency of the F2 layer are not possible. In calculating frequencies for long-distance communications, one must make allowances for the fluctuations of the F2 layer.

Irregular Variations

2-103. Irregular variations in ionospheric conditions also have an important effect on radio wave propagation. Because these variations are irregular and unpredictable, they can drastically affect communications capabilities without any warning. The more common irregular variations are sporadic E, sudden ionospheric disturbances, and ionospheric storms.

2-104. **Sporadic E**. Irregular cloud-like patches of unusually high ionization, called sporadic E, often form at heights near the normal E layer. Exactly what causes this phenomenon is not known, nor can its occurrence be predicted. It is known to vary significantly with latitude, and in the northern latitudes, it appears to be closely related to the aurora borealis or northern lights.

2-105. At times the sporadic E is so thin that radio waves penetrate it easily and are returned to earth by the upper layers. At other times, it extends up to several hundred miles and is heavily ionized.

2-106. These characteristics may be either harmful or helpful to radio wave propagation. For example, sporadic E may blank out the use of higher, more favorable ionospheric layers or cause additional absorption of the radio wave at some frequencies. Also, it can cause additional multipath problems and delay the arrival times of the rays of RF energy.

2-107. On the other hand, the critical frequency of the sporadic E is very high and can be greater than double the critical frequency of the normal ionospheric layers. This condition may permit the long distance transmission of signals at unusually high frequencies. It may also permit short distance communications to locations that would normally be in the skip zone.

2-108. The sporadic E can form and disappear in a short time during either the day or night. However, it usually does not occur at the same time at all transmitting or receiving stations.

2-109. **Sudden ionospheric disturbances**. The most startling of the ionospheric irregularities is known as a sudden ionospheric disturbance (SID). These disturbances may occur without warning and may prevail for any length of time, from a few minutes to several hours. When SID occurs, long distance propagation of HF radio waves is almost totally "blanked out." The immediate effect is that radio operators listening on normal frequencies are inclined to believe that their receivers have gone dead.

2-110. When SID has occurred, examination of the sun has revealed a bright solar eruption. All stations lying wholly, or in part, on the sunward side of the earth are affected. The solar eruption produces an unusually intense burst of ultraviolet light, which is not absorbed by the F2, F1, and E layers, but instead causes a sudden abnormal increase in the ionization density of the D layer. As a result, frequencies above 1 or 2 megahertz are unable to penetrate the D layer and are usually completely absorbed by the layer.

2-111. **Ionospheric storms**. Ionospheric storms are disturbances in the earth's magnetic field. They are associated, in a manner not fully understood, with both solar eruptions and the 27-day intervals, thus corresponding to the rotation of the sun.

2-112. Scientists believe that ionospheric storms result from particle radiation from the sun. Particles radiated from a solar eruption have a slower velocity than ultraviolet light waves produced by the eruption. This would account for the 18-hour or so time difference between a SID and an ionospheric storm. An ionospheric storm that is associated with sunspot activity may begin anytime from 2 days before an active sunspot crosses the central meridian of the sun until four days after it passes the central meridian. At times, however, active sunspots have crossed the central region of the sun without any ionospheric storms occurring. Conversely, ionospheric

storms have occurred when there were no visible spots on the sun and no preceding SID. As you can see, some correlation between ionospheric storms, SID, and sunspot activity is possible, but there are no hard and fast rules. Ionospheric storms can occur suddenly without warning.

2-113. The most prominent effects of ionospheric storms are a turbulent ionosphere and very erratic sky wave propagation. Critical frequencies are lower than normal, particularly for the F2 layer. Ionospheric storms affect the higher F2 layer first, reducing its ion density. Lower layers are not appreciably affected by the storms unless the disturbance is great. The practical effect of ionospheric storms is that the range of frequencies that can be used for communications on a given circuit is much smaller than normal and communications are possible only at the lower working frequencies.

FREQUENCY SELECTION CONSIDERATIONS

2-114. Up to this point, we have covered various factors that control the propagation of radio waves through the ionosphere, such as the structure of the ionosphere, the incidence angle of radio waves, and operating frequencies. There is a very good reason for studying radio wave propagation. One must have a thorough knowledge of radio wave propagation to exercise good judgment when selecting transmitting and receiving antennas and operating frequencies. Selection of a suitable operating frequency (within the bounds of frequency allocations and availability) is of prime importance in maintaining reliable communications.

Note. For successful communications between any two specified locations at any given time of the day, there is a maximum frequency, a lowest frequency, and an optimum frequency that can be used.

Maximum Usable Frequency

2-115. As discussed earlier, the higher the frequency of a radio wave, the lower the rate of refraction by an ionized layer. Therefore, for a given angle of incidence and time of day, there is a maximum frequency that can be used for communications between two given locations. This frequency is known as the maximum usable frequency (MUF).

2-116. Waves at frequencies above the MUF are normally refracted so slowly that they return to Earth beyond the desired location, or pass on through the ionosphere and are lost. You should understand, however, that use of an established MUF certainly does not guarantee successful communications between a transmitting site and a receiving site. Variations in the ionosphere may occur at any time and consequently raise or lower the predetermined MUF. This is particularly true for radio waves being refracted by the highly variable F2 layer. The MUF is highest around noon when ultraviolet light waves from the sun are the most intense. It then drops rather sharply as recombination begins to take place.

Lowest Usable Frequency

2-117. As there is a maximum operating frequency that can be used for communications between two points, there is also a minimum operating frequency. This is known as the lowest usable frequency (LUF). As the frequency of a radio wave is lowered, the rate of refraction increases. So a

wave whose frequency is below the established LUF is refracted back to Earth at a shorter distance than desired, as shown in figure 2-23.

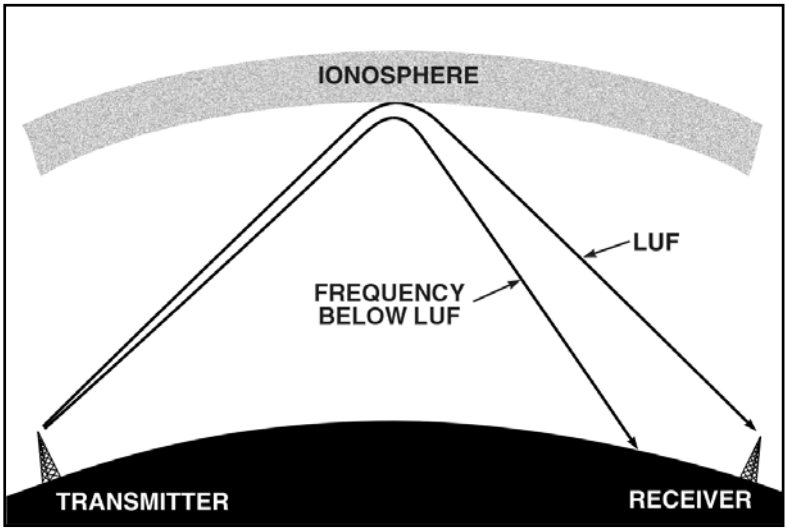


Figure 2-23. Refraction of Frequency below the Lowest Usable Frequency (LUF)

2-118. The transmission path that results from the rate of refraction is not the only factor that determines the LUF. As a frequency is lowered, absorption of the radio wave increases. A wave whose frequency is too low is absorbed to such an extent that it is too weak for reception. Likewise, atmospheric noise is greater at lower frequencies; thus, a low-frequency radio wave may have an unacceptable signal-to-noise ratio.

2-119. For a given angle of incidence and set of ionospheric conditions, the LUF for successful communications between two locations depends on the refraction properties of the ionosphere, absorption considerations, and the amount of atmospheric noise present.

Optimum Working Frequency

2-120. Neither the MUF nor the LUF is a practical operating frequency. While radio waves at the LUF can be refracted back to Earth at the desired location, the signal-to-noise ratio is still much lower than at the higher frequencies, and the probability of multipath propagation is much greater. Operating at or near the MUF can result in frequent signal fading and dropouts when ionospheric variations alter the length of the transmission path.

2-121. The most practical operating frequency is one that you can rely on with the least amount of problems. It should be high enough to avoid the problems of multipath propagation, absorption, and noise encountered at the lower frequencies; but not so high as to result in the adverse effects of rapid changes in the ionosphere.

2-122. A frequency that meets the above criteria has been established and is known as the optimum working frequency. It is abbreviated "FOT" from the initial letters of the French words for optimum working frequency, "frequence optimum de travail." The FOT is roughly about 85 percent of the MUF but the actual percentage varies and may be either considerably more or less than 85 percent.

EFFECTS OF WEATHER ON PROPAGATION

2-123. Weather is an additional factor that affects the propagation of radio waves. In this section, we explain how and to what extent the various weather phenomena affect wave propagation.

2-124. Wind, air temperature, and the water content of the atmosphere can combine in many ways. Certain combinations can cause radio signals to be heard hundreds of miles beyond the ordinary range of radio communications. Conversely, a different combination of factors can cause such attenuation of the signal that it may not be heard even over a normally satisfactory path. Unfortunately, there are no hard and fast rules on the effects of weather on radio transmissions because the weather is extremely complex and subject to frequent change. Therefore, we limit our discussion on the effects of weather on radio waves to general terms.

Precipitation Attenuation

2-125. Calculating the effect of weather on radio wave propagation would be comparatively simple if there were no water or water vapor in the atmosphere. However, some form of water (vapor, liquid, or solid) is always present and must be considered in all calculations. Before we begin discussing the specific effects that individual forms of precipitation (rain, snow, and fog) have on radio waves, you should understand that attenuation because of precipitation is generally proportionate to the frequency and wavelength of the radio wave. For example, rain has a pronounced effect on waves at microwave frequencies. However, rain hardly affects waves with long wavelengths (HF range and below). You can assume, then, that as the wavelength becomes shorter with increases in frequency, precipitation has an increasingly important attenuation effect on radio waves. Conversely, you can assume that as the wavelength becomes longer with decreases in frequency, precipitation has little attenuation effect.

2-126. **Rain**. Attenuation because of raindrops is greater than attenuation because of other forms of precipitation. Attenuation may be caused by absorption, in which the raindrop, acting as a poor dielectric, absorbs power from the radio wave and dissipates the power by heat loss or by scattering (figure 2-24). Raindrops cause greater attenuation by scattering than by absorption at frequencies above 100 megahertz. At frequencies above 6 gigahertz, attenuation by raindrop scatter is even greater.

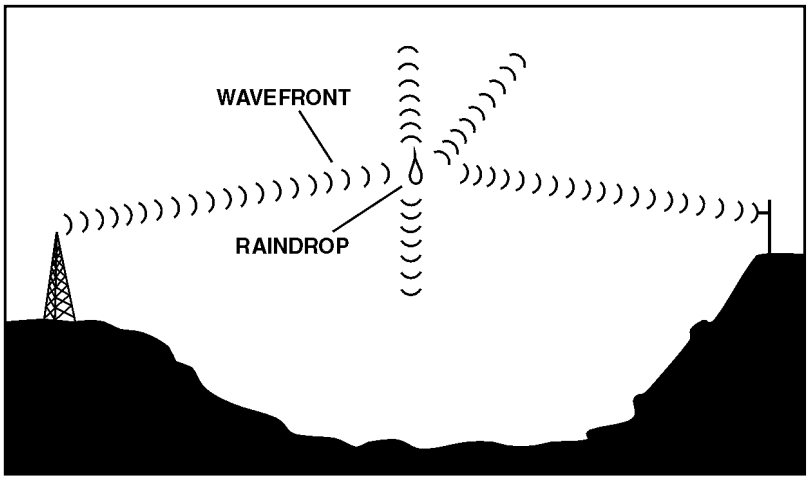


Figure 2-24. RF Energy Losses from Scattering

2-127. **Fog**. In the discussion of attenuation, fog may be considered as another form of rain. Because fog remains suspended in the atmosphere, the attenuation is determined by the quantity of water per unit volume and by the size of the droplets. Attenuation because of fog is of minor importance at frequencies lower than 2 gigahertz. However, fog can cause serious attenuation by absorption at frequencies above 2 gigahertz.

2-128. **Snow**. The scattering effect because of snow is difficult to compute because of irregular sizes and shapes of the flakes. While information on the attenuating effect of snow is limited, scientists assume that attenuation from snow is less than from rain falling at an equal rate. This assumption is borne out by the fact that the density of rain is eight times the density of snow. As a result, rain falling at 1 inch per hour would have more water per cubic inch than snow falling at the same rate.

2-129. **Hail**. Attenuation by hail is determined by the size of the stones and their density. Attenuation of radio waves by scattering because of hailstones is considerably less than by rain.

Temperature Inversion

2-130. Under normal atmospheric conditions, the warmest air is found near the surface of the earth. The air gradually becomes cooler as altitude increases. At times, however, an unusual situation develops in which layers of warm air are formed above layers of cool air. This condition is known as temperature inversion. These temperature inversions cause channels, or ducts, of cool air to be sandwiched between the surface of the earth and a layer of warm air, or between two layers of warm air.

2-131. If a transmitting antenna extends into such a duct of cool air, or if the radio wave enters the duct at a very low angle of incidence, VHF and UHF transmissions may be propagated far beyond normal line-of-sight distances. When ducts are present as a result of temperature inversions, good reception of VHF and UHF television signals from a station located hundreds of miles away is not unusual. These long distances are possible because of the different densities and refractive qualities of warm and cool air. The sudden

change in density when a radio wave enters the warm air above a duct causes the wave to be refracted back toward Earth. When the wave strikes the earth or a warm layer below the duct, it is again reflected or refracted upward and proceeds on through the duct with a multiple-hop type of action. An example of the propagation of radio waves by ducting is shown in figure 2-25.

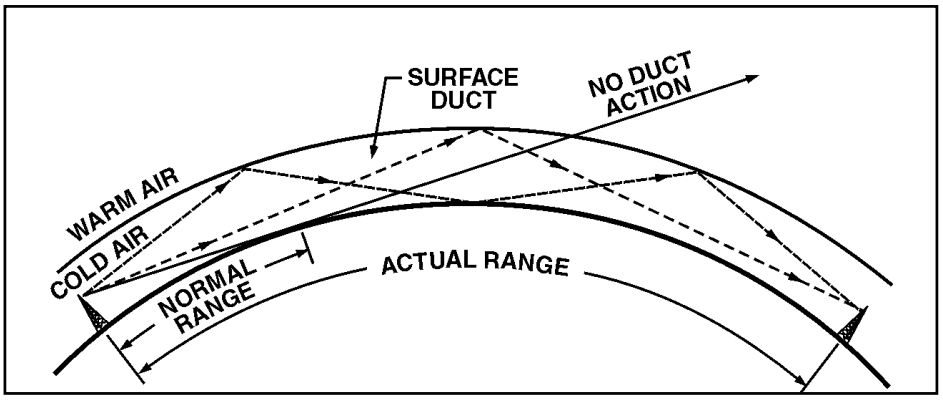


Figure 2-25. Duct Effect Caused by Temperature Inversion

TROPOSPHERIC PROPAGATION

2-132. As the lowest region of the earth's atmosphere, the troposphere extends from the earth's surface to a height of slightly over 7 miles. Virtually all weather phenomena occur in this region. Generally, the troposphere is characterized by a steady decrease in both temperature and pressure as height is increased. However, the many changes in weather phenomena cause variations in humidity and an uneven heating of the earth's surface. As a result, the air in the troposphere is in constant motion. This motion causes small turbulences, or eddies, to be formed, as shown by the bouncing of aircraft entering turbulent areas of the atmosphere. These turbulences are most intense near the earth's surface and gradually diminish with height. They have a refractive quality that permits the refracting or scattering of radio waves with short wavelengths. This scattering provides enhanced communications at higher frequencies.

2-133. Recall that in the relationship between frequency and wavelength, wavelength decreases as frequency increases and vice versa. Radio waves of frequencies below 30 megahertz normally have wavelengths longer than the size of weather turbulences. These radio waves are, therefore, affected very little by the turbulences. On the other hand, as the frequency increases into the VHF range and above, the wavelengths decrease in size, to the point that they become subject to tropospheric scattering. The usable frequency range for tropospheric scattering is from about 100 megahertz to 10 gigahertz.

Tropospheric Scattering

2-134. When a radio wave passing through the troposphere meets turbulence, it makes an abrupt change in velocity. This causes a small amount of the energy to be scattered in a forward direction and returned to Earth at distances beyond the horizon. This phenomenon is repeated as the radio wave meets other turbulences in its path. The total received signal is an accumulation of the energy received from each of the turbulences.

2-135. This scattering mode of propagation enables VHF and UHF signals to be transmitted far beyond the normal line-of-sight. To understand how these signals are transmitted over greater distances, you must first consider the propagation characteristics of the space wave used in VHF and UHF line-of-sight communications. When the space wave is transmitted, it undergoes very little attenuation within the line-of-sight horizon. When it reaches the horizon, the wave is diffracted and follows the earth's curvature. Beyond the horizon, the rate of attenuation increases very rapidly and signals soon become very weak and unusable.

2-136. Tropospheric scattering, on the other hand, provides a usable signal at distances beyond the point where the diffracted space wave drops to an unusable level. This is because of the height at which scattering takes place. The turbulence that causes the scattering can be visualized as a relay station located above the horizon; it receives the transmitted energy and then reradiates it in a forward direction to some point beyond the line-of-sight distance. A high gain-receiving antenna aimed toward this scattered energy can then capture it.

2-137. The magnitude of the received signal depends on the number of turbulences causing scatter in the desired direction and the gain of the receiving antenna. The scatter area used for tropospheric scatter is known as the scatter volume. The angle at which the receiving antenna must be aimed to capture the scattered energy is called the scatter angle. The scatter volume and scatter angles are shown in figure 2-26.

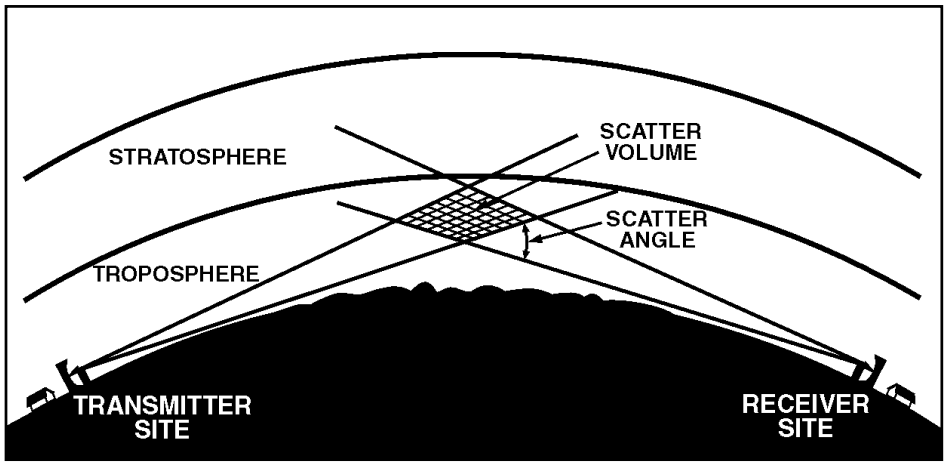


Figure 2-26. Tropospheric Scattering Propagation

2-138. The signal take-off angle (transmitting antenna's angle of radiation) determines the height of the scatter volume and the size of the scatter angle. A low signal take-off angle produces a low scatter volume, which in turn permits a receiving antenna that is aimed at a low angle to the scatter volume to capture the scattered energy.

2-139. As the signal take-off angle is increased, the height of the scatter volume is increased. When this occurs, the amount of received energy decreases. There are two reasons for this: (1) the scatter angle increases as the height of the scatter volume is increased; (2) the amount of turbulence

decreases with height. As the distance between the transmitting and receiving antennas is increased, the height of the scatter volume must also be increased. The received signal level, therefore, decreases as circuit distance is increased.

2-140. The tropospheric region that contributes most strongly to tropospheric scatter propagation lies near the midpoint between the transmitting and receiving antennas and just above the radio horizon of the antennas.

2-141. Because tropospheric scatter depends on turbulence in the atmosphere, changes in atmospheric conditions have an effect on the strength of the received signal. Both daily and seasonal variations in signal strength occur as a result of changes in the atmosphere. These variations are called long-term fading.

2-142. In addition to long-term fading, the tropospheric scatter signal often is characterized by very rapid fading because of multipath propagation. Because the turbulent condition is constantly changing, the path lengths and individual signal levels are also changing, resulting in a rapidly changing signal. Although the signal level of the received signal is constantly changing, the average signal level is stable; therefore, no complete fade-out occurs.

2-143. Another characteristic of a tropospheric scatter signal is its relatively low power level. Because very little of the scattered energy is reradiated toward the receiver, the efficiency is very low and the signal level at the final receiver point is low. Initial input power must be high to compensate for the low efficiency in the scatter volume. This is accomplished by using high-power transmitters and high-gain antennas, which concentrate the transmitted power into a beam, thus increasing the intensity of energy of each turbulence in the volume. The receiver must also be very sensitive to detect the low-level signals.

Application of Tropospheric Scattering

2-144. Tropospheric scatter propagation is used for point-to-point communications. A correctly designed tropospheric scatter circuit will provide highly reliable service for distances ranging from 50 miles to 500 miles. Tropospheric scatter systems may be particularly useful for communications to locations in rugged terrain that are difficult to reach with other methods of propagation. One reason for this is that the tropospheric scatter circuit is not affected by ionospheric and auroral disturbances.

SUMMARY

Now that you have completed this chapter, let us review some of the new terms, concepts, and ideas that you have learned. You should have a thorough understanding of these principles before moving on to chapter 3.

The induction field contains an E field and an H field and is localized near the antenna. The E and H fields of the induction field are 90 degrees out of phase with each other.

The radiation field contains E and H fields that are propagated from the antenna into space in the form of electromagnetic waves. The E and H fields of the radiation field are in phase with each other.

A harmonic frequency is any frequency that is a whole number multiple of a smaller basic frequency. For example, a radio wave transmitted at a fundamental frequency of 3000 hertz can have a second harmonic of 6000 hertz, a third harmonic frequency of 9000 hertz, and so on, transmitted at the same time.

A vertically polarized antenna transmits an electromagnetic wave with the E field perpendicular to the earth's surface. A horizontally polarized antenna transmits a radio wave with the E field parallel to the earth's surface.

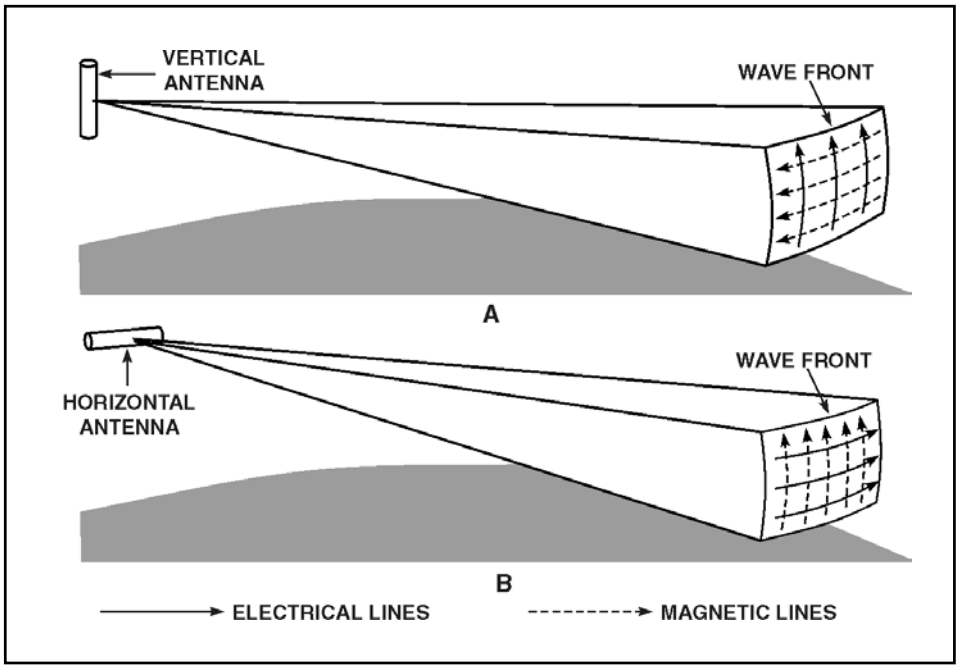


Figure 2-Sum 1. Vertical and Horizontal Polarization

A wavefront is a small section of an expanding sphere of radiated energy and is perpendicular to the direction of travel from the antenna.

Radio waves are electromagnetic waves that can be reflected, refracted, and diffracted in the atmosphere in the same manner as light and heat waves.

Reflected radio waves are waves that have been reflected from a surface and are 180 degrees out of phase with the initial wave.

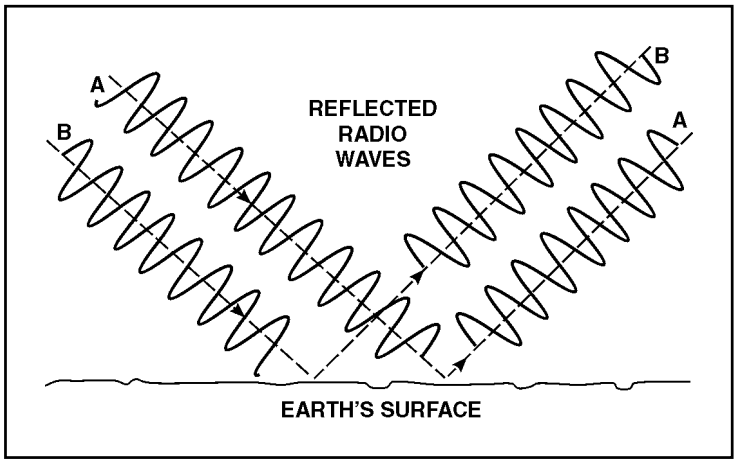


Figure 2-Sum 2. Phase Shift of Reflected Radio Waves

The earth's atmosphere is divided into three separate layers: the troposphere, the stratosphere, and the ionosphere.

The troposphere is the region of the atmosphere where virtually all weather phenomena take place. In this region, RF energy is greatly affected.

The stratosphere has a constant temperature and has little effect on radio waves.

The ionosphere contains four cloud-like layers of electrically charged ions, which aid in long distance communications.

Ground waves and sky waves are the two basic types of radio waves that transmit energy from the transmitting antenna to the receiving antenna.

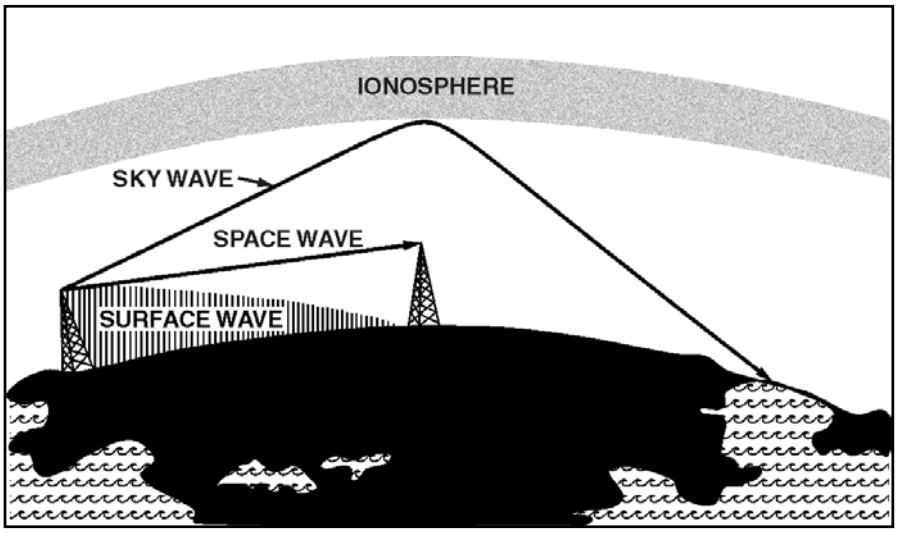


Figure 2-Sum 3. Ground and Sky Waves

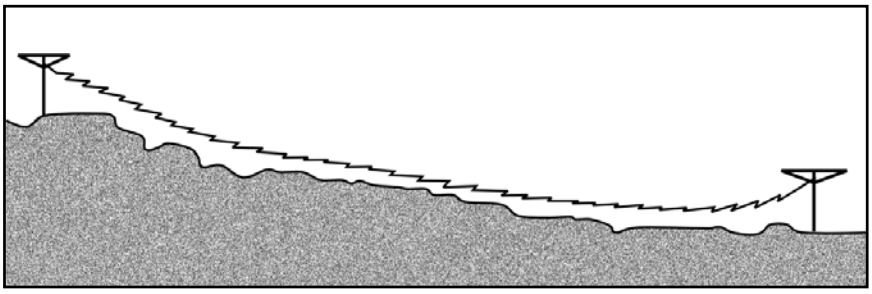


Figure 2-Sum 4. Surface Wave Propagation

Ground waves are composed of two separate component waves: the surface wave and the space wave.

Surface waves travel along the contour of the earth by diffraction.

Space waves can travel through the air directly to the receiving antenna or can be reflected from the surface of the earth.

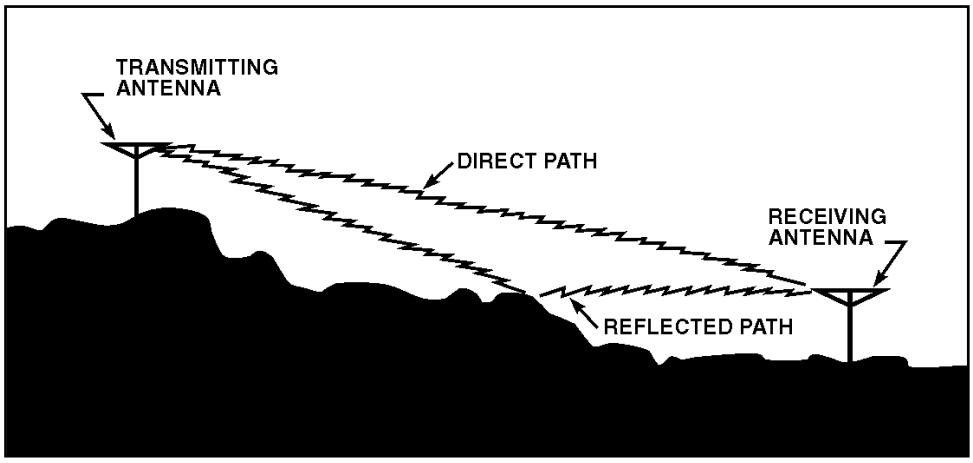


Figure 2-Sum 5. Space Wave Propagation

Sky waves, often called ionospheric waves, are radiated in an upward direction and returned to Earth at some distant location because of refraction.

Natural horizon is the line-of-sight horizon.

Radio horizon is one-third farther than the natural horizon.

The ionosphere consists of several layers of ions, formed by the process called ionization.

Ionization is the process of knocking electrons free from their parent atom, thus upsetting electrical neutrality.

Recombination is the opposite of ionization; that is, the free ions combine with positive ions, causing the positive ions to return to their original neutral atom state.

The D layer is the lowest region of the ionosphere and refracts signals of low frequencies back to Earth.

The E layer is present during the daylight hours, refracts signals as high as 20 megahertz back to Earth; and is used for communications up to 1500 miles.

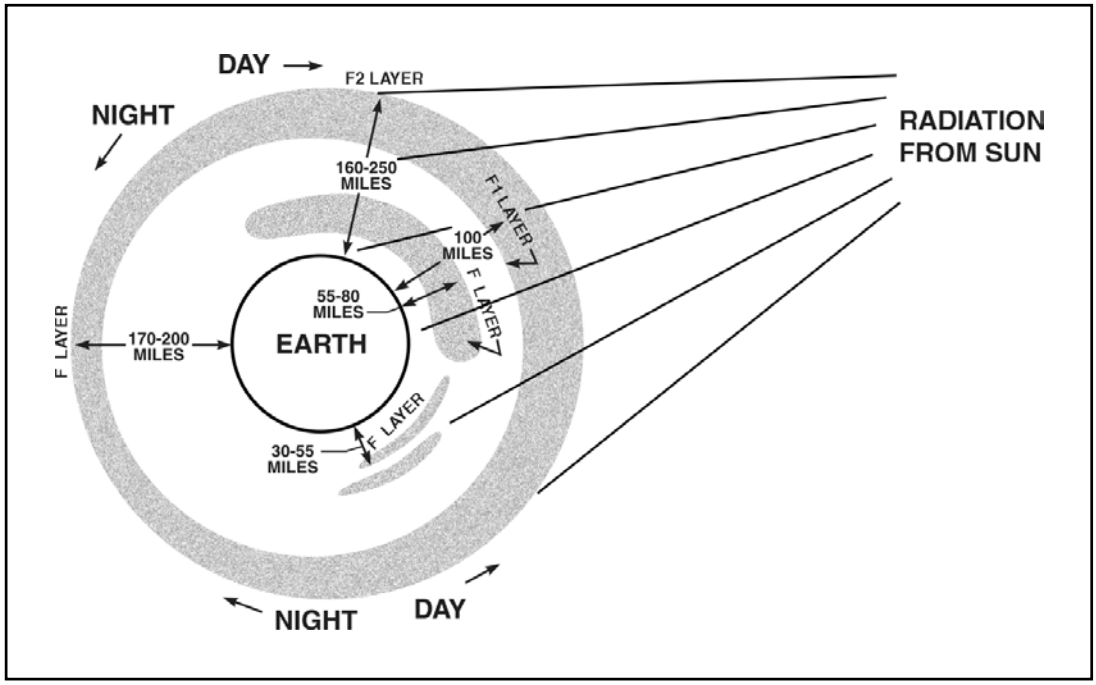


Figure 2-Sum 6. Layers of the Ionosphere

The F layer is divided into the F1 and F2 layers during the day but combine at night to form one layer. This layer is responsible for high frequency, long-range transmission.

The critical frequency is the maximum frequency that a radio wave can be transmitted vertically and still be refracted back to Earth.

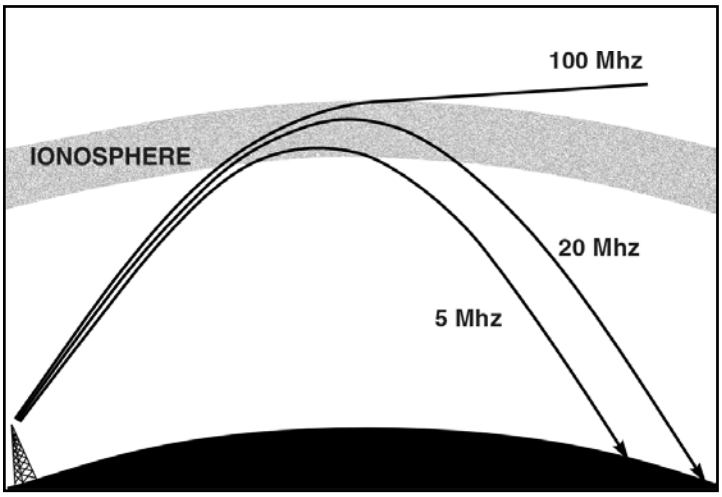


Figure 2-Sum 7. Frequency Versus Refraction and Distance

The critical angle is the maximum and/or minimum angle at which a radio wave can be transmitted and still be refracted back to Earth.

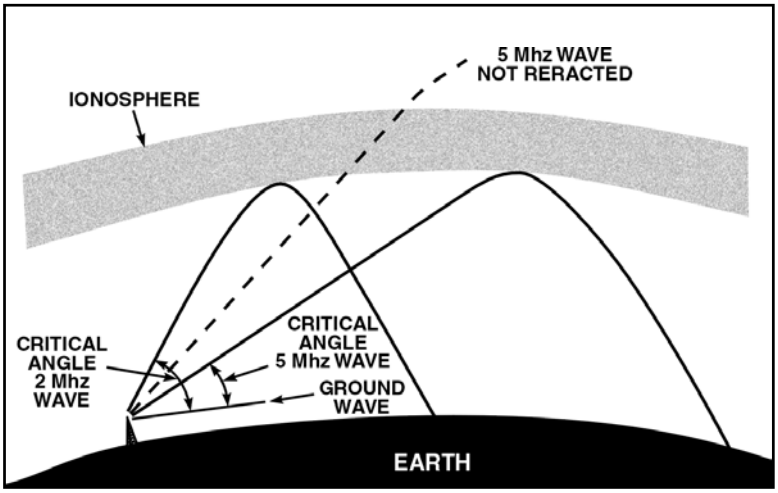


Figure 2-Sum 8. Effects of Frequency on Critical Angle

Skip distance is the distance between the transmitter and the point where the sky wave first returns to Earth.

Skip zone is the zone of silence between the point where the ground wave becomes too weak for reception and the point where the sky wave is first returned to Earth.

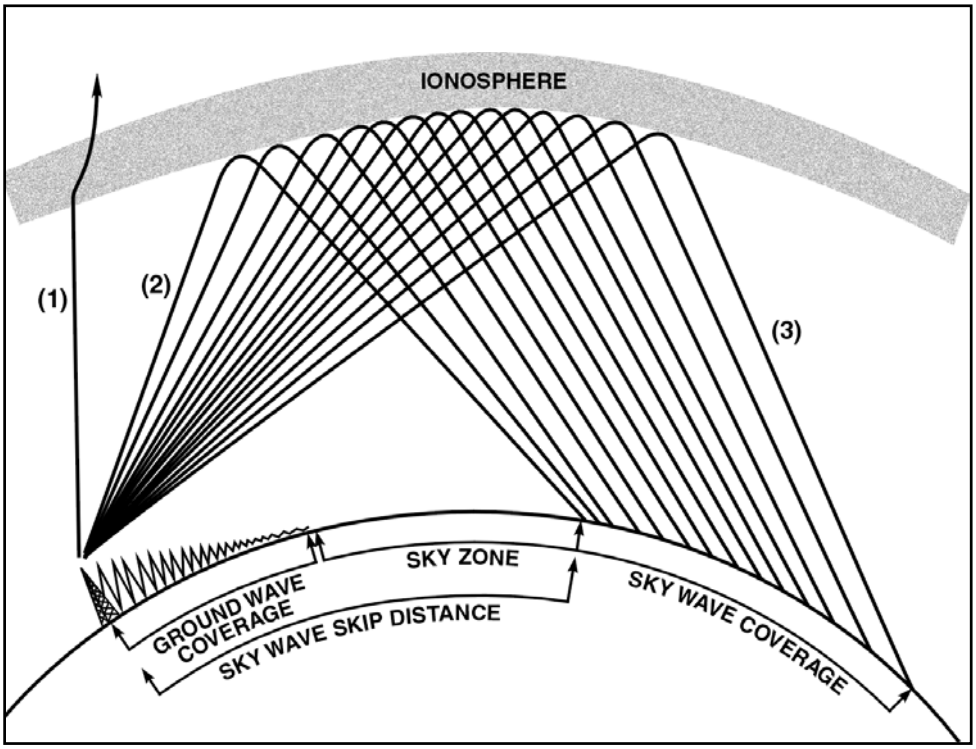


Figure 2-Sum 9. Relationship between Skip Zone, Skip Distance, and Ground Wave

Fading is caused by variations in signal strength, such as absorption of the RF energy by the ionosphere.

Multipath fading occurs when a transmitted signal divides and takes more than one path to a receiver and some of the signals arrive out of phase, resulting in a weak or fading signal.

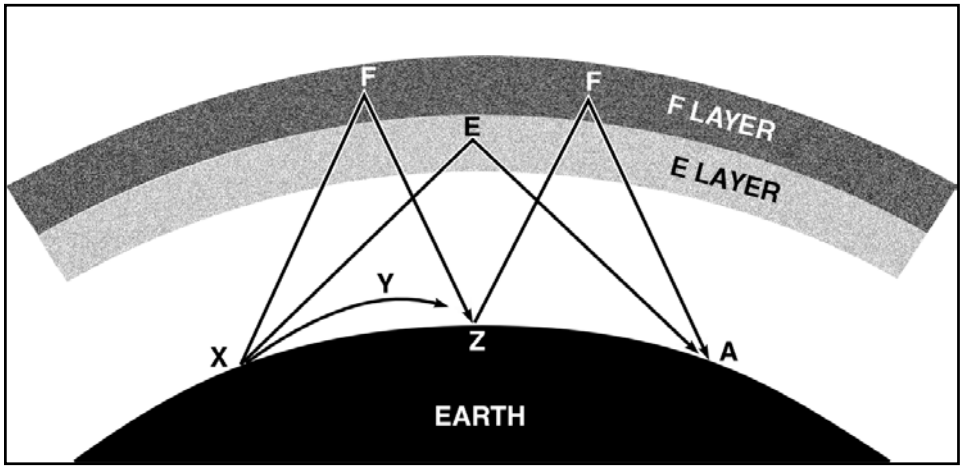


Figure 2-Sum 10. Multipath Transmission

Some transmission losses that affect radio-wave propagation are ionospheric absorption, ground reflection, and free-space losses.

Electromagnetic interference (EMI), both natural and man-made, interferes with radio communications.

The maximum usable frequency (MUF) is the highest frequency that can be used for communications between two locations at a given angle of incidence and time of day.

The lowest usable frequency (LUF) is the lowest frequency that can be used for communications between two locations.

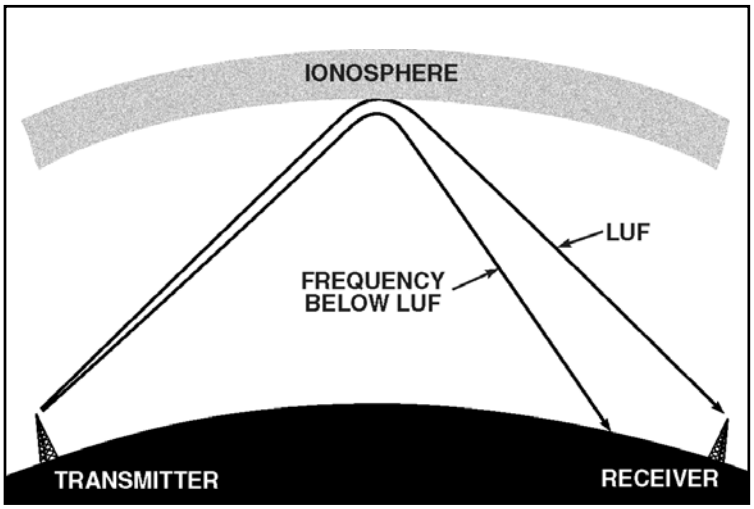


Figure 2-Sum 11. Refraction of Frequency below the Lowest Usable Frequency (LUF)

Optimum working frequency (FOT) is the most practical operating frequency and the one that can be relied on to have the fewest problems.

Precipitation attenuation can be caused by rain, fog, snow, and hail, and can affect overall communications considerably.

Temperature inversion causes channels, or ducts, of cool air to form between layers of warm air, which can cause radio waves to travel far beyond the normal line-of-sight distances.

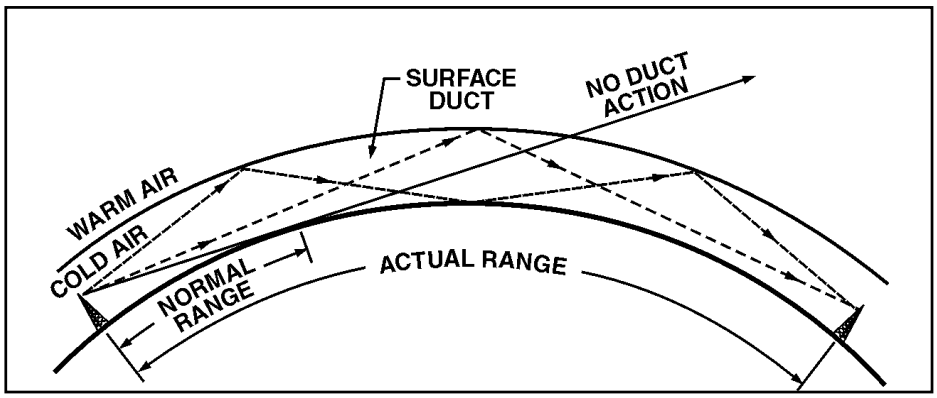


Figure 2-Sum 12. Duct Effect Caused by Temperature Inversion

Tropospheric propagation uses the scattering principle to achieve beyond the line-of-sight radio communications within the troposphere.

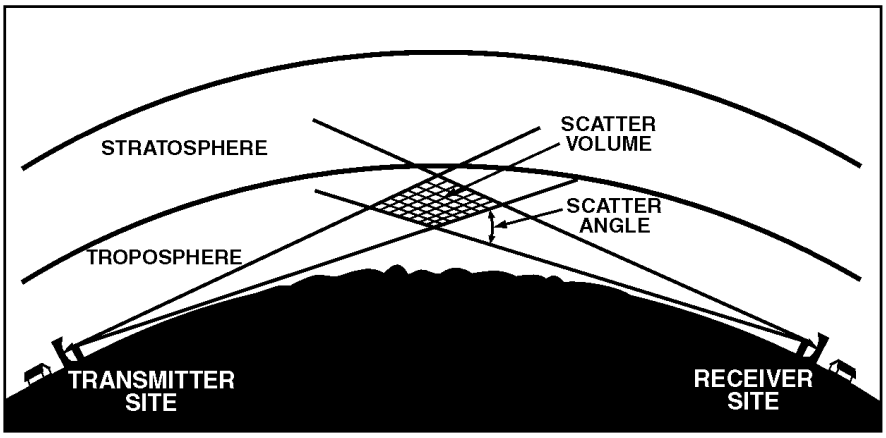


Figure 2-Sum 13. Tropospheric Scattering Propagation

Check-on-Learning Questions

Radio Wave Propagation

1. Which two composite fields (composed of E and H fields) are associated with every antenna?
2. What composite field (composed of E and H fields) is found stored in the antenna?
3. What composite field (composed of E and H fields) is propagated into free space?
4. What is the term used to describe the basic frequency of a radio wave?
5. What is the term used to describe a whole number multiple of the basic frequency of a radio wave?
6. It is known that WWV operates on a frequency of 10 megahertz. What is the wavelength of WWV?
7. A station is known to operate at 60 meters. What is the frequency of the unknown station?
8. If a transmitting antenna is placed close to the ground, how should the antenna be polarized to give the greatest signal strength?
9. In the right-hand rule for propagation, the thumb points in the direction of the E field and the forefinger points in the direction of the H field. In what direction does the middle finger point?
10. What is one of the major reasons for the fading of radio waves that have been reflected from a surface?
11. What are the three layers of the atmosphere?
12. Which layer of the atmosphere has relatively little effect on radio waves?
13. What is the determining factor in classifying whether a radio wave is a ground wave or a space wave?
14. What is the best type of surface or terrain to use for radio wave transmission?
15. What is the primary difference between the radio horizon and the natural horizon?
16. What three factors must be considered in the transmission of a surface wave to reduce attenuation?
17. What causes ionization to occur in the ionosphere?
18. How are the four distinct layers of the ionosphere designated?
19. What is the height of the individual layers of the ionosphere?
20. What factor determines whether a radio wave is reflected or refracted by the ionosphere?
21. There is a maximum frequency at which vertically transmitted radio waves can be refracted back to Earth. What is this maximum frequency called?
22. What three main factors determine the amount of refraction in the ionosphere?
23. What is the skip zone of a radio wave?
24. Where does the greatest amount of ionospheric absorption occur in the ionosphere?
25. What is meant by the term “multipath”?
26. When a wide band of frequencies is transmitted simultaneously, each frequency will vary in the amount of fading. What is this variable fading called?

27. What are the two main sources of electromagnetic interference (EMI) with which radio waves must compete?
28. Thunderstorms, snowstorms, cosmic sources, and the sun are a few examples of EMI sources. What type of EMI comes from these sources?
29. Motors, switches, voltage regulators, and generators are a few examples of EMI sources. What type of EMI comes from these sources?
30. What are three ways of controlling the amount of transmitter-generated EMI?
31. What are three ways of controlling radiated EMI during transmission?
32. What are the two general types of variations in the ionosphere?
33. What is the main difference between these two types of variations?
34. What are the four main classes of regular variation that affect the extent of ionization in the ionosphere?
35. What are the three more common types of irregular variations in the ionosphere?
36. What do the letters MUF, LUF, and FOT stand for?
37. When is MUF at its highest and why?
38. What happens to the radio wave if the LUF is too low?
39. What are some disadvantages of operating transmitters at or near the LUF?
40. What are some disadvantages of operating a transmitter at or near the MUF?
41. What is FOT?
42. How do raindrops affect radio waves?
43. How does fog affect radio waves at frequencies above 2 gigahertz?
44. How is the term “temperature inversion” used when referring to radio waves?
45. How does temperature inversion affect radio transmission?
46. In what layer of the atmosphere does virtually all weather phenomena occur?
47. Which radio frequency bands use the tropospheric scattering principle for propagation of radio waves?
48. Where is the tropospheric region that contributes most strongly to tropospheric scatter propagation?

Chapter 3

Principles of Transmission Lines

LEARNING OBJECTIVES

3-1. Upon completing this chapter, you should be able to do the following:

- State what a transmission line is and how transmission lines are used.
- Explain the operating principles of transmission lines.
- Describe the five types of transmission lines.
- State the length of a transmission line.
- Explain the theory of the transmission line.
- Define the term "lumped constants" in relation to a transmission line.
- Define the term "distributed constants" in relation to a transmission line.
- Define leakage current.
- Describe how the electromagnetic lines of force around a transmission line are affected by the distributed constants.
- Define the term "characteristic impedance" and explain how it affects the transfer of energy along a transmission line.
- State how the energy transfer along a transmission line is affected by characteristic impedance and the infinite line.
- Identify the cause of and describe the characteristics of reflections on a transmission line.
- Define the term "standing waves" as applied to a transmission line.
- Describe how standing waves are produced on a transmission line and identify the types of terminations.
- Describe the types of standing-wave ratios.

INTRODUCTION TO TRANSMISSION LINES

3-2. A transmission line is a device designed to guide electrical energy from one point to another. It is used, for example, to transfer the output RF energy of a transmitter to an antenna. This energy will not travel through normal electrical wire without great losses. Although the antenna can be connected directly to the transmitter, the antenna is usually located some distance away from the transmitter. A transmission line is used to connect the transmitter and the antenna.

3-3. The transmission line has a single purpose for both the transmitter and the antenna. This purpose is to transfer the energy output of the transmitter to the antenna with the least possible power loss. How well this is done depends on the special physical and electrical characteristics (impedance and resistance) of the transmission line.

TERMINOLOGY

3-4. All transmission lines have two ends (see figure 3-1). The end of a two-wire transmission line connected to a source is ordinarily called the input end or the generator end. Other names given to this end are transmitter end, sending end, and source. The other end of the line is called the output end or receiving end. Other names given to the output end are load end and sink.

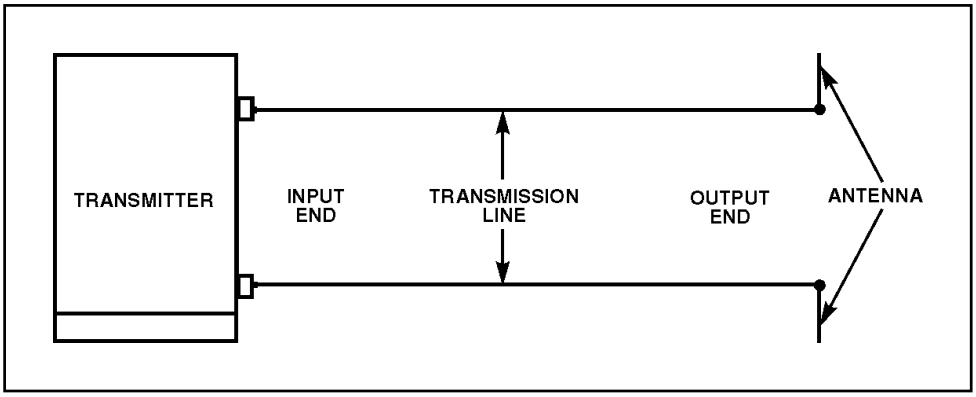


Figure 3-1. Basic Transmission Line

3-5. You can describe a transmission line in terms of its impedance. The ratio of voltage to current (E_{in}/I_{in}) at the input end is known as the input impedance (Z_{in}). This is the impedance presented to the transmitter by the transmission line and its load, the antenna. The ratio of voltage to current at the output (E_{out}/I_{out}) end is known as the output impedance (Z_{out}). This is the impedance presented to the load by the transmission line and its source. If an infinitely long transmission line could be used, the ratio of voltage to current at any point on that transmission line would be some particular value of impedance. This impedance is known as the characteristic impedance.

TYPES OF TRANSMISSION MEDIUMS

3-6. The Army uses many different types of transmission mediums in its electronic applications. Each medium (line or waveguide) has a certain characteristic impedance value, current-carrying capacity, and physical shape and is designed to meet a particular requirement.

3-7. The five types of transmission mediums discussed in this chapter include parallel line, twisted pair, shielded pair, coaxial line, and waveguides. The use of a particular line depends, among other things, on the applied frequency, the power-handling capabilities, and the type of installation.

Note. In the following paragraphs, we mention losses several times. Losses are discussed more thoroughly later in this chapter.

Parallel Line

3-8. One type of parallel line is the two-wire open line illustrated in figure 3-2. This line consists of two wires that are generally spaced from 2 to 6 inches apart by insulating spacers. This type of line is most often used for power lines, rural telephone lines, and telegraph lines. It is sometimes used

as a transmission line between a transmitter and an antenna or between an antenna and a receiver. An advantage of this type of line is its simple construction. The principal disadvantages of this type of line are the high radiation losses and electrical noise pickup because of the lack of shielding. The changing fields created by the changing current in each conductor produce radiation losses.

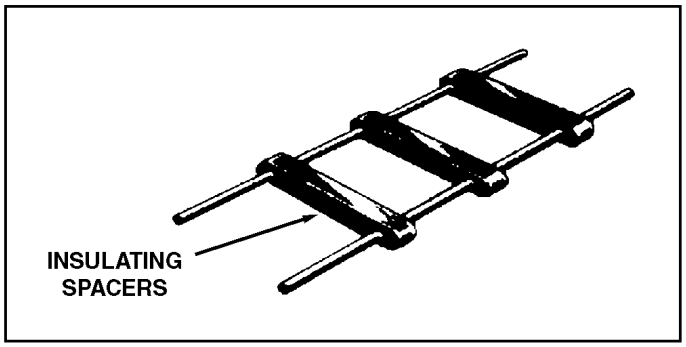


Figure 3-2. Parallel Two-Wire Open Line

3-9. Another type of parallel line is the two-wire ribbon (twin lead) illustrated in figure 3-3. This type of transmission line is commonly used to connect a television-receiving antenna to a home television set. This line is essentially the same as the two-wire open line except that uniform spacing is assured by embedding the two wires in a low-loss dielectric, usually polyethylene. Because the wires are embedded in the thin ribbon of polyethylene, the dielectric space is partly air and partly polyethylene.

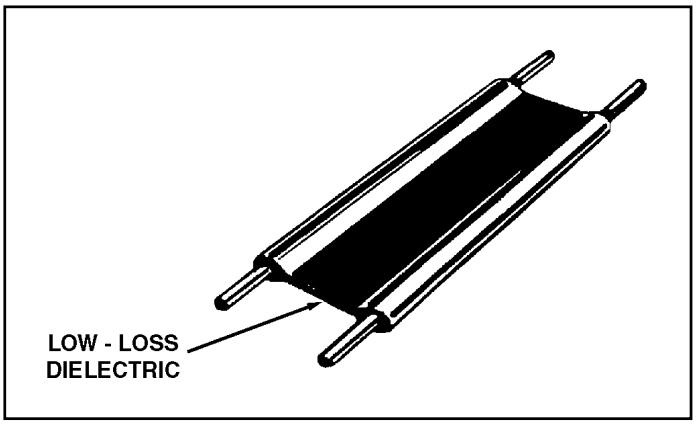


Figure 3-3. Two-Wire Ribbon Line

Twisted Pair

3-10. The twisted pair transmission line is illustrated in figure 3-4. As the name implies, the line consists of two insulated wires twisted together to form a flexible line without the use of spacers. It is not used for transmitting at high frequency because of the high dielectric losses that occur in the rubber insulation. When the line is wet, the losses increase greatly.

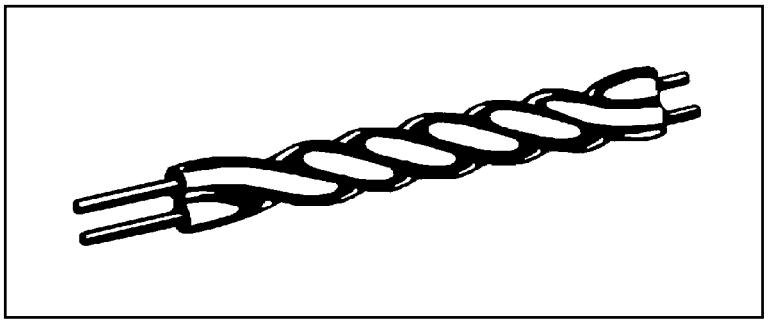


Figure 3-4. Twisted Pair

Shielded Pair

3-11. The shielded pair, shown in figure 3-5 consists of parallel conductors separated from each other and surrounded by a solid dielectric. The conductors are contained within braided copper tubing that acts as an electrical shield. The assembly is covered with a rubber or flexible composition coating that protects the line from moisture and mechanical damage. Outwardly, it looks much like the power cord of a washing machine or refrigerator.

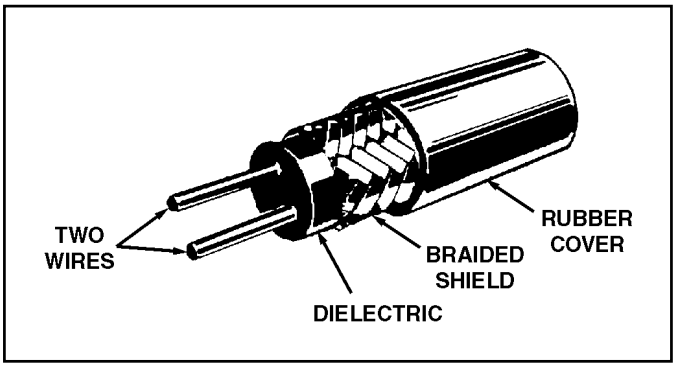


Figure 3-5. Shielded Pair

3-12. The principal advantage of the shielded pair is that the conductors are balanced to ground; that is, the capacitance between the wires is uniform throughout the length of the line. This balance is due to the uniform spacing of the grounded shield that surrounds the wires along their entire length. The braided copper shield isolates the conductors from stray magnetic fields.

Coaxial Lines

3-13. There are two types of coaxial lines: rigid (air) and flexible (solid) coaxial line. The physical construction of both types is basically the same; that is, each contains two concentric conductors.

3-14. The rigid coaxial line consists of a central, insulated wire (inner conductor) mounted inside a tubular outer conductor. This line is shown in figure 3-6. In some applications, the inner conductor is also tubular. Insulating spacers or beads at regular intervals insulates the inner conductor

from the outer conductor. The spacers are made of pyrex, polystyrene, or some other material that has good insulating characteristics and low dielectric losses at high frequencies.

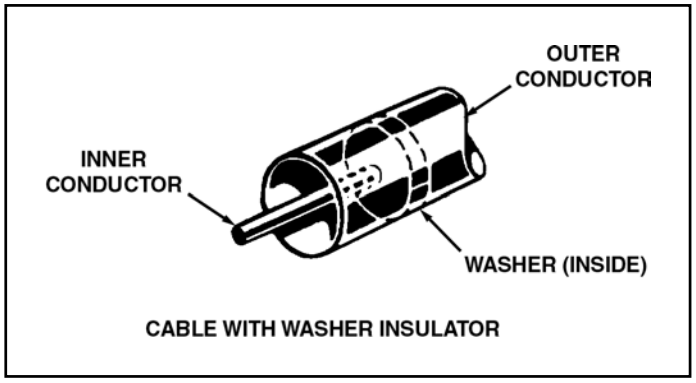


Figure 3-6. Rigid (Air) Coaxial Line

3-15. The chief advantage of the rigid line is its ability to minimize radiation losses. The electric and magnetic fields in a two-wire parallel line extend into space for relatively great distances and radiation losses occur. However, in a coaxial line no electric or magnetic fields extend outside of the outer conductor. The fields are confined to the space between the two conductors, resulting in a perfectly shielded coaxial line. Another advantage is that interference from other lines is reduced.

3-16. The rigid line has the following disadvantages: (1) it is expensive to construct; (2) it must be kept dry to prevent excessive leakage between the two conductors; and (3) although high-frequency losses are somewhat less than in previously mentioned lines, they are still excessive enough to limit the practical length of the line.

3-17. Leakage caused by the condensation of moisture is prevented in some rigid line applications by the use of an inert gas, such as nitrogen, helium, or argon. It is pumped into the dielectric space of the line at a pressure that can vary from 3 to 35 pounds per square inch. The inert gas is used to dry the line when it is first installed and pressure is maintained to ensure that no moisture enters the line.

3-18. Flexible coaxial lines (figure 3-7) are made with an inner conductor that consists of flexible wire insulated from the outer conductor by a solid, continuous insulating material. The outer conductor is made of metal braid, which gives the line flexibility. Early attempts at gaining flexibility involved using rubber insulators between the two conductors. However, the rubber insulators caused excessive losses at high frequencies.

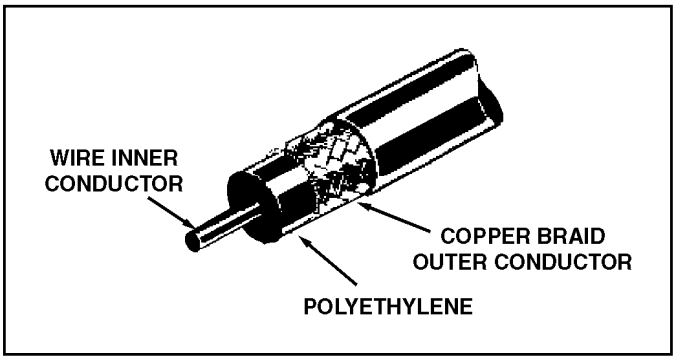


Figure 3-7. Flexible (Solid) Coaxial Line

3-19. Because of the high-frequency losses associated with rubber insulators, polyethylene plastic was developed to replace rubber and eliminate these losses. Polyethylene plastic is a solid substance that remains flexible over a wide range of temperatures. It is unaffected by seawater, gasoline, oil, and most other liquids that may be found aboard ship. The use of polyethylene as an insulator results in greater high-frequency losses than the use of air as an insulator. However, these losses are still lower than the losses associated with most other solid dielectric materials.

Waveguides

3-20. The waveguide is classified as a transmission line. However, the method by which it transmits energy down its length differs from the conventional methods. Waveguides are cylindrical, elliptical, or rectangular (cylindrical and rectangular shapes are shown in figure 3-8). The rectangular waveguide is used more frequently than the cylindrical waveguide.

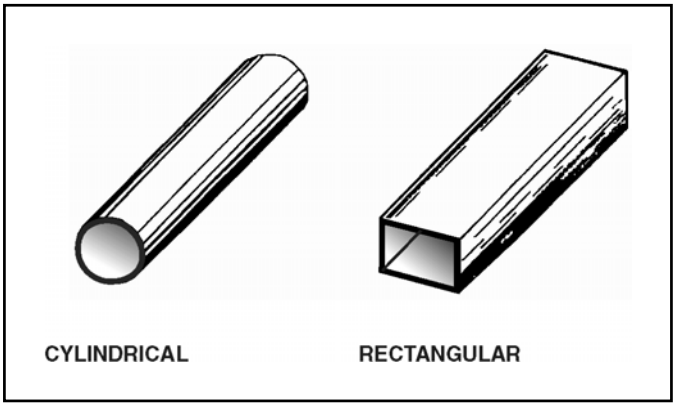


Figure 3-8. Waveguides

3-21. The term waveguide can be applied to all types of transmission lines in the sense that they are all used to guide energy from one point to another. However, usage has generally limited the term to mean a hollow metal tube or a dielectric transmission line. In this chapter, we use the term waveguide only to mean "hollow metal tube." It is interesting to note that the transmission of electromagnetic energy along a waveguide travels at a velocity somewhat slower than electromagnetic energy traveling through free space.

3-22. A waveguide may be classified according to its cross section (rectangular, elliptical, or circular), or according to the material used in its construction (metallic or dielectric). Dielectric waveguides are seldom used because the dielectric losses for all known dielectric materials are too great to transfer the electric and magnetic fields efficiently.

3-23. The installation of a complete waveguide transmission system is somewhat more difficult than the installation of other types of transmission lines. The radius of bends in the waveguide must measure greater than two wavelengths at the operating frequency of the equipment to avoid excessive attenuation. The cross section must remain uniform around the bend. These requirements hamper installation in confined spaces. If the waveguide is dented, or if solder is permitted to run inside the joints, the attenuation of the line is greatly increased. Dents and obstructions in the waveguide also reduce its breakdown voltage, thus limiting the waveguide's power-handling capability because of possible arc-over. Great care must be exercised during installation; one or two carelessly made joints can seriously inhibit the advantage of using the waveguide.

LOSSES IN TRANSMISSION LINES

3-24. The discussion of transmission lines so far has not directly addressed line losses; actually some line losses occur in all lines. Line losses may be any of three types—copper, dielectric, and radiation or induction losses.

Note. Transmission lines are sometimes referred to as RF lines. In this text the terms are used interchangeably.

Copper Losses

3-25. One type of copper loss is I2R loss. In RF lines, the resistance of the conductors is never equal to zero. Whenever current flows through one of these conductors, some energy is dissipated in the form of heat. This heat loss is a power loss. With copper braid, which has a higher resistance than solid tubing, this power loss is higher.

3-26. Another type of copper loss is due to skin effect. When DC flows through a conductor, the movement of electrons through the conductor's cross section is uniform. The situation is somewhat different when AC is applied. The expanding and collapsing fields about each electron encircle other electrons. This phenomenon, called self-induction, retards the movement of the encircled electrons. The flux density at the center is so great that electron movement at this point is reduced. As frequency is increased, the opposition to the flow of current in the center of the wire increases. Current in the center of the wire becomes smaller and most of the electron flow is on the wire surface. When the frequency applied is 100 megahertz or higher, the electron movement in the center is so small that the center of the wire could be removed without any noticeable effect on current. You should be able to see that the effective cross-sectional area decreases as the frequency increases.

3-27. Because resistance is inversely proportional to the cross-sectional area, the resistance will increase as the frequency is increased. Also, because power loss increases as resistance increases, power losses increase with an increase in frequency because of skin effect. Skin effect is a tendency for

alternating current (AC) to flow mostly near the outer surface of a solid electrical conductor, such as metal wire, at frequencies above the audio range. The effect becomes more and more apparent as the frequency increases.

3-28. Copper losses can be minimized and conductivity increased in an RF line by plating the line with silver. Because silver is a better conductor than copper, most of the current will flow through the silver layer. The tubing then serves primarily as a mechanical support.

Dielectric Losses

3-29. Dielectric losses result from the heating effect on the dielectric material between the conductors. Power from the source is used in heating the dielectric. The heat produced is dissipated into the surrounding medium. When there is no potential difference between two conductors, the atoms in the dielectric material between them are normal and the orbits of the electrons are circular. When there is a potential difference between two conductors, the orbits of the electrons change. The excessive negative charge on one conductor repels electrons on the dielectric toward the positive conductor and thus distorts the orbits of the electrons. A change in the path of electrons requires more energy, introducing a power loss.

3-30. The atomic structure of rubber is more difficult to distort than the structure of some other dielectric materials. The atoms of materials, such as polyethylene, distort easily. Therefore, polyethylene is often used as a dielectric because less power is consumed when its electron orbits are distorted.

Radiation and Induction Losses

3-31. Radiation and induction losses are similar in that the fields surrounding the conductors cause both. Induction losses occur when the electromagnetic field about a conductor cuts through any nearby metallic object and a current is induced in that object. As a result, power is dissipated in the object and is lost.

3-32. Radiation losses occur because some magnetic lines of force about a conductor do not return to the conductor when the cycle alternates. These lines of force are projected into space as radiation and this results in power losses. That is, power is supplied by the source, but is not available to the load.

LENGTH OF A TRANSMISSION LINE

3-33. A transmission line is considered to be electrically short when its physical length is short compared to a quarter-wavelength (¼λ) of the energy it is to carry.

Note. In this document, for ease of reading, the value of the wavelength is spelled out in some cases, and in other cases, the numerical value is used.

3-34. A transmission line is electrically long when its physical length is long compared to a quarter-wavelength of the energy it is to carry. You must understand that the terms “short” and “long” are relative ones. For example, a line that has a physical length of 3 meters (approximately 10 feet) is considered quite short electrically if it transmits a radio frequency of

30 kilohertz. On the other hand, the same transmission line is considered electrically long if it transmits a frequency of 30,000 megahertz.

3-35. To show the difference in physical and electrical lengths of the lines mentioned above, compute the wavelength of the two frequencies, taking the 30-kilohertz example first—

Given:

$$\lambda = \frac{v}{f}$$

Where:

λ = wavelength

v = velocity of RF in free space

f = frequency of transmission

Hz = cycles per second

Solution:

$$\lambda = \frac{300 \times 10^6 \text{ meters/second}}{30 \times 10^3 \text{ cycles/second (Hz)}}$$

$$\lambda = 10 \times 10^3 \text{ meters/cycle}$$

λ = 10,000 meters, or approximately 6 miles for a complete wavelength

3-36. Now, computing the wavelength for the line carrying 30,000 megahertz—

$$\lambda = \frac{v}{f}$$

$$\lambda = \frac{300 \times 10^6 \text{ meters/second}}{30{,}000 \times 10^6 \text{ cycles/second (Hz)}}$$

$$\lambda = \frac{1}{100} \text{ meter/cycle}$$

λ = .01 meter or approximately .03 foot for a complete wavelength

3-37. Thus, you can see that a 3-meter line is electrically very short for a frequency of 30 kilohertz. Also, the 3-meter line is electrically very long for a frequency of 30,000 megahertz.

3-38. When power is applied to a very short transmission line, practically all of it reaches the load at the output end of the line. This very short transmission line is usually considered to have practically no electrical properties of its own, except for a small amount of resistance.

3-39. However, the picture changes considerably when a long line is used. Because most transmission lines are electrically long (because of the distance from transmitter to antenna), the properties of such lines must be considered. Frequently, the voltage necessary to drive a current through a long line is

considerably greater than the amount that can be accounted for by the impedance of the load in series with the resistance of the line.

TRANSMISSION LINE THEORY

3-40. The electrical characteristics of a two-wire transmission line depend primarily on the construction of the line. The two-wire line acts like a long capacitor. The change of its capacitive reactance is noticeable as the frequency applied to it is changed. Because the long conductors have a magnetic field about them when electrical energy is being passed through them, they also exhibit the properties of inductance. The values of inductance and capacitance presented depend on the various physical factors that we discussed earlier in this chapter. For example, the type of line used, the dielectric in the line, and the length of the line must be considered. The effects of the inductive and capacitive reactances of the line depend on the frequency applied. Because no dielectric is perfect, electrons manage to move from one conductor to the other through the dielectric. Each type of two-wire transmission line also has a conductance value. This conductance value represents the value of the current flow that may be expected through the insulation. If the line is uniform (all values equal at each unit length), then one small section of the line may represent several feet. This illustration of a two-wire transmission line is used throughout the following discussion of transmission lines; but keep in mind that the principles presented here apply to all transmission lines. We explain the theories using lumped constants and distributed constants to simplify these principles further.

LUMPED CONSTANTS

3-41. A transmission line has the properties of inductance, capacitance, and resistance, just as the more conventional circuits have. Usually, however, the constants in conventional circuits are lumped into a single device or component. For example, a coil of wire has the property of inductance. When a certain amount of inductance is needed in a circuit, a coil of the proper dimensions is inserted. The inductance of the circuit is lumped into the one component. Two metal plates separated by a small space can be used to supply the required capacitance for a circuit. In such a case, most of the capacitance of the circuit is lumped into this one component. Similarly, a fixed resistor can be used to supply a certain value of circuit resistance as a lumped sum. Ideally, a transmission line would also have its constants of inductance, capacitance, and resistance lumped together, as shown in figure 3-9. Transmission line constants are distributed, as described below.

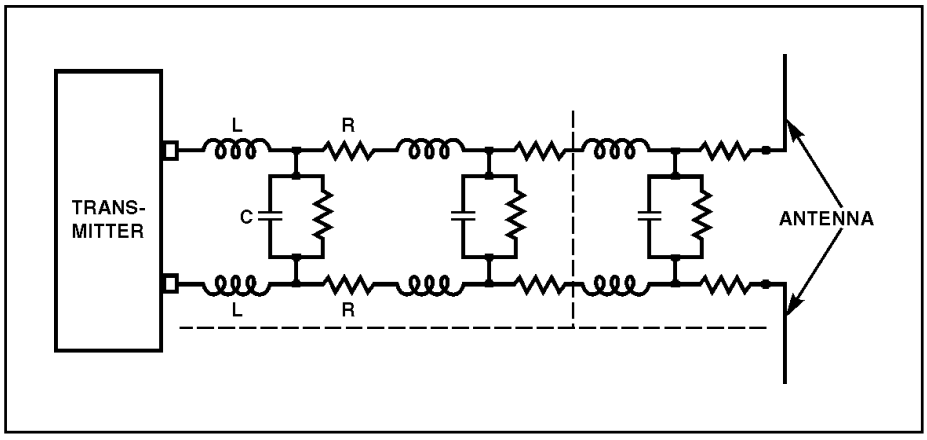


Figure 3-9. Equivalent Circuit of a Two-Wire Transmission Line

DISTRIBUTED CONSTANTS

3-42. Transmission line constants, called distributed constants, are spread along the entire length of the transmission line and cannot be distinguished separately. The amount of inductance, capacitance, and resistance depends on the length of the line, the size of the conducting wires, the spacing between the wires, and the dielectric (air or insulating medium) between the wires.

Inductance of a Transmission Line

3-43. When current flows through a wire, magnetic lines of force are set up around the wire. As the current increases and decreases in amplitude, the field around the wire expands and collapses accordingly. The energy produced by the magnetic lines of force collapsing back into the wire tends to keep the current flowing in the same direction. This represents a certain amount of inductance, which is expressed in microhenrys per unit length. Figure 3-10 illustrates the inductance and magnetic fields of a transmission line.

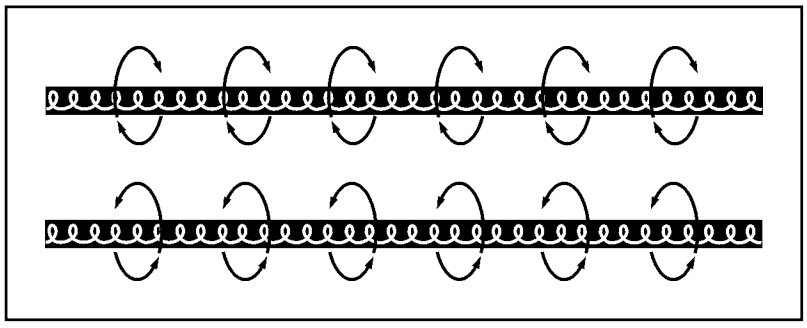


Figure 3-10. Distributed Inductance

Capacitance of a Transmission Line

3-44. Capacitance also exists between the transmission line wires, as illustrated in figure 3-11. Notice that the two parallel wires act as plates of a capacitor and that the air between them acts as a dielectric. The capacitance between the wires is usually expressed in picofarads per unit length. This electric field between the wires is similar to the field that exists between the two plates of a capacitor.

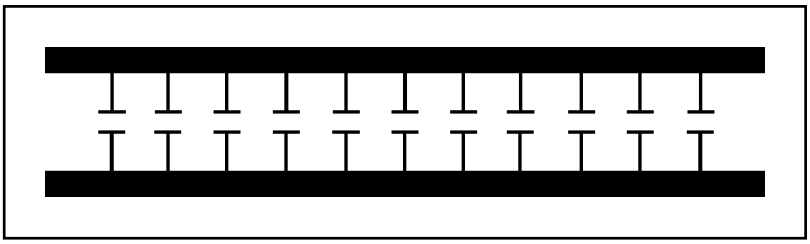


Figure 3-11. Distributed Capacitance

Resistance of a Transmission Line

3-45. The transmission line shown in figure 3-12 has electrical resistance along its length. This resistance is usually expressed in ohms per unit length and is shown as existing continuously from one end of the line to the other.

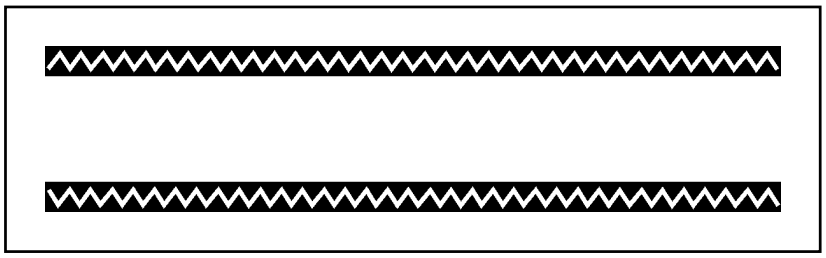


Figure 3-12. Distributed Resistance

Leakage Current

3-46. Because any dielectric, even air, is not a perfect insulator, a small current known as leakage current flows between the two wires. In effect, the insulator acts as a resistor, permitting current to pass between the two wires. Figure 3-13 shows this leakage path as resistors in parallel connected between the two lines. This property is called conductance (G) and is the opposite of resistance. Conductance in transmission lines is expressed as the reciprocal of resistance and is usually given in micromhos per unit length.

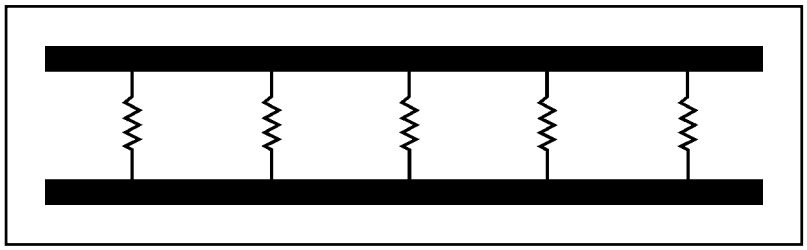


Figure 3-13. Leakage in a Transmission Line

ELECTROMAGNETIC FIELDS ABOUT A TRANSMISSION LINE

3-47. The distributed constants of resistance, inductance, and capacitance are basic properties common to all transmission lines and exist whether or not any current flow exists. As soon as current flow and voltage exist in a transmission line, another property becomes quite evident. This is the presence of an electromagnetic field, or lines of force, about the wires of the transmission line. The lines of force themselves are not visible; however, understanding the force that an electron experiences while in the field of these lines is very important to your understanding of energy transmission.

3-48. There are two kinds of fields; one is associated with voltage and the other with current. The field associated with voltage is called the electric (E) field. It exerts a force on any electric charge placed in it. The field associated with current is called a magnetic (H) field, because it tends to exert a force on any magnetic pole placed in it. Figure 3-14 illustrates the way in which the E fields and H fields tend to orient themselves between conductors of a typical two-wire transmission line. The illustration shows a cross section of the transmission lines. The E field is represented by solid lines and the H field by dotted lines. The arrows indicate the direction of the lines of force. Both fields normally exist together and are spoken of collectively as the electromagnetic field.

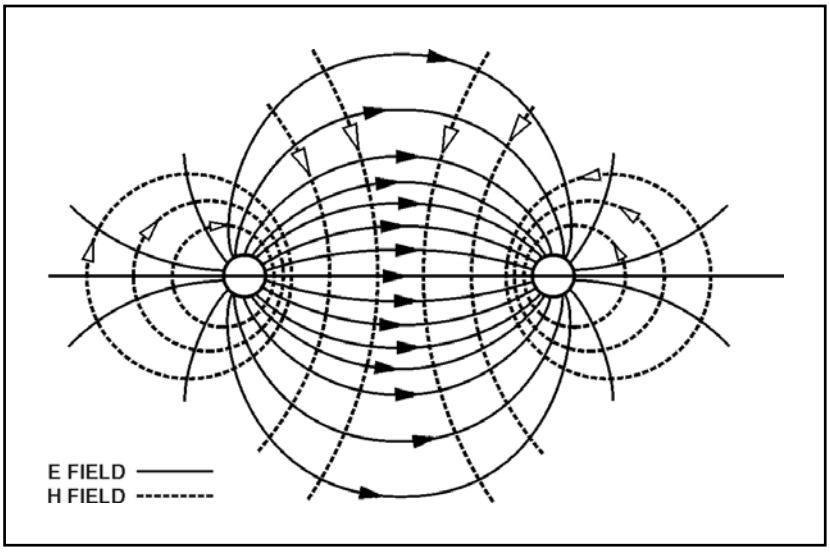


Figure 3-14. Fields between Conductors

CHARACTERISTIC IMPEDANCE OF A TRANSMISSION LINE

3-49. You learned earlier that the maximum (and most efficient) transfer of electrical energy takes place when the source impedance is matched to the load impedance. This fact is very important in the study of transmission lines and antennas. If the characteristic impedance of the transmission line and the load impedance are equal, energy from the transmitter will travel down the transmission line to the antenna with no power loss caused by reflection.

Definition and Symbols

3-50. Every transmission line possesses certain characteristic impedance, usually designated as Z_0. Z_0 is the ratio of E to I at every point along the line. If a load equal to the characteristic impedance is placed at the output end of any length of line, the same impedance will appear at the input terminals of the line. The characteristic impedance is the only value of impedance for any given type and size of line that acts in this way. The characteristic impedance determines the amount of current that can flow when a given voltage is applied to an infinitely long line. Characteristic impedance is comparable to the resistance that determines the amount of current that flows in a DC circuit.

3-51. Lumped and distributed constants were explained earlier in this chapter. Figure 3-15, view A, shows the properties of resistance (R), inductance (L), capacitance (C), and conductance (G) combined in a short section of two-wire transmission line. The illustration shows the evenly distributed capacitance as a single lumped capacitor and the distributed conductance as a lumped leakage path. Lumped values may be used for transmission line calculations if the physical length of the line is very short compared to the wavelength of energy being transmitted. Figure 3-15, view B, shows all four properties lumped together and represented by their conventional symbols.

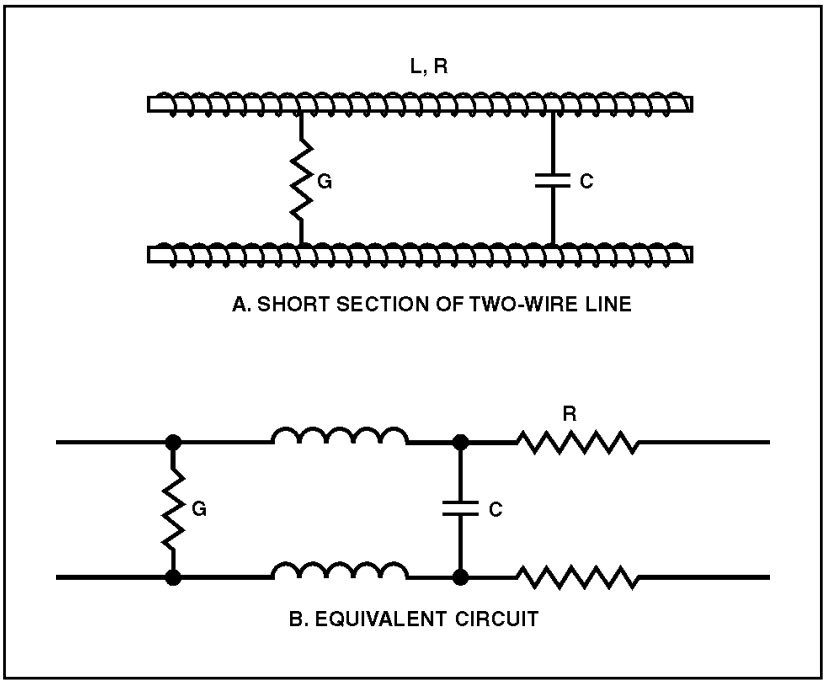


Figure 3-15. Short Section of Two-Wire Transmission Line and Equivalent Circuit

Characteristic Impedance and the Infinite Line

3-52. Like those shown in figure 3-15, several short sections can be combined to form a large transmission line, as shown in figure 3-16. Current will flow if voltage is applied across points K and L. In fact, any circuit, such as that represented in figure 3-16, view A, has a certain current flow for each value of applied voltage. The ratio of the voltage to the current is the impedance (Z), as expressed in the following formula:

$$Z = \frac{E}{I}$$

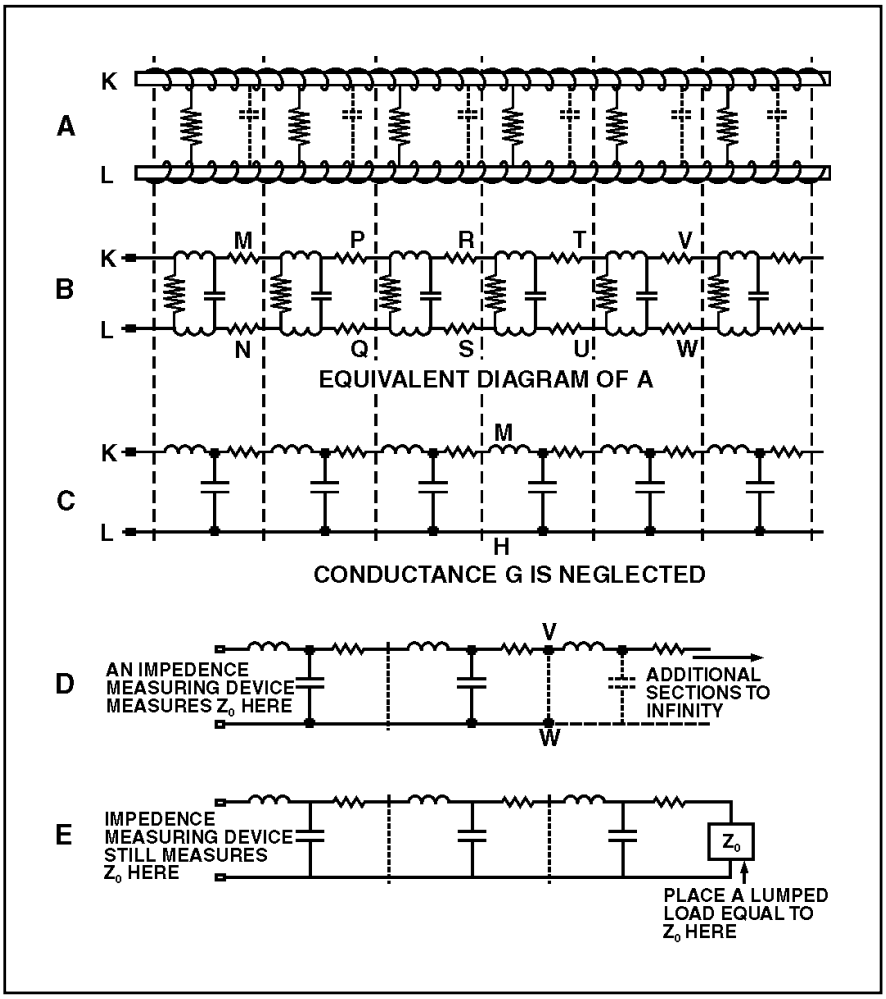


Figure 3-16. Characteristic Impedance

3-53. The impedance presented to the input terminals of the transmission line is not merely the resistance of the wire in series with the impedance of the load. The effects of series inductance and shunt capacitance of the line itself may overshadow the resistance, and even the load, as far as the input terminals are concerned.

3-54. To find the input impedance of a transmission line, determine the impedance of a single section of line. The impedance between points K and L, in figure 3-16, view B, can be calculated by the use of series-parallel impedance formulas, provided the impedance across points M and N is known. But because this section is merely one small part of a longer line, another similar section is connected to points M and N. Again, the impedance across points K and L of the two sections can be calculated, provided the impedance of the third section is known. This process of adding one section to another can be repeated endlessly. The addition of each section produces an impedance across points K and L of a new and lower value. However, after many sections have been added, each successive added section has less and less effect on the impedance across points K and L. If sections are added to

the line endlessly, the line is infinitely long, and a certain finite value of impedance across points K and L is finally reached.

3-55. In this discussion of transmission lines, the effect of conductance (G) is minor compared to that of inductance (L) and capacitance (C), and is frequently neglected. In figure 3-16, view C, G is omitted and the inductance and resistance of each line can be considered as one line.

3-56. Let us assume that the sections of figure 3-16, view C continue to the right with an infinite number of sections. When an infinite number of sections extends to the right, the impedance appearing across K and L is Z_0. If the line is cut at R and S, an infinite number of sections still extends to the right because the line is endless in that direction. Therefore, the impedance now appearing across points R and S is also Z_0, as illustrated in view D. You can see that if only the first three sections are taken and a load impedance of Z_0 is connected across points R and S, the impedance across the input terminals K and L is still Z_0. The line continues to act as an infinite line, as illustrated in view E.

3-57. Figure 3-17, view A illustrates how the characteristic impedance of an infinite line can be calculated. Resistors are added in series parallel across terminals K and L in eight steps, and the resultant impedances are noted. In step 1 the impedance is infinite; in step 2 the impedance is 110 ohms. In step 3 the impedance becomes 62.1 ohms, a change of 47.9 ohms. In step 4 the impedance is 48.5 ohms, a change of only 13.6 ohms. The resultant changes in impedance from each additional increment become progressively smaller. Eventually, practically no change in impedance results from further additions to the line. The total impedance of the line at this point is said to be at its characteristic impedance; which, in this case, is 37 ohms. This means that an infinite line constructed as indicated in step 8 could be effectively replaced by a 37-ohm resistor. View B shows a 37-ohm resistor placed in the line at various points to replace the infinite line of step 8 in view A. There is no change in total impedance.

3-58. In figure 3-17, resistors were used to show impedance characteristics for the sake of simplicity. Figuring the actual impedance of a line having reactance is very similar, with inductance taking the place of the series resistors and capacitance taking the place of the shunt resistors. The characteristic impedance of lines in actual use normally lies between 50 and 600 ohms.

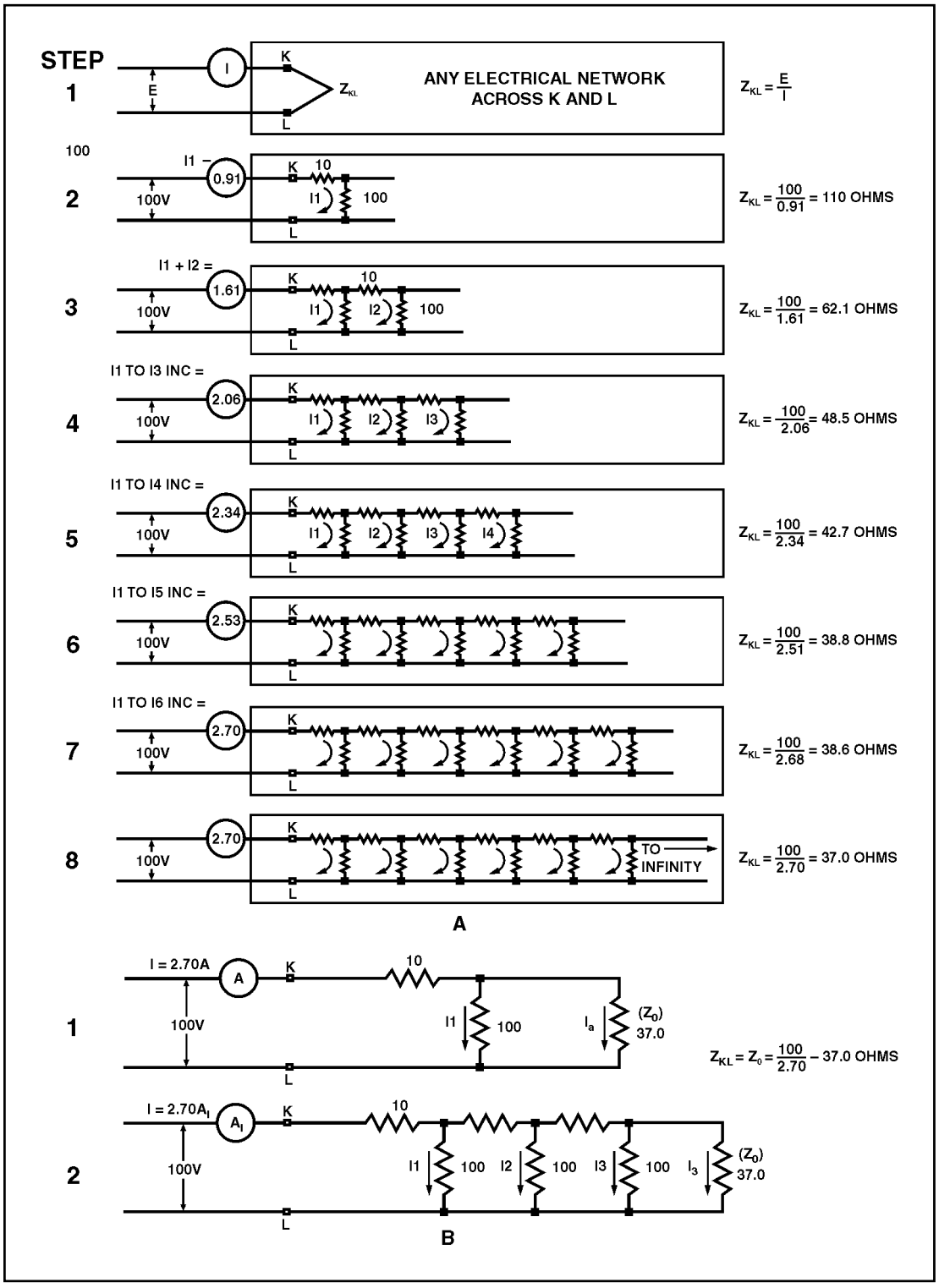


Figure 3-17 Termination of a Line

3-59. When a transmission line is "short" compared to the length of the RF waves it carries, the opposition presented to the input terminals is determined primarily by the load impedance. A small amount of power is dissipated in overcoming the resistance of the line. However, when the line is "long" and the load is an incorrect impedance, the voltages necessary to drive a given amount of current through the line cannot be accounted for by considering just the impedance of the load in series with the impedance of the line. The line has properties other than resistance that affect input impedance. These properties are inductance in series with the line, capacitance across the line, resistance leakage paths across the line, and certain radiation losses.

VOLTAGE CHANGE ALONG A TRANSMISSION LINE

3-60. Let us summarize what we have just discussed. In an electric circuit, energy is stored in electric and magnetic fields. These fields must be brought to the load to transmit that energy. At the load, energy contained in the fields is converted to the desired form of energy.

Transmission of Energy

3-61. When the load is connected directly to the source of energy, or when the transmission line is short, problems concerning current and voltage can be solved by applying Ohm's law. When the transmission line becomes long enough so the time difference between a change occurring at the generator and the change appearing at the load becomes appreciable, analysis of the transmission line becomes important.

DC Applied to a Transmission Line

3-62. In figure 3-18, a battery is connected through a relatively long two-wire transmission line to a load at the far end of the line. At the instant the switch is closed, neither current nor voltage exists on the line. When the switch is closed, point A becomes a positive potential, and point B becomes negative. These points of difference in potential move down the line. However, as the initial points of potential leave points A and B, they are followed by new points of difference in potential which the battery adds at A and B. This is merely saying that the battery maintains a constant potential difference between points A and B. A short time after the switch is closed, the initial points of difference in potential have reached points A' and B'; the wire sections from points A to A' and points B to B' are at the same potential as A and B, respectively. The points of charge are represented by plus (+) and minus (-) signs along the wires. The directions of the currents in the wires are represented by the arrowheads on the line, and the direction of travel is indicated by an arrow below the line. Conventional lines of force represent the electric field that exists between the opposite kinds of charge on the wire sections from A to A' and B to B'. Crosses (tails of arrows) indicate the magnetic field created by the electric field moving down the line. The moving electric field and the accompanying magnetic field constitute an electromagnetic wave that is moving from the generator (battery) toward the load. This wave travels at approximately the speed of light in free space. The energy reaching the load is equal to that developed at the battery (assuming there are no losses in the transmission line). If the load absorbs all of the energy, the current and voltage will be evenly distributed along the line.

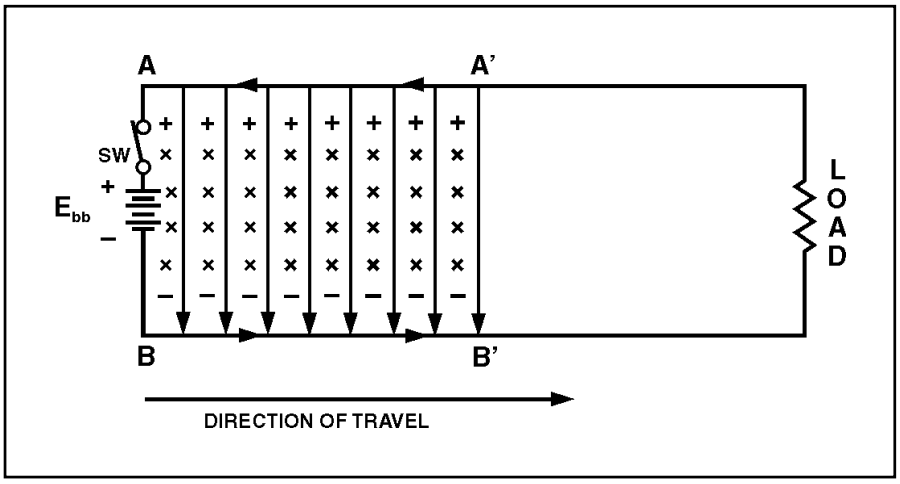


Figure 3-18. DC Voltage Applied to a Line

AC Applied to a Transmission Line

3-63. When the battery of figure 3-18 is replaced by an AC generator (figure 3-19), each successive instantaneous value of the generator voltage is propagated down the line at the speed of light. The action is similar to the wave created by the battery except that the applied voltage is sinusoidal instead of constant. Assume that the switch is closed at the moment the generator voltage is passing through zero and that the next half cycle makes point A positive. At the end of one cycle of generator voltage, the current and voltage distribution will be as shown in figure 3-19.

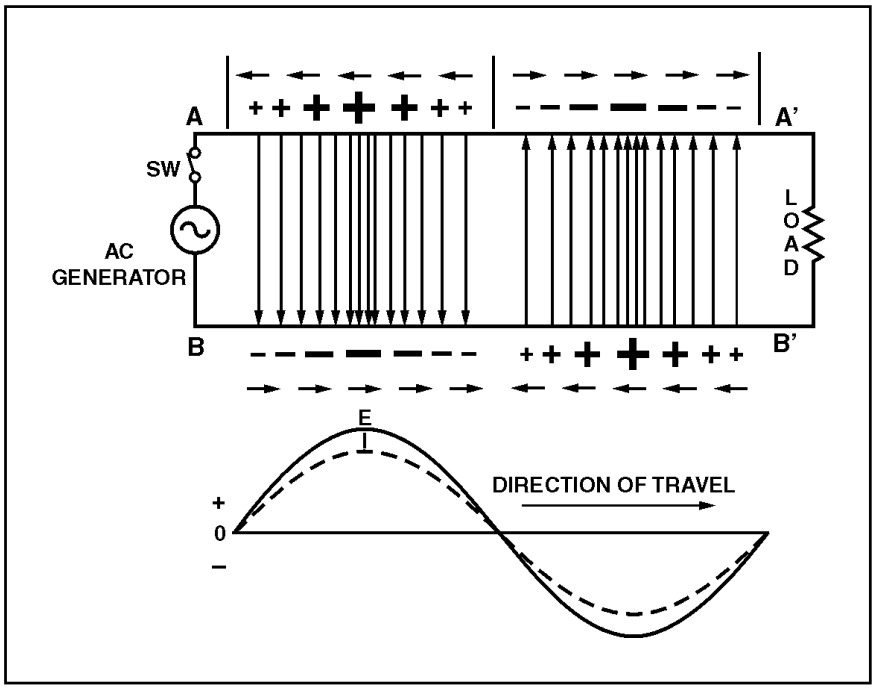


Figure 3-19. AC Voltage Applied to a Transmission Line

3-64. In this illustration the conventional lines of force represent the electric fields. For simplicity, the magnetic fields are not shown. Points of charge are indicated by plus (+) and minus (-) signs, the larger signs indicating points of higher amplitude of both voltage and current. Short arrows indicate direction of current (electron flow). The waveform drawn below the transmission line represents the voltage (E) and current (I) waves. The line is assumed to be infinite in length so there is no reflection. Thus, traveling sinusoidal voltage and current waves continually travel in phase from the generator toward the load, or far end of the line. Waves traveling from the generator to the load are called incident waves. Waves traveling from the load back to the generator are called reflected waves and are explained later in this chapter.

DC Applied to an Infinite Line

3-65. Figure 3-20 shows a battery connected to a circuit that is the equivalent of a transmission line. In this line, the series resistance and shunt conductance are not shown. Also, in the discussion that follows, the line is considered to have no losses.

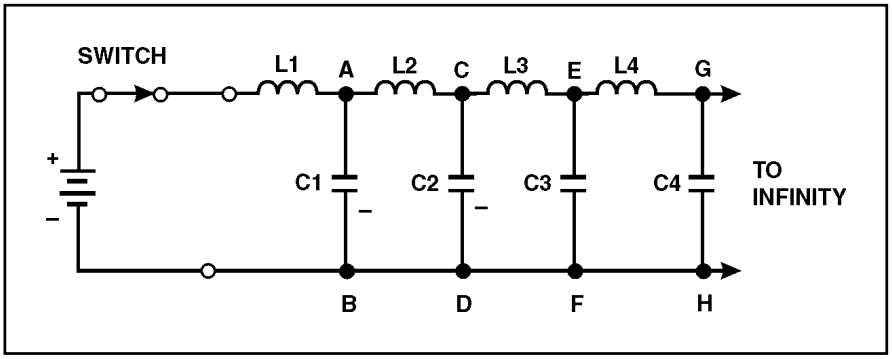


Figure 3-20. DC Applied to an Equivalent Transmission Line

3-66. As the switch shown in figure 3-20 is closed, the battery voltage is applied to the input terminals of the line. Now, C1 has no charge and appears, effectively, as a short circuit across points A and B. The full battery voltage appears across inductor L1. Inductor L1 opposes the change of current (0 now) and limits the rate of charge of C1.

3-67. Capacitor C2 cannot begin to charge until after C1 has charged. No current can flow beyond points A and B until C1 has acquired some charge. As the voltage across C1 increases, current through L2 and C2 charges C2. This action continues down the line and charges each capacitor, in turn, to the battery voltage. Thus, a voltage wave is traveling along the line. Beyond the wavefront, the line is uncharged. Because the line is infinitely long, there will always be more capacitors to be charged, and current will not stop flowing. Thus, current will flow indefinitely in the line.

3-68. Notice that current flows to charge the capacitors along the line. The flow of current is not advanced along the line until a voltage is developed across each preceding capacitor. In this manner voltage and current move down the line together in phase.

AC Applied to an Infinite Line

3-69. An RF line displays similar characteristics when an AC voltage is applied to its sending end or input terminals. In figure 3-21, view A, an AC voltage is applied to the line represented by the circuit shown.

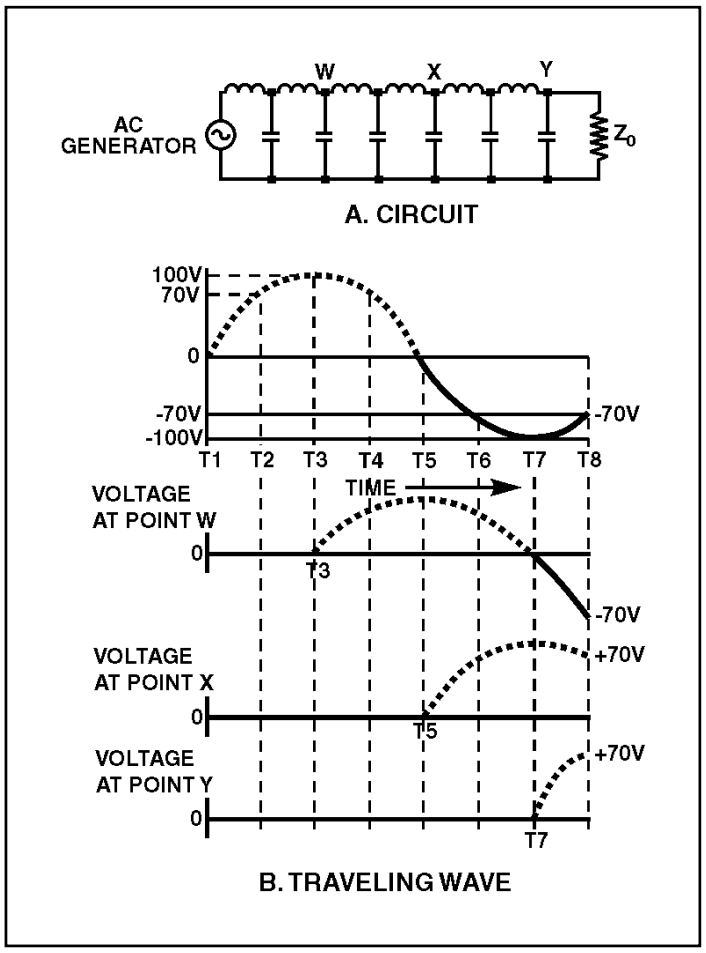


Figure 3-21. AC Applied to an Equivalent Transmission Line

3-70. In figure 3-21, view B, the generator voltage starts from zero (T1) and produces the voltage shown. As soon as a small voltage change is produced, it starts its journey down the line while the generator continues to produce new voltages along a sine curve. At T2 the generator voltage is 70 volts. The voltages still move along the line until, at T3, the first small change arrives at point W, and the voltage at that point starts increasing. At T5, the same voltage arrives at point X on the line. Finally, at T7, the first small change arrives at the receiving end of the line. Meanwhile, all the changes in the sine wave produced by the generator pass each point in turn. The amount of time required for the changes to travel the length of the line is the same as that required for a DC voltage to travel the same distance.

3-71. At T7, the voltage at the various points on the line is as follows:

- At the generator: –100 V
- At point W: 0 V
- At point X: +100 V
- At point Y: 0 V

3-72. If these voltages are plotted along the length of the line, the resulting curve is like the one shown in figure 3-22, view A. Note that such a curve of instantaneous voltages resembles a sine wave. The changes in voltage that occur between T7 and T8 are as follows:

- At the generator: Rise from –100 V to –70 V
- At point W: Drop from 0 V to –70 V
- At point X: Drop from +100 V to +70 V
- At point Y: Rise from 0 V to +70 V

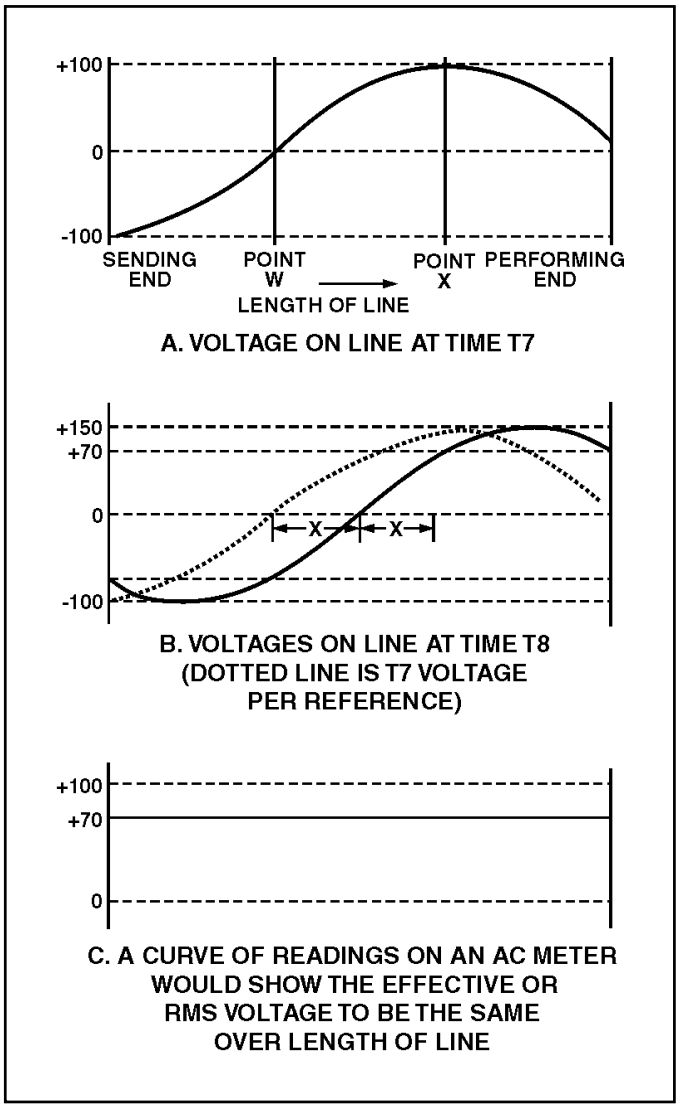


Figure 3-22. Instantaneous Voltages along a Transmission Line

3-73. A plot of these new voltages produces the solid curve shown in figure 3-22, view B. For reference, the curve from T7 is drawn as a dotted line. The solid curve has exactly the same shape as the dotted curve, but has moved to the right by the distance X. Another plot at T9 would show a new curve similar to the one at T8, but moved to the right by the distance Y.

3-74. By analyzing the points along the graph just discussed, you should be able to see that the actions associated with voltage changes along an RF line are as follows:

- All instantaneous voltages of the sine wave produced by the generator travel down the line in the order they are produced.
- At any point, a sine wave can be obtained if all the instantaneous voltages passing the point are plotted. An oscilloscope can be used to plot these values of instantaneous voltages against time.
- The instantaneous voltages (oscilloscope displays) are the same in all cases except that a phase difference exists in the displays seen at different points along the line. The phase changes continually with respect to the generator until the change is 360 degrees over a certain length of line.
- All parts of a sine wave pass every point along the line. A plot of the readings of an AC meter (which reads the effective value of the voltage over a given time) taken at different points along the line shows that the voltage is constant at all points (see figure 3-22, view C).
- Because the line is terminated with a resistance equal to Z_0, the energy arriving at the end of the line is absorbed by the resistance.

VELOCITY OF WAVE PROPAGATION

3-75. If a voltage is initially applied to the sending end of a line, that same voltage will appear later some distance from the sending end. This is true regardless of any change in voltage, whether the change is a jump from zero to some value or a drop from some value to zero. The voltage change will be conducted down the line at a constant rate.

3-76. Recall that the inductance of a line delays the charging of the line capacitance. The velocity of propagation is therefore related to the values of L and C. If the inductance and capacitance of the RF line are known, the time required for any waveform to travel the length of the line can be determined. To see how this works, observe the following relationship:

$$Q = IT$$

This formula shows that the total charge or quantity is equal to the current multiplied by the time the current flows. Also—

$$Q = CE$$

This formula shows that the total charge on a capacitor is equal to the capacitance multiplied by the voltage across the capacitor.

3-77. If the switch in figure 3-23 is closed for a given time, the quantity (Q) of electricity leaving the battery can be computed by using the equation Q = IT. The electricity leaves the battery and goes into the line, where a charge is built up on the capacitors. The amount of this charge is computed by using the equation Q = CE.

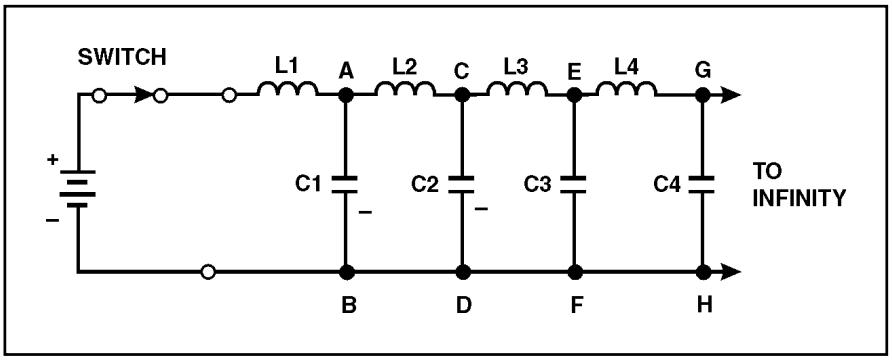


Figure 3-23. DC Applied to an Equivalent Transmission Line

3-78. Because none of the charge is lost, the total charge leaving the battery during T is equal to the total charge on the line. Therefore:

$$Q = IT = CE$$

3-79. As each capacitor accumulates a charge equal to CE, the voltage across each inductor must change. As C1 in figure 3-23 charges to a voltage of E, point A rises to a potential of E volts while point B is still at zero volts. This makes E appear across L2. As C2 charges, point B rises to a potential of E volts as did point A. At this time, point B is at E volts and point C rises. Thus, there is a continuing action of voltage moving down the infinite line.

3-80. In an inductor, these circuit components are related, as shown in the formula—

$$E = L \left(\frac{\Delta I}{\nabla T} \right)$$

3-81. 1-79. This shows that the voltage across the inductor is directly proportional to inductance and the change in current, but inversely proportional to a change in time. Because current and time start from zero, the change in time (ΔT) and the change in current (ΔI) are equal to the final time (T) and final current (I). For this case the equation becomes:

$$ET = LI$$

3-82. If voltage E is applied for time (T) across the inductor (L), the final current (I) will flow. The following equations show how T, L, and C are related:

$$ET = LI$$

$$IT = CE$$

3-83. For convenience, you can find T in terms of L and C by multiplying the left and right members of each of the above equations, and solving for T, as follows:

$$(IT)(ET) = (CE)(LI)$$

$$EIT^2 = LCEI$$

$$T^2 = LC$$

$$T = \sqrt{LC}$$

3-84. This final equation is used for finding the time required for a voltage change to travel a unit length, because L and C are given in terms of unit length. The velocity of the waves may be found by the following equation, where D is the physical length of a unit:

$$v = \frac{D}{T} \text{ Or } v = \frac{D}{\sqrt{LC}}$$

3-85. This is the rate at which the wave travels over a unit length. The units of L and C are henrys and farads, respectively. T is in seconds per unit length and V is in unit lengths per second.

DETERMINING CHARACTERISTIC IMPEDANCE

3-86. As previously discussed, an infinite transmission line exhibits a definite input impedance. This impedance is the characteristic impedance and is independent of line length. The exact value of this impedance is the ratio of the input voltage to the input current. If the line is infinite or is terminated in a resistance equal to the characteristic impedance, voltage and current waves traveling the line are in phase. Recall the following equations:

$$ET = LI$$

$$IT = CE$$

To determine the characteristic impedance or voltage-to-current ratio, use the following procedure:

Divide the equations:

$$ET = LI \text{ and } IT = CE$$

$$\frac{ET}{IT} = \frac{LI}{CE}$$

Multiply the result by $\frac{E}{I}$

$$\frac{E^2T}{I^2T} = \frac{LIE}{CEI}$$

Simplify:

$$\frac{E^2}{I^2} = \frac{L}{C}$$

Take the square root:

$$\frac{E}{I} = \sqrt{\frac{L}{C}} = Z_0 \text{ (characteristic impedance)}$$

3-87. A problem using this equation illustrates how to determine the characteristics of a transmission line.

Assume that the line shown in figure 3-23 is 1,000 feet long. A 100-foot (approximately 30.5 meter) section is measured to determine L and C. The section is found to have an inductance of 0.25 millihenry and a capacitance of 1000 picofarads. Find the characteristic impedance of the line and the velocity of the wave on the line. The characteristic impedance is—

$$Z_0 = \sqrt{LC}$$

$$Z_0 = \sqrt{\frac{0.25 \times 10^{-3}}{1000 \times 10^{-12}}}$$

$$Z_0 = \sqrt{0.25 \times 10^{6}}$$

$$Z_0 = 0.5 \times 10^{3}$$

$$Z_0 = 500\Omega$$

If any other unit length had been considered, the values of L and C would be different, but their ratio would remain the same as would the characteristic impedance.

The formula for T is:

$$T = \sqrt{LC}$$

$$T = \sqrt{0.25 \times 10^{-3} \times 1000 \times 10^{-12}}$$

$$T = \sqrt{0.25 \times 10^{-12}}$$

$$T = 0.5 \times 10^{-6} \text{ second}$$

$$T = 0.5 \text{ microsecond}$$

The formula for the velocity of a wave is:

$$V = \frac{D}{T}$$

$$V = \frac{100 \text{ feet}}{0.5 \times 10^{-6} \text{ second}}$$

$$V = 200 \times 10^{6} \text{ feet/second}$$

$$V = 200{,}000{,}000 \text{ feet/second}$$

REFLECTIONS ON A TRANSMISSION LINE

3-88. Transmission line characteristics are based on an infinite line. A line cannot always be terminated in its characteristic impedance because it is sometimes operated as an open-ended line and at other times as a short-circuit at the receiving end. If the line is open-ended, it has a terminating impedance that is infinitely large. If a line is not terminated in characteristic impedance (Z_0), it is said to be finite.

3-89. When a line is not terminated in characteristic impedance, the incident energy is not absorbed but is returned along the only path available—the

transmission line. Thus, the behavior of a finite line may be quite different from that of the infinite line.

Reflection of DC Voltage from an Open Circuit

3-90. The equivalent circuit of an open-ended transmission line is shown in figure 3-24, view A. Again, losses are to be considered as negligible, and L is lumped in one branch. Assume that (1) the battery in this circuit has an internal impedance equal to the characteristic impedance of the transmission line ($Z_i = Z_0$); (2) the capacitors in the line are not charged before the battery is connected; and (3) because the line is open-ended, the terminating impedance is infinitely large.

3-91. When the battery is connected to the sending end as shown in figure 3-24, view A, a negative voltage moves down the line. This voltage charges each capacitor, in turn, through the preceding inductor. Because Z_i equals Z_0, one-half the applied voltage will appear across the internal battery impedance, Z_i, and one-half across the impedance of the line, Z_0. Each capacitor is then charged to E/2 (view B). When the last capacitor in the line is charged, there is no voltage across the last inductor and current flow through the last inductor stops. With no current flow to maintain it, the magnetic field in the last inductor collapses and forces current to continue to flow in the same direction into the last capacitor. Because the direction of current has not changed, the capacitor charges in the same direction, thereby increasing the charge in the capacitor. Because the energy in the magnetic field equals the energy in the capacitor, the energy transfer to the capacitor doubles the voltage across the capacitor. The last capacitor is now charged to E volts and the current in the last inductor drops to zero.

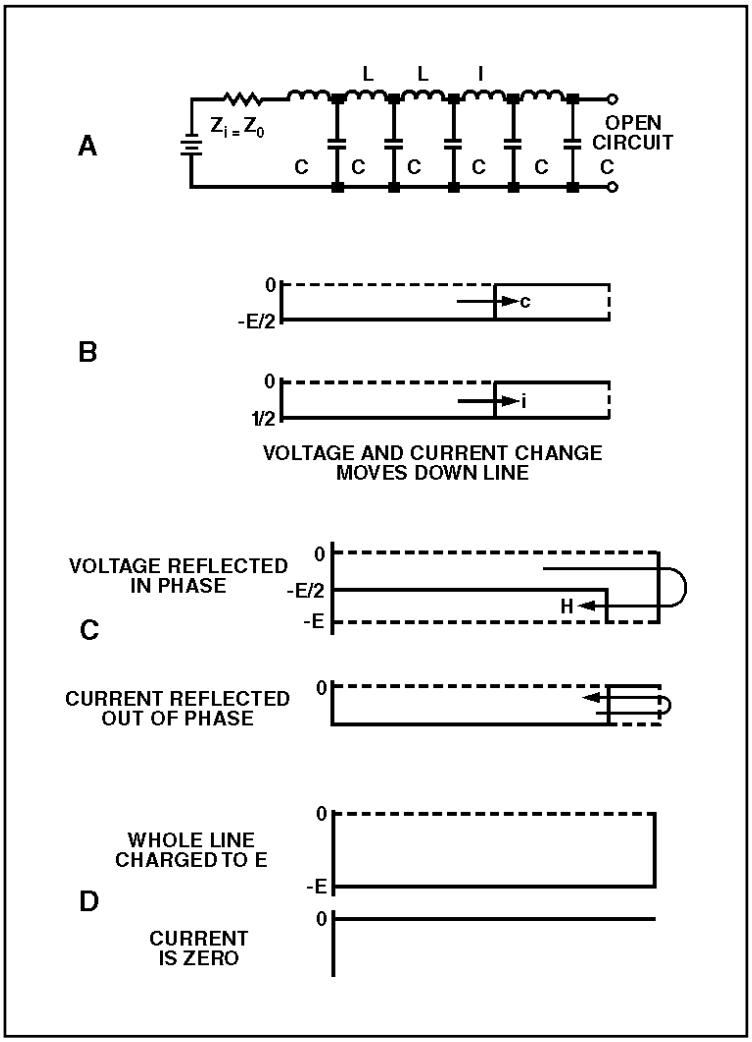


Figure 3-24. Reflection from an Open-Ended Line

3-92. At this point, the same process takes place with the next to the last inductor and capacitor. When the magnetic field about the inductor collapses, current continues to flow into the next to the last capacitor, charging it to E volts. This action continues backward down the line until the first capacitor has been fully charged to the applied voltage. This change of voltage, moving backward down the line, can be thought of in the following manner. The voltage, arriving at the end of the line, finds no place to go and returns to the sending end with the same polarity (figure 3-24, view C). Such action is called reflection.

3-93. When a reflection of voltage occurs on an open-ended line, the polarity is unchanged. The voltage change moves back to the source, charging each capacitor in turn until the first capacitor is charged to the source voltage and the action stops (figure 3-24, view D). As each capacitor is charged, current in each inductor drops to zero, effectively reflecting the current with the opposite polarity (view C). Reflected current of opposite polarity cancels the original current at each point, and the current drops to zero at that point.

When the last capacitor is charged, the current from the source stops flowing (view D).

3-94. Important facts to remember in the reflection of DC voltages in open-ended lines are—

- Voltage is reflected from an open end without change in polarity, amplitude, or shape.
- Current is reflected from an open end with opposite polarity and without change in amplitude or shape.

Reflection of DC Voltage from a Short Circuit

3-95. A short-circuited line affects voltage change differently than the way an open-circuited line affects it. The voltage across a perfect short circuit must be zero; therefore, no power can be absorbed in the short, and the energy is reflected toward the generator.

3-96. The initial circuit is shown in figure 3-25, view A. The initial voltage and current waves (view B) are the same as those given for an infinite line. In a short-circuited line the voltage change arrives at the last inductor in the same manner as the waves on an open-ended line. In this case, however, there is no capacitor to charge. The current through the final inductor produces a voltage with the polarity shown in view C. When the field collapses, the inductor acts as a battery and forces current through the capacitor in the opposite direction, causing it to discharge (view D). Because the amount of energy stored in the magnetic field is the same as that in the capacitor, the capacitor discharges to zero.

3-97. Now there is no voltage to maintain the current through the next to the last inductor. Therefore, this inductor discharges the next to the last capacitor.

3-98. As each capacitor is discharged to zero, the next inductor effectively becomes a new source of voltage. The amplitude of each of these voltages is equal to E/2, but the polarity is the opposite of the battery at the input end of the line. The collapsing field around each inductor, in turn, produces a voltage that forces the current to continue flowing in the same direction, adding to the current from the source to make it 2I. This action continues until all the capacitors are discharged (view E).

3-99. Reflected waves from a short-circuited transmission line are characterized as follows:

- The reflected voltage has the opposite polarity but the same amplitude as the incident wave.
- The reflected current has the same polarity and the same amplitude as the incident current.

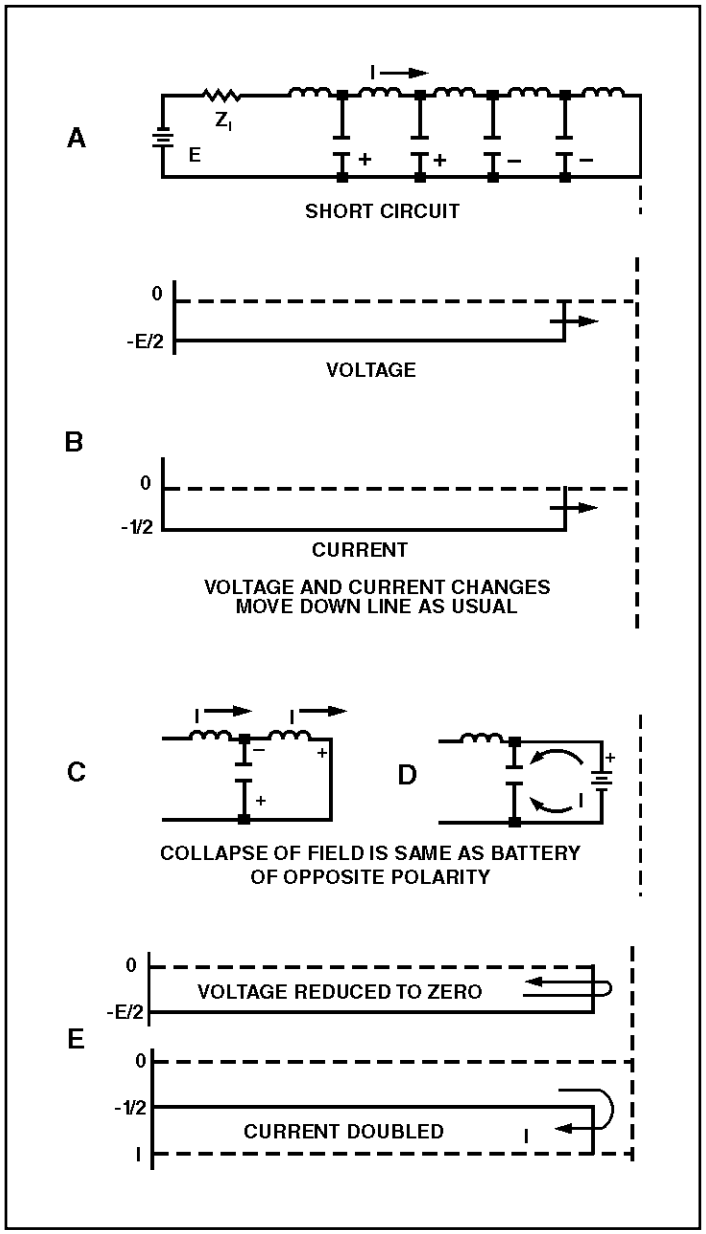


Figure 3-25. Reflection from a Short-Circuited Line

Reflection of AC Voltage from an Open Circuit

3-100. In most cases where RF lines are used, the voltages applied to the sending end are AC voltages. The action at the receiving end of the line is exactly the same for AC as for DC. In the open-ended line, as shown in figure 3-26, view A, the generated AC voltage is distributed along the line, shown in view B. This voltage is distributed in such a way that as each instantaneous voltage arrives at the end, it is reflected with the same polarity and amplitude. When AC is used, this reflection is in phase. Each of the reflected voltages travels back along the line until it reaches the generator. If the generator impedance is the same as the line impedance, energy arriving at the generator is absorbed and not reflected again. Now two voltages are on the line.

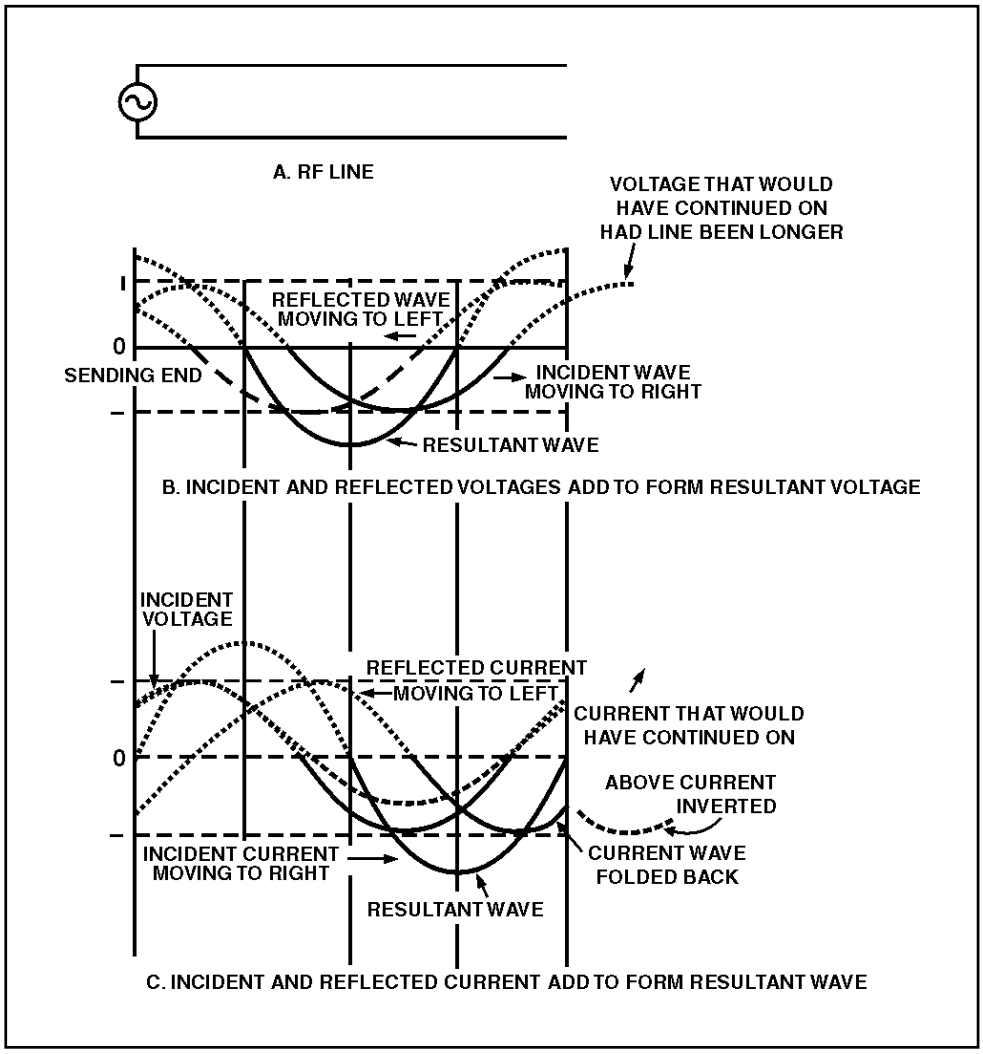


Figure 3-26. Formation of Standing Waves

3-101. View B of figure 3-26 shows how two waves of the same frequency and amplitude moving in opposite directions on the same conductor will combine to form a resultant wave. The small solid line is moving steadily from left to right and is the incident wave (from the source). The broken-line waveform is moving from right to left and is the reflected wave. The resultant waveform, the heavy line, is found by algebraically adding instantaneous values of the two waveforms. The resultant waveform has an instantaneous peak amplitude that is equal to the sum of the peak amplitudes of the incident and reflected waves. Because most indicating instruments are unable to separate these voltages, they show the vector sum. An oscilloscope is usually used to study the instantaneous voltages on RF lines.

3-102. Because two waves of voltage are moving on the line, you need to know how to distinguish between the two. The voltages moving toward the receiving end are called incident voltages, and the whole waveshape is called the incident wave. The wave moving back to the sending end after reflection

is called the reflected wave. The resultant voltage curve (view B of figure 3-26) shows that the voltage is maximum at the end of the line, a condition that occurs across an open circuit.

3-103. Another step in investigating the open-circuited RF line is to see how the current waves act. The incident current wave is the solid line in figure 3-26, view C. The voltage is represented by the dotted line. The current is in phase with the voltage while traveling toward the receiving end. At the end of the line, the current is reflected in the opposite polarity; that is, it is shifted 180 degrees in phase, but its amplitude remains the same. Dashed lines show the reflected wave of current in view C. The heavy-line curve represents the sum of the two instantaneous currents and is the resultant wave. Notice that current is zero at the end of the line. This is reasonable, because there can be no current flow through an open circuit.

3-104. Views B and C of figure 3-26 show the voltage and current distribution along a transmission line at a point about one-eighth wavelength after a maximum voltage or current reaches the end of the line. Because the instantaneous values are continuously changing during the generation of a complete cycle, a large number of these pictures are required to show the many different relationships.

3-105. Figure 3-27 shows the incident and reflected waveshapes at several different times. The diagrams in the left column of figure 3-27 (representing voltage) show the incident wave and its reflection without change in polarity. In figure 3-27, waveform (1), the incident wave and the reflected wave are added algebraically to produce the resultant wave indicated by the heavy line. In waveform (2), a zero point preceding the negative-going cycle of the incident wave is at the end of the line. The reflected wave and incident wave are 180 degrees out of phase at all points. (The reflected wave is the positive cycle that just preceded the negative cycle now approaching the end of the line.) The resultant of the incident and reflected waves is zero at all points along the line. In waveform (3), the waves have moved 1/8 wavelength along the line; the incident wave has moved 45 degrees to the right, and the reflected wave has moved 45 degrees to the left. The resultant voltage, shown by the heavy line, has a maximum negative at the end of the line and a maximum positive 1/2 wavelength from the end of the line.

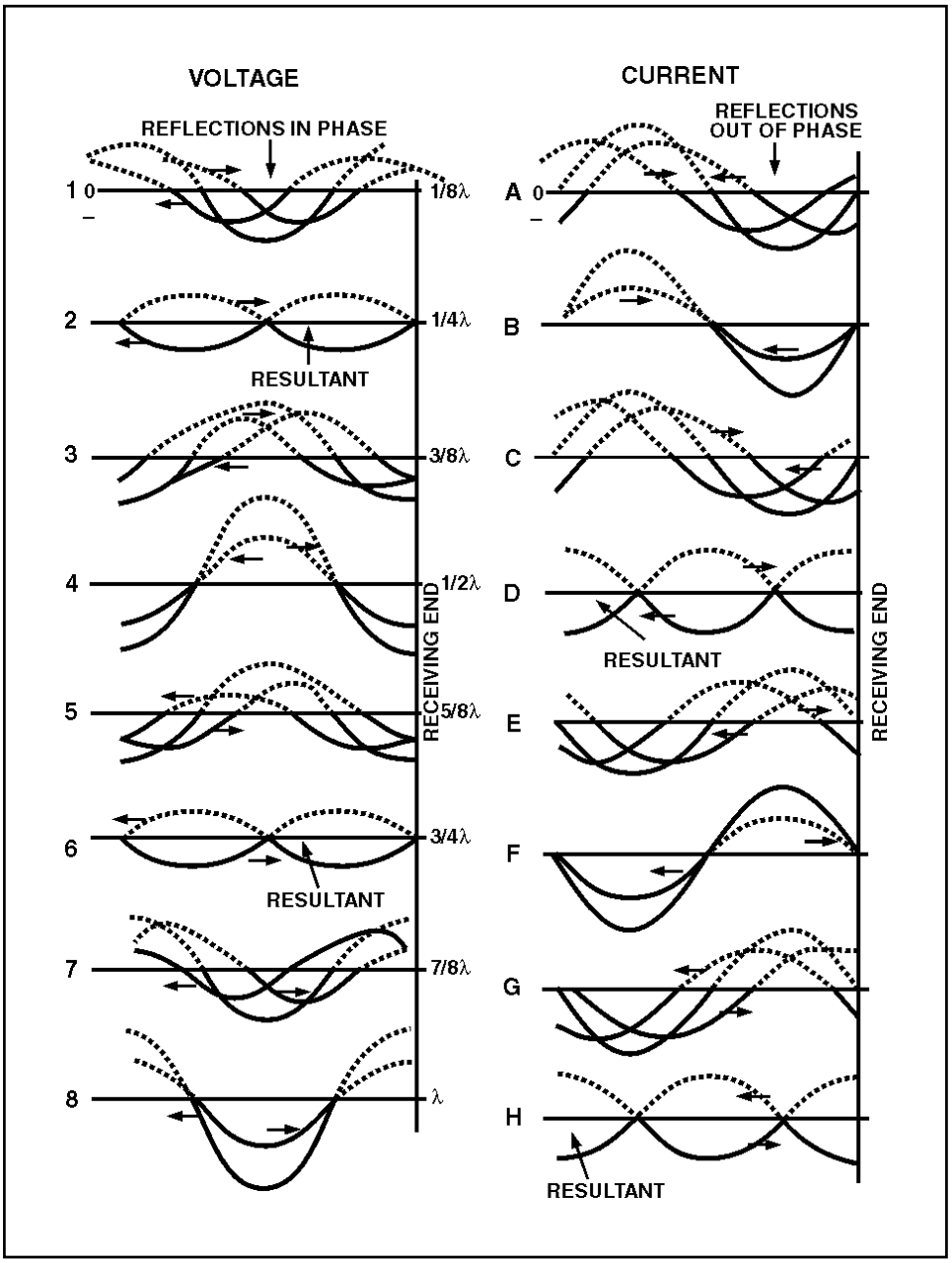


Figure 3-27. Instantaneous Values of Incident and Reflected Waves on an Open-Ended Line

3-106. In waveform (4) of figure 3-27, the incident wave is at a maximum negative value at the end of the line. The wave has moved another 45 degrees to the right from the wave in the preceding illustration. The reflected wave has also moved 45 degrees, but to the left. The reflected wave is in phase with the incident wave. The resultant of these two waves, shown by the dark line, again has a negative maximum at the end of the line and a positive maximum 1/2λ from the end of the line. Notice that these maxima have a greater amplitude than those in waveform (3).

3-107. In waveform (5) of figure 3-27, the incident wave has moved another 45 degrees to the right and the reflected wave 45 degrees to the left. The resultant again is maximum negative at the end and positive maximum 1/2 wavelength from the end. The maxima are lower than those in waveform (4). In waveform (6), the incident and reflected wave have moved another 1/8λ. The two waves again are 180 degrees out of phase, giving a resultant wave with no amplitude. The incident and reflected waves continue moving in opposite directions, adding to produce the resultant waveshapes shown in waveforms (7) and (8). Notice that the maximum voltage in each resultant wave is at the end and 1/2λ from the end.

3-108. Study each part of figure 3-27 carefully and you will get a clear picture of how the resultant waveforms of voltage are produced. You will also see that the resultant voltage wave on an open-ended line is always zero at 1/4λ and 3/4λ from the end of the transmission line. Because the zero and maximum points are always in the same place, the resultant of the incident and the reflected wave is called a standing wave of voltage.

3-109. The right-hand column in figure 3-27 shows the current waveshapes on the open-ended line. Because the current is reflected out of phase at an open end, the resultant waveshapes differ from those for voltage. The two out-of-phase components always cancel at the end of the transmission line, so the resultant is always zero at that point. If you check all the resultant waveshapes shown in the right-hand column of figure 3-27, you will see that a zero point always occurs at the end and at a point 1/2λ from the end. Maximum voltages occur 1/4λ and 3/4λ from the end.

3-110. When an AC meter is used to measure the voltages and currents along a line, the polarity is not indicated. If you plot all the current and voltage readings along the length of the line, you will get curves like the ones shown in figure 3-28. Notice that all are positive. These curves are the conventional method of showing current and voltage standing waves on RF lines.

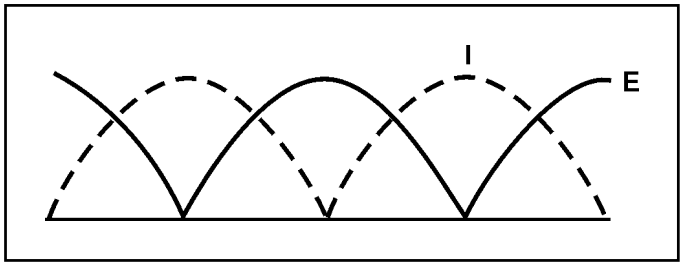


Figure 3-28. Conventional Picture of Standing Waves

3-111. When an RF line is terminated in a short circuit, reflection is complete, but the effect on voltage and current differs from that in an open-ended line. Voltage is reflected in opposite phase, while current is reflected in phase. Again refer to the series of pictures shown in figure 3-27. However, this time the left column represents current, because it shows reflection in phase; and the right column of pictures now represents the voltage changes on the shorted line, because it shows reflection out of phase.

3-112. The composite diagram in figure 3-29 shows all resultant curves on a full-wavelength section of line over a complete cycle. Notice that the amplitude of the voltage varies between zero and maximum in both directions at the center and at both ends as well, but one-fourth of the distance from each end the voltage is always zero. The resultant waveshape is referred to as a standing wave of voltage. Standing waves, then, are caused by reflections, which occur only when the line is not terminated in its characteristic impedance.

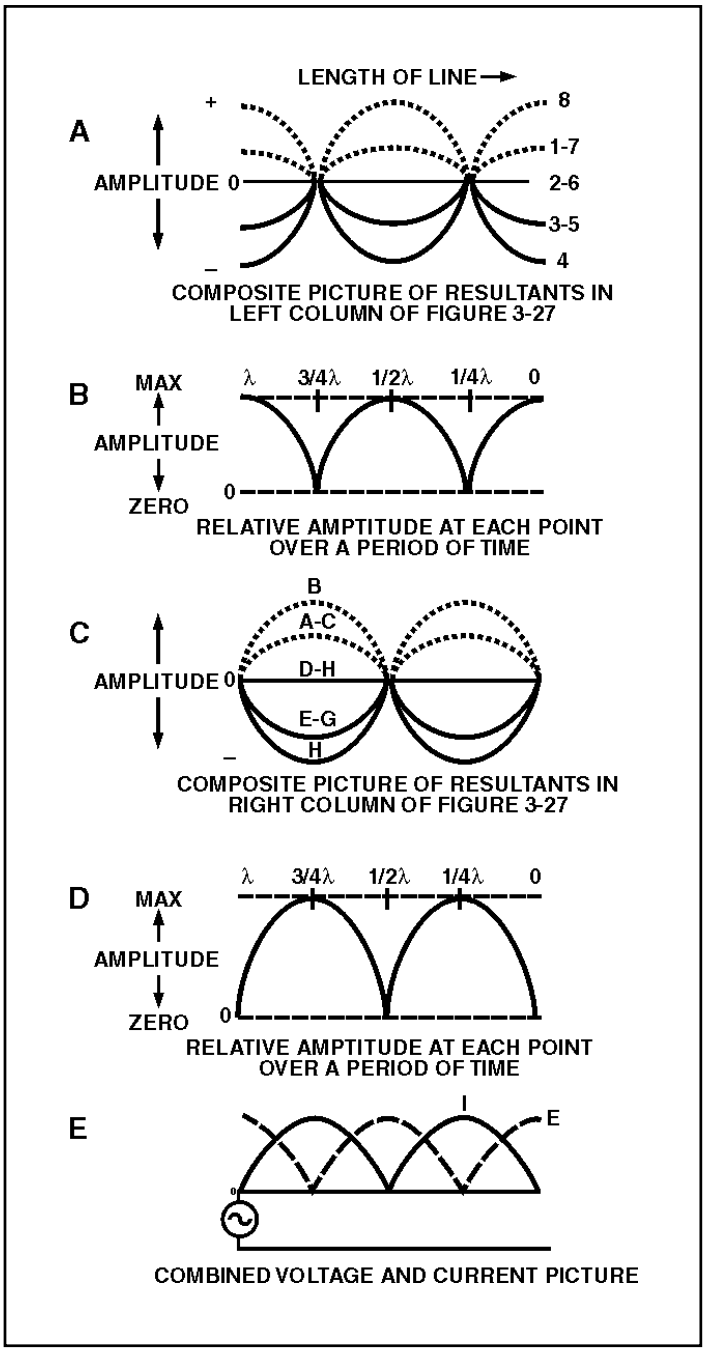


Figure 3-29. Composite Results of Instantaneous Waves

3-113. The voltage at the center and the ends varies at a sinusoidal rate between the limits shown. At the one-fourth and three-fourths points, the voltage is always zero. A continuous series of diagrams such as these is difficult to see with conventional test equipment, which reads the effective or average voltage over several cycles. The curve of amplitude over the length of line for several cycles is shown in figure 3-29, view B. A meter will read zero at the points shown and will show a maximum voltage at the center, no matter how many cycles pass.

3-114. As shown in figure 3-29, view D, the amplitude varies along the length of the line. In this case it is zero at the end and center but maximum at the one-fourth and three-fourths points. The entire diagram of the open-ended line conditions is shown in view E. The standing waves of voltage and current appear together. Observe that one is maximum when the other is minimum. The current and voltage standing waves are one-quarter cycle, or 90 degrees, out of phase with one another.

Reflection of AC Voltage from a Short Circuit

3-115. Reflection is complete when an RF line is terminated in a short circuit, but the effect on voltage and current differs from the effect obtained in an open-ended line. Voltage is reflected in opposite phase, while current is reflected in phase. Again look at the series of diagrams in figure 3-27. The left column represents current, and the right column shows voltage changes on the shorted line. The standard representation of standing waves on a shorted line is shown in figure 3-30; the voltage is a solid line, and the current is a dashed line. The voltage is zero at the end and center (1/2λ) and maximum at the 1/4λ and 3/4λ points, while the current is maximum at the end and center and minimum at the 1/4λ and 3/4λ points.

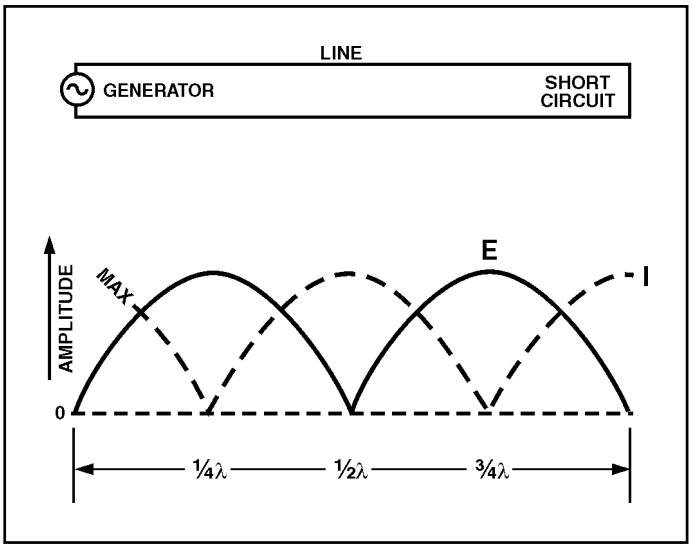


Figure 3-30. Standing Waves on a Shorted Line

3-116. As previously discussed, there are several differences between open and shorted lines in the voltage and current waves on transmission lines. Basic differences also appear in the standing-wave patterns for open and shorted lines. You can see these differences by comparing figure 3-29, view E

and figure 3-30. Notice that the current and voltage standing waves are shifted 90 degrees with respect to the termination. At the open end of a line, voltage is maximum (zero if there are no losses in the line). At a short circuit, current is maximum and voltage is minimum.

TERMINATING A TRANSMISSION LINE

3-117. A transmission line is either nonresonant or resonant. A nonresonant line is a line that has no standing waves of current and voltage. A resonant line is a line that has standing waves of current and voltage.

Nonresonant Lines

3-118. A nonresonant line is either infinitely long or terminated in its characteristic impedance. Because no reflections occur, all the energy traveling down the line is absorbed by the load that terminates the line. Because no standing waves are present, this type of line is sometimes spoken of as a flat line. In addition, because the load impedance of such a line is equal to Z_0, no special tuning devices are required to effect a maximum power transfer; hence, the line is also called an untuned line.

Resonant Lines

3-119. A resonant line has a finite length and is not terminated in its characteristic impedance. Therefore reflections of energy do occur. The load impedance is different from the Z_0 of the line; therefore, the input impedance may not be purely resistive but may have reactive components. Tuning devices are used to eliminate the reactance and to bring about maximum power transfer from the source to the line. Therefore, a resonant line is sometimes called a tuned line. The line also may be used for a resonant or tuned circuit.

3-120. A resonant line is sometimes said to be resonant at an applied frequency. This means that at one frequency the line acts as a resonant circuit. It may act either as a high-resistive circuit (parallel resonant) or as a low-resistive circuit (series resonant). The line may be made to act in this manner by either open- or short-circuiting it at the output end and cutting it to some multiple of a quarter-wavelength.

3-121. At the points of voltage maxima and minima on a short-circuited or open-circuited line, the line impedance is resistive. On a short-circuited line, each point at an odd number of quarter-wavelengths from the receiving end has a high impedance (figure 3-31, view A). If the frequency of the applied voltage to the line is varied, this impedance decreases as the effective length of the line changes. This variation is exactly the same as the change in the impedance of a parallel-resonant circuit when the applied frequency is varied.

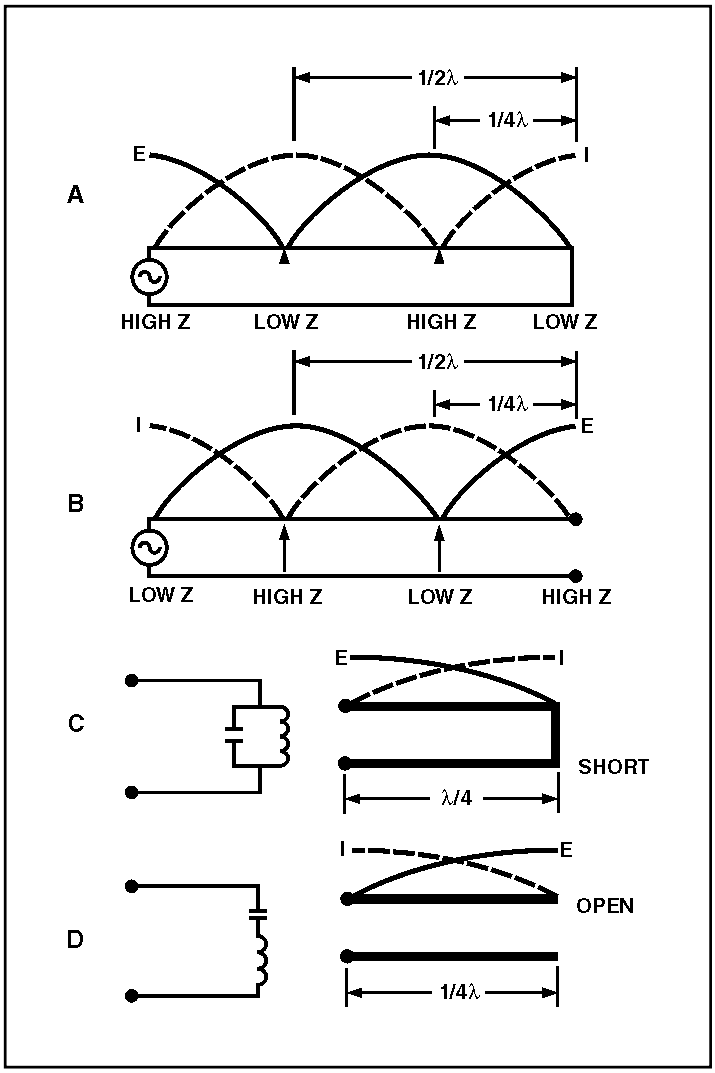


Figure 3-31. Sending-End Impedance of Various Lengths and Terminations

3-122. At all even numbered quarter-wavelength points from the short circuit, the impedance is extremely low. When the frequency of the voltage applied to the line is varied, the impedance at these points increases just as the impedance of a series-resonant circuit varies when the frequency applied to it is changed. The same is true for an open-ended line (figure 3-31, view B), except that the points of high and low impedance are reversed.

3-123. At this point let us review some of the characteristics of resonant circuits so we can see how resonant line sections may be used in place of LC circuits.

3-124. A parallel-resonant circuit has the following characteristics:

- At resonance, the impedance appears as a very high resistance. A loss-free circuit has infinite impedance (an open circuit). Other than at resonance, the impedance decreases rapidly.
- If the circuit is resonant at a point above the generator frequency (the generator frequency is too low), more current flows through the coil than through the capacitor. This happens because X_L decreases with a decrease in frequency, but X_C increases.

3-125. A series-resonant circuit has these characteristics:

- At resonance, the impedance appears as a very low resistance. A loss-free circuit has zero impedance (a short circuit). Other than at resonance, the impedance increases rapidly.
- If the circuit is resonant at a point above the generator frequency (the generator frequency is too low), then X_C is larger than X_L and the circuit acts capacitively.
- If the circuit is resonant at a point below the generator frequency (the generator frequency is too high), then X_L is larger than X_C and the circuit acts inductively.

3-126. Because the impedance a generator sees at the quarter-wave point in a shorted line is that of a parallel-resonant circuit, a shorted quarter-wavelength of line may be used as a parallel-resonant circuit (figure 3-31, view C). An open quarter-wavelength of line may be used as a series-resonant circuit (view D). The Q of such a resonant line is much greater than can be obtained with lumped capacitance and inductance.

Impedance for Various Lengths of Open Lines

3-127. In figure 3-32, the impedance (Z) the generator sees for various lengths of line is shown at the top. The curves above the letters of various heights show the relative value of the impedances presented to the generator for the various line lengths. The circuit symbols indicate the equivalent electrical circuits for the transmission lines at each particular length. The standing waves of voltage and current are shown on each length of line.

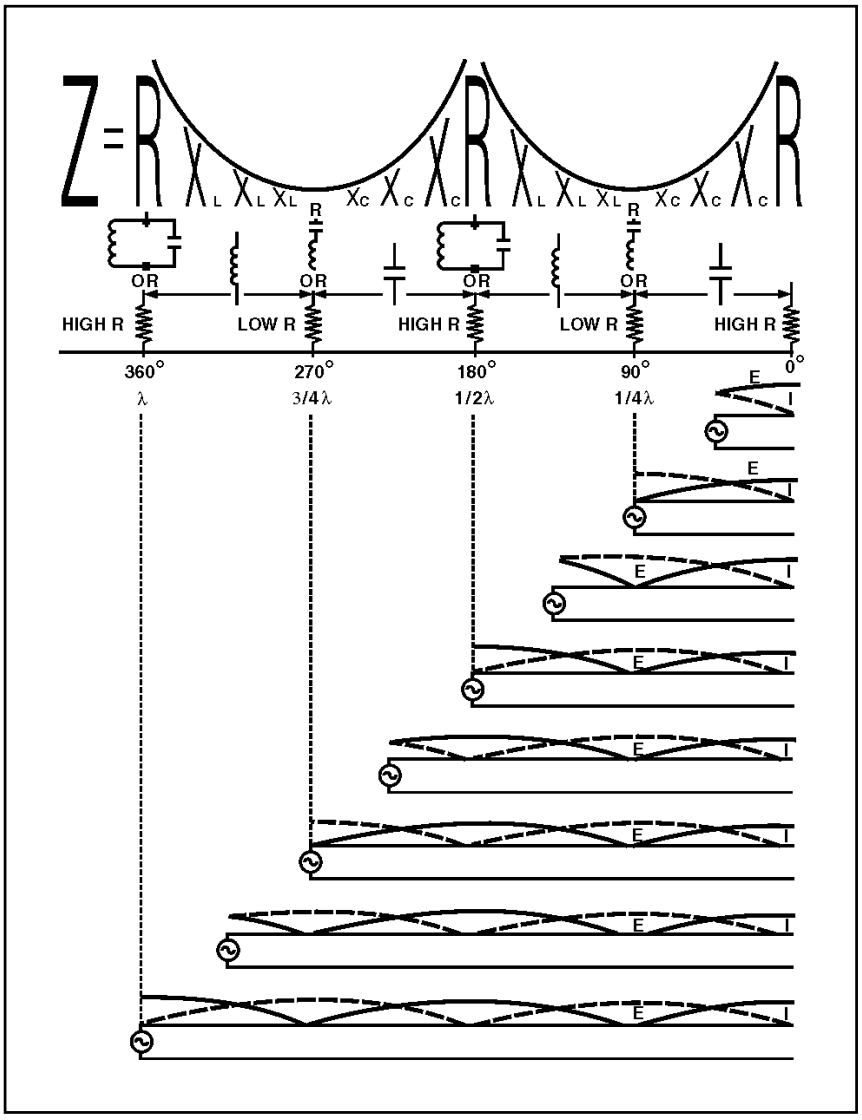


Figure 3-32. Voltage, Current, and Impedance on Open Line

3-128. At all odd quarter-wave points (1/4λ, 3/4λ, etc.), the voltage is minimum, the current is maximum, and the impedance is minimum. Thus, at all odd quarter-wave points, the open-ended transmission line acts as a series-resonant circuit. The impedance is equivalent to a very low resistance, prevented from being zero only by small circuit losses.

3-129. At all even quarter-wave points (1/2λ, 1λ, 3/2λ, etc.), the voltage is maximum, the current is minimum, and the impedance is maximum. Comparison of the line with an LC resonant circuit shows that at an even number of quarter-wavelengths, an open line acts as a parallel-resonant circuit. The impedance is therefore an extremely high resistance.

3-130. In addition, resonant open lines may also act as nearly pure capacitances or inductances. The illustration shows that an open line less than a quarter-wavelength long acts as a capacitance. Also, it acts as an

inductance from 1/4 to 1/2 wavelength, as a capacitance from 1/2 to 3/4 wavelength, and as an inductance from 3/4 to 1 wavelength, and so forth. A number of open transmission lines, with their equivalent circuits, are shown in the illustration.

Impedance of Various Lengths of Shorted Lines

3-131. Refer to figure 3-33 in the following discussion of the shorted line. At the odd quarter-wavelength points, the voltage is high, the current is low, and the impedance is high. Because these conditions are similar to those found in a parallel-resonant circuit, the shorted transmission line acts as a parallel-resonant circuit at these lengths.

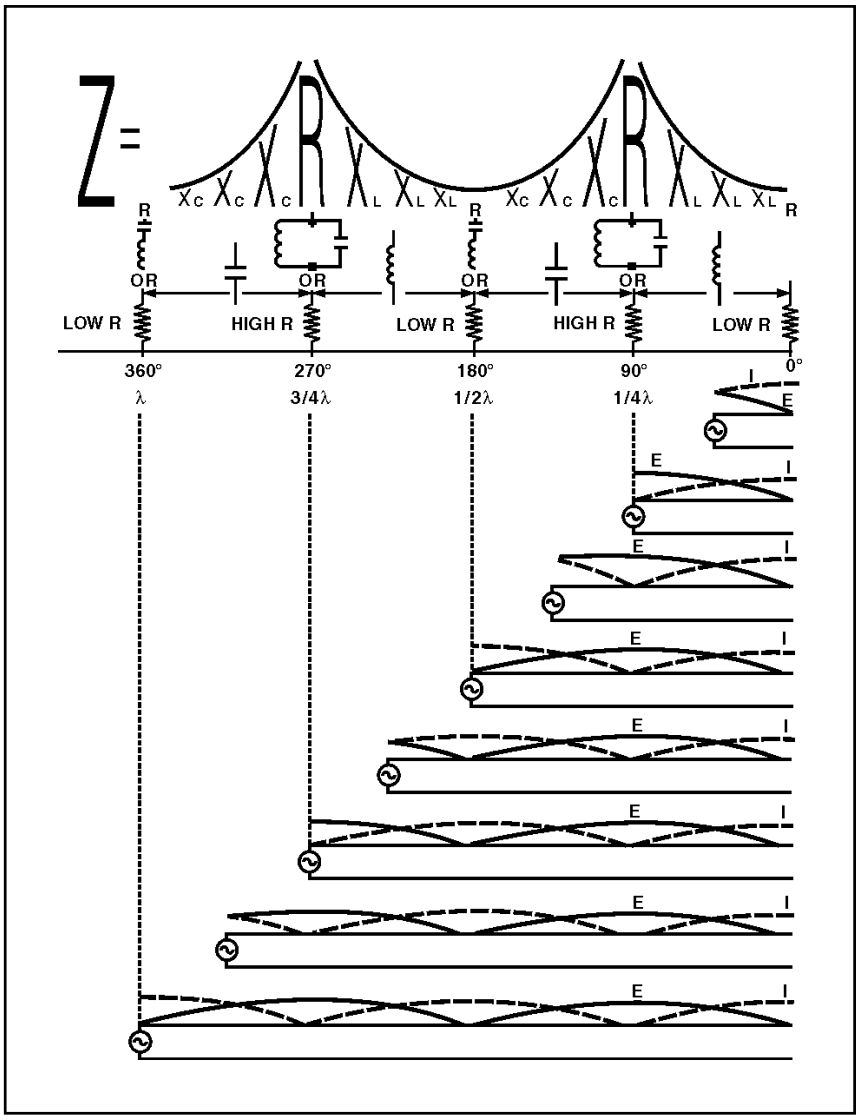


Figure 3-33. Voltage, Current, and Impedance on Shorted Line

3-132. At the even quarter-wave points in figure 3-33, voltage is minimum, current is maximum, and impedance is minimum. Because these characteristics are similar to those of a series-resonant LC circuit, a shorted transmission line whose length is an even number of quarter-wavelengths acts as a series-resonant circuit.

3-133. Resonant shorted lines, like open-end lines, also may act as pure capacitances or inductances. The illustration shows that a shorted line less than 1/4 wavelength long acts as an inductance. A shorted line with a length of from 1/4 to 1/2 wavelength acts as a capacitance. From 1/2 to 3/4 wavelength, the line acts as an inductance; and from 3/4 to 1 wavelength, it acts as a capacitance, and so on. The equivalent circuits of shorted lines of various lengths are shown in the illustration. Thus, properly chosen line segments may be used as parallel-resonant, series-resonant, inductive, or capacitive circuits.

EFFECT OF TERMINATION ON STANDING WAVES

3-134. There is a large variety of terminations for RF lines. Each type of termination has a characteristic effect on the standing waves on the line. From the nature of the standing waves, you can determine the type of termination that produces the waves.

TERMINATION IN Z_0

3-135. Termination in Z_0 (characteristic impedance) will cause a constant reading on an AC meter when it is moved along the length of the line. As illustrated in figure 3-34, view A, the curve—provided there are no losses in the line—will be a straight line. If there are losses in the line, the amplitude of the voltage and current will diminish as they move down the line (view B). The losses are due to DC resistance in the line itself.

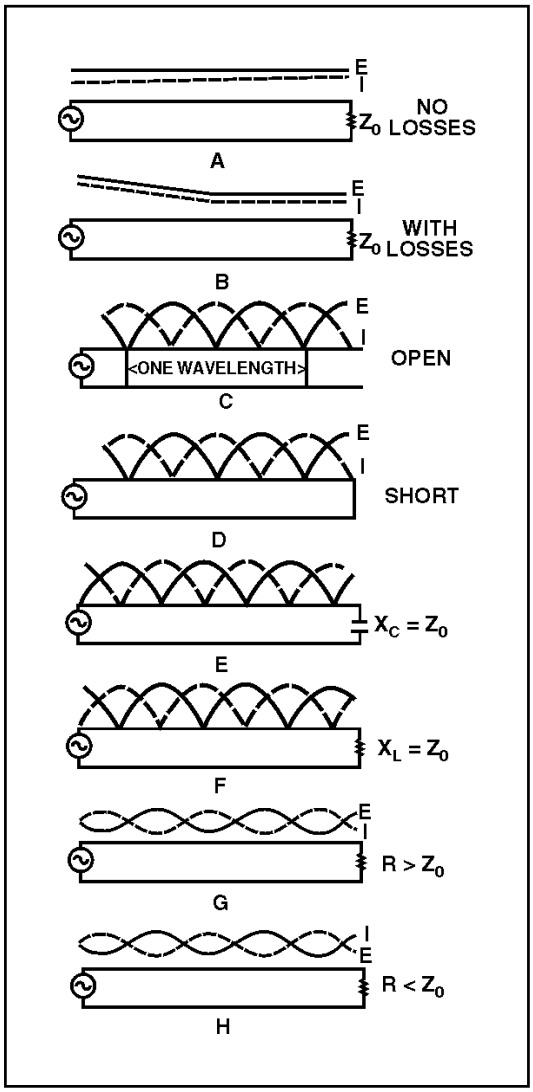


Figure 3-34. Effects of Various Terminations on Standing Waves

TERMINATION IN AN OPEN CIRCUIT

3-136. In an open-circuited RF line (figure 3-34, view C), the voltage is maximum at the end, but the current is minimum. The distance between two adjacent zero current points is 1/2λ, and the distance between alternate zero current points is 1λ. The voltage is zero at a distance of 1/4λ from the end of the line. This is true at any frequency. A voltage peak occurs at the end of the line, at 1/2λ from the end, and at each 1/2λ thereafter.

TERMINATION IN A SHORT CIRCUIT

3-137. On the line terminated in a short circuit, shown in figure 3-34, view D, the voltage is zero at the end and maximum at 1/4λ from the end. The current is maximum at the end, zero at 1/4λ from the end, and alternately maximum and zero every 1/4λ thereafter.

TERMINATION IN CAPACITANCE

3-138. When a line is terminated in capacitance, the capacitor does not absorb energy, but returns all of the energy to the circuit. This means there is 100 percent reflection. The current and voltage relationships are somewhat more involved than in previous types of termination. For this explanation, assume that the capacitive reactance is equal to the characteristic impedance (Z_0) of the line. Current and voltage are in phase when they arrive at the end of the line, but in flowing through the capacitor and the characteristic impedance connected in series, they shift in phase relationship. Current and voltage arrive in phase and leave out of phase. This results in the standing-wave configuration shown in figure 3-34, view E. The standing wave of voltage is minimum at a distance of exactly 1/8λ from the end. If the capacitive reactance is greater than Z_0 (smaller capacitance), the termination looks more like an open circuit; the voltage minimum moves away from the end. If the capacitive reactance is smaller than Z_0, the minimum moves toward the end.

TERMINATION IN INDUCTANCE

3-139. When the line is terminated in an inductance, both the current and voltage shift in phase as they arrive at the end of the line. When X_L is equal to Z_0, the resulting standing waves are as shown in figure 3-34, view F. The current minimum is located 1/8λ from the end of the line. When the inductive reactance is increased, the standing waves appear closer to the end. When the inductive reactance is decreased, the standing waves move away from the end of the line.

TERMINATION IN A RESISTANCE NOT EQUAL TO THE CHARACTERISTIC IMPEDANCE (Z_0)

3-140. Whenever the termination is not equal to Z_0, reflections occur on the line. For example, if the terminating element contains resistance, it absorbs some energy, but if the resistive element does not equal the Z_0 of the line, some of the energy is reflected. The amount of voltage reflected may be found by using the equation:

$$E_R = E_i \left(\frac{R_L - Z_O}{R_L + Z_O} \right)$$

Where:

E_R = the reflected voltage

E_i = the incident voltage

R_L = the terminating resistance

Z_0= the characteristic impedance of the line

3-141. If you try different values of RL in the preceding equation, you will find that the reflected voltage is equal to the incident voltage only when RL equals 0 or is infinitely large. When RL equals Z_0, no reflected voltage occurs. When RL is greater than Z_0, ER is positive, but less than Ei. As RL increases and approaches an infinite value, ER increases and approaches Ei in value. When RL is smaller than Z_0, ER has a negative value. This means that the reflected voltage is of opposite polarity to the incident wave at the termination of the line. As RL approaches zero, ER approaches Ei in value. The smaller the value of ER, the smaller is the peak amplitude of the standing waves and the higher are the minimum values.

TERMINATION IN A RESISTANCE GREATER THAN Z_0

3-142. When RL is greater than Z_0, the end of the line is somewhat like an open circuit; that is, standing waves appear on the line. The voltage maximum appears at the end of the line and also at half-wave intervals back from the end. The current is minimum (not zero) at the end of the line and maximum at the odd quarter-wave points. Because part of the power in the incident wave is consumed by the load resistance, the minimum voltage and current are less than for the standing waves on an open-ended line. Figure 3-34, view G, illustrates the standing waves for this condition.

TERMINATION IN A RESISTANCE LESS THAN Z_0

3-143. When R_L is less than Z_0, the termination appears as a short circuit. The standing waves are shown in figure 3-34, view H. Notice that the line terminates in a current loop (peak) and a voltage node (minimum). The values of the maximum and minimum voltage and current approach those for a shorted line as the value of RL approaches zero.

3-144. A line does not have to be any particular length to produce standing waves; however, it cannot be an infinite line. Voltage and current must be reflected to produce standing waves. For reflection to occur, a line must not be terminated in its characteristic impedance. Reflection occurs on lines terminated in opens, shorts, capacitances, and inductances, because the load absorbs no energy. If the line is terminated in a resistance not equal to the characteristic impedance of the line, some energy will be absorbed and the rest will be reflected.

3-145. The voltage and current relationships for open-ended and shorted lines are opposite to each other, as shown in figure 3-34, views C and D. The points of maximum and minimum voltage and current are determined from the output end of the line, because reflection always begins at that end.

STANDING-WAVE RATIO

3-146. The measurement of standing waves on a transmission line yields information about equipment operating conditions. Maximum power is absorbed by the load when $Z_L = Z_0$. If a line has no standing waves, the termination for that line is correct and maximum power transfer takes place.

3-147. You have probably noticed that the variation of standing waves shows how near the RF line is to being terminated in Z_0. A wide variation in voltage along the length means a termination far from Z_0. A small variation means termination near Z_0. Therefore, the ratio of the maximum to the minimum is a measure of the perfection of the termination of a line. This ratio is called the standing-wave ratio (SWR) and is always expressed in whole numbers. For example, a ratio of 1:1 describes a line terminated in its characteristic impedance (Z_0).

Voltage Standing-Wave Ratio

3-148. The ratio of maximum voltage to minimum voltage on a line is called the voltage standing-wave ratio (VSWR). Therefore—

$$VSWR = \frac{E_{max}}{E_{min}}$$

3-149. The vertical lines in the formula indicate that the enclosed quantities are absolute and that the two values are taken without regard to polarity. Depending on the nature of the standing waves, the numerical value of VSWR ranges from a value of 1 ($Z_L = Z_0$, no standing waves) to an infinite value for theoretically complete reflection. Because there is always a small loss on a line, the minimum voltage is never zero and the VSWR is always some finite value. However, if the VSWR is to be a useful quantity, the power losses along the line must be small in comparison to the transmitted power.

Power Standing-Wave Ratio

3-150. The square of the voltage standing-wave ratio is called the power standing-wave ratio (PSWR). Therefore—

$$PSWR = \frac{P_{max}}{P_{min}}$$

3-151. This ratio is useful because the instruments used to detect standing waves react to the square of the voltage. Because power is proportional to the square of the voltage, the ratio of the square of the maximum and minimum voltages is called the PSWR. In a sense, the name is misleading because the power along a transmission line does not vary.

Current Standing-Wave Ratio

3-152. The ratio of maximum to minimum current along a transmission line is called current standing-wave ratio (ISWR). Therefore—

$$ISWR = \frac{I_{max}}{I_{min}}$$

3-153. This ratio is the same as that for voltages. It can be used where measurements are made with loops that sample the magnetic field along a line. It gives the same results as VSWR measurements.

SUMMARY

This chapter has presented information on the characteristics of transmission lines. The information that follows summarizes the important points of this chapter.

Transmission lines are devices for guiding electrical energy from one point to another.

Input impedance is the ratio of voltage to current at the input end of a transmission line.

Output impedance is the ratio of voltage to current at the output end of the line.

Two-wire open lines are parallel lines and have uses such as power lines, rural telephone lines, and telegraph lines. This type of line has high radiation losses and is subject to noise pickup.

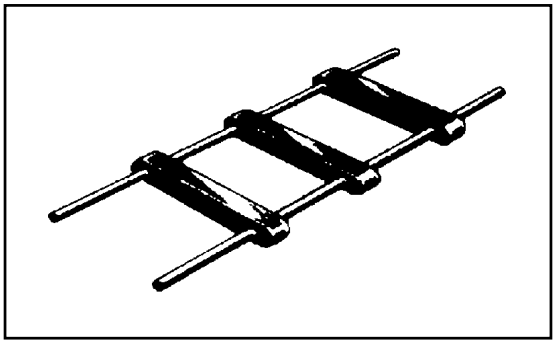


Figure 3-Sum 1. Two-Wire Open Line

The two-wire ribbon (twin lead) has parallel lines and is most often used to connect televisions to their antennas.

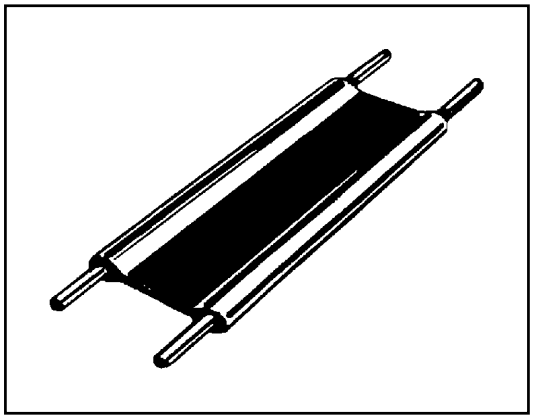


Figure 3-Sum 2. Two-Wire Ribbon Type Line

A twisted pair consists of two insulated wires twisted together. This line has high insulation loss.

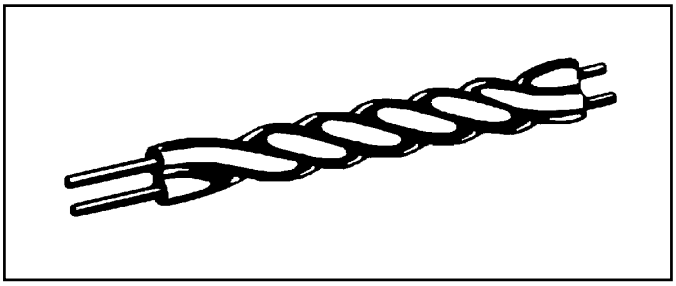


Figure 3-Sum 3. Twisted Pair

A shielded pair has parallel conductors separated by a solid dielectric and surrounded by copper braided tubing. The conductors are balanced to ground.

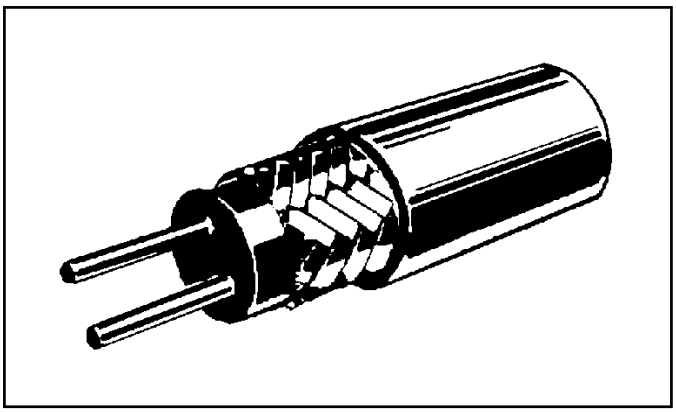


Figure 3-Sum 4. Shielded Pair

Rigid coaxial line contains two concentric conductors insulated from each other by spacers. Some rigid coaxial lines are pressurized with an inert gas to prevent moisture from entering. High-frequency losses are less than with other lines.

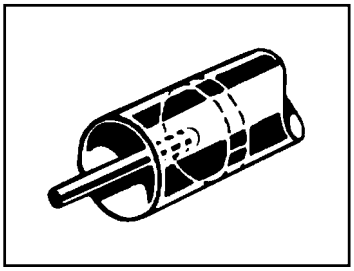


Figure 3-Sum 5. Rigid (Air) Coaxial Line

Flexible coaxial lines consist of a flexible inner conductor and a concentric outer conductor of metal braid. A continuous insulating material separates the two.

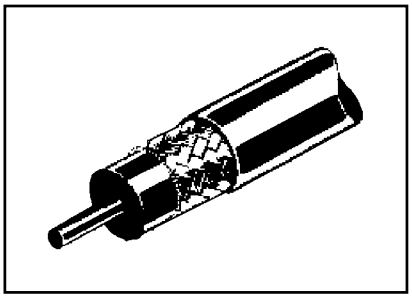


Figure 3-Sum 6. Flexible (Solid) Coaxial Lines

Waveguides are hollow metal tubes used to transfer energy from one point to another. The energy travels slower in a waveguide than in free space.

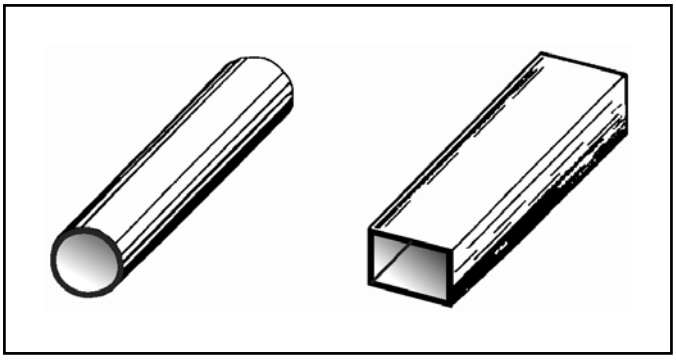


Figure 3-Sum 7. Waveguides

Copper losses can result from power (I2R) loss, in the form of heat, or skin effect. These losses decrease the conductivity of a line.

Dielectric losses are caused by the heating of the dielectric material between conductors, taking power from the source.

Radiation and induction losses are caused by part of the electromagnetic fields of a conductor being dissipated into space or nearby objects.

A transmission line is either electrically long or short if its physical length is not equal to 1/4λ for the frequency it is to carry.

Lumped constants are theoretical properties (inductance, resistance, and capacitance) of a transmission line that are lumped into a single component.

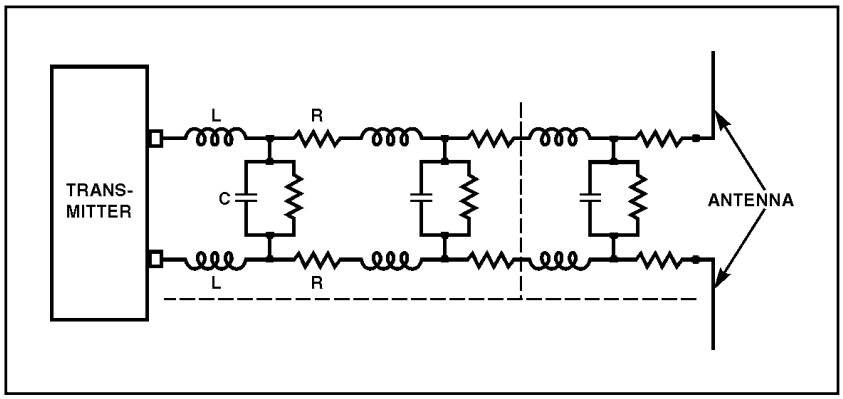


Figure 3-Sum 8. Equivalent Circuit of a Two-Wire Transmission Line

Distributed constants are constants of inductance, capacitance, and resistance that are distributed along the transmission line.

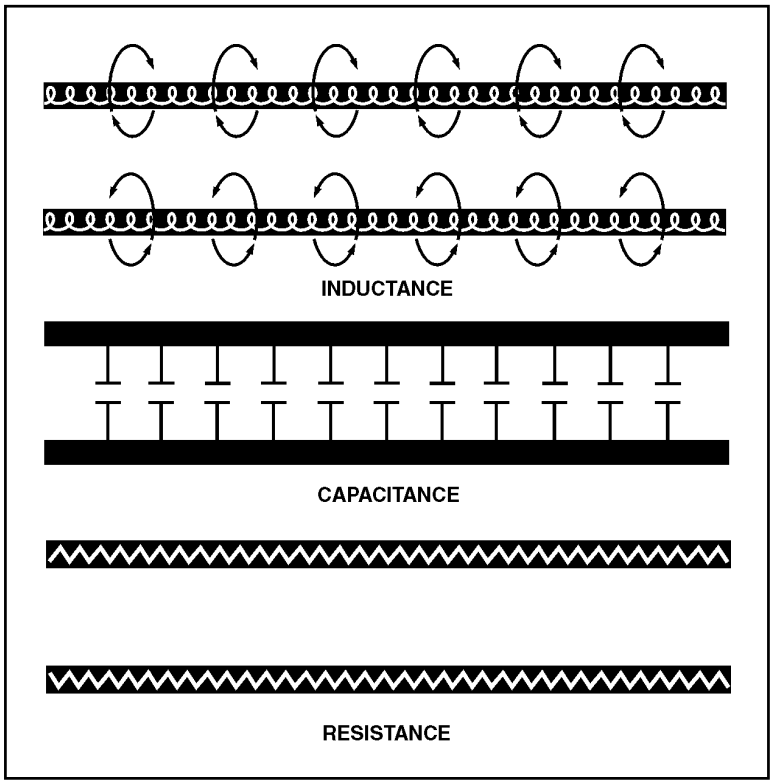


Figure 3-Sum 9. Distributed Constants

Leakage current flows between the wires of a transmission line through the dielectric. The dielectric acts as a resistor.

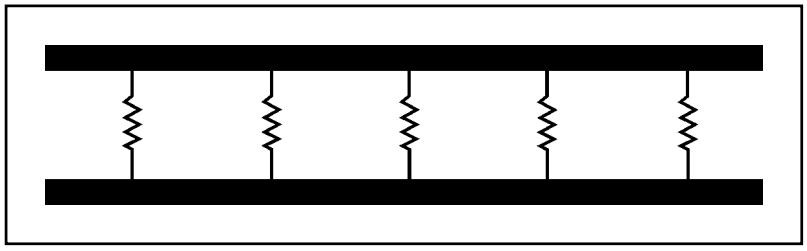


Figure 3-Sum 10. Leakage in a Transmission Line

An electromagnetic field exists along a transmission line when current flows through it.

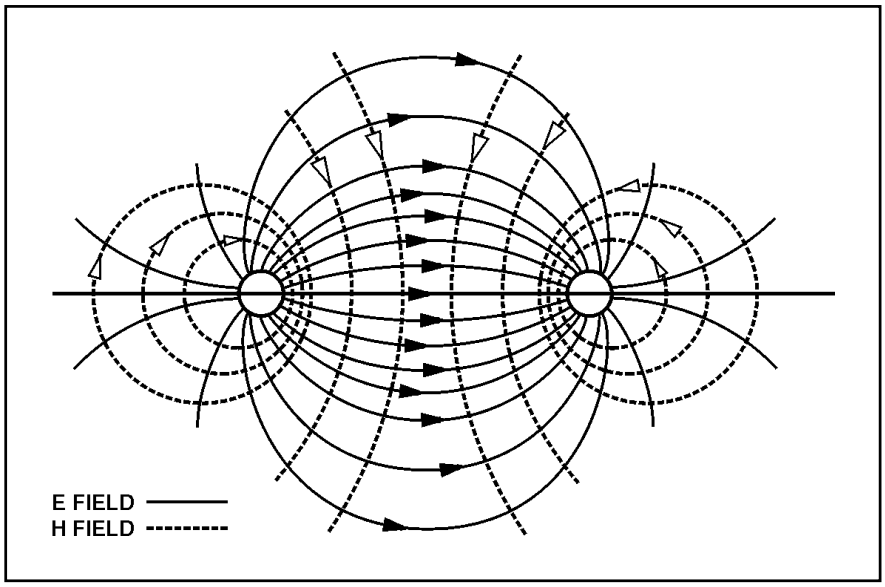


Figure 3-Sum 11. Fields between Conductors

Characteristic impedance, Z_0, is the ratio of E to I at every point along the line. For maximum transfer of electrical power, the characteristic impedance and load impedance must be matched.

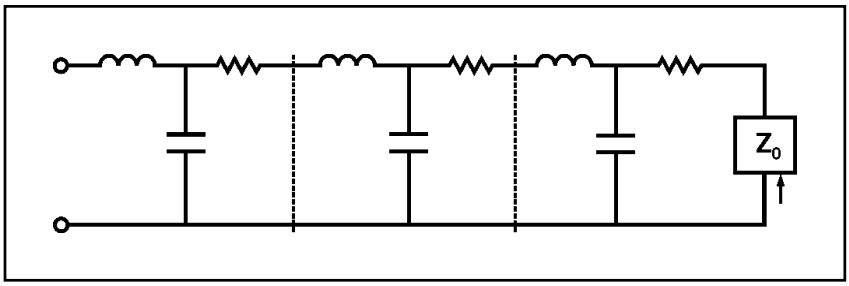


Figure 3-Sum 12. Characteristic Impedance

The velocity at which a wave travels over a given length of transmission line can be found by using the formula:

A transmission line that is not terminated in its characteristic impedance is said to be finite.

When DC is applied to an open-ended line, the voltage is reflected back from the open end without any change in polarity, amplitude, or shape. Current is reflected back with the same amplitude and shape but with opposite polarity.

When DC is applied to a short-circuited line, the current is reflected back with the same amplitude and polarity. The voltage is reflected back with the same amplitude but with opposite polarity.

When AC is applied to an open-end line, voltage is always reflected back in phase with the incident wave and current is reflected back out of phase.

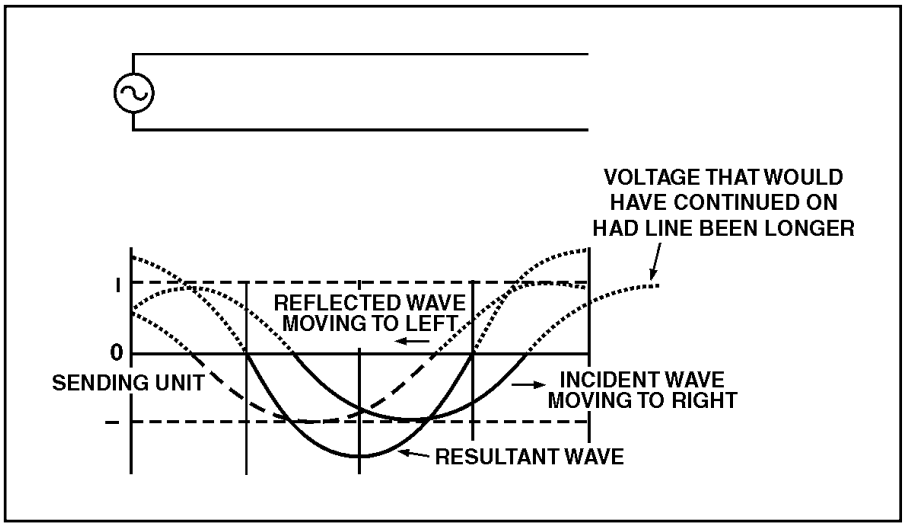


Figure 3-Sum 13. Formation of Standing Wave

When AC is applied to a short-circuited line, voltage is reflected out of phase, while current is reflected in phase.

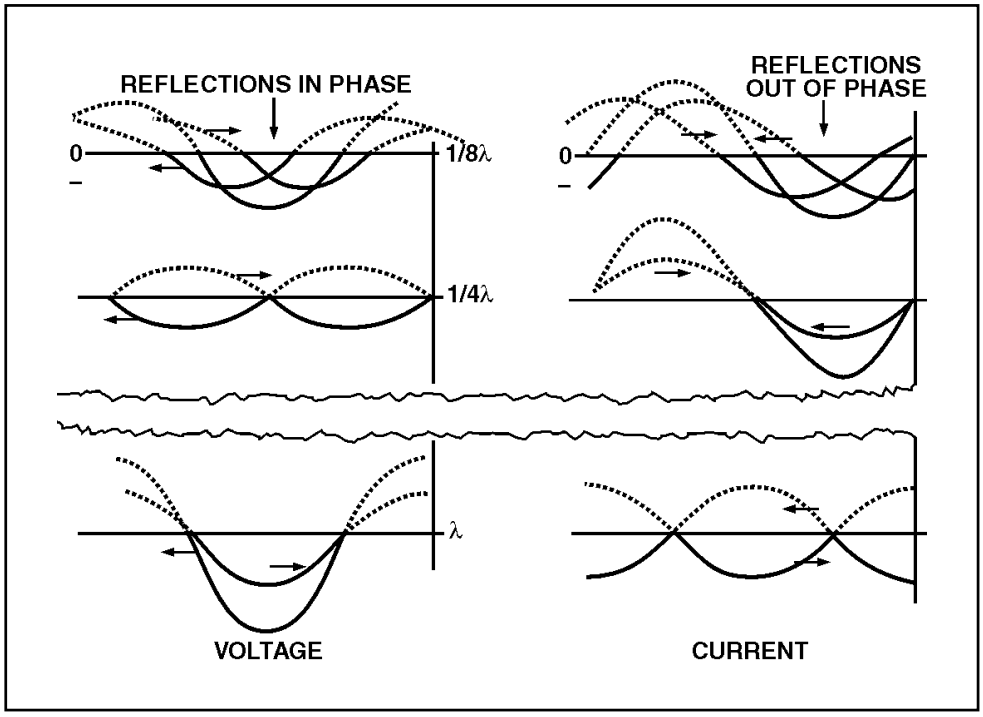


Figure 3-Sum 14. Instantaneous Values of Incident and Reflected Waves

A nonresonant line has no standing waves of current and voltage and is either infinitely long or terminated in its characteristic impedance.

A resonant line has standing waves of current and voltage and is of finite length and is not terminated in its characteristic impedance.

At all odd one-quarter wavelength points on an open-ended resonant line, the voltage is minimum, the current is maximum, and the impedance is minimum. At all even ¼λ points, the voltage is maximum, the current is minimum and the impedance is maximum.

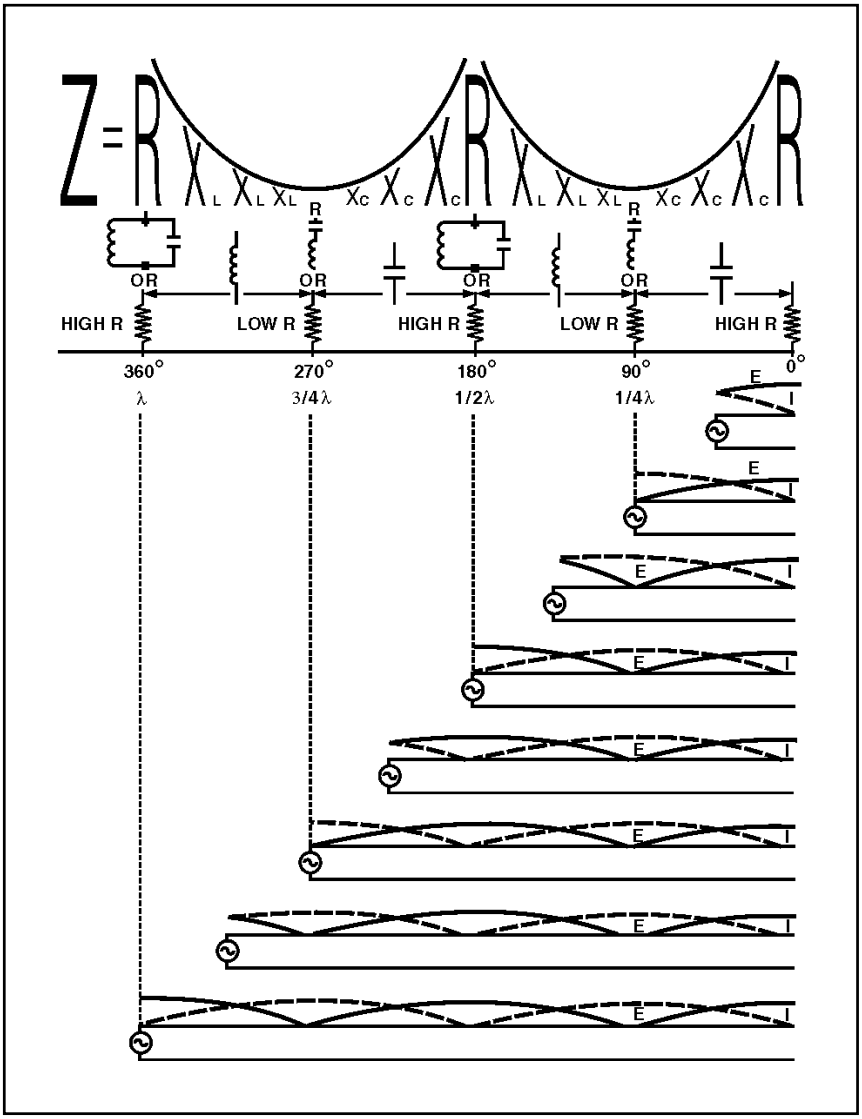


Figure 3-Sum 15. Voltage, Current, and Impedance on a Shorted Line

There are a variety of terminations for RF lines. Each termination has an effect on the standing waves on the line.

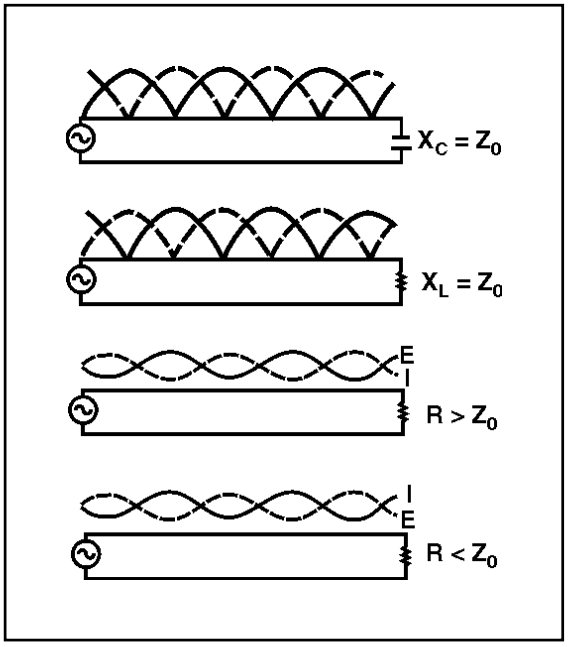


Figure 3-Sum 16. Various Termination Effects on Standing Waves

A transmission line can be terminated in its characteristic impedance as an open- or short-circuit, or in capacitance or inductance.

Whenever the termination on a transmission line is not equal to Z_0, there are reflections on the line. The amount of voltage reflected may be found by using the equation:

$$E_R = E_i\left(\frac{R_L - Z_O}{R_L + Z_O}\right)$$

When the termination on a transmission line equals Z_0, there is no reflected voltage.

The measurement of standing waves on a transmission line yields information about operating conditions. If there are no standing waves, the termination for that line is correct and maximum power transfer takes place.

The standing-wave ratio is the measurement of maximum voltage (current) to minimum voltage (current) on a transmission line and measures the perfection of the termination of the line. A ratio of 1:1 describes a line terminated in its characteristic impedance.

Check-On-Learning Questions

Principles of Transmission Lines

1. What connecting link is used to transfer energy from a radio transmitter to its antenna located on the mast of a ship?
2. What terms are used to describe the end of the transmission line that is connected to a transmitter?
3. What terms are used to describe the end of the transmission line that is connected to an antenna?
4. List the five types of transmission lines in use today.
5. Name two of the three described uses of a two-wire open line.
6. What are the two primary disadvantages of a two-wire open line?
7. What type of transmission line is often used to connect a television set to its antenna?
8. What is the primary advantage of the shielded pair?
9. What are the two types of coaxial lines in use today?
10. What is the chief advantage of the air coaxial line?
11. List the three disadvantages of the air coaxial line.
12. List the two common types of waveguides in use today.
13. What are the three types of line losses associated with transmission lines?
14. Losses caused by skin effect and the I2R (power) loss are classified as what type of loss?
15. What types of losses cause the dielectric material between the conductors to be heated?
16. What must the physical length of a transmission line be if it will be operated at 15,000,000 Hz? Use the formula:

$$\lambda = \frac{V}{f}$$

17. What are two of the three physical factors that determine the values of capacitance and inductance of a transmission line?
18. A transmission line is said to have distributed constants of inductance, capacitance, and resistance along the line. What units of measurement are used to express these constants?
19. Describe the leakage current in a transmission line and in what unit it is expressed.
20. All the power sent down a transmission line from a transmitter can be transferred to an antenna under what optimum conditions?
21. What symbol is used to designate the characteristic impedance of a line, and what two variables does it compare?
22. What is the range of the characteristic impedance of lines used in actual practice?
23. Two types of waves are formed on a transmission line. What names are given to these waves?
24. In figure 3-27, which waveforms on the left have a resultant wave of zero, and what is indicated by these waves?

25. On an open-ended transmission line, the voltage is always zero at what distance from each end of the line?
26. A nonresonant line is a line that has no standing waves of current and voltage on it and is considered to be flat. Why is this true?
27. On an open line, the voltage and impedance are maximum at what points on the line?
28. At what point on an open-circuited RF line do voltage peaks occur?
29. What is the square of the voltage standing-wave ratio called?
30. What does VSWR measure?

Chapter 4

Antennas

If you had been around in the early days of electronics, you would have considered an antenna (aerial) to be little more than a piece of wire strung between two trees or upright poles. In those days, technicians assumed that longer antennas automatically provided better reception than shorter antennas. They also believed that a mysterious medium filled all space, and that an antenna used this medium to send and receive its energy. These two assumptions have since been discarded. Modern antennas have evolved to the point that highly directional, specially designed antennas are used to relay worldwide communications in space through the use of satellites and Earth station antennas (figure 4-1). Present transmission theories are based on the assumption that space itself is the only medium necessary to propagate (transmit) radio energy.

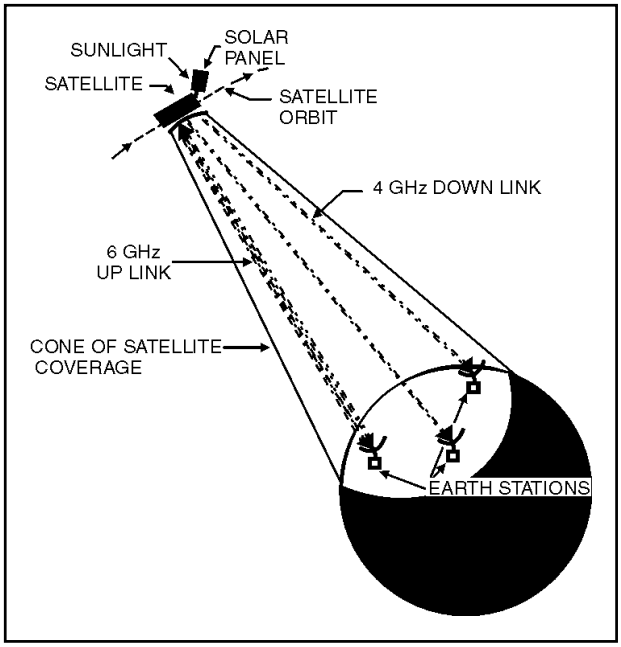


Figure 4-1. Satellite/Earth Station Communications System

4-1. A tremendous amount of knowledge and information has been gained about the design of antennas and radio wave propagation. Still, many old-time technicians will tell you that when it comes to designing the length of an antenna, the best procedure is to perform all calculations and try out the antenna. If it doesn't work right, use a cut-and-try method until it does. Fortunately, enough information has been collected over the last few decades that it is now possible to predict the behavior of antennas. This chapter discusses and explains the basic design and operation of antennas.

LEARNING OBJECTIVES

4-2. Upon completing this chapter, you should be able to do the following:

- State the basic principles of antenna radiation and list the parts of an antenna.
- Explain current and voltage distribution on an antenna.
- Describe how electromagnetic energy is radiated from an antenna.
- Explain polarization, gain, and radiation resistance characteristics of an antenna.
- Describe the theory of operation of half-wave and quarter-wave antennas.
- List the various array antennas.
- Describe the directional array antennas presented and explain the basic operation of each.
- Identify various special antennas presented, such as long-wire, V, rhombic, turnstile, ground-plane, and corner-reflector; describe the operation of each.
- List safety precautions when working aloft and around antennas.

RADIO FREQUENCY SAFETY PRECAUTIONS

4-3. Although electromagnetic radiation from transmission lines and antennas is usually of insufficient strength to electrocute personnel, it can lead to other accidents and compound injuries. Voltages may be induced in ungrounded metal objects, such as wire guys, wire cable (hawser), handrails, or ladders. If you come in contact with these objects, you could receive a shock or radio frequency (RF) burn. This shock can cause you to jump or fall into nearby mechanical equipment or, when working aloft, to fall from an elevated work area. Take care to ensure that all transmission lines or antennas are deenergized before working near or on them.

4-4. Either check or have someone check all guys, cables, rails, and ladders around your work area for RF shock dangers. Use working aloft "chits" and safety harnesses for your own safety. Signing a "working aloft chit" signifies that all equipment is in a nonradiating status. The person who signs the chit should ensure that no RF danger exists in areas where you or other personnel will be working.

4-5. Nearby ships, vans or parked aircraft are another source of RF energy that you must consider when you check a work area for safety. Combustible materials can be ignited and cause severe fires from arcs or heat generated by RF energy. Also, RF radiation can detonate ordnance devices by inducing currents in the internal wiring of the devices or in the external test equipment or leads connected to them.

4-6. Always obey RF radiation warning signs and keep a safe distance from radiating antennas. The six types of warning signs for RF radiation hazards are shown in figure 4-2.

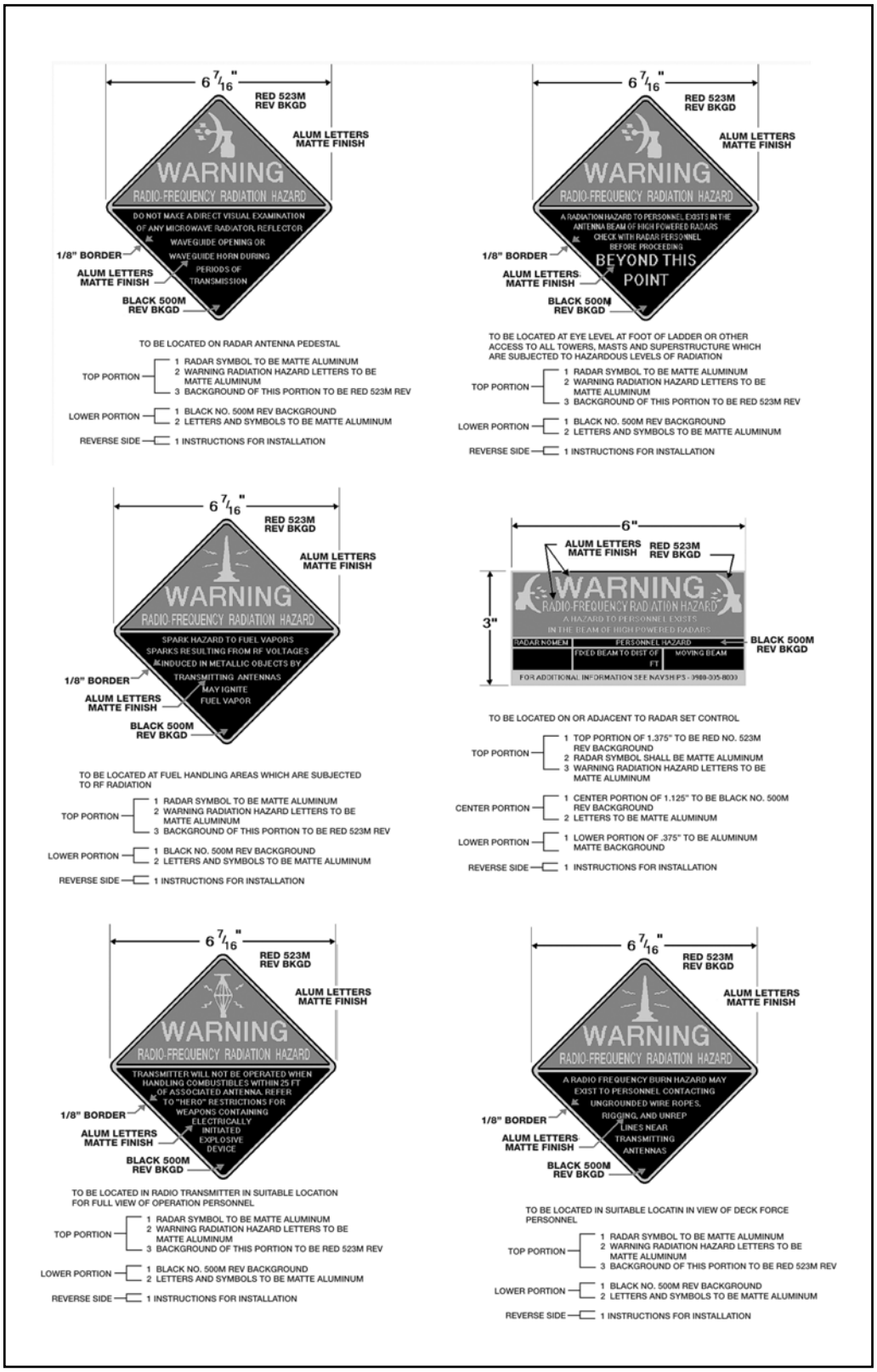


Figure 4-2. Warning Signs for Radio Frequency Radiation Hazards

RF BURNS

4-7. Close or direct contact with RF transmission lines or antennas may result in RF burns. These are usually deep, penetrating, third-degree burns. To heal properly, these burns must heal from the inside to the skin's surface. To prevent infection, you must give proper attention to all RF burns, including the small "pinhole" burns. Petrolatum gauze can be used to cover these burns temporarily, before the injured person reports to medical facilities for further treatment.

DIELECTRIC HEATING

4-8. Dielectric heating is the heating of an insulating material by placing it in a high-frequency electric field. The heat results from internal losses during the rapid reversal of polarization of molecules in the dielectric material.

4-9. In the case of a human in an RF field, the body acts as a dielectric. If the power in the RF field exceeds 10 milliwatts per centimeter, a person in that field will have a noticeable rise in body temperature. The eyes are highly susceptible to dielectric heating. For this reason, you should not look directly into devices radiating RF energy. The vital organs of the body also are susceptible to dielectric heating. For your own safety, you must not stand directly in the path of RF radiating devices.

PRECAUTIONS WHEN WORKING ALOFT

4-10. When radio or radar antennas are energized by transmitters, you must not go aloft unless advance tests show that little or no danger exists. A casualty can occur from even a small spark drawn from a charged piece of metal or rigging. Although the spark itself may be harmless, the "surprise" may cause you to let go of the antenna involuntarily and you may fall. There is also a shock hazard if nearby antennas are energized.

4-11. Rotating antennas also might cause you to fall when you are working aloft. Motor safety switches controlling the motion of rotating antennas must be tagged and locked open before you go aloft near such antennas.

PRINCIPLES OF ANTENNA RADIATION

4-12. After an RF signal has been generated in a transmitter, some means must be used to radiate this signal through space to a receiver. The device that does this job is the antenna. The transmitter signal energy is sent into space by a transmitting antenna; the RF signal is then picked up from space by a receiving antenna.

4-13. The RF energy is transmitted into space in the form of an electromagnetic field. As the traveling electromagnetic field arrives at the receiving antenna, a voltage is induced into the antenna (a conductor). The RF voltages induced into the receiving antenna are then passed into the receiver and converted back into the transmitted RF information.

4-14. The design of the antenna system is very important in a transmitting station. The antenna must be able to radiate efficiently so the power supplied by the transmitter is not wasted. An efficient transmitting antenna must have exact dimensions. The dimensions are determined by the transmitting frequencies. The dimensions of the receiving antenna are not critical for relatively low radio frequencies. However, as the frequency of the signal

being received increases, the design and installation of the receiving antenna become more critical. An example of this is a television-receiving antenna. If you raise it a few more inches from the ground or give it a slight turn in direction, you can change a snowy blur into a clear picture.

4-15. The conventional antenna is a conductor, or system of conductors, that radiates or intercepts electromagnetic wave energy. An ideal antenna has a definite length and a uniform diameter, and is completely isolated in space. However, this ideal antenna is not realistic. Many factors make the design of an antenna for a communications system a more complex problem than you would expect. These factors include the height of the radiator above the earth, the conductivity of the earth below it, and the shape and dimensions of the antenna. All of these factors affect the radiated-field pattern of the antenna in space. Another problem in antenna design is that the radiation pattern of the antenna must be directed between certain angles in a horizontal or vertical plane, or both.

4-16. Most practical transmitting antennas are divided into two basic classifications, hertz (half-wave) antennas and Marconi (quarter-wave) antennas. Hertz antennas are generally installed some distance above the ground and are positioned to radiate either vertically or horizontally. Marconi antennas operate with one end grounded and are mounted perpendicular to the earth or to a surface acting as a ground. Hertz antennas are generally used for frequencies above 2 megahertz. Marconi antennas are used for frequencies below 2 megahertz and may be used at higher frequencies in certain applications.

4-17. A complete antenna system consists of the following three parts (figure 4-3):

- The coupling device (coupling coil).
- The feeder.
- The antenna.

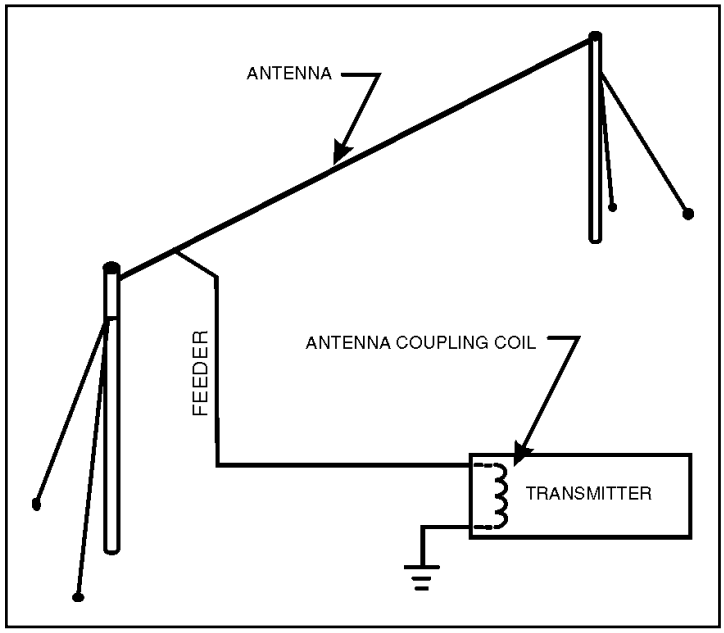


Figure 4-3. Typical Antenna System

4-18. The coupling device (coupling coil) connects the transmitter to the feeder. The feeder is a transmission line that carries energy to the antenna. The antenna radiates this energy into space.

4-19. The factors that determine the type, size, and shape of the antenna are as follows:

- The frequency of operation of the transmitter.
- Amount of power to be radiated.
- General direction of the receiving set.

Some typical antennas are illustrated in figure 4-4.

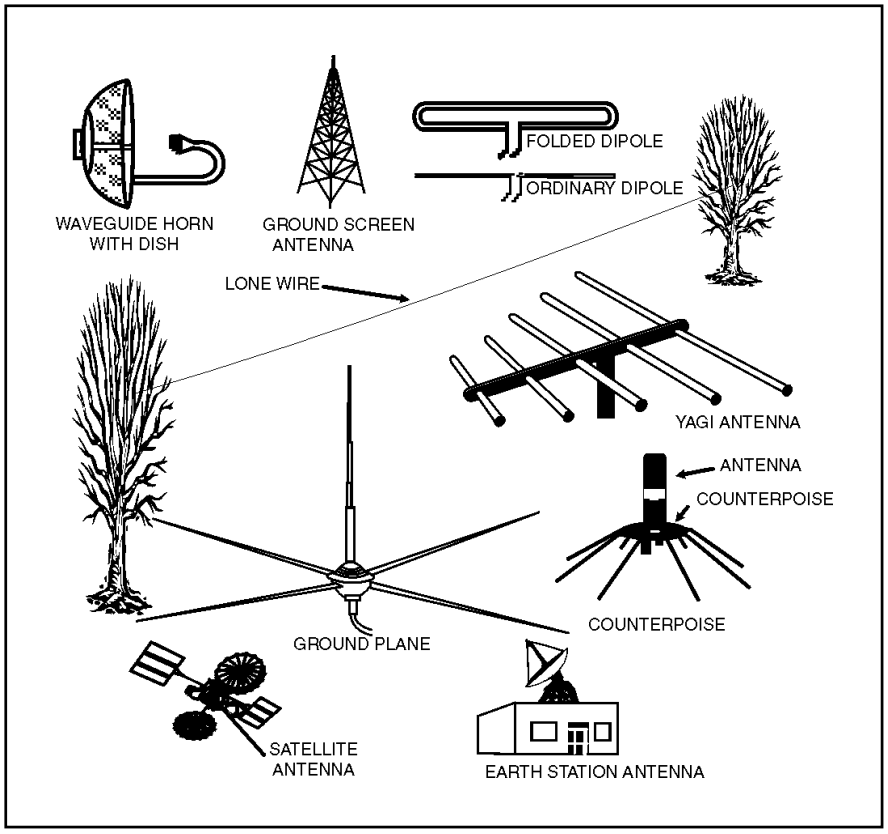


Figure 4-4. Typical Antennas

CURRENT AND VOLTAGE DISTRIBUTION ON AN ANTENNA

4-20. A current flowing in a wire whose length is properly related to the RF produces an electromagnetic field. This field is radiated from the wire and is set free in space. We discuss how these waves are set free later in this chapter. Remember, the principles of radiation of electromagnetic energy are based on two laws:

- A moving electric field creates a magnetic (H) field.
- A moving magnetic field creates an electric (E) field.

4-21. In space, these two fields are in phase and perpendicular to each other at any given time. Although a conductor is usually considered present when a moving electric or magnetic field is mentioned, the laws that govern these

fields say nothing about a conductor. Therefore, these laws hold true whether a conductor is present or not.

4-22. Figure 4-5 shows the current and voltage distribution on a half-wave (hertz) antenna. In figure 4-5, view A, a piece of wire is cut in half and attached to the terminals of a high-frequency AC generator. The frequency of the generator is set so that each half of the wire is one-quarter wavelength of the output. The result is a common type of antenna known as a dipole.

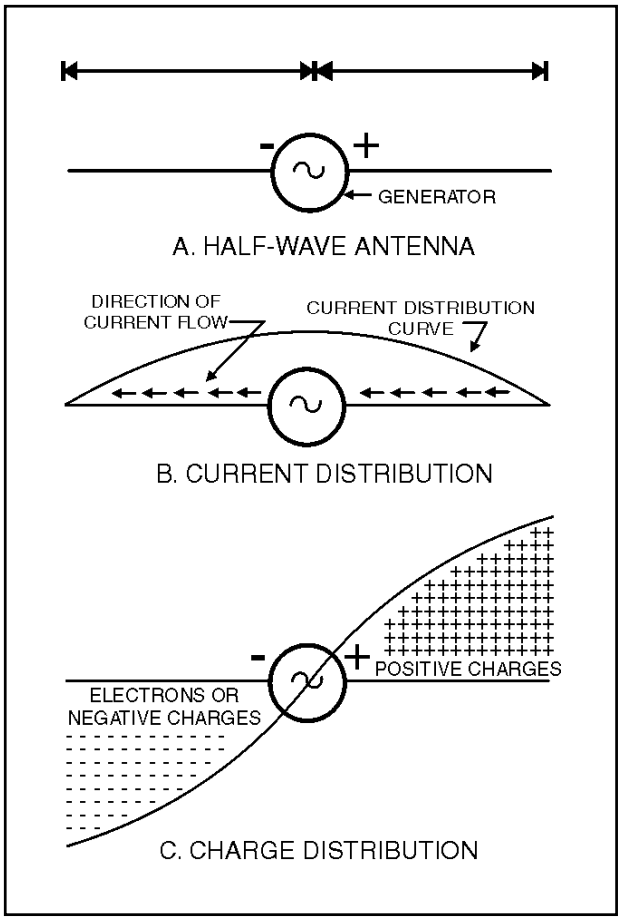


Figure 4-5. Current and Voltage Distribution on a Antenna

4-23. At a given time, the right side of the generator is positive and the left side negative. Remember that like charges repel. Because of this, electrons will flow away from the negative terminal as far as possible, but will be attracted to the positive terminal. Figure 4-5, view B shows the direction and distribution of electron flow. The distribution curve shows that most current flows in the center and none flows at the ends. The current distribution over the antenna will always be the same no matter how much or how little current is flowing. However, current at any given point on the antenna will vary directly with the amount of voltage developed by the generator.

4-24. One-quarter cycle after electrons have begun to flow, the generator will develop its maximum voltage and the current will decrease to 0. At that time the condition shown in figure 4-5 view C will exist. No current will be flowing,

but a maximum number of electrons will be at the left end of the line and a minimum number at the right end. The charge distribution along the wire will vary as the voltage of the generator varies. Therefore, you may draw the following conclusions:

- A current flows in the antenna with an amplitude that varies with the generator voltage.
- A sinusoidal distribution of charge exists on the antenna. Every one-half cycle, the charges reverse polarity.
- The sinusoidal variation in charge magnitude lags the sinusoidal variation in current by one-quarter cycle.

RADIATION OF ELECTROMAGNETIC ENERGY

4-25. The electromagnetic radiation from an antenna is made up of two components: the E field and the H field. These fields are discussed in chapters 1 and 2. The two fields occur 90 degrees out of phase with each other. These fields combine and produce a single electromagnetic field. The total energy in the radiated wave remains constant in space except for some absorption of energy by the earth. However, as the wave advances, the energy spreads out over a greater area and, at any given point, decreases as the distance increases.

4-26. Various factors in the antenna circuit affect the radiation of these waves. In figure 4-6, for example, if an alternating current is applied at the A end of the length of wire that stretches from A to B, the wave will travel along the wire until it reaches the B end. Because the B end is free, an open circuit exists and the wave cannot travel farther. This is a point of high impedance. The wave bounces back (reflects) from this point of high impedance and travels toward the starting point, where it is again reflected. Through this back-and-forth motion (oscillation), the resistance of the wire would gradually dissipate the energy of the wave; however, each time the wave reaches the starting point, it is reinforced by an amount sufficient to replace the energy lost. This results in continuous oscillations of energy along the wire and a high voltage at the A end of the wire. These oscillations are applied to the antenna at a rate equal to the frequency of the RF voltage.

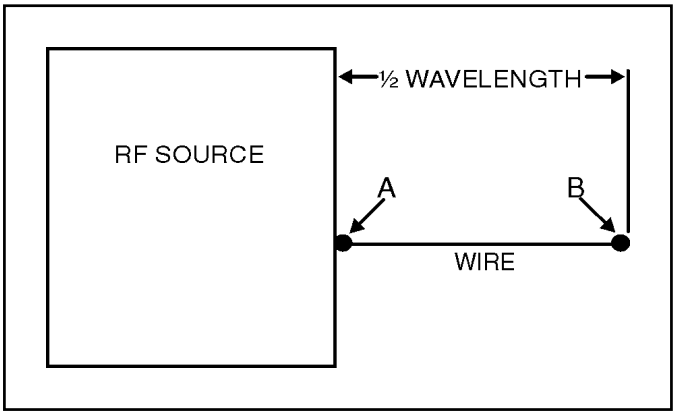


Figure 4-6. Antenna and RF Source

4-27. These impulses must be properly timed to sustain oscillations in the antenna. The rate at which the waves travel along the wire is constant at approximately 300,000,000 meters per second. The length of the antenna must be such that a wave will travel from one end to the other and back again during the period of 1 cycle of the RF voltage. Remember, the distance a wave travels during the period of 1 cycle is known as the wavelength and is found by dividing the rate of travel by the frequency.

4-28. Look at the current and voltage (charge) distribution on the antenna in figure 4-7. A maximum movement of electrons is in the center of the antenna at all times; therefore, the center of the antenna is at low impedance. This condition is called a standing wave of current. The points of high current and high voltage are known as current and voltage loops. The points of minimum current and minimum voltage are known as current and voltage nodes.

4-29. Figure 4-7, view A shows a current loop and current nodes. View B shows voltage loops and a voltage node. View C shows the resultant voltage and current loops and nodes. The presence of standing waves describes the condition of resonance in an antenna. At resonance, the waves travel back and forth in the antenna reinforcing each other and the electromagnetic waves are transmitted into space at maximum radiation. When the antenna is not at resonance, the waves tend to cancel each other and lose energy in the form of heat.

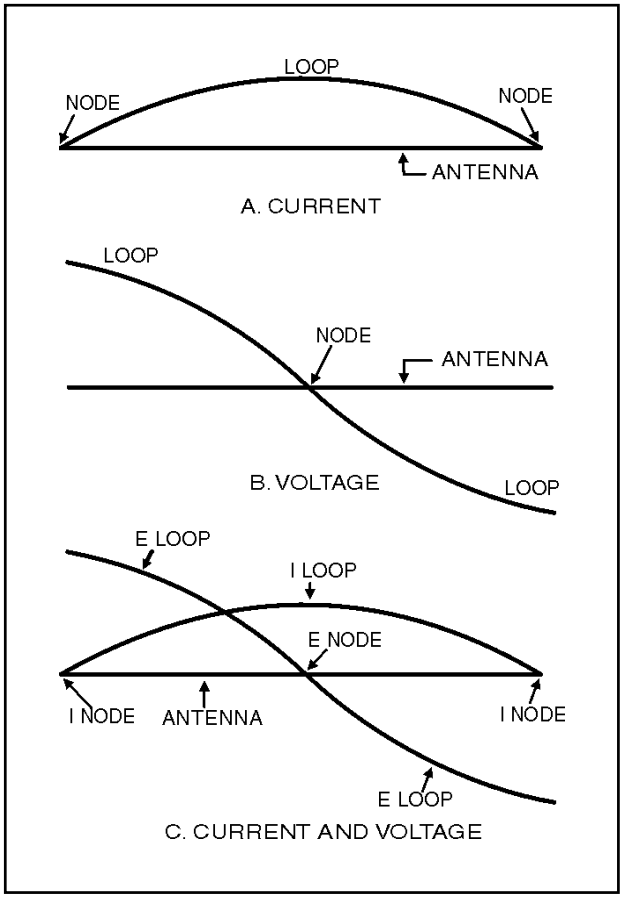


Figure 4-7. Standing Waves of Voltage and Current on an Antenna

ANTENNA CHARACTERISTICS

4-30. You can define an antenna as a conductor or group of conductors used either for radiating electromagnetic energy into space or for collecting it from space. Electrical energy from the transmitter is converted into electromagnetic energy by the antenna and radiated into space. On the receiving end, electromagnetic energy is converted into electrical energy by the antenna and is fed into the receiver.

4-31. Fortunately, separate antennas seldom are required for both transmitting and receiving RF energy. Any antenna can transfer energy from space to its input receiver with the same efficiency that it transfers energy from the transmitter into space. Of course, this is assuming that the same frequency is used in both cases. This property of interchangeability of the same antenna for transmitting and receiving is known as antenna reciprocity. Antenna reciprocity is possible because antenna characteristics are essentially the same for sending and receiving electromagnetic energy.

RECIPROCITY OF ANTENNAS

4-32. In general, the various properties of an antenna apply equally, regardless of whether you use the antenna for transmitting or receiving. The more efficient a certain antenna is for transmitting, the more efficient it will be for receiving on the same frequency. Likewise, the directive properties of a given antenna also will be the same whether it is used for transmitting or receiving.

4-33. Assume, for example, that a certain antenna used with a transmitter radiates a maximum amount of energy at right angles to the axis of the antenna, as shown in figure 4-8, view A. Note the minimum amount of radiation along the axis of the antenna. Now, if this same antenna were used as a receiving antenna, as shown in view B, it would receive best in the same directions in which it produced maximum radiation; that is, at right angles to the axis of the antenna.

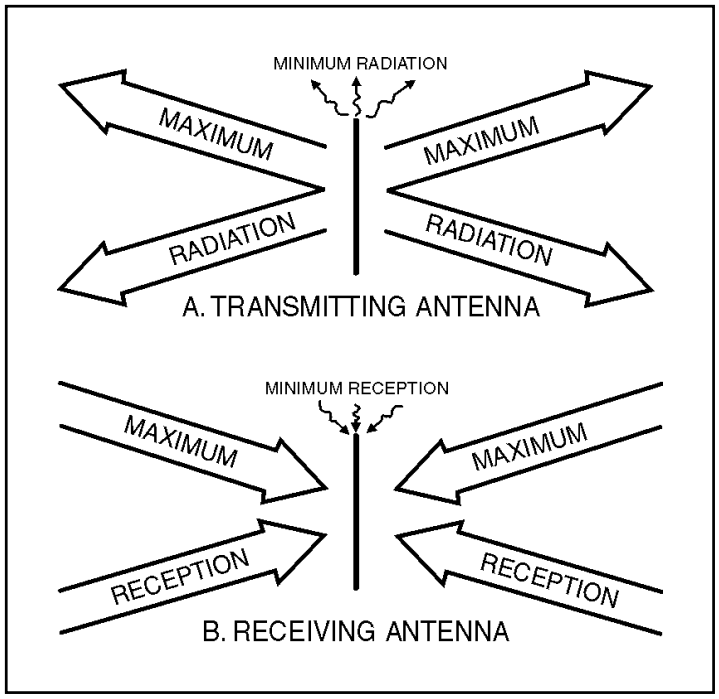


Figure 4-8. Reciprocity of Antenna

ANTENNA GAIN

4-34. Another characteristic of a given antenna that remains the same whether the antenna is used for transmitting or receiving is gain. Some antennas are highly directional; that is, more energy is propagated in certain directions than in others. The ratio between the amount of energy propagated in these directions compared to the energy that would be propagated if the antenna were not directional is known as its gain. When a transmitting antenna with a certain gain is used as a receiving antenna, it will also have the same gain for receiving.

POLARIZATION

4-35. Let us review polarization briefly. In chapter 2 you learned that the radiation field is composed of electric and magnetic lines of force. These lines of force are always at right angles to each other. Their intensities rise and fall together, reaching their maximums 90 degrees apart. The electric field determines the direction of polarization of the wave. In a vertically polarized wave, the electric lines of force lie in a vertical direction. In a horizontally polarized wave, the electric lines of force lie in a horizontal direction. Circular polarization has the electric lines of force rotating through 360 degrees with every cycle of RF energy.

4-36. The electric field was chosen as the reference field because the intensity of the wave is usually measured in terms of the electric field intensity (volts, millivolts, or microvolts per meter). When a single-wire antenna is used to extract energy from a passing radio wave, maximum pickup will result when the antenna is oriented in the same direction as the electric field. Thus, a vertical antenna is used for the efficient reception of vertically polarized

waves, and a horizontal antenna is used for the reception of horizontally polarized waves. In some cases the orientation of the electric field does not remain constant. Instead, the field rotates as the wave travels through space. Under these conditions both horizontal and vertical components of the field exist and the wave is said to have an elliptical polarization.

Polarization Requirements for Various Frequencies

4-37. Ground-wave transmission is widely used at medium and low frequencies. Horizontal polarization cannot be used at these frequencies because the electric lines of force are parallel to and touch the earth. Because the earth acts as a fairly good conductor at low frequencies, it would short out the horizontal electric lines of force and prevent the radio wave from traveling very far. Vertical electric lines of force, on the other hand are bothered very little by the earth. Therefore vertical polarization is used for ground-wave transmission, allowing the radio wave to travel a considerable distance along the ground surface with minimum attenuation.

4-38. Sky-wave transmission is used at high frequencies. Either horizontal or vertical polarization can be used with sky-wave transmission because the sky wave arrives at the receiving antenna elliptically polarized. This is the result of the wave traveling obliquely through the earth's magnetic field and striking the ionosphere. The radio wave is given a twisting motion as it strikes the ionosphere. Its orientation continues to change because of the unstable nature of the ionosphere. The relative amplitudes and phase differences between the horizontal and vertical components of the received wave also change. Therefore, the transmitting and receiving antennas can be mounted either horizontally or vertically.

4-39. Although either horizontally or vertically polarized antennas can be used for high frequencies, horizontally polarized antennas have certain advantages and are therefore preferred. One advantage is that vertically polarized interference signals, such as those produced by automobile ignition systems and electrical appliances, are minimized by horizontal polarization. Also, less absorption of radiated energy by buildings or wiring occurs when these antennas are used. Another advantage is that support structures for these antennas are of more convenient size than those for vertically polarized antennas.

4-40. For frequencies in the VHF or UHF range, either horizontal or vertical polarization is satisfactory. These radio waves travel directly from the transmitting antenna to the receiving antenna without entering the ionosphere. The original polarization produced at the transmitting antenna is maintained throughout the entire travel of the wave to the receiver. Therefore, if a horizontally polarized antenna is used for transmitting, a horizontally polarized antenna must be used for receiving. The requirements would be the same for a vertical transmitting and receiving antenna system.

4-41. For satellite communications, parallel frequencies can be used without interference by using polarized radiation. The system setup is shown in figure 4-9. One pair of satellite antennas is vertically polarized and another pair is horizontally polarized. Either vertically or horizontally polarized transmissions are received by the respective antenna and retransmitted in the same polarization. For example, transmissions may be made in the 3.7 to 3.74 GHz range on the vertical polarization path and in the 3.72 to 3.76 GHz

range on the horizontal polarization path without adjacent frequency (co-channel) interference.

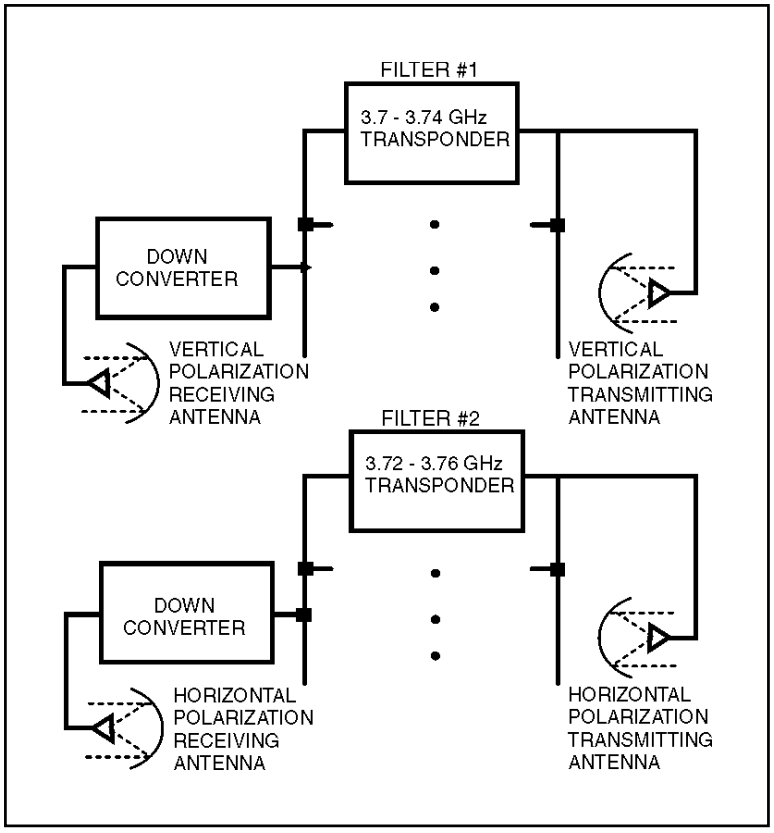


Figure 4-9. Satellite Transmissions Using Polarized Radiation

Advantages of Vertical Polarization

4-42. Simple vertical antennas can be used to provide omnidirectional (all directions) communication. This is an advantage when communications must take place from a moving vehicle.

4-43. In some overland communications, such as in vehicular installations, antenna heights are limited to 3 meters (10 feet) or less. In such instances vertical polarization results in a stronger receiver signal than does horizontal polarization at frequencies up to about 50 megahertz. From approximately 50 to 100 megahertz, vertical polarization results in a slightly stronger signal than does horizontal polarization with antennas at the same height. Above 100 megahertz, the difference in signal strength is negligible.

4-44. For transmission over bodies of water, vertical polarization is much better than horizontal polarization for antennas at the lower heights. As the frequency increases, the minimum antenna height decreases. At 30 megahertz, vertical polarization is better for antenna heights below about 91 meters (300 feet); at 85 megahertz, antenna heights below 15 meters (50 feet); and still lower heights at the high frequencies. Therefore, at ordinary antenna mast heights of 12 meters (40 feet), vertical polarization is advantageous for frequencies less than about 100 megahertz.

4-45. Radiation is somewhat less affected by reflections from aircraft flying over the transmission path when vertical polarization is used instead of horizontal polarization. With horizontal polarization, such reflections cause variations in received signal strength. This factor is important in locations where aircraft traffic is heavy.

4-46. When vertical polarization is used, less interference is produced or picked up because of strong VHF and UHF broadcast transmissions (television and FM). This is because VHF and UHF transmissions use horizontal polarization. This factor is important when an antenna must be located in an urban area having several television and FM broadcast stations.

Advantages of Horizontal Polarization

4-47. A simple horizontal antenna is bidirectional. This characteristic is useful when you wish to minimize interference from certain directions. Horizontal antennas are less likely to pick up man-made interference, which ordinarily is vertically polarized.

4-48. When antennas are located near dense forests or among buildings, horizontally polarized waves suffer lower losses than vertically polarized waves, especially above 100 megahertz. Small changes in antenna locations do not cause large variations in the field intensity of horizontally polarized waves. When vertical polarization is used, a change of only a few meters in the antenna location may have a considerable effect on the received signal strength. This is the result of interference patterns that produce standing waves in space when spurious reflections from trees or buildings occur.

4-49. When simple antennas are used, a horizontally-mounted antenna less affects the transmission line, which is usually vertical. When the antenna is mounted at right angles to the transmission line and horizontal polarization is used, the line is kept out of the direct field of the antenna. As a result, the radiation pattern and electrical characteristics of the antenna are practically unaffected by the presence of the vertical transmission line.

RADIATION RESISTANCE

4-50. Radiated energy is the useful part of the transmitter's signal. However, it represents as much of a loss to the antenna as the energy lost in heating the antenna wire. In either case, the dissipated power is equal to I^2R. In the case of heat losses, the R is real resistance. In the case of radiation, R is an assumed resistance; if this resistance were actually present, it would dissipate the same amount of power that the antenna takes to radiate the energy. This assumed resistance is referred to as the radiation resistance.

4-51. Radiation resistance varies at different points on the antenna. This resistance is always measured at a current loop. For the antenna in free space, that is, entirely removed from any objects that might affect its operation, the radiation resistance is 73 ohms. A practical antenna located over a ground plane may have any value of radiation resistance from 0 to approximately 100 ohms. The exact value of radiation resistance depends on the height of the antenna above the ground. For most half-wave wire antennas, the radiation resistance is about 65 ohms. It will usually vary between 55 and 600 ohms for antennas constructed of rod or tubing. The actual value of radiation resistance, so long as it is 50 ohms or more, has little effect on the radiation efficiency of the antenna. This is because the

ohmic resistance is about 1 ohm for conductors of large diameter. The ohmic resistance does not become important until the radiation resistance drops to a value less than 10 ohms. This may be the case when several antennas are coupled together.

RADIATION TYPES AND PATTERNS

4-52. The energy radiated from an antenna forms a field having a definite radiation pattern. A radiation pattern is a plot of the radiated energy from an antenna. This energy is measured at various angles at a constant distance from the antenna. The shape of this pattern depends on the type of antenna used. The following sections introduce the basic types of radiation (isotropic and anisotropic) and their radiation patterns.

Isotropic Radiation

4-53. Some antenna sources radiate energy equally in all directions. Radiation of this type is known as isotropic radiation. We all know the sun radiates energy in all directions. The energy radiated from the sun measured at any fixed distance and from any angle will be approximately the same. Assume that a measuring device is moved around the sun and stopped at the points indicated in figure 4-10 to make a measurement of the amount of radiation. At any point around the circle, the distance from the measuring device to the sun is the same. The measured radiation will also be the same. The sun is therefore considered an isotropic radiator.

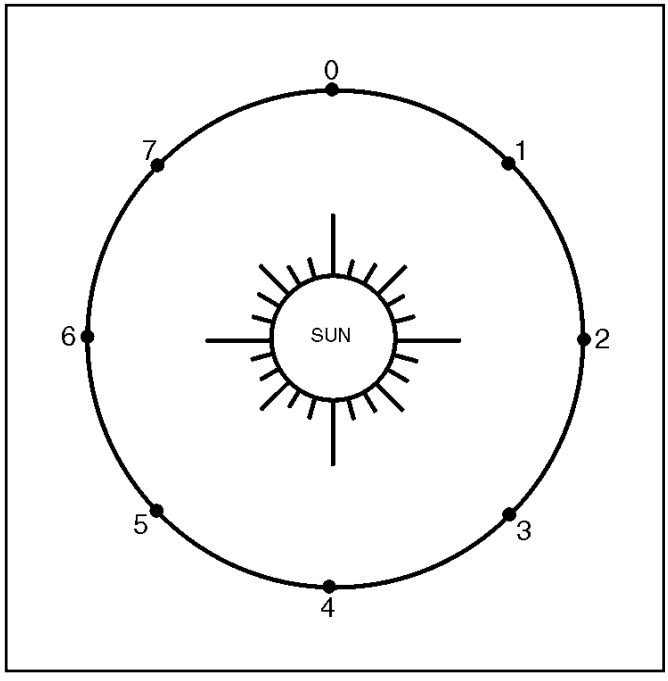


Figure 4-10. Isotropic Radiator

4-54. To plot the pattern shown in figure 4-10, assume that the radiation is measured on a scale of 0 to 10 units and that the measured amount of radiation is 7 units at all points. The measurements can be plotted on two different types of graphs: rectangular-and polar-coordinate graphs. The

rectangular-coordinate graph of the measured radiation, shown in figure 4-11, view A, is a straight line plotted against positions around the circle. View B shows the polar-coordinate graph for the same isotropic source.

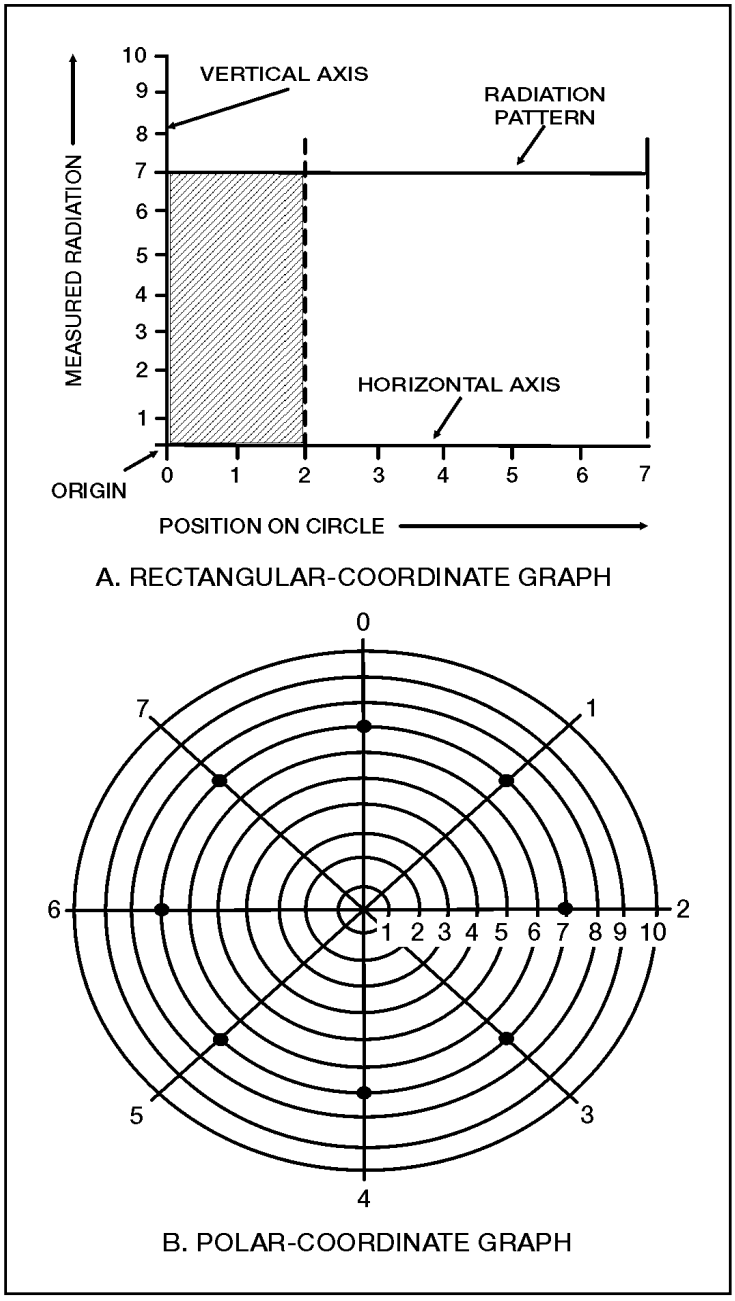


Figure 4-11. Comparison of Rectangular and Polar-Coordinate Graph for an Isotropic Source

4-55. In the rectangular-coordinate graph, points are located by projection from a pair of stationary, perpendicular axes. In the polar-coordinate graph, points are located by projection along a rotating axis (radius) to an intersection with one of several concentric, equally spaced circles. The horizontal axis on the rectangular-coordinate graph corresponds to the circles

on the polar-coordinate graph. The vertical axis on the rectangular-coordinate graph corresponds to the rotating axis (radius) on the polar-coordinate graph.

Rectangular-Coordinate Pattern

4-56. Look at figure 4-11, view A. The numbered positions around the circle are laid out on the horizontal axis of the graph from 0 to 7 units. The measured radiation is laid out on the vertical axis of the graph from 0 to 10 units. The units on both axes are chosen so the pattern occupies a convenient part of the graph.

4-57. The horizontal and vertical axes are at a right angle to each other. The point where the axes cross each other is known as the origin. In this case, the origin is 0 on both axes. Now, assume that a radiation value of 7 units is measured at position 2. From position 2 on the horizontal axis, a dotted line that runs parallel to the vertical axis is projected upwards. From position 7 on the vertical axis, a line that runs parallel to the horizontal axis is projected to the right. The point where the two lines cross (intercept) represents a value of 7 radiation units at position 2. This is the only point on the graph that can represent this value.

4-58. As you can see from the figure, the lines used to plot the point form a rectangle. For this reason, this type of plot is called a rectangular-coordinate graph. A new rectangle is formed for each different point plotted. In this example, the points plotted lie in a straight line extending from 7 units on the vertical scale to the projection of position 7 on the horizontal scale. This is the characteristic pattern in rectangular coordinates of an isotropic source of radiation.

Polar-Coordinate Pattern

4-59. The polar-coordinate graph has proved to be of great use in studying radiation patterns. Compare views A and B of figure 4-11. Note the great difference in the shape of the radiation pattern when it is transferred from the rectangular-coordinate graph in view A to the polar-coordinate graph in view B. The scale of radiation values used in both graphs is identical, and the measurements taken are both the same. However, the shape of the pattern is drastically different.

4-60. Look at figure 4-11, view B, and assume that the center of the concentric circles is the sun. Assume that a radius is drawn from the sun (center of the circle) to position 0 of the outermost circle. When you move to position 1, the radius moves to position 1; when you move to position 2, the radius also moves to position 2, and so on.

4-61. The positions where a measurement was taken are marked as 0 through 7 on the graph. Note how the position of the radius indicates the actual direction from the source at which the measurement was taken. This is a distinct advantage over the rectangular-coordinate graph in which the position is indicated along a straight-line axis and has no physical relation to the actual direction of measurement. Now that we have a way to indicate the direction of measurement, we must devise a way to indicate the magnitude of the radiation.

4-62. Notice that the rotating axis is always drawn from the center of the graph to some position on the edge of the graph (figure 4-11, view B). As the axis moves toward the edge of the graph, it passes through a set of equally

spaced, concentric circles. In this example, they are numbered successively from 1 to 10 from the center out. These circles are used to indicate the magnitude of the radiation.

4-63. The advantages of the polar-coordinate graph are immediately evident. The source, which is at the center of the observation circles, is also at the center of the graph. By looking at a polar-coordinate plot of a radiation pattern, you can immediately see the direction and strength of radiation put out by the source. Therefore, the polar-coordinate graph is more useful than the rectangular-coordinate graph in plotting radiation patterns.

Anisotropic Radiation

4-64. Most radiators emit (radiate) stronger radiation in one direction than in another. A radiator such as this is referred to as anisotropic. An example of an anisotropic radiator is an ordinary flashlight. The beam of the flashlight lights only a portion of the space surrounding it. If a circle is drawn with the flashlight as the center, as shown in figure 4-12, view B, the radiated light can be measured at different positions around the circle. Again, as with the isotropic radiator, all positions are the same distance from the center, but at different angles. However, in this illustration the radiated light is measured at 16 different positions on the circle.

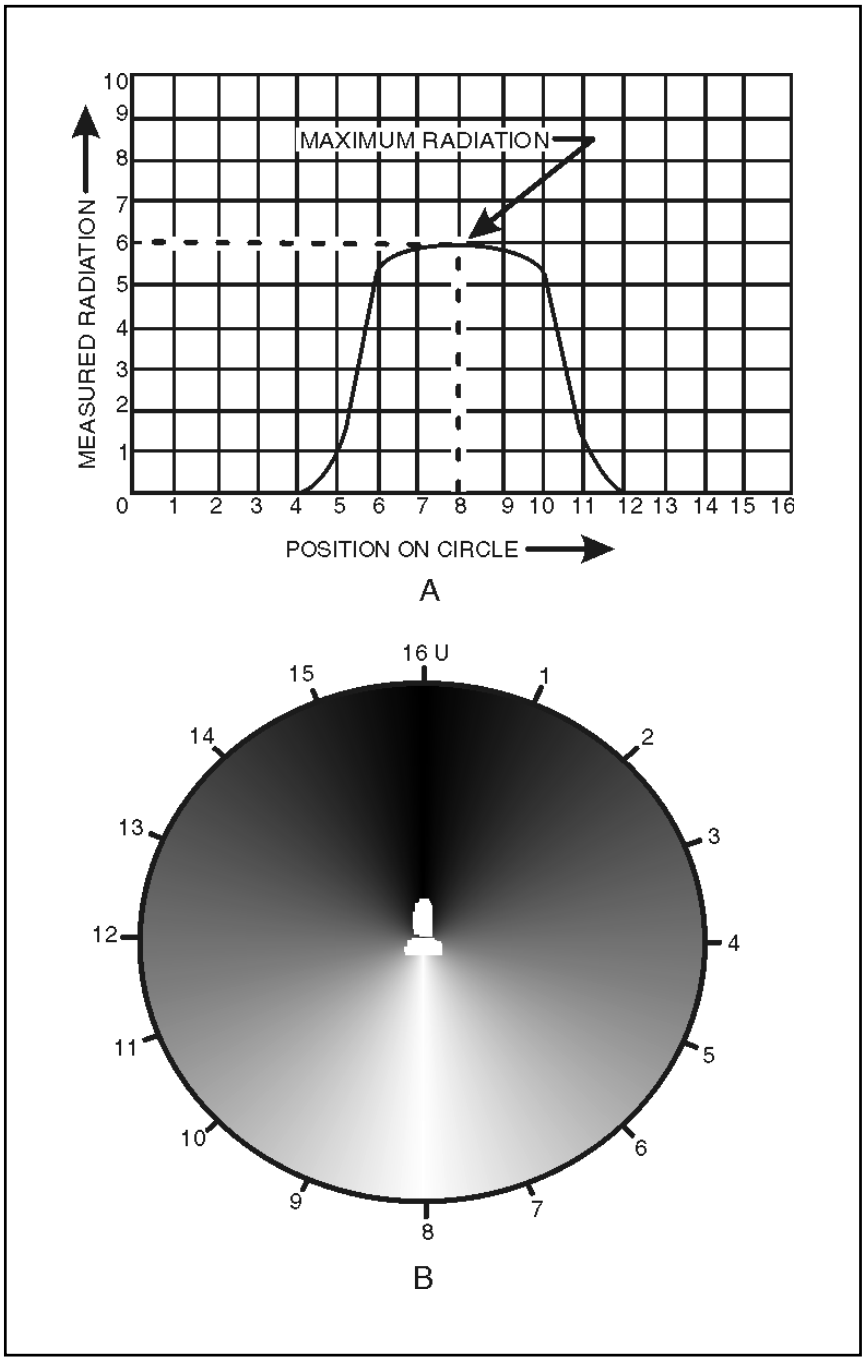


Figure 4-12. Anisotropic Radiator

4-65. Directly behind the flashlight (position 0) the radiation measured is minimum. Accordingly, a 0 value is assigned to this position in the rectangular-coordinate graph (figure. 4-12, view A). This radiation remains at minimum until position 4 is reached. Between positions 4 and 6, the measuring device enters the flashlight beam. You can see this transition from darkness to brightness easily in view B. Radiation is fairly constant between

positions 6 and 10. Maximum brightness occurs at position 8, which is directly in the path of the flashlight beam. From positions 10 to 12, the measuring device leaves the flashlight beam and the radiation measurement falls off sharply. At position 13 the radiation is again at 0 and stays at this value back to position 0.

4-66. Radiation from a light source and radiation from an antenna are both forms of electromagnetic waves. Therefore, the measurement of radiation of an antenna follows the same basic procedure as that just described for the sun and the flashlight. Before proceeding further with the study of antenna patterns, you should be sure you understand the methods used to graph the measured radiation (magnitude of the radiation). Study the rectangular and polar coordinate systems of plotting presented in the following paragraphs.

4-67. In figure 4-12, view A, the radiation pattern of the flashlight is graphed in rectangular coordinates. The illustration of the flashlight beam in figure 4-12, view B clearly indicates the shape of the flashlight beam. This shape is not evident in the radiation pattern plotted on the rectangular-coordinate graph. Now look at figure 4-13. The radiation pattern shown in this figure looks very much like the actual flashlight beam. The pattern in figure 4-13 is plotted using the same values as those of figure 4-12, view A, but is drawn using polar coordinates.

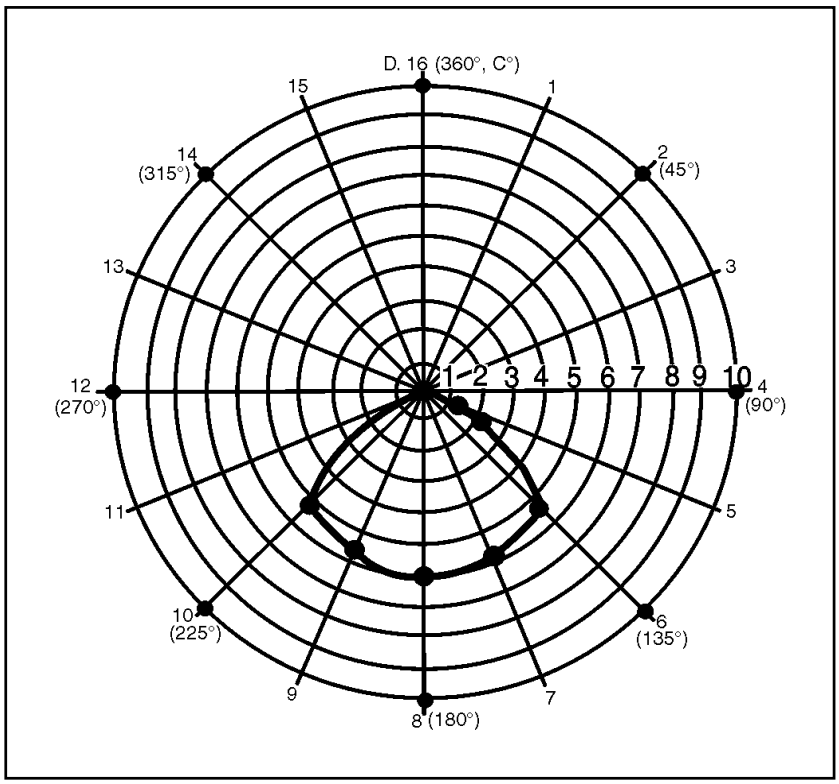


Figure 4-13. Polar-Coordinate Graph for Anisotropic Radiator

4-68. The positions marked off on the two polar-coordinate graphs in figures 4-11 and 4-13 were selected and numbered arbitrarily. However, a standard method allows the positions around a source to be marked off so that one radiation pattern can easily be compared with another. This method is based on the fact that a circle has a radius of 360 degrees. The radius extending vertically from the center (position 0 in figure 4-11) is designated 0 degrees. At position 4 the radius is at a right angle to the 0-degree radius. Accordingly, the radius at position 4 is marked 90 degrees, position 8 is 180 degrees, position 12 is 270 degrees, and position 16 is 360 degrees. The various radii drawn on the graph are all marked according to the angle each radius makes with the reference radius at 0 degrees.

4-69. The radiation pattern in figure 4-13 is obtained by using the same procedure that was used for figure 4 -10, view B. The radiation measured at positions 1, 2, 3, and 4 is 0. Position 5 measures approximately 1 unit. This is marked on the graph and the rotating radius moves to position 6. At this position a reading of 5.5 units is taken. As before, this point is marked on the graph. The procedure is repeated around the circle and a reading is obtained from positions 6 through 11. At position 12 no radiation is indicated, and this continues on to position 16.

4-70. The polar-coordinate graph now shows a definite area enclosed by the radiation pattern. This pattern indicates the general direction of radiation from the source. The enclosed area is called a lobe. Outside of this area, minimum radiation is emitted in any direction. For example, at position 2 the radiation is 0. Such a point is called a null. In real situations, some radiation is usually transmitted in all directions. Therefore, a null is used to indicate directions of minimum radiation. The pattern of figure 4-13 shows one lobe and one continuous null.

ANTENNA LOADING

4-71. You will sometimes want to use one antenna system for transmitting and receiving on several different frequencies. Because the antenna must always be in resonance with the applied frequency, you may need to lengthen or shorten the antenna physically or electrically.

4-72. Except for trailing-wire antennas used in aircraft installations (which may be lengthened or shortened), physically lengthening the antenna is not very practical. But you can achieve the same result by changing the electrical length of the antenna. To change the electrical length, you can insert either an inductor or a capacitor in series with the antenna. This is shown in figure 4-14, views A and B. Changing the electrical length by this method is known as lumped-impedance tuning, or loading. The electrical length of any antenna wire can be increased or decreased by loading. If the antenna is too short for the wavelength being used, it is resonant at a higher frequency than that at which it is being excited. Therefore, it offers a capacitive reactance at the excitation frequency. This capacitive reactance can be compensated for by introducing a lumped-inductive reactance, as shown in figure 4-14, view A. Similarly, if the antenna is too long for the transmitting frequency, it offers an inductive reactance. Inductive reactance can be compensated for by introducing a lumped-capacitive reactance, as shown in view B. An antenna without loading is represented in view C.

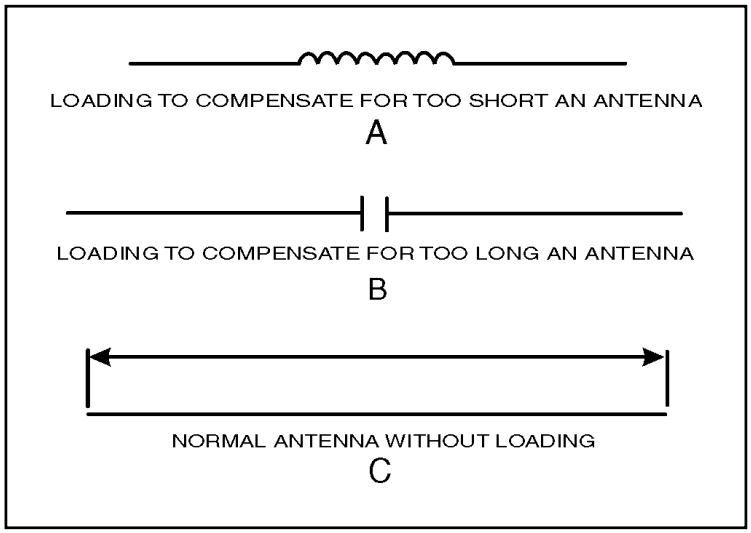


Figure 4-14. Electrically Equal Antenna

BASIC ANTENNAS

4-73. Before you look at the various types of antennas, consider the relationship between the wavelength at which the antenna is being operated and the actual length of the antenna. An antenna does not necessarily radiate or receive more energy when it is made longer. Specific dimensions must be used for efficient antenna operation.

4-74. Nearly all antennas have been developed from two basic types, the Hertz and the Marconi. The basic Hertz antenna is one-half wavelength long at the operating frequency and is insulated from ground. It is often called a dipole or a doublet. The basic Marconi antenna is one-quarter wavelength long and is either grounded at one end or connected to a network of wires called a counterpoise. The ground or counterpoise provides the equivalent of an additional one-quarter wavelength, which is required for the antenna to resonate.

HALF-WAVE ANTENNAS

4-75. A half-wave antenna (referred to as a dipole, Hertz, or doublet) consists of two lengths of wire rod, or tubing, each one-quarter wavelength long at a certain frequency. It is the basic unit from which many complex antennas are constructed. The half-wave antenna operates independently of ground; therefore, it may be installed far above the surface of the earth or other absorbing bodies. For a dipole, the current is maximum at the center and minimum at the ends. Voltage is minimum at the center and maximum at the ends, as shown in figure 4-7.

Radiation Patterns

4-76. In the following discussion, the term dipole is used to mean the basic half-wave antenna. The term doublet is used to indicate an antenna that is very short compared with the wavelength of the operating frequency. Physically, it has the same shape as the dipole.

4-77. **Radiation pattern of a doublet**. The doublet is the simplest form of a practical antenna. Its radiation pattern can be plotted in the same way as the radiation pattern of the flashlight shown in figure 4-13. Figure 4-15 illustrates the development of vertical and horizontal patterns for a doublet. This is not a picture of the radiation, but three-dimensional views of the pattern itself that the radiation makes. In three views (views B, C, and D), the pattern resembles a doughnut. From the dimensions in these views, two types of polar-coordinate patterns can be drawn: horizontal and vertical. The horizontal pattern shown in view A is derived from the solid pattern shown in view C by slicing it horizontally. This produces view B, which is converted to the polar coordinates seen in view A. The horizontal pattern illustrates that the radiation is constant in any direction along the horizontal plane.

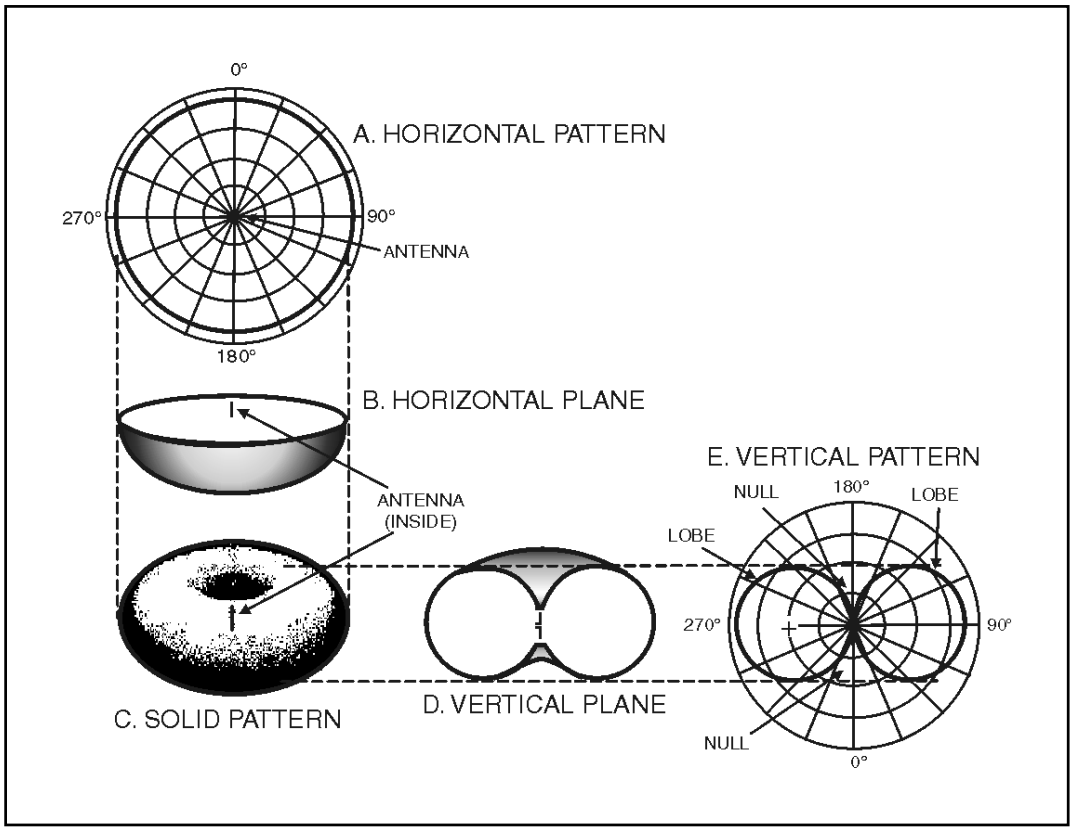


Figure 4-15. Development of Vertical and Horizontal Pattern

4-78. A vertical pattern shown in figure 4-15, view E is depicted from the drawing of the vertical plane (view D) of the radiation pattern shown in view C. The radiation pattern in view C is sliced in half along a vertical plane through the antenna. This produces the vertical plane pattern shown in view D. Note how the vertical plane in view D of the radiation pattern differs from the horizontal plane in view B. The vertical pattern in view E exhibits two lobes and two nulls. The difference between the two patterns is caused by two facts: (1) no radiation is emitted from the ends of the doublet; and (2) maximum radiation comes from the doublet in a direction perpendicular to the antenna axis. This type of radiation pattern is both nondirectional (in a horizontal plane) and directional (in a vertical plane).

4-79. From a practical viewpoint, the doublet antenna can be mounted either vertically or horizontally. The doublet shown in figure 4-15 is mounted vertically, and the radiated energy spreads out about the antenna in every direction in the horizontal plane. Because ordinarily the horizontal plane is the useful plane, this arrangement is termed nondirectional. The directional characteristics of the antenna in other planes are ignored. If the doublet were mounted horizontally, it would have the effect of turning the pattern on edge, reversing the patterns given in figure 4-15. The antenna would then be directional in the horizontal plane. The terms "directional" and "nondirectional" are used for convenience in describing specific radiation patterns. A complete description always involves a figure in three dimensions, as in the radiation pattern of figure 4-15.

4-80. **Radiation pattern of a dipole**. The radiation pattern of a dipole (figure 4-16) is similar to that of the doublet (figure 4-15). Increasing the length of the doublet to one-half wavelength has the effect of flattening out the radiation pattern. The radiation pattern in the horizontal plane of a dipole is a larger circle than that of the doublet. The vertical-radiation pattern lobes are no longer circular. They are flattened out and the radiation intensity is greater.

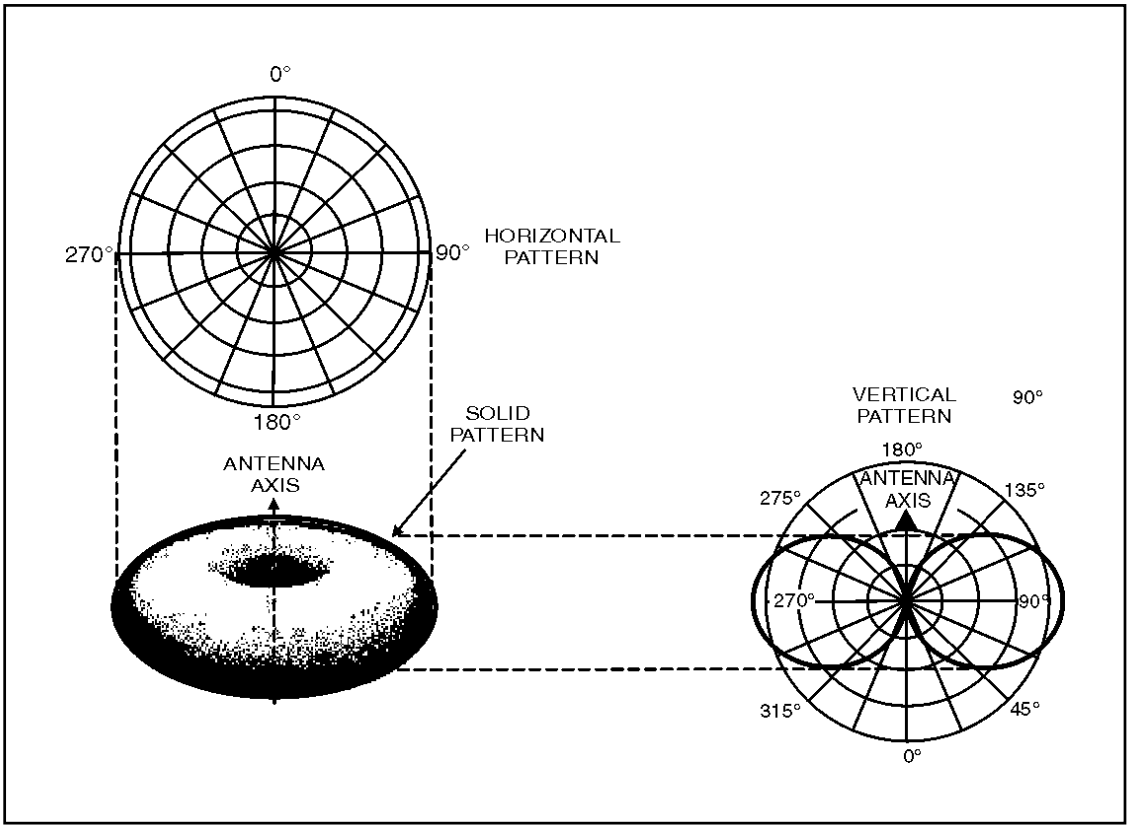


Figure 4-16. Radiation Pattern of a Dipole

Methods of Feeding Energy to an Antenna

4-81. Voltage and current distribution for the half-wave antenna (shown in figure 4-17) is the same as that for the antenna discussed earlier in this chapter. A point closely related to the voltage and current distribution on an antenna is the method of feeding the transmitter output to the antenna. The simplest method of feeding energy to the half-wave antenna is to connect one end through a capacitor to the final output stage of the transmitter. This method is often called the end-feed or voltage-feed method. In this method the antenna is fed at a point of high voltage (the end).

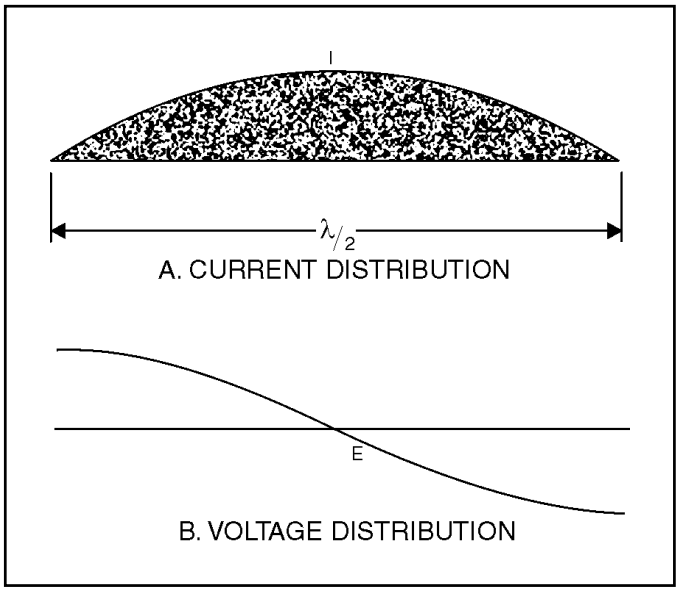


Figure 4-17. Standing Waves of Current and Voltage

4-82. Energy may also be fed to the half-wave antenna by dividing the antenna at its center and connecting the transmission line from the final transmitter output stage to the two center ends of the halved antenna. Because the antenna is now being fed at the center (a point of low voltage and high current), this type of feed is known as the center-feed or current-feed method. The point of feed is important in determining the type of transmission line to be used.

QUARTER-WAVE ANTENNAS

4-83. As you have studied in the previous sections, a one-half wavelength antenna is the shortest antenna that can be used in free space. If we cut a half-wave antenna in half and then ground one end, we will have a grounded quarter-wave or Marconi antenna. This antenna will resonate at the same frequency as the ungrounded half-wave antenna. Quarter-wave antennas are widely used in the military. Most mobile transmitting and receiving antennas (illustrated in figure 4-18) are quarter-wave antennas.

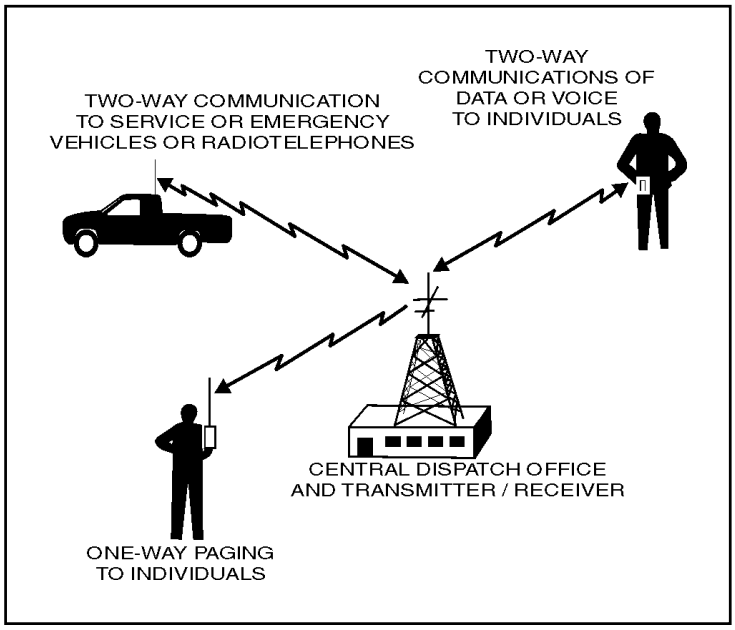


Figure 4-18. Mobile Antennas

4-84. As stated above, a grounded quarter-wave antenna will resonate at the same frequency as an ungrounded half-wave antenna. This is because the ground has high conductivity and acts as an electrical mirror image. This characteristic provides the missing half of the antenna, as shown in the bottom part of figure 4-19. In other words, the grounded quarter-wave antenna acts as if another quarter-wave were actually down in the earth.

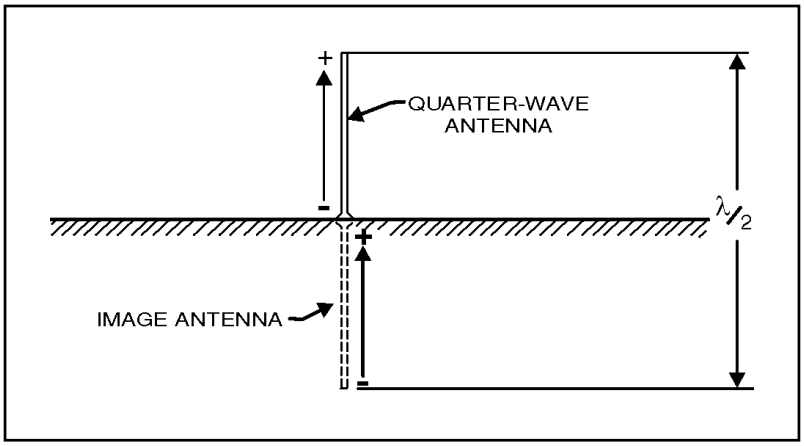


Figure 4-19. Grounded Quarter-Wave Antenna Image

Characteristics of Quarter-Wave Antennas

4-85. The grounded end of the quarter-wave antenna has a low input impedance and has low voltage and high current at the input end, as shown in figure 4-19. The ungrounded end has a high impedance, which causes high voltage and low current. The directional characteristics of a grounded quarter-wave antenna are the same as those of a half-wave antenna in free space.

4-86. As explained earlier, ground losses affect radiation patterns and cause high signal losses for some frequencies. Such losses may be greatly reduced if a perfectly conducting ground is provided in the vicinity of the antenna. This is the purpose of a ground screen (figure 4-20, view A) and counterpoise (view B).

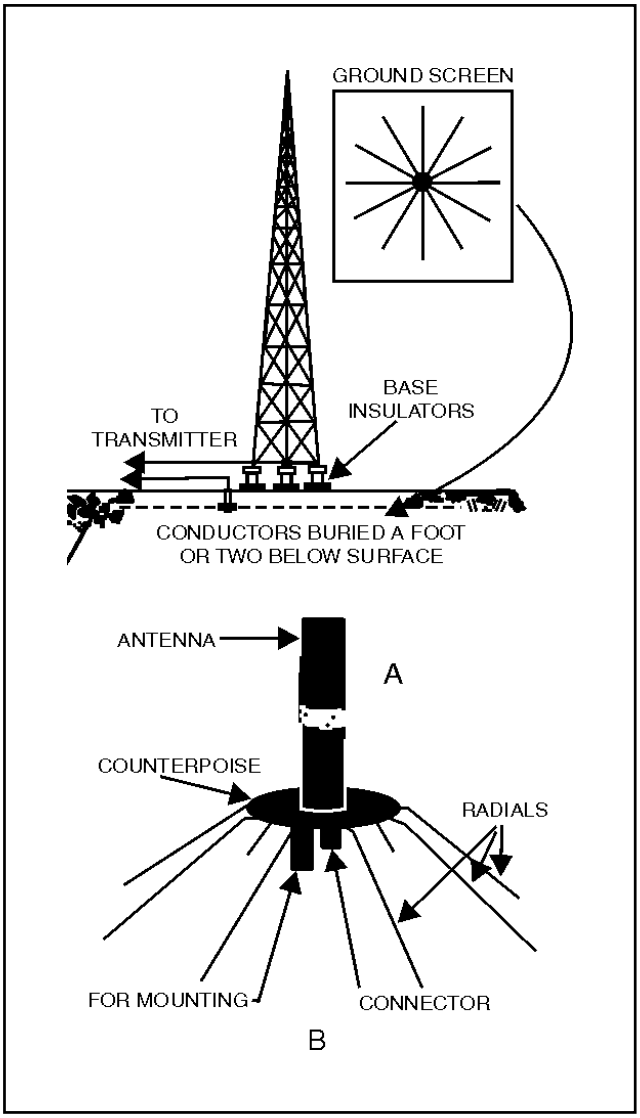


Figure 4-20. Ground Screen and Counterpoise

4-87. The ground screen in figure 4-20, view A is composed of a series of conductors buried 1 to 2 feet (0.3 to 0.6 meter) below the surface of the earth and arranged in a radial pattern. These conductors reduce losses in the ground in the immediate vicinity of the antenna. Such a radial system of conductors is usually one-half wavelength in diameter.

4-88. A counterpoise, as shown in figure 4-20, view B, is used when easy access to the base of the antenna is necessary. It is also used when the earth is not a good conducting surface, such as ground that is sandy or solid rock. The counterpoise serves the same purpose as the ground screen but it is

usually elevated above the earth. No specific dimensions are necessary in the construction of a counterpoise nor is the number of wires particularly critical. A practical counterpoise may be assembled from a large screen of chicken wire or some similar material. This screen may be placed on the ground, but better results are obtained if it is placed a few feet above the ground.

FOLDED DIPOLE

4-89. The use of parasitic elements and various stacking arrangements causes a reduction in the radiation resistance of a center-fed, half-wave antenna. Under these conditions, obtaining a proper impedance match between the radiator and the transmission line is often difficult. A convenient method of overcoming these difficulties is to use a folded dipole in place of the center-fed radiator. (See figure 4-21, views A and B).

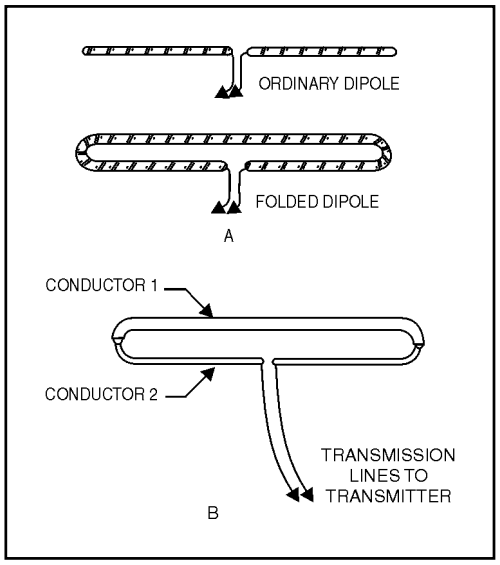


Figure 4-21. Folded-Dipole Antennas

4-90. A folded dipole is an ordinary half-wave antenna that has one or more additional conductors connected across its ends. Additional conductors are mounted parallel to the dipole elements at a distance equal to a very small fraction of a wavelength. Spacing of several inches is common.

4-91. The feed-point impedance can be further increased by using three or four properly spaced parallel conductors. Standard feed-line spreaders are used to maintain this spacing when required. In any folded dipole, the increase of impedance is the square of the number of conductors used in the radiator. Thus, a three-wire dipole has nine times (3^2) the feed-point impedance of a simple center-fed dipole. A second method of stepping up the impedance of a folded dipole is to use two conductors with different radii, as shown in figure 4-21, view B.

4-92. The directional characteristics of a folded dipole are the same as those of a simple dipole. However, the reactance of a folded dipole varies much more slowly as the frequency is varied from resonance. Because of this

difference, the folded dipole can be used over a much wider frequency range than is possible with a simple dipole.

ARRAY ANTENNAS

4-93. An array antenna is a special arrangement of basic antenna components. The discussion of array antennas includes the following new terms that you should study before moving on to the section on phasing.

DEFINITION OF TERMS

4-94. An *array antenna* is made up of more than one element, but the basic element is generally the dipole. Sometimes the basic element is made longer or shorter than a half-wave, but the deviation usually is not great.

4-95. A *driven element* is similar to the dipole you have been studying and is connected directly to the transmission line. It obtains its power directly from the transmitter or, as a receiving antenna; it delivers the received energy directly to the receiver. A parasitic element is located near the driven element from which it gets its power. It is placed close enough to the driven element to permit coupling.

4-96. A *parasitic element* is sometimes placed so it will produce maximum radiation (during transmission) from its associated driver. When it operates to reinforce energy coming from the driver toward itself, the parasitic element is referred to as a *director*. If a parasitic element is placed so it causes maximum energy radiation in a direction away from itself and toward the driven element, that parasitic element is called a reflector.

4-97. If all of the elements in an array are driven, the array is referred to as a *driven array* (sometimes as a *connected array*). If one or more elements are parasitic, the entire system usually is considered to be a *parasitic array*.

4-98. Multi-element arrays frequently are classified according to their directivity. A *bidirectional array* radiates in opposite directions along the line of maximum radiation. A *unidirectional array* radiates in only one general direction.

4-99. Arrays can be described with respect to their radiation patterns and the types of elements of which they are made. However, you will find it useful to identify them by the physical placement of the elements and the direction of radiation with respect to these elements. Generally speaking, the term *broadside array* designates an array in which the direction of maximum radiation is perpendicular to the plane containing these elements. In actual practice, this term is confined to those arrays in which the elements themselves are also broadside, or parallel, with respect to each other.

4-100. A *collinear array* is one in which all the elements lie in a straight line with no radiation at the ends of the array. The direction of maximum radiation is perpendicular to the axis of the elements.

4-101. An *end-fire array* is one in which the principal direction of radiation is along the plane of the array and perpendicular to the elements. Radiation is from the end of the array, which is the reason this arrangement is referred to as an end-fire array.

4-102. Sometimes a system uses the characteristics of more than one of the three types mentioned. For instance, some of the elements may be collinear

while others may be parallel. Such an arrangement is often referred to as a *combination array* or an *array of arrays*. Because maximum radiation occurs at right angles to the plane of the array, the term *broadside array* is also used.

4-103. The *front-to-back ratio* is the ratio of the energy radiated in the principal direction compared to the energy radiated in the opposite direction for a given antenna.

PHASING

4-104. Various reflected and refracted components of the propagated wave create effects of reinforcement and cancellation. At certain distant points from the transmitter, some of the wave components meet in space. Reception at these points is either impaired or improved. If the different components arrive at a given point in the same phase, they add, making a stronger signal available. If they arrive out of phase, they cancel, reducing the signal strength.

Radiation Pattern

4-105. Effects similar to those described in the preceding paragraph can be produced at the transmitting point itself. Consider the antennas shown in figure 4-22, views A and B. View A shows an unobstructed view of the radiation pattern of a single dipole. In view B, two dipoles, shown as points 1 and 2, are perpendicular to the plane of the page. They are spaced one-quarter wavelength apart at the operating frequency. The radiation pattern from either antenna 1 or 2, operating alone, would be uniform in all directions in this plane, as shown in view A. Suppose that current is being fed to both antennas from the same transmitter in such a way that the current fed to antenna 2 lags the current in antenna 1 by 90 degrees. Energy radiating from antenna 1 toward receiving location X will reach antenna 2 after one-quarter cycle of operation. The energy from both antennas will add, and propagation toward X will be strong.

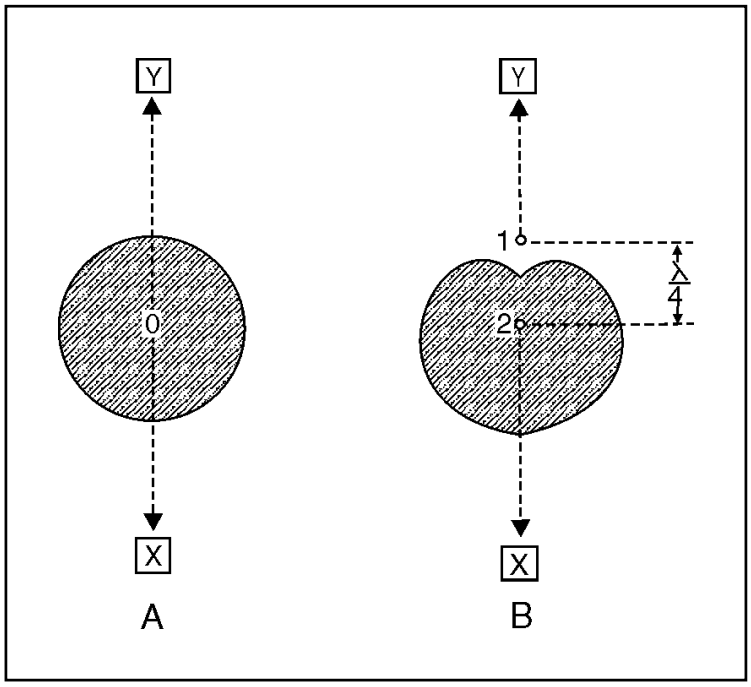


Figure 4-22. Phasing of Antenna in Free Space

4-106. Radiation from antenna 2 toward receiving location Y will reach antenna 1 after one-quarter cycle. The energy in antenna 1 was one-quarter cycle behind that of antenna 2 to begin with; therefore, the radiation from antenna 1 toward receiving point Y will be exactly 180 degrees out of phase with that of antenna 2. As a result, the radiation fields will cancel and there will be no radiation toward Y.

4-107. At receiving points away from the line of radiation, phase differences occur between 0 and 180 degrees, producing varying amounts of energy in that direction. The overall effect can be seen in the radiation pattern illustrated in view B. The physical phase relationship caused by the wavelength spacing between the two elements, as well as the phase of the currents in the elements, has acted to change the radiation pattern of the individual antennas.

Stub Phasing

4-108. In the case just discussed, the currents fed to the two antennas from the same transmitter were 90 degrees out of phase. Sections of transmission line, called stubs, are frequently used for this purpose. These stubs can be adjusted to produce any desired phase relationship between connected elements.

4-109. When two collinear half-wave elements are connected directly so their currents are in the same phase, the effect is the same as that of a full-wave antenna, as shown in figure 4-23, view A. The current in the first one-half wavelength is exactly 180 degrees out of phase with that in the second one-half wavelength. This is the opposite of the desired condition. In the illustration, arrows are used to indicate the direction of current flow in the

antenna. (Using arrows is a convenient means of determining the phase on more complicated arrays.)

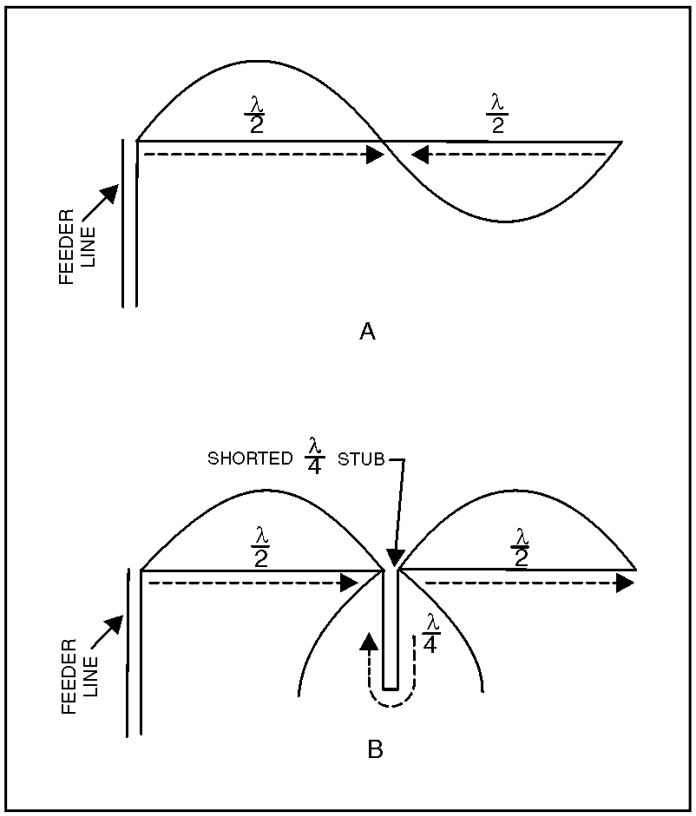


Figure 4-23. Phasing of Connected Elements

4-110. When the two elements are connected by a shorted one-quarter-wavelength stub, as shown in figure 4-23, view B, current travels down one side of the stub and up the other. It travels a distance of one-half wavelength in the stub itself. As a result, the current moves through one-half cycle of change. When the current reaches the second element, it is in the desired phase. Because the current on one side of the stub is equal and opposite to the current on the other side, the fields produced here cancel and no radiation is transmitted from the stub itself.

DIRECTIVITY

4-111. The directivity of an antenna or an array can be determined by looking at its radiation pattern. In an array propagating a given amount of energy, more radiation takes place in certain directions than in others. The elements in the array can be altered in such a way that they change the pattern and distribute it more uniformly in all directions. The elements can be considered as a group of antennas fed from a common source and facing different directions. On the other hand, the elements could be arranged so that the radiation would be focused in a single direction. With no increase in power from the transmitter, the amount of radiation in a given direction would be greater. Because the input power has no increase, this increased directivity is achieved at the expense of gain in other directions.

Directivity and Interference

4-112. In many applications, sharp directivity is desirable although no need exists for added gain. Examine the physical disposition of the units shown in figure 4-24. Transmitters 1 and 2 are sending information to receivers 1 and 2, respectively, along the paths shown by the solid arrows. The distance between transmitter 1 and receiver 1 or between transmitter 2 and receiver 2 is short and does not require high-power transmission. The antennas of the transmitters propagate well in all directions. However, receiver 1 picks up some of the signals from transmitter 2, and receiver 2 picks up some of the signals from transmitter 1, as shown by the broken arrows. This effect is emphasized if the receiving antennas intercept energy equally well in all directions.

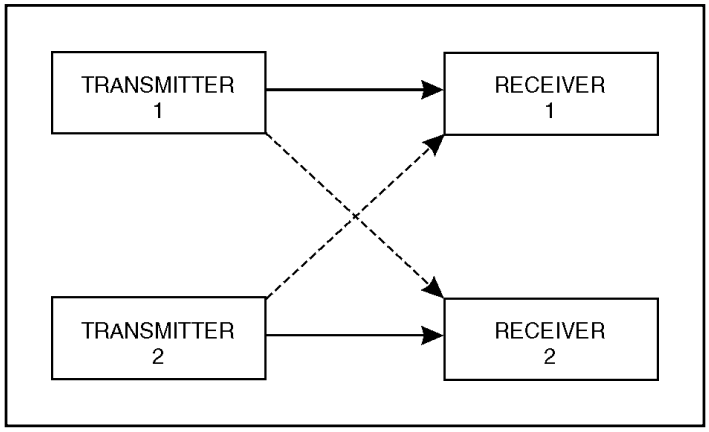


Figure 4-24. Directivity and Interference

4-113. The use of highly directional arrays as radiators from the transmitters tends to solve the problem. The signals are beamed along the paths of the solid arrows and provide very low radiation along the paths of the broken arrows. Further improvement along these lines is obtained by the use of narrowly directed arrays as receiving antennas. The effect of this arrangement is to select the desired signal while discriminating against all other signals. This same approach can be used to overcome other types of radiated interference. In such cases, preventing radiation in certain directions is more important than producing greater gain in other directions.

4-114. Look at the differences between the field patterns of the single-element antenna and the array, as illustrated in figure 4-25. View A shows the relative field-strength pattern for a horizontally polarized single antenna. View B shows the horizontal-radiation pattern for an array. The antenna in view A radiates fairly efficiently in the desired direction toward receiving point X. It radiates equally as efficiently toward Y, although no radiation is desired in this direction. The antenna in view B radiates strongly to point X, but very little in the direction of point Y, which results in more satisfactory operation.

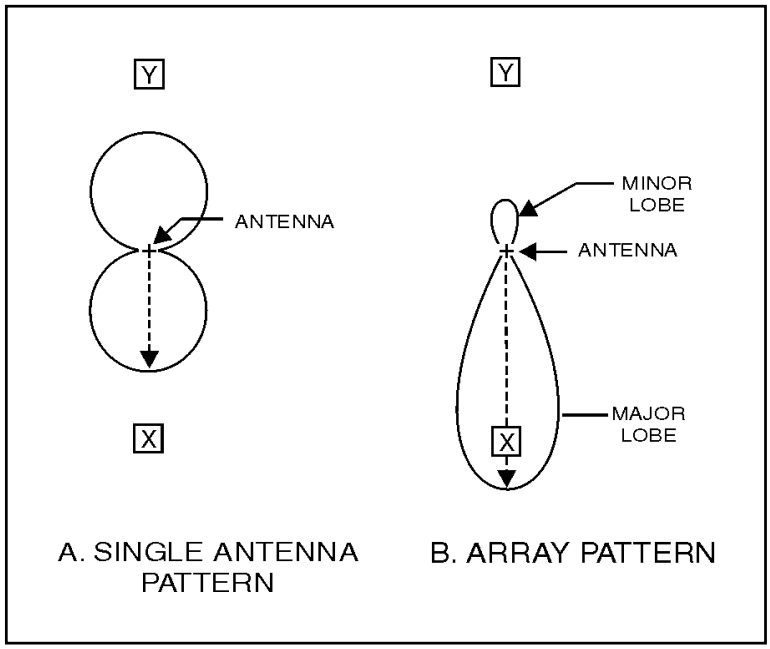


Figure 4-25. Single Antenna Versus Array

Major and Minor Lobes

4-115. The pattern shown in figure 4-25, view B has radiation concentrated in two lobes. The radiation intensity in one lobe is considerably stronger than in the other. The lobe toward point X is called a major lobe; the other is a minor lobe. Because the complex radiation patterns associated with arrays frequently contain several lobes of varying intensity, you should learn to use appropriate terminology. In general, major lobes are those in which the greatest amount of radiation occurs. Minor lobes are those in which the radiation intensity is least.

DIRECTIONAL ARRAYS

4-116. You have already learned about radiation patterns and directivity of radiation. These topics are important to you because using an antenna with an improper radiation pattern or with the wrong directivity will decrease the overall performance of the system. In the following paragraphs, we discuss in more detail the various types of directional antenna arrays mentioned earlier in this chapter.

Collinear Array

4-117. The pattern radiated by the collinear array is similar to that produced by a single dipole. The addition of the second radiator, however, tends to intensify the pattern. Compare the radiation pattern of the dipole (figure 4-26, view A) and the two-element antenna in view B. You will see that each pattern consists of two major lobes in opposite directions along the same axis, QQ1. There is little or no radiation along the PP1 axis. QQ1 represents the line of maximum propagation. You can see that radiation is stronger with an added element. The pattern in view B is sharper, or more directive, than that in view A. This means that the gain along the line of maximum energy propagation is increased and the beam width is decreased.

As more elements are added, the effect is heightened, as shown in view C. Unimportant minor lobes are generated as more elements are added.

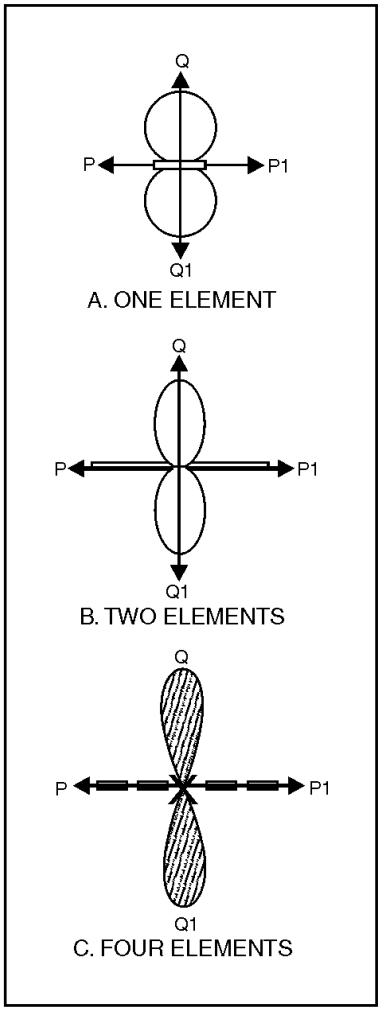


Figure 4-26. Single Half-Wave Antenna versus Two Half-Wave Antenna in Phase

4-118. More than four elements are seldom used because accumulated losses cause the elements farther from the point of feeding to have less current than the nearer ones. This introduces an unbalanced condition in the system and impairs its efficiency. Space limitations often are another reason for restricting the number of elements. Because this type of array is in a single line, rather than in a vertically stacked arrangement, the use of too many elements results in an antenna several wavelengths long.

4-119. **Radiation pattern**. The characteristic radiation pattern of a given array is obtained at the frequency or band of frequencies at which the system is resonant. The gain and directivity characteristics are lost when the antenna is not used at or near this frequency and the array tunes too sharply. A collinear antenna is more effective than an end-fire array when used off its tuned frequency. This feature is considered when transmission or reception is to be over a wide frequency band. When more than two elements are used, this advantage largely disappears.

4-120. **Length and phasing**. Although the one-half wavelength is the basis for the collinear element, you will find that greater lengths are often used. Effective arrays of this type have been constructed in which the elements are 0.7 and even 0.8 wavelength long. This type of array provides efficient operation at more than one frequency or over a wider frequency range. Whatever length is decided upon, all of the elements in a particular array should closely adhere to that length. If elements of different lengths are combined, current phasing and distribution are changed, throwing the system out of balance and seriously affecting the radiation pattern.

4-121. **Spacing**. The lower relative efficiency of collinear arrays of many elements, compared with other multi-element arrays, relates directly to spacing and mutual impedance effects. Mutual impedance is an important factor to be considered when any two elements are parallel and are spaced so that considerable coupling is between them. There is very little mutual impedance between collinear sections. Where impedance does exist, it is caused by the coupling between the ends of adjacent elements. Placing the ends of elements close together is frequently necessary because of construction problems, especially where long lengths of wire are involved.

4-122. The effects of spacing and the advantages of proper spacing can be demonstrated by some practical examples. A collinear array consisting of two half-wave elements with one-half-wavelength spacing between centers has a gain of 1.8 decibels (dB). If the ends of these same dipoles are separated so that the distance from center to center is three-quarters of a wavelength and they are driven from the same source, the gain increases to approximately 2.9 dB.

4-123. A three-dipole array with negligible spacing between elements gives a gain of 3.3 dB. In other words, when two elements are used with wider spacing, the gain obtained is approximately equal to the gain obtainable from three elements with close spacing. The spacing of this array permits simpler construction, because only two dipoles are used. It also allows the antenna to occupy less space. Construction problems usually dictate small-array spacing.

Broadside Arrays

4-124. A broadside array is shown in figure 4-27, view A. Physically, it looks somewhat like a ladder. When the array and the elements in it are polarized horizontally, it looks like an upright ladder. When the array is polarized vertically, it looks like a ladder lying on one side (view B). View C is an illustration of the radiation pattern of a broadside array. Horizontally polarized arrays using more than two elements are not common. This is because the requirement that the bottom of the array be a significant distance above the earth presents construction problems. Compared with collinear arrays, broadside arrays tune sharply, but lose efficiency rapidly when not operated on the frequencies for which they are designed.

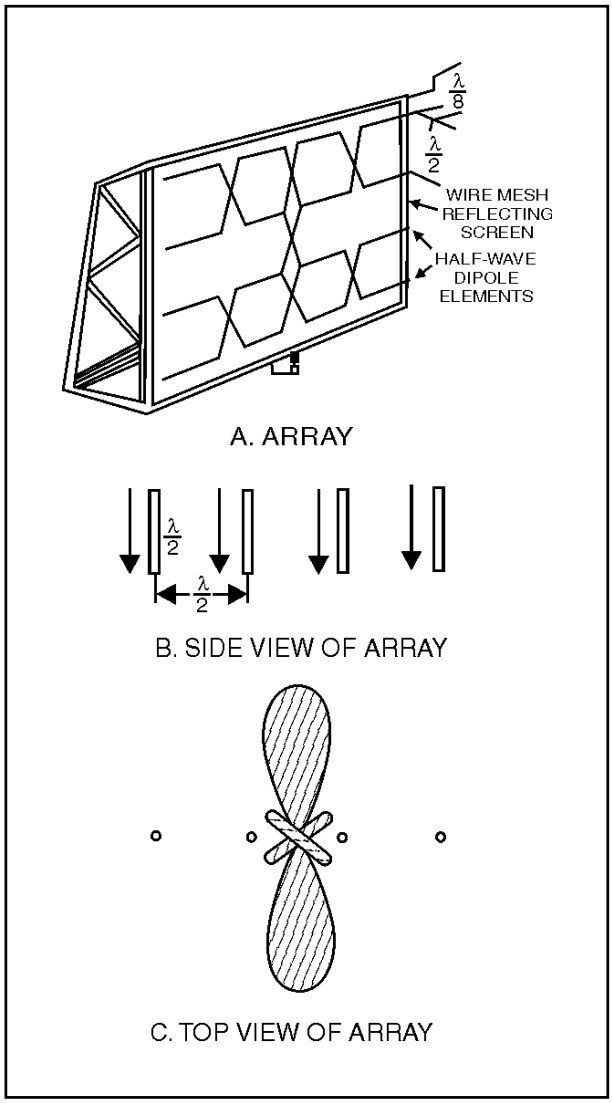


Figure 4-27. Typical Broadside Array

4-125. **Radiation pattern**. Figure 4-28 shows an end view of two parallel half-wave antennas (A and B) operating in the same phase and located one-half wavelength apart. At a point (P) far removed from the antennas, the antennas appear as a single point. Energy radiating toward P from antenna A starts out in phase with the energy radiating from antenna B in the same direction. Propagation from each antenna travels over the same distance to point P, arriving there in phase. The antennas reinforce each other in this direction, making a strong signal available at P. Field strength measured at P is greater than it would be if the total power supplied to both antennas had been fed to a single dipole. Radiation toward point P1 is built up in the same manner.

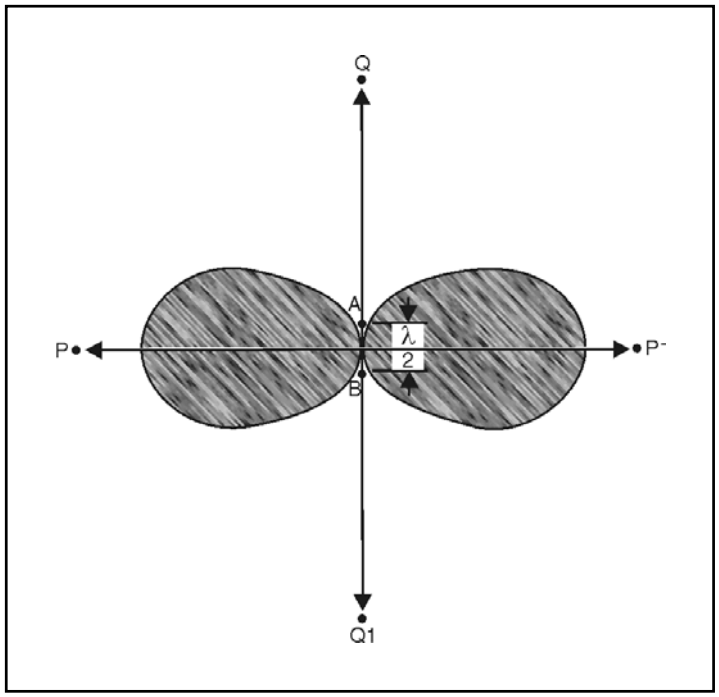


Figure 4-28. Parallel Elements in Phase

4-126. Next consider a wavefront traveling toward point Q from antenna B. By the time it reaches antenna A, one-half wavelength away, one-half cycle has elapsed. Therefore energy from antenna B meets the energy from antenna A 180 degrees out of phase. As a result, the energy moving toward point Q from the two sources cancels. In a like manner, radiation from antenna A traveling toward point Q1 meets and cancels the radiation in the same direction from antenna B. As a result, little propagation takes place in either direction along the QQ1 axis. Most of the energy is concentrated in both directions along the PP1 axis. When both antenna elements are fed from the same source, the result is the basic broadside array.

4-127. When more than two elements are used in a broadside arrangement, they are all parallel and in the same plane, as shown in figure 4-27, view B. Current phase, indicated by the arrows, must be the same for all elements. The radiation pattern shown in figure 4-27, view C, and is always bidirectional. This pattern is sharper than the one shown in figure 4-28 because of the additional two elements. Directivity and gain depend on the number of elements and the spacing between them.

4-128. **Gain and directivity**. The physical disposition of dipoles operated broadside to each other allows for much greater coupling between them than can occur between collinear elements. Moving the parallel antenna elements closer together or farther apart affects the actual impedance of the entire array and the overall radiation resistance as well. As the spacing between broadside elements increases, the effect on the radiation pattern is a sharpening of the major lobes. When the array consists of only two dipoles spaced exactly one-half wavelength apart, no minor lobes are generated at all. Increasing the distance between the elements beyond that point,

however, tends to throw off the phase relationship between the original current in one element and the current induced in it by the other element. The result is that, although the major lobes are sharpened, minor lobes are introduced, even with two elements. These minor lobes, however, are not large enough to be of concern.

4-129. If you add the same number of elements to both a broadside array and a collinear array, the gain of the broadside array will be greater. Reduced radiation resistance resulting from the efficient coupling between dipoles accounts for most of this gain. However, certain practical factors limit the number of elements that may be used. The construction problem increases with the number of elements, especially when they are polarized horizontally.

End-Fire Arrays

4-130. An end-fire array looks similar to a broadside array. The ladder-like appearance is characteristic of both (figure 4-29, view A). The currents in the elements of the end-fire array, however, are usually 180 degrees out of phase with each other as indicated by the arrows. The construction of the end-fire array is like that of a ladder lying on its side (elements horizontal). The dipoles in an end-fire array are closer together (one-eighth wavelength to one-quarter wavelength spacing) than they are for a broadside array.

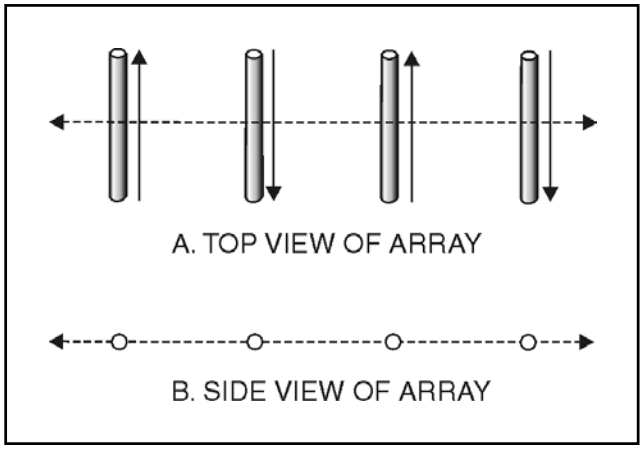


Figure 4-29. Typical End-Fire Array

4-131. Closer spacing between elements permits compactness of construction. For this reason, an end-fire array is preferred to other arrays when high gain or sharp directivity is desired in a confined space. However, the close coupling creates certain disadvantages. Radiation resistance is extremely low, sometimes as low as 10 ohms, making antenna losses greater. The end-fire array is confined to a single frequency. With changes in climatic or atmospheric conditions, the danger of detuning exists.

4-132. **Radiation pattern**. The radiation pattern for a pair of parallel half-wave elements fed 180 degrees out of phase is shown in figure 4-30, view A. The elements shown are spaced one-half wavelength apart. In practice, smaller spacings are used. Radiation from elements L and M traveling toward point P begins 180 degrees out of phase. Moving the same distance over approximately parallel paths, the respective wavefronts from these

elements remain 180 degrees out of phase. In other words, maximum cancellation takes place in the direction of P. The same condition is true for the opposite direction (toward P1). The P to P1 axis is the line of least radiation for the end-fire array.

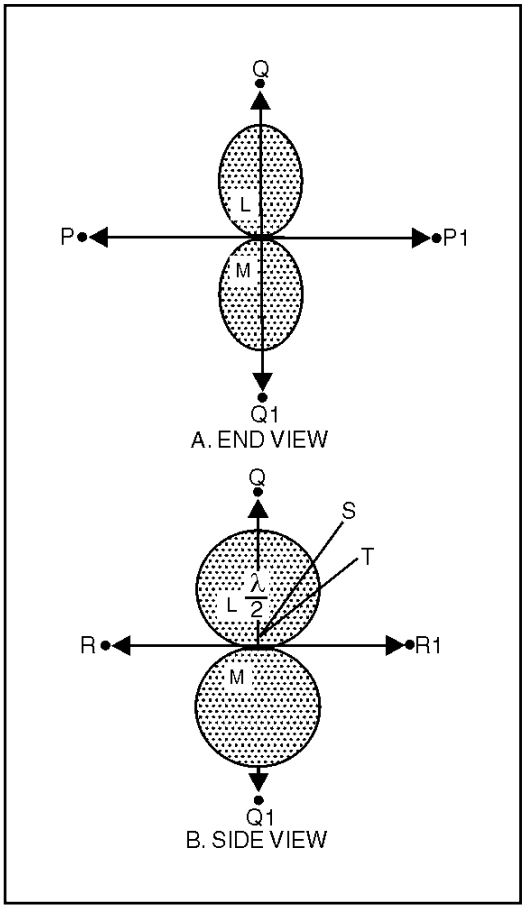


Figure 4-30. Parallel Elements 180 Degrees Out of Phase

4-133. Consider what happens along the QQ1 axis. Energy radiating from element M toward Q reaches element L in about one-half cycle (180 degrees) after it leaves its source. Because element L was fed 180 degrees out of phase with element M, the wavefronts are now in the same phase and are both moving toward Q and reinforcing each other. Similar reinforcement occurs along the same axis toward Q1. This simultaneous movement towards Q and Q1 develops a bidirectional pattern. This is not always true in end-fire operation. Another application of the end-fire principle is one in which the elements are spaced one-quarter wavelength apart and phased 90 degrees from each other to produce a unidirectional pattern.

4-134. In figure 4-30, view A, elements A and B are perpendicular to the plane represented by the page; therefore, only the ends of the antennas appear. In view B, the antennas are rotated a quarter of a circle in space around the QQ1 axis so that they are seen in the plane of the elements themselves. Therefore, the PP1 axis, now perpendicular to the page, is not

seen as a line. The RR1 axis, now seen as a line, is perpendicular to the PP1 axis as well as to the QQ1 axis. The end-fire array is directional in this plane also, although not quite as sharply. The reason for the greater broadness of the lobes can be seen by following the path of energy radiating from the midpoint of element B toward point S in view B. This energy passes the A element at one end after traveling slightly more than the perpendicular distance between the dipoles. Energy, therefore, does not combine in exact phase toward point S. Although maximum radiation cannot take place in this direction, energy from the two sources combines closely enough in phase to produce considerable reinforcement. A similar situation exists for wavefronts traveling toward T. However; the wider angle from Q to T produces a greater phase difference and results in a decrease in the strength of the combined wave.

4-135. Directivity occurs from either one or both ends of the end-fire array, along the axis of the array, as shown by the broken arrows in figure 4-29, view A; hence, the term end-fire is used.

4-136. The major lobe or lobes occur along the axis of the array. The pattern is sharper in the plane that is at right angles to the plane containing the elements (figure 4-30, view A). If the elements are not exact half-wave dipoles, operation is not significantly affected. However, because of the required balance of phase relationships and critical feeding, the array must be symmetrical. Folded dipoles, such as the one shown in figure 4-21, view A, are used frequently because the impedance at their terminals is higher. This is an effective way of avoiding excessive antenna losses. Another expedient to reduce losses is the use of tubular elements of wide diameter.

4-137. **Gain and directivity**. In end-fire arrays, directivity increases with the addition of more elements and with spacings approaching the optimum. The directive pattern for a two-element, bidirectional system is illustrated in figure 4-30. View A shows radiation along the array axis in a plane perpendicular to the dipoles, and view B shows radiation along the array axis in the plane of the elements. These patterns were developed with a 180-degree phase difference between the elements. Additional elements introduce small, minor lobes.

4-138. With a 90-degree phase difference in the energy fed to a pair of end-fire elements spaced approximately one-quarter wavelength apart, unidirectional radiation can be obtained. The pattern perpendicular to the plane of the two elements is shown in figure 4-31, view A. The pattern shown in view B, taken in the same plane, is for a six-element array with 90-degree phasing between adjacent elements. Because both patterns show relative gain only, the increase in gain produced by the six-element array is not evident. End-fire arrays are the only unidirectional arrays wholly made up of driven elements.

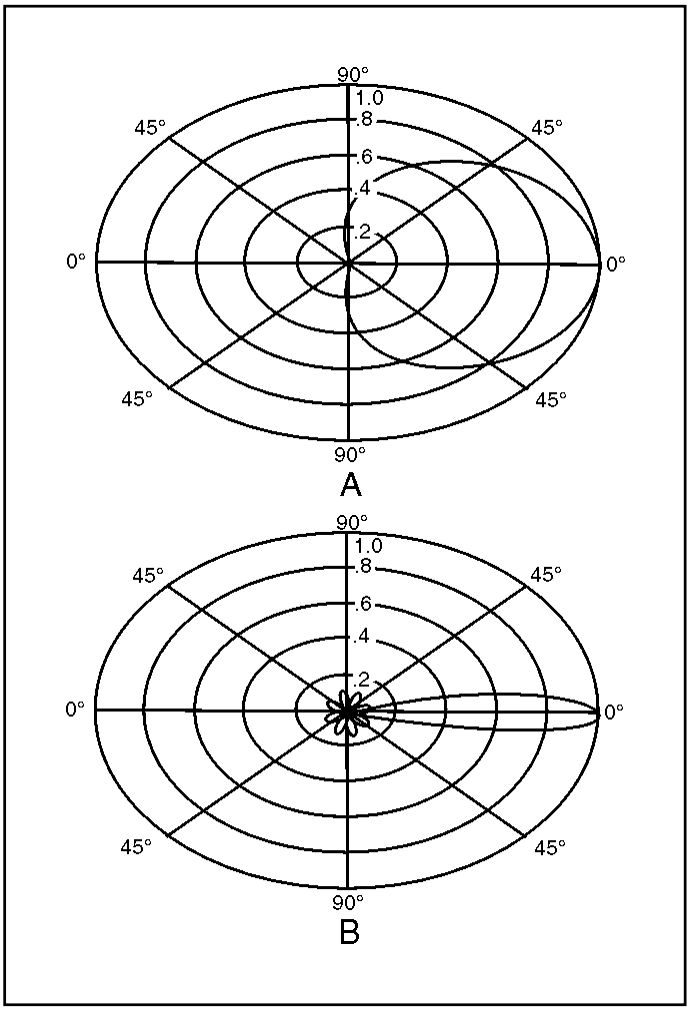


Figure 4-31. Unidirectional End-Fire Arrays

Parasitic Arrays

4-139. If a small light bulb were placed in the center of a large room, the illumination would be very poor. However, if a reflector were placed behind the bulb, the space in front of the reflector would be brighter and the space behind the reflector would be dimmer. The light rays would be concentrated. Also, if a lens were placed in front of the bulb, the light would be even more concentrated and a very bright spot would appear on the wall in front of the lens. A flashlight is a practical combination of the small bulb, the reflector, and the lens. The energy from an antenna can be reflected and concentrated in a similar manner.

4-140. Although we do not usually discuss the gain of a flashlight, we can continue the comparison of an antenna and a flashlight to explain the meaning of antenna gain. Suppose the spot on the wall in front of the flashlight becomes 10 times brighter than it was when only the open bulb was used. The lens and reflector have then produced a 10-fold gain in light. For antennas, the simple half-wave antenna corresponds to the open bulb in

the flashlight. Suppose an antenna system concentrates the radio waves so that at a particular point the field strength is 10 times more than it would be at the same distance from a half-wave antenna. The antenna system is then said to have a gain of 10.

4-141. Parasitic arrays represent another method of achieving high antenna gains. A parasitic array consists of one or more parasitic elements placed in parallel with each other and, in most cases, at the same line-of-sight level. The parasitic element is fed inductively by radiated energy coming from the driven element connected to the transmitter. It is in no way connected directly to the driven element.

4-142. When the parasitic element is placed so that it radiates away from the driven element, the element is a director. When the parasitic element is placed so that it radiates toward the driven element, the parasitic element is a reflector.

4-143. The directivity pattern resulting from the action of parasitic elements depends on two factors:

- The tuning determined by the length of the parasitic element.
- The spacing between the parasitic and driven elements.

To a lesser degree, the directivity pattern also depends on the diameter of the parasitic element, because diameter has an effect on tuning.

4-144. **Operation**. When a parasitic element is placed a fraction of a wavelength away from the driven element and is of approximately resonant length, it will re-radiate the energy it intercepts. The parasitic element is effectively a tuned circuit coupled to the driven element, much as the two windings of a transformer are coupled together. The radiated energy from the driven element causes a voltage to be developed in the parasitic element, which, in turn, sets up a magnetic field. This magnetic field extends over to the driven element, which then has a voltage induced in it. The magnitude and phase of the induced voltage depend on the length of the parasitic element and the spacing between the elements. In actual practice the length and spacing are arranged so that the phase and magnitude of the induced voltage cause a unidirectional, horizontal-radiation pattern and an increase in gain.

4-145. In the parasitic array in figure 4-32, view A, the parasitic and driven elements are spaced one-quarter wavelength apart. The radiated signal coming from the driven element strikes the parasitic element after one-quarter cycle. The voltage developed in the parasitic element is 180 degrees out of phase with that of the driven element. This is because of the distance traveled (90 degrees) and because the induced current lags the inducing flux by 90 degrees (90 + 90 = 180 degrees). The magnetic field set up by the parasitic element induces a voltage in the driven element one-quarter cycle later because the spacing between the elements is one-quarter wavelength. This induced voltage is in phase with that in the driven element and causes an increase in radiation in the direction indicated in figure 4-32, view A. Because the direction of the radiated energy is stronger in the direction away from the parasitic element (toward the driven element), the parasitic element is called a reflector. The radiation pattern as it would appear if you were looking down on the antenna is shown in view B. The pattern as it would look if viewed from the ends of the elements is shown in view C.

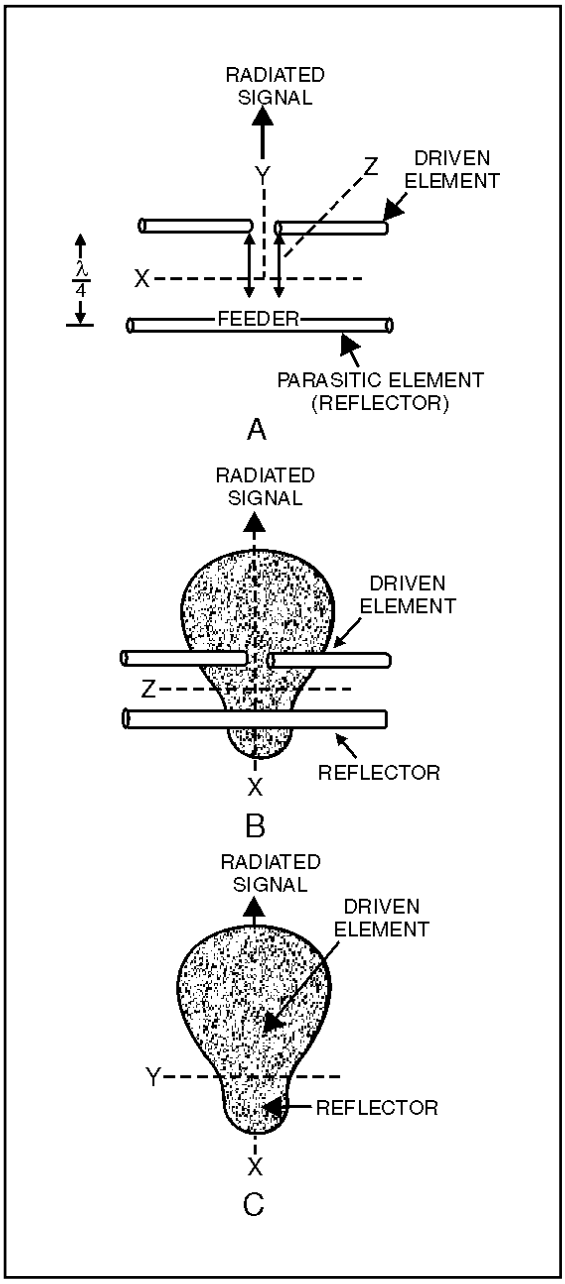


Figure 4-32. Patterns Obtained Using a Reflector with Proper Spacing

4-146. Because the voltage induced in the reflector is 180 degrees out of phase with the signal produced at the driven element, a reduction in signal strength exists behind the reflector. Because the magnitude of an induced voltage never quite equals that of the inducing voltage, even in very closely coupled circuits, the energy behind the reflector (minor lobe) is not reduced to 0.

4-147. The spacing between the reflector and the driven element can be reduced to about 15 percent of a wavelength. The parasitic element must be

made electrically inductive before it will act as a reflector. If this parasitic element is made about 5 percent longer than one-half wavelength, it will act as a reflector when the spacing is 15 percent of a wavelength.

4-148. Changing the spacing and length can change the radiation pattern so that maximum radiation is on the same side of the driven element as the parasitic element. In this instance, the parasitic element is called a director.

4-149. Combining a reflector and a director with the driven element causes a decrease in back radiation and an increase in directivity. This combination results in the two main advantages of a parasitic array—unidirectivity and increased gain. If the parasitic array is rotated, it can pick up or transmit in different directions because of the reduction of transmitted energy in all but the desired direction. An antenna of this type is called a rotary array. Size for size, both the gain and directivity of parasitic arrays are greater than those of driven arrays. The disadvantage of parasitic arrays is that their adjustment is critical and they do not operate over a wide frequency range.

4-150. **Gain and directivity**. Changing the spacing between either the director or the reflector and the driven element results in a change in the radiation pattern. More gain and directivity are obtained by changing the length of the parasitic elements.

4-151. The front-to-back ratio of an array is the proportion of energy radiated in the principal direction of radiation to the energy radiated in the opposite direction. A high front-to-back ratio is desirable because this means that a minimum amount of energy is radiated in the undesired direction. Because completely suppressing all such radiation is impossible, an infinite ratio cannot be achieved. In actual practice, however, rather high values can be attained. Usually the length and spacing of the parasitic elements are adjusted so that a maximum front-to-back ratio is obtained, rather than maximum gain in the desired direction.

Multi-Element Parasitic Array

4-152. A multi-element parasitic array is one that contains two or more parasitic elements with the driven element. If the array contains two parasitic elements (a reflector and a director) in addition to the driven element, it is usually known as a three-element array. If three parasitic elements are used, the array is known as a four-element array, and so on. Generally speaking, if more parasitic elements are added to a three-element array, each added element is a director. The field behind a reflector is so small that additional reflectors would have little effect on the overall radiation pattern. In radar, from one to five directors are used.

4-153. **Construction**. The parasitic elements of a multi-element parasitic array usually are positioned as shown in figure 4-33, views A and B. Proper spacings and lengths are determined experimentally. A folded dipole (view B) is often used as the driven element to obtain greater values of radiation resistance.

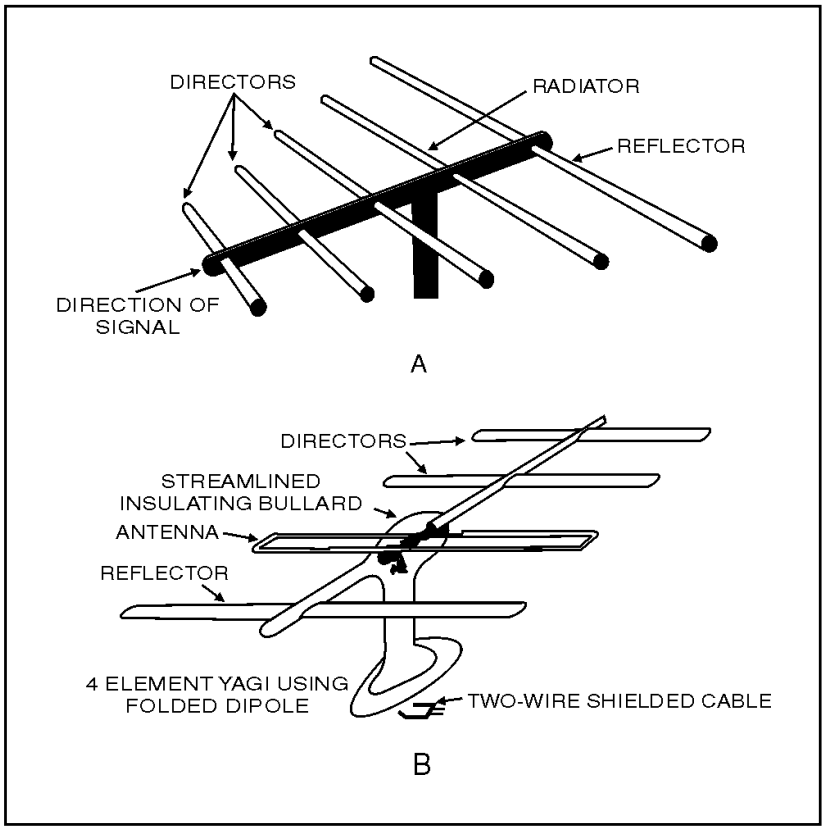


Figure 4-33. Yagi Antenna

4-154. **Yagi antennas**. An example of a multi-element parasitic array is the yagi antenna (figure 4-33, views A and B). The spacings between the elements are not uniform. The radiation from the different elements arrives in phase in the forward direction, but out of phase by various amounts in the other directions.

4-155. The director and the reflector in the yagi antenna are usually welded to a conducting rod or tube at their centers. This support does not interfere with the operation of the antenna. Because the driven element is center-fed, it is not welded to the supporting rod. Using a folded dipole as the driven element can increase the center impedance.

4-156. The yagi antenna shown in figure 4-33, view A, has three directors. In general, the greater number of parasitic elements used, the greater the gain. However, a greater number of such elements cause the array to have a narrower frequency response as well as a narrower beam width. Therefore, proper adjustment of the antenna is critical. The gain does not increase directly with the number of elements used. For example, a three-element yagi array has a relative power gain of 5 dB. Adding another director results in a 2 dB increase. Additional directors have less and less effect.

4-157. A typical yagi array used for receiving and transmitting energy is shown with a support frame in figure 4-34. This antenna is used by the military services. It operates at frequencies of from 12 to 50 megahertz and

consists of two separate arrays (one high frequency and one low frequency antenna array) mounted on one frame. The various elements are indicated in the figure. The high-frequency (HF) array consists of one reflector, one driven element, and two directors; the low-frequency (LF) array has the same arrangement with one less director. The lengths of the elements in the high-frequency array are shorter than those in the low-frequency array. The physical lengths of the elements in the individual arrays are equal, but the electrical lengths can be varied by means of the tuning stubs at the center of the elements. The array can be rotated in any desired direction by a remotely controlled, electrically driven, antenna rotator.

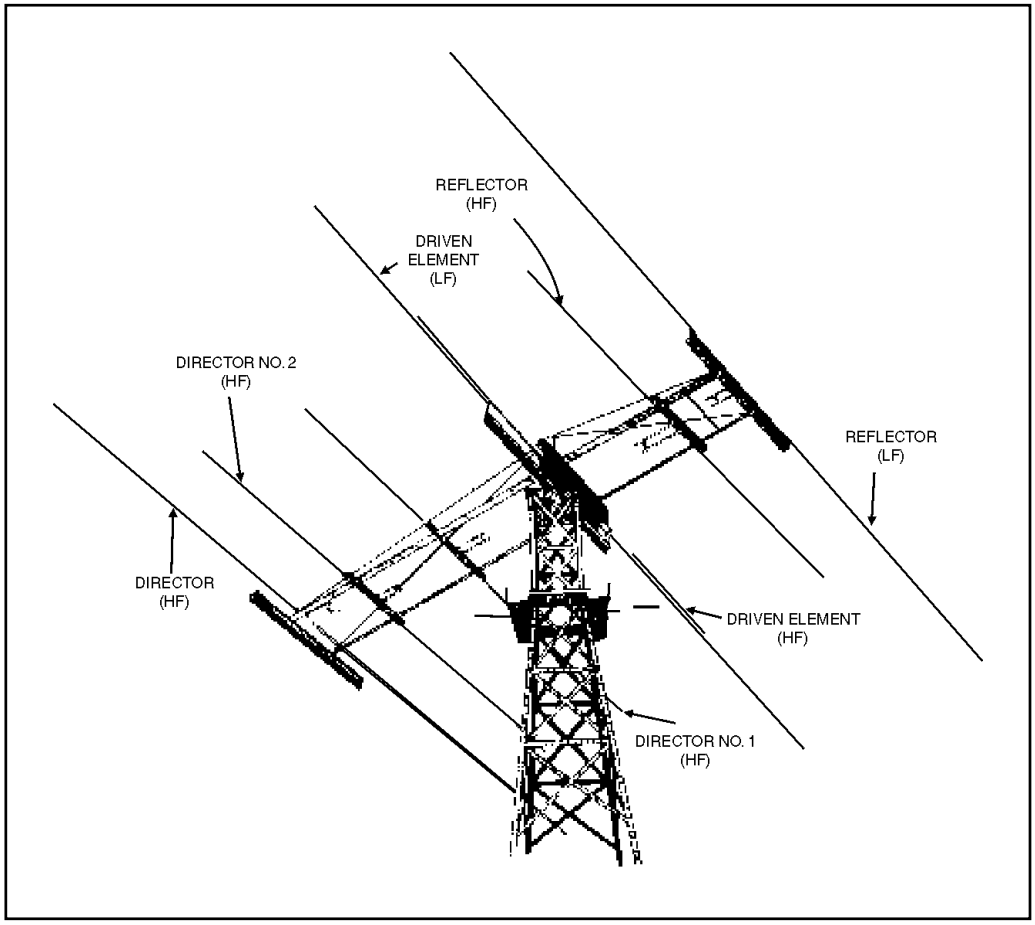


Figure 4-34. Typical Parasitic Array Used for Transmitting and Receiving

SPECIAL ANTENNAS

4-158. In this section we cover some special communications and radar antennas. Some of these antennas we touch on only briefly because they are covered thoroughly in other courses.

4-159. Previously discussed antennas operate with standing waves of current and voltage along the wires. This section deals principally with antenna systems in which the current is practically uniform in all parts of the antenna. In its basic form, such an antenna consists of a single wire grounded at the far end through a resistor. The resistor has a value equal to

the characteristic impedance of the antenna. This termination, just as in the case of an ordinary transmission line, eliminates standing waves. The current, therefore, decreases uniformly along the wire as the terminated end is approached. This decrease is caused by the loss of energy through radiation. The energy remaining at the end of the antenna is dissipated in the terminating resistor. For such an antenna to be a good radiator, its length must be fairly long. Also, the wire must not be too close to the ground. The return path through the ground will cause cancellation of the radiation. If the wire is sufficiently long, it will be practically nonresonant over a wide range of operating frequencies.

Long-Wire Antenna

4-160. A long-wire antenna is an antenna that is one wavelength or longer at the operating frequency. In general, the gain achieved with long-wire antennas is not as great as the gain obtained from the multi-element arrays studied in the previous section. But the long-wire antenna has advantages of its own. The construction of long-wire antennas is simple, both electrically and mechanically, with no particularly critical dimensions or adjustments. The long-wire antenna will work well and give satisfactory gain and directivity over a frequency range up to twice the value for which it was cut. In addition, it will accept power and radiate it efficiently on any frequency for which its overall length is not less than approximately one-half wavelength. Another factor is that long-wire antennas have directional patterns that are sharp in both the horizontal and vertical planes. Also, they tend to concentrate the radiation at the low vertical angles.

4-161. Another type of long-wire antenna is the beverage antenna, also called a wave antenna. It is a horizontal, long-wire antenna designed especially for the reception and transmission of low frequency, vertically polarized ground waves. It consists of a single wire, two or more wavelengths long, supported 3 to 6 meters above the ground, and terminated in its characteristic impedance, as shown in figure 4-35.

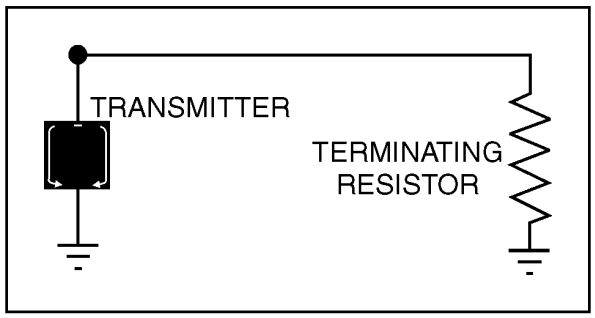


Figure 4-35. Beverage Antenna

V Antenna

4-162. A V antenna is a bidirectional antenna used widely in military and commercial communications. It consists of two conductors arranged to form a V. Each conductor is fed with currents of opposite polarity.

4-163. The V is formed at such an angle that the main lobes reinforce along the line bisecting the V and make a very effective directional antenna (see

figure 4-36). Connecting the two-wire feed line to the apex of the V and exciting the two sides of the V 180 degrees out of phase causes the lobes to add along the line of the bisector and to cancel in other directions, as shown in figure 4-37. The lobes are designated 1, 2, 3, and 4 on leg AA', and 5, 6, 7, and 8 on leg BB'. When the proper angle between AA' and BB' is chosen, lobes 1 and 4 have the same direction and combine with lobes 7 and 6, respectively. This combination of two major lobes from each leg results in the formation of two stronger lobes, which lie along an imaginary line bisecting the enclosed angle. Lobes 2, 3, 5, and 8 tend to cancel each other, as do the smaller lobes, which are approximately at right angles to the wire legs of the V. The resultant waveform pattern is shown at the right of the V antenna in figure 4-37.

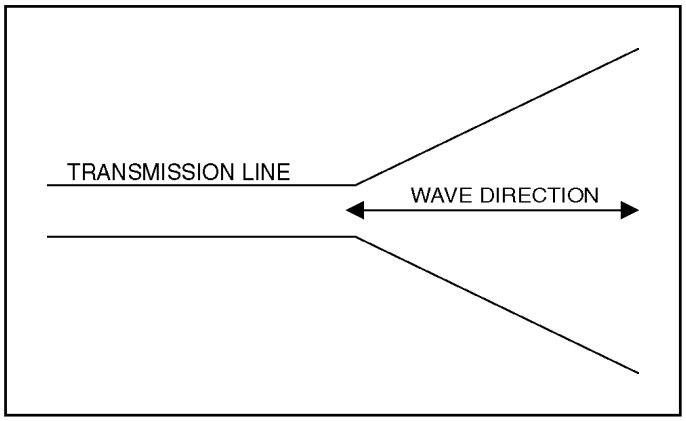


Figure 4-36. Basic V Antenna

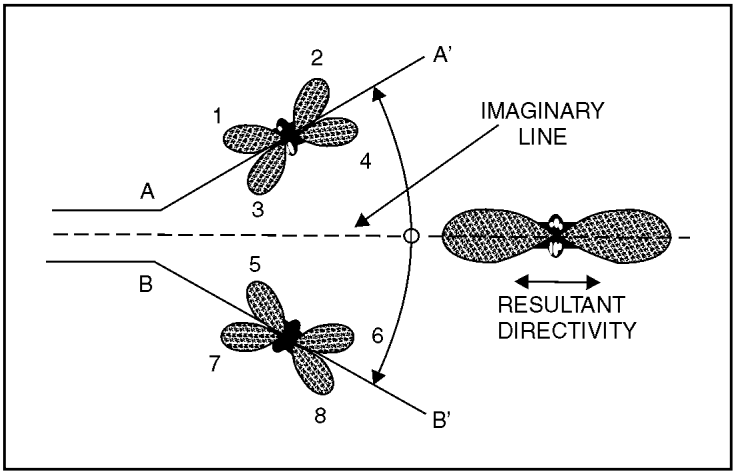


Figure 4-37. Formation of Directional Radiation from a Resonant V Antenna

Rhombic Antenna

4-164. The highest development of the long-wire antenna is the rhombic antenna (see figure 4-38). It consists of four conductors joined to form a rhombus, or diamond shape. The antenna is placed end to end and

terminated by a noninductive resistor to produce a unidirectional pattern. A rhombic antenna can be made of two obtuse-angle V antennas that are placed side by side, erected in a horizontal plane, and terminated so the antenna is nonresonant and unidirectional. The rhombic antenna is widely used for long-distance, high-frequency transmission and reception. It is one of the most popular fixed-station antennas because it is very useful in point-to-point communications.

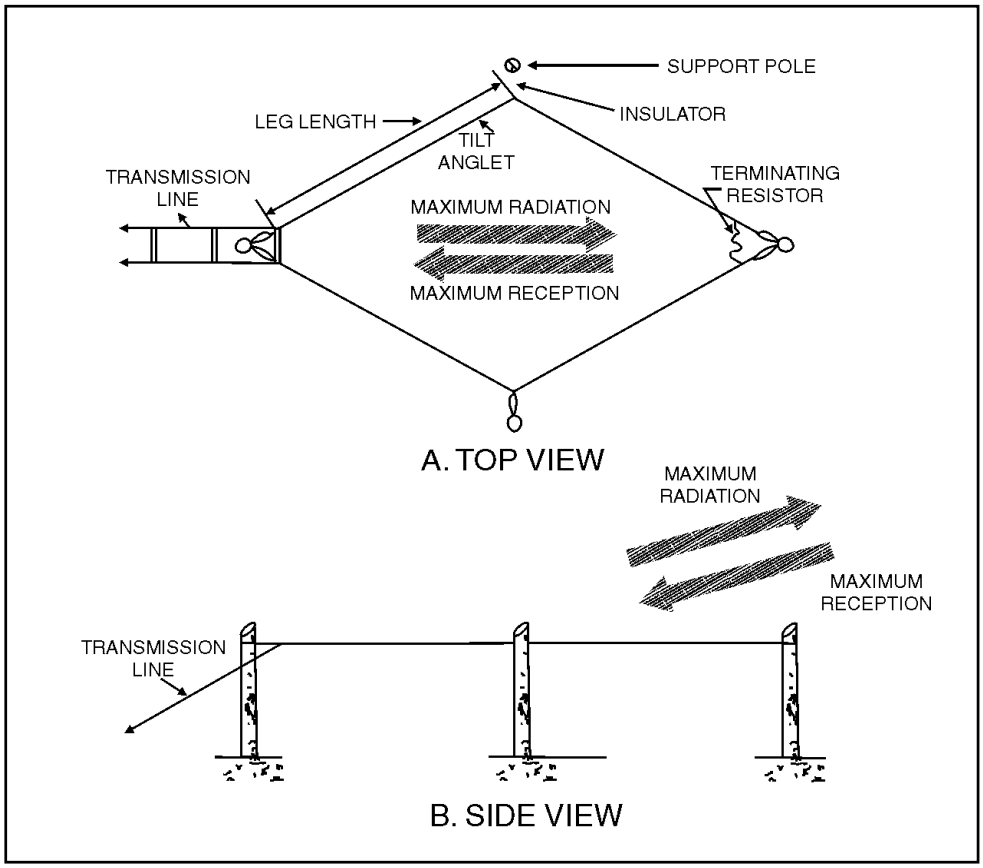


Figure 4-38. Basic Rhombic Antenna

4-165. **Advantages**. The rhombic antenna is useful over a wide frequency range. Although some changes in gain, directivity, and characteristic impedance do occur with a change in operating frequency, these changes are small enough to be ignored.

4-166. The rhombic antenna is much easier to construct and maintain than other antennas of comparable gain and directivity. Only four supporting poles of common heights from 15 to 20 meters are needed for the antenna.

4-167. The rhombic antenna also has the advantage of being noncritical as far as operation and adjustment are concerned. This is because of the broad frequency characteristics of the antenna.

4-168. Still another advantage is that the voltages present on the antenna are much lower than those produced by the same input power on a resonant

antenna. This is particularly important when high transmitter powers are used or when high-altitude operation is required.

4-169. **Disadvantages**. The rhombic antenna is not without its disadvantages. The principal one is that a fairly large antenna site is required for its erection. Each leg is made at least 1 or 2 wavelengths long at the lowest operating frequency. When increased gain and directivity are required, legs of from 8 to 12 wavelengths are used. These requirements mean that high-frequency rhombic antennas have wires of several hundred feet in length. Therefore, they are used only when a large plot of land is available.

4-170. Another disadvantage is that the horizontal and vertical patterns depend on each other. If a rhombic antenna is made to have a narrow horizontal beam, the beam is also lower in the vertical direction. Therefore, obtaining high vertical-angle radiation is impossible except with a very broad horizontal pattern and low gain. Rhombic antennas are used, however, for long-distance skywave coverage at the high frequencies. Under these conditions low vertical angles of radiation (less than 20 degrees) are desirable. With the rhombic antenna, a considerable amount of the input power is dissipated uselessly in the terminating resistor. However, this resistor is necessary to make the antenna unidirectional. The great gain of the antenna more than makes up for this loss.

4-171. **Radiation patterns**. Figure 4-39 shows the individual radiation patterns produced by the four legs of the rhombic antenna and the resultant radiation pattern. The principle of operation is the same as for the V and the half-rhombic antennas.

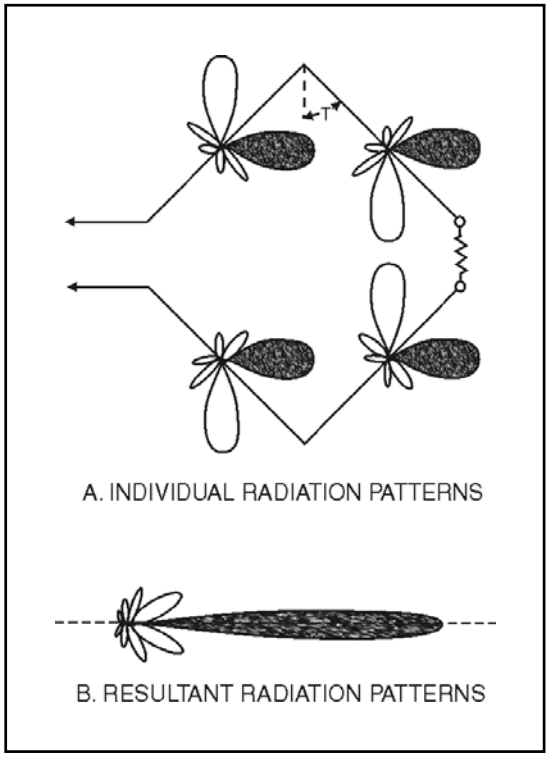


Figure 4-39. Formation of a Rhombic Antenna Beam

4-172. **Terminating resistor**. The terminating resistor plays an important part in the operation of the rhombic antenna. Upon it depend the unidirectivity of the antenna and the lack of resonance effects. An antenna should be properly terminated so it will have constant impedance at its input. Terminating the antenna properly will also allow it to be operated over a wide frequency range without needing to change the coupling adjustments at the transmitter. The reduction of back radiation is perhaps of lesser importance for transmission. When an antenna is terminated with resistance, the energy that would be radiated backward is absorbed in the resistor.

Turnstile Antenna

4-173. The turnstile antenna is one of the many types that has been developed primarily for omnidirectional VHF communications. The basic turnstile consists of two horizontal half-wave antennas mounted at right angles to each other in the same horizontal plane. When these two antennas are excited with equal currents 90 degrees out of phase, the typical figure-eight patterns of the two antennas merge to produce the nearly circular pattern shown in figure 4-40, view A. Pairs of such antennas are frequently stacked, as shown in figure 4-41. Each pair is called a bay. In figure 4-41 two bays are spaced one-half wavelength apart. Their corresponding elements are excited in phase. These conditions cause a part of the vertical radiation from each bay to cancel that of the other bay. This cancellation results in a decrease in energy radiated at high vertical angles and increases the energy radiated in the horizontal plane. Stacking a number of bays can alter the vertical radiation pattern, causing a substantial gain in a horizontal direction without altering the overall horizontal directivity pattern. Figure 4-40, view B, compares the circular vertical radiation pattern of a single-bay turnstile with the sharp pattern of a four-bay turnstile array. A three-dimensional radiation pattern of a four-bay turnstile antenna is shown in figure 4-40, view C.

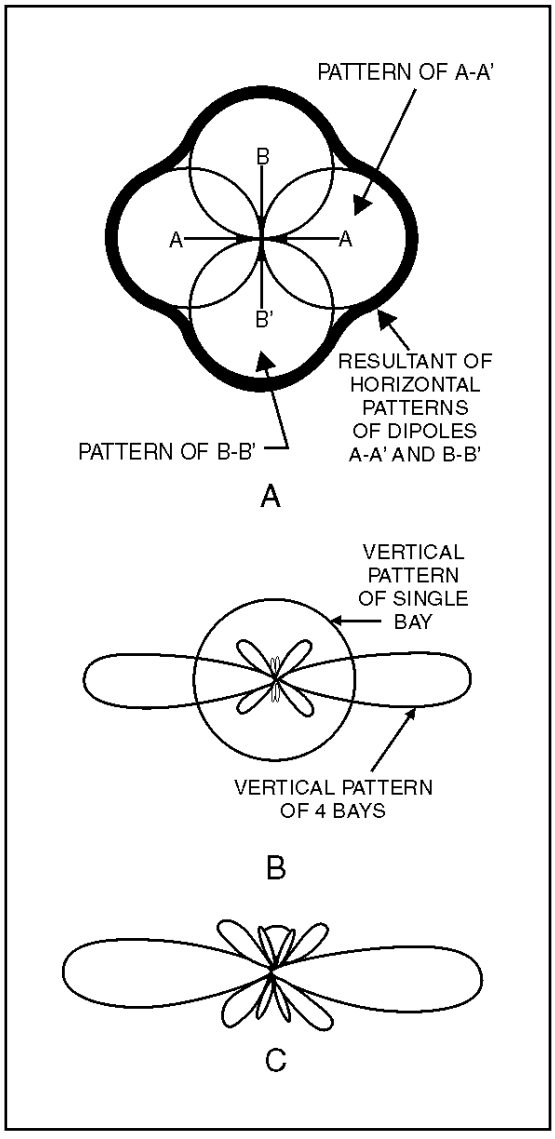


Figure 4-40. Turnstile Antenna Radiation Pattern

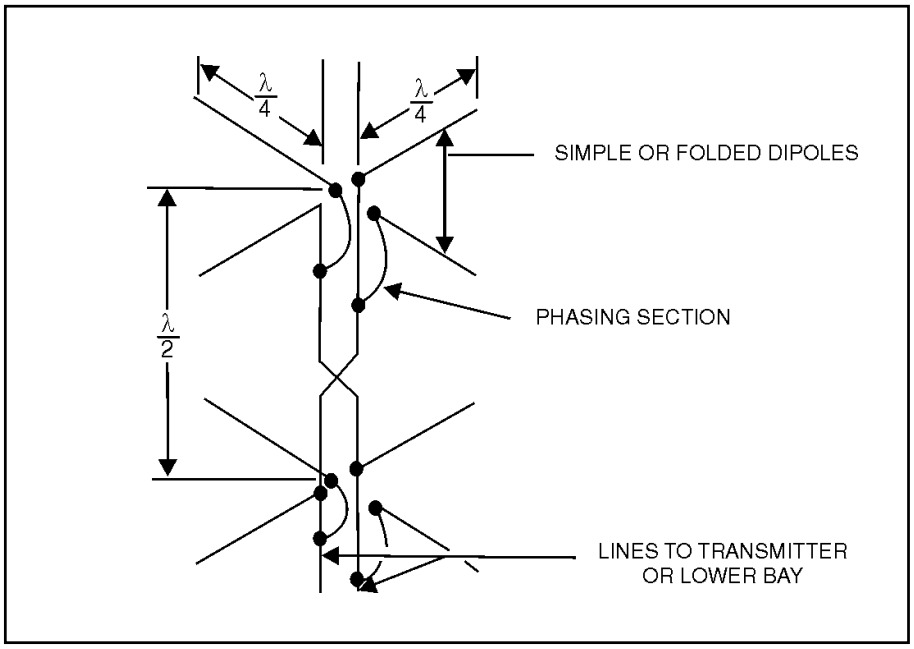


Figure 4-41. Stacked Turnstile Antenna

Ground-Plane Antenna

4-174. A vertical quarter-wave antenna several wavelengths above ground produces a high angle of radiation that is very undesirable at VHF and UHF frequencies. The most common means of producing a low angle of radiation from such an antenna is to work the radiator against a simulated ground called a ground plane. A simulated ground may be made from a large metal sheet or several wires or rods radiating from the base of the radiator. An antenna so constructed is known as a ground-plane antenna. Two ground-plane antennas are shown in figure 4-42, views A and B.

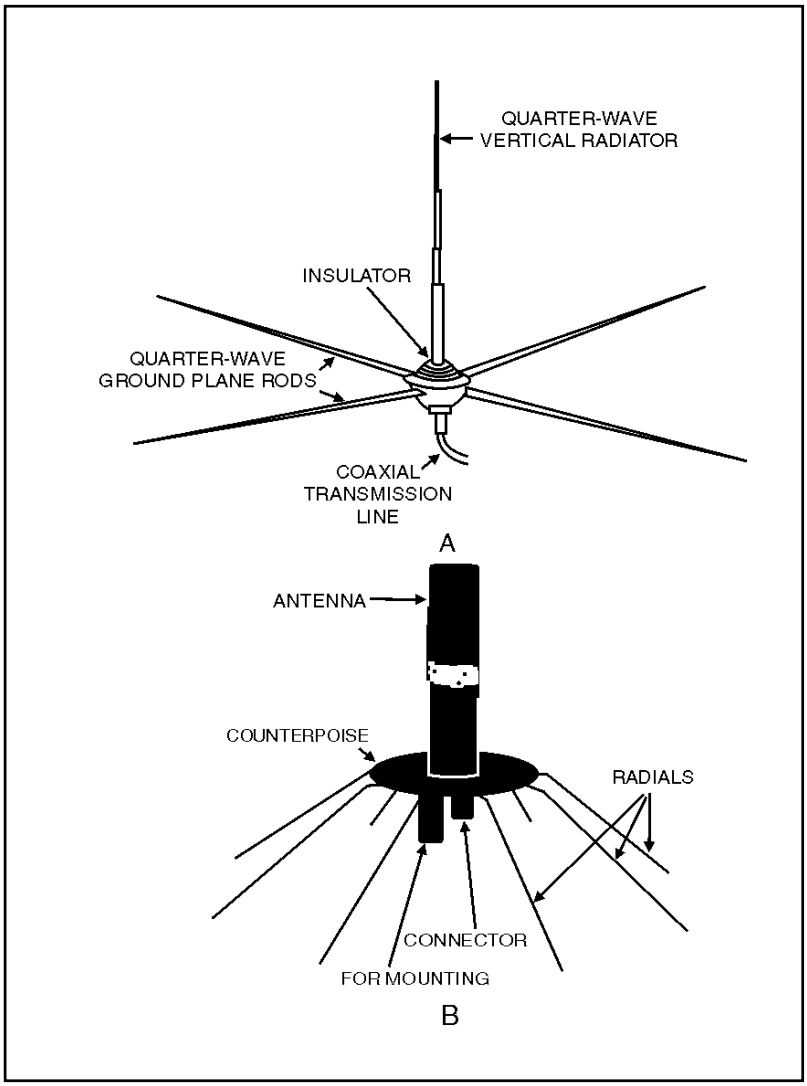


Figure 4-42. Ground-Plane Antenna

Corner Reflector

4-175. When a unidirectional radiation pattern is desired, it can be obtained by using a corner reflector with a half-wave dipole. A corner-reflector antenna is a half-wave radiator with a reflector. The reflector consists of two flat metal surfaces meeting at an angle immediately behind the radiator. In other words, the radiator is set in the plane of a line bisecting the corner angle formed by the reflector sheets. The construction of a corner reflector is shown in figure 4-43, view B Corner-reflector antennas are mounted with the radiator and the reflector in the horizontal position when horizontal polarization is desired. In such cases the radiation pattern is very narrow in the vertical plane, with maximum signal being radiated in line with the bisector of the corner angle. The directivity in the horizontal plane is approximately the same as for any half-wave radiator having a single-rod type reflector behind it. If the antenna is mounted with the radiator and the corner reflector in the vertical position, as shown in view A, maximum

radiation is produced in a very narrow horizontal beam. Radiation in a vertical plane will be the same as for a similar radiator with a single-rod type reflector behind it.

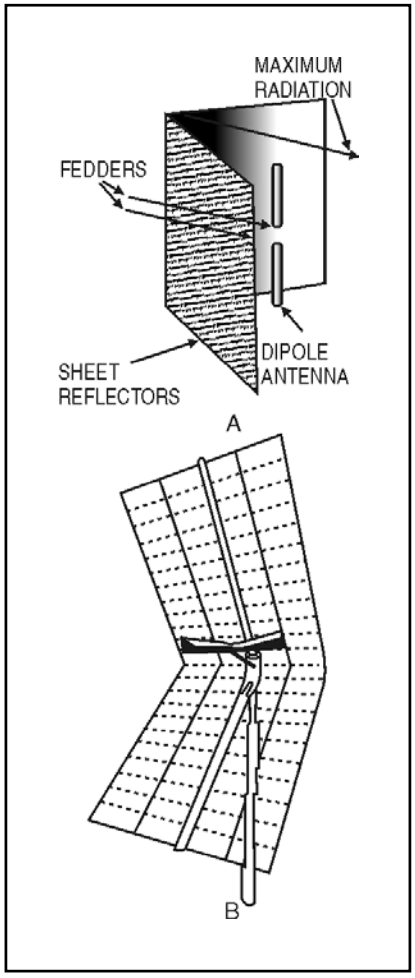


Figure 4-43. Corner-Reflector Antenna

SUMMARY

This chapter has presented information on the various types of antennas. The information that follows summarizes the important points of this chapter.

An antenna is a conductor, or system of conductors, that radiates or receives energy in the form of electromagnetic waves.

Hertz (half-wave) and Marconi (quarter-wave) are the two basic classifications of antennas.

Reciprocity of antennas means that the various properties of the antenna apply equally to transmitting and receiving.

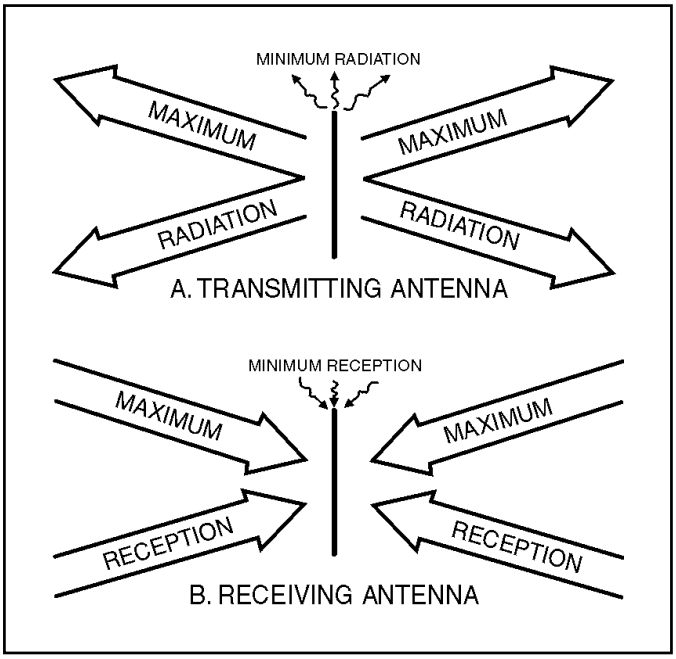


Figure 4-Sum 1. Reciprocity of Antennas

Radiation resistance is the amount of resistance that, if inserted in place of the antenna, would consume the same amount of power that is actually radiated by the antenna.

Radiation patterns can be plotted on a rectangular or polar-coordinate graph. These patterns are a measurement of the energy leaving an antenna.

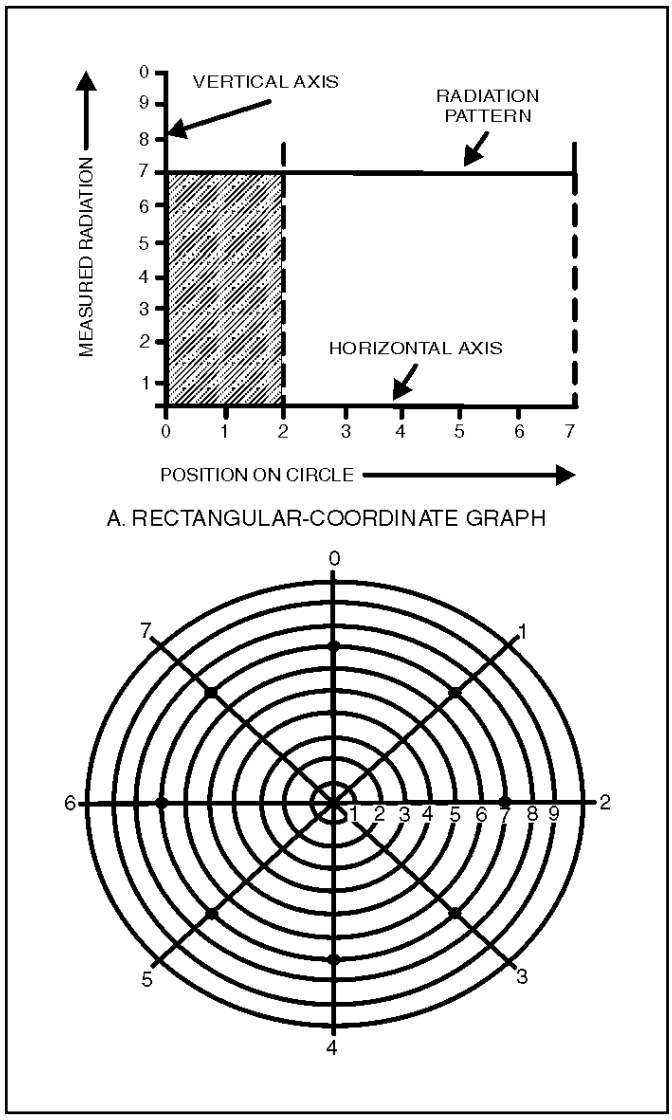


Figure 4-Sum 2. Radiation Patterns

An isotropic radiator radiates energy equally in all directions.

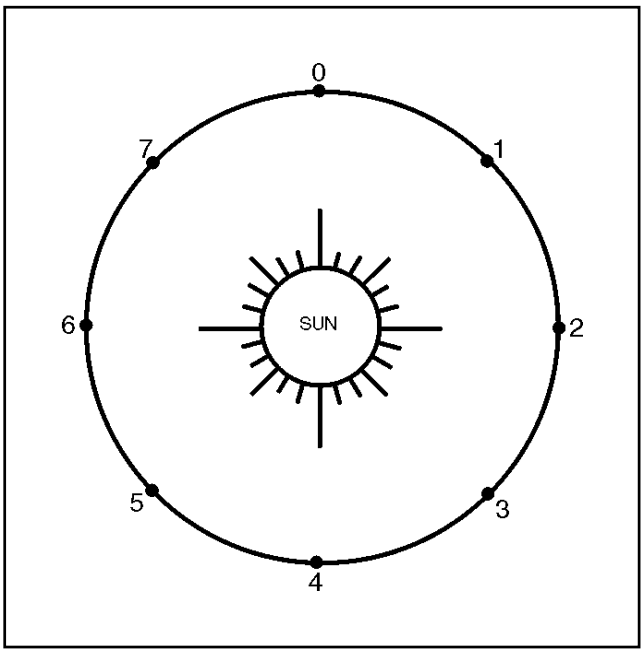


Figure 4-Sum 3. Radiating Energy of an Isotropic Radiator

An anisotropic radiator radiates energy directionally.

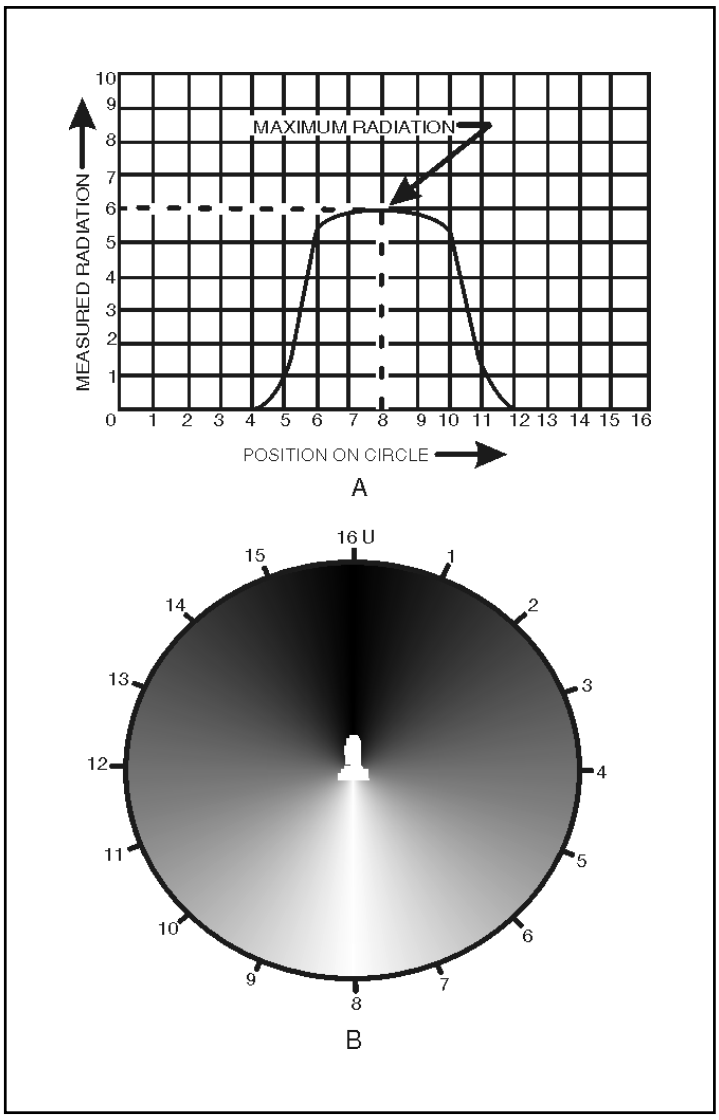


Figure 4-Sum 4. Directional Radiating Energy of an Anisotropic Radiator

A lobe is the area of a radiation pattern that is covered by radiation.

A null is the area of a radiation pattern that has minimum radiation.

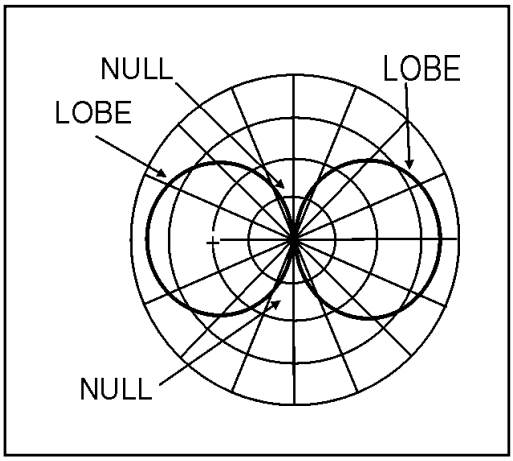


Figure 4-Sum 5. Null and Lobe Radiation Patterns

Antenna loading is the method used to change the electrical length of an antenna. This keeps the antenna in resonance with the applied frequency. It is accomplished by inserting a variable inductor or capacitor in series with the antenna.

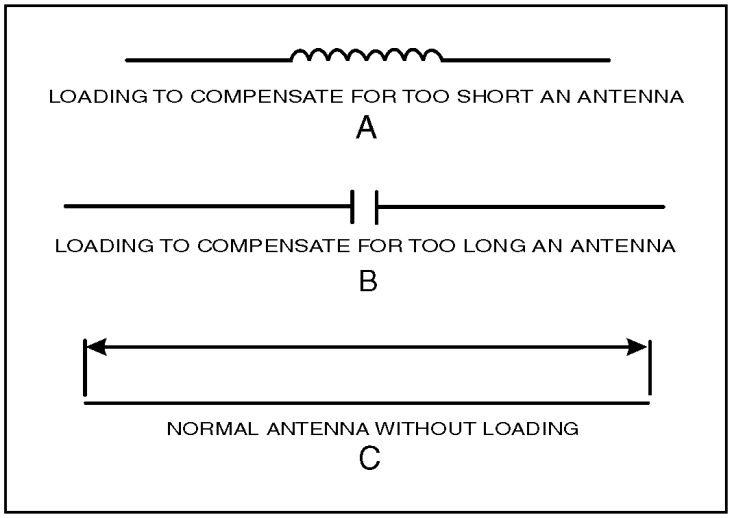


Figure 4-Sum 6. Antenna Loading

A half-wave antenna (Hertz) consists of two lengths of rod or tubing, each a quarter-wavelength long at a certain frequency, that radiate a doughnut pattern.

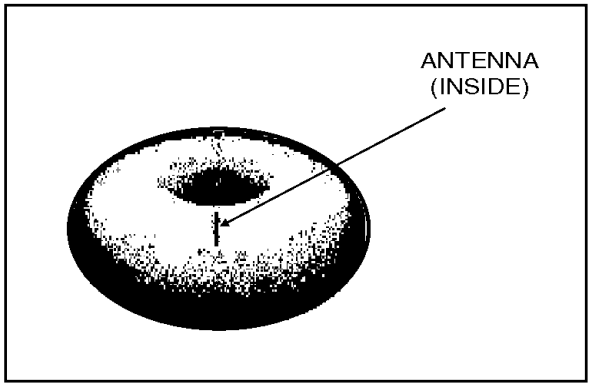


Figure 4-Sum 7. Half-Wave Antenna Pattern

A quarter-wave antenna (Marconi) is a half-wave antenna cut in half with one end grounded. The ground furnishes the missing half of the antenna.

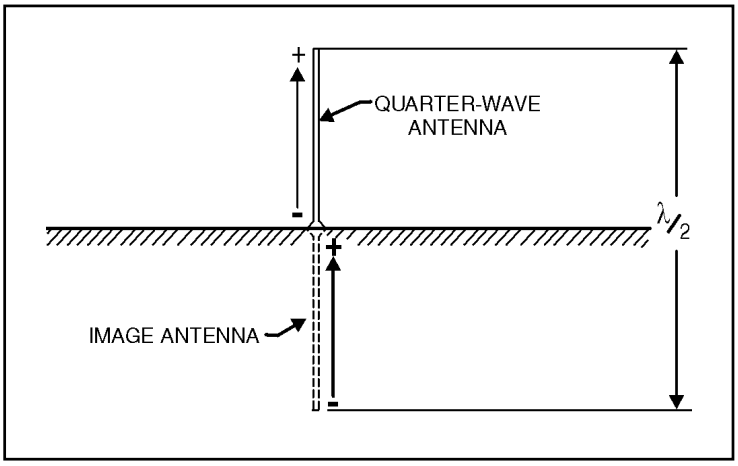


Figure 4-Sum 8. Quarter-Wave Antenna

The ground screen and the counterpoise are used to reduce losses caused by the ground in the immediate vicinity of the antenna. The ground screen is buried below the surface of the earth. The counterpoise is installed above the ground.

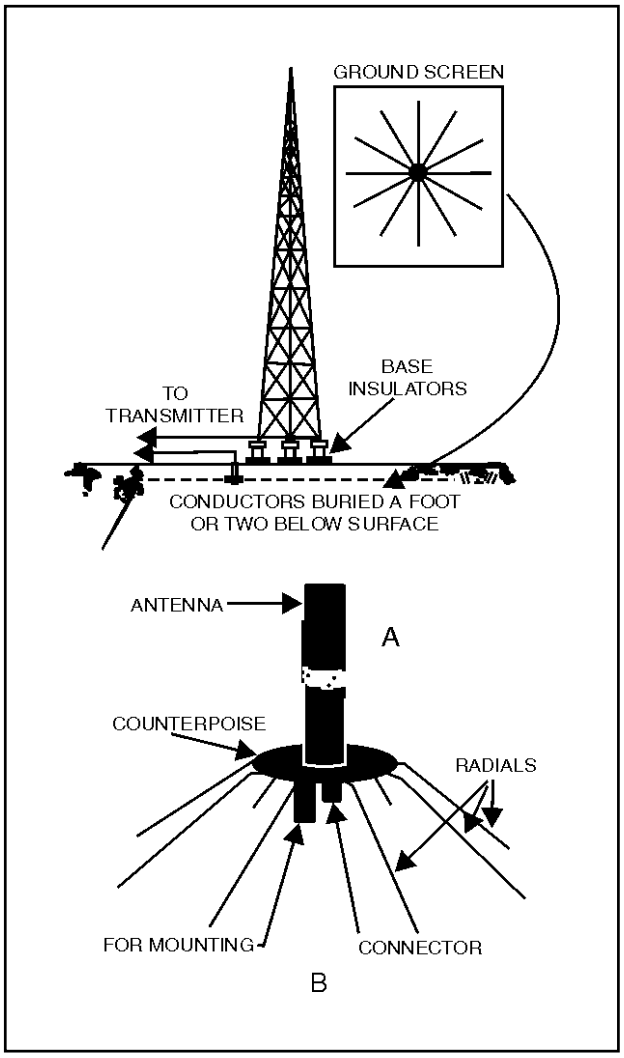


Figure 4-Sum 9. Ground Screen and Counterpoise Antennas

The folded dipole consists of a dipole radiator, which is connected in parallel at its ends to a half-wave radiator.

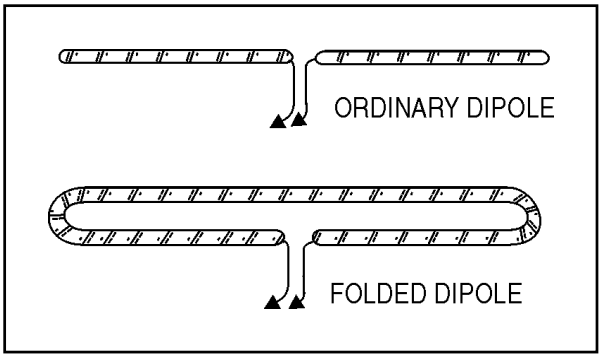


Figure 4-Sum 10. Folded Dipole

An array is a combination of half-wave elements operating together as a single antenna. It provides more gain and greater directivity than single element antennas.

A driven array derives its power directly from the source.

A parasitic array derives its power by coupling the energy from other elements of the antenna.

The bidirectional array radiates energy equally in two opposing directions.

The unidirectional array radiates energy efficiently in a single direction.

The collinear array has elements in a straight line. Maximum radiation occurs at right angles to this line.

The broadside array has elements parallel and in the same plane. Maximum radiation develops in the plane at right angles to the plane of the elements.

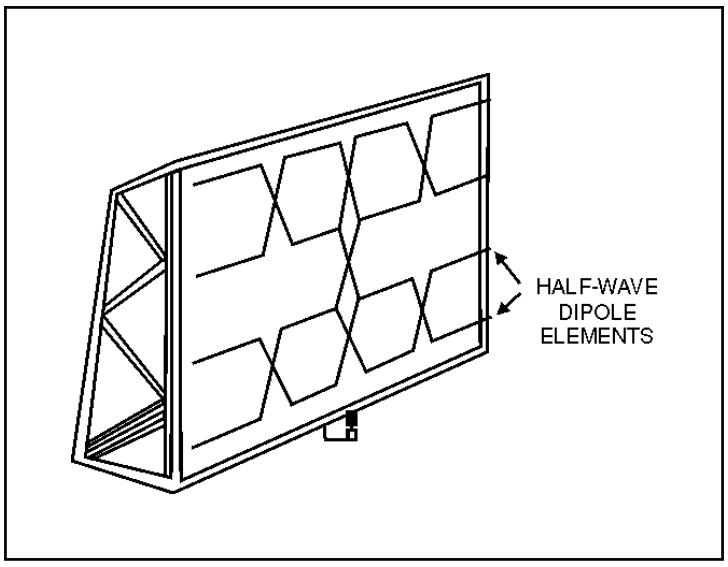


Figure 4-Sum 11. Broadside Array Elements

The end-fire array has elements parallel to each other and in the same plane. Maximum radiation occurs along the axis of the array.

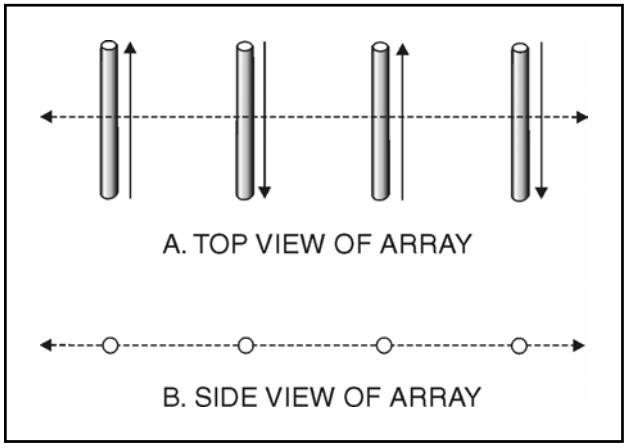


Figure 4-Sum 12. End-Fire Array

Matching stubs are used between elements to maintain current in the proper phase.

The gain of a collinear antenna is greatest when the elements are spaced from 0.4 to 0.5 wavelengths apart or when the number of elements is increased.

The optimum gain of a broadside array is obtained when the elements are spaced 0.65 wavelengths apart.

A parasitic array consists of one or more parasitic elements with a driven element. The amount of power gain and directivity depends on the lengths of the parasitic elements and the spacing between them.

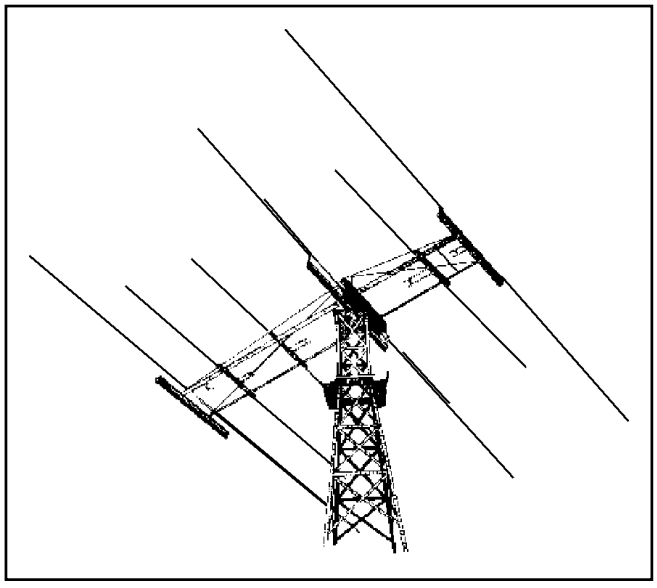


Figure 4-Sum 13. Parasitic Array

Multi-element arrays, such as the yagi, have a narrow frequency response as well as a narrow beam width.

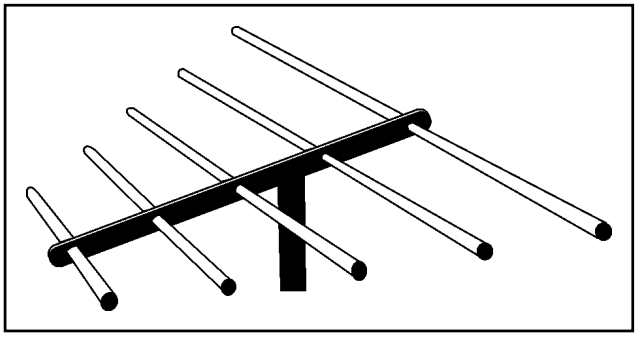


Figure 4-Sum 14. Multi-Element Arrays

A long-wire antenna is an antenna that is a wavelength or more long at the operating frequency. These antennas have directive patterns that are sharp in both the horizontal and vertical planes.

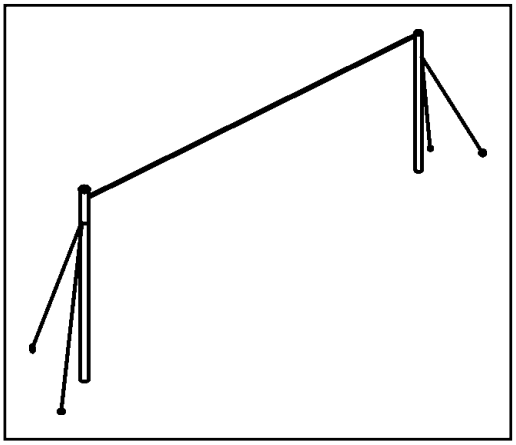


Figure 4-Sum 15. Long-Wire Antenna

Beverage antennas consist of a single wire that is two or more wavelengths long.

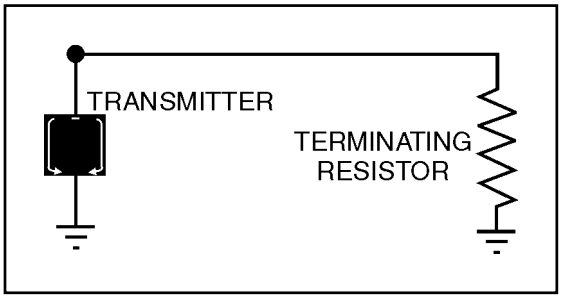


Figure 4-Sum 16. Beverage Antenna Wavelengths

A V antenna is a bidirectional antenna consisting of two horizontal, long wires arranged to form a V.

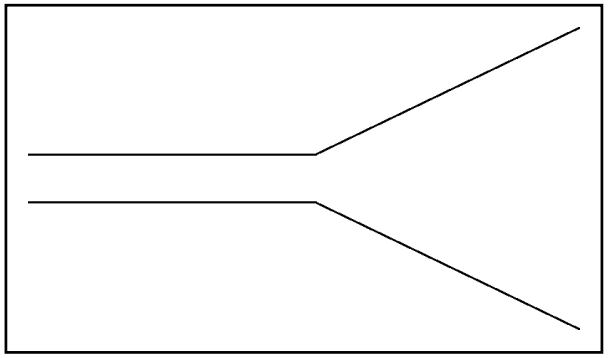


Figure 4-Sum 17. V Antenna Layout

The rhombic antenna uses four conductors joined to form a rhombus shape. This antenna has a wide frequency range, is easy to construct and maintain, and is noncritical as far as operation and adjustment are concerned.

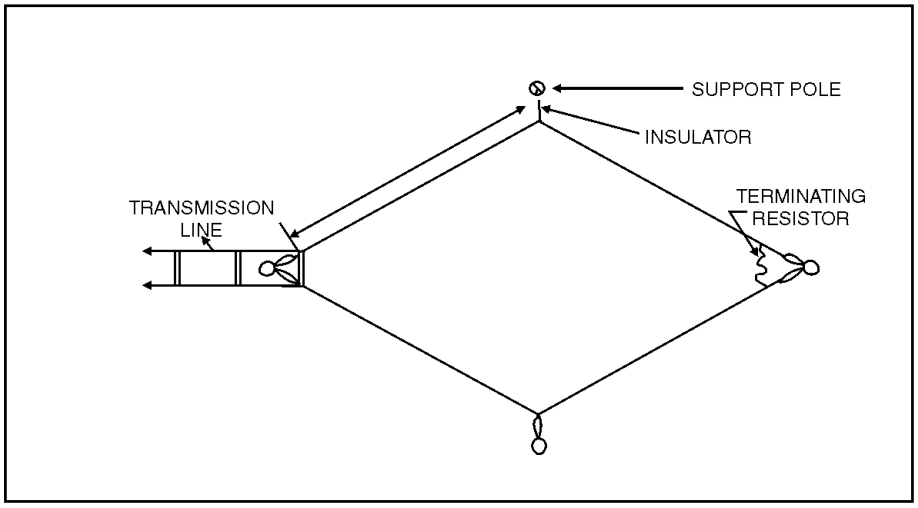


Figure 4-Sum 18. Rhombic Antenna Conductors

The turnstile antenna consists of two horizontal, half-wire antennas mounted at right angles to each other.

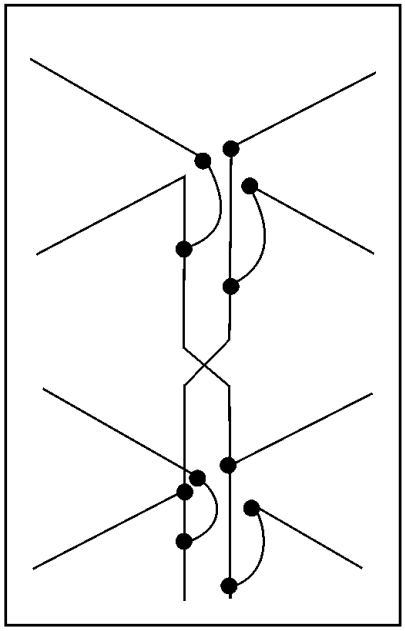


Figure 4-Sum 19. Turnstile Antenna

Check-On-Learning Questions

Antennas

When you are satisfied that you have answered every question to the best of your ability, check your answers using appendix A. If you missed eight or more questions, you should review the chapter, paying particular attention to the areas in which your answers were incorrect.

1. What are the two basic classifications of antennas?
2. What are the three parts of a complete antenna system?
3. What three factors determine the type, size, and shape of an antenna?
4. If a wave travels exactly the length of an antenna from one end to the other and back during the period of 1 cycle, what is the length of the antenna?
5. What are the terms used to identify the points of high current and high voltage on an antenna?
6. What is the term used to identify the points of minimum current and minimum voltage on an antenna?
7. The various properties of a transmitting antenna can apply equally to the same antenna when it is used as a receiving antenna. What term is used for this property?
8. The direction of what field is used to designate the polarization of a wave?
9. If a wave's electric lines of force rotate through 360 degrees with every cycle of RF energy, what is the polarization of this wave?
10. What type of polarization should be used at medium and low frequencies?
11. What is an advantage of using horizontal polarization at high frequencies?
12. What type of polarization should be used if an antenna is mounted on a moving vehicle at frequencies below 50 megahertz?
13. What is the radiation resistance of a half-wave antenna in free space?
14. A radiating source that radiates energy stronger in one direction than another is known as what type of radiator?
15. A radiating source that radiates energy equally in all directions is known as what type of radiator?
16. A flashlight is an example of what type of radiator?
17. What terms are often used to describe basic half-wave antennas?
18. If a basic half-wave antenna is mounted vertically, what type of radiation pattern will be produced?
19. In which plane will the half-wave antenna be operating if it is mounted horizontally?
20. Because the radiation pattern of a dipole is similar to that of a doublet, what will happen to the pattern if the length of the doublet is increased?
21. What is the simplest method of feeding power to the half-wave antenna?
22. What is the radiation pattern of a quarter-wave antenna?
23. Describe the physical arrangement of a ground screen.

24. What is the difference in the amount of impedance between a three-wire dipole and a simple center-fed dipole?
25. Which has a wider frequency range, a simple dipole or a folded dipole?
26. What is the purpose of antenna stubs?
27. What is the primary difference between the major and minor lobes of a radiation pattern?
28. What is the maximum number of elements ordinarily used in a collinear array?
29. Why is the number of elements used in a collinear array limited?
30. How can the frequency range of a collinear array be increased?
31. How is directivity of a collinear array affected when the number of elements is increased?
32. What is the primary cause of broadside arrays losing efficiency when not operating at their designed frequency?
33. When more than two elements are used in a broadside array, how are the elements arranged?
34. As the spacing between elements in a broadside array increases, what is the effect on the major lobes?
35. What are some disadvantages of the end-fire array?
36. Where does the major lobe in the end-fire array occur?
37. To maintain the required balance of phase relationships and critical feeding, how must the end-fire array be constructed?
38. What two factors determine the directivity pattern of the parasitic array?
39. What two main advantages of a parasitic array can be obtained by combining a reflector and a director with the driven element?
40. The parasitic array can be rotated to receive or transmit in different directions. What is the name given to such an antenna?
41. What are the disadvantages of the parasitic array?
42. What is the advantage of adding parasitic elements to a yagi array?
43. The yagi antenna is an example of what type of array?
44. To radiate power efficiently, a long-wire antenna must have what minimum overall length?
45. What is another name for the Beverage antenna?
46. What is the polarity of the currents that feed the V antenna?
47. What is the main disadvantage of the rhombic antenna?
48. What is the primary reason for the development of the turnstile antenna?

Appendix A

Check-On-Learning Answers

CHAPTER 1: WAVE PROPAGATION

1 Propagation means spreading out.

2. A wave is a disturbance that moves through a medium.

3 A means of transferring energy from one place to another.

4. Sound waves, light waves, radio waves, heat waves, water waves.

5. Transverse waves.

6. Radio waves, light waves, and heat waves.

7. A sound wave.

8. A source, medium, and detector (receiver).

9. A sequence of events, such as the positive and negative alternation of electrical current.

10. The space occupied by one cycle of a radio wave at any given instant.

11. The law of reflection states: The angle of incidence is equal to the angle of reflection.

12. When the incident wave is nearly parallel with the surface.

13. When the incident wave is perpendicular to the surface. Also a dull (or black) surface reflects very little regardless of the angle.

14. The density of the two mediums, and the velocity of the waves.

15. The Doppler effect.

16. Sonics.

17. No. The average human ear cannot hear all sounds in the infrasonic and ultrasonic regions.

18. An amplifier.

19. A source, medium, and detector (receiver).

20. Noise and tones.

21. Pitch, intensity, and quality.

22. 20 Hz to 20 kHz.

23. The amount of energy transmitted from a source.

24. Quality.

25. Velocity increases as density decreases and temperature increases.

26. Acoustics.

27. Echo.

28. Reverberation.

29. Resonance.

30. Noise.
31. Mechanical, electrical, and chemical.
32. A photon.
33. Angstrom unit.
34. Red, green and blue.
35. Magenta, yellow and cyan.
36. Reflected or absorbed.
37. None, all colors would be absorbed.
38. Translucent.
39. 186,000 miles per second or 300,000,000 meters per second.
40. Transmitted.
41. Diffused.
42. Light waves, heat waves, and radio waves.
43. The visible spectrum can be seen.
44. Electric field and magnetic field.
45. An antenna.
46. Electric field.
47. Magnetic field.
48. Radiation field.

CHAPTER 2: RADIO WAVE PROPAGATION

1. Induction field and radiation field.
2. Induction field.
3. Radiation field.
4. Fundamental frequency.
5. Harmonic frequency or harmonics.
6. 30 meters.
7. 5 megahertz.
8. Vertically polarized.
9. Direction of wave propagation.
10. Shifting in the phase relationships of the wave.
11. Troposphere, stratosphere, and ionosphere.
12. Stratosphere.
13. Whether the component of the wave is traveling along the surface or over the surface of the earth.
14. Sea water
15. Radio horizon is about one-third farther. .
16. (a) electrical properties of the terrain

    (b) frequency

    (c) polarization of the antenna
17. High energy ultraviolet light waves from the sun.
18 D, E, F1, and F2 layers.
19. D layer is 30 to 55 miles, E layer 55 to 90 miles, and F layers are 90 to 240 miles.
20. Thickness of ionized layer.
21. Critical frequency.
22. (a) density of ionization of the layer

    (b) frequency

    (c) angle at which it enters the layer
23. A zone of silence between the ground wave and sky wave where there is no reception.
24. Where ionization density is greatest.
25. A term used to describe the multiple pattern a radio wave may follow.
26. Selective fading.
27. Natural and man-made interference.
28. Natural.
29. Man-made.

30. (a) filtering and shielding of the transmitter

    (b) limiting bandwidth

    (c) cutting the antenna to the correct frequency

31. (a) physical separation of the antenna

    (b) limiting bandwidth of the antenna

    (c) use of directional antennas

32. Regular and irregular variations.

33. Regular variations can be predicted but irregular variations are unpredictable.

34. Daily, seasonal, 11-year, and 27-day variations.

35. Sporadic E, sudden disturbances, and ionospheric storms.

36. MUF is maximum usable frequency. LUF is lowest usable frequency. FOT is commonly known as optimum working frequency.

37. MUF is highest around noon. Ultraviolet light waves from the sun are most intense.

38. When LUF is too low it is absorbed and is too weak for reception.

39. Signal-to-noise ratio is low and the probability of multipath propagation is greater.

40. Frequent signal fading and dropouts.

41. FOT is the most practical operating frequency that can be relied on to avoid problems of multipath, absorption, and noise.

42. They can cause attenuation by scattering.

43. It can cause attenuation by absorption.

44. It is a condition where layers of warm air are formed above layers of cool air.

45. It can cause VHF and UHF transmission to be propagated far beyond normal line-of-sight distances.

46. Troposphere.

47. VHF and above.

48. Near the mid-point between the transmitting and receiving antennas, just above the radio horizon.

CHAPTER 3: PRINCIPLES OF TRANSMISSION LINES

1. Transmission line.
2. Input end, generator end, transmitter end, sending end, and source.
3. Output end, receiving end, load end and sink.
4. Parallel two-wire, twisted pair, shielded pair and coaxial line.
5. Power lines, rural telephone lines, and telegraph lines.
6. High radiation losses and noise pickup.
7. Twin lead.
8. The conductors are balanced to ground.
9. Air coaxial (rigid) and solid coaxial (flexible).
10. The ability to minimize radiation losses.
11. Expensive to construct, must be kept dry, and high frequency losses limit the practical length of the line.
12. Cylindrical and rectangular.
13. Copper, dielectric, and radiation.
14. Copper losses.
15. Dielectric losses.
16. λ = 20 meters.
17. (1) Type of line used, (2) dielectric in the line, and (3) length of line.
18. Inductance is expressed in microhenrys per unit length, capacitance is expressed in picofarads per unit length, and resistance is expressed in ohms per unit length.
19. The small amount of current that flows through the dielectric between two wires of a transmission line and is expressed in micromhos per unit length.
20. When the characteristic impedance of the transmission line and the load impedance are equal.
21. Z_0 and it is the ratio of E to I at every point along the line.
22. Between 50 and 600 ohms.
23. Incident waves from generator to load. Reflected waves from load back to generator.
24. 2 and 6 have zero resultant wave and they indicate that the incident and reflected waves are 180 degrees out of phase at all parts.
25. One-fourth the distance from each end of the line.
26. The load impedance of such a line is equal to Z_0.
27. Even quarter-wave points (1/2λ, l, 3/2λ, etc.).
28. At 1/2 wavelength from the end and at every 1/2 wavelength along the line.
29. Power standing-wave ratio (PSWR).
30. The existence of voltage variations on a line.

CHAPTER 4: ANTENNAS

1. Half-wave (Hertz) and quarter-wave (Marconi).
2. Coupling device, feeder, and antenna.
3. Frequency of operation of the transmitter, amount of power to be radiated, and general direction of the receiving set.
4. One-half the wavelength.
5. Current and voltage loops.
6. Current and voltage nodes.
7. Reciprocity of antennas.
8. Electric (E) field.
9. Circular polarization.
10. Vertical polarization.
11. Less interference is experienced by man-made noise sources.
12. Vertical polarization.
13. 73 ohms.
14. Anisotropic radiator.
15. Isotropic radiator.
16. Anisotropic radiator.
17. Dipole, doublet and Hertz.
18. Nondirectional.
19. Vertical plane.
20. The pattern would flatten.
21. To connect one end through a capacitor to the final output stage of the transmitter.
22 .A circular radiation pattern in the horizontal plane, or same as a half wave.
23. It is composed of a series of conductors arranged in a radial pattern and buried 1 to 2 feet below the ground.
24. Nine times the feed-point impedance.
25. Folded dipole.
26. To produce desired phase relationship between connected elements.
27. Major lobes have the greatest amount of radiation.
28. Four.
29. As more elements are added, an unbalanced condition in the system occurs which impairs efficiency.
30. By increasing the lengths of the elements of the array.
31. Directivity increases.

32. Lower radiation resistance.
33. Parallel and in the same plane.
34. They sharpen.
35. Extremely low radiation resistance, confined to one frequency, and affected by atmospheric conditions.
36. Along the major axis
37. Symmetrically.
38. Length of the parasitic element (tuning) and spacing between the parasitic and driven elements.
39. Increased gain and directivity.
40. Rotary array.
41. Their adjustment is critical and they do not operate over a wide frequency range.
42. Increased gain.
43. Multi-element parasitic array.
44. One-half wavelength.
45. Wave antenna.
46. Opposite.
47. It requires a large antenna site.
48. For omnidirectional VHF communications.

Glossary

absorption	(1) Absorbing light waves. Does not allow any reflection or refraction. (2) Atmospheric absorption of RF energy with no reflection or refraction (adversely affects long distance communications).
acoustics	The science of sound.
alternating current (AC)	An electrical current, which constantly changes amplitude and polarity at regular intervals.
amplitude	The portion of a cycle measured from a reference line to a maximum value above (or to a maximum value below) the line.
angle of incidence	The angle between the incident wave and the normal.
angle of reflection	The angle between the reflected wave and the normal.
angle of refraction	The angle between the normal and the path of a wave through the second medium.
angstrom unit	The unit used to define the wavelength of light waves.
anisotropic	The property of a radiator to emit strong radiation in one direction.
antenna	A conductor or set of conductors used either to radiate RF energy into space or to collect RF energy from space.
AR	Army regulation
array of arrays	Same as COMBINATION ARRAY.
bay	Part of an antenna array.
beverage antenna	A horizontal, longwire antenna designed for reception and transmission of low-frequency, vertically polarized ground waves.
bidirectional array	An array that radiates in opposite directions along the line of maximum radiation.
broadside array	An array in which the direction of maximum radiation is perpendicular to the plane containing the elements.

center-feed method	Connecting the center of an antenna to a transmission line, which is then connected to the final (output) stage of the transmitter.
characteristic impedance	The ratio of voltage to current at any given point on a transmission line. Represented by a value of impedance.
coaxial line	A type of transmission line that contains two concentric conductors.
collinear array	An array with all the elements in a straight line. Maximum radiation is perpendicular to the axis of the elements.
combination array	An array system that uses the characteristics of more than one array.
complementary (secondary) colors of light	The colors of light produced when two of the primaries are mixed in overlapping beams of light. The complementary colors of light are magenta, yellow, and cyan.
complex wave	A wave produced by combining two or more pure tones at the same time.
compression waves	Longitudinal waves that have been compressed (made more dense) as they move away from the source.
conductance	The opposite of resistance in transmission lines. The minute amount of resistance that is present in the insulator of a transmission line.
connected array	Another term for DRIVEN ARRAY.
copper losses	The I^2R loss in a conductor caused by the current flow through the resistance of the conductor.
corner-reflector antenna	A half-wave antenna with a reflector consisting of two flat metal surfaces meeting at an angle behind the radiator.
counterpoise	A network of wire that is connected to a quarter-wave antenna at one end and provides the equivalent of an additional one-quarter wavelength.
coupling device	A coupling coil that connects the transmitter to the feeder.
crest (top)	The peak of the positive alternation (maximum value above the line) of a wave.

critical angle	The maximum angle at which radio waves can be transmitted and still be refracted back to earth.
critical frequency	The maximum frequency at which a radio wave can be transmitted vertically and still be refracted back to earth.
current-feed method	Same as CENTER-FEED METHOD.
current standing-wave ratio (ISWR)	The ratio of maximum to minimum current along a transmission line.
cycle	One complete alternation of a sine wave that has a maximum value above and a maximum value below the reference line.
damping	Reduction of energy by absorption.
density	(1) The compactness of a substance. (2) Mass per unit volume.
detector	The device that responds to a wave or disturbance.
dielectric heating	The heating of an insulating material by placing it in a high frequency electric field.
dielectric losses	The losses resulting from the heating effect on the dielectric material between conductors.
diffraction	The bending of the paths of waves when the waves meet some form of obstruction.
diffusion	The scattering of reflected light waves (beams) from an object, such as white paper.
dipole	A common type of half-wave antenna made from a straight piece of wire cut in half. Each half operates at a quarter wavelength of the output.
direct current (DC)	An electric current that flows in one direction.
directional	Radiation that varies with direction.
director	The parasitic element of an array that reinforces energy coming from the driver toward itself.
directivity	The property of an array that causes more radiation to take place in certain directions than in others.
dispersion	The refraction of light waves that causes the different frequencies to bend at slightly different angles.

distributed constants	The constants of inductance, capacitance, and resistance in a transmission line. The constants are spread along the entire length of the line and cannot be distinguished separately.
Doppler effect	The apparent change in frequency or pitch when a sound source moves either toward or away from a listener.
doublet	Another name for the dipole antenna.
driven array	An array in which all of the elements are driven.
driven element	An element of an antenna (transmitting or receiving) that is connected directly to the transmission line.
echo	The reflection of the original sound wave as it bounces off a distant surface.
elasticity	The ability of a substance to return to its original state.
electromagnetic field	The combination of an electric (E) field and a magnetic (H) field.
electromagnetic interference	Man-made or natural interference that degrades the quality of reception of radio waves.
electromagnetic radiation	The radiation of radio waves into space.
electric (E) field	The field produced as a result of a voltage charge on a conductor or antenna.
electromagnetic interference (EMI)	Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment.
electromotive force (EMF)	Electromotive force or voltage is electrical pressure that can force the free electrons to move in the direction of negative to positive.
element	A part of an antenna that can be either an active radiator or a parasitic radiator.
end-feed method	Connecting one end of an antenna through a capacitor to the final output stage of a transmitter.
end-fire array	An array in which the direction of radiation is parallel to the axis of the array.
fading	Variations in signal strength by atmospheric conditions.

feeder	A transmission line that carries energy to the antenna.
flat line	A transmission line that has no standing waves. This line requires no special tuning device to transfer maximum power.
flexible coaxial line	A coaxial line made with a flexible inner conductor insulated from the outer conductor by a solid, continuous insulating material.
FM	field manual
folded dipole	An ordinary half-wave antenna (dipole) that has one or more additional conductors connected across the ends parallel to each other.
four-element array	An array with three parasitic elements and one driven element.
free-space loss	The loss of energy of a radio wave because of the spreading of the wavefront as it travels from the transmitter.
frequency	The number of cycles that occur in one second. Usually expressed in hertz.
frequency diversity	Transmitting (and receiving) of radio waves on two different frequencies simultaneously.
frequency modulation (FM)	Frequency modulation is a method of impressing data onto an alternating-current wave by varying the instantaneous frequency of the wave. This scheme can be used with analog or digital data.
front-to-back ratio	The ratio of the energy radiated in the principal direction to the energy radiated in the opposite direction.
fundamental frequency	The basic frequency or first harmonic frequency.
gain	The ratio between the amount of energy propagated from an antenna that is directional to the energy from the same antenna that would be propagated if the antenna were not directional.
generator end	See INPUT END.
ground plane	The portion of a ground plane antenna that acts as ground.

ground-plane antenna	A type of antenna that uses a ground plane as a simulated ground to produce low-angle radiation.
ground reflection loss	The loss of RF energy each time a radio wave is reflected from the earth's surface.
ground screen	A series of conductors buried below the surface of the earth and arranged in a radial pattern. Used to reduce losses in the ground.
ground waves	Radio waves that travel near the surface of the earth.
half-wave dipole antenna	An antenna, consisting of two rods (one-quarter wavelength each) in a straight line, that radiates electromagnetic energy.
harmonic	A frequency that is a whole number multiple of a smaller base frequency.
Hertz antenna	A half-wave antenna installed some distance above ground and positioned either vertically or horizontally.
high frequency (HF)	The range of the radio frequency spectrum extending from 3 MHz to 30 MHz.
horizontal axis	On a graph, the straight line axis plotted from left to right.
horizontal pattern	The part of a radiation pattern that is radiated in all directions along the horizontal plane.
horizontally polarized	Waves that are radiated with their E field component parallel to the earth's surface.
incident wave	(1) The wave that strikes the surface of a medium. (2) The wave that travels from the sending end to the receiving end of a transmission line.
induction field	The electromagnetic field produced about an antenna when current and voltage are present on the same antenna.
induction losses	The losses that occur when the electromagnetic field around a conductor cuts through a nearby metallic object and induces a current into that object.
infrasonic (subsonic)	Sounds below 15 hertz.
input end	The end of a two-wire transmission line that is connected to a source.

input impedance	The impedance presented to the transmitter by the transmission line and its load.
intensity (of sound)	The measurement of the amplitude of sound energy. Sometimes mistakenly called loudness.
interecept	The point where two lines drawn on a graph cross each other.
interference	Any disturbance that produces an undesirable response or degrades a wave.
ionosphere	The most important region of the atmosphere extending from 31 miles to 250 miles above the earth. Contains four cloud-like layers that affect radio waves.
ionospheric storms	Disturbances in the earth's magnetic field that make communications practical only at lower frequencies.
ionization	The process of upsetting electrical neutrality.
isotropic radiation	The radiation of energy equally in all directions.
leakage current	The small amount of current that flows between the conductors of a transmission line through the dielectric.
light rays	Straight lines that represent light waves emitting from a source.
load end	See OUTPUT END.
loading	See LUMPED-IMPEDANCE TUNING.
lobe	An area of a radiation pattern plotted on a polar-coordinate graph that represents maximum radiation.
long-wire antenna	An antenna that is a wavelength or more long at its operating frequency.
longitudinal waves	Waves in which the disturbance (back and forth motion) takes place in the direction of propagation. Sometimes called compression waves.
loop	The curves of a standing wave or antenna that represent amplitude of current or voltage.
low frequency (LF)	The range of the radio frequency spectrum extending from 30 kHz to 300 kHz.
lowest usable frequency (luf)	The minimum operating frequency that can be used for communications between two points.

lumped constants	The properties of inductance, capacitance, and resistance in a transmission line.
lumped-impedance tuning	The insertion of an inductor or capacitor in series with an antenna to lengthen or shorten the antenna electrically.
magnetic (H) field	The field produced when current flows through a conductor or antenna.
major lobe	The lobe in which the greatest amount of radiation occurs.
Marconi antenna	A quarter-wave antenna oriented perpendicular to the earth and operated with one end grounded.
maximum usable frequency (muf)	Maximum frequency that can be used for communications between two locations for a given time of day and a given angle of incidence.
medium	The substance through which a wave travels from one point to the next. Air, water, and wood are examples of a medium.
medium frequency (MF)	The range of the radio frequency spectrum extending from 300 kHz to 3 MHz.
minor lobe	The lobe in which the radiation intensity is less than a major lobe.
multielement array	An array consisting of one or more arrays and classified as to directivity.
multielement parasitic array	An array that contains two or more parasitic elements and a driven element.
multipath	The multiple paths a radio wave may follow between transmitter and receiver.
natural horizon	The line-of-sight horizon.
negative alternation	The portion of a sine wave below the reference line.
node	The fixed minimum points of voltage or current on a standing wave or antenna.
noise (of sound)	An unwanted disturbance caused by spurious waves that originate from man-made or natural sources.
nondirectional	See OMNIDIRECTIONAL.

nonluminous bodies	Objects that either reflect or diffuse light that falls upon them.
nonresonant line	A transmission line that has no standing waves of current or voltage.
normal	The imaginary line perpendicular to the point at which the incident wave strikes the reflecting surface. Also called the perpendicular.
null	On a polar-coordinate graph, the area that represents minimum or 0 radiation.
omnidirectional	Transmitting in all directions.
opaque	A type of substance that does not transmit any light rays.
open-ended line	A transmission line that has an infinitely large terminating impedance.
optimum working frequency (fot)	The most practical operating frequency that can be used with the least amount of problems; roughly 85 percent of the maximum usable frequency.
origin	The point on a graph where the vertical and horizontal axes cross each other.
output end	The end of a transmission line that is opposite the source.
output impedance	The impedance presented to the load by the transmission line and its source.
parallel resonant circuit	A circuit that acts as a high impedance at resonance.
parallel-wire	A type of transmission line consisting of two parallel wires.
parasitic array	An array that has one or more parasitic elements.
parasitic element	The passive element of an antenna array that is connected to neither the transmission line nor the driven element.
period	The amount of time required for completion of one full cycle.
pitch	A term used to describe the frequency of a sound heard by the human ear.

plane of polarization	The plane (vertical or horizontal) with respect to the earth in which the E field propagates.
point of zero displacement	See REFERENCE LINE.
polar-coordinate graph	A graph whose axes consist of a series of circles with a common center and a rotating radius extending from the center of the concentric circles.
positive alternation	The portion of a sine wave above the reference line.
power loss	The heat loss in a conductor as current flows through it.
power standing-wave ratio (PSWR)	The ratio of the square of the maximum and minimum voltages of a transmission line.
primary colors (of light)	The three primary colors of light (red, green, and blue), from which all other colors may be derived.
prism	A triangular-shaped glass that refracts and disperses light waves into component wavelengths.
propagation	Waves traveling through a medium.
quality (of sound)	The factor that distinguishes tones of pitch and loudness.
quarter-wave antenna	Same as the Marconi antenna.
radiation field	The electromagnetic field that detaches itself from an antenna and travels through space.
radiation losses	The losses that occur when magnetic lines of force about a conductor are projected into space as radiation and are not returned to the conductor as the cycle alternates.
radiation pattern	A plot of the radiated energy from an antenna.
radiation resistance	The resistance, which if inserted in place of an antenna, would consume the same amount of power as that radiated by the antenna.
radio frequencies (RF)	Electromagnetic frequencies that fall between 3 kilohertz and 300 gigahertz and are used for radio communications.

radio horizon	The boundary beyond the natural horizon in which radio waves cannot be propagated over the earth's surface.
radio wave	(1) A form of radiant energy that can neither be seen nor felt. (2) An electromagnetic wave generated by a transmitter.
rarefied wave	A longitudinal wave that has been expanded or rarefied (made less dense) as it moves away from the source.
receiver	The object that responds to a wave or disturbance. Same as detector.
receiving antenna	The device used to pick up an RF signal from space.
receiving end	See OUTPUT END.
reciprocity	The property of interchangeability of the same antenna for transmitting and receiving.
rectangular-coordinate graph	A graph in which straight-line axes (horizontal and vertical) are perpendicular.
reference line	The position a particle of matter would occupy if it were not disturbed by wave motion.
reflected wave	(1) The wave that reflects back from a medium. (2) Waves traveling from the load back to the generator on a transmission line. (3) The wave moving back to the sending end of a transmission line after reflection has occurred.
reflection waves	Waves that are neither transmitted nor absorbed, but are reflected from the surface of the medium they encounter.
reflector	The parasitic element of an array that causes maximum energy radiation in a direction toward the driven element.
refraction	The changing of direction as a wave leaves one medium and enters another medium of a different density.
reradiation	The reception and retransmission of radio waves caused by turbulence in the troposphere.
resonance	The condition produced when the frequency of vibrations are the same as the natural frequency (of a cavity). The vibrations reinforce each other.

resonant line	A transmission line that has standing waves of current and voltage.
rest position	See REFERENCE LINE.
reverberation	The multiple reflections of sound waves.
rhombic antenna	frequency transmission and reception.
rigid coaxial line	A coaxial line consisting of a central, insulated wire (inner conductor) mounted inside a tubular outer conductor.
scatter angle	The angle at which the receiving antenna must be aimed to capture the scattered energy of tropospheric scatter.
self-induction	The phenomenon caused by the expanding and collapsing fields of an electron which encircles other electrons and retards the movement of the encircled electrons.
self-luminous bodies	Objects that produce their own light.
sending end	See INPUT END.
series resonant circuit	A circuit that acts as a low impedance at resonance.
shielded pair	A line consisting of parallel conductors separated from each other and surrounded by a solid dielectric.
short-circuited line	A transmission line that has a terminating impedance equal to 0.
sink	See OUTPUT END.
skin effect	Skin effect is a tendency for alternating current to flow mostly near the outer surface of a solid electrical conductor, such as metal wire, at frequencies above the audio range. .
skip distance	The distance from a transmitter to the point where the sky wave is first returned to earth.
skip zone	A zone of silence between the point where the ground wave becomes too weak for reception and the point where the sky wave is first returned to earth.
sky waves	Radio waves reflected back to earth from the ionosphere.

sonic	Pertaining to sounds capable of being heard by the human ear.
source	(1) The object that produces waves or disturbance. (2) The name given to the end of a two-wire transmission line that is connected to a source.
space diversity	Reception of radio waves by two or more antennas spaced some distance apart.
space wave	A radio wave that travels directly from the transmitter to the receiver and remains in the troposphere.
spectrum	(1) The entire range of electromagnetic waves. (2) VISIBLE. The range of electromagnetic waves that stimulate the sense of sight. (3) ELECTROMAGNETIC. The entire range of electromagnetic waves arranged in order of their frequencies.
sporadic E layer	Irregular cloud-like patches of unusually high ionization. Often forms at heights near the normal E layer.
spreader	Insulator used with transmission lines and antennas to keep the parallel wires separated.
standing wave	The distribution of voltage and current formed by the incident and reflected waves which have minimum and maximum points on a resultant wave that appears to stand still.
standing-wave ratio (SWR)	The ratio of the maximum (voltage, current) to the minimum (voltage, current) of a transmission line. Measures the perfection of the termination of the line.
stratosphere	Located between the troposphere and the ionosphere. Has little effect on radio waves.
stub	Short section of a transmission line used to match the impedance of a transmission line to an antenna. Can also be used to produce desired phase relationships between connected elements of an antenna.
sudden ionospheric disturbance (sid)	An irregular ionospheric disturbance that can totally blank out HF radio communications.
supersonic	Speed greater than the speed of sound.
surface wave	A radio wave that travels along the contours of the earth, thereby being highly attenuated.

TC	training circular
temperature inversion	The condition in which warm air is formed above a layer of cool air that is near the earth's surface.
three-element array	An array with two parasitic elements (reflector and director) and a driven element.
TM	technical manual
tones	Musical sounds.
translucent	A type of substance, such as frosted glass, through which some light rays can pass but through which objects cannot be seen clearly.
transmission line	A device designed to guide electrical energy from one point to another.
transmitting antenna	The device used to send the transmitted signal energy into space.
transparent	A type of substance, such as glass, that transmits almost all of the light waves that fall upon it.
transmission mediums	The various types of lines and waveguides used as transmission lines.
transmitter end	See INPUT END.
transverse wave motion	The up and down motion of a wave as the wave moves outward.
troposphere	The portion of the atmosphere closest to the earth's surface, where all weather phenomena take place.
tropospheric scatter	The propagation of radio waves in the troposphere by means of scatter.
trough (bottom)	The peak of the negative alternation (maximum value below the line).
tuned line	Another name for the resonant line. This line uses tuning devices to eliminate the reactance and to transfer maximum power from the source to the line.
turnstile antenna	A type of antenna used in VHF communications that is omnidirectional and consists of two horizontal half-wave antennas mounted at right angles to each other in the same horizontal plane.

twisted pair	A line consisting of two insulated wires twisted together to form a flexible line without the use of spacers.
two-wire open line	A parallel line consisting of two wires that are generally spaced from 2 to 6 inches apart by insulating spacers.
two-wire ribbon (twin lead)	A parallel line similar to a two-wire open line except that uniform spacing is assured by embedding the two-wires in a low-loss dielectric.
ultrahigh frequency (UHF)	The range of the radio frequency spectrum extending from 30 MHz to 3 GHz.
ultrasonic	Sounds above 20,000 hertz.
unidirectional array	An array that radiates in only one general direction.
untuned line	Another name for the flat or nonresonant line.
V antenna	A bidirectional antenna, shaped like a V, which is widely used for communications.
velocity	The rate at which a disturbance travels through a medium.
vertical axis	On a graph, the straight-line axis oriented from bottom to top.
vertical pattern	The part of a radiation pattern that is radiated in the vertical plane.
vertically polarized	Waves radiated with the E field component perpendicular to the earth's surface.
very high frequency (VHF)	The range of the radio frequency spectrum extending from 30 MHz to 300 MHz.
voltage-feed method	Same as END FEED METHOD.
voltage standing-wave ratio (VSWR)	The ratio of maximum to minimum voltage of a transmission line.
wave antenna	Same as BEVERAGE ANTENNA.
wave motion	A recurring disturbance advancing through space with or without the use of a physical medium.
wave train	A continuous series of waves with the same amplitude and wavelength.

wavefront	A small section of an expanding sphere of electromagnetic radiation, perpendicular to the direction of travel of the energy.
waveguide	A hollow metal tube used as a transmission line to guide energy from one point to another.
wavelength	(1) The distance in space occupied by 1 cycle of a radio wave at any given instant. (2) The distance a disturbance travels during one period of vibration.
yagi antenna	A multi-element parasitic array. Elements lie in the same plane as those of the end-fire array.

References

Related Publications

Related publications are sources of additional information. They are not required in order to understand this publication.

DEPARTMENT OF DEFENSE (DOD) PUBLICATIONS

ECAC-CR-83-200. *Field Antenna Handbook.* Electromagnetic Compatibility Analysis Center, Consulting Report. June 1984.

DEPARTMENT OF THE ARMY PUBLICATIONS

Field Manuals (FMs)

FM 4-25.11 (FM 21-11). *First Aid*. 23 December 2002.
FM 7-1 (FM 25-101). *Battle Focused Training*. 30 September 2003.
FM 11-62. *Communications-Electronics Fundamentals: Solid State Devices and Solid State Power Supplies*. 30 September 1983.
FM 11-487-1. *Installation Practices; HF Radio Communications Systems*. 18 April 1991.
FM 24-18. *Tactical Single-Channel Radio Communications Techniques*. 20 September 1987.
FM 24-35 (TC 24-1). *Signal Operation Instructions "The SOI"*. 26 October 1990.

Forms

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

Pamphlets

DA Pam 25-30. *Consolidated Index of Army Publications and Blank Forms*. 1 January 2004.

Index

A

acoustics, 1-21, 1-44, A-1
amplitude, 1-8
antenna gain, 4-11
antenna radiation, principles of, 4-6
arrays, types of, 4-34 to 4-47
  broadside, 4-29, 4-36, 4-64
  collinear, 4-29, 4-34, 4-64
  driven, 4-29, 4-64
  end-fire, 4-29, 4-39
  multi-element parasitic, 4-29, 4-45, 4-66
  parasitic, 4-29, 4-42, 4-64

B

broadside arrays, 4-29, 4-36, 4-64

C

capacitance, 3-12
characteristic impedance, 3-14, 3-15, 3-52
coaxial lines, 3-4, 3-49
collinear arrays, 4-29, 4-34, 4-64
copper losses, 3-7, 3-50
corner reflectors, 4-55
counterpoise, 4-22, 4-27, 4-62
critical frequency, 2-22, 2-43
current standing-wave ratio (ISWR), 3-47

D

dielectric losses, 3-8, 3-50
diffraction, 1-11, 1-14, 1-43, 2-13, 2-16, 2-42
distributed constants, 3-11, 3-13
Doppler effect, 1-11, 1-14, 1-15, 1-43, A-1
driven arrays, 4-29, 4-64

E

echo, 1-22
electromagnetic fields, 2-2, 3-13
electromagnetic interference (EMI), 2-29, 2-30, 2-45
electromagnetic spectrum, 1-31
electromagnetic theory of light, 1-24
end-fire arrays, 4-29, 4-39, 4-65

F

fading, 2-27, 2-45
  long-term, 2-39
  minimizing, 2-28
  multipath, 2-27, 2-45
  selective, 2-28
FOT, 2-34, 2-46
frequency, 1-10
frequency of vibration, 1-9

G

gain, antenna, 4-11
ground plane antennas, 4-54
ground reflection loss, 2-28, 2-45
ground screen, 4-27, 4-62
ground wave, 2-16, 2-41, 2-42

H

half-wave antennas, 2-4, 4-5, 4-14, 4-22, 4-25, 4-57, 4-62

I

incident wave, 1-11, 1-12, 1-42, 3-21, 3-32
inductance, 1-8, 3-11, 3-13
induction field, 1-38, 2-2, 2-6, 2-39
induction losses, 3-50
infinite line, 3-17, 3-21, 3-22
interference, 1-23, 1-44, 2-29
ionization, 2-19, 2-42
ionosphere, 2-14, 2-16, 2-41
  absorption in, 2-26
  structure of, 2-19
ionospheric disturbances, sudden, 2-32
ionospheric storms, 2-32

L

leakage current, 3-12, 3-51

light
absorption of, 1-30
colors of, 1-25
compared to sound, 1-25, 1-30
diffusion of, 1-30
general description of, 1-23 to 1-31, 1-40
measuring wavelength of, 1-44
properties of, 1-27
reflection of, 1-29
refraction of, 1-29
speed of, 1-28, 1-45, 2-8
theories of, 1-23 to 1-25, 1-44
lines of force, 1-34, 1-38, 3-8, 3-13
longitudinal waves, 1-5
long-wire antennas, 4-48, 4-66
lowest usable frequency (LUF), 2-33, 2-45
lumped constants, 3-10, 3-50

M

Marconi antennas, 4-25, 4-26, 4-25 to 4-28, 4-57, 4-62
maximum usable frequency (MUF), 2-33, 2-45
multi-element parasitic arrays, 4-29, 4-45, 4-66

N

noise, 1-18, 1-23, 1-43, 1-44

O

optimum working frequency. *See* FOT

P

parallel lines, 3-48
parasitic arrays, 4-29, 4-42, 4-64, 4-65
period, 1-9, 2-7
polarization, 2-10, 4-11
horizontal, 2-10, 2-40, 4-12, 4-14
vertical, 2-10, 2-40, 4-12
power standing-wave ratio (PSWR), 3-47

Q

quarter-wave antennas, 4-25, 4-26, 4-25 to 4-28, 4-57, 4-62

R

radiation field, 1-38, 2-2, 2-4, 2-6, 2-39, 4-11
radiation losses, 3-50
radiation resistance, 4-14
radio horizon, 2-42
radio wave
definition of, 2-6, 2-40
frequency, 2-7
frequency of (hertz), 1-8
harmonics, 2-7
period, 2-7
shape of, 2-7
speed of (velocity), 2-8
wavelength, 2-8
ratio, standing-wave, 3-46, 3-55
recombination, 2-19, 2-42
reflected waves, 3-30, 3-33
reflection, 1-11
reflection waves, 1-11
refraction, 1-11, 1-12 to 1-14, 1-22, 1-29, 1-42, 2-12, 2-21, 2-42
resistance, 3-12
resonance, 1-23, 1-44, 3-40, 4-9, 4-21
reverberation, 1-22
rhombic antennas, 4-49, 4-67
right-hand rule, 2-11

S

safety, ix, 4-2 to 4-4
shielded pairs, 3-4, 3-49
skip distance/skip zone, 2-24
sky wave, 2-18, 2-41, 2-42, 4-12
sound, 1-1, 1-3, 1-5, 1-6, 1-14, 1-15 to 1-23
characteristics of, 1-18
noise, 1-23
pitch of, 1-18
quality of, 1-20
requirements for, 1-16
science of (acoustics), 1-21
terms used to describe, 1-17
velocity of, 1-20
space wave, 2-16, 2-18, 2-42
special antennas, 4-47 to 4-56
sporadic E, 2-32
standing waves, 3-32, 3-35, 3-36, 3-37, 3-43, 3-55
standing-wave ratio, 3-46, 3-55
stratosphere, 2-14, 2-15, 2-41
sudden ionospheric disturbances (SID), 2-32
surface wave, 2-16, 2-42

T

temperature inversion, 2-36, 2-46

transmission lines
- characteristic impedance, 3-14, 3-15
- definition of, 3-1, 3-47
- description, 3-2
- distributed constants, 3-11, 3-13
- length of, 3-8
- losses, 3-8
- lumped constants, 3-10
- terminating, 3-38
- theory of, 3-10
- types of, 3-2

transverse waves, 1-4

troposphere, 2-14, 2-15, 2-37, 2-41

tropospheric propagation, 2-37, 2-46

tropospheric scatter, 2-37, 2-39

turnstile antennas, 4-52, 4-68

twisted pairs, 3-3, 3-48

V

V antennas, 4-48, 4-67

voltage standing-wave ratio (VSWR), 3-47

W

wave
- definition of, 1-2

waveguides, 3-6, 3-50

wavelength
- definition of, 1-4, 1-7
- formula for, 1-10
- symbol for, 1-9

wavelength-to-frequency conversions, 2-8

waves, types of
- electromagnetic, 1-33, 1-34
- ground, 2-16, 2-41
- light, 1-23 to 1-31
- longitudinal, 1-5
- reflection, 1-11
- sky, 2-18, 2-41
- sound, 1-15 to 1-23
- space, 2-18
- surface, 2-16
- transverse, 1-4

weather, 2-35

TC 9-64
15 JULY 2004

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
0416802

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number (IDN) 110963, requirements for TC 9-64.

PIN: 081636-000

MCRP 8-10B.11
(Formerly MCRP 3-40.3C)

Antenna Handbook

US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000062 00

CD&I (C 116)

2 May 2016

ERRATUM

to

MCRP 3-40.3C

ANTENNA HANDBOOK

1. Change all instances of MCRP 3-40.3C, *Antenna Handbook*, to MCRP 8-10B.11, *Antenna Handbook.*

2. File this transmittal sheet in the front of this publication.

PCN 144 000062 81

MCCDC (C 42)
10 Jul 2001

E R R A T U M

to

MCRP 3-40C

ANTENNA HANDBOOK

1. For administrative purposes, the publication short title has been reidentified. Change "MCRP 6-22D" to read: "MCRP 3-40.3C" of June 1999 wherever it appears in the Manual.

PCN 144 000062 80

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380-1775

1 June 1999

FOREWORD

Communications and information systems (CIS) support collecting, processing, and exchanging information. CIS automate routine functions, freeing commanders and staffs to focus on the aspects of command and control that require experience, judgment, and intuition. Personnel who install, operate, and maintain CIS play a key role in the command and control of the Marine air-ground task force (MAGTF). It is an understatement to say that the success of the MAGTF in the modern battlespace depends on the effective employment of CIS.

One of the most important networks of the MAGTF CIS architecture is single-channel radio (SCR). SCR is the principal means of communications support for maneuver units. SCR communications equipment is easy to operate, and networks are easily established, rapidly reconfigured, and, most importantly, easily maintained on the move. SCR provides secure voice communication and supports limited data information exchange. MAGTF SCR equipment is fielded in many configurations and includes hand-held, manpack, vehicle-mounted, bench-mounted, and sheltered radios. These radios operate in simplex and half-duplex modes. The most widely employed tactical radios provide integrated communications security (COMSEC) and jam resistance through frequency hopping.

Tactical SCRs operate in the three military radio frequency bands (high frequency [HF], very high frequency [VHF], and ultrahigh frequency [UHF]). In the HF band, SCR can support long-range communications, albeit at the expense of mobility. SCR in the VHF and UHF bands is normally limited to line of sight. SCR satellite communications (SATCOM) provide mobility, flexibility, and ease of operation with unlimited range. Limitations of SCR include susceptibility to enemy electronic warfare; cosite, footprint, terrain, and atmospheric interference; the requirement for close coordination and detailed planning; a need for common timing, frequency, and equipment; and limited spectrum availability. The latter is particularly critical for SATCOM.

Of all the variables affecting single-channel radio communications, the one factor that an operator has the most control over is the antenna. With the right antenna, an operator can change a marginal net into a reliable net. Marine Corps Reference Publication (MCRP) 6-22D, *Antenna Handbook*, gives operators the knowledge to properly select and employ antennas to provide the strongest possible signal at the receiving station of the circuit.

MCRP 6-22D builds on the doctrinal foundation established in Marine Corps Warfighting Publication (MCWP) 6-22, *Communications and Information Systems*. This handbook is intended not only for CIS officers and radio operators, but for all personnel desiring information about antenna fundamentals.

MCRP 6-22D supersedes Fleet Marine Force Reference Publication (FMFRP) 3-34, *Field Antenna Handbook*, dated 5 March 1991.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

J. E. RHODES
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: 144 000062 00

Antenna Handbook

Table of Contents

Page

Chapter 1. Radio Principles

Electromagnetic Radiation 1-1
Radio Waves 1-2
- Frequency 1-2
- Frequency Calculation 1-3
- Frequency Bands 1-3

Radio Communication Circuit 1-5
Propagation Fundamentals 1-8
- Earth's Atmosphere 1-8
- Radio Wave Propagation 1-8
- Other Factors Affecting Propagation 1-18
- Path Loss 1-19
- Reflected Waves 1-19
- Diffraction 1-21
- Tropospheric Refraction, Ducting and Scattering 1-22

Noise 1-23
- Natural Noise 1-24
- Manmade Noise 1-24

Chapter 2. Antenna Fundamentals

Section I. Concepts and Terms 2-2

Forming a Radio Wave 2-2
Radiation 2-2
- Radiation Fields 2-3
- Radiation Patterns 2-4

Polarization 2-6
- Polarization Requirements for Various Frequencies 2-8
- Advantages of Vertical Polarization 2-9
- Advantages of Horizontal Polarization 2-10

Directionality 2-10
Resonance 2-11
Reception 2-12
Reciprocity 2-13
Impedance 2-14
Bandwidth 2-15
Gain 2-16
Take-Off Angle 2-18

Section II. Ground Effects 2-19

Grounded Antenna Theory 2-19
Types of Grounds 2-20
- Counterpoise 2-22
- Ground Screen 2-23

Section III. Calculating Antenna Length 2-24

Section IV. Antenna Orientation 2-26

Azimuth 2-26
Improvement of Marginal Communications 2-27
Transmission and Reception of Strong Signals 2-29

Chapter 3. Transmission Lines

Properties 3-1
Transmission Line Types 3-1
Minimizing Energy Loss 3-3
Impedance 3-3
Optimizing Line Length 3-5
Attenuation 3-6
Making the Best Use of Available Transmission Lines 3-7
Twin-Lead Limitations 3-8
Directly Connecting the Transceiver and Antenna 3-9
Baluns 3-10
Cable Connectors 3-11
Balanced Antenna 3-11

Chapter 4. HF Antenna Selection

Antenna Selection Procedure 4-2
Determining Antenna Gain 4-6
Antenna Types 4-8
AS-2259/GR 4-9
Vertical Whip 4-10
Half-Wave Dipole 4-14
Inverted Vee 4-19

Long Wire 4-21
Inverted L 4-24
Sloping Vee 4-28
Sloping Wire 4-33
Vertical Half-Rhombic 4-37
HF NVIS Communications 4-40

Chapter 5. VHF and UHF Antenna Selection

Frequencies 5-1
Polarization 5-2
Gain and Directivity 5-2
Gain 5-3
Directivity 5-3
Transmission Lines 5-4
Radiators 5-5
Vertical Radiator 5-5
Cross Section Radiator 5-5
Insulation 5-5
Interference 5-6
Noise 5-6
Multipath Interference 5-6
Vegetated Areas 5-8
Antenna Types 5-9
Vertical Whip 5-9
OE-254 5-10
Antenna Within Vehicle Interior 5-12
HF Antenna Types Usable at VHF and UHF 5-12
Dual-Function Antennas 5-12

Chapter 6. Field Repair and Expedients

Repair Techniques 6-1
Whip Antennas 6-1
Wire Antennas 6-2
Guys 6-4
Masts 6-4
Tips on Construction and Adjustment 6-4
Constructing the Antenna 6-4
Adjusting the Antenna 6-6
Field Expedient Antennas 6-7
VHF Considerations 6-7
HF Considerations 6-7
End-Fed Half-Wave Antenna 6-8
Center-Fed Doublet Antenna 6-9
Field Expedient Directional Antennas 6-14
Vertical Half-Rhombic and Long-Wire Antennas 6-14
Yagi Antenna 6-14
Vee Antenna 6-16
Sloping Vee Antenna 6-16

Chapter 7. Satellite Communications Antennas

Siting SATCOM Antennas 7-4
Considerations 7-4
Determining Horizon Angles 7-4

Chapter 8. Antenna Farms

Command Post 8-1
Tactical 8-1
Main 8-2
Rear 8-2
Location Selection Considerations 8-2
Doctrinal Considerations 8-2
Tactical Considerations 8-3
Technical Considerations 8-5
Siting VHF Antennas 8-6
Transmitting Antenna Site 8-9
Receiving Antenna Sites 8-11
Antenna Farm Internal Arrangement 8-12
Frequency Band 8-12
Antenna Selection and Placement 8-12
Requirements 8-14
Polarization 8-15
Power and Signal Lines 8-16
Antenna Farm Layout Principles 8-16

Appendices

A Glossary A-1
B References and Related Publications B-1

Chapter 1

Radio Principles

ELECTROMAGNETIC RADIATION

Electromagnetic radiation includes radio waves, microwaves, infrared radiation, visible light, ultraviolet waves, X-rays, and gamma rays. Together they make up the electromagnetic spectrum. They all move at the speed of light (186,000 miles/300 million meters per second). The only difference between them is their wavelength (the distance a wave travels during one complete cycle [vibration]), which is directly related to the amount of energy the waves carry. The shorter the wavelength, the higher the energy. Figure 1-1 lists the electromagnetic spectrum components according to wavelength and frequency (the number of complete cycles [vibrations] per second). A portion of the spectrum which is used for HF, VHF, and UHF radio communication has been expanded to show more detail.

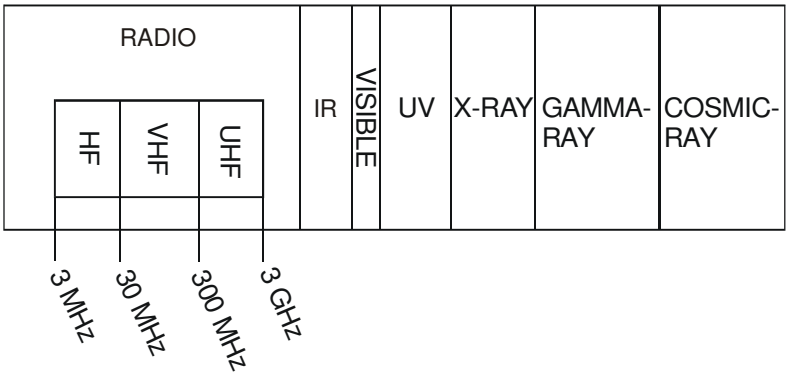


Figure 1-1. Electromagnetic Spectrum.

RADIO WAVES

Radio waves propagate (travel) much like surface water waves. They travel near the Earth's surface and also radiate skyward at various angles to the Earth's surface. As the radio waves travel, their energy spreads over an ever-increasing surface area. A typical radio wave has two components, a crest (top portion) and a trough (bottom portion). These components travel outward from the transmitter, one after the other, at a consistent velocity (speed). The distance between successive wave crests is called a wavelength and is commonly represented by the Greek lowercase lambda (λ) (see fig. 1-2).

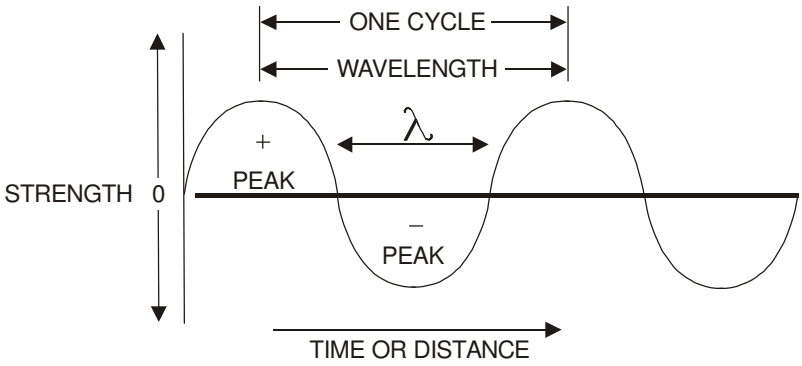


Figure 1-2. Radio Wave.

Frequency

Radio waves transmit radio and television (TV) signals. They have wavelengths that range from less than a centimeter to tens or even hundreds of meters. Frequency modulated (FM) radio waves are shorter than amplitude modulated (AM) radio waves. A radio wave's frequency equals the number of complete cycles that occur in 1 second. The longer the cycle time, the longer the wavelength

and the lower the frequency. The shorter the cycle time, the shorter the wavelength and the higher the frequency.

Frequency is measured and stated in hertz (Hz). A radio wave frequency is very high. It is generally measured and stated in thousands of hertz (kilohertz [kHz]), in millions of hertz (megahertz [MHz]), or sometimes in billions of hertz (gigahertz [GHz]).

1 Hz	=	1 cycle per second
1 kHz	=	1 thousand cycles per second
1 MHz	=	1 million cycles per seconds
1 GHz	=	1 billion cycles per second

Frequency Calculation

For practical purposes, the velocity of a radio wave is considered to be constant, regardless of the frequency or the amplitude of the transmitted wave. To find the frequency when the wavelength is known, divide the velocity by the wavelength.

$$\text{Frequency (hertz)} = \frac{\text{300,000,000 (meters per second)}}{\text{Wavelength (meters)}}$$

To find the wavelength when the frequency is known, divide the velocity by the frequency.

$$\text{Wavelength (meters)} = \frac{\text{300,000,000 (meters per second)}}{\text{Frequency (hertz)}}$$

Frequency Bands

Frequency spectrum designations are—

HF	VHF	UHF
3 to 30 MHz	30 to 300 MHz	300 to 3,000 MHz/3GHz

HF is used primarily for long-range communications. An HF signal is reflected by the outermost portion of the atmosphere, the ionosphere. VHF is used for short-range communications. To use VHF, it is necessary to be able to visualize a direct line of sight (LOS) between the transmitter and receiver. This limits UHF to distances that are not much greater than the distance to the horizon, assuming that there are no massive obstructions in the LOS. When the LOS path exists and VHF transmission is possible, VHF is always preferred to HF because a VHF signal can be made to follow a much narrower and more direct path to the receiver. UHF is a third type of transmission. UHF transmission is like VHF in that both follow the direct or LOS path. But with the proper antenna, UHF transmission can be made to follow an even narrower path to the receiver than VHF.

Each frequency band has unique characteristics. The ranges and power requirements shown in table 1-1 are for normal operating conditions (i.e., proper siting and antenna orientation and correct operating procedures). Ranges will change according to the condition of the propagation medium and the transmitter output power.

Table 1-1. Frequency Range Characteristics.

Band	Ground Wave Range	Sky Wave Range	Power Required
HF	0–50 miles	100–8000 miles	.5–5 kW
VHF	0–30 miles	50–150 miles	.5 or less kW
UHF	0–50 miles	N/A	.5 or less kW

Tactical SCRs operate in the three military radio frequency bands shown in table 1-2.

Table 1-2. Ground SCRs.

Frequency Band	MAGTF SCR Equipment Used	Operating Frequency Range	Typical Application
HF	AN/PRC-104 AN/GRC-193 AN/MRC-138	2–29.999 MHz	Radio LOS and beyond/long range
VHF	AN/PRC-68 AN/PRC-119 AN/VRC-88 (A, D) AN/VRC-89 (A, D) AN/VRC-90 (A, D) AN/VRC-91 (A, D) AN/VRC-92 (A, D) AN/GRC-213 AN/MRC-145	30–88 MHz	Radio LOS and relay/retransmission
	AN/PRC-113 AN/VRC-83	116–150 MHz	Critical LOS (ground to air)
UHF	AN/PRC-113 AN/VRC-83 AN/GRC-171	225–400 MHz	Critical LOS (ground to air)
	AN/PSC-3 AN/PSC-5		SATCOM footprint

RADIO COMMUNICATION CIRCUIT

The radio equipment for communicating between two stations, including the path the radio signal follows through the air, is a radio link. A radio link consists of seven components: transmitter, power supply, transmission lines, transmitting antenna, propagation path, receiving antenna, and receiver.

The transmitter generates a radio signal. The power supply provides power for the operating voltage of the radio (battery or generator). The transmission line delivers the signal from the transmitter to the transmitting antenna. The transmitting antenna sends the radio signal into space toward the receiving antenna. The path in space that the radio signal follows as it goes to the receiving antenna is the propagation path. The receiving antenna intercepts or receives the signal and sends it through a transmission line to the receiver. The receiver processes the radio signal so it can be heard (fig 1-3).

The radio operator's objective is to provide the strongest possible signal to the receiving station. The best possible signal is one that provides the greatest signal-to-noise (S/N) ratio at the receiving antenna.

To implement a radio communications circuit it is necessary to—

- Generate and radiate an electromagnetic wave modulated with information (e.g., voice, Morse code).
- Make the wave propagate efficiently from the transmitting antenna to the receiving antenna.
- Intercept the wave by using a receiving antenna.
- Demodulate the energy so that the information originally transmitted becomes available in a useful form.

Choosing the right antenna and matching its characteristics to the best propagation path are the two most important factors in setting up a communications circuit. The weakest link in the communications circuit is the wrong propagation path. The best transmitter, antenna, and receiver are of little use if the frequency is wrong or the propagation path is improper.

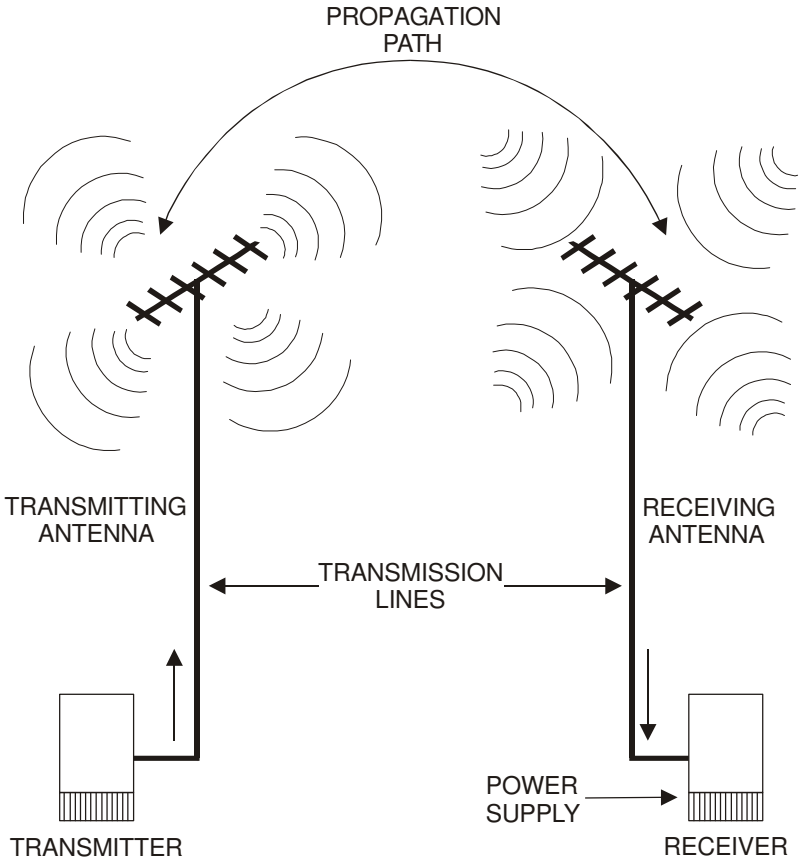


Figure 1-3. Typical Radio Link.

PROPAGATION FUNDAMENTALS

Earth's Atmosphere

Propagation usually takes place within the Earth's atmosphere. The atmosphere surrounding the Earth is divided into several layers, each possessing unique characteristics. The first layer, starting at the Earth's surface and extending to a height of about 10 kilometers (km), is the troposphere. In this layer, the air temperature decreases with altitude at the rate of about 2.5°C every 300 meters.

The second layer of the atmosphere is the stratosphere, which occupies an altitude range extending from about 10 km to 50 km. This layer of air remains at a nearly constant temperature of about -65°C.

Beginning at about 50 km and extending upward to more than 500 km is the ionosphere. The ionosphere gets its name because the molecules of its atmosphere are ionized, i.e., electrons have been stripped away from atoms by the constant bombardment of the Sun's rays and other high energy particles released by the Sun. Because of the large quantities of free electrons, the ionosphere is capable of interacting strongly on radio waves traveling through it.

Radio Wave Propagation

There are two principal ways radio waves travel from the transmitter to the receiver. One is by ground wave, directly from the transmitter to the receiver. The other is by sky wave, up to the ionosphere and refracted (bent downward) back to the Earth. Short-distance, all UHF, and upper VHF transmissions are by ground waves. Long-distance transmissions are principally by sky waves. SCR sets can use either ground wave or sky wave propagation for communications.

Ground Wave Propagation. Radio communications using ground wave propagation do not use or depend on waves refracted from the ionosphere (sky waves). Ground wave propagation is affected by the Earth's electrical characteristics and by the amount of diffraction (bending) of the waves along the Earth's curvature. The ground wave's strength at the receiver depends on the transmitter's power output and frequency, the Earth's shape and conductivity along the transmission path, and the local weather conditions. The ground wave includes three components: the direct wave, the ground reflected wave, and the surface wave (fig. 1-4).

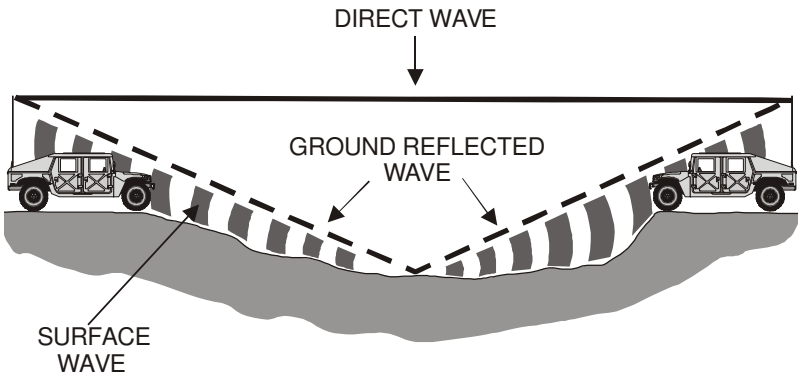


Figure 1-4. Ground Wave.

Direct Wave. **The direct wave travels directly from the transmitting antenna to the receiving antenna. The direct wave is limited to the LOS distance between the transmitting antenna and the receiving antenna plus the short distance added by atmospheric refraction and diffraction of the wave around the Earth's curvature. This distance can be extended by increasing the transmitting or the receiving antenna height, or both.**

Ground Reflected Wave. **The ground reflected wave reaches the receiving antenna after being reflected from the Earth's surface. Cancellation of the radio signal can occur when the ground reflected component and the direct wave component arrive at the receiving antenna at the same time and are 180° out of phase with each other.**

Surface Wave. **The surface wave follows the Earth's curvature. It is affected by the Earth's conductivity and dielectric constant.**

Frequency Characteristics Of Ground Waves. **Various frequencies determine which wave component will prevail along any given signal path. For example, when the Earth's conductivity is high and the frequency of a radiated signal is low, the surface wave is the predominant component. For frequencies below 10 MHz, the surface wave is sometimes the predominant component. However, above 10 MHz, the losses that are sustained by the surface wave component are so great that the other components (direct wave and sky wave) become predominant.**

At frequencies of 30 to 300 kHz, ground losses are very small, so the surface wave component follows the Earth's curvature. It can be used for long-distance communications provided the radio operator has enough power from the transmitter. The frequencies 300 kHz to 3 MHz are used for long-distance communications over sea water and for medium-distance communications over land.

At high frequencies, 3 to 30 MHz, the ground's conductivity is extremely important, especially above 10 MHz where the dielectric constant or conductivity of the Earth's surface determines how much signal absorption occurs. In general, the signal is strongest at the lower frequencies when the surface over which it travels has a high dielectric constant and conductivity.

Earth's Surface Conductivity. **The dielectric constant or Earth's surface conductivity determines how much of the surface wave signal energy will be absorbed or lost. Although the Earth's surface conductivity as a whole is generally poor, the conductivity of varying surface conditions, when compared one with an other, would be as stated in table 1-3.**

Table 1-3. Surface Conductivity.

Surface Type	Relative Conductivity
Large body fresh water	Very good
Ocean or sea water	Good
Flat or hilly loamy soil	Fair
Rocky terrain	Poor
Desert	Poor
Jungle	Very poor

Sky Wave Propagation. Radio communications that use sky wave propagation depend on the ionosphere to provide the signal path between the transmitting and receiving antennas.

Ionospheric Structure. **The ionosphere has four distinct layers. In the order of increasing heights and decreasing molecular densities, these layers are D, E, F1, and F2. During the day, when the rays of the Sun are directed toward that portion of the atmosphere, all four layers may be present. At night, the F1 and F2 layers seem to merge into a single F layer, and the D and E layers fade out. The actual number of layers, their height above the Earth, and their relative intensity of ionization vary constantly.**

The D layer exists only during the day and has little effect in bending the paths of HF radio waves. The main effect of the D layer is to attenuate HF waves when the transmission path is in sunlit regions.

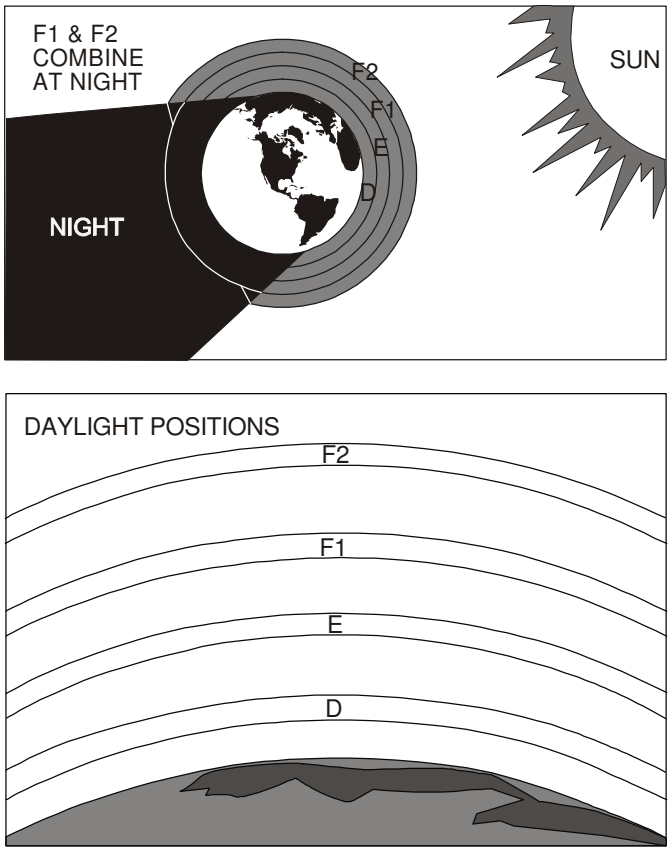
The E layer is used during the day for HF radio transmission over intermediate distances (less than 2,400 km/1,500 miles [mi]). At night the intensity of the E layer decreases, and it becomes useless for radio transmission.

The F layer exists at heights up to 380 km/240 mi above the Earth and is ionized all the time. It has two well-defined layers (F1 and F2) during the day, and one layer (F) at night. At night the F layer remains at a height of about 260 km/170 mi and is useful for long-range radio communications (over 2,400 km/1,500 mi). The F2 layer is the most useful for long-range radio communications, even though its degree of ionization varies appreciably from day to day (fig. 1-5).

The Earth's rotation around the Sun and changes in the Sun's activity contribute to ionospheric variations. There are two main classes of these variations: regular (predictable) and irregular, occuring from abnormal behavior of the Sun.

Regular Ionospheric Variations. **The four regular variations are—**

- **Daily: caused by the rotation of the Earth.**
- **Seasonal: caused by the north and south progression of the Sun.**
- **27-day: caused by the rotation of the Sun on its axis.**
- **1-year: caused by the sunspot activity cycle going from maximum through minimum back to maximum levels of intensity.**



F2 250-500 km (250-420 km at night)
F1 200-250 km
E 90-130 km
D 75-90 km

Figure 1-5. Ionospheric Structure.

Irregular Ionospheric Variations. **In planning a communications system, the current status of the four regular variations must be anticipated. There are also unpredictable irregular variations that must be considered. They have a degrading effect (at times blanking out communications) which cannot be controlled or compensated for at the present time. Some irregular variations are—**

- **Sporadic E. When excessively ionized, the E layer often blanks out the reflections from the higher layers. It can also cause unexpected propagation of signals hundreds of miles beyond the normal range. This effect can occur at any time.**
- **Sudden ionospheric disturbance (SID). A sudden ionospheric disturbance coincides with a bright solar eruption and causes abnormal ionization of the D layer. This effect causes total absorption of all frequencies above approximately 1 MHz. It can occur without warning during daylight hours and can last from a few minutes to several hours. When it occurs, receivers seem to go dead.**
- **Ionospheric storms. During these storms, sky wave reception above approximately 1.5 MHz shows low intensity and is subject to a type of rapid blasting and fading called flutter fading. These storms may last from several hours to days and usually extend over the entire Earth.**

Sunspots. **Sunspots generate bursts of radiation that cause high levels of ionization. The more sunspots, the greater the ionization. During periods of low sunspot activity, frequencies above 20 MHz tend to be unusable because the E and F layers are too weakly ionized to reflect signals back to Earth. At the peak of the sunspot cycle, however, it is not unusual to have worldwide propagation on frequencies above 30 MHz.**

Frequency Characteristics in the Ionosphere. **The range of long-distance radio transmission is determined primarily by the ionization density of each layer. The higher the frequency, the greater the ionization density required to reflect radio waves back to Earth. The upper (E and F) layers reflect the higher frequencies because they are the most highly ionized. The D layer, which is the least ionized, does not reflect frequencies above approximately 500 kHz. Thus, at any given time and for each ionized layer, there is an upper frequency limit at which radio waves sent vertically upward are reflected back to Earth. This limit is called the critical frequency.**

Radio waves directed vertically at frequencies higher than the critical frequency pass through the ionized layer out into space. All radio waves directed vertically into the ionosphere at frequencies lower than the critical frequency are reflected back to Earth. Radio waves used in communications are generally directed towards the ionosphere at some oblique angle, called the angle of incidence. Radio waves at frequencies above the critical frequency will be reflected back to Earth if transmitted at angles of incidence smaller than a certain angle, called the critical angle. At the critical angle, and at all angles larger than the critical angle, the radio waves pass through the ionosphere if the frequency is higher than the critical frequency. As the angle of transmission decreases, an angle is reached at which the radio waves are reflected back to Earth.

Transmission Paths. **Sky wave propagation refers to those types of radio transmissions that depend on the ionosphere to provide signal paths between transmitters and receivers.**

The distance from the transmitting antenna to the place where the sky waves first return to Earth is the skip distance. The skip distance depends on the angle of incidence, the operating frequency, and the

ionosphere's height and density. The antenna's height, in relation to the operating frequency, affects the angle that transmitted radio waves strike and penetrate the ionosphere and then return to Earth. This angle of incidence can be controlled to obtain the desired coverage area. Lowering the antenna height increases the angle of transmission and provides broad and even signal patterns in a large area.

Using near-vertical transmission paths is known as near-vertical incidence sky wave (NVIS). Raising the antenna height lowers the angle of incidence. Lowering the angle of incidence produces a skip zone in which no usable signal is received. This area is bounded by the outer edge of usable ground wave propagation and the point nearest the antenna at which the sky wave returns to Earth. In short-range communications situations, the skip zone is an undesirable condition. However, low angles of incidence make long-distance communications possible.

When a transmitted wave is reflected back to the Earth's surface, the Earth absorbs part of the energy. The remaining energy is reflected back into the ionosphere to be reflected back again. This means of transmission—alternately reflecting the radio wave between the ionosphere and the Earth—is called hops. Hops enable radio waves to be received at great distances from the point of origin.

Fading. Fading is the periodic increase and decrease of received signal strength. Fading occurs when a radio signal is received over a long-distance path in the high frequency range. The precise origin of this fading is seldom understood. There is little common knowledge of what precautions to take to reduce or eliminate fading's troublesome effects. Fading associated with sky wave paths is the greatest detriment to reliable communications. Too often, those responsible for communication circuits rely on raising the transmitter power or increasing antenna gain to overcome fading. Unfortunately, such actions often do not work and seldom improve

reliability. Only when the signal level fades down below the background noise level for an appreciable fraction of time will increased transmitter power or antenna gain yield an overall circuit improvement. Choosing the correct frequency and using transmitting and receiving equipment intelligently ensure a strong and reliable receiving signal, even when low power is used.

Maximum Usable and Lowest Usable Frequencies. Using a given ionized layer and a transmitting antenna with a fixed angle of radiation, there is a maximum frequency at which a radio wave will return to Earth at a given distance. This frequency is called the maximum usable frequency (MUF). It is the monthly median of the daily highest frequency that is predicted for sky wave transmission over a particular path at a particular hour of the day. The MUF is always higher than the critical frequency because the angle of incidence is less than 90°. If the distance between the transmitter and the receiver is increased, the MUF will also increase. Radio waves lose some of their energy through absorption by the D layer and a portion of the E layer at certain transmission frequencies.

The total absorption is less and communications more satisfactory as higher frequencies are used—up to the level of the MUF. The absorption rate is greatest for frequencies ranging from approximately 500 kHz to 2 MHz during the day. At night the absorption rate decreases for all frequencies. As the frequency of transmission over any sky wave path decreases from high to low frequencies, a frequency will be reached at which the received signal overrides the level of atmospheric and other radio noise interference. This is called the lowest useful frequency (LUF) because frequencies lower than the LUF are too weak for useful communications. The LUF depends on the transmitter power output as well as the transmission distance. When the LUF is greater than the MUF, no sky wave transmission is possible.

Propagation Prediction. **Although a detailed discussion of propagation prediction methods is beyond the scope of this publication, it should be noted that propagation predictions can be obtained from a system planning, engineering, and evaluation device (SPEED).**

Other Factors Affecting Propagation

In the VHF and UHF ranges, extending from 30 to 300 MHz and beyond, the presence of objects (e.g., buildings or towers) may produce strong reflections that arrive at the receiving antenna in such a way that they cancel the signal from the desired propagation path and render communications impossible. Most Marines are familiar with distant TV station reception interference caused by high-flying aircraft. The signal bouncing off of the aircraft alternately cancels and reinforces the direct signal from the TV station as the aircraft changes position relative to the transmitting and receiving antennas.

This same interference can adversely affect the ordinary voice communications circuit at VHF and UHF, rendering the received signal unintelligible for brief periods of time. Receiver locations that avoid the proximity of an airfield should be chosen if possible. Avoid locating transmitters and receivers where an airfield is at or near midpoint of the propagation path of frequencies above 20 MHz.

Many other things may affect the propagation of a radio wave. Hills, mountains, buildings, water towers, tall fences, aircraft, and even other antennas can have a marked affect on the condition and reliability of a given propagation path. Conductivity of the local ground or body of water can greatly alter the strength of the transmitted or received signal. Energy radiation from the Sun's surface also greatly affects conditions within the ionosphere and alters the characteristics of long-distance propagation at 2 to 30 MHz.

Path Loss

Radio waves become weaker as they spread from the transmitter. The ratio of received power to transmitted power is called path loss. LOS paths at VHF and UHF require relatively little power since the total path loss at the radio horizon is only about 25 decibels (dB) greater than the path loss over the same distance in free space (absence of ground). This additional loss results from some energy being reflected from the ground, canceling part of the direct wave energy. This is unavoidable in almost every practical case. The total path loss for an LOS path above average terrain varies with the following factors: total path loss between transmitting and receiving antenna terminals, frequency, distance, transmitting antenna gain, and receiving antenna gain.

Reflected Waves

Often, it is possible to communicate beyond the normal LOS distance by exploiting the reflection from a tall building, nearby mountain, or water tower (fig. 1-6 on page 1-20). If the top portion of a structure or hill can be seen readily by both transmitting and receiving antennas, it may be possible to achieve practical communications by directing both antennas toward the point of maximum reflection. If the reflecting object is very large in terms of a wavelength, the path loss, including the reflection, can be very low.

If a structure or hill exists adjacent to an LOS path, reflected energy may either add to or subtract from the energy arriving from the direct path. If the reflected energy arrives at the receiving antenna with the same amplitude (strength) as the direct signal but has the opposite phase, both signals will cancel and communication will be impossible. However, if the same condition exists but both signals arrive in phase, they will add and double the signal strength. These

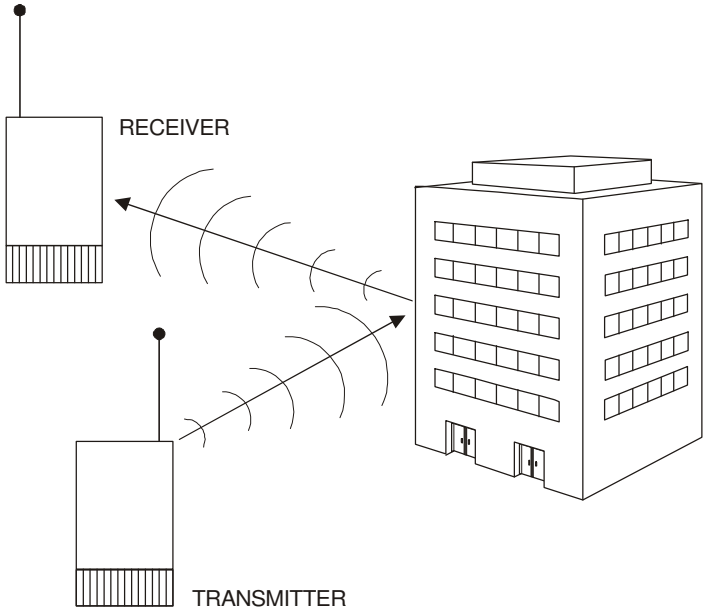


Figure 1-6. Reflected Waves.

two conditions represent destructive and constructive combinations of the reflected and direct waves.

Reflection from the ground at the common midpoint between the receiving and transmitting antennas may also arrive in a constructive or destructive manner. Generally, in the VHF and UHF range, the reflected wave is out of phase (destructive) with respect to the direct wave at vertical angles less than a few degrees above the horizon. However, since the ground is not a perfect conductor, the amplitude of the reflected wave seldom approaches that of the direct wave. Thus, even though the two arrive out of phase, complete cancellation does not occur. Some improvement may result from using vertical polarization rather than horizontal polarization

over LOS paths because there tends to be less phase difference between direct and reflected waves. The difference is usually less than 10 dB, however, in favor of vertical polarization.

Diffraction

Unlike the ship passing beyond the visual horizon, a radio wave does not fade out completely when it reaches the radio horizon. A small amount of radio energy travels beyond the radio horizon by a process called diffraction. Diffraction also occurs when a light source is held near an opaque object, casting a shadow on a surface behind it. Near the edge of the shadow a narrow band can be seen which is neither completely light nor dark. The transition from total light to total darkness does not occur abruptly, but changes smoothly as the light is diffracted.

A radio wave passing over either the curved surface of the Earth or a mountain ridge behaves in much the same fashion as a light wave. For example, people living in a valley below a high, sharp, mountain ridge can often receive a TV station located many miles below on the other side. Figure 1-7 illustrates how radio waves from the

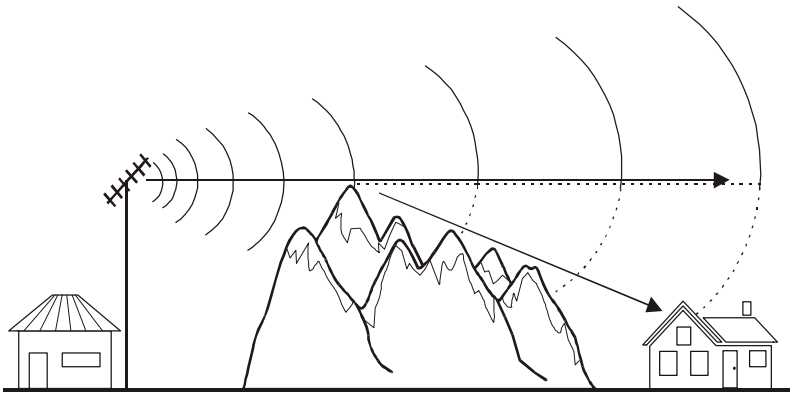


Figure 1-7. Diffracted Wave.

TV station are diffracted by the mountain ridge and bent downward in the direction of the village. It is emphasized, however, that the energy decays very rapidly as the angle of propagation departs from the straight LOS path. Typically, a diffracted signal may undergo a reduction of 30 to 40 dB by being bent only 5 feet by a mountain ridge. The actual amount of diffracted signal depends on the shape of the surface, the frequency, the diffraction angle, and many other factors. It is sufficient to say that there are times when the use of diffraction becomes practical as a means for communicating in the VHF and UHF over long distances.

Tropospheric Refraction, Ducting, and Scattering

Refraction is the bending of a wave as it passes through air layers of different density (refractive index). In semitropical regions, a layer of air 5 to 100 meters thick with distinctive characteristics may form close to the ground, usually the result of a temperature inversion. For example, on an unusually warm day after a rainy spell, the Sun may heat up the ground and create a layer of warm, moist air. After sunset, the air a few meters above the ground will cool very rapidly while the moisture in the air close to the ground serves as a blanket for the remaining heat. After a few hours, a sizable difference in temperature may exist between the air near the ground and the air at a height of 10 to 20 meters, resulting in a marked difference in air pressure. Thus, the air near the ground is considerably denser than the air higher up. This condition may exist over an area of several hundred square kilometers or over a long area of land near a seacoast. When such an air mass forms, it usually remains stable until dawn, when the ground begins to cool and the temperature inversion ends.

When a VHF or UHF radio wave is launched within such air mass, it may bend or become *trapped* (forced to follow the inversion layer). This layer then acts as a *duct* between the transmitting

antenna and a distant receiving site. The effects of such ducting can be seen frequently during the year in certain locations where TV or VHF FM stations are received over paths of several hundred kilometers. The total path loss within such a *duct* is usually very low and may exceed the free space loss by only a few dBs.

It is also possible to communicate over long distances by means of tropospheric scatter. At altitudes of a few kilometers, the air mass has varying temperature, pressure, and moisture content. Small fluctuations in tropospheric characteristics at high altitude create *blobs*. Within a blob, the temperature, pressure, and humidity are different from the surrounding air. If the difference is large enough, it may modify the refractive index at VHF and UHF. A random distribution of these blobs exists at various altitudes at all times. If a high-power transmitter (greater than 1 kW) and high gain antenna (10 dB or more) are used, sufficient energy may be scattered from these blobs down to the receiver to make reliable communication possible over several hundred kilometers. Communication circuits employing this mode of propagation must use very sensitive receivers and some form of diversity to reduce the effects of the rapid and deep fading. Scatter propagation is usually limited to path distances of less than about 500 km.

NOISE

Noise consists of all undesired radio signals, manmade or natural. Noise masks and degrades useful information reception. The radio signal's strength is of little importance if the signal power is greater than the received noise power. This is why S/N ratio is the most important quantity in a receiving system. Increasing receiver amplification cannot improve the S/N ratio since both signal and noise will be amplified equally and S/N ratio will remain unchanged. Normally, receivers have more than enough amplification.

Natural Noise

Natural noise has two principle sources: thunderstorms (atmospheric noise) and stars (galactic noise). Both sources generate sharp pulses of electromagnetic energy over all frequencies. The pulses propagate according to the same laws as manmade signals, and receiving systems must accept them along with the desired signal. Atmospheric noise is dominant from 0 to 5 MHz, and galactic noise is most important at all higher frequencies. Low frequency transmitters must generate very strong signals to overcome noise. Strong signals and strong noise mean that the receiving antenna does not have to be large to collect a usable signal (a few hundred microvolts). A 1.5 meter tuned whip will deliver adequately all of the signals that can be received at frequencies below 1 MHz.

Manmade Noise

Manmade noise is a product of urban civilization that appears wherever electric power is used. It is generated almost anywhere that there is an electric arc (e.g., automobile ignition systems, power lines, motors, arc welders, fluorescent lights). Each source is small, but there are so many that together they can completely hide a weak signal that would be above the natural noise in rural areas. Manmade noise is troublesome when the receiving antenna is near the source, but being near the source gives the noise waves characteristics that can be exploited. Waves near a source tend to be vertically polarized. A horizontally polarized receiving antenna will generally receive less noise than a vertically polarized antenna.

Manmade noise currents are induced by any conductors near the source, including the antenna, transmission line, and equipment cases. If the antenna and transmission line are balanced with respect to the ground, then the noise voltages will be balanced and cancel

with respect to the receiver input terminals (zero voltage across terminals), and this noise will not be received. Near-perfect balance is difficult to achieve, but any balance helps.

Other ways to avoid manmade noise are to locate the most troublesome sources and turn them off, or move the receiving system away from them. Moving a kilometer away from a busy street or highway will significantly reduce noise. Although broadband receiving antennas are convenient because they do not have to be tuned to each working frequency, sometimes a narrowband antenna can make the difference between communicating and not communicating. The HF band is now so crowded with users that interference and noise, not signal strength, are the main reasons for poor communications. A narrowband antenna will reject strong interfering signals near the desired frequency and help maintain good communications.

(reverse blank)

Chapter 2

Antenna Fundamentals

All radios, whether transmitting or receiving, require some sort of antenna. The antenna accepts power from the transmitter and launches it into space as an electromagnetic or radio wave. At the receiving end of the circuit, a similar antenna collects energy from the passing electromagnetic wave and converts it into an alternating electric current or signal that the receiver can detect.

How well antennas launch and collect electromagnetic waves directly influences communications reliability and quality. The function of an antenna depends on whether it is transmitting or receiving.

A transmitting antenna transforms the output radio frequency (RF) energy produced by a radio transmitter (RF output power) into an electromagnetic field that is radiated through space. The transmitting antenna converts energy from one form to another form. The receiving antenna reverses this process. It transforms the electromagnetic field into RF energy that is delivered to a radio receiver.

Section I. Concepts and Terms

To select the right antennas for a radio circuit, certain concepts and terms must be understood. This section defines several basic terms and relationships which will help the reader understand antenna fundamentals. These include: forming a radio wave, radiation fields and patterns, polarization, directionality, resonance, reception, reciprocity, impedance, bandwidth, gain, and take-off angle.

FORMING A RADIO WAVE

When an alternating electric current flows through a conductor (wire), electric and magnetic fields are created around the conductor. If the length of the conductor is very short compared to a wavelength, the electric and magnetic fields will generally die out within a distance of one or two wavelengths. However, as the conductor is lengthened, the intensity of the fields enlarge. Thus, an ever-increasing amount of energy escapes into space. When the length of the wire approaches one-half of a wavelength at the frequency of the applied alternating current, most of the energy will escape in the form of electromagnetic radiation. For effective communications to occur, the following must exist: alternating electric energy in the form of a transmitter, a conductor or a wire, an electric current flowing through the wire, and the generation of both electric and magnetic fields in the space surrounding the wire.

RADIATION

Once a wire is connected to a transmitter and properly grounded, it begins to oscillate electrically, causing the wave to convert nearly all of the transmitter power into an electromagnetic radio wave. The electromagnetic energy is created by the alternating flow of electrons impressed on the bottom end of the wire. The electrons travel

upward on the wire to the top, where they have no place to go and are bounced back toward the lower end. As the electrons reach the lower end in phase, i.e., in step with the radio energy then being applied by the transmitter, the energy of their motion is strongly reinforced as they bounce back upward along the wire. This regenerative process sustains the oscillation. The wire is resonant at the frequency at which the source of energy is alternating.

The radio power supplied to a simple wire antenna appears nearly equally distributed throughout its length. The energy stored at any location along the wire is equal to the product of the voltage and the current at that point. If the voltage is high at a given point, the current must be low. If the current is high, the voltage must be low. The electric current is maximum near the bottom end of the wire.

Radiation Fields

When RF power is delivered to an antenna, two fields evolve. One is an induction field, which is associated with the stored energy; the other is a radiation field. At the antenna, the intensities of these fields are large and are proportional to the amount of RF power delivered to the antenna. At a short distance from the antenna and beyond, only the radiation field remains. This field is composed of an electric component and a magnetic component (see fig. 2-1 on page 2-4).

The electric and magnetic fields (components) radiated from an antenna form the electromagnetic field. The electromagnetic field transmits and receives electromagnetic energy through free space. A radio wave is a moving electromagnetic field that has velocity in the direction of travel and components of electric intensity and magnetic intensity arranged at right angles to each other.

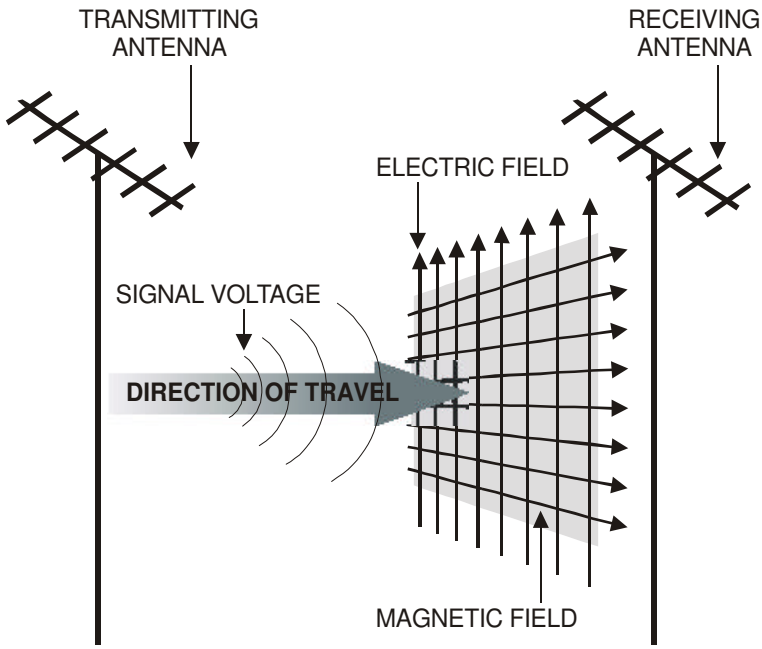


Figure 2-1. Radiation Fields.

Radiation Patterns

The radio signals radiated by an antenna form an electromagnetic field with a definite pattern, depending on the type of antenna used. This radiation pattern shows the antenna's directional characteristics. A vertical antenna radiates energy equally in all directions (omnidirectional), a horizontal antenna is mainly bidirectional, and a unidirectional antenna radiates energy in one direction. However, the patterns are usually distorted by nearby obstructions or terrain features. The full- or solid-radiation pattern is represented as a three-dimensional figure that looks somewhat like a doughnut with a transmitting antenna in the center (fig 2-2).

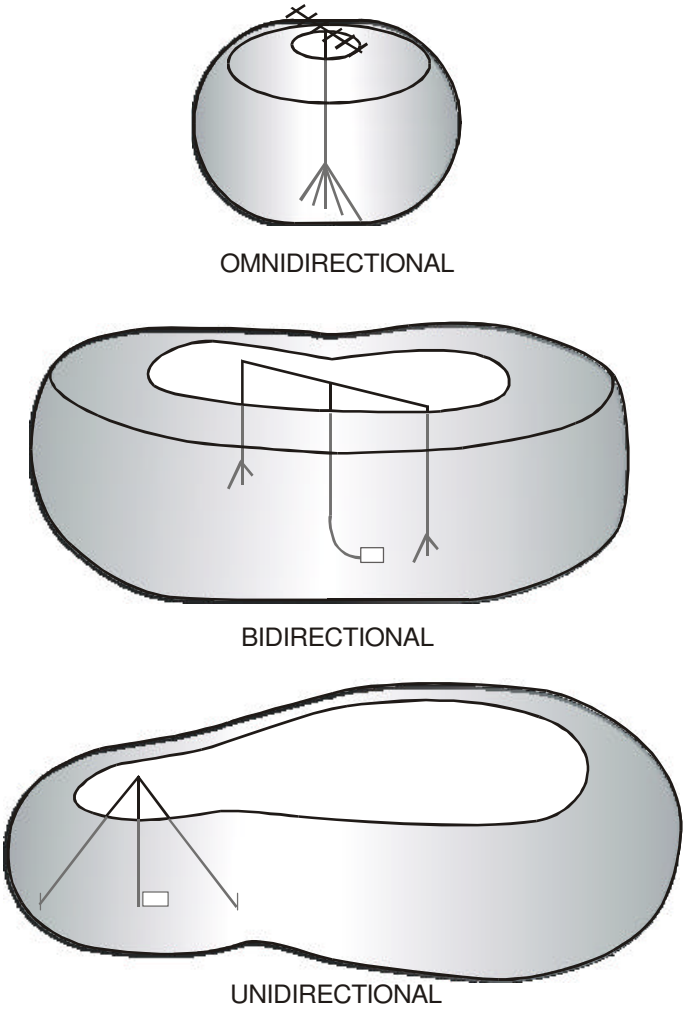


Figure 2-2. Radiation Patterns.

POLARIZATION

A radiated wave's polarization is determined by the direction of the lines of force making up the electric field. If the lines of electric force are at right angles to the Earth's surface, the wave is vertically polarized (fig. 2-3). If the lines of electric force are parallel to the Earth's surface, the wave is horizontally polarized (fig. 2-4). When a single-wire antenna extracts (receives) energy from a passing

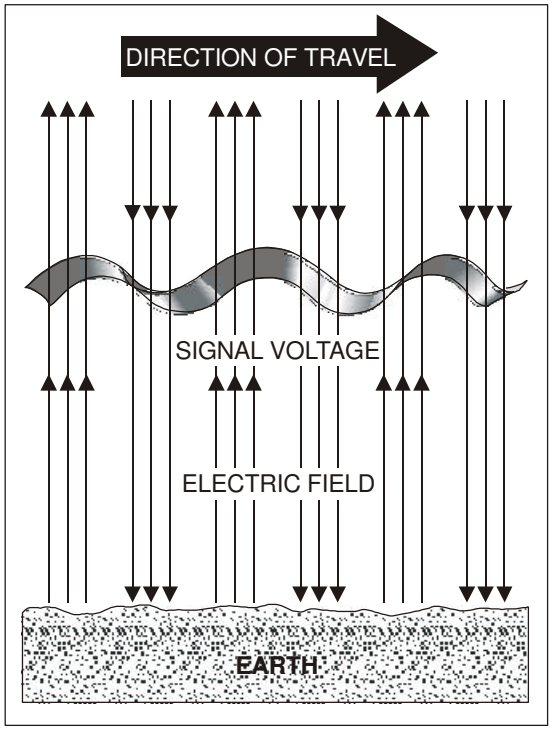


Figure 2-3. Vertical Polarization.

radio wave, maximum pickup results if the antenna is oriented in the same direction as the electric field component. A vertical antenna receives vertically polarized waves, and a horizontal antenna receives horizontally polarized waves. If the field rotates as the waves travel through space, both horizontal and vertical components of the field exist, and the wave is elliptically polarized.

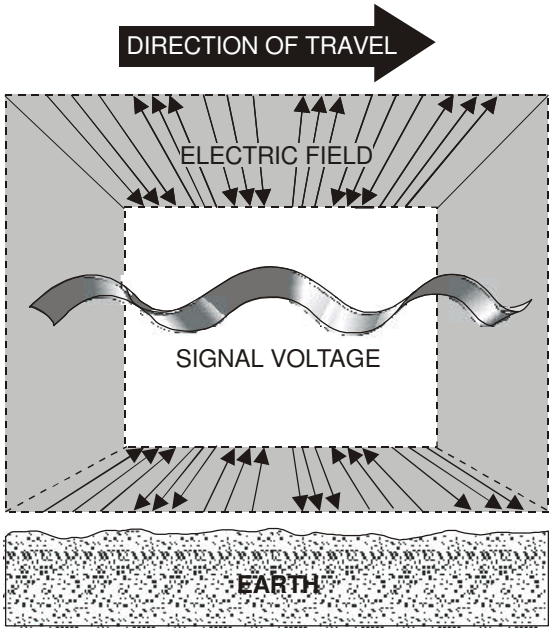


Figure 2-4. Horizontal Polarization.

Polarization Requirements for Various Frequencies

At medium and low frequencies, ground wave transmission is used extensively, and it is necessary to use vertical polarization. Vertical lines of force are perpendicular to the ground, and the radio wave can travel a considerable distance along the ground surface with a minimum amount of loss. Because the Earth acts as a relatively good conductor at low frequencies, horizontal lines of electric force are shorted out, and the useful range with the horizontal polarization is limited.

At high frequencies, with sky wave transmission, it makes little difference whether horizontal or vertical polarization is used. The sky wave, after being reflected by the ionosphere, arrives at the receiving antenna elliptically polarized. Therefore, the transmitting and receiving antennas can be mounted either horizontally or vertically. Horizontal antennas are preferred, since they can be made to radiate effectively at high angles and have inherent directional properties.

For frequencies in the VHF or UHF range, either horizontal or vertical polarization is satisfactory. Since the radio wave travels directly from the transmitting antenna to the receiving antenna, the original polarization produced at the transmitting antenna is maintained as the wave travels to the receiving antenna. If a horizontal antenna is used for transmitting, a horizontal antenna must be used for receiving.

Satellites and satellite terminals use circular polarization. Circular polarization describes a wave whose plane of polarization rotates through 360° as it progresses forward. The rotation can be clockwise or counterclockwise (see fig. 2-5). Circular polarization occurs when equal magnitudes of vertically and horizontally polarized waves are combined with a phase difference of 90°. Rotation in one direction or the other depends on the phase relationship.

Advantages of Vertical Polarization

Simple vertical half-wave and quarter-wave antennas provide omnidirectional communications. This is desirable in communicating with a moving vehicle. The disadvantage is that it radiates equally to the enemy and friendly forces.

When antenna heights are limited to 3.05 meters (10 feet) or less over land, as in a vehicular installation, vertical polarization provides a stronger received signal at frequencies up to about 50 MHz. From about 50 to 100 MHz, there is only a slight improvement over horizontal polarization with antennas at the same height. Above 100 MHz, the difference in signal strength between vertical and horizontal polarization is small. However, when antennas are located near dense forests, horizontally polarized waves suffer lower losses than vertically polarized waves.

Vertically polarized radiation is somewhat less affected by reflections from aircraft flying over the transmission path. With horizontal polarization, such reflections cause variations in received signal

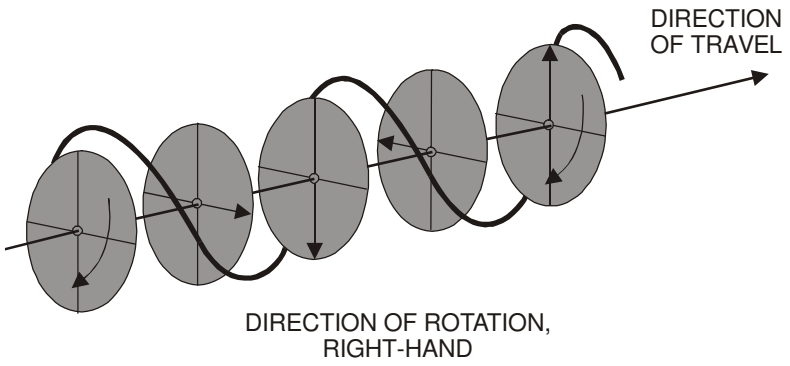


Figure 2-5. Circular Polarization.

strength. An example is the picture flutter in a television set when an aircraft interferes with the transmission path. This factor is important in areas where aircraft traffic is heavy.

When vertical polarization is used, less interference is produced or picked up from strong VHF and UHF transmissions (TV and FM broadcasts) because they use horizontal polarization. This factor is important when an antenna must be located in an urban area that has TV or FM broadcast stations.

Advantages of Horizontal Polarization

A simple horizontal half-wave antenna is bidirectional. This characteristic is useful in minimizing interference from certain directions.

Horizontal antennas are less likely to pick up manmade interference, which is ordinarily vertically polarized. When antennas are located near dense forests, horizontally polarized waves suffer lower losses than vertically polarized waves, especially above 100 MHz. Small changes in antenna location do not cause large variations in the field intensity of horizontally polarized waves when an antenna is located among trees or buildings. When vertical polarization is used, a change of only a few feet in the antenna location may have a significant effect on the received signal strength.

DIRECTIONALITY

Vertical receiving antennas accept radio signals equally from all horizontal directions, just as vertical transmitting antennas radiate equally in all horizontal directions. Because of this characteristic, other stations operating on the same or nearby frequencies may interfere with the desired signal and make reception difficult or

impossible. However, reception of a desired signal can be improved by using directional antennas.

Horizontal half-wave antennas accept radio signals from all directions. The strongest reception is received in a line perpendicular to the antenna (i.e., broadside, and the weakest reception is received from the direction of the ends of the antenna). Interfering signals can be eliminated or reduced by changing the antenna installation so that either end of the antenna points directly at the interfering station.

Communications over a radio circuit is satisfactory when the received signal is strong enough to override undesired signals and noise. The receiver must be within range of the transmitter. Increasing the transmitting power between two radio stations increases communications effectiveness. Also, changing the types of transmission, changing to a frequency that is not readily absorbed, or using a directional antenna aids in communications effectiveness.

Directional transmitting antennas concentrate radiation in a given direction and minimize radiation in other directions. A directional antenna may also be used to lessen interception by the enemy and interference with friendly stations.

RESONANCE

Antennas can be classified as either resonant or nonresonant, depending on their design. In a resonant antenna, almost all of the radio signal fed to the antenna is radiated. If the antenna is fed with a frequency other than the one for which it is resonant, much of the fed signal will be lost and will not be radiated. A resonant antenna will effectively radiate a radio signal for frequencies close to its design frequency (usually only 2 percent above or below the design

frequency). If a resonant antenna is used for a radio circuit, a separate antenna must be built for each frequency to be used on the radio circuit. A nonresonant antenna, on the other hand, will effectively radiate a broad range of frequencies with less efficiency. Resonant and nonresonant antennas are commonly used on tactical circuits. Resonance can be achieved in two ways: physically matching the length of the antenna to the wave and electronically matching the length of the antenna to the wave.

RECEPTION

The radio waves that leave the transmitting antenna will have an influence on and will be influenced by any electrons in their path. For example, as an HF wave enters the ionosphere, it is reflected or refracted back to earth by the action of free electrons in this region of the atmosphere. When the radio wave encounters the wire or metallic conductors of the receiving antenna, the radio wave's electric field will cause the electrons in the antenna to oscillate back and forth in step with the wave as it passes. The movement of these electrons within the antenna is the small alternating electrical current which is detected by the radio receiver.

When radio waves encounter electrons which are free to move under the influence of the wave's electric field, the free electrons oscillate in sympathy with the wave. This generates electric currents which then create waves of their own. These new waves are reflected or scattered waves. This process is electromagnetic scattering. All materials that are good electrical conductors reflect or scatter RF energy. Since a receiving antenna is a good conductor, it too acts as a scatterer. Only a portion of the energy which comes in contact with the antenna is converted into received electrical power; a sizable portion of the total power is re-radiated by the wire.

If an antenna is located within a congested urban environment or within a building, there are many objects which will scatter or re-raditate the energy in a manner that can be detrimental to reception. For example, the electric wiring inside a building can strongly re-radiate RF energy. If a receiving antenna is in close proximity to wires, it is possible for the reflected energy to cancel the energy received directly from the desired signal path. When this condition exists, the receiving antenna should be moved to another location within the room where the reflected and direct signals may reinforce rather than cancel each other.

RECIPROCITY

The various properties of an antenna apply equally, regardless of whether the antenna is used for transmitting or receiving. This is what is meant by reciprocity of antennas. For example, the more efficient a certain antenna is for transmitting, the more efficient it will be for receiving the same frequency. The directive properties of a given antenna will be the same whether it is used for transmission or reception.

For example, figure 2-6 on page 2-14 shows a particular antenna used with a transmitter radiating a maximum amount of energy at right angles to the antenna wire. There is a minimum amount of radiation along the axis of the antenna. If this same antenna is used as a receiving antenna, it receives best in the same directions in which it produced maximum radiation (i.e., at right angles to the axis of the antenna). There is a minimum amount of signal received from transmitters located in line with the antenna wire.

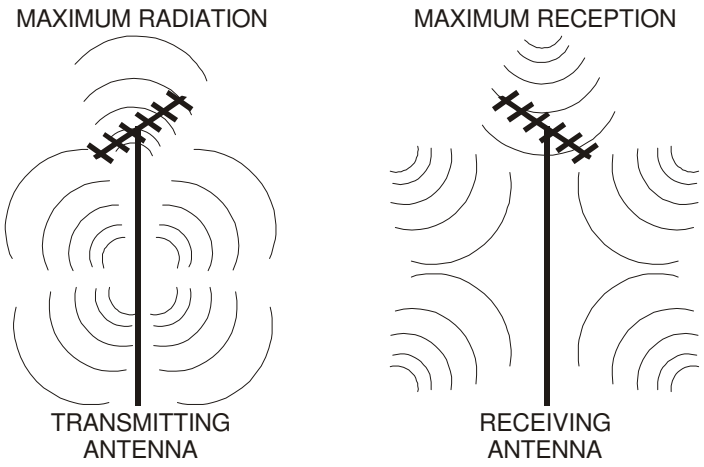


Figure 2-6. Reciprocity.

IMPEDANCE

Impedance is the relationship between voltage and current at any point in an alternating current circuit. The impedance of an antenna is equal to the ratio of the voltage to the current at the point on the antenna where the feed is connected (feed point). If the feed point is located at a point of maximum current, the antenna impedance is 20 to 100 ohms. If the feed point is moved to a maximum voltage point, the impedance is as much as 500 to 10,000 ohms.

The input impedance of an antenna depends on the conductivity or impedance of the ground. For example, if the ground is a simple stake driven about a meter into earth of average conductivity, the impedance of the monopole may be double or even triple the quoted values. Because this additional resistance occurs at a point on the antenna circuit where the current is high, a large amount of

transmitter power will dissipate as heat into the ground rather than radiated as intended. Therefore, it is essential to provide as good a ground or artificial ground (counterpoise) connection as possible when using a vertical whip or monopole.

The amount of power an antenna radiates depends on the amount of current which flows in it. Maximum power is radiated when there is maximum current flowing. Maximum current flows when the impedance is minimized—when the antenna is resonated so that its impedance is pure resistance. (When capacitive reactance is made equal to inductive reactance, they cancel each other, and impedance equals pure resistance.)

BANDWIDTH

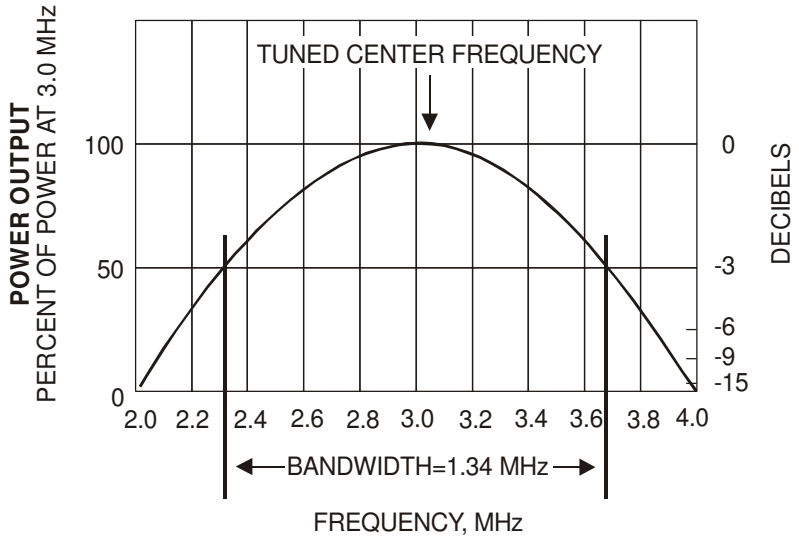
The bandwidth of an antenna is that frequency range over which it will perform within certain specified limits. These limits are with respect to impedance match, gain, and/or radiation pattern characteristics. Typical specification limits are—

- An impedance mismatch of less than 2:1 relative to some standard impedance such as 50 ohms.
- A loss in gain or efficiency of no more than 3 dB.
- A directivity pattern whose main beam is 13 dB greater than any of the side lobes, and a back lobe at least 15 dB below the main beam.
- Bandwidth is measured by changing the frequency of a constant-strength test signal above and below center frequency and measuring power output. The high and low frequencies, where power is one-half (-3 dB) of what it was at center, define the bandwidth. It is expressed as frequency (high minus low) or in percentage (high-low/center x 100%).

In the radio communication process, intelligence changes from speech or writing into a low frequency signal that is used to modulate, or cause change, in a much higher frequency radio signal. When transmitted by an antenna, these radio signals carry the intelligence to the receiving antenna, where it is picked up and reconverted into the original speech or writing. There are natural laws which limit the amount of intelligence or signal that can be transmitted and received at a given time. The more words per minute, the higher the rate and the modulation frequency, so a wider or greater bandwidth is needed. To transmit and receive all the intelligence necessary, the antenna bandwidth must be as wide or wider than the signal bandwidth, otherwise it will limit the signal frequencies, causing voices and writing to be unintelligible. Too wide a bandwidth is also bad, since it accepts extra voices and will degrade the S/N ratio. Figure 2-7 shows how signal bandwidth is defined and gives some examples of bandwidth required to transmit ordinary types of intelligence.

GAIN

The antenna's gain depends on its design. Transmitting antennas are designed for high efficiency in radiating energy, and receiving antennas are designed for high efficiency in picking up (gaining) energy. On many radio circuits, transmission is required between a transmitter and only one receiving station. Energy is radiated in one direction because it is useful only in that direction. Directional receiving antennas increase the energy gain in the favored direction and reduce the reception of unwanted noise and signals from other directions. Transmitting and receiving antennas should have small energy losses and should be efficient as radiators and receptors.



INTELLIGENCE	BANDWIDTH
Voice, AM	6.0 KHz
Voice, FM	46.0 KHz
One microsecond pulses	10,000.0 KHz

Bandwidths necessary to transmit and receive some ordinary kinds of intelligence

Figure 2-7. Bandwidth.

TAKE-OFF ANGLE

The antenna's take-off angle is the angle above the horizon that an antenna radiates the largest amount of energy (see fig. 2-8). VHF communications antennas are designed so that the energy is radiated parallel to the Earth (do not confuse take-off angle and polarization). The take-off angle of an HF communications antenna can determine whether a circuit is successful or not. HF sky wave antennas are designed for specific take-off angles, depending on the circuit distance. High take-off angles are used for short-range communications, and low take-off angles are used for long-range communications.

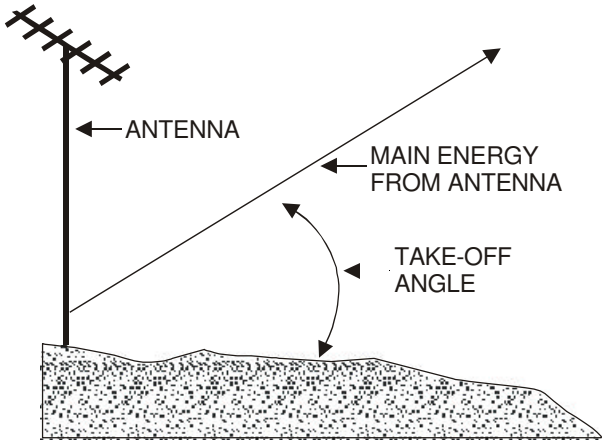


Figure 2-8. Take-Off Angle.

Section II. Ground Effects

Since most tactical antennas are erected over the Earth and not out in free space, except for those on satellites, the ground will alter the free space radiation patterns of antennas. The ground will also affect some of the electrical characteristics of an antenna. It has the greatest effect on those antennas that must be mounted relatively close to the ground in terms of wavelength. For example, medium- and high-frequency antennas, elevated above the ground by only a fraction of a wavelength, will have radiation patterns that are quite different from the free-space patterns.

GROUNDED ANTENNA THEORY

The ground is a good conductor for medium and low frequencies and acts as a large mirror for the radiated energy. The ground reflects a large amount of energy that is radiated downward from an antenna mounted over it. Using this characteristic of the ground, an antenna only a quarter-wavelength long can be made into the equivalent of a half-wave antenna. A quarter-wave antenna erected vertically, with its lower end connected electrically to the ground (fig. 2-9 on page 2-20), behaves like a half-wave antenna. The ground takes the place of the missing quarter-wavelength, and the reflections supply that part of the radiated energy that normally would be supplied by the lower half of an ungrounded half-wave antenna.

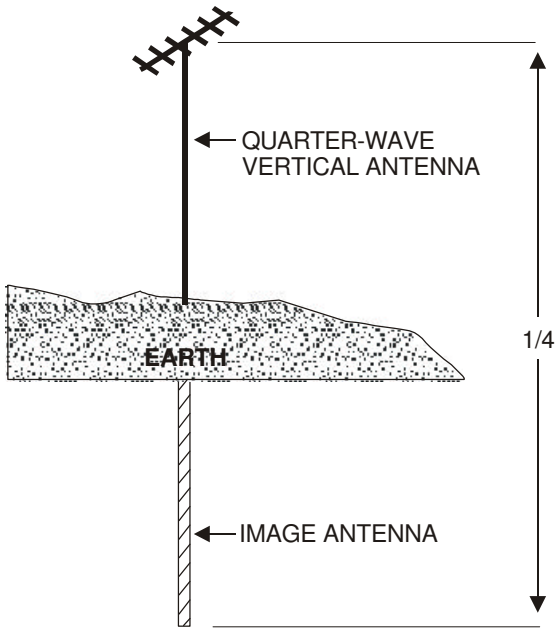


Figure 2-9. Quarter-Wave Antenna Connected to Ground.

TYPES OF GROUNDS

When grounded antennas are used, it is especially important that the ground has as high a conductivity as possible. This reduces ground losses and provides the best possible reflecting surface for the down-going radiated energy from the antenna. At low and medium frequencies, the ground acts as a good conductor. The ground connection must be made in such a way as to introduce the least possible amount of resistance to ground. At higher frequencies, artificial grounds constructed of large metal surfaces are common.

The ground connections take many forms, depending on the type of installation and the loss that can be tolerated. In many simple field installations, the ground connection is made by one or more metal rods driven into the soil. Where more satisfactory arrangements cannot be made, ground leads can be connected to existing devices which are grounded. Metal structures or underground pipe systems are commonly used as ground connections. In an emergency, a ground connection can be made by forcing one or more bayonets into the soil.

When an antenna must be erected over soil with low conductivity, treat the soil to reduce resistance. Treat the soil with substances that are highly conductive when in solution. Some of these substances, listed in order of preference, are sodium chloride (common salt), calcium chloride, copper sulfate (blue vitriol), magnesium sulfate (Epsom salt), and potassium nitrate (saltpeter). The amount required depends on the type of soil and its moisture content.

WARNING

WHEN THESE SUBSTANCES ARE USED, IT IS IMPORTANT THAT THEY DO NOT GET INTO NEARBY DRINKING WATER SUPPLIES.

For simple installations in the field, a single ground rod can be fabricated from pipe or conduit. It is important that a low resistance connection be made between the ground wire and the ground rod. The rod should be cleaned thoroughly by scraping and sandpapering at the point where the connection is to be made, and a clean ground clamp should be installed. A ground wire can then be soldered or joined to the clamp. This joint should be covered with tape to prevent an increase in resistance because of oxidation.

Counterpoise

When an actual ground connection cannot be used because of the high resistance of the soil or because a large buried ground system is not practical, a counterpoise may be used to replace the usual direct ground connection. The counterpoise (fig. 2-10) consists of a device made of wire, which is erected a short distance above the ground and insulated from it. The size of the counterpoise should be at least equal to or larger than the size of the antenna.

When the antenna is mounted vertically, the counterpoise should be made into a simple geometric pattern. Perfect symmetry is not required. The counterpoise appears to the antenna as an artificial ground that helps to produce the required radiation pattern.

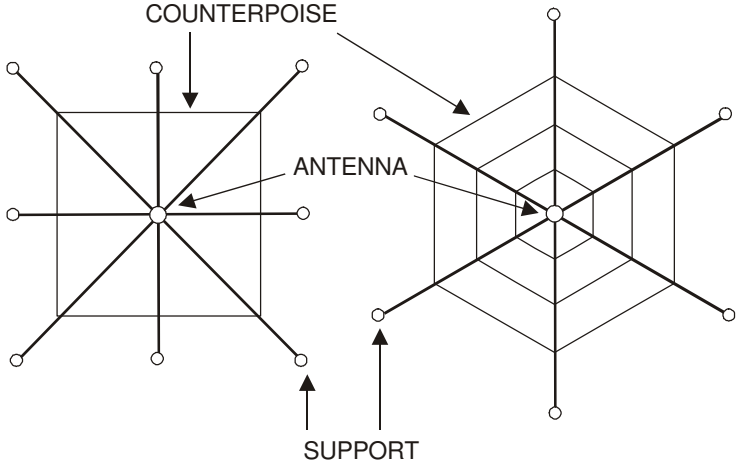


Figure 2-10. Wire Counterpoise.

In some VHF antenna installations on vehicles, the metal roof of the vehicle (or shelter) is used as a counterpoise for the antenna. Small counterpoises of metal mesh are sometimes used with special VHF antennas that must be located a considerable distance above the ground.

Ground Screen

A ground screen consists of a fairly large area of metal mesh or screen that is laid on the surface of the ground under the antenna. There are two specific advantages to using ground screens. First, the ground screen reduces ground absorption losses that occur when an antenna is erected over ground with poor conductivity. Second, the height of the antenna can be set accurately, and the radiation resistance of the antenna can be determined more accurately.

Section III. Calculating Antenna Length

An antenna's length must be considered in two ways: physical and electrical. The two are never the same. The reduced velocity of the wave on the antenna and a capacitive effect (end effect) make the antenna seem longer electrically than physically. The contributing factors are the ratio of the diameter of the antenna to its length and the capacitive effect of terminal equipment (e.g., insulators or clamps) used to support the antenna.

To calculate the antenna's physical length, use a correction of 0.95 for frequencies between 3 and 50 MHz. The figures given are for a half-wave antenna.

$$\text{Length (meters)} = \frac{150 \times 0.95}{\text{Frequency in MHz}} = \frac{142.50}{\text{Frequency in MHz}}$$

$$\text{Length (feet)} = \frac{492 \times 0.95}{\text{Frequency in MHz}} = \frac{468}{\text{Frequency in MHz}}$$

The length of a long-wire antenna (one wavelength or longer) for harmonic operation is calculated by using the following formula, where N = number of half-wavelengths in the total length of the antenna.

$$\text{Length (meters)} = \frac{150\ (N - 0.05)}{\text{Frequency in MHz}}$$

$$\text{Length (feet)} = \frac{492\ (N - 0.05)}{\text{Frequency in MHz}}$$

Example: 3 half-wavelengths at 7 MHz is—

$$\text{Length (meters)} = \frac{150\ (N - 0.05)}{\text{Frequency in MHz}}$$

$$= \frac{150\ (3 - .05)}{7}$$

$$= \frac{150 \times 2.95}{7}$$

$$= \frac{442.50}{7}$$

$$= 63.2 \text{ meters}$$

Section IV. Antenna Orientation

The orientation of an antenna is extremely important. Determining the position of an antenna in relation to the points of the compass can make the difference between a marginal and good radio circuit.

AZIMUTH

If the azimuth of the radio's path is not provided, determine it by the best available means. The accuracy required depends on the radiation pattern of the directional antenna. If the antenna beamwidth is very wide (e.g., 90° angle between half-power points) an error of

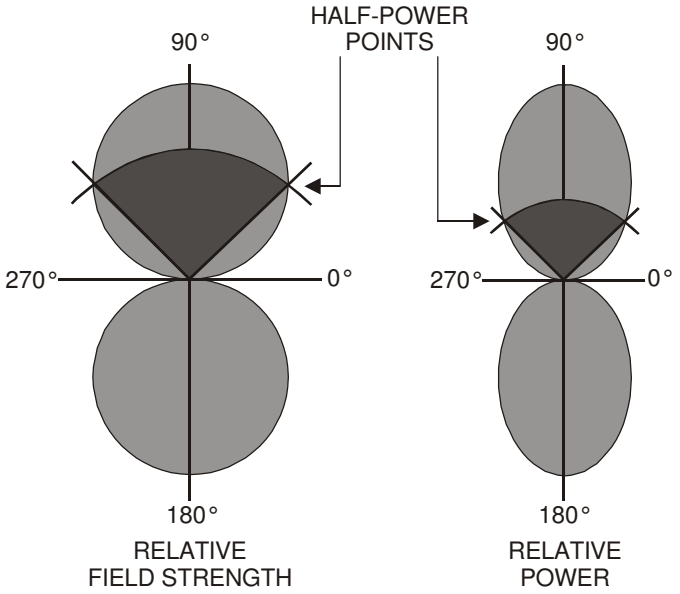


Figure 2-11. Beamwidth Measured on Relative Field Strength and Relative Power Patterns.

10° is of little consequence. In transportable operation, the rhombic and vee antennas may have such a narrow beam that great accuracy is required to determine azimuth. The antenna should be erected for the correct azimuth. Great accuracy is not required to erect broad-beam antennas.

Unless a line of known azimuth is available at the site, the direction of the path is best determined by a magnetic compass. Figure 2-12 on page 2-28 is a map of magnetic declination, showing the variation of the compass needle from the true north. When the compass is held so that the needle points to the direction indicated for the location on the map, all directions indicated by the compass will be true.

Improvement of Marginal Communications

It may not always be feasible to orient directional antennas to the correct azimuth of the desired radio path, and marginal communications may suffer. To improve marginal communications—

- Check, tighten, and tape cable couplings and connections.
- Retune all transmitters and receivers in the circuit.
- Check that the antennas are adjusted for proper operating frequency.
- Change the heights of antennas.
- Move the antenna a short distance away and in different locations from its original location.
- Separate transmitters from receiving equipment, if feasible.

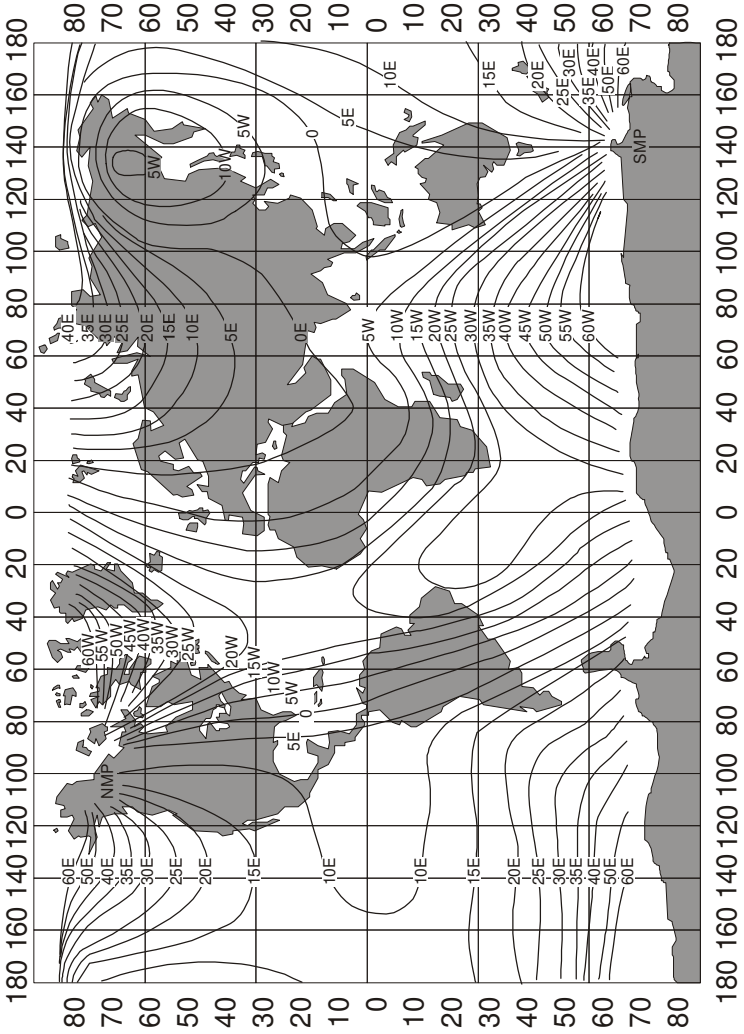


Figure 2-12. Magnetic Declination Over the World.

Transmission and Reception of Strong Signals

After an adequate site has been selected and the proper antenna orientation obtained, the signal level at the receiver will be proportional to the strength of the transmitted signal.

WARNING

EXCESSIVE SIGNAL STRENGTH MAY RESULT IN ENEMY INTERCEPT AND INTERFERENCE OR IN YOUR INTERFERENCE WITH ADJACENT FREQUENCIES.

If a high-gain antenna is used, a stronger signal can be obtained. Losses between the antenna and the equipment can be reduced by using a high quality transmission line, as short as possible, and properly matched at both ends.

WARNING

BE EXTREMELY CAREFUL WHEN PUTTING UP, TAKING DOWN, OR MOVING ANTENNAS LOCATED NEAR HIGH VOLTAGE OR COMMECIAL POWER LINES. ANTENNA CONTACT WITH THESE CAN AND MAY RESULT IN ELECTROCUTION OR SEVERE INJURY TO PERSONNEL HOLDING THE ANTENNA OR THE CONNECTING GUY WIRES AND CABLES.

(reverse blank)

Chapter 3

Transmission Lines

Transmission lines (antenna feed lines) conduct or guide electrical energy from the transmitter to the receiver. This chapter is oriented primarily toward transmission lines with field expedient antennas. For standard issue radios and antennas, use the issued coaxial cable. As long as radios, cables, and antennas are maintained in working order, they will operate as designed and won't require any adjustments or changes based on the information in this chapter.

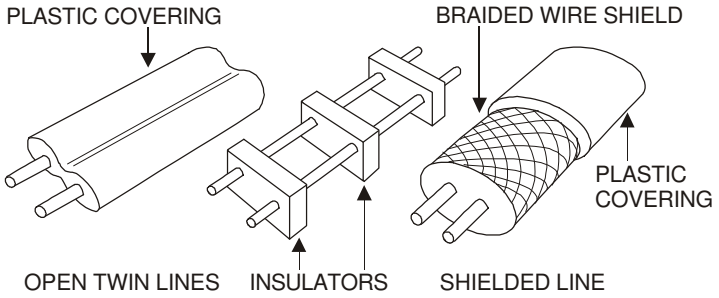
PROPERTIES

Transmission Line Types

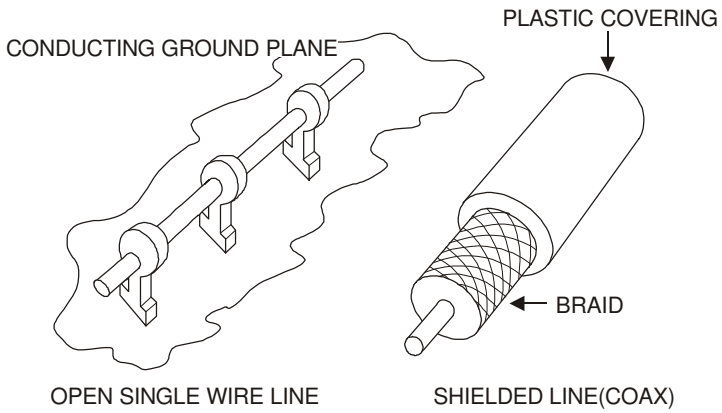
Transmission lines are classified according to construction and length, and fall into two main categories: balanced line and unbalanced line. The terms balanced and unbalanced describe the relationship between transmission line conductors and the Earth. Transmission lines may be classified as resonant or nonresonant lines, each of which may have advantages over the other under a given set of circumstances.

Balanced Line. A balanced line is composed of two identical conductors, usually circular wires, separated by air or an insulating material (dielectric). The voltages between each conductor and ground produced by an RF wave as it moves down a balanced line,

are equal and opposite (i.e. at the moment one of the conductors supports a positive voltage with respect to ground, the other supports a negative voltage of equal magnitude). Some balanced lines carry a third conductor in the form of a braided shield, which acts as ground. Conductor spacings up to several centimeters are commonly used. Figure 3-1 shows balanced and unbalanced lines.



BALANCED TRANSMISSION LINES



UNBALANCED TRANSMISSION LINES

Figure 3-1. Balanced and Unbalanced Transmission Lines.

Unbalanced Line. The unbalanced line is usually open single-wire line or coaxial cable. It is one-half of a balanced line.

Nonresonant Line. A nonresonant line is a line that has no standing waves of current and voltage. It is either infinitely long or is terminated in its characteristic impedance. Because there are no reflections, all of the energy passed along the line is absorbed by the load (except for the small amount of energy dissipated by the line).

Resonant Line. A resonant transmission line has standing waves of current and voltage. The line is of finite length and is not terminated in its characteristic impedance. Reflections are present. A resonant line, like a tuned circuit, is resonant at some particular frequency. The resonant line will present to its source of energy a high or a low resistive impedance at multiples of a quarter-wavelength. Whether the impedance is high or low at these points depends on whether the line is short- or open-circuited at the output end. At points that are not exact multiples of a quarter-wavelength, the line acts as a capacitor or an inductor.

MINIMIZING ENERGY LOSS

To communicate with minimal energy loss, elements such as impedance matching and attenuation (line losses) must be considered.

Impedance

Currents and waves cannot move from place to place without some dissipation; their flow is impeded. Impedance describes the nature and size of whatever impedes their flow. Impedance is an important consideration in selecting the proper transmission line.

A radio wave consists of electric and magnetic fields arranged perpendicularly to each other and to the direction the wave travels. The impedance associated with this wave is the ratio of the potential difference (voltage) to the current (amperage) at a given point along a transmission line. The following formula illustrates this.

$$\frac{\text{Voltage}}{\text{Current}} = \text{Impedance}$$

In transmission lines, because of the length-frequency relationship, the characteristic impedance is more often discussed in terms of capacitance and inductance. In conventional circuits that contain inductors and capacitors, the inductance and capacitance are present in definite lumps. In an RF transmission line, however, these quantities are distributed throughout the entire line and cannot be separated from each other.

If a transmitter is connected to a transmission line that is terminated in a load whose impedance is different from that of the line, only a portion of the available energy will be accepted by the load antenna, and the remainder will be reflected back down the line in the direction of the transmitter. The energy is actually traveling in both directions along the line.

If a transmitter is connected to a transmission line terminated in a load whose impedance exactly equals the impedance of the line, the line will absorb all of the energy except for that lost in the resistive and dielectric losses of the line. Current flowing through the line will be uniformly distributed along its length, and the voltage between the conductors on the line will be equal at all points. When this condition exists, the line is said to be perfectly matched and carries only a forward or incident wave. If the impedance of the transmission line and the load also equal the internal impedance (output impedance) of the transmitter, a maximum transfer of

energy (lowest system loss) is achieved (i.e., the transmitter or receiver, transmission line, and antenna are all the same impedance), and the best possible transfer of signal energy will occur.

Optimizing Line Length

When it is necessary to use a transmission line whose impedance is significantly different from that of the load, it is possible to make good use of standing waves and the repetitive impedance variations along the line to match the antenna to the transmitter or the receiver to the antenna by cutting the line to a specific length. An example is when the only available equipment consists of a 300-ohm twin-lead transmission line; a 50-ohm half-wave dipole antenna; and a 50-ohm internal impedance transceiver. (Note: The internal impedance of most USMC radios is 50 ohms). Ordinarily, this impedance combination would result in lost energy that could affect the quality of communications. However, if a single frequency is used to communicate, the length between the antenna and the receiver can be matched. This occurs because the impedance of the receiver is repeated at intervals of a half-wavelength along the line.

For end-fed, long-wire antennas, a similar impedance match can be made by feeding the long wire with a quarter-wavelength piece of wire that is connected to the transmitter on one end and to the end of the long wire on the other. The quarter-wavelength section doesn't need to be a separate piece of wire. For a 2-wavelength, long-wire antenna, for example, the wire can be cut to 2 1/4 wavelengths. The entire quarter-wavelength section then becomes the transmission line between the radio and the antenna.

Attenuation

Transmission lines do not transfer all of the energy applied at one end of the line to the opposite end. Attenuation is energy that is lost when converted into heart, partially due to conductor (wire) resistance. More energy is lost due to the insulation material used to space the conductors (dielectric loss). Some insulating materials (e.g., Teflon) have extremely low loss while others (e.g., rubber or wood) have relatively high loss, especially at frequencies above about 30 MHz. Old, dry wood (especially redwood) may be boiled in paraffin or bee's wax to make a fairly good insulator at frequencies up to about 200 MHz. Polyethylene, a common insulation material used in coaxial cables, has an average loss of about twice that of Teflon in the 100-MHz range for cables having a diameter of less than about one centimeter. Dry air is a better insulator than most solid, liquid, or flexible materials. Some inert gases (e.g., nitrogen, helium, and argon) are superior to air and are often used under pressure to fill coaxial cables used with high-powered transmitters.

Since attenuation results from conductor resistance and dielectric loss, transmission lines using large diameter conductors lose less energy than cables having small diameter conductors. Also, transmission lines having a large spacing between conductors (high impedance) will lose less energy than those with a smaller spacing (lower impedance) since they carry smaller currents and there is less energy lost in conductor resistance. Thus, 300-ohm twin-lead has less loss than coaxial cable at most frequencies. Among coaxial cables, the larger the diameter, the lower the loss, assuming the same insulator is used. It is also true that coaxial cable, which has an impedance of 75 ohm, has slightly lower loss than 50-ohm cable, when both cables have about the same diameter. When there is a choice, it is best to use the largest available transmission line which matches the impedance of both the antenna and transmitter.

MAKING THE BEST USE OF AVAILABLE TRANSMISSION LINES

It is often necessary to feed a balanced antenna (e.g., horizontal dipole) with coaxial cable. While this is not considered good practice, it will perform satisfactorily under most conditions. When coaxial cable is used for this purpose, it should run perpendicular to the dipole wires for a distance greater than one-half of the length of the dipole. This will help to prevent unwanted RF power from being induced on the outside shield of the cable. It is also advisable to make sure that the total length of the coaxial cable and one side of the antenna is not equal to a half-wavelength or any multiple thereof. This will prevent the outside conductor from becoming resonant and acting as a radiating part of the antenna. The same precaution should be taken with twin-lead transmission line.

Occasionally, it may also be necessary to feed an unbalanced antenna (e.g., a whip with twin-lead or balanced line). Again this is not considered good practice, but the bad effects can be minimized if care is taken. If the transmitter has a balanced output circuit, little difficulty will be experienced. However if the output is unbalanced, the hot terminal or coaxial center at the transmitter output must be connected to the same wire of the twin-lead as is the vertical whip at the other end of the twin-lead. This ensures that the ground side of the transmitter output is connected to the side of the twin-lead that goes to the ground side of the unbalanced antenna.

If the twin-lead is reversed and the antenna ground terminal is connected to the hot terminal of the transmitter, a large portion of the transmitter output may be wasted, making communications either difficult or impossible. Twin-lead of the type commonly used with television sets usually has one tinned and one bare copper conductor. This color coding readily permits correct connection of the transmitter to the antenna. It is also advisable to make the length of

the twin-lead equal to a half-wavelength or any multiple of a half-wavelength. When possible, the twin-lead should be twisted so that it forms a long helix with about one twist every thirty centimeters, or so. Twisting helps to prevent transmission line radiation and reduces noise pickup when receiving.

Twin-Lead Limitations

It is generally best not to use twin-lead or balanced line at frequencies higher than about 200 MHz for three reasons.

First, the spacing between the two wires becomes sufficiently large in terms of a wavelength that radiation from the line occurs. When lengths over 30 meters are employed, this radiation may represent a significant loss of energy.

Second, if the twin-lead or balanced lines must come in close contact (less than 2 or 3 cm) with metal, masonry, or wood surfaces, additional losses will be encountered due to the substantial impedance change which takes place along the section of the line next to the surface. This mismatch loss becomes apparent at frequencies above 200 MHz because the length of the section affected becomes a substantial portion of a wavelength long. At lower frequencies, the section of line involved is too short to be seriously affected.

Third, twin-lead picks up more locally generated interference than coaxial cable since the outer conductor of the coaxial cable acts as a shield for the center conductor. Radiation and noise pickup by twin-lead can be partially prevented by twisting it once every 20 or 30 centimeters.

When using common, TV twin-lead (300 ohm), preference should be given to the deep brown rather than the light, colorless variety. The darker colored twin-lead withstands the effects of sunlight and

moisture after prolonged outdoor exposure much better than the clear type. The clear, colorless, twin-lead tends to crack after a few months exposure to the Sun. It also begins to absorb moisture which greatly increases energy loss.

Directly Connecting the Transceiver and Antenna

In many instances the transmitter or receiver may be connected directly to the antenna wire without using a transmission line. This is particularly true with indoor antennas in the HF range and with many VHF whip antennas designed for use with manpack transceivers.

When a direct connection is made between a transmitter and the antenna at frequencies below 30 MHz or where the length of the antenna wire is much shorter than 0.25 λ, the output circuit of the transmitter usually contains a matching device which may be used to tune the antenna efficiently to resonance. This tuning actually matches the impedance of the antenna to the output impedance of the transmitter.

When a VHF transceiver is designed to connect directly to a short whip or self-contained, collapsible rod, the output circuit is usually designed to accommodate the range of impedances likely to be encountered at the base of the whip or rod.

The efficiency of these devices is usually low since the ground return circuit for the antenna may range from nothing more than the case of the transmitter to the hand and body of an individual holding the device. The impedance of the antenna may vary with frequency over a range of 5 to 1 or greater. Thus, antenna efficiencies of from 25 to 50 percent are not uncommon with such devices.

BALUNS

There are times when a balanced antenna must be used with a transmitter or receiver which has an unbalanced output or input circuit. While it is possible to make a direct connection between balanced and unbalanced devices, it is certainly not good practice. A balun can be used to transform energy from balanced to unbalanced devices and vice versa.

The word balun comes from balanced to unbalanced transformer. Many balun types are easily constructed in the field. Using them can often make the difference between marginal communications and completely solid contact. This may be especially true in the receiving case where a balun can result in a substantial reduction in the amount of manmade noise and interference received by a poorly balanced antenna system. The balun is usually placed at the antenna terminals so that a coaxial transmission line can be used. However, it is possible to feed a balanced antenna with twin-lead or any kind of balanced line, and the balun is placed near the transmitter or receiver terminals (see figs. 3-2 and 3-3).

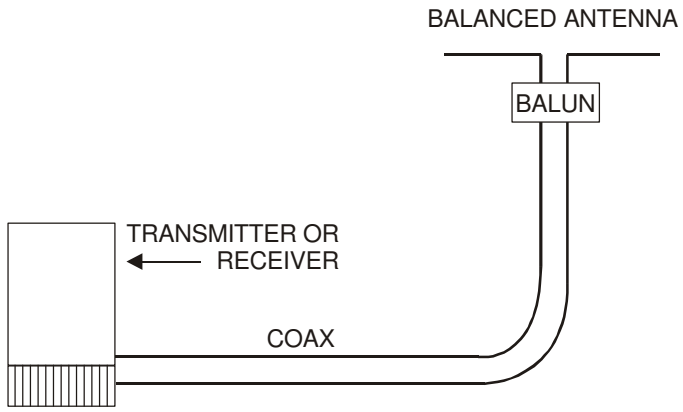


Figure 3-2. A Balun Placed at the Antenna.

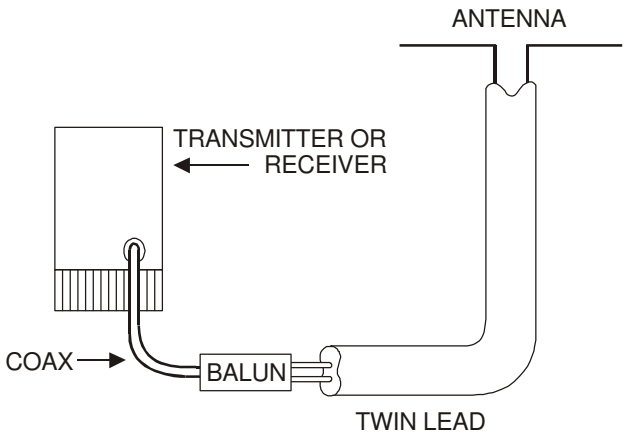


Figure 3-3. Balun Placed at the Transmitter or Receiver.

Cable Connectors

Cable connector fittings are available for all standard transmission lines. Although it takes some time to prepare the cable ends and solder the fittings on, it may be well worth it later if rapid assembly or disassembly of a communications system is necessary.

Balanced Antenna

It is highly desirable to use a receiving antenna which is balanced with respect to ground. This insures the antenna's insensitivity to locally generated noise. Balancing only the receiving antenna is not enough. The entire receiving system must be balanced to successfully reject noise. The antenna should be connected to its receiver so as not to disrupt the antenna's balance. Receivers are supplied with either balanced or unbalanced antenna terminals, and sometimes both.

(reverse blank)

Chapter 4

HF Antenna Selection

The HF portion of the radio spectrum is very important to communications. Radio waves in the 3 to 30 MHz frequency range are the only ones that are capable of being reflected or returned to Earth by the ionosphere with predictable regularity. To optimize the probability of a successful sky wave communications link, select the frequency and take-off angle that is most appropriate for the time of day transmission is to take place.

Merely selecting an antenna that radiates at a high elevation angle is not enough to ensure optimum communications. Various large conducting objects, in particular the Earth's surface, will modify an antenna's radiation pattern. Sometimes, nearby scattering objects may modify the antenna's pattern favorably by concentrating more power toward the receiving antenna. Often, the pattern alteration results in less signal transmitted toward the receiver.

When selecting an antenna site, the operator should avoid as many scattering objects as possible. How the Earth's surface affects the radiation pattern depends on the antenna's height. The optimum height above electrical ground is about 0.4 λ at the transmission frequency. However, the exact height is not critical.

Although NVIS is the chief mode of short-haul HF propagation, the ground wave and direction (LOS) modes are also useful over short paths. How far a ground wave is useful depends on the electrical conductivity of the terrain or body of water over which it travels. The direct wave is useful only to the radio horizon, which extends slightly beyond the visual horizon.

ANTENNA SELECTION PROCEDURE

Selecting the right antenna for an HF radio circuit is very important. When selecting an HF antenna, first consider the type of propagation. Ground wave propagation requires low take-off angle and vertically polarized antennas. The whip antenna included with all radio sets provides good omnidirectional ground wave radiation.

If a directional antenna is needed, select one with good, low-angle vertical radiation. An example is an AN/MRC-138 with its component 32-foot whip set up on a 200-mile circuit. With the radiation characteristics of the whip antenna, the radiated power of the transmitter or whip could be 300 watts for the take-off angle required for a 200-mile circuit.

If a 35-foot half-wave horizontal dipole is used instead of the whip, the radiated power would be 5,000 watts. By using the dipole instead of the whip, the radiated power is increased more than 16 times. A circuit with 5,000 watts of radiated power produces a better signal than a 300-watt circuit using the same frequency.

Selecting an antenna for sky wave propagation is more complex. First, find the circuit (range) distance so that the required take-off angle can be determined. Table 4-1 gives approximate take-off angles for daytime and nighttime sky wave propagation. A circuit distance of 966 kilometers (600 miles) requires a take-off angle of approximately 25° during the day and 40° at night. Select a high-gain antenna (25° to 40°). If propagation predictions are available, skip this step, since the predictions will probably give the take-off angles required.

Next, determine the required coverage. A radio circuit with mobile (vehicular) stations or several stations at different directions from the transmitter requires an omnidirectional antenna. A point-to-point

circuit uses either a bidirectional or a directional antenna. Normally, the receiving station locations dictate this choice (see table 4-1).

Table 4-1. Take-Off Angle vs. Distance.

Take-off Angle (Degrees)	Distance			
	F2 Region Daytime		F2 Region Nighttime	
	kilometers	miles	kilometers	miles
0	3220	2000	4508	2800
5	2415	1500	3703	2300
10	1932	1200	2898	1800
15	1450	900	2254	1400
20	1127	700	1771	1100
25	966	600	1610	1000
30	725	450	1328	825
35	644	400	1127	700
40	564	350	966	600
45	443	275	805	500
50	403	250	685	425
60	258	160	443	275
70	153	95	290	180
80	80	50	145	90
90	0	0	0	0

Before selecting a specific antenna, examine the available construction materials. At least two supports are needed to erect a horizontal dipole, with a third support in the middle for frequencies of 5 MHz or less. If these supports or other items to use as supports are unavailable, the dipole cannot be constructed, and another antenna should be selected. Examine the proposed antenna site to determine if the antenna will fit. If not, select a different antenna.

The site is another consideration. Usually, the tactical situation determines the position of the communications antennas. The ideal setting would be a clear, flat area (i.e., no trees, buildings, fences, power lines, or mountains). Unfortunately, an ideal location is seldom available. Choose the clearest, flatest area possible. If the proposed site is obstructed, try to maintain the horizontal distance listed in table 4-2. Often, an antenna must be constructed on irregular sites. This does not mean that the antenna will not work. It means that the site will affect the antenna's pattern and function.

Table 4-2. Assuming a 30-Foot Antenna and 75-Foot Trees

Take-Off Angle (Degrees)	Required Horizontal Distance from Trees	
0	18	kilometers
5	1932	meters
10	966	meters
15	644	meters
20	483	meters
25	370	meters
30	298	meters
35	241	meters
40	201	meters
45	169	meters
50	145	meters
60	105	meters
70	64	meters
80	32	meters
90	0	meters

After selecting the antenna, determine how to feed the power from the radio to the antenna (fig. 4-1). Most tactical antennas are fed with coaxial cable (RG-213). Coaxial cable is a reasonable compromise of efficiency, convenience, and durability. Issued antennas include the necessary connectors for coaxial cable or for direct connection to the radio.

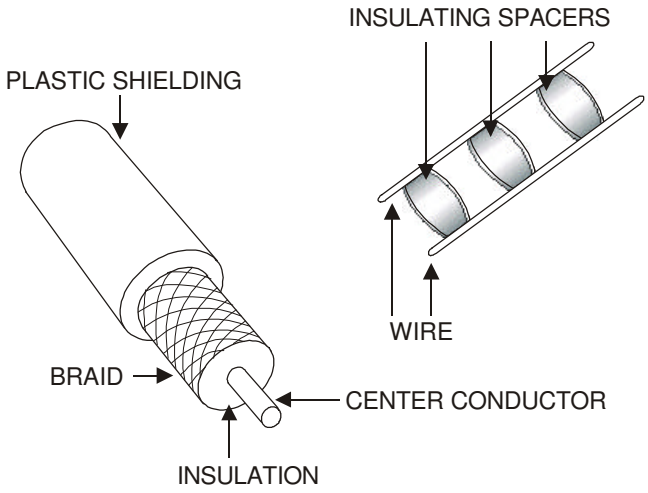


Figure 4-1. Antenna Feed Lines.

Problems may arise in connecting field expedient antennas. The horizontal half-wave dipole uses a balanced transmission line (open-wire). Coaxial cable can be used, but it may cause unwanted RF current.

A balun prevents unwanted RF current flow, which causes a radio to be hot and shock the operator. Install the balun at the dipole feed point (center) to prevent unwanted RF current flow on the coaxial cable. If a balun is unavailable, use the coaxial cable that feeds the

antenna as a choke (see fig. 4-2). Connect the cable's center wire to one leg of the dipole and the cable braid to the other antenna leg. Form the coaxial cable into a 6-inch coil (consisting of ten turns), and tape it to the antenna under the insulator for support.

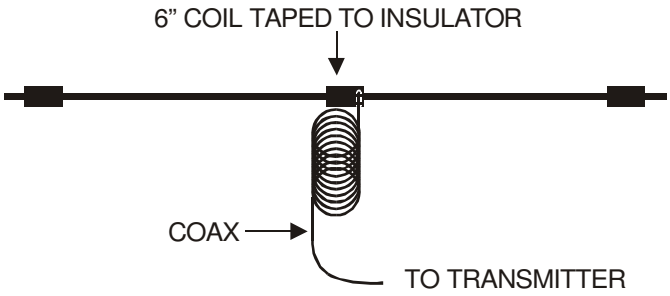


Figure 4-2. Coax RF Current Choke.

DETERMINING ANTENNA GAIN

Determine antenna gain at a specific take-off angle from the vertical radiation pattern. Figure 4-3 shows the vertical antenna pattern for the 32-foot vertical whip. The numbers along the outer ring (90°, 80°, 70°) represent the angle above the Earth; 90° would be straight up, and 0° would be along the ground. Along the bottom of the pattern are numbers from -10 (at the center) to +15 (at the edges). These numbers represent the gain in decibels over an isotropic radiator (dBi).

To find the antenna gain at a particular frequency and take-off angle, locate the desired take-off angle on the plot. Follow that line toward the center of the plot to the pattern of the desired frequency. Drop down and read the gain from the bottom scale. If the gain of a 32-foot vertical whip at 9 MHz and 20° take-off angle is desired, locate 20° along the outer scale. Follow this line to the 9-MHz

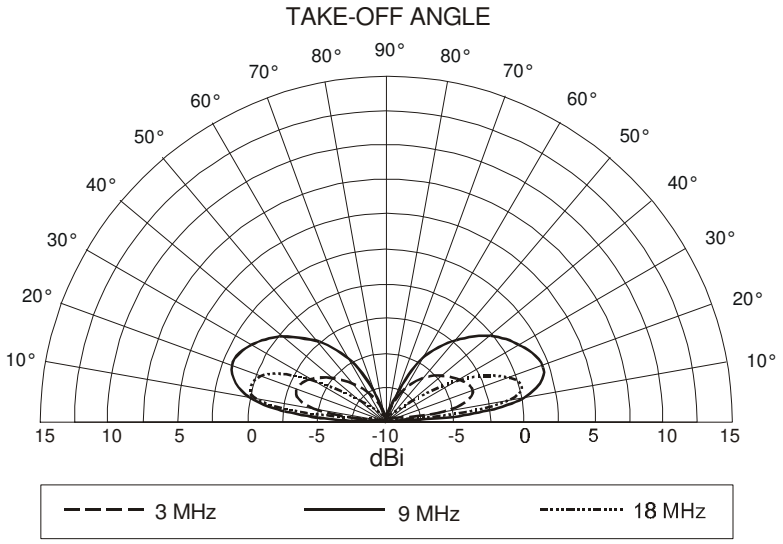


Figure 4-3. 32-Foot Vertical Whip, Vertical Pattern.

pattern line. Move down to the bottom scale. The gain is a little less than 2.5 dBi (the line between 0 and 5 dBi). The gain of the 32-foot vertical whip at 9 MHz and 20° is 2 dBi.

Once the antenna's overall characteristics are determined, use the antenna selection matrix (table 4-3 on page 4-8) to find the specific antenna for a circuit. If the proposed circuit requires a short-range, omnidirectional, wideband antenna, the selection matrix shows that the only antenna that meets all the criteria is the AS-2259/GR.

If the circuit requires a medium-range directional antenna, several antennas could be used (e.g., long wire, sloping vee, or vertical half-rhombic). The antenna choice depends on available installation space, available components, and required highest gain take-off angle. For a required take-off angle of 25° at a frequency of 9 MHz,

the 100-foot vertical half-rhombic antenna is the best choice because it provides the highest gain at the required take-off angle.

Table 4-3. Antenna Selection Matrix.

	Use				Directivity			Polar-ization		Band-width	
		Sky Wave									
	Ground Wave	Short (500 Miles)	Medium (500 to 1200 Miles)	Long (1200 Miles)	Omnidirectional	Bidirectional	Directional	Horizontal	Vertical	Wide	Narrow
AS-2259/GR		X			X					X	
Vertical Whip	X				X				X	X	
Half-Wave Dipole		X	X			X		X			X
Inverted Vee	X	X	X			X		X	X		X
Long Wire	X		X	X		X	X		X	X	
Inverted L	X	X	X		X	X		X	X		X
Sloping Vee	X		X	X			X	X		X	
Sloping Wire	X		X	X		X	X		X	X	
Vertical Half-Rhombic	X		X	X			X		X	X	

ANTENNA TYPES

The AS-2259/GR, vertical whip, half-wave dipole, inverted vee, long wire, inverted L, sloping vee, sloping wire, and vertical half-rhombic antennas are described and illustrated.

AS-2259/GR

The AS-2259/GR antenna (fig. 4-4) provides NVIS propagation for short-range radio circuits. It consists of two crossed sloping dipoles positioned at right angles to each other and is supported at the center by a 15-foot mast. In use, the dipole's components provide guying support for the mast. Characteristics are—

Frequency range:	**2 to 30 MHz**
Polarization:	**Horizontal and vertical simultaneously**
Power capability:	**1,000 watts**
Radiation pattern	
Azimuthal (bearing):	**Omnidirectional**
Vertical (take-off angle):	**See figure 4-5 on page 4-10**

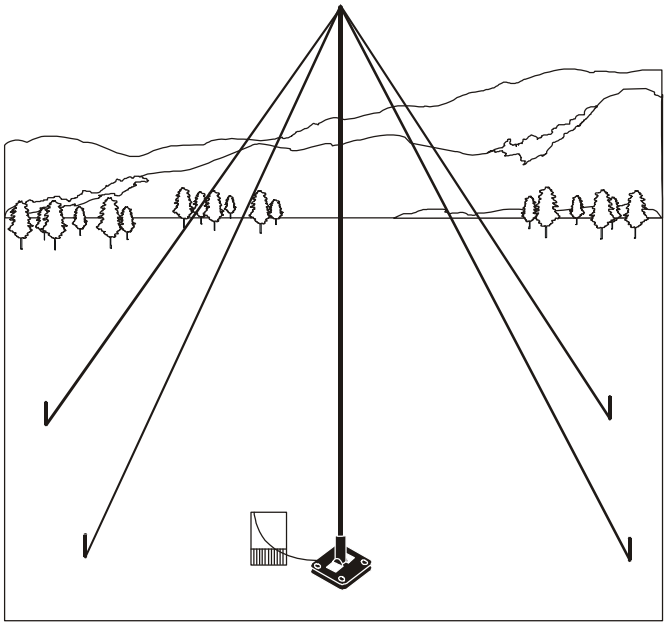


Figure 4-4. AS-2259/GR.

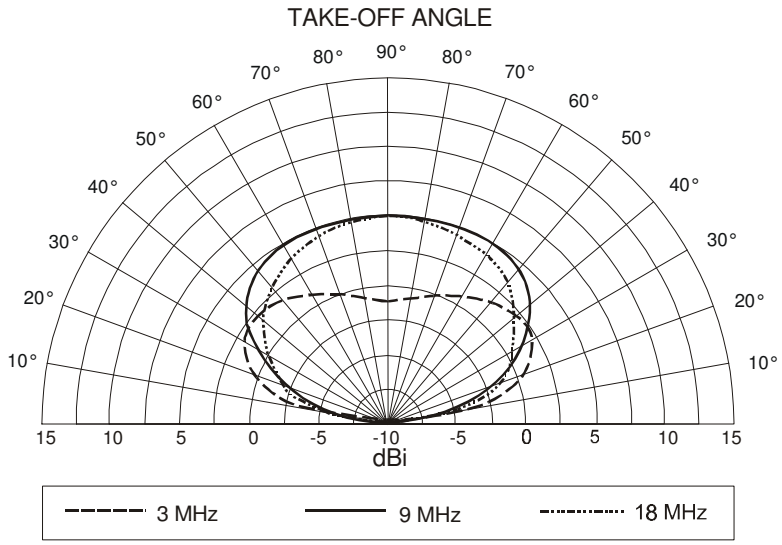


Figure 4-5. AS-2259 Vertical Radiation Pattern.

Vertical Whip

The vertical whip is a component of all Marine Corps radio sets (see fig. 4-6). It is available and easy to use on almost all radio circuits; however, it is probably the worst antenna to use on sky wave circuits. Unless the radio circuit involves omnidirectional ground wave propagation, any other antenna would provide better communications. For example, vertical whips are often used for long-range point-to-point circuits with marginal success. Since the circuit is point-to-point, there is no need to radiate energy in all directions. Radiation in directions other than at the distant station is wasted and serves no useful purpose. Concentrating the omnidirectional radiation at the distant station produces a better received signal and reduces interference around the transmitting antenna. Concentrate radiation in a single direction with a directional antenna. Figures

4-7 on page 4-12, 4-8 on page 4-13, and 4-3 on page 4-7 illustrate various vertical whip antenna patterns.

Characteristics are—

Frequency range:	**2 to 30 MHz**
Polarization:	**Vertical**
Power capability:	**Matched to specific radio**
Radiation pattern	
Azimuthal (bearing):	**Omnidirectional**
Vertical (take-off angle):	**See figures 4-7 on page 4-12, 4-8 on page 4-13, and 4-3 on page 4-7**

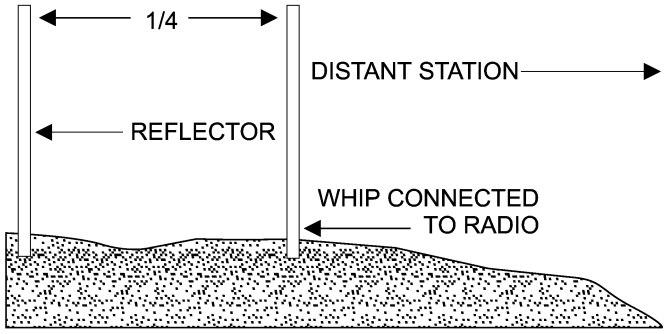


Figure 4-6. Vertical Whip with Reflector.

If a vertical whip must be used, there are several techniques to improve the antenna radiation. If the antenna is mounted directly to the radio, ground the radio. If the antenna is remoted from the radio ground the antenna base plate. A 6-foot ground rod is preferable for both. Ground radials (wires spread out like wheel spokes with the antenna at the center) may improve the antenna radiation. Connect these radials to the ground rod directly beneath the antenna.

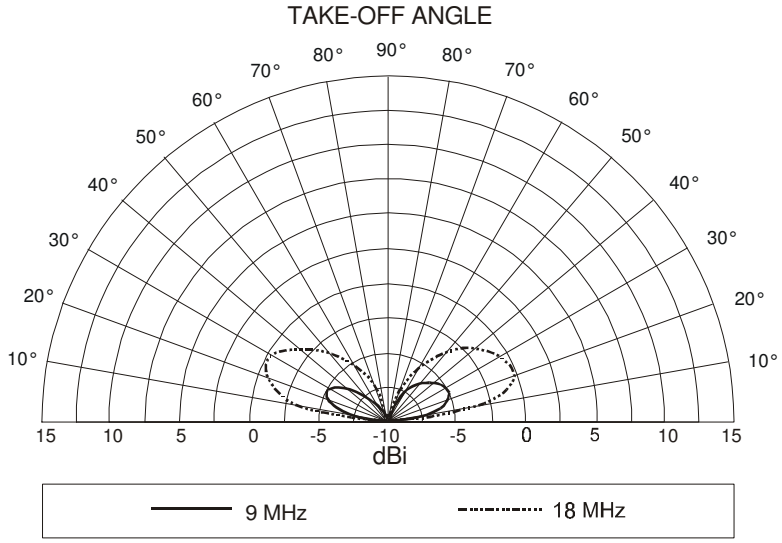


Figure 4-7. 10-Foot Vertical Whip (Vertical Pattern).

A ground radial system can be constructed easily from field telephone wire (WDl/TT) and can be kept with the radio. Cut the field wire into twenty 45-foot lengths, and remove 6 inches of insulation from one end. Using twine or a clamp, bundle together the uninsulated (bare) ends. Attach a 2-foot length of thick wire to the bare ends so that the thick wire extends about one foot beyond the wire bundle. Solder the wire bundle to ensure good electrical contact. In use, the thick wire extending from the bundle connects the radials to a ground rod. The radials are then spread out like wheel spokes with the vertical whip at the center. Radio operators should experiment with different radial systems to determine which one provides the best connectivity.

A reflector placed approximately one-quarter wavelength behind a vertical whip may also improve the whip's performance. A reflector

is a vertical wire, metallic pole, or another whip that is insulated from the ground. It is placed so that the reflector, the whip, and the distant station are on a straight line. The reflector will reflect radio energy striking it and cause the energy to travel toward the distant station, increasing the total energy radiated in the desired direction. To work properly, the reflector must be longer than the whip. If the reflector is shorter, it will act as a director, directing the radio signal away from the distant station. A reflector is longer and is placed behind the whip; a director is shorter and is placed between the whip and the distant station. Adjust the position of the reflector while listening to the distant station until the strongest signal is received.

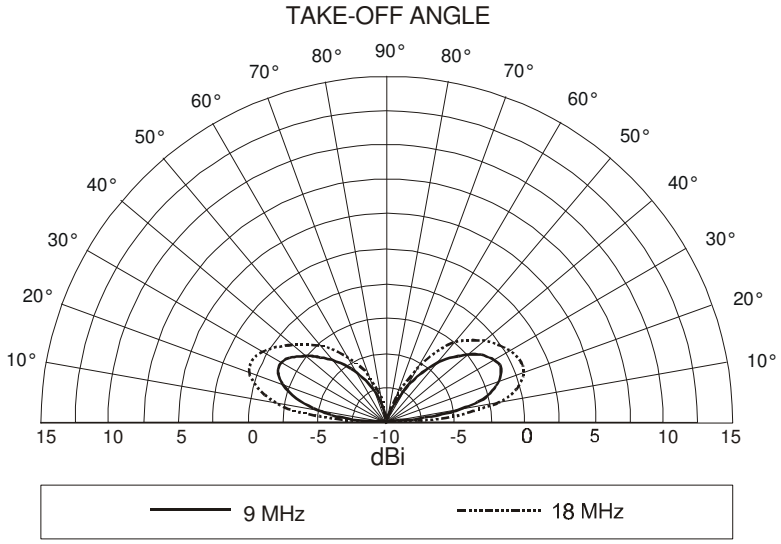


Figure 4-8. 15-Foot Vertical Whip (Vertical Pattern).

The length of a vertical whip antenna is calculated from the following formula:

$$\text{Length in feet} = \frac{234}{\text{Frequency in MHz}}$$

For WD-l/TT

$$\text{Length in feet} = \frac{225.50}{\text{Frequency in MHz}}$$

Half-Wave Dipole

The horizontal half-wave dipole (doublet) antenna is used on short- and medium-length sky wave paths (up to approximately 1,200 miles). Since it is relatively easy to design and construct, the doublet is the most commonly used field expedient wire antenna. It is a very versatile antenna; by adjusting the antenna's height above ground, the maximum gain can vary from medium take-off angles (for medium path-length circuits) to high take-off angles (for short path-length circuits). When the antenna is constructed for medium take-off angle gain (a height of approximately one-half wavelength), the doublet is a bidirectional antenna (i.e., the maximum gain is at right angles to the wire). This is the broadside pattern normally associated with a half-wave dipole antenna. Format A in figure 4-9 shows this pattern in polar plot format.

Format B shows the radiation off the ends of the wire. It is easily seen by comparing with format A that for maximum gain, a doublet one-half wavelength above ground should be constructed so that the side of the antenna points in the direction of the distant station. If the antenna is lowered to only one-quarter wavelength above ground, format C results. This lower antenna height produces

maximum gain at high take-off angles. In format D, the radiation off the ends of the doublet also has maximum gain at high take-off angles. This means that for short path-length circuits, which require high take-off angles, a doublet antenna one-quarter wavelength above ground produces almost omnidirectional coverage.

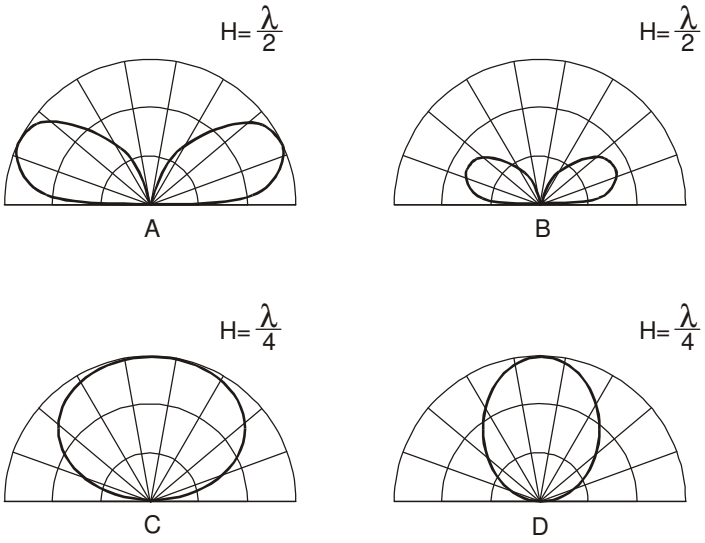


Figure 4-9. Illustrative Doublet Antenna Patterns.

The vertical plots included for half-wave dipole antennas are given for heights from 8 to 12 meters. The plot for 8 meters shows that for 3 and 9 MHz the antenna has high-angle radiation. At those frequencies the antenna is close to ground (compared to a half-wavelength). The pattern for 18 MHz shows the characteristic bidirectional pattern since 8 meters is a half-wave at 18 MHz.

The half-wave dipole is a balanced resonant antenna (see fig. 4-10 on page 4-16). It produces its maximum gain for a very narrow

range of frequencies, normally 2 percent above or below the design frequency. Since frequency assignments are usually several megahertz apart, it is necessary to construct a separate dipole for each frequency assigned (see figs. 4-11 and 4-12 on page 4-17, and 4-13 on page 4-19). If space and other resources are unavailable to erect separate dipoles, three or four dipoles can be combined to occupy the space normally required for one.

Each wire is a half-wavelength for an assigned frequency. The separate dipoles are connected to the same center insulator, or preferably a balun, and are fed by a single coaxial cable. When the antenna is

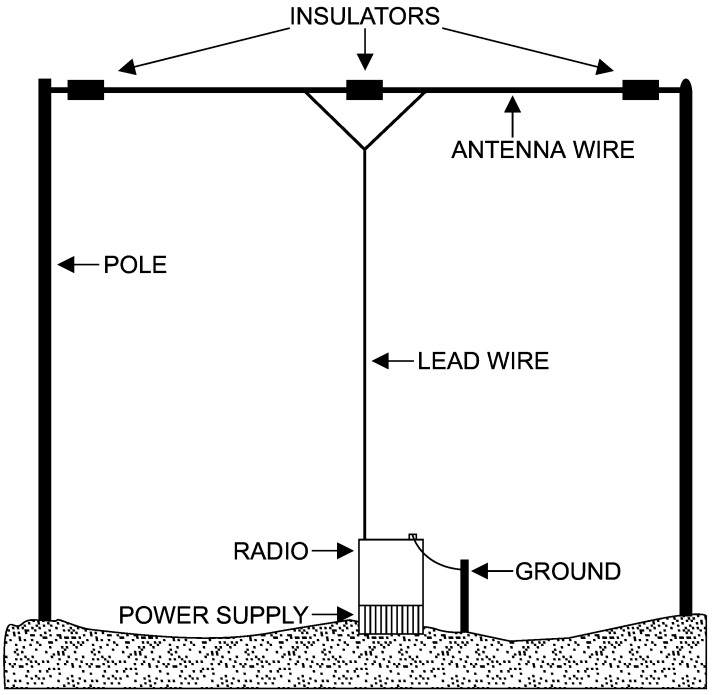


Figure 4-10. Half-Wave Dipole Antenna.

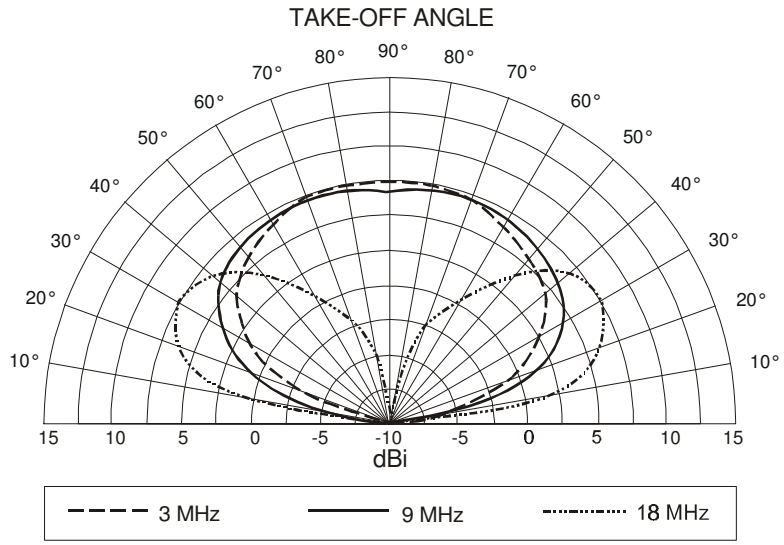


Figure 4-11. 8-Meter Half-Wave Dipole (Vertical Pattern).

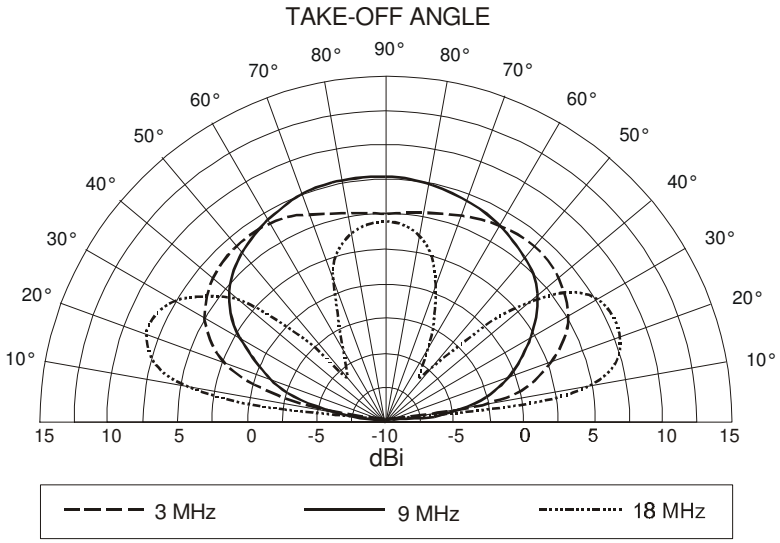


Figure 4-12. 10-Meter Half-Wave Dipole (Vertical Pattern).

fed with an assigned frequency, the doublet cut for that frequency will radiate the energy. Up to four separate dipoles can be combined in this manner. When constructing this antenna, examine the individual frequency assignments to determine if one frequency is three times as large as another. If this relationship exists between two frequencies, one dipole cut in length for the lower of the two frequencies will work well for both frequencies.

The length of a half-wave dipole is calculated from the following relationship:

$$\text{Dipole length} = \frac{\text{142 meters}}{\text{Frequency in MHz}} \quad \text{or} \quad \frac{\text{468 feet}}{\text{Frequency in MHz}}$$

The height of a half-wave dipole is figured using—

$$\text{Height X/4} = \frac{\text{75 meters}}{\text{Frequency in MHz}} \quad \text{or} \quad \frac{\text{246 feet}}{\text{Frequency in MHz}}$$

$$\text{Height X/2} = \frac{\text{150 meters}}{\text{Frequency in MHz}} \quad \text{or} \quad \frac{\text{492 feet}}{\text{Frequency in MHz}}$$

Use the right relationship for the right purpose. If the height relationship is used for the dipole length, the antenna will be too long and will not work properly. Characteristics are—

Frequency range:	± 2% of design frequency
Polarization:	Horizontal
Power capability:	1,000 watts
Radiation Pattern	
Azimuthal (bearing):	Bidirectional λ/2 high basically omnidirectional at λ/4 high
Vertical (takeoff angle):	See figures 4-11 and 4-12 on page 4-17, and 4-13 on page 4-19

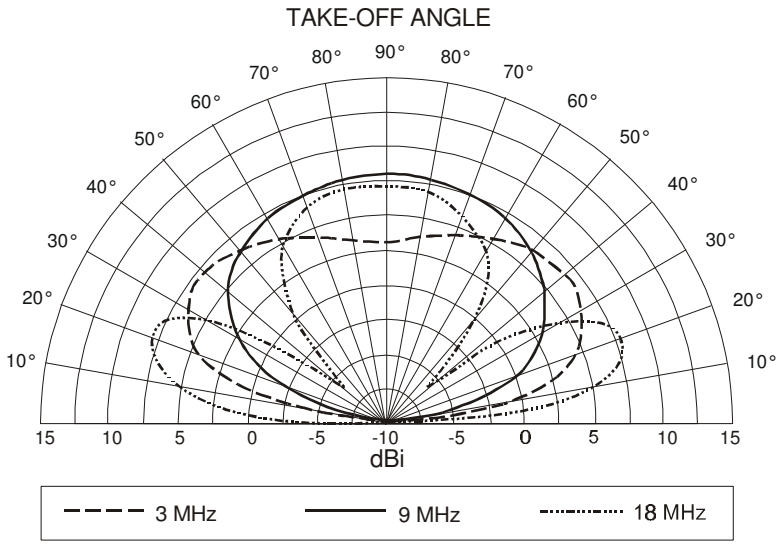


Figure 4-13. 12-Meter Half-Wave Dipole (Vertical Pattern).

Inverted Vee

The inverted vee, or drooping dipole, is similar to a dipole but uses only a single center support (see fig. 4-14 on page 4-20). Like a dipole, it is designed and cut for a specific frequency and has a bandwidth of 2 percent above or below the design frequency. Because of the inclined sides, the inverted vee antenna produces a combination of horizontal and vertical radiation—vertical off the ends and horizontal broadside to the antenna. All the construction factors for a dipole also apply for the inverted vee. The inverted vee has less gain than a dipole, but using only a single support could make this antenna the preferred antenna in some tactical situations (see fig. 4-15 on page 4-21).

Characteristics are—

Frequency range:	**± 2% of design frequency**
Polarization:	**Horizontal**
Power capability:	**1,000 watts**
Radiation pattern	
Azimuthal (bearing):	**Basically omnidirectional with combination polarization**
Vertical (take-off angle):	**See figure 4-15**

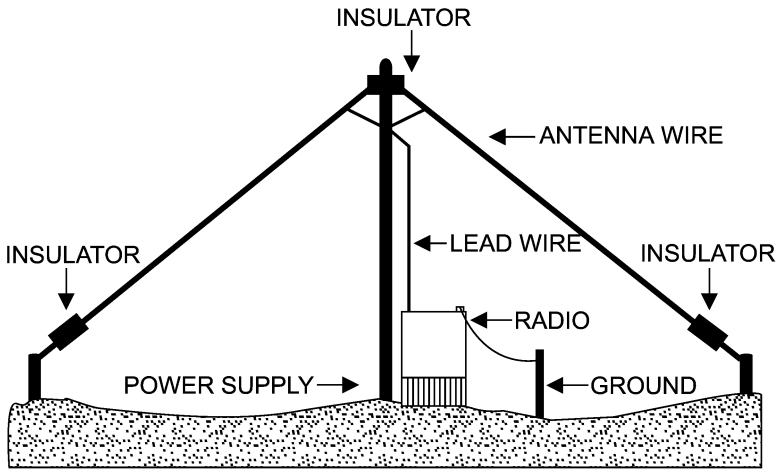


Figure 4-14. Inverted Vee Antenna.

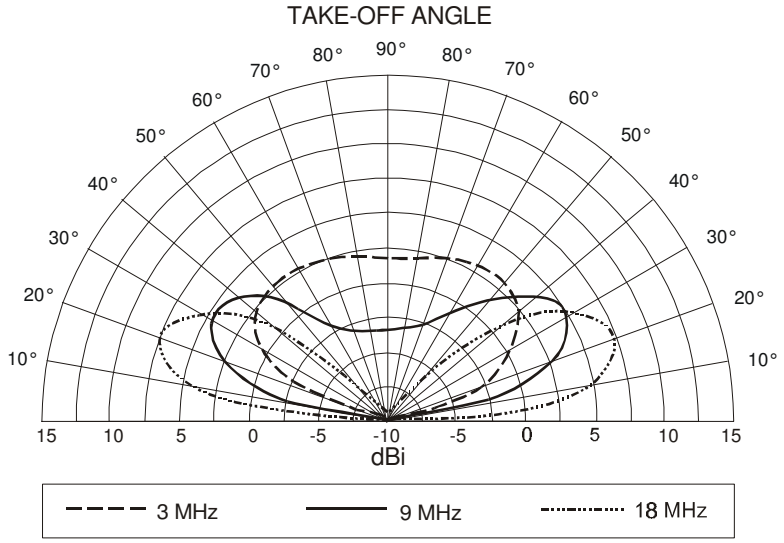


Figure 4-15. Inverted Vee (Vertical Pattern).

Long Wire

A long wire antenna is one that is long compared to a wavelength (see fig. 4-16 on page 4-22). A minimum length is one-half wavelength. However, antennas that are at least several wavelengths long are needed to obtain good gain and directional characteristics. Constructing long wire antennas is simple, and there are no critical dimensions or adjustments. A long wire antenna will accept power

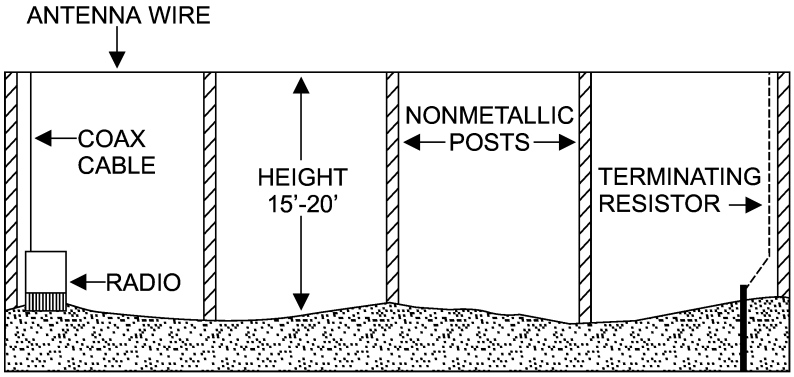


Figure 4-16. Long Wire Antenna.

and radiate it well on any frequency for which its overall length is not less than one-half wavelength.

The gain and take-off angle of a long wire antenna depend on the antenna's length. The longer the antenna, the more gain, and the lower the take-off angle. Gain has a simple relationship to length; however, take-off angle is a bit more complicated. A long wire antenna radiates a cone of energy around the tie wire, much like a funnel with the antenna wire passing through the funnel opening. The narrow part of the funnel would be the feed point, and the open part would be toward the distant station. If the funnel were cut in half, the resulting half cone would represent the pattern of the antenna. As the antenna is lengthened, the cone of radiation (funnel) moves closer and closer to the wire. Figure 4-17 shows pattern

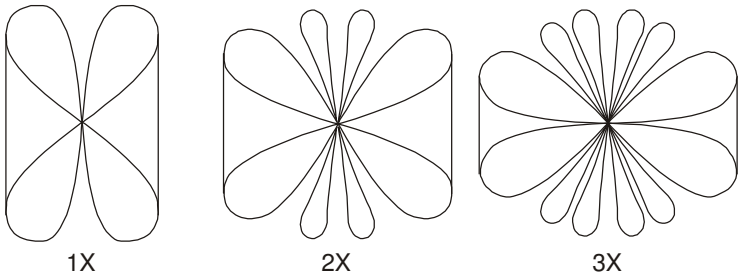


Figure 4-17. Long Wire Radiation Patterns.

changes as the wire is lengthened. The patterns represent a view from directly below the antenna.

In the three-wavelength pattern, for very low-angle radiation, position the wire somewhat away from the direction of the distant station so that the main lobe of radiation points at the receiving station. If a higher take-off angle is required, point the wire directly at the distant station. For take-off angles from 5 to 25 feet, the following general off-axis angles will provide satisfactory radiation on toward the distant station (see table 4-4).

Table 4-4. Off-Axis Angle.

Wire Length (Feet)	2	3	4	5	6
Off-Axis Angle (Degrees)	30	20	13	10	10

To make a long wire antenna directional, place a terminating device at the distant station end of the antenna. The terminating device should be a 600-ohm, noninductive resistor capable of absorbing at

least one-half of the transmitter power. Terminating resistors are components of some radio sets but can also be fabricated locally using supply system components (100-watt, 106-ohm resistor).

Constructing a long wire antenna requires only wire, support poles, insulators, and a terminating resistor (if directionality is desired). The only requirement is that the antenna be strung in as straight a line as the situation permits. The antenna is only 15 to 20 feet above ground, so tall support structures are not required. The antenna is normally fed through a coupler that can match the antenna's 600-ohm impedance. Coaxial cable can be used if a 12 to 1 balun is available to convert the coaxial cable 50-ohm impedance to the required 600 ohms. Vertical radiation plots of this antenna are not presented because of the great variation in the pattern as the length changes. For take-off angles between 5 and 25 feet, use the off-axis graph (table 4-4 on page 4-23) and the gain versus length graph (table 4-5) to determine the proper antenna length. Characteristics are—

Frequency range:	2 to 30 MHz
Polarization:	Vertical
Power capability:	1,000 watts
Radiation pattern	
Azimuthal (bearing):	Bidirectional with terminating resistor
Vertical (take-off angle):	Depends on length

Inverted L

The inverted L is a combination antenna made up of a vertical section and a horizontal section (see fig. 4-18). It provides omnidirectional radiation for ground wave propagation from the vertical element and high-angle radiation from the horizontal element for short-range sky wave propagation. The classic inverted L has a quarter-wave vertical section and a half-wave horizontal section

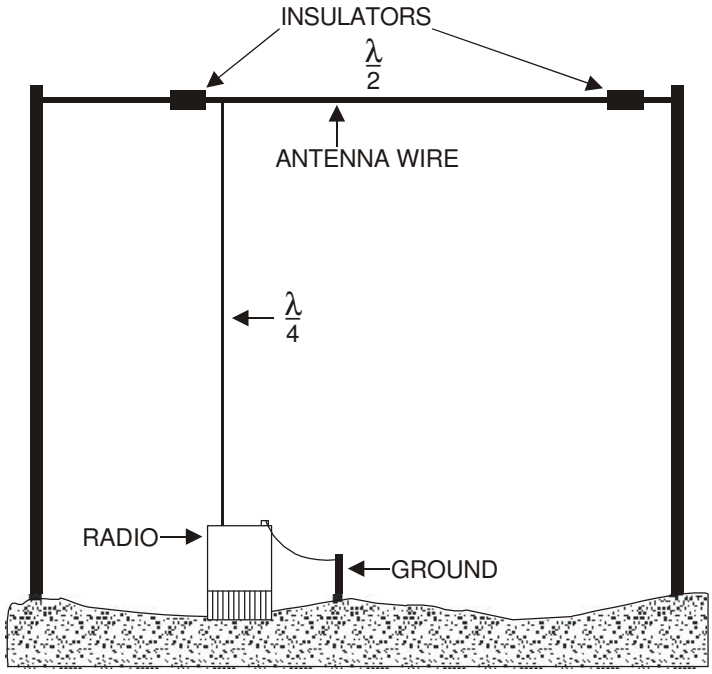


Figure 4-18. Inverted L Antenna.

and is used for a very narrow range of frequencies. By using the antenna couplers that are part of many radio sets, the dimensions of the inverted L can be modified to allow ground wave and short-range sky wave propagation over a range of frequencies. Using a vertical height of 35 to 40 feet, the following horizontal lengths will give reasonable performance for short-range sky wave circuits.

Table 4-5. Gain Versus Length.

Frequency Range (MHz)	2.5 to 4.0	3.5 to 6.0	5.0 to 7.0
Horizontal Length (Feet)	150	100	80

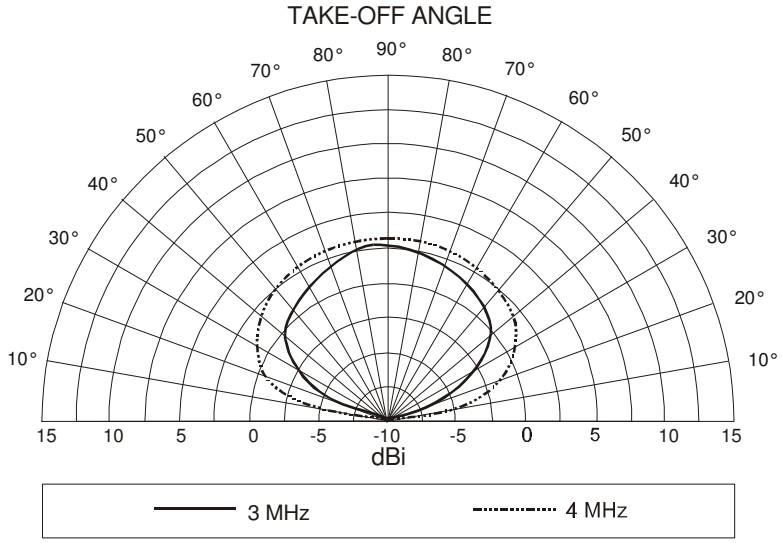


Figure 4-19. 40-Foot Inverted L (Vertical Pattern), 150 Feet Long.

Orient the antenna like a dipole (i.e., the broad side of the antenna should be toward the distant station). These lengths should not be used outside the frequency ranges specified because the antenna radiation pattern changes, and for frequencies much removed from the range, the antenna will become directional off the wire end. (See the sloping wire paragraphs on page 4-34 for using this directional characteristic.) The inverted L antenna can be used as a substitute for the dipole; however, it has less gain than a dipole, and its radiation pattern varies with frequency (unlike a dipole). Figures 4-19,

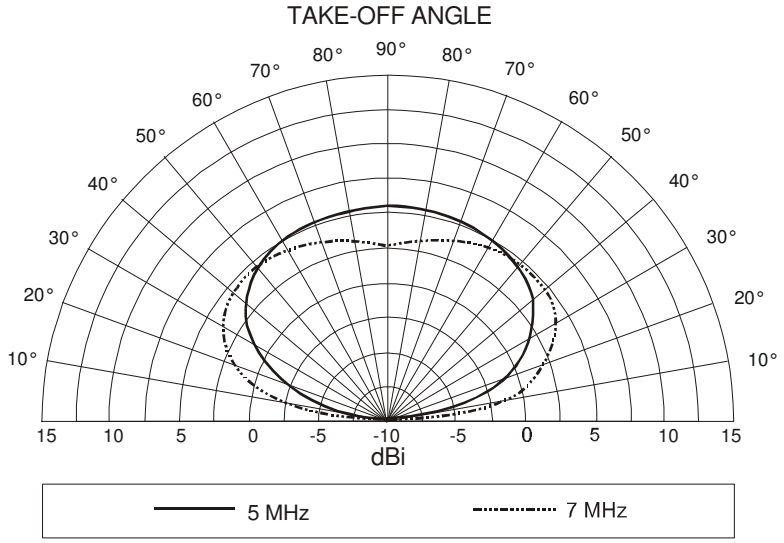


Figure 4-20. 40-Foot Inverted L Antenna (Vertical Pattern), 80 Feet Long.

4-20, and 4-21 on page 4-28 illustrate vertical patterns of various inverted L antennas. Characteristics are—

Frequency range:	**Less than 2:1 over design frequency**
Polarization:	**Vertical from vertical section** **Horizontal from horizontal section**
Power capability:	**1,000 watts**
Radiation pattern	
Azimuthal (bearing):	**Omnidirectional**
Vertical (take-off angle):	**See figures 4-19, 4-20, and 4-21 on page 4-28**

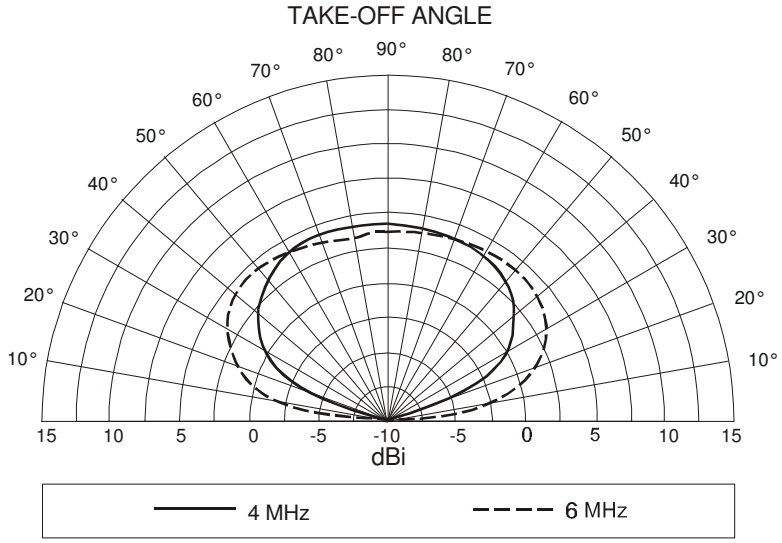


Figure 4-21. 40-Foot Inverted L (Vertical Pattern), 100 Feet Long.

Sloping Vee

The sloping vee is a medium- to long-range sky wave antenna that is simple to construct in the field. Antenna gain and directivity depend on the leg length. For reasonable performance, the antenna

should be at least one wavelength long, but preferably several wavelengths long (see fig. 4-22).

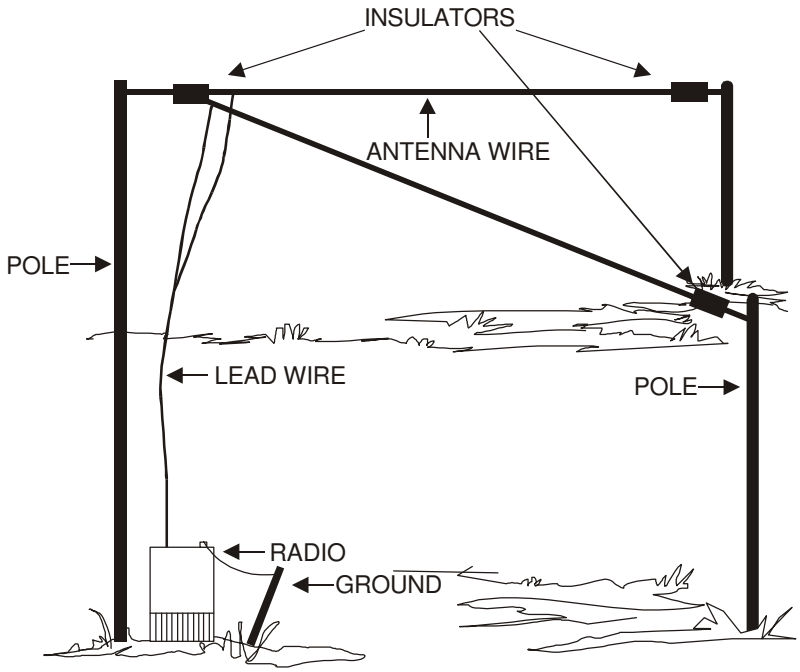


Figure 4-22. Sloping Vee Antenna.

A compromise tactical sloping vee can be constructed using 500-foot legs and a 40-foot support mast. The angle between the two legs is adjusted to provide maximum radiation at the desired take-off angle. Table 4-6 shows the angles between legs (apex angle) that will give poor results for the distances indicated.

Table 4-6. Angle Between Antenna Legs for Poor Results.

Path Length (Miles)	700 to 1000	1000 to 1500	over 1500
Apex Angle (Degrees)	60	45	30

To make the antenna directional, use terminating resistors on each leg on the open part of the vee. The terminating resistors should be 300 ohms and be capable of handling one-half of the transmitter's power output. These terminations are either procured or fabricated locally using supply system parts (100-watt, 106-ohm resistor). Using the terminating resistors, the antenna is aimed so that the line cutting the vee in half is pointed at the distant station.

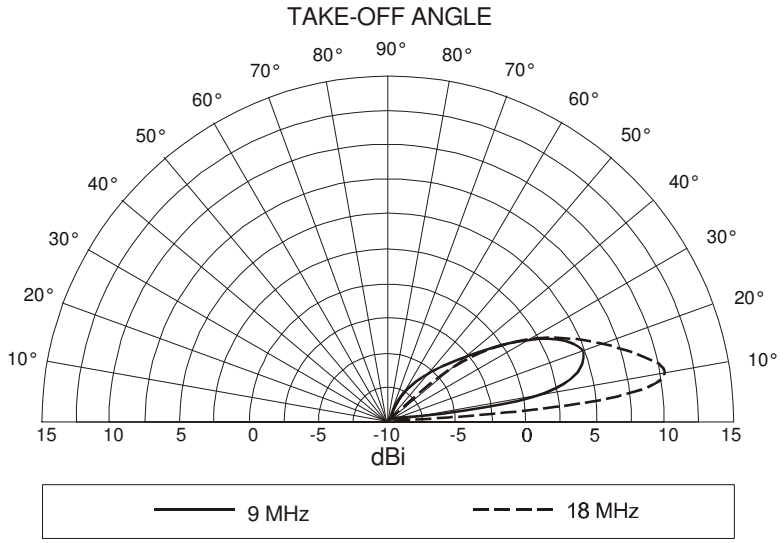


Figure 4-23. 40-Foot Sloping Vee (Vertical Pattern), 500 Feet Long, 30° Apex Angle.

The sloping vee is normally fed with a 600-ohm, open-wire feed line. One side of the feed line is connected to one leg with the other side connected to the other leg. The open-wire feed line can be connected to a 12 to 1 balun, which is then connected to standard coaxial cable. Figures 4-23, 4-24 on page 4-32, and 4-25 on page 4-33 illustrate the vertical patterns for various sloping vee antennas.

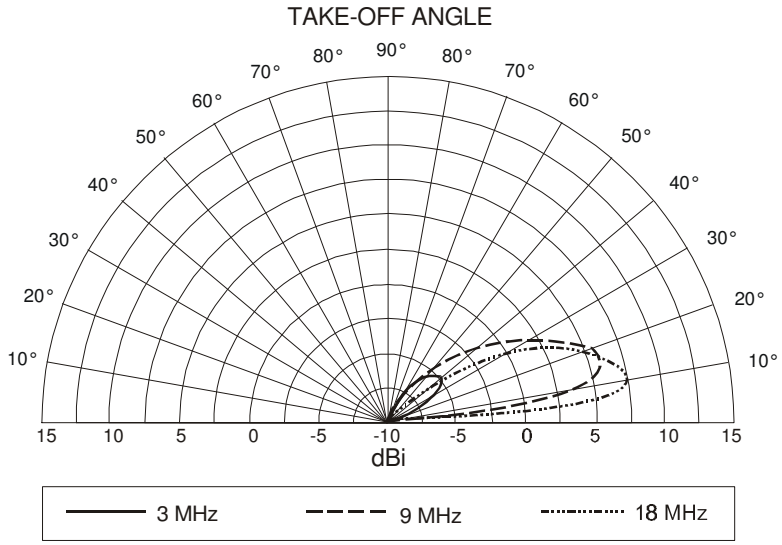


Figure 4-24. 40-Foot Sloping Vee Antenna (Vertical Pattern), 500 Feet Long, 45° Apex Angle.

Characteristics are—

Frequency range:	**3 to 30 MHz**
Polarization:	**Horizontal**
Power capability:	**Depends on terminating resistors**
Radiation pattern	
Azimuthal (bearing):	**Directional (20° either side of direction of radiation)**
Vertical (takeoff angle):	**See Figures 4-23, 4-24 on page 4-32, and 4-25 on page 4-33**

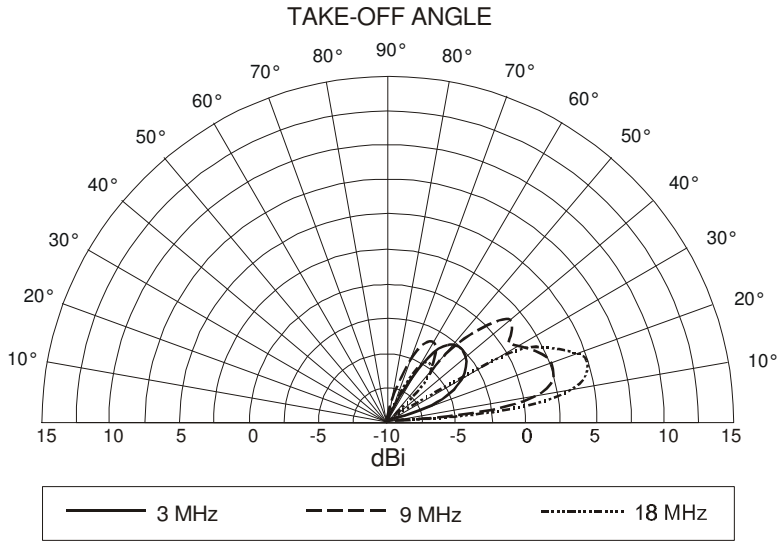


Figure 4-25. 40-Foot Sloping Vee Antenna (Vertical Pattern), 500 Feet Long, 60° Apex Angle.

Sloping Wire

The sloping wire antenna is simple and easy to construct. It requires only one support (see fig. 4-26 on page 4-34). A version of the long wire antenna, the sloping wire produces best results when it is long compared to a wavelength. Tactical sloping wires vary in length from 45 to over 500 feet. The shorter lengths perform rather poorly and should be used only when no other antenna can be erected. The

longer lengths (e.g., 250 feet, 500 feet) can produce good radiation for medium to long sky wave paths.

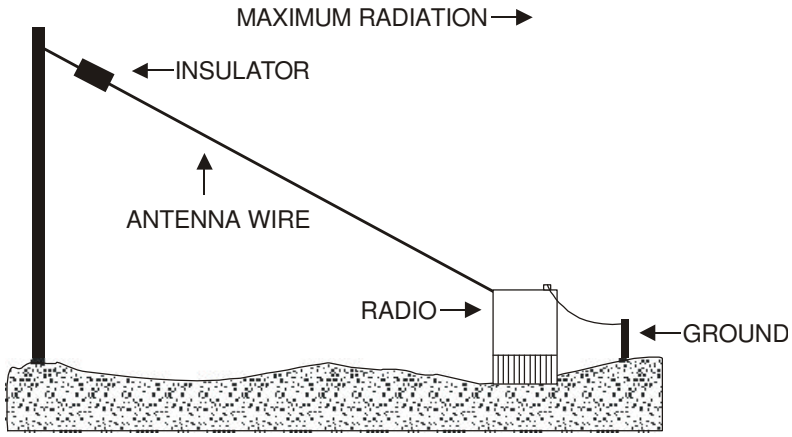


Figure 4-26. Sloping Wire.

A sloping wire can be either terminated or unterminated. If available, use 600-ohm termination because this makes the antenna impedance fairly constant, and a balun can be used to match the antenna to a transmitter. If the antenna is unterminated, use a coupler to match the transmitter to the antenna.

The low end of the wire should be oriened toward the receiving station. If the wire is unterminated, feed the antenna at the low end. If a terminating resistor is used, feed the antenna low end. Figure 4-27 and figures 4-28 and 4-29 on page 4-36 illustrate the vertical patterns for various sloping wire antennas.

Characteristics are—

Frequency range:	**Depends on wire length/configuration**
Polarization:	**Vertical**
Power capability:	**Determined by terminating resistor**
Radiation pattern	
Azimuthal (bearing):	**Bidirectional for unterminated** **Directional for terminated**
Vertical (take-off angle):	**See figure 4-27 and figures 4-28 and 4-29 on page 4-36**

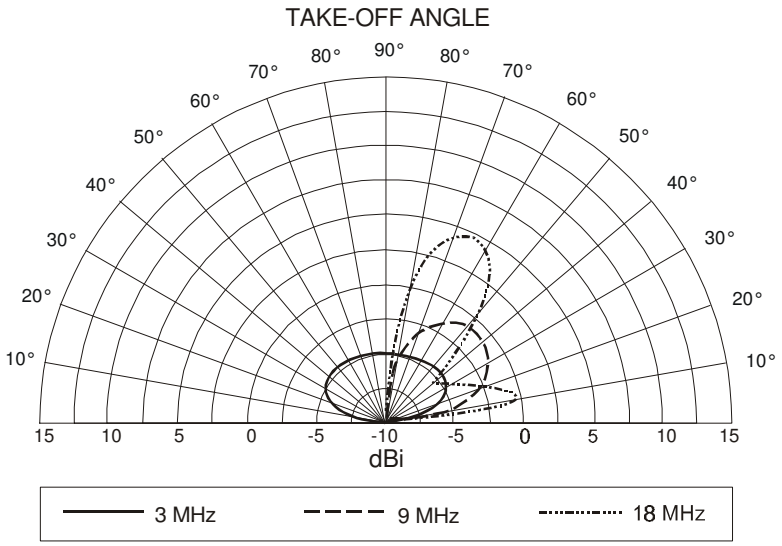


Figure 4-27. 100-Foot Sloping Wire (Vertical Pattern).

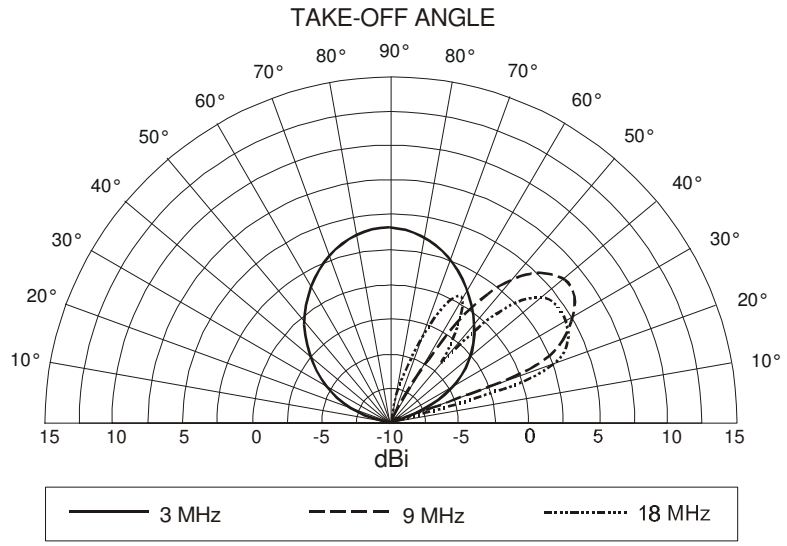


Figure 4-28. 250-Foot Sloping Wire (Vertical Pattern).

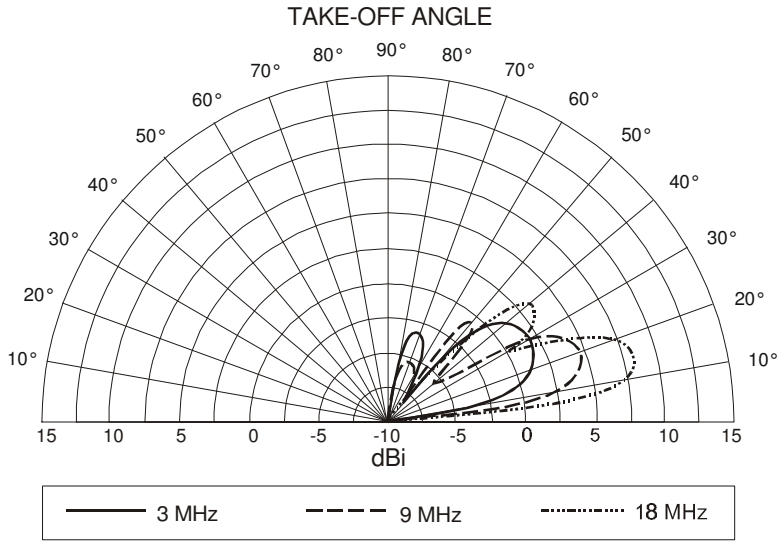


Figure 4-29. 234-Foot Sloping Wire (Vertical Pattern).

Vertical Half-Rhombic

The vertical half-rhombic antenna is a version of the long wire antenna that uses a single center support (see fig. 4-30). Easily constructed, this antenna has a narrow width (as wide as the center support guys), which allows several to be installed in a relatively narrow area. The vertical half-rhombic antenna radiates a medium- to low-angle signal, making it a good choice for medium- to long-range sky wave circuits. Normally, the 500-foot version is the maximum length of antenna that most tactical situations will allow; however, the vertical radiation pattern for a 1,000-foot version is included, so that if the opportunity exists, the antenna can be used for excellent results.

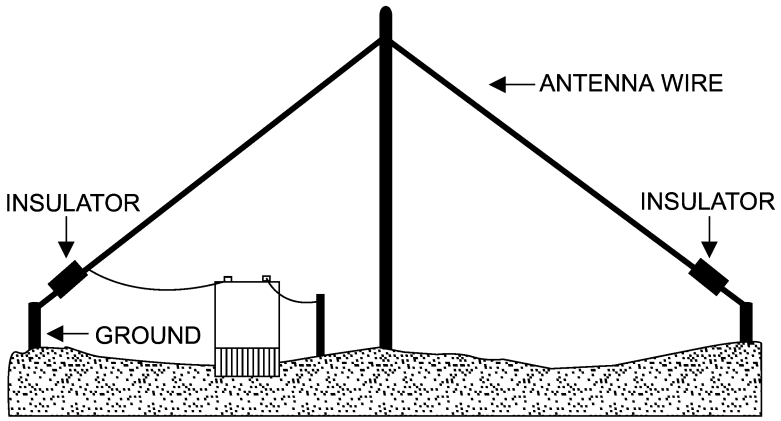


Figure 4-30. Vertical Half-Rhombic Antenna.

The vertical half-rhombic uses a single wire feed either through a coupler or a balun (12 to 1). One of the two terminals of the coupler or balun is attached to the antenna, while the other terminal is grounded. Like other terminated antennas, the terminating resistor (600 ohms) should be able to handle one-half of the transmitter's power output. Terminators can be procured or fabricated locally (100-watt, 106-ohm resistor).

The orientation of this antenna depends on the frequency bands being worked. Below 12 MHz, point the terminated end of the antenna at the distant station; above 12 MHz, aim the antenna 10 feet to either side of the distant station. Figures 4-31 and 4-32 illustrate the vertical patterns for various vertical half-rhombic antennas. Characteristics are—

Frequency range:	**2 to 30 MHz**
Polarization:	**Vertical**
Power capability:	**Determined by terminating resistor**
Radiation pattern	
Azimuthal (bearing):	**Directional**
Vertical (take-off angle):	**See Figures 4-31 and 4-32**

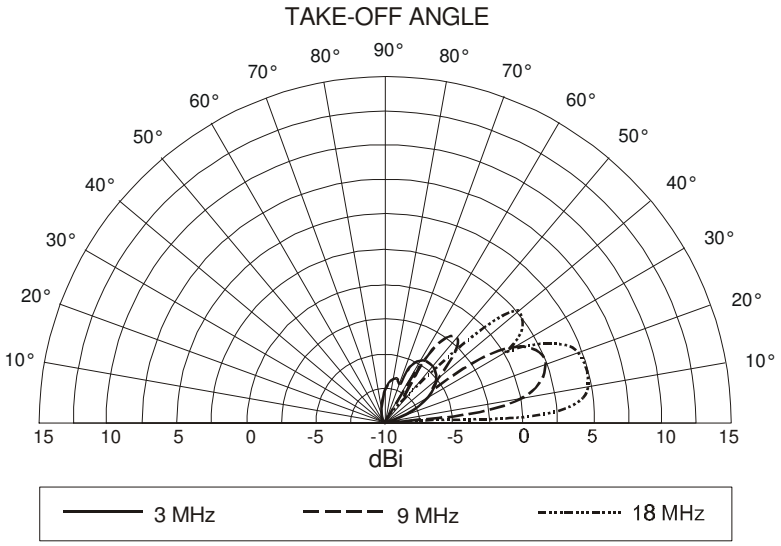


Figure 4-31. 50-Foot Vertical Half-Rhombic (Vertical Pattern), 500 Feet Long.

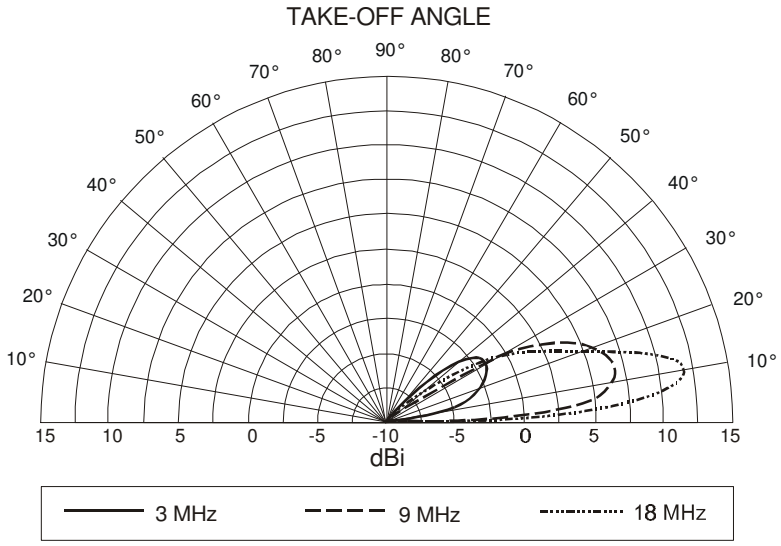


Figure 4-32. 50-Foot Vertical Half-Rhombic (Vertical Pattern), 1,000 Feet Long.

HF NVIS COMMUNICATIONS

NVIS propagation is simply sky wave propagation that uses antennas with high-angle radiation and low operating frequencies. Just as the proper selection of antennas can increase the reliability of a long- range circuit, short-range communications also require proper antenna selection. NVIS propagation is one more weapon in the communicator's arsenal.

To communicate over the horizon to an amphibious ship on the move, or to a station 100 to 300 kilometers away, the operators should use NVIS propagation. The ship's low take-off angle antenna is designed for medium and long-range communications. When the ship's antenna is used, a skip zone is formed. This skip zone is the area between the maximum ground wave distance and the shortest sky wave distance where no communications are possible. Depending on operating frequencies, antennas, and propagation conditions, this skip zone can start at roughly 20 to 30 kilometers and extend out to several hundred kilometers, preventing communications with the desired station.

NVIS propagation uses high take-off angle (60° to 90°) antennas to radiate the signal almost straight up. The signal is then reflected from the ionosphere and returns to Earth in a circular pattern all around the transmitter. Because of the near-vertical radiation angle, there is no skip zone. Communications are continuous out to several hundred kilometers from the transmitter. The nearly vertical angle of radiation also means that lower frequencies must be used. Generally, NVIS propagation uses frequencies up to 8 MHz.

The steep up and down propagation of the signal gives the operator the ability to communicate over nearby ridge lines, mountains, and dense vegetation. A valley location may give the operator terrain shielding from hostile intercept and also protect the circuit from

ground wave and long-range sky wave interference. Antennas used for NVIS propagation need good high take-off angle radiation with very little ground wave radiation (see fig. 4-33).

Using the HF antenna selection matrix (table 4-4 on page 4-8), the AS-2259/GR and half-wave dipole are the only antennas listed that meet the requirements of NVIS propagation. While the inverted vee and inverted L antennas have high-angle radiation, they also can have strong ground wave radiation that could interfere with the close-in NVIS communications. These antennas could be used if terrain shielding prevented the ground wave signal from propagating to the distant station.

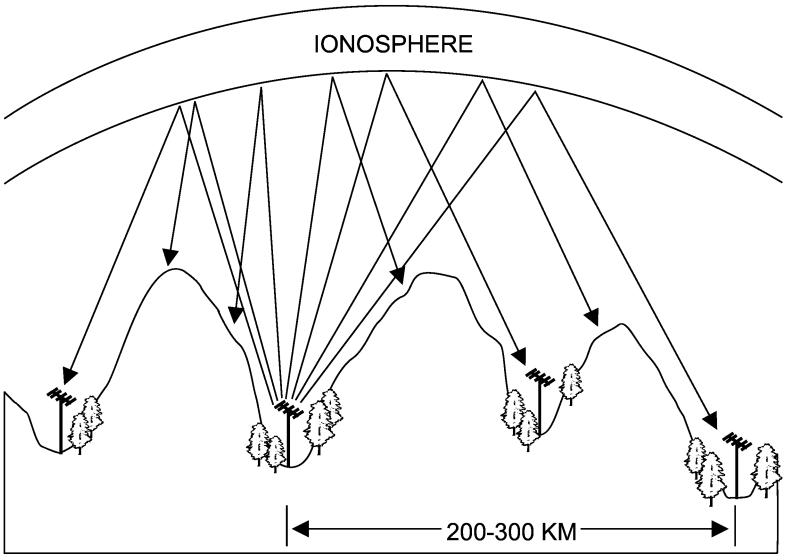


Figure 4-33. NVIS Propagation.

The dipole antenna pattern is illustrated in figures 4-11 and 4-12 on page 4-17 and figure 4-13 on page 4-19. The patterns for 3 and 9 MHz show that large amounts of energy are directed up in the 60° to 90° range. Also, the pattern is the same on both sides of the 90° line. This means that a low dipole would be a good antenna for NVIS propagation. The pattern at 18 MHz is not important because NVIS propagation normally does not use frequencies much above 8 MHz. Set up dipoles on whatever supports are available. Ensure that the height is below a quarter-wavelength, which at 8 MHz is about 30 feet.

Mobile CPs do not always have time to set up a dipole antenna or an AS-2259/GR. Several options are possible. If a Marine is in an MRC-138 vehicle, then use a tilt whip adapter and the 16-foot whip antenna to try to obtain high-angle radiation (fig. 4-34). Tilt the antenna at least 30°. Another option is disconnecting the whip antenna and connecting a 32-foot wire to the antenna base. Run the wire parallel to the ground, and stake it at the distant end the same height above the ground as the radio end. Insulate the staked end from the ground to prevent radio damage (fig 4-35).

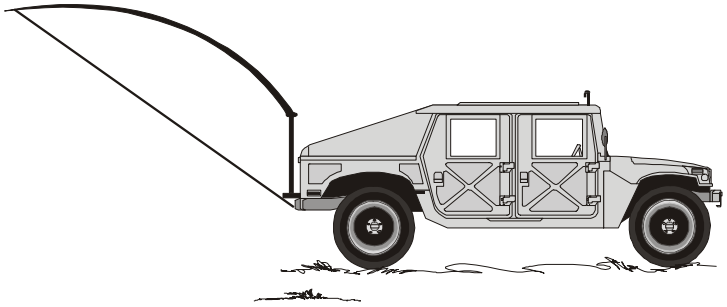


Figure 4-34. AN/MRC-138 with NVIS Antenna.

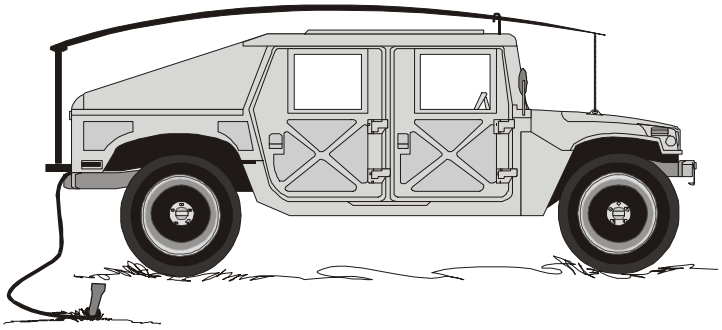


Figure 4-35. AN/MRC-138 with Stationary NVIS Antenna.

WARNING

THE WIRE MUST BE PROTECTED SO THAT MARINES DO NOT WALK INTO IT. IT CARRIES ENOUGH RF ENERGY DURING TRANSMISSION TO CAUSE SEVERE INJURIES.

When using a manpack radio like the AN\PRC-104, the whole radio can be rotated so that the 8-foot antenna is tilted at least 30°. Because of the antenna's flexibility, it will need support on the far end. This support must be a good insulator. Ensure that Marines keep clear of the antenna. Characteristics are—

Frequency range:	**2 to 30 MHz**
Polarization:	**Vertical or horizontal**
Power capability:	**100 to 400 Watts**
Radiation pattern	
Azimuthal (bearing):	**Basically omnidirectional**
Vertical (take-off angle):	**Minimizes skip zone using 90°, 40°, and 20° take-off angle**

(reverse blank)

Chapter 5

VHF and UHF Antenna Selection

FREQUENCIES

The VHF portion of the radio spectrum extends from 30 to 300 MHz. The UHF range reaches from 300 to 3,000 MHz (3 GHz). Both frequency ranges are extremely useful for short-range (less than 50 km) communications. This includes point-to-point, mobile, air-to-ground, and general purpose communications. A wavelength at these frequency ranges is considerably shorter than those in the HF range, and simple antennas are much smaller.

Because the VHF and UHF antennas are small, it is possible to use multiple radiating elements to form arrays, which provide a considerable gain in a given direction or directions. An array is an arrangement of antenna elements, usually dipoles, used to control the direction in which most of the antenna's power is radiated.

Generally, many more types of antennas are available and useful in the VHF and UHF range than at HF. Several of these types will be discussed in this chapter since they are useful for various field applications.

Within the VHF and UHF portion of the spectrum, there are several subfrequency bands for specific uses. The 118 to 136 MHz range is generally reserved on a worldwide basis for air-to-ground communications and is known as the VHF aircraft band. The 225 to 400 MHz range is also allocated for air-to-ground use and is known as the UHF aircraft band. The 148 to 174 MHz and 450 to 470 MHz

ranges are assigned to many activities, including citizens (public) communications (e.g., mobile, police, weather, taxis, and general purpose).

POLARIZATION

In many countries, FM and TV broadcasting in the VHF range use horizontal polarization. One reason is because it reduces ignition interference, which is mainly vertically polarized. Mobile communications often use vertical polarization for two reasons. First, the vehicle antenna installation has physical limitations, and second, so that reception or transmission will not be interrupted as the vehicle changes its heading to achieve omnidirectionality.

Using directional antennas and horizontal polarization (when possible) will reduce manmade noise interference in urban locations. Horizontal polarization, however, should be chosen only where an antenna height of many wavelengths is possible. Ground reflections tend to cancel horizontally polarized waves at low angles. Use only vertically polarized antennas when the antenna must be located at a height of less than about 10 meters above ground, or where omnidirectional radiation or reception is desired.

GAIN AND DIRECTIVITY

VHF and UHF (above 30 MHz) antenna gain and directivity are extremely important for several reasons. Assuming the same antenna gain and propagation path, the received signal strength drops as frequency is increased. At VHF and UHF, more of the received signal is lost in the transmission line than is lost at HF. A 10 to 20 dB loss is not uncommon in a 30 meter length of coaxial line at 450 MHz.

At frequencies below 30 MHz, system sensitivity is almost always limited by receiver noise rather than by noise external to the antenna (e.g., atmospheric and manmade interference). Generally, wider modulation or signal bandwidths are employed in VHF and UHF transmissions than at HF. Since system noise power is directly proportional to bandwidth, additional antenna gain is necessary to preserve a usable S/N ratio.

VHF and UHF antenna directivity (gain) aids security by restricting the amount of power radiated in unwanted directions. Receiver sensitivity is generally poorer at VHF and UHF (with the exception of high quality state-of-the-art receivers). Obstructions (e.g., buildings, trees, hills) may seriously decrease the signal strength available to the receiving antenna because VHF and UHF signals travel a straight LOS path.

Gain

Obtaining communications reliability over difficult VHF and UHF propagation paths requires considerable attention to the design of high-gain, directive antenna arrays at least at one end of the communications link. Unlike HF communications, the shorter VHF and UHF wavelengths support walkie-talkie transceivers and simple mobile transmission units. Communicating or receiving with such devices over distances beyond 1 or 2 km requires maximum antenna gain at the base station site or fixed end of the link.

Directivity

Because VHF and UHF wavelengths are so short, reliable prediction of diffraction, refraction, and reflection effects are not practical. One must depend entirely on LOS paths. For best results, attempt to establish VHF and UHF communications paths that are as free of obstacles as possible. The VHF and UHF wavelengths are

short enough that it is possible to construct resonant antenna arrays. An array provides directivity (the ability to concentrate radiated energy into a beam that can be aimed at the intended receiver). Arrays of resonant elements, (e.g., half-wave dipoles), can be constructed of rigid metal rods or tubing or of aluminum or copper foil laid out or pasted on a flat nonconducting surface. Directing power helps to increase the range of the communications path and tends to decrease the likelihood of interception or jamming from hostile radio stations. However, such highly directive antennas place an added burden on the operator to ensure that the antenna is pointed properly.

TRANSMISSION LINES

Choosing transmission lines at VHF and UHF depends on many factors. Generally, twin-lead has much lower loss than small diameter coaxial cable. Twin-lead is preferred over coaxial when transmission line lengths exceed 10 meters. Twin-lead is much more susceptible to picking up objectionable manmade noise than is well shielded coaxial cable. Also, most modern VHF and UHF equipment employs unbalanced input and output circuitry with a 50-ohm impedance. Such equipment requires either using coaxial cable or a balun to feed a twin-lead or two-wire balanced transmission line. Noise pickup by twin-lead transmission lines may be considerably reduced by twisting the line along its length.

When using twin-lead, the spacing between the wires of the line should not exceed 0.05 λ. If the spacing is an appreciable part of a wavelength, the line will radiate and receive energy like the antenna. This effect will alter the intended antenna radiation pattern. To further reduce local noise pickup, keeping twin-lead clear of metal objects (e.g., gutters and window frames). Twice the wire spacing in the twin-lead is sufficient clearance.

RADIATORS

A radiator is the antenna component that transmits RF energy.

Vertical Radiator

A vertical radiator for general coverage use at UHF should be one-quarter wavelength long. Longer vertical antennas do not have their maximum radiation at right angles to the line of the radiator. They are not practical for use where the greatest possible radiation parallel to the Earth is desired. It is important that the antenna be decoupled from the coaxial transmission line. This will prevent unwanted radiation currents from flowing along the outside of the cable, which will distort the antenna pattern. Use a sleeve, ground plane, or counterpoise to perform decoupling.

Cross Section Radiator

Aluminum tubing is commonly used for dipoles and radiation elements. They are so short that the expense of larger diameter conductors is relatively low. With such conductors, the antenna will tune much more broadly. This is very desirable, particularly when an antenna or array is used over an entire frequency band.

Large cross section radiators have a shorter resonant length than a radiator or mode of small diameter wire. A tubing radiator mode is seldom longer than 90 percent of a half-wavelength for a dipole at frequencies above 100 MHz.

INSULATION

Insulation or dielectric material quality is more important at VHF and UHF than at frequencies below 30 MHz. Many insulators that perform well in the HF range are poor or unusable for fabricating

antennas operating at frequencies above 100 MHz. Ordinary wood is a good example. In minimal rainfall climates, using very dry redwood, maple, or fir boiled in paraffin wax for several hours is fairly successful up to frequencies as high as 560 MHz. The neck of a glass soft drink bottle or other similar items work reasonably well up to frequencies as high as 1 GHz. Several modern plastics, used throughout the world, also make excellent insulators (e.g., fiberglass, polystyrine, polyethylene, and Styrofoam). Pieces of these plastics in usable shapes can be found almost everywhere, and, with a little ingenuity, can be used as insulation in the design of many VHF and UHF antennas. Avoiding insulation entirely is possible by choosing an antenna design with elements supported at lower voltage (high current) points (e.g., the Yagi antenna).

INTERFERENCE

Obtaining optimum coupling between the antenna and transmission line and between the transmission line and the receiver or transmitter circuits is a major concern.

Noise

While atmospheric and manmade noise usually limit the ultimate sensitivity of an HF receiving system, a VHF or UHF receiving system is almost always limited by receiver noise. External (atmospheric) noise is virtually nonexistent at frequencies higher than 100 MHz. Automobile ignition and other forms of manmade static affect frequencies well into the UHF band.

Multipath Interference

VHF and UHF radio waves are highly attenuated when they travel through most materials. Select a location which is as free as possible of obstacles in the direction of desired propagation. It is possible

to use relay stations or carefully placed reflectors when obstacles interfere with the direct path.

When operating from areas where the transmission path is bounded rather closely by reflective objects (e.g., buildings or metal towers) the possibility of multipath exists. Whenever conditions are such that radio signals travel two or more separate paths from the transmitting to the receiving antenna, a phenomenon known as an interference pattern is created around the receiving antenna. There will be zones where the incoming signal is received very strongly (constructive interference) with areas of weak signal between (destructive interference). If each of the two signal has the same strength, complete cancellation will occur in the destructive interference zones, and no signal will be received. At VHF and UHF the created interference patterns are small enough to permit moving out of a destructive zone and into a constructive zone within the space of only a meter or so.

It is difficult to predict the location of an interference pattern. Optimizing antenna location is a must for good results. Sometimes a secondary path is created as the result of reflection from a moving object (e.g., an automobile or airplane). The resulting interference pattern will not be stationary, but will move past the antenna so that the received signal appears to flutter between good and poor reception. Multipath problems can be particularly severe when either the transmitting or receiving antenna is moving. Diversity techniques such as two separated antennas or circular polarization should help to alleviate the effects of multipath interference. High gain (highly directive) antennas, both on the transmitter and the receiver, can reduce signal loss from multipath interference.

Vegetated Areas

VHF and UHF communications through a dense forest over distances of more than a few kilometers can often be very difficult. In many tropical regions, trees and underbrush absorb VHF and UHF radio energy. In addition to the ordinary free space loss between transmitting and receiving antennas, a radio wave passing through a forest undergoes an additional loss that is measured in dBs per km. This extra loss increases rapidly as the transmission frequency increases.

Near the ground (i.e., antenna heights of less than 3 meters) vertical polarization is preferred. However, if it is possible to elevate both receiving and transmitting antennas as much as 10 to 20 meters, horizontal polarization is preferable to vertical polarization. Considerable reduction in total path loss results if either or both the transmitting and receiving antennas can be placed above the tree level through which communications must be made.

Increasing antenna gain may provide an improved signal strength that exceeds the added antenna gain by reducing the number of multipath reflections from trees along the propagation path. The higher gain antenna exhibits a much narrower radiation pattern which includes fewer trees in its beam. Generally, this effect is most noticeable with antenna gains higher than 15 dB or azimuthal half-power beam of less than 35°.

Communications through heavily forested areas over distances greater than 10 kms may require a transmitter power of at least 10 watts and antenna gains of 10 dB or more, depending on antenna height, terrain features, type of trees, moisture content, and numerous other factors. If communication is required over distances

exceeding 30 kms, it may be necessary to use high-angle ionospheric propagation in the 3 to 10 MHz frequency range (i.e., HF) to obtain a reliable circuit.

ANTENNA TYPES

The vertical whip is the most commonly used antenna. The OE-254 is a broadband, omnidirectional, biconical antenna. Antennas located in places which are enclosed mostly in a metal shell or container (e.g., an automobile) cannot be expected to perform as well as if located outside the enclosure. Most of the antenna types usable in the HF range are also usable in the VHF and UHF bands. In the VHF and UHF ranges, use the same antenna for transmitting and receiving.

Vertical Whip

It is easy to use and part of every radio set. In mobile situations, it is the only antenna that can be used. In stationary operations, the vertical whip is not a good choice. It cannot be elevated for good omnidirectional VHF LOS communications, and it radiates in useless directions if communications are point-to-point.

If the tactical situation prevents using an antenna other than the vertical whip, steps can be taken to improve its performance. Ensure that the antenna is vertical. This can be a problem when using the manpack short whip or tape in the prone position. Use the flexible base on the tape to ensure that the antenna is in a vertical position.

Place a reflector behind the whip to direct radiation in a general direction. A reflector is a vertical wire or another whip placed one-quarter wavelength behind the radiating whip. Place the reflector at the same height as the whip, and insulate it from the ground. The

reflector reflects some of the radio energy back towards the whip and provides a broad beam of energy towards the distant station. Characteristics are—

Frequency range:	30 to 88 MHz
Polarization:	Vertical
Power capability:	Matched to specific radio
Radiation pattern	
Azimuthal (bearing):	
Vertical (take-off angle):	

OE-254

The OE-254 (fig. 5-1) is scheduled to replace the RC-292. Unlike the RC-292, the OE-254 does not require tuning for specific bands and can cover the 30 to 87.975 MHz VHF band without adjustments. Three upward and three downward radial elements simulate two cones which provide omnidirectional VHF LOS radiation. The antenna is usually mounted on a 33-foot 8-inch mast for an overall height of 41 feet 9 inches. The antenna may be installed at lower heights; however, care should be taken to ensure that the lower and upper mast adapter assemblies are always used. An 80-foot coaxial cable comes with the antenna for direct connection to a radio.

Frequency range:	30 to 88 MHz
Polarization:	Vertical
Power capability:	350 watts
Radiation pattern	
Azimuthal (bearing):	Omnidirectional
Vertical (take-off angle):	

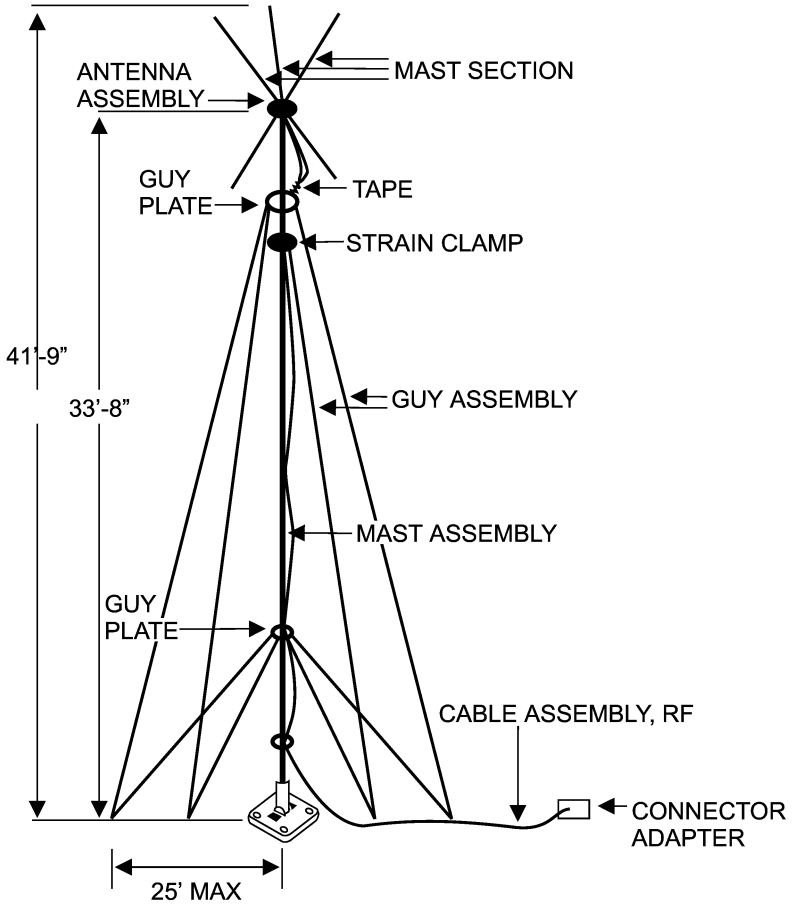


Figure 5-1. Installed OE-254 Antenna.

Antenna Within Vehicle Interior

Antennas located inside vehicles will lose some radiation through the window openings. It is difficult to predict how much radiation will escape or how much the original antenna radiation pattern will be affected by the enclosure. The pattern modification depends on the vehicle size and its openings and on the location of the antenna inside. Select antennas which operate above the cutoff frequency of the window openings. An opening in a metal container which is less than 0.5 λ in the dimension perpendicular to the plane of polarization will be severely attenuated or cutoff as it traverses the opening. Lower frequency waves will suffer even greater attenuation.

HF Antenna Types Usable at VHF and UHF

Simple vertical half-wave dipole and quarter-wave monopole antennas are very popular for omnidirectional transmission and reception over short-range distances. For longer distances, rhombic antennas made of wire and somewhat similar in design to HF versions may be used to good advantage at frequencies as high as 1 GHz. Another HF antenna, the Yagi, is equally popular in the VHF and UHF ranges. However, while Yagis with more than three or four elements are seldom used at HF, Yagi designs with as many as 15 elements, or more, are quite common at VHF and UHF.

Dual-Function Antennas

Because there is no sure method of accurately pointing a transmitting antenna, accomplish this task by first using the antenna in reception and orienting it for the best received signal. Positioning the antenna in this manner assures that, according to the reciprocity theorem, the antenna is optimally oriented for transmitting. If two-way communications are desired (i.e., transmitting and receiving alternately) a switch to toggle quickly back and forth between transmitter and receiver is required. Design the switch so that it will not

upset the impedance on the transmission line, causing unwanted received or transmitted power loss. When using coaxial cable as transmission line, use suitable, commercially available, low-loss coaxial antenna switching relays if possible.

In the 225 to 400 MHz and 450 to 470 MHz frequency ranges, most antennas are quite small. Mount two identical antennas, using one for transmitting and one for receiving. Separate transmission lines may then be used, eliminating the need for an antenna relay.

(reverse blank)

Chapter 6

Field Repair and Expedients

Antennas sometimes break or sustain damage, causing poor communications or communications failure. If a spare is available, use it to replace the damaged antenna. When there is no spare, construct an expedient antenna. The following paragraphs discuss antenna and support repair and constructing and adjusting expedient antennas.

REPAIR TECHNIQUES

Whip Antennas

A broken antenna (whip) can be repaired temporarily. If the whip is broken into two sections, rejoin the sections. Remove the paint and clean the sections where they will rejoin to ensure a good electrical connection. Place the sections together, secure them with a pole or branch, and lash them with bare wire or tape above and below the break (see fig. 6-1 (A) on page 6-2).

If the whip is badly damaged, use a length of field wire (WD1/TT) the same length as the original antenna. Remove the insulation from the lower end of the field wire antenna, twist the conductors together, stick them in the antenna base connector, and secure with a wooden block. Use either a pole or a tree to support the antenna wire (see fig. 6-1 (B) on page 6-2).

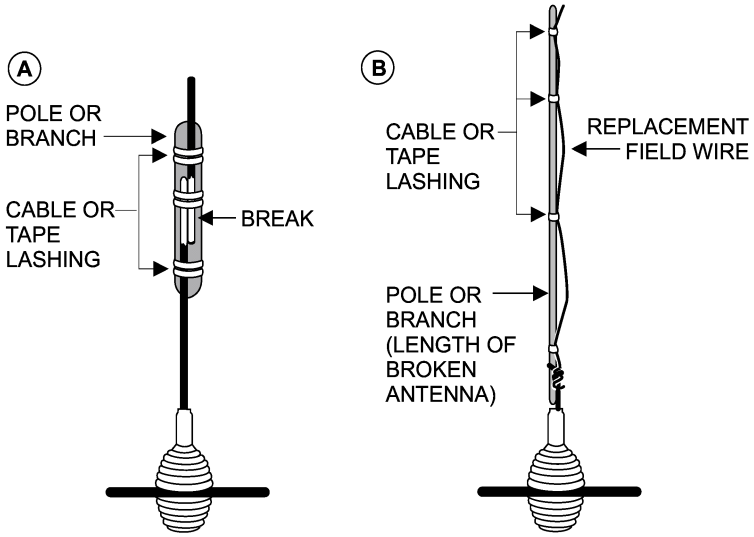


Figure 6-1. Emergency Repair of Broken Whip.

Wire Antennas

Expedient wire antenna repair may involve repairing or replacing the antenna or transmission line wire or repairing or replacing the assembly that supports the antenna. When one or more antenna wires are broken, repair the antenna by reconnecting the broken wires. Lower the antenna to the ground, clean the ends of the wires, and twist the wires together. Solder the connection if possible. If the antenna is damaged beyond repair, construct a new one. Make sure that the substitute wire is the same length as the original.

Antenna supports may also require repair or replacement. Use a substitute item in place of a damaged support. If properly insulated, any material of adequate strength can be used. If the radiating element is not properly insulated, field antennas may be shorted to ground and rendered ineffective. Many commonly found items can

be used as field expedient insulators (fig. 6-2). The best are plastic or glass, including plastic spoons, buttons, bottle necks, and plastic bags. Less effective than plastic or glass, but better than no insulators at all, are wood and rope, or both, in that order. The radiating element—the actual antenna wire—should touch only the antenna terminal and be physically separated from all other objects, other than the supporting insulator.

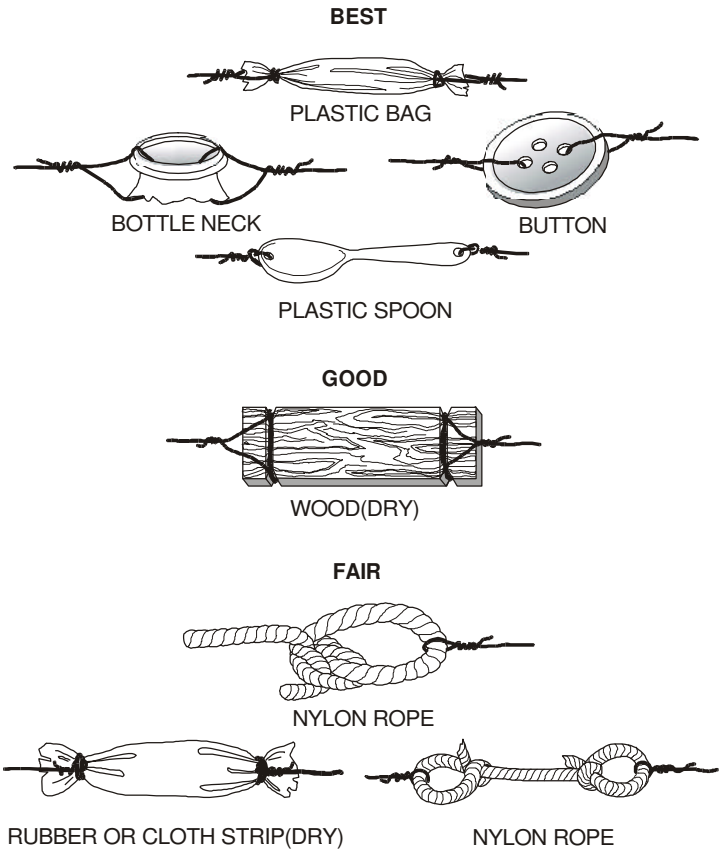


Figure 6-2. Improvised Insulators.

Guys

Lines used to stabilize antenna supports are called guys. These lines are usually wire, manila rope, or nylon rope. If a rope breaks, repair it by tying the two broken ends together. If the rope is too short after tying, lengthen it by adding another piece of rope or a piece of dry wood or cloth. If a guy wire breaks, replace it with another piece of wire. Figure 6-3 shows how to repair a guy line with a spoon.

Masts

Some antennas are supported by masts. If a mast breaks, replace it with another mast the same length. If long poles are not available, overlap short poles and lash them with rope or wire to provide a pole of the required length. Figure 6-3 shows how to make an expedient mast repair.

TIPS ON CONSTRUCTION AND ADJUSTMENT

Constructing the Antenna

The best kinds of wire for antennas are copper and aluminum. In an emergency, use any type that is available. The exact length of most antennas is critical. An expedient antenna should be the same length as the antenna it replaces.

Antennas supported by trees can usually survive heavy wind storms if the trunk of a tree or a strong branch is used as a support. To keep the antenna taut and to prevent it from breaking or stretching as the trees sway, attach a spring or old inner tube to one end of the antenna. Another technique is to pass a rope through a pulley or eyehook, attach the rope to the end of the antenna, and load the rope with a heavy weight to keep the antenna tightly drawn.

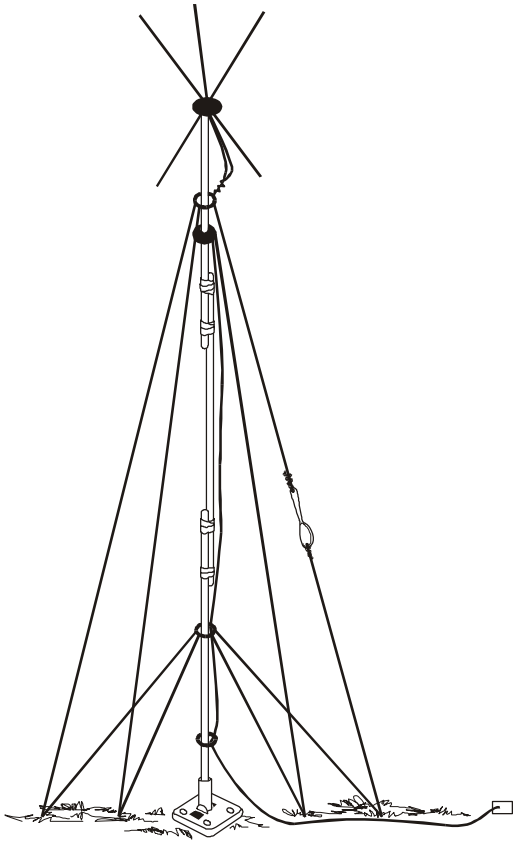


Figure 6-3. Repaired Guy Line and Mast.

Guys used to hold antenna supports are made of rope or wire. To ensure that wire guys will not affect antenna operation, cut the wire into several short lengths and connect the pieces with insulators.

Adjusting the Antenna

An improvised antenna may change a radio set's performance. Use the following methods to determine if the antenna is operating properly.

Use a distant station to test the antenna. If the signal received from this station is strong, the antenna is operating satisfactorily. If the signal is weak, adjust the antenna and transmission line height and length to receive the strongest signal at a given receiver volume control setting. This is the best method of tuning an antenna when transmission is dangerous or forbidden.

Most Marine Corps cadets use the transmitter to adjust the antenna. Set the transmitter controls in position for normal operation. Then, tune the system by adjusting the antenna height and length and the transmission line length to obtain the best transmission output.

WARNING

SERIOUS INJURY OR DEATH CAN RESULT FROM CONTACT WITH THE RADIATING ANTENNA OR MEDIUM- OR HIGH-POWER TRANSMITTER. TURN THE TRANSMITTER OFF WHILE MAKING ADJUSTMENTS TO THE ANTENNA.

Impedance-matching a load to its source is an important consideration in transmissions' systems. If the load and source are mismatched, part of the power is reflected back along the transmission line towards the source. This reflection prevents maximum power transfer, causes erroneous measurements of other parameters, or causes circuit damage in high-power applications.

The power reflected from the load interferes with the incident (forward) power, creating standing waves of voltages and current along the line. The ratio of standing-wave maximal to minimal is directly related to the impedance mismatch of the load. The standing-wave ratio (SWR) provides the means to determine impedance and mismatch.

FIELD EXPEDIENT ANTENNAS

VHF Considerations

SINCGARS VHF radios provide the primary means of communications means for Marine Corps forces around the world. SINCGARS radios operate in both single-channel and frequency hopping modes. It is important for CIS personnel to remember that when using SINCGARS radios in the frequency hopping mode, field expedient VHF antennas should not be used. CIS personnel should only use the whip antenna or the OE-254 antenna when operating in the frequency hopping mode.

HF Considerations

Vertical antennas are omnidirectional. They transmit and receive equally well in all directions. Most manpack portable radios use a vertical whip antenna. Improvise a by using a metal pipe or rod of the correct length, held erect by guys. Insulate the lower end of the antenna from the ground by placing it on a large block of wood or other insulating material. Support a vertical wire antenna with a tree or a wooden pole (fig. 6-4 on page 6-8). For short, vertical antennas, use the pole without guys (if properly supported at the base). If the vertical mast is too short to support the wire upright, modify the connection at the top of the antenna.

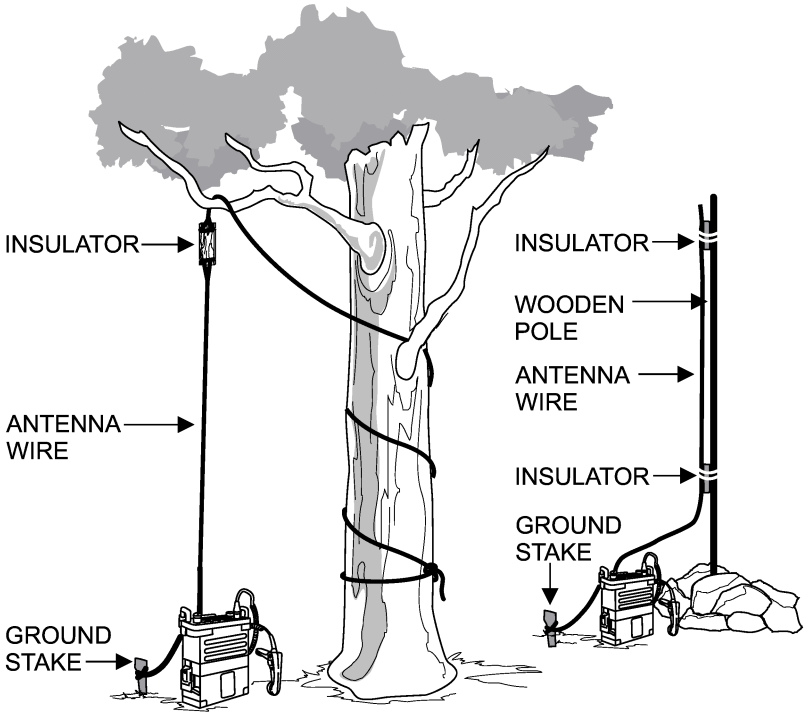


Figure 6-4. Field Substitutes for Support of Vertical Wire Atennas.

End-Fed Half-Wave Antenna

Construct an expedient, end-fed half-wave antenna from available materials (e.g., field wire, rope, and wooden insulators). This antenna's electrical length is measured from the antenna terminal on the radio set to the far end of the antenna (fig. 6-5).

For best performance, construct the antenna longer than necessary, then shorten it, as required, until best results are obtained. Connect the radio set's ground terminal to a good Earth ground for functional efficiency.

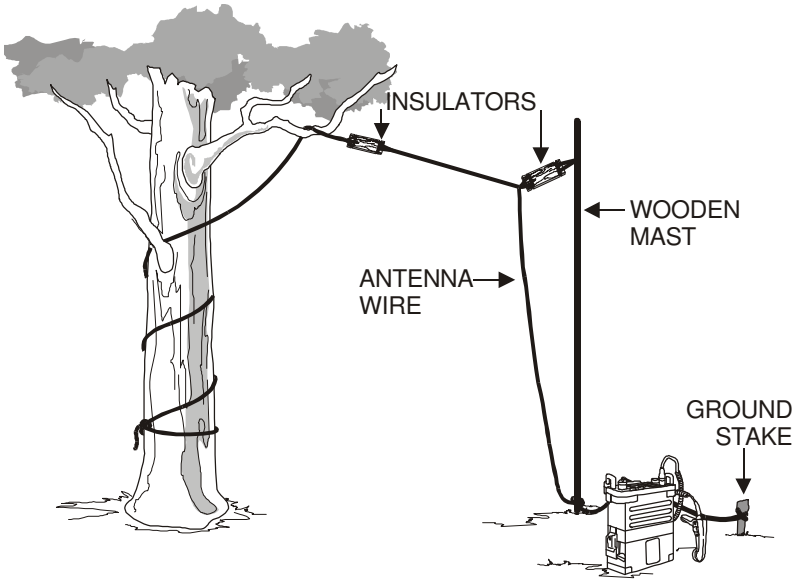


Figure 6-5. End-Fed Half-Wave Antenna.

Center-Fed Doublet Antenna

The center-fed doublet is a half-wave antenna consisting of two quarter-wavelength sections on each side of the center. See figure 6-6 on page 6-10 for constructing an improvised doublet antenna for use with FM radios.

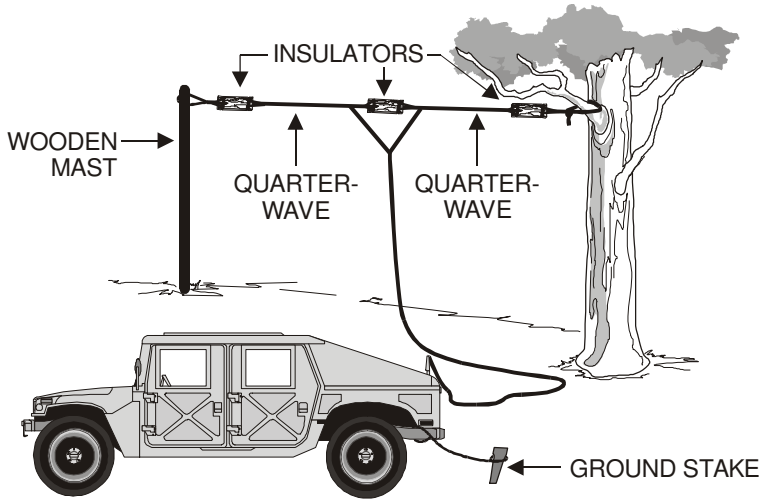


Figure 6-6. Center-Fed Doublet Antenna.

Doublet antennas are directional broadside to their length, which makes the vertical doublet antenna essentially omnidirectional. The radiation pattern is doughnut shaped. The horizontal doublet antenna is bidirectional.

Compute the length of a half-wave antenna by using the formula in chapter 4. Cut the wires as closely as possible to the correct length because the antenna wires' lengths are important.

A transmission line conducts electrical energy from one point to another and transfers the output of a transmitter to an antenna. Although it is possible to connect an antenna directly to a transmitter, the antenna generally is located some distance away. In a vehicular installation, for example, the antenna is mounted outside, and

the transmitter is inside the vehicle. A transmission line, therefore, is necessary as a connecting link.

Center-fed half-wave FM antennas can be supported entirely by pieces of wood. See figure 6-7 (A) for a horizontal antenna of this type. See figure 6-7 (B) for a vertical antenna. These antennas can be rotated to any position to obtain the best performance. If the antenna is erected vertically, the transmission line should be brought out horizontally from the antenna for a distance equal to at least one-half of the antenna's length before it is dropped down to the radio set.

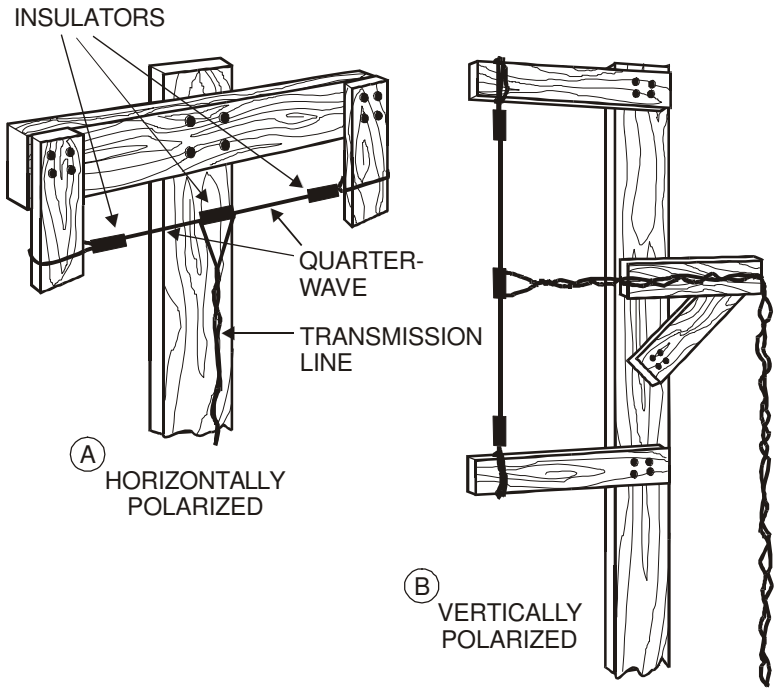


Figure 6-7. Center-Fed Half-Wave Antenna.

A short, center-fed half-wave antenna is shown in figure 6-8. The antenna ends are connected to a piece of dry wood (e.g., a bamboo pole). The bend in the pole holds the antenna wire straight. Another pole, or bundle of poles, serves as the mast.

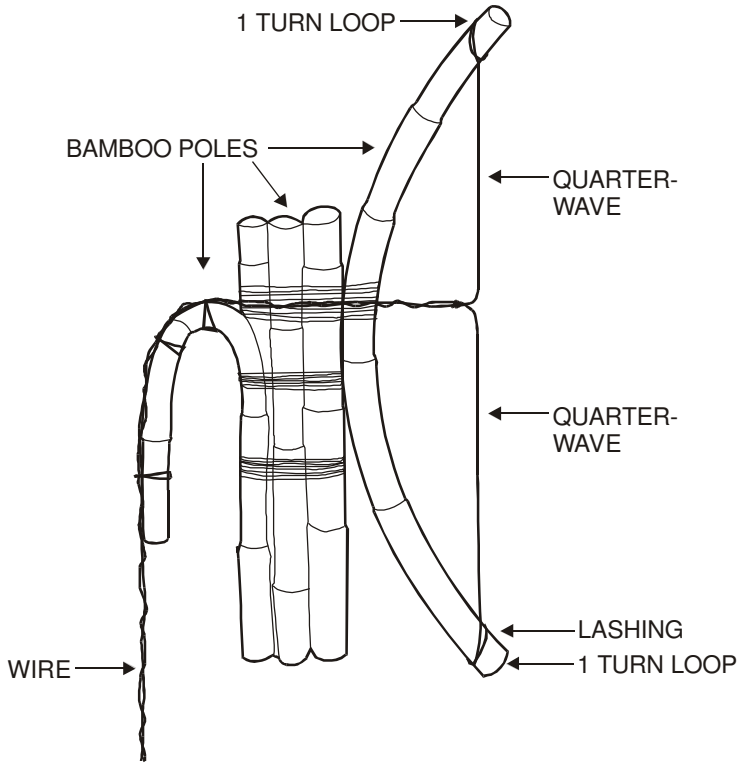


Figure 6-8. Bent Bamboo Antenna.

Figure 6-9 shows an improvised vertical half-wave antenna. This technique is used primarily with FM radios. In heavily wooded areas it is effective for increasing the range of portable radios. The

top guy wire can be connected to a limb or passed over the limb and connected to the tree trunk or a stake.

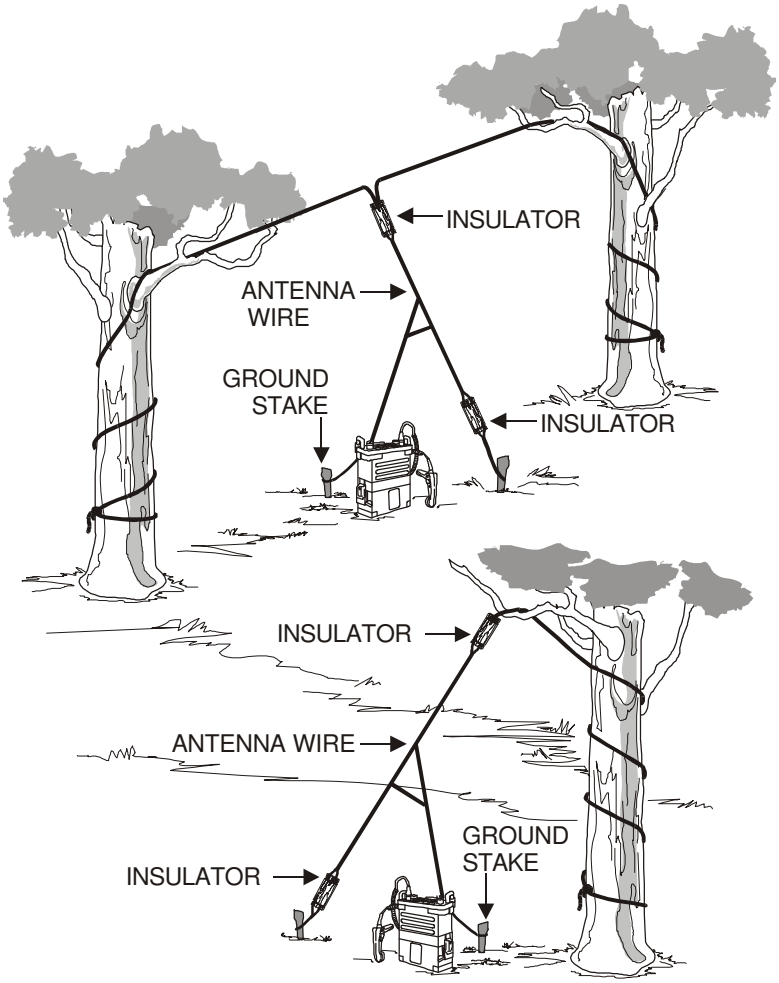


Figure 6-9. Improvised Vertical Half-Wave Antenna.

FIELD EXPEDIENT DIRECTIONAL ANTENNAS

The vertical half-rhombic, the long wire, and the yagi are field expedient directional antennas.

Vertical Half-Rhombic and Long-Wire Antennas

The vertical half-rhombic antenna (fig. 6-10) and the long-wire antenna (fig. 6-11) radiate a directional pattern and primarily transmit or receive HF signals. They consist of a single wire, preferably two or more wavelengths, supported on poles at a height of 3 to 7 meters (10 to 20 feet) above the ground. The antennas also operate satisfactorily as low as 1 meter (approximately 3 feet) above the ground. Connect the far end of the wire to a ground through a noninductive 500- to 600-ohm resistor. To ensure the transmitter's output power does not burn out the resistor, use a resistor that is rated at least one-half the wattage output of the transmitter. Use a reasonably good ground (e.g,. a number of ground rods or a counterpoise) at both antenna ends.

Yagi Antenna

The Yagi antenna (fig. 6-12) is a dipole with an additional wire behind it (reflector) and an additional wire in front of it (director).

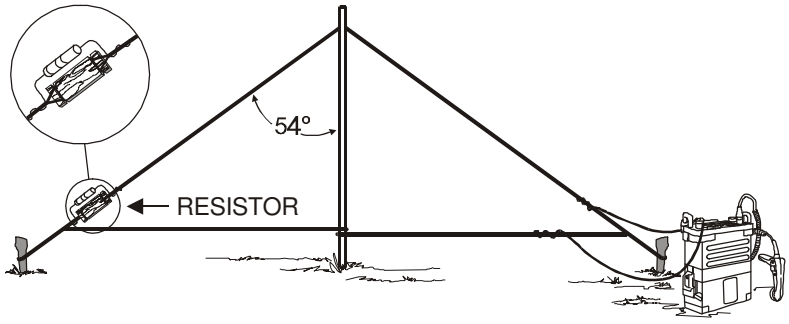


Figure 6-10. Vertical Half-Rhombic Antenna.

These additional wires increase the power to the front of the antenna while decreasing the power to the rear.

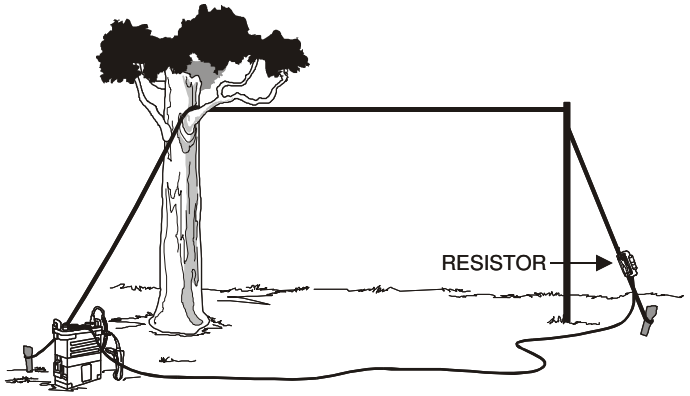


Figure 6-11. Long Wire Antenna.

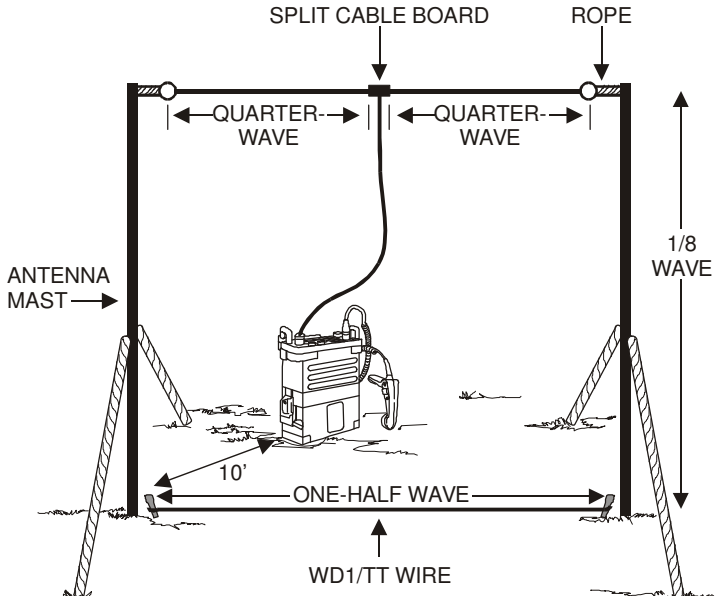


Figure 6-12. Yagi Antenna.

Vee Antenna

The vee antenna is another field expedient, directional antenna. It consists of two wires forming a vee with the open area of the vee pointing in the desired direction of transmission or reception (see fig. 6-13). The antenna must be fed by a balanced transmission line.

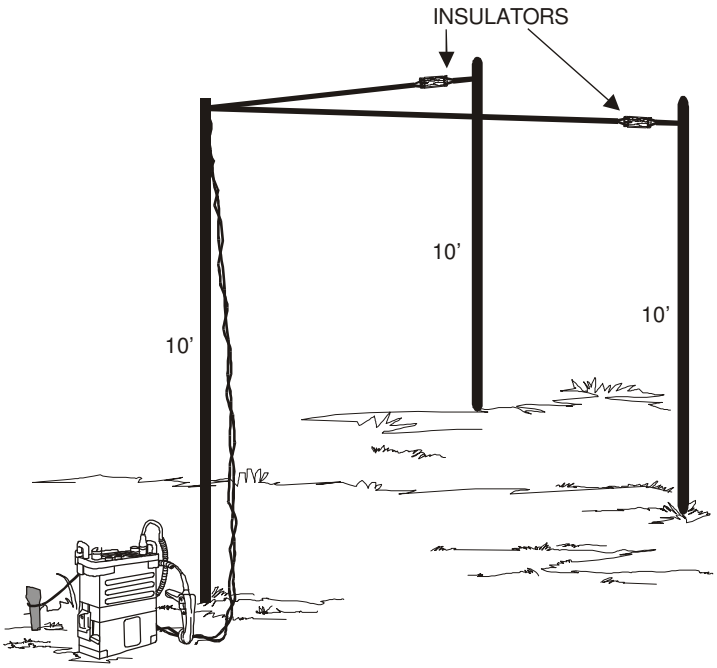


Figure 6-13. Vee Antenna.

Sloping Vee Antenna

To simplify construction, the legs may slope downward from the apex of the vee (this is called a sloping vee antenna [see fig. 6-14]).

The angle between the legs varies with the length of the legs in order to achieve maximum performance.

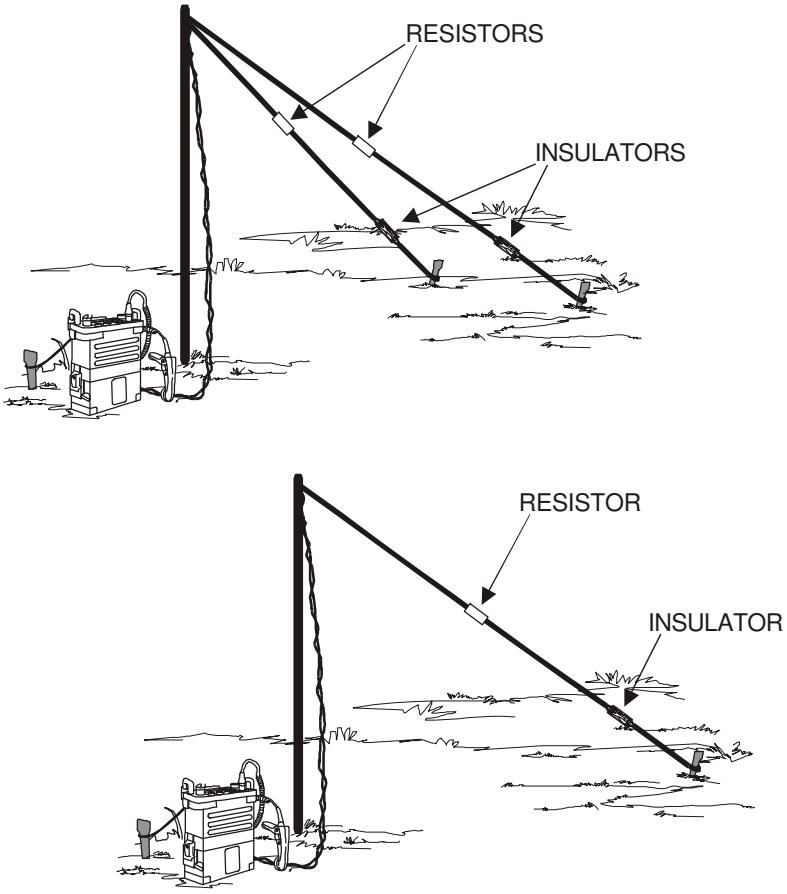


Figure 6-14. Sloping Vee Antenna.

Use table 6-1 to determine the angle and length of the legs..

Table 6-1. Leg Length and Angle for Vee Antennas.

Antenna Length (Wavelength)	Optimum Apex Angle (Degrees)
1	90
2	70
3	58
4	50
6	40
8	35
10	33

When the antenna is used with more than one frequency or one wavelength, use an apex angle that is midway between the extreme angles determined by the chart.

To make the antenna radiate in only one direction, add noninductive terminating resistors from the end of each leg (not at the apex) to ground. The resistors should be approximately 500 ohms and have a power rating at least one-half of the transmitter's output. Without the resistors, the antenna radiates bidirectionally, both front and back.

Chapter 7

Satellite Communications Antennas

The Marine Corps' primary LOS and SATCOM radio set, the AN/PSC-5 enhanced manpack UHF terminal, operates at 5 to 25 kHz and provides data and voice communications. It replaces all man-packable and vehicular-mounted UHF SATCOM radios. The AN/PSC-5 provides LOS communications with the AS-3566 and long-range SATCOM with the AS-3567 and AS-3568 antennas.

Characteristics of the AS-3566 (fig. 7-1) are—

Frequency range (LOS):	**30 to 400 MHz**
Demand assignment multiple access (DAMA):	**225 to 400 MHz**
Non-DAMA:	**225 to 400 MHz**
Polarization:	**Directional**
Power capability:	**Determined by terminating resistor**
Radiation pattern Azimuthal (bearing):	**Directional**

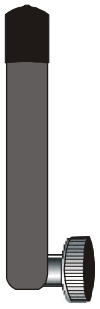


Figure 7-1. AS-3566 Low-Gain Antenna.

Characteristics of the AS-3567 (fig. 7-2) are—

Frequency range:	**225 to 399.995 MHz**
Beamwidth:	**85°**
Orientation:	**Directional**
	Elevation (0 to 90°)
Input impedance:	**50 ohms**
VSWR:	**1.5:1**
Gain:	**6 dB (225 to 318 MHz)**
	5 dB (318 to 399.995 MHz)

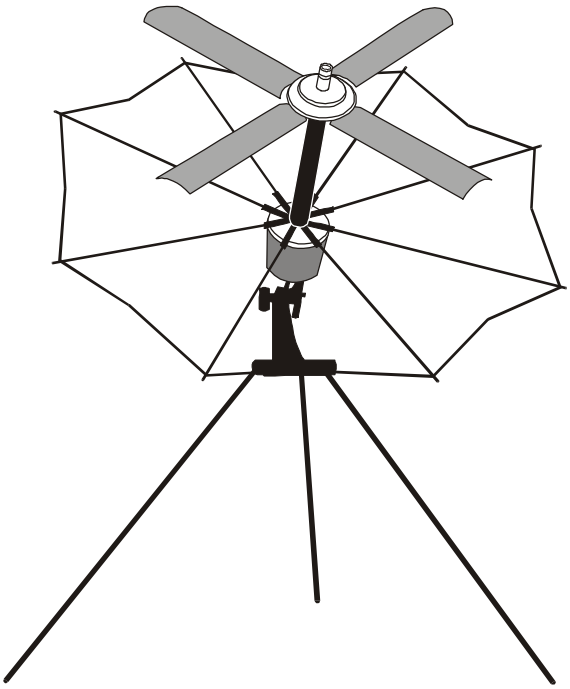


Figure 7-2. AS-3567 Medium-Gain Antenna.

Characteristics of the AS-3568 (fig. 7-3) are—

Frequency range:	**240 to 400 MHz**
Beamwidth:	**77°**
Orientation:	**Directional**
	Elevation (0 to 90°)
	Azimuth: ± 180°
Imput impedance:	**50 ohms**
VSWR:	**1.5:1 maximum**
Gain:	**8 dB (240 to 318 MHz)**
	6 dB (318 to 400 MHz)
Power	**Up to 150 watts continuous**

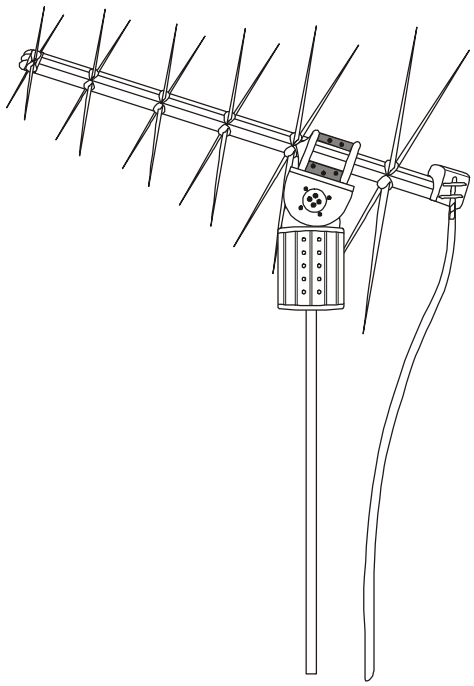


Figure 7-3. AS-3568 High-Gain Antenna.

SITING SATCOM ANTENNAS

The most important consideration in siting LOS SATCOM equipment is the antenna elevation with respect to the path terrain. Choose sites that exploit natural elevations.

Considerations

The most important consideration in siting over-the-horizon systems is the antenna horizon angles (screening angles) at the terminals. As the horizon angle increases, the transmission loss increases, resulting in a weaker received signal.

The effect of the horizon angle on transmission loss is very significant. Except where the consideration of one or more other factors outweighs the effect of horizon angles, the site with the most negative angle should be first choice. If no sites with negative angles exist, the site with the smallest positive angle should be the first choice.

Determining Horizon Angles

The horizon angle can be determined by using a transit at each site and sighting along the circuit path. Strictly speaking, the on-site survey will determine the visual horizon angle. The radio horizon angle is slightly different from the visual horizon angle; however, the difference is generally insignificant.

The horizon angle is measured between the tangent at the exact location of the antenna and a direct LOS to the horizon. The tangent line is at a right angle (90°) to a plumb line at the antenna site. If the LOS to the horizon is below the tangent line, the horizon angle is negative.

Trees, buildings, hills, or the Earth can block a portion of the UHF signal, causing an obstruction loss. To avoid signal loss due to obstruction and shielding, clearance is required between the direct LOS and the terrain. Path profile plots are used to determine if there is adequate clearance in LOS systems.

Weak or distorted signals may result if the SATCOM set is operated near steel bridges, water towers, power lines, or power units. The presence of congested air-traffic conditions in the proximity of microwave equipment can result in significant signal fading, particularly when a nondiversity mode is employed.

(reverse blank)

Chapter 8

Antenna Farms

The antenna farm (also referred to as the radio hill or the antenna hill) is a component of a command echelon. It is the location of the bulk of the unit's antennas and radio and cryptographic equipment. It is also the portion of the command echelon that produces the majority of the electromagnetic radiation. Antenna farms can be located in several different areas: inside the command echelon, outside the command echelon but near it, or outside the command echelon but far from it.

COMMAND POST

The commander exercises command and control through establishing a command post (CP). CPs provide the headquarters facilities from which the commander and staff operate. Battalions and larger units may divide the headquarters into three echelons—tactical, main, and rear. The CP then becomes the echelon at which the commander is physically located.

Tactical

The tactical echelon (main group) is a mobile unit that contains a minimal personnel and equipment. Its main focus is tactical control of current operations. The antenna farm will generally be located within the CP.

Main

The main echelon is where the commander is normally located together with those elements of the staff required to plan and direct operations and control forces. The antenna farm will generally be located outside of and far from the CP.

Rear

The rear echelon, located to the rear of the main echelon, focuses on administrative and logistics functions. It is normally established by regiments and larger units. It may be located in or near the rear echelon of the senior headquarters or remain aboard ship. The antenna farm will generally be located outside of and far from the CP.

LOCATION SELECTION CONSIDERATIONS

There are doctrinal, tactical, and technical considerations involved in deciding of how far the antenna farm should be from the CP. The CIS officer and CIS chief need to list considerations relevant to the situation before determining the best location for the antenna farm.

Doctrinal Considerations

MCWP 6-2 (under development), *MAGTF Command and Control,* FMFM 6 (MCWP 3-1 under development), *Ground Combat Operations*, and MCWP 6-22, *Communications and Information Systems*, contain Marine Corps doctrinal guidance on command echelon organization and location.

Some areas to consider when deciding on the antenna farm location are communications, electronic warfare (EW), tactical situation, and accessibility.

Communications

- Take a radio along on reconnaissance to ensure that communication from the proposed site is possible.
- Choose another site if communication is not possible.

Electronic Warfare

- Enemy capability.
- Projected electronic signature of the command.

Tactical Situation

- Cover and concealment.
- Offense/defense.
- Moving/static.
- Intended length of stay.
- Future operational plans.
- Speed of displacement.

Accessibility

- Terrain.
- Climate.
- Personnel and equipment available.

Tactical Considerations

Once the doctrinal issues have been addressed, locating the antenna farm must be reviewed in the light of tactical considerations. Since the antenna farm contains the majority of the unit's radios, cryptographic equipment, antennas, and a fair portion of the radio operators, the physical safety of the site is an important aspect of the

antenna farm location decision. At the division/force service support group/wing levels, the antenna farm should be remoted 1,000 meters away from the CP, if possible.

Security. The antenna's physical security depends on the ability to protect it. The requirement to provide protection depends on the considerations listed above. Protection considerations also depend, in part, on the proximity of the antenna farm to the CP. For an antenna within the CP, no additional protective measures are required beyond those employed to protect the CP. Additional considerations for the antenna farms located at remote sites follow.

Far Remote Sites

- Security forces available.
- Natural obstacles.
- Perimeter defense, avenues of approach.
- Barbed wire, automatic weapons, deployment.
- Mines and sensors.
- Supporting coverage.

Near Remote Sites

- Same factors as above apply.
- Take increased EW measures.
- Enforce strict circuit discipline.
- Use messengers.

Cover and Concealment. Whether the antenna farm is located inside the unit perimeter or at a remote location, using cover and concealment is imperative. Security assets make it possible to select a site that has the best available cover and concealment. Cover and concealment is a trade-off with the ability to communicate with and

from the site. A thoroughly covered and concealed site that prevents communications is worthless.

Obstacles. As with any other defensive position, use natural or manmade obstacles to enhance the antenna farm's security.

Terrain. Studying the terrain in the vicinity of remote antenna farms is essential to developing an adequate plan for defense. Studying the terrain is also of paramount importance to ensuring that a unit can communicate from the site.

Technical Considerations

Siting VHF antennas greatly effects communications reliability. In an ideal setting, the antenna would be as high as possible above a flat, clear area. In tactical situations, the antenna location must be a compromise of propagation consideration, EW considerations, and cover and concealment.

When it is possible to see the distant station but not communicate with it, the receiving station is experiencing destructive multipath interference. This combining of direct and reflected rays out of phase, results in complete signal cancellation. This interference can also result in a very weak signal or one that flutters. To improve communications, either raise or lower the antenna or move the antenna to several different sites. Usually, one or both of these actions will result in good communications.

Another cause of weak communications is antenna cross-polarization. This means that the transmitting and receiving antennas have a different polarization. For best communications, both antennas should be vertically or horizontally polarized.

Another problem could be misaligned directional antennas. If directional antennas are not correctly pointed at each other, communication is degraded. The directional antennas' electrical characteristics can change over several field deployments, especially if the antenna is subjected to harsh use. These electrical characteristic changes can cause the radiation pattern to change. Then, when the antenna is physically pointed at the distant station, the main radiation may be aimed in another direction.

To correct these electrical characteristic changes, have the distant station transmit. Slowly turn the receiving antenna while listening to the received signal. When the received signal is strongest, the antenna is properly aligned for the circuit. Secure the antenna in this position and have the distant station align its antenna in the same way. When both antennas are properly adjusted, the maximum radiation from each antenna is directed at the other antenna.

SITING VHF ANTENNAS

Antenna sites should be as high as possible and clear of obstructions such as hills, dense woods, and buildings. If it is necessary to site the antennas on or around hills, choose a site that allows LOS to the distant station or stations. If possible, place the antenna on the military crest of a hill, *not* on the ridge line. Antennas located on the ridge line provide an aiming stake for enemy observation and fire (fig. 8-1).

Place high ground between the antenna and the enemy to block the enemy's observation and the antenna's radiation, reducing the enemy's intercept capability (fig. 8-2).

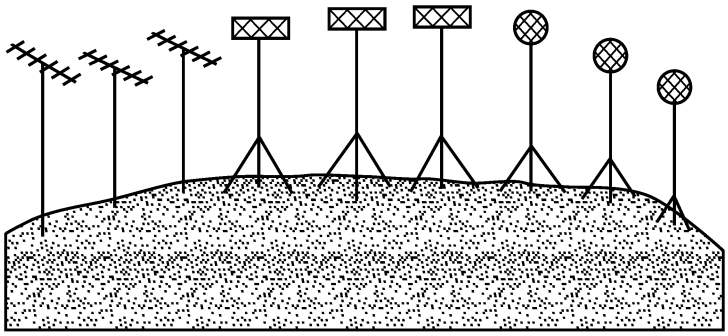


Figure 8-1. Ridge Line Antenna Farm.

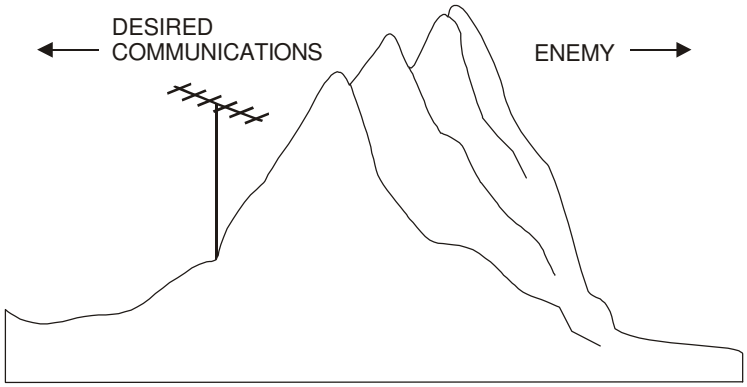


Figure 8-2. Antenna Sited on a Military Crest.

In a dense forest, get the antenna tip above the treetops. This height allows the radio signal to propagate in the clear space above the trees. If it is impossible to raise the antenna above the trees, a horizontally polarized antenna provides better communications through

trees than a vertically polarized antenna. Figure 8-3 shows good, fair, and poor antenna siting in dense trees.

A clearing in a forest improves propagation if the antenna is placed so that the clearing is between the antenna and the distant station (for a directional antenna). Place an omnidirectional antenna in the center of a clearing, with the antenna as high as possible (fig. 8-4).

A communicator may have little choice in selecting a transmitter or receiver site location. Often the site is determined by the operational requirements of a superior command. However, when a choice is available, determine the HF antenna site by wave-path geometry.

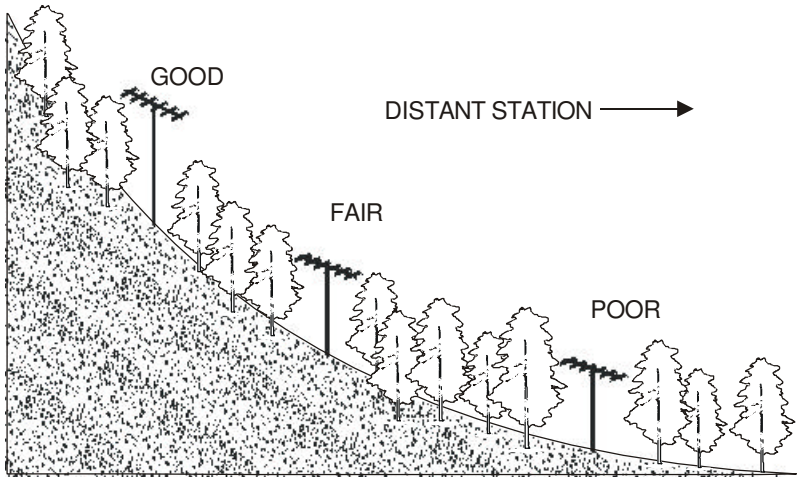


Figure 8-3. Antennas Sited in Dense Trees.

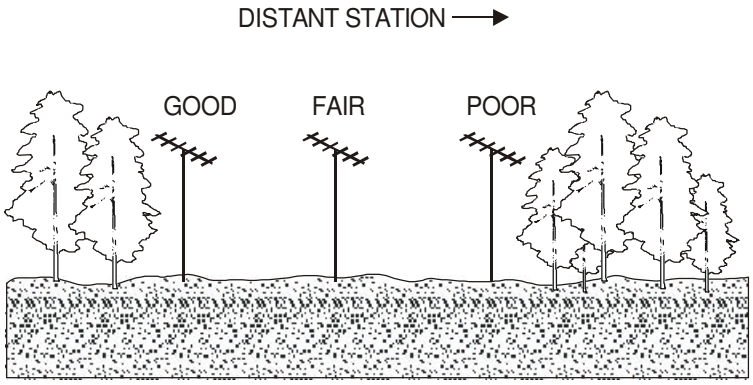


Figure 8-4. Directional Antennas Sited in a Clearing.

Transmitting Antenna Site

Any site that has a horizon whose obstructions subtend vertical angles of less than 2° from level in any of the directions of transmission can be considered immediately as a satisfactory site from the standpoint of radiation. As a simple rule, a satisfactory horizon clearance exists when any obstruction subtends a vertical angle that does not exceed one-half of the desired beam angle in the vertical plane in that direction. If the vertical beam angle for a given circuit is low for the lowest order hop, then the horizon in that direction can be as much as 5° above level as seen from the antenna location.

In hilly or mountainous country, choosing a site for long-distance transmission, requiring very low beam angles, can be difficult. When the only possible site presents horizon obstructions in the preferred wave path, it may be necessary to design an antenna that uses a higher order of hop, and to direct the beam at a corresponding higher angle to obtain the desired 2-to-1 horizon clearance angle.

For example, if the computed vertical beam angle for a one-hop circuit is 6° at an azimuth of 332°, and the horizon in this direction is a range of mountains with a height of 8° as seen from the antenna site, the performance of the circuit would be greatly compromised by the obstruction of the mountains. It might be better to work this circuit with two hops—a vertical beam of 20° could be used instead, with adequate horizon clearance for the wave path. If the circuit required 6° for a two-hop circuit 5,400 kilometers long with the same obstruction sited, the circuit could be changed to three hops, which, for the same layer heights, would permit using a beam at 14°. The latter solution lacks the full 2-to-1 horizon-clearance angle, but it may be an acceptable compromise and perhaps preferable to using four hops.

Short-range, sky wave circuits using one-hop high-angle radiation give a great latitude in the choice of sites. For F layer transmission to distances of 500 miles and less, the vertical beam or angles are always greater than 30°. Satisfactory sites for such transmission can often be located in rather deep valleys without any compromise on the circuit performance.

Forests on or near the site require some consideration. Because the theoretical radiation pattern is calculated on perfect reflectivity from ground, some precautions are necessary to obtain actual performance that substantially agrees with theoretical performance. Choose a site that provides conditions as nearly perfect as possible with respect to wave-reflecting surfaces around the antenna. There should be few or no trees and buildings out to the necessary distance from the antenna. The point of wave reflection should be flat and cleared. An excellent choice is a site that borders the sea or a lake. Water is a wave-reflecting surface.

Receiving Antenna Sites

Choosing a receiving antenna site is similar to choosing a transmitting antenna site. The dominant angles of arrival of the incoming waves at the site are determined mainly by the characteristics of the transmitting antenna. Best results are obtained with complementary transmitting and receiving antennas. If a horizon obstruction exists at the optimum angle of wave arrival, a compromise, noncomplementary antenna may be necessary. When possible, move the transmitting antenna to align with the receiving antenna.

The receiving site must be as free as possible from electrical noise. The tolerable amount of manmade noise at a particular receiving station site depends on the prevailing natural atmospheric noise levels. At a well selected site, reception should always be limited only by natural atmospheric noise. Any manmade noise at the site should always be substantially less than the atmospheric noise received during the low-noise periods.

Aside from broadcast systems, most communications systems require that antennas be positioned so that their main lobes of radiation are aligned with each other. This requires knowledge of the great circle bearing to the other antenna and the local magnetic variation from true north.

The great circle bearing between two locations is calculated by methods that are beyond the scope of this publication. A way to find the great circle bearings is to request a frequencies of optimum transmission chart from the Electromagnetic Compatibility Analysis Center.

ANTENNA FARM INTERNAL ARRANGEMENT

Frequency Band

The higher the frequency, the shorter the wavelength. The shorter the wavelength, the more nearly LOS. The more nearly LOS, the more critical is a clear LOS path for the signal.

Antenna Selection and Placement

Selection. The key to antenna selection rests with the answers to the following three questions:

- **To whom will you be transmitting? Where will they be?**
- **What is the path between you and them?**
- **What kind of net? Point-to-point or multistation?**

Placement. Antenna placement within the antenna farm should take into account the following three factors:

Cosite Interference. **Evaluating interference can be difficult because of the nature of the systems involved and the complexity of the signals. The mechanisms are varied. In the simpler cases they may be direct interference into the radio receiver. In other cases, they may be spurious products or combinations of products which arrive at the receiver input and produce a net resultant interference into the receiver intermediate frequency section. The latter may be frequency translations resulting from sum and difference products within the same system. In still other cases, the receiver may see an identical signal to the regular signal.**

Interference produces beats or noise in a radio receiver which have detrimental effects depending on the frequency, deviation, channel separation and linearity of the transmission medium, as well as the

nature of the interfering signal. Sometimes the interfering signals combine with other frequencies in the system, including carrier-sum and difference frequencies, to produce interference in a third radio channel. The products may hold up automatic gain control during critical fading periods, with serious effect on system noise. Usually, noise in the base band channels is an end product.

Radio system interference may be introduced through antennas, wave guides, cabling, or by spurious products produced in the radio equipment itself. Interference introduced into the cabling or in the equipment can be prevented by good installation practices, including proper separation of high- and low-level cabling, proper grounding practices, shielding where necessary, and good equipment design and assembly. Interference introduced by coupling between wave guides in the same station is usually produced by radiation from wave guide and filter flanges which are not properly tightened, or which are damaged and cannot be mated properly.

Antenna Coupling. Antenna coupling is a frequency-independent problem that may occur whenever other antennas (whether transmitting or not) or metallic objects are located within one wave of the transmitting antenna. Antenna coupling may be either beneficial or detrimental. Yagis, log periodic arrays, and half-square antennas, for example, derive their gain and directivity from antenna coupling. Unintended antenna coupling, on the other hand, may significantly reduce the signal strength in the desired direction and either degrade or stop communications.

Coupling is based on two principles. One, that current flowing through a wire creates a magnetic field around it; and, two, that signals in phase reinforce each other whereas signals out of phase cancel each other. Receiving antennas have current flowing in them (the received signal). Because there is a flowing current that creates a magnetic field, a receiving antenna will simultaneously receive and reradiate the same signal. Receiving antennas, in fact, tend to

reradiate about one-half of the power they receive. If the receiving antenna is within one wavelength of a transmitting antenna (it makes absolutely no difference whether or not the receiving antenna's radio is tuned to the same frequency as the transmitting radio), the receiving antenna will reradiate a portion of the signal which may be out of phase with the original signal, altering the transmitting antenna's radiation pattern.

Direction of Desired Transmission. **Separate antennas according to the direction of desired transmission. For example: If antenna A is used to communicate to the east, and antenna B is used to communicate to the north, then locate antenna A south and east of antenna B.** ***Do not*** **make the signal from one antenna pass through, or around, another antenna on the way to its intended receiver. Accomplish this by the physical location of the antennas, by masking the antennas, or by placing the antennas at different elevations.**

Requirements

Separate antennas based on the frequencies at which they will operate and the power they will transmit to avoid cosite interference.

For a 10 percent separation—

Power	Distance (Meters)
1 kilowatt	500
400 watts	315
150 watts	200
100 watts	150
40 watts	100
20 watts	70
10 watts	50
2 watts	22
1 watt	15

Multiply separations by 10 for each halving of frequency separation (i.e., 10 for 5 percent; 100 for 2.5 percent).

For a 5 percent separation—

Power (Watts)	Distance (Meters)
10	500
2	220
1	150

For a 2.5 percent separation—

Power (Watts)	Distance (Meters)
10	5000
2	2200
1	1500

Separate antennas by a minimum of wavelength at the lowest frequency at which they will operate to alleviate antenna coupling.

Band	Lowest Frequency (MHz)	Minimum Separation (Feet)
HF	2	492
VHF	30	32.8
UHF	225	4.37

Separate antennas according to the desired direction of transmission (i.e., don't send the propagated wave through other antennas).

Polarization

The preferable polarization with respect to vegetation depends on the forest and the amount of foliage. Use a polarization with an inherent advantage when heavy vegetation cannot be avoided. Any

advantage based on polarization will be determined by the polarization of possible sources of interference. In deciduous forests the sources are evenly divided between vertical and horizontal. In mature coniferous forests the sources are predominately vertical, so horizontal polarization has an advantage.

Power and Signal Lines

Distribute power and signal lines to eliminate and avoid crossovers. If power and signal lines must cross, arrange them so that they cross at right angles, and separate them by 4 feet of elevation. Do not run power and signal lines parallel to each other.

ANTENNA FARM LAYOUT PRINCIPLES

- Segregate HF, VHF, and UHF channels.
- Maintain separation between antennas.
- Separate power and signal lines. Keep them out of the main ground phase of antennas.
- Keep transmitters close to the feed point of their antennas (i.e., keep them short).
- Establish good RF and safety grounds for each antenna.
- Use ground radials for each antenna.
- Site LOS antennas on the highest ground.
- Site antennas to avoid the main lobes and significant side lobes of directional antennas.
- Remote antenna farms 1 kilometer from the CP if practical.

Appendix A

GLOSSARY

Section I
Acronyms and Abbreviations

AM ..... **amplitude modulationn**

C ..... **centigrade**
CIS ..... **communications and information systems**
cm ..... **centimeter**
COMSEC ..... **communications security**
CP ..... **command post**

dB ..... **decibel**
dBi ..... **decibels over an isotropic radiator**

e.g. ..... **for example**
EW ..... **electronic warfare**

FM ..... **frequency modulation**
FMFM ..... **Fleet Marine Force manual**
FMFRP ..... **Fleet Marine Force reference publication**

GHz ..... **gigahertz**

HF ..... **high frequency**

i.e. ..... **that is**

kHz ..... **kilohertz**
km ..... **kilometer**
kW ..... **kilowatt**

LOS ..... **line of sight**
LUF ..... **lowest usable frequency**

MAGTF ..... **Marine air-ground task force**
MCDP ..... **Marine Corps doctrinal publication**
MCRP ..... **Marine Corps reference publication**
MCWP ..... **Marine Corps warfighting publication**
MHz ..... **megahertz**
mi ..... **mile/miles**
MUF ..... **maximum usable frequency**

NVIS ..... **near-vertical incidence sky wave**

RF ..... **radio frequency**

SATCOM ..... **satellite communications**
SCR ..... **single-channel radio**
SID ..... **sudden ionospheric disturbance**
SINCGARS ..... **single-channel ground and airborne radio system**
S/N ..... **signal-to-noise**
SPEED ..... **system planning, engineering, and evaluation device**
SWR ..... **standing wave ratio**

TV ..... **television**

UHF ..... **ultrahigh frequency**

VHF ..... **very high frequency**
VHF-LOS ..... **very high frequency line of sight**
VSWR ..... **voltage standing-wave ratio**

W ..... **watt**

Section II
Definitions

A

alternating current—Current that is continually changing in magnitude and periodically in direction from a zero reference level. Also called AC.

amplification—The process of increasing the strength (current, voltage, or power) of a signal.

amplitude—The level of an audio or other signal in voltage or current. The magnitude of variation in a changing quantity from its zero value.

amplitude modulation—Modulation in which the amplitude of the carrier wave is varied above and below its normal value in accordance with the intelligence of the signal being transmitted. Also called AM.

angle of incidence—The acute angle (smaller angle) at which a wave of energy strikes an object or penetrates a layer of the atmosphere or ionosphere.

antenna—A device used to radiate or receive electromagnetic energy (generally RF).

antenna bandwidth—The frequency range over which a given antenna will accept signals.

antenna feed—Means by which power is transferred to and from the antenna and the connecting transmission line.

antenna gain—The effectiveness of a directional antenna as compared to a standard nondirection antenna. It is usually expressed as the ratio in decibels of standard antenna input power to directional antenna input power that will produce the same field strength in the desired direction. For a receiving antenna, the ratio of signal power values produced at the receiver input terminals is used. The more directional an antenna is, the higher is its gain.

array—Several simple antennas, usually dipoles, used together to control the direction in which most of the antenna's power is radiated.

attenuation—Power loss resulting from conductor resistance and dielectric loss within the insulating material used to separate the conductors.

azimuth—An angle measured in a horizontal plane from a known reference point.

B

balanced antenna—An antenna is balanced with respect to ground when both its arms have the same electrical relationship to ground.

balanced transmission line—A transmission line whose conductors have voltages of opposite polarity and equal magnitude with respect to the Earth.

balun—A device for feeding a balanced load with an unbalanced line, or vice versa.

bandwidth—The width of a band of frequencies used for a particular purpose.

baud—The number of times per second the carrier signal changes value.

bidirectional—In two directions, usually opposite.

blob—Small areas of the atmosphere where temperatures and pressure differences produce conditions suitable for the refraction of radio waves.

broadband antenna—An antenna capable of operation over a wide band of frequencies

C

cable connectors—Fittings for cable ends which permit rapid connection and disconnection with equipment or other cables.

capacitance—A natural property of an electrical circuit which opposes the rate of change of voltage.

capacitor—A device for storing electrical charge.

center-fed—Transmission line connection at the electrical center of an antenna radiator.

coaxial cable—A transmission line consisting of two conductors, one inside the other, and separated by insulating material. The inner conductor may be a small copper tube or wire; the outer conductor may be metallic tubing or braid. Radiation loss from this type of line is very little.

command post—The headquarters of a unit or subunit where the commander and staff perform their functions.

communications circuit—The means by which information is transferred between two or more places.

conductor—A material (usually metal) that has low resistance to the flow of electrical current. A wire, cable, or other object capable of carrying electric current. Good conductors are made of metals such as silver, copper, and aluminum.

connections—Points at which two or more conductors are brought into contact.

counterpoise—A conductor or system of conductors used as a substitute for ground in an antenna system; a wire or group of wires mounted close to the ground, but insulated from ground, to form a low-impedance, high-capacitance path to ground.

critical frequency—The highest frequency at which a signal may be transmitted directly overhead and be reflected back to Earth from the ionosphere.

cross-polarized—The polarization of a received signal is 90 degrees to the polarization of the receiving antenna.

current—The flow of electrons along any path.

D

decibel—The standard unit used to express transmission gain or loss and relative power levels. Also called dB.

deflection—The displacement of an electron beam from its line of sight path.

demodulate—To recover the information originally impressed on the radio wave.

dielectric—A material that does not conduct electricity, such as rubber or glass, i.e. an insulator.

diffraction—The process by which electromagnetic waves are bent so that they appear behind an obstruction.

dipole antenna—A center-fed wire antenna whose conductors are in a straight line.

directional antenna—An antenna designed to transmit and receive RF energy in a specific direction(s).

direct waves—Waves which propagate in a straight line from the transmitting to the receiving antennas.

directivity—The property of radiating more energy in some directions than in others.

director—A conductor placed in front of a driven element to cause directivity.

ducting—The propagation of VHF/UHF wave by bouncing between the Earth's surface and the interface between layers of air having different dielectric constants.

E

efficiency—The ratio of power output to power input.

electromagnetic field—The field of force that an electrical current produces around the conductor through which it flows.

electromagnetic waves—A wave propagating as a periodic disturbance of the electric and magnetic fields and having a frequency in

the electromagnetic spectrum; the means by which energy is transmitted from one place to another.

end-fed—An antenna whose power is applied to one end rather than at some point between the ends.

F

fading— A periodic decrease in received signal strength.

feedpoint impedance—Impedance that is measured at the input terminals of an electrical device such as an antenna.

fields—Regions in which each point has a value of a physical quantity (voltage, magnetic force, velocity, mass, etc.).

free space—The absence of ground.

frequency—The rate at which a process repeats itself. In radio communications, frequency is expressed in cycles per second.

frequency hopping—A method of jumping from frequency to frequency in synchronization with one another in a random order at a rate of up to 100 times per second. Frequency hopping is the preferred method of communication with SINCGARS radios.

frequency modulation—The process of varying the frequency of a carrier wave, usually with an audio frequency, in order to convey intelligence. Also called FM.

frequency of optimum transmission—85 percent of the maximum usable frequency (MUF). A practical frequency selection which allows for MUF variations.

G

gain—The increase in signal strength that is produced by an amplifirer.

generator—A device that changes mechanical energy into electrical energy.

ground—A very large semiconductive surface (the Earth) or a smaller highly conductive surface.

ground radials—Wires on or in the earth to improve its conductivity near the antenna.

ground screen—A wire mesh ground plane.

ground wave—A radio wave that travels along the Earth's surface rather than through the upper atmosphere.

H

half-wave dipole antenna—A center-fed antenna whose electrical length is half the wavelength of the transmitter or received signal.

half-wave vertical dipole antenna—A half-wave dipole constructed vertical to the Earth's surface.

hertz—One cycle per second.

high frequency—frequencies between 3 and 30 MHz.

hop—A single reflection of the wave back to Earth at a point beyond the horizon.

horizontal dipole—A dipole constructed parallel to the Earth's surface.

horizontal pattern—The horizontal cross-section of an antenna's three-dimensional radiation pattern.

horizontal polarization—Transmission of radio waves in such a way that the electric lines of force are horizontal (parallel to the Earth's surface).

I

impedance—The total opposition offered by a circuit or component to the flow of alternating current.

impedance match—The condition where the load impedance equals the characteristic impedance of a transmission line.

inductance—The natural property of an electrical circuit which opposes the rate of change or current, i.e., electrical "intertia."

in phase—Two or more signals of the same frequency passing through their maximum and minimum values of like polarity at the same instant.

insulator—A device or material that has a high electrical resistance; a nonconductor of electricity.

interference—A degradation of a received signal caused by another transmitter, a noise source, or the desired signal propagation over two or more different routes.

inverted L antenna—A half-wave dipole fed by a one-quarter wavelength long vertical section.

inverted vee antenna—A half-wave dipole erected in the form of an upside-down vee, with the feed point at the apex. It is essentially omnidirectional, and is sometimes called a "dropping doublet."

ionization—The process where radiation and particles from the Sun make some of the Earth's atmosphere partially conductive.

ionosphere—A partially conducting region of the Earth's atmosphere between 50 kms and 400 kms high.

L

lambda—Greek lower case letter (λ) used to represent a wavelength with reference to electrical dimensions in antenna work.

linearly polarized antennas—Antennas that produce only one polarization.

line of sight—The transmission path of a wave that travels directly from the transmitting antenna to the receiving antenna. Also called LOS.

load—A device that consumes electrical power.

loading—Providing or connecting an electrical device capable of accepting power to match the impedance of an antenna to a transmitter so that maximum power is radiated from a generating device, such as a transmitter.

lobe—A bulge on an antenna radiation pattern which indicates the direction in which radiated power is concentrated.

long-wire antenna—An end-fed single wire antenna usually one wavelength or longer.

lowest usable frequency—The lowest frequency that will not be absorbed by the ionosphere or smothered by atmospheric noise. Also called LUF.

M

maximum usable frequency—The highest frequency for a given elevation angle that will reflect from an ionospheric layer. Also called MUF.

megahertz—One million cycles per second. Also called MHz.

modulate—To change the output of a transmitter in amplitude phase, or frequency in accordance with the information to be transmitted.

monopole antenna—An antenna with a single radiating element; a whip antenna.

N

noise—Random pulses of electromagnetic energy generated by lightning or electrical equipment.

O

offset angle—The angle at which a long wire antenna must be aimed on either side of the direction to the base station.

omnidirectional antenna—An antenna whose radiation pattern shows equal radiation in all horizontal directions.

oscillation—A periodic, repetitive motion or set of values (voltage, current, velocity).

out of phase—Two alternating quantities not passing through corresponding values at the same time (e.g., if the current in a circuit reaches its maximum value before or after the applied voltage does, the current is out of phase with the voltage).

P

path loss—The ratio of received power to transmitted power.

polarization—The direction of the electric field of a radiated wave relative to the surface of the Earth (vertical, horizontal, linear, and circular).

polarization fading—Fading due to polarization rotation of a received signal. The received signal decreases when the incoming wave does not have the same polarization as the receiving antenna.

power gain—The directive gain of an antenna multiplied by its efficiency

propagation—A phenomenon by which any wave moves from one point to another; the travel of electromagnetic waves through space of along a transmission line.

propagation path—The path or route over which power flows from the transmitter to the receiver.

Q

quarter-wave antenna—An antenna with an electrical length that is equal to one-quarter wavelength of the signal being transmitter or received.

R

radiate—To transmit RF energy.

radiation—Energy that moves through space as electromagnetic waves.

radiation patterns—A chart of relative radiation intensity (or power) versus direction.

radio frequency—Any frequency of electrical energy capable of propagation into space (usually above 20 kHz). Also called RF.

radio horizon—The greatest distance on the Earth at which a transmitted wave can be received by the direct path from a transmitter located on the Earth.

radio waves—Electromagnetic waves at a frequency lower than 3,000 GHz and propagated through space without and artificial guide.

receiver—Amplifying and selecting equipment that receives radio frequencies and delivers a duplicate of the information impressed on the transmitter.

reception—The process of recovering transmitted information; the process of converting electromagnetic fields to current in wires.

reciprocity—The various properties of an anntenna apply equally whether the antenna is transmitting or receiving.

reflected waves—Waves that change their direction of propagation after striking a surface that is either a conductor or an insulator.

reflection—The turning back of a radio wave from an object or the surface of the Earth.

reflector type antenna—An antenna placed in front of a conducting surface (reflector) for the purpose of increasing radiation in one direction, at the expense of radiation in other directions.

refraction—The bending, or changing direction, of a radio wave passing into or through layers of the atmosphere or the ionosphere that have different density (dielectric constant).

refractive index—A measure of the degree by which the speed of an electromagnetic wave is slowed as it propagates through a given material.

resistance—The property of a material or substance to oppose the passage of current through it, thus causing electrical energy to be converted into heat energy.

resonance—The state or frequency of vibration, electrical or mechanical, in which forces that impede the motion are minimum.

resonant length—The proper length of an antenna to render it resonant

rhombic antenna—An antenna made of four wires of equal length connected together in the shape of a rhombus.

S

scattering—The spreading or breaking up of electromagnetic waves when they encounter objects of different electrical properties than those in which the wave is traveling.

shortened dipole—A dipole antenna made to resonate at a lower frequency by use of a coil.

signal—A radio wave that contains the transmitted message.

signal loss—The amount of signal power lost between the transmitter and receiver.

signal-to-noise ratio—The power intensity of the signal compared to that of the noise.

skip distance—The distances on the Earth's surface between the points where a radio wave sky wave leaves the antenna and is successfully reflected and/or refracted back to Earth from the ionosphere.

skip zone—The space or region within the transmission range where signals from a transmitter are not received, i.e., between the ground wave and the point where the refracted wave returns.

sky wave—A radio wave that is reflected from the ionosphere.

sloping long-wire antenna—A wire antenna of length greater than one wave-length and supported in an inclined orientation with respect to the ground.

standing-wave ratio—The ratio of the maximum to minimum amplitudes of voltage, or current, along a transmission line.

standing waves—Waves that appear not to be moving as the result of power traveling in both directions along a transmission line.

stratosphere—The second layer of the Earth's atmosphere, extending from 10 to 50 km.

sunspots—Activity on the Sun's surface which is seen as a series of blemishes that vary in size, number, and location.

T

take-off angle—The angle measured from the Earth's surface or horizontal up to the direction of propagation towards the ionosphere.

transistor—A minute electronic device that permits a small current to control the flow of a larger current.

transmission line—A conductor that transfers radio frequency RF energy from the transmitter to the antenna or from the antenna to the receiver.

transmitter—A piece of equipment that generates and amplifies a radio frequency, adds intelligence to this signal, and then sends it out into the air as a radio frequency wave.

troposphere—The region of the Earth's atmosphere from the surface to a height of about 10 km.

tuning—The process of adjusting a radio circuit so that it resonates at the desired frequency.

twin-lead transmission line—A balanced transmission line generally used with balanced antennas.

two element array—An antenna composed of two element antennas.

U

ultrahigh frequency—Frequencies between 300 and 3,000 MHz.

unbalanced transmission line—A transmission line one of whose conductors is grounded.

unidirectional—In one direction only.

V

vee antenna—Two long-wire antennas connected to form a vee.

velocity—The speed of a radio wave through the dielectric medium it is in.

vertical dipole—A balanced or dipole antenna oriented vertically.

vertical polarization—Transmission of radio waves in such a way that the electric lines of force are vertical (perpendicular to the Earth's surface).

vertical quarter-wave antenna—A monopole (whip) antenna that is oriented vertically.

very high frequency— Frequencies between 30 and 300 MHz; transmissions that follow the line of sight path.

voltage—Electrical pressure, expressed in volts, which is the result of squeezing electrons together.

voltage standing-wave ratio—The ratio of the amplitude of the electric field or voltage at a voltage maximum to that at an adjacent voltage minimum. Also called VSWR.

W

wavelength—The distance a wave travels during one complete cycle. It is equal to the velocity divided by the frequency.

wave propagation—The transmission of RF energy through space.

whip antenna—A vertical monopole.

wire—Conductors in one of many different sizes with different kinds of insulation.

Y

yagi antenna—A combination of dipoles to increase the gain.

Appendix B

References and Related Publications

Marine Corps

Warfigthing Publication (MCWP)

6-22 **Communications and Information Systems**

Reference Publications (MCRPs)

6-22A **TALK-II SINCGARS: Mutiservice Communications Procedures for the Single-Channel Ground and Airborne Radio System**

6-22C **Radio Operator's Handbook (under development)**

Technical Manual (TM)

2000-15/2B **Principal Technical Characteristics of U.S. Marine Corps Communications-Electronic Equipment**

Army

Field Manuals (FMs)

11-32 **Combat Net Radio Operations**

11-43 **Signal Leader's Guide**

11-65 **High Frequency Radio Communications**

24-2 **Spectrum Management**

24-18 **Tactical Single-Channel Radio Communications Techniques**

24-19 **Radio Operator's Handbook**

(reverse blank)

NATIONAL SYSTEM FOR GEOSPATIAL INTELLIGENCE

GEOSPATIAL INTELLIGENCE (GEOINT) BASIC DOCTRINE

Publication 1.0
April 2018

Approved for public release, 18-142

MESSAGE FROM THE GEOINT FUNCTIONAL MANAGER

I am pleased to present *Publication 1.0: GEOINT Basic Doctrine, 2018*, to the NSG Community. This publication serves as an introduction to GEOINT, establishes common references and terminology, and directly supports our NSG Strategic Priority "Professionalization – Inspire the Next Generation Talent."

Publication 1.0 is unique because it was created by the NSG Community and carefully crafted to avoid terms and language specific to any Agency or Service. The NSG Working Group (which included representatives from Services and Agencies that train GEOINT professionals) guided and approved all content prior to formal NSG coordination.

One contribution of Publication 1.0 is the establishment of a common, NSG-coordinated GEOINT glossary. This is a basic but very important step to achieve standardized training and certification, shared curricula, and a workforce that can provide GEOINT support in any environment. These goals are also supported by Chapter Four, which contains the first GEOINT Tradecraft Chart to map military occupations to civilian tradecraft roles.

Other key features of Publication 1.0 include:

- Reference charts for platforms and phenomenology
- User-friendly descriptions of GEOINT concepts and functions
- Introduction and definition of the term "GEOINT Enterprise"
- Definitions of GEOINT, NSG, ASG, CAC
- Charts that show members of the NSG, ASG, CAC, and GEOINT Enterprise

Finally, I am proud we were able to complete an unclassified, publically releasable document to help ensure the widest distribution and use across the NSG, ASG, and beyond.

Onward,

R T Cardillo

Robert Cardillo
GEOINT Functional Manager

TABLE OF CONTENTS

INTRODUCTION

PURPOSE, SCOPE, APPLICABILITY, AND OVERVIEW.....1

CHAPTER ONE

GEOINT DEFINITION & DESCRIPTION.....3

CHAPTER TWO

DATA.....6

CHAPTER THREE

PRODUCTS.....15

CHAPTER FOUR

TRADECRAFT.....23

CHAPTER FIVE

GEOINT COMMUNITY & GOVERNANCE.....28

ACRONYM LIST.....32

GLOSSARY.....34

APPENDIX

A: REFERENCES.....40

B: GEOINT DEFINITION.....41

INTRODUCTION

PURPOSE.

Geospatial Intelligence (GEOINT) Basic Doctrine, Publication 1.0, (hereinafter referred to as *Pub 1.0*) provides decision makers and intelligence producers a basis for understanding GEOINT to help plan and execute their assigned missions. This document also serves as a common frame of reference for the GEOINT Enterprise Community. As the highest level of doctrine for GEOINT, NSG Pub 1.0 is written at an unclassified level and in a manner that can be readily understood by consumers (non-producers) and new producers of GEOINT. Pub 1.0 also complements the doctrine, tactics, techniques, and procedures and guidance outlined in Joint Publication 2-03, *Geospatial Intelligence Support to Joint Operations*.

GEOINT doctrine is prepared under the auspices of the GEOINT Functional Manager (GFM). Executive Order (E.O.) 12333 "United States Intelligence Activities" (as amended in 2008), Section 1.3 (b) (12) (A) (iii), designates the Director of the National Geospatial-Intelligence Agency (NGA) as the GFM for the U.S. Intelligence Community (IC). The title of GFM encompasses the roles and responsibilities of the Department of Defense (DoD) GEOINT Manager, as defined in DoD Directive 5105.60 "National Geospatial-Intelligence Agency," and the IC Functional Manager for GEOINT, in accordance with applicable law and Director of National Intelligence (DNI) and DoD directives, guidance, and agreements. The GFM leads the National System for Geospatial Intelligence (NSG), as described in Chapter Five.

SCOPE.

This document supersedes *Geospatial Intelligence (GEOINT) Basic Doctrine Publication 1-0*, dated September 2006. As NSG community doctrine, it documents fundamental principles to guide the operation of the NSG and how it produces, maintains, and employs GEOINT. Pub 1.0 includes the legal definition of GEOINT, an overview of data used for GEOINT products, a basic understanding of GEOINT products, an understanding of the GEOINT professional work roles, and a description of the governance framework for the function of GEOINT. GEOINT is rapidly evolving to incorporate capabilities such as data analytics, artificial intelligence, machine learning, deep learning, and computer vision. However, these topics are beyond the scope of this introductory document.

APPLICABILITY.

Pub. 1.0 applies to the NSG, as defined in Chapter Five. It also applies to NSG Partners and the GEOINT Enterprise (also defined in Chapter Five), to the extent defined by their distinct roles. As doctrine, this publication is authoritative but not directive. It does not include policy or strategy but does serve as a foundational guide for the production, maintenance, and sustainment of GEOINT across the NSG Community.

OVERVIEW.

Chapter One presents the legal definition of GEOINT, including a description of its three complementary elements: Imagery, Imagery Intelligence, and Geospatial Information. Since the term GEOINT is used broadly to include the supporting aspects of GEOINT, the chapter also addresses areas that are critical to the function of GEOINT but not included in its definition.

Chapter Two addresses GEOINT data used to create each of the three elements of GEOINT and provides information on how that data is collected. The chapter includes a section that clearly delineates different types of collection platforms, sensors, and GEOINT phenomenologies, and lists the advantages and disadvantages of each type for various circumstances and purposes. Chapter Two also describes additional types of data used for imagery intelligence and geospatial information.

Chapter Three is focused on Products. This chapter describes how GEOINT products are developed using any combination of three types of layers—Geospatial, Mission, and Intelligence—and then explains how elevation, time, motion, and activity may be added to create a more dynamic, realistic, and comprehensive GEOINT product. For the purposes of this document, products are separated into three broad categories: Mission/Event Preparation, Assessment, and Detection. The chapter describes what each of those areas encompasses and provides multiple examples of products in each category to illustrate how they may be used to support specific mission requirements.

Chapter Four discusses GEOINT professionals and defines tradecraft areas. The chapter includes a chart with specific civilian work roles and corresponding military designations for GEOINT professionals.

Chapter Five describes the GEOINT Community, from the entire GEOINT Enterprise to its key elements such as the NSG—which includes U.S. Government GEOINT entities and activities—and the Allied System for Geospatial Intelligence (ASG). The chapter references authorities that designate the Director of NGA as the GEOINT Functional Manager and DoD GEOINT Manager, and outline GFM authorities and responsibilities. Chapter Five also describes GEOINT Community forums and the important role they play in helping the GFM to shape and guide the function of GEOINT.

Approved for public release, 18-142

CHAPTER ONE – WHAT IS GEOINT?

Geospatial Intelligence, also known as GEOINT, is defined by law in Title 10 of the U.S. Code, Section 467 (2005) as:

> **GEOINT:** "The term 'geospatial intelligence' means the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information."

Section 467 also provides definitions of the three elements of GEOINT:

- **Imagery.** A likeness or presentation of any natural or man-made feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems and likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means.

  Imagery includes handheld photography, but, within the context of GEOINT, "does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations."

- **Imagery Intelligence.** The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.

- **Geospatial Information.** Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the earth and includes: statistical data; information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data, and related products.

Title 10 U.S. Code, Section 442: MISSIONS

This section of the U.S. Code codifies NGA's national mission and addresses systems and tasking of GEOINT. Although the language does not define GEOINT, it provides additional context about the definition and is shown below to ensure awareness. Title 10, Section 442(a)(2) states:

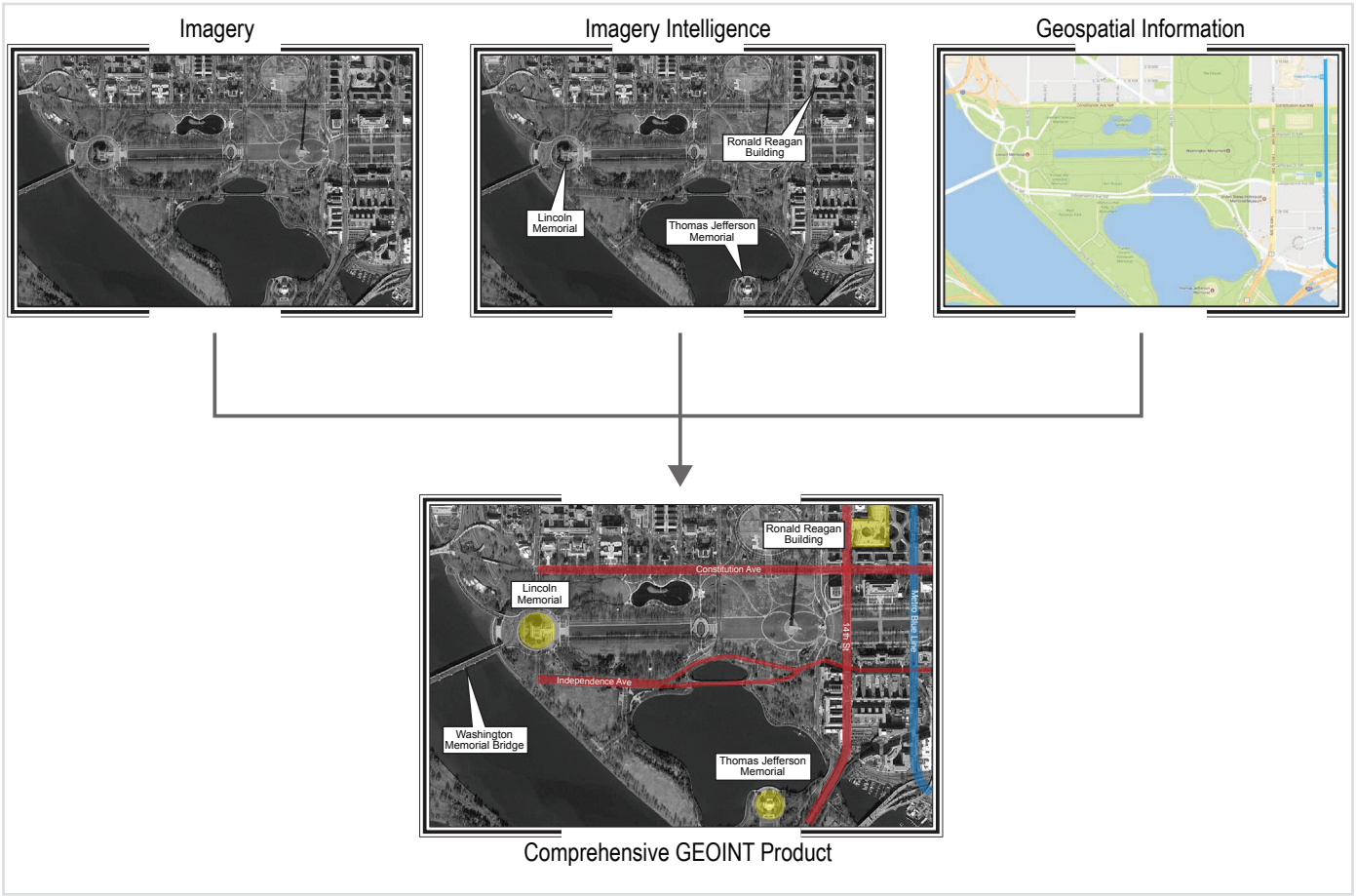
"As directed by the Director of National Intelligence, the National Geospatial-Intelligence Agency shall develop a system to facilitate the analysis, dissemination, and incorporation of likenesses, videos, and presentations produced by ground-based platforms, including handheld or clandestine photography taken by or on behalf of human intelligence collection organizations or available as open-source information, into the National System for Geospatial Intelligence."

"The authority provided by this paragraph does not include authority for the National Geospatial-Intelligence Agency to manage tasking of handheld or clandestine photography taken by or on behalf of human intelligence collection organizations."

Any one or a combination of the three elements, and/or the data used to create them, may be considered GEOINT. GEOINT data is described in Chapter Two.

The graphic below shows an example of each of the three GEOINT elements and the effects of combining all of them into a single product.

- The first frame in the graphic shows **Imagery**, which looks similar to a photograph.
- The second frame shows the same image with notational **Imagery Intelligence**, which refers to the analysis of the image or the information used to develop the analysis. For example, if analysis of the image indicated that the buildings shown are part of a factory used to make a particular type of weapon, that information would be considered imagery intelligence and noted on the image, as illustrated by the white callout boxes.
- The third frame depicts a map with **Geospatial Information,** which provides details— such as roads, transporation networks, location and shape of buildings, and elevation data.



NGA, Analytic Production & Design Center (ATC) Imagery Copyright 2017, DigitalGlobe

The large frame at the bottom is a comprehensive **GEOINT** product that combines all three components in a more informative and useful form to satisfy specific requirements/Essential Elements of Information (EEI)/Requests for Information (RFI) better than any of the individual components can when used separately.

Chapters Two and Three provide other examples of imagery, imagery intelligence, and geospatial information and related products.

Approved for public release, 18-142

Although the legal definition of GEOINT refers only to the **exploitation and analysis** of imagery and geospatial information—which includes processing and analyzing GEOINT data and the resulting products—there are many key areas that enable and are integral to the GEOINT function but are not part of the legal definition. These include training, architecture, data collection, technology, research and development, storage, and dissemination of GEOINT.

GEOINT DEFINITION: UPDATES AND AMPLIFICATION

Changes to the definition of GEOINT are not valid unless they are issued in U.S. Public Law, and amplifications of the definition are not valid unless they are issued or approved by the DNI or the Director of NGA.

Several documents provide amplifications to the 2005 Title 10 legal definition of GEOINT, in accordance with the guidelines stated above, but do not amend the definition provided in U.S. Code:

- The DNI issued a memo on 5 July 2005 that addressed details of what GEOINT collection activities and exploitation and analysis encompass as well as some specifics on what they do not include.
- The DNI issued a memo on 17 October 2005 that provided a detailed description of what "imagery" encompasses, including the capabilities formerly known as imagery-derived Measurement and Signatures Intelligence (MASINT) and Advanced Geospatial Intelligence (AGI).

Language from the unclassified documents, as well as the corresponding language in DoD Directive 5105.60, is provided in Appendix B.

CHAPTER TWO – DATA

This chapter describes the major categories and sources of data for all three elements of GEOINT: Imagery, Imagery Intelligence, and Geospatial Information.

1. IMAGERY

This type of GEOINT Data is collected by a system of sensors and platforms. Sensors collect the data, and platforms are the vehicles or objects to which sensors are attached. The sensor or platform used depends on the type of data to be collected, the conditions in which it is collected, and the purpose for which it will be used. The range of platforms and sensors are described below.

PLATFORMS: This section addresses satellite, aircraft, ground-based, and sea-based platforms. Aircraft, drones, aerostats, balloons, and dirigibles are referred to as *airborne* platforms. Airborne, ground-based, and sea-based platforms may be manned or unmanned/unattended.

Satellites – Imagery data is collected from space by two satellite sources: Government-owned satellites and private industry-owned satellites, known as *commercial systems.* U.S. Government satellites are used for both unclassified and classified purposes. Satellites orbit at a far higher altitude than airborne platforms, enabling them to collect above any airspace, including sovereign airspace of any nation, hostile territory, and areas to which airborne platforms are denied access.

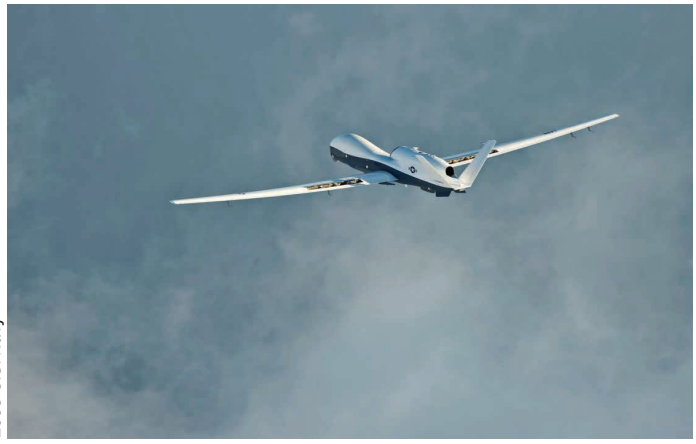
NGA

Government and Commercial

Government Systems – Sensors attached to government systems are a significant source of GEOINT data used for intelligence and national security purposes. These systems are employed when the government needs discretion in when or where it collects the data. They are used for more sensitive data collection and circumstances. Note that E.O. 12333 restricts U.S. Government systems from imaging U.S. persons.

Commercial Systems – The sensors attached to these vehicles produce unclassified data. The U.S. Government uses unclassified commercial data whenever possible, and increasingly is using commercial systems as a primary source of data. In addition, products derived from commercial system data can be more easily shared with government and military organizations outside the intelligence community, non-governmental organizations (such as non-profit relief organizations), private industry partners, foreign allies, and other foreign nations.

Approved for public release, 18-142



2008 U.S. Navy

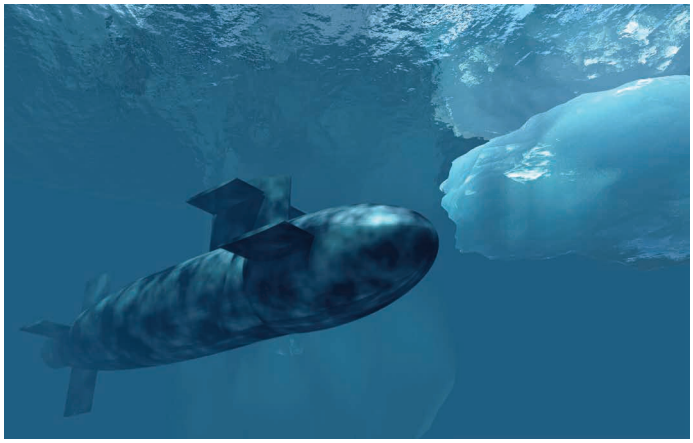
Airborne

Airborne platforms consist of manned, unmanned, fixed wing, and rotatory aircraft, as well as balloons and dirigibles. The sensors and cameras mounted on airborne platforms can provide continuous (known as *persistent*) coverage of a location or target. U.S. Government airborne platforms can often be employed more rapidly than satellites in part because military regional combatant commanders have authority over the platforms, and can re-task the platform in near real time, as required. The effectiveness of airborne GEOINT collection can be limited, however, by denied or contested airspace and adverse weather or atmospherics.

Department of Defense

Ground-based

Ground-based platforms are stationary or moving objects on or beneath the ground that have a camera or sensor attached. These platforms may be manned or unattended. The platforms can be as simple as a pole in the ground, a building, a vehicle, or a human taking photographs (known as *hand-held photography*).



Thinkstock

Sea-based/Maritime

Sea-based platforms include ships, underwater survey vessels, submarines, or buoys. They carry cameras or sensors that may be above or below the surface of the water. The platforms may be manned and unmanned.

PLATFORM CHART

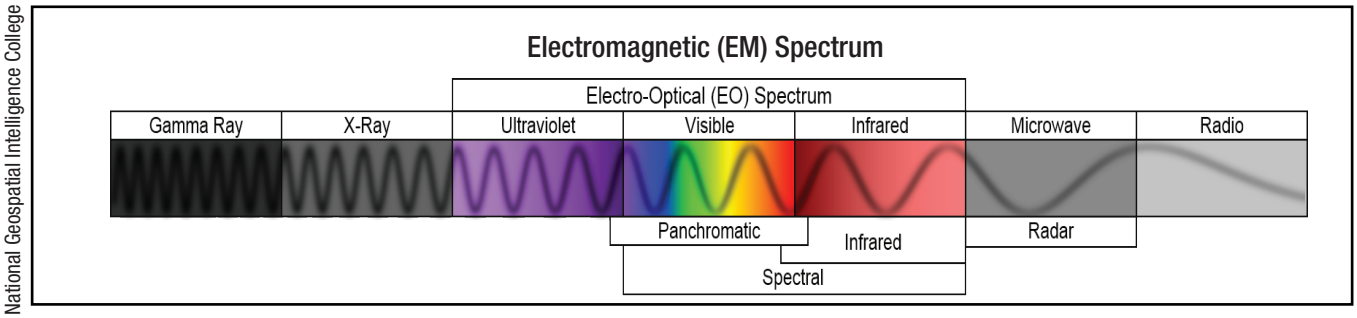
This chart provides examples of common satellite, airborne, sea-based, and ground platforms, and discusses the basic advantages and disadvantages of using each.

PLATFORM TYPE	EXAMPLES	ADVANTAGES	DISADVANTAGES
Satellite – (Government)	LANDSAT GOES-R	• Global coverage/access • No cost to most users for data • Data is in Government control	• Limited collection opportunities • Limited persistent coverage of target/area • Competition for tasking priority
Satellite – (Commercial)	GeoEye-1, Worldview 1/2/3/4 Radarsat 2	• Global coverage/access • Unclassified - easily releasable • Avoids competition with higher priority IC requirements	• Competition w/ other consumers • Slower availability of products • Tasking/acquisition information generally not secure
Airborne – High Altitude (manned)	U-2/Dragonlady	• Moderate duration/persistence • Rapidly re-tasked under Theater Commander control • Wider sensor area of coverage • Can carry variety of sensors	• Less persistence than possible with UAV • Limited collection into hostile/denied airspace
Airborne – High Altitude (unmanned aerial vehicle, or *UAV*)	RQ-4/ Global Hawk MQ-4/Triton	• Very long duration; persistent surveillance • Rapidly re-tasked under Theater Commander tasking control • Moderate sensor area of coverage	• Limited collection into hostile/denied airspace
Airborne – Medium Altitude (manned)	P-3/AIP	• Moderate duration/persistence • Moderate sensor field of view/range from platform track • Rapidly re-tasked under Theater Commander tasking control • Can carry a variety of sensors	• Less persistence than possible with UAV • Very limited collection into hostile/denied airspace
Airborne – Medium Altitude Long Endurance (MALE), UAV/RPV**	MQ-1/Predator MQ-9/Reaper RQ-7/Shadow MQ-5/Hunter MQ-1C/Gray Eagle	• Long duration; persistent surveillance • Rapidly re-tasked under Theater Commander tasking control	• Narrow field of sensor view • Very limited sensor range from platform • No collection (or high risk) in hostile/denied airspace, A2AD* environment.
Ground	Buildings, Poles, Vehicles, People, Unattended Ground Sensor (UGS)	• High resolution/detail possible • Long duration availability • Less expensive than most other types of platforms • 24-7, open source coverage	• Difficult placement/access in A2AD* environment • Very limited sensor range • Authentication
Sea	Ships, Buoys, Submarines	• Underwater imagery, topography • High-resolution bathymetry	• Limited to good sea conditions • Narrow sensor swaths

Graphic Credit: GEOINT Enterprise Office

*Anti-Access/Area Denial
**Unmanned Aerial Vehicle or Remotely Piloted Vehicle

Approved for public release, 18-142



Portions of the Electromagnetic Spectrum used for Phenomenologies

SENSORS: The two primary categories of sensors are electro-optical (EO) and radio detecting and ranging (radar), and both have several types or variants, known as phenomenologies. Each phenomenology achieves different results with the data. Descriptions of sensor characteristics and phenomenologies are listed below. At the end of this chapter, we discuss how sensors are used to capture and characterize motion.

ELECTRO-OPTICAL (EO)

EO derives data from the ultraviolet through the infrared portions of the electromagnetic (EM) spectrum. Each part of the EM spectrum provides a different representation of the object imaged, depending on the sensor phenomenology used. EO sensors are passive (with the exception of light detecting and ranging, or lidar, described below), which means they use natural EM energy sources such as the sun, naturally occurring radiation, or emitted heat. They generate data by capturing the reflected or emitted electromagnetic energy from an object. These sensors, which operate only in a passive or "receive" mode,* do not emit energy. This factor diminishes the adversary's ability to detect whether they are being imaged. The effectiveness of electro-optical sensors can be degraded or denied by adverse weather, light conditions, and atmospherics.

*Except Lidar

EO PHENOMENOLOGIES

PANCHROMATIC IMAGING (PAN)

Copyright 2008, DigitalGlobe

PAN uses the visible part of the EM spectrum, along with a portion of IR spectrum, and produces an image similar to a black and white aerial photograph. The images can provide a very detailed and accurate likeness of an area or object, and can show shadows and other distinguishing features that help identify characteristics of an object or environment.

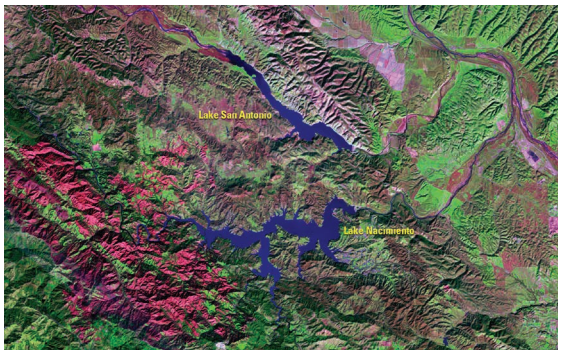
INFRARED (IR)

USGS

IR uses the infrared part of the EM spectrum to detect heat and radiance/reflection, and displays that information in a gray-scale image.

Thermal Infrared (TIR) – TIR is similar to IR, but it uses different wavelengths of the infrared spectrum to indicate the temperature of objects or radiated/reflected heat. The shape and size of the object or environment emitting energy (heat) is shown as a different shade than the rest of the image. Cooler objects appear darker, warmer objects appear lighter, and hot objects appear bright white.

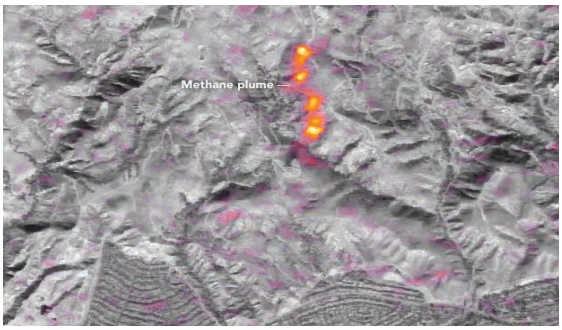
MULTISPECTRAL IMAGING (MSI)



USGS

MSI provides a color image by using tens of additional bands of the visible and infrared portions of the spectrum. It also provides more detail to images, showing characteristics that are not otherwise visible. The bands can be combined in various ways to highlight different manmade or natural features.

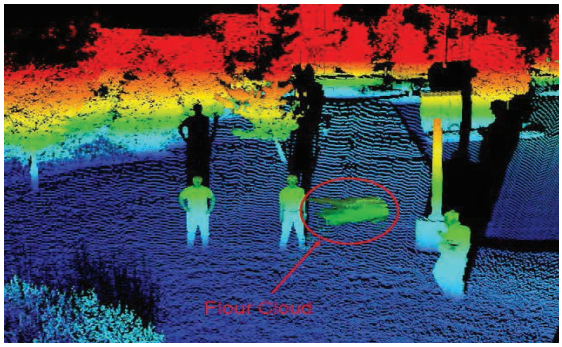
HYPERSPECTRAL IMAGING (HSI)



NASA

HSI is similar to MSI but uses hundreds, rather than tens, of bands of the visible and infrared portions of the EM spectrum. These extra bands can provide greater fidelity and characteristics of an object than MSI. For example, HSI allows users to detect materials by their unique spectral signature.

LIGHT DETECTION AND RANGING (LIDAR)



NGA Office of Corporate Communications

Lidar uses laser pulses in the visible and infrared portions of the EM spectrum. The sensor emits a pulse of laser light toward an object, which reflects back some of the energy to the sensor. The time it takes for the energy to return provides information that helps identify many characteristics of an object and the environment, including distances and heights. For example, shorter roundtrips indicate higher elevations and longer roundtrips indicate lower elevations. The process can be used to develop three-dimensional models of an object, such as a building.

Approved for public release, 18-142

OVERHEAD PERSISTENT INFRARED (OPIR)

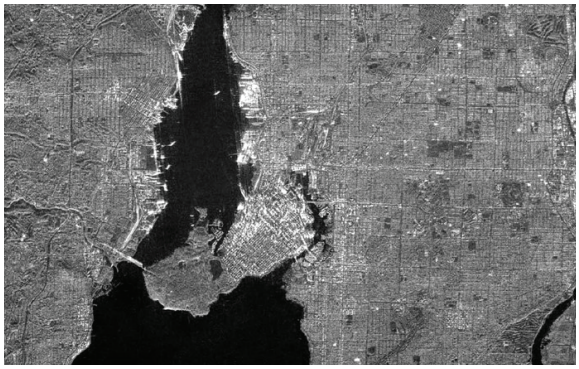
OPIR combines several EO sensor phenomenologies described above to create a unique collection capability that detects energy radiation from tactical and strategic targets and allows continuous (known as persistent) coverage of a mission area. OPIR can detect energy radiance in the visible and near infrared, short-wave infrared and mid-wave infrared parts of the spectrum to characterize energy as an event or process it as a scene.

RADAR

Radars are active sensors that emit manmade electromagnetic energy to illuminate the environment or object they are imaging, and then use the characteristics of the response to create an image. These sensors use reflected radar energy to illuminate objects in day or night and in almost any weather conditions. A radar image is non-literal, which means it does not appear as a photo that shows an exact likeness of an object or environment. It is similar to an X-ray of an area or object, with the ability to detect characteristics that a literal picture would not show. An important feature is that it can be used for poor light and weather conditions in which EO technologies are less effective.

RADAR PHENOMENOLOGIES

SYNTHETIC APERTURE RADAR (SAR)



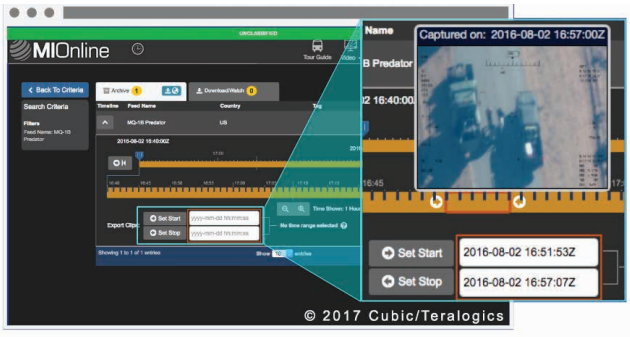
Copyright 2008, Macdonald, Dettwiler & Associates

SAR illuminates objects with pulses of microwave energy. It applies signal processing to a series of many pulses to produce imagery.

Interferometric SAR (IFSAR) – IFSAR uses a SAR sensor to observe a location from two separate positions. This method generates elevation data of the Earth's surface.

MOTION GEOINT

Both EO and radar sensors can create or capture motion by collecting multiple frames over a short period of time. This activity is known as Motion GEOINT. The most common types of Motion GEOINT include the following:



Search

Full Motion Video (FMV) – FMV uses many frames per second to create a near-real-time video capability, which may be displayed as visible or IR and may be recorded by digital or analog means. This near-real time capability allows observation of rapidly developing events and is a valuable tool for ongoing operations. It also provides continuous observation of an object, such as a person or vehicle, to analyze its patterns over long periods.

Moving Target Indicator (MTI) – This predominantly radar capability shows only those objects that are in motion and provides information on the speed and direction that objects are moving. Some EO sensors can detect motion in a small area but generally are not considered an MTI capability.

Wide Area Motion Imagery (WAMI) – A set of motion imagery sensors with a wide field of view (FOV) diameter of up to 8 km, which provides continuous surveillance of a broad area.

FMV, MTI, and WAMI are primary sources of collection that allow persistent coverage of a target or area. All three enable forensic backtracking of kinetic events, network analysis, pattern of life (PoL) studies and security monitoring. Motion imagery is also a key enabler of Activity Based Intelligence, as discussed in Chapter Three.

SENSOR & PHENOMENOLOGY CHART

SENSOR/PHENOMENOLOGY	ACRONYM/ SHORT FORM	CHARACTERISTICS	USED FOR (EXAMPLES)
ELECTRO-OPTICAL SENSOR	**EO**	**Typically a passive sensor, uses natural energy sources, ultraviolet through infrared portions of EM spectrum**	**For detailed, literal, photo-like picture of a scene and the objects within it.**
PANCHROMATIC	PAN	Uses the visible section of the spectrum to create black and white (grayscale) images.	Provides a literal picture of a scene, area, and/ or objects. Used in daytime, good weather conditions.
INFRARED	IR	Uses the infrared portion of the spectrum to detect heat/ radiance.	Detects presence of living entities and active vehicles and equipment in day or night. May be limited by bad weather/light conditions, smoke.
• Thermal Infrared	TIR	Uses infrared portions of the spectrum to indicate temperature level of heat/radiance.	Determines operational status of equipment, factories, and nuclear facilities. Penetrate smoke, track activities at airfields, ports, etc.
MULTISPECTRAL IMAGING	MSI	Uses tens of visible ***and*** infrared bands to provide a color image with more detail.	Sees beneath the water; detects camouflage, vegetation density and cover type, mineral, soils, and material analysis; illuminates shadowed material.
HYPERSPECTRAL IMAGING	HSI	Uses hundreds of visible ***and*** infrared bands to provide a greater detail and additional characteristics.	Same as multispectral but with greater levels of detail.
LIGHT DETECTION & RANGING	Lidar	Uses laser pulses in the visible and infrared sections of spectrum.	See objects beneath vegetation canopy, battlefield visualization
OVERHEAD PERSISTENT INFRARED	OPIR	Uses visible and near infrared bands. Characterizes energy as an event, processes as a scene.	Provides persistent coverage. Detects missile launches, wildfires, hostilities, volcanos, and identifies weapons.
RADAR SENSOR	**Radar**	**Active sensor, emits manmade energy sources, uses microwave and radio wave portions of EM Spectrum.**	**Unlike EO, can be used in most weather, day or night.**
SYNTHETIC APERTURE RADAR	SAR	Illuminates objects with microwave energy pulses. Applies signal processing to a series of pulses to produce a single image.	Penetrates foliage, material, and ground (with limitations), detects barriers and overhead power lines. Used in most weather, light conditions. Creates a black & white (grayscale) image.
• Interferometric SAR	IFSAR	Uses SAR sensor to observe from two separate positions to generate elevation data of the Earth's surface.	Identifies elevation data.

Adapted from graphic in U.S. Army Doctrine ATP 2-22-7 "Geospatial Intelligence," March 2015 – Appendix C

Approved for public release, 18-142

2. IMAGERY INTELLIGENCE

Imagery intelligence data is produced during analysis of the imagery and geospatial data. The data may be derived from analytic expertise, classified data, unclassified information, analysis techniques, or any combination of those sources. For example, an analyst may determine that two objects on an image are foreign aircraft from a specific country based on expert knowledge of foreign aircraft. The analyst may then use unclassified publications to determine the exact nomenclature of the aircraft and review classified intelligence reporting to assess whether this is the first appearance of such aircraft in this location and if the arrival of the aircraft is related to military or political activity in the area. The analyst might also employ analysis techniques to determine other information about the aircraft, location, or arrival details.

3. GEOSPATIAL INFORMATION

Geospatial Information is derived from data collected through many different sources including: platforms and sensors used for imagery data; subsurface sensors, such as sonar (sound navigation and ranging) attached to water-based platforms including ships, submarines, and buoys; ground sensors, such as seismic, attached to land-based platforms such as vehicles, stationary poles, or humans; and open source information, such as population.

Geospatial Information can be separated into seven major categories, as described below.

Aeronautical: Safety of Navigation information such as vertical obstructions, no-fly zones, flight routes, approach procedures, airfield infrastructure and layout, and aeronautical charts.

Maritime: Safety of Navigation information such as shipping routes, underwater obstructions, sailing restrictions, port infrastructure and layout, approach procedures, and nautical charts.

Topographic: Safety of Navigation information such as trafficability and obstacles to movement, and other ground/surface feature-related information including infrastructure (roads, power grids), man-made features, population data, vegetation, and hydrography. Topography may also include connectivity of network elements within a geospatial database that allow for ground-based routing, navigation, and hydrology flow.

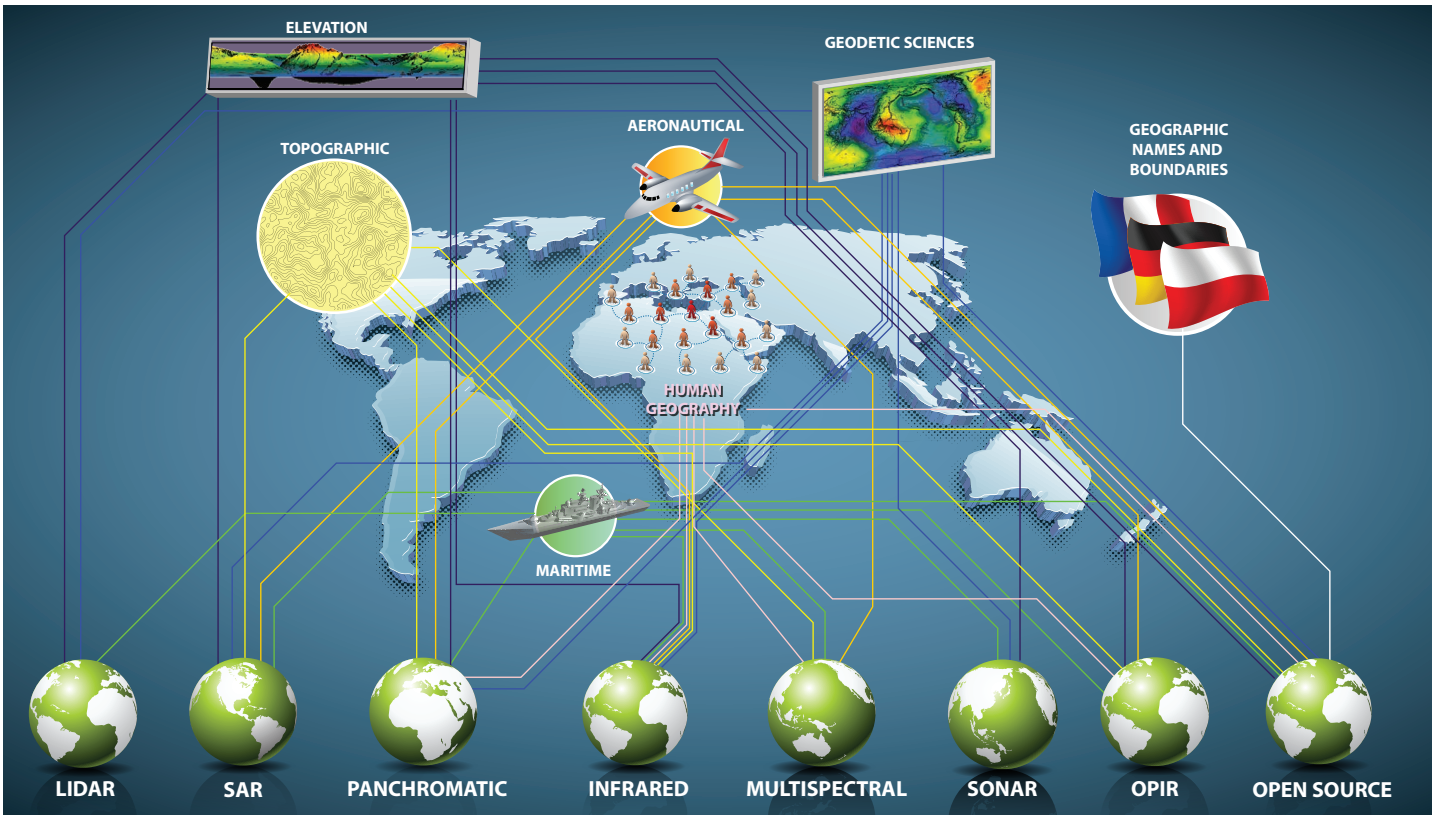
Elevation: Information about the height of objects on or in relation to the Earth. Elevation data includes heights of objects above the surface of the Earth (spaceborne and airborne), on the surface of the Earth (buildings and physical relief), and below the surface (bathymetry and underground facilities).

Human Geography: A social science discipline based on analyzing the interconnections between people and places, including patterns of human activities, in the context of their environment. It also seeks to explain how actions taken in one place/population can impact another place/population. Human Geography includes sub-disciplines such as: population geography, political geography, cultural geography, and religious/ethnic geography. It may include both classified and unclassified information.

Geographic Names and Boundaries: Names and boundaries of cities, towns, provinces, regions, states, and countries. Identification of major landmarks, facilities, and buildings.

Geodetic: Magnetic and gravimetric data (which have an impact on geo-positional systems), navigation tools, surveying, and systems of map grids and coordinate systems.

NOTE: The combination of these seven categories and a category called “Controlled Imagery,” may be referred to as “Foundation GEOINT.”



National Geospatial Intelligence College

Sources from which Geospatial Info usually is requested

DATA SOURCE	AERONAUTICAL	MARITIME	TOPOGRAPHIC	HUMAN GEOGRAPHY	GEOGRAPHIC NAMES & BOUNDARIES	ELEVATION	GEODETIC SCIENCES
PANCHROMATIC	X	X	X	X	X	X	X
MULTISPECTRAL	X	X	X	X	X		
INFRARED	X	X	X	X		X	X
SAR	X	X	X			X	X
LIDAR	X	X	X			X	X
SONAR		X				X	X
OPIR	X	X	X	X		X	
OPEN SOURCE	X	X	X	X	X	X	X

(Adapted from a graphic by the National Geospatial Intelligence College)

Approved for public release, 18-142

CHAPTER THREE – PRODUCTS

GEOINT products enable the visualization and geo-location of intelligence gathered from intelligence disciplines, known as INTs, as well as information from non-intelligence sources. Products range from simple to advanced, depending on the type and amount of information used, level of analytic complexity, and use of different processing techniques. Sometimes, a simple product, such as a map or image with annotations, may be all that a user needs. In some cases, a more sophisticated product is required in order to provide the type of information or level of detail needed to accomplish a mission or answer a question. In the first section, we will describe GEOINT products, from the most basic form through the most advanced. The second section "Product Examples & Applications" will show a variety of products and provide examples of how they are used for different missions and purposes.

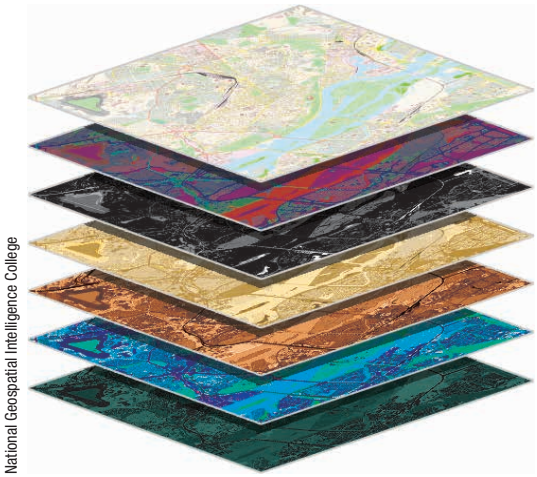
BASE PRODUCTS

The foundation (first layer) of a GEOINT product may consist of any one or combination of the GEOINT components described in the Section "What is GEOINT?" This foundation usually* is a map or image of a specific location and shows visible terrain, objects, and other features in that location. GEOINT images and maps are unique because they can display highly accurate geo-coordinates of the location, as well as additional information on objects or features depicted.

*As noted earlier, data is used to create a product. But in some cases, the processed data itself is the product. For example, certain forms of data are used to create a product called a Digital Point Positioning Database, which is used to derive digital information that is fed directly into weapons systems to ensure accuracy. However, to simplify the explanation of GEOINT products, this section focuses on describing how products are created using maps and images as a foundation.

LAYERING

Different types of information can be layered onto the foundation to provide more detail and context. However, the information must be geospatially referenced, meaning that it is shown in the precise location, within the exact associated grid coordinates, that it appears on the image or map. There is a wide variety of information that can be added to customize the image for its intended purpose, as described below.


National Geospatial Intelligence College

GEOSPATIAL LAYERS: Comprise geospatial information including boundaries, infrastructure (such as sewer lines, power grids), elevation data, geodetic data, human geography data (population, cultural, political/religious geography), safety of navigation data, and identification of key facilities and natural or manmade features.

MISSION LAYERS: Provide general information relevant to the purpose and area for which the product is being used. The information may include weather conditions and climate, logistics data, locations of friendly forces, routes and alternatives, characteristics of the local terrain, population and government information, and other data obtained through commonly used, unclassified sources.

INTELLIGENCE LAYERS: Customize products for a specific mission or purpose and consist of information derived from various intelligence sources, or a combination of those sources. Examples include locations of friendly and enemy forces, presence of chemical or biological hazards, weapons facilities, routes and alternatives, and potential targets. GEOINT serves as a base for the depiction of data from other intelligence disciplines (INTs), each of which is described below. (These are user-friendly descriptions approved by the agencies responsible for each INT. They are not the official definitions in law.)

- Human Intelligence (HUMINT) – Intelligence obtained through clandestine or overt HUMINT activities, or operations and activities utilizing human sources or other human assets.

- Imagery Intelligence (IMINT) – The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.

- Signals Intelligence (SIGINT) – A form of technical intelligence derived from the exploitation of foreign electronic emissions. SIGINT can be in the form of the actual information content of a signal or in the form of its temporal and spectral characteristics, called signal operating parameters. SIGINT includes both the raw data and the analysis product of that data. This category of intelligence includes all Communications Intelligence, Electronic Intelligence, and Foreign Instrumentation Signals Intelligence.

- Measurement and Signature Intelligence (MASINT) – Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data. MASINT, which is derived from specific technical sensors, identifies distinctive features associated with the source, emitter, or sender. It can measure physical characteristics of targets and events of interest to determine composition, location, and/or performance.

- Open Source Intelligence (OSINT) – Intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.

Conflation or adding one or more of these layers to a GEOINT product is considered *Multi-INT*, which means that input from at least one additional INT was used to provide as much context as possible to a GEOINT product depicting a specific object, area, or activity. Multi-INT GEOINT should not be confused with all-source intelligence, in which data and products from all INTs are used to provide a comprehensive strategic assessment. Even the most comprehensive Multi-INT GEOINT product may only be one part of an all-source analysis subject, such as a matter spanning multiple regions, networks, or governments or an issue that involves strategic relationships and intentions.

ADVANCED ANALYTICS: ELEVATION, INTERACTION, AND ACTIVITY

Analysts may introduce any of the following elements to create a more dynamic, realistic, and advanced GEOINT product.

Elevation: The majority of GEOINT products use one or more of the layers described above. However, a more sophisticated product can be developed by adding elevation to create a three-dimensional (3D) model or simulation that provides a more realistic representation of an environment or object.

Time: The element of time can be used to create temporal products. These products can simulate factors such as speed, tides, wind direction, and changing daylight to help the analyst determine how each factor will affect a mission or event.

Motion: Location, elevation and time can be combined to create a virtual, interactive scene that allows users to familiarize or train in a simulated environment before operating in a real situation. Such simulations also allow analysts to experience different perspectives from which to analyze objects and scenarios.

Activity: Most GEOINT analysis and products focus on providing as much information as possible about a specific object or area. However, activity-based analysis examines human, vehicular, and other activity related to that object or area, which can lead to different areas and show correlations between areas, people, and objects. This method allows for a more complex level of analysis. Three processes that contribute to activity-based analysis are listed below.

- **Object-Based Production (OBP):** OBP is the standardized IC process in which observations from sensors are captured, structured, stored, and shared. The process also brings together information from all available sources of intelligence—and from systems of different security levels—related to an object. Thus, the most comprehensive and up-to-date information is available to everyone at the same time, and analysts from any location or organization can rapidly access the data. Examples of objects include natural features, people, vehicles, buildings, and events.

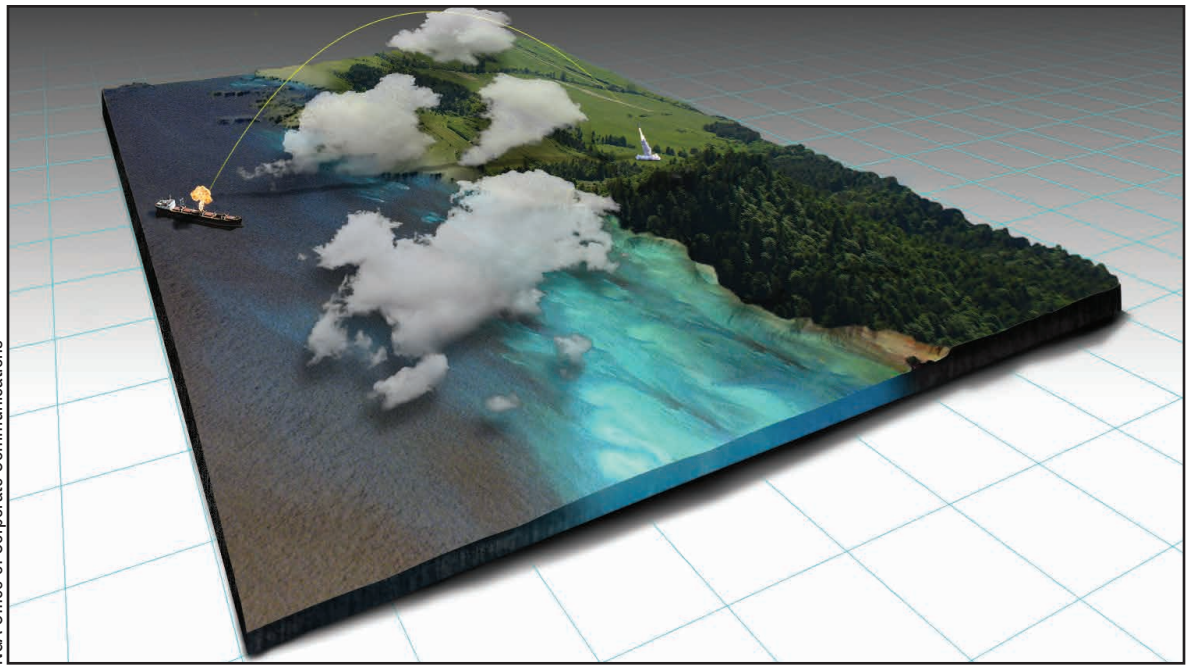
Approved for public release, 18-142

- **Structured Observation Management (SOM):** SOM is the method in which GEOINT observations from satellites and sensors and other sources are captured, structured, stored, and shared in a standardized format compatible with the OBP format. This ensures that GEOINT information can be integrated into the IC's OBP process.

- **Activity-Based Intelligence (ABI):** ABI is a methodology that incorporates the OBP information into a process that can detect when the object changes or activities related to an object occur, and then provide an electronic "alert" to analysts interested in that object. By examining this new information about the object, analysts can discover relationships with other objects or locations and detect patterns of activity and behavior.

PRODUCT EXAMPLES AND APPLICATIONS

A wide variety of products can be created to satisfy specific mission requirements by using different types of data, data processing, or analysis. Most products provide a common, accurately geo-located visualization of a scene or environment to enable planning and collaboration among different organizations. In this section, we will provide examples of products grouped in categories that are related to the overall missions and purposes for which the products are used: Mission/Event Preparation, Assessments, and Detection.



NGA Office of Corporate Communications

3D Simulation that incorporates elevation, time, and motion.

Mission/Event Preparation – Used to prepare for a mission, operation, or major event. These products focus on familiarization with the area, including identification of key landmarks and existing or potential hazards. They usually are map or imagery products that facilitate safety of navigation by identifying elements such as buildings, routes, water depth, terrain features, obstacles, and threats. The products assist with activities such as route planning and security preparations.

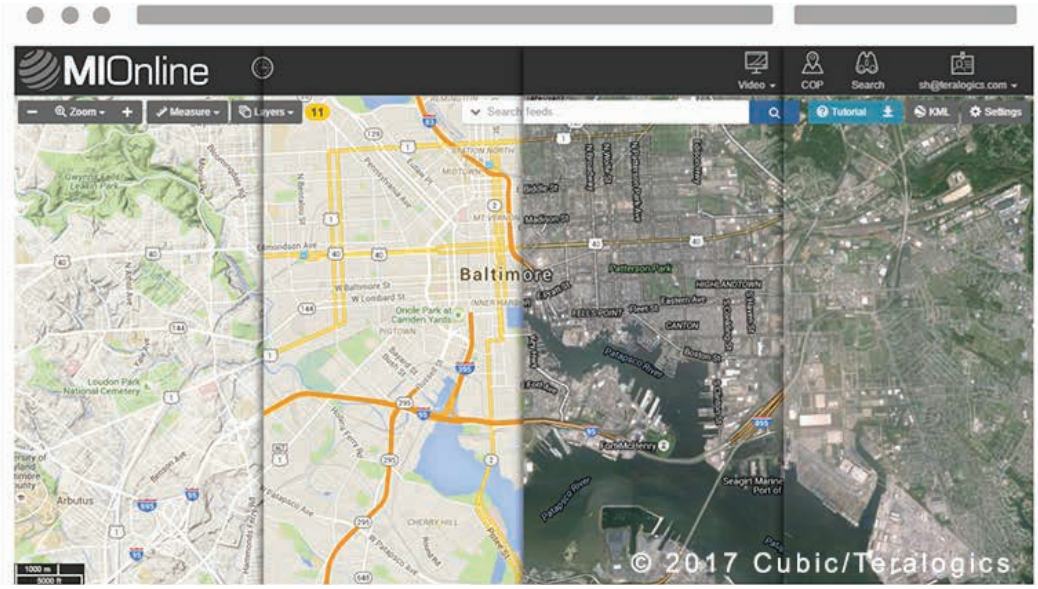
Assessment – Provide analysis for what is shown in an image or on a map, and provide information on the "who, what, when, where, how, and why," usually in the context of the purpose or mission for which it has been developed. Such products may be a simple image of a facility and parking lot, with notations that indicate the type of facility, information on how many cars are parked there now compared with the usual volume, and an assessment of how many people may be in the facility and what types of activities they may be conducting. A more complex product may show a hazardous material leak, with notations on potential effects over time using variable factors such as wind speed and tides.

Detection – Designed to find natural and manmade materials that are not visible or easily identifiable to the human eye. A variety of EO or radar sensor phenomenologies and specialized data processing techniques are used to develop detection products. These products may be used for many purposes, such as to "see" beneath foliage and camouflage or identify heat and other emissions.

PRODUCT EXAMPLES AND APPLICATIONS

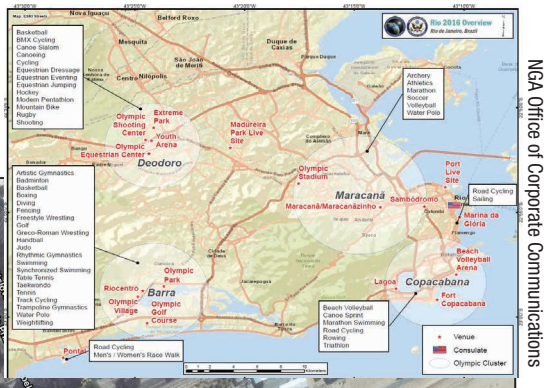
Below are examples of products for each of the categories described above.

MISSION/EVENT PREPARATION



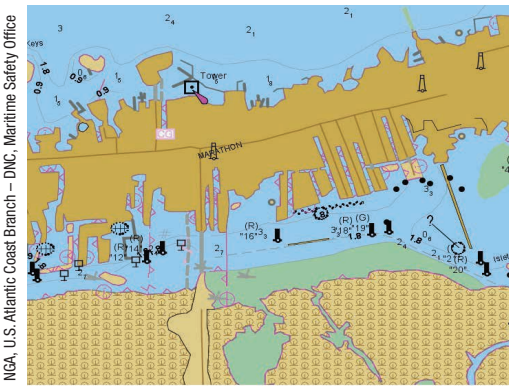
Map Overlays

Products such as map overlays and digital nautical charts are used to analyze locations for potential security threats and emergency operations, well in advance of a major event or VIP visit. Examples include the beach volleyball venue for the 2016 Olympics in Rio, Brazil, and the stadium area for the Super Bowl in Jacksonville, Florida.



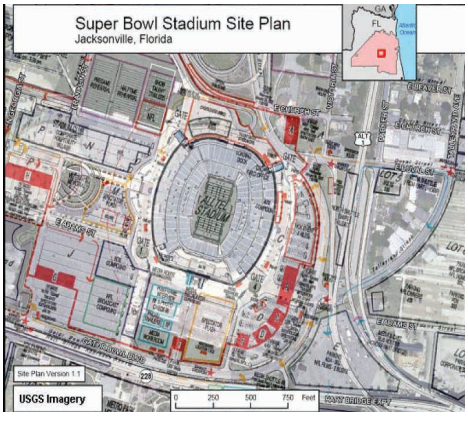
NGA Office of Corporate Communications

2016 DigitalGlobe, NextView License



NGA, U.S. Atlantic Coast Branch – DNC, Maritime Safety Office

Digital Nautical Chart



USGS image

Annotated Image
National Security Special Event (NSSE)

Approved for public release, 18-142

ASSESSMENTS

2015 DigitalGlobe NextView License

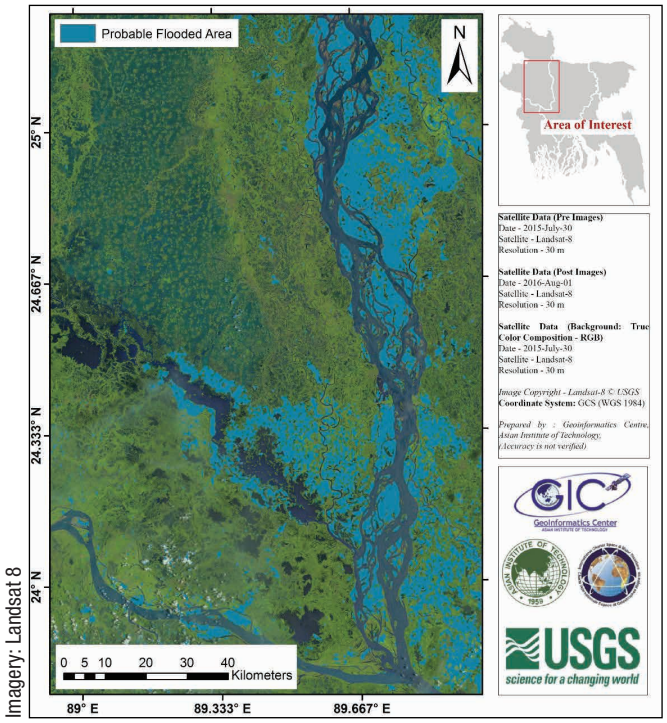
This example is from the 2015 earthquake in Nepal. On the left is an image from before the earthquake and on the right is an image after the earthquake. Analysts compared the two images to identify damaged structures, accessible roadways, and internally displaced persons. The results of that analysis were sent to the U.S. State Department, which provided the information to first responders and NGOs assisting in the recovery effort.

2015 DigitalGlobe NextView License

This image shows two separate camps for persons displaced after the earthquake. Analysts estimate the number of displaced persons in this area by counting the number and size of the tents. This information allows the State Department to determine the appropriate amount of food, water, clothing, and other supplies or support the affected people may need.

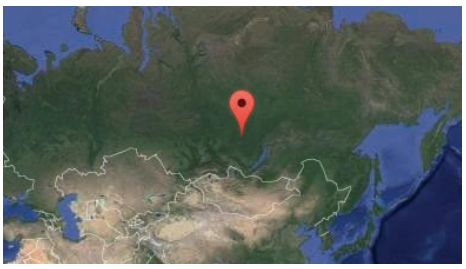
Flood inundation along the Brahmaputra River in Bangladesh

Over 3.2 Million people were affected by flooding in Bangladesh with 250,000 houses fully or partially damaged and 25,000 people displaced.

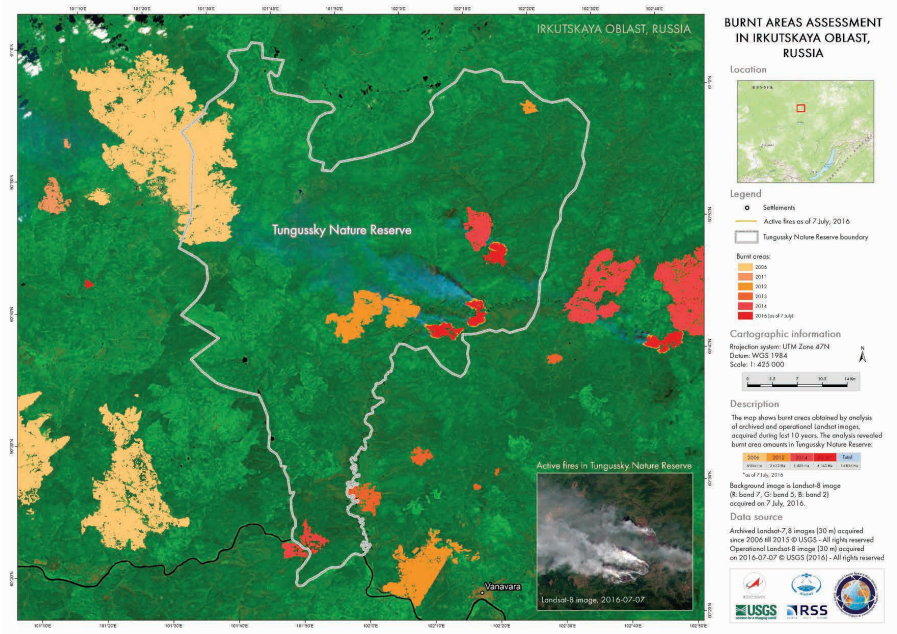


A total of 38 people have drowned since flooding began on July 25, 2016.

Burnt areas assessment in Irkutskaya Oblast, Russia



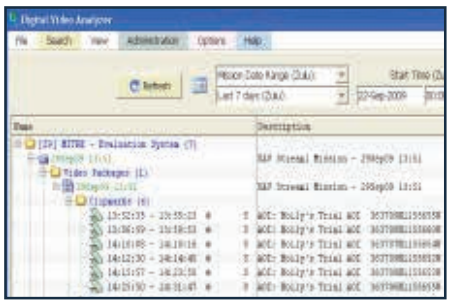
The Siberian Wildfires were triggered by lightning in late June and burned around 3,000 hectares.

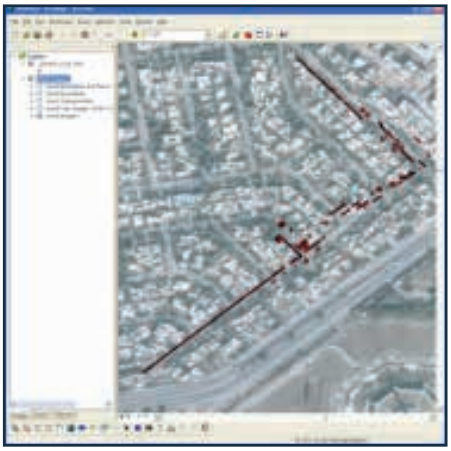


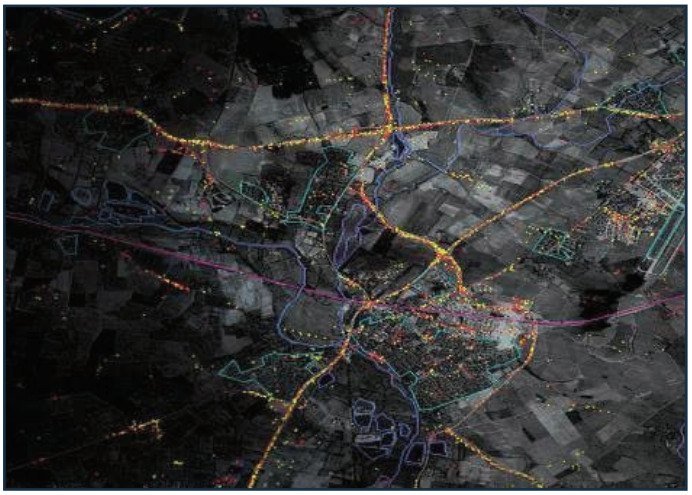
The fires were located in remote areas and did not pose a threat to inhabited areas at the time.

Approved for public release, 18-142

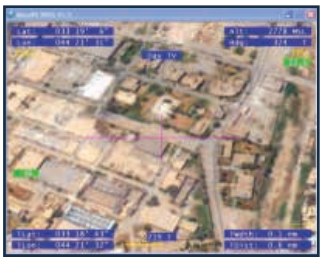
DETECTION

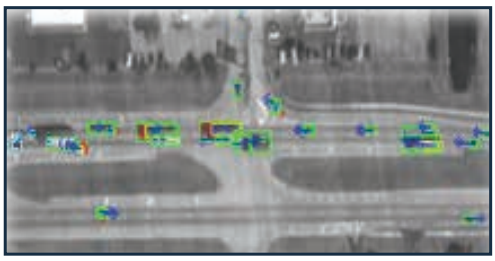






JSTARS image (DoD)





This Activity Based Intelligence (ABI) product illustrates how information extracted from large-scale data (also called *big data*) can be used to detect activity, patterns, networks, and anomalies. The NSG increasingly is using automation, which serves as a framework for advancing GEOINT to its future state.

Copyright 2014, 2016, DigitalGlobe

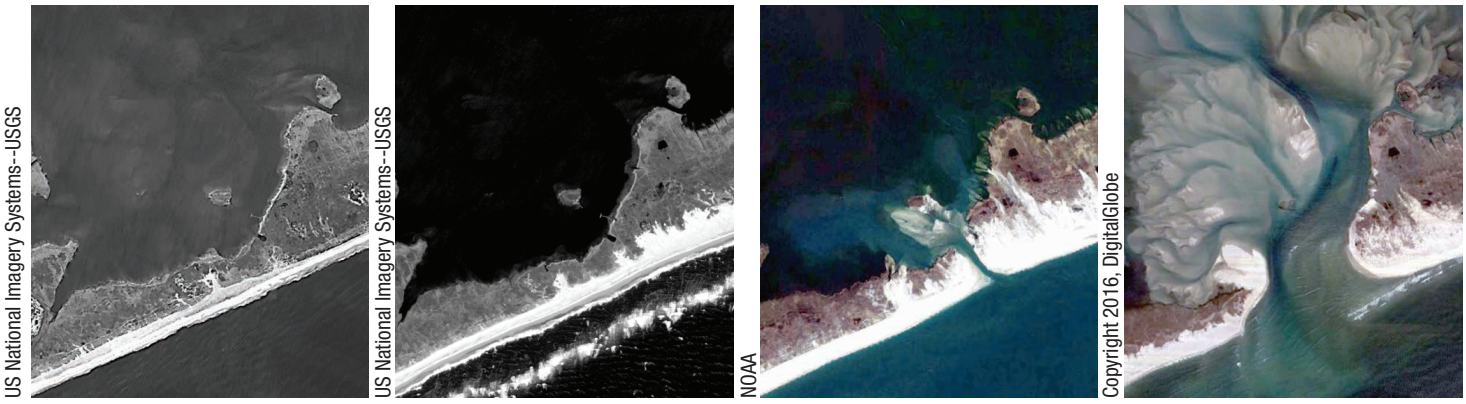
FEB. 15, 2014

DEC. 6, 2014

APRIL 1, 2016

Spratly Islands, South China Sea

Construction of man-made island reefs with pumped sand is documented by DigitalGlobe's satellites over a period of 25 months. Change detection using EO sensor.



Fire Island National Seashore, New York
Five Global Fiducial Program (GFP) time series images showing changes that occurred at Fire Island National Seashore, New York during the 17+ year period from March 1999 to May 2016. The GFP uses imagery from multiple sources to document dynamic Earth processes and change.

PRODUCT STORAGE, DISSEMINATION, AND ACCESS

GEOINT data and products are accessed by or delivered to producers and users via storage and dissemination systems. The system used may depend on the classification level of the data or products, type of sensor platform used to obtain the data, level and type of organization that produced the products, or whether hardcopy or electronic versions are needed. There are numerous national, military, and commercial GEOINT libraries for GEOINT data and products. However, the Director of NGA, as the GFM, established the NSG Consolidated Library (NCL) for long-term, large-volume storage of GEOINT data.

Traditionally, products were "pushed" to users via a variety of dissemination systems. However, with the advancement of technology, users may readily access many repositories themselves and can select and independently "pull" the specific data or products they need from storage systems.

Approved for public release, 18-142

CHAPTER FOUR – TRADECRAFT

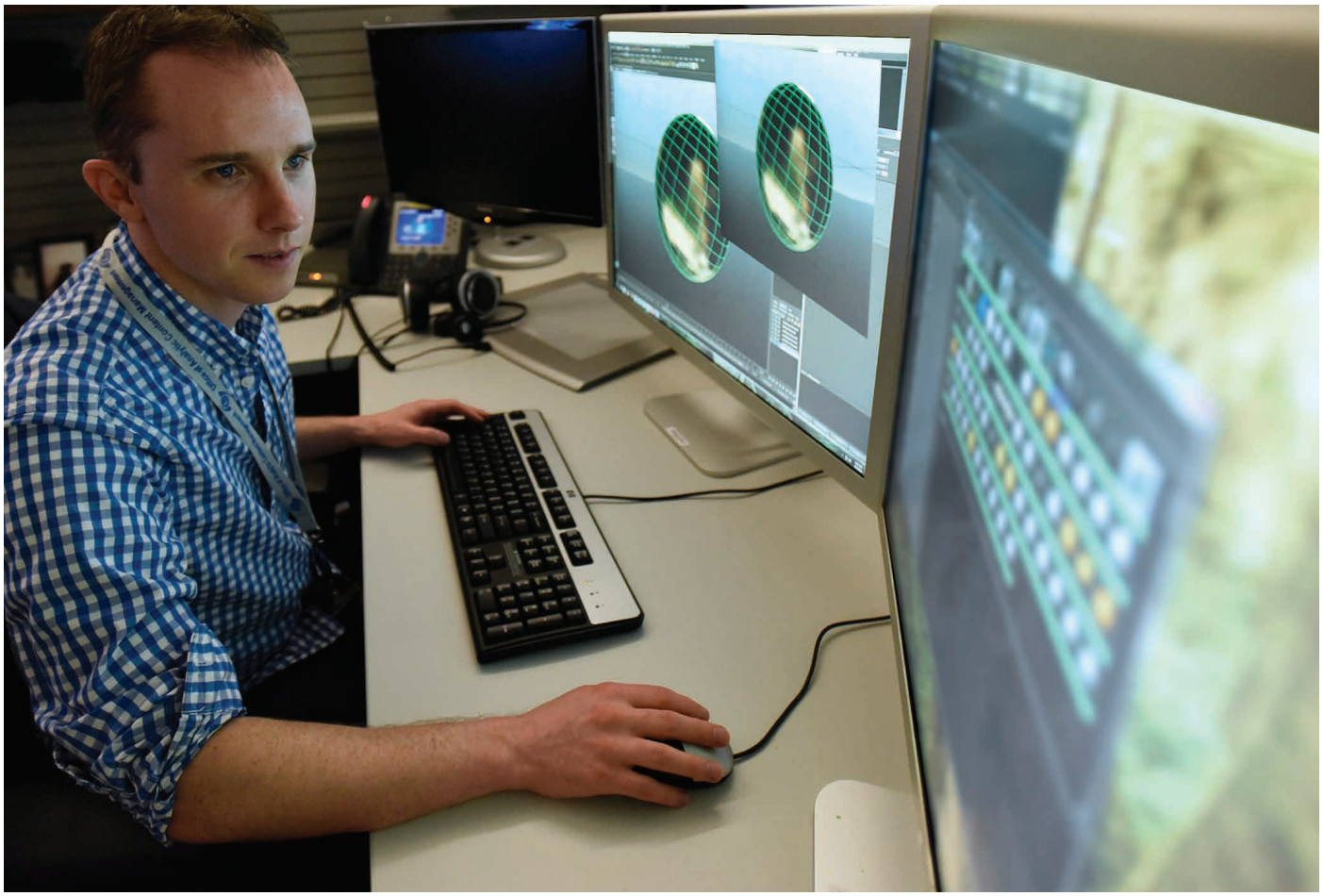


Photo by Erica Knight, NGA Office of Corporate Communications

GEOINT is a specialized field of practice, with a U.S. Government professional certification program that is mandatory for most Agencies and Services. The GEOINT discipline encompasses all activities involved in the planning, collection, processing, analysis, exploitation, and dissemination of spatial information in order to gain intelligence about the national security or operational environment, visually depict this knowledge, and fuse the acquired knowledge with other information through analysis and visualization processes.

The GEOINT discipline is much more than systems, processes, and products; it includes highly skilled, educated professionals and the many specialized tradecraft areas in which they work. GEOINT Tradecraft is the application of skills, technology, techniques, leadership, continuing education, mentoring, special experiences, and knowledge of GEOINT in one or more occupational specialties, which are described below.

GEOINT PROFESSIONAL TRADECRAFT AREAS

NGA Photos

- **Aeronautical Analysis –** The analysis and exploitation of worldwide aeronautical data and other sources in support of safety of navigation and national security goals, concerns, requirements, and strategies.
- **Applied Sciences –** The analysis of the Earth's gravity and magnetic fields, geophysical structure, material properties, and dynamics for geospatial intelligence and DoD applications. Professionals in the applied sciences provide in-depth technical expertise on Geodetic and geophysical issues and satellite issues.
- **Cartography –** The art and science of making maps and charts.
- **GEOINT Collection –** The collaboration with customers and source providers to develop comprehensive GEOINT, multi-source strategies to address intelligence problems. Professionals in this field create tasking and dissemination requirements, adjudicate requirements, analyze and investigate collection performance, assess collection opportunities, assess and report on the end-to-end GEOINT system performance data, advise customers, and satisfy essential elements of information (EEI) requirements.
- **Geospatial Analysis –** The science of extracting meaning from geospatial data and using geographic information systems to uncover and investigate relationships and patterns in all forms of geospatial data to address intelligence or military issues.
- **Geospatial Data Management –** The management of the development, approval, and population of geospatial data within a feature database to ensure that it can be used to satisfy customer requirements. This requires knowledge of the wide range of products and a solid understanding of the capabilities of various systems used to support the extraction, analysis, and finishing of in-house, co-production, commodity, and contract data.

Approved for public release, 18-142

- **Human Geography –** The science of understanding, representing, and forecasting activities of individuals, groups, organizations, and social networks with a geo-temporal context. Human Geography professionals gather, assess, and evaluate source materials and ensure its quality and suitability to build foundational data and apply knowledge and expertise in physical, socio-cultural, and political aspects of countries, regions, and urban areas to support national security goals, concerns, and strategies. This data is analyzed to characterize events, discover relationships and trends, infer conclusions, and predict behaviors.

- **Imagery Analysis –** The science of converting information, extracted from imagery, into intelligence about activities, issues, objects, installations, and/or areas of interest.

- **Imagery Science –** The generation, collection, duplication, analysis, modification, and visualization of images. It includes the use of advanced techniques to identify objects that cannot be detected by the human eye. Imagery science is used to develop algorithms, evaluate tools, and create customized methodologies and products to address a variety of geospatial intelligence problems. Imagery scientists typically specialize in precision mensuration, radar, spectral, infrared, and other specialized collection systems.

- **Maritime Analysis –** The acquisition, analysis, compilation, and dissemination of maritime safety of navigation information to populate and update nautical databases to support the Digital Nautical Chart, hardcopy charts, digital publications, and Electronic Chart Display and Information Systems. Marine Analysts generate datasets, promulgate worldwide navigational warnings, and respond to queries from foreign hydrographic offices and the users of our products and services.

Each GEOINT tradecraft area has specific duties within it. Civilian and military GEOINT professionals often perform similar functions but have different job titles. The chart below shows the GEOINT civilian job titles/categories and the corresponding military designations for each tradecraft area.

Evolving Work Role - Data Scientist. This work role will soon become a primary GEOINT tradecraft role. A community-coordinated definition will be provided in the next Publication 1.0 update.

GEOINT TRADECRAFT WORK ROLE/DESIGNATION CHART

TRADECRAFT AREA	GOVERNMENT CIVILIAN DESIGNATION	MILITARY DESIGNATION
Aeronautical Analysis	GEOINT Analyst (Aeronautical Intelligence)	Geospatial Engineer (Army–12Y) Geospatial Engineering Technician (Army–125D) Air Traffic Control Terps Specialist (Air Force–1C1X1) Geographic Intelligence Specialist (Marine Corps–0261)
Applied Sciences	GEOINT Analyst (Geodetic Earth Science) GEOINT Analyst (Geodetic Survey) GEOINT Analyst (Geodetic Orbit Sciences) GEOINT Analyst (Bathymetry) GEOINT Analyst (Oceanography) GEOINT Analyst (Meteorology) GEOINT Analyst (Hydrography) GEOINT Analyst (Precise Time/Astrometry)	Technical Applications Specialist (Air Force–9S100) Technical Engineer (Army–12T) Geospatial Engineering Technician (Army–125D) Diver (Army–12D) Aerographer's Mate (Navy Officer–1800) Geospatial Engineer (Army–12Y)
Cartography	GEOINT Analyst (Cartography) GEOINT Analyst (Photogrammetric Cartography)	Geospatial Engineer (Army–12Y) Geospatial Engineering Technician (Army–125D) Geographic Intelligence Specialist (Marine Corps–0261)
GEOINT Collection	GEOINT Analyst (Foundation Strategies) GEOINT Analyst (Open Source Research) GEOINT Analyst (Persistent Operations) GEOINT Analyst (Source Strategies) GEOINT Analyst (Throughput Strategies) GEOINT Analyst (Requirements & Integration)	Operations Intelligence Officer (Air Force–14N) Operations Intelligence Technician (Air Force–1N0) GEOINT Imagery Technician (Army–350G) GEOINT Imagery Analyst (Army–35G) GEOINT Officer (Army–35D–1D) Technical Engineer (Army–12T) Engineer Officer (Army–12A–W2) Imagery Analysis Specialist (Marine Corps–0241)
Geospatial Analysis	GEOINT Analyst (Geospatial Analysis) GEOINT Analyst (Analytical Methodologies) GEOINT Analyst (Infrared Source Analysis)	Targeteer (Air Force–1N1X1B) Technical Applications Specialist (Air Force–9S100) Geographic Intelligence Specialist (Marine Corps–0261) Geospatial Engineer (Army–12Y) Geospatial Engineering Technician (Army–125D) Engineer Officer (Army–12A-W2)
Geospatial Data Management	GEOINT Analyst (Data Stewardship) GEOINT Analyst (Database Management)	Geospatial Engineer (Army–12Y) Geospatial Engineering Technician (Army–125D) GEOINT Imagery Technician (Army–350G) GEOINT Imagery Analyst (Army–35G) GEOINT Officer (Army–35D–1D) Engineer Officer (Army–12A–W2) Geographic Intelligence Specialist (Marine Corps–0261)

Approved for public release, 18-142

Human Geography	GEOINT Analyst (Political Geography) GEOINT Analyst (Regional Geography) GEOINT Analyst (Regional Source) GEOINT Analyst (Scientific Linguistics)	GEOINT Imagery Technician (Army–350G) GEOINT Imagery Analyst (Army–35G) GEOINT Officer (Army–35D-1D) Engineer Officer (Army–12A-W2) Geospatial Engineering Technician (Army–125D) Geographic Intelligence Specialist (Marine Corps–0261) Master Analyst (Marine Corps–0205) Intelligence Specialist (Marine Corps–0231) Geospatial Engineer (Army–12Y)
Imagery Analysis	GEOINT Analyst (Imagery Intelligence)	Imagery Analysis Specialist (USMC–0241) GEOINT Analyst (Air Force–1N1X1A) GEOINT Imagery Technician (Army–350G) GEOINT Imagery Analyst (Army–35G) GEOINT Officer (Army–35D-1D) Navy Imagery Interpreter (IS–3910) Engineer Officer (Army–12A-W2) Geospatial Engineer (Army–12Y) Geospatial Engineering Technician (Army–125D)
Imagery Science	GEOINT Analyst (Lidar Image Science) GEOINT Analyst (Photogrammetric Image Science) GEOINT Analyst (Radar Image Science) GEOINT Analyst (Spectral Image Science) GEOINT Analyst (Thermal Infrared Image Science) GEOINT Analyst (OPIR Image Science)	GEOINT Imagery Technician (Army–350G) GEOINT Imagery Analyst (Army–35G) GEOINT Officer (Army–35D-1D) Technical Applications Specialist (Air Force–9S100) Geospatial Engineer (Army–12Y) Geospatial Engineer Technicians (Army–125D) Engineer Officer (Army–12A-W2) Geospatial Engineer (Army–12Y)
Maritime Analysis	GEOINT Analyst (Maritime)	Naval Imagery Interpreter (IS–3910) Imagery Analysis Specialist (Marine Corps–0241) Geographic Intelligence Specialist (Marine Corps–0261)

CHAPTER FIVE – GEOINT COMMUNITY & GOVERNANCE

This chapter has two sections. The GEOINT Community section addresses the National System for Geospatial Intelligence (NSG), an organization comprised of IC and DoD elements, and identifies the NSG's Principal Partners. It also defines and describes the GEOINT Enterprise, which encompasses a wide range of U.S and foreign entities that contribute to and influence the function of GEOINT. The Governance section describes the role of the GEOINT Functional Manager, the functional management governance structure, and related NSG organizations and forums. It also includes information on the governance structure of our Commonwealth partners, who have a significant impact on U.S. Government GEOINT activities.

GEOINT COMMUNITY

THE NATIONAL SYSTEM FOR GEOSPATIAL INTELLIGENCE (NSG)

The term "NSG" is used to describe the U.S. Government community, capabilities, assets, and other aspects of GEOINT that support U.S. national security decision making and U.S. military operations. The full definition of the NSG, shown in the box below, is established in both national Intelligence Community and DoD GEOINT doctrine. The NSG Community consists of Members and Partners.

NSG Members

NSG Members are IC and DoD organizations that fall under GEOINT Functional Management authorities, as outlined in EO 12333, DoD Directive 5105.60, and Intelligence Community Directive 113. NSG Members include the IC, the Joint Staff, the Military Departments (including the Services), and Combatant Commands (CCMDs).

National System for Geospatial Intelligence (NSG): The NSG is the combination of technology, policies, capabilities, doctrine, activities, people, data, and organizations necessary to produce GEOINT in an integrated multi-intelligence, multi-security domain environment. Its mission is to create an integrated, collaborative community of common practice promoting the GEOINT discipline across a diverse group of producers and consumers. It consists of members and partners that produce and employ GEOINT across the full range of national, military, and civil domains.

NSG MEMBERS

THE INTELLIGENCE COMMUNITY

Intelligence Agencies
- Central Intelligence Agency
- Defense Intelligence Agency
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- National Security Agency

Intelligence Components:
- Air Force Intelligence
- Army Intelligence
- Coast Guard Intelligence
- Marine Corps Intelligence
- Naval Intelligence
- Federal Bureau of Investigation (Office of Intelligence)
- Dept. of Energy (Office of Intelligence)
- Dept. of Homeland Security (Directorate of Intelligence & Analysis)
- Dept. of State (Bureau of Intelligence and Research)
- Dept. of Treasury (Office of Intelligence Support)
- Drug Enforcement Administration (Office of National Security Intelligence)

THE JOINT STAFF

MILITARY DEPARTMENTS
- Dept. of the Army (US Army)
- Dept. of the Air Force (US Air Force)
- Dept. of the Navy (US Navy and US Marine Corps)

COMBATANT COMMANDS
- US Africa Command (AFRICOM)
- US Central Command (CENTCOM)
- US Cyber Command (CYBERCOM)
- US European Command (EUCOM)
- US Northern Command (NORTHCOM)
- US Pacific Command (PACOM)
- US Southern Command (SOUTHCOM)
- US Special Operations Command (SOCOM)
- US Strategic Command (STRATCOM)
- US Transportation Command (TRANSCOM)

Approved for public release, 18-142

NSG PRINCIPAL PARTNERS

NSG Principal Partners include U.S. federal and civil agencies, allied Commonwealth countries, and certain members of U.S. industry, academia, and non-profit organizations. These Partners are organizations with which NSG Members work on a consistent basis. However, NSG Members continuously develop other U.S. and foreign partnerships, often just for the duration of specific missions and situations.

PRINCIPAL PARTNERS

U.S. FEDERAL AND CIVIL AGENCIES

NSG Member-organizations are closely linked with a number of federal agencies—such as the Defense Logistics Agency and Defense Information Services Agency—and work with most U.S. civil agencies via the Civil Applications Committee (CAC). The CAC is an interagency committee that facilitates the appropriate civil uses of remote sensing technologies and data collected by military and intelligence overhead capabilities, including commercial capabilities. This Committee is chaired by the USGS Director or his/her delegate on behalf of the Secretary of Interior, and the Vice Chair is a senior executive from a non-DOI member organization. The CAC is comprised of Principal Members (Federal civil organizations), Associate Members (IC and DoD organizations) and Ex-Officio Members. Principal members include the Departments of Interior, Agriculture, Commerce, Health and Human Services, and Transportation, as well as the U.S. Army Corps of Engineers, U.S. Coast Guard, Environmental Protection Agency, Federal Emergency Management Agency, National Science Foundation, National Aeronautics and Space Agency, and Tennessee Valley Authority.

The Civil Applications Committee (CAC): The CAC is an interagency committee that facilitates the appropriate civil uses of remote sensing technologies and data collected by military and intelligence overhead capabilities, including commercial capabilities.

U.S. FEDERAL & CIVIL AGENCY MEMBERS

CIVIL APPLICATIONS COMMITTEE (CAC)

- Department of Agriculture
- Department of Commerce
- Department of Health and Human Services
- Department of Interior*
- Department of Transportation
- Environmental Protection Agency
- Federal Emergency Management Agency
- National Science Foundation
- National Aeronautics and Space Administration
- Tennessee Valley Authority
- U.S. Army Corps of Engineers
- U.S. Coast Guard

OTHER U.S. FEDERAL AGENCIES

- Defense Information Services Agency
- Defense Logistics Agency
- Other

*The Department of Interior's U.S Geological Survey (USGS) serves in key roles as Chair of the Civil Applications Committee and voting member of the National Geospatial Intelligence Committee (GEOCOM).

ALLIED COMMONWEALTH COUNTRIES

NSG Principal Partners in the Commonwealth countries are represented by an organization body known as the Allied System for Geospatial Intelligence (ASG). The ASG manages the relationship of the geospatial intelligence organizations of the Commonwealth Allied partners (Australia, Canada, New Zealand, United Kingdom) and the United States. Each nation is represented by its lead GEOINT organization(s) and is an equal partner in the coalition. The United States provides the permanent Chair of the ASG Senior Management Council (ASMC) and the ASG Coordination Executive (ACE), which serve functions similar to that of the NSMC and GEOCOM (described in the Governance Section) respectively.

The Allied System for Geospatial Intelligence (ASG): The ASG manages the relationship of the geospatial intelligence organizations of the Commonwealth Allied partners—Australia, Canada, New Zealand, United Kingdom—and the United States.

ASG MEMBERS

- Australia
- Canada
- New Zealand
- United Kingdom
- United States

THE GEOINT ENTERPRISE

The term "GEOINT Enterprise" is used to describe the full breadth of U.S. and foreign government, commercial, and academic entities that produce, use, or contribute to one or more of the three elements of GEOINT (imagery, imagery intelligence, and geospatial data), and thereby influence the entire function. Given the widespread use and practice of GEOINT, it is essential to maintain awareness of activities and advancements occurring throughout the entire GEOINT Enterprise.

GEOINT Enterprise: The combination of technology, data, people, policies, capabilities, doctrine, activities, and organizations necessary to produce GEOINT in any government, academic, or commercial environment in the U.S. and partner countries.

THE GEOINT ENTERPRISE COMMUNITY

NSG MEMBERS
- Intelligence Community
- Joint Staff
- Military Departments
- Combatant Commands

ASG
- Australia
- Canada
- New Zealand
- United Kingdom
- United States

INTERNATIONAL GEOINT ENVIRONMENT
- Foreign Governments
- Foreign Industry
- Foreign Academic Institutions

OTHER U.S. PARTNERS
- U.S. Industry
- U.S. Academic Institutions
- U.S. State, Local, Tribal Organizations
- U.S. Law Enforcement

FEDERAL & CIVIL ORGANIZATIONS

Civil Applications Committee (CAC)
- Dept. of Agriculture
- Dept. of Commerce
- Dept. of Health & Human Services
- Dept. of Interior
- Dept. of Transportation
- Environmental Protection Agency
- Federal Emergency Management Agency
- National Science Foundation
- National Aeronautics and Space Administration
- Tennessee Valley Authority
- U.S. Army Corps of Engineers
- U.S. Coast Guard

Other U.S. Federal Agencies
- Defense Information Services Agency
- Defense Logistics Agency
- Other

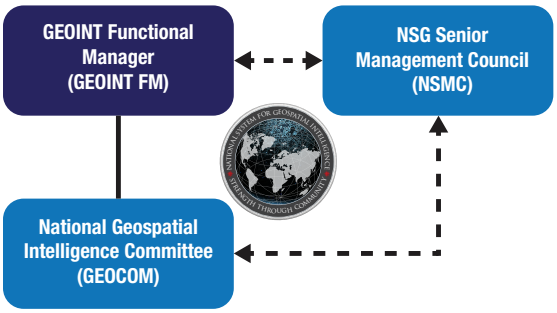
The term Global GEOINT Enterprise is sometimes used to emphasize the international aspects of the GEOINT Enterprise, but there is no difference between the terms or the communities associated with them.

Approved for public release, 18-142

NSG GOVERNANCE

The NSG is led by the GEOINT Functional Manager (GFM) in concert with a DNI-mandated "Committee of Record" and a GFM-appointed advisory council composed of members of the U.S. Government GEOINT Community. Each governing body has an important role to play in the management and future planning of the GEOINT function, and ensures that the GFM receives input from a wide range of users and producers of GEOINT. This section outlines the roles and responsibilities of the GFM and each governing body. Of note, the ASG has a parallel construct to the NSG framework.

Geospatial Intelligence Governing Framework



The three elements of the NSG governing structure are interdependent and serve collectively to advance the GEOINT function. The GFM may directly task the GEOCOM.

GEOINT Functional Manager (GFM): Executive Order 12333, "United States Intelligence Activities," as amended in 2008, legally designates the Director of NGA (D/NGA) as the GEOINT Functional Manager (GFM) for the Intelligence Community. Department of Defense Directive (DoDD) 5105.60, "National Geospatial-Intelligence Agency," 2009, designates the D/NGA as the DoD GEOINT Manager. The title GFM refers to both roles, thereby encompassing the Intelligence Community and DoD. The GFM is the authoritative GEOINT advisor to the Director of National Intelligence (DNI) and the Secretary of Defense.

The Functional Manager's role is defined by both obligations and authorities. Intelligence Community Directive (ICD) 113 "Functional Managers," 2009, states that a functional manager's primary obligation is to "oversee and guide the function in a manner that is distinct from organizational affiliations." Functional managers have other obligations as well, such as "maintaining knowledge of the totality of activities and resources pertaining to the function," and they "are accountable for continuously improving the performance of the function and for enhancing cross-function integration." ICD 113 and DoDD 5105.60 provide details on the full range of GFM authorities and responsibilities, such as issuing GEOINT standards for the DoD and IC. Please reference those documents for additional details.

NSG Senior Management Council (NSMC): Chaired by the GFM, the National System for Geospatial Intelligence (NSG) Senior Management Council, or NSMC, is the senior, three-star equivalent functional management advisory council of the NSG. Members discuss strategic, community-wide GEOINT issues and jointly address areas of common concern. The GFM brings a variety of issues before the NSMC for review, deliberation, endorsement, and/or decision. Commonwealth "Five Eyes (FVEY)" counterparts and issues are included at the discretion of the GFM. (FVEY is a term often used in classification of documents to indicate that the information can be shared with the five members of the Allied System for Geospatial Intelligence, or ASG.)

Geospatial Intelligence Committee (GEOCOM): The GEOCOM is a DNI-chartered forum for GEOINT. This Committee also provides a venue for community members to discuss, coordinate, and vote on substantive issues of common concern, and to develop recommendations on high-priority issues for the GFM or DNI. The GEOCOM is comprised of civilian Senior Executive Service (SES)/DISL and military Flag Officer (GOFO)-level members from key government GEOINT stakeholders, including the IC, DoD, and federal civil agencies, which are represented by the Civil Applications Committee (CAC)—a permanent NSG Partner. The GEOCOM administers subcommittees and working groups composed of subject matter experts from GEOCOM-member organizations. Each subcommittee is responsible for a specific GEOINT discipline such as collection, information systems and architecture, analysis and production, and training and professional development.

ABBREVIATIONS AND ACRONYMS

3D	Three Dimensional
ABI	Activity-Based Intelligence
ACE	ASG Coordination Executive
ASG	Allied System for Geospatial Intelligence
ASMC	ASG Senior Management Council
CAC	Civil Applications Committee
CCMD	Combatant Command
DCGS	Distributed Common Ground System
DISL	Defense Intelligence Senior Leader
DNI	Director of National Intelligence
DoD	Department of Defense
EEI	Essential Elements of Information
EM	Electromagnetic
EO	Electro-Optical
E.O.	Executive Order
FMV	Full Motion Video
FVEY	Five Eyes
GEOCOM	Geospatial Intelligence Committee
GEOINT	Geospatial Intelligence
GFM	GEOINT Functional Manager
GI&S	Geospatial Information and Services
GOFO	General Officer/Flag Officer
HSI	Hyperspectral Imaging
HUMINT	Human Intelligence
IC	Intelligence Community
ICD	Intelligence Community Directive
IFSAR	Interferometric Synthetic Aperture Radar
IMINT	Imagery Intelligence
INT	Intelligence Discipline
IR	Infrared
LIDAR	Light Detecting and Ranging (Also can be written as the word “lidar”)
MALE	Medium Altitude Long Endurance
MASINT	Measurement and Signatures Intelligence
MSI	Multispectral Imaging
MTI	Moving Target Indicator
NGA	National Geospatial-Intelligence Agency
NCL	NSG Consolidated Library
NSG	National System for Geospatial Intelligence
NSMC	NSG Senior Management Council
OBP	Object-Based Production
ODNI	Office of the Director of National Intelligence
OPIR	Overhead Persistent Infrared
OSINT	Open Source Intelligence
PAN	Panchromatic
PoL	Patterns of Life
RADAR	Radio Detecting and Ranging (Also may be written as the word “radar”)
SAR	Synthetic Aperture Radar
SES	Senior Executive Service
SIGINT	Signals Intelligence
SOM	Structured Observation Management
SONAR	Sound Navigation and Ranging (Also may be written as the word “sonar”)

Approved for public release, 18-142

TERPS	Terminal Instrument Procedures
TIR	Thermal Infrared
UAV	Unmanned Aerial Vehicle
UGS	Unattended Ground Sensor
USD(I)	Undersecretary of Defense for Intelligence
WAMI	Wide Area Motion Imagery

GLOSSARY

Activity-Based Intelligence (ABI): ABI refers to a methodology and automated technical process that contributes to intelligence analysis and products. It is defined as "An IC analytic method applied to structured data from all sources, to discover objects, relationships, or behaviors by resolving significant activity." Most GEOINT products focus on a specific object or area and seek to analyze everything about it. ABI enables more complex analysis by linking human, vehicular, and other activity related to the object or area, which can lead to different areas or objects and show patterns.

Aeronautical Analysis: A tradecraft involving the analysis and exploitation of worldwide aeronautical data and other sources in support of safety of navigation and national security goals, concerns, requirements, and strategies.

Aeronautical Data: Aerial Safety of Navigation data such as vertical obstructions, no-fly zones, flight routes, approach procedures, airfield infrastructure and layout, and aeronautical charts.

Applied Sciences: A tradecraft involving the analysis of the Earth's gravity and magnetic fields, geophysical structure, material properties, and dynamics for geospatial intelligence and DoD applications. Professionals in the applied sciences provide in-depth technical expertise on Geodetic and geophysical issues and satellite issues.

Assessment Products: Provide analysis of what is shown in an image or on a map, and provide information on the "who, what, when, where, how, and why," usually in the context of the purpose or mission for which it has been developed.

Base Layer: The first layer of a GEOINT product, also called the Foundation Layer, which consists of any combination of the three components of GEOINT: imagery, imagery intelligence, and geographic information. The base/foundation usually* is a map or image of a specific location and shows visible terrain, objects, and other features in that location. GEOINT images and maps contain highly accurate geo-coordinates of the location shown, as well as of any object or feature depicted in the map or image. *In some cases, the processed data itself is the product.

Cartography: The art and science of expressing graphically, by maps and charts, the known physical features of the Earth, or of another celestial body.

Detection Products: Designed to find natural and manmade materials that are not visible or easily identifiable to the human eye. A variety of EO or radar sensor phenomenologies and specialized data processing techniques are used to develop detection products. These products may be used for many purposes, such as to "see" beneath foliage and camouflage or to identify heat and other emissions.

Electro-Optical (EO): EO derives data from the ultraviolet through the infrared portions of the electromagnetic (EM) spectrum. Each part of the EM spectrum provides a different type of data or magnifies the results of the data, depending on the phenomenology used. Electro-optical sensors include panchromatic (visible), infrared, spectral (multispectral and hyperspectral), and light detection and ranging (lidar).

Elevation Data: Information about the height of objects on or in relation to the Earth. Elevation data includes heights of objects above the surface of the Earth, (spaceborne and airborne), on the surface of the Earth (buildings and physical relief), and below the surface (bathymetry and underground facilities).

Foundation Layer: See definition of Base Layer.

Full Motion Video (FMV): FMV, typically an EO capability, uses many still frames per second, creating a near-real-time video capability, which may be displayed as visible or infrared and may be recorded by digital or analog means. This near-real time capability allows observation of rapidly developing events and is a valuable tool for ongoing operations. It is also useful for continuous observation of an object to analyze its patterns over a long period of time.

Approved for public release, 18-142

Geodetic Data: Terrestrial, airborne, and satellite data used to scientifically measure the size, shape, and parameters of the earth, model the gravity field of the earth, and compute three-dimensional positions and coordinates of points above, on, and below the surface of the earth. This data has an impact on geo-positional systems (GPS), navigation tools, and systems of map grids and coordinate systems.

Geographic Names and Boundaries: Names and boundaries of cities, towns, provinces, regions, states, and countries. Identification of major landmarks, facilities, and buildings.

GEOINT: See the definition for Geospatial Intelligence.

GEOINT Collections: A GEOINT tradecraft involving collaboration with customers and source providers to develop comprehensive multi-INT, multi-source strategies to address intelligence problems. Professionals in this field create tasking and dissemination requirements, adjudicate requirements, analyze and investigate collection performance, assess and report on the end-to-end GEOINT system performance data, and advise customers in support of the National System for Geospatial-Intelligence (NSG).

GEOINT Enterprise. The combination of technology, data, people, policies, capabilities, doctrine, activities, and organizations necessary to produce GEOINT in any government, academic, or commercial environment in the U.S. and partner countries.

GEOINT Functional Manager (GFM): The authoritative advisor to the Director of National Intelligence (DNI) and Secretary of Defense, though the Undersecretary of Defense for Intelligence (USD(I)), on GEOINT issues and resources. Executive Order 12333, "United States Intelligence Activities," as amended in 2008, legally designates the Director of NGA (D/NGA) as the GFM for the Intelligence Community. Department of Defense Directive (DoDD) 5105.60, "National Geospatial-Intelligence Agency," 2009, designates the D/NGA as the DoD GEOINT Manager. The title GFM refers to both roles, thereby encompassing the Intelligence Community and DoD.

Geospatial Analysis: The science of extracting meaning from geospatial data and using geographic information systems to uncover and investigate relationships and patterns in all forms of geospatial data to answer intelligence or military issues. A scientific discipline that brings physical and human geography together in a digital environment in order to solve problems with regard to spatial analysis, physiography, socio-cultural aspects, and temporal relationships.

Geospatial Data Management: A tradecraft involving management of the development, approval, and population of geospatial data within NGA's feature/geospatial information database to ensure that it can be used to satisfy customer requirements. Requires knowledge of the wide range of products and a solid understanding of the capabilities of various systems used to support the extraction, analysis, and finishing of in-house, co-production, commodity, and contract data.

Geospatial Information: "Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the earth and includes: statistical data; information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data, and related products." (This legal definition is in Title 10 of the U.S. Code, Section 467.)

Geospatial Information and Services (GI&S): The collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery, gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the Earth's surface.

Geospatial Intelligence (GEOINT): "The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information." (Statutory definition codified in Title 10 of the U.S. Code, Section 467 (5)). Imagery, imagery intelligence, and geospatial information are defined separately in the glossary. Any one or combination of these three elements may be considered GEOINT.

GEOCOM: See the definition for "National Geospatial Intelligence Committee."

Geospatial Layer: A product layer composed of geospatial information including boundaries, infrastructure (such as sewer lines, power grids), elevation data, human geography data (population, cultural, political/religious geography), and identification of key facilities and natural or manmade features.

Global GEOINT Enterprise: A term sometimes used to emphasize the international aspects of the GEOINT Enterprise, but there is no difference between the terms or communities associated with them.

Human Geography (component of geospatial information): A social science discipline based on analyzing interconnections between people and places, including patterns of human activities, in the context of their environment. It also seeks to explain how actions taken in one place/population can impact another place/population. Human Geography includes sub-disciplines such as: population geography, political geography, cultural geography, and religious/ethnic geography. It may include both classified and unclassified information.

Human Geography (tradecraft): The art and science of understanding, representing, and forecasting activities of individuals, groups, organizations, and social networks with a geo-temporal context. Human Geography professionals gather, assess, and evaluate source materials and ensure its quality and suitability to build foundational data and apply knowledge and expertise in physical, socio-cultural, and political aspects of countries, regions, and urban areas to support national security goals, concerns, and strategies. This data is analyzed to characterize events, discover relationships and trends, infer conclusions, and predict behaviors.

Human Intelligence (HUMINT): Intelligence obtained through clandestine or overt HUMINT activities, or operations and activities utilizing human sources or other human assets.

Hyperspectral Imaging (HSI): An electro-optical phenomenology similar to MSI but uses hundreds, rather than tens, of bands of the visible and infrared portions of the EM spectrum. These extra bands can provide greater fidelity and characteristics than MSI. For example, HSI allows users to detect materials by their unique spectral signature.

Interferometric Synthetic Aperture Radar (IFSAR): A radar phenomenology that uses a SAR sensor to observe a location from two separate positions. This method generates elevation data of the Earth's surface.

Imagery: A likeness or presentation of any natural or man-made feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems, and likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means. (This legal definition is in Title 10 of the U.S. Code, Section 467.)

Imagery Analysis: The science of converting information, extracted from imagery, into intelligence about activities, issues, objects, installations, and /or areas of interest.

Imagery Intelligence (IMINT): The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. (This legal definition is in Title 10 of the U.S. Code, Section 467.)

Imagery Science: Tradecrafts involving the generation, collection, duplication, analysis, modification, and visualization of images. It includes the use of advanced techniques to identify objects that cannot be detected by the human eye. Imagery science is used to develop algorithms, evaluate tools, and create customized methodologies and products to address a variety of geospatial intelligence problems. Imagery scientists typically specialize in precision mensuration, radar, spectral, infrared, and other specialized collection systems.

Infrared (IR): IR is an electro-optical phenomenology that uses the infrared part of the spectrum to detect heat and radiance/reflection, and displays that information in a gray-scale image.

Intelligence Layer: A GEOINT product layer customized for a specific mission or purpose that consists of information derived from various intelligence sources, or a combination of those sources. Examples include locations of friendly and enemy forces,

Approved for public release, 18-142

presence of chemical or biological hazards, weapons facilities, routes and alternatives, and potential targets. GEOINT serves as a base for the depiction of data from other intelligence disciplines (INTs), including Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Measures and Signatures Intelligence (MASINT) and Open Source Intelligence (OSINT).

Light Detection and Ranging (Lidar): An electro-optical phenomenology that uses laser pulses in the visible and infrared portions of the EM spectrum. The sensor emits a pulse of laser light toward an object, which reflects back some of the energy to the sensor. The time it takes for the energy to return provides elevation values—shorter roundtrips indicate higher elevations and longer roundtrips indicate lower elevations. This process helps measure distances to, heights of, and other characteristics of an object. The process can be used to develop three-dimensional models of an object, such as a building.

Maritime Analysis: A GEOINT tradecraft involving acquisition, analysis, compilation, and dissemination of maritime safety information to populate and update nautical databases to support the Digital Nautical Chart, hardcopy charts, digital publications, and Electronic Chart Display and Information Systems. Marine Analysts generate mission specific datasets, promulgate worldwide navigational warnings, and respond to queries from foreign hydrographic offices and the users of our products and services.

Maritime Data: Maritime Safety of Navigation data such as shipping routes, underwater obstructions, sailing restrictions, port infrastructure and layout, approach procedures, bathymetry, soundings, and nautical charts.

Measurement and Signature Intelligence (MASINT): Scientific and technical intelligence information obtained by quantitative and qualitative analysis of the physical and technical attributes of data. MASINT, which is derived from specific technical sensors, identifies distinctive features associated with the source, emitter, or sender. It can measure physical characteristics of targets and events of interest to determine composition, location, and/or performance.

Mission/Event Preparation Products: Used to prepare for a mission, operation, or major event. These products focus on familiarization with the area, including identification of key landmarks and existing or potential hazards. They usually are map or imagery products that facilitate safety of navigation by identifying elements such as buildings, routes, water depth, terrain features, obstacles, and threats. The products assist with activities such as route planning and security preparations.

Mission Layer: A GEOINT product layer that provides general information relevant to the purpose and area for which the product is being used. The information may include weather conditions, logistics data, characteristics of the local terrain, population, and government, and other data obtained through commonly used, unclassified sources.

Motion GEOINT: Both EO and radar sensors can create or capture motion by collecting two or more frames per second. This activity is known as Motion GEOINT. The most common types are Full Motion Video (FMV), Moving Target Indicator (MTI), and Wide Area Motion Imagery (WAMI).

Moving Target Indicator (MTI): This EO and radar capability shows only those objects that are in motion, and provides information on the speed and direction that objects are moving.

Multispectral Imaging (MSI): MSI is an electro-optical phenomenology that provides a color image by using tens of additional bands of the visible and infrared portions of the spectrum. It also provides more detail to images, showing characteristics that are not otherwise visible.

National Geospatial Intelligence Committee (GEOCOM): The GEOCOM is a Director of National Intelligence-chartered forum to discuss, coordinate, and vote on substantive issues in order to provide recommendations to the GEOINT Functional Manager. It is comprised of Senior Executive Service and General Officer/Flag Officer-level members from key government GEOINT stakeholders, including the IC, military Services, Combatant Commands, the U.S. Geological Survey and civil agencies, which are represented by the Civil Applications Committee (CAC). The GEOCOM manages subcommittees and working groups composed of subject matter experts from GEOCOM-member organizations. Each subcommittee focuses on a different substantive area such as collection, information systems and architecture, analysis and production, and training and professional development.

National System for Geospatial Intelligence (NSG): The combination of technology, policies, capabilities, doctrine, activities, people, data, and organization necessary to produce GEOINT in an integrated, multi-intelligence, multi-security domain environment. It includes members and partners that produce and employ GEOINT across the full range of national, military, and civil domains.

NSG Senior Management Council (NSMC): Chaired by the GFM, the NSMC is the senior, three-star equivalent functional management advisory council of the NSG. Members discuss strategic, community-wide GEOINT issues and jointly address areas of common concern. The GFM brings a variety of issues before the NSMC for review, deliberation, and/or decision. Five Eyes (FVEY) counterparts and issues are included at the discretion of the GFM.

Object: Representations of physical objects of interest, such as a person, unit, facility, or type of equipment.

Object-Based Production (OBP): The process of formatting and organizing intelligence related to objects. This structured approach enables automated identification of the object, or identical objects, and access to all sources of known information about that object. It also facilitates Activity Based Intelligence analysis.

Observation: Information or image gleaned from data captured by a sensor.

Open Source Intelligence (OSINT): Intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.

Overhead Persistent Infrared (OPIR): OPIR sensors operate in the visible and near infrared, short-wave infrared, and mid-wave infrared portions of the spectrum to characterize this energy as an event or process it as a scene. OPIR sensors provide persistent (i.e. continuous) coverage of mission areas and energy radiation detection from both tactical and strategic targets including missiles launches and events, wildfires, enemy hostilities, weather, volcanos, and weapons characterization.

Panchromatic (PAN): PAN uses the visible part of the EM spectrum, along with a portion of IR spectrum, and produces an image similar to a black and white aerial photograph. The images can provide a very detailed and accurate likeness of an area or object, and can show shadows and other effects that help identify characteristics of an object or environment.

Phenomenology: The study of natural occurring and measurable activity (e.g., effluent emission as a result of a chemical reaction). As used in this document, it refers to sensor technology, literal and non-literal, which allows discovery, observation, and characterization of natural and measurable occurrences (spatial, spectral, radiometric and temporal). Various phenomenologies discussed in Publication 1.0 include electro-optical imagery, multispectral imagery, hyperspectral imagery, light detection and ranging, and radar.

Platform: The vehicle to which one or many sensors are attached. Platforms include satellites, aircraft (known as “airborne” platforms, and include unmanned aerial vehicles, balloons, and dirigibles), ground-based (for example, vehicles, stationary objects such as poles, and humans who carry sensors), and water-based platforms (such as ships, submarines, sonars and buoys).

Radar: Active sensors that emit manmade electromagnetic energy to illuminate the environment or object they are imaging, and then use the characteristics of the response to create an image. These sensors use reflected radar energy to illuminate objects in day or night and in almost any weather conditions. A radar image is non-literal, which means it does not appear as a photo that shows an exact likeness of an object or environment. It is similar to an X-ray of an area or object, with the ability to detect characteristics that a literal picture would not show. An important feature is that it can be used for poor light and weather conditions in which EO technologies are ineffective.

Approved for public release, 18-142

Sensor: A technical device designed to detect and respond to at least one stimulus and that may record and/or transmit a resultant impulse for interpretation or measurement. Two primary categories of sensors are electro-optical (EO) and radar, both of which have several types or variants, known as phenomenologies. Sensors may be active or passive, as described below.

- Active Sensor: Sensors that generate the electromagnetic energy needed to illuminate the object that is being imaged. They broadcast energy and process returning portions of it in order to image a targeted area. Active imagery sensing capabilities include real-aperture radar, synthetic aperture radar, interferometric synthetic aperture radar, moving target indicator, and light detection and ranging systems.

- Passive Sensor: Sensors that use natural electromagnetic energy sources such as the sun, naturally occurring radiation, or objects that generate heat. They generate data by capturing the reflected or emitted electromagnetic energy from an object. Passive sensors, which operate in "receive" mode and do not emit energy, diminish the adversary's ability to detect the fact that they are being imaged. Electro-optical sensors (except lidar) are passive.

Signals Intelligence (SIGINT): A form of technical intelligence derived from the exploitation of foreign electronic emissions. SIGINT can be in the form of the actual information content of a signal or in the form of its temporal and spectral characteristics, called signal operating parameters. SIGINT includes both the raw data and the analysis product of that data. This category of intelligence includes all Communications Intelligence, Electronic Intelligence, and Foreign Instrumentation Signals Intelligence.

Structured Observation Management (SOM): An organized method to capture, store, standardize, and provide data and information from GEOINT sources (sensors). This approach decreases the time required for analysts to search for data, enabling them to focus on conducting analysis and developing products.

Synthetic Aperture Radar (SAR): A radar phenomenology that illuminates an object with pulses of microwave energy. It applies signal processing to a series of many pulses to produce imagery.

Terminal Instrument Procedures (TERPS): Process of data extraction and analysis to produce Department of Defense Instrument Approach Procedures. Analysis includes imagery derived features, host nation, and vertical obstruction data.

Thermal Infrared (TIR): TIR is a type of Infrared phenomenology, but uses different wavelengths of the infrared spectrum to indicate the temperature level of the heat or radiance/reflection. The shape and size of the object or environment emitting heat is shown as a different shade than the rest of the image. Cooler objects are darker, warmer objects are lighter, and hot objects are bright white.

Topographic Data: Ground/surface-related information including infrastructure (roads, power grids), man-made features, population data, vegetation, and hydrography.

Wide Area Motion Imagery (WAMI): A set of motion imagery sensors with a wide field of view (FOV) diameter of up to 8 km, which provides persistent surveillance of a broad area of coverage. WAMI data enables forensic backtracking of kinetic events, network analysis, pattern of life (PoL) studies, and security monitoring.

Appendix A: REFERENCES

GEOINT FUNCTIONAL MANAGEMENT AUTHORITIES

a. Executive Order 12333, "United States Intelligence Activities," as revised, 30 July 2008

b. United States Code, Title 50, "War and National Defense," 2014

c. United States Code, Title 10, "Armed Forces of the United States," 2010

d. Intelligence Community Directive 113, "Functional Managers," 19 May 2009

e. Department of Defense Directive 5105.60, "National Geospatial-Intelligence Agency (NGA)," 29 July 2009

Approved for public release, 18-142

Appendix B: GEOINT DEFINTION

(Including Amplifications)

Exact language from:

- *NSG GEOINT Basic Doctrine (2018)*
- *Title 10, U.S. Code, Section 467 (2005 & 2010)*
- *DoD Directive 5105.60 (2009)*
- *Director of National Intelligence Memo (2005)*

NSG GEOSPATIAL INTELLIGENCE (GEOINT) BASIC DOCTRINE: PUB 1.0,

(Updated in 2018)

This GEOINT Definition contains the same language as the Title 10, Section 467 Definition (shown in next entry) but provides slight changes in organization to improve clarity and readability.

GEOINT DEFINITION

"The term 'geospatial intelligence' means the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information."

- **Imagery.** "A likeness or presentation of any natural or man-made feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems, and likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means." Imagery includes handheld photography, but "does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations."
- **Imagery Intelligence.** "The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials."
- **Geospatial Information.** "Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the earth, including: statistical data; information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data, and related products."

TITLE 10, US CODE: ARMED FORCES

(2005)

Subtitle A – General Military Law
PART I – Organization and General Military Powers
CHAPTER 22 – National Geospatial-Intelligence Agency
SUBCHAPTER I – Missions and Authority
§ 467. "Definitions"

§ 467. Definitions

Release date: 2005-07-12

In this chapter:
(1) The term "function" means any duty, obligation, responsibility, privilege, activity, or program.
(2)
(A) The term "imagery" means, except as provided in subparagraph (B), a likeness or presentation of any natural or man-made feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including—
I. products produced by space-based national intelligence reconnaissance systems; and
II. likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means.
(B) Such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations.
(3) The term "imagery intelligence" means the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.
(4) The term "geospatial information" means information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the earth and includes—
(A) statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and
(B) mapping, charting, geodetic data, and related products.
(5) The term "geospatial intelligence" means the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.

*NOTE: Title 10, Section 442, was updated in 2010 to include language on the NGA Mission. The new paragraphs address systems and tasking, and do not impact the definition of GEOINT in Section 467. However, the language is shown below because it provides context to the handheld photography language in the definition.

Section 442(a) of title 10, United States Code, is amended—

by redesignating paragraph (2) as paragraph (3); (2) by inserting after paragraph (1) the following new paragraph (2): "(2) (A) As directed by the Director of National Intelligence, the National Geospatial-Intelligence Agency shall develop a system to facilitate the analysis, dissemination, and incorporation of likenesses, videos, and presentations produced by ground-based platforms, including handheld or clandestine photography taken by or on behalf of human intelligence collection organizations or available as open-source information, into the National System for Geospatial Intelligence.
"(B) The authority provided by this paragraph does not include authority for the National Geospatial-Intelligence Agency to manage tasking of handheld or clandestine photography taken by or on behalf of human intelligence collection organizations"; and (3) in paragraph (3), as so redesignated, by striking "paragraph (1)" and inserting "paragraphs (1) and (2)".

Approved for public release, 18-142

DODD 5105.60

"NATIONAL GEOSPATIAL- INTELLIGENCE AGENCY"
(July 29, 2009)

GLOSSARY, DEFINITIONS

GEOINT. The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information (section 467 of Reference (a)). **[Pub 1.0 Note: the following portion of this definition was derived from a classified July 2005 ONDI/C memo]** GEOINT collection encompasses all aspects of: literal, infrared (IR) and synthetic aperture radar (SAR) imagery; overhead persistent infrared capabilities; and geospatial information and services. The terms imagery intelligence and advanced geospatial intelligence are encompassed within this definition of GEOINT. GEOINT includes the exploitation and analysis of electro-optical, IR, and radar imagery; and of geospatial, spectral, laser, IR, radiometric, SAR phase history, polarimetric, spatial, and temporal data. It employs all ancillary data, signature information, and fused data products, as necessary. Integrated GEOINT products may also include data and information from collateral sources.

Geospatial information. Defined in sections 455(c) and 467 of Reference (a) [Title 10, U.S. Code].

Imagery. Defined in section 467 of Reference (a) [Title 10, U.S. Code].

Imagery intelligence. Defined in section 467 of Reference (a)

DNI MEMO

"Statutory Definition of Geospatial Intelligence and its Amplification"
(17 October 2005)

2. The following amplifies the statutory definition [of GEOINT] and represents the full manifestation of NGA's missions per section 442(a) Title 10. The relevance of this amplification derives from the "terms of art" unique to the GEOINT discipline.

GEOINT encompasses all aspects of imagery (including capabilities formerly referred to as Advanced Geospatial Intelligence and imagery-derived MASINT) and geospatial information and Services (GI&S; formerly referred to as mapping, charting, and geodesy). It includes, but is not limited to, data ranging from the ultraviolet through the microwave portions of the electromagnetic spectrum, as well as information derived from the analysis of literal imagery; geospatial data, and information technically derived from the processing, exploitation, literal, and non-literal analysis of spectral, spatial, temporal, radiometric, phase history, polarimetric data, fused products (that is, products created out of two or more data sources), and the ancillary data needed for data processing and exploitation, and signature information (to include development, validation ,simulation, data archival, and dissemination). These types of data can be collected on stationary and moving targets by electro-optical (to include IR, MWIR, SWIR TIR, Spectral, MSI, HSI, HD), SAR (to include MTI), related sensor programs (both active and passive), and non-technical means (to included geospatial information acquired by personnel in the field).

3. The statutory definition, as amplified, provides the basis for a clear distinction between GEOINT and MASINT. The relevant Intelligence Community Directives should reflect this definition and amplification.

OCC 170901-038 | April 2018

Approved for public release, 18-142

MCWP 2-15.4

Imagery Intelligence

U.S. Marine Corps

PCN 143 000088 00

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380-1775

6 September 2002

FOREWORD

Marine Corps Doctrinal Publication 2, *Intelligence*, and Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations*, provide doctrine and higher order tactics, techniques, and procedures for intelligence operations. MCWP 2-15.4, *Imagery Intelligence*, complements and expands upon this information by detailing doctrine, tactics, techniques, and procedures for the conduct of imagery intelligence operations in support of the Marine air-ground task force (MAGTF). The primary target audience of this publication is intelligence personnel responsible for planning and execution of imagery intelligence operations. Personnel who provide support to imagery intelligence or who use results from these operations should also read this publication.

MCWP 2-15.4 describes aspects of imagery intelligence operations including doctrinal fundamentals, equipment, command and control, communications and information systems support, planning, execution, and training. MCWP 2-15.4 provides the information needed by Marines to understand, plan, and execute imagery intelligence operations in support of the MAGTF across the spectrum of conflict.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

EDWARD HANLON, JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

Publication Control Number: 143 000088 00

IMAGERY INTELLIGENCE

TABLE OF CONTENTS

Chapter 1. Doctrinal Fundamentals

Overview 1-1
IMINT Information vs. Intelligence 1-1
Objectives of IMINT 1-2
Capabilities and Limitation of IMINT 1-2
Responsibilities and Products 1-2
Overview 1-2
Marine Corps IMINT Responsibilities 1-2
Types of IMINT Products 1-3
Related Terminology 1-4
Reconnaissance 1-4
Battlefield Surveillance 1-4
Point Target 1-4
National Imagery 1-4
Theater Imagery 1-5
Organic Imagery 1-5
IMINT vs. Imagery 1-5
Role and Functions 1-5
General 1-5
Tactical IMINT Principles 1-5
IMINT and the Intelligence Cycle 1-6
Planning and Direction 1-6
Collection 1-8
Processing and Exploitation 1-9
Production 1-9
Dissemination 1-9
Utilization 1-9
G-2/S-2 Role in the Intelligence Cycle 1-10
Levels of IMINT 1-10
National IMINT 1-10
Theater and Joint Task Force IMINT 1-11
Tactical IMINT 1-12

Chapter 2. Organizations and Responsibilities

MEF Key Personnel Responsibilities 2-1
The Role of the Commander 2-1
MEF Command Element G-2 Section and the Intel Bn 2-2
Other Command Element Staff 2-8
MEF Major Subordinate Commands' Intelligence Officers 2-9
National Imagery Organizations 2-9
Director of Central Intelligence 2-9
National Imagery and Mapping Agency 2-10
National Reconnaissance Office 2-10
Defense Intelligence Agency 2-11
Marine Corps Supporting Establishment Imagery Intelligence Organizations 2-11
Headquarters, U.S. Marine Corps 2-11
Marine Corps Combat Development Command 2-12
Marine Corps Systems Command 2-12
Marine Corps Intelligence Activity 2-12

Chapter 3. MAGTF IMINT Units and Organizations

Imagery Intelligence Platoon, Intelligence Battalion 3-1
Mission 3-1
Tasks 3-1
Organization 3-1
Command and Control 3-1
Concept of Employment 3-2
Miscellaneous 3-2
Joint Surveillance Target Attack Radar System Common Ground Station 3-4
Mission 3-4
Tasks 3-4
Organization 3-4
Command and Control 3-4
Concept of Employment 3-4
Miscellaneous 3-5
Direct Support Teams, Production and Analysis Company, Intelligence Battalion 3-5
Mission 3-5
Tasks 3-6
Organization 3-6
Command and Control 3-6
Concept of Employment 3-6
Miscellaneous 3-6
Marine Unmanned Aerial Vehicle Squadron 3-7
Mission 3-7
Tasks 3-7

Organization 3-7
Command and Control 3-7
Concept of Employment 3-8
Miscellaneous 3-8
Marine All-Weather Fighter Attack Squadron 3-8
Mission 3-8
Tasks 3-9
Organization 3-9
Command and Control 3-9
Concept of Employment 3-9
Miscellaneous 3-10
Marine Light/Attack Helicopter Squadron 3-10
Mission 3-10
Tasks 3-10
Organization 3-11
Command and Control 3-11
Concept of Employment 3-11
Miscellaneous 3-12
Ground Reconnaissance Units 3-13
Mission 3-13
Command and Control 3-13
Manpack SIDS Concept of Employment 3-14
Tactical Intelligence Photographic Capability 3-15

Chapter 4 Imagery Intelligence Systems, C2 Nodes, Communications Information Systems, and Other Systems

Basic Imagery Intelligence Communications and Information Systems Requirements 4-1
Imagery Intelligence and Key Related Command and Control Nodes. . . 4-2
Organization 4-2
JTF J-2 and the Joint Intelligence Support Element 4-6
Amphibious Forces 4-7
MEF Command Element 4-8
Imagery Intelligence Information Systems and Supporting Communications 4-13
Imagery Direction and Collection Management 4-13
Imagery Collection 4-16
Imagery Processing, Exploitation, and Production Capabilities . . . 4-21
Imagery CIS Architecture 4-25
IMINT Communications and Information Systems Planning Considerations 4-25

Chapter 5. Operational Planning and Execution

Marine Corps Planning Process 5-1
Mission Analysis 5-1
COA Development 5-2

COA Wargaming 5-2
COA Comparison and Decision 5-2
Orders Development 5-2
Transition 5-2
Joint Planning Processes 5-2
Joint Deliberate Planning 5-2
Crisis Action Planning 5-2
Planning and Imagery Intelligence 5-4
Planning and Intelligence Cycle 5-4
Basic IMINT Planning Process 5-4
Planning Responsibilities 5-7
Intelligence Officer 5-7
Intelligence Battalion Commander/Detachment OIC 5-7
General Planning Considerations 5-7
Principles 5-7
Concept of Operations 5-8
Terrain 5-8
Weather 5-8
Threat 5-9
Specific Planning Considerations and Execution Activities 5-9
Planning and Direction 5-9
Collection 5-10
Processing and Exploitation 5-20
Production 5-21
IMINT Utilization 5-27
IMINT Operations Appendix 5-28
IMINT Plans within Other Portions of Annex B 5-28
Appendix 11 (Intelligence Estimate) 5-28
Appendix 14 (Reconnaissance and Surveillance Plan) 5-29
Appendix 16 (Intelligence Operations Plan) 5-30
Appendix 17 (Support to Survival, Evasion, Resistance, and Escape) 5-31

Appendices

A Imaging Sensors A-1
B National Imagery Interpretability Rating Scale B-1
C Request Formats for Aerial Imagery Collection Missions C-1
D Unmanned Aerial Vehicle Squadron Equipment and Performance Characteristics D-1
E MAGTF Imagery Intelligence Planning Checklist. E-1
F Imagery Intelligence Report Formats F-1
G Imagery Intelligence Support to Intelligence Studies G-1
H Imagery and Supporting Intelligence Reports H-1
I Imagery Intelligence Target Folders I-1
J National Imagery Transmission Format Compression J-1
K Imagery Intelligence Appendix Format K-1
L Unmanned Aerial Vehicle Plan Format L-1
M Aerial Imagery Plan Format M-1
N Glossary N-1
O References and Related Publications O-1

CHAPTER 1. FUNDAMENTALS

If you can't get behind enemy lines and peer around with your own good eyes, what's your next best bet? A photograph, isn't it?

—FMFRP 12-16, Front Line Intelligence

Imagery is the representation of objects reproduced electronically or by optical means on film, electronic display devices or other media.

Imagery, along with the graphical, geospatial, and textual intelligence products derived from it, is an increasingly critical element in the planning and decisionmaking efforts of commanders and supporting staffs at all echelons. Much of the imagery available to the Marine air-ground task force (MAGTF) commander requires detailed analysis by highly trained specialists to fully exploit its value. Imagery and imagery-related information—when processed, exploited, analyzed, and fused with other intelligence information—results in imagery intelligence (IMINT).

Principal sources of imagery and related data are national overhead intelligence systems such as satellites; manned aircraft such as the F-14 or F/A-18 with the advanced tactical airborne reconnaissance system (ATARS); the U-2 and the joint surveillance target attack radar system (JSTARS); unmanned aerial vehicles (UAVs); and various hand-held cameras.

Overview

IMINT Information vs. Intelligence

A critical distinction must be made when discussing, planning for, and executing IMINT operations and operations yielding imagery-related combat information. IMINT is the function performed by the G-2/S-2 that involves imagery analysis and integration with other intelligence activities to produce all-source intelligence products. The intelligence battalion's (intel bn's) imagery intelligence platoon (IIP), unit intelligence personnel, and Marine Corps Intelligence Activity (MCIA) conduct IMINT operations, planning, collecting, producing, and disseminating information or intelligence to the commander, staff, and major subordinate commands (MSCs). To provide imagery analysis for fusion into intelligence, specifically trained technical personnel, adequate time, and sophisticated equipment are required. Imagery and related combat and sensor data from JSTARS, UAVs, and various reconnaissance sources with hand-held cameras may sometimes be rapidly disseminated to tactical commanders to effect decisions without extensive intelligence processing and analysis. This type of intelligence support is provided directly to the tactical commander without being analyzed or evaluated against other intelligence. Caution should be exercised to ensure that the commander is apprised of the strong potential for misleading information when the provided intelligence is based on a single, unevaluated intelligence source.

IMINT aids commanders and planners primarily through two forms of support. First, IMINT provides situational awareness for the terrain, both natural and manmade, to support the commander's intelligence preparation of the battlespace (IPB) effort through various baseline IMINT and geographic intelligence (GEOINT) based studies such as helicopter landing zones (HLZs); beach, coastal, port and airfield studies; and gridded reference graphics (GRG). Second, support is provided through imagery as a confirming source of intelligence for another discipline such as signals intelligence (SIGINT) or human intelligence (HUMINT).

Objectives of IMINT

Reduce Uncertainty

IMINT must support the commander's decisionmaking process by reducing uncertainty about the hostile situation and the surrounding environment.

Counterintelligence and Force Protection

IMINT supports the identification of hostile intelligence collection operations; aids with the identification of MAGTF vulnerabilities that could be exploited by the enemy; and assists with the evaluation of friendly security measures to counter these.

Capabilities and Limitations of IMINT

Capabilities

IMINT is an extremely valuable part of intelligence. IMINT provides concrete, detailed, and precise information on the location and physical characteristics of both the threat and the environment. It is the primary source of information concerning key terrain features, installations, and infrastructure used to build detailed intelligence studies, reports, and target materials. Order of battle (OOB) analysis, enemy courses of action assessments, development of target intelligence, and battle damage assessment (BDA) are intelligence functions that rely heavily upon IMINT.

Limitations

The major limitations of IMINT are the time required to task, collect, process, analyze, and disseminate the imagery product; the detailed planning and coordination required to ensure the collected imagery is received in time to impact the decisionmaking process; and the requirement for considerable assets in personnel, equipment, and communications connectivity to conduct IMINT operations. Also, imagery operations can be hampered by weather; enemy air defense capability; and enemy camouflage, cover, concealment and deception activities.

Sensors

Appendix A describes the basic capabilities and limitations of electro-optical (EO), radar, and infrared imagery sensors.

Responsibilities and Products

Overview

The Marine Corps relies on a complementary mix of tactical, theater, and national IMINT sources to support its intelligence planning and operations. The MAGTF must use the full range of US intelligence capabilities, from national through theater to organic, in support of the assigned mission. Due to the nature of expeditionary operations, the employment of organic MAGTF intelligence collection assets within the assigned area of operations (AO) is not feasible until just prior to the introduction of forces. This means that national or theater intelligence assets must be relied upon for predeployment IMINT support.

The MAGTF will rely almost exclusively on external support during the planning and deployment phases of any operation. Even when employed, the MAGTF will continue to require national and theater support in specific areas to add depth to the reconnaissance effort and cover gaps in organic collection capabilities.

Marine Corps IMINT Responsibilities

The MAGTF G-2/S-2 has staff responsibility for intelligence, counterintelligence (CI), and reconnaissance, to include support of IMINT operations. In conjunction with the G-3/S-3, the G-2/S-2 develops the intelligence operations plan (appendix 16 to annex B), the supporting IMINT plan (appendix 7 to annex B), and the reconnaissance and surveillance (R&S) plan (appendix 14 to annex B), which allocate resources and assign specific imagery reconnaissance and supporting missions to MAGTF and supporting elements. Together, these intelligence plans assign intelligence missions,

reconnaissance missions, and tasks, and also allocate supporting resources.

Factors affecting the development of intelligence and supporting IMINT plans are—

- Priority intelligence requirements (PIR) and intelligence requirements, to include the specific intelligence questions to be answered for each.
- Communications connectivity and information systems capabilities available, both in IMINT units as well as in supported commands.
- Time available.
- Available information and intelligence from other sources.
- Redundancy required.
- Assets available.
- Knowledge of the enemy situation.
- Enemy counter-reconnaissance capabilities.

Based on these factors, the commander's intent, anticipated enemy activity, the MAGTF concept of operations, and the overall intelligence operations plan, the G-2/S-2 develops specific intelligence, reconnaissance, and imagery-related tasks. Individual units are assigned reconnaissance tasks per the intelligence plan. The intelligence support coordinator (ISC), under the staff cognizance of the MAGTF G-2/S-2, establishes an intelligence operations center (IOC) to perform intelligence requirements management, staff cognizance of ongoing organic and supporting collection operations, intelligence production and analysis, and intelligence dissemination. The following are the key elements within the IOC:

- **Support Cell.** Primary element for conducting Marine expeditionary force (MEF)-wide intelligence requirements management; weather support; collections and dissemination planning and direction; and intelligence staff cognizance of MEF organic and supporting intelligence and reconnaissance operations.
- **Surveillance and Reconnaissance Cell (SARC).** Primary element for supervising the execution of organic and supporting intelligence and reconnaissance plans.
- **Production and Analysis (P&A) Cell.** Primary production and analysis element of the MAGTF. Processes and produces all-source intelligence products in response to requirements of the MAGTF. Additionally, principal IMINT and GEOINT production element of the MEF.

MAGTF subordinate units also conduct intelligence and reconnaissance planning and operations in support of their own efforts through a variety of means. Close coordination with the ISC and IOC is essential to ensure overall effective MAGTF intelligence operations and intelligence support to all commanders. IMINT and imagery-related data and information are collected by a variety of assets, each with unique capabilities and limitations. The following MAGTF units and organizations are those most likely to be tasked with imagery-related collection missions and production support:

- Imagery intelligence platoon, intel bn.
- Marine unmanned aerial vehicle squadrons (VMUs).
- JSTARS common ground station (CGS).
- Marine fighter/attack (all weather) squadrons (VMFA[AW]s) F/A-18D.
- Marine light/attack helicopter squadron (HML/A).
- Ground reconnaissance units with Manpack secondary imagery dissemination system (SIDS) or tactical intelligence photographic (TACPHOTO) capability.

Types of IMINT Products

Major types of IMINT products include IMINT reports, hard copy prints, mosaics, overlays, annotated photographs, and various hard copy and electronic all-source intelligence products. See chapter 5 for a detailed discussion of imagery and IMINT products.

Related Terminology

Reconnaissance

A reconnaissance mission is undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (JP 1-02)

Broad Area Coverage, Broad Area Search, and Directed Search Area

These imaging strategies provide a reconnaissance capability to cover large areas of the earth's surface. These techniques are especially suited for providing large area coverage for baseline studies of terrain and lines of communication. On the negative side, they take extended time to produce large format mosaic prints, are normally produced at a low National Imagery Interpretation Rating Scale (NIIRS) rating, and possess imagery quality of only fair to poor (see appendix B for a discussion of NIIRS).

Broad area coverage (BAC), also known as broad area search (BAS), are missions entailing imagery coverage of large areas of the earth's surface that enable analysis of a greater amount of area and provide the imagery needed for the creation of large area mosaics.

Directed search area (DSA) imagery missions identify a geographic region in the shape of a polygon that may contain from 3 to 24 corner points with latitude and longitude coordinates. This gives intelligence planners the flexibility to tailor intelligence collection and other operations plans to meet commanders' needs.

Route Reconnaissance or Lines of Communications Coverage

This imagery coverage is defined by a road, mobility corridor or other form of transportation passageway delineated by a specific start and end point. This type of reconnaissance is not limited to enemy areas but may be requested to facilitate friendly logistics or troop movements. The image product is normally produced as a variation of a standard mosaic, a strip map or as a GRG.

Battlefield Surveillance

Battlefield surveillance is the systematic observation of the battle area to provide timely information and combat intelligence. The primary difference between reconnaissance and surveillance is that reconnaissance is normally a single "look" while surveillance denotes a continuous observation. Surveillance is not normally considered a capability of the imagery process, with the exception of JSTARS and UAVs. Both the JSTARS and UAV platforms have endurance limitations that do allow for the long-term continuous observation often required for operational support.

Point Target

A point target is a specified imaging target that is normally less than 1 nautical mile in diameter. It is meant for higher resolution imagery such as EO NIIRS (see appendix B for a discussion of NIIRS) of 5.0 or better to provide the clarity of detail required for specific equipment identification or for precision targeting solutions. This type of target is best suited for static/semistatic targets that will require detailed analysis to answer specific PIR and intelligence requirements (IRs). Point targets are the most common technique used in imagery collection operations.

National Imagery

National imagery refers to imagery platforms under the control of a US Government agency such as the National Imagery and Mapping Agency (NIMA). These platforms normally consist of imagery satellites used for military operations, treaty verification, mapping, and foreign humanitarian assistance.

Theater Imagery

Theater imagery refers to the imagery platforms under the cognizance of the theater combatant commander. These may include airborne platforms such as the U-2, high altitude or extended endurance UAVs, and F-14 tactical aerial reconnaissance pod system (TARPS).

Organic Imagery

Organic imagery refers to all other types of imagery platforms organic to or under the control of the MAGTF commander. These platforms range from hand-held cameras with ground reconnaissance teams to F/A-18D ATARS aircraft.

IMINT vs. Imagery

IMINT is fully analyzed and evaluated imagery and supporting detailed intelligence text reports (which may also include information from other intelligence disciplines such as SIGINT), whereas imagery consists of the raw, unevaluated pictures of an area or target. An annotated target graphic represents IMINT while either the on-screen picture or prints from the screen of a downlinked UAV represent imagery in an unevaluated form.

Role and Functions

General

IMINT and other intelligence disciplines provide information regarding the enemy and the battlespace (weather and terrain) that help the commanders reduce uncertainty; identify opportunities for success; assess risk; outline their intent; make decisions that provide focus, generate speed, and tempo; and achieve decisive results.

IMINT provides MAGTF commanders operational and tactical intelligence support. Imagery and IMINT contribute to all six specific intelligence functions: support to the commander's estimate, situation development, indications and warning (I&W), force protection, targeting, and combat assessment. Specifically, IMINT assists intelligence personnel by providing commanders with I&W of hostile action; IPB; identification of enemy disposition, location, and strength; situational development to confirm or deny enemy intentions and courses of action; and BDA to allow continual assessment of the effectiveness of friendly attacks and their effects on enemy strengths, vulnerabilities, and capabilities.

Tactical IMINT Principles

Focus on Tactical Intelligence

National and theater imagery assets support the strategic and operational levels of war as well as tactical operations. MAGTF IMINT operations focus on the generation of tactical intelligence and utilization of strategic/operational IMINT for tactical purposes. However, consideration should always be given to required timelines for processing, exploitation, production, and dissemination of imagery and IMINT products in relation to the MAGTF operational tempo when selecting an imagery system to provide tactical support. For example, a theater system may not able to tailor imagery or IMINT in the format required of the battle area in a timely enough manner to support tactical I&W decisions.

Intelligence is Focused Downward

While the management of IMINT collection and production is centralized in the MAGTF command element (CE), the focus is on providing imagery support needed to plan and execute the mission to every unit involved in the operation.

Critical products will be pushed down to the tactical commander, who will be able to pull additional IMINT support as needed.

Intelligence Activities Require Centralized Management

Scarcity of IMINT assets, the broad geographic range and operational capabilities, and the requirement to focus IMINT resources on the commander's PIR require centralized coordination and management. This centralization will be done in the MAGTF IOC, under the direction of the intel bn commander as the ISC. Although centralized management is generally required to best plan and use IMINT resources, mission, enemy, terrain and weather, troops and support available-time available (METT-T) may require the MAGTF commander to either attach or place task-organized IMINT elements in direct support of MAGTF subordinate elements to satisfy their IRs.

G-2/S-2 Facilitates Utilization of Intelligence

The intelligence officer enables effective utilization of IMINT and all other intelligence and reconnaissance activities and products throughout the unit. As the principal disseminator of intelligence and a full and continuous participant in the planning process, the intelligence officer ensures that the full implications of the IMINT and overall intelligence picture are understood. This and the full intelligence operations mission are accomplished through three key subordinate officers. The first, the G-2 operations officer, is responsible for the provision and effective use of intelligence to the commanding general, the battlestaff, the current and future operations sections, and force fires. The second, the G-2 plans officer, is responsible for this support to the future plans team. Finally, the third is the intel bn commander as the assistant chief of staff (AC/S) G-2's ISC, having principal staff responsibility for the timely dissemination of intelligence throughout the MAGTF and ensuring it is understood, complete, and if any new IRs result from it.

Tailored and Timely Intelligence

Intelligence tailored to the requirements of the user provide a useful format, effect the development of pertinent IMINT and all-source intelligence products, and thus support decisionmaking. Dissemination of these intelligence products—not simply data, pictures or information—to the right place at the right time is the guiding principle of all intelligence dissemination activities.

Utilization: The Final Step

IMINT's value is derived from its support of decisionmaking. The IMINT intelligence cycle is not complete until the IMINT that has been developed is used to plan and/or execute operations. Central to this principle is the need for intelligence personnel to ensure that disseminated IMINT and other intelligence products have been received by all needing it; that they understand it; the degree to which it satisfies their previously stated IRs; and whether it leads to new IRs.

IMINT and the Intelligence Cycle

The IMINT cycle mirrors the intelligence cycle (see figure 1-1). These steps define both a sequential and an interdependent process for developing IMINT. These steps differ from the joint intelligence cycle in its emphasis on utilization of intelligence. Imagery-related data and intelligence should be passed directly to the appropriate user—depending upon the situation, either an intelligence command and control (C2) node or directly to commanders—to meet the requirement for rapid action related to the demands of current and future operations.

Planning and Direction

Planning and directing MAGTF IMINT operations includes:

- Determining IMINT intelligence collection requirements (ICRs) intelligence production requirements (IPRs), and intelligence dissemination requirements (IDRs).

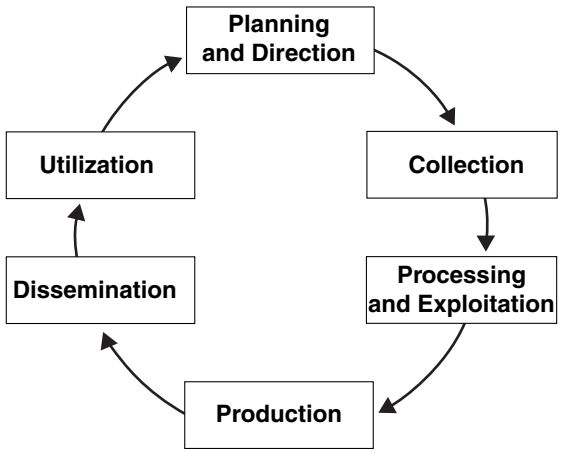


Figure 1-1. The Intelligence Cycle.

- Reviewing on-hand/accessible all-source and IMINT products and databases to see if the needed intelligence is available.
- Planning supporting collection, production, and dissemination efforts for validated requirements.
- Issuing orders and requests to IMINT and all-source agencies.
- Integrating and coordinating intelligence operations with maneuver, fires, communications and information systems (CIS) and combat service support (CSS).
- Supervising to assess the productivity of these agencies to determine if PIRs and IRs are being satisfied, and to rapidly respond to changing battlespace conditions, modifying old or initiating new IMINT orders and operations as appropriate.

The core nodes for all MAGTF intelligence planning are the G-2 plans branch within the MEF G-2 section for intelligence support to future plans; the G-2 operations branch for intelligence support to the current and future operations cells; and the support cell within the IOC established by the intelligence battalion, under the direction of the ISC, for all detailed internal and supporting intelligence and reconnaissance planning.

Effectively identifying IMINT requirements is critical to successful IMINT operations. This is true for several reasons. IMINT operations are only successful if integrated intelligence planning and direction, collection and production management, exploitation, and dissemination functions are effectively accomplished, and especially since generally limited imagery collection and production assets are available. Finally, each and every IMINT requirement requires a well-planned and potentially different technology mix of tools, significant computing power, and technically qualified personnel.

Stating IMINT requirements well is the best way to improve a unit's chances of satisfying their imagery-related intelligence requirement.

Requests for imagery support are submitted via the chain of command using the Joint Tactical Air Reconnaissance/Surveillance (JTAR/S) format shown in appendix C. These will be processed in the IOC by the ISC in coordination with the G-2 operations officer and the G-2 air officer. Requests for imagery must include the following:

Mission

State what must be accomplished, such as finding unlocated enemy forces, distinguishing certain types of tanks, assessing the status of a bridge, etc.

Type of Target

Most MAGTF tactical IMINT requirements will be for point targets of 10 nautical miles or less. Broad area search requirements are taxing in terms of communications bandwidth requirements and man-hours; and should be avoided unless absolutely necessary.

Date Desired

Date desired (DATEDES) is the date-time-group of when the requester requires either the imagery or the IMINT product.

Latest Time Intelligence Is of Value

The latest time intelligence is of value (LTIOV) is the time by which information must be delivered to the requestor in order to provide decision-makers with timely intelligence.

Intelligence Requirements

The requester must identify the specific IRs associated with the imagery/IMINT request. This should also include a statement as to the preferred format/method and quantity for the desired intelligence products.

It is critical that commanders and nonintelligence planners understand what is required of them when stating an IMINT requirement. The following actions are necessary to ensure that IMINT requirements are effectively articulated to intelligence planners, collectors, producers, and disseminators:

- State clearly what is wanted to obtain from the imagery, what specifically it will be used to support, and when you anticipate these actions to occur.

  Example
  I want to be able to clearly identify all obstacles on both approaches to the bridge across river X located at point Y to move tracked and wheeled vehicles across the bridge during the period 14-17 Oct 2000.

- State your DATEDES, which is the date and time you require the imagery or IMINT product be provided to you. This provides IMINT planners with a way of prioritizing their missions, especially when there are limited assets available. This also allows intelligence personnel the option of providing a partial or lower quality product by the DATEDES and using the limited assets for an operation in the execution phase.

  Example
  DATEDES is 1200 14 Oct 00 to support planning and briefing.

- State your LTIOV and what it will support. It is critical that the user carefully considers the date and time submitted as LTIOV, because if IMINT planners cannot meet the LTIOV, the request will be rejected.

  Example
  LTIOV 0500 15 Oct 00, 1 hour prior to the estimated crossing of the line of departure.

  Note: IMINT and intelligence planners must notify supported commanders immediately once it is identified that a LTIOV cannot be met, and that their IMINT requirement will not be supported.

- State the format you desire and at least one acceptable alternative for the IMINT products to be produced. If you have any specific requirements such as specific annotation, state that as well.

  Example
  Request that a finished imagery product be posted in JPEG format on the MEF imagery homepage accessible via either the MAGTF tactical data network (TDN) or SIPRNET. Request standard annotation set. Acceptable alternate format is hard copy print (10 each) in 11x17 inch format.

Collection

Collection is defined as the gathering of intelligence data and information to satisfy identified validated IRs. Within the MAGTF, collection management is a function of the collection management and dissemination (CMD) section that is established during operations within the IOC support cell. For IMINT, the collection phase of the intelligence cycle is complete when the imagery information and data are provided to the processing and production elements in the P&A cell. Imagery collectors available to support the MAGTF may be manned/unmanned, airborne/ground-based, systems or sensors that can operate across the MAGTF areas of interest in day or night, all-weather conditions. The IOC may substitute or supplement organic capabilities by receiving photographic, EO, infrared, radar/multispectral imagery, and IMINT from national, theater, other

Services, host country, embassy team sources, and other multinational allies.

Processing and Exploitation

Processing and exploitation involves the conversion of collected data into information suitable for the production of intelligence. Imagery processing for IMINT purposes refers to the conversion/transformation of exposed film or electronic photographic, EO, infrared, and radar imagery into a form usable for interpretation and analysis. Softcopy imagery is manipulated electronically, internal to a processing/production system. Imagery exploitation by the IIP's imagery analysts is driven by specified PIR and IRs and allows the MAGTF to gain the fullest possible advantage derived from imagery data by identifying specific pieces of equipment, measuring the dimensions of structures found on an image, identifying potential targets, assessing BDA and I&W factors, and otherwise producing IMINT from imagery data.

Production

Production is the activity that converts information into intelligence through the integration, analysis, evaluation, and interpretation of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. IMINT production refers to writing imagery reports; annotating imagery products; creating imagery-derived products; integrating and fusing IMINT into all-source intelligence products; and identifying new or remaining intelligence gaps requiring follow-on intelligence collection or production support. Most IMINT production is accomplished by the IIP, while the P&A cell within the IOC is the principal producer of all-source intelligence products.

Dissemination

Dissemination is the timely conveyance of intelligence to users in a suitable form. The ISC, per the direction and guidance of the AC/S G-2, has principal responsibly for intelligence dissemination within the MEF. The ISC must identify intelligence reporting criteria for both routine and time-sensitive intelligence, determine the forms/formats to be used, and then select the means for delivering intelligence and IMINT products to all supported commanders. For example, intelligence reporting criteria will provide imagery collectors and IMINT producers necessary guidance for when data and products will be delivered to intelligence production or C2 nodes, and when these will be disseminated directly to commanders. Formats selected may be text, graphics or other intelligence products depending upon a variety of factors (available time, capabilities of users, etc.). Further, IMINT operations must be planned and coordinated with supporting MAGTF CIS and courier operations to ensure IMINT products can be delivered or transmitted to users in a timely manner. The core nodes for intelligence dissemination execution are the IOC support cell, and the G-2 section watch within the MEF's current operations center (COC).

Utilization

The commander is responsible for the effective use of intelligence for decisionmaking purposes. Utilization of intelligence for decisionmaking during planning and execution is the ultimate objective of intelligence. The G-2/S-2 facilitates the effective use of intelligence, and thus of IMINT, by supervising the entire intelligence development effort and assisting the commander and staff in understanding intelligence products and their application. Additionally, the utilization phase provides the basis for the continuous functioning of the intelligence and supporting IMINT cycles. It will determine whether IRs have been completely satisfied; those that have not will then require additional intelligence development effort. Finally, as some IRs are satisfied, new ones will be generated. In all cases, utilization provides guidance, feedback, and orders for subsequent intelligence and IMINT operations.

G-2/S-2 Role in the Intelligence Cycle

Figure 1-2 depicts the G-2/S-2 role in the intelligence cycle and highlights that IMINT is one of the capabilities needed to support overall MAGTF intelligence requirements and operations. Since IRs are numerous, complex, and challenging, no single intelligence discipline, source or sensor can provide all of the required data and intelligence in the correct usable format. Some specific data must be processed and all of the seemingly unrelated, individual pieces of information must be evaluated, analyzed, and integrated into a usable, fused, all-source intelligence product that satisfies the commander's operational information needs.

Levels of IMINT

MAGTFs rely on a complementary mix of tactical, joint, theater, other Services, and national imagery and IMINT sources to support planning and operations (see figure 1-3). External imagery support is particularly important in viewing denied areas and assisting the MAGTF in pre-deployment planning and imagery archive development. As the MAGTF moves towards an AO, imagery support is provided by a mix of national, theater, and other Services' assets. Once a MAGTF is within the AO, its organic assets will take on greater importance and provide significant imagery support; however, support is still required from external assets to broaden the commander's view.

National IMINT

National IMINT is extremely valuable for MAGTF purposes, particularly in the early phases of MAGTF operational planning and for viewing denied areas. MAGTF requirements for national IMINT support are submitted via the operational chain of command to the Defense Intelligence Agency (DIA) for ultimate validation,

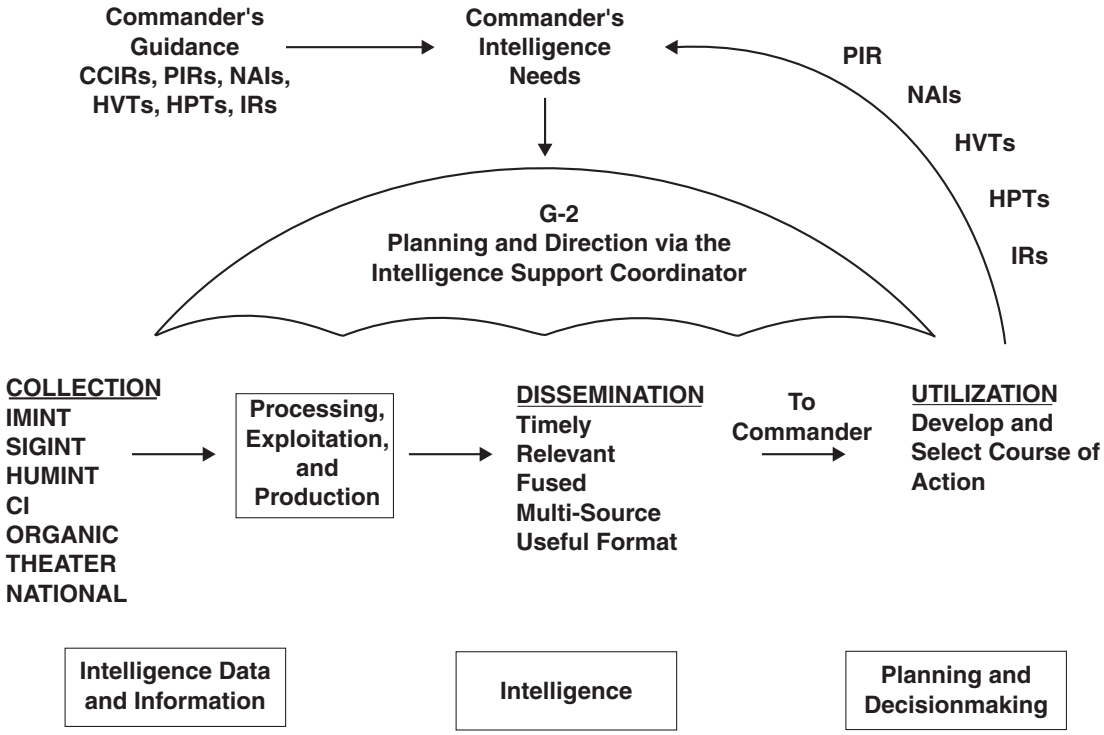
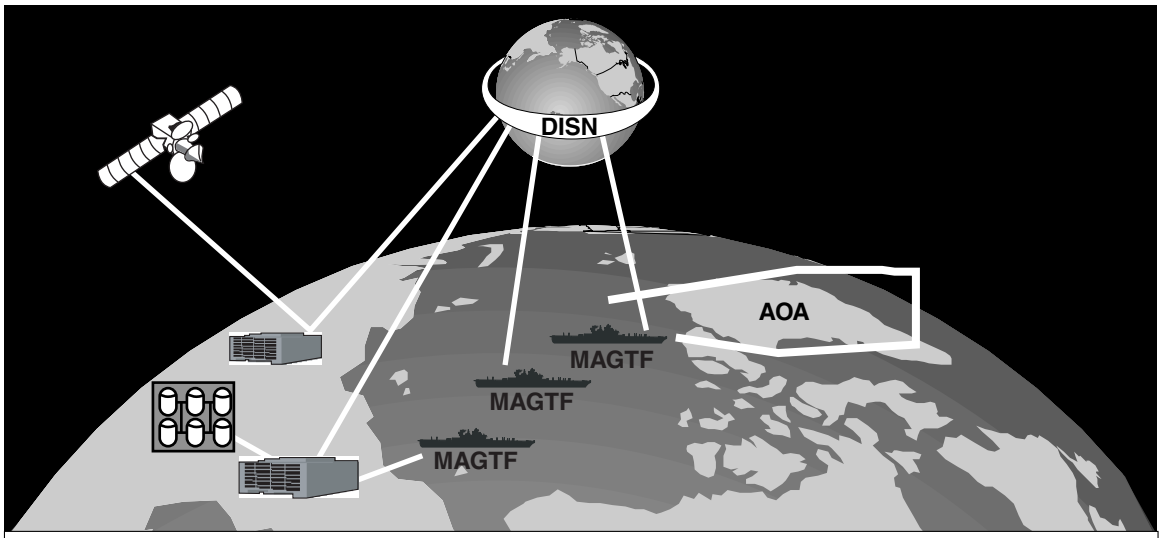


Figure 1-2. G-2/S-2 Role in the Intelligence Cycle.



Imagery Support to MAGTF Operations

Pre-deployment
- Load MAGTF IPLs with imagery
- Pre-deployment packages (CD ROM)
- Digital Imagery Database
  - Area Coverage Baseline
  - Baseline Target/Mission Data
  - Geospatial Information
  - Image Maps
  - Mosaics

En route to Area of Operations
- Over-the-Air-Updates (OTAU)
  - Automatic/Profiled Update
  - Target Update Images
  - Special Area Imagery
  - Information and Service Updates

Area of Operations
- (OTAU) and "Pull"
  - Support MAGTF Operations Plan
    - › Landing Zone Analysis
    - › Mission Planning
    - › All-source Visualization and Analysis
  - Support ATO Cycle
    - › Mission Planning
    - › Damage Assessment
  - Support Special Operations

A goal of imagery architecture development is to ensure that imagery products are available to support the MAGTF during all phases of the operation, regardless of geographic location.

Figure 1-3. External Imagery Support Request Chain.

prioritization, and coordination with pertinent elements of the national imagery community (see figure 1-4 on page 1-12). National imagery reconnaissance assets, when available, can be very responsive when at least a 6-hour lead-time exists. The passive nature of most national IMINT collection operations has the advantage of requiring minimal coordination efforts by the MAGTF beyond the initial nomination, validation, and forwarding of the imagery request. Planning time over target (TOT) parameters for most joint force air component commander (JFACC) operations is 72 hours, with aviation combat element (ACE) mission planners generally operating on a 48-hour cycle; Marine expeditionary unit (special operations capable) (MEU[SOC]) ACE and squadron level mission planners typically operate on a cycle of 24 hours or less. (Specific technical and operational capabilities and procedures for most national IMINT resources are classified; refer to either the *Joint Tactical Exploitation of National Systems* manual or theater tactics, techniques, and procedures (TTP) for additional information.)

Theater and Joint Task Force IMINT

Theater combatant commanders play a significant role in imagery support to MAGTFs because of the critical requirement for component interoperability during joint operations. Joint and theater IMINT is provided by the combatant command's organic imagery assets, such as the JSTARS, U-2, and theater UAVs. Combatant commands, through

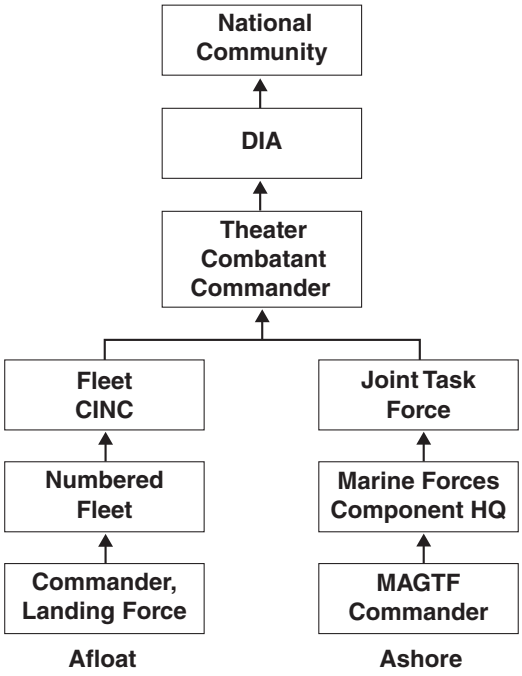


Figure 1-4. External Imagery Support Request Chain.

their joint intelligence centers and joint analysis centers, meet operational IMINIT requirements of component, subordinate intelligence centers, and joint task forces (JTFs).

Tactical IMINT

MAGTF Tactical IMINT

MAGTF tactical IMINT operations include intelligence derived from the collection, processing, exploitation, production, and dissemination of imagery derived from organic collectors (e.g., F/A-18 with ATARS), as well as imagery collected by national or theater collectors but exploited, tailored to MAGTF requirements, and fused into all-source intelligence products, and then disseminated throughout the MAGTF from the IOC. Organic collectors of imagery and imagery-related information, such as UAVs and hand-held cameras, can provide both routine and time-sensitive tactical intelligence. Because MAGTFs are task-organized, their organic capabilities and the degree of external support they require may vary. Forward-deployed MEU(SOC) engaged in forward presence missions normally have only a nucleus of imagery analysts (military occupational specialty [MOS] 0241) providing support within the CE's intelligence section and rely heavily upon external support to fulfill their imagery needs. A MEF with its significant organic imagery capability will need to rely less on external support. In either situation, a MAGTF must plan for a tailored combination of organic, joint, theater, and national imagery that meets the MAGTF's needs for imagery support. Chapters 3 and 4 address current and planned Marine Corps imagery organizations and capabilities available as organic to MAGTFs.

Amphibious Force IMINT

Landing force (LF) and amphibious task force (ATF) intelligence officers collaboratively execute ATF and LF IMINT operations. The organic IMINT capabilities of the ATF and LF are generally limited, necessitating reliance for IMINT support from secondary imagery dissemination from fleet intelligence organizations. A key IMINT resource is the three F-14 Tomcats configured with the TARPS in one of two F-14 Squadrons assigned to each carrier battle group (CVBG). TARPS has two optical sensors (day-only) and one day/night infrared imagery sensor. Navy imagery specialists exploit the film-based TARPS imagery and provide either IMINT reports or actual images to the MAGTF.

CHAPTER 2. ORGANIZATIONS AND RESPONSIBILITIES

A man trusts his ears less than his eyes.

— Herodotus, 484-424 B.C.

Developing the imagery capabilities and executing the IMINT operations to satisfy the wide variety of MAGTF requirements are extremely difficult challenges that require extensive cooperation and coordination among all members of the intelligence community—MAGTF, other Services, joint, and national. This chapter addresses the major roles and responsibilities of various IMINT-related organizations and key personnel within the operating forces and supporting establishment of the Marine Corps, as well as those external to the Corps.

MEF Key Personnel Responsibilities

The Role of the Commander

Command Attention

Intelligence is an inherent and essential responsibility of command. Command attention is critical to military success. The commander must ensure that members of the unit understand the importance placed on intelligence and the requirement to support the intelligence effort. The commander's involvement in the intelligence process encompasses focusing the intelligence effort, participating in the intelligence process, using intelligence in decisionmaking, supporting the intelligence effort, and providing personal evaluation of the intelligence effort.

Intelligence Requirements

The commander focuses intelligence and supporting IMINT efforts through articulation of commander's intent and planning guidance and identification of PIRs. These drive all resulting intelligence collection, production, and dissemination activities.

Resource Allocation

A detailed and well thought out concept of intelligence support, developed in accordance with the commander's intent and concept of operations, will provide appropriate allocation of intelligence capabilities between the MAGTF's main and supporting efforts, and between intelligence support to current operations and the continuous planning efforts for future operations. IMINT resources are limited; trained imagery analysts—as well as IMINT collection, processing, and dissemination assets—compete with nonintelligence missions for their use. Some MAGTF imagery collection assets, such as the F/A-18 ATARS and UAVs, have multimission roles and may be tasked with command and control, targeting, other intelligence, electronic warfare, or other missions in addition to imagery collection. For IMINT operations, therefore, the commander's role in mission prioritization of organic imagery airborne collection and other IMINT assets is particularly important.

Communications and Information Systems Support

The extent to which a MAGTF can request and receive JTF, theater, and national imagery support is a function of the level and effectiveness of its CIS connectivity and throughput capability from the tactical through the theater and national levels. The commander must assess CIS intelligence needs against all competing MAGTF CIS requirements to ensure necessary support is provided.

MEF Command Element G-2 Section and the Intel Bn

Assistant Chief of Staff, G-2

The AC/S G-2 has staff responsibility for intelligence and intelligence operations, to include IMINT (see figures 2-1 and 2-2). The commander relies on the intelligence officer to provide the necessary information on the weather, terrain, and enemy capabilities, status, and intentions.

Through the intelligence operations plan and supporting intelligence and R&S plans, the MEF AC/S G-2 validates and plans IRs; coordinates intelligence priorities; integrates collection, production and dissemination activities; allocates resources; assigns specific intelligence and reconnaissance missions to subordinate elements; and supervises the IMINT and overall intelligence and reconnaissance efforts. Specific all-source and key IMINT responsibilities include:

- Developing and answering outstanding MEF and subordinate units' PIR and IRs by planning, directing, integrating, and supervising organic IMINT and multidiscipline MEF and supporting intelligence operations.
- Preparing appropriate IMINT and other intelligence and reconnaissance plans and orders for the MEF, and reviewing and coordinating the IMINT and all-source intelligence plans of JTFs, theaters, and other organizations.
- Submitting and coordinating all-source and IMINT collection, production, and dissemination requirements beyond the capability of the MEF to satisfy to higher headquarters for JTF, theater or national IMINT systems support.
- Ensuring IMINT and other intelligence information is rapidly processed, analyzed, incorporated (where appropriate in all-source intelligence products), and rapidly disseminated to all MEF and external units requiring these.
- Evaluating JTF, theater, and national IMINT and all-source intelligence support and adjusting stated IRs, if necessary.
- Identifying and correcting deficiencies in IMINT and other intelligence and reconnaissance personnel and equipment resources.
- Incorporating exercise IMINT in training exercises to improve MEF individual, collective, and unit readiness.
- Facilitating understanding and use of IMINT and other intelligence in support of the planning and execution of MEF operations.

G-2 Operations Officer

The G-2 operations officer, under direction of the MEF AC/S G-2, has primary responsibility for intelligence support to the commanding general (CG) and the remainder of the MEF CE in support of current and future operations.

Specific all-source and key IMINT related duties include:

- Coordinating and providing intelligence support (to include key IMINT support) to the CG, the G-3 operations section, and the remaining MEF CE's battlestaff.
- Serving as G-2 representative to the MEF CE crisis action team (CAT).
- Coordinating, providing, and supervising intelligence support to the MEF CE COC, future operations center (FOC), and force fires.
- Planning, directing, and supervising the threat or red cell.
- Providing recommendations on PIR and IR validation, prioritization, and taskings to the AC/S G-2 and the ISC.
- Coordinating and supervising the transition of intelligence planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations, to effectively support the MEF's single battle transition process.

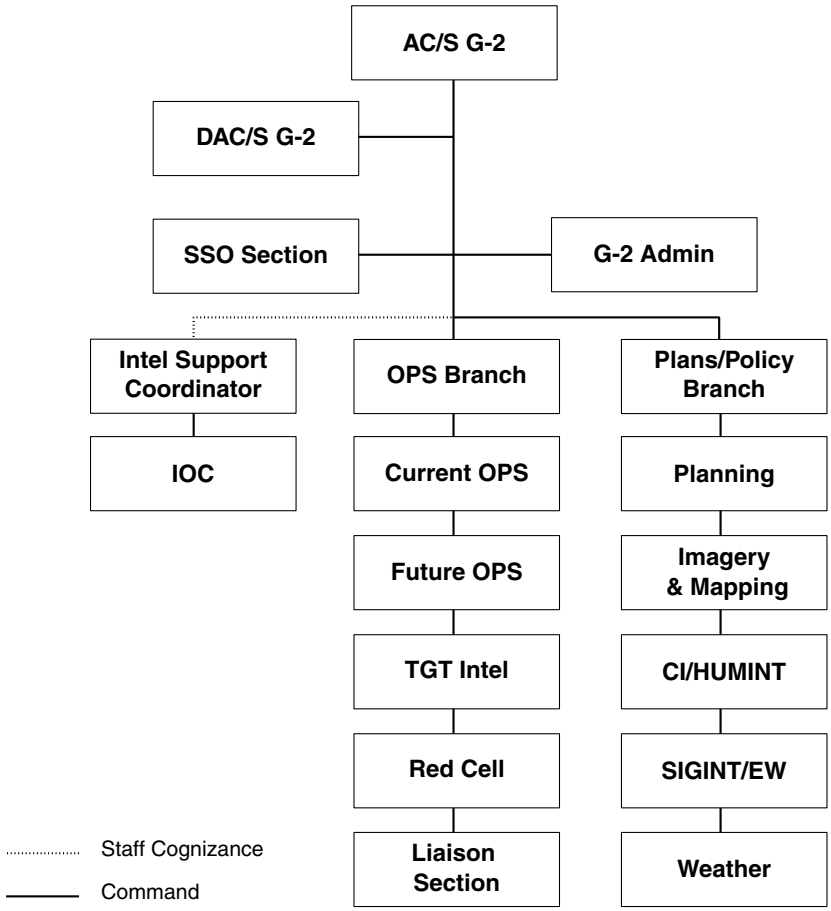


Figure 2-1. MEF G-2 Division Principal Staff Officers and Relationships.

- Planning, directing, and supervising MEF liaison teams to external commands (e.g., the JTF and joint functional components headquarters) and intelligence organizations.
- Coordinating with the ISC and MEF MSCs' G-2 operations officers to ensure unity of effort of MEF intelligence operations.
- Providing intelligence input and other support to MEF warning and fragmentary orders and to operations related reporting (e.g., periodic situation reports).
- Coordinating intelligence training for the MEF G-2 section and providing G-2 oversight for and integration of the MEF intelligence training program.
- Accomplishing other intelligence support and tasks as directed by the AC/S G-2.

G-2 Plans Officer

The G-2 plans officer, under the direction of the MEF AC/S G-2, has primary responsibility for intelligence support to the MEF CE's future plans cell. Specific all-source and key IMINT related duties include:

- Planning the MEF concept of intelligence operations for approval by the AC/S G-2 and subsequent implementation by the ISC based upon the mission, threat, commander's intent, guidance, and concept of operations. This concept of intelligence operations includes a supporting IMINT concept of operations.
- Leading, coordinating, and providing intelligence support to the MEF G-5 future plans section.

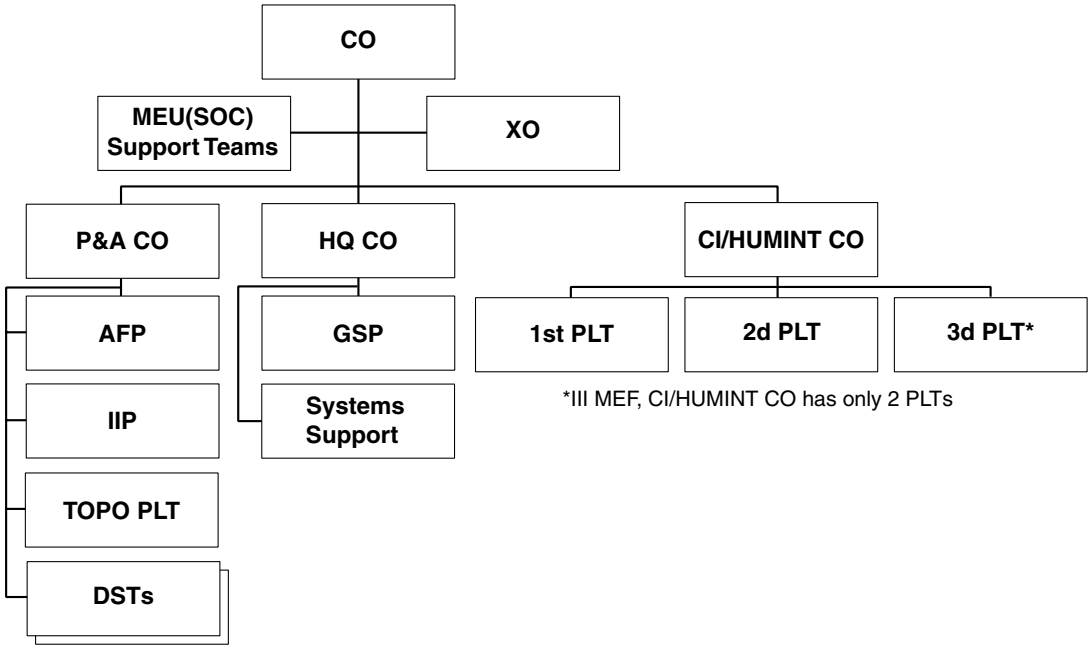


Figure 2-2. Intelligence Battalion.

- Planning and coordinating intelligence support requirements for and the deployment of intelligence elements and resources into the AO.
- Providing recommendations on PIR and IR validation, prioritization, and taskings to the AC/S G-2 and the ISC.
- Coordinating with the ISC, G-2 development of Annex B (Intelligence) and Annex M (Geospatial Information and Services) to MEF operation plans (OPLAN), their supporting appendices (such as the appendix 7, Imagery Intelligence), and all intelligence input to other annexes of OPLANs.
- Keeping the G-2 section, other CE staff sections, intelligence liaison personnel, augmentees, and others apprised of MEF intelligence planning actions and requirements.
- Identifying requirements and providing recommendations to the G-2 operations officer for MEF intelligence liaison teams to external commands (e.g., the JTF or other components' headquarters) and intelligence agencies.
- Coordinating and developing policies for MEF intelligence, CI, and reconnaissance operations.
- Planning, directing, and supervising the MEF G-2's imagery and mapping, CI/HUMINT, SIGINT, and weather sections.
- Accomplishing other intelligence support and tasks as directed by the AC/S G-2/S-2.

Intel Bn Commander/ Intelligence Support Coordinator

The intel bn commander is responsible for planning and directing, collecting, processing, producing and disseminating intelligence, and providing CI support to the MEF, MEF MSCs, subordinate MAGTFs, and other commands as directed.

Garrison. The principal task of the intel bn commander in garrison is to organize, train, and equip detachments that support MAGTFs or other designated commands to execute integrated collection, intelligence analysis, production, and dissemination of intelligence products.

Actual Operations. During operations, the intel bn commander is dual-hatted as the ISC, serving as such under the direct staff cognizance of the MEF AC/S G-2. The intel bn's S-3 section, along with the

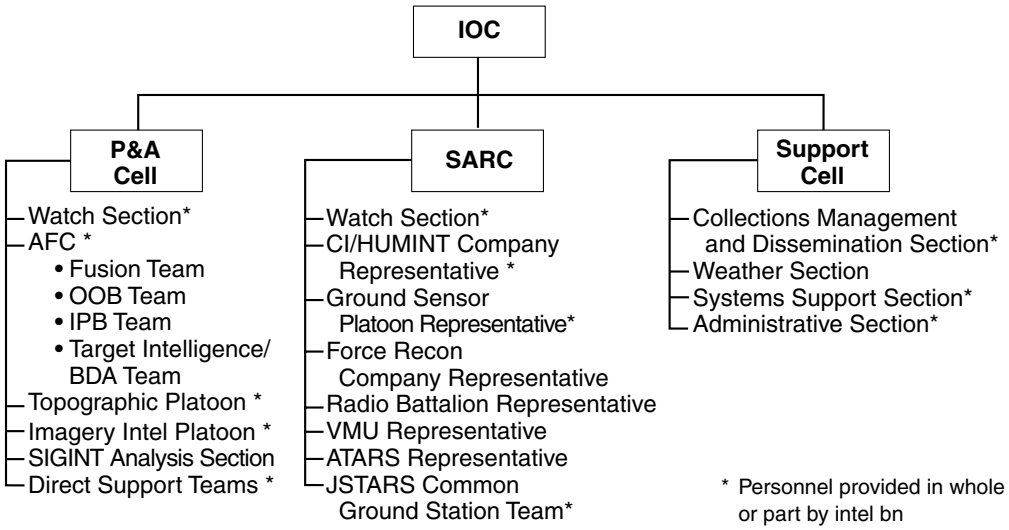


Figure 2-3. Intelligence Operations Center.

operations center element of the MEF G-2, forms the core of the ISC support effort, with planning, direction, and C2 conducted within the IOC's support cell. As the ISC, the commander is responsible to the MEF AC/S G-2 for the overall planning and execution of MEF all-source intelligence operations. Specific all-source and key IMINT responsibilities of the ISC during actual operations include:

- Implementing the concept of intelligence operations (and the supporting IMINT concept of operations) developed by the G-2 plans officer and approved by the AC/S G-2.
- Establishing and supervising operation of the MEF IOC, which includes the support cell, the SARC, and the P&A cell (see figure 2-3). Generally, the IOC will be collocated with the MEF CE's main command post.
- Developing, consolidating, validating, and prioritizing recommended PIR and IRs to support MAGTF planning and operations.
- Planning, developing, integrating, and coordinating MEF intelligence collection, production, and dissemination plans, to include the effective organic and external integration and employment of MAGTF IMINT as well as staff cognizance of MEF SIGINT, CI, HUMINT, GEOINT, ground remote sensors, ground reconnaissance, and tactical air reconnaissance intelligence collections, production, and dissemination operations.
- Developing and completing, with the G-2 plans officer and G-2 operations officer, Annex B (Intelligence) and Annex M (Geospatial Information and Services) to MEF operation orders (OPORDs), their supporting appendices (such as appendix 7, Imagery Intelligence), and all intelligence input to other annexes of OPORDs.
- Planning, developing, integrating, and coordinating intelligence and CI support for the commander's estimate, situation development, indications and warning, force protection, targeting, and combat assessment.
- Managing and fusing the threat (or red) common operational picture (COP)/common tactical picture (CTP) inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.
- Providing intelligence support to the MEF CE G-2 section and the MSCs.
- Preparing the intelligence and CI estimates to support G-2 plans.
- Planning, developing, and coordinating intelligence communications and information systems architecture, to include its integration with and support of MEF IMINT and other intelligence and reconnaissance requirements.

- Coordinating and integrating MEF IMINT and all-source intelligence operations with other service components, JTF joint intelligence support element (JISE), theater joint intelligence center (JIC) or joint analysis center (JAC), and national intelligence agencies and operations (e.g., NIMA), to include all aspects of intelligence reachback support.
- Assisting with the evaluation and improvement of MEF IMINT and all-source intelligence operations.
- Accomplishing other intelligence support and tasks as directed by the AC/S G-2.

(See table 2-1 for the principal responsibilities of the AC/S G-2's three principal staff subordinate officers.)

Collection Management/Dissemination Officer

The collection management/dissemination officer (CMDO) is sourced from the intel bn's S-3 section and is a key subordinate to the intel bn commander/ISC during operations. The CMDO is responsible for formulating detailed ICRs and IDRs and tasking and coordinating internal and external operations to satisfy these. The CMDO receives validated PIR and IRs and direction from the ISC, and then plans and manages the best methods to employ organic and supporting collection and dissemination resources through the intelligence collection and dissemination plans (tabs to Appendix 16, Intelligence Operations Plan, to Annex B), which includes all IMINT collection and dissemination activities. The CMDO is also responsible for validating and forwarding national and theater IMINT and other collection requests from the MEF and MSCs typically using appropriate intelligence tools and TTP. The CMDO also is responsible for coordinating intelligence CIS requirements and maintaining awareness of available CIS connectivity throughout the MAGTF and with key external organizations. During operations, the CMDO works within the support cell.

In coordination with the P&A cell officer in charge (OIC), the SARC OIC, G-2 operations officer, IMINT-related unit commanding officers (COs)/OICs, and the MEF G-6, the CMDO is responsible to the ISC for the following IMINT-related tasks. Determining and coordinating the collection effort of PIR/IRs that may be collected via imagery (ATARS, UAVs, national imagery databases) and supporting resources (i.e., force reconnaissance company) Determining of PIR/IRs and preparing requests for intelligence that are beyond organic capabilities and

Table 2-1. AC/S G-2ís Principal Subordinate Staff Officers and Responsibilities.

ISC	G-2 Operations Officer	G-2 Plans Officer
Planning and execution of intelligence operations to support all MEF IRs.	Providing intelligence support to MEF CE battle staff and current operations center agencies.	Providing intelligence support to the plans officer's future planning team for future planning IRs.
Establishing and directing the IOC (P&A cell, SARC, and support cell).	Coordinating intelligence support to higher and adjacent headquarters and agencies.	Recommending IR validation, prioritization, and tasking to AC/S G-2.
Managing IRs (collection, production, and dissemination), validating, prioritizing, and tasking IRs, per AC/S G-2 direction.	Recommending IR validation, prioritization, and tasking to AC/S G-2.	Establishing and directing the G-2 future planning intelligence element.
Exercising C2 of intel bn and staff cognizance over SIGINT, CI, HUMINT, measurement and signature intelligence, IMINT, and air and ground reconnaissance, including staff cognizance of designated G-2 elements.	Establishing and directing intelligence elements and support to the combat operations center, future operations center, target intelligence section, force fires, red cell, and MEF intelligence liaison teams.	Establishing and operating the intelligence section's imagery and mapping, CI, HUMINT, SIGINT, and weather sections (less that under staff cognizance of the ISC).

preparing submissions to higher headquarters and external agencies for support.

- Recommending dissemination priorities, development of intelligence reporting criteria, and advising on and selecting dissemination means.
- Developing and coordinating IMINT and all-source intelligence collection plans, coordinating and integrating these with MEF, other components, JTF, theater, and national intelligence production operations.
- Developing and coordinating IMINT and all-source intelligence dissemination plans and supporting architectures for both voice and data networked communications, and coordinating and integrating these with MEF, other components, JTF, theater, and national intelligence CIS and dissemination operations.
- Monitoring the flow of IMINT throughout the MAGTF and ensuring that it is delivered to intended recipients in a timely fashion and satisfactorily meets their needs.
- Evaluating the effectiveness of MEF and supporting IMINT collection and dissemination operations.

SARC OIC

The SARC OIC is the second immediate subordinate of the ISC and supervises the execution of the integrated organic, attached, and direct support intelligence collection and reconnaissance operations. The SARC OIC is responsible to the ISC for accomplishing the following specific IMINT-related responsibilities.

- Coordinating, monitoring, and maintaining the status of all ongoing imagery collection operations. This includes—
  - Missions, tasked ICRs, and reporting criteria for collection missions.
  - Locations and times for all pertinent fire support control measures.
  - Primary and alternate CIS plans for both routine and time-sensitive requirements, for IMINT collectors as well as between the collectors or the SARC and key MEF CE and MSC C2 nodes, to support ongoing C2 of IMINT collection operations and dissemination of acquired data and intelligence to those needing it via the most expeditious means.
- Conducting detailed IMINT collection planning and coordination with the MSCs and IMINT organizations planners, with emphasis on ensuring understanding of the collection plan and specified intelligence reporting criteria.
- Ensuring other MAGTF C2 nodes (e.g., the current operations center, force fires, etc.) are apprised of ongoing IMINT and other intelligence and reconnaissance operations.
- Receiving routine and time-sensitive IMINT-related reports from deployed collection elements; cross-cueing among intelligence collectors, as appropriate; and the rapid dissemination of IMINT reports to MAGTF C2 nodes and others in accordance with standing PIR/IRs, intelligence reporting criteria and dissemination plan, and the current tactical situation.

Production and Analysis Cell OIC

The P&A cell OIC is the third principal subordinate to the ISC, with primary responsibility for managing and supervising MEF all-source intelligence processing and production efforts, to include all aspects of IMINT production. Key all-source and IMINT-related responsibilities include:

- Planning, directing, and managing operations of the all-source fusion platoon (to include the fusion, OOB, IPB, and target intelligence/BDA teams), the topographic platoon (topo plt), the IIP, the direct support teams (DSTs), and other P&A elements as directed.
- Coordinating and integrating P&A cell operations, estimates and products with the MEF G-2 section's G-2 operations branch and its red cell operations and estimates.
- Maintaining all-source automated intelligence databases, files, workbooks, country studies, and other intelligence studies.

- Planning and maintaining imagery, mapping, and topographic resources and other intelligence references.
- Administering, integrating, operating, and maintaining intelligence processing and production systems, both unclassified general service (GENSER) and sensitive compartmented information (SCI) systems (e.g., the image product library [IPL], joint deployable intelligence support system [JDISS], intelligence analysis system [IAS]).
- Analyzing and fusing IMINT with other intelligence into tailored all-source intelligence products to satisfy all supported commanders' stated or anticipated PIRs and IRs.
- Developing and maintaining current and future intelligence situational, threat, and environmental assessments and target intelligence based upon all-source analysis, interpretation, and integration.
- Managing and fusing the threat COP/CTP inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.

IIP Commander/Detachment OIC

The IIP commander is responsible for planning and providing the MEF, and other commands as directed, with imagery and imagery analysis to support operations. Specific tasks include:

- Exploiting and analyzing all-source, multisensor imagery to derive intelligence pertaining to installations, dispositions, strengths, and activities of various conventional and nonconventional forces.
- Employing imagery methods and techniques in the planning and tasking of multisensor platforms, both those organic and external to the MAGTF.
- Conducting imagery exploitation and assisting in imagery management.
- Providing IMINT reports, limited imagery-derived products, and secondary imagery to the MEF and other commanders.
- Conducting liaison with the MCIA for obtaining imagery products in support of MEF intelligence requirements.
- Administering and managing the MEF IPL.

Other Command Element Staff

G-1

The G-1 is responsible for all personnel requirements with regard to the IMINT effort. MEF IMINT requirements may require personnel augmentation to satisfy all requirements. All requests for IMINT personnel augmentation will be developed by the MEF G-2 and provided to the G-1 for either internal sourcing or forwarding to higher headquarters for action (e.g., global sourcing).

G-3

The G-3 is responsible for planning, coordinating, and supervising the tactical employment of units. As such, the movement and operations of IMINT and supporting units must be coordinated by the G-2 with the G-3 for integration in future and current operations planning. Since some imagery supporting units also provide certain nonintelligence capabilities, close coordination between the G-2 and G-3 is necessary for mission prioritization and deconfliction. The G-3 has primary responsibility for the planning and operations of maneuver and fires, and is typically a principal staff user of IMINT, requiring close coordination throughout the planning process to ensure effective IMINT support. Accordingly, G-3 personnel must understand the capabilities of the different IMINT collection systems and exploitation and advantages and limitations of different types of imagery and IMINT products to form realistic expectations of IMINT support, to effectively and efficiently request appropriate support, and to integrate intelligence into operations.

G-4

The G-4 is responsible for the logistic support of attached IMINT units. To ensure the required support is available, arrangements should be developed early in the deployment that meet the particular needs of the deployed IMINT-supported unit. Special attention is drawn to logistics requirements of IMINT units' unique and sometimes sizable equipment (e.g., IIP).

G-5

The G-5 is the principal staff officer responsible for all long-range (future) planning and joint planning matters. Normally, a G-5 is found only at the MEF and Marine Corps forces (MARFOR) levels; at lower MEF echelons future planning is the responsibility of the G-3. The G-5 understanding of imagery/IMINT and the type of support required parallels that of the G-3.

G-6

The G-6 provides for and protects CIS connectivity and operations, both within and external to the MEF. This includes providing the communication paths, network accesses, and frequencies for IMINT organizations organic, attached to and/or supporting the command, which requires significant systems knowledge across IMINT and all-source intelligence CIS.

MEF Major Subordinate Commands' Intelligence Officers

The MSC intelligence officers must understand imagery, IMINT, and their capabilities and uses. Additionally, MSC intelligence officers must be able to articulate in detail all IMINT requests they submit through the chain of command and integrate IMINT support with other command intelligence and reconnaissance operations. Because IMINT resources are generally limited, MSC intelligence officers must recognize that their units' IMINT requirements will compete with all others from throughout the MAGTF. Close coordination among all unit intelligence officers will identify opportunities where small adjustments to IMINT requirements result in satisfying more than one unit's requirement during the same collection and/or production tasks.

Key MSC intelligence officers' IMINT tasks can include:

- Planning and implementing a concept for intelligence support based on the mission, concept of operations, and commander's intent.
- Providing centralized direction for command intelligence operations, to include IMINT elements attached to or placed in direct support of the unit.
- Consolidating, validating, and prioritizing unit IRs and IMINT needs.
- Submitting consolidated requests for external IMINT support to the MEF CE.
- Coordinating operational and CIS links to pertinent supporting external IMINT collection and production elements and operations.
- Providing timely, accurate feedback on the level of unit satisfaction regarding IMINT support received.

National Imagery Organizations

Director of Central Intelligence

The Director of Central Intelligence (DCI) is responsible for the procurement, operation, and management of national imaging systems and programs that support activities from the level of the President and/or the Secretary of Defense to forward deployed MAGTFs.

The DCI's imagery responsibilities cover all phases of the intelligence cycle including direction, collection, processing, production, and dissemination. Responsibility also includes determining current and future requirements, developing imagery-related systems, and establishing security procedures.

To fulfill IMINT-related responsibilities, the DCI has established a network of committees, subcommittees, working groups, and panels composed of representatives from national organizations, Department of Defense (DOD) agencies, and Military Services. The Marine Corps is represented on the DCI's imagery-related committees to ensure Marine Corps support requirements are identified and incorporated at the national level. These national efforts affect both current and future operations. In the near term, this Marine Corps representation maximizes programmatic support for developing new imagery systems and strategies that will provide critical support to MAGTF operations.

National Imagery and Mapping Agency

NIMA is designated a DOD Combat Support Agency. Specified tasks of the NIMA director can include:

- Organizing, directing, and managing NIMA resources.
- Planning, coordinating, and managing the tasking of national IMINT collection operations in support of military operations.
- Providing advisory tasking for theater and tactical IMINT assets, including advising imagery collection elements on collection of imagery to meet national intelligence requirements when collection elements are assigned to or under the operational control of the secretary of a Military Department or the commander of a combatant command, and not allowed by the Secretary of Defense to meet national intelligence requirements.
- Providing and managing imagery and geospatial production and analysis.
- Disseminating imagery, IMINT, and geospatial information by the most efficient, expeditious, and secure means available.
- Developing and making recommendations on national and non-national policy for imagery and geospatial intelligence.
- Developing and coordinating DOD and intelligence community systems and technical standards.

NIMA's Marine Corps Customer Support Team is the focal point for Marine Corps customer support and provides the point of accountability through which requirements are identified and needs are met. Key IMINT tasks include:

- Understanding and coordinating NIMA resources to support Marine Corps needs.
- Assessing, defining, tasking, and coordinating Marine Corps needs into IMINT production actions.
- Providing single point of accountability to the Marine Corps for requirements satisfaction.
- Prioritizing Marine Corps needs into NIMA business plans.
- Managing execution of Marine Corps programs approved for development.
- Measuring Marine Corps satisfaction with NIMA IMINT programs.
- Providing feedback on the status of Marine Corps IMINT production requirements.
- Providing IMINT production expertise to Marine operating forces.

National Reconnaissance Office

The mission of the National Reconnaissance Office (NRO) is to enable US global information superiority. The NRO is responsible for the unique and innovative technology, large-scale systems engineering, development and acquisition, and operation of space reconnaissance systems—to include critical imagery resources—and related intelligence activities needed to support

global information superiority. Its capabilities include support to I&W, monitoring arms control agreements, and support to military operations. The NRO accomplishes its mission through the on-going research and development, acquisition, and operation of spaceborne and airborne intelligence systems. NRO assets and capabilities may be tasked to support MAGTF operations under procedures described in the Joint Tactical Exploitation of National Systems manual.

Defense Intelligence Agency

DIA is a primary coordinator of several departmental imagery programs and activities that contribute to the development and operations of imagery capabilities and IMINT activities. DIA coordinates the Services' and combatant commands' imagery and IMINT requirements; manages centralized DOD collection and production management requirements programs (e.g., requirements for multispectral imagery); coordinates operational and technical interoperability requirements for intelligence dissemination (e.g., by setting data standard formats for secondary imagery dissemination systems); and sponsors and participates in numerous imagery working groups, programs, and panels to address imagery and IMINT capabilities issues. Additionally, DIA coordinates and manages National Intelligence Support Team (NIST) support to joint operations. The NIST is a deployable intelligence team comprised of special intelligence planning, CIS, and analytical support, to include national IMINT support. NIST composition may include elements from DIA, the National Security Agency (NSA), the Central Intelligence Agency (CIA), and NIMA.

Marine Corps Supporting Establishment Imagery Intelligence Organizations

The Commandant of the Marine Corps (CMC) is directly responsible for the internal organization, training, efficiency, and readiness of the Marine Corps; for the operation of its material support system; and for the total performance of the Marine Corps.

Various Marine Corps supporting establishment organizations are staffed with personnel carrying out responsibilities pertaining to IMINT and imagery-related matters. Major organizations are listed below.

Headquarters, U.S. Marine Corps

Intelligence Department
Imagery Plans and Policies Branch

The Marine Corps Director of Intelligence implements those CMC responsibilities as they relate to IMINT and other imagery matters through the Imagery and Geospatial Plans and Policy Branch. Specific imagery and IMINT-related tasks include:

- Developing Marine Corps plans and policies for IMINT.
- Validating Marine Corps requirements for national imagery collection, production, and dissemination of imagery and all-source intelligence products. As the Marine Corps Departmental Requirements Officer (DRO), Imagery and Geospatial Plans and Policy is the final service validation and adjudication authority for all USMC national imagery and IMINT requests submitted through the service (vice operational) chain of command.
- Executing duties as the Marine Corps national imagery community representative on numerous DOD and intelligence community committees, subcommittees, working groups, and panels.
- Advising NIMA on matters pertaining to Marine Corps imagery capabilities and limitations in a joint and multinational environment.
- Coordinating with Marine Corps Combat Development Command (MCCDC) and Marine Corps Systems Command (MARCORSYSCOM) on matters related to IMINT doctrine, organization, training and education, equipment, and support combat capabilities development.

Aviation Department

The Deputy Commandant for Aviation, Headquarters, Marine Corps (HQMC) Aviation Department (AVN), coordinates closely with Navy aviation elements for procurement of manned and unmanned tactical aviation platforms and sensors. In this capacity, critical IMINT programs, such as ATARS and UAV, fall under AVN cognizance.

Marine Corps Combat Development Command

The mission of MCCDC is to develop Marine Corps warfighting concepts and to determine associated required capabilities in the areas of doctrine, organization, training and education, equipment and support facilities to enable the Marine Corps to field combat-ready forces; and participate in and support other major processes of the Combat Development System.

Marine Corps Systems Command

MARCORSYSCOM plans and manages research, development, and acquisition programs through equipment production and fielding for employment by MAGTF forces, to include most imagery and IMINT supporting equipment programs (e.g., SIDS).

Marine Corps Intelligence Activity

The Marine Corps maintains a Service-level intelligence capability within MCIA. MCIA provides tailored intelligence and services that support HQMC; develops Marines Corps doctrine, force structure, force modernization, training and education, acquisition policy and programming; and Marine Corps forces contingency planning and other requirements for intelligence products not satisfied by theater, other Service or national research and analysis capabilities. MCIA focuses on crisis and predeployment support to expeditionary warfare. It complements the efforts of theater, other Services, and national intelligence organizations and provides unique all-source threat, technical, and GEOINT products tailored to Marine Corps operating forces needs. It also coordinates Marine Corps Service imagery collection, production, and dissemination requirements by acting as the Marine Corps Service IMINT collection, production, and dissemination manager, to include taskings of the USMC Reserve's IIP. MCIA is collocated with the National Maritime Intelligence Center (NMIC), Suitland, MD, and at Marine Corps Base, Quantico, VA.

CHAPTER 3. MAGTF IMINT UNITS AND ORGANIZATIONS

Within the Marine Corps, units responsible for the conduct of tactical IMINT are the IIPs, intelligence direct support teams, VMUs, VMFA(AW)s, and ground reconnaissance elements. This chapter describes these units' missions, tasks, organization, and concepts of employment.

Imagery Intelligence Platoon, Intelligence Battalion

Mission

The mission of the IIP is to provide imagery analysis and IMINT support to MAGTFs and other commands as directed.

Tasks

- Exploit and analyze all-source, multisensor imagery to derive intelligence pertaining to installations, dispositions, strengths, and activities of various conventional and nonconventional forces.
- Employ imagery methods and techniques in the planning and tasking of multisensor platforms, organic and external to the MEF or supported MAGTF.
- Conduct exploitation and assist in imagery management.
- Provide IMINT reports, limited imagery-derived products, and secondary imagery to the MEF and other commanders.
- Conduct liaison with the MCIA for the purpose of obtaining imagery products in support of MEF or supported commander's IRs.

Organization

Each MEF has one organic IIP. It is a subordinate unit of the P&A company, intel bn. Each IIP is organized into three elements: a platoon headquarters, two tactical imagery analysis sections, and three imagery analysis teams (see figure 3-1).

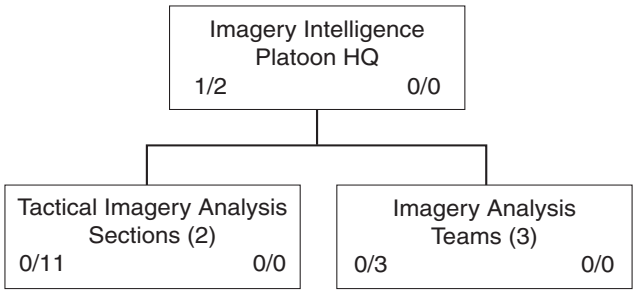


Figure 3-1. IIP Organization.

The 4th Imagery Interpretation Unit (IIU) is in the Reserves. It is organized into a headquarters section, four imagery teams, and a general intelligence support team. It is OPCON to Marine Corps Forces Reserve and ADCON to Marine Air Control Squadron 23. A memorandum of understanding exists that enables the MCIA to task and coordinate 4th IIU imagery exploitation, production, and training support of operating forces requirements.

Command and Control

The IIP is a subordinate unit of the intel bn, with the intel bn commander maintaining full command of its operations. When supporting smaller MAGTFs, the IIP or its detachments will operate under the C2 of either the intel detachment OIC or the supported unit's G-2/S-2.

MEF CE Staff Cognizance

The MEF commander usually exercises C2 over the intel bn elements, to include the IIP, via the MEF intelligence officer. The ISC performs this

function, however, under the staff cognizance of the AC/S G-2.

The ISC in turn exercises C2 of topo plt via the P&A cell OIC. This allows for the centralized direction and effective integration of IIP operations with other MEF IMINT operations and the broader all-source intelligence concept of operations.

Support Relationships

General Support. The IIP will typically operate in general support of the MEF. Under general support, the MEF commander, through the G-2 and the ISC, determines priorities of intelligence collections and production support, locations of IMINT support nodes, and IMINT and all-source intelligence dissemination.

Direct Support and Attached. Depending upon METT-T considerations, the IIP or task-organized imagery analysis detachments from it may be employed in direct support of or attached to a particular unit or MSC of the MEF. In such cases the scope of the supported commander's C2 authority over assigned IIP elements will usually be specified to ensure effective support to operations while allowing the MEF commander to maintain effective C2 of broader intelligence and IMINT operations. Direct support or attachment may consist of dedicated imagery exploitation support, placement of IIP assets with the supported unit, or simply establishing an IMINT node to provide direct dissemination of imagery and IMINT to the supported unit's intelligence section or COC. In the latter relationship, an IIP liaison element should be provided to the supported unit and continuing relationships between IMINT elements and supported units should be established whenever possible.

Concept of Employment

An IIP is capable of supporting one MEF. In support of a Marine Expeditionary Brigade (MEB), MEU(SOC) or other MAGTF, a task-organized imagery analysis detachment may be attached to the MAGTF CE either independently or as part of a larger intel bn detachment. (Some operations may require the activation of X/C-coded billets or global sourcing from other IIPs.)

The reserve 4th IIU conducts peacetime training and production activities in garrison at Buckley Air National Guard Base, Aurora, CO. All IIP production activities support Marine Corps operating forces' OPLAN intelligence requirements. The 4th IIU is capable of providing 24-hour contingency support on-site or providing limited personnel for active duty support.

During MEF operations, the operation of the tactical exploitation group (TEG) will be a focal point of IIP support (see figure 3-2). Each IIP in the operating force will have one TEG. It is packaged in three high mobility, multipurpose wheeled vehicles (HMMWVs). The TEG has the capability to receive, exploit, and produce imagery and IMINT products and reports in support of MAGTF requirements. As such, it will be interoperable with EO, infrared, and radar imagery from ATARS-equipped USMC F/A-18D; the synthetic aperture radar (SAR) system (ASARS-2) aboard the U-2R/U-2S; and with the MCIA, combatant command JICs, and other imagery platforms and organizations. Additionally, the TEG provides the capability to exploit film-based imagery and output from digital cameras and various aircraft heads-up displays/forward-looking infrared (FLIR) and gun camera tapes. Once received and processed/exploited, the imagery is then transmitted over available SIDS device(s) or via other CIS means. Exploited imagery from the TEG may then be hosted on the IPL server located with the IIP, from which MEF users can pull images to support future IRs.

Miscellaneous

Communications and Information Systems

The IIP has sufficient communications resources to support internal and detachment C2 requirements. The IIP will require access to various networks to conduct its operations, to include the SECRET Internet Protocol Router Network (SIPRNET), the

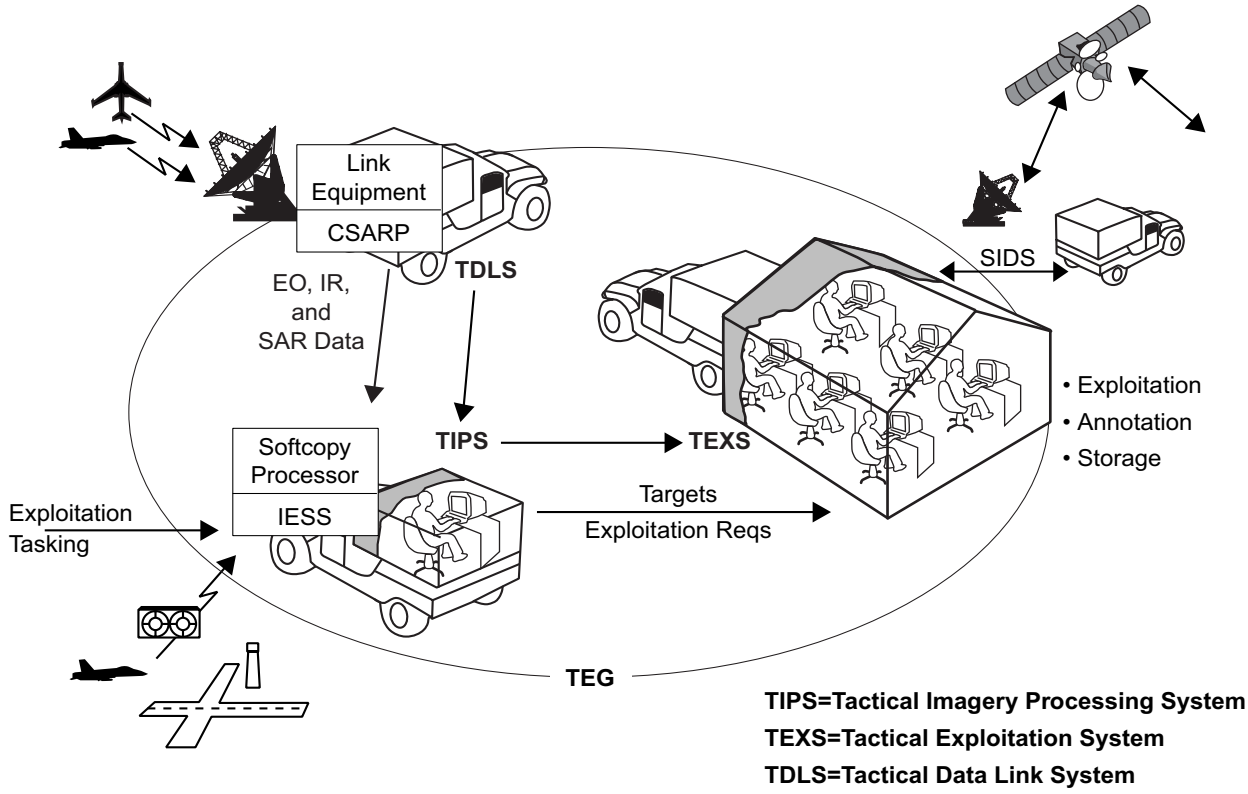


Figure 3-2. Tactical Exploitation Group Concept of Employment.

Joint Worldwide Intelligence Communications System (JWICS), pertinent MEF local area networks (LANs), and designated wide area networks (WANs). There are, however, no communications personnel organic to the IIP or to the intel bn. Communications requirements beyond these must be provided by communications battalion or the supported unit.

The IIP will require at a minimum a dedicated 512 kilobytes per second communications connectivity via SIPRNET to pull imagery from national, theater, and other sources and to disseminate finished IMINT products throughout the MEF and to others as required. This communication requirement is based upon providing a sustained new imagery production rate of 75 images per day for the IIP which is equivalent to their maximum exploitation capability (based upon the current numbers of imagery interpreters and equipment in the IIP's table of organization [T/O] and table of equipment [T/E]) and the baseline projected requirement for the MEF CE and all MSCs to pull from the imagery archive.

Maintenance

The IIP is capable of 1st through 4th echelon maintenance of organic imagery equipment through Marines and civilian contract technicians organic to the platoon. All other maintenance support must be provided by the MEF headquarters group (MHG), combat service support element (CSSE) or supported unit.

Transportation

Intel bn has limited organic vehicular transportation assets to support IIP operations. External transportation support from the MHG, the CSSE, or the supported unit is necessary to displace the entire IIP simultaneously.

Joint Surveillance Target Attack Radar System Common Ground Station

Mission

The primary mission of the JSTARS CGS is to provide the MEF with near-real-time (NRT) access to the moving target indicator (MTI), fixed target indicator (FTI), and SAR data from the Air Force JSTARS collection platform, the E-8C.

Tasks

- Receive, process, manipulate, store, and display MTI, FTI, and SAR data from the JSTARS sensors simultaneously.
- Disseminate JSTARS data to the MEF G-2, other elements of the MEF, and other forces as directed.
- Assist with the planning and direction of JSTARS operations in support of the MEF.
- Provide the capability to communicate, via voice or digital link, with the JSTARS aircraft.

Organization

I, II, and III MEF have one JSTARS CGS and one JSTARS work station that will be used to source all MAGTF JSTARS requirements.

Command and Control

Intel bn commander maintains full command of JSTARS CGS activities.

MEF CE Staff Cognizance

The MEF commander will usually exercise C2 over the intel bn elements, to include the JSTARS CGS, via the MAGTF intelligence officer. The intel bn commander, as the ISC, performs this function under the staff cognizance of the AC/S G-2. This allows for the centralized direction and effective integration of JSTARS operations with other MAGTF IMINT operations and the broader all-source intelligence concept of operations.

Support Relationships

The JSTARS CGS will operate in general support of the MEF.

Concept of Employment

E-8C

Although the JSTARS aircraft is operated and maintained by the Air Force, it is considered a national asset. Its primary mission is the dedicated support of a JTF's joint force land component commander or ground component commander under the overall direction of the joint force commander (JFC).

Properly employed, JSTARS is capable of performing intelligence support, attack support, and battle management functions, along with support to special missions. Its sensor suite provides detection and tracking of moving targets through use of MTI, FTI, and SAR radars. Radar data collected by the E-8C is distributed via an onboard LAN to an encrypted, highly jam-resistant surveillance and control data link (SCDL) for real-time transmission to an unlimited number of CGS.

CGS

The CGS generally will be located within the IOC, near the P&A cell. Once the JSTARS information is received from the E-8C at the CGS, the entire MTI/FTI/SAR image will be disseminated throughout the MEF in accordance with intelligence reporting criteria stipulated by the MAGTF intelligence officer. Under routine conditions this data will be disseminated to the P&A cell for follow-on analysis and fusion with other intelligence data into all-source intelligence products.

Additionally, METT-T factors may require that E-8C data be provided to other elements of the MEF. Under such situations, this data is disseminated to subordinate units via the MEF TDN. The MTI/FTI/SAR image, with its associated data, will be viewed by recipients using common USMC hardware and software suites (potentially down to and including the regimental/group level).

Miscellaneous

Communications and Information Systems

The JSTARS CGS has sufficient communications resources to support internal C2, operations, and intelligence requirements as well as external CIS with the E-8C aircraft. Typically, the JSTARS CGS will require access to the SIPRNET, Nonsecure Internet Protocol Router Network (NIPRNET), possibly JWICS, and pertinent LANs and WANs. CGS team members operate all organic CIS equipment. CIS requirements beyond these must be provided by the MEF communications battalion.

Maintenance

The JSTARS CGS team is capable of 1st through 4th echelon maintenance of organic imagery equipment. All other maintenance support must be provided by the MHG or CSSE.

Transportation

The JSTARS CGS team has sufficient resources to displace all CGS equipment. Additional support will be necessary from the MHG or CSSE to displace CGS personnel simultaneously.

Selected Items of Equipment

CGS. The JSTARS CGS consists of two heavy HMMWVs with integrated shelters and an organic mobile electric power generator. The mission vehicle contains two workstations and associated communications equipment that enable the CGS operators to download, manipulate, and disseminate MTI, FTI, and SAR data received from the JSTARS aircraft. The support vehicle provides transportation for the crew and contains the SCDL antenna that links the CGS to the aircraft.

E-8C. The E-8C is a 707-300 series aircraft that has been extensively remanufactured and modified to achieve like-new performance and a greatly extended service life (see figure 3-3). The most prominent external feature of the modified aircraft is the 26-foot long, canoe-shaped radome located under the forward fuselage. An in-flight refueling system extends the E-8C's 11-hour mission endurance, making missions of 20 hours or more possible. The E-8C's 140-foot long cabin readily accommodates the operator workstations communications suite and associated equipment, with space for rest areas and other crew facilities (see figure 3-4). The standard mission crew complement is 21, but an augmented mission crew of 34 can be easily accommodated.

Figure 3-3. E-8C JSTARS Aircraft.

Figure 3-4. E-8C JSTARS Air Force and Army Crew Onboard Positions.

Direct Support Teams, Production and Analysis Company, Intelligence Battalion

Mission

The mission of DST is to provide enhanced intelligence planning and direction, analytical, production,

and dissemination capabilities to designated supported-unit(s) intelligence sections.

Tasks

- Provide connectivity to the P&A cell for the receipt and dissemination of intelligence to the supported unit.
- Assist the supported unit's intelligence officer in the formulation and management of external intelligence support requirements and other intelligence planning and direction activities.
- Tailor P&A cell and other external-source intelligence products to the needs of the supported unit.
- Perform IPB in support of future operations planning.
- Prepare intelligence products to support detailed mission planning and execution by MEF MSCs or other supported units.
- Augment and enhance the dissemination efforts of the supported unit's intelligence section.
- Act as liaison between the supported unit and the P&A cell.

Organization

There are two DSTs within the P&A company, intel bn. Each team is led by a gunnery sergeant, MOS 0231. Each team also has one imagery analyst (a staff sergeant) to assist with imagery planning and IMINT activities. Other team members include one terrain analyst, two intelligence specialists, and one intelligence clerk. The DST, however, does not have any specialized IMINT equipment.

Command and Control

The DSTs are subordinate units of intel bn, with the intel bn commander maintaining full command of its activities. Under their principal concept of employment, DSTs are under the OPCON of the supported unit commander. The supported commander will exercise OPCON via the unit's intelligence officer. Intelligence taskings to the DSTs will be via the DST team leader in accordance with the supported unit's concept of intelligence operations.

Concept of Employment

The DSTs are primarily employed as organic teams either attached to or placed in direct support of a designated subordinate commander (e.g., the MEF main effort, a MEU/MEB, a special purpose MAGTF). When not employed, DSTs generally augment the P&A cell.

Miscellaneous

Communications and Information Systems

The DSTs have sufficient CIS resources to support internal and detachment C2 and intelligence requirements. They typically will require access to the SIPRNET, NIPRNET, possibly JWICS, and pertinent LANs and WANs. There are no communications personnel organic to the DST. CIS requirements beyond these must be provided by the supported unit.

Maintenance

The DST is capable of 1st echelon maintenance of organic equipment. All higher maintenance is provided by the MHG, CSSE or the supported unit.

Transportation

Intel bn has limited organic vehicular transportation assets to support battalion and DST operations. External transportation support from the MHG, CSSE or the supported unit generally will be necessary to displace the full DST.

Marine Unmanned Aerial Vehicle Squadron

Mission

The VMU operates and maintains a UAV system to provide unmanned aerial reconnaissance support to the MEF or other supported units.

Tasks

- Conduct aerial reconnaissance (to include imagery collection and reporting), surveillance, and target acquisition. This includes performing airborne surveillance of designated target areas, MEF or other areas of interest, and other areas as directed; airborne surveillance for search and rescue and tactical recovery of aircraft and personnel; and reconnaissance of helicopter approach and retirement lanes in supporting vertical assaults.
- Provide real-time target information to the direct air support center and fire support coordination center(s) to facilitate adjusting fire missions and close air support.
- Provide real-time intelligence reporting to the SARC to support MEF IRs and facilitate all-source intelligence operations.
- Provide information to assist adjusting indirect-fire weapons and to support and facilitate direct air support and air interdiction.
- Collect information to support BDA and combat assessment.
- Support rear area security.
- Provide VMU remote receive station (RRS) capability and liaison to designated units.

Organization

The VMU is organic to the Marine aircraft wing (MAW) and is structured to operate as a subordinate unit of one of the Marine air control groups (MACGs). There are two VMUs within the Marine Corps: VMU-1 (MACG-38, 29 Palms, CA) and VMU-2 (MACG-28, Cherry Point, NC). The VMU is organized into various sections that give it the capability to operate and maintain one UAV system and associated support equipment. Regarding IMINT operations, VMU has one Pioneer short-range (SR) system with five UAVs. Key squadron sections include: the S-2 section, including collections, all-source intelligence and five imagery analysts; UAV systems mission commanders and the external and internal UAV operators within the S-3 section; and the Marine aviation logistics squadron augment section that provides intermediate-level aviation maintenance and supply support.

Command and Control

General

VMU is under the command of the MAW CG or, when deployed in support of MAGTFs smaller than a MEF, the ACE commander. The commander exercises C2 via the ACE G-3/S-3 and the Marine air command and control system (see MCWP 3-25, *Control of Aircraft and Missiles*). Air operations (flight taskings, airspace deconfliction, etc.) are planned, coordinated, and controlled by the ACE G-3/S-3 via the tactical air command center (TACC). Intelligence missions, however, are in accordance with the intelligence and reconnaissance mission requirements designated by the MEF or supported unit commander, requiring close coordination between the intel bn's IOC and the MAW's TACC. To assist with UAV mission planning and execution, VMU will generally provide a task-organized team to the IOC, which will typically operate from within the SARC.

Support Relationships

General Support. VMU typically operates in general support of the MEF. Under general support, the MEF commander, through the G-2, determines VMU intelligence priorities and information and intelligence dissemination flow. The AC/S G-2 will exercise staff cognizance of VMU intelligence operations via the ISC.

Direct Support. Depending upon METT-T considerations, specified VMU missions may be in direct support of a particular MEF unit or MSC (e.g., to the Marine division or its main effort). In such cases the scope of the supported commander's C2 authority over VMU missions will usually be specified to ensure effective support to the operations while allowing the MAGTF commander to maintain effective C2 of broader intelligence and IMINT operations. Direct support may entail dedicated C2, planning, and exploitation support to the supported unit via a VMU detachment with a RRS capability.

Concept of Employment

Operational

VMU can support any size MAGTF. Normal employment would be as an integral unit of the MAGTF's ACE in support of MAGTF operations. The squadron is also capable of limited independent operations.

Intelligence

The VMU may conduct limited imagery exploitation or analysis. Generally, UAV imagery is screened by VMU imagery analysts for information of immediate tactical value in accordance with the intelligence collection and reporting criteria stipulated by the ISC or the supported unit's intelligence officer. Imagery tapes are subsequently delivered by VMU to the IIP for further detailed imagery analysis and IMINT and all-source intelligence production. The MAGTF intelligence officer is responsible for subsequent IMINT dissemination (to include secondary imagery dissemination).

Miscellaneous

Communications and Information Systems

Together with CIS resources supporting the Marine air command and control system (MACCS), VMU has sufficient CIS resources to support internal and squadron C2, operations, and intelligence requirements. VMU typically requires access to various networks to conduct its operations, to include SIPRNET and NIPRNET, and to pertinent LANs and WANs.

Maintenance

VMU is capable of conducting 1st and 2d echelon maintenance on assigned ground equipment, including motor transport, engineering, and communications equipment. The force service support group (FSSG) or supporting CSS detachment performs 3d and 4th echelon maintenance on ground equipment. The squadron is also capable of performing organizational maintenance on its aviation equipment. The Marine aviation logistics squadron performs limited, specialized intermediate-level maintenance on squadron aviation equipment.

Equipment

See appendix D for detailed information on VMU equipment and performance characteristics.

Marine All-Weather Fighter Attack Squadron

Mission

The mission of the VMFA(AW) is to attack and destroy surface targets, day or night, under adverse weather conditions; conduct multisensor imagery reconnaissance; provide supporting arms

coordination; and intercept and destroy enemy aircraft under all weather conditions.

Tasks

- Conduct day and night close air support, under all weather conditions.
- Conduct day and night deep air support, under adverse weather conditions, including armed reconnaissance, radar search and attack, air interdiction, and strikes against enemy installations, by using all types of weapons that are compatible with assigned aircraft.
- Conduct multisensor imagery reconnaissance, including prestrike and poststrike target damage assessment and visual reconnaissance.
- Conduct day and night supporting arms coordination, including forward air control, tactical air coordination, and artillery/naval gunfire spotting.
- Intercept and destroy enemy aircraft in conjunction with ground and airborne fighter direction.
- Conduct battlespace illumination and target illumination.
- Conduct armed escort of friendly aircraft.
- Maintain the capability to conduct suppression of enemy air defense operations.

Organization

There are six F/A-18D VMFA(AW)s in the operating forces. Each squadron has 12 reconnaissance-capable aircraft. However, only four can be configured with ATARS at any one time to provide this aerial reconnaissance capability. The VMFA(AW) will normally function as an integral unit. It is structured to operate as a subordinate unit of a MAG.

Command and Control

General

The VMFA(AW)s are under the command of their parent group commander. Overall, OPCON rests with the MAW or ACE commander. The commander exercises C2 via the ACE G-3/S-3 and the MACCS (see MCWP 3-25). Air operations (flight taskings, airspace deconfliction, etc.) are planned, coordinated, and controlled by the ACE G-3/S-3 via the TACC. Intelligence missions, however, are in accordance with the mission requirements designated by the MEF or supported unit commander, requiring close coordination between the intel bn's IOC, the TACC, and supported commanders.

Support Relationships

General Support. VMFA(AW)s typically operates in general support of the MAGTF in accordance with missions contained in the air tasking order (ATO).

Direct Support. Depending upon METT-T considerations, specified VMFA(AW) missions may be in direct support of a particular unit or the ACE or CSSE of the MAGTF. The ATO will identify such missions and pertinent C2 and intelligence operations direction.

Concept of Employment

Operational

The VMFA(AW) will normally be employed as an integral unit of an ACE in support of MAGTF operations.

Intelligence

When equipped with ATARS and tasked to conduct imagery collection missions, the squadron coordinates operations closely with the IOC, the MAW's G-2, the IIP, and others as appropriate. Prior to the fielding of the common data link (CDL), exploitation and processing of ATARS imagery will take place once the aircraft has returned to base and the imagery data tapes are physically downloaded and delivered to the IIP.

Once the CDL is fielded, VMFA(AW) will be capable of NRT downlinking of selected images; the remaining imagery data will be recorded on

tape and downloaded postmission for follow-on delivery to the IIP for imagery exploitation. Figure 3-5 provides an overview of VMFA(AW) ATARS operations.

Miscellaneous

Administrative

The VMFA(AW) is capable of self-administration.

Communications and Information Systems

Together with CIS resources supporting the MACCS, VMFA(AW) has sufficient CIS resources to support internal and squadron C2, operations, and intelligence requirements. VMFA(AW) typically will require access to various networks to conduct its operations, to include SIPRNET, NIPRNET, and pertinent LANs and WANs.

Maintenance

The squadron is capable of conducting 1st echelon maintenance on all assigned equipment. It is also capable of performing organizational maintenance on assigned aircraft and support equipment. Maintenance beyond these capabilities is provided by other ACE and CSSE elements.

Marine Light/Attack Helicopter Squadron

Mission

The HML/A provides combat utility helicopter support, attack helicopter fire support, and fire support coordination during expeditionary operations.

Tasks

- Provide fire support and security for forward and rear area forces.
- Conduct point target/antiarmor operations.
- Conduct antihelicopter operations.
- Provide armed escort, control, and coordination for assault support operations.

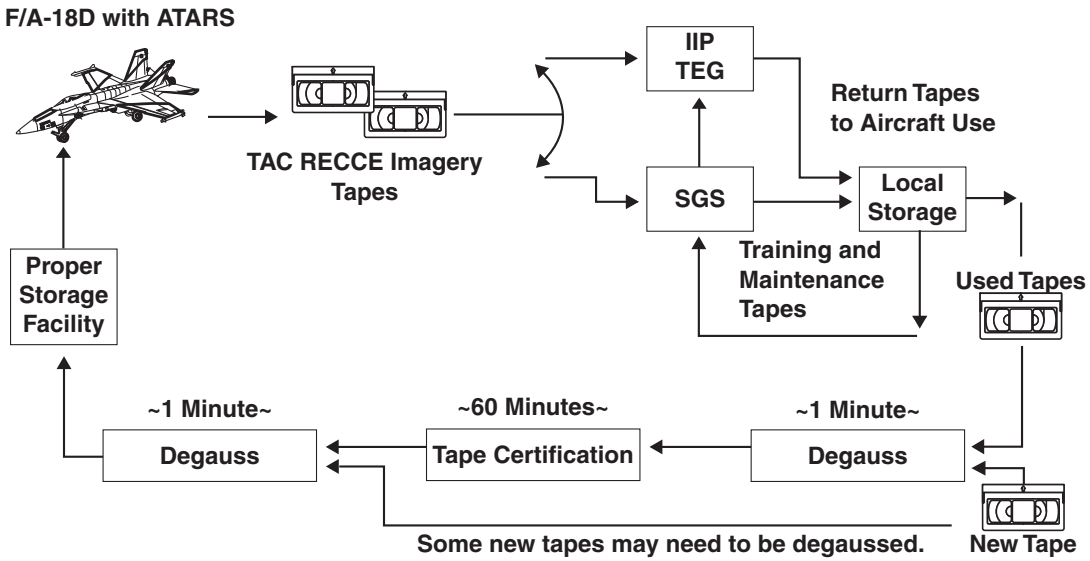


Figure 3-5. F/A-18 ATARS Tactical Reconnaissance Imagery Tape Processing Flow.

- Control, coordinate, and provide terminal ordnance for supporting arms, including close air support, artillery, mortars, and naval gunfire.
- Provide point and limited-area air defense from threat fixed-wing aircraft.
- Conduct armed imagery and visual reconnaissance.
- Augment local search and rescue assets.
- Maintain the capability to operate from amphibious shipping, other floating bases, and austere shore bases as required.
- Maintain the capability to operate at night, in adverse weather conditions, and under instrument flight conditions at extended ranges.
- Perform organizational maintenance on assigned aircraft in all environmental conditions.

Organization

There are six HML/As in the operating forces. Each squadron has 18 AH-1W Super Cobras and 9 UH-1N Huey aircraft, all are reconnaissance capable. An HML/A will normally function as an integral unit, and is structured to operate as a subordinate unit of a MAG.

Command and Control

General

The HML/As may remain under the command of their parent group commander. An HML/A may be attached to a MAGTF where they would operate under the direction of an ACE commander. The commander exercises C2 via the ACE G-3/S-3 and the MACCS (see MCWP 3-25). Air operations (flight taskings, airspace deconfliction, etc.) are planned, coordinated, and controlled by the ACE G-3/S-3 via the TACC. Intelligence missions, however, are in accordance with the intelligence and reconnaissance mission requirements designated by the MEF or supported MAGTF/unit commander and exercised via the staff cognizance of the MAGTF G-2/S-2, requiring close coordination between IOC, the TACC, the squadron, and the supported commanders.

Support Relationships

General Support. HML/As typically operate in general support of the MAGTF in accordance with missions contained in the ATO.

Direct Support. Depending upon METT-T considerations, specified HML/A missions may be in direct support of a particular unit or major subordinate elements of the MAGTF. The ATO will identify such missions and pertinent C2 direction.

Concept of Employment

Operational

HML/A will function either as an integral unit or as a squadron (-) with separate aircraft composite detachments. Each HML/A can support the simultaneous deployment of three detachments consisting of six AH-1W and three UH-1N aircraft per detachment. This concept of organization facilitates dual-site operations, provides for the support of simultaneous contingencies, and allows for the fulfillment of continuous unit deployment program requirements.

Intelligence AH-1W Night Targeting System

The night targeting system (NTS) is an airborne EO system designed to provide the AH-1W crew with the capability to detect, recognize, identify, track, laser range and laser designate targets during day, night, and adverse weather conditions. The NTS is comprised of the following subsystems: FLIR, charged coupled device (CCD) low light level television; direct view optics; AN/ASQ-211 laser designator/rangefinder system and television tracker (TVT); and a super video cassette recorder. The TVT (commonly called the autotracker) and videocassette recorder operate in conjunction with the CCD-TV and FLIR only.

With incorporation of the NTS, the AH-1W Super Cobra provides enhanced air reconnaissance capabilities to include day/night optical and FLIR imagery collection, precision automatic target tracking, laser designation, and video recording. Although the principal purpose of the NTS is to provide Super Cobra gunners the ability to use TOW and Hellfire II missiles and other weapons at full range both at night and through most battlefield obscuration, it is used to collect imagery of a variety of targets during armed reconnaissance missions for follow-on intelligence processing, production, and use.

UH-1N Night Thermal Imaging System

The night thermal imaging system (NTIS) is an airborne EO system designed to provide the UH-1N crew with the capability to detect, recognize, identify, and laser range targets during day, night, and adverse weather conditions, as well as provide a basic pilotage function. The NTIS is comprised of the following subsystems: FLIR, laser rangefinder system, and a videocassette recorder.

Imagery Mission Employment

When AH-1W or UH-1N aircraft is tasked to conduct imagery collection missions, the squadron coordinates operations closely with the MEF's IOC, the ACE G-2/S-2, the IIP and others as appropriate.

Follow-on intelligence processing and exploitation of NTS and NTIS imagery will take place once the aircraft has returned to base and the imagery videotapes are physically downloaded and delivered to the IIP. (Figures 3-6 and 3-7 identify the NTS and NTIS equipment on the AH-1W and UH-1N.)

Miscellaneous

Administrative

The HML/A is capable of self-administration.

Communications and Information Systems

Together with CIS resources supporting the ACE's MACCS, HML/As have sufficient CIS

Figure 3-6. AH-1W with the NTS.

Figure 3-7. UH-1N with the NTIS.

resources to support internal and squadron C2, operations, and intelligence requirements. It typically requires access to various networks to conduct its operations, to include SIPRNET, NIPRNET, and pertinent LANs and WANs.

Maintenance

The squadron is capable of conducting 1st echelon maintenance on all assigned equipment, and capable of performing organizational maintenance on assigned aircraft and support equipment. Maintenance beyond these capabilities is provided by other elements of the ACE and CSSE.

Ground Reconnaissance Units

Mission

The force reconnaissance company and division reconnaissance battalions provide amphibious, deep ground, and ground reconnaissance; surveillance; battlespace shaping; and limited scale raids in support of the Marine division, it's subordinate elements, and the MEF, other MAGTFs or a joint force. IMINT capability fielded to these units is the man packable secondary imagery dissemination system (Manpack SIDS).

Command and Control

Force reconnaissance company and the division reconnaissance battalion are under the command of the supported unit's commanders.

MAGTF CE Staff Cognizance

For intelligence and reconnaissance missions the commander will exercise C2 over ground reconnaissance via the unit's intelligence officer. At the MEF level, the AC/S G-2 will exercise this staff cognizance via the ISC. This allows for the centralized direction and effective integration of ground reconnaissance operations with the broader all-source intelligence concept of operations.

Support Relationships

General Support. Ground reconnaissance units normally operate in general support of the unit.

Direct Support and Attached. Depending upon METT-T considerations, ground reconnaissance units may be employed in direct support of or attached to a particular subordinate unit (e.g., force reconnaissance teams attached to advance force elements for an expeditionary operation; division reconnaissance battalion's platoons or teams

attached to or in direct support of the division's main effort). The scope of the supported commander's C2 authority over designated ground reconnaissance teams will usually be specified to ensure effective support to the operations while allowing the MEF or division commander to maintain effective C2 of broader intelligence and reconnaissance operations.

Manpack SIDS Concept of Employment

Manpack SIDS is a self-contained system comprised of three outstations, a base station, digital cameras, and other specialized devices; communications support must come from other resources. It enables ground reconnaissance units to take pictures of designated targets and then send the images back to the base station over selected communications paths (e.g., high and very high frequency [HF and VHF] single-channel radios and ultra high frequency satellite radios).

The base station then feeds the images into the MAGTF TDN for follow-on dissemination to other MAGTF or other units (figure 3-8 depicts one possible communications architecture for Manpack SIDS). This provides the means to process the images or photocopy sketches even before the team is extracted.

The outstation, with its digital camera component, will be employed by ground reconnaissance teams during missions for imagery acquisition. Imagery collected by the outstation may be stored for subsequent delivery to and analysis by the IIP, or may be electronically transmitted to the base station over organic tactical communications assets for near-real time analysis by the IIP. The base station generally will be employed at the reconnaissance operations center (ROC) collocated with the supported unit's main command echelon for receipt, manipulation, annotation, and subsequent retransmission of imagery collected by the outstation teams.

Depending upon the tasked IRs and the situation, the base station will then disseminate acquired imagery and related information to the P&A cell within the IOC (force reconnaissance team operations), to the division's combat intelligence center for follow-on intelligence analysis, production, and dissemination (division reconnaissance battalion operations) or directly to pertinent unit(s) C2 centers.

Dissemination will generally be in accordance with the intelligence reporting criteria stipulated by the ISC (for force reconnaissance company operations) or the division's intelligence operations officer or supported unit's intelligence officer (for reconnaissance battalion operations) via the MAGTF TDN to the recipient's IAS.

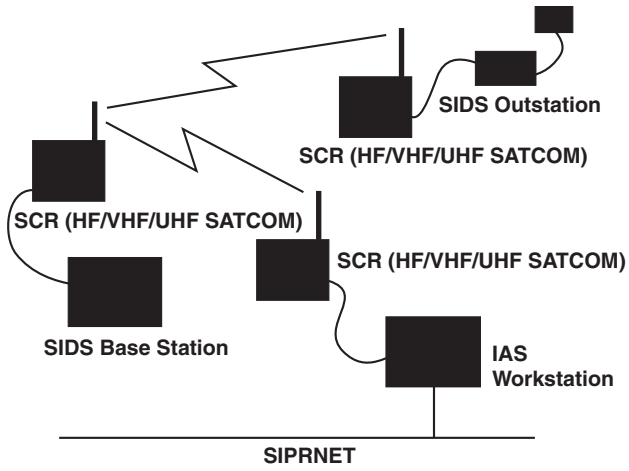


Figure 3-8. Manpack SIDS Communications Connectivity.

Tactical Intelligence Photographic Capability

TACPHOTO is a program related to Manpack SIDS. TACPHOTO provides an organic digital camera collection and processing capability—but without the palmtop processor and base station organic to Manpack SIDS—to a wide range of MAGTF units (see figure 3-9). TACPHOTO allows ground patrols, flight crews and others to collect images per their unit's IRs or external taskings. Upon mission completion and return to base, the acquired images will be downloaded into supporting processing resources for follow-on intelligence production and use. Digitized images can also be further disseminated throughout the MAGTF via the TDN.

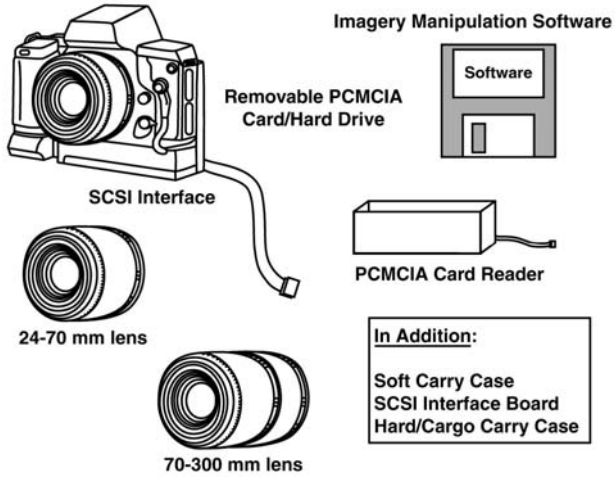


Figure 3-9. Tactical Intelligence Photographic Capability.

CHAPTER 4. IMAGERY INTELLIGENCE SYSTEMS, C2 NODES, COMMUNICATIONS INFORMATION SYSTEMS, AND OTHER SYSTEMS

Communications dominate war; broadly considered, they are the most important single element in strategy, political or military.

—Alfred Thayer Mahan

MAGTFs require significant C2 and CIS support to execute IMINT operations. Imagery systems technological developments have the potential to provide the commander with outstanding imagery support. However, the technical (particularly message and data traffic volumes versus available communications channels bandwidth) and operational needs (i.e., routine versus time-sensitive tailored IMINT support) require detailed planning and coordination of CIS support to conduct effective IMINT operations.

The Marine Corps receives and disseminates imagery as part of the Global Command and Control System (GCCS), via the Defense Information Systems Network (DISN), using Ground Mobile Forces (GMF), digital backbone, tactical radios, and Trojan Spirit II (TS-II). This chapter describes the MAGTF's major current and future IMINT C2 and CIS nodes.

Key to providing the MAGTF commander with IMINT support is understanding the size of imagery data and the capacities of communications pipelines required to transmit this data throughout the MAGTF and to pertinent external organizations. As a general rule, a high capacity (at least T-12) communications pipeline is required for incoming imagery data to the MAGTF, with lesser but still significant capacities required at times for internal MAGTF imagery data dissemination. While most MAGTF requirements can be satisfied via GENSER communications channels (e.g., SIPRNET), the MAGTF must also have SCI communications support (e.g., JWICS) to satisfy some critical requirements.

Basic Imagery Intelligence Communications and Information Systems Requirements

The standard IMINT CIS requirements for a MAGTF operation are—

- **The capability to C2 subordinate units.** Intelligence officers and IMINT element commanders/OICs must be capable of positive C2 of subordinate units and integration of their operations with broader MAGTF and external intelligence and operations C2. Traditionally single-channel radio and record message traffic have been used to support C2 of MAGTF IMINT units. In semistatic situations, secure e-mail or telephone may be the method of choice, while in highly fluid or mobile scenarios, cellular, SATCOM, and VHF and HF radio may be used.
- **The ability to receive collected data and information from the full range of organic and external IMINT organizations.** The CIS architecture must provide connectivity between organic and supporting IMINT elements (such as the VMU, Manpack SIDS capable ground reconnaissance teams), IMINT production and analysis centers (e.g., JTF's NIST, IIP and MCIA), and supported MAGTF operations and intelligence centers. Requirements include the capability to transmit image data files and IMINT reports digitally via fiber-optics, wire, or radio in formats (both voice and data) that are readily usable by imagery and all-source intelligence analysts.

- **The ability to provide intelligence to supported commanders.** IMINT CIS requirements will be influenced by supported commanders' intents, concepts of operations and intelligence, command relationships, and standing PIR and IRs. The CIS architecture must be capable of integrating IMINT element C2 and supporting CIS operations (to include both GENSER and SCI communications) with the primary CIS channels used by supported commanders.
- **The ability to share IMINT products and reports with MAGTF P&A Cell and with IMINT and all-source JTF, other components, theater, and national IMINT and intelligence centers.** The traditional means for providing this capability are MAGTF GENSER secure record and voice communications. While these techniques continue to be used, they are rapidly becoming secondary in importance to the use of JWICS, SIPRNET, and other CIS capabilities that allow participants to access each others' imagery and IMINT products and databases and to immediately pull required data, intelligence, and other IMINT products.

Imagery Intelligence and Key Related Command and Control Nodes

A wide variety of IMINT operations and supporting C2 and CIS may support military operations.

Organization

NIMA

The Director, NIMA, coordinates national CIS support to military and intelligence agencies. NIMA established CIS interoperability standards and data formats for all IMINT operations. Military forces and intelligence agencies use these standards and data formats to support interoperable planning and direction, collection, production, and dissemination of IMINT.

A NIMA Customer Support Response Team (CSRT) may be integrated into a NIST or may be deployed in direct support of a military force. The CSRT will typically contain a deployable imagery/geospatial server known as the Quick Response System (QRS). The QRS is self-contained and generally requires only satellite communications (SATCOM) channel access support from the JTF or other supported unit. The JTF J-2 coordinates SATCOM channel and communications security (COMSEC) support through the JTF J-6. Additionally, depending upon the situation, other CIS and related support that a NIST may require from the supported unit includes information systems technical support and an access controlled secure area (generally within the supported unit's tactical sensitive compartmented information facility [TSCIF]).

During operations, the CSRT QRS provides a MAGTF with a wide range of imagery and geospatial information and services support. In support of garrison operations, a NIMA CSRT provides special training and exercise support to MAGTFs. Also, NIMA may provide MAGTFs temporary specialized equipment to meet unique operational needs or to satisfy critical deficiencies.

National Reconnaissance Office

The NRO has theater-focused customer support teams to provide direct operational support to MAGTFs and other forces. These teams include on-site military/contractor personnel collocated with the combatant and other commands. Basic support includes education on NRO systems and capabilities; training on tasking; and receiving, processing, and analyzing data collected by NRO systems. Equipment and personnel are available to support MAGTF operations during contingencies. NRO support elements are usually self-sufficient, requiring no MAGTF CIS operational support beyond routine communications coordination.

National Intelligence Support Team

All-source national intelligence level IMINT and other intelligence assets may deploy in support

of JTF (and even directly in support of MAGTF) operations as well as providing critical support via reach back and collaborative capabilities. The NIST is the most typical method used. The NIST is a task-organized unit generally consisting of DIA, NSA, CIA, and, as appropriate, NIMA personnel and equipment. Its mission is to provide a tailored, national level all-source intelligence team to deployed commanders (generally at the JTF headquarters level, but support could be provided to other commands) during crisis or contingency operations. Depending upon the supported unit's requirements, a NIST can be task-organized to provide coordination with national intelligence agencies, analytical expertise, I&W, special assessments, targeting support, streamlined and rapid access to national intelligence databases and other products, and assistance facilitating request for intelligence (RFI) management (see figure 4-1).

DIA, through the joint staff J-2, controls the NIST for deployment and administrative purposes (see figure 4-2 on page 4-4 for an overview of a NIST's deployment cycle). During operations a NIST will usually be in direct support of the JFC, who exercises C2 of it via the JTF J-2. Once deployed, the intelligence agencies with representatives on the NIST provide leadership. The basic C2 relationships between the NIST and the JTF (or other supported commands) command relationship are direct support. The NIST will be under the staff cognizance of the JTF J-2, performing intelligence support functions as so designated. The basic NIST concept of operations is to take the J-2's RFIs and collection and production requirements, discuss and deconflict these internally within the NIST to determine which element(s) should take these for action. Each NIST element leader, and as coordinated by the NIST team chief, will conduct liaison with their parent national intelligence organization. Intelligence generated by the NIST is available to the JTF J-2 JISE, the JFC, and other elements of the JTF with the usual restriction based on clearance and programs.

The composition and capabilities of each NIST deployment is unique based on the mission, duration, agencies representation, and capabilities required (see figure 4-3 on page 4-4). A NIST, however, is not a totally self-contained element. It requires logistic and other support from the supported command. Depending upon the situation, support that a NIST requires from the supported

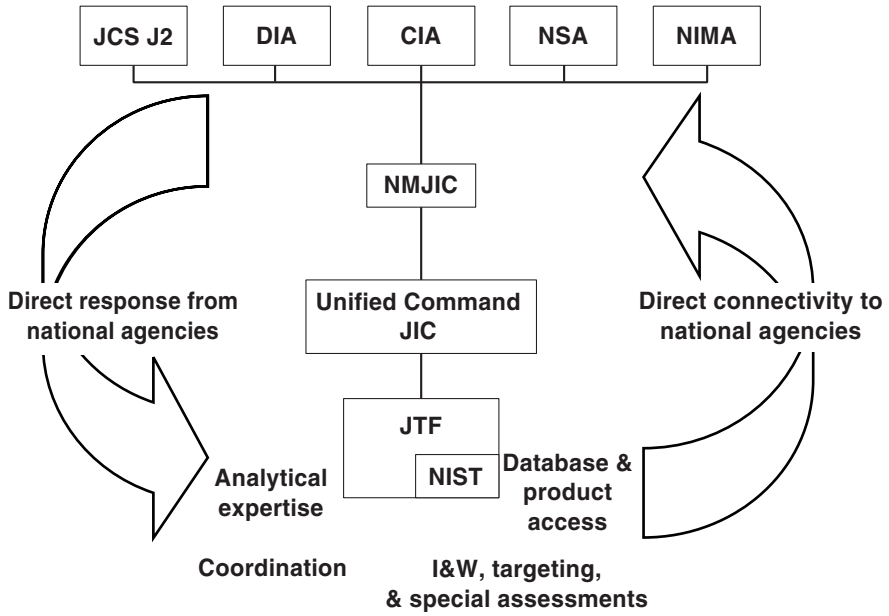


Figure 4-1. NIST Capabilities.

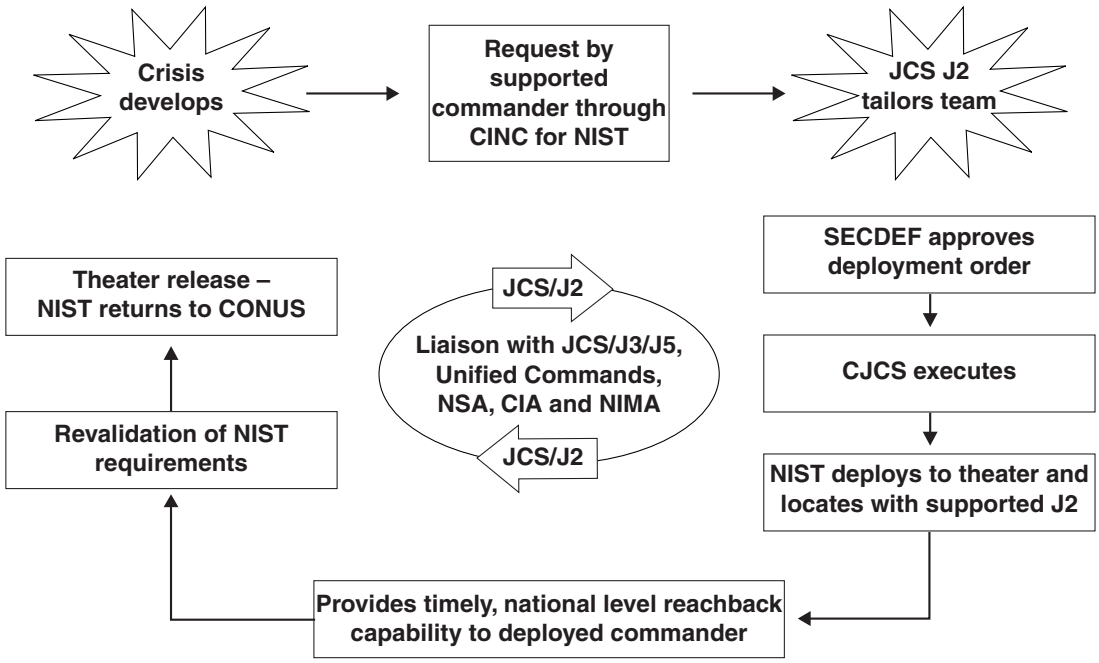


Figure 4-2. NIST Deployment Cycle.

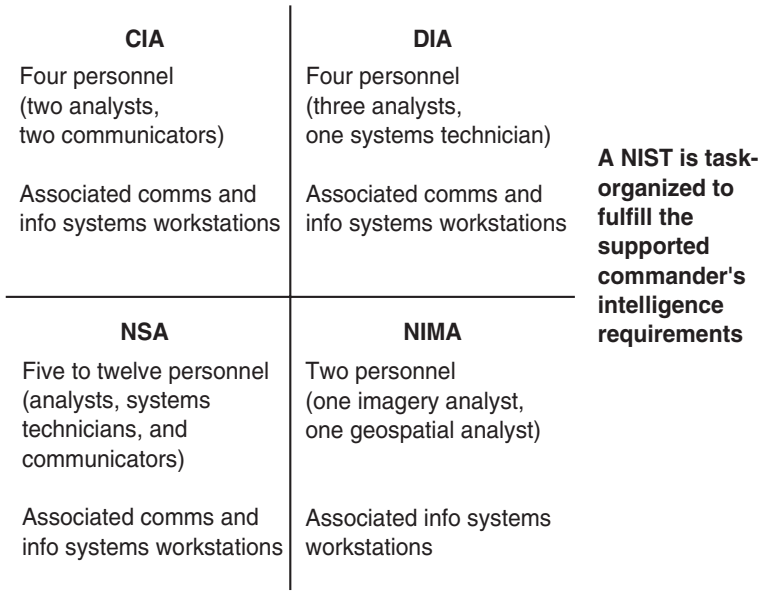


Figure 4-3. Notional Composition of a NIST.

unit includes information systems technical support and an access controlled secure area (generally within the supported unit's TSCIF).

A NIST's organic capabilities generally encompass only intelligence and some unique CIS support. NIST CIS capabilities will be task-organized. A NIST may range from a single agency element's voice connectivity to a fully equipped NIST with JISE and JWICS video teleconferencing (VTC) capabilities (see figure 4-4 for one of a NIST's key sophisticated CIS capabilities). Current methods of operation continue to rely on both agency and supported command-provided communications paths to

Figure 4-4. NIST JWICS Mobile Integrated Communications System.

support deployed NIST elements. The systems that each element is capable of deploying are discussed in greater detail in JP 2-02, *National Intelligence Support to Joint Operations*, appendix C.

Theater

Combatant Commands' Joint Intelligence/ Analysis Centers. The combatant commands' JICs and JAC are the cornerstones for fulfilling the IRs of the geographic combatant commanders and their subordinate commanders. The JICs and JAC are the primary sources from which subordinate JTFs receive intelligence support for their areas of interest, providing finished intelligence products supporting theater mission planning and execution.

Collection. The combatant commander's J-2 retains full collection management authority (i.e., to validate, modify or non-concur) over all intelligence collection requirements against targets within their area of responsibility. Such authority may be delegated to a subordinate JFC. Validated collection requirements, to include imagery collection, that cannot be satisfied by organic JTF means will be submitted to the combatant command's JIC/JAC.

Processing and Exploitation. The JIC/JAC processes and exploits imagery in theater. Downlinked imagery data signals may be transmitted to workstations for either immediate exploitation, stored on tape, sent to digital archives for later use or laid out on film for exploitation.

Production. Combatant commands, services, and defense agency intelligence production centers' production responsibilities are clearly delineated within the DOD Intelligence Production Program (DODIPP). The DODIPP is structured to capitalize on the analytical and production resources of the entire DOD intelligence production community. It supports the efficient use of production resources, prevents duplication of effort, and enhances timely support to user IRs. The Community On-Line Intelligence System for End-Users and Managers (COLISEUM) automates DODIPP procedures for stating and tracking theater IRs and other intelligence production requirements. Results from imagery exploitation and the annotated images may

be incorporated into all-source intelligence products, stand-alone IMINT products or into various IMINT and intelligence databases.

Dissemination. The JDISS, which mainly uses JWICS for connectivity, is the primary intelligence system used by the JIC/JACs for both the receipt and dissemination of imagery and other intelligence products. Using these systems, multimedia intelligence dissemination (e.g., voice, data, imagery, record message, e-mail, graphics, and video) can be supported. Internally, the JIC/JACs use the Imagery Data Exploitation System (IDEX) for manipulation and exploitation of imagery, with JDISS and JWICS used for secondary imagery and other intelligence dissemination. File servers maintained by the JIC/JACs are key components of intelligence support. For imagery, the current capability is provided by the demand driven direct digital dissemination (5D) server, with NIMA's IPL planned as its replacement. These file servers can be accessed using JDISS providing subordinate commands and other users the ability to pull imagery and other intelligence when required. The JICs have access to all of the government-owned, common user networks used by the intelligence community: Automated Digital Network/Defense Message System, (AUTODIN/DMS), Defense Special Security Communications System (DSSCS), NIPRNET, SIPRNET, JWICS, and the Defense Switched Network (DSN). Access to military satellite systems includes the Defense Satellite Communications Systems (DSCS) and the Fleet Satellite Communications System. Commercial satellite access is also available through the International Maritime Satellite System and INTELSAT.

JTF J-2 and the Joint Intelligence Support Element

The JTF J-2 organizational structure and capabilities will be situation and mission dependent as determined by the JFC and the JTF J-2. The JISE is the principal intelligence C2 node within the JTF J-2. The JISE is the focus for JTF intelligence operations, providing the JFC and component commanders with situational awareness and other intelligence support regarding adversary air, space, ground and maritime capabilities and activities.

A NIST provided in support of the JTF headquarters will integrate its operations within the JISE. Key JISE functions and capabilities include collection management support, OOB analysis, identification of threat centers of gravity and critical vulnerabilities, and intelligence support to targeting and force protection.

All IMINT collection, production, and dissemination activities will be conducted within the JISE. Once IMINT products and support have been provided to the JTF and its components, updates will be accomplished by the JISE using push/pull dissemination techniques. Intelligence CIS based on the JDISS/JWICS functionality provide the JTF with the ability to query theater and national IMINT servers and databases for the most current intelligence.

Collection

The JTF J-2 collection manager will plan, coordinate, and use direct imagery collection operations in support of the JTF. As shown in figure 4-5, theater and JTF imagery collection assets include the U-2, JSTARS, theater UAVs, and other-Service assets such as the Navy's F-14/TARPS and the Air Force's RF-16. MAGTF interfaces with these collection assets are depicted by the lines in figure 4-5. Communication support planning provides connectivity from these major nodes into the TEG and MAGTF TDN.

Production

IMINT production requirements are managed by the JISE in accordance with the JFC's PIR and other validated IRs.

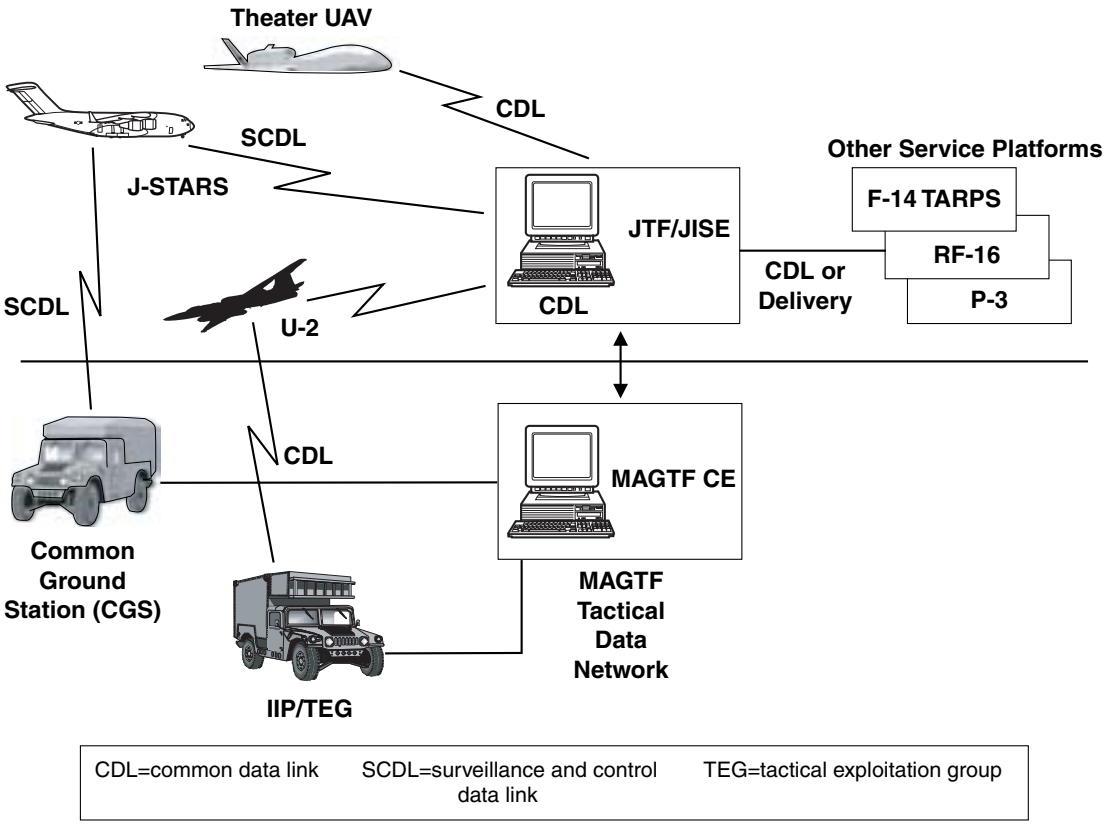


Figure 4-5. Theater/JTF Imagery Collection.

Dissemination

Once basic and current intelligence and imagery have been provided to a deploying JTF and its components, updates will be accomplished using push/pull dissemination techniques. Intelligence CIS based on the JDISS/JWICS functions provide the JTF with the ability to query theater and national IMINT servers and databases for the most current intelligence.

Amphibious Forces

LFs, when afloat, use the ATF's imagery dissemination backbone, such as Challenge Athena and Joint Services Imagery Processing System (JSIPS)-Naval, and continue to receive imagery support from the Navy once ashore, via doctrinal communications.

Intelligence Center

During amphibious operations, the intelligence sections of the ATF and the LF will generally integrate their operations. The principal intelligence C2 node afloat is the intelligence center located aboard the AF flagship. The intelligence center is composed of designated shipboard spaces with installed CIS systems that support the intelligence operations of the ATF and LF while reducing duplicative functions and producing more comprehensive and timely intelligence for the naval task force. Standard CIS connectivity is available (JWICS, SIPRNET, NIPRNET, AUTODIN, DSN). Access is provided via the flagship's GENSER communication center and the special intelligence communications center within the intelligence center's ship's signals exploitation space.

CVBGs/TARPS Squadrons

TARPS support to MAGTF operations requires no unique CIS support. Most often, TARPS imagery is delivered to the intelligence center located aboard the AF flagship via courier. Processed TARPS imagery may be digitized and disseminated to the ATF and LF via JDISS, JWICS or the Global Command and Control System-Maritime.

MEF Command Element

Combat Intelligence Center

The CIC and its subordinate elements are the principal MAGTF intelligence C2 node providing the facilities and infrastructure for the centralized direction for the MEF's comprehensive intelligence, CI, and reconnaissance operations. Since the CIC must effectively support the entire MEF, it must remain responsive to the requirements of all elements of the MAGTF. Supporting this objective, the CIC integrates and supports both MEF G-2 section and intel bn operations. While integrated, the organizational approach differs for each of these. The CIC is the overarching intelligence operations center established within the MEF main command post. It encompasses the primary functions of the MEF intelligence section and intel bn. The CIC includes the subelements listed in table 4-1.

Table 4-1. MEF CE CIC and Intel Bnís IOC Key Elements.

Element	Responsibilities
G-2 Plans	Serves as the G-2 section's main element for coordinating and providing intelligence support to the MEF CE future plans team and leadership and direction of the G-2 section's imagery and mapping, SIGINT, and weather sections.
G-2 Operations	Serves as the G-2 section's main element for coordinating and providing intelligence support to the MEF CG, battle staff, and current operations center elements; target intelligence support to the force fires and future operations; G-2 section intelligence requirements management activities; red cell support; and MEF intelligence liaison with external commands and organizations.
IOC	Serves as the principal MEF intelligence operations and C2 center that is established by intel bn; performs intelligence requirements management, staff cognizance of ongoing organic and supporting collection operations, intelligence production and analysis, and intelligence dissemination.
• Support Cell	Serves as primary element for conducting MEF-wide intelligence requirements management, weather support, collections and dissemination planning and direction, and intelligence staff cognizance of MEF organic and supporting intelligence and reconnaissance operations.
• P&A Cell	Serves as the primary production and analysis element of the MEF; processes and produces all-source intelligence products in response to requirements of the MEF; serves as the principal IMINT and GEOINT production element of the MEF.
• SARC	Serves as the primary element for the supervision of MEF collection operations; directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets.
CI/HUMINT Company Command Post	Serves as the primary element for conducting CI/HUMINT planning and direction, C2, and coordination of MEF CI/HUMINT operations with external CI/HUMINT organizations.
Operations Control and Analysis Center	Serves as the main node for the C2 of radio battalion SIGINT operations and the overall coordination of MEF SIGINT operations; processes, analyzes, produces, and disseminates SIGINT-derived information; and directs the ground-based electronic warfare activities of the radio battalion.
Reconnaissance Operations Center	Serves as the main node for the C2 of force reconnaissance company's operations and the overall coordination of MEF ground reconnaissance operations; processes, analyzes, produces, and disseminates ground reconnaissance-derived information in support of MEF intelligence requirements.

The key G-2 nodes are organized to effectively align and support the MEF CE's staff cross-functional cellular staff organization (see figure 4-6) and concept of operations. The G-2 plans branch provides intelligence support to the MEF CE's future plans cell efforts. The G-2 operations branch provides intelligence support to the MEF CE's COC, FOC, force fires center and directs and manages the G-2's red cell and the MEF's external intelligence liaison teams.

CIC facilities, CIS, and other support must allow the AC/S G-2 and G-2 section to perform the following major tasks:

- Developing and answering outstanding MEF and subordinate units' PIR and IRs by planning, directing, integrating, and supervising MEF organic and supporting intelligence, CI, and reconnaissance operations.

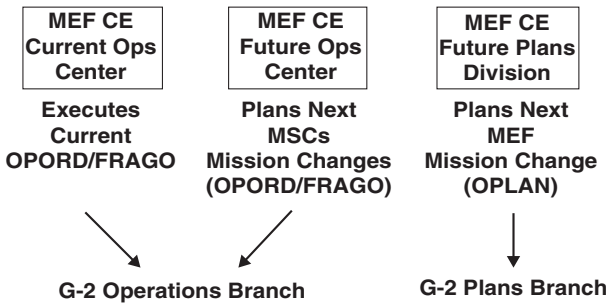


Figure 4-6. MEF CE Cross-Functional Cellular Organization and Intelligence Support.

- Planning the MEF concept of intelligence operations for approval by the AC/S G-2 and subsequent implementation by the ISC based upon the mission, threat, commander's intent, guidance, and concept of operations.
- Recommending CI and force protection measures and countermeasures.
- Preparing appropriate intelligence plans and orders for the MEF, to include reviewing, coordinating, and integrating the intelligence plans of JTFs, combatant commands and other organizations.
- Coordinating, providing, and facilitating the use of intelligence to the MEF CG, the battlestaff, the future plans cells, the FOC, the COC, and the force fires center.
- Planning, directing, and supervising MEF liaison teams to external commands (e.g., the JTF and joint functional components headquarters) and intelligence organizations.
- Coordinating and supervising the transition of intelligence planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations, to effectively support the MEF's single battle transition process.

Intelligence Operations Center

The IOC is the other principal MEF CE intelligence node. The key subordinate elements within the IOC and their typical composition are the support cell, the SARC, and the P&A cell (see figure 4-7). It provides

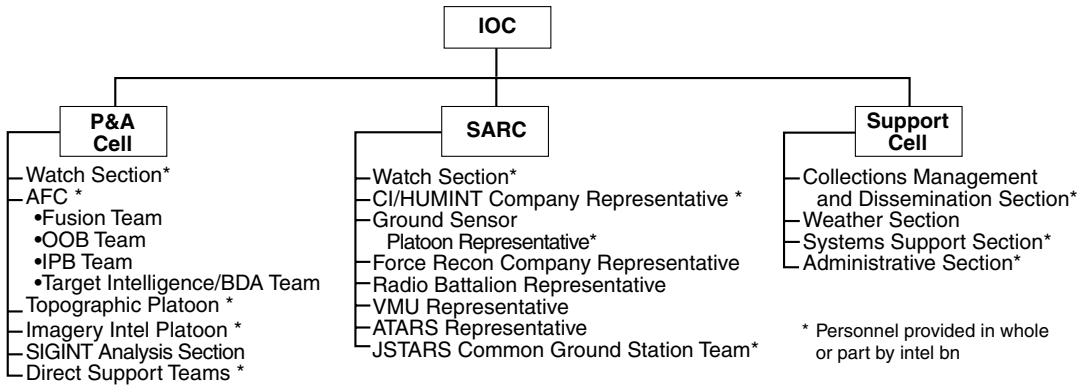


Figure 4-7. Intelligence Operations Center Elements and Composition.

the facilities, CIS, and other support to allow the ISC and intel bn to perform the following tasks:

- Provide centralized direction for MEF intelligence operations under the staff cognizance of the AC/S G-2. The IOC is the core for this task, with key assistance from the G-2 plans and G-2 operations elements.
- Consistent with the commander's priorities, consolidate, validate, and prioritize IRs of the entire force. The key element providing this is the CMD section within the IOC's support cell. Intelligence specialists from all disciplines, to include IMINT, generally are organic to this section.
- Plan, develop, and direct the MEF collection, production, and dissemination plans and operations. The key elements providing for this are the CMD section within the IOC's support cell and the P&A cell.
- Submit consolidated requests for external intelligence support through the Marine component headquarters to appropriate agencies. The key element providing this is the CMD section within the IOC's support cell, assisted by the P&A cell and the G-2 operations branch.
- Allow ISC to exercise, per AC/S G-2 cognizance, principal staff cognizance of MEF organic and supporting intelligence, CI and reconnaissance operations, to include SIGINT, IMINT, HUMINT, GEOINT, CI, measurement and signature intelligence (MASINT), ground reconnaissance, and aerial reconnaissance operations.
- Coordinate and manage the employment of MEF organic collection assets through the IOC's SARC. Within the SARC will be representatives from most organic and supporting intelligence and reconnaissance units to provide C2 and reporting of ongoing intelligence operations.
- Maintain a consolidated, all-source intelligence production center in the P&A cell. Intelligence specialists from all intelligence disciplines generally are organic to the P&A cell. The other node with significant intelligence production involvement is the radio battalion's OCAC.
- Link the MEF CE to national, theater, joint, other-Service, and multinational intelligence assets and operations. All intel bn and G-2 section nodes have common and unique capabilities to perform critical tasks within the function. In addition to MEF CE common communications pathways provided by the communications battalion, the IOC generally will also have unique intelligence communications capability, such as TS II.

CIS Support

CIS support to CIC and IOC operations vary from operation to operation based upon METT-T. Generally all nodes will have access to IAS and JDISS (each with COLISEUM and other specialized applications) and connectivity with the full range of communications (JWICS, SIPRNET, NIPRNET, DSN, defense message system, voice, video-teleconferencing, etc.) via either MEF CE common communications or unique intel bn CIS capabilities. Examples of unique intelligence CIS capabilities are those integral to the VMU squadron RRS, the radio battalion technical control and analysis center and the AN/MSC-63A special security communications central, the ground sensor platoon's tactical remote sensor system, the IIP's TEG, the Marine tactical electronic warfare squadron's tactical electronic reconnaissance processing and evaluation system, the CI/HUMINT automated tool set, Manpack SIDS, TS-II, and the JSTARS CGS. See figure 4-8 for a notional depiction of an overarching MEF intelligence CIS architecture.

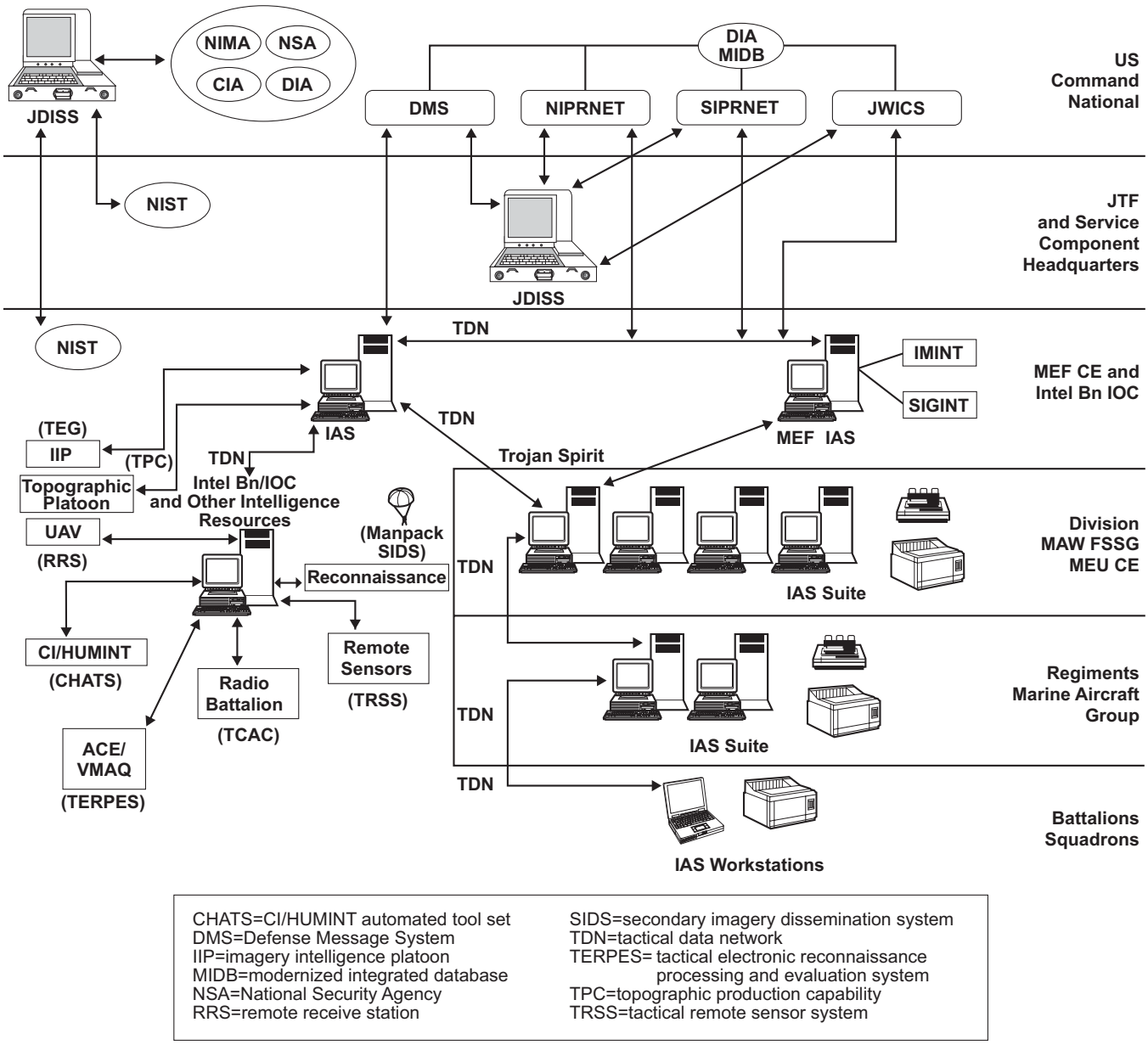


Figure 4-8. Notional MEF Intelligence Communications and Information Systems Architecture.

Overall MEF Intelligence C2 Relationships

The MEF G-2 section and intel bn's overall C2 relationships and resulting all-source intelligence support flow throughout the MEF are indicated in figure 4-9 on page 4-12.

CIC/IOC Operations and IMINT

IMINT activities will be integral to many CIC/IOC operations.

Key activities include:

Collection. The CMD section, headquarters, intel bn, provides the core for MEF CIC collection operations. During operations the CMD section is located within the IOC's support cell. Intelligence specialists from all disciplines, to include IMINT, are organic to this section. Key CIS resources required included IAS (with COLISEUM and other specialized applications) and access to the full range of communications: JWICS, SIPRNET, NIPRNET, DSN, etc.

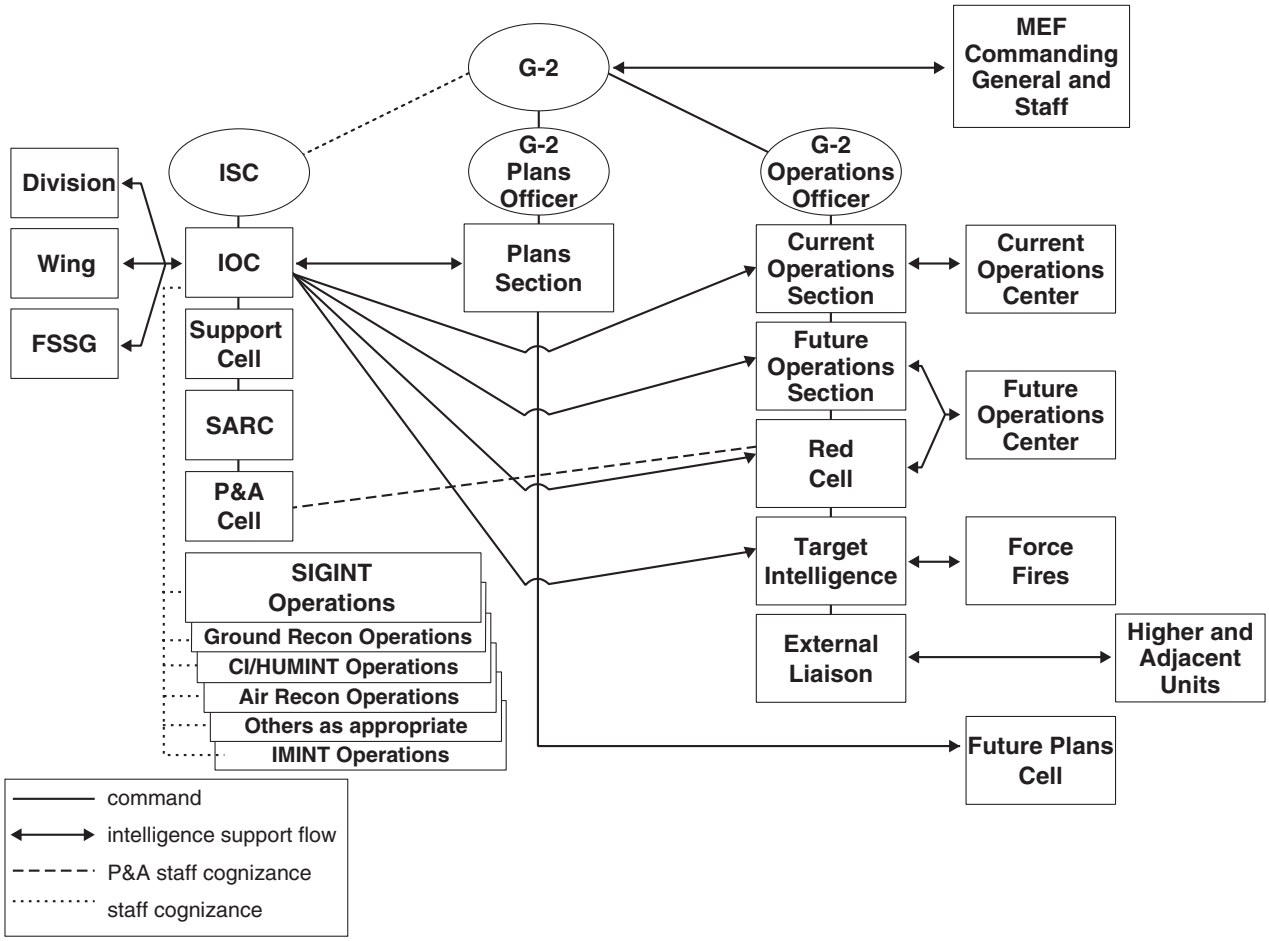


Figure 4-9. MEF Intelligence C2 Relationships and Intelligence Support Flow.

The SARC, another key element within the IOC, provides the other key component of collection operations. Within the SARC will be representatives from most organic and supporting intelligence and reconnaissance units to provide C2 and reporting of ongoing intelligence operations. Regarding IMINT, these representatives will include a UAV squadron element with supporting CIS resources to monitor ongoing UAV operations and report time-sensitive intelligence.

Production. The P&A cell, intel bn, provides the core for MEF intelligence production operations. Similar to collection, intelligence specialists from all intelligence disciplines are organic to the P&A cell. Key CIS resources required included IAS and JDISS, with access to the full range of communications (JWICS, SIPRNET, NIPRNET, DSN, etc.). The IIP and intel bn generally will be integrated into P&A cell operations to efficiently support both IMINT and all-source production operations.

Dissemination. The CMD section, headquarters, intel bn, provides the core C2 for MEF intelligence dissemination operations. Key CIS resources required included IAS and JDISS, with access to the full range of communications (JWICS, SIPRNET, NIPRNET, DSN, etc.) for external dissemination; and IAS via the TDN and other MEF communications resources for internal dissemination.

The MEF CE will exploit all of the external capabilities discussed earlier to satisfy its IRs, with heavy reliance on the MCIA for national imagery support and the JIC/JAC for theater and national support. National imagery and related

products are received over dedicated terrestrial links that terminate at the MCIA's JSIPS National Dissemination Element (DE); standard communications connectivity from the deployed MEF to the MCIA via the DISN are normally provided by satellite communications. Currently, these links are predominantly super high frequency (X-Band) military SATCOM using GMF terminals. In the future, more C-Band and Ku-Band commercial SATCOM will be employed, using mobile Tri-Band SATCOM terminals. The limited capacity of these links to DISN remains a significant choke point for deployed MAGTFs. Efficient use of these links is critical to higher effective traffic throughput.

In addition to the MAGTF TDN and other common user communications capabilities, certain imagery units have specialized capabilities to support IMINT dissemination. The UAV squadron's RRS, attached to MEF MSEs (e.g., the MEF main effort), provides direct, time-sensitive UAV support.

Within the MEF, the IAS is the principal information system resource to support secondary imagery and other IMINT product dissemination. IAS will be available at all command echelons down to the maneuver battalion/squadron levels.

Communications connectivity between the MEF CE and its MSE headquarters are predominantly provided by SATCOM, supplemented where practical with terrestrial line-of-sight and troposcatter multi-channel radio systems. Connectivity to the regiment/group level is principally via the TDN (with current capabilities of between 16 and 32 kilobytes per second [kbps]) and various multichannel radio resources. Finally, communications connectivity below the regiment/group command echelon depends principally on single channel radio primarily designed for voice traffic, with limited range and limited data capacities (1.2 kbps to 16 kbps). Although these units possess tactical data systems, their ability to exchange data traffic is currently limited due to the far less available bandwidth connectivity with the MAGTF TDN.

Imagery Intelligence Information Systems and Supporting Communications

Imagery Direction and Collection Management

IAS and the Requirements Management System (RMS) are the key automated information systems resources supporting MAGTF IMINT operations (see figure 4-10 on page 4-14).

Intelligence Analysis System

IAS is the principal intelligence information system tool. IAS automates MAGTF intelligence activities of direction, collection, processing, production, and dissemination of critical tactical intelligence from embedded databases and multiple sources. It is interoperable with JDISS and a wide range of other intelligence and reconnaissance systems. This allows for better identification and tracking of MAGTF IRs, and development and C2 of supporting collection, production, and dissemination activities, both within the MAGTF as well as with other services, JTF, theater, and national intelligence operations. Various configurations of IAS are fielded from the MEF CE through battalion and squadron command echelons. IAS contains a limited automated collection management tool for imagery, as well as for other organic intelligence collection.

Basic System. IAS is capable of communication and data exchange at both the GENSER and SCI levels via the MAGTF TDN. Composition and size will vary at each echelon, but the IAS essentially consists of data storage devices, workstations, and input/output devices. Workstations at all echelons will share common software applications.

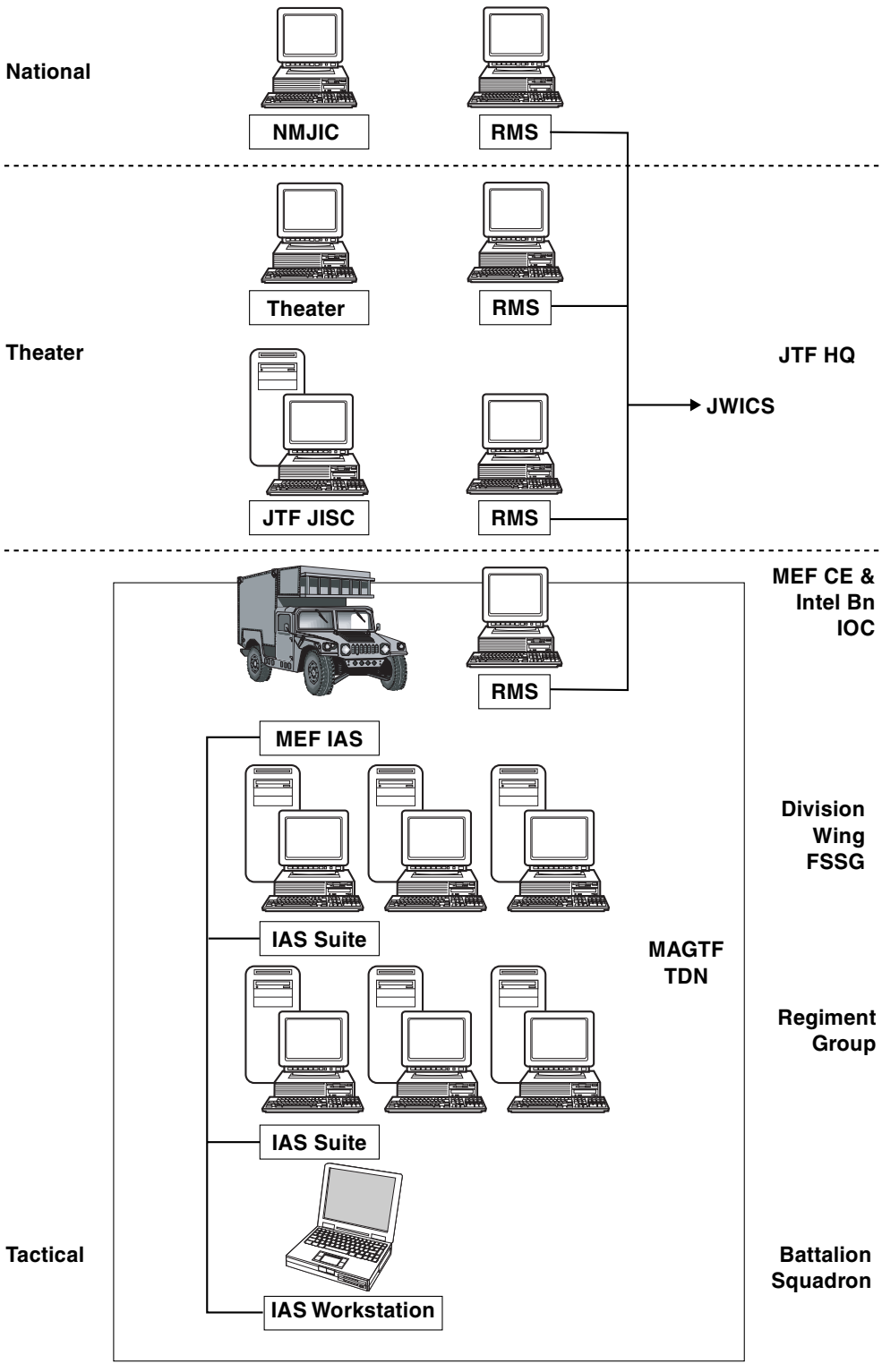


Figure 4-10. Imagery Direction and Collection Management.

Configuration. IAS consists of three configurations (see figure 4-11): MEF IAS, IAS suite, and the IAS workstation. The MEF IAS consists of two shelters mounted on HMMWVs and is used at the MEF CE level. The IAS suite consists of team portable equipment and will be used in the MEU CE and at division, MAW, regiment, and MAG headquarters. Finally, the IAS workstation consists of a single computer workstation and will be organic to battalion and squadron intelligence sections.

Features. The IAS provides connectivity and interoperability with most MAGTF intelligence, reconnaissance and other C2 systems, and with other services, JTF, theater and national intelligence organizations and data bases. IAS features improve the intelligence functions at all echelons of the MAGTF by providing a semi-automated all-source intelligence fusion center. It is capable of rapid access to and dissemination of critical, perishable tactical intelligence concerning terrain, weather, and enemy situation at all command levels. The IAS incorporates the capability to disseminate imagery throughout the MAGTF via SIDS. It facilitates display, processing, analysis, preparation of intelligence products, and dissemination of intelligence products.

Requirements Management System

RMS provides the MAGTF and other users with a comprehensive national imagery collection management capability. RMS allows MEF collection managers to access the national imagery requirements tasking and tracking system (RMS terminals are also located at the MARFOR headquarters, MCIA Suitland and with the Marine Corps DRO). RMS users generate imagery requirements nominations interactively via networked RMS or RMS-supported workstations. The nominations are automatically transferred to the appropriate review authority, and upon validation and prioritization, taskings are transmitted by RMS to the collection, exploitation, production, and dissemination organizations.

System Configuration. RMS is an SCI-high system. The major components include a file server,

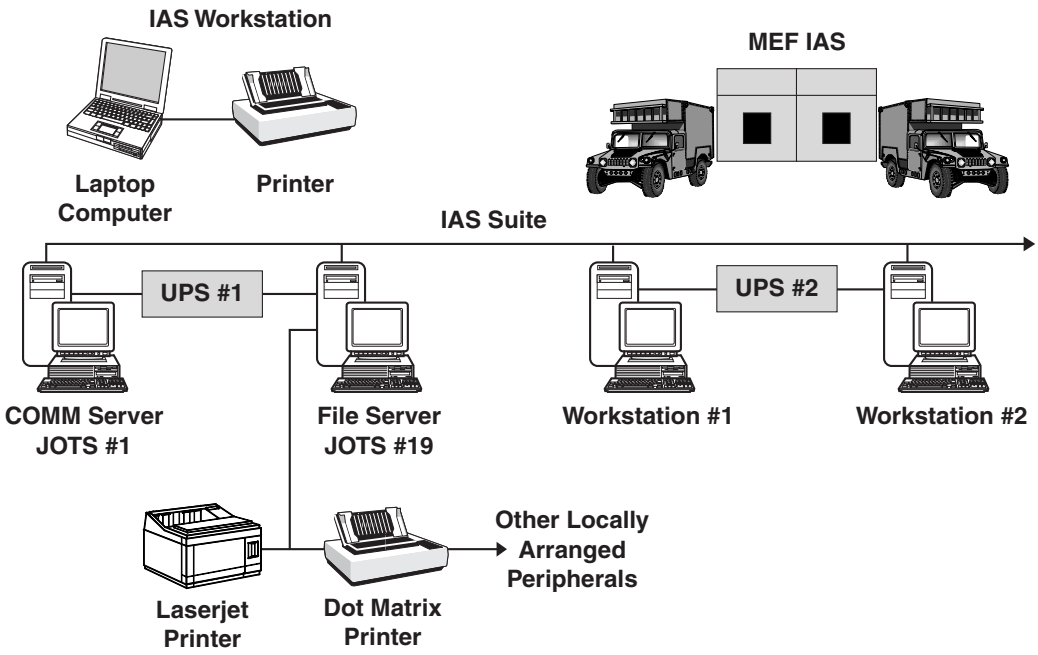


Figure 4-11. Intelligence Analysis System.

tape library system, access server for remote troubleshooting, a network laser printer, and the workstation itself.

RMS Connectivity. RMS communications connectivity requirements include JWICS and defense special security communications system (DSSCS).

Imagery Collection

The Marine Corps relies on both organic (see figure 4-12) and external collection assets for its imagery. The following paragraphs present MAGTF organic imagery collection assets and key C2-related information.

Advanced Tactical Airborne Reconnaissance System

The ATARS suites reside with the F/A-18D squadrons. ATARS-equipped F/A-18D aircraft will provide the MAGTF with organic manned aerial imagery reconnaissance capability in support of IMINT operations. ATARS is capable of infrared, EO, and radar imagery collection, and provides high resolution, day and night imagery support in all weather conditions, through both overflight and long-range standoff. The F/A-18D's long-range standoff capability is made possible with the installation of an upgraded, all-weather SAR system. Imagery is recorded and data-linked via integration with the ATARS sensor suite. The tactical interoperable ground data link (TIGDL) CDL will provide limited near-real time capability for dissemination of data on selected critical targets (down linked to the IIP's TEG), with subsequent manual tape download for exploitation of the complete track. Figure 4-13 depicts the F/A-18D systems architecture.

Unmanned Aerial Vehicles

UAVs provide MAGTFs a valuable aerial reconnaissance and imagery (video and infrared) capability.

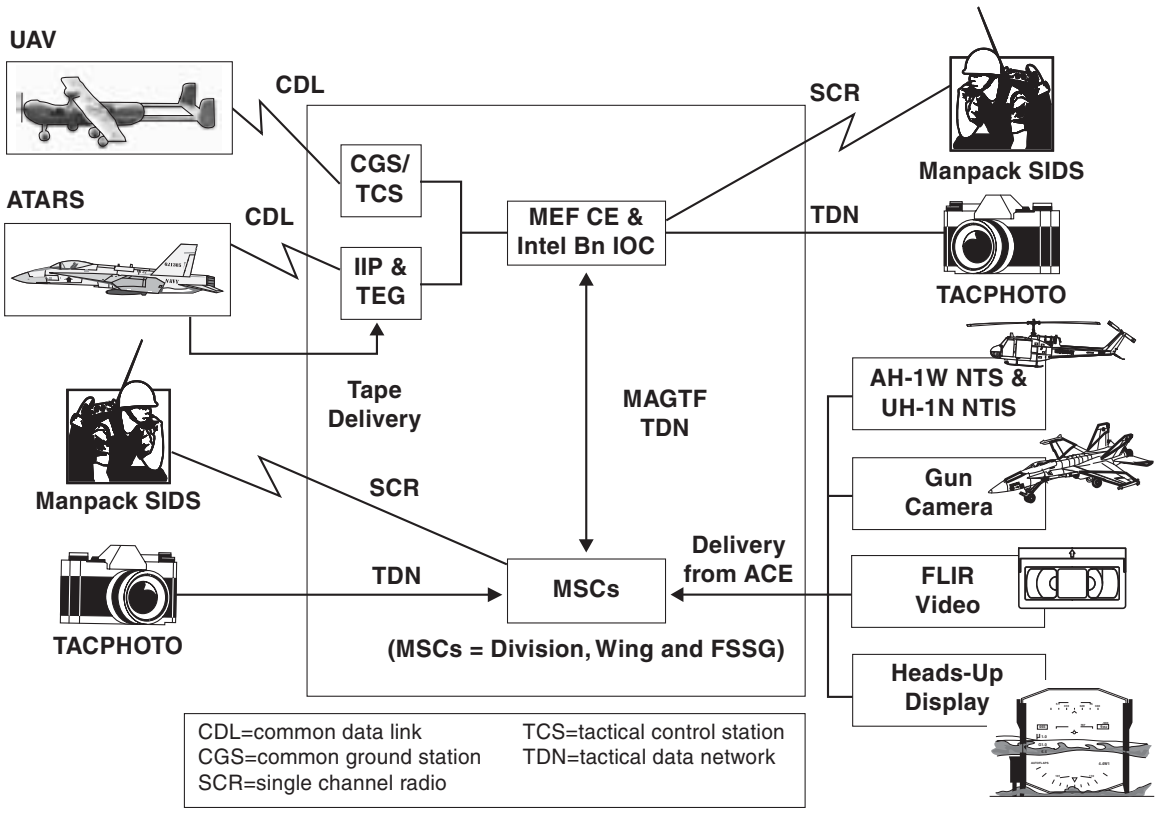


Figure 4-12. MEF Organic Imagery Collection.

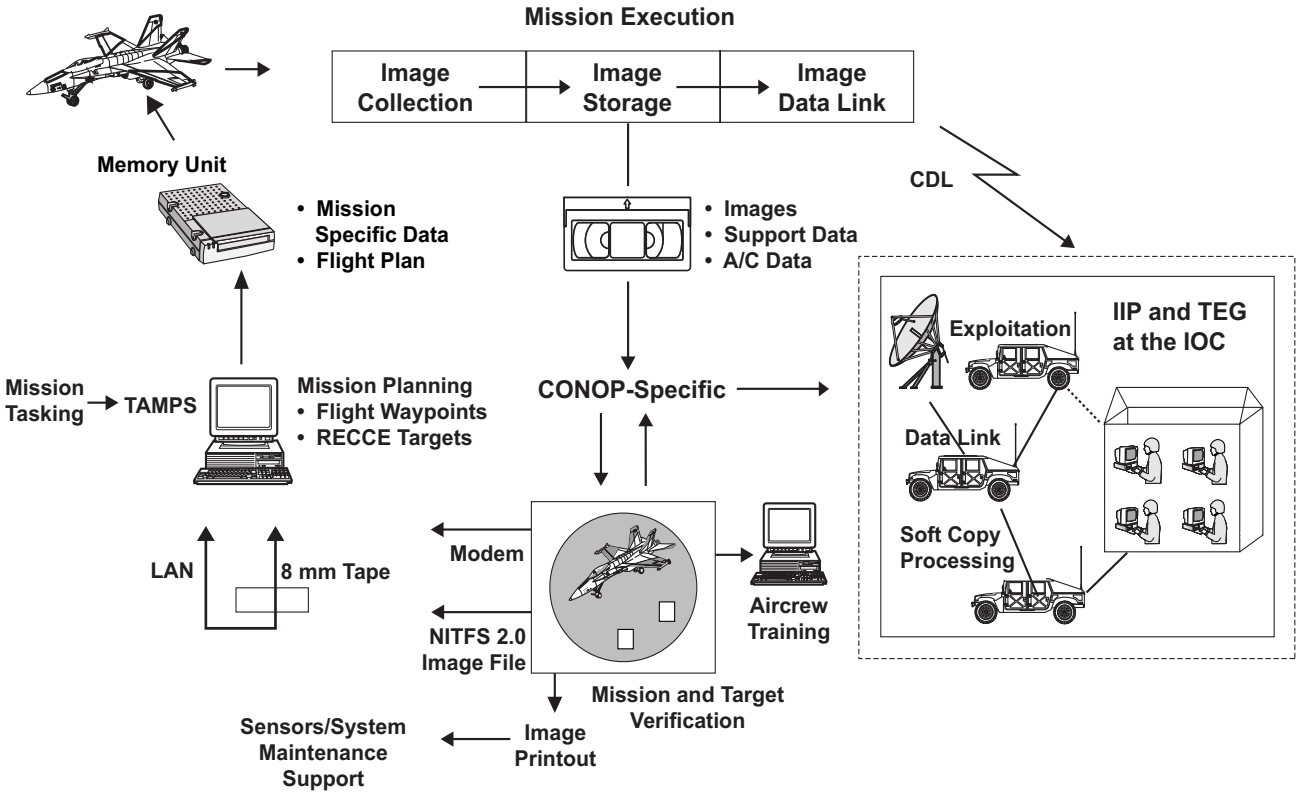


Figure 4-13. ATARS.

The Pioneer UAV resides in the VMU squadrons. Key UAV CIS resources are discussed in the following subparagraphs. See appendix D for additional information on UAV equipment and performance characteristics.

Ground Control Station 2000. The GCS-2000 is a small, modular, transportable control station for the UAV system. It controls and monitors the operations of the UAV and the installed payload. Since all pre-flight, takeoff, landing, post-flight, and maintenance procedures and functions can be performed from the GCS-2000, it can be used for controlling the UAV during all mission steps.

Portable Control Station. The portable control station (PCS) system—containing a flight control subsystem, a communications subsystem, and a power supply subsystem—allows UAV launch and recovery from a remote site, afloat or ashore, up to 40 kilometers from the GCS. The PCS allows the external pilot to perform takeoff/landing and flight control until command of the UAV is transferred to the internal pilot in the GCS.

Tracking Control Unit. The TCU controls all UAV tracking and communication functions, manages all up and down link data processing, and performs preflight and system diagnostic tests. The TCU houses all internal communication equipment and antenna subsystems for the GCS and is slaved to it by remoting cables.

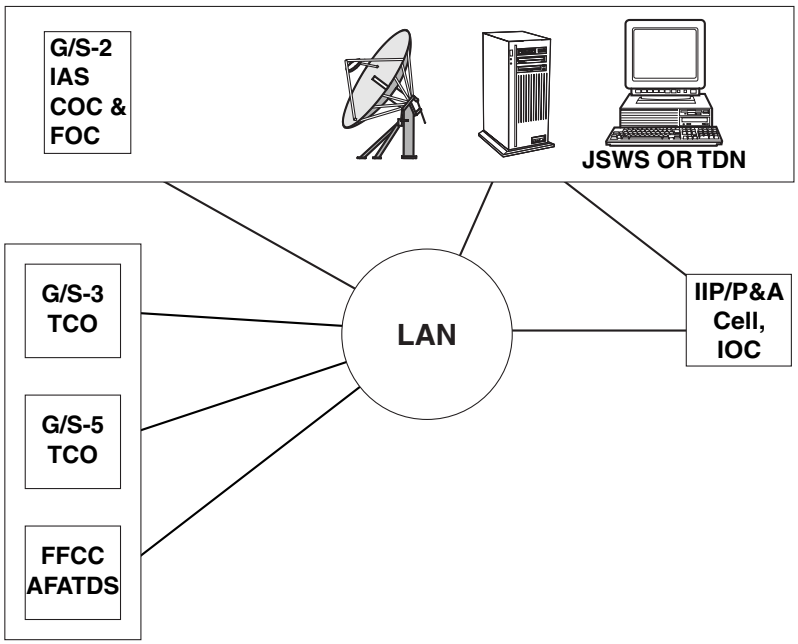
Remote Receiving Station. The RRS system is a miniature television receiver that can be attached or placed in direct support of commanders for real-time video pictures, supplemented with voice intelligence reports received from the GCS. There are two RRSs with each UAV system. Directional antennas allow video reception up to 30 kilometers from the UAV.

JSTARS Common Ground Station

Overview. The CGS is a mobile, tactical, multisensor ground station that provides the MAGTF CE with communications connectivity with the Air Force's E-8C and the capability to display, process, and disseminate acquired information. The CGS is organic to the MEF intel bn. Also receiving and processing MTI, FTI, and SAR data from the E-8C aircraft, the CGS is capable of receiving video data from UAVs, processed SIGINT from the Intelligence Broadcast Network, and secondary imagery from theater and national sources.

Basic System. The CGS is a HMMWV-mounted shelter system with component communications, computer, and mobile electric power systems. The CGS can be operated from either fixed positions or while mobile. Its crew of six operators can set up or tear down this system in 30 minutes and can support continuous operations. The CGS features an open-system architecture that enables rapid insertion of the latest government and commercial off-the-shelf technology. The ultrahigh frequency (UHF) SCDL provides the digital communications connectivity between the E-8C JSTARS airborne element and the MAGTF CE G-2 section's CGS, enabling the transmission of MTI, SAR, and FTI data acquired by JSTARS to support MAGTF target acquisition, situation development, battlespace management, and targeting functions. Figure 4-14 depicts the JSTARS CGS MAGTF systems architecture and concept of operations.

Subsystems. The CGS is comprised of six subsystems: data communications group, sensor interface group, distributed data processing group,



AFATDS=advanced field artillery tactical data system
COC=combat operations center
FOC=future operations center
FFCC=force fires coordination center
IAS=intelligence analysis system
IIP=imagery intelligence platoon
IOC=intelligence operations center
JSWS=JSTARS workstation
LAN=local area network
P&A Cell=production and analysis cell
TCO=tactical combat operations system
TDN=tactical data network

Figure 4-14. JSTARS and MAGTF Operations.

peripheral system group, voice communications group, and workstation group. CGS uses high performance CHS-2 SPARC 20 workstations, compatible with the MAGTF TDN.

Collection Capabilities. The E-8C carries a phased-array radar antenna in a 26-foot canoe-shaped radome under the forward part of the fuselage. The radar is capable of providing targeting and battle management data to all JSTARS operators, both in the aircraft and in the CGS module. These operators prepare intelligence reports or help coordinate aircraft, missiles or artillery fire support. With a range in excess of 155 miles, this radar covers an estimated 386,100 square miles in a single 8-hour sortie.

- **Wide Area Surveillance and Moving Target Indicator (WAS/MTI).** WAS/MTI are the radar's fundamental operating modes. WAS/MTI detects, locates, and identifies slow-moving targets. Through advanced signal processing, JSTARS can differentiate between wheeled and tracked vehicles. By focusing on smaller terrain areas, the radar image can be enhanced for increased resolution display. This high resolution defines moving targets and provides combat units with accurate information for attack planning.
- **Synthetic Aperture Radar/Fixed Target Indicator (SAR/FTI).** SAR/FTI produces a photographic-like image or map of selected geographic regions. SAR data maps contain precise locations of critical non-moving targets such as bridges, harbors, airports, buildings, or stopped vehicles. The FTI display is available while operating in the SAR mode to identify and locate fixed targets within the SAR area. The SAR and FTI capability used in conjunction with MTI and MTI history display allows post-attack assessments made by onboard or ground operators following a weapon attack on hostile targets.

Manpack SIDS

Overview. Manpack SIDS system provides the primary MAGTF capability for hand-held digital imagery reconnaissance (see figure 4-15 on page 4-20). Manpack SIDS consists of three digital cameras, three palmtop processors, and a base station providing ground reconnaissance units with the capability to take pictures and send the images back to the base station over selected communications paths. The base station then disseminates the images to the supported unit's intelligence section's IAS for follow-on analysis, production, and dissemination via the MAGTF TDN or other CIS resources.

Concept. Manpack SIDS is a tactical hand-held digital imagery collection and dissemination system designed to acquire, store, manipulate, and electronically transmit images derived from ground reconnaissance patrols. The system is comprised of a man-transportable outstation camera with processor and a base station processor with printer. The outstation, with its digital camera component, will be employed by MAGTF ground reconnaissance elements during operations for image acquisition. Imagery collected by the outstation may be stored for subsequent analysis or electronically transmitted to the base station over organic tactical communications for more timely analysis and intelligence production. The base station will be located at the ROC for receipt, manipulation, annotation, and subsequent dissemination of imagery to other intelligence elements or direct to subordinate units in accordance with specified intelligence reporting criteria.

Components and Connectivity. Manpack SIDS consists of three manportable outstations and one base station. The outstation's primary components are a digital camera with three lenses and a palm top computer. In addition, there is one night vision device per system used with the camera in low light situations. The outstation also comes with cables that attach the camera to the palm top, and the palm top to the encryption device and radio. The base station is primarily made up from the lap top computer and thermal printer. It also comes with the cables required to connect with the encryption device and radio (it is interoperable with the PRC-104, PRC-113, single-channel ground and airborne radio system,

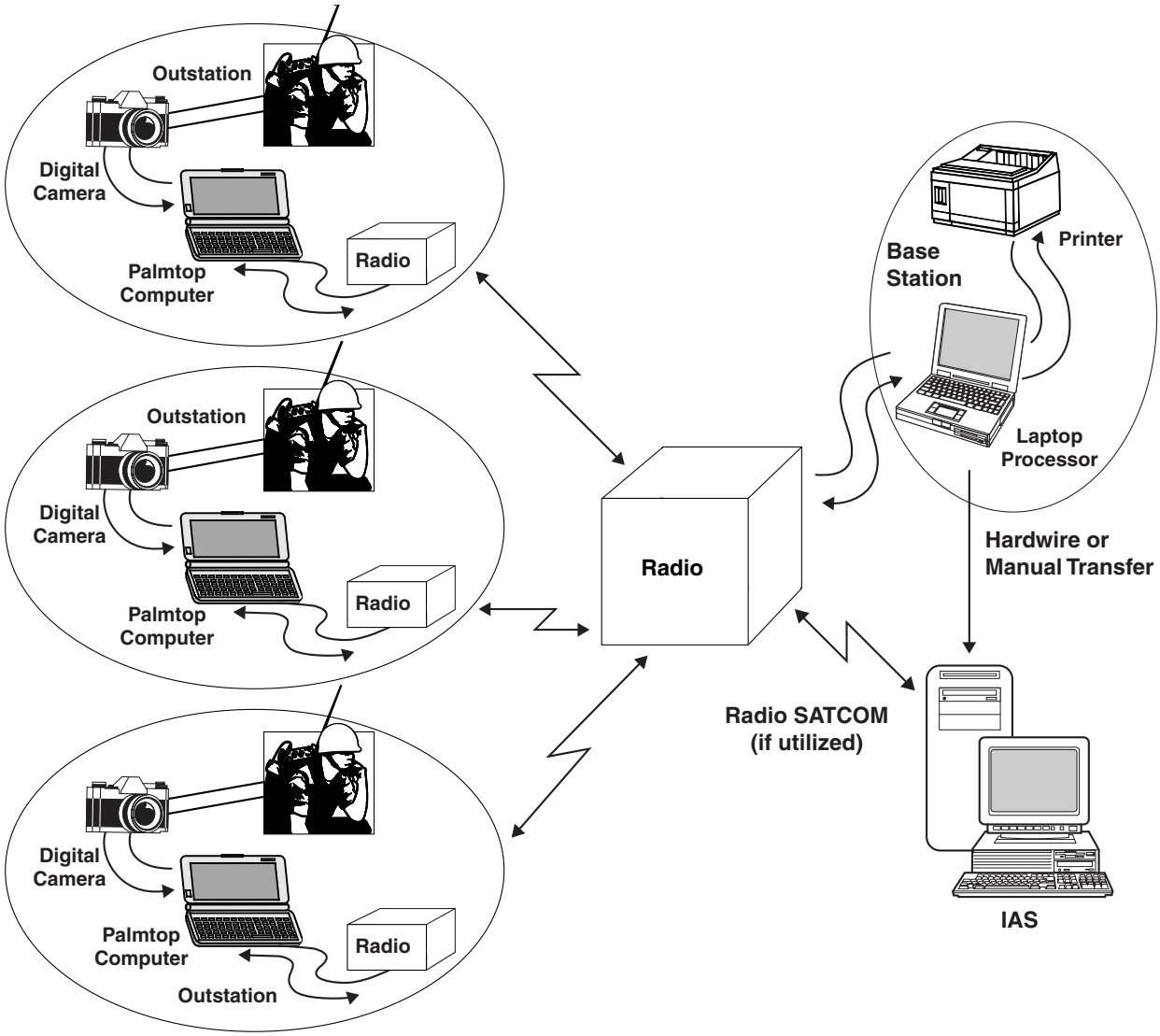


Figure 4-15. Manpack SIDS.

and various satellite communications resources). The base station is interoperable with the IAS via either the MAGTF TDN or other organic communications.

HML/A's NTS and NTIS

Components

- **AH-1W Night Targeting System.** The NTS FLIR's linear scanning array consists of 120 mercury cadmium telluride detector elements that scan left to right, then right to left to interlace the image. Information is then doubled to provide 480 lines of information. The super videocassette recorder (SVCR) automatically starts recording when the laser designator or weapons firing is activated or through command from the crew, and records in both super very high speed (VHS) and standard VHS formats. Finally, the television tracker is a video autotracker that works with both video and FLIR modes.
- **UH-1N Night Thermal Imaging System.** The NTIS components are similar to that of the NTS less the NTS's laser designator and television tracker capabilities. Its videocassette recorder (VCR) records only in standard VHS format.

Employment. The NTS and NTIS systems were fielded to provide the MAGTF with all-weather, day/night, autonomous attack, C2 and utility helicopter capabilities. Embedded within each system is a VCR to allow the aircrew to record engagements for debrief, collect BDA information, and to aid in target identification, acquisition, and engagement in a high threat environment while minimizing exposure time. The fielding of these systems greatly expanded the HML/A squadrons' traditional reconnaissance and surveillance capabilities because of their upgraded sensors and the VCR capabilities. However, the VCR does not record any other supporting information (e.g., geographic coordinates) beyond the basic imagery. Accordingly, helicopter aircrews will record concurrently an audio of the mission to make the tape more useful for post-mission debriefings and users.

Both helicopters, the AH-1W and UH-1N, can be employed in sections or as part of teams to scout ahead of friendly troops or to conduct visual and/or imagery reconnaissance of areas of interest, objectives, routes, point targets, etc. Because each is vulnerable to ground fire and provides other critical support to MAGTF (e.g., the AH-1W's fires capability; the UH-1N's C2 and utility capabilities), rarely will either be employed in a dedicated reconnaissance role. A more likely role for the AH-1W would be an armed reconnaissance mission as a function of offensive air support to deep air support operations. In such a mission the AH-1W would seek out and engage a given target set within a specified area, with a concurrent mission to collect intelligence data. Another likely mission for the AH-1W is armed interdiction, in which AH-1's would be deployed to engage a specific, known target and collect intelligence information.

Finally, both the AH-1W and UH-1N can be employed to conduct point or route reconnaissance missions of designated objective areas or by flying a route while video/FLIR recording to provide GCE, ACE or CSSE forces with a valuable early look at planned areas of operation.

All intelligence missions typically will be performed in addition to the primary missions of armed escort and rotary-wing close air support. During the conduct of any mission, both aircraft have a secondary mission of conducting aerial reconnaissance, and the aircrew would employ the NTS and NTIS to collect and store imagery data for post-mission follow-on analysis.

Tactical Photo

TACPHOTO is a digital camera system for units that normally return to base (i.e., flight crews, CI teams, and scout snipers), and have the capability to download acquired images into other intelligence information systems for follow-on intelligence exploitation. TACPHOTO uses the same digital camera and a similar concept of employment as Manpack SIDS. It consists of a digital camera, three lenses, PCMCIA card hard drive and card reader, cables, and the imagery receive and manipulate software.

Imagery Processing, Exploitation, and Production Capabilities

The Marine Corps possesses a limited organic imagery processing, exploitation, and production capability. Access to national, joint, theater, and other-Service processing and production capabilities will therefore be important elements of the Marine Corps imagery architecture (see figure 4-16 on page 4-22). The following provides descriptions of key IMINT processing, exploitation, and production information systems.

Dissemination Element

The MCIA's DE (formerly known as JSIPS) provides exploitation and dissemination of national imagery to MAGTFs and other Marine Corps units (to include the supporting establishment). The DE receives, stores, and exploits digital NRT imagery from national and theater imagery collection platforms. It also displays imagery in softcopy format for immediate exploitation. MCIA's intelligence, imagery, and database systems and requirements include defense message system,

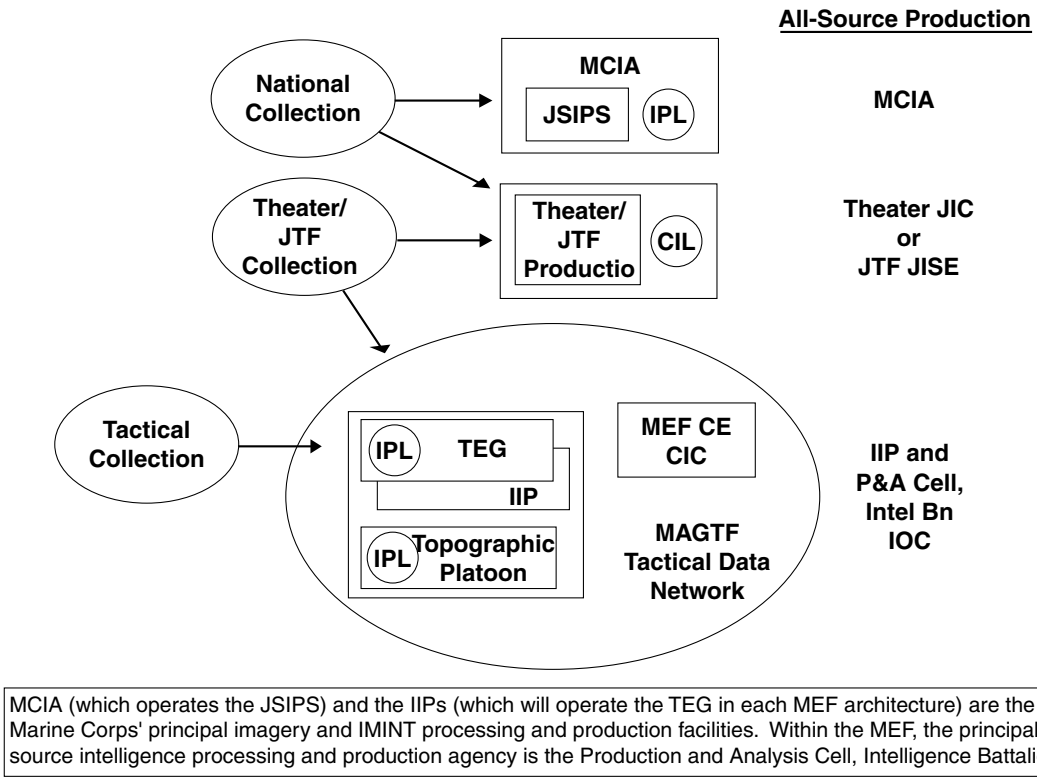


Figure 4-16. MEF Imagery Processing and Production.

JWICS, SIPRNET, 5D imagery server or IPL, RMS, imagery exploitation software system (IESS) data base, and the NIMA Delivery System (NDS).

Tactical Exploitation Group

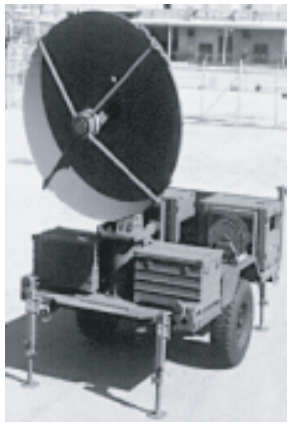
The TEG is a key MAGTF IMINT system and the only imagery exploitation and analysis tool available within the MEF (see figure 4-17). It is organic to each MEF's intel bn's IIP. It is capable of receiving, exploiting, and producing imagery and IMINT products and reports via its system architecture (see figure 4-18). The TEG provides the capability to receive, process, store, exploit, and disseminate imagery, to include ATARS EO, infrared, and radar imagery; U-2 SAR imagery; and secondary imagery products from the MCIA and theater JIC/JACs. Additionally, the TEG's equipment suite provides the capability to exploit film-based imagery and output from digital cameras such as Manpack SIDS, and heads-up displays, FLIR, and gun camera tapes from various tactical aircraft. Once received, processed, and exploited, the imagery is then transmitted over available SIDS device(s), MAGTF TDN or other CIS resources. Upon fielding of the TIGDL CDL, NRT exploitation and processing of ATARS imagery will be possible; until then, imagery data tapes must be downloaded and disseminated to the TEG post-mission. Even with the TIGDL CDL, only selected priority images will be down linked; the remaining imagery data is stored on tape and downloaded following recovery.

The TEG is packaged in three HMMWVs and three trailers. Due to its weight and balance, the TEG requires additional external lift capability to move the IIP and TEG within the area of operations. This additional lift is not resident within the intel bn and must be provided either by the MEF headquarters group or some other external source.

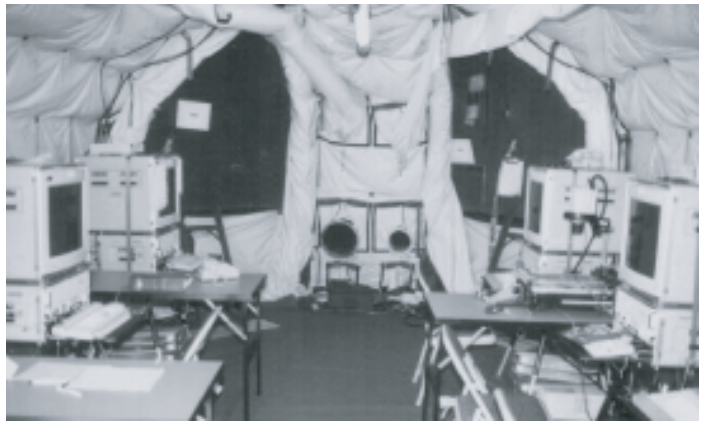
The initial operational capability TEG allows for the processing of F/A-18(R/C) mission tapes and data link and handles preprocessed national, U-2, UAV, and digital camera systems imagery. The

Vehicles and Power

Vehicle and Work Tent



Tactical Data Link



TEG Workstations

Figure 4-17. TEG Components.

full capability TEG provides interoperability with all Common Imagery Ground/Surface Systems (CIGSSs) baseline sensors (e.g., ATARS, Global Hawk) and handles all other preprocessed national imagery transmission format (NITF) imagery data.

Image Product Library

The IPL is the migration system to replace the legacy 5D System. IPL supports the storage and dissemination of imagery and imagery products, providing a library of information to imagery customers worldwide. IPL uses a standard Intelink or Intelink-S client to provide user access to this library, and supports both data push and data pull, via user profiling. The IPL stores imagery in NITF 2.0, TIFF, and other graphical formats.

Libraries are composed of three types: product, command, and national. The three types are differentiated by content, storage size, performance, and responsibility for operations and management. They are alike in that each type may contain digital imagery or digital imagery products from all sources including tactical, theater, national, civil, and commercial collection systems. All libraries share common digital imagery standards.

IPLs contain shared, restricted, or both types of imagery and imagery products required to support individual organizations. Each organization will determine the population of and manage its IPLs. The imagery and imagery-based products consist of tactical, theater, national, civil, and commercial imagery and imagery-based products. Most of the data stored on IPLs will be imagery products with

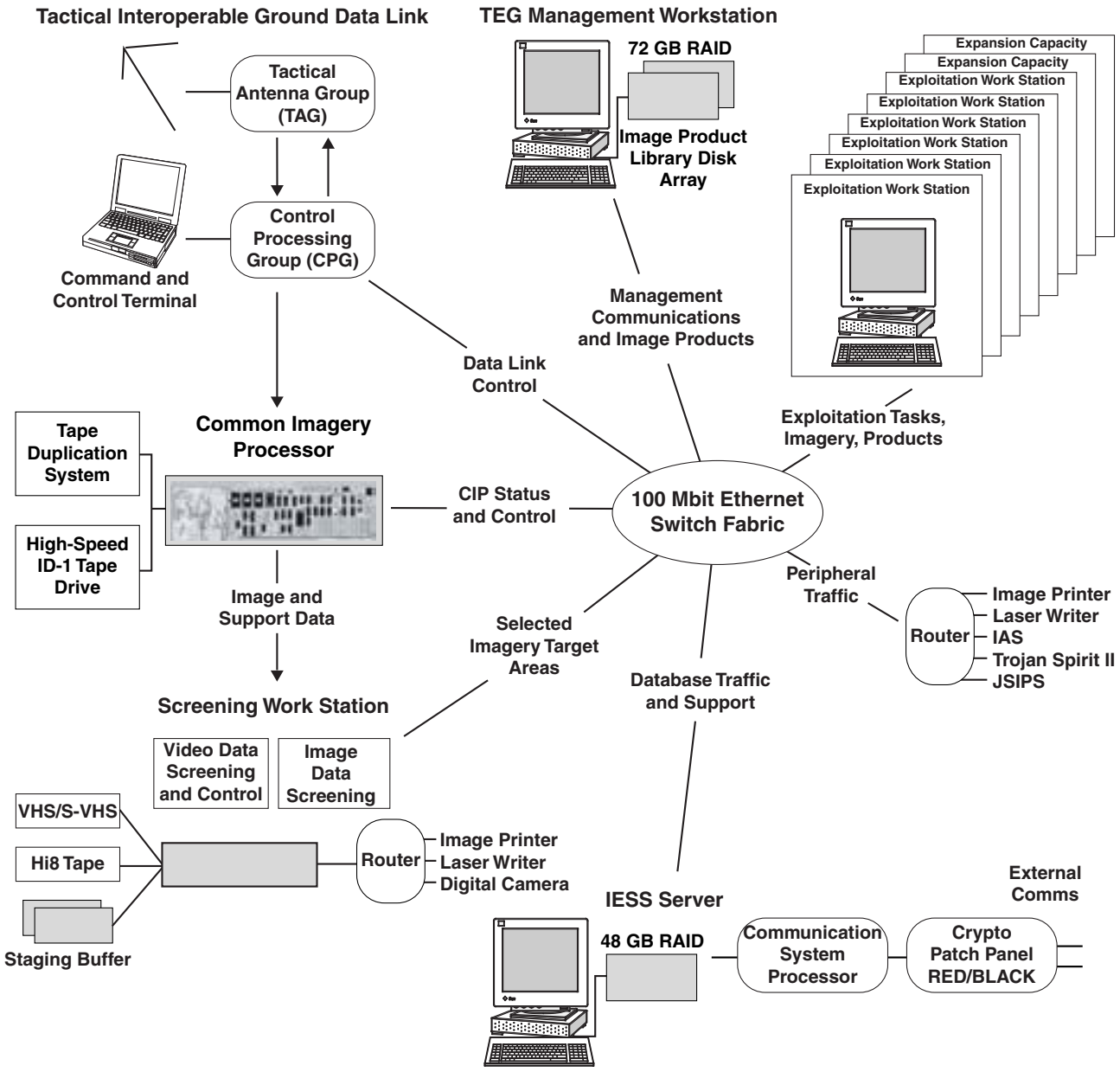


Figure 4-18. IIP/TEG Systems Architecture.

the owner determining the mix between imagery and imagery products, the size of their IPLs, their interfacing organizations, and the products requiring storage. NIMA will provide the updated IPL management software. IPLs are based upon existing 5D capabilities, scaled for size and performance, and some are portable. IPLs support various levels of command, CIGSS sites, and other organizations outside the command structure of the services requiring the use of libraries. When IPLs are integrated into the 17+ CIGSS ground station architectures, processed tactical imagery (still or motion) is fed to an IPL, acting as an imagery buffer, at the ground station. Stored imagery is then pulled or pushed to the exploitation workstations, exploited, then sent to the public access IPL for dissemination.

IPLs will be capable of importing, storing, exporting and managing imagery, image-based

products, and associated metadata. IPLs have the capability to retain digital imagery data in on-line, near-line, and off-line storage media. Each IPL maintains a catalog populated with metadata of its imagery and imagery product holdings. The national IPL supports up to 1,300 image requests per day and up to 900 gigabytes (GB) for on-line imagery storage. The IPL should not take longer than 8 minutes to transfer a full frame (930 megabytes [MB]) national image to any requesting client (assuming fiber distributed data interface and no LAN contention).

Figure 4-19 provides a broad depiction of the services, applications, and scope within the IPL.

Imagery CIS Architecture

Figures 4-20 on page 4-26 and 4-21 on page 4-27 summarize the information discussed throughout this chapter and depict the internal IMINT CIS architecture for a MEF, and the broader IMINT CIS architecture through the theater and national levels.

IMINT Communications and Information Systems Planning Considerations

The following identifies key CIS requirements and planning considerations in support of MAGTF IMINT operations.

- Ensure that the MAGTF CE, IIP elements, and other MAGTF units are included in the distribution of IMINT-related address indicator groups to receive pertinent JTF, Navy, theater, and national intelligence and IMINT products.
- Determine and coordinate radio net requirements, supporting frequencies, and operational

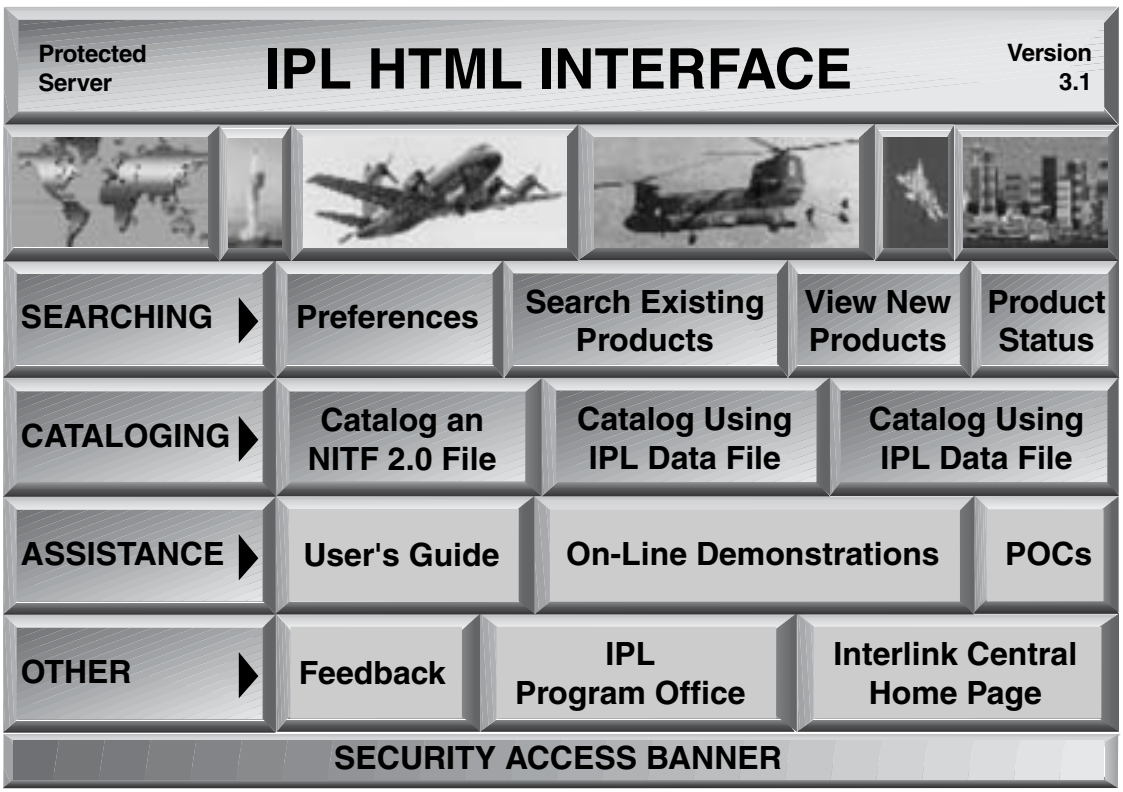


Figure 4-19. Image Product Library.

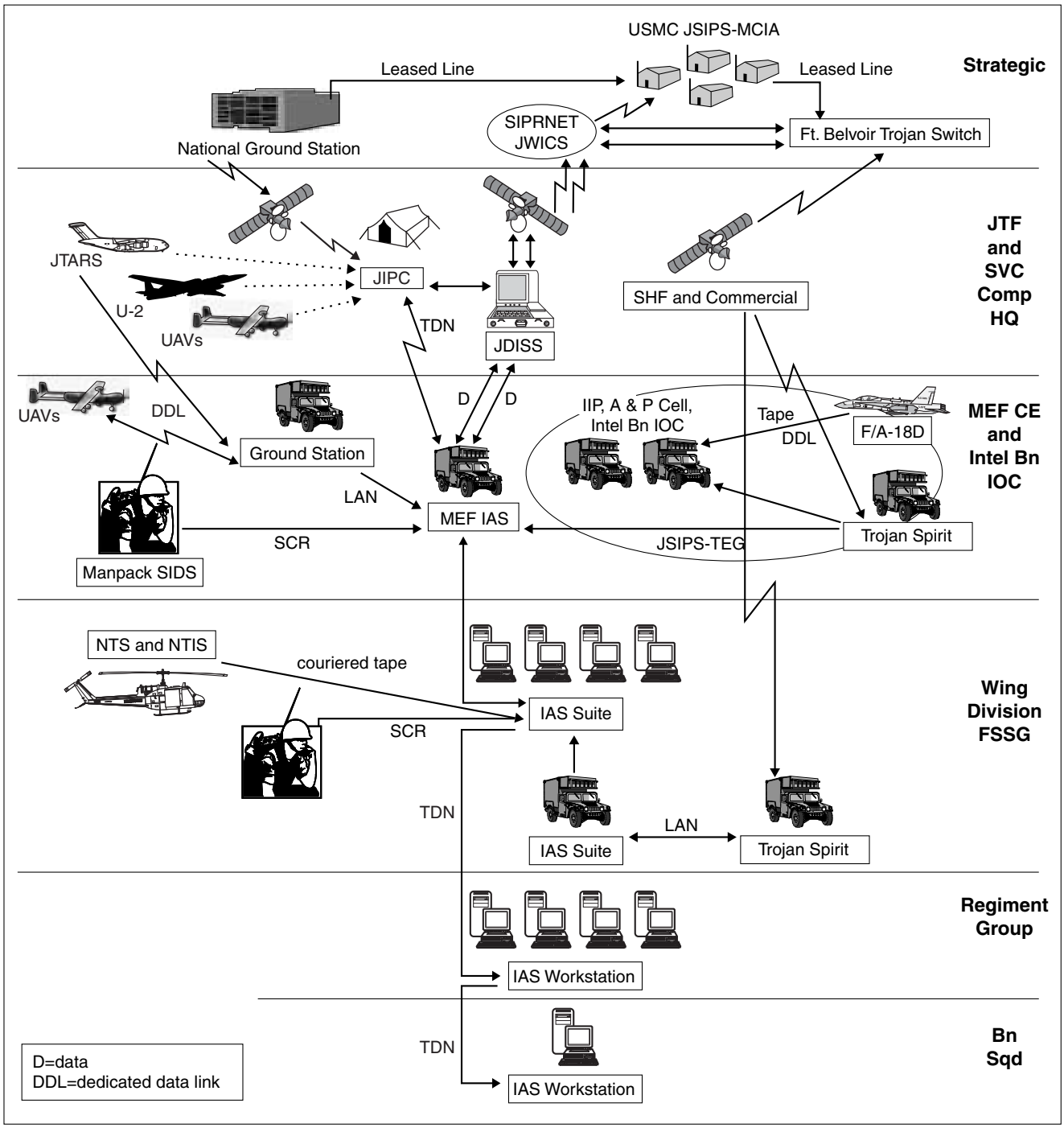


Figure 4-20. MEF Internal Imagery CIS Intelligence Architecture.

procedures in support of IMINT operations (external to MAGTF, internal MAGTF, intelligence broadcasts, retransmission sites, routine and time-sensitive operations, etc.).

- Coordinate IMINT CIS activation and restoration priorities and supporting procedures.
- Establish, operate, and manage unique IMINT communications requirements (e.g., with MCIA for the JSTARS CGS).
- Identify and procure communications security materials system (CMS) requirements for unique IMINT communications.

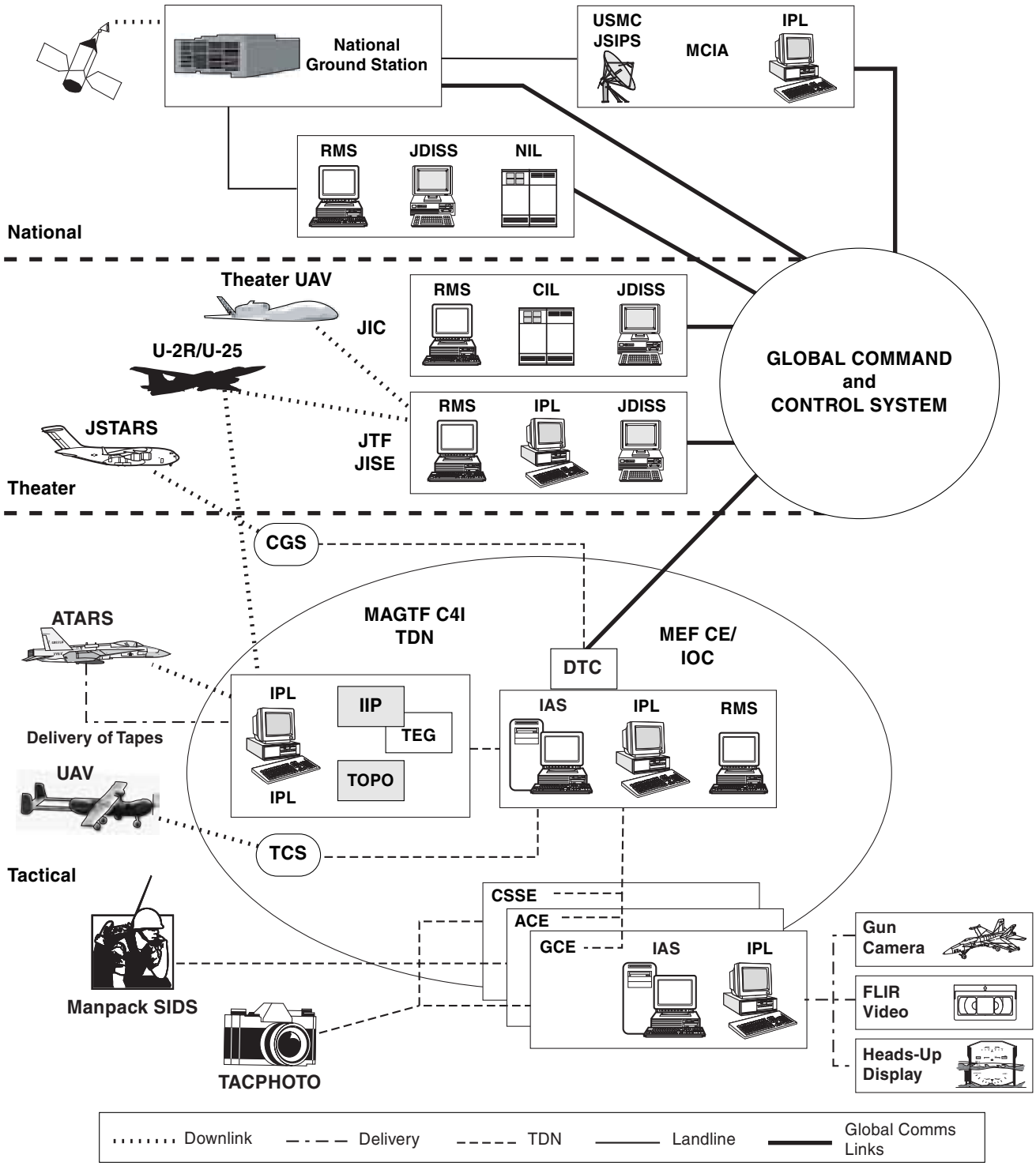


Figure 4-21. MEF Through National IMINT CIS Intelligence Architecture.

- Determine and coordinate wire communications (to include telephones) supporting IMINT operations.
- Determine and coordinate LANs and WANs and unique intelligence network information systems requirements in support of IMINT operations (hardware, software, internet protocol addresses, etc.).
- Integrate MAGTF IMINT elements' CIS operations with those of other MAGTF and pertinent JTF and other components intelligence and reconnaissance units (mutual support, cueing, etc.).
- Integrate CIS of IMINT elements employed in general support with collocated GCE, ACE, CSSE, and other MAGTF elements (e.g., integration of UAV squadron RRS with supported GCE units to provide time-sensitive reporting, coordination of maneuver).
- Coordinate MAGTF IPL and Manpack SIDS administration and operations.
- Coordinate IMINT CIS and collection, production, and dissemination operations and procedures with other Services', allied and coalition forces' IMINT and all-source intelligence operations.

CHAPTER 5. OPERATIONAL PLANNING AND EXECUTION

Whether performed at the national or the battalion/squadron level, the key functions of planning are—

- Lead to a plan that directs and coordinates action.
- Develop a shared situational awareness.
- Generate expectations about how actions will evolve and how they will affect the desired outcome.
- Support the exercise of initiative.
- Shape the thinking of planners.

Marine Corps Planning Process

The Marine Corps Planning Process (MCPP) helps organize the thought processes of a commander and the staff throughout the planning and execution of military operations. The MCPP focuses on the threat and is based on the Marine Corps warfighting philosophy of maneuver warfare. It capitalizes on the principle of unity of effort and supports the establishment and maintenance of tempo. The MCPP steps can be as detailed or as abbreviated as time, staff resources, experience, and the situation permit. The command and staff actions at all echelons must apply the MCPP. From the Marine Corps component headquarters to the battalion/squadron level, commanders and staff members must master the MCPP to be full participants in integrated planning. Additionally, the MCPP complements deliberate or crisis action planning (CAP) as outlined in the Joint Operation Planning and Execution System (JOPES).

The MCPP establishes procedures for analyzing a mission, developing and analyzing courses of action (COAs) against the threat, comparing friendly COAs against the commander's criteria and each other, selecting a COA, and preparing an OPORD for execution. The MCPP organizes the planning process into six steps (see figure 5-1).

The MCPP provides the commander and the commander's staff a means to organize their planning activities and transmit the plan to subordinates and subordinate commands. Through this process, all MAGTF levels of command can begin their planning effort with a common understanding of the mission and commander's guidance. The six integrated steps of this process follow.

Mission Analysis

Mission analysis is the first step in planning. Mission analysis reviews and analyzes orders, guidance,

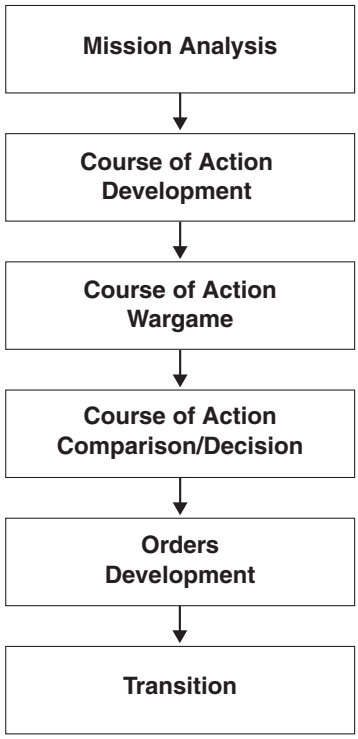


Figure 5-1. The Marine Corps Planning Process.

and other information provided by higher headquarters and produces a unit mission statement. Mission analysis drives the MCPP.

COA Development

During COA development, the planners use the mission statement including higher headquarters tasking and intent, commander's intent, and commander's planning guidance to develop the COA(s). Each prospective COA is examined to ensure that it is suitable, feasible, distinguishable, acceptable, and complete with respect to the current and anticipated situation, the mission, and the commander's intent. In accordance with the commander's guidance, approved COAs are further developed in greater detail.

COA Wargaming

COA wargaming involves a detailed assessment of each COA as it pertains to the enemy and the battlespace. Each friendly COA is war-gamed against selected threat COAs. COA wargaming assists the planners in identifying strengths and weaknesses, associated risks, and asset shortfalls for each friendly COA. COA wargaming identifies branches and potential sequels requiring additional planning. COA wargaming provides the most reliable basis for understanding and improving each COA.

COA Comparison and Decision

In COA comparison and decision, the commander evaluates all friendly COAs—against established criteria, then against each other—and selects the COA deemed most likely to accomplish the mission.

Orders Development

During orders development, the staff takes the commander's COA decision, mission statement, commander's intent, and guidance and develops orders to direct the actions of the unit. Orders serve as the principal means where the commander expresses decision, intent, and guidance.

Transition

Transition is an orderly handover of a plan or order as it is passed to those tasked with execution of the operation. It provides those who will execute the plan or order with the situational awareness and rationale for key decisions necessary to ensure there is a coherent shift from planning to execution.

Interactions among various planning steps allow a concurrent, coordinated effort that maintains flexibility, makes efficient use of time available, and facilitates continuous information sharing. Appendix F captures major IMINT planning considerations and activities in support of MAGTF operations, cross-referencing each with the MCPP step and major staff planning activities that they are most associated.

Joint Planning Processes

Joint Deliberate Planning

The deliberate planning process is used by the joint staff and combatant commanders to develop plans in support of national strategy. The Joint Strategic Capabilities Plan (JSCP) apportions forces and resources for use during deliberate planning by the combatant commanders and their Service component commanders. Figure 5-2 illustrates how the MCPP fits within and supports the joint deliberate planning process.

Crisis Action Planning

CAP is conducted in response to crises where national interests are threatened and a military response is being considered. In CAP, the time available for planning at the national level may

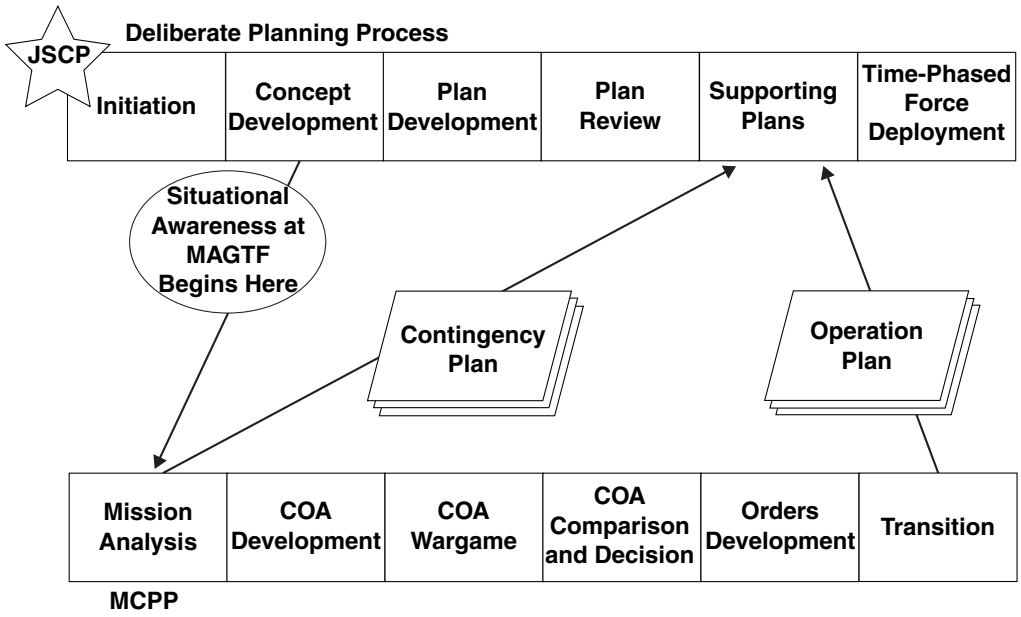


Figure 5-2. The MCPP and the Joint Crisis Action Planning Process.

be reduced to as little as a few days. CAP procedures promote the logical, rapid flow of information and the timely preparation of campaign plans or OPORDs. Figure 5-3 illustrates how the MCPP fits within and supports the joint crisis action planning process.

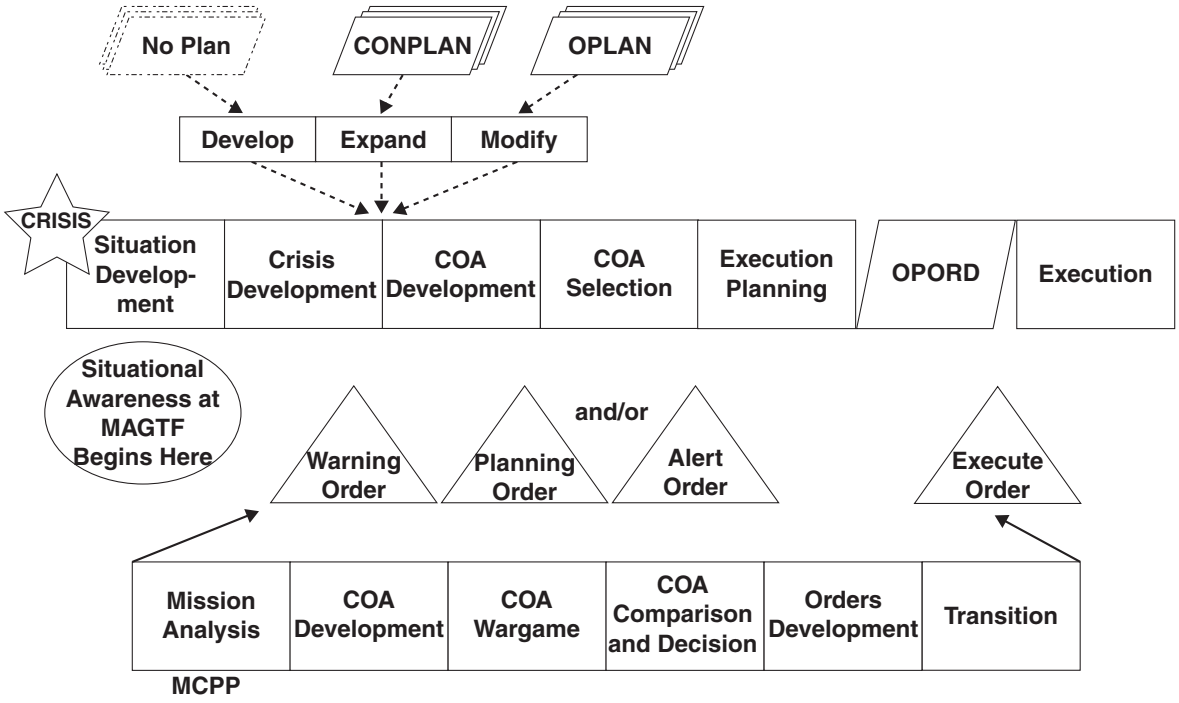


Figure 5-3. The MCPP and the Joint Deliberate Planning Process.

Planning and Imagery Intelligence

Planning and Intelligence Cycle

IMINT planning and execution is conducted concurrent with six phases of the intelligence cycle. The first phase is planning and direction. It consists of those activities that identify pertinent IRs and provides the means for satisfying those requirements. Intelligence planning and direction is a continuous function and a command responsibility. The commander directs the intelligence effort; the intelligence officer manages this effort for the commander based on the intent, designation of commander's critical information requirements (CCIR), and specific guidance provided during the planning process. Planning and direction functions include:

- Requirements development.
- Requirements management.
- Collection management.
- Production management.
- Dissemination management.
- Planning the intelligence support system.

The intelligence cycle is a procedural framework for the development of mission-focused intelligence support. It is not an end, nor should it be viewed as a rigid set of procedures carried out in an identical manner on all occasions. The intelligence cycle must be applied in a manner that develops the required intelligence in the most effective way.

The application of the intelligence cycle will vary during mission planning and execution. Application of the intelligence cycle is driven by IRs. In theory, a unique iteration of the intelligence cycle is carried out for each individual IR. In practice, particularly during planning, IRs are grouped together and satisfied through a single, intelligence development process that concurrently addresses all IRs, including IMINT requirements. During planning, the application of the intelligence cycle supports mission analysis, course of action development and course of action wargame by providing basic intelligence, including IMINT, in the form intelligence estimates, supporting studies, and IPB analysis that describe the battlespace and threat. During course of action comparison and analysis, orders development and transition, the intelligence cycle is applied to satisfy emerging IRs and update the intelligence estimate and IPB products, all of which may be supported by IMINT. During execution the intelligence cycle is applied to implement the intelligence collection, production, and dissemination plan; refine IPB analysis, and generate mission-specific multi-discipline intelligence operations and intelligence products (including IMINT), all of which are integrated with the concept of operations. During execution, IRs are satisfied on a more individualized basis. New IRs are usually generated in response to a specific operational need. Each IR is unique and must be satisfied in a timely manner to facilitate rapid decisionmaking and the generation or maintenance of tempo (see figure 5-4).

Basic IMINT Planning Process

There are eight steps in the basic IMINT planning and execution process.

- **Planning.** The first step to receiving IMINT support is to determine that an IR exists. Exact needs are carefully determined—to include key collection, production, and dissemination requirements—so priorities can be accurately determined, resources are not overwhelmed, and timely support is received.

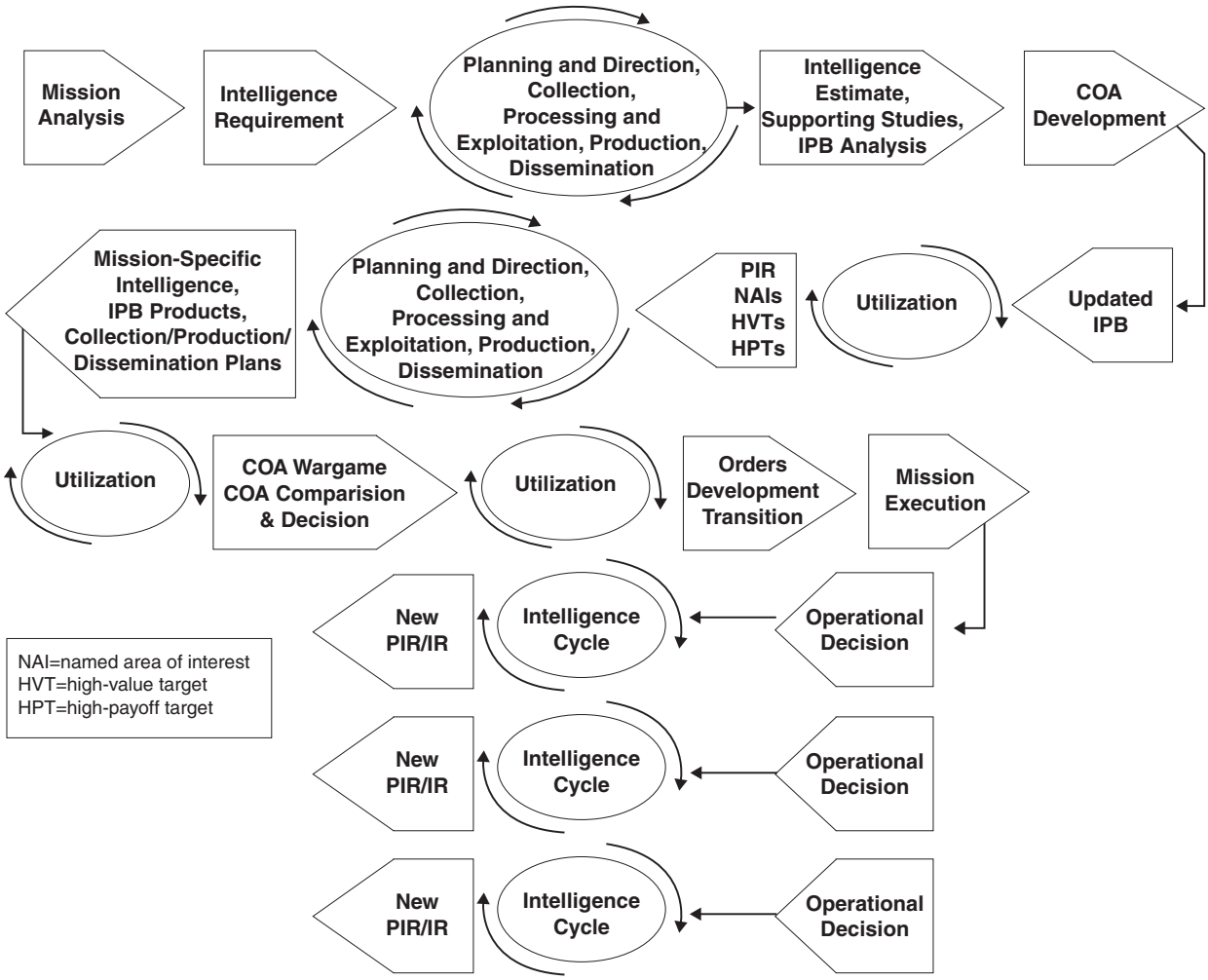


Figure 5-4. Application of the Intelligence Cycle.

- **Requesting.** The most important first step of any request is to clearly articulate IRs (to include desired imagery and other specific IMINT support). Statement of an IR should include the mission and how the intelligence product sought will get the job done.
- **Validating.** On-hand intelligence and imagery is reviewed to determine if the IR can be immediately answered. If not, it is then checked against previously validated IRs and ongoing/ planned intelligence operations to avoid unnecessary duplication. Finally, it will be checked against the capabilities of the unit's and supporting intelligence assets. If then validated, a priority will be assigned to it and associated ICRs, IPRs, and IDRs developed and prioritized.
- **Plans and Taskings.** A determination will also be made as to whether organic or external intelligence operations will be tasked to satisfy the IR. If collection is required, CMDO will determine the best intelligence asset suited to perform the mission. Concurrently, CMDO will develop plans and taskings to ensure eventual dissemination requirements can be achieved, while the P&A cell OIC will develop necessary

production plans and tasking. If organic intelligence resources will be used, appropriate orders are issued. If external support will be required, the IR will be submitted to higher headquarters or supporting organizations.

- **Collecting.** The validated ICRs and IPRs will be used to ensure the most effective type of imagery is collected to satisfy the overall IRs. The image can be recorded hardcopy or softcopy single frame or continuous (video), depending on the actual sensor. Capabilities and limitations of each imagery collection element (e.g, maximum and optimal ranges), the time the collection must occur, and the weather will influence the nature of collection operations.
- **Exploiting.** For IMINT exploitation, requirements are defined in terms of three phases of analysis, production, and reporting. Each phase represents a greater degree of analysis and a longer period of time available to accomplish the exploitation and production.
  - Phase One is the rapid exploitation of newly acquired imagery and reporting of imagery-derived intelligence and intelligence information within a specified time from receipt of imagery. This phase satisfies priority requirements of immediate need and/or identifies changes or activity of immediate significance.
  - Phase Two is the detailed exploitation of newly acquired imagery and the reporting of imagery-derived intelligence and intelligence information within the bounds of analytic requirements and timeliness of need. This phase provides an organized and comprehensive account of the intelligence or intelligence information extracted from newly acquired imagery and supported by other intelligence source materials as appropriate.
  - Phase Three is the indepth analysis of available imagery pertinent to an IR and the reporting of results within a specified time. This phase provides the most comprehensive, indepth analysis of a target or topic in response to IRs, using imagery as the primary data source but incorporating data and intelligence from other sources as appropriate.
- **Disseminating.** Imagery and IMINT products are disseminated either as hardcopy or softcopy (e.g., digital or electronic) products. Hardcopy products will go via couriers or some type of mail system. Softcopy products may also be distributed as hardcopy products (e.g., on CDs and floppy/zip disks) or electronically via the MAGTF TDN. The requestor and the supporting intelligence officers, with assistance from units' G-6/S-6s, must ensure that the requested product can be transmitted over available supporting CIS. The length of time required to receive a product electronically depends on the size of the file. Low rates of compression (e.g., 4 to 1) allow an image to be transmitted, decompressed, recompressed, and retransmitted. Higher rates of compression generally will not allow a product to be recompressed. It is recommended that if a product will be retransmitted, a copy be made before it is compressed. Once it is determined that a product meets the need of the command, the compressed copy can be transmitted without losing data.
- **Use.** The last step of the IMINT planning and execution process, as with the intelligence process, is the most important—effective utilization. Commanders and other imagery/IMINT users should quickly notify the intelligence officer as to how well the products answered their CCIRs and IRs. Additionally, new IRs that result from the new imagery/IMINT should be rapidly identified and action initiated to most effectively plan future operations. Finally, providing the intelligence officer and IMINT elements feedback will identify problems (e.g., product formats, missing or excessive information, etc.) and allow improvements to be quickly developed and implemented.

Planning Responsibilities

Intelligence Officer

Primary staff responsibility for IMINT operations planning lies with the G-2/S-2. Specific responsibilities are—

- Preparation of integrated, multi-discipline intelligence and reconnaissance operations and supporting IMINT plans, orders, annexes, and appendices.
- Coordination with the G-3/S-3 to ensure that the planned IMINT effort supports the concept of operations and scheme of maneuver, and ensures effective prioritization and integration of IMINT operations.
- Coordination with the G-6/S-6 officer for CIS support to the IMINT elements, including circuits, network access, frequency assignment, equipment, and call signs.
- Liaison with IMINT agencies and units external to the MAGTF.
- Coordination with the G-4/S-4 to ensure adequate logistics support of IMINT elements (in particular, the transportation and maintenance of IMINT units' unique and sizable equipment).

Intelligence Battalion Commander/Detachment OIC

The intel bn commander/detachment OIC is responsible to the G-2/S-2 (or the MAGTF intelligence operations officer) for the planning, direction, and execution of MAGTF IMINT operations. Specific duties include:

- Advise the G-2/S-2 on IMINT employment and its integration with other services, JTF, theater, and national IMINT operations.
- Prepare MAGTF IMINT plans and orders in conjunction with other intelligence section staff officers and key intel bn subordinates (e.g., IIP platoon commander).
- Plan, supervise, and assist IMINT collection requirements and taskings for MAGTF operations in conjunction with the collection management officer.
- Coordinate the movement, operation, and reporting of IMINT units in coordination with the SARC OIC and the G-3/S-3.
- Coordinate MAGTF all-source fusion center (AFC) analyst exchanges with IMINT analysts, and the integration of imagery and IMINT products with all-source intelligence production in conjunction with MAGTF AFC OIC.
- Plan for the timely reporting of IMINT-derived intelligence to MAGTF and external elements and the rapid handling of perishable IMINT information in coordination with the dissemination officer.
- Plan and coordinate IMINT communications paths and information systems management and operations in conjunction with the G-6/S-6.

General Planning Considerations

Principles

Provide Imagery and IMINT to Meet Requirements

The IMINT plan must ensure imagery data is collected, processed, and reported to satisfy the IRs set forth in the commander's guidance and collection plan. Particular attention must be paid to the timeliness and formats of the data provided.

IMINT Operations Must be Integrated with Operations

The IMINT plan must take into account the location and activities of the supported units. Planned missions must be scheduled where and when they can best collect sensor data, and C2 and CIS arrangements coordinated ensuring imagery data and IMINT reports are reported to the supported units. Enemy activity may be anticipated at certain

phases of the operation; IMINT operations and analytical personnel must have a situational awareness of both intelligence estimates and ongoing operations to focus their efforts at a particular time and area. Finally, the requirement for timeliness in processing and reporting may vary depending upon the stage of the operation; personnel must be aware of current timeliness requirements as well as the availability of CIS resources with all supported commands.

Provide Redundancy in the Intelligence Plan

The IMINT plan must be integrated with other intelligence and reconnaissance operations to ensure that the needed data can still be acquired even if a planned imagery mission is canceled or if equipment malfunctions occur. The ability to provide this redundancy is dependent upon a number of factors, primarily the number of imagery missions available, capability of other intelligence resources to acquire the information needed, and the availability of production resources.

Make Full Use of All IMINT Resources

While some imagery collection resources may be held in reserve, most such units and systems can fulfill multiple missions and thus will likely be employed (e.g., ATARS). Close coordination and integration of operations and intelligence activities will aid with identifying and prioritizing such multi-purpose missions. IMINT production resources are not held in reserve.

Concept of Operations

The IMINT effort must support and adapt to the MAGTF commander's intent, concepts of intelligence and operations, and the supporting scheme of maneuver. Key questions to answer include:

- What is the MAGTF AO and the area of interest (AOI)?
- What is the MAGTF concept of operations, task organization, and main and supporting efforts?
- What are the standing PIR and IRs? Which have been tasked to supporting IMINT units? What specific information is the commander most interested (e.g., enemy ground operations, enemy air operations, target BDA, friendly force protection or enemy future intentions)?
- What is the concept of MAGTF fires support? How will MAGTF target development and target intelligence be conducted? What are the specific imagery needs in support of these?
- What are the IMINT and intelligence concepts of operations of other JTF, component, and theater resources? What is the task-organization and command/support relationships for all MAGTF intelligence and reconnaissance units?
- How can Navy IMINT assets and other Services, JTF, theater, and national IMINT assets be employed and integrated to support MAGTF operations?

Terrain

Terrain factors have a significant impact on IMINT operations; such as the ability of IMINT sensors to see through vegetation and IMINT's requirements for line-of-sight (LOS) communications. All IMINT collection systems require LOS with the target area to be effective. Accordingly, IMINT planners must assess the effects of mountains, defilade, vegetation, and other potential terrain obstacles on planned IMINT operations.

Weather

Weather is a key limiting factor for IMINT operations. Bad weather degrades the identification and location of targets. Weather can also limit the type of imagery collection capabilities that may be employed. Finally, low ceilings and poor visibility decreases visual reconnaissance effectiveness as well as the resolution of photographic systems.

Precipitation

Visible moisture degrades optical and visual reconnaissance systems. A UAV is not an all-weather

aircraft. Exposure to rain, ice, and snow can severely damage or destroy a UAV.

Wind

UAVs, due to their lighter weight, are significantly more affected by wind than manned aircraft. The Pioneer UAV has a crosswind limitation of 16 knots for takeoff and landing and a total wind component limitation of 30 knots in flight. The UAV currently under development will have a crosswind limitation of 25 knots and a total wind component limitation of 30 knots in flight.

Clouds, Haze, and Smoke

In addition to affecting an aircrew's ability to conduct visual reconnaissance, these conditions also affect EO and infrared systems in manned aircraft and UAVs.

Daylight, Sun Angles, and Shadows

The angle of the sun affects visual, TV, and FLIR observation in varying degrees. The quality of FLIR imaging decreases as the sun rises and reaches a point where a target can be seen visually. At this point the target cannot be detected by a FLIR. Prior to sunset and just after sunrise, long shadows are cast by large terrain features and can obscure objects in their path. The ideal time to take photographs or observe a target is midmorning or midafternoon. During these periods, shadows are cast long enough to add definition and dimension to a target.

Threat

General

Detailed threat analysis must be conducted to determine which IMINT sensors and platforms can be employed effectively against a given enemy and how to employ limited MAGTF and external resources to obtain the best possible IMINT. Imagery operations can be hampered by the enemy's air defense capability and its camouflage, cover, concealment, and deception activities.

Aviation-Related

Enemy air defenses have a direct effect on aerial imagery collection missions. Significant antiaircraft artillery (AAA) and surface-to-air missile (SAM) threats may degrade visual reconnaissance due to a need for aircraft to stay beyond threat air defense ranges. IMINT planners must assess threat air defense and air-to-air threats when evaluating risk and determining routes. Because of a UAV's slow speed, AAA is its greatest threat, while SAMs pose greater risks to MAGTF fixed-wing aircraft. Finally, threat electronic warfare capabilities must be determined to assess their effects on UAV and manned imagery platforms radio uplinks and imagery downlinks.

Specific Planning Considerations and Execution Activities

Planning and Direction

Objectives

IMINT planning is a continuous function that requires close interaction between the G-2/S-2 and IMINT unit planners. Key objectives include:

- Identify IMINT requirements.
- Prepare IMINT operations plan.
- Plan and establish the IMINT support system (CIS, logistics, etc.).
- Issue orders/tasking to IMINT units.
- Supervise and coordinate IMINT operations.

Key Considerations

Effective IMINT planning and execution require close coordination, liaison, and integration with all-source intelligence elements. IMINT collection management often will be driven by tip-offs (or cueing) from SIGINT, HUMINT, and other sources of intelligence. Also, fusion of IMINT with other intelligence ultimately drives the conduct of future IMINT operations and the development of IMINT products. Related concerns include:

- **Split-basing.** IMINT operations favorably lend themselves to using a split-basing concept of operations and should be considered for many deployment situations. CIS connectivity, bandwidth availability, and equipment and combat service support requirements are key factors in determining the IMINT concept of operations that must be considered.
- **Liaison elements.** Identifying, preparing, and locating IMINT or all-source intelligence liaison elements to support MAGTF IMINT operations is a critical early planning action. IMINT liaison teams will be small in number due to limited availability of imagery personnel. Placing IMINT liaison elements where they can coordinate operational planning and providing them necessary CIS support are the keys (e.g., IMINT liaisons with JTF collection and ATO planners).
- **Physical demands.** IMINT planners must take into account the strenuous mental and physical demands (especially visual) on imagery analysts during sustained operations, particularly when planning watch schedules for imagery analysts performing detailed imagery exploitation tasks. Additional IMINT planning considerations for specific type MAGTF operations include:
  - **Expeditionary operations.** Multispectral imagery, hyperspectral imagery, and other new special imagery capabilities can provide unique support to ship-to-objective maneuver (STOM) operations, such as in the detection of sandbars and obstacles in the water.
  - **Peacekeeping and humanitarian assistance operations.** National imagery usually provides the initial baseline to support planning for peacekeeping and humanitarian assistance operations. The typical multinational nature of these operations, however, leads to critical planning and dissemination requirements. National imagery is not releasable to most multi-national partners without prior approval from NIMA. Each type imagery has specific requirements (e.g., waivers are often given for EO imagery dissemination).

Collection

A variety of organic imagery collection capabilities is available to a MAGTF (see figure 5-5). The following planning considerations are critical to effective direction and employment of these resources.

General Imagery Collection Planning Considerations

Imagery collection resources have excellent capabilities to locate and identify major threat forces, moving vehicles, weapons systems, structures and other topographic features contrasting with their surroundings. Conversely, it can be difficult to locate small, stationary and/or well-camouflaged enemy forces blending in with their surroundings. Generally it is better to employ imagery collection resources against point targets, vice in a wide area search mode. Effective integration with other intelligence operations can cue imagery collectors against key targets, reducing the general search area and more rapidly producing useful intelligence. Some basic imagery collection planning considerations follow.

Area Reconnaissance Imagery Collection. Area reconnaissance is the systematic and complete coverage of an area using visual and/or imaging means. Area reconnaissance is normally conducted for locating and identifying potential targets for further analysis or in support of terrain analysis. Area reconnaissance imagery is accomplished in one of two ways:

- By imaging back and forth across a predetermined area in such a way that the flight lines and individual images overlap. This provides complete stereographic coverage of all objects within the area at the expense of increased sensor utilization time.
- By adjusting focal lengths and/or altitudes to allow a lesser number of images to cover the target area. This reduces TOT as well as the

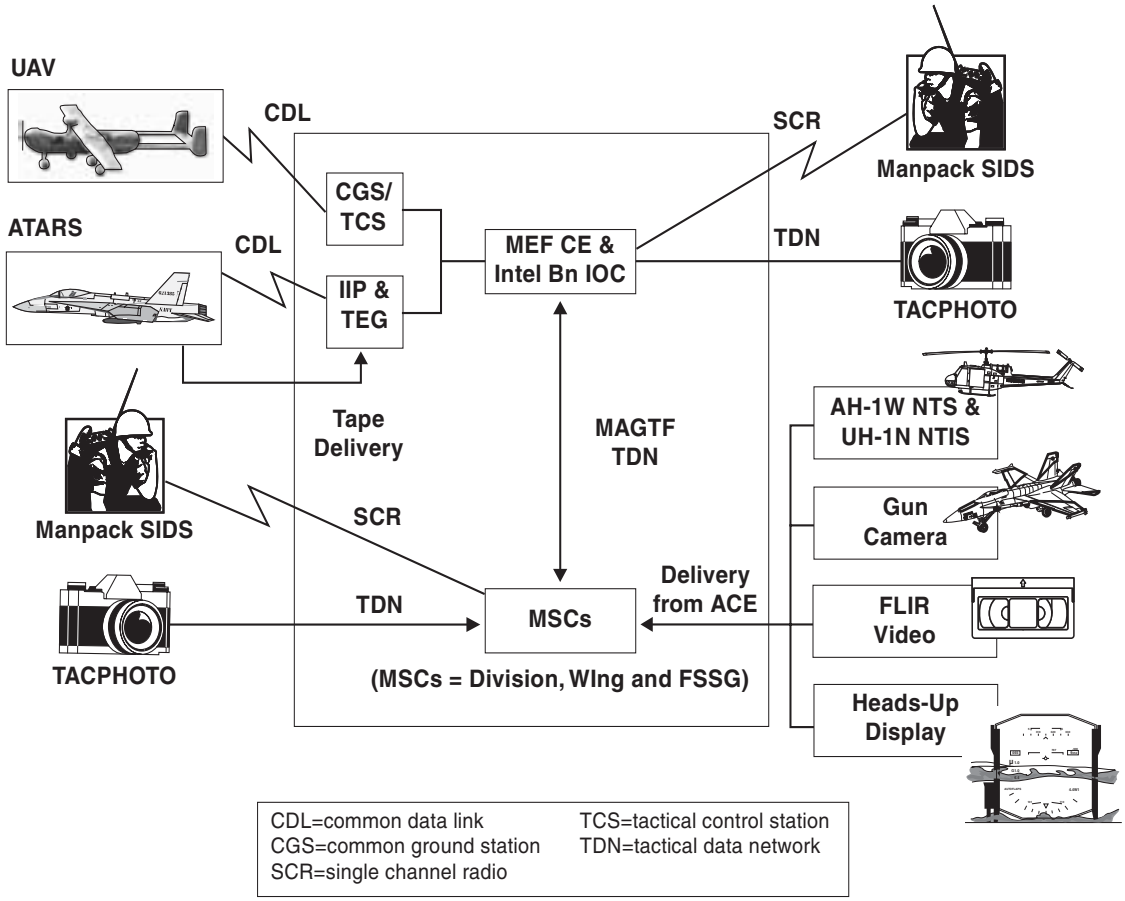


Figure 5-5. MEF Imagery Collection Capabilities.

processing, exploitation, and dissemination time at the expense of reduced resolution.

Types of area reconnaissance imagery missions include:

- BAC and BAS are area reconnaissance imagery collection tactics that are good for providing an overview of an entire area. During the early phases of an operation, these may be done for two intelligence purposes: providing a basis for the procurement of larger scale imagery of selected areas for subsequent detailed analysis; or to serve as a comparative baseline for determining the nature and extent of changes identified on subsequent missions. BAC and BAS should not be used to hunt for OOB information, as exploitation of these is very manpower and time intensive. During such area collection operations, the flight tracks (or routes) are planned and the image exposures adjusted so that each successive image will overlap the previous one.
- DSA missions provide focus and detail and are useful for OOB confirmation counts.

Point Reconnaissance Imagery Targets. Point reconnaissance imagery target (also called pinpoint reconnaissance) is a small area. While sizes may vary, at the tactical levels (e.g., MSE and below command echelons) this area is usually not larger than one kilometer by one kilometer, while at the MAGTF CE/operational level this area will generally be of 10 nautical

miles or less. Point reconnaissance missions are normally tasked to provide the highest resolution possible of a specific target to allow for detailed analysis. A command post, bridge, airfield or SAM site would be considered point targets.

Route Reconnaissance Imagery. Route reconnaissance imagery is simply imaging along specific transportation routes such as roads, railroads or waterways. This type of reconnaissance is normally conducted to determine enemy movement, to determine usability of the route, or in support of GEOINT mapping or terrain analysis requirements. This tactic is good for LOC and maneuverability studies, but generally requires significant time for effective exploitation. Route reconnaissance imagery missions should be done as a contingency baseline, ahead of time. This coverage is typically done by one or two collectors flying at a low altitude along a specified route.

Strip Search Reconnaissance Imagery. Strip search reconnaissance missions are similar to the route reconnaissance except that the collector will fly in a straight line from one point to another or along predetermined flight paths not necessarily related to transportation routes. This type of mission is frequently conducted using oblique or side-looking sensors to monitor activity across enemy lines or demilitarized zones, while allowing the aircraft to fly over friendly territory.

Aerial imagery collectors provide the flexibility to respond rapidly to changing battlespace conditions. UAVs offer the added advantage of operating in areas of heavier enemy air defenses and providing the needed intelligence without the risk of exposure of manned aircraft. Using the results of IPB and the MAGTF's concept of operations and scheme of maneuver, intelligence imagery collection planners will generally establish detailed preplanned imagery collection routes, areas, and point targets encompassing the AOI to streamline intelligence and operational planning.

In addition to the intelligence planning considerations, such missions require detailed operational planning, particularly regarding their integration with other ACE operations. As all aerial imagery collection platforms are multipurpose, close coordination between MAGTF CE imagery planners and ACE operational planners is necessary to identify, reconcile, prioritize, and integrate competing requirements for these resources. Additionally, all aerial imagery missions must be included on the ATO and coordinated with other air operations and, where pertinent, supporting arms. This is particularly critical regarding UAV operations. UAVs enter the airspace control system via the appropriate airspace control agency, normally the direct air support center (DASC). UAV controllers maintain communications with the appropriate ACE C2 agency (e.g., the DASC) during missions to receive routing, altitude, and other pertinent airspace control information.

The commander who directly tasks or controls an imagery collection mission will receive the most responsive support. The responsiveness of the mission to other commanders depends on the number of echelons through which the mission request and resulting intelligence must flow. Accordingly, when planning imagery collection operations, the advantages and disadvantages of dedicating missions to a single command (i.e., direct support) must be assessed against the MAGTF's total IRs and the current situation.

Previously acquired imagery and IMINT products should always be reviewed to see if they can satisfy IRs without need of additional imagery collection missions.

Often the intelligence acquired from an imagery collection mission (vice the actual image itself) will be all that is required to satisfy many IRs. Likewise, dissemination challenges are generally simpler and faster when users' IRs can be satisfied without the images. Accordingly, commanders must understand the pros and cons of various imagery-related IRs to ensure optimum support.

Usually collected imagery will require additional processing and fusing with other intelligence to provide the necessary support. Depending on the situation, this may be a time-intensive task. Commanders should assess likely processing and production times and other requirements when developing IMINT plans.

Intelligence acquired from a number of imagery collectors may be disseminated directly to users with minimal additional intelligence processing and all-source intelligence analysis. Supporting dissemination plans must ensure identification of the type products likely disseminated and, the technical requirements associated with these. In the case of resources such as the UAV or JSTARS, dissemination planning includes the establishment of dedicated communications links directly between the collector and the supported unit (e.g., by assigning a UAV RRS detachment with organic communications to the supported unit's command echelon).

Types of Imagery

Vertical Imagery. Vertical imagery coverage of a target is obtained by direct overhead photography (see figure 5-6). It provides imagery of a relatively constant scale. It also allows the imagery analyst to achieve optimum results from stereovision and to accomplish the most accurate measurements. Stereovision is the effect obtained when overlapping photographs are viewed with the aid of special optical equipment, enabling height and slope determinations, as well as other detail not visible to the naked eye. Figure 5-7, on page 5-14, is an example of a vertical image.

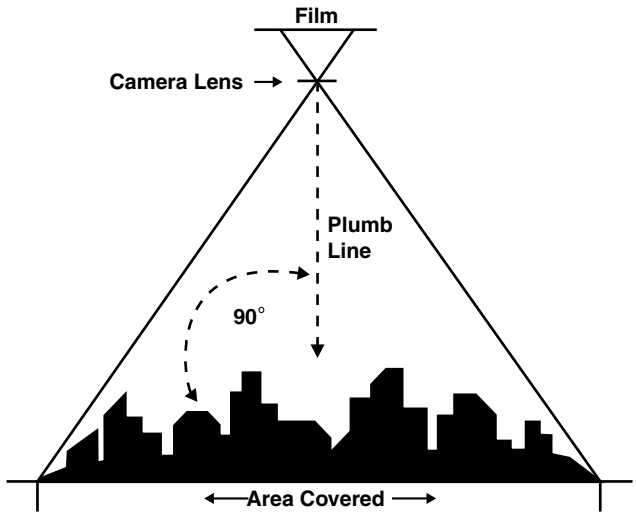


Figure 5-6. Vertical Imagery.

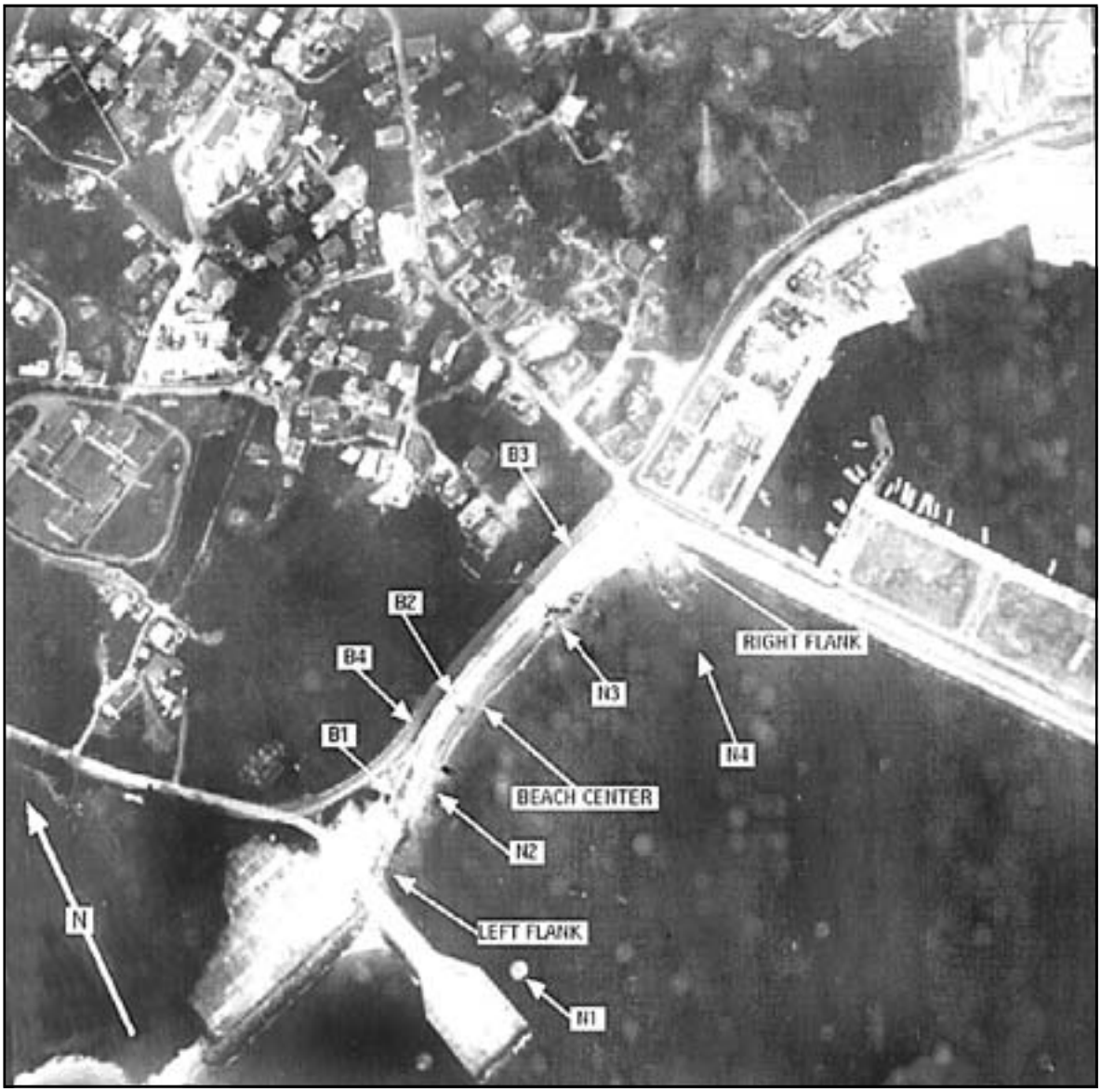


Figure 5-7. Vertical Imagery Example.

Oblique Imagery. Oblique imagery coverage is obtained by imagery taken at an angle from the vertical. High oblique imagery includes the horizon and has a large ground coverage (see figure 5-8); low oblique imagery does not include

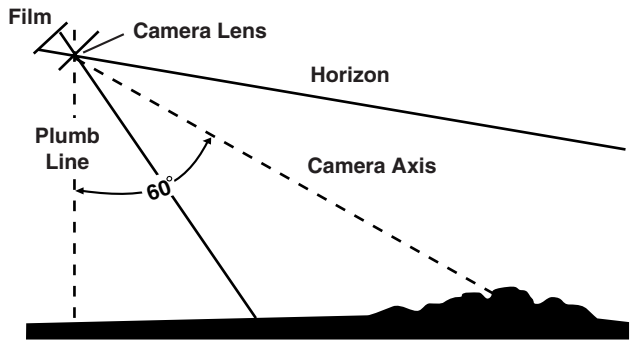


Figure 5-8. High Oblique Imagery.

the horizon and has a small ground coverage (see figure 5-9). Oblique imagery provides a representation of the target comparable to flying towards or parallel to it. It closely resembles a normal eye view and allows the imagery analyst to see into an area in a normal fashion. Measurements of oblique imagery are more difficult than with vertical imagery since the scale is not constant across the image, and precise subject distances cannot be determined. An operational advantage to such imagery, however, is the possible increased survivability it offers to manned and unmanned aircraft.

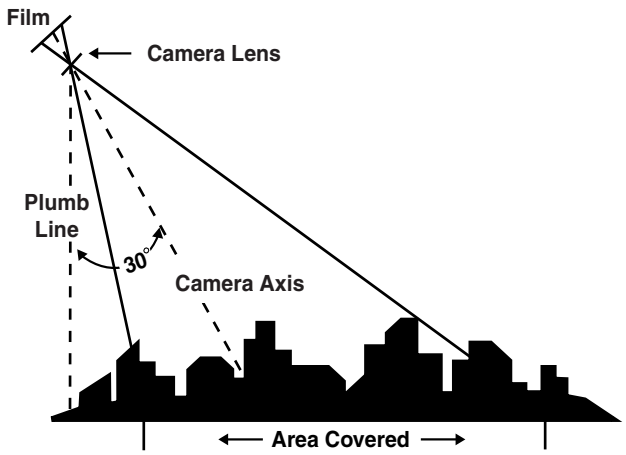


Figure 5-9. Low Oblique Imagery.

Panoramic Imagery. Panoramic imagery scans a wide area. Generally it is categorized according to the altitude at which the mission is flown and the angle of the scan. Low panoramic imagery is taken at low altitudes and scans a wide area, including the horizon on either side of the collector's flight line (see figure 5-10). High panoramic imagery is taken from higher altitudes with a smaller scan angle; generally the horizon is not visible on the image (see figures 5-11 and 5-12). This type of imagery can be useful when only one collection pass over the target area is possible as it provides coverage of

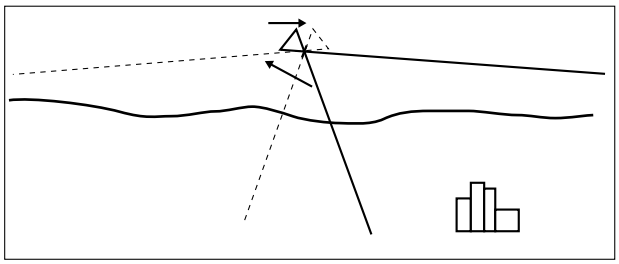


Figure 5-10. Low Panoramic Imagery.

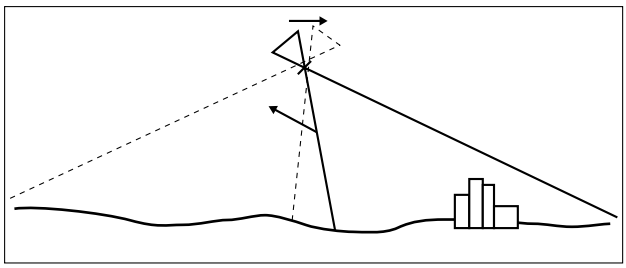


Figure 5-11. High Panoramic Imagery.

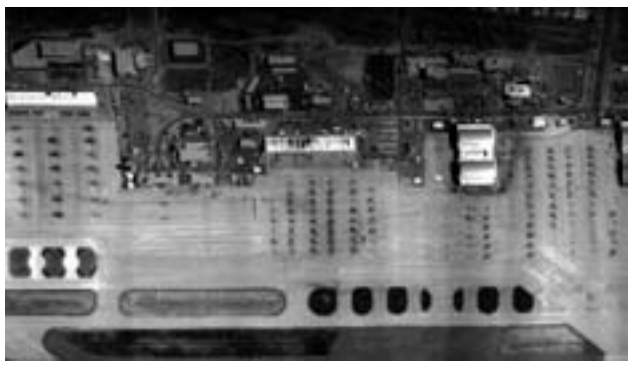


Figure 5-12. Panoramic Imagery Example.

large areas on both sides of the flight path. It is, however, more difficult and time-consuming to analyze and measure owing to the distortion of the recorded image.

Infrared Imagery. Infrared imagery is the remote sensing of a target's radiant temperatures. The system is used to measure the temperature differences between terrain features and surrounding objects on the ground, producing a near-optical quality infrared image (see figure 5-13).

Figure 5-13. Infrared Imagery Example.

These systems can operate during either day or night and under all weather conditions. However, they are less effective during day/night transition periods or when backgrounds and targets have the least difference in temperature. Also, infrared imagery uses temperature differential to generate the image so anything that degrades infrared transmission will impact the imagery.

Infrared imagery complements photographic imagery by day, and they are commonly used together. Unique infrared imagery capabilities include imaging the shadow on a heat-absorbing surface or the thermal scar of a heat-generating object (e.g., aircraft after it has moved).

Radar Imagery. As a radar can penetrate virtually all atmospheric conditions, radar imagery generally is limited only by the capability of the platforms conducting the collection mission. Radar operates on two principles: all materials reflect a portion of electromagnetic radiation; and electromagnetic energy is directed in a beam from the antenna to the target area. It is then reflected by the target back to the collecting platform. Variations in pattern and tone of the returned pulses are recorded and displayed as radar images. Figure 5-14 is an example of JSTARS SAR imagery. The geometry and surface composition of targets and their surroundings can greatly affect the intensity of the radar pulse return. To detect moving targets, radars employ the principle of doppler shift. Doppler shift is the result of a moving object causing a subtle change in the frequency of the reflected pulse energy. This change is detected by comparing the original pulse energy frequency to the frequency of the reflected energy. Advantages of radar imagery include its superb capabilities over great distances under a wide variety of conditions; it provides great operational flexibility, particularly during mid to higher intensity combat

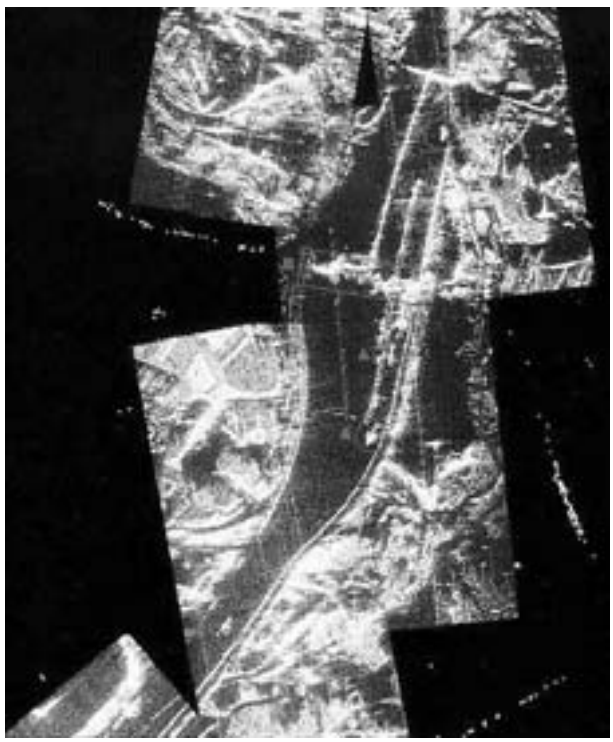


Figure 5-14. JSTARS Synthetic Aperature Radar Imagery Example.

operations; and it provides constant scale. However, radar imagery is not useful as a stand-alone intelligence product. Unlike optical imagery, it presents an abnormal view of the battlespace, requiring special skills and time to analyze properly. (See figure 5-15 for an example of an MTI image.)

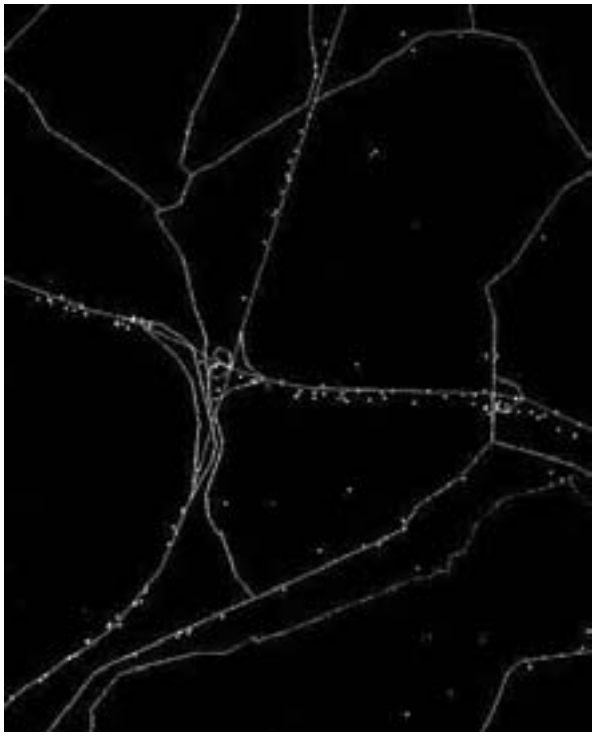


Figure 5-15. JSTARS Moving Target Indicator Imagery Example.

Electroptical Imagery. EO imagery employs digital imaging techniques to extend and complement other imagery. Advantages include the dynamic range of the sensor generally is greater than other types of imagery; it can penetrate atmospheric conditions that are opaque to other sensors; and, like radar imagery, EO imagery is readily exploitable by automated processors and analytical aids. EO uses the visual spectrum, so anything that impacts this (dust, smoke, haze, clouds, rain, fog, light level, angle of illumination, etc.) will affect the quality of the imagery.

Multispectral Imagery. Multispectral imagery (MSI) records views in a number of spectral bands or frequencies simultaneously, providing a wider range of processing and analytical techniques to be employed. The key to interpretation lies in identifying the spectral signatures of different surfaces and targets. Every surface or target gives off its own distinctive pattern of radiation, whether it is generated by itself or reflected. This will depend on its reflective qualities, its heat, whether it is a solid or liquid, how smooth its surface is, and many other factors. MSI usually has less resolution in the visible spectrum but can reveal details not apparent on the latter. This allows MSI the capability of providing map-like products to support area familiarization and orientation. Unlike other types of imagery, most MSI products are acquired from commercial sources. NIMA is responsible for purchasing, archiving, and disseminating MSI products for DOD.

Commercial Imagery. The commercial imagery industry is planning the launch of several new high resolution visible, MSI, and other imagery systems within the next 5 years. These systems will provide an increased capability to supplement and complement our national imagery technical collection. HQMC Imagery and Geospatial Plans and Policy works closely with NIMA on numerous commercial imagery issues. Marine Corps policies and procedures for requesting, tracking, obtaining, and purchasing commercial imagery are being developed and will be promulgated once NIMA's Commercial Imagery Management Office (CIMO) develops a commercial imagery plan to provide better DOD and intelligence community access to commercial imagery.

Domestic Imagery Collection. Domestic imagery collection is satellite and aerial imagery of any part of the US, its territories or its possessions, including the 12 nautical miles seaward of these land areas. A Proper Use Statement and approval are required before domestic imagery collection may be conducted. Central to this process is a thorough review of planned missions to ensure that the constitutional rights of US persons are protected in accordance with current laws and executive orders that restrict intelligence activities directed against US persons within the US. Once approval has been

obtained, proper use statements must be retained in the permanent files of the requesting unit and higher headquarters up through the combatant command headquarters. (See the NIMA Imagery Policy Series [section 9, part B], *Domestic Imagery* [IPS-001/98-S9A] for additional information on domestic imagery collection.) Request channels for domestic imagery collection are:

- **Marine Corps specific requirements.** Proper use statements are submitted via the service chain of command to HQMC Imagery and Geospatial Plans and Policy.
- **Joint operations requirements.** Proper use statements are submitted via the operational chain of command to combatant commander for adjudication or follow-on action as appropriate.

Aerial Imagery Collection Missions

Preplanned Missions. Preplanned aerial imagery missions (UAVs, ATARS, JSTARS) are requested using the joint tactical air reconnaissance/surveillance request (JTAR/SR) format (see appendix C, section I). Within the MAGTF, preplanned aerial imagery requests are routed through the intelligence chain and consolidated by the MAGTF CE's intelligence section for validation, prioritization, and follow-on planning and coordination. Once a decision is made to conduct an aerial imagery collection mission, the G-2/S-2 concurrently will: refine the JTAR/SR as required and submit it to the G-3/S-3 for follow-on planning and integration within the MAGTF and/or JTF ATO; and, plan and coordinate supporting intelligence production and dissemination plans. Key planning information included on JTAR/SRs are—

- Date-time factors: dates and time on targets desired and latest time desired intelligence will be of value (LTIOV).
- Type intelligence collection mission. (It is emphasized that the same request and planning process is used not only for aerial imagery collection missions, but also for aerial electronic intelligence/electronic warfare support missions and aerial visual reconnaissance missions.)
- Target, route or area coordinates.
- Target categories and associated PIR.
- Type intelligence products desired (i.e., reports and photos or reports only).
- Units to whom the resulting intelligence products will be disseminated.

The long lead time required for JTAR/SR submission needed by ACE operations planners is not often conducive to effective intelligence and IMINT planning. Therefore, effective standing operating procedures (SOPs) must be developed between G-2/S-2 and ATO planners to both meet air operations deadlines and strive to accommodate the intelligence planning aspects of rapidly changing situations. One method that may be used by intelligence planners is to initially provide ATO planners the most comprehensive JTAR/S request possible (i.e., specify desired aerial imagery platforms, type of imagery mission, targets, and anticipated IRs). At a designated time (i.e., no later than 6 hours prior to mission start), imagery planners will provide ATO and imagery collection units with the final detailed intelligence tasking information for each mission-detailed target point/route/area location information, specific IRs, and final C2, reporting criteria and CIS channels to be used.

Immediate Missions. Immediate requests for aerial imagery collection may be submitted directly to the DASC. However, as available resources are generally limited and operating in general support of MAGTF requirements, approval from the mission's controlling intelligence officer must be obtained prior to diverting an aerial imagery platform from a preplanned mission.

The joint tactical air strike request format shown in appendix C, section II, may be used to request immediate aerial imagery collection support. If approved, the mission may be executed in one of the following ways:

- An ongoing mission can be diverted by its controlling authority to conduct the immediate mission.
- An on-call/standby mission may be allocated.

Air Planning and the Air Tasking Cycle. Whether for preplanned or immediate air missions, the air tasking cycle is the key tool used by MAGTF planners to most effectively plan air operations to support mission accomplishment. It is an integral part of the MAGTF planning process. By using and completing the tasking cycle, planners can ensure that limited aviation assets are used to achieve their maximum effect with correct prioritization, C2 and CIS in support of the MAGTF's main and other key efforts. The principal planning product of the air tasking cycle is the MAGTF ATO or air plan. The six phases of the ATO cycle are command aviation guidance, target/air support mission development, allocation and allotment, tasking, force execution, and combat assessment (see figure 5-16).

The ATO is a document generated by the JFACC or the ACE commander. It tasks and disseminates to JTF components, subordinate units, and C2 agencies the specific missions and targets of projected air sorties, capabilities, and forces. It normally provides both general instructions and specific instructions, including call signs, targets, and controlling agencies. The airspace control order is included in the ATO. Special instructions, providing amplifying notes, important details, and changes are included in the ATO or issued separately. The ATO, airspace control order, and special instructions provide operational and tactical direction at appropriate levels of detail.

Each ATO covers a 24-hour period. There are usually three ATOs at any given time:

- The ATO in execution (today's plan), monitored by the ACE current operations staff.
- The ATO in production (tomorrow's plan).
- The ATO in planning (the following day's plan) by the ACE future operations planners.

Because input to the joint ATO must be provided 3 to 4 days in advance, the ATO can represent only a starting point for daily MAGTF flight operations. It is impractical to predict every need in advance. The MAGTF commander must have the flexibility to launch or to divert any aircraft as necessary to complete the mission, even if this requires short-notice deviations from the ATO.

In accordance with maneuver warfare, the ATO must be flexible enough to change with the needs of the force as the situation changes. It is not a

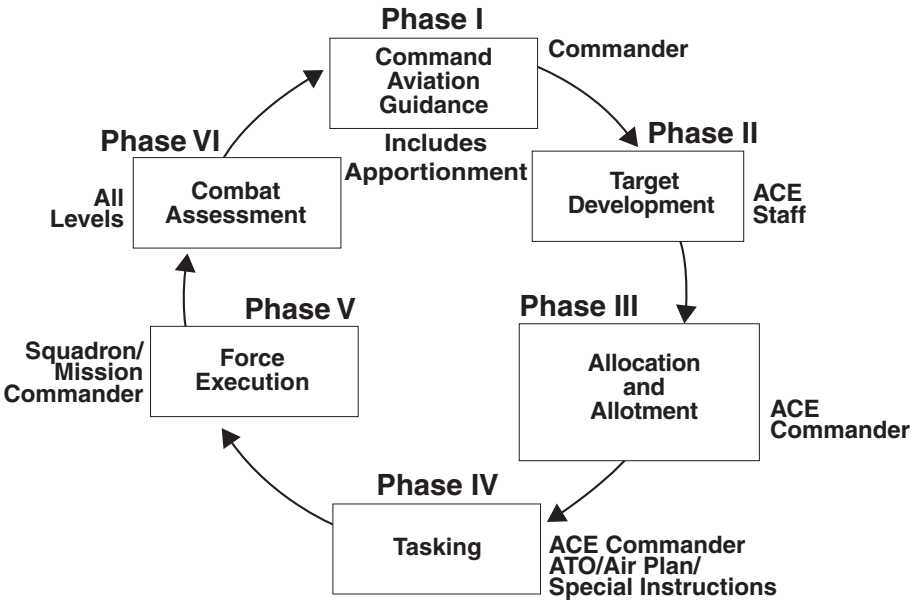


Figure 5-16. The Six-Phase Aviation Tasking Cycle.

rigid constraint on operational flexibility. Because the ATO represents a great deal of necessary coordination and deconfliction of air assets and airspace, however, necessary deviations from the ATO should be well-justified and relevant. Headquarters should be informed as quickly and as fully as possible. The process by which changes are made to the ATO is directed by the JFC.

During purely Navy/Marine Corps operations afloat, there may be no ATO as such. All squadron flight schedules are consolidated with the needs of the MAGTF/ship/amphibious ready group (ARG)/carrier battle group (CVBG) at an air board. The air board meets every day in the supporting arms coordination center (SACC). It works on current and future plans for air support. The results are published as the ship/ARG/CVBG air plan. The air board also provides the input for the joint ATO. Generally the MAGTF intelligence section will have a representative from its future plans section or intel bn's CMD section at all air board meetings to coordinate aerial imagery and other air intelligence mission needs.

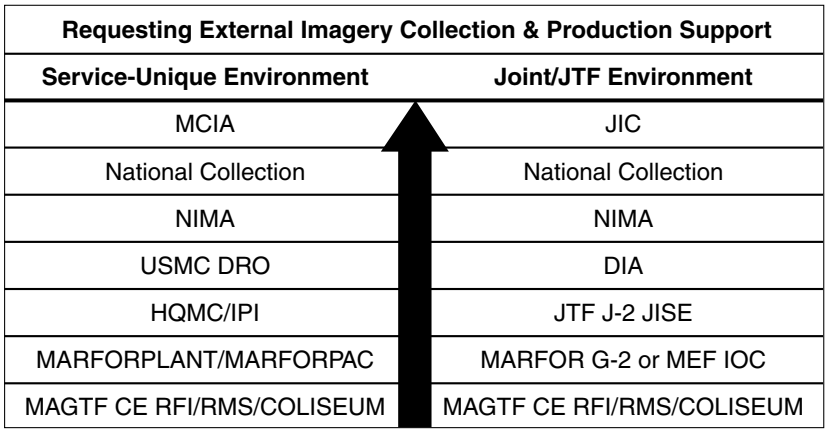
Not every mission on squadron flight schedules and air plans will appear on the joint ATO. Flights that are within the MAGTF's airspace and made in support of the MAGTF; e.g., not in support of the JTF, may or may not be included in the joint ATO. Such flights are mostly helicopter flights and functional check flights. Such flights may include tactical missions generated to respond to the changing battlespace situations. Often, ships (particularly aircraft carriers) may operate outside of the JTF's airspace entirely. In such cases, missions that do not enter JTF airspace will not appear on the joint ATO. Nonetheless, every mission that is submitted and approved for the joint ATO must appear on squadron flight schedules and the MAGTF/ship/ARG/CVBG air plan.

Requesting JTF, Theater and National Imagery Support. Significant imagery and IMINT support is available to the MAGTF from external sources ranging from dissemination of existing imagery and products through the integration of existing information into new products and execution of new imagery collection and IMINT production. MAGTF IRs that cannot be satisfied via organic resources will be submitted to the next higher command echelon for validation, prioritization and, if possible, satisfying the request for intelligence or collection requirements through its organic resources before forwarding it to the next higher command echelon. The specific IR will determine how the requirement is identified and submitted. Techniques range from use of the standard request for information format, using the RMS resources and procedures (for new imagery collection requirements) or using COLISEUM resources and procedures (for IMINT or all-source production requirements). Figure 5-17 identifies the two different tracks external imagery and IMINT requirements may take.

Processing and Exploitation

Processing and exploitation involve the conversion of collected data into information that is suitable for the production of intelligence. Processing is largely a technical function that does not add meaning to the data, but instead is necessary to convert the data into a form that commanders and planners can understand (e.g., developing a piece of film into a usable image). Some types of data require minimal processing—they may be collected in a form that is already suitable for production. Other types of data require extensive processing to incorporate amplifying data not available on the raw image products, affecting the timeliness and accuracy of the resulting information.

The degree of automated processing resident in IMINT resources varies. For example, the video downlink from a UAV can provide the geographical coordinates of acquired targets—but only to select C2 nodes. Likewise, the JSTARS CGS is capable of automatically processing, storing, and displaying acquired MTI, FTI, and SAR imagery. Usually acquired imagery requires additional processing and exploitation before it is usable. This processing and



Requests for national-level imagery collection and IMINT production take one of two tracks: via peacetime service-unique channels (e.g., exercises, planning); or via joint/operational channels for actual operations.

Figure 5-17. Requesting External Imagery and IMINT Support.

exploitation of imagery data into IMINT is accomplished by the IIP or MCIA imagery analysts or by CGS personnel. They refine raw imagery into clear and usable imagery products by using manipulation tools available at their workstations (e.g., annotation of images, immediate identification of key pieces of threat equipment, measurement of a structure's dimensions). Situational factors and standing IRs will be assessed to determine to what degree such products may be immediately disseminated or whether additional intelligence analysis is required.

Production

Production is the activity that converts information into intelligence. It fuses new information and existing intelligence from all sources to provide meaningful knowledge that can be used for decisionmaking. Production involves the evaluation, interpretation, integration, analysis, and synthesis of all information that is relevant to a particular IR to answer the question(s) that have been asked.

The results of exploited and analyzed imagery and imagery data form the basis for IMINT reports and derived products provided to the G-2/S-2 for the further production and analysis of all-source intelligence, directly to tactical commanders and to other users. User needs will rarely be fully satisfied simply via uninterpreted image prints. Instead, IMINT production planning and management will be closely coordinated with all-source intelligence production management and planning to determine the scope, content, and format for each product; to plan and schedule the development of products; to assign priorities among the various IMINT product requirements; to determine who needs what products and in what quantities; to allocate IMINT processing, exploitation, and production resources; and to coordinate production efforts with IMINT and all-source collection and dissemination activities. The goal is effective and efficient use of limited resources while ensuring that IMINT production is focused on validated PIRs and IRs and associated specified intelligence reporting criteria.

IMINT production can range from the preparation of highly sophisticated multimedia products to the selection of suitable imagery forms for either stand-alone use or for integration and fusing within all-source intelligence products.

A wide variety of IMINT products may be developed, either as stand-alone, single source products or as part of all-source intelligence products: annotated prints, mosaics, oblique panoramas, supporting detailed IMINT, and all-source intelligence text reports.

Imagery Graphic Products

Imagery graphic products of objective areas (target areas, beaches, helicopter landing zones, etc.) are useful for a variety of planning and decision-making activities. Such products include:

- **Photographic prints.** A photographic print represents a single frame of imagery from a mission. Photographs often portray an idea more rapidly and concisely than words. For this reason, prints can provide a picture of significant items of interest to users in addition to any written reports. Prints will usually be annotated in some fashion to emphasize significant military information. Minimum annotations usually will be a titling strip, to include a grid reference or geographic coordinates for the illustrated target(s) and the date-time-group of the imagery, and a north arrow or other orientation aid to help with orienting the print to a map. Other annotations may include target categories and descriptions.
- **Mosaics.** A photographic mosaic is a combination of two or more overlapping prints that form a single picture. Mosaics can be of significant value in providing an updated picture of a large area to supplement map data. Usually vertical photographs are used and produce "map-like" results, but oblique photographs may be used to produce a panorama. Mosaics supplement map data and text intelligence reports by displaying current information on roads, trails, built-up areas, and the conditions of terrain and vegetation.

IMINT Text Products

Commander's timeliness requirements will drive the type and preparation of each of the below IMINT text products. (Appendix F provides the formats and instructions for the following IMINT reports).

- **Reconnaissance Exploitation Report (RECCEXREP).** The RECCEXREP is used to report the results from the first rapid analysis of imagery, to include the debriefing of the aircrew when possible. It addresses those targets requested in the original imagery collection mission tasking, normally with each target addressed separately. It is prepared by the IIP (with input from the supporting collecting unit's intelligence section) and disseminated in accordance with the dissemination plan. The specified time limit in which the RECCEXREP must be completed and disseminated will be per unit SOP.
- **Initial Photographic Interpretation Report (IPIR).** The IPIR provides information on tasked imagery collection missions not previously reported (e.g., in the RECCEXREP) when extensive or detailed data from a systematic review of the imagery is required or if the rapid response required by the RECCEXREP would be hindered by the format, size or quality of the imagery involved. It also is prepared by the IIP (with input from the supporting collecting unit's intelligence section) and disseminated in accordance with the dissemination plan. The specified time limit in which the IPIR must be completed and disseminated will be per unit SOP.
- **Supplemental Photographic Interpretation Report (SUPIR).** The SUPIR provides information not previously included in a RECCEXREP or IPIR. It reports on significant targets covered by the mission and other required supplemental data. It is prepared by the IIP (with input from the supporting collecting unit's intelligence section) and disseminated in accordance with the dissemination plan. Generally, the unit SOP specifies the time limit for completing and disseminating the SUPIR.
- **SALUTE Report.** The standard SALUTE (size, activity, location, unit, time, equipment) report is used to report any known or suspected enemy activity. It may also report any characteristics of the area of operations that affect mission accomplishment. The SALUTE report

may be used by UAV squadron, ground reconnaissance, aircrew or other personnel to report key information obtained during ongoing imagery collection operations. It will be disseminated in accordance with the dissemination plan—generally from the collector to the SARC or directly from the collector to other supported units.

IMINT Support to Other All-Source Intelligence Products

Imagery alone will provide useful intelligence to commanders and planners. See appendix G for detailed information regarding imagery and IMINT support to IPB and other all-source intelligence products.

Usually IRs will be satisfied more effectively and in greater detail via the complementary combination of an image and supporting IMINT or all-source intelligence products. Review appendix H for an appreciation of the greater intelligence value of a complementary imagery/intelligence report product, vice simply an image product.

Photogrammetry

Photogrammetry includes the precise measurement and computation required in imagery analysis. Measurements of objects/targets as they appear on imagery can be used to compute lengths, widths, heights, and imagery scale. Depending upon the IR, the photogrammetric process can be difficult and time-consuming. Vertical images are relatively straightforward and quick to measure, but oblique and panaoramic images will require greater effort, which can degrade timeliness requirements (particularly at tactical levels). Photogrammetry provides information on—

- Vehicle and equipment dimensions as an aid for identification and for technical analysis.
- Building, storage and other facilities, as well as installations' sizes and capacities.
- Bridges, roads, and other LOCs dimensions and compositions.
- Image scales.
- Speed and the direction of movement of targets and other objects.
- Targeting and weaponeering.

Target Analysis

Generally the imagery analyst's first responsibility is the detection and accurate identification of areas and activities for situation development and support to targeting.

Target detection begins with one of two search modes: general and specific. General search is undertaken in response to requests for broad area intelligence and usually involves the analytical examination of the entire image. Such searches should be kept to a minimum. Specific search is undertaken in response to an IR that requires point, strip or route reconnaissance imagery. Its scope and objectives are more limited than general search.

Target identification consists of the interpretation of visual cues or distinctive features of targets/objects detected during collection. The distinctive features are analyzed using the six Ss: size, shape, shadow, shade, surroundings, and signal strength. The depth and scope of the analysis is highly dependent upon the purpose of the analysis and the associated IR time constraints. Target identification may include:

- Determining the OOB and battle damage assessments of threat units and systems at different echelons.
- Identifying both equipment and its intended use by the threat forces.
- Determining the purpose and composition of ports, harbors, waterways, airfields, roadways, railways, and installations.
- Detecting and identifying nonthreat forces and equipment and sensitive targets (e.g., religious facilities).

See appendix I for information on target folders and IMINT support to these.

Exploitation

Satisfying many IRs will require greater imagery exploitation. Such situations include functional analysis of an object, equipment or environmental analysis; previously unknown objects, equipment or modifications, and activities; unusual concentrations of military or nonmilitary personnel or objects; etc.

National Imagery Interpretation Rating Scale

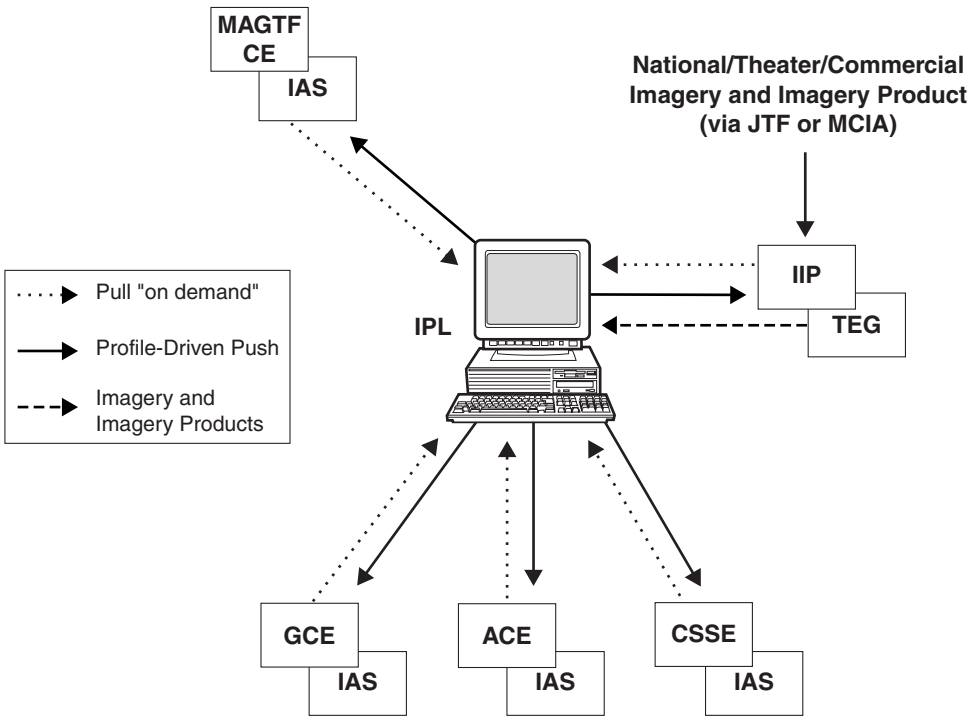
National imagery interpretation rating scale (NIIRS) is used by collection managers as an aid to the identification of the quality of imagery needed to satisfy their IRs. Additionally, imagery analysts use NIIRS to rate the quality and interpretability of acquired imagery. (See appendix B for the visible, infrared, radar, multispectral, and civil NIIRS.)

Imagery Databases

In addition to the development of these products, production also entails the indexing, maintenance, and administration of imagery and IMINT product databases as an aid to future IMINT activities. Imagery analysts must ensure that acquired imagery is incorporated into the MAGTF IPL (see figure 5-18). Generally the IPL will include images in reduced resolution format reviewed by intelligence personnel and other users throughout the MAGTF. Those full-resolution images that meet their IRs can then be downloaded and disseminated.

Dissemination and Reporting

IMINT dissemination planning and management involves establishing dissemination priorities, stipulating dissemination and reporting criteria, selecting



Major subordinate commands (MSCs) down to the regiment/group level will have IPLs with which to store imagery and imagery products and access the Imagery Library Network. IPLs will be populated on the basis of demand-driven "pull" and user-developed profiles ("push").

Figure 5-18. MAGTF Image Product Library.

dissemination means, and monitoring the flow of IMINT reporting. The goal is to deliver IMINT products to the appropriate user in the proper form and at the right time, while concurrently preventing the dissemination of irrelevant products and avoiding information overload. The following paragraphs address the most common considerations for intelligence dissemination planners in developing IMINT dissemination plans.

Identify Dissemination Requirements

When identifying requirements, the four Ws—the who, where, what, and when questions—are a good start for identifying the broad scope of dissemination needs.

The Whos. Commander preferences, standing theater OPLAN/concept plans (CONPLANs), type mission analyses, unit SOPs, TTPs, playbooks, and previous postexercise analyses and lesson learned reports are all key sources for identifying organizations, units, and other elements that the intelligence section must disseminate imagery and IMINT. Identifying and grouping by common imagery and IMINT product requirements by typical command relationship/task organization provide the operational perspective to begin dissemination planning.

- **Internal MEF/MAGTF Headquarters.** Current operations center, future operations center, tactical command echelon (when deployed), force fires coordination center, rear area operations center (when established), civil-military operations center (when established).
- **Subordinate Elements and Unit.** Intelligence sections of the GCE, ACE, and CSSE; other MAGTFs and independent task forces; organic/attached/direct support intelligence and reconnaissance units for whom the MEF retains operational control (via either the SARC, other G-2 sections, direct support teams, and/or direct to the intelligence/reconnaissance units' command posts); and other C2 nodes and facilities, when required (e.g., DASC, enemy prisoners of war compound, rear area operations center, airfield arrival control group).

The Wheres. Usually this will correspond to the location of each identified "who." However, command relationships, the specific operational phase, task organization or other factors may identify other answers to "where" dissemination requirements.

The Whats. With the above information in hand, dissemination planners now seek answers to the "what" of each requirement. Here planners strive to establish or anticipate what type intelligence support—finished intelligence, particular formats—each "who" typically requires to supporting its planning and decisionmaking needs. As with the "who" determinations, commander preferences, standing theater OPLAN/CONPLANs, type mission analyses, unit SOPs, TTPs, and playbooks, and previous post-exercise analyses and lesson learned reports all are key sources for isolating "what" needs and will provide the dissemination SOP foundation. Additionally, planners' research should encompass how differing intelligence resource task organizations affect what requirements and to how the possible "whats" historically have been combined to satisfy the "whos" requirements. Cross-referencing the "who" and "what" answers with the following groupings completes this step:

- Typical stand-alone imagery and IMINT products; and IMINT support to all-source intelligence products.
- Alarm intelligence support (e.g., I&W reports, time-sensitive target of opportunity reporting).
- Preferred level(s) of classified information that the who desires (further subdivided into what they require access to and what they can actually retain on hand).

The Whens. The final dissemination planning information requirement is to determine each "whos" typical or stated "whens". The same sources used to research the previous Ws likewise are recommended for acquiring initial when

answers and baseline planning criteria. However, this factor is arguably the most variable during tactical operations. Key planning considerations include:

- Nature of the requirement (e.g., is it a PIR or in support of another functional information requirement).
- Rapidly assessing the feasibility of satisfying the decisionmaker's or planner's stated LTIOVs (Is intelligence already on-hand? Can organic assets acquire or produce needed intelligence? Will external support be needed?).
- Communications and networks transmission requirements for the who's desired format (voice, text, digital, bulk delivery, etc.)
- Capabilities/current status of MAGTF CIS.

Develop Dissemination Plan

The answers to the four Ws can now be translated into an IMINT dissemination plan. IMINT personnel must maintain close coordination with all G-2/S-2 officers, G-3/S-3 planners, and pertinent intelligence personnel at higher, adjacent, supporting, and subordinate organizations.

Design and Coordinate Architecture. The architecture should be designed schematically so that it depicts organizations, type intelligence systems, and CIS connectivity among the forces' (MAGTF, joint, naval) intelligence collectors/producers and the supported decisionmakers/planners. Since planned architectures must incorporate sufficient flexibility to adjust quickly to changing tactical circumstances, it must depict both primary and alternate pipeline and alarm channels and the demand-pull and supply-push methodologies.

The large data communications bandwidths associated with much imagery dissemination requires close planning and coordination between MAGTF intelligence and CIS planners (see figure 5-19). Also, see appendix J for additional technical information on national imagery transmission format (NITF) compression that is useful when designing and coordinating CIS support to IMINT dissemination.

Establish IMINT Dissemination Procedures. Comprehensive, MAGTF-wide integrated operations/CIS/intelligence procedures are mandatory if intelligence dissemination is to be effective. Answers to the four Ws will provide the initial foundation for development of a MEF's intelligence dissemination architecture and operations. General dissemination procedures should be established for the delivery of IMINT and imagery from the controlling producers or agencies to designated recipients. The precedence of transmission—ranging from routine to flash—should be agreed upon by all involved parties in advance. Audiences should be predetermined as well by defining broadcast parameters (e.g., general or specific). Further, irrelevant intelligence can be better eliminated if reporting regimes, thresholds, and filters are identified early.

Allocate or Obtain Resources. The intelligence officer, in concert with the unit's CIS officer and G-3/S-3, should allocate available resources to accommodate dissemination of the requested IMINT. If resources do not exist to transmit the required information, a request for augmentation from higher headquarters or assistance from lateral units should be initiated immediately. Often it may be necessary to arrange for the delivery of intelligence directly from the producer to the requester if means are in place.

Coordinate. Once IMINT requirements have been identified and the initial plans developed, planners will develop and coordinate detailed dissemination plans. Key considerations include:

- Close coordination among MAGTF CE IMINT, ACE intelligence, and imagery collection units' planners to ensure planned imagery collection missions, specific IRs, routes, and reporting criteria reflect ongoing developments.

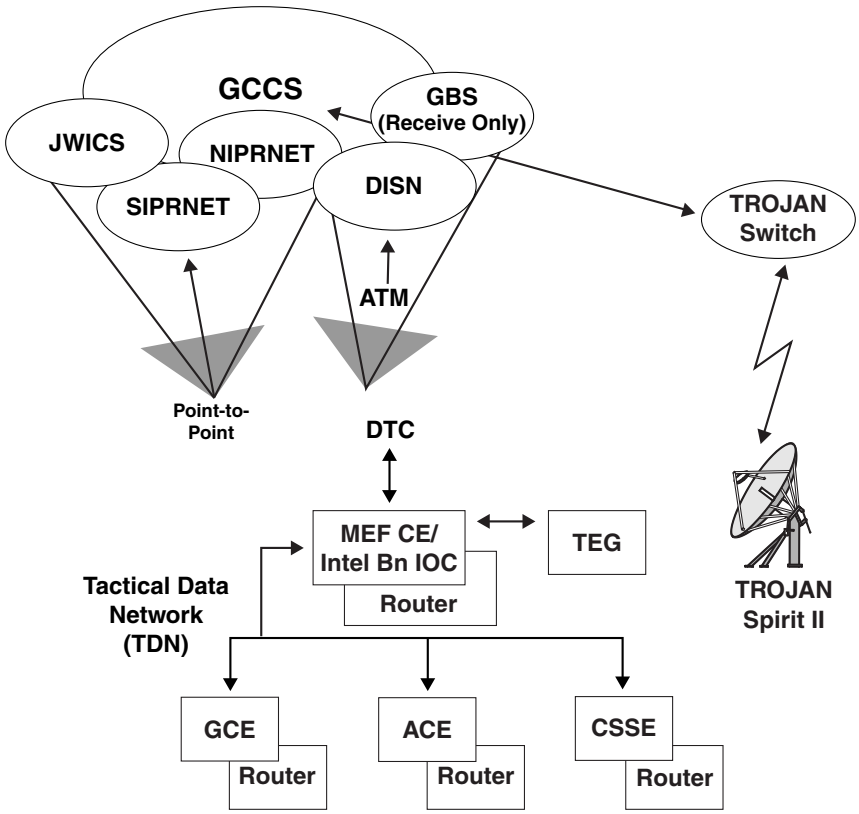


Figure 5-19. Key CIS Pathways for Imagery Dissemination.

- Close coordination between MAGTF CE IMINT planners and subordinate units' intelligence personnel to ensure that they are cognizant of planned imagery collection missions. In addition to voice and e-mail coordination, a useful technique for keeping everyone apprised of planned imagery missions is by including in MAGTF intelligence summaries a detailed paragraph describing specific planned imagery collection missions and associated priorities, collection times, targets, routes, IRs, and primary and alternate reporting channels.

Monitor Execution. Once imagery or IMINT products have begun to be disseminated to the requester, it is important to constantly evaluate the flow of information to determine if the user is satisfied with the quantity and quality of intelligence; and, to ensure that preplanned filters are eliminating circular reporting. Frequent checks with the requester can ensure intelligence utilization and preclude unanticipated demands on the G-2/S-2 staff.

IMINT Utilization

The specific utilization of IMINT is based upon the concept of operations and the imagery application being employed. Commanders, G-2/S-2s, and G-3/S-3s must continuously evaluate IMINT products and reports for timeliness, usefulness, overall quality and responsiveness to stated PIR and IRs, and provide feedback to the MAGTF G-2/S-2 and IMINT planners to improve future IMINT operations. Ultimately, IMINT utilization will provide guidance and determine requirements to support ongoing IR management and supporting IMINT operations.

IMINT Operations Appendix

Guidance for the conduct of IMINT operations comes from many sources. DIA and NIMA issue policies, direction, guidance, and instructions on compliance with national IMINT standards, architectures, and request procedures.

Since MAGTFs will normally be part of a JTF or naval expeditionary force, reference to pertinent combatant, joint force, and fleet commanders' orders, guidance, and IMINT TTPs are necessary to identify unique operating concepts, methodologies, support procedures, and formats. Marine IMINT plans and orders are prepared by the G-2/S-2 (under the staff lead of the ISC and with the assistance of the other G-2 section and intel bn staff officers and commanders) and the COs/OICs of the supporting IMINT units. MAGTF IMINT plans and orders appear as appendix 7 to the intelligence annex of the MAGTF operation plan or order and will focus on internal MAGTF IMINT requirements, operations, and TTP.

Appendix 7 (Imagery Intelligence) to annex B (Intelligence) to an OPLAN or OPORD will provide detailed planning and direction for the conduct of MAGTF IMINT operations. The ISC is responsible for its development. It will be prepared consistent with format outlined in the JOPES, tailored as necessary consistent with the situation and the MAGTF's needs. (See appendix K for a sample IMINT operations appendix format.) The IMINT operations appendix should include friendly IMINT forces to be used, including:

- Personnel augmentation requirements.
- IMINT units of adjacent or other theater forces and support expected.
- Joint force maritime component commander (JFMCC), naval task force and/or amphibious force IMINT elements that provide support to the LF in amphibious operations.
- Pertinent IMINT capabilities and support from the JTF headquarters, combatant command's JIC/JAC, and other component commanders/task forces within JTF operations.
- Planned arrangement and employment of external IMINT support, including special collection, production, dissemination, and CIS.
- Establishment of coordinating instructions for the planning and control of IMINT operations to include the technical support expected from higher headquarters.
- Tasking of MAGTF IMINT elements.
- IMINT production, priorities, and plans.
- IMINT dissemination priorities and plans, to include CIS support to the MAGTF IMINT effort.
- IMINT unique equipment/logistics requirements.

IMINT Plans within Other Portions of Annex B

In addition to appendix 7, there are other portions of annex B that IMINT provides critical contributions or that provide critical operational and intelligence integration plans pertinent to IMINT operations.

Appendix 11 (Intelligence Estimate)

Once a basic understanding of the mission, AO, threat and other pertinent matters is known, it is necessary to view the situation through the adversary's eyes and provide this intelligence assessment to all MAGTF commanders and planners. The intelligence estimate is the principal comprehensive intelligence product that does this. The intelligence estimate seeks to accomplish a number of critical tasks: to state conditions of the area of operations that exist and indicate the effect of these conditions on enemy capabilities and the assigned mission, and assess the estimated effects of these conditions on both enemy and friendly capabilities and operations; to provide basic and current intelligence on threat forces compositions, organizations, strengths, dispositions, locations, activities, C2, logistics, and equipment; to provide an assessment of each en-

emy capability (attack, defend, delay, reinforce, withdraw), to include strengths and vulnerabilities, indicators that point to possible adoption of the capability, and estimates of the effects the enemy's adoption of each capability will have on the accomplishment of the MAGTF's mission; and, finally, intelligence conclusions of the likelihood of each capability being adopted by the enemy (generally listed from the most to least probable) and its associated center of gravity and vulnerabilities and estimated exploitability of these by the MAGTF. The intelligence estimate is an all-source intelligence product that will contain substantial input from IMINT and usually supported by extensive imagery. Additionally, it is where the following intelligence studies will be found, each requiring substantial IMINT and imagery support:

- Tab A, Tactical Study of Terrain.
- Tab B, Beach Studies.
- Tab D, Airfield Studies.
- Tab E, HLZs, and Drop Zones Studies.
- Tab F, Port Studies.
- Tab G, Lines of Communications Studies.
- Tab H, Order of Battle Study.
- Tab I, Survival, Evasion, Resistance, and Escape Safe Areas.

The intelligence estimate and supporting studies will be updated periodically (or new ones developed) throughout an operation, generally through all-source intelligence reports and summaries (again, each will usually have substantial input from IMINT and supporting imagery). The intel bn commander/ISC, through the commander's P&A cell OIC, is responsible for the analysis underlying and preparation of the intelligence estimate and subsequent reports.

Appendix 14 (Reconnaissance and Surveillance Plan)

The reconnaissance and surveillance (R&S) plan is a key tool developed to coordinate and integrate MAGTF R&S operations. Specifically, it provides guidance and orders for establishing and conducting ground reconnaissance, aerial reconnaissance, UAV operations, and remote sensor operations. The R&S plan will generally be developed by the SARC OIC, under the supervision of the intel bn commander/ISC and the CMDO, with the assistance of senior IMINT and R&S planners from force reconnaissance company, UAV squadron, and the ground sensor platoon (GSP). In particular, the following two tabs to the R&S plan appendix require extensive support from IMINT planners.

Tab C, Unmanned Aerial Vehicle Plan

This tab provides detailed intelligence orders, guidance and instructions for MAGTF UAV operations. Responsibility for its development rests with the SARC OIC, assisted by UAV squadron and imagery planners. Its specific content and formats will be mission and situation dependent. It will include information on UAV sortie routine and surge capabilities; preplanned point, route, strip, and area reconnaissance missions; UAV squadron C2 nodes locations; allocation and capabilities of squadron elements (e.g., RRS team assignments and missions); and other similar information. Although it may include tentative planning information on specific PIR and IRs supported as well as type imagery desired, usually this information will be too perishable; instead, when developed it will be incorporated in subsequent specific intelligence mission orders. (See appendix L for a recommended format for a MAGTF UAV plan.)

Tab D, Aerial Imagery Plan

This tab provides detailed intelligence orders, guidance, and instructions for the conduct of MAGTF aerial imagery operations. Responsibility for its development rests with the SARC OIC, assisted by imagery planners. Its specific content and formats will be mission and situation dependent. Generally it will include information on ACE imagery capable aircraft and systems capabilities and sortie routine and surge capabilities; preplanned point, route, strip and area reconnaissance missions; key C2

nodes locations; allocation and capabilities of squadron elements; and other similar information. Although it may include tentative planning information on specific PIR and IRs supported as well as type imagery desired, usually this information will be too perishable. When developed it will be incorporated in subsequent specific intelligence mission orders. (See appendix M for a recommended format for a MAGTF aerial imagery plan.)

Appendix 16 (Intelligence Operations Plan)

This appendix may be developed depending upon the complexity and scope of MAGTF operations and supporting intelligence operations (to include IMINT). It will provide additional guidance not already covered in SOPs for planning and direction of all-source intelligence and CI operations; and for intelligence C2, C2 nodes and facilities, and supporting CIS. It will also identify priority and unique requirements and procedures for the integration of MAGTF intelligence operations with MAGTF C2, maneuver, fires, logistics, and force protection operations; and the integration and interoperability of MAGTF intelligence operations with naval, JTF, theater, national and non-US intelligence operations. The following separate tabs may be included.

Tab A, Intelligence Collections Plan

Provide guidance for executing and managing collection activities not otherwise covered by regulation or SOP, including reconnaissance operations, equipment status, reports, unique intelligence disciplines requirements, and other specialized forms of collection activity to support the plan. Provide guidance on both routine and time-sensitive reporting of collected intelligence information by all collection sources to be employed in support of the plan.

Tab B, Intelligence Production Plan

Identify the intelligence production objectives and effort, including any intelligence and CI products, required to support the OPLAN. Include details of management of intelligence production requirements along with guidance on intelligence production and data bases, forms/formats for intelligence products, production schedules, intelligence products and reports distribution, etc. Include as appropriate requirements and guidance for the following: I&W, support to targeting, combat assessment (to include BDAs), and force protection.

Tab C, Intelligence Dissemination Plan

Stipulate the requirements, means, and formats for disseminating intelligence reports and products (e.g., units responsible for each, periods covered, distribution, timelines standards). Establish the supporting intelligence communications and information systems plan and the supporting procedures and criteria to satisfy expanded requirements for vertical and lateral dissemination of routine and time-sensitive intelligence products and reports. Address voice, network, courier, briefings, and other communications methods, to include point-to-point and alarm methods. Establish alternate means to ensure that required intelligence will be provided to subordinate and supported units. Provide guidance regarding intelligence and information security, to include the dissemination of sensitive compartmented information within the force and the releasibility of intelligence to non-US forces.

Tab D, Intelligence Communications and Information Systems Plan

Provide any specific instruction necessary regarding the establishment, operation, and maintenance of intelligence and pertinent supporting CIS resources and databases, to include those dedicated to intelligence operations as well as multipurpose MAGTF CIS resources used for intelligence purposes.

Note: This tab may be consolidated with Tab C.

Tab E, Intelligence Reports

Provide any instructions necessary regarding intelligence reports, both all-source and single discipline.

Appendix 17 (Support to Survival, Evasion, Resistance, and Escape)

The support to survival, evasion, resistance and escape (SERE) appendix provides guidance, procedures, intelligence products and orders for intelligence support to MAGTF SERE preparations and operations. A variety of intelligence products are developed to support MAGTF SERE readiness. Together with Tab I (Survival, Evasion, Resistance, and Escape Safe Areas) to Appendix 11 (Intelligence Estimate) these constitute the standard SERE support products. The P&A cell OIC is responsible for preparing these products. IMINT and, critically, imagery provide key support to each SERE support intelligence product. These include:

- SERE guides and bulletins. They provide basic information to help an individual survive, successfully evade and, if captured, resist enemy interrogations. The guidelines and bulletins cover an entire country or region and provide information on topography, hydrography, food and water sources, safe and dangerous plants and animals, customs and cultures, recognition of hostile forces, resistance techniques, and other types of information.
- Select areas for evasion (SAFE) area intelligence descriptions (SAID). SAIDs provide essential intelligence concerning specific SAFEs to assist evasion and resistance planners and potential evaders in planning and conducting recovery operations.
- Evasion and recovery (E&R) studies. E&R studies are similar to SAIDs. They differ in that not all conventional selection criteria for SAFE areas can be met because of current political, military or environmental factors prevailing within the area.

APPENDIX A. IMAGING SENSORS

Optical Cameras

Optical cameras detect and record electromagnetic radiation within the visible light and near-infrared portions of the electromagnetic spectrum. The operation principles are the same as for a common box camera. There are three types of optical imaging systems—vertical, oblique, and panoramic.

Vertical

The optical axis of the camera is approximately perpendicular to the surface of the earth (see figure A-1). Vertical imagery is ideal for performing terrain analysis, beach studies, and HLZ studies.

Oblique

Oblique imagery is obtained by imaging the ground at an angle to the vertical. The optical axis of the sensor is intentionally directed between the horizontal and the vertical. This axis can provide left or right oblique coverage. Oblique imagery requires oblique metrics, and is also ideal for observation at canopy baseline.

There are two standard types of oblique imagery, high and low. High oblique imagery (see figure A-2 on page A-2) will include the horizon, while low oblique imagery (see figure A-3 on page A-2) will not. Because of the angle, high oblique imagery covers a larger area than low oblique. Oblique imagery is referred to as left or right oblique or forward looking, based on the look angle in respect to the platform.

Panoramic

Panoramic imagery is taken with a special camera that is able to scan a wide area. The optical axis of the camera utilizes a system of optics that can scan

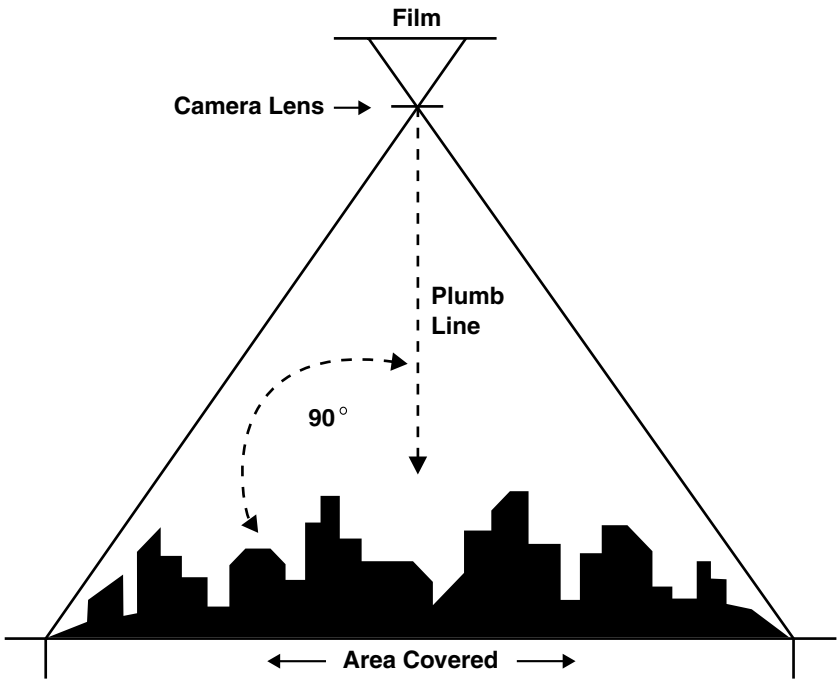


Figure A-1. Relationship of a Vertical Aerial Image with the Ground.

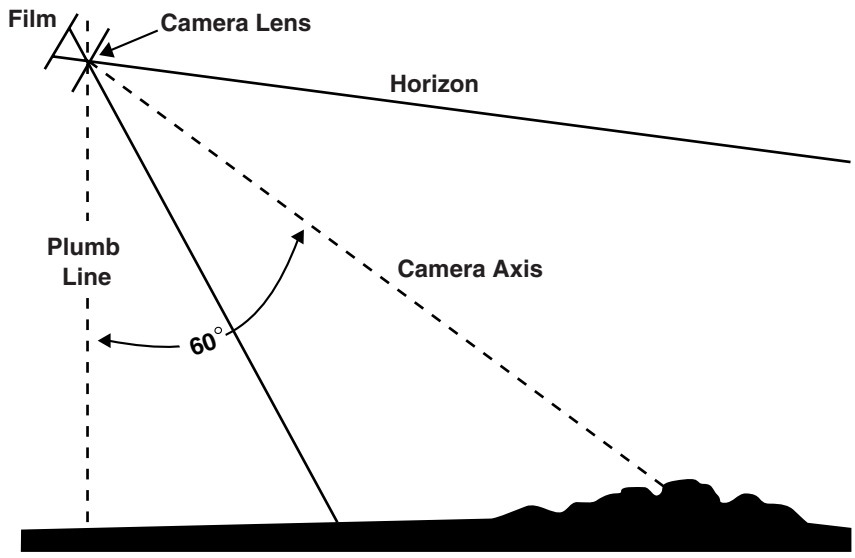


Figure A-2. Relationship of High Oblique Photograph to the Ground.

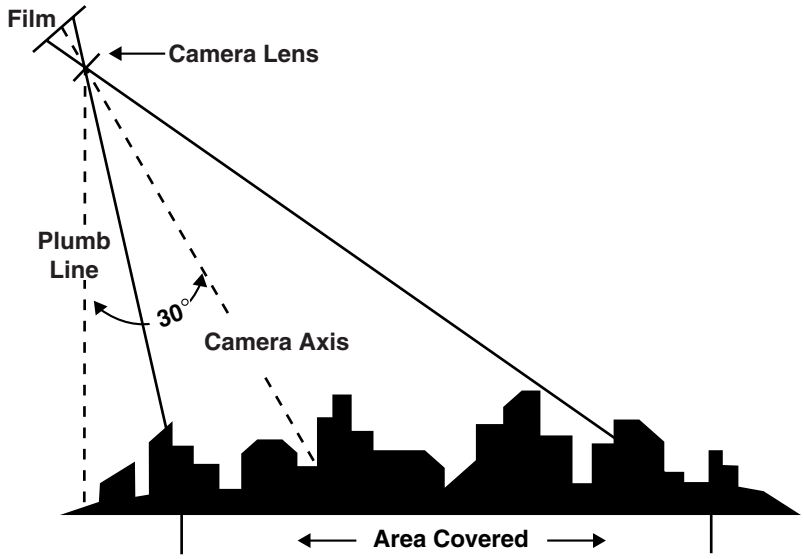


Figure A-3. Relationship of Low Oblique Imagery to the Ground.

an area from 0 to 180 degrees. There are two types of panoramic imagery, low and high.

- Low panoramic imagery (see figure A-4) is taken at low altitudes and scans a wide angle that includes the horizon at either side of the aircraft flight path.
- High panoramic imagery (see figure A-5) is taken at high altitudes with a smaller scan angle.

The horizon is not normally visible on high panoramic imagery. In only one pass over the target area, panoramic photography provides coverage of large areas of terrain on both sides of the aircraft flight path. Although it provides both vertical and oblique views of the image area, it is the most difficult and time-consuming photography to analyze and measure, owing to the distortion of the recorded image. Table A-1 on page A-4

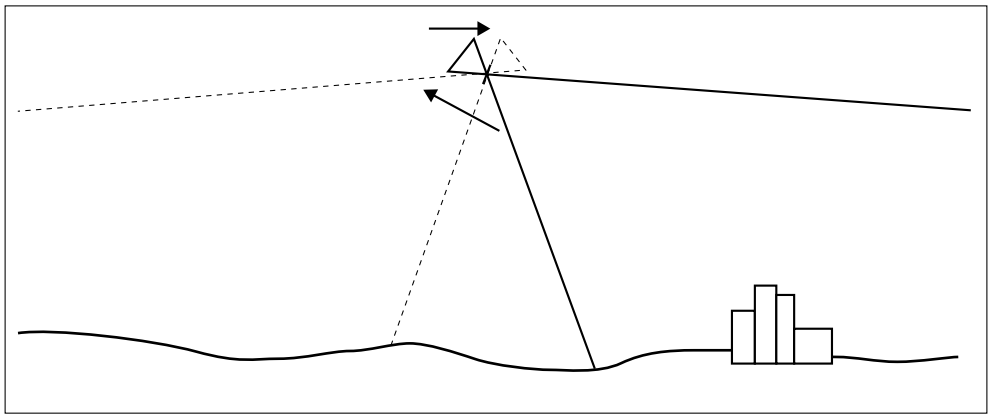


Figure A-4. Low Panoramic Imagery.

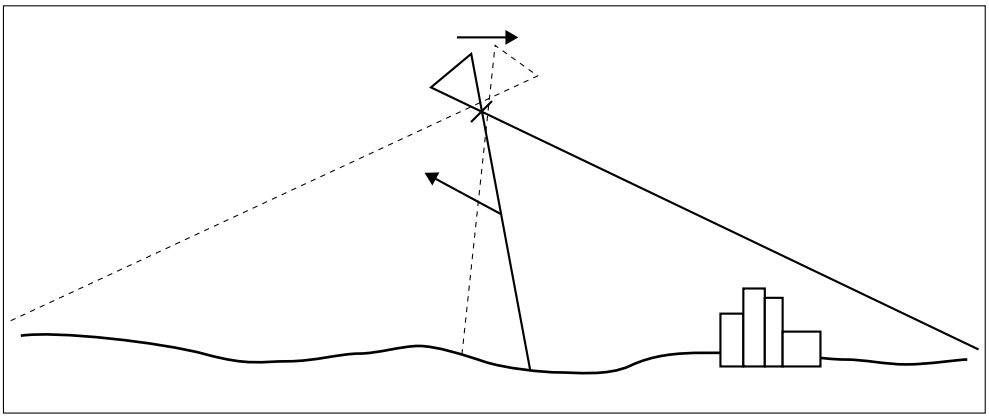


Figure A-5. High Panoramic Imagery.

summarizes both the advantages and disadvantages of each type of imaging system.

Capabilities of optical sensors are—

- High quality photograph (good resolution).
- Passive system, which cannot be detected or jammed.
- Flexibility of sensors.

Limitations of optical sensors are—

- Light source needed.
- Hampered during periods of reduced visibility.
- Susceptible to enemy deception.
- LOS dependent.

High Resolution Radar

Radar is an active sensing technique that detects and records differences in reflected electromagnetic energy.

Capabilities of high resolution radar are—

- Offers day and night operations.
- All-weather capability.
- Standoff capability.

Table A-1. Advantages and Disadvantages of Imaging Systems.

Sensor System	Advantages	Disadvantages
Vertical	Fairly constant scale. Can construct mosaics. Obtains accurate measurements. Allows stereographic viewing. Accurate interpretation.	Aircraft or air vehicles must fly directly over the target. Objects under overhead cover cannot be viewed. Unnatural view angle. Some areas are inaccessible due to restrictions in over-flights (tactical systems).
Oblique	Large area coverage. More natural view. Aircraft or air vehicle does not fly over the target. Can view objects under cover due to angle.	Terrain masking. Scale varies. Measurements difficult.
Panoramic	Large area coverage. Satisfies both vertical and oblique mission requirements.	Scale varies. Aircraft has limited standoff capability. Measurements difficult.

Limitations of high resolution radar are—

- Poor resolution.
- Active sensing techniques.
- LOS dependent.

Infrared

Infrared (IR) sensors detect and record electromagnetic radiation that is emitted from a given target surface in the IR portion of the electromagnetic spectrum.

Capabilities of IR are—

- Offers day and night operations.
- Has passive sensing techniques.
- Detects camouflage equipment and activity.

Limitations of IR are—

- Poor resolution.
- Susceptible to enemy deception.
- Hampered by rain, snow, hail, etc.
- LOS dependent.

APPENDIX B. NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

Background

Imagery analysts use the National Imagery Interpretability Rating Scale (NIIRS) to define and measure the quality of images and performance of imaging systems. Through a process referred to as rating an image, the NIIRS is used by imagery analysts to assign a number indicating the interpretability of a given image. The NIIRS concept provides a means to directly relate the quality of an image to the interpretation tasks for use. Although the NIIRS has been primarily applied in the evaluation of aerial imagery, it also provides a systematic approach to measuring the quality of photographic or digital imagery, the performance of image capture devices, and the effects of image processing algorithms.

The NIIRS is a task-based scale consisting of nine graduated levels. At each level, representative exploitation tasks (termed criteria) indicate the level of information extracted with an image of a given interpretability level. For example, with a NIIRS 2 image, imagery analysts should be able to detect large hangars at an airfield, while with a NIIRS 8 image; they should be able to identify the rivet lines on bomber aircraft. At a higher NIIRS level, more detailed information can be obtained from an image.

The NIIRS is designed to relate to a wide range of image quality. A NIIRS level of 0 is defined as having no value for intelligence purposes. The definition of that level is open to debate. The upper end of the scale is defined by the best available imagery of a given type; i.e., a portion of the spectrum. The upper end of a scale is not necessarily indicative of any specific operational system.

The NIIRS measures the information potential; i.e., interpretability of an image. This means that specific objects listed in the criteria need not be present, but the physical attributes of the image are such that the image would have the specified information value if the necessary content were present. The NIIRS relies on the experience of imagery analysts to be able to extrapolate, or imagine, how well criteria would be rendered if those features were present in the image to be rated. Because each rating refers to specific tasks the imagery analyst can or could do, it has a more precise meaning than, for example, when such subjective words as good or fair are used. Thus, judgments become more uniform, because imagery analysts can use the same yardstick to measure interpretability.

The NIIRS accounts for the major factors that affect image interpretability. Image resolution, measured as ground resolved distance or ground sample distance, has a significant effect on interpretability. Spatial resolution alone does not determine the NIIRS of an image, since sharpness, noise, and contrast also influence the NIIRS. These effects may be due to system parameters (e.g., optical quality, focal plane characteristics), acquisition conditions (e.g., sun angle, atmospheric haze), and exploitation conditions (e.g., duplicate film quality, softcopy monitor quality). By design, the NIIRS is independent of a particular imaging system. NIIRS ratings and ranges are—

NIIRS Rating	Range in Meters
0	N/A
1	over 9.0
2	4.5–9.0
3	2.5–4.5
4	1.2–2.5
5	0.75–1.2
6	0.40–0.75
7	0.20–0.40
8	0.10–0.20
9	less than 0.10

Principal Uses of NIIRS

There are several primary uses for the NIIRS. These are—

- Communicating imagery interpretability. (Can this image answer the IR, both now and archived?
- Developing collection requirements. (Can an imagery system collect the required information? Can the currently available imagery missions collect the information?)
- Assessing mission collection satisfaction. (Does the image satisfy the intelligence requirement?)
- Assessing technical performance. (Is the imagery system working as planned?)

Procedure for Assigning NIIRS Rating Levels Criteria

The NIIRS criteria are expressed in terms of detect, identify or distinguish between objects, features or activities.

Detect is the capability to find or discover the presence or existence of an installation, object, activity or item of intelligence interest based on its general shape (configuration) and on other contextual information in the scene. Some level of identification is implied in detection, so that the relatively gross feature or item detected can be properly named or classified.

Identify is the capability to name an object by type or class based primarily on its configuration and detailed components. As used in NIIRS, identification is based on observation of actual physical detail and not through information from other sources.

Distinguish between is the capability to determine that two detected objects are of different types or classes based on one or more distinguishing features.

Guidelines

The following guidelines allow NIIRS to be used to communicate image interpretability, to evaluate mission performance, and to plan for new imagery systems.

- When assigning a NIIRS level, the imagery analyst evaluates a target within an imagery segment or the entire area on the segment, as necessary, to meet the imagery analyst's task. The imagery analyst will assign a NIIRS level that best characterizes the overall interpretability of the target or area.
- The imagery analyst should neither ignore nor emphasize exceptionally good or poor portions of the image segment.
- When considering clouds, shadows or other localized degradations, the imagery analyst rates the target or area with NIIRS level 0 only when the degradation precludes using it for interpretation. If the area of interest is degraded but interpretable, the imagery analyst should assign a NIIRS that best represents its interpretability.
- The imagery analyst should ignore shadows cast by individual items of intelligence interest.

SECTION I. VISIBLE NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

NIIRS Rating	Description
0	Interpretability of the imagery is precluded by obscuration, degradation or very poor resolution.
1	Detect a medium-sized port facility and/or distinguish between taxiways and runways at a large airfield.
2	Detect large hangars at airfields. Detect large static radars (e.g., AN/FPS-85, COBRA DANE, PECHORA, HENHOUSE). Detect military training areas. Identify an SA-5 site based on road pattern and overall site configuration. Detect large buildings at a naval facility (e.g., warehouses, construction hall). Detect large buildings (e.g., hospitals, factories).
3	Identify the wing configuration (e.g., straight, swept delta) of all large aircraft (e.g., 707, CONCORD, BEAR, BLACKJACK). Identify radar and guidance areas at a SAM site by the configuration, mounds, and presence of concrete aprons. Detect a helipad by the configuration and markings. Detect the presence/absence of support vehicles at a mobile missile base. Identify a large surface ship in port by type (e.g., cruiser, auxiliary ship, noncombatant/merchant). Detect trains or strings of standard rolling stock on railroad tracks (not individual cars).
4	Identify all large fighters by type (e.g., FENCER, FOXBAT, F-15, F-14). Detect the presence of large individual radar antennas (e.g., TALL KING). Identify, by general type, tracked vehicles, field artillery, large river-crossing equipment, wheeled vehicles when in groups. Detect an open missile silo door. Determine the shape of the bow (pointed or blunt/rounded) on a medium-sized submarine (e.g., ROMEO, HAN, Type 209, CHARLIE II, ECHO II, VICTOR II/III). Identify individual tracks, rail pairs, control towers, and switching points in rail yards.
5	Distinguish between a MIDAS and a CANDID by the presence of refueling equipment (e.g., pedestal and wing pod). Identify radar as vehicle-mounted or trailer-mounted. Identify, by type, deployed tactical SSM systems (e.g., FROG, SS-21, SCUD). Distinguish between SS-25 mobile missile TEL and missile support vans in a known support base, when not covered by camouflage. Identify TOP STEER or TOP SAIL air surveillance radar on KIROV-, SOVREMENNY-, KIEV-, SLAVA-, MOSKVA-, KARA-, or KRESTA-II-class vessels. Identify individual rail cars by type (e.g., gondola, flat, box) and/or locomotives by type (e.g., steam, diesel).
6	Distinguish between models of small/medium helicopters (e.g., HELIX A from HELIX B from HELIX C, HIND D from HIND E, HAZE A from HAZE B from HAZE C). Identify the shape of antennas on EW/GCI/ACQ radars as parabolic, parabolic with clipped corners or rectangular. Identify the spare tire on a medium-sized truck. Distinguish between SA-6, SA-11, and SA-17 missile airframes. Identify individual launcher covers (8) of vertically launched SA-N-6 on SLAVA-class vessels. Identify automobiles as sedans or station wagons.
7	Identify fitments and fairings on a fighter-sized aircraft (e.g., FULCRUM, FOXHOUND). Identify ports, ladders, and vents on electronics vans. Detect the mount for antitank guided missiles (e.g., SAGGER on BMP-1). Detect details of the silo door hinging mechanism on Type III-F, III-G, and II-H launch silos and Type III-X launch control silos. Identify the individual tubes of the RBU on KIROV-, KARA-, and KRIVAK-class vessels. Identify individual rail ties.
8	Identify the rivet lines on bomber aircraft. Detect horn-shaped and W-shaped antennas mounted atop BACKTRAP and BACKNET radars. Identify a hand-held SAM (e.g., SA-7/14, REDEYE, STINGER). Identify joints and welds on a TEL or TELAR. Detect winch cables on deck-mounted cranes. Identify windshield wipers on a vehicle.
9	Differentiate cross-slot from single slot heads on aircraft skin panel fasteners. Identify small light-toned ceramic insulators that connect wires of an antenna canopy. Identify vehicle registration numbers (VRNs) on trucks. Identify screws and bolts on missile components. Identify braid of ropes (1 to 3 inches in diameter). Detect individual spikes in railroad ties.

SECTION II. INFRARED NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

NIIRS Rating	Description
0	Interpretability of the imagery is precluded by obscuration, degradation or very poor resolution.
1	Distinguish between runways and taxiways on the basis of size, configuration or pattern at a large airfield. Detect a large (e.g., greater than 1 square kilometer) cleared area in dense forest. Detect large ocean-going vessels (e.g., aircraft carrier, super-tanker, KIROV) in open water. Detect large areas (e.g., greater than 1 square kilometer) of marsh/swamp.
2	Identify individual thermally active engine vents. Detect large aircraft (e.g., C-141, 707, BEAR, CANDID, CLASSIC). Detect individual large buildings (e.g., hospitals, factories) in an urban area. Distinguish between densely wooded, sparsely wooded, and open fields. Identify an SS-25 base by the pattern of buildings and roads. Distinguish between naval and commercial port facilities based on type and configuration of large functional areas.
3	Distinguish between large (e.g., C-141, 707, BEAR, A-300 AIRBUS) and small aircraft (e.g., A-4, FISHBED, L-39). Identify individual thermally active flues running between the boiler hall and smoke stacks at a thermal power plant. Detect a large air warning radar site based on the presence of mounds, revetments, and security fencing. Detect a driver-training track at a ground forces garrison. Identify individual functional areas (e.g., launch sites, electronics area, support area, missile handling area) of an SA-5 launch complex. Distinguish between large (e.g., greater than 200 meter) freighters and tankers.
4	Identify the wing configuration of small fighter aircraft (e.g., FROGFOOT, F-16, FISHBED). Detect a small (e.g., 50 meter square) electrical transformer yard in an urban area. Detect large (e.g., greater than 10-meter diameter) environmental domes at an electronics facility. Detect individual thermally active vehicles in garrison. Detect thermally active SS-25 missile support vans in garrison. Identify individual closed cargo hold hatches on large merchant ships.
5	Distinguish between single-tail (e.g., FLOGGER, F-16, TORNADO) and twin-tailed (e.g., F-15, FLANKER, FOXBAT) fighters. Identify outdoor tennis courts. Identify the metal lattice structure of large (e.g., approximately 75 meter) radio relay towers. Detect armored vehicles in a revetment. Detect a deployed transportable electronics tower at an SA-10 site. Identify the stack shape (e.g., square, round, oval) on large (e.g., greater than 200 meters) merchant ships.
6	Detect wing-mounted stores (i.e., ASM, bombs) protruding from the wings of large bombers (e.g., B-52, BEAR, BADGER). Identify individually thermally active engine vents atop diesel locomotives. Distinguish between a FIX FOUR and FIX SIX site based on antenna pattern and spacing. Distinguish between thermally active tanks and APCs. Distinguish between a 2-rail and 4-rail SA-3 launcher. Identify missile tube hatches on submarines.
7	Distinguish between ground attack and interceptor versions of the MIG-23 FLOGGER based on the shape of the nose. Identify automobiles as sedans or station wagons. Identify antenna dishes (less than 3 meters in diameter) on a radio relay tower. Identify the missile transfer crane on an SA-6 transloader. Distinguish between an SA-2/CSA-1 and a SCUD-B missile transporter when missiles are not loaded. Detect mooring cleats or bollards on piers.
8	Identify the RAM airscoop on the dorsal spine of FISHBED J/K/L. Identify limbs (e.g., arms, legs) on an individual. Identify individual horizontal and vertical ribs on a radar antenna. Detect closed hatches on a tank turret. Distinguish between fuel and oxidizer multi-system propellant transporters based on twin or single fitments on the front of the semi-trailer. Identify individual posts and rails on deck edge life rails.
9	Identify access panels on fighter aircraft. Identify cargo (e.g., shovels, rakes, ladders) in an open bed, light-duty truck. Distinguish between BIRDS EYE and BELL LACE antennas based on the presence or absence of small dipole elements. Identify turret hatch hinges on armored vehicles. Identify individual command guidance strip antennas on an SA-2/CSA-1 missile. Identify individual rungs on bulkhead-mounted ladders.

SECTION III. RADAR NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

NIIRS Rating	Description
0	Interpretability of the imagery is precluded by obscuration, degradation or very poor resolution.
1	Detect the presence of aircraft dispersal parking areas. Detect a large cleared swath in a densely wooded area. Detect, based on presence of piers and warehouses, a port facility. Detect lines of transportation (either road or rail), but do not distinguish between.
2	Detect the presence of large (e.g., BLACKJACK, CAMBER, COCK, 707, 747) bombers or transports. Identify large phased-array radars (e.g., HEN HOUSE, DOG HOUSE) by type. Detect a military installation by building pattern and site configuration. Detect road pattern, fence and hardstand configuration at SSM launch sites (missile silos, launch control silos) within a known ICBM complex. Detect large non-combatant ships (e.g., freighters or tankers) at a known port facility. Identify athletic stadiums.
3	Detect medium-sized aircraft (e.g., FENCER, FLANKER, CURL, COKE, F-15). Identify an ORBITA site on the basis of a 12-meter dish antenna normally mounted on a circular building. Detect vehicle revetments at a ground forces facility. Detect vehicles/pieces of equipment at a SAM, SSM or ABM fixed missile site. Determine the location of the superstructure (e.g., fore, amidships, aft) on a medium-sized freighter. Identify a medium-sized (approx. six track) railroad classification yard.
4	Distinguish between large rotary-wing and medium fixed-wing aircraft (e.g., HALO helicopter vs. CRUSTY transport). Detect recent cable scars between facilities or command posts. Detect individual vehicles in a row at a known motor pool. Distinguish between open and closed sliding roof areas on a single bay garage at a mobile missile base. Identify square bow shape of ROPUCHA class (LST). Detect all rail/road bridges.
5	Count all medium helicopters (e.g., HIND, HIP, HAZE, HOUND, PUMA, WASP9). Detect deployed TWIN EAR antenna. Distinguish between river-crossing equipment and medium/heavy armored vehicles by size and shape (e.g., MTU-20 vs. T-62 MBT). Detect missile support equipment at an SS-25 RTP (e.g., transporter-erector-launcher, missile support van). Distinguish bow shape and length/width differences of SSNs (attack submarines, nuclear). Detect the break between railcars (count railcars).
6	Distinguish between variable and fixed-wing fighter aircraft (e.g., FENCER vs. FLANKER). Distinguish between the BAR LOCK and SIDE NET antennas at a BAR LOCK/SIDE NET acquisition radar site. Distinguish between small support vehicles (e.g., UAZ-69, UAZ-469) and tanks (e.g., T-72, T-80). Identify SS-24 launch triplet at a known location. Distinguish between the raised helicopter deck on a KRESTA II (CG) and the helicopter deck with main deck on a KRESTA I (CG). Identify a vessel by class when singly deployed (e.g., YANKEE I, DELTA I, KRIVAKII FFG). Detect cargo on a railroad flatcar or in a gondola.
7	Identify small fighter aircraft by type (e.g., FISHBED, FITTER, FLOGGER). Distinguish between electronics van trailers (without tractor) and van trucks in garrison. Distinguish, by size and configuration, between a turreted, tracked APC and a medium tank (e.g., BMP-1/2 vs. T-64). Detect a missile on the launcher in an SA-2 launch revetment. Distinguish between bow mounted missile system on KRIVAK I/II and bow mounted gun turret on KRIVAK III. Detect road/street lamps in an urban, residential area or military complex.
8	Distinguish the fuselage difference between a HIND and a HIP helicopter. Distinguish between the FAN SONG E missile control radar and the FAN SONG F based on the number of parabolic dish antennas (three vs. one). Identify the SA-6 transloader when other SA-6 equipment is present. Distinguish limber hole shape and configuration differences between DELTA I and YANKEE I (SSBNs). Identify the dome/vent pattern on rail tank cars.
9	Detect major modifications to large aircraft (e.g., Airings, pods, wingless). Identify the shape of antennas on EW/GCI/ACQ radars as parabolic, parabolic with clipped corners or rectangular. Identify, based on presence or absence of turret, size of gun tube, and chassis configuration, wheeled or tracked APCs by type (e.g., BTR-80, BMP-1/2, MT-LB, M113). Identify the forward fins on an SA-3 missile. Identify individual hatch covers of vertically launched SA-N-6 surface-to-air system. Identify trucks as cab-over-engine or engine-in-front.

SECTION IV. MULTISPECTRAL NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

The traditional OOB criteria categories (air, electronic, ground, missile, and naval) found in the NIIRS are not present in the multispectral imagery (MSI) national imagery interpretability rating scale. Five new categories more relevant to MSI exploitation were developed: military, urban/industrial/lines of communication, vegetation/agricultural, terrain, and water resources.

NIIRS Rating	Description
1	Distinguish between urban and rural areas. Identify a large wetland (greater than 100 acres). Detect meander flood plains (characterized by features such as channel scars, oxbow lakes, meander scrolls). Delineate coastal shoreline. Detect major highway and rail bridges over water (e.g., Golden Gate, Chesapeake Bay). Delineate extent of snow or ice cover.
2	Detect multilane highways. Detect strip mining. Determine water current direction as indicated by color differences (e.g., tributary entering larger water feature, chlorophyll or sediment patterns). Detect timber clear-cutting. Delineate extent of cultivated land. Identify riverine flood plains.
3	Detect vegetation/soil moisture differences along a linear feature (suggesting the presence of a fenceline). Identify major street patterns in urban areas. Identify golf courses. Identify shoreline indications of predominant water currents. Distinguish among residential, commercial, and industrial areas within an urban area. Detect reservoir depletion.
4	Detect recently constructed weapon positions (e.g., tank, artillery, self-propelled gun) based on the presence of revetments, berms, and ground scarring in vegetated areas. Distinguish between two-lane improved and unimproved roads. Detect indications of natural surface airstrip maintenance or improvements (e.g., runway extension, grading, resurfacing, bush removal, vegetation cutting). Detect landslide or rockslide large enough to obstruct a single-lane road. Detect small boats (15–20 feet in length) in open water. Identify areas suitable for use as light fixed-wing aircraft (e.g., Cessna, Piper Cub, Beechcraft) landing strips.
5	Detect automobile in a parking lot. Identify beach terrain suitable for amphibious landing operation. Detect ditch irrigation of beet fields. Detect disruptive or deceptive use of paints or coatings on buildings/structures at a ground forces installation. Detect raw construction materials in ground forces deployment areas (e.g., timber, sand, gravel).
6	Detect summer woodland camouflage netting large enough to cover a tank against a scattered tree background. Detect foot trail through tall grass. Detect navigational channel markers and mooring buoys in water. Detect livestock in open but fenced areas. Detect recently installed minefields in ground forces deployment area based on a regular pattern of disturbed earth or vegetation. Count individual dwellings in subsistence housing areas (e.g., squatter settlements, refugee camps).
7	Distinguish between tanks and three-dimensional tank decoys. Identify individual 55-gallon drums. Detect small marine mammals (e.g., harbor seals) on sand/gravel beaches. Detect underwater pier footings. Detect foxholes by ring of spoil outlining hole. Distinguish individual rows of truck crops.
8–9	Not applicable.

SECTION V. CIVIL NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

The Civil National Imagery Interpretability Rating Scale (NIIRS) supplements the Visible NIIRS by expanding the number of criteria categories.

NIIRS Rating	Description
0	Interpretability of the imagery is precluded by obscuration, degradation or very poor resolution.
1	Distinguish between major land use classes (urban, agricultural, forest, water, barren). Detect a medium sized port facility. Distinguish between runways and taxiways at a large airfield. Identify large area drainage patterns by type (dendritic, trellis, radial).
2	Identify large (greater than 160 acres) center pivot irrigated fields during the growing season. Detect large buildings (hospitals, factories). Identify road patterns, like clover leafs, on major highway systems. Detect icebreaker tracks. Detect the wake from a large (greater than 300 feet) ship.
3	Detect large area (larger than 160 acres) contour plowing. Detect individual houses in residential neighborhoods. Detect trains or strings of standard rolling stock on railroad tracks (not individual cars). Identify inland waterways navigable by barges. Distinguish between natural forest stands and orchards.
4	Identify farm buildings as barns, silos, or residences. Count unoccupied railroad tracks along right-of-way or in a railroad yard. Detect basketball court, tennis court, and volleyball court in urban areas. Identify individual tracks, rail pairs, control towers, and switching points in rail yards. Detect jeep trails through grassland.
5	Identify Christmas tree plantations. Identify individual rail cars by type (gondola, flat, box) and locomotives by type (steam, diesel). Detect open-bay doors of vehicle storage buildings. Identify tents (larger than 2 person) at established recreational camping areas. Distinguish between stands of coniferous and deciduous trees during leafoff condition. Detect large animals (elephants, rhinoceros, and giraffes) in grassland.
6	Detect narcotics intercropping based on texture. Distinguish between row (corn and soybean) crops and small grain (wheat and oats) crops. Identify automobiles as sedans or station wagons. Identify individual telephone and electric poles in residential neighborhoods. Detect foot trails through barren areas.
7	Identify individual mature cotton plants in a known cotton field. Identify individual railroad ties. Detect individual steps on a stairway. Detect stumps and rocks in forest clearings and meadows.
8	Count individual baby pigs. Identify a U.S. Geological Survey benchmark set in a paved surface. Identify grill detailing and/or the license plate on a passenger or truck-type vehicle. Identify individual pine seedlings. Identify individual water lilies on a pond. Identify windshield wipers on a vehicle.
9	Identify individual grain heads on small grain (wheat, oats, and barley). Identify individual barbs on a barbed wire fence. Detect individual spikes in railroad ties. Identify individual bunches of pine needles. Identify an ear tag on large game animals (deer, elk, moose).

APPENDIX C. REQUEST FORMATS FOR AERIAL IMAGERY COLLECTION MISSIONS

Section I. Joint Tactical Air Reconnaissance/ Surveillance (JTAR/S) Request Format

PRECEDENCE

FROM:

TO:

INFO:

CLASSIFICATION

SUBJ: JTAR/S REQ

L. REQUEST NO.___ PREPLANNED IMMEDIATE A. PRIORITY C. PRIORITY B. PRECEDENCE ___

M. DATE/TIME FACTORS

1. DATE MISSION DESIRED
2. TOT (IF REQ)
3. LTIOV
4. PRIOR COVERAGE ACCEPTABLE (DAYS PRIOR)

N. TYPE RECON REQUESTED

1. TYPE MISSION

   A. VISUAL
   B. IMAGERY
   C. ELECTRONIC

2. TYPE COVERAGE

   A. PINPOINT
   B. STRIP/LINES OF COMMUNICATION
   C. ROUTE RECONNAISSANCE
   D. AREA SEARCH
   E. AREA COVERAGE
   F. AFLOAT

*3. SENSOR TYPE

A. OPTICAL
B. INFRARED
C. SLAR
D. ELECTRONIC
E. LASER
F. OTHER

*4. TYPE PHOTO

A. VERTICAL
B. OBLIQUE
C. PANORAMIC

*5. TYPE FILM

A. BLACK AND WHITE
B. COLOR
C. CAMOUFLAGE DETECTING

6. STEREO PHOTO

A. NOT REQUIRED
B. REQUIRED

O. MAP REFERENCE

TYPE AND SCALE_____
SERIES_____
SHEET_____
EDITION_____
DATE_____

P. TARGET COORDINATES

1. UTM
2. LAT/LONG
3. OTHER (SPECIFY)

Q. TARGET CATEGORY/PRIORITY INTELLIGENCE REQUIREMENT(S) (SEE DETAILED INSTRUCTION)

1. AIRFIELD
2. ARMOR/ARTY/TROOPS/VEH
3. BRIDGE
4. DEF POS/STRONG PT/GUN
5. ELECTRONIC SITE
6. HARBOR SITE
7. INDUSTRIAL
8. LOC
9. MIL. INST/STORAGE AREA

10. MISSILE SITE
11. POWER PROD. FACILITY
12. RAILROAD YARD
13. SHIPS
14. OTHER (SPECIFY)

R. REPORTS

1. IN-FLIGHT REPORT (CS/FREQ)_____ VALID FM_____ Z TO_____ Z
   (CS/FREQ)_____ VALID FM_____ Z TO_____ Z
2. MISSION REPORT
3. RECEXREP
4. IPIR
5. SUPIR

S. IMAGERY PRODUCTS (IF REQUIRED)

1. TYPE
2. QUANTITY
3. ADDITIONAL INFORMATION

T. DELIVERY ADDRESS

1. UNIT_____
2. AIR DROP (IF REQ): COORDS:_____
   CALL SIGN/FREQ_____
   RUN HEADING (MAG) (OPTIONAL)_____

U. REMARKS/SPECIAL INSTRUCTIONS

1. TARGET AREA CONTROL (CALL SIGN/FREQ)_____
2. OTHER (SPECIFY)_____

Notes:
1. Designate minimum mandatory items for immediate requests.
*2. * Indicates use as applicable or when known.*
3. The format provided has been published as STANAG 3277 and has been approved by NATO as a standard format for aerial requests. The letters A to K have special significance for certain organizations and are purposely omitted.
4. When submitting message JTAR/S, the paragraph headings are not required, but the alpha-numeric paragraphs will not be changed.
5. Instructions for completing a JTAR/S are on pages C-4 through C-8.

PARAGRAPH LETTERS INSTRUCTIONS

L. REQUEST NUMBER: As directed.

A&C Priority:	Use numerical designation below to define the tactical urgency for preplanned and immediate requests.
PRIORITY:	It is the responsibility of the requestor to establish the priority.

Priority No.	Definition
1	Takes precedence over all other requests except previously assigned Priority 1 requests. The results of these requests are of paramount importance to the immediate battle situation or objective.
2	The results of these requirements are in support of the general battle situation and will be accomplished as soon as possible after Priority 1 requests. These are requested to gain current battle information.
3	The results of these requests update the intelligence database but do not effect the immediate battle situation.
4	The results of these requests are of a routine nature and will be fulfilled when the reconnaissance effort permits.

M. DATE/TIME FACTORS

1. Self-explanatory.
2. a. State the Time on Target only when required.
   b. Justify U2.
3. Latest time intelligence is of value (LTIOV). Indicate, if it is a factor, the LTIOV. Deliver prior to this date/time.
4. Self-explanatory.

N. TYPE RECONNAISSANCE REQUESTED

1. Type Mission—Self-explanatory.
2. Type Coverage
   a. Pinpoint—Self-explanatory.
   b. Strip/Lines of Communications—Search continuous photography of a route of LOC.
   c. Route Reconnaissance—Visual reconnaissance of a route of LOC with photo of targets of military significance.
   d. Area Search—Visual search of a specified area with photos of targets of military significance.
   e. Area Coverage—Photographic coverage of a specified area.
   f. Afloat—Reconnaissance of vessels afloat.

   3, 4, and 5. Self-explanatory. These lines should be left blank unless it is fully understood what the selected sensor, photo, and film can accomplish.

O. MAP REFERENCE. Self-explanatory.

P. TARGET COORDINATES. Provide reference system used and indicate actual coordinates.

Q. TARGET CATEGORY/PRIORITY INTELLIGENCE REQUIREMENT(S). Provide the appropriate category and indicate the desired PIR by selecting the number(s) from the target list category below.

CATEGORY 1—AIRFIELD

A. Activity: Number, type, and location of aircraft.
B. Runways: Number, orientation, and surface type.
C. Taxiway and parking areas: Location and shape.
D. POL: Number, size, and location.
E. Ammunition storage areas: Number and location.
F. Hangars: Number, size, and type construction.
G. Electronic facilities: Number, type, and location.
H. Defenses: Number, type, and location.
I. Other: (specify).

CATEGORY 2—ARMOR/ARTY/TROOPS/VEHICLES

A. Type: Infantry, armor, engineering, artillery, etc.
B. Number and type of vehicles.
C. Number and type of armor.
D. Number and type of artillery.
E. Activity: Direction of movement, dug in, etc.
F. Terrain: Description.
G. Other: (specify).

CATEGORY 3—BRIDGE

A. Purpose: Flood, rail, over road, etc.
B. Type: Railroad, vehicular, agricultural, etc.
C. Construction: Wood, steel, concrete, etc.
D. Construction: Piers, abutments, approaches, stringers, beam, truss, etc.
E. Number of spans.
F. Length and width (height if significant).
G. Number of lanes/tracks.
H. Bypass in vicinity of bridge.
I. Activity.
J. Other: (specify).

CATEGORY 4—DEFENSIVE POSITIONS/STRONG POINTS/GUNS

A. Type and size of position or fortification.
B. Type weapons: Number.
C. Fire control system.
D. Supporting positions.
E. Transportation access.
F. Routes of ingress and egress.
G. Nature of surrounding terrain and foliage barriers.
H. Activity.
I. Other: (specify).

CATEGORY 5—ELECTRONIC SITE

A. Type site: Microwave relay, EW, etc.
B. Antennas: Number and type.
C. Mobile or permanent.
D. Primary buildings and support equipment.
E. Activity.
F. Security measures.
G. Size of area.
H. Other: (specify).

CATEGORY 6—HARBOR/PORT FACILITIES

A. Type port: Maritime or inland waterway.
B. Activity.
C. Berthing and cargo handling facilities.
D. POL facilities: Type, number, and locations.
E. Storage facilities.
F. Shipbuilding and repair facilities.
G. Transportation.
H. Defenses.
I. Other: (specify).

CATEGORY 7—INDUSTRIAL SITE

A. Type of industry.
B. Size of area.
C. Buildings: Number, size, and construction.
D. Open storage: Quantity by type.
E. Activity.
F. Transportation facilities.
G. Source of power.
H. Defenses.
I. Other: (specify).

CATEGORY 8—LINES OF COMMUNICATIONS (LOC)

A. Type: Road, rail, canal, etc.
B. Description of the route.
C. Chokepoints.

D. Significant activity.
E. Significant static targets.
F. Other: (specify).

CATEGORY 9—MILITARY INSTALLATIONS/STORAGE AREAS

A. Function: Assembly, admin, barracks, depot, etc.
B. Activity: Number of vehicles and/or personnel.
C. Size of the area.
D. Number of buildings: Predominant construction only.
E. Storage: Type and location.
F. Transportation.
G. Defenses.
H. Other: (specify).

CATEGORY 10—MISSILE SITE

A. Type.
B. Launch site: Mobile/fixed, number of pads, etc.
C. Number and orientation of launchers/number loaded.
D. Control center: Location and construction.
E. Number, type, and location antenna(s).
F. Auxiliary equipment.
G. Activity.
H. Defenses.
I. Other: (specify).

CATEGORY 11—POWER PRODUCTION FACILITY

A. Type: Nuclear, coal, oil, hydroelectric, etc.
B. Size and construction.
C. Boiler/generators: Number and location.
D. Transformer yard: Size and location.
E. Cooling towers: Number and location.
F. Penstock/turbine outlet (hydroelectric).
G. Activity.
H. Defenses.
I. Other.

CATEGORY 12—RAILROAD YARD

A. Type: Classification, repair, other.
B. Length and width: Chokepoint to chokepoint.
C. Number of tracks.
D. Facilities: Repair shops, roundhouses, other.
E. Rolling stock.
F. Defenses.
G. Other: (specify).

CATEGORY 13—SHIPS

A. Class/type/number.
B. Heading/movement.
C. Nationality.
D. Identification.
E. Cargo.
F. Activity.
G. Other.

CATEGORY 14—OTHER

Narrative report is rendered under this heading in sufficient detail to ensure that the request or purpose of the mission is satisfied.

R. REPORTS

1. IN-FLIGHT—An in-flight report to friendly units.
2. MISSION REPORT—A mission report of the results and significant sightings gathered.
3. RECONNAISSANCE EXPLOITATION REPORT—A brief, concise, high priority report on time-sensitive targets of significant tactical importance of a perishable nature.
4. INITIAL PHOTOGRAPHIC INTERPRETATION REPORT—An initial photo interpretation report that contains intelligence on mission objectives and additional significant intelligence.
5. SUPPLEMENTAL PHOTOGRAPHIC INTERPRETATION REPORT—A supplemental photo interpretation report that provides detailed intelligence acquired through a comprehensive study of imagery.

S. IMAGERY PRODUCTS—Specify type and quantity of imagery products required. Only mission essential imagery products should be requested.

T. DELIVERY ADDRESS

1. Unit—Delivery address for mission essential imagery products.
2. Air Drop—Coordinates, call sign, frequency, and run-in heading for aerial delivery of imagery products.

U. REMARKS/SPECIAL INSTRUCTIONS

1. Target Area Control—Indicate, when applicable, the call sign and radio frequency of the control element. Control of the mission will require close coordination with ground forces.
2. Other—Self-explanatory (use this space to specify scale if required and to request specific TOT).

Section II. Immediate Joint Tactical Air Reconnaissance/ Surveillance (JTAR/S) Request Format

Source format: Joint Tactical Air Strike Request format.

(Voice Template)

1. UNIT CALLED THIS IS _____ REQUEST # _____

2. B IMMEDIATE _____ C PRECEDENCE _____

PRIORITY _____

3. TARGET IS/NUMBER OF

A. PERS IN OPEN _____/_____
B. PERS DUG IN _____/_____
C. WPNS/MG/RR/AT _____/_____
D. MORTARS/ARTY _____/_____
E. AAA, ADA _____/_____
F. RKTS, MISSILE _____/_____
G. ARMOR _____/_____
H. VEHICLES _____/_____
I. BLDGS _____/_____
J. BRIDGES _____/_____
K. PILLBOX BNKRS _____/_____
L. SUPPLIES, EQUIP _____/_____
M. CNTR (CP, COM) _____/_____
N. AREA _____/_____
O. ROUTE _____/_____
P. MOVING NESW _____/_____
Q. REMARKS _____

4. TARGET LOCATION/ROUTE/AREA IS

A. _____ (COORDINATES)
B. _____(COORDINATES)
C. _____(COORDINATES)
D. _____(COORDINATES)
E. TARGET ELEVATION _____
F. SHEET # _____
G. SERIES _____
H. CHART # _____

5. TARGET TIME/DATE

A ASAP _____
B. NLT _____
C. AT _____
D.TO _____

6. DESIRED RESULTS/MISSION/PIRs

(FREE TEXT _____)

7. REMARKS

(FREE TEXT _____)

APPENDIX D. UNMANNED AERIAL VEHICLE SQUADRON EQUIPMENT AND PERFORMANCE CHARACTERISTICS

Pioneer UAV System

The UAV system found in the Marine Corps VMU squadrons consists of the following:

- Pioneer UAV aircraft (see figure D-1).
- Ground control station (GCS) in an S-280 shelter (see figure D-2).
- Tracking control unit (TCU) in an S-250 shelter.
- Portable control station (PCS).
- Remote receiving stations (RRSs) (one to four).
- Rocket-assisted takeoff (RATO) rail and/or truck-mounted pneumatic launchers.
- Arresting gear recovery equipment.

Table D-1 on page D-2 provides Pioneer UAV characteristics.

Figure D-1. Pioneer UAV Aircraft.

Figure D-2. Pioneer UAV Aircraft with GCS.

Table D-1. Pioneer UAV Characteristics.

Altitude	
Service ceiling	15,000 feet
Maximum ceiling	15,000 feet
Endurance	5 to 6.5 hours
Radius of Action	
Nominal	87 nautical miles/160 kilometers
Maximum	101 nautical miles/185 kilometers
Speed	
Maximum speed	176 kilometers per hour/110 knots
Cruise speed	120 kilometers per hour/85 knots
Loiter speed	95 kilometers per hour/65 knots
Maximum endurance	95 kilometers per hour/65 knots
Propulsion Reciprocating Two-Stroke, Two-Cylinder	
Engine	26 horsepower
Fuel type	100-octane, low-lead aviation gasoline/2-stroke oil (50:1 ratio)
Weight	
Empty	125 kilograms/276 pounds
Fuel capacity	30 kilograms/65 pounds
Sensor payload (maximum)	34 kilograms/75 pounds
Maximum takeoff weight	189 kilograms/ 416 pounds
Dimensions	
Wing span	5.2 meters
Wing area	2.8 square meters
Avionics	
Power supply	28 volts direct current
Transponder	mode III identification friend or foe
Navigation	dead reckoning/global positioning system/ground track
Data Link	C-Band and UHF Tadiran/MKD-200/MKD-400 Versatron/DS-12
Sensors	visible light/infrared
Miscellaneous	
Deployment	shipboard—landing platform docks, land based
Launch and recovery	RATO/runway/pneumatic net/runway/hook
Operation	remote control or pre-programmed
Lightning protection system	yes
Releasable imagery	yes
Sensor imagery	C-Band
Command and control	C-Band/UHF

APPENDIX E. MAGTF IMAGERY INTELLIGENCE PLANNING CHECKLIST

This appendix identifies typical IMINT planning actions of the MAGTF G-2/S-2, its IMINT staff, other key G-2/S-2 intelligence staff officers, the intel bn commander/intelligence support coordinator, the imagery intelligence platoon, and subordinate units' intelligence officers during each phase of the MCPP.

MCPP Step	Actions of MAGTF Staff	Actions of MAGTF G-2/S-2 and Intel Bn	
Mission Analysis	Identify the higher headquarters' (HHQ)/supported headquarters' intent. Identify tasks. Determine the AO and AOI. Review available assets and identify personnel and equipment resource shortfalls. Determine constraints and restraints. Determine recommended commander's critical information requirements (priority intelligence requirements, friendly force information requirements, essential elements of friendly information). Identify requests for information. Determine assumptions. Draft the mission statement. Present a mission analysis brief. Draft the warning order. Convene/alert red cell (if appropriate). Begin staff estimates. Refine the commander's intent. Develop the commander's planning guidance.	Review HHQ and MAGTF standing intelligence plans (e.g., Annex B to an OPLAN), pertinent memorandums of understanding, etc. Assist with determination of the MAGTF AO and AOI. Assess NIMA, combatant command's and other external organizations' imagery coverage of the AO and AOI. Provide digital imagery data and other IMINT products to support initial planning (ensure needs of subordinate commands are met). Determine specified, implied, and essential IMINT tasks. Begin development of proposed IMINT concepts of operation; obtain G/S-2 approval. Identify organic/supporting IMINT elements and imagery points of contact in all subordinate units; determine operational status of each; determine personnel and equipment deficiencies (special attention to data management, production, and distribution). Identify JTF/multinational imagery interoperability issues; provide recommendations.	Establish/review/update the MAGTF IPL SOP and database; special attention to— • Identify imagery support requirements. • Prepare imagery data profiles. • Populate IPLs. • Digitize relevant imagery and geospatial products. • Identify external organizations' IMINT production plans and assess against MAGTF's initial requirements; determine deficiencies; initiate augmentation requests (coordinate with intelligence operations officer). • Assign/task-organize organic IMINT elements. • Validate/update JTF IMINT tactics, techniques, and procedures and MAGTF IMINT SOP (coordinate with HHQ and subordinate units). • Validate and prioritize IMINT requirements; special attention to those needed for COA development. • Begin development of IMINT operations plan; issue orders to IMINT production elements (coordinate with P&A cell). • Determine initial IMINT CIS requirements and dissemination plan; identify deficiencies (coordinate with dissemination manager). • Validate IMINT database management procedures (coordinate with JTF). • Ensure subordinate units' IMINT POCs kept advised of actions and developments.

MCPP Step	Actions of MAGTF Staff	Actions of MAGTF G-2/S-2 and Intel Bn	
Course of Action (COA) Development	Continue intelligence preparation of the battlespace (throughout all steps of the planning process). Array friendly forces. Assess relative combat power. Centers of gravity and critical vulnerabilities analysis. Brainstorm possibilities. Develop roughcut COA(s). Commander's input. COA(s) refinement. COA(s) validation. COA(s) graphic and narrative development. Prepare and present COA(s) briefing. Commander selects/modifies COA(s).	Assist with development and continued updating of the intelligence estimate. Develop an IMINT concept of operations for each COA; begin preparation of Appendix 7 (IMINT) and Tab C (UAV and other Aerial Reconnaissance Plans) to Appendix 14 (Recon and Surveillance Plan) to Annex B (Intelligence). Assist the intelligence section and other staff sections with COA development. Determine IMINT capabilities required for each COA.	Assist with the IMINT and related portions of Appendix 11 (Intelligence Estimate), Appendix 14 (Reconnaissance & Surveillance Plan), Appendix 16 (Intelligence Operations Plan), and Appendix 17 (Support to Survival, Evasion, Resistance, and Escape) to Annex B. Assist intelligence section with development of other portions of Annex B. Coordinate production of necessary IMINT products for each COA. Ensure subordinate units' IMINT POCs kept advised of pertinent actions and developments.
COA Analysis	Conduct COA analysis wargaming. Refine staff estimates and estimates of supportability. Develop concepts based upon warfighting functions (as required). Prepare COA analysis brief.	Complete IMINT estimates of supportability. Assist intelligence section with completing the intelligence estimate and the friendly intelligence estimate of supportability. Continue to monitor and update IMINT production operations.	Ensure subordinate units receive necessary IMINT products; verify understanding; identify/update subordinates current IMINT IRs. Validate and update IMINT information requirements. Ensure subordinate units' IMINT POCs kept advised of pertinent actions and developments.
COA Comparison and Decision	Evaluation of each COA. Comparison of COAs. Commander's decision. Issuance of warning order.	Assist intelligence section with evaluation and comparison of each COA. Continue development of Appendix 7 and Tab C to Appendix 14 to Annex B consistent with the selected COA. Continue providing IMINT assistance to appendices 11, 14, 16, and 17 to Annex B. Update, validate, and prioritize IMINT information and production requirements for the selected COA; issue orders as appropriate to IMINT elements. Coordinate IMINT element task-organization needs associated with the selected COA. Validate MAGTF IMINT IRs.	Continue coordination with the G-6/S-6 regarding IMINT CIS requirements; coordinate with G-1/S-1 as necessary for physical couriering of IMINT products to subordinate units. Continue coordination with the G-4/S-4 regarding IMINT supply and transportation requirements. Review actions associated with satisfying IMINT personnel and equipment deficiencies associated with the selected COA. Ensure subordinate units receive pertinent IMINT products; verify understanding; identify/update subordinates' current IMINT IRs. Ensure subordinate units' IMINT POCs kept advised of pertinent actions and developments.
Orders Development	Commander's intent is refined. Concept of operations turned into an operations order or a fragmentary order. Staff estimates and other planning documents are updated and converted into OPORD annexes and appendices. Commander approves OPORD.	Complete development of Appendix 7 and Tab C to Appendix 14 to Annex B; ensure copies provided to subordinate units and are understood. Provide final IMINT support required for Appendices 11, 14, 16, and 17 to Annex B. Update, validate, and prioritize IMINT information requirements and associated collection operations. Maintain coordination with external IMINT organizations.	Ensure pertinent IMINT products are disseminated to all subordinate units. Complete actions associated with personnel and equipment augmentation, interoperability issues, multinational dissemination, etc. Complete IMINT-related CIS, transportation, and supply actions. Monitor ongoing IMINT production operations; update and issue orders as appropriate to IMINT elements.

MCPP Step	Actions of MAGTF Staff	Actions of MAGTF G-2/S-2 and Intel Bn	
Transition	Transition brief Drills Plan refinements (as required)	Assist intelligence section with transition brief. Modify IMINT plans as necessary. Monitor ongoing IMINT collection and production operations; update and issue orders as appropriate to IMINT elements.	Ensure all IMINT POCs in JTF, other components, and subordinate units fully understand plans and standing requirements, and ensure they have received necessary IMINT products. Participate in drills, as appropriate. Remain engaged in MAGTF future plans activities.

APPENDIX F. IMAGERY INTELLIGENCE REPORT FORMATS

Section I. Reconnaissance Exploitation Report (RECCEXREP)

PAGE 1 EXREP 15TH 102 CLASSIFICATION:_____ 831122 03346

UNCLASSIFIED EXERCISE NEVERLAND

MSG ID/RECCEEXREP/15TH/NO2222/3456

EFDT238442Z DEC 90

NARR: REF ITMOOS, LG ACTY NOTED THROUGHOUT TGT AREA

ITEM P6

ITM: 001 0380EX0000 CTY: MS 363219M1263214E

A. 52SDR46118324

B. 230422Z DEC 90

C. CAT: 06 Command Post.
   1. Mobile Command Post.
   2. Static, Camouflaged.
   3. 10 T-62 Tanks, 3 M-1979 SP Guns, 5 UAZ69As, 5 LG Tents, 2 Spoon Rests, 50 PERS (count approx).
   4. No defense noted.
   5. Terrain is flat with little vegetation, approx 13 km SE of post, A AAA site was noted.

NO REPORT TO FOLLOW

D. 1. ACFT was fired upon AAA site.
   2. 0081X.
   3. Yes.

PAGE 1 EXREP 15TH 102 CLASSIFICATION:_____ 831122 03346

Section II. Initial Photo Interpretation Report (IPIR) and Supplemental Photo Interpretation Report (SUPIR) Format

PRECEDENCE

FROM: IIIC

TO: REQUESTOR

INFO:

REF: (a) As applicable.

(A) CLASSIFICATION

(B) SECTION 01 OF 01 SECTION

(C) IPIR: FIRST IIP SER: UVO157 PRJ: RD MSN: Z198A DTZ: 75022W

(D) IMAGE QUALITY RANGE WAS GOOD TO EXCELLLENT. EIGHT OF TWELVE OF THE COLLECTION REQUIREMENTS WERE SATISFIED.

(E) PART I. MISSION HIGHLIGHTS

(F) NO EVIDENCE OF SURFACE-TO-SURFACE MISSILES OR RELATED ACTIVITY WAS NOTED. VEHICULAR AND TROOP MOVEMENT ACTIVITY IS VERY LIGHT. NO ANTIAIR ACTIVITY OR REACTIONS TO THE RECONNAISSANCE PLATFORM WERE OBSERVED.

(G) PART II. SIGNIFICANT RESULTS

(H) A. PERISHABLE ITEMS

(I) ITMOOA: 0213-OOOOO CAT: 80000 AIRCRAFT IN FLIGHT

(J) REQ: CTY: LA211929N1061934E UTM: MRG:

(K) STA: TRM AI NRG:

(L) AOB:
0001 CONF PA-23 INFLIGHT HDG NORTHEAST

(M) IMR: PAN FRM: 1011, 1012 URG
AID: E AO CL BB FRM TOT: 1035Z

(H) B. NEW ITEMS

(I) ITM002: 0213UV0006 CAT: 87200 PURTEE SAM SITE

(J) REQ: CTY: LA210815N1055619E UTM: MRG:

(K) STA: UCO

(L) DES: SA-O SITE IS BEING ESTABLISHED APROX ONE-HALF KM FROM THE RED RIVER. SITE CONSISTS OF SIX RVTD PSNS IN A STAR FORMATION. FULL DESCRIPTION NOT YET POSSIBLE. NO EQUIPMENT EXCEPT FOR CONSTRUCTION AND GROUND FORCE RELATED WAS IN THE AREA.

GFW:
0008 CONF DUMP TRUCK
0001 CONF ZAZ-7 CRANE
0001 PROB A-2 TRACTORURG:

(O) IMR PAN FRM: 976-980 TOT: 1039Z
AID: G AO SC SH BB

(H) C. CHANGE AND OB ITEMS

(I) ITM OO02: 0213-02351 CAT: 09100 WATERTON BARRACKS AREA

(J) REQ: 4A02316 CTY: LA221600N1053012E UTM: MTG:

(K) STA: OPR AI NAC DQ B1236 750102 NRG: NDA04/0014/5

(L) RMK: PREVIOUSLY REPORTED U/I ARMORED EQUIPMENT HAVE NOW BEEN IDENTIFIED AS SWG-99 TANKS.

GFW: AREA A-REGT A
0103 CONF SWG-99 TANK
0092 CONF DTR-12 TRUCK
0002 CONF MT-3 CRANE

GFW: AREA B-REGT AREA NAC DQ B1236 750102
GFW: AREA C-REGT AREA NAC UP 298A 741209
GFW: AREA C-AAA BN NAC UP 208A 741209

(M) IMR: PAN FRM: 500.490-516 URG: 234118

AID: G AO CL BB FRM: 135-138 TOT:1025Z
IDC: 221615N1053045E MPR:

(N) EQM

(O) PART III. OTHER RESULTS

(P) A. Mission Requirements

(Q) Categorization of Target Entries. An introductory statement categorizing a set of like items to increase readability. DIAM 57-5 contains more detailed information on the structure of part III.

(R) PART IV. COLLECTION OBJECTIVES SATISFIED AND NOT SATISFIED

Explanatory Notes

1. ( ) Shown for explanation only. Line identification is not shown on an actual message.

2. The IPIR/SUPIR/MIPIR format has been revised to accommodate the growth of automated intelligence systems. Detailed definitions and instructions for completing them are included in DIAM 57-05. However, as a user's guide to understanding the reports, the following definitions are provided.

Cable Line

Ref

(A) Self-explanatory

(B) Self-explanatory

(C) Report Type

Reporting Organization

Report Number

Reports will be numbered sequentially by the producing unit. A two-character alpha unit identifier as listed in DIAM 57-5 will be used followed by a four-digit sequential number.

Reconnaissance Project Identification

Two characters indicating the project of which this mission is part. This stands for mission independent. Project identifiers may be derived from DIA reconnaissance program directives or DIAM 57-5-1.

Mission Number

Date/Time Zone

(D) General Mission Statement

Free text reporting information applying to the entire mission such as graphic reference, sensors, sensor on/off times and coordinates, overall image quality, overall image scale range, other general mission data or any other information deemed useful. If the objectives of the mission and the requesting authority can be given (consider length and classification), these will be included. The general mission statement will be written as the interpreted mission and appropriate data will be reported.

(E) Part I. MISSION HIGHLIGHTS

Title for major division of the report.

(F) Textual Data for Mission Highlights.

Part I, Mission Highlights allows for a concise free text statement of the significant information derived from the mission. It may be used to highlight individual items reported

elsewhere in the message and to summarize information relative to a category of targets. Mission Highlights may also be utilized for summations of trends of individual categories such as logistics studies or combat information of a significant nature.

(G) Part II. SIGNIFICANT RESULTS

Title for second major division of the report.

(H) Categories of Items That May be Reported

A—Perishable Items. This section is for items of perishable intelligence value, including transitory targets.
B—New Items. This section is for items upon which the reporting organization has no previous image-derived data.
C—Change and OB Items. This section is for items that reflect significant changes since the last available interpretation and targets, which OB is required. For DOD combat reconnaissance programs, this section includes mission requirement objectives. A mission objective could also be reported under Perishable Items of Damage Assessment.
D—Bonus Items. This section includes significant changes to any known installation that is not a specified mission requirement objective.
E—Damage Assessment. This section is for the description of damage to targets from nonnuclear attacks. This section includes known strike objectives not damaged.

(I) Identification Data.
Item Number.
Basic Encyclopedia (BE) Number or Imagery Basic Encyclopedia Number.
Functional Classification Code. See DIAM 65-3-1.
Installation Name or Description of Object Imaged.

(J) Other Identification Data.
Requirement Number.
Country Code.
Geographic Coordinates.
Universal Transverse Mercator Coordinates.
Military District. Entered when applicable.

(K) Status/Activity Data

NEG. Negated (nonexistent). Target/installation does not exist at or near the coordinates given in the requirement.

UCO. Under Construction.

COM. Complete. The target/installation appears to be externally complete. Appears capable of operating but operational status cannot be determined.

UNK. Unknown. Status of the target cannot be determined.

MOP. Not Operational. Essential elements of a target/installation are observed not to be in operation; equipment essential to the operation of the installation is either missing or observed as not to be operational.

OPR. Operational.

OCC. Occupied.

DEC. Deception.

UNP. Unoccupied.

ABN. Abandoned.

RMV. Removed. Target/Installation has been razed, dismantled or moved.

TRN. Transitory. Fleeting targets or targets that appear to be only temporarily situated.

DMG. Damaged. Target is damaged to some extent, but it may be restored to usable condition.

DST. Destroyed. Target is so damaged that it cannot function as intended or be restored to usable condition.

CNA. Coverage not available.

Exploitation Level

AI -IPIR

AS-SUPIR

MI-MIPIR

Significance

The significance code indicates the interpreter's assessment of the degree of change in the installation status, capability or function since previous mission coverage. If a significance code in entered, the reference mission number and date will be entered. Codes are as follows:

NEW. Newly detected activity.

SIG. Significant change has occurred.

UNK. Significance of change is not known or change, if any, cannot be determined.

NAC. No apparent change.

Reference Graphic

When a national basic reference graphic, exists, the number may be required for certain specific programs. In all other cases, it will be left blank.

(L) Additional Interpretation Data
Additional photo interpretation data will be organized under one of the following codes.

DES. Physical description. A DES will be accomplished when an installation is covered for the first time, a basic description of the installation has not been previously written, the installation reflects a significant physical change, or first reporting an installation as abandoned or destroyed.

RMK. Remarks. This prefix will be used when providing less than a complete description of a known target and/or additional explanatory comments relating to status/activity.

Only a DES or RMK will be used for each entry, not both. If NAC is entered on the status line, a DES will not be used.

The remark will include the project code and mission numbers of the coverages used to prepare the report in those cases where more than one mission is used.

For multiple reporting (MIPIR), the actual OB count will be taken from a representative mission flown during the reporting period.

OOB Designations

MIS. Missile and missile related equipment.

AOB. Air OOB.

NVL. Naval and merchant vessels.

GFW. Ground force weapons and equipment.

ELC. Electronic OOB.

AAA. Antiaircraft OOB.

DMY. Dummy.

OBJ. Associated objects. Information relative to objects and equipment not reported under OOB entries.

Area Delineation

Refers to area delineation of the National Basic Reference Graphic or other descriptive location data. When Unpegs are not available, locational reporting is permitted (e.g., assembly area). Multicoverage dates may be included following each locational entry or as unique entries.

(M) Imagery Reference Data

IMR. Imagery Reference. A minimum of one IMR line is required; however, more lines may be required to indicate different coverage. For MIPIR, only those missions that contributed to a specific degree are entered on the IMR line. Initial information in the IMR line may include date of coverage, project code, mission number, and camera station. The following coded items may then be used.

IMR. Frame number.

SLR. Slide-looking radar.

INF. Thermal.

URG. Universal reference grid. Six position URG coordinates (see DIAM 57-23).

AID. Additional imagery data. AID is used to provide interpretability data. Interpretability codes are as follows:

E-Excellent

G-Good

F-Fair

P-Poor

Extent of Coverage and Mode

A-Complete coverage/stereo

B-Complete coverage/partial stereo

C-Complete coverage/mono

D-Partial coverage/stereo

E-Partial coverage/partial stereo

F-Partial coverage/mono

Type of Coverage

O-Oblique

V-Vertical

Weather Conditions

CL-Clear

SC-Scattered

HC-Heavy Clouds

HA-Haze

Other Conditions

SN-Snow

SH-Shadow

OL-Degrading obliquity

SD-Semidarkness

BL-Blurred image

TR-Terrain masking

HD-Heavy smoke/dust

Type of Film

B-Black and white

C-Natural color

G-Green record

I-Color rear infrared

R-Red record

T-Thermal

S-Radar

N-Nonstandard

(Note: For stereo or partial stereo, two letters will be used, one for the first frame and one for the second frame; e.g., BB, black and white on both frames.)

FRM. Additional frame reference for a given target.

TOT. Time over target.

IDC. Imagery derived coordinates, derived from comparing imagery with a map or chart.

MPR. Map reference.

PPC. Precision photo derived coordinates.

(O) Part III. OTHER RESULTS. Third major division of the report, as indicated by the sample; Part III may be omitted.

(P) A. Mission Requirements. Provides for reporting items/targets not properly placed in Part II.

(Q) Categorization of Target Entries. The format in part IV will contain collection objectives satisfied and not satisfied, plus a textual statement indicating any reasons for non satisfaction. Items contained in part IV can be understood from the codes listed earlier.

(R) Part IV. COLLECTION OBJECTIVES SATISFIED AND NOT SATISFIED. Part IV of the format will contain collection objectives satisfied and not satisfied, plus a textual statement indicating any reasons for non satisfaction. Items contained in part IV can be understood from the codes listed earlier.

APPENDIX G. IMAGERY INTELLIGENCE SUPPORT TO INTELLIGENCE STUDIES

IPB is a systematic, continuous process of analyzing the threat and environment in a specific geographic area. It supports commander and staff estimates and decisionmaking. Applying the IPB process helps the commander selectively apply and maximize combat power at critical points in time and space on the battlefield. When taken in IPB's entirety, imagery plays a small and focused role. However, imagery's role is vital, especially in terrain analysis and mapping tasks.

IMINT Support to Drop Zone Studies

A drop zone (DZ) is a specific area where troops (e.g., a radio reconnaissance team), equipment or supplies are air-dropped. DZs are preplanned locations determined after careful consideration. IAs take on an important role and must consider the following DZ factors:

- Minimum DZ dimensions (DZ length/width computations).
- Maximum slope percentage for DZs is 30 percent.
- Surface and obstacle considerations.
- DZ accessibility and trafficability.
- Easy exit from the DZ.
- Type of aircraft employed.
- Altitude at which air delivery is to be made.
- Types of loads to be delivered.
- Availability of adequate aircraft approach and departure routes.
- Method of airdrop: free drop, high or low velocity.
- Potential approaches and exits.
- Proximity to mission objective.
- Enemy disposition.
- Alternate DZs and landing zones (LZs).
- Supporting fires (in coordination with the G-3/S-3 and the FSC).

DZ Length/Width Computations

The request for DZ identification and supporting intelligence will usually include the rate of speed the aircraft will fly over the proposed area and the amount of time required to deliver a load. The IA (or all-source intelligence analyst) must be informed of the prevailing wind velocity and wind direction, which have an impact on the aircraft's ground speed. When the wind velocity at the delivery altitude cannot be determined, use the aircraft's air speed as the ground speed. Use the steps outlined below to compute the DZ size.

Step 1. Compute the minimum required DZ length by multiplying the ground speed of the aircraft by the time needed to release its cargo.

Length computation formula: L = R x T

L = DZ length (in meters)

S = Aircraft speed in knots

R = Ground speed of aircraft: S x .51

.51 = Conversion factor of knots to meters per second

T = Time required for aircraft to release its cargo and personnel

Step 2. Compute ground speed R

R = (S ± wind speed) x .51

Add tail wind component of wind velocity to aircraft speed or subtract head wind component of wind velocity from aircraft speed (see figure G-1).

Convert knots to meters per second by multiplying aircraft speed by .51.

Step 3. Calculate DZ length (L) by multiplying R x T. The result is in meters. Always round up the required DZ length to the nearest meter.

EXAMPLE: If the aircraft speed is 110 knots, head wind is 20 knots, and drop time is 20 seconds, the required length of the DZ is:

L = R x .51 x T

L = (110 - 20) x .51 x 20 = 918 m

Step 4. Compute required DZ width. The required DZ width depends upon the method and/or type of airdrop, wind drift, and formation of the aircraft, usually provided in the request. When it is not specified, you must give the requester the widths of all proposed DZs that also possess the required length. The wind drift formula is used to determine the minimum required width of a DZ. In this formula, K is a constant that represents the characteristic drift of a certain model parachute. Always round up the required DZ width to the nearest meter.

Wind drift formula: D = K x A x V

D = Width of DZ (in meters)

K = 4.1 (constant) for personnel parachutes

2.6 (constant) for all other parachutes

V = Velocity of surface wind (in knots)

A = Altitude of the aircraft (in hundreds of feet above ground level [AGL])

EXAMPLE: An aircraft flying at 2,000 feet AGL is to drop a cargo load with wind speed of 11 knots.

D = K x A x V

K = 2.6 (G13 cargo parachutes)

V = 11 knots

A = (2,000 ft /100) = 20

D = 2.6 x 11 x 20 = 572 m

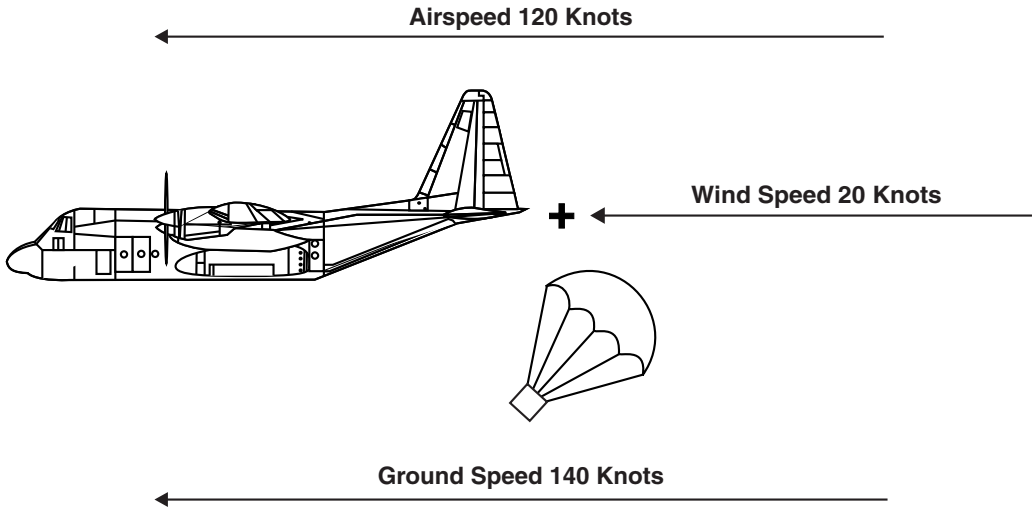


Figure G-1. Prevailing Wind Speed.

Step 5. Now that the required dimensions are known, the IA searches the imagery (or map if imagery is not available) for suitable DZs. Using a photo interpreter (PI) scale or equivalent scale, the IA measures the potential DZ length on the imagery and then computes the ground distance (GD) in meters. Always round down the potential DZ length to the nearest meter.

Imagery length computation formula:
GD = PD x DPRF

Map length computation formula:
GD = MD x DMRF

GD = Ground distance (length) in meters

PD = Photo distance (if in feet, then x .3048 = Conversion factor of feet to meters)

DPRF = Denominator of the photo representative scale

MD = Map distance

DMRF = Denominator of the map representative scale

Scale = 1: DPRF or DMRF

EXAMPLE: An image has a scale of 1:25,000. Using your scale, you measure a potential DZ to be .06 foot.

PD = .06 ft

DPRF = 25,000

GD = .06 ft x 25,000 x .3048 = 457.2 m = 457 m

Step 6. The IA now measures the potential DZ width on the imagery (or map if imagery is not available) and then computes the ground distance in meters the same as in step 5 above. Always round down the potential DZ width to the nearest meter.

EXAMPLE: An image has a scale of 1:25,000. Using your scale you measure a potential DZ to be .04 foot.

PD = .04 ft

DPRF = 25,000

.3048 = Conversion factor of feet to meters

GD = .04 ft x 25,000 x .3048 =
304.8 m = 304 m

Step 7. In those cases where the plot of the potential DZ is irregular in shape, the lengths and widths will be determined as shown in the sketch in figure G-2. The usable length is measured along a centerline while width used is the minimum dimension of the plotted areas with ends perpendicular to the centerline. Width is 140 meters in this example and length is 380 meters.

Step 8. Compute flight time. For safety requirements, a DZ should be as large or larger than the commander's request. Normally an area 460 meters long and 180 meters wide is the minimum requirement for the delivery of supplies. If a DZ of the desired length is not available, the flight time over the DZ (whatever its length) must be computed to determine how much of the load can be released in

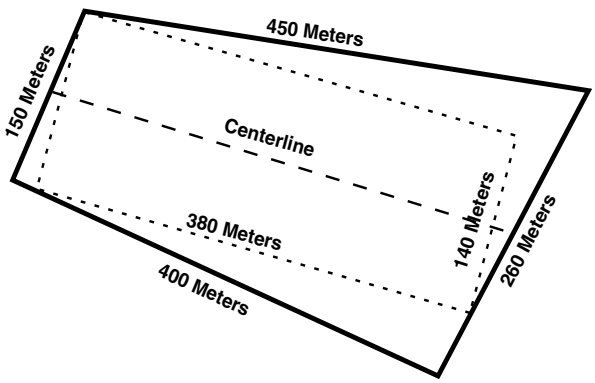


Figure G-2. Irregular-Shaped DZ.

one pass and/or how many passes must be made to release the entire load. Always round the flight time down to the next lower whole second.

Flight time computation formula: $T = \frac{L}{R \times .51}$

T = Time over the DZ in seconds

L = Length of the DZ in meters

R = Aircraft ground speed in knots

.51 = Conversion factor of knots to meters per second

EXAMPLE: An aircraft is flying at 105 knots over a DZ that measures 150 meters long.

L = 150 m

R = 105 knots x .51 = 53.55 = 53 m/seconds

$T = \frac{150}{(105 \times .51)} = \frac{150}{53} = 2.83 = 2$ seconds

Slope Calculations

After the DZ area has been determined, the IA computes the slope. For this task a map of the area is required. The slope of a DZ should not be more than 30 percent. Always round up the slope to the nearest percent. Both vertical distance (VD) and horizontal distance (HD) must use the same unit of measurement (feet or meters). Use 3.281 as the conversion factor from meters to feet or .3048 to convert feet to meters. Use the following formula to compute the terrain's slope, which will be expressed as a percentage:

$SL = \frac{VD}{HD} \times 100$

SL = Percent of slope

VD = Vertical distance of the DZ (altitude difference between each end of the DZ length)

HD = Horizontal distance of the DZ

100 = Conversion factor for percent

EXAMPLE: The length of the DZ is 900 meters, one end is at an altitude of 150 feet and the other end at 200 feet, the percent of slope is 1.7%, rounded up to 2%.

$SL = \frac{(200\ 150)}{(900 \times 3.281)} \times 100 = 1.7\% = 2\%$

The contour intervals on maps are in feet or meters. The bar scales are usually in meters, yards, statute miles or nautical miles. If the bar scale is used, a conversion from one unit of measure to another may have to be performed. If a Pl scale is used, be sure to multiply the measurements by the map scale. To determine slope using a map, refer to the following steps and figure G-3 on page G-5 and figure G-4 on page G-6.

Step 1. Determine the elevation of each point. Neither point is on a contour line, so it will be necessary to interpolate. Point Y is located on an intermittent stream symbol, confused with a contour line if care is not taken. The contour interval is 50 feet.

Step 2. Measure the distance between points X and Y using a piece of paper, Pl scale or boxwood scale. Make measurements from the center of one dot to the center of the other dot (see figure G-4 on page G-6). A tube magnifier may be required to exactly align the scale with the centers of the two points to accurately determine the distance found.

In figure G-4 on page G-6, the map distance (MD) is 2.95 centimeters (cm). GD is found by solving the following formula:

GD = MD x DMRF, the latter of which is 50,000

GD = 2.95 cm x 50,000 = 147,500 cm = 1,475 m

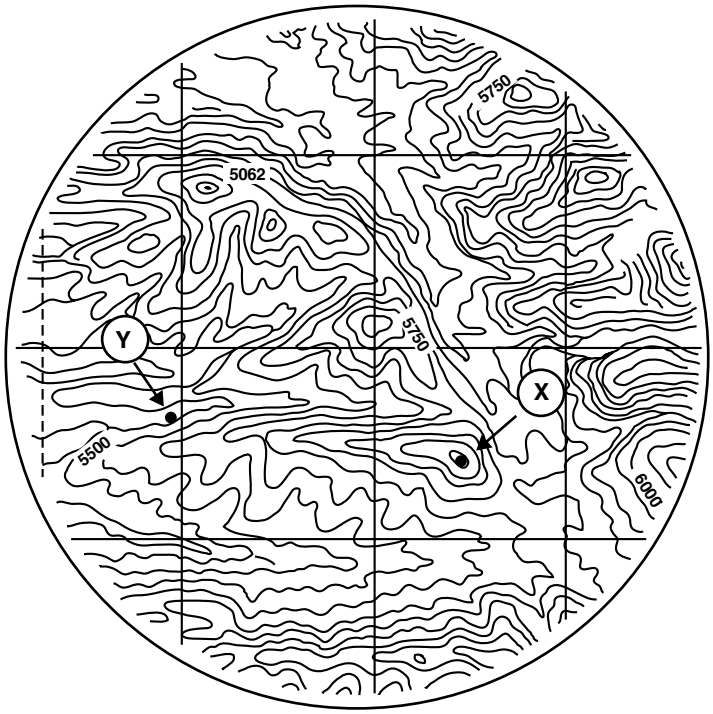


Figure G-3. Map Extract (map not to scale).

In comparing elevations and horizontal distance, elevation is in feet and distance in meters, so a conversion from one to the other is required.

GD = 1,475 m x 3.281 ft/m =
4,839.475 (rounded up to 4,840 ft)

Step 3. Use the slope formula:

VD = change in elevation from point V to point Y

$$SL = \frac{VD}{HD} \times 100 = \frac{X\ Y}{HD} \times 100$$

EXAMPLE: A DZ with a length of 4,840 feet has elevations of 5,925 feet and 5,475 feet.

$$SL = \frac{5{,}925 \text{ ft } 5{,}475 \text{ ft}}{4{,}840 \text{ ft}} \times 100$$

$$SL = \frac{450}{4{,}840} \times 100 = 9.2975; \text{ rounded up to } 10\%$$

SL = 10%

Surface and Obstacle Considerations

When both size and slope of a proposed DZ are acceptable, inspect imagery of the area for the presence of obstacles and potentially hazardous surface conditions. This requires examination of photography in stereoscopic pairs as well as a review of available maps. Two major reasons for the examination of imagery are to protect troops from injury during a drop and to prevent the unsuccessful drop of equipment. The most acceptable DZ is a flat, resilient surface without obstructions.

Unfavorable or hazardous surface conditions are normally provided by the terrain detachment, to include information on—

- Water.
- Marshland.
- Gullies.
- Drop-offs (cliffs).
- Dense trees.
- Dense low vegetation.
- Large rocks.

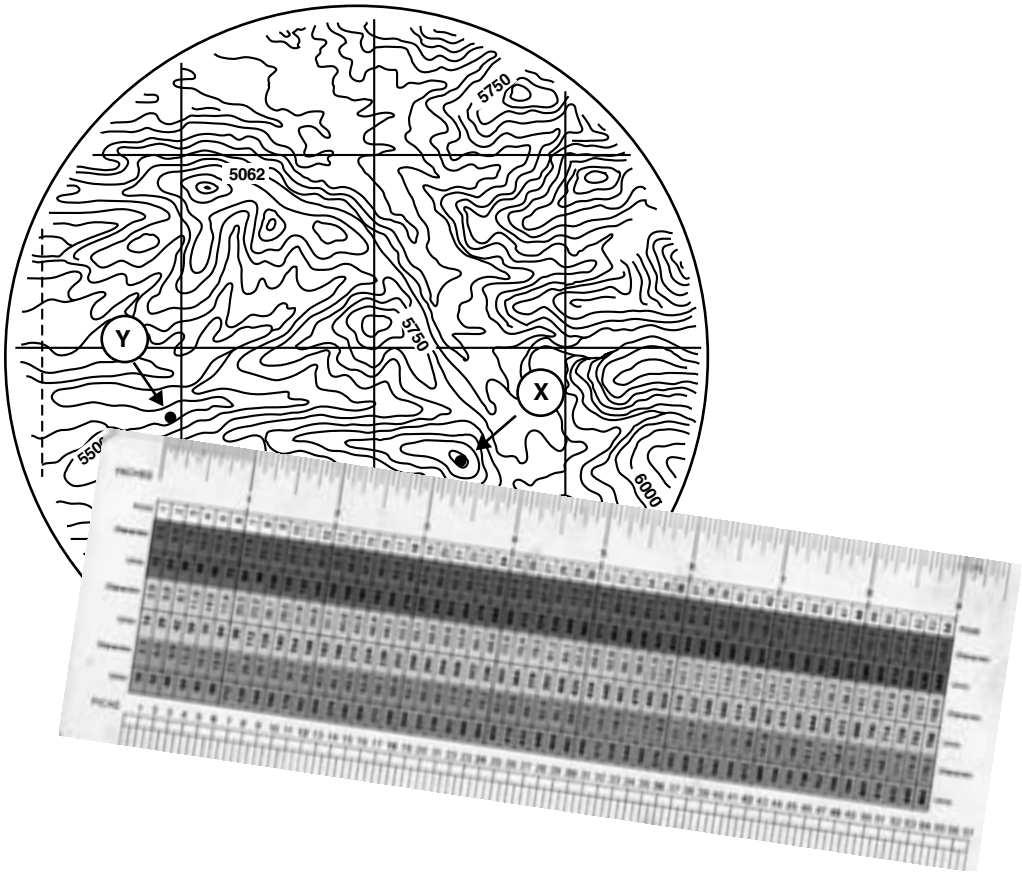


Figure G-4. Measuring from Dot to Dot (map not to scale).

Obstacles that are manmade features, such as—

- Power lines and poles.
- Buildings.
- Towers.
- Fences.
- Military impediments (e.g., stakes, barriers, barbed wire).

DZ Accessibility and Trafficability

A favorable DZ must have easy accessibility for both approach and exit. If possible, DZs near LOCs should be selected.

Certain questions must be answered before identification can occur; the tactical situation will add other questions:

- Will the approach involve more or less troops and equipment than the exit?
- Will the exit involve more or less troops and equipment than the approach?
- Will the approach or exit occur during daylight or night?

When troops are parachuted into a DZ, it is important they have an easy exit. The exit should be in the general direction supporting the ground tactical plan. When supplies or equipment comprise the load, personnel on the ground must be able to approach the area, recover the material, and then exit with the material. When evaluating a potential DZ for accessibility, the type of load will be a major consideration.

EXAMPLE: If wheeled vehicles are parachuted into a DZ, troops on the ground may be able to approach the DZ through a densely wooded area or up a steep slope. However, the vehicles may not be able to exit through the forest or negotiate the slope.

Related to accessibility is the trafficability of the soil. Swampy soil, or in some cases fine sand, may rule out the selection of a DZ. The parachuted equipment may bog down or troops may not be able to approach or exit the area rapidly. Therefore, trafficability of access routes must be considered to afford easy cross-country movement of vehicles and personnel in and out of the DZ.

DZ Reports and Overlays

Normally, the IA assists all-source intelligence and geographic intelligence (GEOINT) analysts with preparing a report in accordance with local SOPs. A primary DZ and alternate DZs will be selected that meet the specified intelligence requirements. This information is provided to the P&A cell OIC, who in turn recommends these to the ISC and G-2. Upon request, an overlay of the primary and alternate DZs will be prepared. GEOINT analysts generally will prepare this overlay.

IMINT Support to Helicopter Landing Zones Studies

A helicopter landing zone (HLZ) is a specified ground area for landing assault helicopters to embark or disembark troops and/or cargo. An LZ may contain one or more landing sites. Primary and alternate HLZs that meet the IRs will be identified, analyzed, and provided to the supported ground unit and aviation commanders. The ground unit commander (or helicopter unit commander) in coordination with the supporting air mission commander (AMC) will select the final location of the HLZ to best support the ground tactical plan.

General HLZ Criteria

In selecting an HLZ from maps, aerial photographs, and actual ground or aerial reconnaissance, the same criteria used for determining a DZ apply. Additional information, normally supplied by the ACE commander or AMC, should be used when selecting an HLZ. Information should include the type of HLZ and type and the number of helicopters used. HLZs have the following specifications:

- An HLZ is a helicopter landing area that encompasses one or more helicopter landing sites.
- A helicopter landing site is a subdivision of an HLZ. The size of a landing site depends on the number of landing points (LPs) and the size of the LPs.
- An LP is a designated or selected touchdown point where a single helicopter lands.

As previously stated, the size of the landing site will depend on the number of LPs within it, and the size of these LPs. As a guide, a helicopter requires a relatively level, cleared, circular area of 20 to 75 meters in diameter, depending on the type of helicopter. A helicopter requires more usable landing area at night than during the day. The criteria provided in figures G-5 on page G-8, G-6 on page G-8, and G-7 on page G-9, represent guidance on LP preparation. Helicopter units will designate the size (small, medium or large) to be used by their units for specific operations. Numerous considerations such as helicopter type, unit proficiency, nature of loads, and weather conditions may apply to size of LPs used. General distances between LPs within a landing site in daytime landing are as follows (measured center to center):

- Small landing points 80 feet, or 25 meters.
- Medium landing points 115 feet, or 35 meters.
- Large landing points 165 feet, or 50 meters.

Most helicopters cannot land or take off vertically when they are fully loaded; therefore, a larger area or a better approach is needed.

The ACE commander has the final authority in establishing the landing area criteria for assigned helicopters in daytime and nighttime missions. This may change from time to time, depending on how heavily loaded the aircraft will be, the place and time of landing, and the anticipated weather conditions. During specific missions, the

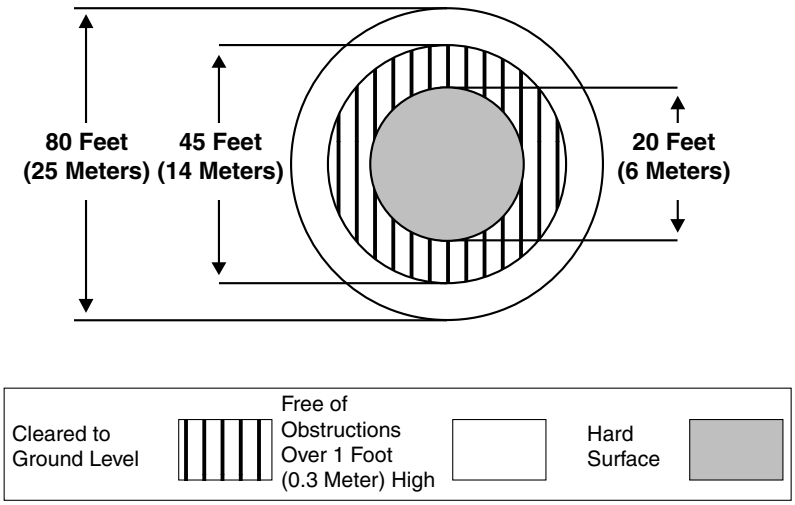


Figure G-5. Small Landing Point Dimensions.

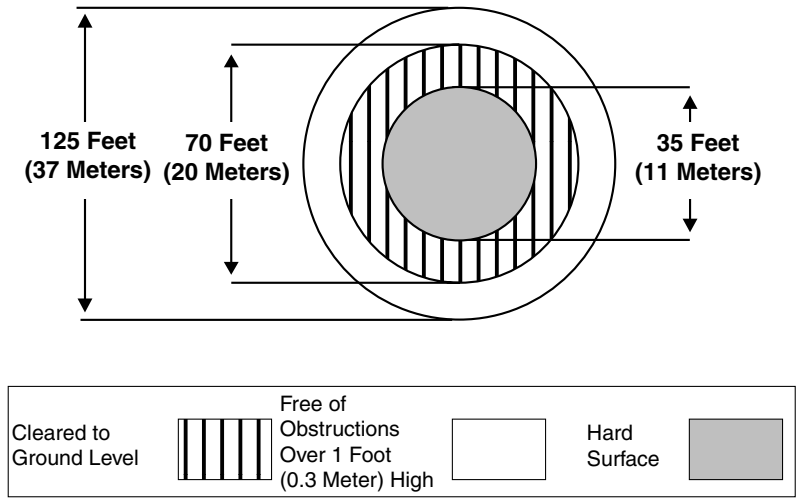


Figure G-6. Medium Landing Point Dimensions.

AMC may exercise this authority. For example, the area requirement may be larger when—

- A helicopter is heavily loaded.
- Helicopter cargo is sling loaded.
- Landing must be made at night or during other periods of reduced visibility.
- There are terrain obstructions or obstacles in the area.
- An area is located at high elevation.
- Temperature is hot or when humidity is high.

The ACE commander or AMC should provide the G-2 or ISC with required dimensions for all HLZs based on various flight and landing formations. This action will assist the IA and all-source intelligence analyst in locating potential HLZs.

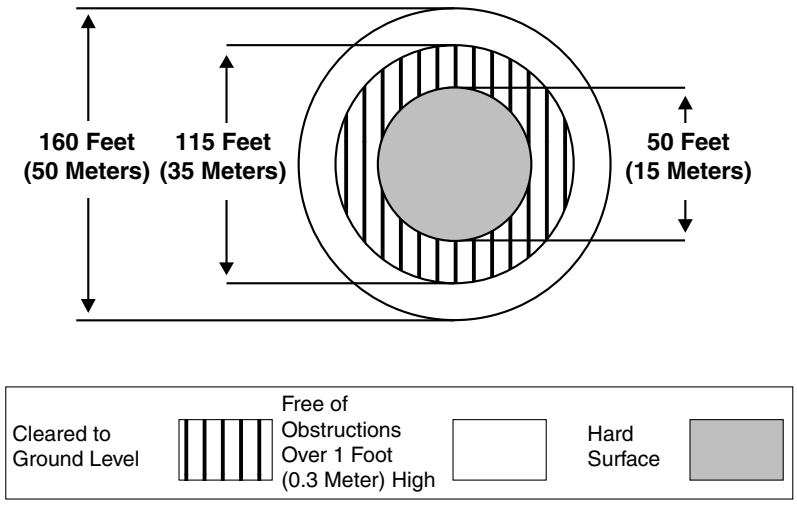


Figure G-7. Large Landing Point Dimensions.

HLZ Computations

In determining the HLZ area size, proceed in the same manner as for the DZ area. First, compute the required and then the potential HLZ areas. To determine the HLZ area, use the procedures shown below.

Step 1. Determine HLZ dimensions on photographs or maps. If the results are in fractions, round down to the nearest foot or meter. Use the same basis for all measurements (either feet or meters). FORMULA:

Potential HLZ length when measuring:

- Imagery: GD = PD x DPRF
- On a map: GD = MD x DMRF

Potential HLZ width when measuring:

- Imagery: GD = PD x DPRF
- On a map: GD = MD x DMRF

Step 2. Determine how may helicopters can land in the potential HLZ area in a two-trail formation during daytime. Round up converted LP dimensions.

Step 3. Determine the number of LPs (or helicopters) from front to rear of the potential HLZ. Round down number of helicopters. FORMULA:

LPs from front to rear = Potential HLZ length
Minimum recommended LP length

Step 4. Determine number of lateral LPs of the potential HLZ. FORMULA:

Lateral LPs = Potential HLZ width
Minimum recommended LP width

Step 5. Determine the total number of helicopters LPs of the potential HLZ. FORMULA:

Total # helicopter LPs = # of LPs from front to rear x # of lateral LPs

Slope Computations

The slope for an HLZ should not exceed 8 percent if the helicopter is to land. However, at the pilot's discretion it may be possible for a helicopter to hover just in contact with the ground on slopes greater than 8 percent.

When you compute the slope, do not depend entirely on the map. Study the area on imagery, too.

The map contour intervals may indicate that the percent of slope is sufficient, but sloping or rugged terrain can be seen only with a stereoscope.

When the slope is greater than the allowable 8 percent, report this to the requester. The site may still be usable if the commander chooses to hover the aircraft and load/unload troops and supplies by rope or ladder. When the slope is more than 8 percent, provide the requester with the exact percent figure so he can assess alternatives and decide. This is important because when the ground slope is less than 8 percent, helicopters should be landed up-slope. When the slope is more than 8 percent, helicopters should land side-slope. See figure G-8.

Now you are ready to compute the slope of each potential HLZ. Do this the same way as the DZs using the formula:

$$SL = \frac{VD}{HD} \times 100$$

When you compute the HLZ slope, consider the following:

- Direction of positive slope. This is important for the approach and exit direction.
- Number of aircraft used. The AMC will provide this information.
- The density altitude. The altitude, temperature, and humidity determine the density altitude (DA). For planning purposes, as DA increases, the landing area should increase proportionately.
- Approach/departure directions. When possible, approach and departure should be into the wind. However, if there is only one suitable approach direction due to obstacles, the tactical situation, or if it is desired to make maximum use of the available HLZ, most helicopters can land with a crosswind (10 knots or less) or a tailwind (5 knots or less). The same applies to departures from the HLZ.
- Loads. When fully loaded, most helicopters cannot ascend or descend vertically.

Aircraft Landing Zone

An aircraft LZ (also referred to as runway or landing strip) is a specified location used for landing aircraft. Potential aircraft landing zones are selected to meet the intelligence requirements of the supported ground and aviation units' commanders. Potential aircraft LZ locations will be identified and analyzed based on aerial imagery, current maps, and other available intelligence.

Aircraft Landing Zone Criteria

An aircraft LZ is established so aircraft can safely land and take off. It also provides guidance for aircraft while they are taxiing and parking. It has one or more landing strips. The landing strip consists of a runway and may include taxiways, parking points, and dispersal areas. Selection of a potential aircraft LZ depends on the type aircraft, runway dimension requirements (see table G-1), surface, and location.

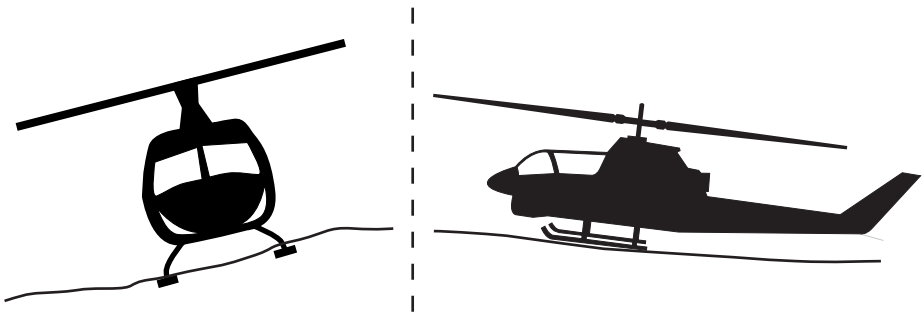


Figure G-8. Helicopter Landing on Side-Slope and Up-Slope.

Table G-1. Runway Dimension Requirements.

	Airfield Type	Runway Length (in feet)	Runway Width (in feet)	Runway Shoulder (in feet)
Forward Area	Attack & Utility	N/A	N/A	N/A
	Vertical	N/A	N/A	N/A
	Light Lift	1,200	60	10
	Medium Lift	2,500	80	10
Support Area	Attack & Utility	N/A	N/A	N/A
	Vertical Lift	N/A	N/A	N/A
	Light Lift	1,500	60	10
	Medium Lift	3,500	60	10
	Heavy Lift	6,000	100	10
	Tactical	5,000	60	4
Rear Area	Medium Lift	6,000	72	10
	Heavy Lift	10,000	156	10
	Tactical	8,000	108	20

Airfield Type

There are two types of aircraft landing zones, classified according to their size and degree of improvement:

A hasty landing strip has an unimproved surface, which normally is acceptable for marginal weather, but is unusable during prolonged poor weather. After a period of occupation, most pioneer landing strips (terrain permitting) can be improved to meet the requirements of a hasty landing strip. This strip has the following characteristics:

- Minimum length: 3,000 feet, plus a 10 percent overrun at each end.
- Minimum width: 50 feet, plus a 10 feet shoulder on each side.
- Minimum lateral clearance: 100 feet on each side of runway centerline.
- Has taxiways, parking areas, and may include dispersal areas.

A deliberate landing strip has an all-weather capability. As a minimum, it should have all the characteristics of a hasty landing strip, plus any other facilities needed to meet the standards required by any aircraft. A deliberate strip is usually a permanent installation with a control tower, hard surface runways, taxiways, and parking ramps.

Aircraft Landing Zone Computations

To determine the length and width of the area, use the same formula as for measuring a DZ or HLZ. Then identify the potential aircraft LZ by type.

EXAMPLE: If the photo scale is 1:20,000, the photo distance (length) is .08 feet and the photo distance (width) is .004 feet, then the potential aircraft LZ could be either a hasty or deliberate type depending on construction and facilities.

Slope Computations

In computing the slope (SL), the maximum slope for a potential aircraft LZ should not exceed 10 percent. Always round slope up to the nearest percent. Use the same formula as for computing SL of a DZ or HLZ:

$$\text{SL (expressed as a percentage)} = \frac{\text{VD}}{\text{HD}} \times 100$$

Surface and Obstacle Considerations

The surface of a potential aircraft LZ must be firm and smooth enough to allow heavily loaded aircraft to land, taxi, park, and take off without delay or damage to the aircraft. It should be located away from obstacles such as mountains, telephone wires, tall buildings, and trees. The area should be free of heavy rocks and stumps so troops can clear it easily. This is particularly important for pioneer and hasty strips, which may have to be established quickly. The area should be dry, as water or marshland can cause early erosion.

LZ Accessibility

An aircraft LZ should have convenient access to and from the area, such as roadways or other level terrain. If there are prevailing winds, the runway should be oriented, if possible, so that aircraft can land and take off into the wind.

The minimum size of an aircraft LZ depends on the type of loads, the direction and velocity of winds, and the condition of the ground. Consider the following factors in establishing an aircraft LZ:

- Soft, wet, slippery or any other unfavorable surface conditions will increase the length of the aircraft LZ.
- Crosswinds may require an increase in width of the aircraft LZ.
- Uphill take off and downhill landings will require longer runways. The maximum slope on any aircraft LZ should not exceed 10 percent.
- Obstacle clearance is measured from the obstacle to the approach and departure end (if there are obstacles at the approach and departure ends of the aircraft LZ). Ensure a 10:1 clearance ratio is obtained (same as used for an HLZ).

Aircraft Landing Zones Overlays

Per the intelligence production requirement, all-source intelligence analysts, assisted by IAs and GEOINT analysts, will prepare an overlay of the potential primary aircraft landing zone and an alternate aircraft LZ if deemed necessary. A relief and drainage overlay may also be provided. Aircraft LZs are normally referred to by their nickname or a color. Situation and time permitting, GEOINT analysts will prepare this overlay.

IMINT Support to Beaches Studies

A beach is the area extending from the shoreline inland to a marked change in physiographic form or material or to the line of permanent vegetation. In amphibious operations, a beach is that portion of the shoreline designated for landing of a tactical organization. A landing beach is that portion of a shoreline usually required for the landing of a battalion landing team. However, it may also be that portion of a shoreline constituting a tactical

locality (such as the shore of a bay) over which a force larger or smaller than a battalion landing team may be landed. A beach landing site (BLS) is a geographic location selected for across-the-beach infiltration, exfiltration or resupply operations. A beachhead is a designated area on a hostile or potentially hostile shore that, when seized and held, ensures the continuous landing of troops and materiel, and provides maneuver space requisite for subsequent projected operations ashore. Finally, a landing area is the part of the objective area within which are conducted the landing operations of an amphibious force. It includes the beach, the approaches to the beach, the transport areas, the fire support areas, the air occupied by close supporting aircraft, and the land included in the advance inland to the initial objective.

Beach Landing Site Factors

A BLS is a continuous segment of coastline over which troops, equipment, and supplies can be landed by surface means.

Primary and alternate BLS are selected and prioritized after considering the commander's intent and guidance, concept of operations and scheme of maneuver, enemy disposition, size of the area required, terrain features, weather factors, supporting fire, and proximity of the objectives. Amphibious operations require a detailed study of hydrography, weather, climate, and terrain. The terrain portion is primarily the responsibility of MAGTF GEOINT analysts. A tactical study of the terrain is prepared by all-source intelligence analysts with major assistance from IAs and GEOINT analysts. (See MCWP 2-12, *Intelligence Production and Analysis*, and MCWP 2-12.1, *Geographic Intelligence*, for additional information on tactical studies of the terrain.)

The landing force commander selects specific landing beaches from available beach landing sites. When the amphibious task force is composed of two or more attack groups with related landing groups, a landing area may be selected for each attack group. In this case, each landing group commander selects the landing beaches from within the assigned area.

The principal factors in the selection of landing beaches are—

- Suitability for beaching landing ships, landing craft, and amphibious vehicles.
- Beach trafficability.
- Suitability of offshore approaches.
- Number, location, and suitability of beach support areas and beach exits.
- Location, type, and density of beach obstacles, including underwater obstacles.
- Nature of the terrain immediately inland from the beaches.
- Suitability of LOCs, including roads, railroads, and waterways.
- Suitability of the beach from the standpoint of expected weather and tidal conditions.
- Known hostile force dispositions, strengths, and capabilities.

Beaches are categorized by their shape (see figure G-9 on page G-14):

- Concave (Point A to Point B).
- Convex (Point B to Point C).
- Straight (Point C to Point D).
- Irregular (Point A to Point D).

Beach types include the following:

- Coastal plain.
- Coastal ridge.
- Cliff or terrace.
- Coral reef.
- Glacial.
- River mouth or delta.
- Pocket.

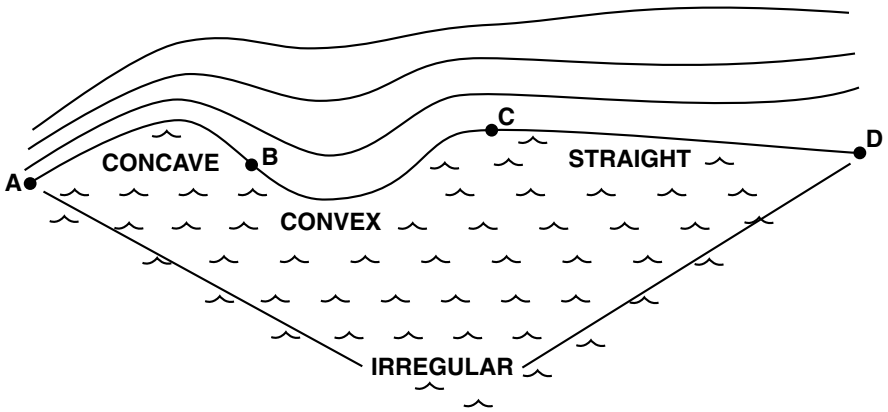


Figure G-9. Beach Catagories.

Coastal Plain Beaches

A landing on a wide coastal plain beach provides unrestricted maneuver room, and a subsequent advance from the beach can be made in any direction. Boundaries and objectives are more difficult to locate on this type of terrain; there are few prominent registration points for artillery, naval gunfire, and aerial bombardment. Usually there is no natural defensive terrain on the flanks of the beachhead, so more troops are required to protect the flanks. Some coastal plain beaches are near marshy and swampy terrain, which may hinder movement from the beach.

Coastal Ridge Beach

A coastal ridge beach has terrain that rises evenly to a considerable distance back from the beach that gives the defender excellent observation and fields of fire. More commonly, the coastal area remains flat for some distance and then rises in a steep gradient to a coastal ridge.

Cliff or Terrace Beach

A cliff or terrace beach is usually quite narrow. The delineation of a cliff beach from a terrace beach basically is established by the height of the landmass immediately behind the beach. Cliff beaches may have rocks and debris that accumulate by erosion of the adjoining severe terrain. The surface is made up of the same type of material as the major adjacent landform. If wave action is strong on a cliff beach, any fine material is washed away resulting in a beach covered with boulders or barren rock. Cliff beaches isolated from strong wave action are usually composed of sand and similar to coastal plain beaches as far as surface materials are concerned. A terrace beach may be composed of loose sand or rocks; it may be barren rock or strewn with boulders.

Coral Reef Beach

A coral reef beach is located in the coral region (normally between 30 degrees north latitude and 30 degrees south latitude) protected by a barrier reef with fringing reef along the shoreline, or it is located on an atoll. Any beach protected by a barrier reef is composed primarily of fine coral sand (coral skeletal remains, broken shells, and hardened algae) and is usually firm and narrow. When the beach or fringing reef is exposed to wave action, the foreshore is eroded. The coral reefs themselves normally present significant obstacles with abrupt seaward slope and the exposed offshore edge of the reef is steep. The upper surface of the reef may be extremely rough with

jagged coral formations rising above the surface and deep pits indenting the surface of the reef. An atoll is a ring-shaped coral island or group of coral islands enclosing a lagoon or another island. It has the same basic characteristics as the coral barrier reef.

Glacial Beaches

Glacial beaches are usually found in the higher latitudes, normally above 60 degrees north and 60 degrees south latitude. These beaches were eroded by glacial action and have round and irregular shorelines with numerous inlets; some may be quite deep, long, and narrow, with almost perpendicular, smooth mountain walls rising to great heights. This type of coast is very dangerous to navigation because of the islands and rocks off entrances to the inlets. The beach may be composed of material that has no geologic relationship to the coastline with depositions of material carried from the hinterland by the glaciers. This is often a mixture of silt, sand, gravel, and rocks.

River Mouth or Delta Beach

This type beach is easy to identify due to its proximity to the mouth of a major stream or river. It undergoes a greater physical change than the other beach types, and the foreshore is composed primarily of the type of sediment carried by the stream or river.

Pocket Beach

A pocket beach is found on many of the coasts throughout the world and has a wide range of composition and topography. The irregular coastlines, where pocket beaches are quite common, are made up of headlands and indentations with the pocket beaches found in the indentations. This type of beach is divided into two general areas: the end zones and central zone.

- The end zones are those areas on the flanks inside the beach termination points. They are protected from direct wave action by the headlands and subsequently the beach soil is usually fine sand.
- The central zone is that portion of the entire beach between the end zones and exhibits the same characteristics and soil conditions of any beach exposed to wave action. Any highlands behind the beach may provide the source material continually washed down and deposited on the beach. Lowlands behind the beach, however, will have little effect on its character.

A common problem affecting some pocket beaches is that many of the bays or other indentations fronting the beach may become blocked by sandbars built up by sand drifting along the coast in long shore currents. These sandbars may become attached to the mainland at the upstream end, and any open channel that might exist will occur at the downstream end. Sometimes these sandbars connect offshore islands to the mainland. Pocket beaches are usually concave shaped.

Beach Landing Site Criteria

The required beach area for amphibious operations is calculated based on original requester's guidance, type forces conducting the ship-to-shore maneuver, local SOPs and METT-T.

To identify whether an area is suitable for beach landings, intelligence analysts will require the following information:

- Minimum length of beachfront necessary.
- Types of equipment being landed.
- Types of transports to be used, to include length and width of each transport type.
- Transport capability. (Can it land on the beach? What minimum depth [draft] is required?)

Beach Landing Site Computations

Beach landing length is computed using the formula GD = PD x DPRF similarly as for DZs, HLZs, and aircraft LZs. Measurements are taken from one termination point to another (see figure G-10) and rounded down to the nearest meter.

- The beach termination points are the extreme ends of the beach selected. The total length of the beach is measured between these points following the natural coastline.
- The beach width is the horizontal dimensions of the beach measured at right angles to the shoreline from the line of extreme low water inland to the landward limit of the beach (the coastline). It usually will not be uniform and, therefore, is determined at various points along the beach.
- The beachhead line, roughly semicircular, encompasses that area near the coast large enough for the deployment of the assault force and its supplies and equipment, and usually includes terrain features that are the initial objectives of the assault force. The beachhead line, if established, must be held so the subsequent landing forces can land and deploy in proper battle order. Loss of or major enemy force penetration into the beachhead line places the entire amphibious operation in jeopardy.
- The beachfront extends from low tide limit to the high tide limit and usually coincides with the foreshore (see figure G-11).

Percent of Slope and Gradient Computations

Use the same formula as for determining percent of slope of a DZ, HLZ or aircraft LZ with different specifications. Measurements are made of the width of the beachfront. Always round up percent of slope to the nearest percent.

$$SL = \frac{VD}{HD} \times 100$$

SL = Percent of slope

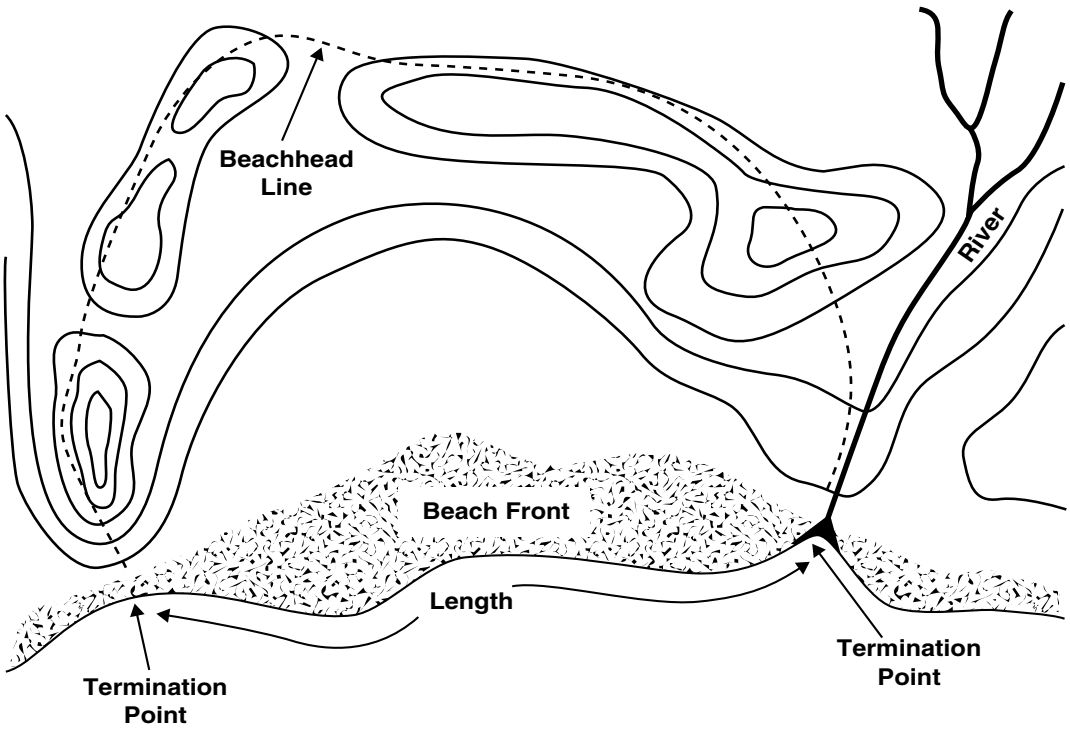


Figure G-10. Landing Beach Length.

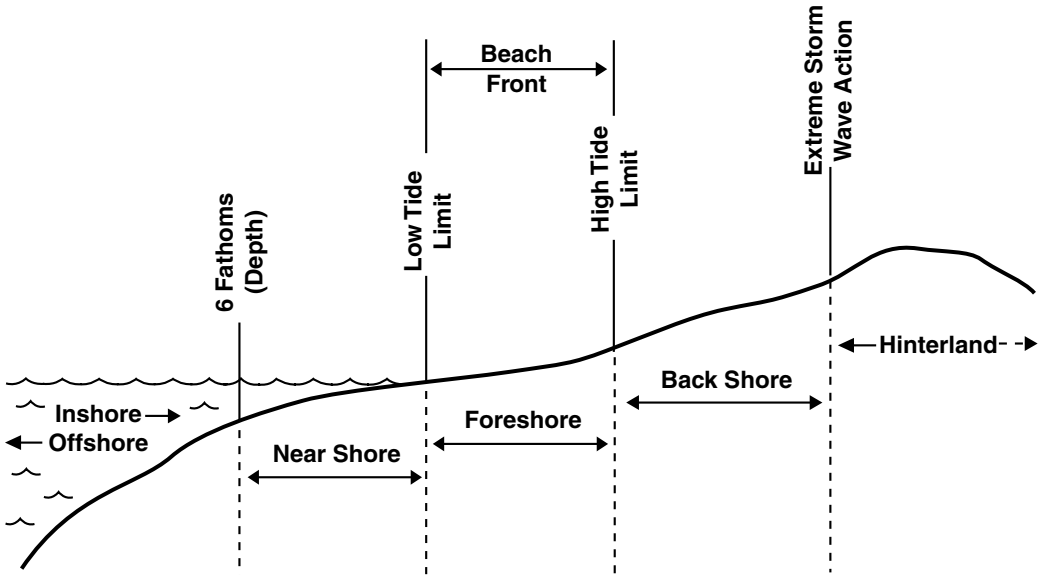


Figure G-11. Shores.

VD = The height difference of the beachfront, which is from the edge of the beachfront (low tide limit) to the high tide limit.

HD = The horizontal (ground) distance of the beachfront.

Combined offshore or foreshore/back shore beach gradient is expressed as a ratio of the rise in elevation of one unit of measure to the horizontal (ground) distance in a number of the same unit of measure; e.g., 1:15.

FORMULA:

$$\text{Gradient} = \frac{VD}{HD}$$

A quick way to obtain the gradient (1:) is to invert the fraction and divide the denominator by the numerator. Round up any fractions to the next whole number (e.g., 1:50.52 = 1:51).

EXAMPLE: If VD = 150 m and HD = 3,000 m

$$\text{Gradient} = 1: \frac{3{,}000}{150} = 1:20$$

In computing the combined foreshore/back shore gradient, measure from the shoreline to the nearest 20 meter contour line used for the start of the hinterland. You should transfer the 20 meter contour line from the map to the photograph by interpolation prior to making your measurement. The gradient is further expressed as shown in table G-2.

Table G-2. Beach Gradients.

Less than 1:120	Flat
1:120 to 1:60	Mild
1:59 to 1:30	Gentle
1:29 to 1:15	Moderate
1:14 or more	Steep

The depth lines or curves illustrated at 1, 2, and 3 fathoms (1 fathom = 6 feet) (see figure G-12 on page G-18) are established to determine the offshore gradient and to assist in the safe approach of the landing craft. The depth curves may be a series of dots (as shown) or solid lines.

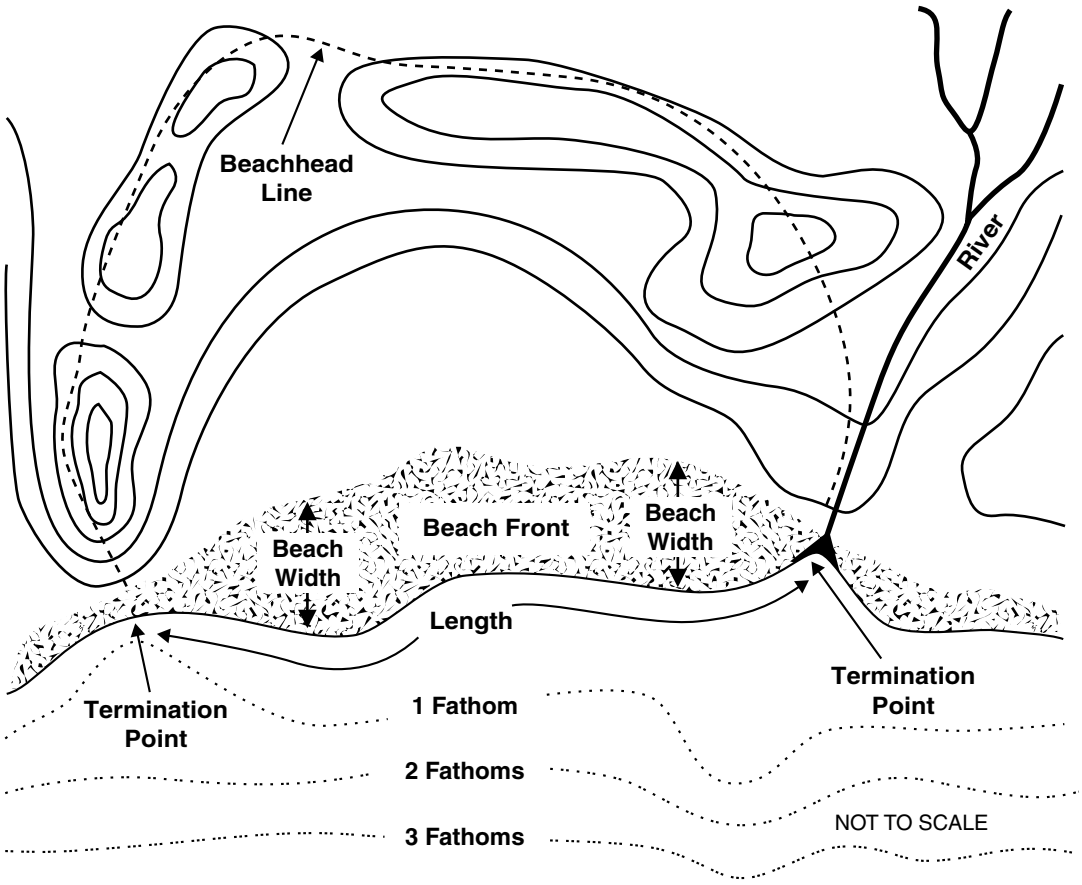


Figure G-12. Typical Beach Landing Area.

Surface and Obstacle Considerations

Normally, the surface condition of the combined foreshore and back shore areas is considered critical upon landing. The foreshore is generally white; the back shore begins where the beach discoloration changes from white to brownish gray and ends at the beginning of the hinterland by revealing a darker tone and taller vegetation on aerial photography.

Unfavorable or hazardous surface conditions include—

- Large rocks or reefs.
- Drop-offs (cliffs).
- Dense trees.
- Dense vegetation.

Obstacles include—

- Buildings.
- Military impediments (e.g., landing craft barriers, barbed wire).

BLS Accessibility

Because of the configuration of shorelines, usually the area most suitable for the execution of a landing operation is also the most easily organized for defense. The ideal beach for amphibious landing is one with—

- No obstructions in the sea approaches.
- Deep-water close inshore.
- Near shore gradients sufficiently deep for dry-ramp beaching of landing craft and ships.

- Soil composed of firm sand with gentle gradients or slopes.
- Small tides.
- No currents.
- No surfs.

The beach terrain should be—

- Gently rising, relatively clear, and with a firm surface that has adequate drainage.
- Flat or gently rising terrain, backed by a coastal range high enough to mask the landing area.

Ideal conditions are rarely found, so suitable areas must be evaluated to determine those that come nearest to optimum requirements. Other terrain considerations include:

- **Dunes.** Ground that is sharply broken by extensive dunes or a low coastal plateau provides the attacker with concealment from the defender's observation. The small compartments and corridors limit the range of defensive fire.
  - Transverse dunes are mounds of sand with their longest dimensions oriented at right angles to the prevailing wind. They usually have a steeper leeward slope than they have on the windward side.
  - Longitudinal dunes are sand formations whose longest dimensions are oriented in the same direction as the prevailing wind. They may have a symmetrical shape or may be without any particular shape at all. Longitudinal dunes may be over 100 miles in length. They are usually not backed by areas of standing water, such as swamps or marshes.
  - Because they are formed by windblown sand, coastal dunes are quite unstable landforms, appearing in one location as a transverse dune, only to disappear and reform as a longitudinal dune elsewhere. The winds responsible for their formation may also be the means for their destruction.
- **Mountains.** Mountains located directly on the sea usually limit the number of beaches large enough to accommodate a landing force of effective size. Where steep ground is lightly defended or neglected by the defender, a small force may seize it and gain surprise. Airborne or airmobile troops may be used to block the movement of defensive reserves to the landing area or to secure passes through the mountains and thus prevent the defender from interfering with the amphibious landing.
- **Sandbars.** These offshore sand formations are usually found near coastlines with a gentle beach gradient. During stormy weather the sandbars will be found further offshore than during calmer weather conditions. Sandbars paralleling the coast may cause a lagoon to form between themselves and the coastline; direct access to the shore is dependent on openings (channels) through the sandbar areas. The locations of these channels are highly variable, and current photography is required before the actual landing takes place. Soil analysis, beach materials, and other trafficability aspects are normally reported by terrain and soil analysts. However, IAs will determine beach exits (roads, airstrips, etc.).

Beach Landing Site Collection Checklist Preparation

A collection checklist must be prepared for each potential BLS using the following items:

- Identification. Local name and military designation.
- Location
  - Map reference—include series and sheet number(s) of both tactical and air/ground series.
  - Political unit, area, universal transverse mercator (UTM) coordinates, and geographic coordinates of the termination points.
  - Landmark reference—description and location of the landmark and azimuth and distance from landmark to termination point.
- Related water body or watercourses. Cross-reference to appropriate collection file.

- Length between termination points. Self-explanatory.
- Seashore form. Concave, convex, straight or irregular.
- Coastal terrain type. Emergent, submergent, compound, coral reef, delta, volcanic, fault, manmade, and so on.
- Alignment. High-water shoreline and low-water shoreline.
- Beach width at low water. Self-explanatory.
- Beach width at high water. Self-explanatory.
- Backshore
  - Slope.
  - Material (composition, texture, trafficability).
  - Obstacles.
  - Vegetation.
- Foreshore
  - Slope.
  - Material (composition, texture, and trafficability).
  - Obstacles.
  - Vegetation.
- Near shore. (Give alignment and distance from low water shoreline).
  - 10 m (5 fathoms) depth line at low water.
  - 6 m (3 fathoms) depth line at low water.
  - 4 m (2 fathoms) depth line at low water.
  - 2 m (1 fathom) depth line at low water.
  - Obstacles.
  - Reefs (near shore):
    - Type and location.
    - Distance from low water shoreline.
    - Length and width.
    - Slope (direction).
    - Depth to surface of reef at low tide.
    - Depth to surface of reef at high tide.
    - Height of surface above water at high and low tide.
    - Effects of surf.
    - Effects on tide.
    - Channel through reef (alignment, width, and depth at low water).
  - Reefs (offshore):
    - Type and location.
    - Distance from low water shoreline.
    - Length and width.
    - Slope (direction).
    - Depth to surface of reef at low tide.
    - Depth to surface of reef at high tide.
    - Height of surface above water at high and low tide.
    - Effects of surf.
    - Effects on tide.
    - Channel through reef (alignment, width, and depth at low water).
- Offshore Conditions
  - Water depth.
  - Offshore islands (location and characteristics).
  - Sandbars.
    - Location and distance from low water shoreline.
    - Length and width.
    - Consistency.
    - Slope (seaward and landward).
    - Passages (alignment, width, and depth).
    - Depth at high and low waters.
    - Obstacles (type, location, and characteristics).
- Beach features. Natural and manmade features such as cusps, runners, stream mouths, groins, piers, and outfall pipes, etc.
  - Type and location.
  - Number and extent.
  - Bypass possibilities.
  - Influence on operations.
- Tide
  - Type (diurnal, semi-diurnal, or mixed).
  - Type range (spring, topic, and diurnal).
  - Range.
  - Meteorological effects.
- Surf
  - Breakers (type, average height, distance formed from shore, f lines).
  - Period.
  - Width of surf zone.

  - Direction from which swells approach coast.
  - Weather and seasonal effects.
- Currents. Location, direction, and velocity.
- Beach exits.
  - Type and location.
  - Number and condition.
- Coastal terrain. Cross-reference to appropriate collection file.
  - Critical terrain features (location, type, bypasses, and influence on operations).
  - Obstacles (location, type, extent, bypasses, and influence on operations).
  - Cross-country movement (troops, wheeled vehicles, and tracked vehicles).
- Support area concealment and cover (location and type).
- Dispersal and storage area. Location and description.
- Availability of fresh water. Location and quantity.
- Defenses. Location and type.

Terrain overlays are normally prepared by the terrain analysis detachment and added to the checklist. Overlays include presentations depicting cross-country movement, vegetation, slope, soil drainage pattern, ridgelines, etc.

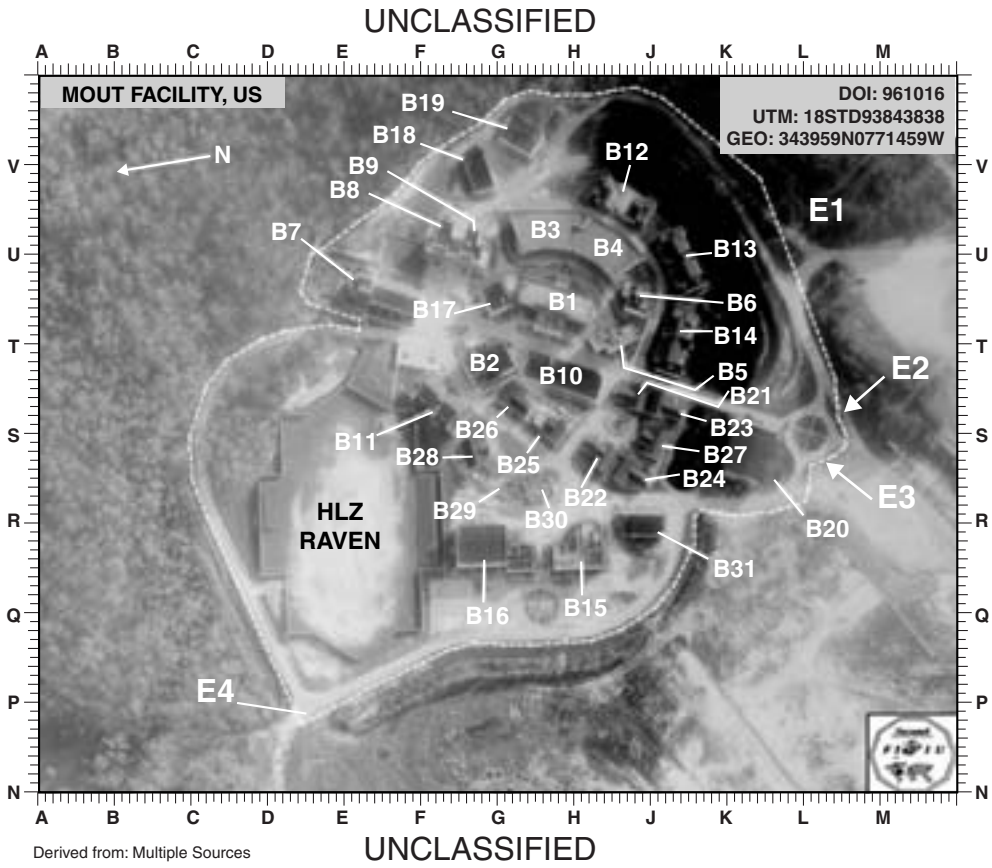
Beach Landing Site Overlays

IAs assist all-source intelligence and GEOINT analysts with preparing overlays of the proposed primary and alternate beach landing sites. Beach landing sites are referred to by their nickname. See MCWP 2-12.1 for information on preparation of overlays.

APPENDIX H. IMAGERY AND SUPPORTING INTELLIGENCE REPORTS

This appendix provides examples of MAGTF intelligence products derived from the fusion of available imagery and supporting IMINT and all-source intelligence reports. Such products support tactical planning and decisionmaking. The examples provided are:

- Image and supporting intelligence report for the MOUT facility, Camp LeJeune, NC.
- Image and supporting intelligence report for the Marine Corps Air Station, New River, NC.
- Image and supporting intelligence report for Helicopter Landing Zone Vulture, Camp LeJeune, NC.
- Image and supporting intelligence report for Onslow Beach North, Camp LeJeune, NC.
- Image and supporting intelligence report for Kin Red Beach, Okinawa, Japan.



MOUT FACILITY

Center Coordinates
UTM 18STD93843838
GEO 343959N0771459W

Map Reference
Sheet: Camp Lejeune MIM
Series: V742S
Edition: 1-DMA
Datum: NAD 83/WGS 84

Size
Length 1025 ft (312 m)
Width 800 ft (244 m)

Surface Material
Silty sand
Gravel

Remarks: The MOUT facility is located approximately 2 km ENE of OP-2. The primary use of the MOUT facility is combat training in an urban environment. The MOUT facility consists of 31 buildings of varying sizes and shapes. Roof types are a mixture of garbled and flat. The facility is surrounded by trees of varying heights. The exit from the MOUT facility is a loose surface road which provides access to Lyman road. Note: All building measurements are listed at length x width x height.

Exits

Anno. #	Type	True Bearing	Distance	Width	Surface Material
E1	Road, loose-surfaced	146	169.8 m (557 ft)	7.6 m (25 ft)	Earth and sand
E1	Road, loose-surfaced	175	163.1 m (535 ft)	6.4 m (21 ft)	Earth and sand
E1	Road, loose-surfaced	181	165.0 m (541 ft)	6.7 m (22 ft)	Earth and sand
E1	Road, loose-surfaced	281	204.3 m (670 ft)	5.6 m (18 ft)	Earth and sand

Remarks: E1 leads approximately 100 meters (328 feet) southeast to F-3 Range Road. E2 and E3 lead approximately 1.0 km (0.5 nm) to Lyman. E4 exits onto an unnamed road.

Buildings

B1—Three-story, T-shaped building (hotel), 120' x 58' x 37' (37 x 18 x 11 m) with near-flat roof. Helicopter landing point is painted with non-reflective white airfield markings and consists of a concrete slab roof. HLZ is 38' x 33' (12 x 10 m). OP building roof is outlined by a parapet with scuppers and a gutter. (Scupper is an opening in the wall of a building through which water can drain). The front portion of the roof is comprised of tube trusses or transverse monitors. Grappling and rappeling anchors are located throughout the roof.

B2—Two-story, square-shaped building (city hall), 72' x 60' x 31' (22 x 18 x 9 m) consisting of a near flat roof outlined by a parapet, however the NW corner is lower than the main roof. The roof has grappling and rappeling anchors throughout the roof. The corner of the roof is open to a crawl space.

B3, B4—Two-story, crescent-shaped buildings (apartment buildings) outer edge 121' x 60' x 31' (37 x 18 x 9 m) inner edge 84' x 60' x 31' (26 x 18 x 9 m) outlined by a parapet with scuppers. Grappling and rappeling anchors are located throughout the roof. The roofs are near flat with a ridge dissecting each building's roof, a near flat roof dissected by a ridge separates the two buildings.

B5—Three-story, basically rectangular-shaped building (office building) 72' x 36' x 38' (22 11 x 12 m). Grappling and rappeling anchors located on the SE and NW sides of roof. The southern end of the building is two stories, 23 ft (7 m) in height. An elevator shaft is located in the center of the roof.

B6—Two-story, "l"-shaped building (office building) 44' x 36' x 25' (13 x 11 x 8m). NW portion of the roof is a concrete slab.

B7—Rectangular "T"-shaped building with dormers (church building) 121' x 73' x 77' (37 x 22 x 23 m) with a gable roof made of asphalt and fiberglass shingles. Height of main building is 48 ft (15 m), steeple 29 ft (9 m).

B8—Three-story, irregular-shaped building (business/ residential building) 53' x 34' x 39' (16 x 10 x 12 m) with near flat roof. Grappling and rappeling anchors are located throughout the roof.

B9—Three-story, irregular-shaped building (business/ residential building) 50' x 47' x 39' (15 x 14 x 12 m) with near flat roof.

B10—Single-story, rectangular-shaped building (business/ residential building) 128' x 46' x 18' (39 x 14 x 5 m) with flat roof.

B11—Two-story, rectangular-shaped building (townhouse) 103' x 53' x 30' (31 x 16 x 9 m) has gable roof with dormer. Roof consists of fiberglass shingles reinforced by wood trusses.

B12—Two-story, rectangular-shaped building (townhouse) 103' x 53' x 30' (31 x 16 x 9 m), front and rear portions of building walls are incomplete. Gable-roofed dormer with fiberglass shingles and reinforced wooden trusses.

B13, B14—Two-story, rectangular-shaped buildings (townhouses) 103' x 53' x 30' (31 x 16 x 9 m) with gable roof and dormers. Roof consists of fiberglass shingles reinforced with wooden trusses.

B15—Two-story, irregular-shaped building (school) 88' x 73' x 25' (27 x 22 x 18 m) with near flat roof built up on A 2" slab of concrete. Rappeling anchors are located throughout the roof. Two fire escape ladders are located on the NE and SW sides of the roof.

B16—Two-story, irregular-shaped building (gymnasium) 128' x 74' x 25' (38 x 23 x 8 m) with a near flat roof, fire escape ladders located on the S side of the building.

B17—Two-story, square-shaped building (retail bank) 43' x 36' x 26' (13 x 11 x 8 m) with a near-flat roof. Grappling anchors located throughout the roof. Roof access by ladder is located on the NW corner of the building.

B18—Single-story, basically rectangular-shaped buildings with hipped roofs (service stations) 74' x 32' x 17' (23 x 10 x 5 m).

B19—Single-story, rectangular-shaped building (warehouse) 63' x 43' x 23' (19 x 13 x 7 m) with a near flat roof. Roof consists of standing seam metal on metal purlins. Purlins are horizontal timbers supporting the rafters of a roof.

B20—Single-story, square-shaped building (warehouse) 83' x 63' x 25' (25 x 19 x 8 m) with a near flat roof on metal purlins, with a mellaine (mellaine is a partial story between two main stories of a building). The MOUT CTF administration building is not a part of the MOUT training facility.

B21, B22—Single-story, "T"-shaped buildings with basements (residential buildings) 52' x 40' x 15' (16 x 12 x 5 m). Gable style roof is reinforced with wooden trusses. Chimney height extends 2 ft (.6 m) above the peak of the roof.

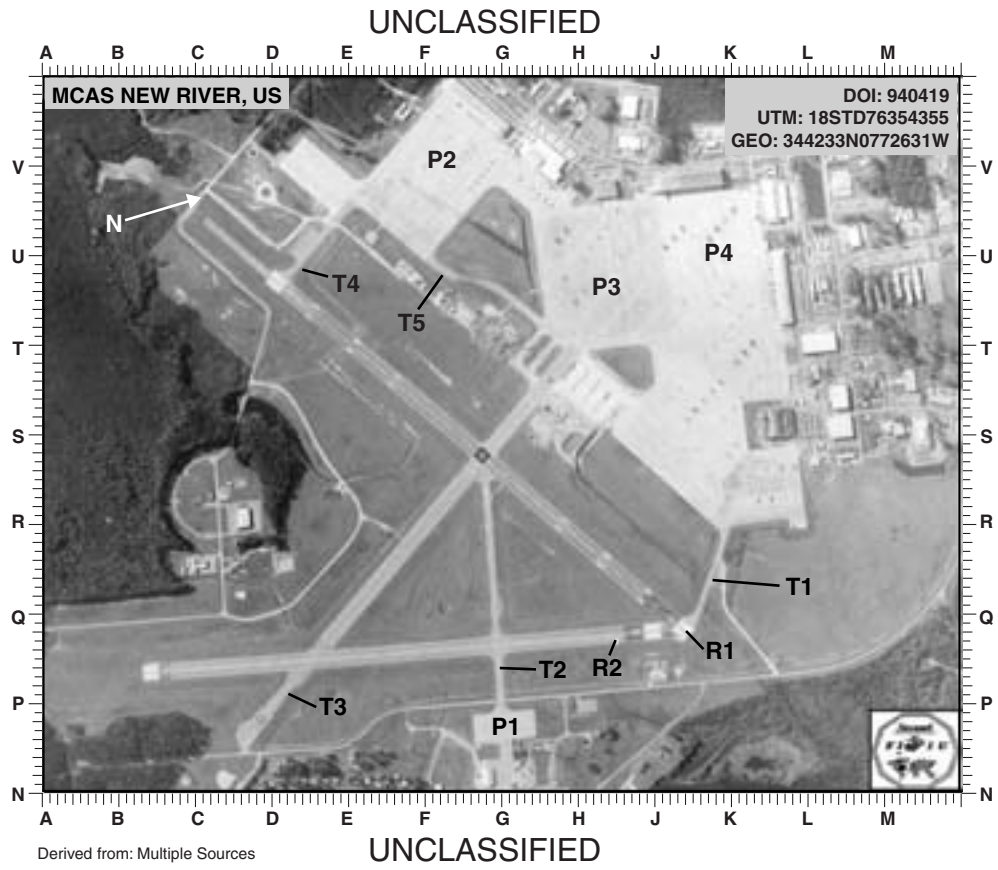
B23, B24, B26—Single-story, "T"-shaped buildings (residential buildings) 52' x 40' x 15' (16 x 12 x 5 m) with gable style roof reinforced with wood trusses. Chimney extends 2 ft (.6 m) above peak.

B25—Residential irregular-shaped building 52' x 40' x 15 (16 x 12 x 5 m) with a gable style roof reinforced with wood trusses.

B27, B28—Single-story, "T"-shaped buildings (residential buildings) 44' x 40' x 17' (13 x 12 x 5 m) with reinforced wooden trusses. Gable roofing consists of fiberglass shingles.

B29, B30—Small "T"-shaped buildings 44' x 40' x varies (13 x 12 x varies m). Nearly destroyed buildings may provide some shelter from direct fire.

B31—Single-story, rectangular-shaped buildings with hipped roofs (service stations) 74' x 32' x 17' (23 x 10 x 5 m).



MCAS NEW RIVER

Center Coordinates

UTM 18STD76354355

GEO 344233N0772631W

Elevation 25 ft (8 m)

Night landing capable: Yes

Map Reference

Sheet: Camp Lejeune MIM

Series: V742S

Edition: 1-DMA

Datum: NAD 83/WGS 84

Runways

No.	Mag Bearing	Length	Width	Surface Material	Capability
R1	50/230	5098 ft (1554 m)	150 ft (46 m)	Asphalt	C-141
R2	10/190	5075 ft (1547 m)	150 ft (46 m)	Asphalt	C-130

Taxiways

No.	Length	Width	Surface Material	Type	Remarks
T1	775 ft (236 m)	25 ft (8 m)	Asphalt	Link	Connects to P4 to R1 and R2
T2	1850 ft (564 m)	38 ft (11 m)	Asphalt	Link	Connects R1 and R2 to T3
T3	3500 ft (1066 m)	107 ft (33 m)	Asphalt	Link	Connects R1 and R2 to P3
T4	718 ft (219 m)	55 ft (17 m)	Asphalt	Link	Connects R1 to P2
T5	2500 ft (762 m)	53 ft (16 m)	Asphalt	Link	Connects P2 to P3 and P4

Parking Areas

No.	Length	Width	Surface Material
P1	582 ft (177 m)	263 ft (80 m)	Concrete
P2	1328 ft (405 m)	894 ft (272 m)	Concrete
P3	1388 ft (423 m)	973 ft (297 m)	Concrete
P4	3144 ft (958 m)	1222 ft (372 m)	Concrete

Remarks: MCAS new river is bordered to the east by New River and to the southwest by Southwest Creek. Trees and buildings of various heights surround the airfield.

HLZ VULTURE

Center Coordinates

UTM 18STD76123004

GEO 343516NO772627W

Map Reference

Sheet: Camp Lejeune MIM

Series: V742S

Edition: 1-DMA

Datum: NAD 83/WGS 84

HLZ Shape

Irregular

HLZ Type

Open Field:

Surface Material

Scrub Grass

HLZ Size

Length 1209 ft (369 m)

Width 215 ft (66 m)

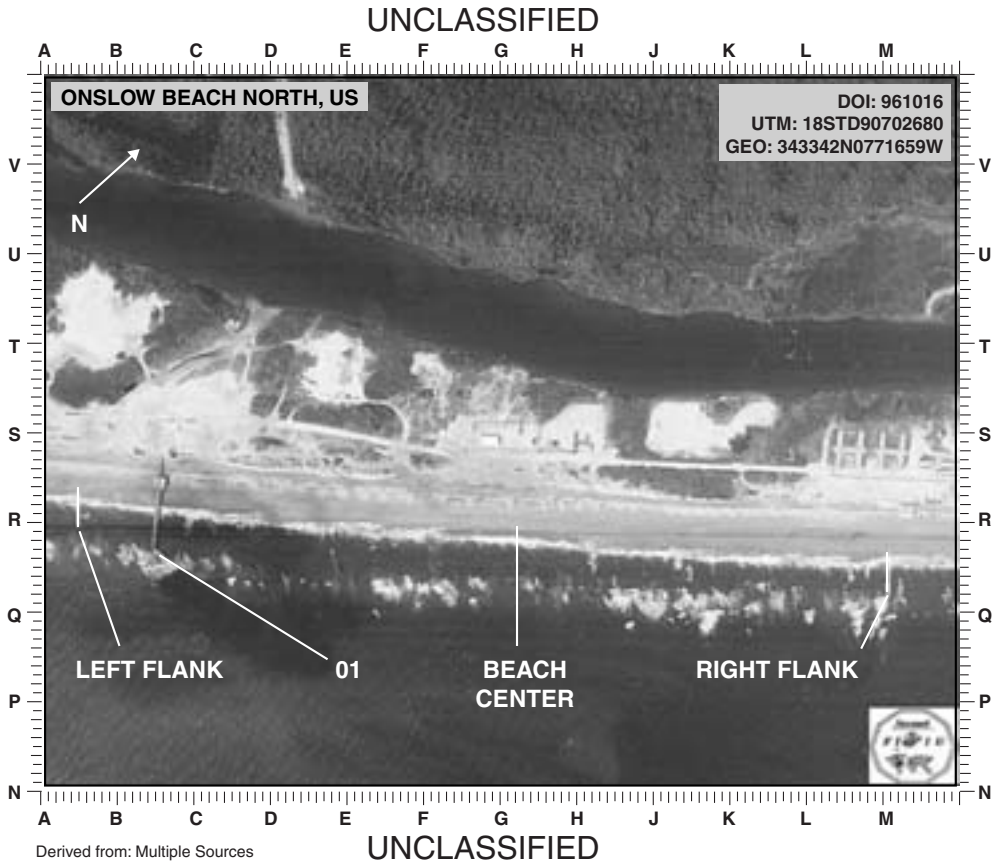
Exits

No.	Type	Distance and Grid Azimuth from HLZ Center	Width
E1	Loose surface road	182 ft (55 m) 280 Deg	20 ft (6 m)

Flight Hazard

No.	Type	Height and Grid Azimuth to HLZ Center
See remarks		

Remarks: The HLZ is located 600 m S of stone bay rifle range. E1 exits the HLZ on the W side extending N on Booker Washington Boulevard to the rifle range or W to range road. The western perimeter of the HLZ has four (4) buildings that may present flight hazards. The HLZ is surrounded on the N, S, and E sides by trees of varying height which may constitute flight hazards to low-flying aircraft. Blowing sand and debris caused by rotor wash may produce flight hazards. Adjacent terrain consists of a dissected plain, vegetated with trees and brush.



Onslow Beach North

Map Reference

Sheet: Camp Lejeune MIM
Series: V742S
Edition: 1-DMA
Datum: NAD 83/WGS 84

Left Flank
UTM 18S2901338263F
GEO 343327N0771714W

Beach Center
UTM 18S29071382670
GEO 343341N0771636W

Right Flank
UTM 18S2930382730
GEO 34335N0771633W

Length
Total: 1,393.4 m (4,752 ft)
Usable: 1,373.1 m (4,505 ft)

Width
Average Backshore Width: 66.4 m (218 ft)
Visible Foreshore Width: 24.0 m (79 ft)

Surface Material

Nearshore: Sand and mud

Foreshore: Sand

Backshore: Sand

Trafficability

Personnel:	Wet—Fair Dry—Good
Wheeled:	Wet—Fair Dry—Good
Tracked:	Wet—Fair Dry—Good

Tides

Tidal type: Diurnal	Average beach gradient: 1:116	Matting recommended: Yes
Tidal range: 1.0 m (3 ft.)	Firmness: Firm when wet	

MFP capable:	JLOTS capable:	LCAC offload capable:
No; see remarks.	No; see remarks.	Yes; see remarks.

Location: Onslow Beach North is approximately 13.1 km (7.1 nm) south-southeast of the U.S. Embassy. It is 3.7 km (2.0 nm) east-northeast of HLZ BLUEBIRD and 1.4 km (0.8 nm) east-southeast of HLZ Albatross.

Characteristics remarks: Onslow Beach North is not MPF capable since there is no MPF capable port within 92.7 km (50 nm) of the beach. It is not JLOTS capable due to insufficient beach gradient. It is, however, LCAC off-load capable due to average backshore width of 66.4 m (218 ft). All coordinates provided in this report were derived from the 1:50,000 scale map sheet listed in the reference above. All measurements were derived by MEF imagery analysts from mensurated imagery.

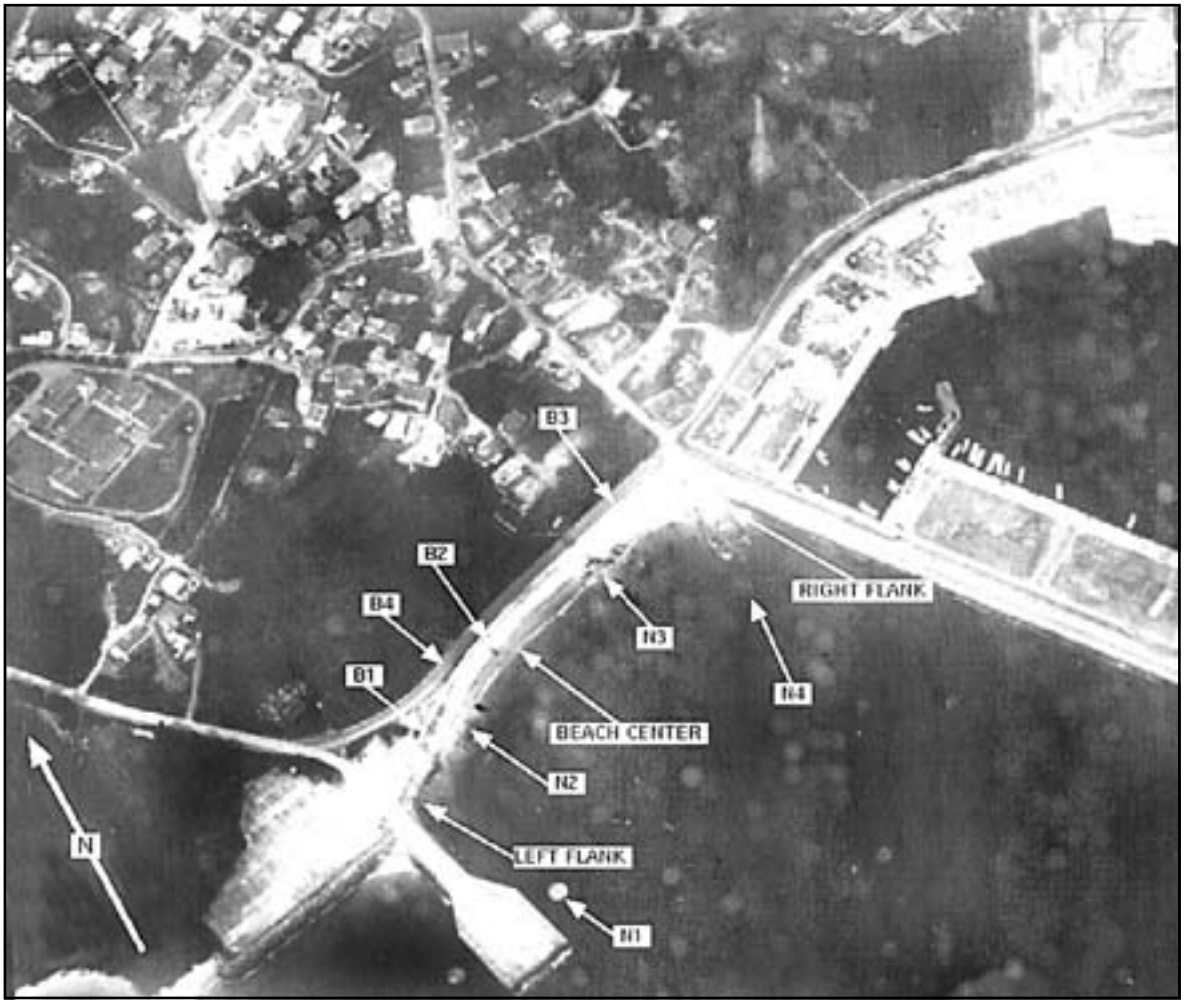
Obstructions

Anno. #	Type	True Bearing	Distance	Length	Width
N1	Pier	225	542.0 m (1,778 ft)	20.3 m (67 ft)	4.5 m (15 ft)

Obstruction remarks: None

Exit remarks: Cross-country to partial cross-country exits are available along the entire beach. These exits are too numerous to list individually. Parallel to the beach is a road that extends 6.3 km (3.4 nm) southwest to New River Inlet and 1.4 km (0.8 nm) northeast to Onslow Beach Road which leads approximately 2.8 km (1.5 nm) north-northeast to Highway 172. There are several buildings and compounds in the hinterland along the road.

KIN RED BEACH **GEOCORD: 262636N1275454E**



DERIVED FROM: MULTIPLE SOURCES
DECLASSIFY ON: XI
PRODUCED BY: IIP, P&A Co, 3D INTEL BN

PHOTO DATE: 09 AUG 96

KIN RED

Left Flank
UTM: 52RCE91642500
GEO: 262636N1275449E

Beach Center
UTM: 52RCE91782515
GEO: 262636N1275454E

Right Flank
UTM: 52RCE91922496
GEO: 262635N1275459E

Shape: Straight

Length
Total: 274 m (899 ft)
Usable: 151 m (496 ft)

Width
Average backshore width: 16.4 m (218 ft)
Visible foreshore width: 24.0 m (79 ft)

Surface Material

Nearshore: Sand/Coral

Foreshore: Sand/Coral

Backshore: Sand

Trafficability

Personnel:	Wet—Good Dry—Fair
Wheeled:	Wet—Good Dry—Fair
Tracked:	Wet—Fair Dry—Poor

Tides

Tidal type: Mixed	Average beach gradient: 1:116	Matting recommended: Yes
Tidal range: 1.7 m (5.6 ft)	Firmness: Firm when wet	

Location and general remarks: Kin Red Beach is located 17.6 km northeast of Kadena Airfield. Four islands obstruct the mouth of Kin Bay. The beach is flanked by a RO/RO pier to the west and a breakwater to the east. There are intermittent streams that cross the beach that could hinder lateral movement during inundation.
Personnel exit via cross-country along the entire beach length. The beach is backed by a concrete stepped seawall (B4) that severely restricts tracked vehicle and prevents wheeled vehicle movement. The town of Kin Cho further hinders and channels movement from the beach. Hinterland consists of hills covered with dense vegetation of varying heights, cultivated fields, numerous urban developments and/or tombs.

Obstructions

Anno. #	Type	True Bearing	Distance	Length	Width
N1	Dolphin	226	157 m (515 ft)	3 m (10 ft)	3 m (10 ft)
N2	Coral	250	86 m (282 ft)	18 m (59 ft)	20 m (66 ft)
N3	Coral	090	46 m (150 ft)	32 m (105 ft)	12 m (38 ft)
N4	Coral	113	92 m (302 ft)	40 m (131 ft)	32 m (105 ft)
B1	Coral	261	94 m (308 ft)	8 m (26 ft)	7 m (23 ft)
B2	Coral	270	26 m (85 ft)	14 m (46 ft)	9 m (30 ft)
B3	Coral	077	51 m (167 ft)	16 m (52 ft)	13 m (43 ft)
B4	Coral	270 thru 070	Varies	270 m (886 ft)	9 m (30 ft)

Obstruction remarks: Obstructions are measured from the beach center to the obstruction.

Exit remarks: See location and general remarks above.

APPENDIX I. IMAGERY INTELLIGENCE TARGET FOLDERS

A target folder contains intelligence that provides location, the components of a target or target complex, indicates its vulnerability(ies), and its relative importance. It also contains related materials prepared for planning and executing actions against a specific target. A major prerequisite for starting a target folder is the relative degree of permanence of the potential target. In addition, local command SOPs will provide guidance as to targets needed to have folders maintained.

Imagery Analysis

IMINT is often the definitive information source of intelligence support to targeting. IMINT input is reliable, accurate, and current, and often forms the basis for targeting decisions. Imagery analysis is a vital component in the tactical and strategic targeting process. It is often the IA, during the analysis of imagery, who—

- Discovers potential targets and draws them to the attention of the command (CMD section).
- Conducts the target study that is an analysis of the proposed target from imagery and other pertinent sources.
- Takes the information provided by the target analysis and puts it into a target folder format.

Target Analysis

The intelligence support coordinator (ISC) is responsible to the AC/S G-2 for imagery intelligence efforts supporting the MEF's targeting process. Before a possible target can be selected for attack, it must be developed to the point where its composition, strengths, and vulnerabilities are well known.

- The analysis of a target requires the collection and evaluation of many items of information. The target folder is an instrument for the compilation and organization of relevant data produced by the target analysis. Decisions by the force fires coordinator and FSCs regarding whether to attack a proposed target and weapon system selection are critically influenced by the information in the target folder.
- Once a possible target has been identified and approved for inclusion in the target intelligence data base, the IA and all-source intelligence analysts will prepare a target folder. This analysis presents all available pertinent information on the proposed target from the following sources:
  - **Reference Materials.** Perform a thorough check of all available intelligence reference materials. Interrogation, CI, ground reconnaissance, and signals intelligence reports all may be useful.
  - **GEOINT.** Ensure current maps (latest editions) and other GEOINT are available of the target area.
  - **Mission Coverage.** Examine comparative coverage of the target area from past and ongoing imagery collections missions. If the latest available coverage is old, incomplete, poor quality or the installation is under construction or renovation, new collection missions may be required.

Specifications

A target folder is a unit-created and maintained reference file on permanent potential targets in the AO and AOI. It contains the results of the target study (analysis) and any updates or collateral intelligence. Target folders—

- May be used as a pre-mission briefing aid for aircrews to orient them on target location, recognition, defenses, and obstacles. IAs may use target folders strictly as a reference file on important

intelligence targets within the unit's AO. Such folders can be compiled to show an installation's development or an enemy unit's organization.

- Have common characteristics and contain a minimum of important elements.
- Are for permanent targets. A permanent C2 node, troop training area, warehouse area, port facility or fixed missile site are good potential targets for target folders. Temporary targets such as troops in the field, supply dumps, and ships in port or truck convoys are usually not proper subjects for target folders.
- Are current. Because the information within a target folder may be used for target planning, it must be kept current. The target folder must be updated to reflect changes in defenses, physical characteristics, unit reorganization, important equipment, and so on.
- Are concise. Target folders are compact; only intelligence and other information pertinent to the commander's PIRs or IRs are included.
- Are accurate. Intelligence and other information within a target folder must be accurate to allow realistic targeting plans to be made. Answers to intelligence requirements must be specific to provide maximum value. For example, explicitly describe enemy defenses, target dimensions, shape, construction, use, and capacities.

Note: Target folders should be reviewed periodically or with each new photograph mission (intelligence priorities, resources, and time permitting) and their contents checked against new information or intelligence requirements.

Format and Components

There is no standard format for a target folder. Instead, it is a product tailored to meet all supported commanders' intelligence requirements.

Although the contents of a target folder will vary according to unit SOP, most will at a minimum contain the following components:

- Target folder index.
- Target worksheet.
- Target information sheet.
- Target illustration sheet.

The following items can be used to supplement the target folder:

- Target history sheet (supplement to the target worksheet).
- Map extract (supplement to the target information sheet).
- Sketch map or photographic overlay (supplement to the target information sheet).
- Building dimensions (supplement to the target illustration sheet). See appendix H for appropriate formulas for computing dimensions on imagery.

Target Folder Index

The index is located on the outside cover or on the first page of the target folder. It displays the contents of the folder (see figure I-1).

TARGET FOLDER INDEX

(Target Name)

	Page
Target worksheet	1
Target history sheet	2
Target Information sheet	3
Map extract	4
Sketch map	5
Target illustration sheet	6
Building or facility dimensions	7

Figure I-1. Sample Target Folder Index.

Target Worksheet

The target worksheet (see figure I-2) is organized with seven subheadings:

TARGET WORKSHEET

TARGET NUMBER:	2345-A23456
TARGET DESCRIPTION:	Sulphur Springs Valley Electric Power Station
TARGET LEADS:	Location: 320423N1105035W Elevation: 4,200 Feet Accuracy: Horizontal = +/- 100 Meters Vertical = +/- 10 Meters Datum: WGS 84 Source: V798, Douglas, AZ, Ed 5, 4048-1, Jun 86, DMAAC
SOURCES OF INFORMATION:	MSN 06-2028, 16TRS, 22 Jun 89, Photos V001-V010; EPW, 31 May 89 (F-6)
DATE OF INFORMATION:	10 Jun 99
DATE CONFIRMED AND SOURCE:	22 Jun 99, Imagery
DISTRIBUTION:	G-3, Force Fires Center, 1st MARDIV, 3d MAW

Figure I-2. Sample Target Worksheet.

Target Number

This number indicates the number of targets evaluated. For example, if the target number is 086, then it is the 86th target that the section has processed.

Target Description

Enter the name of the target and/or type of target. The type of target could be an airport, oil refinery, electric company, munitions plant, chemical plant, bunker complex or base area. If you have more than one of the same types of targets in the same area, you will number them (e.g., Bamberg SAM Site No. 3).

Target Leads

LEADS stands for: location (geographic coordinates), elevation, accuracy (horizontal and vertical), datum, and source (imagery, maps, etc.).

- Enter the geographic coordinates of the target, expressed in degrees, minutes, seconds; North or South (N or S) and East or West (E or W), depending on the location in regard to the equator and the prime meridian. Coordinates will represent the center of mass of the target.
- Include the elevation.
- Include horizontal and vertical accuracy.
- Include the datum (basis for the accuracy of the coordinates) used to derive the target location.
- Include the source of the information.

Sources of Information

Enter all other sources of information and intelligence available on the target. If possible, a P&A cell evaluation of the information and intelligence would be included (e.g., A-2, F-6). The map reference must include: series, sheet name, edition, sheet number, date, and production agency.

Date of Information

The date of the information is recorded on the target worksheet.

Date Confirmed and Source

Enter the date the target was confirmed and how it was confirmed. When using imagery, the date of information becomes the date of confirmation.

Distribution

Include those units and other agencies that normally receive the intelligence. Additionally, include all those that have requested the intelligence.

Target Information Sheet

A target information sheet (see figure I-3 on page I-4) is a detailed target description and continuation of the target worksheet information.

TARGET INFORMATION SHEET

BE NO:	0501-D57010	TARGET NO:	023
DATE OF INFO:	24 Nov 89	MAP SERIES:	V798
DATE COMPILED:	(Completion or update)	MAP SHEET NO:	4048 I
PROD CMD & NO:	5IDM-02	GEO REF GRID:	320423N1105035W
ELEVATION (MSL):	4,200 ft	UTM REF GRID:	12SXL00450474

LOCATION: The Sulphur Springs Valley Electric Power Station is located 36 mi SW of WILCOX, AZ, and 15 mi SE of the Southern Pacific Railroad tracks.

PHYSICAL CHARACTERISTICS: The target is 1,773 ft x 1,420 ft, located west of the highway. The RP is the generator hall that is a 56 ft x 174 ft, probably reinforced, with the following components: Boiler house is 59 ft from the RP on a 320-degree MAG heading. Substation (Transformer Yard) is 260 ft from RP on a 145-degree MAG heading. Fixed-top non-pressure liquid storage tank is 462 ft from RP on a 304-degree MAG heading. Coal Crushing Tower is 462 ft from RP on a 255-degree MAG heading. American Deck Coolers are 304 ft from RP on a 019-degree MAG heading. Smokestack is 174 ft from RP on a 320-degree MAG heading.

SIGNIFICANCE: The destruction of this target would stop or reduce electrical power to enemy military units in the vicinity.

OBSTRUCTIONS: The following obstruction is located within the target complex: 173 ft high smokestack 174 ft from RP on a 320-degree MAG heading. There are no visible obstructions outside the complex.

WEAPON RECOMMENDATIONS:

1. MEAN POINT OF IMPACT:	
2. PRIMARY WEAPON:	FUZING:
3. ALTERNATE WEAPON:	FUZING:
4. ON TARGET TONNAGE:	LEVEL:
5. OVER TARGET TONNAGE:	LEVEL:

OTHER INFORMATION: There are no visible bunkers, SAM sites or other antiaircraft emplacements.

Figure I-3. Sample Target Information Sheet.

Heading

The heading includes the classification and sheet name (TARGET INFORMATION SHEET).

Main Portion

The main portion of the target information sheet contains the following:

- BASIC ENCYCLOPEDIA (BE) NO: This is a number assigned to a specific target by the DIA. If a permanent BE number does not exist, an interim BE number may be used in accordance with unit or JTF SOP. The interim BE number must consist of 10 characters. The first four characters are composed of the World Aeronautic Chart Number on which the target is located; the remaining 6 characters are a combination of digits and letters determined by the unit SOP. Once this interim BE number is used, it must be used in all subsequent reporting on the target until DIA assigns a permanent BE number.
- DATE OF INFO: Enter the date of the most recent aerial imagery available in the target folder.
- DATE COMPILED: Enter the date when the target information sheet is completed or updated.
- PRODUCING COMMAND & NUMBER: Enter the producing command abbreviation and number.
- ELEVATION (MSL): Enter the target's actual elevation above mean sea level (MSL). This is obtained from the map sheet and is the elevation read from the contour lines, using the contour interval. The elevation may have to be interpolated when the target falls between two contour lines.

- TARGET NO: Transcribe the target number from the target worksheet.
- MAP SERIES: This is obtained from the map the target is located on. Transcribe map series from target worksheet (see figure I-2).
- MAP SHEET NO: This is obtained from the map. Transcribe map sheet number from the target worksheet (see figure I-2).
- GEO REF GRID: This is obtained from the map. Transcribe GEO coordinates from the target worksheet (see figure I-2).
- UTM REF GRID: This is obtained from the map. Transcribe UTM coordinates from the target worksheet (see figure I-2).
- LOCATION: Enter the physical location. For example, the Sulphur Springs Valley Electric Power Station is 3.6 miles (mi) SW of Wilcox, AZ, and 15 mi SE of the Southern Pacific Railroad tracks.
- PHYSICAL CHARACTERISTICS:
  - This is a complete description of the target. Identify the critical item within the target complex. The critical item is defined as: A component of the entire complex without which the complex would stop operation for the longest period of time. This critical item then becomes the primary target (PT). Determine the construction of the PT. Calculate the dimensions of the reference point (RP) to the target complex. Provide answers to the following questions: Is it operational? How far and in what direction or magnetic (MAG) heading are the other components of the complex from this RP?
  - The RP must be readily identifiable by the aircrews. If the critical item or PT is not readily identifiable from the air, determine through a process of elimination that RP the aircrews could distinguish from the air (e.g., smokestack, isolated storage tank, water tower). From this RP indicate in what direction and distance the PT is located. Are there railroads and highways close to the complex and in which direction? How many lanes are in the highway and what is it numbered (Hwy 40)? Are there service roads entering the complex? From which direction? How many lanes? Is the complex serviced by a rail spur? If so, from which direction does it enter the complex?
  - If extremely detailed target intelligence analysis is required, a sketch map or appendix may be used for enhancement.
  - To calculate dimensions to the target complex, use the formula GD = PD x DPRF.

    Example: If PD is .008 ft and DPRF is 10,000, then GD = .008 ft x 10,000 = 80 ft.
  - MAG is determined by placing the cross of the coordinate scale over the RP and shooting an azimuth toward the target. Read the grid-azimuth and add or subtract the grid-magnetic (GM) angle as specified in the map sheet legend. The GM angle is positive when it is being added to the grid azimuth, negative when subtracted from the grid azimuth. The RP is the roasting and sintering building. The grid azimuth to the receiving and handling building in the copper smelter complex is 299 degrees. By subtracting the GM angle, the MAG heading is 296 degrees.
- SIGNIFICANCE: This is a statement as to the significance of the target.

  Example: "Destruction of this target will deny the enemy 100,000 barrels of POL."
- OBSTRUCTIONS: List all obstructions in or near the target area that would hamper low-flying aircraft. External obstructions include urban areas, radio and television towers, power line towers, bridges and/or mountain ranges in proximity to the target RP. Obstructions within the target complex include smokestacks, water towers, high-tension power lines or towers, conveyor systems, etc.

- WEAPON RECOMMENDATIONS: Enter the format sub-headers that FFC or FSCC personnel will complete in this section.
- OTHER INFORMATION: Enter data not covered by the other subheadings that could have a bearing on the target, such as defenses.

  Examples: There are no visible bunkers, SAM sites, or antiaircraft emplacements. The target is encircled by SAM sites with 10 bunkers 2,000 ft from the center of the complex.

Target Illustration Sheet

A target folder is incomplete without illustrations. This includes as a minimum of one up-to-date annotated vertical photograph of the target. All imagery must have an accurately positioned magnetic north arrow, and the vertical photograph should have the boundaries of the target area outlined conspicuously. Oblique imagery can be included in the folder because it will aid in identifying the target from the air. Radar and infrared signatures are also helpful.

Target History Sheet

The target history sheet is a supplement to the target worksheet. It will follow the target worksheet in numerical sequence (see figure I-4).

Top

The top of the target history sheet contains a heading composed of the target's BE number (or unit assigned identification number), target name, target data inventory (TDI) category (optional), country, GEO/UTM coordinates, and map reference.

Body

The body of the target history sheet contains a listing of all reconnaissance missions with reference to the target. The columns are for mission date, mission number, quality of the imagery, action taken because of information extracted from the imagery (for example, "none," "new sketch map," "new target description," "significant change," etc), and the name of the IA who completed the imagery analysis.

Map Extract

A map extract of the target area may be used to supplement the target information sheet.

Sketch Map or Photograph Overlay

Some unit SOPs may require that a sketch map or photographic overlay of the target be included in

TARGET HISTORY SHEET

BE NO: _____ TARGET NAME _____

TDI CATEGORY _____ COUNTRY _____

GEO/UTM COORDS _____/_____

MAP REFERENCE _____

COMPONENT _____

	DATE	MISSION NO.	QUALITY	ACTION	IA
1					
2					
3					
4					

Figure I-4. Sample Target History Sheet.

the folder as supplementary information. The sketch map is a graphic representation of the target showing sufficient detail to satisfy IRs. Usually the sketch map will illustrate critical buildings and structures, transportation facilities (including roads), obstacles, defenses, and security measures.

A photographic overlay or sketch must convey a picture of what is on the ground (target and components) with the numbers or letters used to identify the important components and areas. RP is to represent the primary target or a more prominent feature. A properly prepared overlay should resemble the one in figure I-5 on page I-8. The location of numbers and lines need to be identical to the illustration. Avoid having lines cross features and other lines on the overlay.

General Information

Sketch maps are drawn freehand and are not to scale. If the photograph or map is drawn to scale, the scale is indicated. A magnetic north arrow, title, annotation, legend, date, and sketcher's unit, rank, name, are needed for a complete map. The classification must be indicated at top and bottom of the sketch map in larger than normal lettering.

Annotations

The following are methods of annotating on an overlay or photograph:

- The banding method is used when the photographs are of a large enough scale to place the annotations on top of each item so the item can still be seen. In this method, you would start to number the item at the upper left and continue across the illustration in a band; then return to the left edge and repeat. If there is a primary installation, number it "1," whatever its location in the illustration. Number 2 will then be the first designation in the upper left.
- The most preferred method is annotating by priority (listing in sequence of target components' significance), which is accomplished for those targets selected for tactical planning and bombing.
- Another method is alphanumeric code. In this method targets are grouped together by function and given an alphabetic designator (i.e., headquarters = A). The individual elements within the group are given a numeric designator (i.e., division headquarters A1, brigade headquarters A2, A3, etc.) The designators are given in order of priority. So A is the most important group and 1 is the most important element within the group.
- The last method is as specified in unit SOP.

The following suggestions may prove helpful in preparing your overlay:

- Do NOT place numbers or letters on top of small items being identified.
- Do NOT draw the lines so they intersect other lines or pass over important items.
- Place magnetic north arrow away from other annotation lines and orient it toward the top of the illustration.

Building Dimensions

Building and facility dimensions may be added to the target illustration sheet as supplementary information (see figure I-6 on page I-9). It should show the title (e.g., building dimensions), installation name (e.g., Sulpher Springs Valley Electric Power Station), RP annotation, type building or facility (e.g., generator hall), and dimensions (e.g., in feet or meters).

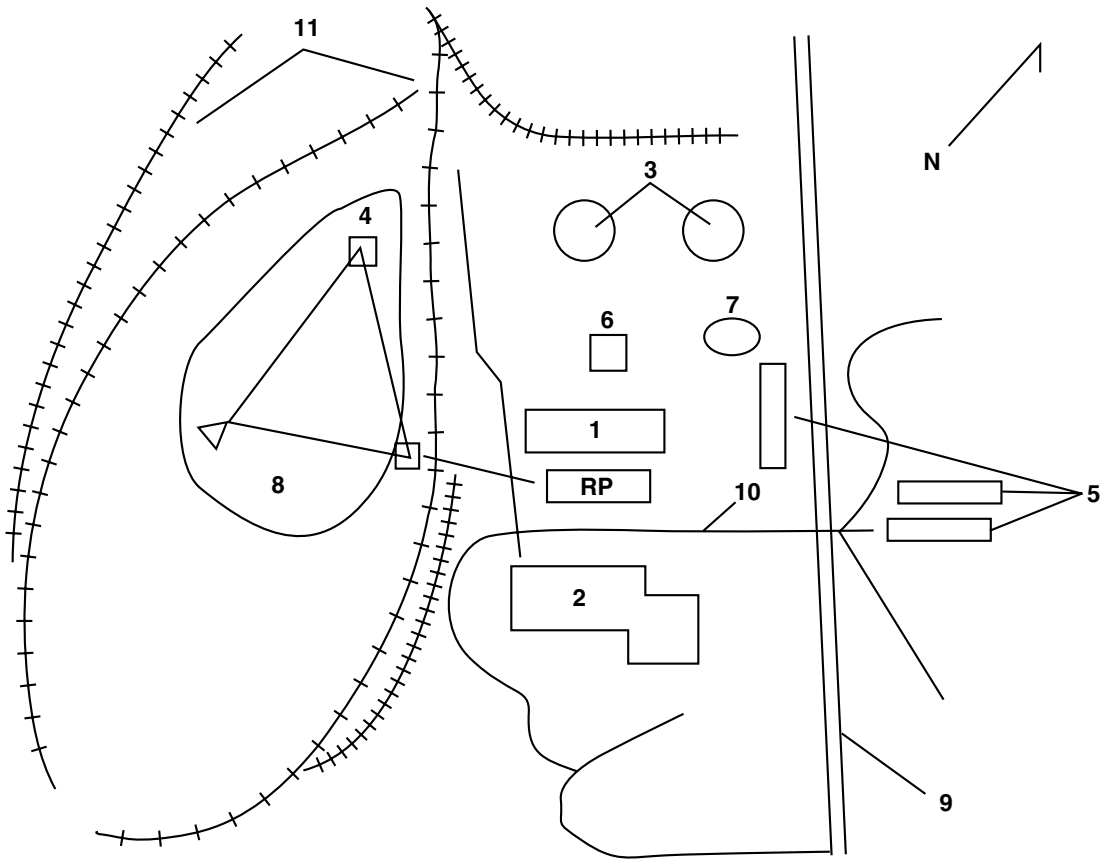
UNCLASSIFIED

TARGET SKETCH

TARGET NAME: Sulphur Springs Valley Electric Power Station
BE NO: 0501-D57010
DATE OF INFO: 21 Jun 81
GEO REF GRID: 320423N1105035W
UTM REF GRID: 12SXL00450474
SCALE: 1:5,000

ANNOTATIONS:

RP: Generator hall - PRIMARY TARGET
1. Boiler house
2. Substation
3. Storage tanks
4. Coal crushing towers
5. American deck coolers
6. Smokestack
7. Water tower
8. Coal storage area
9. Highway 666
10. Service road
11. Railroad tracks



UNCLASSIFIED

Figure I-5. Sketch Map.

TARGET ILLUSTRATION SHEET

BUILDING DIMENSIONS

Sulpher Springs Valley Electric Power Station

Annotation	Type Building/Facility	Dimensions
RP	Generator hall	56.0 ft x 174.0 ft
1	Boiler house	85.6 ft x 120.0 ft
2	Transformer yard	50.0 ft x 200.0 ft
3	Fixed top non-pressure liquid storage tank	20.0 ft x 10.0 ft
4	Coal crushing tower	20.0 ft tall
5	American deck coolers	20.0 ft x 120.0 ft
6	Smokestack	223.0 ft tall

Figure I-6. Sample of Building Dimensions.

APPENDIX J. NATIONAL IMAGERY TRANSMISSION FORMAT COMPRESSION

We use compression to decrease imagery file sizes to transmit usable images in as short a time as possible. Remember that the average image size used in the tactical intelligence community is around 4 megabytes (MB). Transmission time over a T1 line is 4 minutes, but over a regular telephone line at 9,600 bits per second (bps), the transmission time goes up to 55 minutes. If we compress the image by 50 percent, or a 2:1 compression ratio, it will take only one-half the time (see figure J-1). Note that the times are still excessive for our original 4 MB image until around the 25:1 compression point for the 2,400 and 9,600 rates.

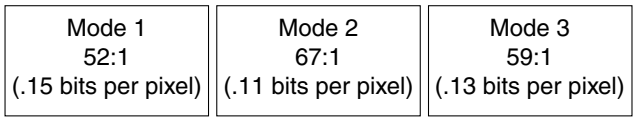


Figure J-1. Bi-Level Image Compression Results.

The first NITF algorithm that will be addressed is the Joint Photographic Experts Group (JPEG) image compression algorithm. The complete specifications are contained in MIL-STD-188-198A.

JPEG is one of the most popular and widely used compression algorithms. It is used on the World Wide Web and was adapted for use in the NITF in the early 1990s.

NITF JPEG also follows a model similar to those discussed previously to produce a compressed image. NITF JPEG's Forward Discrete Cosine Transform (FDCT) is just another mathematical formula. JPEG divides the image into 8 by 8-minimum coding units or neighborhoods, and then calculates the FDCT of each neighborhood. The quantizer rounds off or smooths the FDCT coefficients according to the table specifications, and then is encoded.

For decompression, JPEG recovers the quantized FDCT coefficients from the compressed data stream, takes the inverse transform (using embedded tables), and displays the image. This is a simple description; technical details are in the military standard. We need to know two things: How the various Q settings impact the quality of an image, and the time available to transmit the compressed image.

NITF JPEG provides several variants, Discrete Cosine Transform (DCT) lossy (8 and 12 bit), downsample JPEG, and lossless.

APPENDIX K. IMAGERY INTELLIGENCE
APPENDIX FORMAT

The IMINT operations appendix should explain how IMINT and relevant imagery-related elements under the OPCON or supporting the MAGTF will be used to support this plan. It should also provide guidance to subordinate commanders for the conduct of IMINT operations and the support of IMINT elements and personnel identified to fulfill the IMINT requirements.

CLASSIFICATION

Copy no. ___ of ___ copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

APPENDIX 7 TO ANNEX B (INTELLIGENCE) TO MAGTF OPORD XXX (U)
Imagery Intelligence (U)

(U) REFERENCES: Identify DOD, NIMA, and other directives; combatant commander, JTF or other higher authorities' operations orders and tactics, techniques and procedures or SOP for intelligence and IMINT operations; pertinent maps and other geospatial information resources; and any other relevant references that pertain to anticipated IMINT operations.

1. (U) Situation

a. (U) Definition of the Area of Operations (AO) and Area of Interest (AOI). Describe the limits of the AO and AOI. Summarize pertinent weather, terrain and other AO's characteristics and conditions that may influence the conduct of IMINT operations.

b. (U) Enemy. Refer to Annex B and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and OOB pertinent to IMINT operations.

c. (U) Assigned MAGTF Organic and Supporting IMINT Assets. Identify organic and supporting forces available to perform IMINT and imagery-related functions.

CLASSIFICATION

d. (U) Facts and Assumptions. Derived during the mission analysis step of the MCPP.

e. (U) IMINT Considerations. List key IMINT, intelligence or other considerations that impact this OPLAN or CONPLAN.

(1) (U) Availability of national source and commercial imagery.

(2) (U) IMINT support to and from JTF and other component headquarters.

(3) (U) Creation and manning of forward IMINT elements.

2. (U) Mission. State concisely the IMINT mission as it relates to the command's planned operation.

3. (U) Execution

a. (U) Concept of Operations. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations Plan) to Annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall concept of operations as they relate to IMINT operations. Outline the purpose and concept of IMINT operations, specified priorities, and summarize the means and agencies to be employed in planning and directing, collecting, processing and exploiting, analyzing and producing, disseminating, and using IMINT during execution of the OPORD. Address the integration of JTF, other components, theater, national, and allied forces' IMINT operations.

b. (U) Tasks for IMINT and Related Units and Organizations, Subordinate Units, and Task Force Commanders/OICs.

(1) (U) Orders to Subordinate, Attached and Supporting Units. Use separate numbered subparagraphs to list detailed instructions for each unit conducting IMINT operations, including the originating headquarters, subordinate commands, and separate intelligence support units.

(a) (U) Major Subordinate Commanders

(b) (U) Commanding Officer, Intel Bn

1 Platoon Commander, Imagery Intelligence Platoon

2 OIC, JSTARS Common Ground Station Section

CLASSIFICATION

3 SNCOICs, Direct Support Teams

4 OIC, Support Cell

5 OIC, Surveillance and Reconnaissance Cell

6 OIC, Production and Analysis Cell

7 (Others as appropriate)

(c) (U) Commanding Officer, VMU Squadron

(d) (U) Commanding Officer, Force Reconnaissance Company

(2) (U) Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached or supporting and from which IMINT support is requested, including other components, JTF headquarters, allied or coalition forces, theater and national operational and intelligence elements.

c. (U) Coordinating Instructions. (Reference Appendix 16 (Intelligence Operations Plan), and command and other pertinent forces and organizations intelligence and CI SOPs. Detail here or in supporting tabs key changes to SOPs. Additional topics to include or emphasize here are requesting IMINT support; direct liaison among subordinate commanders, MAGTF IMINT units, staff officers, and pertinent external organizations and agencies; routine and time-sensitive reporting procedures and formats, etc.)

4. (U) Administration and Logistics

a. (U) Logistics. Reference Annex D (Logistics). Identify IMINT unique logistic requirements and concerns, such as: any unique combat service support requirements, procedures, and other guidance to support MAGTF IMINT units and operations; or procedures for specialized technical logistic support necessary from external organizations.

b. (U) Personnel. Identify intelligence unique IMINT personnel requirements and concerns.

5. (U) Command and Control

a. (U) Command Relationships. Reference Annex J (Command Relationships). Provide any instructions necessary regarding MAGTF command relationships that will influence unit IMINT operations.

CLASSIFICATION

b. (U) Information Management. Reference Annex U (Information Management), Annex C (Operations) and Appendix 16 (Intelligence Operations Plan). Provide any instructions necessary regarding information management (time-sensitive and routine reporting criteria, intelligence databases, reports, etc.) that will influence MAGTF IMINT operations.

c. (U) Communications and Information Systems. Reference Appendix 16 (Intelligence Operations Plan) and Annex K (Communications and Information Systems). Provide any instructions necessary regarding CIS that will influence MAGTF IMINT operations.

d. (U) Intelligence C2 Nodes and Facilities. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations Plan). Provide guidance and instructions necessary regarding the establishment and operations of intelligence and IMINT C2 nodes and facilities (e.g., the surveillance and reconnaissance cell).

TABS: (As necessary)

APPENDIX L. UNMANNED AERIAL VEHICLE PLAN FORMAT

CLASSIFICATION

Copy no._____ of_____ copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

TAB C TO APPENDIX 14 TO ANNEX B TO OPLAN XXX
UNMANNED AERIAL VEHICLE PLAN

(U) REFERENCES: (As appropriate)

1. (U) Mission. Conduct real-time surveillance, target acquisition, and imagery intelligence throughout the MAGTF area of responsibility until termination of hostilities, per Annex B (Intelligence) and Annex C (Operations) to the MAGTF OPLAN.

2. (U) Execution. The UAV squadron will provide UAVs and C2 crews in support of MAGTF operations. The MAGTF G-2, in coordination with the G-3, will exercise operational control of all tactical surveillance UAVs within the AO unless otherwise directed. The ISC, under the staff cognizance of the AC/S G-2, plans, coordinates, and supervises MAGTF UAV intelligence missions.

3. (U) Tasks. Detachment,_____,_____UAV Squadron will—

a. (U) Prepare a UAV employment plan and overlay to depict the UAV's concept of employment supporting combat operations ashore and submit these to the MAGTF G-2 (Attn: ISC or CMDO).

b. (U) Assign surveillance UAV equipment, and personnel to provide real-time video/imagery intelligence in support of MAGTF operations as directed by Annex B (Intelligence) to the MAGTF OPLAN, daily ATOs, and other intelligence orders.

c. (U) Provide RRS detachments at designated locations afloat and ashore.

d. (U) Initiate action to obtain approved frequencies for UAV support, per Annex K (CIS) to the MAGTF OPLAN.

CLASSIFICATION

e. (U) Coordinate flight operations through appropriate air control agencies as assigned in Annex N (Aviation Operations) to the MAGTF OPLAN.

4. (U) MAGTF UAV Surveillance Sectors/Routes. To facilitate the assignment and coordination of tactical surveillance missions, UAV loiter areas and surveillance routes are designated in the enclosures to this tab.

ENCLOSURES:

1 —UAV Employment Plan
2 —UAV Employment Overlay

CLASSIFICATION

Copy no._____ of_____ copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

ENCLOSURE 1 TO TAB C TO APPENDIX 14 TO ANNEX B TO OPLAN XXX UAV EMPLOYMENT PLAN

(U) REFERENCES: (a) Maps: NIMA stock no._____

The following UAV and surveillance routes, targets, and loiter areas have been preplanned in support of MAGTF operations:

MSN NUMBER	COORDINATES	ALT	TOT	FOOTNOTES
	_____to	TBD	TBD	
	_____to			
	_____to			
	_____to			
	close			
	_____to	TBD	TBD	
	_____to			
	_____to			
	_____to			
	close			

Note: (1) Tasked intelligence requirements and reporting criteria.
(2) (Others as appropriate)

APPENDIX M. AERIAL IMAGERY PLAN FORMAT

CLASSIFICATION

Copy no. ___ of ___ copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

TAB D TO APPENDIX 14 TO ANNEX B TO OPLAN XXX
AERIAL IMAGERY PLAN

(U) REFERENCES: (a) Maps. See appendix 15 (Geographic Intelligence) to Annex B (Intelligence) and Annex M (Geospatial Information and Services)

1. The following aerial imagery missions have been preplanned.

MSN NO.	COORD	PHOTO VERT OR OBL	PHOTO OVER-LAP	PHOTO FILM SCALE	SLR MODE	IR/ALT	DATE OF MSN	REMARKS
1.	XXXX XXXX XXXX XXXX	VERT	60% FOR 40%	B&W 1:20K	Low ALT Mode 10B	N/A	D-30	Basic Coverage
2.	XXXX XXXX XXXX XXXX	VERT	60% FOR 40% SIDE	B&W Color & CD 1:5K	Low ALT MTIR or MTIR	D-3 only	D-1	Beach Study Survey
3.	N/A	N/A	N/A	N/A	N/A	N/A	D+1	On call

CLASSIFICATION

APPENDIX N. GLOSSARY

SECTION I. ACRONYMS

AAA . . . . . antiaircraft artillery
ACE . . . . . aviation combat element
ADCON . . . . . administrative control
AFC. . . . . all-source fusion center
AGL . . . . . above ground level
AMC . . . . . air mission commander
AO. . . . . area of operations
AOI . . . . . area of interest
ATARS . . . . . advanced tactical airborne reconnaissance system
ATF. . . . . amphibious task force
ATO . . . . . air tasking order
AVN . . . . . aviation department HQMC
AW . . . . . all weather

BAC . . . . . broad area coverage
BAS. . . . . broad area surveillance
BDA . . . . . battle damage assessment
BE . . . . . basic encyclopedia
BLS . . . . . beach landing site
BPS . . . . . bits per second

C2 . . . . . command and control
CCD . . . . . charged-coupled device
CCDTV . . . . . charged-coupled device television
CCIR . . . . . commander's critical information requirements
CDL . . . . . common data link
CE . . . . . command element
CGS. . . . . common ground station
CI . . . . . counterintelligence
CIA . . . . . Central Intelligence Agency
CIC . . . . . combat intelligence center
CIGSS . . . . . Common Imagery Ground/Surface System
CIS . . . . . communications and information systems
CMD . . . . . collection management and dissemination
CMDO . . . . . collection management/ dissemination officer
CMS . . . . . communications security materials system
CO. . . . . commanding officer
COA . . . . . course of action
COC . . . . . current operations center
COLISEUM . . . . . Community On-Line Intelligence System for End-Users and Managers
CONPLAN . . . . . concept plan
COP. . . . . common operational picture
COTS . . . . . commercial off-the-shelf
CSRT . . . . . customer support response team
CSS . . . . . combat service support
CSSD . . . . . combat service support detachment
CSSE. . . . . combat service support element
CTP . . . . . common tactical picture
CVBG . . . . . carrier battle group

DASC . . . . . direct air support center
DATEDES . . . . . date desired
DCI . . . . . Director of Central Intelligence
DCT . . . . . discrete consine transform
DE. . . . . dissemination element
DIA . . . . . Defense Intelligence Agency
DISN . . . . . defense information systems network
DMRF . . . . . denominator of the map representative factor
DMS . . . . . defense message system
DOD . . . . . Department of Defense
DODIPP . . . . . Department of Defense Intelligence Production Program
DPL. . . . . digital photo lab
DPRF . . . . . denominator of the photo representative factor
DRO . . . . . Departmental Requirements Officer
DS . . . . . downsample
DSA . . . . . directed search area
DSCS . . . . . defense satellite communications system
DSN . . . . . defense switched network
DSSCS . . . . . defense special security communications system
EO . . . . . electro-optical

E&R . . . . . evasion and recovery
EW . . . . . electronic warfare

5D . . . . . demand driven direct digital dissemination
FDCT . . . . . forward discrete consine transform
FLIR . . . . . forward-looking infrared
FSCC. . . . . fire support coordination center
FSSG. . . . . force service support group
FTI . . . . . fixed target indicator

GB. . . . . gigabytes
GCCS . . . . . global command and control system
GCE . . . . . ground combat element
GCS. . . . . ground control station
GD. . . . . ground distance
GDT . . . . . ground data terminal
GENSER. . . . . general service
GEOINT . . . . . geographic intelligence
GRG . . . . . gridded reference graphic
GSP . . . . . ground sensor platoon

HD. . . . . horizontal distance
HML/A . . . . . Marine light/attack helicopter squadron
HQMC . . . . . Headquarters Marine Corps
HUMINT . . . . . human intelligence

I&W . . . . . indications and warning
IA . . . . . imagery analyst
IAS . . . . . intelligence analysis system
ICR . . . . . intelligence collection requirement
IDR . . . . . intelligence dissemination requirement
IESS . . . . . imagery exploitation software system
IIP . . . . . imagery intelligence platoon
IMINT. . . . . imagery intelligence
INMARSAT . . . . . international maritime satellite system
intel bn . . . . . intelligence battalion
IOC . . . . . intelligence operations center
IPB . . . . . intelligence preparation of the battlespace
IPIR. . . . . initial photo interpretation report
IPL . . . . . imagery product library
IPR . . . . . intelligence production requirement
IR . . . . . intelligence requirement
ISC . . . . . intelligence support coordinator
JAC . . . . . joint analysis center
JDISS . . . . . joint deployable intelligence support system
JFACC . . . . . joint force air component commander
JFC . . . . . joint force commander
JFLCC. . . . . joint force land component commander
JFMCC . . . . . joint force maritime component commander
JIC. . . . . joint intelligence center
JISE. . . . . joint intelligence support element
JOPES . . . . . Joint Operation Planning and Execution System
JPEG . . . . . joint photographic experts group
JSIPS. . . . . Joint Services Imagery Processing System
JSTARS . . . . . joint surveillance, target attack radar system
JTAR/S . . . . . joint tactical air reconnaissance/surveillance
JTF . . . . . joint task force
JWICS. . . . . Joint Worldwide Intelligence Communications System

kbps. . . . . kilobytes per second
kw . . . . . kilowatt

LAN . . . . . local area network
LAR . . . . . light armored reconnaissance
LEADS . . . . . location, elevation, accuracy, datum, source
LF . . . . . landing force
LOC . . . . . lines of communications
LOS. . . . . line of sight
LP . . . . . landing point
LTIOV . . . . . latest time intelligence is of value

MACCS . . . . . Marine air command and control system
MACG . . . . . Marine air control group
MAG. . . . . Marine aircraft group
MAGTF . . . . . Marine air-ground task force
MASINT. . . . . measurement and signature intelligence
mbps . . . . . megabits per second

Manpack SIDS . . . . . man packable secondary imagery dissemination system
MARCORSYSCOM. . . . . Marine Corps Systems Command
MARFOR . . . . . .Marine Corps forces
MARFORRES . . . . . Marine Corps Forces Reserve
MAW . . . . . Marine aircraft wing
MB . . . . . megabyte
MCCDC . . . . . Marine Corps Combat Development Command
MCIA . . . . . Marine Corps Intelligence Activity
MD . . . . . .map distance
MEF . . . . . Marine expeditionary force
MEU(SOC) . . . . . Marine expeditionary unit (special operations capable)
MHG . . . . . MEF headquarters group
mi . . . . . .miles
MIPIR . . . . . .multimission imagery photo interpretation report
MOS . . . . . military occupational specialty
MSC . . . . . major subordinate command
MSI . . . . . .multispectral imagery
MSL . . . . . mean sea level
MTI . . . . . moving target indicator
MWSS. . . . . Marine wing support squadron

NAI . . . . . named area of interest
NDS . . . . . .NIMA delivery system
NIIRS . . . . . National Imagery Interpretability Rating Scale
NIMA . . . . . .National Imagery and Mapping Agency
NIPRNET . . . . . .Nonsecure Internet Protocol Router Network
NIST . . . . . .national intelligence support team
NITF . . . . . .national imagery transmission format
NRO . . . . . National Reconnaissance Office
NRT . . . . . .near-real-time
NSA . . . . . National Security Agency
NTIS . . . . . night thermal imaging system
NTS. . . . . night targeting system

OIC . . . . . .officer in charge
OOB . . . . . .order of battle
OPCON. . . . . .operational control

P&A . . . . . production and analysis
PCMCIA . . . . . Personal Computer Memory Card International Association
PCS . . . . . portable control station
PD . . . . . photo distance
PI. . . . . .photo interpreter
PIR . . . . . priority intelligence requirement
POL. . . . . .petroleum, oils, and lubricants
PT . . . . . .primary target

QRS. . . . . quick response system

R&S . . . . . reconnaissance and surveillance
RAOC . . . . . .rear area operations center
RATO . . . . . .rocket-assisted takeoff
RECCEXREP . . . . . .reconnaissance exploitation report
RFI . . . . . .request for intelligence
RMS . . . . . .requirements management system
ROC . . . . . .reconnaissance operations center
RP . . . . . .reference point
RRS. . . . . remote receive station
RS . . . . . .receive segment
RVT . . . . . remote video terminal

SACC . . . . . .supporting arms coordination center
SAFE. . . . . selected area for evasion
SAM . . . . . .surface-to-air missile
SAID . . . . . SAFE area intelligence description
SAR. . . . . synthetic aperture radar
SARC . . . . . .surveillance and reconnaissance cell
SATCOM . . . . . .satellite communications
SCDL . . . . . .surveillance and control data link
SCI . . . . . .sensitive compartmented information
SCR. . . . . .single channel radio
SERE. . . . . .survival, evasion, resistance, and escape
SGS . . . . . .squadron ground station
SHF . . . . . super high frequency
SI. . . . . .special intelligence
SIDS . . . . . .secondary imagery dissemination system
SIG . . . . . sensor interface group

SIGINT . . . . . signals intelligence
SIPRNET . . . . . SECRET Internet Protocol . . . . . Router Network
SL . . . . . slope
SOP . . . . . standing operating procedure
SR . . . . . short range
STOM . . . . . ship to objective maneuver
SVCR . . . . . super videocassette recorder

TACC . . . . . tactical air command center
TACPHOTO . . . . . tactical intelligence photographic capability
TARPS . . . . . tactical airborne reconnaissance pod system
TCU . . . . . tracking control unit
TDI . . . . . target data inventory
TDN . . . . . tactical data network
TEG. . . . . tactical exploitation group
TIGDL . . . . . tactical interoperable ground data link
T/O . . . . . table of organization
TOT. . . . . time over target
TRAP . . . . . tactical recovery of aircraft and personnel
TTP . . . . . tactics, techniques, and procedures
TUAV . . . . . tactical unmanned aerial vehicle

UAV . . . . . unmanned aerial vehicle
UHF . . . . . ultrahigh frequency

VCR . . . . . videocassette recorder
VD. . . . . vertical distance
VHS . . . . . very high speed
VMFA(AW) . . . . . Marine fighter/attack (all weather) squadron
VMU . . . . . Marine unmanned aerial vehicle squadron
VRN . . . . . vehicle registration number

WAN. . . . . wide area network
WG . . . . . workstation group
WICP . . . . wing initial communications package

SECTION II. DEFINITIONS

administrative control—Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. Also called ADCON. (JP 1-02)

air contingency MAGTF—An on-call, combat-ready MAGTF that deploys by airlift. Air contingency MAGTFs vary in size based on mission requirements and the availability of airlift. Because they deploy by air, they generally have a limited organic logistics capability, and require an arrival airfield. Air contingency MAGTFs usually are activated to respond to developing crises, and may deploy independently or in conjunction with other expeditionary forces. Also called ACM.

all-source intelligence—1. Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data, in the production of finished intelligence. **2.** In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 1-02)

area of interest—That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (JP 1-02)

area of operations—An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. Also called AO. (JP 1-02)

assessment—1. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. **2**. Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 1-02)

attach—1. The placement of units or personnel in an organization where such placement is relatively temporary. **2**. The detailing of individuals to specific functions where such functions are secondary or relatively temporary, e.g., attached for quarters and rations; attached for flying duty. (JP 1-02)

aviation combat element—The core element of a Marine air-ground task force (MAGTF) that is task-organized to conduct aviation operations. The aviation combat element (ACE) provides all or a portion of the six functions of Marine aviation necessary to accomplish the MAGTF's mission. These functions are antiair warfare, offensive air support, assault support, electronic warfare, air reconnaissance, and control of aircraft and missiles. The ACE is usually composed of an aviation unit headquarters and various other aviation units or their detachments. It can vary in size from a small aviation detachment of specifically required aircraft to one or more Marine aircraft wings. The ACE itself is not a formal command. Also called ACE. (JP 1-02)

basic intelligence—Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in

evaluating subsequent information relating to the same subject. (JP 1-02)

battle damage assessment—The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (JP 1-02) In Marine Corps usage, the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCRP 5-12C)

battlespace—The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest. (JP 1-02)

battlespace dominance—The degree of control over the dimensions of the battlespace which enhances friendly freedom of action and denies enemy freedom of action. It permits force sustainment and application of power projection to accomplish the full range of potential operational and tactical missions. It includes all actions conducted against enemy capabilities to influence future operations. (MCRP 5-12C)

beach—1. The area extending from the shoreline inland to a marked change in physiographic form or material or to the line of permanent vegetation (coastline). **2.** In amphibious operations, that portion of the shoreline designated for landing of a tactical organization. (JP 1-02)

beachhead—A designated area on a hostile or potentially hostile shore that, when seized and held, ensures the continuous landing of troops and materiel, and provides maneuver space requisite for subsequent projected operations ashore. (JP 1-02)

beach landing site—A geographic location selected for across-the-beach infiltration, exfiltration or resupply operations. Also called BLS. (JP 1-02)

beach width—The horizontal dimensions of the beach measured at right angles to the shoreline from the line of extreme low water inland to the landward limit of the beach (the coastline). (JP 1-02)

centers of gravity—Those characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight. (JP 1-02)

centralized control—In military operations, a mode of battlespace management in which one echelon of command exercises total authority and direction of all aspects of one or more warfighting functions. It is a method of control where detailed orders are issued and total unity of action is the overriding consideration. (MCRP 5-12C)

collection (acquisition)—The obtaining of information in any manner, including direct observation, liaison with official agencies, or solicitation from official, unofficial, or public sources. (JP 1-02) In Marine Corps usage, the gathering of intelligence data and information to satisfy the identified requirements. (MCRP 5-12C)

collection agency—Any individual, organization or unit that has access to sources of information and the capability of collecting information from them. (JP 1-02)

collection management—In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 1-02)

collection plan—A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02)

collection requirement—An established intelligence need considered in the allocation of intelligence resources to fulfill the essential elements of information and other intelligence needs of a commander. (JP 1-02)

combatant command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

combat data—Data derived from reporting by operational units. (MCRP 5-12C)

combat service support element—The core element of a Marine air-ground task force that is task-organized to provide the combat service support necessary to accomplish the Marine air-ground task force mission. The combat service support element varies in size from a small detachment to one or more force service support groups. It provides supply, maintenance, transportation, general engineering, health services, and a variety of other services to the Marine air-ground task force. It may also contain other Service or foreign military forces assigned or attached to the MAGTF. The combat service support element itself is not a formal command. Also called CSSE. (Approved for inclusion in next edition of MCRP 5-12C)

combat surveillance—A continuous, all-weather, day-and-night, systematic watch over the battle area in order to provide timely information for tactical combat operations. (JP 1-02)

command and control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1-02) Also in Marine Corps usage, the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCRP 5-12C)

command element—The core element of a Marine air-ground task force that is the headquarters. The command element is composed of the commander, general or executive and special staff sections, headquarters section, and requisite communications support, intelligence and reconnaissance forces, necessary to accomplish the MAGTF's mission. The command element provides command and control, intelligence, and other support essential for effective planning and execution of operations by the other elements of the MAGTF. The command element varies in size and composition. Also called CE. (JP 1-02)

commander's critical information requirements—A comprehensive list of information requirements identified by the commander as being critical in facilitating timely information management and the decisionmaking process that affect successful mission accomplishment. The two key subcomponents are critical friendly force information and priority intelligence requirements. (JP 1-02) Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR.

NOTE: CCIRs are normally divided into three primary subcategories: priority intelligence requirements; friendly force information requirements; and essential elements of friendly information. (MCRP 5-12C)

commander's intent—A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

contingency—An emergency involving military forces caused by natural disasters, terrorists, subversives, or by required military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response, and special procedures to ensure the safety and readiness of personnel, installations, and equipment. (JP 1-02)

control—1. Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. **2.** In mapping, charting, and photogrammetry, a collective term for a system of marks or objects on the earth or on a map or a photograph, whose positions or elevations or both, have been or will be determined. **3.** Physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. **4.** An indicator governing the distribution and use of documents, information, or material. Such indicators are the subject of intelligence community agreement and are specifically defined in appropriate regulations. (JP 1-02)

coordinating authority—A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more Military Departments or two or more forces of the same Service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations. (JP 1-02)

coordination—The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (MCRP 5-12C)

counterintelligence—1. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons or international terrorist activities. Also called CI. See also counterespionage; security. (JP 1-02) **2.** Within the Marine Corps, counterintelligence (CI) constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. (MCRP 5-12C)

countermeasures—That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

critical vulnerability—An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. Also called CV. (MCRP 5-12C)

current intelligence—One of two categories of descriptive intelligence that is concerned with describing the existing situation. (JP 1-02)

damage assessment—1. The determination of the effect of attacks on targets. **2.** A determination of

the effect of a compromise of classified information on national security. (JP 1-02)

decentralized control—In military operations, a mode of battlespace management in which a command echelon may delegate some or all authority and direction for warfighting functions to subordinates. It requires careful and clear articulation of mission, intent, and main effort to unify efforts of subordinate leaders. (MCRP 5-12C)

descriptive intelligence—Class of intelligence which describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: basic intelligence, which is general background knowledge about established and relatively constant conditions; and current intelligence, which is concerned with describing the existing situation. (MCRP 5-12C)

detachment—1. A part of a unit separated from its main organization for duty elsewhere. **2.** A temporary military or naval unit formed from other units or parts of units. (JP 1-02)

dissemination—Conveyance of intelligence to users in a suitable form. (JP 1-02)

dissemination management—Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12C)

drop zone—A specific area upon which airborne troops, equipment or supplies are airdropped. (JP 1-02)

essential elements of friendly information—Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. Also called EEFI. (JP 1-02) Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. (MCRP 5-12C)

estimative intelligence—Class of intelligence which attempts to anticipate future possibilities and probabilities based on an analysis of descriptive intelligence in the context of planned friendly and assessed enemy operations. (MCRP 5-12C)

evasion and escape intelligence—Processed information prepared to assist personnel to escape if captured by the enemy or to evade capture if lost in enemy-dominated territory. (JP 1-02)

executive agent—A term used in DOD and Service regulations to indicate a delegation of authority by a superior to a subordinate to act on behalf of the superior. An agreement between equals does not create an executive agent. For example, a Service cannot become a DOD Executive Agent for a particular matter with simply the agreement of the other Services; such authority must be delegated by the Secretary of Defense. Designation as executive agent, in and of itself, confers no authority. The exact nature and scope of the authority delegated must be stated in the document designating the executive agent. An executive agent may be limited to providing only administration and support or coordinating common functions or it may be delegated authority, direction, and control over specified resources for specified purposes. (JP1-02)

force protection—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to

enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. (JP 1-02)

friendly force information requirements—Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition, readiness, personnel status, and logistics status could become a friendly force information requirement. Also called FFIR. (MCRP 5-12C)

fusion—In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 1-02)

global sourcing—A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

ground combat element—The core element of a Marine air-ground task force that is task-organized to conduct ground operations. It is usually constructed around an infantry organization but can vary in size from a small ground unit of any type, to one or more Marine divisions that can be independently maneuvered under the direction of the MAGTF commander. The ground combat element itself is not a formal command. Also called GCE. (JP 1-02)

helicopter landing zone—A specified ground area for landing assault helicopters to embark or disembark troops and/or cargo. A landing zone may contain one or more landing sites. (JP 1-02)

high-payoff target—A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through wargaming, which must be acquired and successfully attacked for the success of the friendly commander's mission. Also called HPT. (JP 1-02)

high-value target—A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. Also called HVT. (JP 1-02)

human intelligence—A category of intelligence derived from information collected and provided by human resources. Also called HUMINT. (JP 1-02) In Marine Corps usage, HUMINT operations cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of CI force protection source operations. (MCRP 5-12C)

imagery—Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices or other media. (JP 1-02)

imagery exploitation—The cycle of processing and printing imagery to the positive or negative state, assembly into imagery packs, identification, interpretation, mensuration, information extraction, the preparation of reports, and the dissemination of information. (JP 1-02)

imagery intelligence—Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices or other media. Also called IMINT. (JP 1-02)

imagery interpretation—1. The process of location, recognition, identification, and description of objects, activities, and terrain represented on imagery. (NATO) **2.** The extraction of information from photographs or other recorded images. Also called interpretation. (JP 1-02)

indications and warning—Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political,

or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear or non-nuclear attack on the United States, its overseas forces, or allied and/or coalition nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (JP 1-02)

indications (intelligence)—Information in various degrees of evaluation, all of which bears on the intention of a potential enemy to adopt or reject a course of action. (JP 1-02)

indicator—In intelligence usage, an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action. (JP 1-02)

information—1. Facts, data, or instructions in any medium or form. **2.** The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

information exchange requirement—The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom, as well as why the information is necessary and how that information will be used. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement. Also called IER. (MCRP 5-12C)

infrared imagery—That imagery produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared position of the electromagnetic spectrum (approximately 0.72 to 1,000 microns). (JP 1-02)

integration—1. A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. **2.** In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print or the process by which several photographic images are combined into a single image. (JP 1-02)

intelligence—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. **2.** Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02) Also in Marine Corps usage, intelligence is knowledge about the enemy or the surrounding environment needed to support decisionmaking. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence data—Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline—A well defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are seven major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), open-source intelligence, technical intelligence, and counterintelligence. (JP 1-02)

intelligence estimate—The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (JP 1-02)

intelligence preparation of the battlespace—An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive

database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (JP 1-02) In Marine Corps usage, the systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCRP 5-12C)

intelligence-related activities—Those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. (Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.) (JP 1-02)

intelligence report—A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP. (JP 1-02)

intelligence reporting—The preparation and conveyance of information by any means. More commonly, the term is restricted to reports as they are prepared by the collector and as they are transmitted by the collector to the latter's headquarters and by this component of the intelligence structure to one or more intelligence-producing components. Thus, even in this limited sense, reporting embraces both collection and dissemination. The term is applied to normal and specialist intelligence reports. (JP 1-02)

intelligence requirement—Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. Also called IR. (JP 1-02) In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. (MCRP 5-12C)

interpretation—A part of the analysis and production phase in the intelligence cycle in which the significance of information is judged in relation to the current body of knowledge. See also intelligence cycle. (JP 1-02)

joint force—A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (JP 1-02)

joint force commander—A general term applied to a combatant commander, subunified commander or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. Also called JFC. (JP 1-02)

joint intelligence—Intelligence produced by elements of more than one Service of the same nation. (JP 1-02)

joint intelligence center—The intelligence center of the combatant command headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the combatant commander and staff, components, subordinate joint forces and elements, and the national intelligence community. Also called JIC. (JP 1-02)

Joint Worldwide Intelligence Communications System—The sensitive compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (JP 1-02)

landing area—1. That part of the operational area within which are conducted the landing operations of an amphibious force. It includes the

beach, the approaches to the beach, the transport areas, the fire support areas, the airspace occupied by close supporting aircraft, and the land included in the advance inland to the initial objective. **2.** (Airborne) The general area used for landing troops and materiel either by airdrop or air landing. This area includes one or more drop zones or landing strips. **3.** Any specially prepared or selected surface of land, water, or deck designated or used for takeoff and landing of aircraft. (JP 1-02)

landing beach—That portion of a shoreline usually required for the landing of a battalion landing team. However, it may also be that portion of a shoreline constituting a tactical locality (such as the shore of a bay) over which a force larger or smaller than a battalion landing team may be landed. (JP 1-02)

liaison—That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action. (JP 1-02)

main effort—The designated subordinate unit whose mission at a given point in time is most critical to overall mission success. It is usually weighted with the preponderance of combat power and is directed against a center of gravity through a critical vulnerability. (MCRP 5-12C)

maintenance levels—The categories of maintenance and corresponding echelons of maintenance are organizational (first and second echelons), intermediate (third and fourth echelons), and depot (fifth echelon). (MCO 4790.2C)

maneuver warfare—A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. (MCRP 5-12C)

Marine air-ground task force—The Marine Corps principal organization for all missions across the range of military operations, composed of forces task-organized under a single commander capable of responding rapidly to a contingency anywhere in the world. The types of forces in the Marine air-ground task force (MAGTF) are functionally grouped into four core elements: a command element, an aviation combat element, a ground combat element, and a combat service support element. The four core elements are categories of forces, not formal commands. The basic structure of the Marine air-ground task force never varies, though the number, size, and type of Marine Corps units comprising each of its four elements will always be mission dependent. The flexibility of the organizational structure allows for one or more subordinate MAGTFs, to be assigned. Also called MAGTF. (JP 1-02)

Marine Corps Planning Process—A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of mission analysis, course of action development, course of action analysis, comparison/decision, orders development, and transition. Also called MCPP. NOTE: Tenets of the MCPP include top down planning, single battle concept, and integrated planning. (MCRP 5-12C)

Marine expeditionary force—The largest Marine air-ground task force (MAGTF) and the Marine Corps principal warfighting organization, particularly for larger crises or contingencies. It is task- organized around a permanent command element and normally contains one or more Marine divisions, Marine aircraft wings, and Marine force service support groups. The Marine expeditionary force is capable of missions across the range of military operations, including amphibious assault and sustained operations ashore in any environment. It can operate from a sea base, a land base or both. Also called MEF. (JP 1-02)

Marine expeditionary unit—A Marine air-ground task force (MAGTF) that is constructed around an infantry battalion reinforced, a helicopter squadron reinforced, and a task-organized combat service support element. It normally fulfills Marine Corps forward sea-based deployment requirements. The Marine expeditionary unit provides an immediate reaction capability for crisis response and is capable of limited combat operations. Also called MEU. (JP 1-02)

Marine expeditionary unit (special operations capable)—The Marine Corps standard, forward-deployed, sea-based expeditionary organization. The MEU(SOC) is a Marine expeditionary unit, augmented with selected personnel and equipment, that is trained and equipped with an enhanced capability to conduct amphibious operations and a variety of specialized missions, of limited scope and duration. These capabilities include specialized demolition, clandestine reconnaissance and surveillance, raids, in-extremis hostage recovery, and enabling operations for follow-on forces. The MEU(SOC) is not a special operations force but, when directed by the National Command Authorities, the combatant commander, and/or other operational commander, may conduct limited special operations in extremis, when other forces are inappropriate or unavailable. It may also contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. Also called MEU (SOC). (JP 1-02)

measurement and signature intelligence—Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target, source, emitter, or sender measurement of the same. The detected feature may be either reflected or emitted. (JP 1-02)

multispectral imagery—The image of an object obtained simultaneously in a number of discrete spectral bands. (JP 1-02)

National Imagery Transmission Format Standard (NITFS)—The standard for formatting digital imagery and imagery-related products and exchanging them among members of the Intelligence Community as defined by the Executive Order 12333, the DOD, and other departments and agencies of the United States Government, as governed by Memoranda of Agreement (MOA) with those departments and agencies. (MIL-STD-2500A)

national intelligence—Integrated departmental intelligence that covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency. (JP 1-02)

near real time—Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP 1-02)

open source intelligence—Information of potential intelligence value that is available to the general public. Also called OSINT. (JP 1-02)

operational control—Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority

is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization or unit training. Also called OPCON. (JP 1-02)

order of battle—The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called OOB. (JP 1-02)

photogrammetry—The science or art of obtaining reliable measurements from photographic images. (JP 1-02)

priority intelligence requirements—Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called PIR. (JP 1-02) In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCRP 5-12C)

production management—Encompasses determining the scope, content, and format of each intelligence product, developing a plan and schedule for the development of each product, assigning priorities among the various production requirements, allocating processing, exploitation, and production resources, and integrating production efforts with intelligence collection and dissemination. (MCRP 5-12C)

radar imagery—Imagery produced by recording radar waves reflected from a given target surface. (JP 1-02)

reach back—The ability to exploit resources, capabilities, expertise, etc. not physically located in the theater or a joint operations area, when established. (MCRP 5-12C)

rear area—For any particular command, the area extending forward from its rear boundary to the rear of the area assigned to the next lower level of command. This area is provided primarily for the performance of support functions. (JP 1-02)

rules of engagement—Directives issued by competent military authority which delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE. (JP 1-02)

safe area—A designated area in hostile territory that offers the evader or escapee a reasonable chance of avoiding capture and of surviving until he can be evacuated. (JP 1-02)

sanitize—To revise a report or other document in such a fashion as to prevent identification of sources, or of the actual persons and places with which it is concerned, or of the means by which it was acquired. Usually involves deletion or substitution of names and other key details. (JP 1-02)

sensitive compartmented information—All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DOD 5200.1-R, Information Security Program Regulation.) Also called SCI. (JP 1-02)

sensor data—Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radars, counterbattery radars, and remote ground sensors. (MCRP 5-12C)

signals intelligence—1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. **2.** Intelligence derived from communications,

electronics, and foreign instrumentation signals. Also called SIGINT. (JP 1-02)

situational awareness—Knowledge and understanding of the current situation which promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. Also called SA. (MCRP 5-12C)

source—1. A person, thing, or activity from which information is obtained. **2.** In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. **3.** In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. (JP 1-02)

special operations—Operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic or informational objectives by unconventional military means in hostile, denied or politically sensitive areas. These operations are conducted across the full range of military operations, independently or in coordination with operations of conventional, non-special operations forces. Political-military considerations frequently shape special operations, requiring clandestine, covert, or low visibility techniques and oversight at the national level. Special operations differ from conventional operations in degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets. Also called SO. (JP 1-02)

special purpose Marine air-ground task force—A Marine air-ground task force organized, trained and equipped with narrowly focused capabilities. It is designed to accomplish a specific mission, often of limited scope and duration. It may be any size, but normally it is a relatively small force-the size of a Marine expeditionary unit or smaller. It may contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. Also called SPMAGTF. (JP 1-02)

split base—Two or more portions of the same force conducting or supporting operations from separate physical locations. (MCRP 5-12C)

surveillance—The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic or other means. (JP 1-02)

sustained operations ashore—The employment of Marine Corps forces on land for an extended duration. It can occur with or without sustainment from the sea. Also called SOA. (MCRP 5-12C)

synthetic aperture radar—A radar in which a synthetically long apparent or effective aperture is constructed by integrating multiple returns from the same ground cell, taking advantage of the Doppler effect to produce a phase history film or tape that may be optically or digitally processed to reproduce an image. (MIL-HDBK-850)

tactical intelligence—Intelligence that is required for planning and conducting tactical operations. (JP 1-02) In Marine Corps usage, tactical intelligence is concerned primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather within the battlespace. (MCRP 5-12C)

tactical warning—1. A warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources.

2. In satellite and missile surveillance, a notification to operational command centers that a specific threat event is occurring. The component elements that describe threat events are: Country of origin-country or countries initiating hostilities. Event type and size-identification of the type of event and determination of the size or number of weapons. Country under attack-determined by observing trajectory of an object and predicting its impact point. Event time-time the hostile event occurred. Also called integrated tactical warning. (JP 1-02)

target—1. A geographical area, complex or installation planned for capture or destruction by military forces. **2.** In intelligence usage, a country, area, installation, agency or person against which intelligence operations are directed. **3.** An area designated and numbered for future firing. **4.** In gunfire support usage, an impact burst which hits the target. (JP 1-02)

target intelligence—Intelligence which portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (JP 1-02)

technical control—The performance of specialized or professional service or the exercise of professional guidance or direction through the establishment of policies and procedures. (Proposed USMC definition for next revision of MCRP 5-12C.)

terrain intelligence—Intelligence on the military significance of natural and manmade characteristics of an area. (JP 1-02)

unconventional warfare—A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape. Also called UW. (JP 1-02)

validation—A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. (JP 1-02)

warfighting functions—The six mutually supporting military activities integrated in the conduct of all military operations are:

1. command and control—The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.

2. maneuver—The movement of forces for the purpose of gaining an advantage over the enemy.

3. fires—Those means used to delay, disrupt, degrade or destroy enemy capabilities, forces or facilities as well as affect the enemy's will to fight.

4. intelligence—Knowledge about the enemy or the surrounding environment needed to support decisionmaking.

5. logistics—All activities required to move and sustain military forces.

6. force protection—Actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing or eliminating friendly critical vulnerabilities.

Also called WF. (MCRP 5-12C)

APPENDIX O. REFERENCES AND RELATED PUBLICATIONS

Presidential Executive Orders

12333	United States Intelligence Activities
12334	President's Intelligence Oversight Board

Director of Central Intelligence Directives (DCIDs)

1/14	Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information
1/16	Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks
1/21	Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)

Department of Defense Directives (DODDs)

5040.5	Alteration of Official DoD Imagery
5200.1	DoD Information Security Program
5240.1	DoD Intelligence Activities

Department of Defense (DOD) Manuals

5105.21-M-1	Sensitive Compartmented Information (SCI) Administrative Security Manual
5240.1-R	Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons

Department of Defense (DOD) Publications

TS-5105.21-M-2	Sensitive Compartmented Information (SCI) Security Manual, Communications Intelligence (COMINT) Policy
TS-5105.21-M-3	Sensitive Compartmented Information (SCI) Security Manual, TK Policy

Defense Intelligence Agency Manuals (DIAMs)

50-4	Department of Defense Intelligence Information System (DODIIS) Information Systems Security (INFOSEC) Program

58-5	Imagery Requirements (U) SECRET/US ONLY SAO Supplement
R 50-7	Department of Defense Exploitation of Multisensor Imagery

Joint Publications (JPs)

1-02	Department of Defense Dictionary of Military and Associated Terms
2-0	Doctrine for Intelligence Support to Joint Operations
2-01	Joint Intelligence Support to Military Operations
2-02	National Intelligence Support to Joint Operations
2-03	Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations
3-02	Joint Doctrine for Amphibious Operations
3-13.1	Joint Doctrine for Command and Control Warfare (C2W)
3-54	Joint Doctrine for Operations Security
5-0	Doctrine for Planning Joint Operations
6-0	Doctrine for C4 Systems Support to Joint Operations

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
2	Intelligence
3	Expeditionary Operations
4	Logistics
5	Planning
6	Command and Control

Marine Corps Warfighting Publications (MCWPs)

2-1	Intelligence Operations
2-12	MAGTF Intelligence Production and Analysis
2-12.1	Geographic Intelligence
2-15.2	Signals Intelligence
3-40.3	Communications and Information Systems

Marine Corps Reference Publications (MCRPs)

5-12C	Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms
5-12D	Organization of Marine Corps Forces

Fleet Marine Force Reference Publication (FMFRP)

5-71	MAGTF Aviation Planning Documents

Marine Corps Order (MCO)

3500.32	Intelligence Training and Readiness Manual

U.S. Army Field Manuals (FMs)

34-2	Collection Management and Synchronization Planning
34-130	Intelligence Preparation of the Battlefield (IPB)

Miscellaneous

Joint Tactical Exploitation of National Systems (JTENS) Manual

Imagery System Overview (IMSO)

National Imagery System User's Guide (NIMSUG)

National Imagery Interpretability Rating Scale (NIIRS)

National Imagery and Mapping Agency Imagery Policy Series (Sections 1-9)

MCRP 2-10B.5
(Formerly MCWP 2-21)

Imagery Intelligence

US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000243 00

CD&I (C 116)

2 May 2016

ERRATUM

to

MCWP 2-21

IMAGERY INTELLIGENCE

1. Change all instances of MCWP 2-21, *Imagery Intelligence*, to MCRP 2-10B.5, *Imagery Intelligence.*

2. Change PCN 143 000088 00 to PCN 144 000243 00

3. File this transmittal sheet in the front of this publication.

PCN 144 000243 80

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, D.C. 20350-3000

29 February 2016

FOREWORD

Marine Corps Doctrinal Publication 2, *Intelligence*, and Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations*, describe the doctrine and higher order tactics, techniques, and procedures employed in intelligence operations. Marine Corps Warfighting Publication 2-21, *Imagery Intelligence*, complements these publications by detailing the specific doctrine and tactics, techniques, and procedures for producing and collecting imagery intelligence (IMINT) in support of Marine Corps operational requirements.

The primary target audience of this publication is intelligence personnel responsible for the planning and execution of IMINT operations. Personnel who provide support to intelligence requirements through imagery operations, or personnel who utilize imagery intelligence, will also benefit from studying this publication.

Marine Corps Warfighting Publication 2-21 describes all aspects of IMINT, including basic doctrine, command and control relationships, communications and information systems, planning and execution, equipment, security, and training. It provides the fundamental information Marines need to understand, plan, and execute IMINT operations in support of the operating forces.

This publication supersedes MCWP 2-21, *Imagery Intelligence*, dated 6 September 2002, (formerly MCWP 2-15.4, modified to current short title by erratum dated 13 July 2004).

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

ROBERT S. WALSH
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development and Integration

Publication Control Number: 143 000088 00

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

Table of Contents

Chapter 1. Fundamentals

Introduction to Geospatial Intelligence 1-1
Elements of Geospatial Intelligence 1-1
Components of Geospatial Intelligence 1-2
Marine Corps Geospatial Intelligence Enterprise 1-3
Mission 1-3
Purpose 1-3
Method 1-3
Imagery Versus Imagery Intelligence 1-3
Objectives of Imagery Intelligence 1-4
Capabilities and Limitations of Imagery Intelligence 1-4
Capabilities 1-4
Limitations 1-4
Responsibilities and Products 1-4
Marine Corps Imagery Intelligence Responsibilities 1-5
Types of Imagery Intelligence Products 1-6
Role and Functions 1-6
Tactical Imagery Intelligence Principles 1-7
Focus on Tactical Intelligence 1-7
Centralized Management 1-7
G-2/S-2 Facilitation 1-7
Tailored and Timely Intelligence 1-7
Intelligence and Imagery Intelligence Cycles 1-8
General 1-8
Tasking, Collection, Processing, Exploitation, and Dissemination Process 1-8
Imagery-Derived Products 1-10
G-2/S-2 Role in the Intelligence Cycle 1-11
Levels of Imagery Intelligence 1-12
National Imagery Intelligence 1-13
Tactical Imagery Intelligence 1-13
Theater Imagery Intelligence 1-15

Chapter 2. Organizations and Responsibilities

Marine Expeditionary Force Key Personnel Responsibilities 2-1
Role of the Commander 2-1
Marine Expeditionary Force Command Element: G-2 Section and the Intelligence Battalion 2-2
Marine Expeditionary Force Command Element: Other Staff Sections 2-9
Intelligence Officers at Marine Expeditionary Force Major Subordinate Commands 2-10

National Imagery Organizations 2-10
Office of the Director of National Intelligence 2-10
National Geospatial-Intelligence Agency 2-11
National Intelligence Support Team 2-12
National Reconnaissance Office 2-15
Defense Intelligence Agency 2-15
Marine Corps Supporting Establishment Imagery Intelligence Organizations 2-15
Headquarters, United States Marine Corps 2-15
Deputy Commandant for Combat Development and Integration 2-16
Marine Corps Systems Command 2-16
Marine Corps Intelligence Activity 2-17
National Geospatial-Intelligence Agency Support Teams 2-17

Chapter 3. MAGTF Imagery Intelligence Units and Organizations

Imagery Intelligence Platoon Intelligence Battalion 3-1
Mission and Tasks 3-1
Organization 3-1
Command and Control 3-2
Concept of Employment 3-3
Miscellaneous 3-3
Tactical Analysis and Combat Tracking Exploitation Team, Intelligence Battalion 3-5
Mission and Tasks 3-5
Organization 3-6
Command and Control 3-6
Concept of Employment 3-6
Miscellaneous 3-7
Marine Unmanned Aerial Vehicle Squadron 3-8
Mission and Tasks 3-8
Organization 3-8
Command and Control 3-8
Concept of Employment 3-9
Miscellaneous 3-9
Marine Fighter/Attack (All-Weather) Squadron 3-10
Mission and Tasks 3-10
Organization 3-10
Command and Control 3-11
Concept of Employment 3-11
Miscellaneous 3-11
Ground Reconnaissance 3-12
Mission 3-12
Organization 3-12
Command and Control 3-13
Concept of Employment 3-13

Chapter 4. Imagery Intelligence Systems, C2 Nodes, CIS, and Other Systems

Basic Imagery Intelligence Communications and Information Systems Requirements 4-1
Managing Subordinate Imagery Intelligence Units 4-1
Receiving Data and Information From Organic/External Imagery Intelligence Organizations 4-1
Providing Intelligence to Supported Commanders 4-1
Providing Imagery Intelligence Products and Reports to National Intelligence Centers, Theater, Joint Task Force, MAGTF, and Other Components 4-1
Imagery Intelligence and Related Command and Control Nodes 4-2
Combatant Commander Joint Intelligence Operation Center 4-2
Joint Task Force J-2 and the Joint Intelligence Support Element 4-2
Marine Expeditionary Force Command Element 4-3
Imagery Intelligence Information Systems and Supporting Communications 4-7
Imagery Direction and Collection Management 4-7
Geospatial Intelligence Information Management Services 4-9
Imagery Collection 4-9
Imagery Tasking, Processing, Exploitation, and Dissemination Capabilities 4-16
Imagery Communications and Information Systems Architecture 4-17
Geospatial Intelligence Communications and Information Systems Planning Considerations 4-17

Chapter 5. Planning

Support to the Planning Process 5-1
Planning for Imagery Intelligence 5-1
Types of Imagery 5-9
Aerial Imagery Collection Missions 5-12
Processing, Exploitation, and Dissemination of Imagery and Imagery Intelligence 5-14

Chapter 6. Training

Imagery Training 6-1
Requirements 6-1
Training Objectives 6-1
Planning and Employment Training 6-2
MAGTF Training 6-2
Training Courses 6-3
Basic-Level: Tactical Imagery Analysis Course 6-3
Intermediate- and Advanced-Level Training 6-4
Follow-On Training Subject Areas 6-5

Appendices

A Imaging Sensors A-1

B Imagery and Supporting Intelligence Reports B-1

C Imagery Intelligence Support to Intelligence Studies C-1

D National Imagery Interpretability Rating Scale D-1

E Video National Imagery Interpretability Rating Scale E-1

F Imagery Intelligence Report Formats F-1

G Example of a Marine Unmanned Aerial Vehicle Squadron Equipment and Performance Characteristics G-1

H Request Formats for Aerial Imagery Collection Missions H-1

I Target Folders I-1

J National Imagery Transmission Format Compression J-1

K Imagery Intelligence Appendix Format K-1

L Unmanned Aircraft System Formats L-1

M Aerial Imagery Plan Format M-1

Glossary

References and Related Publications

To Our Reader

CHAPTER 1
FUNDAMENTALS

INTRODUCTION TO GEOSPATIAL INTELLIGENCE

Geospatial intelligence (GEOINT) was originally formed by integrating imagery, imagery intelligence (IMINT), and geospatial information. The meteorological and oceanographic (METOC) capability was added to the discipline in 2006. Advances in technology, along with the development of geospatial data standards, have created an environment in which the elements of GEOINT can be combined with one another as well as with other information sources. This fusion of resources has provided the means for conducting complex analysis and creating new specialized products.

Elements of Geospatial Intelligence

Geospatial intelligence is composed of four elements: imagery, IMINT, geospatial information, and METOC information.

Imagery. Imagery is a likeness or presentation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems and likenesses or presentations produced by satellites, airborne platforms, unmanned aircraft systems (UASs), or other similar means.

Imagery Intelligence. Imagery intelligence is derived from the exploitation of collected images—by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar (SAR)—wherein the images are reproduced optically or electronically on film, electronic display devices, or other media.

Geospatial Information. Geospatial information identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth. Geospatial information includes statistical data and information derived from remote sensing, mapping, and surveying technologies as well as mapping, charting, geodetic data and related products.

Meteorological and Oceanographic. Collectors of METOC information assess and characterize the current and future conditions, phenomena, and associated effects influencing the operational area's physical environment and integrate these time-sensitive essential elements of information (EEIs) into the continuous Marine Corps Planning Process (MCPP) to mitigate adverse conditions/exploit conditions of opportunity.

Components of Geospatial Intelligence

The components of GEOINT are the GEOINT discipline, GEOINT data, and GEOINT products and services.

The Geospatial Intelligence Discipline. Geospatial intelligence encompasses all of the activities related to the planning, collection, processing, analysis, exploitation, and dissemination of spatial information in order to gain intelligence about the national security or operational environment, depict this knowledge visually, and fuse the acquired knowledge with other information through analysis and visualization processes.

Geospatial Intelligence Data. Geospatial data refers to any data used to create GEOINT products. This data can be derived from either a single source or from multiple classified or unclassified sources. Analysts within the GEOINT discipline also incorporate data from other intelligence disciplines, such as human intelligence (HUMINT) or signals intelligence (SIGINT), to create fused all-source intelligence products.

Geospatial Intelligence Products and Services. Geospatial intelligence products range from standard geospatial data-derived products to specialized products that incorporate data from multiple sensors.

Standard Products. These data-derived products (i.e., maps, charts, imagery and digital information to support visualization activities such as a common operational picture [COP]) may be used alone or with multiple layers of data (e.g., vegetation, culture, languages, and weather) and intelligence information. Standard products are derived primarily from electro-optical (EO) sensors and existing geospatial data.

Specialized Products. Each specialized product is tailored for a particular purpose. The products may be developed using advanced technology to integrate multiple types of geospatial data as well as data from other intelligence sources; they may even incorporate the fourth dimension—time. These features enable analysts to create more comprehensive GEOINT products (e.g., two-color multiview, change detection, multi/hyper-spectral, line-of-sight products; environmental intelligence products; and fly-through studies).

Geospatial Intelligence Services. Geospatial intelligence services include all of the tools that enable users to access and manipulate data, such as the following:

- Geodetic surveys.
- Software development.
- Products and services tailored to support weapon systems.
- Calculation of precise locations for targeting of precision munitions.
- Training.
- On-site technical support.

MARINE CORPS GEOSPATIAL INTELLIGENCE ENTERPRISE

The Marine Corps GEOINT Enterprise is the geospatial component of the Marine Corps Intelligence, Surveillance, and Reconnaissance-Enterprise (MCISR-E) providing geospatial information and services (GI&S) to meet Marine Corps requirements.

Mission

The Marine Corps GEOINT Enterprise provides timely, relevant, and accurate GEOINT for planning, decisionmaking, and action in support of Marine Corps, joint, and combined operations.

Purpose

The Marine Corps GEOINT Enterprise integrates GEOINT systems, sensors, processes, and organizations into the distributed common ground/surface system-Marine Corps (DCGS-MC) and the larger MCISR-E architecture in order to provide a horizontally and vertically integrated GEOINT Enterprise that is capable of supporting all Marine Corps operational objectives.

Method

The Marine Corps adheres to established data standards to facilitate data sharing across the enterprise. This compliance enables end users to manipulate existing data for their particular mission requirements rather than recollecting data from previously serviced targets.

IMAGERY VERSUS IMAGERY INTELLIGENCE

Imagery and IMINT are not the same thing. Imagery is a likeness or representation containing embedded positional data; it has not yet been analyzed or evaluated against other intelligence. Imagery intelligence, on the other hand, is the function performed by the G-2/S-2 that involves imagery analysis and integration with other intelligence-related activities to produce all-source intelligence products. Imagery interpretation personnel conduct planning and perform tasking, collection, processing, exploitation, and dissemination (TCPED) of intelligence to the commander. Properly trained personnel, adequate time, and sophisticated equipment are needed to produce and provide IMINT. Raw imagery may be disseminated to tactical commanders in support of operations; however, caution must be exercised to ensure those commanders are aware of the potential for misleading information when intelligence is based on a single, unevaluated source. Imagery intelligence aids commanders and planners in the following two ways:

- It provides situational awareness of the natural, manmade, and cultural terrain in support of the intelligence preparation of the battlespace (IPB).
- It is a source for confirming the analysis produced by other intelligence disciplines.

OBJECTIVES OF IMAGERY INTELLIGENCE

The objectives of imagery intelligence are to increase the situational awareness of the commander and provide counterintelligence and force protection support. Imagery intelligence supports the commander's decisionmaking process by reducing uncertainty about the situation and the surrounding environment. It supports the identification of hostile intelligence collection operations, aids with the identification of Marine air-ground task force (MAGTF) vulnerabilities that could be exploited by the enemy, and assists with the evaluation of friendly security measures to counter these vulnerabilities.

CAPABILITIES AND LIMITATIONS OF IMAGERY INTELLIGENCE

Imagery intelligence has discipline-specific capabilities and limitations.

Capabilities

Imagery intelligence provides detailed and precise information regarding the location and the physical characteristics of the threat and the environment in which it is operating. It is the primary source of information concerning key terrain features, installations, and infrastructure used to build detailed intelligence studies, reports, and target materials. Order of battle (OOB) analysis, enemy course of action (COA) assessments, target intelligence development, and battle damage assessment (BDA) are intelligence functions that rely heavily upon IMINT.

Limitations

The two types of limitations for imagery intelligence are general limitations and sensor limitations.

General Limitations. The general limitations to IMINT are tied to the availability of resources, such as collection platforms, exploitation systems, high capacity communications, skilled personnel, and the time available to complete the TCPED cycle. The intelligence shortfalls associated with these general limitations are compounded by weather effects; enemy air defense capabilities; and enemy camouflage, concealment, and deception (CCD) activities.

Sensor Limitations. See appendix A for information on sensor limitations. It describes the basic capabilities and limitations of EO, radar, and infrared imagery sensors.

RESPONSIBILITIES AND PRODUCTS

The Marine Corps relies on a combination of national, theater, and organic IMINT sources to support both intelligence planning and intelligence operations. The employment of organic MAGTF intelligence collection assets within the assigned area of operations (AO) is not feasible until just prior to the introduction of forces due to the nature of expeditionary operations.

Consequently, national and/or theater intelligence assets should be exploited for IMINT support prior to entering the AO.

The MAGTF leverages external support during the planning and deployment phases of any operation. Even when employed, the MAGTF will continue to require national and theater support in specific areas to add depth and breadth to the reconnaissance effort and cover gaps in organic collection capabilities.

Marine Corps Imagery Intelligence Responsibilities

Imagery intelligence responsibilities differ depending on the type and echelon of the unit.

MAGTF G-2/S-2. The MAGTF assistant chief of staff (AC/S) for intelligence (G-2/S-2) has staff responsibility for intelligence, surveillance, and reconnaissance (ISR)—including support of IMINT operations. In conjunction with the AC/S for operations (G-3/S-3), the G-2/S-2 develops the intelligence operations plan (appendix 16 to annex B), the supporting IMINT plan (appendix 7 to annex B), and the reconnaissance and surveillance plan (appendix 14 to annex B), which allocate resources and assign specific imagery reconnaissance and supporting missions to the MAGTF and supporting elements. Factors affecting the development of intelligence and supporting IMINT plans are as follows:

- Priority intelligence requirements (PIRs).
- Commander's critical information requirements (CCIRs).
- Communications connectivity and information systems.
- Time available.
- Available information and intelligence from other sources.
- Redundancy.
- Assets available.
- Enemy situation.
- Enemy counterreconnaissance capabilities.

The MAGTF G-2/S-2 develops specific intelligence, reconnaissance, and imagery-related tasks based on the commander's intent, anticipated enemy activity, the MAGTF concept of operations (CONOPS), and the overall intelligence operations plan. Individual units are assigned reconnaissance tasks per the intelligence plan. The intelligence support coordinator (ISC), under the staff cognizance of the MAGTF G-2/S-2, establishes an intelligence operations center (IOC).

The Intelligence Operations Center. The IOC is established by the MAGTF G-2/S-2 to perform intelligence requirements management; staff cognizance of ongoing organic and supporting collection operations; and intelligence production, analysis, and dissemination. Key elements of the IOC follow:

- *Support cell*. The support cell is the primary element for conducting Marine expeditionary force (MEF)-wide intelligence requirements management, METOC support, collections and dissemination planning and direction, and intelligence staff cognizance of MEF organic and supporting intelligence and reconnaissance operations.

- *Surveillance and reconnaissance center*. The surveillance and reconnaissance center (SARC) is the primary element that supervises the execution of organic and supporting intelligence and reconnaissance plans.
- *Production and analysis cell*. The primary production and analysis (P&A) element of the MAGTF is the P&A cell. It processes and produces all-source intelligence products in response to requirements of the MAGTF. Additionally, it is the principal IMINT/GEOINT production element of the MEF.

Imagery Intelligence Units in the MAGTF. The MAGTF subordinate units conduct intelligence and reconnaissance planning and operations in support of their own efforts through a variety of means. Close coordination with the ISC and IOC is essential to ensure overall effective MAGTF intelligence operations and intelligence support to all commanders.

Imagery intelligence and imagery-related data and information are collected by a variety of assets, each with unique capabilities and limitations. The following MAGTF units and organizations are likely to be tasked with imagery-related collection missions and production support:

- Intelligence battalions.
- Marine aircraft wings (MAWs): Marine unmanned aerial vehicle squadrons (VMUs), Marine fighter/attack (all weather) squadrons (VMFA[AW]s).
- Force/division reconnaissance units.

Types of Imagery Intelligence Products

Imagery intelligence products include reports, mosaics, overlays, annotated images, and fused intelligence products. For a detailed discussion of imagery and IMINT products, see chapter 5. Appendix B provides examples of imagery products, while appendix C provides details on developing these products.

ROLE AND FUNCTIONS

Imagery intelligence provides MAGTF commanders operational and tactical intelligence support. Imagery and IMINT support the following intelligence functions:

- Support to the commander's estimate.
- Situation development.
- Indications and warning (I&W).
- Force protection.
- Targeting.
- Combat assessment.

TACTICAL IMAGERY INTELLIGENCE PRINCIPLES

The principles of tactical imagery intelligence are a focus on tactical intelligence; centralized management; G-2/S-2 facilitation; and a tailored, timely intelligence support.

Focus on Tactical Intelligence

National and theater imagery assets support operations by all echelons of the MAGTF. The MAGTF IMINT operations combine the generation of tactical intelligence and utilization of strategic/operational IMINT for tactical purposes. Consideration should always be given to TCPED of products in support of MAGTF operations.

While the management of IMINT collection and production is centralized in the MAGTF command element, the overall focus is to support the planning and executing of missions by every element involved in the operation. Critical products are disseminated to tactical commanders, who will be able to request additional IMINT support as required.

Centralized Management

Centralized collection and production management is essential due to the scarcity of IMINT assets, the broad dispersion of supported units, the limitations of range and capability, and the need to focus IMINT resources on the commander's PIRs. This centralizing of effort will be accomplished in the MAGTF IOC under the direction of the intelligence battalion commander functioning as the ISC. The MAGTF commander may attach or place task-organized IMINT elements in direct support of MAGTF subordinate elements.

G-2/S-2 Facilitation

The MAGTF intelligence officer enables effective use of IMINT and other intelligence and reconnaissance activities and products throughout the unit. The MAGTF intelligence officer has three key subordinate officers:

- Intelligence operations officer, who is responsible for managing the information flow between the battle staff and the commander, current and future operations sections, and force fires.
- Intelligence plans officer, who is responsible for supporting the future plans team.
- Intelligence battalion commander, who, as the AC/S G-2's ISC, has principal staff responsibility for both disseminating intelligence throughout the MAGTF and ensuring that intelligence is understood. He must also facilitate responses to any new CCIRs that may result.

Tailored and Timely Intelligence

The guiding principle that underpins all intelligence dissemination activities is to disseminate time sensitive intelligence products to the right people at the right time.

INTELLIGENCE AND IMAGERY INTELLIGENCE CYCLES

The intelligence and imagery intelligence cycle are processes that the Marine Corps uses to develop and utilize intelligence.

General

Intelligence is the output of a process that converts data and information into knowledge that impacts military decisions. The process used to develop intelligence is called the intelligence cycle (see fig. 1-1).

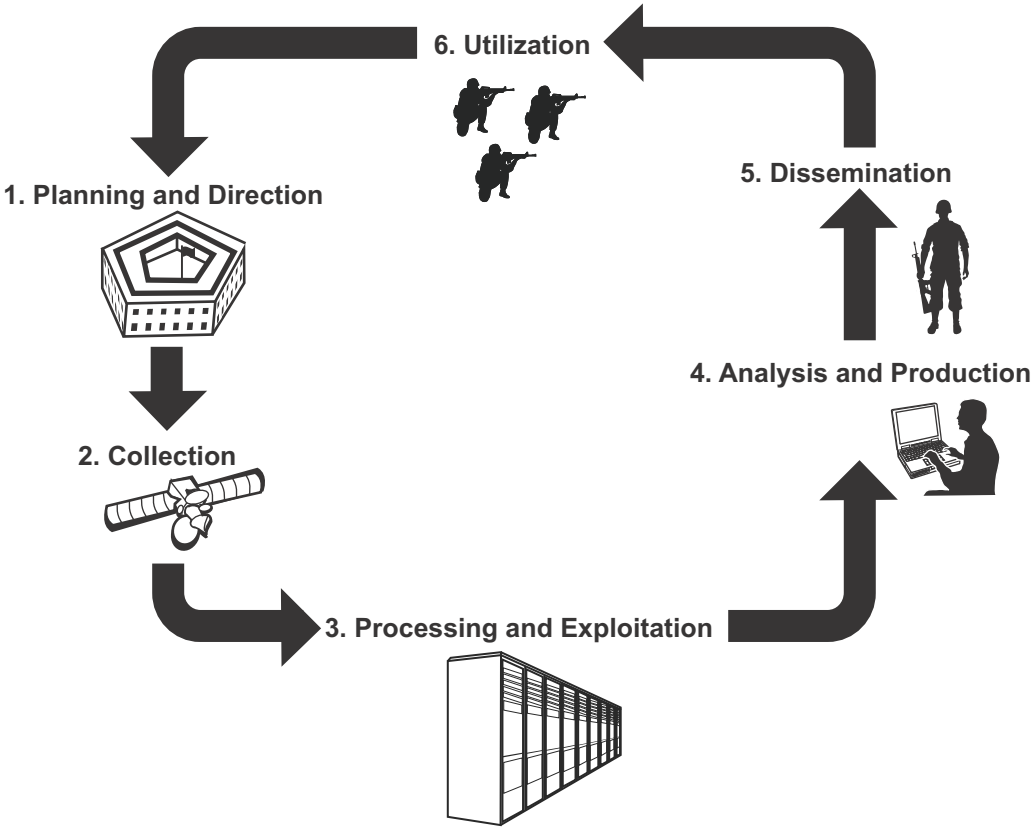


Figure 1-1. United States Marine Corps Intelligence Cycle.

The IMINT cycle mirrors the intelligence cycle. The steps in this cycle define a sequential, interdependent process for developing IMINT. Chapter 5 provides greater details on these cycles.

> ***Note:*** The steps in the Marine Corps intelligence cycle differ from those that constitute the joint intelligence cycle, which de-emphasizes the utilization step of the cycle in favor of continuous evaluation and feedback.

Tasking, Collection, Processing, Exploitation, and Dissemination Process

The TCPED process supports the flow of the intelligence cycle. It begins with the commander's request for information and ends with delivery of IMINT to the end-user. The success of the

TCPED process is tied to the decisionmaking cycle of that end-user (i.e., did the end-user get the IMINT needed to affect the commander's decision).

Tasking. Tasking is the process by which collection assets are assigned to collect against the commander's requirements. Additionally, it implies management of the entire TCPED process. Each user of imagery/GEOINT products will have distributed, seamless, and real-time access to existing databases located at each echelon of command. This access will show the user the coverage and types of information available. If no existing resources cover the requirement, then the user can request new imagery/imagery products (i.e., geospatial source information or a combination of products).

Collection. Collection managers (CMs) create, review, approve, and track imagery collection requirements. Imagery analysts determine whether or not imagery collection requirements have been satisfied and report user satisfaction to the CM.

Processing. Processing involves the conversion of collected data into information that is suitable for the production of intelligence. Processing is accomplished during collection and/or production. Some types of imagery data require minimal processing: they may be collected in a form that is already suitable for production. Other types of imagery data require extensive processing to incorporate amplifying data not available on the raw image products, which affects the timeliness and accuracy of the resulting information.

Exploitation. Exploitation is the extraction, analysis, and compilation of information from collected imagery to answer the CCIRs and EEIs as part of the IPB process. Exploitation occurs at all echelons of the MAGTF. Exploitation is the activity that converts information into intelligence.

The results of exploited and analyzed imagery and imagery data form the basis for IMINT reports and the derived products that are provided directly to tactical commanders, to the G-2/S-2 for inclusion into all-source intelligence products, and to other users. User needs are rarely satisfied by uninterpreted imagery; rather, IMINT exploitation planning and management should be coordinated with all-source intelligence production management and planning. The goal is effective and efficient use of limited resources while ensuring that IMINT production is focused on validated PIRs, intelligence requirements, and associated specified intelligence reporting criteria. This coordination includes:

- Determining the scope, content, and format for each product.
- Planning and scheduling the development of products.
- Assigning priorities among the various IMINT product requirements.
- Determining who needs what products and in what quantities.
- Allocating IMINT processing and exploitation resources.
- Coordinating production efforts with IMINT and all-source collection and dissemination activities.

Still frame imagery is exploited in the following three phases:

- First phase still frame imagery analysis is the rapid exploitation of newly acquired imagery and reporting of imagery-derived information (reconnaissance exploitation report [RECCEXREP]) within a specified time from receipt of imagery. This phase satisfies priority requirements of immediate need and/or identifies changes or activity of immediate significance. First phase still frame imagery analysis results in an initial photographic interpretation report (IPIR).
- Second phase still frame imagery analysis is the detailed exploitation of newly acquired imagery and the reporting of imagery-derived intelligence and information while meeting the production and timeliness requirements. Other intelligence discipline source material may support such imagery as appropriate. Second phase still frame imagery analysis yields a supplemental photographic interpretation report (SUPIR).
- Third phase still frame imagery analysis is the detailed analysis of all available imagery pertinent to a specific information requirement and the subsequent production and reporting resulting from this analysis within a specified time. This phase provides an organized detailed analysis of an imagery target or topic, using imagery as the primary data source but incorporating data from other sources as appropriate.

Likewise, motion imagery is exploited in the following three phases:

- First phase motion imagery analysis includes rapid, real-time callouts (i.e., size, activity, location, unit, time, and equipment [SALUTE] reports) of full motion video (FMV) via voice or chat.
- Second phase motion imagery analysis encompasses initial FMV annotated stills and video. Second phase motion imagery can supplement first phase motion imagery.
- Third phase motion imagery analysis includes in-depth analysis of FMV data, possibly fused with other sources, resulting in an intelligence product.

Dissemination. All echelons of the MAGTF generate information; therefore, the information must flow up and down the echelons of command. Dissemination is the process for providing the MAGTF and other users with products for all operations, including navigation, targeting, operational planning, mission rehearsal, and support to modeling and simulations. Imagery intelligence products are disseminated through all available delivery methods, including multisecurity level, Web-based, accessible storage devices that maintain imagery and IMINT relevant to the customer.

Imagery-Derived Products

Imagery-derived products are secondary products that can be disclosed and released to coalition partners. They are useful for a variety of planning and decisionmaking activities. Several of the most commonly requested products include beach studies, helicopter landing zone (HLZ) studies, and raid studies.

National Imagery Interpretability Rating Scale. Still and motion imagery are also rated for quality of the imagery acquired from various types of imaging systems. The National Imagery Interpretability Rating Scale (NIIRS) is considered the standard for rating image quality by most imagery analysts and scientists. The NIIRS defines different levels of image quality/ interpretability based on the types of tasks an analyst can perform with images of a given NIIRS

rating. The idea is that imagery analysts should be able to perform more demanding interpretation tasks as the quality of the imagery increases. Examples of these scales are in appendices D and E.

Imagery Intelligence Text Products. Imagery intelligence text products are selected to meet the specific needs of the commander. Appendix F provides the format and instructions for completing the RECCEXREP, the IPIR, and the SUPIR.

The RECCEXREP is used to report the results from the first rapid analysis of imagery, including the debriefing of the aircrew when possible. It addresses the targets requested in the original imagery collection mission tasking, normally with each target addressed separately. It is prepared by intelligence personnel, such as the imagery intelligence platoon (IIP), MAW, or Marine logistics group (MLG), based on input from the supporting collecting unit's intelligence section. The report is then disseminated in accordance with the dissemination plan. The specified time limit in which the RECCEXREP must be completed and disseminated must be in accordance with unit standing operating procedure (SOP).

The IPIR provides information regarding tasked imagery collection missions not previously reported (e.g., in the RECCEXREP); when extensive or detailed data from a systematic review of the imagery is required; or when the rapid response required by the RECCEXREP would be hindered by the format, size or quality of the imagery involved. It also is prepared by the IIP (with input from the supporting collecting unit's intelligence section) and disseminated in accordance with the dissemination plan. The timeline for completing this report will be in accordance with the unit SOP.

The SUPIR provides information not previously included in a RECCEXREP or IPIR. It reports on significant targets covered by the mission and other required supplemental data. It is prepared by intelligence personnel, such as the IIP, MAW, or MLG, based on input from the supporting collecting unit's intelligence section. The report is then disseminated in accordance with the dissemination plan. The specified time limit in which the SUPIR must be completed and disseminated will be in accordance with unit SOP.

Size, Activity, Location, Unit, Time, and Equipment Report. The standard SALUTE report is used to report any known or suspected enemy activity. It may also be used to report any characteristics of the AO that affect mission accomplishment. The SALUTE report may be used by a VMU, ground reconnaissance unit, aircrew, or other personnel to report key information obtained during ongoing imagery collection operations. This report will be disseminated in accordance with the dissemination plan: generally from the collector to the SARC or directly from the collector to other supported units.

G-2/S-2 Role in the Intelligence Cycle

Figure 1-2, on page 1-12, depicts the G-2/S-2 role in the intelligence cycle and highlights the relationship of IMINT to MAGTF intelligence requirements and operations. Intelligence requirements can be complex and challenging; rarely will a single intelligence discipline, source, or sensor provide the complete answer to a request. Specific data must be processed and all of the seemingly unrelated, individual pieces of information must be evaluated, analyzed, and integrated into a usable, fused, all-source intelligence product that satisfies particular CCIRs. The planning process is discussed in greater detail in chapter 5.

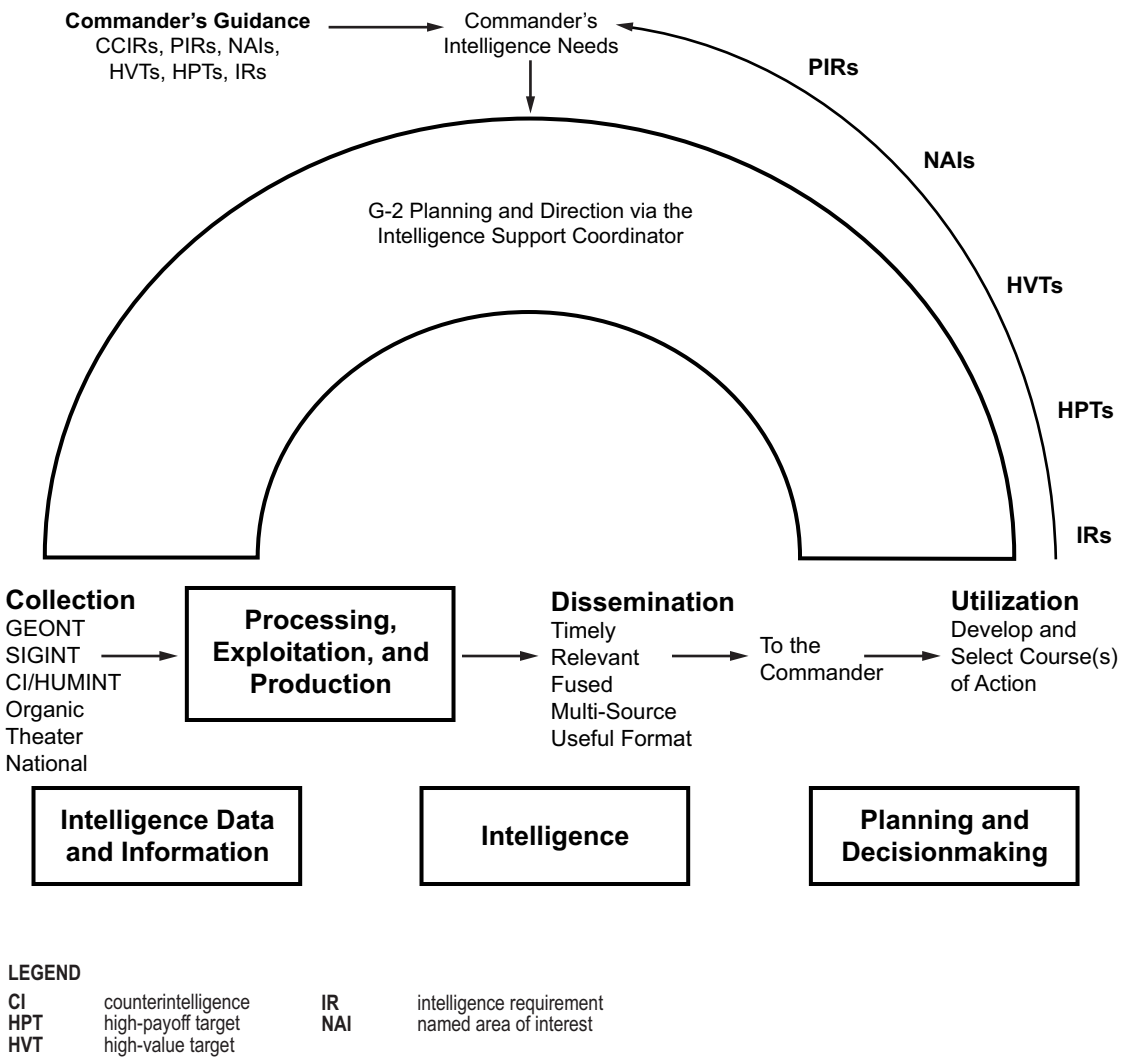


Figure 1-2. Intelligence Officer's Role in the Intelligence Cycle.

LEVELS OF IMAGERY INTELLIGENCE

The MAGTF relies on tactical, theater, and national imagery to support planning and operations. A goal of imagery architecture development is to ensure that imagery products are available to support the MAGTF during all phases of every operation, regardless of geographic location (see fig. 1-3 on page 1-13). External imagery support assists the MAGTF during pre-deployment planning and imagery archive development. It also enables the MAGTF to view denied portions of the AO. As the MAGTF transits to the AO, imagery support is provided by a combination of national and theater assets. Once a MAGTF is within the AO, its organic assets will take on a greater role in providing imagery support.

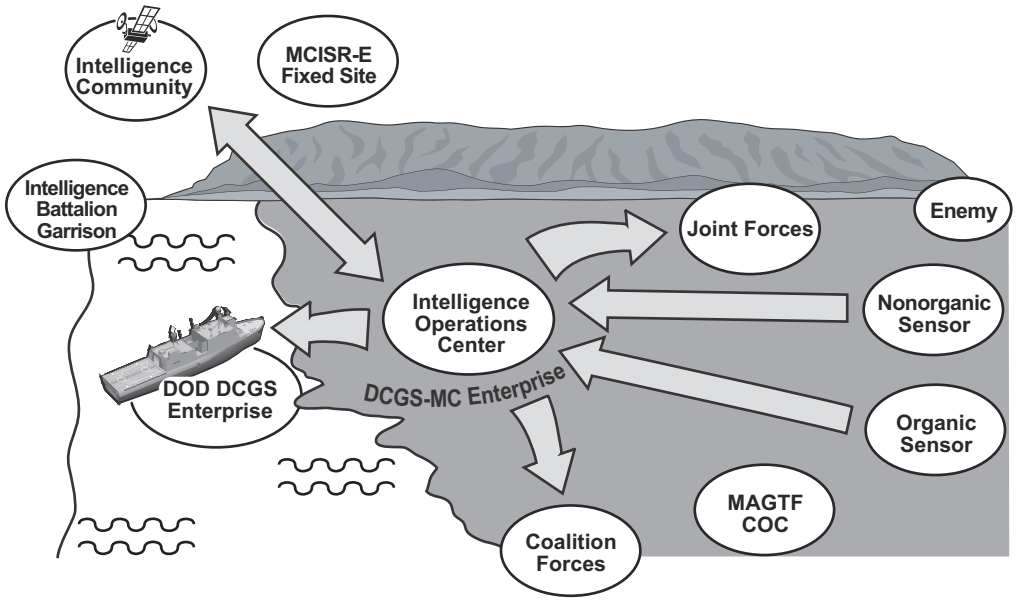


Figure 1-3. Imagery Architecture from IOC to COC.

National Imagery Intelligence

The MAGTF CMs submit requirements for national IMINT support to the appropriate departmental requirements office (DRO) via the appropriate operational chain of command (see fig. 1-4 on page 1-14 and fig. 1-5 on page 1-15). The DRO used is determined by the operational situation and operating environment. As a general rule, all continental United States-based exercises, pre-deployment planning, and/or requirements mandated by the United States Code, Title 10, *Armed Forces*, are submitted via the chain of command to the United States Marine Corps DRO. Once a MAGTF is underway or deployed, requirements are submitted via the operational command for action by the Defense Intelligence Agency (DIA) DRO.

Tactical Imagery Intelligence

Organic collectors of imagery and imagery-related information can support either routine or time-sensitive tactical intelligence. Because MAGTFs are task-organized, their organic capabilities and the degree of external support they require can vary.

Chapters 3 and 4 address Marine Corps imagery organizations and capabilities organic to MAGTFs. Examples of the types of external imagery support the MAGTF may require are discussed in the following subparagraphs.

Pre-deployment. The MAGTF may require the following pre-deployment support:

- MAGTF imagery storage devices loaded with current imagery.
- Pre-deployment packages (e.g., external hard drives, CD ROM[compact disc read-only memory]).

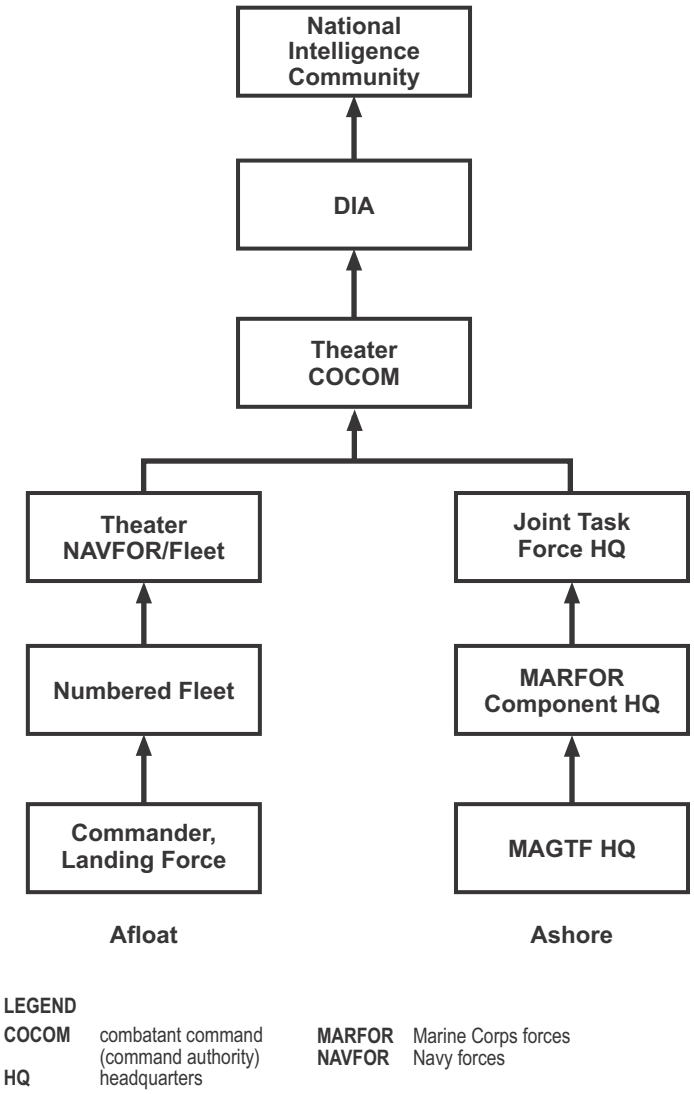


Figure 1-4. External Imagery Support Request Chain.

- Digital imagery database:
  - Area coverage baseline.
  - Baseline target/mission data.
  - Geospatial information.
  - Image maps.

En route to Area of Operations. The MAGTF may require the following support en route to the AO:

- Reachback capability for updated imagery.
- Automatic/profiled update.
- Target-update images.
- Special area imagery.

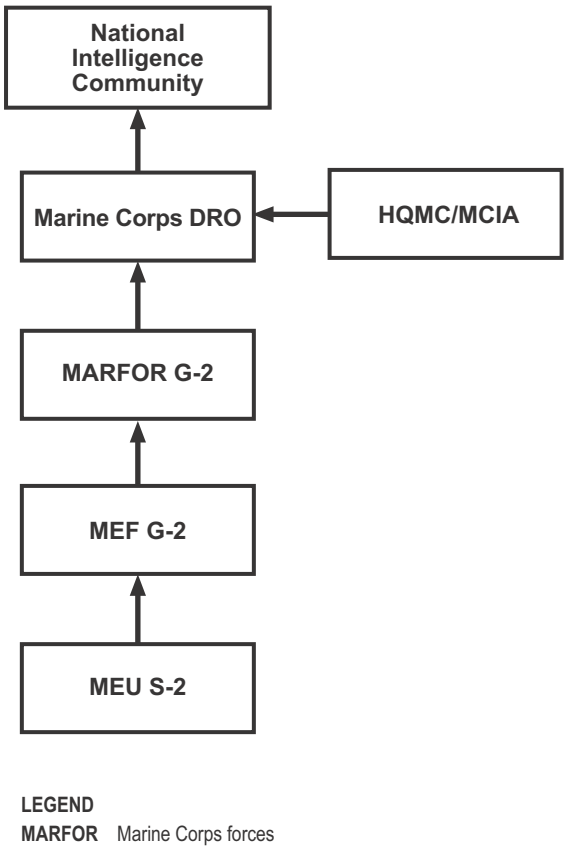


Figure 1-5. Internal Imagery Support Request Chain.

Area of Operations. The MAGTF may require the following support at the AO:

- Reachback and pull capabilities.
- MAGTF operations plan support:
  - Landing zone (LZ) analysis.
  - Mission planning.
  - All-source visualization.
- Air tasking order (ATO) cycle support, including special area imagery.

Theater Imagery Intelligence

Combatant commanders play a significant role in providing imagery support to MAGTFs due to the critical need for component interoperability during joint operations. Joint and theater IMINT is provided by the imagery assets organic to the combatant commander. Their joint intelligence operation centers (JIOCs) and joint analysis centers fulfill operational IMINT requirements of component, subordinate intelligence centers and joint task forces (JTFs).

CHAPTER 2
ORGANIZATIONS AND RESPONSIBILITIES

This chapter describes the roles and responsibilities of organizations and personnel conducting and supporting IMINT operations.

Marine Expeditionary Force Key Personnel Responsibilities

Within the MEF, the key personnel who have specific responsibilities for imagery intelligence operation are the commander, the G-2 staff and intelligence battalion, other staff sections, and intelligence officers at MEF major subordinate commands.

Role of the Commander

The responsibilities of the commander for imagery intelligence are command attention, intelligence requirements, resource allocation, and communications and information systems support.

Command Attention. Intelligence is an essential responsibility of command. The commander's involvement in the intelligence process includes focusing and supporting the intelligence effort, participating in the intelligence process, using intelligence, and providing personal evaluation of the intelligence effort.

Intelligence Requirements. The commander focuses intelligence in general and imagery collection in particular by communicating the commander's intent and planning guidance and the CCIRs, of which PIRs are a part. These later requirements drive all intelligence collection, production, and dissemination activities.

Resource Allocation. Imagery intelligence collection platforms are a high demand, low density asset. Some MAGTF imagery collection platforms have additional mission roles. Consequently, they may be tasked to perform command and control, targeting, electronic warfare (EW), or other intelligence collection missions in addition to imagery collection. Therefore, when it comes to IMINT operations, the commander's role in mission prioritization of organic imagery airborne collection and other IMINT assets is particularly important. A logical, detailed, and realistic concept of intelligence support, developed in accordance with the commander's intent and CONOPS, will facilitate the appropriate allocation of intelligence capabilities between the MAGTF's main and supporting efforts, as well as between intelligence support to current operations and the planning efforts for future operations.

Communications and Information Systems Support. The commander must assess the communication and information systems (CIS) requirements for intelligence against all competing MAGTF CIS's needs to ensure the required support is provided. Ultimately, the extent to which a MAGTF can request/receive JTF, theater, and national imagery support is a function of the connectivity and throughput of this CIS from the tactical level to theater and national levels.

Marine Expeditionary Force Command Element: G-2 Section and the Intelligence Battalion

Within the G-2 section and intelligence battalion, key personnel that have specific responsibilities for imagery intelligence operation are the AC/S G-2, G-2 operations officers, G-2 plans officer, intelligence battalion commander/intelligence support coordinator, collection management/ dissemination officer, surveillance and reconnaissance center officer in charge (OIC), the production and analysis company commander, and the imagery intelligence platoon commander.

Assistant Chief of Staff G-2. The AC/S G-2 has staff responsibility for intelligence and intelligence operations—including IMINT (see fig. 2-1 on page 2-3 and fig. 2-2 on page 2-4). The commander relies on the intelligence officer to keep him informed about the weather and terrain, as well as the capabilities, status, and intentions of enemy forces. The MEF AC/S G-2 uses the intelligence operations plan to formulate and validate intelligence requirements; coordinate intelligence priorities; integrate collection, production, and dissemination activities; allocate resources; assign specific intelligence and reconnaissance missions to subordinate elements; and supervise all intelligence and reconnaissance efforts. The key all-source and IMINT responsibilities of the AC/S G-2 include—

- Developing and answering outstanding CCIRs, PIRs, and intelligence requirements by planning, directing, integrating, and supervising organic IMINT and multidiscipline intelligence operations conducted by the MEF and supporting organizations.
- Preparing appropriate IMINT and other intelligence and reconnaissance plans and orders for the MEF, and reviewing and coordinating the IMINT and all-source intelligence plans developed by other organizations.
- Submitting requests to higher headquarters for JTF, theater/national IMINT systems to support all-source and IMINT collection, production, and dissemination requirements.
- Ensuring IMINT/other intelligence information is processed, analyzed, incorporated (where appropriate in all-source intelligence products), and disseminated to appropriate MEF and external units.
- Evaluating JTF, theater, and national IMINT and all-source intelligence support and adjusting stated intelligence requirements when necessary.
- Identifying and correcting deficiencies in IMINT and other intelligence and reconnaissance personnel and equipment.
- Incorporating exercise IMINT into training exercises to improve individual, collective, and unit readiness within the MEF.
- Facilitating the use of IMINT and other intelligence to support the planning and execution of MEF operations.

G-2 Operations Officer. The G-2 operations officer works directly for the AC/S G-2 and provides support to the commander and the MEF command element for current and future operations. The all-source and IMINT responsibilities of the G-2 operations officer include—

- Coordinating and providing intelligence support (including key IMINT support) to the commanding general, the G-3 operations section, and the remaining MEF command element battle staff.
- Serving as the G-2 representative to the MEF command element crisis action team.

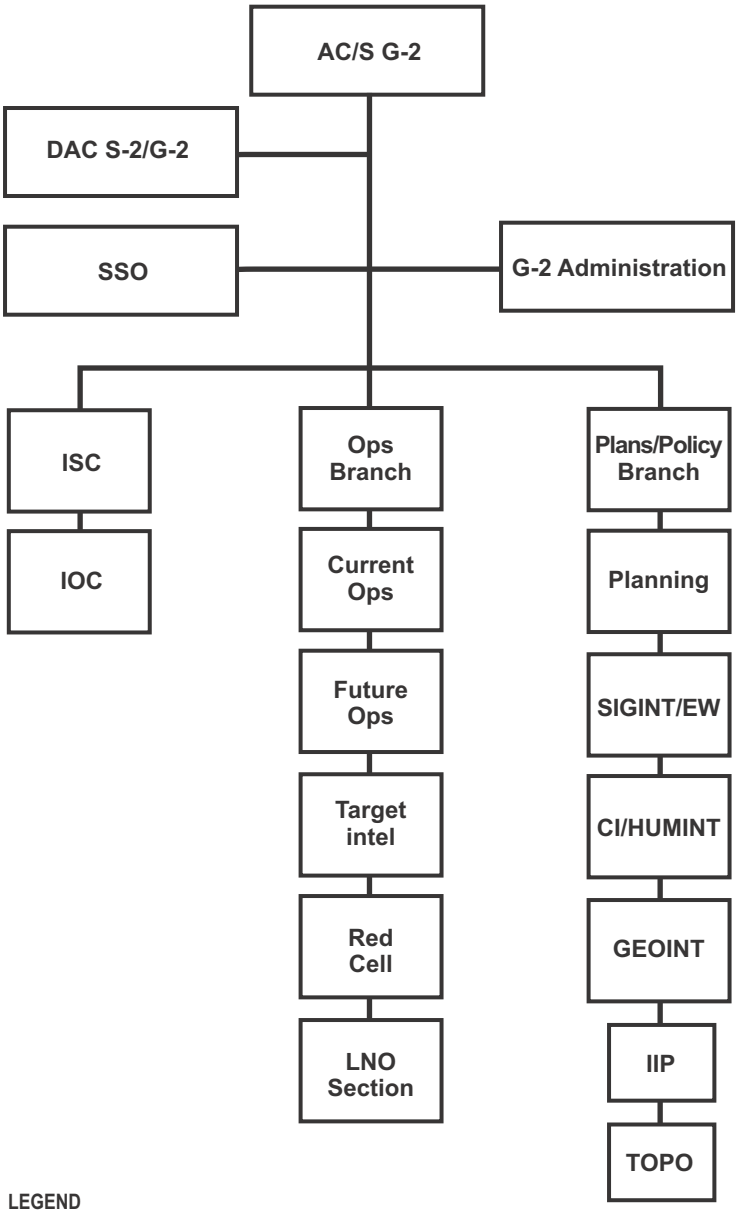
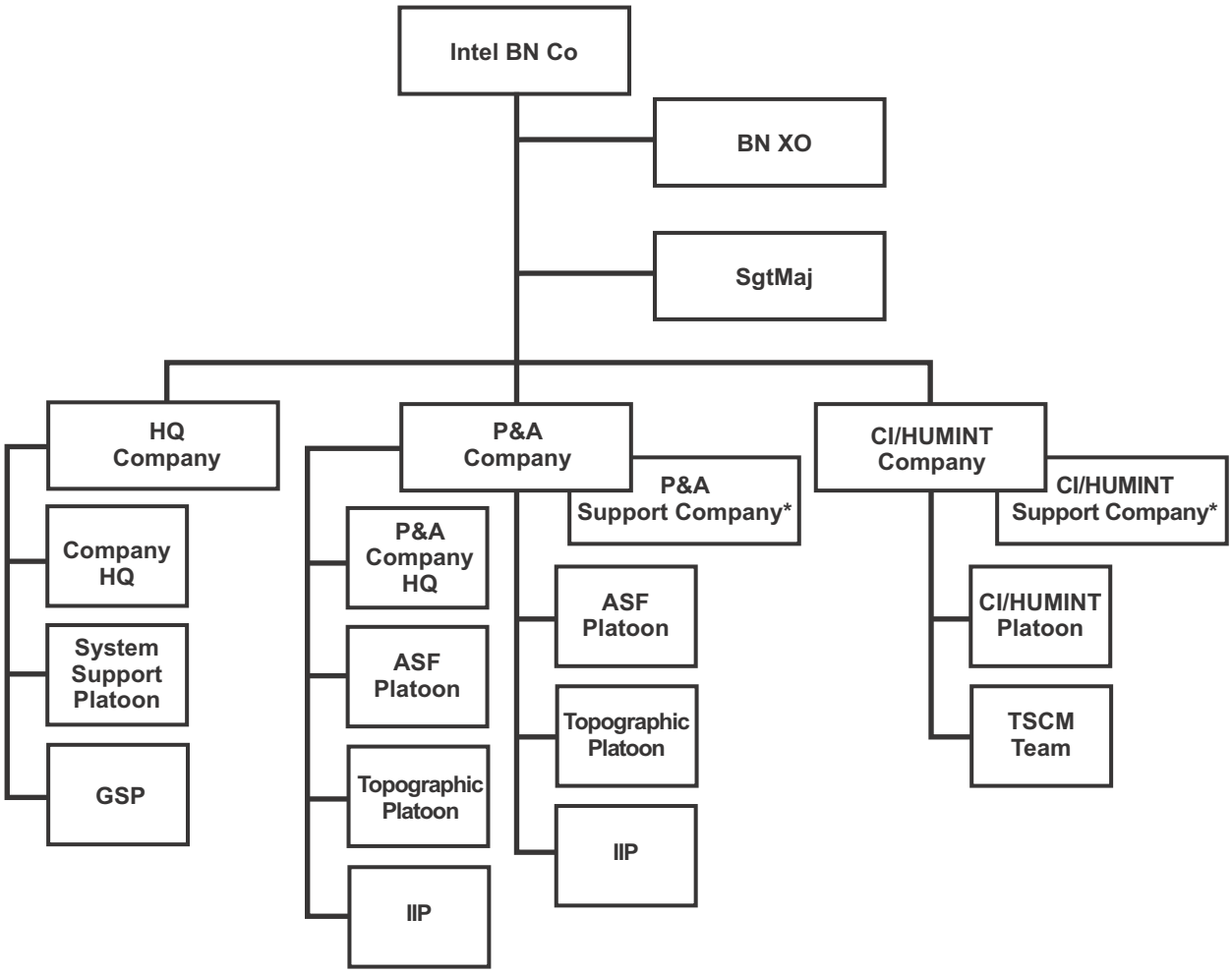


Figure 2-1. Marine Expeditionary Force G-2 Division Principal Staff Officers and Relationships.

- Providing, coordinating, and supervising intelligence support to the MEF command element combat operations center (COC), future operations cell (FOC), and force fires.
- Planning, directing, and supervising the threat or red cell.
- Providing recommendations regarding CCIR, PIR, and intelligence requirement validation, prioritization, and tasking to both the AC/S G-2 and the ISC.
- Coordinating and supervising the transition of intelligence planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations, in order to support the MEF's single battle transition process.



*3d Intelligence Battalion does not have a P&A support company or a CI/HUMINT support company.

LEGEND

ASF	auxiliary security force	**HQ**	headquarters
BN	battalion	**SgtMaj**	sergeant major
CI	counterintelligence	**TSCM**	technical surveillance countermeasures
Co	commanding officer	**XO**	executive officer
GSP	ground sensor platoon		

Figure 2-2. Intelligence Battalion.

- Planning, directing, and supervising MEF liaison officers or teams to external commands (e.g., the JTF and joint functional components headquarters) and intelligence organizations.
- Coordinating with the operations officers and MEF major subordinate commands (MSC) G-2/S-2s to ensure unity of effort of all MEF intelligence operations.
- Providing intelligence input and other support to MEF warning and fragmentary orders and to all other operations-related reporting (e.g., periodic situation reports).
- Coordinating intelligence training for the MEF G-2 section and providing oversight for and implementation of the MEF G-2 intelligence training program.
- Accomplishing other intelligence support tasks as directed by the AC/S G-2.

G-2 Plans Officer. The G-2 plans officer works directly for the AC/S G-2 and provides intelligence support to the G-3 future plans cell. The key all-source and IMINT responsibilities of the G-2 plans officer include—

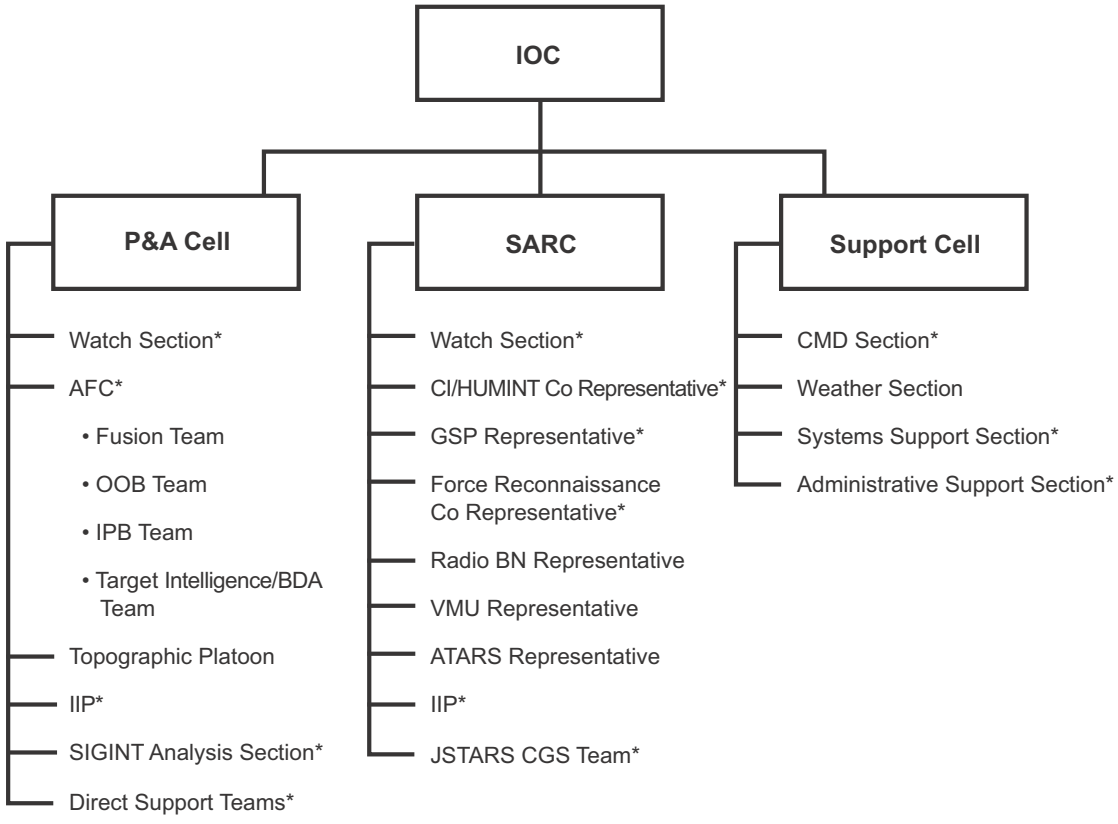
- Planning the MEF concept of intelligence operations for approval by the AC/S G-2, and its subsequent implementation by the ISC based upon the mission, threat, commander's intent, guidance, and CONOPS. This concept of intelligence operations includes a supporting IMINT CONOPS.
- Leading, coordinating, and providing intelligence support to the MEF G-5 future plans section.
- Planning and coordinating intelligence support requirements for the deployment of intelligence elements and resources into the AO.
- Providing recommendations regarding PIR and intelligence requirement validation, prioritization, and taskings to both the AC/S G-2 and the ISC.
- Coordinating with the ISC and G-2 to develop the Annex B (Intelligence), Annex H (METOC), and Annex M (GI&S), as well as their supporting appendices (e.g., Appendix 7, Imagery Intelligence), of MEF operation plans (OPLANs). And in addition, providing intelligence input to other annexes of MEF OPLANs.
- Keeping the G-2 section, other command element staff sections, intelligence liaison personnel, augmentees, and personnel apprised of MEF intelligence planning actions and requirements.
- Identifying requirements and providing recommendations to the G-2 operations officer regarding MEF intelligence liaison teams to external commands (e.g., the JTF or other component headquarters) and intelligence agencies.
- Coordinating and developing policies for MEF intelligence, counterintelligence, and reconnaissance operations.
- Planning, directing, and supervising the MEF G-2's GEOINT (i.e., imagery, METOC, and GI&S), counterintelligence/HUMINT, and SIGINT.
- Accomplishing other intelligence support tasks, as directed by the AC/S G-2.

Intelligence Battalion Commander/Intelligence Support Coordinator. The intelligence battalion commander is responsible for TCPED of intelligence and for providing counterintelligence support to the MEF, MEF MSCs, subordinate MAGTFs, and other commands, as directed. While in garrison, the intelligence battalion commander is responsible for organizing, training, and equipping detachments that will support either MAGTFs or other designated commands by executing integrated collection, intelligence analysis, production, and dissemination of intelligence products.

While operational, the intelligence battalion commander is dual-hatted, also serving as the ISC under the direct staff cognizance of the MEF AC/S G-2. As the ISC, the intelligence battalion commander is responsible to the MEF AC/S G-2 for the overall planning and execution of MEF

all-source intelligence operations. Specific all-source and key IMINT responsibilities of the ISC during actual operations include—

- Implementing the concept of intelligence operations developed by the G-2 plans officer and approved by the AC/S G-2.
- Establishing and supervising operation of the MEF IOC (see fig. 2-3), which includes the support cell, the SARC, and the P&A cell. The IOC will normally be collocated with the MEF command element's main command post.
- Developing, consolidating, validating, and prioritizing recommended PIRs and intelligence requirements to support MAGTF planning and operations.
- Planning, developing, integrating, and coordinating MEF intelligence collection, production, and dissemination plans. Such plans include the effective organic and external integration and employment of MAGTF IMINT as well as staff cognizance of MEF GEOINT; counterintelligence; HUMINT; SIGINT; ground sensor platoon; ground reconnaissance; and tactical air reconnaissance intelligence collections, production, and dissemination operations.



*Personnel provided wholly or partially by intelligence BN.

LEGEND

AFC	all-source fusion center	**Co**	company
BN	battalion	**GSP**	ground sensor platoon
CI	counterintelligence		

Figure 2-3. Intelligence Operations Center.

- Developing, in conjunction with the G-2 operations officer and G-2 plans officer, Annex B (Intelligence), Annex H (METOC), and Annex M (GI&S), as well as their supporting appendices (e.g., Appendix 7, Imagery Intelligence), of MEF operation orders (OPORDs). And in addition, providing intelligence input to other annexes of MEF OPORDs.
- Planning, developing, integrating, and coordinating intelligence and counterintelligence support for the commander's estimate, situation development, I&W, force protection, targeting, and combat assessment.
- Managing and fusing the threat inputs from subordinate units, external commands, and intelligence agencies into the MEF COP/common tactical picture (CTP).
- Providing intelligence support to the G-2 sections at both the MEF and its MSCs.
- Preparing intelligence and counterintelligence estimates to support G-2 plans.
- Planning, developing, and coordinating intelligence CIS architecture, including its integration with and support of MEF IMINT and other intelligence and reconnaissance requirements.
- Coordinating and integrating MEF IMINT and all-source intelligence operations with other Service components, JTF, the joint intelligence support element (JISE), theater JIOC or joint analysis center, and national intelligence agencies, including all aspects of intelligence reachback support such as the Marine Corps Intelligence Activity (MCIA).
- Assisting with the evaluation and improvement of both MEF IMINT and all-source intelligence operations.
- Accomplishing other intelligence support tasks as directed by the AC/S G-2.

Collection Management/Dissemination Officer. The collection management/dissemination officer (CM/DO) is sourced from the S-3 section of the intelligence battalion. The CM/DO is a key subordinate to the intelligence battalion commander/ISC during operations. The CM/DO is responsible for formulating detailed intelligence collection requirements (ICRs) and intelligence dissemination requirements. He is also responsible for tasking and coordinating internal and external operations to satisfy these requirements.

The CM/DO receives PIRs, intelligence requirements, and direction from the ISC; he then plans and manages the employment of organic and supporting collection and dissemination resources (Appendix 16, Intelligence Operations Plan, to Annex B [Intelligence]). Additionally, the CM/DO is responsible for validating and forwarding MEF and MSC collection requests for theater and national IMINT to the appropriate agencies for action. The CM/DO is responsible for coordinating intelligence CIS requirements and maintaining awareness of available CIS connectivity both inside the MAGTF and with key external organizations. During operations, the CM/DO works within the support cell. The CM/DO (in coordination with the P&A company commander, the SARC OIC, G-2 operations officer, and the G-6) determines and coordinates the collection effort of PIRs/ intelligence requirements. The CM/DO is responsible to the ISC for the following several important IMINT-related tasks:

- Recommending dissemination priorities, developing intelligence reporting criteria, and advising on and selecting dissemination means.
- Developing and coordinating IMINT and all-source intelligence collection plans; coordinating and integrating these plans with MEF, other component, JTF, theater, and national intelligence production operations.

- Developing and coordinating IMINT and all-source intelligence dissemination plans and supporting networked communications architectures and coordinating and integrating these requirements with MEF, other component, JTF, theater, and national intelligence CIS and dissemination operations.
- Monitoring the flow of imagery requirements throughout the MAGTF and ensuring imagery products are delivered in a timely manner.
- Evaluating the effectiveness of MEF and supporting IMINT collection and dissemination operations.

Surveillance and Reconnaissance Center Officer in Charge. The SARC OIC supervises the execution of intelligence collection and reconnaissance operations conducted by organic, attached, and direct support assets. The SARC OIC is responsible to the ISC for accomplishing the following specific IMINT-related tasks:

- Coordinating, monitoring, and maintaining the status of all ongoing organic imagery collection operations, including the following:
  - Missions, tasked ICRs, and reporting criteria for collection missions.
  - Locations and times for all pertinent fire support control measures.
  - Primary and alternate CIS plans, which support both routine and time-sensitive requirements for IMINT collectors.
- Ensuring other MAGTF command and control (C2) nodes, such as the current operations center or force fires, are apprised of ongoing IMINT and other intelligence and reconnaissance operations.
- Receiving routine, time-sensitive IMINT-related reports from dispersed collection elements and cross-cueing among intelligence collectors.
- Disseminating IMINT reports according to standing PIR/intelligence requirements, intelligence reporting criteria, dissemination plans, and the current tactical situation.

Production and Analysis Company Commander. The P&A company commander has primary responsibility for coordinating intelligence processing and production requirements directed by the MEF, including the following:

- Planning, directing, and managing operations of the all-source fusion platoon (AFP), IIP, METOC, topographic platoon, direct support teams, and other P&A elements, as directed.
- Coordinating and integrating P&A company operations, estimates, and products with the MEF G-2 sections.
- Planning, managing, and maintaining all-source and GEOINT data.
- Operating, maintaining, and integrating intelligence processing and production systems.
- Analyzing and fusing GEOINT with other intelligence to create tailored all-source intelligence products that satisfy all supported commanders' PIRs and intelligence requirements.

- Developing and maintaining current and future intelligence situational, threat, and environmental assessments and target intelligence based upon all-source analysis, interpretation, and integration.
- Managing and fusing the threat COP/CTP inputs from subordinate units, external commands, and intelligence agencies into the MEF command element's threat COP/CTP.

Imagery Intelligence Platoon Commander. The IIP commander is responsible for planning and providing the MEF, and other commands as directed, with imagery products to support operations. Tasks specific to the IIP commander include the following:

- Exploiting and analyzing all-source, multisensor imagery to derive intelligence pertaining to installations, dispositions, strengths, and activities of various conventional and nonconventional forces.
- Planning and tasking multisensor platforms (both organic platforms and platforms external to the MAGTF).
- Managing imagery data and exploitation.
- Providing imagery-derived products and reports to the MEF commander and other pertinent commanders.
- Conducting liaison activities with the Service intelligence center and pertinent external agencies to obtain imagery products that support MEF intelligence requirements.

Marine Expeditionary Force Command Element: Other Staff Sections

Other staff sections that have specific responsibilities for imagery intelligence are AC/S G-1, AC/S G-3, AC/S G-4, AC/S G-5, and AC/S G-6.

Assistant Chief of Staff G-1—Personnel Section. The AC/S G-1 provides personnel support to the IMINT effort, including coordinating augmentation by qualified personnel. Requests for IMINT personnel augmentation will be developed by the MEF AC/S G-2 and provided to the AC/S G-1 for either internal sourcing or forwarding to higher headquarters for global sourcing.

Assistant Chief of Staff G-3—Operations Section. The AC/S G-3 is responsible for planning, coordinating, and supervising the movement and employment of maneuver units and fires. Imagery intelligence provides valuable support for each of those tasks. Consequently, G-3 personnel must understand the capabilities of the various IMINT collection systems, exploitation capabilities and requirements, and the advantages and limitations of different types of imagery and IMINT products. Additionally, when planning current and future operations, the movement and employment of IMINT personnel and their supporting units must be coordinated between the AC/S G-2 and G-3. Since some imagery supporting units also provide nonintelligence capabilities, close coordination between the AC/S G-2 and G-3 is necessary for mission prioritization and deconfliction.

Assistant Chief of Staff G-4—Logistics Section. The AC/S G-4 is responsible for the logistic support of attached IMINT units. All policies, procedures, and other support requirements should be coordinated between the G-4 and the supported IMINT personnel as soon as possible. Special attention should be directed towards logistic requirements related to the unique (i.e., large/bulky) equipment organic to IMINT units.

Assistant Chief of Staff G-5—Future Plans Section. The AC/S G-5 is responsible for all long-range (i.e., future) planning and joint planning matters. Normally, an AC/S G-5 is found only at the MEF and Marine Forces levels; at lower echelons of the MEF, the AC/S G-3 is responsible for the future planning task. Assistant chief of staff G-5 personnel must understand the capabilities of the various IMINT collection systems, exploitation capabilities and requirements, and the advantages and limitations of different types of imagery and IMINT products.

Assistant Chief of Staff G-6—Communications Systems Section. The AC/S G-6 provides and protects interior and exterior CIS connectivity and operations for the MEF, which includes providing the communication pathways, network accesses, and frequencies for IMINT organizations organic, attached to, and/or supporting the command. Therefore, the AC/S G-6 requires significant systems knowledge across IMINT and all-source intelligence CIS.

Intelligence Officers at Marine Expeditionary Force Major Subordinate Commands

The MSC intelligence officers must understand imagery and IMINT, as well as their capabilities and uses. Additionally, they must be able to integrate IMINT support with other command intelligence and reconnaissance operations. Close coordination among all unit intelligence officers can identify opportunities where small adjustments to IMINT requirements yield results that satisfy the collection/production tasks for more than one unit. Key IMINT-related tasks for MSC intelligence officers include—

- Planning and implementing a concept for intelligence support based on the mission, CONOPS, and commander's intent.
- Providing centralized direction for command intelligence operations, including IMINT elements attached to/placed in direct support of the unit.
- Consolidating, validating, and prioritizing unit intelligence requirements and IMINT needs.
- Submitting consolidated requests for external IMINT support to the MEF command element.
- Coordinating operational and CIS links in support of external IMINT collection and production elements and operations.
- Providing timely and accurate feedback from supported units regarding their level of satisfaction with the IMINT support provided.

NATIONAL IMAGERY ORGANIZATIONS

The national imagery organizations are the Office of the Director of National Intelligence, National Geospatial-Intelligence Agency (NGA), national intelligence support team (NIST), the National Reconnaissance Office (NRO), and the DIA.

Office of the Director of National Intelligence

Two elements of the Office of the Director of National Intelligence are the Director of National Intelligence (DNI) and the DNI organization.

The Director of National Intelligence. The DNI serves as the head of the intelligence community (IC) and is the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security. Additionally, the DNI both oversees and directs the implementation of the National Intelligence Program. The President appoints the DNI and the principal deputy director with the advice and consent of the Senate. The responsibilities of the Director of National Intelligence include—

- Leading the IC.
- Overseeing the coordination of foreign relationships between elements of the IC and the intelligence services of foreign governments.
- Establishing requirements and priorities for collection, analysis, production, and dissemination of national intelligence.
- Coordinating reform of security clearance and acquisition processes.
- Ensuring IC financial statements are auditable.
- Supporting legislative, legal, and administrative requirements.
- Ensuring compliance with statutory and Presidentially-mandated responsibilities.
- Transforming the IC into a unified, collaborative, and coordinated enterprise.

Director of National Intelligence Organization. The DNI organization is composed of the DNI staff and IC mission and support activities. The DNI staff is responsible for developing IC policy and overseeing its implementation. It is also responsible for preparing the National Intelligence Program budget. The mission and support activities are responsible for providing IC-wide substantive intelligence, counterintelligence strategy and strategic analysis, research and development, and training and education. The Director of Intelligence (DIRINT) staff is responsible for synchronizing and integrating efforts across Office of the Director of National Intelligence.

National Geospatial-Intelligence Agency

The NGA has specific authorities, produces various products, provides various services, manages the GEOINT workforce, and provides deployable support teams.

National Geospatial-Intelligence Agency Authorities. By law, the NGA is a combat support agency (CSA) as well as a national intelligence organization. As functional manager of GEOINT, the NGA is directly subordinate to the Secretary of Defense and the Under Secretary of Defense for Intelligence. The NGA is the primary source for GEOINT analysis and products at the national level. In addition to the GEOINT support identified in Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations*, the NGA supports national and homeland security, defense policy and force structure, and advanced weapons and systems development.

National Geospatial-Intelligence Agency Products. The NGA disseminates data and standard products. It also makes them available in repositories where GEOINT-trained personnel throughout the IC, including military personnel in the field, can access the data to develop their own GEOINT analysis and nonstandard products.

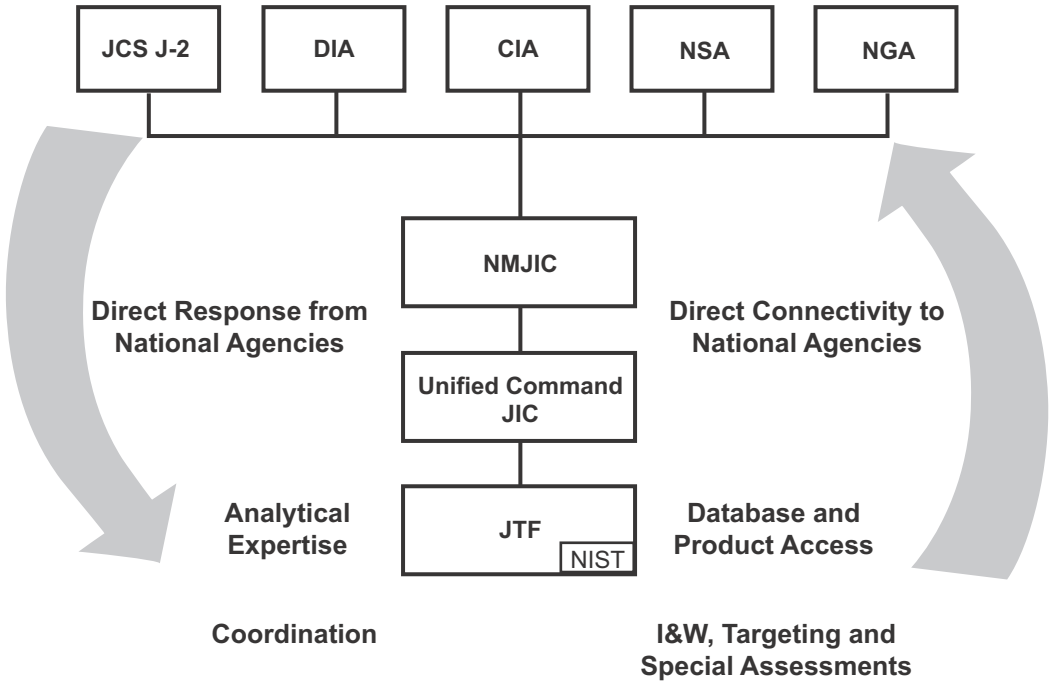
National Geospatial-Intelligence Agency Services. The NGA works with commercial imagery and geospatial data vendors to procure diverse unclassified imagery and geospatial information to support its customers, collaborative efforts with allies and coalition partners, other IC agencies, Department of Defense (DOD) organizations, and other civil and government entities.

National Geospatial-Intelligence Agency Workforce. The NGA provides GEOINT strategic workforce planning and specific training for general and specialized tradecraft skills through the National Geospatial-Intelligence College.

National Geospatial-Intelligence Agency Deployable Support. The NGA deploys a National Geospatial-Intelligence Agency support team (NST) in direct support of the Services, other IC organizations, and the JIOC at each combatant command (CCMD).

National Intelligence Support Team

National intelligence support teams are task-organized, national-level, all-source intelligence teams—generally consisting of DIA, National Security Agency (NSA), Central Intelligence Agency (CIA), and NGA personnel and equipment. They provide deployed commanders (generally at the JTF headquarters level) with coordination with national intelligence agencies, analytical expertise, I&W, special assessments, targeting support, streamlined and rapid access to national intelligence databases and other products, and assistance facilitating request for intelligence (RFI) management (see fig. 2-4).



LEGEND

JCS	Joint Chiefs of Staff
JIC	joint information center
NMJIC	National Military Joint Intelligence Center

Figure 2-4. National Intelligence Support Team Capabilities.

National Intelligence Support Teams Command and Control. National intelligence support teams are managed by the DIA's defense joint IOC. The DIA, through the joint staff J-2, controls each NIST for deployment and administrative purposes. See figure 2-5 for an overview of a NIST's deployment cycle.

During operations, a NIST will typically be in direct support of the joint force commander (JFC). The NIST falls under the staff cognizance of the JTF J-2, performing intelligence support functions as tasked. The basic NIST CONOPS is to take the JTF J-2's RFIs and collection and production requirements and discuss and deconflict these within the NIST to determine which element(s) should fulfill these requirements.

Each NIST element leader will maintain contact with their parent national intelligence organization and coordinate their actions with the NIST team chief. Intelligence generated by the NIST is available to the JTF J-2 JISE, the JFC, and other elements of the JTF with the usual caveats (i.e., restriction based on clearance and programs).

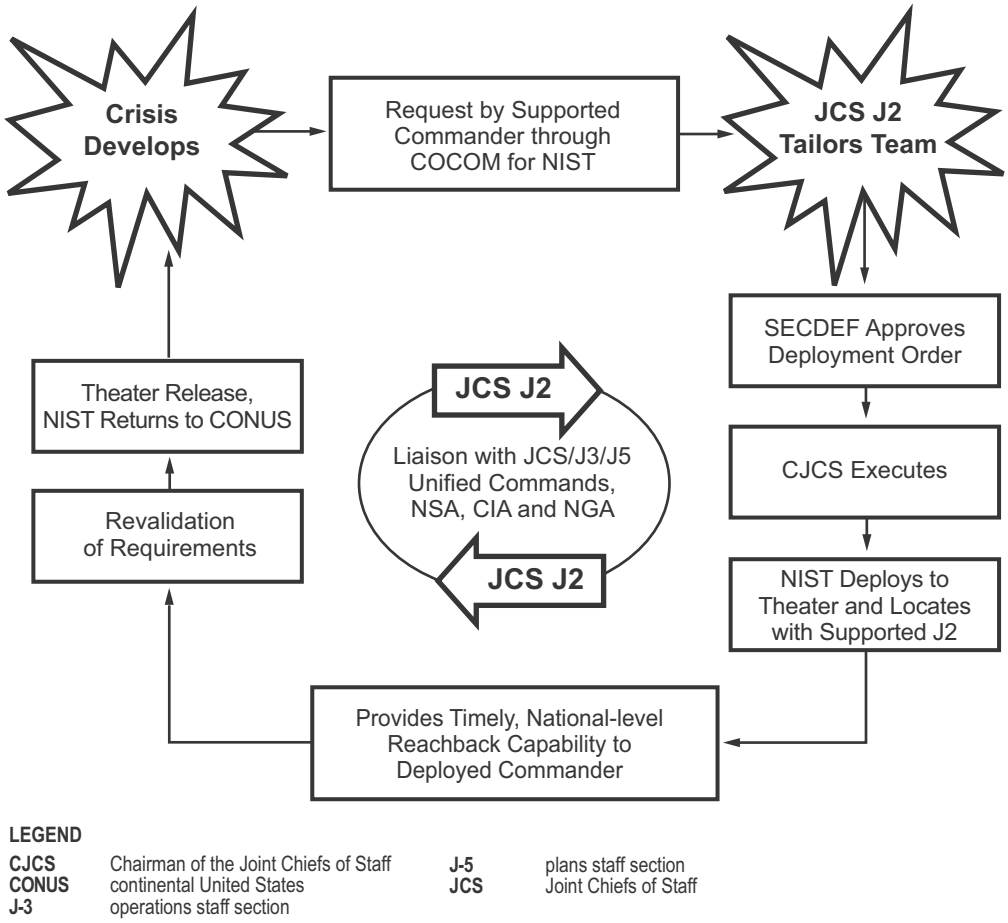


Figure 2-5. National Intelligence Support Team Deployment Cycle.

National Intelligence Support Teams Composition and Capabilities. The composition and capabilities of each deployed NIST are dictated by the mission, duration of the deployment, agencies represented, and capabilities required (see table 2-1). A NIST is not a self-contained element; it requires logistic and other support from the supported command (e.g., information systems technical support and an access-controlled secure area generally within the supported unit's tactical sensitive compartmented information facility).

Table 2-1. Notional Composition of a National Intelligence Support Team.

CIA	CIA
2 analysts 2 communicators Associated communications and information systems workstations	2 analysts 2 communicators Associated communications and information systems workstations
NSA	**NSA**
5–12 personnel (analysts, technicians, and communicators) Associated communications and information systems workstations	1 imagery analyst 1 geospatial analyst Associated communications and information systems workstations
Each NIST is task-organized to fulfill the supported commander's intelligence requirements.	

A NIST's organic capabilities generally encompass only intelligence and some unique CIS support. A NIST's CIS capabilities are task-organized and a NIST may range from a single agency element's voice connectivity to a fully-equipped NIST with JISE and Joint Worldwide Intelligence Communications System (JWICS) mobile integrated communications system video teleconferencing capabilities. For an example of the NIST's deployed footprint with the JWICS Mobile Integrated Communications System, see figure 2-6. Current methods of operation rely on both agency and supported command-provided communications pathways to support the deployed NIST element.

Figure 2-6. National Intelligence Support Team Joint Worldwide Intelligence Communications System Mobile Integrated Communications.

National Reconnaissance Office

The NRO designs, builds, and operates the nation's reconnaissance satellites. These satellites comprise one of the primary collection sources for GEOINT data and provide significant imagery to support DOD requirements related to targeting and mapping. These data are used for I&W, monitoring of arms control agreements, and the planning and execution of military operations. Once GEOINT data is collected, processed, and stored, the NGA takes the lead with respect to analysis and access/distribution for both national and DOD customers.

Defense Intelligence Agency

The DIA is both a national and defense-level intelligence agency. It is also designated as a CSA. The DIA is subordinate to the Secretary of Defense and the Under Secretary of Defense for Intelligence. The DIA has various programs that it manages and has certain responsibilities and management roles within the IC.

Defense Intelligence Agency Programs. The Director, DIA is the program manager of the General Defense Intelligence Program, which provides funding for the DIA and the intelligence organizations of each military department. The Director, DIA also manages a DIA program in the Military Intelligence Program, which includes select DIA programs and the intelligence resources of the eleven CCMDs. The Military Intelligence Program manages more than 500 military imagery analysts in support of the CCMDs.

Defense Intelligence Agency Responsibilities. The Director, DIA is responsible for coordinating collection requirements between national-level organizations and theater users for national and airborne imagery.

Defense Intelligence Agency Functional Management. The Director, DIA is the functional manager for the non-GEOINT-related components of measurement and signature intelligence (MASINT).

MARINE CORPS SUPPORTING ESTABLISHMENT IMAGERY INTELLIGENCE ORGANIZATIONS

The supporting establishment imagery intelligence organizations in the Marine Corps are Headquarters, Deputy Commandant for Capabilities Development and Integration; Systems Command; MCIA; and NSTs.

Headquarters, United States Marine Corps

Within Headquarters, United States Marine Corps (HQMC) there are two organizations that focus on imagery intelligence, Headquarters, Marine Corps-Imagery & Geospatial Intelligence Branch (HQMC-IPI) and HQMC, Department of Aviation.

Imagery/Geospatial Plans and Policies Branch, Intelligence Department. The HQMC-IPI serves as the principal Marine Corps representative for the DIRINT within the national and joint GEOINT communities. The HQMC-IPI personnel are responsible for developing and coordinating Marine

Corps imagery and geospatial programs. Specific HQMC-IPI personnel responsibilities include the following:

External to the Marine Corps

- Representing the DIRINT in meetings with the national agencies and other Services regarding policies affecting the planning and direction, collection, processing and production, dissemination, and utilization of GEOINT.
- Coordinating and validating Marine Corps Service-level imagery special collections and standing requirements for submission to the NGA source directorate.
- Ensuring Marine Corps imagery and geospatial intelligence architectures are interoperable with primary and alternate national imagery dissemination paths.
- Conducting liaison with the NGA and the CIA Office of General Counsel regarding matters related to IMINT oversight and domestic coverage.
- Responding to the Freedom of Information Act Office for requests to the Marine Corps for imagery materials, products, and derivative textual information/analytical methodologies.

Internal to the Marine Corps

- Identifying and coordinating issues related to intra-Service imagery and geospatial intelligence to ensure that organic resources available to the Marine Corps are exploited fully.
- Establishing policy guidance for disseminating national-level imagery to the operating forces afloat or ashore.
- Coordinating with the Deputy Commandant for Combat Development and Integration, Capabilities Development Directorate, Marine Corps Systems Command (MARCORSYSCOM) and other HQMC staff elements on imagery and geospatial intelligence issues related to—
  - GEOINT requirements and capabilities.
  - Dissemination architectures.
  - The Marine Corps Concept Based Requirements System process for GEOINT.
- Sponsoring the annual Marine Corps GEOINT conference.

Headquarters, Marine Corps, Department of Aviation. The Deputy Commandant for Aviation coordinates with Navy aviation elements to procure manned and unmanned tactical aviation platforms and sensors.

Deputy Commandant for Combat Development and Integration

The Deputy Commandant for Combat Development and Integration develops fully integrated warfighting capabilities—including doctrine, organization, training, materiel, leadership and education, personnel, and facilities—to enable the Marine Corps to field combat-ready forces.

Marine Corps Systems Command

Marine Corps Systems Command serves as the Commandant's principal agent for equipping the operating forces so they can accomplish their warfighting mission. Marine Corps Systems Command plans and manages research, development, and acquisition programs through equipment production and fielding for employment by MAGTF forces, including most equipment programs that support GEOINT.

Marine Corps Intelligence Activity

The MCIA is the Marine Corps' Service intelligence production center. In addition, the MCIA supports other Services and government organizations as appropriate. It provides the Marine Corps with intelligence for planning, training, operations, systems development, and exercises. The MCIA can be tasked to provide expeditionary warfare intelligence to support any national, theater, or operational command in the US Armed Forces. The MCIA's analysis and production supports not only the Marine Corps, but also national decisionmakers, theater commanders, and tactical warfighters.

National Geospatial-Intelligence Agency Support Teams

The NGA provides support teams to the Marine Corps with a specific mission, organization, and responsibilities.

National Geospatial-Intelligence Agency Support Team Mission. The NST representatives train and work with the MEF, MSCs, and other intelligence personnel to integrate IMINT and GI&S and future National System for Geospatial Intelligence (NSG) capabilities into MEF operations. The NSTs also evaluate the use of IMINT and GI&S and NSG concepts and products supporting the MAGTF mission.

National Geospatial-Intelligence Agency Support Team Organization. The NSTs are collocated with supported Marine Corp units and are an extension of both the NST-Marine Corps and the NGA staff officer. The NSTs provide direct access to the NGA geospatial libraries and support interoperability between the Marine Corps and the NGA. The NSTs execute all tasks in coordination with guidance provided by NST-Marine Corps, the NGA staff officer, and the MEF GEOINT chief.

National Geospatial-Intelligence Agency Support Team Responsibilities. The responsibilities of the NST include the following:

- Serving as the focal point for NGA GEOINT activity within each MEF and assisting each MEF with identifying IMINT and GI&S requirements.
- Installing and maintaining NGA application software and new NGA prototype systems and products as they become available and familiarizing imagery personnel with the software applications.
- Training IIP and MEF intelligence personnel to use NGA data and applications for planning and integration into organizational systems.
- Developing, maintaining, and presenting demonstrations of current and projected GEOINT capabilities.
- Evaluating GEOINT software and data, reporting findings to NST-Marine Corps, the NGA staff officer, HQMC-IPI, MEFs, intelligence battalions, and topographic platoons.
- Coordinating actions affecting MAGTFs with NST-Marine Corps, the NGA staff officer, HQMC-IPI, MEFs, intelligence battalions, and IIPs.
- Providing technical support for NGA products used in MAGTF systems.
- Assisting with developing tactics, techniques, and procedures (TTP) to support the rapid generation of new data and/or intensification of existing data sets.

- Assisting with technical reviews of developmental data sets, products, systems, and associated documents to ensure standard NGA data are used and new GEOINT product requirements are promptly identified.
- Assisting the imagery analysts with the technical use of NGA and NSG products.
- Assisting with the integration of the NGA's NSG concept into existing MAGTF architectures and migration plans.

CHAPTER 3
MAGTF IMAGERY INTELLIGENCE UNITS AND ORGANIZATIONS

This chapter describes the missions, tasks, organization, and CONOPS for Marine Corps units responsible for conducting tactical IMINT.

IMAGERY INTELLIGENCE PLATOON INTELLIGENCE BATTALION

The IIP is responsible for certain missions and tasks; it is organized to provide IMINT to supported units and has a specified command and control relationship and a concept of employment.

Mission and Tasks

The mission of the IIP is to provide IMINT support to MAGTFs and other commands, as directed. Specific IIP tasks include—

- Exploiting and analyzing all-source, multisensor imagery to derive intelligence pertaining to installations, troop dispositions, strengths, and activities of various conventional and nonconventional forces.
- Planning for and tasking multisensor platforms, including both those that are organic to and those that are external to the MAGTF.
- Conducting imagery exploitation and data management.
- Providing imagery derived products and reports to the MEF commander and other commanders.
- Conducting liaison with the Service-level intelligence center and external agencies for obtaining imagery products in support of MEF intelligence requirements.

Organization

An IIP is organic to each MEF and is subordinate to the P&A company of the intelligence battalion. Each IIP has a platoon headquarters, two tactical imagery analysis sections, and three imagery analysis teams (see fig. 3-1 on page 3-2).

In 2006, the 4th Imagery Interpretation Unit was incorporated into Company B, Intelligence Support Battalion of United States Marine Corps Forces Reserve (MARFORRES) and redesignated as an IIP. The 4th IIP is organized into one headquarters section, two tactical imagery analysis sections, and three imagery analysis teams. Reserve imagery analysts are also assigned to the AFP geospatial production detachment. During regular Reserve drills, the imagery analysts of

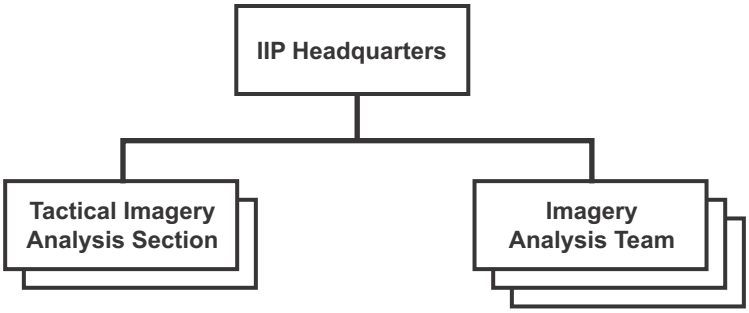


Figure 3-1. Imagery Intelligence Platoon Structure.

the IIP and geospatial intelligence directorate participate in federated imagery production in support of the MCIA. They also frequently perform active duty operational support to the operating forces and the national intelligence community. Reserve imagery analysts may also be mobilized as units, in teams, or as individual augments in support of operations and exercises.

Command and Control

The intelligence battalion commander is in charge of command and control of the IIP, while the MEF staff has cognizance over their activities. The platoon also has other support relationships with various units.

Intelligence Battalion Commander. The IIP is a subordinate unit of the intelligence battalion and the intelligence battalion commander retains full command of its operations. When supporting smaller MAGTFs, the IIP (or its detachments) will operate under the command and control of either the intelligence detachment OIC or the supported unit's G-2/S-2.

Marine Expeditionary Force Staff Cognizance. The MEF commander exercises command and control over all intelligence battalion elements, including the IIP, via the MEF AC/S G-2 systems officer. The systems officer directs the integration of IIP operations with other MEF IMINT operations.

Support Relationships. The IIP operates in general support of the MEF. Under this command relationship, the MEF commander, in consultation with both the AC/S G-2 and the ISC, determines priorities for intelligence collections and production support, locations of IMINT support nodes, and the means for IMINT and all-source intelligence dissemination.

The IIP, or task-organized imagery analysis detachments, may be employed in direct support of, or attached to, a particular MSC or unit of the MEF, based upon mission, enemy, terrain and weather, troops and support available-time available (METT-T) considerations. In these cases the scope of the supported commander's C2 authority over assigned IIP elements will be specified to ensure effective support to operations while allowing the MEF commander to maintain effective command and control of broader intelligence and IMINT operations. Direct support or attachment relationships may consist of dedicated imagery exploitation support, placement of IIP assets with the supported unit, or simply establishing an IMINT node at the supported unit to provide direct dissemination of imagery and IMINT to the intelligence section or COC. In the latter of these relationships, an IIP liaison element should be provided to the supported unit. Generally,

continuing relationships between IMINT elements and supported units should be established whenever possible.

Concept of Employment

An IIP supports each MEF. Task-organized imagery analysis detachments may be attached to MAGTF command elements, either independently or as part of a larger intelligence battalion detachment, when supporting a Marine expeditionary brigade, Marine expeditionary unit (MEU), or other special purpose MAGTF, as the mission requires.

The Reserve IIP conducts peacetime training and production activities in garrison at Buckley Air National Guard Base, Aurora, Colorado. The IIP and geospatial intelligence directorate of the AFP participate in federated imagery production in support of MARFORRES units, the MCIA, or the CCMDs during regularly scheduled reserve drill periods. The Reserve IIP also provides services and task-organized detachments of intelligence personnel to augment active component elements, joint commands, and national agencies in peacetime, times of crisis, contingency, or war.

The Marine imagery analysis specialists' primary imagery exploitation system is the tactical exploitation group (TEG) (see fig. 3-2 on page 3-4). The modular and scalable TEG employs commercial off-the-shelf, government off-the-shelf, and nondevelopmental item computer hardware and software to enable rapid upgrades and maintain commonality and interoperability with other Marine Corps and joint intelligence and imagery systems. The TEG provides the MAGTF commander with an organic capability to produce IMINT products in support of all operations. The TEG provides the capability to data-link imagery from theater and tactical assets as well as resourcing repositories via classified networks to support tailored imagery analysis. The TEG also disseminates imagery products and imagery exploitation reports to the MAGTF commander and subordinate commanders in support of tactical operations, strike planning, detection and location of targets of opportunity, and combat damage assessment for restrike planning and intelligence assessment. Anticipated upgrades will enable the processing of imagery from additional manned and unmanned platforms, improve video capture and exploitation capabilities, enhance net-centric functionality, and increase modularity. The TEG has two echelon-tailored configurations: virtual imagery processing-Marine Corps (VIP-MC) and tactical exploitation group-remote workstation (TEG-RWS).

The VIP-MC is the IMINT ground station for the MEF. Each IIP in the operating force has one VIP-MC; there is no VIP-MC dedicated to MARFORRES. The TEG-RWS is the deployable IMINT workstation for deploying units of the MEF. Imagery analysts of intelligence support battalion, MARFORRES maintain a limited deployable TEG-RWS capability.

Miscellaneous

Other miscellaneous items relating to IIP's operations are communications and information systems and the maintenance concept for their equipment.

Communications and Information Systems. The IIP requires a significant amount of communication resources to support internal and detachment C2 requirements. Additionally, the IIP needs access to various classified networks to conduct its operations.

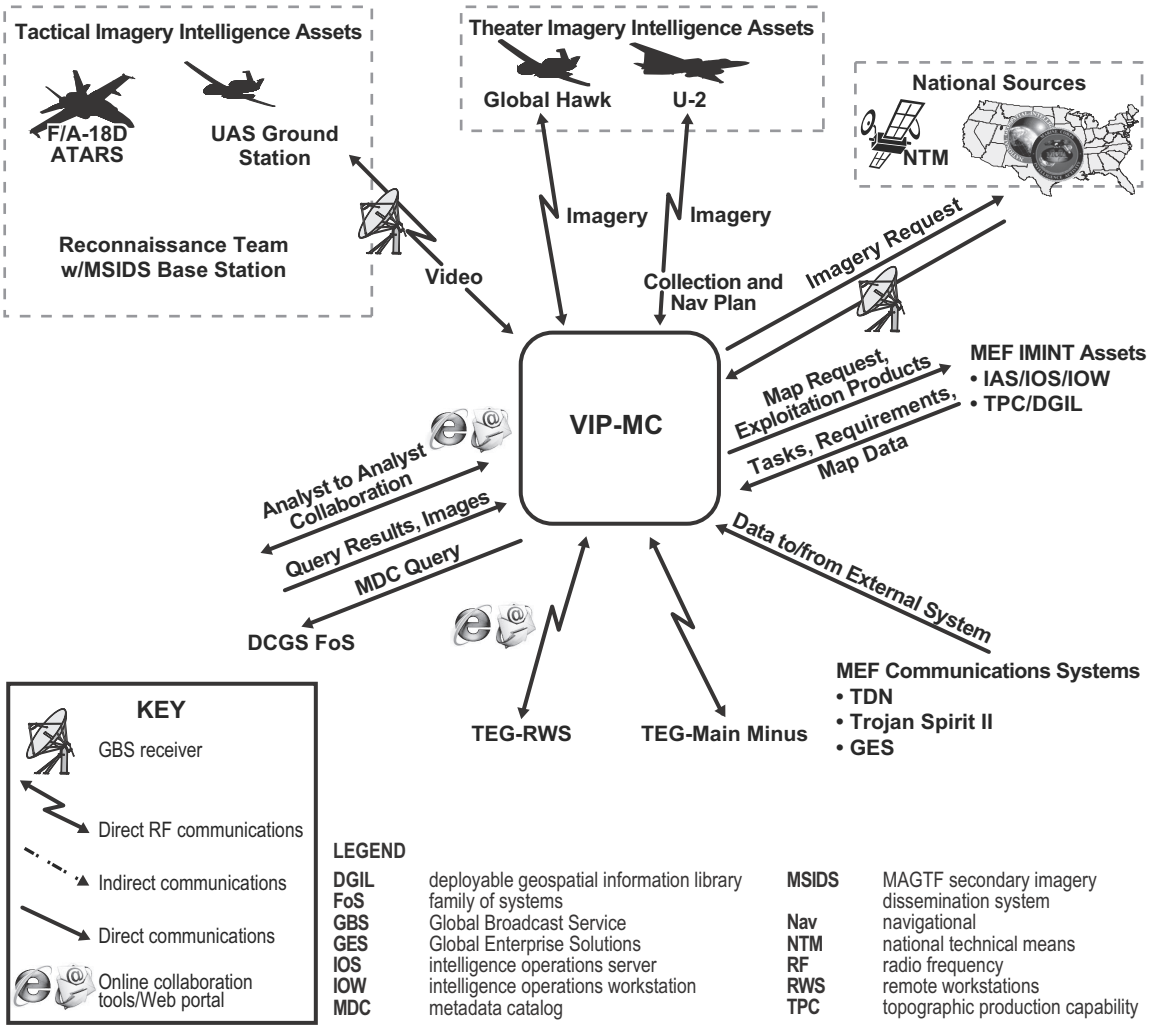


Figure 3-2. Virtual Imagery Processing-Marine Corps.

Maintenance Concept. The chosen product support strategy is to use contractor logistics support (CLS) supply chain management and field support representatives (FSRs) and to use the lead systems integrator (LSI) to track warranties, establish maintenance contracts, and provide software support solutions as well as to perform technology refreshes.

The TEG family of systems (FoS) is supported by the two-level maintenance concept (field and depot) per Marine Corps Order (MCO) 4790.25, *Ground Equipment Maintenance Program*. Tactical exploitation group FoS field level maintenance is performed using standard Marine Corps operating procedures and organic personnel. The Marine-performed maintenance is supported by program manager office-shared FSRs that are currently supporting the fielded TEG-RWS via a LSI contract. Equipment requiring depot level maintenance is evacuated to CLS personnel. Depot level software maintenance is performed by the LSIs. Depot level hardware maintenance is performed by the original equipment manufacturer.

With respect to unit-level maintenance, each intelligence battalion is responsible for organizational-level preventive maintenance on the TEG FoS and all associated organic Marine Corps equipment based on the unit's table of organization.

The MARCORSYSCOM TEG program office is responsible for the budgeting and funding of the CLS contract for the entire life cycle of the TEG FoS. The TEG FoS is supported by the two-level maintenance concept (field and depot) per MCO 4790.25, *Ground Equipment Maintenance Program.*

Regarding transportation, the intelligence battalion has limited organic rolling stock to support IIP operations. External transportation support from the Marine expeditionary force headquarters groups, the MLG/supported unit is needed to move all parts of the IIP simultaneously.

TACTICAL ANALYSIS AND COMBAT TRACKING EXPLOITATION TEAM, INTELLIGENCE BATTALION

The tactical analysis and combat tracking exploitation (TACTEX) team is responsible for certain missions and tasks. It is organized to provide the moving target indicator (MTI) capability to supported units, has a specified C2 relationship, and has its own concept of employment. The duties of the TACTEX team may be performed by an imagery analysis specialist (military occupational specialty [MOS] 0241) or by an intelligence analyst (MOS 0231). An MTI is a graphical representation of moving objects on the Earth's surface. These objects are detected by radar through Doppler shift. The radar detects moving vehicles, surface vessels, rotating antennas, slow-moving aircraft, and smaller targets (such as personnel).

Mission and Tasks

The TACTEX team provides the MEF with near real time (NRT) and forensic access in order to receive, process, exploit, and analyze multiple levels of MTI, fixed target indicator (FTI), SAR imagery, high range resolution data, UAS video data, and SIGINT/communications intelligence data via the integrated broadcast service from any MTI collection platforms. Specific TACTEX tasks, performed by MOS(s) 0241 and 0231 include—

- Receiving, processing, manipulating, storing, and displaying NRT MTI, FTI, and SAR data from MTI sensors simultaneously.
- Disseminating MTI data and textual analysis to the MEF AC/S G-2, other elements of the MEF, and other forces, as directed.
- Assisting with the planning and directing of MTI collection operations in support of the MEF.
- Retrieval of historical MTI data from local databases or mission archive services to conduct forensics analysis. An MTI forensics analysis involves analyzing MTI data within specified parameters (time, location, size, speed) that is correlated with other intelligence data to add context and meaning, and produce actionable intelligence.
- Providing the capability to communicate, via voice and/or digital link, with a variety of the MTI platforms, including but not limited to the E-8 Joint Surveillance Target Attack Radar System (JSTARS), the P3 Orion Littoral Surveillance Radar System (LSRS), the Sentinel's Airborne Standoff Radar, the Sea King Mk7 Airborne Surveillance and Control helicopter, and the vehicle dismount and exploitation radar (VADER) platform.

Organization

A TACTEX team is organic to each MEF and is currently located at the corresponding intelligence battalion. Cell structures within the battalions vary. For example, the 1st Intelligence Battalion maintains its cell under collections and the 2d Intelligence Battalion maintains its cell under the IIP. Regardless of the cell structures, however, teams will be moved to the battlefield surveillance company when they are formed, in accordance with the MCISR-E roadmap.

Each MEF has one JSTARS antenna suite (JAS) (comprised of a transit cased surveillance control data link [SCDL] ground data terminal [GDT] and SATCOM suite) and tactical exploitation group–remote workstations (TEG-RWS) variant integrated with the VANTAGE™ Ascent Software (VAS) and MOVINT Client (MC) exploitation software. Together the JAS and TEG-RWS, form the Moving Target Indicator Operation Suite (MTI OS). The MTI OS will be used to source all MAGTF MTI analysis requirements.

Command and Control

The TACTEX team operates in general support of the MEF. The intelligence battalion commander, as the ISC, retains full control of TACTEX team activities. The MEF commander exercises command and control over intelligence battalion elements via the MAGTF intelligence officer, including the TACTEX MTI OS, which is a scalable, expeditionary/rapid-deployment capability.

Concept of Employment

The majority of MTI platforms are national assets that support either a JTF joint force land component commander or a ground component commander under the overall direction of the JFC.

Once the TACTEX team receives data at the MTI OS from the MTI collection platform, the MTI analyst develops a report and/or MTI product that can be disseminated throughout the MEF according to the intelligence reporting criteria directed by the MAGTF intelligence officer. Under routine conditions, these data are disseminated to the P&A cell for follow-on analysis and fusion with other intelligence data to produce all-source intelligence products.

The METT-T factors may require that E-8C data be provided to other elements of the MEF and subject data be disseminated to subordinate units via the MEF tactical data network (TDN). The MTI/FTI/SAR image, with its associated data, will be viewed by recipients (potentially down to and including the regimental/group level) using common Marine Corps hardware and software suites.

Equipment. The TACTEX team's equipment is discussed in the following subparagraphs.

Moving Target Indicator Operation Suite (MTI OS). The MTI OS consists of the JAS and any TEG-RWS variant. The JAS contains a transit cased SCDL GDT, SCDL Masthead and supplementary gear, and the SATCOM Suite, comprised of a PSC-5D SATCOM radio, ancillary gear and antennas. The JAS provides a direct data link to the JSTARS E-8C for receipt of near-real-time (NRT) MTI data, fixed target indicators (FTI) and SAR imagery.

When connected to the SIPRNET, the MTI OS can access MTI from other MTI collection platform ground stations and online MTI databases such as mission archive services and

real-time dissemination and online transmission services. The mission archive services is a Web-accessible environment that provides a data enterprise to store, retrieve, and share archived MTI data and related information. Real-time dissemination and online transmission services' primary function is to provide dissemination of current MTI data.

Each TEG-RWS variant has the VAS and MC exploitation software. The VAS has a JSTARS interface, where the MTI operator can configure the SCDL and SATCOM suite hardware, and submit radar service requests and exchange free text messages. The MC is used to exploit the MTI and fuse the MTI data with other intelligence products.

Intelligence, Surveillance, and Reconnaissance Forensic Analysis System. The ISR Forensic Analysis Systems are Windows-based operating systems capable of providing NRT support to the MTI effort by means of SECRET Internet Protocol Router Network (SIPRNET)-data streaming. These systems are also optimal for providing detailed forensic analysis of historical data. Though not limited strictly to these functions, forensic analysis missions generally focus on studies of the following types: line of communications (LOC), traffic pattern analysis, counter-improvised explosive device backtrackings, high-value individual and high-value target, pattern of life, border crossing, littoral and maritime, cache site, traffic density, and density plot and analysis. Intelligence, surveillance, and reconnaissance forensic analysis systems are not organic program of record assets to a TACTEX team and, as a result, must be maintained as additional/ supplemental CIS resources provided internally by the MEF communication battalions.

Miscellaneous

Miscellaneous issues that affect TACTEX units are communications and information systems, maintenance, and transportation issues.

Communications and Information Systems. The MTI OS has no organic communication resources, but when communications and information systems (CIS) resources are made available the MTI operator can support internal command and control, operations, and intelligence requirements, as well as external communications with MTI platforms and ground stations. Typically, the MTI OS will require access to the SIPRNET and pertinent local area networks (LANs) and wide-area networks (WANs). The TACTEX team members can operate all organic CIS equipment; however, all CIS resources must be provided by the MEF communications battalion.

Maintenance. As part of the TEG FoS, the MTI OS is supported by the two-level maintenance concept (field and depot) per MCO 4790.25, *Ground Equipment Maintenance Program*. The TEG FoS field level maintenance is performed using standard Marine Corps operating procedures and organic personnel. The Marine-performed maintenance is supported by program manager office-shared FSRs that are currently supporting the fielded TEG-RWS via an LSI contract. Equipment requiring depot level maintenance is evacuated to CLS personnel. Depot level software maintenance is performed by the LSIs. Depot level hardware maintenance is performed by the original equipment manufacturer.

Transportation. The TACTEX team has sufficient resources to displace all MTI OS equipment. Additional sup-port will be needed from the MEF headquarters group or the MLG to displace common ground station and joint Services workstation personnel simultaneously.

MARINE UNMANNED AERIAL VEHICLE SQUADRON

The VMU is responsible for certain missions and tasks. It is organized to support the MEF, has a specified command and control relationship, and a concept of employment.

Mission and Tasks

The mission of the VMU is to operate and maintain UASs that support the MEF/other supported units. Specific VMU tasks include the following:

- Conducting aerial reconnaissance (including imagery collection and reporting), surveillance (including airborne surveillance of designated target areas, MEF or other areas of interest, and other areas, as directed), and target acquisition.
- Conducting airborne surveillance for search and rescue and tactical recovery of aircraft and personnel.
- Conducting reconnaissance of helicopter approach and retirement lanes in supporting vertical assaults.
- Providing real-time target information to the direct air support center (DASC) and fire support coordination center(s) (FSCCs) to facilitate adjusting fire missions and close air support.
- Providing real-time intelligence reporting to the SARC to support MEF intelligence requirements and to facilitate all-source intelligence operations.
- Providing information to assist adjusting indirect-fire weapons and to support and facilitate direct air support and air interdiction operations.
- Providing remote receive capability and liaison to designated units.
- Collecting information to support BDA and combat assessment.
- Supporting rear area security.

Organization

The VMU has an external and an internal organization.

External Organization. The VMU is organic to the MAW and is structured to operate as a subordinate unit of one of the Marine air control groups (MACGs).

Internal Organization. Each of the three active component VMUs can be organized into 12 self-contained detachments: three RQ-7B SHADOW UAS suites and nine RQ-21A BLACKJACK UAS suites. Each detachment can operate and maintain one UAS suite. The RQ-7B SHADOW UAS suite is comprised of four air vehicles, two ground control stations, one launcher, and associated recovery gear. The RQ-21A BLACKJACK UAS suite is comprised of five air vehicles, two ground control stations, one launcher, and one recover device.

Command and Control

The VMU is under the command of the MAW commanding general or the aviation combat element (ACE) MAGTF commander (when deployed in support of MAGTFs smaller than a MEF). The supported commander exercises command and control via the ACE G-3/S-3 and the Marine air command and control system (MACCS) (see Marine Corps Warfighting

Publication [MCWP] 3-25, *Control of Aircraft and Missiles*). Air operations (e.g., flight tasking, airspace deconfliction) are planned, coordinated, and controlled by the ACE G-3/S-3 via the Marine tactical air command center (TACC). However, intelligence missions are tasked per the intelligence and reconnaissance mission requirements designated by the MEF or supported unit commander; this action requires close coordination between the intelligence battalion IOC and the MAW Marine TACC.

Normally, a VMU operates in general support of a MEF. The MEF commander, through the AC/S G-2, determines VMU intelligence priorities and information and intelligence dissemination flow when the VMU is operating in the general support role. The AC/S G-2 will exercise staff cognizance of VMU intelligence operations via the ISC.

Marine unmanned aerial vehicle squadron missions may be flown in direct support of particular MEF units or MSCs (e.g., the Marine division or its main effort). In these cases, the scope of the supported commander's C2 authority over VMU missions should be specified to ensure effective support to the operations while allowing the MAGTF commander to maintain effective command and control of broader intelligence and IMINT operations. Direct support missions may require that dedicated command and control, planning, and exploitation be provided to the supported unit via a VMU detachment.

Concept of Employment

A VMU can support any size MAGTF; however, normal employment would be as an integral unit of the MAGTF's ACE. The VMU can also conduct limited independent operations.

The VMU's intelligence section consists of 2 officers, 10 intelligence specialists (MOS 0231), and 38 imagery analysis specialists (MOS 0241). The intelligence section is responsible for planning collections, collecting IMINT, producing and disseminating imagery reports, imagery products, and all-source intelligence analysis.

The VMU can conduct limited imagery exploitation/analysis. Generally, UAS imagery is screened by VMU imagery analysts for information of immediate tactical value per the intelligence collection and reporting criteria stipulated by the ISC or the supported unit's intelligence officer. In most cases, the information and imagery products are sent directly to the supported unit. Imagery is also disseminated by VMU to the IIP for further detailed imagery analysis and all-source intelligence production. The MAGTF intelligence officer is responsible for subsequent IMINT dissemination, including secondary imagery dissemination.

Miscellaneous

The miscellaneous issues that affect the VMU are communications and information systems, maintenance, and equipment.

Communications and Information Systems. Each VMU has sufficient CIS resources, which include those associated with the MACCS, to support internal and squadron command and control, operations, and intelligence requirements. The VMU normally needs access to Nonsecure Internet Protocol Router Network (NIPRNET), SIPRNET, and pertinent LANs and WANs.

Maintenance. Each VMU can perform organizational maintenance on its aviation equipment. The squadron can also perform first echelon maintenance on assigned ground equipment, including motor transport, engineering, and communications equipment. The MLG or supporting combat logistics battalion performs third and fourth echelon maintenance on ground equipment.

Equipment. See appendix G for VMU equipment and performance characteristics.

MARINE FIGHTER/ATTACK (ALL-WEATHER) SQUADRON

Mission and Tasks

The mission of the VMFA(AW) is to attack and destroy surface targets, day or night, under adverse weather conditions; conduct multisensor imagery reconnaissance; provide supporting arms coordination; and intercept and destroy enemy aircraft under all weather conditions. Specific VMFA(AW) tasks include the following:

- Conducting airborne surveillance for search and rescue and the tactical recovery of aircraft and personnel.
- Conducting day and night close air support under all weather conditions.
- Conducting day and night deep air support under adverse weather conditions (e.g., armed reconnaissance, radar search and attack, air interdiction, and strikes against enemy installations) using all weapons that are compatible with the aircraft.
- Conducting multisensor imagery reconnaissance (e.g., pre-strike and post-strike target damage assessment and visual reconnaissance).
- Conducting day and night supporting arms coordination (e.g., forward air control, tactical air coordination, and artillery/naval gunfire spotting).
- Intercepting and destroying enemy aircraft in conjunction with ground and airborne fighter direction.
- Conducting battlespace and target illumination.
- Conducting armed escorts of friendly aircraft.
- Conducting the suppression of enemy air defense operations.

Organization

There are five F/A-18D VMFA(AW)s in the operating forces. Each squadron has 12 aircraft; only three to four aircraft are configured with the advanced tactical airborne reconnaissance system (ATARS) at any one time. The VMFA(AW) normally functions as a unit: it is structured to operate as a subordinate unit of a Marine aircraft group in support of the MAGTF. Key squadron intelligence personnel include the S-2, two all-source intelligence analysts, and four imagery analysts.

Command and Control

Each VMFA(AW) falls under the command of its parent group commander. Overall, depending on the configuration of the MAGTF, operational control rests with the MAW or ACE commander. The commander exercises command and control via the ACE G-3/S-3 and the MACCS (see MCWP 3-25 for more information). Air operations (e.g., flight tasking, airspace deconfliction) are planned, coordinated, and controlled by the G-3/S-3 via the Marine TACC. However, intelligence missions are conducted according to the mission requirements designated by the MAGTF or supported unit commander and require close coordination among the intelligence battalion IOC, the Marine TACC, and supported commanders.

Marine fighter/attack (all weather) squadrons typically operate in support of the MAGTF as assigned in the ATO. However, their VMFA(AW) missions may be in direct support of a particular unit of the MAGTF (i.e., ground component, the ACE, or logistics combat element [LCE]) based on METT-T considerations. The ATO will identify these missions, pertinent command and control, and intelligence operations direction.

Concept of Employment

The VMFA(AW)'s concept of employment should be considered in terms of operations and intelligence. When viewed in operational terms, the VMFA(AW) is normally employed as a unit of an ACE in support of MAGTF operations. With respect to intelligence, the VMFA(AW), when equipped with ATARS and tasked to conduct imagery collection missions, coordinates operations closely with the IOC, the MAW AC/S G-2, the IIP, and others as appropriate.

The processing of ATARS imagery is completed on the VMFA(AW), utilizing the TEG-RWS. Each VMFA(AW) is equipped with a TEG-RWS and has the capability to exploit and produce imagery as well as IMINT products and reports in support of requirements. The ATARS imagery is screened by VMFA(AW) imagery analysts for information of immediate tactical value according to intelligence collection and reporting criteria. Exploited imagery from the VMFA(AW) may be hosted on a designated imagery server. Each VMFA(AW) can conduct limited imagery exploitation or analysis. Each VMFA(AW) is interoperable with the VIP-MC, providing NRT downlinking of selected images; the remaining imagery data will be processed with the TEG-RWS. It may also be disseminated to the IIP for additional imagery exploitation support. Figure 3-3, on page 3-12, provides an overview of VMFA(AW) ATARS imagery processing flow.

Miscellaneous

Each VMFA(AW) has sufficient CIS resources to support internal and squadron command and control, operations, and intelligence requirements. The VMFA(AW) needs access to various networks to conduct its operations, including NIPRNET and SIPRNET as well as other pertinent LANs and WANs.

The VMFA(AW) can conduct first echelon maintenance on all assigned equipment. It can also perform organizational maintenance on assigned aircraft and support equipment. Maintenance requirements that exceed these capabilities are provided by other ACEs and LCEs.

Each VMFA(AW) can fulfill its own particular administrative requirements.

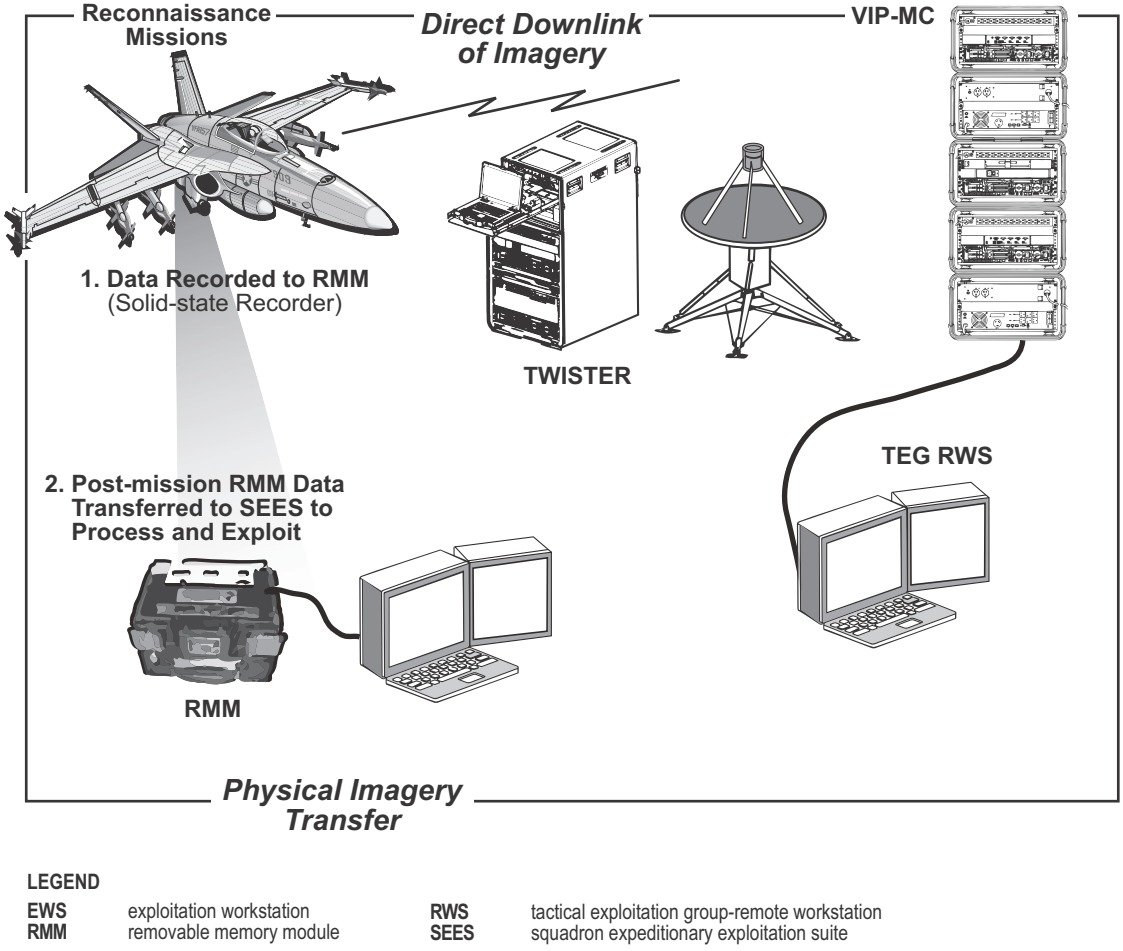


Figure 3-3. An F/A-18 Advanced Tactical Airborne Reconnaissance System Tactical Reconnaissance Imagery Processing Flow.

GROUND RECONNAISSANCE

Mission

The force reconnaissance company and the division reconnaissance battalion provide amphibious, deep ground, and ground reconnaissance; surveillance; battlespace shaping; and limited-scale raids in support of the Marine division, its subordinate elements, the MEF, other MAGTFs, or a joint force. The IMINT capability fielded to these units is the MAGTF secondary imagery dissemination system (SIDS).

Organization

There are three Active Component and one Reserve Component reconnaissance battalions. A standard reconnaissance platoon within a battalion consists of a headquarters section and three six-man reconnaissance teams.

Command and Control

The force reconnaissance company and the division reconnaissance battalion are under the operational control of the supported unit's commander. For intelligence and reconnaissance missions, the commander exercises command and control over ground reconnaissance via the unit's intelligence officer. At the MEF level, the AC/S G-2 exercises this staff cognizance via the ISC. This structure allows for the centralized direction and effective integration of ground reconnaissance operations with the broader all-source intelligence CONOPS.

Ground reconnaissance units normally operate in a general support relationship to supported units. Depending upon tactical considerations, ground reconnaissance units may be employed in direct support of, or attached to, particular subordinate units (e.g., force reconnaissance teams attached to advance force elements for an expeditionary operation; division reconnaissance battalion's platoons; or teams attached to, or in direct support of, the division's main effort). To ensure effective support to the operations while allowing the MEF or division commander to maintain effective command and control of broader intelligence and reconnaissance operations, the scope of the supported commander's C2 authority over designated ground reconnaissance teams is usually specified.

Concept of Employment

The force reconnaissance company normally operates under the staff cognizance of the MAGTF G-2/S-2 for reconnaissance and surveillance missions and under the staff cognizance of the MAGTF G-3/S-3 for offensive missions. The basic operating unit is the team; however, platoons or task-organized elements may be employed to accomplish certain tasks.

Force reconnaissance operations should have a defined scope and duration, with planned exfiltration. Teams are usually inserted into the supported commander's area of interest (AOI) (usually the deep area), often well beyond the supporting arms and reserve elements of the enemy's committed forces, in order to collect and report information in response to the commander's PIRs.

When required by the situation, the company or detachments may be placed in direct support of, or attached to, smaller MAGTFs or to MEF elements other than the command element. Normally, a force reconnaissance detachment is attached to a MEU.

Because force reconnaissance company units routinely operate beyond the range of the MAGTF's supporting arms, the company must maintain the capability to clandestinely insert and extract units over extended distances. Such means include foot movement, surface or subsurface swimming, vehicles, rotary- or fixed-wing aircraft, small boats, landing craft, and commercial assets. All teams are capable of using closed-circuit underwater breathing apparatuses, open-circuit SCUBAs [self-contained underwater breathing apparatuses], and submarine lock-outs. Also, all teams are capable of static-line and military free-fall parachuting.

Deployed teams use standard techniques of small-unit scouting and individual movement. Unless the mission requires otherwise, force reconnaissance teams will avoid contact with the enemy or indigenous people. Teams either observe from vantage points or physically reconnoiter the AOIs. As directed, teams report by radio and/or during post mission debriefings. When conducting offensive operations, force reconnaissance company elements employ the previously described

techniques to reach their objective sites. Conducting actions at the objective area, they employ close-quarter battle, standard tactical assault, or sniper techniques to neutralize or destroy enemy targets and/or to recover designated personnel or materiel.

Teams assigned to initial terminal guidance missions reconnoiter the landing area and provide last-minute visual or electronic terminal guidance to flight, wave, or stick leaders. Initial terminal guidance missions terminate with the arrival of the helicopter support team, US Navy beach party, landing craft air cushion LZ control teams, US Army Pathfinder teams, or US Air Force combat control teams, which then assume traffic-control functions.

CHAPTER 4
IMAGERY INTELLIGENCE SYSTEMS, C2 NODES, CIS, AND OTHER SYSTEMS

This chapter addresses the major MAGTF IMINT C2 and CIS nodes from a systems perspective and describes the impacts of processing, exploitation, and dissemination on these nodes.

BASIC IMAGERY INTELLIGENCE COMMUNICATIONS AND INFORMATION SYSTEMS REQUIREMENTS

Managing Subordinate Imagery Intelligence Units

Intelligence officers and IMINT element OICs must maintain positive command and control of subordinate units and integrate their operations with broader MAGTF and external intelligence and operational command and control. Traditionally, single-channel radio and recorded message traffic has been used to support command and control of MAGTF IMINT elements. In semi-static situations, secure e-mail or telephone may be the method of choice for communicating; whereas, in highly fluid or mobile scenarios, cellular telephones, SATCOM, and radio may be used.

Receiving Data and Information From Organic/External Imagery Intelligence Organizations

Communication and information systems architecture must provide connectivity between organic and supporting IMINT elements, IMINT production and analysis centers, and supported MAGTF operations and intelligence centers. Requirements include the ability to transmit images and related data files and IMINT reports digitally via fiber optics, wire/radio in both voice and data formats that are readily usable by imagery and all-source intelligence analysts.

Providing Intelligence to Supported Commanders

Imagery intelligence CIS requirements are influenced by the supported commanders' intent, CONOPS and intelligence, command relationships, and standing PIRs and intelligence requirements. Communication and information systems architecture must be capable of integrating IMINT element command and control and supporting CIS operations with the primary CIS channels used by the supported commanders.

Providing Imagery Intelligence Products and Reports to National Intelligence Centers, Theater, Joint Task Force, MAGTF, and Other Components

Imagery intelligence products are provided to designated organizations via the MAGTF's organic secured/nonsecured communications networks.

IMAGERY INTELLIGENCE AND RELATED COMMAND AND CONTROL NODES

The national nodes for imagery intelligence, NST, and NRO were discussed in chapter 2.

Within a theater, there are different levels of nodes, such as the combatant commander JIOC, the JTF J-2, and the JISE.

Combatant Commander Joint Intelligence Operation Center

The combatant commander, JIOC is responsible for fulfilling the intelligence requirements of both the combatant commander and his subordinate commanders. By providing finished intelligence products supporting theater mission planning and execution, the JIOCs are the primary sources from which subordinate JTFs receive intelligence support for their AOI.

Collection. Combatant commander J-2s retain full collection management authority over all ICRs against targets within their area of responsibility. This authority may be delegated to a subordinate JFC. Validated collection requirements that cannot be satisfied by organic means, including imagery collection, are submitted to the CCMD JIOC.

Processing and Exploitation. Each JIOC processes and exploits imagery in its particular theater. Downlinked imagery data signals may be transmitted to workstations for immediate exploitation/archiving.

Production.Combatant command and Service Intelligence Center production responsibilities are clearly delineated within the Department of Defense Intelligence Production Program (DODIPP). The DODIPP is structured to capitalize on the analytical and production resources of the entire DOD intelligence production community. The community on-line intelligence system for end-users and managers automates DODIPP procedures for stating and tracking theater intelligence requirements and other intelligence production requirements. Results from imagery exploitation and the annotated images may be incorporated into all-source intelligence products, standalone IMINT products, or into various GEOINT databases.

Dissemination. Dissemination of digital products is done via the DCGS-MC and the primary dissemination medium for intelligence is SIPRNET. Along with e-mail distribution, the JIOC utilizes Web sites and portals as hubs to collaborate and post finished intelligence products.

Joint Task Force J-2 and the Joint Intelligence Support Element

The JTF J-2 organizational structure and capabilities are driven by the mission. Intelligence CIS, based on functionality, enables the JTF to query theater and national IMINT servers and databases for current intelligence.

The JISE is the principal intelligence C2 node within the JTF J-2 and is the focus for JTF intelligence operations, providing the JFC and component commander with situational awareness and other intelligence support regarding adversary air, ground, maritime, and space capabilities and activities. A NIST, supporting the JTF headquarters, integrates its operations within the JISE. Key JISE functions and capabilities include collection management support, OOB analysis,

identification of threat critical capabilities (i.e., critical requirements), critical vulnerabilities, and intelligence support to targeting and force protection.

All IMINT collection, production, and dissemination activities are conducted within the JISE. Once IMINT products and support have been provided to the JTF and its components, updates are delivered by the JISE using multiple dissemination techniques.

Collection. The JTF J-2 collection manager plans, coordinates, and employs direct imagery collection operations to support the JTF. The MAGTF interfaces with the collection assets, as is depicted in figure 3-2, on page 3-4. Communication support planning provides connectivity from these major nodes into the TEG and MAGTF TDN.

Production. Imagery intelligence production requirements are managed by the JISE per the JFC's PIRs and validated intelligence requirements.

Dissemination. Once basic and current intelligence and imagery have been provided to a deploying JTF and its components, updates will be accomplished using multiple dissemination techniques. Intelligence CIS, based on the applicable networks, provides the JTF with the ability to query theater and national IMINT servers and databases for current intelligence.

Amphibious Task Forces. While afloat, landing forces use the amphibious task force (ATF) imagery architecture to access/transfer GEOINT data. Once ashore, the landing force communications responsibilities transfer to its organic G-6/S-6 for communications.

Intelligence Center. During amphibious operations, the intelligence sections of the ATF and the landing force normally integrate their operations. The principal intelligence C2 node afloat is the intelligence center located aboard the ATF flagship. The intelligence center has installed CIS systems that support the intelligence operations of the ATF and landing force while reducing duplicative functions and producing more comprehensive and timely intelligence for the naval task force. Standard CIS connectivity is available.

Marine Expeditionary Force Command Element

Combat Intelligence Center. The combat intelligence center (CIC) is the principal MAGTF intelligence C2 node providing the facilities and infrastructure for the centralized direction of the MEF's comprehensive intelligence, counterintelligence, and reconnaissance operations. The CIC is the primary IOC established within the MEF main command post. It encompasses the primary functions of the MEF intelligence section and intelligence battalion. The CIC includes the subordinate elements listed in table 4-1 on page 4-4.

Table 4-1. Marine Expeditionary Force Command Element Combat Intelligence Center.

Element	Responsibilities
G-2 Plans	Serves as the G-2 section's main element for coordinating and providing intelligence support to the MEF command element future plans team and leadership of the G-2 sections GEOINT, SIGINT, and METOC sections.
G-2 Operations	Serves as the G-2 section's main element for coordinating and providing intelligence support to the MEF commanding general, battle staff, and current operations center elements; target intelligence support to the force fires and future operations; G-2 section intelligence requirements management activities; red cell support; and MEF intelligence liaison with external commands and organizations.
IOC	Serves as the principal MEF intelligence operations and C2 center established by the intelligence battalion; performs intelligence requirements management, staff cognizance of ongoing organic and supporting collection operations, intelligence production and analysis, and intelligence dissemination.
Support Cell	Serves as the primary element for conducting MEF-wide intelligence requirements management, weather support, collections and dissemination planning and direction, and intelligence staff cognizance of MEF organic and supporting intelligence and reconnaissance operations.
P&A Cell	Serves as the primary production and analysis element of the MEF; processes and produces all-source intelligence products in response to requirements of the MEF; serves as the principal GEOINT production element of the MEF.
SARC	Serves as the primary element for the supervision of MEF collection operations; directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets.
Counterintelligence/ HUMINT Company	Serves as the primary element for conducting counterintelligence/HUMINT planning and direction, C2, and coordination of MEF counterintelligence/HUMINT operations with external counterintelligence/HUMINT organizations.
Operations Control and Analysis Center	Serves as the main node for the command and control of radio battalion SIGINT operations and the overall coordination of MEF SIGINT operations; processes, analyzes, produces, and disseminates SIGINT-derived information; and directs the ground based electronic warfare activities of the radio battalion.
Reconnaissance Operations Center	Serves as the main node for the command and control of a force reconnaissance company's operations and the overall coordination of MEF ground reconnaissance operations; processes, analyzes, produces, and disseminates ground reconnaissance-derived information in support of MEF intelligence requirements.

Intelligence Operations Center. The IOC is the other key MEF command element intelligence node. The subordinate elements within the IOC and their typical composition are the support cell, the SARC, and the P&A cell (see fig. 4-1 on page 4-5).

Overall Marine Expeditionary Force Intelligence C2 Relationships. The MEF G-2 section and intelligence battalion's overall C2 relationships, along with the resulting all-source intelligence support flow throughout the MEF are depicted in figure 4-2, on page 4-6.

Combat Intelligence Center/Intelligence Operations Center Operations and Imagery Intelligence. Imagery intelligence is an integral component of many CIC/IOC operations. Key activities include collection, production, and dissemination.

Collection. The CMD section, intelligence battalion, provides the core for MEF CIC collection operations. During operations, the CMD section is located within the IOC support cell.

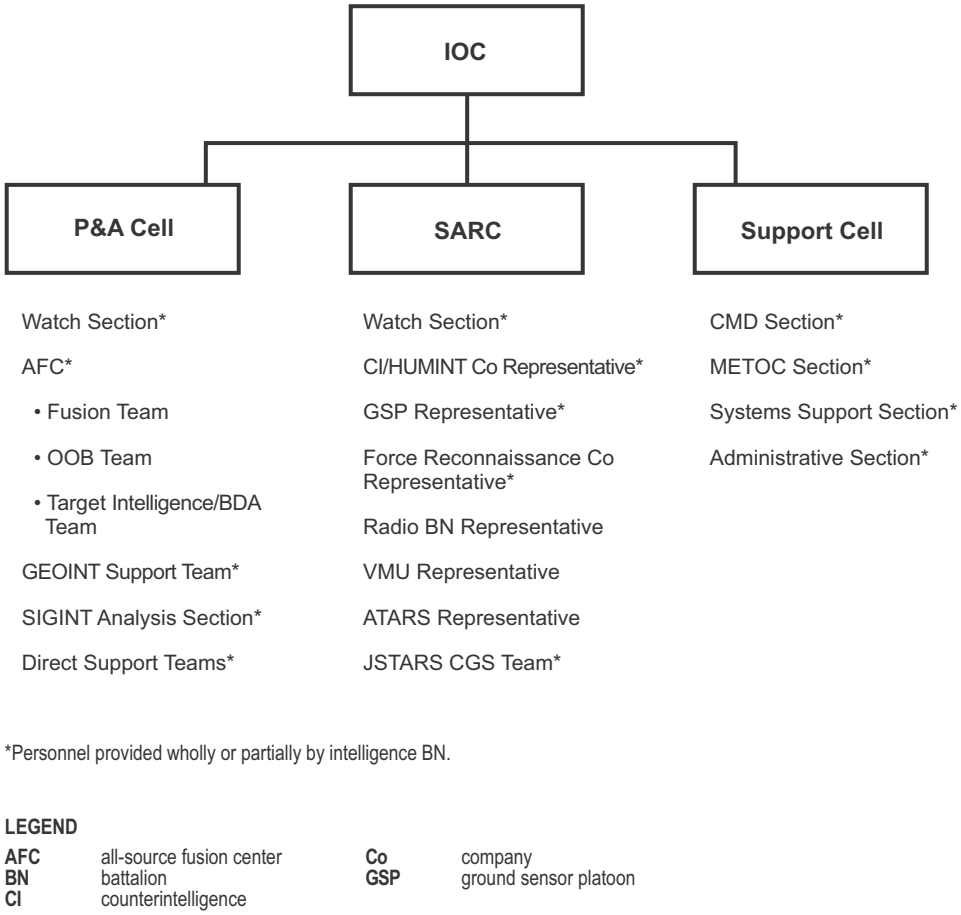


Figure 4-1. Intelligence Operations Center Elements and Composition.

Intelligence specialists from all disciplines are organic to this section. Key CIS resources required include an Intelligence Analysis System (IAS), with community on-line intelligence system for end-users and managers and other specialized applications, and access to the full range of communications (e.g., JWICS, SIPRNET, NIPRNET). The SARC provides the other component of collection operations. The SARC should have representation from most organic and supporting intelligence and reconnaissance units. Imagery intelligence representation should include a VMU element with supporting CIS resources that will monitor ongoing UAS operations and report time-sensitive intelligence.

Production. The P&A cell, intelligence battalion, provides the core for MEF intelligence production operations. Intelligence specialists from all intelligence disciplines are organic to the P&A cell. Key CIS resources required included IAS and the joint deployable intelligence support system, with access to the full range of communications (e.g., JWICS, SIPRNET, NIPRNET). Generally, the IIP and intelligence battalion will be integrated with P&A cell operations to support both IMINT and all-source production operations.

Dissemination. The CMD section, intelligence battalion, provides the core command and control for MEF intelligence dissemination operations. Key CIS resources include IAS and the joint deployable intelligence support system, with access to the full range of communications (e.g., JWICS, SIPRNET, NIPRNET) for external dissemination and IAS via the TDN and other MEF

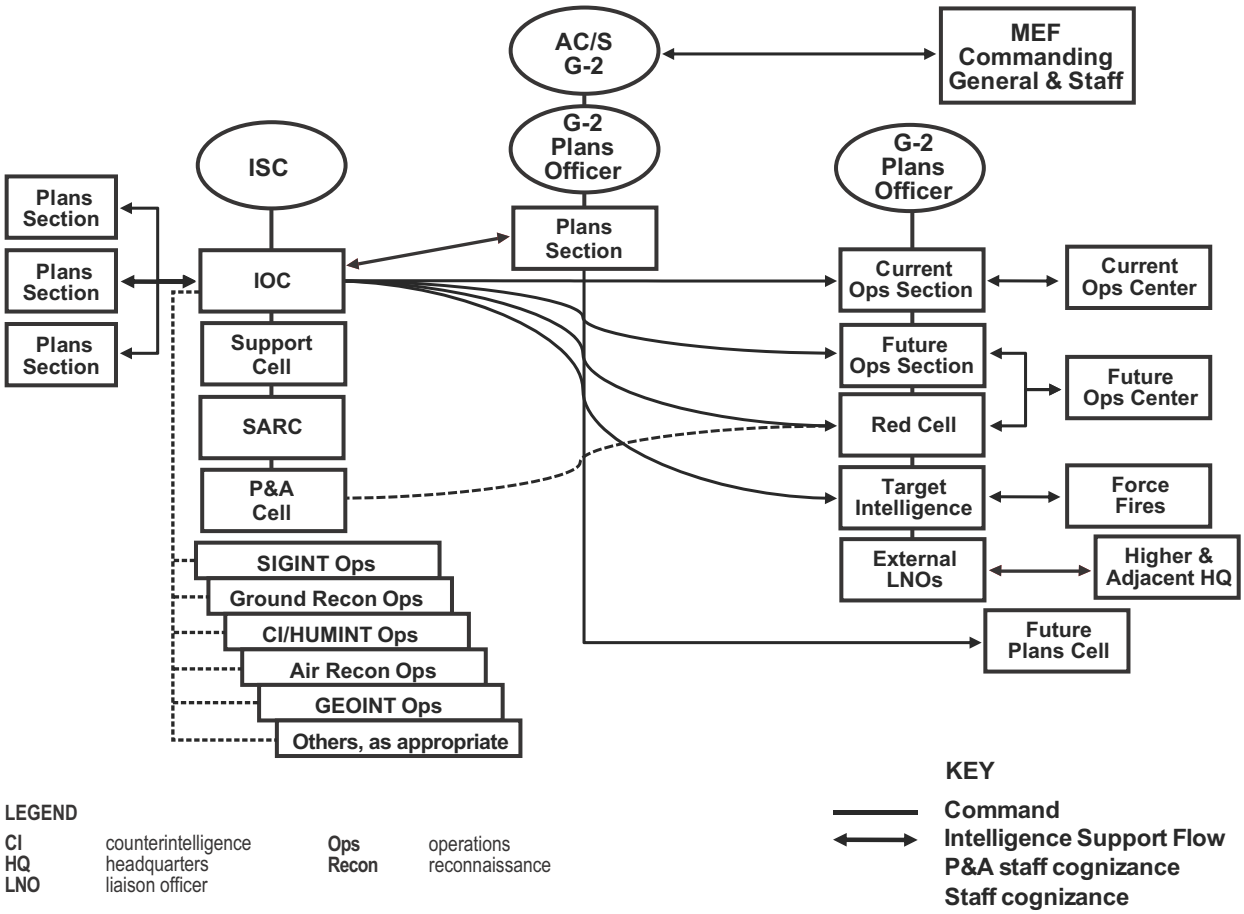


Figure 4-2. Marine Expeditionary Force C2 Relationships and Intelligence Support Flow.

communications resources for internal dissemination. The MEF command element should exploit all of the external capabilities to satisfy its intelligence requirements, with heavy reliance on the MCIA for national imagery support and the JIOC/joint analysis center for theater and national support.

National imagery and related products are received over dedicated terrestrial links that terminate at the MCIA's direct feed imagery product library; standard communications connectivity from the deployed MEF to the MCIA via the Defense Information Systems Network are normally provided by satellite communications. Currently, these links are super-high frequency (X-Band) military SATCOM using ground mobile forces terminals. In the future, more C-Band and Ku-Band commercial SATCOM, using mobile Tri-Band SATCOM terminals, will be employed. The limited capacity of these links to Defense Information Systems Network are a significant chokepoint for deployed MAGTFs. Efficient use of these links is critical to maintaining high traffic throughput.

In addition to the MAGTF TDN and other common-user communications capabilities, several imagery units have specialized capabilities to support IMINT dissemination. The VMU's remote receiving station, attached to MEF MSCs (i.e., the MEF main effort), provides direct, time-sensitive UAS support. Within the MEF, the IAS is the principal information system resource that supports secondary imagery and other IMINT product dissemination. The IAS should be available at all command echelons down to the maneuver battalion/squadron levels. Communications

connectivity between the MEF command element and its MSC headquarters are predominantly provided by SATCOM, supplemented where practical with terrestrial line-of-sight and tropospheric scatter (known as troposcatter) multichannel radio systems. Connectivity to the regiment/group level is principally via the TDN and various multichannel radio resources.

Finally, communications connectivity below the regiment/group command echelon depends on single-channel radio primarily designed for voice traffic, with limited range and limited data capacities. Although these units possess tactical data systems, their ability to exchange data is currently limited due to reduced bandwidth connectivity with the MAGTF TDN.

IMAGERY INTELLIGENCE INFORMATION SYSTEMS AND SUPPORTING COMMUNICATIONS

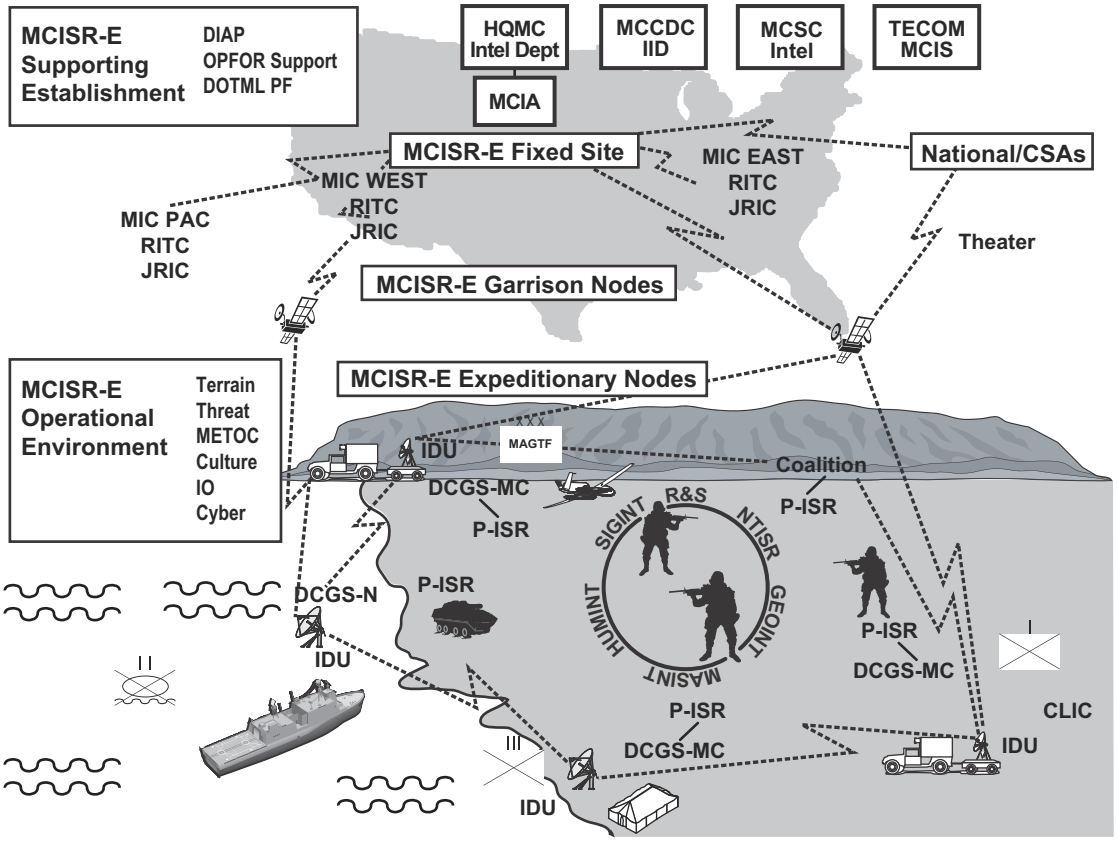
Imagery Direction and Collection Management

The GEOINT community uses a variety of systems to support and direct MAGTF IMINT operations. The DCGS-MC integrates surveillance and reconnaissance processing and exploitation capabilities into a single, integrated net-centric capability (see fig. 4-3, on page 4-8). Increment 1 of the DCGS-MC will integrate the TEG FoS and the topographic production capability into a common hardware/software baseline for GEOINT support.

The DCGS MC is interoperable with other distributed common ground/surface systems (DCGSs) including DCGS-Army, DCGS-Air Force, DCGS-Navy, DCGS-Special Operations Forces, and DCGS-intelligence community. The use of distributed common ground/surface system integration backbone (DIB) standards allows DCGS-MC interoperability with all other agencies that comply with those standards. These agencies include the NGA, NSA, NRO, DIA, and some allied and coalition forces, as well as the national intelligence architecture. The DCGS MC supports multidiscipline joint, national, multinational (coalition/allied) force commanders, JTF commanders, and below with critical multisource, multi-intelligence data and products to support JTF-level campaign planning and execution.

While embarked aboard amphibious shipping, MAGTF units use the DCGS MC in conjunction with DCGS-Navy assets for all ISR requirements. Once it is transitioned ashore, DCGS MC enterprise provides support to the naval forces through DCGS interoperability. The DCGS MC connects intelligence analysts to multidiscipline national, joint/multinational organic collection assets, data sources, and analytic assessments. It is the backbone of the MAGTF's ability to produce targeting information, correlate surveillance data and other intelligence, and rapidly disseminate information to MAGTF commanders in order to achieve decision superiority.

The DCGS-MC data feeds the COP. The DCGS-MC provides local data discovery and exposes designated MAGTF intelligence data, reports, and products to the DOD DCGS enterprise. The DCGS-MC can integrate sensor data from the broad range of current and planned Marine Corps tactical ISR and nontraditional ISR assets. It accommodates receipt of these data via MAGTF command and control, LANs, the Global Information Grid, and directly from intermediate systems, such as UASs via direct data link, ground control stations, or the removable memory media for ATARS imagery. The DCGS-MC has three nodes: fixed, garrison, and expeditionary.



LEGEND

CLIC	company level intelligence cell	MCSC	Marine Corps Systems Command
DIAP	Defense Intelligence Analysis Program	MIC	Multinational Interoperability Council
DOTMLPF	doctrine, orgranization, training, materiel, leadership and education, personnel, and facilities	N	Navy
		NTISR	non-traditional intelligence, surveillance, and reconnaissance
IDU	intelligence dissemination and utilization	OPFOR	opposing force
Intel	intelligence	PAC	Pacific
IO	intelligence oversight	P-ISR	persistent-intelligence, surveillance, and reconnaissance
JRIC	joint reserve intelligence center	R&S	reconnaissance and surveillance
MCCDC	Marine Corps Combat Development Command	RITC	Regional Intelligence Training Center
MCIS	Marine Corps imagery support	TECOM	Training and Education Command (MCCDC)

Figure 4-3. The Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise.

The MCISR-E fixed site node is hosted at the MCIA and supports information searching, archiving, and collaboration. The MCISR-E fixed site provides data repository services and metadata tagging services that enable a requester to access specific information, data, products, or services. The MCISR-E fixed site is the DCGS-MC exposure site for Marine Corps intelligence data and the Marine Corps metadata registry and catalog. Additionally, when bandwidth restrictions or the characteristics of combat prevent DIB exposure by a deployed MAGTF, the fixed site will serve as an entry point to MAGTF-produced information for national-level intelligence agencies and other external organizations, data, and products.

Garrison nodes, located at each MEF, provide the DCGS-MC with DIB-enabled functional capabilities (i.e., GEOINT, all-source analysis, SIGINT, MTI). They mirror the basic capabilities of expeditionary nodes and, where required, include increased capability (e.g., additional data storage). Garrison nodes can be deployed if necessary. Garrison nodes provide the MEF with the capacity to duplicate capabilities of deployed MAGTFs while serving broader remain behind MEF elements. Garrison nodes are also located at each MEF intelligence center, regional

intelligence training center, and joint reserve intelligence center. These centers provide reachback support to deployed forces, expose data to the larger DCGS enterprise, and provide a baseline intelligence capability for federated production with MCISR-E guidelines.

The expeditionary nodes are linked to the garrison and fixed site nodes. Expeditionary node equipment and capabilities can be scaled to support any size MAGTF. The primary role of the expeditionary nodes is to provide processing, exploitation, analysis, and production capabilities to deployed MAGTFs. When deployed with a MAGTF, expeditionary node capabilities will include the ability to maintain local, tactical intelligence data storage and expose MAGTF intelligence data within the MAGTF, as well as to multidiscipline joint, national, multinational partners. Due to frequent bandwidth restricted operations (i.e., aboard ship or during remote operations), the MAGTF commander retains control of the amount of information exposed directly to the larger DOD DCGS enterprise, MCISR-E garrison nodes, and the fixed site node.

Geospatial Intelligence Information Management Services

Geospatial intelligence information management services provide the MAGTF and other users with a comprehensive national and commercial imagery collection management capability. As the primary tool for imagery collection needs, geospatial intelligence information management services—

- Allow MEF collection managers to generate national and commercial imagery requests, search and order simple to complex GEOINT products, visualize data, and provide mission awareness.
- Enable collection managers to compute, display, and monitor enterprise metrics.
- Task and transmit to collection, exploitation, production, and dissemination organizations the geospatial intelligence needs, formally known as nominations, which, upon validation and prioritization, are automatically transferred to the appropriate review authority.

Imagery Collection

The Marine Corps relies on both organic and external collection assets for its imagery (see fig. 4-4 on page 4-10).

F/A-18D and Advanced Tactical Airborne Reconnaissance System. The ATARS suites are organic to the F/A-18D squadrons (see fig. 3-3 on page 3-12). These ATARS-equipped F/A-18D aircraft provide the MAGTF with an organic manned aerial imagery reconnaissance capability in support of IMINT operations. The ATARS suites are capable of infrared, EO, and radar imagery collection, and provide high-resolution day and night imagery support in all weather conditions through both overflight and long-range standoff.

The F/A-18D's long-range standoff capability is made possible by the upgraded, all-weather SAR system. Imagery is recorded and data-linked via the ATARS sensor suite. The tactical interoperable ground data link II common data link provides a limited NRT capability for disseminating data from selected critical targets—downlinked to the IIP's TEG—with subsequent removable memory media download for the exploitation of the complete track at the squadron. Figure 4-5, on page 4-11, depicts the F/A-18D systems architecture.

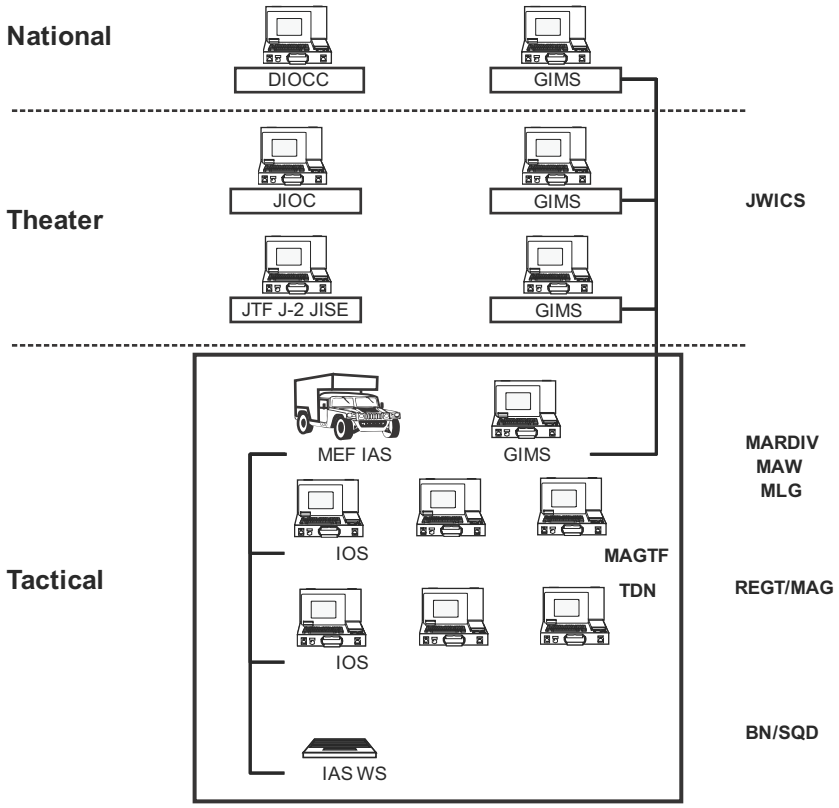


Figure 4-4. MAGTF Imagery Operations.

Unmanned Aircraft Systems. Full motion video feeds have been by far the most effective use of UAS. This live TV coverage of enemy actions or friendly events has contributed more to the commander's situational awareness than any other system in the commander's inventory. See appendix G for additional information regarding UAS equipment and performance characteristics. The following subparagraphs discuss UAS CIS resources.

Remote Video Terminals. Supported units can use/access FMV with a remote video terminal (RVT). The RVT is often the most practical means by which tactical users (e.g., platoon and company commanders, forward air controllers, and air officers) receive video and telemetry information.

The RVT is a ruggedized laptop computer with antenna and software that enable data processing and direct viewing of sensor imagery and telemetry information. Typically, the RVT has limited range (approximately 15 km from the UAS). Some RVTs have much larger directional antennas that can receive video from beyond 45 km. The RQ-7 Shadow is equipped with four one-system remote video transceivers. The one-system remote video transceivers can be used by supported units, such as a regimental COC, to receive video and telemetry from an RQ-7B and certain other types UASs from greater distances.

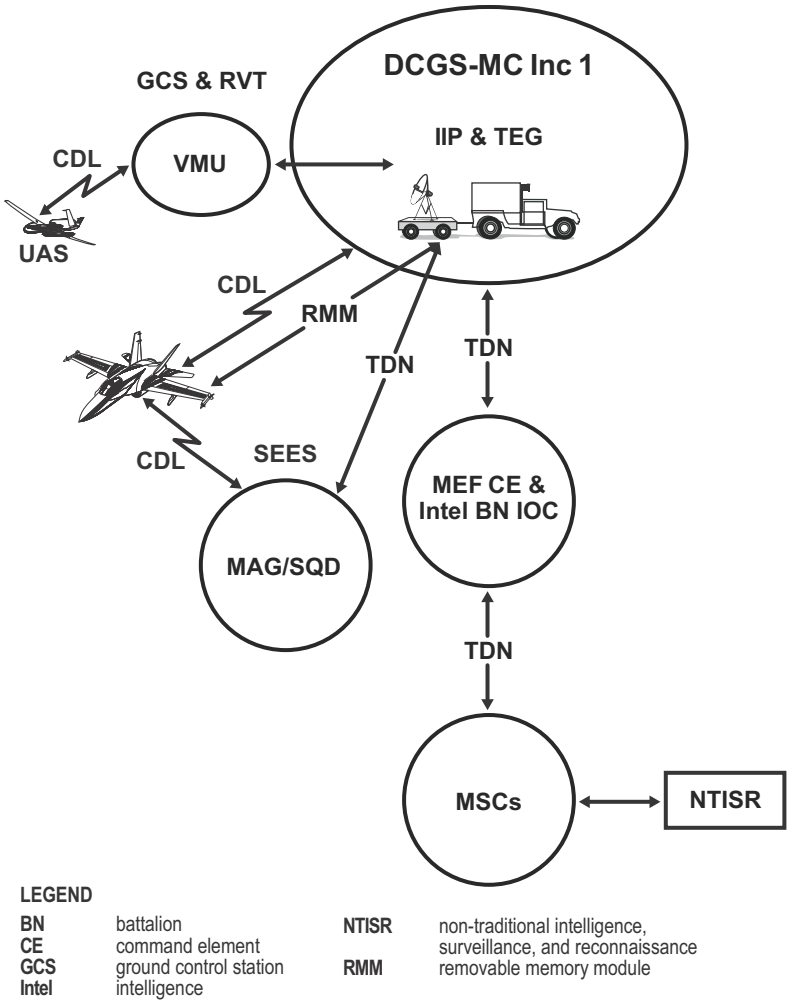


Figure 4-5. The F/A 18D Systems Architecture.

The primary RVT for the Marine Corps is the VideoScout system being fielded to tactical air control parties and battalion air officers. VideoScout can view video on analog or digital L, S, C, and Ku frequency bands.

Video and Data Distribution Networks. Video and data distribution networks provide a multilayer distribution capability that ensures multiple paths for UAS imagery and reduces latency for high priority users.

Supported units in the field can receive video and telemetry directly from the UAS using organic VideoScout or Remote Operations Video Enhanced Receiver III systems. Other units or headquarters equipped with a VideoScout and within range of the UAS can also receive the same video imagery.

For situations where a remote unit or agency desires video and telemetry data, communications architecture that can facilitate the transmission of large volumes of FMV/telemetry data need to be developed by the MAGTF G-6.

Marine UASs provide an interoperable data stream that is compliant with NATO STANAG [standardization agreements]. The data stream interfaces or plugs in to systems devised by the MAGTF G-6. The plug-in would be applied to a system integral to the unit operations center/COC. The unit operations center/COC would then provide the interface for the DCGS-MC. Consequently, all MAGTF units connected to the DCGS-MC should have access to the video/telemetry data provided by the UAS; however, the data should be at an increased level of imagery latency.

Moving Target Indicator Operation Suite. The MTI OS is organic to the MEF intelligence battalion. It provides the MAGTF command element with both communications connectivity with the Air Force's JSTARS E-8C and the capability to display, process, and disseminate acquired information. Figure 4-6 depicts the MAGTF JSTARS systems architecture and CONOPS. The following are capabilities of the MTI OS:

- The MTI OS receives and processes MTI, FTI, and SAR data from the JSTARS E-8C aircraft.
- The MTI OS receives UAS video data via the SIPRNET.
- The MTI OS receives processed SIGINT from the Integrated Broadcast Service.
- The MTI OS receives secondary imagery from theater and national sources.

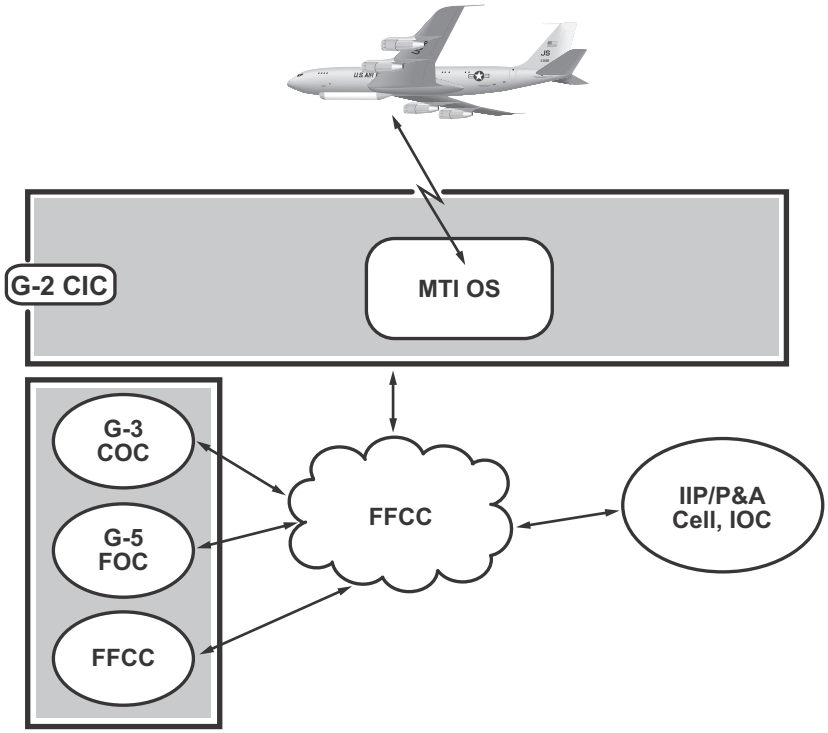


Figure 4-6. Joint Surveillance Target Attack Radar System Common Ground Station Systems Architecture.

- The encrypted, highly jam-resistant SCDL provides the digital communications connectivity between the E-8C JSTARS airborne element and the MAGTF command element G-2 section's MTI OS, enabling the transmission of MTI, SAR, and FTI data acquired by JSTARS to support MAGTF target acquisition, situation development, battlespace management, and targeting functions.
- The MTI OS features an open-system architecture that enables rapid insertion of the latest government and commercial off-the-shelf technology.

Collection Capabilities. The E-8C carries a phased-array radar antenna in a 26-foot canoe-shaped radome under the forward part of the fuselage. With a range in excess of 155 miles, this radar covers an estimated 386,100 square miles in a single 8-hour sortie. It is capable of providing targeting and battle management data to all MTI operators, both in the aircraft and on ground. These operators prepare intelligence reports and/or help coordinate aircraft, missiles, or artillery fire support.

Wide-Area Airborne Surveillance Sensor and Moving Target Indicator. The wide-area airborne surveillance sensor and the MTI are the primary operating modes for the radar. They detect, locate, and identify slow-moving targets. By focusing on smaller terrain areas, the radar image can be enhanced for increased resolution display. High resolution enables analysts to identify moving targets.

Synthetic Aperture Radar/Fixed Target Indicator. The SAR and FTI produce a photo-like image or map of a selected geographic region. A SAR data map contains precise locations of critical nonmoving targets, such as bridges, harbors, airports, buildings, or stopped vehicles. The FTI display is available while operating in the SAR mode to identify and locate fixed targets within the SAR area. The SAR and FTI capability, used in conjunction with MTI and MTI history display, allow for post-attack assessments made by onboard or ground operators following a weapon attack on hostile targets.

Ground Moving Target Indicator Forensics Tool. The MTI OS has a ground MTI forensics tool, which enables it to exploit MTI imagery analysis from points of interest or to compare movement over time. Such comparison enables the development of tracks and the conduct of meaningful historical intelligence analysis. The ground MTI forensics tool gives the MTI OS workstation operators and ground MTI analysis cells the ability to exploit historical MTI imagery from multiple sources.

MAGTF Man-Packed Secondary Imagery Dissemination System. The MAGTF SIDS (see fig. 4-7 on page 4-14) contains multiple configurations consisting of base stations, outstations, and video exploitation workstations depending on each unit's configuration and mission requirements (e.g., MEU structure requires six outstations, three base stations, and one video exploitation workstation). The mission of MAGTF SIDS is to enable the MAGTF to capture, manipulate, annotate, and transmit imagery products in NRT both internally with subordinate commands that are widely separated throughout the AO and externally with higher and adjacent commands (see fig. 4-8 on page 4-15). The MAGTF SIDS is employed according to the doctrine TTP prescribed in doctrinal publications associated with Marine Corps operations. The MAGTF SIDS may be employed in many different scenarios worldwide in which a MAGTF is expected to operate including shipboard, garrison, or tactical environments. The MAGTF SIDS is capable of supporting all phases of operational maneuver from the sea, sustained operations ashore, and other expeditionary operations.

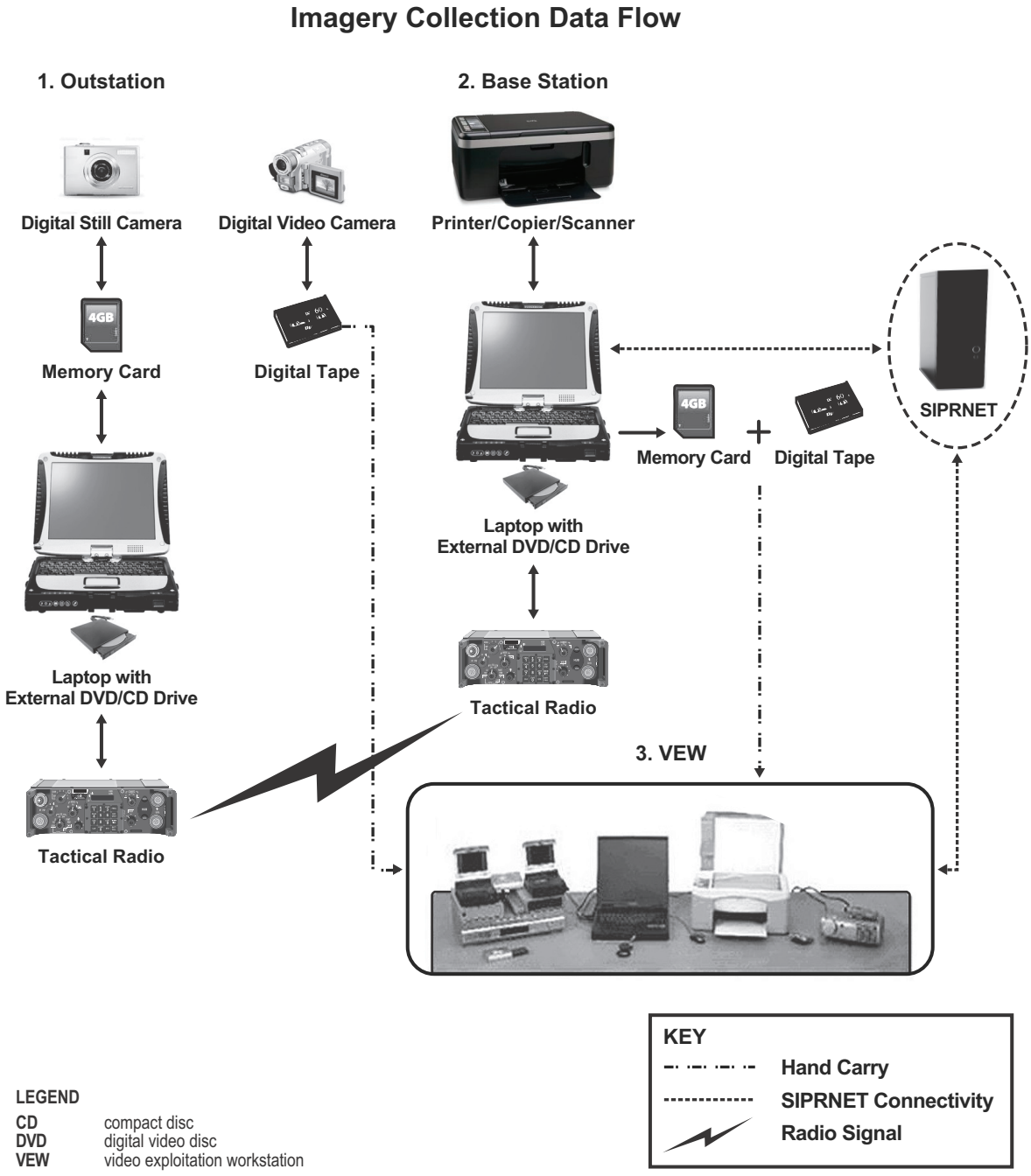


Figure 4-7. MAGTF Secondary Imagery Dissemination System Diagram.

MAGTF Secondary Imagery Dissemination System Base Station. The MAGTF SIDS base station suite is the receiver terminal for the MAGTF SIDS outstation. The MAGTF SIDS base station also provides dissemination and connectivity between the MAGTF and external sources (e.g., theater, national, other Services) via SIPRNET or other organic electronic communications channels that are external to and separate from MAGTF SIDS.

MAGTF Secondary Imagery Dissemination System Outstation. The MAGTF SIDS outstation suite is used to collect and transmit tactical imagery to the MAGTF SIDS base station. The MAGTF SIDS

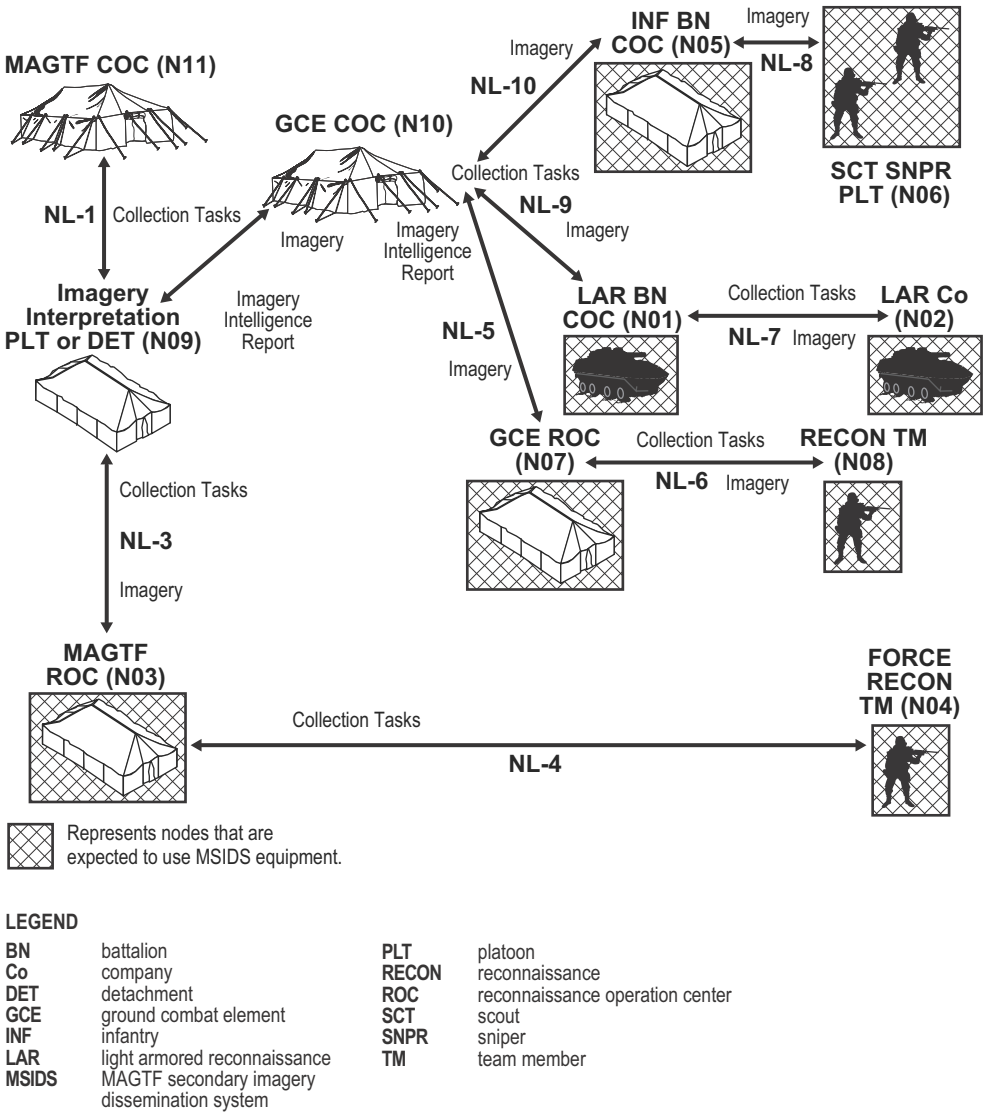


Figure 4-8. MAGTF Secondary Imagery Dissemination System Network Architecture.

outstation also provides dissemination and connectivity between reconnaissance teams and the reconnaissance operation center or command operations center via organic electronic communication channels that are external to and separate from MAGTF SIDS.

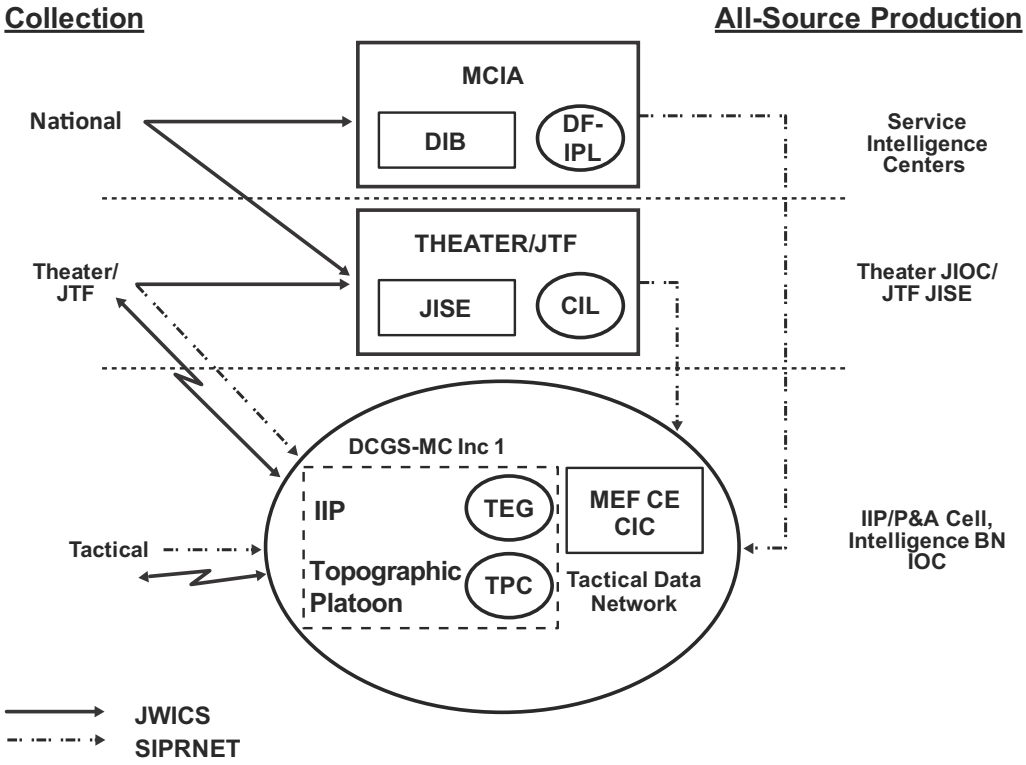
MAGTF Secondary Imagery Dissemination System Video Exploitation Workstations. The MAGTF SIDS video exploitation workstation enables scanning, editing, copying, printing, manipulation, cataloging, and presenting of still and video images from various sources, including captured media. It enables users to select and sort through large amounts of data gathered from either the operating forces or supporting aircraft. Imagery can be imported into the MAGTF SIDS video exploitation workstation in an analog format, such as Hi8, mini-digital video or DV, VHS [video home system] tape. It could also be imported in a digital format through DVD [digital video disc]/CD [compact disc], scanner, directly from a digital camera, with digital camera cards via a multicard reader, or through SIPRNET.

Imagery Tasking, Processing, Exploitation, and Dissemination Capabilities

The Marine Corps possesses organic imagery tasking, processing, exploitation, and dissemination capability. Access to national, joint, theater, and Service processing and production capabilities will therefore be important elements of the Marine Corps imagery architecture (see fig. 4-9). The following subparagraphs provide descriptions of key IMINT processing, exploitation, and production information systems.

Imagery Reachback Site—Marine Corps Intelligence Activity. The MCIA provides 24-hour dissemination of national and commercial imagery to MAGTFs and other Marine Corps units (including the supporting establishment). Dissemination of imagery is accomplished via the Global Broadcast System or SIPRNET. The MCIA's intelligence, imagery, database systems, and requirements include direct feed imagery product library and imagery exploitation support system. The MCIA—

- Receives, stores, and exploits digital NRT imagery from national, commercial, and theater imagery collection platforms.
- Allows general message-level imagery access to Marine Corps elements and a select group of remote clients for imagery analysis.



MCIA and the IIP are the Marine Corps' principal imagery and GEOINT processing and production facilities.
Within the MEF, the principal all-source intelligence processing and production organization is the P&A cell, intelligence BN.

LEGEND

BN	battalion	DF-IPL	Direct Feed Imagery Product Library
CE	command element	TPC	topographic production capability
CIL	command information libraries		

Figure 4-9. Marine Corps Imagery Architecture.

- Provides customers with a search tool for querying its holdings.
- Maintains a current set of national imagery on pre-selected locations relevant to expeditionary operations. These images are updated continually.

Tactical Exploitation Group. The TEG family of systems provides the Marine Corps with a highly mobile tactical imagery ground station capability to analyze aerial imagery from national, theater, and tactical reconnaissance assets and develop imagery products/reports for dissemination in support of both MAGTF and joint operations.

The primary goal of the TEG FoS is to provide responsive imagery exploitation support to the Marine air-ground task force (MAGTF) for tactical operations, strike planning, detection, location of targets of opportunity, and battle damage assessment (BDA) for re-strike planning and intelligence assessment. The Tactical Exploitation Group (TEG) System is the primary tactical imagery exploitation system in the Marine Corps and is one of the capabilities comprising the Distributed Common Ground/Surface System-Marine Corps (DCGS-MC) Geospatial Intelligence (GEOINT). This equipment will be used by the 0241's in garrison, field, shipboard operations, and training exercises. The TEG FoS is comprised of modular and scalable configurations and employs Commercial Off-the-Shelf, Government-Off-the-Shelf, and Non-Developmental Item computer hardware and software to enable rapid upgrade and to maintain commonality with Marine Intelligence and Joint Imagery Systems. The TEG FoS is comprised of the VIP-MC and TEG-RWS (see fig. 3-2 on page 3-4).

Imagery Communications and Information Systems Architecture

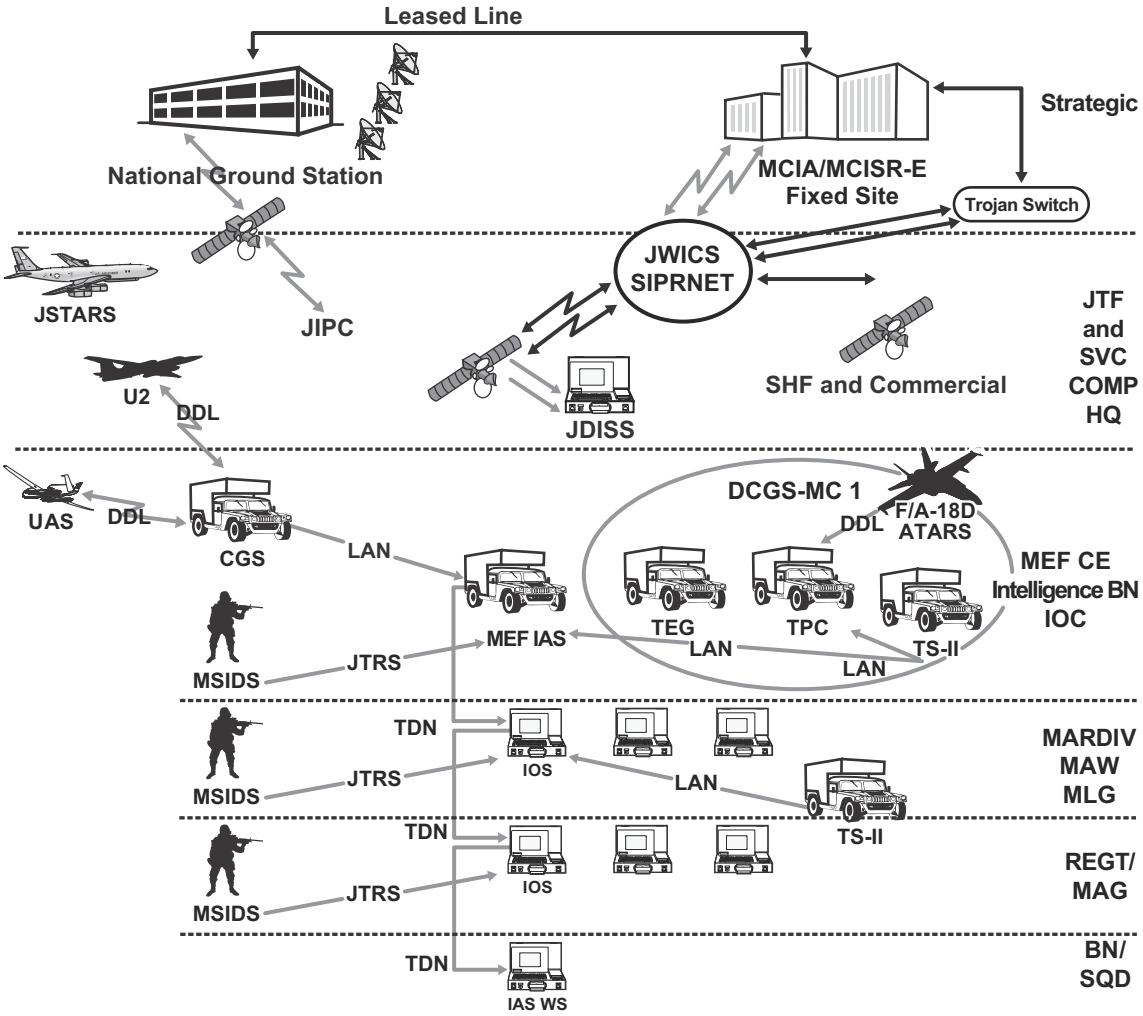
Figure 4-10, on page 4-18, and figure 4-11, on page 4-19, depict the internal IMINT CIS architecture for a MEF and the broader IMINT CIS architecture through the theater and national levels.

Geospatial Intelligence Communications and Information Systems Planning Considerations

The MAGTF CIS requirements and planning considerations for GEOINT operations include the following:

- Ensuring the MAGTF command element and subordinate elements are included in the distribution of IMINT-related address indicator groups to receive pertinent tactical, theater, and national intelligence and GEOINT products.
- Determining, establishing, and coordinating communication requirements and operational procedures in support of GEOINT operations.
- Coordinating IMINT CIS activation and restoration priorities and supporting procedures.
- Identifying and procuring community security materiel system requirements for unique IMINT communications.
- Determining and coordinating intelligence network information systems requirements in support of IMINT operations, such as hardware, software, internet protocol addresses, accreditation, or authority to operate/connect.
- Integrating MAGTF IMINT element CIS operations with those of other MAGTF, pertinent JTF, and other components intelligence and reconnaissance units, such as mutual support and cueing.

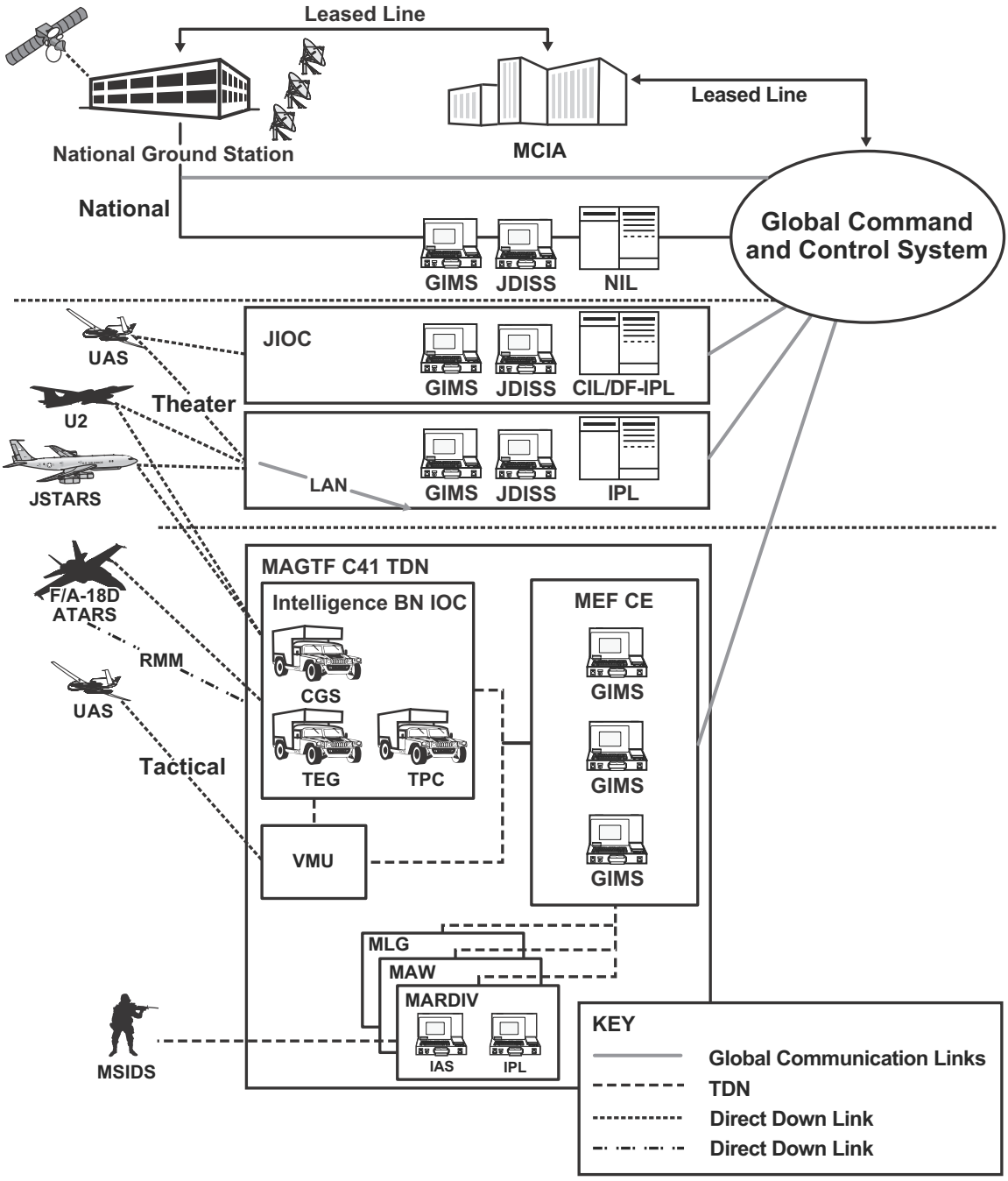
- Integrating CIS of IMINT elements employed in general support with collocated ground combat element, ACE, LCE, and other MAGTF elements.
- Coordinating MAGTF GEOINT databases administration and operations.
- Coordinating GEOINT CIS and TCPED operations and procedures with other Services, as well as allied and coalition forces.



LEGEND

BN	battalion	MSIDS	MAGTF secondary imagery dissemination system
CE	command element	REGT	regiment
COMP	component	SHF	super-high frequency
DDL	dedicated data link	SQD	squad
HQ	headquarters	SVC	Service
IOS	intelligence operations server	TPC	topographic production capability
JIPC	joint imagery production complex	U2	reconnaissance aircraft
JTRS	joint tactical radio system	WS	workstation
MAG	Marine aircraft group		
MARDIV	Marine division		

Figure 4-10. Internal Communication and Information Systems Imagery Intelligence Architecture.



LEGEND

BN	battalion
CE	command element
CIL	Command Information Library
CM	collection management
DF-IPL	Direct Feed Imagery Product Library
FoS	family of systems
GIMS	Geospatial Information Management System
MARDIV	Marine division
MDC	metadata catalog
MSIDS	MAGTF secondary imagery dissemination system
Nav	navigational
NIL	National Information Library
RMM	removable memory module
TPC	topographic production capability

Figure 4-11. Broader Communications and Information Systems Imagery Intelligence Architecture.

CHAPTER 5
PLANNING

The following functions are key to planning:

- Developing a plan that directs and coordinates action.
- Fostering shared situational awareness.
- Generating common expectations about how actions will evolve and affect the desired outcome.
- Supporting the exercise of initiative.
- Shaping the thought processes of planners.

SUPPORT TO THE PLANNING PROCESS

When providing support to the planning process the following should be considered: planning for imagery intelligence; types of imagery; aerial imagery collection missions; and processing, exploitation, and dissemination of imagery and imagery intelligence.

Planning for Imagery Intelligence

Planning for IMINT includes implementing the IMINT planning process, integrating imagery intelligence planning with the intelligence cycle, fulfilling imagery intelligence planning considerations, and understanding planning responsibilities.

Imagery Intelligence Planning Process. There are eight steps in the IMINT planning process.

Planning. The first step is to determine the exact needs—including key collection, production, and dissemination requirements—so that priorities are accurately determined, resources are not overwhelmed, and timely support is provided.

Requesting. The most important part of any request is to clearly articulate the IMINT intelligence requirement. Each intelligence request should include the mission and how the intelligence product being sought will fulfill the stated need.

Validating. Intelligence and imagery should be reviewed to determine whether or not the intelligence requirement can be answered immediately. If not, the intelligence requirement should be checked against previously validated intelligence requirements and ongoing/planned intelligence operations to avoid unnecessary duplication. Finally, the intelligence requirement should be checked against the capabilities of the intelligence assets supporting the unit. If the intelligence

requirement is validated using these criteria, then a priority will be assigned to the intelligence requirement and associated intelligence collection, production, and/or dissemination requirements (e.g., ICRs, intelligence production requirements, and intelligence dissemination requirements) will be developed and prioritized.

Planning and Tasking. The collection manager determines the tasking by which the intelligence requirement will be satisfied—either organic or external intelligence operations will be tasked to satisfy the intelligence requirement. If collection is required, the CM/DO determines the best intelligence asset to perform the mission. Concurrently, the CM/DO develops plans and tasks to ensure projected dissemination requirements can be fulfilled, while the geospatial support team develops necessary production plans and tasking. The requirements can be fulfilled using either organic or external assets: when organic intelligence resources are used, appropriate orders shall be issued; when external support is required, the intelligence requirement shall be submitted to either higher headquarters or supporting organizations.

Collecting. The validated ICRs and intelligence production requirements are used to ensure the most effective type of imagery is collected to satisfy the overall intelligence requirements. The capabilities and limitations of each imagery collection element, the time the collection must occur, and the weather influence is the nature of collection operations.

Exploiting. Requirements for IMINT exploitation are defined in terms of three phases. Each phase represents a greater degree of analysis and a longer period of time available to accomplish the exploitation and associated production.

The first phase includes the rapid exploitation of newly acquired imagery, and reporting of imagery-derived intelligence and intelligence information within a specified period of time from the receipt of imagery. Phase one satisfies priority requirements related to immediate needs and/or identifies changes or activity of immediate significance.

Like phase one, the second phase includes the detailed exploitation of newly acquired imagery; however, the reporting of imagery-derived intelligence and intelligence information is weighed by analytic requirements and timeliness of need. Phase two provides for an organized and comprehensive account of the intelligence or intelligence information extracted from newly acquired imagery and is supported by other intelligence source materials, as appropriate.

The third phase includes the in-depth analysis of available imagery pertinent to an intelligence requirement and the reporting of results within a specified time. In response to intelligence requirements, phase three provides the most comprehensive analysis of a target or topic using imagery as the primary data source but, when appropriate, incorporates data and intelligence from other sources. The last steps of this phase are disseminating and utilizing.

Disseminating. Imagery intelligence products are disseminated either as hardcopy or softcopy products. Hardcopy products are disseminated via couriers or the available mail system. Softcopy products may also be distributed as hardcopy products or electronically via the MAGTF communications network. The requestor and the supporting G-2/S-2s, with assistance from units' G-6/S-6, must ensure that the requested product can be transmitted over the available supporting CIS.

Use. As it is with the intelligence process, the last step of the IMINT planning and execution process, effective utilization, is the most important. Commanders and other imagery/IMINT users should notify the G-2/S-2 regularly regarding both the quality of the products and how well particular products answered their CCIRs and intelligence requirements. Additionally, new intelligence requirements that result from new imagery/IMINT should be identified and action should be initiated to plan future operations effectively. Finally, providing the G-2/S-2 and IMINT elements with feedback will help to identify problems and allow improvements to be developed and implemented quickly.

Integrating Imagery Intelligence Planning with the Intelligence Cycle. The intelligence cycle is a procedural framework used for developing mission-focused intelligence support for the range of military operations. The intelligence cycle should be applied in a manner that develops the required intelligence in the most effective way. The application of the intelligence cycle will vary during mission planning and execution. Application of the intelligence cycle is driven by intelligence requirements. In theory, a unique iteration of the intelligence cycle is carried out for each individual intelligence requirement. However, in practice intelligence requirements are grouped together and satisfied through a single, intelligence development process that addresses all intelligence requirements, including IMINT requirements, concurrently.

During planning, the application of the intelligence cycle supports mission analysis, COA development, and COA wargaming by providing basic intelligence, including IMINT, in the form of intelligence estimates, supporting studies, and IPB analyses that describe the battlespace and threat. (See app. C for detailed information regarding imagery and IMINT support to IPB and other all-source intelligence products.)

During COA comparison and analysis, orders development, and transition, the intelligence cycle is applied to satisfy emerging intelligence requirements and update the intelligence estimate and IPB products—all of which may be supported by IMINT.

During execution, the intelligence cycle is applied to implement the intelligence collection, production, and dissemination plan; refine IPB analysis, and generate mission-specific multidiscipline intelligence operations and intelligence products—all of which are integrated with the CONOPS.

During execution, intelligence requirements are satisfied individually. New intelligence requirements are generated in response to specific operational needs. Each intelligence requirement is unique and must be satisfied in a timely manner to facilitate rapid decisionmaking and the generation or maintenance of tempo (see fig. 5-1 on page 5-4).

Imagery Intelligence Planning Considerations. The IMINT plan should reflect proven planning principles. Considerations for IMINT planning are discussed in the following subparagraphs.

Fulfill the Stated Requirements. The IMINT plan should fulfill the stated requirements. It should ensure imagery data is collected, processed, and reported to satisfy the intelligence requirements set forth in the commander's guidance and collection plan. Particular attention must be paid to the timeliness and formats of the data provided.

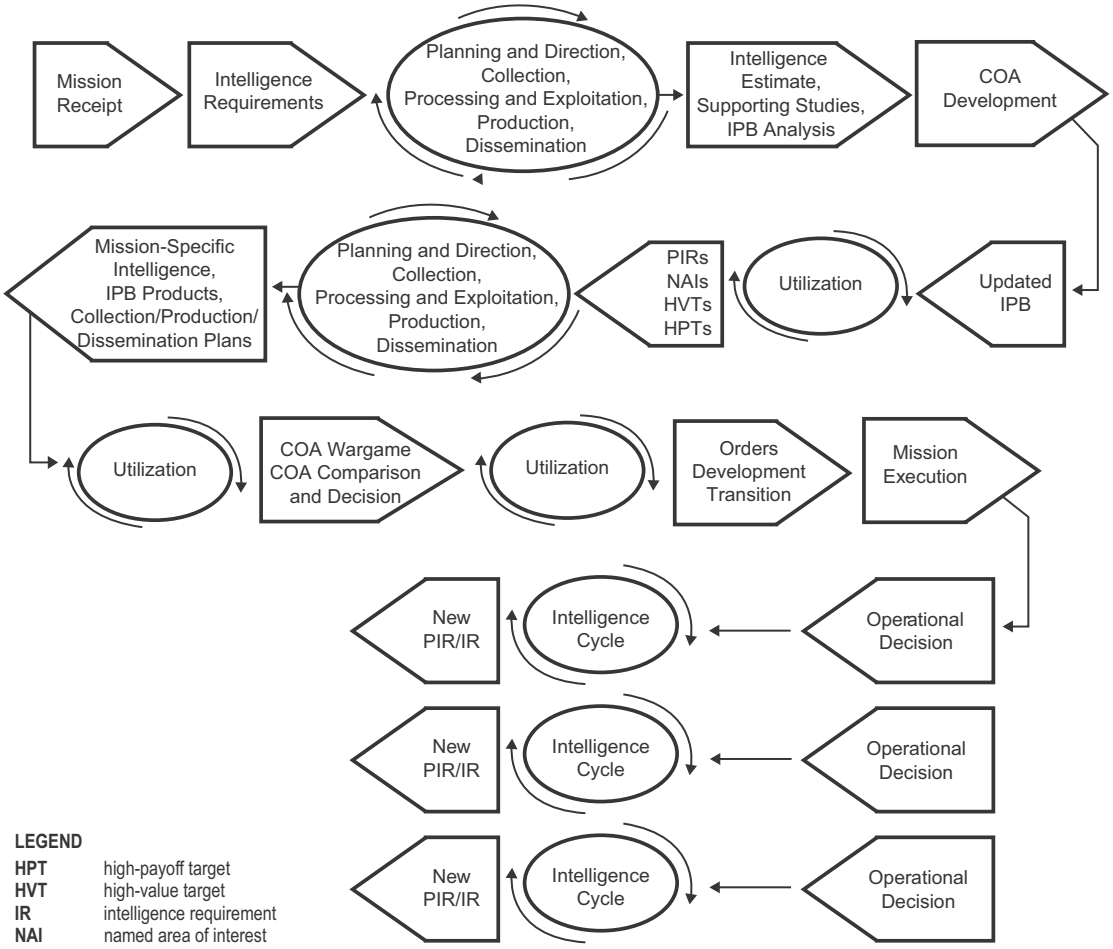


Figure 5-1. Application of the Intelligence Cycle.

Integrate with Other Intelligence Plans. The IMINT plan should be integrated with other intelligence plans. Effective IMINT planning and execution require close coordination, liaison, and integration with all-source intelligence elements. Frequently, IMINT collection management is driven by cross-cueing from SIGINT, HUMINT, and other sources of intelligence. Also, fusion of IMINT with other intelligence ultimately drives the conduct of future IMINT operations and the development of IMINT products.

Integrate with Other Operations. The IMINT plan must take into account the location and activities of the supported units. Planned missions must be scheduled where and when they can best collect sensor data. Additionally, C2 and CIS arrangements must be coordinated in order to ensure imagery data and IMINT are reported to the supported units. Because enemy activity may be anticipated at certain phases of military operations, IMINT operations and analytical personnel must have a situational awareness of both intelligence estimates and ongoing operations to focus their efforts at a particular time and area. Finally, the requirement for timeliness in processing and reporting may vary depending upon the stage of the operation; personnel must be aware of current timeliness requirements as well as the availability of CIS resources with all supported commands.

Integrate into the Overall Collection Plan. The IMINT plan should be integrated with other intelligence and reconnaissance operations to ensure the required data can still be acquired even when a planned

imagery mission is canceled or critical equipment malfunctions. The ability to provide this redundancy depends upon the number of imagery missions available, capability of other intelligence resources to acquire the information needed, and the availability of production resources.

Make Use of All Imagery Intelligence Resources. The IMINT plan should make use of all IMINT resources. While some imagery collection resources may be held in reserve, most units and systems can fulfill multiple missions and should be employed. Close coordination and integration of operations and intelligence activities will aid with identifying and prioritizing these multipurpose missions. Imagery intelligence production resources should not be held in reserve.

Support the Concept of Operations. The IMINT plan should support the CONOPS. Imagery intelligence efforts must support and adapt to the MAGTF commander's intent, concepts of intelligence and operations, and the supporting scheme of maneuver. Key questions to be answered regarding supporting the CONOPS include—

- What are the MAGTF AO and the AOI?
- What are the MAGTF CONOPS, task organization, and main and supporting efforts?
- What are the standing PIRs and intelligence requirements? Which have been tasked to supporting IMINT units? What specific information most interests the commander (e.g., enemy ground operations, enemy air operations, target BDA, friendly force protection, or enemy future intentions)?
- What is the concept of MAGTF fires support? How will MAGTF target development and target intelligence be conducted? What are the specific imagery needs in support of these tasks?
- What are the IMINT and intelligence CONOPS of other JTF, component, and/or theater resources? What are the task-organization and command/support relationships for all MAGTF intelligence and reconnaissance units?
- How can external assets be incorporated to support MAGTF operations?

Take Into Account the Physical Environment. The IMINT plan should take into account the physical environment, including terrain and weather. Terrain factors have a significant impact on IMINT operations, such as the ability of IMINT sensors to see through vegetation and IMINT's requirements for line of sight (LOS) communications. To be effective, all IMINT collection systems require LOS to the target area. Accordingly, IMINT planners must assess the effects of mountains, defilade, vegetation, and other potential terrain obstacles on all planned IMINT operation.

Consider Weather as a Key Limiting Factor. Bad weather degrades the identification and location of targets and can limit the type of imagery collection capabilities that may be employed. In addition, low ceilings and poor visibility decrease both visual reconnaissance effectiveness and the resolution of photographic systems. Weather factors to consider include the following:

- *Precipitation*. Visible moisture degrades optical and visual reconnaissance systems. Most UASs are not all-weather aircraft. Consequently, rain, ice, and snow can severely damage or even destroy a UAS.
- *Wind*. UASs are significantly more affected by wind than manned aircraft.

- *Clouds, Haze, and Smoke*. In addition to affecting the aircrew's ability to conduct visual reconnaissance, cloudy, hazy, and smoky conditions also affect EO and infrared systems on both manned aircraft and UASs.
- *Daylight, Sun Angles, and Shadows*. The angle of the sun affects visual, EO, and forward-looking infrared (FLIR) observations differently. The quality of FLIR imaging decreases as the sun rises and reaches a point where a target can be seen visually. At this point the target cannot be detected by a FLIR. Prior to sunset and just after sunrise, long shadows are cast by large terrain features and can obscure objects in their path. The ideal time to take photographs or observe a target is mid-morning or mid-afternoon. During these periods, shadows are cast long enough to add definition and dimension to a target.

Consider the Threat. Threats can be general or aviation related. For a general threat, a detailed threat analysis must be conducted to determine which imagery sensors and platforms can be employed effectively against a given enemy target, and then how to employ the limited resources available to the MAGTF to obtain the required IMINT. The enemy can, in turn, impede imagery operations by employing CCD activities as well as focusing their air defense capabilities.

Enemy air defenses have a direct effect on aerial imagery collection missions. Since aircraft must stay beyond threat air defense ranges, significant antiaircraft artillery (AAA) and surface-to-air missile (SAM) threats may degrade visual reconnaissance. Imagery intelligence planners must assess threat air defense and air-to-air threats when evaluating risk and determining routes. Finally, threat EW capabilities must be identified and assessed in order to determine their effects on UAS and manned imagery platforms radio uplinks and imagery downlinks.

Consider the Type of Collection. The IMINT plan shall consider the various types of imagery collection capabilities. A variety of organic imagery collection capabilities are available to a MAGTF (see fig. 5-2 on page 5-7). The following planning considerations are critical to effective direction and employment of these resources. Imagery collection resources readily locate and identify large threat forces, moving vehicles, weapon systems, structures and other topographic features that contrast with their surroundings. Conversely, small, stationary/well-camouflaged enemy forces blending into their surroundings can be difficult to locate and identify. Generally, it is better to employ imagery collection resources against point targets rather than in a wide area search mode. Effective integration with other intelligence operations can cue imagery collectors to key targets, reducing the search area, thereby reducing the time required to produce actionable intelligence.

Area Reconnaissance. Area reconnaissance is the systematic and complete coverage of an area using visual/imaging means. Area reconnaissance is normally used to locate/identify specific targets for further collection and analysis. It is also used to support terrain analysis. Area reconnaissance imagery can be collected two different ways: first, by imaging back and forth across a predetermined area so that flight lines and individual images overlap—this process provides complete coverage of all objects within the area at the expense of increased sensor utilization time; second, by adjusting focal lengths/altitudes to allow a lesser number of images to cover the target area. This process reduces time on target (TOT) as well as the processing, exploitation, and dissemination time at the expense of reduced resolution. Types of area reconnaissance imagery missions include broad area coverage/surveillance and directed search area missions.

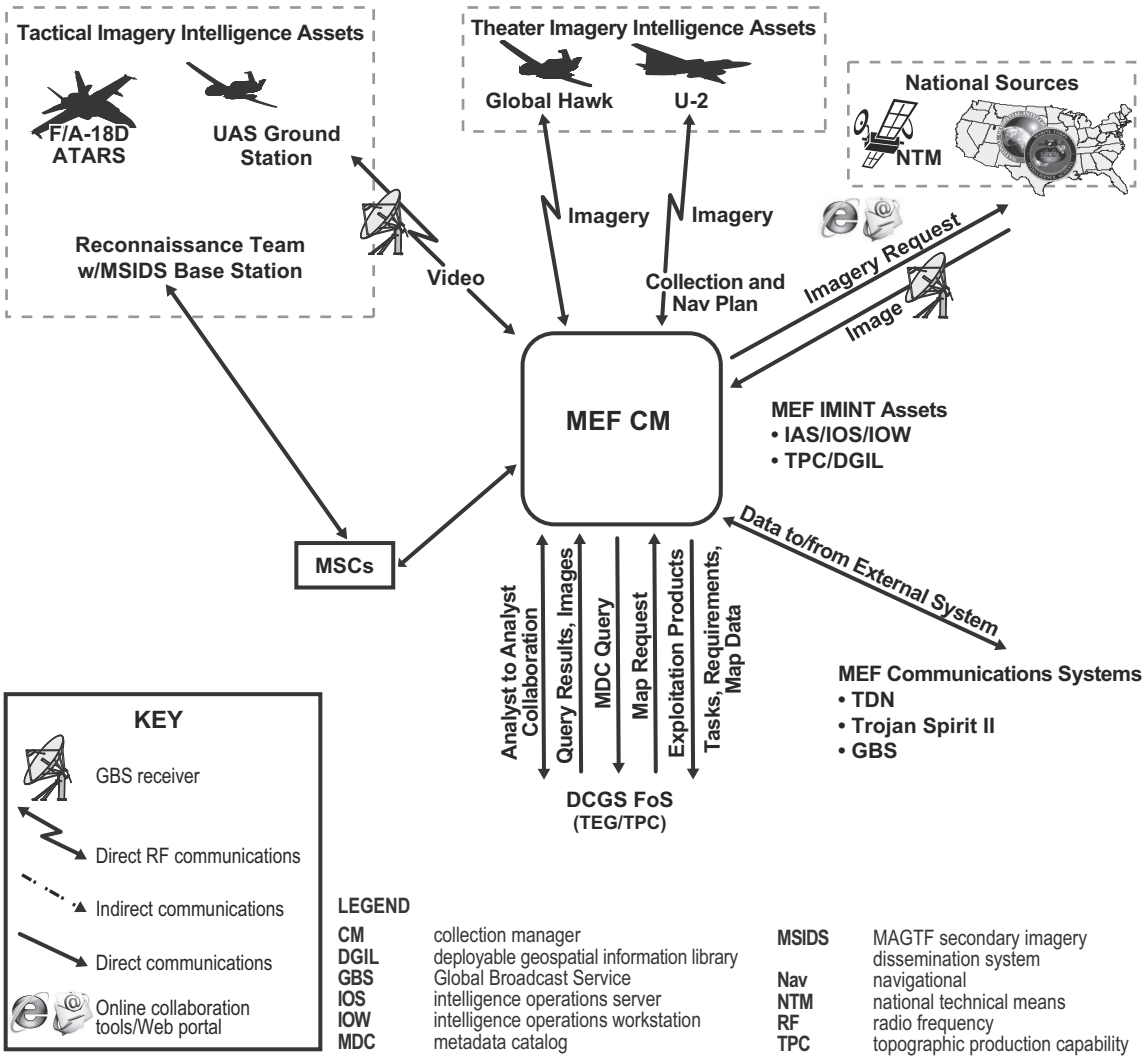


Figure 5-2. Marine Expeditionary Force Imagery Collection Capabilities.

Broad area coverage/broad area surveillance are area reconnaissance imagery collection tactics that provide an overview of an entire area. They should not be the primary collection tactics utilized to collect against known point targets. (During area collection operations, the flight tracks/ routes are planned and the image exposures adjusted so that each successive image will overlap the previous one.) During the early phases of an operation broad area coverage and broad area surveillance may be conducted for two intelligence purposes: first, providing a basis for the procurement of larger scale imagery of selected areas for subsequent detailed analysis; second, serving as a comparative baseline for determining the nature and extent of changes identified on subsequent missions.

Directed search area missions provide focus and detail, and are useful for OOB confirmation counts.

Point Targets. Point targets are normally tasked to provide the highest possible resolution of a specific target that allows for detailed analysis. Point targets can vary in size and include command posts, bridges, airfields, and SAM sites.

Line of Communications. Line of communications collections involve imaging along specific transportation routes, such as roads, railroads, or waterways. This type of reconnaissance is normally conducted to determine enemy movement or potential usability of a route; it can also support mapping or terrain analysis requirements. This methodology is good for maneuverability studies, but generally requires significant time for effective exploitation. Line of communications missions should be conducted ahead of time as a contingency baseline.

Planning Responsibilities. Imagery intelligence planning is a continuous function that requires close interaction between the G-2/S-2 and IMINT unit planners. Key objectives include the following:

- Identifying IMINT requirements.
- Preparing IMINT operations plans.
- Planning and establishing the IMINT support system.
- Issuing orders/tasking to IMINT units.
- Supervising and coordinating IMINT operations.

Assistant Chief of Staff G-2/S-2. Primary staff responsibility for the planning of IMINT operations lies with the AC/S G-2/S-2. Specific responsibilities of the AC/S G-2/S-2 include the following:

- Preparation of integrated, multidiscipline intelligence and reconnaissance operations and supporting IMINT plans, orders, annexes, and appendices.
- Coordination with the G-3/S-3 to ensure the planned IMINT plan supports both the CONOPS and scheme of maneuver.
- Coordination with the G-6/S-6 officer for CIS support to the IMINT elements, including circuits, network access, frequency assignment, equipment, and call signs.
- Liaison with IMINT agencies and units external to the MAGTF. Identifying, preparing (including all required equipment), and locating IMINT or all-source intelligence liaison elements to support MAGTF IMINT operations is a critical early planning action. The IMINT liaison teams will be small in number due to the limited availability of imagery personnel.
- Coordination with the G-4/S-4 to ensure adequate logistic support of IMINT elements.

Intelligence Battalion Commander/Detachment Officer in Charge. The intelligence battalion commander/detachment OIC is responsible to the AC/S G-2/S-2 (or in some cases the MAGTF intelligence operations officer) for the planning, direction, and execution of MAGTF IMINT operations. Specific duties of the battalion commander/detachment OIC include the following:

- Advising the G-2/S-2 on IMINT employment and its integration with other Services, JTF, theater, and national IMINT operations.
- Preparing MAGTF IMINT plans and orders in conjunction with other intelligence section staff officers and key intelligence battalion subordinates.
- Planning, supervising, and assisting IMINT collection requirements and tasking for MAGTF operations, in conjunction with the CM/DO.

- Coordinating the movement, operation, and reporting of IMINT units in coordination with the SARC OIC and the G-3/S-3.
- Coordinating MAGTF IOC analyst exchanges with IMINT analysts and the integration of GEOINT products with all-source intelligence production in conjunction with the MAGTF IOC OIC. The battalion commander/detachment OIC must take into account the strenuous mental and physical demands on imagery analysts during sustained operations, particularly when planning watch schedules for imagery analysts performing detailed imagery exploitation tasks.
- Planning for the timely reporting of IMINT to both MAGTF and external elements and the rapid handling of time sensitive information in coordination with the CM/DO.
- Planning and coordinating IMINT communications paths and information systems management and operations in conjunction with the G-6/S-6.

Types of Imagery

The types of imagery are electro-optical, infrared, radar, multispectral, hyperspectral, and commercial. Certain policies apply to imagery of the United States.

Electro-Optical Imagery. Electro-optical imagery employs digital imaging techniques to extend and complement other imagery. Electro-optical imagery is readily exploitable by automated processors and analytical aids. It uses the visual spectrum, so anything that impacts this spectrum, such as dust, smoke, haze, clouds, rain, fog, light level, or angle of illumination, will affect the quality of the imagery.

Infrared Imagery. Infrared imagery systems can operate day or night under favorable weather conditions. They are less effective during day/night transition periods or when backgrounds and targets have negligible differences in temperature.

Infrared imagery is the remote sensing of the radiant temperature associated with a target. The system is used to measure the temperature differences between terrain features and surrounding objects on the ground, producing a near-optical-quality infrared image (see fig. 5-3 on page 5-11).

Unique infrared imagery capabilities include imaging the shadow on a heat-absorbing surface or the thermal scar of a heat-generating object.

Radar Imagery. Radar imagery can be collected day or night and under all weather conditions. Generally, it is limited only by the capability of the platforms conducting the collection mission. Radar imagery is best utilized in conjunction with other imagery sensors. Unlike EO imagery, it presents a nonliteral image of the battlespace, requiring special skills and time to analyze properly. See figure 5-4, on page 5-10, for an example of SAR imagery.

Radar Reflection. Radio-frequency energy is transmitted to and reflects from the reflecting object. A small portion of the energy is reflected and returns to the radar set. This returned energy is called an echo, just as it is in sound terminology. Variations in the pattern and tone of the echo are recorded and displayed as radar images.

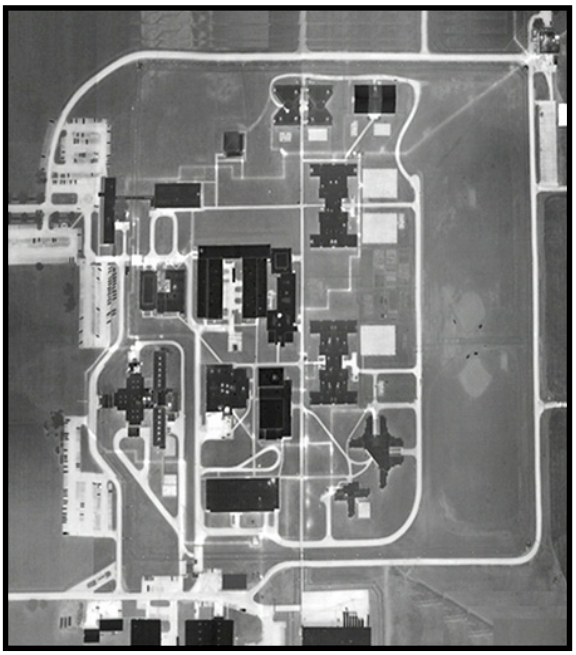


Figure 5-3. Infrared Imagery.

Figure 5-4. Synthetic Aperture Radar Imagery Example.

Doppler Shift. The geometry and surface composition of targets and their surroundings can greatly affect the intensity of the radar pulse return. To detect moving targets, radars employ the principle of Doppler shift. Doppler shift is the result of a moving object causing a subtle change in the frequency of the reflected pulse energy. This change is detected by comparing the original pulse energy frequency to the frequency of the reflected energy. See figure 5-5, on page 5-11, for an example of an MTI image.

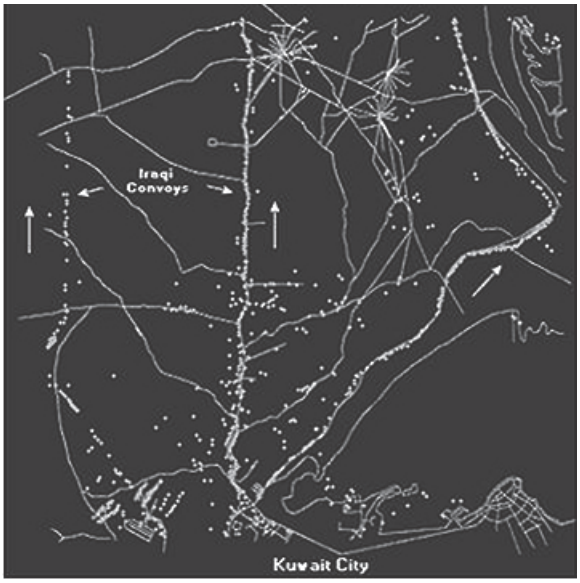


Figure 5-5. Joint Surveillance Target Attack Radar System Moving Target Indicator Imagery.

Multispectral Imagery. Multispectral imagery records multiple views in several spectral bands or frequencies simultaneously. The key to interpreting these images lies in the identification of the spectral signatures of the various surfaces and targets. Whether it is generated by itself or reflected, every surface or target gives off a unique pattern of radiation. The shape of the pattern depends on the reflective qualities of the material, its heat, whether it is a solid or liquid, the smoothness of the surface, and several other factors.

Hyperspectral Imagery. Hyperspectral imagery sensors use hundreds of very narrow wavelength bands to *see* reflected energy from objects on the ground. This energy appears in the form of "spectral fingerprints" across the light spectrum. Once these fingerprints are detected, special algorithms—repetitive, problem-solving mathematical calculations—are used to assess them so that various natural and manmade substances can be differentiated from one another. Signature libraries may also be used to identify specific materials, such as rooftops, parking lots, grass, or mud, by comparing a library's pre-existing reference catalogs with freshly taken hyperspectral images of the battlefield from space. Image processing equipment then portrays the various types of terrain and objects upon it in different colors forming a "color cube," each based on the wavelength of the reflected energy captured by the image. These colors are subsequently "translated" into maps that correspond to certain types of material or objects to detect or identify military targets, such as a tank or a mobile missile launcher.

Commercial Imagery. The commercial imagery industry has launched and will continue to launch new high-resolution panchromatic, multispectral imagery, and other imagery systems. These systems will provide an increased capability to supplement and complement our national imagery technical collection. The HQMC Imagery and Geospatial Intelligence Branch works closely with NGA on commercial imagery issues. Marine Corps policies and procedures for requesting, tracking, obtaining, and purchasing commercial imagery are under development. These policies and procedures are promulgated from NGA's Commercial Imagery Management Office, which publishes commercial imagery plans that improve DOD and intelligence community access to commercial imagery.

Domestic Imagery Collection. Domestic imagery collection includes satellite and aerial imagery of any part of the United States and its territories or possessions, including the 12 nautical miles seaward of these land areas. Before domestic imagery collection in the aforementioned geographic areas may be conducted, an approved proper use statement is required. Central to this process is a thorough review of planned missions to ensure that the constitutional rights of US citizens are protected according to current laws and executive orders restricting intelligence activities directed against US citizens within the United States. Approved proper use statements must be retained in the permanent files of the requesting unit and higher headquarters up through the combatant command headquarters. For additional information on domestic imagery collection, see NGA Imagery Policy Series [IPS] [section 9, part B], Domestic Imagery [IPS-001/98-S9A]. Request channels for domestic imagery collection are Marine Corps-specific requirements (proper use statements are submitted via the service chain of command to the MCIA/DRO) and joint operations requirements (proper use statements are submitted via the operational chain of command to the combatant commander for adjudication or follow-on action, as appropriate).

Aerial Imagery Collection Missions

Aerial imagery collectors provide the flexibility to respond rapidly to changing battlespace conditions. Unmanned aircraft systems provide both the added advantage of operating in areas of heavy enemy air defenses and the needed intelligence without the risk of exposure of manned aircraft. Intelligence imagery collection planners establish detailed preplanned imagery collection routes, areas, and point targets encompassing the AOI using the results of IPB, the MAGTF's CONOPS, and scheme of maneuver.

Aerial imagery collection missions require detailed operational planning, particularly with respect to their integration with other ACE operations. Since all aerial imagery collection platforms are multipurpose, close coordination between MAGTF command element imagery planners and ACE operational planners is necessary to identify, reconcile, prioritize, and integrate competing requirements for resources. Additionally, all aerial imagery missions must be included on the ATO and coordinated with other air operations and, where pertinent, supporting arms. This coordination is particularly critical with regard to UAS operations. Unmanned aircraft systems enter the airspace control system via the appropriate airspace control agency, normally the DASC. Unmanned aircraft system controllers maintain communications with the appropriate ACE C2 agency, such as the DASC, during missions in order to receive routing, altitude, and other pertinent airspace control information.

The commander who directly tasks or controls an imagery collection mission will receive the most responsive support. The responsiveness of the mission to other commanders depends on the number of echelons through which the mission request and resulting intelligence must flow. Accordingly, when planning imagery collection operations, the advantages and disadvantages of dedicating missions to a single command (i.e., direct support) must be assessed against the MAGTF's total intelligence requirements and the current situation. Previously acquired imagery and IMINT products should always be reviewed to see if they can satisfy intelligence requirements without need of additional imagery collection missions.

Often, the intelligence acquired from an imagery collection mission (vice the actual image) will be all that is required to satisfy many intelligence requirements. Likewise, dissemination challenges

are generally simpler and faster when users' intelligence requirements can be satisfied without the images. Accordingly, to ensure optimum support, commanders must understand the pros and cons of various imagery-related intelligence requirements.

Usually, collected imagery will require additional processing and fusing with other intelligence to provide the necessary support. Depending on the situation, this may be a time-intensive task. Commanders should assess likely processing and production timelines and other requirements when developing IMINT plans.

Intelligence acquired from a number of imagery collectors may be disseminated directly to users with minimal additional intelligence processing and all-source intelligence analysis. Supporting dissemination plans must ensure identification of the type products likely disseminated as well as the technical requirements associated with these products. In the case of resources, such as the UAS or JSTARS, dissemination planning includes the establishment of dedicated communications links directly between the collector and the supported unit.

Preplanned Missions. Preplanned aerial imagery missions (e.g., UAS, ATARS) are requested using the joint tactical air reconnaissance/surveillance (JTAR/S) request format (see app. H, section I). Within the MAGTF, preplanned aerial imagery requests are routed through the intelligence chain and consolidated by the MAGTF command element's intelligence section for validation, prioritization, and follow-on planning and coordination.

Immediate Missions. Immediate requests for aerial imagery collection will be submitted via the operational chain of command to the DASC. However, this is rarely done because available resources are generally limited and operate in general support of MAGTF requirements. The joint tactical air strike request format (see app. H, section II) may be used to request immediate aerial imagery collection support. When approved, the mission may be executed in one of the following ways:

- An ongoing mission can be diverted by its controlling authority to conduct the immediate mission.
- An on-call/standby mission may be allocated.

Air Planning and the Air Tasking Cycle. The air tasking cycle is the key tool used by MAGTF planners to plot most air operations (i.e., pre-planned and immediate) to support mission accomplishment. By using and completing the air tasking cycle, planners can ensure that, with correct prioritization, aviation assets can be used most effectively, while maintaining command and control and CIS in support of the MAGTF.

The Air Tasking Order. The principal planning product of the air tasking cycle is the MAGTF ATO or air plan. The ATO is a document generated by the joint force air component commander or the ACE commander. It tasks and disseminates the specific missions and targets of projected air sorties, capabilities, and forces to JTF components, subordinate units, and C2 agencies. It normally provides both general and specific instructions, including call signs, targets, and controlling agencies. The airspace control order is included in the ATO. Special instructions that provide amplifying notes, important details, and changes are included in the ATO or issued

separately. The ATO, airspace control order, and special instructions provide operational and tactical direction at appropriate levels of detail. For further information on the air tasking order, see MCWP 3-25.

Phases of the Air Tasking Order. The six phases of the ATO cycle are command aviation guidance, target/air support mission development, allocation and allotment, tasking, force execution, and combat assessment (see fig. 5-6).

Requesting Joint Task Force, Theater, and National Imagery Support. Significant imagery and IMINT support is available to the MAGTF from external sources, ranging from dissemination of existing imagery and products through the integration of existing information into new products and execution of new imagery collection and IMINT production. Those MAGTF intelligence requirements that cannot be satisfied by organic resources will be submitted to the next higher command echelon for validation, prioritization and, if possible, satisfying the RFI or collection requirements through its organic resources, before forwarding it to the next higher command echelon. The specific intelligence requirement will determine how the requirement is identified and submitted. Techniques include the use of the standard RFI and the use of collection/ production management systems and procedures. Figure 5-7, on page 5-15, identifies the two different tracks external imagery and IMINT requirements may take.

Processing, Exploitation, and Dissemination of Imagery and Imagery Intelligence

Processing. The processing of imagery and IMINT involves the conversion of collected data into information that is suitable for the production of intelligence.

Exploitation. The exploitation of imagery and IMINT is the activity that converts information into intelligence. It fuses new information and existing intelligence from all sources to provide

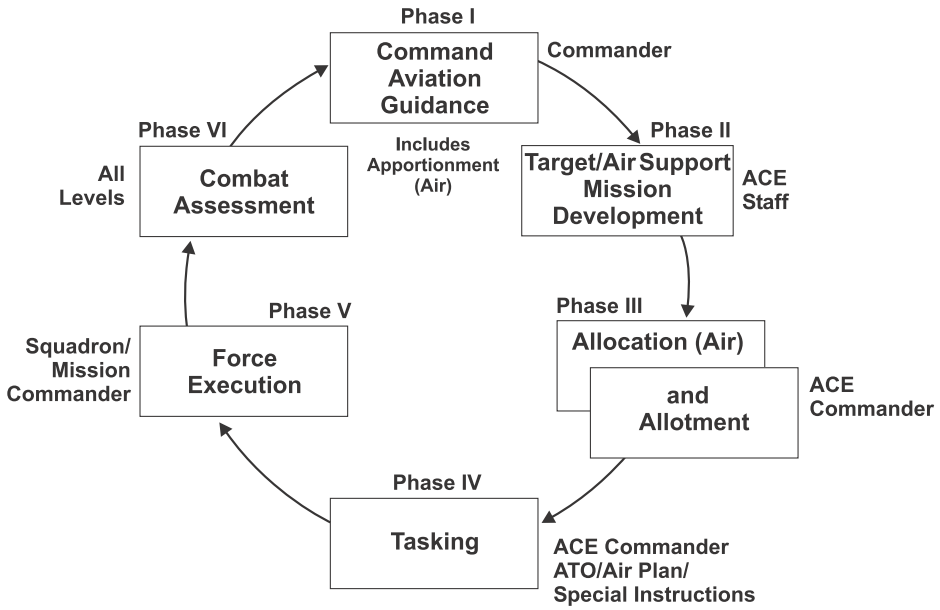


Figure 5-6. The Six-Phase Aviation Tasking Cycle.

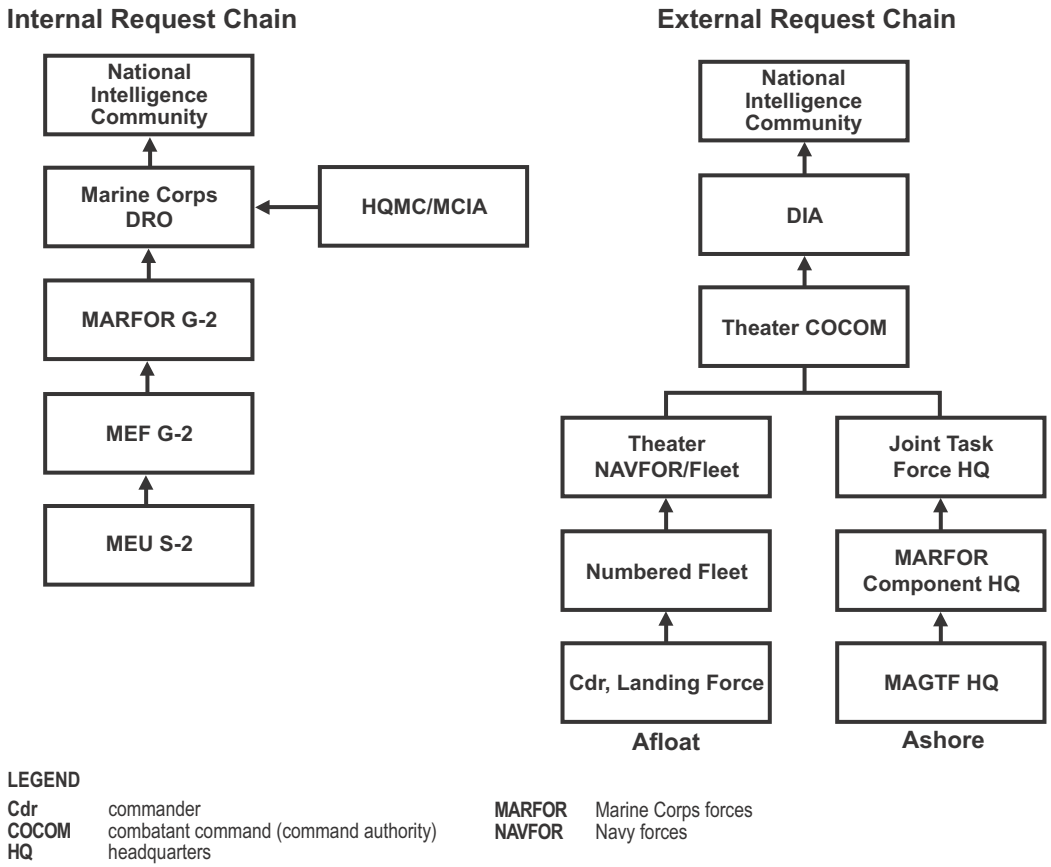


Figure 5-7. Requesting Imagery and Imagery Intelligence Support.

meaningful knowledge that can be used for decisionmaking. Exploitation involves the evaluation, interpretation, integration, analysis, and synthesis of all information that is relevant to a particular intelligence requirement in order to answer the question(s) that have been asked.

Imagery Derived Products. Imagery derived products are secondary products that can be used to facilitate disclosure and release to coalition partners. They are useful for a variety of planning and decisionmaking activities. Several of the most commonly requested products include the following:

- Beach studies.
- HLZ studies.
- Raid studies.

Imagery Intelligence Text Products. Imagery intelligence text products are selected to meet the specific needs of the commander. Appendix F provides the format and instructions for completing the basic IMINT reports described in the following subparagraphs.

Reconnaissance Exploitation Report. The RECCEXREP is used to report the results from the first rapid analysis of imagery, including the debriefing of the aircrew when possible. It addresses the targets requested in the original imagery collection mission tasking, normally with each target addressed separately. It is prepared by intelligence personnel, such as IIP, MAW, or MLG, based on input

from the supporting collecting unit's intelligence section. The report is then disseminated according to the dissemination plan. The SOP designates the specified time limit in which the RECCEXREP must be completed and disseminated.

Initial Photo Interpretation Report. The IPIR provides information regarding tasked imagery collection missions not previously reported (e.g., in the RECCEXREP), when extensive or detailed data from a systematic review of the imagery is required, or when the rapid response required by the RECCEXREP would be hindered by the format, size, or quality of the imagery involved. It also is prepared by the IIP—with input from the supporting collecting unit's intelligence section—and disseminated in accordance with the dissemination plan. The timeline for completing this report is in accordance with the unit SOP.

Supplemental Photographic Interpretation Report. The SUPIR provides information not previously included in a RECCEXREP or IPIR. It reports on significant targets covered by the mission and other required supplemental data. It is prepared by intelligence personnel (e.g., IIP, MAW, MLG) based on input from the supporting collecting unit's intelligence section. The report is then disseminated in accordance with the dissemination plan. The SOP designates the specified time limit in which the SUPIR must be completed and disseminated.

SALUTE Report. The standard SALUTE format is used to report any known or suspected enemy activity. It may also be used to report any characteristics of the AO that affect mission accomplishment. The SALUTE report may be used by a VMU, ground reconnaissance unit, aircrew, or other personnel to report key information obtained during ongoing imagery collection operations. It will be disseminated in accordance with the dissemination plan, generally from the collector to the SARC or directly from the collector to other supported units.

Imagery Intelligence Support to Other All-Source Intelligence Products. Imagery alone will provide useful intelligence to commanders and planners (see app. C). However, intelligence requirements usually will be satisfied more effectively and in greater detail via the complementary combination of an image and supporting IMINT or all-source intelligence products. Review appendix H for an appreciation of the greater intelligence value of a complementary imagery/intelligence report product, vice simply an image product. Target analysis and target material production are examples of such support.

Target Analysis. Generally, the imagery analyst's first responsibility is the detection and accurate identification of areas and activities for situation development and support to targeting. Target detection begins with either general or specific search modes.

General search is undertaken in response to requests for broad area intelligence and usually involves the analytical examination of the entire image. Such searches should be kept to a minimum.

Specific search is undertaken in response to an intelligence requirement that requires point, strip, or route reconnaissance imagery. Its scope and objectives are more limited than general search. Target identification consists of the interpretation of visual cues or distinctive features of targets/objects detected during collection. The distinctive features are analyzed using the six Ss: size, shape, shadow, shade, surroundings, and signal strength. The depth and scope of the analysis is

highly dependent upon the purpose of the analysis and the time constraints of the associated intelligence requirement. Target identification may include the following:

- Determining the OOB and BDAs of threat units and systems at different echelons.
- Identifying both equipment and its intended use by the threat forces.
- Determining the purpose and composition of ports, harbors, waterways, airfields, roadways, railways, and installations.
- Detecting and identifying non-threat forces and equipment and sensitive targets (e.g., religious facilities).

Target Material Production. In accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3505.01B, *Target Coordinate Mensuration Certification and Program Accreditation*, a number of imagery analysis specialists at each MEF, the MCIA, and other locations must be certified under an NGA-accredited program to perform precise point mensuration in support of coordinates-seeking weapons and other precision-guided munitions. During fiscal year 2012, III MEF and the MCIA became the first organizations to be certified in precise point mensuration. During fiscal year 2015, II MEF became certified through the Air Force Precise Point Positioning Program (AFP4). I MEF will be certified during fiscal years 2016, with full program implementation planned for fiscal year 2016.

See appendix I for information on target folders and IMINT support to these activities.

Dissemination and Reporting. Imagery intelligence dissemination planning and management involves establishing dissemination priorities, stipulating dissemination and reporting criteria, selecting dissemination means, and monitoring the flow of IMINT reporting. The goal of this process is to deliver IMINT products to the appropriate user in the proper format at the right time, while preventing the dissemination of irrelevant products and avoiding information overload. The following subparagraphs address the most common considerations for intelligence dissemination planners when developing IMINT dissemination plans.

Identify Dissemination Requirements. When identifying requirements, the four Ws—who, where, what, and when—are a good start for determining the broad scope of dissemination needs.

Who. Commander preferences, standing theater OPLAN/concept plans (CONPLANs), type mission analyses, unit SOPs, TTP, playbooks, and previous post-exercise analyses and lessons learned reports are all key sources for identifying organizations, units, and other elements to which the intelligence section must disseminate imagery and IMINT. Identifying and grouping by common imagery and IMINT product requirements by typical command relationship/task organization provides the operational perspective to begin dissemination planning. *Who* receives this imagery can either be internal or subordinate elements and units.

Internal MEF/MAGTF headquarters include a current operations center, future operations center, tactical command echelon (when deployed), force fires coordination center, rear area operations center (when established), civil-military operations center (when established). The subordinate elements and units include intelligence sections of the ground combat element, ACE, and LCE; other MAGTFs and independent task forces; organic/attached/direct support intelligence and

reconnaissance units over which the MEF retains operational control (via either the SARC, other G-2 sections, geospatial support team, and/or direct to the intelligence/reconnaissance units' command posts); and other C2 nodes and facilities, when required (e.g., DASC, enemy prisoners of war compound, rear area operations center, and/or airfield arrival control group).

Where. Generally, the answer to the *where* question will be the location of each identified *who*. However, command relationships, the specific operational phase, task organization, or other factors may identify additional answers to *where* requirements are to be disseminated.

What. With the above information in hand, dissemination planners seek answers to the *what* of each requirement. Here, planners strive to establish or anticipate what type intelligence support (e.g., finished intelligence, particular formats) each *who* typically requires to support his planning and decisionmaking needs. As with the *who* determinations, commander preferences, standing theater OPLAN/CONPLANs, type mission analyses, unit SOPs, TTP and playbooks, and previous post-exercise analyses and lessons learned reports will provide the dissemination SOP foundation and isolate the necessary information. Additionally, planners' research should encompass how differing intelligence resource task organizations affect such requirements and to how they historically have been combined to satisfy the *who* requirements. Cross-referencing the *who* and *what* answers with the following groupings completes this step:

- Typical standalone imagery and IMINT products and IMINT support to all-source intelligence products.
- Alarm intelligence support (e.g., I&W reports, time-sensitive target of opportunity reporting).
- Preferred level(s) of classified information that the *who* desires (further subdivided into what they require access to and what they can actually retain on hand).

When. The final dissemination planning information requirement is to determine to which organizations, units, and other elements (*who*) the intelligence section must disseminate imagery and IMINT or to define the stated *when*. The same sources used to research the previous Ws likewise are recommended for acquiring initial *when* answers and baseline planning criteria. However, this factor is arguably the most variable during tactical operations. Key planning considerations include the following:

- Nature of the requirement (e.g., is it a PIR or in support of another functional information requirement?).
- Rapidly assessing the feasibility of satisfying the decisionmaker's or planner's stated latest time intelligence is of value (LTIOV): Is intelligence already on-hand? Can organic assets acquire or produce needed intelligence? Will external support be needed?
- Communications and networks transmission requirements to support the desired format for the *who* (e.g., voice, text, digital, bulk delivery).
- Capabilities/current status of MAGTF CIS.

Develop Dissemination Plan. Once the four Ws have been completed, the answers can be translated into an IMINT dissemination plan. Imagery intelligence personnel must maintain close coordination with all G-2/S-2 officers, G-3/S-3 planners, and pertinent intelligence personnel at higher, adjacent, supporting, and subordinate organizations.

Design and Coordinate Architecture. The architecture should be designed schematically so that it depicts organizations, type intelligence systems, and CIS connectivity among the forces' (i.e., MAGTF, national, theater) intelligence collectors/producers and the supported decisionmakers/planners. Since planned architectures must incorporate sufficient flexibility to adjust quickly to changing tactical circumstances, it must depict both primary and alternate pipeline and alarm channels and the demand-pull and supply-push methodologies. The large data communications bandwidths associated with imagery dissemination require close planning and coordination between MAGTF intelligence and CIS planners. See appendix J for additional technical information on NITF compression that is useful when designing and coordinating CIS support to IMINT dissemination.

Establish Imagery Intelligence Dissemination Procedures. If intelligence dissemination is to be effective, comprehensive, MAGTF-wide integrated operations—CIS—intelligence procedures are mandatory. The answers to the four Ws will form the foundation on which the MEF's intelligence dissemination architecture and operations can be built.

Allocate or Obtain Resources. The G-2/S-2, in concert with the unit's CIS officer and G-3/S-3, should allocate available resources to accommodate dissemination of the requested IMINT. If resources do not exist to transmit the required information, a request for augmentation from higher headquarters or assistance from lateral units should be initiated immediately. It may be necessary to arrange for the delivery of intelligence directly from the producer to the requester if means are in place.

Coordinate. Once IMINT requirements have been identified and the initial plans developed, planners should develop and coordinate detailed dissemination plans.

Monitor Execution. Following the dissemination of imagery or IMINT products to the requester, it is important to evaluate the flow of information to determine whether or not the user is satisfied with the quantity and quality of intelligence and to ensure that preplanned filters are eliminating circular reporting. Frequent checks with the requestor can ensure intelligence utilization and preclude unanticipated demands on the G-2/S-2 staff.

Imagery Intelligence Utilization. The specific utilization of IMINT is based upon the CONOPS and the imagery application being employed. Commanders, G-2/S-2s, and G-3/S-3s must evaluate IMINT products and reports continuously for timeliness, usefulness, overall quality, and responsiveness to stated PIRs and intelligence requirements. Additionally, evaluators should provide feedback to the MAGTF G-2/S-2 and IMINT planners to improve future IMINT operations.

Imagery Intelligence Operations Appendix. Guidance for conducting IMINT operations comes from many sources. The DIA and the NGA issue policies, direction, guidance, and instructions regarding compliance with national IMINT standards, architectures, and request procedures. Deployed MAGTFs may also need to reference pertinent combatant, joint force, and fleet orders, guidance, and IMINT. Tactics, techniques, and procedures are necessary to identify unique operating concepts, methodologies, support procedures, and formats. Marine IMINT plans and orders are prepared by the G-2/S-2 (under the staff lead of the ISC and with the assistance of the other G-2 section and intelligence staff officers and commanders) and the commanding officers/OICs of the supporting IMINT units. The MAGTF IMINT plans and orders appear as appendix 7

of the intelligence annex of the MAGTF OPLAN or OPORD and will focus on internal MAGTF IMINT requirements, operations, and TTP.

Appendix 7 (Imagery Intelligence) to Annex B (Intelligence) to an OPLAN or OPORD will provide detailed planning and direction for conducting MAGTF IMINT operations. The ISC is responsible for its development. It should be prepared consistently with the format outlined in the Joint Operation Planning and Execution System, tailored as necessary to remain consistent with the situation and the particular needs of the MAGTF (see app. K for a sample IMINT operations appendix format). The IMINT operations appendix should include friendly IMINT forces to be used, and the following:

- Personnel augmentation requirements.
- IMINT units of adjacent or other theater forces and support expected.
- Joint force maritime component commander and naval task force/amphibious force IMINT elements that provide support to the landing force in amphibious operations.
- Pertinent IMINT capabilities and support from the JTF headquarters, combatant command's JIOC, and other component commanders/task forces within JTF operations.
- Planned arrangement and employment of external IMINT support, including special collection, production, dissemination, and CIS.
- Establishment of coordinating instructions for the planning and control of IMINT operations, including the technical support expected from higher headquarters.
- Tasking of MAGTF IMINT elements.
- IMINT production, priorities, and plans.
- IMINT dissemination priorities and plans, including CIS support to the MAGTF IMINT effort.
- Equipment/logistic requirements unique to IMINT.

Imagery Intelligence Planning Considerations in Other Portions of Annex B. The following are other portions of annex B (in addition to appendix 7) where IMINT is incorporated:

- Appendix 11 (Intelligence Estimate). The format for the intelligence estimate is found in appendix A of MCWP 2-3, *MAGTF Intelligence Production and Analysis*.
- Appendix 14 (Reconnaissance and Surveillance Plan):
  - Tab C (Unmanned Aircraft System Plan) (see app. L).
  - Tab D (Aerial Imagery Plan) (see app. M).
- Appendix 16 (Intelligence Operations Plan):
  - Tab A (Intelligence Collections Plan). The format for the intelligence collection plan is contained in appendix C of MCWP 2-2, *MAGTF Intelligence Collection*.
  - Tab B (Intelligence Production Plan). The format for this plan is found in MCWP 2-3.
  - Tab C (Intelligence Dissemination Plan). The format for this plan is found in MCWP 2-4, *Marine Air-Ground Task Force Intelligence Dissemination*.

  - Tab D (Intelligence Communications). The format for this tab is found in MCWP 2-4.
  - Tab E (Intelligence Reports). The format for this tab is found in MCWP 2-3.
- Appendix 17 (Support to Survival, Evasion, Resistance, and Escape—SERE).

CHAPTER 6
TRAINING

The HQMC-Imagery and Geospatial Intelligence Branch—through the Training and Education Command and Marine Corps Intelligence Schools Command—is responsible for implementing and maintaining GEOINT training and education programs. Unit training plans should cover imagery, imagery platforms and sensors, GEOINT data types, post-processing techniques, collections, software, hardware, established and emerging dissemination techniques, production management, and full spectrum geospatial intelligence.

IMAGERY TRAINING

The leadership within each imagery, FMV, and MTI section is responsible to both the Marine Corps Intelligence 0241 occupational field and unit commanding officer for implementing training requirements.

Requirements

Initial training for all IMINT specialists (MOS 0241) is conducted via the tactical imagery analysis course, which is operationally supported by The National Geospatial-Intelligence College located at Fort Belvoir, Virginia. Administrative support for the tactical imagery analysis course is provided by the Marine detachment, Fort Belvoir and Marine Corps Intelligence School. The HQMC-Intelligence Manpower and Training Branch, in conjunction with the occupational field monitor and sponsor, manages student assignments to the operating forces as well as orders to many of the follow-on and advanced training courses.

Training Objectives

Entry-level, intermediate, and advanced training for MAGTF IMINT specialists should include—

- Joint and Marine Corps GEOINT doctrine.
- IC, DOD, and Marine Corps intelligence structure and policies.
- FMV platforms, sensors, and exploitation systems.
- MTI platforms, sensors, and exploitation systems.
- Strategic, theater, organic, and commercial imagery platforms and sensors.
- DOD and Marine Corps imagery exploitation networks, systems, hardware, and software, as well as basic system administration.
- Identification of tactical orders-of-battle.
- Report writing and dissemination systems.
- Support to MAGTF through imagery and IMINT products.

- Exploitation techniques to extract EEIs.
- Tools for discovery, retrieval, and exploitation of imagery and geospatial data.
- Littoral studies in support of amphibious operations.
- LZ studies in support of fixed- and rotary-wing MAGTF assets.
- LOC studies in support of MAGTF assets.
- JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*.
- Research of intelligence and information.
- GEOINT collaboration with GIS and METOC elements of the MAGTF.

Planning and Employment Training

Planning and employment training is essential to preparing the IMINT specialist for intelligence operations in support of the MAGTF. This training provides—

- Familiarity with the nuances of setting up and configuring equipment for use on classified networks.
- Firsthand experience operating within the systems' constraints created by an expeditionary environment.
- Understanding of when and how to adjust production workflows in order to fulfill the MAGTF commander's intelligence requirements.

System Administration Training. During the tactical imagery analysis course, Marines receive basic system administration training on the TEG FoS. Subsequent formal/managed on-the-job training (MOJT) is needed to ensure analysts have a working knowledge of equipment set up, configuration, utilization, and tear down in austere environments. Each unit should establish its own training cycle to develop and enhance system administration proficiency.

Maintenance Training. Organizational level maintenance of imagery exploitation hardware and software enables the analyst to ensure the unhindered continuation of production workflows and dissemination of completed IMINT studies when systems experience technical difficulties. A significant number of interruptions to the intelligence cycle can be mitigated through user-level familiarity with hardware and software, because the analyst will not need to consult maintenance echelons for assistance. User-level troubleshooting should include a general emphasis on finding alternate means of gathering data and exploiting and disseminating imagery and IMINT studies when primary methods are unavailable.

Database Management Training. Imagery production elements require significant amounts of storage space on local and network servers. The proper management of these storage elements—including directory structure, proper data archive, and production workflows—ensures production cycles are not hindered by server failures and assists in federated production and collaboration through centrally located and properly managed working files.

MAGTF Training

Imagery and IMINT production is incorporated into all MAGTF training. During training exercises, imagery operations should be conducted under a variety of C2 support relationships to improve organizational and employment flexibility. Repeated exposure to imagery capabilities

and employment strategies will enhance the MAGTF's ability to use imagery and IMINT effectively to increase situational awareness and shape operations.

Command Post Exercise/Staff Exercise. The production and use of imagery should be included in every exercise. Training exercises should emphasize the planning of imagery support requirements and production procedures, the dissemination of imagery within MAGTF Marine Corps enterprise network systems, and the use of imagery within the MCPP. The unit intelligence officer should use the planning cycle and develop a realistic imagery production plan. Imagery intelligence analysts should be assigned to the exercise control group in order to validate the planning and production plan and to simulate the dissemination of mission-specific data from national and theater production facilities.

Field Training Exercise. Field training exercises may be used to introduce IMINT analysts to exploitation procedures within the MAGTF IOC. Additionally, a field training exercise provides an operational context in which to integrate, intensify, produce, and disseminate tailored mission-specific data sets in support of C2, intelligence, fire support, aviation, logistic, and maneuver operations. The imagery section should coordinate with staffs and units at all echelons of command. Interaction helps to increase the supported organization's understanding of imagery in general and the capabilities afforded by imagery and IMINT.

TRAINING COURSES

Basic- and advanced-level imagery training programs are available at National Geospatial-Intelligence Agency College. Alternative education imagery programs include correspondence courses, distance courses, and contractor or vendor supported training.

Basic-Level: Tactical Imagery Analysis Course

Active duty students in the tactical imagery analysis course are traditionally sergeants or senior corporals. Reservists are typically privates through sergeants. The tactical imagery analysis course is divided into 10 annexes and spans 91 training days (approximately 5 months). Each annex includes multiple graded events and ends with a comprehensive phase completion exercise during which students employ all skills taught within that annex as follows:

- Annex A: information assurance, classification procedures, intelligence doctrine, operations, maps/charts, intelligence writing, and impromptu briefing.
- Annex B: principles of imagery interpretation, sensor phenomenology, imagery platforms, the ATO, and collections.
- Annex C: identification of orders of battle and facilities.
- Annex D: research techniques and tools, use of software for production, symbology, and cross-referencing geographic locations between various data sources.
- Annex E: production techniques for extracting, analyzing, and annotating completed intelligence studies.
- Annex F: an introduction to full spectrum GEOINT and critical thinking.

- Annex G: dissemination methods.
- Annex H: imagery reports and briefs.
- Annex I: setup, basic systems administration, and teardown of the current imagery exploitation workstation.
- Annex J: the capstone exercise to familiarize the students with operating in a MAGTF IOC.

Intermediate- and Advanced-Level Training

Intermediate- and advanced-level training is available in various skill areas by multiple government and nongovernment entities. Unit training managers should determine the most effective method of training for ensuring that IMINT analysts are properly prepared to meet mission requirements.

Government and Nongovernment Training Sources. The following list contains government and nongovernment training sources:

- Federal agencies.
- DOD agencies.
- Services.
- Corporations.
- Base education centers.
- Colleges and universities.

Delivery Methods for Training. The following list contains delivery methods for training:

- Resident courses/formal schools.
- Primer courses.
- Mobile training teams.
- Computer-based training.
- Web-based training.
- Distance courses.
- MOJT.

Training Considerations. Since the majority of follow-on training is provided by organizations outside of the Marine Corps, leadership of imagery sections must ensure that their analysts are able to integrate these tactics and techniques into the MAGTF mission using existing methods while following established or emerging Marine Corps intelligence doctrine and operational concepts. Training managers are also responsible for ensuring that the knowledge and experience gained through training supports the unit mission and the Marine Corps mission by considering the following:

- Special hardware or software to make use of advanced exploitation techniques.
- Classification and releasability.

Training Entities. Creative utilization of available training resources ensures the individual analyst, unit, and occupational field are prepared to support the MAGTF mission. Funding and unit mission should be carefully scrutinized and training managers should ensure training dollars are spent on the most qualified and deserving analysts. Training is available from the following resources:

- National Geospatial-Intelligence Agency College.
- Joint Intelligence Virtual University.
- National Defense Intelligence College.
- Software vendors.
- Hardware vendors.

Follow-On Training Subject Areas

The subject areas discussed in the following subparagraphs should be considered essential to the continued development of individual analysts and MOS 0241 by training managers.

Marine Corps and Joint Intelligence Doctrine. Doctrine provides analysts with an established reference for joint and MAGTF procedures and operations; moreover, knowledge of doctrine prepares the analyst to anticipate the MAGTF commander's needs. This doctrine facilitates greater speed and focus of analytical effort and, when coupled with knowledge of the enemy, facilitates predictive analysis.

Intelligence Writing. The ability to communicate the numerous pieces of information and intelligence on written reports is a skill needed by all intelligence analysts. Completed imagery and IMINT studies can often be difficult to disseminate due to network constraints and may need to be supplemented by textual reports.

Imagery and Imagery Intelligence Production. Repetition provides analysts with an intimate working knowledge of production techniques, procedures, timelines, software operation, and hardware operation; builds analytical efficiency; and equips analysts with the necessary skills to operate autonomously. Unit training events, MOJT, exercises, and real world production scenarios should be utilized to develop the analytical processes that consistently produce the necessary results, as well as develop the analytical mind that can effectively advise the MAGTF commander on proper utilization of imagery production assets.

Imagery, Imagery Intelligence, and Geospatial Intelligence Data. Imagery intelligence analysts need a thorough knowledge of the differences in data types, uses, and special handling issues. This knowledge enables analysts to integrate other data sets quickly into production workflows and generate IMINT and GEOINT products and reports in support of operations. Analysts should be familiar with software operating files, hardware operating files, imagery files, and the differences between each; post-processed data file types; and any other files they will commonly utilize in accomplishment of the mission.

Imagery, Imagery Intelligence, and Geospatial Intelligence Databases. The proper storage of both raw data and finished intelligence products is essential. Analysts must be able to configure servers

properly for use on exploitation networks, manually and semi-manually store information and IMINT studies, and archive data.

Spectral Exploitation and Spectral Systems. Basic and advanced training in analysis of spectral data is designed to provide students with a deeper understanding of spectral imagery processing as well as literal and nonliteral spectral imagery analysis techniques. Multispectral and hyperspectral imagery exploitation and processing techniques should be covered. Familiarity with essential software and plug-ins for exploitation are also essential to exploitation.

Commercial Imagery. Marines must understand proper copyright procedures, as well as how licensing affects the dissemination of commercial imagery and data outside of licensed users. This knowledge impacts the ability of the Marine Corps to do the following:

- Share data with various governments, agencies, nongovernmental organizations, and personnel during MAGTF operations, which can often be hindered by security classifications.
- Research, retrieve, properly exploit, and disseminate commercial data available to DOD entities, which is essential to these operations.

Airborne Imagery. The understanding of strategic, theater, and tactical airborne platforms, sensors, and data, as well as how to gain access to airborne libraries greatly increases the data available to the imagery analyst for exploitation.

Motion Imagery. Reliance on FMV for persistent ISR has continued to grow within the Marine Corps and DOD. Knowledge of UASs and their associated systems provides analysts with the necessary skills to manage the tasking, processing, exploitation, and dissemination process.

Moving Target Indicator. Training in the use of MTI data and systems to support the MAGTF is accomplished via formal schooling. Basic analysts should possess familiarity with raw MTI data, exploitation hardware and software, completed products, and processes in order to facilitate collaboration.

Synthetic Aperture Radar. Training in the use of MTI data and systems to support the MAGTF is accomplished via intermediate training based at a government facility or provided directly to the unit. The MTI operator training course will supply MOSs 0231 and 0241 with MTI fundamentals, hardware and software setup and configuration, exploitation tools, product development, and various MTI support missions.

Advanced Phenomenologies and Imagery Techniques. Formal training in the software, techniques, and releasability of thermal infrared imagery, polarimetric imagery, and overhead persistent infrared is essential to ensuring analysts can seamlessly integrate solutions into MAGTF intelligence problems. Familiarity with essential software and plug-ins for exploitation is also essential to exploitation.

Foreign Disclosure. Marines must be familiar with foreign disclosure procedures. Military information is a national security asset that must be conserved and protected. It may be shared with foreign representatives only when there is a clearly defined advantage to the United States.

Only designated foreign disclosure officers may approve of the disclosure of classified and controlled unclassified military information to foreign representatives. The Secretary of the Navy Manual, *Department of the Navy Foreign Disclosure Manual*, and MCO 5510.20B, *Disclosure of Military Information to Foreign Governments and Interests*, are two of the many references which should be reviewed and understood.

Imagery Classification Marking. While it is important that the public be informed concerning the activities of its government, certain information concerning the national defense and foreign relations must be protected against unauthorized disclosure. This information is called national security information and is classified if its disclosure might cause damage to the nation's security. Marines must be aware of the rules regarding classification of the imagery products they produce as well as those produced by other courses. Executive Order 13526, *Classified National Security Information*, and Executive Order 12951, *Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems*, are just two of the references on classified material.

Full Spectrum Geospatial Intelligence. Full spectrum geospatial intelligence, also known as imagery-derived MASINT, includes all types of information technically derived from the processing, exploitation, and nonliteral analysis (including integration or fusion) of spectral, spatial, temporal, radiometric, phase history, and polarimetric data. These types of data can be collected on both stationary and moving targets by electro-optical, infrared, radar, and related sensor programs (both active and passive).

APPENDIX A
IMAGING SENSORS

This appendix describes the basic capabilities and limitations of EO, radar, and infrared imagery sensors.

OPTICAL SENSORS

Optical sensors detect and record electromagnetic radiation within the visible light and near-infrared portions of the electromagnetic spectrum. The operating principles are the same as those of a common digital camera. There are three types of optical imaging systems: vertical, oblique, and panoramic.

Vertical

The optical axis of the sensor is approximately perpendicular to the surface of the earth (see fig. A-1). Vertical imagery is ideal for performing terrain analysis, beach studies, and HLZ studies.

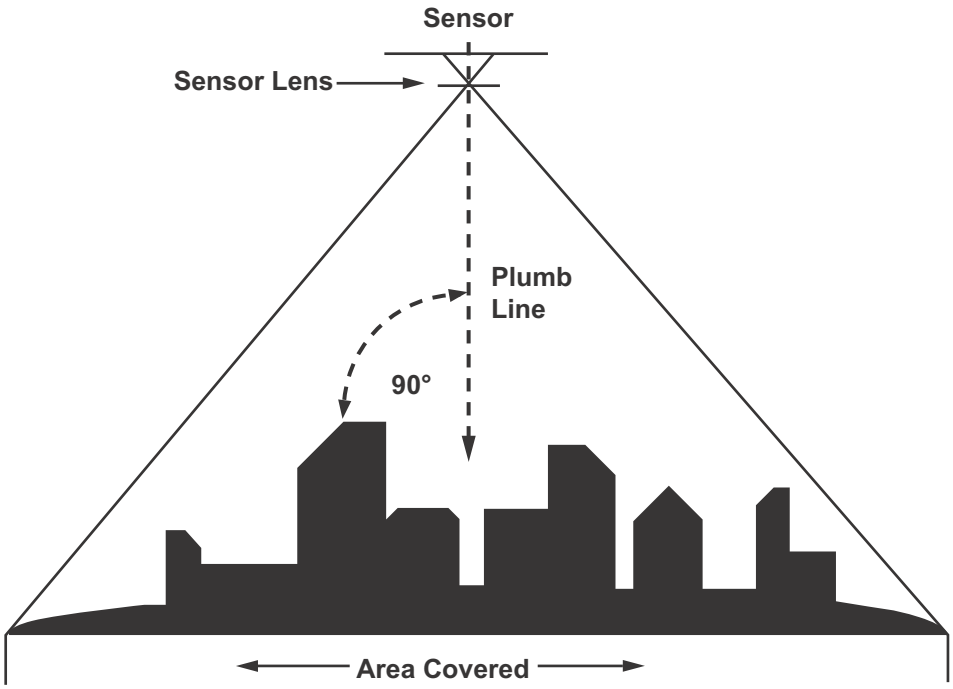


Figure A-1. Vertical Optical Sensor and Ground Relationship.

Oblique

Oblique imagery is obtained by imaging the ground at an angle to the vertical and requires oblique metrics. The optical axis of the sensor is intentionally directed between the horizontal and the vertical. This axis can provide left or right oblique coverage and is ideal for observation at canopy baseline as well.

There are two standard types of oblique imagery: high and low. High oblique imagery will include the horizon (see fig. A-2), while low oblique imagery will not (see fig. A-3). Because of the angle, high oblique imagery covers a larger area than low oblique. Oblique imagery is referred to as left or right oblique or forward looking, based on the look angle in relation to the platform.

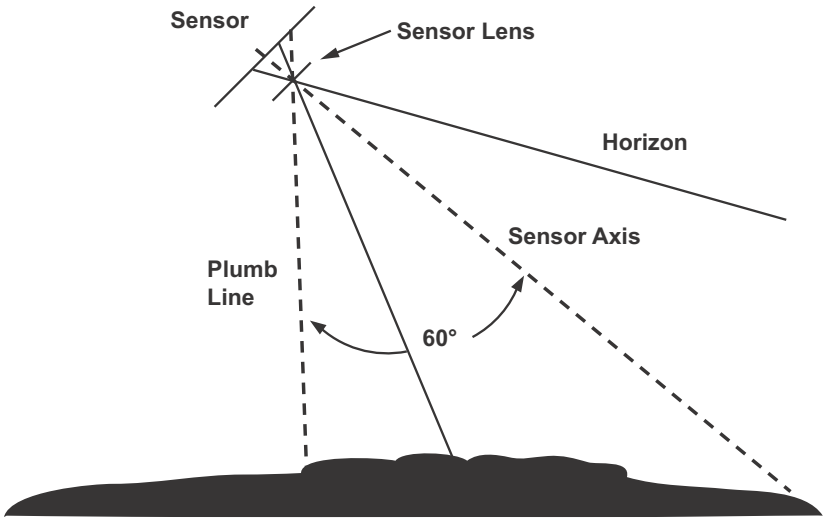


Figure A-2. High Oblique Sensor to Ground Relationship.

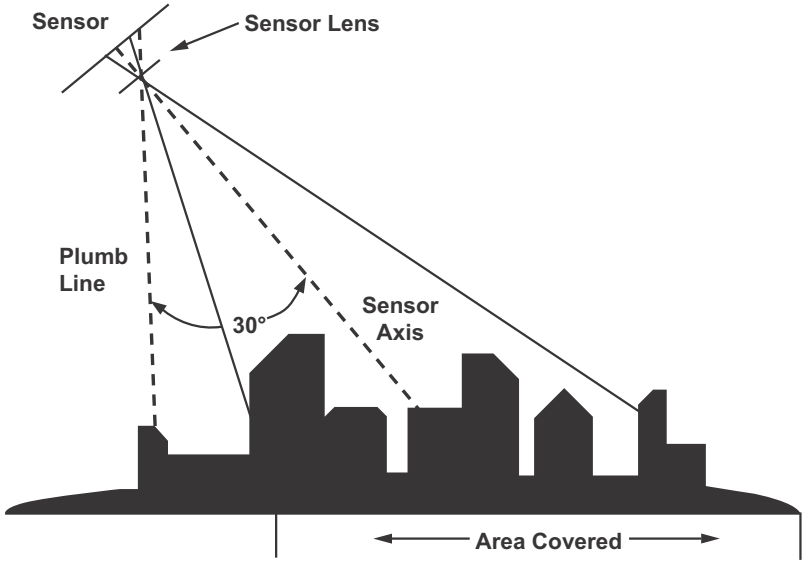


Figure A-3. Low Oblique Sensor to Ground Relationship.

Panoramic

Panoramic imagery is taken with a special sensor that scans a wide area. The optical axis of the sensor uses a system of optics that can scan an area from 0 to 180 degrees. There are two types of panoramic imagery: low and high. Low panoramic imagery is taken at low altitudes and scans a wide angle that includes the horizon at either side of the aircraft flight path (see fig. A-4).

High panoramic imagery is taken at high altitudes with a narrow scan angle (see fig. A-5). The horizon is not normally visible on high panoramic imagery.

In only one pass over the target area, panoramic photography provides coverage of large areas of terrain on both sides of the aircraft flight path. Although it provides both vertical and oblique views of the image area, it is the most difficult and time-consuming photography to analyze and measure due to the distortion of the recorded image. Table A-1, on page A-4, summarizes both the advantages and disadvantages of each type of imaging system.

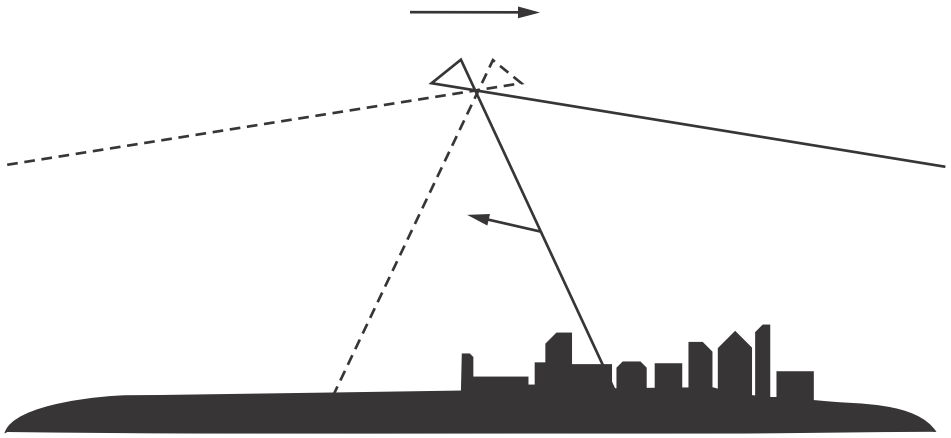


Figure A-4. Low Panoramic Imagery.

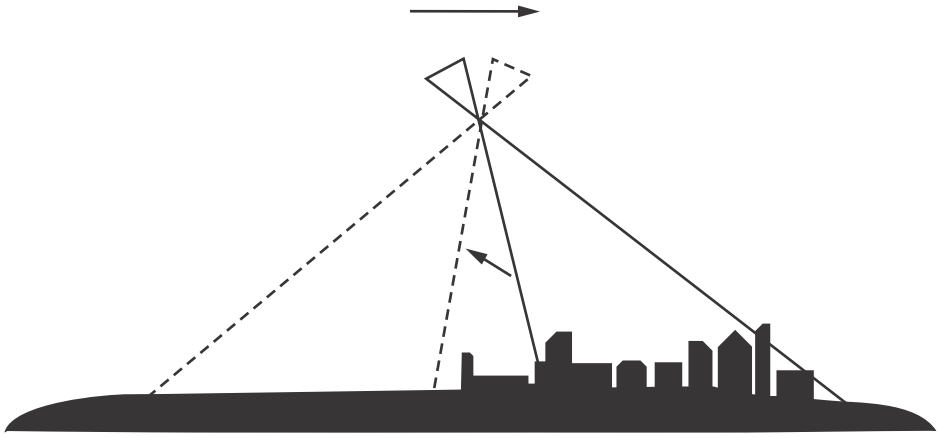


Figure A-5. High Panoramic Imagery.

Table A-1. Optical Sensor Advantages and Disadvantage.

Sensor System	Advantages	Disadvantages
Vertical	Provides fairly constant scale Can construct mosaics Obtains accurate measurements Allows stereographic viewing Allows for accurate interpretation	Flight path is directly over the target Covered objects cannot be viewed View angle is unnatural It is susceptible to flight restrictions
Oblique	Provides large area coverage Provides natural view Offsets flight path from target Allows for covered objects viewing, due to angle	Terrain masking Scale varies Measurements are difficult
Panoramic	Provides large area coverage Satisfies both vertical and oblique mission requirements	Scale varies Platform has limited standoff capability Measurements are difficult

The capabilities of optical sensors are as follows:

- They produce high-quality photographs (good resolution).
- They are a passive system, which cannot be detected or jammed.
- Their sensors offer flexibility.

The limitations of optical sensors are as follows:

- They require a light source.
- They are hampered during periods of reduced visibility.
- They are LOS dependent.

Radar

Radar is an active sensing technique that detects and records differences in reflected electromagnetic energy. The capabilities of radar are as follows:

- It can be used for day and night operations.
- It provides all-weather capability.
- It provides constant scale and resolution.
- It provides standoff capability.

The limitations of radar are as follows:

- It provides poor resolution.
- It is an active system, which can be detected or jammed.
- It is LOS dependent.

Infrared

Infrared sensors detect and record electromagnetic radiation that is emitted from a given target surface in the infrared portion of the electromagnetic spectrum. The capabilities of infrared are as follows:

- It can be used for day and night operations.
- It is a passive system, which cannot be detected or jammed.
- It detects camouflaged equipment and activity.

The limitations of infrared are as follows:

- It offers poor resolution, when compared to EO imagery.
- It is susceptible to adversary deception.
- It is not all-weather; it is hampered by such disturbances as rain, snow, or hail.
- It is LOS dependent.

APPENDIX B
IMAGERY AND SUPPORTING INTELLIGENCE REPORTS

This appendix provides examples of MAGTF intelligence products that are derived from the fusion of available imagery. Such products support IMINT and all-source intelligence reports, tactical planning, and decisionmaking. The examples and formulas in this appendix are provided to aid in the preparation of imagery and supporting intelligence products and studies. They are meant to be used as general guides for these types of products and not to replace or supersede any products being developed in accordance with local SOPs. Additionally, the MCIA maintains a set of instructions distributed across the Marine Corps for imagery analysts including all of the material provided herein.

Examples of imagery products included in this publication are as follow:

- Image and supporting intelligence report for the military operations on urbanized terrain (MOUT) facility, Camp Lejeune, North Carolina.
- Image and supporting intelligence report for the Marine Corps Air Station, New River, North Carolina.
- Image and supporting intelligence report for HLZ Vulture, Camp Lejeune, North Carolina. Image and supporting intelligence report for Onslow Beach North, Camp Lejeune, North Carolina.
- Image and supporting intelligence report for Kin Red Beach, Okinawa, Japan.

Legend for Appendix B:
DMA–Defense Mapping Agency
GEO–geographic coordinate
JLOTS–joint logistics over-the-shore
LCAC –landing craft air cushion
MIM–military installation map
MPF–maritime prepositioning force
NAD–North American datum
nm–nautical miles
No–number
OP-2–Outpost 2
RO/RO–roll on/roll off
STD–standard
WGS–World Geodetic System

Urban Imagery Product Example: Image and Supporting Intelligence Report for the Military Operations on Urbanized Terrain Facility, Camp Lejeune, North Carolina

Center Coordinates
UTM: 18STD93843838
GEO: 343959N0771459W

Size
Length: 1,025 ft (312 m)
Width: 800 ft (244 m)

Surface Material
Silty sand
Gravel

Map Reference
Sheet: Camp Lejeune MIM
Series: V742S
Edition: 2-DMA
Datum: NAD 83/WGS 84

Remarks
The MOUT facility is located approximately 2 km east-north-east of OP-2. The primary use of the MOUT facility is combat training in an urban environment. The MOUT facility consists of 31 buildings of varying sizes and shapes. Roof types are a mixture of garbled and flat. The facility is surrounded by trees of varying heights. The exit from the MOUT facility is a loose surface road which provides access to Lyman Road.

Note: All building measurements are listed as length x width x height.

Exits

Anno. #	Type	True Bearing	Distance	Width	Surface Material
E1	Road, loose-surfaced	146	169.8 m (557 ft)	7.6 m (25 ft)	Earth and sand
E2	Road, loose-surfaced	175	163.1 m (535 ft)	6.4 m (21 ft)	Earth and sand
E3	Road, loose-surfaced	181	165.0 m (541 ft)	6.7 m (22 ft)	Earth and sand
E4	Road, loose-surfaced	281	204.3 m (670 ft)	5.6 m (18 ft)	Earth and sand

Descriptions of the buildings shown in figure B-1 are as follows:

B1. Three-story, 120 ft x 58 ft x 37 ft (37 m x 18 m x 11 m), T-shaped building (hotel), with near-flat roof. A helicopter landing point (LP) is painted with non-reflective white airfield markings and consists of a concrete slab roof. The helicopter landing point is 38 ft x 33 ft (12 m x 10 m). The building's roof is outlined by a parapet with scuppers and a gutter. (A scupper is an opening in the wall of a building through which water can drain). The front portion of the roof consists of tube trusses or transverse monitors. Grappling and rappelling anchors are located at points throughout the roof.

B2. Two-story, 72 ft x 60 ft x 31 ft (22 m x 18 m x 9 m), square-shaped building (city hall), consisting of a near-flat roof outlined by a parapet; however, the northwest corner is lower than the main roof. The roof has grappling and rappelling anchors at points throughout the roof. The corner of the roof is open to a crawl space.

B3, B4. Two-story, crescent-shaped buildings (apartments), with an outer edge measuring 121 ft x 60 ft x 31 ft (37 m x 18 m x 9 m), and an inner edge measuring 84 ft x 60 ft x 31 ft (26 m x 18 m x 9 m), outlined by a parapet with scuppers. Grappling and rappelling anchors are located at points throughout the roofs. The roofs are near flat with a ridge dissecting each building, and a near-flat roof dissected by a ridge separates the two buildings.

B5. Three-story, 72 ft x 36 ft x 38 ft (22 m x 11 m x 12 m), quasi-rectangular-shaped building (office). Grappling and rappelling anchors located on the southeast and northwest sides of roof. The southern end of the building is two stories, 23 ft (7 m) high. An elevator shaft is located in the center of the roof.

B6. Two-story, 44 ft x 36 ft x 25 ft (13 m x 11 m x 8 m), L-shaped building (office). The northwest portion of the roof is a concrete slab.

B7. Rectangular, 121 ft x 73 ft x 77 ft (37 x 22 x 23 m), T-shaped building with dormers (church) with a gable roof made of asphalt and fiberglass shingles. The height of the main building is 48 ft (15 m), the steeple is 29 ft (9 m).

B8. Three-story, 53 ft x 34 ft x 39 ft (16 m x 10 m x 12 m), irregular-shaped building (business/residential) with near-flat roof. Grappling and rappelling anchors are located at points throughout the roof.

B9. Three-story, 50 ft x 47 ft x 39 ft (15 m x 14 m x 12 m), irregular-shaped building (business/residential) with near-flat roof.

B10. Single-story, 128 ft x 46 ft x 18 ft (39 m x 14 m x 5 m), rectangular-shaped building (business/residential) with flat roof.

B11. Two-story, 103 ft x 53 ft x 30 ft (31 m x 16 m x 9 m), rectangular-shaped building (townhouse) that has a gable roof with a dormer. The roof consists of fiberglass shingles reinforced by wooden trusses.

B12. Two-story, 103 ft x 53 ft x 30 ft (31 m x 16 m x 9 m), rectangular-shaped building (townhouse). The front and rear portions of the building's walls are incomplete. It has a gable-roofed dormer with fiberglass shingles and reinforced wooden trusses.

B13, B14. Two-story, 103 ft x 53 ft x 30 ft (31 m x 16 m x 9 m), rectangular-shaped buildings (townhouses) with gable roof and dormers. The roof consists of fiberglass shingles reinforced with wooden trusses.

B15. Two-story, 88 ft x 73 ft x 25 ft (27 m x 22 m x 18 m), irregular-shaped building (school) with near-flat roof built on a 2-inch slab of concrete. Rappelling anchors are located at points throughout the roof. Two fire escape ladders are located on the northeast and southwest sides of the roof.

B16. Two-story, 128 ft x 74 ft x 25 ft (38 m x 23 m x 8 m), irregular-shaped building (gymnasium) with a near flat roof. Fire escape ladders are located on the south side of the building.

B17. Two-story, 43 ft x 36 ft x 26 ft (13 m x 11 m x 8 m), square-shaped building (retail bank) with a near-flat roof. Grappling anchors located at points throughout the roof. Roof access by ladder is located on the northwest corner of the building.

B18. Single-story, 74 ft x 32 ft x 17 ft (23 x 10 x 5 m), quasi-rectangular-shaped building with hipped roofs (service stations).

B19. Single-story, 63 ft x 43 ft x 23 ft (19 m x 13 m x 7 m), rectangular-shaped building (warehouse) with a near-flat roof. The roof consists of standing seam metal on metal purloins. (Purloins are horizontal timbers supporting the rafters of a roof.)

B20. Single-story, 83 ft x 63 ft x 25 ft (25 m x 19 m x 8 m), square-shaped building (warehouse) with a near-flat roof on metal purloins and a mezzanine. (A mezzanine is an intermediate floor between two main floors of a building.)

B21, B22. Single-story, 52 ft x 40 ft x 15 ft (16 m x 12 m x 5 m), T-shaped buildings with basements (residential). The gable-style roof is reinforced with wooden trusses. The chimney height extends 2 ft (.6 m) above the peak of the roof.

B23, B24, B26. Single-story, 52 ft x 40 ft x 15 ft (16 m x 12 m x 5 m), T-shaped buildings (residential) with gable style roof reinforced with wood trusses. Chimney extends 2 ft (.6 m) above peak.

B25. Residential, 52 ft x 40 ft x 15 ft (16 m x 12 m x 5 m), irregular-shaped building with a gable-style roof reinforced with wood trusses.

B27, B28. Single-story, 44 ft x 40 ft x 17 ft (13 m x 12 m x 5 m), T-shaped buildings (residential) with reinforced wooden trusses. The gable roofing consists of fiberglass shingles.

B29, B30. Small, 44 ft x 40 ft x varies (13 m x 12 m x varies), T-shaped buildings, nearly destroyed; may provide some shelter from direct fire.

Airfield Product Example: Image and Supporting Intelligence Report for the Marine Corps Air Station, New River, North Carolina

Center Coordinates
UTM: 18STD76354355
GEO:
344233N0772631W
Elevation: 25 ft (8 m)

Map Reference
Sheet: Camp Lejeune
MIM
Series: V742S
Edition: 2-DMA

Runways

No.	Magnetic Bearing	Length	Width	Surface Material	Capability
R1	50/230	5,098 ft (1,554 m)	150 ft (46 m)	Asphalt	C-141
R2	10/190	5,075 ft (1,547 m)	150 ft (46 m)	Asphalt	C-130

Taxiways

No.	Length	Width	Surface Material	Type	Remarks
T1	775 ft (236 m)	25 ft (8 m)	Asphalt	Link	Connects to P4 to R1 and R2
T2	1,850 ft (564 m)	38 ft (11 m)	Asphalt	Link	Connects R1 and R2 to T3
T3	3,500 ft (1,066 m)	107 ft (33 m)	Asphalt	Link	Connects R1 and R2 to P3
T4	718 ft (219 m)	55 ft (17 m)	Asphalt	Link	Connects R1 to P2
T5	2,500 ft (762 m)	53 ft (16 m)	Asphalt	Link	Connects P2 to P3 and P4

Parking Areas

No.	Length	Width	Surface Material
P1	582 ft (177 m)	263 ft (80 m)	Concrete
P2	1,328 ft (405 m)	894 ft (272 m)	Concrete
P3	1,388 ft (423 m)	973 ft (297 m)	Concrete
P4	3,144 ft (958 m)	1,222 ft (372 m)	Concrete

Remarks

Marine Corps Air Station, New River is bordered on the east by New River and on the southwest by Southwest Creek. Trees and buildings of various heights surround the airfield.

Helicopter Landing Zone Study Example: Image and Supporting Intelligence Report for Helicopter Landing Zone Vulture, Camp Lejeune, North Carolina

Center Coordinates
UTM: 18STD76123004
GEO: 343516N0772627W

Map Reference
Sheet: Camp Lejeune MIM
Series: V742S
Edition: 2-DMA
Datum: NAD 83/WGS 84

HLZ Shape	HLZ Type	Surface Material	HLZ Size
Irregular	Open Field	Scrub Grass	Length: 1,209 ft (369 m) Width: 215 ft (66 m)

Exits

No.	Type	Distance and Grid Azimuth from HLZ Center	Width
E1	Loose surface road	182 ft (55 m) 280°	20 ft (6 m)

Flight Hazard

No.	Type	Height and Grid Azimuth to HLZ Center
See remarks		

Remarks

The HLZ is located 600 m south of stone bay rifle range. E1 exits the HLZ on the west side extending north on Booker Washington Boulevard to the rifle range or west to range road. The western perimeter of the HLZ has four buildings that may present flight hazards. The HLZ is surrounded on the north, south, and east sides by trees of varying height that may constitute flight hazards to low-flying aircraft. Blowing sand and debris caused by rotor wash may produce flight hazards. Adjacent terrain consists of a dissected plain, vegetated with trees and brush.

Beach Study Example: Image and Supporting Intelligence Report for Onslow Beach North, Camp Lejeune, North Carolina

Sheet: Camp Lejeune MIM
Series: V742S
Edition: 2-DMA
Datum: NAD 83/WGS 84

Left Flank	Beach Center	Right Flank
UTM: 18STD90132636	UTM: 18STD90702680	UTM: 18STD93032730
GEO: 343327N0771714	GEO: 343341N0771636	GEO: 343354N0771633W

Length	Width
Total: 1,393.4 m (4,752 ft) average backshore	Width: 66.4 m (218 ft)
Usable: 1,373.1 m (4,505 ft) visible foreshore	Width: 24.0 m (79 ft)

Surface Material	Trafficability
Nearshore: sand and mud	Personnel: dry—good wet—fair
Foreshore: sand	Wheeled: dry—good wet—fair
Backshore: sand	Tracked: dry—good wet—fair

Tides

Tidal type: diurnal	Average beach gradient: 1:116	Matting recommended: yes
Tidal range: 1.0 m (3 ft)	Firmness: firm when wet	
MFP capable: no; see remarks.	JLOTS capable: no; see remarks.	LCAC offload capable: yes; see remarks.

Location: Onslow Beach North is approximately 13.1 km (7.1 nm) south-southeast of the US Embassy. It is 3.7 km (2.0 nm) east-northeast of HLZ Bluebird and 1.4 km (0.8 nm) east-southeast of HLZ Albatross.

Characteristics remarks: Onslow Beach North is not MPF-capable since there is no MPF-capable port within 92.7 km (50 nm) of the beach. It is not JLOTS-capable due to insufficient beach gradient. It is, however, LCAC offload-capable due to average backshore width of 66.4 m (218 ft). All coordinates provided in this report were derived from the 1:50,000 scale map sheet listed in the reference above. All measurements were derived by MEF imagery analysts from mensurated imagery.

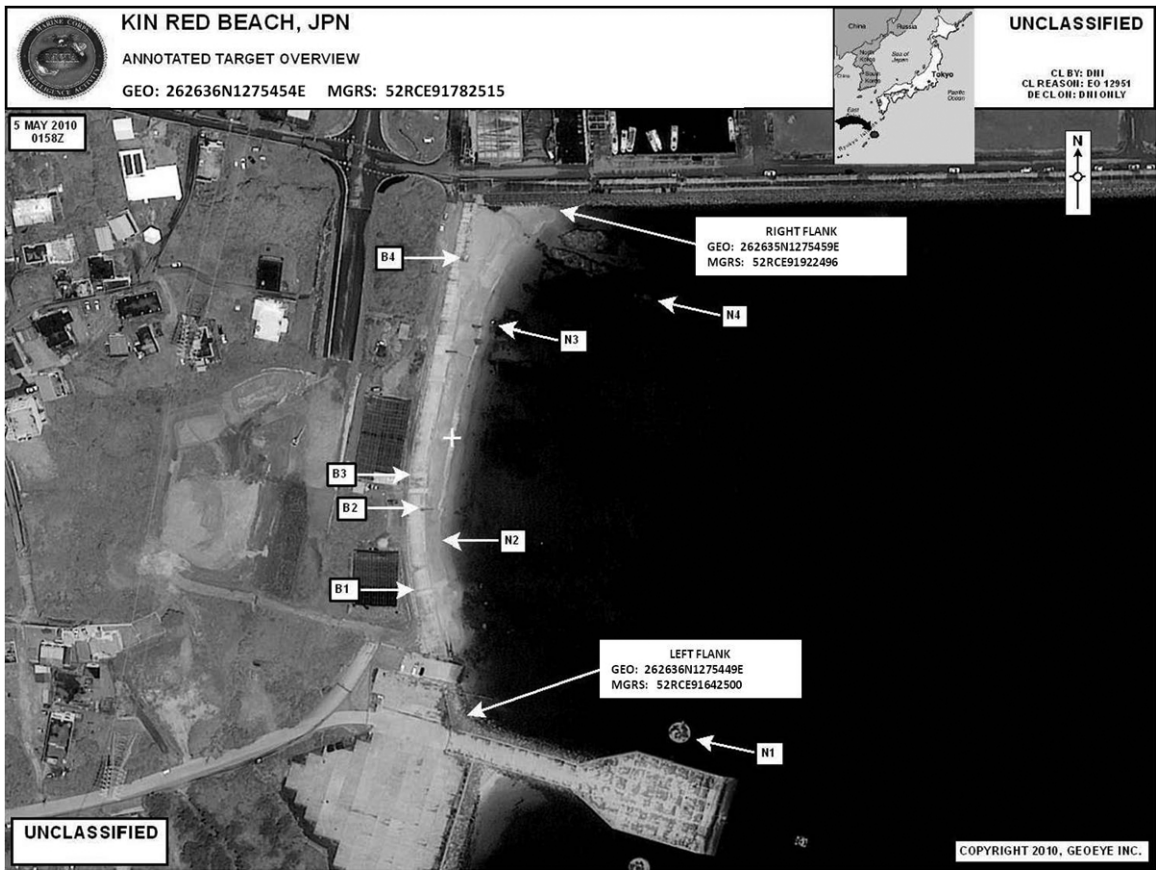
Obstructions

Anno. #	Type	True Bearing	Distance	Length	Width
N1	Pier	225	542.0 m (1,778 ft)	20.3 m (67 ft)	4.5 m (15 ft)

Obstruction remarks: None

Exit remarks: Cross-country to partial cross-country exits are available along the entire beach. These exits are too numerous to list individually. Parallel to the beach is a road that extends 6.3 km (3.4 nm) southwest to New River Inlet and 1.4 km (0.8 nm) northeast to Onslow Beach Road which leads approximately 2.8 km (1.5 nm) north-northeast to Highway 172. There are several buildings and compounds in the hinterland along the road.

Beach Study Example: Image and Supporting Intelligence Report for Kin Red Beach, Okinawa, Japan



Sheet: Kin Red MIM
Series: V742S
Edition: 1-DMA
Datum: NAD 83/WGS

Left Flank	Beach Center	Right Flank
UTM: 52RCE91642500	UTM: 52RCE91782515	UTM: 52RCE91922496
GEO: 262636N1275449E	GEO: 262636N1275454E	GEO: 262635N1275459E

Shape: straight

Length	Width
Total: 274 m (899 ft) average backshore	width: 16.4 m (218 ft)
Usable: 151 m (496 ft) visible foreshore	width: 24.0 m (79 ft)

Surface Material	Trafficability
Nearshore: sand/coral	Personnel: wet—good dry—fair
Foreshore: sand/coral	Wheeled: wet—good dry—fair
Backshore: sand	Tracked: wet—fair dry—poor

Tides

Tidal type: mixed	Average beach gradient: 1:116	Matting recommended: yes
Tidal range: 1.7 m (5.6 ft)	Firmness: firm when wet	

Location and general remarks: Kin Red Beach is located 17.6 km northeast of Kadena Airfield. Four islands obstruct the mouth of Kin Bay. The beach is flanked by a RO/RO pier to the west and a breakwater to the east. There are intermittent streams that cross the beach that could hinder lateral movement during inundation. Personnel exit via cross-country along the entire beach length. The beach is backed by a concrete stepped seawall (B4) that severely restricts tracked vehicle and prevents wheeled vehicle movement. The town of Kin Cho further hinders and channels movement from the beach. Hinterland consists of hills covered with dense vegetation of varying heights, cultivated fields, numerous urban areas and/or tombs.

Obstructions

Anno. #	Type	True Bearing	Distance	Length	Width
N1	Dolphin	226	157 m (515 ft)	3 m (10 ft)	3 m (10 ft)
N2	Coral	250	86 m (282 ft)	18 m (59 ft)	20 m (66 ft)
N3	Coral	090	46 m (150 ft)	32 m (105 ft)	12 m (39 ft)
N4	Coral	113	92 m (302 ft)	40 m (131 ft)	32 m (105 ft)
B1	Coral	261	94 m (308 ft)	8 m (26 ft)	7 m (23 ft)
B2	Coral	270	26 m (85 ft)	14 m (46 ft)	9 m (30 ft)
B3	Coral	077	51 m (167 ft)	16 m (52 ft)	13 m (43 ft)
B4	Seawall	270–070	Varies	270 m (886 ft)	9 m (30 ft)

Obstruction remarks: Obstructions are measured from the beach center to the obstruction.

Exit remarks: See location and general remarks above.

APPENDIX C
IMAGERY INTELLIGENCE
SUPPORT TO INTELLIGENCE STUDIES

Intelligence preparation of the battlespace is the systematic, continuous process of analyzing the threat and environment in a specific geographic area. (Marine Corps Reference Publication 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*) It supports commander and staff estimates and decisionmaking. Applying the IPB process helps the commander selectively apply and maximize combat power at critical points in time and space on the battlefield. When viewed within the scope of the entirety of the IPB, imagery plays a small and focused role; however, its role is vital, especially with respect to terrain analysis and mapping tasks. In the following paragraphs, examples and formulas are provided to aid in the preparation of IPB support products and studies. They are meant as general guides for these products and not meant to replace or supersede any products being developed in accordance with local SOPs.

IMAGERY INTELLIGENCE SUPPORT TO DROP ZONE STUDIES

A drop zone (DZ) is a specific area upon which airborne troops (e.g., a radio reconnaissance team), equipment, or supplies are air-dropped. (JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*) Drop zones are preplanned locations that are determined after careful consideration. When evaluating DZs, imagery analysts must consider the following factors:

- Minimum DZ dimensions (length/width computations).
- Maximum slope percentage for DZs is 30 percent.
- Surface and obstacle considerations.
- DZ accessibility and trafficability.
- Easy exit from the DZ.
- Type of aircraft employed.
- Altitude at which air delivery is to be made.
- Types of loads to be delivered.
- Availability of adequate aircraft approach and departure routes.
- Method of airdrop: free drop, high or low velocity.
- Potential approaches and exits.
- Proximity to mission objective.

- Enemy disposition.
- Alternate DZs and LZs.
- Supporting fires (in coordination with the G-3/S-3 and the fire support coordinator).

Drop Zone Length/Width Computations

The request for DZ identification and supporting intelligence usually includes the rate of speed the aircraft will fly over the proposed area and the amount of time required to deliver a load. The imagery analyst (or all-source intelligence analyst) must be informed of the prevailing wind velocity and wind direction, both of which have an impact on the aircraft's ground speed. When the wind velocity at the delivery altitude cannot be determined, the aircraft's air speed should be used as the ground speed. The steps used to compute DZ size are discussed in the following subparagraphs.

Computing Drop Zone Length. The minimum required DZ length (in meters) is computed by multiplying the ground speed of the aircraft (R) (accounting for windspeed) by the time needed to release its cargo (T): L = R x T. The ground speed is computed by multiplying the aircraft speed in knots (S) by .51, which is the conversion factor of knots to meters per second: R = S x .51.

When computing ground speed (R), add tail wind component of wind velocity to aircraft speed (S) or subtract head wind component of wind velocity from aircraft speed (S) (see fig. C-1). Always round up the required DZ length to the nearest meter. For example, if the aircraft speed (S) is 110 kts, head wind is 20 kts, and drop time (T) is 20 seconds, the required length of the DZ (L) is:

L = R x T = S x .51 x T

L = (110 - 20) x .51 x 20 = 918 m

Computing Dropzone Width. The required DZ width depends upon the method/type of airdrop, wind drift, and formation of the aircraft—all of which is usually provided in the request. When it is not specified, the requester must be given the widths of all proposed DZs that also possess the required

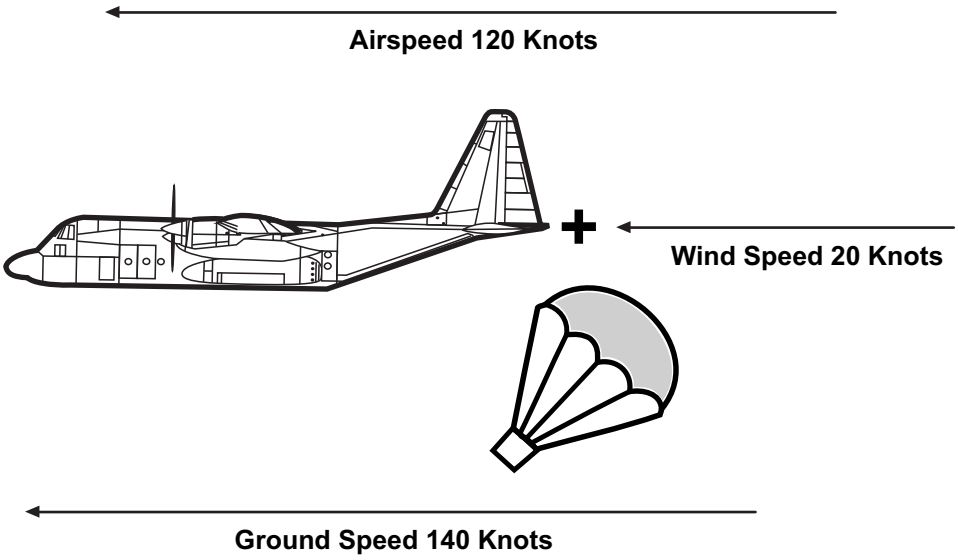


Figure C-1. Prevailing Wind Speed.

length. The wind drift formula—D = K x A x V—is used to determine the minimum required width of a DZ. In this formula, K is a constant that represents the characteristic drift of a certain model parachute. As with the length, the required DZ width is rounded to the nearest meter.

Wind drift has the following factors:

- D = width of DZ (in meters).
- K = 4.1 (constant) for personnel parachutes; 2.6 (constant) for all other parachutes.
- V = velocity of surface wind (in knots).
- A = altitude of the aircraft (in hundreds of feet above ground level).

For example, an aircraft flying at 2,000 ft above ground level (A) is to drop a cargo load with wind speed of 11 kts (V). In this case, G13 cargo parachutes are used (2.6 constant [K]).

D = K x A x V

D = 2.6 x (2,000 ft ÷ 100) x 11

D = 2.6 x 20 x 11 = 572 m

Searching for a Suitable Drop Zone. Now that the required dimensions are known, the imagery analyst searches the imagery (or map if imagery is not available) for suitable DZs. Using a photo interpreter scale or equivalent scale, the imagery analyst measures the potential DZ length on the imagery and then computes the ground distance in meters, rounding down to the nearest meter. The following formulas are used:

- Imagery length: GD = PD x DPRF.
- Map length: GD = MD x DMRF.

The following legend applies to the imagery and map length formulas:

- GD = ground distance (length) (in meters).
- PD = photo distance (if in feet, then multiply by .3048, the conversion factor of feet to meters).
- DPRF = denominator of the photo representative scale factor.
- MD = map distance.
- DMRF = denominator of the map representative scale factor.
- The scale is noted as 1: DPRF or DMRF.

For example, an image has a scale of 1:25,000 (DPRF). Using a scale, the analyst measures a potential DZ to be .06 ft (PD).

GD = PD x DPRF

GD = (.06 x .3048) x 25,000 = 457.2 m = 457 m

The imagery analyst measures the potential DZ width on the imagery (or map if imagery is not available) and then computes the ground distance in meters, rounded down to the nearest meter.

For example, an image has a scale of 1:25,000 (DPRF). Using a scale, the analyst measures a potential DZ to be .04 ft (PD).

GD = PD x DPRF

GD = (.04 x .3048) x 25,000 = 304.8 m = 304 m

In those cases where the plot of the potential DZ is irregular in shape, the lengths and widths will be determined as shown in the sketch in figure C-2. The usable length is measured along a center line while width used is the minimum dimension of the plotted areas with ends perpendicular to the center line. In this example, the width is 140 m and the length is 380 m.

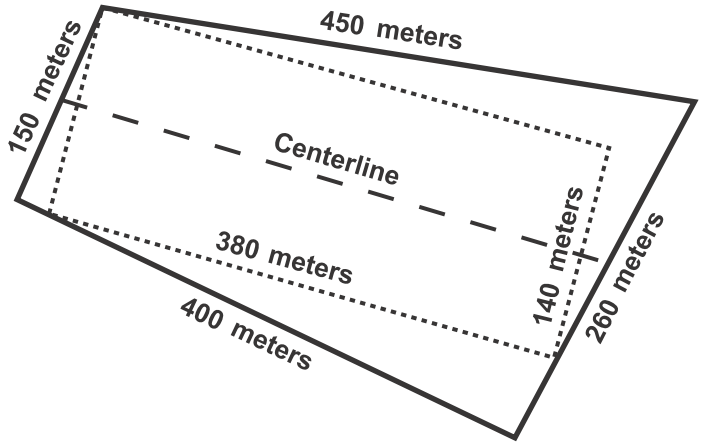


Figure C-2. Irregular-Shaped Drop Zone.

The imagery analyst computes flight time. For safety requirements, a DZ should be as large, or larger, than the commander's request. Normally, an area 460 m long and 180 m wide is the minimum requirement for the delivery of supplies. If a DZ of the desired length is not available, the flight time over the DZ (whatever its length) must be computed to determine how much of the load can be released in one pass and/or how many passes must be made to release the entire load. Always round the flight time down to the next lower whole second.

Flight time is computed using the following formula: T = L ÷ R = L ÷ (S x .51). The following legend applies:

- T = time over the DZ (in seconds).
- L = length of the DZ (in meters).
- R = aircraft ground speed (in meters per second).
- S = aircraft speed (in knots).
- .51 = conversion factor of knots to meters per second.

For example, an aircraft is flying at 105 kts (S) over a DZ measuring 150 m long (L).

$T = L \div R = L \div (S \times .51)$

$T = 150 \div (105 \times .51)$

$T = 150 \div 53.55$

$T = 150 \div 53$

$T = 2.83 = 2$

Slope Calculations

After the DZ area has been determined, the imagery analyst computes the slope. A map of the area is required for this task. The slope of a DZ should not be more than 30 percent, and should be round up to the nearest percent. Both vertical distance and horizontal distance must use the same unit of measurement (feet or meters). Use 3.281 as the conversion factor from meters to feet or .3048 to convert feet to meters. Use the following formula, which will be expressed as a percentage, to compute the terrain's slope: $SL = (VD \times 100) \div HD$. The following legend applies to the formula:

- SL = percent of slope.
- VD = vertical distance of the DZ (altitude difference between each end of the DZ length).
- HD = horizontal distance of the DZ.
- 100 = conversion factor for percent.

For example, the length of the DZ is 900 m, one end is at an altitude of 150 ft and the other end at 200 ft, the percent of slope is 1.7%, rounded up to 2%.

$SL = ([200-150] \times 100) \div (900 \times 3.281)$

$SL = (50 \times 100) \div 2{,}953$

$SL = 1.7 = 2\%$

The contour intervals on maps are in feet or meters. The bar scales are usually in meters, yards, statute miles or nautical miles. If the bar scale is used, a conversion from one unit of measure to another may have to be performed. If a Pl scale is used, the analyst must multiply the measurements by the map scale. To determine slope using a map, refer to the following steps and figures C-3 and C-4.

Step 1. Determine the elevation of each point. Neither point is on a contour line, so it will be necessary to interpolate. Point Y is located on an intermittent stream symbol, which may be confused with a contour line if care is not taken. The contour interval is 50 ft.

Figure C-3. Map Extraction (map not to scale).

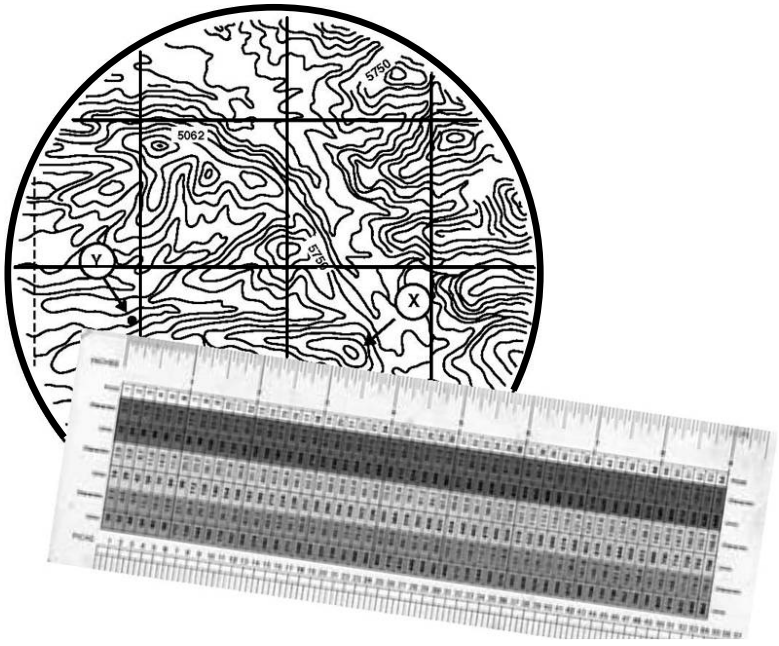


Figure C-4. Measuring from Dot to Dot (map not to scale).

Step 2. Measure the distance between points X and Y using a piece of paper, Pl scale, or boxwood scale. Make measurements from the center of one dot to the center of the other dot (see fig. C-4). A tube magnifier may be required to exactly align the scale with the centers of the two points to accurately determine the distance found. In figure C-4, the map distance (MD) is 2.95 cm. The ground distance is found by solving the following: GD = MD x DMRF.

GD = 2.95 cm x 50,000 = 147,500 cm = 1,475 m

When comparing elevations and horizontal distance, elevation is measured in feet and distance is measured in meters, so a conversion from one to the other is required.

GD = 1,475 m x 3.281 ft/m = 4,839.475 (rounded up to 4,840 ft)

Step 3. Use the slope formula: VD = change in elevation from point V to point Y:

SL = (VD ÷ HD) x 100 = (XY ÷ HD) x 100

For example, a DZ with a length of 4,840 ft (HD) has elevations of 5,925 ft and 5,475 ft.

SL = ([5,925 ft - 5,475 ft] ÷ 4,840 ft) x 100

SL = (450 ft ÷ 4,840 ft) x 100 = 9.2975; rounded up to 10%

SL = 10%

Surface and Obstacle Considerations

When both size and slope of a proposed DZ are acceptable, inspect imagery of the area for the presence of obstacles and potentially hazardous surface conditions. This requires the examination of photography in stereoscopic pairs as well as a review of available maps. Two major reasons for the examination of imagery are to protect troops from injury during a drop and to prevent the unsuccessful drop of equipment. The most acceptable DZ is a flat, resilient surface without obstructions.

Unfavorable or hazardous surface conditions are normally provided by the terrain detachment, including information on—

- Water.
- Marshland.
- Gullies.
- Drop-offs (cliffs).
- Dense trees.
- Dense low vegetation.
- Large rocks.
- Obstacles that are manmade features, such as—
  - Power lines and poles.
  - Buildings.
  - Towers.
  - Fences.
  - Military impediments (e.g., stakes, barriers, barbed wire).

Drop Zone Accessibility and Trafficability

A favorable DZ must have easy accessibility for both approach and exit. If possible, DZs near LOCs should be selected. Certain questions must be answered before DZ identification can occur and the tactical situation will add other questions, such as the following:

- Will the approach involve more troops and equipment or fewer troops and less equipment than the exit?
- Will the exit involve more troops and equipment or fewer troops and less equipment than the approach?
- Will the approach or exit occur during daylight or night?

When troops are parachuted into a DZ, it is important that they have an easy exit. The exit should be in the general direction supporting the ground tactical plan. When supplies or equipment comprise the load, personnel on the ground must be able to approach the area, recover the material, and exit with the material. When evaluating a potential DZ for accessibility, the type of load will be a major consideration. For example, if wheeled vehicles are parachuted into a DZ, troops on the ground may be able to approach the DZ through a densely wooded area or up a steep slope; however, the vehicles may not be able to exit through the forest or negotiate the slope.

A factor related to accessibility is the trafficability of the soil. Swampy soil or in some cases fine sand may rule out the selection of a DZ. The parachuted equipment may bog down or troops may not be able to approach or exit the area rapidly. Therefore, in order to afford easy cross-country movement of vehicles and personnel in and out of the DZ, trafficability of access routes must be considered.

Drop Zone Reports and Overlays

Normally, the imagery analyst assists all-source intelligence and GEOINT analysts with preparing a report in accordance with local SOPs. A primary DZ and alternate DZs that meet the specified intelligence requirements will be selected. This information is provided to the P&A cell OIC, who in turn recommends these to the ISC and G-2. Upon request, an overlay of the primary and alternate DZs will be prepared. Geospatial intelligence analysts generally will prepare this overlay.

IMAGERY INTELLIGENCE SUPPORT TO HELICOPTER LANDING ZONES STUDIES

An LZ may contain one or more landing sites. An HLZ is a ground area specified for landing assault helicopters to embark or disembark troops/cargo. Primary and alternate HLZs that meet the intelligence requirements will be identified, analyzed, and provided to the supported ground unit and aviation commanders. The ground unit commander (or helicopter unit commander) in coordination with the supporting air mission commander (AMC) will select the final location of the HLZ to best support the ground tactical plan.

General Helicopter Landing Zone Criteria

The same criteria used for determining a DZ apply when selecting an HLZ from maps, aerial photographs, and physical ground or aerial reconnaissance. However, additional information, normally supplied by the ACE commander or AMC, should also be used when selecting an HLZ. This should include the HLZ type and the number and type of helicopters used. An HLZ is a helicopter landing area that encompasses one or more helicopter landing sites, making a helicopter landing site a subdivision of an HLZ. The size of a landing site depends on the number of LPs and the size of the LPs. An LP is a designated touchdown point where a single helicopter may land.

The size of the landing site will depend on the number and size of LPs within it. As a guide, a helicopter requires a relatively level, cleared, circular area of 20 to 75 m in diameter. However, this may vary depending on the type of helicopter and because helicopters require more usable landing area at night than during the day. The criteria provided in figures C-5 and C-6 and C-7, on page C-10, represent guidance on LP preparation. Helicopter units will designate the size (small, medium, or large) to be used by their units for specific operations. Numerous considerations, such as helicopter type, unit proficiency, nature of loads, and weather conditions, may apply to the size of LPs used. General distances between LPs within a landing site in daytime landing are as follows (measured center to center):

- Small LPs: 80 ft (25 m).
- Medium LPs: 115 ft (35 m).
- Large LPs: 165 ft (50 m).

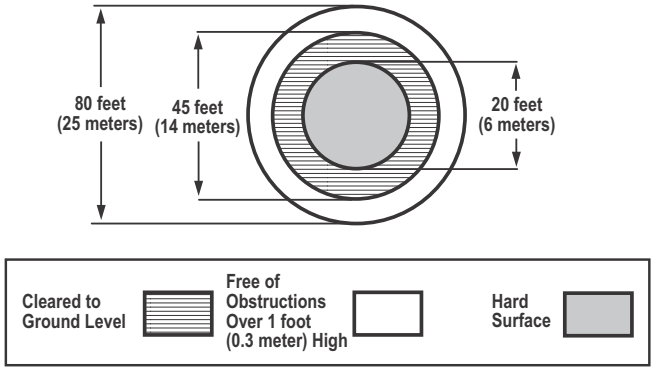


Figure C-5. Small Landing Point Dimensions.

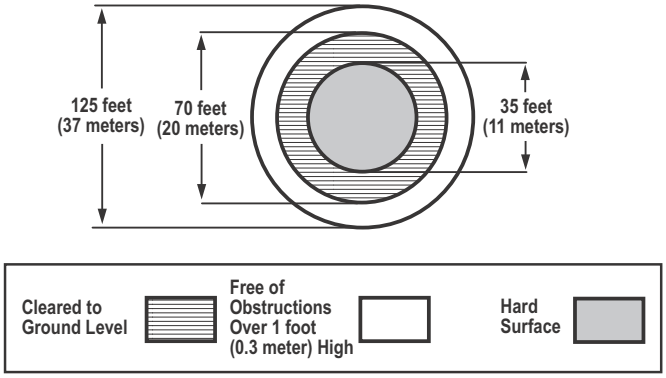


Figure C-6. Medium Landing Point Dimensions.

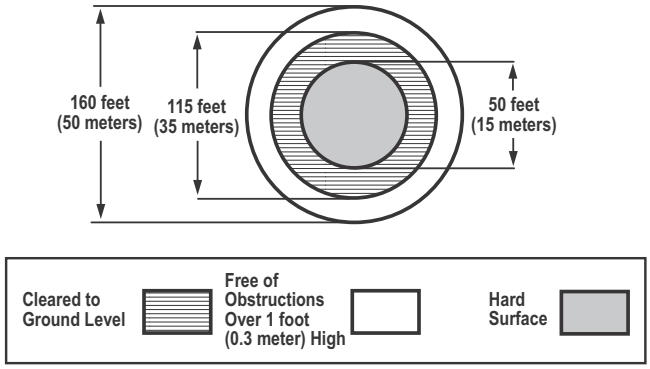


Figure C-7. Large Landing Point Dimensions.

Most helicopters cannot land or take off vertically when they are fully loaded; therefore, when they are, a larger area or a better approach is needed. The ACE commander has the final authority in establishing the landing area criteria for assigned helicopters in daytime and nighttime missions. This may change from time to time, depending on how heavily loaded the aircraft will be, the place and time of landing, and the anticipated weather conditions. During specific missions, the AMC may exercise this authority. For example, the area requirement may be larger when—

- A helicopter is heavily loaded.
- Helicopter cargo is sling loaded.
- A landing must be made at night or during other periods of reduced visibility.
- There are terrain obstructions or obstacles in the area.
- An area is located at high elevation.
- The temperature is hot or when humidity is high.

The ACE commander or AMC should provide the G-2 or ISC with the required dimensions for all HLZs, based on various flight and landing formations. This action will assist imagery analysts and all-source intelligence analysts with locating potential HLZs.

Helicopter Landing Zone Computations

When determining the size of the HLZ area, proceed in the same manner as for calculating the DZ area: first computing the required and then the potential HLZ areas. To determine the HLZ area, use the procedures explained in the following subparagraphs.

Step 1. Determine HLZ dimensions on photographs or maps. If the results are in fractions, round down to the nearest foot or meter. Use the same basis for all measurements (either feet or meters).

Potential HLZ length when measuring:	Potential HLZ width when measuring:
Imagery: GD = PD x DPRF	Imagery: GD = PD x DPRF
On a map: GD = MD x DMRF	On a map: GD = MD x DMRF

Step 2. Determine how many helicopters will be able to land in the potential HLZ area in a two-trail formation during daytime. Round up converted LP dimensions.

Step 3. Determine the number of LPs (or helicopters) from front to rear of the potential HLZ. Round down number of helicopters.

LPs from front to rear = potential HLZ length

Minimum recommended LP length

Step 4. Determine number of lateral LPs of the potential HLZ.

Number of lateral LPs = potential HLZ width

Minimum recommended LP width

Step 5. Determine the total number of helicopters LPs of the potential HLZ.

Total number of helicopter LPs = number of LPs from front to rear x number of lateral LPs

Slope Computations

The slope for an HLZ should not exceed 8 percent if the helicopter is to land. When the slope is more than 8 percent, provide the requester with the exact percent figure so he can assess alternatives and decide. Slope is important because when the ground slope is less than 8 percent, helicopters should land upslope. When the slope is more than 8 percent, helicopters should land side-slope (see fig. C-8 on page C-11). At the pilot's discretion, it may be possible for a helicopter to hover just in contact with the ground on slopes greater than 8 percent.

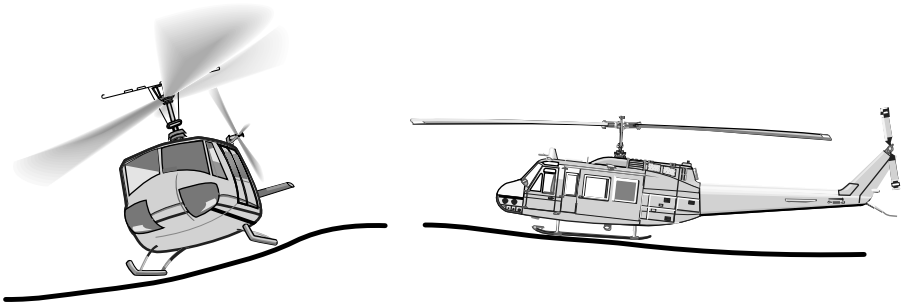
When the slope is greater than the allowable 8 percent, report this to the requester. The site may still be usable if the commander chooses to hover the aircraft and load/unload troops and supplies by rope or ladder.

When computing the slope, do not depend entirely on the map. Study imagery of the area as well. The map contour intervals may indicate that the percent of slope is sufficient, but sloping or rugged terrain can be seen only with a stereoscope.

To compute the slope of each potential HLZ, use the same formula that was used to find the slope for DZs: SL = (VD ÷ HD) x 100.

When computing the HLZ slope, consider the following:

- *Direction of positive slope*. The direction of positive slope is important for the approach and exit direction.
- *Number of aircraft used*. The AMC will provide the number of aircraft used.
- *The density altitude*. The altitude, temperature, and humidity determine the density altitude. For planning purposes, as density altitude increases, the landing area should increase proportionately.



Side Slope Up Slope

Figure C-8. Helicopter Landing on Side Slope and Up Slope.

- *Approach/departure directions*. When possible, the direction of approach and departure should be into the wind. However, if there is only one suitable approach direction due to obstacles or the tactical situation or in order to make maximum use of the available HLZ, most helicopters can land with a crosswind (10 kts or less) or a tailwind (5 kts or less). The same applies to departures from the HLZ.
- *Loads*. When fully loaded, most helicopters cannot ascend or descend vertically.

AIRCRAFT LANDING ZONE

An aircraft LZ (also referred to as runway or landing strip) is a specified location used for landing aircraft. Potential aircraft LZs are selected to meet the intelligence requirements of the supported ground and aviation units' commanders. Potential aircraft LZ locations will be identified and analyzed based on aerial imagery, current maps, and other available intelligence.

Aircraft Landing Zone Criteria

Aircraft LZs are established so aircraft can safely land and take off. They also provide guidance for aircraft while they taxi and park. They have one or more landing strips. The landing strip consists of a runway and may include taxiways, parking points, and dispersal areas. Selection of a potential aircraft LZ depends on the type of aircraft, runway dimension requirements (see Table C-1 on page C-13), surface, and location.

Unmanned aircraft systems sometimes require landing strips. The requirements for these vary. In order to ensure these requirements are met, close coordination with the aviation units that plan to use the landing zone is required for any aircraft landing zone products.

Table C-1. Runway Dimension Requirements.

	Airfield Type	Runway Length (in feet)	Runway Width (in feet)	Runway Shoulder (in feet)
Forward Area	Attack & Utility	N/A	N/A	N/A
	Vertical Lift	N/A	N/A	N/A
	Light Lift	1,200	60	10
	Medium Lift	2,500	80	10
Support Area	Attack & Utility	N/A	N/A	N/A
	Vertical Lift	N/A	N/A	N/A
	Light Lift	1,500	60	10
	Medium Lift	3,500	60	10
	Heavy Lift	6,000	100	10
	Tactical	5,000	60	4
Rear Area	Medium Lift	6,000	72	10
	Heavy Lift	10,000	156	10
	Tactical	8,000	108	20

Airfield Type

There are two types of aircraft LZs, classified according to their size and degree of improvement: a hasty landing strip and a deliberate landing strip. A hasty landing strip has an unimproved surface, which normally is acceptable for marginal weather, but is unusable during prolonged poor weather. After a period of occupation, most landing strips (terrain permitting) can be improved to meet the requirements of a hasty landing strip. A hasty landing strip has the following characteristics:

- Minimum length: 3,000 ft, plus a 10 percent overrun at each end.
- Minimum width: 50 ft, plus a 10-ft shoulder on each side.
- Minimum lateral clearance: 100 ft on each side of runway centerline.
- Has taxiways, parking areas, and may include dispersal areas.

A deliberate landing strip, at minimum, should have all the characteristics of a hasty landing strip plus any other facilities needed to meet the standards required by any aircraft. It has an all-weather capability and is usually a permanent installation with a control tower, hard surface runways, taxiways, and parking ramps.

Aircraft Landing Zone Computations

To determine the length and width of the area, use the same formula that was used to measure a DZ or an HLZ, and then identify the potential aircraft LZ by type. For example, if the photo scale is 1:20,000, the photo distance (length) is .08 ft and the photo distance (width) is .004 ft, then the potential aircraft LZ could be either a hasty or deliberate type depending on construction and facilities.

Slope Computations

When computing the slope, the maximum slope for a potential aircraft LZ should not exceed 10 percent. Always round slope up to the nearest percent. Use the same formula that was used to compute the SL of a DZ or HLZ:

$$\text{SL (expressed as a percentage)} = \frac{\text{VD}}{\text{HD}} \times 100$$

Surface and Obstacle Considerations

The surface of a potential aircraft LZ must be firm and smooth enough to allow heavily loaded aircraft to land, taxi, park, and take off without delay or damage to the aircraft. It should be located away from obstacles, such as mountains, telephone wires, tall buildings, and trees. The area should be free of heavy rocks and stumps so troops can clear it easily. This is particularly important for hasty strips, which may have to be established quickly. The area should be dry, as water or marshland can cause early erosion.

Landing Zone Accessibility

An aircraft LZ should have convenient access, such as roadways or other level terrain, to and from the area. If there are prevailing winds, the runway should be oriented, if possible, so that aircraft can land and take off into the wind. The minimum size of an aircraft LZ depends on the type of loads, the direction and velocity of winds, and the condition of the ground. Consider the following factors when establishing an aircraft LZ:

- Soft, wet, slippery, or any other unfavorable surface conditions will increase the need for a longer aircraft LZ.
- Crosswinds may require an increase in width of the aircraft LZ.
- Uphill take off and downhill landings will require longer runways. The maximum slope on any aircraft LZ should not exceed 10 percent.
- Obstacle clearance is measured from the obstacle to the approach and departure end (if there are obstacles at the approach and departure ends of the aircraft LZ). Be sure to obtain a 10:1 clearance ratio (same as used for an HLZ).

Aircraft Landing Zones Overlays

Per the intelligence production requirement, all-source intelligence analysts, assisted by imagery analysts and GEOINT analysts, will prepare an overlay of the potential primary aircraft LZ and an alternate aircraft LZ, if deemed necessary. A relief and drainage overlay may also be provided. Aircraft LZs are normally referred to by their nickname or a color. Situation and time permitting, GEOINT analysts will prepare this overlay.

IMAGERY INTELLIGENCE SUPPORT TO BEACHES STUDIES

Imagery intelligence support is crucial for amphibious operations. Imagery intelligence helps to provide commanders with the information they need to decide which beaches to use and how those beaches can be used for amphibious operations. They do this through detailed analysis of the beaches and surrounding areas.

Beach Definitions

A beach is the area extending from the shoreline inland to a marked change in physiographic form or material, or to the line of permanent vegetation. In amphibious operations, a beach is that portion of the shoreline designated for landing of a tactical organization. A landing beach is that portion of a shoreline usually required for the landing of a battalion landing team. However, it may also be that portion of a shoreline constituting a tactical locality (such as the shore of a bay) over which a force larger or smaller than a battalion landing team may be landed. A beach landing site (BLS) is a geographic location selected for across-the-beach infiltration, exfiltration, or resupply operations. A beachhead is a designated area on a hostile or potentially hostile shore that, when seized and held, ensures the continuous landing of troops and materiel and provides maneuver space requisite for subsequent projected operations ashore. Finally, a landing area is the part of the operational area within which are conducted the landing operations of an amphibious force. It includes the beach, the approaches to the beach, the transport areas, the fire support areas, the airspace above it, and the land included in the advance inland to the initial objective.

Beach Landing Site Factors

A BLS is a continuous segment of coastline over which troops, equipment, and supplies can be landed by surface means. Primary and alternate BLSs are selected and prioritized after considering the commander's intent and guidance, CONOPS and scheme of maneuver, enemy disposition, size of the area required, terrain features, weather factors, supporting fire, and proximity of the objectives.

Amphibious operations require a detailed study of hydrography, weather, climate, and terrain. The terrain portion is primarily the responsibility of MAGTF GEOINT analysts. A tactical study of the terrain is prepared by all-source intelligence analysts with major assistance from imagery analysts and GEOINT analysts. (See MCWP 2-3 and MCWP 2-26, *Geographic Intelligence*, for additional information on tactical studies of the terrain.)

The landing force commander selects specific landing beaches from available beach landing sites. When the amphibious task force is composed of two or more attack groups with related landing groups, a landing area may be selected for each attack group. In this case, each landing group commander selects the landing beaches from within the assigned area. The principal factors in the selection of landing beaches are—

- Suitability for beaching landing ships, landing craft, and amphibious vehicles.
- Beach trafficability.
- Suitability of offshore approaches.
- Number, location, and suitability of beach support areas and beach exits.
- Location, type, and density of beach obstacles, including underwater obstacles.
- Nature of the terrain immediately inland from the beaches.
- Suitability of LOCs—including roads, railroads, and waterways.
- Suitability of the beach from the standpoint of expected weather and tidal conditions.
- Known hostile force dispositions, strengths, and capabilities.

Beaches are categorized by their shape (see fig. C-9):

- Concave (point A to point B).
- Convex (point B to point C).
- Straight (point C to point D).
- Irregular (point A to point D).

Beach Types

Beach types include the following:

- Coastal plain.
- Coastal ridge.
- Cliff or terrace.
- Coral reef.
- Glacial.
- River mouth or delta.
- Pocket.

Coastal Plain. A landing on a wide coastal plain beach provides unrestricted maneuver room, so a subsequent advance from the beach can be made in any direction. Boundaries and objectives are more difficult to locate on this type of terrain; there are few prominent registration points for artillery, naval gunfire, and aerial bombardment. Usually there is no natural defensive terrain on the flanks of the beachhead, so more troops are required to protect the flanks. Some coastal plain beaches are near marshy and swampy terrain, which may hinder movement from the beach.

Coastal Ridge. A coastal ridge beach has terrain that rises evenly to a considerable distance back from the beach that gives the defender excellent observation and fields of fire. More commonly, the coastal area remains flat for some distance and then rises in a steep gradient to a coastal ridge.

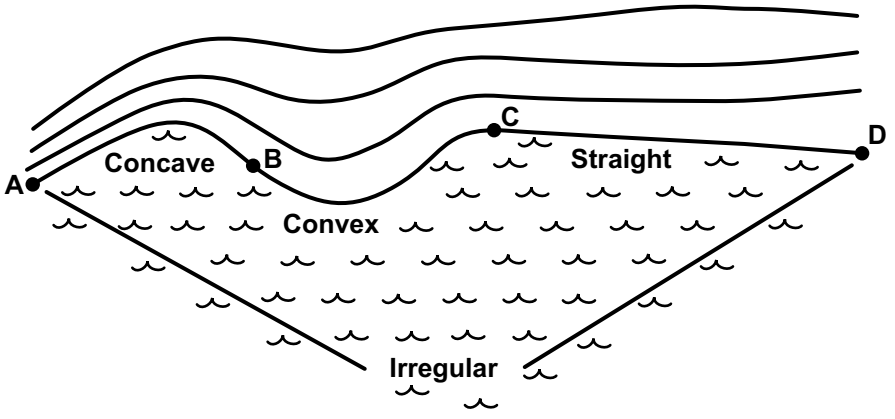


Figure C-9. Beach Categories.

Cliff or Terrace. A cliff or terrace beach is usually quite narrow. The delineation of a cliff beach from a terrace beach basically is established by the height of the landmass immediately behind the beach. Cliff beaches may have rocks and debris that accumulate by erosion of the adjoining severe terrain. The surface is made up of the same type of material as the major adjacent landform. If wave action is strong on a cliff beach, any fine material is washed away resulting in a beach covered with boulders or barren rock. Cliff beaches isolated from strong wave action are usually composed of sand and are similar in surface materials to coastal plain beaches. A terrace beach may be composed of loose sand or rocks; it may be barren rock or strewn with boulders.

Coral Reef. A coral reef beach is located in the coral region (normally between 30 degrees north latitude and 30 degrees south latitude) protected by a barrier reef with fringing reef along the shoreline, or it is located on an atoll. Any beach protected by a barrier reef is composed primarily of fine coral sand (coral skeletal remains, broken shells, and hardened algae) and is usually firm and narrow. When the beach or fringing reef is exposed to wave action, the foreshore is eroded. The coral reefs themselves normally present significant obstacles with abrupt seaward slope and the exposed offshore edge of the reef is steep. The upper surface of the reef may be extremely rough with jagged coral formations rising above the surface and deep pits indenting the surface of the reef. An atoll is a ring-shaped coral island or group of coral islands enclosing a lagoon or another island. It has the same basic characteristics as the coral barrier reef.

Glacial. Glacial beaches are usually found in the higher latitudes, normally above 60 degrees north and 60 degrees south latitude. These beaches were eroded by glacial action and have round and irregular shorelines with numerous inlets; some may be quite deep, long, and narrow, with almost perpendicular, smooth mountain walls rising to great heights. This type of coast is very dangerous to navigation because of the islands and rocks off entrances to the inlets. The beach may be composed of material that has no geologic relationship to the coastline with depositions of material carried from the hinterland by the glaciers. This is often a mixture of silt, sand, gravel, and rocks.

River Mouth or Delta. This type beach is easy to identify due to its proximity to the mouth of a major stream or river. It undergoes a greater physical change than the other beach types, and the foreshore is composed primarily of the type of sediment carried by the stream or river.

Pocket. A pocket beach is found on many of the coasts throughout the world and has a wide range of composition and topography. The irregular coastlines, where pocket beaches are quite common, are made up of headlands and indentations with the pocket beaches found in the indentations. This type of beach is divided into two general areas: the end zones and central zone.

The end zones are those areas on the flanks inside the beach termination points. They are protected from direct wave action by the headlands and subsequently the beach soil is usually fine sand.

The central zone is that portion of the entire beach between the end zones. It exhibits the same characteristics and soil conditions of any beach exposed to wave action. Any highlands behind the beach may provide the source material continually washed down and deposited on the beach. Lowlands behind the beach, however, will have little effect on its character.

A common problem affecting some pocket beaches is that many of the bays or other indentations fronting the beach may become blocked by sandbars built up by sand drifting along the coast in long shore currents. These sandbars may become attached to the mainland at the upstream end, and any open channel that might exist will occur at the downstream end. Sometimes these sandbars connect offshore islands to the mainland. Pocket beaches are usually concave shaped.

Beach Landing Site Criteria

The required beach area for amphibious operations is calculated based on the original requester's guidance, the type of forces conducting the ship-to-shore maneuver, local SOPs, and METT-T. To identify whether an area is suitable for beach landings, intelligence analysts will require the following information:

- Minimum length of beachfront necessary.
- Types of equipment being landed.
- Types of transports to be used, including length and width of each transport type.
- Transport capability. (Can it land on the beach? What is the required minimum depth [draft]?)

Beach Landing Site Computations

As with the calculation of measurements of DZs, HLZs, and aircraft LZs, beach landing length is computed using the formula GD = PD x DPRF. Measurements are taken from one termination point to another (see fig. C-10) and rounded down to the nearest meter.

The beach termination points are the extreme ends of the selected beach. The total length of the beach is measured between these points following the natural coastline.

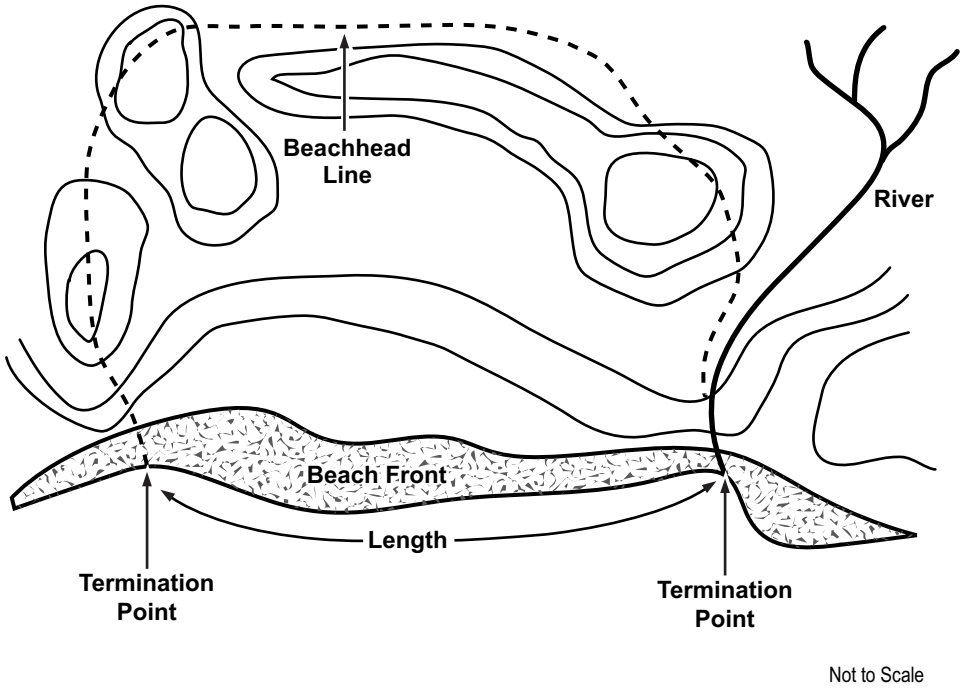


Figure C-10. Landing Beach Length.

The beach width is calculated using the horizontal dimensions of the beach measured at right angles to the shoreline from the line of extreme low water inland to the landward limit of the beach (the coastline). It usually will not be uniform and, therefore, is determined at various points along the beach.

The beachhead line is roughly semicircular and encompasses the area near the coast large enough for the deployment of the assault force and its supplies and equipment, and usually includes terrain features that are the initial objectives of the assault force. The beachhead line, if established, must be held so the subsequent landing forces can land and deploy in proper battle order. Loss of the beachhead—or major enemy force penetration into it—places the entire amphibious operation in jeopardy.

The beachfront extends from low tide limit to the high tide limit and usually coincides with the foreshore (see fig. C-11).

Percent of Slope and Gradient Computations

Measurements of the width of the beachfront are taken to calculate a beach landing length. Apply the same formula that was used to determine the percent of slope of a DZ, HLZ, or aircraft LZ:

SL = (VD ÷ HD) x 100

The VD is the height difference of the beachfront, which is from the edge of the beachfront (low tide limit) to the high tide limit. The HD is the horizontal (ground) distance of the beachfront. Always round up the percent of slope to the nearest percent.

Combined offshore or foreshore/back shore beach gradient is expressed as a ratio of the rise in elevation of one unit of measure to the horizontal (ground) distance in a number of the same unit of measure (e.g., 1:15).

Gradient = VD ÷ HD

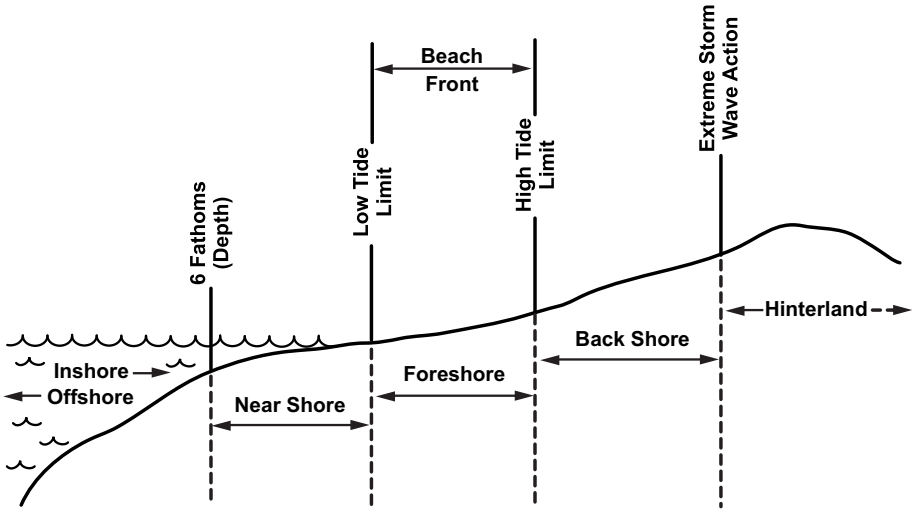


Figure C-11. Shores.

A quick way to obtain the gradient (1:) is to invert the fraction and divide the denominator by the numerator. Round up fractions to the next whole number (e.g., 1:50.52 = 1:51). For example, if VD equals 150 m and HD equals 3,000 m, then the gradient is—

Gradient = 1: (3,000 ÷ 150) = 1:20

When computing the combined foreshore/back shore gradient, measure from the shoreline to the nearest 20-m contour line used for the start of the hinterland. Be sure to transfer the 20-m contour line from the map to the photograph by interpolation prior to making the measurement. The gradient is further expressed as shown in table C-2.

Table C-2. Beach Gradients.

Less than 1:120	Flat
1:120 to 1:60	Mild
1:59 to 1:30	Gentle
1:29 to 1:15	Moderate
1:14 or more	Steep

The depth lines or curves illustrated at 1, 2, and 3 fathoms (1 fathom = 6 ft) (see fig. C-12) are established to determine the offshore gradient and to assist in the safe approach of the landing craft. The depth curves may be a series of dots (as shown) or solid lines.

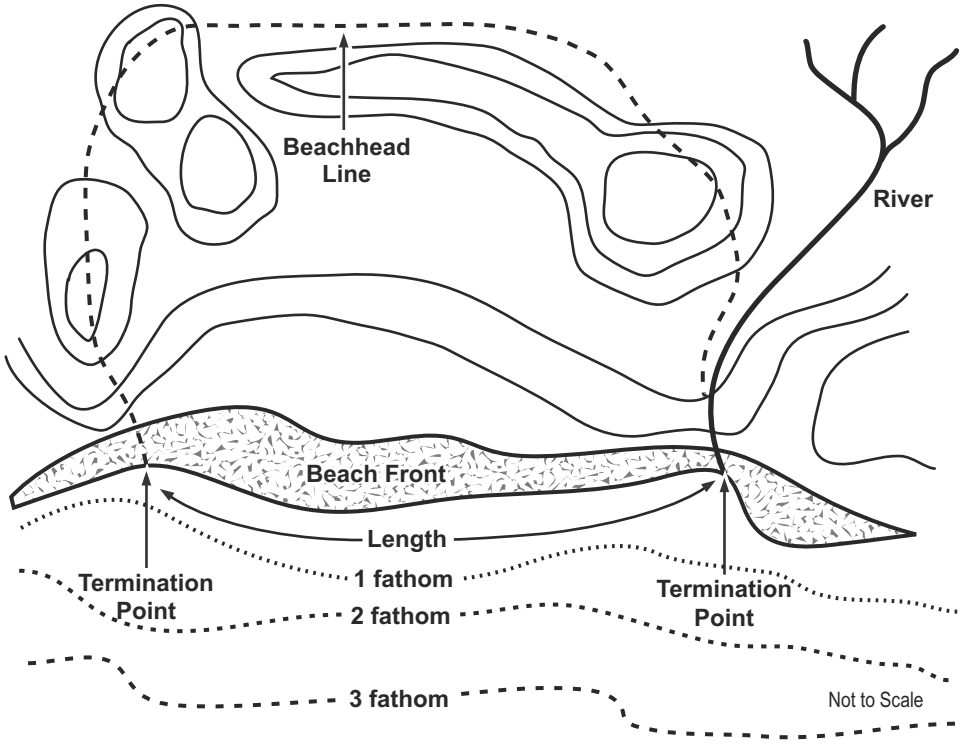


Figure C-12. Typical Beach Landing Area.

Surface and Obstacle Considerations

Normally, the surface condition of the combined foreshore and back shore areas is considered critical upon landing. The foreshore is generally white; the back shore begins where the beach discoloration changes from white to brownish gray and ends at the beginning of the hinterland by revealing a darker tone and taller vegetation on aerial photography. Unfavorable or hazardous surface conditions include the following:

- Large rocks or reefs.
- Drop-offs (cliffs).
- Dense trees.
- Dense vegetation.

Obstacles include the following:

- Buildings.
- Military impediments (e.g., landing craft barriers, barbed wire).

Beach Landing Site Accessibility

Because of the configuration of shorelines, usually the area most suitable for the execution of a landing operation is also the most easily organized for defense. The ideal beach for amphibious landing is one with—

- No obstructions in the sea approaches.
- Deep-water close inshore.
- Near shore gradients that are sufficiently deep for dry ramp beaching of landing craft and ships.
- Soil composed of firm sand with gentle gradients or slopes.
- Small tides.
- No currents.
- No surfs.

The beach terrain should be—

- Gently rising, relatively clear, and have a firm surface that has adequate drainage.
- Flat or gently rising terrain, backed by a coastal range high enough to mask the landing area.

Ideal conditions are rarely found, so suitable areas must be evaluated to determine those that come nearest to optimum requirements. Other terrain considerations include dunes, mountains, and sandbars.

Dunes. Ground that is sharply broken by extensive dunes or a low coastal plateau provides the attacker with concealment from the defender's observation. However, small compartments and corridors limit the range of defensive fire. Dunes are classified as transverse, longitudinal, and coastal.

Transverse dunes are mounds of sand with their longest dimensions oriented at right angles to the prevailing wind. They usually have a steeper slope on the leeward side than they have on the windward side.

Longitudinal dunes are sand formations with their longest dimensions oriented in the same direction as the prevailing wind. They may have a symmetrical shape or may be without any particular shape at all and may be over 100 miles long. They are usually not backed by areas of standing water, such as swamps or marshes.

Coastal dunes, because they are formed by windblown sand, are quite unstable landforms. They may appear in one location as a transverse dune, only to disappear and reform as a longitudinal dune elsewhere. The winds responsible for their formation may also be the means of their destruction.

Mountains. Mountains located directly on the sea usually limit the number of beaches large enough to accommodate a landing force of effective size. Where steep ground is lightly defended or neglected by the defender, a small force may seize it and gain surprise. Airborne or airmobile troops may be used to block the movement of defensive reserves to the landing area or to secure passes through the mountains. Such action prevents the defender from interfering with the amphibious landing.

Sandbars. These offshore sand formations are usually found near coastlines with gentle beach gradients. During stormy weather the sandbars will be found further offshore than during calmer weather conditions. Sandbars paralleling the coast may cause a lagoon to form between themselves and the coastline; direct access to the shore is dependent on openings (channels) through the sandbar areas. The locations of these channels are highly variable, and current photography is required before the actual landing takes place. Soil analysis, beach materials, and other trafficability aspects are normally reported by terrain and soil analysts; however, imagery analysts will determine beach exits, such as roads or airstrips.

Beach Landing Site Collection Checklist Preparation

A collection checklist must be prepared for each potential BLS using the following items:

- Identification: local name and military designation.
- Location:
  - Map reference, including the series and sheet number(s) of both tactical and air/ground series.
  - Political unit, area, universal transverse mercator (UTM) coordinates, and geographic coordinates of the termination points.
  - Landmark reference, a description and location of the landmark and azimuth and distance from landmark to termination point.
- Related water body or watercourses (cross-reference to appropriate collection file).
- Length between termination points.
- Seashore form (concave, convex, straight, or irregular).

- Coastal terrain type, such as emergent, submergent, compound, coral reef, delta, volcanic, fault, or manmade.
- Alignment (high-water shoreline and low-water shoreline).
- Beach width at low water.
- Beach width at high water.
- Backshore:
  - Slope.
  - Material (composition, texture, trafficability).
  - Obstacles.
  - Vegetation.
- Foreshore:
  - Slope.
  - Material (composition, texture, and trafficability).
  - Obstacles.
  - Vegetation.
- Near shore (give alignment and distance from low water shoreline):
  - 10 m (5 fathoms) depth line at low water.
  - 6 m (3 fathoms) depth line at low water.
  - 4 m (2 fathoms) depth line at low water.
  - 2 m (1 fathom) depth line at low water.
  - Obstacles.
- Reefs (near shore):
  - Type and location.
  - Distance from low water shoreline.
  - Length and width.
  - Slope (direction).
  - Depth to surface of reef at low tide.
  - Depth to surface of reef at high tide.
  - Height of surface above water at high and low tide.
  - Effects of surf.
  - Effects on tide.
  - Channel through reef (alignment, width, and depth at low water).
- Reefs (offshore):
  - Type and location.
  - Distance from low water shoreline.
  - Length and width.
  - Slope (direction).
  - Depth to surface of reef at low tide.
  - Depth to surface of reef at high tide.

  - Height of surface above water at high and low tide.
  - Effects of surf.
  - Effects on tide.
  - Channel through reef (alignment, width, and depth at low water).
- Offshore conditions:
  - Water depth.
  - Offshore islands (location and characteristics).
  - Sandbars:
    * Location and distance from low water shoreline.
    * Length and width.
    * Consistency.
    * Slope (seaward and landward).
    * Passages (alignment, width, and depth).
    * Depth at high and low waters.
    * Obstacles (type, location, and characteristics).
- Beach features (natural and manmade, such as cusps, runners, stream mouths, groins, piers, or outfall pipes):
  - Type and location.
  - Number and extent.
  - Bypass possibilities.
  - Influence on operations.
- Tide:
  - Type (diurnal, semi-diurnal, or mixed).
  - Type range (spring, topic, and diurnal).
  - Range.
  - Meteorological effects.
- Surf:
  - Breakers (type, average height, distance formed from shorelines).
  - Period.
  - Width of surf zone.
  - Direction from which swells approach coast.
  - Weather and seasonal effects.
- Currents:
  - Location.
  - Direction.
  - Velocity.
- Beach exits:
  - Type and location.
  - Number and condition.
- Coastal terrain (cross-reference to appropriate collection file):

  - Critical terrain features (location, type, bypasses, and influence on operations).
  - Obstacles (location, type, extent, bypasses, and influence on operations).
  - Cross-country movement (troops, wheeled vehicles, and tracked vehicles).
- Support area concealment and cover (location and type).
- Dispersal and storage area (location and description).
- Availability of fresh water (location and quantity).
- Defenses (location and type).

Terrain overlays are normally prepared by the terrain analysis detachment and added to the checklist. Overlays include presentations depicting cross-country movement, vegetation, slope, soil drainage pattern, and ridgelines.

Beach Landing Site Overlays

Imagery analysts assist all-source intelligence and GEOINT analysts with preparing overlays of the proposed primary and alternate beach landing sites. Beach landing sites are referred to by their nicknames. See MCWP 2-26 for information on the preparation of overlays.

APPENDIX D
NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

BACKGROUND

Imagery analysts use the NIIRS to define and measure the quality of images and performance of imaging systems. Through a process called rating an image, imagery analysts use the NIIRS to assign a number indicating the interpretability of a given image. The NIIRS concept provides a means to directly relate the quality of an image to the interpretation tasks for its use. Although the NIIRS has been applied primarily in the evaluation of aerial imagery, it also provides a systematic approach to measuring the quality of photographic or digital imagery, the performance of image capture devices, and the effects of image processing algorithms.

The NIIRS is a task-based scale consisting of nine graduated levels. At each level, representative exploitation tasks (termed criteria) indicate the level of information extracted with an image of a given interpretability level. For example, in an NIIRS 2 image, imagery analysts should be able to detect large hangars at an airfield; whereas, in an NIIRS 8 image, they should be able to identify the rivet lines on bomber aircraft. Even more detailed information can be obtained from an image at a higher NIIRS level.

The NIIRS was designed to refer to a wide range of image quality. An NIIRS level of 0 is defined as having no value for intelligence purposes; however, the definition of level 0 is open to debate. While, the upper end of the scale is defined by the best available imagery of a given type, it is not necessarily indicative of any specific operational system.

The NIIRS measures the information potential (i.e., interpretability of an image). This means that specific objects listed in the criteria, such as aircraft, need not be present, but the physical attributes of the image would have the specified information value if the specific object from the criteria were present.

The NIIRS relies on the experience of imagery analysts to be able to extrapolate or imagine how well criteria would be rendered if those features were present in the image to be rated. Because each rating refers to specific tasks the imagery analyst can or should be able to do, it has a more precise meaning than, for example, when such subjective words as *good* or *fair* are used. Thus, because imagery analysts can use the same yardstick to measure interpretability, judgments become more uniform.

The NIIRS takes into account the important factors that affect image interpretability. For example, image resolution, measured as ground resolved distance or ground sample distance, has a significant effect on interpretability; moreover, spatial resolution alone does not determine the NIIRS of an image, since sharpness, noise, and contrast also influence the NIIRS. These effects may be due to system parameters (e.g., optical quality, focal plane characteristics), acquisition conditions (e.g., sun angle, atmospheric haze), and exploitation conditions (e.g., duplicate film quality, softcopy monitor quality). By design, the NIIRS is independent of a particular imaging system. See table D-1 for a listing of NIIRS ratings and ranges.

Table D-1. National Imagery Interpretability Rating Scale Rangers.

NIRS Rating	Range in Meters
0	N/A
1	Over 9.0
2	4.5–9.0
3	2.5–4.5
4	1.2–2.5
5	0.75–1.2
6	0.4–0.75
7	0.2–0.4
8	0.1–0.2
9	Less than 0.1

PRINCIPAL USES OF THE NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

There are several primary uses for the NIIRS, including—

- Communicating imagery interpretability. (Can this image answer the intelligence requirement, both now and when archived?)
- Developing collection requirements. (Can an imagery system collect the required information? Can the currently available imagery missions collect the information?)
- Assessing mission collection satisfaction. (Does the image satisfy the intelligence requirement?)
- Assessing technical performance. (Is the imagery system working as planned?)

PROCEDURE FOR ASSIGNING THE NATIONAL IMAGERY INTERPRETABILITY RATING SCALE RATING LEVELS CRITERIA

The NIIRS criteria are expressed in terms of how one is able to *detect*, *identify*, or *distinguish between* objects, features, or activities. *Detect* is the capability to find or discover the presence or existence of an installation, object, activity, or item of intelligence interest based on its general

shape (configuration) and on other contextual information in the scene. Some level of identification is implied in detection, so that the relatively gross feature or item detected can be properly named or classified. *Identify* is the capability to name an object by type or class based primarily on its configuration and detailed components. As used in NIIRS, identification is based on the observation of actual physical detail and not through information from other sources. *Distinguish between* is the capability to determine that two detected objects are of different types or classes based on one or more distinguishing features.

The following guidelines allow NIIRS to be used to communicate image interpretability, evaluate mission performance, and plan for new imagery systems:

- When assigning an NIIRS level, the imagery analyst should evaluate a target within an imagery segment or the entire area on the segment, as necessary, to meet the imagery analyst's task. The imagery analyst will assign an NIIRS level that best characterizes the overall interpretability of the target or area.
- The imagery analyst should neither ignore nor emphasize exceptionally good or poor portions of the image segment.
- When considering clouds, shadows or other localized degradations, the imagery analyst should rate the target or area with NIIRS level 0 only when the degradation precludes using it for interpretation. If the AOI is degraded but interpretable, the imagery analyst should assign an NIIRS that best represents its interpretability.
- The imagery analyst should ignore shadows cast by individual items of intelligence interest.

PANCHROMATIC NATIONAL IMAGERY INTERPRETABILITY RATING SCALE, OCTOBER 2008

Air Order of Battle

Rating Level 0: not applicable.

Rating Level 1: not applicable.

Rating Level 2:

- Distinguish between taxiways and runways at medium to large airfields.
- Identify individual revetments/hardened aircraft bunkers.
- Detect the presence of large airfields by the configuration of the facility (e.g., petroleum, oils, and lubricants [POL] storage, major support facilities, and runways).

Rating Level 3:

- Identify the wing configuration (e.g., straight, swept, delta) of all large aircraft (e.g., 707, 747, BEAR, BLACK JACK).
- Detect the presence of small fighter aircraft.

- Detect weapons storage areas by their physical security and configuration (e.g., 5 or more buildings/bunkers).
- Identify a control tower at an airfield.
- Detect radar sites (e.g., ground control intercept, ground controlled approach, and instrument landing system) at an airfield.

Rating Level 4: identify a BADGER, BACKFIRE, or CANBERRA by overall configuration.

Rating Level 5:

- Identify the propellers on transport aircraft (e.g., RS-COOT, COKE, CURL; CA-DASH 7, BUFFALO; INT-F27).
- Detect canvas covering on small fighter aircraft.
- Identify small fighter aircraft by type (e.g., RS-FLOGGER, FISHBED; US F-16; INT-TORNADO, JAGUAR; FR-SUPER ENTENDARD, MIRAGE).
- Identify medium helicopters (e.g., RS-HIP, HIND; US-Blackhawk; FR-SUPER FRELON, PUMA).

Rating Level 6:

- Identify dummy fighter aircraft by observation of discrepancies in wing sweep, root chord, or other features.
- Detect the presence of missiles loaded onto medium or large fighter aircraft.
- Distinguish between FITTER-A and other FITTER models by the number of wing fences.
- Identify individual approach lights at the end of a runway.

Rating Level 7:

- Detect canard on missiles carried on fighter aircraft.
- Distinguish between fairings, bulges, and antennas on fighter-sized aircraft.
- Identify the individual steps on a mobile passenger stairway.
- Detect canopy seam on small fighter aircraft (e.g., RS-FLOGGER, FISHBED; US F-16; INT-TORNADO, JAGUAR; FR-SUPER ENTENDARD, MIRAGE).
- Identify all structural lines, including butt joints, lap joints, rivet lines, and weld seams on large commercial or military transports (e.g., 747, Condor, C-5, AIRBUS 340).

Rating Level 8:

- Identify separate rungs on cockpit ladders.
- Detect elements internal to the cockpit (e.g., seat, other cockpit components).

Rating Level 9: not applicable.

Cultural Order of Battle

Rating Level 0: interpretability of the imagery is precluded by obscuration, degradation, or very poor resolution.

Rating Level 1: identify a small cluster of houses in a rural area by overall pattern.

Rating Level 2: detect individual two or three story buildings.

Rating Level 3:

- Detect trains or strings of standard rolling stock on railroad tracks (not individual cars).
- Detect large vehicles (e.g., trucks/buses) on highways.
- Detect rows of vehicles parked in a parking area.

Rating Level 4:

- Distinguish between rail tank cars, box cars, and gondola cars.
- Distinguish between large trucks and buses.

Rating Level 5:

- Identify the front windshield on a light-colored automobile.
- Identify trucks as cab-over-engine or engine-in-front.
- Detect (but not necessarily distinguish) cattle, camels, horses, and similar sized animals in open areas.

Rating Level 6:

- Detect a sunroof on a light-colored automobile.
- Detect people on sidewalks or market areas (including the shadows cast by people).
- Detect individual oil drums/55-gallon barrels.

Rating Level 7:

- Determine the presence of a luggage rack on the roof of a light colored vehicle.
- Determine the direction a railroad switch is set based upon rail position.

Rating Level 8:

- Identify the arms and legs on an individual.
- Distinguish between a person on a motorcycle and a person on a motor scooter.
- Identify the ribbing in the bed of a pick-up truck.

Rating Level 9:

- Distinguish hands/feet from limbs.
- Distinguish between types of military small arms being carried by an individual (e.g., rifle or rocket propelled grenade [RPG]).
- Identify farm or construction tools by general shape (e.g., shovel, pitchfork, pick, ax, sledge hammer).

Electronic Order of Battle

Rating Level 0: not applicable.

Rating Level 1: not applicable.

Rating Level 2: not applicable.

Rating Level 3: identify radar/guidance areas of a SAM site, based on configuration.

Rating Level 4: identify the presence of a SATCOM site (Orbit A) by the presence of large SATCOM dishes (10 m or greater in size).

Rating Level 5:

- Detect civilian SATCOM dish (approx 1.62 m) on a rooftop.
- Detect a building-mounted VHF communication antenna.
- Identify the individual posts in a rhombic or quadrant array.
- Distinguish between TALL KING A, B, C, and D radars.

Rating Level 6:

- Distinguish between an ODD PAIR and an ODD GROUP by the antenna placement on the van.
- Detect the leveling/transport equipment on a TIN SHIELD radar.
- Identify the leveling/transport equipment on a BARLOCK or BACKTRAP radar.
- Distinguish between a SPOON REST C/D by the number of elements.

Rating Level 7:

- Identify the DATA LINK ANTENNA on BILL BOARD EW radar.
- Identify the feed structure of the target acquisition radar on the 2S6 when deployed.
- Distinguish between the individual FEED HORNS on a SQUARE PAIR radar.
- Identify whip antennas on box body vans and trailers.
- Detect individual elements of a Yagi array on a mobile electronics van.

Rating Level 8:

- Identify feed horn on small dish antenna (1.7 m or smaller in size).
- Identify framework on rear sides of CLAM SHELL parabolic dish.

Rating Level 9: not applicable.

Ground Order of Battle

Rating Level 0: not applicable.

Rating Level 1: not applicable.

Rating Level 2: not applicable.

Rating Level 3: identify the areas of a ground forces installation (e.g., living areas, athletic fields, motor pools, parade grounds, obstacle course).

Rating Level 4:
- Identify riveted bunkers at a ground forces facility.
- Identify an AAA gun site.
- Detect a small convoy of civilian vehicles (cars, pick-ups, sport utility vehicles).

Rating Level 5:
- Identify tracked vehicles by general type, when in groups.
- Detect the gun tube on large field artillery guns.

Rating Level 6: identify the shape of a tank turret as round, elliptical, or angular.

Rating Level 7:
- Identify gun barrels on 2S6.
- Distinguish between tracks made by wheeled and tracked vehicles.
- Identify a ZSU-23/4 self-propelled antiaircraft gun by the GUN DISH radar.

Rating Level 8:
- Detect a stack of military small arms (e.g., rifles, shoulder-fired weapons).
- Identify type of muzzle brake on towed field guns as multiple baffles.
- Identify individual grates in engine vents on tanks and armored personnel carriers.
- Identify the muzzle brake perforations on a D-30 howitzer.
- Detect a person carrying military small arms (e.g., rifle, RPG).

Rating Level 9:
- Identify the type of clothing (e.g., civilian attire or military uniform) on an individual.
- Identify shoulder-fired weapons (e.g., RPG/SA-7/14, REDEYE, STINGER).
- Detect whether an individual is wearing external body armor.
- Read tactical vehicle markings.
- Distinguish between types of military small arms (e.g., rifle or RPG) being carried by an individual.

Missile Order of Battle

Rating Level 1: not applicable.

Rating Level 2: not applicable.

Rating Level 3:
- Detect a mobile intercontinental ballistic missile (ICBM) or an intermediate-range ballistic missile base by patterns of buildings and roads.

- Detect a SAM support facility for SA-2/CSA-1 missiles on the basis of its configuration.
- Identify a major missile test range (e.g., Tyuratam) by the presence of roads with wide radius curves, railroad loading docks, and the presence of heavy equipment, such as missile gantries.
- Detect a launch complex at a known missile test range.
- Identify a SA-10 A/B launch site based on site configuration.
- Identify radar and guidance areas at a SAM site by the site configuration, mounds, and presence of numerous concrete aprons.

Rating Level 4:

- Distinguish between an occupied and an unoccupied fixed SAM site.
- Detect a security fence erected around a missile launch site or transporter.
- Detect a field deployed SAM unit on the basis of equipment types present (e.g., launcher, missile, transloader).
- Detect individual single-bay garages at SS-25/27 bases.

Rating Level 5:

- Detect an erected missile on a short-range ballistic missile (SRBM)/medium-range ballistic missile transporter-erector-launcher (TEL) missile platform.
- Distinguish between open and closed sliding roofs on a single-bay garage at an SS-25/27 mobile missile base.
- Identify propellant/warhead/oxygen (26-m), hydrogen (44-m), fuel and oxidizer containers/ canisters/tanks.
- Distinguish between mobile missile TELs and missile support vans in a known support base, when not covered by camouflage.
- Identify missile transporter vehicles with prime movers.

Rating Level 6:

- Identify individual SA-3, missiles on launchers.
- Identify an SA-2/CSA-1 transporter by overall configuration and details of chassis construction.
- Distinguish between SA-6 TEL and its associated STRAIGHT FLUSH radar when in travel mode.
- Identify mobile-tracked/wheeled SAM equipment by model (e.g., RS SA-6, SA-13, SA-9, SA-8; US-CHAPARRAL; FR-CROTALE; INT-ROLAND).
- Identify an SA-2 or CSA-1 missile by the presence and relative positions of wings and control fins.

Rating Level 7:

- Identify exhaust nozzle on an SA-5 solid fuel booster.
- Detect support bands on a SA-12 (types A and B) canister.
- Identify the hinge line on the control surface of sustainer fins of an SA-3.
- Identify a MOD III or IV SA-2 missile by sustainer fin tip chord variations.

Rating Level 8:

- Identify joints and welds on a TEL and radar.
- Identify seams, welds, joints, and construction lines on a No-Dong class medium-range ballistic missile.
- Identify factory markings on a missile canister to determine possible model number or dummy SA-5 missile.
- Identify screws and bolts on missile components.

Rating Level 9: not applicable.

Naval Order of Battle

Rating Level 1: not applicable.

Rating Level 2:

- Detect the presence of a large ocean-going vessel in open water.
- Detect a large shallow-water marina.
- Detect a mid-sized port facility.

Rating Level 3:

- Detect small boats (e.g., fishing vessels, small combatants, patrol boats).
- Distinguish between naval and civilian port facilities by type and configuration of large functional areas.
- Identify a dry dock at a known port facility.
- Identify a large surface ship in port by type (e.g., auxiliary ship, combatant, noncombatant/merchant).
- Identify aircraft carriers by the size of the ship and the shape of the deck.

Rating Level 4:

- Identify a Soviet ship as either a cruiser or a destroyer by its relative size and hull shape.
- Identify a TYPHOON in port or at anchorage.
- Determine if ship holds are open or closed.
- Detect aircraft on an aircraft carrier.
- Distinguish between a freighter and a tanker on the basis of equipment on deck.
- Identify cranes at a port by type (e.g., jib, gantry, shear leg).

Rating Level 5:

- Distinguish between fleet ballistic missile submarines and other classes of submarines (e.g., attack submarine, nuclear attack submarine, cruise missile submarine).
- Identify a KASHIN-class destroyer by the twin pair of square smoke stacks.
- Detect the presence of a medium-caliber bow gun on a destroyer.

Rating Level 6:

- Identify SAM launch tubes or canisters on combatants (e.g., SA-N-3 GOBLET).
- Detect a BANDSTAND communications system on a SOVREMENNYY-class ship.
- Identify missile tracking and control radars on guided missile cruisers/destroyers (e.g., RS – TOP DOME, FRONT DOME, KITE SCREECH).
- Identify the 12 individual hatch covers of inclined launched SA-N-6 forward of superstructure on KIROV [Soviet tank]-class.
- Identify individual gun barrels on a KIROV.
- Identify missile doors on cruise missile submarines, nuclear or fleet ballistic-missile submarines.

Rating Level 7:

- Detect the gun turret hatches.
- Detect the presence of personnel on deck.
- Identify individual posts and rails of protective railing around the perimeter of the deck.
- Identify the hull numbers on a Iranian COMBATTANTE IIB-class PTG [guided-missile patrol craft] (also known as: KAMAN P-227 SHAMSHIR).
- Identify detail on torpedo tubes (e.g., banding).
- Identify individual elements of weapons and electronics systems (e.g., feed horns, muzzle breaks, screens, feed mounts).
- Identify winch cables on deck-mounted cranes.
- Identify the configuration (e.g., shape, number of blades) of a submarine propeller in dry dock.

Rating Level 8:

- Identify mounting rings on the life support/rescue canisters.
- Identify ship's pendant number on life rings mounted on bulkheads.
- Identify individual rungs on between-deck ladders.

Rating Level 9: not applicable.

INFRARED NATIONAL IMAGERY INTERPRETABILITY RATING SCALE, APRIL 1996

Rating Level 0: interpretability of the imagery is precluded by obscuration, degradation, or very poor resolution.

Rating Level 1:

- Distinguish between runways and taxiways on the basis of size, configuration, or pattern at a large airfield.
- Detect a large (e.g., greater than 1 square km) cleared area in dense forest.
- Detect large oceangoing vessels (e.g., aircraft carrier, supertanker, KIROV) in open water.
- Detect large areas (e.g., greater than 1 square km) of marsh/swamp.

Rating Level 2:

- Detect large aircraft (e.g., C141, 707, BEAR, CANDID, CLASSIC).
- Detect individual large buildings (e.g., hospitals, factories) in an urban area.
- Distinguish between densely and sparsely wooded and open fields.
- Identify an SS-25 base by the pattern of buildings and roads.
- Distinguish between naval and commercial port facilities based on type and configuration of large functional areas.

Rating Level 3:

- Distinguish between large (e.g., C141, 707, BEAR, A300 AIRBUS) and small aircraft (e.g., FISHBED, L39).
- Identify individual thermally active flues running between the boiler hall and smokestacks at a thermal power plant.
- Detect a large air warning radar site based on the presence of mounds, revetments, and security fencing.
- Detect a driver training track at a ground forces garrison.
- Identify individual functional areas (e.g., launch sites, electronics area, support area, missile handling area) of an SA-5 launch complex.
- Distinguish between large (e.g., greater than 200 m) freighters and tankers.

Rating Level 4:

- Identify the wing configurations of small fighter aircraft (e.g., FROGFOOT, F-16, FISHBED).
- Detect a small (e.g., 50-m square) electrical transformer yard in an urban area.
- Detect large (e.g., greater than 10 m in diameter) environmental domes at an electronics facility.
- Detect individual thermally active vehicles in garrison.
- Detect thermally active SS-25 missile support vehicles in garrison.
- Identify individual closed-cargo hold hatches on large merchant ships.

Rating Level 5:

- Distinguish between single tail (e.g., FLOGGER, F-16, TORNADO) and twin tailed (e.g., F-15, FLANKER, FOXBAT) fighters.
- Identify outdoor tennis courts.
- Identify the metal lattice structure of large (e.g., approximately 75 m) radio relay towers.
- Detect armored vehicles in a revetment.
- Detect a deployed transportable electronics tower at an SA-10 site.
- Identify the stack shape (e.g., square, round, oval) on large (e.g., greater than 200 m) merchant ships.

Rating Level 6:

- Detect wing-mounted stores (e.g., air-to-surface missiles, bombs) protruding from the wings of large bombers (e.g., B-52, BEAR, BADGER).
- Identify individual thermally active engine vents atop diesel locomotives.
- Distinguish between a FIX FOUR and FIX SIX site based on antenna pattern and spacing.
- Distinguish between thermally active tanks and armored personnel carriers.
- Distinguish between a two-rail and four-rail SA-3 launcher.
- Identify missile tube hatches on submarines.

Rating Level 7:

- Distinguish between ground attack and interceptor versions of the MIG-23 FLOGGER based on nose shape.
- Identify automobiles as sedans or station wagons.
- Identify antenna dishes (smaller than 3 m in diameter) on a radio relay tower.
- Identify the missile transfer crane on an SA-6 transloader.
- Distinguish between an SA-2/CSA-1 and a SCUD-B missile transporter when missiles are not loaded.
- Detect mooring cleats or bollards on piers.

Rating Level 8:

- Identify the ram air scoop on the dorsal spine of FISHBED J/K/L.
- Identify limbs (e.g., arms, legs) on an individual.
- Identify individual horizontal and vertical ribs on a radar antenna.
- Detect closed hatches on a tank turret.
- Distinguish between fuel and oxidizer multisystem propellant transporters based on twin or single fitments on the front of the semitrailer.
- Identify individual posts and rails on deck edge life rails.

Rating Level 9:

- Identify access panels on fighter aircraft.
- Identify cargo (e.g., shovels, rakes, ladders) in an open bed, light-duty truck.
- Distinguish between BIRDS EYE and BELL LACE antennas based on the presence or absence of small dipole elements.
- Identify turret hatch hinges on armored vehicles.
- Identify individual command guidance strip antennas on an SA-2/CSA-1 missile.
- Identify individual rungs on bulkhead-mounted ladders.

RADAR NATIONAL IMAGERY INTERPRETABILITY RATING SCALE, APRIL 1999

Rating Level 0: interpretability of the imagery is precluded by obscuration, degradation, or very poor resolution.

Rating Level 1:

- Detect field delineation based on vegetation differences.
- Identify golf courses.
- Detect natural surface runways (e.g., grass, bare earth) in open terrain.
- Detect shoreline quays outside of a port facility in absence of ships.
- Detect vessel (~300 ft long) at suspected narcotics transshipment point in open ocean.

Rating Level 2:

- Identify natural drainage pattern in tidal flats.
- Detect extent of recent flooding based on soil moisture differences.
- Detect windbreaks/hedgerows between fields.
- Identify composition of runway/taxiways/parking aprons (e.g., concrete, asphalt).
- Detect wetland areas unsuitable for mobile ICBM traffic.
- Detect submerged spoil field from dredging operations near a port facility.
- Detect the presence of offshore surface vegetation along a beach LZ.

Rating Level 3:

- Distinguish between fallow and abandoned fields.
- Detect effluent discharge into water from industrial facility.
- Distinguish between an open pit coal mine and a limestone quarry.
- Identify large cargo aircraft as military or commercial based on paint color/scheme.
- Detect rows of vehicles in a parking area.
- Identify beach terrain suitable for amphibious landing operations.

Rating Level 4:

- Detect vegetation stress/aging in narcotics crops in reported eradication area.
- Identify tennis court composition (grass, clay, or rubber/composite).
- Detect CCD efforts (cut vegetation, camouflage netting) at suspected coca processing facilities.
- Identify azimuth markings (numbers) on runway.
- Detect tanks and self-propelled guns in revetted positions.
- Detect blast marks from mobile- or silo-based ICBM launches on concrete.
- Detect presence of sea land containers on a ship’s deck.
- Distinguish between coal and sand loaded onto a dumb barge.

Rating Level 5:

- Detect individual trees with indications of vegetation stress.
- Identify color of unfurled sails on sailboats (20 to 30 ft long).
- Distinguish between military and civilian helicopter paint schemes.
- Identify large ground forces' equipment by type (e.g., tanks, self-propelled guns, armored recovery vehicles).
- Detect foxholes by ring of spoil outlining hole.
- Detect the presence of sailors in formation on the deck of a large combatant during parade/ review.
- Identify colors of stripes/deck markings on major surface combatants.

Rating Level 6:

- Detect a foot trail through tall grass.
- Identify colored bands on rail cars.
- Identify support personnel performing maintenance while on an aircraft.
- Identify the colors of stack markings on merchant ships.
- Detect the presence of an algae line on the dark surface of a submarine hull.

Rating Level 7:

- Identify medium farm animals by type (e.g., sheep, hogs, goats).
- Distinguish road safety signs by color.
- Detect wing flaps and other articulating surfaces on fighter aircraft.
- Distinguish between open and closed hatches on the turret of an MTLB [Russian transport combat vehicle] chassis.
- Detect windsock on helicopter deck.
- Identify canvas covering the muzzles of an ADMG630 gun.

Rating Level 8:

- Detect different species of trees based on color variation.
- Detect a soccer ball in play at a sports field.
- Detect a person (with helmet) in a fighter aircraft with the canopy open.
- Identify turret-mounted smoke grenade dischargers on an M1 main battle tank.
- Detect color-pattern-of-life rings on surface vessels.

Rating Level 9:

- Identify rock layers in sedimentary outcropping.
- Identify and count cleats on a civilian ski boat.
- Detect red/green wing lights on fighter aircraft.
- Distinguish between armed soldiers and armed civilians based on clothing.
- Identify the draft marks numbers on submarine bows.

MULTISPECTRAL NATIONAL IMAGERY INTERPRETABILITY RATING SCALE, JANUARY 2001

Rating Level 0: interpretability of the imagery is precluded by obscuration, degradation, or very poor resolution.

Rating Level 1:

- Detect field delineation based on vegetation differences.
- Identify golf courses.
- Detect natural surface runways (e.g., grass, bare earth) in open terrain.
- Detect shoreline quays outside of a port facility in absence of ships.
- Detect vessel (~300 ft long) at suspected narcotics transshipment point in open ocean.

Rating Level 2:

- Identify natural drainage pattern in tidal flats.
- Detect extent of recent flooding based on soil moisture differences.
- Detect windbreaks/hedgerows between fields.
- Identify composition of runway/taxiways/parking aprons (e.g., concrete, asphalt).
- Detect wetland areas unsuitable for mobile ICBM traffic.
- Detect submerged spoil field from dredging operations near a port facility.
- Detect the presence of offshore surface vegetation along a beach LZ.

Rating Level 3:

- Distinguish between fallow and abandoned fields.
- Detect effluent discharge into water from industrial facility.
- Distinguish between an open pit coal mine and a limestone quarry.
- Identify large cargo aircraft as military or commercial based on paint color/scheme.
- Detect rows of vehicles in a parking area.
- Identify beach terrain suitable for amphibious landing operations.

Rating Level 4:

- Detect vegetation stress/aging in narcotics crops in reported eradication area.
- Identify tennis court as being composed of grass, clay, or rubber/composite.
- Detect CCD efforts (cut vegetation camouflage netting) at suspected coca processing facilities.
- Identify azimuth markings (numbers) on runway.
- Detect tanks and self-propelled guns in revetted positions.
- Detect blast marks from mobile or silo-based ICBM launches on concrete.
- Detect presence of sea land containers on a ship's deck.
- Distinguish between coal and sand loaded on dumb barge.

Rating Level 5:

- Detect individual trees with indications of vegetation stress.
- Identify color of unfurled sails on sailboats (20 to 30 ft long).
- Distinguish between military and civilian helicopter paint schemes.
- Identify large ground forces' equipment by type (e.g., tanks, self-propelled guns, armored recovery vehicles).
- Detect foxholes by ring of spoil outlining hole.
- Detect the presence of sailors in formation on the deck of a large combatant during parade/ review.
- Identify colors of stripes/deck markings on major surface combatants.

Rating Level 6:

- Detect a foot trail through tall grass.
- Identify colored bands on rail cars.
- Identify support personnel performing maintenance while on an aircraft.
- Identify the colors of stack markings on merchant ships.
- Detect the presence of an algae line on the dark surface of a submarine hull.

Rating Level 7:

- Identify medium farm animals by type (e.g., sheep, hogs, goats).
- Distinguish road safety signs by color.
- Detect wing flaps and other articulating surfaces on fighter aircraft.
- Distinguish between open and closed hatches on the turret of an MTLB chassis.
- Detect windsock on helicopter deck.
- Identify canvas covering the muzzles of an ADMG630 gun.

Legend for Appendix D
CA–Canada
FR–France
INT–International
RS–Russia
US–United States of America

APPENDIX E
VIDEO NATIONAL IMAGERY INTERPRETABILITY RATING SCALE

The Video NIIRS is used to document the subjective quality scale for airborne motion imagery in the visible spectrum. When used in this context, "quality" refers to the interpretability or "intelligence value" of a video clip; it is not a measure of esthetic value. The Video-NIIRS is designed to account for differences in resolution, sampling rate (frame-rate), scene complexity, and human activity or behavior (see Motion Imagery Standards Board (MISB) Recommended Practice, Video-National Imagery Interpretability Rating Scale, RP0901.1, approved for public release, NGA Case 09-13715, June 2011).

SCALE DESIGN

The Video-NIIRS is designed to be log-linear in resolution space, meaning that each successive Video-NIIRS level from zero (lowest) to nine (highest) represents a halving of ground sampling distance (i.e., doubling the resolution from Video-NIIRS 3 to Video-NIIRS 4 and so on). It provides criteria tasks for the seven orders of battle or content domains: air forces, ground forces, electronics, missile, naval forces, culture, and security. Some Video-NIIRS levels have more than one criterion example per OOB/content domain.

Each written criterion contains specific components separated by a bullet point to add clarity and aid readers understanding of the content. These components are arranged for each criterion as follows:

- Analyst task. (Verbs like 'track' or 'confirm' infer an analyst's ability to do so consistently over an ensemble of clips of equal quality.)
- Object of interest.
- Associated activity or behavior.
- Environment.
- Object reference examples.

The analyst rates a video clip by determining if he or she can perform the most relevant criteria listed for a particular Video-NIIRS level, but cannot do the same for the next higher level. In other words, if an analyst can perform the Video-NIIRS 4 criteria on a video clip, but cannot perform the Video-NIIRS 5 criteria, the analyst rates the video clip Video-NIIRS level 4.

USING THE VIDEO NATIONAL IMAGERY INTERPRETABILITY RATING SCALE IN ANALYST EVALUATIONS

Video-NIIRS ratings are a measure of interpretability (intelligence value). The ability (or inability) to perform the tasks provided in Video-NIIRS criteria is either possible or it is not possible; therefore, the rating should be given using a whole number. There can and will be significant differences in the visual preferences an analyst may have regarding videos of the same Video-NIIRS rating level. While these preferences may be undefined, they are, by definition, not measures of interpretability. They do, however, represent human factors that can impact the quality of analysis and should be addressed.

These undefined visual preferences are not task based and can be assessed in quality studies using the double-stimulus continuous quality scale method described in International Telecommunications Union-Radiocommunication Sector BT.500-12, *Methodology for the Subjective Assessment of the Quality of Television Pictures*. Any study using Video-NIIRS to extract analyst ratings that are fractional or decimal in nature may not meet the criteria for construct validity.

MOTION IMAGERY DEFINED

Motion imagery is defined as imagery [a likeness or representation of any natural or man-made feature or related object or activity] utilizing sequential or continuous streams of images that enable observation of the dynamic, temporal behavior of objects within the scene. Motion imagery temporal rates are nominally expressed in frames per second and must be sufficient to characterize the desired dynamic phenomena. Motion imagery is defined as including metadata and nominally beginning at frame rates of 1-frame per second (expressed here in Hertz) or higher within a common field of regard. Full motion video falls within the context of these standards (see *Motion Imagery Standards Profile (MISP), version 6.4*).

VIDEO NATIONAL IMAGERY INTERPRETABILITY RATING SCALE CRITERIA BY QUALITY LEVEL

Video National Imagery Interpretability Rating Scale: Level 2

At Video-NIIRS level two, motion imagery data lacks sufficient spatial and/or temporal resolution for intelligence surveillance. For example, high EO-NIIRS still imagery would be rated Video-NIIRS two regardless of spatial resolution, as it provides no dynamic content. High frame-rate video of a resolution too low to discern most human activity would be rated Video-NIIRS zero because it provides insufficient spatial content.

Assuming a suitably wide field of view, gross spatial and temporal resolution motion imagery data could support monitoring of commercial sea lanes (tracking tankers and other large surface ships) as well as conducting macro-pattern analysis of populated regions. Such data may also support dynamic earth sciences, such as oceanography and meteorology.

Video National Imagery Interpretability Rating Scale: Levels 3–11

Table E-1 explains levels 3 through 11 of the Video-NIIRS, according to the Recommended Practice, Video-National Imagery Interpretability Rating Scale.

Order of Battle	Video NIIRS Level 3
AIR FORCES	Track movement of an identified heavy cargo/passenger aircraft during taxi or tow at a primary airfield/airport installation (aircraft length: 50 m or more, e.g., MD11, A300, B747, B767, DC8). Note: Under-resolved smaller aircraft may be evident based on movement or behavior.
ELECTRONICS	Track the movement of a convoy of unidentified radar/radar support vehicles in column formation or road march traveling on an open roadway in the vicinity of a known EW or SAM radar site (four to eight vehicles with total column length 50 m or longer). Note: Vehicles comprising the convoy and other under-resolved vehicles are evident based on movement or behavior.
GROUND FORCES	Track the movement of an unidentified military convoy company sized or larger consisting of armor or mechanized infantry in a column or “road march” on an open highway/roadway (four to eight vehicles with total column length 50 m or longer). Note: Vehicles comprising the convoy and other under-resolved vehicles are evident based on movement or behavior.
MISSILE	Track the movement of a convoy of ICBM transporter and support vehicles during deployment or road march on an improved road near missile base, launch site, or silo (Dong Feng 4, Taepodong 2, Agni V: transporter with support vans—convoy length 60 m or longer). Note: Support vehicles comprising the convoy and other under-resolved vehicles may be evident based on movement or behavior.
NAVAL FORCES	Track the movement of an unidentified coastal patrol craft conducting normal operations at sea several miles beyond a harbor or port (e.g., US Cyclone Class: average 58 m length, 8 m beam). Note: Under-resolved smaller craft may be evident based on movement, behavior, or wake.
CULTURE	Track the movement of an oversized heavy hauler tractor and trailer driving in a convoy on the open highway (movers of houses, cranes, drilling and large earth moving equipment), such as 100-ton, big-rig tractors with multiaxle lowboy special use trailer, total length 40 m to 50 m). Note: Under-resolved smaller trucks may be evident based on behavior.
	Track the movement of an oversized container carrying flatbed railcar in motion at a rail yard (46 m length flatbed rolling stock). Note: Under-resolved smaller trucks or rolling stock may be evident based on behavior.
SECURITY	Track the movement of an unidentified convoy of three or more sea/land containers driving in a column formation exiting a rail yard or port facility, such as big-rig tractors hauling sea/land containers, total convoy length 50 m or more. Note: Under-resolved smaller trucks may be evident based on behavior.

Order of Battle	Video NIIRS Level 4
AIR FORCES	Track movement of an identified large fighter/attack aircraft during taxi or tow at a primary airfield/airport installation (aircraft length: 15 m or longer; e.g., F-15, F-16, Eurofighter, F-22, MIG-29, F-35). Note: Under-resolved smaller aircraft may be evident based on movement or behavior.
	Confirm rotor wash effects of an unidentified light/medium helicopter on tall grass, sand, or dirt during takeoff or landing in the field, at a tactical LZ or forward arming and refueling point (diameter of disturbance: 25 m to 50 m). Note: The helicopter causing rotor wash, as well as other under-resolved aircraft or ground support vehicles may be evident based on movement or behavior.
ELECTRONICS	Confirm movement of large EW radar or signal intercept vehicles and vans with trailers in column/convoy or deploying at or near a known improved electronics site (large flatbed tractor-trailer with mast mounted antennas: 20 m vehicle length). Note: Under-resolved smaller vehicles (vans or cars) may be evident based on behavior.
GROUND FORCES	Track the movement of individual, tracked engineering vehicles and wheeled prime mover/trailer combinations during tactical road march/deployment in the field or on an unpaved road (e.g., engineer recovery vehicles, scissor bridges, tank carriers: average length 15 m to 25 m). Note: Under-resolved smaller vehicles (light trucks, support vehicles) may be evident based on behavior.
MISSILE	Track the movement of an individual ICBM while being transported overland on an improved road near missile base, launch site or silo (Dong Feng 4, Taepodong 2, Agni V: airframe length approximately 20–30 m). Note: Under-resolved smaller support vehicles may be evident based on behavior.
NAVAL FORCES	Track the movement of an unidentified small near-shore or inter-coastal patrol boat conducting normal operations in the coastal or near-shore littoral environment (e.g., US Mark V Special Operations Craft: approximately 85 ft in length, 6 m beam). Note: Under-resolved smaller boats may be evident based on movement, behavior, or wake.
	Track movement of an identified large fighter/attack aircraft during shipboard air operations on the deck of an attack aircraft carrier (aircraft length: 15 m or more, e.g., F-18, Harrier, F-35). Note: Under-resolved smaller aircraft or deck handling equipment may be evident based on movement or behavior.
CULTURE	Track the movement of a large freight/transport vehicle type: 18-wheel tractor-trailer rig, metro-bus, large recreational vehicle driving independently on an urban road in light traffic (commercial freight and public transports: 15 m to 23 m in length). Note: Under-resolved smaller vehicles (cars, sport utility vehicles) may be evident based on behavior.
SECURITY	Track the movement of an individual sea/land container tractor-trailer rig driving independently on a highway in light traffic (commercial freight transports: 15 m to 23 m long). Note: Under-resolved smaller vehicles (cars, sport utility vehicles) may be evident based on movement or behavior.

Order of Battle	NIIRS Level 5
AIR FORCES	Confirm rotation of main rotor blades on an identified medium helicopter during warm up or taxi at a primary airfield/airport installation (rotor-blade diameter: 12 m to 18 m; e.g., RAH66, KA50, AH64, NH90, UH60). Note: Under-resolved ground crew or grouped dismounts may be evident based on movement or behavior.
ELECTRONICS	Confirm movement of a large electronics vehicle's mast and mast-mounted antenna while being raised or lowered at a known improved electronics site (vehicle-/trailer- mounted mast and antenna: mast height 20 m or more). Note: Under-resolved crew members or grouped dismounts may be evident based on movement or behavior.
GROUND FORCES	Confirm the rotation of the turret on a main battle tank as the main gun slews during training, live fire exercise, or combat at a gunnery range, field deployment site, or battle zone (e.g., M1-A2, Challenger-2, Leopard-2, T-80: average chassis 9 m long by 3.5 m wide). Note: Under-resolved dismounts may be evident based on movement or behavior.
MISSILE	Track the movement of an individual mobile SRBM while being transported or during launch preparations on or near a road in the vicinity of a surveyed launch site (mobile Fajr-5 or SCUD: airframe length approximately 10 m to 15 m). Note: Under-resolved dismounts may be evident based on movement or behavior.
NAVAL FORCES	Track the movement of a light riverine/deep inter-coastal patrol boat during operations/patrol in the riverine environment (e.g., light patrol boat or rigid inflatable boat 8 m to 11 m long, 2.5 m to 3 m beam). Note: Under-resolved personal water-craft or swimmers may be evident based on movement, behavior, or wake.
CULTURE	Track the movement of a car, sport utility vehicle, van, or light truck driving independently on roadways in medium traffic (mid and full size cars and trucks: 5 m to 6 m in length). Note: Under-resolved two-wheeled vehicles or dismounts may be evident based on movement or behavior.
SECURITY	Track the movement of a suspect car, sport utility vehicle, or light truck driving erratically/aggressively or employing evasive driving measures on roadways in light traffic (mid and full size cars and trucks: 5 m to 6 m in length). Note: Under-resolved two-wheeled vehicles or dismounts may be evident based on movement or behavior.
Order of Battle	**Video NIIRS Level 6**
AIR FORCES	Confirm movement of control surfaces on an identified heavy cargo/passenger aircraft during preflight checkout or taxi at a primary airfield/airport installation (flaps and ailerons on aircraft having wingspan of 112 m or more; e.g., MD11, A300, B747, B767, DC8).
ELECTRONICS	Confirm the movement of a vehicle- or building- mounted parabolic mesh antenna as it slews or rotates at a known improved electronics site (e.g., parabolic mesh antennas, approximate diameter of 30 ft).
GROUND FORCES	Confirm the movement/operation of crew-served or vehicle-mounted antiaircraft systems as the launchers/guns slew to an aimed firing position during operation at a riveted, defensive field position (e.g., Avenger, Tunguska M1, Rapier: launcher pods average 2 m–3 m long).
MISSILE	Confirm the movement of vans, cranes/hoists supporting a mobile SRBM during maintenance, transloading, deployment preparation at a garrison or field maintenance facility (e.g., support vans and equipment lengths approximately 3 m to 5 m).

Order of Battle	Video NIIRS Level 6–Continued
NAVAL FORCES	Confirm the movement of a deck-mounted defensive armament as it slews and elevates to aim and fire on the surface combatant, cruiser, or frigate (e.g., 20 mm and 40 mm guns and mounts/ turrets, average diameter of 5 m to 6 m).
CULTURE	Track the movement of a full sized motorcycle driving independently on roadways in medium traffic (large cruising motorcycle, 2.5 m in length). Note: Under-resolved dismounts may be evident based on behavior.
SECURITY	Track the general movement of groups (25+) of under-resolved dismounts as they cross the street at a busy intersection in an open public square or pedestrian thoroughfare (i.e., commuters, shoppers, or event participants).
Order of Battle	**Video NIIRS Level 7**
AIR FORCES	Confirm the movement of control surfaces on an identified light transport aircraft during preflight checkout or taxi at an international or municipal airfield/airport installation (flaps and ailerons on aircraft having wingspan of 18 m or less; e.g., Beech Model 200 Super King Air, flaps approximately 0.75 m to 2.5 m in length).
	Confirm heat distortion waves/effects from the exhaust plume of a large fighter jet during warm up or taxi at a secondary/dispersal airfield (diameter of visible distortion approximately 5 m to 10 m).
ELECTRONICS	Confirm movement of large access panels as they are opened or closed on a site or field deployed electronics/radar van or mobile hut (individual panels of 2 m to 2.5 m diameter).
GROUND FORCES	Confirm the movement/operation of crew-served or vehicle-mounted antiarmor weapons as the launcher is aimed or slews to its firing position during live fire exercise or combat at a gunnery range, field deployment site, or battle zone (TOW 2, Milan, Javelin: launcher 1 m to 1.5 m in length).
MISSILE	Confirm the movement of the crew supporting a mobile SRBM during maintenance or launch preparations at a maintenance facility or launch site (individuals of average height and weight).
NAVAL FORCES	Confirm the movement of unidentified deckborne objects as they are dumped over the side or stern of any surface ship or fishing vessel at sea (e.g., container drums, bales, crab traps 2 m to 2.5 m diameter).
CULTURE	Confirm the movement of a car hood/bonnet or deck-lid/trunk/boot as it is opened or closed while stopped along a roadway or street (conventionally hinged midsize car hood or deck-lid).
SECURITY	Isolate pockets of unrest/potential violence in large groups (50+) of otherwise peaceful dismounts as they demonstrate or protest in an open public square or pedestrian thoroughfare (i.e., political demonstrators, bystanders, observers, security forces).
Order of Battle	**Video NIIRS Level 8**
AIR FORCES	Confirm the movement of individual pilot(s) or flight crew conducting external pre-flight checkout at a tactical/dispersal airfield or forward operating base (individuals of average height and weight).
ELECTRONICS	Confirm movement of individual crewmembers entering or exiting hatches or climbing ladders on a site- or field-deployed electronics/radar van or mobile hut (individuals of average height and weight).
GROUND FORCES	Confirm the movement of an individual holding a shoulder fired antiaircraft missile as the launcher is raised to the aimed firing position in the field, in a defensive position, or in the vicinity of an airfield or airport approaches (Stinger, SA-16/18-IGLA: launch tube average length is 1.7 m).
MISSILE	Track the movement of an individual member of a Katyusha rocket crew during transportation and deployment en route to/near a launch site (individuals of average height and weight).

Order of Battle	Video NIIRS Level 8–Continued
NAVAL FORCES	Confirm the movement of individual deck crew handling seaborne mines as they are readied for deployment off the stern of any surface ship/boat, especially a noncombatant modified/co-opted for terrorist or military use (seaborne mines, approximate 1 m in diameter).
CULTURE	Confirm the movement of a car door as it is opened or closed while stopped along a roadway or street (conventionally hinged midsized car door).
SECURITY	Isolate and track the movement of small subgroups (associates) in a larger crowd of people as they walk in an open public area or pedestrian walkway (i.e., subgroups of 2 to 5 individual pedestrians in a crowd of 20 or more, based on movement and proximity).
Order of Battle	**Video NIIRS Level 9**
AIR FORCES	Consistently track the movement of the body and arms of ground/flight crew member hand lock/unlock an external panel, hatch or compartment on any aircraft at any airfield or base (individuals of average height and weight).
ELECTRONICS	Consistently track the movement of an individual's body and arms while using an unidentified portable handheld communications device in an open public area or pedestrian walkway (individual of average height and weight holding device up to ear or bringing hands together for text entry).
GROUND FORCES	Consistently track the movement of the body and arms of an individual holding a long rifle or sniper rifle as the weapon is raised to an aimed firing position—either standing, sitting, or prone at a practice range, during live fire exercise, or during an engagement (e.g., Barrett M82-A1, Remington Model 700 series: 1 m to 2 m in overall length).
MISSILE	Consistently track the movement of an individual Katyusha crew member's body and arms during set up and launch preparation at a tactical launch site in a rural or urban environment (Individuals of average height and weight).
NAVAL FORCES	Consistently track the movement of an individual deck crew's body and arms as they conduct a patrol or operations on a light surface combatant; i.e., patrol boat (individual of average size and weight).
CULTURE	Consistently track the movement of a pedestrian's body and arms as he walks in a busy public area, market, or walkway (individual of average height and weight).
SECURITY	Confirm a conversation is underway based on the movement of the body and arms of participants as they walk or stand in an open public area or pedestrian walkway (i.e., subgroups of two to three individual pedestrians speaking among a meandering crowd of 20 or more).
Order of Battle	**Video NIIRS Level 10**
AIR FORCES	Confirm the movement of the hands and forearms of a ground crew/mechanic using an identified hand tool or power tool while servicing any aircraft or support vehicle at any airfield, base, or aircraft maintenance facility (individual of average size using socket wrench or power driver with length of 0.15 m to 0.3 m).
ELECTRONICS	Confirm movement of an individual's hands and forearms holding a visible handheld communications device in the process of sending/receiving information (e.g., speaking, text-messaging) in an busy public area or pedestrian walkway (cell phone or personal data assistant average diameter 0.1 m to 0.15 m).
GROUND FORCES	Confirm the movement of the hands and forearms of an individual holding a compact assault weapon or large frame handgun as the weapon is raised to an aimed firing position—either standing, crouched, or prone—at a practice range, during live fire exercise, or during an engagement (MP-5, AK74, Colt Commando, UZI, M-1911: 0.25 m to 0.8 m overall length).
MISSILE	Confirm the movement of an individual Katyusha crew member's hands and forearms while connecting leads/wires between rockets and trigger mechanism at a tactical launch site in a rural or urban environment (individuals of average height and weight).

Order of Battle	Video NIIRS Level 10–Continued
NAVAL FORCES	Confirm the movement of individual deck crew member's forearms and hands as he performs weapons check of pedestal mounted arms on a patrol boat in a riverine environment (individual of average size and weight manning a mounted .50 cal. or MK19 grenade launcher).
CULTURE	Confirm the movement of a pedestrian's forearms and hands as they make a purchase from a street vendor in a busy open market or square (individual of average height and weight, exchanging payment for goods).
SECURITY	Confirm an individual is speaking based on the movement of an individual's head and mouth as they engage in a conversation in an open public area or pedestrian walkway (i.e., determine if a person is speaking based on head and mouth movement).
	Confirm the movement of an individual's forearms and hands as they gesture or sign in an open public area or pedestrian walkway (i.e., confirm/read gestures or body language while subject is conversing, or partially interpret sign language).
	Confirm the functions of individuals based on the movement of body, head, forearms, and hands as a protected individual is moved to or from a vehicle/motorcade or in an open public area (i.e., isolate behavior to determine the function of individuals in a small group: armed security, principals, and VIPs).
	Confirm the exchange of a parcel based on the movement of the hands and forearms of two individual pedestrians as one walks past the other in a crowded public area or pedestrian walkway (i.e., confirm the exchange of a letter-sized envelope between two pedestrians in a crowd).
Order of Battle	**Video NIIRS Level 11**
AIR FORCES	Confirm the movement of the fingers/hand of a ground crew/mechanic changing the socket on a ratchet/socket wrench while servicing any aircraft or support vehicle at any airfield, base, or aircraft maintenance facility (socket able to fit in palm of workers hand).
ELECTRONICS	Confirm movement of an individual's mouth/jaw while speaking into a Bluetooth wireless mobile phone earpiece in a crowded public area or pedestrian walkway (average-sized person wearing an over the ear device with internal or boom microphone, average diameter: 2.5 cm to 5.0 cm).
GROUND FORCES	Confirm the movement of the fingers and hands of an individual holding a fragmentation grenade as the weapon's safety is released and the device is readied at a practice range, during live fire exercise, or during an engagement (spherical or cylindrical device, palm sized with metal pull ring/pin and spring loaded spoon: 6 cm to 8 cm diameter).
MISSILE	Confirm the movement of individual's fingers and hands while aiming a shoulder-fired antitank missile as they release safeties and arm the device at a tactical position in a rural or urban environment (individuals of average height and weight holding AT-4 or RPG).
NAVAL FORCES	Confirm the movement of an individual combat swimmer's hands and fingers as they check out and test scuba equipment on a light surface combatant; i.e., patrol boat near the littoral zone (individual of average size and weight).
CULTURE	Confirm the movement of a pedestrian's hands and fingers as they make change or sort coins in a busy open market or square (individual of average height and weight, sorting coins in a change purse or the palm of one hand).
	Confirm the movement of a pedestrian's hands and fingers as they communicate through sign language in an open public area (i.e., fully interpret sign language to include the spelling out of individual letters).

Order of Battle	Video NIIRS Level 11–Continued
SECURITY	Isolate and investigate an individual or group based on the movement of their hands, fingers, and face as they observe the movement of a protected individual from a crowd behind a rope line or police barrier (i.e., isolate behavior to determine if an individual or individuals pose an immediate threat to a VIP).
	Isolate and investigate an individual apparently burdened with significant concealed weight, based on his gait, posture, hands, fingers, and overall body language as he meanders into a crowd in a public square, market, or shopping mall (i.e., based on gait, determine if an individual is a public threat or concealing an explosive vest or belt).
	Isolate suspicious movement/behavior of the hands and fingers of a suspect individual or known operative as they leave an inconspicuous signal or message on a light pole or mailbox in a crowded urban street (i.e., traditional espionage tradecraft: a chalk mark or sticker on a predetermined location to signal a meeting or dead drop).

Legend:
cal–caliber
cc–cubic centimeter
LCAC–landing craft air cushion
VIP–very important person

APPENDIX F
IMAGERY INTELLIGENCE REPORT FORMATS

Reconnaissance Exploitation Report Example

PAGE 1 EXREP 15TH 102 CLASSIFICATION:_____ 831122 03346

UNCLASSIFIED EXERCISE NEVERLAND

MSG ID/RECCEXREP/15TH/NO2222/3456

EFDT: 230442Z DEC 90

NARR: REF ITMOOS, LG ACTY NOTED THROUGHOUT TGT AREA

ITEM P6

ITM: 001 0380EX0000 CTY: MS 363219M1263214E

A. 52SDR46118324

B. 230422ZDEC90

C. CAT: 06 Command Post.

1. Mobile command post.
2. Static, camouflaged.
3. 10 T-62 tanks, 3 M-1979 self-propelled guns, 5 UAZ69As, 5 LG tents, 2 spoonrests, 50 PERS (count approx).
4. No defense noted.
5. Terrain is flat with little vegetation, approx 13 km SE of post, a AAA site was noted.

D. NO REPORT TO FOLLOW

1. ACFT was fired upon AAA site.
2. 0081X.
3. Yes.

PAGE 1 EXREP 15TH 102 CLASSIFICATION:_____ 831122 03346

Initial Photographic Interpretation Report and Supplemental Photographic Interpretation Report Format

PRECEDENCE

FROM: IIIC

TO: REQUESTOR

INFO:

REF: (a) As applicable.

(A) CLASSIFICATION

(B) SECTION 01 OF 01 SECTION

(C) IPIR: FIRST IIP SER: UVO157 PRJ: RD MSN: Z198A DTZ: 75022W

(D) IMAGE QUALITY RANGE WAS GOOD TO EXCELLENT. EIGHT OF TWELVE OF THE COLLECTION REQUIREMENTS WERE SATISFIED.

(E) PART I. MISSION HIGHLIGHTS

(F) NO EVIDENCE OF SURFACE-TO-SURFACE MISSILES OR RELATED ACTIVITY WAS NOTED. VEHICULAR AND TROOP MOVEMENT ACTIVITY IS VERY LIGHT. NO ANTIAIR ACTIVITY OR REACTIONS TO THE RECONNAISSANCE PLATFORM WERE OBSERVED.

(G) PART II. SIGNIFICANT RESULTS

(H) 1. PERISHABLE ITEMS

(I) ITMOOA: 0213-OOOOO CAT: 80000 AIRCRAFT IN FLIGHT

(J) REQ: CTY: LA211929N1061934E UTM: MRG:

(K) STA: TRM AI NRG:

(L) AOB:

0001 CONF PA-23 INFLIGHT HDG NORTHEAST

(M) IMR: PAN FRM: 1011, 1012 URG

AID: E AO CL BB FRM TOT: 1035Z

(H) 2. NEW ITEMS

(I) ITM002: 0213UV0006 CAT: 87200 PURTEE SAM SITE

(J) REQ: CTY: LA210815N1055619E UTM: MRG:

(K) STA: UCO

(L) DES: SA-O SITE IS BEING ESTABLISHED APROX ONE-HALF KM FROM THE RED RIVER. SITE CONSISTS OF SIX RVTD PSNS IN A STAR FORMATION. FULL DESCRIPTION NOT YET POSSIBLE. NO EQUIPMENT EXCEPT FOR CONSTRUCTION AND GROUND FORCE RELATED WAS IN THE AREA.

GFW:

0008 CONF DUMP TRUCK

0001 CONF ZAZ-7 CRANE

0001 PROB A-2 TRACTOR URG:

(O) IMR PAN FRM: 976-980 TOT: 1039Z

AID: G AO SC SH BB

(H) 3. CHANGE AND OOB ITEMS

(I) ITM OO2: 0213-02351 CAT: 09100 WATERTON BARRACKS AREA

(J) REQ: 4A02316 CTY: LA221600N1053012E UTM: MTG:

(K) STA: OPR AI NAC DQ B1236 750102 NRG: NDA04/0014/5

(L) RMK: PREVIOUSLY REPORTED U/I ARMORED EQUIPMENT HAVE NOW BEEN IDENTIFIED AS SWG-99 TANKS.

GFW: AREA A-REGT A

0103 CONF SWG-99 TANK

0092 CONF DTR-12 TRUCK

0002 CONF MT-3 CRANE

GFW: AREA B-REGT AREA NAC DQ B1236 750102

GFW: AREA C-REGT AREA NAC UP 298A 741209

GFW: AREA C-AAA BN NAC UP 208A 741209

(M) IMR: PAN FRM: 500.490-516 URG: 234118

AID: G AO CL BB FRM: 135-138 TOT: 1025Z

IDC: 221615N1053045E MPR:

(N) EQM

(O) PART III. OTHER RESULTS

(P) Mission Requirements

(Q) Categorization of Target Entries. An introductory statement is written here categorizing a set of like items to increase readability. Defense Intelligence Agency Manual (DIAM) 57-5, *DOD Exploitation of Multisensor Imagery*, contains more detailed information on the structure of part III.

(R) PART IV. COLLECTION OBJECTIVES SATISFIED AND NOT SATISFIED

Paragraph Instructions for Initial Photographic Interpretation Report and Supplemental Photographic Interpretation Report Format

The following are instructions for completing each paragraph of an IPIR and SUPIR.

> ***Note:*** Information in parentheses is shown for explanation only. Line identification is not shown on an actual message. The IPIR/SUPIR/ multimission imagery photo interpretation report (MIPIR) format has been revised to accommodate the growth of automated intelligence systems. However, as a user's guide to understanding the reports, the following definitions are provided.

Cable Line.

References.

(A) Self-explanatory.

(B) Self-explanatory.

(C) Report type identifies the following:

- Reporting organization.
- Report number: reports will be numbered sequentially by the producing unit. (A two-character alpha unit identifier followed by a four-digit sequential number.)
- Reconnaissance project identification: Two characters indicating the project of which this mission is part. This stands for mission independent.
- Mission number.
- Date/time zone.

(D) General Mission Statement. Free text reporting information applying to the entire mission, such as graphic reference, sensors, sensor on/off times and coordinates, overall image quality, overall image scale range, other general mission data, or any other information deemed useful. If the objectives of the mission and the requesting authority can be given (consider length and classification), these will be included. The general mission statement will be written as the interpreted mission and appropriate data will be reported.

(E) Part I. MISSION HIGHLIGHTS. Title for first major division of the report.

(F) Textual Data for Mission Highlights. Part I, Mission Highlights allow for a concise free text statement of the significant information derived from the mission. It may be used to highlight individual items reported elsewhere in the message and to summarize information relative to a category of targets. Mission highlights may also be utilized for summations of trends of individual categories, such as logistic studies or combat information of a significant nature.

(G) Part II. SIGNIFICANT RESULTS. Title for second major division of the report.

(H) Categories of Items That May be Reported.

1. Perishable Items. This section is for items of perishable intelligence value, including transitory targets.

2. New Items. This section is for items upon which the reporting organization has no previous image-derived data.

3. Change and OOB Items. This section is for items that reflect significant changes since the last available interpretation and targets for which OOB is required. For DOD combat reconnaissance programs, this section includes mission requirement objectives. A mission objective could also be reported under perishable items of damage assessment.

4. Bonus Items. This section includes significant changes to any known installation that is not a specified mission requirement objective.

5. Damage Assessment. This section is for the description of damage to targets from nonnuclear attacks. This section includes known strike objectives not damaged.

(I) Identification data:

- Item number.
- Basic encyclopedia (BE) number or imagery basic encyclopedia number.
- Functional classification code. See DIA Publication 5210.002-M, *Standard Coding Systems Functional Classification Handbook*.
- Installation name or description of object imaged.

(J) Other identification data:

- Requirement number.
- Country code.
- Geographic coordinates.
- Universal transverse mercator coordinates.
- Military district. Entered when applicable.

(K) Status/activity data:

- NEG. Negated (nonexistent). Target/installation does not exist at or near the coordinates given in the requirement.
- UCO. Under construction.
- COM. Complete. The target/installation appears to be externally complete. Appears capable of operating but operational status cannot be determined.

- UNK. Unknown. Status of the target cannot be determined.
- NOP. Not operational. Essential elements of a target/installation are observed not to be in operation; equipment essential to the operation of the installation is either missing or observed as not to be operational.
- OPR. Operational.
- OCC. Occupied.
- DEC. Deception.
- UNP. Unoccupied.
- ABN. Abandoned.
- RMV. Removed. Target/Installation has been razed, dismantled, or moved.
- TRN. Transitory. Fleeting targets or targets that appear to be only temporarily situated.
- DMG. Damaged. Target is damaged to some extent, but it may be restored to usable condition.
- DST. Destroyed. Target is so damaged that it cannot function as intended or be restored to usable condition.
- CNA. Coverage not available.

Exploitation Level:

- AI - IPIR
- AS - SUPIR
- MI - MIPIR

Significance. The significance code indicates the interpreter's assessment of the degree of change in the installation status, capability, or function since previous mission coverage. If a significance code in entered, the reference mission number and date will be entered. Codes are as follows:

- NEW. Newly detected activity.
- SIG. Significant change has occurred.
- UNK. Significance of change is not known or change, if any, cannot be determined.
- NAC. No apparent change.

Reference Graphic. When a national basic reference graphic exists, the number may be required for specific programs. In all other cases, it will be left blank.

(L) Additional Interpretation Data. Additional photo interpretation data will be organized under one of the following codes:

- DES. Physical description. A DES will be accomplished when an installation is covered for the first time, a basic description of the installation has not been previously written, the installation reflects a significant physical change, or first reporting an installation as abandoned or destroyed.
- RMK. Remarks. This prefix will be used when providing less than a complete description of a known target/additional explanatory comments relating to status/activity. Only a DES or RMK

will be used for each entry, not both. If NAC is entered on the status line, a DES will not be used. The remark will include the project code and mission numbers of the coverage used to prepare the report in those cases where more than one mission is used. For MIPIR, the actual OOB count will be taken from a representative mission flown during the reporting period.

Order of Battle Designations:

- MIS. Missile and missile related equipment.
- AOB. Air OOB.
- NVL. Naval and merchant vessels.
- GFW. Ground force weapons and equipment.
- ELC. Electronic OOB.
- AAA. Antiaircraft OOB.
- DMY. Dummy.
- OBJ. Associated objects. Information relative to objects and equipment not reported under OOB entries.

Area Delineation. Refers to area delineation of the national basic reference graphic or other descriptive location data. When reference graphics are not available, location reporting is permitted (e.g., assembly area). Multicoverage dates may be included following each location entry or as unique entries.

(M) Imagery Reference Data (IMR). A minimum of one IMR line is required; however, more lines may be required to indicate different coverage. For MIPIR, only those missions that contributed to a specific degree are entered on the IMR line. Initial information in the IMR line may include date of coverage, project code, mission number, and camera station. The following coded items may then be used:

- IMR. Frame number.
- SLR. Side-looking radar.
- INF. Thermal.
- URG. Universal reference grid. Six position URG coordinates.
- AID. Additional imagery data. AID is used to provide interpretability data. Interpretability codes are as follows:
  - E-Excellent.
  - G-Good.
  - F-Fair.
  - P-Poor.

Extent of Coverage and Mode:

- A-Complete coverage/stereo.
- B-Complete coverage/partial stereo.

- C-Complete coverage/mono.
- D-Partial coverage/stereo.
- E-Partial coverage/partial stereo.
- F-Partial coverage/mono.

Type of Coverage:

- O-Oblique.
- V-Vertical.

Weather Conditions:

- CL-Clear.
- SC-Scattered.
- HC-Heavy Clouds.
- HA-Haze.

Other Conditions:

- SN-Snow.
- SH-Shadow.
- OL-Degrading obliquity.
- SD-Semidarkness.
- BL-Blurred image.
- TR-Terrain masking.
- HD-Heavy smoke/dust.

Type of Film:

- B-Black and white.
- C-Natural color.
- G-Green record.
- I-Color rear infrared.
- R-Red record.
- T-Thermal.
- S-Radar.
- N-Nonstandard.

> ***Note:*** For stereo or partial stereo, two letters will be used, one for the first frame and one for the second frame; e.g., BB, black and white on both frames.

- FRM. Additional frame reference for a given target.
- TOT. Time on target.
- IDC. Imagery derived coordinates, derived from comparing imagery with a map or chart.
- MPR. Map reference.
- PPC. Precision photo derived coordinates.

(O) Part III. OTHER RESULTS. Third major division of the report, as indicated by the sample; part III may be omitted.

(P) Mission Requirements. Provides for reporting items/targets not properly placed in part II.

(Q) Categorization of Target Entries. The format in part IV will contain collection objectives satisfied and not satisfied, plus a textual statement indicating any reasons for nonsatisfaction. Items contained in part IV can be understood from the codes listed earlier.

(R) Part IV. COLLECTION OBJECTIVES SATISFIED AND NOT SATISFIED. Part IV of the format will contain collection objectives satisfied and not satisfied, plus a textual statement indicating any reasons for nonsatisfaction. Items contained in part IV can be understood from the codes listed earlier.

APPENDIX G
EXAMPLE OF A MARINE UNMANNED AERIAL VEHICLE SQUADRON EQUIPMENT AND PERFORMANCE CHARACTERISTICS

SHADOW UNMANNED AIRCRAFT SYSTEM

The Shadow UAS consists of the following:

- Shadow UAS aircraft (see fig. G-1 on page G-2).
- Ground control station (see fig. G-2 on page G-2). The ground control station provides control of air vehicle and payload out to 125 km.
- Pneumatic launcher (see fig. G-3 on page G-3).
- Portable ground control station.
- Ground data terminal tracking system consists of track control unit on a pedestal antenna assembly and an interrogator unit. This system provides communication between aircraft and ground control station.
- Tactical automatic landing system. The airborne system consists of transponder onboard aircraft. This system provides for automatic landing guidance and control of the aircraft.
- Portable ground data terminal.
- Remote video terminal.
- Modular mission payload.

Figure G-1. Shadow Aircraft with Unmanned Aircraft System.

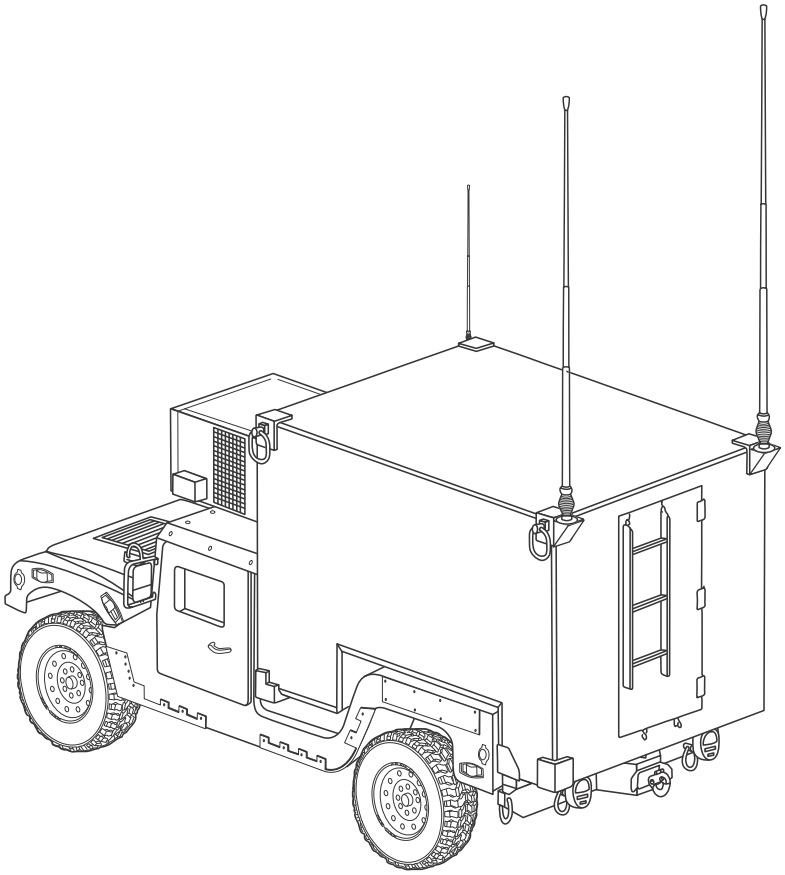


Figure G-2. Shadow Ground Control Station.

SHADOW UNMANNED AIRCRAFT SYSTEM CHARACTERISTICS

Figure G-3. Shadow Unmanned Aircraft System on Pneumatic Launcher.

Table G-1. Shadow Unmanned Aircraft System Characteristics.

Engine Limitations	
Maximum Operational	8,000 RPM for 2 minutes
Maximum Continuous Climb	7,800 RPM
Maximum Continuous Cruise	7,500 RPM
Minimum In-Flight	3,800 RPM
Maximum Static Full Throttle	7,200 RPM
Minimum Static Full Throttle	6,300 RPM
Rotor Temperature Operating Range	64°C–175°C
Maximum Continuous Cylinder Head Temperature	259°C for 2 minutes in a climb
Maximum Transient Cylinder Head Temperature	249°C
Minimum Cylinder Head Temperature	80°C
Static Idle RPM (Payload and IFF On)	3,600 RPM–3,840 RPM
Bus Voltage	
Bus Voltage (with engine operating)	26V–30 volts
Battery Fail	less than 19 volts
Airspeed Limitations	
TALS Automatic Abort High	78 kts for 2 seconds
TALS Automatic Abort Low	52 kts for 2 seconds
Low Airspeed Alert	55 kts
Turbulence (Rough Air)	70 kts
Maximum Airspeed Limits	60 kts–110 kts
Altitude Envelope	
Minimum Safe FTS Deploy	1,000 ft AGL
Minimum Altitude	Electric line of sight
Service Ceiling	15,000 MSL
Maximum Launch Altitude	9,000 density altitude
Wind Limitations (Takeoff and Landings)	
Maximum Headwind/Crosswind	20 kts gusting 25 kts
Maximum Tailwind For Launch	IAW maximum tailwind for launch and minimum precharge pressure tables
Maximum Tailwind Upon Selecting “Land AV”	0 kts
Maximum Tailwind During TALS Auto Recovery	5 kts

Legend:
AV–air vehicle
AGL–above ground level
°C–degrees Celsius
FTS–flight termination system
IAW–in accordance with
IFF–identification, friend or foe
kts–knots
MSL–modified surf limit
RPM–revolutions per minute
TALS–tactical automated landing system

APPENDIX H
REQUEST FORMATS FOR
AERIAL IMAGERY COLLECTION MISSIONS

Joint Tactical Air Reconnaissance/Surveillance Request Format Example

PRECEDENCE

FROM:

TO:

INFO:

CLASSIFICATION

SUBJ: JTAR/S REQ

L. REQUEST NO.___ PREPLANNED A. PRIORITY___ B. PRECEDENCE ___

___IMMEDIATE C. PRIORITY___

M. DATE/TIME FACTORS

1. DATE MISSION DESIRED
2. TOT (IF REQUIRED)
3. LTIOV
4. PRIOR COVERAGE ACCEPTABLE (DAYS PRIOR)

N. TYPE RECON REQUESTED

1.TYPE MISSION

A. VISUAL

B. IMAGERY

C. ELECTRONIC

2. TYPE COVERAGE

A.PINPOINT

B.STRIP/LINES OF COMMUNICATION

C.ROUTE RECONNAISSANCE

D.AREA SEARCH

E.AREA COVERAGE

F.AFLOAT

3. *SENSOR TYPE

A. OPTICAL

B. INFRARED

C. SLR

D. ELECTRONIC

E. LASER

F. OTHER

4. * TYPE PHOTO

A. VERTICAL

B. OBLIQUE

C. PANORAMIC

5. * TYPE FILM

A. BLACK AND WHITE

B. COLOR

C. CAMOUFLAGE DETECTING

6. STEREO PHOTO

A. NOT REQUIRED

B. REQUIRED

O. MAP REFERENCE

TYPE AND SCALE_____

SERIES_____

SHEET_____

EDITION_____

DATE_____

P. TARGET COORDINATES

1. UTM

2. LAT/LONG

3. OTHER (SPECIFY)

Q. TARGET CATEGORY/PRIORITY INTELLIGENCE REQUIREMENT(S) (SEE DETAILED INSTRUCTION)

1. AIRFIELD

2. ARMOR/ARTILLERY/TROOPS/VEHICLE

3. BRIDGE

4. DEF POS/STRONG PT [primary target]/GUN

5. ELECTRONIC SITE

6. HARBOR SITE

7. INDUSTRIAL

8. LOC

9. MIL. INST/STORAGE AREA

10. MISSILE SITE

11. POWER PROD. FACILITY

12. RAILROAD YARD

13. SHIPS

14. OTHER (SPECIFY)

R. REPORTS

1. IN-FLIGHT REPORT (CS/FREQ)_____ VALID FM_____ Z TO_____ Z

(CS/FREQ)_____ VALID FM_____ Z TO_____ Z

2. MISSION REPORT

3. RECEXREP

4. IPIR

5. SUPIR

S. IMAGERY PRODUCTS (IF REQUIRED)

1. TYPE

2. QUANTITY

3. ADDITIONAL INFORMATION

T. DELIVERY ADDRESS

1. UNIT_____

2. AIR DROP (IF REQ): COORDS:_____

CALL SIGN/FREQ_____

RUN HEADING (MAG) (OPTIONAL)_____

U. REMARKS/SPECIAL INSTRUCTIONS

1. TARGET AREA CONTROL (CALL SIGN/FREQ)_____

2. OTHER (SPECIFY)_____

Note: Designate minimum mandatory items for immediate requests. An * indicates use as applicable or when known. The format provided has been published as STANAG 3277 and has been approved by NATO as a

standard format for aerial requests. The letters A through K have special significance for certain organizations and are purposely omitted. When submitting message JTAR/S, the paragraph headings are not required, but the alpha-numeric paragraphs will not be changed. Instructions for completing a JTAR/S follow in this appendix.

Paragraph Instructions

The following are instructions for paragraphs L through U of a JTAR/S request.

L. REQUEST NUMBER: As directed.

A&C Priority: Use numerical designation below to define the tactical urgency for preplanned and immediate requests.

PRIORITY: It is the responsibility of the requestor to establish the priority.

Priority No.	Definition:
1	Takes precedence over all other requests except previously assigned Priority 1 requests. The results of these requests are of paramount importance to the immediate battle situation or objective.
2	The results of these requirements are in support of the general battle situation and will be accomplished as soon as possible after Priority 1 requests. These are requested to gain current battle information.
3	The results of these requests update the intelligence database but do not affect the immediate battle situation.
4	The results of these requests are of a routine nature and will be fulfilled when the reconnaissance effort permits.

M. DATE/TIME FACTORS

1. Self-explanatory.

2. State the TOT only when required and justify U2.

3. Indicate the LTIOV, if it is a factor. Deliver prior to this date/time.

4. Self-explanatory.

N. TYPE RECONNAISSANCE REQUESTED

1. Type of Mission (self-explanatory).

2. Type of Coverage.

   a. Pinpoint (self-explanatory).

   b. Strip/LOCs (search continuous photography of a route of LOC).

   c. Route Reconnaissance (visual reconnaissance of a route of LOC with photo of targets of military significance).

d. Area Search (visual search of a specified area with photos of targets of military significance).

e. Area Coverage (photographic coverage of a specified area).

f. Afloat (reconnaissance of vessels afloat).

Numbers 3, 4, and 5 are self-explanatory. These lines should be left blank unless it is fully understood what the selected sensor, photo, and film can accomplish.

O. MAP REFERENCE (self-explanatory).

P. TARGET COORDINATES. Provide reference system used and indicate actual coordinates.

Q. TARGET CATEGORY/PRIORITY INTELLIGENCE REQUIREMENT(S). Provide the appropriate category and indicate the desired PIR by selecting the number(s) from the target list category below.

CATEGORY 1—AIRFIELD

A. Activity: number, type, and location of aircraft.

B. Runways: number, orientation, and surface type.

C. Taxiway and parking areas: location and shape.

D. POL: number, size, and location.

E. Ammunition storage areas: number and location.

F. Hangars: number, size, and type of construction.

G. Electronic facilities: number, type, and location.

H. Defenses: number, type, and location.

I. Other: (specify).

CATEGORY 2—ARMOR/ARTILLERY/TROOPS/VEHICLES

A. Type: infantry, armor, engineering, artillery, etc.

B. Number and type of vehicles.

C. Number and type of armor.

D. Number and type of artillery.

E. Activity: direction of movement, dug in, etc.

F. Terrain: description.

G. Other: (specify).

CATEGORY 3—BRIDGE

A. Purpose: flood, rail, over road, etc.

B. Type: railroad, vehicular, agricultural, etc.

C. Construction: wood, steel, concrete, etc.

D. Construction: piers, abutments, approaches, stringers, beam, truss, etc.

E. Number of spans.

F. Length and width (height if significant).

G. Number of lanes/tracks.

H. Bypass in vicinity of bridge.

I. Activity.

J. Other: (specify).

CATEGORY 4—DEFENSIVE POSITIONS/STRONG POINTS/GUNS

A. Type and size of position or fortification.

B. Type weapons: number.

C. Fire control system.

D. Supporting positions.

E. Transportation access.

F. Routes of ingress and egress.

G. Nature of surrounding terrain and foliage barriers.

H. Activity.

I. Other: (specify).

CATEGORY 5—ELECTRONIC SITE

A. Type of site: microwave relay, EW, etc.

B. Antennas: number and type.

C. Mobile or permanent.

D. Primary buildings and support equipment.

E. Activity.

F. Security measures.

G. Size of area.

H. Other: (specify).

CATEGORY 6—HARBOR/PORT FACILITIES

A. Type port: maritime or inland waterway.

B. Activity.

C. Berthing and cargo handling facilities.

D. POL facilities: type, number, and locations.

E. Storage facilities.

F. Shipbuilding and repair facilities.

G. Transportation.

H. Defenses.

I. Other: (specify).

CATEGORY 7—INDUSTRIAL SITE

A. Type of industry.

B. Size of area.

C. Buildings: number, size, and construction.

D. Open storage: quantity by type.

E. Activity.

F. Transportation facilities.

G. Source of power.

H. Defenses.

I. Other: (specify).

CATEGORY 8—LINE OF COMMUNICATIONS

A. Type: road, rail, canal, etc.

B. Description of the route.

C. Chokepoints.

D. Significant activity.

E. Significant static targets.

F. Other: (specify).

CATEGORY 9—MILITARY INSTALLATIONS/STORAGE AREAS

A. Function: assembly, administration, barracks, depot, etc.

B. Activity: number of vehicles and/or personnel.

C. Size of the area.

D. Number of buildings: predominant construction only.

E. Storage: type and location.

F. Transportation.

G. Defenses.

H. Other: (specify).

CATEGORY 10—MISSILE SITE

A. Type.

B. Launch site: mobile/fixed, number of pads, etc.

C. Number and orientation of launchers/number loaded.

D. Control center: location and construction.

E. Number, type, and location antenna(s).

F. Auxiliary equipment.

G. Activity.

H. Defenses.

I. Other: (specify).

CATEGORY 11—POWER PRODUCTION FACILITY

A. Type: nuclear, coal, oil, hydroelectric, etc.

B. Size and construction.

C. Boiler/generators: number and location.

D. Transformer yard: size and location.

E. Cooling towers: number and location.

F. Penstock/turbine outlet (hydroelectric).

G. Activity.

H. Defenses.

I. Other: (specify).

CATEGORY 12—RAILROAD YARD

A. Type: classification, repair, other.

B. Length and width: chokepoint to chokepoint.

C. Number of tracks.

D. Facilities: repair shops, roundhouses, other.

E. Rolling stock.

F. Defenses.

G. Other: (specify).

CATEGORY 13—SHIPS

A. Class/type/number.

B. Heading/movement.

C. Nationality.

D. Identification.

E. Cargo.

F. Activity.

G. Other: (specify).

CATEGORY 14—OTHER

Narrative report is rendered under this heading in sufficient detail to ensure that the request or purpose of the mission is satisfied.

R. REPORTS.

1. In-flight report to friendly units.

2. Mission report of the results and significant sightings gathered.

3. Reconnaissance exploitation report, a brief, concise, high priority report on time-sensitive targets of significant tactical importance of a perishable nature.

4. IPIR that contains intelligence on mission objectives and additional significant intelligence.

5. SUPIR that provides detailed intelligence acquired through a comprehensive study of imagery.

S. IMAGERY PRODUCTS (specify type and quantity of imagery products required. Only mission essential imagery products should be requested).

T. DELIVERY ADDRESS.

1. Unit (delivery address for mission essential imagery products).

2. Air drop (coordinates, call sign, frequency, and run-in heading for aerial delivery of imagery products).

U. REMARKS/SPECIAL INSTRUCTIONS.

1. Target area control (indicate, when applicable, the call sign and radio frequency of the control element. Control of the mission will require close coordination with ground forces).

2. Other (self-explanatory, use this space to specify scale if required and to request specific TOT).

Immediate Joint Tactical Air Reconnaissance/Surveillance Request Format Sample

Source: Joint Tactical Air Strike Request Format (Voice Template)

1.UNIT CALLED THIS IS _____ REQUEST # _____

2.IMMEDIATE _____ C PRIORITY _____

3.TARGET IS/NUMBER OF

A. PERS IN OPEN _____/_____

B. PERS DUG IN _____/_____

C. WPNS/MG/RR/AT _____/_____

D. MORTARS/ARTILLERY _____/_____

E. AAA, ADA _____/_____

F. RKTS, MISSILE _____/_____

G. ARMOR _____/_____

H. VEHICLES _____/_____

I. BLDGS _____/_____

J. BRIDGES _____/_____

K. PILLBOX BNKRS _____/_____

L. SUPPLIES, EQUIP _____/_____

M. CNTR (CP, COM) _____/_____

N. AREA _____/_____

O. ROUTE _____/_____

P. MOVING NESW _____/_____

Q. REMARKS _____

4.TARGET LOCATION/ROUTE/AREA IS

A. _____ (COORDINATES)

B. _____(COORDINATES)

C. _____(COORDINATES)

D. _____(COORDINATES)

E. TARGET ELEVATION _____

F. SHEET # _____

G. SERIES _____

H. CHART # _____

5.TARGET TIME/DATE

A. ASAP _____

B. NLT _____

C. AT _____

D. TO _____

6.DESIRED RESULTS/MISSION/PIRs

(FREE TEXT _____)

7.REMARKS

(FREE TEXT _____)

APPENDIX I
TARGET FOLDERS

A target folder contains intelligence that provides the location and components of a target or target complex and indicates its vulnerabilities and relative importance. It also contains related materials prepared for planning and executing actions against a specific target. A major prerequisite for starting a target folder is the relative degree of permanence of the potential target. In addition, local command SOPs will provide guidance as to targets needed to have folders maintained.

IMAGERY ANALYSIS

Imagery intelligence is often the definitive information source of intelligence support to targeting. Imagery intelligence input is reliable, accurate, and current and often forms the basis for targeting decisions. Imagery analysis is a vital component in the tactical and strategic targeting process. It is often the imagery analyst, during the analysis of imagery, who—

- Discovers potential targets and draws them to the attention of the command (CMD section).
- Conducts the target study that is an analysis of the proposed target from imagery and other pertinent sources.
- Takes the information provided by the target analysis and puts it into a target folder format.

TARGET ANALYSIS

The ISC is responsible to the AC/S G-2 for imagery intelligence efforts supporting the MEF's targeting process. Before a possible target can be selected for possible engagement, it must be developed such that its composition, strengths, and vulnerabilities are well known.

The analysis of a target requires the collection and evaluation of many items of information. The target folder is an instrument for the compilation and organization of relevant data produced by the target analysis. Decisions by the force fires coordinator and fire support coordinators regarding whether to attack a proposed target and which weapon system to select are critically influenced by the information in the target folder.

Once a possible target has been identified and approved for inclusion in the target intelligence data base, the imagery analyst and all-source intelligence analysts will prepare a target folder.

This analysis presents all available pertinent information on the proposed target from the following sources:

- *Reference materials*. Perform a thorough check of all available intelligence reference materials, such as interrogation, counterintelligence, ground reconnaissance, and SIGINT reports. All may be useful.
- *GEOINT*. Ensure current maps (latest editions) and other GEOINT materials of the target area are available.
- *Mission coverage*. Examine comparative coverage of the target area from past and ongoing imagery collections missions. If the latest available coverage is old, incomplete, poor quality, or the installation is under construction or renovation, then new collection missions may be required.

Specifications

A target folder is a reference file on permanent potential targets in the AO and AOI that has been created and maintained by the unit. It contains the results of the target study (analysis) and any updates or collateral intelligence. Target folders—

- May be used as a pre-mission briefing aid for aircrews to orient them on target location, recognition, defenses, and obstacles. Imagery analysts may use target folders strictly as reference files on important intelligence targets within the unit's AO. Such folders can be compiled to show an installation's development or an enemy unit's organization.
- Have common characteristics and contain a minimum of important elements.
- Are for permanent targets. A permanent C2 node, troop training area, warehouse area, port facility, or fixed missile site is a good potential target for target folders. Temporary targets, such as troops in the field, supply dumps, and ships in port or truck convoys, are usually not proper subjects for target folders.
- Are current. Because the information within a target folder may be used for target planning, it must be kept current. The target folder must be updated to reflect changes in defenses, physical characteristics, unit reorganization, important equipment, and so on.
- Are concise. Target folders are compact; only intelligence and other information pertinent to the commander's PIRs or intelligence requirements are included.
- Are accurate. Intelligence and other information within a target folder must be accurate to allow realistic targeting plans to be made. Answers to intelligence requirements must be specific to provide maximum value. For example, explicitly describe enemy defenses, target dimensions, shape, construction, use, and capacities.

> ***Note:*** Target folders should be reviewed periodically—or with each new imagery mission (intelligence priorities, resources, and time permitting)—and their contents should be checked against new information or intelligence requirements.

Format and Components

Enclosure F of CJCSI 3370.01, *Target Development Standards*, provides standards for developing electronic target folders (ETFs), hard copy target folders, and target materials.

Marine Corps imagery analysts will adhere to these guidelines and, within technological limitations, provide a product tailored to meet all supported commanders' target intelligence requirements. Although the contents of a target folder may vary slightly according to unit SOP, they will be in accordance with the Military Targeting Intelligence Committee guidelines and contain, at minimum, the following components:

- Heading.
- Target summary.
- Supporting materials.
- Weaponeering support.
- Assessment.
- Associated/collocated targets.
- Objectives and guidance.
- Folder notes/other related information.

Electronic target folders may be expanded to meet specific MAGTF or unit requirements. Additional information, such as supplemental graphics, vector (shapefile) overlays, capability specific supporting materials, three dimensional graphics, and other analytical or source documentation, may be entered into the ETF. The structure of ETFs will be standard across all target types and is intended to support use by all CCMDs, Services, CSAs, and allied producers in a joint/combined environment. Enclosure F of CJCSI 3370.01 provides details on ETF structure and content.

Heading. The heading contains the general identification details for each target entity and will include the following information:

- Classification and release (self-explanatory).
- Entity identifier (EID). (Use the EID, such as the BE number or communications transmission identifier, for the entity from the modernized integrated database [MIDB], when available. If an MIDB EID is not available, the target analyst must coordinate with the appropriate responsible analytic center to obtain a suitable unique EID.)
- Name. (Use the entity [i.e., facility] name as it appears in MIDB. If no record is available, the target analyst must liaise with the appropriate responsible analytic center to develop a suitable name using an approved naming convention.)
- Category and function code:
  - Installation/facility. If available, use the category code from the MIDB or consult DIA Publication 5210.002-M, which contains the complete numbering breakdown.
  - Other entity types (See appendix B to enclosure E of CJCSI 3370.01.).
- O-suffix (facilities only) (as assigned by MIDB).
- Location:
  - Latitude/longitude.
  - Military grid reference system.
  - Datum.

- Country code. (Use the country code from MIDB.)
- Original production date/last update. (Note the year, month, and day the ETF was produced or last updated in a nine-digit format, e.g., YYYYMMMDD.)

Target Summary. The target summary has the following characteristics:

- *Significance statement (basic)*. Use the data from the MIDB to state the significance of the target. For example, "Destruction of this target will deny the enemy 100,000 barrels of POL."
- *Target description (intermediate)*. Producers will identify the target type and provide a comprehensive description of the target, including any EEIs and any associated critical elements.
- *Functional characterization (intermediate)*. This statement elaborates on the function of the target.
- *Expectation statement (intermediate)*. When feasible, use data from MIDB.
- *Collateral concerns (intermediate)*. For facility/installation target types, if the nearest collateral object falls within the collateral damage estimation (CDE) level 1 collateral effects radius, it must be functionally characterized and identified by distance and direction from the target. The CDE is documented in the weaponeering section of the ETF.

Supporting Materials. At minimum, all ETFs produced on installations or facilities will include both an installation outline graphic and a facility (O-suffix) outline graphic. All details and supporting examples of imagery required form ETFs are detailed in appendix D, enclosure F of CJCSI 3370.01.

Weaponeering Support. Weaponeering support will include the following information:

- *Aimpoint (advanced)*. An aimpoint is a weapon placement term that applies to a variety of capabilities (e.g., a joint desired point of impact is a type of aimpoint).
- *Unique target characteristics*. The EFT should provide a detailed description of unique target/element/aimpoint or joint desired point of impact characteristics that would support weaponeering for all weapons/weapon types.
- S*uggested weaponeering solutions (advanced)*. Force fires center or FSCC personnel will complete in this section.
- *Collateral damage estimate*. The CDE will be accomplished in accordance with CJCSI 3160.01A, *No-Strike and the Collateral Damage Estimation Methodology*. The force fires center or FSCC personnel will complete in this section.

Assessment. At minimum, the assessment section will include areas for physical damage/change and functional damage assessments.

Physical Damage/Change Assessment. Physical damage assessment estimates the quantitative extent of physical damage (through munitions blast, fragmentation, and/or fire damage effects) to a target resulting from the application of military force. (JP 1-02) Change assessment is the identification and assessment of measurable change/damage to the target resulting from nonlethal methods or weapons.

Functional Damage Assessment. Functional damage assessment estimates the effect of military force to degrade or destroy the functional or operational capability of the target to perform its intended mission and on the level of success in achieving operational objectives established against the target. (JP 1-02)

Munitions Effectiveness Assessment. The munitions effectiveness assessment is the assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and recommend any required changes to the methodology, tactics, weapon system, munitions, fusing, and/or weapon delivery parameters to increase force effectiveness. (JP 1-02)

Reattack Recommendation. The reattack recommendation is an assessment that is derived from the results of the BDA and munitions effectiveness assessment, providing the commander systematic advice on reattack of targets and further target selection to achieve objectives. The reattack recommendation is a combined operations and intelligence recommendation.

Associated/Collocated. The associated/collocated section provides a textual list of entities collocated to the primary installation or facility that the ETF was produced to support. At minimum, this list should provide a name, BE number, category code, O-suffix, and coordinates for each entity. These entities could include, but are not limited to, the following:

- Units.
- Equipment.
- Facilities.
- Individuals/personnel.
- Groups/organizations.
- Resources.

Objectives and Guidance. The objectives and guidance section should include any associated strategic, operational, or tactical objectives or tasks related to the target on which the ETF was produced. This section should also include target damage and change objectives for the target.

Related Information. The related information section is an open section for additional information or intelligence that targeteers assess as important to complete or augment the ETF.

APPENDIX J
NATIONAL IMAGERY TRANSMISSION FORMAT COMPRESSION

COMPRESSION BASICS

Compression is a process used to decrease imagery file sizes so that usable images can be transmitted as quickly as possible. The national imagery transmission format (NITF) uses Huffman coding which is statistically based and produces a single code for each symbol. Coding varies the length of the symbol in proportion to its information content. Symbols with a low probability of appearance are represented with a code consisting of many bits. Conversely, symbols with a high probability of appearance are represented with a code of fewer bits. Most compression applications are designed with predetermined quality settings. These settings are referred to as Q settings or Q levels. The lower the Q setting is, the greater the compression and, therefore, the greater potential loss of image quality.

Joint Photographic Experts Group Image Compression

Joint Photographic Experts Group (JPEG) image compression is one of the most popular and widely used compression algorithms. It was adapted for use in the NITF in the early 1990s. The complete specifications are contained in MIL-STD-188-198A, *Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format Standard*. National Imagery Transmission Format JPEG's forward discrete cosine transform (FDCT) is a mathematical formula that divides the image into 8 by 8 minimum coding units or neighborhoods and then calculates the FDCT of each neighborhood. The quantizer *rounds off* or *smoothes* the FDCT coefficients according to the table specifications, and then the image is encoded.

For decompression, JPEG recovers the quantized FDCT coefficients from the compressed data stream, computes the inverse transform (using embedded tables), and displays the image. This description is simple; technical details are in the military standard. It is important, though, to understand how the various Q settings impact the quality of an image and the time available to transmit the compressed image.

The NITF JPEG provides several variants—discrete cosine transform (DCT) lossy (8- and 12-bit), downsample JPEG, and lossless.

Discrete Cosine Transform Lossy. In lossy compression some quality is sacrificed for increased compression ratios. When users employ DCT lossy, they can choose from five different Q levels (Q1–Q5). Level Q1 provides the greatest compression and, therefore, the greatest quality loss; while, Q5 provides the least compression and, consequently, the highest image quality (see table J-1).

Table J-1. Discrete Cosine Transform Joint Photographic Experts Group Results Summary.

Image	Original	Q1	Q2	Q3	Q4	Q5
Color	1:1 12:11	43:1 00:13	34:1 00:15	16:1 00:36	12.6:1 00:44	8.7:1 01:04
B&W	1:1 58:18	13.9:1 04:10	11.8:1 04:54	8:1 07:14	7:1 08:16	5.4:1 10:37
IR	1:1 08:32	43.6:1 00:11	33.9:1 00:15	25.9:1 00:19	14.6:1 00:35	5:1 01:35
SAR	1:1 13:21	9.9:1 01:20	7:1 01:53	6:1 02:10	4:1 03:03	2:1 06:11
UAS	1:1 17:05	25:1 00:39	17.9:1 00:57	17:1 00:59	8.7:1 01:57	2.5:1 06:41
Multi-spectral	1:1 21:50	17:1 01:16	10.5:1 02:04	6:1 03:36	3.8:1 05:41	2.1:1 10:23
Compression ration (n:1) Time to Transmit (mm:ss) @ 9600 bits per second						

Legend:
B&W–black and white
IR–intelligence requirement

Downsample Joint Photographic Experts Group. Downsample JPEG uses a compression technique that is essentially the same DCT JPEG compression applied to an image that has been downsampled. This means that the image size has been reduced by discarding image data. This process is illustrated in the figure J-1: the original 2,048 x 2,048 size is downsampled to 1,024 x 1,024 and then to 512 x 512. In this process the algorithm selectively throws away image data in both the X and Y axes to reach the next smaller file size until the smallest is reached. In the reverse process (upsampling), the image is restored to its original size.

Lossless Joint Photographic Experts Group. Lossless data compression techniques will generate exact duplicates of input data streams (or original images) once the data has been compressed. In other words, the data stream (or image) is decompressed back into its original form with no differences to be found. However, lossless compression rates are very small (approximately 2:1 or 2.5:1) and offer no significant reduction in image file sizes.

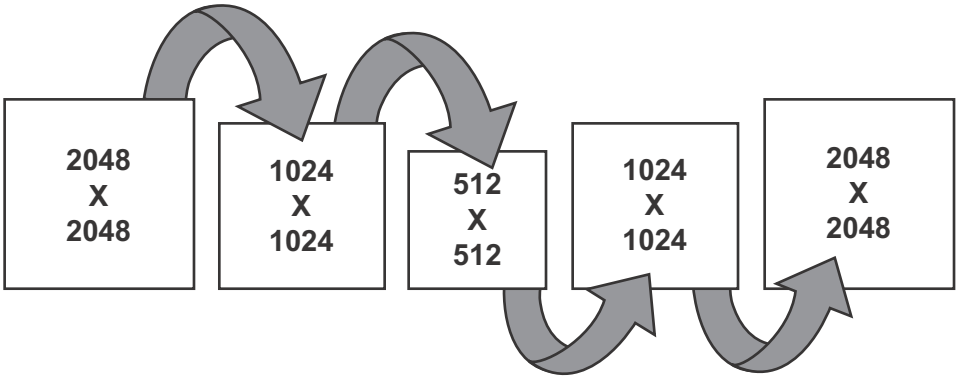


Figure J-1. Downsample and Upsample Process.

Bi-Level Image Compression

The NITF handles textual information as well. Bi-level compression uses the same algorithm that is used in commercial facsimile devices. If users must learn more about this type of lossless compression or facsimile devices, MIL-STD-188-161, *Interoperability and Performance Standards for Digital Facsimile Equipment*, and MIL-STD-188-196, *Department of Defense Interface Standard: Bi-Level Image Compression for the National Imagery Transmission Format Standard*, contain relevant technical information. The NITF implementation of bi-level compression provides three different modes of operation: mode 1 (one-dimensional coding); mode 2 (two-dimensional coding with standard vertical resolution), and mode 3 (two-dimensional coding with higher vertical resolution) (see fig. J-2). It is not necessary to know the details of bi-level compression. Users only need to know that the fundamental concept of this coding algorithm is to detect run lengths of one of two colors (for example, black or white) in an image. These run lengths are then replaced with Huffman codes. Synchronization codes that indicate the beginning of an image, the end of a line, or similar information are embedded.

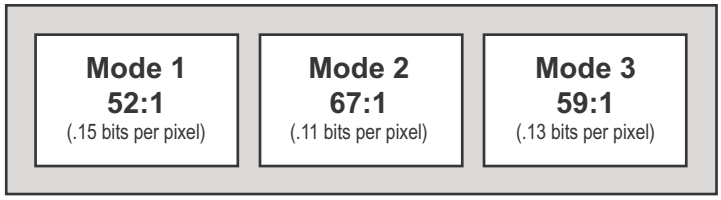


Figure J-2. Bi-Level Image Compression Results.

Video Compression

Motion imagery (or video imagery) is defined as imaging sensor/systems that generate sequential or continuous streaming images at specified temporal rates (normally expressed as frames per second). This type of imagery includes EO (video and television), infrared, complex waveforms based on radar imaging, MTI, and acoustic waterfalls. It is not within the scope of this publication to address all of these technologies, but it is necessary to know of their existence and that the NGA has published *MISP version 6.4*. This profile summarizes the results of work accomplished by the DOD/IC/NSG Motion Imagery Standards Board. The profile identifies MPEG [Motion Picture Expert Group]-2 as the standard video compression format. Additionally H.264 shall be the standard for applications constrained by low bandwidth channels (typically less than 1 megabyte per second that may not be adequately supported by MPEG-2). The MISP also allows the use of H.264 for higher bandwidth applications.

National Image Compression

The following are some of the items that are different in the national image compression arena:

- National compresses 8-, 11-, and 12-bit imagery data using both JPEG lossy and JPEG lossless compression (as well as other non-JPEG compression algorithms). The compressed data is transmitted in NITF format. Uncompressed national image data is stored in 2 bytes (11- and 12-bit data).
- For national systems, the term quality levels applies to the three different bit rates, plus lossless.
- In addition to image compression within national systems, there is a separate technique called pre-processing that is conducted to remap the pixel values in order to optimize the compression process. This requires the receiver to conduct a post-processing function after decompressing the image. Receivers of this data must understand the post-processing of this algorithm.

COMPRESSION STANDARDS

The following current standards are related to the aforementioned compression types:

- MIL-STD 188-161_.
- MIL-STD 188-196.
- MIL-STD 188-198A.
- MIL-STD 188-199, *Vector Quantization Decompression for the National Imagery Transmission Format Standard*.
- MIL-STD 2500C, *National Imagery Transmission Format (Version 2.1) for the National Imagery Transmission Format Standard*.
- MISP version 6.4.
- NGA Standard Identification (STDI)-0001 V1.3/CN2, *National Support Data Extension (SDE) (Version 1.3/CN2) for the National Imagery Transmission Format (NITF)*.
- NGA STDI-006, *National Imagery Transmission Format (NITF) Version 2.1 Commercial Dataset Requirements Document (NCDRD)*.

APPENDIX K
IMAGERY INTELLIGENCE APPENDIX FORMAT

The IMINT operations appendix should explain how IMINT and relevant imagery-related elements under the operational control of or supporting the MAGTF will be used to support this plan. It should also provide guidance to subordinate commanders for the conduct of IMINT operations and the support of IMINT elements and personnel identified to fulfill the IMINT requirements.

CLASSIFICATION

Copy no. ___ of ___ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

APPENDIX 7 TO ANNEX B (INTELLIGENCE) TO MAGTF OPORD XXX (U)
IMAGERY INTELLIGENCE (U)

(U) REFERENCES: Identify DOD, NGA, and other directives; combatant commander, JTF, or other higher authorities' OPORDs and TTP or SOP for intelligence and IMINT operations; pertinent maps and other geospatial information resources; and any other relevant references that pertain to anticipated IMINT operations.

1. (U) Situation

a. (U) Definition of the AO and AOI. Describe the limits of the AO and AOI. Summarize pertinent weather, terrain, and other AO's characteristics and conditions that may influence the conduct of IMINT operations.

b. (U) Enemy. Refer to annex B and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and OOB pertinent to IMINT operations.

c. (U) Assigned MAGTF Organic and Supporting IMINT Assets. Identify organic and supporting forces available to perform IMINT and imagery-related functions.

d. (U) Facts and Assumptions. Derived during the mission analysis step of the MCPP.

e. (U) IMINT Considerations. List key IMINT, intelligence, or other considerations that impact this OPLAN or CONPLAN.

(1) (U) Availability of national source and commercial imagery.

(2) (U) IMINT support to and from JTF and other component headquarters.

(3) (U) Creation and manning of forward IMINT elements.

1

CLASSIFICATION

CLASSIFICATION

2. (U) Mission. State concisely the IMINT mission as it relates to the command's planned operation.

3. (U) Execution

a. (U) Concept of Operations. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations Plan) to annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall CONOPS as they relate to IMINT operations. Outline the purpose and concept of IMINT operations; specify priorities; and summarize the means and agencies to be employed in planning and directing, collecting, processing and exploiting, analyzing and producing, disseminating, and using IMINT during execution of the OPORD. Address the integration of JTF, other components, theater, national, and allied forces' IMINT operations.

b. (U) Tasks for IMINT and Related Units and Organizations, Subordinate Units, and Task Force Commanders/OICs

(1) (U) Orders to Subordinate, Attached, and Supporting Units. Use separate numbered subparagraphs to list detailed instructions for each unit conducting IMINT operations, including the originating headquarters, subordinate commands, and separate intelligence support units.

(a) (U) Major subordinate commanders.

(b) (U) Commanding officer, intelligence battalion.

1 Platoon commander, IIP.

2 MTI section.

3 Staff noncommissioned officers in charge (SNCOICs), direct support teams.

4 OIC, support cell.

5 OIC, surveillance and reconnaissance cell.

6 OIC, P&A cell.

7 Others, as appropriate.

CLASSIFICATION

(c) (U) Commanding officer, VMU.

(d) (U) Commanding officer, force reconnaissance company.

(2) (U) Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached, or supporting and from which IMINT support is requested, including other components, JTF headquarters, allied or coalition forces, theater and national operational and intelligence elements.

c. (U) Coordinating Instructions. Reference Appendix 16 (Intelligence Operations Plan) and command and other pertinent forces' and organizations' intelligence and counterintelligence SOPs. Detail key changes to SOPs here or in supporting tabs. Additional topics to include or emphasize here include requesting IMINT support; direct liaison among subordinate commanders, MAGTF IMINT units, staff officers, and pertinent external organizations and agencies; and routine and time-sensitive reporting procedures and formats.

4. (U) Administration and Logistic

a. (U) Logistics. Reference Annex D (Logistics). Identify IMINT unique logistic requirements and concerns, such as any unique combat service support requirements, procedures, and other guidance to support MAGTF IMINT units and operations or procedures for specialized technical logistic support necessary from external organizations.

b. (U) Personnel. Identify intelligence unique IMINT personnel requirements and concerns.

5. (U) Command and Control

a. (U) Command Relationships. Reference Annex J (Command Relationships). Provide any instructions necessary regarding MAGTF command relationships that will influence unit IMINT operations.

b. (U) Information Management. Reference Annex U (Information Management), Annex C (Operations), and Appendix 16 (Intelligence Operations Plan). Provide any necessary instructions regarding information management (e.g., time-sensitive and routine reporting criteria, intelligence databases, reports) that will influence MAGTF IMINT operations.

c. (U) Communications and Information Systems. Reference Appendix 16 (Intelligence Operations Plan) and Annex K (Communications and Information Systems). Provide any instructions necessary regarding CIS that will influence MAGTF IMINT operations.

CLASSIFICATION

d. (U) Intelligence C2 Nodes and Facilities. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations Plan). Provide guidance and necessary instructions regarding the establishment and operations of intelligence and IMINT C2 nodes and facilities (e.g., the surveillance and reconnaissance cell).

TABS: (As necessary)

APPENDIX L
UNMANNED AIRCRAFT SYSTEM FORMATS

Unmanned Aircraft System Plan

CLASSIFICATION
Copy no._____ of_____ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

TAB C TO APPENDIX 14 TO ANNEX B TO OPLAN XXX (U)
UNMANNED AIRCRAFT SYSTEM PLAN (U)

(U) REFERENCES: (As appropriate).

1. (U) Mission. Conduct real-time surveillance, target acquisition, and imagery intelligence throughout the MAGTF area of responsibility until termination of hostilities, per Annex B (Intelligence) and Annex C (Operations) to the MAGTF OPLAN.

2. (U) Execution. The VMU will provide UAS and C2 crews in support of MAGTF operations. The MAGTF G-2, in coordination with the G-3, will exercise operational control of all tactical surveillance unmanned aircraft within the AO unless otherwise directed. The ISC, under the staff cognizance of the AC/S G-2, plans, coordinates, and supervises MAGTF UAS intelligence missions.

3. (U) Tasks. Detachment, _____, _____VMU will—

a. (U) Prepare a UAS employment plan and overlay to depict the UAS concept of employment supporting combat operations ashore and submit these to the MAGTF G-2 (attn: ISC or CM/DO).

1

CLASSIFICATION

CLASSIFICATION

b. (U) Assign surveillance UAS equipment and personnel to provide real time video/ imagery intelligence in support of MAGTF operations as directed by Annex B (Intelligence) to the MAGTF OPLAN, daily ATOs, and other intelligence orders.

c. (U) Provide remote receiving station detachments at designated locations afloat and ashore.

d. (U) Initiate action to obtain approved frequencies for UAS support, per Annex K (CIS) to the MAGTF OPLAN.

e. (U) Coordinate flight operations through appropriate air control agencies as assigned in Annex N (Aviation Operations) to the MAGTF OPLAN.

4. (U) MAGTF UAS Surveillance Sectors/Routes. To facilitate the assignment and coordination of tactical surveillance missions, UAS loiter areas and surveillance routes are designated in the enclosures to this tab.

ENCLOSURES:

1–UAS Employment Plan

2–UAS Employment Overlay

Unmanned Aircraft System Employment Plan

CLASSIFICATION
Copy no._____ of_____ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

ENCLOSURE 1 TO TAB C TO APPENDIX 14 TO ANNEX B TO OPLAN XXX
UAS EMPLOYMENT PLAN

(U) REFERENCES: (a) Maps: NGA stock no._____

The following UAS and surveillance routes, targets, and loiter areas have been preplanned in support of MAGTF operations:

Note:
1) Tasked intelligence requirements and reporting criteria.
2) Others, as appropriate.

MSN NUMBER	COORDINATES	ALT	TOT	FOOTNOTES
	_____to	TBD	TBD	
	_____to			
	_____to			
	_____to			
	Close			
	_____to	TBD	TBD	
	_____to			
	_____to			
	_____to			
	Close			

1

CLASSIFICATION

APPENDIX M
AERIAL IMAGERY PLAN FORMAT

CLASSIFICATION
Copy no. ___ of ___ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

TAB D TO APPENDIX 14 TO ANNEX B TO OPLAN XXX (U)
AERIAL IMAGERY PLAN (U)

(U) REFERENCES: (a) Maps. See Appendix 15 (Geographic Intelligence) to Annex B (Intelligence) and Annex M (GI&S).

1. The following aerial imagery missions have been preplanned.

		PHOTO						
MSN NO.	**COORD**	**VERT OR OBL**	**OVERLAP**	**FILM SCALE**	**SLR MODE**	**IR/ALT**	**DATE OF MSN**	**REMARKS**
1.	XXXXX XXXXX XXXXX XXXXX	VERT	60% FOR 40%	B&W 1:20K	Low ALT Mode 10B	N/A	D-30	Basic Coverage
2.	XXXXX XXXXX XXXXX XXXXX	VERT	60% FOR 40% SIDE	B&W Color & CD 1:5K	Low ALT MTIR Or MTIR	D-3 Only	D-1	Beach Study Survey
3.	N/A	N/A	N/A	N/A	N/A	N/A	D+1	On call

1

CLASSIFICATION

GLOSSARY

Section I. Acronyms

AAA ..... antiaircraft artillery
AC/S ..... assistant chief of staff
ACE ..... aviation combat element
AFP ..... all-source fusion platoon
ALT ..... altitude
AMC ..... air mission commander
AO ..... area of operations
AOI ..... area of interest
ATARS ..... advanced tactical airborne reconnaissance system
ATF ..... amphibious task force
ATO ..... air tasking order

BDA ..... battle damage assessment
BE ..... basic encyclopedia
BLS ..... beach landing site

C2 ..... command and control
CCD ..... camouflage, concealment, and deception
CCIR ..... commander's critical information requirement
CCMD ..... combatant command
CDE ..... collateral damage estimation
CDL ..... common data link
CGS ..... common ground station
CIA ..... Central Intelligence Agency
CIC ..... combat intelligence center
CIS ..... communications and information systems
CJCSI ..... Chairman of the Joint Chiefs of Staff instruction
CLS ..... contractor logistics support
cm ..... centimeter(s)
CM ..... collection manager
CM/DO ..... collection management/dissemination officer
CMD ..... command
COA ..... course of action
COC ..... combat operations center
CONOPS ..... concept of operations
CONPLAN ..... concept plan
COP ..... common operational picture
CSA ..... combat support agency
CTP ..... common tactical picture

DASC ..... direct air support center
DCGS ..... distributed common ground/surface system
DCGS-MC ..... distributed common ground/surface system-Marine Corps
DCT ..... discrete cosine transform
DIA ..... Defense Intelligence Agency
DIB ..... distributed common ground/surface system integration backbone
DIRINT ..... Director of Intelligence
DMRF ..... denominator of the map representative scale factor
DNI ..... Director of National Intelligence
DOD ..... Department of Defense
DODIPP ..... Department of Defense Intelligence Production Program
DPRF ..... denominator of the photo representative scale factor
DRO ..... departmental requirements office
DZ ..... drop zone

EEI ..... essential element of information
EID ..... entity identifier
EO ..... electro-optical
ETF ..... electronic target folder
EW ..... electronic warfare

FDCT ..... forward discrete cosine transform
FLIR ..... forward-looking infrared
FMV ..... full motion video
FOC ..... future operations cell
FoS ..... family of systems
FSCC ..... fire support coordination center
FSR ..... field service representative
ft ..... foot (feet)
FTI ..... fixed target indicator

G-1 ..... manpower or personnel staff officer
G-2 ..... intelligence staff officer
G-3 ..... operations staff officer
G-4 ..... logistics staff officer
G-5 ..... assistant chief of staff, plans
G-6 ..... command, control, communications, and computer systems staff officer
GD ..... ground distance
GDT ..... ground data terminal
GEOINT ..... geospatial intelligence
GI&S ..... geospatial information and services

HD ..... horizontal distance
HLZ ..... helicopter landing zone
HQMC ..... Headquarters, Marine Corps
HQMC-IPI ..... Headquarters, Marine Corps-Imagery & Geospatial Intelligence Branch
HUMINT ..... human intelligence

I&W ..... indications and warning
IAS ..... intelligence analysis system
IC ..... intelligence community
ICBM ..... intercontinental ballistic missile
ICR ..... intelligence collection requirement
IIP ..... imagery intelligence platoon
IMINT ..... imagery intelligence
IMR ..... imagery reference
IOC ..... intelligence operations center
IPB ..... intelligence preparation of the battlespace
IPIR ..... initial photographic interpretation report
ISC ..... intelligence support coordinator
ISR ..... intelligence, surveillance, and reconnaissance

J-2 ..... intelligence staff section
JAS ..... JSTARS antenna suite
JFC ..... joint force commander
JIOC ..... joint intelligence operations center
JISE ..... joint intelligence support element
JP ..... joint publication
JPEG ..... Joint Photographic Experts Group
JSTARS ..... Joint Surveillance Target Attack Radar System
JTAR/S ..... joint tactical air reconnaissance/surveillance
JTF ..... joint task force
JWICS ..... Joint Worldwide Intelligence Communications System

km ..... kilometers
kts ..... knots

LAN ..... local area network
LCE ..... logistics combat element
LOC ..... line of communications
LOS ..... line of sight
LP ..... landing point
LSI ..... lead systems integrator
LSRS ..... littoral surveillance radar system
LTIOV ..... latest time information is of value
LZ ..... landing zone

m ..... meter(s)
MACCS ..... Marine air command and control system
MACG ..... Marine air control group
MAGTF ..... Marine air-ground task force
MARFORRES ..... United States Marine Corps Forces Reserve
MASINT ..... measurement and signature intelligence
MAW ..... Marine aircraft wing
MC ..... MOVINT client

MCIA ..... Marine Corps Intelligence Activity
MCISR-E .....Marine Corps Intelligence, Surveillance, and Reconnaissance-Enterprise
MCO .....Marine Corps order
MCPP ..... Marine Corps Planning Process
MCRP .....Marine Corps reference publication
MARCORSYSCOM..... Marine Corps Systems Command
MCWP .....Marine Corps warfighting publication
MEF .....Marine expeditionary force
METOC .....meteorological and oceanographic
METT-T .....mission, enemy, terrain and weather, troops and support available-time available
MEU .....Marine expeditionary unit
MIDB .....modernized integrated database
MIPIR ..... multimission imagery photo interpretation report
MISP .....Motion Imagery Standards Profile
MLG..... Marine logistics group
MOJT ..... managed on-the-job training
MOS ..... military occupational specialty
MOUT..... military operations on urbanized terrain
MSC .....major subordinate command
MSN ..... mission
MTI ..... moving target indicator
MTI OS ..... moving target indicator operation suite

NATO .....North Atlantic Treaty Organization
NGA.....National Geospatial-Intelligence Agency
NIIRS ..... National Imagery Interpretability Rating Scale
NIPRNET.....Nonsecure Internet Protocol Router Network
NIST..... national intelligence support team
NITF.....national imagery transmission format
NRO .....National Reconnaissance Office
NRT .....near real time
NSA .....National Security Agency
NSG ..... National System for Geospatial Intelligence
NST ..... National Geospatial-Intelligence Agency support team

OIC..... officer in charge
OOB .....order of battle (also known as OB)
OPLAN .....operation plan
OPORD ..... operation order

P&A .....production and analysis
PD ..... photo distance
PIR .....priority intelligence requirement
POL ..... petroleum, oils, and lubricants

RECCEXREP .....reconnaissance exploitation report
RFI .....request for intelligence

RPG ..... rocket propelled grenade
RVT ..... remote video terminal

S-2 ..... intelligence staff officer
S-3 ..... operations staff officer
S-4 ..... logistics staff officer
S-6 ..... communications system officer
SALUTE ..... size, activity, location, unit, time, and equipment
SAM ..... surface-to-air missile
SAR ..... synthetic aperture radar
SARC ..... surveillance and reconnaissance center
SATCOM ..... satellite communications
SCDL ..... surveillance control data link
SIDS ..... secondary imagery dissemination system
SIGINT ..... signals intelligence
SIPRNET ..... SECRET Internet Protocol Router Network
SL ..... percent of slope
SOP ..... standing operating procedure
SRBM ..... short-range ballistic missile
SUPIR ..... supplemental photographic interpretation report

TACC ..... tactical air command center
TACTEX ..... tactical analysis and combat tracking exploitation
TCPED ..... tasking, collection, processing, exploitation, and dissemination
TDN ..... tactical data network
TEG ..... tactical exploitation group
TEG-RWS ..... tactical exploitation group-remote workstation
TEL ..... transporter-erector-launcher
TOT ..... time on target
TTP ..... tactics, techniques, and procedures

UAS ..... unmanned aircraft system
US ..... United States
UTM ..... universal transverse mercator

VADER ..... vehicle and dismount exploitation radar
VAS ..... vantage ascent software
VD ..... vertical distance
VHF ..... very high frequency
VIP-MC ..... virtual imagery processing-Marine Corps
VMFA(AW) ..... Marine fighter/attack (all weather) squadron
VMU ..... Marine unmanned aerial vehicle squadron

WAN ..... wide-area network

Section II. Definitions

airfield—An area prepared for the accommodation (including any buildings, installations, and equipment), landing, and takeoff of aircraft. See also **departure airfield**; **landing area**; **landing site**. (JP 1-02)

all-source intelligence—1. Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 1-02)

amphibious force—An amphibious task force and a landing force together with other forces that are trained, organized, and equipped for amphibious operations. Also called **AF**. (JP 1-02)

area of interest—That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called **AOI**. (JP 1-02)

area of operations—An operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. Also called **AO**. (JP 1-02)

assessment—3. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. 4. Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 1-02) (Parts 3 and 4 of a 4-part definition.)

attach—1. The placement of units or personnel in an organization where such placement is relatively temporary. 2. The detailing of individuals to specific functions where such functions are secondary or relatively temporary. (JP 1-02)

aviation combat element—The core element of a Marine air-ground task force (MAGTF) that is task-organized to conduct aviation operations. The aviation combat element (ACE) provides all or a portion of the six functions of Marine aviation necessary to accomplish the MAGTF's mission. These functions are antiair warfare, offensive air support, assault support, electronic warfare, air reconnaissance, and control of aircraft and missiles. The ACE is usually composed of an aviation unit headquarters and various other aviation units or their detachments. It can vary in size from a small aviation detachment of specifically required aircraft to one or more Marine aircraft wings. In a joint or multinational environment, the ACE may contain other Service or multinational forces assigned or attached to the MAGTF. The ACE itself is not a formal command. Also called **ACE**. (MCRP 5-12C)

battle damage assessment—The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force. (JP 1-02) The timely and accurate estimate of the damage resulting from the application of military force. Battle damage assessment estimates physical damage to a

particular target, functional damage to that target, and the capability of the entire target system to continue its operations. Also called **BDA**. (MCRP 5-12C)

battlespace—The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas, areas of interest, and areas of influence. (MCRP 5-12C)

beach—1. The area extending from the shoreline inland to a marked change in physiographic form or material, or to the line of permanent vegetation (coastline). 2. In amphibious operations, that portion of the shoreline designated for landing of a tactical organization. (JP 1-02)

beachhead—A designated area on a hostile or potentially hostile shore that, when seized and held, ensures the continuous landing of troops and materiel, and provides maneuver space requisite for subsequent projected operations ashore. (JP 1-02)

beach width—The horizontal dimensions of the beach measured at right angles to the shoreline from the line of extreme low water inland to the landward limit of the beach (the coastline). (JP 1-02)

collection—(See JP 1-02 for core definition. Marine Corps amplification follows.) The gathering of intelligence data and information to satisfy the identified requirements. (MCRP 5-12C)

collection management—In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 1-02)

collection plan—A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02)

collection requirement—2. An established intelligence need, validated against the appropriate allocation of intelligence resources (as a requirement) to fulfill the essential elements of information and other intelligence needs of an intelligence consumer. (JP 1-02) (Part 2 of a 2-part definition.)

combatant commander—A commander of one of the unified or specified combatant commands established by the President. Also called **CCDR**. (JP 1-02)

command and control—(See JP1-02 for core definition. Marine Corps amplification follows.) The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. Command and control is one of the six warfighting functions. Also called **C2**. (MCRP 5-12C)

command element—The core element of a Marine air-ground task force (MAGTF) that is the headquarters. The command element is composed of the commander, general or executive and special staff sections, headquarters section, and requisite communications support, intelligence, and reconnaissance forces, necessary to accomplish the MAGTF's mission. The command element provides command and control, intelligence, and other support essential for effective planning and execution of operations by the other elements of the MAGTF. The command element varies in size and composition; and, in a joint or multinational environment, it may contain other Service or multinational forces assigned or attached to the MAGTF. Also called **CE**. (MCRP 5-12C)

commander's critical information requirement(s)—(See JP1-02 for core definition. Marine Corps amplification follows.) Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. The two subcategories are priority intelligence requirements and friendly force information requirements. Also called **CCIRs**. (MCRP 5-12C)

commander's intent—(See JP1-02 for core definition. Marine Corps amplification follows.) A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

contingency—A situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect US interests. (JP 1-02)

control—1. Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. 2. In mapping, charting, and photogrammetry, a collective term for a system of marks or objects on the Earth or on a map or a photograph, whose positions or elevations (or both) have been or will be determined. 3. Physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. 4. An indicator governing the distribution and use of documents, information, or material. Such indicators are the subject of intelligence community agreement and are specifically defined in appropriate regulations. (JP 1-02)

coordination—The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (MCRP 5-12C)

counterintelligence—(See JP1-02 for core definition. Marine Corps amplification follows.) The active and passive measures intended to deny the enemy valuable information about the friendly

situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. (MCRP 5-12C)

countermeasures—That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

current intelligence—One of two categories of descriptive intelligence that is concerned with describing the existing situation. (JP 1-02)

damage assessment—1. The determination of the effect of attacks on targets. 2. A determination of the effect of a compromise of classified information on national security. (JP 1-02)

detachment—1. A part of a unit separated from its main organization for duty elsewhere. 2. A temporary military or naval unit formed from other units or parts of units. (AAP-06)

dissemination—Conveyance of intelligence to users in a suitable form. (MCRP 5-12C)

drop zone—A specific area upon which airborne troops, equipment, or supplies are airdropped. Also called **DZ**. (JP 1-02)

essential elements of friendly information—(See JP1-02 for core definition. Marine Corps amplification follows.) Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. Also called **EEFI**. (MCRP 5-12C)

fires—(See JP1-02 for core definition. Marine Corps amplification follows.) Those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight. Fires is one of the six warfighting functions. (MCRP 5-12C)

force protection—(See JP1-02 for core definition. Marine Corps amplification follows.) Actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. Force protection is one of the six warfighting functions. (MCRP 5-12C)

fusion—In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 1-02)

global sourcing—A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

ground combat element—The core element of a Marine air-ground task force (MAGTF) that is task-organized to conduct ground operations. It is usually constructed around an infantry organization but can vary in size from a small ground unit of any type to one or more Marine divisions that can be independently maneuvered under the direction of the MAGTF commander. It includes appropriate ground combat and combat support forces, and in a joint or multinational environment, it may also contain other Service or multinational forces assigned or attached to the

MAGTF. The ground combat element itself is not a formal command. Also called **GCE**. (MCRP 5-12C)

helicopter landing zone—A specified ground area for landing assault helicopters to embark or disembark troops and/or cargo. A landing zone may contain one or more landing sites. Also called **HLZ**. (JP 1-02)

human intelligence—A category of intelligence derived from information collected and provided by human sources. Also called **HUMINT**. (JP 1-02)

human intelligence operations—Operations that cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations. Also called **HUMINT operations**. (MCRP 5-12C)

imagery—A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (JP 1-02)

imagery exploitation—The cycle of processing and printing imagery to the positive or negative state, assembly into imagery packs, identification, interpretation, mensuration, information extraction, the preparation of reports, and the dissemination of information. (JP 1-02)

imagery intelligence—The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. Also called **IMINT**. (JP 1-02)

imagery interpretation—1. The process of location, recognition, identification, and description of objects, activities, and terrain represented on imagery. 2. The extraction of information from photographs or other recorded images. (AAP-6)

indications—In intelligence usage, information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (JP 1-02)

indications and warning—Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of hostile actions or intentions against the United States, its activities, overseas forces, or allied and/or coalition nations. Also called **I&W**. (JP 1-02)

indicator—In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (JP 1-02)

information—Unprocessed data of every description which may be used in the production of intelligence. (AAP-06)

information requirements—In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 1-02)

infrared imagery—That imagery produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared position of the electromagnetic spectrum (approximately 0.72 to 1,000 microns). (JP 1-02)

integration—3. In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or the process by which several photographic images are combined into a single image. (JP 1-02) (Part 3 of a 3-part definition.)

intelligence—(See JP1-02 for core definition. Marine Corps amplification follows.) Knowledge about the enemy or the surrounding environment needed to support decisionmaking. Intelligence is one of the six warfighting functions. (MCRP 5-12C)

intelligence data—Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline—A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. There are seven major disciplines: human intelligence, geospatial intelligence, measurement and signature intelligence, signals intelligence, open-source intelligence, technical intelligence, and counterintelligence. (JP 1-02)

intelligence estimate—The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 1-02)

intelligence preparation of the battlespace—(See JP1-02 for core definition. Marine Corps amplification follows.)The systematic, continuous process of analyzing the threat and environment in a specific geographic area. Also called **IPB**. (MCRP 5-12C)

intelligence-related activities—Those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. (Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.) (JP 1-02)

intelligence report—A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called **INTREP**. (JP 1-02)

intelligence reporting—The preparation and conveyance of information by any means. More commonly, the term is restricted to reports as they are prepared by the collector and as they are transmitted by the collector to the latter's headquarters and by this component of the intelligence structure to one or more intelligence-producing components. Thus, even in this limited sense, reporting embraces both collection and dissemination. The term is applied to normal and specialist intelligence reports. (JP 1-02)

intelligence requirement(s)—(See JP1-02 for core definition. Marine Corps amplification follows.) Questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called **IRs**. (MCRP 5-12C)

interpretation—(See JP1-02 for core definition. Marine Corps amplification follows.) A part of the production phase in the Marine Corps intelligence cycle that supports the commander's decisionmaking process. (MCRP 5-12C)

joint force—A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (JP 1-02)

joint force commander—A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. Also called **JFC**. (JP 1-02)

joint intelligence—Intelligence produced by elements of more than one Service of the same nation. (JP 1-02)

joint intelligence operations center—An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. Also called **JIOC**. (JP 1-02)

Joint Worldwide Intelligence Communications System—The sensitive, compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called **JWICS**. (JP 1-02)

landing area—1. That part of the operational area within which are conducted the landing operations of an amphibious force. It includes the beach, the approaches to the beach, the transport areas, the fire support areas, the airspace above it, and the land included in the advance inland to the initial objective. 2. (Airborne) The general area used for landing troops and materiel either by airdrop or air landing. This area includes one or more drop zones or landing strips. 3. Any specially prepared or selected surface of land, water, or deck designated or used for takeoff and landing of aircraft. See also **airfield**; **amphibious force**; **landing beach**; **landing force**. (JP 1-02)

landing beach—That portion of a shoreline usually required for the landing of a battalion landing team. However, it may also be that portion of a shoreline constituting a tactical locality (such as the shore of a bay) over which a force larger or smaller than a battalion landing team may be landed. (JP 1-02)

landing force—A Marine Corps or Army task organization formed to conduct amphibious operations. The landing force, together with the amphibious task force and other forces, constitute the amphibious force. Also called **LF**. (JP 1-02)

liaison—That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action. (JP 1-02)

logistics—(See JP1-02 for core definition. Marine Corps amplification follows.) 1. The science of planning and executing the movement and support of forces. 2. All activities required to move and sustain military forces. Logistics is one of the six warfighting functions. (MCRP 5-12C)

logistics combat element—The core element of a Marine air-ground task force (MAGTF) that is task-organized to provide the combat service support necessary to accomplish the MAGTF's mission. The logistics combat element varies in size from a small detachment to one or more Marine logistics groups. It provides supply, maintenance, transportation, general engineering, health services, and a variety of other services to the MAGTF. In a joint or multinational environment, it may also contain other Service or multinational forces assigned or attached to the MAGTF. The logistics combat element itself is not a formal command. Also called **LCE**. (MCRP 5-12C)

main effort—The designated subordinate unit whose mission at a given point in time is most critical to overall mission success. It is usually weighted with the preponderance of combat power and is directed against a center of gravity through a critical vulnerability. (MCRP 5-12C)

maneuver—The movement of forces for the purpose of gaining an advantage over the enemy. Maneuver is one of the six warfighting functions. (MCRP 5-12C)

Marine air-ground task force—The Marine Corps' principal organization for all missions across a range of military operations, composed of forces task-organized under a single commander capable of responding rapidly to a contingency anywhere in the world. The types of forces in the Marine air-ground task force (MAGTF) are functionally grouped into four core elements: a command element, an aviation combat element, a ground combat element, and a logistics combat element. The four core elements are categories of forces, not formal commands. The basic structure of the MAGTF never varies, though the number, size, and type of Marine Corps units comprising each of its four elements will always be mission dependent. The flexibility of the organizational structure allows for one or more subordinate MAGTFs to be assigned. In a joint or multinational environment, other Service or multinational forces may be assigned or attached. Also called **MAGTF**. (MCRP 5-12C)

Marine Corps Planning Process—A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the mission and the threat and is based on the Marine Corps philosophy

of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of problem framing, course of action development, course of action war game, course of action comparison and decision, orders development, and transition. Also called **MCPP**. *(Note: Tenets of the MCPP include top-down planning, single-battle concept, and integrated planning.)* (MCRP 5-12C)

Marine expeditionary force—The largest Marine air-ground task force (MAGTF) and the Marine Corps' principal warfighting organization, particularly for larger crises or contingencies. It is task-organized around a permanent command element and normally contains one or more Marine divisions, Marine aircraft wings, and Marine logistic groups. The Marine expeditionary force is capable of missions across the range of military operations, including amphibious assault and sustained operations ashore in any environment. It can operate from a sea base, a land base or both. In a joint or multinational environment, it may also contain other Service or multinational forces assigned or attached to the MAGTF. Also called **MEF**. (MCRP 5-12C)

Marine expeditionary unit—A Marine air-ground task force (MAGTF) that is constructed around an infantry battalion reinforced, a composite squadron reinforced, and a task-organized logistics combat element. It normally fulfills Marine Corps' forward sea-based deployment requirements. The Marine expeditionary unit provides an immediate reaction capability for crisis response and is capable of limited combat operations. In a joint or multinational environment, it may contain other Service or multinational forces assigned or attached to the MAGTF. Also called **MEU**. (MCRP 5-12C)

measurement and signature intelligence—Intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted. Also called **MASINT**. (JP 1-02)

multispectral imagery—The image of an object obtained simultaneously in a number of discrete spectral bands. Also called **MSI**. (JP 1-02)

National Imagery Transmission Format Standard—The suite of standards for formatting digital imagery and imagery-related products and exchanging them among members of the Intelligence Community (IC) as defined by the Executive Order 12333, and other United States Government departments and agencies. Also called **NITFS**. (MIL-STD-2500C)

national intelligence—All intelligence, regardless of the source from which derived, and including that which is gathered within or outside the United States, that pertains to more than one agency, and involves (1) threats to the United States, its people, property, or interests, (2) the development, proliferation, or use of weapons of mass destruction, or (3) any other matter bearing on US national or homeland security. (JP 1-02)

near real time—Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. Also called **NRT**. (AAP-06)

operational control—Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called **OPCON**. (JP 1-02)

order of battle—The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called **OOB**. (JP 1-02)

priority intelligence requirement—(See JP1-02 for core definition. Marine Corps amplification follows.) An intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. Also called **PIR**. (MCRP 5-12C)

production management—Encompasses determining the scope, content, and format of each intelligence product; developing a plan and schedule for the development of each product; assigning priorities among the various production requirements; allocating processing, exploitation, and production resources; and integrating production efforts with intelligence collection and dissemination. (MCRP 5-12C)

radar imagery—Imagery produced by recording radar waves reflected from a given target surface. (JP 1-02)

reachback—(See JP1-02 for core definition. Marine Corps amplification follows.) The ability to exploit resources, capabilities, expertise, etc., not physically located in the theater or a joint operations area, when established. (MCRP 5-12C)

rear area—That area extending forward from a command's rear boundary to the rear of the area assigned to the command's subordinate units. This area is provided primarily for the performance of combat service support functions. (MCRP 5-12C)

security—1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (JP 1-02)

sensitive compartmented information—All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DOD 5200.1-R, Information Security Program Regulation.) Also called **SCI**. (JP 1-02)

sensor data—Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radars, counterbattery radars, and remote ground sensors. (MCRP 5-12C)

signals intelligence—1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT**. (JP 1-02)

situational awareness— Knowledge and understanding of the current situation that promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. Also called **SA**. (MCRP 5-12C)

source—1. A person, thing, or activity from which information is obtained. 2. In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. 3. In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. (JP 1-02)

special operations—Operations requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk. Also called **SO**. (JP 1-02)

surveillance—(See JP1-02 for core definition. Marine Corps amplification follows.) The systematic visual or aural observation of an enemy force or named area of interest or an area and the activities in it to collect intelligence required to confirm or deny adversary courses of action or identify adversary critical vulnerabilities and limitations. (MCRP 5-12C)

sustained operations ashore—The employment of Marine Corps forces on land for an extended duration. It can occur with or without sustainment from the sea. Also called **SOA**. (MCRP 5-12C)

synthetic aperture radar—A radar in which a synthetically long apparent or effective aperture is constructed by integrating multiple returns from the same ground cell, taking advantage of the Doppler effect to produce a phase history film or tape that may be optically or digitally

processed to reproduce an image. Also called **SAR** and known as **radar, synthetic aperture**. (MIL-HDBK-850)

tactical intelligence—(See JP1-02 for core definition. Marine Corps amplification follows.) Intelligence concerned primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and the tactical aspects of terrain and weather within the battlespace. (MCRP 5-12C)

target—1. An entity or object considered for possible engagement or other action. 2. In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. 3. An area designated and numbered for future firing. 4. In gunfire support usage, an impact burst that hits the target. (JP 1-02)

target intelligence—Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (JP 1-02)

technical control—The performance of specialized/professional service or the exercise of professional guidance/direction through the establishment of policies and procedures. Also called **TECHON**. (MCRP 5-12C)

validation—1. A process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. 3. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. (JP 1-02) (Parts 1 and 3 of a 4-part definition.)

warfighting functions—The six mutually supporting military activities integrated in the conduct of all military operations. The six warfighting functions are command and control, fires, force protection, intelligence, logistics, and maneuver.

REFERENCES AND RELATED PUBLICATIONS

Executive Orders

12333	United States Intelligence Activities
12951	Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems
12968	Access to Classified Information
13462	President's Intelligence Advisory Board and Intelligence Oversight Board
13526	Classified National Security Information

Federal Publications

United States Code, Title 10, *Armed Forces*

Department of Defense Issuances

Department of Defense Directive (DODD)

5240.01	DOD Intelligence Activities

Department of Defense Instruction (DODI)

5040.02	Visual Information (VI)

Department of Defense Manuals (DODMs)

5105.21, vol. 1	Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security
5200.01, vols. 1–4	DoD Information Security Program: Overview, Classification, and Declassification

Defense Intelligence Agency Manuals (DIAMs)

50-4	Department of Defense Intelligence Information System (DODIIS) Information Systems Security (INFOSEC) Program
57-5	DOD Exploitation of Multisensor Imagery

Defense Intelligence Agency Publications (DIAP)

5210.002-M	Standard Coding Systems Functional Classification Handbook (U)

Chairman of the Joint Chiefs of Staff Publications

Chairman of the Joint Chiefs of Staff Instruction (CJCSI)

3160.01	No-Strike and the Collateral Damage Estimation Methodology (U)
3370.01	Target Development Standards (U//FOUO)
3505.01	Target Coordinate Mensuration Certification and Program Accreditation

Chairman of the Joint Chiefs of Staff Manual (CJCSM)

3122.01_	Joint Operation Planning and Execution System (JOPES) Volume 1 (Planning Policies and Procedures)

Joint Publications (JPs)

1-02	Department of Defense Dictionary of Military and Associated Terms
2-0	Joint Intelligence
2-01	Joint and National Intelligence Support to Military Operations
2-01.3	Joint Intelligence Preparation of the Operational Environment
2-03	Geospatial Intelligence in Joint Operations
3-02	Amphibious Operations
3-13.1	Electronic Warfare
3-13.3	Operations Security
3-32	Command and Control for Joint Maritime Operations
3-59	Meteorological and Oceanographic Operations
3-60	Joint Targeting
5-0	Joint Operation Planning
6-0	Joint Communications System

Secretary of the Navy Manual (SECNAV)

Department of the Navy Foreign Disclosure Manual

North Atlantic Treaty Organization (NATO) Standardization Agreement (STANAG)

3277	Air Reconnaissance Request/Task Form

Allied Administrative Publications

AAP-6	North Atlantic Treaty Organization (NATO) Glossary of Terms and Definitions

Army Publication

Field Manual Interim (FMI)

2-01	Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization

Marine Corps Publications

Marine Corps Warfighting Publications (MCWPs)

2-2	MAGTF Intelligence Collection
2-3	MAGTF Intelligence Production and Analysis
2-4	Marine Air-Ground Task Force Intelligence Dissemination
2-26	Geographic Intelligence
3-25	Control of Aircraft and Missiles
5-1	Marine Corps Planning Process

Marine Corps Reference Publications (MCRPs)

5-12C	Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms

Marine Corps Order (MCO)

3500.32	Intelligence Training and Readiness Manual
P4790.2C	MIMMS Field Procedures Manual
5510.20B	Disclosure of Military Information to Foreign Governments and Interests

Marine Corps Intelligence Agency Publication (MCIA-)

1540-0003-03	Generic Intelligence Requirements Handbook (GIRH)

Director of Central Intelligence Directives (DCIDs)

1/8	Management of National Imagery, Imagery Intelligence, Geospatial Activities and Related Information
6/1	Security Policy for SCI and Security Policy Manual

Intelligence Community Directives (ICDs)

1	Policy Directive for Intelligence Community Leadership
104	Budgeting for Intelligence Programs
113	Functional Managers
204	Roles and Responsibilities for the National Intelligence Priorities Framework
503	Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation
700	Protection of National Intelligence
704	Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information
705	Sensitive Compartmented Information Facilities
710	Classification and Control Markings System

National Systems for Geospatial-Intelligence Documents

NSG Directives (NSGDs)

FM 1100	(U) Roles and Responsibilities of the Department of Defense (DOD) Geospatial Intelligence (GEOINT) Manager and the Intelligence Community (IC) Functional Manager for GEOINT

NSG Instructions (NSGIs)

FM 1101	(U) The National System for Geospatial-Intelligence (NSG) Policy Program
FM 1103	Governance Structure for Geospatial Intelligence (GEOINT) Functional Management
ST 8101	(U) GEOINT Data, Products, and Sources Storage Management (S//NOFORN[not releasable to foreign nationals])

NSG Manuals (NSGM)

CS 9300.02	National System for Geospatial Intelligence (NSG), (U) Marking and Dissemination Guidance (S//REL TO [release to] USA, FVEY)
CS 9300.03	National System for GEOINT–Geospatial Intelligence Classification Guide (TS//SCI//NOFORN)
CS 9300.04	National System for GEOINT–Geospatial Intelligence Classification Guide For Common Wealth Partners (TS//SCI//REL TO USA, AUS, CAN, GBR, NZL)
FA 1806	Domestic Imagery (U//FOUO)

Military Standards (MIL-STD-)

188-161_	Interoperability and Performance Standards for Digital Facsimile Equipment
188-196	Department of Defense Interface Standard: Bi-Level Image Compression for the National Imagery Transmission Format Standard
188-198A	Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format
188-199	Vector Quantization Decompression for the National Imagery Transmission Format
2500C	National Imagery Transmission Format (Version 2.1) for the National Imagery Transmission Format Standard

Military Handbooks (MIL-HDBK-)

850	Glossary of Mapping, Charting, and Geodetic Terms

Miscellaneous

Controlled Access Program Coordination Office (CAPCO), Authorized Classification and Control Markings Register (Located on JWICS)

Geospatial Integrated Digital Environment (GIDE) via Defense Intelligence Agency (Located on JWICS)

Geospatial Intelligence Classification Guide (Located on JWICS)

Imagery System Overview (IMSO) (October 2008) (Located on JWICS)

Joint Tactical Exploitation of National Systems (JTENS) Manual (Located on JWICS)

Modernized Integrated Database (MIDB) via Gemini Intelligence Portal (Located on JWICS)

National Geospatial-Intelligence Agency Imagery Policy Series [IPS] [section 9, part B], Domestic Imagery [IPS-001/98-S9A]

National Geospatial-Intelligence Agency STDI-0001V1.3/CN2 National Support Data Extensions (SDE) (Version 1.3/CN2) for the National Imagery Transmission Format (NITF)

National Geospatial-Intelligence Agency STDI-006, National Imagery Transmission Format (NITF) Version 2.1 Commercial Dataset Requirements Document (NCDRD), 18 February 2010.

National Imagery System User's Guide (NIMSUG) (May 2008)

National Imagery Interpretability Rating Scale (NIIRS)

National Imagery and Mapping Agency Imagery Policy Series (Sections 1–9)

International Telecommunications Union-Radiocommunication Sector BT.500-12, Methodology for the Subjective Assessment of the Quality of Television Pictures

Motion Imagery Standards Board, MISB RP 0901.1, Recommended Practice, Video-National Imagery Interpretability Rating Scale

Motion Imagery Standards Profile, MISP version 6.4

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes through the Universal Need Statement (UNS) process. The UNS submission process is delineated in Marine Corps Order 3900.15_, *Marine Corps Expeditionary Force Development System*, which can be obtained from the on-line Marine Corps Publications Electronic Library:

http://www.marines.mil/News/Publications/ELECTRONICLIBRARY.aspx.

The UNS recommendation should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Addition/deletion of text
  - Proposed new text

Additional copies: If this publication is not an electronic only distribution, a printed copy may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status*. An electronic copy may be obtained from the United States Marine Corps Doctrine web page:

https://www.doctrine.usmc.mil.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

RESTRICTED

FM 30-21

WAR DEPARTMENT

BASIC FIELD MANUAL

MILITARY INTELLIGENCE
ROLE OF AERIAL PHOTOGRAPHY

RESTRICTED

BASIC FIELD MANUAL

MILITARY INTELLIGENCE

ROLE OF AERIAL PHOTOGRAPHY

CHANGES
No. 1

WAR DEPARTMENT,
WASHINGTON, May 27, 1942.

FM 30–21, November 1, 1940, is changed as follows:

■ 16. TITLING OF NEGATIVES.

* * * * * * *

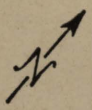
c. Method.

* * * * * * *

(4) Scale of photograph expressed as a representative fraction or as altitude above ground in feet and focal length of camera.

* * * * * * *

(8) Serial number of negative. In addition to a north point, the following is the legend on a vertical:



Saranac, N. Y.—(321–437)—1: 20,000—(2:00 P. M.)—(24–Aug–40)—97th—M5.

The information given above may also appear in different sequence, giving approximately the same information.

* * * * * * *

[A. G. 062.11 (3–27–42).] (C 1, *May 27, 1942.*)

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
Chief of Staff.

OFFICIAL:

J. A. ULIO,
Major General,
The Adjutant General.

U. S. GOVERNMENT PRINTING OFFICE: 1942

RESTRICTED

BASIC FIELD MANUAL

MILITARY INTELLIGENCE

ROLE OF AERIAL PHOTOGRAPHY

CHANGES No. 2

WAR DEPARTMENT,
WASHINGTON, December 28, 1942.

FM 30–21, November 1, 1940, is changed as follows:

SECTION VII (ADDED)

GRAPHICAL REPRESENTATION OF INFORMATION

■ 57. RECORDING CHANGE.—*a.* In the G–2 section of any unit, information on enemy activity is obtained by a number of different types of studies. A means of recording changes should be used which fits both the situation and the purpose for which the information is obtained.

b. In forward positions, changes in such activities as entrenchments, obstacles, antitank fortifications, barbed wire, communications, supply installations, and dummy positions must be recorded. The most common means of recording such information is by conventional signs and symbols on maps or overlays. However, in the case of installations far to the rear or in the event of stabilization in a forward area, there are certain types of information which may best be recorded graphically.

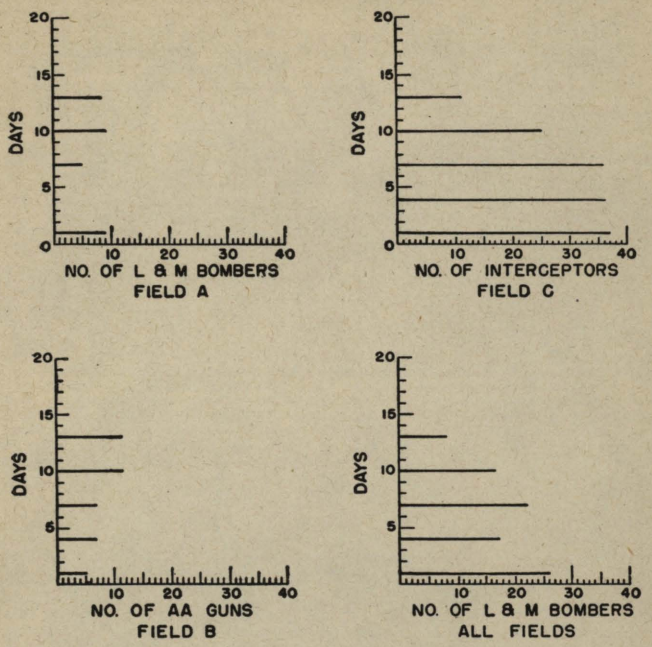
■ 58. GRAPHICAL REPRESENTATION.—Quantitative changes in enemy installations which occur over a period of time are best recorded graphically. Examples of such installations are dumps, camps, and landing fields. Graphic representation gives the degree of use of such installations, whereas indicating them on a map merely shows their presence.

■ 59. EXAMPLE.—The following is an example of the use of graphic representation: In a given theater three advance landing fields have been located and all have been photographed from 25,000 feet. The intelligence mission requires photographing

499962°—42

those fields every 3 days in order to determine enemy activity there. At the end of 13 days the following information is available from interpretation of the aerial photographs:

	Planes present			Dumps	Anti-aircraft		Vehicles	Buildings		Tents
RECORD—FIELD A										
Day	L. & M. bombers	Interceptors	Others	Present	Guns	Machine guns	Present	Under construction	Present	Present
1st	9	10	2	2	12	15	15	0	0	2
4th	0	0	2	2	12	15	12	0	0	2
7th	6	0	2	2	12	15	8	0	0	2
10th	9	10	1	2	12	15	13	0	0	2
13th	9	8	1	2	12	15	12	0	0	0
RECORD—FIELD B										
1st	0	0	1	1	4	12	3	0	1	6
4th	0	3	0	1	8	12	8	0	1	6
7th	0	9	1	1	8	12	5	0	1	6
10th	0	9	3	2	12	24	23	4	1	18
13th	0	8	2	2	12	24	17	4	1	18
RECORD—FIELD C										
1st	18	36	5	5	20	30	23	0	8	3
4th	18	35	5	5	20	30	27	0	8	0
7th	18	35	3	5	20	30	19	0	8	0
10th	9	24	0	5	12	24	14	0	7	0
13th	0	10	0	5	12	24	11	0	4	0
RECORD—ALL FIELDS										
1st	27	46	8	8	36	57	41	0	9	11
4th	18	38	7	8	40	57	47	0	9	8
7th	24	44	6	8	40	57	32	0	9	8
10th	18	43	4	9	36	63	50	4	8	20
13th	9	26	3	9	36	63	40	4	5	18



The line graphs shown above give one method of plotting graphically the information in the preceding table. Anyone interested in any particular installation or operation can tell at a glance by the length of the horizontal lines what change or progress is taking place.

[A. G. 062.11 (10–22–42).] (C 2, Dec. 28, 1942.)

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
Chief of Staff.

OFFICIAL:

J. A. ULIO,
Major General,
The Adjutant General.

U. S. GOVERNMENT PRINTING OFFICE: 1942

RESTRICTED

FM 30–21

BASIC FIELD MANUAL

MILITARY INTELLIGENCE
ROLE OF AERIAL PHOTOGRAPHY

Prepared under direction of the Chief of Staff

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1940

WAR DEPARTMENT,
WASHINGTON, *November 1, 1940.*

FM 30–21, Military Intelligence, Role of Aerial Photography, is published for the information and guidance of all concerned.

[A. G. 062.11 (7–30–40).]

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
Chief of Staff.

OFFICIAL:

E. S. ADAMS,
Major General,
The Adjutant General.

TABLE OF CONTENTS

		Paragraph	Page
SECTION I.	GENERAL.		
	Purpose	1	1
	Scope	2	1
	Importance of photographs	3	1
	Vertical aerial photographs	4	2
	Oblique aerial photographs	5	4
	Night photographs	6	4
	Infrared photography	7	4
	Color photography	8	5
	Quick work photography	9	5
	Specialist examiners of aerial photographs	10	5
	References	11	6
II.	COORDINATION OF AERIAL PHOTOGRAPHY.		
	Responsibility	12	7
	Photographic reconnaissance	13	7
	Photographic capabilities of aviation units	14	8
	Requests for aerial photographs	15	8
	Titling of negatives	16	9
	Execution of photographic missions	17	10
	Action of G–2 upon receipt of photographs	18	11
	Action of topographic engineers	19	12
	Filing of negatives	20	12
III.	USE TO BE MADE OF AERIAL PHOTOGRAPHS.		
	General	21	13
	As a map	22	13
	In preparation of objective folders	23	13
	In engineering planning	24	14
	In planning for attack upon fortifications	25	14
	In determining information of enemy	26	14
	By artillery	27	15
	In landing operations	28	16
	In river crossings	29	16
	In counterintelligence	30	17
IV.	IDENTIFICATION OF OBJECTS FROM AERIAL PHOTOGRAPHS.		
	General	31	17
	Purpose	32	17
	Basis of identification	33	17
	Method of examination	34	19

TABLE OF CONTENTS

	Paragraph	Page
SECTION V. IDENTIFICATION OF ENEMY ACTIVITIES FROM AERIAL PHOTOGRAPHS.		
General	35	20
Camouflage	36	21
Roads, tracks, and paths	37	21
Types of works	38	22
Trenches	39	22
Breastworks	40	23
Organized shell holes	41	23
Wire	42	24
Dugouts	43	24
Machine guns	44	24
37-mm guns or similar weapons	45	26
Listening, observation, and command posts	46	26
Antitank obstacles and road blocks	47	26
Mine shafts	48	27
Concrete fortifications	49	27
Location of batteries	50	27
Study of effect of our own artillery fire	51	29
Buried cables and overhead telegraph and telephone lines	52	29
Rear installations	53	30
VI. INTERPRETATION.		
General	54	31
Evidence of enemy's intentions as revealed by aerial photographs	55	31
Interpretation during our own offensive operations	56	33
APPENDIX. LIST OF REFERENCES		85
INDEX		87

RESTRICTED

BASIC FIELD MANUAL

MILITARY INTELLIGENCE

ROLE OF AERIAL PHOTOGRAPHY

(The matter contained herein supersedes TR 210–10, January 4, 1926.)

SECTION I

GENERAL

■ 1. PURPOSE.—The purpose of this manual is to prescribe the procedure for the coordination of aerial photography, to furnish a guide for the determination and interpretation of military information shown on aerial photographs, and to serve as a reference in the training of personnel in the tactical study of aerial photographs.

■ 2. SCOPE.—In addition to providing the necessary coordination between ground and air troops in the production and utilization of aerial photographs, this manual covers the fundamentals of tactical interpretation of aerial photographs to the extent needed by military intelligence personnel. The manual does not duplicate the information contained in FM 21–25 and FM 21–26 (now published as TM 2180–5). Those manuals cover the more detailed instruction needed by all map users, while this manual is confined to the coordination and tactical aspects only.

■ 3. IMPORTANCE OF PHOTOGRAPHS.—Aerial photographs are one of the most important sources of information available to a commander as well as to all echelons of command. As a source of combat intelligence they are of paramount importance to all intelligence sections, for when successfully interpreted they frequently reveal the most carefully guarded secrets in hostile territory. When properly titled, they are a

type of map showing innumerable details and later information not shown on the best topographic maps. When examined stereoscopically, they are of the greatest importance in studying the terrain. In the field of counterintelligence, they are important as a check upon the use of natural and artificial concealment and of camouflage discipline.

■ 4. VERTICAL AERIAL PHOTOGRAPHS.—*a. General.*—A vertical aerial photograph is one which is taken when the lens axis of the camera is approximately perpendicular to the earth's surface. Such photographs are very useful in making terrain studies and in gaining information of enemy activity, in the preparation and revision of maps, and, when suitably marked, as map substitutes.

b. Pinpoints.—Two or more stereoscopic vertical photographs of an isolated object or spot constitute a pinpoint. Airdromes, supply depots, dumps, road crossings, bridges, or other bottlenecks on lines of communication requiring detailed study are suitable objects for pinpoint photography. (Fig. 1.)

c. Mosaics.—An aerial mosaic is an assembly of two or more overlapping vertical photographs as described in FM 30–20. The mosaic is the most common form of photomap which will be encountered. In intelligence studies, the mosaic is especially useful in studying features that cannot be followed out completely on one photograph, such as paths, roads, railroads, etc. The principal purpose is to show an entire area in one photograph for use as a check upon new information, and to assist examining officers in comparing data on photographs with data shown on existing maps.

d. Stereo-pairs.—(1) *General.*—For details concerning stereoscopic photography and stereoscopic examination of aerial photographs see FM 21–26 (now published as TM 2180–5).

(2) *Use.*—As it is customary to make vertical aerial photographs, with an overlap, stereoscopic examination of any photographed area is possible. This should be the normal procedure in studying aerial photographs for military information. In addition to furnishing valuable information concerning the topography of a given area, stereo-pairs supply

still more valuable information concerning enemy activities. They are useful in overcoming the effect of camouflage and in locating various installations. They facilitate the detection of numerous details which could not otherwise be recognized on the ground. A stereoscopic examination makes it possible to determine in advance the effect of the terrain upon the location of defensive positions and of covered routes thereto, upon lines of supply and evacuation, upon tanks, upon observation and command posts, and upon axes of signal communication.

e. Scale.—(1) *General.*—Vertical photographs for intelligence purposes should be made of small, medium, or large scale, depending upon the purpose for which required.

(2) *Small.*—Small scale aerial photographs (1:15,000 or smaller) cover a large area but show comparatively little detail. They are of value, for they furnish considerable information concerning camps, dumps, railway activity, large demolitions such as the destruction of bridge spans 150 feet or more in length, and heavy mine craters, trench systems in open terrain, new road and rail construction, and large bodies of troops except in wooded or brush-covered country. They are also used in the preparation and revision of maps. (Figs. 12 and 50.)

(3) *Medium.*—Medium scale aerial photographs (1:10,000 to 1:15,000) show sufficient detail for ordinary intelligence and counterbattery purposes. Partly organized trench systems, airplanes on the ground, outlines of airdromes and airfields, railroad trains, columns in close formation on roads, partly concealed dumps and depots, areas upon which heavy artillery concentrations have been placed, battery positions, detail of trenches, and other field works may be seen. (Fig. 28.)

(4) *Large.*—Large scale aerial photographs (1:5,000 to 1:10,000) show great detail and are of use in distinguishing between genuine and dummy gun positions, in locating camouflage work, tank mine fields, railway cars, motorized and horse-drawn vehicles, shell holes and exploded tank mines, observation and command posts, machine gun emplacements, road barriers, demolitions of small bridges and culverts, indications of troop concentrations, such as tracks, paths,

poorly concealed equipment, pole lines carrying telegraph and telephone circuits, open wire and cable lines, bands of wire entanglements, and many other details. Large scale photographs should be limited to pinpoints. (Figs. 1 and 17.)

■ 5. OBLIQUE AERIAL PHOTOGRAPHS.—*a. General.*—Any aerial photograph which is not a true vertical is an oblique. In an oblique photograph the perspective is somewhat distorted due to the inclination of the lens, and the scale varies rapidly from the foreground to the rear. Information obtained from such photographs should always be carefully checked against a vertical photograph or map or both; otherwise the distorted perspective may cause serious errors in the location of points.

b. High oblique photographs.—A high oblique photograph is an oblique which shows the terrain up to the line of the horizon. It is very useful to the command, showing clearly the general form of the terrain and the succession of enemy organizations just as one would see them from a very high point of observation. (Fig. 2.)

c. Low oblique photographs.—Low oblique photographs, particularly those taken close to the ground, cover less terrain than high obliques but give more detail. They facilitate a correct understanding of relief, make slopes and sunken roads stand out, and reveal the breaks and gaps not visible on single vertical photographs. (Fig. 3.)

■ 6. NIGHT PHOTOGRAPHS.—Under favorable conditions, vertical photographs can be taken at night with the aid of auxiliary lighting equipment at elevations up to about 8,000 feet above the ground. Because of the fleeting nature of the light, night photographs are usually limited to single exposures, although small strip mosaics can be made. There is little difference between the detail shown on night and daylight photographs, but because the former must be taken at a comparatively low altitude one exposure necessarily covers a smaller area. (Fig. 4.)

■ 7. INFRARED PHOTOGRAPHY.—Infrared photography is taken on a special film which, while it is somewhat sensitive to most colors, is especially sensitive to infrared light. On this film,

objects register in black, white, or gray, primarily according to the amount of infrared light they reflect. Thus the relative shades of gray in which objects register on infrared film differ from the relative shades of gray in which they register on panchromatic film.

■ 8. COLOR PHOTOGRAPHY.—Color transparencies render colors in approximately their true values from altitudes of about 5,000 feet. At very low altitudes, color film requires such long exposure that motion is apparent. At altitudes in the vicinity of 10,000 feet and higher, color pictures are far too blue to be of great value. Color transparencies, except Dufay color transparencies, are slow and difficult to make and reproduce. However, because they give a grainless, easily interpreted picture and under suitable conditions render colors about as seen by the human eye, they will be used in war. Increased use may be expected as color photography is improved.

■ 9. QUICK WORK PHOTOGRAPHY.—Aerial photographs can be produced in whole or in part in the airplane by the quick work process and delivered direct to appropriate headquarters. In this type of photography no negatives are prepared, the image being recorded directly on the print itself. Normally, the photographic quality of the print will not be equal to that of a print processed in the usual manner. Neither can reproductions be made without rephotographing the picture. Quick work photography will have its greatest application during the actual progress of maneuver warfare, when time does not permit the orderly processing of films and the printing and distribution of the prints. This process makes possible the delivery of photographic information to the intelligence officer a matter of minutes only.

■ 10. SPECIALIST EXAMINERS OF AERIAL PHOTOGRAPHS.—*a.* In divisions and higher echelons of command, the intelligence section may include one or more specialists in the examination of aerial photographs. These specialists should have a thorough knowledge of the organization, marching and bivouacking characteristics, transportation, methods of combat, field fortifications, supply system, disposition of aviation units

on the ground, camouflage, and intelligence procedure of our own Army. In addition, they should have a thorough knowledge of the same things in the enemy's army. They should be patient and persevering and possess keen, observant, analytical minds.

b. The examiner should have, in proper working order, all necessary equipment and material for his work. Among essential items in all echelons should be included the enemy's or our own field fortification and camouflage regulations, maps and aerial photographs of the area, drafting equipment, stereoscope, mimeoscope, rubber cement, and files. The lower echelons will have only simple equipment.

c. The examiners should collaborate closely with intelligence personnel charged with the examination of prisoners, repatriates, and captured documents; with terrestrial and aerial observation agencies; and with sound and flash ranging troops. In this way it will frequently be possible to clarify doubtful items. As assistant intelligence officers, these specialists should be familiar with the intelligence plan and the essential elements of information of the unit to which they pertain. In the course of operations they should be kept fully informed concerning the enemy's organization, plans, activities, fortifications, and movements.

d. During the progress of operations, the specialist examiner should make a detailed study of terrain, objects, and defenses captured from the enemy. If practicable, he should be accompanied by a Signal Corps photographer for the purpose of securing close-up ground photographs of items shown on aerial photographs. In this way he perfects his knowledge of the enemy and completes a working album to assist him in his future work. Whenever possible, he should also study the appearance of identified enemy objects and works from the air.

■ 11. REFERENCES.—Field Manuals pertaining to aerial photography, mapping, and camouflage are listed in the Appendix.

SECTION II

COORDINATION OF AERIAL PHOTOGRAPHY

■ 12. RESPONSIBILITY.—*a.* The *commanding officer* of an organization to which Air Corps units are assigned or attached is responsible for the coordination of photographic missions within his own and subordinate units. He is also responsible for policies relative to the distribution of aerial photographs to all subordinate echelons within the command. In the performance of these duties he is assisted by his assistant chief of staff, G–2.

b. The assistant chief of staff, G–2 of the organization to which photographic aviation is assigned or attached, acting under the authority of the commanding officer thereof, is directly responsible for the coordination between Air Corps units and available topographic engineers, and, with due regard to the essential elements of information announced by the commander, for the coordination of photographic missions of the aviation of his own and subordinate echelons. He is also responsible for the coordination of aerial photography with the other collecting agencies and for making the necessary aerial photographs available to them.

■ 13. PHOTOGRAPHIC RECONNAISSANCE.—*a.* Aerial photographs may be made by aviation units while engaged on combat or reconnaissance missions without specific instructions from higher headquarters. Such photographs are frequently of great importance in making studies of certain activities or terrain features.

b. Photographic reconnaissance missions may be directed by higher headquarters. As far as practicable, such missions must be executed as prescribed in order that the results expected may be obtained.

c. Photography as a means of securing military information has certain definite advantages and disadvantages as compared with visual reconnaissance. It furnishes an exact and convenient document for study and a detailed, accurate, and complete record, since nothing escapes the lens of the camera. However, it is quite sensitive to atmospheric conditions and enemy antiaircraft activities, and the resulting information is delayed in reaching the user by the technical

processes incident to developing and titling the negative and making and delivering the prints. Before making requests for photographs, all responsible officers should take these considerations into account.

d. For the successful accomplishment of aerial photographic missions, it is imperative that all training emphasize the necessity for speed during the several steps in processing while maintaining a high technical quality in the finished product. The necessity of reducing to the minimum the time between exposure of the negative and the delivery of the print must be appreciated by all observation personnel.

■ 14. PHOTOGRAPHIC CAPABILITIES OF AVIATION UNITS.—*a.* The GHQ reconnaissance squadrons and army and corps observation squadrons are provided with trailer laboratory facilities. Working at maximum speed under favorable conditions, a trained photographic section is capable of the following photographic production:

Photographs	Time requisite to produce		Remarks
	From trailer laboratory	From trailer laboratory and other facilities	
Negatives	*Hours*	*Hours*	
15 (5 prints each)	2	1½	Prints partially dried; titled but not interpreted.
50 (5 prints each)	4	3	Do.
100 (5 prints each)	5	4	Do.
Prints			
1,500–2,000	24		Do.
3,000–5,000		24	Do.

b. All agencies making requests for photographs should understand these capabilities.

■ 15. REQUESTS FOR AERIAL PHOTOGRAPHS.—*a.* Requests for aerial photographs will be made through normal channels to the commander of a unit to which observation aviation is attached or assigned. They may be made in writing or

orally, but in any case must contain the following essential information:

(1) Map area or point to be photographed.

(2) Approximate hour of exposure.

(3) For oblique photograph, direction from which to be taken and elevation.

(4) For vertical photograph, the scale expressed as R. F.

(5) Purpose for which the photograph is desired.

(6) Number of prints desired and time and place of delivery.

b. Acting under the authority of the commander thereof, the assistant chief of staff, G–2, of a unit will coordinate all requests for aerial photographic missions and assign a priority to each, taking into account the essential elements of information and the needs of other sections of the general staff and of subordinate units. Requests which remain unexecuted at the end of the day will be considered in connection with later requests and assigned a new priority in conformity with their urgency.

■ 16. TITLING OF NEGATIVES.—*a. General.*—The titling of negatives is the responsibility of the Air Corps. The method employed must be uniform and must include data necessary for ready identification of the area represented, both on the map and on the ground. All prints should be made from the full negative without masks, so that every portion of the negative, including title, will show on the print.

b. Grid systems.—(1) AR 300–15 prescribes various types of grid systems applicable to military maps. All personnel concerned with the production and use of aerial photographs should be familiar with the various systems.

(2) The coordinates of the center of photographs will be indicated (*c* below). If the military grid appears on any of the maps existing for the theater, it will be used in expressing these coordinates. If the military grid is not available, the atlas grid shown on the largest scale map issued to the troops will then be substituted. If neither the military nor the atlas grid is available, a geographic grid will be improvised. For example, a point at 117°40′30″ west longitude; 50°38′00″ north latitude, should be expressed by coordinates

as: 11740W5038N, the nearest minute only being used to express the coordinates.

c. Method.—The titling of aerial photographs made for intelligence purposes in the theater of operations and in all tactical exercises will be in letters and numerals ⅛ inch in height along the black strip at the bottom, reading from left to right, as follows (figs. 6 and 7):

(1) An arrow ½ inch in length in lower left-hand corner of the negative indicating north, with letter N superimposed over center of the shaft.

(2) Name of locality or nearest locality.

(3) Approximate coordinates of the center of the photograph.

(4) Scale of the photograph expressed as representative fraction, in case of a vertical; altitude above the ground in feet and focal length of camera, in case of an oblique.

(5) Hour.

(6) Date arranged in the following order: day, in figures; month, in letters; and year, in figures.

(7) Designation of squadron.

(8) Serial number of the negative.

d. Reconnaissance strips.—The first photographs of a reconnaissance strip will be titled as prescribed in *c* above. The other photographs of the strip will only be numbered serially.

■ 17. EXECUTION OF PHOTOGRAPHIC MISSIONS.—*a. General.*—The commander of a designated observation squadron executes photographic missions in accordance with the priority and conditions specified on the approved request of the headquarters to which assigned or attached.

b. Preparation of photographs.—Upon the successful completion of a photographic mission, the negatives are developed and titled without delay, and a minimum of from 5 to 22 prints, except those made exclusively for mapping purposes, are prepared in accordance with the instructions of G–2.

c. Distribution of photographs.—One print is retained by the observation squadron, and the remaining prints and the negatives are sent to the G–2 of the unit to which the squadron pertains. The intelligence liaison officer from the corps

or army, if present, studies the retained print for information of immediate importance, which, if found, is transmitted to the G–2 of the higher unit by the most rapid means of communication available.

■ 18. ACTION OF G–2 UPON RECEIPT OF PHOTOGRAPHS.—*a. Redistribution.*—Upon the receipt of aerial photographs from the observation squadron, G–2 will ordinarily redistribute them as follows:

	Number of copies
Commander of next higher unit	1
Retained by G–2 of unit	2
Unit topographic company or battalion	1
Unit air officer	1
Unit artillery officer	1
Commander of subordinate unit requesting photograph [1]	([2])

[1] To be redistributed as directed by the commander concerned.
[2] Remaining copies (ordinarily not more than 15).

b. Final study for determination of military information.—One copy of each aerial photograph retained by G–2 should be studied in great detail, including stereoscopic examination if stereo-pairs are available, and in connection with other photographs of the same area and items of information made available by other collecting agencies, with a view of determining all possible military information shown on the photograph. The study should be coordinated with the specialized studies of other copies of the photograph made by the artillery intelligence section and the Air Corps intelligence service. Only when interpretation has been definitely made will items of information be reported as facts. All doubtful items will be referred to other collection agencies for verification. All items definitely determined will be disseminated by G–2 and considered by him in the preparation of estimates of the enemy capabilities and intentions. After this copy of the photograph has otherwise served its purpose, the area shown on the photograph and its serial number and date are entered on a graphic index map (fig. 5), and the photograph is then filed according to the area for future reference. The index of the 1:20,000 map will be the filing index. Each print will be filed in folders according to its coordinates, each folder to cover the area of one of the 1:20,000 map sheets.

c. Study to determine value as a map.—While the first copy of the aerial photograph retained by G–2 is being studied for military information, the second copy should be evaluated for its possible use by subordinate echelons of command as a map or as a supplement to existing maps. Based upon this study, G–2 will issue instructions to the appropriate topographic company or battalion for its reproduction by lithography or contact printing by the multiple rapid printer when available, and for its distribution to subordinate units. Each photograph will frequently be useful to subordinate units down to and including the infantry platoon and tank section. As many as 400 copies of such lithographs or contact prints may be required, and these must receive early distribution to be of maximum value. When this copy has otherwise served its purpose, it should be turned over to the officer charged with examination of enemy personnel, repatriates, and captured documents for possible use in connection with his work.

d. G–2 report.—In order that all elements of command may be informed of available photographs, a list of successful photographic missions will be included in each G–2 report.

■ 19. ACTION OF TOPOGRAPHIC ENGINEERS.—*a. Determination of topographic data.*—The copy of each aerial photograph furnished the topographic company or battalion should be studied in connection with the best available map, photomap, or mosaic with a view of determining topographic data that may be of value in any future revision of the map, photomap, or mosaic. When this study is completed, the print is filed for future reference in the same manner as prescribed in paragraph 18*b*.

b. Distribution of lithographs or contact prints.—From the negatives of each photograph furnished by G–2, the topographic company or battalion completes and distributes in the manner prescribed in FM 30–20 lithographs or contact prints of each aerial photograph as directed by the commanding officer.

■ 20. FILING OF NEGATIVES.—G–2 of the corps or army will maintain a file of negatives of aerial photographs. If requests are made for additional photographs, the topographic

company or battalion will be directed to reproduce as contact prints or as lithographs the necessary copies. Negatives will be retained by G–2 as long as required, ordinarily not longer than 3 months, and then sent to a central record section to be designated by the theater commander, where they will be filed for final disposition upon the termination of hostilities.

SECTION III

USE TO BE MADE OF AERIAL PHOTOGRAPHS

■ 21. GENERAL.—There are many uses for aerial photographs in modern warfare. They are of value not only in determining information of the enemy and the terrain but also in the preparation and execution of all types of operations. This section deals only with some of their more important uses as intelligence documents.

■ 22. AS A MAP.—*a.* Maps are graphic representations of the terrain; aerial photographs are detailed representations of the terrain as it appears at a particular time. Therefore, when properly titled, vertical photographs should be considered as maps, even though the exact scale is not known and some distortion of detail may exist. If taken shortly before the time of use they are extremely important as supplements to maps, showing all details at the time of exposure.

b. High oblique photographs taken in the direction of march are especially convenient and valuable as road maps. They are also of great value in the preparation of operation maps. However, there is a certain amount of danger involved in the use of the oblique as a map because of the distortion of scale and the false perception of increased elevation in the background of such a photograph.

■ 23. IN PREPARATION OF OBJECTIVE FOLDERS.—Aerial photographs of fixed installations, towns, bottlenecks on lines of communication, and important terrain features are extremely significant in air operations and should be included in objective folders whenever available. (Fig. 1.) They are also of great assistance in planning and executing mechanized operations.

■ 24. IN ENGINEERING PLANNING.—*a.* In planning the engineering work which will be required in territory held by the enemy, but over which an advance is planned, study of aerial photographs of the area is essential. The amount of destruction, actual or to be expected, can be estimated, width of structures or streams computed, amount of materials estimated, mine fields located, conditions of roads determined, location of engineering supplies revealed, and much other preliminary planning work completed, prior to occupation of the terrain.

b. Aerial photographs may be of great value in planning demolitions, particularly for demolitions over a large area. The photographs have greatest value in making detailed studies of demolitions in defiles and on river lines and in planning antitank mine fields. Since demolitions on a large scale are normally planned for terrain which is to be released to the enemy, photographs may frequently be secured at a larger scale than can be expected of terrain held by the enemy. In making the demolition plan, the study of these aerial photographs should supplement personal reconnaissance and assure that no important structures or works at critical points are overlooked. When time for personal reconnaissance is not available, aerial photographs are of maximum value and if of sufficiently large scale may reveal sufficient data on which to plan the demolition.

■ 25. IN PLANNING FOR ATTACK UPON FORTIFICATIONS.—Detailed information concerning defensive arrangements, areas that cannot be covered by the defender's fire, and camouflage, especially on lines of communication necessary for the attack of a fortification or fortified position, may be gained from a study of aerial photographs. Results of these studies should be confirmed by terrain studies and reconnaissance in force, if this is necessary. Based upon this information, the composition of the troops as well as the necessary equipment and material and the special training measures to insure the successful execution of the attack can be determined. (Fig. 8.)

■ 26. IN DETERMINING INFORMATION OF ENEMY.—*a.* If systematically exploited as a direct source and as a check upon

other sources, aerial photographs will disclose information about the enemy that can be obtained by no other means. Information derived from all sources should be coordinated and items from the various collecting agencies checked against each other and studied under the direction of the G–2 of the unit concerned. Latest aerial photographs should be compared with earlier ones to determine the most recent work or activities of the enemy.

b. An aerial mosaic of the area traversed by a prisoner of war or repatriated national is frequently of great value in the examination of such personnel. Based upon information which he furnishes, the route traversed by a prisoner prior to his capture is marked on a mosaic. The prisoner is then questioned concerning doubtful items shown on pinpoints along the route. In this way, much information is acquired concerning objects which otherwise cannot be identified. Information furnished by a prisoner or repatriate should be checked against items which are already known or verified by rephotographing and restudying the object. The accuracy of a prisoner's or repatriate's statements concerning items that have been definitely verified will establish the degree of credence to accord him.

c. Captured documents frequently constitute an excellent means of identifying objects on aerial photographs especially if made on the same date. Sketches should be carefully examined for notations of machine guns, mortars, fake works, and other items which can be checked by use of aerial photographs.

d. Appropriate artillery intelligence sections will study aerial photographs to determine enemy artillery activities and the location of bottlenecks on lines of communication, railheads, dumps, observation and command posts, and bivouac or assembly areas. The work of the artillery intelligence sections of subordinate echelons is reviewed and their findings compared with and incorporated in those of the artillery section of the higher unit. In this manner the enemy artillery situation on the front of the division, corps, army, and the entire front is established and kept up to date.

■ 27. By Artillery.—Aerial photographs are of particular value to the artillery in the determination of targets and the

effect of fire. (Figs. 9 and 10.) In the absence of an accurate map, they are indispensable as a means of planning fire support and of controlling unobserved fire. They are very useful in the reconnaissance and selection of positions and of routes thereto; by the use of suitable aerial photographs many artillery survey operations may be avoided. They are valuable in testing the effectiveness of artillery camouflage and are a means of verifying the reports of other information gathering agencies such as observation battalions.

■ 28. IN LANDING OPERATIONS.—*a.* Aerial photographs of beaches and the adjacent terrain made prior to a landing will prove of greatest value. (Fig. 11.) In good weather both natural and man-made obstructions to landing operations can be located from photographs. The nature of the beach, whether steeply shelving or gently shelving, which is very important to a landing force commander in his decision as to the feasibility of landing on a certain beach, can also be determined. A very accurate estimate of wave heights can also be made from a study of stereoscopic pairs. Color transparencies are especially valuable in studies of the beaches and frequently reveal the unobstructed channels and the nature of the bottom.

b. Photographs taken during and after landing, if completed by the quick work process, will prove of the greatest value in determining the enemy reaction and the progress of our own troops. They should be delivered to the troops ashore as well as to the higher command afloat.

■ 29. IN RIVER CROSSINGS.—In planning a river crossing, aerial photographs should be made of those reaches of the river for which crossings are contemplated. These photographs, particularly when examined stereoscopically, will facilitate the selection of ferrying points and bridge sites for the various crossings. They may reveal conditions existing on both sides of the river, the character of the river banks, the river bed, the location of underwater obstructions, both natural and man-made, the defensive arrangements of the enemy, and the location of shoal spots or rapids in the river. Cover for preliminary concentration of material may also be located by study of aerial photographs. (Fig. 12.)

■ 30. IN COUNTERINTELLIGENCE.—*a.* Aerial photographs of areas or positions occupied by our own troops furnish the very best evidence of success or failure of counterintelligence measures adopted for the protection of troops on the ground. Faulty camouflage work, breaches of camouflage discipline, and failure to utilize natural cover may be detected easily on photographs. (Figs. 13 and 14.) Photographs are also valuable in planning dummy works, installations, and airdromes and in checking their deceptive worth.

b. Photographs are of great importance to the engineers charged with the development of measures for the protective coloration and camouflage of individual and organizational equipment and matériel.

SECTION IV

IDENTIFICATION OF OBJECTS FROM AERIAL PHOTOGRAPHS

■ 31. GENERAL.—Man is accustomed to viewing objects horizontally or, if looking down from a height, obliquely. A vertical aerial photograph portrays military objects in an unfamiliar aspect. Objects which form regular lines, in general, are easy to identify on aerial photographs, but difficulties are encountered in identifying concealed or small objects which present no contrast of shade with surrounding objects, and in identifying deliberately concealed military features. The solution of these difficulties requires special knowledge, training, and experience.

■ 32. PURPOSE.—The purpose of identification is to determine the objects shown on an aerial photograph and to discover obscure or hidden features through related visible ones.

■ 33. BASIS OF IDENTIFICATION.—*a. General.*—To identify objects shown on aerial photographs, the examiner relies in general on familiarity with the characteristic appearance of certain objects on aerial photographs, shadows, texture, differences as compared with former photographs, and information from other intelligence sources.

b. Characteristic appearance.—Through experience gained in working with aerial photographs and by frequent flights

in the air, the interpreter should acquire a knowledge of the appearance of objects as viewed from above.

c. Light and shade.—(1) *General.*—Objects on aerial photographs are generally identified by a study of light and shadows. If not correctly understood, shadows will give a reversed impression, causing elevations to appear as depressions and depressions as elevations. *Vertical aerial photographs should be held so that the shadows fall toward the examiner.* In an oblique aerial photograph, shadows play no part. If observed in the direction of exposure, they will give a clear impression of what has been photographed.

(2) *Shadows and form.*—Shadows will show the shape of an object which is perhaps otherwise unrecognizable on a vertical photograph.

(3) *Shadows and size.*—The shadows cast by different objects will be in direct proportion to their height. The approximate size of objects may, therefore, be determined by comparing their shadows with those of objects of known height. This should be done with caution because of the effect of slope of ground upon length of shadow.

(4) *Shadows and relief.*—While gentle slopes usually cannot be distinguished on vertical aerial photographs, the crests of sharper slopes as a rule may be identified by the difference in light reflected by the two slopes. Ravines and the deeper depressions are indicated by the darker coloring of such areas. Hills may also be indicated by their shadows.

(5) *Shadows and camouflage.*—Shadows will reveal camouflage which otherwise might be invisible. Fake shadows which are sometimes employed in camouflage work should be easily identified on aerial photographs.

d. Texture.—The arrangement of the constituent parts of a material is known as "texture." A change in this arrangement has a direct effect upon the reflection or absorption of light and therefore upon photograph negatives. As footprints, trails, tracks, spoil, works, and sometimes camouflage itself cause a change in the texture of the earth's surface or the vegetation thereon, they will be revealed on aerial photographs and will establish a record of many activities in a given area.

e. Confirmation.—Information gleaned from aerial photographs should be confirmed by evidence from other collecting agencies whenever possible. Liaison between the specialist examiner of aerial photographs and assistant intelligence officers specializing in other fields should facilitate this work.

■ 34. METHOD OF EXAMINATION.—*a. General.*—Aerial photographs should be examined systematically and objectively. The examiner should concentrate on each detail of a photograph. He should avoid jumping at conclusions, but should bear in mind every possible identification of any particular detail. After considering the various probabilities, he should determine whether or not there is sufficient evidence to justify a definite decision. Photographs taken on a single mission may give little definite information, but if considered with other photographs, intelligence summaries, and statements of prisoners, much valuable positive or negative information may be obtained.

b. Procedure.—(1) *Preliminary examination.*—The preliminary examination begins with the orientation and location on the best available map of the area shown on the photograph. Conspicuous terrain features, such as stream lines, railways, highways, and villages, are oriented with the map. The photograph is first examined with the naked eyes. After this is completed, a detailed examination of the picture is made with a magnifying glass and with a stereoscope, if stereo-pairs are available, to determine information that might have been overlooked.

(2) *Comparison of old and new photographs.*—A comparison of old and new photographs of the same area will reveal changes which have been made in the intervening period. On arriving in a new area, it is advantageous to photograph the terrain to show its exact condition at the time of arrival. Later this will facilitate the gathering of information in the area. Upon relief, a unit should turn over its file of photographs to the relieving unit.

(3) *Study of area as a whole.*—The defensive organization of an area is generally based upon a plan which coordinates all defensive arrangements. Information derived from a study of an aerial mosaic of the area, supplemented by information from other sources, frequently makes it possible

to determine, at least partially, the enemy's plan of defense. The study is facilitated by low oblique photographs.

(4) *Study of details.*—Details are studied on vertical photographs and stereo-pairs, supplemented at times by oblique photographs. The actual examination of stereo-pairs should be made in a good light with the aid of a magnifying glass and a stereoscope. The examiner should study each object in detail, covering the whole photograph in a methodical manner. He should suspect all regular forms, as there are few geometrical figures or straight lines in nature. *He must try to establish facts and in doing so should confine himself to military essentials.* The examiner should be thoroughly familiar with the terrain and all available enemy information in the area under consideration. He should compare the photographs with a map of the area, for this will enable him to avoid serious errors.

(5) *Annotation.*—Aerial photographs should not be marked or annotated until they have been thoroughly examined and then only in such a way as not to obliterate detail. Objects should be indicated on the photograph without obliterating essential detail. A distinction should be made between objects actually identified and those located from prisoners' statements or otherwise. If markings are made on the photograph, the ordinary conventional signs should be used. The names of topographic features, such as villages, trenches, roads, and map coordinates, should rarely be shown on photographs. (Fig. 15.)

(6) *Report.*—The final report is made by noting the results of the study on the photograph by means of a sketch, or by sketching the items on tracing paper pasted to the aerial photograph. A complete report must answer the questions: What, where, and when?

SECTION V

IDENTIFICATION OF ENEMY ACTIVITIES FROM AERIAL PHOTOGRAPHS

■ 35. GENERAL.—*a.* Military operations have a profound effect upon the terrain of the area involved, depending, of course, upon their intensity and the size of the forces engaged.

These activities make marks upon the terrain which are reproduced on aerial photographs and thus become a source of valuable military information.

b. The methods used in studying enemy activities are similar to those employed in ordinary aerial photograph reading except that greater attention is paid to minute details, for the smallest detail on an aerial photograph taken during active operations may be of great importance.

■ 36. CAMOUFLAGE.—The enemy will try to make objects deceptive or invisible to the eye and camera, but generally it is not possible to accomplish both at the same time. Camouflage invisible to the eye is occasionally visible to the camera, and vice versa. Color effects are generally used to camouflage from the eye. To camouflage from the camera, nets may be used to break up shadows, and tracks and blast marks may be covered up or concealed by confining them to locations near roads or hedges or inside buildings where they cannot be seen. Spoil may be covered up, scattered, or disguised. Breaches of camouflage discipline tend to defeat the best efforts at concealment by means of artificial cover. Ordinary camouflage is more visible after a snowfall. With a white background a different type of camouflage is required. For more complete information see FM 5–20. (Figs. 14 and 16.)

■ 37. ROADS, TRACKS, AND PATHS.—*a.* Roads, tracks, and paths are among the most revealing features of enemy activities found on aerial photographs. Dead-end trails and roads are of especial significance. An abrupt ending usually means that some activity such as a dump, an observation post, or a machine-gun emplacement is near the end of the trail or path. Development and deployment for action will show up clearly in maneuver warfare in all but close terrain. In defensive operations, tracks and paths will disclose the enemy's activities in great detail, frequently furnishing the clue to the location of many defensive installations. The main communication trenches will generally be indicated by paths parallel to them, which are made by carrying parties at night. Trenches in bad condition are also frequently indicated by parallel paths. On quiet parts of the front the appearance of new tracks or the gradual disappearance of

tracks will frequently give positive or negative information of the enemy's activites in a locality. During artillery preparation, new tracks near dugouts under bombardment are sure signs that the dugouts have not been destroyed or that they have been reoccupied. Tanks and other mechanized weapons moving into assembly positions make unmistakable tracks. (Figs. 17, 20, 22, 23, and 25.)

b. The presence of troops may be disclosed by the cutting of new paths, trails, or roads, by fire or smoke, and by a general lightening of the appearance of the area. The presence of vehicles may be disclosed by the disruption of the road shoulder at the point at which they left the road, and the crushing of the vegetation incident to their movement into concealed positions which show very plainly in night as well as in day photographs. Troops deploying for action leave unmistakable trails and tracks as they fan out from march columns. Marching troops are easily detected on main roads but are more difficult to detect if they use the shoulders. Dust arising from dirt roads will reveal troop movements even in heavily wooded areas. (Fig. 25.)

■ 38. TYPES OF WORKS.—*a.* The works, installations, and tactical dispositions employed by various armies in different situations will vary in details of shape, appearance, and relative locations. The types of works used by the enemy must be carefully studied, especially those on ground recently captured. G–2's of higher echelons should keep an album of interpreted aerial photographs for use in studying new photographs.

b. The illustrations in this manual are largely from the World War and exemplify what was accomplished at that time with available means under the conditions of position warfare.

■ 39. TRENCHES.—*a.* Trenches are readily distinguished by their traversed or zigzag trace revealed by the shadow of trench walls or by spoil. Shadows indicate the depth; shallow, dummy, or incomplete trenches cast little shadow. The conspicuousness of spoil depends upon the type of soil and the newness of the work, chalky or light-colored spoil being very difficult to conceal. Recent work is generally indicated

by a different appearance than surrounding soil. Any unusual amount of spoil should be scrutinized carefully, as it may indicate subterranean work. When a trench system has been heavily shelled, the previous contrasts rapidly disappear, and the study of photographs becomes increasingly difficult. Trenches in use are generally more distinct in outline than those not being used because they are kept in condition, but aerial photographs can seldom be relied upon to indicate whether or not they are occupied. (Figs. 26 to 29, incl.)

b. Fire trenches usually have straight firing bays separated by variously shaped traverses, while communicating trenches generally zigzag.

c. Trenches can be analyzed in snow pictures, due to the contrast of the shadows against the white background. If the trenches are occupied, the repeated trackings of the men may show, and dummy trenches are easily identified from real trenches. (Fig. 30.)

■ 40. BREASTWORKS.—Breastworks are usually constructed in city streets or in marshy or swampy terrain where trenches would quickly fill with water. They may be identified by their regular trace and characteristic shadows.

■ 41. ORGANIZED SHELL HOLES.—*a.* Shell holes are frequently organized for defense. They may be prepared and organized prior to an offensive or consolidated quickly during a battle.

b. When systematically organized, shell holes will generally be in pairs, constructed in well-drained ground, and connected by underground passages leading to a common dugout. The sides of shell holes may be revetted and the tops roofed and camouflaged. Such shell holes are not difficult to find on large scale photographs, and may be distinguished from ordinary shell holes by their more definite outline, the spoil dumped in the vicinity, tracks, and the entrance to the dugout.

c. Makeshift shell hole systems are more difficult to detect, but may be distinguished from ordinary shell holes by their darker appearance if they have been deepened. Occupied shell holes are generally found on patches of dry ground, which should be scrutinized carefully. Tracks are by far the surest indication of occupancy.

■ 42. WIRE.—*a.* Broad wire entanglements show on photographs as a band or line varying from light to gray to almost black, depending upon the age of the entanglement and its contrast with the color and texture of the adjacent ground and vegetation. New wire is more difficult to detect than old wire, as grass and other vegetation growing in old areas give them a distinctive, darker appearance. The study of photographs to locate wire should include not only the trench system but also fortified shell holes, battery positions, villages, hedges, and ditches. (Figs. 27 to 29, incl.)

b. As ground is cut up by bombardment, wire becomes increasingly difficult to identify. It should not be concluded that no wire exists because there are no signs of it on a vertical photograph. An oblique photograph may reveal wire not visible on a vertical photograph. (Fig. 29.)

c. The presence of wire may be betrayed by the tracks of working parties on either side of it, or by paths which suddenly change direction in passing through the entanglement.

d. As wire appears as a black band in snow, it is then visible when not otherwise apparent. It is rarely possible to discover wire entanglements in woods. (Fig. 30.)

■ 43. DUGOUTS.—The first indication of a dugout is usually the spoil thrown up during its construction. Earlier photographs of a defensive system should be compared with more recent ones in order to discover fresh spoil, which should be carefully noted, as the actual location of the dugout may be concealed by scattering the spoil. Frequently the first indication of a new defensive position is the appearance of a line of dugouts. The position of these dugouts should be carefully plotted, as they may be so camouflaged as to be no longer visible in photographs taken after the trench has been completed. The size of dugouts may sometimes be estimated by the amount of spoil. Occupied dugouts are sometimes revealed by the melting of snow from the heat of the fires inside.

■ 44. MACHINE GUNS.—*a. General.*—Machine guns are so difficult to locate on photographs that as a rule they can be detected only by knowing where to look for them. Aerial

photographs should be used mainly to corroborate reports from front-line troops and information from other sources.

b. Mobile situations.—Because machine-gun emplacements are simple in type and utilize all available natural cover, it is extremely difficult to identify them in mobile situations. In the attack, machine guns are generally placed on high ground where they can furnish support by overhead fire or grouped in batteries on a reverse slope about 1,500 yards in rear of the front line. In the defense, they will be found in positions with a good field of fire and covering approaches, such as ravines, bridges, etc., or flanking the edges of woods or elevations. High ground is usually defended by guns posted on the flanks of the elevation instead of on the crest. Ground which offers the best positions for flanking strong points should be carefully studied, for machine guns are often posted about 1,000 yards from the defenses which they protect by flanking fire. Sometimes they are indicated by the absence of wire and grass in the field of fire. When a machine gun location is suspected—

(1) Look carefully for tracks between the position and the roads or paths.

(2) As a machine gun is rarely employed alone, look for indications of adjacent machine-gun positions.

(3) Draw an arc with the position as the center to determine the probable field of fire.

(4) Note if the field of fire of the machine gun covers the terrain effectively; if it does not, look for a probable new position.

c. Position warfare.—In position warfare, machine guns are generally located close to the trenches, so they can deliver cross fire along the front of wire belts or cover the flanks and rear of fortified areas. Open emplacements in a trench can usually be recognized by the firing platform cut into the parapet, and covered emplacements by the V-shaped embrasure. They may be found—

(1) Where an angle occurs in the trace.

(2) Within easy reach of a communication trench.

(3) At the end of a path in front of a trench.

(4) Outside the trench system where a small forward sap leads to an emplacement protected by a semicircle of wire or in excavations behind the front line.

(5) In wire or on higher ground behind first-line trenches.

■ 45. 37-MM GUNS OR SIMILAR WEAPONS.—In searching for the positions of 37-mm guns or similar weapons, the examiner should understand the characteristics of the weapon and then proceed in the same manner as outlined for machine guns.

■ 46. LISTENING, OBSERVATION, AND COMMAND POSTS.—*a. Listening posts.*—Listening posts appear on aerial photographs as small excavations either under the first belt of wire or just behind it. Their positions are generally disclosed by tracks and saps leading to them. Detached listening posts are frequently constructed in no man's land. They may be camouflaged, encircled by wire, and provided with a covered approach. If the contour of the ground permits, listening posts may also be used as machine-gun positions. (Fig. 31.)

b. Observation posts.—(1) Observation posts are usually carefully camouflaged. They should be looked for on commanding ground in the vicinity of deep shelter or in or near such objects as a group of trees, hedges, or structures. They are often near the end of a dead-end path and should be suspected whenever a trail or path ends.

(2) An observation post is indicated by tracks or paths, telephone lines, and in organized ground by small trenches leading off from the main system.

c. Command posts.—Command posts will generally be located in buildings, in protected positions on reverse slopes, and in sheltered woods. They will usually be revealed by the trails, paths, or telephone lines which converge upon them. Panels for communication with friendly aviation will frequently reveal the location of command posts. (Fig. 32.)

■ 47. ANTITANK OBSTACLES AND ROAD BLOCKS.—*a.* In an organized position, antitank obstacles may consist of ditches, wire rolls, concrete pillars connected by steel cables, concrete blocks, railroad rails embedded in the ground or in concrete, wooden piling, or rubble masonry. An antitank mine field, consisting of a broad band of contact mines either buried or laid checkerwise on the surface of terrain suitable for the movement of

tanks or mechanized vehicles, constitutes an effective obstacle. Such mine fields may be detected by spoil, paths, or vehicle tracks parallel to the front.

b. In mobile situations, tank traps, and road blocks will usually be found along roads, generally at defiles or at crossroads. In order to hold the vehicle under fire a barrier is built consisting of a ditch, a covered or uncovered crater with vertical sides, or a heavy obstacle. Antitank mines will normally be found in or flanking the exposed sides of the barrier. Crossroads, defiles, causeways, bridges, deep road cuts, and side hill road cuts, as well as adjacent fields, should be examined for these articles. (Fig. 33.)

■ 48. MINE SHAFTS.—Mine shafts are difficult to distinguish on an aerial photograph, because great care is usually taken to conceal the spoil, which is often carried some distance by light railways. Proper interpretation can best be made by experts who are familiar with the mining technique. The results of mining operations can be checked by means of aerial photographs. (Fig. 34.)

■ 49. CONCRETE FORTIFICATIONS.—As concrete fortifications are located with a view of avoiding observation, or are provided with artificial concealment, they are often difficult to identify until the whole area has been cleared by heavy shell fire. After intense bombardment they appear on a photograph as geometrical figures standing above the level of the ground, having in most cases survived the prevailing destruction due to their superior powers of resistance. Concrete fortifications under construction are often disclosed by the whiteness of the concrete and the appearance of the ground where the concrete was mixed, by tracks of vehicles, or by narrow gage lines which transported the material (Fig. 35.)

■ 50. LOCATION OF BATTERIES.—*a. Natural cover.*—The enemy will take every precaution to conceal battery emplacements, utilizing villages, hedges, ditches, orchards, woods, thickets, ravines, and sunken roads for the purpose. Positions in the open may be dug in. They are usually provided with camouflage. Emplacements in ravines and sunken roads are frequently dug in and so well hidden that they are difficult to

locate, as the roads, being used for other purposes, will not show any signs of extra activity near the batteries. The primary considerations in the location of batteries are to provide concealment and cover for men and guns. Unless the batteries are in or near a village where the personnel can be housed in adjacent buildings or cellars, each battery will usually have dugouts and ammunition dumps close to the gun positions. During an advance or withdrawal, however, battery positions will generally afford no protection either for the personnel or for the guns, although locations near a road or some natural feature of the ground may give some protection. For each battery position a number of dummy or alternate emplacements are usually constructed. (Fig. 36.)

b. Artificial cover.—Natural cover will be supplemented by camouflage designed to furnish the maximum protection from both ground and aerial observation. Positions in the open will be camouflaged if time permits. Alternate and dummy positions will be constructed for purposes of deception. (Fig. 37.) Antiaircraft artillery is difficult to camouflage from aerial view. Patches in woods which appear lighter or darker than their surroundings may indicate the location of artillery positions. Such areas should be carefully studied for additional indications, such as trails and paths.

c. Evidence of battery positions.—(1) Batteries are usually spotted on photographs by tracks leading to them, by increased traffic on nearby roads and trails, by faulty camouflage, by piles of ammunition, and by latrines, dugouts, bivouacs, and kitchens. Sometimes horse lines or vehicles can be seen. Guns are only a part of the evidence of the existence of a battery. Batteries concealed by overhead cover may be detected by trails or narrow gage railroads leading to them, or by the tracks of the gun crew. Even if the battery emplacement is hidden, it is difficult to conceal the activity in its vicinity. Blast marks made by the guns tend to defeat camouflage, showing up as white scores where the surface has been blown away by the discharge and as black smudges on snow. During dry weather, blast marks may be visible for some time after the position has been vacated, and so are

no proof that an emplacement is occupied, but rather that a position has been active—a distinction which is liable to be overlooked. A photograph revealing blast marks when snow is on the ground usually indicates an active emplacement but may be only a well-prepared dummy. (Figs. 38 to 40, incl.)

(2) Guns hidden by camouflage or protected by overhead cover and firing through embrasures may be detected by the shadow of the camouflage or by blast marks. Dummy batteries can usually be distinguished by the exaggerated blast marks and tracks of too regular a pattern. The stereoscope is essential in studying such positions.

(3) Batteries in the woods are revealed by slashings, by white marks on the ground due to construction of emplacements or to traffic around guns or shelters, and by trails, narrow gage railroads, and wire lines leading to battery positions.

(4) Antiaircraft guns are generally grouped by batteries of three or four guns in regular pattern. (Fig. 14.)

d. Study of our battery positions.—Examiners should study photographs of our own battery positions taken during both peace and war, so that they may be familiar with the appearance of batteries in different situations.

■ 51. STUDY OF EFFECT OF OUR OWN ARTILLERY FIRE.—Aerial photographs may be used in adjusting artillery fire and in studying its effects. Photographs taken for these purposes should be developed by quick work methods and made available at the earliest practicable moment. (Figs. 41 and 42.)

■ 52. BURIED CABLES AND OVERHEAD TELEGRAPH AND TELEPHONE LINES.—*a. Buried cables.*—Open cable trenches can usually be distinguished on photographs by their fairly straight course and construction, and by their irregular outline when filled in. They should be marked on a map when first discovered, as they are difficult to find after being established for some time. Cable trenches aid in discovering command posts, headquarters, telephone exchanges, camouflaged batteries, observation posts, and other important centers.

b. Overhead lines.—Overhead lines appear as regularly spaced white dots, these being the displaced earth where the

poles have been erected. These dots are connected by a thin white track made by the men walking from pole to pole when putting up the wire. Overhead lines in a cultivated field will frequently stand out clearly as small dark spots because the soil around the posts has not been disturbed. Overhead lines can be determined on clear photographs if the shadows thrown by the poles can be seen. In melting snow the overhead lines may appear as evenly spaced black dots.

c. Ground lines.—Advancing troops lay ground lines as they progress. These always lead from one important communications center to another. The repair of these lines caused by frequent breaks goes on constantly and results in the making of telltale tracks or paths.

■ 53. REAR INSTALLATIONS.—*a. General.*—Military operations require large concentrations of troops, ammunition, and supplies; the construction of airdromes and hospitals; the preparation of railheads, detraining points, and other facilities. All of these are generally revealed by aerial photographs. A study of the area in rear of the enemy's front lines is, therefore, highly important.

b. Reserves.—(1) Local reserves are held in concealed positions close to the front. Evidences of their presence which may be found on aerial photographs are huts or other temporary shelters, numerous paths and tracks, picket lines and motor or gun parks, watering places, and kitchens.

(2) General reserves are usually held well back from the front or in training camps still farther to the rear. Large billets, extensive training facilities, and considerable activity are evidences of their presence. (Fig. 43.)

c. Supply and ammunition dumps.—Depots and dumps are points of supply for front-line units. Their location depends upon the accessibility of railroads and highways. Points where various means of communication join should be carefully examined. If open storage is used, dumps can usually be identified by the regular segregation of the various types of property. Forward supply points are usually more carefully concealed or camouflaged than those in the rear. Because of the increased range and importance of aviation, it will be necessary to camouflage all supply installations. They may be detected on aerial photographs by signs of activity

in their vicinity. Supply points become smaller toward the front. Signs of unusual traffic at certain points will indicate the location of forward dumps even when concealed. Abandoned dumps will soon show lack of use. (Figs. 44 and 45.)

d. Detraining points.—Military activity at detraining points is difficult to conceal during daylight hours and may even be detected at night. Aerial photographs will frequently reveal not only the detrainment but also the composition of the forces detrained. They are also of value as a check on the results of aerial bombardment. (Figs. 46 and 47.)

e. Hospitals.—Hospitals are generally located on railroads or other lines of communication at points where there is no ammunition. They are usually identified by the Red Cross sign but in the forward areas may be concealed or camouflaged. (Fig. 44.)

f. Landing fields and airdromes.—(1) Enemy aviation will probably be widely scattered throughout his rear. On the ground the airplanes will be concealed by camouflage or natural cover and may be provided with overhead protection.

(2) Enemy airdromes and landing fields may be indicated by hangars; by landing devices, such as tees, smoke contrivances, lights, and wind vanes; by especially prepared landing areas and distinctive accessory buildings which are difficult to camouflage or conceal. (Figs. 48 to 50, incl.)

(3) Permanent airdromes may be built underground, and the landing fields may be concealed by natural planting supplemented by camouflage.

g. Balloon beds.—Captive balloons behind the enemy's front lines are extremely difficult to conceal except when deflated.

SECTION VI

INTERPRETATION

■ 54. GENERAL.—Information derived from aerial photographs and all other evaluated information will be given consideration by G–2 in the preparation of his conclusions relative to the enemy's capabilities. The procedure followed is outlined in FM 30–5.

■ 55. EVIDENCE OF ENEMY'S INTENTIONS AS REVEALED BY AERIAL PHOTOGRAPHS.—*a. General.*—The general attitude of the

enemy, whether offensive or defensive, can usually be ascertained by a study of aerial photographs in connection with information from other sources. The kind and degree of completion of enemy works, the number and location of dumps, and the amount and location of reserves, if shown on aerial photographs, will furnish evidence of the offensive or defensive plans of the enemy. Aerial photographs will be of greatest utility in these studies during periods of stabilization. In maneuver warfare it will be difficult to distinguish between offensive and defensive preparations.

b. Offensive preparations.—(1) *General.*—Offensive preparations by the enemy usually leave unmistakable marks upon the terrain, which, if properly interpreted in connection with information from other sources, furnish the commander advance notice of the enemy's intentions. Among the indications of an impending attack may be an increase in artillery and antiaircraft artillery battery positions, and a general forward displacement of mechanized units, artillery, reserves, airdromes, and supplies, and dumps of bridge material near a river. New or improved roads, deviations from existing roads, new or extended railroad lines, and a general increase in both road and railroad traffic may also be observed.

(2) *Position warfare.*—New and improved communication trenches, new and unusual trails, saps pushed in advance of the front line and linked up to form jumping-off trenches, new and improved dugouts and assembly trenches, new trench mortar emplacements, such as shell holes connected by trenches, new practice trenches, sometimes modeled after our own, and new gas projection emplacements may furnish indications of an attack.

c. Defensive preparations.—Defensive preparations are indicated by tank barriers or obstructions, by traverses and dugouts marking an intended new line, by strengthening and deepening of trenches, by additions to existing wire, by new switch trenches, and by an increase in battery positions especially toward the rear. After a defensive position has been well-defined, it will be studied for the distribution of defending troops, for details of organization, and for the probable routes by which reserves can be engaged. The study should include both front and rear, and should anticipate the en-

trance into line of division reserves and even of reinforcing divisions for sustained counterattacks. Therefore, all shelters, camps, roads, observation stations, and battery emplacements in the rear zone will be given the closest attention.

■ 56. INTERPRETATION DURING OUR OWN OFFENSIVE OPERATIONS.—*a.* In position warfare, interpretation during our own offensive operations falls into three distinct phases:

(1) Preparatory.

(2) Destruction of enemy's works.

(3) During and after an attack.

b. Preparatory.—The purpose of studying aerial photographs in conjunction with maps in preparation for offensive operations is to give the various elements of command detailed information concerning critical terrain features and bottlenecks on the enemy's lines of communications and the disposition of his troops on the ground and their defensive organization. Evaluated photographs are used by all elements as supplements to the designated maps. They are of particular importance to the Air Corps, parachute troops, air infantry, and mechanized troops and in operations incident to landing on a hostile shore or a river crossing.

c. Destruction of enemy's works.—(1) The aerial photograph is of real value in studying the destruction of enemy works. It shows the effect of our artillery and aerial bombardment and can be studied and compared with older photographs of the same area, thus facilitating the evaluation of operations in preparation for an attack. Three degrees of destruction should be considered: Destroyed, seriously affected, and only slightly affected. A field work should be considered destroyed when its offensive value has been reduced to a condition equivalent to that of connecting shell holes. It has been seriously affected when it can only partially fulfill the function for which it was intended. It is only slightly affected when it is still able to fulfill its defensive role.

(2) The degree of destruction of enemy works may be shown by marking each hit on the photograph. An overlay is then prepared showing in different colors the areas corresponding to the three classes of destruction indicated above.

These overlays should also show any works reconstructed or maintained by the enemy in spite of the bombardment. Such overlays should be prepared at the close of the day or at designated hours.

d. During and after attack.—(1) *During battle.*—Aerial photographs taken during battle may reveal among other things the—

(*a*) Position of attacker.
(*b*) Location of hitherto unknown defenses.
(*c*) Preparations for withdrawal or counterattack.
(*d*) Movement of reserves and their destination.
(*e*) New targets for our artillery.

(2) *After battle.*—After battle, aerial photographs may give the most accurate information concerning the situation, revealing among other things the organization and the connection of shell holes to form trenches, the construction of temporary dugouts, the location of obstacles, and the movement of reserves for counterattack. They are of greatest value in determining whether or not trenches or their remains are occupied by the enemy. The only sure indication of activity is the presence of trails for supply and relief. Aerial photographs taken during and after battle should be carefully studied for indications of new command posts, location of reserves, supply arrangements, communications, and new locations of machine guns and artillery.

FIGURE 1.—One photograph of pinpoint of communication center at Thiaucourt 21 Aug 18. Scale 1:7,800.

FIGURE 2.—High oblique photograph.

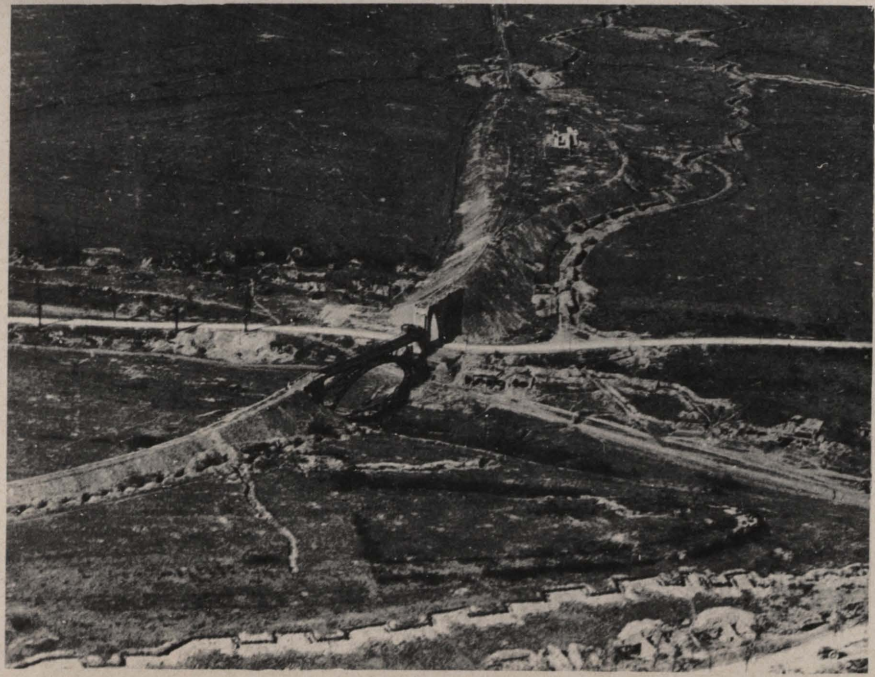


FIGURE 3.—Low oblique photograph showing demolished railway bridge west of Flirey and trenches.

FIGURE 4.—Night photograph taken at 5,000 feet showing faulty disposition of airplanes.

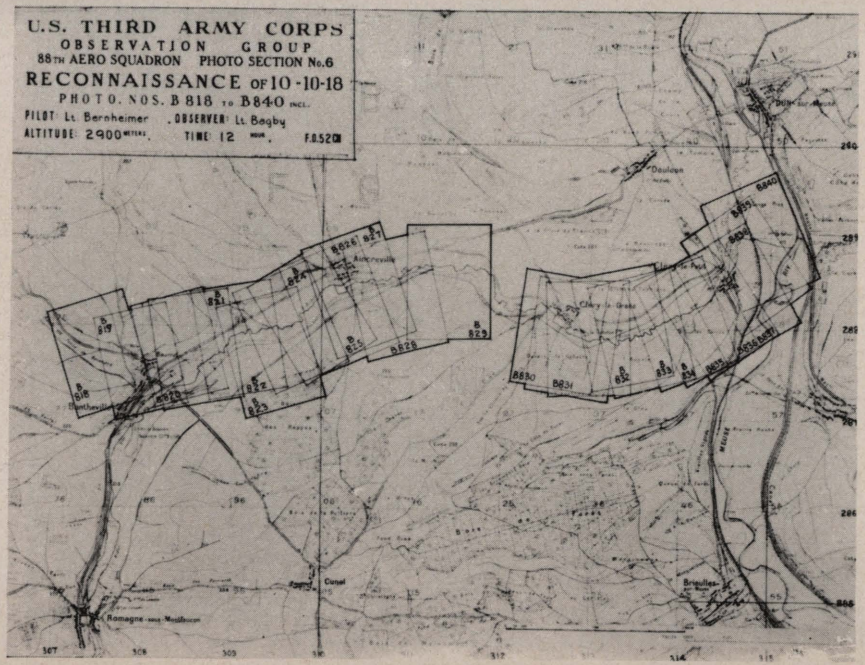


FIGURE 5.—Graphic index map.

FIGURE 6.—Method of titling a vertical photograph.

FIGURE 7.—Method of titling an oblique photograph.

FIGURE 8.—Photographic study of section of Siegfried line east of Sarrebruck. 30 Sept. 39; scale 1:4,000. Note recent work and older work at bottom of photograph; tank barriers; casemates connected by communication trenches.

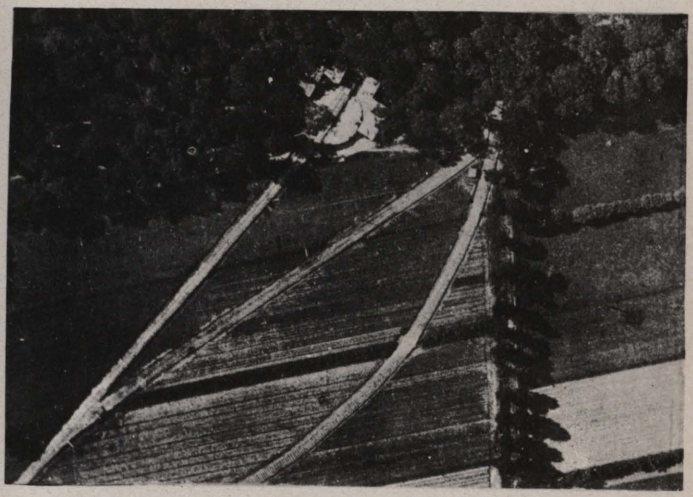


FIGURE 9.—Railway artillery position under construction.

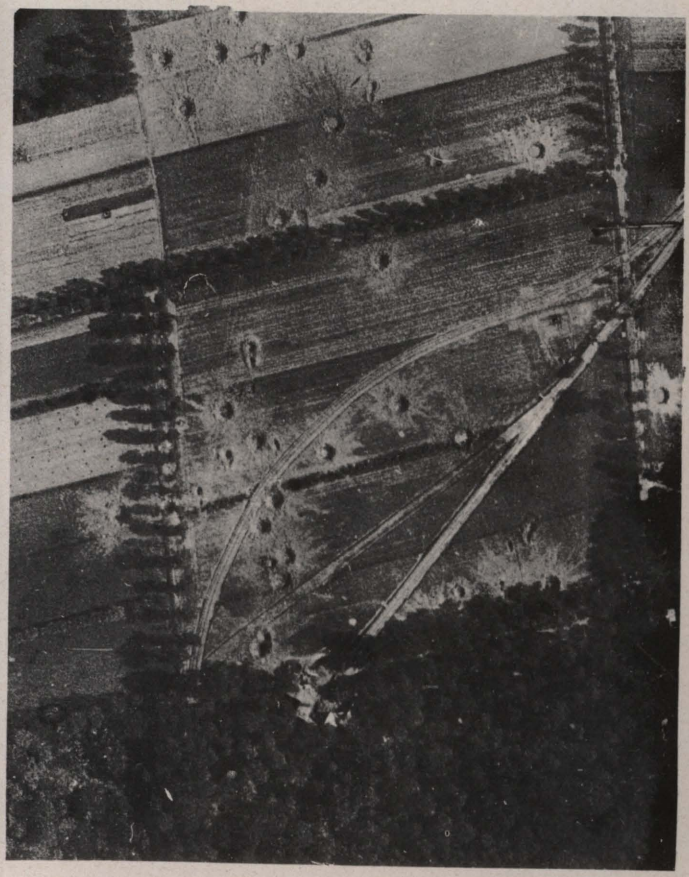


FIGURE 10.—Registration on railway artillery position shown in figure 9.

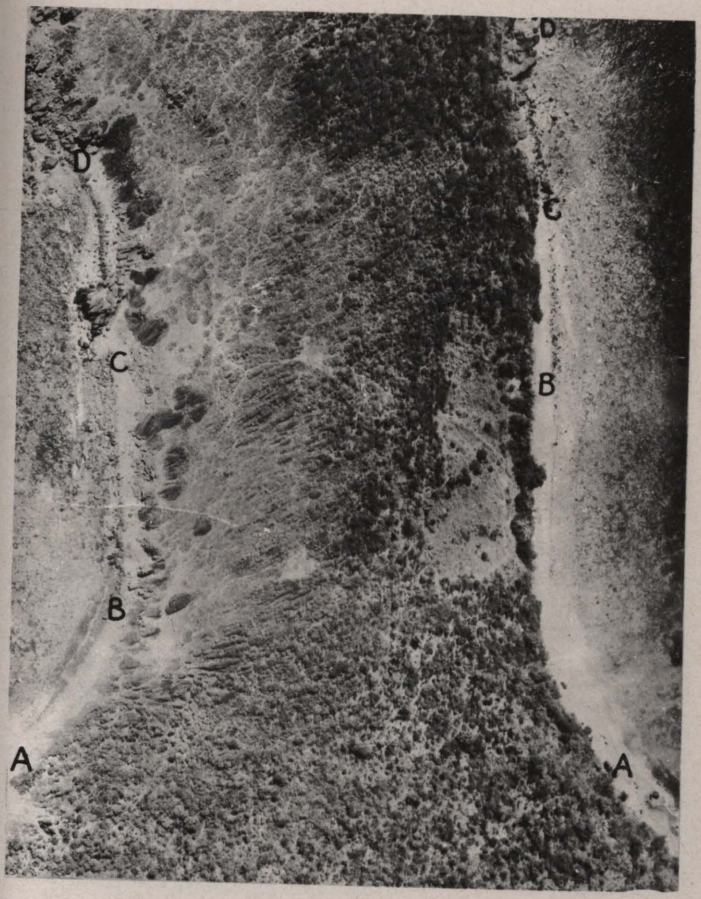


FIGURE 11.—Photographic study of possible landing beaches by 1st Marine Aircraft Group; scale 1:2,900. A–B, sandy beach with trails leading thereto and with no under-water obstructions offshore; B–C, narrow beach with steep banks inland and under-water rocks offshore, not satisfactory for landing; and C–D, rocky shore line with no beach.

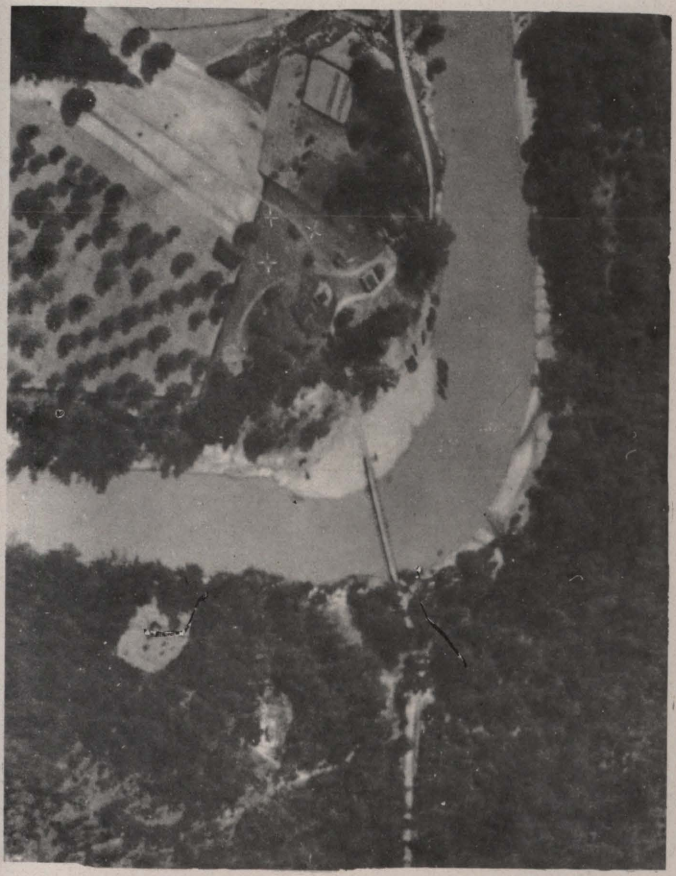


FIGURE 12.—Ponton bridge north of Burr Ferry, La., taken at 20,000 feet with 60-inch focal-length camera; antiaircraft artillery gun positions plainly visible.

FIGURE 13.—Night photograph of a bivouac area near Leesville, La., 24 May 40; scale 1:4,400. Trucks lined up draw immediate attention; available cover has not been utilized.

FIGURE 14.—Antiaircraft artillery gun positions southwest of Leesville, La., 20 May 40; scale 1:3,000. Faulty camouflage work and tracks disclose location.

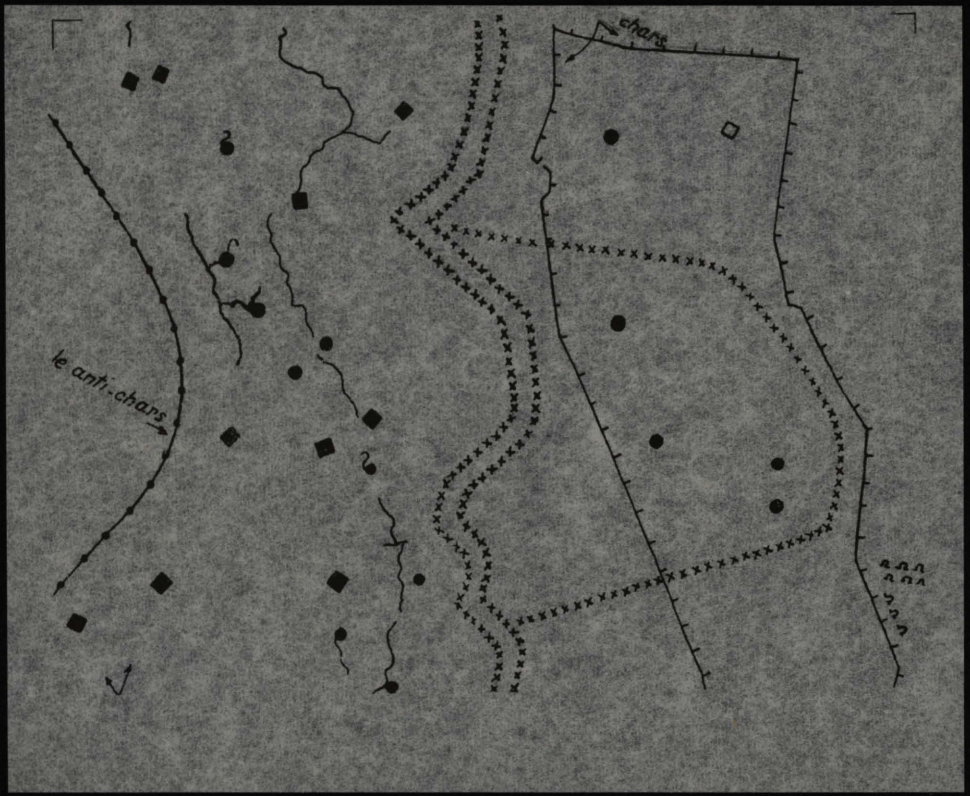

chars
le anti-chars

FIGURE 15.—Method of annotation used by the French section of the Siegfried line northeast of Wissembourg, 25 Mar 40; scale 1:7,000.

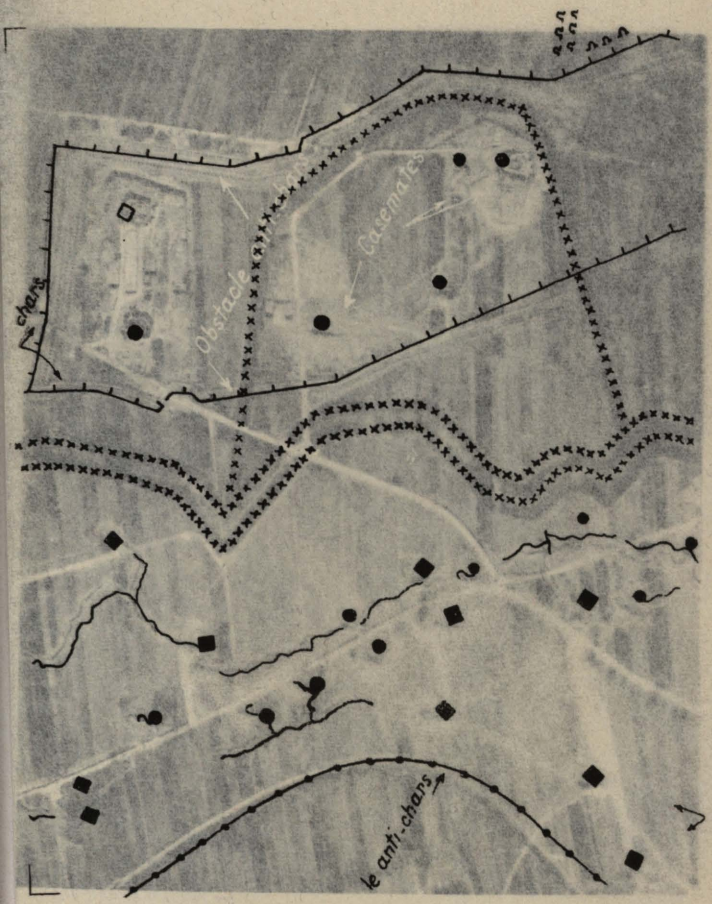


FIGURE 15.—Method of annotation used by the French section of the Siegfried line northeast of Wissembourg, 25 Mar 40; scale 1:7,000.

FIGURE 16.—Faulty camouflage and disposition of aircraft on the ground. Neither the hangars nor the camouflage painting conforms to the ground pattern. The aircraft are not scattered.

FIGURE 17.— Truck movement near Fort Benning, Ga., 22 Apr 40; scale 1:5,000.

FIGURE 18.—British photograph of demolished bridge over Albert Canal at Locht; newly constructed light ponton bridge. Road mine and troops detouring around the mine can be observed.

FIGURE 19.—Trucks near Flatwood, La. Photograph taken at 23,000 feet with 60-inch focal-length camera.

FIGURE 20.—Trucks and troops well concealed in woods, but tracks at edge of wood draw attention and a stereoscopic study reveals all details. Photograph taken south of Ellaville, Ga., 22 Apr 40; scale 1:5,200.

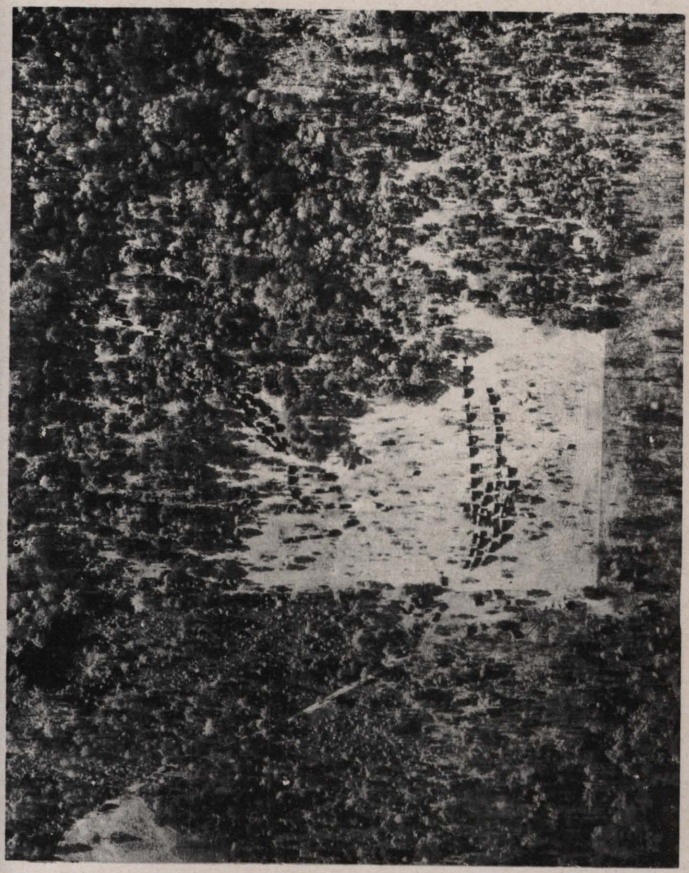


FIGURE 21.—Truck columns forming-up in the open. Photograp taken in the early morning; scale 1:5,200.

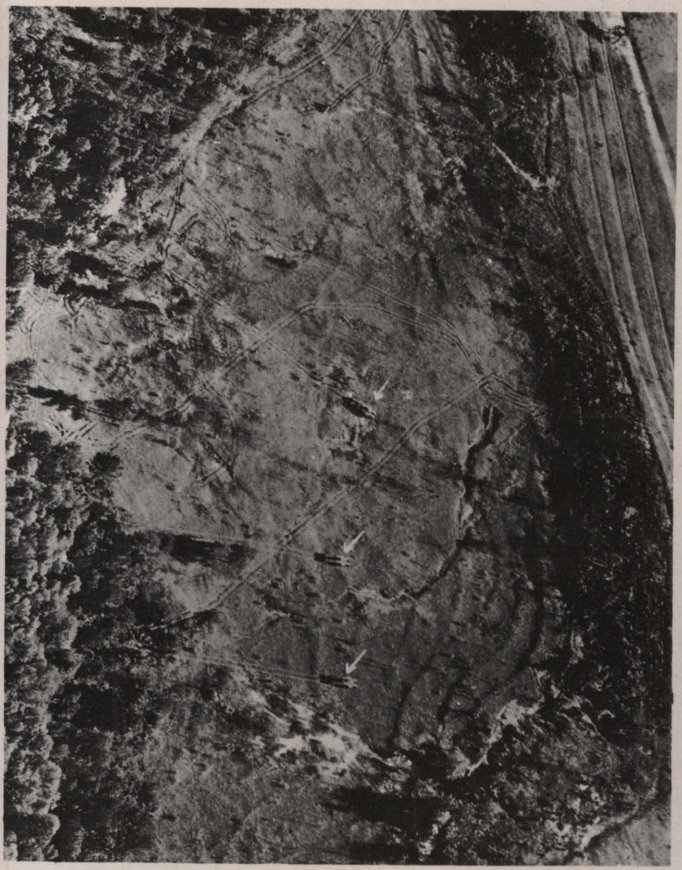


FIGURE 22.—Tank tracks in the vicinity of assembly areas and tanks moving from assembly area, Fort Benning, Ga.; scale 1:1,000.

FIGURE 23.—Numerous trails, paths, and tracks leading from main highways near Montfaucon show important troop activities. Photograph taken at 5,700 feet, 5 Mar 18.

FIGURE 24.—Briquenay village. If snow is on the ground, roads and trails in use show black.

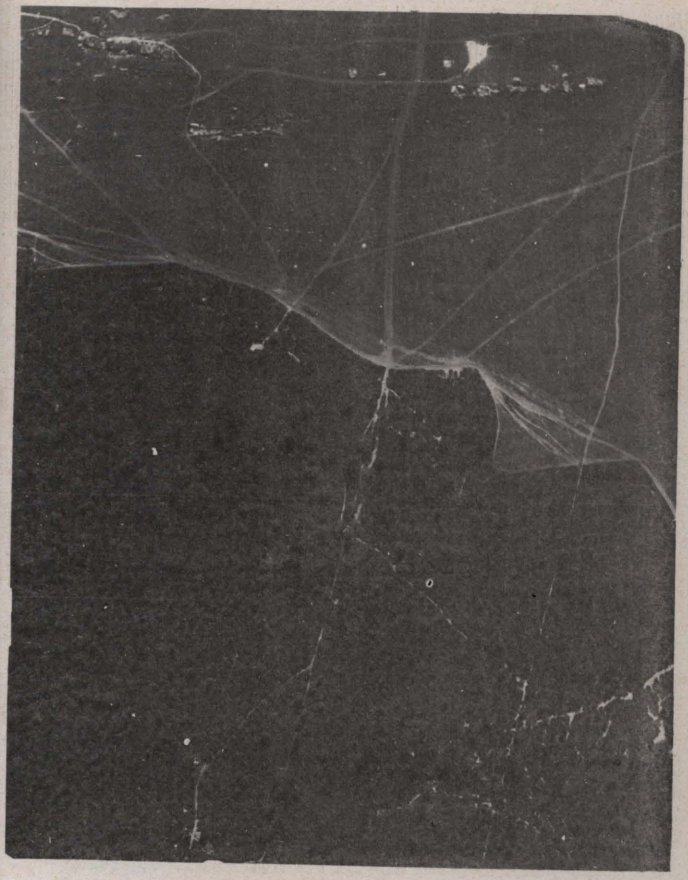


FIGURE 25.—Numerous paths and tracks leading into woods south east of Flirey, 2 Sept 18; scale 1: 6,900.

FIGURE 26.—Trenches and wire entanglement west of Rembercourt, 20 Sept 18; scale 1:6,700.

FIGURE 27.—German World War photograph. French and German positions along the Alger-Auberge road near Prunay. At points marked 1 can be seen wire entanglements and at 2 are to be seen passages through the wire.

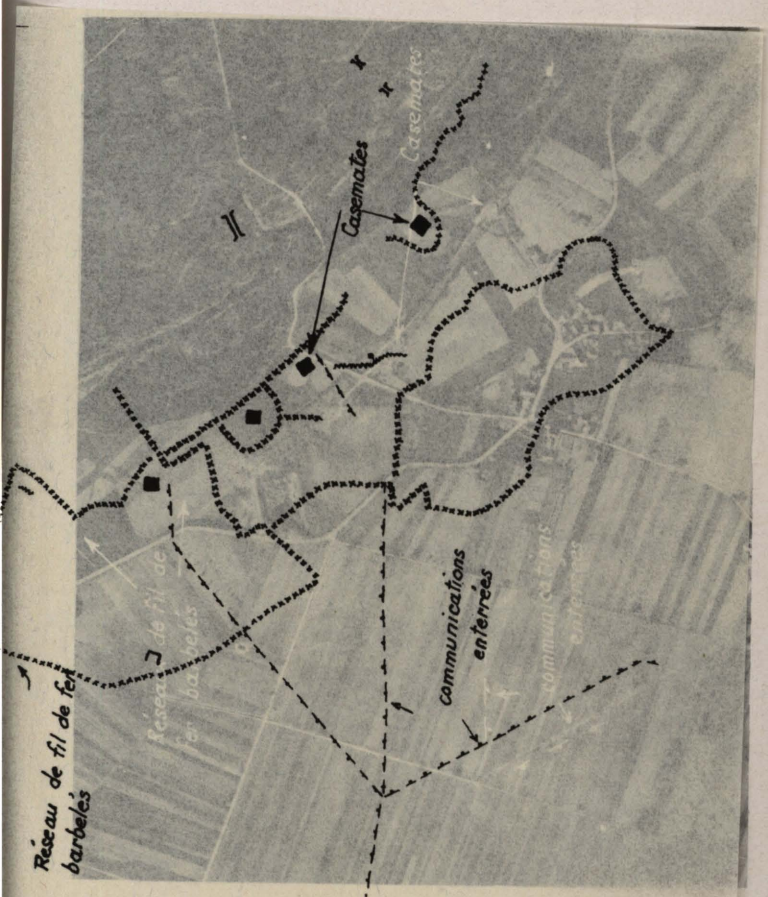


FIGURE 28.—German defenses east of the Rhine [illegible] lines of wire, casemates, and buried communications. 1:13,000.

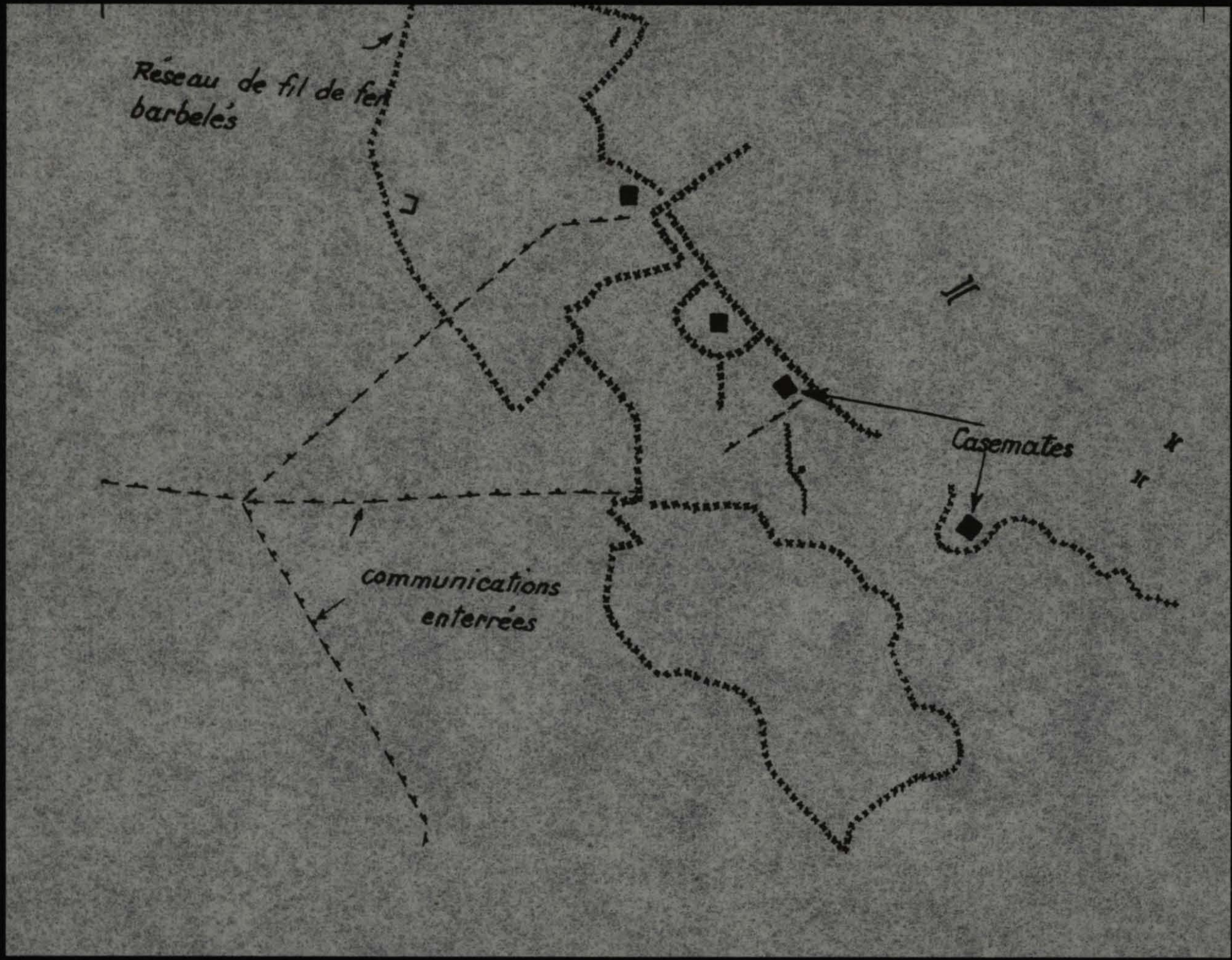

Réseau de fil de fer barbelés
Casemates
communications enterrées

FIGURE 28.—German defenses east of the Rhine, 2 Feb 40, showing lines of wire, casemates, and buried communication lines; scale 1:13,000.

FIGURE 29.—Breaches in wire made by artillery fire.

FIGURE 30.—Trenches and wire entanglement showing on photograph taken soon after snowfall.

FIGURE 31.—Listening posts as developed in the World War. At points marked 1 can be seen listening posts in round holes at the end of a communication trench; at 2 and 3 can be seen listening posts in haystacks.

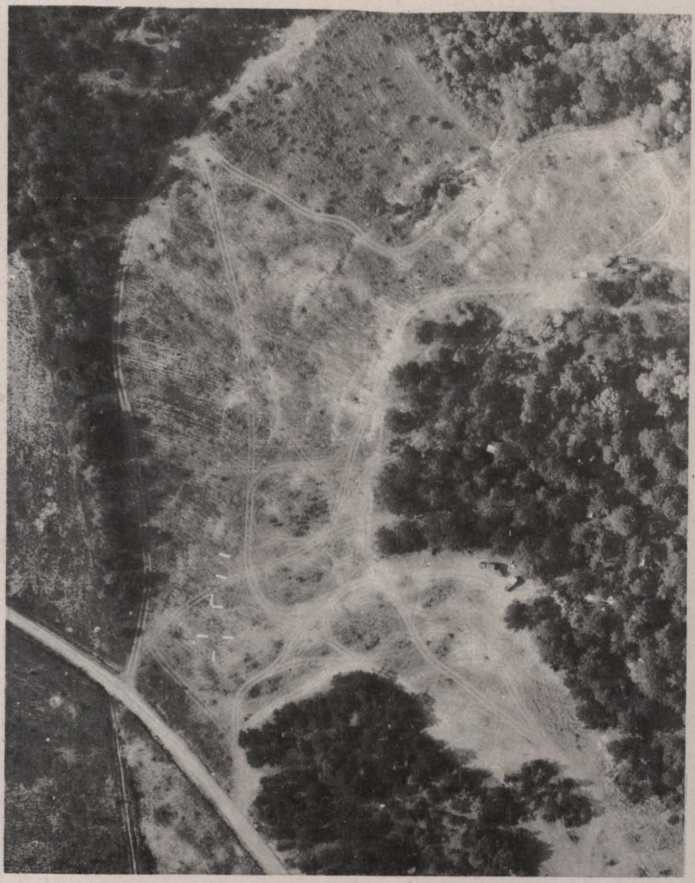


FIGURE 32.—Panels reveal the presence of a command post; tracks reveal the scope of activity in the area. Fort Benning, Ga., 25 Apr 40; scale 1: 2,500.

FIGURE 33.—Tank barriers at points marked A; tank mines along the line BB.

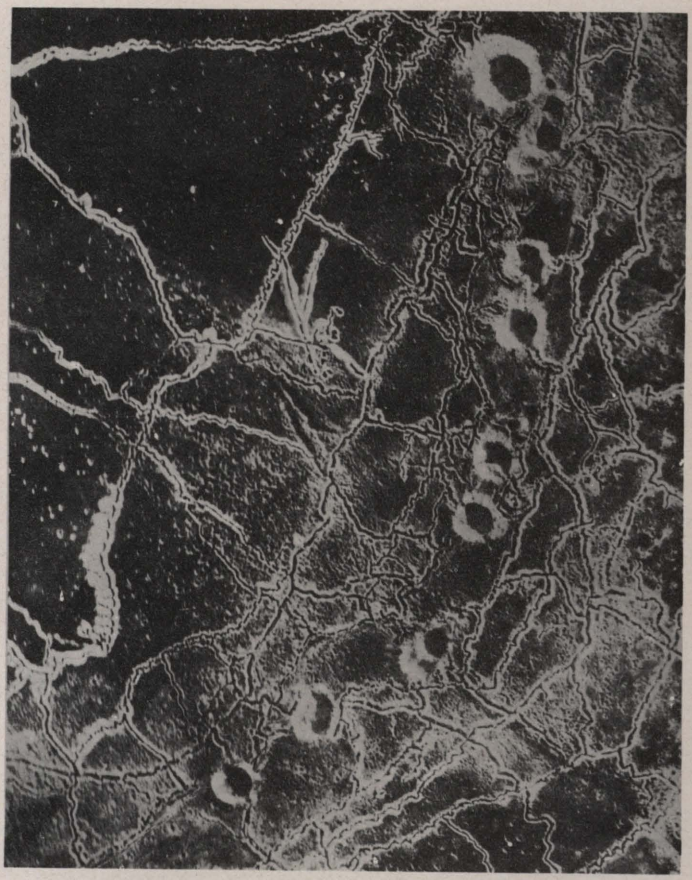


FIGURE 34.—Results of mining operations. Crater area near Corney due to both French and German mining operations.

FIGURE 35.—Bands of wire and concrete pill boxes under construction near La Chausee, 14 Sept 18; scale 1:9,000.

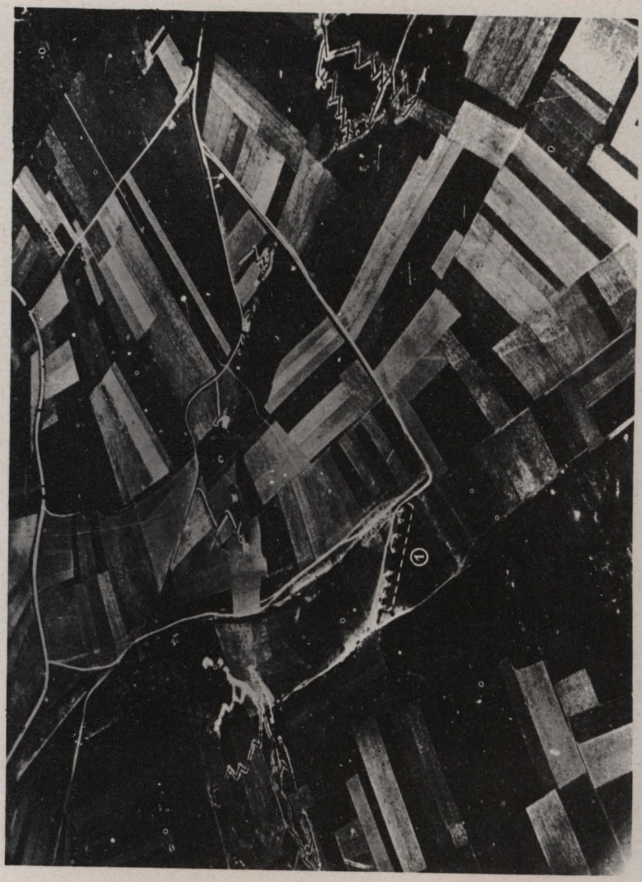


FIGURE 36.—German battery behind hedge at point marked 1. Tracks and openings in hedge are conspicuous.

FIGURE 37.—Camouflage batteries at points marked 2 and 3; trench leading to dugout at 5; narrow gage railway at 6; and patches where sod has been removed for camouflage purposes at 7.

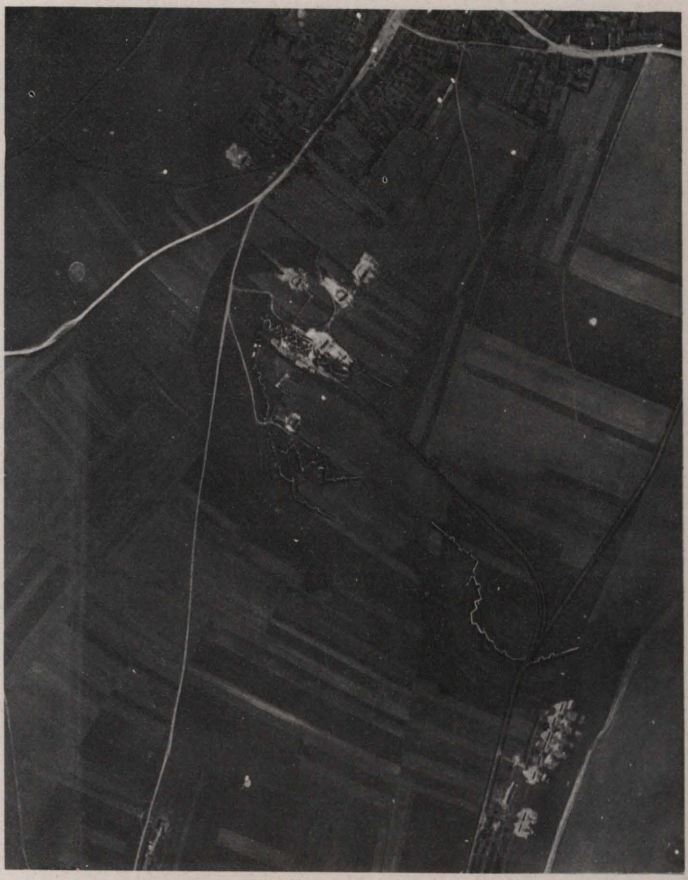


FIGURE 38.—Artillery battery position and strongpoint near Ornay, 15 Aug 18; scale 1:9,400.

FIGURE 39.—Photograph of battery positions taken soon after snowfall. At points marked 2 and 6 are blast marks revealing active guns in houses; at 3 are two inactive guns; at 4 are two active guns; and at 5 is a turn-around for vehicular traffic.

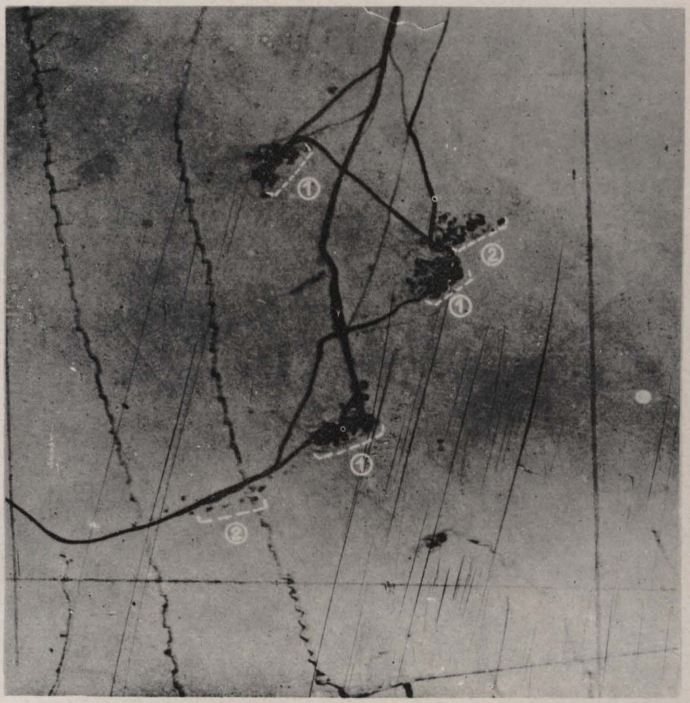


FIGURE 40.—Photograph of battery positions taken immediately after snowfall; occupied positions at points marked 1 and unoccupied positions at 2.

FIGURE 41.—Results of artillery fire upon a crossroad.

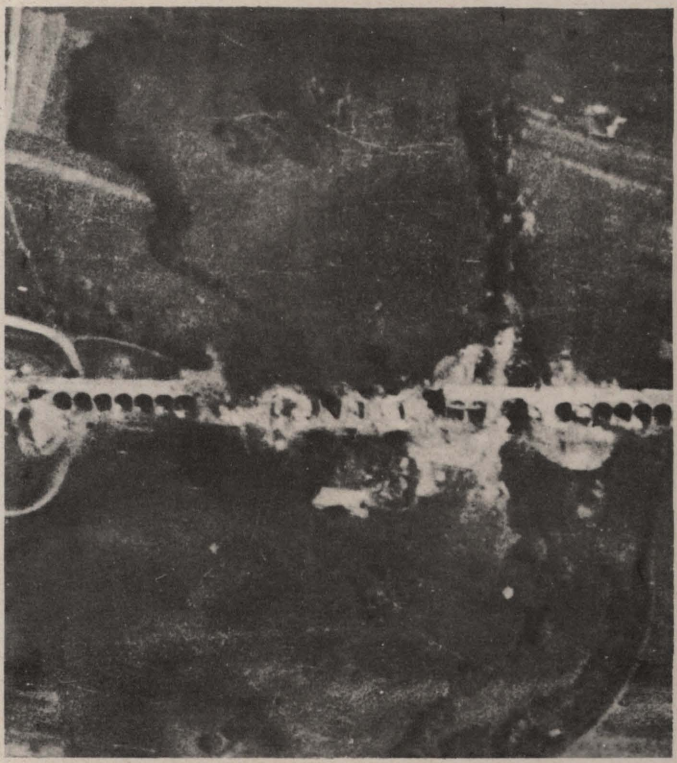


FIGURE 42.—Results of artillery bombardment of railway viaduct. The structure is demolished for a length of 300 feet.

FIGURE 43.—Billets, much used roads, and tracks

FIGURE 44.—Supply depot and hospital north of Chambley, 11 Aug 18; scale 1: 7,700.

FIGURE 45.—Ammunition dump along road near Thiacourt.
4 Sept 18; scale 1: 6,900.

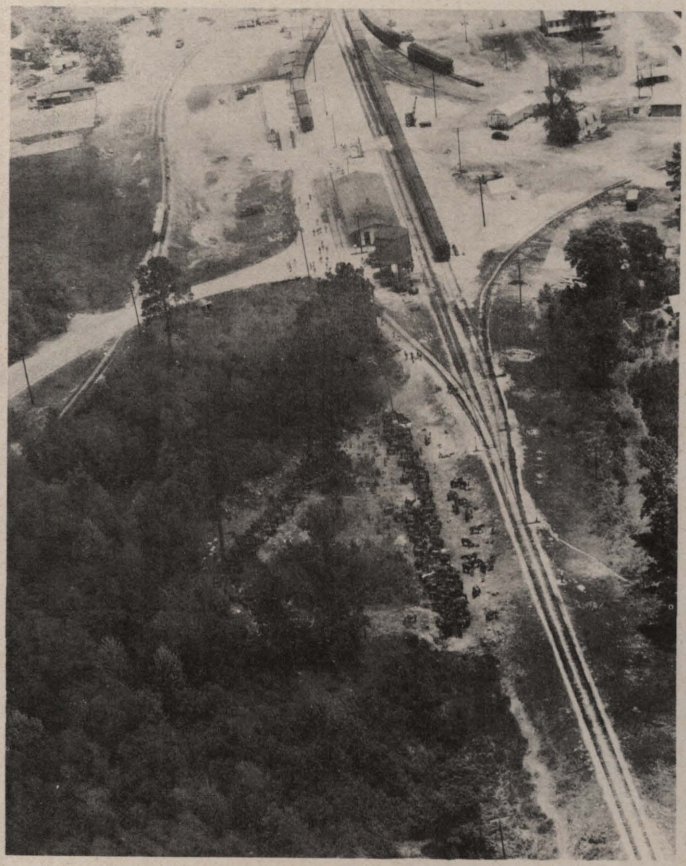


FIGURE 46.—Detraining point at Jasper, Tex., 26 Apr 40. Note faulty disposition of animals after detraining.

FIGURE 47.—British photograph showing salvo of ten bombs bursting on part of Dinant during the German advance in May 1940. Four bombs have struck the railway lines on the west bank of the Meuse, and two have struck the workshop on the opposite bank. A convoy of vehicles can be seen passing through Dinant on the Dinant-Liscogne road in the direction of a new ponton bridge.

FIGURE 48.—Ourches airdrome and paths.

FIGURE 49.—Showing a portion of the Ourches airdrome (fig. 48) as seen from an adjacent hill.

FIGURE 50.—Airfield southwest of Treves; French photograph taken 7 Apr 40. Scale 1:30,000. Stereoscopic study shows scattered airplanes on the airfield and antiaircraft artillery battery positions.

APPENDIX

LIST OF REFERENCES

Instructions relative to aerial photograph reading	FM 21–25; FM 21–26 (now published as TM 2180–5).
Regulations pertaining to aerial photography	FM 1–35
Measures for coordination of Engineer-Air Corps mapping team	FM 30–20
Instructions on camouflage	FM 5–20

	Paragraph	Page
Aerial—		
Photographs:		
Enemy's intentions, evidence of revealed by	55	31
Examiners, specialist	10	5
Identification of—		
Activities, enemy	35–53	20
Battery locations	50	27
Breastworks	40	23
Cables, buried	52	29
Camouflage	36	21
Dugouts	43	24
Fortifications, concrete	49	27
Guns:		
Machine	44	24
37-mm or similar weapons	45	26
Mine shafts	48	27
Objects	31	17
Basis of	33	17
Methods	34	19
Purpose	32	17
Obstacles, antitank	47	26
Posts, listening, observation, and command	46	26
Rear installations	53	30
Road blocks	47	26
Roads, tracks, and paths	37	21
Shell holes, organized	41	23
Telegraph and telephone lines, overhead	52	29
Trenches	39	22
Wire	42	24
Work, types of	38	22
Importance of	3	1
Interpretation of	54	31
During own offensive operations	56	33
Night	6	4
Oblique	5	4
Requests for	15	8
Study of effect of own artillery fire by	51	29
Use	21	13
As a map	22	13
Attack on fortifications, planning for	25	14
By artillery	27	15
Counterintelligence	30	17
Determining information of enemy by	26	14
Engineering planning	24	14
Landing operations	28	16
Preparation of objective folders	23	13
River crossings	29	16
Vertical	4	2
Photography coordination, responsibility for	12	7
Aviation units, photographic capabilities of	14	8

	Paragraph	Page
Counterintelligence, use of aerial photographs in	30	17
Enemy—		
Activities, identification of from aerial photographs	35–53	20
Intentions, evidence of, revealed by aerial photographs	55	31
Engineering planning, use of aerial photographs in	24	14
Engineers, topographic, action of	19	12
Examiners, specialist, aerial photographs	10	5
Filing of negatives	20	12
G–2, action of on receipt of photographs	18	11
Identification, from aerial photographs:		
Enemy activities	35–53	20
Objects	31–34	17
Interpretation of aerial photographs	54	31
During own offensive operations	56	33
Landing operations, use of aerial photographs in	28	16
Military intelligence:		
Scope	2	1
Purpose	1	1
References on	11	6
Missions, photographic, execution of	17	10
Negatives:		
Filing	20	12
Titling	16	9
Photographic—		
Capabilities of aviation units	14	8
Missions, execution of	17	10
Reconnaissance	13	7
Photographs, aerial:		
Evidence of enemy's intentions revealed by	55	31
Examiners, specialist	10	5
Identification of—		
Activities, enemy	35–53	20
Battery locations	50	27
Breastworks	40	23
Cables, buried	52	29
Camouflage	36	21
Dugouts	43	24
Fortifications, concrete	49	27
Guns:		
Machine	44	24
37-mm, and similar weapons	45	26
Mine shafts	48	27
Objects	31	17
Basis of	33	17
Method	34	19
Purpose	32	17
Obstacles, antitank	47	26

	Paragraph	Page
Photographs, aerial—Continued.		
Identification of—Continued.		
Posts, listening, observation, and command	46	26
Rear installations	53	30
Road blocks	47	26
Roads, tracks, and paths	37	21
Shell holes, organized	41	23
Telegraph and telephone lines, overhead	52	29
Trenches	39	22
Wire	42	24
Work, types of	38	22
Importance of	3	1
Interpretation of	54	31
During own offensive operations	56	33
Night	6	4
Oblique	5	4
Receipt of, action on by G-2	18	11
Requests for	15	8
Study of effect of own artillery fire by	51	29
Use	21	13
As a map	22	13
Attack upon fortifications, planning for	25	14
By artillery	27	15
Counterintelligence	30	17
Engineering planning	24	14
Enemy information determination	26	14
Landing operations	28	16
Preparation of objective folders	23	13
River crossings	29	16
Vertical	4	2
Photography:		
Aerial, responsibility for coordination of	12	7
Color	8	5
Infrared	7	4
Quick work process	9	5
Reconnaissance, photographic	13	7
Titling of negatives	16	9
Topographic engineers, action of	19	12

RESEARCH REPORT 1210

ADA086455

LEVEL II

IMAGERY INTELLIGENCE (IMINT) PRODUCTION MODEL

Christine A. Montgomery
John R. Thompson
Robert V. Katter
Operating Systems, Inc.

DTIC
ELECTE
JUL 1 0 1980
D
C

HUMAN FACTORS TECHNICAL AREA, ARI
OFFICE of DEPUTY CHIEF of STAFF-SYSTEMS, INSCOM

This document has been approved for public release and sale; its distribution is unlimited.

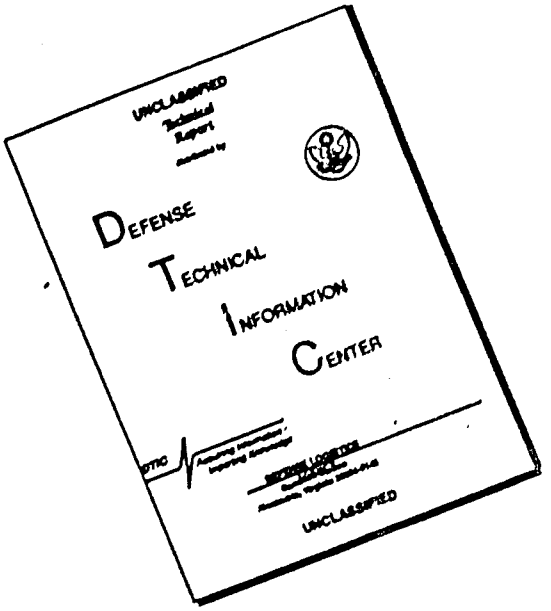
Prepared for

S ARMY RESEARCH INSTITUTE
the BEHAVIORAL and SOCIAL SCIENCES
Eisenhower Avenue
ndria, Virginia 22333

US ARMY INTELLIGENCE
and SECURITY COMMAND
Arlington Hall Station
Arlington, Virginia 22312

80 7 10 038

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

U. S. ARMY RESEARCH INSTITUTE FOR THE BEHAVIORAL AND SOCIAL SCIENCES

A Field Operating Agency under the Jurisdiction of the Deputy Chief of Staff for Personnel

JOSEPH ZEIDNER
Technical Director

FRANKLIN A. HART
Colonel, US Army
Commander

Research accomplished for the
Department of the Army

Operating Systems, Inc.

NOTICES

DISTRIBUTION Primary distribution of this report has been made by ARI. Please address correspondence concerning distribution of reports to: U. S. Army Research Institute for the Behavioral and Social Sciences, ATTN: PERI-TP, 5001 Eisenhower Avenue, Alexandria, Virginia 22333.

FINAL DISPOSITION: This report may be destroyed when it is no longer needed. Please do not return it to the U. S. Army Research Institute for the Behavioral and Social Sciences.

NOTE: The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: Research Report 1210	2. GOVT ACCESSION NO.: AD-A086455
3. RECIPIENT'S CATALOG NUMBER:	
4. TITLE (and Subtitle): IMAGERY INTELLIGENCE (IMINT) PRODUCTION MODEL	5. TYPE OF REPORT & PERIOD COVERED: Interim
6. PERFORMING ORG. REPORT NUMBER: OSI-R79-003	
7. AUTHOR(s): Christine A. Montgomery, John R. Thompson, Robert V. Katter	8. CONTRACT OR GRANT NUMBER(s): MDA 903-78-C-2044
9. PERFORMING ORGANIZATION NAME AND ADDRESS: Operating Systems, Inc., 21031 Ventura Boulevard, Woodland Hills, CA 91364	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: 3810011
11. CONTROLLING OFFICE NAME AND ADDRESS: US Army Intelligence & Security Command, IASYS-R, Arlington Hall Station, Arlington, VA 22312	12. REPORT DATE: January 1980
	13. NUMBER OF PAGES: 166
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): US Army Research Institute for the Behavioral & Social Sciences (PERI-OS), 5001 Eisenhower Avenue, Alexandria, VA 22333	15. SECURITY CLASS. (of this report): Unclassified
	15a. DECLASSIFICATION DOWNGRADING SCHEDULE:

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

163

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

ARI RR-1210

18. SUPPLEMENTARY NOTES: This effort was jointly sponsored by the US Army Intelligence and Security Command (USAINSCOM) and the Army Research Institute (ARI). Dr. Edgar M. Johnson (ARI) and Mr. Philip Lavigne (INSCOM) provided program direction; Dr. Stanley M. Halpin (ARI), MAJ William Franklin (INSCOM), and Dr. Ruth H. Phelps (ARI) monitored technical progress.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Analysis
Intelligence
Imagery
Analytic Procedures

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Imagery Intelligence (IMINT) Production Model presented in this report was developed as a part of a study entitled "Investigation of Methodologies and Techniques for Intelligence Analysis," which is aimed at constructing a model of the cognitive processes underlying intelligence analysis. The approach to constructing such a model is based on the investigation of analytical processing in two types of single source analysis (SIGINT and IMINT), subsequently generalizing to multisource analysis. For the purposes of

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

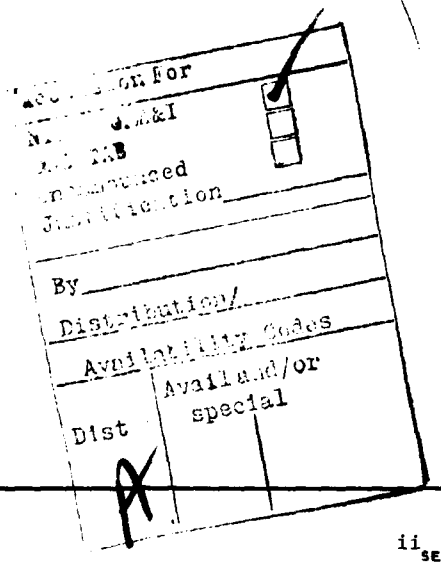
391994

20. (continued)

this investigation, intelligence analysis was defined as a spectrum of analytical judgmental activities involved in the processing and production of intelligence, where particular individuals may devote more or less time to different aspects of such activities according to their individual roles in the intelligence cycle.

The IMINT production model described in this report was developed to serve as a basis for selecting IMINT processes involving high analytical and judgmental content for further study, directed at understanding the cognitive functions that underlie these IMINT processes. Thus, the model was constructed with a specialized focus, for the purposes of the study described above. Rather than concentrating exclusively on either strategic or tactical IMINT, the model was designed to encompass both dimensions of IMINT. The rationale for this decision was the fact that imagery interpretation analysts (IIAs) with more than minimum length of service are likely to operate in each type of mission at some time in their career, demonstrating the practical assumption that the required knowledge base and cognitive skills are similar for the two dimensions of IMINT. The imagery interpretation analyst is the true generic focus of the IMINT production model presented in this report; in order to gather data for developing the model 56 interviews with IIAs were carried out at 8 sites, including both strategic and tactical missions.

The report contains three sections: an introduction, an overview of the IMINT production model, and the model description. Section 1 describes the IMINT model in the context of the study discussed above, and also treats the scope of the model and the collection of the information on which the model is based. Section 2 presents an overview of the model, describing findings about the role of the imagery interpretation analyst, the impact of management on analysis, the IMINT time dimension, and the special role of informal information channels in IMINT analysis. This section also describes the format of the model description, which is represented in terms of hierarchical input-process-output (HIPO) charts. Section 3 presents the model, which is segmented into two major parts: IMINT production management activities and IMINT processing, analysis, and reporting activities.



RESEARCH REPORT 1210

IMAGERY INTELLIGENCE (IMINT) PRODUCTION MODEL

Christine A. Montgomery, John R. Thompson, and
Robert V. Katter
Operating Systems, Inc.

Stanley M. Halpin, Team Chief

Submitted by:
Raymond C. Sidorsky, Acting Chief
HUMAN FACTORS TECHNICAL AREA

Approved By:
Edgar M. Johnson Acting Director
ORGANIZATIONS AND SYSTEMS
RESEARCH LABORATORY

U.S. ARMY RESEARCH INSTITUTE FOR THE BEHAVIORAL AND SOCIAL SCIENCES
5001 Eisenhower Avenue, Alexandria, Virginia 22333

Office, Deputy Chief of Staff for Personnel
Department of the Army

January 1980

Army Project Number
2Q163743A774

Intelligence Systems

Approved for public release; distribution unlimited.

ARI Research Reports and Technical Reports are intended for sponsors of R&D tasks and for other research and military agencies. Any findings ready for implementation at the time of publication are presented in the last part of the Brief. Upon completion of a major phase of the task, formal recommendations for official action normally are conveyed to appropriate military agencies by briefing or Disposition Form.

FOREWORD

Intelligence collection systems have proliferated over the past several years, increasing in complexity and in volume of output. However, there has been no corresponding improvement in the ability of intelligence personnel to analyze this flood of data. US Army Intelligence and Security Command (INSCOM) studies and Army Research Institute (ARI) research indicate that improved support to and training of analysts are necessary to effectively utilize the increased collection capability and satisfy increasing demands for intelligence within current personnel constraints. INSCOM and ARI therefore initiated a joint research program to provide improved support to the intelligence analyst. During early discussions of the issues it became clear that any procedural, training, organizational, or system changes to support analysis will be effective only if based upon a detailed understanding of the analysts' role, methods and thought processes in intelligence production. The first need was to evaluate and describe the human analytic processes underlying intelligence analysis, synthesis and production. The present paper, one of several products of this initial effort, provides a production model of imagery intelligence which focuses on the human processes and factors involved.

The methodological approach used to study current imagery intelligence production involved interviews with image interpretation personnel in different organizations with varying levels of experience, familiar with either tactical or strategic operations, as well as observation of operations during field exercises. Imagery intelligence documentation

and research reports obtained from INSCOM and ARI as well as analyst files also provided data and background material as a basis for the imagery production model. Invaluable and outstanding support was received by the research team from personnel at numerous imagery interpretation training or production facilities.

The research was accomplished by a government-contractor team under contract MDA 903-78-C-2044 and monitored jointly by INSCOM and ARI. Continuous interaction and collaboration of personnel from Operating Systems, Inc., INSCOM and ARI insured a multidisciplinary approach to this research.

This report and a corresponding model of signals intelligence production previously developed by INSCOM provide a basis for the development of a detailed functional model of the intelligence analyst. The current report should be very useful during the development or evaluation of training materials, procedures, doctrine and automated support for the image interpreter analyst.

Dr. Joseph Zeidner
Technical Director of ARI and
Chief Psychologist, US Army

MG William I. Rolya
Commander, US Army
Intelligence and Security
Command

IMAGERY INTELLIGENCE (IMINT) PRODUCTION MODEL

BRIEF

Requirement:

To develop a model of the processes involved in the production of imagery based intelligence. This model will be used to support subsequent research on the cognitive functions of both single mode (e.g., signals intelligence; imagery intelligence) and multi-source intelligence analysts.

Approach:

A series of structured interviews was conducted with image interpretation personnel in a variety of organizations. An attempt was to include persons with various levels of experience, familiar with tactical or strategic operations. Interviews with developers of training materials, and observation of classroom instruction and of field exercises, provided additional information on individual and group responsibilities. The interviews and observation were supplemented by documentation and research reports from INSCOM and ARI. The various findings and viewpoints were consolidated and integrated into a model of the processes being examined.

Product:

The model of imagery intelligence production processes is presented as a series of hierarchical input-process-output (HIPO) charts with parallel verbal discussion of critical points. This format, discussed in detail in the text, provides a convenient means for representing the complex processes involved at a usable level of detail. The model is divided into two major parts: activities associated with production management; and activities associated with processing, analysis, and reporting.

Utilization:

The model presented lays an important foundation for a continuing effort to describe in detail the cognitive processes involved in intelligence analysis and to develop training and system support to analysts. The model will be useful during the development or evaluation of training materials, procedures, doctrine of employment, and automated support for the image interpreter.

TABLE OF CONTENTS

		Page
1.0	INTRODUCTION	1-1
1.1	Background	1-1
1.2	Scope of IMINT Production Model	1-2
1.3	Data Collection	1-3
2.0	IMINT PRODUCTION PROCESSING MODEL OVERVIEW	2-1
2.1	Concept of IMINT Production	2-3
2.1.1	The Role of the Image Interpretation Analyst (IIA)	2-3
2.1.2	Management of an II Production Facility	2-4
2.1.3	Timeliness in IMINT Analysis and Reporting	2-5
2.1.4	Informal Information Channels	2-6
2.2	Representation of IMINT Production Activities	2-8
2.3	Process Description Format	2-11
3.0	IMINT PRODUCTION PROCESSING MODEL DESCRIPTION	3-1
B.1	IMINT Production Management	3-3
B.1.1	Production Planning	3-5
B.1.2	Tasking	3-10
B.1.3	Monitoring and Evaluation	3-14
B.1.3.1	Evaluate Backlog	3-16
B.1.3.2	Evaluate Capabilities	3-18
B.1.3.3	Evaluate Requirements	3-21
B.1.3.4	Evaluate Products	3-23
B.2	IMAGERY Intelligence Processing, Analysis, and Reporting	3-25
B.2.1	Imagery Intelligence Analysis	3-27
B.2.1.1	Search	3-33
B.2.1.2	Registration/Plotting	3-37
B.2.1.3	Target Detection	3-41
B.2.1.4	Target Identification	3-45
B.2.1.5	Target Quantification	3-54
B.2.1.6	Unusualness Analysis	3-56

PRECEDING PAGE BLANK - NOT FILMED

Page

B.2.1.7 Function Analysis---------- 3-60
B.2.1.8 Complex Studies---------- 3-62
B.2.1.9 Photogrammetric Sciences---------- 3-80

B.2.2 Reporting---------- 3-84

B.2.2.1 First Phase Reporting---------- 3-88
B.2.2.2 Second Phase Reporting---------- 3-90
B.2.2.3 Third Phase Reporting and Products----- 3-93

B.2.3 Support Activities---------- 3-95

B.2.3.1 Collection Coordination---------- 3-97
B.2.3.2 All Source Data Review and Reduction--- 3-102
B.2.3.3 History of Coverage Maintenance------- 3-104
B.2.3.4 Target Analysis/Development---------- 3-108
B.2.3.5 Imagery Interpretation Key Development---------- 3-116
B.2.3.6 Knowledge and Skill Development-------- 3-120

B.2.4 Administrative Support---------- 3-126

B.2.4.1 Computer System Operations---------- 3-126
B.2.4.2 Data Categorization, Filing, and Distribution---------- 3-127
B.2.4.3 Typing, Graphics, and Reproduction---- 3-129

APPENDIX A---------- A-1

REFERENCES---------- R-1

DISTRIBUTION---------- D-1

1.0 INTRODUCTION

1.1 Background

The Imagery Intelligence (IMINT) Production Model has been developed as part of a study entitled 'Investigation of Methodologies and Techniques for Intelligence Analysis' aimed at constructing a model of the cognitive processes underlying intelligence analysis. There are three basic assumptions motivating this research. First, it is assumed that there exists a set of common analytical processes which crosscut the various intelligence disciplines, constituting the core processes of intelligence analysis. Second, it is assumed that the set of core processes represents a continuum of analytical complexity ranging from those lower in cognitive and judgmental content to those involving a high degree of cognition and judgment. Third, it is postulated that a better understanding of these core analytical processes will

- facilitate efforts to develop and evaluate training programs and training doctrine for intelligence analysts;
- provide criteria for the development and evaluation of advanced system designs in support of intelligence analysis,
- provide assistance in personnel selection, motivation, and career planning;
- provide criteria for evaluating intelligence analysis processes, and for modifying and adapting such processes;
- contribute to the improvement of intelligence analysis management and formulation of operating policies and procedures.

The approach to identifying the set of core analytical processes and developing a generic cognitive model based on these is to investigate analytical processing as currently practiced in two types of single source analysis, subsequently generalizing to all source analysis. The initial task thus involved a preliminary investigation of signal intelligence (SIGINT) to isolate those SIGINT processes which appeared to have a high analytical and judgmental content for further study directed at an understanding of the cognitive processes that underlie them. The basis for the initial investigation was the SIGINT production model prepared by the Kuras-Alterman Corporation [Ref. 29].

The second intelligence discipline investigated under this study was imagery intelligence (IMINT). Since no comparable production model existed for IMINT, the model described in this document was prepared to serve as a basis for selecting IMINT processes involving high analytical and judgmental content, and to compare these with similar SIGINT processes in order to provide an initial definition of the core analytical processes that crosscut the various intelligence disciplines.

This initial definition of core analytical processes and the cognitive processes underlying them based on SIGINT and IMINT analytical processing will then be expanded to all source analytical processing, including HUMINT. A generic cognitive model for intelligence analysis will then be developed, which will demonstrate the nature of, and relationships between, specific cognitive components used in intelligence analysis activities. Such components operate within the head of the analyst and include, among others, memory, perceptual, conceptual, decision, and learning aspects.

When completed, the generic model will highlight the commonalities and differences among various intelligence analysis disciplines, and will provide a systematic, meaningful framework which will prove useful in a number of ways. The design of tasks and tasking procedures, training regimens, and task-supportive technologies can benefit from a systematic framework for the comparative description of intelligence analysis specialties formulated in terms of cognitive functioning. Areas of analytic practice may be identified for which unrealistic demands are now made on various aspects of an analyst's cognitive resources. Components of emergent new analytic tasks may present themselves, and the model may suggest better ways to process them. A comparative framework such as the model can provide a systematic, rationalized means for the borrowing of insights and techniques by different specialties from one another. The generic model can provide a common ground to promote better understanding, coordination, and orchestration between the efforts of different specialties. For each of the possibilities just mentioned, the model may operate to suggest research questions and research approaches for the solution of problems.

As indicated earlier, to insure that the generic cognitive model is representative of a range of intelligence, it will be based on several kinds of information. Specifically:

(1) A model of processing activities for SIGINT production [Ref.29];

(2) A model of processing activities for IMINT production;

(3) A range of interview and observational data involving SIGINT, IMINT, and HUMINT.

This document presents the IMINT production model. IMINT interview and observational data outside the scope of this model will be treated in a later paper.

1.2 Scope of the IMINT Production Model

The IMINT production model presented in this report was developed with a specialized emphasis and focus, to serve the specific needs of the research study described in the preceding paragraphs. The model should not be construed as having detailed applicability for other purposes, although it may provide useful insights outside the original intent of the study. In its main outlines, the model represents a framework

within which the common aspects of various IMINT specialties are described. It is neither an exhaustive nor a detailed description of any particular IMINT specialty, although some of the dimensions of variation among specialties are noted.

1.2.1 Strategic versus Tactical IMINT. A major issue in developing the model of IMINT production involved the decision to use IMINT processing as practiced on the tactical level as a basis for the model, or IMINT processing as performed by the national strategic resources, or to construct a model that would represent both tactical and strategic IMINT. The last alternative was selected for two reasons. First, an imagery interpretation analyst (IIA) who has a career of any length is likely to serve at some time on both levels, indicating that the analytical and cognitive processing is at least presumed to be similar; this makes it important to accommodate both processing environments within the same IMINT production model, in order to accomplish the objectives of the basic study described in Section 1.1. Second, preliminary investigation of IMINT indicated apparent parallels between IMINT processing on the strategic and tactical levels. With the exception of a few real time imagery interpretation tasks that are exclusive to the tactical mission -- i.e., Side-Looking Airborne Radar (SLAR), and Infrared (IR) processing -- there are obvious parallels in almost all aspects of IMINT production (including imagery media, IMINT analysis, collateral resources, time phasing, and products). The main differences between the strategic and tactical processing environments involve the percentage of time devoted to various IMINT analytical and information handling activities (reflecting differences in mission requirements), support availability, and the range in skill levels and knowledge of individual IIAs working in the mission (Army strategic II facilities, for example, apparently do not utilize the lower skill levels).

1.2.2 Format of the Model. The detailed processing steps in different IMINT specialties, and between the same activities performed at the tactical and the strategic levels vary as to both inclusion and sequence within the activities and processes, making a detailed flow charting form of representation inappropriate. The parallels between specialties, and between tactical and strategic level IMINT processing emerge more clearly at a less detailed level of description, and are consequently best illustrated by hierarchical input-process-output (HIPO) charts. The representation conventions for these charts are explained in Section 2. Thus, unlike the SIGINT production model [Ref.29], the IMINT model does not consist of step-by-step flow diagrams of detailed task activities.

1.3 Data Collection

The sources of information on which the IMINT production model is based include the documents listed in the references (INSCOM and ARI reports, Army training manuals and field manuals), site visits to the strategic and tactical II facilities listed in Appendix A, and numerous detailed interviews with IIAs at all levels.

The majority of available documentation in the II field addresses training of lower skill level tactical analysts and the more mechanical aspects of the IMINT production process. There exists no formal documentation describing IMINT production in the national strategic environment.

The more complex aspects of IMINT analysis -- especially those aspects which are relevant to development of a generic cognitive model of intelligence analysis -- are passed on as an 'oral tradition', or are spontaneously learned by an IIA. The high security classification of many IMINT products is a major contributing factor in sustaining this 'oral tradition' and restricting the availability of reference documents and other materials, such as training imagery and II keys, in the tactical environment. Interviews with IIAs were thus the most important source of information for the model.

2.0 IMINT PRODUCTION MODEL OVERVIEW

B. IMAGERY INTELLIGENCE PRODUCTION MODEL

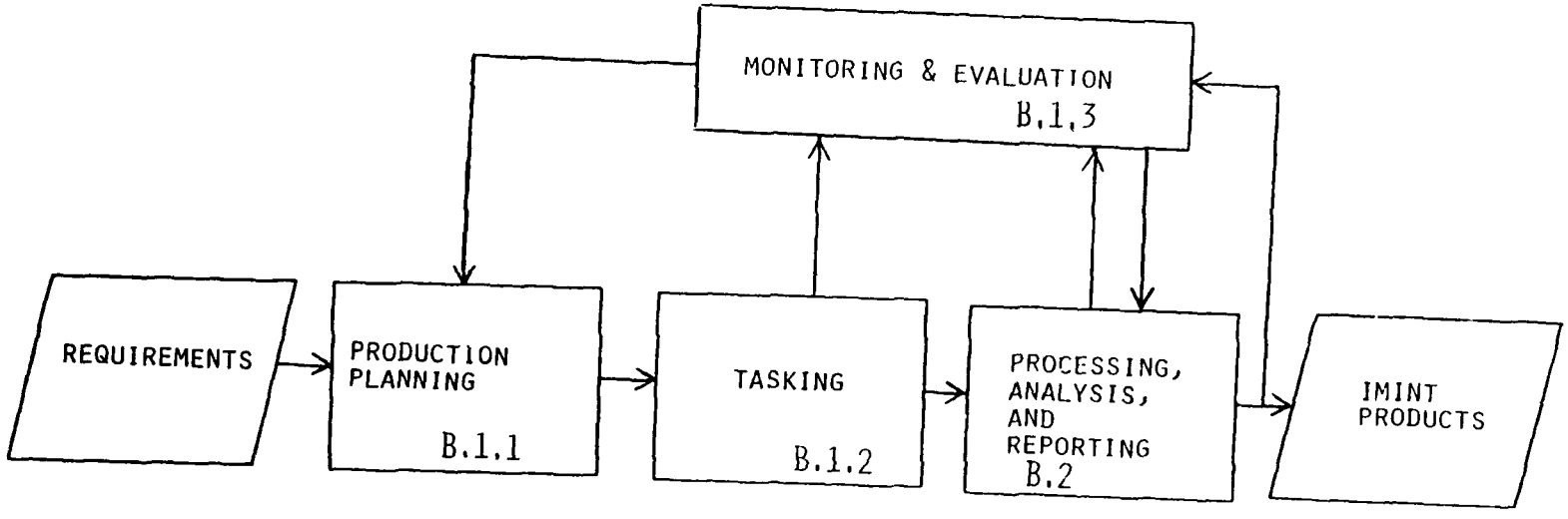


Figure 2-1. Model Overview

2.1 Concept of IMINT Production

The IMINT production process involves a combination of management, analytical, and support activities that operate against defined requirements and generate specified products. In attempting to determine the analytical and cognitive processing that occurs during imagery interpretation, it became clear that the management functions of planning, tasking, and evaluation had major impacts on the performance of imagery interpretation activities, and on the role of the image interpretation analyst (Section 2.1.1). As shown in the overview chart of the IMINT production model, Figure 2-1, these management activities are included as an integral component. Each of the management activities is discussed in the model description (Section B.1), although the amount of detail is less than for the analytical activities (Section B.2), which are the focus of the model development. Management of the II facility, which also affects the performance of IMINT activities, is discussed in Section 2.1.2, while the important impacting factor of timeliness is treated in Section 2.1.3. The formal lines of communication in the model overview chart show the use of feedback mechanisms through monitoring of tasking, analytical processing, and products. Feedback is one of the most ubiquitous and powerful mechanisms that occurs in the IMINT context, and is thus addressed throughout the IMINT production model. In addition to these formal lines of communication, and perhaps more effective, are the informal lines of communication described in Section 2.1.4.

2.1.1 The Role of the Image Interpretation Analyst (IIA). The obvious focus of the study of IMINT production was the role of the imagery interpretation analyst (IIA). No documentation describes how the IIA actually derives intelligence information from imagery. As noted above, the training manuals and relevant reports listed in the references concentrate on what IIAs do -- on the mechanical, observable activities -- rather than on how they do it. Thus much of the information on which the IMINT production model is based is derived from interviews with practicing IIAs or IIA instructors. These interviews allowed the construction of a role model for the IIA which is quite different from the image conveyed by the documents listed in the references.

Imagery interpretation is a highly skilled profession with areas of specialization. As in any intelligence field, the IIA must adapt rapidly to the changing world situation, as well as to evolving imagery collection capabilities and changes in tasking.

In performing imagery interpretation tasks, IIAs bring to bear the cumulation of their professional skills, experience, and knowledge in attempting to derive a product that will satisfy the needs of the user community within the constraints of available time and resources. IMINT analysts have a challenging task; their perception of threat is often the ultimate basis for critical strategic and tactical decision making.

Far from 'bean counting', the IMINT analytical activity involves complex processes of deductive reasoning. IIAs do not simply look at objects: they must be concerned with the associations between a given object and other objects which are not visible, between visible objects and configurations (e.g., TO&Es) indicating organizational size and strength, between objects and their function, and therefore, the degree of threat indicated by a given piece of equipment in a particular state of readiness, or by a particular activity in process. A strategic level IMINT instructor teaches his students the 'LST' principle, which he sums up in the following terms:

- L - Look at all the imagery.
- S - See what is in the optical field of view. Discovery and recognition of a target must come from within you. It is a function of background knowledge and concentration.
- T - Think about what you see. Combine logic, knowledge, curiosity, and most important, imagination, in the search. Only at the thinking level can one be considered an analyst.*

The issue of background knowledge is an important one. IIAs prepare for the IMINT production activities not only by practicing the mechanical skills of IMINT production, but also by developing a background in geographic, cultural, and technical aspects associated with the area of responsibility. They must be familiar with the geography and cultural background of an area in order to distinguish unusual objects and conditions from normality. IIAs in general are highly concerned with pursuing available information resources, both background and collateral. They are information entrepreneurs and archivists, whose external memory store of information is as important as the internal one it supports.

Successful IIAs appear to be highly motivated, and have a natural or developed curiosity about the area of analysis, frequently comparing themselves to 'detectives'. IIAs tend to be highly individualistic in their methods and take pride in their accomplishments; however, this individualism is balanced by a strong 'team' sentiment. IIAs feel responsible for assisting other members of an II group in the education of novice IIAs and in carrying out complex tasks.

2.1.2 Management of an II Production Facility. II facilities exhibit considerable difference in production processing based on their mission and resources in terms of staff, support, and imagery collection inputs. The activities of the II facility as a whole may vary considerably as a function of time depending on the active missions the facility has at the time of observation. A tactical unit in garrison may have only a training and exercise mission.

Facilities with active missions have problems in allocating scarce personnel and support resources to perform tasks. Facilities without active missions are faced with the problem of preparing for contingency operations and maintaining the proficiency of the IIA staff. In the latter cases, the dedication of the II facility management and senior analysts is the determining factor in how actively the facility engages

*From the instructional materials of John Schlegel.

in training and preparation for contingency operations of various types.

A case in point which was referred to frequently by interviewed analysts was that, especially in peacetime, Army corps level II operations tended to assume division II functions. This condition occurs because most decisions are made at corps level, where intelligence operations have ready access to national assets and direct knowledge of the broader context of intelligence operations. Division level intelligence resources thus tend not to be regularly tasked except for major exercises (such as Reforger), and must rely on their own initiative to maintain an active proficiency in imagery interpretation.

Support capabilities can also constrain the activity of the II facility. Lack of storage for classified material, secure communication channels, and photo lab facilities has a major impact on the II facility capacity for performing active missions.

A given facility may not engage in a complete spectrum of imagery interpretation tasks, because of area of responsibility, constrained resources, and/or lack of support capabilities. The II facility management can provide training or exercises to complement its active mission role, to diversify its capabilities, and satisfy general training requirements for the II MOS skill area.

2.1.5 Timeliness in IMINT Analysis and Reporting. The intelligence products which derive from imagery analysis may support a diversity of missions, including Indications and Warning (I&W), targeting, collection exploitation, basic intelligence, or direct support. The scope and form of these products vary substantially between tactical and strategic missions. An attribute of these missions and products that is common for both strategic and tactical imagery interpretation is timeliness. In IMINT production, timeliness requirements are defined in terms of First Phase, Second Phase, and Third Phase processing. Definition of IMINT processing in terms of three phases is a convention which is normally applied only in the environment of the national strategic IMINT resources. For purposes of this model, the three phased definition is also applied to tactical level processing because of the parallelism which exists in terms of analytical and reporting time constraints. The effect of these phases on analytical and reporting activities is described in detail in Section 6.2 of the model; the following paragraphs present brief definitions of the approximate time periods represented by these phases.

First Phase processing refers to derivation of intelligence from the initial scan of imagery (or from real time imagery generated by SLAR, IR, or video devices) and is normally tasked by time-critical applications.

Second Phase processing refers to exploitation of imagery within a period of more than one and less than 24 hours, and applies primarily to current intelligence applications.

Third Phase processing includes periodic reporting, special support-processing wih 48-hour or longer turnaround, and basic intelligence reporting.

While organizations within a national strategic IMINT facility may specialize in only one phase of processing, a tactical II facility more commonly engages in all three phases of IMINT production, depending on operational requirements.

2.1.4 Informal Information Channels. One of the more powerful mechanisms that operates to make the IMINT production process more efficient and adaptive to the environment is the informal information flow and coordination that takes place during the course of imagery interpretation production. As with other intelligence analysis disciplines, imagery interpretation is an inexact process because results can be partially speculative, data are incomplete, ambiguities are prevalent, and the environment being monitored is continually changing. Informal communications channels allow the IMINT production process to exploit all available information sources in the generation of useful intelligence products.

Informal information flow tends to be more direct because it bypasses chain of command delays and avoids the overhead of filling out forms and having paperwork reviewed. Personal contact or secure voice conversations are the most common communications channels for informal information flow, but secure TTY circuits (OPSCOMM, INDICOM) are also used.

Informal communication channels do not conflict with standard operating policies or formal reporting policies, but in fact act as a supplement. Experienced II analysts are allowed to initiate external communications without management approval when the context is within the given IIA's area of responsibility. Imagery interpretation is the type of process which cannot be monitored at the process level. Management would have to replicate the IIA's entire task in order to determine if the analyst was performing that task correctly. II management must depend on the professionalism of the II analyst to seek informal help from other IIAs in problem areas. Direct control of the II analyst is generally achieved only by monitoring the IIA's time, productivity, and quality of the products he generates, as well as by tasking the IIA in areas where his proficiency is known.

The major types of informal information flow that were identified through interviews with II analysts and instructors are shown in Figure 2-2. Actual flow is more in terms of a network, where analysts in the network are tied together by mutual area of interest. Creation of these networks is also an informal process resulting from joint working groups, personal references, appearance of analyst names on intelligence products, and past experiences in dealing with other agencies. The informal networks seem to be sustained on the basis of credibility of the analyst's information and sharing of information resources that are either not globally available or are more easily understood when interpreted by a specialist in the area.

Two types of informal communications most often mentioned by interviewed analysts as having positive effects on the quality of IMINT products were:

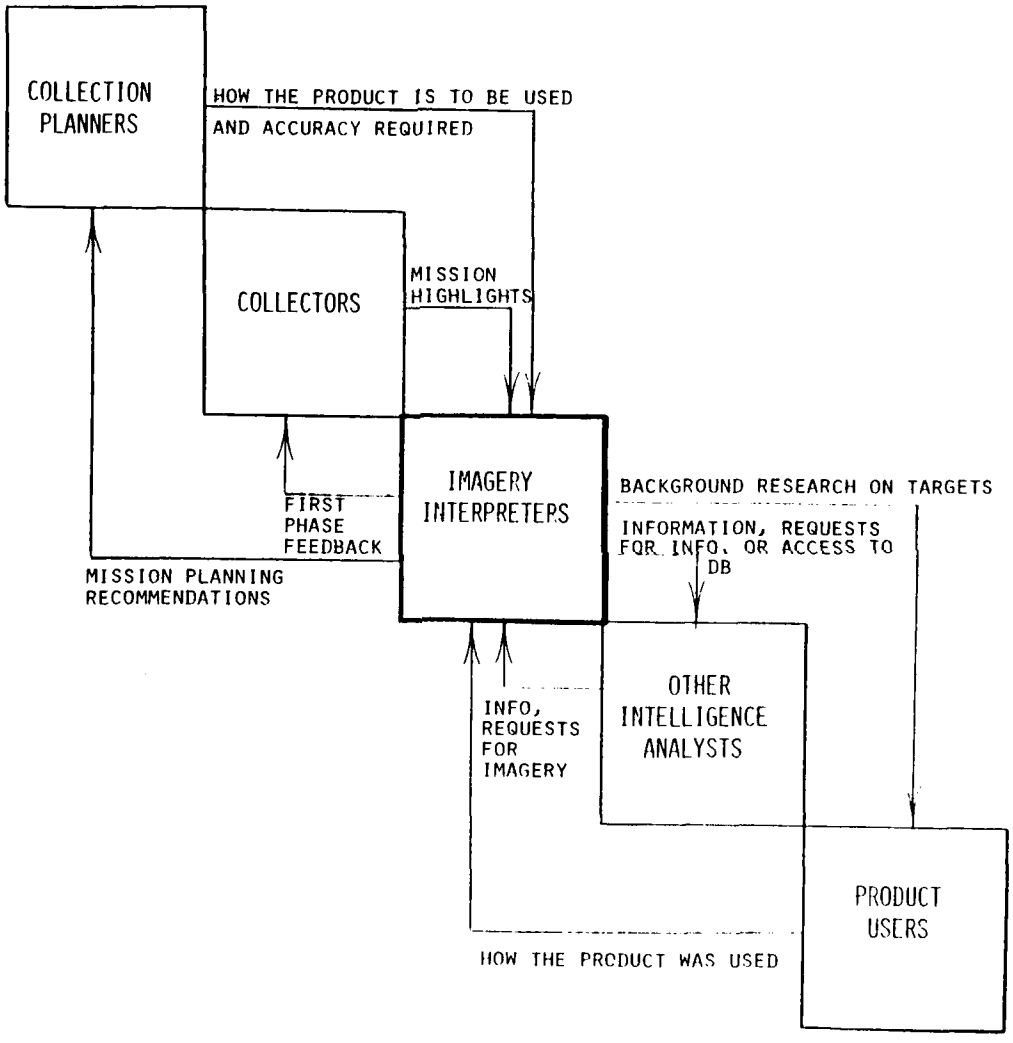


Figure 2-2. Informal Information Flow

1) communications regarding how the product will be used, and accuracy required when the requirement is issued; or

2) recognition of work well done.

2.2 Representation of IMINT Production Activities

The primary variables in determining the breakdown of IMINT production activities are mission, skill level, and time. As mentioned above, the variable of time tends to be dominant at the strategic level, where the IMINT production organizations may be described as having a mission which is single phase (in terms of the discussion of Section 2.1.3). On the other hand, tactical II facilities tend to carry out all three types of processing, depending on the operational requirements. Within both environments, assignment of analytical and reporting tasks depends on the skill level of the individual IIA. These three variables focus on different dimensions of IMINT production process, which must be represented in some way in the model.

The representativeness of the model of different types of IMINT activity also depends on the manner of observation of the IMINT production process. The time of observation of an IMINT production activity could range from a 'snapshot' of peak processing activity to a long term observation of a unit and its operation cycles. The long term observation could also be interpreted as the expected or probable assignments that an individual IIA would receive over his career in the IMINT field: i.e., covering multiple skill levels and a diversity of active missions and training in various II schools and facilities.

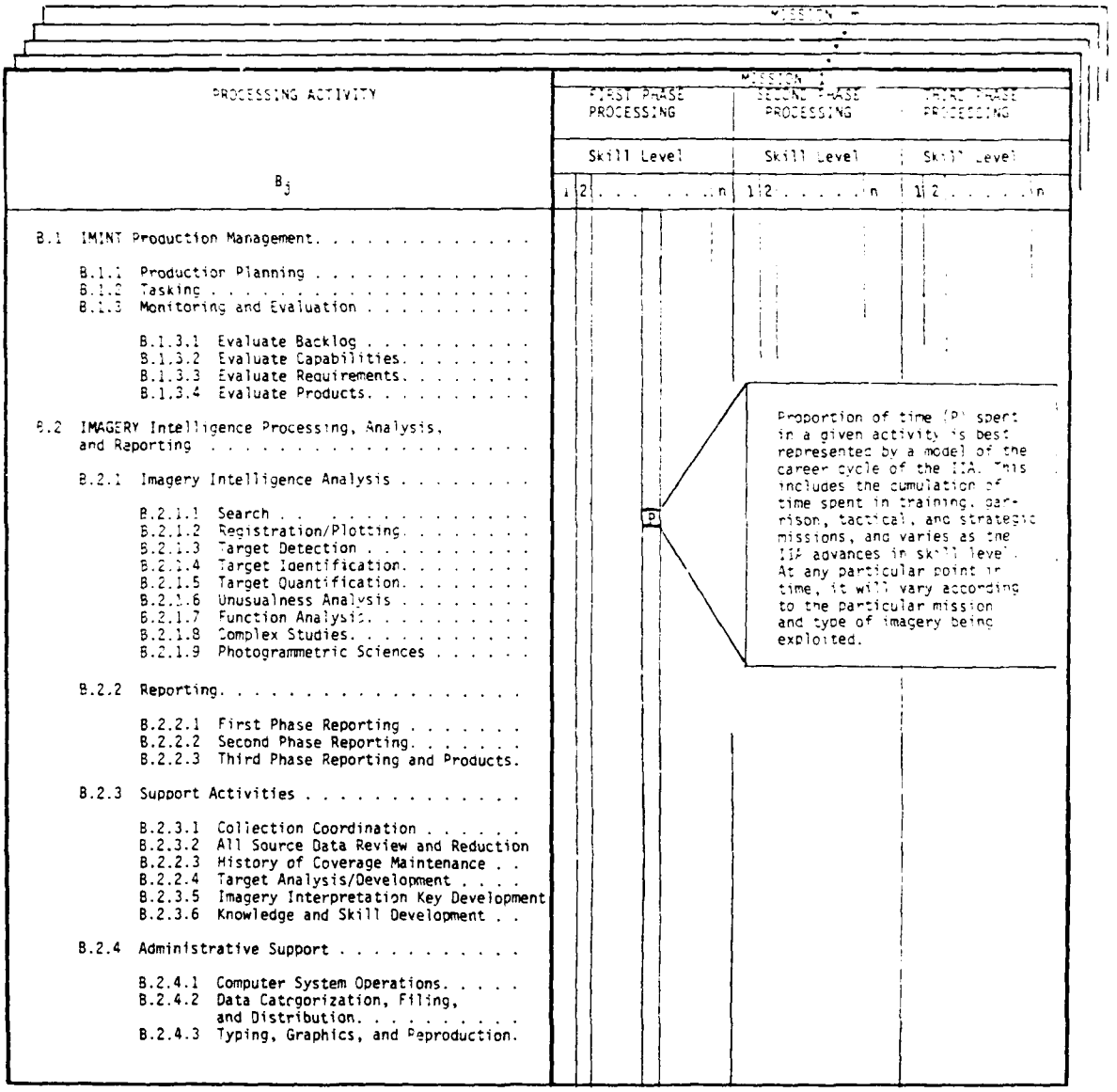
In addition to these general issues of process representation, there are several specific problems in devising a format for accurately representing IMINT production activities. Some performance steps for IMINT activities are in fixed sequence, others show high variability in sequence; some sequences are logically mandatory, others optional. Moreover, some activity steps are restricted to certain work roles and organizational slots, while others are distributed very generally; some steps occur rarely, some occur with great frequency. II analysts may be assigned concurrent processing tasks, resulting in a time-sliced, priority-driven allocation of daily activities. As a direct consequence of these practices, an analysis is needed to reflect time spent by an IIA in various processing activities. As shown in the processing activity matrix of Table 1, the activities of a given facility can be represented by the proportion of time spent in particular activities.

The formula for computing level of activity in a given task is equivalent to the statistics produced by a standard Management Information System (MIS) which keeps track of II analyst activity on an hour-by-hour basis. This type of MIS data is in fact maintained at national strategic level organizations for use in planning and allocation of personnel resources.

This form of activity representation is useful in examining crucial areas of skill development, as well as life cycle impacts of management

Table 1

IMAGERY INTERPRETATION PRODUCTION - PROCESSING ACTIVITY MATRIX



and support activities. The existence of a particular type of activity or processing task -- whatever the level of activity -- is important in determining the information structure and complexity of cognitive processing, pursuant to the ultimate objectives of this research described in Section 1.1.

The left hand column in Table 1 reflects the higher level structure of production activities in terms of staff organizations, time sequence, and processing sequence. Since facilities will tend to have more than one type of mission, this table is in fact multiplied by each type of mission.

This type of probabilistic representation of IMINT production activities has several uses:

(1) as an illustration of the diverse activities for which IIAs must be trained over the long term,

(2) as an indication of which activities analyst resources are utilized in,

(3) as a comparison of skill needs to skill training.

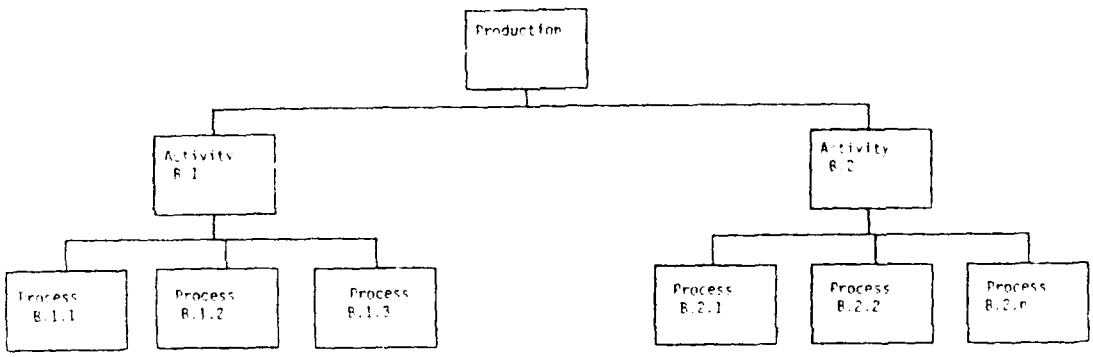
Since the model presented in this report is intended only as a generic representation of the spectrum of IMINT production processing activities, no attempt has been made to fill in the comparative level-of-activity values for individual task areas.

2.3 Process Description Format

IMINT production processes are described in Section 3.0 using the HIPO (Hierarchical Input-Process-Output) format. This format was selected over the more conventional flow diagramming format for the reasons discussed in the preceding section -- especially because the processes forming a particular IMINT production activity are not necessarily sequential. The HIPO format provides a means for systematically describing IMINT production in terms of a hierarchy of management and analytical activities. These activities are further subdivided into processes, which are in turn composed of subprocesses, where all three levels may have specific or general inputs and outputs. While the management activities described in Section B.1 of the model are not elaborated to the subprocess level, the analytical activities described in Section B.2 are specified in more detail. A further description of the conventions used in the HIPO charts on analytical activities is contained in Section B.2.1.

As illustrated in Figure 2-3, the HIPO descriptions are composed of hierarchical charts which identify major production activities, and Input-Process-Output diagrams providing in depth descriptions of each activity. The HIPO format thus presents a top-down description of the overall IMINT production process, outlining a generic IMINT production facility which encompasses a broad range of both tactical and strategic IMINT production activities.

FUNCTIONAL HIERARCHY



PLUS

INPUT-PROCESS-OUTPUT DIAGRAMS

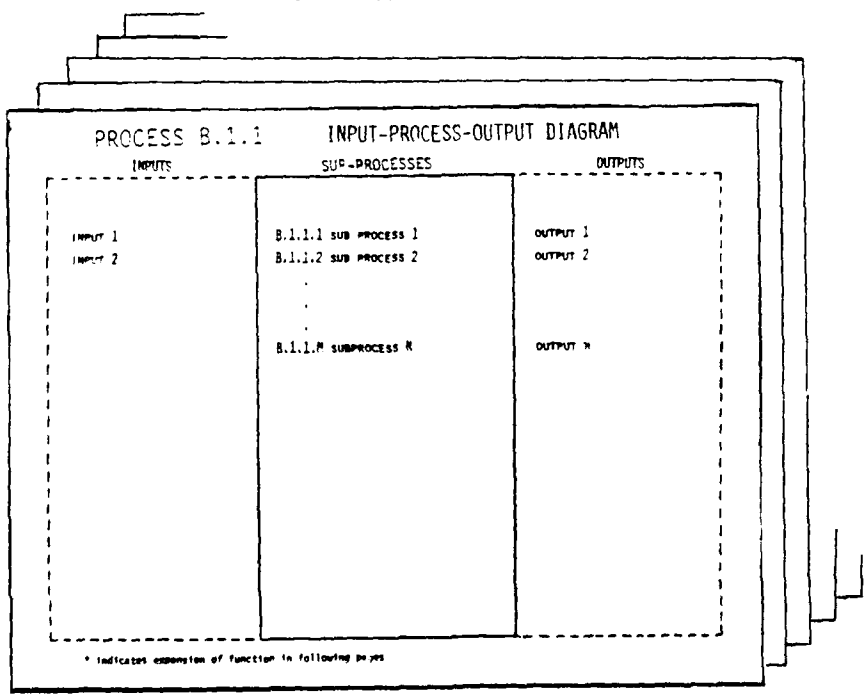


Figure 2-3. HIPO Format Used in II Model Description (Page 1 of 2)

HIPO Conventions

*An asterisk appearing in a diagram block indicates that a more detailed expansion of that block will appear in the immediately following pages.

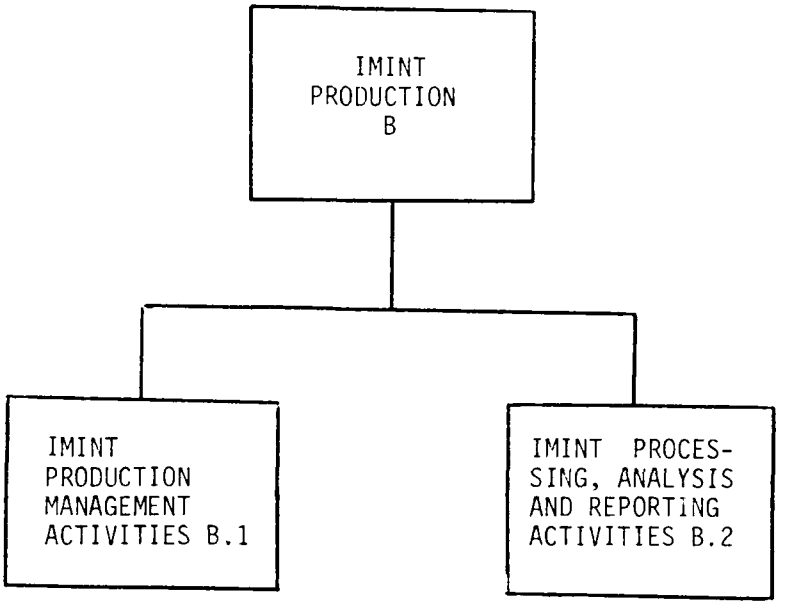
Input 1
Input 2
Input 3

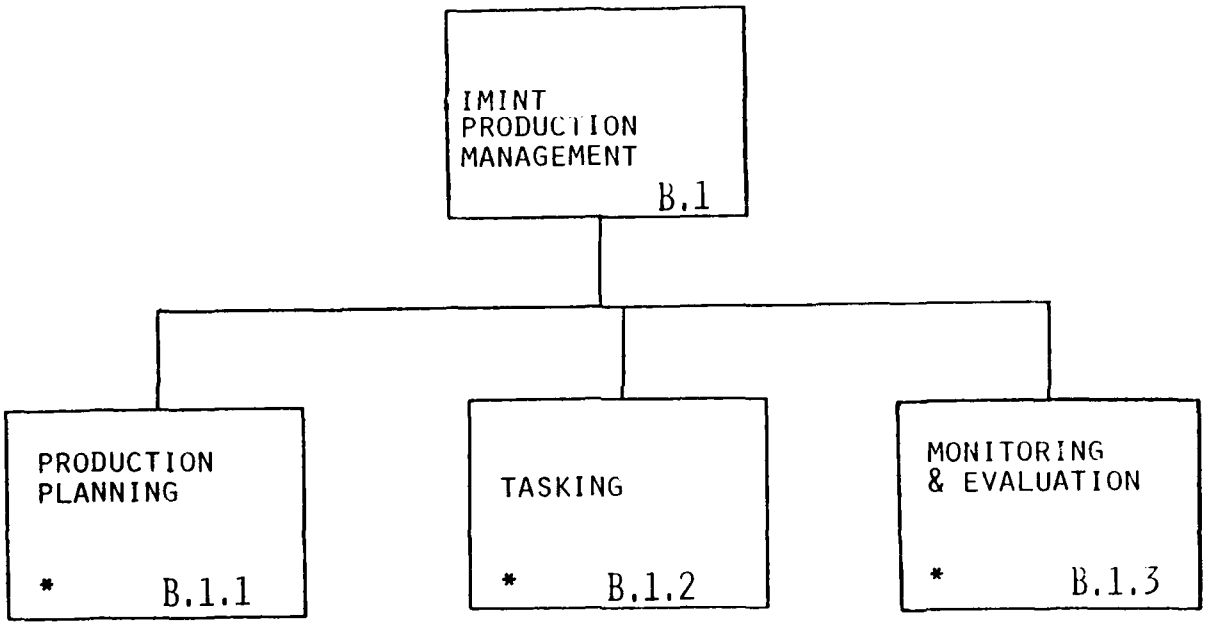
Bracketed inputs are general inputs to an activity or a process and are not specific to any particular process or subprocess; otherwise inputs are lined up with the particular process or subprocess to which they apply (similarly for outputs).

Output 2 (B.2.3.1) A model process or subprocess number appearing next to an output name indicates that the output is specifically an input to the referenced process (similarly for inputs with number references).

Figure 2-3. HIPO Format Used in II Model Description (Page 2 of 2)

3.0 IMAGERY INTERPRETATION PRODUCTION PROCESSING MODEL DESCRIPTION



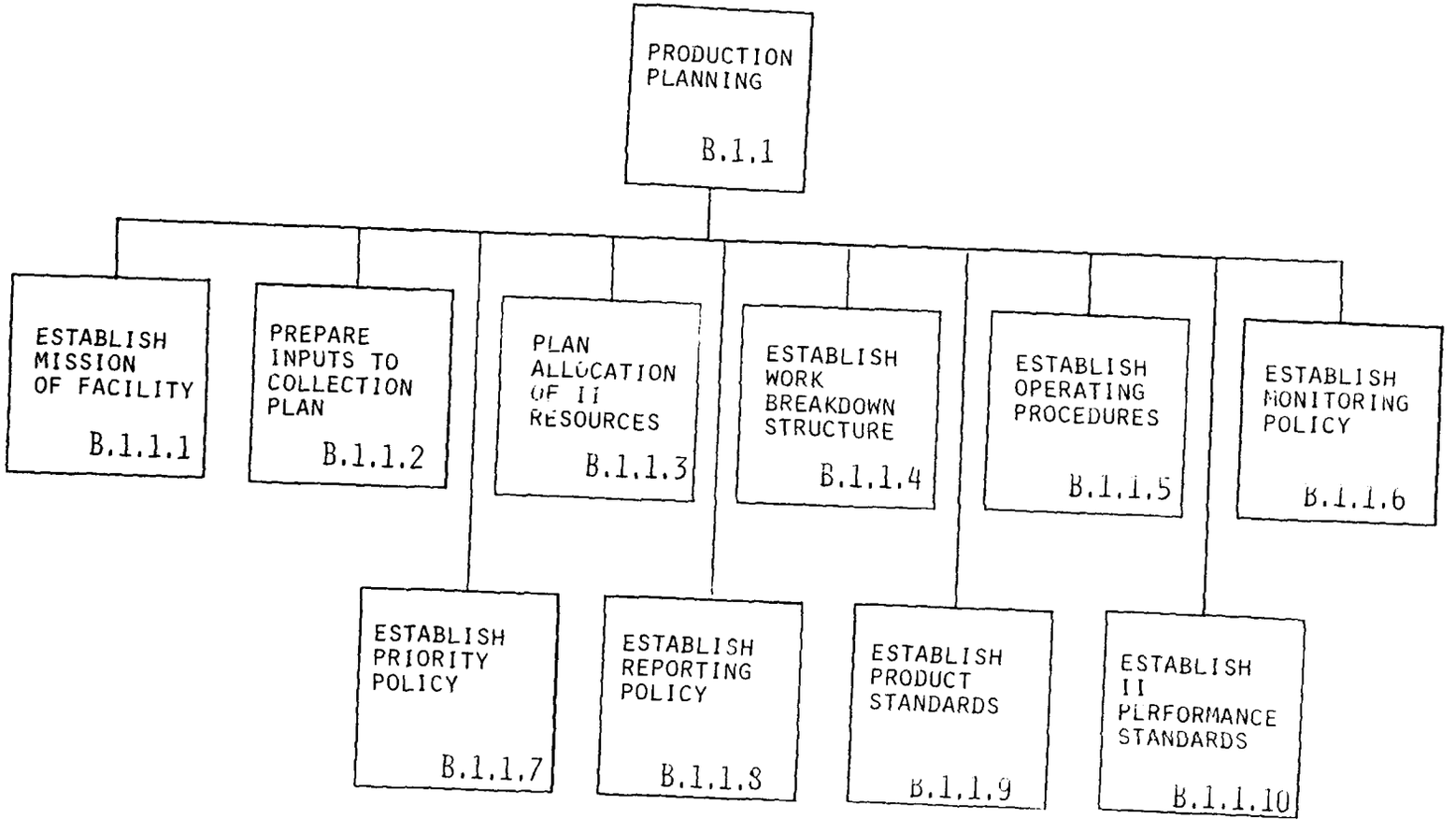


*INDICATES EXPANSION OF DETAIL IN FOLLOWING PAGES

B.1 IMINT Production Management

IMINT production management has the function of allocating and controlling the use of II facility resources for the production of imagery intelligence. IMINT production is a technological activity. Management of a technological activity is different from managing a manufacturing process because the capabilities of the personnel are the principal factors in productivity and output product quality.

The IMINT production manager's primary control mechanisms are the assignment of personnel and the use of time (including the time between active missions).


PRODUCTION PLANNING
B.1.1
ESTABLISH MISSION OF FACILITY
B.1.1.1
PREPARE INPUTS TO COLLECTION PLAN
B.1.1.2
PLAN ALLOCATION OF II RESOURCES
B.1.1.3
ESTABLISH WORK BREAKDOWN STRUCTURE
B.1.1.4
ESTABLISH OPERATING PROCEDURES
B.1.1.5
ESTABLISH MONITORING POLICY
B.1.1.6
ESTABLISH PRIORITY POLICY
B.1.1.7
ESTABLISH REPORTING POLICY
B.1.1.8
ESTABLISH PRODUCT STANDARDS
B.1.1.9
ESTABLISH II PERFORMANCE STANDARDS
B.1.1.10

B.1.1 Production Planning

Production planning is the set of activities involved in preparing the II facility to perform its assigned mission. For well-established strategic II facilities, the production operates according to precedents, and much of the planning information structure is unwritten. Formal planning activities are of more importance to a tactical facility in a pre-deployment stage where personnel may be less experienced, and unfamiliar with the deployment area. Planning requirements are influenced by the list of factors presented on the associated chart, which are discussed in the following paragraphs.

Mission. The mission of an Army II facility establishes which agencies task the facility and defines the facility's areas of responsibility. The mission of the facility will vary depending on resources and course of the battle in a combat situation. Area of responsibility may be defined in terms of geographic area, type of target, or imagery source.

Collection Plan. The II facility coordinates with collection planning groups and has responsibility for recommending targets and missions within the scope of their tasking. Collection planning is necessarily controlled from the big picture perspective. The ability of a particular facility to exploit specific types of imagery will influence the collection plan.

Allocation of II Resources. The II facility is tasked concurrently in many areas of imagery interpretation. The II production manager must allocate resources for different areas of tasking and support activities. The manager has responsibility for coordinating additional resources needed to meet requirements. Using estimates of current processing backlog and projected workload, the II facility manager can produce a tasking plan to assist in deciding allocation of resources.

B.1.1 PRODUCTION PLANNING

INPUTS	PROCESS		OUTPUTS
MISSION	B.1.1.1	EVALUATE MISSION OF II FACILITY	EVALUATION OF II FACILITY MISSION
RECOMMENDED INPUTS TO COLLECTION PLAN (B.1.3)	B.1.1.2	PREPARE INPUTS TO COLLECTION PLAN	INPUTS TO COLLECTION PLAN
BACKLOG AND BACKLOG PROJECTION (B.1.3.1)	B.1.1.3	PLAN ALLOCATION OF II RESOURCES	TASKING PLAN
STANDARD OPERATING PROCEDURES FIELD MANUALS HANDBOOKS (B.1.3.2.1)	B.1.1.4	ESTABLISH WORK BREAKDOWN STRUCTURES	WORK BREAKDOWN STRUCTURE
	B.1.1.5	ESTABLISH VOCAL OPERATING PROCEDURES	OPERATING PROCEDURES
	B.1.1.6	ESTABLISH MONITORING POLICY	MONITORING POLICY
NATIONAL/TACTICAL PRIORITIES	B.1.1.7	ESTABLISH PRIORITY POLICY	PRIORITY POLICY
STANDARD REPORTING PROCEDURES	B.1.1.8	ESTABLISH REPORTING POLICY	REPORTING POLICY
COMMUNITY STANDARDS	B.1.1.9	ESTABLISH PRODUCT STANDARDS	PRODUCT STANDARDS
	B.1.1.10	ESTABLISH II SKILL DEVELOPMENT REQUIREMENTS	UNIT TRAINING PLAN

* indicates expansion of function in following pages

Work breakdown Structure. In order to utilize specialties and available skill levels. A typical facility will have branches organized by geographic area, technical specialty, target type, imagery source, or administrative function.

Operating Procedures. Procedures for conduct of imagery interpretation processes are derivatives of procedures from handbooks, field manuals, equipment operating manuals, or standard operating procedures. In most cases, these procedures are adapted to the particular needs of a facility and its production operations. Formalized operating procedures are of more importance for training than for day-to-day production operations. Units conduct their training for processes peculiar to that facility.

Monitoring. Policies for monitoring and evaluating production processes aim at outgoing product quality and timeliness. Branch and senior level analysts are assigned to review product content and quality. Policies are established to ensure consistency in producing quality. Timeliness of products is monitored by estimating production time and maintaining regular status checking of progress and analyst workload.

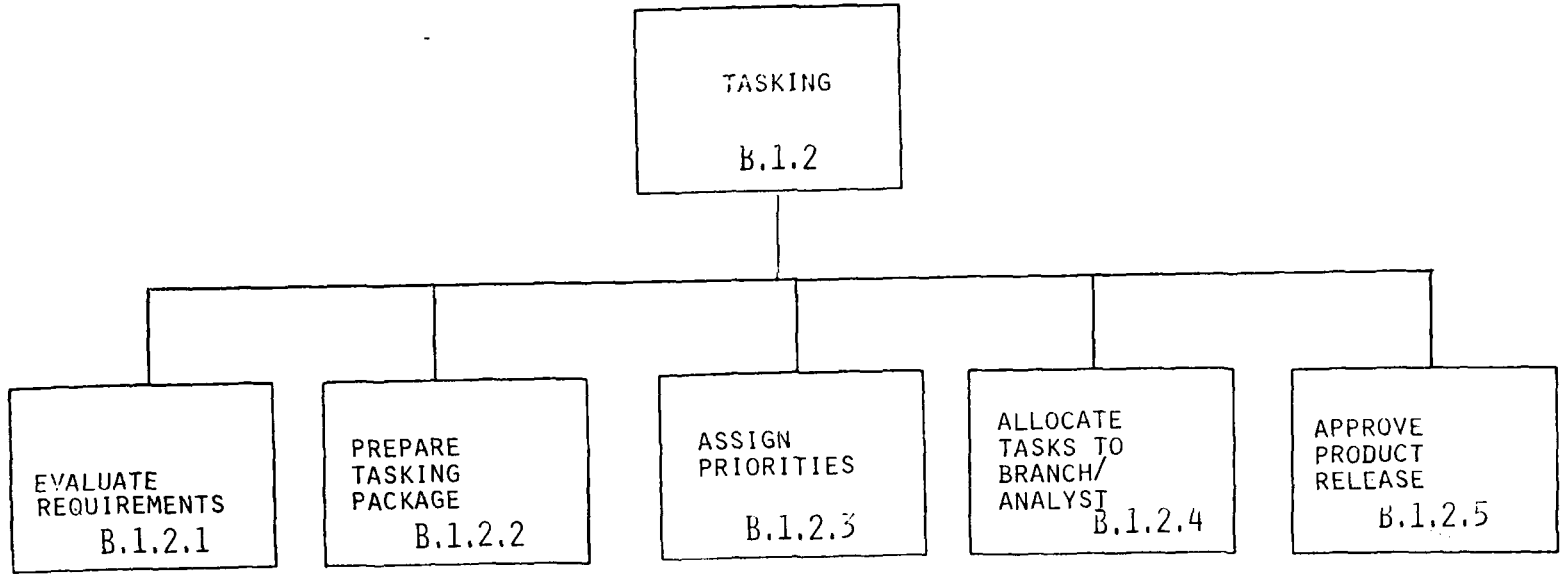
Priority Policy. Priority policies aid the facility in handling a mixture of imagery interpretation requirements with varying timeliness constraints. Priorities are adjusted when necessary to meet product suspense times.

Reporting Policy. Policies are established for the type of reporting vehicle to be used, classification of content, and distribution. Policy provides general guidelines, each report being evaluated individually on its own merit under the particular circumstances.

Product Standards. Product standards vary with respect to allowable production time, priority of requirement, extent of distribution, and resources available for production. A product may be a typeset and printed report with professional graphics, a reproduced photograph with attached notes, a record message, or an informal teletype or telephone response to a specific user.

II Skill Development Planning. In order to accomplish the IMINT production with which it is tasked, an II facility is assigned a complement of personnel who have the requisite levels of skill to operate IMINT products that meet the standards for the particular type of facility mission. The II facility staff composition may include personnel with formal training only at skill levels 1 and 2 and rotating personnel with no experience in the local mission. Some positions in the II facility may be unfilled. The II facility has the responsibility of providing unit training to adapt its available staff to the local mission and to general Army standards for the II MOS.

General standards are set by the Department of the Army in terms of the Skill Qualification Test (SQT) for promotion to higher rank in the II specialty area. Requirements for advancing in the II's analyst's specialty area may require a broader range of skills than normally needed for day-to-day tactical unit operations. Unit training must be broad in scope to insure the individual IIA's development for future mission requirements. The II facility management must plan the use of time between active missions for skill development via exercises, special training, cooperation with analysts in other technical areas, expanding the knowledge base of geographic or cultural features and conducting basic intelligence research. Although much of the responsibility for skill development rests on the individual analyst's own initiative, management must encourage this endeavor and allocate time and resources to support those activities as a normal function of the facility operation.


TASKING
B.1.2
EVALUATE REQUIREMENTS
B.1.2.1
PREPARE TASKING PACKAGE
B.1.2.2
ASSIGN PRIORITIES
B.1.2.3
ALLOCATE TASKS TO BRANCH/ ANALYST
B.1.2.4
APPROVE PRODUCT RELEASE
B.1.2.5

B.1.2 Tasking

The function of the tasking process is to delegate processing tasks to individual II analysts, management, and support personnel as the II facility develops its workload. Production planning establishes the general work breakdown structure and responsibilities of individuals but workload may vary as a function of time. The product goals for the facility are established by the II mission.

The tasking process is a complex decision-making activity, because limited personnel resources must be allocated to produce multiple products with limited varying timeliness requirements. The personnel limitations are not just in numbers, but in skill levels and prior experience with the target type or geographic area. As a result, the tasking activity is one of balancing requirements and production priorities against capabilities. In order to make the most efficient use of available resources, tasking is performed under the following general guidelines.

(1) time-sensitive requirements are addressed first;

(2) organization of tasking into geographic or target-oriented branches to make maximum use of analyst prior knowledge;

(3) rating of interpretation tasks by skill level requirements so that appropriate skill levels can be used whenever possible;

(4) division or organization to provide special support groups not requiring II skills;

(5) time variant priority scheme which allows periodic production tasks to gain priority as their suspense date nears;

B.1.2 TASKING

INPUTS	PROCESS		OUTPUTS
REQUIREMENTS II MISSION (B.1.1.1)	B.1.2.1	EVALUATE REQUIREMENTS	
	B.1.2.1.1	REVIEW REQUIREMENTS	
	B.1.2.1.2	ACCEPT REQUIREMENTS IF THEY ARE WITHIN FACILITY MISSION	
	B.1.2.2	PREPARE TASKING PACKAGE	
WORKLOAD ESTIMATE (B.1.3.1)	B.1.2.2.1	REQUEST EVALUATION OF PRODUCTION LOAD TO SATISFY REQUIREMENTS	
	B.1.2.2.2	INITIATE REQUEST FOR ADDITIONAL RESOURCES IF REQUIRED	REQUEST FOR ADDITIONAL RESOURCES (B.1.1.5)
	B.1.2.2.3	PREPARE TASKING PACKAGE	
PRIORITY POLICY (B.1.1.7)	B.1.2.3	ASSIGN PRIORITIES	
	B.1.2.3.1	ASSIGN PRIORITIES TO NEW TASKS	
TASK PROGRESS (B.1.3.1.1)	B.1.2.3.2	REASSIGN PRIORITIES IF NEEDED	
TASKING PLAN (B.1.1.3)	B.1.2.4	ALLOCATE TASKS TO BRANCH/ANALYST	TASKING PACKAGE (B.2, B.1.3.1)
WORKBREAKDOWN STRUCTURE (B.1.1.4)			
PRODUCT REVIEW EVALUATION (B.1.3.4)	B.1.2.5	APPROVE PRODUCT RELEASE	
	B.1.2.5.1	APPROVE RELEASE OF REVIEW PRODUCTS	REPORT RELEASE APPROVAL (B.2.2)
	B.1.2.5.2	ASSIGN REWORK	REWORK TASKING (B.2)
	B.1.2.5.3	ASSIGN FOLLOW-UP TASKS	FOLLOW-UP TASKING (B.2)

* indicates expansion of function in following pages

(6) monitoring of production time for previous products and estimating production time for new work allows management to control total workload of the facility. The tasking manager can refer to these workload estimates in deciding whether new requirements can be accepted or in initiating requests for additional resources;

(7) using non-peak production periods for pre-mission preparation, training, knowledge base development, or other support tasks;

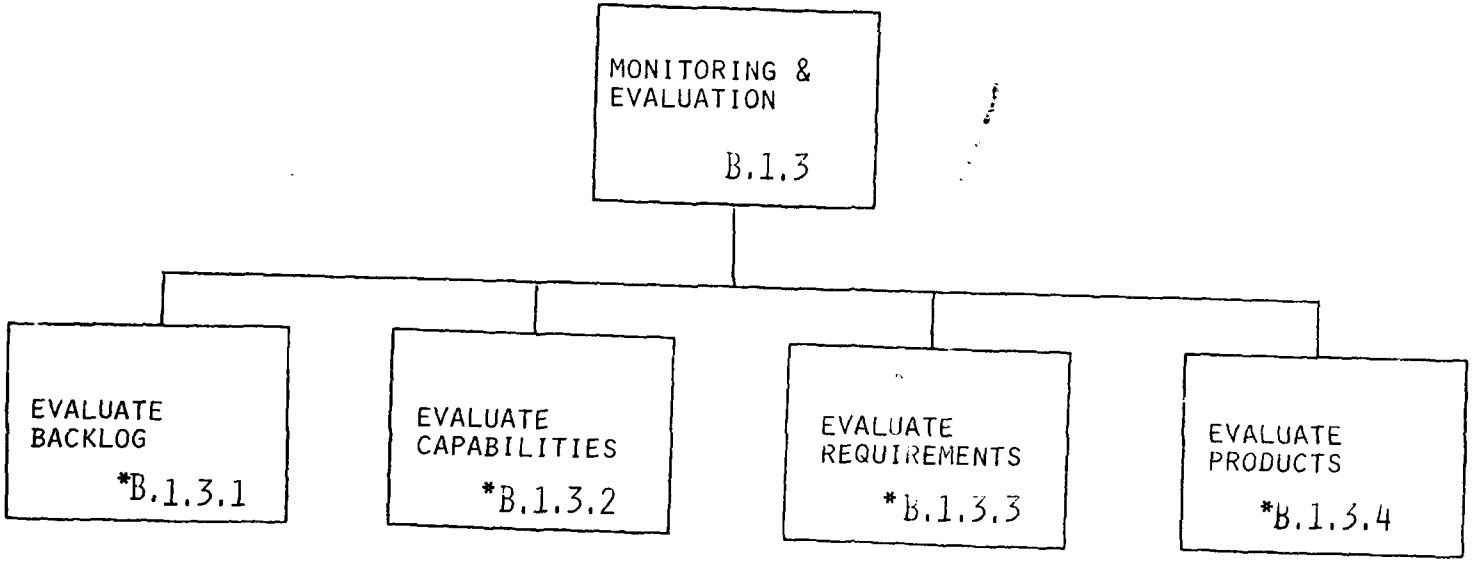
(8) informal technical assistance among analysts within the facility.

The actual control of tasking is a combination of 1) established work breakdown by branches within the II facility and specialties of analysts, 2) directed tasking in response to new requirements and 3) allocation of time for tasks.

Assigned Targets. An II may have continuing responsibilities for surveillance in a particular area, or for monitoring particular targets. Tasking is automatic whenever the area or target is covered. Continuity in target following is an essential factor in the cognitive capabilities required for unusualness analysis change detection, and identification processes (B.2.1.4.6). Continuity in following target types or a geographic area allows the II to build a data base of related collateral materials and a broader knowledge base of the technical or cultural/geographic area.

Direct Support Tasking. Army commands or other users with direct tasking authority may levy special case requirements. These requirements are evaluated and given priorities; estimates of workload are generated; and tasking assignements are made within the facility.

Management and Support Activity Tasking. In addition to imagery interpretation tasks, management activities and support activities must also be explicitly tasked. The division of labor within the II facility is designed for efficient use of resources but correspondingly creates a larger organization to be managed with additional branches to be tasked. Supporting activities such as skill development and collateral material collection are more heavily tasked during non-peak production periods.



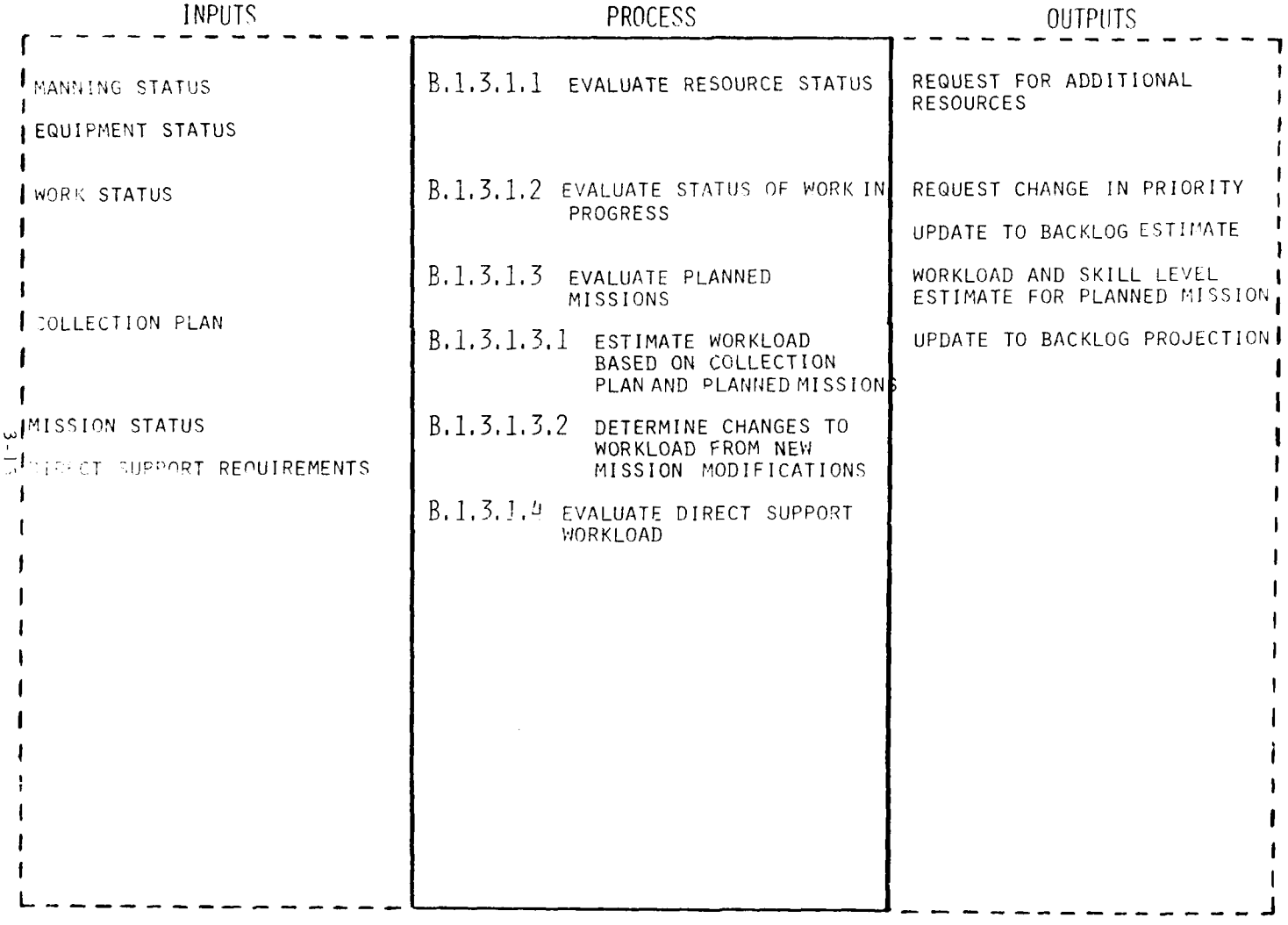
*INDICATES EXPANSION OF DETAIL IN FOLLOWING PAGES

B.1.3 Monitoring and Evaluation

Monitoring of product quality and processing status provides feedback information to the IMINT production manager for planning and tasking. Monitoring and evaluation also provides feedback to the II analyst in terms of his performance and time available to complete his task. IMINT production overall is a highly adaptive process that can trade product timeliness against product quality.

Monitoring and evaluation activities are functionally oriented toward backlog, capabilities, requirements, and products. These four areas are detailed in hierarchical INPUT-PROCESS-OUTPUT (HIPO) in order to show the flow of information necessary to manage the II production process.

B.1.3.1 EVALUATE BACKLOG



* indicates expansion of function in following pages

B.1.3.1 Evaluate Backlog

The II facility, whether in a tactical environment or deployed at the national strategic level, will be subject to a cyclically varying time pressure for production output. It is essential that the II facility manager monitor not only the work in progress but the workload that will accrue from planned missions and regular reporting requirements. The priority scheduling system allows the II facility manager to exploit the cyclical nature of collection missions to produce periodic reports or basic intelligence products when there is a lull in mission activity. It is the responsibility of the monitoring function to recognize when a task is behind schedule and request an adjustment in priority to ensure completion of the task.

The backlog projection provides the II facility manager with the information necessary in deciding if he has sufficient resources to support the collection plan. If a significant difference exists between the collection plan and the II facility capabilities, coordination will be initiated to resolve the difference.

B.1.3.2 EVALUATE CAPABILITIES

INPUTS	PROCESS		OUTPUTS
STANDARD OPERATING PROCEDURES	B.1.3.2.1	EVALUATE EQUIPMENT AND PROCEDURES	RECOMMENDED CHANGES TO PROCEDURES
MANNING STATUS	B.1.3.2.2	EVALUATE STAFF CAPABILITIES	EFFICIENCY RATING
COLLECTION PLAN OPERATING PLAN FRAG ORDERS COLLATERAL MATERIAL	B.1.3.2.3	EVALUATE COLLECTION CAPABILITIES	RECOMMENDED INPUTS TO COLLECTION PLAN
		- MISSIONS AVAILABLE	PRE-MISSION BRIEFINGS
		- SENSOR SYSTEM CAPABILITIES	
		- WEATHER	
		- ENEMY DEFENSE CONSIDERATIONS	
		- CAMOUFLAGE AND DECEPTION	
		- ALL SOURCE INTELLIGENCE RESOURCES	
		- IMAGERY QUALITY OF PREVIOUS MISSIONS	
SUPPORT ACTIVITY STATUS	B.1.3.2.4	EVALUATE SUPPORT CAPABILITIES	RECOMMENDATIONS FOR CHANGES TO SUPPORT ACTIVITY TASKING

* indicates expansion of function in following pages

B.1.3.2 Evaluate Capabilities

The II facility is able to adapt to new operating environments and changing requirements by continual evaluation of its own capabilities for production. Capabilities are of concern in the areas of procedures and equipment, staff skill levels and knowledge base, imagery, and support capabilities. The following paragraphs describe the processes shown in the associated chart for the evaluation activity.

B.1.3.2.1 Evaluate Equipment and Procedures

Procedures for interpretation, equipment operation, and report preparation are based initially on standard operating procedures from handbooks and field manuals. These procedures need regular evaluation and updating to reflect new techniques and peculiarities of the changing operating environment. Procedures must be appropriate within mission and time constraints.

B.1.3.2.2 Evaluate Staff Capabilities

II analysts are the most critical component of the production process. II skills represent a technology which is developed through training, working experience, technical exchange with peers, and knowledge base development in specialty areas. Imagery interpretation is such that evaluating an II process is virtually impossible without redoing the entire process for comparison. Effective utilization of a staff with varying skill levels is achieved by organizing work in terms of skill level requirements. Apprentice IIAs may work with an experienced analyst and teams of II analysts may be assigned to complex tasks. In the majority of interpretation activities, the IIA will have sole responsibility for his performance. The success of this method depends on analysts initiating requests for assistance when encountering difficult problems or targets which are unfamiliar to them, and analysts of all skill levels are encouraged to confer with peers. Individual IIAs are frequently identified with specific IMINT reports. This personal identification is an aid to users who may request additional data or clarification, and is a means of giving professional recognition to the individual. Monitoring and support of staff development is recognized as an effective means of upgrading the capabilities of the II facility. Personal attention to skill development needed for promotion and career advancement is a major factor in optimizing production capability. The high technical proficiency gained by Army trained II analysts is readily marketable as a civilian skill. This factor combined with limited career opportunities in the Army II skill specialty frequently results in high staff turnover rates.

B.1.3.2.3 Evaluate Collection Capabilities

Because the II facility is partially dependent on its collection sources for its product impact, there must be feedback mechanisms between the II facility and the collection systems. To support this information feedback channel, the II facility engages in a variety of collection capability evaluations aimed at maximizing exploitation of these sources. The most important feedback mechanism appears to be the informal coordination which takes place at the analyst level rather than the management level.

Mutual understanding of capabilities is essential in maximizing the exploitation of imagery. Interpreters have flown reconnaissance missions in order to appreciate the problems of the reconnaissance pilot. Pilots in turn may work with interpreters in evaluating the success of the collection missions and gaining feedback on how improvements can be made.

B.1.3.2.4 Evaluate Support Capabilities

Supporting activities may be as vital as interpretation processes to the production capabilities of the II facility. These activities (described in B.2.3) must be tasked and monitored. Where production conflicts occur in support activities, priorities are assigned.

B.1.3.3 EVALUATE REQUIREMENTS

INPUTS	PROCESS		OUTPUTS
II FACILITY MISSION REQUIREMENTS	B.1.3.3.1	EVALUATE REQUIREMENTS RELATIVE TO II FACILITY MISSION	ACCEPT OR REQUEST CHANGES IN REQUIREMENTS
HISTORY OF COVERAGE (B.2.3.3)	B.1.3.3.2.	DETERMINE IF EXISTING IMAGERY CAN BE USED	IDENTIFIED IMAGERY FOR INTERPRETATION TASK (B.1.2.2)
MISSION PLANS	B.1.3.3.3	DETERMINE IF NEW COLLECTION MISSIONS ARE REQUIRED	RECOMMENDED INPUTS TO COLLECTION PLAN

* indicates expansion of function in following pages

B.1.3.3 Evaluate Requirements

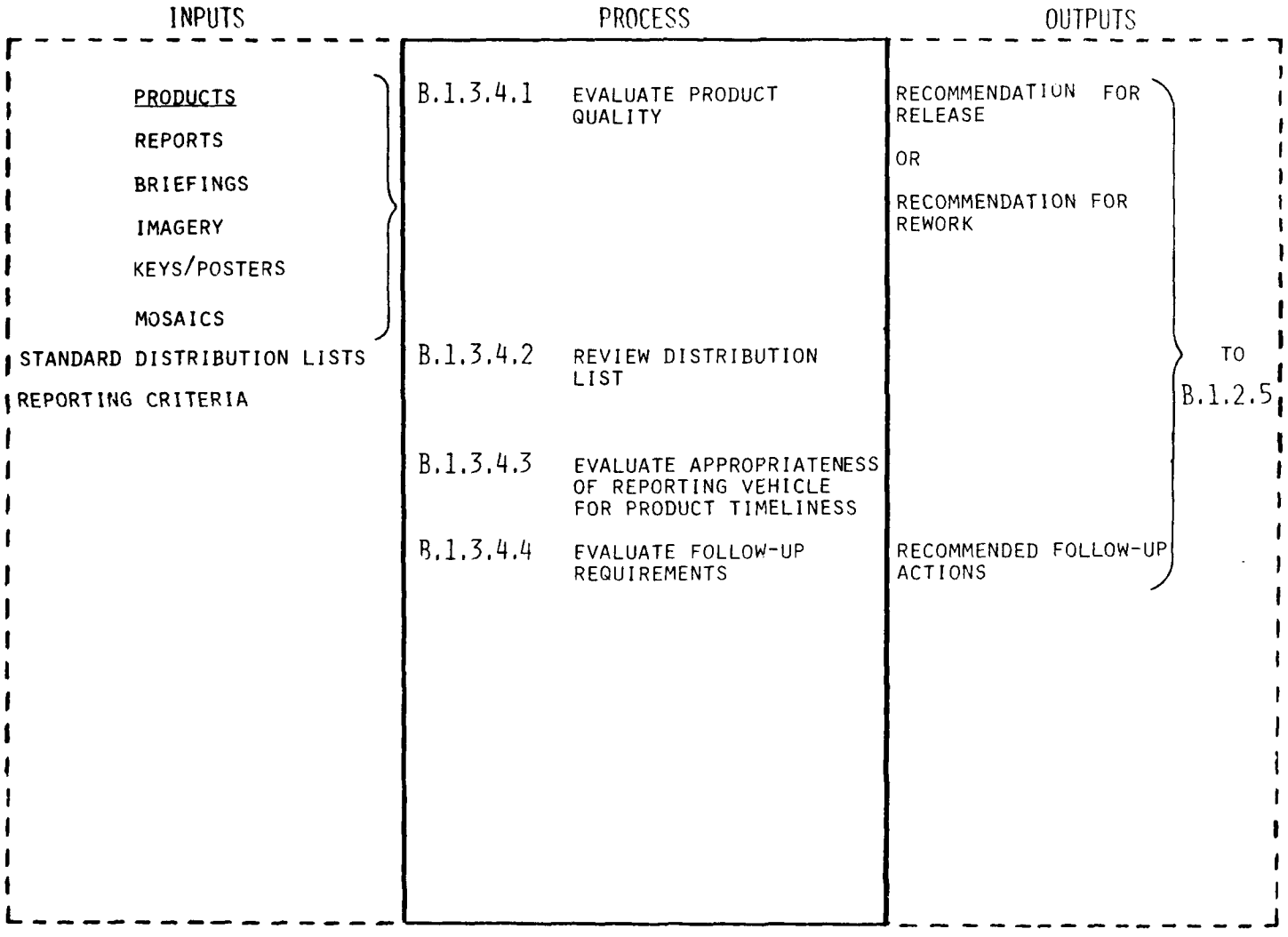
Requirements for imagery intelligence are diverse and may be received from a number of different tasking agencies. Requirements may be categorized into one of three general types: standing, direct support, or basic intelligence.

Standing Requirements. Imagery interpretation requirements that are relatively fixed over time are referred to as standing requirements. A standing requirement may require following of particular target types or surveillance of particular areas of interest. Reporting requirements may be on a periodic schedule, reported each time coverage occurs, or on an unusualness basis. Standing requirements are usually reflected in the facility mission statement. Standing requirements are evaluated on the basis of their impact on processing load and collection requirements.

Direct Support. The II facility generally has in its mission the requirement to provide direct support to various authorized tasking agencies. Direct support requirements involve all three phases of interpretation production and vary in priority and complexity. Direct support requirements must be evaluated carefully from a mission standpoint so that overlapping interpretation tasks do not occur between facilities.

Basic intelligence. Imagery interpretation is utilized to produce a wide variety of basic intelligence such as order of battle. The II facility may be tasked with providing inputs to basic intelligence files or preparing Basic Imagery Interpretation Reports (BIIRs). Characteristically, basic intelligence tasks are more complex, take longer to process, and involve extensive use of all-source intelligence materials.

B.1.3.4 EVALUATE PRODUCTS

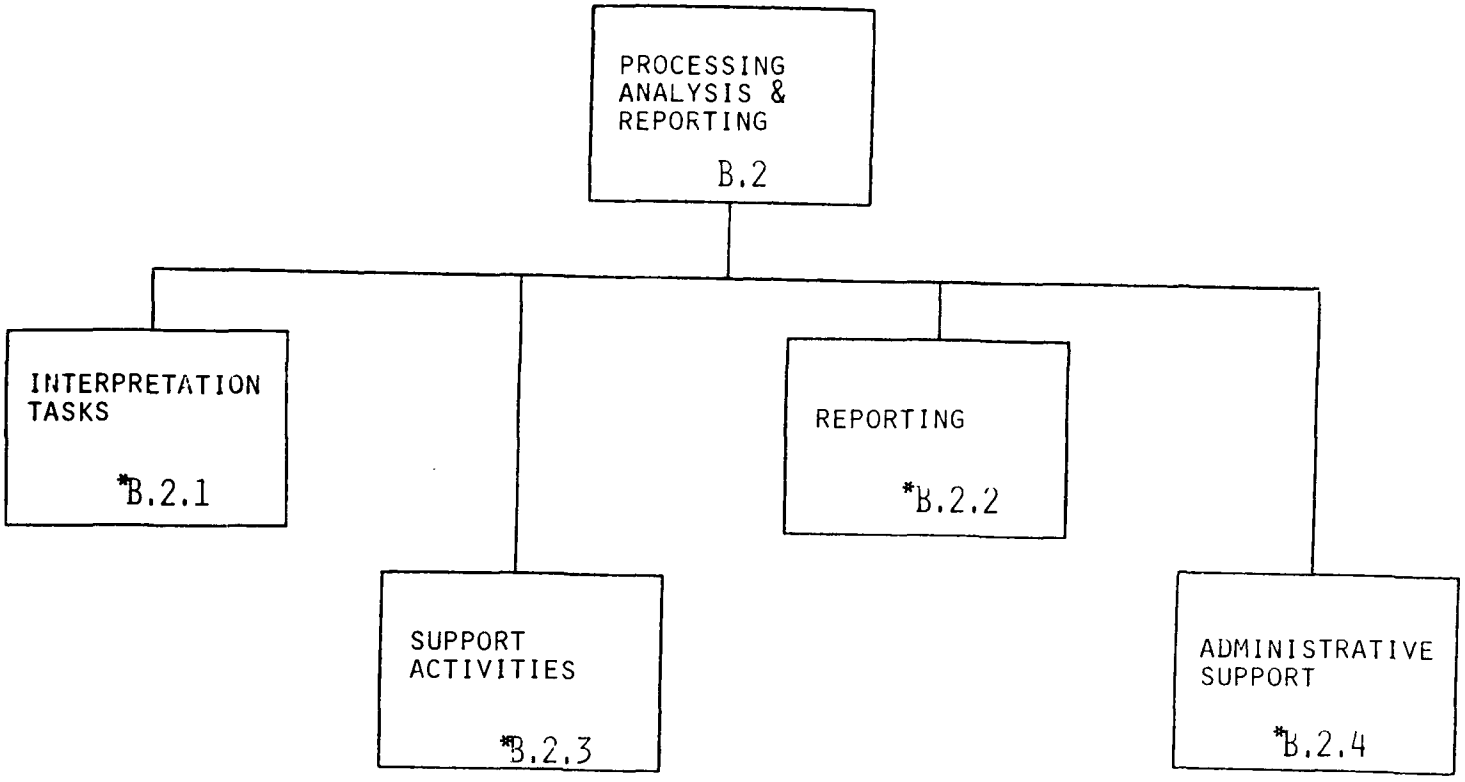


* indicates expansion of function in following pages

B.1.3.4 Evaluate Products

All products are reviewed prior to release for distribution with the exception of informal technical exchange between analysts. Products are reviewed for grammatical and technical quality, correctness of distribution, classification level, and reporting vehicle. In some cases reviewers may be able to also look at the source imagery. This is not practical in those cases such as search or complex studies involving a large amount of imagery. Review tasks are normally handled by senior analysts, branch chiefs, or a technical area review committee. Quality standards, report formats, reporting policy, and standard distribution lists are used as references in the product review process.

Certain types of products require follow-up actions. Follow-up reports may be required to expand the detail in an immediate report; or, collection plan modifications might be appropriate as a consequence of a product's content.

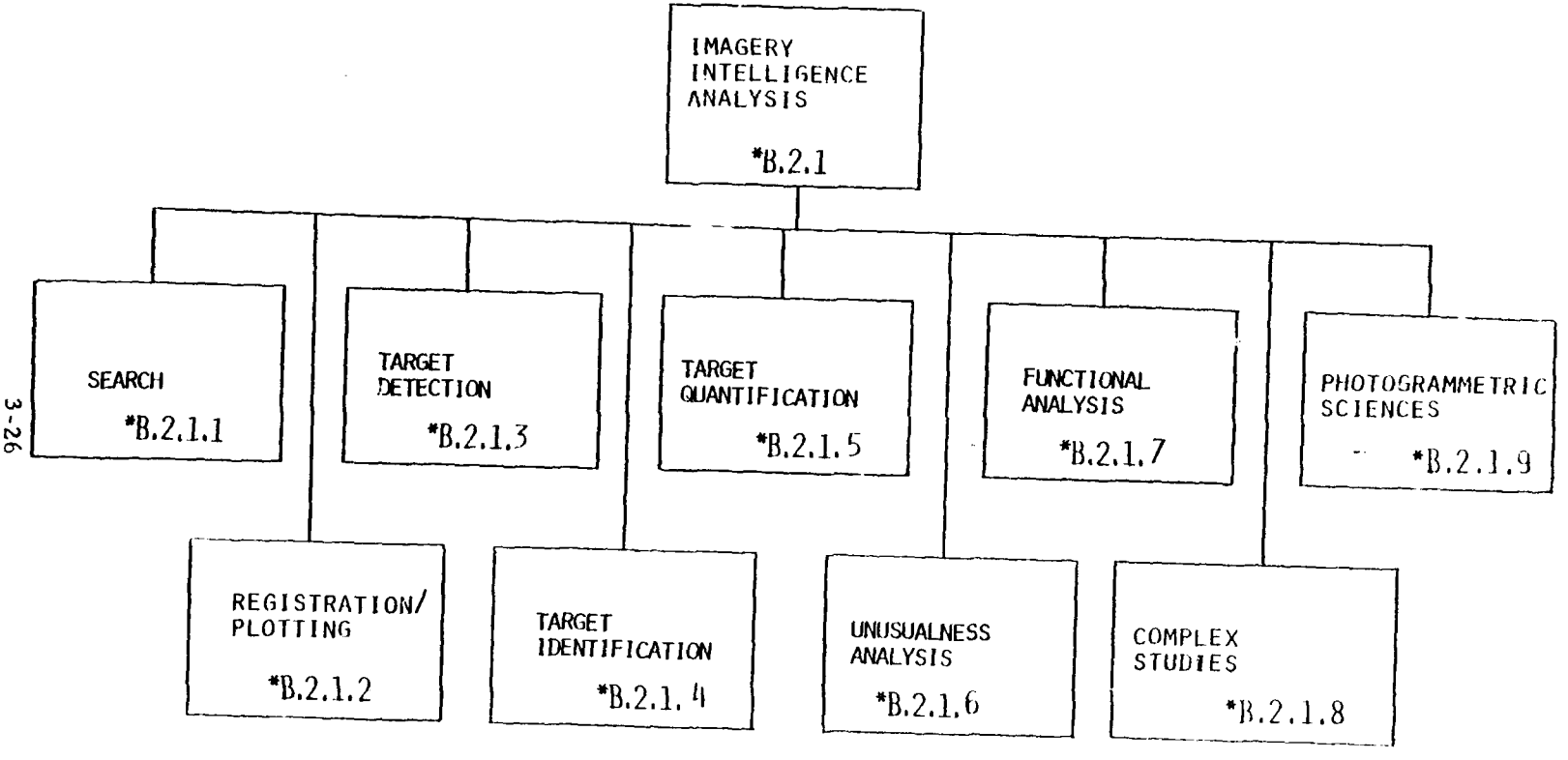


*INDICATES EXPANSION OF DETAIL IN FOLLOWING PAGES

B.2. Imagery Intelligence Processing, Analysis, and Reporting

The imagery intelligence production activities described in part B.1 of the model deal with planning, tasking, and evaluation of the product. Although the impact of those activities upon the analytical and reporting activities discussed here in part B.2 is substantial, the latter activities are of primary interest in this model, since specification of the analytical, cognitive and judgmental content of the activities described below is fundamental to the development of a cognitive model of intelligence analysis (see Section 1.1). In fact, the title of this part is selected to facilitate comparision with analogous SIGINT activities, referred to as Processing, Analysis, and Reporting (PAR) in the model document [Ref. 8] used for a preliminary investigation of SIGINT activities involving cognitive processing.

The Processing, Analysis, and Reporting activities of an imagery intelligence production facility are organized along lines of skills and function, and are further segmented in terms of product suspense times that allow the IMINT production process to adapt to different loading conditions and operating environments. The major areas of activity are analysis, reporting, support activities, and administrative functions. These areas of activity are readily observable in larger II facilities and less distinct in smaller facilities where staff functions are more general. These subdivisions of activity are important from a tasking point of view, because the level of activity shifts dramatically between these areas over time. Short term variations will occur on an hourly, daily, and weekly cycle during normal operations. Larger shifts in activity will occur as the facility experiences mission changes due to the dynamics of the international situation, with concomitant changes in intelligence collection and tasking.



*INDICATES EXPANSION OF DETAIL IN FOLLOWING PAGES

B.2.1 Imagery Intelligence Analysis

As an introduction to the analysis of imagery, several issues which are generic to the variety of analytical activities shown on the facing page merit discussion. These include the concept of imagery analysis as opposed to 'bean counting', and the constraints imposed on the analytical process by time, the quality of the imagery, and the knowledge and experience of the IIA assigned to a particular task. In addition, the chart format for describing the analytical activities is described.

The Imagery Interpretation Process

The imagery interpretation process essentially consists of identification of physical objects, such as equipment, in the context of its environment, which includes associations between such equipment and the function of the military unit that uses it, leading to identification of such a unit -- e.g., engineering equipment indicates the presence of an engineering unit, possibly a headquarters. In addition, characteristics or conditions of interest (e.g., the modification of terrain by excavation) should be identified; -- and to the extent possible -- activities, such as bridge construction, river crossing training, which may reveal the intent of the enemy. These sets of objects, conditions, and activities are of interest because they have military significance: in the broad sense of the word, they are potential targets for military exploitation. Use of the term 'target' in the following discussion is intended to convey this broader meaning, rather than a particular installation in a targets file as a specific target, since such an installation in fact may contain a large variety of objects and equipments which are targets in themselves.

As mentioned above, the imagery interpretation activity involves to some extent the association of objects with other objects (e.g., a type of support equipment with a particular type of missile), the association of (equipment) objects with a known T&E configuration of equipment (e.g., six 120 mm mortars indicates a battery, seven indicates two batteries), the association of equipment with an organizational unit of a particular size (e.g., one mortar battery may indicate a motorized rifle battalion while two could indicate the presence of a motorized rifle regiment), the association of equipment with function, and consequently, with a degree of threat (e.g., a SAM on a launcher is ready to fire, a SAM on a transporter is not). All of these associational processes require deductive reasoning, and distinguish the function of imagery interpretation from simple 'bean counting'.

The Time Factor

Imagery interpretation analysts are aware of these inferential processes and can apply them to the categories of targets within their competence. However, the depth of analysis is often severely limited by the length of time available to perform the analysis. An IIA preparing Hot Photo Interpretation Reports (HOTPHOTOREPs) in a Tactical Imagery Interpretation Facility (TIIF) may have only a few minutes to actually analyze imagery, since substantial segments of the time period from engine shutdown to report filing deadline must be devoted to film processing and to registering, plotting, and validating the mission trace. Time is thus a critical limiting factor in the analysis which provides the basis for a HOTPHOTOREP. This limitation is compensated by the additional analysis which optionally follows, resulting in a supplement to the original HOTPHOTOREP within the next hour. The problem is that such supplements have lower priorities than the HOTREPs themselves, so should additional missions continue to arrive, no further analysis on an earlier mission already covered by a HOTREP is possible.

Although the above scenario is tactically oriented, the inverse relationship of time and depth of analysis also exists on the strategic level. In fact, the three temporally defined phases of IMINT processing described in Section 2.1.3 are applicable to both tactical and strategic environments. Many IIAs on both levels are concerned with the preeminence of the time factor over analytical performance, even in the third phase, basic study context. Others seem to have accepted time constraints as an occupational parameter, and do not appear to be unduly concerned with the possibility of missed information.

The Quality of Imagery

An important aspect of IMINT analysis is that imagery utilized by any facility -- whether a local TIIF or a national imagery interpretation resource -- will not have consistent quality. Sensor and platform capabilities, range, height, and atmospheric conditions all contribute to wide variations in the quality of imagery. Each IIA essentially evaluates imagery from the perspective of his own processing task, in order to determine the extent to which the image can be exploited in the context of that task. For example, a 50% cloud coverage on an area would reduce the effectiveness of an imagery interpretation search function by 50%, but may or may not affect particular targets within the imagery frame. For oblique imagery, near objects would have better resolution and could thus be more accurately identified than remotely located objects. Haze produced from various causes might obstruct identification of certain objects, but not others.

For these reasons, an IIA cannot usually anticipate the quality of imagery related to his interpretation tasks until he is actually viewing a particular segment of imagery. Productivity is not affected by this lack of prior evaluation in tasks which require search of previous imagery files. Methods are currently being established for evaluating imagery products across the broad range of imagery interpretation applications. In particular, a national standard, called the National Imagery Interpretability Rating System (NIIRS), has recently been implemented on the national level; this standard will presumably be adopted in some form on all imagery interpretation echelons in the near future.

Knowledge and Experience of the Individual IIA

An additional factor in IMINT analysis is the set of experiences, background, and knowledge that an individual IIA brings to bear on a particular analytical task. A new IIA who has previously served in the infantry or artillery has an advantage in identifying equipment and in knowing where to look for it. Such a person may also be able to infer enemy intent from the disposition of equipment and personnel, thus providing an in depth analysis of an enemy situation that would be very difficult for a novice IIA with a civilian background to duplicate. Similarly, an IIA with experience in a strategic level II position in an active mission will have acquired a detailed background in a specific area relevant to that mission, which may or may not be directly exploitable in a tactical environment. For example, equipment relevant to strategic missions does not generally include US or NATO equipment, which is used in tactical exercises. Thus equipment learned in detail in the course of a strategic assignment may not be directly relevant to a tactical assignment; however, the methodological knowledge and experience of analyzing equipment of any kind is an important part of the knowledge base of an IIA, and gives the IIA with strategic experience an advantage in performing tactical or strategic imagery analysis. The IIA in a tactical assignment is a generalist, prepared to deal with any imagery analysis task. Basic Army IIA training therefore includes course blocks dealing with targets which are not normally Army responsibilities, such as ports, harbors, inland waterways, and strategic industries. On the other hand, strategic level assignments tend to be more specific, requiring an IIA to become an expert in a particular set of targets or types of equipment.

B.2.1.3 TARGET DETECTION

INPUTS	PROCESSES		OUTPUTS
SPECIFIC REQUESTS FOR INFORMATION (SRI GENERAL MISSION REQUIREMENTS INTERPRETATION PRIORITIES	B.2.1.3.1	OBTAIN RELEVANT IMAGERY	IMAGERY
	B.2.1.3.2	OBTAIN COMPARATIVE COVER IMAGERY	
	B.2.1.3.3	OBTAIN RELEVANT DEBRIEFING/MISSION REPORTS	DEBRIEFING/ TO MISSION REPORTS B.2.1.3.5
	B.2.1.3.4	RETRIEVE RELEVANT MAPS/OVERLAYS	MAPS/OVERLAYS
	*B.2.1.3.5	PERFORM TARGET DETECTION PROCESS	
	B.2.1. .6	GENERATE DATA FOR REPORTS/BRIEFINGS	REPORT DATA (TO B.2.2.

Figure 3.1 A

B.2.1.3.5 TARGET DETECTION PROCESS

INPUTS	SUBPROCESSES		OUTPUTS
IMAGERY (B.2.1.3.1) DEBRIEFING/MISSION REPORTS (B.2.1.3.3) MAPS/OVERLAYS (B.2.1.3.4)	B.2.1.3.5.1	DISPLAY INPUT IMAGERY	
	B.2.1.3.5.2	DISPLAY MAP/OVERLAY	
	B.2.1.3.5.3	SCAN IMAGERY	
	B.2.1.3.5.4	DETECT POSSIBLE TARGETS, OBJECTS OR CHARACTERISTICS OF MILITARY SIGNIFICANCE	
	B.2.1.3.5.5	DETERMINE LOCATION OF ITEMS OR CHARACTERISTICS DETECTED	
	B.2.1.3.5.6	RECORD LOCATION OF DETECTED ITEMS AND MARK FRAME FOR FURTHER ANALYSIS	RECORD OF DETECTED ITEMS (TO B.2.1.4)
	B.2.1.3.5.7	MAKE COMPARISONS WITH PAST COVERAGE OR OTHER INTELLIGENCE REPORTS	

Figure 3.1 B

* indicates expansion of function in following pages

Presentation of Analytical Activities in HIPO Charts

In the following discussion and associated charts, the set of imagery analysis activities is segmented functionally for convenience of analysis in terms of cognitive processes underlying particular functions, in line with the larger context of the cognitive model for intelligence analysis for which this II model has been constructed (see Section 1.1). An IIA in the field may in fact perform the whole range of activities at some level in the course of a typical work day. Moreover, the detection, identification, quantification, and unusualness analysis activities (B.2.1.3-6) are performed to some level in all phases of interpretation, although the more detailed analysis represented by the functions identified as B.2.1.7-9 (where B.2.1.8 includes such functions as Order of Battle, terrain, and entry zone analysis) are essentially third phase, less time sensitive, activities.

Partition of Information Handling versus Analytical Processes in Charts

The chart presentations of the majority of these activities differ from those of the preceding section in level of detail and process segmentation. The charts are more detailed and the majority are organized in terms of a segmentation into information manipulation processes versus analytical processes. As an illustration, Figure 3-1a treats information handling processes for the target detection activity, and identifies an analytical process which is expanded into subprocess descriptions in the following chart (signaled by an asterisk), shown in Figure 3-1b.

The inputs of the information handling activities are general mission requirements on the one hand, and on the other, Specific Requests for Information (SRI), and interpretation priorities driving the particular activity in a given case (for example, the the EEI at a given point in time in a particular situation). The outputs of the information handling processes -- for example, the acquisition of imagery and relevant reference materials shown by the processes labeled b.2.1.3.1-4 in Figure 3-1a -- have as outputs the given imagery and materials aligned in the output column with the associated processes. These outputs are labeled with the analytical process (B.2.1.3.5) to which they are sent, and appear as inputs to that process in Figure 3-1b, labeled with the number of the process which generated them. The outputs of the given analytical process then are sent to the next activity, B.2.1.3.4, Target Identification, and are simultaneously sent to reporting (B.2.2).

It should be remembered, as discussed in Section *.1, that all the listed processes may not occur in any given case, or may not be performed in the sequence in which they are listed. In many cases, time pressure or lack of reference materials eliminates one or more of the information acquisition steps, while many of the analytical processing steps may be performed essentially simultaneously, or omitted as irrelevant in a given case.

B.2.1.1 SEARCH

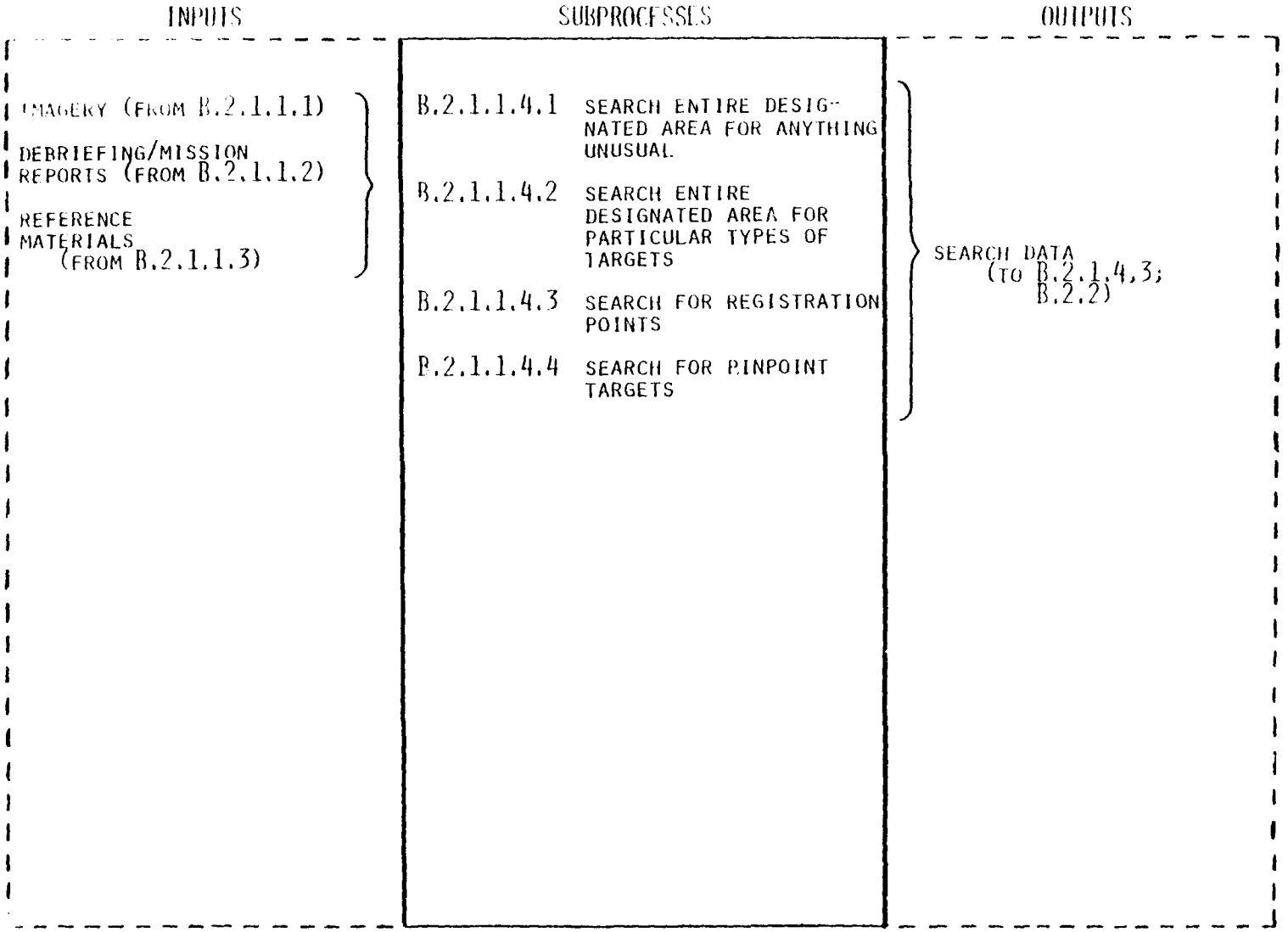
INPUTS	PROCESSES		OUTPUTS
SPECIFIC REQUESTS FOR INFORMATION (SRI)	B.2.1.1.1	OBTAIN RELEVANT IMAGERY	IMAGERY
GENERAL MISSION REQUIREMENTS	B.2.1.1.2	OBTAIN RELEVANT DEBRIEFING/ MISSION REPORTS	REPORTS
INTERPRETATION PRIORITIES	B.2.1.1.3	RETRIEVE RELEVANT REFERENCE MATERIALS/ STUDIES	REFERENCE MATERIALS
	B.2.1.1.4	PERFORM SEARCH PROCESSING	TO B.2.1.1.4
	B.2.1.1.5	GENERATE DATA FOR REPORTS/BRIEFINGS	REPORT DATA (TO B.2.2)

* indicates expansion of function in following pages

B.2.1.1 Search

The following description of the imagery analysis activity assumes two modes of search, as well as the three phases of interpretation discussed above. The two modes of search are general or 'accountable' search (as it is described on the strategic level), and specific search for selected items. General search is driven by all-inclusive mission or tasking requirements, by which a particular imagery interpretation element must account for all targets in its functional and geographic areas of responsibility, examining every square inch of film within a given period of time after receipt of imagery. Specific search, on the other hand, is driven by Specific Requests for Information (SRI), limiting the scope and objectives of the search. Both types of search are characteristic of the imagery interpretation process at the level of the tactical unit, as well as at the level on which national strategic and service-wide imagery interpretation resources operate.

B.2.1.1.4 PERFORM SEARCH PROCESSING



* indicates expansion of function in following pages

B.2.1.1.4 Perform Search Processing

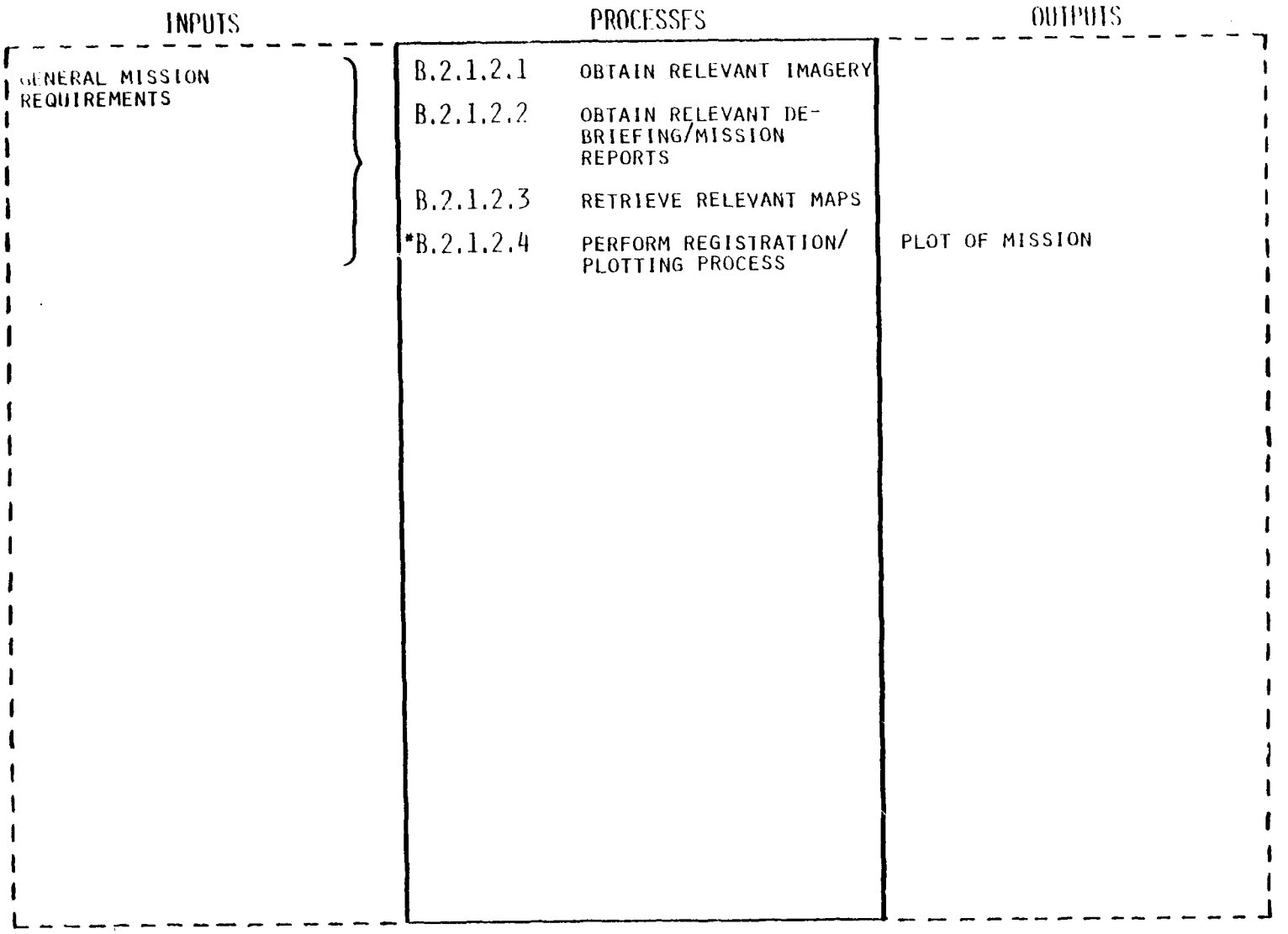
The search activity is differently practiced at the various levels of the IMINT production effort. On the level of national strategic imagery interpretation resources, search is more closely associated with unusualness analysis and change detection (see B.2.1.6 for discussion). The search activity as practiced there is a specialized form of accountable search, in which special techniques and equipment are used to simulate 'flying' over the imagery on a light table. As every square inch of the film is 'overflown', the IIA looks for unusual aspects of the terrain or known targets in the area to determine whether any changes have occurred since the last imagery was obtained. If possible changes are detected, a retrospective search of previous imagery is performed to pinpoint the time at which the change occurred by locating imagery antedating the particular unusual characteristic. Thus if an excavation for a possible missile silo is noted, comparative cover imagery will be examined to 'negate' the excavation condition: i.e., to determine the date of coverage when such a condition did not exist, in order to bracket the time frame within which the change occurred. A second aspect of accountable search involves specific checking for new targets of a particular type, assigned as a functional responsibility to an individual IIA or an IIA group.

On the level of the tactical II facility, an analogous type of search activity occurs. An example of this search related to unusualness analysis and change detection is provided by tactical image interpretation operations in Vietnam. Imagery analysis was generally segmented by geographical area and, in most cases, sufficient image interpretation capability was available to allow fairly small areas to be assigned to individual IIAs. These IIAs thus tended to become experts in their particular area of responsibility, which meant that they could easily distinguish objects and configurations associated with the Vietnamese cultural background from objects and configurations of military significance (e.g., grave mounds from weapons emplacements). In a careful search of every inch of film from each new mission flown, the experienced IIA could notice anything at all unusual (for example, possible camouflage), or immediately detect the slightest change in his area of responsibility ("I could tell if they'd moved one tree," a veteran IIA said).

A similar type of search activity associated with target detection (see B.2.1.4) is practiced in tactical units performing real time processing of imagery produced by Side-Looking Airborne Radar(SLAR), Forward-Looking Infrared (FLIR), and video devices. Also, where an aircraft was directed to photograph between coordinates rather than to photograph pinpoint targets, a detailed search of the film precedes the analytical activities of target detection, identification, etc.

In addition, the registration and plotting activity involved in tracing the route flown by a reconnaissance aircraft is also preceded by a type of search activity -- in this case, a search of the imagery for registration points required to calibrate the mission photography with the IIA's map and with the pilot's concept of the route flown in the particular mission. Similarly, a search precedes the detection and identification of pinpoint targets photographed on a particular reconnaissance mission.

B.2.1.2 REGISTRATION/PLOTTING



* indicates expansion of function in following pages

B.2.1.2 Registration/Plotting

Before an IIA can begin to detect or identify targets photographed in the course of a tactical reconnaissance mission, the strip of film which is to be analyzed must be registered with the IIA's map and a preliminary plot of the mission trace must be made. Registration involves identifying features on the film which correspond to prominent features on the map likely to endure for some period of time (i.e., terrain features, man-made features such as roads, urban areas, airfields, etc.). Once the film has been registered to the IIA's map, an approximate plot of the mission can be prepared, using code matrix data on the film as necessary to determine specific coordinates.

The first phase registration and plotting activities are extremely important in an environment where an II facility is associated with a tactical reconnaissance squadron -- for example, a collocated MIBARS detachment in a temporary deployment for the purpose of an exercise, or on permanent assignment to a tactical air base. In this environment, most imagery interpretation tasking is directed at immediate readout of aerial photographic missions, where the registration/plotting activity provides the vital parameter of location to the analytical and reporting activities that follow immediately, all three activities (as well as film processing) being accomplished usually within an hour of engine shutdown.

B.2.1.2.4 PERFORM REGISTRATION/ PLOTTING PROCESS SUBPROCESSES

INPUTS		OUTPUTS
IMAGERY (B.2.1.2.1) DEBRIEFING/MISSION REPORTS (B.2.1.2.2) MAPS (B.2.1.2.3)	B.2.1.2.4.1 LOCATE PERMANENT FEATURES ON IMAGERY B.2.1.2.4.2 ORIENT PERMANENT FEATURES ON IMAGERY TO IDENTICAL FEATURES ON MAP B.2.1.2.4.3 LOCATE STARTING POINT OF IMAGERY B.2.1.2.4.4 DETERMINE PATH COVERED BY MISSION B.2.1.2.4.5 CONVERT GEOGRAPHIC TO UTM COORDINATES	

* indicates expansion of function in following pages

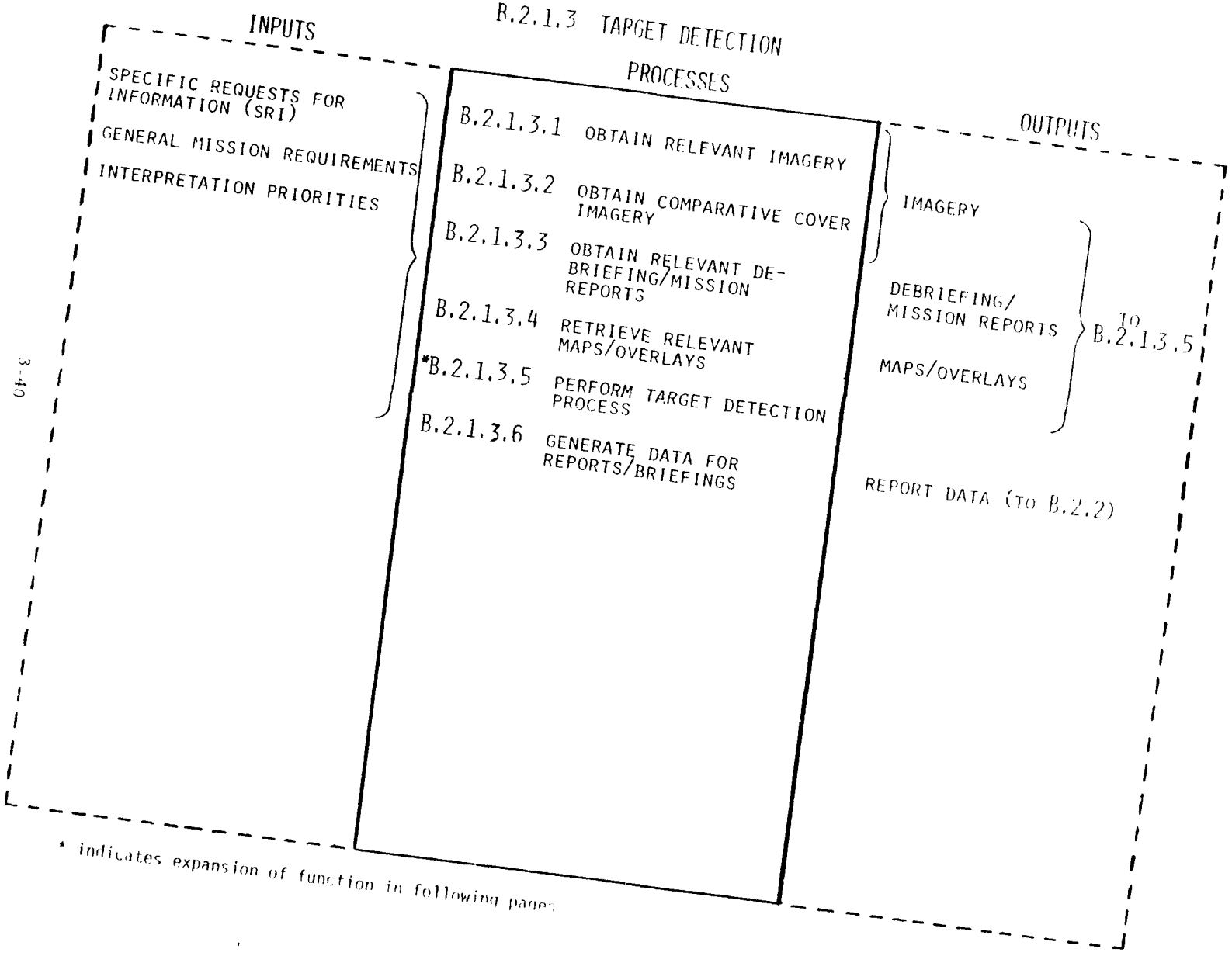
B.2.1.2.4 Perform Registration/Plotting Process

In theory, the basis for this activity is the pilot's trace of the mission flown, as well as the ARLO's debriefing and the mission report or MISREP (which, in the training exercises observed, was substantially prepared before engine shutdown, from the mission plan and inflight reports received from the pilot).

In practice, the pilot and/or navigator appear in the II facility as soon as the imagery has been developed, and the orientation of the mission imagery to the IIA's map is carried out with the active participation of pilot and/or navigator, in the interest of making the most rapid assessment of the mission for a Hot Photo Interpretation Report (HOTPHOTOREP).

The difficulty is that the reconnaissance mission may not have covered the area identified in the mission plan, nor photographed the targets in the planned sequence, nor turned the cameras on and off at the planned points. Weather, enemy fire, and other considerations may change planned coverage. The orientation/registration problem involved in plotting the mission is complicated by such factors, and the difficulty of registering the mission in terms of a map is inversely proportional to the number of salient features in the area of mission coverage. For this reason, IIA's in a MIBARs detachment have estimated that the registration and plotting of a mission occupies about 80% of the time spent in active interpretation, report preparation the next highest percent of time (around 15%), and analysis of the imagery, the smallest proportion of image interpretation time.

The plotting function is also an important second phase function, where accuracy is emphasized (see B.2.3.3). On the national resource level, the plotting function is required for first and second phase analysis of all imagery produced by airborne platforms.



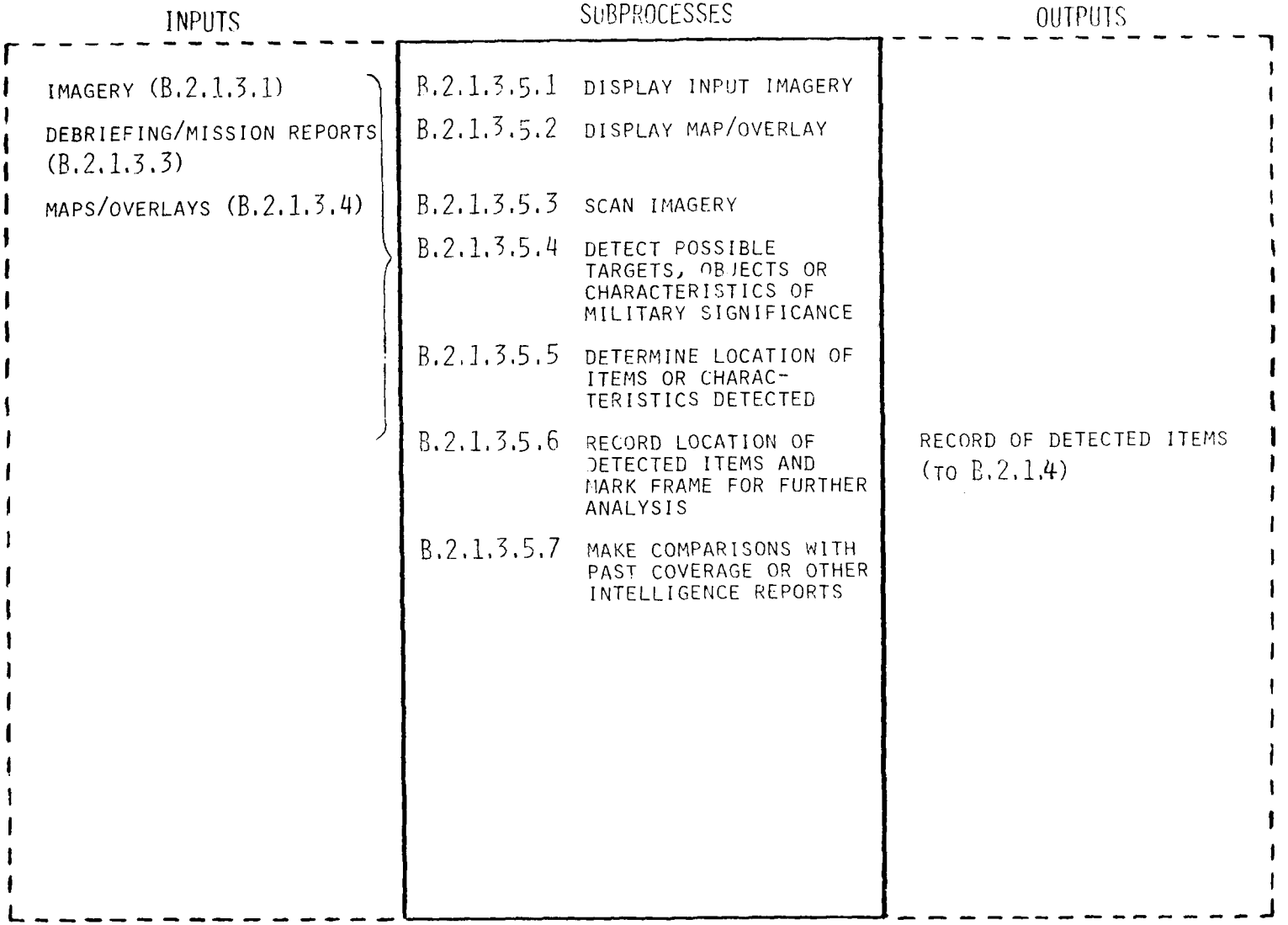
* indicates expansion of function in following page

B.2.1.3. Target Detection

Target detection is essentially the perception of a potential target, which is then validated through the identification activity (B.2.1.4). The activity of target detection includes real time imagery analysis (e.g., involving Side-Looking Airborne Radar (SLAR), Forward-Looking Infrared (FLIR), or video devices), or interpreting wet or dry film under less severe time constraints. In dynamic processing of SLAR imagery, the image interpretration activity is limited to detection of probable moving targets via the Moving Target Indicator (MTI) capability of the SLAR, as identification of the particular target as armor, personnel transports, etc., is not possible. SLAR systems -- when provided with ground-based or airborne interpreter stations to perform detection in real time -- can be exploited for quick response targeting and area activity monitoring.

In the case of SLAR interpretation then, the necessary information for target identification is not present in the medium, thus the analytical activities of detection and identification are distinct, conforming to the separation of these two activities in the model. Since the necessary information for identification is usually present in the case of infrared imagery (IR), video or film (whether real time or not), the distinction between the detection and identification activities is somewhat arbitrary, as some type of identification will usually be made simultaneously with detection. When the visual cues constituting the necessary information for identification are not present -- for example, when the quality of the imagery is low -- identification requires additional analysis involving comparative cover imagery, keys, etc., such that the detection and identification activities are functionally separate, as presented here.

B.2.1.3.5 TARGET DETECTION PROCESS



* indicates expansion of function in following pages

B.2.1.3.5 Target Detection Process

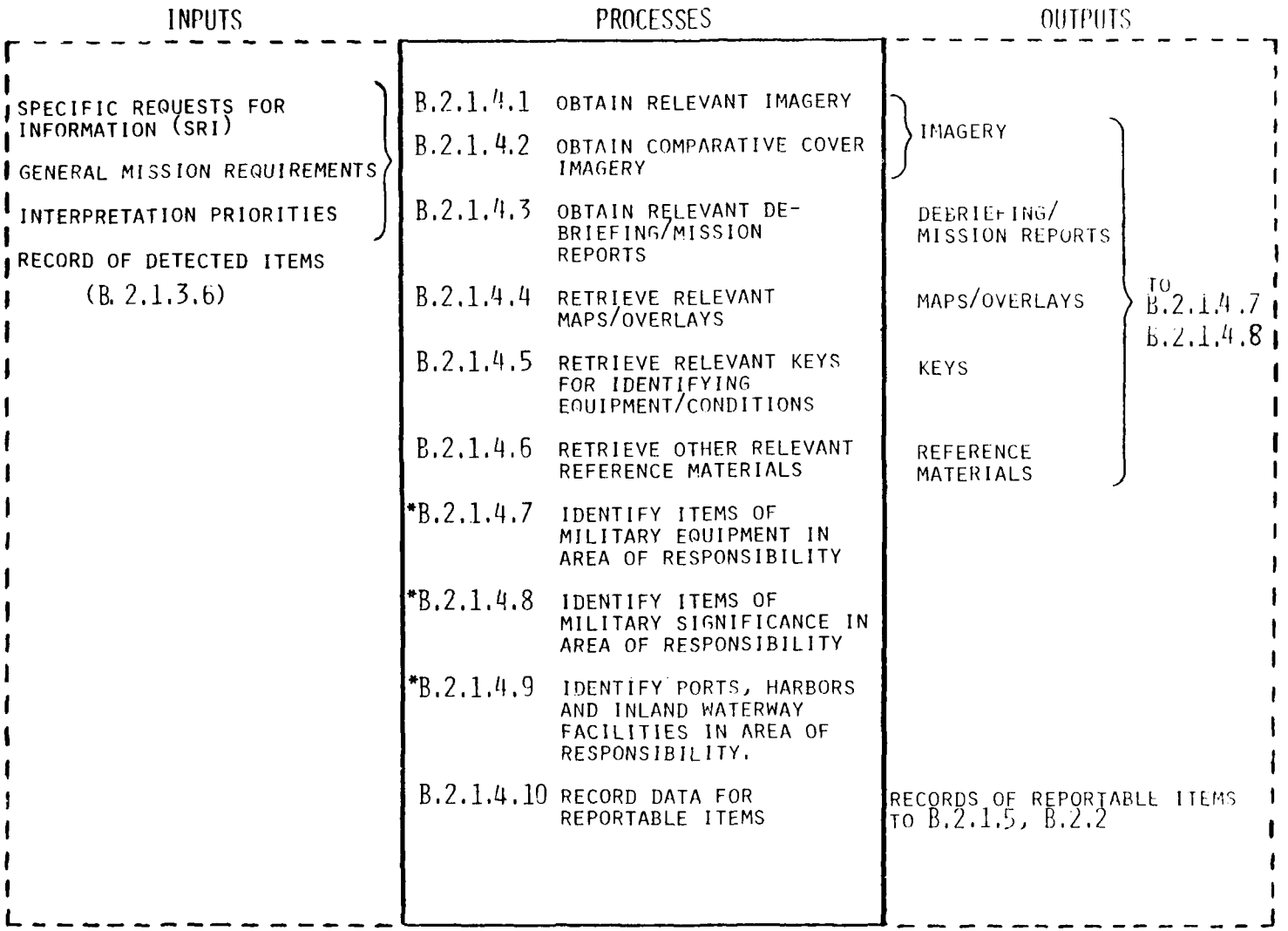
For first phase search, the preliminary screening function associated with detection generally does not involve comparative cover imagery, reports, imagery interpretation keys, or other reference materials because of the time critical nature of such scans, exemplified on the tactical level by the initial screening for items requiring generation of a HOTPHOTOREP. A minimum of comparative material -- e.g., a SITMAP -- is used to detect changes in the location of moving targets.

In second phase search, (roughly, within 24 hours) exemplified on the tactical level by search for items meriting an 'Immediate' report, there is sufficient time to utilize aids and reference materials for more precise and detailed reporting.

In third phase interpretation, the detection effort is largely directed at guaranteeing that no reportable items in the functional and geographic areas of responsibility of the particular imagery interpretation element have been missed in the previous, time-constrained, scans (for example, because of camouflage or concealment practiced by non-friendly forces).

Thus, time-critical reporting of items detected may involve only the recording of an approximate location and marking of the particular frame of imagery for further analysis, identification, and quantification, while less time sensitive scans are directed at full exploitation of available imagery, based on all available data. The latter type of detection processing can therefore include the so-called 'negation' analysis, where the coverage history of an object or condition is followed to the point before the item appeared.

B.2.1.4 TARGET IDENTIFICATION



* indicates expansion of function in following pages

B.2.1.4 Target Identification

The identification of targets is the primary activity of an IIA. It consists in interpreting the visual cues or distinctive features of imaged objects and terrain conditions in order to determine their identity. The distinctive features are analyzed using the five 'S's (size, shape, shadow, shade, and surroundings). The depth of analysis involved in target identification is highly dependent on the time constraints for completion of the identification process. An object may be tentatively identified as a medium tank, without specifying what type of tank it is, in order to produce a HOTPHOTOREP indicating a change in an area where no armor was previously noted. Where time is less critical, careful and complete identification of equipment and its implications (e.g., headquarters unit in area) can be carried out using all available reference data and analytical aids.

In performing the identification function (especially under time pressure), the problems of errors of invention, misidentification, and missed information must be considered. Suppose an IIA mistakes rectangular grave mounds for weapons emplacements or grain stacked in shocks as a minefield pattern, or logs and debris on a river for small boats. These inventive errors could result in the sending of forces against such false targets at no small cost, economically or tactically speaking, to the commander.

Another problem involves missing a target representing a potential threat -- e.g., a SAM site -- by interpreting it as an object having no military significance. The cost of missing such information is proportional to the threat associated with the given target: failing to identify a tank is presumably less costly (tactically and economically) than missing a SAM site.

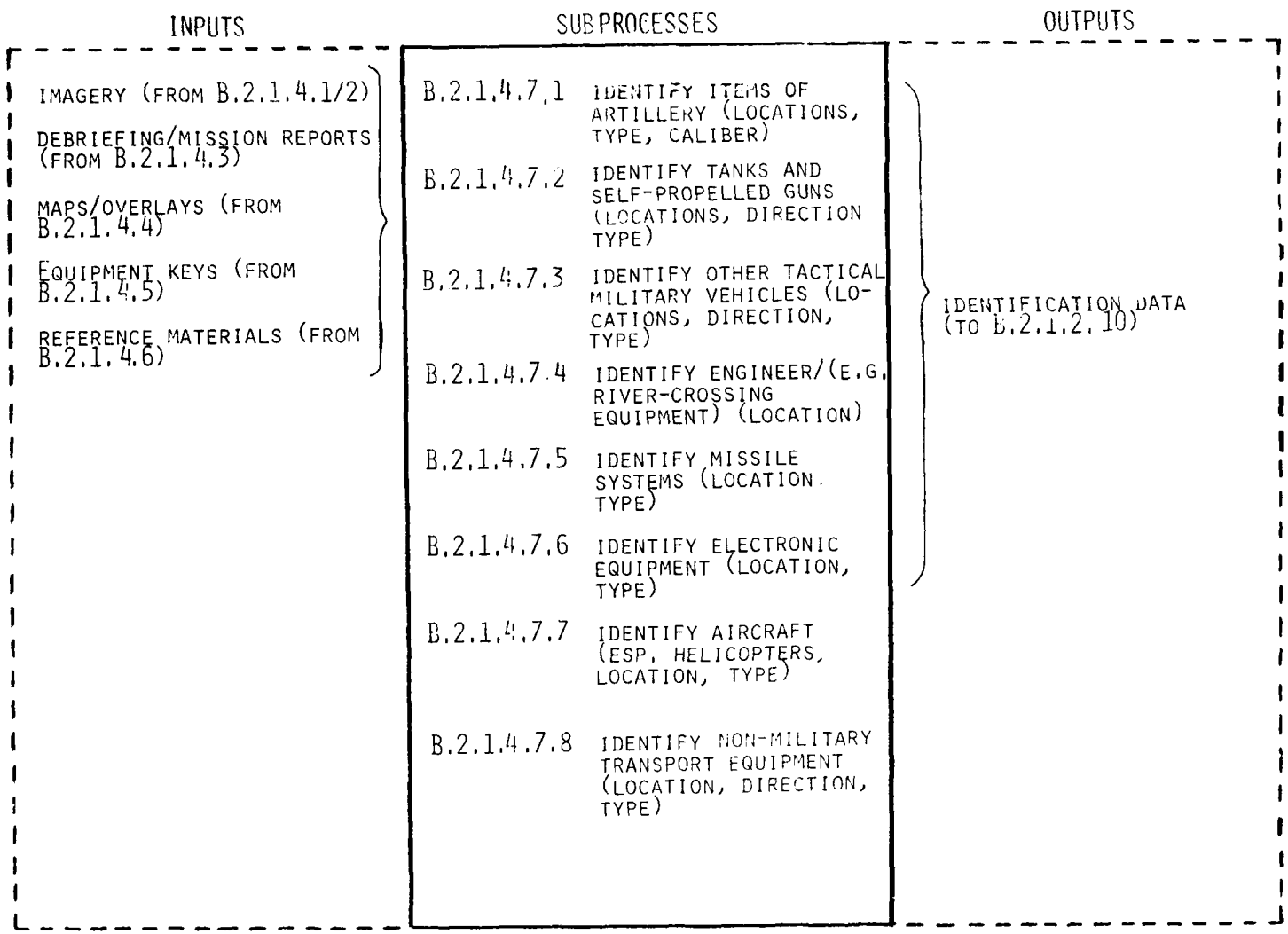
The cost of misidentification errors (identifying one type of military object as another) is also associated with the potential threat represented by the misidentified object. For example, identification of a missile transporter as another type of transport trailer could be serious in the absence of other information indicating the presence of missiles in the the area of interest.

The use of error keys, such as the key designed by ARI for use in Vietnam [Ref. 24], can be more productive than "rights" keys in avoiding interpretation errors in some cases. Both error and "rights" key products are designed to encourage use even in time-critical reporting situations.

Also, IIAs tend to specialize in identifying and reporting particular classes of targets, and are often functionally organized along these lines. Responsibilities may be assigned only for particular types of equipment and conditions, improving identification accuracy and timeliness, but also requiring that multiple scans be made of the same imagery. Any type of available intelligence to aid in confirming target identifications or guiding hypotheses as to probable areas of operation or associated units is exploited by the IIA in searching for and identifying targets. Of particular importance is the IIA's knowledge of 'surroundings' -- the fifth 'S' in image analysis. The concept of surroundings includes associations between types of equipment and between equipment and organizational units mentioned above (B.2.1). Thus some types of targets imply the presence of others, leading to a more detailed investigation of the particular imagery.

Apart from the IIA's internal knowledge of targets and associations and the external knowledge sources represented by keys, reference materials, and comparative cover imagery, an extremely valuable external knowledge source is embodied in other IIAs. Although IIAs are highly individualistic in their approach to interpretation and in their information acquisition behavior (see B.2.3.2), they are essentially team workers who respect the ability of fellow IIAs and utilize their knowledge in areas where they feel the need of assistance or expert opinion. This attitude is consistent with the experienced IIA's concern and feeling of responsibility for the acquisition of knowledge by novice IIAs (B.2.3.6).

B.2.1.4.7 IDENTIFY ITEMS OF MILITARY EQUIPMENT



* indicates expansion of function in following pages

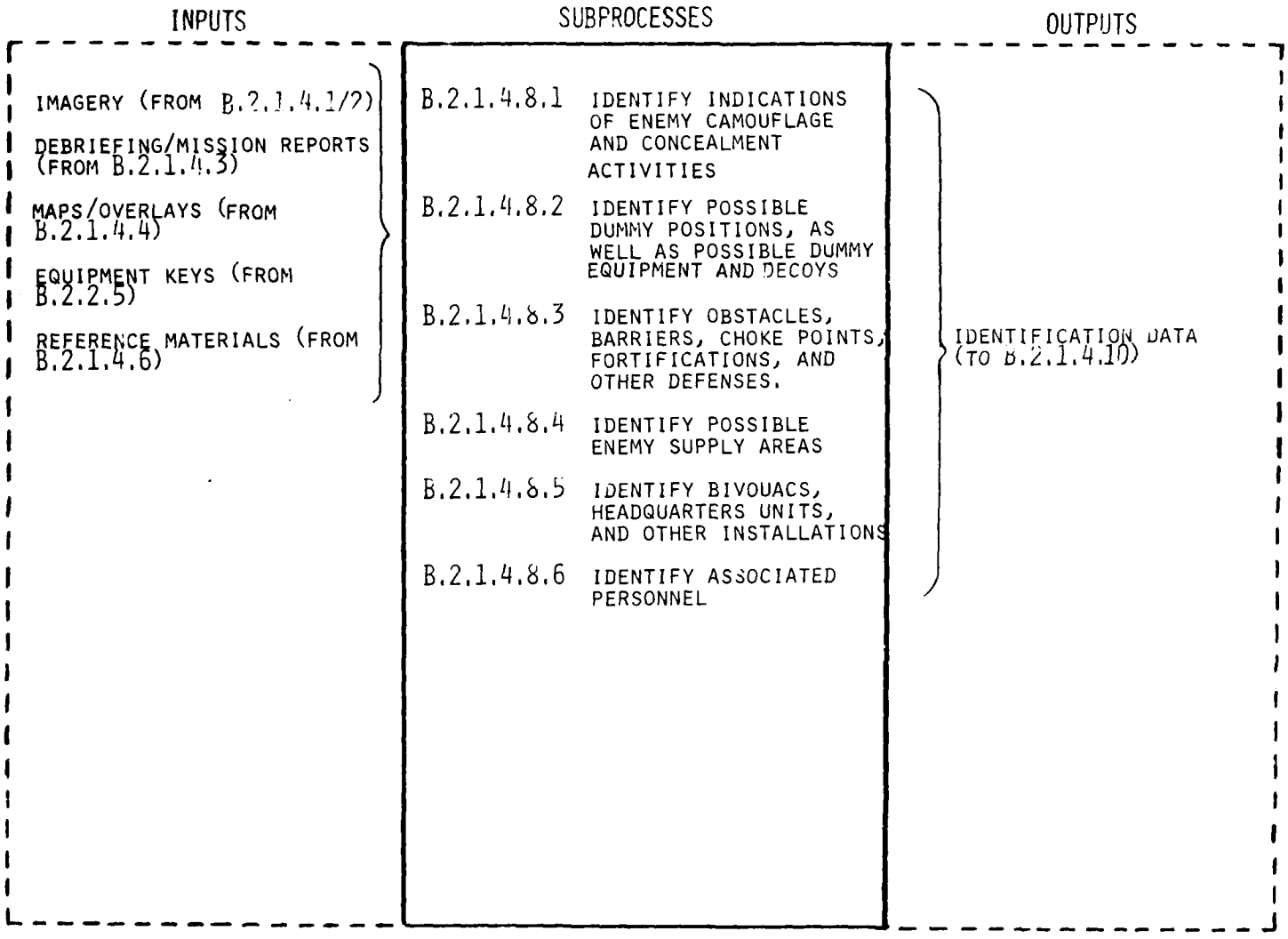
B.2.1.4.7 Identify Items of Military Equipment

The major classes of military equipment a tactical IIA is concerned with are artillery, wheeled vehicles (non-military as well, since these may also be used for military purposes), tanks and self-propelled guns, special types of engineering equipment, CBR equipment, missile systems, electronic equipment, and aircraft. In identifying mobile items of military equipment, IIAs are also concerned with determining direction of movement, and noting changes in location and direction from previously reported activities and condition (e.g., state of combat readiness -- a missile observed on a transporter versus a missile on a launcher).

In third phase interpretation at the strategic level, identification of equipment, both in development and deployed, is carried out on an extremely detailed level, in support of analytical activities aimed at developing an extensive knowledge of foreign technology.

In evaluating equipment and the important factor of 'surroundings', the association between equipments, and between equipments and organizations leads to detailed searches of the imaged area, as noted under B.2.1.4.

B.2.1.4.8 IDENTIFY ITEMS OF MILITARY SIGNIFICANCE

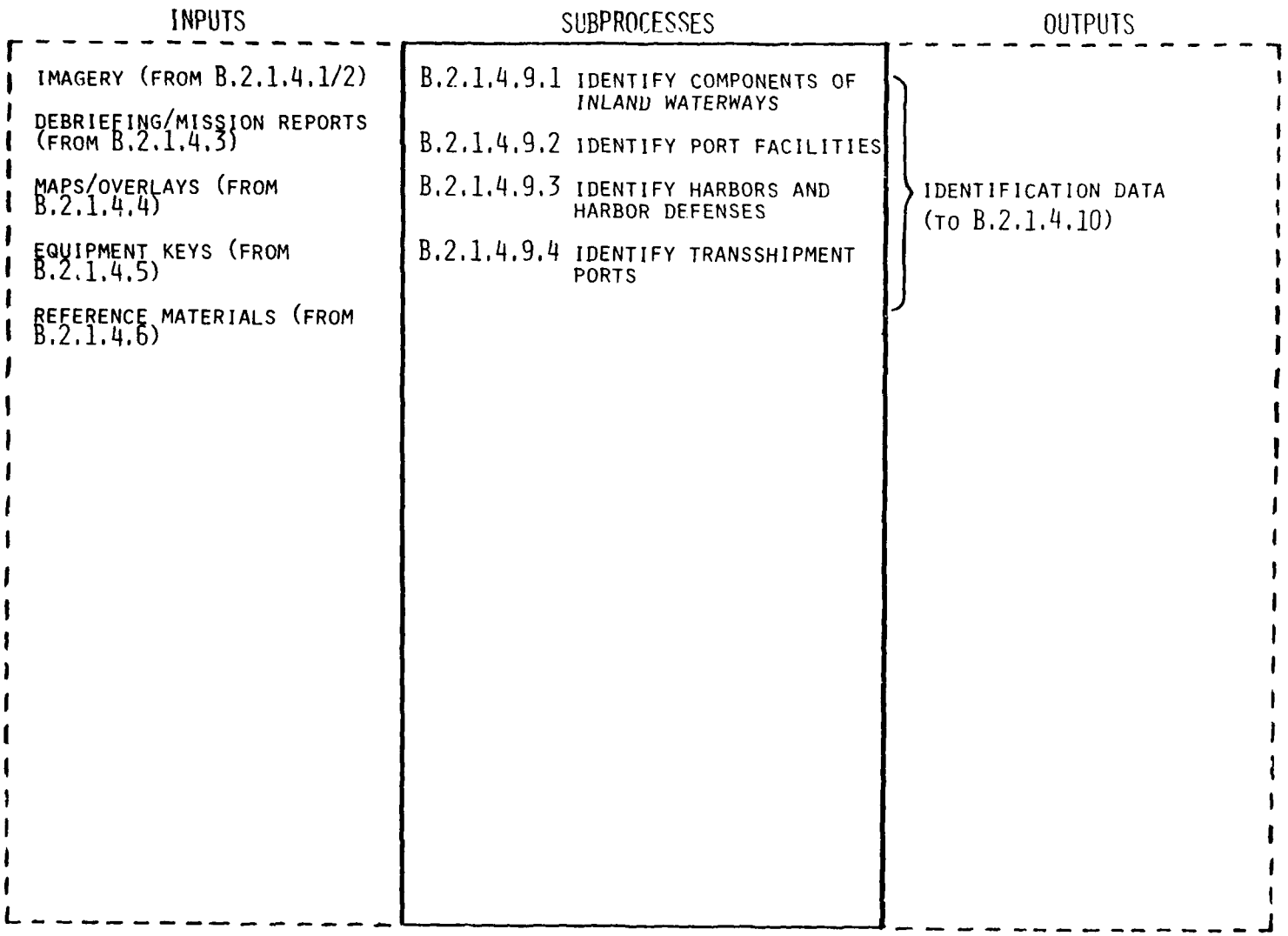


* indicates expansion of function in following pages

B.2.1.4.8 Identify Items of Military Significance

In addition to items of military equipment, all objects, characteristics and conditions of military significance must be identified, using the IIA's personal knowledge of distinctive features of items of military significance, in terms of the principles discussed under B.2.1.4. A particularly important task involves the determination of the presence of indicators of camouflage and concealment, since such activities may cause reportable objects or conditions (e.g., an excavation for a missile site) to be missed. Other indications of attempted deception, such as dummy positions, equipment, and decoys are also extremely critical in terms of establishing intent of unfriendly forces. Other important objects and conditions of military significance to be identified include route-associated items such as barriers, obstacles, and choke points, having significance both for enemy and friendly movements. In addition, enemy supply areas, bivouacs, headquarters units, installations, and associated personnel must be identified and reported.

B.2.1.4.9 IDENTIFY PORTS, HARBORS, AND INLAND WATERWAYS



* indicates expansion of function in following pages

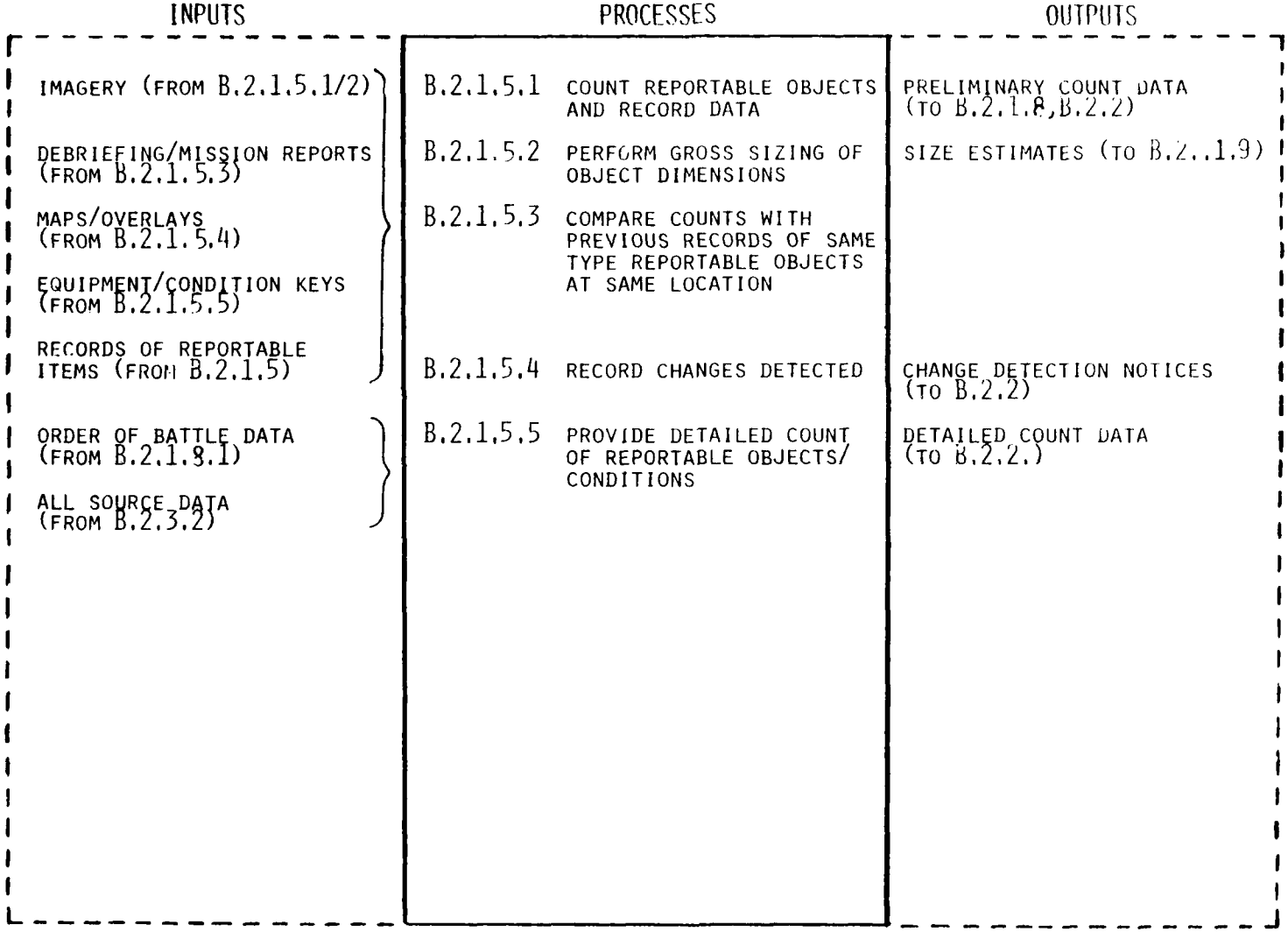
B.2.1.4.9 Identify Ports, Harbors, and Inland Waterways

Although the analysis of port and harbor targets tends to be a naval responsibility at the national level, the tactical image interpreter is expected to be a generalist. If such port and harbor facilities exist in the planned area of operations, the image interpreter must be able to analyze and report on them. Especially important are evidences of transshipment of military equipment and material, POL supplies, and other logistics information of military significance.

The basic image interpretation course taught at Fort Huachuca thus includes the identification and analysis of port and harbor facilities among the subject blocks presented.

Analogously, although strategic analysis of such naval facilities is primarily a naval responsibility in the national tasking, transshipment ports associated with particular targets (e.g., missile test ranges) are an important source of information on status of development and readiness, and target activity of reporting significance.

B.2.1.5 TARGET QUANTIFICATION



* indicates expansion of function in following pages

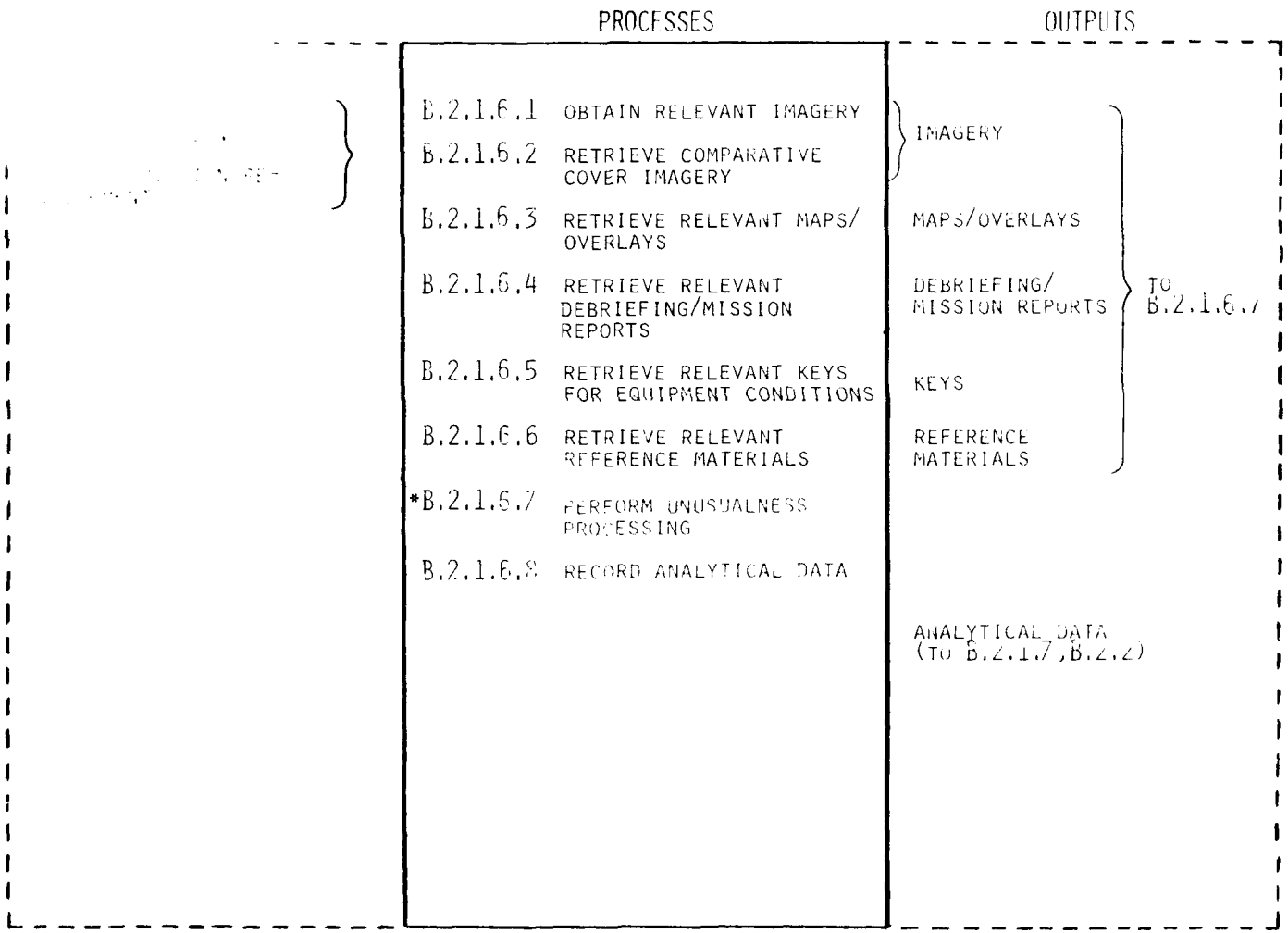
B.2.1.5 Target Quantification

The division between the target identification (B.2.1.4) and quantification activities on the one hand, and the quantification and photogrammetric (B.2.1.7) activities on the other is often blurred in a tactical field situation where a single individual performs all these functions with respect to a given target. Even on the level of strategic imagery interpretation resources, however, an estimate of the number of identified objects of a particular type will be recorded simultaneously with the identification data, although photogrammetry is usually handled by a separate, specialized, element.

An important difference exists between the rough counts made in the course of first phase interpretation for immediate detection of significant changes in the situation and the detailed counts made in later phases of interpretation to validate records of such changes. Detailed counts involve reference to all available data to determine, for example, where the missing aircraft from a group of 28 reported earlier might be (in hangars, on a reconnaissance mission, camouflaged, lost or destroyed, returned to base of origin).

Similarly, gross sizing estimates of reportable items ("slit trenches approximately 50 feet long and 4 feet deep") are usually recorded with location and identification data. However, where required by reason of potential significance, gross sizing estimates and associated imagery are input to the photogrammetric function for exact mensuration.

B.2.1.6 UNUSUALNESS ANALYSIS



* indicates expansion of function in following pages

B.2.1.6 Unusualness Analysis

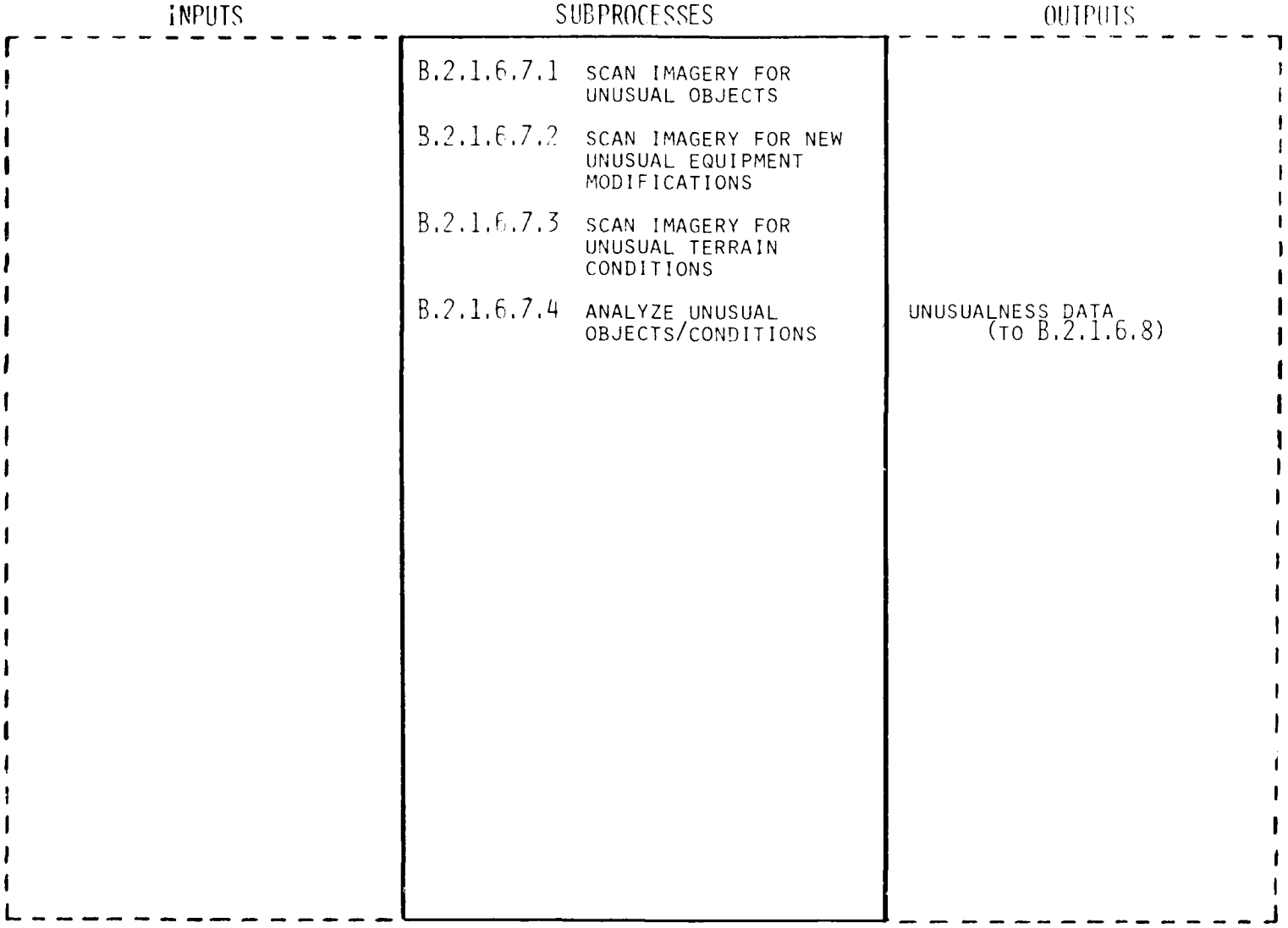
An important activity of an IIA is alertness to unusual objects, previously unknown equipments or novel modifications of known equipments, numbers and concentrations of military objects or personnel, terrain modifications, dispositions of equipment, directions of movement, etc. Where the knowledge of the IIA is insufficient, it can be supplemented with analytical aids and reference materials, which, in the context of the experience and skills of the particular IIA, can assist in distinguishing unusual objects and patterns of activities from normal phenomena.

Like target detection (B.2.1.3), identification (B.2.1.4), and quantification (B.2.1.5), unusualness analysis may be driven by the general requirements of the given mission, EEI in effect at that time, and Standing Requirements List (SRL), or by a Specific Request for Information (SRI) of the type "Notify me if you see anything unusual in Sector x".

Although unusual objects or conditions may be noted in a first phase or preliminary screening interpretation process, unless such manifestations are fairly dramatic, it is more likely that unusualness will be perceived during a second or third phase interpretation activity, or will be resolved at that level. If a novel item of equipment appears on a tank, exact mensuration and special functional analysis of the part may be required in order to determine the significance of the new addition.

Unusual activities or objects may be tipped off or interpreted via all- source data channels. Messages and other all source reference materials are therefore critical inputs to the recognition and analysis of unusualness.

B.2.1.6.7 UNUSUALNESS PROCESSING



* indicates expansion of function in following pages

B.2.1.7 FUNCTION ANALYSIS

INPUTS	SUBPROCESSES		OUTPUTS	
SPECIFIC REQUESTS FOR INFORMATION (SRI)	B.2.1.7.1	OBTAIN RELEVANT IMAGERY	IMAGERY	TO B.2.1.7.4
GENERAL MISSION REQUIREMENTS	B.2.1.7.2	RETRIEVE RELEVANT KEYS	KEYS	
	B.2.1.7.3	RETRIEVE RELEVANT REFERENCE MATERIALS	REFERENCE MATERIALS	
MENSURATION DATA (FROM B.2.1.9)	B.2.1.7.4	PERFORM FUNCTIONAL ANALYSIS OF NEW OR UNUSUAL EQUIPMENT		
	B.2.1.7.5	INTERACT WITH EXPERTS AS NECESSARY	FUNCTION DATA (TO B.2.2)	
	B.2.1.7.6	RECORD FUNCTION DATA		

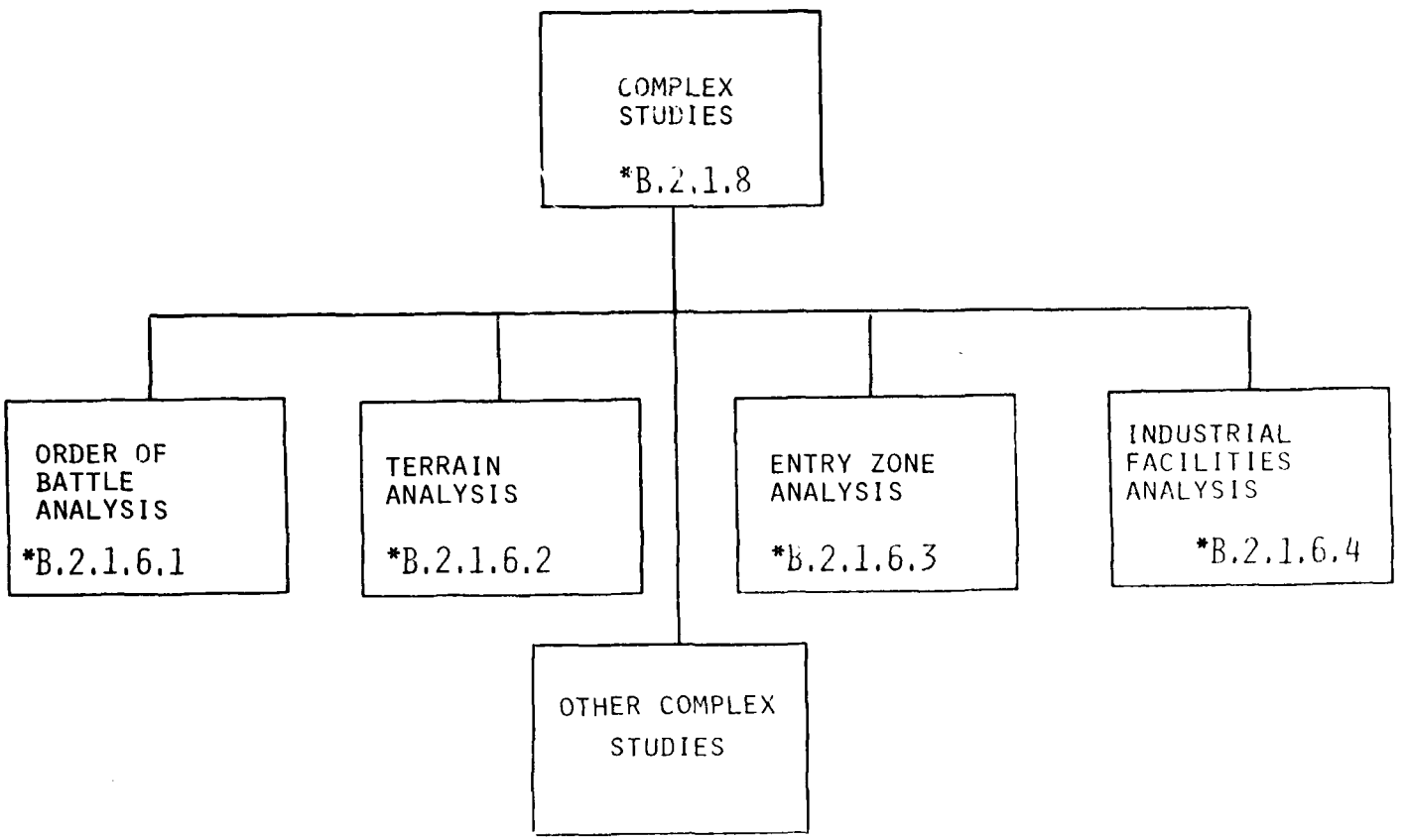
* indicates expansion of function in following pages

PRECEDING PAGE BLANK - NOT FILMED

B.2.1.7 Function Analysis

In contrast to the previously described image interpretation process steps, analysis of the function of an object, equipment modification, or environment modification is mainly limited to third phase interpretation, where detailed analysis can be carried out without affecting time-critical deliveries of information.

Function analysis is especially important in image interpretation for support of basic intelligence production related to developments in foreign science and technology.

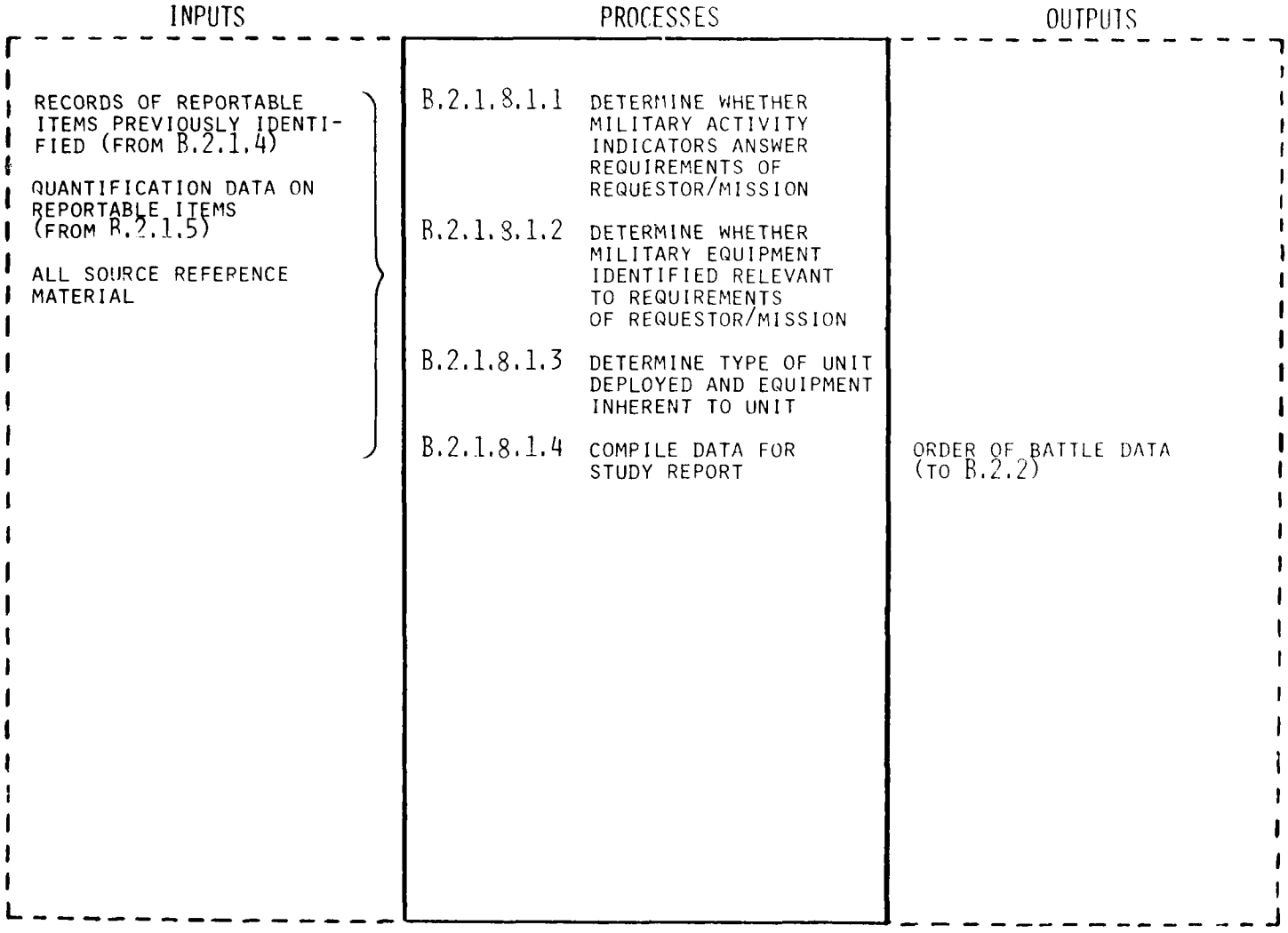

COMPLEX STUDIES
*B.2.1.8
ORDER OF BATTLE ANALYSIS
*B.2.1.6.1
TERRAIN ANALYSIS
*B.2.1.6.2
ENTRY ZONE ANALYSIS
*B.2.1.6.3
INDUSTRIAL FACILITIES ANALYSIS
*B.2.1.6.4
OTHER COMPLEX STUDIES

B.2.1.8 Complex Studies

The analytical work described under the topic of 'Complex Studies' is seen primarily as third phase, in-depth imagery interpretation activity, without the severe time constraints associated with first and second phase interpretation processes. Although some aspects of these topics may apply equally to first and second phase processing (for example, some Order of Battle analysis may in fact be carried out simultaneously with identification and quantification of objects of military significance (B.2.1.4., B.2.1.5)), the type of detailed analysis exemplified by these studies requires more processing time and the use of more reference materials than is possible in the preliminary scanning and continued processing phases.

The complex studies shown in the accompanying chart are intended as examples of the types of studies which are performed by IIAs at the tactical and strategic levels. The examples given are more typical of tactical level analytical activities. At the strategic level, detailed studies of weapon systems, missile and space technology, and other types of in-depth analytical studies involving imagery are performed.

B.2.1.8.1 ORDER OF BATTLE ANALYSIS



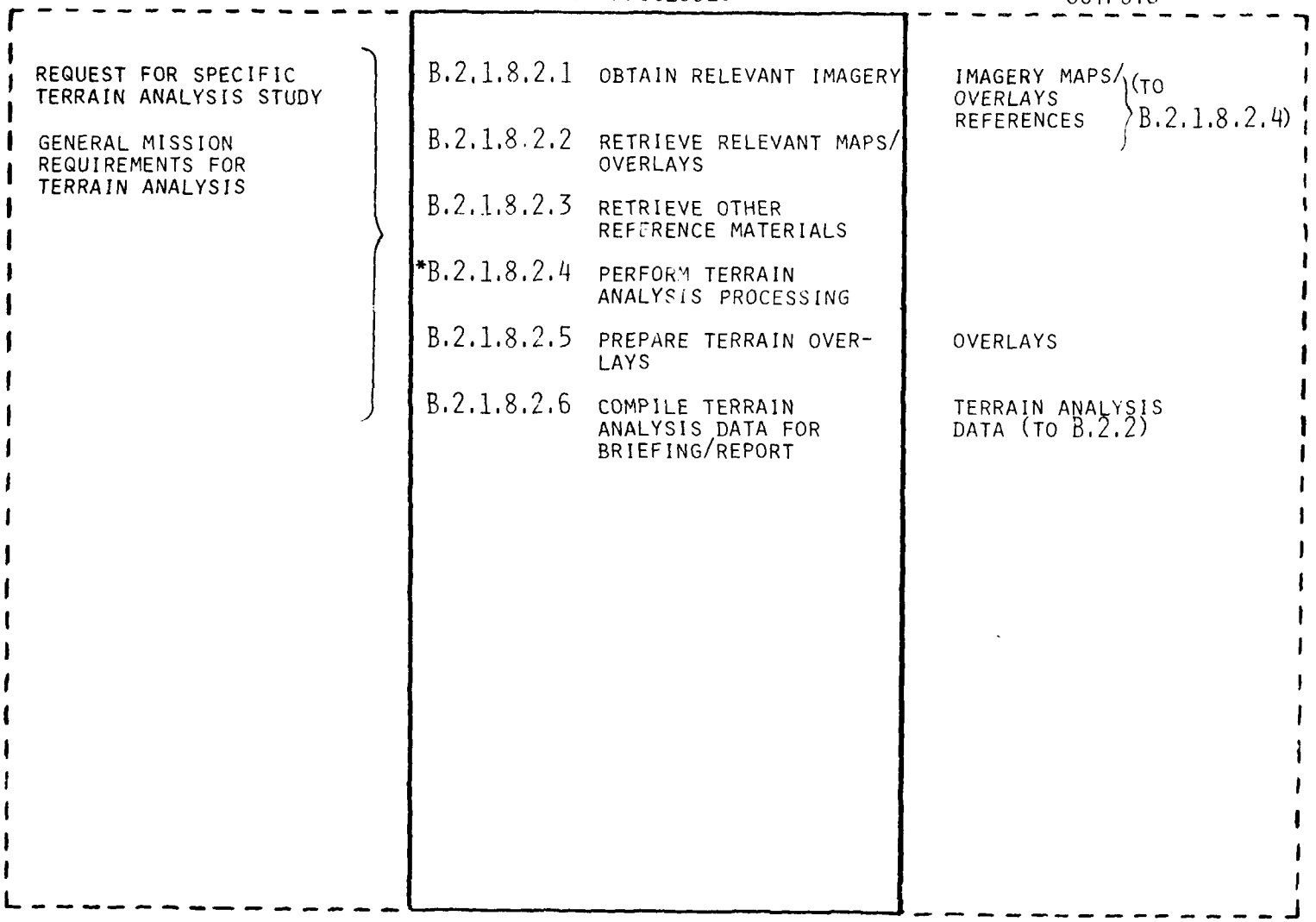
* indicates expansion of function in following pages

B.2.1.8.1 Order of Battle Analysis

Using identification and quantification data from the functions represented in B.2.1.4 and B.2.1.5, the image interpreter determines the significance of these data in terms of Order of Battle. In the identification and quantification processes, the image interpreter is concerned with what type of equipment is shown in the imagery, and how many of these equipments are represented. In Order of Battle analysis, he associates these equipments with particular elements, evaluates the significance of the movement and direction of the given units, and determines what impact these deployments have on the Order of Battle of non-friendly forces by comparing current with previously reported dispositions. For example, the image interpreter may determine that the 2 T-62s previously reported are subordinate to the 103rd Tank Battalion, that they are moving toward the forward area, and may represent the vanguard of the 39th Tank Division, indicating a replacement of the previously noted 42nd Tank Division in the forward area.

In order to perform this type of analysis, the image interpreter requires -- in addition to his usual maps, overlays, and reference material -- all source reference material, including all current message traffic relevant to his area of responsibility and hard copy reports containing Order of Battle data.

B.2.1.8.2 TERRAIN ANALYSIS



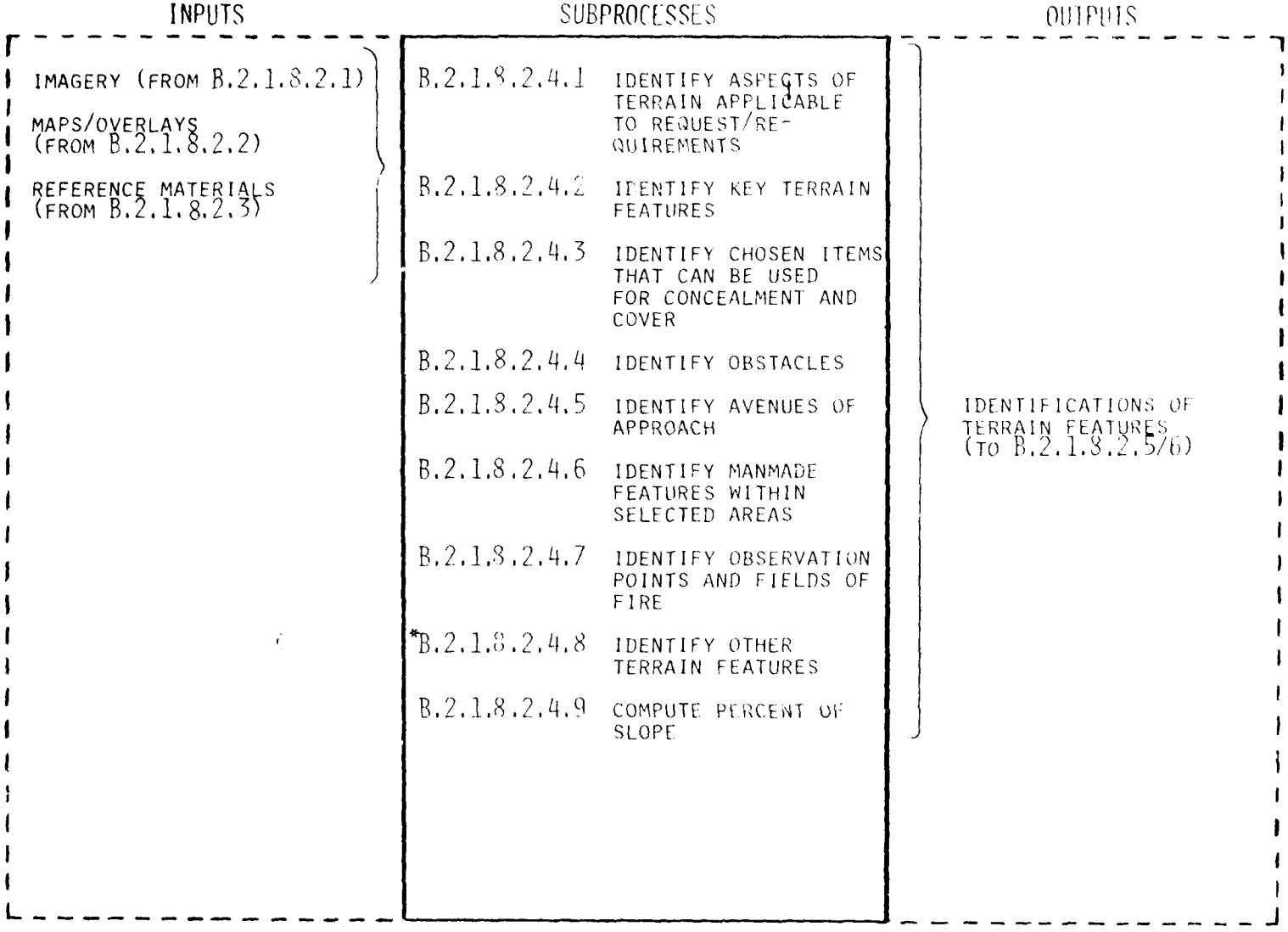
* indicates expansion of function in following pages

B.2.1.8.2 Terrain Analysis

Terrain analysis studies are generally carried in accordance with some mission-related requirement, although special requests for terrain analysis of particular areas may also occur. In addition to imagery, maps, and overlays, the image interpreter will use other types of reference material giving details of density of forestation, width of trees, specifics of natural obstacles such as rivers and canyons, specifics of urban areas such as width of streets, height of buildings, population of the area, and other data, as required.

The analytical data resulting from this process may be presented in the form of a briefing, with graphics and overlays; as terrain overlays or templates for SITMAPS; or in the form of a message or hardcopy report.

B.2.1.8.2.4 PERFORM TERRAIN ANALYSIS PROCESSING



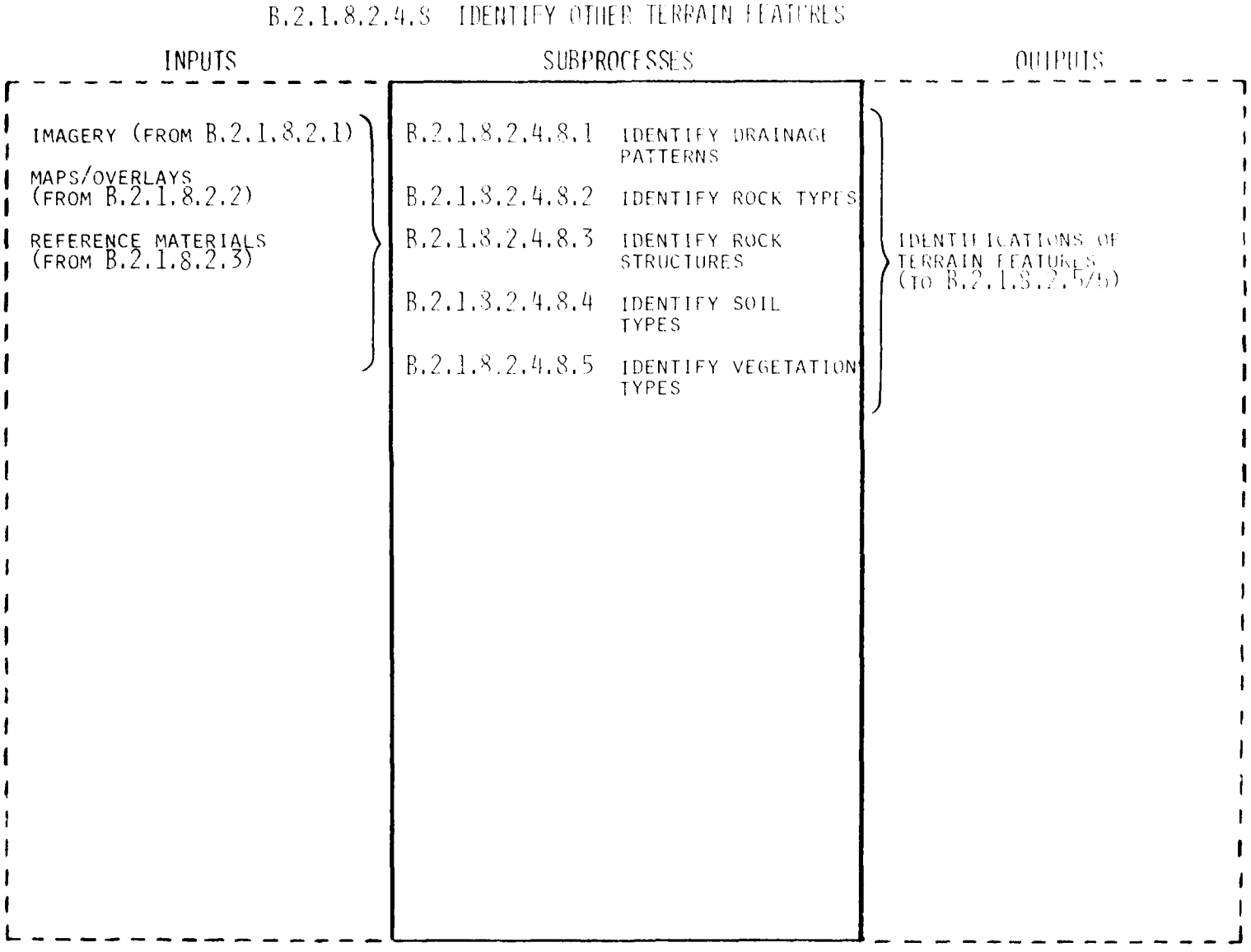
* indicates expansion of function in following pages

6.2.1.8.2.4 Perform Terrain Analysis Processing

In performing the terrain analysis subfunction, the image interpreter is first concerned with identifying key features of the terrain under investigation. For example, a particular hill mass in a given sector might provide an essential offensive or defensive advantage -hence possession of it is key to the friendly forces' position. Similarly, a particular bridge or river crossing (such as a fording area) may provide the unique means of controlling access to and egress from a given sector.

Terrain features which can be utilized for concealment and cover are of obvious importance in a tactical situation. To illustrate, a deciduous forest will normally carry a dense canopy of leaves during at least six months of the year, thus providing protection
providing good cover from ground fire and partial cover from aerial observation; however, a planted area such as an orchard would provide very minimal cover.

Natural obstacles would include such terrain features as rivers, dense forests, mountainous or steep hilly terrain, while avenues of approach are rolling or flat areas free from such obstacles. Man-made features include building construction (e.g., buildings with basements or underground areas provide cover from enemy fire), roads, bridges, railroads, airports, etc. Observation points may be manmade, such as a church steeple, or natural, such as an escarpment. Fields of fire may be defined in terms of proximity to a terrain feature providing a good defensive or offensive position, range in terms of line-of-sight firing, relationship of cultivated land to forested areas, and so forth.

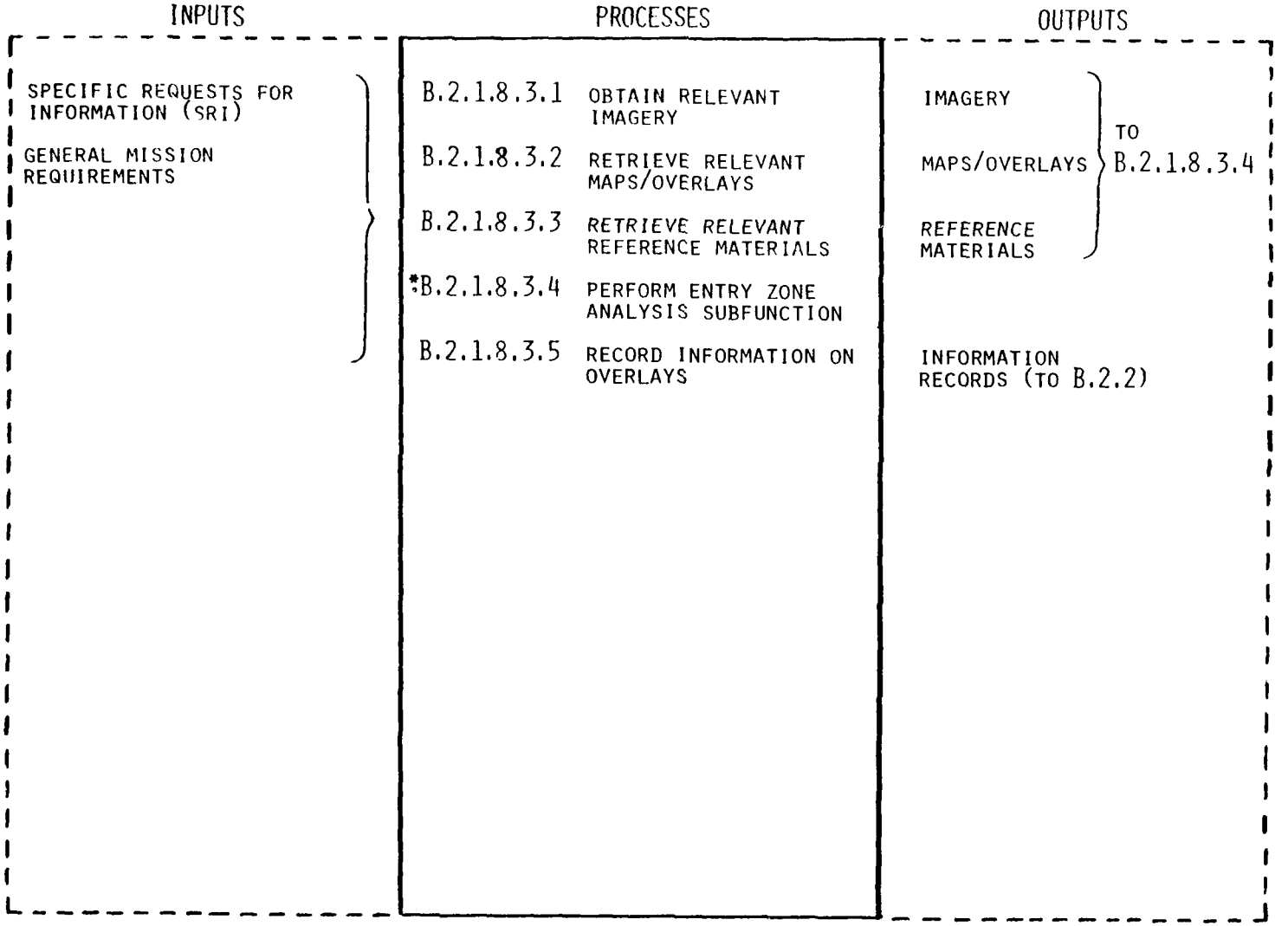


* indicates expansion of function in following pages

B.2.1.8.2.4.8 Identify Other Terrain Features

In addition to the more specific delineation of terrain features in terms of tactical significance, general features of the given area are also important to analyze. Knowledge of drainage patterns is critical to evaluating trafficability of roads and low-lying areas in wet seasons, information on rock types and surface materials is required for evaluating whether off-road areas can support armored vehicles and other heavy military traffic, or whether rock structures can serve as gun emplacements, etc. Information on vegetation types is also important in a tactical situation, since -- for example -- a coniferous forest is generally far more open than a deciduous forest, having less underbrush to impede movement of troops, and offering less potential for concealment from ground fire.

B.2.1.8.3 ENTRY ZONE ANALYSIS

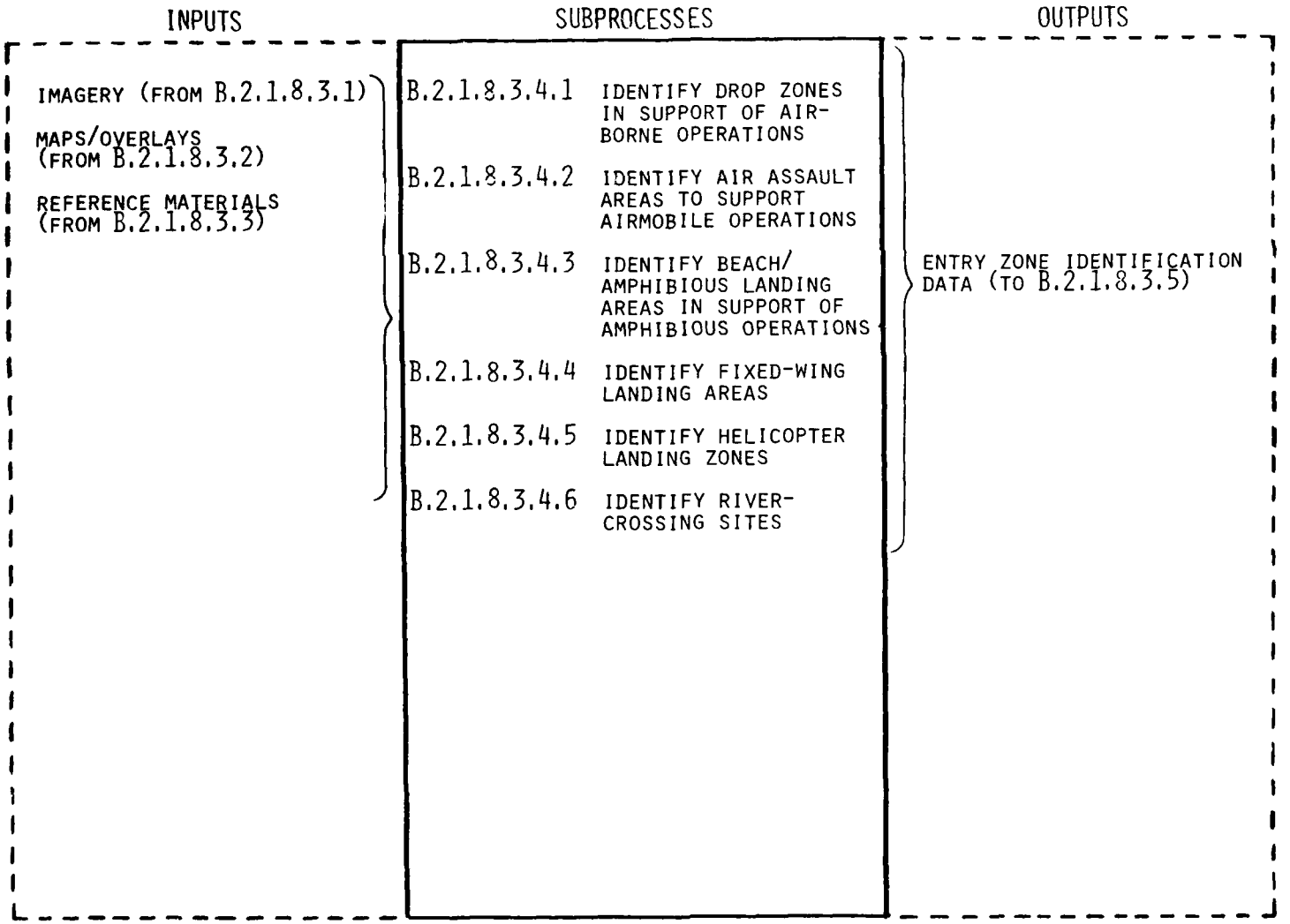


* indicates expansion of function in following pages

B.2.1.8.3 Entry Zone Analysis

Another important activity in tactical imagery interpretation is analysis of potential zones for introducing assault troops into forward areas, which may be unoccupied, or held by non-friendly forces. In the latter case, materials utilized as background for the analytical study include all source message traffic and hard copy reports as well as the imagery, maps, and other reference materials indicated in the associated chart. Potential zones that are identified by the IIA tasked with the analytical study are indicated on overlays to assist in assault planning based on a SITMAP, or other map of the given area.

B.2.1.8.3.4 PERFORM ENTRY ZONE ANALYSIS PROCESSING

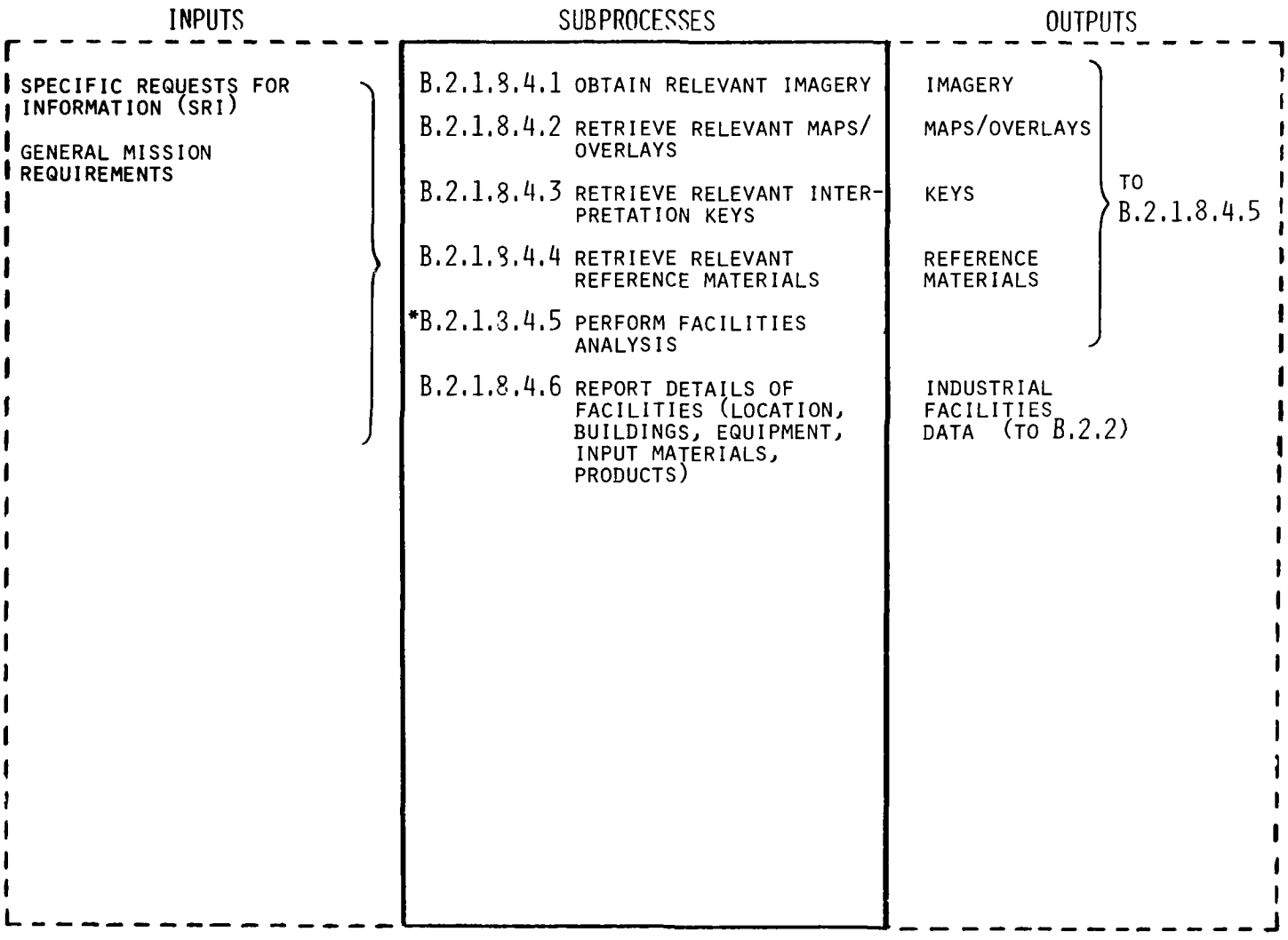


* indicates expansion of function in following pages

B.2.1.8.3.4 Perform Entry Zone Analysis Process

The entry zone identification process covers a range of potential means of entry and offers alternate zones where possible. The analytical process thus includes identification of potential drop zones for possible airborne operations, air assault areas in support of airmobile operations, beach and amphibious landing areas for amphibious operations, fixed-wing and helicopter aircraft landing areas, and potential river crossings.

B.2.1.8.4 INDUSTRIAL FACILITIES ANALYSIS



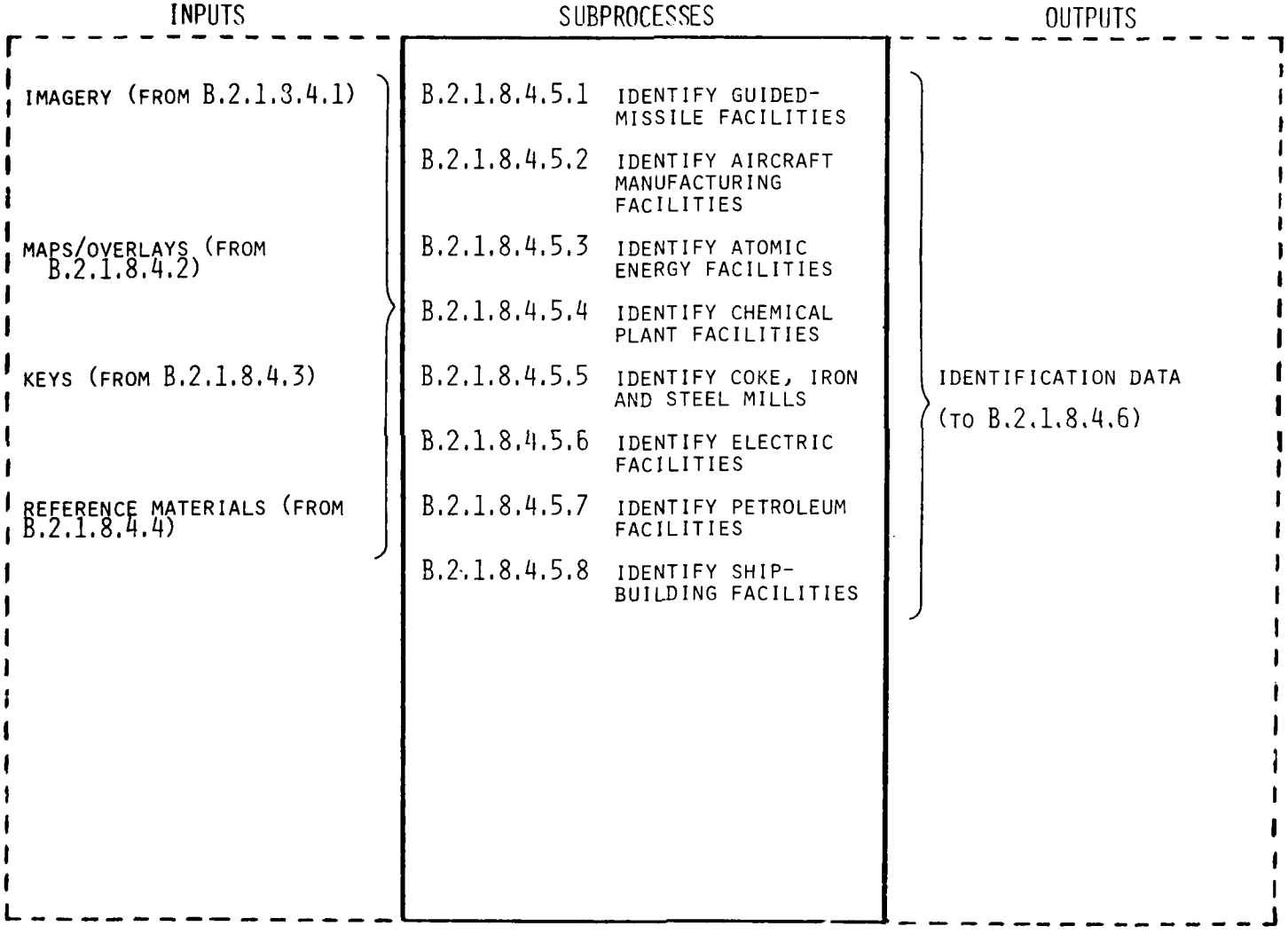
* indicates expansion of function in following pages

B.2.1.8.4 Industrial Facilities Analysis

At the national level, studies of strategic industrial targets are an important responsibility for continuing evaluation (e.g., analysis of new construction, changes in input materials or output products, changes in flow of materials among the various components of an industrial complex). Industrial facilities directly involved in the production of military equipment such as tanks, guns, or missiles are of special interest, with respect to information that may be gleaned concerning modifications or product developments.

In a tactical environment, industrial facilities may also be assigned for special study, if they are present in the area of operations, or are involved in support of military organizations operating in the area.

B.2.1.8.4.5 PERFORM INDUSTRIAL FACILITIES ANALYSIS

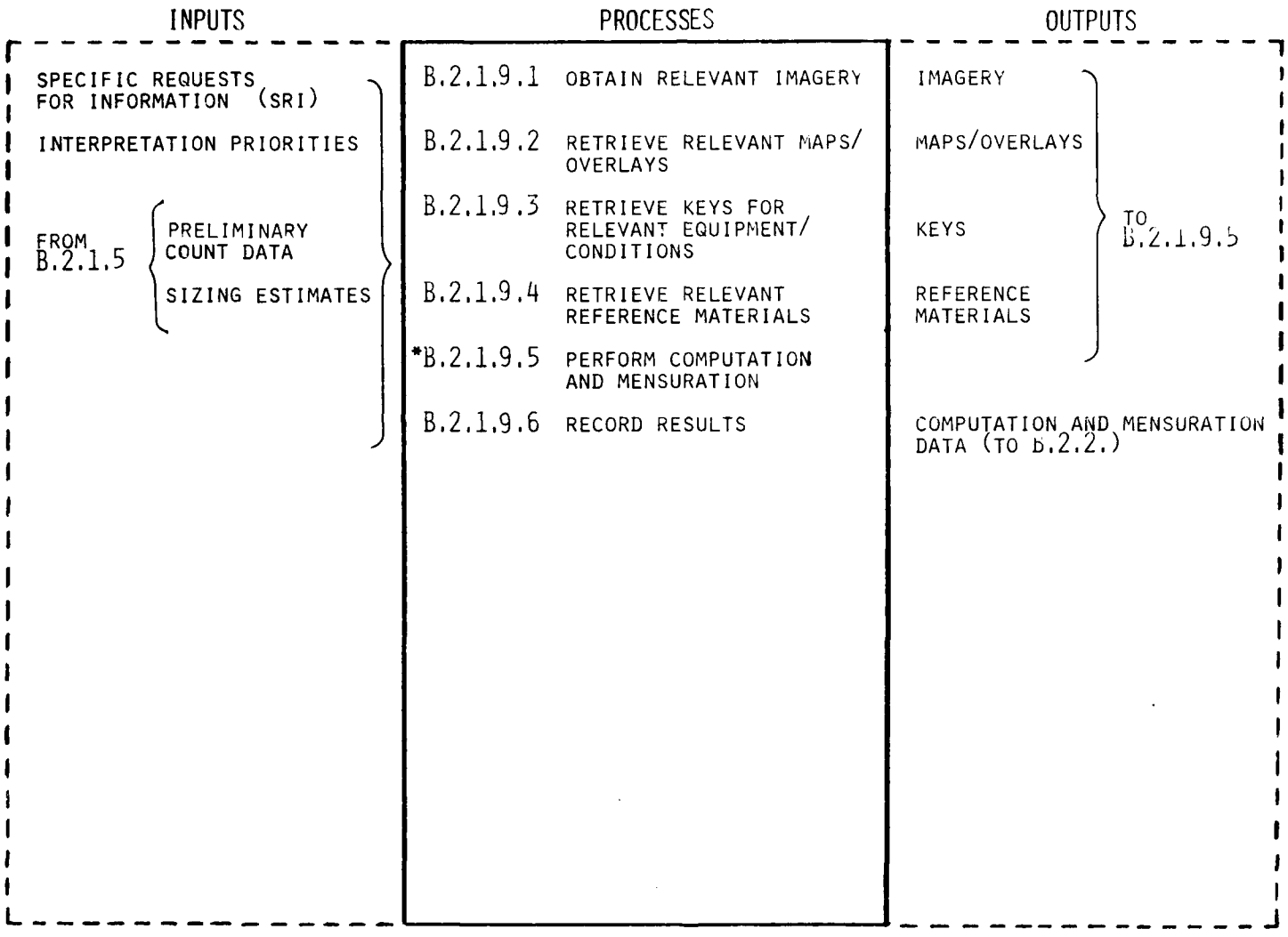


* indicates expansion of function in following pages

B.2.1.8.4.5 Perform Industrial Facilities Analysis

In analyzing industrial facilities for a detailed study, the IIAs charged with the study task must perform an identification and analysis in sufficient detail to provide a complete description of the given facilities (in terms of available imagery and reference materials). Such a description should include the specific location and layout of all buildings belonging to the industrial complex, all related equipment, input materials, output products, and insofar as possible, the flow of such materials and products within the complex.

B.2.1.9 PHOTOGRAMMETRIC SCIENCES



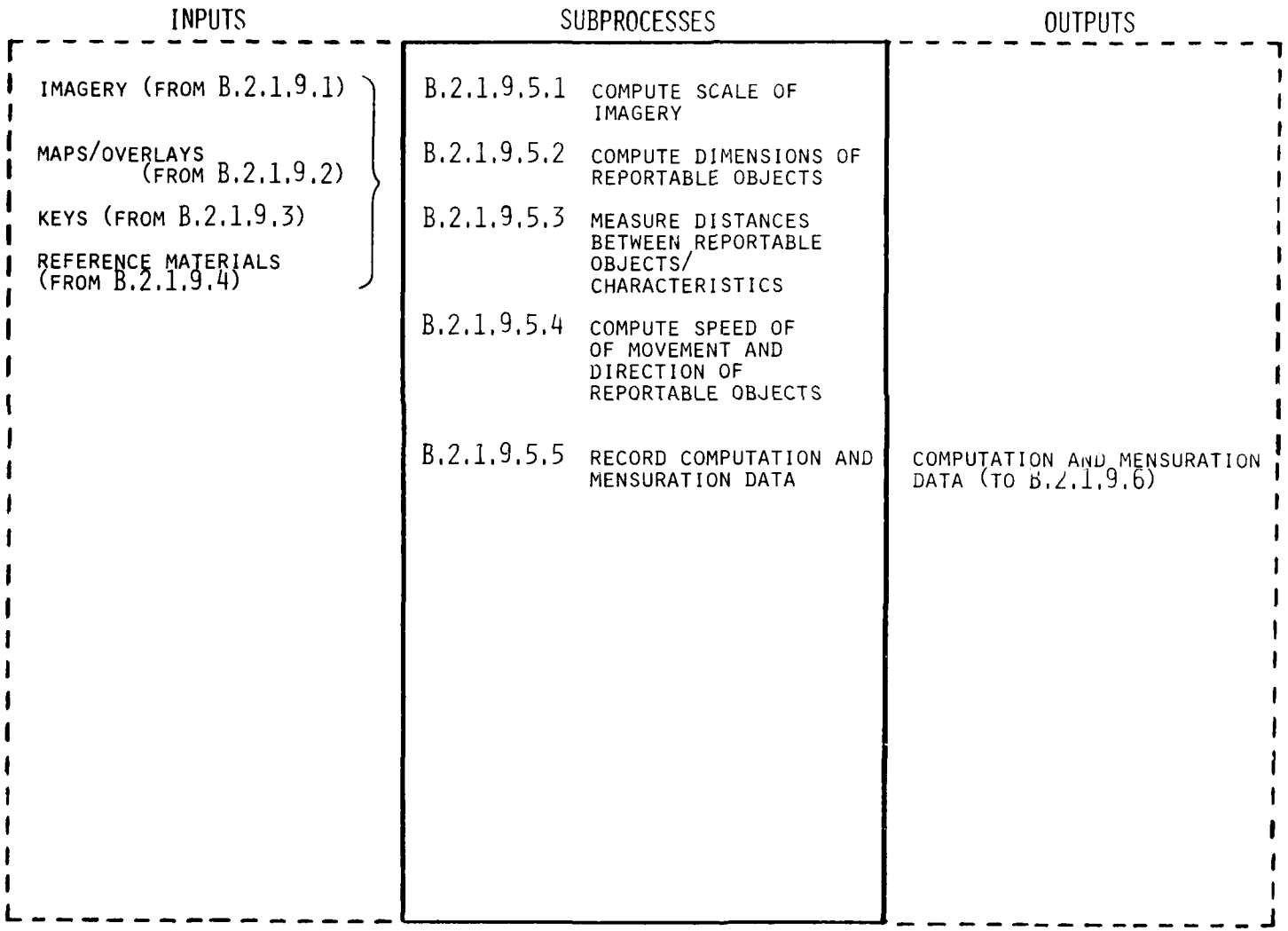
* indicates expansion of function in following pages

B.2.1.9 Photogrammetric Sciences

The photogrammetric activity includes all detailed mensuration and computation which is required in imagery interpretation. At the lower level tactical facilities, an IIa may carry out his own complex mensuration and computation activities. On the other hand, at higher level tactical facilities and at the national resource level, photogrammetry tends to be a specialized function supported by a group of image interpreters with extensive experience in computation and mensuration, who are solely involved in photogrammetric processing.

Inputs to the photogrammetric process are mainly driven by Specific Requests for Information (SRI) in the sense that the mission of the photogrammetric specialists is to respond to such requests from the non-specialist image interpreters supported by the particular photogrammetric element. Preliminary count data and sizing estimates may provide data for validation, or in cases where there is no specialized photogrammetry support, a basis for detailed computation and mensuration.

B.2.1.9.5 PERFORM COMPUTATION AND MENSURATION

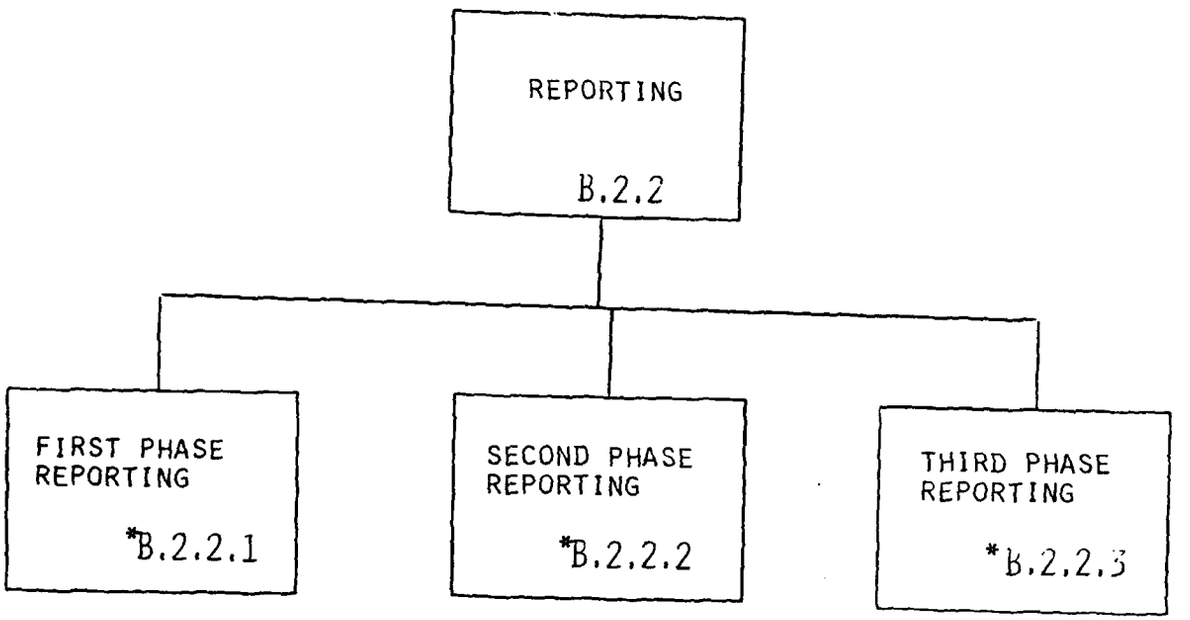


* indicates expansion of function in following pages

B.2.1.9.5 Perform Computation and Mensuration

The most basic photogrammetric task is that of computing the scale of the imagery involved in analysis. Although most scale computation on the national level is precalculated, because the collection effort is planned far in advance, this is an important task on the tactical level. IIAs in the tactical environment are trained to compute scale using focal length of the camera and altitude of the aircraft. If these are not available, the IIA uses computations involving determination of scale in terms of the largest and best defined scale indicator on the imagery, where photo distance and ground distance are established in terms of this indicator. More complex methods of scale determination are required when the imagery is produced by oblique or panoramic cameras.

In computing the dimensions of objects appearing on the imagery, the IIA may choose the relief displacement method (where an object with a visible base is involved), or the shadow proportion method, where film taken in full sun is available.



*INDICATES EXPANSION OF DETAIL IN FOLLOWING PAGES

B.2.2 Reporting

Reports are the primary product of the image interpretation facility. The content of reports and the procedures for generating reports are nearly always dependent upon the amount of time available to produce the report. Because of the time factor in report generation, both at the strategic and tactical level reporting tends to fall into one of the three phases defined in Section 2.:

First phase reporting: preliminary scan on receipt of imagery. (This category also includes real time processing of SLAR, IR, and video imagery.)

Second phase reporting: within 24 hours of receipt of imagery;

Third phase reporting: longer than 24 hours, and periodic reporting.

The time boundaries of these phases as indicated above are only intended to be suggestive, since actual time periods differ slightly between the national strategic IMINT resources and tactical and II organizations, and are also affected by production load and priority. From this point of intelligence utilization of these phases generally corresponds to Indications and Warnings (I&W), Current Intelligence, and Basic Intelligence, respectively. Handling time is a major factor in determining the pace of analysis and reporting. Film development time, duplication of positives, and hardcopy distribution times are significant factors in determining minimum times for reporting imagery interpretation production results.

Because there is less time to analyze imagery in First and Second Phase processes, the detail and accuracy of reports is affected.

A first phase report might identify detected trends simply as light, medium, or heavy; whereas, a second phase report would also provide type identification and unit subordination.

With the increased time available for analysis, in second and third phase reporting the target information carried in the report can become more detailed but the potential for exploiting the target information for tactical or warning purposes decreases. Distribution lists for reports generally reflect the different uses of II reports from first, second, or third phase analysis.

Imagery interpretation reports are composed of the following elements which are relevant to the IMINT products:

Source identification

- Facility
- Time of preparation
- Analyst

Mission

- Mission ID
- Time
- Frame reference
- Sensor parameters
- Location parameters

Requirement reference

- Agency
- Desk
- Requirement number (or message reference)
- Priority

Classification

Content codes report priority Imagery Interpretation Text
Graphics (optional)
Imagery copy (optional)
Target Description

All-source material references (optional)

Imagery quality rating

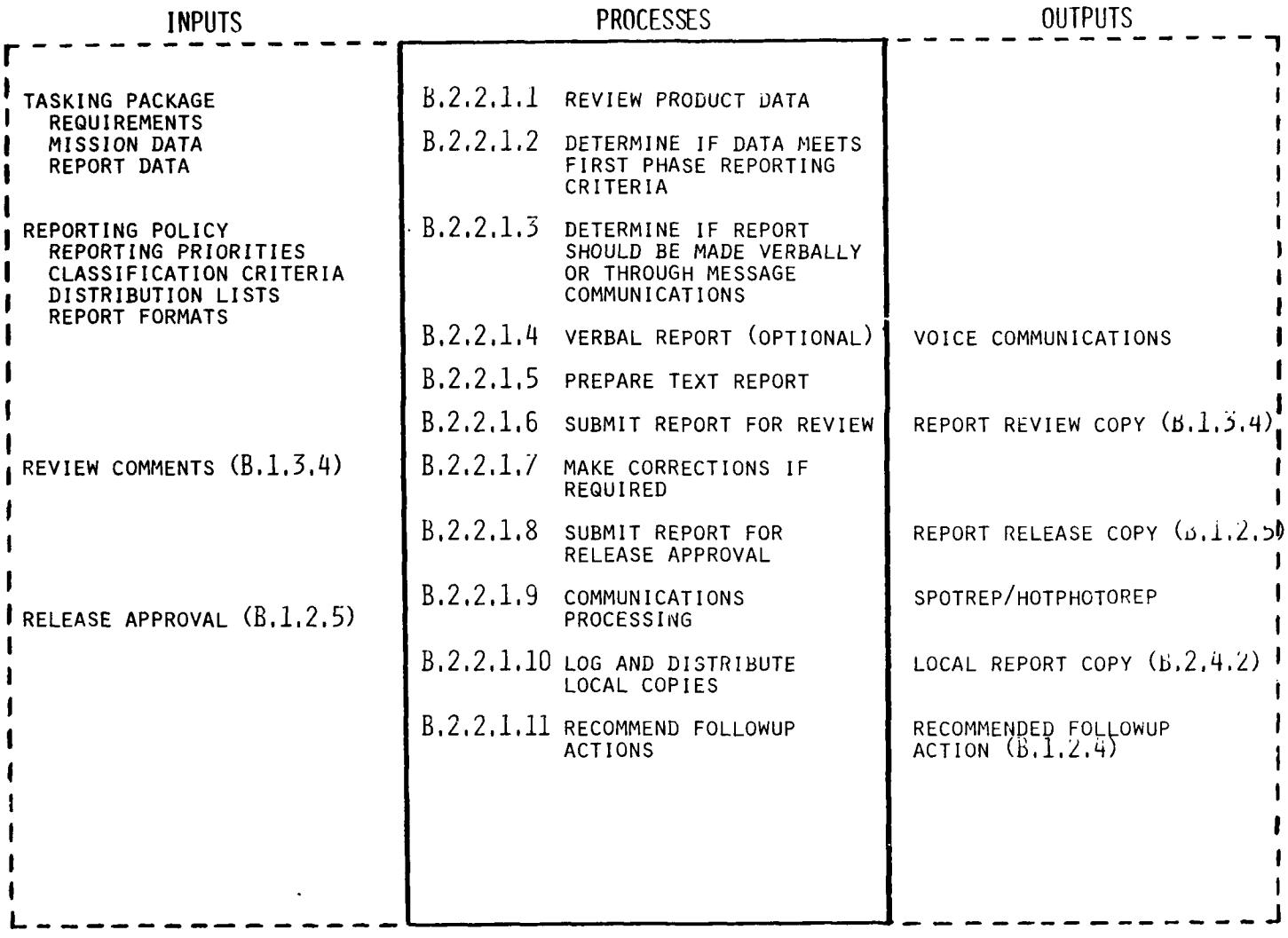
NIIRS
Previous report references (optional)
Follow-up information (optional)

Release authority

Access control information
Distribution list
Communication channel data
Report reference

The imagery interpretation report as an information entity can be viewed from the perspective of the mission, the target, the tactical or strategic threat significance, security, classification, and communications. These different perspectives are the framework within which sets of messages are dealt with in various stages of production. These perspectives are highly significant to analysis of the information structure and data base requirements of the II facility.

B.2.2.1 FIRST PHASE REPORTING



* indicates expansion of function in following pages

B.2.2.1 First Phase Reporting

First phase reporting supports strategic Indications and Warning and current operations at the tactical level. First phase processing activities include target detection, target identification, target quantification, and unusualness analysis. These activities are scheduled with the time frame of First Phase analysis but may not result in a First Phase report unless the results meet First Phase reporting criteria.

Second and Third Phase imagery interpretation processes might result in a First Phase type of reporting if the results are of immediate intelligence significance.

Several types of reports are normally associated with First Phase reporting. Voice reports through secure communications networks are the most direct means of reporting significant items. This reporting mode is particularly effective in the tactical environment when IR or SLAR imagery interpretation is being used to exploit detection of moving targets. Verbal reports are sufficient only if the requirement is limited to a single user. Items of general interest must be recorded and reported in textual form. SPOTREPORT is a term normally associated with an in-flight intelligence report. HOTPHOTOREP is a term associated with reports resulting from the first scan of a wet or dry negative film at the completion of a mission.

First Phase interpretation products may be used to guide followup tasking in subsequent interpretation processing.

B.2.2.2 SECOND PHASE REPORTING

INPUTS	PROCESSES	OUTPUTS
TASKING PACKAGE TARGET FOLDER REPORT DATA REQUIREMENTS PHOTO ENCLOSURES GRAPHIC ENCLOSURES	B.2.2.2.1 REVIEW PRODUCT DATA	
	B.2.2.2.2 REVIEW REQUIREMENTS AND RANK SIGNIFICANCE OF DATA	
REPORTING POLICY REPORTING PRIORITIES CLASSIFICATION CRITERIA DISTRIBUTION LISTS REPORTING FORMATS	B.2.2.2.3 DETERMINE REPORTING VEHICLE(S)	
FIRST PHASE REPORTS	B.2.2.2.4 MAKE VERBAL REPORT IF APPROPRIATE	VOICE COMMUNICATIONS
AIRCREW DEBRIEFING REPORT	B.2.2.2.5 PREPARE TEXT REPORT	
	B.2.2.2.6 SUBMIT REPORT FOR REVIEW	REPORT REVIEW COPY (B.2.3.4)
REVIEW COMMENTS (B.1.3.4)	B.2.2.2.7 MAKE CORRECTIONS IF REQUIRED	
	B.2.2.2.8 SUBMIT REPORT FOR RELEASE APPROVAL	REPORT RELEASE COPY(B.1.2.5)
RELEASE APPROVAL(B.1.2.5)	B.2.2.2.9 COMMUNICATIONS PROCESSING	IPIR,GPIR,MIPIR,MISREP
	B.2.2.2.10 LOG AND DISTRIBUTE LOCAL COPIES	LOCAL REPORT COPY (B.2.4.2)
	B.2.2.2.11 RECOMMEND FOLLOWUP ACTIONS	RECOMMENDED FOLLOWUP ACTIONS (B.1.2.4)
	B.2.2.2.12 HOLD ITEMS FOR SUMMARY OR HIGHLIGHT REPORTS	

* indicates expansion of function in following pages

B.2.2.2 Second Phase Reporting

Second Phase reporting would nominally occur within 24 hours after receipt of imagery. A 24-hour cycle is consistent with mission scheduling during daylight hours and exploiting of Second Phase production products for current operations planning in the tactical environment.

Individual products or responses to specific requests for image interpretation products may be produced much sooner and reported when available. Other products may be delayed by workload and preemption by higher priority tasks.

Second Phase reports generally are transmitted as messages but may have accompanying photographs or graphics. Verbal reports may be used to satisfy special requirements with limited distribution. Data produced by Second Phase processing generally has a wide distribution through message communication networks. Not all users are interested in the same level of detail, so the II facility generally sorts reporting items by significance for immediate reporting, daily reporting, weekly reporting, highlighting, or summary type reports. Sorting of reportable products for these types of reports may be done on the basis of mission, geographic area, target type, or other predetermined criteria.

Since Second Phase interpretation products may be accumulated, summarized, and extracted from at the reporting stage, there must be a means of temporarily holding product data. This is normally accomplished through transfer of target folders or tasking packages which contain requirements, mission data, processing results, and appropriate enclosures. Automated data processing

systems have been utilized within the larger national level facilities to manage the requirements, tasking, mission, and text reports produced during Second Phase processing. Report preparation is likely to be done by a person other than the II analyst that performed the analysis.

Typical reporting forms for Second Phase products are:

IPIR Immediate Photo Interpretation Report

SUPIR Supplemental Photo Interpretation Report

GPIR General Photo Interpretation Report

MIPIR Machine IPIR (Computer-generated report)

MISREP Mission Report

All but the MISREP generally follow the same standardized Military Message Format. The MISREP is limited to tactical environments and includes a summary of all pertinent flight parameters, sensor parameters, aircrew observations, and summary of imagery interpretation results.

B.2.2.3 THIRD PHASE REPORTING AND PRODUCT OUTPUT

INPUTS	PROCESSES		OUTPUTS
TASKING PACKAGE TARGET FOLDER/DATA REPORT DATA REQUIREMENTS PHOTO ENCLOSURES GRAPHIC ENSLOSURES MAP ENCLOSURES REFERENCES	B.2.2.3.1	REVIEW PRODUCT DATA	
REPORTING POLICY	B.2.2.3.2	DETERMINE REPORTING VEHICLE OR PRODUCT FORM	
	B.2.2.3.3	VERBAL REPORT (OPTIONAL)	VOICE COMMUNICATIONS
	B.2.2.3.4	PREPARE TEXT REPORT	
	B.2.2.3.5	SUBMIT GRAPHICS AND PHOTOCOPY TASKS	GRAPHICS AND PHOTOCOPY TASKING (B2.4.3)
	B.2.2.3.6	ASSEMBLE FINAL PRODUCT FORM FOR REVIEW	REPORT/PRODUCT REVIEW COPY (B.1.3.4)
	B.2.2.3.7	MAKE CORRECTIONS IF REQUIRED	
	B.2.2.3.8	SUBMIT PRODUCT FOR RELEASE APPROVAL	PRODUCT RELEASE COPY(B.1.2.5)
	B.2.2.3.9	COMMUNICATIONS OR PUBLICATION PROCESSING	DSIIR BIIR BRIEFINGS INTERPRETATION KEYS IDENTIFICATION POSTERS MOSAICS
	B.2.2.3.10	LOG AND DISTRIBUTE LOCAL COPIES	II FACILITY PRODUCTION PLANNING DOCUMENTS
	B.2.2.3.11	RECOMMEND FOLLOWUP ACTIONS	RECOMMENDED FOLLOWUP ACTIONS (B.1.2.4)

* indicates expansion of function in following pages

B.2.2.3 Third Phase Reporting and Products

The greatest diversity in reporting forms occurs in Third Phase II processing. Responses to tasking can be anything from a yes/no answer to a detailed document with enclosed graphics and photocopies Distribution of products may be highly selective and directed on an analyst to analyst basis. If the product is basic intelligence the report may be published as general intelligence information and receive wide distribution.

The suspense time for producing Third Phase reports may range from several days to periodic updates of basic intelligence spanning several years. Third Phase processing requires much greater use of collateral and all-source intelligence materials. All forms of imagery are exploited, and utilization of technical exchanges between intelligence analysts in different fields is possible because of the extended time available for analysis.

Information sources and reporting channels tend to be informal as well as formal. Third Phase imagery interpretation introduces a wider range of products besides written reports including:

Direct Support Imagery Interpretation Reports (DSIIR)

Basic Imagery Interpretation Reports

briefings

imagery interpretation keys

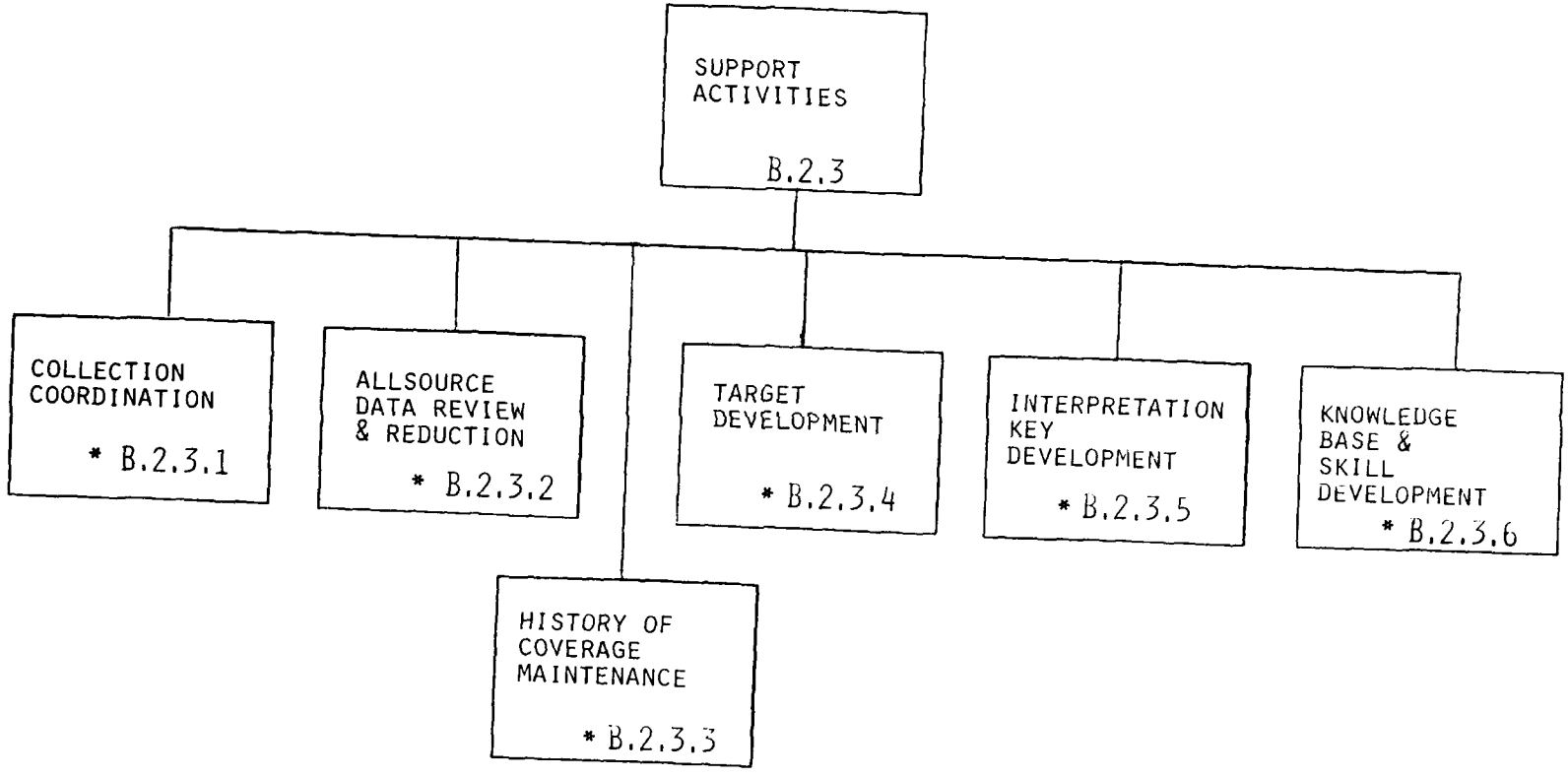
target identification posters

mosaics

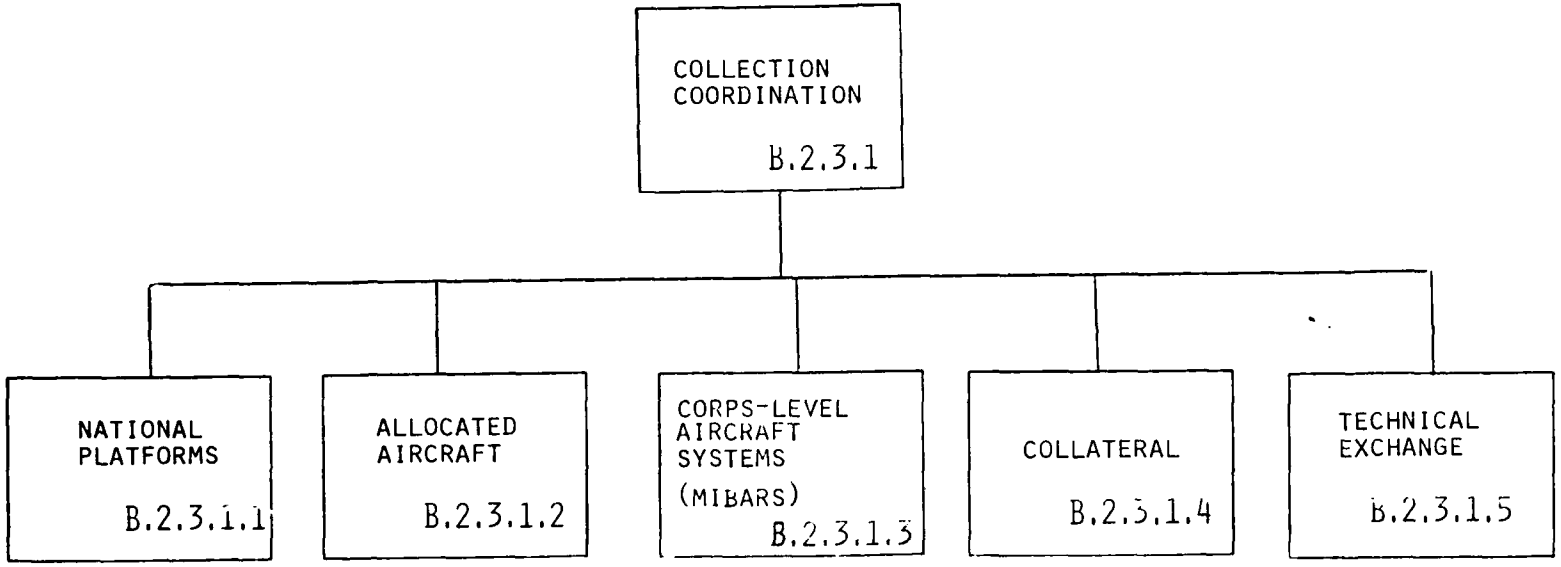
II facility production planning documents

The division of labor for Third Phase processing activities follows specialty lines including the area of product preparation. Specialized support is provided for graphics and photocopies which are used extensively for Third Phase products.

One of the products of Third Phase processing is the technology to sustain the capabilities of the overall imagery interpretation mission. Imagery interpretation keys, updates to operating procedures, technical exchange between analysts, and individual skill and knowledge base development are products that aid in adapting to new requirements and improving current capabilities.



* INDICATES EXPANSION OF DETAIL IN FOLLOWING PAGES


COLLECTION COORDINATION
B.2.3.1
NATIONAL PLATFORMS
B.2.3.1.1
ALLOCATED AIRCRAFT
B.2.3.1.2
CORPS-LEVEL AIRCRAFT SYSTEMS (MIBARS)
B.2.3.1.3
COLLATERAL
B.2.3.1.4
TECHNICAL EXCHANGE
B.2.3.1.5

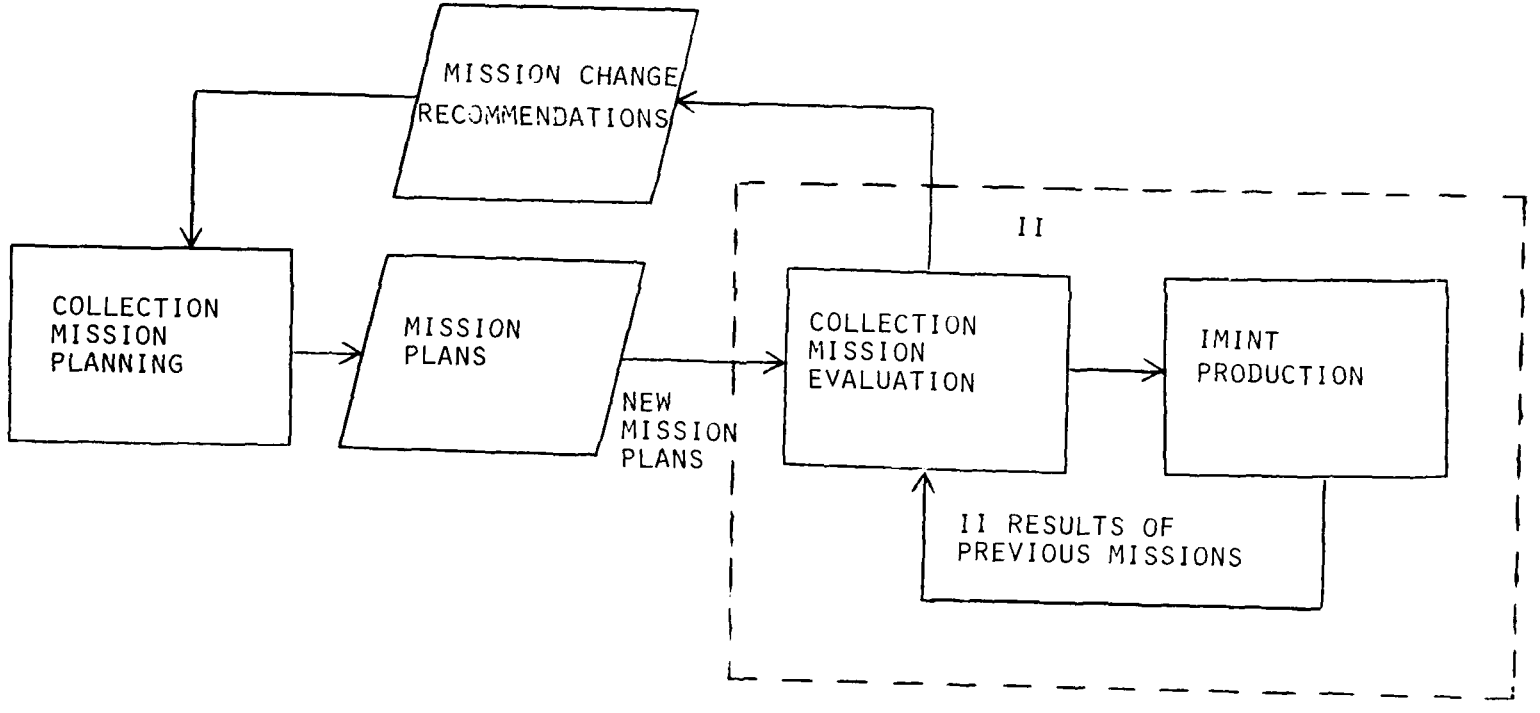
B.2.3.1 Collection Coordination

From the perspective of the IMINT production model, exploitation of collection capabilities is more of a concern than the control of collection itself. The II facility does not control collection operations or assign collection missions. However, the II facility exerts a high degree of influence on the planning of imagery collection missions through information which helps maximize the exploitation of imagery intelligence. This influence is exerted through a feedback mechanism in which the II facility manager informs the mission planner of his ability to meet production requirements with the planned collection missions. Mission planning is nearly always a limited resource problem, where an attempt is made to achieve maximum intelligence value. The feedback from the II facility to the imagery collection mission planner influences the selection of type of coverage, frequency of coverage, and priority of mission. Evaluation of previous mission results may be brought into the mission planning process where weather conditions inhibit interpretation or unusual activity is detected.

The importance of collection coordination in the imagery interpretation production model hinges on the flow of mission planning information to the II facility and the feedback of mission evaluations and recommendations to the collection planner. The benefits of this information exchange are greatest when the imagery collection missions are controlled in near real time.

As in any feedback control system, responsiveness is constrained by the delay in the feedback loop. Since the II analyst is the critical component in this loop, faster feedback can be achieved when the II analyst has an awareness of planned missions. II analysts interviewed were able to cite instances where they were able to coordinate changes in new missions in order to exploit results of newly processed imagery or adapt missions to new requirements. Filtering of information through chain of command has a dampening effect on this feedback mechanism. However, the time delay due to chain-of-command filtering can be minimized if collection coordination is implemented as a monitoring and technical exchange function and not as a formal interface.

B.2.3.1 COLLECTION MISSION COORDINATION



The particular communication channel used for coordinating collection missions depends on the collection system used and the controlling agency. Typically this communication channel is from the IMINT production manager to a liaison officer within the mission planning group. For strategic missions, an Army IMINT production facility has representation via OACSI on national level tasking committees and liaison with all U. S. intelligence agencies. In support of a theater of operations, the IMINT production unit may have the collection services of special aerial surveillance aircraft that are allocated for use on a mission per unit time basis. At the tactical level, both Army corps and division commanders will require imagery interpretation support. The MIBARS* does not have any organic collection assets. Allocation of collection assets is coordinated through the G-2 Air in the Tactical Operations Center. The G-2 will be cognizant of both division and corps level IMINT production capabilities. The G-2 will also coordinate the prioritization and allocation of collection assets for meeting the needs of Corps and Division commanders.

The MIBARS detachments interface directly with the tactical squadrons (Mohawk or AF tactical reconnaissance) that fly the missions through the Air Reconnaissance Liaison Officer (ARLO), who will be collocated with the tactical unit. In some cases, one or more MIBARS detachments may be resident at the tactical air base with the reconnaissance aircraft. The MIBARS has U-8 and U-21 aircraft for use in pickup and delivery of film or imagery products.

Mission coordination at the tactical level includes two additional activities:

(1) Pre-flight briefings of pilots on requirements and threats (responsibility of ARLO)

(2) In-flight mission coordination to exploit real-time imagery transmitted to ground interpretation stations.

The scope of interpretation that can be performed by an II is heavily dependent on awareness brought about by exposure to collateral intelligence and awareness of other intelligence activities and capabilities. This category of information is extremely broad and includes HUMINT and open source

*Military Intelligence Battalion Air Reconnaissance Support

materials. Characteristically, it is at the II analyst's own initiative that these materials are collected, organized by area of interest, and applied to the imagery interpretation process.

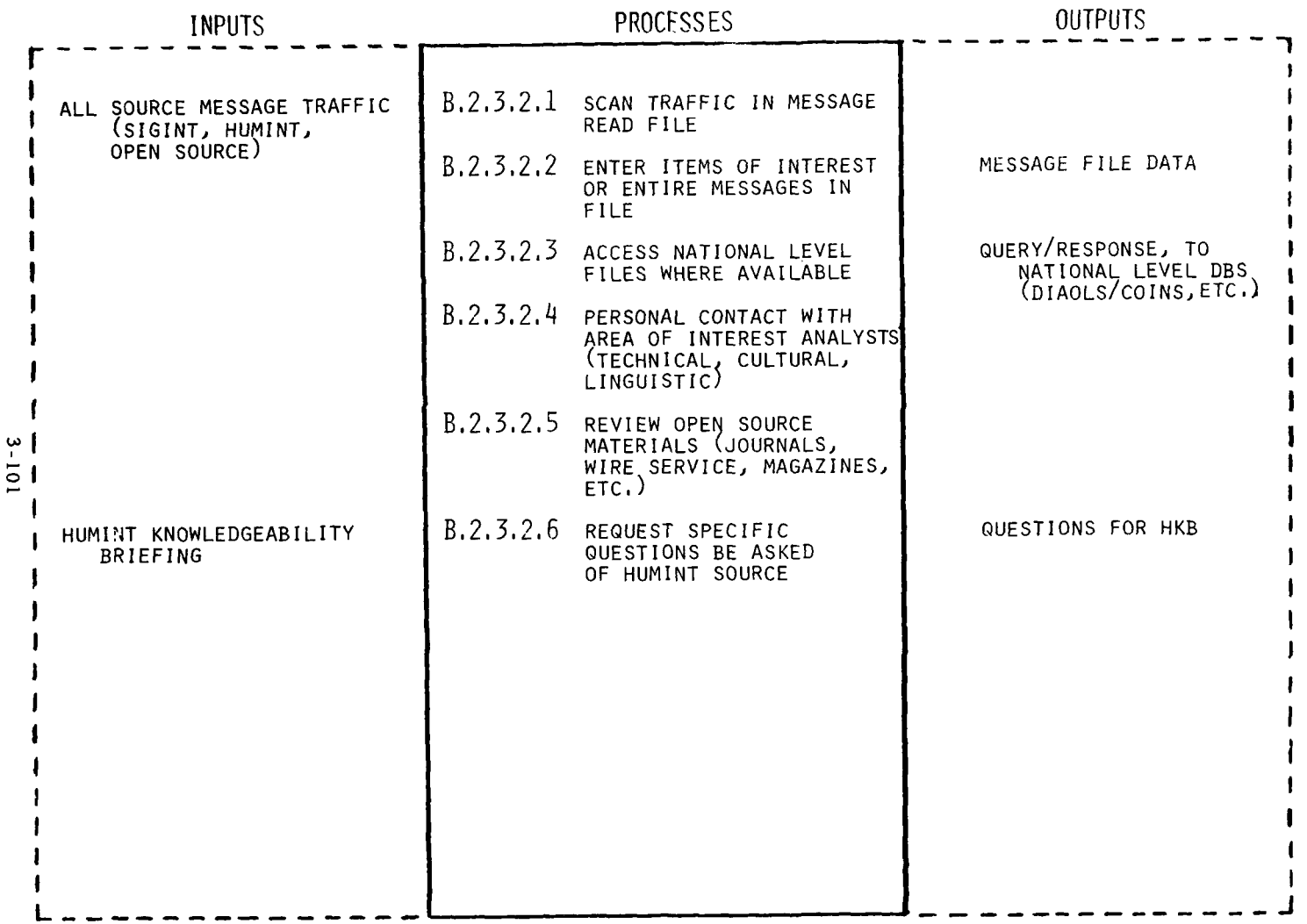
In many cases the collateral materials work in an indirect manner, such as open-source photographs of non-military targets which aid in screening potential military targets in surveillance photography. Collateral materials such as HUMINT intelligence reports can identify general areas and types of military targets that are to be searched for and identified through image interpretation.

In terms of the IMINT Production model, collection of collateral intelligence materials is of concern from the following perspectives:

(1) Are there means of formal representation of an II analyst's area of interest for screening useful collateral materials?

(2) How can the content and application of collateral materials be represented in terms of entry points to a data base that can be managed and exploited by the overall IMINT production facility?

B.2.3.2 ALL SOURCE DATA REVIEW AND REDUCTION



* indicates expansion of function in following pages

B.2.3.2. All Source Data Review and Reduction

An IIA is essentially an entrepreneur whose success or failure depends upon his own intelligence, intuition, and aggressiveness in the pursuit of information. Although some national level imagery interpretation resources such as NPIC have a position dedicated to collateral research in each branch, most image interpreters carry out their own collateral and all source research. In general, IIAs will receive message traffic presumably relevant to their particular imagery interpretation area, but in most cases, such traffic does not come to them directly, but must be selected by individual image interpreters from the volume of traffic disseminated to a particular group or element. Similarly, data reduction from this volume of traffic is carried out by individual IIAs, who conduct a continuous 'reconnaissance' for particular items of interest in their area of responsibility. In the case of the national resources, some of this burden of continued awareness toward new information from any source is alleviated by the message, installation and target data bases existing at this level, but generally speaking, the IIA is his own information researcher.

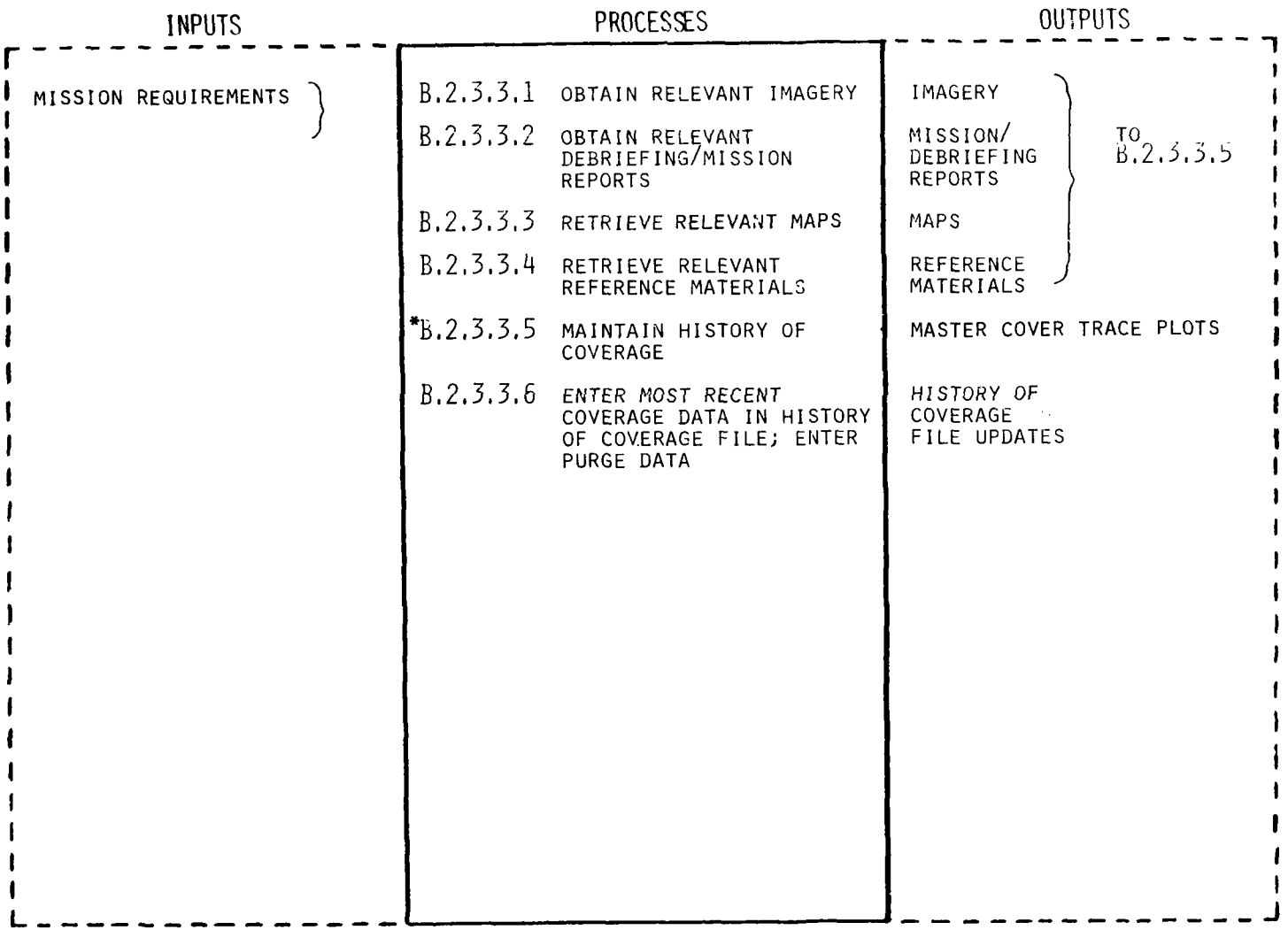
The IIA may have the opportunity to gain directly related intelligence information through personal contacts with other analysts in other intelligence disciplines with interests in the same targets (e.g., SIGINT, OB areas). The IIA is in turn an informal information source to those analysts.

Queries to national or theater level data bases can be made directly if terminals are available or indirectly through a support group.

Analysts may have interaction with HUMINT sources indirectly through HUMINT knowledgeability briefings or directly where they are collocated with an IPW group.

Interviewed analysts gave examples of Vietnam experiences in which imagery analysts were able to provide cues to interrogators for lines of questioning.

B.2.3.3 HISTORY OF COVERAGE MAINTENANCE



* indicates expansion of function in following pages

B.2.3.3 History of Coverage Maintenance

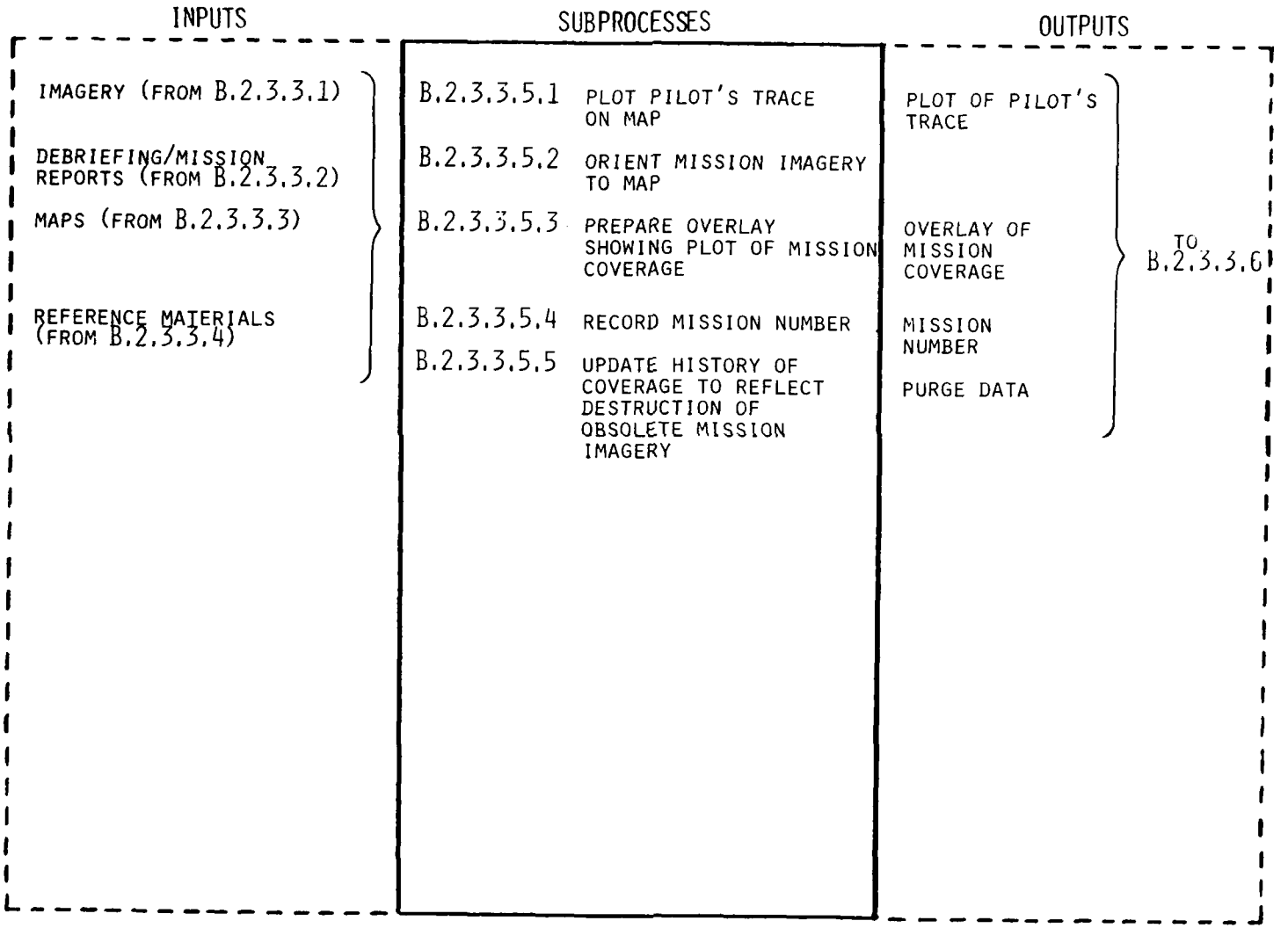
An extremely important support activity of the imagery interpretation process is the generation and maintenance of a detailed history of all imagery on hand -- that is, the support of a history of coverage file.

In the tactical area, such a history is maintained in terms of the so-called 'Master Cover Trace', a basic map with all associated missions represented in terms of the pilot's trace, or flight line flown by the airborne platform, and related debriefing and mission report indexes. On the national level, most coverage data is maintained by automated systems designed for this purpose.

In second and third phase II processing, past imagery coverage is extremely important in change detection and performing negation analysis when a target is detected.

Because of large volumes of imagery that can be accumulated by a facility with an active mission, a library capability -- often a rudimentary one constrained by the availability of important personnel, and storage -- is required for storage, indexing (by mission, target, location), and control of film and hardcopy materials.

B.2.3.3.5 MAINTAIN HISTORY OF COVERAGE

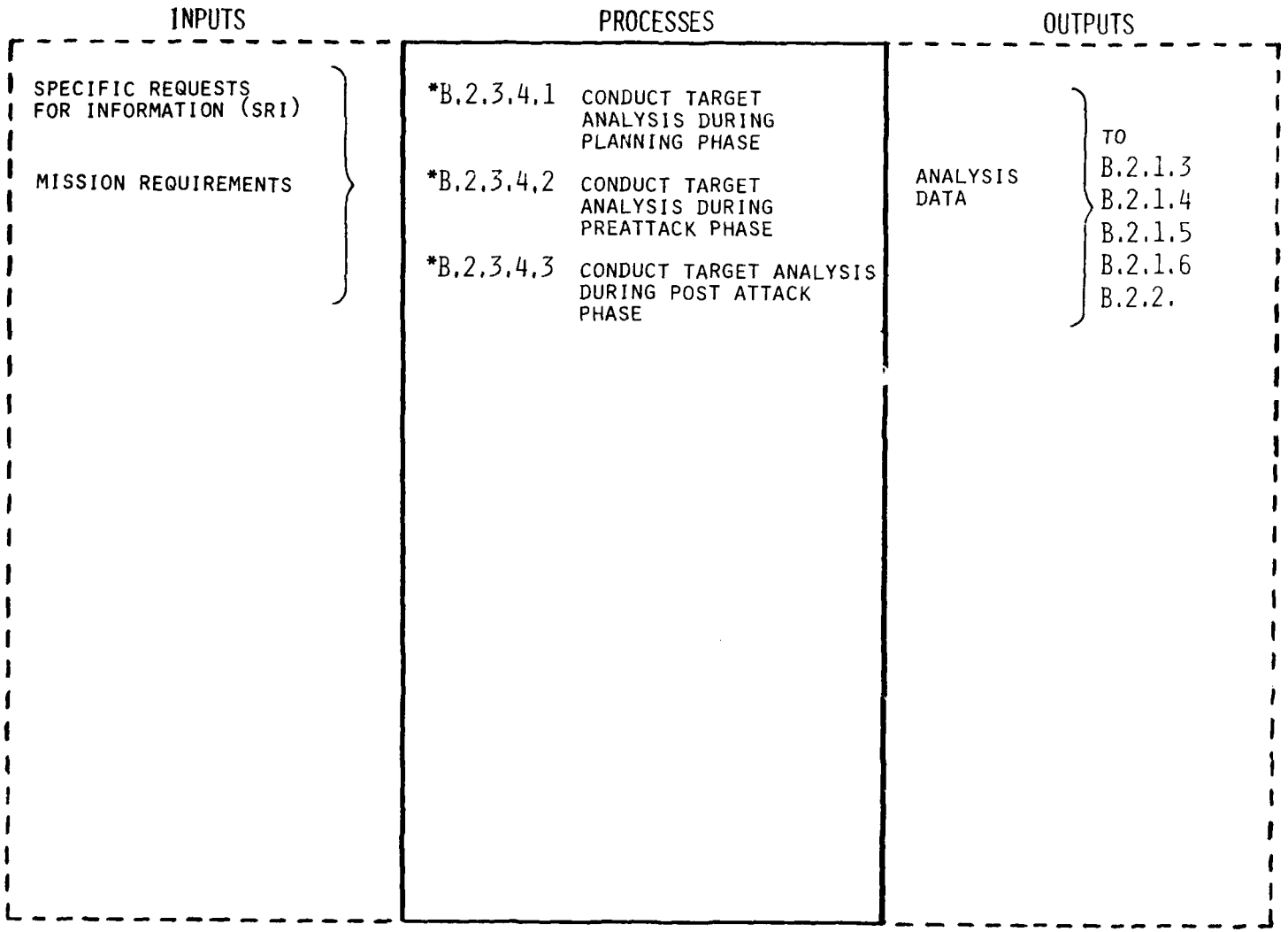


* indicates expansion of function in following pages

B.2.3.3.5 Maintain History of Coverage

The basic subprocesses involved in this activity are the relation of a particular mission flown by a given aircraft to a map designating the coverage of a particular geographic area, the update of such a master cover record in terms of each new mission flown, and the amendment of mission records to reflect eventual purge and destruction of associated imagery, as it becomes obsolete.

B.2.3.4 TARGET ANALYSIS/DEVELOPMENT

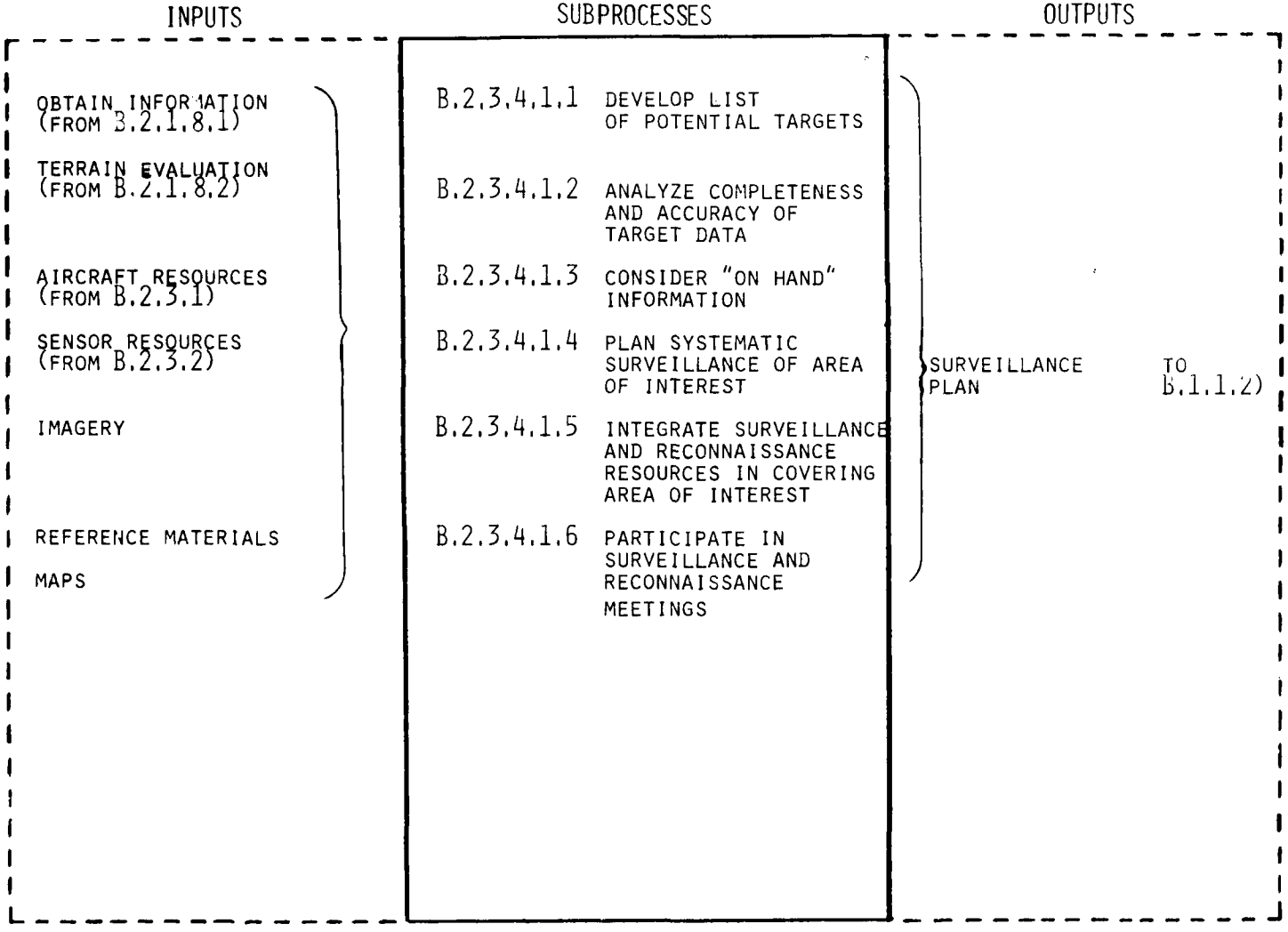


* indicates expansion of function in following pages

B.2.3.4 Target Analysis/Development

Although target analysis and development is being continually carried out on the strategic level in the areas of foreign technology assessment and other scientific and technological areas, target analysis and development processing on a tactical level tends to be more oriented toward a specific objective and associated plans of attack. In the following discussion and the associated charts, the tactical view is treated.

B.2.3.4.1 CONDUCT TARGET ANALYSIS DURING PLANNING PHASE



* indicates expansion of function in following pages

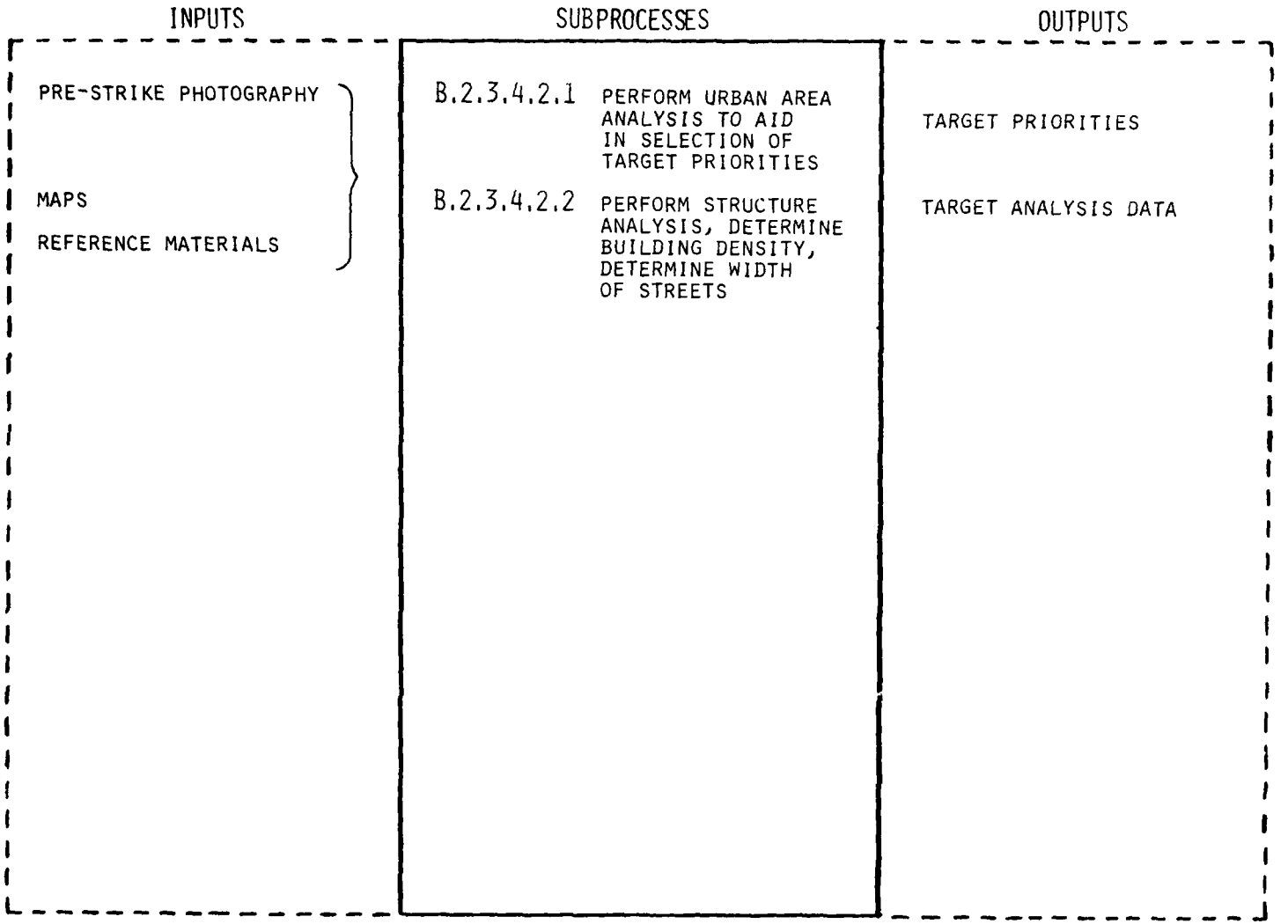
B.2.3.4.1 Conduct Target Analysis During Planning Phase

In a tactical situation, for any given state of affairs in crisis or wartime, the processing associated with the development of detailed information on targets begins with the creation of an inventory of potential targets in the affected area relevant to the planned attack. The initial steps involve an assessment of the completeness and accuracy of target data immediately available, and on hand within a given targeting information system.

This initial review of available information is followed by a planning phase aimed at developing additional required information -- essentially, the filling in of the variety of gaps which may exist in target information -- by systematic surveillance of the area or areas of immediate military interest.

This plan for systematic surveillance of areas of interest for particular elements must then be integrated with other similar plans generated by other elements in order to provide for an integration of surveillance and reconnaissance resources in providing the desired coverage of the area(s) of interest.

B.2.3.4.2 CONDUCT TARGET ANALYSIS DURING PRE-ATTACK PHASE



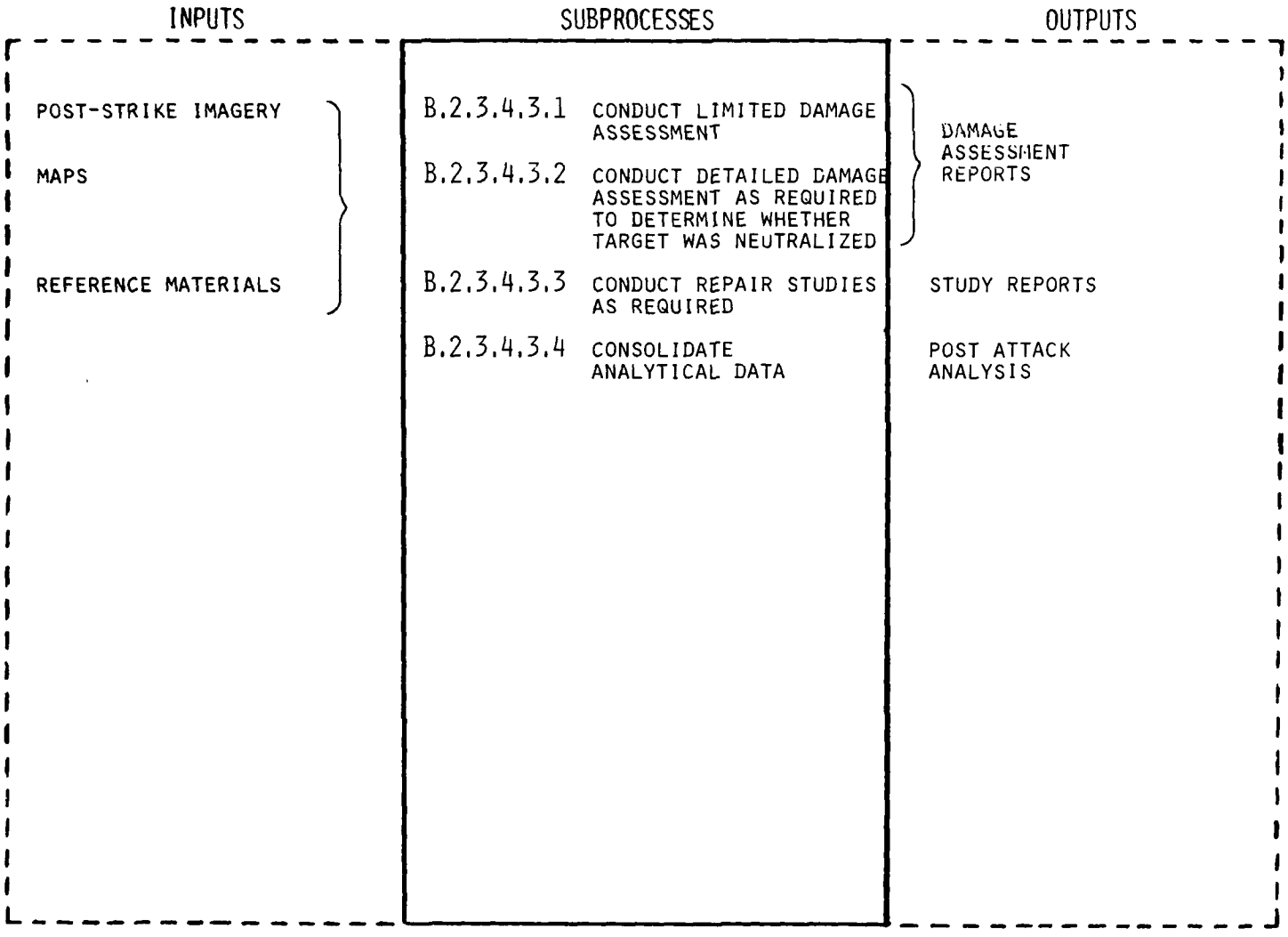
* indicates expansion of function in following pages

B.2.3.4.2 Conduct Target Analysis During Pre-Attack Phase

In the pre-attack phase of tactical operations, particular attention is devoted to urban area analysis, as a basis for selecting target priorities for attack forces, assuming urban targets of interest in the combat area.

Detailed urban area analysis calls for structural analysis of buildings to determine height, degree of reinforcement, special characteristics, such as built-in air raid or nuclear shelters, observation points, and the like, density of building structures in various sectors of the urban area, width of streets and trafficability for armored forces of various types, population density by sector, etc.

B.2.3.4.3 CONDUCT TARGET ANALYSIS DURING POST-ATTACK PHASE

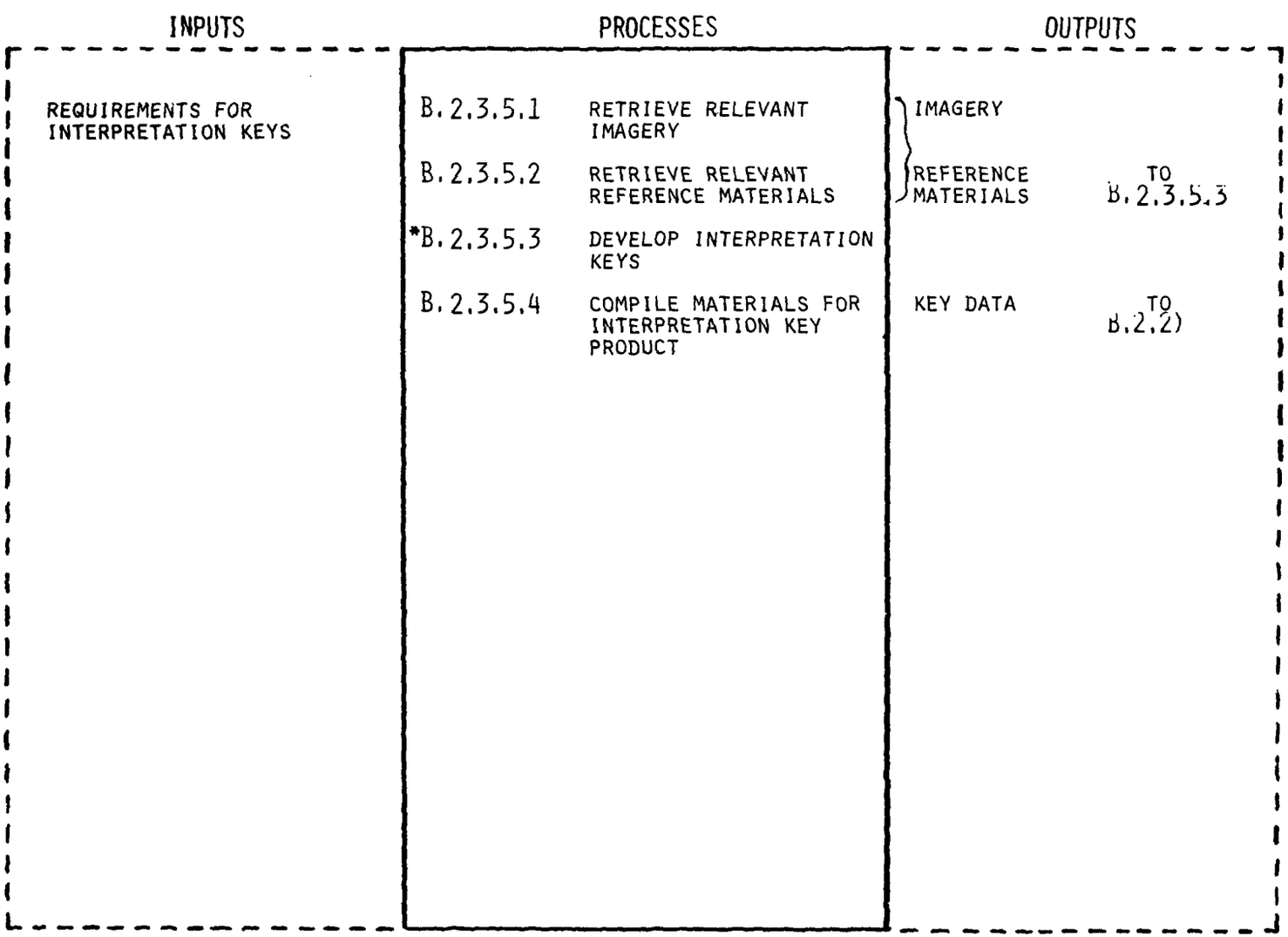


* indicates expansion of function in following pages

B.2.3.4.3 Conduct Target Analysis During Post Attack Phase

Target analysis in a tactical level post-attack context is primarily concerned with assessing the amount of damage inflicted by the given attack, evaluation of suppression or neutralization of a particular target, and estimates of repairs involved before the particular target facilities can become operational again.

B.2.3.5 INTERPRETATION KEY DEVELOPMENT

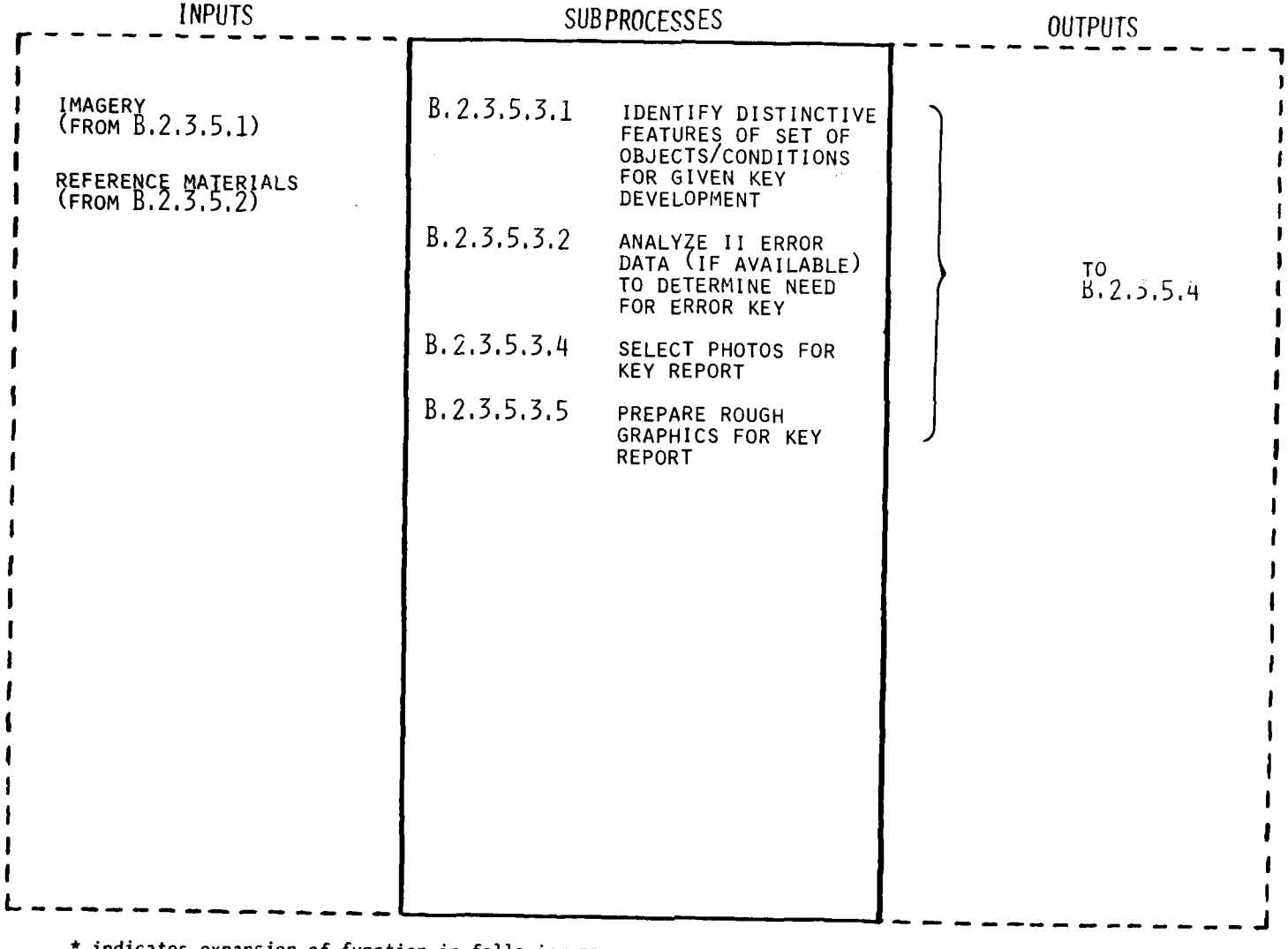


* indicates expansion of funct ı in following pages

B.2.3.5 Imagery Interpretation Key Development

On the level of the national imagery interpretation resources, development and maintenance of aids to the imagery interpretation process is an important research area. Based on all available materials -- including all source message traffic and hard copy reports, as well as all types of imagery relevant to the particular object, equipment, condition, or characteristic -- the objective is to develop concise and accurate materials for distinguishing items of known or potential military significance.

B.2.3.5.3 DEVELOP INTERPRETATION KEYS



* indicates expansion of function in following pages

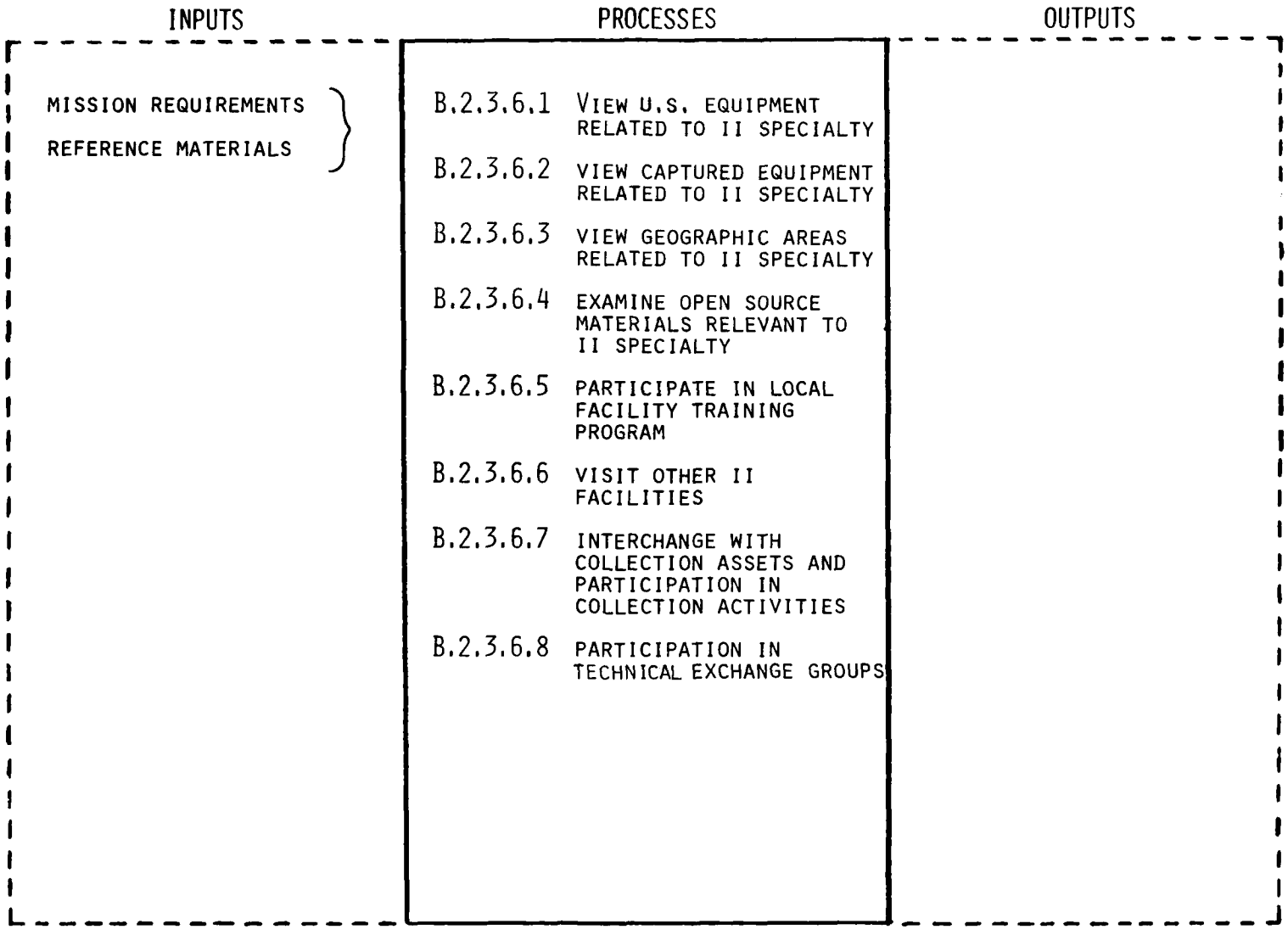
B.2.3.5.3 Develop Interpretation Keys

In developing a key for a particular set of objects, special care is devoted to identification and specification of features distinguishing different members of the given set. To illustrate: in the distinction of members of the set of U. S. Army trucks, an important distinctive feature is existence of an engine hood (distinguishes infantry weapons carrier versus cargo trucks), and number of bows on the top (cargo vehicles of differing capacities).

A related consideration involves the requirement for error keys (discussed under B.2.1.4) to avoid misidentification of items of military significance as non-military items which exhibit considerable similarity in structure, and conversely, the misidentification of non-military items as objects or charcteristics of military significance.

The materials developed in the light of these guiding principles will form chapters of the imagery interpretation documentation currently under development, and will utilize the best of available imagery supplemented by artist drawn graphics in a readily comprehensible format to provide effective imagery interpretation aids.

B.2.3.6 KNOWLEDGE BASE AND SKILL DEVELOPMENT



* indicates expansion of function in following pages

B.2.3.6 Knowledge Base and Skill Development

The training, maintenance, and enhancement of an image interpreter's skills and abilities is of paramount importance to effective, reliable, imagery interpretation at all levels. At the national level, in addition to the customary training and proficiency maintenance programs, image interpreters are involved in programs for enhancing their effectiveness and ability by a series of travel programs aimed at exposing them to U. S. equipment or developments related to their specialty, at viewing captured equipment in an environment similar to the actual operational environment in which it functions, and at viewing geographic areas similar to those in the image interpreter's area of responsibility. Moreover, image interpreters are provided with a variety of open source materials which complement and supplement the imagery they are required to interpret. Although such intensive programs do not currently exist on the level of the tactical image interpretation element, the need for them is widely recognized.

Formal Training

Formal training in general II skills is not available for all skill levels in the Army 96D II specialty. The USAICS II courses at Fort Huachuca cover only skill levels 1 and 2 plus the 35C officer course. The enlisted course for skill level 1 addresses 22 basic field skills:

(1) Security

(2) Photo interpretation

(3) Code matrix

(4) PI slide rule

(5) Photogrammetry

(6) Overlay preparation

(7) Plotting

(8) Terrain

(9) Road classification

(10) Bridges

(11) Ports, Harbors, Inland Waterways

(12) Railroads

(13) Airfields

(14) Tactical identification

(15) Installations

PRECEDING PAGE BLANK - NOT FILMED

(16) Order of Battle

(17) SLAR

(18) IR

(19) Mosaics

(20) Reports

(21) References

(22) TIIF

These courses introduce the novice II to the field but do not fully prepare the individual for an operational role. Unit training and apprenticeship type experience are expected to qualify the II for an active role in the II production process.

Advanced schools such as the DSIATP at Offutt Air Force Base or the NPIC school are aimed primarily at analysts going into assignments within national level organizations. These programs must cover military doctrine and technical subjects as well as imagery interpretation technique. Students in general will not have sufficient field experience, prior training, or technical backgrounds to permit the courses to focus exclusively on technique. Organization of the advanced courses is substantially different from basic courses in orientation toward target types. The segments taught at Offutt are:

Introduction

Military Geography

Photogrammetry

Ground Forces

Strategic Industries

Electronics

Offensive Missiles

Air Forces

Defensive Missiles

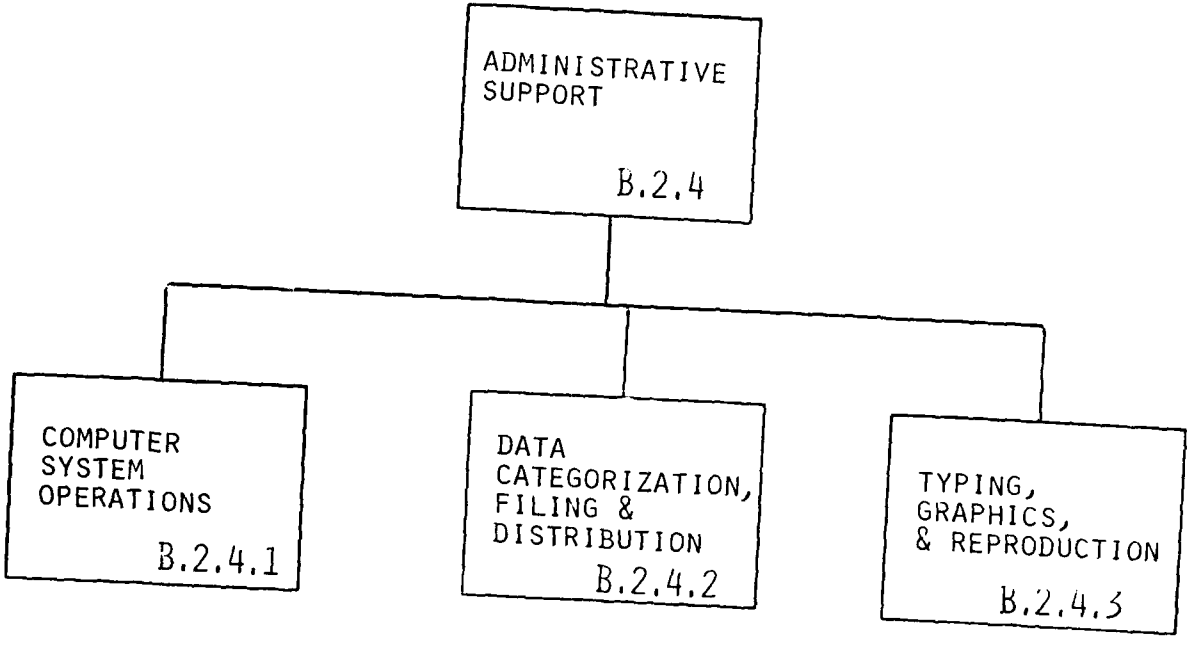
Naval Forces

Unit Training

A graduate of the DSIATP school has been trained to think like an imagery interpreter but unless his DSIATP training was preceded by relevant operational experience, he will not be capable of assuming responsibility for an active mission until he receives additional unit training at his next assignment. It is left to unit training to convey the "big picture" knowledge and tricks of the trade to the inexperienced.

Staff rotation also creates a need for the same type of unit training. It was frequently stated by interviewed analysts, that overlap time between beginning and leaving personnel was insufficient to pass along the legacy of past experience, thereby creating a necessity for self-taught skills and knowledge. An agressive, motivated analyst considers this type of environment as a professional challenge especially when supportive assistance and positive feedback are provided by management and peers.

Image interpretation was described by an advanced training instructor as essentially "an oral tradition". One image interpreter learns from another by working with him and talking about his methodology. Moreover, experienced image interpreters seem to share a special concern for informal training of novice image interpreters. Thus, although the importance of formal training cannot be underestimated, much of the image interpreter's skill derives from informal, learning, relationships with other II's.


ADMINISTRATIVE SUPPORT
B.2.4
COMPUTER SYSTEM OPERATIONS
B.2.4.1
DATA CATEGORIZATION, FILING & DISTRIBUTION
B.2.4.2
TYPING, GRAPHICS, & REPRODUCTION
B.2.4.3

B.2.4 Administrative Support

Administrative support processes in the II facility are tailored to suit the production level, mission, and data processing needs.

B.2.4.1 Computer System Operations

Operation of computer systems which support the management of tasking, production data, or data bases can be considered as falling within this category. Tasking would include computer system operator functions (starting, shutdown, configuration control, diagnostics, etc.) data entry, data base management, report generation, and user assistance. Use of computers for administrative support in II facilities is mostly restricted to national level facilities, at the current time. Field level use of computers such as in the TIIF is mainly for computational applications. Future systems will make extensive use of computers for communications and data base management as well as computation.

B.2.4.2 Data Categorization, Filing, and Distribution

An important administrative task is the handling of materials coming into the facility, generated within the facility, and leaving the facility. Major categories of material include:

- Procedures
- Handbooks
- Manuals
- Technical References
- Maps
- Requirements (message, letter, etc.)
- Handheld photography
- Mission film
- Open source technical journals, books, magazines, newspapers, wire service stories
- Intelligence reports
- Message traffic
- Technical exchange memoranda
- Production schedules
- Photocopy/graphic requests
- Imagery duplicates
- Personnel and equipment status
- Weather data
- Coverage history file
- Product file
- Target folders
- Mission data
- Collection Plan
- Sensor capabilities
- Intelligence analyst directories
- All-source intelligence materials

Much of the responsibility for collecting, categorizing and filing these materials rests with the analysts and control of the process may be informal along lines of interest. However, on a broad scale, informal control results in a much narrower range of materials available to individual analysts, awareness of other intelligence information is lost, and duplication of efforts cannot be controlled.

The availability of automated data processing technology has had an impact in two important aspects of this function. First, it has made it possible to maintain an integrated data base of mission parameters, tasking, and output reports. This data base capability alone has greatly improved the productivity and responsiveness of the II facility and helped eliminate duplication of effort.

The second area where automated data processing is beginning to have an impact is in the area of accessing and distributing intelligence materials on the basis of content. An automated data base containing past imagery coverage that can be searched by location parameters, time, or mission number is extremely valuable in exploiting previous missions. On a broader scale, all-source intelligence can be made more readily available for exploitation in the imagery interpretation process if it is available in a computerized file that is searchable by:

location parameters

country name

place name

time

keywords

Certain types of all-source intelligence materials are searchable in data bases maintained at the national level. Access is limited to special terminals, some which can be connected remotely through communication channels. Multiple terminals and query languages are required to access the host computer systems that maintain these data bases. Frequently, a specialist is required to operate the terminal systems for the analyst without time to learn the protocols and peculiarities of the different systems.

One means of distributing time-critical requirements and intelligence information is through global message communication networks that are accessible by every II facility. Current Army tactical facilities interface with the message communication network through hardcopy for both sending and receiving. New automated message handling technology which is in use at the national level and in prototype tactical facilities provides a direct interconnection to the world wide message communication network from computer terminals. Using these automated systems, image interpreters and other intelligence analysts can review intelligence reports or other message traffic relevant to their work area. Most time critical intelligence information passes through the message handling network, either when first generated or as an exploitation product. Message dissemination technology has been developed for automatic monitoring of the message traffic flow, filtering out relevant messages, and filing these messages for subsequent use in intelligence processing. This technology would replace the existing manual operation in the II facility which involves each analyst in perusing stacks of hardcopy messages distributed to the facility in general.

B.2.4.3 Typing, Graphics, and Reproduction

The level of administrative support provided in the II facility for product preparation and publication is variable depending on the staff size, workload, and applicable product standards for the user community. Products which have extremely wide distribution and a longer useful life are published to higher standards. Special staffing is provided to produce graphics, photocopy, and final type for facilities which produce a substantial volume of high quality products. Most facilities have some level of administrative support for these activities to give interpreters more time for analysis tasks. Automated data processing systems are beginning to impact this area.

In new systems, analysts are being given CRT terminals for entering processing data, editing, and report generation, typically referred to as word processing systems.

Integration of the word processing capabilities, data handling, and computational capabilities in a single data processing system is being planned for future systems.

APPENDIX A

Organizations Visited During Data Collection for IMINT Production Model

1. Army Research Institute (ARI)/Human Factors Technical Area
2. HQ US Army Intelligence and Security Command (INSCOM)/IASYS
3. US Army Intelligence Center and School/Director of Training, Fort Huachuca, AZ
4. National Photographic Interpretation Center (NPIC) Imagery Exploitation Group (IEG)
5. Intelligence and Threat Analysis Center (ITAC)/Imagery Interpretation Production Division (IIPD)
6. 3428th Technical Training Squadron, Defense Advanced Sensor Interpretation and Applications Training Program (DSIATP), Offutt Air Force Base, NE
7. 525th Military Intelligence Group, Fort Bragg, NC
8. 363rd Tactical Reconnaissance Wing, Shaw Air Force Base

BIBLIOGRAPHY

---

1. Aerial Photography Airborne Sensor Imagery, Forwarding, Titling, and Plotting. DIAM 55-5, September 1971.

2. Birnbaum, A.H., Sadacca, R., Andrews, R.S. and Narva, M.A. Summary of BESRL Surveillance Research. ARI Technical Research Report 1160, September 1969. (AD 701 907)

3. Bowen, R.J., Halpin, J.A., Russell, P.T. and Staniforth, B.J. Tactical Order of Battle: A State-of the Art Survey. ARI Technical Paper 265, US ARI, October 1975. (AD A018 368)

4. Department of Defense Exploitation of Multisensor Imagery. DIAM 57-5A.

5. Department of Defense Joint Imagery Interpretation Keys Structure, Military Aircraft of the World - Part 4, Vol. XII. DIAM 57-7, June 1967. (Confidential)

6. FM 30-05G Soldier's Manual MOS 05G Signal Security Specialist. HQ Department of the Army, 1 February 1978.

7. FM 30-05H Soldier's Manual MOS 05H Electronic Warfare/Signal Intelligence Morse Interceptor. HQ Department of the Army, 1 February 1978.

8. FM 30-5 Combat Intelligence. HQ, Department of the Army, 30 October 1973.

9. FM 30-10 Field Military Geographic Intelligence (Terrain). HQ Department of the Army, March 1972.

10. FM 30-40 Handbook on Soviet Ground Forces. HQ Department of the Army, June 1975.

11. FM 30-96D Soldier's Manual MOS 96D Image Interpreter. HQ Department of the Army, 26 January 1978.

12. FM 100-5 Operations. HQ, Department of the Army, 1 July 1976.

13. Graduation Criteria for Assistant Image Interpreter Course (96D1). USAICS, 18 January 1979.

14. Graduation Criteria for Intelligence Officer Basic Tactical Surveillance (35C). USAICS, 22 March 1978.

15. Ground Forces. USAINSCOM/IASA, January 1978. (Secret)

16. Intelligence Reports Handbook. SUPR 96B1024A, USAICS, October 1976.

17. Interpret Aerial Vertical Photography - Programmed Text. USAICS, November 1977.

18. Lepkowski, J.R. Image Interpreter Performance as Affected by Resolution, Presentation Rate, and Scale. ARI Technical Paper 335, September 1978. (AD A064 262)

19. Lepkowski, J.R. and Jeffrey, T. Some Factors Affecting Mensuration Variability Among Image Interpreters. ARI Research Memorandum 72-7, September 1972.

20. Levin, J.M. and Eldredge, D. Effects of Ancillary Information Upon Photo Interpreter Performance. ARI Technical Paper 255, September 1974. (AD 785 706)

21. Martinek, H. and Bigelow, G.F. Compendium of BESRL Performance Measures for Image Interpretation Research. ARI Research Study 70-1, April 1970.

22. Martinek, H. and Hilligoss, R.E. Accuracy and Completeness of Interpretation as a Function of Time for Selected Conditions. ARI Research Memorandum 72-6, October 1972.

23. Martinek, H. and Zarin, A. The Effects of Bandwidth Compression on Image Interpreter Performance. ARI Technical Report 396, (In Press).

24. Martinek, H., Hilligoss, R.E. and Herrington, B. Effectiveness of an Error Key for Image Interpretation in Vietnam. ARI Technical Research Note 230, September 1972.

25. Sewell, E., Harabedian, A. and Jeffrey, T. Total System Accuracy for APPS (The Analytical Photogrammetric Positioning System). ARI Technical Paper 348, October 1978. (AD A063 595)

26. Side-Looking Airborne Radar - Programmed Text. USAICS, January 1978. PI Slide Rule - Programmed Text. USAICS, December 1977.

27. Soviet Ground Force Organizational Guide. USAINSCOM/IASA, February 1978. (Secret)

28. Strasel, H.C., Hansen, O.K., Colson, K.R. and L. Vettese. A Method for Developing a Laboratory Model of an Image Interpretation System (U). TRN 185, U.S. Army Behavioral Science Research Laboratory, June 1967. (Confidential)

29. Technical Report - SIGINT Production Model. The Kuras-Alterman Corp., July 1977. (Confidential)

30. Tentative Task List Authentication for Military Intelligence Officer's Advanced Course. USAICS, 24 April 1978.

31. The Role of Human Intelligence (HUMINT) in Strategic Decisions. Air War College, April 1978. (Secret)

32. United States Army Combat Developments Command Functional Area Description for Enemy Situation. USACDCINTA, December 1969. (Confidential).

33. United States Army Combat Developments Command Functional Area Description for Intelligence Collection Management, Vol. I and II. USACDCINTA, June 1969. (Confidential)

34. United States Army Combat Developments Command Functional Area Description for Order of Battle, Vol. I and II. USACDCINTA, November 1968. (Confidential)

35. Vecchiotti, R.A., Berrey, J.L. and Bedarf, E.W. Development of Resource Management Materials for the G2 Air Officer. ARI Technical Paper 333, September 1978. (AD A061 695)

36. Vecchiotti, R.A., Berrey, J.L. and Narva, M.A. Training in Utilization of Surveillance and Reconnaissance Resources by Combat Arms Officers. ARI Technical Paper 325, September 1978. (AD 061 577)

37. Youngling, E.W., Vecchiotti, R.A., Bedarf, E.W. and Root, R.T. Job Requirements of G2 Air and Image Interpretation Personnel. ARI Research Report 1181, May 1974. (AD 780 815)

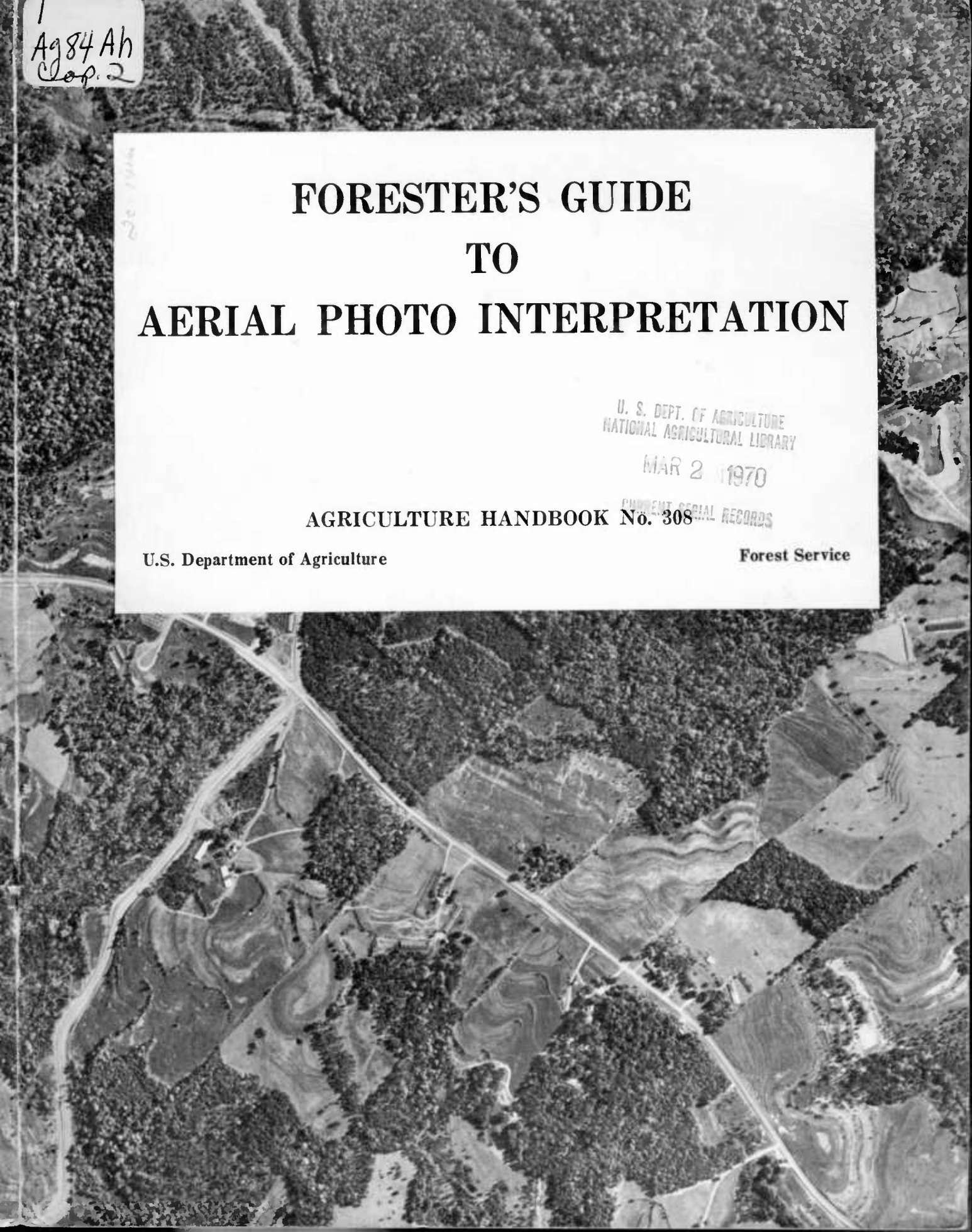
DISTRIBUTION

ARI Distribution List

4 OASD (M&RA)
2 HQDA (DAMI-CSZ)
1 HQDA (DAPE-PBR)
1 HQDA (DAMA-AR)
1 HQDA (DAPE-HRE-PO)
1 HQDA (SGRD-ID)
1 HQDA (DAMI-DOT-C)
1 HQDA (DAPC-PMZ-A)
1 HQDA (DACH-PPZ-A)
1 HQDA (DAPE-HRE)
1 HQDA (DAPE-MPO-C)
1 HQDA (DAPE-DW)
1 HQDA (DAPE-HRL)
1 HQDA (DAPE-CPS)
1 HQDA (DAFD-MFA)
1 HQDA (DARD-ARS-P)
1 HQDA (DAPC-PAS-A)
1 HQDA (DUSA-OR)
1 HQDA (DAMO-RQR)
1 HQDA (DASG)
1 HQDA (DA10-PI)
1 Chief, Consult Div (DA-OTSG), Adelphi, MD
1 Mil Asst, Hum Res, ODDR&E, OAD (E&LS)
1 HQ USARAL, APO Seattle, ATTN: ARAGP-R
1 HQ First Army, ATTN: AFKA-OI-TI
2 HQ Fifth Army, Ft Sam Houston
1 Dir, Army Stf Studies Ofc, ATTN: OAVCSA (DSP)
1 Ofc Chief of Stf, Studies Ofc
1 DCSPER, ATTN: CPS/OCP
1 The Army Lib, Pentagon, ATTN: RSB Chief
1 The Army Lib, Pentagon, ATTN: ANRAL
1 Ofc, Asst Sect of the Army (R&D)
1 Tech Support Ofc, OJCS
1 USASA, Arlington, ATTN: IARD-T
1 USA Rsch Ofc, Durham, ATTN: Life Sciences Dir
2 USARIEM, Natick, ATTN: SGRD-UE-CA
1 USATTC, Ft Clayton, ATTN: STETC-MO-A
1 USAIMA, Ft Bragg, ATTN: ATSU-CTD-OM
1 USAIMA, Ft Bragg, ATTN: Marquat Lib
1 US WAC Ctr & Sch, Ft McClellan, ATTN: Lib
US WAC Ctr & Sch, Ft McClellan, ATTN: Tng Dir
1 USA Quartermaster Sch, Ft Lee, ATTN: ATSM-TE
1 Intelligence Material Dev Ofc, EWL, Ft Holabird
1 USA SE Signal Sch, Ft Gordon, ATTN: ATSO-EA
1 USA Chaplain Ctr & Sch, Ft Hamilton, ATTN: ATSC-TE-RD
1 USATSCH, Ft Eustis, ATTN: Educ Advisor
1 USA War College, Carlisle Barracks, ATTN: Lib
2 WRAIR, Neuropsychiatry Div
1 DLI, SDA, Monterey
1 USA Concept Anal Agcy, Bethesda, ATTN: MOCA-MR
1 USA Concept Anal Agcy, Bethesda, ATTN: MOCA-JF
1 USA Arctic Test Ctr, APO Seattle, ATTN: STEAC-PL-MI
1 USA Arctic Test Ctr, APO Seattle, ATTN: AMSTE-PL-TS
1 USA Armament Cmd, Redstone Arsenal, ATTN: ATSK-TEM
1 USA Armament Cmd, Rock Island, ATTN: AMSAR-TDC
1 FAA-NAFEC, Atlantic City, ATTN: Library
1 FAA-NAFEC, Atlantic City, ATTN: Human Engr Br
1 FAA Aeronautical Ctr, Oklahoma City, ATTN: AAC-44D
2 USA Fld Arty Sch, Ft Sill, ATTN: Library
1 USA Armor Sch, Ft Knox, ATTN: Library
1 USA Armor Sch, Ft Knox, ATTN: ATSB-DI-E
1 USA Armor Sch, Ft Knox, ATTN: ATSB-DT-TP
1 USA Armor Sch, Ft Knox, ATTN: ATSB-CD-AD
2 HQUSACDEC, Ft Ord, ATTN: Library
1 HQUSACDEC, Ft Ord, ATTN: ATEC-EX-E-Hum Factors
2 USAEEC, Ft Benjamin Harrison, ATTN: Library
1 USAPACDC, Ft Benjamin Harrison, ATTN: ATCP-HR
1 USA Comm-Elect Sch, Ft Monmouth, ATTN: ATSN-EA
1 USAEC, Ft Monmouth, ATTN: AMSEL-CT-HDP
1 USAEC, Ft Monmouth, ATTN: AMSEL-PA-P
1 USAEC, Ft Monmouth, ATTN: AMSEL-SI-CB
1 USAEC, Ft Monmouth, ATTN: C, Facl Dev Br
1 USA Materials Sys Anal Agcy, Aberdeen, ATTN: AMXSY-P
1 Edgewood Arsenal, Aberdeen, ATTN: SAREA-BL-H
1 USA Ord Ctr & Sch, Aberdeen, ATTN: ATSL-TEM-C
2 USA Hum Engr Lab, Aberdeen, ATTN: Library/Dir
1 USA Combat Arms Tng Bd, Ft Benning, ATTN: Ad Supervisor
1 USA Infantry Hum Rsch Unit, Ft Benning, ATTN: Chief
1 USA Infantry Bd, Ft Benning, ATTN: STEBC-TE-T
1 USASMA, Ft Bliss, ATTN: ATSS-LRC
1 USA Air Def Sch, Ft Bliss, ATTN: ATSA-CTD-ME
1 USA Air Def Sch, Ft Bliss, ATTN: Tech Lib
1 USA Air Def Bd, Ft Bliss, ATTN: FILES
1 USA Air Def Bd, Ft Bliss, ATTN: STEBD-PO
1 USA Cmd & General Stf College, Ft Leavenworth, ATTN: Lib
1 USA Cmd & General Stf College, Ft Leavenworth, ATTN: ATSW-SE-L
1 USA Cmd & General Stf College, Ft Leavenworth, ATTN: Ed Advisor
1 USA Combined Arms Cmbt Dev Act, Ft Leavenworth, ATTN: DepCdr
1 USA Combined Arms Cmbt Dev Act, Ft Leavenworth, ATTN: CCS
1 USA Combined Arms Cmbt Dev Act, Ft Leavenworth, ATTN: ATCASA
1 USA Combined Arms Cmbt Dev Act, Ft Leavenworth, ATTN: ATCACO-E
1 USA Combined Arms Cmbt Dev Act, Ft Leavenworth, ATTN: ATCACC-CI
1 USAECOM, Night Vision Lab, Ft Belvoir, ATTN: AMSEL-NV-SD
3 USA Computer Sys Cmd, Ft Belvoir, ATTN: Tech Library
1 USAMERDC, Ft Belvoir, ATTN: STSFB-DQ
1 USA Eng Sch, Ft Belvoir, ATTN: Library
1 USA Topographic Lab, Ft Belvoir, ATTN: ETL-TD-S
1 USA Topographic Lab, Ft Belvoir, ATTN: STINFO Center
1 USA Topographic Lab, Ft Belvoir, ATTN: ETL-GSL
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: CTD-MS
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: ATS-CTD-MS
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: ATSI-TE
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: ATSI-TEX-GS
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: ATSI-CTS-OR
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: ATSI-CTD-DT
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: ATSI-CTD-CS
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: DAS/SRD
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: ATSI-TEM
1 USA Intelligence Ctr & Sch, Ft Huachuca, ATTN: Library
1 CDR, HQ Ft Huachuca, ATTN: Tech Ref Div
2 CDR, USA Electronic Prvg Grd, ATTN: STEEP-MT-S
1 HQ, TCATA, ATTN: Tech Library
1 HQ, TCATA, ATTN: AT CAT-OP-Q, Ft Hood
1 USA Recruiting Cmd, Ft Sheridan, ATTN: USARCPM-P
1 Senior Army Adv., USAFAGOD/TAC, Elgin AF Aux Fld No. 9
1 HQ, USARPAC, DCSPER, APO SF 96558, ATTN: GPPE-SE
1 Stimson Lib, Academy of Health Sciences, Ft Sam Houston
1 Marine Corps Inst., ATTN: Dean-MCI
1 HQ, USMC, Commandant, ATTN: Code MTMT
1 HQ, USMC, Commandant, ATTN: Code MPI-20-28
2 USCG Academy, New London, ATTN: Admission
2 USCG Academy, New London, ATTN: Library
1 USCG Training Ctr, NY, ATTN: CO
1 USCG Training Ctr, NY, ATTN: Educ Svc Ofc
1 USCG, Psychol Res Br, DC, ATTN: GP 1/62
1 HQ Mid-Range Br, MC Det, Quantico, ATTN: P&S Div

1 US Marine Corps Liaison Ofc, AMC, Alexandria, ATTN: AMCGS-F
1 USATRADOC, Ft Monroe, ATTN: ATRO-ED
5 USATRADOC, Ft Monroe, ATTN: ATPR-AD
1 USATRADOC, Ft Monroe, ATTN: ATTS-EA
1 USA Forces Cmd, Ft McPherson, ATTN: Library
2 USA Aviation Test Bd, Ft Rucker, ATTN: STEBG-PO
1 USA Agcy for Aviation Safety, Ft Rucker, ATTN: Library
1 USA Agcy for Aviation Safety, Ft Rucker, ATTN: Educ Advisor
1 USA Aviation Sch, Ft Rucker, ATTN: PO Drawer O
1 HQUSA Aviation Sys Cmd, St Louis, ATTN: AMSAV-ZDR
2 USA Aviation Sys Test Act., Edwards AFB, ATTN: SAVTE-T
1 USA Air Def Sch, Ft Bliss, ATTN: ATSA TEM
1 USA Air Mobility Rsch & Dev Lab, Moffett Fld, ATTN: SAVDL-AS
1 USA Aviation Sch, Res Trng Mgt, Ft Rucker, ATTN: ATST-T-RTM
1 USA Aviation Sch, CO, Ft Rucker, ATTN: ATST-D-A
1 HQ, DARCOM, Alexandria, ATTN: AMXCD-TL
1 HQ, DARCOM, Alexandria, ATTN: CDR
1 US Military Academy, West Point, ATTN: Serials Unit
1 US Military Academy, West Point, ATTN: Ofc of Milt Ldrshp
1 US Military Academy, West Point, ATTN: MAOR
1 USA Standardization Gp, UK, FPO NY, ATTN: MASE-GC
1 Ofc of Naval Rsch, Arlington, ATTN: Code 452
3 Ofc of Naval Rsch, Arlington, ATTN: Code 458
1 Ofc of Naval Rsch, Arlington, ATTN: Code 450
1 Ofc of Naval Rsch, Arlington, ATTN: Code 441
1 Naval Aerospc Med Res Lab, Pensacola, ATTN: Acous Sch Div
1 Naval Aerospc Med Res Lab, Pensacola, ATTN: Code L51
1 Naval Aerospc Med Res Lab, Pensacola, ATTN: Code L5
1 Chief of NavPers, ATTN: Pers-OR
1 NAVAIRSTA, Norfolk, ATTN: Safety Ctr
1 Nav Oceanographic, DC, ATTN: Code 6251, Charts & Tech
1 Center of Naval Anal, ATTN: Doc Ctr
1 NavAirSysCom, ATTN: AIR-5313C
1 Nav BuMed, ATTN: 713
1 NavHelicopterSubSqua 2, FPO SF 96601
1 AFHRL (FT) Williams AFB
1 AFHRL (TT) Lowry AFB
1 AFHRL (AS) WPAFB, OH
2 AFHRL (DOJZ) Brooks AFB
1 AFHRL (DOJN) Lackland AFB
1 HQUSAF (INYSO)
1 HQUSAF (DPXXA)
1 AFVTG (RD) Randolph AFB
3 AMRL (HE) WPAFB, OH
2 AF Inst of Tech, WPAFB, OH, ATTN: ENE/SL
1 ATC (XPTD) Randolph AFB
1 USAF AeroMed Lib, Brooks AFB (SUL-4), ATTN: DOC SEC
1 AFOSR (NL), Arlington
1 AF Log Cmd, McClellan AFB, ATTN: ALC/DPCRB
1 Air Force Academy, CO, ATTN: Dept of Bel Scn
5 NavPers & Dev Ctr, San Diego
2 Navy Med Neuropsychiatric Rsch Unit, San Diego
1 Nav Electronic Lab, San Diego, ATTN: Res Lab
1 Nav TrngCen, San Diego, ATTN: Code 9000-Lib
1 NavPostGraSch, Monterey, ATTN: Code 55Aa
1 NavPostGraSch, Monterey, ATTN: Code 2124
1 NavTrngEquipCtr, Orlando, ATTN: Tech Lib
1 US Dept of Labor, DC, ATTN: Manpower Admin
1 US Dept of Justice, DC, ATTN: Drug Enforce Admin
1 Nat Bur of Standards, DC, ATTN: Computer Info Section
1 Nat Clearing House for MH-Info, Rockville
1 Denver Federal Ctr, Lakewood, ATTN: BLM
12 Defense Documentation Center
4 Dir Psych, Army Hq, Russell Ofcs, Canberra
1 Scientific Advsr, Mil Bd, Army Hq, Russell Ofcs, Canberra
1 Military Air Attache, Austrian Embassy
1 Centre de Recherche Des Facteurs Humaine de la Defense Nationale, Brussels
2 Canadian Joint Staff, Washington
1 C Air Staff, Royal Canadian AF, ATTN: Pers Std Anal Br
3 Chief, Canadian Def Rsch Staff, ATTN: C CRDS(W)
4 British Def Staff, British Embassy, Washington
1 Def & Civil Inst of Enviro Medicine, Canada
1 AIR CRESS, Kensington, ATTN: Info Sys Br
1 Militaerpsykologisk Tjeneste, Copenhagen
1 Military Attache, French Embassy, ATTN: Doc Sec
1 Medecin Chef, C.E.R.P.A.-Arsenal, Toulon/Naval France
1 Prin Scientific Off, Appl Hum Engr Rsch Div, Ministry of Defense, New Delhi
1 Pers Rsch Ofc Library, AKA, Israel Defense Forces
1 Ministeris van Defensie, DOOP/KL Afd Sociaal Psychologische Zaken, The Hague, Netherlands

Ag84Ah
cop. 2



FORESTER'S GUIDE TO AERIAL PHOTO INTERPRETATION

U. S. DEPT. OF AGRICULTURE
NATIONAL AGRICULTURAL LIBRARY
MAR 2 1970
CURRENT SERIAL RECORDS

AGRICULTURE HANDBOOK No. 308

U.S. Department of Agriculture — Forest Service

FORESTER'S GUIDE TO AERIAL PHOTO INTERPRETATION

T. Eugene Avery

U.S. Department of Agriculture
Forest Service

Agriculture Handbook No. 308
October 1966
Slightly revised December 1969

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price 75 cents

This handbook is a revised and enlarged version of Occasional Paper 156, issued by the Southern Forest Experiment Station, New Orleans, La., in January 1957. The text and illustrations have been broadened to include most of the United States and parts of Canada.

Dr. T. Eugene Avery, formerly with the Division of Forest Economics Research at the Southern Forest Experiment Station, is Professor of Forestry and Head, Department of Forestry, University of Illinois, Urbana, Ill.

CONTENTS

	Page
Types of aerial photographs	1
Obtaining aerial photography	2
Preparing photographs for stereo-viewing	5
Equipment needed	5
Preparing the photographs	6
Photo scale, bearings, and distances	7
Identifying forest types and tree species	9
Mapping from aerial photographs	11
Measuring areas	24
Tree height, crown diameter, and crown closure	26
Tree height	26
Tree crown diameter	29
Tree crown closure	30
Aerial cruising	32
Individual tree volumes	32
Stand volume per acre	32
Photo stratification for ground cruising	38
Literature cited	40

FORESTER'S GUIDE TO AERIAL PHOTO INTERPRETATION

This handbook was written as a practical reference on techniques of aerial photo interpretation in forest inventory. It is for the forester with a casual knowledge of the subject. While oblique photographs are occasionally useful for interpretation, this manual emphasizes stereoscopic interpretation of vertical aerial photographs available from various agencies of the U.S. Department of Agriculture (USDA). Figure 1 (foldout, inside back cover) is an example of a vertical aerial photograph.

With training, the forester can use aerial photographs to locate property boundaries and trails, determine bearings and distances, identify classes of vegetation, and measure areas. Experience will enable him to improve the efficiency of forest inventories by distributing field samples on the basis of photo stratifications. In some instances, he may even be able to estimate timber volumes directly from the photographs.

While photo interpretation may make the forester's job easier, there are limitations. Accurate measurements of such items as tree diameter, form class, and stem defect are possible only on the ground. Aerial photographs are best used to complement, assist, or reduce field work rather than take its place.

TYPES OF AERIAL PHOTOGRAPHS [1]

Oblique photographs are taken with the axis of the aerial camera at various angles between the horizon and the ground. *High* obliques show the horizon on the photograph; *low* obliques do not. An oblique photograph covers a larger area compared with a vertical photograph from the same altitude, but its usefulness is limited to fairly level terrain where the view is not obstructed by ridges. For this reason, and because obliques do not readily lend themselves to stereoscopic viewing, they are seldom used by foresters in the United States.

Vertical photographs are taken with the aerial camera pointed straight down at the ground, or as nearly so as feasible. Overlapping exposures in each fight line permit an interpreter to study vertical photographs three-dimensionally with a stereoscope. Because such prints have become so useful for mapping and interpretation, the term "aerial photo" is normally assumed to denote a vertical photograph and will be thus applied in this handbook.

Composite photography is accomplished either by several cameras taking simultaneous pictures, or by one camera having several lenses to provide multiple exposures.

The first approach is exemplified by *trimetrogon* photography, which uses one vertical and two oblique cameras. Combining the three pictures gives photo coverage from horizon to horizon. The system provides relatively inexpensive, small-scale coverage for reconnaissance mapping of large or remote areas.

A second technique, used by the U.S. Coast and Geodetic Survey, employs a special camera having nine lenses. This multiple lens system has proved successful for topographic mapping, but requires expensive photographic and plotting equipment. Its specialized nature makes it generally unsuitable for foresters.

Mosaics are composite pictures assembled from vertical aerial photographs. Individual photographs are cut, matched, and pasted together to give the appearance of a single large print. A mosaic assembled by reference to known points on the ground is called a controlled mosaic; if ground control of linear distances is lacking, the mosaic is called uncontrolled. When carefully assembled, both types provide good map approximations. Mosaics are often used as pictorial displays in offices and public buildings. Professionally prepared mosaics are expensive and cannot be studied three-dimensionally; hence their use by foresters is somewhat restricted.

[1] Adapted from "Forestry uses of aerial photographs," an unpublished training manual of the U.S. Forest Service, Pacific Northwest Forest and Range Experiment Station, 1961.

OBTAINING AERIAL PHOTOGRAPHY

Users of this guide will ordinarily rely on prints of existent photography flown for public agencies. Thus there is no need here to discuss specifications for new aerial photography. Details of flight planning and photographic contracts are covered in the *Manual of Photogrammetry* and the *Manual of Photographic Interpretation* (*1*, *2*).[2]

Sources of aerial photography.—Most of the United States has been photographed in recent years for various Federal agencies. The key to this photography is available free in map form as the "Status of Aerial Photography in the U.S." Copies may be obtained by writing to:

Map Information Office
U.S. Department of the Interior
Geological Survey
Washington, D.C. 20240

This map shows all areas of the United States, by counties, that have been photographed by or for: Agricultural Stabilization and Conservation Service, Soil Conservation Service, Forest Service, Geological Survey, Corps of Engineers, Air Force, Coast and Geodetic Survey, and commercial firms. Names and addresses of agencies holding the negatives for the photographs are printed on the back of the map, and inquiries should be sent directly to the appropriate organization. There is no central laboratory that can furnish prints of all Government photography.

The Agricultural Stabilization and Conservation Service (ASCS) of the Department of Agriculture holds the largest share of the recent aerial photography. ASCS was formerly known as the Agricultural Adjustment Administration (AAA), the Production and Marketing Administration (PMA), and the Commodity Stabilization Service (CSS).

Forest industries often have aerial surveys made of their lands, and ownerships adjacent to or within such areas may be included. Such surveys often are an additional source of photography. The aerial mapping company usually retains the negatives and must have the written permission of the original purchaser before it can sell prints.

Films, season, and date of photography.—Two types of black-and-white aerial film are in common use: panchromatic and infrared. Infrared is usually modified by a minus-blue filter to reduce extreme contrast and improve image resolution. Panchromatic photography offers better resolution and lighter shadows but exhibits little tonal contrast among forest types. Modified infrared photography presents a maximum of contrast between conifers and deciduous hardwoods, but wet sites and shadows register in black, thus restricting interpretation. In Western United States, where coniferous trees predominate, panchromatic film is more likely to be used. Conversely, foresters managing eastern hardwoods often prefer infrared photography because of easier forest type separations. In figure 2, dark-toned pines (A) are readily differentiated from the light-colored upland hardwoods (B) on the infrared stereogram, but there is little tonal contrast on the panchromatic exposures. Also, the farm pond at (C) is immediately seen on the infrared prints, but may be completely overlooked on the panchromatic photographs.

If measurements are needed for deciduous species, both kinds of photography should be taken during the growing season. Infrared is likely to be flown specifically for forestry purposes and usually meets this requirement. On panchromatic photographs taken in winter, conifers can be distinguished from hardwoods, but interpretation of hardwood stand-sizes is difficult. Modified infrared photography is occasionally available for tracts near large forest ownerships or National Forests, but most interpreters will be limited to use of USDA panchromatic photography.

If there is a choice between photography of different dates, one should consider the most recent. In regions characterized by rapid tree growth and frequent cutting, the value of photos more than 5 years old is questionable.

Photo scales and enlargements.—Available aerial photographs range in nominal scale from about 1:12,000 to 1:20,000. Contact prints are standardized at the 9- by 9-inch size. Forest industries often contract for photography at 1:15,840 (4 inches per mile), and some areas in Western United States have been photographed at 1:12,000.

USDA photography is normally at a scale of 1:20,000 (1,667 feet per inch). This is the smallest scale that nonprofessional interpreters with a minimum of equipment can use efficiently. Although enlargements of USDA photography can be obtained, they cost more, yield no additional detail, and cannot be viewed with simple stereoscopes. Contact prints are recommended for general use, unless enlargements present definite advantages in transfer of photo detail to base maps.

Paper surface, weight, and contrast.—USDA prints are available with either glossy or semimatte finishes. Glossy prints exhibit a high degree of resolution and tonal contrast, but their shiny surfaces are difficult to write upon. Semimatte prints are often preferred because they have a minimum of glare, an easily marked on "toothed" surface, and fair resolution qualities.

[2] Italic numbers in parentheses refer to Literature Cited, page 40.

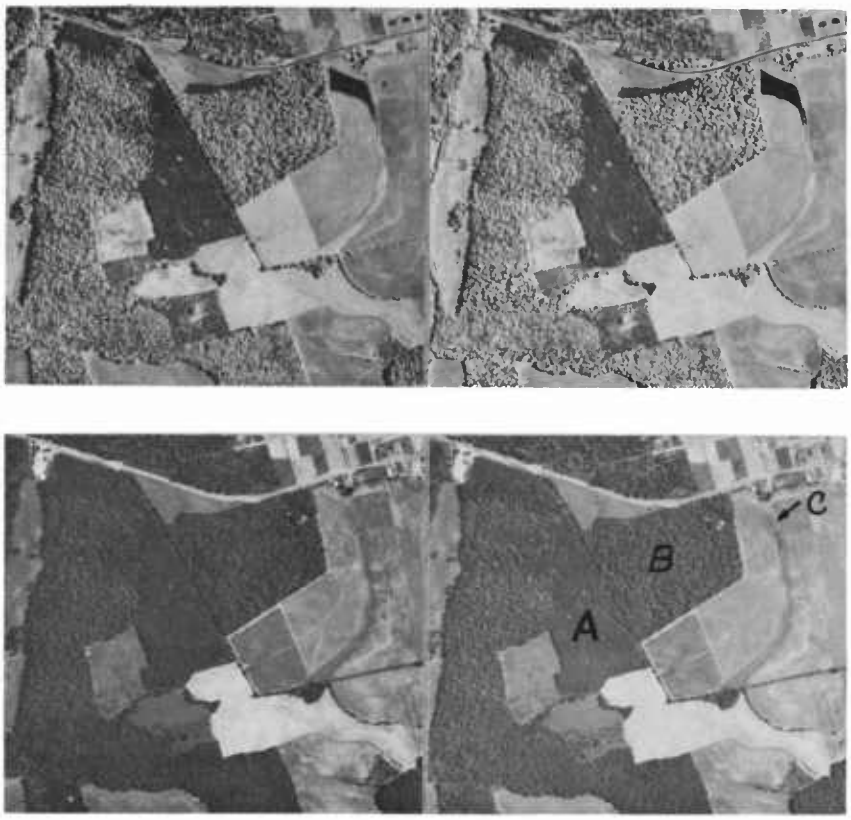


Figure 2.—**Modified infrared (above) and panchromatic photography made in the North Carolina Piedmont during June. Exposures were made simultaneously with a dual aerial camera system. Scale is 1,320 feet per inch. Prints may be viewed three-dimensionally with a lens stereoscope.**

Photographs are available on either single- or double-weight paper. Single-weight paper is suitable for office use, conserves filing space, and is easy to handle under the lens stereoscope. Double-weight paper is preferred for field use, however, because it is more durable and less subject to dimensional changes. Most USDA photography is furnished on double-weight, semimatte paper unless otherwise specified. Contact prints may be obtained on special low-shrink, waterproof paper at a slight increase in price.

Some USDA laboratories offer three degrees of print contrast: "soft" for mapping, "normal" for general use, and "contrast" for timber survey work. The contrast of aerial prints should be specified if a choice is available. The photograph should present maximum tonal differences between timber types without loss of image detail in light and dark areas. Although contrast is limited primarily by the quality of the original exposure, new electronic printing devices get excellent contrast from all but the poorest negatives.

Ordering Agricultural Stabilization and Conservation Service photography.—Photo index sheets or index mosaics, showing the relative positions of all individual photographs within a given county (fig. 3), can be examined at local offices of the Agricultural Stabilization and Conservation Service or the Soil Conservation Service. The number of index sheets per county varies from one to six or more. Foresters working regularly with aerial photographs may want to purchase a set of index sheets for areas where their work is concentrated.

To decide which photographs to order, outline the desired area on the photo index. Include all photographs which overlap this area, partially or completely. Prints are ordered by county symbol, roll number, and exposure number (fig. 1). Other items to specify are:

Date of photography—appears in upper left corner of each print.

Scale—such as 1:20,000 or 1,667 feet per inch.

Reproduction—such as 9- by 9-inch contact prints, double-weight, semimatte paper, with "contrast" finish.

Figure 3.—Portion of an aerial photo index sheet issued by the U.S. Department of Agriculture. Prints are lapped in mosaic fashion to form a composite picture of the county. The serpentine white line indicates that the county boundary is a river.

Photographs of the following States should be ordered from:

Western Laboratory
Aerial Photography Division
Agricultral Stabilization and Conservation Service
U.S. Department of Agriculture
2505 Parley's Way
Salt Lake City, Utah 84109

Arizona	Louisiana	Oklahoma
Arkansas	Minnesota	Oregon
California	Montana	South Dakota
Colorado	Nebraska	Texas
Hawaii	Nevada	Utah
Idaho	New Mexico	Washington
Kansas	North Dakota	Wyoming

Photography of Alaska and Vermont is not available through the ASCS. Photographs of the remaining States should be ordered from:

Eastern Laboratory
Aerial Photography Division
Agricultural Stabilization and Conservation Service
U.S. Department of Agriculture
45 South French Broad Avenue
Asheville, N.C. 28802

Alabama	Maine	North Carolina
Connecticut	Maryland	Ohio
Delaware	Massachusetts	Pennsylvania
Florida	Michigan	Rhode Island
Georgia	Mississippi	South Carolina
Illinois	Missouri	Tennessee
Indiana	New Hampshire	Virginia
Iowa	New Jersey	West Virginia
Kentucky	New York	Wisconsin

Photo index sheets, usually at a scale of 1 inch per mile, cost $2.50 for a sheet 20 by 24 inches. Prices for 9- by 9-inch contact prints, untrimmed and on single- or double-weight paper, are as follows:

Quantity	*Price per print*
First 25	$1.25
Over 25	.90

Contact prints on waterproof (low-shrink) paper are available at an additional 50 cents per print. Quantity prices apply only when an order is shipped to one address. Enlargements are available at four scales ranging from 1:15,840 on prints 14 by 14 inches to 1:4,800 on prints 40 by 40 inches. Prices range from about $2.50 to $8.00 per print.

These prices are as of Oct. 1968, but are subject to revision periodically. Payment must be made in advance, preferably by money order, and 6 to 8 weeks should be allowed for delivery.

Ordering Soil Conservation Service photography.—Some areas of the United States, notably counties bordering the Atlantic Ocean, are not covered by ASCS photography. In some instances, photo coverage of these areas may be purchased from:

Soil Conservation Service
Cartographic Division
U.S. Department of Agriculture
Hyattsville, Md. 20251

Ordering Forest Service photography.—Aerial photographs of the National Forests are available at scales of 1:15,840 (1,320 feet per inch) or 1:12,000 (1,000 feet per inch). Coverage includes the Chugach and part of the Tongass National Forests in Alaska, but does not include Hawaii. Some photographs are on infrared film. The prices quoted for ASCS coverage will generally apply to the Forest Service.

Forest Service photography of Eastern United States may be ordered from:

Chief, Forest Service
U.S. Department of Agriculture
Washington, D.C. 20250

Photographic coverage of Western United States (Forest Service, Regions 1–6 and 10) is obtained through the appropriate Regional Forester as follows:

Region	*Address*
1	Federal Building, Missoula, Mont., 59801
2	Federal Center, Building 85, Denver, Colo., 80225
3	Federal Building, 517 Gold Ave. SW., Albuquerque, N. Mex., 87101
4	Forest Service Building, Ogden, Utah, 84403
5	630 Sansome St., San Francisco, Calif., 94111
6	P.O. Box 3623, Portland, Oreg., 97208
10	Regional Forester, U.S. Forest Service, P.O. Box 1628, Juneau, Alaska, 99801

PREPARING PHOTOGRAPHS FOR STEREO-VIEWING

Equipment Needed

Equipment considered essential by one interpreter may be of limited use to another; nevertheless, the forester who anticipates a continued use of aerial photographs will probably find the following list closely approximates his minimum needs.

Lens stereoscope, folding pocket type.
Parallax bar or parallax wedge for measuring object heights.
Engineer's scale, graduated to 0.02 inch.
Tree crown-density scale.
Tree crown-diameter scale.
Dot grids for acreage determination.
China-marking pencils for writing on photographs.
Carbon tetrachloride and cotton for cleaning photographs.
Drafting instruments, triangles, and drafting tape.
Needles for point-pricking.
Tracing table.
Magnetic or spring-clipboard for holding stereo-pairs.
Proportional dividers.

367-547 O—69—— 2

If purchased with discretion, the items can be obtained for less than $250. For a price list of photo interpretation aids available from the Forest Service, write to the Division of Engineering, Forest Service, U.S. Department of Agriculture, Washington, D.C. 20250.

Many foresters will already own drafting instruments, dot grids, and pocket stereoscopes. A satisfactory tracing table can be improvised by installing a uniform light source under a glass surface. Fluorescent tubes are better than incandescent bulbs because they produce less heat. A sheet of frosted cellulose acetate between two pieces of ordinary single-weight glass serves well when special frosted glass is not available.

If the forester uses aerial photographs regularly and becomes adept in interpretation and mapping, he may wish to acquire more expensive equipment, such as a mirror stereoscope, vertical sketchmaster, reflecting projector, or radial plotting devices. The *Manual of Photogrammetry* (*1*) contains information on such equipment.

Preparing the Photographs

Photographic flights are planned so that prints will overlap about 60 percent in the line of flight and about 30 percent between flight strips. For effective stereo-viewing, prints must be trimmed to the nominal 9- by 9-inch size, preserving the four fiducial marks at the midpoint of each of the edges (fig. 1). Then:

1. *Locate the principal point (PP) or center of each photograph.* Aline opposite sets of fiducial marks with a straightedge or triangle. Draw a cross at the center with a wedge-pointed pencil, and make a fine needle hole at the intersection.
2. *Locate the conjugate principal points (CPP's) on each photograph*—the points that correspond to PP's of adjacent photographs. Adjust the stereoscope until distance between centers of lenses corresponds with interpupillary distance (usually about 2.5 inches). Arrange the first two photographs of a given flight line so that corresponding gross features overlap. Shadows should be toward the observer; if they fall away from the viewer there is a tendency to see relief in reverse. Clip down one photograph. Move adjacent photograph in direction of line of flight until corresponding images on each print are about 2.2 inches apart. Place lens stereoscope over prints *parallel to line of flight* so that the left-hand lens is over the left photograph and the right-hand lens is over the same image on the right photograph. The area around the PP will be seen as a three-dimensional image. The movable photograph should then be fastened down. While viewing this area through the stereoscope, place a needle in the same area on the adjacent photograph until it appears to fall precisely in the hole pricked for the PP. This locates the CPP (fig. 1), though a monocular check should be made before the point is permanently marked. Repeat for all photographs; each will then have one PP and two CPP's except that prints falling at the ends of the flight lines will have only one CPP. Ink a 0.2-inch diameter circle around each PP and CPP (fig. 1).
3. *Locate the flight lines on each print by alining the PP's and CPP's.* Connect the edges of the alined circles with a fine ink line (fig. 1). Because of lateral shifting of the photographic plane in flight, a straight line will rarely pass through the PP and *both* CPP's on a given print.
4. *Determine the photo base length for each stereo-overlap* by averaging the distance between the PP and CPP on one print and the corresponding distance on the overlapping print. Measure to the nearest 0.02 inch and record on the back of each overlap. There will be two average base lengths for each print, i.e., one for each set of overlapping flight lines.

Alining prints for stereoscopic study.—A print is selected and clipped down with shadows toward the viewer. The adjacent print is placed with its CPP 2.2 inches from the corresponding PP on the first print. With flight lines superimposed, the second print is positioned and clipped down. The stereoscope is placed with its long axis parallel to the flight line and with the lenses over corresponding images. In this way an overlapping strip 2.2 inches wide and 9 inches long can be viewed by moving the stereoscope up and down the overlap area (fig. 4).

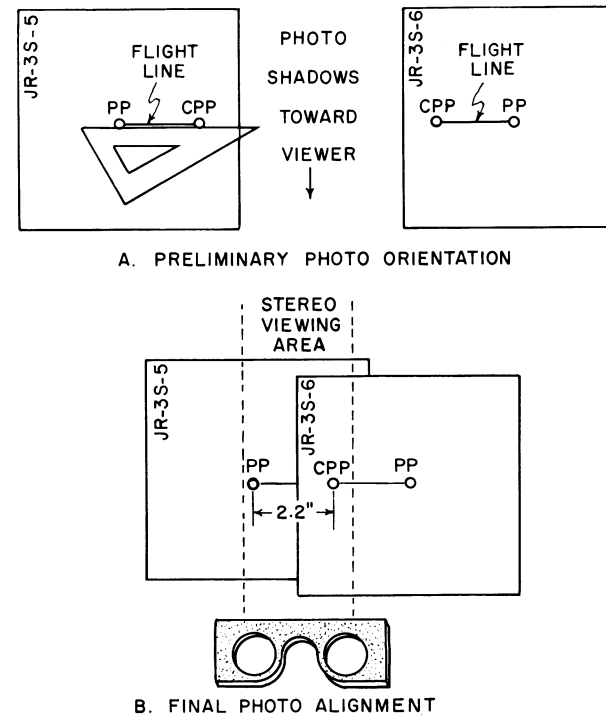


***Figure 4.*—Method of alining 9- by 9-inch contact prints for viewing with a lens stereoscope. Compare this diagram with figure 1.**

While the photos are still clipped down, the prints can be flipped into reverse position with the opposite photo on top. This presents another area of the overlap for stereo-viewing. To study the narrow strip between, the edge of one print must be curled upward or downward and the stereoscope moved parallel to the flight line until the "hidden area" comes into view (fig. 5).

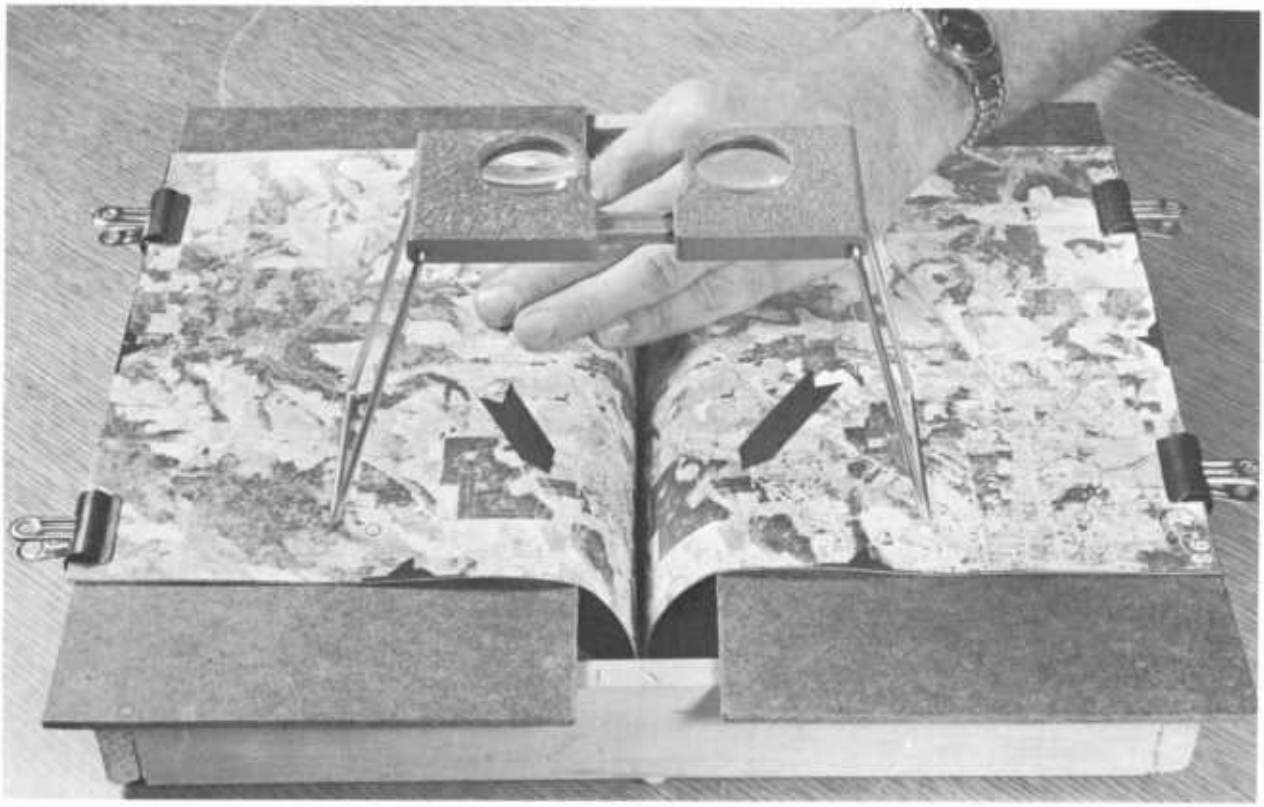


Figure 5.—**Slotted clip board for viewing the "hidden area" of overlapping contact prints with a lens stereoscope. The area indicated by arrows cannot be stereoscopically studied when prints are lapped as in figures 1 and 4.**

PHOTO SCALE, BEARINGS, AND DISTANCES

The vertical aerial photograph presents a true record of angles, but measures of horizontal distances vary widely with changes in ground elevations and flight altitudes. The nominal scale (as 1:20,000) is representative only of the datum, an imaginary plane passing through a specified ground elevation above sea level. Calculation of the average photo scale will increase the accuracy of subsequent photo measurements.

Aerial cameras in common use have focal lengths of 6, 8.25, or 12 inches (0.5, 0.6875, or 1.0 ft.). This information, with the altitude of the aircraft above ground datum, makes it possible to determine the representative fraction (RF) or natural scale:

$$RF=\frac{\text{Focal length (ft.)}}{\text{Flying height above ground (ft.)}}$$

The height of the aircraft is rarely known to the interpreter, however, and photo scale is more often calculated by this proportion:

$$RF=\left[\frac{\text{Photographic distance between two points (ft.)}}{\text{Ground or map distance between same points (ft.)}}\right]$$

Determining scale from ground measurements.—Select two points on opposite sides of the print so that a line connecting them passes near the PP. If the points are approximately equidistant from the PP, the effect of photographic tilt will be minimized. (Tilt results when the camera axis deviates from the vertical at the instant of exposure. It is often present, but generally not enough to be readily noticed.) Points must be easily identifiable on the ground so that the distance between them can be precisely measured. Gas and power line rights-of-way, highways, and railroads offer clearings where ground distances can be quickly chained. It is not necessary to calculate the scale of every photograph in a flight

strip. In hilly terrain, every third or fifth print may be used; in flat topography, every tenth or twentieth. Scales of intervening photographs can be obtained by interpolation.

Office checks of photo scale.—Scale determination from ground measurements is laborious and expensive; hence other methods should be used wherever possible. If a U.S. Geological Survey quadrangle sheet is available, the map distance can be measured and used in the formula, provided the same distance can be identified for photo measurement (fig. 6).

Another alternative is presented in areas of flat terrain where General Land Office subdivisions of sections, quarter-sections, and forties are visible on the photographs. Since the lengths of these subdivisions will be known, they can also be used as ground distances. A given section may rarely be exactly 5,280 feet on a side, but determining scale by this method is more accurate than accepting the nominal scale.

Compass bearings and distances.—Although flight lines usually run north-south or east-west, few photographs are oriented exactly with the cardinal directions. For this reason, a reference line must be located before bearings can be determined. The method described is used by field teams on the U.S. Forest Survey:

1. Select a straight-line feature such as a highway, section line, or field edge and determine its bearing. Draw this reference line on the photograph, extend it as necessary, and record the bearing (fig. 7).

Figure 6.—Determination of photo scale from a U.S. Geological Survey map. Map scale is 1:24,000 or 2,000 feet per inch. Map distance between X and Y is 2.00 inches, or 4,000 feet on the ground. Photo distance is 4.80 inches. Thus the photo scale is $4.80 \div 4{,}000 \times 12$, or 1:10,000. (Courtesy of Abrams Aerial Survey Corporation.)

2. Pick a point of beginning (PB) from which the line of approach to a field location will be run. This should be some feature visible on both photograph and ground, such as a fence corner, barn, road intersection, or stream fork. Draw a line on the photograph from the PB to the location, and extend until it intersects the reference line. Measure the angle between the two lines with a protractor and determine the bearing of the line of approach.

3. Measure the distance between the PB and the field location to the nearest 0.01 inch and convert to feet or chains at the calculated photo scale. At a scale of 1:20,000, a measure of 0.01 inch equals 16.67 feet or about 25 links. In figure 7, the distance from PB to the center of the circular field plot is 1.15 inches, or about 29 chains. Common scale conversions are given in table 1.

TABLE 1.—*Scale conversions for vertical aerial photographs* [1]

Representative fraction (scale)	Feet per inch	Chains per inch	Inches per mile	Acres per square inch	Square miles per square inch
(1)	(2)	(3)	(4)	(5)	(6)
1:7,920	660.00	10.00	8.00	10.00	0.0156
1:8,000	666.67	10.10	7.92	10.20	.0159
1:8,400	700.00	10.61	7.54	11.25	.0176
1:9,000	750.00	11.36	7.04	12.91	.0202
1:9,600	800.00	12.12	6.60	14.69	.0230
1:10,000	833.33	12.63	6.34	15.94	.0249
1:10,800	900.00	13.64	5.87	18.60	.0291
1:12,000	1,000.00	15.15	5.28	22.96	.0359
1:13,200	1,100.00	16.67	4.80	27.78	.0434
1:14,400	1,200.00	18.18	4.40	33.06	.0517
1:15,000	1,250.00	18.94	4.22	35.87	.0560
1:15,600	1,300.00	19.70	4.06	38.80	.0606
1:15,840	1,320.00	20.00	4.00	40.00	.0625
1:16,000	1,333.33	20.20	3.96	40.81	.0638
1:16,800	1,400.00	21.21	3.77	45.00	.0703
1:18,000	1,500.00	22.73	3.52	51.65	.0807
1:19,200	1,600.00	24.24	3.30	58.77	.0918
1:20,000	1,666.67	25.25	3.17	63.77	.0996
1:20,400	1,700.00	25.76	3.11	66.34	.1037
1:21,120	1,760.00	26.67	3.00	71.11	.1111
1:21,600	1,800.00	27.27	2.93	74.38	.1162
1:22,800	1,900.00	28.79	2.78	82.87	.1295
1:24,000	2,000.00	30.30	2.64	91.83	.1435
1:25,000	2,083.33	31.57	2.53	99.64	.1557
1:31,680	2,640.00	40.00	2.00	160.00	.2500
Method of calculation	$\frac{RFD}{12}$	$\frac{RFD}{792}$	$\frac{63,360}{RFD}$	$\frac{(RFD)^2}{6,272,640}$	$\frac{\text{Acres/sq. in.}}{640}$

[1] Conversions for scales not shown can be made from the relationships listed at the bottom of each column. With the scale of 1:7,920 as an example (column 1, line 1), the number of feet per inch is computed by dividing the representative fraction denominator (RFD) by 12 (number of inches per foot). Thus, 7,920÷12=660 feet per inch (column 2). By dividing the RFD by 792 (inches per chain), the number of chains per inch is derived (column 3). Other calculations can be made similarly. Under column 4, the figure 63,360 represents the number of inches in one mile; in column 5, the figure 6,272,640 is the number of square inches in one acre; and in column 6, the number 640 is acres per square mile.

IDENTIFYING FOREST TYPES AND TREE SPECIES

Forest types and tree species can often be delineated with greater accuracy and lower cost on aerial photographs than by ground methods. The degree to which species groups can be recognized depends on the quality, scale, and season of photography; the type of film used; and the interpreter's training. A general knowledge of forest associations and plant ecology is helpful, but field experience in the specific area to be mapped is far more valuable.

A generalized map of forest regions in the United States is shown in figure 8. The tree species listed provide the first step in identification, i.e., the elimination of those cover types not likely to occur in a given locality. The second step, heavily dependent on a knowledge of local

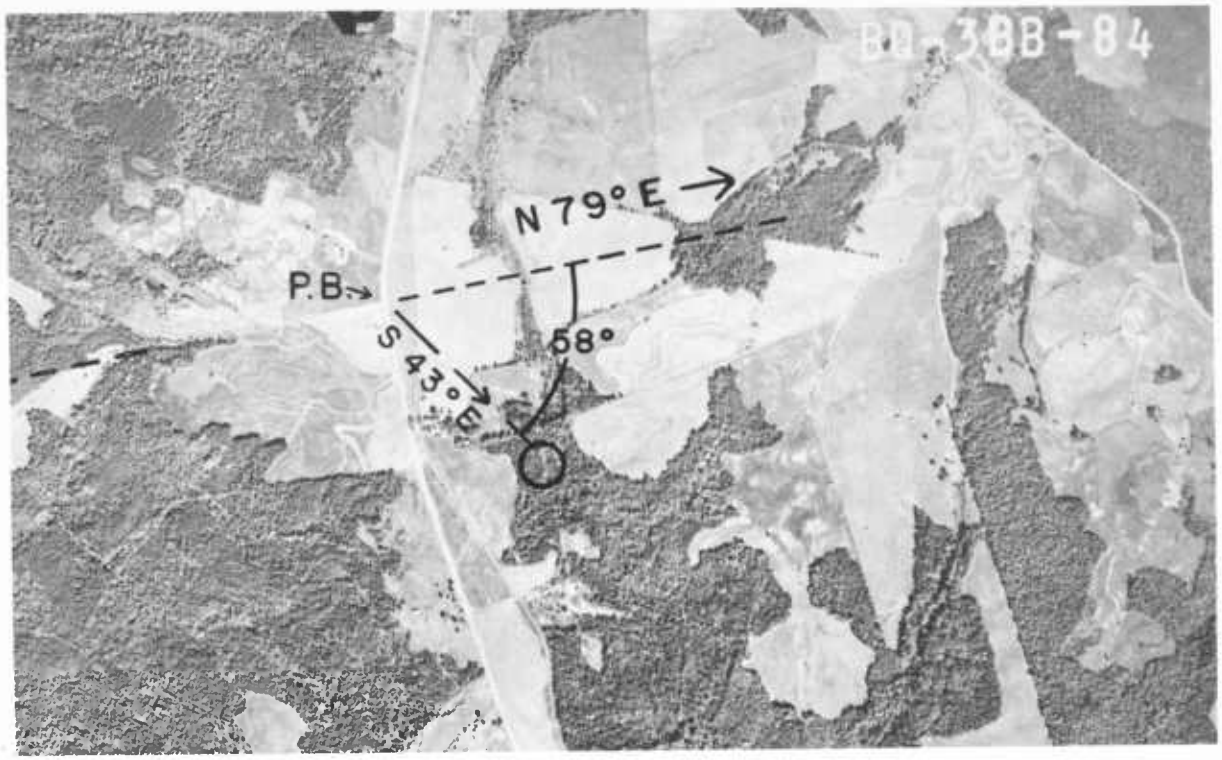


Figure 7.—**Determination of compass bearing and distance to a field plot on a USDA contact print. Scale is 1,667 feet per inch.**

vegetation, is to establish which forest types may be encountered in the area to be mapped.

Recognition of an individual species, often feasible only on large-scale photography, is normally the culmination of intensive study. Obviously the forest interpreter must be familiar with branching patterns and crown shapes of all important species in his region. Mature conifers in sparsely stocked stands can often be recognized on 1:20,000 USDA photography by the configuration of their crown shadows falling on level ground (fig. 9). Studying oblique photographs of trees has been helpful to many foresters.

Recognition of species on vertical photographs also requires a familiarity with tree crowns as seen in overhead views (fig. 10). While overhead crown characteristics are not always apparent on 1:12,000 to 1:20,000 photographs, they can be highly useful on large-scale stereograms. Photo scales as large as 50 feet per inch have been utilized for tree species identifications in Canada (*16*, *20*).

Aside from shadows, crown shapes, and branching patterns, the features to consider in identifying tree species are photographic texture (smoothness or coarseness of images), tonal contrast, relative sizes of tree images at a given photo scale, and topographic location or site. Most of these are rather weak clues when observed singly, yet together they may be the final link in identification by elimination.

For some parts of the United States and Canada, vegetation keys are available aids in tree species recognition. Keys are useful for training new interpreters and for reference by more experienced personnel. Depending on the method of presenting diagnostic features, photo interpretation keys may be grouped into two general classes: *selective* keys and *elimination* keys. Selective keys are usually illustrations and descriptions of trees in a specific region, e.g., pines of Florida. They are organized for comparative use; the interpreter merely selects the key example that most nearly coincides with the forest stand he must identify. By contrast, elimination keys require the user to follow a step-by-step procedure, working from the general to the specific. One of the more common forms of elimination keys is the dichotomous type. Here the interpreter must continually select one of two contrasting alternatives until he progressively eliminates all but the item being sought.

A sample elimination key for identifying northern conifers is reproduced here. It may be used to identify tree species pictured in the large-scale stereograms in figure 11. In original form, this Canadian key had additional descriptive materials and illustrations such as those shown in figures 9 and 10 (*16*).

Vegetation keys are most easily constructed for northern and western forests where conifers predominate, because there are relatively few species to be considered and crown patterns are rather distinctive for each important group. By con-

trast, few if any, reliable keys are available for the highly variable hardwood forests of Southern and Eastern United States.

While the scope of this handbook does not permit a detailed treatment of all important forest types throughout the United States and Canada, examples are given in figures 12 through 18.

Key to the Northern Conifers [3]

1. Crowns small, or if large then definitely cone-shaped.
   2. Crown broadly conical, usually rounded tip, branches not prominent ---------- cedar
   2. Crowns have a pointed top, or coarse branching, or both.
      —crowns narrow, often cylindrical, trees frequently grow in swamps------ swamp type black spruce
      —crowns conical, deciduous, very light-toned in fall, usually associated with black spruce-------- tamarack
      —crowns narrowly conical, very symmetrical, top pointed, branches less prominent than in white spruce ---------- balsam fir
      —crowns narrowly conical, top often appears obtuse on photograph (except northern white spruce), branches more prominent than in balsam fir ---------- white spruce, black spruce (except swamp type)
      —crowns irregular, with pointed top, has thinner foliage and smoother texture than spruce and balsam fir---------- jack pine
1. Crowns large and spreading, not narrowly conical, top often not well defined.
   3. Crowns very dense, irregular or broadly conical.
      4. Individual branches very prominent, crown usually irregular ---------- white pine
      4. Individual branches rarely very prominent, crown usually conical ---------- eastern hemlock
   3. Crowns open, oval (circular in plain view)---------- red pine

MAPPING FROM AERIAL PHOTOGRAPHS

Type maps are no longer considered essential by all foresters, but at times their cost may be justified. A general ownership map showing principal roads, streams, forest types, and condition classes may be desired for management planning and illustrative purposes. Also, in making a photo-controlled ground cruise where precise forest-area estimates are required, it may be necessary to measure stand areas on controlled maps of known scale rather than directly on contact prints. This is particularly important where topography causes wide variation in photo scales.

The wise interpreter will delineate only those types that he can consistently recognize. For maximum accuracy, type lines should be drawn under the stereoscope. As lines made with a china-marking pencil are easily removed with carbon tetrachloride or benzene, this method is recommended for preliminary work. Water-soluble ink is also suitable. Permanent markings can be made with drawing ink after types have been verified by ground reconnaissance.

Uncontrolled maps.—Where area measurement is not critical, simple uncontrolled type maps can be prepared at photo scale by direct tracing. Tract boundaries are drawn within the "effective area" [4] of alternate prints in each flight strip. Photographs are interpreted under the stereoscope, and all types and planimetric data are outlined. The detail is then traced onto frosted acetate or vellum, from one annotated print at a time. If boundaries are accurately drawn on interpreted prints to include all of the tract without duplication, the traced data from adjoining prints should match up without difficulty. To assure standardization in type recognition, it is desirable to have one man perform all interpretation work.

Uncontrolled maps are no more accurate for area measurement than the photographs from which they were prepared, but they may suffice for management plans and illustrations. Where flat terrain predominates, average photo scales vary only slightly and tracings may approach the accuracy of controlled maps.

Controlled maps.—Base maps of uniform scale may be required for photo-controlled ground cruises, as precise measures of forest area by type and stand size are essential for accurate volume estimates. In flat terrain, average photo scale can be determined and acreages measured directly on contact prints, but in steep topography variations in photo scale require the transfer of forest types to base maps for accurate area measurement. The most common way of adjusting variable photo scales to controlled maps is by constructing "radial line plots" or by preparing plat sheets from field notes of the General Land Office. As construction of a radial line plot is complex and has been ade-

[3] Reproduced by permission of L. Sayn-Wittgenstein, Forest Research Branch, Canada Department of Forestry (*16*).

[4] If 9- by 9-inch photographs with 60-percent endlap and 30-percent sidelap are assumed, alternate photographs will have effective areas of about 7.2 by 6.3 inches.

PRINCIPAL TREES OF THE FOREST REGIONS

NOTE.—The order indicates the relative importance or abundance of the trees

ROCKY MOUNTAIN FOREST

Northern Portion (Northern Idaho and Western Montana):

Lodgepole pine
Douglas-fir
Western larch
Engelmann spruce
Ponderosa pine
Western white pine
Western redcedar
Grand and alpine firs
Western and mountain hemlocks
Whitebark pine
Balsam poplar

Eastern Oregon, Central Idaho, and Eastern Washington:

Ponderosa pine
Douglas-fir
Lodgepole pine
Western larch
Engelmann spruce
Western redcedar
Western hemlock
White, grand, and alpine firs
Western white pine
Oaks and junipers (in Oregon)

Central Montana, Wyoming, and South Dakota:

Lodgepole pine
Douglas-fir
Ponderosa pine
Engelmann spruce
Alpine fir
Limber pine
Aspen and cottonwoods
Rocky Mountain juniper
White spruce

Central Portion (Colorado, Utah, and Nevada):

Lodgepole pine
Engelmann and blue spruces
Alpine and white firs
Douglas-fir
Ponderosa pine
Aspen and cottonwoods
Pinyons
Rocky Mountain and Utah junipers
Bristlecone and limber pines
Mountain-mahogany

Southern Portion (New Mexico and Arizona):

Ponderosa pine
Douglas-fir
White, alpine, and corkbark firs
Engelmann and blue spruces
Pinyons
One-seed, alligator, and Rocky Mountain junipers
Aspen and cottonwoods
Limber, Mexican white, and Arizona pines
Oaks, walnut, sycamore, alder, boxelder
Arizona cypress

PACIFIC COAST FOREST

Northern Portion (Western Washington and Western Oregon):

Douglas-fir
Western hemlock
Grand, noble, and Pacific silver firs
Western redcedar
Sitka and Engelmann spruces
Western white pine
Port Orford cedar and Alaska cedar
Western and alpine larches
Lodgepole pine
Mountain hemlock
Oaks, ashes, maples, birches, alders, cottonwoods, madrone

Southern Portion (California):

Ponderosa and Jeffrey pines
Sugar pine
Redwood and giant sequoia
White, red, grand, and Shasta red firs
California incense-cedar
Douglas-fir
Lodgepole pine
Knobcone and Digger pines
Bigcone-spruce
Monterey and Gowen cypresses
Sierra and California junipers
Singleleaf pinyon
Oaks, buckeye, California-laurel, alder, madrone

SOUTHERN FOREST

Pine Lands:

Shortleaf, loblolly, longleaf, slash, and sand pines
Southern red, black, post, laurel, cherrybark, and willow oaks
Sweetgum
Winged, American, and cedar elms
Black, red, sand, and pignut hickories
Eastern and southern redcedars
Basswoods

Alluvial Bottoms and Swamps:

Sweetgum and tupelos
Water, laurel, live, overcup, Texas, and swamp white oaks
Southern cypress
Pecan, water and swamp hickories
Beech
River birch
Ashes

Alluvial Bottoms and Swamps:

Red and silver maples
Cottonwoods and willows
Sycamore
Hackberry
Honeylocust
Holly
Redbay and sweetbay
Southern magnolia
Pond and spruce pines
Atlantic white-cedar

CENTRAL HARDWOOD FOREST

Northern Portion:

White, black, northern red, scarlet, bur, chestnut, and chinquapin oaks
Shagbark, mockernut, pignut, and bitternut hickories
White, blue, green, and red ashes
American, rock, and slippery elms
Red, sugar, and silver maples
Beech
Pitch, shortleaf, and Virginia pines
Yellow-poplar
Sycamore
Chestnut
Black walnut
Cottonwoods
Hackberry
Black cherry
Basswoods
Ohio buckeye
Eastern redcedar

Southern Portion:

White, post, southern red, blackjack, Shumard, chestnut, swamp chestnut, and pin oaks
Sweetgum and tupelos
Mockernut, pignut, southern shagbark, and shellbark hickories
Shortleaf and Virginia ("scrub") pines
White, blue, and red ashes
Yellow-poplar
Black locust
Elms
Sycamore
Black walnut
Silver and red maples
Beech
Dogwood
Persimmon
Cottonwoods and willows
Eastern redcedar
Osage-orange

Texas Portion:

Post, southern red, and blackjack oaks
Eastern redcedar, Ashe juniper

FLORIDA AND TEXAS FOREST—TROPICAL

Mangrove, false mangrove
Royal and thatch palms; palmettos
Florida yew
Wild figs
Seagrapes ("pigeon plum")
Blolly
Bahama lysiloma ("wild tamarind")
Wild-dilly
Gumbo-limbo
Poisontree
Inkwood
Button-mangrove
False-mastic ("wild olive")
Fishpoison-tree ("Jamaica dogwood")

NORTHERN FOREST

Northern Portion:

Red, black, and white spruces
Balsam fir
Eastern white, red ("Norway"), jack, and pitch pines
Hemlock
Sugar and red maples
Beech
Northern red, white, black, and scarlet oaks
Yellow, paper, sweet, and gray birches
Quaking and bigtooth aspens
Basswoods
Black cherry
American, rock, and slippery elms
White and black ashes
Shagbark and pignut hickories
Butternut
Northern white-cedar
Tamarack

Southern Portion (Appalachian Region):

White, northern red, chestnut, black, and scarlet oaks
Chestnut
Hemlock
Eastern white, shortleaf, pitch, and Virginia ("scrub") pines
Sweet, yellow, and river birches
Basswood
Sugar and red maples
Beech
Red spruce
Fraser fir
Yellow-poplar
Cucumber magnolia
Black walnut and butternut
Black cherry
Pignut, mockernut, and red hickories
Black locust
Tupelos ("blackgums")
Buckeye

ALASKA FOREST

Coast Forest:

Western hemlock (important)
Sitka spruce (important)
Western redcedar
Alaska cedar
Mountain hemlock
Lodgepole pine
Black cottonwood
Red and Sitka alders
Willows

Interior Forest:

White (important) and black spruces
Alaska paper (important) and Kenai birches
Black cottonwood
Balsam poplar
Aspen
Willows
Tamarack

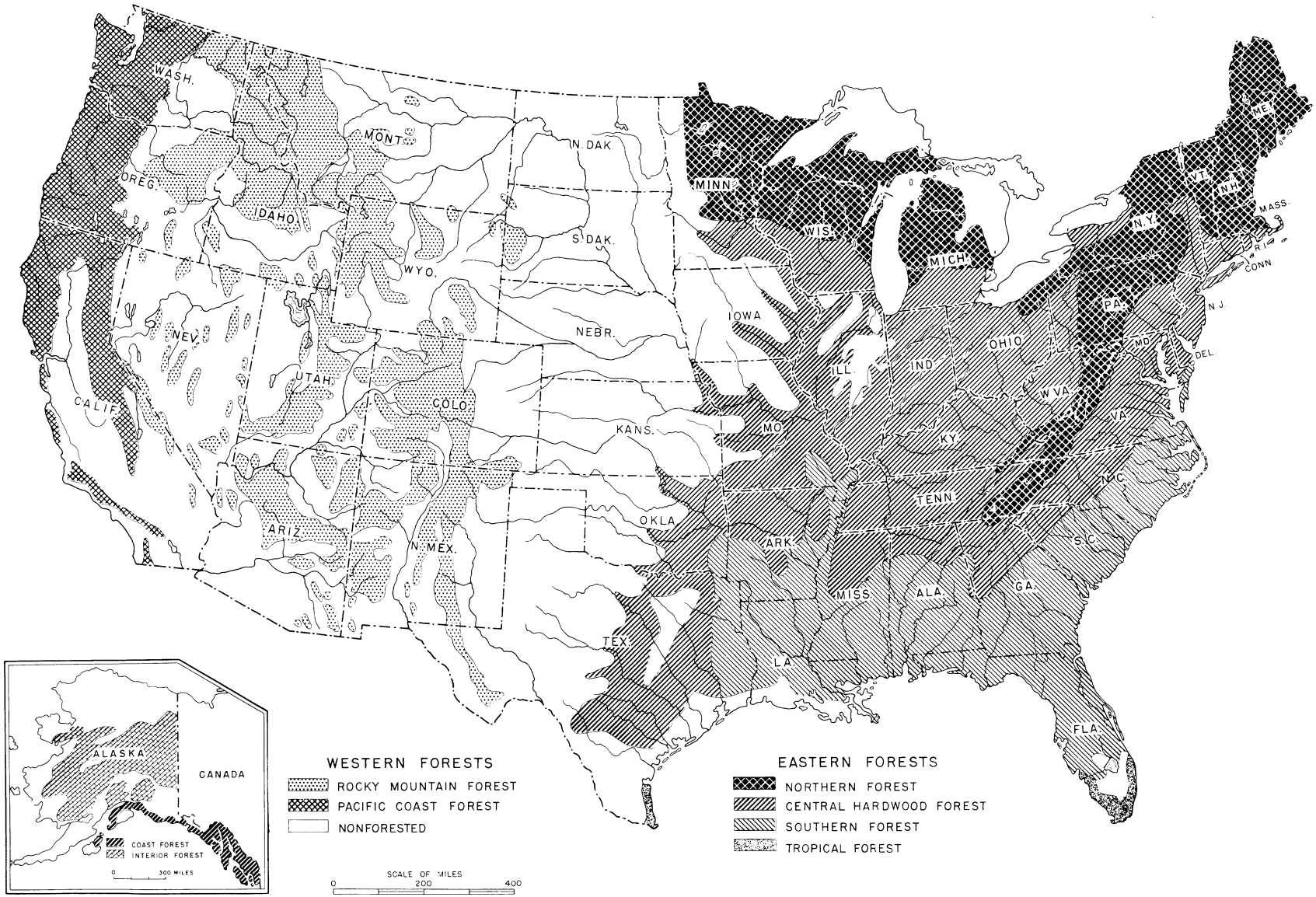


Figure 8.—**Forest regions of the United States.**

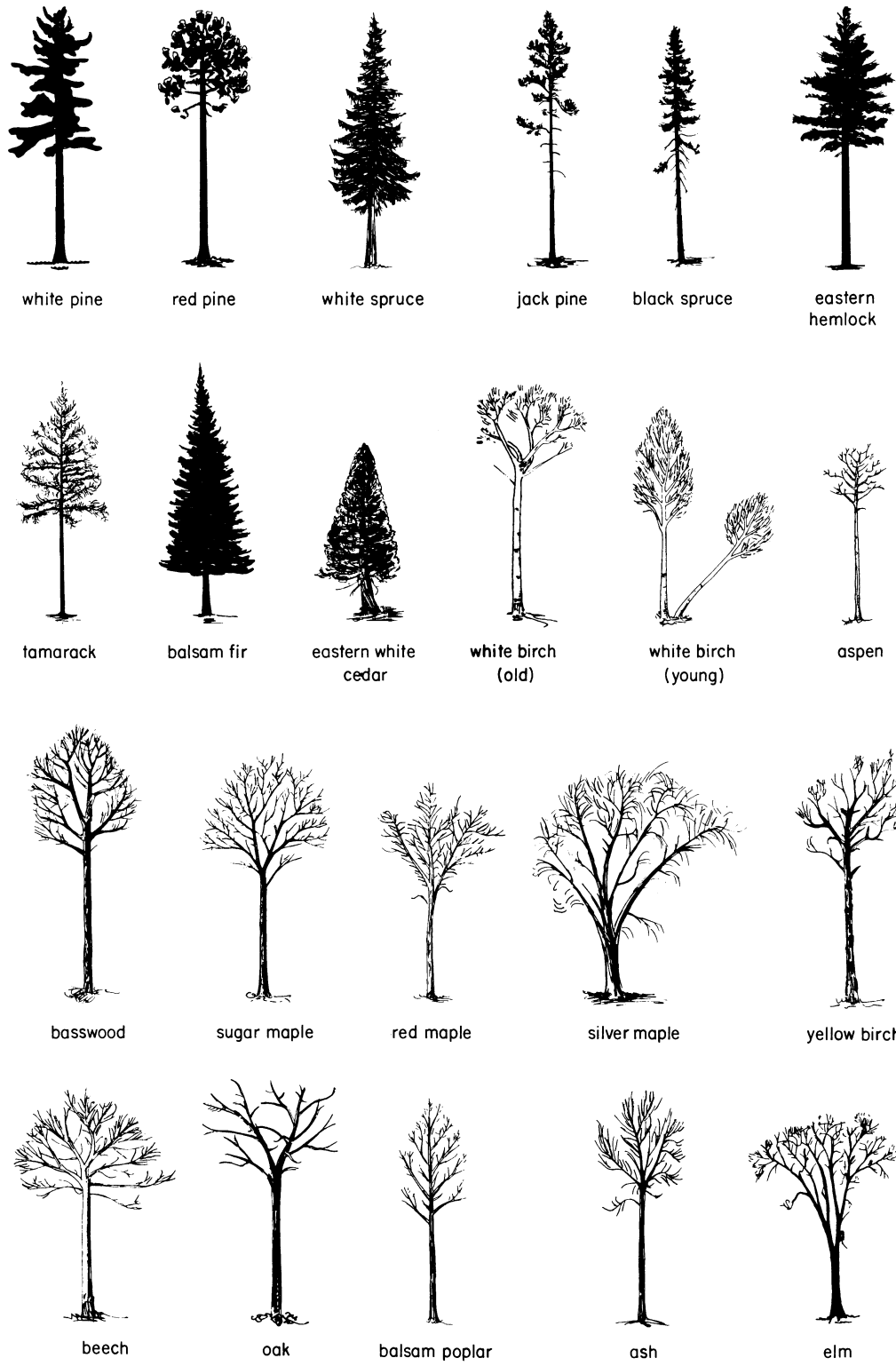


Figure 9.—**Silhouettes of forest trees. When tree shadows fall on level ground, they often permit identification of individual species. (Reprinted by permission of L. Sayn-Wittgenstein, Forest Research Branch, Canada Department of Forestry.)**

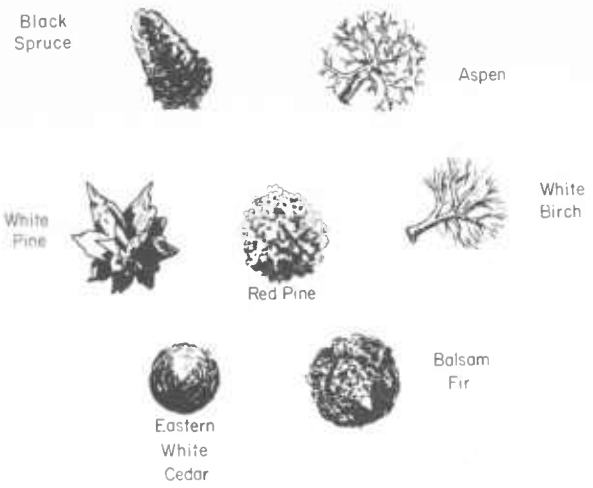


Figure 10.—Vertical views of tree crowns. Compare with stereograms in figure 11. (Reprinted by permission of L. Sayn-Wittgenstein, Forest Research Branch, Canada Department of Forestry.)

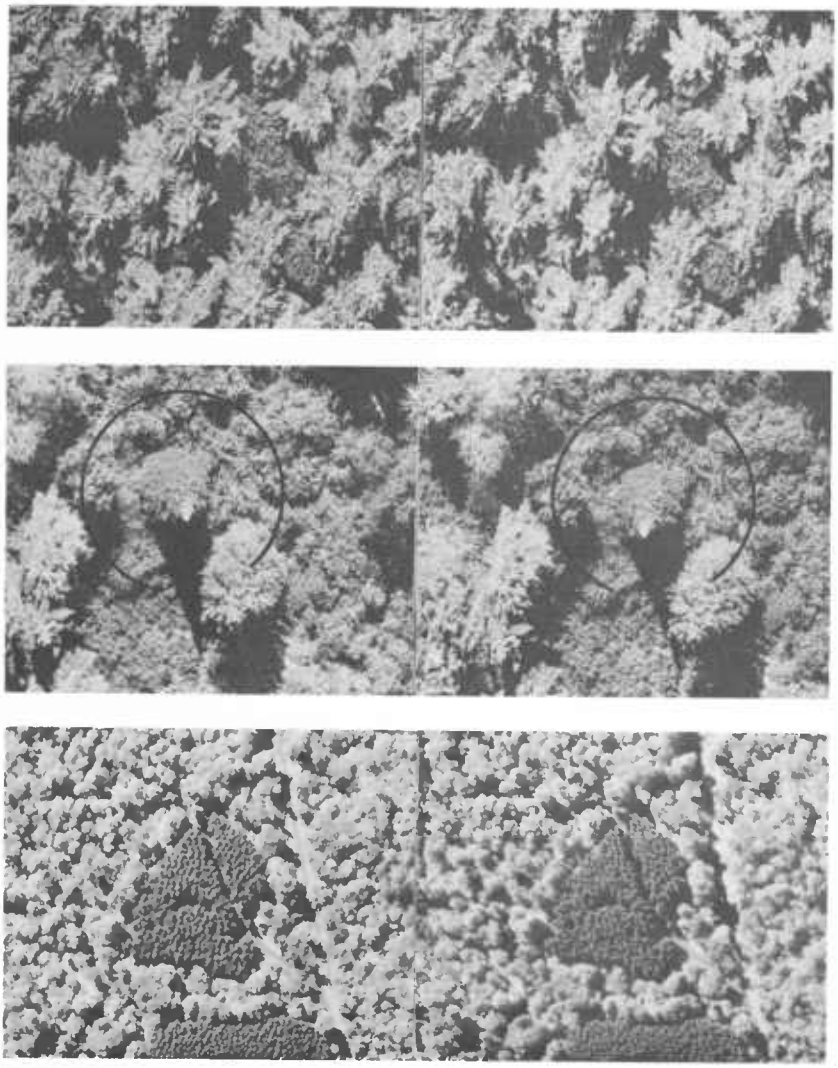


Figure 11.—Large-scale stereograms showing star-shaped white pine crowns (top), cone-shaped balsam fir crowns (center), and a red pine plantation surrounded by a stand of basswood (bottom). The two upper stereograms are on panchromatic film at a scale of 50 feet per inch. The bottom pair is on infrared film at a scale of 330 feet per inch. (Reprinted by permission of L. Sayn-Wittgenstein, Forest Research Branch, Canada Department of Forestry.)

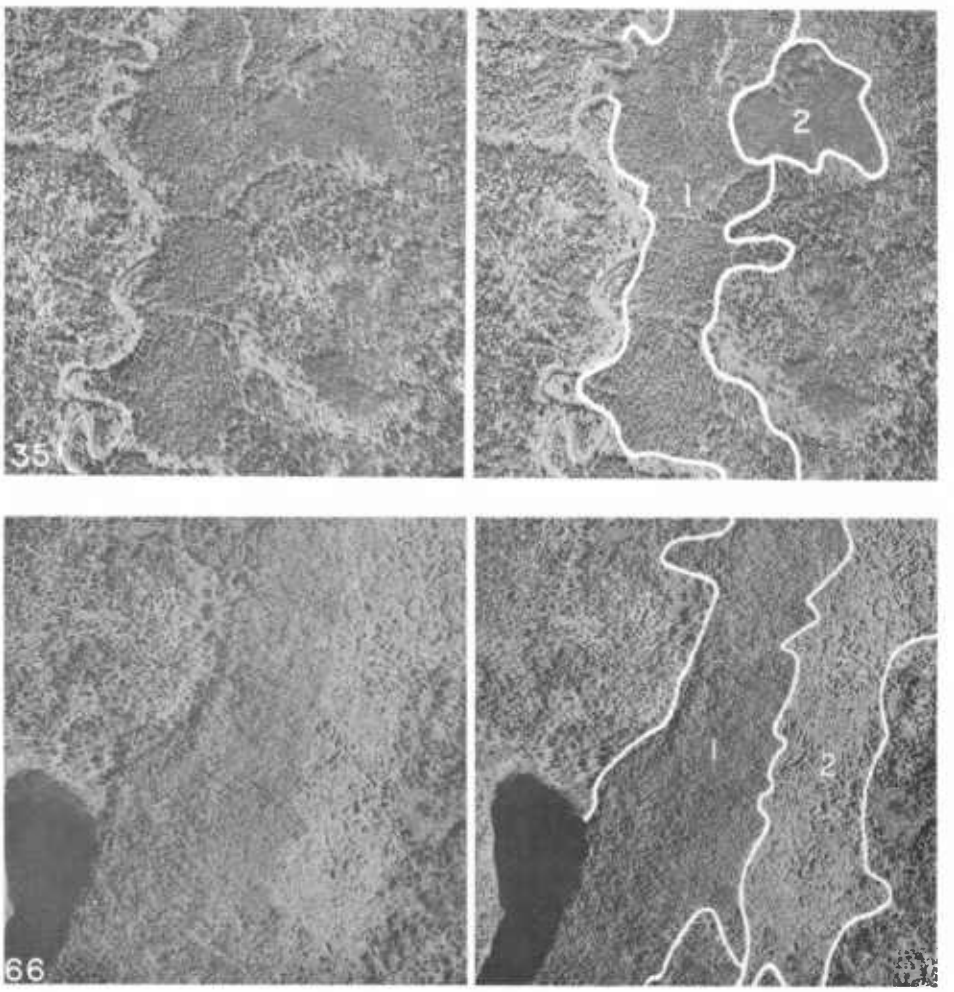


Figure 12.—Summer panchromatic photography in Ontario. In the upper stereogram (No. 35) stand 1 is balsam fir and stand 2 is black spruce. In the lower stereogram (No. 66) stand 1 is aspen-white birch and stand 2 is beech. Scale is 1,320 feet per inch. (Reprinted by permission of V. Zsilinszky, Ontario Department of Lands and Forests, Canada.)

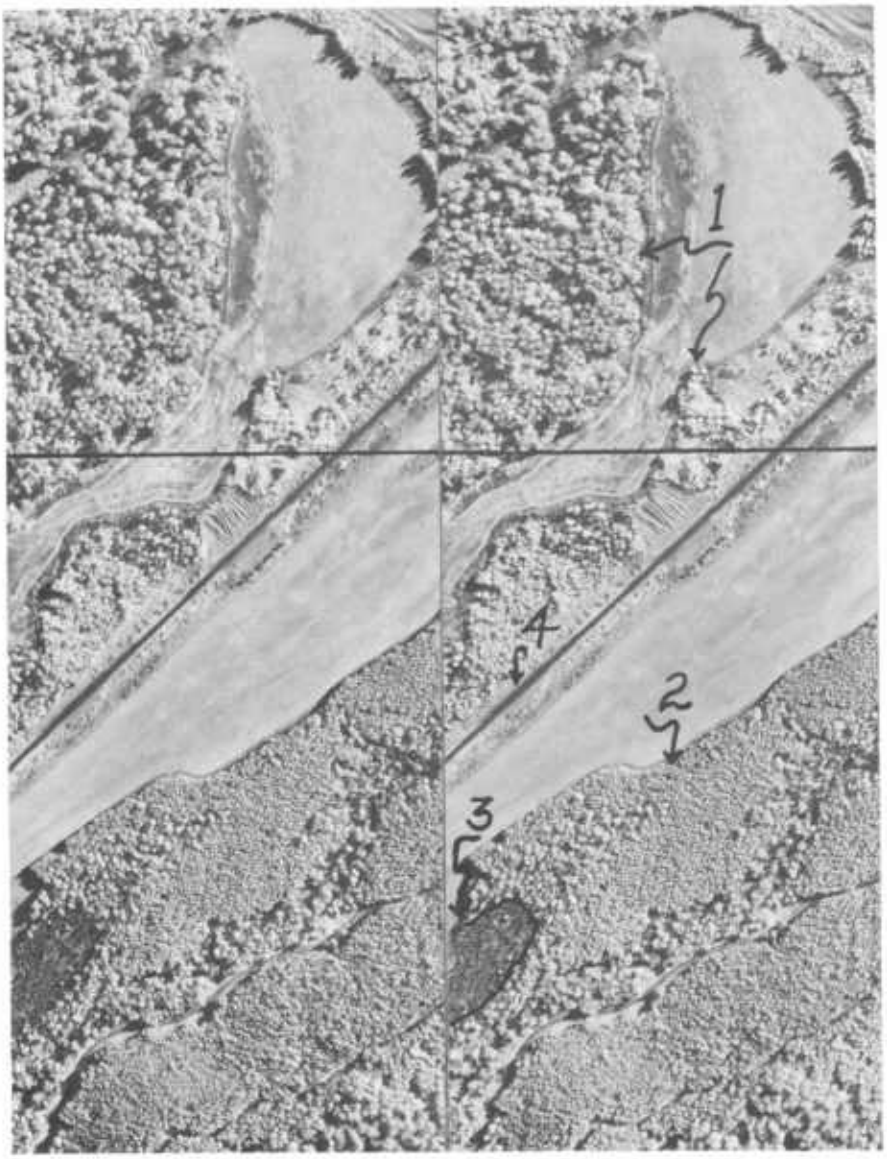


Figure 13.—Infrared stereogram illustrating forest associations in central Alaska. Types are (1) paper birch, (2) aspen, and (3) white spruce. A portion of the Alaska Railroad is shown at (4). Scale is about 420 feet per inch.

Figure 14.—USDA panchromatic stereogram from Del Norte County, Calif. Enclosed trees are primarily redwood, with lesser numbers of Douglas-fir, spruce, and hemlock. Clear stereo-viewing is hindered by the heavy displacement of trees, some of which are 250 to 300 feet tall. Scale is about 1,667 feet per inch.

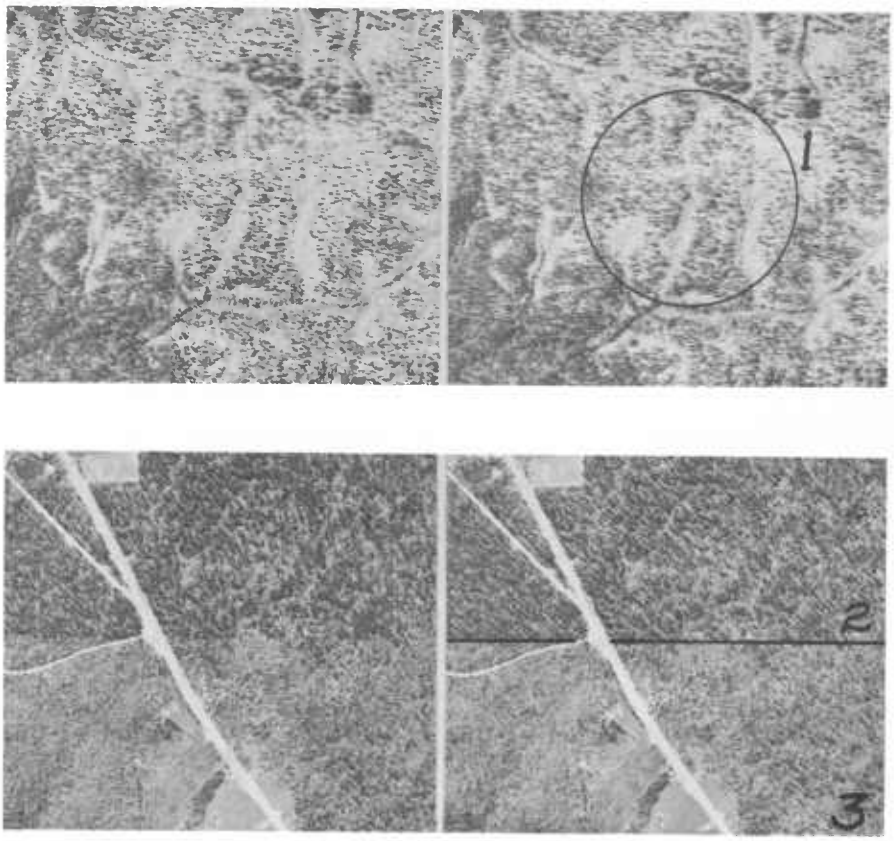
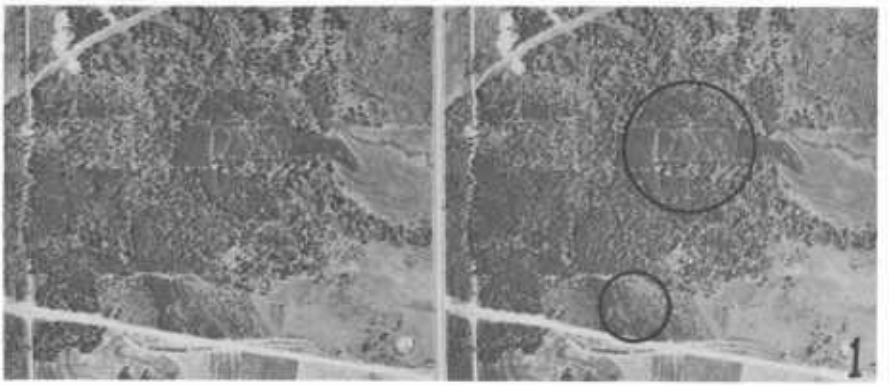


Figure 15.—USDA panchromatic stereograms from Jackson (above) and Clarke Counties, Miss. At (1) is a natural stand of longleaf and slash pines; loblolly-shortleaf pines are pictured at (2) and leafless upland hardwoods at (3). Scale is about 1,667 feet per inch.



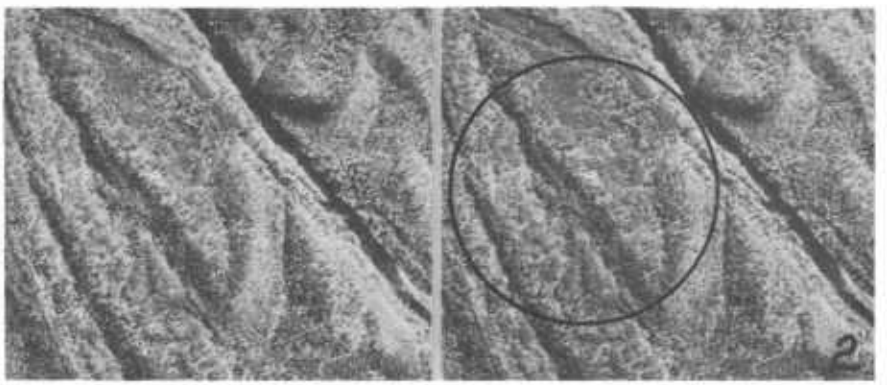


Figure 16.—USDA panchromatic stereograms from Columbia (above) and Sevier Counties, Ark. Two loblolly pine plantations are pictured at (1), while the mountainous terrain at (2) supports a mixture of upland hardwoods and shortleaf pine. Scale is about 1,667 feet per inch.

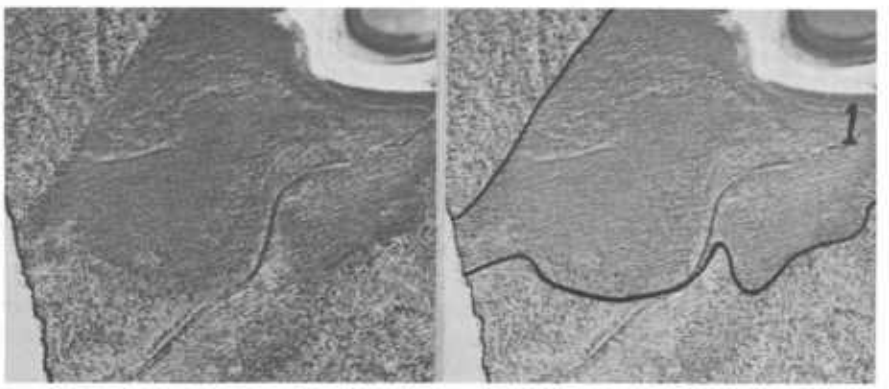


Figure 17.—USDA panchromatic stereograms from Bolivar County, Miss. The fine-textured stand at (1) is willow and cottonwood growing on a recent deposition of sand and silt. At (2) is a stand of bottom-land hardwoods, i.e., oaks, gums, maples, and other wet-site species. Scale is about 1,667 feet per inch.

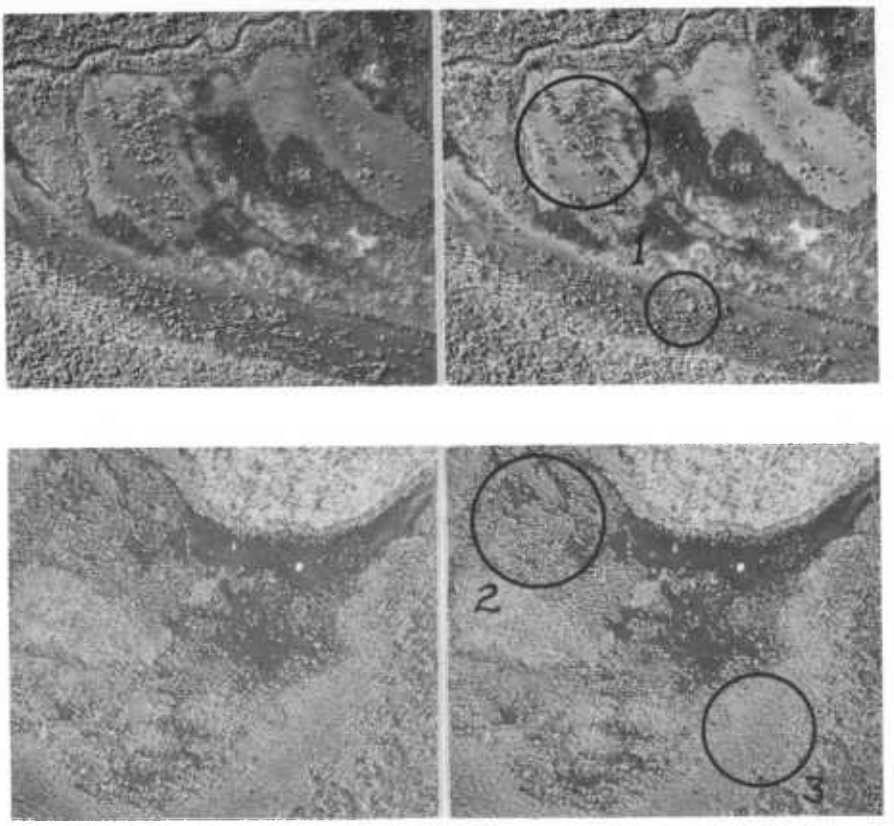


Figure 18.—**USDA panchromatic stereograms from Lafayette County, Ark. Pure stands of southern cypress are shown at (1); the irregular and somewhat star-shaped crowns of this species can be clearly discerned against the water. At (2) is a mixture of cypress and tupelo gum, while a pure stand of tupelo gum is pictured at (3). Scale is about 1,667 feet per inch.**

quately treated in several readily available publications (*1*, *17*, *18*), it will not be reviewed here.

General Land Office (GLO) plats.—Most of the United States west of the Mississippi River and north of the Ohio River, plus Alabama, Mississippi, and portions of Florida, was originally subdivided under the U.S. Public Land Survey. Township, range, and section lines are often visible on aerial photographs. If enough such lines and corners can be identified, GLO plats can be constructed for use as base maps from field notes available at State capitals or county offices. To do this, a GLO plat showing sections, quarter sections, and forties is drawn to average photo scale from field notes. As many as possible of the same lines and corners are pinpointed on the aerial photographs, preferably arranged in a systematic framework throughout the forest property. Ownership maps, county highway maps, and topographic quadrangle sheets may help to identify such corners, but additional points must usually be found by taking the photographs into the field. The accuracy of this method depends upon the number of grid lines and corners which can be pinpointed on the aerial photographs. The technique described is adapted from Johnson (*7*).

When photo interpretation of forest types has been completed, the detail is transferred to the plat, one square of the grid being completed at a time. If the plat and photographs are of the same scale, transfer can be made by direct tracing on a light table; where scales differ, a vertical sketchmaster is recommended (fig. 19). By moving this instrument up or down on its adjustable legs, maps can be drawn at scales of seven-tenths to one and one-half times the scale of the contact print. The sketchmaster accommodates a single, annotated print, which is placed face up on the platform under a large mirror. Photo images are reflected from the large mirror to a semisilvered mirror in the eyepiece housing. The semitransparent eyepiece mirror thus provides a monocular view of the reflected photo image superimposed on the base map. When the grid points on photograph and map have been matched, the transfer of detail becomes a simple procedure (fig. 20).

Topographic and county maps.—Topographic quadrangle sheets and county highway maps are often useful in preparing base maps and identifying features on aerial photographs. When available, 7½-minute quadrangle maps at a scale of 1:24,000 provide excellent base maps, and can be

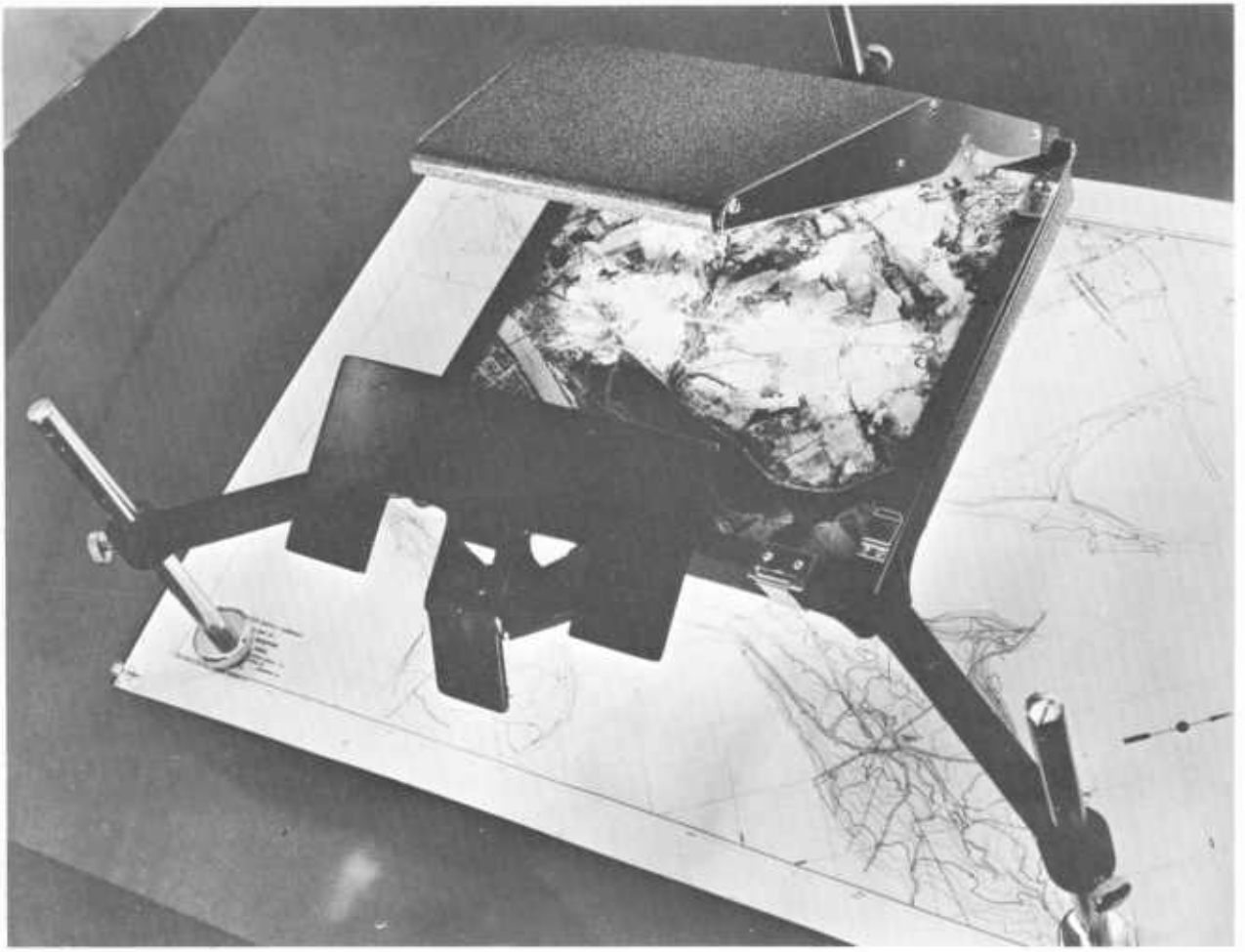


Figure 19.—**Vertical sketchmaster for transferring detail from single contact prints to a base map. A semisilvered eyepiece mirror enables the operator to view photograph and map simultaneously. (Courtesy of Aero Service Corporation.)**

purchased for about 30 cents per copy. Maps for areas west of the Mississippi River, including all of Louisiana and Minnesota, can be purchased from

U.S. Geological Survey
Distribution Section
Federal Center
Denver, Colo. 80225

For areas east of the Mississippi River, including Puerto Rico and the Virgin Islands, maps may be purchased from

U.S. Geological Survey
Distribution Section
Washington, D.C. 20240

Maps of Hawaii may be ordered at either address. All orders must be paid in advance. Other sources of topographic quadrangle maps are the Maps and Surveys Branch of the Tennessee Valley Authority, Chattanooga, Tenn.; the Mississippi River Commission, U.S. Army Corps of Engineers, Vicksburg, Miss.; and the U.S. Coast and Geodetic Survey, Department of Commerce, Washington, D.C.

County maps, usually obtained from State highway departments, may serve as base maps when a high level of accuracy is not required. They show township, range, and section lines, in addition to geographic coordinates (longitude and latitude) to the nearest 5 minutes. They are usually printed at a scale of about one-half inch per mile. Although bearings of section lines are not shown, such maps are more reliable than oversimplified plats showing idealized sections oriented exactly with the cardinal directions. Portions of county maps can be enlarged to photo scale and sections subdivided into quarters or forties by proportionate measurement. These maps may be especially helpful in preparing GLO plats as previously outlined.

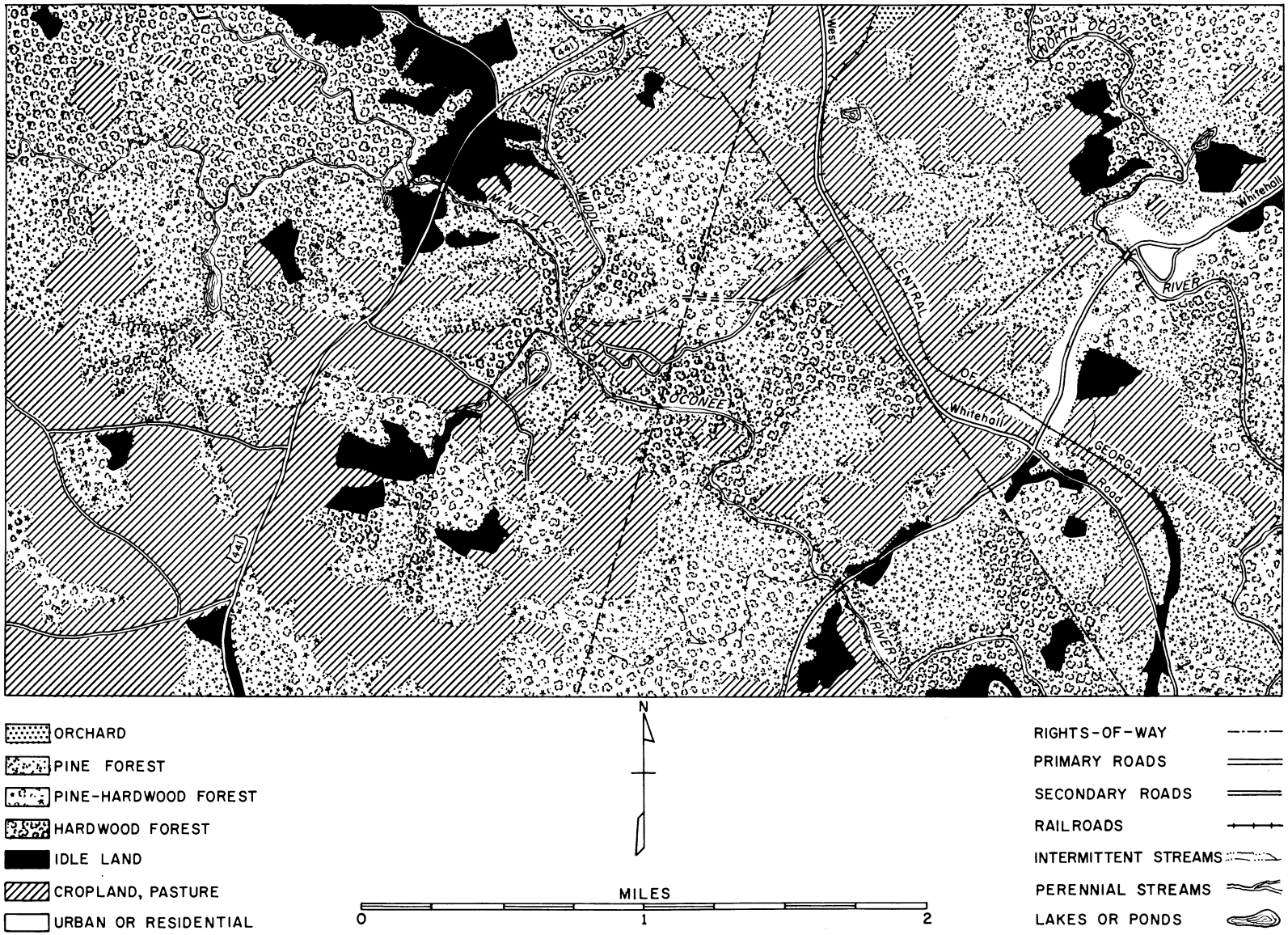


Figure 20.—**Photo mosaic assembled from 1960 USDA prints, and corresponding map compiled with the vertical sketchmaster. The area is in Clarke County, Ga.**

MEASURING AREAS

Both aerial and ground cruising require accurate measurement of forest areas. Photographs offer an inexpensive means of making such determinations. In locations where photo scales are not appreciably altered by topographic changes, areas can be measured directly on contact prints. Greater accuracy is possible if forest types are transferred to controlled base maps before area is determined. This procedure is essential for mountainous terrain. On the other hand, if only relative proportions of the forest types are needed and measurements are limited to the effective areas of contact prints, no bias results from using photographs, even when local relief ranges from 500 to 1,000 feet (*12, 19*). (This statement assumes that, for large tracts, errors in measurement of areas below the datum plane are compensated by errors of a similar magnitude above the datum plane.) Small tracts in rough topography should be measured on controlled maps. Measurement techniques are similar in both cases, so the procedures outlined for measuring area on photographs generally apply to map determinations.

Devices for area measurement.—The principal devices for area measurement are polar planimeters, transects, and dot grids.

The planimeter is relatively expensive and its use somewhat tedious. The pointer is carefully run clockwise around the boundaries of an area two or more times (for an average reading). From the vernier scale, the area is read in square inches and then converted to the desired units, usually acres, on the basis of photo or map scale.

The transect method is analogous to determining forest area by a strip cruise in which the chainage encountered in each forest type is recorded. An engineer's scale is alined on the photographs to cross topography and drainage at approximately right angles. The length of each type along the scale is recorded to the nearest tenth of an inch. Proportions for each type are developed by relating the total measure of that type to the total linear measure. For example, if six equally spaced parallel lines 6 inches long are tallied on a given photograph, the total transect length is 36 inches. If hardwoods are intercepted for a total measure of 7.2 inches, this particular type would be assigned an acreage equivalent to $7.2 \div 36$, or 20 percent of the total area. The transect method is simple and requires a minimum of equipment. For making rough area estimates on photo index sheets, special transparent overlays for location of transect lines can be improvised (*9*).

Use of a dot grid is the preferred method for determining area on aerial photographs. A dot grid is a transparent overlay with dots systematically arranged on a grid pattern. In use, the grid is alined with a straight-line feature to avoid positioning bias, and then dots are tallied for each forest type (fig. 21). Type areas are calculated by proportions: the number of dots on a given type divided by the total number of dots counted yields a percentage value that is multiplied by the total area to obtain the acreage of the type. If total acreage is not known, the number of acres per square inch is determined. This figure is then divided by the number of dots per square inch to find the acreage represented by each dot.

Intensity of dot sampling.—The number of dots that must be counted for a given accuracy depends upon the estimated proportion of the total area occupied by the most important classification to be recognized. For example, suppose area breakdowns are needed for 10 square miles photographed at a scale of 1:15,840. Estimated proportions of each area classification are as follows: forest, 25 percent; agricultural lands, 60 percent; urban areas, 10 percent; and rivers and lakes, 5 percent. If the most important category is agricultural land, the dot grid intensity would be calculated on this basis. If the population being sampled is large, the number of samples may be computed by a formula based on the binomial distribution:

$$n = p(1-p)\left[\frac{t}{E}\right]^2$$

Where: n = total number of samples (dots) to be counted.
p = estimated proportion of the total area in the most important type classification (0.60 in this case).
t = a constant denoting the reliability of the estimate or level of statistical significance (the value 1.96 used here denotes a statistical probability of being correct 95 times in 100).
E = maximum permissible error, expressed as a percent of total area. (In this case, ±2 percent or 0.02.)

Substituting the above values, we get:

$$n = 0.60(1-0.60)\left[\frac{1.96}{0.02}\right]^2 = 2{,}305 \text{ dots}$$

Thus if we are correct in the assumption that the true percentage of agricultural land is 60, then 2,305 dots should be spaced over the total area to insure a 95-percent probability of obtaining an estimated proportion lying between 58 and 62 percent. At the specified photo scale of 1:15,840, the total print area represented by 10 square miles would be 160 square inches. Therefore, the number of dots needed per square inch would be 2,305 ÷160, or about 14. Here, it would be most expedient to select a square-spaced grid having 16 dots per square inch.

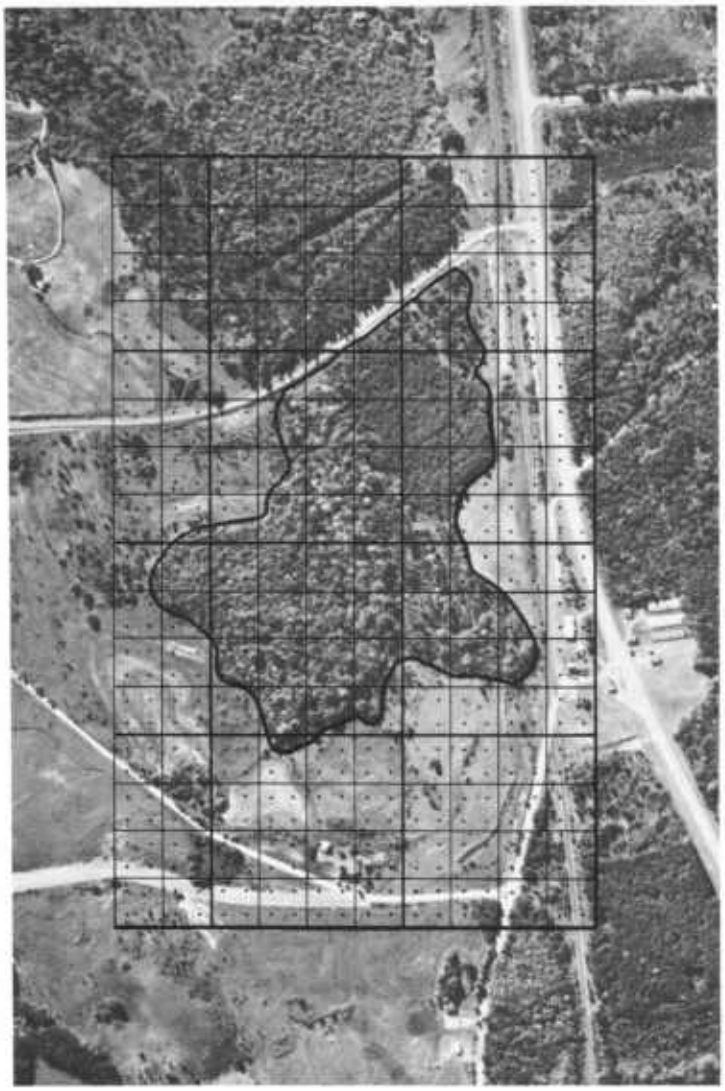


Figure 21.—**Dot grid positioned over part of an enlarged USDA print for acreage determination. The delineated stand contains about 25 acres. Photo scale is 660 feet per inch.**

The principal drawback to the formula method is that a prior knowledge of p is required, which is actually the value being sought. By definition, however, p always lies between 0 and 1, and it can be shown that $p(1-p)$ reaches a maximum value of 0.25 when p is set at 0.50 or 50 percent. Therefore, the equation may be revised to read:

$$n=0.25\left[\frac{t}{E}\right]^2$$

And, substituting values from the previous solution:

$n=0.25\left[\frac{1.96}{0.02}\right]^2=2{,}401$ dots, an increase of 96 dots over the first estimate.

A grid with 16 dots per square inch will still be adequate for the desired degree of accuracy ($16\times160=2{,}560$ dots).

For areas of 1,000 acres or less, grids with closely spaced dots are needed. Grids with 64 dots per square inch are commonly used with 1:20,000 photographs. As 1 square inch equals 63.77 acres at photo scale, each dot represents 0.996 acres. For 1:15,840 photography (40 acres per square inch), grids having 40 dots per square inch are available. It is not essential, of course, that a separate grid be used for each photo scale or that the number of dots per square inch be equal to the acreage per square inch. Wherever feasible, the preceding equation should be used to determine the grid intensity.

Tree Height

Tree heights are commonly determined on aerial photographs by measuring either stereoscopic parallax or shadow lengths. Though more difficult for the beginner, the parallax method is faster, requires fewer calculations, and is more adaptable to a variety of stand conditions. Anyone who can use a stereoscope can train himself to measure stereoscopic parallax, and even the occasional interpreter will find this method of measuring heights advantageous.

Shadow-length measurements are reliable only in open-grown stands where individual shadows fall on level ground. Accurate measurement is almost impossible in dense, irregular stands or on slopes. Furthermore, the conversion of shadow length to tree height is complex in comparison to the conversion of parallax measurements. For these reasons only the parallax method will be discussed. Foresters interested in details of shadow-height calculations should refer to Johnson's article (*8*), which includes a special form for making tree-height conversions.

The concept of parallax.—The Manual of Photogrammetry (*1*) defines parallax as "the apparent displacement of the position of a body with respect to a reference point or system, caused by a shift in the point of observation." In measuring object heights on stereoscopic pairs of aerial photographs, two types of parallax must be measured or approximated—the absolute and the differential. The absolute stereoscopic parallax of a point is "the algebraic difference, parallel to the air base, of the distances of the two images from their respective principal points" (*18*). The parallax difference, or differential parallax, of an object being measured for height determination is the difference in the absolute stereoscopic parallax at the top and the base of the object, measured parallel to the air base or flight line.

The formula for converting parallax measurements to tree height on aerial photographs is:

$$h=\frac{H\times dP}{P+dP}$$

where h = height of object
H = altitude of aircraft above ground datum
P = absolute stereoscopic parallax at base of object being measured
dP = differential parallax

If object heights are to be determined in feet, the height of the aircraft (H) must also be in feet. Absolute stereoscopic parallax (P) and differential parallax (dP) must be expressed in the same units; ordinarily, these units will be thousandths of inches or hundredths of millimeters.

The height of the aircraft above ground datum is calculated from the basic scale formula, transposed to the more convenient form: Flight altitude (H) = focal length × scale denominator. With photographs of 1:20,000 scale and a camera of 8.25-inch focal length, the flight altitude would be $0.6875\times20{,}000=13{,}750$ feet.

In flat terrain, the average photo base length is ordinarily substituted as the absolute stereoscopic parallax (P). If the ground elevation at the base of the tree being measured differs from the elevation of the principal points by more than 200 or 300 feet, however, the following method (*17*) should be used to calculate a new value for P:

1. Orient the stereo-pair with flight lines superimposed and images separated about 2.2 inches. Clip down photographs.
2. Measure the distance between the two principal points to the nearest 0.01 inch with an engineer's scale.
3. Measure the distance between corresponding images on the two photographs at or near the base of the tree to the nearest 0.01 inch.
4. Subtract (3) from (2) to obtain the absolute stereoscopic parallax at the base of the tree.

Differential parallax (dP) is usually measured stereoscopically with either a parallax wedge or parallax bar, employing the "floating mark" principle. Such instruments are discussed in the section that follows. The concept of differential parallax can be illustrated by direct measurement of severely displaced images such as in the large-scale stereogram of a water tank in figure 22. With a photo scale of 1:7,800 and a camera focal length of 6 inches, flight altitude above ground (H) is computed as $0.5\times7{,}800$ or 3,900 feet. Average photo base length (P) for the stereo-pair is 3.70 inches.

Absolute stereoscopic parallax at the base and top of the water tank is measured parallel to the line of flight with an engineer's scale; the difference (2.27−2.13 inches) is dP, the differential parallax of the displaced images. As the tank is somewhat tapered in form, measurements were made at the midpoint of the base and vertically above this position at the center of the top. Substituting in the parallax formula:

$$\text{Height of tank } (h)=\frac{3{,}900\times0.14}{3.70+0.14}=\frac{546.00}{3.84}=142 \text{ feet}$$

Parallax wedges.—Parallax wedges are usually printed on transparent film or glass. The basic design consists of two rows of dots or graduated lines beginning about 2.5 inches apart and converging to about 1.8 inches apart. The graduations on each line are calibrated for making parallax readings to the nearest 0.002 inch. The "training wedge" in figure 23 is graduated for reading to the nearest 0.01 inch only.

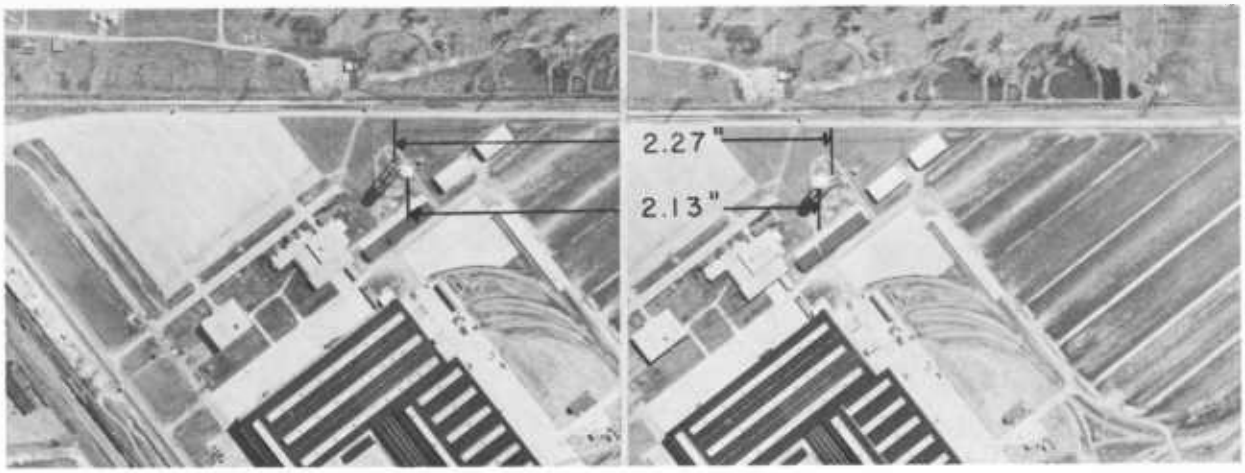


Figure 22.—Large-scale stereogram showing an industrial plant and heavily displaced water tank. Measurements of stereoscopic parallax shown can be used to determine height of the tank above ground. (Courtesy of Abrams Aerial Survey Corporation.)

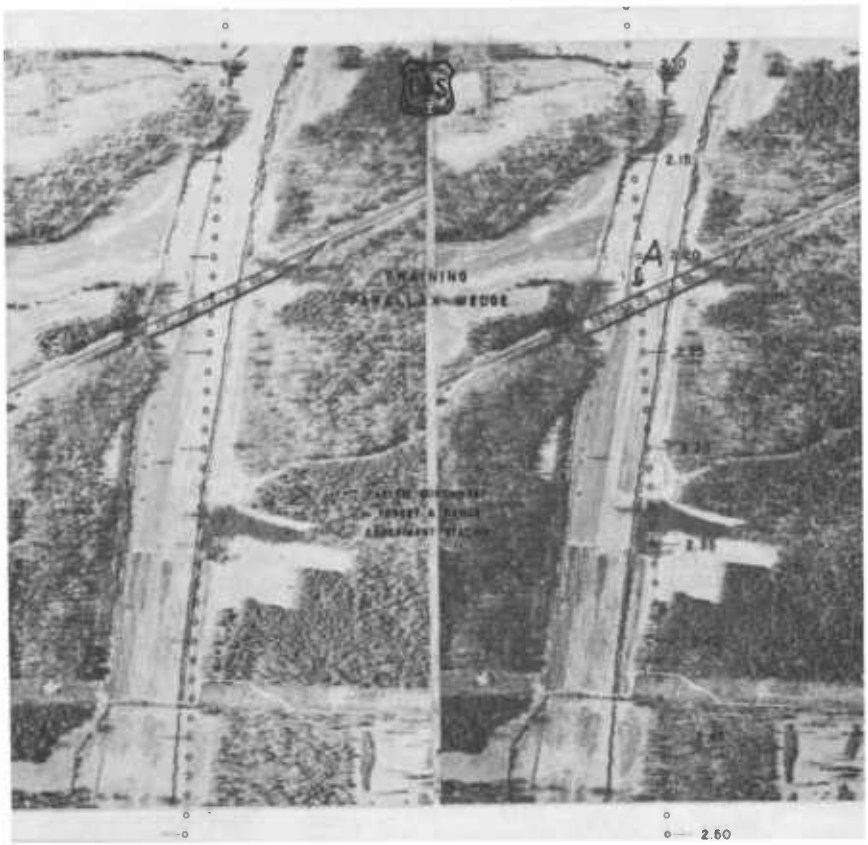


Figure 23.—Parallax wedge correctly oriented over a large-scale stereogram of a railroad trestle. Graduations on right-hand row of dots refer to separation of the converging lines in inches. (Courtesy of Abrams Aerial Survey Corporation.)

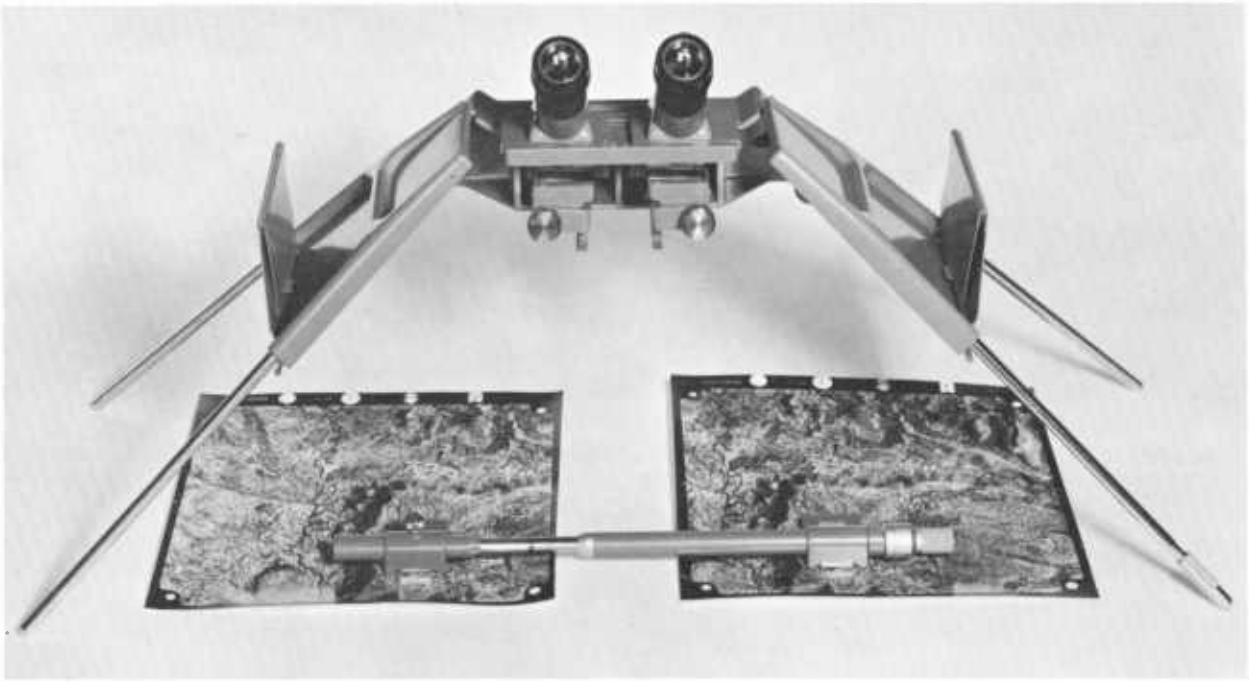


Figure 24.—**Modern mirror stereoscope with inclined magnifying binoculars. Positioned across the two photographs is a parallax bar (stereometer) for measuring heights of objects. (Courtesy of Wild-Heerbrugg Instruments, Inc.)**

The parallax wedge is placed over the stereoscopic image with the converging lines perpendicular to the line of flight and adjusted until a single fused line of dots or graduations is seen sloping downward through the stereoscopic image. If the photo images are separated by exactly 2 inches, a portion of the parallax wedge centering around the 2-inch separation of converging lines will fuse and appear as a single line. The line will appear to split above and below this section. Using the fused line of graduations, the differential parallax is obtained by counting the number of dots or intervals between the point where a graduation appears to rest on the ground and the point where a graduation appears to "float" in the air at the same height as the top of the object. In figure 23, for example, the dot resting on top of the railroad trestle yields a reading of 2.22 inches. When this value is subtracted from a ground reading of 2.26 inches, dP is determined as 0.04 inches. If flight altitude (H) of 4,000 feet and a photo base length of 3.56 inches, the parallax formula yields:

$$\text{Height of trestle } (h) = \frac{4{,}000 \times 0.04}{3.56 + 0.04} = \frac{160.00}{3.60} = 44 \text{ feet}$$

The interpreter should remember that the degree of stereoscopic parallax normally encountered on 1:12,000 to 1:20,000 USDA photographs is much less than that illustrated here. Nevertheless, the principle and the methods of measurement are exactly the same. Where P is large in relation to dP, tables 2 and 3 can be used as shortcut approximations in converting parallax measurements to object heights on USDA photographs.

The parallax bar.—This instrument is more expensive than the parallax wedge and yields results of comparable accuracy. But many interpreters prefer the parallax bar because the floating dot is movable and thus easier to place on the ground and at crown levels. A parallax bar designed to measure heights with a mirror stereoscope is shown in figure 24.

The bar has two lenses attached to a metal frame that houses a vernier and a graduated metric scale. The left lens contains the fixed reference dot; the dot on the right lens can be moved laterally by means of the vernier. The bar is placed over the stereoscopic image parallel to the line of flight. The right-hand dot is moved until it fuses with the reference dot and appears to rest on the ground at the base of the tree. The vernier reading is recorded to the nearest 0.01 millimeter. The vernier is then turned until the fused dot appears to "float" at treetop level, and a second reading recorded. The difference between the readings is the parallax difference (dP) in millimeters. This value can be substituted in the parallax formula without conversion if the absolute parallax (P) is also expressed in millimeters.

Accuracy of height measurements.—Accuracy in

TABLE 2.—*Parallax-wedge conversion factors for wedges reading to 0.002-inch parallax (dP)*[1]

Photo base (*P*) (inches)	Object height in feet per 0.002 inch of *dP*, at flight altitudes of —				
	6,000 feet	8,000 feet	10,000 feet	12,000 feet	14,000 feet
2.6	4.6	6.1	7.7	9.2	10.8
2.7	4.4	5.9	7.4	8.9	10.4
2.8	4.3	5.7	7.1	8.6	10.0
2.9	4.1	5.5	6.9	8.3	9.6
3.0	4.0	5.3	6.7	8.0	9.3
3.1	3.9	5.2	6.4	7.7	9.0
3.2	3.7	5.0	6.2	7.5	8.7
3.3	3.6	4.8	6.1	7.3	8.5
3.4	3.5	4.7	5.9	7.0	8.2
3.5	3.4	4.6	5.7	6.8	8.0
3.6	3.3	4.4	5.6	6.7	7.8
3.7	3.2	4.3	5.4	6.5	7.6
3.8	3.1	4.2	5.3	6.3	7.4
3.9	3.1	4.1	5.1	6.1	7.2
4.0	3.0	4.0	5.0	6.0	7.0

[1] To use table, measure parallax difference (*dP*) of object to nearest 0.002-inch (as 0.016 or 8 dot intervals on wedge). If average photo base (*P*) is 3.6 inches and flight altitude is 14,000 feet, the table value of 7.8 is multiplied by the 8 dot intervals for an object height of 62 feet.

TABLE 3.—*Parallax-bar conversion factors for use with devices reading to 0.01-mm. parallax (dP)*[1]

Photo base (*P*) (inches)	Object height in feet per millimeter of dP at flight altitudes of—				
	6,000 feet	8,000 feet	10,000 feet	12,000 feet	14,000 feet
2.6	90	119	149	179	209
2.7	86	115	144	172	201
2.8	83	111	139	166	194
2.9	80	107	134	161	187
3.0	78	104	130	155	181
3.1	75	100	125	151	176
3.2	73	97	122	146	170
3.3	71	94	118	142	165
3.4	69	92	114	137	160
3.5	67	89	111	133	156
3.6	65	87	108	130	152
3.7	63	84	105	126	147
3.8	62	82	103	123	144
3.9	60	80	100	120	140
4.0	58	78	97	117	136

[1] To use table, measure parallax difference (*dP*) of object to nearest hundredth of a millimeter (as 0.57 mm., for example). If average photo base (*P*) is 3.1 inches and flight altitude is 12,000 feet, the table value of 151 is multiplied by 0.57 for an object height of 86 feet.

measuring total heights of trees and stands depends upon a number of factors, not the least of which is the interpreter's ability to determine stereoscopic parallax. Usually interpreters can detect differences in parallax of about 0.002 inch, or 0.05 mm., and this graduation interval is used on most parallax wedges.

The interpreter who can detect a difference of 0.002 inch of stereoscopic parallax will be able to stratify forest stands into 10-foot total height classes on contact prints of 1:15,840 to 1:20,000 scales (*18*). Greater accuracy may be possible in flat terrain where photo scale changes are not pronounced and less skill is required in selecting the point for the base parallax reading. The ground parallax must be read on the same contour as the base of the tree.

The interpreter should consider the following points to improve accuracy in height measurement:

1. In rough terrain, a new photo scale and flight altitude should be calculated for each overlap. For stands on high ridges or in deep ravines, it is better to calculate new values for absolute stereoscopic parallax than to use the average photo base length.
2. Once a pair of photographs have been alined for stereo-viewing, they should be fastened down. A slip of either photograph between the parallax reading at the base and the top of a tree may cause highly inaccurate height readings.
3. To avoid single measurements of high variability, several measurements should be made of the same tree or stand and the results averaged.

Tree Crown Diameter

For most conifers and many hardwoods, tree crown diameter is related to stem diameter. It is thus a useful photographic measurement when estimating individual tree volumes or stand-size classes. Actual determination of crown diameter is a distance measurement, somewhat complicated by the small sizes of tree images and the effects of crown shadows.

Crown diameters are measured with either wedges or dot-type scales reading in thousandths of an inch. With a crown wedge, the diverging lines are placed tangent to both sides of the crown for making the reading. Dot-type scales have circles of graduated sizes for direct comparison with tree crowns (fig. 25). For converting measurements, the scale of photography is calculated in feet per thousandth of an inch. At 1:20,000, each 0.001 inch of crown measure equals 1.667 feet. A reading of 0.010 inch would imply a crown diameter of 17 feet (table 4).

Tree crowns are rarely circular, but, because individual limbs are often invisible on aerial photographs, they usually appear roughly circular or elliptical. Since only the parts visible from above can be evaluated, photo measures of crown diameter are often lower than ground checks of the same trees. Nevertheless, most interpreters can determine average crown diameter with reasonable precision if they take several readings.

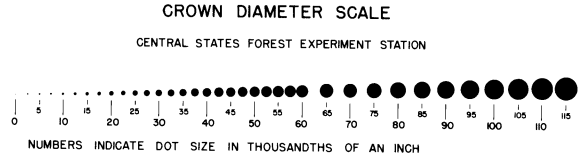


***Figure 25.*—Dot-type scale for measuring crown diameters. Such scales are usually printed on transparent film.**

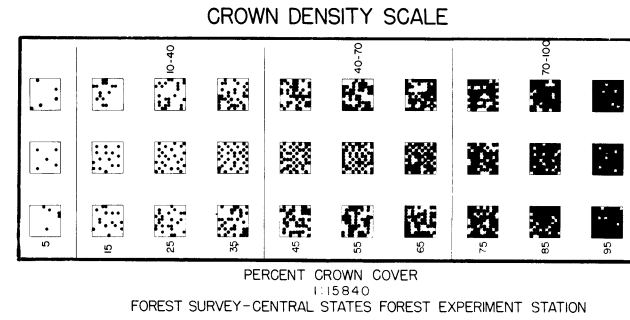


***Figure 26.*—Density scale for comparison with photo images in estimating crown closure percent.**

Obviously, crown diameter measurements of individual trees are most accurate in open-grown stands. In dense stands, measurements are generally confined to determination of an average for the dominant trees. Crowns of mature conifers can usually be classified into 5-foot classes without difficulty (*18*).

Tree Crown Closure

Crown closure percent, also referred to as crown density, is the proportion of the forest canopy occupied by trees. Crown density may refer to all crowns in the stand regardless of canopy level or only to the dominants. Estimates are purely ocular, and stands are commonly grouped into 10-percent density classes. Printed density scales (fig. 26) may aid the interpreter, though the patterns of black dots on a white background bear little resemblance to photographic images of trees. Comparative stereograms illustrating various stand densities have also proved useful (fig. 27).

Evaluation of crown closure is much more subjective than the determination of tree height or crown diameter. Actual measurement is virtually impossible on most USDA photographs, and accuracy is thus dependent on the interpreter's judgment. Inexperienced interpreters tend to overestimate closure by ignoring small stand openings or including portions of crown shadows. Devices for checking closure on the ground fail to provide estimates that are truly comparable to those made on vertical photographs. Thus the neophyte must rely on practice, checked by skilled interpreters, to develop proficiency.

Crown closure is useful because of its relation to stand volume per acre. It is applied in lieu of basal area or number of trees per acre, as these cannot be accurately determined on available photography. Measurements of crown diameter and estimates of closure should always be made under the stereoscope.

Tree counts.—Complete tallies of individual trees can seldom be made accurately on available USDA photographs. In dense stands, suppressed trees and many intermediates cannot be seen. Clumps of two or three trees often appear as single

TABLE 4.—*Actual crown widths for various photo-crown widths and photo scales*

Photo crown width (thousandths of an inch)	1:10,000 or 833 ft./in.	1:12,000 or 1,000 ft./in.	1:15,840 or 1,320 ft./in.	1:18,000 or 1,500 ft./in.	1:20,000 or 1,667 ft./in.	1:24,000 or 2,000 ft./in.
	Feet	*Feet*	*Feet*	*Feet*	*Feet*	*Feet*
2.5	2	3	3	4	4	5
5.0	4	5	7	8	8	10
7.5	6	8	10	11	13	15
10.0	8	10	13	15	17	20
12.5	10	13	17	19	21	25
15.0	12	15	20	23	25	30
17.5	15	18	23	26	29	35
20.0	17	20	26	30	33	40
22.5	19	23	30	34	38	45
25.0	21	25	33	38	42	50
27.5	23	28	36	41	46	55
30.0	25	30	40	45	50	60
32.5	27	33	43	49	54	----
35.0	29	35	46	53	58	----
37.5	31	38	50	56	63	----
40.0	33	40	53	60	67	----
42.5	35	43	56	----	----	----
45.0	37	45	59	----	----	----
47.5	40	48	63	----	----	----
50.0	42	50	66	----	----	----

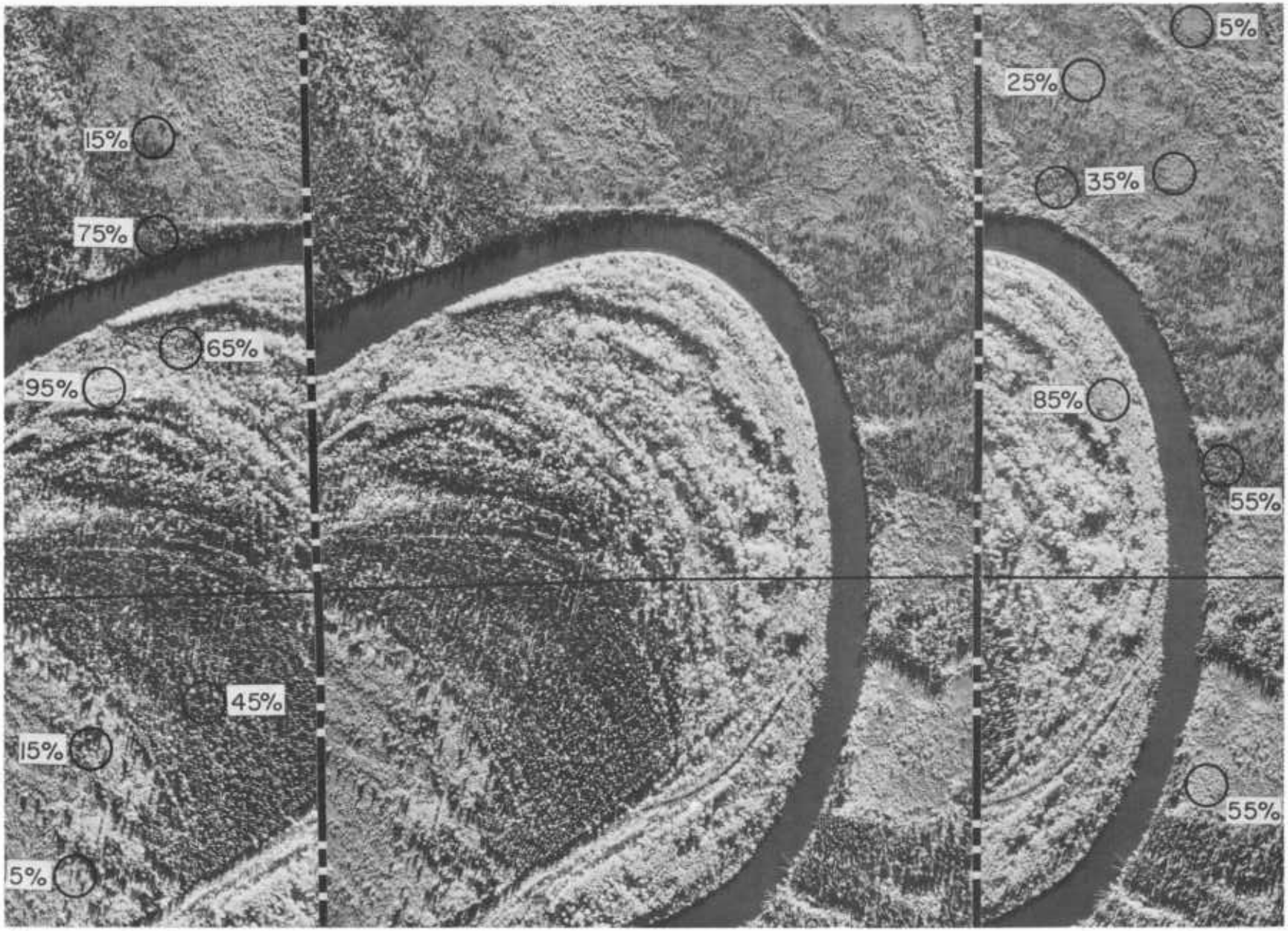


Figure 27.—Infrared stereo-triplet from central Alaska, showing estimates of tree crown closure. Scale is about 420 feet per inch; each circle represents approximately 0.25 acre. The solid black line indicates the path of the aircraft.

crowns, and ragged individual crowns may look like two trees. Only in even-aged, open-grown forests can all trees in a stand be separated. Counting all trees on a plot is tedious, and this measure of density is seldom used. Where large-scale photographs are available (1:1,000 to 1:5,000), individual-tree counts may be much more reliable.

AERIAL CRUISING

Individual Tree Volumes

Ordinary tree volume tables can be easily converted to aerial volume tables when correlations can be established between tree crown diameters and stem diameters (*10*). The photographic determinations of crown diameter and total tree height are merely substituted for the usual field measures of stem diameter (d.b.h.) and merchantable height, respectively (fig. 28). Photographic measurements are usually limited to well-defined open-grown trees, and crown counts are required to obtain total volume for a given stand of timber.

The construction and application of aerial tree volume tables depends on a well-established relationship between photographic measures of crown diameter and ground determinations of tree d.b.h. Such relationships can often be established for individual species or species groups, notably even-aged conifers in the middle diameter classes (*18*). By contrast, stem-crown diameter correlations rarely have been used for estimating volumes of mixed hardwoods.

The aerial tree table (table 5) provides volumes in terms of gross cubic feet. In making an aerial cruise, photographic measurements may include all trees on 0.2- to 1-acre circular plots, or stands may be delineated according to height classes for determination of the average tree per unit area. In the latter instance, a tree count must be made to obtain the total stand volume.

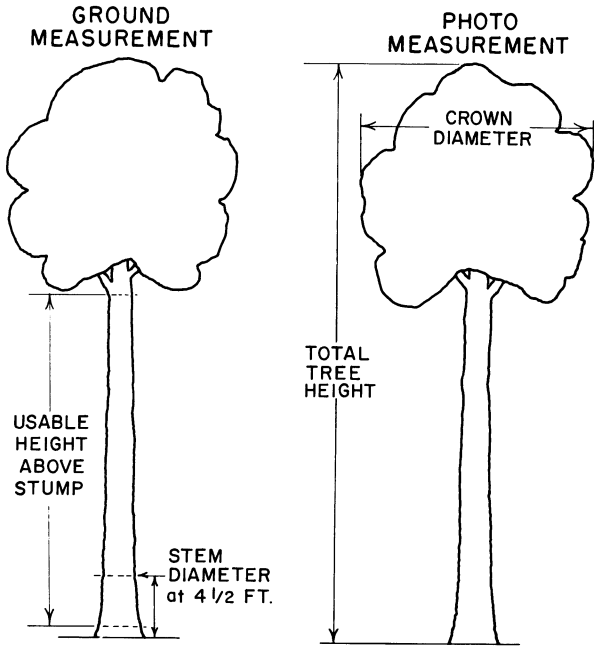


Figure 28.—**Comparison of ground and photographic measurements in the determination of individual tree volumes.**

In general, the individual-tree approach to aerial crusing is of limited value when the interpreter is restricted to use of 1:12,000 to 1:20,000 USDA photographs. At this scale, images are usually too small for accurate assessment of individual trees.

Stand Volume Per Acre

If recent photographs and reliable aerial stand-volume tables can be obtained, average stand volume per acre can be estimated with a minimum of field work. Estimates are made in terms of gross volume, as amount of cull or defect cannot be adequately evaluated. Even-aged stands of simple species structure are best suited for this type of estimating, especially if gross and net volumes are essentially identical. All-aged stands of mixed hardwoods are more difficult to assess, but satisfactory results can be obtained if field checks are made to adjust the photographic estimate of stand volume per acre and to determine allowance for defect. Though volumes from photographs cannot be expressed by species and diameter classes, total gross volumes for areas as small as 40 acres can be estimated within 10 to 15 percent of volumes derived from conventional ground cruises (*13*).

Most aerial stand-volume tables for mixed species are constructed in terms of cubic feet per acre. Tables for species in pure stands, such as Douglas-fir, may be expressed either in board feet or cubic feet per acre. Three photographic measurements of the dominant stand are generally required for entering an aerial stand volume table: average total height, crown diameter, and crown closure percent.

Aerial volume tables have been constructed for many of the important timber associations in the United States. Included here are tables for Douglas-fir (table 6), Rocky Mountain conifers (table 7), and Kentucky hardwoods (table 8). Composite tables, applicable in mixed stands, are presented for northeast Mississippi (table 9) and for northern Minnesota (table 10). Crown diameter was eliminated as a variable in tables 6 and 10.

TABLE 5.—*Volumes of individual second-growth southern pines* [1]

Crown diameter class (feet)	Total tree height, in feet						
	50	60	70	80	90	100	110
	Cu. ft.	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*
10	9. 5	11. 5	12. 5	15. 0	17. 5	19. 5	-----
12	12. 5	14. 5	16. 5	18. 0	20. 5	22. 5	-----
14	15. 0	17. 0	19. 0	23. 5	25. 0	27. 5	30. 5
16	17. 5	20. 5	24. 0	27. 5	30. 5	33. 0	36. 0
18	------	23. 5	27. 0	30. 5	34. 5	38. 0	42. 5
20	------	28. 0	33. 5	36. 0	40. 0	45. 5	49. 0
22	------	32. 5	37. 0	42. 5	46. 5	52. 0	57. 5
24	------	37. 0	42. 5	48. 5	54. 5	60. 0	66. 0
26	------	42. 5	47. 5	54. 0	61. 0	67. 5	75. 5
28	------	------	53. 0	60. 5	70. 5	76. 0	83. 0
30	------	------	60. 5	68. 0	78. 0	85. 5	94. 5

[1] Based on 342 trees in Arkansas, Lousiana, and Mississippi. Gross volumes are inside bark and include the merchantable stem to a variable top averaging 6 inches i.b. Reprinted from (*4*).

One of the several procedures for making aerial volume estimates is as follows:

1. Outline tract boundaries on the photographs, utilizing the effective area of every other print in each flight line. This assures stereoscopic coverage of the area on a minimum number of photographs and avoids duplication of measurements.
2. Delineate all forest types. Except where type lines define stands of relatively uniform stocking and total height, they should be further broken down into homogeneous units so that measures of height, density, and crown diameter will apply to the entire unit. Generally it is unnecessary to recognize stands smaller than 5 to 10 acres.
3. Determine the acreage of each condition class with dot grids. This determination can often be made on contact prints.
4. By stereoscopic examination, measure the variables for entering the aerial stand volume table. From the table, obtain the average volume per acre for each condition class.
5. Multiply gross volumes per acre from the table by condition class areas to determine gross volume.
6. Add class volumes for the total gross volume on the tract.

A practical application is illustrated by the stereogram in figure 29 and the corresponding cordwood volume summary. In this particular inventory, hardwood components in each stand were ignored, and estimates were derived only for pine timber. The aerial cruise, fortified by fre-

TABLE 6.—*Aerial stand volume per acre values* [1] *for even-aged Douglas-fir in the Pacific Northwest*

Stand height [2] (feet)	Crown closure percent [3]								
	15	25	35	45	55	65	75	85	95
	Cu. ft.	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*
40	500	800	1, 100	1, 300	1, 400	1, 500	1, 500	1, 400	1, 300
50	700	1, 100	1, 500	1, 800	2, 000	2, 100	2, 200	2, 100	2, 000
60	900	1, 500	2, 000	2, 400	2, 700	2, 900	3, 000	2, 900	2, 800
70	1, 200	1, 900	2, 500	3, 100	3, 400	3, 700	3, 900	3, 900	3, 800
80	1, 400	2, 400	3, 100	3, 800	4, 300	4, 600	4, 800	4, 900	4, 900
90	1, 700	2, 800	3, 800	4, 500	5, 200	5, 600	5, 900	6, 100	6, 100
100	2, 100	3, 300	4, 500	5, 400	6, 100	6, 700	7, 200	7, 400	7, 500
110	2, 400	3, 900	5, 200	6, 300	7, 200	7, 900	8, 500	8, 800	9, 000
120	2, 800	4, 500	6, 000	7, 300	8, 300	9, 200	9, 900	10, 300	10, 600
130	3, 100	5, 100	6, 800	8, 300	9, 500	10, 600	11, 400	12, 000	12, 400
140	3, 500	5, 700	7, 700	9, 400	10, 800	12, 100	13, 000	13, 800	14, 300
150	4, 000	6, 400	8, 600	10, 500	12, 200	13, 600	14, 800	15, 700	16, 300
160	4, 400	7, 100	9, 600	11, 800	13, 600	15, 300	16, 600	17, 700	18, 500
170	4, 900	7, 900	10, 600	13, 000	15, 200	17, 000	18, 500	19, 800	20, 800
180	5, 400	8, 700	11, 700	14, 400	16, 800	18, 800	20, 600	22, 000	23, 200
190	5, 900	9, 500	12, 800	15, 800	18, 400	20, 800	22, 700	24, 400	25, 700
200	6, 400	10, 400	14, 000	17, 300	20, 200	22, 800	25, 000	26, 900	28, 400
210	7, 000	11, 300	15, 200	18, 800	22, 000	24, 900	27, 400	29, 500	31, 300
220	7, 500	12, 200	16, 500	20, 400	23, 900	27, 100	29, 800	32, 200	34, 200
230	8, 100	13, 200	17, 800	22, 000	25, 900	29, 300	32, 400	35, 100	37, 300
240	8, 700	14, 200	19, 200	23, 800	28, 000	31, 700	35, 100	38, 000	40, 600
250	9, 400	15, 200	20, 600	25, 600	30, 100	34, 200	37, 900	41, 100	43, 900
260	10, 000	16, 300	22, 100	27, 400	32, 300	36, 700	40, 800	44, 300	47, 400

[1] Gross volume, in trees 5.0 inches and larger, from stump to top limit of 4.0 inches diameter inside bark. Reprinted from (*15*).

[2] Average height of dominants and codominants as measured in the field.

[3] Average estimates of several experienced interpreters includes all trees in the major canopy (occasionally excludes small trees definitely below the general canopy).

TABLE 7.—*Aerial volume per acre for Rocky Mountain conifers* [1]

Average stand height (feet)	Crown closure percent									
	5	15	25	35	45	55	65	75	85	95
	Cu. ft.	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*
4- TO 7-FOOT CROWN DIAMETER										
30	-------	100	300	450	550	650	750	850	1, 000	1, 150
35	-------	200	400	550	650	750	850	1, 000	1, 200	1, 400
40	-------	300	500	650	750	850	1, 000	1, 150	1, 400	1, 650
45	50	400	600	750	850	950	1, 100	1, 300	1, 550	1, 800
50	100	500	700	850	1, 000	1, 150	1, 350	1, 600	1, 850	2, 100
55	200	600	850	1, 050	1, 200	1, 400	1, 600	1, 850	2, 100	2, 350
60	350	800	1, 100	1, 350	1, 600	1, 800	2, 000	2, 250	2, 500	2, 750
65	500	1, 050	1, 400	1, 700	1, 950	2, 150	2, 350	2, 550	2, 800	3, 050
8- TO 12-FOOT CROWN DIAMETER										
30	-------	150	350	500	600	700	800	950	1, 200	1, 350
35	-------	250	450	600	750	850	950	1, 100	1, 300	1, 500
40	-------	350	550	700	850	950	1, 050	1, 250	1, 500	1, 750
45	-------	400	650	800	950	1, 100	1, 250	1, 450	1, 700	1, 950
50	100	500	700	950	1, 100	1, 250	1, 450	1, 700	1, 950	2, 150
55	300	700	900	1, 100	1, 300	1, 500	1, 750	2, 000	2, 225	2, 500
60	450	900	1, 200	1, 500	1, 750	1, 950	2, 150	2, 350	2, 550	2, 650
65	700	1, 200	1, 600	1, 900	2, 100	2, 300	2, 500	2, 700	2, 900	3, 100
70	900	1, 600	2, 000	2, 300	2, 500	2, 700	2, 850	3, 000	3, 200	3, 300
75	1, 200	2, 000	2, 400	2, 700	2, 850	3, 000	3, 200	3, 400	3, 600	3, 800
80	1, 700	2, 500	2, 800	3, 100	3, 300	3, 450	3, 600	3, 800	4, 000	4, 200
85	2, 200	3, 000	3, 300	3, 550	3, 750	3, 950	4, 150	4, 350	4, 550	4, 750
13- TO 17-FOOT CROWN DIAMETER										
30	-------	200	400	550	700	800	900	1, 050	1, 200	1, 350
35	-------	300	500	700	800	900	1, 050	1, 200	1, 500	1, 700
40	-------	400	600	800	900	1, 000	1, 250	1, 450	1, 700	1, 950
45	100	500	700	850	1, 000	1, 150	1, 350	1, 600	1, 850	2, 100
50	200	600	850	1, 000	1, 150	1, 350	1, 600	1, 850	2, 100	2, 350
55	300	750	1, 000	1, 250	1, 500	1, 700	1, 900	2, 150	2, 350	2, 550
60	500	1, 000	1, 300	1, 600	1, 850	2, 050	2, 250	2, 450	2, 650	2, 850
65	750	1, 300	1, 700	2, 000	2, 200	2, 400	2, 600	2, 800	3, 000	3, 200
70	1, 000	1, 700	2, 100	2, 400	2, 600	2, 750	2, 900	3, 100	3, 300	3, 500
75	1, 300	2, 100	2, 500	2, 750	2, 950	3, 150	3, 300	3, 500	3, 700	3, 900
80	1, 800	2, 600	2, 900	3, 200	3, 400	3, 600	3, 750	3, 900	4, 100	4, 300
85	2, 300	3, 100	3, 450	3, 700	3, 900	4, 050	4, 200	4, 400	4, 600	4, 800
90	2, 800	3, 600	3, 900	4, 150	4, 350	4, 500	4, 650	4, 850	5, 050	5, 250
95	3, 300	4, 100	4, 400	4, 600	4, 800	5, 000	5, 200	5, 400	5, 600	5, 800
100	3, 700	4, 500	4, 850	5, 150	5, 350	5, 550	5, 750	5, 950	6, 150	6, 350
18- TO 22-FOOT CROWN DIAMETER										
30	-------	300	500	700	800	900	1, 050	1, 200	1, 400	1, 600
35	-------	400	650	800	900	1, 050	1, 200	1, 400	1, 600	1, 800
40	100	500	750	900	1, 050	1, 200	1, 400	1, 600	1, 800	2, 000
45	200	600	850	1, 050	1, 200	1, 400	1, 600	1, 800	2, 000	2, 200
50	350	750	1, 000	1, 200	1, 400	1, 600	1, 800	2, 050	2, 250	2, 450
55	450	850	1, 150	1, 400	1, 650	1, 900	2, 100	2, 300	2, 500	2, 700
60	650	1, 150	1, 500	1, 800	2, 050	2, 250	2, 450	2, 650	2, 850	3, 050
65	850	1, 500	1, 900	2, 200	2, 400	2, 600	2, 750	2, 900	3, 100	3, 300
70	1, 100	1, 900	2, 300	2, 550	2, 750	2, 900	3, 100	3, 300	3, 500	3, 700
75	1, 600	2, 400	2, 700	2, 950	3, 100	3, 250	3, 450	3, 650	3, 850	4, 050
80	1, 950	2, 750	3, 050	3, 300	3, 500	3, 700	3, 900	4, 100	4, 300	4, 500
85	2, 500	3, 300	3, 600	3, 850	4, 050	4, 250	4, 400	4, 550	4, 750	4, 950
90	2, 900	3, 700	4, 050	4, 300	4, 500	4, 700	4, 850	5, 050	5, 300	5, 500
95	3, 400	4, 200	4, 500	4, 800	5, 000	5, 200	5, 400	5, 600	5, 800	6, 000
100	3, 900	4, 700	5, 000	5, 300	5, 500	5, 700	5, 900	6, 100	6, 300	6, 500
105	4, 600	5, 400	5, 800	6, 000	6, 200	6, 400	6, 550	6, 700	6, 850	7, 050
110	5, 200	6, 000	6, 400	6, 600	6, 800	7, 000	7, 200	7, 400	7, 600	7, 800

TABLE 7.—*Aerial volume per acre for Rocky Mountain conifers* [1]—Continued

23-FOOT AND LARGER CROWN DIAMETER

Average stand height (feet)	Crown closure percent									
	5	15	25	35	45	55	65	75	85	95
	Cu. ft.	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*
30	100	500	750	900	1, 050	1, 250	1, 450	1, 650	1, 900	2, 150
35	200	650	850	1, 050	1, 250	1, 450	1, 650	1, 850	2, 100	2, 350
40	300	750	1, 000	1, 200	1, 400	1, 600	1, 800	2, 050	2, 300	2, 550
45	400	850	1, 100	1, 350	1, 600	1, 800	2, 000	2, 250	2, 500	2, 750
50	550	1, 000	1, 300	1, 600	1, 850	2, 050	2, 250	2, 450	2, 650	2, 850
55	700	1, 200	1, 600	1, 900	2, 100	2, 300	2, 500	2, 700	2, 900	3, 100
60	850	1, 550	1, 950	2, 250	2, 450	2, 650	2, 850	3, 050	3, 250	3, 450
65	1, 200	1, 900	2, 300	2, 550	2, 750	2, 900	3, 100	3, 300	3, 500	3, 700
70	1, 550	2, 250	2, 650	2, 900	3, 100	3, 300	3, 450	3, 650	3, 850	4, 050
75	2, 050	2, 750	3, 050	3, 300	3, 500	3, 650	3, 800	4, 000	4, 200	4, 400
80	2, 450	3, 150	3, 450	3, 700	3, 900	4, 050	4, 200	4, 400	4, 600	4, 800
85	2, 900	3, 600	3, 950	4, 200	4, 400	4, 550	4, 700	4, 900	5, 100	5, 300
90	3, 400	4, 100	4, 400	4, 650	4, 850	5, 050	5, 250	5, 450	5, 650	5, 850
95	3, 850	4, 550	4, 850	5, 150	5, 350	5, 550	5, 750	5, 950	6, 150	6, 350
100	4, 400	5, 100	5, 400	5, 700	5, 900	6, 100	6, 250	6, 400	6, 600	6, 800
105	5, 100	5, 800	6, 100	6, 400	6, 550	6, 700	6, 850	7, 000	7, 150	7, 300
110	6, 600	6, 400	6, 700	6, 900	7, 050	7, 200	7, 350	7, 500	7, 700	7, 850
115	6, 150	6, 900	7, 200	7, 400	7, 600	7, 750	7, 900	8, 050	8, 200	8, 350

[1] Based on 168 field plots taken in southeastern Idaho, southwestern Wyoming, and northeastern Utah. Aggregate deviation: Table 1.5 percent low. Standard error of estimate: ± 48 percent of average plot volume. Reprinted from (*11*).

TABLE 8.—*Aerial volume per acre for Kentucky hardwoods* [1]

10- TO 14-FOOT AVERAGE CROWN DIAMETER

Average stand height (feet)	Crown closure percent								
	15	25	35	45	55	65	75	85	95
	Cu. ft.	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*
30	300	375	450	475	500	570	635	700	770
40	350	425	500	550	600	650	700	750	800
50	400	475	550	625	700	770	835	900	970
60	550	675	800	875	950	1, 035	1, 115	1, 200	1, 285
70	900	1, 075	1, 250	1, 325	1, 400	1, 470	1, 535	1, 600	1, 670

15- TO 19-FOOT AVERAGE CROWN DIAMETER

30	350	400	450	500	550	620	685	750	820
40	400	450	500	575	650	720	785	850	920
50	450	525	600	675	750	835	920	1, 000	1, 085
60	600	725	850	950	1, 050	1, 100	1, 150	1, 200	1, 250
70	1, 000	1, 150	1, 300	1, 400	1, 500	1, 550	1, 600	1, 650	1, 700
80	1, 500	1, 625	1, 750	1, 825	1, 900	1, 970	2, 035	2, 100	2, 170

20- TO 29-FOOT AVERAGE CROWN DIAMETER

40	500	625	750	850	950	1, 035	1, 115	1, 200	1, 285
50	600	750	900	1, 000	1, 100	1, 185	1, 270	1, 350	1, 435
60	900	1, 050	1, 200	1, 275	1, 350	1, 420	1, 485	1, 550	1, 620
70	1, 350	1, 475	1, 600	1, 675	1, 750	1, 820	1, 885	1, 950	2, 020
80	1, 750	1, 900	2, 050	2, 125	2, 200	2, 270	2, 335	2, 400	2, 470
90	2, 220	2, 360	2, 500	2, 575	2, 650	2, 720	2, 785	2, 850	2, 920
100	2, 700	2, 850	3, 000	3, 075	3, 150	3, 200	3, 250	3, 300	3, 350

TABLE 8.—*Aerial volume per acre for Kentucky hardwoods* [1]—Continued

30-FOOT AND LARGER AVERAGE CROWN DIAMETER

Average stand height (feet)	Crown closure percent								
	15	25	35	45	55	65	75	85	95
	Cu. ft.	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*
40	850	1, 025	1, 200	1, 275	1, 350	1, 420	1, 485	1, 550	1, 620
50	1, 050	1, 200	1, 350	1, 425	1, 500	1, 570	1, 635	1, 700	1, 770
60	1, 300	1, 450	1, 600	1, 650	1, 700	1, 785	1, 870	1, 950	2, 035
70	1, 700	1, 850	2, 000	2, 075	2, 150	2, 220	2, 285	2, 350	2, 420
80	2, 150	2, 275	2, 400	2, 500	2, 600	2, 670	2, 735	2, 800	2, 870
90	2, 600	2, 725	2, 850	2, 925	3, 000	3, 070	3, 135	3, 200	3, 270
100	3, 050	3, 175	3, 300	3, 375	3, 450	3, 500	3, 550	3, 600	3, 650
110	3, 600	3, 700	3, 800	3, 875	3, 950	4, 020	4, 085	4, 150	4, 220

[1] Gross volumes include the merchantable stems of all trees 5 inches d.b.h. and larger to a 4-inch top diameter i.b. Expanded from (*14*) by linear interpolation.

TABLE 9.—*Composite aerial volume per acre for northeast Mississippi* [1]

10-FOOT AVERAGE CROWN DIAMETER

Average stand height (feet)	Crown closure percent								
	15	25	35	45	55	65	75	85	95
	Cu. ft.	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*
30	190	310	430	560	690	810	940	1, 060	1, 180
40	230	380	530	690	840	990	1, 140	1, 300	1, 450
50	260	440	620	800	980	1, 150	1, 330	1, 510	1, 680
60	300	500	690	890	1, 090	1, 290	1, 490	1, 680	1, 880
70	340	570	800	1, 030	1, 260	1, 490	1, 720	1, 950	2, 180
80	380	640	890	1, 140	1, 400	1, 650	1, 910	2, 160	2, 420
15-FOOT AVERAGE CROWN DIAMETER									
30	210	350	500	640	780	930	1, 070	1, 220	1, 360
40	260	430	610	780	950	1, 130	1, 300	1, 480	1, 650
50	310	510	730	930	1, 140	1, 350	1, 550	1, 770	1, 970
60	360	590	830	1, 070	1, 300	1, 550	1, 780	2, 030	2, 260
70	400	660	940	1, 200	1, 460	1, 740	2, 000	2, 280	2, 540
80	440	740	1, 040	1, 330	1, 620	1, 930	2, 220	2, 530	2, 820
90	480	800	1, 140	1, 450	1, 770	2, 100	2, 420	2, 760	3, 070
20-FOOT AVERAGE CROWN DIAMETER									
40	270	450	630	820	1, 000	1, 190	1, 370	1, 550	1, 720
50	320	540	750	970	1, 190	1, 410	1, 630	1, 840	2, 040
60	360	610	860	1, 110	1, 360	1, 600	1, 850	2, 100	2, 330
70	410	680	960	1, 240	1, 520	1, 800	2, 080	2, 360	2, 610
80	450	760	1, 070	1, 380	1, 690	2, 000	2, 310	2, 620	2, 900
90	500	840	1, 190	1, 530	1, 870	2, 220	2, 560	2, 900	3, 220
100	540	920	1, 290	1, 670	2, 040	2, 410	2, 790	3, 160	3, 500
25-FOOT AVERAGE CROWN DIAMETER									
50	320	550	770	1, 000	1, 220	1, 450	1, 670	1, 900	2, 120
60	370	620	880	1, 130	1, 390	1, 650	1, 900	2, 160	2, 410
70	410	700	980	1, 270	1, 550	1, 840	2, 130	2, 410	2, 700
80	460	780	1, 100	1, 420	1, 740	2, 060	2, 380	2, 700	3, 020
90	510	860	1, 220	1, 570	1, 930	2, 280	2, 640	2, 990	3, 350
100	550	940	1, 320	1, 710	2, 090	2, 480	2, 860	3, 250	3, 630

[1] Gross volumes are inside bark and include the merchantable stem to a variable top not smaller than 3 inches i.b. Reprinted from (*3*).

TABLE 10.—*Composite aerial volume per acre* [1] *for northern Minnesota* [2]

Average total height (feet)	Crown closure percent									
	5	15	25	35	45	55	65	75	85	95
	Cu. ft.	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu. ft.*	*Cu.ft.*	*Cu. ft.*
30	40	120	200	280	360	440	520	600	680	760
35	80	190	300	410	520	630	740	850	960	1, 070
40	180	310	440	570	700	830	960	1, 090	1, 220	1, 350
45	460	590	720	850	980	1, 110	1, 240	1, 370	1, 500	1, 630
50	740	870	1, 000	1, 130	1, 260	1, 390	1, 520	1, 650	1, 780	1, 910
55	1, 020	1, 150	1, 280	1, 410	1, 540	1, 670	1, 800	1, 930	2, 060	2, 190
60	1, 300	1, 430	1, 560	1, 690	1, 820	1, 950	2, 080	2, 210	2, 340	2, 470
65	1, 580	1, 710	1, 840	1, 970	2, 100	2, 230	2, 360	2, 490	2, 620	2, 750
70	1, 860	1, 990	2, 120	2, 250	2, 380	2, 510	2, 640	2, 770	2, 900	3, 030
75	2, 140	2, 270	2, 400	2, 530	2, 660	2, 790	2, 920	3, 050	3, 180	3, 310
80	2, 420	2, 550	2, 680	2, 810	2, 940	3, 070	3, 200	3, 330	3, 460	3, 590
85	2, 700	2, 830	2, 960	3, 090	3, 220	3, 350	3, 480	3, 610	3, 740	3, 870
90	2, 980	3, 110	3, 240	3, 370	3, 500	3, 630	3, 760	3, 890	4, 020	4, 150
95	3, 260	3, 390	3, 520	3, 650	3, 780	3, 910	4, 040	4, 170	4, 300	4, 430
100	3, 540	3, 670	3, 800	3, 930	4, 060	4, 190	4, 320	4, 450	4, 580	4, 710

[1] Gross volumes are inside bark and include all trees 5.0 inches d.b.h. and larger from stump to a variable top diameter not less than 4.0 inches i.b. Volumes may be converted to rough cords per acre by dividing by 80.

[2] Based on 50 1-acre plots in Carlton County, Minn. Heavy lines indicate limits of basic data. Reprinted from (*5*).

quent field checks, was within 10 percent of a ground inventory made by an independent agency.

Adjusting volumes by field checks.—When aerial volume tables are not sufficiently reliable for acceptance of pure photographic estimates and allowance must be made for defective trees, some of the plots interpreted should be mechanically selected for field measurement. For example, if 350 plots were interpreted and every 10th plot selected, 35 plots would be visited in the field. If the field volumes averaged 600 cubic feet per acre as opposed to 800 cubic feet per acre for the photo plots, the adjustment ratio would be $600 \div 800$ or 0.75. If the 35 field plots are representative of the total, the ratio can be applied to the average photo volume per acre to determine the adjusted volume. Ratios should be computed by forest types, because hardwoods are likely to require larger adjustments than conifers.

The accuracy of aerial cruises depends not only upon the volume tables but also on the availability of recent photographs and the interpreter's ability to measure correctly. This last item may be the greatest single source of error. Each photo variable should be measured twice for an average, or two interpreters should assess each plot.

Photo estimates of pine cordwood volumes for a tract in the Georgia Piedmont [1]

County: Oconee
Photo No.: BQ–3BB–85, 86
Owner: J. Reynolds
Photo date: 11–1–60
Pine area: 177 acres
Scale: 1,667 ft./inch

Pine stand [2]	Stand area	Total height	Crown diameter	Crown closure	Pine volumes per acre		Stand volume
	Acres	*Feet*	*Feet*	*Percent*	*Cubic feet*	*Cords*	*Cords*
1	18	40	10	25	380	4. 75	85. 5
2	29	30	10	5	60	. 75	21. 8
3	11	30	10	5	60	. 75	8. 3
4	18	40	15	35	610	7. 62	137. 2
5	5	30	10	15	190	2. 37	11. 8
6	11	40	15	35	610	7. 62	83. 8
7	9	30	10	65	810	10. 12	91. 1
8	17	40	15	15	260	3. 25	55. 2
9	20	50	15	15	310	3. 87	77. 4
10	27	40	15	25	430	5. 37	145. 0
11	12	30	10	15	190	2. 37	28. 4
Total pine volume (cords)							745. 5

[1] Cubic volumes derived from table 9 and divided by 80 for conversion to cords.

[2] Stands are numbered as in figure 29.

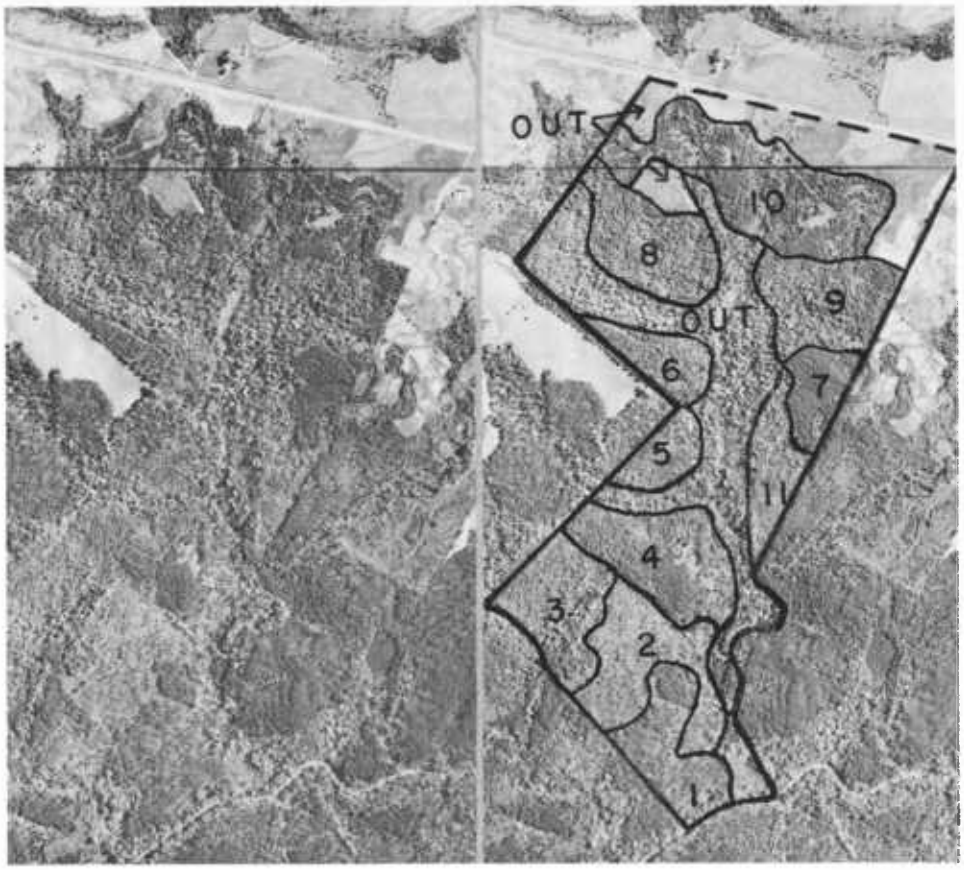


Figure 29.—**USDA panchromatic stereogram of a forest area in the Georgia Piedmont. Area and pine volume estimates were made for each of the stands numbered. Scale is about 1,667 feet per inch.**

PHOTO STRATIFICATION FOR GROUND CRUISING

A photo-controlled ground cruise combines the features of both aerial and ground estimating, offering a means of obtaining timber volumes with maximum efficiency. Photographs are used for area determination, for allocation of field samples by forest type and stand-size classes, and for designing the pattern of field work. Tree volumes, growth, cull percents, form class, and other data are obtained on the ground by conventional methods. A photo-controlled cruise may increase the efficiency, while reducing the total cost, of an inventory on tracts as small as 100 acres.

The approach to an inventory of this kind depends largely on the types of strata recognized and the method of allocating field samples. Cost and the statistical accuracy required determines the total number of field samples to be measured. Once this number has been determined, there are several ways in which the samples may be distributed among various photo classifications:

1. By area of each class. Though sometimes used, this method is often unsatisfactory because stands of low value may occupy the greatest acreage while high-value stands may be insufficiently sampled. The opposite extreme may result if value alone (volume-per-acre classes) is used.
2. By applying different cruising intensities to each class. A 20-percent cruise might be used for high-value stands, 10 percent for medium value, and 5 percent or less for low-value areas. This arbitrary method is better than using acreage alone, but it may not be the most economical and efficient.
3. By statistical methods. A preliminary cruise or a good estimate of the variability within each class must be made before the required number of plots per class can be computed. This approach is best for large tracts; for small ones it may be costly or unwieldy.

4. By a combination of area and value (volume). This is the preferred approach for small areas. A suggested procedure adopted from Johnson (*6*) and Spurr (*18*) follows.

Plot allocation by area and volume.—Assume that the tract is 1,600 acres and that 400 field plots are to be distributed among three forest types (pine, pine-hardwood, and hardwood) and three volume classes within each type (5, 8, and 12 cords per acre).

1. Stratify each forest type into volume-per-acre classes on the basis of personal experience or with aerial stand-volume tables. Precision is not required, as the volume classes are used only as a guide. Tabulate by type and acreage:

Cords per acre	*Pine (acres)*	*Pine-hardwood (acres)*	*Hardwood (acres)*
5	120	200	100
8	100	500	350
12	80	100	50
Total	300	800	500

2. Multiply the number of acres in each class by the cord volume per acre. The product is the number of cords per class:

Pine	*Pine-hardwood*	*Hardwood*
5×120= 600	5×200=1, 000	5×100= 500
8×100= 800	8×500=4, 000	8×350=2, 800
12× 80= 960	12×100=1, 200	12× 50= 600
2, 360	6, 200	3, 900

3. Add the cordage in each class to get the total for the entire area: 2,360+6,200+3,900=12,460 cords. Divide by the number of plots to get the number of cords to be represented by each plot:

$$\frac{12,460}{400}=31.15 \text{ cords per plot}$$

4. Divide the volume for each class (item 2) by the cord volume per plot to get the number of plots assigned to each class. Round to the nearest whole number. Add the plots for each class to make sure the total (400) is correct.

Pine	*Pine-hardwood*	*Hardwood*
$\frac{600}{31.15}=19.26(19)$	$\frac{1,000}{31.15}=32.10\ (32)$	$\frac{500}{31.15}=16.05(16)$
$\frac{800}{31.15}=25.68(26)$	$\frac{4,000}{31.15}=128.41(128)$	$\frac{2,800}{31.15}=89.88(90)$
$\frac{960}{31.15}=30.82(31)$	$\frac{1,200}{31.15}=38.52\ (39)$	$\frac{600}{31.15}=19.26(19)$
(76)	(199)	(125)

Total: 400 plots

Arrangement of ground samples.—If type boundaries have been accurately delineated and stands are homogeneous within the recognized classes, field plots can sometimes be taken along routes of easy travel without introducing much bias. Usually, though, it is necessary to lay out line-plot or strip cruises at right angles to topography. The cruise lines should be drawn to scale on a type map in such a way that the required number of samples within each class can be obtained. The number of plots or chains of strip that a crew can complete per day is the basis for calculating the lengths of the lines. To minimize travel, lines may be triangular or U-shaped, beginning and ending near the same starting point on a road or trail. Compass bearings and distances can be determined on the map to avoid location bias in the field. The cruise lines can then be placed on the photographs for use in the field, if desired.

Field measurements are taken by conventional procedures. Cumulative tally sheets or point-sampling may be employed to speed the tree tally. After the cordage per acre for each volume class has been determined by field sampling, the values are multiplied by the appropriate stand acreages. The result is the total volume on the tract, by forest types:

Assumed volume class (cords per acre)	*Field plots (number)*	*Field volumes per acre (cords)*	*Type area (acres)*	*Volume per class (cords)*
PINE TYPE				
5	19	3. 9	120	468. 0
8	26	8. 2	100	820. 0
12	31	11. 3	80	904. 0
Total	76		300	2, 192. 0
PINE-HARDWOOD TYPE				
5	32	5. 8	200	1, 160. 0
8	128	7. 7	500	3, 850. 0
12	39	14. 1	100	1, 410. 0
Total	199		800	6, 420. 0
HARDWOOD TYPE				
5	16	4. 7	100	470. 0
8	90	8. 6	350	3, 010. 0
12	19	13. 5	50	675. 0
Total	125		500	4, 155. 0

LITERATURE CITED

(1) American Society of Photogrammetry.
1952. Manual of photogrammetry. Ed. 2, 876 pp., illus. Menasha, Wis.: Banta.

(2) ————————
1960. Manual of photographic interpretation. 868 pp., illus. Menasha, Wis.: Banta.

(3) Avery, T. Eugene.
1958. Composite aerial volume table for southern pines and hardwoods. Jour. Forestry 56: 741–745, illus.

(4) ————————
1962. Interpretation of aerial photographs. 192 pp., illus. Minneapolis, Minn.: Burgess.

(5) ——— ——— and Meyer, Merle P.
1959. Volume tables for aerial timber estimating in northern Minnesota. U.S. Forest Serv. Lake States Forest Expt. Sta., Sta. Paper 78, 21 pp., illus.

(6) Johnson, Evert W.
1952. Timber volume determinations using aerial photographs. Ala. Polytech. Inst., 43 pp., illus.

(7) ————————
1954. Ground control for planimetric base maps. Jour. Forestry 52: 89–95, illus.

(8) ————————
1954. "Shadow-height" computations made easier. Jour. Forestry 52: 438–442, illus.

(9) Kramer, P. R., and Sturgeon, E. E.
1942. Transect method of estimating forest area from aerial photo index sheets. Jour. Forestry 40: 693–696, illus.

(10) Minor, C. O.
1951. Stem-crown diameter relations in southern pine. Jour. Forestry 49: 490–493, illus.

(11) Moessner, Karl E.
1957. Preliminary aerial volume tables for conifer stands in the Rocky Mountains. U.S. Forest Serv. Intermountain Forest and Range Expt. Sta. Res. Paper 41, 17 pp., illus.

(12) ————————
1957. How important is relief in area estimates from dot sampling on aerial photos? U.S. Forest Serv. Intermountain Forest and Range Expt. Sta. Res. Paper 42, 16 pp., illus.

(13) ———————— and Jensen, C. E.
1951. Timber cruising on aerial photos. U.S. Forest Serv. Central States Forest Expt. Sta. Tech. Paper 126, 27 pp., illus.

(14) ————————, Brunson, D. F., and Jensen, C. E.
1951. Aerial volume tables for hardwood stands in the Central States. U.S. Forest Serv. Central States Forest Expt. Sta. Tech. Paper 122, 15 pp., illus.

(15) Pope, Robert B.
1962. Constructing aerial photo volume tables. U.S. Forest Serv. Pacific Northwest Forest and Range Expt. Sta. Res. Paper 49, 25 pp., illus.

(16) Sayn-Wittgenstein, Leo.
1961. Recognition of tree species on air photographs by crown characteristics. Photogrammetric Engin. 27: 792–809, illus.

(17) Society of American Foresters.
1955. Forestry handbook. 23 sects., illus. N.Y.: Ronald Press.

(18) Spurr, S. H.
1948. Aerial photographs in forestry. 340 pp., illus. N.Y.: Ronald Press.

(19) Wilson, R. C.
1949. The relief displacement factor in forest area estimates by dot templets on aerial photographs. Photogrammetric Engin. 15: 225–236, illus.

(20) Zsilinszky, Victor G.
1963. Photographic interpretation of tree species in Ontario. Ontario Dept. Lands and Forests, 80 pp., illus.

U.S. GOVERNMENT PRINTING OFFICE: 1969 O—367–547

Figure 1.—An aerial stereo-pair, from 9- by 9-inch contact prints. Note that the print showing the time of day is the last one in the flight line. The principal point (PP) of one photo coincides with the conjugate principal point (CPP) on the overlapping print. The flight path of the aircraft is indicated by the lines connecting the PP and CPP.

573

LIBRARY

LIBRARY
U.S. BUREAU OF MINES
Western Field Operation Center
East 360 3rd Ave.
Spokane, Washington 99202

Aerial Photographs in Geologic Interpretation and Mapping

GEOLOGICAL SURVEY PROFESSIONAL PAPER 373

BUREAU OF MINES
LIBRARY
SPOKANE, WASH.
JUN - 9 1961

PLEASE RETURN
TO LIBRARY

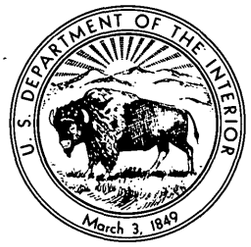
6/61
Spokane

Aerial Photographs in Geologic Interpretation and Mapping

By RICHARD G. RAY

GEOLOGICAL SURVEY PROFESSIONAL PAPER 373

The use of aerial photographs to obtain qualitative and quantitative geologic information, and instrument procedures employed in compiling geologic data from aerial photographs



BUREAU OF MINES
LIBRARY
SPOKANE, WASH.
JUN - 9 1961
PLEASE RETURN
TO LIBRARY

UNITED STATES GOVERNMENT PRINTING OFFICE, WASHINGTON : 1960

UNITED STATES DEPARTMENT OF THE INTERIOR

FRED A. SEATON, *Secretary*

GEOLOGICAL SURVEY

Thomas B. Nolan, *Director*

The U.S. Geological Survey Library has cataloged this publication as follows:

Ray, Richard Godfrey, 1920–

Aerial photographs in geologic interpretation and mapping. Washington, U.S. Govt. Print. Off., 1960.

vi, 230 p. illus., maps, diagrs. 30 cm. (U.S. Geological Survey. Professional paper (373)

Bibliography: p. 224–227.

1. Aerial photography. 2. Photographic surveying. 3. Geology-Maps. (Series)

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington 25, D.C. - Price $2. (paper cover)

CONTENTS

	Page
Abstract	1
Introduction	1
The aerial photograph	2
Factors that affect the photographic image	2
Focal length and flying height	2
Film and filter combinations	4
Lens angle	4
Viewing of photographs	4
Interpretation	5
Interpretation factors	6
Recognition elements	6
Photographic tone	6
Color	8
Texture	9
Pattern	9
Relation to associated features	11
Shape	12
Size	13
Combinations of recognition elements	13
Vertical exaggeration	13
Scale of photographs	14
Photogeology in geologic mapping	14
Kinds and amounts of information	15
Lithologic character of rocks	16
Sedimentary rocks	16
Igneous rocks	17
Metamorphic rocks	18
Structure	19
Flat-lying beds	19
Dipping beds	19
Folds	19
Faults	21
Joints	23
Cleavage and foliation	24
Unconformities	24
Interpretation of aerial photographs in petroleum geology	24
Folds	26
Bedding	26
Drainage	26
Topography	27
Soils	29
Faults	29
Facies	30
Regional studies	30
Interpretation of aerial photographs in search for ore deposits	30
Structural guides	30
Lithologic guides	31
Physiographic guides	31
Botanical guides	32
Interpretation—Continued	
Interpretation of aerial photographs in engineering geology	33
Surficial materials	33
Ground conditions	33
Elements of soil pattern	34
Landform	34
Drainage characteristics	34
Erosional characteristics	35
Photographic tone	35
Color	36
Vegetation	36
Land use	37
Permafrost	37
Distribution and type of vegetation	37
Polygonal relief patterns	37
Pingos	38
Features resulting from thawing	38
Absence of permafrost	38
Erosion, transportation, and deposition	39
Landslides	39
Beach erosion	39
Bedrock	39
Geologic structure and type of rock	39
Interpretation of aerial photographs in hydrologic studies	40
Locating potential ground-water sources	40
Water-loss studies	40
Other applications	40
Instrumentation	41
Kinds of instruments	41
Measuring devices for use with paper prints	41
Plotting devices for use with paper prints	42
Measuring and plotting devices for use with paper prints	45
Measuring and plotting devices for use with glass-plate diapositives	45
Other instruments	48
Exaggerated-profile plotter	48
Interval-measuring device	48
Universal tracing table	48
Measurement	48
Principles of vertical measurement	48
Determination of altitude differences by the parallax method	50
Use of stereometer-type instruments	51
Use of double-projection instruments	54
Tilt	55
Determination of altitude differences from a single photograph	56

	Page
Instrumentation—Continued	
Measurement—Continued	
Geologic uses of parallax measurements	56
Determining strikes and dips	56
Determining stratigraphic thickness	57
Isopach mapping	58
Facies change	59
Structure contouring	60
Notom-15 quadrangle	60
Discovery anticline	61
Determining displacements on faults	61
Determining stream gradients	63
Direct determination of slope	63
Dipping platen	63
Stereo slope comparator	63
Dip estimation	64
Other methods of determining angles of slopes	64
Other methods for determining quantitative data	64
Instrumentation—Continued	
Plotting	66
Construction of control layout	67
Orthographic positioning	67
Plotting on orthographic base maps or control layouts	67
Plotting on orthophotographs	69
Plotting on gridded base maps	69
Vertical positioning in cross sections	69
Interpretation, measuring, and plotting systems	69
Instrument capability	72
Relation between instrument capability, scale, and vertical measurements	74
Horizontal positioning	74
Source and identifying data of aerial photographs	222
References cited	224
Index	229

ILLUSTRATIONS

		Page
FIGURE 1.	Geometry of the vertical aerial photograph	3
2.	Spectral reflectance curves of weathered samples of Bernal formation and San Andres limestone	8
3.	Drainage map of large area in vicinity of ring dike shown in figure 54	10
4.	Generalized soil map of area shown in figure 48	12
5.	Sketch showing long tributary streams on updip side of strike valley in area of low dips	20
6.	Sketch showing long tributary streams on downdip side of strike valley in area of steep dips	20
7.	Drainage map of area shown in figure 74 and vicinity	22
8.	Drainage map of area shown on left half of figure 73	25
9.	Drainage map of area shown in figure 94	28
10.	Stereometers	43
11.	Stereo slope meter	43
12.	Parallax ladder	43
13.	Sketchmaster	44
14.	Radial planimetric plotter	44
15.	Stereotope	44
16.	Multiplex	46
17.	ER–55 plotter	46
18.	Kelsh plotter	46
19.	Exaggerated-profile plotter (lever and fulcrum type)	49
20.	Exaggerated-profile plotter (pantograph type)	49
21.	Interval measuring instrument	49
22.	Universal tracing table	49
23.	Diagram showing relation between absolute stereoscopic parallaxes and horizontal distances actually measured with stereometer-type instruments in determining differences in altitude from paper prints	50
24.	Diagram showing relation between absolute stereoscopic parallaxes and vertical distance measured with double-projection type instruments in determining differences in altitude from glass plates	51
25.	Sketch showing correct orientation of photographs for stereoscopic viewing	52
26.	Diagram of gently dipping beds showing relation of stratigraphic thickness to differential parallax determined at any two points along dip direction and at the formation contacts	57
27.	Diagram of gently dipping beds showing relation of stratigraphic thickness to differential parallax determined by floating-line method	58
28.	Diagram of steeply dipping beds showing relation of stratigraphic thickness to dip angle and horizontal distance between top and bottom of bed	59
29.	Diagram showing graphic reconstruction of marker bed along line of section	61
30.	Diagram showing graphic construction in positioning structure-contour lines on top of marker bed and the projecting of these lines to their relative horizontal positions along the line of section	62
31.	Diagram showing relation of structure-contour positions along two lines of section at different altitudes	62
32.	Dipping platen	63
33.	Stereo slope comparator	63

Page

FIGURE 34. Slope conversion chart showing relation of exaggeration factor, exaggerated slope, and true slope ... 65
35. Diagram, based on tangent functions, showing relation of true dips to exaggerated dips seen in stereoscopic models ... 66
36. Photogrammetric systems for geologists ... 70
37. Photogrammetric measuring and plotting systems for geologists showing relation of different instruments to vertical-measurment and horizontal-positioning errors ... 71
38. Diagram showing datum-curvature relation to maximum expected error in measuring vertical intervals from leveled double-projection stereoscopic model ... 73
39. Poorly resistant pyroclastic rocks overlain by resistant capping formation (Colorado) (stereoscopic pair) ... 77
40. Area underlain predominantly by gently folded sandstone, shale, conglomerate, and graywacke (northern Alaska) (stereoscopic pair) ... 78
41. Extrusive volcanic rocks and associated cinder cone (Utah) (stereoscopic pair) ... 79
42. Flat-lying sandstone (southern Utah) (stereoscopic pair) ... 80
43. Sandstone and conglomerate beds intruded by diorite porphyry laccolith (Utah) (stereoscopic pair) ... 81
44. Gently dipping beds of sandstone, siltstone, and conglomerate that locally contain channel-fill deposits (Arizona) (stereoscopic pair) ... 82
45. Gneiss, schist, and granite flanked by dipping sedimentary rocks truncated by pediment gravel (Colorado) (stereoscopic pair) ... 83
46. Landslide area (Colorado) (stereoscopic pair) ... 84
47. Orthophotograph and perspective photograph of same area ... 85
48. Area showing relation of residual soils to underlying rock types and structure (South Carolina) (stereoscopic pair) ... 86
49. Shale and thin sandstone interbeds capped by poorly consolidated gravel and sand (Texas) (stereoscopic pair) ... 88
50. Recently faulted strand lines of former lake (Nevada) (stereoscopic pair) ... 90
51. Steeply dipping sedimentary rocks intruded by quartz diorite (California) (stereoscopic pair) ... 92
52. Area showing drainage characteristics in surficial materials (Wyoming) (stereoscopic pair) ... 94
53. Area of basalt flows (Idaho) (stereoscopic pair) ... 96
54. Ring-dike area (North Carolina) (stereoscopic pair) ... 98
55. Area in Maine showing esker landform on photographs of two different scales (stereoscopic pairs) ... 100
56. Stabilized sand dunes (central Alaska) (stereoscopic pair) ... 102
57. Morainal deposits of two glaciations (central Alaska) (stereoscopic pair) ... 104
58. Morainal deposits of continental glaciation (South Dakota) (stereoscopic pair) ... 106
59. Gently dipping sedimentary rocks lying unconformably on gneiss-granite-schist complex (Utah) (stereoscopic pair) ... 108
60. Gently dipping sedimentary rocks cut by numerous near-vertical faults (Utah) (stereoscopic pair) ... 110
61. Flat-lying beds of sandstone, limestone, and shale (Texas) (stereoscopic pair) ... 112
62. Area of faulted gently dipping sedimentary rocks (Utah) (stereoscopic pair) ... 114
63. Shale in semiarid climatic area (Utah) (stereoscopic pair) ... 116
64. Shale and limestone in humid climatic area (Virginia) (stereoscopic pair) ... 118
65. Area of gently dipping limestone and shale (Pennsylvania) (stereoscopic pair) ... 120
66. Area mantled by glacial deposits (South Dakota) (stereoscopic pair) ... 122
67. Glaciated area in southeastern Alaska (stereoscopic pair) ... 124
68. Approximately flat-lying limestone and interbedded sandstone and marlstone beds covered locally by alluvium and windblown deposits (Texas) (stereoscopic pair) ... 126
69. Area of basalt flows (Idaho) (stereoscopic pair) ... 128
70. Area of granite (South Dakota) (stereoscopic pair) ... 130
71. Area of granitic intrusive rocks (Wyoming) (stereoscopic pair) ... 132
72. Area showing vegetation differences in igneous and metamorphic terrain (southeastern Alaska) (stereoscopic pair) ... 134
73. Area underlain by silicic volcanic tuffs and flows and bedded argillite or slate (North Carolina) (stereoscopic pair) ... 136
74. Area of folded, faulted, and highly metamorphosed rocks (North Carolina) (stereoscopic pair) ... 138
75. Area underlain by phyllite and slightly metamorphosed slaty rocks (Alabama) (stereoscopic pair) ... 140
76. Heavily vegetated terrain underlain by metamorphic and extrusive volcanic rocks (southeastern Alaska) (stereoscopic pair) ... 142
77. Flat-lying beds of limestone and shale (Kansas) (stereoscopic pair) ... 144
78. Flat-lying beds of sandstone, limestone, and shale (Texas) (stereoscopic pair) ... 146
79. Area of sparse outcrops underlain largely by gently folded sandstone, conglomerate, and shale (northern Alaska) (stereoscopic pair) ... 148
80. Gently to steeply dipping sedimentary rocks overlying schist-gneiss-granite complex (Wyoming) (stereoscopic triplet) ... 150
81. Gently folded sedimentary rocks (central Utah) (stereoscopic pair) ... 152
82. Ring dike in New Hampshire (stereoscopic pair) ... 154
83. Gently dipping sedimentary rocks offset by near-vertical fault (Utah) (stereoscopic pair) ... 156

		Page
FIGURE 84.	Faulted, gently dipping sedimentary rocks (Utah) (stereoscopic pair)	158
85.	Vegetated terrain underlain by igneous and metamorphic rocks locally covered by basalt flows (southeastern Alaska) (stereoscopic pair)	160
86.	Area of crystalline rocks (Wyoming) (stereoscopic pair)	162
87.	Lava flow lying unconformably on gently dipping sedimentary rocks (New Mexico) (stereoscopic pair)	164
88.	Gently dipping sedimentary rocks overlain in part by river gravels (Utah) (stereoscopic pair)	166
89.	Gently folded sedimentary rocks in heavily vegetated area (northern Guatemala) (stereoscopic pair)	168
90.	Plunging anticline in gently folded rocks (southern Utah) (stereoscopic pair)	170
91.	Stratigraphic section across gently folded anticline (Utah) (stereoscopic pair)	172
92.	Gently dipping sedimentary rocks, on east side of San Rafael Swell (Utah) (stereoscopic pair)	174
93.	Uncontrolled mosaic of Umiat anticline area, northern Alaska, underlain by shale, sandstone, conglomerate, and graywacke	176
94.	Subsurface structure reflected in surface drainage characteristics (Texas) (stereoscopic pair)	178
95.	Same photographs as figure 94, but reversed to show pseudoscopic effect as an aid to interpretation (stereoscopic pair)	180
96.	Uncontrolled mosaic of Wainwright area, northwestern Alaska	182
97.	Area underlain predominantly by gently dipping sandstone and shale (northern Alaska) (stereoscopic pair)	184
98.	Gently dipping sedimentary rocks cut by high-angle faults (Nevada) (stereoscopic pair)	186
99.	Complexly folded and faulted area of greenstone, schist, limestone and marble (southeastern Alaska) (stereoscopic pair)	188
100.	Igneous and metamorphic terrain (southeastern Alaska) (stereoscopic pair)	190
101.	Gently tilted and faulted lava flows (Oregon) (stereoscopic pair)	192
102.	Area of pegmatite dikes (South Dakota) (stereoscopic pair)	194
103.	Metamorphosed sedimentary rocks intruded by quartz monzonite (California) (stereoscopic pair)	196
104.	Distinctive landform of gravel terraces along a major stream (northeastern Utah) (stereoscopic pair)	198
105.	Areas showing drainage characteristics in surficial material that is predominantly loess (stereoscopic pairs)	200
106.	Area of surficial deposits, primarily windblown (central Nebraska) (stereoscopic pair)	202
107.	Mottled soils of drift plain (Iowa) (stereoscopic pair)	204
108.	Coastal plain underlain by clay, sand, and gravel (New Jersey) (stereoscopic pair)	206
109.	Polygonally patterned ground in permafrost area along major stream (northern Alaska) (stereoscopic pair)	208
110.	Well-developed pingo in area of permafrost (northern Alaska) (stereoscopic pair)	210
111.	Area of permafrost (northern Alaska) (stereoscopic pair)	212
112.	Conspicuous beaded drainage in area of permafrost (northern Alaska) (stereoscopic pair)	214
113.	Landslide area in volcanic and sedimentary terrain (New Mexico) (stereoscopic pair)	216
114.	Damsite area (southeastern Alaska) (stereoscopic pair)	218
115.	Gridded photograph	220
116.	Gridded base map	221

AERIAL PHOTOGRAPHS IN GEOLOGIC INTERPRETATION AND MAPPING

By Richard G. Ray

ABSTRACT

Aerial photographs today are widely used to obtain both qualitative and quantitative geologic information; vertical aerial photographs are used almost to the exclusion of other types. Techniques and procedures described herein relate primarily to vertical photography.

Geologic interpretation of aerial photographs is based on the fundamental recognition elements of photographic tone, color, texture, pattern, relation of associated features, shape, and size. The scale of photographs, as well as the vertical exaggeration that is present in most stereoscopic models, also are significant in photointerpretation.

The amount of geologic information that may be obtained from aerial photographs is primarily dependent on the type of terrain (igneous, metamorphic, or sedimentary), climatic environment, and stage of the geomorphic cycle. Because features are more readily recognized where strong differences exist in the erosional resistance of adjacent rocks, sedimentary terrain may be expected to yield the greatest amount of information from aerial photographs. Metamorphic terrain may yield the least information because metamorphic processes tend to destroy differences that may have existed in the unmetamorphosed rocks. Combinations of criteria such as photographic tone, texture, pattern, and vertical exaggeration permit inferences as to rock type and geologic structure, which are important in petroleum exploration, ore-deposits search, and engineering geology.

In petroleum exploration aerial photographs provide a wealth of information primarily with regard to potential structural traps. Folds commonly may be interpreted from a study of strike and dip of bedding and from stream patterns; anomalous stream characteristics, such as stream deflections, may suggest subsurface structures. The variety of photorecognition criteria that suggests faults permits aerial photographs to be of particular use in many ore-deposits studies. Analysis of soil patterns yields information regarding permeability of the surficial materials that are a concern of the engineering geologist.

The instruments used for viewing photographs, measuring geologic features, and compiling geologic maps range from simple stereoscopes and stereometers, or measuring bars, to complex double-projection instruments such as the multiplex or Kelsh plotter. Some instruments require the use of paper prints; others require the use of glass-plate diapositives. Measuring devices primarily provide spot heights or differences in altitudes; these quantitative data may be geologically significant in measurement of stratigraphic thickness and dip of beds and in structure contouring. Accuracy of vertical measurements is related fundamentally to the scale of photography and the instruments used for making measurements. In general, accuracy of measurement is greater when large-scale photographs are used and when double-projection instruments rather than simple parallax bars are employed.

INTRODUCTION

Use of aerial photographs to obtain geologic information—popularly called photogeology—has contributed to mineral and fuel discoveries, and to engineering geology studies, as well as to the general geologic mapping of many areas; it also has increased the efficiency of many geologic mapping groups by adding speed, economy, and accuracy to areal mapping as well as adding certain geologic information that is impossible, difficult, or economically impractical to obtain by routine field-mapping methods. The past financial success of consultants in geologic interpretation of aerial photographs attests to successful geologic application of photogeologic procedures and techniques, particularly in petroleum geology, and to lesser extent in mining and engineering geology.

Many technical papers on the geologic interpretation of aerial photographs have been published, primarily since the end of World War II; on several occasions symposia on photointerpretation, and specifically photogeology, have been presented. Much of the information currently available has been published as individual articles and they are scattered throughout the literature; comprehensive treatments on the geologic interpretation of aerial photographs are generally unavailable now (1959) (see Eardley, A. J., 1942; Smith, H. T. U., 1943b; and Petrusevich, M. N., 1954). In addition to the published information much unpublished information also has accumulated in recent years. The collection and synthesis of much of this information, together with discussion of photointerpretive and related photogrammetric procedures, are the main objectives of this paper. The paper is particularly intended as a guide to geologic interpretation of aerial photographs as applied as a tool in reconnaissance geologic mapping, and as a reference to published papers representative of the photogeologic literature.

The primary objectives of photogeology are (a) to contribute to geologic mapping, which in turn is basic to mineral and fuel exploration, engineering geology studies, some water-resources investigations, and related studies, and (b) to contribute to geologic knowledge through research. The objectives of photogeology may be economic or academic, and procedures used can be expected to differ widely, ranging, for example, from use solely of simple lens stereoscopes for qualitative interpretation to employment of precision stereoplotters for making geologic measurements. Regardless of procedures used, however, photogeology to date has contributed principally to the broad aspects of geologic study, that is, in mapping distribution of rock types and structures. The interpreter can only infer the composition of rock types from photographs; he cannot identify mineral types or absolute ages of rocks. Thus, maximum use of photogeologic procedures is attained by combining photogeologic studies with various laboratory studies and with field investigations.

The uses of aerial photographs and the various photogeologic procedures are discussed herein under the general headings of interpretation and instrumentation. The part dealing with interpretation is widely illustrated with stereoscopic pairs and triplets, single photographs, and mosaics, together with explanatory notes, to demonstrate the kinds and amounts of geologic information that can be obtained from aerial photographs of differing geologic terrains and to illustrate some uses of photographs in specific studies, such as the search for petroleum. These photographs demonstrate primarily the qualitative uses of the fundamental recognition elements in geologic interpretation; they represent only a sampling of the tremendous number of illustrations available. Because reproduction processes tend to obscure details only subtly expressed on aerial photographs, selection of photographs used in this paper was confined principally to those that illustrate clearly defined recognition elements and geologic features. All aerial photographs (figs. 39–114) are at the end of the paper. Agencies holding the negatives of these photographs are given in a list that follows the photographs.

Methods and significance of determining quantitative geologic information from aerial photographs are described under the heading of instrumentation.

THE AERIAL PHOTOGRAPH

The aerial photograph is an instantaneous record of the ground details as determined chiefly by the focal length of the camera lens, the flying height of the airplane at the time of exposure, and the film and filters used. It may also be defined as a composite of photographic images, which make up the recognition elements used for interpretation. The aerial photograph is a perspective photograph that is geometrically related to the type of camera in which it is taken; it may be a vertical photograph, taken with the camera axis pointing essentially vertically down, or it may be an oblique photograph, taken with the camera axis purposely tilted from vertical, generally 20° or more. Vertical photographs currently are used almost to the exclusion of oblique photographs for geologic interpretation, and most photogrammetric instruments used in photogeology in the United States are designed to accommodate vertical photographs; hence the following discussion is limited to techniques applicable to the study of vertical photography. Twin low-oblique photographs—those in which the apparent horizon is not shown—generally may be transformed and the resulting paper prints used as vertical photographs; however, low-oblique photographs cannot be used in many stereoplotting instruments unless the instruments are specially designed.

A general knowledge of the geometry and terminology used with vertical aerial photographs is necessary if one is to understand and make maximum use of photographs for interpretation and mapping purposes. The terminology and geometry of the vertical photograph are presented in figure 1.

FACTORS THAT AFFECT THE PHOTOGRAPHIC IMAGE

Factors that affect the photographic image, and hence interpretation, may be divided into two groups: (a) The relatively constant man-controlled factors, such as focal length of lens, flying height, film and filter combinations, and lens angle; and (b) the variable natural factors including color of objects photographed, position of an object with respect to the angle of sun, amount of haze in the atmosphere, and others. The constant factors are discussed briefly below; effects of natural factors on the photographic image are described where appropriate throughout the text.

FOCAL LENGTH AND FLYING HEIGHT

Focal length and flying height may be considered together because of the relation of photograph scale to these two factors. In terms of focal length and flying height, the average scale of a photograph is expressed as

$$S=\frac{f}{H}$$

or

$$\text{Scale}=\frac{\text{focal length (feet)}}{\text{flying height (feet)}}.$$

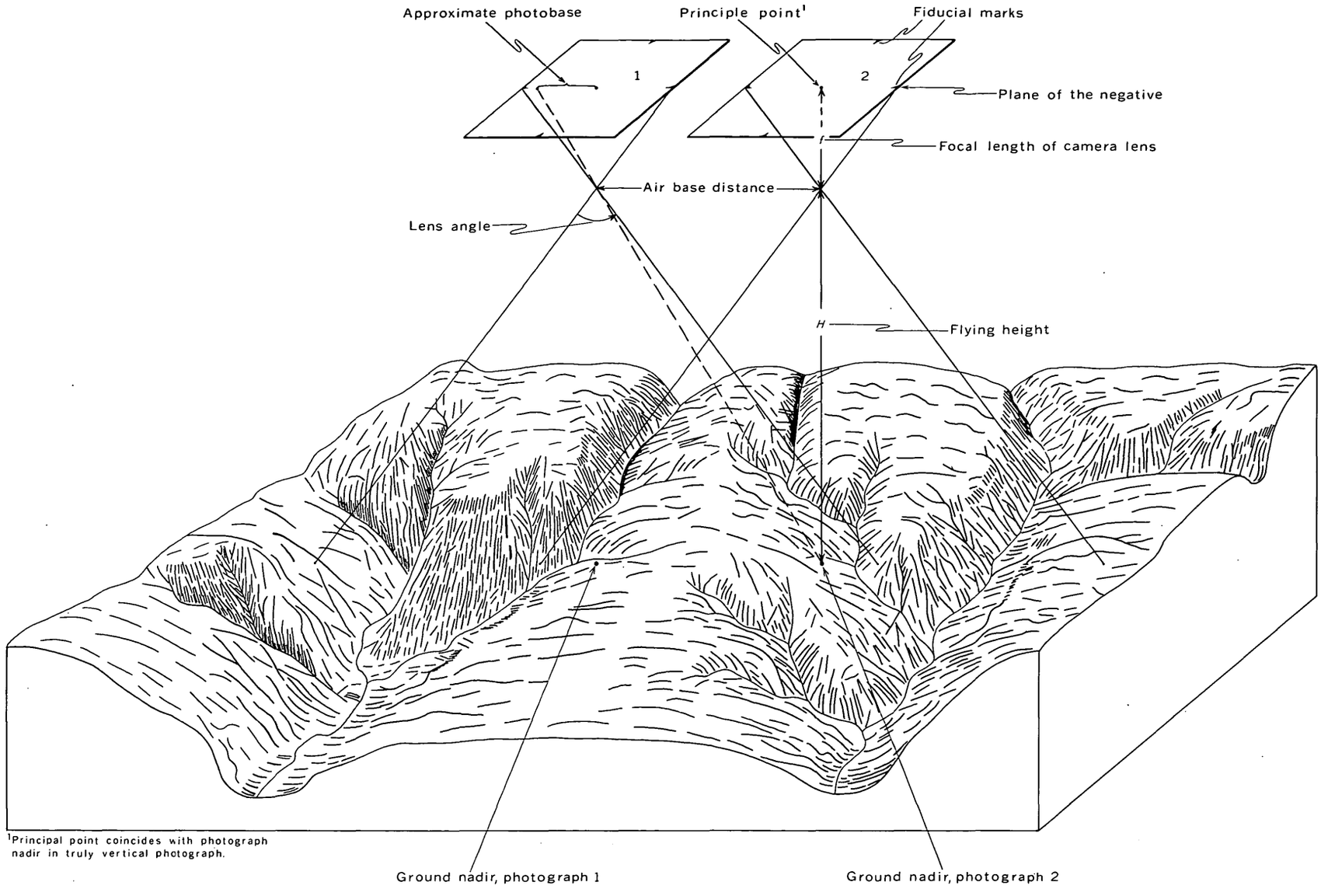


FIGURE 1.—Geometry of the vertical aerial photograph.

Thus, for example, the scale of photographs taken at 10,000 feet above mean terrain with a 6-inch (0.5 foot) focal-length lens is

$$\frac{0.5}{10{,}000}=1:20{,}000.$$

It is evident that as focal length increases, the scale of photographs becomes larger, but as flying height increases, scale of photographs becomes smaller. Therefore, at any given flying height, long-focal-length lenses result in larger scale photographs than short-focal-length lenses. It follows also that at a given flying height a greater number of photographs are necessary to cover a given ground area when long-focal-length lenses are used. Doubling the focal length of the lens, for example, will quadruple the number of photographs required to cover a given area at a given flying height.

It should be noted that if a photograph is enlarged or reduced, the "effective" focal length for that photograph is also changed in direct proportion to the amount of enlargement or reduction. Thus, if photographs taken with a 6-inch-focal-length lens are enlarged two times, the effective focal length is changed from 6 inches to 12 inches. Parallax measurements (see p. 53), used in determining differences in altitude, are increased, but the absolute value for each unit of parallax measurement is decreased. Reducing or enlarging photographs thus has a significant effect with respect to choosing appropriate measuring and plotting instruments, and in measuring differences in altitudes.

For determining scale from the formula $S = f/H$ the effective focal length must be used where photographs have been reduced or enlarged. Particular note should be made in the use of transformed low-oblique photographs, in which the effective focal length is almost always less than the focal length of the camera.

FILM AND FILTER COMBINATIONS

The appearance of the photographic image may be controlled to marked extent by the sensitivity of the film and by the light transmission of the filter employed. The sensitivity of a film emulsion may be controlled when the film is manufactured so that all or only selected parts of the visible spectrum are recorded, or so that part of the invisible spectrum, such as infrared light, is recorded. Also, the wave length of light reflected from an object and actually recorded may be controlled in part by filter combinations. The recording of selected wave lengths of light, controlled by filters or type of film, or by combinations of film and filters, affects the photographic image, primarily by affecting the photographic tone. Conventional panchromatic aerial film is generally exposed through a minus-blue filter and permits the recording of blue-green, yellow, orange, and red light. When color film is used the entire visible spectrum is commonly recorded and a greater number of color differences can be distinguished than on conventional black-and-white film. Special color film or color film used with filters may distort the color of the objects photographed, but if differentiation of geologic features is permitted, then lack of color fidelity may not be detrimental to interpretation. Ideally, film and filter combinations may be used to accentuate specific features for a given type of interpretation (see p. 7–8).

LENS ANGLE

The angle of the camera lens—that is, the apex angle of the cone of rays passing through the lens—is important indirectly in relation to radial displacement and parallax measurements, which are in turn significant with regard to photogrammetric applications in geologic interpretation. Characteristically, long-focal-length lenses (greater than 6 inches) have a narrower lens angle than short-focal-length lenses (6 inches or less). Thus, to maintain a given scale and format size, photographs taken with a narrow-angle (long-focal-length) lens requires flying at a higher altitude than with a wide-angle (short-focal-length) lens. Under these conditions, radial displacement (also termed "relief displacement") of similar image points is less when narrow-angle lenses are used, but only because of the greater flying height required by the narrow-angle lens to maintain the given scale and format size. The parallax difference for an object of specific height is in turn affected as a result of the difference in flying height, the parallax difference decreasing directly with increased flying height for a given focal-length lens (see p. 53). Thus it can be said that lens angle indirectly affects parallax measurement. When a constant flying height is maintained, however, lens angle does not affect parallax measurements of similar image points. Image distortion at the margins of photographs taken with a wide-angle lens may be greater than on photographs taken with a narrow-angle lens and this is considered by many to be detrimental to photointerpretation, especially in high-relief terrain.

VIEWING OF PHOTOGRAPHS

Photographs may be viewed singly, as mosaics, or as stereoscopic pairs. Most commonly stereoscopic pairs of paper prints are viewed in reflected light with simple lens, prism, or mirror stereoscopes, notes are made directly on the prints or on transparent overlays, and information is later transferred to a base map or

mosaic. Many paper prints can also be viewed with transmitted light, which may be helpful in revealing photographic detail. If vertical measurements are made from paper prints a separate measuring device must be commonly employed with the stereoscope. In recent years double-projection instruments, employing the anaglyph principle in forming the stereoscopic model from glass-plate diapositives, have been used increasingly in geologic interpretation.

When photographs are viewed singly or in a mosaic, a two-dimensional view is obtained. The single photograph or mosaic is normally viewed along a line generally perpendicular to the photograph surface, but for some subtle linear features, an oblique view of the surface with a reflected light source moved to different positions may reveal photographic details otherwise difficult or impossible to see (see Lattman, 1958, p. 575). Many valuable relations of geologic and associated features can be observed, particularly as a result of the overall view permitted by mosaics or single prints of small scale, but a two-dimensional view reveals only part of the data available to the interpreter; the value of three-dimensional, or stereoscopic, examination of aerial photographs in contrast to studying the two-dimensional view cannot be overemphasized. Conspicuous geologic features are commonly visible on single aerial photographs or mosaics of aerial photographs, but the wealth of information seen in stereoscopic view is many times greater. Details, such as fine lines or textural differences not readily seen on single photographs—or even on the ground—commonly are shown clearly in the stereoscopic model. Such clarity is in many places a direct result of the common association of fine lines and textures with relief changes, which are exaggerated in most stereoscopic models. To take advantage of the exaggerated vertical dimension, which is so helpful in photointerpretation, aerial photographs should of course be viewed stereoscopically. It may be desirable also to view the photographs pseudoscopically by reversing the print positions so that hills appear as valleys and vice versa. In pseudoscopic view, stream patterns or anomalies may stand out (see fig. 95), or because of the unnatural view other features may be accentuated. Aschenbrenner (1954, p. 401) demonstrated by the use of a seemingly random distribution of dots, which may be likened to silver grains of a photographic emulsion, that information not visible on a single picture can be clearly seen in stereoscopic view.

INTERPRETATION

Interpretation was defined broadly by Summerson (1954, p. 397) as the prediction of what cannot actually be seen; and thus geologic interpretation of aerial photographs is not unlike certain geologic interpretations of field-observed data. Colwell (1952, p. 535; 1954, p. 433) defined interpretation as "* * * the act of examining photographic images of objects for the purpose of identifying the objects and deducing their significance." However, geologic interpretation, more often than not, is a result of combined deductive and inductive reasoning, based on the principle of cause and effect. For example, certain features easily identified on aerial photographs, such as terminal moraines and kettle holes, are inductively concluded to have resulted from glaciation, and this in turn may lead by deductive reasoning to the specific identification of less readily recognizable features, such as certain kame terraces. Further deduction may lead to conclusions concerning the type of material present in these terraces. On the other hand, interpretation may be directed mainly toward understanding the geologic significance or history of a broad area, and specific features such as positions of beds and measurements of stratigraphic thicknesses combine by inductive reasoning to reveal the probable geologic conditions that resulted in those features.

Geologic interpretation of aerial photographs can be considered generally a two-step process. The first step includes observation, fact-gathering, measurement, and identification of features on the photographs. The second step involves deductive or inductive mental processing of these data in terms of geologic significance. According to Stone (1951, p. 755) a procedural or methodical approach to interpretation should be used because "The establishment of procedure prepares the way for orderly and complete analyses of complex subjects." A procedural or methodical approach appears to be especially applicable to the observational phase of a photogeologic study, and it will give a firm basis on which the interpretive phase is dependent.

Observational data, also termed "first-order" information (see Hopkins, Karlstrom, and others, 1955, p. 142), may be subjected to either the empirical or rational method of processing (Smith, H. T. U., 1953, p. 9–10). According to Smith (1953, p. 9) the empirical process is largely mechanical rather than perceptive, and involves matching images of a photograph with similar reference images; reasoning is largely by analogy and this "Reasoning by analogy alone is notoriously deceptive, unless extreme care is taken to make certain that the analogy is truly complete." Smith (1953, p. 9) also made the particularly significant statement that "Nature is not always so obliging as to provide the desired simplicity and uniformity of conditions" that would permit the ready application of empirical methods. Indeed, much in nature is com-

plex and nonuniform, many terrain features are polygenetic, and thus interpreting the geologic significance of observational data is dependent largely upon a thorough understanding of the principles of the sciences that explain the observational data. "The physical conditions of a particular terrain change, and the adjustment to that change is a gradual one, allowing all manner of intermediate forms and combinations between the norm for the old situation and that for the new" (Summerson, 1954, p. 396).

Surface expressions of geologic features—the observational data—range from the very obvious to the very subtle. Sorting those data that are significant to a particular problem and properly relating these features one to another provide a measure of the ability of the individual interpreter. Where more than one plausible explanation of observational data is possible, the experience as well as the fundamental geologic ability of the interpreter become especially significant. Thus a rational processing of observational data will yield the most meaningful interpretive results. This does not imply that an empirical method of processing observational data, exemplified by the numerous photointerpretation "keys," may not yield satisfactory results in certain geologic problems and terrains, but the logical, scientific approach demands a rational processing of observational data, particularly where inferences based on subjective interpretations are required.

If observational data cannot be rationally interpreted, they may still be of some empirical value. For example, an interpreter may recognize two zones of vegetation on aerial photographs. Without knowledge of plant ecology, he may infer that a geologic contact exists between the two vegetation types. But a knowledge of plant ecology, permitting a rational interpretation, might well have allowed a further inference that one type of rock or soil was likely to be highly permeable in contrast with the other, thus revealing information with regard to certain physical characteristics of the rock or soil, which in turn may suggest something of the lithologic character. Thus "* * * the understanding of any particular terrain requires more than the knowledge of the geology * * *" (Summerson, 1954, p. 397). The greatest understanding will be by individuals grounded in the natural sciences and who understand, as a result, the various factors that contribute to a particular region. Because any geologic terrain is normally a complex that also includes features of fundamental interest to the botanist, forester, soil scientist, and others, photogeologic interpretation must take cognizance of these related sciences. The combined use of vegetation, soils, and geologic features to interpret geology is an example of what has been termed the "convergence of evidence" principle (Colwell, 1952, p. 566).

Interpretation, then, begins with the observation, identification, and measurement of features on photographs. One of the most obvious features is that of landform, and it has been stated by Johnstone (1953, p. 265) that analysis of landforms constitutes the basis of photogeology. Smit Sibinga (1948) also pointed out the importance of landform, or geomorphic expression, in interpreting the lithologic character of rocks; but analysis of landform, however important, cannot be the complete basis for photogeologic interpretation, for there is additional "first-order" information such as vegetation patterns, soil patterns, and stream patterns; photogrammetric measurements also provide first-order data. Features other than landform may actually be more important for certain structural interpretations. For example, vegetation may grow along and mark the location of a fault. Thus, interpretation is based not only on landform but also on photographic tone differences, color differences, drainage patterns, erosion patterns, soil patterns, vegetation patterns, and any other surface expression of underlying geology. It is fundamental that photointerpretation is only applicable to those geologic features that do develop such surface expressions.

The many features of surface expression used in photogeologic interpretation are identified on the basis of recognition elements—characteristics of the photographs that result from the scale selected; the color of the rocks, vegetation, and soils of the terrain photographed; the kind of film and filters used; the processing of the film; and related factors. The most significant recognition elements are relative photographic tone, color, texture, pattern, and association of features. Shape is important in identifying many constructional landforms. Finite size as a recognition element for geologic interpretation has been used very little, although relative size is commonly considered by the interpreter. The increasing use of photogrammetry in geologic interpretation, however, portends an increasing importance for size, not so much as a recognition element in the usual sense of the word, but as an interpretation element (see p. 13). Shadows may help in distinguishing certain tree types, which in turn may have geologic significance.

INTERPRETATION FACTORS

RECOGNITION ELEMENTS

PHOTOGRAPHIC TONE

Photographic tone is a measure of the relative amount of light reflected by an object and actually

recorded on a black-and-white photograph; it is fundamental to all other recognition elements, except color. Tones on conventional photographs are usually shades of gray, but may be black or white. Because of the ability of the human eye to differentiate subtle tone changes, relative photographic tone is a significant asset in geologic interpretation of aerial photographs. However, photographic tone is subject to wide variation and there are limits to its usefulness as a recognition element because of the many factors that can influence it.

Photographic tone depends on light reflectivity, which in turn depends on location of an object with respect to the sun; thus the time of day and month of year are influencing factors. Haze strongly scatters light, particularly at the short or blue end of the spectrum and hence affects photographic tone unless corrective filters are used. Geographic latitude, angle of reflected light, sensitivity of film, light transmission of filters, and processing also may exert considerable effect on photographic tone. Hence a standardized tone scale (Daehn, 1949, p. 287) would appear to have little usefulness unless relative photographic tones on different photographs could be equated in terms of the tone scale. It is probable that the use of a densitometer to measure relative photographic tone in terms of the density of the negative would be a satisfactory measure of tone, even though many factors influence the density. Particularly in quantitative studies the use of a densitometer to measure relative photographic tone may prove very worthwhile in differentiating certain geologic features (Ray and Fischer, 1960).

Photographic tone, despite the many factors that may affect it, can be a particularly useful interpretation element; its usefulness depends on the problem under consideration and on how tone is used in conjunction with other recognition elements. For example, if the fracture pattern of an area were studied and it were known that a lush and dark-toned vegetation grew along the fractures because of concentration of moisture, the relative photographic tone probably would be a significant recognition element regardless of the limiting factors mentioned above. On the other hand, as a means of distinguishing between two types of trees that reflect similar amounts of light but which might signify differences in the underlying geology, photographic tone might be of little value unless used in conjunction with other recognition elements, such as crown texture.

Raup and Denny (1950, p. 120), in work along the Alaska Highway, considered photographic tone the least satisfactory criterion in identifying and interpreting vegetation. But Tator (1951, p. 717) considered tonal contrasts to be major keys for recognizing landscape features of low relief in the coastal region of the Gulf States, such tonal differences resulting mainly from soil and vegetation differences. Schulte (1951, p. 697) pointed out, with regard to pure stands of trees, that at large scales photographic detail is more important, but at small scales tone becomes relatively more important.

Because the analysis of photographic tone is highly subjective it has been suggested that photographic tone might not be as useful as other recognition elements in interpretation. Because of differences that may arise from position, angle of reflected light, processing, and other factors, Stone (1956, p. 125) stated that photographic tone in interpretation probably has been overemphasized. This is true if the factors that affect tone prevent photographic distinction of images that might otherwise be made. But if changes in relative photographic tone are present on a photograph, the interpreter should expect that these changes might be geologically significant. Indeed, photographic tone is probably the most used recognition and interpretation element, although it is generally used in conjunction with one or more other recognition elements. The absence of photographic-tone changes, as a result of processing and other factors, where such tone changes might normally be expected, does not detract from the possible usefulness of tone changes on other parts of a photograph. It merely suggests that the potential of photographic tone differences has not been accomplished for the photographs in question.

It is worthy of note that in interpretation strong tonal contrasts are generally desirable. Yet modern automatic dodging devices commonly used in printing photographs generally reduce overall tonal contrasts, although locally, as in darkly shaded areas or brightly lighted areas, automatic dodging may strengthen tonal contrasts. Because most aerial negatives are slightly lighter in the corners than in the center, hand dodging is commonly necessary if automatic dodging is not employed in making prints. However, undodged or hand-dodged prints are probably the best for general photointerpretation.

For special interpretation problems it may be possible to enhance tonal contrasts within a limited range of the tone scale by film intensifiers or other photographic processes, such as use of selected filters. Ray and Fischer (1960) used selected filters in photographing weathered samples of the Bernal and San Andres formations of New Mexico. The Bernal formation is a red thin-bedded shale and shaly siltstone; the San Andres limestone is primarily a grayish limestone. Spectral reflectance curves, based on spectrophotome-

ter studies, show significant differences for these two formations (fig. 2). Particularly at the short or blue end of the spectrum a strong difference in intensity of reflected light is present; the San Andres limestone reflects almost twice as much light as the Bernal formation. A noticeable difference is also present at the long or red end of the spectrum. But the spectral reflectance curves of the Bernal and San Andres formations within 500 to 675 millimicrons—the wave lengths generally recorded on conventional black-and-white aerial photographs—show that the overall light reflectance from these two formations would average out to be generally similar and little photographic distinction should be expected within this range. It is significant that strong reflectance differences which exist in one part of the spectrum may be masked by reflectance characteristics in another part of the spectrum, and therefore to achieve photographic distinction of two features, it would probably be necessary to record a restricted part of the spectrum. Photographs of the Bernal and San Andres formations taken through filters that permit recording only of reflected light at the short or long end of the spectrum show a marked photographic distinction of the two formations.

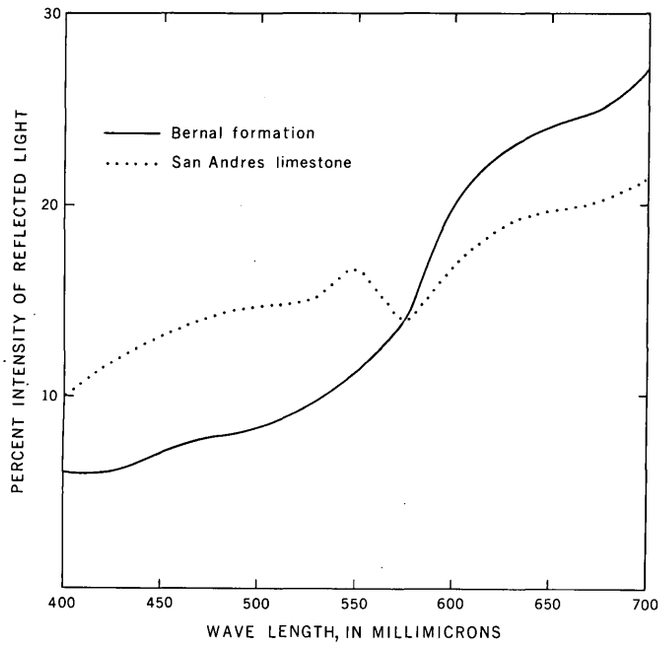


FIGURE 2.—Spectral reflectance curves of weathered samples of Bernal formation (red thin-bedded shale and shaly siltstone) and San Andres limestone (primarily a grayish limestone), New Mexico.

COLOR

Color as a recognition element could be one of the most useful, if not the most useful, criterion for interpretive purposes (see Kent, 1957; Ray, 1958; Fischer, 1958; and Minard, 1960). The significance of differences within a photograph is interpretation and the greater the number of differences, such as color contrasts, the greater is the potential for detailed interpretations. It is a well-established fact that the human eye can differentiate about 1,000 times as many tints and shades of color as it can tints and shades of gray, characteristic of black-and-white photographs, and hence it may be concluded that color aerial photographs will permit a greater amount of detail to be recognized and interpreted. However, it is possible that two rock types of similar color might be differentiated more easily on certain black-and-white photographs than on color photographs because of mineralogic, chemical, or other differences that may permit significant contrasts in reflected light to be recorded when selected films and filters are used.

Petrusevich and Kazik (1955, p. 5, 8) reported that where color contrasts of rocks are not strong, boundaries between these rocks are more clearly seen on black-and-white photographs than on color photographs. Where color contrasts are strong, interpretation is facilitated in areas where individual beds are rather thick and the color of formations is retained for considerable distances along the strike. Petrusevich and Kazik (1955, p. 8) also reported that "A comparison of aerial color photographs of scales 1:15,000; 1:10,000; 1:8,000; and 1:5,000 for the same area, taken under the same conditions, shows that * * * the practical use of aerial color photography for geological purposes should be limited to a scale of 1:10,000 and larger." This conclusion was based on a study of photographs taken with an 8.25-inch lens. Recently developed short-focal-length lenses (3.5 inches and 6 inches) now permit useful color aerial photography to be achieved at a scale smaller than 1:10,000.

Aerial color negative film may prove particularly useful in photointerpretive studies. Unlike positive transparencies (reversible-type color film), which require use of filters during exposure of the film, negative-type color film is processed with filters inserted during the printing process. It is thus possible to vary the color contrasts through the simple medium of printing, with the possible advantages that certain features of geologic significance, such as alteration zones, may be emphasized. Petrusevich and Kazik (1955, p. 5) noted that a greater contrast often can be obtained in a black-and-white print from a color negative than in a print from the corresponding black-and-white negative. Fischer (1958, p. 546) in turn stated that black-and-white positive prints from Ektachrome aero positive transparencies also show stronger tone

contrasts between various rock units than the conventional black-and-white photographs.

TEXTURE

Texture was defined by Colwell (1952, p. 538) as "* * * the frequency of tone change within the image * * * [and] * * * is produced by an aggregate of unit features too small to be clearly discerned individually on the photograph." The scale of the photographs thus has an important bearing on this definition of texture. For example, a network of fine lines described as a texture on one scale of photographs may well be recognizable as a network of joints on a larger scale of photographs; this bears out Schulte's statement (1951, p. 697), made with regard to plant distribution, that at large scales photographic detail is more important, whereas at small scales tone becomes relatively more important. Such a texture, due to tone change within the image, may be called a "photographic texture" (figs. 43, 56, and 85). Photographic texture is therefore a comparative feature within any one general scale of photography. Although photographic tone is a fundamental element of photographic texture, the photographic conditions that affect tone may vary and yet permit such a texture to be a diagnostic recognition element. This is due to the fact that texture in the photographic sense is really a composite of several fundamental characteristics, namely photographic tone, shape, size, and pattern, and, of these elements, slight variations of tone would least significantly affect the recognition of a given texture.

Photographic textures have been described by various workers (Spurr, 1948; Raup and Denny, 1950) as coarse, fine, rough, and fluffy, but such descriptive terminology would seem to have very limited use unless accompanied by photographic illustrations. Furthermore, unless these descriptive terms are themselves clearly defined, comparisons of photographic textures with specific commonly known objects might be more useful. It may also be suggested that because photographic textures are normally considered as two dimensional, the use of a densitometer in conjunction with a coordinatograph-type instrument to determine tone changes per millimeter within the image might permit mathematical classification of such textures. However, such a classification might fail where a strong textural fabric prevailed, for two textures differing primarily because of shape or preferred orientations within the image might well be assigned to the same mathematical classification.

In addition to the use of the term "texture" as described above, texture has other meanings, as in reference to soils. The application of aerial photographs to soils and engineering geology studies has resulted in the introduction of "soil texture" in some photogeologic literature; the obvious distinction between photographic texture, which can be directly observed, and soil texture, which must be interpreted from other recognition elements, must of course be made. Texture also has been used in relation to the density of a drainage network; wide spacing of streams results in a "coarse" texture of drainage and close spacing of streams results in a "fine" texture of drainage (figs. 3, 42, 49, 51, 62, 63, 79, and 106). Unless quantitative meaning is given to drainage texture, the term must be used on a comparative basis within any one general scale of photography. Horton (1945, p. 283–284) defined drainage density in quantitative terms but little use has been made of this classification by geologists.

Topographic texture has been used to describe the degree of dissection of the land surface (see Smith, K. G., 1950, p. 655–668). Like texture of drainage, topographic texture may be described as fine or coarse (figs. 39, 51, 62, 75, and 106). Quantitative study of topographic texture, based on map study, has shown that the texture ratio, a mathematical expression of the dissection of the ground surface, bears a logarithmic function relation to drainage density (Smith, K. G., 1950, p. 667–668). Therefore, because drainage density can be determined readily, aerial photographs may be useful in a comparative study of erosional topographies.

When texture is used to designate drainage density or erosional characteristics of the terrain, rather than to designate a photographic texture, the use should be so qualified as to make the definition clear. Although textures are commonly considered in terms of the two-dimensional plan view, it is important to note that erosional texture may well be significant or at least more readily recognized when viewed from the third dimension of the stereoscopic model (see fig. 39).

PATTERN

Pattern, as used herein, refers to the orderly spatial arrangement of geologic, topographic, or vegetation features. The spatial arrangement of pattern is normally considered by interpreters to be a two-dimensional or plan-view arrangement of features, but it may also be a three-dimensional arrangement. If features that make up a pattern become too small to identify, as on small-scale photographs, they may then form a photographic texture.

Patterns resulting from particular distributions of gently curved or straight lines are common and are frequently of structural significance; they may represent faults, joints, dikes, or bedding. But a single line, or lineation, is also an illustration of pattern; it

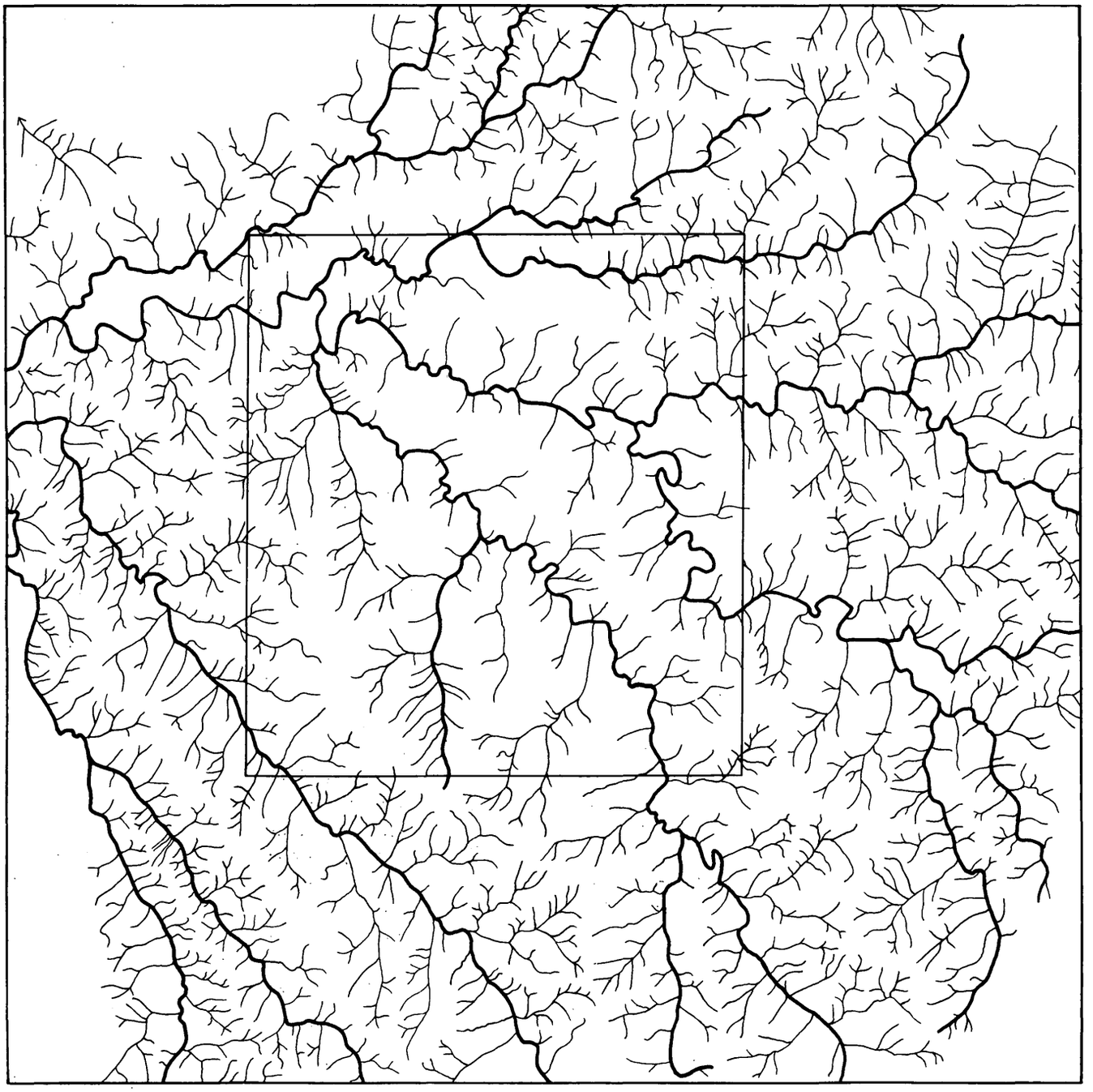


FIGURE 3.—Drainage map of large area in vicinity of ring dike shown in figure 54.

A separate tracing of drainage over a large area in the vicinity of the ring dike of figure 54 shows a marked decrease in drainage density within the ring-dike area. The contrast in drainage densities inside and outside of the ring dike is more readily seen on a separate tracing of drainage than in the stereoscopic model. (See also fig. 9.) Inset shows area of figure 54.

may result from an orderly arrangement of stream segments, trees, depressions, or other features (figs. 74 and 84). This arrangement may be a continuous alinement of geologic, topographic, or vegetation features, but more commonly it is a discontinuous alinement. Because lineations are especially important as expressions of fractures they may indicate areas of considerable economic significance.

Drainage patterns are an important element in geologic interpretation of aerial photographs (figs. 48, 94, and 96). In bedrock areas these patterns "* * * depend for the most part on the lithologic character of the underlying rocks, the attitude of these rock bodies * * * and the arrangement and spacing of the planes * * * of lithologic and structural weakness encountered by the runoff" (Tator, 1954, p. 412). Stream patterns thus reflect the control exerted by underlying structure and rock type. But stream characteristics may be influenced by thickness and kind of surficial material where structural control is at a minimum. Under these conditions the drainage may reflect differences in surficial materials that are significant to the engineering geologist. (See Belcher, 1945, 1948; Jenkins, Belcher, Greeg, and Woods, 1946; Frost, 1946; Frost and Woods, 1948; Hittle, 1949; and Parvis, 1947, 1950.) In areas where resistance to erosion may be more or less uniform, as in many surficial deposits or in bedrock without pronounced structure, the drainage pattern is commonly dendritic or modified dendritic (see figs. 70, 77, and 106). Where structures are well developed, as in folded mountains, characteristic trellis, annular, or other drainage patterns may develop (see fig. 64).

Because the sensitivity of drainage to strike and dip directions is pronounced, changes in a drainage pattern, or deviation from an established norm, may be as important or more important than interpretation of any one stream pattern. "It is therefore important that relatively large areas be examined so that local drainage patterns [or anomalies] may be readily differentiated from regional drainage patterns" (Alliger, 1955, p. 180). A change in drainage may thus have significant structural implications (see figs. 9, 94, and 96). But a difference in stream pattern may also suggest variations in lithologic character of the underlying rocks.

Patterns of vegetation are also commonly of geologic significance and may reflect structural conditions or lithologic character of rock types (see figs. 40, 43, 54, 72, and 85). Woolnough (1934a, p. 213) suggested that a distinction be made between two types of vegetation distribution which he called "blocks" and "alinements;" the former occurs on extensive outcrops of rock of uniform character, the latter along narrow rock bands, faults, or similar limited features. Alinements further may be subdivided as linear, parallel, and curved (see Woolnough, 1934a, p. 213). It is suggested that narrow linear or palallel alinements of vegetation may represent fractures (figs. 50, 60, 71, and 101), whereas wide, curved alinements may signify the distribution of outcrop of low, moderately or even steeply dipping beds (figs. 40 and 72); where curved alinements form closed loops they generally represent horizontal or nearly flat lying beds (figs. 61 and 77).

The term "pattern" has also been used in the literature in quite a different sense than described above. In the study of surficial materials the term "soil pattern" —a poorly chosen term—refers to the combination of surface expressions, such as landform, drainage characteristics, and vegetation, that are used in the interpretation of ground conditions (see p. 34–37). Thus pattern as defined above may be included as an element of the broad term "soil pattern," commonly used in engineering geology descriptions. Soil patterns may reveal information of direct use in engineering geology studies, as in the location of granular materials (figs. 52, 88, 104, and 108; and p. 34–37); in addition soil patterns may be important in suggesting the distribution of certain rock types; this distribution in turn may reflect geologic structures (see figs. 4, 48, and 81).

RELATION TO ASSOCIATED FEATURES

The relation of one feature to its surroundings is commonly important because a single feature by itself may not be distinctive enough to permit its identification. The significance of this relation may be spatial or genetic. For example, depressions may be identified as kettle holes because of their location near readily identified terminal moraines, and because of their genetic association with glaciated terrain. With regard to spatial association this recognition element has also been called the "site factor" (Colwell, 1952, p. 540); it may be particularly useful in determining the significance of vegetation with respect to the underlying geology. For example, certain tree groups growing on topographically high areas in interior Alaska suggest well-drained underlying materials. The landform, especially, in combination with the vegetation characteristics suggests stabilized sand dunes (fig. 56). The relation of associated features may thus permit specific identifications and inferences concerning surficial materials or rock types.

Photograph scale may be important in the interpretation of associated features; that is, a geologic feature on small-scale photographs may be interpreted because of its position with regard to other features,

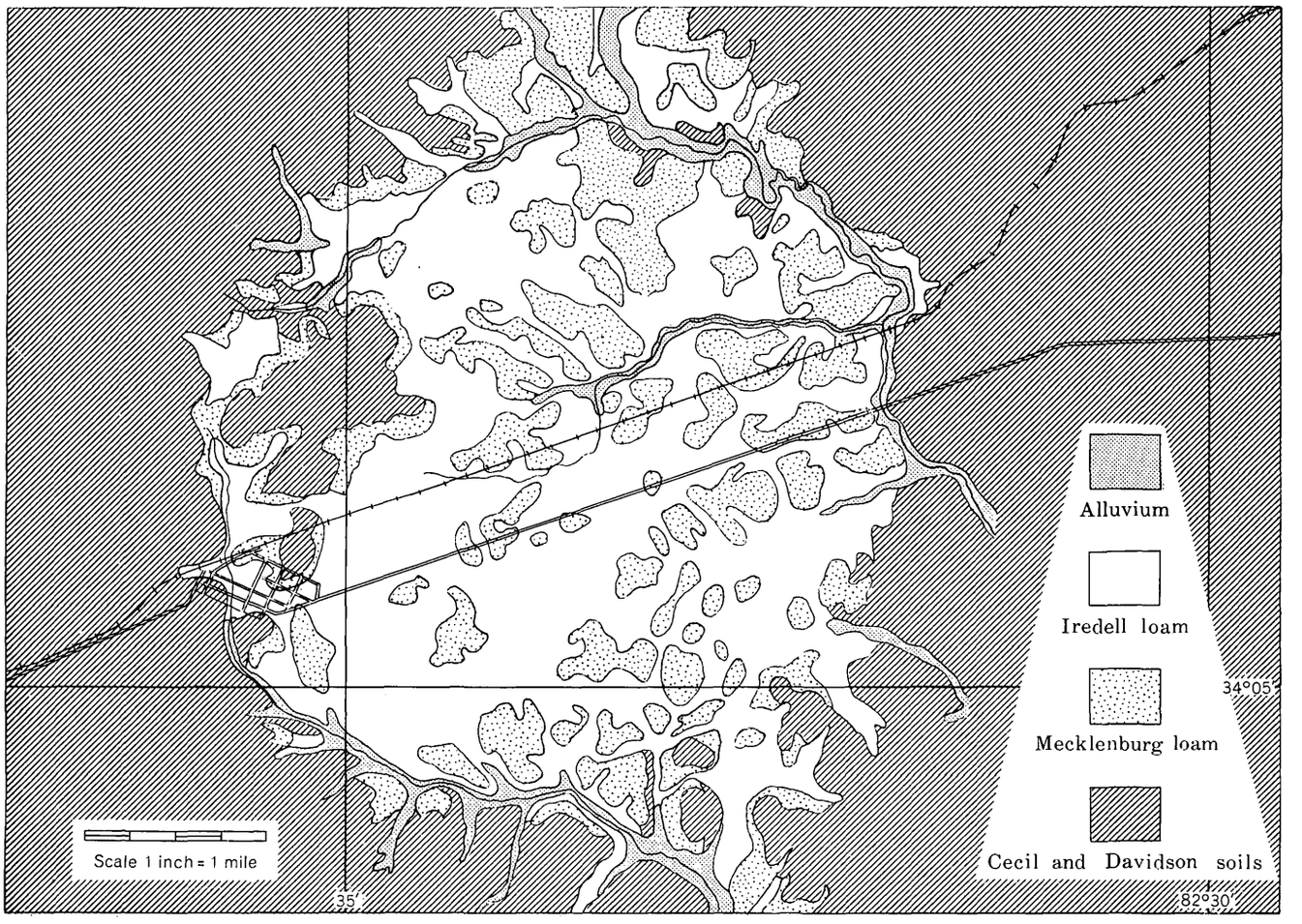


FIGURE 4.—Generalized soil map of area shown in figure 48 (modified from soil survey map of Abbeville County, South Carolina).

The circular area underlain by Mecklenburg loam and Iredell loam is conspicuous. These soils delimit an area of mafic intrusive rocks from a surrounding area of silicic rock types. Particularly where outcrops are sparse or lacking, soil maps may provide significant geologic information, especially in areas of residual soils. The soil maps may provide structural or lithologic data with respect to underlying rocks, or they may provide pedologic data concerning the surficial materials that is useful to the engineering geologist.

all of which can be seen at the same time (fig. 55), whereas on large-scale photographs direct identification might be made because photographic details are visible. The usefulness of association as a recognition element also will vary not only with photograph scale but with the objective of the study. The engineering geologist may be confronted with the immediate identification and location of kames as a source of gravel near a proposed highway route, whereas the geologist mapping the entire area would be interested in the identification, orientation, and distribution of all kames, with respect to geologic history of the area.

SHAPE

Shape as a recognition element in geologic interpretation is significant primarily only in its broadest definition, which involves relief or topographic expression. In this regard shape is very important in recognizing constructional landforms, such as volcanic cones, sand dunes, river terraces, and certain glacial features (figs. 41, 55–58, 60, and 104); it is also useful in differentiating rock units where one formation is expressed in bold cliffs and overlies a second formation that shows a lesser angle of slope (figs. 62, 84, and 91), or where adjacent rocks show significant differences in topographic relief (fig. 65). Rectilinear depressions may be expressions of faults (figs. 60, 85, 86, 99, and 103). The general surface configuration, as in the "beehive" weathering of some massive sandstones, also may be regarded as an expression of shape that is useful in recognition. According to Belcher (1945, p. 140–141)

shapes of gully cross sections are important to the interpretation of surficial materials for engineering purposes. However, in its strictest definition, as "a spatial form with respect to a relatively constant contour or periphery" (Webster's New International Dictionary, 1950) shape has been of little importance as a recognition element because nature may reveal the same geologic feature in an infinite number of different shapes, and because common scales of photography (1:20,000) restrict an interpreter's ability to see details of shape. Where local field criteria have been established, shape may be useful, for example, in the interpretation of patterned areas (fig. 53) or in the study of gully cross sections, particularly when large-scale photographs are available (fig. 88).

Shadow as a recognition element is primarily a use of shape and photographic tone. Because vertical aerial photographs are commonly used for interpretation, shadows may permit an effective side view of some features. For example, shadows may be useful in interpreting tree types, such as conifers, which generally have pointed tops; the type of tree in turn may have a relation to underlying geologic materials and particularly to soil-moisture conditions (Stoeckeler, 1952, p. 4). For interpreting most natural features, however, the shape of shadows probably contributes little in direct identification. Insofar as shadows contribute to textures and patterns, they are of course of great importance. Even slight topographic breaks may be accentuated by shadows (figs. 88 and 97).

SIZE

The quantitative element of size, as it relates to surface or volume dimensions of an object, has been little used in recognition of geologic features from aerial photographs, although relative size has been useful as an interpretation aid. Size as an interpretation element is being used increasingly with the adoption of photogrammetry as a fundamental part of photogeology; it is most appropriately considered in relation to interpretations based on thickness of strata, amount of offset along faults, or other finite measurements (see p. 56–63). Geologically significant measurements may be directly related to topographic expression; that is, measurements between topographic positions may yield direct information such as stratigraphic thickness. But generally other influencing factors, such as dip of beds or other structural elements, must be considered just as in field measurement (see p. 56–58). If the thickness of a formation is known, it may aid in location of formation contacts on aerial photographs, because measurements may be made from known points that would permit the positioning of the obscured contacts (fig. 39); or it may aid in correlation of beds across fault zones. Determining the range of thicknesses over a broad area may be essential to understanding the regional geology of that area (see p. 59–60).

Studies in quantitative geomorphology suggest that size, in terms of finite measurements, may be an extremely important parameter of geologic interpretation of aerial photographs. Measurement of geologic data can be expected to become an even more important part of photogeology in the future as techniques of quantifying geologic information become more widely used.

COMBINATIONS OF RECOGNITION ELEMENTS

The usefulness of recognition elements, of course, is enhanced where they may be used in combination. Indeed, photographic tone, useful alone as a recognition factor under some conditions, is a fundamental photographic characteristic without which there could be no recognition elements at all on black-and-white photographs. As mutually supporting recognition elements an association of photographic tone, topographic expression, and texture may permit the interpretation of bedding, even in areas of sparse or no outcrops (fig. 40). Faults are commonly expressed as straight or gently curved lines; they may be further identified by an abrupt photographic tone change on opposite sides of these lines as well as by a pronounced offset of recognizable rock types (fig. 83). Surficial materials are commonly identified on the combined basis of stream patterns, shapes of gully cross sections, texture, and photographic tone as well as by their relation to associated features (see p. 34–37).

VERTICAL EXAGGERATION

In addition to those recognition elements that are based on factors, such as film and filter used and processing, that directly affect the photographic image, certain other factors are important in interpretation. Especially significant is vertical exaggeration—the exaggeration of vertical distances with respect to horizontal distances—which is characteristic of almost all stereoscopic models; this exaggeration makes slopes appear steeper than they are and objects seem taller than they are. Vertical exaggeration is generally present not only in viewing stereoscopic models formed from paper prints but also in viewing projected stereoscopic models formed from glass-plate diapositives in double-projection instruments.

An understanding of vertical exaggeration is fundamental in the study of stereoscopic models, not only because of the exaggerated heights and the somewhat unnatural view that results, but because in many geologic problems the interpreter relies on visual dip

estimations rather than on any measuring devices (see p. 64). The amount of exaggeration of a dip angle in a stereoscopic model is fundamentally related to the tangent of the dip angle; that is, in a stereoscopic model exaggerated 3 times, for example, any true dip angle would be exaggerated to an angle whose tangent function was equal to 3 times the tangent of true dip. Exaggeration of low dips is generally an aid in structural interpretation and in detecting tilt from aerial photographs.

Minor topographic differences, which may reflect underlying geologic structure, are also exaggerated and in turn easily recognized (figs. 40, 88, and 97). The exaggeration of relief in a stereoscopic model of 1:20,000-scale photographs taken with a 6-inch-focal-length lens commonly permits an interpreter to distinguish differences in altitude as small as 1 foot. As a consequence vertical exaggeration then is most important where small but significant differences in altitude may be present in the stereoscopic model.

Vertical exaggeration results from the wide spacing of the camera positions at the time of exposure, as contrasted to the spacing of the human eyes with respect to normal viewing arrangement in examining stereoscopic models. Vertical exaggeration in normal viewing arrangement is fundamentally related to base-height ratio, which is the ratio of the air base distance to the flying height (see fig. 1). As this ratio increases, vertical exaggeration increases. Thus the greater the distance between camera stations (equivalent to air base distance), flying height remaining constant, the greater is the vertical exaggeration. The resulting photographs will have an increasingly smaller overlap area and consequently a lesser area within the stereoscopic model. It should be noted, however, that in normal photographing procedure when flying height is increased for any given focal-length lens, the air base distance is also increased so that a relatively constant base-height ratio is maintained. Under these conditions vertical exaggeration is not affected by flying height. When the base-height ratio is increased through the use of short-focal-length lenses, vertical exaggeration will also increase, the photographs taken with the shorter focal-length lens showing the greater exaggeration. Effective vertical exaggeration may also be increased by moving the two photographs farther apart at the time of viewing, or by increasing the viewing distance.

SCALE OF PHOTOGRAPHS

Small-scale photographs may be advantageous for interpreting some geologic terrains, particularly where reconnaissance information is desired. Small-scale photographs are normally taken at relatively high altitudes and have scales of 1:60,000 or smaller; their usefulness results chiefly from showing a large area in a single view (approximately 80 square miles on a single photograph having a scale of 1:60,000), which may reveal overall relations, as in geologic structures, drainage patterns, or other features, that could not be readily seen otherwise (figs. 48 and 55). Photomosaics commonly serve this same purpose (fig. 96). The association of features over a large area provided by the small scale is the significant factor to be considered. However, the reduction in image size due to high flying heights or short-focal-length lenses may be detrimental to the identification of some features, and hence make such photographs of little use for some interpretation problems. For example, details of jointing may be entirely lost on small-scale photographs. Also, use of small-scale photographs obtained by using extremely short-focal-length lenses, that is, 2 inches or shorter, may be undesirable, especially in areas of moderate to high relief, because many topographically low areas will be masked from view. Nevertheless, small-scale photographs have definite advantages in qualitative interpretation (Hemphill, 1958b) and may be especially useful if employed in conjunction with large-scale photographs or with instruments that enlarge the photography scale (see p. 47). Where quantitative study is involved, small-scale photographs are advantageous in that less control is needed within a given area than with large-scale photographs; but this advantage may be offset by the decrease in the reliability of measurements (see p. 72–74).

PHOTOGEOLOGY IN GEOLOGIC MAPPING

In geologic mapping maximum use of aerial photographs is attained by closely integrating field and photogeologic studies. It generally is desirable to precede the field phase of geologic study by a study of aerial photographs, which should include the compilation of a preliminary map on which all interpretations, however reliable or questionable, have been noted. Such a preliminary photogeologic study affords several advantages: it may point out areas that must be mapped primarily by field methods; it may eliminate or reduce extensive field surveys in certain areas; it may direct attention to anomalous areas where detailed field study is particularly warranted; and it commonly provides a basis for organizing the geologic plan of field study. In addition, attention is directed to those areas where field study will most likely result in establishing criteria that will permit a refinement of further photogeologic mapping. Also, a preliminary study of photographs gives a geographic familiarity of the area

that would be useful in choosing camp sites, routes of traverse, and optimum locations of instrument survey stations.

Continuing use of aerial photographs during the field phase of geologic study permits a firsthand correlation of geologic features and photographic images, which corroborates or refutes preliminary interpretations and provides information for subsequent detailed photointerpretive study. Refinements in interpretation may be made in the field or in a followup photogeologic study.

The delineation of rock types and structures from aerial photographs may involve mere observation; or more commonly interpretation is involved. In some areas it is possible only to map similar photographic units, as no diagnostic or suggestive criteria as to rock type may be present. Such areas are usually poorly exposed because of heavy vegetation or surficial debris; relief may be very low. But in other areas, where wide expanses of rock crop out, specific formations or rock types may be easily delimited on the photographs; thus much of the routine work of mapping geologic contacts, as well as determining structural measurements, can be accomplished readily by photogeologic methods. Where geologic structures are small and complex, aerial photographs may provide only limited information as contrasted to areas where geologic structures are large and simple. Depending chiefly on factors related to geologic environment, climate, and erosional cycle, the extent to which photogeologic methods can be applied thus may vary widely.

KINDS AND AMOUNTS OF INFORMATION

Geologic information that can be interpreted from aerial photographs may be grouped broadly into two categories: lithologic and structural. In general or reconnaissance mapping the geologist is interested largely in determining the distribution of rock units, including surficial deposits, and in delineating geologic structures. Special studies may require a more rigorous application of photogeologic procedures, which includes quantitative as well as qualitative study of the stereoscopic models. But regardless of the objective of a particular study, the kinds and amounts of geologic information available from aerial photographs will depend primary on the type of terrain—whether igneous, metamorphic, or sedimentary—, the climatic environment, and stage of the geomorphic cycle.

It is generally believed that sedimentary rock areas will yield more information from aerial photographs than igneous rock areas, and that regions underlain by metamorphic rocks will reveal the least information. Putnam stated (1947, p. 560, 562) that "* * * geologic features * * * tend to be more recognizable where strong differences exist in the erosional resistance of adjacent rocks. Thus, sedimentary rocks, as sandstone, shale, and limestone, are likely to be more apparent than relatively homogeneous rocks like granite, especially if the sedimentary rocks have a moderate dip." Bentor (1952, p. 162), based on his work in Israel, was of the opinion that "As a whole, air-photographs are much less useful in regions of crystalline rocks than in those composed of sedimentary formations." With regard to igneous and metamorphic terrains, which are generally believed to be more difficult to interpret than sedimentary terrains, Melton (1956, p. 57) concluded that "Discovery of hitherto unknown or abnormal structures and [mineral] deposits, rather than detailed mapping, will probably be the most rewarding use of aerial photographs * * *."

Except for high mountainous areas where vegetative growth is restricted by altitude, arid and semiarid regions generally will have the largest areas of rock outcrop, and tropical regions the least; hence the arid and semiarid regions may be expected to yield the greatest amount of geologic information from aerial photographs. In addition to relatively wide areas of rock exposure, the arid and semiarid regions may be expected to show a greater number of significant plant-rock associations than other climatic areas, because weathered material in the arid and semiarid regions is not excessively leached and a close relation of soil to parent formation therefore persists. Where this close association of parent rock and residual soils exists the distribution of different vegetation, reflecting the effect of bedrock on the composition of the soils, may facilitate the mapping of different rock types (see Levings, 1944, p. 27–30). In areas of much precipitation, under temperate or tropical climatic conditions, soils tends to be leached of salts, and there is a further tendency for soils from different parent formations to become more similar at maturity (Murray, 1955, p. 104). Murray stated (1955, p. 104) that under tropical conditions where rainfall is abundant, the ratios of potassium, sodium, and calcium to aluminum, which are widely different in silicic and mafic rocks, become smaller on weathering and are nearly equal in mature soils. Thus differences in vegetation as related to specific formations might be less well developed in tropical areas, except for those plant associations that may depend primarily on physical characteristics of the soil rather than chemical. Grantham (1953, p. 329) noted that in semiarid areas of Africa the soils reflect geology through vegetation differences more strongly than in wet temperate areas.

Sedimentary terrains yield a greater amount of lithologic and structural information than igneous and metamorphic areas because of the generally nonhomogeneous nature of sedimentary terrain, which results in marked differential erosion characteristics that stand out on aerial photographs. Sedimentary rocks of strongly differing physical characteristics commonly crop out within short distances whereas plutonic rocks, particularly, are likely to be relatively homogeneous over wide areas. Locally, diagnostic landforms, such as volcanic cones, may be important in study of igneous terrains, especially where extrusive rocks prevail. Metamorphic terrains, on the other hand, may reveal the least amount of information from aerial photographs because of the very nature of the metamorphic processes, which tend to destroy the erosional and landform characteristics of sedimentary and igneous rocks from which the metamorphic rocks are derived.

In any area where vegetative cover is dense and where surficial debris is widespread, aerial photographs generally can be expected to yield more structural information than lithologic information. The amount of structural information in turn generally will be greater, for any one type of terrain and climatic environment, during the mature stage of the geomorphic cycle, at which time streams show their greatest adjustment to and reflection of structure, and at which time a greater third dimension of the terrain is visible for study in the stereoscopic model. Where the lithologic character of rocks is interpreted on geomorphic or landform expression, maturely dissected areas may reveal the greatest amount of information.

Although the extent to which photogeologic procedures contribute to the geologic mapping of an area depends on the climatic and geologic environment, as well as the stage of the erosional cycle, some generalizations may be stated with regard to differentiating and interpreting sedimentary, igneous, and metamorphic terrains. These generalizations are grouped into two categories: lithologic character of rocks and geologic structure.

LITHOLOGIC CHARACTER OF ROCKS

SEDIMENTARY ROCKS

Consolidated.—The presence of bedding in most sedimentary rocks is fundamental to their interpretation from aerial photographs. Because of differential resistance to erosion of sedimentary beds the typical banded patterns of these rocks are seen on aerial photographs. This is a result of what Rich (1951, p. 189) termed the "etching concept" wherein more resistant beds are brought into relief and less resistant beds lowered as a result of weathering and removal of materials largely by sheet wash and creep (figs. 87, 91, and 97). Back slopes of steeply dipping beds, especially, may contrast strongly because they commonly expose to erosion within a given area a wider variety of lithologic types than dip slopes of gently dipping beds. Although topographic expression is thus important in recognition of bedding, banding due to vegetation or soil differences, expressed by photographic tone may likewise delineate beds, in absence of topographic expression or in combination with it (figs. 40 and 81). Bedding is especially prominent in the mature stage of the geomorphic cycle, particularly in terrain underlain by interbedded hard and soft sedimentary rocks that are tilted. However, bedding may be masked by the massive character of some sedimentary rocks, such as certain sandstones, in which case the sedimentary rocks may appear to be homogeneous and similar to some metamorphic rocks or intrusive igneous rocks as seen on aerial photographs (contrast figs. 71 and 92). A notable exception is massive limestone in which sinkholes have developed (fig. 68).

As seen on aerial photographs shales and similar fine-grained sedimentary rocks tend to have relatively dark photographic tones, a fine-textured drainage, and relatively closely and regularly spaced joints (figs. 49, 62, 63, and 91). Coarse-grained clastic rocks, in contrast, tend to have relatively light photographic tones, a coarse-textured drainage, and relatively widely and regularly spaced joints (figs. 42, 91, and 92). These generalizations are probably most applicable to marine sedimentary rocks. However, some fine-grained clastic rocks may be light toned and some coarse-grained sedimentary rocks, such as the continental red beds, may be dark colored rather than light colored and be expressed as relatively dark photographic tones on aerial photographs. Drainage density in a given climatic area is related primarily to resistance of a rock to erosion; drainage density increases with decrease of resistance to erosion. Resistance to erosion in turn is fundamentally related to permeability; generally resistance to erosion is less in rocks of low permeability. Hence, fine-grained clastic rocks commonly have a fine-textured drainage (fig. 79).

Physico-chemical precipitates are in many places closely associated with fine-grained clastic sedimentary rocks; where these rocks are interbedded the drainage texture and joint pattern both may be fine, as with fine-grained clastic rocks alone, but photographic tone of physico-chemical precipitates may commonly be relatively light, as with some fresh-water limestone, rather than dark, despite the fine grain size.

Although fine-textured drainage commonly characterizes nonresistant fine-grained sedimentary rocks and coarse-textured drainage suggests resistant coarse-grained sedimentary rocks, drainage is probably more significant as an indicator of structure than it is of lithology. Drainage characteristics may suggest broad rock groupings, but no one drainage pattern is diagnostic of sedimentary rocks, although annular and trellis drainage generally suggest sedimentary rocks or close metamorphic equivalents. The association of specific drainage characteristics with rocks of certain lithologic or physical characteristics presents an interesting field of study; quantitative study of stream data measureable from aerial photographs, such as drainage density, may indicate certain drainage-lithology relations.

The type of vegetation may be useful in differentiating specific rock types (see figs. 43 and 61). Hemming (1937) noted that striking vegetation differences were exhibited by limestone and quartzite in northern Rhodesia where the trees *Acacia* and *Albizzia* grew on limestone and *Brachystegia* and *Isoberlinia* grew on quartzite.

Unconsolidated.—Most surficial deposits—the unconsolidated sedimentary rocks—are readily distinguished on aerial photographs from consolidated rock types, although thin veneers of surficial material may be difficult to identify. Many recognition criteria are used in identifying and interpreting surficial deposits from aerial photographs, but the most significant criterion is probably landform. Landform is significant because many surficial deposits, particularly those useful to the engineering geologist, are transported materials that have diagnostic topographic form. The importance of landform is seen in the identification of sand dunes, eskers, kames, alluvial fans, river terraces, and similar constructional geologic features (figs. 52, 55, 56, 58, and 104). On the other hand extensive deposits of surficial debris, such as the drift plains of north-central United States, may show little or no diagnostic landform, but their general makeup may be inferred from drainage characteristics, photographic tone, analysis of slope, and related criteria (fig. 107). These criteria are discussed more fully under uses of aerial photographs in engineering geology studies (p. 33–37).

IGNEOUS ROCKS

Extrusive rocks.—Extrusive igneous rocks commonly have diagnostic landforms (figs. 41, 60, and 76) in contrast to the intrusive igneous rocks, which are revealed on aerial photographs primarily by other recognition features such as drainage, texture, massive character of the rock, and crosscutting association with country rocks.

In addition to landform certain other criteria may be useful in identifying extrusive rocks, if the terrain is relatively undeformed. The structural relation of flows to associated rocks, for example, may be diagnostic in little-deformed areas, but where flows have been strongly tilted, folded, or otherwise disturbed, recognition and interpretation from aerial photographs may be extremely difficult or impossible. Only those relatively undeformed flows, mainly of Tertiary age and younger, are readily identified from aerial photographs without some knowledge from ground surveys. The ground plan of flows showing lobate patterns of vegetation and topography, especially at the terminations of suspected flows, is commonly diagnostic (figs. 76, 85, and 113), and association with volcanic cones makes misinterpretation difficult (figs. 41, 60, and 76). Locally flow channels may be visible. The surface of a flow may be rather hummocky and irregular, in contrast to surfaces of sedimentary strata, and where several flows have piled up, present topography may show several terracelike forms with irregular surfaces. The unconformable contact between flows and underlying rocks may aid in recognizing extrusive rocks (fig. 87), and where flows cascade down over older topography their identity is obvious (fig. 60). The basaltic or mafic flows may show dark photographic tones on conventional photographs, particularly in well-exposed areas, whereas rhyolitic or silicic flows may have light photographic tones. Locally distinctive patterns are present on mafic flows (fig. 53), and in some areas erosional characteristics permit differentiation of flows and associated rocks (fig. 69).

Where flows have been extruded over deformed igneous and metamorphic terrains, a low-dipping surface associated with lobate patterns of vegetation and topography is suggestive of extrusive rocks, and in some areas faults in the underlying rocks are seen to terminate abruptly at the edge of a lava flow (fig. 85).

Intrusive rocks.—Intrusive igneous rocks have a wide variety of structural relations to surrounding rocks that commonly aid in their identification from aerial photographs. Dikes may be revealed on aerial photographs as rectilinear or curved ridges that stand up because of greater resistance to erosion than surrounding rocks (figs. 81, 82, 87 and 90); they may also contrast in photographic tone with the surrounding rocks either because of the difference in rock types (fig. 90), or because of distinctive vegetation that covers dikes in some areas (Mogg, 1930, p. 662 and 668, pl. 5). Dikes may follow fractures in other igneous rocks and contrast in photographic tone with the host

rock. Where dikes are less resistant than the country rock, they may be expressed as rectilinear depressions that appear similar to fault expressions.

Because sills occur parallel to bedding in sedimentary rocks, they may be difficult to interpret as igneous from aerial photographs, even though strong tonal contrasts of the sills and sedimentary rocks are present. Mogg (1930, p. 656) pointed out that the diabases of Pretoria, South Africa, although relatively hard rocks, weather easily to deep soils that support distinctive deep-rooted vegetation, but the vegetation type differs from area to area. The tree *Kirkia wilmsii* grows conspicuously and exclusively on diabase sheets in the sedimentary rocks of the Pyramid Hills area of Pretoria (Mogg, 1930, p. 658), but in the Magaliesberg area *Acacia caffra* characteristically marks the diabase (Mogg, 1930, p. 662). Vegetation thus may be important locally as an indicator of rock types, but commonly it must be interpreted with caution because the same rock type may carry a different flora in different areas.

Igneous plugs, laccoliths, stocks, and batholiths, by nature of their mode of origin, commonly tilt the sedimentary rocks which they intrude, and in areas where plutonic rocks are exposed the pattern of dips in surrounding rocks may support other criteria suggestive of igneous rocks. Domal areas due to intrusion may also be reflected in radial drainage patterns (fig. 48), just as are certain folds in sedimentary rocks. But if areas of plutonic rocks are large, the characteristic homogeneous nature of such rocks may result in a dendritic drainage pattern, unless drainage is controlled by a fracture system (figs. 51, 70, 71, and 86). Because of the generally homogeneous nature of plutonic rocks as contrasted to sedimentary rocks they will have a massive appearance on aerial photographs, and banding typical of sedimentary and some metamorphic rocks will generally be lacking (figs. 59, 70, and 71). Also because of the homogeneous character of many igneous bodies, elements essential to plant growth may be distributed more or less uniformly throughout the mass (Murray, 1955, p. 103) and significant differences in vegetation can be expected to be absent from any one plutonic rock mass (fig. 70), except for those differences controlled by altitude or by structural conditions, such as faults that may trap an abundance of moisture (fig. 71).

In addition, topographic and erosional characteristics may aid in the interpretation of some igneous terrains. Granite at low altitudes in some tropical areas is expressed in hummocky, rounded topography on which a uniform type of vegetation is present; dendritic drainage may characterize this terrain. Similar rounded topography may also be present at high altitudes, but where glaciers have been active all rocks may stand out in sharply angular topography. Regardless of surface expression, however, a crisscross pattern of joints, nearly always present in igneous rocks, commonly can be seen not only in the well-exposed areas (see figs. 70, 71, 100, and 103) but also in many vegetation-covered areas (fig. 72). Topographic expression of most plutonic rocks, as with other rock types, is dependent in large part on climate and stage of the erosional cycle, although within an area underlain by different igneous rock types difference in resistance to erosion may be significant and specific rocks may stand topographically high (see fig. 82). The homogeneous character of many intrustive rocks and characteristic jointing, on the other hand, are related primarily to the rock type and its mode of occurrence, and are independent of climate and erosional cycle.

METAMORPHIC ROCKS

The identification and interpretation of metamorphic rocks from aerial photographs is commonly difficult because large-scale distinguishing characteristics are generally lacking. Bedding, so necessary to structural interpretation, may be difficult or impossible to recognize because of physical changes brought about by metamorphism, including the superposition of metamorphic structures of small scale. Indeed, many structural trends that can be interpreted from aerial photographs represent foliation rather than bedding (figs. 73 and 74). Where exposures are good, differences in photographic tone offer the best clue to recognition of bedding, especially where the metamorphic rocks are derived from thin-bedded sedimentary rocks of contrasting lithologic makeup (fig. 103). Thick formations of quartzite and marble might readily retain the photographic characteristics of the original sedimentary beds, however, because the metamorphic changes of induration of sandstone and recrystallization of limestone would likely have little effect on the gross physical appearance of these rock types as seen on aerial photographs. It is possible, however, that talus from quartzite ledges might take the form of large blocks in contrast to smaller chunks of rubble at the base of sandstone cliffs. The preference of vegetation for one rock type such as limestone, as a result of its chemical makeup, might well persist, even if the formation were metamorphosed to marble; but vegetation that might show a preference for sandstone because of its physical makeup, especially its high porosity, might well be lacking on its metamorphic equivalent, quartzite.

Strong parallel alinements of ridges and intervening low areas may be due to regional cleavage, foliation,

or fold axes, and thus the "topographic grain" of an area may suggest underlying metamorphic rocks (figs. 73, 76, 100, and 102), but in glaciated areas this evidence must be used with caution (fig. 67). In an area where a pronounced regional trend, or "topographic grain," is shown on the aerial photographs, the likelihood that metamorphic rocks are present is supported by the occurrence of widely spaced lineations at right angles to the regional trend. These lineations commonly represent regional cross joints and may be reflected in abrupt deflections of drainage along conspicuous straight stream segments of major streams (fig. 74) or in the development of tributary streams along these joints (figs. 73–75). Where bedrock is well exposed the profuse fractures in certain metamorphic rocks may be visible (figs. 46 and 99). Cady (1945) pointed out that in some areas in central Alaska talus slopes are developed much more extensively where the peaks are of metamorphic rocks rather than of granitic rocks; this distinguishes these two rock types locally (fig. 103).

STRUCTURE

FLAT-LYING BEDS

Flat-lying or nearly horizontal beds are most easily recognized where different sedimentary rock types exhibit contrasting photographic tones expressed as bands that extend along the topographic contour (figs. 77 and 78). Where both resistant and nonresistant rocks are present slope characteristics commonly are suggestive of horizontal strata—the resistant rocks have steep slopes or vertical cliffs, and the nonresistant rocks have a lesser angle of slope; the significant changes in slope between two beds extend generally along the topographic contour (figs. 77 and 78). Photographic tone and slope characteristics are associated in many places as mutually supporting evidence of flat-lying beds.

Because of the uniform resistance of one rock type to erosion, particularly in a horizontal direction, the drainage on flat-lying beds is generally dendritic unless controlled by joints or faults (figs. 42, 61, and 77). However, dendritic drainage alone, although suggestive, is not necessarily diagnostic of flat-lying sedimentary rocks; other rock types, such as granite, also may be uniformly resistant to erosion and may also exhibit dendritic drainage.

DIPPING BEDS

Numerous expressions of dip of sedimentary beds may be seen on aerial photographs. Dip direction is readily apparent where topographic surfaces coincide with bedding surfaces (figs. 87, 90, 92). Even in heavily vegetated areas the direction of dip commonly stands out as a result of the overall view afforded by the aerial photograph, which shows the tree crowns to fall in a dipping plane (fig. 89). In those areas where dips are very low, the aerial photographs are advantageous, if the beds are clearly expressed, because vertical exaggeration, which is present in most stereoscopic models, permits low dips to be readily interpreted (see fig. 91 and p. 64). The degree of dip may be estimated from the stereoscopic model by experienced photointerpreters or it may be measured photogrammetrically.

Where bedding is expressed by bands of differing photographic tone or by topographic breaks in slope due to resistance of beds, the rule of V's may be applied to determine the direction of dip; that is, where the trace of a bed intersects a stream valley a V in the outcrop pattern will point in the direction of dip (figs. 80, 81, and 98) unless the direction of dip and direction of streamflow are the same and the stream has a gradient greater than the amount of dip (fig. 59).

In many areas, particularly those of low relief, where beds are obscured by surficial materials or vegetation the direction of dip may be inferred from drainage characteristics. Where dips are gentle the relatively long tributary streams commonly flow down the dip slopes (Lattman, 1954, p. 361–365), whereas short tributary streams will characterize back slopes (figs. 5, 7, and 74). It is interesting to note that the relation of short and long tributary streams may be reversed where dips are steep, that is, about 45° or more (fig. 6). Other photorecognition criteria, such as distribution of photographic tones, should be sought to indicate whether dips are gentle or steep; or scattered field observations may provide sufficient information for making an analysis of dip direction based on stream characteristics. In such an analysis it may be desirable to trace all streams, however small, on a separate overlay (fig. 7). This is best done from the stereoscopic model. Exact positioning of tributaries is not essential to this technique of determining dip direction, but lengths of tributaries must be sketched carefully as the length relations of updip to downdip tributaries is significant. Viewing the stereoscopic model pseudoscopically (fig. 95) may be helpful in delineating the drainage.

FOLDS

Folds are commonly expressed as obvious features on aerial photographs especially where a fold is shown in its entirety within a single view and an orderly structural arrangement of beds is discernible (fig. 90) or where erosion has exposed a cross section of the

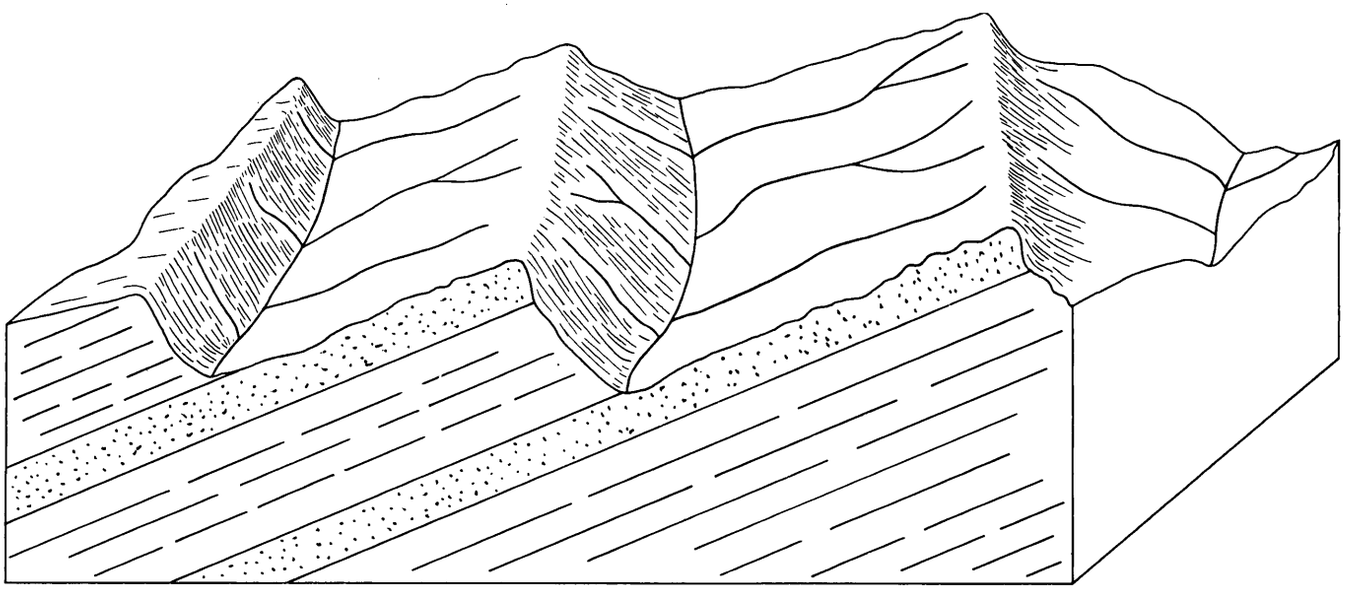


FIGURE 5.—Sketch showing long tributary streams on updip side of strike valley in area of low dips.

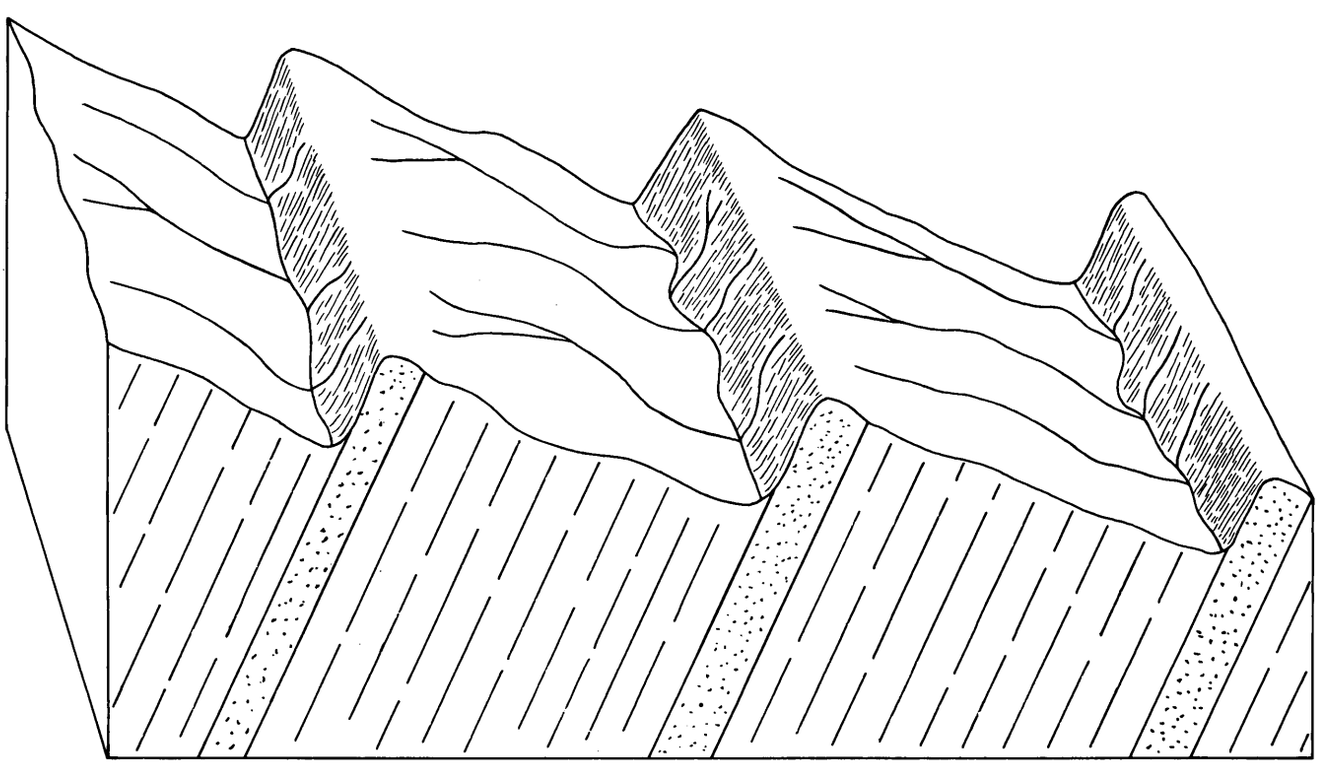


FIGURE 6.—Sketch showing long tributary streams on downdip side of strike valley in area of steep dips.

structure (fig. 91). Drainage characteristics may also aid in recognizing and delimiting the fold. Wengerd (1947, p. 596) noted that in parts of northern Alaska streams flowing in synclinal valleys were sluggish and meandering, and had low banks and swampy border areas with meandering tributaries; in contrast, streams flowing in anticlinal valleys were steep walled and less meandering. Wengerd also noted that dip slopes and back slopes in some areas commonly exhibited different drainage densities (fig. 79).

Where folds are plunging, major streams commonly curve around the nose of the fold; the convex side of the curve indicates the direction of plunge of anticlinal folds (figs. 81, 89, and 90). However, in areas where relief is low or bedrock is obscured by vegetation or surficial materials, drainage patterns or drainage anomalies may be the primary expression of folds (see figs. 9, 94, and 96; and p. 26–27). Drainage patterns or anomalies generally are best seen on small-scale photographs or mosaics where segments of streams combine to form significant patterns when observed in a single view (fig. 96). The significance of drainage characteristics may not be immediately apparent when large-scale photographs are viewed.

FAULTS

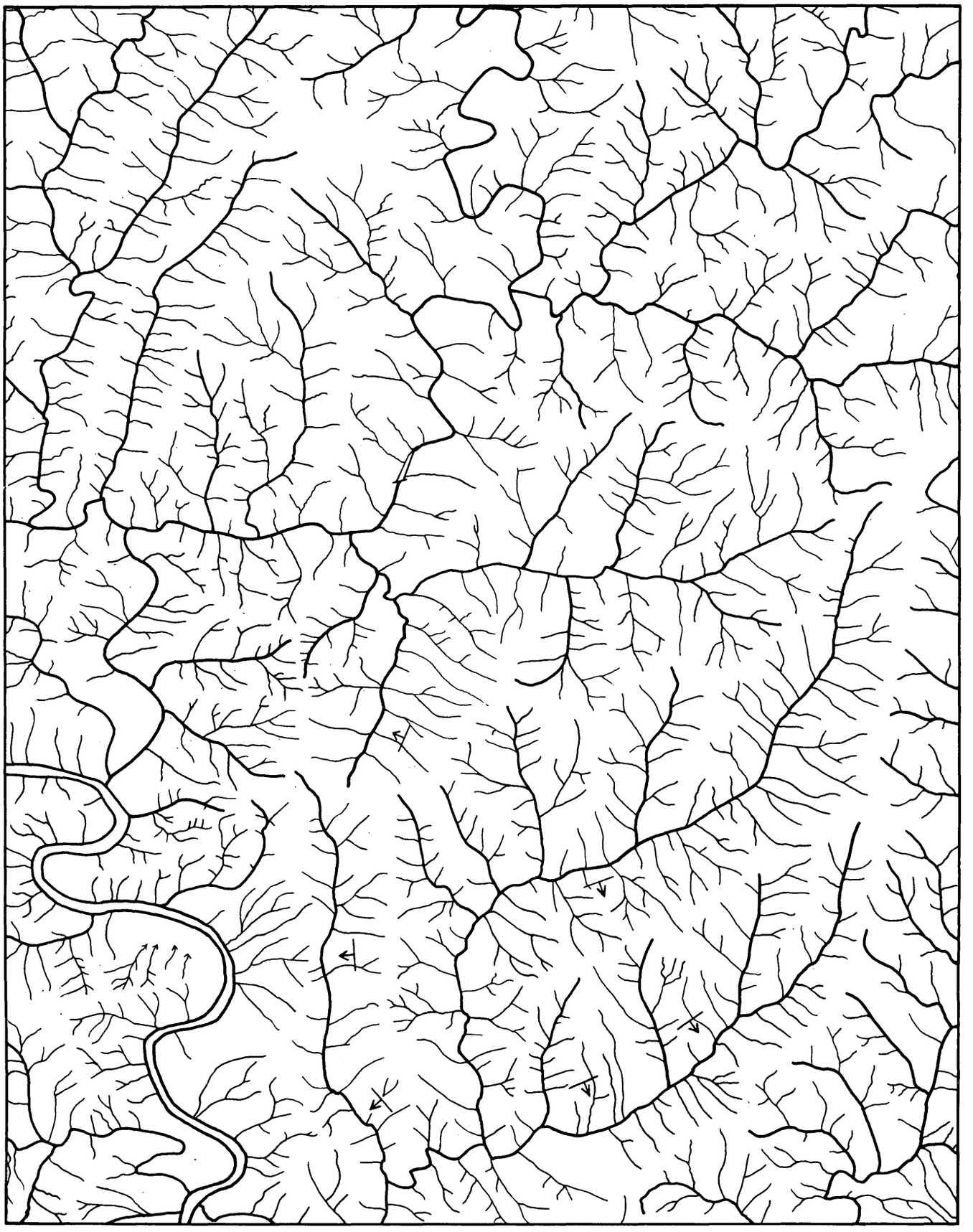
One of the advantages in study of aerial photographs is that of delineating high-angle faults or suspected faults. This advantage is a direct result of the aerial view, which allows a large area and the gross features within it to be seen at one time. For example, many alinements that are inconspicuous on the ground are readily seen on aerial photographs (figs. 74 and 83). Although many alinements are conspicuous because of their independence of stream valleys or ridges and uplands which they cross (see Barton, 1933, p. 1198), alinements of stream segments and small drainage courses are probably the most common indicators of faults. Most high-angle faults are expressed on photographs as straight or gently curving lines, and this characteristic is probably the most important clue that a fault may exist. All linear features should be examined with care even though other criteria are needed to prove the existence of faults.

Lines indicative of faults may be expressed as alinements of vegetation, straight segments of stream courses, and waterfalls across streams; alinements of lakes, ponds, and springs; conspicuous changes in photographic tone or drainage and erosional texture on opposite sides of a linear feature, or tone change along a linear feature because of vegetation which may appear darker; alinements of topography, including saddles, knobs, or straight scarps; rectilinear depressions; or any combination of these. Faults may also be expressed by horizontal or vertical offsets of beds or recognizable rock units (figs. 50, 60, 62, 74, 79, 80, 82–84, 86, 98, 99, 101, and 114). Where bedrock is well exposed the actual physical break may be seen. In some places a lineament, or broad linear depression, may be conspicuous but not distinct. Where such areas of possible faults occur, beds on one side of the general lineament should be examined for change of dip and strike as well as abnormal stratigraphic position with respect to beds on the other side (see fig. 80). Commonly in sedimentary terrain, offsets on opposite sides of a linear feature are easily detected, owing to the vertical exaggeration which is inherent in most stereoscopic models and which generally assists in the identification of correlative beds (figs. 83 and 84).

Suspected faults should be examined carefully because other features may be represented, at least in part, on aerial photographs in the same manner as faults, particularly if a single photograph is being viewed. In some areas jointing in one direction within a formation may be prominent and where an apparent offset is present owing to the occurrence of an erosion scarp along a joint plane, the scarp line may be misinterpreted as a fault trace. Where channels have been cut in sedimentary formations, and a rock type of different lithologic character now occupies the channels, a distinct lineation between the channel filling and the original sedimentary rock, now truncated, may suggest a fault trace. A line between two distinct types of vegetation, although possibly reflecting the presence of a fault, may well be due to differences in underlying rock types in normal sequence, or to the moisture content of the soil, or even to manmade features. In some areas the simple erosion of dipping strata may result in an alinement of topographically high points that suggests a fault. Or vegetation and drainage alinements may be present along easily eroded dikes. The need for caution in interpreting faults from aerial photographs is thus dictated by the very presence of numerous other geologic features that are expressed photographically in a similar manner.

Low-angle faults are more difficult to interpret from aerial photographs than high-angle faults. Discordance of structures within different rock types combined with strongly curving or irregular traces of the fault contact of the rocks involved offer the best clue to the presence of low-angle faults. Angular unconformities may show similar photographic expression.

In a study of azimuth, frequency, and length measurements, Gross (1951) demonstrated that in some covered areas of the Canadian Shield certain lineations very likely represent faults. The study involved the



construction of histograms in which the length and frequency of topographic lineations as seen on aerial photographs were plotted against geographic orientation within 10° segments of the compass. Similarly, histograms were plotted from a sampling of field data of strike of strata, schistosity, dikes, glacial striae, faults, and other features considered to have a bearing on the configuration of the topography. One peak on the histograms compiled from aerial photographs was found to represent a direction of prominent faulting.

JOINTS

Joints, like faults, are most commonly expressed on aerial photographs as linear features. In flat-lying or gently folded sedimentary rocks, most joints are steeply dipping or vertical, evenly or regularly spaced, and commonly consist of two prominent sets that are expressed on aerial photographs as lines intersecting approximately at right angles, which gives a blocky appearance to the topography (fig. 42); however, joints may be well developed in only one direction, which gives a strong linearity to the fracture plan (fig. 92). In fine-grained clastic rocks the joints are generally more closely spaced than in coarse clastic rocks. Joints may become widened through weathering and erosion processes and appear as particularly conspicuous linear features; the similarity of these joints to faults is superficially striking, especially where well-developed regional cross joints have formed in metamorphic rocks and other criteria of faulting are lacking. Identification of many joints is enhanced by the presence of vegetation along them, due perhaps to greater moisture along these lines. Lattman and Olive (1955, p. 2087) described the use of solution-widened joints in Texas as a guide to indicate steepening of dip and to locate changes in dip direction. Joints more nearly parallel to the dip direction were widened by solution of meteoric water. Rubble, soil, and water trapped in these joints gave rise to dense vegetation expressed on aerial photographs as conspicuous, even-spaced parallel lines. A good clue to the identification of joints in relatively undisturbed sedimentary rocks is the general abundance of short lineations on a photograph, and a more or less uniform trend of these lineations within a given area of a few square miles extent.

Lattman and Nickelsen (1958) described azimuth-frequency measurements from aerial photographs in a study of fracture traces in western Pennsylvania. The fracture traces are expressions of natural linear features that consist of topographic, vegetation, or soil

FIGURE 7.—Drainage map of area shown in figure 74 and vicinity. (Strike and dip positions based on analysis of stream-length relations.)

The separate drainage tracing allows a study of drainage characteristics divorced from the abundant imagery of the photograph. Patterns and tributary stream-length relations, for example, are readily observed on the separate tracing. Relative lengths of tributary streams at many places might easily be overlooked in the stereoscopic model. However, a study of the planimetric disposition of streams must be considered a supplement to a study of the stereoscopic model in which significant features in the third dimension, such as elongate hills or other features that may represent structure, are seen.

alinements exposed continuously for less than 1 mile. The term "fracture trace" is used by Lattman (1958, p. 569) to differentiate these alinements from natural linear features exposed continuously for at least 1 mile or more, called "lineaments." A histogram of frequency and orientation of the fracture traces showed maximums closely corresponding to those of prevailing directions of joints as seen in the field, with the exception of one fracture-trace maximum which had no counterpart in exposed rocks of the area (Lattman and Nickelsen, 1958). This one maximum of frequency and orientation of traces, however, was found to correspond with joints in underlying coal beds; the joints apparently were reflected through an overlying thickness of shale and sandstone to be expressed at the surface in a manner discernible on aerial photographs but not in routine field-mapping procedure. The close correspondence of fracture traces and joint directions in the test area suggest that aerial photographs may be used to extend mapping of joints into nearby areas of no outcrop.

Joints in igneous rocks are likely to be seen readily on aerial photographs (figs. 70, 71, 100, and 103). Commonly three and sometimes four prominent joint sets are developed. Where these joints are primary joints, dips may be low, moderate, or steep, depending on the orientation of flow structures within the igneous mass; this contrasts with the generally steep dipping joints of little-disturbed sedimentary rocks. Because of the wide range of dips of joints in igneous rocks, and because at least three joint sets are almost always developed, the surface traces of these joints, shown as lineations on aerial photographs, intersect at widely varying angles. The resulting crisscross pattern is distinctive of intrusive rocks in many areas. Joints in igneous rocks also may be irregularly spaced in contrast to those in sedimentary rocks.

Joints in metamorphic rocks may not be as conspicuous on photographs as joints in sedimentary or igneous rocks. Joints previously formed in igneous or sedimentary rocks may be destroyed by metamorphic processes and much of the energy of metamorphism spent in development of schistosity, fracture cleavage, or other small-scale metamorphic structures, rather than conspicuous joints. This is particularly true of metamorphic rocks formed from fine-grained clastic rocks, which comprise more than 50 percent of the sedimentary rock group. Where metamorphic rocks are recognizable by strong lineations that represent fold axes or trend of foliation, widely spaced regional cross joints perpendicular to the fold-axes direction may be prominent; streams developed along the cross joints accentuate these structures (figs. 8, 73, and 74).

CLEAVAGE AND FOLIATION

Cleavage or foliation, which is almost universally present in metamorphic rocks, especially in those that were originally shale or other thin-bedded clastic rocks, is difficult to differentiate on most aerial photographs. The "grain" of metamorphic terrain as expressed on aerial photographs by stream and vegetation patterns, as well as by parallel ridges and gullies, however, may well reflect pronounced cleavage or foliation (figs. 76 and 100). Turner (1952) pointed out that prominent topographic alinements in the schists of central Otago, New Zealand, are clearly expressed on aerial photographs. These alinements, generally parallel to the trend of *b* lineations, are believed to have resulted from differential weathering controlled by cleavage, foliation, and other elements of the schist fabric.

UNCONFORMITIES

Unconformities are generally difficult to interpret from aerial photographs. An angular unconformity may be inferred from the discordance of bedding, either in strike, dip, or both, at a contact line that has an irregular trace across a wide area. But discordance alone does not prove the presence of a stratigraphic unconformity since a discordance of bedding may be due to faulting, or locally to crossbedding. The areal distribution of rocks or structures as seen on small-scale photographs or mosaics, or after plotting geologic data over a large area, may also suggest the presence of an unconformity. On a local scale, the separation of unconsolidated, nearly horizontal, river gravel from the truncated, underlying strata is a good example of an unconformity (fig. 88). Pediment gravel that overlies truncated bedrock (fig. 45), or channel-fill deposits that truncate the underlying bedrock (fig. 44), may be clearly expressed on aerial photographs.

INTERPRETATION OF AERIAL PHOTOGRAPHS IN PETROLEUM GEOLOGY

Aerial photographs have been widely used by geologists of the petroleum industry particularly in the mapping of many large-scale geologic structures, which are readily recognized on aerial photographs because of direct surface expressions of dipping beds. The use of photogeologic techniques in the search for structures that may contain oil is continuously increasing. However, as the obvious and well-exposed structures in many areas have long been discovered, considerable attention is now being given to indirect, or geomorphic evidence of subsurface structures. In addition, photogrammetric methods for making measurements needed to compile structure contours and to

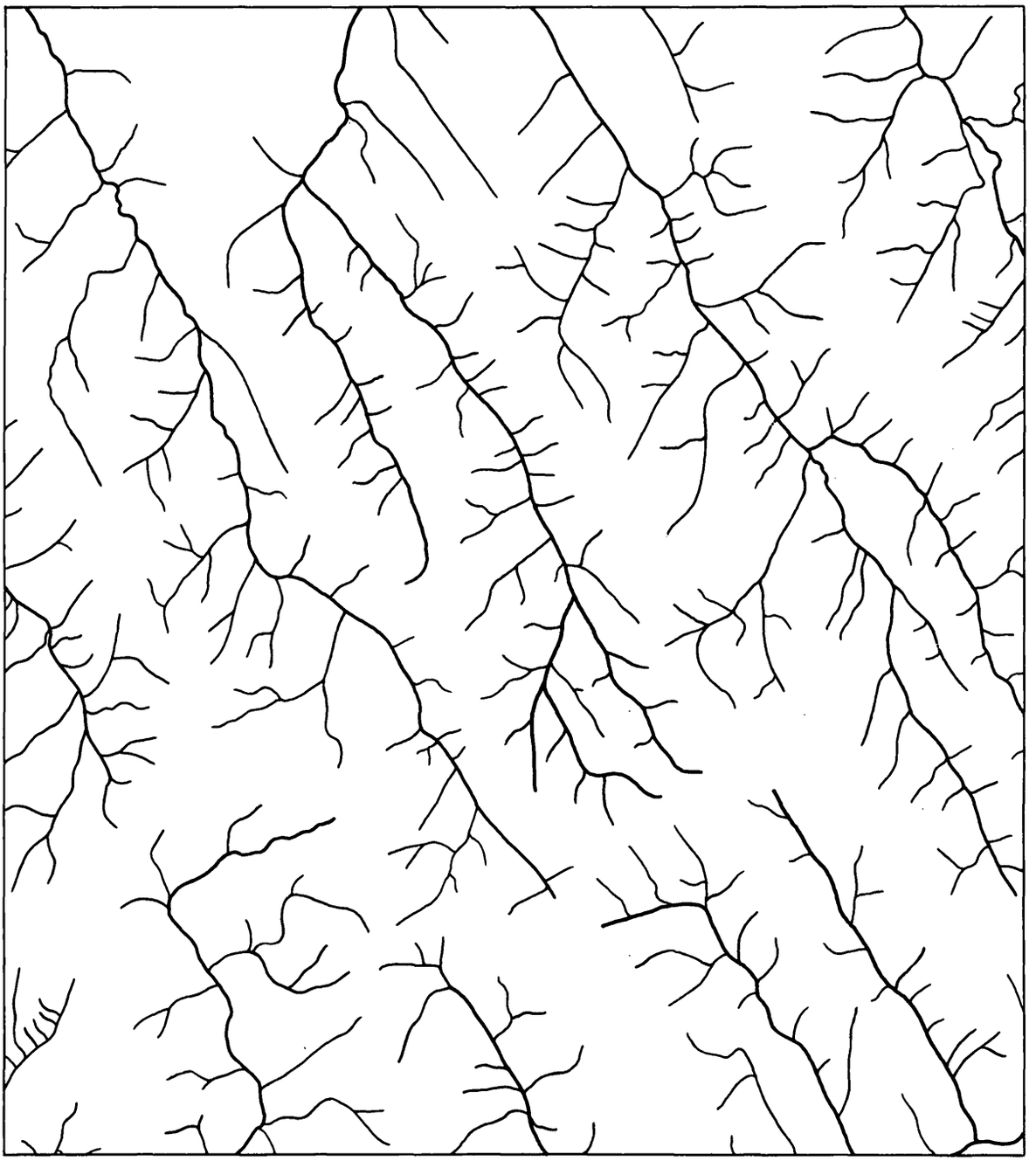


FIGURE 8.—Drainage map of area shown on left half of figure 73.

The regional cross-joint trend, expressed by the main streams on figure 73, is strongly brought out on the drainage map. Note tributary streams flowing at right angles to the main streams. Stream trends are obscured commonly by the abundant imagery of the photograph and it may be desirable to compile separate drainage maps when stream characteristics are used to interpret lithologic or structural features of an area.

determine strike, dip, stratigraphic thickness, and closure are being used increasingly.

The indirect evidence yielded by photointerpretive studies is based on the premise that subsurface structures may be reflected in surface expressions of various kinds, such as stream or vegetation patterns or anomalies. Indirect evidence is particularly useful in the interpretation of areas of few or no outcrops, such as areas of low relief, or areas of dense vegetation. Commonly in such areas, the evidence points not directly to a structure, but to an anomaly, such as a variation in drainage characteristics from the norm established for a local region. The anomaly in turn suggests a possible subsurface structure. Thus even though surface evidence alone may not be conclusive in the interpretation of subsurface structure, it may provide clues and stimulus for exploration (Alliger, 1955, p. 183). However, Wheeler and Smith (1952, p. 112) cautioned that "* * * strong deformation, periodically rejuvenated, is restricted to the mobile belts * * *," and structures farthest away from maximum deformation are "* * * therefore more difficult to infer from physiographic abnormalities at the surface * * * that without the genetic background of those events in the geologic history of the tectonic province responsible for surface and subsurface indications of structure, photogeology may be unfavorably speculative."

FOLDS

Folds may be expressed on aerial photographs by the distribution of bedding, by drainage characteristics, by topography, by distribution of soils, or by combinations of these criteria. The surface manifestations of folded or domed structures thus may range from obvious, where direct surface expression of dipping beds is present, to subtle, where subsurface structures are reflected only indirectly by physiographic criteria.

BEDDING

Many folded structures can be delineated readily because bedding is clearly expressed at the surface. Particularly in areas where rocks are well exposed and structural deformation has been mild, beds may be clearly defined by photographic tone together with topographic relief or hogback landform (figs. 90, 91, and 92); strike and dip of beds are easily determined and the structure delineated from the distribution of beds (see also p. 19).

In areas where bedding may be obscured by low plant and grass vegetation, differences in vegetation together with slight topographic relief changes, enhanced by vertical exaggeration of the stereoscopic model, may permit bedding to be delineated and structures to be structure contoured (see fig. 40 and p. 6).

DRAINAGE

In areas where bedding is largely obscured, for example by vegetation or surficial materials, stream patterns, anomalies, or textures may be helpful in determining dip slopes and outlining folds. In some areas dip-slope streams have a coarse-textured arrangement in contrast to the fine-textured arrangement of back-slope streams (fig. 79). These textures probably reflect coarse-grained and fine-grained rocks, respectively. The distributions of such textures in turn may suggest the location of structural axes.

In many areas stream adjustment to structure will result in a sweeping curve of the stream particularly across a structural axis and around the nose of a plunging fold; the convex side of the curve indicates the direction of anticlinal plunge (figs. 81 and 90). But such curves may also develop on dip slopes and thus not be indicative of the location of a structural axis. This situation may prevail where anticlinal structures are breached into softer material. Streams developing on the more resistant dip slope of the structural flank may curve on that flank and along soft interbeds, and not across the axis of the structure (fig. 93). Such a condition would probably be most pronounced during the mature phase of the geomorphic cycle. In geomorphically young areas streams may not have had sufficient time to adjust to folded structures, and may have a tendency to follow joints or preexisting faults (Howard, 1940, p. 195). In areas where stream pattern or anomaly is the primary surface reflection of underlying structure, as in some jungle-covered areas, other criteria, such as vegetation pattern, should be sought to corroborate the location of a structural axis suggested by stream characteristics.

Stream patterns or anomalies are undoubtedly the most useful indirect evidence of subsurface structures in many areas. This is especially true for coastal areas of low relief, many interior basins, or areas of dense vegetation or other surficial cover. Tator (1951, 1954) and DeBlieux (1949) discussed the structural significance of drainage anomalies in the coastal region of the Gulf States; in these low, swampy areas of aggradation it is important to establish the drainage norm by studying the drainage characteristics over a large area. Deviations from this norm may give the first indication of a structural anomaly. DeBlieux (1949, p. 1259) described abrupt locally restricted changes in drainage considered to be the result of subsurface structure. Over the Lafitte field in Louisiana a relic distributary of the Mississippi River forms two

sharp meander bends, although for miles upstream and downstream from this area, the stream channel is simple and straight. Over the Scully dome "* * * two relic distributaries of Bayou Lafourche followed simple courses, but suddenly changed to an anastomosing pattern over the dome, then resumed simple courses south of the structure." (DeBlieux, 1949, p. 1259.)

Structural implications of stream pattern or anomaly may be corroborated by other geomorphic evidence. Over the Lafitte field the presence of distinct remnants of natural levees on either side of the channel, the only such ridges over the length of the relic course of the stream, was considered significant supporting evidence of underlying structure (DeBlieux, 1949, p. 1259). The levee-ridge remnants presumably were held up by subsurface structure as surrounding areas subsided.

In a study of tonal and textural anomalies in west-central Texas DeBlieux and Shepherd (1951) described anomalous compressed meanders over structural highs. In the same area annular and radial drainage patterns and stream deflections in the flank areas were important criteria that supported an interpretation of subsurface structure (fig. 94). The importance of abrupt changes in direction of streamflow in relation to possible subsurface structures has recently been emphasized by Buttorff (1958) and Elliott (1958), based on work in the Powder River Basin, Wyoming. Such deviations from the norm for an area commonly stand out when a separate drainage map of an area is studied (see fig. 9) or when stereoscopic models are viewed pseudoscopically (see p. 5 and fig. 95).

In areas of aggradation and active subsidence it is to be expected that abnormal drainage characteristics rather than any specific drainage pattern might be indicative of subsurface structure. The combination of emergence, due to recent rise of salt plugs, and subsidence of the general coastal-plain area is responsible for many of the anomalous drainage characteristics of the coastal area of the Gulf States; such characteristics are anastomosing stream segments, abruptly widened levee ridges, or abrupt changes in direction of streamflow.

In areas of active degradation, patterns of drainage rather than abnormal drainage characteristics can be expected to be indicators of structure. However, Wheeler and Smith stated (1952, p. 82) that the analysis of stream pattern with regard to structure—which they called "creekology"—is somewhat outmoded as a photogeologic procedure; they implied that anomalies in drainage characteristics may be far more important than specific drainage patterns. However, drainage pattern may actually be anomalous with respect to the drainage norm for an area; such examples of drainage patterns have been found along the northwest coast of Alaska on the Arctic coastal plain. Here, in an area of northward-flowing streams, slight topographic highs have resulted in radial-dendritic drainage patterns, which outline areas of subsurface structure (fig. 96). Commonly no other surface expression of structure is present. Because of low relief, outcrops are few.

TOPOGRAPHY

The presence of topographic highs has been significant in locating subsurface folds or domal structures even in many areas where relief is very slight. Many of the "islands" of the coastal area of the Gulf States are surface expressions of salt domes. Topographic features such as natural levees, which represent areas of higher ground only a few feet or tens of feet above the delta or flood plain, are also significant interpretation criteria in the search for subsurface structure (Tator, 1951). Tator reported (1951, p. 717) that "* * * cheniers and natural levees * * * provide linear patterns of higher ground supporting distinctive vegetation growths." These higher areas are also favored for cultivation. According to Tator (1951, p. 717) "Tonal contrasts in the photographs are the major keys used for recognition of landscape features of extremely low relief, such tonal variations being largely the result of soil and vegetation differences." The significance of low relief, is shown by DeBlieux's description (1949, p. 1254) of Felicity Island, a 2-mile-long natural levee ridge separated by several miles of marsh from the area where the levees normally could be expected to die out. The preservation of the "island" in an area of active subsidence has been attributed to local subsurface structure. Abrupt widening of levees on one or both sides of a channel, in areas of subsidence, also has been noted over subsurface domal structures (DeBlieux, 1949, p. 1254, and fig. 2, p. 1255); widening of levees may be due to other causes, such as coalescence of two levees, however, and this feature of the flood plain must be interpreted carefully.

In a study in northern Alaska, Fischer (1953) used topography as the principal interpretation criterion in locating the Square Lake anticline. The area is a treeless waste of low relief that is underlain by permafrost; tundra grasses cover the region, and no bedrock is exposed. Fischer (1953, p. 208) reported that the original photogeologic study showed small hills in the area elongate in the same direction as the regional

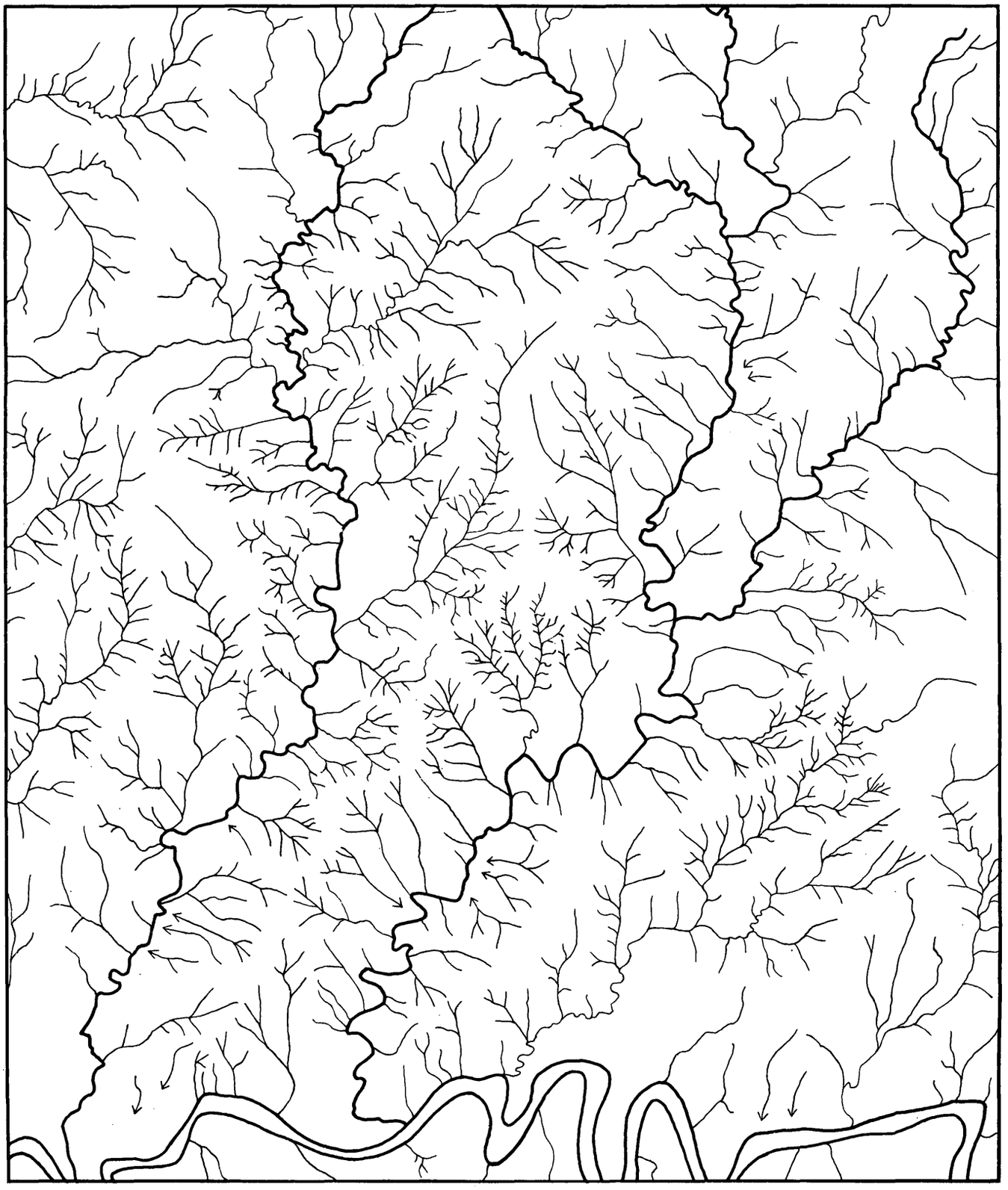


FIGURE 9.—Drainage map of area shown in figure 94.

Radial drainage over structure, *A* of figure 94, stands out on the drainage map which is unobscured by the abundant details of the photograph. Note that the radially draining streams flow into larger streams that have an annular pattern around the structure. Stream deflections, as at *D* in figure 94, are commonly more readily observed on the separate drainage map or in pseudoscopic view of the model (see fig. 95).

structural trend. Normal to this trend other elongate hilltops sloped in the direction of the inferred dip of beds. Also, streams flowing in the dip direction had a slightly less well developed dendritic pattern than those flowing opposite to the dip direction. There also appeared to be a correlation between slopes of the tops of cut banks and the direction of dip. Plotting of all such data gave a consistent apparent structural pattern —a plunging anticline—of unknown reliability. A subsequent seismic survey corrobrated the photogeologic interpretation.

SOILS

In some areas devoid of outcrops, soil patterns or soil distributions may be useful in delineating or suggesting structures. Both Woolnough (1934b, p. 221, 224) and Christensen (1956, p. 858–859) cited examples of the usefulness of aerial photographs in this regard. Wheeler and Smith (1952, p. 106) stated that contrasts in soil tone accentuate unusual drainage relations on the northern flank of a structure in the southwest Maysville area, Oklahoma; and in southwestern Alabama differences in cultivation pattern reflect relief and soil characteristics by which geologic units of Tertiary age beneath younger unconsolidated materials can be differentiated.

DeBlieux and Shepherd (1951, p. 98) described tonal and textural anomalies in west-central Texas that resulted from differences in soil types, soil-moisture content, and erosional characteristics. They cited an anomaly at Salt Fork on the Brazo River where "* * * dark and coarsely hummocky surface strongly contrasts with the lighter color and finer texture of the surrounding surface * * *" (DeBlieux and Shepherd, 1951, p. 98). The anomaly was strikingly similar to that of a reef producer in Scurry County. DeBlieux and Shephard (1951, p. 88) emphasized that how a structure forms is unimportant in a study of tonal, textural and other anomalies, because the surface evidence is identical, whether the structure has resulted from upward movement, differential downwarping, reef or residual topography, or combination of these features; it is important initially that a surface anomaly can be recognized.

FAULTS

Faults are significant in the geologic interpretation of petroleum areas because they may be deep seated and of major importance in localizing oil accumulation. Where faults are genetically related to structures that may be oil bearing the distribution pattern of faults may be of considerable use for interpreting the locations of those structures. The many surface expressions of faults are described above (p. 21).

Desjardins (1952, p. 82) stated that surface fault and fracture lines, expressed as lineations on aerial photographs, form patterns that bear a definite relation to deep-seated salt domes and to subsurface faults of the Gulf Coastal Plain. Disturbance centers, believed to be underlain at depth by salt domes, may be indicated by the fault patterns, shown on photographs as "Sharply curving lines which are strikingly concentric" or as "Prominent transverse lines radiating usually from some marginal point rather than from the center of the structure" (Desjardins, 1952, p. 82). Desjardins believed that such fault patterns were the result of continuous application of small stresses caused by rising salt masses rather than an accumulation of stresses that would produce large amounts of movement; he also felt that faults probably would form in interdome areas as well as over the domes. The genetic significance of the fault pattern is thus critical if distribution of faults is used as a basis for locating the dome itself. Desjardins (1952, p. 83) made a strong distinction between surface expressions of faults, which he associated with deep-seated domes, and other criteria, such as topographic expression, widening of natural levees, and looping of stream channels, which he associated with shallow-seated domes.

Although most interpretations of faults are based on qualitative characteristics of observed data, such as the dislocation of correlative beds, or the contrast in light and dark photographic tones on opposite sides of a straight line, a quantitative approach to such studies may provide additional useful data. On the basis of azimuth-frequency studies Blanchet (1957, p. 1748) suggested that structural and stratigraphic anomalies in some areas may be located by a statistical analysis of fractures, which he defined as the generally abundant, natural lineations discernible on aerial photographs. The basis for analysis is a comparison of local deviations in the statistical mean direction of fracture sets with regional norms for each fracture set. Regional norms are first established by plotting fracture-azimuth frequency diagrams of the region involved. Then statistical mean directions of fracture sets are determined by analyzing samples within circular areas centered at relatively small horizontal intervals of a few miles. These local mean directions are in turn studied for local deviations which are entered into empirical equations that yield structure-intensity values. These structure-intensity values are then contoured, to form a structure-intensity map, which may reflect structural anomaly. The structure-intensity map is supported by a fracture-incidence map, prepared in contour form, and by an analysis of drainage characteristics of the area in question. Blanchet applied this method to a study of petroleum structures.

FACIES

Although the widest application of aerial photographs in petroleum geology has been with regard to structural traps, a study of aerial photographs may contribute to the location of stratigraphic traps, particularly if photogrammetric measurements of formation thicknesses can be made at many points within the streoscopic model (see p. 59–60). From a qualitative standpoint it can be seen in figure 97 that a rapid loss of sandy section can sometimes be detected on aerial photographs. Such "shaling" or loss of sandy section due to facies change may be important in the search for stratigraphic traps and in some areas it may be measured photogrammetrically. In other areas well-defined formational units may thin or thicken without facies change, but this also may be significant in regional studies with regard to stratigraphic traps (Christensen, 1956, p. 861, fig. 6). Measurements of stratigraphic sections needed in such studies commonly can be made from aerial photographs.

REGIONAL STUDIES

The significance of aerial photographs in regional petroleum studies is widely recognized, but very little information is present in the literature with regard to this phase of photograph use. Not only may measurements be made from aerial photographs with regard to strike, dip, stratigraphic thickness, and closure, but the regional view of the mosaic or small-scale photographs permits a continuity of photographic criteria that may be of structural or stratigraphic significance. Overall geologic relations are brought together, and areas where detailed study is needed may be indicated. However, the limitations of the photogeologic technique must be constantly borne in mind. As Wheeler and Smith (1952, p. 112) pointed out, the validity of the technique "* * * depends a good deal upon the human element and the utilization of all applicable geologic data." They warned that "* * * the student of photogeology may * * * become overly impressed with geometric design of lines, masses, and tones so that, in the absence of understanding of the tectonic history he may find compatible alignments of stream courses, structurally inexplicable lineations or shapes and soil patterns that are not consistent with the known or expectable products of diastrophism" (1952, p. 112). An emphasis on regional study is indeed justified, however, if maximum use is to be made of aerial photographs, and this is true whether photographs are used in long-range exploration programs, as in reconnaissance mapping of broad basin areas, or in the ultimate study of local structures.

INTERPRETATION OF AERIAL PHOTOGRAPHS IN SEARCH FOR ORE DEPOSITS

The search for ore deposits, similar to that for petroleum, requires favorable host rocks or structures, or both, and it is therefore necessary to determine the general lithologic character and distribution of rocks and associated structures as a basis for carrying out a mineral survey of an area. Aerial photographs may contribute geologic data not only with regard to the fundamental guides of lithology and structure in ore search, but they also may reveal details of physiography, which may be an important ore guide in the search for placer deposits. Botanical guides to ore bodies may also be detected on aerial photographs of some areas, although little work has been done in this field.

STRUCTURAL GUIDES

Where fractures have been significant in localizing ore deposits aerial photographs may reveal significant structural data relating to trends and offsets of fractures, even in areas where surficial cover is extensive. This is due in large part to the great variety of criteria suggestive of fractures (see p. 21). In many areas it is possible to determine spatial relations of sets of fractures, and to infer the relative ages of the fractures from the aerial photographs, although results of field study are necessary to determine the significance of the patterns.

Aerial photographs are presently most useful in study of those ore deposits associated with fractures. In many mining districts where mineralized fractures form a vein pattern that is repeated throughout the district, an analysis of the fracture pattern and distribution may provide significant data in the search for new ore bodies. Reed (1940) described the use of aerial photographs in a mineral-deposits study of the heavily timbered Chichagof mining district of Alaska where gold-bearing quartz veins are associated with faults and shear zones (see fig. 99). There the faults are commonly expressed as depressions owing to greater erosion of soft material from fault zones (see also Twenhofel and Sainsbury, 1958, p. 1433). Reed (1940, p. 44) stated that many faults of moderate surface expression would probably have been overlooked on the ground, and that many faults of weak surface expression were seen only on aerial photographs. Joliffe (1945, p. 604), in a discussion of photogeologic prospecting in the Yellowknife area of Canada, noted that some of the largest gold-ore bodies "* * * lie in strong shear zones that are marked by rather distinctive gullies in relatively massive, resistant volcanic rocks." Many of these shear zones and other lineaments are conspicuously shown on aerial photographs.

Gross (1951) pointed out that in the glaciated Drysden-Kenora area of northern Ontario and the Goldfields area of northern Saskatchewan, Canada, there are many linear features seen on aerial photographs but that only certain ones represent faults. He devised a scheme of statistical analysis to show the likelihood that certain linear trends were faults (see p. 21). Concentration of prospecting along these linear features in the Goldfields area resulted in discovery of pitchblende deposits.

Because faults commonly are interpreted readily from aerial photographs, photogeologic study may aid in locating extensions of faulted ore bodies. Faults that offset an ore body may show an orderly spatial arrangement, and information regarding direction of displacement may be extrapolated to similar faults whose displacement is masked by vegetation or surficial debris. Willett (1940) found that aerial photographs provide significant information on the location of faults cutting the Invincible Lode, a gold-quartz deposit in the Glenorchy district of New Zealand. The photographs strikingly show the offset of a lode east of the Invincible Lode by a series of parallel faults, which suggest that similar conditions exist at the Invincible Lode where the evidence is not as readily observed because of surficial debris. In the Invincible Lode area one major stream flows parallel to the strike of the faults, and a second stream is deflected along a fault for about 1,000 feet, then bends back to its old course; the direction of deflection also indicates the horizontal direction of displacement of the quartz lode. The pattern of displacement, based on photogeologic evidence together with ground evidence, suggests the location of faulted extensions of the lode.

Major anticlinal and domal structures, readily interpreted from aerial photographs of many areas on the basis of drainage characteristics or strike and dip patterns, are with notable exceptions of relatively little importance in ore search. Where folds have been a factor in localizing ore, as in some metamorphic rocks, they commonly are too small or the geology too complex for existing aerial photographs to provide useful guides in prospecting.

LITHOLOGIC GUIDES

Lithologic guides may be considered from the standpoint of the parent and host rocks, or from the standpoint of mineralized or altered zones, which are more appropriately termed mineralogic guides. Photogeologic interpretation of rock types (see p. 16–19) may outline broad target areas of favorable parent and host rocks (fig. 100). Lueder (1953, p. 823) suggested that various locations can be rated on the basis of favorable photogeologic evidence; the most favorable area would become the prime target area for further investigation. Where some local field criteria are available, specific ore-bearing formations may be traced on photographs (fig. 98). At Ross Lake, Canada, the fact that rare-earth-bearing pegmatites of small areal extent were recognizable on photographs was a major factor in the discovery of certain tantalite deposits (Joliffe, 1945, p. 604).

The use of color aerial photography will increase many times the amount of lithologic information that can be obtained from a photogeologic study. This additional information will contribute not only to the reliable interpretation of host or parent rocks, but may permit local guides, such as alteration zones, to be readily recognized. In a study of the hydrothermally altered volcanic terrain near Tonopah and Goldfield, Nevada, information obtained from reversible-type color transparencies was contrasted with data obtained from thin sections of rock types. Kent (1957, p. 868) stated that "In both areas a general correspondence between coloration and alteration was observed. Zones of different coloration within a lithologic unit represent different stages of alteration. Colors of rocks in early stages of alteration are useful in recognizing lithology, but highly altered rocks have the same color within several different lithologic units. The colors associated with highly altered rocks are easily recognized on color aerial photographs; thus their distribution and their relationship to structural features can be studied." In addition Ray (1958, p. 37) wrote that "In one area of altered andesites a pale green color on color aerial photographs was found to represent an intermediate stage in the alteration resulting from partial silicification, with pale green chalcedony, and deuteric alteration and later oxidation of iron opaques. A light color in another zone was found to result from brecciation of dacite and attendant alteration to carbonates. A rather intense orange color was indicative of highly altered zones in all localities observed. However, the orange coloration did not indicate the rock type involved nor the type of alteration present, but rather was the result primarily of weathering of iron minerals following their partial breakdown by deuteric alteration."

PHYSIOGRAPHIC GUIDES

Some ore deposits are topographically expressed or are related to structures, rock types, or surficial deposits that are so expressed (fig. 102). Hence, topography may be considered a guide in ore search, although it does not by itself indicate the presence of ore. Because fractures commonly are topographically ex-

pressed as rectilinear depressions, a possible physiographic guide to ore as interpreted from aerial photographs may be said to exist in many areas. Where fractures have been mineralized, and the vein filling stands in relief, topography may be a useful guide in ore search. However, many mineralized veins are poorly resistant to weathering and erosion, and occur as topographically low areas.

Where topography results in a photographic texture it may be possible to delineate areas of favorable host rocks, as the paraschists in Surinam (Zonneveld and Cohen, 1952, p. 155). Grantham (1953, p. 336) pointed out that in the wet Sierra Leonne area of Africa, the "* * * sharp change in topography from linearly arranged hills, controlled by schist and migmatite, contrasts with the irregular features of structureless granite."

An analysis of the physiography of an area may provide significant information, particularly in relation to placer deposits. As many placers have a complex history, it may be necessary to work out the alluvial history of a valley or valley system for maximum information in locating placer pay streaks. The arrangement and positions of old stream channels may be interpreted from meander scars, oxbow lakes, and different terrace levels that are commonly seen on aerial photographs. Photographs also may provide gradient measurements of present or past streams; this information may be significant inasmuch as placer concentrates occur especially where stream gradients flatten.

Buried stream channels, also the site of some ore deposits, may be interpreted from photographs of some areas on the basis of topographic expression (fig. 101). In many parts of the western Sierra Nevada, Tertiary stream valleys have been filled and gold-bearing gravel buried by younger lava flows. The greater resistance of the lava flows compared with the surrounding rocks has resulted locally in sinuous cappings of volcanic rocks that stand above the present-day stream system. Table Mountain, California (Loel, 1941, p. 384, 386–387), is an outstanding example of basalt capping auriferous gravel of a buried channel.

The location of stream-channel deposits recently has received wide attention in the search for uranium deposits on the Colorado Plateau in Western United States. There the Triassic Shinarump member of the Chinle formation is thicker in channels cut in the underlying Moenkopi formation, which is also of Triassic age. Some channels can be observed directly on aerial photographs (fig. 44); others may be inferred from isopach measurements, which in some areas may be obtained from aerial photographs. (See p. 58–59). The uranium is associated with carbonaceous materials, largely plant remains, scattered throughout the channels.

BOTANICAL GUIDES

Much field and laboratory work has been accomplished with regard to plant distribution and plant concentration of certain elements as indicators of ore. Little has been done, however, on plant characteristics or associations that may be observed or interpreted from aerial photographs, and herein lies a field of research that has much potential. There appear to be three aspects of botanical study from aerial photographs that may contribute to the location of ore deposits. These involve (a) color differences in vegetation brought about by concentration of certain chemical elements, (b) species differences or absence of vegetation owing to concentration of certain chemical elements, and (c) distribution of vegetation suggesting favorable structures or rock types. Color differences in vegetation, due to mineral and chemical concentrations, that may be reflected on aerial photographs have received almost no attention, and offer an interesting field of study. Species differences or lack of vegetation has likewise received little attention in ore search, although Walker (1929, p. 50–51) noted that air search was made for "dambos" as indicators of copper deposits in central Africa. Dambos are open spots in the bush cover, where vegetation does not grow because of the concentration of poisonous copper salts in the soils. Walker noted that the Roan Antelope copper deposit was marked by such a dambo, although the deposit extended beyond the limits of open area. Identification of species from color differences due to concentrations of certain chemical elements may be particularly amenable to detection on color or other special aerial photography.

Plant and tree distribution may be useful indicators of structures or of rock types favorable to ore deposition; vegetation distribution may reflect physical characteristics of the rocks, such as porosity or presence of fractures, although some rocks, such as limestone, may be preferentially covered by a certain type of tree because of chemical concentrations in those rocks (see fig. 72) rather than because of physical properties. Or vegetation may grow preferentially or trees grow higher and be alined along a fault or shear zone, which might in turn be a favorable site for ore deposition (see fig. 71). Such indirect guides in ore search contrast highly, however, with color or species differences, which might suggest more strongly the presence of ore minerals.

Levings and Herness (1953, p. 456–457) stated that heavy timber growth in the Corbin-Wickes area of Montana shows a preference for unaltered quartz mon-

zonite, which has a darker photographic tone than the surrounding andesite and dacite; ore occurs in the volcanic rocks. Zonneveld and Cohen (1952, p. 153) mention that vegetation differences permit photographic differentiation of the clay savannahs and sand savannahs of Surinam, South America. Bauxite production at Surinam's Billeton mine (Hemphill, oral communication, 1958) is from a clay area, and hence it is important to know the distribution of such clay areas.

INTERPRETATION OF AERIAL PHOTOGRAPHS IN ENGINEERING GEOLOGY

Aerial photographs have been used for many years to provide topographic and land-use information in locating routes for pipelines, highways, or other rights-of-way, but only in recent years have photographs attained wide recognition as a source of geologic information for engineering purposes. Many kinds of geologic information for engineering use may be obtained from aerial photographs. These include (a) identification and location of soil materials, particularly granular materials, which would provide suitable foundation sites for industrial and airport developments, or highway rights-of-way; (b) identification and location of clay and clayey silt soils, which would have detrimental properties with regard to building, airport, and highway sites; (c) location of aggregate materials; (d) delineation of areas that may be underlain by permafrost; (e) interpretation of distressed conditions in landslide areas; (f) analysis of structural geology in areas of tunnel, dam, and reservoir sites; and (g) location of sample areas for detailed investigation of soil and rock materials.

SURFICIAL MATERIALS

Surficial materials generally are interpreted in terms of gross physical characteristics, rather than the detailed physical characteristics used by the pedologist. Knowledge of the gross physical properties is sufficient for many reconnaissance studies in engineering geology. Indeed, it is the grouping of several pedologic soil types into a few classifications that permits aerial photographs to be of significant engineering use. In the preparation of soil-engineering maps from agricultural reports of an area in Illinois, Thornburn (1951, p. 91) was able to reclassify 99 different pedologic soil types into 13 engineering groups. Lueder (1951) described the use of aerial photographs as a major tool in preparing soil-engineering maps.

The inability to interpret fine details with regard to physical characteristics of the soil thus does not preclude the use of aerial photographs in many engineering geology studies. From the standpoint of engineering significance a granular material, for example, which exhibits certain diagnostic photographic characteristics such as coarse-textured drainage, will generally react favorably to drainage, compactability, and other engineering tests, regardless of whether it is a residual granular material that has resulted primarily from weathering in place or whether it is a transported gravel derived from different rock types. However, Jenkins, Belcher, Greeg, and Woods (1946) pointed out exceptions to the general thought that photographic characteristics common to granular materials always signify suitable granular materials for engineering purposes. For example, the soil profile of well-drained limestone has a granular texture due to aggregation of clay particles into lumps. The surface drainage may be coarse textured; but the soils break down on compaction and react as plastic soil material, and not as a granular material (Jenkins, Belcher, Greeg, and Woods, 1946, p. 80).

Where pedologic data are already available they may be very useful to the engineer when interpreted in terms of engineering test data (fig. 4). Indeed, certain soil mechanics tests by the engineer, such as plasticity or soil-texture tests, are similar to those used by the pedologist. Greenman (1951) suggested that the pedologic method can become the nucleus around which aerial photo interpretive and field geologic information can be accumulated. But Eardley (1943, p. 567) pointed out that "In many places conditions unfavorable for the development of a normal soil, such as rugged mountains, wide sandy plains, or swampy basins may cover rather large areas. The important construction materials in such places may be better interpreted as a result of geological processes than from the standpoint of a soil classification * * *."

GROUND CONDITIONS

The interpretation of ground conditions probably has received more attention in recent years than any other engineering geology application of aerial photographs. Much of the literature concerns reconnaissance studies of soils in general and granular materials in particular; granular materials are essential for building sites and highway and airport development (Jenkins, Belcher, Greeg, and Woods, 1946; and Purdue University, 1953). Special attention also has been given to photointerpretation of permafrost conditions in northern latitudes.

With regard to highway engineering, Belcher (1945, p. 144) stated that "* * * the soil problem resolves itself into two parts, one in which the soil in place is satisfactory as subgrade, and the second, where the soil is unsuitable. In areas of unsuitable soils some form

of improvement, by stabilization or insulation, is required. Insulation involves the economic location of granular materials in the form of rock to be crushed, cinders (volcanic), or sand and gravel * * *. Inasmuch as sand and gravel or other granular deposits exist to some extent in nearly every county in the country the significance of soil patterns indicating granular materials is of considerable economic importance to engineers." In fact, a large percentage of construction and maintenance expenses are in the costs of sand, gravel, crushed rock, and similar materials. As a tool for interpreting areas of gravel, sand, silt, and clay, aerial photographs offer an inexpensive and rapid method of reconnaissance, and according to Schultz and Cleaves (1955, p. 370) "* * * planning and exploration for large engineering projects should almost never be undertaken without a thorough study of aerial photographs of the region * * *."

Photointerpretation of surficial materials must consider not only the surface expressions of these materials but also the geologic factors reflecting the origin of these materials. A knowledge of the origin of materials permits inferences as to what kind of materials can be expected in an area, and in what locations with respect to other geologic features. Field-sampling programs also could be based on the analysis of the photogeologic data, and subsequent mineralogic and related studies by the engineering geologist could provide the soils engineer with information that would eliminate the need for many of the soil mechanics tests now performed as part of the routine laboratory analysis of all soil samples.

ELEMENTS OF SOIL PATTERN

The surface expressions of granular and other soils materials have been termed collectively the "soil pattern." The soil pattern consists of several elements of which the most important ones for nonpermafrost areas are considered to be landform, drainage, erosion, relative photographic tone, and color; vegetation cover and land use may also be significant (Belcher, 1944, 1945, 1948; Jenkins, Belcher, Greeg, and Woods, 1946; Frost, 1946; Mollard, 1947; Hittle, 1949; and Purdue University, 1953). Schultz and Cleaves (1955, p. 371) considered that "interpretation of soils by means of aerial photographs rests largely on the interrelationships of soils and geomorphic features"; consequently landform is considered by some to be the most important element in photointerpretation of soils. Landform, however, is only one element of the soil pattern and it is clearly evident that the association of several elements of the soil pattern will provide the greatest amount of information from aerial photographs.

Landform

Identifying the landform commonly identifies the natural process that formed it, and commonly limits the type of soils or soil characteristics that can be expected. The emphasis on landform is probably valid in reconnaissance soils investigations where broad areas of several different landforms are studied and mapping is at a small scale. But where detailed engineering information is needed, as in foundation studies, it is likely that the area of study will be within one landform, mapping will be on a large scale, and other elements of the soil pattern, such as differences in relative photographic tone, which may reflect soil-moisture content, will be of prime importance.

In small-scale mapping the emphasis on landform is probably warranted particularly for constructional landforms of transported materials, such as sand dunes, river terraces, alluvial fans, and many glacial landforms, all of which have distinctive shapes, although not necessarily unique (see figs. 52, 55–57, and 104); here the transported soil materials make up the landform. In contrast residual soils associated with destructional landforms may be more difficult to interpret from aerial photographs, for here the parent rock makes up the landform, and the significance of soils rests in part on the subjective interpretation of rock types. However, the interpretation of other elements of the soil pattern with regard to physical characteristics of soils are just as valid for residual as for transported materials; the engineering significance of many residual soil areas can be interpreted readily from aerial photographs on the basis of these other elements, such as drainage and erosional characteristics (figs. 63 and 65).

Drainage characteristics

Highly permeable soils will have good drainage regardless of their origin, provided that topographic positions will permit draining. In well-drained soils surface drainage normally will be coarse textured or even absent (figs. 49, 52, 66, 104, 106, and 108); in soils of low permeability drainage will normally be fine textured (fig. 63) or ponds may be numerous (figs. 57 and 66). The presence of fine- or coarse-textured drainage in surficial materials, like that in bedrock (p. 16), is primarily related to the relative resistance of the different materials to erosion, and hence related to permeability and grain size. Coarse materials characteristically are resistant to erosion, are permeable, and have a coarse-textured drainage; fine materials commonly are less resistant to erosion, are impermeable, and have a fine-textured drainage. These relations are significant in the interpretation of engineering soils from aerial photographs because drain-

age texture can be readily observed. However, exceptions to these relations may exist, as with loess, which is commonly characterized on aerial photographs by a relatively fine-textured drainage (see figs. 105 and 106); yet, loess in its natural environment is generally considered well drained internally.

Flow or channel markings, for example on terraces, indicate that the material was deposited by running water and further suggest that the material may be granular. Frost (1946, p. 121) described flow markings in an area in the midwest as consisting of light and dark streaks usually parallel to the direction of flow. The light streaks are ridges of sand or fine gravel that are probably sand and gravel bars; the dark streaks are fine clay or organic material deposited in depressions that once contained standing bodies of water. Frost (1946, p. 121) stated that "The chief significance of such markings lies in the fact that they suggest stream deposition and in order to have stream deposition at such elevated positions and occurring on * * * a large scale, there must have been large volumes of swiftly flowing water. Since swiftly flowing water allows only coarse material to settle, the terrace must contain a large percentage of gravel." It may be debatable that channel markings always indicate swiftly flowing water, but where some doubt exists other elements of the soil pattern may reveal the character of the terrace material.

In broad areas of aggradation, such as the Mississippi embayment, drainage characteristics revealed by aerial photographs are significant to the engineering geologist, as different soil characteristics are associated with the several features of valley alluviation. For example, backswamp areas contain clay and silty clay of high organic content, whereas natural levees consist of silt, silty sand, and some silty clay (Fisk, 1944, p. 18, 20). The levees commonly "* * * provide linear patterns of higher ground supporting distinctive vegetation growths" (Tator, 1951, p. 717). Low areas may be swampy and also contain distinctive vegetation. Graveliferous deposits fill the old valleys and in turn are covered by various other deposits; sandbars contain permeable sand that grades downward into the gravel. The distribution of features of the flood-plain drainage may be significant in analyzing ground conditions and locating favorable engineering materials in highway, railroad, and airport development.

Erosional characteristics

Closely related to the drainage characteristics of a soil are its erosional characteristics; these are important in photointerpretation studies chiefly from the standpoint of gully erosion, which is controlled largely by the physical properties of the soil and especially by cohesion. The usefulness of gully erosion characteristics in photointerpretation primarily involves the shape of transverse profiles, although longitudinal profiles may provide additional information. According to research workers at Purdue University (1953, p. 15–16) "* * * there are three basic gully characteristics which are associated with three major soil textural groups." Granular soils commonly develop sharp, V-shaped gullies that have short, steep gradients. Nongranular cohesive and plastic soils are generally indicated by uniform gentle gradient of gullies that extend well back into the upland, and by broadly rounded shallow V-shaped transverse profiles. The loess soils and sandy-clay soil exhibit U-shaped cross sections of gullies that have flat bottoms and low gradients.

Although there may be a general adherence of gully characteristics to the major soil textural groups, exceptions are not uncommon. For example combinations of the basic gully characteristics "* * * occur in 'layered soils' or in soils exhibiting a 'strong profile' ". (Purdue University, 1953, p. 16), and compound gradients may develop. In addition to the steep or vertical slopes in deep gullies, windblown silt may develop silt pinnacles and catsteps or terracettes (Purdue University, 1953, p. 45). It has been pointed out (Purdue University, 1953, p. 27) that climatic environment under which gullies form is an important consideration; for example, soft clay shale in an arid region where flash floods may occur commonly exhibit abnormally steep slopes in contrast to clay shale in areas of uniform rainfall where such slopes are usually softly rounded. Under certain conditions, such as gravel capping on clay soils in the New Jersey coastal plain (fig. 108), gullies in the underlying clay soils may be steep and deeply incised, in contrast to the usual broad shallow transverse gully profile of the clay soil group in humid regions.

In permafrost areas different materials may yield the same cross-sectional profile. Gravel deposits cemented by ice may have vertical gully walls, or may have gullies that are asymmetric in cross section if one side is preferentially exposed to the sun and thaws at a faster rate than the shadow side. The insulating materials overlying frozen deposits also affect the rate of thawing and hence the erosional characteristics of gullies. Interpreted carefully, however, the erosional characteristics—gully cross section and gradient—may reveal useful information on texture and other engineering characteristics of the soil.

Photographic tone

On black-and-white photographs the significance of color must be interpreted in terms of relative gray photographic tones. Belcher stated (1948, p. 486) that

"Light color tones (grays) are usually associated with well-drained soils, while clays, principally because of their water-retention capacity, appear dark." Frost (1946, p. 122), in describing the mottled soils in Indiana, stated that mottling nearly always indicates gravel. The mottling is due to "dark areas" which are "* * * small clay-like pockets that have been formed by the normal weathering processes of the gravel-sized material" (Frost, 1946, p. 122). These pockets are depressions that "* * * act as small infiltration basins which result in a higher moisture content and a darker color pattern" (Frost, 1946, p. 122). This mottled soil pattern contrasts with that of the drift plains in other areas where light-toned patches of slightly higher and dryer silty soils adjoin lower areas of wet plastic silty clays. Somewhat similar mottled patterns have been described by Gwynne (1942, p. 202–205) from the drift plain in Iowa (see fig. 107). But light photographic tones also may result from lack of moisture, owing to lack of precipitation as in many arid regions, rather than because of good drainage, and thus tone may be of little significance in evaluating soil texture in some areas. Or light tones may be the result of topographic position, and it is probable for example that a "* * * sand dune on a sand plain in a humid region will photograph light in color against a dark background" (Purdue University, 1953, p. 26) not because of differences in soil textures but because of topographic position. Climatic conditions also influence the colors of soils, especially the residual soils, and dark color rather than light color may be associated with well-drained materials, as certain red soils developed from limestone (Jenkins, Belcher, Greeg, and Woods, 1946, p. 84). Yet, provided climatic conditions are considered and provided relative photographic tone is borne in mind, the generalization that light photographic tones suggest good drainage and dark tones poor drainage may be useful in the overall interpretation of soils with regard to moisture content. Where tone is due to moisture, infrared photography will result in strong tonal contrasts between soils of different moisture content.

Color

Color has been cited as a principal element of the soil pattern that may yield information on the texture and drainage character of the soil profile, but to date very little interpretive work has been done with color photography. Belcher (1945, p. 138) briefly mentioned experimental color photography taken in different parts of the United States and stated that "The value of color * * * lies in the added detail that it furnishes with respect to these two elements of the soil pattern" (that is, soil color and details of vegetative cover). It would seem that color photography would reveal pedologic information significant in engineering evaluation of soils, especially the residual soils, which may be more difficult to interpret in general than transported soils, particularly from black-and-white photographs.

Vegetation

Vegetation as an element of the soil pattern has been considered one of the most difficult to interpret. It is known, for example, that certain trees, such as aspen, are tolerant of many different soils and soil conditions, but some types of vegetation are strongly influenced by soil type. Furthermore, vegetation may be influenced significantly by climatic factors. Where permafrost is close enough to the surface to affect tree and shrub roots the kind of vegetation that will grow may be restricted (see p. 37). Species identification may be difficult in any area unless large-scale photographs are available or unless pure stands are present. Nevertheless, vegetation may reveal significant information in engineering studies provided valid interpretations are made with regard to how vegetation is associated with soil textures, soil-moisture content, and topography; thus a knowledge of plant ecology is necessary if maximum information on soil conditions is to be obtained from aerial photographs. Willows, for example, indicate wet ground, poplar indicates dry ground, and jack pine implies sand and gravel beds (Belcher, 1945, p. 139). However, where abrupt changes in soil conditions exist, it is likely that vegetation changes will also occur (figs. 56 and 72), and areas needing further ground surveys may be easily delineated by inspection of aerial photographs without any basic knowledge of plant ecology. For example, stabilized sand dunes in interior Alaska can be easily delineated because they are marked by stands of dark-toned spruce (see fig. 56), in contrast to light-toned brush and grass of the interdune areas. This relation may be found where the topographically higher, well-drained sand of the dunes contrasts with frozen silty deposits of the interdune areas.

Where phreatophytes—plants and trees that obtain water from the water table—can be delineated (see p. 40), aerial photographs may provide significant engineering data because phreatophytes may choke overflow channels and thus increase the flood potential of some areas. Information pertaining to the downstream de-silting effect of phreatophytes with regard to dams and reservoirs may also be obtained from aerial photographs of some areas (see Robinson, 1958, p. 28–29). However, little interpretative work in this field has been done.

Land use

Land use may also reveal information on the soil conditions of an area. Belcher (1945, p. 142) reported that "Orchards thrive in well-drained locations and therefore, when observed on level ground, good subdrainage is implied." Shallow drainage ditches in areas of little relief commonly signify plastic, poorly drained soils. Schultz and Cleaves (1955, p. 378) stated that in eastern France and western Germany "* * * rugged topography and associated sandy soils developed on sandstones are generally left in forest; the comparatively level topography and associated clayey soils developed on shales and limestones are cultivated * * *." On the flood plain of the Mississippi River the silty sand of the natural levees is cultivated primarily because of its topographic position above the lower backswamps. In parts of the Valley and Ridge province of Eastern United States the limestone areas commonly are farmed whereas shale areas may be left in forest.

PERMAFROST

Permafrost has a significant effect on engineering characteristics of soils of the far northern latitudes and has received considerable attention in recent years, particularly from the standpoint of photointerpretation (Cabot, 1947; Woods, Hittle, and Frost, 1948; Benninghoff, 1950; Frost and Mintzer, 1950; Frost, 1951; Sager, 1951; Black, 1952; Hopkins, Karlstrom, and others, 1955). Considerable disagreement exists, however, on the significance of photointerpreted data in the study of permafrost areas (see Black, 1952, p. 126–127, 129), although it is generally agreed that aerial photographs can be particularly useful in such studies. The following discussion of ground conditions in permafrost areas is taken from the work of Hopkins and Karlstrom (Hopkins, Karlstrom, and others, 1955), except as noted by specific references.

Muller (1947, p. 219) defined permafrost as "a thickness of soil or other surficial deposit or even bedrock, at a variable depth beneath the surface of the earth in which a temperature below freezing has existed continuously for a long time (from two to tens of thousands of years)." Muller (1947, p. 30) also stated that "From the standpoint of engineering, the content of ice in frozen ground is of paramount importance * * * [because] * * * thawing of this ice produces excessive wetting and undesired plasticity of the ground and renders it unstable and susceptible to settling, caving, and even flowing." Building foundations, highways, railbeds, and airport runways may be considerably damaged unless the presence of permafrost is taken into consideration and measures taken to eliminate or minimize the effect of the thawing that results from the disturbance of the natural thermal regimen. Where bedrock or thick frozen gravel deposits that contain local drainage channels are the primary foundation materials, permafrost is not normally detrimental to construction.

Although aerial photographs are useful in the interpretation of areas that may be underlain by permafrost, criteria used for interpreting soil conditions of nonfrozen areas apply only to a limited extent to permafrost zones. Gully characteristics of an impermeable gravel deposit cemented by ice, for example, will not necessarily be the same as the characteristics of gullies in impermeable nonfrozen soils. Because of the altered permeability and porosity of soils owing to permafrost, erosional characteristics, as applied to the interpretation of nonpermafrost areas, may have little significance in the perenially frozen regions. Other criteria, such as the common landforms, although suggestive of type of material present, are of limited use in determining the presence or absence of permafrost. Few diagnostic indicators of permafrost appear to exist. More often than not the criteria are suggestive rather than indicative; they include distribution and type of vegetation, polygonal relief patterns, pingos, and features resulting primarily from thawing.

Distribution and type of vegetation

Distribution patterns of trees and shrubs commonly supplement topographic expression in recognizing landforms; these patterns may contribute indirectly to the interpretation of probable permafrost conditions based upon inferences concerning the age of the land surface, climate, and character of the underlying material. In addition, the type of vegetation may be useful in delineating areas where permafrost is likely to be present. Hopkins and Karlstrom (1955) reported that recognition of shallow-rooted species on aerial photographs aids in delineating the areas where permafrost is most likely to occur at shallow depth, and that recognition of deep-rooted species helps delineate areas least favorable for the formation or preservation of permafrost. Thus, black spruce may suggest areas underlain by permafrost at shallow depth, whereas tall willow shrubs and isolated pure stands of balsam popular on river flood plains generally indicate unfrozen ground. The distribution patterns of trees and shrubs, however, are most significant only when evaluated together with other information, such as type of landform, concerning permafrost distribution in the region under study.

Polygonal relief patterns

Polygonal relief patterns commonly can be identified on aerial photographs, but as they may be present

in both permafrost and nonpermafrost areas this criterion is not, by itself, always diagnostic in evaluating permafrost conditions; however, in conjunction with other features it may be very significant. Polygonal patterns may be divided into two broad groups: those formed by frost-stirring and those formed by contraction. The formation of frost-stirred polygons is favored by the presence of permafrost at shallow depth, but these polygons are not necessarily an infallible indicator of shallow permafrost as they are also known to occur where permafrost is absent or is at a considerable depth.

Contractional polygons are subdivided into low-center, high-center, and frost-crack polygons. Low-center polygons, one of the most dependable indicators of permafrost, are commonly found in poorly drained depressions. The presence of pools of water in the centers of some polygons is a diagnostic recognition feature, and it is common to find low-center polygons expressed on aerial photographs as dark-toned centers surrounded by light-toned marginal ridges (figs. 109–112). High-center polygons occur in slightly better drained areas than those in which low-center polygons are found; generally, the centers are relatively level, although they may be domed where frost is extremely active. In contrast to low-center polygons, drainage around high-center polygons is commonly concentrated in marginal trenches, and pools of water are present at trench intersections. Because of the high centers, these polygons are commonly expressed on aerial photographs as light-toned centers surrounded by dark-toned margins (figs. 40 and 109–112). Frost-crack polygons may be difficult to distinguish on aerial photographs, as they are similar to high-center polygons; they may be present in some areas where permafrost is absent.

Other relief patterns in conjunction with vegetation distribution result in striped slopes that are commonly present in permafrost areas (fig. 40).

Pingos

Pingos are rounded or elliptical steep-sided hills formed by the "downward freezing of a body or lens of water or of semi-fluid mud" (Muller, 1947, p. 59). They may be as much as 300 feet high. Fissures may develop along the axis of a pingo or radiate from the crest. Pingos usually are found in poorly drained areas and normally are readily distinguished on aerial photographs by their distinctive local landform (figs. 110 and 111); they are almost always a reliable indicator of permafrost, although locally they may be confused with erosional knolls or hills.

Features resulting from thawing

Two features associated with thawing are suggestive of the presence of permafrost. These are thaw lakes (sometimes called thermokarst lakes) and beaded drainage. Thaw lakes occur in frozen fine-grained sedimentary deposits that generally contain clear lenses and masses of ice whose volume is greatly in excess of the porosity of the unfrozen material. As this ice melts the ground subsides and forms a basin in which a thaw lake may accumulate (figs. 110 and 111). When caving is progressing, banks are ragged and steep or overhanging. Tilted trees known as "drunken forests," along the margins of such lakes are indicative of active caving. In treeless areas active caving may be indicated by tension cracks parallel to the banks. Other indications of thawing, such as serrated margins of lakes, also may be present (figs. 109–111). The usefulness of thaw lakes as permafrost indicators, however, is limited by the difficulty of distinguishing on aerial photographs between active thaw lakes, relict thaw lakes, and similar-appearing lakes that are in no way related to permafrost.

Beaded drainage occurs particularly in perennially frozen peat and silt containing ice wedges; it is characterized by small pools connected by short watercourses that may be sharply incised (figs. 40 and 112). The pool banks commonly are steep as a result of thawing and caving of frozen materials.

Absence of permafrost

In areas of discontinuous permafrost it is not only desirable for the engineer to know where permafrost is present, but it may be equally important to determine where permafrost is absent. Certain hydrologic phenomena and elements of the soil pattern commonly indicate or suggest the absence of permafrost. For example, subterranean drainage in unfrozen zones within permafrost may be detected on aerial photographs of some areas. The recognition criteria are in part similar to those applied in evaluating soil conditions in nonpermafrost areas of the world. That is, streams may disappear into the bottoms of closed depressions or by percolating into a gravel-covered surface. In addition, the presence of dry depressions in permafrost areas may indicate locally well-drained areas, inasmuch as there is generally a source of water during the summer months. Such areas contrast with other areas of the earth's surface where dry depressions may be due to absence of precipitation or other immediate source of water. Locally unfrozen zones within permafrost areas may also be suggested by springs, which are commonly indicated by flood-plain icings, shown as flat, white surfaces on some aerial

photographs, or indicated by more luxuriant vegetation along a pronounced lineation or within a dark-toned area on low hill slopes. These unfrozen zones may be favorable as a source of ground water. In addition, because permafrost generally causes soils to be impermeable, drainage characteristics indicative of permeable materials (see p. 34) may be interpreted to mean lack of permafrost, at least in the immediately underlying materials. Certain tree species may also suggest absence of permafrost (see p. 37).

EROSION, TRANSPORTATION, AND DEPOSITION

LANDSLIDES

Natural movement or potential movement of materials is a significant consideration in many construction engineering problems. Foremost in this regard is the movement of soils and rock materials by landslides. Ritchie (1958, p. 67) stated that "All landslide investigations must start with recognition of a distressed condition in the natural or artificial slope * * *." Distressed conditions are commonly interpretable from aerial photographs. "The evidence for distressed conditions that may be present, or that may be induced, lies chiefly in evidence of movements, minor or major, that have already taken place or of geologic, soil, and hydrologic conditions that are likely to cause movement in the future" (Ritchie, 1958, p. 67). Geologic, soil, and hydrologic conditions signifying potential landslide areas include the presence of unfavorable geologic structures and rock type, prevalence of fine-grained materials, and an abundance of water or conditions that would permit access of water to fine-grained materials.

Because remedial measures for landslides or prevention of landslides are generally not only difficult but costly, avoidance of landslide areas is important in highway route layout. Existing landslides are commonly identified on the basis of landform (figs. 46 and 113). Liang and Belcher (1958, p. 70) stated that some landforms are more susceptible to landsliding than others, and thus identifying the landform is highly important. "Potential slides of the rockfall and soilfall type can commonly be foreseen simply by recognizing geologic conditions that are likely to produce overhanging or oversteepened cliffs" (Ritchie, 1958, p. 51). Basalt cappings underlain by easily eroded shale (figs. 53, 87, and 113) illustrate a condition where rockfalls may occur as a result of failure and slump in the underlying materials.

Movement of unconsolidated materials by flowage is likely to produce the most damaging landslides. Existing flows and slides (figs. 46 and 113) commonly have a "hummocky" surface. Landslide scars, where soils and vegetation have been stripped off the bedrock, may be easily recognized on aerial photographs by the light photographic tone of the bedrock in contrast to darker tones of surrounding areas. Areas of potential flow of unconsolidated materials may be revealed by tension cracks or crevices, or suggested by the presence of seepage zones or springs, shown by dark tones of dense or luxuriant vegetation or by dark tones of the soil.

Ritchie (1958, p. 50) warned, however, that although aerial photographs are of significant help in developing the setting for detailed studies, they seldom contain the detail needed by the engineer to carry out preventative or remedial measures. The prime application of aerial photographs in landslide studies appears to be in interpreting ground conditions to determine areas that should be avoided in highway route layout and similar problems.

BEACH EROSION

In a shoreline study in California, Munk and Traylor (1947) showed that variation in wave height and refraction of waves along the shore was controlled in part by sea-floor topography. Where refraction causes a convergence of waves the rate of shoreline erosion may increase. Krumbein stated (1950, p. 203) that "Refraction diagrams are becoming an essential part of any study concerned with shore processes, and graphic methods have been developed for preparing them from hydrographic charts or aerial photographs." Photographs taken periodically of shoreline areas would also provide information, both qualitative and quantitative, in studies of erosion and deposition, which might thus be useful in planning remedial action against the eroding currents. In a study of shoreline erosion by the U.S. Army Corps of Engineers (U.S. Beach Erosion Board 1946, p. 13) aerial photographs taken in 1941 were compared with land surveys of 1836 to obtain rates of erosion along the shore of Lake Michigan. The rate of erosion plays a significant part in planning corrective measures for eroding currents.

BEDROCK

GEOLOGIC STRUCTURE AND TYPE OF ROCK

Because of the influence that faults may have on construction design and costs, it is important that faults be located and studied in the beginning stages of an engineering project. Aerial photographs may provide significant information in this regard as some faults are recognized from subtle expressions on photographs but are identified only with difficulty on the ground. The usefulness of photographs in mapping a proposed damsite in southeastern Alaska is shown in a

study of the Swan Lake area (fig. 114) where faults stand out in aerial view as conspicuous lineations, which are primarily reflections of rectilinear depressions on the ground. In a damsite study in Malaya, Alexander and Proctor (1955) used large-scale aerial photographs taken 750 feet above the ground. These photographs showed clearly the attitude and distribution of faults and joints in granitic country rock. In connection with the San Jacinto tunnel project in California, Henderson (1939) noted that aerial photographs revealed indications of unsuspected faults and corroborative evidence of those previously suspected. Fault locations underground were found to be close to that predicted from study of photographs.

In addition to showing faults, aerial photographs commonly shown dipping beds that are important in some foundation studies for pier and abutment location. Or dipping beds may indicate potential rockslide conditions where the dip is in the same direction as the hill slope.

Lithologic characteristics of bedrock materials are also significant in many engineering problems, as in foundation work, or in locating road metal sources. Criteria useful for interpreting the general lithologic character of rock types from aerial photographs are discussed on pages 16–19.

INTERPRETATION OF AERIAL PHOTOGRAPHS IN HYDROLOGIC STUDIES

LOCATING POTENTIAL GROUND-WATER SOURCES

Little has been written on the interpretation and uses of aerial photographs specifically in hydrologic studies, although photogeologic techniques offer both practical and research applications in this field. Practical application of aerial photographs in hydrologic study are at present confined largely to assisting the geologic mapping in ground-water investigations, particularly in areas covered by surficial materials. As an aid in ground-water mapping, elements of the soil pattern are evaluated in terms of ground conditions, just as in many engineering geology studies (see p. 34–37). Thus, for example, coarse-textured drainage or absence of drainage may signify highly permeable materials (figs. 52, 66, 88, 104, and 105*B*; and p. 34–35) or the landform (figs. 52 and 104) may suggest the kinds of materials that compose it, which permits an evaluation of permeability and porosity and potential as a water reservoir. In addition, aerial photographs may reveal information directly suggesting the presence of water, such as a preferential distribution of vegetation at the margins of a gravel cap (see figs. 104 and 108). The type of vegetation in turn may permit inferences with regard to the general quality of water. For example, salt cedar is tolerant of relatively high content of salt in water, whereas cottonwood trees are intolerant. Howe (1958) described briefly the use of aerial photographs with specific reference to locating possible water-bearing formations.

WATER-LOSS STUDIES

In a study of water loss caused by phreatophytic plants and trees, which take their water from the water table, Turner and Skibitzke (1952) used aerial mosaics and contact prints for delineating areas of different densities of phreatophytes. The areas were then measured by planimeter and used in conjunction with vertical foliage density, determined by field methods, to arrive at volume density to which water loss by transpiration for specific species could be equated. Data pertaining to tree species and heights were determined by ground methods. Turner and Skibitzke (1952, p. 67) stated that "The comparison between results obtained by air and by ground mapping led to the conclusion that the former offers a much faster and more accurate method, particularly in areas of dense growth." Further use of aerial photographs in collecting basic data for studies of water loss by phreatophytes could probably be made. For example, it may be possible to determine tree or plant species, especially when large-scale black-and-white photographs are available or where color photographs have been taken. In addition, for many areas where the ground surface can be observed through the trees, photogrammetric measurements may provide rapidly those height measurements needed in water-loss studies. For areal measurements of differing vegetation types or densities a simple dot-templet method may be useful (Wilson, 1949). Like many other studies, however, where vegetation and ground features must be observed, measured, and plotted, maximum use of aerial photographs will result from combined use of field and photogeologic methods.

OTHER APPLICATIONS

Aerial photographs as a tool in hydrologic studies provide a medium for obtaining basic data, such as cross-section profiles, linear, areal, slope, and volume measurements. Some of the suggested uses of photogrammetric techniques in hydrologic studies are: (a) for definition of channel size and shape of cross section to be used in studies of the effect of channel geometry in flood characteristics of streams; (b) for determining channel storage capacity used in flood-frequency correlations; (c) for definition of the three-dimensional sinuosity of natural channels to be used in studies of the rate of energy loss; (d) for definition of the geometry of bed roughness of alluvial channel

models (Thompson, 1958); (e) for measuring topographic characteristics of drainage basins such as stream slopes and drainage density; and (f) for determining areas of lakes and swamps in water-storage studies.

INSTRUMENTATION

Instruments in photogeologic study serve three objectives, namely, interpretation, measurement, and plotting of data. The instruments used thus may be photogrammetric or nonphotogrammetric—photogrammetry is the art of making reliable measurements from photographs. Usually different instruments are used for attaining each of the three objectives, as, for example, in using a stereoscope, parallax bar, and radial planimetric plotter, respectively. But all three operations may be combined in a single piece of equipment, such as the Kelsh plotter (fig. 18). Whether interpretation is done with a simple stereoscope and paper prints or with a precision stereoplotting instrument using glass-plate diapositives, the criteria of recognition, described in the first part of this paper, remain the same except insofar as scale and resolution of photographic details are involved. Both measurement and plotting are here considered as mechanical aids that provide quantitative information to be further used in geologic interpretation of an area, and instruments are discussed primarily with this objective in mind.

Measurement involves (a) the determination from aerial photographs of vertical and horizontal distances, which in turn are used to compute stratigraphic thicknesses, angles of dip, and other quantitative data of geologic use; (b) the direct determination of inclined distances, commonly the stratigraphic thickness of a formation; (c) the direct determination of angles of slopes or beds; and (d) other quantitative determinations of possible significance in geologic interpretation, such as light-transmission measurements.

Plotting primarily involves the orthographic positioning of geologic data from aerial photographs to base maps or compilation sheets. It also involves direct plotting of geologic data in cross-sectional views, and may include positioning data such as geologic contacts, which are not directly recognizable in the stereoscopic model, by use of the floating dot or spatial reference mark that is found in many photogrammetric instruments.

KINDS OF INSTRUMENTS

Many different photogrammetric instruments are available for making measurements and plotting geologic data to base sheets or cross-sectional profiles (see Fischer, 1955; Ray, 1956; Pillmore, 1957; and Hemphill, 1958a). Certain instruments permit only the measurement of altitude differences, others permit only the orthographic positioning of geologic data, but many instruments are used for both measuring and plotting. Most measuring and plotting devices are designed to accommodate standard 9- by 9-inch photographs; enlarged photographs can be used with only a few instruments, such as the overhead projector, in transferring data to a base sheet.

MEASURING DEVICES FOR USE WITH PAPER PRINTS

One of the most commonly used and widely available types of instrument for determining altitudes from paper prints of aerial photographs is the stereometer or parallax bar. Several varieties of stereometers are available for use with either the lens or mirror-type stereoscope (see fig. 10); they consist of two small plates, usually of glass or plastic, that have inscribed dots, or other targets, that can be centered over conjugate image points in a stereoscopic pair of photographs. The plates are attached to a supporting bar along which they may be separated horizontally. The supporting bar generally has graduated readings in millimeters or inches and a slow-motion adjustment drum that permits readings of hundredths of millimeters or thousandths of inches. All stereometers are based on the "floating-dot" principle, where two target dots, one seen with each eye, are fused stereoscopically into a single dot that appears to float in space within the stereoscopic model. The apparent height of the single fused dot, used as a reference mark in determining altitude differences, is related to the horizontal separation of the individual dots being viewed. Thus by measuring the horizontal separation between individual dots when the fused dot in the stereoscopic model is placed at the top of an object (such as a hill or cliff) whose height is to be determined, and subtracting from it the measurement of the horizontal separation between individual dots when the fused dot is placed at the bottom of that object, a measure of the height, called differential parallax, is obtained. Differential parallax is converted to feet by simple mathematical calculations (see p. 53). Stereometers are thus merely devices that permit reliable measurement of differences of horizontal distances between two or more pairs of conjugate image points as seen on two photographs that form a stereoscopic pair.

Parallax ladders also may be used for determining differences in altitudes from aerial photographs. Like the stereometer, the parallax ladder is based on the floating-dot or floating-line principle. The instrument may consist of two diverging rows of dots on plastic or glass arms; thus, a series of pairs of dots exist with

different horizontal separations, and this in turn results in several floating dots all at different altitudes within the stereoscopic model (see fig. 12). Or the instrument may consist of two diverging lines with intercepts of specific horizontal separations ticked off; thus a single plunging line would be seen in stereoscopic view. The instrument, oriented at right angles to the flight line, is used by sliding it over the stereoscopic model until a pair of dots or line intercepts—seen stereoscopically as a single dot or cross in space—appears to fall on the base of the object whose height is to be determined. A reading of the horizontal separation of the two dots or intercepts is then made. The parallax ladder is moved until a different pair of dots or intercepts—also seen stereoscopically as a single dot or cross in space—appears to fall on the top of the object whose height is to be determined. Again a reading of the horizontal separation of dots or intercepts is made. The difference in readings obtained is then used in a simple formula to determine the difference in altitude of the two points (see p. 53). A direct-reading parallax ladder that eliminates the need for most of the mathematical computation has also been devised. The differences in horizontal separation of pairs of dots has been calculated by the manufacturer in terms of heights in feet for different flying heights and photobases, and this permits a direct reading of relative altitudes within the stereoscopic model.

Also for use with paper prints is a stereo slope meter, designed primarily for determining degrees or percentage of slope. The instrument consists of two transparent disks each scribed with eccentric circles of specific diameters (fig. 11). These disks are mounted in a frame so as to be movable horizontally in a fashion similar to the dots of the stereometer. In stereoscopic view the two sets of eccentric circles appear as a cone that is divided into several zones. By proper horizontal spacing of the two disks, the resulting cone seen stereoscopically can be raised or lowered so that some two circles will rest on the slope or grade to be determined. By appropriate simple calculations the slope can be determined. Center dots present on each of the transparent disks also permit relative altitudes to be determined just as with a stereometer.

PLOTTING DEVICES FOR USE WITH PAPER PRINTS

Instruments have been designed specifically for plotting information from paper prints to base maps or control sheets. An instrument widely employed in the past is the sketchmaster (fig. 13), which uses the camera-lucida principle in transferring data from the photographs to the base sheet. The sketchmaster allows the operator to view a single photograph image superposed on the base map. Adjustments for scale changes in the perspective photograph permit coincidence or near coincidence of photograph control points and base-map control points. Geologic detail is sketched directly on the base map. This instrument can be adjusted to remove small amounts of tilt inherent in some vertical photographs, but like any direct-reflecting projector, large amounts of radial displacement due to relief cannot be effectively removed.

The radial planimetric plotter has been devised especially for transferring photographic detail to a base map or control sheet. Unlike the sketchmaker, this instrument is designed to eliminate displacement due to relief. The plotter consists of a mirror stereoscope mounted above two photograph tables (fig. 14). A transparent plastic arm with a centrally scribed line extends from and pivots around the center of each table. These arms are linked to a pantograph attachment. Because the plastic arms radiate from different centers they cross each other in stereoscopic view to form the so-called plotting cross.

In operating the radial planimetric plotter a pair of vertical photographs is oriented on the photograph tables for proper stereoscopic viewing, and control points on the photographs are oriented to control points on the base manuscript by means of the radial arms and pantograph. Movement of the pantograph attachment moves the plotting cross over the stereoscopic model and permits tracing of photograph detail on the base manuscript. Inasmuch as the radial arms that intersect a terrain feature on each photograph represent azimuth lines from known points on the base manuscript, the intersection of these two arms will represent the true map position of that feature, just as will the intersection of two azimuth lines shot from different instrument stations in the field. Thus the relief displacement of a feature on a photograph is effectively removed; this is one of the chief advantages in using the radial planimetric plotter. However, the radial lines do not intersect along the principal line—or flight-line direction—between photographs, and the photograph tables must be shifted to their alternate centers before the central area of stereoscopic model can be delineated. Because the photograph tables are mounted in a horizontal position, the instrument does not permit removal of tilt that may be present in the photographs, but tilt is usually small in present-day photography and generally does not cause significant errors in horizontal positioning of geologic data.

The multiscope is a combination of mirror stereoscope and camera lucida that has received limited use

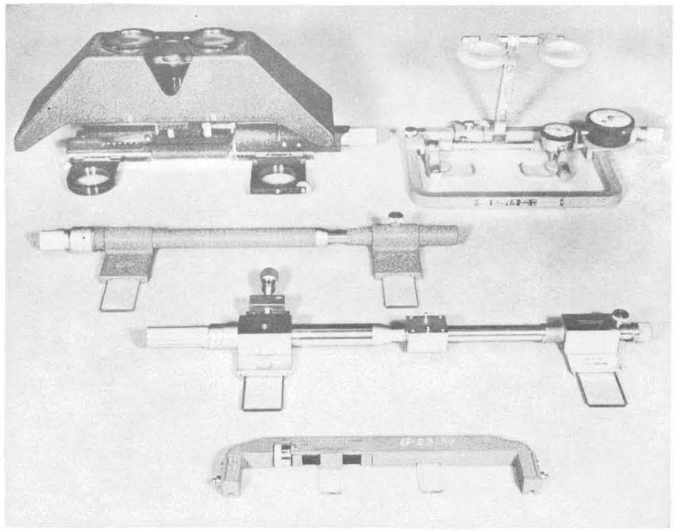


FIGURE 10.—Stereometers.

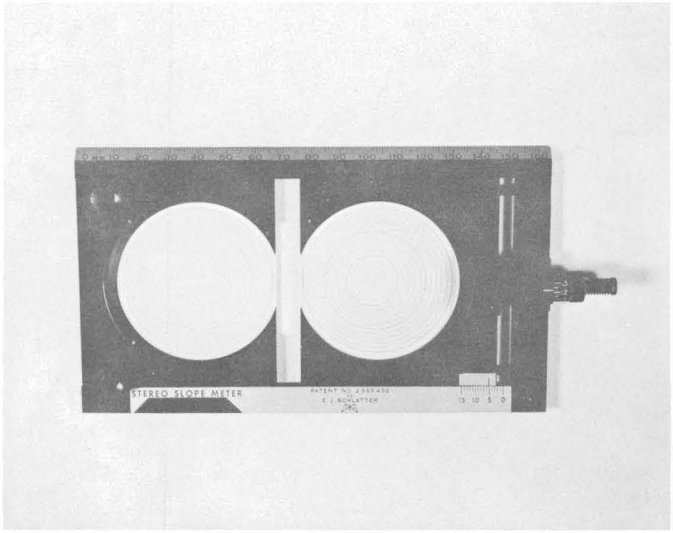


FIGURE 11.—Stereo slope meter.

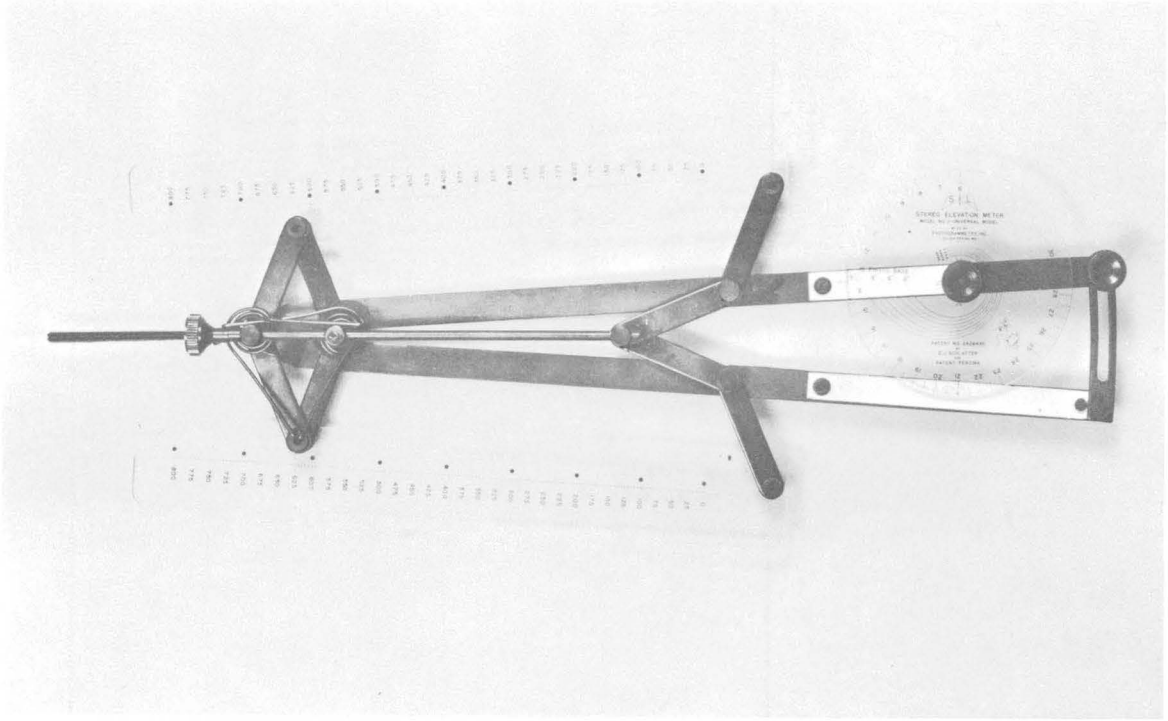


FIGURE 12.—Parallax ladder.

MEASURING INSTRUMENTS FOR USE WITH PAPER PRINTS

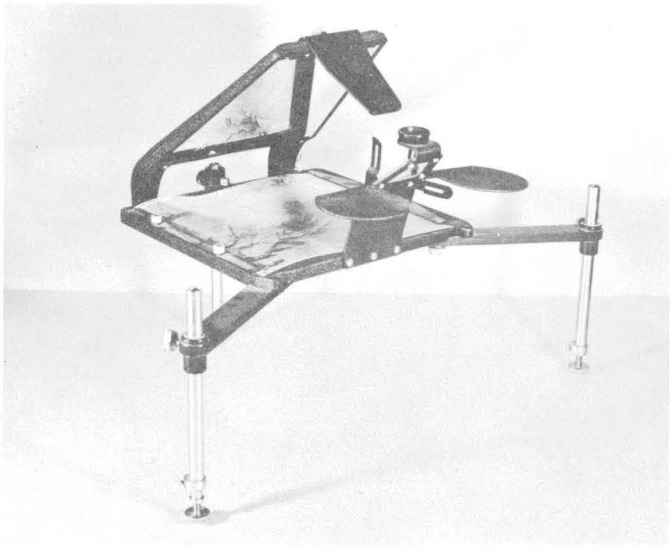


FIGURE 13.—Sketchmaster.

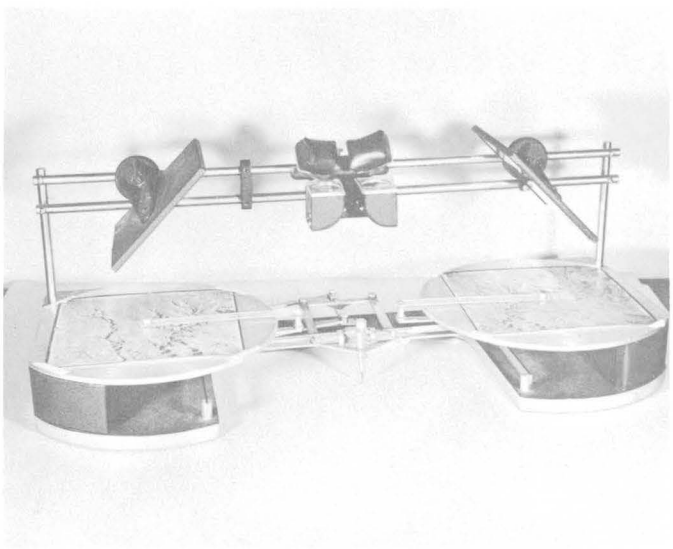


FIGURE 14.—Radial planimetric plotter.

PLOTTING INSTRUMENTS FOR USE WITH PAPER PRINTS

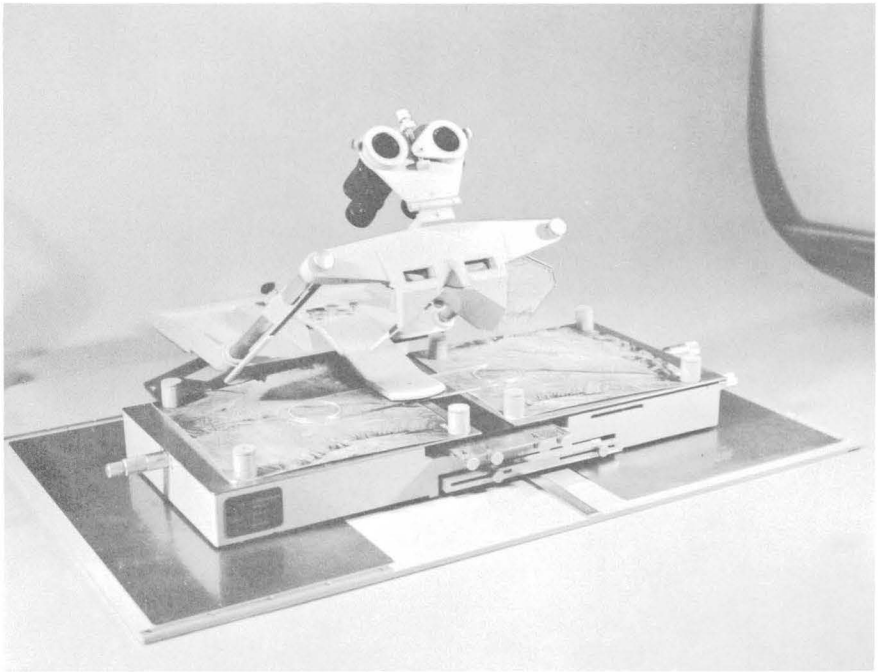


FIGURE 15.—Stereotope.

COMBINED MEASURING AND PLOTTING INSTRUMENT FOR USE WITH PAPER PRINTS

in plotting geologic data from photographs to base maps or control sheets. Photographs are mounted on movable photograph plates that permit small adjustments for tilt. The viewing assembly is constructed to allow the insertion of one or two half-silvered mirrors in the eyepiece, so that in operation either the image of a single photograph or the stereoscopic model may be superposed optically on the map or control base. Although the stereoscopic model may be seen at all times, use of only one half-silvered mirror permits the eye to see only the image of one photograph superposed on the map base; the resulting plot is similar to that from the sketchmaster—or reflecting projector—no errors due to relief displacement are removed. If, however, two half-silvered mirrors are used, appropriate manipulations permit true orthographic plotting of detail from the stereoscopic model. Scale adjustments between photographs and map base are made by interchanging special lenses in the viewing assembly together with changing manually the distance of the viewing assembly above the map base. The instrument is said to permit measurement of altitudes when coupled rotary prisms are inserted under the half-silvered mirrors, or when a device similar to the multiplex tracing table is placed in the field of stereoscopic view (Spurr and Brown, 1945, p. 177).

MEASURING AND PLOTTING DEVICES FOR USE WITH PAPER PRINTS

Some instruments have been designed both for measuring altitudes and for plotting data from paper prints of aerial photographs. These instruments are commonly termed "paper-print plotters" and include the KEK plotter, the Mahan plotter, and the stereotope.

The KEK plotter consists of a stereoscope, two photograph tables, floating-dot assembly, and drawing attachment. The plotting cross of the radial planimetric plotter is replaced in the KEK plotter by the fused dot floating in space. By raising or lowering the photograph plates the fused dot is positioned on the ground in the stereoscopic model. Vertical motion of the photograph plates is linked to a drum scale on which relative altitudes can be read directly in feet. Movement of the pantograph drawing attachment allows geologic detail to be sketched directly on the map base, but during this sketching the fused dot must be held on the ground in the stereoscopic model by simultaneous vertical movement of the photograph plates. The photograph plates may be tilted to make an approximate correction for tilt that may be inherent in the photography. Because the floating-dot assembly lies above and is physically separated from the photograph tables, small amounts of extraneous parallax and significant amounts of horizontal shift in the map position of a point may result by moving one's head in viewing the stereoscopic model.

The Mahan plotter is generally similar in principle to the KEK plotter but differs slightly in operation. The floating dot is positioned on the ground in the stereoscopic model by vertical motion of the disks on which the dots are scribed, whereas in the KEK plotter the position of the disks containing the scribed dots is fixed and the photograph plates are moved vertically in order to position the floating dot at a particular level in the stereoscopic model. The stereoscope of the Mahan plotter is adjustable, which permits very nearly the recovery of the perspective from photography ranging in focal length from about 8.25 to 12 inches. As with the KEK plotter, a shift of the viewer's head when viewing the model may cause horizontal positioning errors and the presence of small amounts of extraneous parallax. The stereoscopic model of the KEK and Mahan plotters may be effectively leveled, in absence of vertical control, by visual reference to certain physiographic features of the terrain (see p. 55).

A somewhat different paper-print plotter is the stereotope. The instrument consists of a stereoscope with binoculars of × 4 magnification mounted over a photoholding assembly that contains a parallax bar and attachments for pantograph hookup, as well as a mechanism, when vertical control is available, for effectively leveling tilted models, for correcting errors of horizontal position, and for orthographic plotting of geologic data (fig. 15). The stereotope is an elaborate instrument that corrects for tilt by mechanical linkages within the photoholding assembly. No physical tilting of the photoholders takes place and thus the instrument differs significantly from the KEK and Mahan plotters. In addition, the targets of the stereometer attachment for altitude determinations are in contact with the paper prints, and no extraneous parallax can be introduced by movement of the operator's viewing position. In the absence of vertical control, which permits tilt correction through mechanical linkages, the stereotope as a measuring device must be used as a simple parallax bar.

MEASURING AND PLOTTING DEVICES FOR USE WITH GLASS-PLATE DIAPOSITIVES

The Kelsh plotter, multiplex, and ER–55 plotter, all of which require glass-plate diapositives, are used in the United States both to measure quantitative geologic data and to plot geologic detail to base maps or control sheets (figs. 16–18). These double-projection precision-plotting instruments are designed to accom-

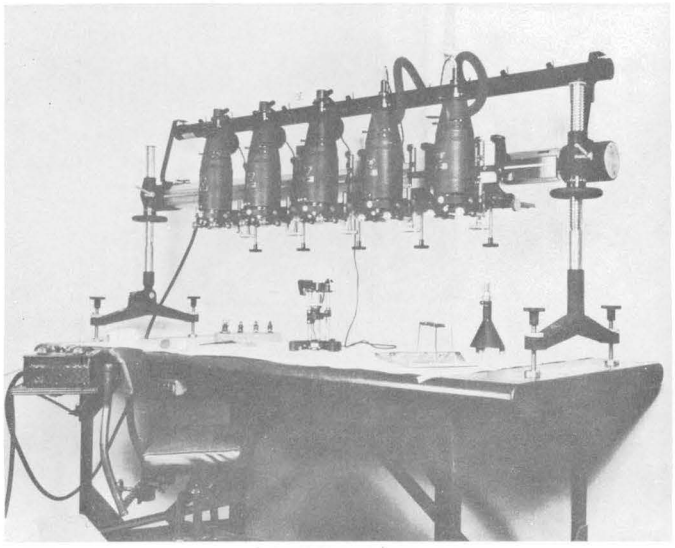


FIGURE 16.—Multiplex.

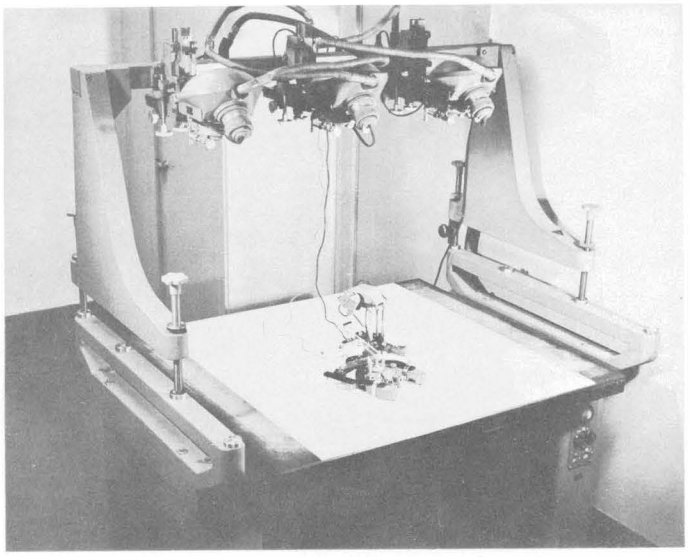


FIGURE 17.—ER–55 plotter.

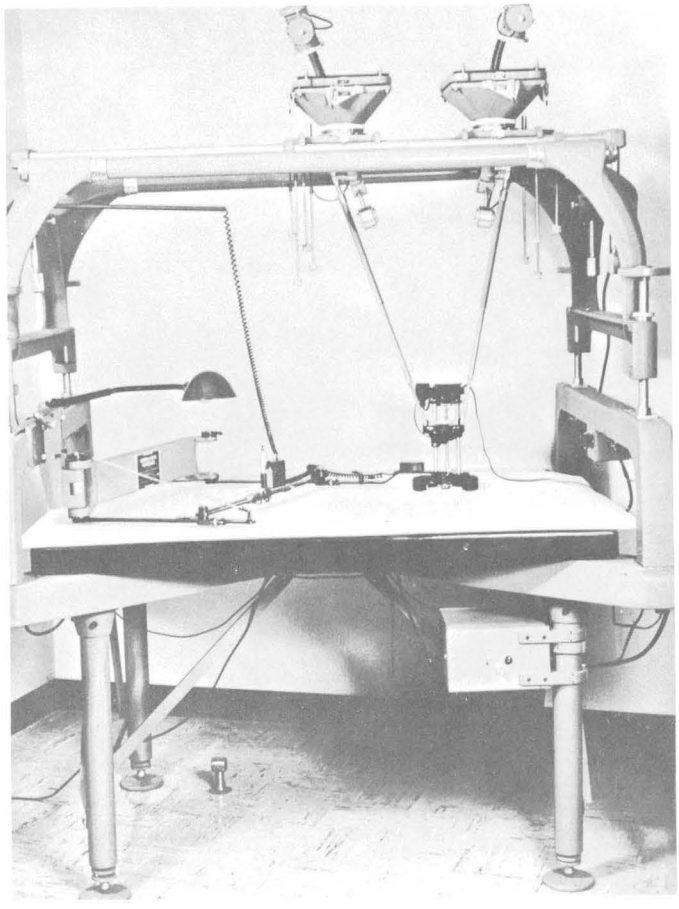


FIGURE 18.—Kelsh plotter.

COMBINED MEASURING AND PLOTTING INSTRUMENTS FOR USE WITH GLASS-PLATE DIAPOSITIVES

modate photography of specific focal lengths, usually 6 or 8.25 inches. All utilize the anaglyph principle of projection of light of complementary colors, red and blue-green, through glass-plate diapositives to create the third dimension. The stereoscopic model is viewed through glasses of the same color as the filters used in the light-source projectors. Because double-projection, or anaglyphic-type, stereoplotting instruments simulate in miniature the spatial relations of the camera stations at the time the photographs were taken, all features of the terrain are optically re-created in the stereoscopic model in essentially true relation with respect to the measuring mark or floating dot. Where sufficient vertical control is available any tilt inherent in the photography can be removed so that accurate measurements of altitudes can be made and true orthographic positioning of detail obtained. Without vertical control the stereoscopic model of many terrains commonly can be leveled within 1° of the horizontal datum by visual reference to certain physiographic characteristics of the terrain (see p. 55); under these conditions approximate orthographic positioning may be obtained, but significant errors in vertical measurements may result (see p. 69–75).

The stereoscopic model is usually viewed on a small white-surfaced table called a platen, which may be raised and lowered so that an illuminated floating dot in its center is kept in contact with the surface of the ground, as seen in stereoscopic view. Vertical motion of the platen is transmitted to a scale reading in millimeters of vertical measurement, or, on some instruments, to a scale that converts readings directly to heights in meters or feet. Geologic features are traced orthographically on the base map by a pencil located directly beneath the illuminated dot on the platen, or by a reduction pantograph attached to the tracing table. Interpretation, measuring, and plotting can be carried out in one continuous operation.

The Kelsh plotter is designed to accommodate glass-plate diapositives the same scale as the original photography. For many geologic problems film positives may be substituted for the more expensive glass-plate diapositives. The scale of the projected stereoscopic model is usually about 5 times that of the original photography. Only that part of the stereoscopic model appearing on the platen is illuminated; this results in a concentration of light and a brightly illuminated model but prevents viewing of the entire model at one time. Because the glass-plate diapositives are the same scale as the original photography the resolution of the stereoscopic image is excellent.

The multiplex uses glass-plate diapositives on which the original 9- by 9-inch negative is reduced about 5 times. The small diapositive image is then enlarged approximately 12 times in projection of the stereoscopic model. The projected stereoscopic model is about 2.5 times the original photography scale. As a result of the large amount of reduction of the original photograph negative, some of the photographic detail is lost and fine details of terrain, important in geologic interpretation, may not be visible. In multiplex projection the entire model area is illuminated, and if the terrain being viewed has only low or moderate relief the stereoscopic model may be observed in its entirety by substituting a large white surface for the platen. This overall view of the stereoscopic model is often of considerable use in geologic interpretation, because of the association of geologic features that can be seen at one time. The overall view is generally accomplished by projecting the stereoscopic model to the multiplex table slate; no plotting or measuring can be done when the model is viewed on this surface.

The ER–55 plotter uses glass-plate diapositives on which the original 9- by 9-inch negative is reduced about 2.8 times; this amount of reduction does not seriously affect image resolution. The projected stereoscopic model is about 3.5 or 5 times the scale of the original photographs, depending on the projector model. Ellipsoidal reflector-type projectors result in a brightly illuminated model in which terrain detail has a high degree of resolution. Like the multiplex, the ER–55 plotter permits viewing the entire stereoscopic model at one time. In addition to accommodating vertical photography the ER–55 projectors are adaptable to twin low-oblique photography taken with the camera axis inclined 20° from the vertical position.

Geologic study of stereoscopic models in double-projection plotters has numerous advantages over the study of paper prints. The ability to interpret, measure, and plot in one continuous operation has already been cited. In addition, the geologist works with an enlarged stereoscopic model that ranges from about 2.5 times to 5 times the original photography scale, depending on the instrument used; thus small-scale photography commonly may be used. A higher degree of image resolution is maintained on glass diapositives than on paper prints, and results in more detail that can be observed in the double-projection stereoscopic models, except for the multiplex, in which some resolution needed in qualitative and quantitative interpretation is lost in the projected model. Because all features of the terrain are optically re-created in essentially true relation, reliable measurements for structure contouring, for drawing isopach lines, for computing strikes and dips, and for determining fault displacements can be obtained for many areas with stereo-

scopic plotters; measurements can be made rapidly and hence economically (see Pillmore, 1957).

OTHER INSTRUMENTS

Other photogrammetric instruments such as the stereoplanigraph and autograph permit precise measurements from aerial photographs, but these heavy plotters are generally unavailable to the geologist. Beside permitting precision of measurement, these instruments are designed to accommodate different sizes of diapositives and photography taken with different focal-length lenses.

Certain modifications or additions to existing instruments have been made specifically for geologic purposes; and some new instruments, described below, have been designed expressly for geologic study.

EXAGGERATED-PROFILE PLOTTER

The exaggerated-profile plotter is a device attached to the tracing table of double-projection plotters, such as the Kelsh, multiplex, and ER–55 plotters, for drawing terrain profiles. As the tracing table is moved along the line of profile and as the platen of the tracing table is moved vertically a pencil attachment records the profile on a vertical tracing board. Profiles exaggerated as much as 5 times may be plotted. An arm on the tracing table slides in a groove along the base of the tracing board so that a selected cross-section direction is maintained. Two models of the exaggerated-profile plotter have been developed. One is based on the lever and fulcrum principle (fig. 19); the other is based on the pantograph principle (fig. 20). The exaggerated-profile plotter was first developed to aid in solving a specific geologic problem in correlating thin and closely spaced intraformational sandstone beds in rocks of Cretaceous and Jurassic age in Wyoming (Pillmore, C. L., oral communication, 1958). The plotter may be very useful also in quantitative geomorphic studies or in studies involving the qualitative correlation of shape characteristics of terrain.

INTERVAL-MEASURING DEVICE

A floating-dot instrument that permits the maintenance of a desired vertical interval between two floating dots in a stereoscopic model from paper prints, as well as serving as a conventional stereometer, also has been developed in the course of photogeologic study (Hackman, R. J., oral communication, 1959). Two floating dots, representing different altitudes in the stereoscopic model, may be useful for example in positioning an obscured formation contact when other contacts are readily observed and formation thicknesses are known. The instrument consists of two transparent circular disks mounted on a frame with two worm screws, one of which permits separation of the disks in the x direction, and the other of which permits both disks to be rotated equally but in opposite directions (see fig. 21). A series of dots, evenly spaced, are arranged in a straight line so as to pass through the center of each disk. One dot coincides with the center of each disk and can be moved only in the x direction, as in most stereometer-type instruments. The other dots may also be moved in the plane of the disk by rotating the disk, thus providing a parallax ladder as seen stereoscopically. By proper adjustment a pair of dots, one on each disk, can be separated by rotation of the disks to provide a direct-reading parallax ladder, or the dot separation may be referred to millimeters of parallax and differences in altitude calculated in the usual manner (see p. 53). The center dots of each disk can be floated in the stereoscopic model at a desired point and the distance above or below this point measured merely by rotation of the disks. Scales graduated to record hundredths of millimeters of parallax permit readings of separation of the center dots of the disks as well as reading of total x parallax resulting from rotation or x motion of the disks.

UNIVERSAL TRACING TABLE

Some research in development of instruments carried out to date has centered around the modification of existing instruments. Important in this group is the universal tracing table (fig. 22), which is a multiplex tracing table that has been modified in design by R. H. Morris and C. L. Pillmore of the Geologic Survey. It is used for direct measurement of inclined distances, such as stratigraphic thickness of dipping beds, in stereoscopic models from double-projection plotters. The platen and underlying assembly can be tilted as much as 45°. A separate worm-screw drive on the tilted assembly distinct from the conventional worm-screw drive for vertical movement, permits movement of the platen in an inclined direction perpendicular to the surface of the platen. A scale on this auxilliary worm-screw-drive assembly permits the reading of measured intervals in hundredths of millimeters; conversion to feet is made in the usual manner for double-projection stereoscopic models (see p. 54–55). A series of holes drilled through the platen to the underlying light source provides a plane of floating dots in the stereoscopic model.

MEASUREMENT

PRINCIPLES OF VERTICAL MEASUREMENT

Vertical measurements of altitude differences provide by far the greatest amount of quantitative information in geologic interpretation from aerial photographs. Differences of altitudes are generally deter-

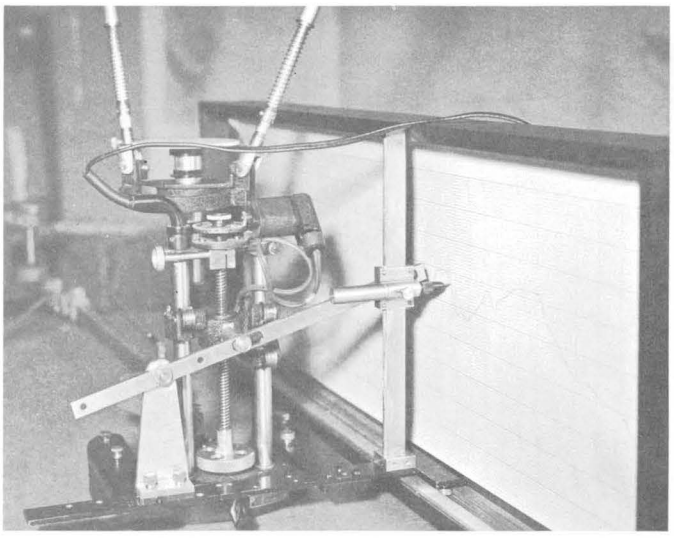


FIGURE 19.—Lever and fulcrum type of exaggerated-profile plotter.

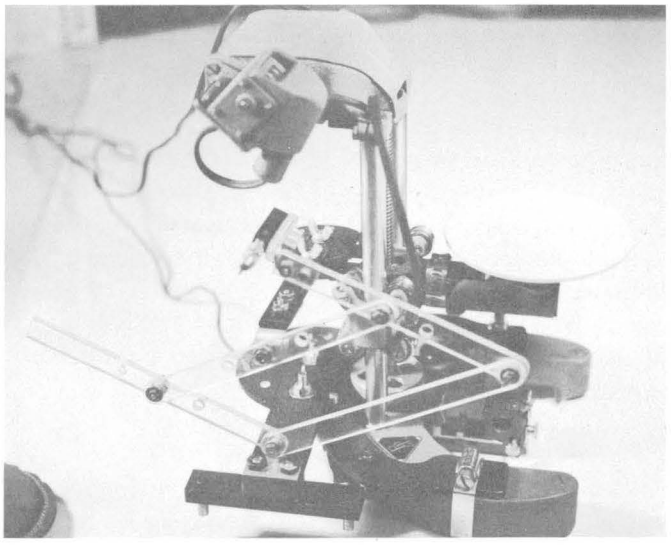


FIGURE 20.—Pantograph type of exaggerated-profile plotter.

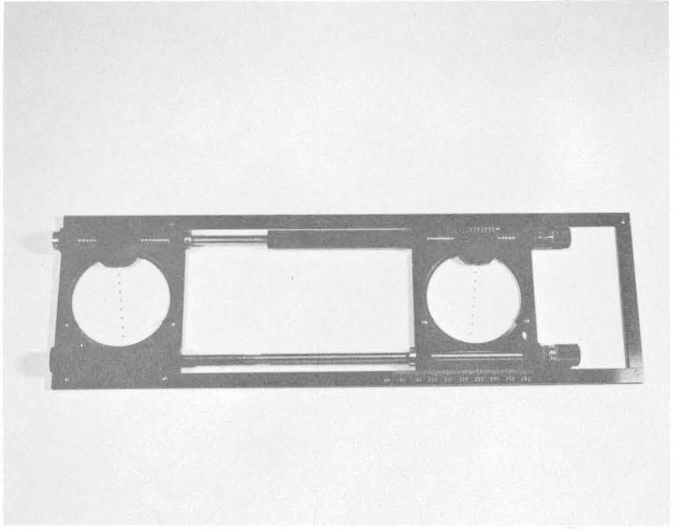


FIGURE 21.—Interval-measuring instrument.

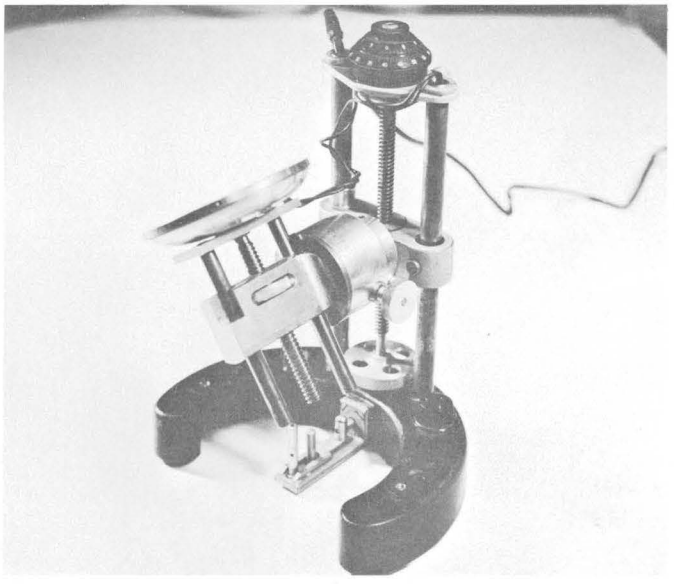


FIGURE 22.—Universal tracing table.

INSTRUMENTS DESIGNED OR MODIFIED FOR GEOLOGIC USE

mined from overlapping aerial photographs, although they may under special circumstances be determined from a single photograph. When overlapping prints are used, the altitude difference between any two points is determined by measuring the horizontal linear parallax difference between the two points and relating it to appropriate geometry of the stereoscopic model. Altitude determinations from glass plates in double-projection plotters require the measurement of actual vertical distances within the stereoscopic model. In the uncommon circumstance when a single photograph may be used, altitudes are determined by measuring relief displacement and relating it to appropriate geometry of the aerial photograph.

DETERMINATION OF ALTITUDE DIFFERENCES BY THE PARALLAX METHOD

When an object is viewed or photographed from two different positions, as on two overlapping vertical aerial photographs, an apparent shift in the position of that object takes place, which is known as parallactic displacement. On overlapping aerial photographs this is a measurable linear distance that is directly related to the height of the object. In photogrammetric terms parallax of an image point appearing on two overlapping photographs is called absolute stereoscopic parallax and is represented by the algebraic difference, parallel to the flight line, of the distances of the conjugate image points from their respective principal points (see fig. 23). The difference in absolute stereoscopic parallaxes between two different image points is a measure of the distance one point is above the other. On overlapping paper prints the parallax difference may be measured reliably by using a stereometer-type instrument, based on the floating-dot principle; parallax difference may also be measured with a ruler, although this procedure is rarely used because of inaccuracy of measurement.

In double-projection stereoplotting instruments (Kelsh, multiplex, and ER–55 plotters) an actual vertical measurement of altitude difference is made within

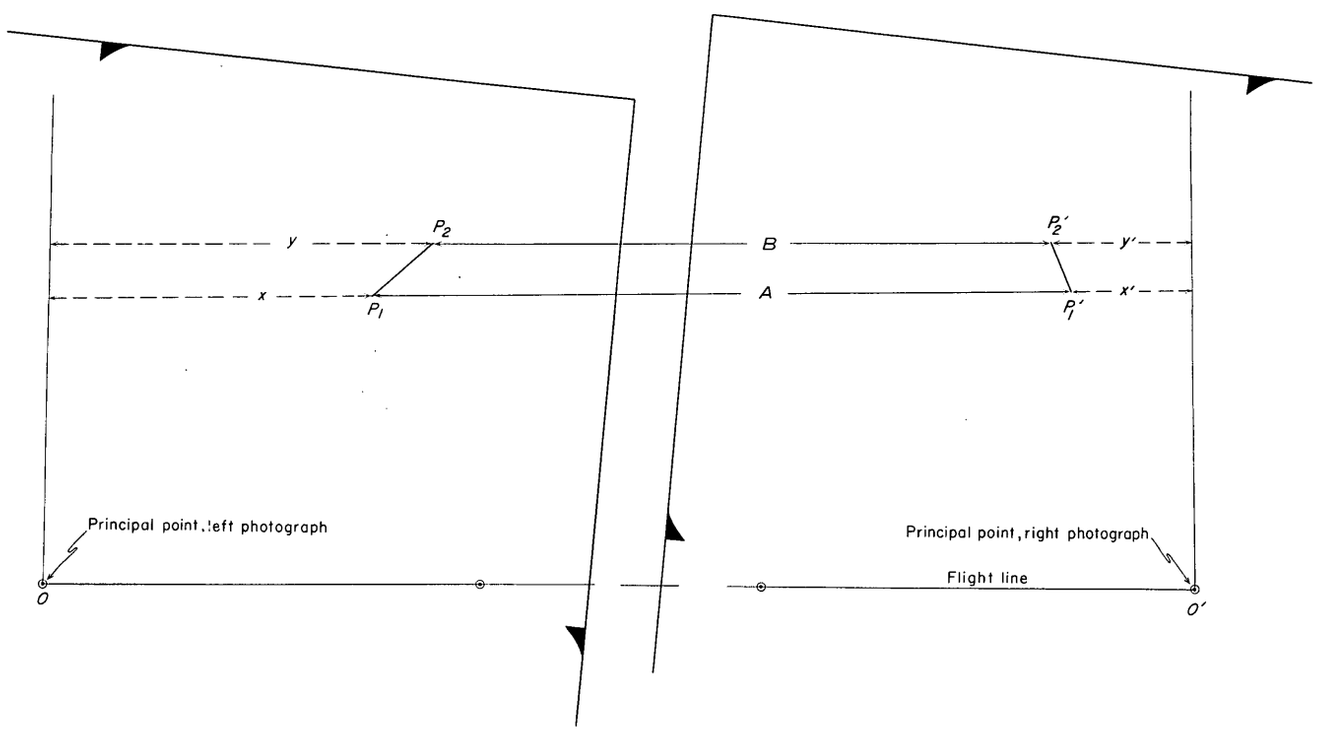


FIGURE 23.—Diagram showing relation between absolute stereoscopic parallaxes and horizontal distances actually measured with stereometer-type instruments in determining differences in altitude from paper prints.

Let images P_1'–P_2' and P_1'–P_2' represent the photographic expression of a pole on the left and right photographs of a stereoscopic pair. The absolute stereoscopic parallax of the base of the pole is $x-(-x')=(x+x')$. The absolute stereoscopic parallax of the top of the pole is $y-(-y')=(y+y')$. (Distances measured to the right of the principal point are positive, to the left, negative). The parallax difference between the top and bottom of the pole then is $(y+y')-(x+x')$.

From the figure:

$$y+y'+B=x+x'+A$$
$$y+y'-x-x'=A-B$$
$$(y+y')-(x+x')=A-B.$$

Thus the difference in absolute stereoscopic parallaxes is equal to $A-B$. The distances A and B are the actual distances measured with stereometer-type instruments, generally in hundredths of millimeters, in determining altitude differences from paper prints.

the stereoscopic model; the linear parallax recorded on the photograph is translated into a vertical distance as a result of angular parallax in the viewing arrangement. Figures 23 and 24 show diagrammatically the distances that are actually measured when stereometer-type instruments and double-projection instruments are used respectively in altitude determinations.

USE OF STEREOMETER-TYPE INSTRUMENTS

When paper prints of aerial photographs are used in conjunction with a stereometer-type instrument and a stereoscope, two linear horizontal distances must be measured to obtain the parallax difference between two different image points. These distances are simply A and B as shown on figure 23. They can be measured with a finely graduated ruler but more commonly a

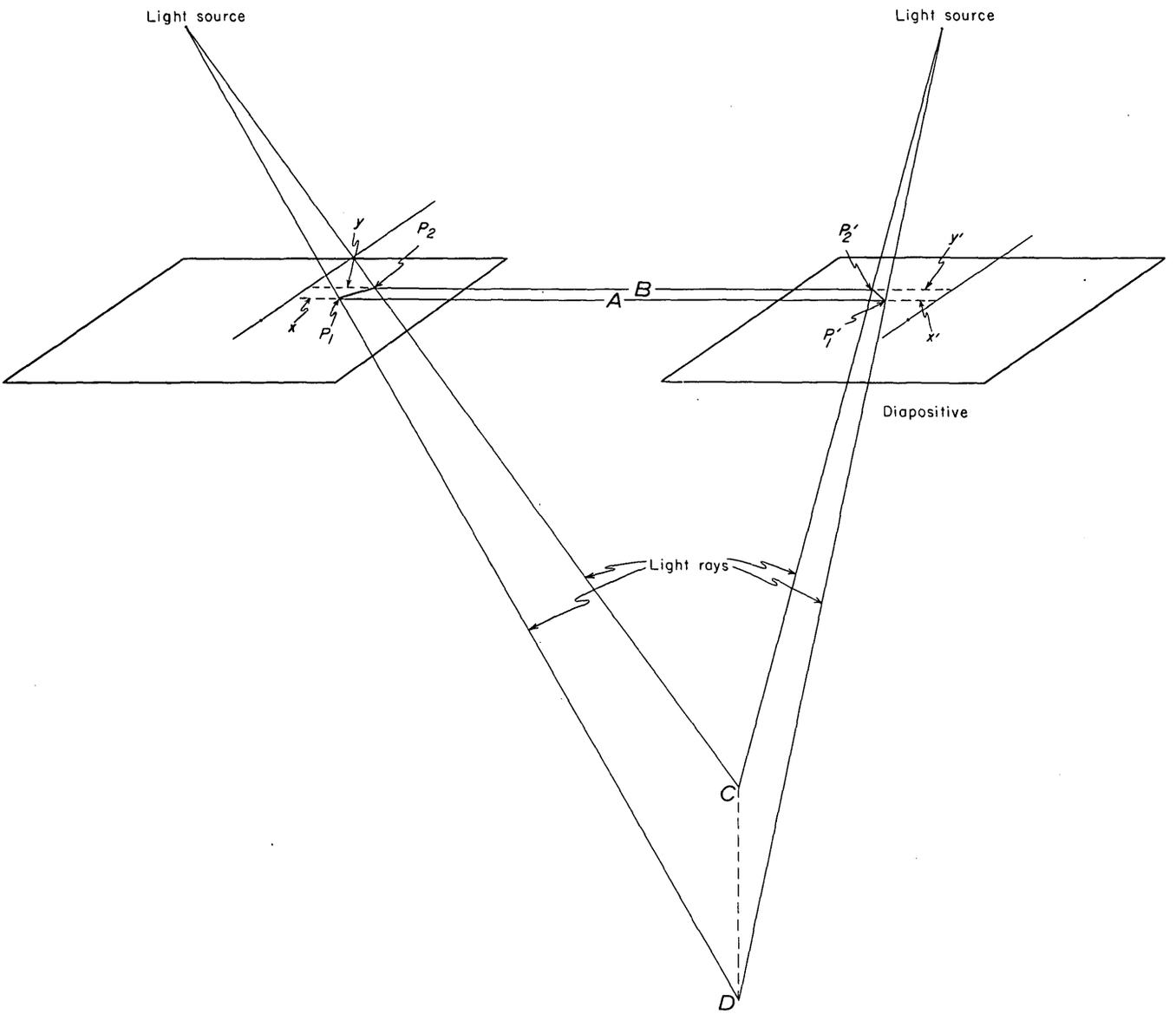


FIGURE 24.—Diagram showing relation between absolute stereoscopic parallaxes and vertical distance measured with double-projection type instruments in determining differences in altitude from glass plates.

The absolute stereoscopic parallaxes of the top and bottom of a pole represented on the left photograph by P_1–P_2 and on the right photograph by P_1'–P_2' are $(y + y')$ and $(x + x')$, as in figure 23, and differential parallax between the top and bottom of the pole is $(y + y') - (x + x')$ *or* $A - B$. With double-projection instruments the vertical distance CD is actually measured, rather than the horizontal distances that are measured on paper prints. The distance CD, measured generally in tenths of millimeters, is converted to feet by multiplying by the K factor, which represents the number of feet on the ground per 0.1 millimeter in the stereoscopic model. Points C and D represent the intersections of those light rays that pass through the top and bottom of the pole respectively.

stereometer-type instrument or parallax bar is used because it permits more consistent readings of smaller increments of length than a ruler. Stereometers are generally constructed with a principal scale graduated in millimeters and a subordinate drum scale calibrated in hundredths of millimeters for recording parallax measurements; a few instruments are designed to record in inches.

To make parallax measurements from aerial photographs it is first necessary to orient the photographs properly for stereoscopic viewing. This is accomplished by alining the photograph centers and conjugate centers along a straight line—the equivalent of the flight-line direction—and separating the photographs for comfortable viewing (fig. 25). Photograph centers are located by marking the intersections of lines drawn between fiducial marks at the opposite sides of each print. Each center is then transferred stereoscopically to the other photograph of the stereoscopic pair and its conjugate image point marked. Parallax measurements are then made in the so-called x direction, parallel to the flight line. Measurement is accomplished by adjusting the separation of the dots of the parallax bar until a single fused dot, seen stereoscopically, appears to rest on the ground at the first point selected. The instrument reading is recorded and the procedure is repeated for the second point selected. The difference in readings is the parallax difference between the two points. In making parallax measurements the fused dot will be seen readily when it floats above the apparent ground surface of the stereoscopic model but will appear to split into its two component dots as it is lowered below the ground surface. If the fused dot, as it is being lowered, appears to split at some point just above the ground surface, a slight change in the separation of the photographs may be necessary to permit simultaneous viewing of the floating dot and the stereoscopic model.

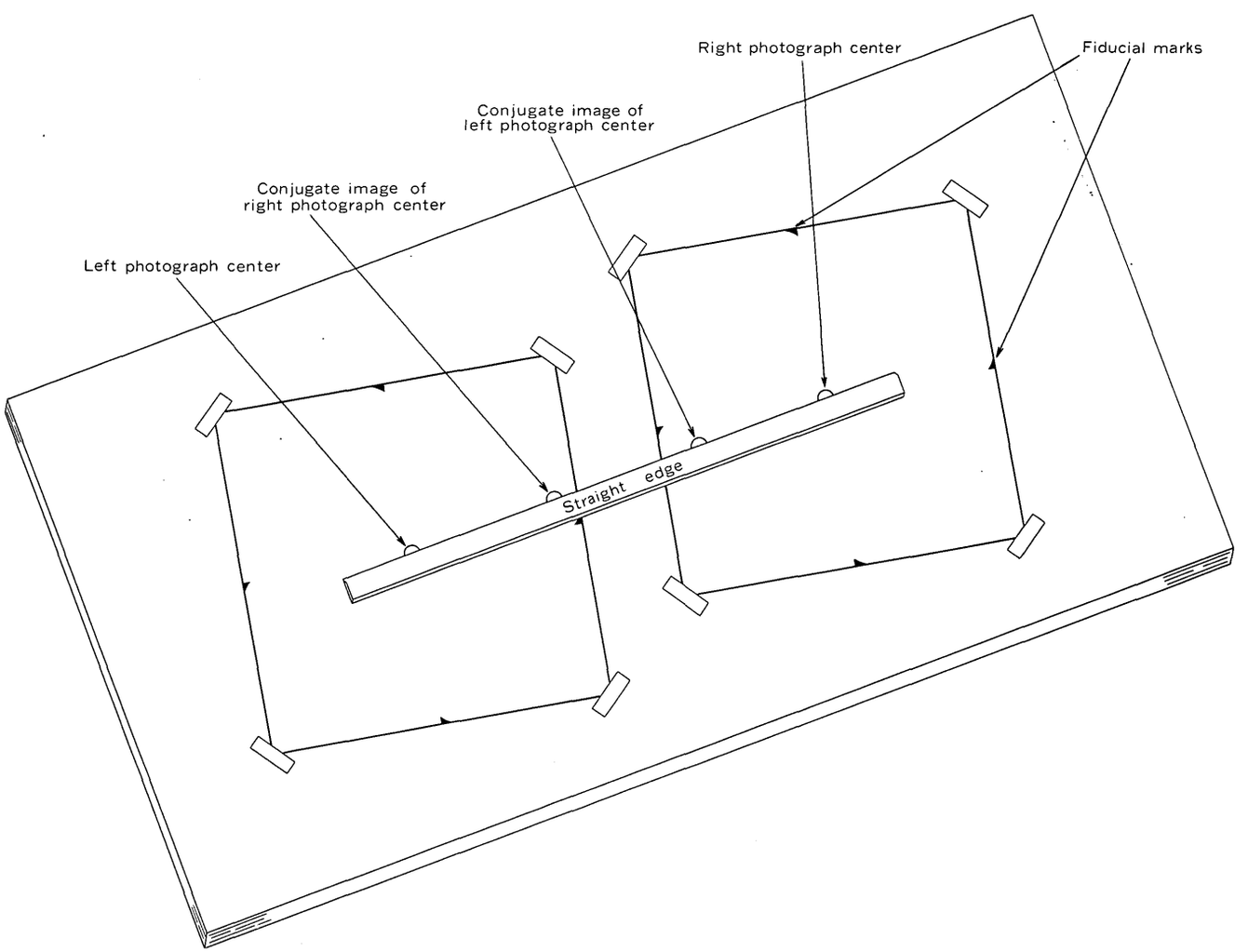


FIGURE 25.—Sketch showing correct orientation of photographs for stereoscopic viewing.

To obtain the height of an object or difference in altitude between two points the difference in parallax must be related to the geometry of the stereoscopic model. For measuring heights from paper prints this relation is best expressed by a formula which, in its simplest terms, is

$$h=\frac{H}{b}\cdot\Delta p \qquad (1)$$

where h=height of the object, in feet, or difference in altitude being determined;
H=height of airplane, in feet, above mean terrain (determined from specifications of photographic mission or relation $H=f/S$, see below);
b=photobase (commonly determined by averaging the distances between the center and conjugate center of each photograph of the stereoscopic pair); units of measure may be millimeters or inches but must be the same as Δp;
and Δp=parallax difference, in millimeters or inches, as determined with stereometer-type instrument (distance A–B of figure 23).

It will be noted that as H increases, the measure of Δp for any given vertical interval will decrease; however, the absolute value for any one unit of Δp will increase correspondingly. On the other hand, if focal length is increased and flying height remains constant the measure of Δp for a given vertical interval will increase but the absolute value for any one unit of Δp will decrease correspondingly.

The above formula (1) may be used without any appreciable error if relief in an area is low; Δp will be small. If relief in an area is high one of the following two formulas, (2) or (3), should be used:

$$h=\frac{H'}{ab+\Delta p}\cdot\Delta p \qquad (2)$$

where h=height of the object, in feet, or difference in altitude being determined;
H'=height of airplane, in feet, above the lower of the two points whose parallax difference has been measured;
ab=photobase adjusted to the lower of the two points whose parallax difference has been measured (commonly determined by measuring the distance between photograph centers—*0–0′* of fig. 23—and subtracting from it the distance between conjugate image points at the lower altitude—distance A of fig. 23); units of measure may be millimeters or inches but must be the same as Δp;
and Δp=parallax difference, in millimeters or inches, measured with stereometer-type instrument (distance A–B of figure 23);

or

$$h=\frac{H'}{ab-\Delta p}\cdot\Delta p \qquad (3)$$

where h=height of the object, in feet, or difference in in altitude being determined;
H'=height of airplane, in feet, above the upper of the two points whose parallax difference has been measured;
ab=photobase adjusted to the upper of the two points whose parallax difference has been measured (commonly determined by measuring the distance between photograph centers—*0–0′* of fig. 23—and subtracting from it the distance between conjugate image points at the upper altitude—distance B of fig. 23); units of measure may be millimeters or inches but must be the same as Δp;
and Δp=parallax difference, in millimeters or inches, measured with stereometer-type instrument (distance A–B of figure 23).

Formula (2) is used when H' and ab are determined by referring to the lower of the two points whose altitude difference is desired, as in measuring upward from the base to the top of a cliff. Formula (3) is used when H' and ab are referred to the upper point, as in measuring downward from the top to the bottom of a cliff. Most commonly the lower of two points is selected as the reference point and measurements are made from that point to some higher point in the stereoscopic model; thus formula (2) is more widely used than formula (3).

Parallax differences generally can be read within small tolerances (see p. 73), and errors in computing differences in altitude result mainly in the determination of flying height and photobase, assuming photographs have little or no tilt. It is therefore generally desirable to determine flying height (H') and adjusted photobase (ab) carefully because a given percentage error in one of them may cause a similar percentage error in the computation of altitude difference. In addition, failure to use formula (2) or (3) when parallax difference (Δp) is large will also cause a considerable error in the final result even though the adjusted photobase (ab) has been carefully determined.

For calculation of absolute heights as is necessary, for example, in determining stratigraphic thickness or displacement on faults, the factor H' may be determined from a base map of known scale or from other control using the relation $H'=f/S$. If the altitude difference between some two points, A and B, is desired

and if neither A nor B falls in a convenient map position for scaling a distance and determinnig H' for one of them, it may be necessary to make parallax measurements with respect to some selected third point, C, for which the flying height (H') can be readily calculated.

Where altitudes are to be used for computing angles of dip it is not necessary to know the absolute height of H'; the tangent relation of angles

$$\text{Tan angle of dip} = \frac{\text{vertical distance}}{\text{horizontal distance}} \qquad (4)$$

involves only relative horizontal distances and relative differences of altitudes, and thus any value may be assumed for H' when measuring parallax difference and determining the scale of the photograph to be used in computing dips. In photogrammetric terms this relation may be expressed as

$$\text{Tan angle of dip} = \frac{\text{flying height (feet)} \times \text{parallax difference}}{\text{horizontal distance on ground (feet)} \times \text{adjusted photobase}} \qquad (5)$$

$$\text{or Tan angle of dip} = \frac{H' \cdot \Delta p}{d \cdot (ab \pm \Delta p)}. \qquad (6)$$

Since

$$\frac{\text{flying height (feet)}}{\text{horizontal distance on ground (feet)}}$$

is also equal to

$$\frac{\text{focal length (inches)}}{\text{horozontal distance on photograph (inches)}}$$

the following formula may also be used to calculate angles of dip when flying height, H', is not known or cannot be determined:

$$\text{Tan angle of dip} = \frac{\text{focal length} \times \text{parallax difference}}{\text{horizontal distance on photograph} \times \text{adjusted photobase}}. \qquad (7)$$

The tangent of dip, in photogrammetric terms, has been described in more detail by Desjardins (1943b, p. 1536–1538) and Elliott (1952, p. 8). When angles of dip are determined from enlarged photographs and formula (7) is used, the effect of photographic enlargement on focal length must be considered; effective focal length is increased in direct proportion to the amount of photographic enlragement (see p. 4).

Hemphill (1958a, p. 43) has devised a chart that shows the number of feet represented by each millimeter of parallax change as H' and ($ab + \Delta p$) of formula (2) vary. The factor determined from the chart is then multiplied by Δp to arrive at h, in feet, provided formula (2) is used. A simple circular photogrammetric computer has also been designed that permits easy computation of the number of feet represented by each millimeter or hundredth millimeter of parallax as flying height and photobase vary. In addition, the computer allows multiplication of this factor by the parallax change to give altitude differences in feet. The number of feet represented by each hundredth millimeter of parallax measured on paper prints may also be determined from the ratio

$$\frac{\text{Flying height (feet)}}{\text{Photobase (millimeters)} \times 100}.$$

This relation is further discussed on page 73.

Need for correct orientation of photographs.—Misorientation of a stereopair of photographs can be considered from the standpoint of rotation around the center of one or both of the photographs. This rotation results in misalinement of the stereopair and flight line. Parallax differences are not then measured in the true x direction, or flight-line direction, but at a slight angle to it; an error in the adjusted photobase also results. The measurement of parallax difference is not normally significantly affected but the adjusted photobase on a stereopair misoriented by a few degrees, even though the human eyes can tolerate a certain amount of error and yet see a well-defined stereoscopic image, may be in error by as much as 5 to 10 percent. This will cause a similar error in differences in altitudes determined by the parallax method when paper prints are used.

USE OF DOUBLE-PROJECTION INSTRUMENTS

When double-projection instruments are used to determine altitude difference between two points, only one distance need be measured. This is a vertical distance within the stereoscopic model that results from the translation of linear parallax recorded on the glass-plate diapositives to angular parallax in the viewing arrangement (fig. 24). The vertical position of intersecting light rays to the lower point to be measured is determined by placing the floating dot on the apparent ground in the stereoscopic model and recording the instrument reading. The vertical position of the upper point is recorded in a similar manner. The difference in readings is a measure of the parallactic displacement and is related to the difference in altitude of the two points. With double-projection instruments measurements are normally made in increments of tenths of millimeters, although some instruments are so designed that selection of proper gear trains permits readings to be converted directly to heights in meters or feet.

In stereoscopic models formed in double-projection instruments the vertical scale remains constant with

respect to the horizontal scale and a simple multiplication factor—called the K factor—for relating increments of vertical measurement to absolute feet can be determined by converting the standard fractional scale (representative fraction) of the model to feet per unit of vertical measurement, that is, per 0.1 millimeter. This is most rapidly accomplished using the formula

$$K=\frac{\text{model scale denominator}}{3{,}048\ (\text{number of tenths of millimeters in 1 foot})}.$$

Thus a stereoscopic model with a scale of 1:4,000 would have a K factor of 4,000/3,048 or 1.31 feet per 0.1 millimeter of vertical measurement. Increments of vertical measurement are merely multiplied by the appropriate K factor to obtain differences in altitude in feet. A constant factor for converting increments of vertical measurement to feet is appropriate because the horizontal and vertical scales are equal and constant throughout the stereoscopic model, but when paper prints are used, the horizontal scale is not constant throughout the model and hence different multiplication factors must be determined for different levels in the model.

Because the horizontal and vertical scales in stereoscopic models from double-projection instruments are equal and constant throughout the model, inclined distances, such as stratigraphic thicknesses of dipping beds, may also be measured. A special device for measuring distances in inclined directions was developed by R. H. Morris and C. L. Pillmore of the Geological Survey; it consists of a multiplex tracing table modified so that the platen, platen socket, and light source can be tilted as a unit (fig. 22). An additional worm-screw drive, separate from the conventional worm-screw drive, allows the platen to move in an inclined direction perpendicular to the surface of the platen. The resulting measured distance within the model is converted to feet in the usual manner, and a measure of the inclined distance is obtained.

TILT

Tilt in present-day vertical photography is generally small—under good flying and photographic conditions 50 percent of the photographs taken for domestic mapping are reported to be tilted less than 1° and 90 percent tilted less than 2° (see Tewinkel, 1952, p. 319). But tilt may be significant in the photogrammetric calculation of many geologic measurements, and care must therefore be exercised in determining altitudes from parallax measurements. The significance of tilt on vertical measurements used in geologic interpretation depends in large part on the geologic problem. Where vertical measurements must be referred to a horizontal datum, as in structure contouring, tilt may cause significant errors, but where relative vertical measurements between pairs of points are desired, as in constructing isopach lines, tilt may have relatively little effect especially where points of any one pair are separated by only a small horizontal distance (see p. 73). If only simple streometers are available for parallax determinations it may be necessary to entirely discard some photograph prints unless (a) vertical control is available and the geologist carries out the tedious task of constructing a correction graph (Desjardins, 1950, p. 2304–2305; McNeil, 1952, p. 610–615; and Visser, 1954, p. 849–853), or (b) points of measurement are selected so that the effect of tilt will be minimized (Hemphill, 1958a, p. 46–47, 49). It is also possible to partially correct for tilt locally on planar orientations, such as the strike and dip of beds, by stereographic projection and appropriate rotations in stereographic constructions.

If photogrammetric instruments are available that allow photographs to be tilted, it is generally possible to eliminate any large amount of tilt (greater than 1°) by careful inspection of physiographic features of the stereoscopic model, thereby permitting reliable parallax measurements to be made even though vertical control is not available for leveling the model. For example, lakes or other standing bodies of water may appear tilted, or certain streams or stream meanders may appear to flow uphill (fig. 109). Tilt is also often detected by observing that headwater tributaries in subdued divide areas where gradients are very low appear to flow uphill. Adjustment of the instrument so that the lakes appear flat and streams have a normal gradient will minimize tilt, and parallax measurements can then be made.

For certain sensitive measurements, such as measurement of low stream gradients or measurements used to determine the strike of low-dipping beds, it is essential that vertical control for leveling models be available and that a precision plotting instrument, such as the Kelsh plotter, be used. Because a small amount of tilt may seriously affect the measure of stream gradient the economic advantage of photogrammetric techniques may be lost where the measure of gradients is the primary photogrammetric objective, inasmuch as a considerable amount of vertical control must be obtained by ground survey to level the stereoscopic models. However, for many geologic measurements, particularly where relative intervals are to be measured, ground control, although desirable, is not essential for making satisfactory parallax determinations, either from paper prints or glass-plate diapositives.

DETERMINATION OF ALTITUDE DIFFERENCES FROM A SINGLE PHOTOGRAPH

Under certain conditions altitude differences between two points may be determined by making appropriate measurements of radial displacement on a single photograph and substituting them in the formula

$$h=\frac{mH}{r}$$

where h=difference in altitude desired;
m=relief displacement of upper image point with respect to the lower image point;
H=height of airplane above lower image point;
and r=radial distance from principal point of photograph to lower image point.

The distance m and r must be measured in the same units. The height, h, will then be in terms of the units chosen for H.

This procedure is only applicable to vertical objects where the upper point is known to be directly above the lower point. Under these restricted conditions, the length of the image of an object, such as a tree, or a cliff face at right angles to a radial line from the principal point, is a measure of the relief displacement. The radial distance to the lower point can be easily measured, and the flying height can be obtained from the formula $H=f/S$ (see p. 53–54) when base maps are available, or from the specifications of the photographic mission. Thus, for example, if the radial displacement of a cliff is 0.03 inch, the flying height of the airplane 10,000 feet, and the lower point is 3 inches from the photograph center, the height of the cliff will be

$$h=\frac{0.03\times 10{,}000}{3.0}$$

$$h=100 \text{ feet.}$$

Because relief displacement is generally small, a small error in measuring such a distance on a single photograph will result in a relatively large error in the height of the object, which further limits the usefulness of the formula for determining vertical intervals.

GEOLOGIC USES OF PARALLAX MEASUREMENTS

Parallax measurements always result in the determination of spot altitudes or vertical intervals when papers prints are used; and generally result in spot altitudes or vertical intervals when glass-plate diapositives are used in double-projection instruments, except when a special tracing table is used that permits measurement of inclined distances (fig. 22). These spot altitudes and differences in altitudes combined with horizontal distances determined from the stereoscopic model, or under some circumstances from a single photograph, may be used to compile structure-contour maps and to determine dips of beds, thicknesses of beds, offsets on faults, gradients of streams, and related data.

Because of relief displacement, however, it may be necessary to correctly locate the relative horizontal positions of points, whose altitudes have been measured, before computing strikes and dips, determining stratigraphic thicknesses, or any other geologic measurements where dips are involved. Because tilt is usually negligible in present-day photography, horizontal positions of points generally may be plotted satisfactorily with any instrument that removes relief displacement, such as the radial planimetric plotter, paper-print plotters, and double-projection plotters even though the stereoscopic model cannot be leveled. Horizontal distances may then be scaled off. However, in the absence of plotters for locating the relative map positions of radially displaced points when measurements are made with parallax bar and paper prints, an overlay or similar procedure may be used to determine corrected horizontal distances, unless orthophotographs (see page 69) are available from which correct horizontal distances may be scaled.

The overlay procedure requires first laying out on transparent material a line equal in length to the adjusted photobase. The overlay is then placed over the right photograph of the stereoscopic pair so that the line drawn is coincident with the flight direction and its right end terminates at the photograph center. Radial lines are then drawn on the overlay from the photograph center through all points whose relative horizontal positions are to be determined. The procedure is repeated with the overlay positioned over the left photograph, again with the original line coincident with the flight direction and its left end terminating at the photograph center. The intersection of a pair of lines through the same image points is the corrected horizontal position for that point.

DETERMINING STRIKES AND DIPS

Where bedding surfaces coincide with topographic surfaces it is generally sufficient to measure the altitude difference between only two points, one directly downdip from the other in calculating the amount of dip. The horizontal distance between these two points, together with the difference in altitude, gives the required information for determining the angle of dip from the trigonometric relation

$$\frac{\text{Vertical distance}}{\text{Horizontal distance}}=\text{tangent of angle dip.}$$

If relief in an area is low the horizontal distance may be scaled directly from a single photograph with-

out significant error in computing the dip, but where relief is moderate or high a correction for the relief displacement of the upper point with respect to the lower point generally should be made. In the unique circumstance where the strike is radial from a photograph center or where the surface on which the dip to be measured is at or near a photograph center, there is little or no relief displacement in the dip direction, and no correction in scaling the horizontal distance need be made. Hemphill (1958a, p. 53) suggested that the corrected horizontal distance between the upper and lower points should be at least 0.2 inch for computing dip angles. Where dips are greater than 50°, a longer horizontal distance is needed to determine the dip angle reliably, as the tangent increment per degree of dip is significantly greater for steep angles of dip than for low angles of dip.

The strike line generally can be determined readily by inspection of the stereoscopic model and noting two points of equal altitude on a bed. Where dips are low, however, tilt in the photographs will affect the direction of strike; the lower the dip, the greater the effect, generally, on the amount of shift in the azimuth of the strike line. Graphs may be constructed to show the effect of tilt on low-dipping beds. (See Hemphill, 1958a, p. 48.)

Where a bed crops out in a valley wall it will generally be necessary to determine the altitudes of three points on the bed. In areas of moderate or high relief corrections for relief displacement must be made before distances between these points can be determined; otherwise distances may be scaled directly from the single photograph. Determination of the strike direction and amount of dip are then made graphically or graphically and trigonometrically.

DETERMINING STRATIGRAPHIC THICKNESS

In areas where beds are horizontal or nearly horizontal the stratigraphic thickness may be determined directly by converting to feet the parallax difference between the top and the bottom of the bed. No correction is necessary for relief displacement. However, if beds are inclined, the angle of dip must first be determined; then corrections must be made for relief displacement and for the effect of dip on the stratigraphic thickness. The thickness may be calculated by simple trigonometry or by graphic solution (fig. 26).

Desjardins (1950, p. 2308–2309; 1951, p. 829–830) suggested that floating lines be employed with paper prints for determining stratigraphic thicknesses where beds do not dip more than 15°. In the "floating line" procedure, lines are drawn on transparent strips of

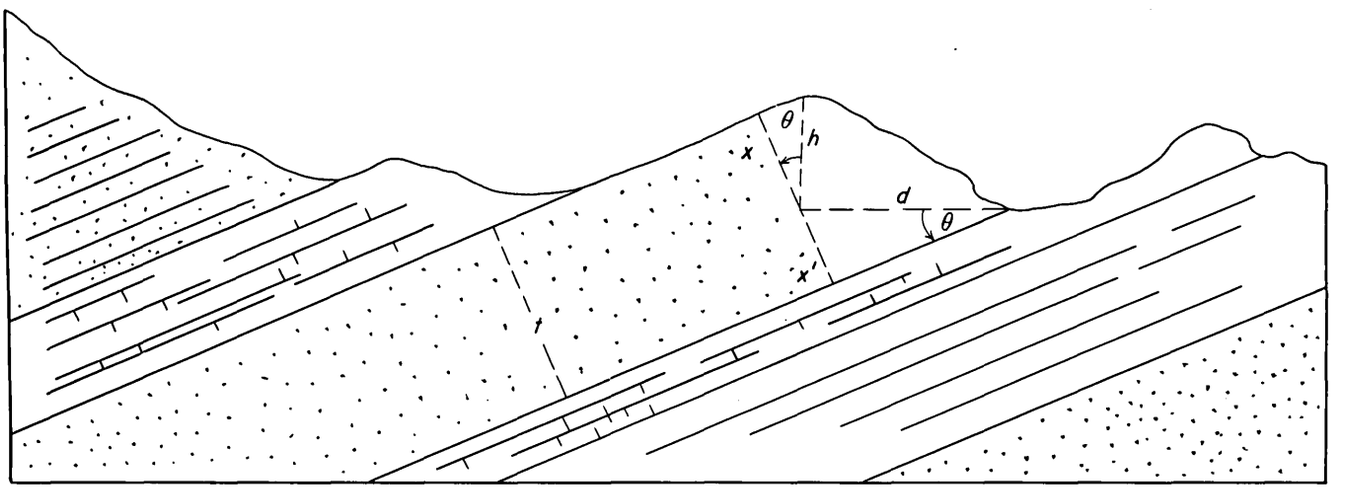


FIGURE 26.—Diagram of gently dipping beds showing relation of stratigraphic thickness to differential parallex determined at any two points along dip direction and at the formation contacts.

Stratigraphic thickness is determined from the formula

$$t = x + x' = \frac{h}{\cos\theta} + \frac{d}{\sin\theta}$$

where t = stratigraphic thickness;
h = difference in altitude between some point on the lower contact of the bed and some point, along a line at right angles to the strike line, at the upper contact of the bed; altitude h is determined from the parallax formula;
d = corrected horizontal distance between points at lower and upper contacts of the bed;
and θ = angle of dip.

material that are superposed over each of the photographs. When one line over one photograph is positioned parallel to a line over the second photograph, a single floating line will appear when viewed streoscopically unless the lines are parallel to the flight direction. The line will float above or within the model and appear to be horizontal; its vertical position in the model will depend on the separation of the two individual lines in the flight direction. A series of lines will form a grid or reference plane (Smith, H. T. U., 1943a, p. 171; Desjardins, 1943a, p. 219; Hackman, 1957, p. 593). When any one pair of lines is divergent rather than parallel the floating line in the stereoscopic model will appear to plunge. By changing the horizontal separation of any two lines in the flight direction the floating line can be made to rise or fall in the model, just as with the floating dot of the parallax bar. When the floating-line procedure is used in measuring stratigraphic thicknesses, a line is first floated preferably in the bedding plane at the upper formational contact, and parallax measurements are then made at the lower formational contact and on the floating line at a position in space vertically above this point (see fig. 27). If beds are horizontal or nearly horizontal the parallax difference will be approximately a measure of the stratigraphic thickness. If the beds dip, the stratigraphic thickness will bear a cosine relation to the dip angle and parallax measurement (see fig. 27).

Where dips are steep it may be desirable to measure a horizontal distance along a line at right angles to the strike direction between two formation contacts and relate this distance and dip angle to stratigraphic thickness. Points must be chosen at approximately the same altitude in the stereoscopic model (fig. 28).

ISOPACH MAPPING

The use of aerial photographs in studies of certain areas in the Colorado Plateau of Western United States has included the photogrammetric compilation of isopach maps that show local thickenings of certain formations in which uranium minerals are likely to occur. These thickenings of formations are channel-fill deposits in stream channels that were cut in the underlying formation. Uranium minerals are locally concentrated in these deposits. In the Monument Valley area of southern Utah it has been demonstrated that isopach lines, indicating the trends and thicknesses of different channel-fill deposits, could be drawn

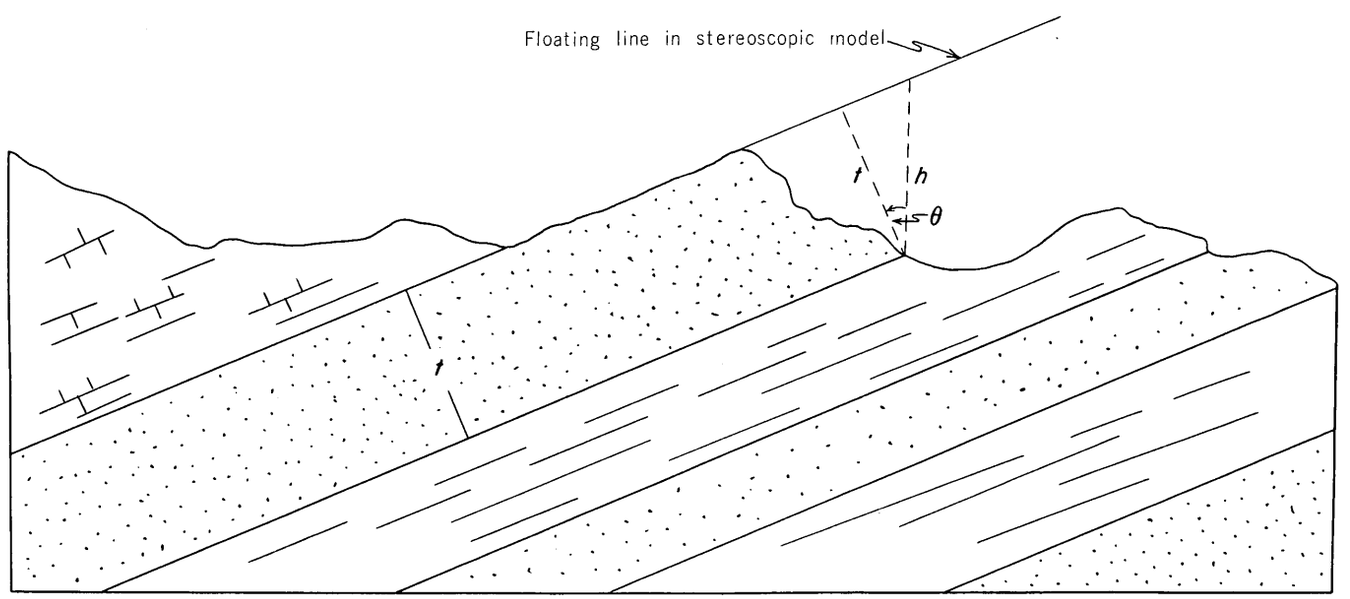


FIGURE 27.—Diagram of gently dipping beds showing relation of stratigraphic thickness to differential parallax determined by floating-line method.

Stratigraphic thickness is found from the formula

$$t=\frac{h}{\cos\theta}$$

where t=stratigraphic thickness;
h=difference in altitude between bottom of bed and point on floating line vertically above, as determined from the parallax formula;
and θ=angle equivalent to angle of dip.

on the basis of measurements made on vertical aerial photographs. In this area uranium minerals are present in channel-fill deposits at the base of the Shinarump member of the Chinle formation of Triassic age. However, because the top of the Shinarump member is eroded away in many areas, or because it is gradational with the overlying member of the Chinle formation, a stratigraphic unit below the Shinarump member was chosen as the unit for which isopach lines were drawn. A thinning of this underlying unit then was interpreted to indicate a thickening of, or channel deposits of, the overlying Shinarump member. The unit selected for isopach measurements, the Moenkopi formation, is expressed on aerial photographs as a dark-toned slope-forming unit that contrasts markedly with the light-toned cliff-forming units of both the underlying De Chelly sandstone member of the Cutler formation and the overlying Shinarump member of the Chinle formation (fig. 44).

A series of altitude measurements was then made along the contact of the Moenkopi and Shinarump formations from aerial photographs by means of the Kelsh plotter, and the locations of these measurements were plotted on a base sheet. Similarly, a series of altitude measurements was made along the contact of the De Chelly and Moenkopi formations and the locations were plotted on the base sheet. Measurements along the respective geologic contacts were generally spaced at horizontal distances of about 500 feet. Because the stratigraphic units dip locally it was necessary to compute the strike and dip of the beds and to correct for the dip angle in determining the stratigraphic thicknesses of the Moenkopi interval. Thickness computations were plotted at the points of altitude measurements along the contact of the Moenkopi and the Shinarump, and isopach lines were drawn at 10-foot intervals on the basis of the distribution of thickness figures. The relatively large number of readings, both for strike and dip of beds as well as for altitude measurements, permitted elimination of certain computations that were inconsistent with regard to the overall mass of statistical data. The locations and depths of channels of Shinarump member as shown by isopach lines based on photogrammetric measurements and plotting were generally in close agreement with those determined by field methods. Details of the photogeologic study are described by Witkind, Hemphill, Pillmore, and Morris (1960).

FACIES CHANGE

Measurements from aerial photographs in conjunction with stratigraphic studies of Cretaceous rocks in northern Alaska have demonstrated the rate and direction of "shaling," or facies change, of certain formations. In the Utukok-Corwin area resistant rocks of the Kukpowruk formation, which is predominantly silty shale, siltstone, and sandstone, overlie less resistant

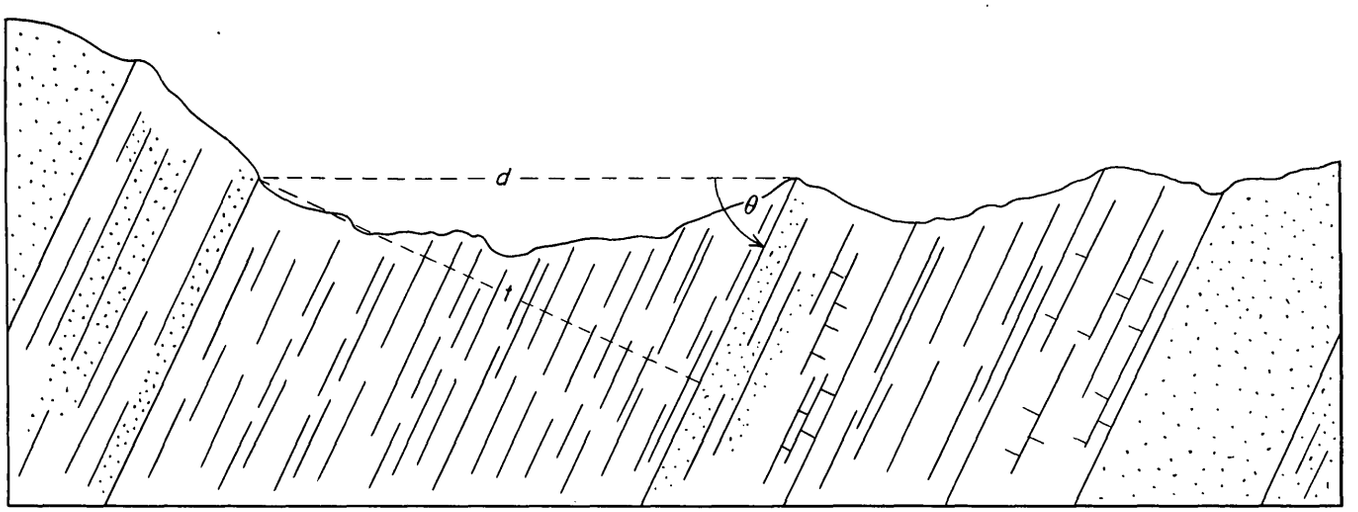


FIGURE 28.—Diagram of steeply dipping beds showing relation of stratigraphic thickness to dip angle and horizontal distance between top and botton of bed.

Stratigraphic thickness is determined from the formula

$$t=\frac{d}{\sin\theta}$$

where t=stratigraphic thickness;
d=horizontal distance at right angles to strike line between points at same altitude on top and bottom of bed;
and θ=angle of dip.

rocks of the Torok formation, which is largely clay shale, claystone, and silty shale. The Torok formation commonly forms the lowlands, which are characterized by rather uniform and low-dipping topographic slopes. The Kukpowruk formation forms high, resistant ridges that can be traced many miles. The contact of the two formations is marked by a break in topography that has been mapped in the field in conjunction with the study of aerial photographs. Slopes below the contact are generally smooth and unbroken; slopes above the contact are marked by conspicuous topographic breaks caused by hard, resistant sandstone beds in the basal part of the Kukpowruk formation. Vertical exaggeration of the stereoscopic model accentuates these topographic breaks in slope. Photogeologic and field studies show that these resistant beds pinch out usually in an easterly or northerly direction (see fig. 97). It is significant that their topographic expression is lost. Ground observations along stream cuts indicate that the resistant beds grade laterally into shaly sections.

Quantitative studies from aerial photographs of the amount of section affected by facies change in the Utukok-Corwin area show that several thousand feet of sandy section of the Kukpowruk formation grade laterally to the east and north into shale of the Torok formation. Chapman and Sable (1960) stated that the methods used in these studies included tracing on vertical aerial photographs a resistant unit within the Kukpowruk formation around the flanks of a large open structure and then measuring the stratigraphic intervals between the resistant bed and the contact of the Kukpowruk and Torok formations to determine the new relative stratigraphic positions of the contact in different parts of the area. Photogrammetric measurements were made whenever possible in localities of good field control; a few stratigraphic thicknesses were determined solely by photogrammetric methods without field control. Locations for measurements were chosen along east-west and north-south lines. Relative stratigraphic positions of the contact of the Kukpowruk and Torok formations were then plotted graphically against lateral distances between points of measurement; this resulted in a line whose gradient showed the average rate of rise of the contact between points of measurement. An average eastward-rising gradient of 58 feet per mile and an average northward-rising gradient of 97 feet per mile were calculated.

It was concluded on the basis of plotting these average gradients as vector quantities that a resultant maximum gradient of 115 feet per mile exists and that more than 10,000 feet of sandy beds grade into shaly sections over the area studied. The maximum gradient direction was further interpreted to lie at right angles to the direction of minimum facies change, which is believed to indicate the general trend of the old shoreline during the period of deposition of the Kukpowruk and Torok sediments. Thus the photogeologic measurement of stratigraphic intervals not only permitted determination of the directions and amounts of facies change, but further allowed inferences concerning the geologic history and environment, which may be significant in the search for petroleum in that area.

STRUCTURE CONTOURING

Structure contours are usually constructed on the basis of a series of spot altitudes, some of which may be photogrammetrically determined at the top of the horizon to be contoured, but many of which will be measured at formation contacts above or below that horizon. Photogeologic procedure is similar to field procedure and requires adjusting the altitudes of all points not on the horizon to be contoured by making appropriate considerations of strike and dip and stratigraphic thickness. Structure-contour lines are then adjusted to the resultant series of altitudes projected to the same formation contact.

NOTOM–15 QUADRANGLE

In photogeologic interpretation and mapping of the Notom-15 quadrangle, Utah, (Hackman and Tolbert, 1955) altitudes for structure contouring were measured using a Kelsh plotter. No previous geologic or topographic mapping had been done in the area; geologic data and altitude measurements were plotted to a control net established by photogrammetric methods. The Notom-15 quadrangle is well-exposed canyon country typical of the Colorado Plateau of Utah. Gently folded sedimentary rocks of Triassic and Jurassic age underlie the area. Canyons transecting the general structure trend made the application of photogeologic procedures ideal. A series of altitude measurements were made along the contact of the Wingate sandstone of Triassic age and the overlying Kayenta formation of Triassic(?) age. The wide exposure of this contact throughout the area permitted sufficient measurements to control structure contouring. Structure contours were then drawn on the top of the Wingate sandstone. Subsequent fieldwork corroborated the general structure as contoured by Kelsh plotter from aerial photographs and also corroborated the distributions of rock formation as interpreted and mapped from photographs. Positioning of other planimetric data, such as streams, was shown to be in excellent agreement with the subsequently compiled standard topographic map of the quadrangle. The positioning of data and altitude determinations by Kelsh plotter thus resulted in a highly reliable geologic map of the area.

DISCOVERY ANTICLINE

Procedures used in contouring the Discovery anticline in northern Alaska included stereometer measurement of altitudes combined with simple trigonometric computations and graphic constructions to compile a generalized structure-contour map (Marshall and Rosendale, 1953). These procedures contrast markedly with the Kelsh-plotter compilation of the Notom-15 quadrangle, but demonstrate that simple methods may be useful in obtaining structural information of a reconnaissance nature from aerial photographs.

Discovery anticline, a gently folded structural feature approximately 25 miles long and 7 miles wide, is underlain primarily by Cretaceous rocks. The area is generally covered with tundra grasses, but resistant beds within the stratigraphic section are expressed topographically as ridges, or breaks in slope, that can be traced for many miles; some beds are expressed by photographic tone due to differences in vegetation (see fig. 40). Dip slopes rarely coincide with topographic surfaces.

Procedures for obtaining and positioning data for structure contouring involved the arbitrary selection of cross-section lines normal to the general structural trend. Strikes and dips of beds were then determined by simple stereometer methods at numerous localities and projected to the nearest cross-section line. Where the strike line did not intersect the line of section at right angles the apparent dip was determined and plotted on the section line. This procedure was followed for all strikes and dips, and resulted in cross-section lines along which the different dips were plotted. A marker bed was then selected and its profile along the line of section graphically reconstructed on the basis of the positions and amounts of dip previously plotted (fig. 29). It was assumed that bedding throughout the stratigraphic section was parallel. Structure contours were then positioned along each line of section by further graphic constructions (fig. 30). However, the datum for each line of section commonly was different, depending on which part of the stratigraphic section was expressed in any one local area, and it was necessary to obtain stereometer measurements of altitudes between cross-section lines so that structure contours, as positioned along each line of section, could be tied together (fig. 31). The resulting reconnaissance map, plotted on an uncontrolled photomosaic, indicated the general magnitude and closure of the anticline and the attitude and steepness of bedding. Figures 29–31 show graphic constructions in reconnaissance structure contouring from measurements made with stereometer-type instruments.

DETERMINING DISPLACEMENTS ON FAULTS

The vertical component of displacement on some faults may be readily determined from parallax measurements made on marker beds on opposite sides of the fault by simple conversion of parallax difference to feet or other appropriate unit of measurement. If the fault plane dips, relative altitudes on marker beds may be related to the down-dip component of displacement by trigonometric or graphic solution.

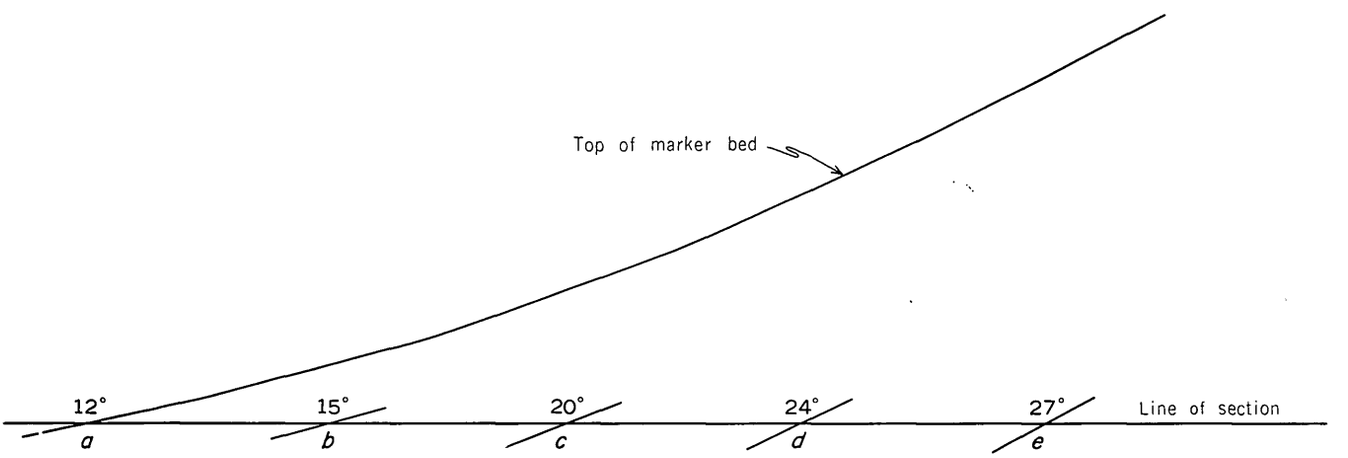


FIGURE 29.—Diagram showing graphic reconstruction of marker bed along line of section.

Dips determined from aerial photographs are first plotted along line of section. The marker bed is then reconstructed by extending bed upward from point *a* at 12° dip for half the distance between *a* and *b*. From this point the bed is extended at 15° dip to a point half the distance between *b* and *c*. From this point the bed is again extended at 20° dip to a point half the distance between *c* and *d*, and so on. A smooth curve is then drawn to represent the marker bed.

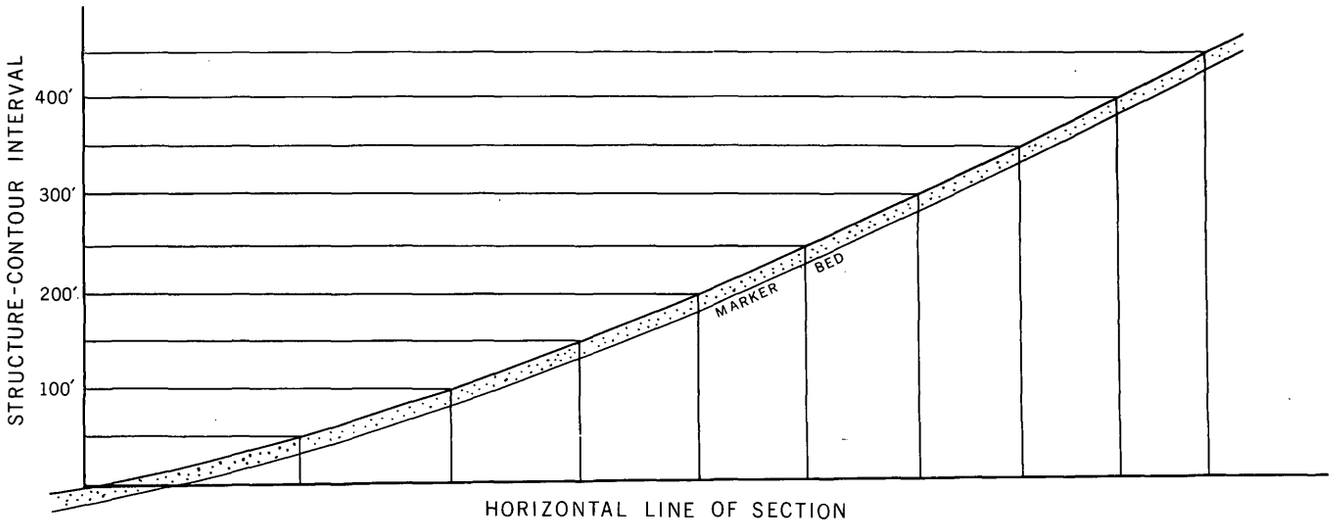


FIGURE 30.—Diagram showing graphic construction in positioning structure-contour lines on top of marker bed and the projecting of these lines to their relative horizontal positions along the line of section.

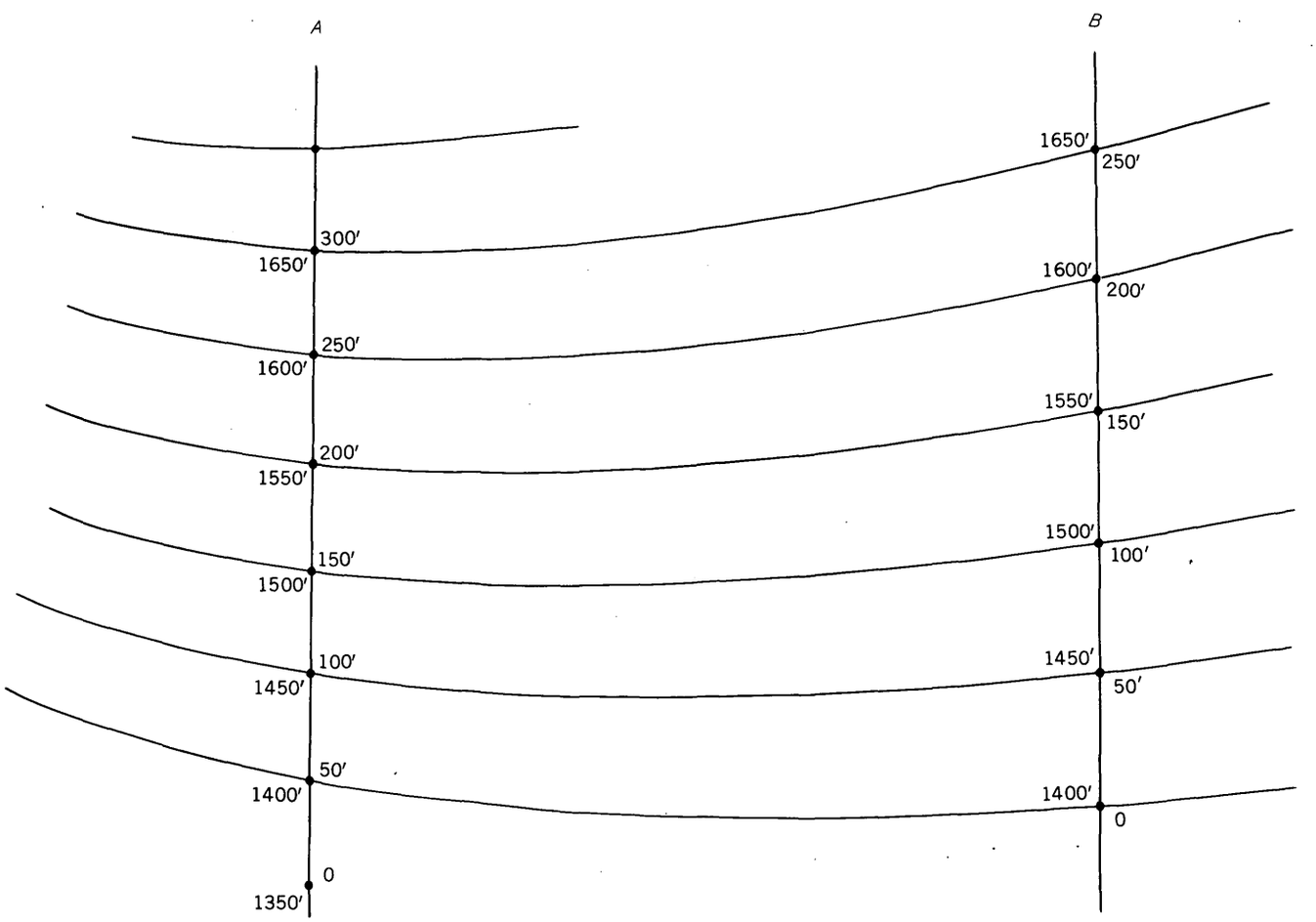


FIGURE 31.—Diagram showing relation of structure-contour positions along two lines of section at different altitudes.

Relative positions of 50-foot structure contours along each line of section are shown to the right of each line. Absolute altitudes of structure-contour positions are shown to the left of each line of section. Because the zero points on the reconstructed marker bed along lines *A* and *B* lie at 1,350 and 1,400 feet, respectively, it is necessary to connect the 50-foot contour position on line *A* with the zero contour position on line *B*, in compiling the structure-contour map.

DETERMINING STREAM GRADIENTS

Stream gradients may be calculated from parallax measurements under certain circumstances. Because many stream gradients are very low—a few feet or tens of feet per mile—an instrument should be used that will permit correction for tilt in the photographs. It will also be desirable to have vertical control for the removal of tilt, as a small amount of tilt not removed from the stereoscopic model could seriously affect the computation of stream gradient. If a stream has a meandering course, then the horizontal distance along the stream between points of measured parallax must be determined by a chartometer or similar instrument for measuring distances along a curved path.

DIRECT DETERMINATION OF SLOPE

DIPPING PLATEN

In addition to the indirect determination of slope by the use of parallax measurements in conjunction with trigonometry or graphic solution, direct measurements of some slopes may be made, both from glass-plate dispositives in double-projection instruments and from paper prints. The simplest procedure is with double-projection instruments and involves the use of a modified platen that can be tilted to coincide with the dip of a topographic surface or bedding plane (fig. 32). Because all features of the terrain are optically re-created in the stereoscopic model of double-projection instruments in essentially true relation, the dip of the platen when made to coincide with the ground surface, or to intersect three or more points on a bedding plane, will be a true measure of the dip of that surface. The dip can be measured with a clinometer attached to the platen or by an accessory device such as a "devil level" or Brunton compass. Dips below 40° can be readily obtained by this method, provided topographic expression or rock outcrops permit positioning of the platen. Dips greater than 40° are difficult to determine owing to the difficulty of positioning the dipping platen in the plane of a steeply dipping surface; steep dips should be computed using the parallax methods described above.

STEREO SLOPE COMPARATOR

A unique method for determining angles of slope from paper prints is employed with the stereo slope comparator (fig. 33), which was developed by the U.S. Geological Survey (Hackman, 1956b, p. 893–898). The instrument consists of two gear housings each containing a horizontal shaft on which small targets are mounted that can be fused stereoscopically into a single target. Swing of the horizontal shafts permits positioning the targets in any direction of strike. The gear housings are mounted on sliding tubes that permit the targets to be separated horizontally so that the fused target appears to rise or fall in space, just as the dot in stereometer-type instruments. However, the dip is determined by physical tilting of the target in space. The instrument is unique in that it measures the exaggerated dip of the imaginary slope created by stereoscopic viewing. With vertical photographs of normal 60 percent overlap, most individuals see the terrain exaggerated in height from 2.5 to 3.5 times. The exaggerated dip, recorded on a protractor attachment on the stereo slope comparator, must be reduced to a true dip. This is accomplished by reference to

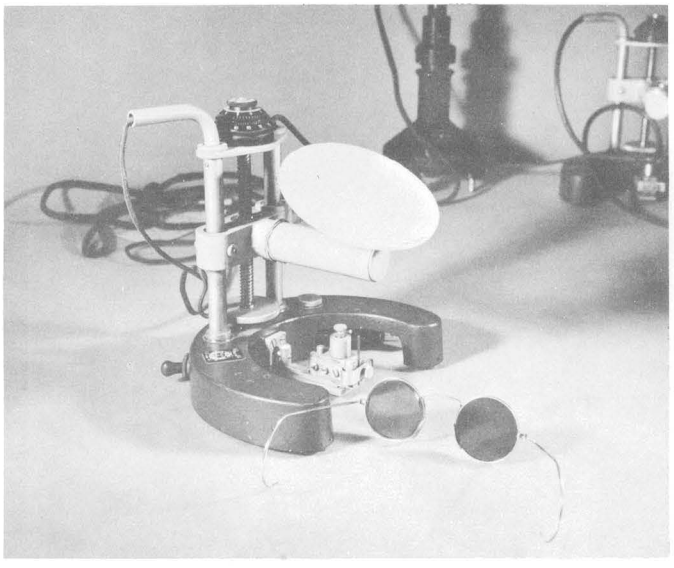


FIGURE 32.—Dipping platen.

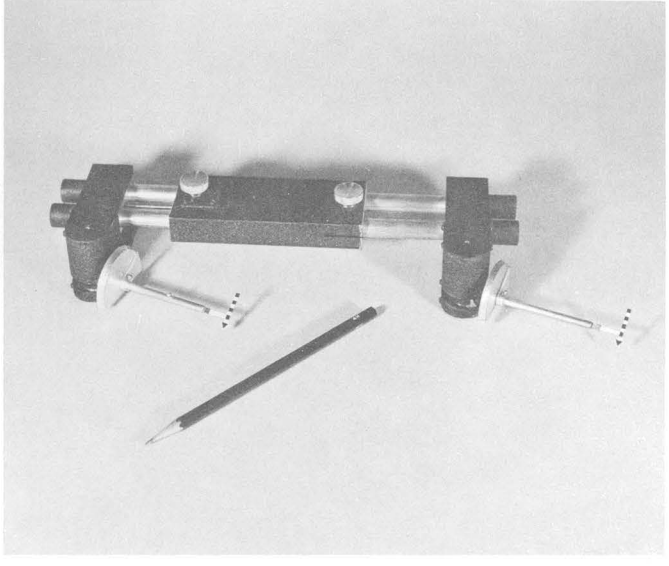


FIGURE 33.—Stereo slope comparator.

INSTRUMENTS FOR DIRECT DETERMINATION OF SLOPE

a slope-conversion graph made up of intersecting lines that represent true angle of slope, exaggerated angle of slope, and exaggeration factor (fig. 34). Construction of the graph is based on the relation

$$\text{Tangent true angle of dip} = \frac{\text{tangent exaggerated angle of dip}}{\text{exaggeration factor}}.$$

In determining dips from a pair of paper prints it is necessary to know the exaggeration factor of the interpreter for that stereoscopic model. This factor varies slightly with different individuals and is determined by reference to a supplementary slope chart on which a dipping surface of specific dip has been constructed by methods described by Hackman (1956a, p. 387–391). By measuring the exaggerated dip of this constructed surface, known to represent a given true angle of dip, an exaggeration factor is obtained; it is then possible to make measurements on a specific pair of photographs and to convert any exaggerated dip to a true dip. Because of the difficulty of placing the tilted target in a steeply dipping plane, the instrument is most reliably used where true dips are 20° or less.

DIP ESTIMATION

From paper prints an experienced interpreter can estimate dips, particularly in the range of 1° to 5°, with considerable reliability, as a result of vertical exaggeration in the stereoscopic model. Because of vertical exaggeration, angles of slope in terms of their tangent functions are exaggerated in the stereoscopic models as much as 2.5 to 3.5 times, with the result that low-dipping surfaces, which are in places difficult to observe in the field, are readily interpreted (figs. 45, 88, 90, 91, and 97). For example, a true dip of 1° may appear to be a dip of 3° or 4° in the stereoscopic model, and a dip of 5° may appear to be 15° to 20°. For true dips below 20° an error of a few degrees in estimating the exaggerated dip has only a small effect on the true dip (see fig. 35), and an interpreter is able to make reliable visual determinations of these dips from most stereoscopic models. But steeply dipping surfaces are also exaggerated and made more difficult to evaluate. Any small error in determining the angle of exaggerated dip of steep slopes results in a relatively larger error in the true dip calculation for that slope. Brundall and Harder (1953, p. 150) stated that "the accuracy of individual estimation is generally inversely proportional to the steepness of dip." In estimating dips a correction obviously must be made for the oversteepened slopes as they appear in the stereoscopic model (see figs. 34 and 35).

Factors affecting vertical exaggeration in stereoscopic models have been discussed by several writers (Treece, 1955; Goodale, 1953; Thurrell, 1953; Miller, 1953; Aschenbrenner, 1952; and Stone, 1951), but complete agreement has not been reached concerning the effects of specific factors such as viewing distance and image separation. However, once an interpreter has correlated amounts of dip, determined photogrammetrically or by field procedure, with a given set of conditions such as type of stereoscope, focal length of photography, photobase, and image separation, reliable estimates of true dip can be made over wide areas without reference to known dips.

OTHER METHODS OF DETERMINING ANGLES OF SLOPES

Another method of determining slopes in stereoscopic models is based on the floating-line principle. Brundall and Harder (1953, p. 150–151) briefly mentioned a device consisting of two lines scribed on plastic plates. The lines, seen stereoscopically as a single line floating within the model, can be made to converge so that the floating line appears to plunge in space. The plunging floating line is placed in the component of dip direction at right angles to the flight line. The angular rotation of the scribed lines required to obtain a given amount of steepness of plunge of the floating line is then related to true dip by means of a graph. As this method would result in true dip only for beds striking parallel to the flight line, the correction graph must also consider the azimuth of the dip component observed with respect to the strike of the beds.

Wallace (1950) has used angular relations in the plane of the aerial photograph as the basis for a method of determining strikes and dips from aerial photographs. The method is best applied where erosion has exposed bedding trace lines as contrasted to broad topographic surfaces that coincide with bedding. No parallax measurements are required. It is necessary to measure the angular relation of two bedding trace lines with respect to a known or assumed azimuth line on each photograph of a stereoscopic pair and to determine the plunge of the line of sight from the camera position to the outcrop, or bedding-trace line. These data are then plotted on a stereographic net to determine the strike and dip of the bed (Wallace, 1950, p. 275).

OTHER METHODS OF DETERMINING QUANTITATIVE DATA

Measurement of geologic data, other than altitudes and direct determinations of slope angles, are only infrequently made from aerial photographs. However, the possible applications of light-transmission measurements, from both black-and-white and color pho-

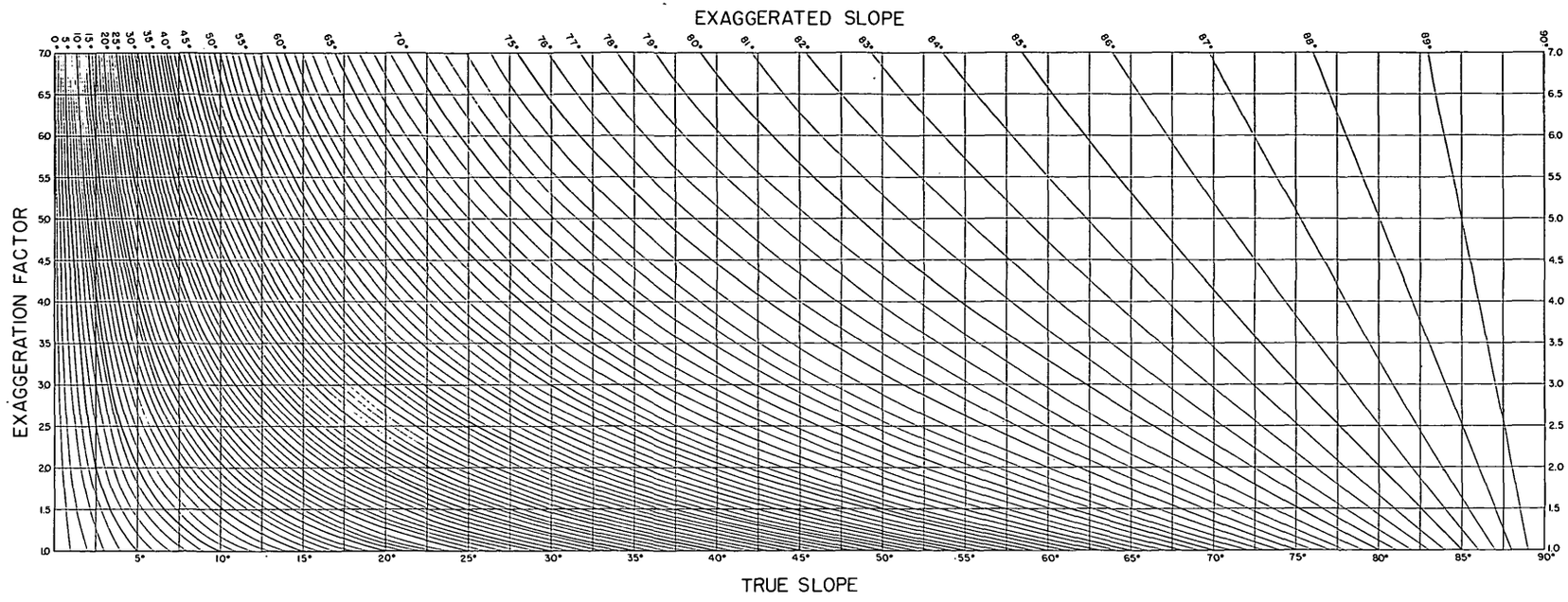


FIGURE 34.—Slope-conversion chart showing relation of exaggeration factor, exaggerated slope, and true slope.

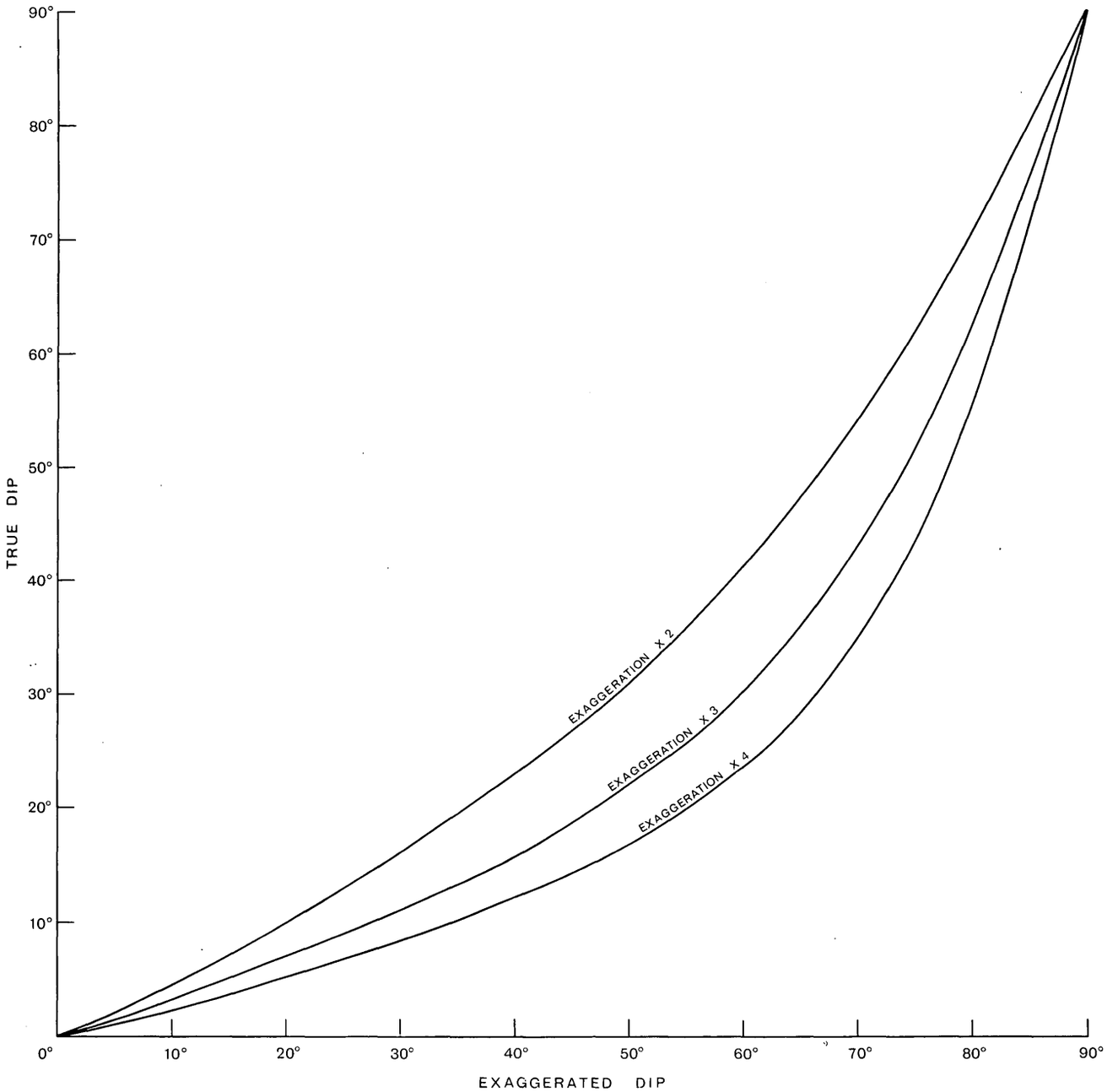


FIGURE 35.—Diagram, based on tangent functions, showing relation of true dips to exaggerated dips seen in stereoscopic models.

tography, light-reflectance measurements, measurements related to heat-retention characteristics of terrain photographed, infrared absorption, size, frequency, and orientation measurements of physiographic features, and perhaps others, offer challenging opportunities for future study (see Ray and Fischer, 1960).

PLOTTING

Map compilation—planimetric positioning of data—is basic to most geologic studies and generally requires methods of plotting data orthographically. Thus, data plotted or interpreted on vertical aerial photographs, most of which are perspective in view, must be replotted on an orthographic base. The orthographic base may be planimetric or topographic. Where no base map exists perspective aerial photographs provide a medium for constructing a control layout on which geologic and other data may be plotted orthographically.

CONSTRUCTION OF CONTROL LAYOUT

A control layout is an orthographic plot of a series of points selected on aerial photographs that cover a given area. These points are used to control the positioning of data plotted from the perspective photograph. Plotting, or transfer, of data from the photograph may be done with simple overhead projectors or sketchmasters under some circumstances, or with stereoplotting instruments described above. The accuracy of the final plot will depend primarily upon the control net and the instrument used in plotting (see p. 74–75).

Basically a control layout or control net is established by triangulation from the aerial photographs in much the same manner as field triangulation is carried out. This aerial triangulation requires mechanical construction of templets which are assembled together into the triangulation network. There are two general methods of constructing templets. One method involves radial triangulation using the principal point of the single photograph as a principal triangulation station to construct radial templets; the other method involves radial triangulation using some orthographically positioned pass point from the stereoscopic model as a principal triangulation station to construct stereotemplets.

Where single photographs are used for triangulation it is generally assumed that the photographs are truly vertical and have no tilt; relief displacement is radial from the photograph centers. However, a tilt of 1° or 2° does not significantly affect horizontal positioning over small areas. Templets from single photographs may be constructed by the hand-templet method, the radial-arm ("spider"-templet) method or the slotted-templet method. Photographs are first prepared by marking the centers, conjugate centers, and selected pass points, usually six in number, along the margins of a photograph; pass points are selected which are common to adjoining flight strips and common to succeeding and preceding photographs within the flight strip. From each photograph, azimuth lines are then constructed from the photograph center through all other selected points to form a templet for that photograph. Azimuth lines may be drawn in pencil on an overlay sheet (hand-templet method); they may be constructed of metal arms ("spider"-templet method), or they may be cut as slots in a piece of cardboard (slotted-templet method). After templets have been constructed for all photographs they are assembled into a triangulation network in which the intersections of azimuth lines locate the orthographic positions of the points selected. The result is a base sheet with a series of points located in their correct relative horizontal positions. Where horizontal control points are available, the distance between plotted positions of any two of them determines the scale of the control layout. Details of constructing and assembling these templets are described by Kelsh (1952, p. 419–429).

Construction of stereotemplets requires the use of a stereoplotting device to plot selected points common to adjoining flight strips and within the flight strip. The templet is actually a double templet of the area of the stereoscopic model rather than the single photograph. Azimuth lines are constructed for each part of the templet using one of the pass points as a principal triangulation station for one part of the templet, and using a different, generally diagonally opposite, pass point as the principal triangulation station for the second part of the templet. These two parts are joined together to form the completed templet for each stereoscopic model. Details of constructing and assembling the stereotemplets have been described by Scher (1955). Because of the longer base line of stereotemplets the resulting triangulation network is said to have a stronger scale solution than can be obtained from radial templets constructed from single photographs. Other photogrammetric advantages are mentioned by Scher (1955).

ORTHOGRAPHIC POSITIONING

PLOTTING ON ORTHOGRAPHIC BASE MAPS OR CONTROL LAYOUTS

The main objective in orthographic plotting of geologic data is to show the true planimetric relations of geologic features by removing relief and tilt displacement that may be present in perspective vertical aerial photographs. Relief displacement is commonly large, but tilt displacement is generally small and is usually disregarded when positioning geologic data on a planimetric base sheet. When positioning geologic data to a topographic base both relief and tilt displacement may be significant and require plotting from a leveled stereoscopic model. For horizontal positioning of data to a planimetric base in areas of low relief the relief displacement will be small; overhead projectors may be used to transfer data from the photograph to base map or control net. For example, with common photography of 1:20,000 scale taken with a 6-inch-focal-length lens, radial displacement near the edge of the photograph will only amount to about 0.1 inch where topographic relief does not exceed 300 feet. Basically relief displacement of a given amount of relief is a function of flying height and is independent of focal length and scale (see p. 74–75).

Where relief displacement is excessive it is possible

553966 O-60—4

to change the photograph scale by racking the overhead projector up and down and, provided base map control is sufficiently dense, to scale small areas of the photograph to the base, thus compensating for much of the radial displacement of the perspective photograph. The reliability of the final plot will be in part a function of the density of control points on the base. The suitability of the final plot will depend on the geologic objective. On most radial triangulation networks it is common to find eight control points, exclusive of the photograph center, for each photograph; this number of points will not normally be sufficient to give a reliable plot of the geologic detail in areas of moderate or high relief unless a stereoplotting instrument is used. The vertical sketchmaster, in which the image of a single photograph is seen superposed on the base map or control sheet, generally is used in the same way that overhead projectors are used in plotting. The same general limitations of the overhead projector apply to the sketchmaster; that is, radial displacement due to moderate or high relief cannot be effectively removed.

Orthographic plotting may also be accomplished with the radial planimetric plotter (fig. 14), or with the more complex paper-print plotters, such as the KEK or Mahan plotters. (See p. 42, 45). The radial planimetric plotter is the simplest to operate. It is easily scaled to control points on the base map or triangulation network and effectively corrects for the radial displacement of vertical aerial photographs. Fine detail, such as the configuration of reentrants in contact lines, may be lost in plotting, however. Tilt inherent in photographs cannot be eliminated, but horizontal positioning due to small amounts of tilt found in present-day photography do not significantly effect horizontal positioning of photographic detail for most geologic interpretations. The KEK and Mahan plotters may also be used to plot geologic data from paper prints. These instruments permit compensation for any inherent tilt that may be present in the photographs but are more difficult to operate than the planimetric plotter.

Whenever paper prints are used in plotting or transferring geologic data to base maps or control sheets it may be desirable to annotate, or mark, the geologic features to be transferred. This is particularly desirable when overhead projectors are used and is usually a necessity for all instruments if someone other than the interpreter is to do the plotting.

Double-projection instruments afford a high degree of reliability in plotting geologic data from aerial photographs. The ability to correct for tilt and relief displacement combined with an enlarged view of the stereoscopic model when the Kelsh, multiplex, or ER–55 plotters are used permits a highly reliable compilation of geologic data. Even when vertical control is lacking, it is possible to remove most of any tilt inherent in the stereoscopic model by careful reference to physiographic manifestations of tilt such as oversteepened or reverse stream gradients, tilted meanders of a stream, or tilted bodies of standing water (see p. 55).

True orthographic positioning is not always attained, however, in geologic compilations from aerial photographs. Not only is there a question at times of the reliability of interpretation because of the subjective nature of much photogeologic study, but the various instruments themselves have differing degrees of accuracy inherent in their construction. Positioning of clearly identified geologic features by overhead projector, which does not permit adjustments for tilt or effective removal of relief displacement, would be far less reliable under most circumstances than positioning by double-projection instruments. However, the geologic product sought should determine in part the procedure to be used in plotting. Normally there is no reason to use an instrument that will plot detail more accurately than is needed to satisfy the geologic requirement. For example, in small-scale reconnaissance mapping, it is hardly necessary to use a precision plotting instrument for horizontal positioning. The problem of instrument requirement in relation to the geologic problem is further considered under a discussion of interpretation and plotting systems (see p. 69–75).

Only where a significant saving in time and money can be shown is it justifiable to use an instrument whose capability exceeds the minimum requirements of the geologic problem. Such a condition may exist for example where small-scale photographs of an area are available. Much of the United States is now covered by photographs at a scale of approximately 1:60,000. The use of such small-scale photographs in an instrument such as the Kelsh plotter may reduce by as much as 90 percent the number of stereoscopic models that would normally be oriented for interpretation, measuring, and plotting if 1:20,000-scale photographs were used. Even when 1:20,000-scale photographs are used with simple instruments the common practice is to separate the operations; that is, the stereoscope is used to interpret geologic detail and another instrument, such as the stereometer, is used to determine vertical measurement. Thus, by using a precision plotter, which combines interpretation, measuring, and plotting, a significant saving in time and money may be expected.

PLOTTING ON ORTHOPHOTOGRAPHS

An orthophotograph is a photograph that has the position and scale qualities of a map. In addition it has the abundant imagery of the conventional perspective photograph and hence a wealth of photographic detail (fig. 47). Theoretically the orthophotograph, with tilt and radial displacement eliminated in preparation (Bean and Thompson, 1957), has the desirable detail of a photograph and the geometric characteristics of an accurate planimetric map. The method of constructing the orthophotograph from double-projection stereoscopic models results in a small loss of photographic resolution, but horizontal positioning accuracy is comparable to that of the standard topographic map of the same scale.

The orthophotograph, when viewed with an alternate perspective aerial photograph, forms a stereoscopic model, although with only a small amount of stereoscopic relief as contrasted to viewing two perspective photographs. In viewing an orthophotograph with a perspective photograph it is generally best to use the same perspective photography as was used in the preparation of the orthophotograph. Combining the orthophotograph with a perspective photograph permits plotting of geologic detail from the perspective photograph to the orthophotograph and gives a reliable photomap. Geologic data on the orthophotograph then can be transferred by direct projection to a topographic or other base, if desired, or merely traced off to give a reliable planimetric map of areas where no base maps exist. As an aid to field geologic mapping, in which a daily plot of observed data is desirable, the orthophotograph may be especially helpful.

The range of potential applications of orthophotography has been summarized by Bean and Thompson (1957, p. 178) who stated that "* * * whenever there is an advantage in being able to determine accurately on an aerial photograph the positions of points, the lengths or directions of lines, the courses of curved lines, or the shapes or areas of given tracts, the orthophotograph offers a potential means of accomplishing the desired end." In addition, as the basis for constructing mosaics the orthophotograph has a significant application, especially in areas of moderate or high relief.

PLOTTING ON GRIDDED BASE MAPS

Gridded base maps may be especially valuable for field plotting of geologic data without the assistance of photogrammetric instruments. In constructing a gridded base map a grid made up of small squares, usually 1 centimeter on a side, is first superposed photographically onto the perspective aerial photograph. The same grid is then orthographically transferred to the base map by a photogrammetric technician using stereoplotting instruments (Landen, David, oral communication, 1958). The grid lines are straight as superposed on the perspective photograph but are curved on the base map (figs. 115 and 116). By dividing the photograph into many small grid squares the effects of tilt and relief displacement become so small as to be negligible within any one square. Information sketched within grid squares on the perspective photograph is transferred visually to the base map by matching grid squares on the photograph with those on the map. The method may be especially useful in the field where it is desirable to keep a compilation of each day's work.

VERTICAL POSITIONING IN CROSS SECTIONS

In addition to the orthographic positioning of photogeologic data on base maps it is commonly desirable to plot geologic cross sections. The third dimension of the stereoscopic model is then added in part to the normal two-dimensional planimetric presentation of geologic information. Vertical positioning of geologic data, as shown in cross section, may be helpful to the geologist interpreting the aerial photographs of an area, as well as to the map reader who may be less familiar with the geology of the area.

Cross sections are easily and rapidly constructed with a profile plotter from streoscopic models in double-projection plotters. Modification of the tracing table permits profiles to be drawn in any direction within the stereoscopic model (figs. 19 and 20). Sections may be drawn at a horizontal-vertical ratio of 1:1 or they may be exaggerated as much as 5 times. When a 1:1 ratio is used, dips of beds or components of dip, stream gradients, thickness of beds, and similar data may be obtained directly from the section. Exaggerated profiles may be desirable where relief of terrain is low, or, for example, when interpreting the significance of vertical position of thin stratigraphic units in correlation studies. Vertical positioning in sections may also show information suggesting the presence of faults.

INTERPRETATION, MEASURING, AND PLOTTING SYSTEMS

An interpretation, measuring, and plotting system (see fig. 36) may be defined as a combination of photographs and instruments that will permit attaining specific qualitative and quantitative geologic information from stereoscopic models. The optimum system is generally achieved by combining the minimum

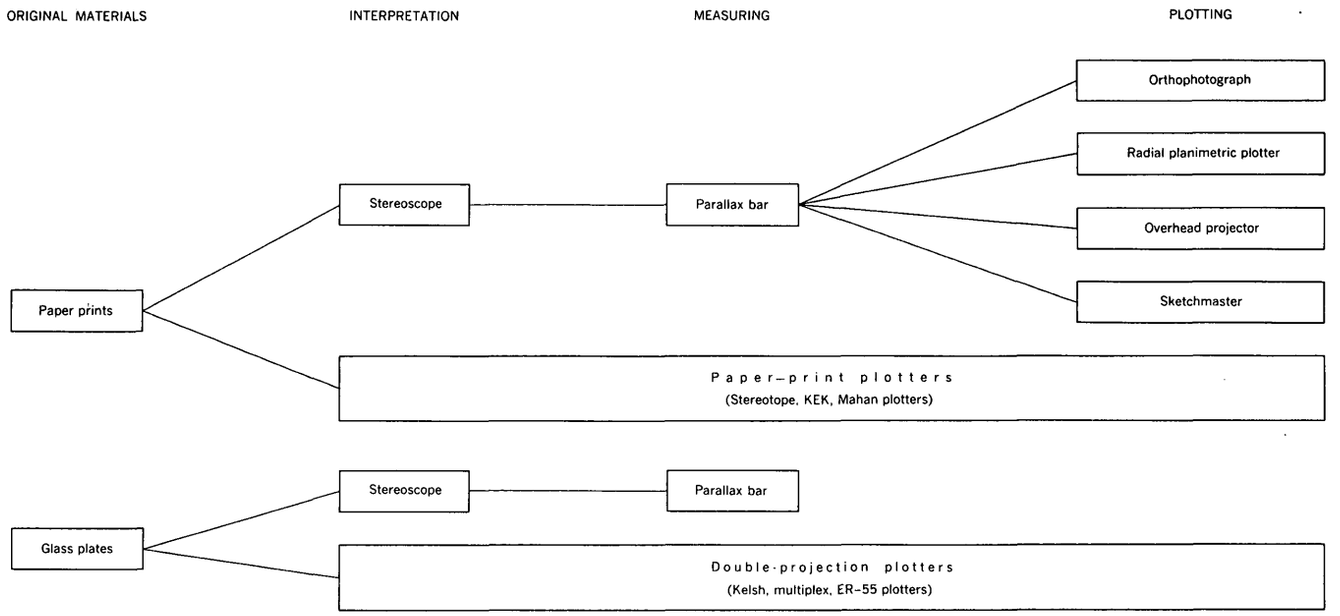


FIGURE 36.—Photogrammetric systems for geologists.

scale photographs and minimum instrument capability that will provide the desired geologic measurements within given accuracy requirements. That is, the scale of photographs should be the smallest that will permit differentiation of photographic detail needed for qualitative interpretation, as well as the smallest that will permit photogrammetric measurements within specified limits. Fundamentally, the geologic objective of a particular study is the controlling factor in the choice of the optimum system of interpretation, measuring, and plotting. The geologic objective may permit the use of existing instruments and photograph scales or it may necessitate new photography or instruments to attain given accuracy requirements.

The type of geologic map and its intended use—the geologic objective—can be considered on the basis of accuracy requirements or limits of error, both in obtaining vertical measurements and in plan positioning of geologic features, provided photographic detail is adequate for qualitative interpretation. For example, a detailed structure-contour map may require an accuracy of vertical measurement within ± 5 feet of altitude and a horizontal position of geologic features within 1/25 inch of true map position. In contrast a small-scale structure-reconnaissance map for planning purposes may permit a vertical tolerance of ±50 feet and have only general horizontal positioning requirements. Thus the choice of an interpretation, measuring, and plotting system may be reduced to certain mathematical requirements that can be satisfied by combining instrument capability with appropriate photography; or the geologic objective or tolerances of measurement may be modified to permit the use of existing photography and instruments.

However, geologic maps, unlike topographic maps, have no standard accuracy limits except those imposed by the individual geologist, with the one exception in the Geological Survey that solid lines, representing faults, contacts, or similar geologic features, should generally be within 1/25 inch of their correct map positions for general geologic maps at a scale of 1:63,360 or larger. Horizontal positioning of data within 1/25 inch of true map position may be accomplished with almost any plotting instrument or plotting system, especially if relief of the area is low and excessive tilt is not present in the photographs. Hence, the vertical-accuracy requirement specified by the geologist for a given geologic problem is ideally the determining factor in choosing an interpretation, measuring, and plotting system. This accuracy requirement, as well as the maximum range of measurements expectable for any system, may be equated against instrument capability and photograph scale as follows:

Geologic requirement of vertical-measurement accuracy
or
Expected maximum range of vertical-measurement error
$\rightleftarrows$
Instrument capability in terms of K and V factors (see fig. 37).

Figure 37 is an elaboration of this equation and shows the general relations between the geologic requirements of vertical accuracy or expected maximum error in measuring spot altitudes or vertical intervals

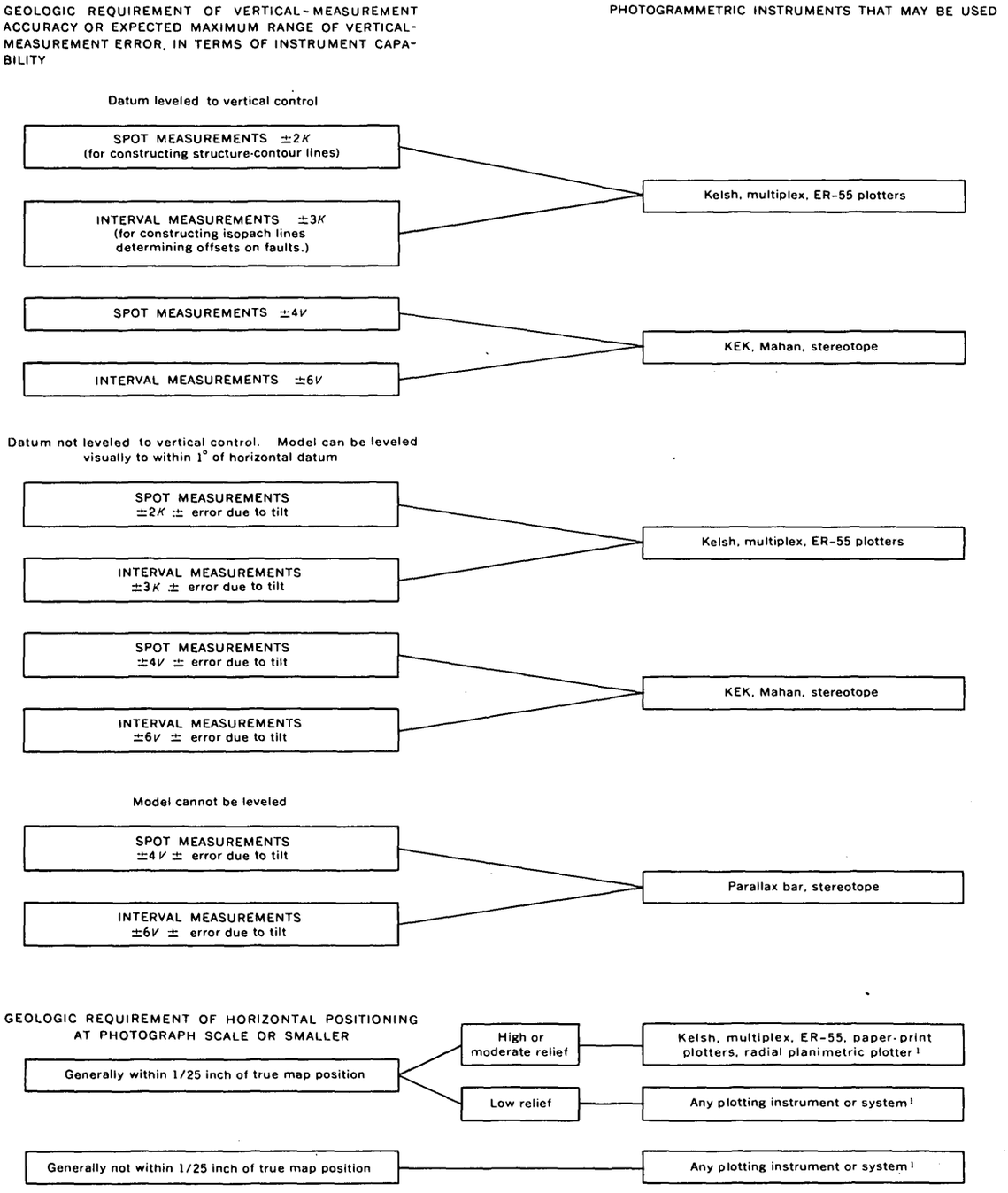


FIGURE 37.—Photogrammetric measuring and plotting systems for geologists showing relation of different instruments to vertical-measurement and horizontal-positioning errors.

where K factor = difference in altitude, in feet, on the ground per unit of vertical measurement in an anaglyphic-type model, that is, per 0.1 millimeter

$$= \frac{\text{model-scale denominator}^2}{3{,}048}.$$

where V factor = difference in altitude, in feet, on the ground per unit of measurement from a parallax bar or a paper-print plotter, that is, per 0.01 millimeter

$$= \frac{\text{flying height (feet)}}{\text{photobase (millimeters)} \times 100}.$$

[1] No excessive tilt assumed to be present for paper-print models that cannot be leveled.

[2] Model scale for Kelsh plotter is usually about 5 times original photography scale; for ER-55 usually about 3.5 or 5 times, depending on the projector model; and for multiplex usually about 2.5 times.

in terms of instrument capability on one hand and photogrammetric instruments that may be used for measuring and plotting on the other hand. The determination of spot altitudes or relative vertical intervals satisfies most geologic requirements of altitude measurements from stereoscopic models and permits construction of structure-contour lines, and isopach lines, and the determination of dips of slopes, displacements on faults, and similar data. Figure 37 can be used in choosing the best selection from existing photograph scales and instruments for measuring vertical distances, or it can be used to determine what combination of photograph scale and instruments would be optimum in making vertical measurements within certain specified tolerances. For economic reasons the geologist more often than not will be concerned with the best selection of existing photographs and instruments but this selection may not be the optimum interpretation, measuring, and plotting system. This may require modification of his geologic objective, at least in reporting the limits of measurement.

INSTRUMENT CAPABILITY

Instrument capability, selected as the principal basis for the systems shown in figure 37, is an empirically derived factor generally considered with respect to topographic mapping systems as the minimum contour interval—stated in terms of a fraction of the flying height—that can be plotted to fulfill certain accuracy requirements. For geologic measurements it is desirable to consider instrument capability as the minimum increment of vertical measurement that generally can be determined by the geologist from the stereoscopic model. This permits a simple evaluation of expected maximum errors in geologic measurements when double-projection stereoscopic models are used, or when stereoscopic models from paper prints are used. It also allows the geologist to determine what photograph scale and instrument combinations will give him a desired accuracy of measurement. Because the minimum increment of vertical measurement is empirically derived, the limits of error for vertical measurements described below may be subject to modification.

To determine the expected maximum error for a given combination of photograph scale and instrument three possible individual errors must be considered. These are (a) instrument capability in terms of the geologist's ability to measure horizontal linear parallaxes and increments of vertical measurement, (b) curvature of the datum within a stereoscopic model when double-projection instruments are used, or paper and lens distortions when paper prints are used, and (c) tilt. Consideration of the cumulative effect of all three possible errors is necessary in determining the expected maximum error for a particular measuring and plotting system, except for leveled models where tilt has been eliminated. In measuring spot altitudes or relative intervals these errors may be compensating rather than cumulative and therefore many measurements will be well within the expected maximum error determined for a particular combination of photograph scale and instrument.

Experience has shown that for double-projection plotters, it is generally possible for the geologist to determine any one reading to one unit of vertical measurement. One unit of vertical measurement is equal to 0.1 millimeter. With care the increment of measurement may be read closer than one unit of vertical measurement. The amount of altitude difference, in feet, on the ground represented by one unit of vertical measurement in the model—called the K factor—depends solely on the scale of the projected stereoscopic model, and is determined by the ratio

$$\frac{\text{Model-scale denominator}}{3{,}048}.$$

This factor is constant throughout the stereoscopic model. Hence spot altitude readings generally may be read within an amount equal to $\pm K$, that is, the geologist may read a point one unit (0.1 millimeter) too high or one unit (0.1 millimeter) too low. In addition, an error of $\pm K$ is added for curvature of the model datum. Thus the maximum error for spot altitudes can be expected to be on the order of $\pm 2K$ for models leveled to vertical control. Where errors due to reading and to curvature of the datum are compensating a minimum error approaching zero can be obtained. For interval measurements the altitudes of two image points in the stereoscopic model of course must be measured. Each point may be read within an amount equal to $\pm K$, or a total reading error $\pm 2K$. Curvature of the model datum may affect the reading of each point a similar amount and can be disregarded when relative intervals are measured on points close together in plan view; for points close together the expected maximum error generally will be similar to that for spot altitudes. But if points of measurement are not selected close together an added error of $\pm K$ due to datum curvature may be introduced. Thus the maximum error for relative interval measurements is on the order of $\pm 3K$ (figs. 37 and 38).

When vertical control is absent many double-projection stereoscopic models and some models from paper prints may be leveled visually to within 1° of a horizontal datum by observing certain physiographic

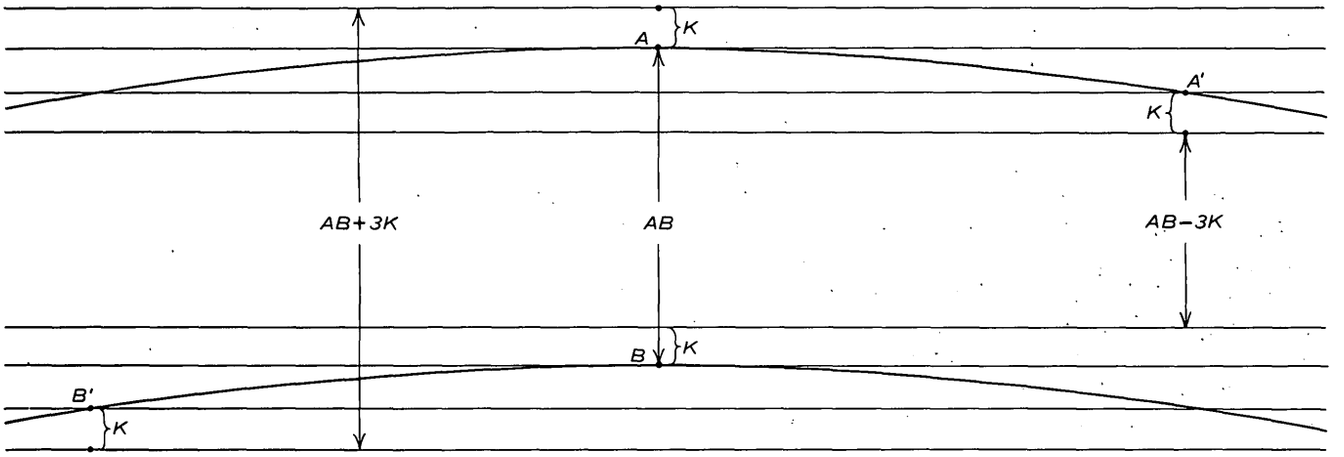


FIGURE 38.—Diagram showing datum-curvature relation to maximum expected error in measuring vertical intervals from leveled double-projection stereoscopic model.

Let AB equal the interval desired. If the upper point is measured at A' an error equal to $-K$, or one unit of measurement, may result from datum curvature; when point B' is measured an error of $+K$ may result. If points A and B' are chosen for measuring the interval and point A is measured one unit too high (equivalent to $+K$) and point B' is measured one unit too low (also equivalent to $+K$) a maximum expected error, including datum-curvature error, of $+3K$ may result. Likewise if points A' and B are chosen for measuring the interval a maximum expected error, including datum-curvature error, of $-3K$ may result.

features in the model (see p. 55) and making appropriate instrument adjustments. For double-projection stereoscopic models that are leveled visually some error due to tilt thus may be present in addition to possible errors in reading and curvature of the model datum; the order of maximum error for spot altitudes becomes $\pm 2K$ ± error due to tilt, and for relative interval measurements becomes $\pm 3K$ ± error due to tilt. When relative stratigraphic thicknesses, displacements on faults, or similar geologic measurements are being made, errors due to tilt or from curvature of the model datum may be minimized by measuring points close together in the stereoscopic model. For points spaced far apart the error due to tilt can exceed the error in reading intervals.

Limits can also be placed on reading units of measurement with paper-print plotters or parallax bars, except that a V factor rather than a K factor is employed. A differentiation of factors is necessary as the V factor, unlike the K factor, is not constant throughout the model, but varies slightly due to differences in scale at different altitudes in models formed from paper prints. For practical purposes, V is the ratio:

$$\frac{\text{Flying height (feet)}}{\text{Photobase (millimeters)} \times 100}$$

The V factor represents the difference in altitude in feet on the ground per unit of measurement from a parallax bar or paper-print plotter, that is per 0.01 millimeter. Experience has shown that parallax measurements from paper prints may be read within about ± 0.02 millimeter or $\pm 2V$. Considering possible errors due to paper or lens distortion and due to tilt, total expected errors for spot altitudes and relative intervals may be determined as shown on figure 37. (See also p. 74.) Errors resulting from paper and lens distortions are considered to be equivalent to about two units of measurement or about $2V$.

Thus two different factors are considered in relating geologic accuracy requirements or expected maximum vertical measurement errors to photograph scale and instrument capability. These factors are the K factor for use with stereoscopic models from glass plates in double-projection plotters, and the V factor for use with stereoscopic models formed from paper prints. For any given system of measurement it is likely that many measurements will fall well within the expected maximum errors as determined from figure 37, especially if high-resolution photographs are available that may permit reading units of vertical measurement less than K or V, and if points of measurement are carefully chosen. Also, errors of reading and datum curvature or tilt may be compensating rather than cumulative, as stated above. In a recent test of determining altitudes of gravity stations with multiplex leveled to vertical control, Kinoshita and Kent (1960) found that 96 per cent of the points measured fell approximately within the limits of $\pm K$ and that 71 percent of the points measured fell approximately within the limits of $\pm K/2$. Results of this special test do not represent the general order of vertical ac-

curacy that geologists may expect to obtain by photogrammetric methods, but they do suggest that many measurements made will be well within the limits shown in figure 37.

RELATION BETWEEN INSTRUMENT CAPABILITY, SCALE, AND VERTICAL MEASUREMENTS

Let it be desired to determine the accuracy of spot altitudes for compiling a structure-contour map of an area covered by recent, high-quality 1:20,000-scale photography flown at 10,000 feet. Adequate vertical control is available for leveling stereoscopic models and a Kelsh plotter is available for measurement and compilation. The expected maximum error shown in figure 37 for spot altitudes for leveled models is $\pm 2K$. Because the scale of the Kelsh model is approximately 5 times that of the original 1:20,000-scale photography (fig. 37), a projected stereoscopic model at a scale of 1:4,000 would result. Thus the K factor for this model would be 4,000/3,048 or 1.31 feet (fig. 37). Spot altitude measurements could be expected to be correct within $\pm 2K$ or ± 2.62 feet for most points in the model.

Many geologists will have only paper prints and simple measuring devices to use so as a second example let it be desired to determine the expected maximum error in measuring a stratigraphic interval with a parallax bar and paper prints already available. Photographs at a scale of 1:20,000 and taken at 10,000 feet are available. Inspection of physiographic characteristics of the terrain indicates that very little tilt, estimated not to exceed 1°, is present. Rock units are clearly expressed, the formations are essentially flat lying, and points of measurement are within ¼ inch on photographs or a distance of about 400 feet on the ground. The photobase distance is 90 millimeters. Figure 37 shows that with parallax bar the expected range of error for relative intervals is $\pm 6V$ ± error due to tilt,

$$\text{where } V = \frac{10{,}000}{90 \times 100} = 1.1 \text{ (fig. 37)}.$$

The maximum error due to tilt, however, could amount to 14 feet in this example and thus a total expected error of 20.6 feet could result. But the reading error plus paper and lens distortion error may well be less than $\pm 6V$ and the points of measurement may well lie in a direction other than the maximum tilt direction; thus, a measurement error of much less than 20.6 feet will probably result. Figure 37 is constructed to show only the order of maximum error. The percentage of error will depend on the total thickness of the stratigraphic interval; the percentage of error becomes smaller as the thickness of the interval increases.

The geologist will be concerned generally with the expected maximum error of measurement that photographs and instruments already at his disposal will give, and figure 37 is readily used to determine expected maximum errors of measurement for a given photograph scale and instrument combination. However, to determine what photograph scale and instrument combination would be needed to attain specified accuracy requirements is not so easy, as the photograph scale and instrument may be varied and yet give the same required tolerances of vertical measurements. For practical purposes it may be best to equate the vertical-accuracy requirement against instrument capabilities, and to determine from this the scale of photographs that would be needed. Thus, if a requirement for measuring vertical intervals of ±5 feet is specified it can be seen, for leveled double-projection stereoscopic models, for example, that $\pm 3K$, the maximum expected error for relative intervals, must equal 5 feet or K must equal 1.66 approximately. It follows (see fig. 37) that the projected model-scale denominator must equal 1.66×3,048 or about 1:5,000.

The scale of photographs required to provide a projected stereoscopic model of 1:5,000 depends on the double-projection plotter used. For the Kelsh plotter, the original photography scale would be approximately 1:25,000; for the ER–55 plotter, approximately 1:17,000 or 1:25,000 depending on the projector model; and for the multiplex, approximately 1:12,000 (fig. 37). Similar computations can be made for other instrument capabilities and requirements of vertical measurements. Where two different combinations of instruments and photograph scales will provide the desired accuracy of vertical measurement, the optimum interpretation, measuring, and plotting system will be determined by the smallest scale of photography that will allow recognition and qualitative interpretation of geologic features pertinent to the given geologic objective.

HORIZONTAL POSITIONING

Horizontal positioning within 1/25 inch of true map position generally can be accomplished at photograph scale or smaller with any of the plotting instruments that removes relief and tilt displacement. Such instruments include the double-projection plotters and some of the paper-print plotters. The small amount of tilt inherent in present-day vertical photography is generally of little significance in horizontal positioning of geologic features, however, and the radial planimetric plotter may also be used to plot geologic features within 1/25 inch of true map position. Orthophotographs may also be used for reliable horizontal positioning of data (see p. 69). In addition, geologic features in areas of

low relief may be plotted within 1/25 inch of true map position by sketchmaster or overhead reflecting projector if tilt is negligible. Where relief is low, radial displacement (also called relief displacement) of image points is commonly less than $\frac{1}{25}$ inch. For example, on vertical photographs taken from a flying height of 10,000 feet, displacement where the relief is 100 feet amounts to 1/25 inch at a point 4 inches from the center of the photograph. Nearer the center of the photograph the displacement is less. Thus, geologic data on such photographs can be plotted generally within 1/25 inch at photograph scale or smaller with simple overhead reflecting projectors, or can even be traced directly from the photographs and still be within the 1/25-inch tolerance for general geologic maps. The amount of radial displacement, m in inches, is determined from the formula

$$m=\frac{rh}{H}$$

where r=radial distance on the photograph, in inches, from principal point to base of image displaced;

h=height of object displaced, in feet above datum (height of terrain);

and H=flying height, in feet, above datum;

(h and H must be referred to the same datum and be measured in the same units. The amount of displacement, m, is then in the same units of measure as chosen for r). Thus, the limit of relief that can be adequately plotted within the 1/25-inch tolerance for general geologic maps is basically a function of flying height and not of focal length. Displacement due to relief varies inversely with flying height.

FIGURE 39.—POORLY RESISTANT PYROCLASTIC ROCKS OVERLAIN BY RESISTANT CAPPING FORMATION (COLORADO).

[Approximate scale 1 : 20,000. Photographs by Soil Conservation Service]

Coarse pyroclastic rocks, *A*, are highly dissected in contrast to the more resistant and protecting welded tuff caprock, *B*, in this area of flat-lying formations. Deep dissection of pyroclastic rocks, occurring here preferentially on one slope, permits delineation of contacts that can be traced into nearby areas where strong dissection has not taken place. The use of the floating-dot reference mark of many photogrammetric instruments may be especially helpful in tracing a geologic contact from an area where the contact is well expressed to an area where the contact is obscured. Sandstone and shale below the pyroclastic rocks are in large part poorly exposed because of the slope wash that covers the deposits.

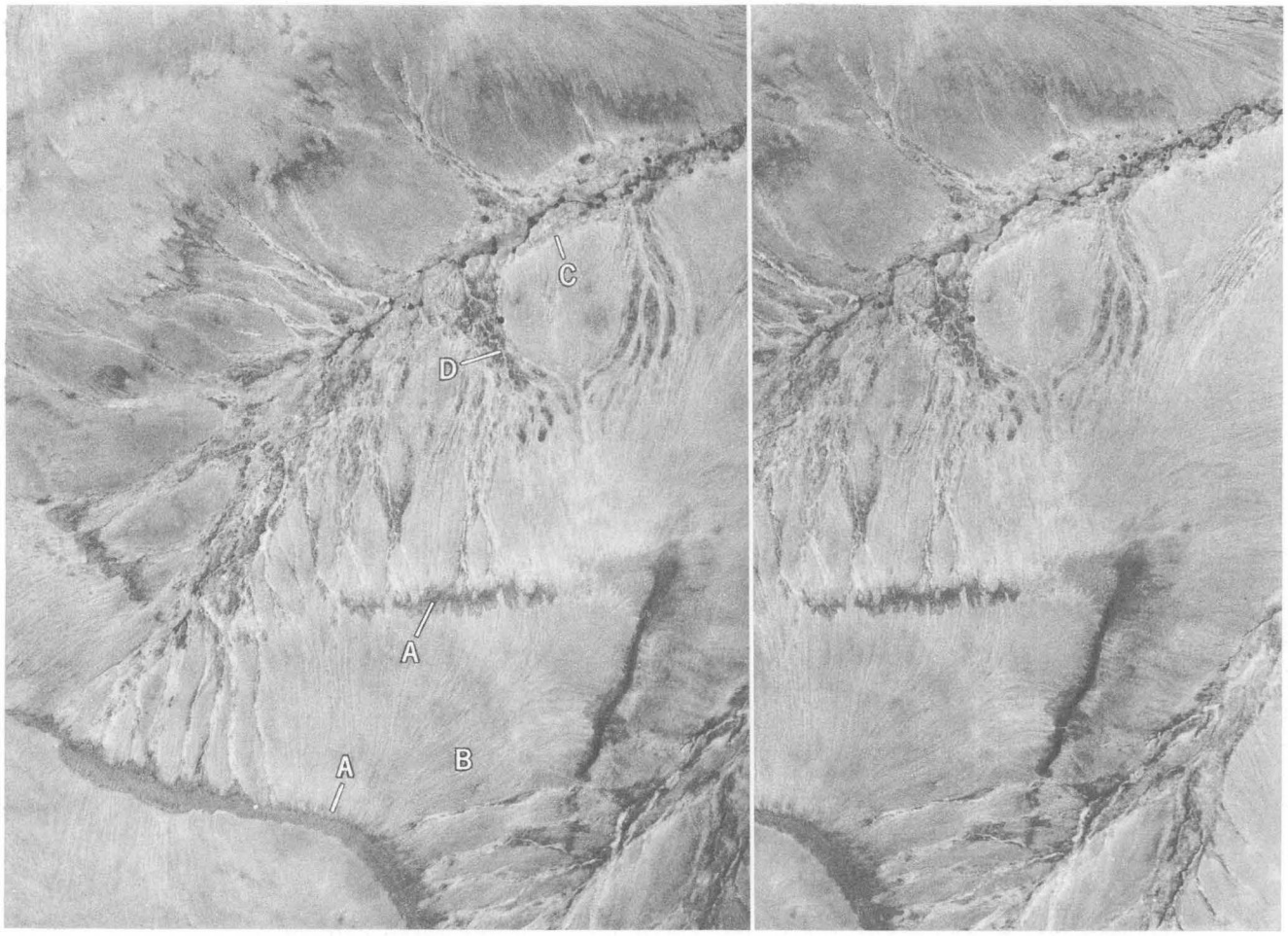


FIGURE 40.—AREA UNDERLAIN PREDOMINANTLY BY GENTLY FOLDED SANDSTONE, SHALE, CONGLOMERATE, AND GRAYWACKE (NORTHERN ALASKA).

[Approximate scale 1 : 20,000. Photographs by U.S. Navy]

In some areas where outcrops are sparse or lacking bedding may be traced on the basis of topography and vegetation. Resistant beds of sandstone and conglomerate cause small topographic rises, in some areas as little as 2 feet, which are easily discerned in the stereoscopic model because of vertical exaggeration present in viewing most stereoscopic pairs. The steepened slope caused by the resistant bed is commonly populated with a different mossy and grassy vegetation from that of surrounding areas, and bedding is revealed as wide, strongly curved bands of vegetation that are recognized on photographs by their lighter or darker photographic tone than surrounding areas. Such bands of vegetation, as at *A*, are commonly seen clearly on aerial photographs or from a distance on the ground, but are not always readily distinguished when standing directly on them on the ground.

Permafrost is shown by the presence of beaded drainage, indicated by isolated pools of water connected by short, incised watercourses along main stream. Striped slopes, *B*, are typical but not unique to permafrost areas (contrast fig. 53). Note high-center polygons, *C*, that exhibit raised centers surrounded by depressed dark-toned edges. Angular drainage channels, *D*, are related to melting out of ice wedges and are common in permafrost areas.

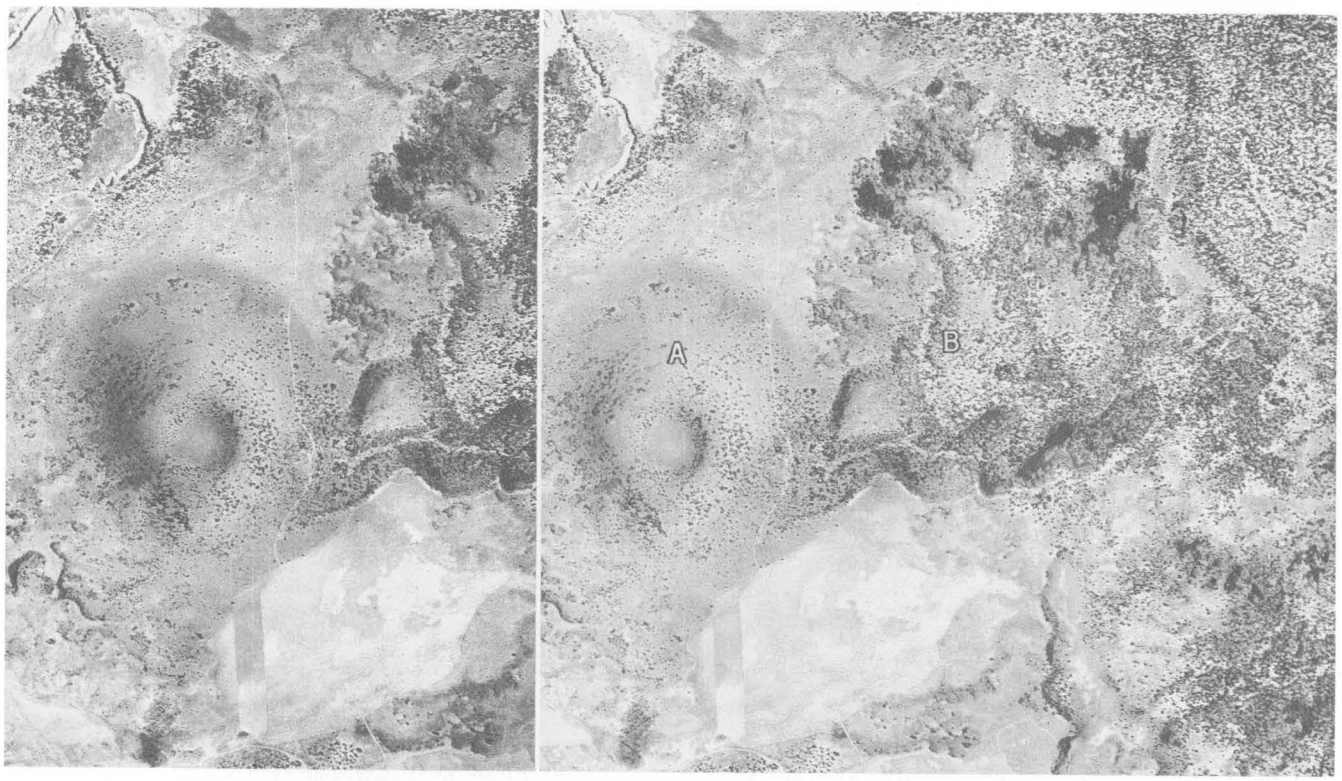


FIGURE 41.—EXTRUSIVE VOLCANIC ROCKS AND ASSOCIATED CINDER CONE (UTAH).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Cinder cone, *A*, is readily identified on the basis of shape of the constructional landform. Associated flows, *B*, are dark toned, irregular in ground plan, and marked by very uneven topographic surfaces. Many lava flows lack surface drainage rills, which suggests permeable material. Note especially the lack of surface drainage channels on flanks of cinder cone.

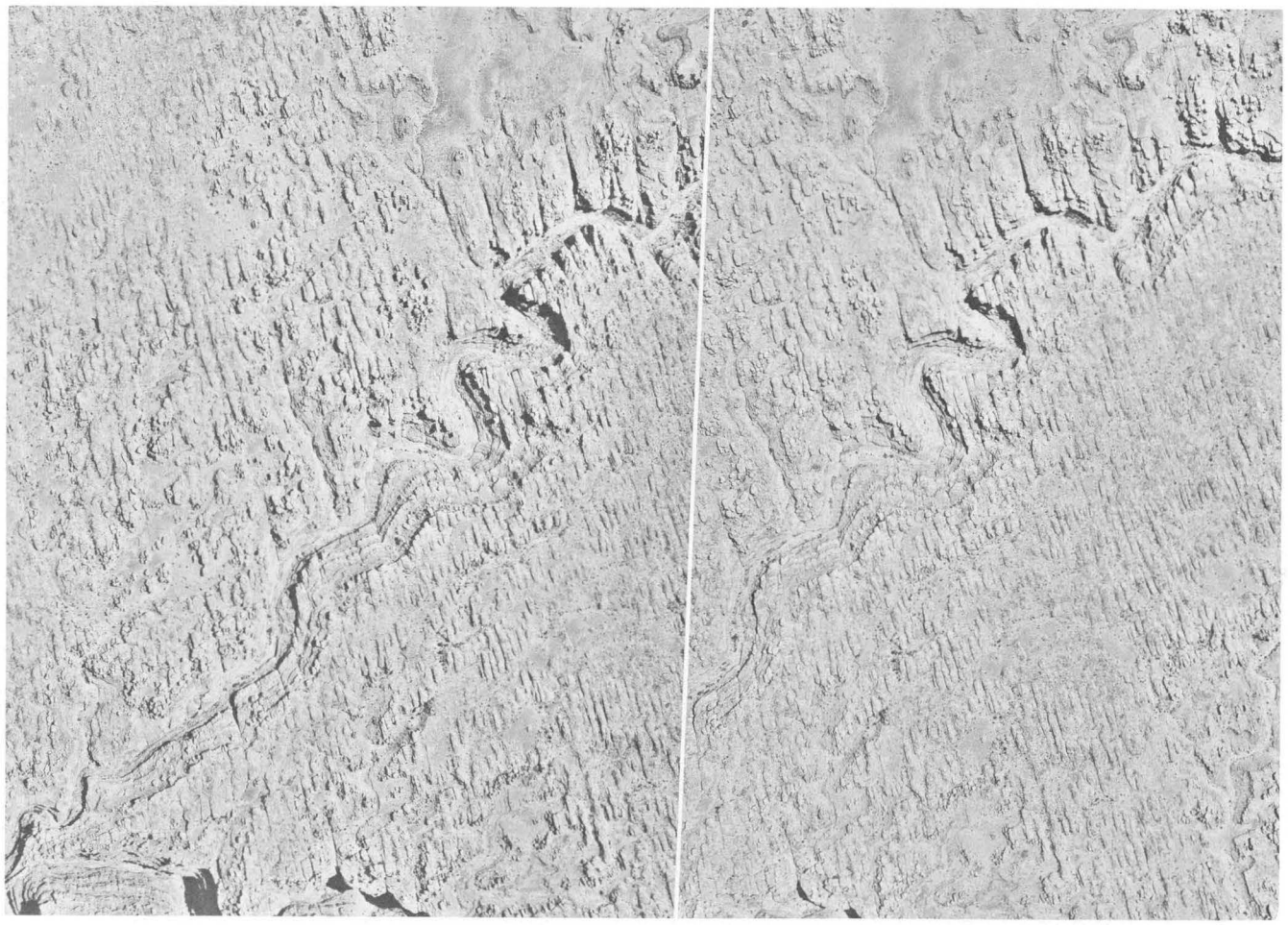


FIGURE 42.—FLAT-LYING SANDSTONE (SOUTHERN UTAH).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

Prominent wide-spaced joints are shown by many short lineations. Where beds are essentially flat lying, joints commonly form in a right-angle pattern and give the terrain a blocky appearance locally, although one direction of jointing may dominate and give a conspicuous linearity to the topographic grain. The light photographic tone and coarse-textured drainage is typical of coarse sedimentary rocks. Major drainage is dendritic; this pattern is commonly characteristic of flat-lying rocks. Minor drainage is controlled by joints.

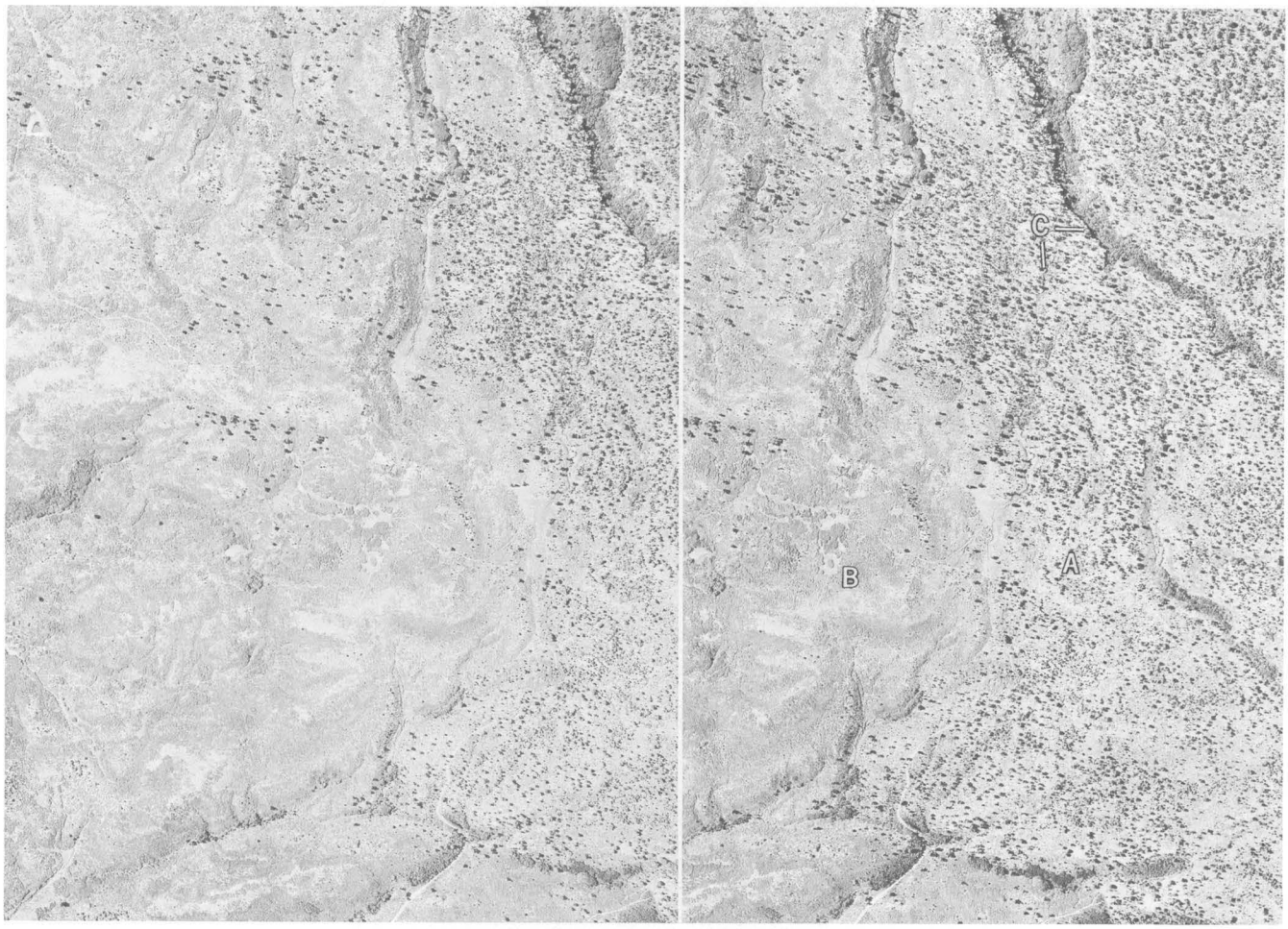


FIGURE 43.—SANDSTONE AND CONGLOMERATE BEDS INTRUDED BY DIORITE PORPHYRY LACCOLITH (UTAH).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Conspicuous contrast in vegetation results from different lithologic types. Sandstone and conglomerate beds, *A*, are covered largely with scattered tall jack, yellow, and ponderosa pine trees. Diorite porphyry, *B*, is covered with scrub oak as much as 10 feet high. This dense growth of scrub oak forms a photographic texture that contrasts with areas covered with pines. Note serrated edges of bluffs, *C*, which are expressions of joints in sandstone and conglomerate beds.

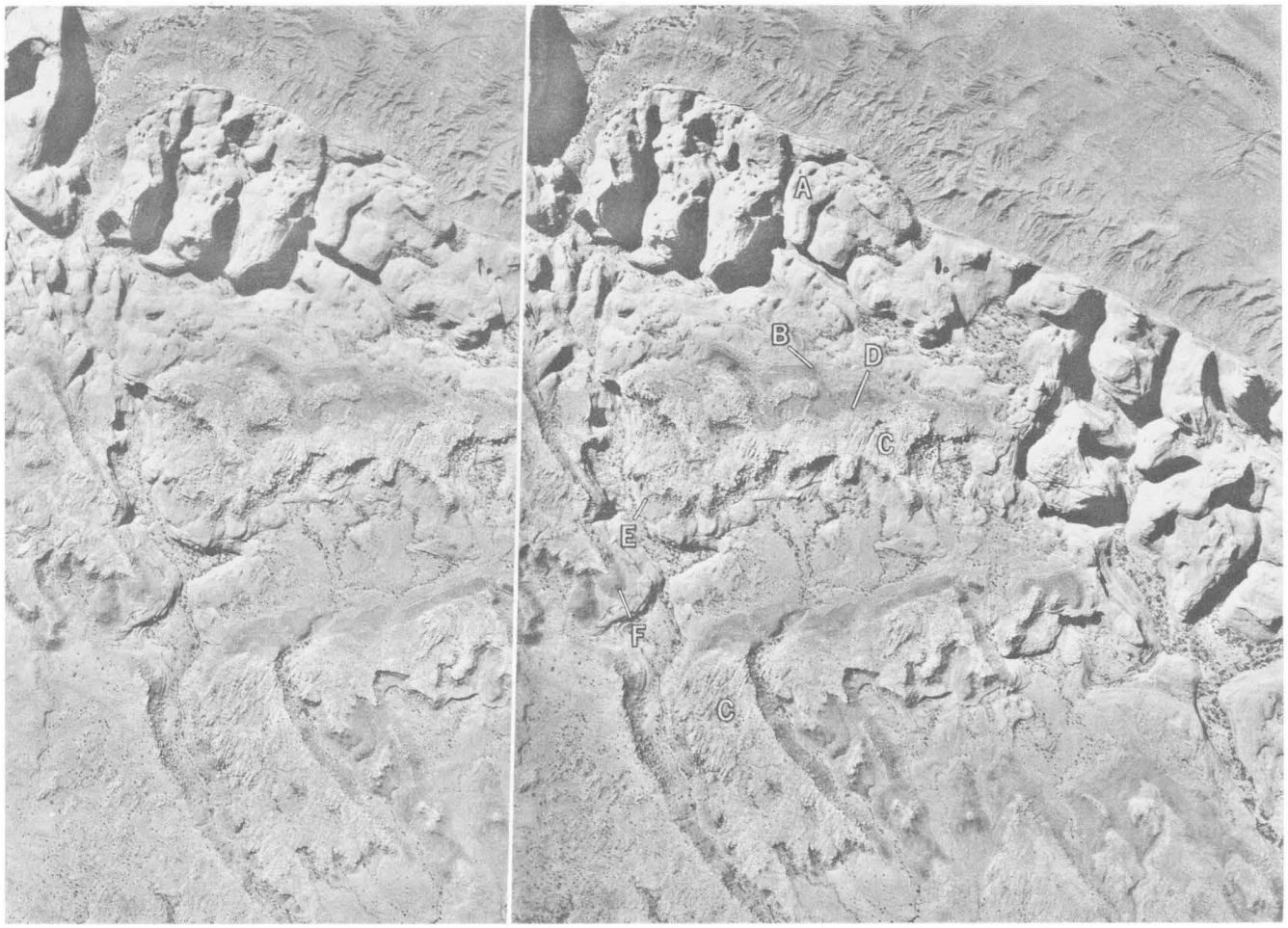


FIGURE 44.—GENTLY DIPPING BEDS OF SANDSTONE, SILTSTONE, AND CONGLOMERATE THAT LOCALLY CONTAIN CHANNEL-FILL DEPOSITS (ARIZONA).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

Light photographic tone of rocks, *A*, is typical of massive crossbedded sandstone in this area. Dark-toned rocks, *B*, are reddish thin-bedded shaly siltstone, shale, and fine-grained sandstone. Light-toned conspicuously jointed rocks, *C*, are uranium-bearing sandstone, conglomerate, and mudstone. Locally the dark-toned rocks have been eroded by channel scour, and the channels have been filled with sandstone and conglomerate that now lie unconformably on the older rocks. Erosion of dark-toned rocks along line *D*, which represents the line of unconformity and orientation of a channel in this area, is conspicuous by the photographic tone change. At *E* the dark-toned rocks have been completely eroded away and light-toned jointed sandstone and conglomerate rest on the light-toned massive crossbedded sandstone. At *F* the dark-toned rocks again become conspicuous where overlying rocks thin. Differences in stratigraphic thicknesses of the dark-toned rocks, which reflect a thickening of overlying rocks that were deposited in old river channels, can be measured photogrammetrically. Isopach lines may be drawn to indicate the orientation of the channel and the general depth of the channel.

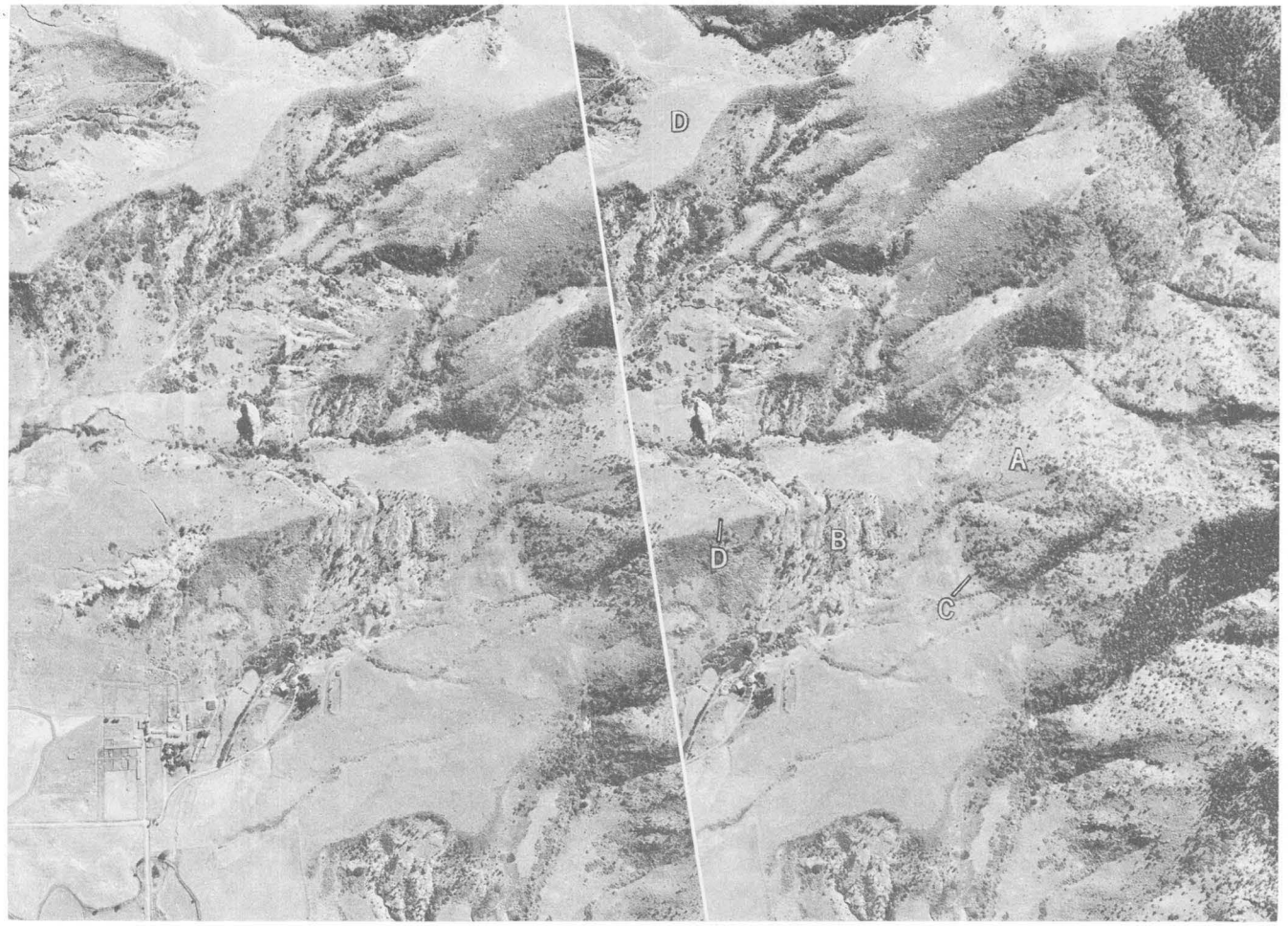


FIGURE 45.—GNEISS, SCHIST, AND GRANITE FLANKED BY DIPPING SEDIMENTARY ROCKS TRUNCATED BY PEDIMENT GRAVEL (COLORADO).

[Approximate scale 1 : 21,000. Photographs by U.S. Air Force]

Topographically high, vegetated area, *A*, is underlain by gneiss, schist, and granite. Light-toned sedimentary rocks, *B*, lying unconformably on the igneous and metamorphic rocks, are primarily arkose and sandstone. Trace of unconformity between sedimentary rocks and igneous and metamorphic rocks is indicated by break in slope, *C*, which is locally accentuated by contrast of trees on steep slope uphill from the trace of the unconformity with grassy vegetation on the gentler slope below. Note effect on dip of vertical exaggeration in the stereoscopic model. The arkose and sandstone unit dips about 25°. The grass-covered pediment gravel, *D*, which truncates the underlying sedimentary rocks, dips 2° to 3°.

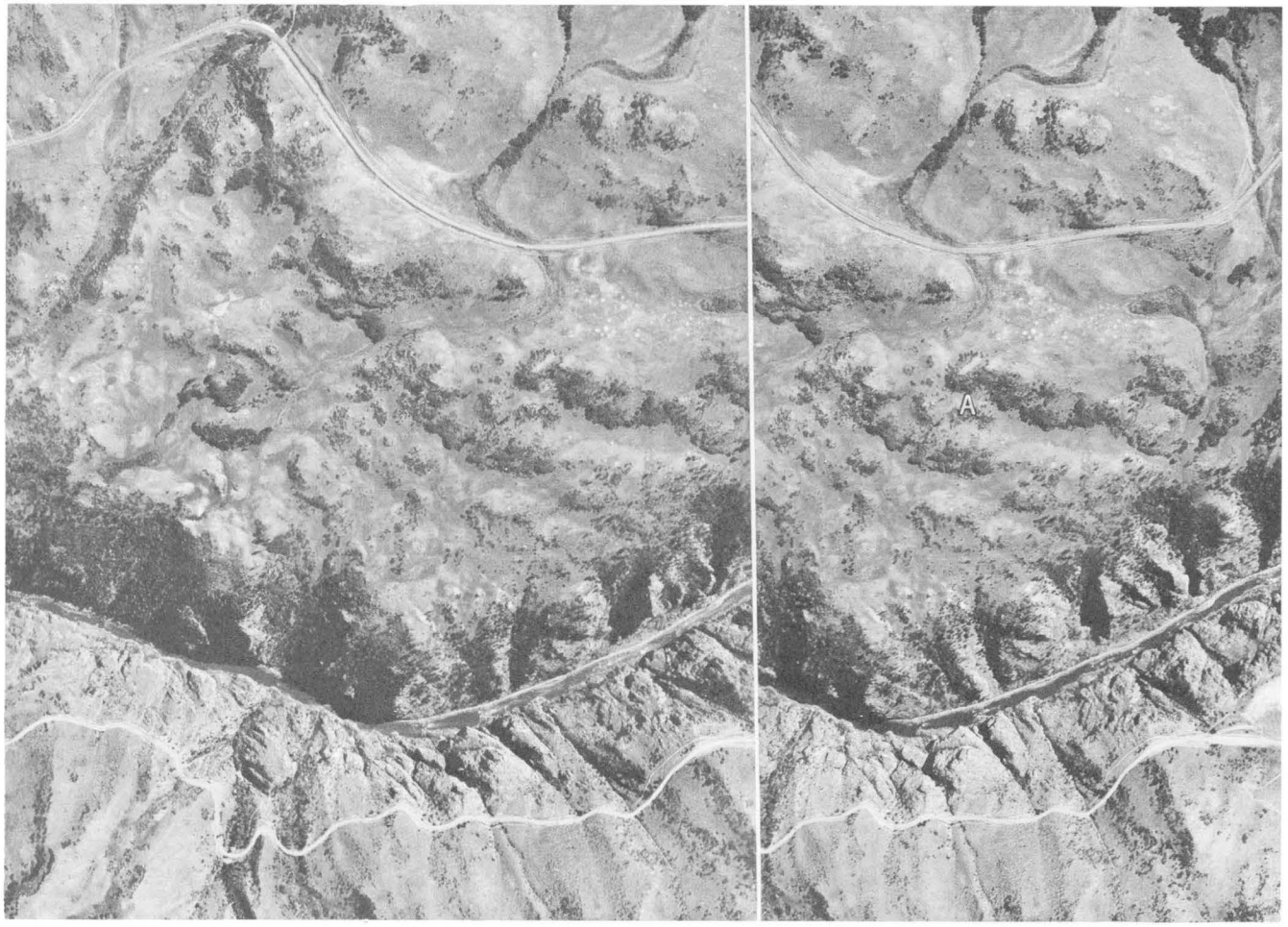


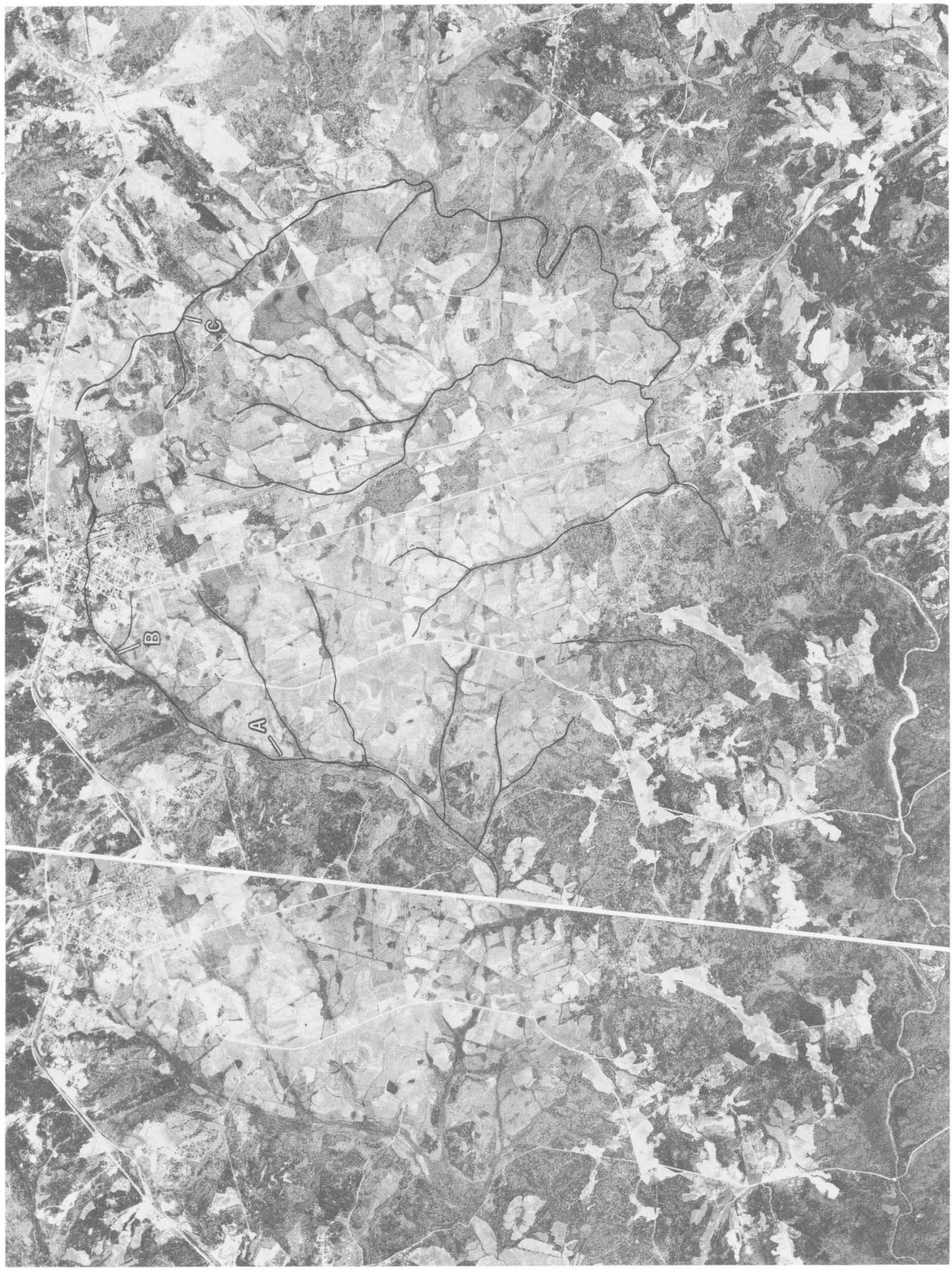
FIGURE 46.—LANDSLIDE AREA (COLORADO).

[Approximate scale 1 : 37,000. Photographs by U.S. Geological Survey]

Landslides are indicated primarily by landform. Note the characteristic hummocky topography of slide material prominent at *A*. Minor ridges of the slide area are commonly parallel to the contour of the slope; clumps of vegetation locally are oriented parallel to the contour of the slope also. Poorly resistant sedimentary rocks underlie the landslide debris; resistant volcanic flows (not shown) cap the sedimentary rocks. In many areas where poorly resistant rocks underlie a resistant caprock, conditions for landsliding are favorable. Highly fractured rocks in canyon are schist and gneiss.

FIGURE 47.—ORTHOPHOTOGRAPH AND PERSPECTIVE PHOTOGRAPH OF SAME AREA.

(Left) Part of perspective aerial photograph showing distortions in powerline caused by relief displacement of image points. (Right) Orthophotograph of the same area showing that relief displacement has been eliminated in preparing orthophotograph. Note that the powerline is straight.



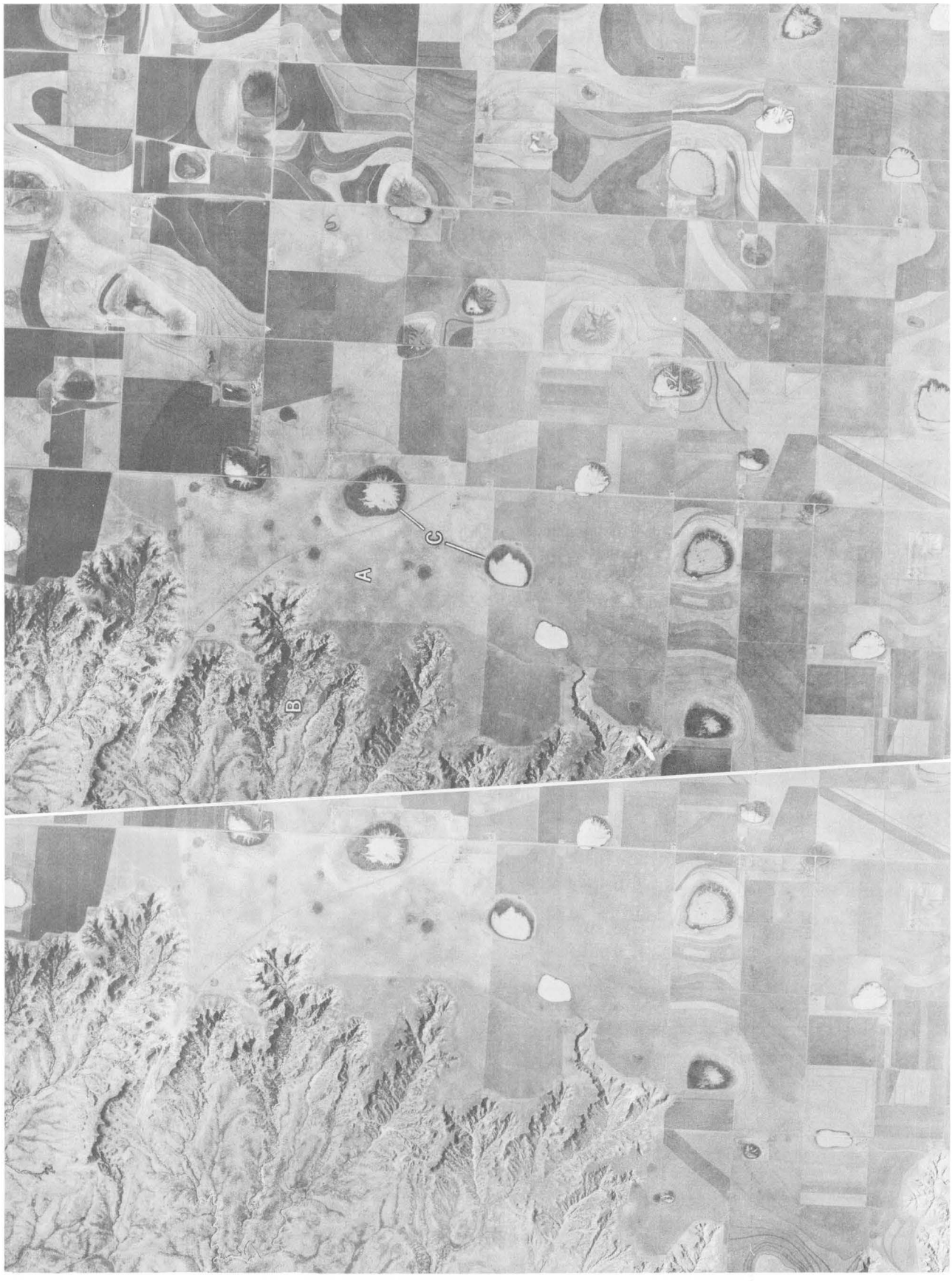
Stereoscopic pair

Approximately 1 mile

FIGURE 48.—AREA SHOWING RELATION OF PHOTOGRAPHIC TONE, LAND-USE PATTERN, AND DRAINAGE TO RESIDUAL SOIL, ROCK TYPE, AND GEOLOGIC STRUCTURE (SOUTH CAROLINA).

[Approximate scale 1 : 60,000. Photographs by Army Map Service]

Aerial photographs commonly show an association of features that is meaningful to the interpreter. Here photographic tones, land-use pattern, and drainage pattern are associated with specific soils, rock types, and geologic structure. Note that the small scale of the photographs is a significant factor in showing the striking land-use pattern and drainage pattern (see also fig. 4). The circular land-use pattern of the farmed area generally bounded by vegetated areas, as at *A*, represents soils developed on underlying mafic rocks. Rocks in the immediately surrounding vegetated areas are largely silicic intrusive types. The drainage characteristics of the area also suggest a pluglike or domal geologic structure. Streams at *B* and *C* form a conspicuous annular pattern around the area of mafic rocks and probably mark the contact of the mafic rock body.



Stereoscopic pair

Approximately 1 mile

FIGURE 49.—SHALE AND THIN SANDSTONE INTERBEDS CAPPED BY POORLY CONSOLIDATED GRAVEL AND SAND, LOCALLY CEMENTED WITH CALCAREOUS MATERIAL (TEXAS).

[Approximate scale 1 : 63,360. Photographs by Army Map Service]

Lack of surface drainage at *A* indicates high degree of permeability in capping material. Note in contrast the striking fine-textured drainage on the relatively impermeable shale area, *B*. Broad depressions, *C*, in capping gravel and sand are very shallow and show little relief even with vertical exaggeration found in the stereoscopic model. These depressions resulted in large part from wind action; some solution of local calcareous cementing material also may have taken place. Dark areas within depressions represent a darker vegetation growth; light-toned areas represent in part washed-in fine materials that were dry and hence light colored at the time the photographs were taken. Locally some light-toned evaporite deposits may be present.

Stereoscopic pair
Approximately 1 mile
E
D
B
B
A
C
F
A

553966 O-60—5

FIGURE 50.—RECENTLY FAULTED STRAND LINES OF FORMER LAKE (NEVADA).

[Approximate scale 1 : 20,000. Photographs by Soil Conservation Service]

Strand lines of beach sand, *A*, are shown strikingly by dark photographic tone and slightly higher altitudes than surrounding surficial material. Note that strand lines are truncated by a recent fault, *B*, shown by narrow band of dark vegetation and by low scarp. Drainage density is relatively high on the thin alluvial cover, *C*, but decreases noticeably on opposite side, *D*, of fault where better drained, thicker deposits of alluvial material are present. Strand line is faulted up about 25 feet at *E* by recent fault movement. An irregular fault trace is also seen at *F*.

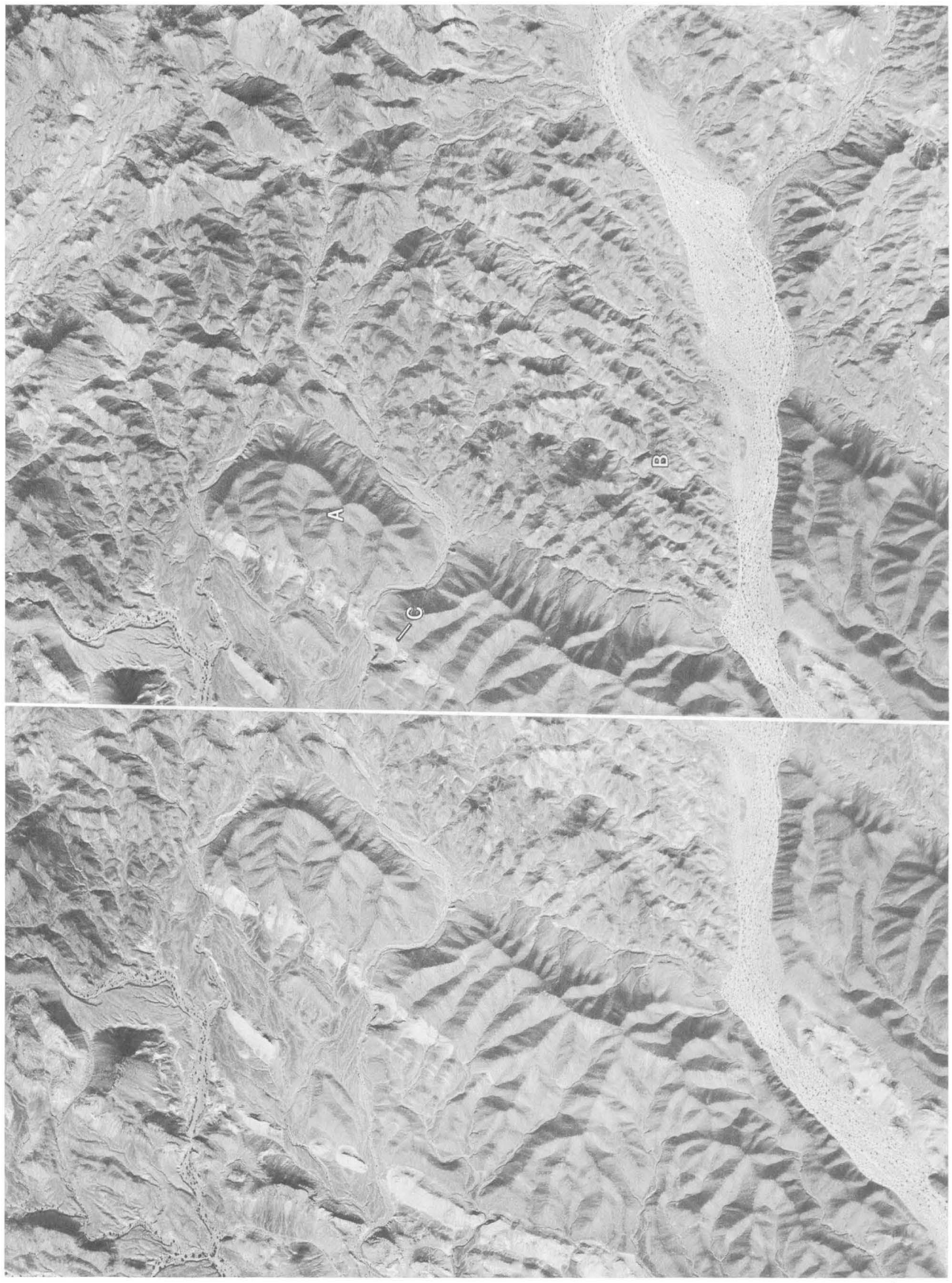
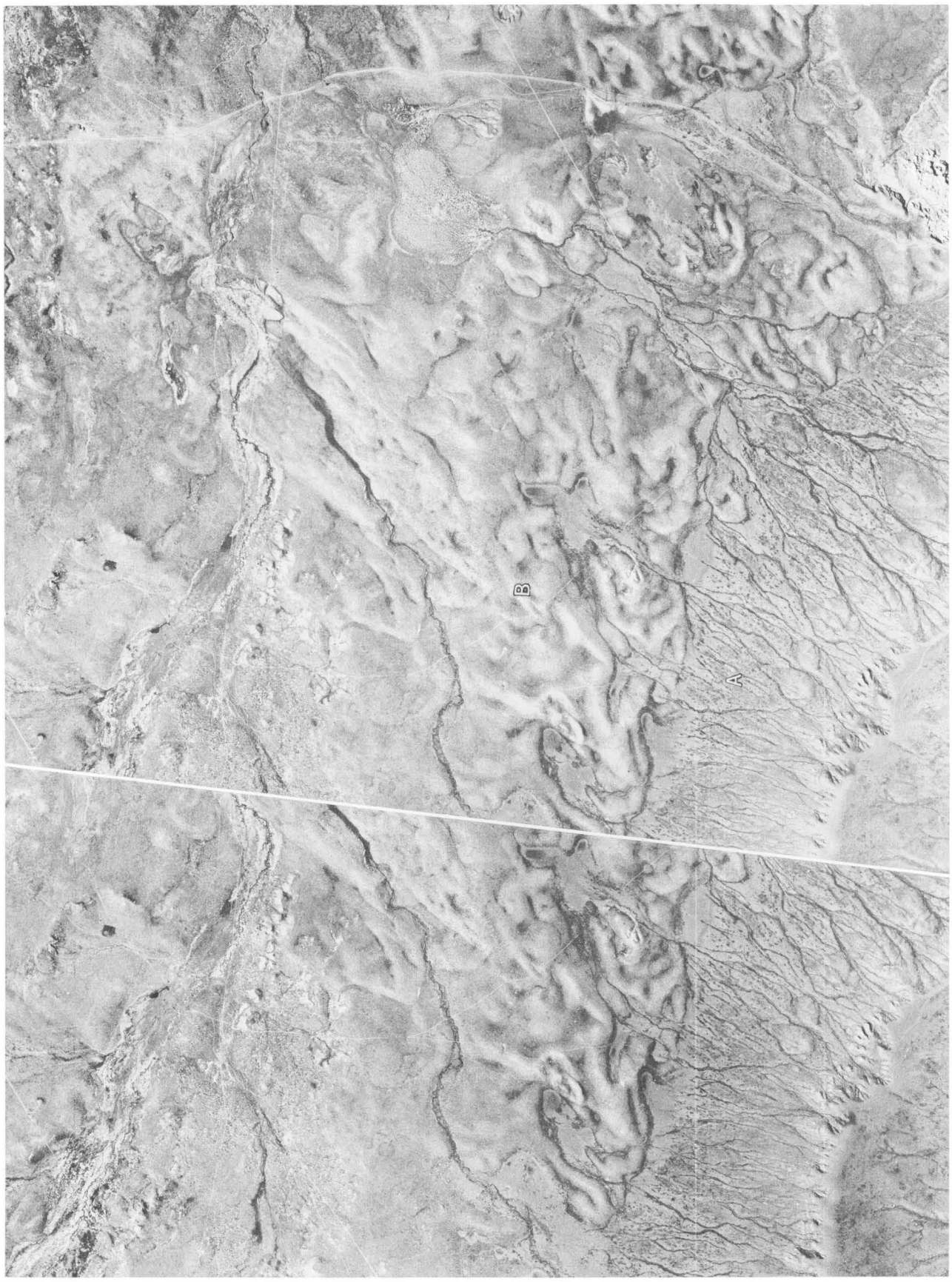

A
B
C
Stereoscopic pair
Approximately 1 mile

FIGURE 51.—STEEPLY DIPPING SEDIMENTARY ROCKS INTRUDED BY QUARTZ DIORITE (CALIFORNIA).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

Generally massive dark-toned conglomerate sequence, *A*, exhibits coarse-textured drainage and erosional characteristics, whereas fine-grained weakly foliated quartz diorite, *B*, has a fine-textured drainage and erosional topography. Widely spaced joints, conspicuous in many intrusive masses, are not present in the quartz diorite. Dendritic drainage in the conglomerate sequence is not typical of most dipping sedimentary rocks; the dendritic drainage pattern suggests a massive character and uniformity of the conglomerate sequence and general lack of bedding which might control the drainage. Local light-toned interbeds, *C*, indicate strike and dip of the sedimentary rock sequence.



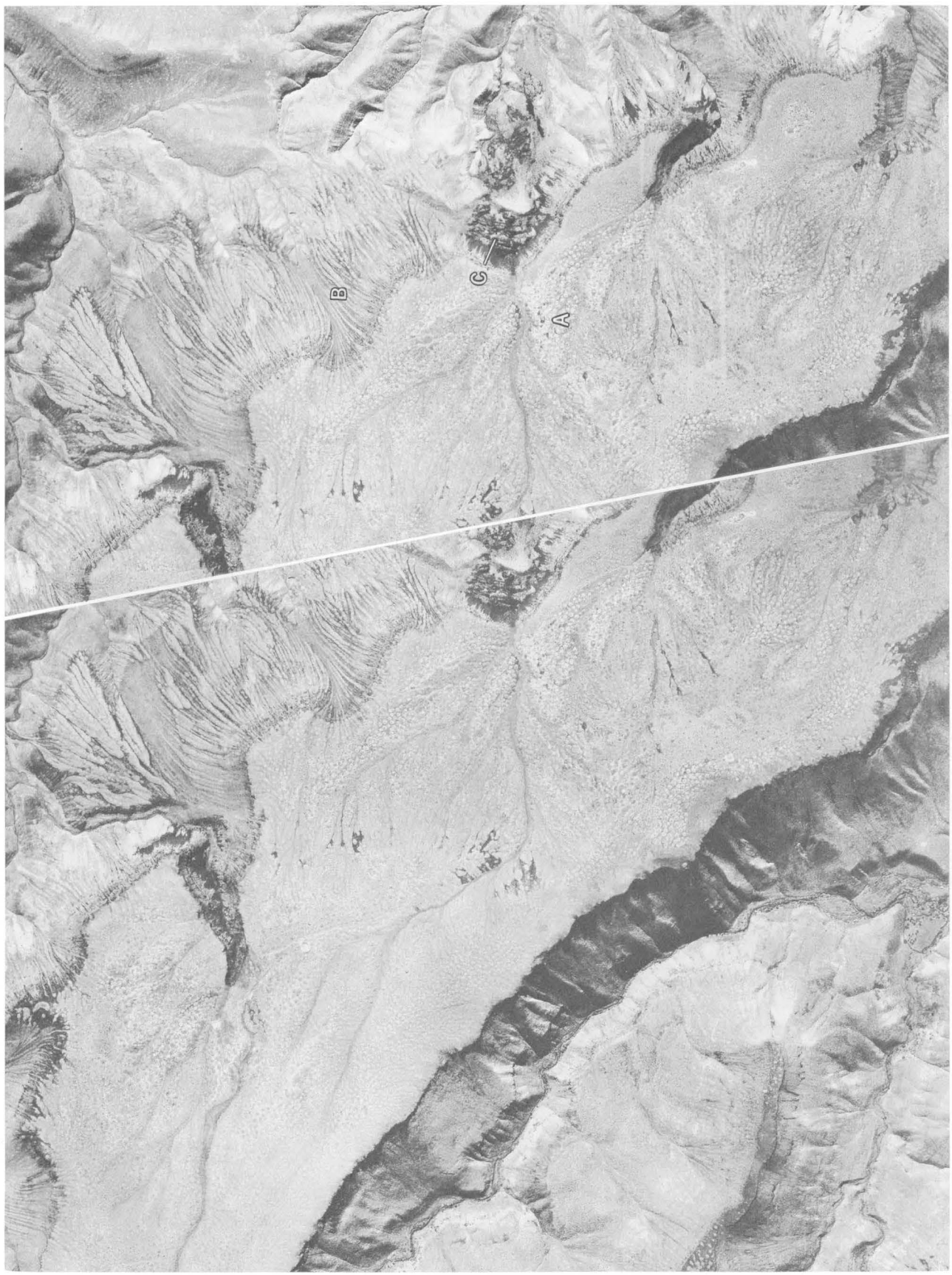
Stereoscopic pair

Approximately 1 mile

FIGURE 52.—AREA SHOWING DRAINAGE CHARACTERISTICS IN SURFICIAL MATERIALS (WYOMING).

[Approximate scale 1 : 28,000. Photographs by U.S. Geological Survey]

Strong contrast in drainage densities of areas *A* and *B* reflect differences in underlying materials. Fine-grained surficial sedimentary deposits, *A*, that form a thin cover on impermeable shale here exhibit fine-textured drainage. The many drainage rills flowing across the fine-grained surficial material disappear into sand dune area, *B*, which is composed of granular material of high permeability. Although partly stabilized and covered by vegetation the sand dunes locally show barchan shapes, which aid in their identification.



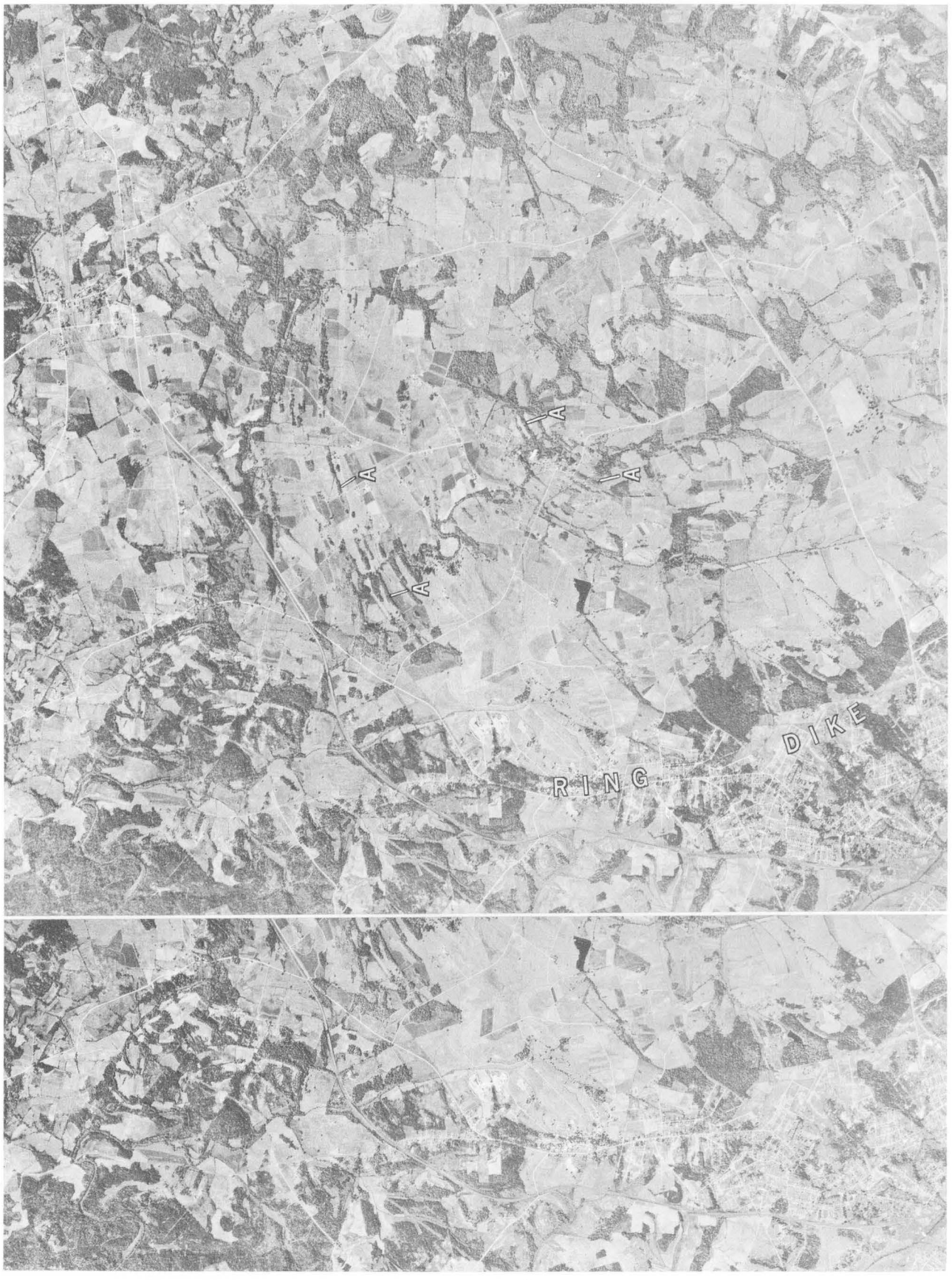
Stereoscopic pair

Approximately 1 mile

FIGURE 53.—AREA OF BASALT FLOWS (IDAHO).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Conspicuous "snakeskin" pattern is commonly found on the undissected basalt flows, *A*; it is not observed on other rock types in this area. The pattern consists of white or light-toned spots scattered in a dark field. Note that a rounded "shape" is a distinctive part of the pattern. The light-toned rounded areas are mounds of clay and silt 20 feet or more across and 2 or 3 feet high. Grass grows on these areas and causes the light photographic tone; the basalt is typically barren or covered with sagebrush and has a dark photographic tone. The striped pattern of closely spaced drainage rills, *B*, is also typical of basalt talus slopes in this area; however, similar-appearing stripes are found on a variety of rock types in other areas (see fig. 40). Where basalt cappings are underlain by poorly resistant rocks, conditions are favorable for landslides, as at *C*.



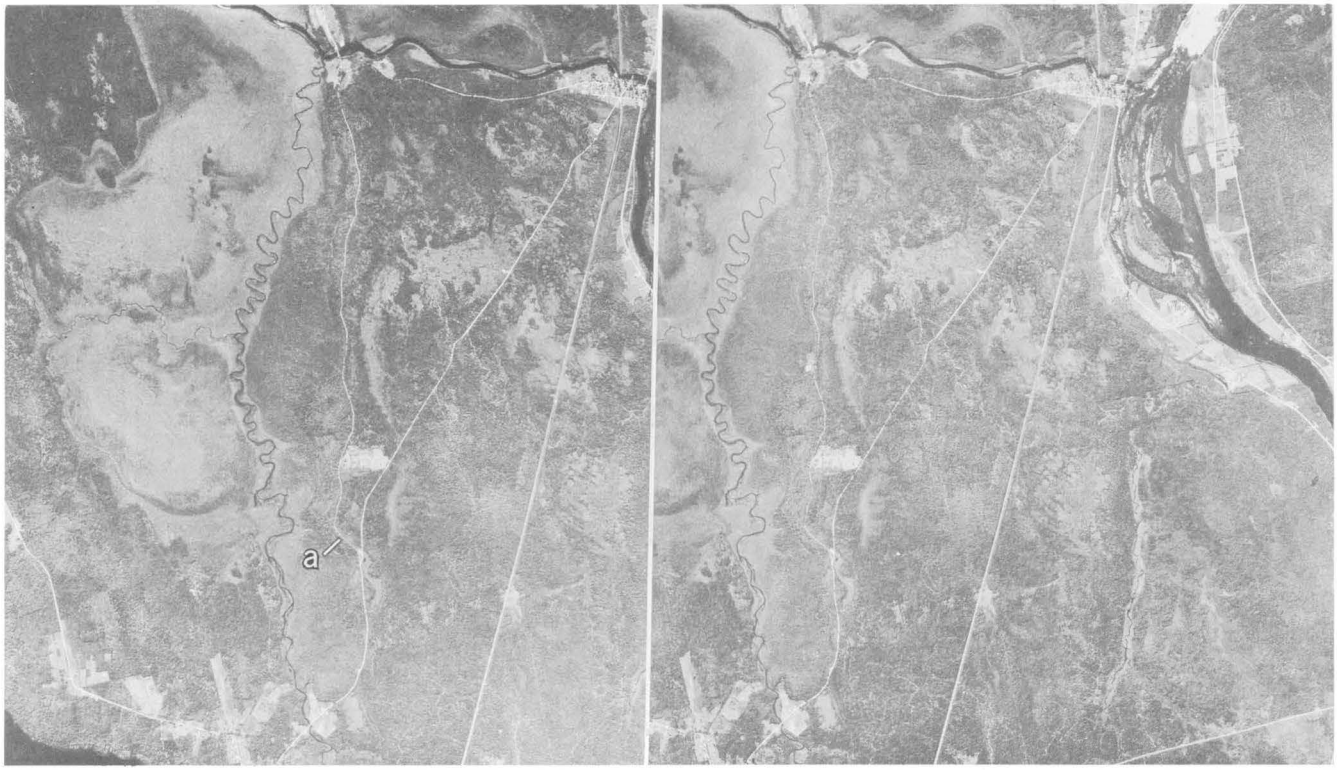
Stereoscopic pair

Approximately 1 mile

FIGURE 54.—RING-DIKE AREA (NORTH CAROLINA).

[Approximate scale 1 : 58,000. Photographs by Army Map Service]

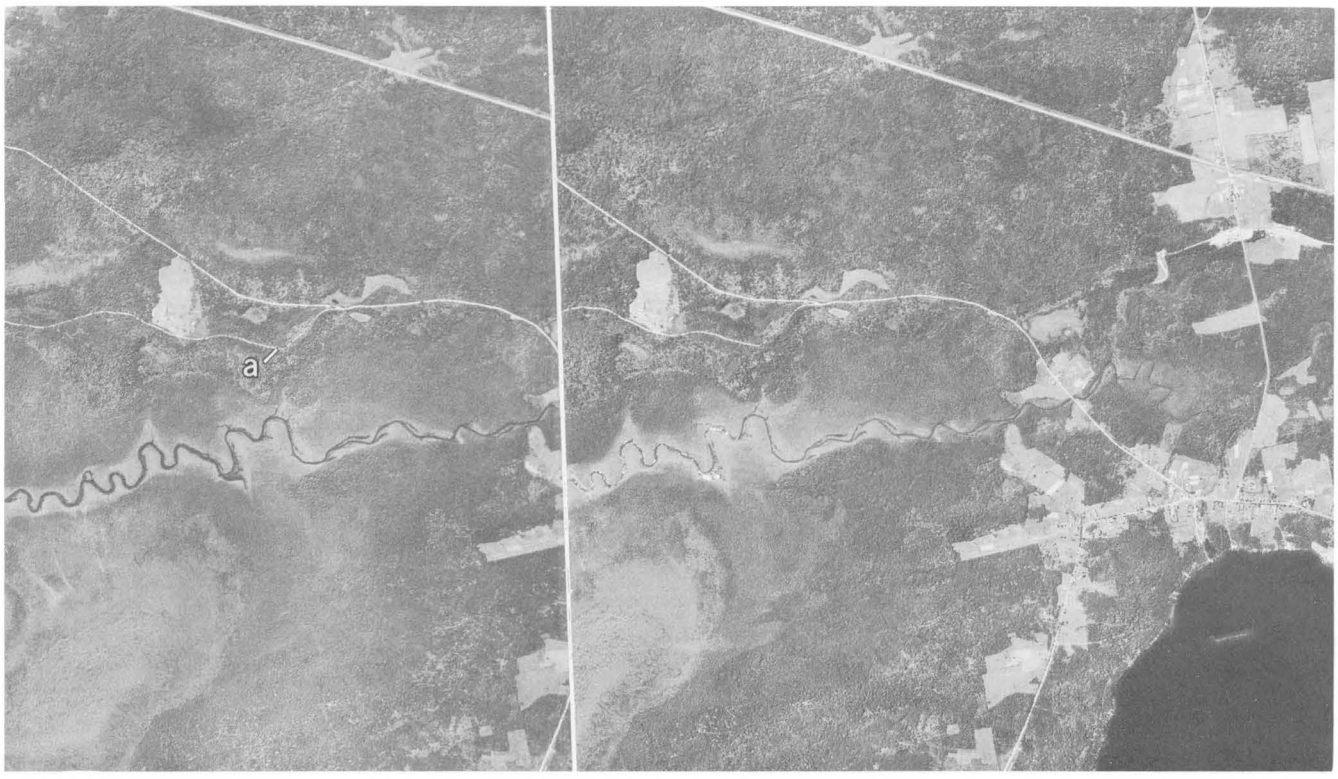
Ring dike about 1 mile wide and an area of gabbro-diorite within the ring dike can be differentiated from surrounding areas primarily on the basis of the lesser tree coverage and greater land use within the ring-dike area. A ring structure is also suggested by the concentric pattern of trees, *A*, which may reflect structure within the igneous rocks. The contact of syenite of the ring dike and gabbro-diorite of surrounding areas cannot be identified in the stereoscopic model, and aerial photographs of this terrain serve primarily to differentiate anomalous features which then must be examined in the field. Note excavation in syenite of the ring dike.



A

Stereoscopic pair

Approximately 1 mile



B

Stereoscopic pair

Approximately 1 mile

FIGURE 55.—AREA IN MAINE SHOWING ESKER LANDFORM ON PHOTOGRAPHS OF TWO DIFFERENT SCALES.

[*A:* Approximate scale 1 : 70,000. Photographs by Army Map Service]
[*B:* Approximate scale 1 : 44,000. Photographs by U.S. Geological Survey]

The serpentine shape in plan view and local topographic relief of the esker are readily distinguished in the stereoscopic view of figure *A*. The esker ridge is discontinuous, but the various segments are clearly part of the same ridge. The association of isolated ridge segments is readily made when small-scale photographs showing a large area are viewed. Landform is the primary recognition feature of esker ridges. In figure *B* the esker landform is not as readily identified as in figure *A*, and on commonly available 1:20,000-scale photographs the serpentine shape would probably not be seen in any one stereoscopic model. Esker sands and gravels are commonly well drained and are a source of borrow material for the construction engineer. Note old secondary road, *a*, built along the top of the esker, probably because of good subgrade and drainage.

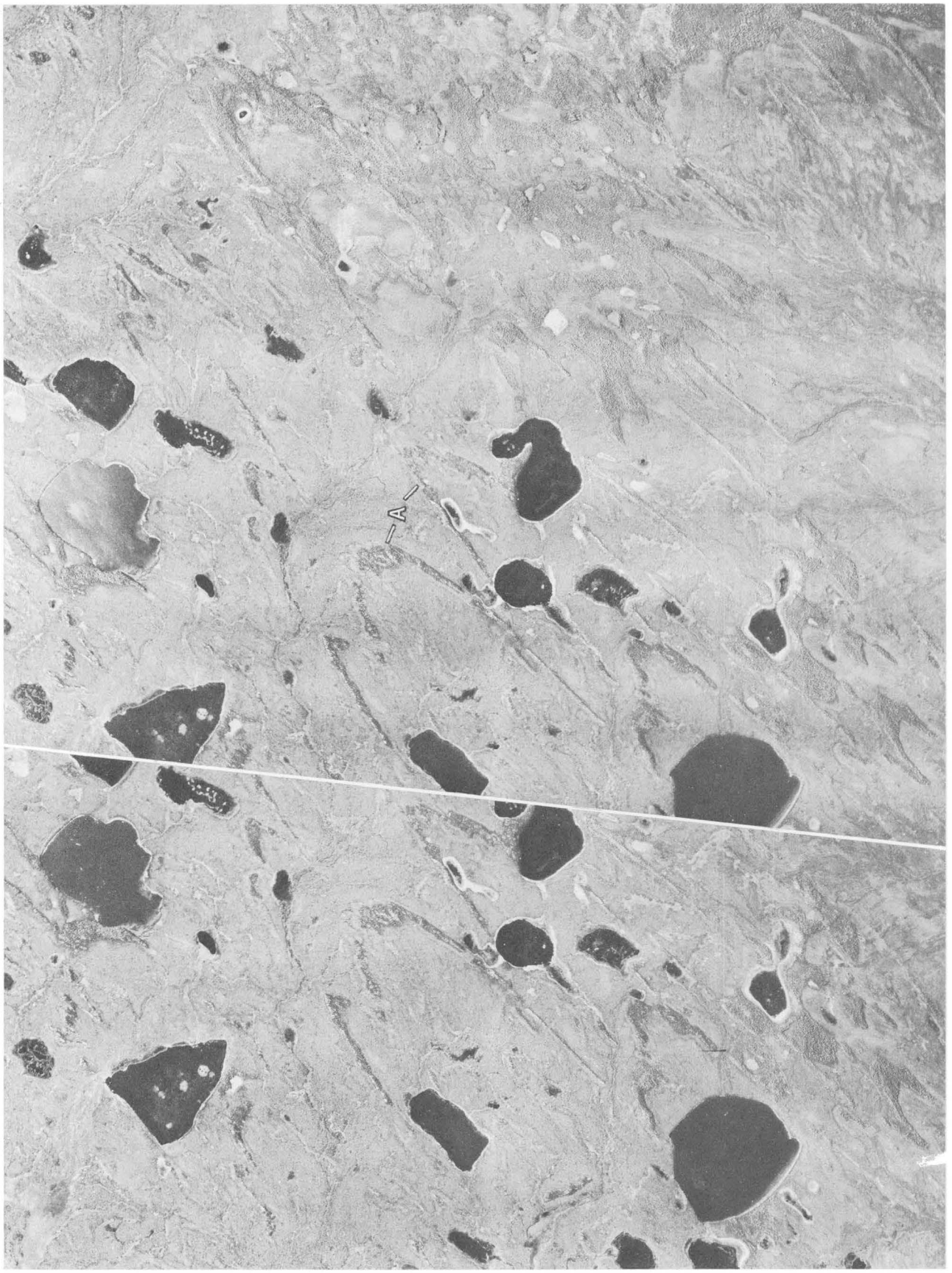
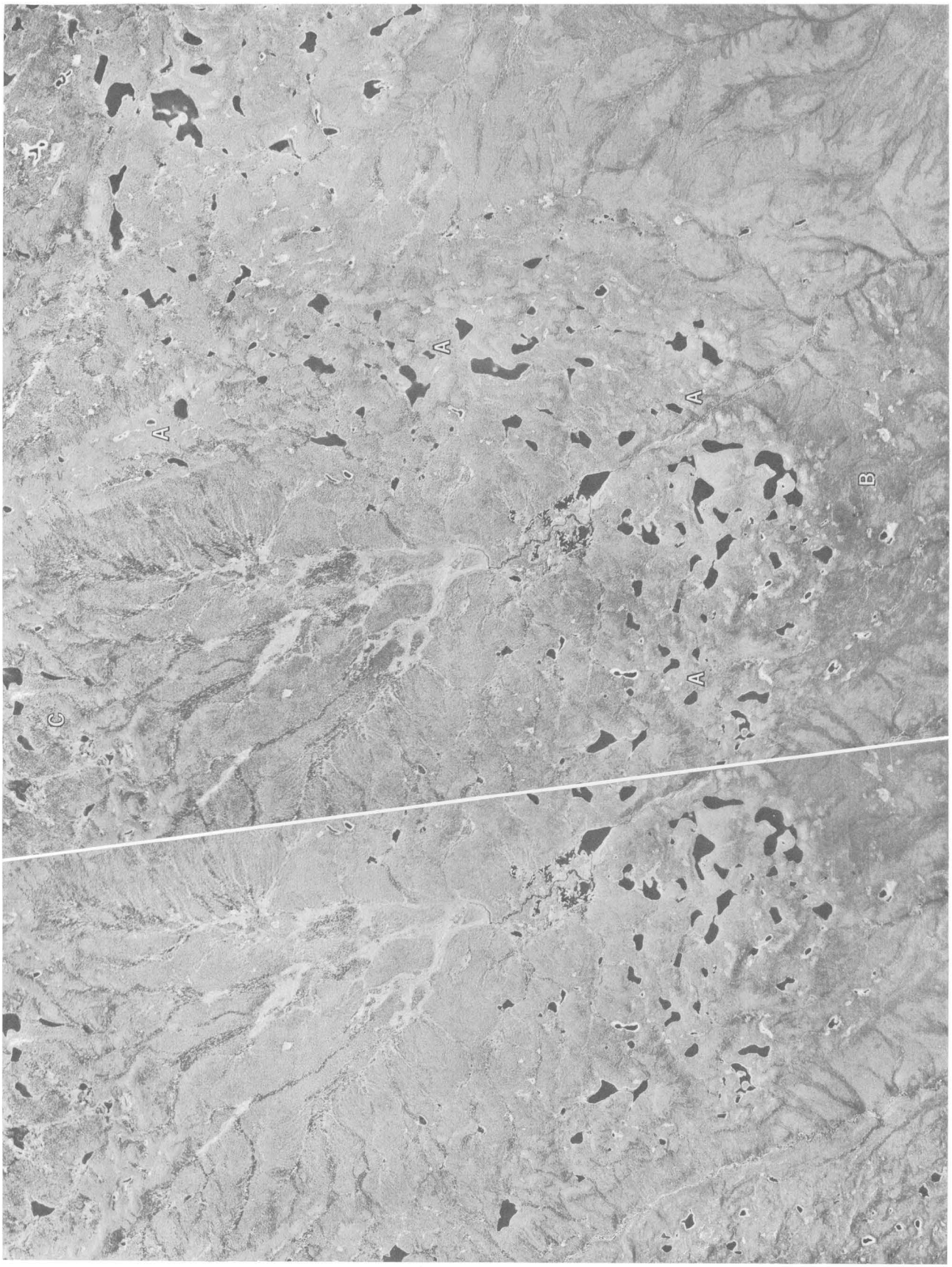

A
A
Stereoscopic pair
Approximately 1 mile

FIGURE 56.—STABILIZED SAND DUNES (CENTRAL ALASKA).

[Approximate scale 1 : 40,000. Photographs by U.S. Air Force]

Strong contrasts in photographic tone and photographic texture mark sand dunes and interdune areas. Dunes, as at *A*, are now stabilized and covered with trees. Coarse well-drained sands of the dunes support dark-toned black spruce. Light-toned interdune areas of frozen silt support grasses. Lakes were formed on the original glacial outwash plain, which was the source of sand for dune formation. The shape of the dune landform is an important aid to recognition, and the association of trees is significant in the interpretation of the soils and ground conditions. Relief of the dunes is vertically exaggerated in the stereoscopic model.



Stereoscopic pair

Approximately 1 mile

FIGURE 57.—MORAINAL DEPOSITS OF TWO GLACIATIONS (CENTRAL ALASKA).

[Approximate scale 1 : 40,000. Photographs by U.S. Air Force]

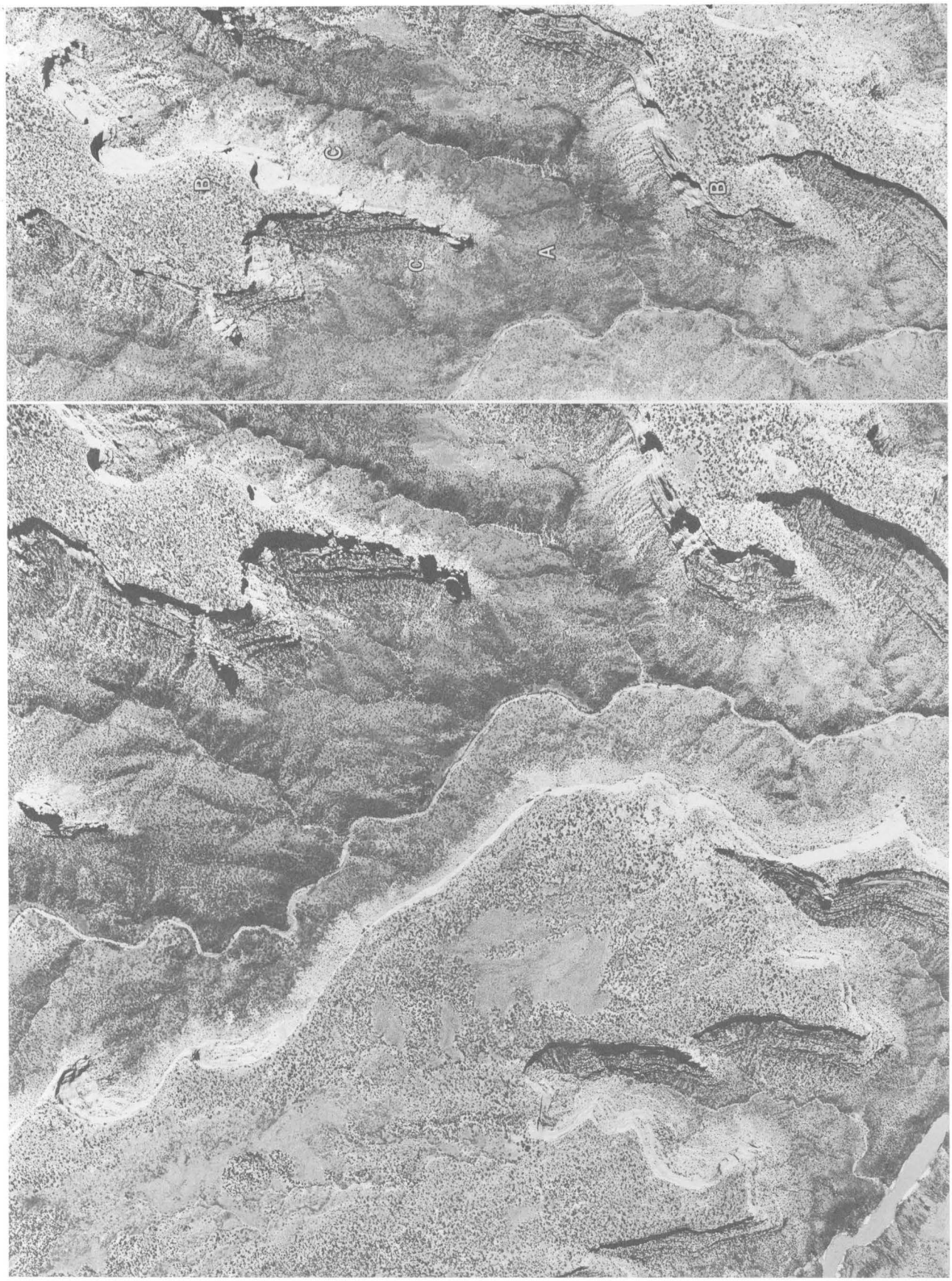
Arcuate plan-view shape of terminal moraine, *A*, is marked by a lighter photographic tone than that of the surrounding area. This moraine is characterized by an abundance of small undrained lakes and ponds and by poorly integrated drainage. In older terminal moraine, *B*, lakes and ponds are largely drained, but arcuate plan of this moraine is still preserved. Terminal moraine, *C*, represents an advance only slightly younger than *A*. Note similarity of topographic expression and development of ponds and lakes in moraines *A* and *C*.

Stereoscopic pair
Approximately 1 mile

FIGURE 58.—MORAINAL DEPOSITS OF CONTINENTAL GLACIATION (SOUTH DAKOTA).

[Approximate scale 1 : 60,000. Photographs by Army Map Service]

Terminal moraine, *A*, contains generally few lakes and ponds in contrast with older ground moraine, *B*, in which water-filled kettle holes are numerous. Arcuate plan-view shape and higher relief than surrounding ground moraine are typical of the terminal moraine. Note drainage rills developed on parts of topographically high terminal moraine, but general lack of well-developed surface drainage in ground-moraine areas. Ponding also indicates poor drainage in this area. Linear trends parallel to arcuate border of terminal moraine—which represent depositional and erosional characteristics—are similar to some linear trends indicative of faults in other areas.



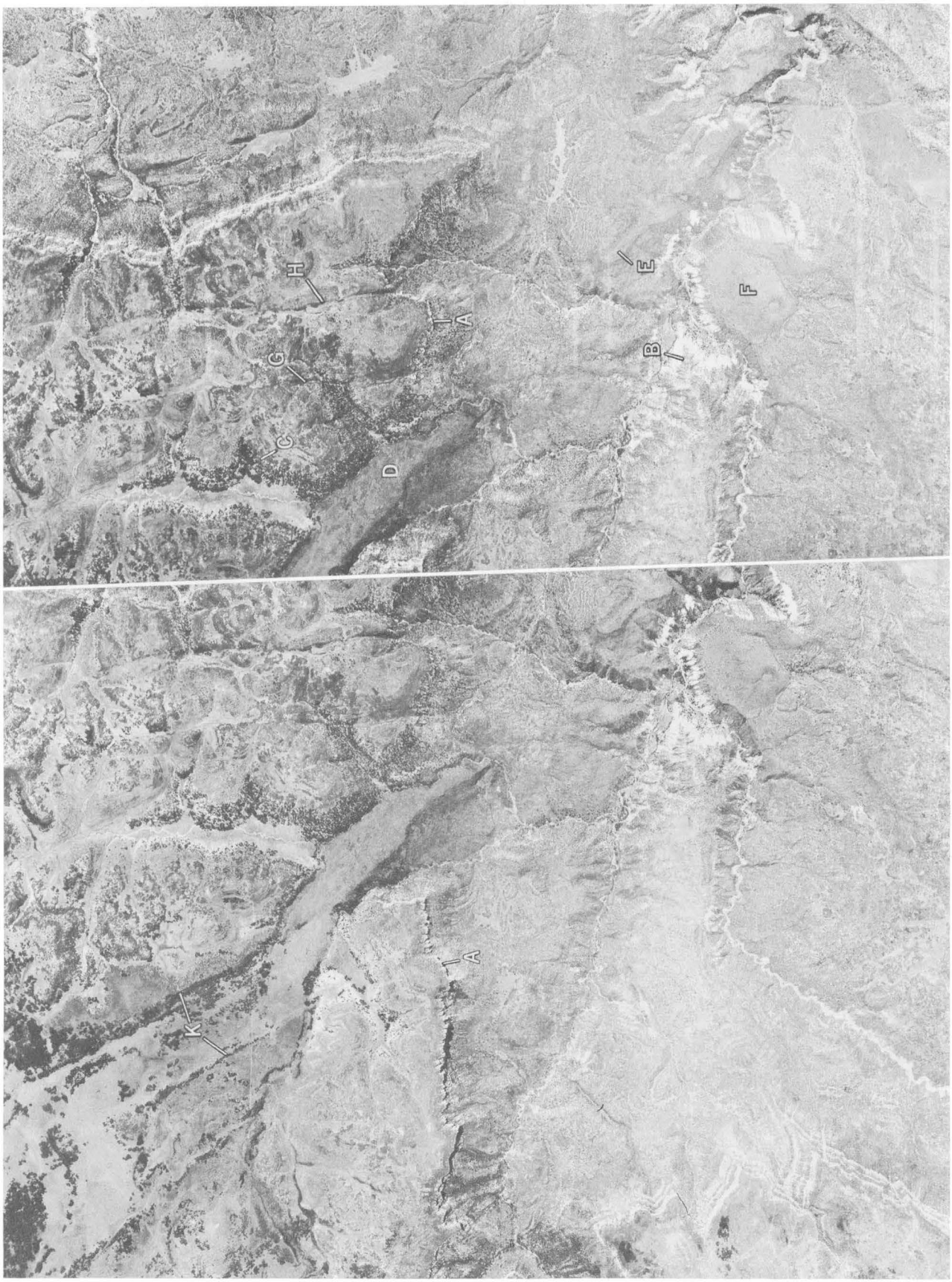
Stereoscopic pair

Approximately 1 mile

FIGURE 59.—GENTLY DIPPING SEDIMENTARY ROCKS LYING UNCONFORMABLY ON GNEISS-GRANITE-SCHIST COMPLEX (UTAH).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

Strong photographic tone differences mark the gneiss-granite-schist area, *A*, and the sedimentary rocks, *B*. Relatively even dip-slope surfaces of sedimentary rocks contrast strongly with hummocky erosional topography of underlying crystalline rocks. The fine-textured dendritic drainage on the crystalline rocks stands out, although such fine-textured drainage is not necessarily diagnostic or typical of igneous and metamorphic areas. The gneiss-granite-schist area shows no bedding, but bedding is marked in the overlying sedimentary rocks by topographic breaks in slope. Light photographic tone and vertical cliffs are characteristic of thick sandstone formation in this area. Large talus blocks, at base of slope, *C*, indicate massive and resistant character of overlying rocks. Shale and silty shale unit below sandstone has a lesser angle of slope, but this slope is masked in part by debris from overlying sandstone.



Stereoscopic pair

Approximately 1 mile

FIGURE 60.—GENTLY DIPPING SEDIMENTARY ROCKS CUT BY NUMEROUS NEAR-VERTICAL FAULTS (UTAH).

[Approximate scale 1 : 63,360. Photographs by Army Map Service]

Sedimentary rocks are indicated particularly by topographic expression. Jointed, resistant sandstone beds stand in bold cliffs, *A*. Soft rocks have lesser angles of slope. Strong photographic tone differences mark contacts of some rock units, as at *B*; locally vegetation changes are suggestive of different rock types, *C*.

Lava flow, *D*, cuts discordantly across formational contacts. Remnant lava flow at *E* appears to have been continuous with flow at *D*. Small cinder cone, *F*, demonstrates use of shape as a recognition element of constructional landforms.

Faults are commonly marked by conspicuous topographic alinements (*G*, *H*). Throw on fault *G* is about 100 feet; on *H* the throw is about 150 feet. Note narrow alinements of vegetation marking faults, *K*.

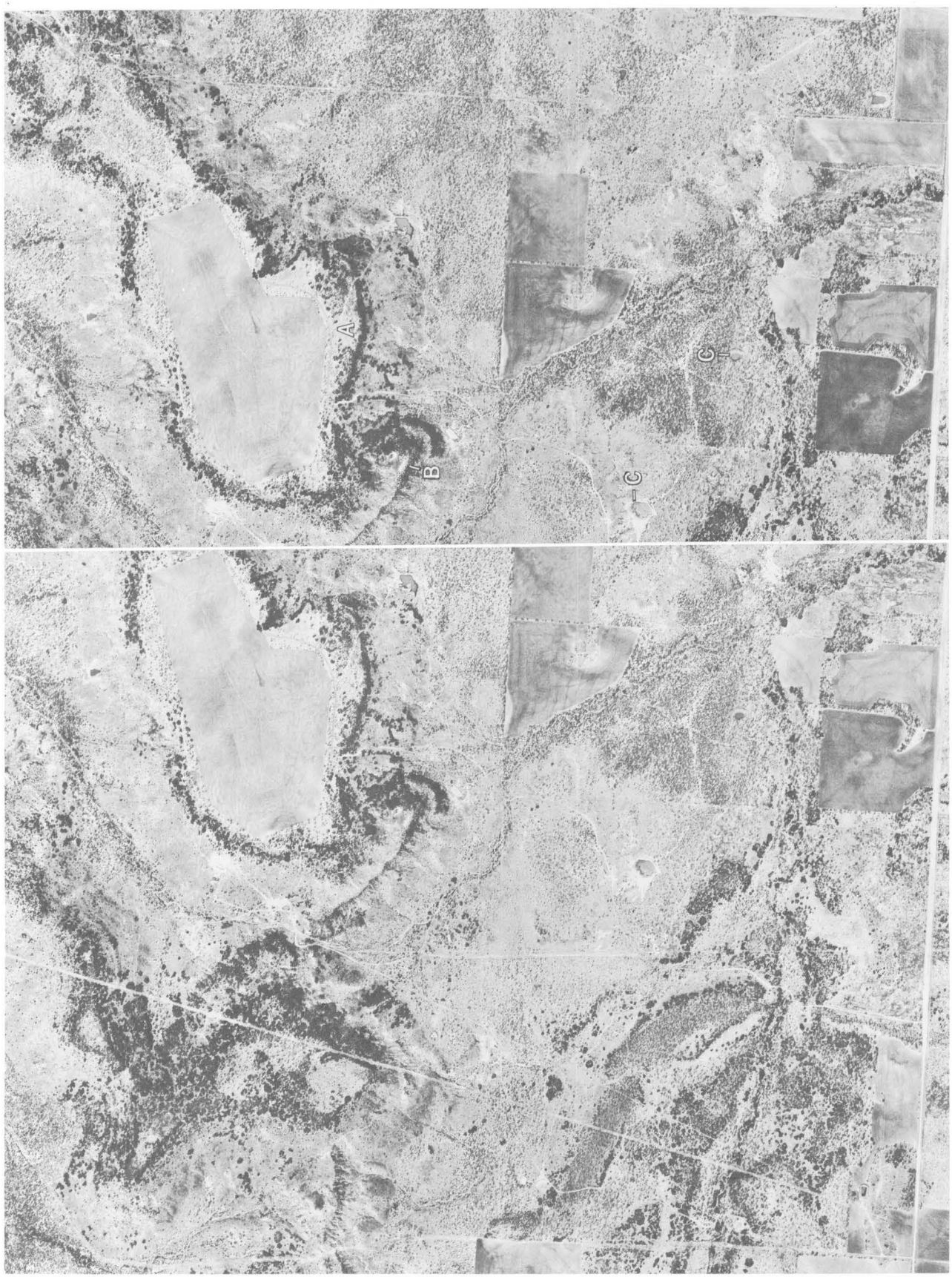
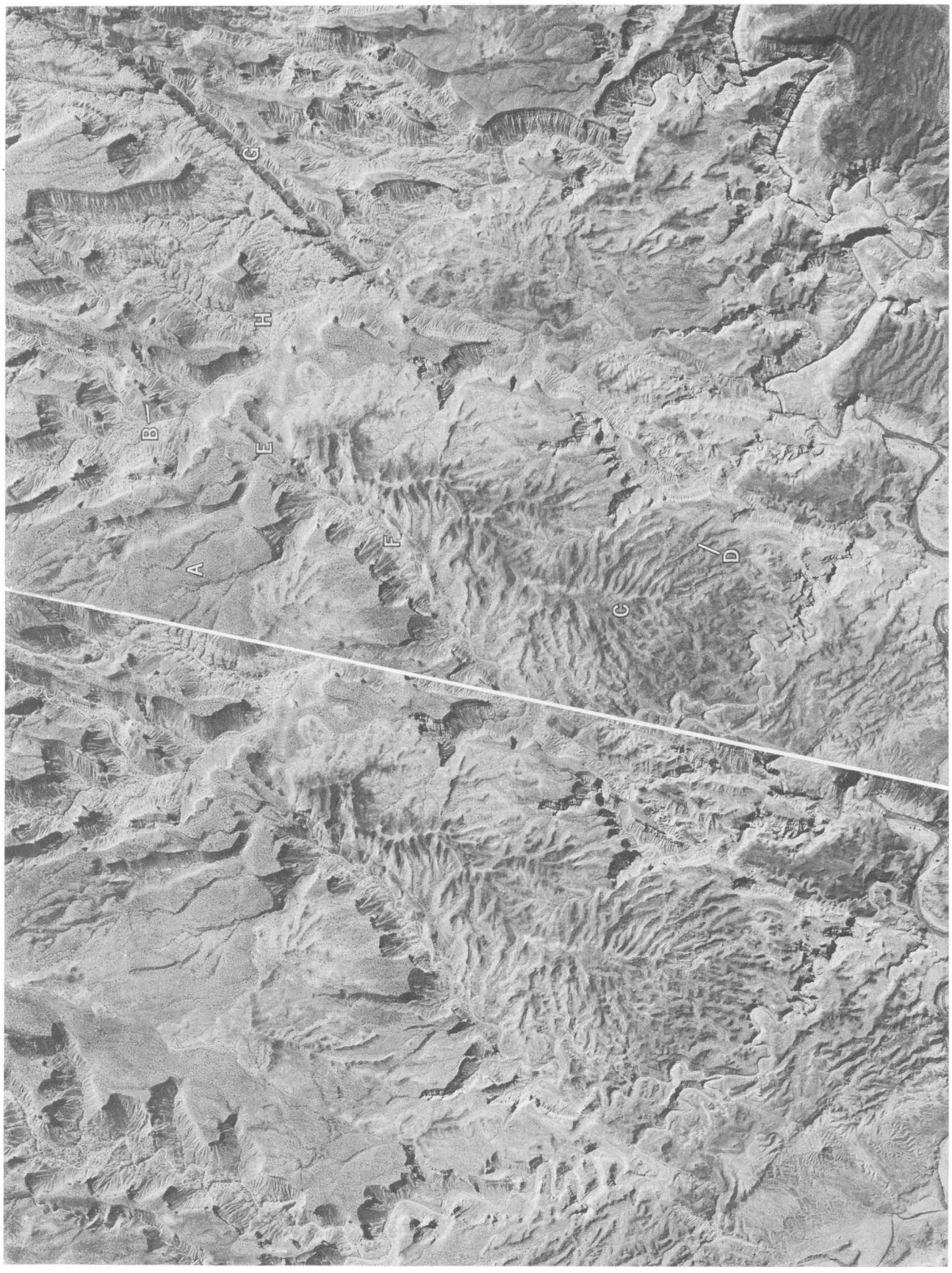

A
B
C
C
Stereoscopic pair
Approximately 1 mile

FIGURE 61.—FLAT-LYING BEDS OF SANDSTONE, LIMESTONE, AND SHALE (TEXAS).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Limestone caprock, *A*, shows a concentration of oak trees along rim but not across capping bench, which is covered by a veneer of cherty conglomerate. Sandstone break at *B* also has oak trees. Certain oaks have an affinity for limestone soils and some for sandy soils, but oak types are not distinguishable on conventional black-and-white photographs at a scale of 1:20,000. Shale valleys are covered with mesquite and locally have stock tanks, *C*, which suggest underlying impermeable materials. Note dendritic drainage and distribution of vegetation bands along the topographic contour, which in places form closed loops and suggest flat-lying or nearly flat-lying beds.



Stereoscopic pair

Approximately 1 mile

553966 O-60—6

FIGURE 62.—AREA OF FAULTED, GENTLY DIPPING SEDIMENTARY ROCKS (UTAH).

[Approximate scale 1 : 37,000. Photographs by U.S. Geological Survey]

Strong contrasts in drainage densities and in erosional features of the terrain result from different sedimentary rock types. Coarse-textured drainage of little-dissected area, *A*, marks a persistent limestone bed that locally forms bluffs. These bluffs overlie fine-grained sandstone and shale, *B*, which have a lesser angle of slope than the limestone, although the difference in slope angle is masked by the vertical exaggeration of the stereoscopic model. Note that top of limestone and topographic surface coincide permitting ready estimate of the amount of dip. Dark-toned shale and fine-grained sandstone and sandy shale at *C* show fine-textured drainage and erosional topography. Note closely spaced joints in fine-grained sandstone beds at *D*. Vertical offsets of resistant limestone bed at *E* are conspicuous. Drainage along trace of faults is prominent at *F* and *G*. A lower sandstone, *H*, contrasts locally with overlying dark sandstone and shale as a result of its light photographic tone and cover of scattered small trees.

Stereoscopic pair

Approximately 1 mile

FIGURE 63.—SHALE IN SEMIARID CLIMATIC AREA (UTAH).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

Fine-textured drainage is typical of shale and other fine-grained clastic rock types. Relief is commonly subdued and divide areas gently rounded. Note that rounding of some divide areas may not be conspicuous because of vertical exaggeration of the stereoscopic model. For example, the relief at *B* is only about 70 feet. The fine-textured drainage and erosional topography suggest plastic soils. The numerous angular crenulations in minor tributaries probably reflect closely spaced joints. Thin light-toned bands, *A*, are expressions of bedding.

Stereoscopic pair

Approximately 1 mile

FIGURE 64.—SHALE AND LIMESTONE IN HUMID CLIMATIC AREA (VIRGINIA).

[Approximate scale 1 : 43,000. Photographs by U.S. Geological Survey]

Gently dipping shale, *A*, shows a fine-textured drainage. Main streams draining shale flow almost directly in the downdip direction. Limestone underlies anticlinal ridge, *B*. Sinkholes are present locally, *C*, but are not conspicuous within the area. In general the limestone areas are less dissected than shale areas because of better internal drainage in limestone. Valley, *D*, is underlain by shale. Note discordance of strike of steeply dipping beds, *E*, with scarp, *F*, which suggests presence of a fault along this topographic break in slope. Thin resistant bed of sandstone, *G*, crops out conspicuously on flank of anticlinal ridge. Trellis drainage in area *D* is typical of folded sedimentary rocks.

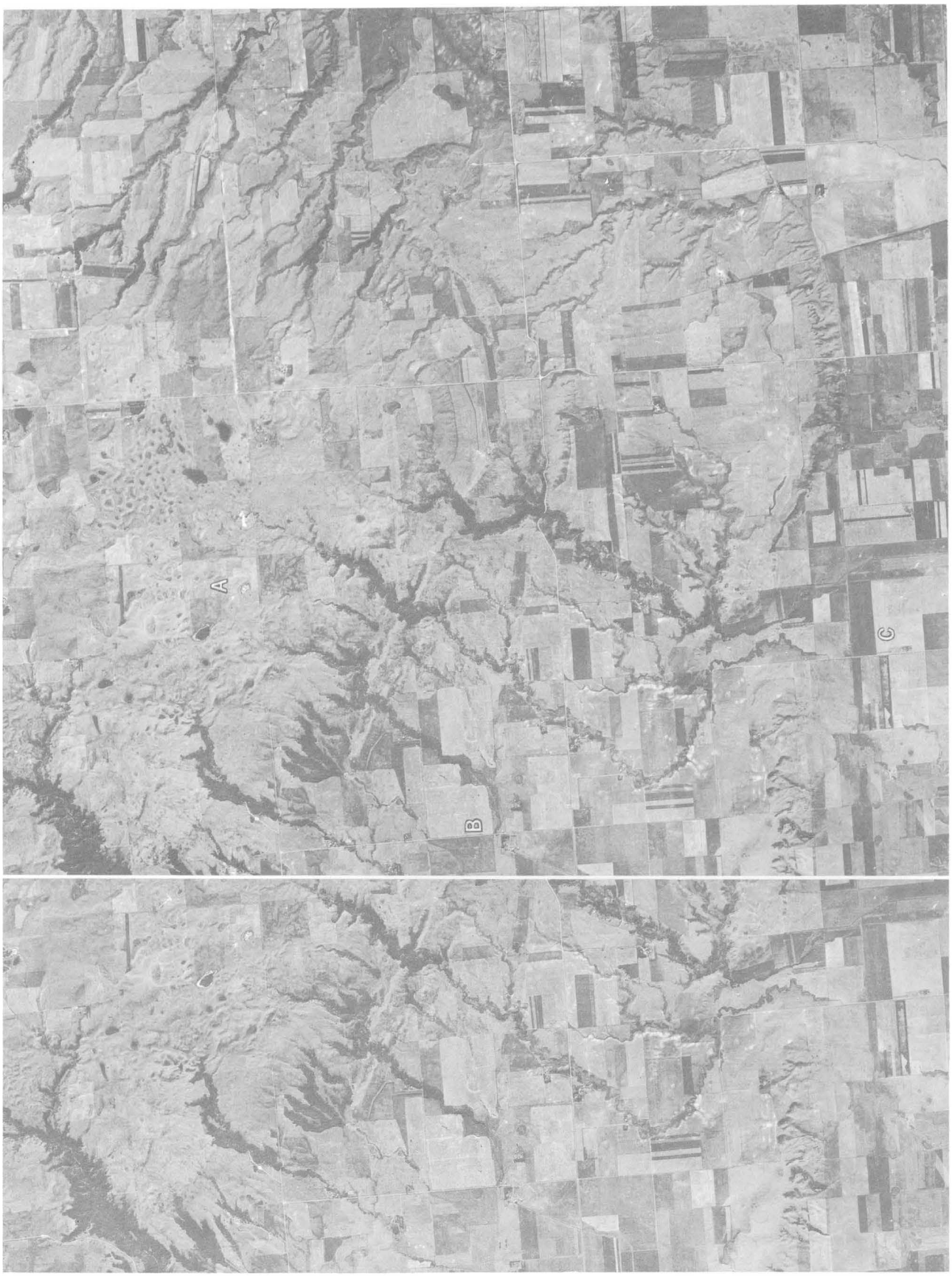
Stereoscopic pair

Approximately 1 mile

FIGURE 65.—AREA OF GENTLY DIPPING LIMESTONE AND SHALE (PENNSYLVANIA).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Impermeable shale, *A*, has a greater resistance to erosion than the limestone, *B*, and stands topographically high in this area. The contact of shale and limestone is marked by a pronounced topographic break, as at *C*. The shale has been noticeably dissected by stream erosion in contrast to the limestone in which drainage is in large part internal. Note orchards in well-drained limestone areas. Vegetation along stream valleys in the shale accentuates the drainage contrast of shale and limestone areas. Soil mottling, *D*, in limestone areas occurs where soil cover is thin and allows differences in moisture conditions, believed to result from drainage channels in the limestone bedrock, to stand out. Despite good drainage in the limestone area residual soils developed on limestone may react to engineering tests as a plastic soil and not as a granular soil. Limestone quarry is at *E*.



Stereoscopic pair

Approximately 1 mile

FIGURE 66.—AREA MANTLED BY GLACIAL DEPOSITS (SOUTH DAKOTA).

[Approximate scale 1 : 60,000. Photographs by Army Map Service]

Topographically high area, *A*, with typical knob-and-kettle topography is covered by morainal material; ponds are common but surface drainage channels are conspicuously absent. Rim of high ground has been noticeably dissected by deep channels. The distribution of these channels, accentuated by dark-toned vegetation, forms a radial pattern similar to that over some subsurface structures in other areas. Drainage disappears in permeable material, *B*, surrounding the high area. Contrast lack of surface drainage rills in moraine at *A*, where drainage is poor, as indicated by ponds, with lack of surface drainage rills in outwash at *B*, where internal drainage is good. Well-drained area, *C*, probably also represents glacial outwash.

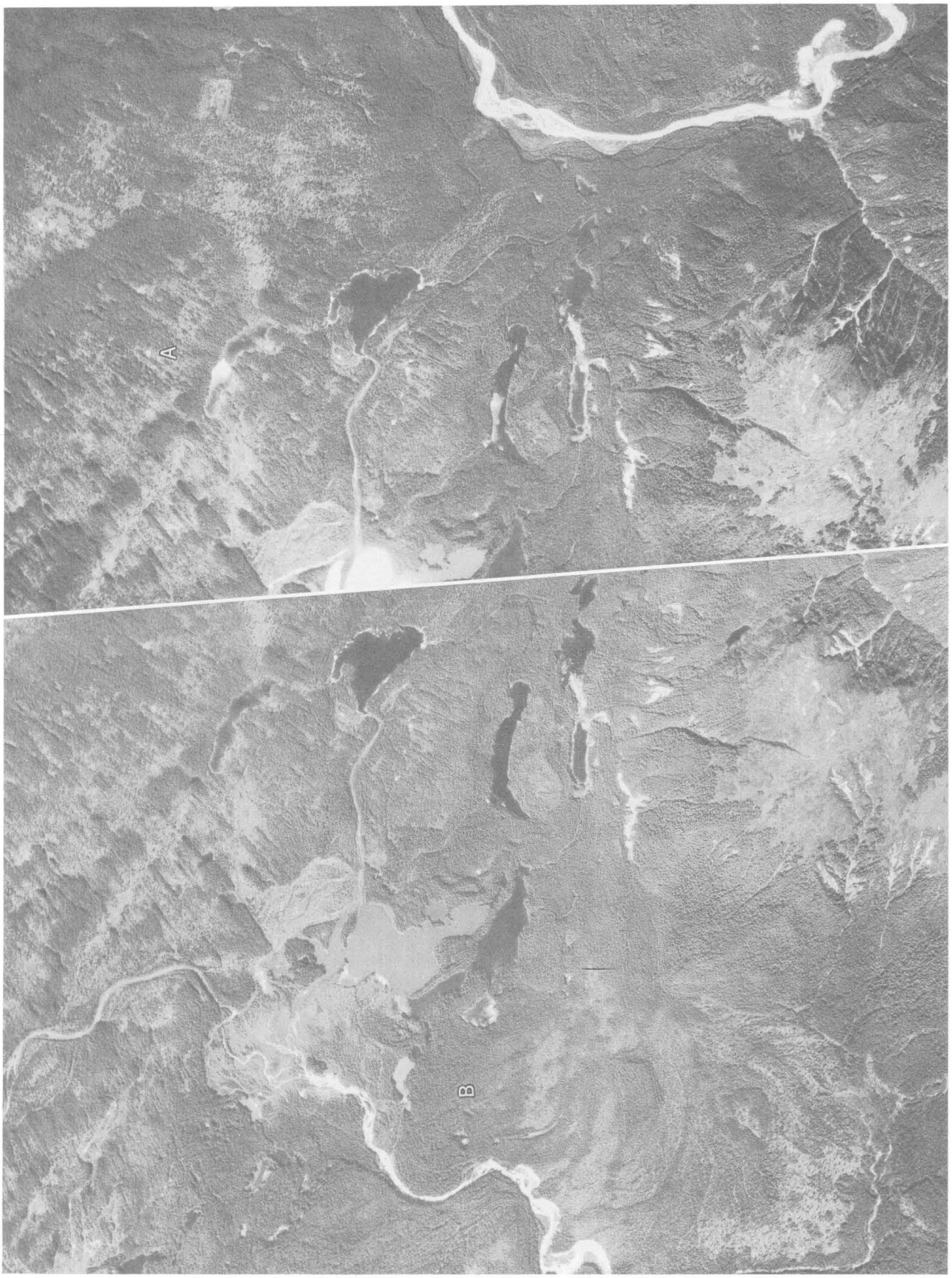

A
B
Stereoscopic pair
Approximately 1 mile

FIGURE 67.—GLACIATED AREA IN SOUTHEASTERN ALASKA.

[Approximate scale 1 : 40,000. Photographs by U.S. Navy]

Conspicuous linear trends, *A*, represent glacial grooving. These lineations, except for the fanning out in the direction of ice movement, may appear on photographs similar to lineations that represent foliation in metamorphic rocks. Drumlinoid features that give rise to this linear pattern are generally found in broad, flat, and topographically low areas, such as the floors of broad valleys. Commonly the drumlinoid features are elongated parallel or subparallel to the valley or general topographic grain. Lineations representing foliation on the other hand may transect or parallel the topographic grain; unlike drumlinoid features they are not restricted to any one topographic level. Pock-marked area, *B*, is glacial outwash and probably some glacial lake deposits.

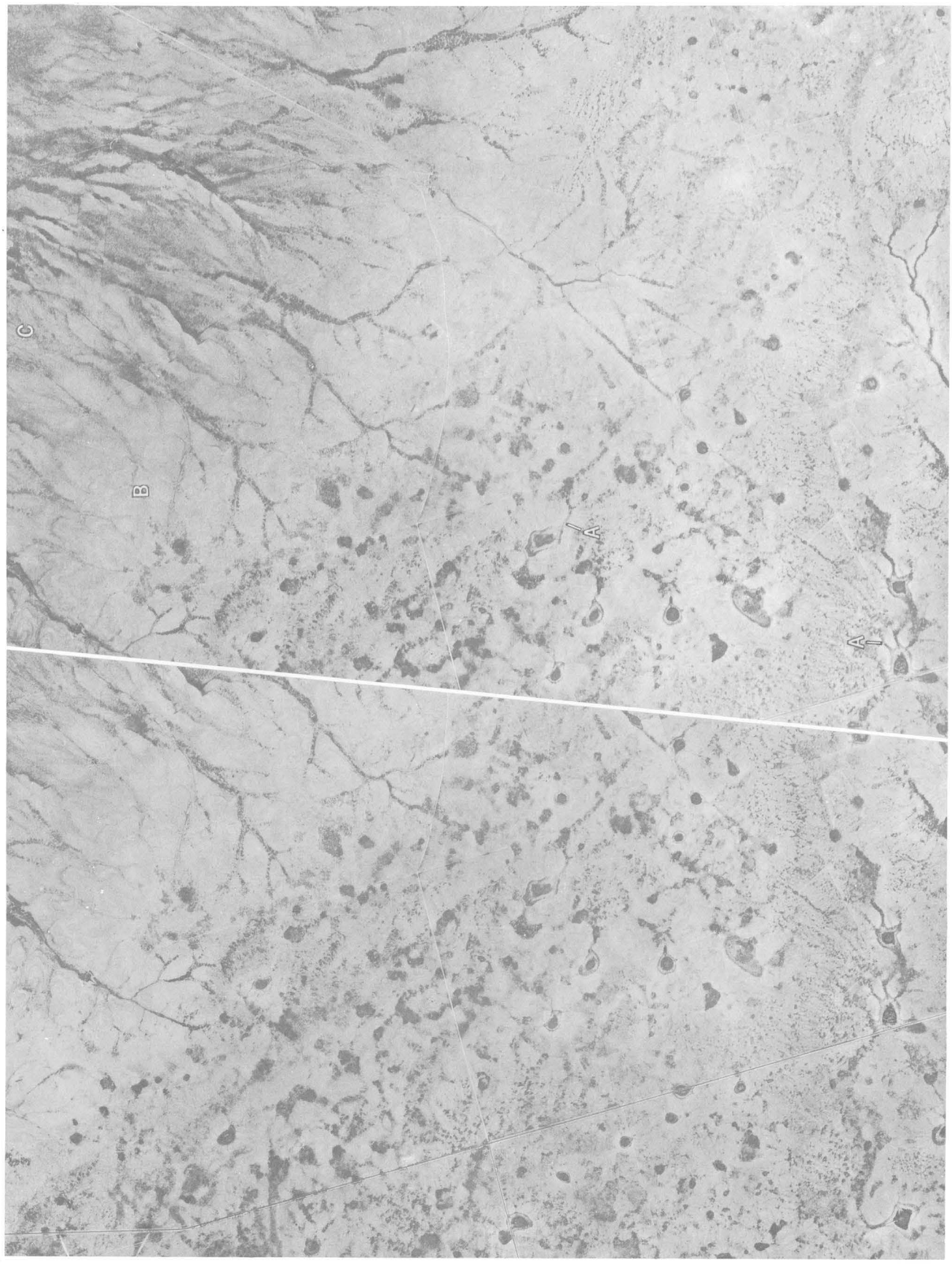
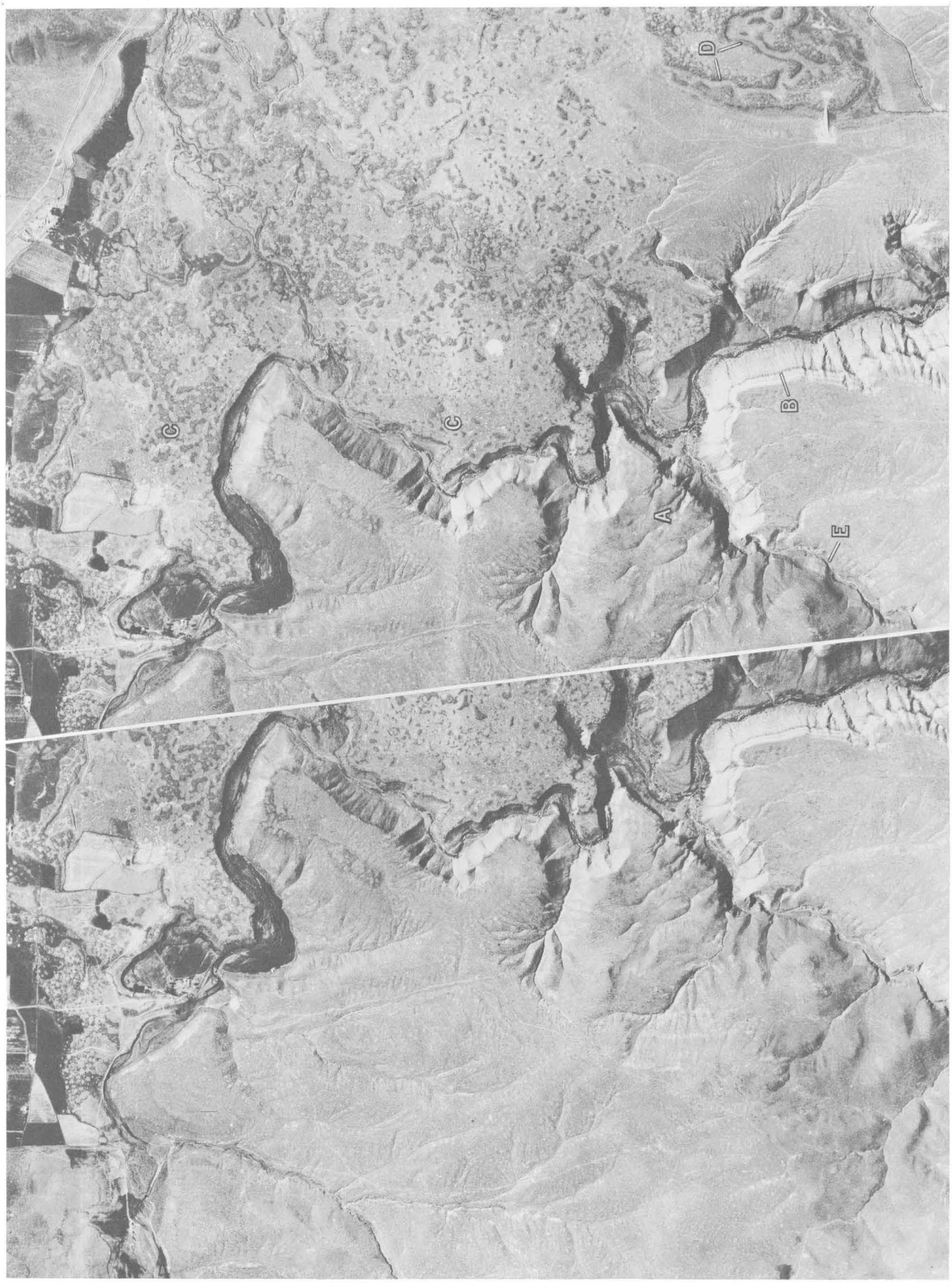

C
B
A
A
Stereoscopic pair
Approximately 1 mile

FIGURE 68.—APPROXIMATELY FLAT-LYING LIMESTONE AND INTERBEDDED SANDSTONE AND MARLSTONE BEDS COVERED LOCALLY BY ALLUVIUM AND WINDBLOWN DEPOSITS (TEXAS).

[Approximate scale 1 : 63,360. Photographs by Army Map Service]

Rounded dark-toned depressions are sink holes that mark area of limestone. Drainage is primarily internal and few surface drainage channels may be seen; a few short surface rills drain into the sink holes, as at *A*. In contrast to the limestone area, surface drainage is conspicuously developed in the interbedded sandstone and marlstone, *B*, but becomes less well developed in permeable alluvium and windblown deposits, *C*.



Stereoscopic pair

Approximately 1 mile

FIGURE 69.—AREA OF BASALT FLOWS (IDAHO).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

The oldest basalt, *A*, shows subdued rounded topography and well-developed surface drainage. A younger basalt, *B*, is interbedded with light-toned sedimentary rocks. Some surface drainage has developed on the sedimentary rocks. The youngest basalt, *C*, shows a "lizard skin" appearance on aerial photographs; locally a collapse structure may be present as at *D*. Almost no integrated surface drainage is present on the youngest basalt. Stream *E* flows in a fault valley. The fault is younger than, and separates, basalts *A* and *B*; basalt *A* has been upthrown.

Stereoscopic pair
Approximately 1 mile

FIGURE 70.—AREA OF GRANITE (SOUTH DAKOTA).

[Approximate scale 1 : 24,000. Photographs by U.S. Geological Survey]

Dendritic drainage, seen best in stereoscopic view, is typical of many terrains underlain by intrusive igneous rocks or other generally homogeneous rocks. The irregularly spaced joints in several different orientations are characteristic of granite and other intrusive rocks; extremely irregular topography is also common in such terrain. Banding, suggestive of sedimentary or metamorphic rocks, is absent. The occurrence of trees predominantly of one variety and the lack of conspicuous preferred orientation of vegetation is suggestive of uniform composition of bedrock.

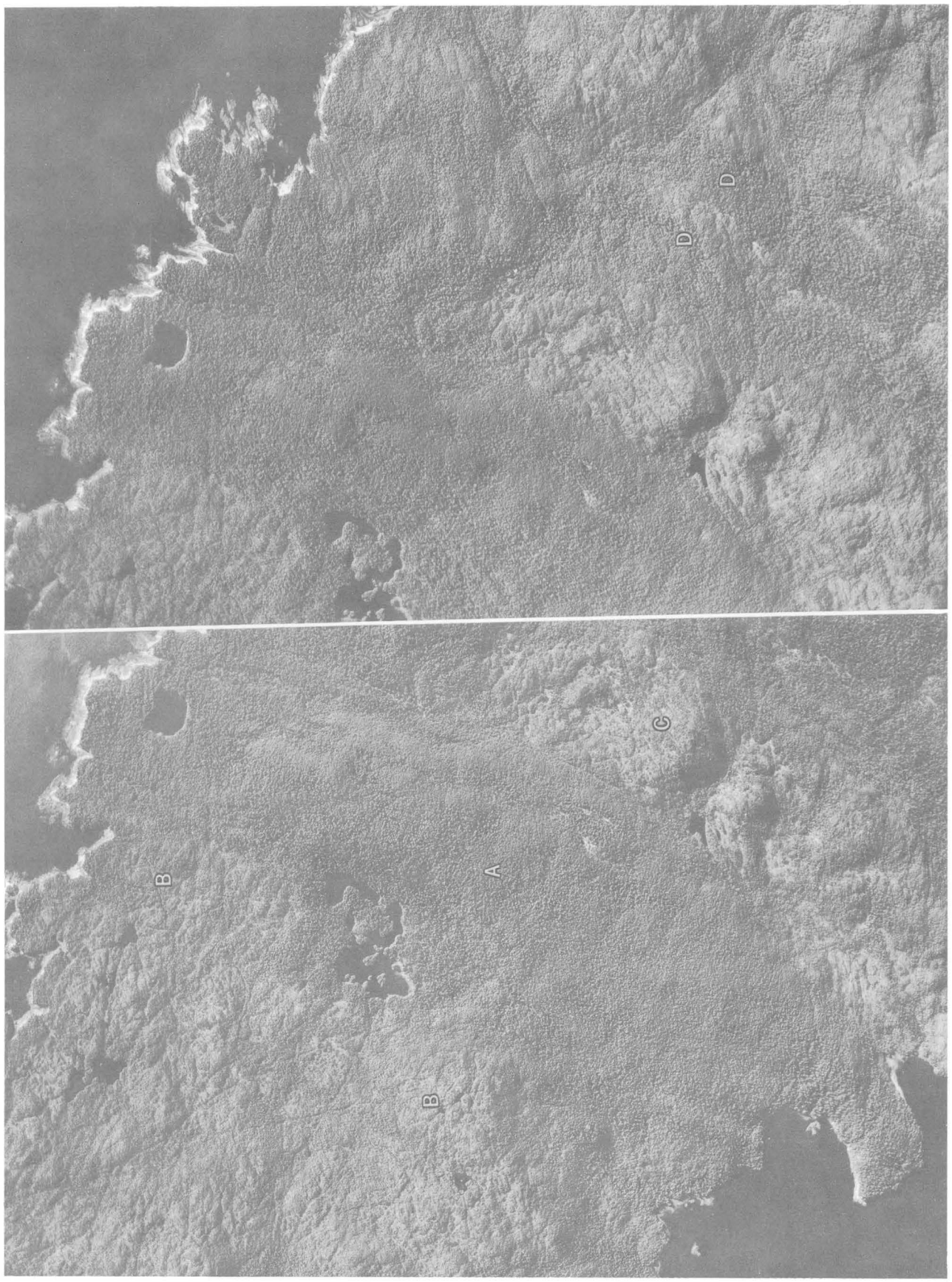
Stereoscopic pair

Approximately 1 mile

FIGURE 71.—AREA OF GRANITIC INTRUSIVE ROCKS (WYOMING).

[Approximate scale 1 : 28,000. Photographs by U.S. Geological Survey]

Profuse, irregularly spaced joints in several different orientations are typical, although not necessarily diagnostic, of intrusive igneous rocks. The massive character of the rocks and apparent lack of bedding in turn suggest igneous intrusive rocks, although locally the rocks shown appear similar to some highly fractured massive sandstone. Conspicuous rectilinear depressions, as at *A*, marked by dark-toned vegetation, are shear zones that are more easily eroded than surrounding rock areas, and probably have a higher concentration of moisture that supports vegetation growth. In places, as at *B*, older shear zones have been offset by younger fractures. Note strong control of drainage by faults and joints.



Stereoscopic pair

Approximately 1 mile

FIGURE 72.—AREA SHOWING VEGETATION DIFFERENCES IN IGNEOUS-METAMORPHIC TERRAIN (SOUTHEASTERN ALASKA).

[Approximate scale 1 : 40,000. Photographs by U.S. Navy]

Dense stand of coniferous trees, *A*, is typical of massive marble and related carbonate rocks in this area. Diorite, *B*, has only patchy tree growth but shows typical crisscross joint pattern of short lineations common in many intrusive rocks. Area *C* is schist. The surface expression of the schist is similar to that of the diorite in patchy tree cover and irregular topography but the schist has a dominant lineation direction not present in the intrusive rocks. Vegetation bands, *D*, may cover thin beds of marble. Note that gently curved vegetation bands suggest steeply dipping rock units.

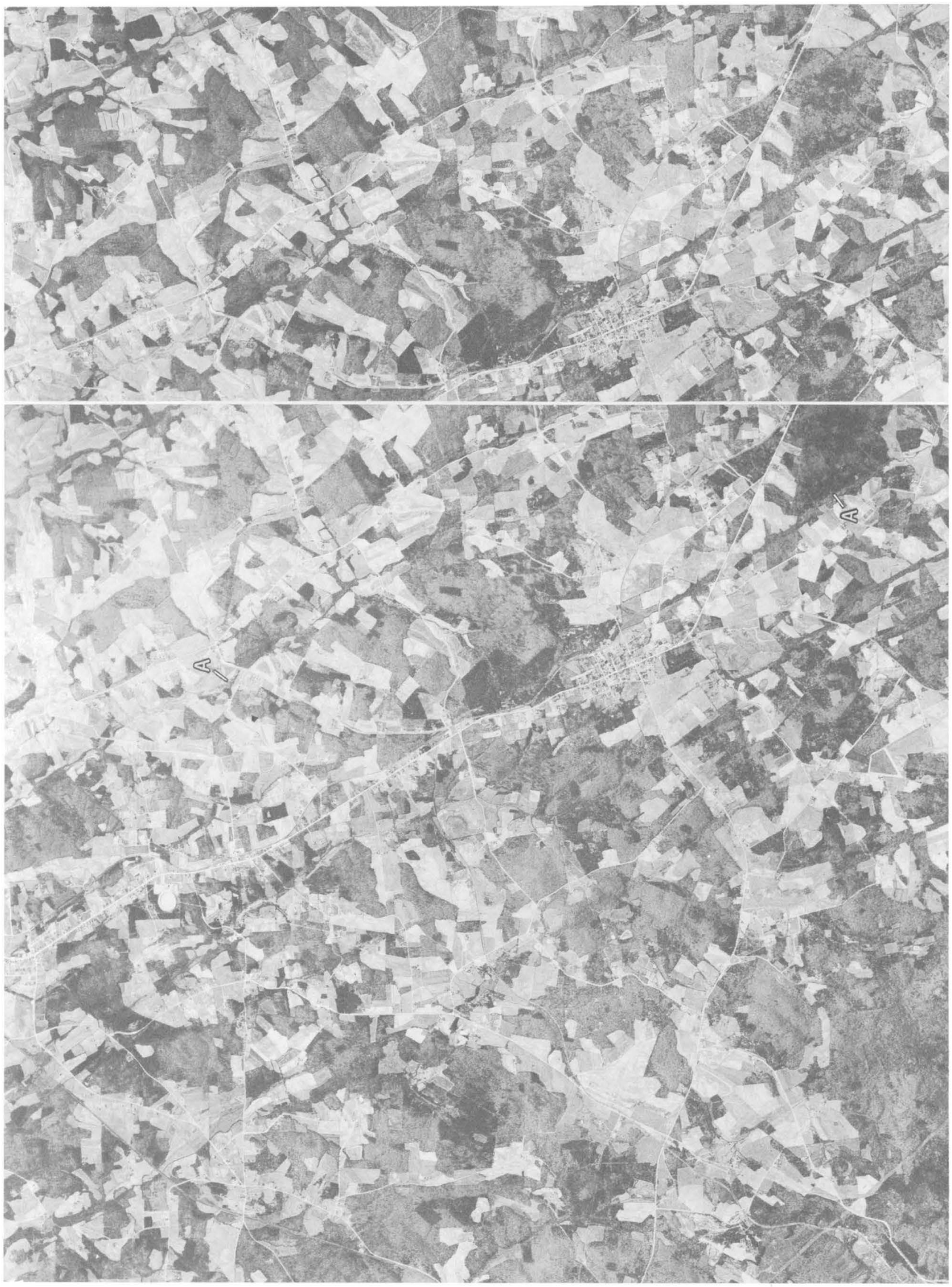
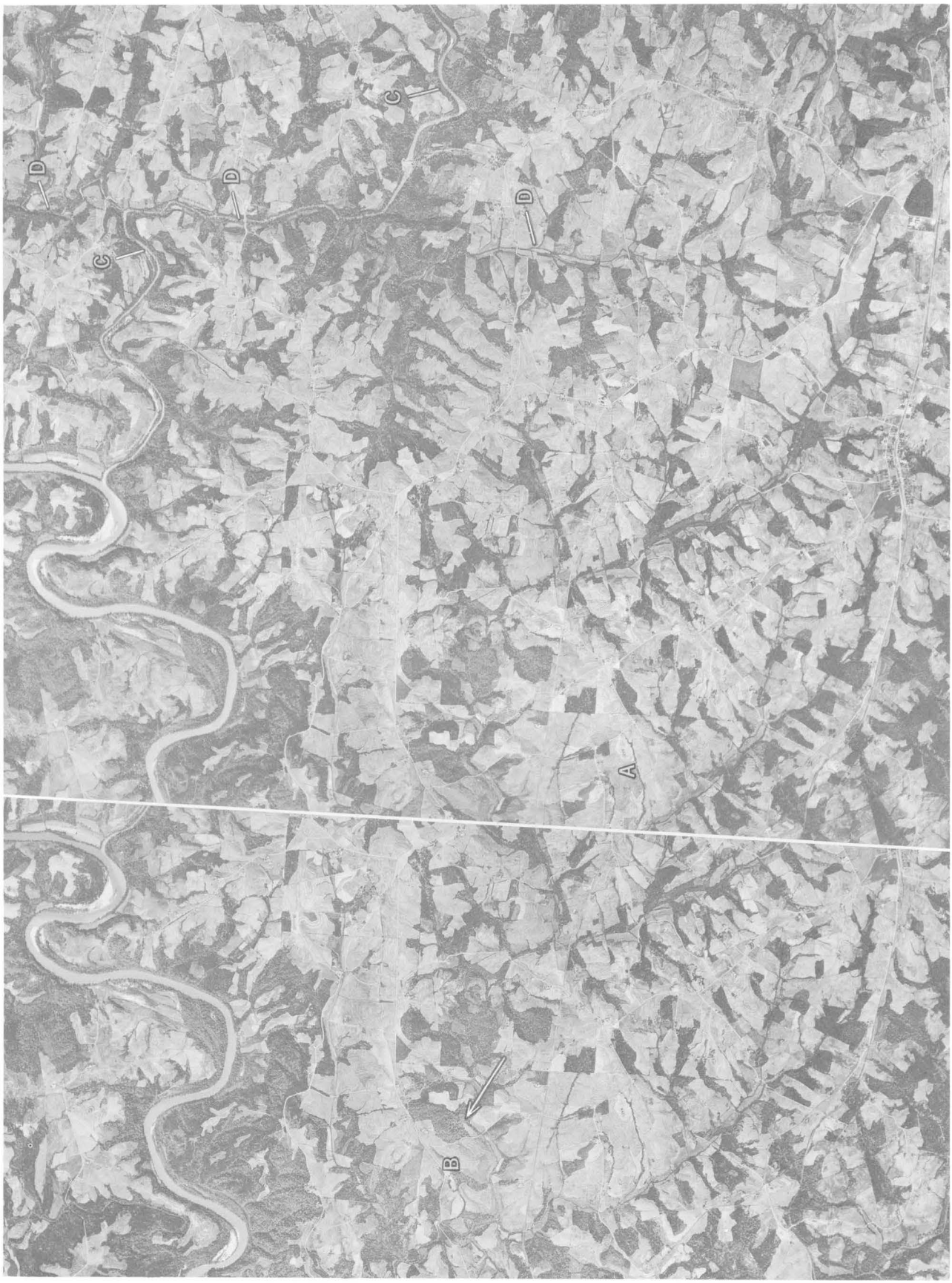

A
A
Stereoscopic pair
Approximately 1 mile

FIGURE 73.—AREA UNDERLAIN BY SILICIC VOLCANIC TUFFS AND FLOWS AND BEDDED ARGILLITE OR SLATE (NORTH CAROLINA).

[Approximate scale 1 : 58,000. Photographs by Army Map Service]

Major streams, *A*, are developed along the regional cross-joint direction. Roads extending generally parallel to the major streams accentuate the cross-joint direction. Minor tributary streams flow predominantly parallel to the regional structural trend and at right angles to the cross joints. Hills are commonly elongate in the direction of the regional strike, which may represent foliation or flow cleavage rather than bedding. In such low-relief areas the extensive land-use pattern tends to obscure structural trends; commonly the structural trends can be better observed from a mosaic composed of several photographs. Any one stereoscopic pair can only show a small part of the regional geologic structure. Structural interpretation may also be facilitated by study of separate drainage maps, as in figure 8.



Stereoscopic pair

Approximately 1 mile

553966 O-60—7

FIGURE 74.—AREA OF FOLDED, FAULTED, AND HIGHLY METAMORPHOSED ROCKS (NORTH CAROLINA).

[Approximate scale 1 : 57,000. Photographs by Army Map Service]

This pair of photographs illustrates a use of drainage characteristics in the interpretation of geologic structure. Where dips are gentle, tributary streams developed on the updip side of a strike valley commonly will be longer than tributary streams developed on the downdip side of the valley, as at *A*. The direction of dip of strata is thus indicated. Length relations of streams are commonly best studied on a separate drainage overlay (see fig. 7) where vegetation and other obscuring features in the stereoscopic model are not present. In the area shown, a plunging fold is also suggested by the distribution of photographic tones and gentle curvature of streams around the nose, *B*, of the fold. Arrow indicates direction of plunge. Many streams in highly metamorphosed terrain have developed in response to, and therefore reflect, the strike and dip of foliation rather than bedding. Prominent cross joints are expressed by linear segments of major streams, as at *C*, and by alinement of vegetation along some tributary streams. Note conspicuous fault indicated by alinement of stream segments, *D*; this fault is inconspicuous on the ground.

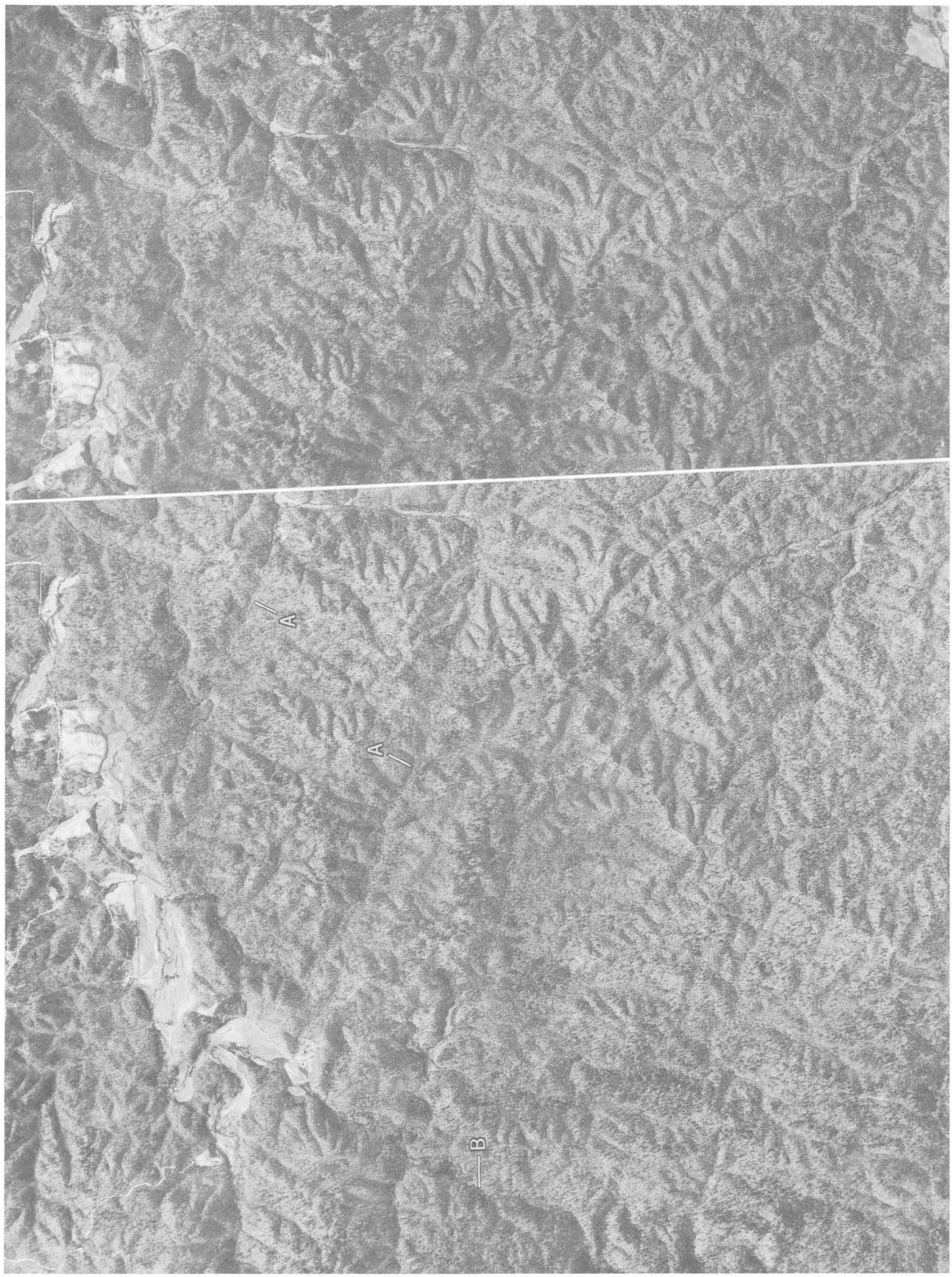
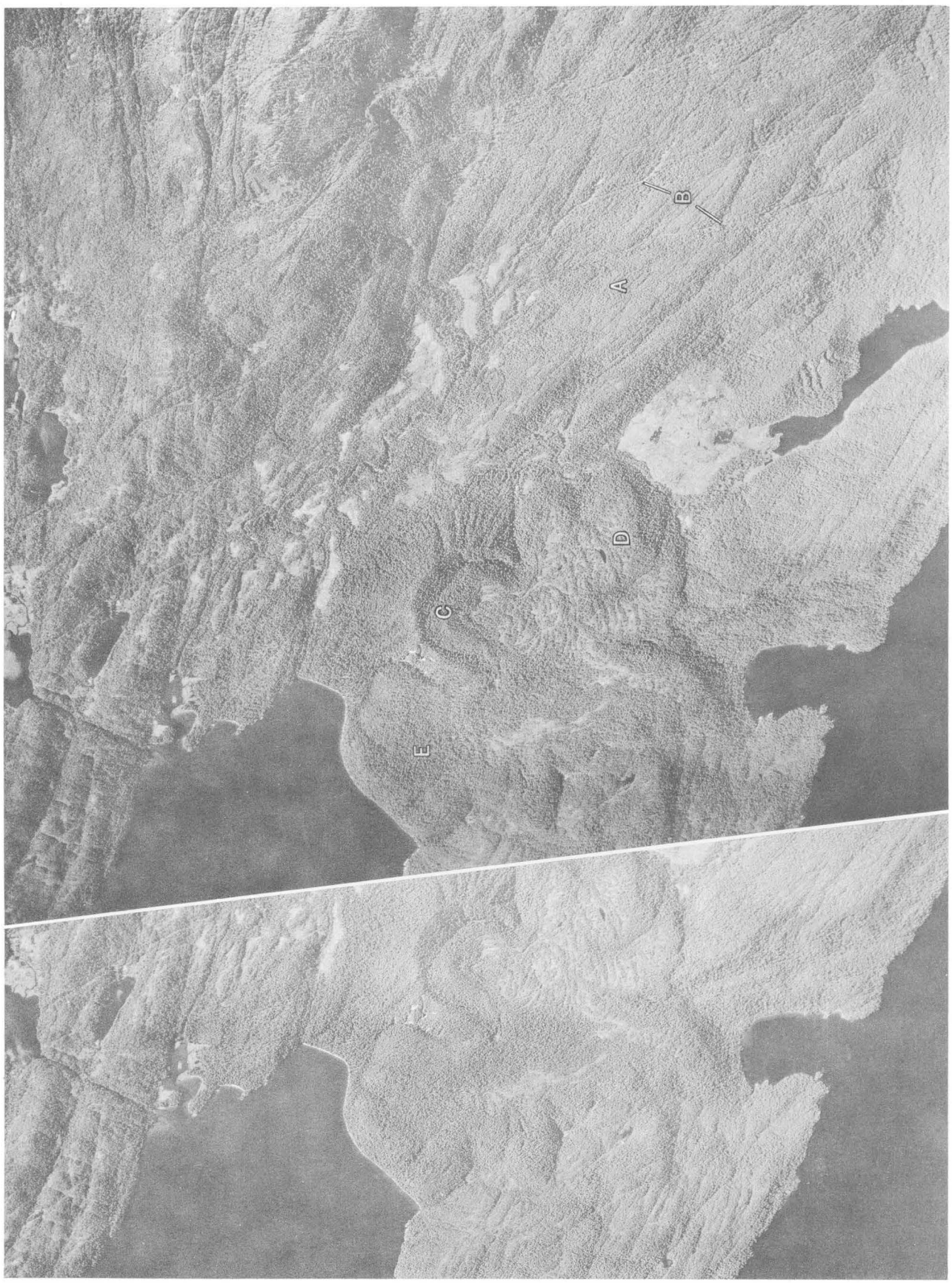

A
A
B
Stereoscopic pair
Approximately 1 mile

FIGURE 75.—AREA UNDERLAIN BY PHYLLITE AND SLIGHTLY METAMORPHOSED SLATY ROCKS (ALABAMA).

[Approximate scale 1 : 29,000. Photographs by U.S. Geological Survey]

Poorly resistant phyllite and slightly metamorphosed slaty rocks here are characterized by fine-textured drainage, commonly found in fine-grained clastic rocks. The area also has a fine-textured erosional topography. Several conspicuous linear trends, *A*, are at right angles to the regional strike of bedding. These trends probably represent regional cross joints. In areas of metamorphic rocks the prominent regional cross joints commonly are widely spaced and streams flow along them. The linear trend of the stream at *B* is parallel to the regional strike of bedding. There is no direct surface manifestation of bedding. Headwater tributaries form a generally dendritic drainage pattern that suggests uniformity of rock type, but principal streams show rectangular drainage probably influenced by bedding and cross joints.



Stereoscopic pair

Approximately 1 mile

FIGURE 76.—HEAVILY VEGETATED TERRAIN UNDERLAIN BY METAMORPHIC AND EXTRUSIVE VOLCANIC ROCKS (SOUTHEASTERN ALASKA).

[Approximate scale 1 : 40,000. Photographs by U.S. Geological Survey]

Numerous subparallel lineations, *A*, represented primarily by rectilinear depressions that channel the drainage, are expressions of foliation in the metamorphic rocks. Conspicuous rectilinear depressions, *B*, transecting the foliation direction, represent faults. The remnant of a recent volcanic cone, *C*, is recognized by its shape. Note lobate patterns of vegetation, *D*, suggesting areas of flow rocks. Absence of lineations in area *E* suggests that flows also are present there.

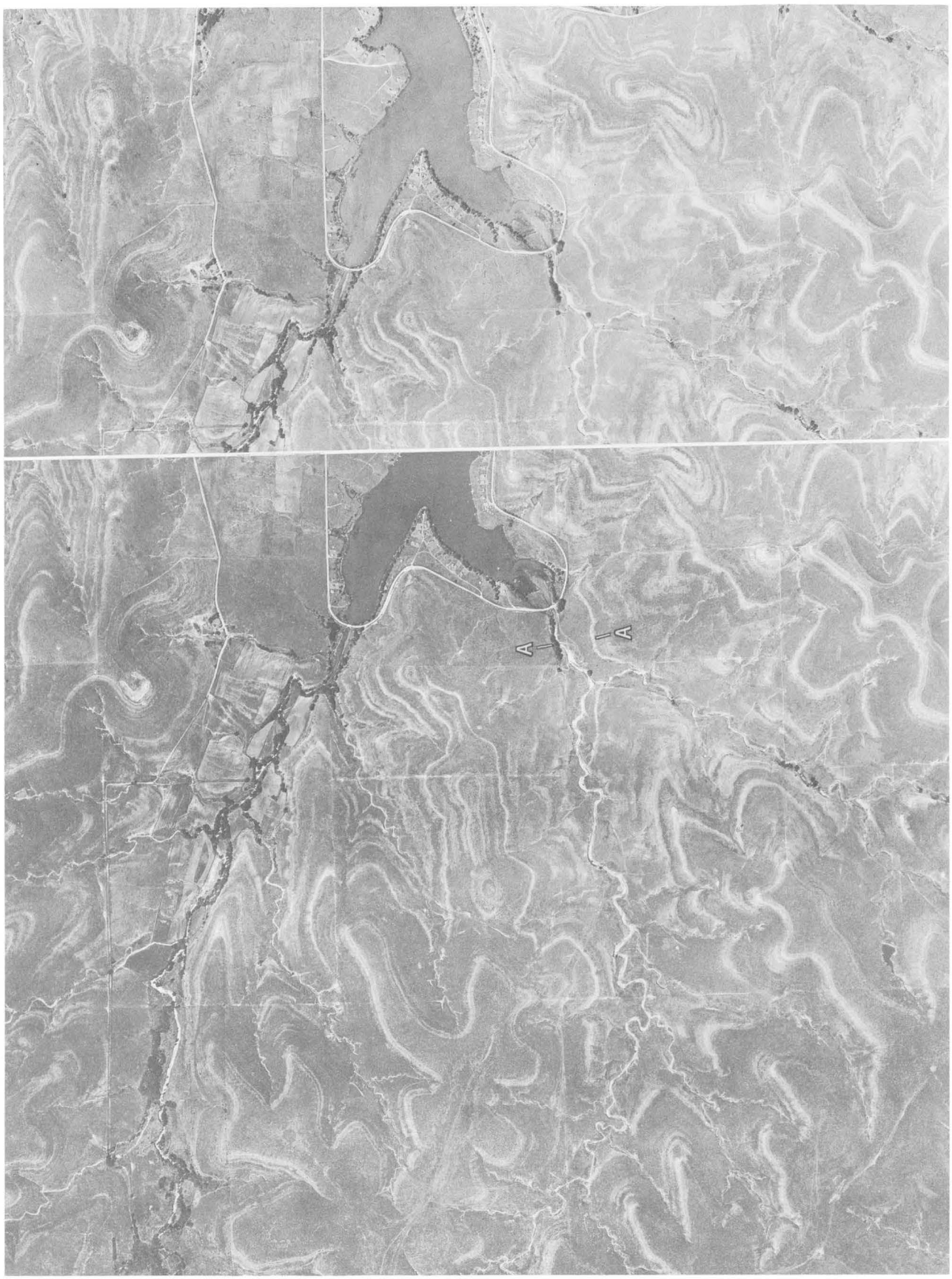

A
A
Stereoscopic pair
Approximately 1 mile

FIGURE 77.—FLAT-LYING BEDS OF LIMESTONE AND SHALE (KANSAS).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Strong contrasts in photographic tone result primarily from different lithologic characteristics of underlying formations; dark-toned beds are shale with some grassy vegetation; light-toned beds are limestone. The near-coincidence of bedding traces and topographic contours, closed loops of tonal patterns, as well as the dendritic drainage pattern are typical of flat-lying beds. Small thickness of limestone interbeds is not conducive to development of sink holes. In some places individual limestone beds can be distinguished on the basis of weathering and erosional characteristics; massive cherty limestone benches may show rounded rims, whereas thin platy limestone benches may show a sharp break at the rim. Abundant trees and shrubs along part of bed *A* suggest a plentiful supply of water. Bed *A* is locally an aquifer.

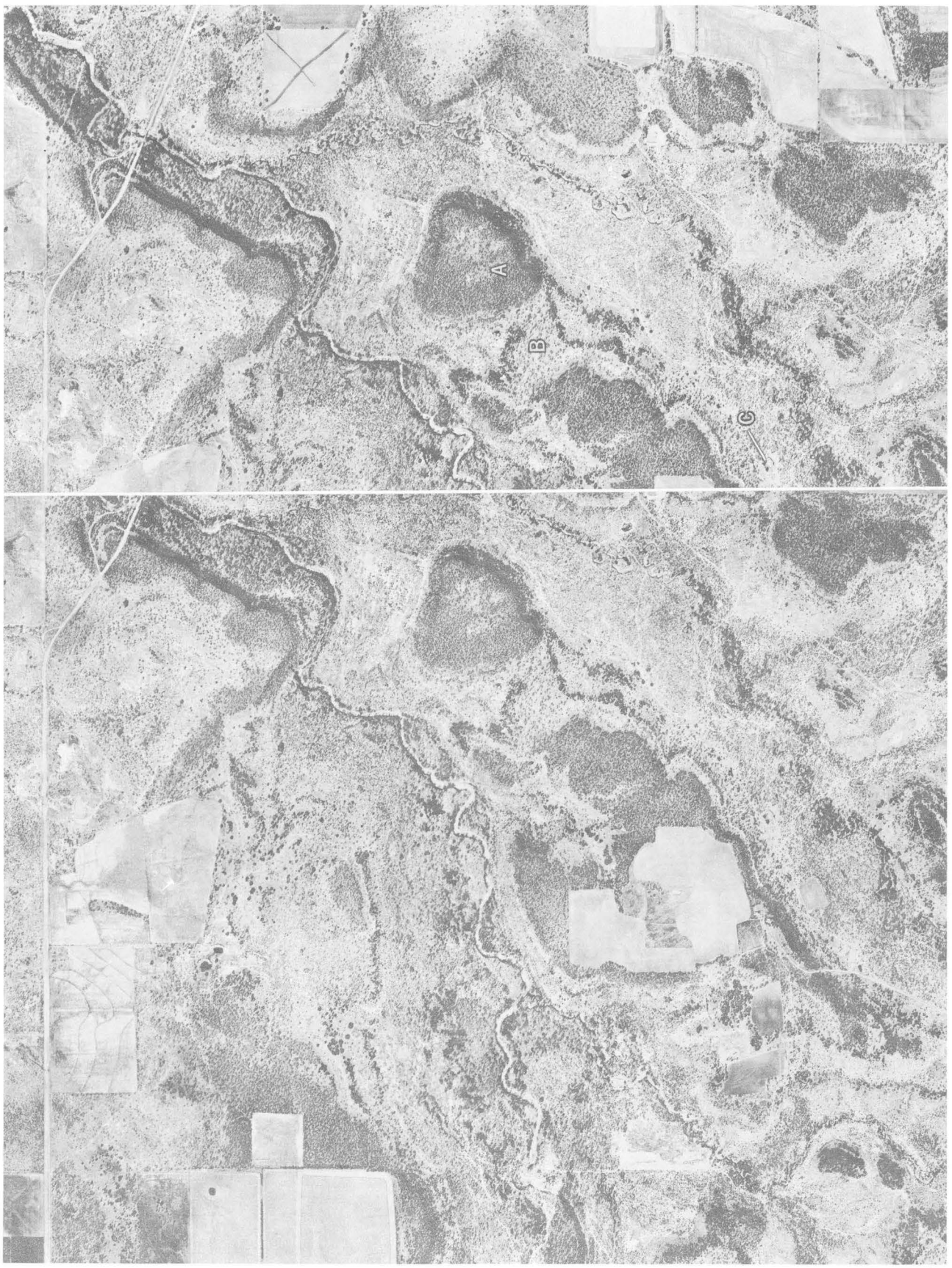

A
B
C
Stereoscopic pair
Approximately 1 mile

FIGURE 78.—FLAT-LYING BEDS OF SANDSTONE, LIMESTONE, AND SHALE (TEXAS).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Flat-lying beds are indicated by benchlike landform, extension of tonal bands along topographic contour, and by dendritic drainage. Dark photographic tone on sandstone caprock, *A*, results from growth of oak trees. Benches of limestone, *B*, exhibit concentration of oak growth along rims but not across flats. Valley areas are underlain by shale, which is covered predominantly by mesquite growth. Stock tanks, *C*, are common in impermeable material and where present suggest shale in this region.

A
A
Stereoscopic pair
Approximately 1 mile

FIGURE 79.—AREA OF SPARSE OUTCROPS UNDERLAIN LARGELY BY GENTLY FOLDED SANDSTONE, CONGLOMERATE, AND SHALE (NORTHERN ALASKA).

[Approximate scale 1 : 20,000. Photographs by U.S. Navy]

Dip slopes are characterized by few streams in contrast to back slopes on which a system of numerous subparallel streams has developed. Drainage in the dip-slope direction is generally coarse textured except for profuse channels developed at heads of tributaries. Drainage on the back slopes is fine textured. The textural difference, or drainage density difference, rather than any specific drainage pattern, stands out. The back slope, with its fine-textured drainage, is predominantly a shale section in contrast to the sandstone and conglomerate of the dip slope. Note horizontal offset of light-toned sandstone beds by near-vertical faults, illustrated at *A*, transverse to the strike.

Stereoscopic triplet

Approximately 1 mile

FIGURE 80.—GENTLY TO STEEPLY DIPPING SEDIMENTARY ROCKS OVERLYING SCHIST-GNEISS-GRANITE COMPLEX (WYOMING).

[Approximate scale 1 : 59,000. Photographs by Army Map Service]

Striking discordance in dip of beds can be seen between beds at *A* and *B* and between near-vertical beds at *C* and flat-lying beds at *D*. Such a discordance in dip may represent tightly folded structures in some areas but here it represents faulting. Note also the conspicuous discordance in strike between beds at *A* and *C* and between beds at *B* and *C*. The locations of fault traces may be inferred from the positions of discordant beds, but details of fault structure and positions of formation contacts cannot be seen clearly on the photographs of many parts of this complex area. Dark-toned rocks, *E*, lacking bedding or banding are schist-gneiss-granite complex. Light-toned jointed rocks, *F*, are predominantly limestone and dolomite. Where light-toned rocks are cut by a stream, as at *G*, the outcrop pattern forms a V in the direction of dip.

Stereoscopic pair

Approximately 1 mile

FIGURE 81.—GENTLY FOLDED SEDIMENTARY ROCKS (CENTRAL UTAH).

[Approximate scale 1 : 20,000. Photographs by Soil Conservation Service]

Contrasting photographic tones, representing different soil and rock types, strongly outline plunging anticline. Plunge of anticline is also indicated by stream curvature at *A* and *B*. Note that major stream has generally consistent direction of flow until it reaches anticlinal nose at *C*, at which point it is deflected in the direction of plunge of the structure. Outcrop pattern of contact between light- and dark-toned rocks, *D*, along flank of the anticline forms pronounced V's, which point in the direction of dip. Local intrusions of basalt dikes, *E*, stand in topographic relief above softer surrounding rocks.

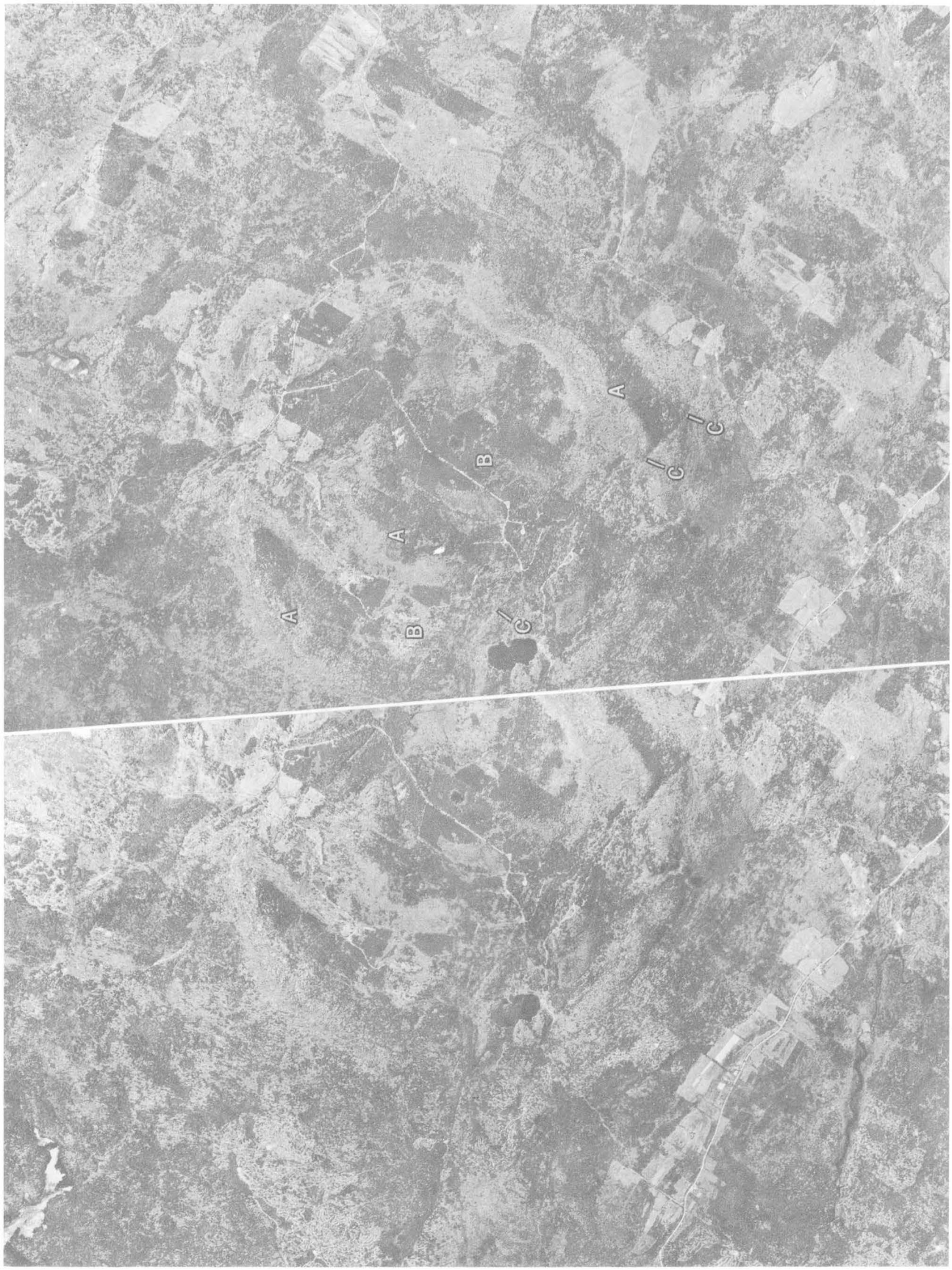

A
A
B
C
A
B
C
C
Stereoscopic pair
Approximately 1 mile

FIGURE 82.—RING DIKE IN NEW HAMPSHIRE.

[Approximate scale 1 : 34,000. Photographs by U.S. Geological Survey]

The ring dike, composed of several types of igneous rock, is the most conspicuous feature of the terrain. Different rock types in places are reflected in the topographic expression of terrain. An outer ring and partial inner ring, *A*, composed of monzonite stand in conspicuous topographic relief. Hornblende diorite, in places foliated, forms the low areas, *B*. Some geologic contacts may be located on the basis of topography. However, specific placement of contacts cannot be made from the stereoscopic model; but in igneous terrain, where one rock type may grade into another, contacts are difficult to select in the field. The ring dike is cut by several faults, *C*, indicated by alinements of scarps, depressions, and vegetation.

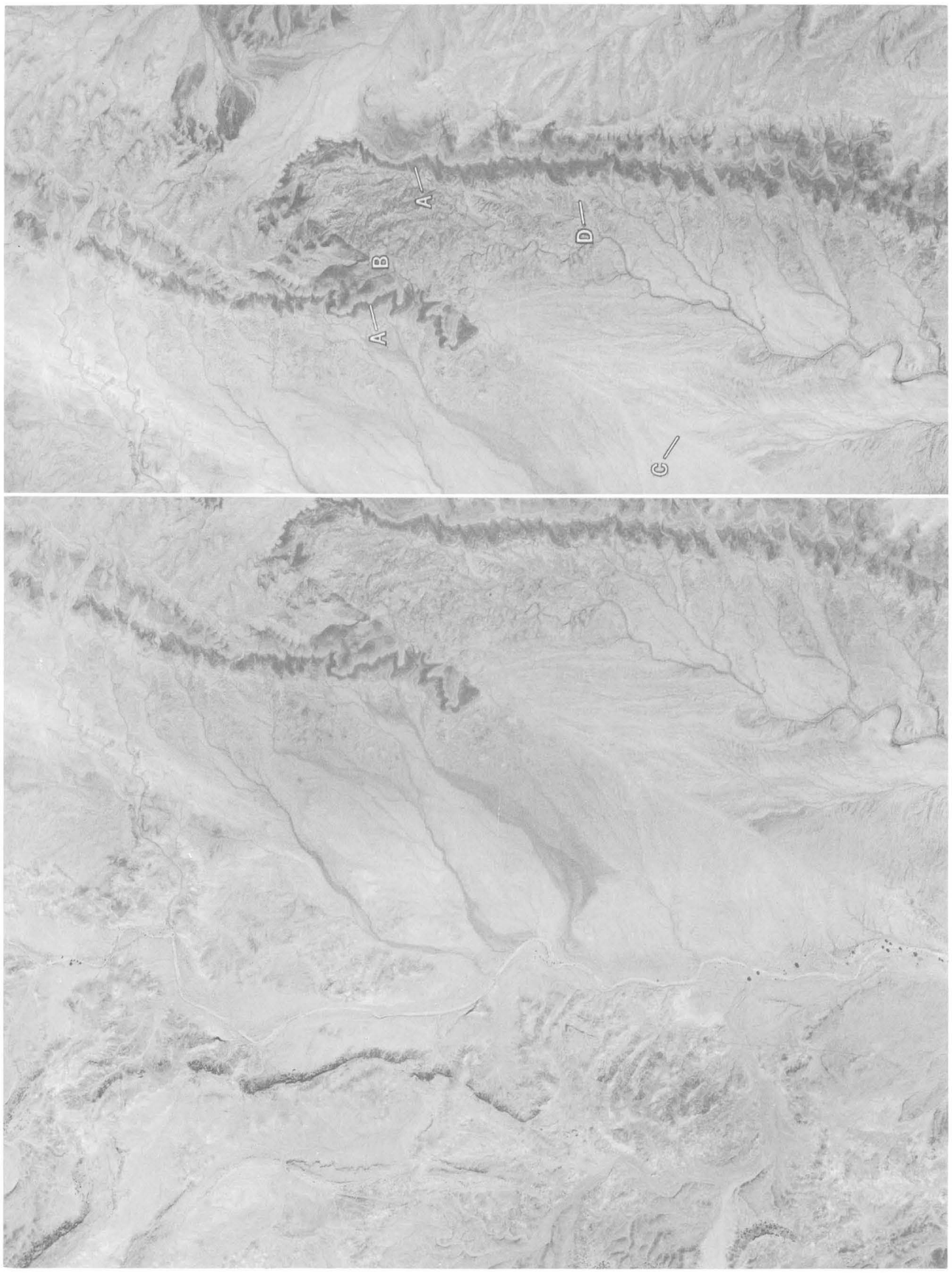
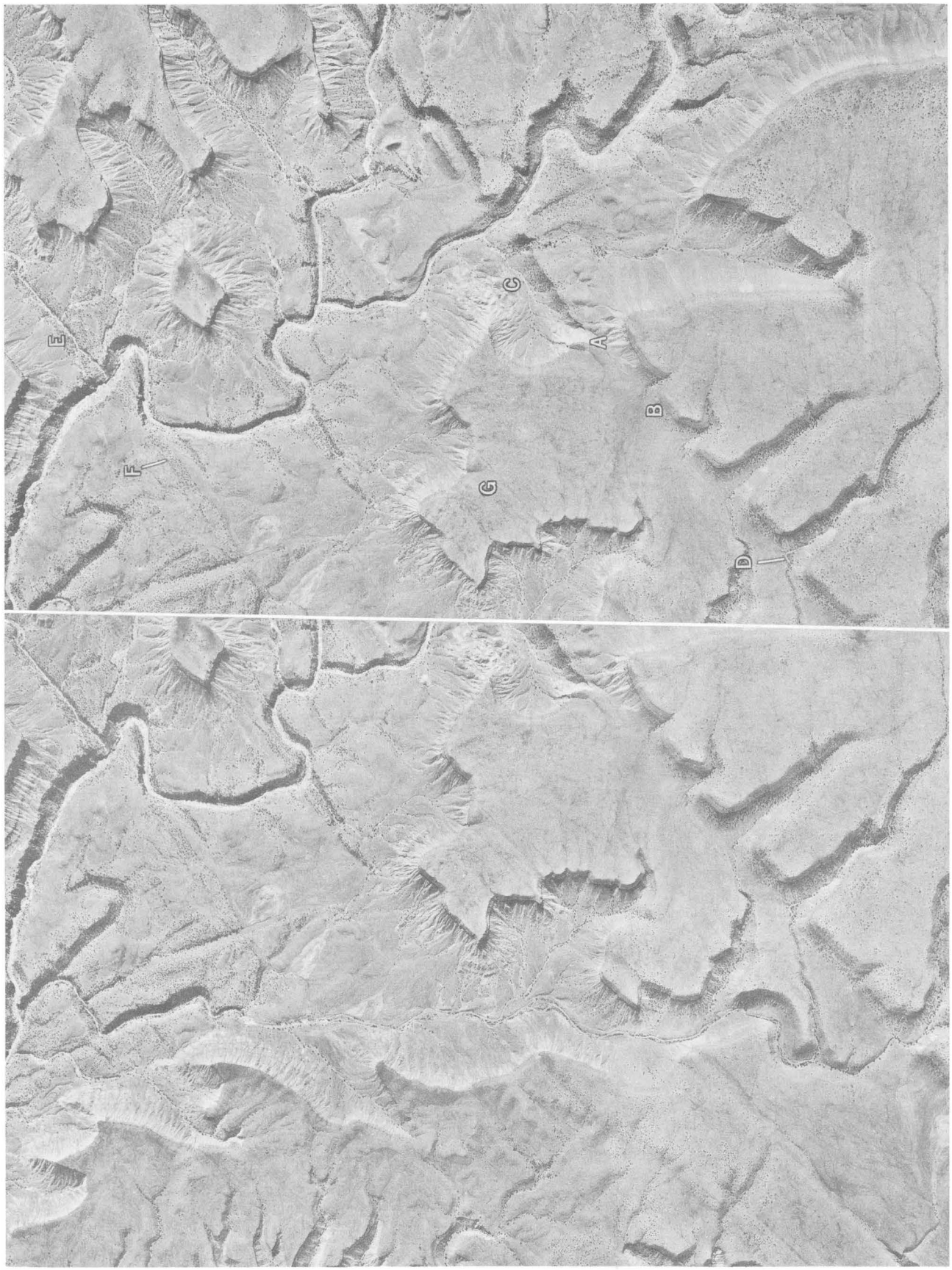

A
A
B
D
C
Stereoscopic pair
Approximately 1 mile

FIGURE 83.—GENTLY DIPPING SEDIMENTARY ROCKS OFFSET BY NEAR-VERTICAL FAULT (UTAH).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

Line separating areas of contrasting photographic tones is trace of fault. The straightness of the fault trace indicates that the fault has approximately a vertical dip. Note vertical offset of dark-toned shale bed, *A*, and difference in erosional character of topography on opposite sides of fault at *B*. Faint trace of fault in alluvium at *C* is locally marked by differences in drainage on opposite sides of the fault. Light-toned sandstone interbeds, *D*, cap local areas and exhibit serrated margins as a result of closely spaced joints. Fine-textured drainage is typical of the poorly resistant shale and thin sandstone interbeds.



Stereoscopic pair

Approximately 1 mile

FIGURE 84.—FAULTED, GENTLY DIPPING SEDIMENTARY ROCKS (UTAH).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

Conspicuous high-angle faults offset beds in many places, as at *A*, where limestone caprock is down-faulted about 125 feet. Note the effect of vertical exaggeration in the stereoscopic model on the amount of offset. Fault is indicated by scarp, *B*, and its alinement with stream at *C*. Note right-angle bend in stream at *D* along trace of fault. Another fault is indicated by alinement of stream *E* and break in vegetation *F*. Several other faults with only small displacements are shown by alinements at *G*. Resistant limestone caprock stands in vertical bluffs overlying less resistant shale and shaly siltstone that have a lesser angle of slope.

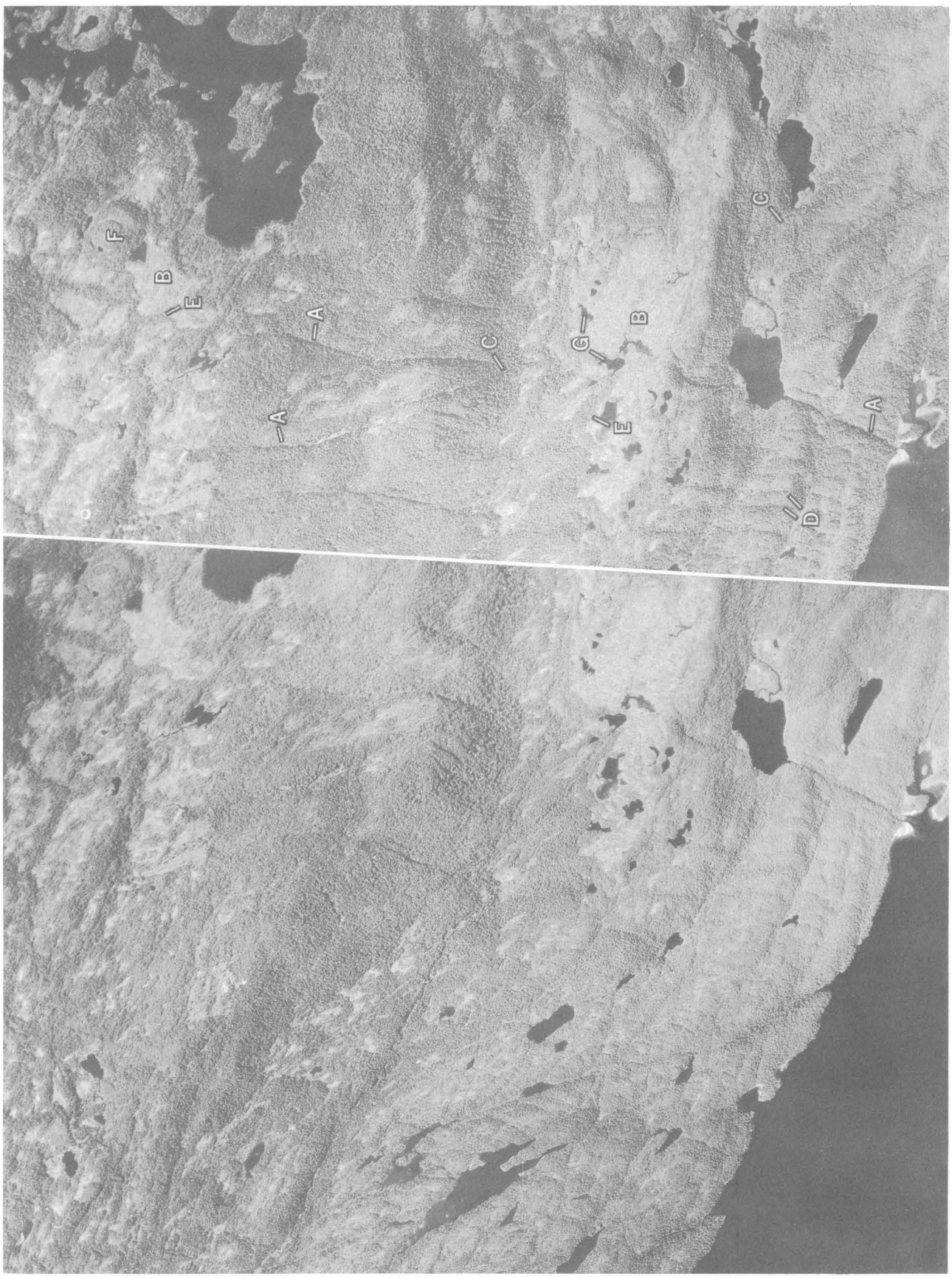
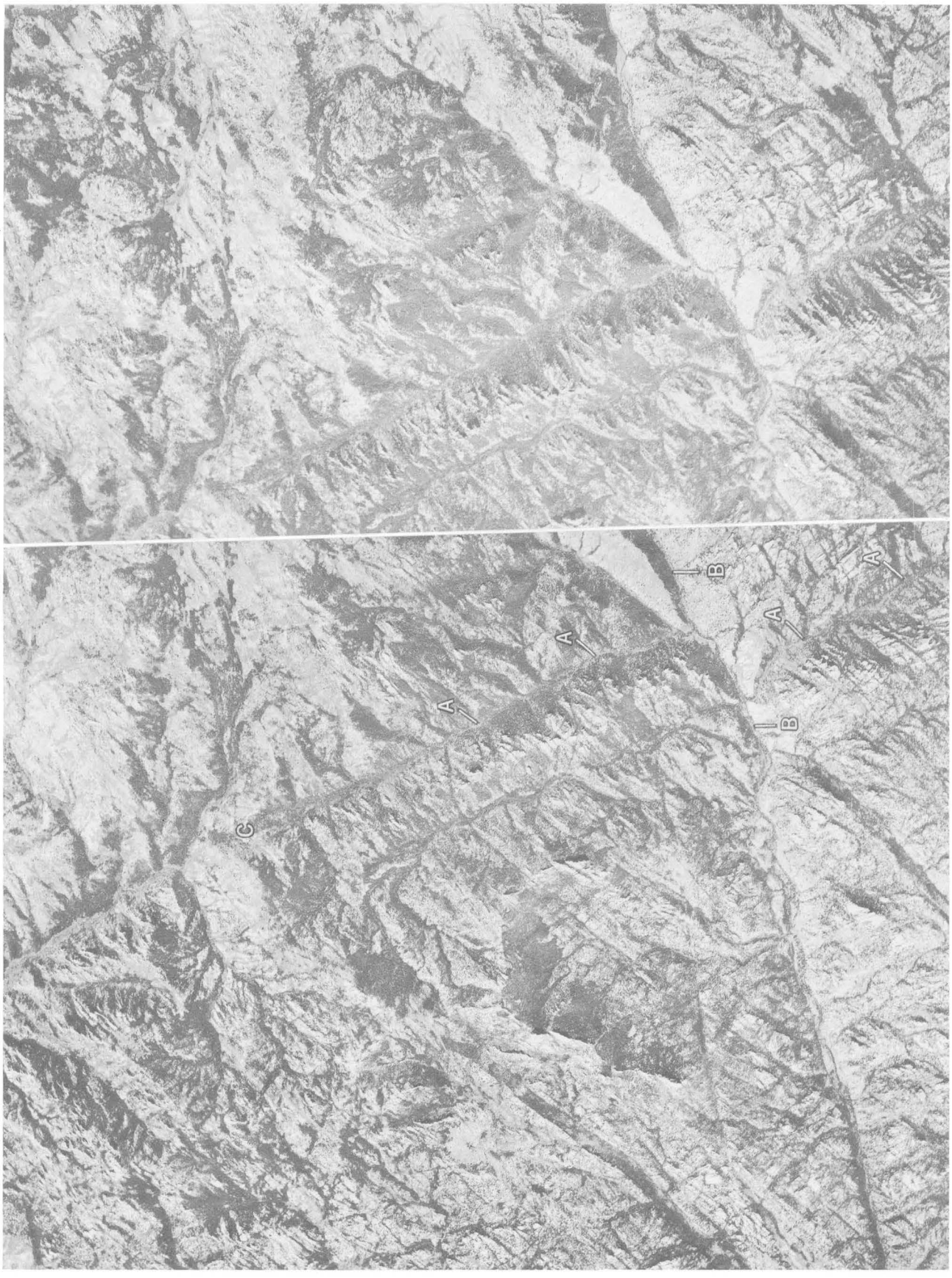

F
B
E
A
A
C
G
E
B
C
A
D
Stereoscopic pair
Approximately 1 mile

FIGURE 85.—VEGETATED TERRAIN UNDERLAIN BY IGNEOUS AND METAMORPHIC ROCKS LOCALLY COVERED BY BASALT FLOWS (SOUTHEASTERN ALASKA).

[Approximate scale 1 : 40,000. Photographs by U.S. Navy]

A significant contrast between the igneous and metamorphic complex and younger volcanic flows is shown in the distribution of faults and vegetation. Faults, indicated primarily by rectilinear depressions, *A*, are common in the igneous and metamorphic rocks, but are absent from the area of lava flows, *B*. Note that certain faults, as at *C*, may be traced up to the lava flows and that continuations of these faults may be picked up on the opposite side of the flow area. Some of the shorter lineations, as at *D*, probably represent wide-spaced joints. Lobate patterns of dark-toned vegetation, *E*, commonly delineate the edges of individual lava flows. Small cone at *F* is suggested by shape of constructional landform. Relatively flat, muskeg-covered flows are generally poorly drained and locally contain numerous shallow ponds, *G*, that lack any integrated drainage. The muskeg areas have a relatively light photographic tone because of the mossy vegetation and do not appear dark despite the abundance of moisture. The photographic texture of the muskeg areas is also distinctive.



Stereoscopic pair

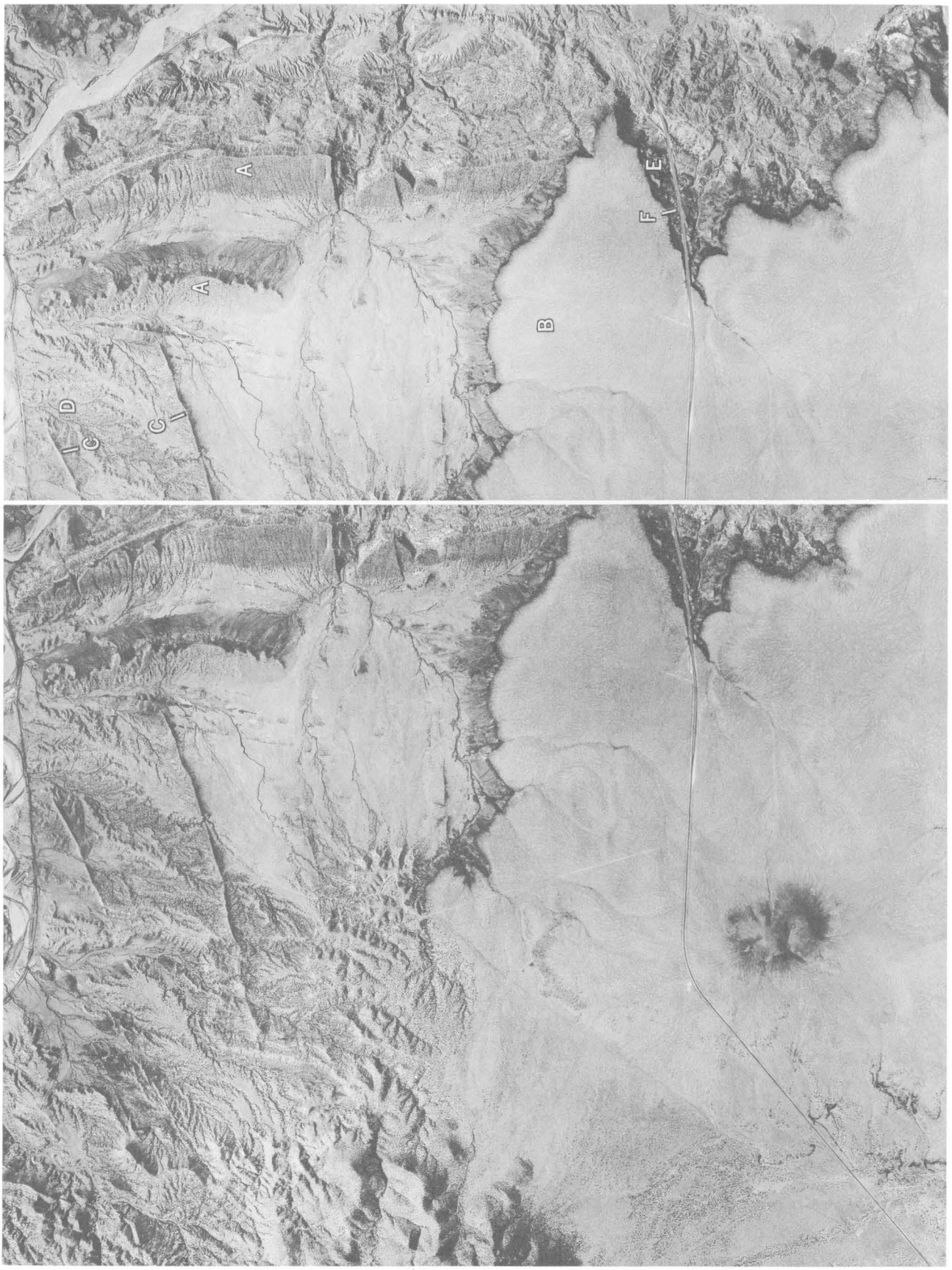
Approximately 1 mile

553966 O-60—8

FIGURE 86.—AREA OF CRYSTALLINE ROCKS (WYOMING).

[Approximate scale 1 : 60,000. Photographs by Army Map Service]

Numerous widely spaced joints, typical of many intrusive masses, are conspicuous, although widely varying orientations of joints, found in most plutonic rocks, are not prominent. Drainage is markedly controlled by faults and joints; the dendritic drainage that is normally characteristic of crystalline masses is thus subdued. Although the rocks shown here are locally gneissic, evidence of bedding of original sediments or gneissic structure is generally lacking. Major fault, *A*, marked by stream alinement, is offset by younger fault, *B*, also delineated by stream alinement. Note alinement of streams on opposite side of divide, *C*.



Stereoscopic pair

Approximately 1 mile

FIGURE 87.—LAVA FLOW LYING UNCONFORMABLY ON GENTLY DIPPING SEDIMENTARY ROCKS (NEW MEXICO).

[Approximate scale 1 : 54,000. Photographs by Army Map Service]

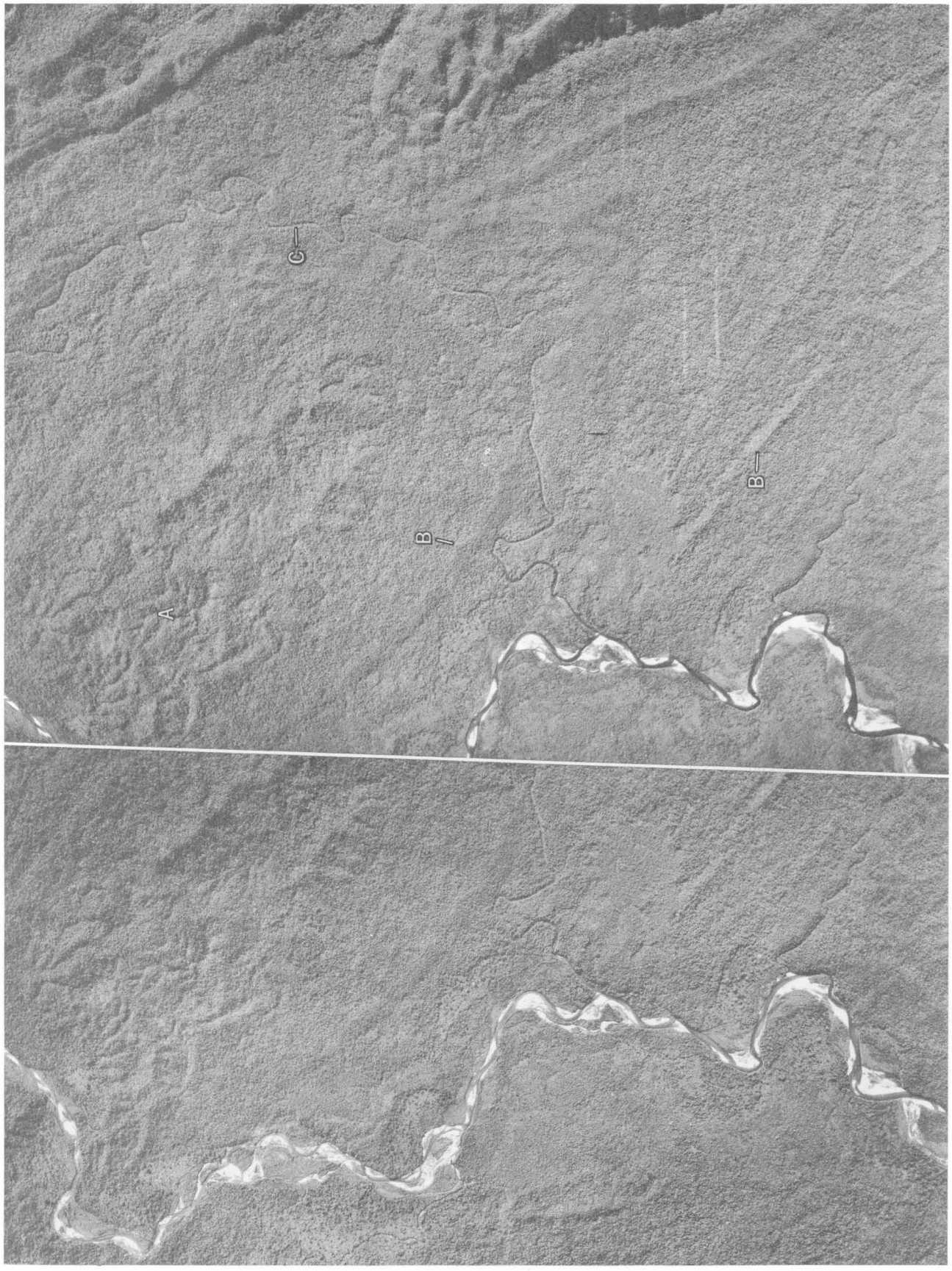
Resistant sandstone beds, *A*, dipping 15° are truncated by overlying lava flow, *B*. Bedding stands out where topographic and bedding surfaces coincide. Hogback landform is also prominent where resistant sandstone beds and intervening shale areas have been etched by erosion. Note how vertical exaggeration of dip causes unconformable relation between sedimentary beds and overlying lava flow to stand out. Surface of lava flow has mottled appearance that is typical of basalt flows in many areas. Basaltic dikes, *C*, stand in topographic relief above soft shale shown by fine-textured drainage at *D*. Some landsliding has taken place at *E* where resistant lava overlies less resistant rocks. Road alinement *F* is subject to potential destructive action of additional slides.

A
B
C
D
E
Stereoscopic pair
Approximately 1 mile

FIGURE 88.—GENTLY DIPPING SEDIMENTARY ROCKS OVERLAIN IN PART BY RIVER GRAVELS (UTAH).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Flat-lying gravel cap, *A*, truncates underlying sedimentary rocks. Traces of bedding below granular material of gravel cap are indicated by minor breaks in slope, *B*, accentuated by shadows. Surface drainage is conspicuously absent from well-drained broad gravel flat, *D*, which represents a younger, lower and less dissected terrace than *A*. Gullies in silty valley-fill, *E*, exhibit near-vertical slopes where recent stream dissection has taken place. Note effect of vertical exaggeration in the stereoscopic model. True dip of beds at *C* is about 6°.



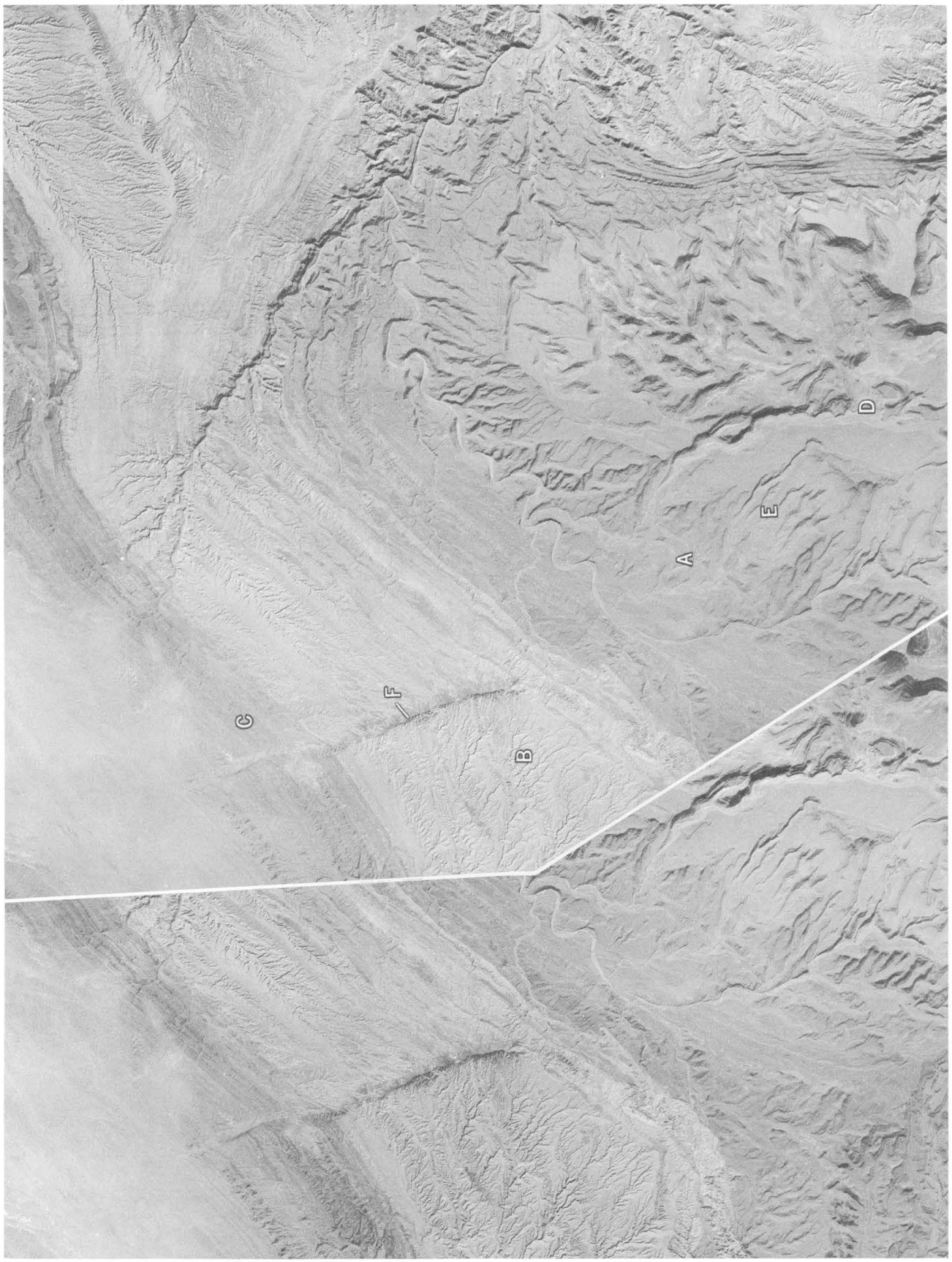
Stereoscopic pair

Approximately 1 mile

FIGURE 89.—GENTLY FOLDED SEDIMENTARY ROCKS IN HEAVILY VEGETATED AREA (NORTHERN GUATEMALA).

[Approximate scale 1 : 65,000. Photographs by Army Map Service; published with permission of the Guatemala Government]

Anticlinal structural feature in heavily vegetated jungle area is indicated by erosional characteristics of terrain and by drainage. Core of anticline, *A*, is topographically higher than surrounding area and is somewhat more dissected. Bedding and direction of dip are suggested by the topographically high bands of ground at *B*; note that tree crowns appear to fall in a dipping plane. Stream, *C*, has been deflected around the nose of the anticline; the convex side of the curve indicates the direction of plunge, but the major stream of the area has maintained its course across the anticline.



Stereoscopic pair

Approximately 1 mile

FIGURE 90.—PLUNGING ANTICLINE IN GENTLY FOLDED ROCKS (SOUTHERN UTAH).

[Approximate scale 1 : 37,000. Photographs by U.S. Geological Survey]

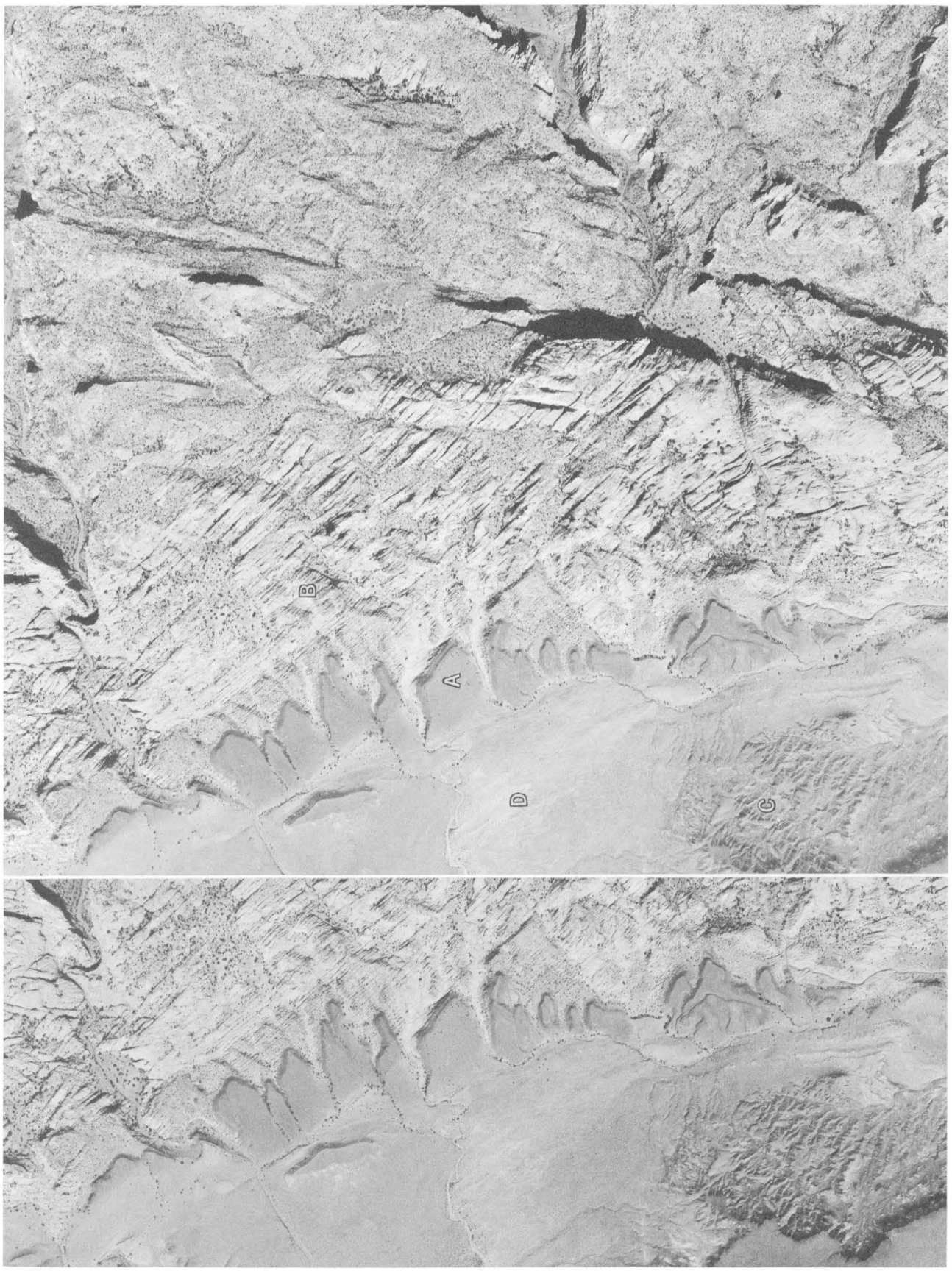
Distribution of rock types and characteristics of drainage clearly outline plunging anticline. Note that major stream curves around nose of the anticline and the convex side of the curve indicates the direction of plunge. Lithologic differences between formations are conspicuously shown by contrasts in photographic tone and erosional characteristics of terrain. Dark-toned formation, *A*, is an interbedded sequence predominantly of red sandstone and some mudstone and shale. Light-toned formation, *B*, is made up of a rather uniform weakly cemented massively bedded sandstone showing a fine-textured dendritic drainage. Drainage rills in formation *A* and *C* are controlled in part by hard, resistant sandstone interbeds that locally channel the drainage along the interbeds. Formation *C* largely comprises a series of red to brown silty sandstone and shale. Rocks at *D* include predominantly thin-bedded red sandstone and limestone interbeds. Bedding is prominently shown because topographic surfaces and bedding surfaces coincide in many places. Dip of sedimentary beds is exaggerated as in most stereoscopic models. True dip at *E* is 5°. Dark-toned resistant basalt dike, *F*, stands in relief above light-toned rocks.

A
D
D
E
B
E
F
F
C
Stereoscopic pair
Approximately 1 mile

FIGURE 91.—STRATIGRAPHIC SECTION ACROSS GENTLY FOLDED ANTICLINE (UTAH).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

Breaching of anticline by major river has exposed cross section of the fold. Bedding is clearly represented at *A* where bedding surfaces coincide with topographic surfaces. Effect of vertical exaggeration on dip is shown on both flanks of the anticline. True dip at *A* is about 20°; at *B* the beds are horizontal; at *C* the dip is about 4°. Shale, siltstone, and fine-grained sandstone, *D*, exhibit dark photographic tones; relatively closely spaced joints may be seen locally. Coarse sandstone with some conglomerate, *E*, has light photographic tone; widely spaced joints are present as at *F*. The coarse-grained rocks characteristically form cliffs. Where beds are nearly horizontal the fine-grained rocks have slopes that are less steep than those of the coarse-grained rocks. Where beds are dipping, the softer rocks are in many places etched out by erosion leaving hogbacks of resistant rock types.



Stereoscopic pair

Approximately 1 mile

FIGURE 92.—GENTLY DIPPING SEDIMENTARY ROCKS ON EAST SIDE OF SAN RAFAEL SWELL (UTAH).

[Approximate scale 1 : 20,000. Photographs by U.S. Geological Survey]

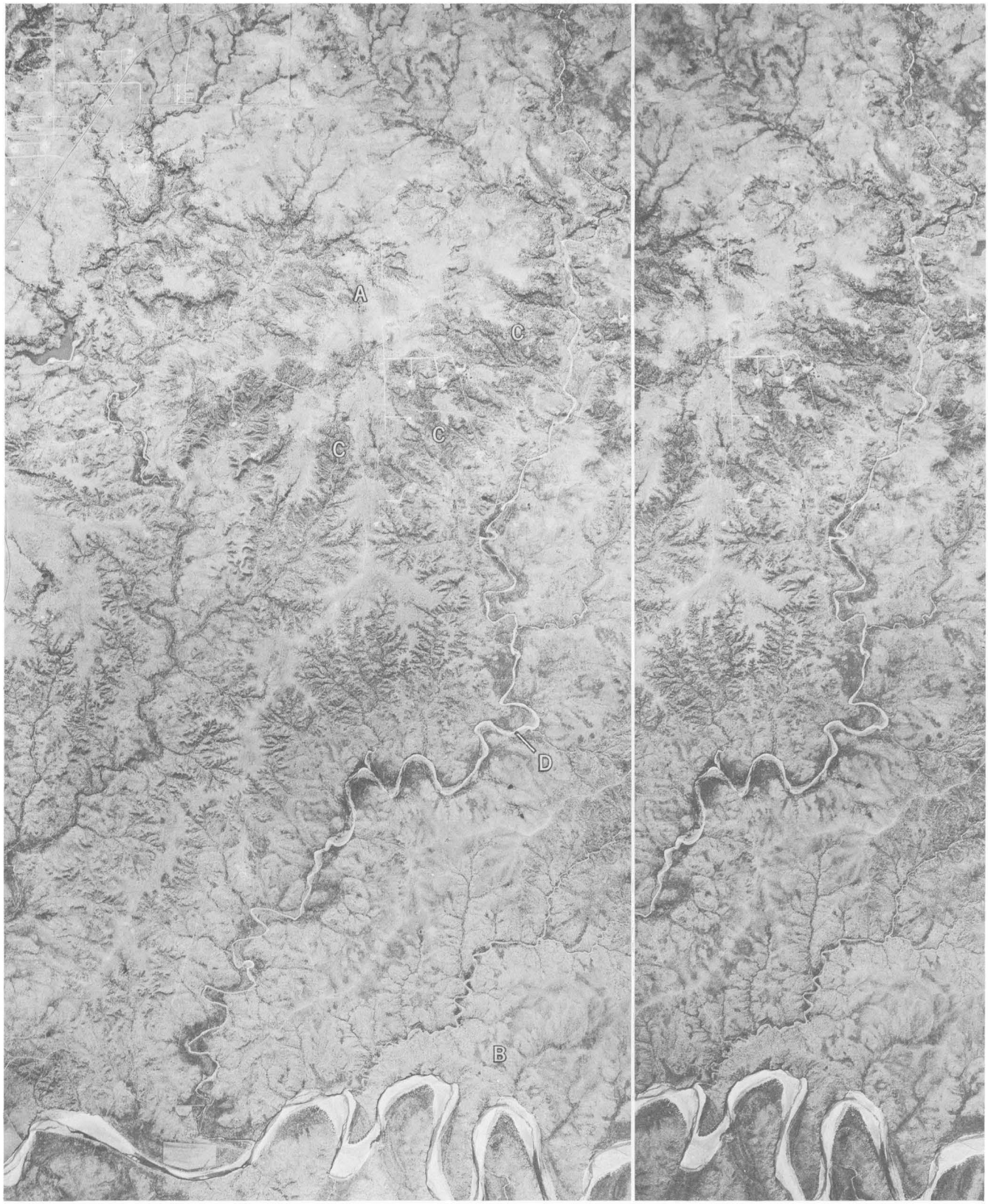
Bedding on flank of fold is clearly shown by photographic tone differences and hogback landform where dip surfaces and topographic surfaces coincide. Note effect of vertical exaggeration on dip in the stereoscopic model; beds at *A* have true dip of 6°. Massive crossbedded sandstone, *B*, has light photographic tone and widely spaced joints oriented predominantly in one direction; locally its appearance on aerial photographs is similar to some igneous rocks. Dark-toned resistant beds, *A*, are red mudstone and lenticularly bedded medium-grained sandstone. Poorly resistant interbedded red limy sandstone, mudstone, and limestone, *C*, is easily eroded and has fine-textured drainage. Beds at *C* are flat lying. Windblown sand, *D*, is marked by absence of surface drainage channels.

A
A
A
A
1 Mile

FIGURE 93.—UNCONTROLLED MOSAIC OF UMIAT ANTICLINE AREA, NORTHERN ALASKA, UNDERLAIN BY SHALE, SANDSTONE, CONGLOMERATE, AND GRAYWACKE.

[Photographs by U.S. Navy]

Curvature of streams, *A*, has developed on flank of anticline where hard and soft interbeds are exposed. Anticline has been breached into soft shale permitting streams developed on the more resistant dip slope to curve along soft interbeds and not across the axis of the fold. Contrast figure 81 where stream curvature indicates position of structural axis and direction of structural plunge.



Stereoscopic pair

Approximately 1 mile

FIGURE 94.—SUBSURFACE STRUCTURE REFLECTED IN SURFACE DRAINAGE CHARACTERISTICS (TEXAS).

[Approximate scale 1 : 63,360. Photographs by Army Map Service]

Subsurface structures at *A* and *B* are suggested by drainage characteristics of the area. Streams flanking the structure at *A* curve around the structure in their headwater portions. Tributary streams drain radially off the structure (see figures 9 and 95). In addition, the crudely circular pattern of more highly dissected ground and the pattern of dark photographic tone, *C*, which results from a concentration of vegetation, suggest subsurface structure. Compressed meanders are present over a subsurface structure at *B*. Also note stream deflection downstream from *D* which is a further suggestion of subsurface structure in area *B*.

Stereoscopic pair

Approximately 1 mile

FIGURE 95.—SAME PHOTOGRAPHS AS FIGURE 94, BUT REVERSED TO SHOW PSEUDOSCOPIC EFFECT AS AN AID TO INTERPRETATION.

[Approximate scale 1 : 63,360. Photographs by Army Map Service]

Reversal of the positions of two aerial photographs of a stereoscopic pair produces the well-known pseudoscopic effect, in which stream valleys appear as ridges and hills look like depressions. This unnatural view of the terrain commonly accentuates stream characteristics, which may be significant indicators of subsurface structure, as at *A*. The pseudoscopic view also commonly facilitates plotting of drainage.

KUGRUA RIVER
KUNGOK RIVER
N
2 Miles

FIGURE 96.—UNCONTROLLED MOSAIC OF WAINWRIGHT AREA, NORTHWESTERN ALASKA.

[Photographs by U.S. Navy]

The radial-dendritic drainage pattern shown is anomalous to the Arctic coastal plain where northward-flowing streams predominate. Local relief across the area is only a few feet per mile. The radial drainage pattern, suggestive of subsurface structure, is readily seen on the small-scale mosaic but could be easily overlooked on single photographs or individual stereoscopic pairs. Note the northward deflection of the Kugrua River; the abrupt change in direction of streamflow is believed due to subsurface structure. Seismic work indicates a structural nose plunging southeast in the north-central part of the area. Outcrops are sparse in the area and surface indications of structure, other than drainage pattern, are generally lacking. The drainage pattern of this area is similar to that of an area to the southeast where gas was found in a subsurface structure that had been defined by geophysical methods.

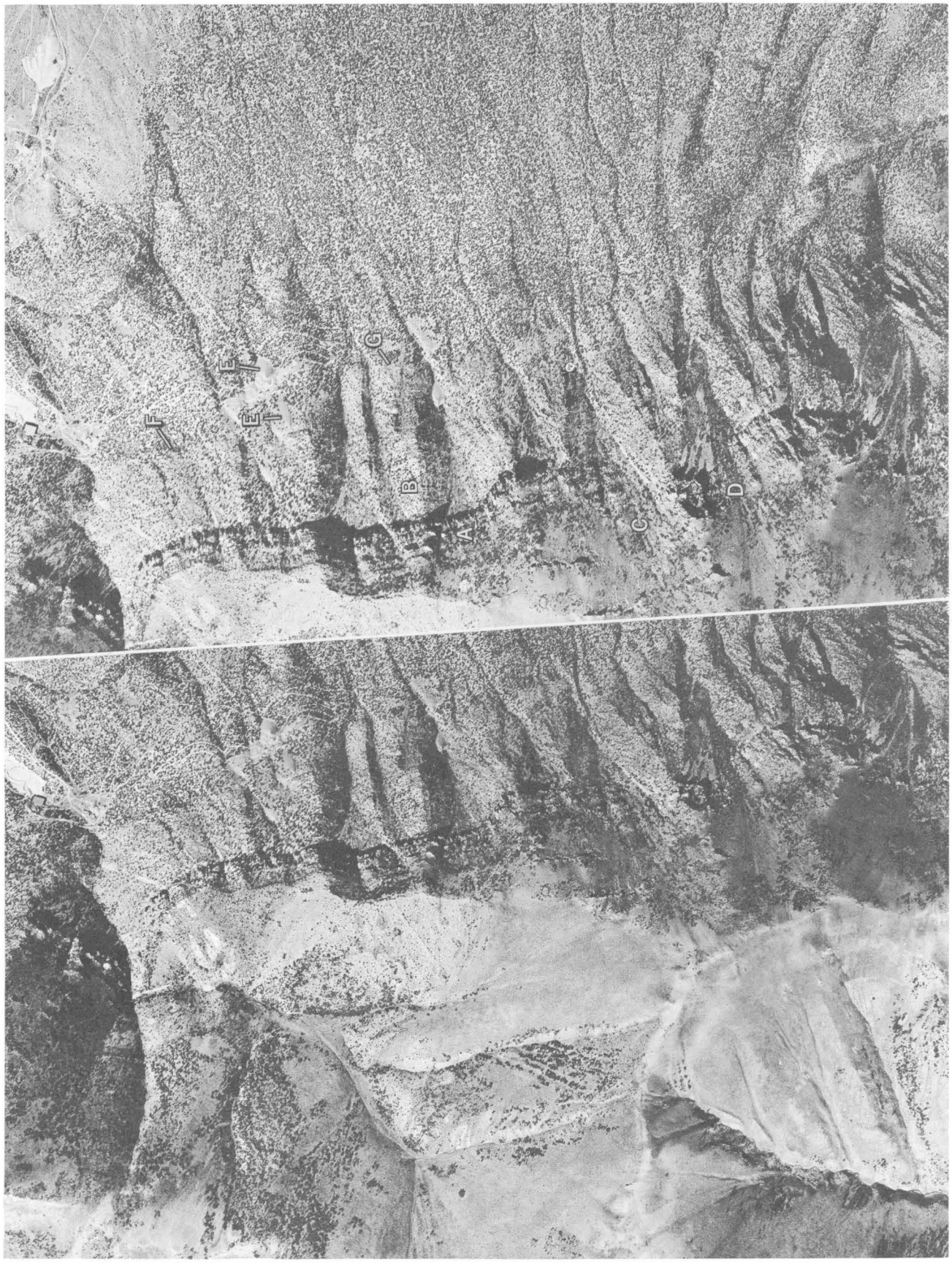
Stereoscopic pair

Approximately 1 mile

FIGURE 97.—AREA UNDERLAIN PREDOMINANTLY BY GENTLY DIPPING SANDSTONE AND SHALE (NORTHERN ALASKA).

[Approximate scale 1 : 20,000. Photographs by U.S. Navy]

Sandstone beds stand out because of photographic tone, relief, and vegetation changes, as at *A*. As these sandstone beds are traced across the area they lose their topographic expression, as at *B*, and are replaced by shale of the underlying formation. The rate of "shaling" or change of facies from sandstone to shale can be calculated from quantitative studies of the aerial photographs, and the direction of maximum thinning of the sandstone section determined. Note the effect of vertical exaggeration on dip of resistant sandstone beds; true dip is 7° to 8° in this area. Effect of vertical exaggeration is also shown at *C* where minor topographic breaks in slope, accentuated by shadows, reflecting thin resistant beds stand out.



Stereoscopic pair

Approximately 1 mile

553966 O-60—9

FIGURE 98.—GENTLY DIPPING SEDIMENTARY ROCKS CUT BY HIGH-ANGLE FAULTS (NEVADA).

[Approximate scale 1 : 20,000. Photographs by Soil Conservation Service]

Topographic expression of resistant, jointed quartzite bed, *A*, permits differentiation of quartzite and underlying carbonate sequence of rocks, *B*. High-angle faults, transverse to the strike of bedding are shown at *C* and *D* by the vertical offset of the quartzite bed. The contact of quartzite and underlying carbonate rocks is the locus of polymetal sulfide veins, but the veins cannot be seen in the stereoscopic model. Note mine dumps, *E*, marking location of crosscuts to base of the quartzite, which dips into the slope about 20° to 25°. Direction of dip is clearly indicated by V in outcrop pattern of quartzite bed where major stream cuts through the ridge. Trace of a major fault with several thousand feet displacement is only weakly shown parallel to slope at *F* and *G* where density of vegetation is slightly greater on the downhill side of the fault trace.

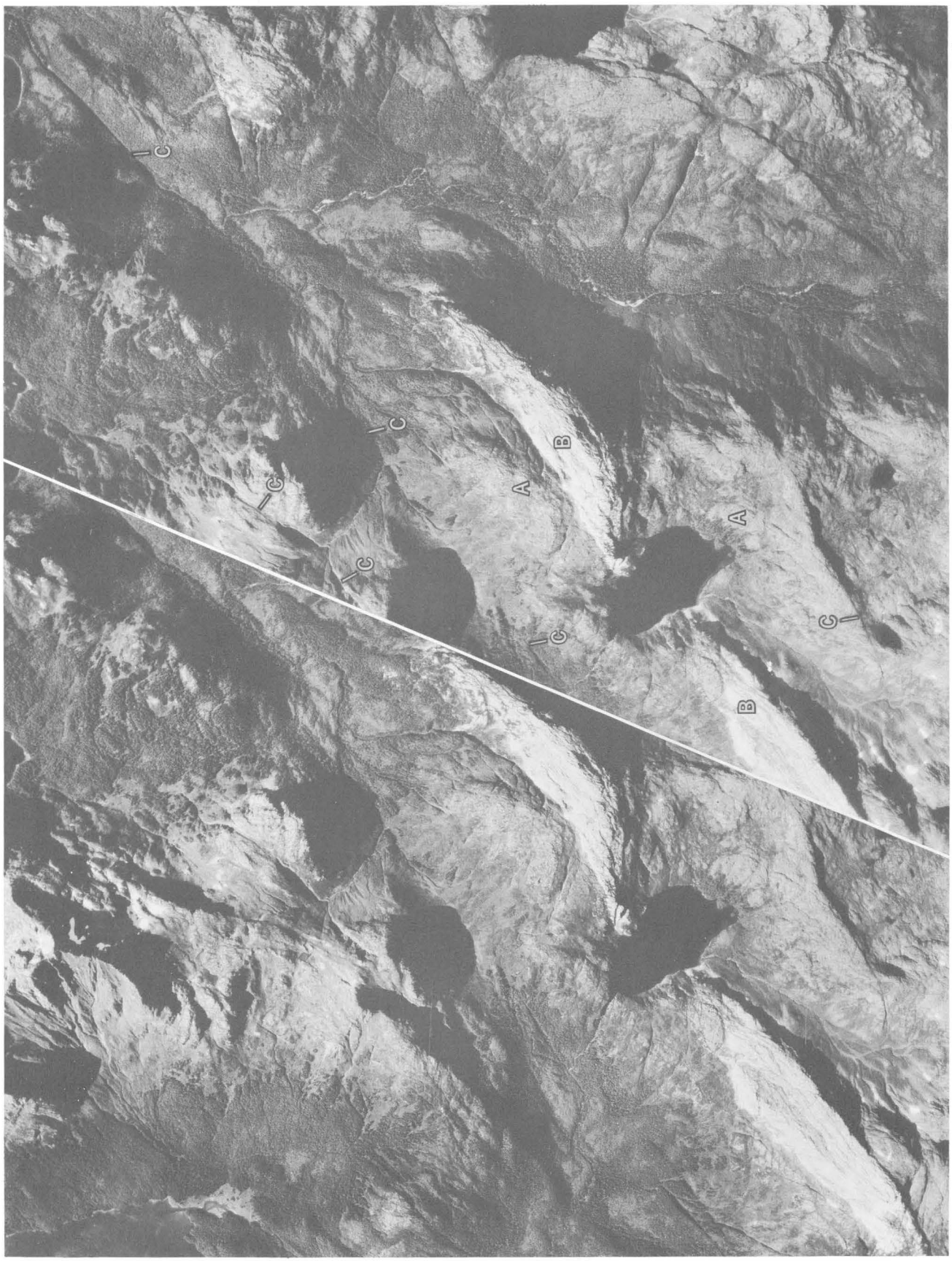

C
C
C
C
C
C
C
A
B
A
B
B
Stereoscopic pair
Approximately 1 mile

FIGURE 99.—COMPLEXLY FOLDED AND FAULTED AREA OF GREENSTONE, SCHIST, LIMESTONE AND MARBLE (SOUTHEASTERN ALASKA).

[Approximate scale 1 : 40,000. Photographs by U.S. Navy]

Relatively dark-toned highly fractured rocks, *A*, are greenstone and greenstone schist. Light-toned profusely fractured rocks, *B*, are limestone and marble. Prominent lineations, *C*, are representative of faults along which rich gold-quartz veins have been found in this area. Note that fault lineations characteristically are rectilinear depressions.

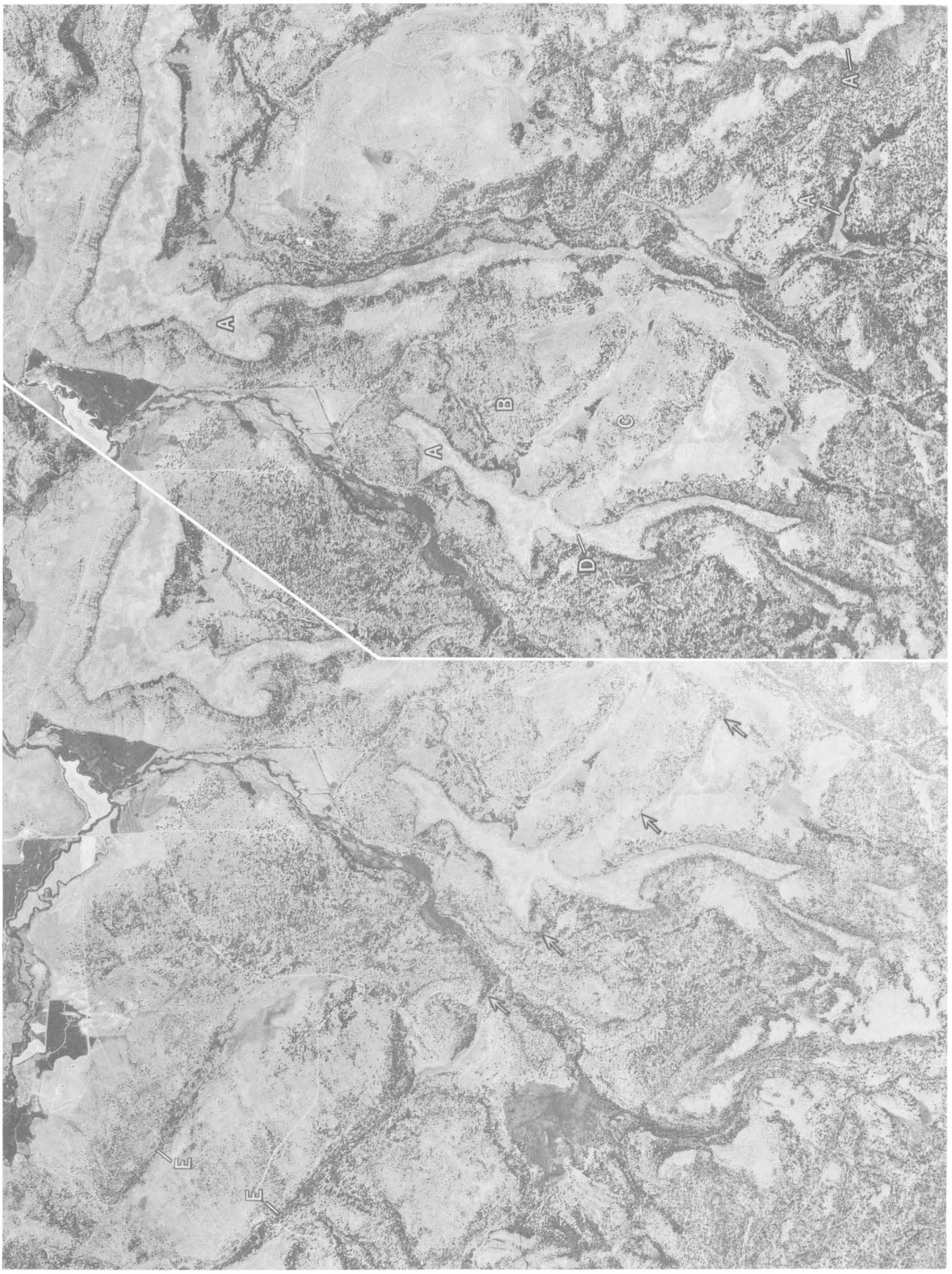
Stereoscopic pair

Approximately 1 mile

FIGURE 100.—IGNEOUS AND METAMORPHIC TERRAIN (SOUTHEASTERN ALASKA).

[Approximate scale 1 : 40,000. Photographs by U.S. Navy]

In this area lead and silver deposits are found locally along the contact of intrusive quartz diorite and metamorphic rocks. Smooth slopes, *A*, are underlain by metamorphic rocks. The closely spaced parallel ridges and depressions, *B*, reflect foliation in the metamorphic rocks. Depressions, *C*, probably represent solution cavities in carbonate interbeds. Lineations, *D*, transecting the foliation direction are believed to be expressions of faults. The uneven surface, *E*, cut by a crisscross of joints is underlain by quartz diorite. This pattern of lines representing joints is typical, but not necessarily diagnostic, of intrusive rocks. The contact of igneous and metamorphic rocks is in the conspicuous saddle between *A* and *E*.



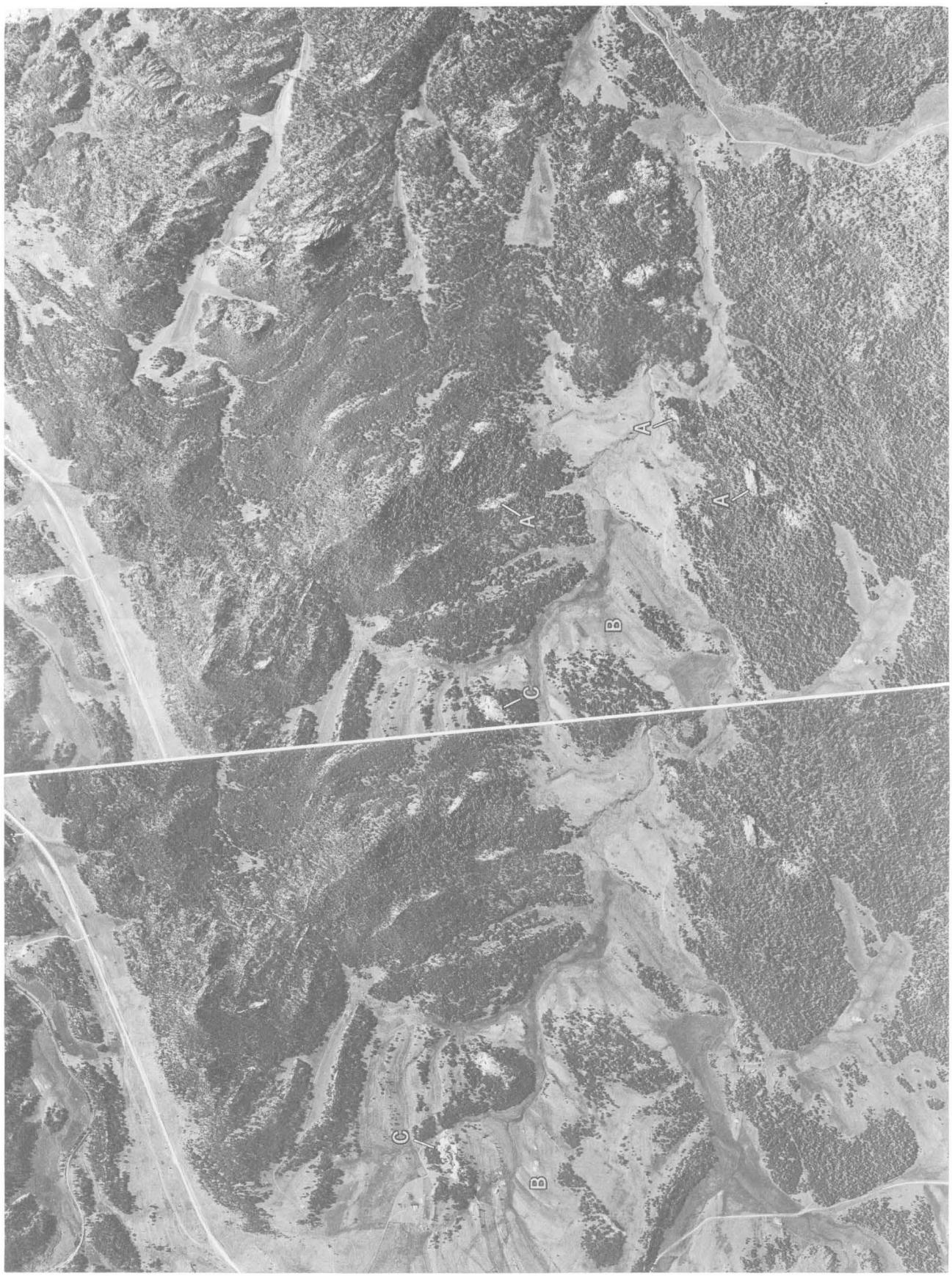
Stereoscopic pair

Approximately 1 mile

FIGURE 101.—GENTLY TILTED AND FAULTED LAVA FLOWS (OREGON).

[Approximate scale 1 : 54,000. Photographs by Army Map Service]

Perched remnants of basaltic lava, *A*, form skeletal dendritic pattern, which suggests that lava filled former stream valleys. In some areas perched lava remnants are known to cover older auriferous stream gravel. Several faults are indicated by alinements of stream segments, vegetation lines, and photographic tone contrasts (see alinement of arrows). Dip on flow surfaces, as at *B*, may be readily estimated or measured from aerial photographs because of the relatively large area examined in a single view, and because of vertical exaggeration of the dip slope. Note that the younger flow, *A*, has a gentler dip than the older flows, *B* and *C*. Surfaces *B* and *C* may be correlative and separated by a fault in the intervening valley. At point *D* the younger perched lava flows are also faulted, but throw is considerably less than where older lava flows are displaced by the same fault. In some areas faults displace only the older rocks and do not offset the most recent flows. A long period of fault activity is thus suggested. Note that in monoscopic view fault alinements, *E*, accentuated by vegetation, are striking.



Stereoscopic pair

Approximately 1 mile

FIGURE 102.—AREA OF PEGMATITE DIKES (SOUTH DAKOTA).

[Approximate scale 1 : 24,000. Photographs by U.S. Geological Survey]

Pegmatites in the area shown are generally concordant with schistosity and bedding of quartz-mica schist country rock. In many places the pegmatite dikes stand in topographic relief above the surrounding schist, as at *A*. The massive, jointed character of the larger pegmatite dikes is similar to other intrusive rocks and contrasts with the thin-bedded schistose rocks. Thin pegmatite dikes commonly cannot be distinguished in the aerial photographs and only general contact areas can be mapped for most of the wide pegmatite dikes because of the vegetation cover. Locally steeply dipping schist also stands in topographic relief; these rocks can be distinguished by the sheeted character of the outcrops. General structural trends are reflected in topographic expression of parallel ridges and in photographic tones of vegetation in fields, *B*. Note mining activity in pegmatite at *C*.

A
B
C
D
E
E
E
Stereoscopic pair
Approximately 1 mile

FIGURE 103.—METAMORPHOSED SEDIMENTARY ROCKS INTRUDED BY QUARTZ MONZONITE (CALIFORNIA).

[Approximate scale 1 : 47,000. Photographs by U.S. Geological Survey]

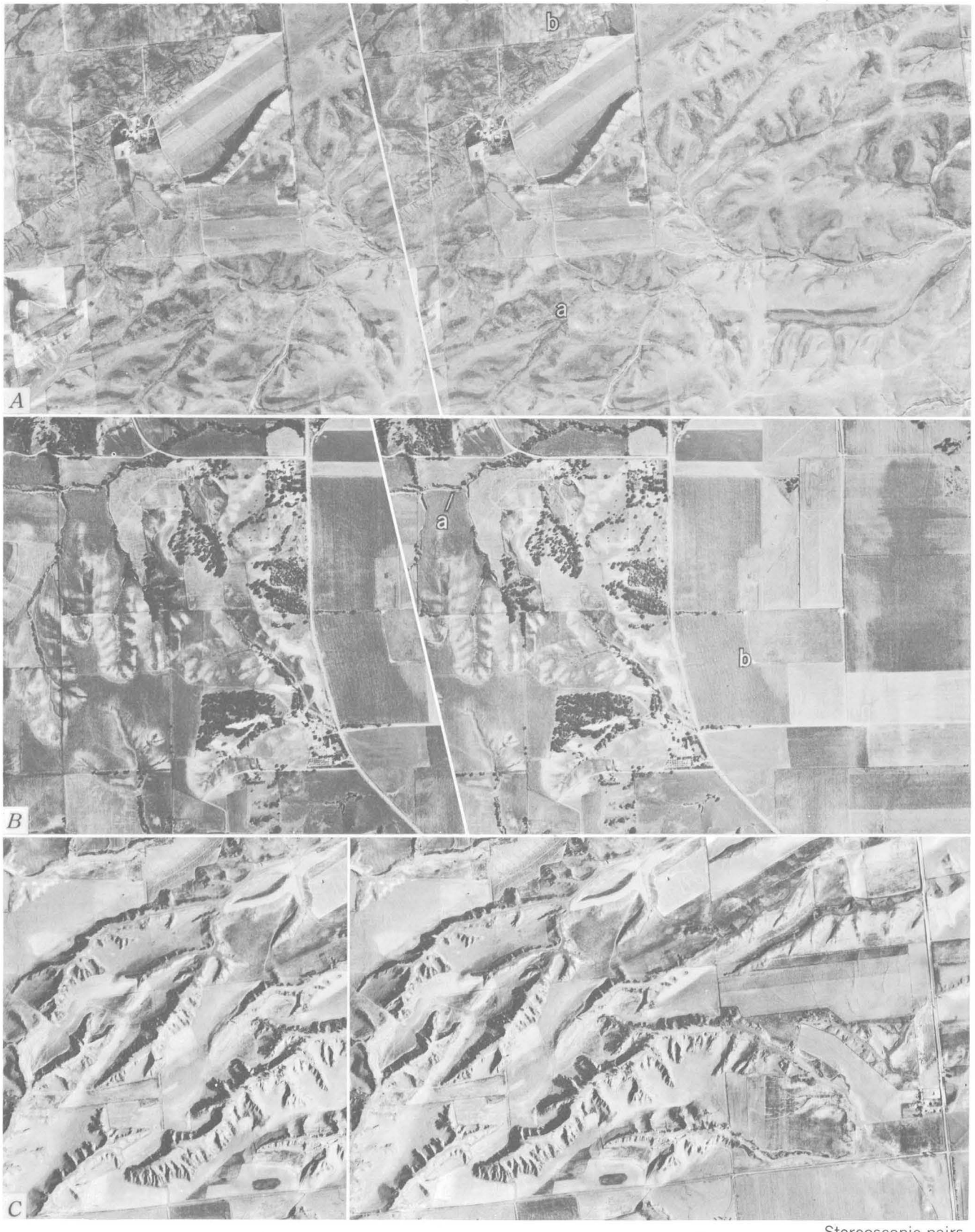
Metamorphic rocks here are generally dark toned, as at *A*, and locally show prominent banding; joints are closely spaced and are not conspicuously shown on the photographs. Quartz monzonite, *B*, is relatively light toned and lacks banding, but like most intrusive igneous rocks it has a strong development of irregularly and widely spaced joints that are readily seen in the stereoscopic model. Light-toned streaked, prominent talus slopes, *C*, have formed where the fine-grained metamorphic rocks are present. In areas of igneous rocks the talus slopes are less well developed; locally large individual talus blocks can be observed at the bases of slopes. A fault trace is suggested by conspicuous linear feature, *D*. Note alinement of short straight linear segments, *E*, on opposite sides of divide; these linear traces may represent the trace of a fault or the prominent development of joints.

A
B
B
B
C
D
D
D'
D'
Stereoscopic pair
Approximately 1 mile

FIGURE 104.—DISTINCTIVE LANDFORM OF GRAVEL TERRACES ALONG A MAJOR STREAM (NORTHEASTERN UTAH).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

The steplike landform of terraces is conspicuous. Other elements of the soil pattern—vegetation, drainage, and erosional characteristics—provide significant information to the photointerpreter. Absence of surface drainage, as at *A*, suggests well-drained materials. At *A* the material is composed of coarse bouldery gravel that has good internal drainage. Vegetation, *B*, is prominent along edges of upper terrace gravel cap where water emerges from the gravel. Lower terraces, as at *C*, are more continuous and less dissected than the older terraces at higher altitudes, although recent streams in conspicuous V-shaped gullies, *D*, dissect the edge of the terrace. Terrace deposits commonly are favorable reservoirs for ground-water storage; in addition they provide a ready source of some materials used by the construction engineer.



Stereoscopic pairs

Approximately 1 mile

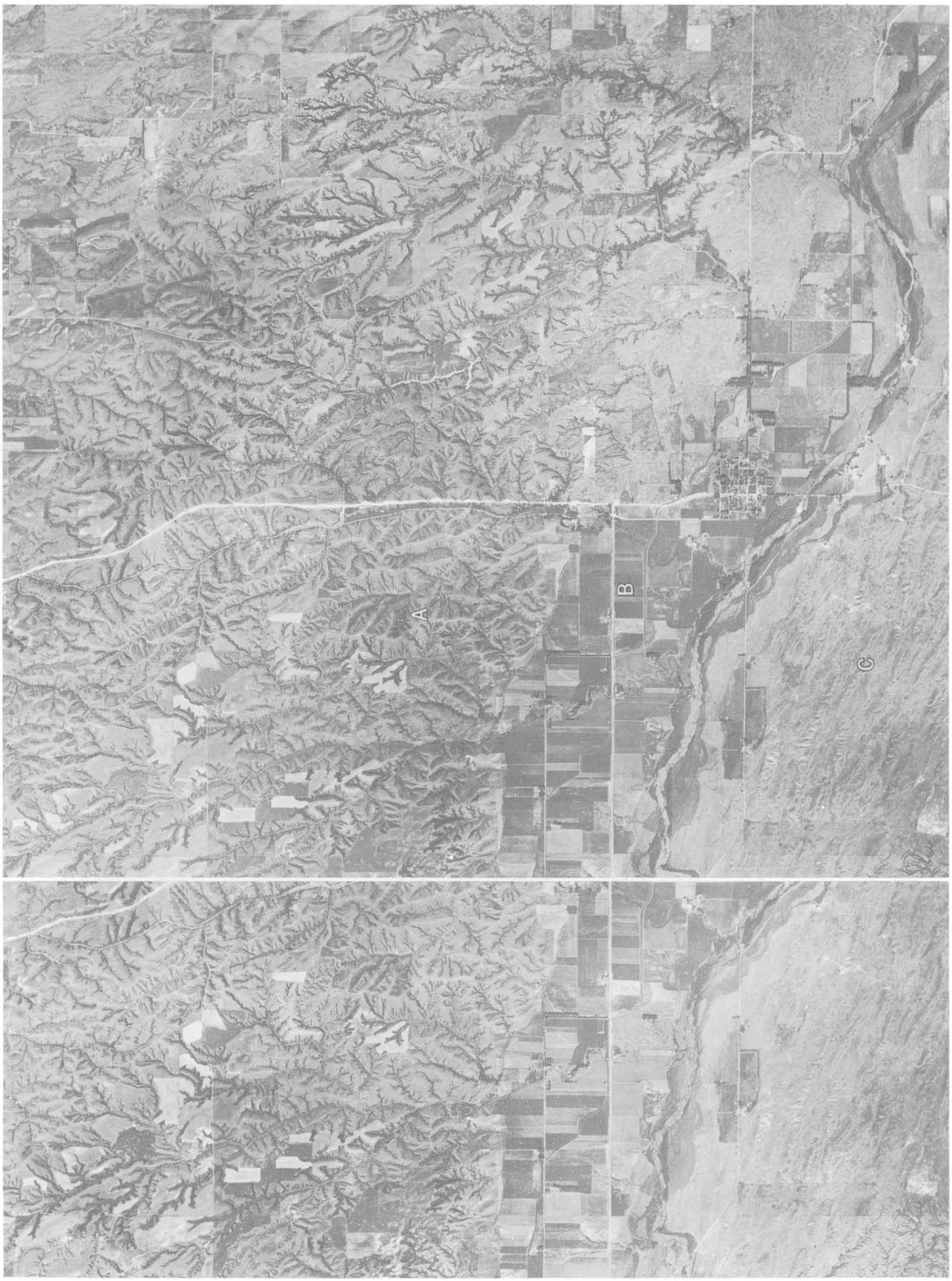
FIGURE 105.—AREAS SHOWING DRAINAGE CHARACTERISTICS IN SURFICIAL MATERIAL THAT IS PREDOMINANTLY LOESS.

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Figure *A*. Contrasting drainage characteristics and differences in photographic tones in areas *a* and *b* suggest differences in character of the surficial materials. The modified dendritic drainage and scoop-shaped valley heads are typical of dissected loess areas, *a*. Lack of surface drainage rills is a feature of sand dune areas, *b*, where materials are coarse-grained, highly permeable, and drainage is largely internal. Note light-and-dark mottled soils in sand dune area. The fine-grain size of loess is believed responsible for the fine-textured drainage (Iowa).

Figure *B*. As in area shown in figure *A*, the dissected loess hills exhibit a modified dendritic drainage pattern. Recent erosion has cut deep narrow and sharply defined channels in the bottoms of broad valleys, as at *a*. Gully walls are essentially vertical. Note characteristic scoop shape of side drainage and serrated ridges along some divides. Light streaks due to thin grass cover or to cultivation are typical of many loess areas. Broad, flat river flood plain, *b*, has good internal drainage and exhibits a lack of visible surface drainage channels (Nebraska).

Figure *C*. Deeply dissected loess hills have drainage pattern similar to areas shown in figures *A* and *B*, but erosion may have proceeded more rapidly than in other areas. Valley walls are sharply defined. Steep valley walls commonly characterize loess (Nebraska).



Stereoscopic pair

Approximately 1 mile

FIGURE 106.—AREA OF SURFICIAL DEPOSITS, PRIMARILY WINDBLOWN (CENTRAL NEBRASKA).

[Approximate scale 1 : 67,000. Photographs by Army Map Service]

Highly dissected loess hills, *A*, abut against well-drained alluvial terraces, *B*. Extensive dissection of loess has resulted in a fine texture of erosional topography and fine-textured drainage. Bottoms of many valleys in loess are notched by recent stream dissection. The modified dendritic drainage pattern is typical of loess area. Note absence of surface drainage rills in terrace alluvium, *B*, and elongate windblown sand hills, *C*, indicating the highly permeable nature of the underlying materials. Loess is generally considered well drained internally and is thus an exception to the general association of fine-textured drainage and impermeable soils. The fine-textured drainage in loess is believed to be a result of the fine grain size. Contrast appearance here of drainage density in loess with drainage density on large-scale photographs of figure 105.

Stereoscopic pair

Approximately 1 mile

FIGURE 107.—MOTTLED SOILS OF DRIFT PLAIN (IOWA).

[Approximate scale 1 : 27,000. Photographs by U.S. Geological Survey]

Light-toned areas are generally slightly higher than surrounding dark-toned areas. High areas of light photographic tone are somewhat better drained than the intervening dark areas, and generally contain silty soils with a lesser accumulation of organic material than the depressions. Clay materials and humus have accumulated in depressions to impart dark photographic tone. Linear pattern of light-toned areas may represent minor recessional moraines. They trend across the direction of movement of ice. Near major streams the reworked glacial drift may be better sorted and locally an important source of borrow material for the construction engineer.

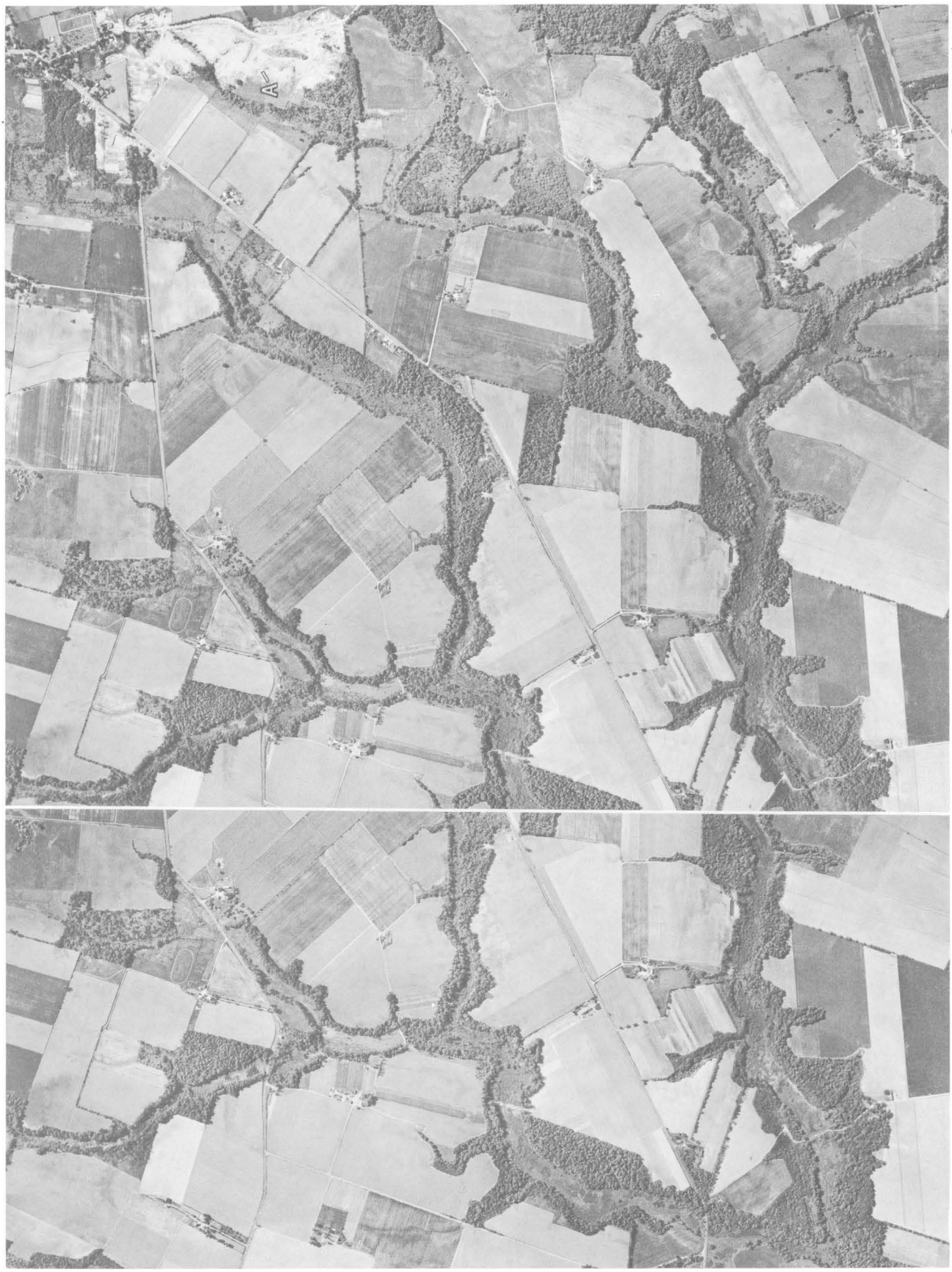
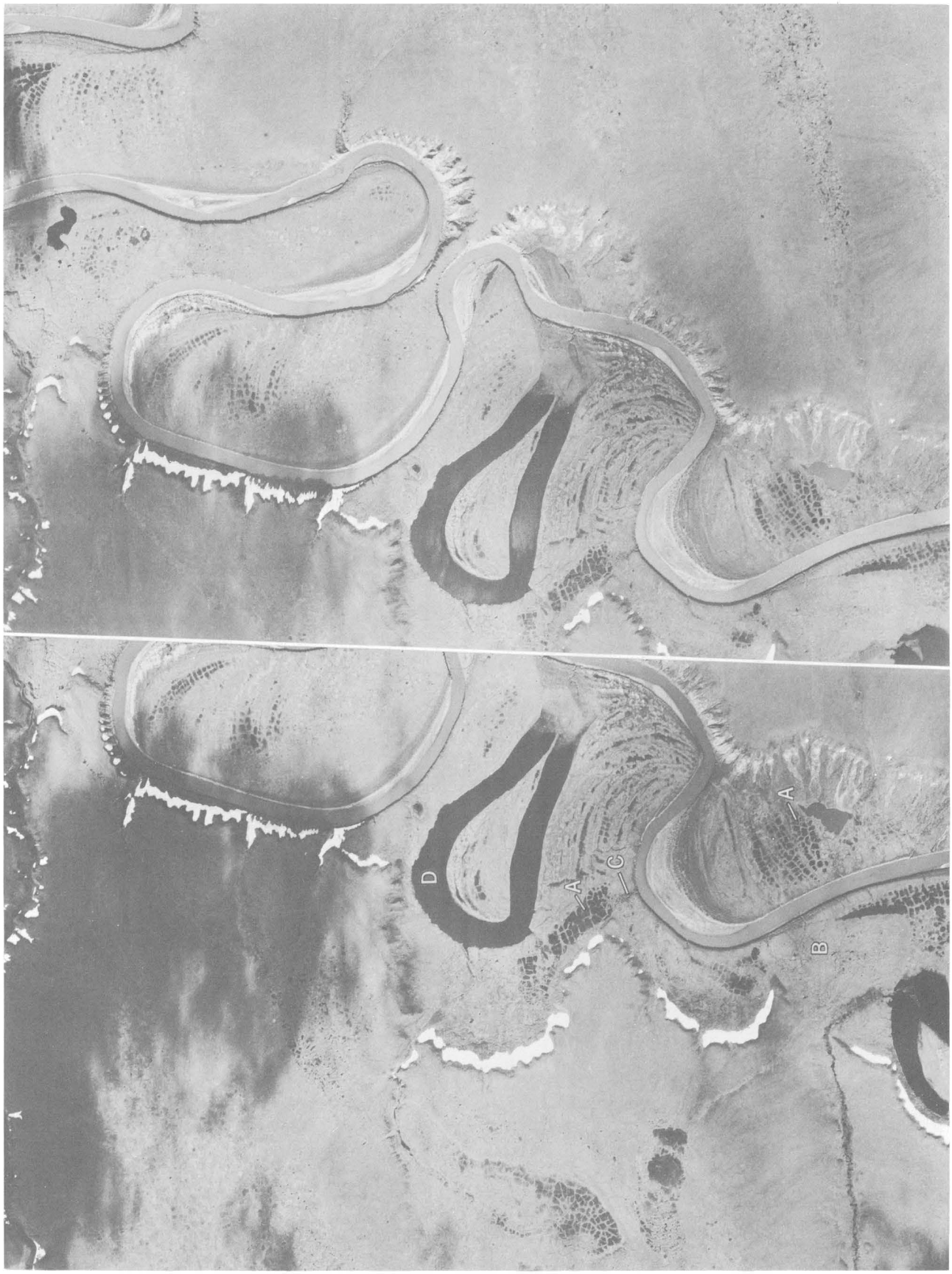

A
A'
Stereoscopic pair
Approximately 1 mile

FIGURE 108.—COASTAL PLAIN UNDERLAIN BY CLAY, SAND, AND GRAVEL (NEW JERSEY).

[Approximate scale 1 : 20,000. Photographs by Commodity Stabilization Service]

Cultivated areas are thin cappings of sand and gravel overlying clay formation. Lack of surface drainage rills in sand and gravel indicate that the capping material is well drained internally. Except for dark-toned crop vegetation the cultivated areas also have the general light tones commonly associated with well-drained materials. Note borrow pit in granular material at *A*. Streams flow in clay. The steep walls and flat bottoms of gullies may not be typical of plastic clays in humid regions, however. Headward extent of small gullies generally ends abruptly against contact of clay with overlying sand and gravel. Vegetation growth is conspicuous along steep sides of gullies where trees have not been cleared for cultivation. Vegetation growth is locally favored by relatively constant supply of water that flows to surface along contact of clay with overlying sand and gravel.



Stereoscopic pair

Approximately 1 mile

FIGURE 109.—POLYGONALLY PATTERNED GROUND IN PERMAFROST AREA ALONG MAJOR STREAM (NORTHERN ALASKA).

[Approximate scale 1 : 20,000. Photographs by U.S. Navy]

The susceptibility of low, poorly drained areas to the development of polygonally patterned ground resulting from ice-wedge formation is shown conspicuously along this major stream valley. Development of polygons, primarily low-center polygons, *A*, shown with relatively dark-toned centers and light-toned marginal ridges, has followed old channel scars representative of old slip-off slopes. Some high-center polygons, *B*, are also present. The angular gully pattern, *C*, is commonly found where ice wedges are melting out of polygonally patterned ground. Also note serrated edges of oxbow lake, *D*, and rim of river terraces were ice wedges in polygonally patterned ground have melted out. Contrast appearance of poorly drained river terraces here with river terraces in nonpermafrost areas where internal drainage is generally good. The conspicuous tilt of the oxbow lake and up-hill flow of stream meanders indicate that tilt is present in the aerial photographs.

Stereoscopic pair

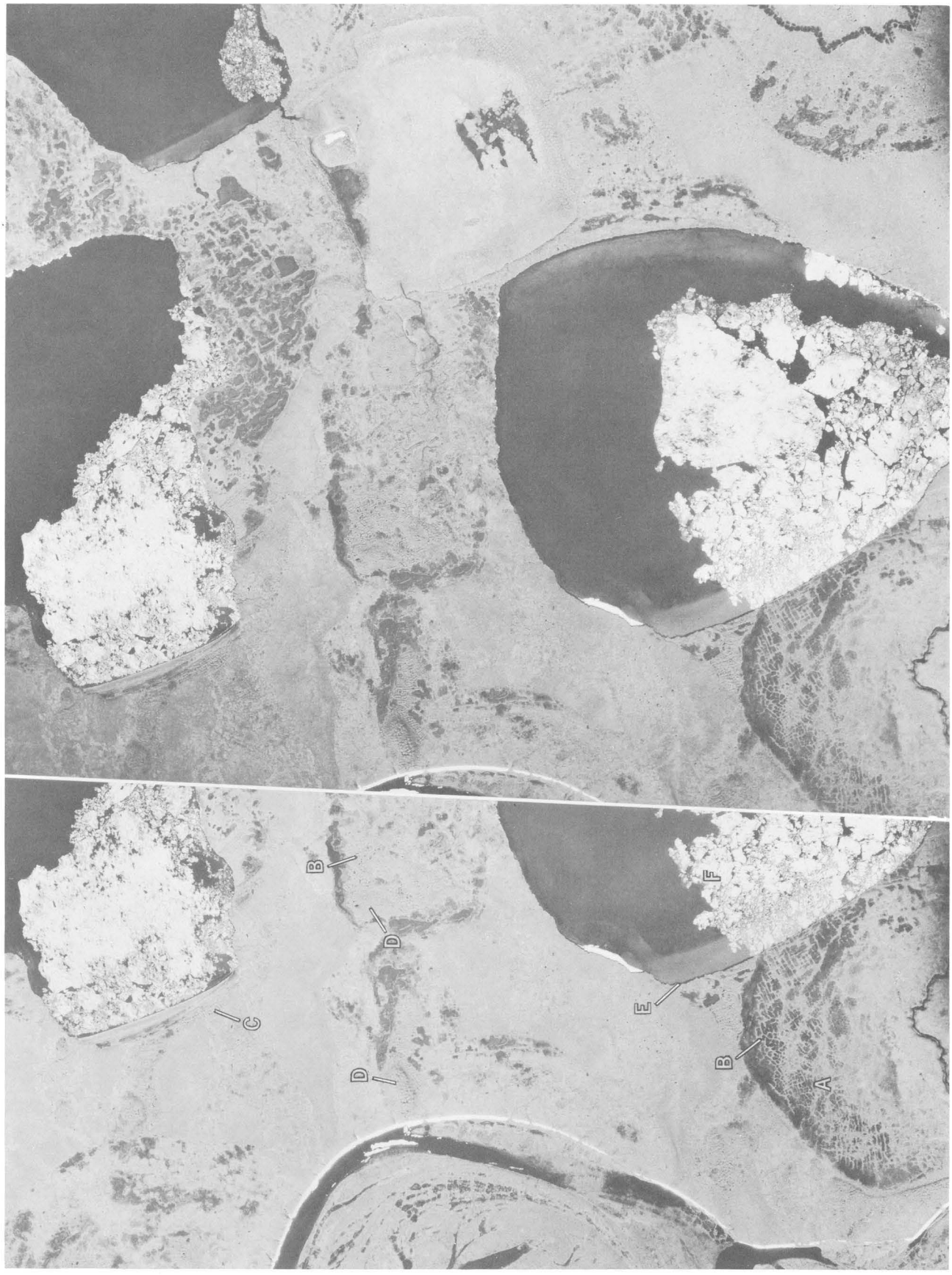
Approximately 1 mile

553966 O-60—10

FIGURE 110.—WELL-DEVELOPED PINGO IN AREA OF PERMAFROST (NORTHERN ALASKA).

[Approximate scale 1 : 20,000. Photographs by U.S. Navy]

Partly drained lake basin, *A*, a particularly favorable area for development of permafrost, is conspicuous. Note old beach lines, *B*, shown by narrow bands of contrasting photographic tones and along which polygonal ground has developed. Low-center polygons having dark-toned centers and light-toned marginal ridges are abundant, as at *C*. High-center polygons with light-toned centers and dark-toned marginal trenches, are also conspicuous in many places, as at *D*. Pingo, *E*, with a single crest crack here, is almost always diagnostic of underlying permafrost conditions. Also note pingolike forms, *F*, covered with polygonally patterned ground.



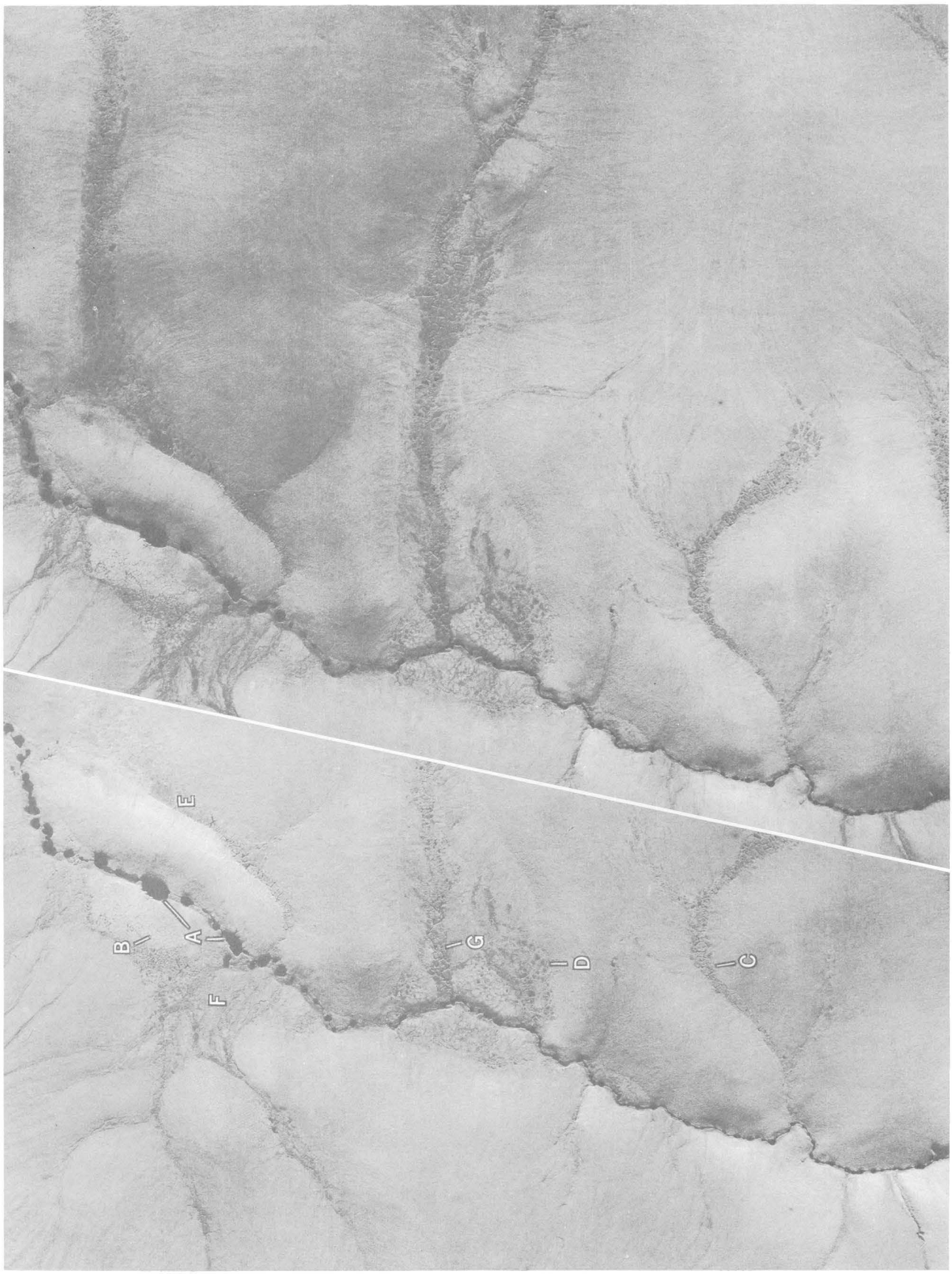
Stereoscopic pair

Approximately 1 mile

FIGURE 111.—AREA OF PERMAFROST (NORTHERN ALASKA).

[Approximate scale 1 : 20,000. Photographs by U.S. Navy]

Low, wet but drained lake basins, as at *A*, are favorable areas for the development of permafrost. Low-center polygons, *B*, shown as dark-toned depressed centers and light-toned raised edges are common. High-center polygons, *C*, exhibiting high, light-toned centers, and dark-toned marginal trenches, are also present. Pingolike forms, *D*, also covered with polygonally patterned ground, are highly indicative of permanently frozen ground conditions. The serrated shoreline, *E*, of some lakes is typical of the thawing of polygonal ground and further suggests the presence of permafrost. Note floating ice, *F*; bottom of lake may be seen at edge of ice, and in places depth of water may be measured from the aerial photographs.



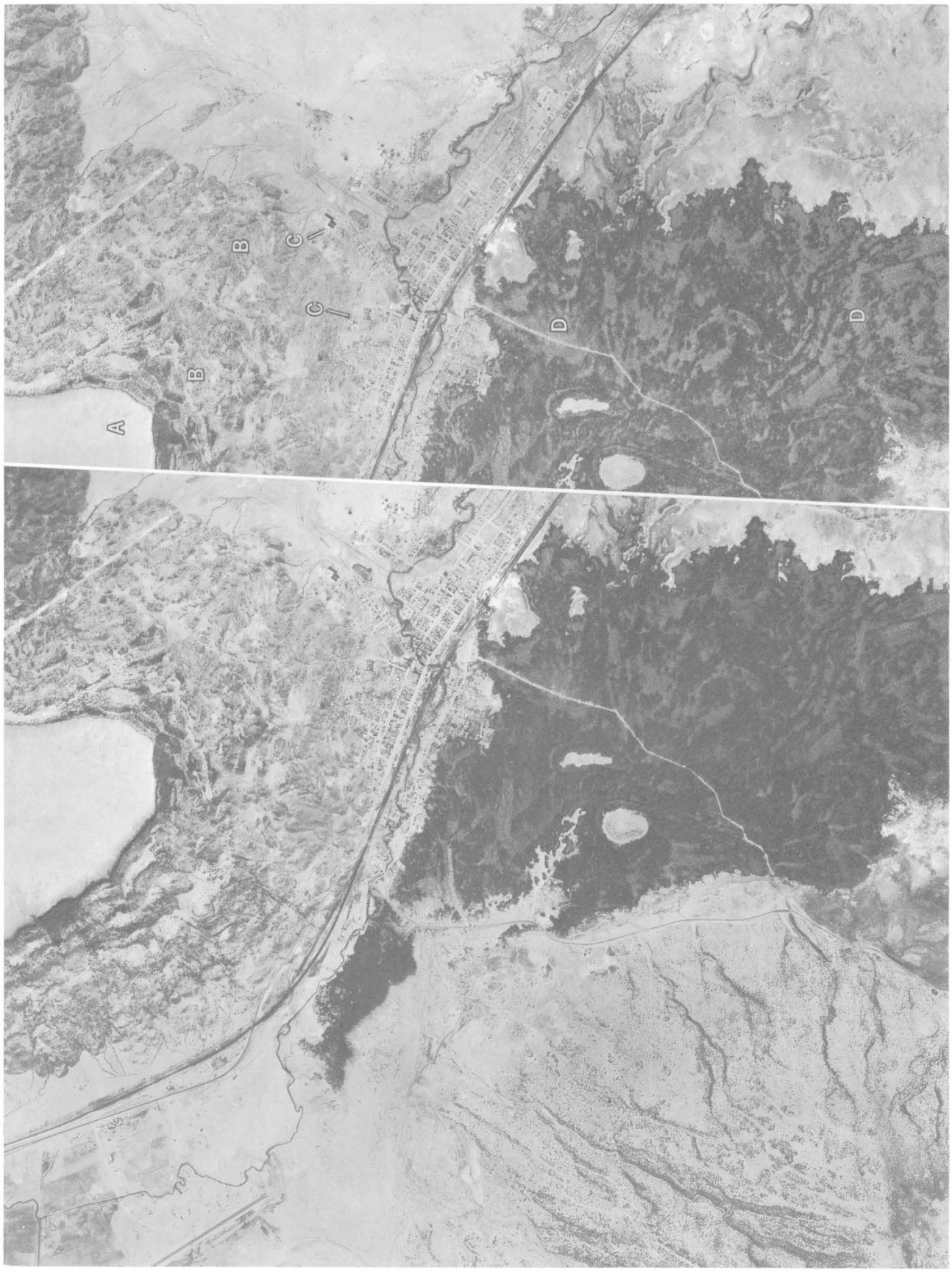
Stereoscopic pair

Approximately 1 mile

FIGURE 112.—CONSPICUOUS BEADED DRAINAGE IN AREA OF PERMAFROST (NORTHERN ALASKA).

[Approximate scale 1 : 20,000. Photographs by U.S. Navy]

Beaded drainage along main stream, shown as rounded pools of water connected by deeply incised watercourses, typically forms in areas underlain by permafrost. Note steep banks of pools, as at *A*, which have resulted from thawing of frozen ground and subsequent caving. Interpretation of permafrost conditions is supported by presence of high-center and low-center polygons. High-center polygons, *B*, generally are shown by relatively light-toned centers and dark-toned rims, although locally, as at *C*, the reverse tonal contrasts may be present. Low-center polygons with relatively dark-toned depressed centers and light-toned raised rims are shown at *D*. The wetter areas, as in the partly abandoned drainage channel, *E*, or upper reaches of minor drainageways, are especially susceptible to formation of polygons. Area *F*, probably a small alluvial fan area, shows well-developed drainage. The angular pattern may indicate incipient polygon formation in contrast to the angular pattern of drainage, *G*, which is typical of areas where melting of ice wedges in polygonal ground is taking place.



Stereoscopic pair

Approximately 1 mile

FIGURE 113.—LANDSLIDE AREA IN VOLCANIC AND SEDIMENTARY TERRAIN (NEW MEXICO).

[Approximate scale 1 : 37,000. Photographs by U.S. Geological Survey]

Resistant flat-lying basaltic lava, *A*, caps mesa underlain by weakly resistant mudstone, shale, siltstone, and sandstone, a geologic environment particularly susceptible to the occurrence of landslides. Landslides, *B*, below lava cap are characterized by hummocky topography and local lobate form suggestive of flowage. Note buildings, *C*, constructed on toe of slide areas. Recent lava flows are indicated by the dark photographic tone and irregular surfaces, *D*. The lobate character typical of flows can also be seen.

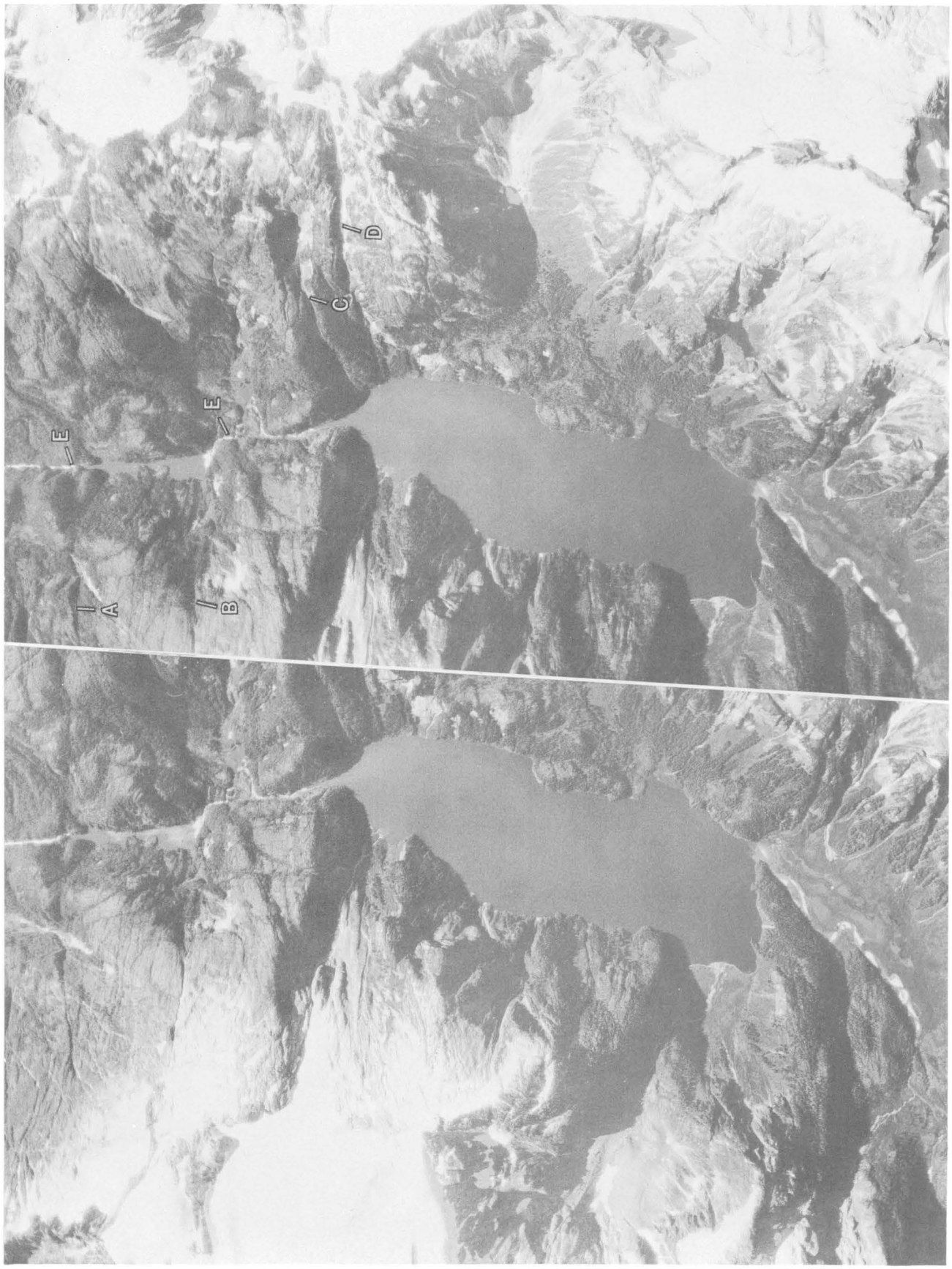

A
B
E
E
C
D
Stereoscopic pair
Approximately 1 mile

FIGURE 114.—DAMSITE AREA (SOUTHEASTERN ALASKA).

[Approximate scale 1 : 40,000. Photographs by U.S. Navy]

Conspicuous faults, indicated by linear topographic depressions *A*, *B*, *C*, and *D*, are present. The outlet of the lake itself appears to flow along a fault marked by the rectilinear depression *E*; this fault is probably the most significant geologic structure in the area because a dam would have to straddle it. Highly fractured rocks comprise metamorphic types and intrusive quartz diorite.

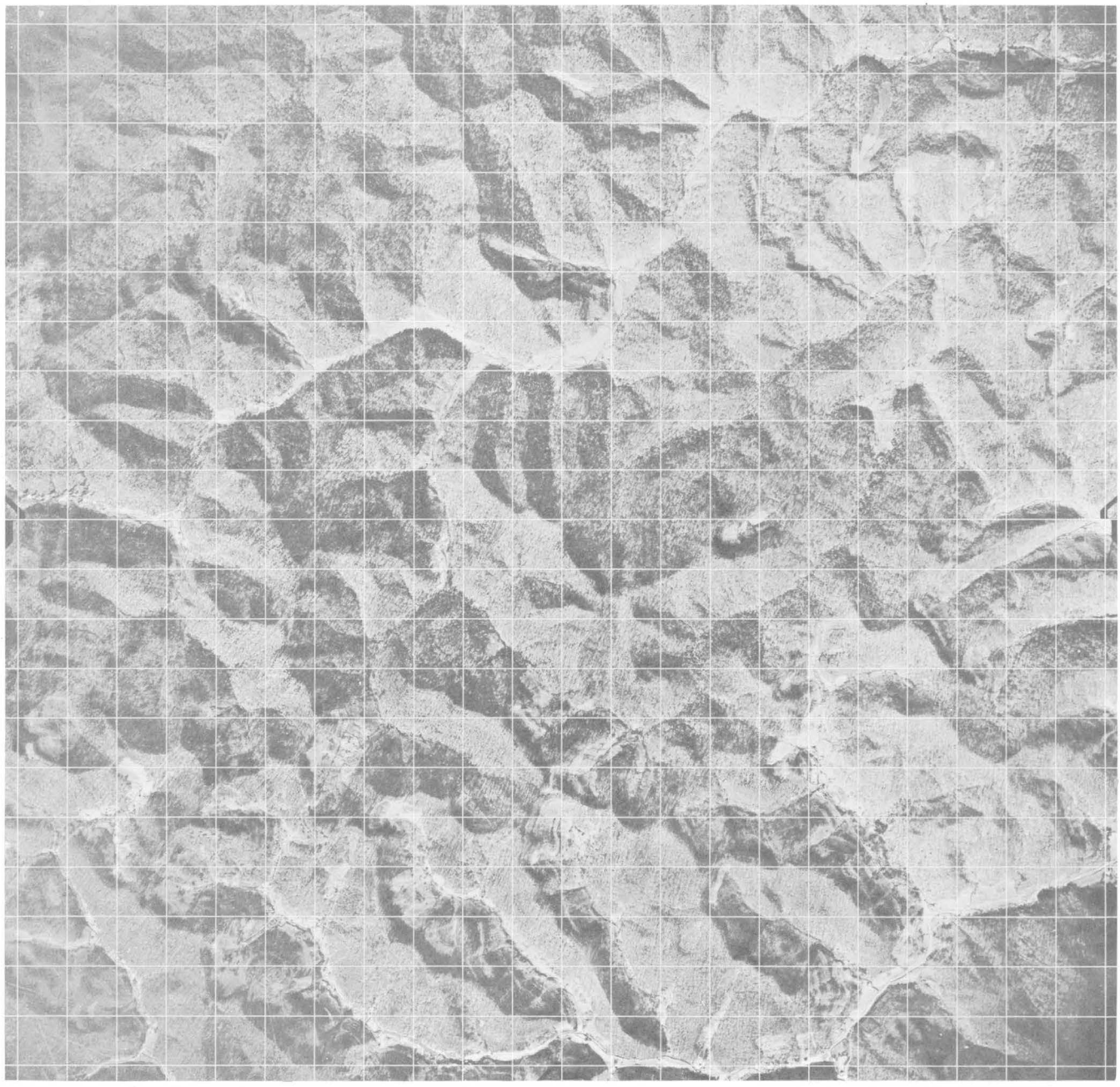


FIGURE 115.—GRIDDED PHOTOGRAPH.

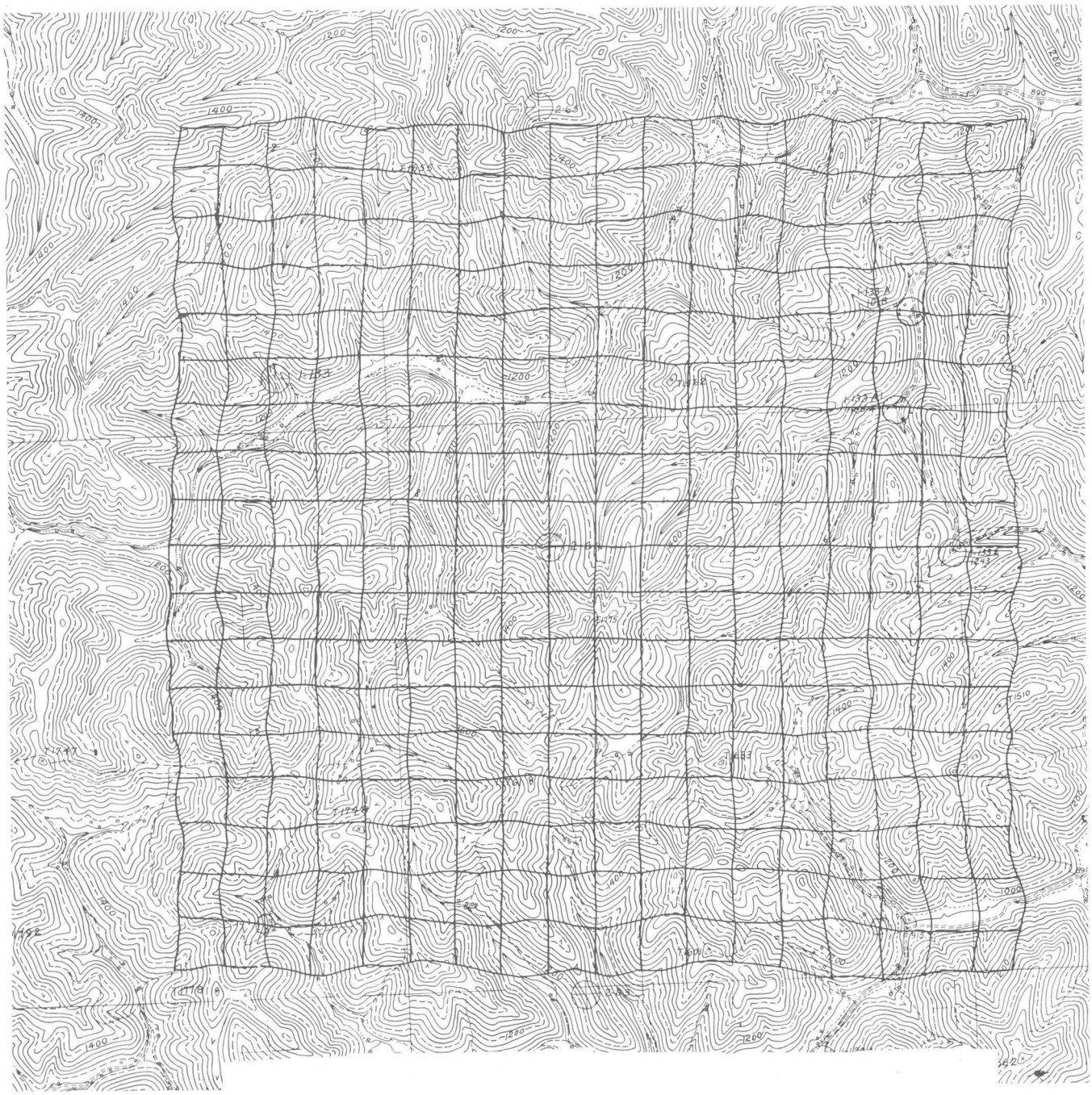


FIGURE 116.—GRIDDED BASE MAP OF AREA SHOWN IN FIGURE 115.

SOURCE AND IDENTIFYING DATA OF AERIAL PHOTOGRAPHS

The following table gives all data needed to identify the aerial photographs and also the agencies from which the aerial photographs may be purchased. Note that the agency holding the negatives is not necessarily the one that originally acquired the photographs.

Figure	Identifying photographic data					Negatives held by [1]—
	Project code	Roll	Exposures	Focal length of lens, in inches	Area	
39	DKK	3	16–17	8.25	"DKK" Gunnison area, Colorado	E
40	BAR	309	071–072	6	Alaska	A
41	DSA	2K	19–20	8.25	Kane County, Utah	D
42	GS–WI	12	146–147	6	Utah	A
43	DIG	1F	127–128	8.25	San Juan County, Utah	D
44	GS–RR	3	147–148	6	Arizona	A
45	AFTRC/3415TTW/49–10/M–1.		697VV–698VV	12	Golden, Colorado	B
46	GS–VJV	3	150–151	6	Colorado	A
47						N
48	71	60	8395–8396	6	South Carolina	A
49	138	3	489–490	5.2	Texas	A
50	DRK	21	3–4	8.25	"DRK" Addition to Humboldt River, Nevada.	E
51	GS–COL	3	56–57	6	California	A
52	GS–JF	6	11–12	6	Wyoming	A
53	DLG	7G	97–98	8.25	Elmore County, Idaho	D
54	71	26	3514–3515	6	North Carolina	A
55*A*	73	4	117–118	6	Maine	A
B	GSM	3	31–32	5.2	do	A
56	Mission 649		0120–0121	6	Alaska	A
57	Mission 648		0161–0162	6	do	A
58	113	16	1746–1747	6	South Dakota	A
59	GS–WI	10	102–103	6	Utah	A
60	126	18	1723–1724	6	do	A
61	CUU	8G	141–142	8.25	Stephens County, Texas	D
62	GS–RO	1	125–126	6	Utah	A
63	GS–WI	36	68–69	6	do	A
64	GS–AZ	2	119–120	5.2	Virginia	A
65	AQV	1D	55–56	8.25	Northampton County, Pennsylvania	C
66	113	21	2600–2601	6	South Dakota	A
67	SEA	92	019–020	6	Alaska	A
68	138	10	1919–1920	5.2	Texas	A
69	CNP	1C	11–12	8.25	Gooding County, Idaho	D
70	GS–VE	5	26–27	6	South Dakota	A
71	GS–OMA	32	88–89	5.2	Wyoming	A
72	SEA	29	028–029	6	Alaska	A
73	71	50	7084–7085	6	North Carolina	A
74	71	7	820–821	6	do	A
75	GSY	1	145–146	5.2	Alabama	A
76	SEA	112	181–182	6	Alaska	A
77	ZF	2G	174–175	8.25	Wabaunsee County, Kansas	D
78	CUU	8G	152–153	8.25	Stephens County, Texas	D
79	BAR	44	61–62	6	Alaska	A
80	131	11	1711–1712–1713	6	Wyoming	A
81	BPM	11	63–64	6	Muddy River area, Utah	E
82	GS–PB	1	50–51	6	New Hampshire	A
83	GS–WI	5	156–157	6	Utah	A
84	GS–RR	17	43–44	6	do	A
85	SEA	112	077–078	6	Alaska	A
86	131	7	1187–1188	6	Wyoming	A
87	120	70	10110–10111	6	New Mexico	A
88	DRW	1K	94–95	8.25	Duchesne County, Utah	D
89						N
90	GS–RO	4	167–168	6	Utah	A
91	GS–RR	2	64–65	6	do	A
92	GS–RR	17	64–65	6	do	A
93						N
94	138	5	867–868	6	Texas	A
95	138	5	867–868	6	do	A
96					Wainwright, area index quadrangle D–19, Alaska.	A
97	BAR	44	139–140	6	Alaska	A
98	DRK	21	197–198	8.25	"DRK" Addition to Humboldt River, Nevada.	E

See footnote at end of table.

SOURCE AND IDENTIFYING DATA OF AERIAL PHOTOGRAPHS—Continued

Figure	Identifying photographic data					Negatives held by [1]—
	Project code	Roll	Exposures	Focal length of lens, in inches	Area	
99	SEA	133	019–020	6	Alaska	A
100	SEA	106	125–126	6	do	A
101	109	43	5283–5284	6	Oregon	A
102	GS–VE	5	112–113	6	South Dakota	A
103	GS–QQ	1	89–90	6	California	A
104	DRW	1K	47–48	8. 25	Duchesne County, Utah	D
105*A*	BKP	4G	14–15	8. 25	Pottawattamie County, Iowa	C
B	BNQ	172	15–16	8. 25	Valley County, Nebraska	C
C	BNQ	96	30–31	8. 25	Valley County, Nebraska	C
106	128	5	751–752	6	Nebraska	A
107	GS–DY	5	40–41	5. 2	Iowa	A
108	CMU	3R	139–140	8. 25	Burlington County, New Jersey	C
109	BAR	72	087–088	6	Alaska	A
110	BAR	72	098–099	6	do	A
111	BAR	72	093–094	6	do	A
112	BAR	92	010–011	6	do	A
113	GS–VID	1	46–47	6	New Mexico	A
114	SEA	114	008–009	6	Alaska	A

[1] Code is as follows:
A—U.S. Geological Survey, Map Information Office, Washington 25, D. C.
B—U.S. Air Force, Photographic Records and Services Division, Office of Research and Liaison, USAF Aeronautical Chart and Information Center, Washington 25, D.C.
C—Eastern Laboratory, Performance Division, Commodity Stabilization Service, U.S. Department of Agriculture, Washington 25, D.C.
D—Western Laboratory, Performance Division, Commodity Stabilization Service, U.S. Department of Agriculture, 2505 Parleys Way, Salt Lake City 9, Utah.
E—Division of Cartography, Soil Conservation Service, Agricultural Research Center, Beltsville, Maryland
N—Negatives not available.

553966 O–60—11

REFERENCES CITED

Alexander, J. B., and Proctor, W. D., 1955, Investigations upon a proposed dam site at Klang Gates, Federation of Malaya: Colonial Geology and Mineral Resources, v. 5, no. 4, p. 409–415.

Alliger, J., 1955, Application of photogeology to oil exploration in western Canada: Alberta Soc. Petroleum Geologists Jour., v. 3, no. 10, p. 179–184, 194.

Aschenbrenner, C. M., 1952, A review of facts and terms concerning the stereoscopic effect: Photogramm. Eng., v. 18, no. 5, p. 818–823.

——— 1954, Problems in getting information into and out of air photographs: Photogramm. Eng., v. 20, no. 3, p. 398–401.

Barton, D. C., 1933, Surface fracture system of south Texas: Am. Assoc. Petroleum Geologists Bull., v. 17, no. 10, p. 1194–1212.

Bean, R. K., and Thompson, M. M., 1957, Use of the orthophotoscope: Photogramm. Eng., v. 23, no. 1, p. 170–179.

Belcher, D. J., 1944, Identifying landforms and soils by aerial photographs, *in* Purdue Univ. 30th Ann. Road School Proc.: Purdue Univ. Eng. Bull., Ext. Ser. no. 56, p. 133–154.

——— 1945, The engineering significance of soil patterns: Photogramm. Eng., v. 11, no. 2, p. 115–148.

——— 1948, Determination of soil conditions from aerial photographs: Photogramm. Eng., v. 14, no. 4, p. 482–488.

Benninghoff, W. S., 1950, Use of aerial photographs in mapping vegetation and surficial geology in subarctic regions: Photogramm. Eng., v. 16, no. 3, p. 428–429.

Bentor, Y. K., 1952, Air-photographs and geological mapping with special reference to the geological conditions in the Negev (southern Israel): Israel Research Council Bull., v. 2, no. 2, p. 157–169.

Black, R. F., 1952, Polygonal patterns and ground conditions from aerial photographs: Photogramm. Eng., v. 18, no. 1, p. 123–134.

Blanchet, P. H., 1957, Development of fracture analysis as exploration method: Am. Assoc. Petroleum Geologists Bull., v. 41, no. 8, p. 1748–1759.

Brundall, Laurence and Harder, B. P., 1953, Photogeologic evaluation in the Montana Plains area, *in* Billings Geol. Soc. Guidebook 4th Ann. Field Conf., Little Rocky Mountains—Montana, southwestern Saskatchewan, 1953: p. 150–155.

Butorff, Curtis L., 1958, Geomorphic anomalies, Dead Horse Creek area, Wyoming, *in* Wyoming Geol. Assoc. Guidebook 13th Ann. Field Conf., Powder River Basin, 1958: p. 215–217.

Cabot, E. C., 1947, The northern Alaska coastal plain interpreted from aerial photographs: Geog. Rev., v. 37, no. 4, p. 639–648.

Cady, W. M., 1945, Aerial photos as an adjunct to Arctic and Subarctic geologic reconnaissance: New York Acad. Sci. Trans., Ser. 2, v. 7, p. 135–138.

Chapman, R. M., and Sable, E. G., 1960, Geology of the Utukok-Corwin area, northwestern Alaska: U.S. Geol. Survey Prof. Paper 303–C. (In press)

Christensen, D. J., 1956, Eagles of geology: Photogramm. Eng., v. 22, no. 5, p. 857–864.

Colwell, R. N., 1952, Photographic interpretation for civil purposes, *in* Am. Soc. Photogrammetry, Manual of Photogrammetry: 2d ed., Washington, D.C., p. 535–602.

Colwell, R. N., 1954, A systematic analysis of some factors affecting photographic interpretation: Photogramm. Eng., v. 20, no. 3, p. 433–454.

Daehn, R. E., 1949, A standardized tone scale as an aid in photo interpretation: Photogramm. Eng., v. 15, no. 2, p. 287.

DeBlieux, Charles, 1949, Photogeology in Gulf Coast exploration: Am. Assoc. Petroleum Geologists Bull., v. 33, no. 7, p. 1251–1259.

DeBlieux, Charles, and Shepherd, G. F., 1951, Photogeologic study in Kent County, Texas: Oil and Gas Jour., v. 50, no. 10, p. 86, 88, 89, 98–100.

Desjardins, Louis, 1943a, Contouring and elevation measurement on vertical aerial photographs: Photogramm. Eng., v. 9, no. 4, p. 214–224.

——— 1943b, Measurements of dip angles on aerial photographs: Am. Assoc. Petroleum Geologists Bull., v. 27, no. 11, p. 1534–1538.

——— 1950, Techniques in photogeology: Am. Assoc. Petroleum Geologists Bull., v. 34, no. 12, p. 2284–2317.

——— 1951, The measurement of formational thickness by photogeology: Photogramm. Eng., v. 17, no. 5, p. 821–830.

——— 1952, Aerial photos may locate deep-seated salt domes: Oil and Gas Jour., v. 51, no. 13, p. 82–84.

Eardley, A. J., 1942, Aerial photographs—their use and interpretation: New York, Harper and Bros. Publishers, 203 p.

——— 1943, Aerial photographs and the distribution of constructional materials: Natl. Research Council, Highway Research Board, 23d Ann. Mtg. Proc., v. 23, p. 557–568.

Elliott, D. H., 1952, Photogeologic interpretation using photogrammetric dip calculations: California Div. Mines Spec. Rept. 15, 21 p.

——— 1958, Drainage analysis—Donkey Creek area, Powder River Basin, Wyoming, *in* Wyoming Geol. Assoc. Guidebook 13th Ann. Field Conf., Powder River Basin, 1958: p. 214.

Fischer, W. A., 1953, Photogeologic studies of Arctic Alaska and other areas, *in* Selected papers on photogeology and photo interpretation: U.S. Research and Devel. Board, Washington, D.C., p. 207–214.

——— 1955, Photogeologic instruments used by the U.S. Geological Survey: Photogramm. Eng., v. 21, no. 1, p. 32–39.

——— 1958, Color aerial photography in photogeologic interpretation: Photogramm. Eng., v. 24, no. 4, p. 545–549.

Fisk, H. N., 1944, Geological investigations of the alluvial valley of the lower Mississippi River: U.S. Mississippi River Comm., Vicksburg, U.S. Army, Corps of Engineers.

Frost, R. E., 1946, Identification of granular deposits by aerial photography: Natl. Research Council, Highway Research Board, 26th Ann. Mtg. Proc., v. 25, p. 116–129.

——— 1951, Frost action in soils, *in* A symposium, interpretation of permafrost features from airphotos: Natl. Research Council, Highway Research Board Spec. Rept., no. 2, p. 223–246.

Frost, R. E., and Mintzer, O. W., 1950, Influence of topographic position in airphoto identification of permafrost, *in* Soil exploration and mapping: Natl. Research Council, Highway Research Board Bull. no. 28, p. 100–121.

Frost, R. E., and Woods, K. B., 1948, Airphoto patterns of soils of the western United States: U.S. Civil Aeronautics Admin. Tech. Devel. Rept. no. 85, 76 p.

Goodale, E. R., 1953, An equation for approximating the vertical exaggeration ratio of a stereoscopic view: Photogramm. Eng., v. 19, no. 4, p. 607–616.

Grantham, D. R., 1953, Aerial photography, vegetation and geology: Mining Mag., v. 88, no. 6, p. 329–336.

Greenman, R. L., 1951, The Engineer looks at pedology, *in* Symposium on surface and subsurface reconnaissance: Am. Soc. Testing Materials Spec. Tech. Pub. no. 122, p. 46–56.

Gross, W. H., 1951, A statistical study of topographic linears and bedrock structures: Geol. Assoc. Canada Proc., v. 4, p. 77–87.

Gwynne, C. S., 1942, Swell and swale pattern of the Mankato Lobe of the Wisconsin drift plain in Iowa: Jour. Geology, v. 50, no. 2, p. 200–208.

Hackman, R. J., 1956a, The graphic construction of controlled stereoscopic models: Photogramm. Eng., v. 22, no. 2, p. 387–391.

——— 1956b, The stereo-slope comparator—an instrument for measuring angles of slope in stereoscopic models: Photogramm. Eng., v. 22, no. 5, p. 893–898.

——— 1957, The "Flying Carpet"—a stereoscopic grid used in photo interpretation: Photogramm. Eng., v. 23, no. 3, p. 593–594.

Hackman, R. J., and Tolbert, G. E., 1955, Photogeologic map, Notom-15 quadrangle, Garfield County, Utah: U.S. Geol. Survey Misc. Geol. Inv. Map I–34.

Hemming, H., 1937, Air survey as a factor in empire development: Mine and Quarry Eng., v. 2, no. 7, p. 254–263.

Hemphill, W. R., 1958a, Determination of quantitative geologic data with stereometer-type instruments: U.S. Geol. Survey Bull. 1043–C, p. 35–56.

——— 1958b, Small-scale photographs in photogeologic interpretation: Photogramm. Eng., v. 24, no. 4, p. 562–567.

Henderson, L. H., 1939, Detailed geological mapping and fault studies of the San Jacinto tunnel line and vicinity: Jour. Geology, v. 47, no. 3, p. 314–324.

Hittle, J. E., 1949, Air photo interpretation of engineering sites and materials: Photogramm. Eng., v. 15, no. 4, p. 589–603.

Hopkins, D. M., Karlstrom, T. N. V., and others, 1955, Permafrost and ground water in Alaska: U.S. Geol. Survey Prof. Paper 264–F, p. 113–146.

Horton, R. E., 1945, Erosional development of streams and their drainage basins: Hydrophysical approach to quantitative morphology: Geol. Soc. America Bull., v. 56, p. 275–370.

Howard, W. V., 1940, Aerial photographic surveys valuable on Gulf Coast: Oil and Gas Jour., v. 38, no. 50, p. 194–195.

Howe, R. H. L., 1958, Procedures of applying air photo interpretation in the location of ground water: Photogramm. Eng., v. 24, no. 1, p. 35–49.

Jenkins, D. S., Belcher, D. J., Greeg, L. E., and Woods, K. B., 1946, The origin, distribution and airphoto identification of United States soils: U.S. Civil Aeronautics Adm. Tech. Devel. Rept. no. 52, 202 p.

Johnstone, W. E., 1953, Photogeology and mineral exploration: Mining Mag., v. 88, no. 5, p. 265–270.

Joliffe, A. W., 1945, Aeroprospecting in the Yellowknife area: Canadian Inst. Mining and Metallurgy Trans., v. 48, p. 588–609.

Kelsh, H. T., 1952, Radial triangulation, *in* Am. Soc. Photogrammetry, Manual of Photogrammetry: 2d ed., Washington, D.C., p. 409–447.

Kent, B. H., 1957, Experiments in the use of color aerial photographs for geologic study: Photogramm. Eng., v. 23, no. 5, p. 865–868.

Kinoshita, W. T., and Kent, B. H., 1960, Photogrammetric determinations of elevations for regional gravity surveys: Geophysics, v. 25, no. 2, p. 445–450.

Krumbein, W. C., 1950, Geological aspects of beach engineering, *in* Application of geology to engineering practice: Geol. Soc. America Berkey Volume, p. 195–220.

Lattman, L. H., 1954, The one-sided development of tributaries in tilted sedimentary rocks in eastern Allegheny Plateau of West Virginia: Michigan Acad. Sci., Arts, and Letters, Papers, v. 39, p. 361–365.

——— 1958, Technique of mapping geologic fracture traces and lineaments on aerial photographs: Photogramm. Eng., v. 24, no. 4, p. 568–576.

Lattman, L. H., and Nickelsen, R. P., 1958, Photogeologic fracture-trace mapping in Appalachian Plateau: Am. Assoc. Petroleum Geologists Bull., v. 42, no. 9, p. 2238–2245.

Lattman, L. H., and Olive, W. W., 1955, Solution widened joints in Trans-Pecos, Texas: Am. Assoc. Petroleum Geologists Bull., v. 39, no. 10, p. 2084–2087.

Levings, W. S., 1944, Aerogeology in mineral exploration: Colorado School Mines Quart., v. 39, no. 4, 77 p.

Levings, W. S., and Herness, S., 1953, Air photo criteria of ore localization in Corbin-Wickes mining district, Jefferson County, Montana: Photogramm. Eng., v. 19, no. 3, p. 450–460.

Liang, Ta., and Belcher, D. J., 1958, Airphoto interpretation, *in* Landslides and engineering practice: Natl. Research Council, Highway Research Board Spec. Rept. no. 29, p. 69–92.

Loel, Wayne, 1941, Use of aerial photographs in geologic mapping: Am. Inst. Mining Metall. Eng. Trans., v. 144, p. 356–409.

Lueder, D. R., 1951, The preparation of an engineering soil map of New Jersey, *in* Symposium on surface and subsurface reconnaissance: Am. Soc. Testing Materials Spec. Tech. Pub. no. 122, p. 73–81.

——— 1953, Airphoto interpretation as an aid in mineral reconnaissance and development: Photogramm. Eng., v. 19, no. 5, p. 819–830.

Marshall, C. H., and Rosendale, A. B., 1953, Structure of the Discovery anticline: U.S. Geol. Survey open-file rept.

McNeil, G. T., 1952, Map compilation with stereometer-type instruments, *in* Am. Soc. Photogrammetry, Manual of Photogrammetry: 2d ed., Washington, D.C., p. 603–622.

Melton, F. A., 1956, Problems of the photogeologist in "flatland" regions of low dip: Photogramm. Eng., v. 22, no. 1, p. 52–63.

Miller, V. C., 1953, Some factors causing vertical exaggeration and slope distortion on aerial photographs: Photogramm. Eng., v. 19, no. 4, p. 592–607.

Minard, J. P., 1960, Color aerial photographs facilitate geologic mapping on the Atlantic Coastal Plain of New Jersey: Photogramm. Eng., v. 26, no. 1, p. 112–116.

Mogg, A. O. D., 1930, A preliminary account of the flora of Pretoria in relation to geology: Internat. Geol. Cong., 15th, South Africa 1929, Compte Rendus, p. 651–669.

Mollard, J. D., 1947, Airphoto mapping of Montgomery County soils for engineering purposes, *in* Purdue Univ. 33d Ann. Road School Proc.: Purdue Univ. Eng. Bull., Ext. Ser. no. 63, p. 223–226.

Muller, S., 1947, Permafrost, or permanently frozen ground, and related engineering problems: Ann Arbor, Mich., J. W. Edwards, Inc., 231 p.

Munk, W. H., and Traylor, M. A., 1947, Refraction of ocean waves—a process linking underwater topography to beach erosion: Jour. Geology, v. 55, no. 1, p. 1–26.

Murray, A. N., 1955, Growing vegetation identifies formations: World Oil, v. 141, no. 1, p. 102–104.

Parvis, M., 1947, Regional drainage patterns of Indiana, *in* Purdue Univ. 33d Ann. Road School Proc.: Purdue Univ. Eng. Bull., Ext. Ser. no. 63, p. 192–222.

Parvis, M., 1950, Drainage pattern significance in airphoto identification of soils and bedrocks: Photogramm. Eng., v. 16, no. 3, p. 387–409.

Petrusevich, M. N., 1954, Geological surveying and reconnaissance based on photogeologic methods [in Russian]: Moscow, 108 p.

Petrusevich, M. N., and Kazik, L. I., 1955, Aerial color photography in geological mapping: Soviet Geol. no. 42, 7 p. (translated by Associated Technical Services).

Pillmore, C. L., 1957, Application of high-order stereoscopic plotting instruments to photogeologic studies: U.S. Geol. Survey Bull. 1043–B, p. 23–34.

Purdue University, 1953, A manual on the airphoto interpretation of soils and rocks for engineering purposes: Purdue Univ., School of Civil Engineering and Engineering Mechanics.

Putnam, W. C., 1947, Aerial photographs in geology: Photogramm. Eng., v. 13, no. 4, p. 557–565.

Raup, H. M., and Denny, C. S., 1950, Photo interpretation of the vegetation along the southern part of the Alaska Highway: U.S. Geol. Survey Bull. 963–D, p. 95–135.

Ray, R. G., 1956, Photogeologic procedures in geologic interpretation and mapping: U.S. Survey Bull. 1043–A, p. 1–21.

——— 1958, Color aerial photography: Western Miner and Oil Rev., v. 31, no. 3, p. 35–37.

Ray, R. G., and Fischer, W. A., 1960, Quantitative photography—a geologic research tool: Photogramm. Eng., v. 26, no. 1, p. 143–150.

Reed, J. C., 1940, The use of airplane photographs in the geologic study of the Chichagof Mining District, Alaska: Photogramm. Eng., v. 6, no. 1, p. 35–44.

Rich, J. L., 1951, Geomorphology as a tool for the interpretation of geology and earth history: New York Acad. Sci. Trans., Ser. 2, v. 13, no. 6, p. 188–192.

Ritchie, A. M., 1958, Recognition and identification of landslides, *in* Landslides and engineering practice: Natl. Research Council, Highway Research Board Spec. Rept. no. 29, p. 48–68.

Robinson, T. W., 1958, Phreatophytes: U.S. Geol. Survey Water-Supply Paper 1423, 84 p.

Sager, R. C., 1951, Aerial analysis of permanently frozen ground: Photogramm. Eng., v. 17, no. 4, p. 551–571.

Scher, M. B., 1955, Stereotemplet triangulation: Photogramm. Eng., v. 21, no. 5, p. 655–664.

Schulte, O. W., 1951, The use of panchromatic, infrared and color aerial photography in the study of plant distribution: Photogramm. Eng., v. 17, no. 5, p. 688–714.

Schultz, J. R., and Cleaves, A. B., 1955, Geology in engineering: New York, John Wiley and Sons, Inc., 592 p.

Smit Sibinga, G. L., 1948, On the geomorphic and geologic analysis and interpretation of aerial photographs: Koninkl. Nederlandsch Aardrijksk. Genootschap Tijdschr., p. 692–700.

Smith, H. T. U., 1943a, Aids in teaching photogrammetry: Photogramm. Eng., v. 9, no. 3, p. 167–171.

——— 1943b, Aerial photographs and their interpretation: New York, Appleton-Century-Crofts, Inc., 372 p.

——— 1953, Photo interpretation of terrain, *in* Selected papers on photogeology and photo interpretation: U.S. Research and Devel. Board, Washington, D.C., p. 7–53.

Smith, K. G., 1950, Standards for grading texture of erosional topography: Am. Jour. Sci., v. 248, p. 655–668.

Spurr, S. H., 1948, Aerial photographs in forestry: New York, Ronald Press Co., 340 p.

Spurr, S. H., and Brown, C. T., Jr., 1945, The multiscope—a simple stereoscopic plotter: Photogramm. Eng., v. 21, no. 3, p. 171–178.

Stoeckeler, E. G., 1952, Trees of interior Alaska, their significance as soil and permafrost indicators, *in* Investigations of military construction in Arctic and Subarctic regions: St. Paul District, U.S. Corps of Engineers, 25 p.

Stone, Kirk, 1951, Geographical air-photo-interpretation: Photogramm. Eng., v. 17, no. 5, p. 754–759.

——— 1956, Air photo interpretation procedures: Photogramm. Eng., v. 22, no. 1, p. 123–132.

Summerson, C. H., 1954, A philosophy for photo interpreters: Photogramm. Eng., v. 20, no. 3, p. 396–397.

Tator, B. A., 1951, Some applications of aerial photographs to geographical studies in the Gulf Coast regions: Photogramm. Eng., v. 17, no. 5, p. 716–725.

——— 1954, Drainage anomalies in coastal plains regions: Photogramm. Eng., v. 20, no. 3, p. 412–417.

Tewinkel, G. C., 1952, Basic mathematics of photogrammetry, *in* Am. Soc. Photogrammetry, Manual of Photogrammetry: 2d ed., Washington, D.C., p. 309–380.

Thompson, M. M., 1958, Photogrammetric mapping of sand beds in a hydraulic test flume: Photogramm. Eng., v. 24, no. 3, p. 468–475.

Thornburn, T. H., 1951, The preparation of soil-engineering maps from agricultural reports: Natl. Research Council, Highway Research Board Bull. no. 46, p. 87–95.

Thurrell, R. F., Jr., 1953, Vertical exaggeration in stereoscopic models: Photogramm. Eng., v. 19, no. 4, p. 579–588.

Treece, W. A., 1955, Estimation of vertical exaggeration in stereoscopic viewing of aerial photographs: Photogramm. Eng., v. 21, no. 4, p. 518–527.

Turner, F. J., 1952, "Gefügerelief" illustrated by "schist tor" topography in central Otago, New Zealand: Am. Jour. Sci., v. 250, no. 11, p. 802–807.

Turner, S. F., and Skibitzke, H. E., 1952, Use of water by phreatophytes in 2000-foot channel between Granite Reef and Gillespie Dams, Maricopa County, Arizona: Am. Geophys. Union Trans., v. 33, no. 1, p. 66–72.

Twenhofel, W. S., and Sainsbury, C. L., 1958, Fault patterns in southeastern Alaska: Geol. Soc. America Bull., v. 69, no. 11, p. 1431–1442.

[U.S.] Beach Erosion Board, 1946, Beach erosion study—Lake Michigan shore line of Milwaukee County, Wis.: U.S. 79th Cong., 2d sess., House Doc. 526.

Visser, J., 1954, The construction of the datum-correction graph for map compilation with stereometer-type instruments: Photogramm. Eng., v. 20, no. 5, p. 849–853.

Walker, G. L., 1929, Surveying from the air in central Africa: Eng. Mining Jour., v. 127, no. 2, p. 49–52.

Wallace, R. E., 1950, Determination of dip and strike by indirect observations in the field and from aerial photographs: Jour. Geology, v. 58, no. 3, p. 269–280.

Wengerd, S. A., 1947, Geologic interpretation of trimetrogon photographs—northern Alaska: Photogramm. Eng., v. 13, no. 4, p. 586–600.

Wheeler, R. R., and Smith, N. C., 1952, Finding faded structures: World Oil, v. 135, no. 1, p. 73–74, 76, 82; v. 135, no. 2, p. 105–106, 108, 110, 112.

Willett, R. W., 1940, The Invincible quartz Lode: New Zealand Jour. Sci. and Technology, v. 21, Sec. B, p. 273B–280B.

Wilson, R. C., 1949, The relief displacement factor in forest area estimates by dot-templets on aerial photographs: Photogramm. Eng., v. 15, no. 2, p. 225–236.

Witkind, I. J., Hemphill, W. R., Pillmore, C. L., and Morris, R. H., 1960, Isopach mapping by photogeologic methods as an aid in the location of swales and channels in the Monument Valley area, Arizona: U.S. Geol. Survey Bull. 1043–D. (In press)

Woods, K. B., Hittle, J. E., and Frost, R. E., 1948, Use of aerial photographs in the correlation between permafrost and soils: Military Engineer, v. 40, no. 277, p. 497–499.

Woolnough, W. G., 1934a, notes on the technique of aerial photographic survey for geological purposes in Australia: World Petroleum Cong., 1st, London 1933, Proc., v. 1, p. 210–219.

——— 1934b, Results of experimental aerial survey with special reference to oil prospecting: World Petroleum Cong., 1st, London 1933, Proc., v. 1, p. 220–229.

Zonneveld, J. I. S., and Cohen, A., 1952, Geological reconnaissance, *in* The use of aerial photographs in a tropical country (Surinam): Photogramm. Eng., v. 18, no. 1, p. 151–157.

INDEX

A

Page

Accuracy, in horizontal positioning 74–75
in vertical measurement 72–74
Altitude, determining differences of 53–54, 56
See also Flying height.
Anaglyph principle 45, 47
Annular drainge. *See* Drainage, pattern.
Anomaly, in drainage 26–27
in photographic tone 29
Anticline. *See* Folds.
Association of features 11–12
Automatic dodging. *See* Photographs, printing of.

B

Base-height ratio 14
Beach erosion 39
Beaded drainage 38
Bedding 16, 19, 26
Botanical guides 32–33

C

Cleavage 24
Climate, relation of soils to 15
Color, negative-type film 8
recognition element 8–9, 31, 36
transparencies 8, 31
Contours. *See* Structure contouring.
Contrast. *See* Photographs, printing of.
Control net or layout 67

D

Dendritic drainage. *See* Drainage, pattern.
Density, drainage 9
film 7
See also Drainage, texture.
Diapositives 45–47
Difference in altitude, methods of determining 50–54, 56
Dipping beds, effect of vertical exaggeration 13–14, 64
estimation of dip 64
measure of dip 54, 56–57, 63–64
Dipping platen ..... 63; fig. 32
Displacement, on faults 61
See also Radial displacement.
Dodging. *See* Photographs, printing of.
Double-projection instruments 45–48
Drainage, anomaly 26–27
beaded 38
pattern 11, 18, 19, 26, 27
texture 9, 16, 17, 26, 34–35
tributary-length relations 19

E

Effective focal length 4
Elements of soil pattern 34–37
Engineering geology, interpretation of aerial photographs in 33–40
Engineering soil maps 33
Enlargement, of double-projection stereoscopic model 47–48
of paper prints 4, 54
ER–55 plotter ..... 46, 47; fig. 17
Exaggerated-profile plotter ..... 48; figs. 19, 20
Exaggeration. *See* Vertical exaggeration.
Exaggeration factor 64
Extrusive rocks. *See* Igneous rocks.

F

Page

Facies 30, 59–60
Faults, measuring displacement on 61
recognition 21, 29
Film and filters, effect on photographic image 4
panchromatic film-minus blue filter 4
Flat-lying beds 19
Floating dot 41, 47
Floating line 57–58, 64
Flying height 2, 4, 53–54
relation to radial displacement 75
relation to scale 2, 4, 53
relation to vertical exaggeration 14
Focal length, effective 4
relation to radial displacement 4
relation to scale and flying height 2, 4
relation to vertical exaggeration 14
Folds 19, 21, 26
Foliation. *See* Cleavage.
Formulas, for determining differences in altitude 53, 56
for determining feet-equivalent of parallax measurements 54, 55, 72, 73
for determining radial displacement 75
for determining scale 2, 4
for determining stratigraphic thickness of inclined beds ..... figs. 26, 27, 28
Fractures. *See* Faults; Joints.

G

Gradient. *See* Stream gradient.
Granular materials 33, 34, 35
Gridded base map ..... 69; fig. 116
Gridded photograph ..... 69; fig. 115
Ground conditions 33–39
Ground water 40

H

Height, flying. *See* Flying height; *also* Difference in altitude.
Horizontal position, accuracy of plotting 74–75
correction for 56–57
Hydrology, photogrammetric applications in 40–41
use of aerial photographs in 40–41

I

Igneous rocks, extrusive 17
intrusive 17–18
Instrument capability 72–74
See specific instruments.
Interpretation, defined 5
Interval measuring device ..... 48; fig. 21
Intrusive rocks. *See* Igneous rocks.
Isopach mapping 58–59

J

Joints 16, 18, 19, 23–24

K

KEK plotter 45
Kelsh plotter ..... 47; fig. 18
K factor ..... 54–55, 72–74; fig. 37

L

Landform 6, 12–13, 17, 34
Landslides 39
Land use 37
Layout. *See* Control net.
Lens angle, relation to parallax measurement 4
relation to radial displacement 4
Lineations 21, 29, 30–31
Lithologic guides 31

Page

Lithology. *See* Igneous rocks; Metamorphic rocks; Sedimentary rocks.

M

Mahan plotter 45
Measurement, vertical. *See* Parallax.
Metamorphic rocks 16, 18–19
Multiplex plotter ..... 47; fig. 16
Multiscope 42, 45

O

Ore deposits, interpretation of aerial photographs in search for 30–33
Orientation of photographs ..... 52; fig. 25
need for correct orientation 54
Orthophotographs 69
Overhead projectors 67, 68
Overlay, drainage 19
in correcting horizontal position 56

P

Parallax, formulas 53
geologic uses of 56–63
measure of 50–55
Parallax bar. *See* Stereometer.
Parallax ladder ..... 41–42; fig. 12
Pattern, drainage 11, 26, 27
lines 9, 11, 29
soils 11, 29
vegetation 11
See also Elements of soil pattern.
Permafrost 37–39
Permeability 16, 34–35
Petroleum geology, interpretation of aerial photographs in 24–30
Photogrammetric systems 69–72
Photographic tone 6–8, 16, 35–36
Photographs, geometry of ..... fig. 1
printing of 7
scale 2, 4
twin low-oblique 2, 4
Physiographic guides 31–32
Physiography. *See* Landform.
Pingos 38
Platen 47
Plotting, in cross section 69
orthographic 67–68, 69
Plutonic rocks. *See* Igneous rocks.
Polygonal microrelief 37–38
Pseudoscopic view ..... 5; fig. 95

R

Radial displacement, correction for 56, 68
measure of 56, 74–75
use in determining heights 56
Radial drainage. *See* Drainage, pattern.
Radial planimetric plotter ..... 42; fig. 14
Recognition elements 6–13
Reflectance. *See* Photographic tone; Spectral reflectance.
Relief displacement. *See* Radial displacement.

S

Scale of photographs, relation to focal length and flying height 2, 4
relation to parallax measurements 4, 74
significance in interpretation 11–12, 14, 21
Sedimentary rocks 15, 16–17
Shadows 13

Page

Shape ... 12–13, 34, 35
Size ... 13
Sketchmaster ... 42; fig. 13
Slope, direct determination of ... 63–64
  measurement by parallax method ... 54, 56–57
Soils, permeability ... 34–35
  transported, landform of ... 34
Spectral reflectance ... 7–8
Stereometer ... 41; fig. 10
Stereo slope comparator ... 63; fig. 33
Stereo slope meter ... 42; fig. 11
Stereotemplets ... 67
Stereotope ... 45; fig. 15
Stratigraphic thickness, determination of ... 57–58
Stream gradient, determination of ... 63
  use in detecting tilt ... 55
Structure ... 19–24
Structure contouring ... 60–62
Structural guides ... 30–31
Surficial materials ... 17, 33
Syncline. *See* Folds.

T

Templets ... 67
Texture, drainage ... 9, 17, 26–27, 34–35
  photographic ... 9
  soil ... 9
  topographic ... 9
Thaw lakes ... 38
Tilt ... 55
Tone. *See* Photographic tone.
Topography, significance in delineating structure ... 19, 21, 24, 27, 29
  See also Landform; Shape.
Trellis drainage. *See* Drainage, pattern.
Twin low-oblique photography. *See* Photographs.

U

Unconformity ... 24
Universal tracing table ... 48, 55; fig. 22

V

Page

Vegetation, as indicator of structure ... 11, 21, 23
  in interpretation of permafrost ... 37
  in interpretation of soils ... 36
  significance in search for ground water ... 40
  use in differentiating rock types ... 15, 17, 18
  See also Elements of soil pattern.
Vertical exaggeration, cause of ... 13–14
  correction for ... 63, 64
  relation to true distances and slopes ... 13–14
Vertical positioning ... 69
Viewing, methods of ... 4–5
Volcanic rocks. *See* Igneous rocks.
V factor ... 73–74

W

Water supply. *See* Ground water.
Wave length ... 4, 7–8

U.S. GOVERNMENT PRINTING OFFICE : 1960 O—553966

MHI
Copy 3

FM 21-25

WAR DEPARTMENT

BASIC FIELD MANUAL

&

ELEMENTARY MAP AND AERIAL PHOTOGRAPH READING

April 12, 1941

FM 21-25

BASIC FIELD MANUAL

ELEMENTARY MAP AND AERIAL PHOTOGRAPH READING

Prepared under direction of the
Chief of Engineers

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1941

For sale by the Superintendent of Documents, Washington, D. C.

WAR DEPARTMENT,
WASHINGTON, *April 12, 1941.*

FM 21–25, Elementary Map and Aerial Photograph Reading, is published for the information and guidance of all concerned.

[A. G. 062.11 (12–9–40).]

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
Chief of Staff.

OFFICIAL:

E. S. ADAMS,
Major General,
The Adjutant General.

DISTRIBUTION:

B and H (3); R (10); Bn (5); C (10).

TABLE OF CONTENTS

		Paragraphs	Page
SECTION I.	General	1–5	1
II.	Conventional signs and military symbols	6–7	3
III.	Map measurements	8–10	11
IV.	Direction and azimuth	11–20	15
V.	Location by coordinates	21–24	29
VI.	Elevation and relief	25–32	35
VII.	Map reading in the field	33–38	54
VIII.	Aerial photograph reading	39–48	70
APPENDIX			97
INDEX			99

BASIC FIELD MANUAL

ELEMENTARY MAP AND AERIAL PHOTOGRAPH READING

(This manual supersedes chapter 5, Basic Field Manual, volume I, April 2, 1938.)

SECTION I

GENERAL

■ 1. PURPOSE.—The purpose of this manual is to present in simplified form necessary information for instruction of all military personnel in elementary map and aerial photograph reading.

■ 2. SCOPE.—*a.* This manual covers elementary map reading, including conventional signs and military symbols, distances and scales, directions and azimuths, coordinates, relief, slopes, profiles and visibility, map reading in the field, and aerial photograph reading to an extent sufficient to permit soldiers and platoon leaders to read aerial photographs and aerial mosaics.

b. FM 21–26 takes up the subject where this manual stops, and covers more technical phases of the subject. Other publications of a general nature pertaining to maps, mapping, and aerial photograph reading are listed in the appendix.

■ 3. NECESSITY FOR TRAINING.—Modern warfare makes it essential that personnel of all grades have the ability to read maps and aerial photographs. The detailed study of maps assists higher commanders in arriving at their tactical decisions. In transmitting orders, they often will use maps which outline their plans to their subordinate commanders. In order to carry out these orders intelligently, the subordinate commanders must be able to read any type of map involved. Maps are used to move various combat units to their assigned positions and to identify their boundaries, areas, and objectives. The supporting fires of many weapons are usually controlled by use of map data. Frequently soldiers will be given individual missions requiring them to travel long distances with only a map as a guide. Since aerial photographs or photomaps made from aerial photographs are

constantly being used as maps or to supplement maps, the necessity for training in their use is equally important as training in use of maps.

■ 4. MAPS AND AERIAL PHOTOGRAPHS.—Types of maps or aerial photographs generally issued to troops will vary a great deal depending on location of operations. Large scale topographic maps desirable for tactical operations of small units exist for only limited areas, so some of lesser accuracy normally may be expected. These may range from ordinary automobile road maps to some type of map substitute. Various types of maps and map substitutes which may be encountered are—

a. Maps compiled from existing maps.—Normally troops may expect to be furnished some type of map hastily compiled from such maps as exist at the outbreak of hostilities. These maps may vary from crude, small scale maps such as ordinary automobile road maps to accurate, large scale, topographic maps. Large scale topographic maps suitable for tactical operations of small units may be expected only in isolated areas of limited size.

b. Map substitutes.—This is a general term used to designate substitute maps that may be produced in a few hours. The map substitute may consist of direct reproduction of wide coverage aerial photographs, photomaps or mosaics, or of provisional maps. The term "photomap" is used as a general term to describe reproductions of various types of aerial photographs. A provisional map is produced by compiling existing map detail or by tracing information from aerial photographs.

c. Battle maps (fig. 1) (back of manual).—This is a map prepared normally from aerial photographs on a scale of 1:20,000, which is suitable for tactical and technical needs of all arms. Normally, this type of map would not be made available for any extensive area until at least 3 weeks after outbreak of hostilities.

■ 5. MAP CLASSIFICATION.—Military maps are generally classified according to scale as small, intermediate, medium, and large scale. (For a discussion of scales, see par. 8.) The battle map (fig. 1) referred to in paragraph 4*c*, is classed as

a large scale map. The compiled map described in paragraph 4*a* will probably be of a scale from 1:50,000 to 1:125,000, which is classed as a medium scale map. Figure 2 (back of manual) is an example of a medium scale map. Small and intermediate scale maps are used by staffs of larger units and seldom will concern commanders of small units.

SECTION II

CONVENTIONAL SIGNS AND MILITARY SYMBOLS

■ 6. CONVENTIONAL SIGNS.—*a.* Map makers have devised a common set of signs which to the map reader have a definite meaning. For instance, there are signs for a house, for a road, for a bridge, etc. These are called conventional signs. Some of them look enough like the object they are intended to represent to be easily recognized such as conventional signs for lakes or bridges. The meanings of some are not so obvious and must be learned just as new words are learned. Complete lists of conventional signs authorized for use on military maps are published in FM 21–30. Figure 3 shows some of those most commonly used.

b. Conventional signs vary in size with the scale of maps. On small scale maps comparatively few objects can be shown and the signs are reduced to their most elementary form. As the scale is increased more objects can be represented.

c. Locations of some objects are shown with more accuracy than others due to manner in which the topographer and map draftsman work. Some of these in order of accuracy are—

(1) Triangulation stations.
(2) Surveying monuments.
(3) Railroads and canals.
(4) Important bridges.
(5) Main roads.
(6) Isolated buildings on main roads, including churches and schoolhouses.
(7) Secondary roads.
(8) Streams, contours, and woodlands, cleared areas, etc.

In choosing landmarks for determining location, these relative values should be kept in mind.

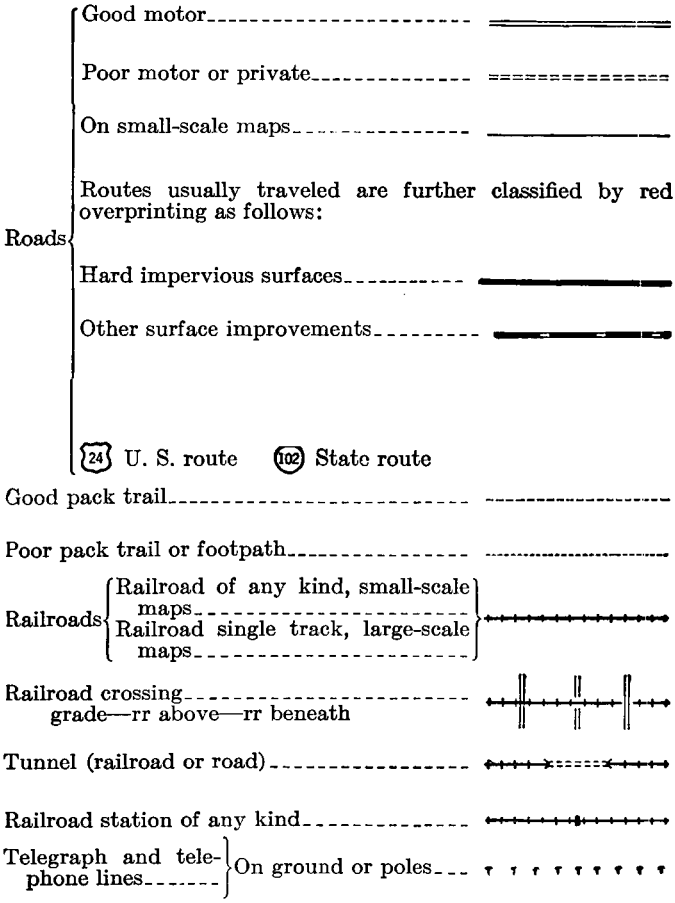


FIGURE 3.—Conventional signs.

Electric power transmission line

Bridges
- General symbol (capacity in tons indicated by figures)
- Foot
- Ponton

Ferries

Fords
- General symbol (for vehicles)
- Equestrian

Dam

Buildings in general

Church

Hospital

Schoolhouse

Cemetery — CEM or

Mine or quarry of any kind (or open cut)

Fences
- Stone
- Worm
- Wire — Barbed, Smooth
- Hedge (Printed in green.)

FIGURE 3.—Conventional signs—Continued.

Triangulation point or primary traverse station

Permanent bench mark (and elevation) BM X 1232

Streams in general (Printed in blue.)

Intermittent streams (Printed in blue.)

Spring (Printed in blue.)

Wells and water tanks (Printed in blue.)

Depression contours (Printed in brown.)

Cuts (Printed in brown.)

Fills (Printed in brown.)

Marsh in general (interior salt marshes and coastal fresh marshes are to be indicated as such) (Printed in blue.)

Woodland (or as shown below) (Printed in green.)

Woodland (or broad-leaved trees) (Printed in green.)

Orchard (Printed in green.)

FIGURE 3.—Conventional signs—Continued.

d. When colors are used for War Department maps, they are used as follows: black for works of man and for grid lines; brown for contours, cuts, and fills; blue for water; green for woods and vegetation; red to indicate road conditions.

■ 7. MILITARY SYMBOLS.—Conventional signs indicate various types of terrain feaures. Military symbols have been developed to represent various types of military organizations, activities, and installations. FM 21–30 lists various standardized military symbols. Figure 4 shows some of those most frequently used. These symbols are used to indicate size and identity of various units and installations, type and location of supporting weapons, and necessary lines and boundaries for an operation. A material saving of time in giving orders for military operations may be achieved by using military symbols to outline operations on a map or a map substitute.

1. *To indicate purpose or character of activity.*

Military post or station; command post or headquarters—

(Lower end of staff or symbol will terminate at point of establishment represented.)

Troop unit—

(On large scale maps where troop units can be shown to scale, this symbol may be modified so as to show area occupied by units in column or line, thus:

Line Column .)

Observation post—

Dump, park, or distributing point (temporary depot in combat zone)—

Supply train or transportion unit—

2. *To indicate arm or service or activity of arm or service.*—These symbols will be placed generally within the symbols shown in 1 above.

Air Corps—

Armored Force—

FIGURE 4.—Special military symbols.

Artillery ●

Cavalry /

Chemical Warfare Service G

Engineers E

Infantry (except military police) X

Military police MP

Medical Department +

Ordnance Department

Ammunition only

Prisoners of war PW

Quartermaster Corps Q

Class I supplies

Gasoline and oil only

Signal Corps S

3. *To indicate size of units.*—These symbols will be placed above the symbols shown in 1 above, or used for indicating boundaries as shown in 4 below.

Squad •

Section ••

Platoon •••

Company, troop, battery, or Air Corps flight I

Battalion, cavalry squadron, or Air Corps squadron II

Regiment or Air Corps group III

Brigade or Air Corps wing X

Division XX

Corps XXX

Army XXXX

FIGURE 4.—Special military symbols—Continued.

General headquarters ---------- GHQ

4. *To indicate boundaries.*

Squad ----------

Section ----------

Platoon ----------

Company or similar unit ----------

Battalion or similar unit ----------

Regiment or similar unit ----------

Brigade ----------

Division ----------

Front line ----------

Limit of wheeled traffic by day ---------- —DY—

Limit of wheeled traffic by night ---------- —NT—

5. *Miscellaneous.*

Area, gassed, to be avoided ---------- (RED)

Automatic rifle ----------

(Dotted when emplacement is not occupied, thus) ----------

Machine gun ----------

(Arrow to point in principal direction of fire. When used alone it indicates machine gun, water-cooled, cal. .30.)

Machine-gun symbol under symbol of unit of any arm indicates machine-gun unit of that arm.

Caliber .50 (antitank) ---------- 50 AT

Gun ----------

Gun battery ----------

Howitzer or mortar ----------

Open when emplacement is unoccupied, thus ----------

FIGURE 4.—Special military symbols—Continued.

37-mm gun (AT or AA to be added where applicable.) 37-mm

81-mm mortar 81-mm

Machine gun (single gun)

(Arrows to indicate sectors of fire, shaded portion to show danger space when fire is placed in final protective line.)

Machine-gun section (two guns)

Message center

Tank trap

Traffic:

One-way

Two-way

Trench for one squad

(For each additional squad add one traverse.)

6. *Application of special symbols.*

Light Machine-Gun Platoon, Troop A, 2d Cavalry A 2

Machine-Gun Troop, Caliber .50, 2d Cavalry 2 .50

Troop F, 2d Cavalry F 2

Company A, 2d Engineers (combat) A 2

Battery F, 2d Field Artillery F 2

One squad, Company A, 4th Infantry A 4

Light Machine-Gun Section, Company A, 2d Infantry A 2

1st Platoon, Company B, 2d Infantry 1B 2

Machine-Gun Platoon, Caliber .50, Company H, 29th Infantry 3H 29 .50

Headquarters Company, 3d Infantry HQ 3

Company D, 20th Infantry D 20

Command Post, 3d Battalion, 4th Infantry 3 4

Observation Post, 6th Infantry 6

FIGURE 4.—Special military symbols—Continued.

SECTION III

MAP MEASUREMENTS

■ 8. SCALES.—In map reading the scale of the map is a first consideration. The scale is the relation between measurements on the map and actual distances on the ground. The scale of a map is expressed in one or more of the following ways:

a. Words and figures.—Actual equivalents given in words and figures as 3 inches equal 1 mile means that 3 inches on the map equal 1 mile on the ground; 1 inch equals 200 feet means that 1 inch on the map equals 200 feet on the ground.

b. Representative fraction.—The scale of a map may be shown as a representative fraction (usually abbreviated to RF). This fraction expresses the ratio between a given distance on a map and the corresponding distance on the ground. The RF is shown thus: 1:62,500 or $\frac{1}{62,500}$ which means one unit of distance on the map equals 62,500 such units of distance on the ground. The same kind of units of distance measured from the map must be applied to distances on the ground. For instance, in the RF shown above, 1 inch on the map equals 62,500 inches (or about 1 mile) on the ground and 1 foot on the map equals 62,500 feet (or about 12 miles) on the ground. The greater the denominator the smaller the scale; a 1:20,000 map is a large-scale map, and a 1:1,000,000 is a small-scale map.

c. Graphic scales.—The figure resembling a small ruler printed on the map is also called a scale (see fig. 5). It is divided into parts, each division being marked not with its actual length but with the distance each length represents on the ground. Usually there will be one part graduated into mile units and fractions of a mile. The other part is graduated in yards for more exact measurements of ranges, frontages, and depths. Many maps also show the kilometer scale, but this normally is used only in countries where the metric system is employed. Each graphic scale consists of a primary scale to the right of zero, and an extension to the left of zero. The extension consists of one primary unit of

the graphic scale subdivided into appropriate fractions. Typical graphical scales as used on American maps can be seen on the lower margin of figure 2 (back of manual). The scale in figure 5 has 1,000-yard units for the primary scale and ten 100-yard units for the extension.

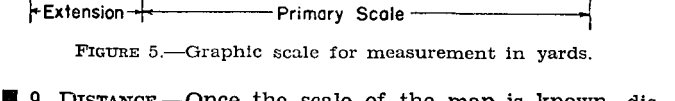


FIGURE 5.—Graphic scale for measurement in yards.

■ 9. DISTANCE.—Once the scale of the map is known, distances on the ground which are represented on the map can be determined. Even though the scale is given in words and figures or as a RF, some sort of graphic scale is usually necessary. The graphic scale is the most accurate and the most common means of determining distances from a map. Some methods of employing the graphic scale follow:

a. To find distance between two points on map (fig. 6).—(1) Lay the straight edge of a piece of paper or other material along the two points on the map. Mark the location of the two points on the straightedge by using short straight marks called "ticks" at right angles to the edge of the paper.

(2) Take the marked straightedge and place it below the graphic scale on the margin of the map to determine the ground distance required. Where the distance is greater than the length of the graphic scale, apply the primary scale one or more times until the remainder can be measured as explained above. Distances between the smallest divisions of the scale are estimated.

(3) *Example.*—(*a*) *Problem.*—Figure 6① shows a portion of a 1: 20,000 map. Required, to find actual distance on the ground between the house at A and the house at B.

(*b*) *Solution.*—Lay the straightedge of a strip of paper along A and B on the map and make tick marks. Take the strip of paper and lay its marked edge along the graphic scale on the margin of the map as shown in figure 6②. The required distance between ticks is read directly from the scale as 3,160 yards.

b. To find distance along irregular line of map.—It is sometimes necessary to measure the distance along irregular lines on a map such as a stream or a winding road. To do this, either divide the line into several approximately straight sections or, if a piece of transparent paper is available, proceed

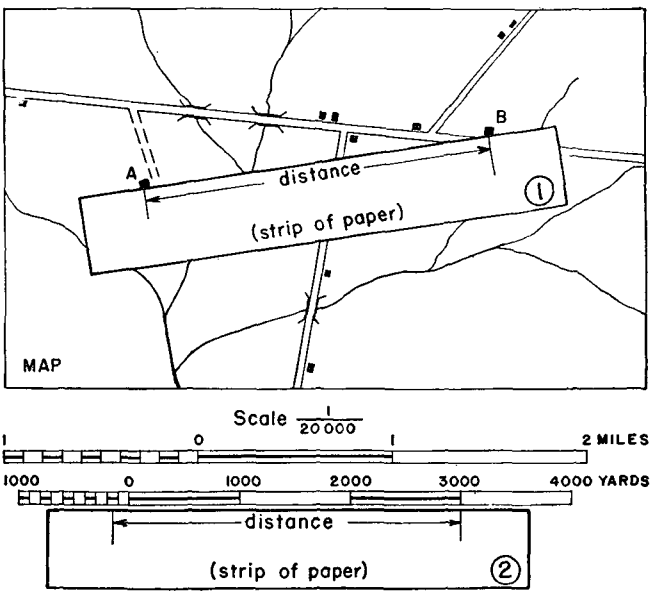


FIGURE 6.—Using graphic scale to measure distance on map.

as in (2) below. Measure the length of each section as in *a*(2) above. The sum of the lengths of the sections is the required distance.

(1) *Example.*—(*a*) *Problem.*—Required, to find distance along winding road shown in figure 7.

(*b*) *Solution.*—Take a suitable strip of paper and place it so that a tick mark along its edge coincides with A, and the edge of the paper coincides with the course A–1. Make a tick mark –1 on the paper opposite the point 1 on the map. With mark –1 on the paper held opposite 1 on the map, rotate the paper until its edge is along the line 1–2. Make

a second mark on the paper opposite 2 on the map. Continue this until B is reached; the entire distance is measured as in *a* above.

(2) *Example.*—This method also describes how to measure the distance A–B on figure 7. By means of a straightedge and a sharp pencil draw a long straight line generally down the center of any transparent piece of paper. For a starting point, draw a straight line (tick) perpendicular to and near one end of the first line. Lay the paper on the road with the starting tick over A so that the long line extends through 1. Place the pencil point at 1 and pivot the paper until the long line lies along the course 1–2. Place the pencil point at 2 and pivot the paper as before. Continue until

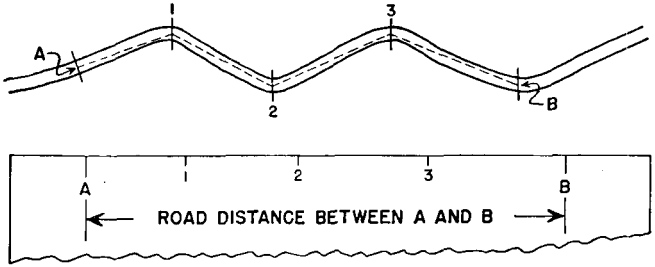


FIGURE 7.—Measuring distance along winding road.

the long line lies along course 3–B. Mark the position of B by a tick on the long line. Measure the distance along the graphic scale as described above.

■ 10. TIME.—*a. Conversion of march time to distance.*—It will often be necessary to determine the distance a column can march in a given period of time. The distance is the product of the time in hours multiplied by the hourly rate of march. For example, a motorized unit averaging 30 miles per hour can cover $4 \times 30 = 120$ miles in 4 hours. This whole distance is plotted on the edge of a strip of paper by means of the mile graphic scale. Then the distance may be laid off along the straight portions of the road by marking ticks for each change of direction along the measured portion of the strip of paper, reversing the methods shown in para-

graph 9. Thus the position of the head of the column at the end of any given time may be determined.

b. Conversion of distance to march time.—To determine how long it will take to move troops from one point to another, the distance between the two points is taken as above from any suitable map. The distance divided by the hourly rate of march gives the time required to move the troops. The habitual daytime rate of march for foot troops, making allowance for customary halts, averages 2½ miles per hour. For example, the time to march foot troops a distance found to be 15 miles on the map is 15 divided by 2.5, or 6 hours.

SECTION IV

DIRECTION AND AZIMUTH

■ **11. NEED FOR DIRECTION.**—To locate objects both direction and distance are needed. For example, an object can be located by telling in what direction and how far away it is from a given point. Most persons are familiar with the established geographic terms north, south, east, and west. These are the directions that are indicated by the common military watch compass shown in figure 8.

■ **12. UNIT OF ANGULAR MEASURE.**—*a. General.*—Angles may be measured in degrees, minutes and seconds, or in mils (see fig. 9). Normally only personnel in artillery or heavy weapons units have to use the mil since their fire-control instruments are generally graduated in mils rather than degrees. Other personnel usually use degrees, minutes, and seconds.

b. Angles.—(1) *In degrees, minutes, and seconds.*—If the circumference of a circle is divided into 360 equal parts by lines drawn from the center to the circumference, the angle at the center between any two adjacent lines is one degree. There are 60 minutes in a degree, and 60 seconds in a minute. Thus—

60″ (seconds) = 1′ (minute).
60′ (minutes) = 1° (degree).
360° (degrees) = 1 circle or a circumference.

Angles are written as 137°45′23″.

(2) *In mils.*—If the circumference of a circle is divided into 6,400 equal parts by lines from the center to the circum-

ference, the angle at the center between any two adjacent lines is 1 mil. Thus an angle would be written in mils as 1,327 mils.

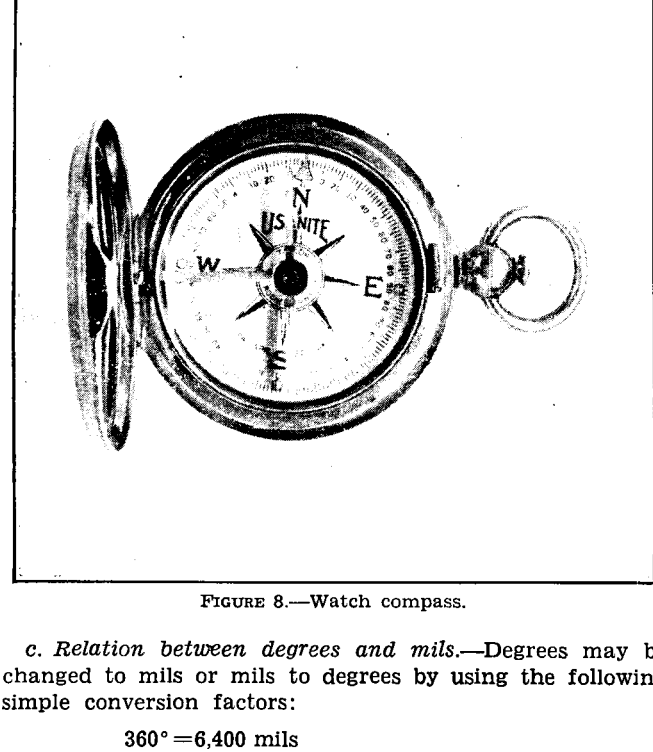


FIGURE 8.—Watch compass.

c. Relation between degrees and mils.—Degrees may be changed to mils or mils to degrees by using the following simple conversion factors:

$$360° = 6{,}400 \text{ mils}$$

$$1° = \frac{6{,}400}{360} = 17.8 \text{ mils (or 18 approximately)}$$

$$\text{Hence } 10° = 10 \times 17.8 = 178 \text{ mils (or 180 approximately)}$$

$$1 \text{ mil} = \frac{360}{6{,}400} = .056° \text{ (or 3.4′ approximately)}$$

$$\text{Hence } 100 \text{ mils} = 100 \times .056 = 5.6° \text{ or } 5°36′$$

■ 13. BASE DIRECTION.—For military purposes direction from one point to another is always expressed in terms of an angle at the initial point between the line joining the points and

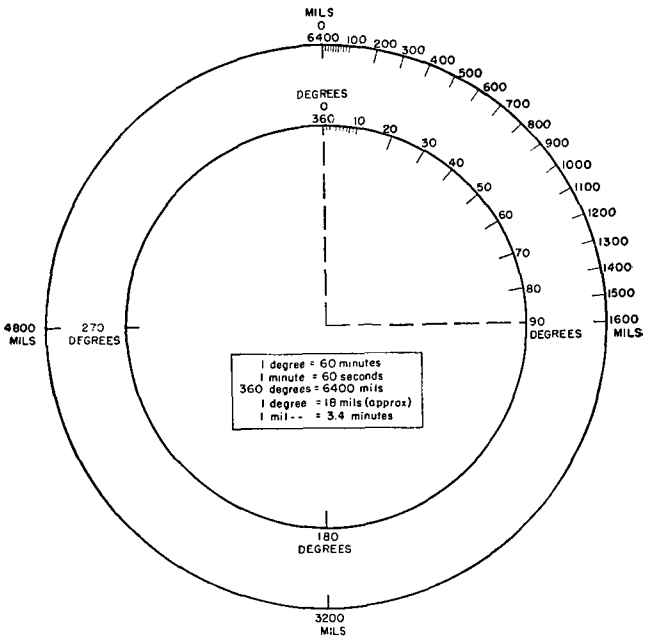
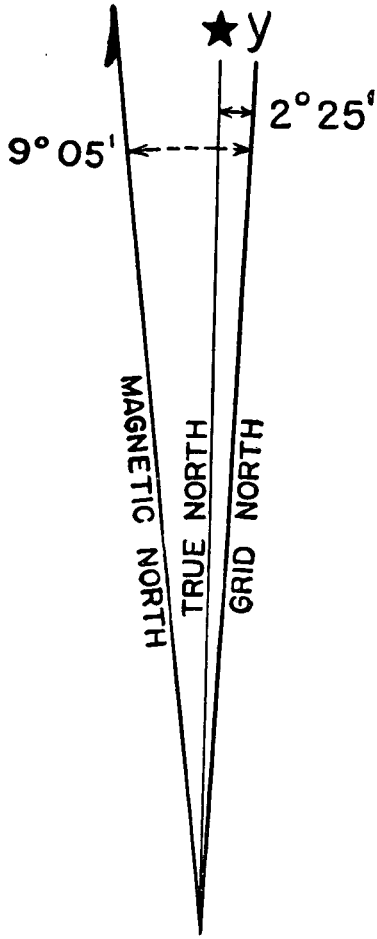


FIGURE 9.—Units of measurement.

some fixed or easily established base direction line. There are three base directions from which other directions are commonly measured, namely, true north, magnetic north, and grid north, shown on maps by a star, half arrowhead, and *y*, respectively (fig. 10).

a. True north.—The direction to the true north pole. It is used in surveying or other permanent work where great accuracy is required. Where meridian or longitude lines are shown on maps they represent true north and south directions. For ordinary military map reading in the field, true



APPROXIMATE MEAN DECLINATION 1935
ANNUAL MAGNETIC CHANGE 3' INCREASE

FIGURE 10.—Declination.

north normally will be used only as base from which declinations are computed. It normally is not used as a direction in marching by compass or orienting a map. The true north line on the declination shown in figure 10 has been purposely made very light to emphasize its relative unimportance in general map reading use.

b. Magnetic north.—The direction of the north magnetic pole. It is indicated by the N (north seeking) end of all compass needles. It is ordinarily used for field work because it can be found directly by means of the common compass.

c. Grid north.—The direction of the vertical grid lines (north-south grid lines) usually found on military maps. On maps with military grid, determination of directions from grid north is convenient because grid lines are located at frequent intervals.

■ 14. DECLINATION.—Declination is the difference in direction between true north and magnetic north or between true north and grid north. There are therefore two declinations, magnetic and grid; in figure 10, magnetic declination is 9°05′—2°25′=6°40′ and grid declination is 2°25′.

a. Magnetic.—Magnetic declination is the difference between true north and magnetic north. In some localities the compass needle points east of true north; in these localities its magnetic declination is east. In some localities the compass needle points west of true north and in these localities the magnetic declination is west. In some instances, true north and magnetic north are the same, in which case the magnetic declination is zero. The magnetic declination may vary annually by small amounts. On military maps there is usually shown in the margin a diagram of the declination with the annual change, if any. For example, in figure 10 the magnetic declination is 6°40′ west as of 1935, and the annual change is 3′ increase. In 1940 (5 years later) the magnetic declination is 6°40′ plus 5×3′ or 6°55′.

b. Grid.—Grid declination is the fixed difference in direction between true north and grid north. This declination is always the same on any given map. Grid declination reaches a maximum of 3° either east or west of true north depending on the locality. On military maps it is shown on the same

diagram as the magnetic declination. Thus in figure 10 the grid declination is 2°25′ east and there is no annual variation.

c. Use.—Figure 11 illustrates three positions of grid, magnetic, and true north. There are other possible positions. In ordinary map reading the difference in direction between grid north and magnetic north is desired rather than their difference from true north. This can be found in the three examples as follows: in figure 11① the difference between mag-

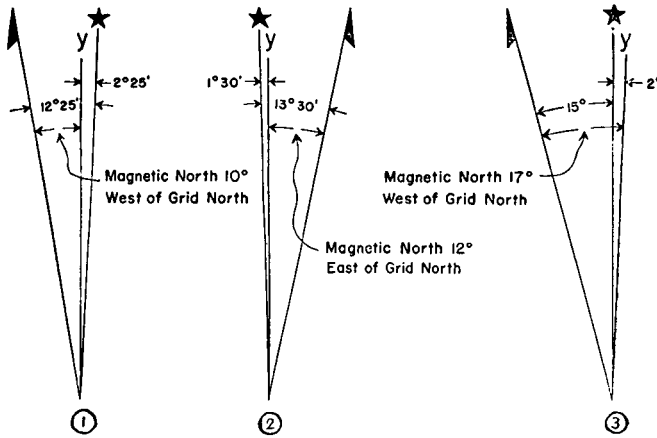


FIGURE 11.—Determining difference in direction between grid and magnetic north.

netic and grid declination is seen by inspection to be 10°0′ (12°25′—2°25′). In ② it is 12°0′ (13°30′—1°30′). In ③ it is 17°0′ (15°0′+2°0′). In the other possible positions of these lines, the declination is determined in a similar manner. When starting to use a map, determine the angle between magnetic north and grid north as described above. Write this down on the map and figure all azimuths on this basis.

■ 15. AZIMUTH.—In describing the position of one point on a map or in the field with reference to some other point, we use a standard system of measuring direction. In military work the azimuth method has been adopted for the purpose. Military azimuths are generally measured clockwise from mag-

netic, true, or grid north. Thus there are three kinds of azimuth for any given line: magnetic, true, and grid.

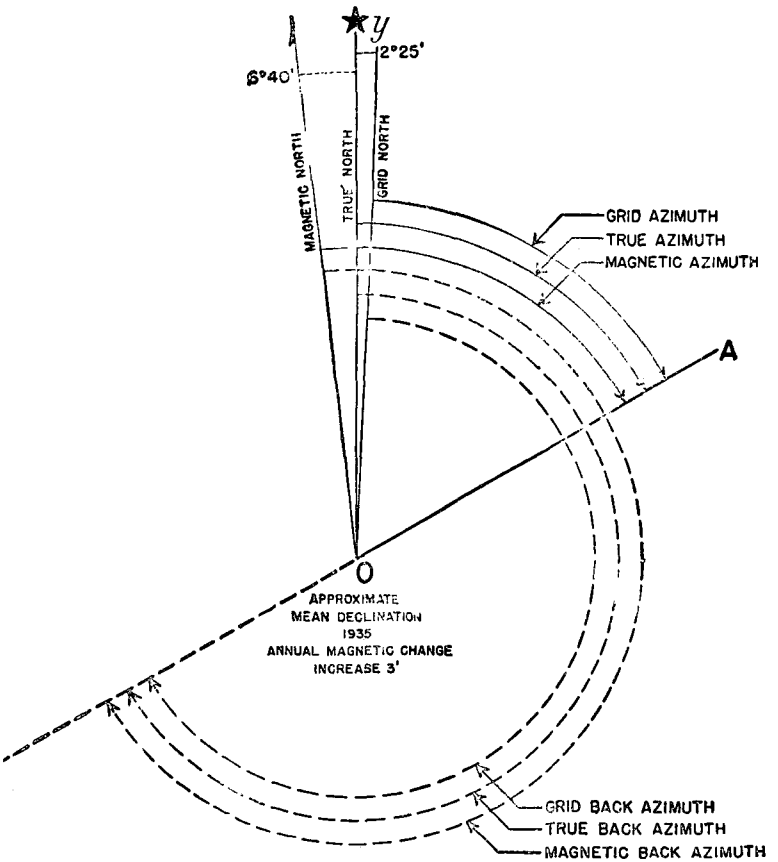


FIGURE 12.—Example of relationship between three base directions on a map, showing corresponding azimuths and back azimuths of line *OA*.

a. Magnetic.—The magnetic azimuth of any given line is the angle measured clockwise from magnetic north to the given line (fig. 12).

b. True.—The true azimuth of any given line is the angle measured clockwise from true north to the given line (fig. 12).

c. Grid.—The grid azimuth of any given line is the angle measured clockwise from grid north to the given line (fig. 12).

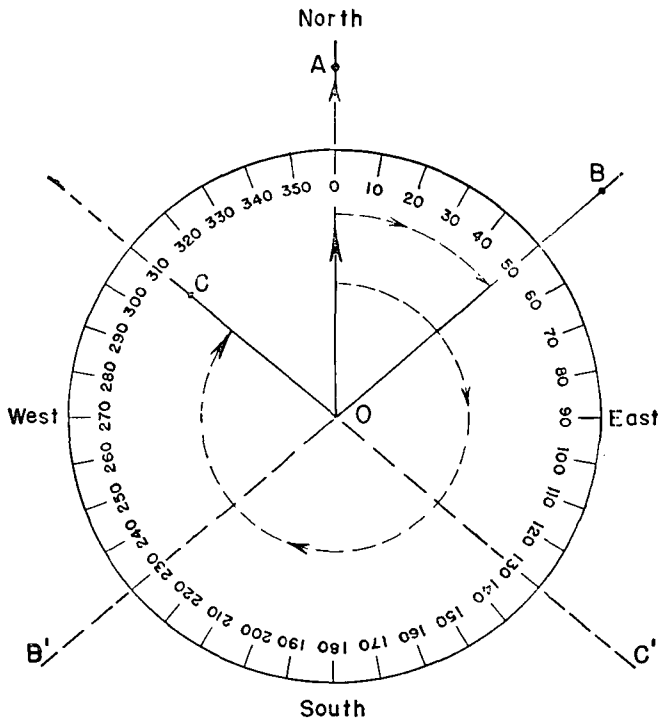


FIGURE 13.—Azimuth circle.

d. Back.—Depending on the direction in which a line extends, its azimuth may be expressed in two ways, either as forward azimuth or as back azimuth. The back azimuth of a line is its forward azimuth plus 180°. (If the sum is greater than 360°, subtract 180° from the forward azimuth to secure the back azimuth.) For example, in figure 13 the azimuth of the line extending in the direction O to B would be 50°.

The azimuth of the same line extending in the direction B to O is 50° plus 180° or 230°, which is the same as the azimuth of OB'. Similarly the forward azimuth of the line extending from O to C is 310°. Since the sum of the forward azimuth plus 180° is greater than 360°, the back azimuth or the azimuth of the line extending from C to O is 130° (310°—180°), which is the same as the azimuth of OC'. Back azimuths may be magnetic, grid, or true the same as forward azimuths and the proper designation should be included in the expression as, "Azimuth OC' 130° (magnetic)."

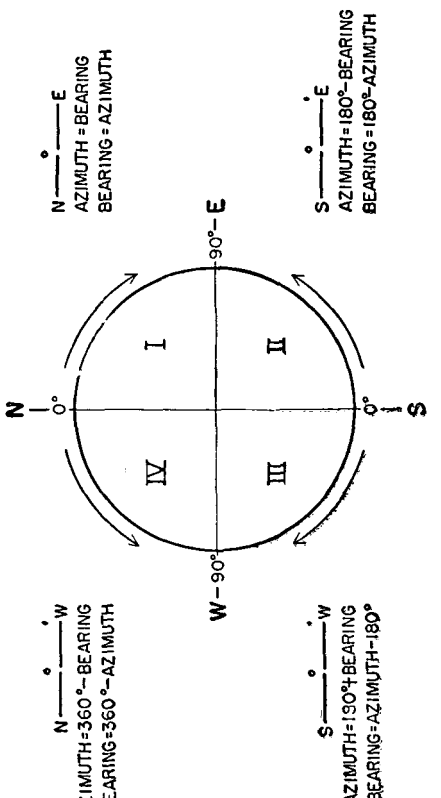


FIGURE 14.—Diagram indicating relation between bearing and azimuth.

■ 16. BEARING.—The new lensatic compass gives direction by magnetic azimuths. Watch compasses, many of which are still in use, give directions by bearings. A bearing of a

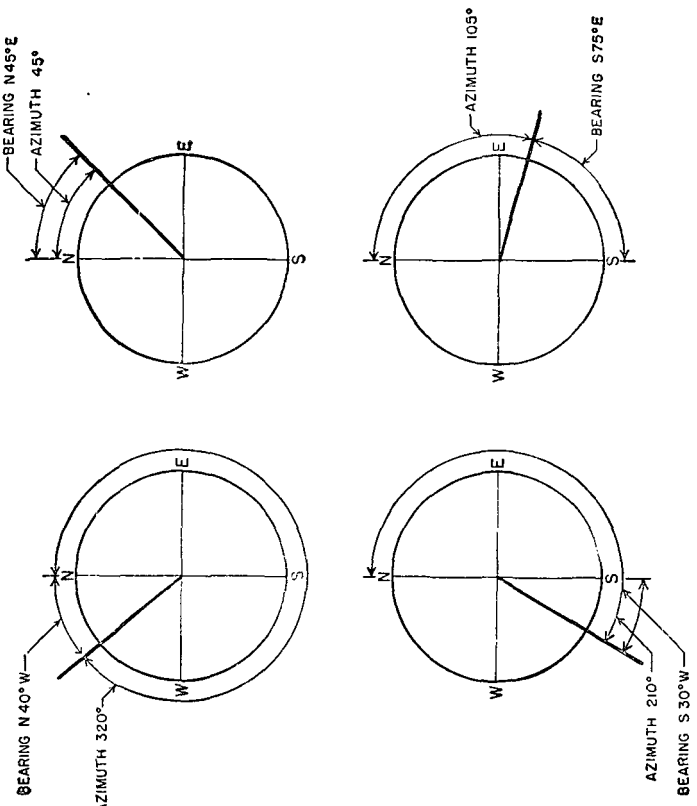
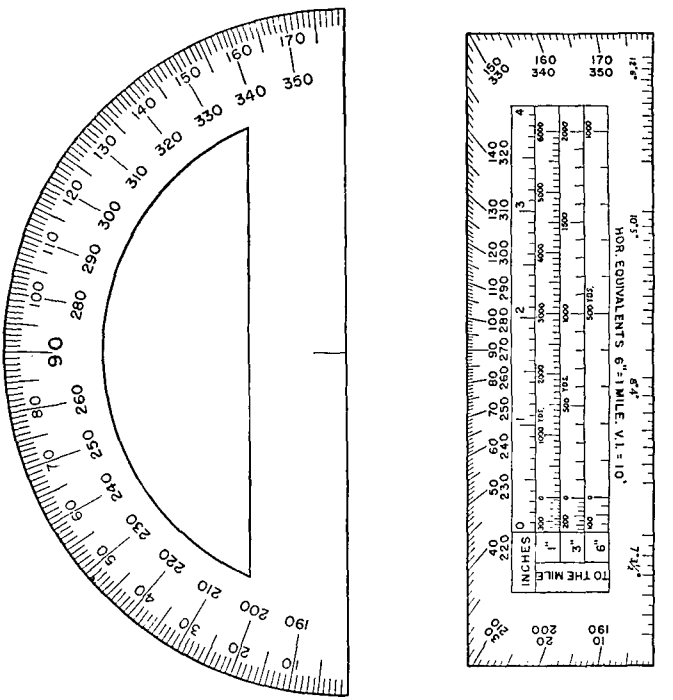


FIGURE 15.—Typical direction expressed as azimuth and as bearing.

given line is an angle and direction which the line makes with respect to a north or south direction line. Bearings are stated by quadrants (quarters of circles) and never exceed 90°. Figure 14 shows how bearings are measured and

indicates relationship between bearings and azimuths. Figure 15 illustrates the expression of a typical direction in each quadrant both as an azimuth and a bearing.

■ 17. PROTRACTOR.—Angles of azimuth or bearing are measured or laid off on a map by means of an instrument called a


INCHES
TO THE MILE
1" = 1 MILE
6" = 1 MILE
1:63,360
1:31,680
1:15,840
1:7,920
1:3,960
1:2,000
1:1,000
1:500
1:250
1:125
1:63.36
1:31.68
1:15.84
1:7.92
1:3.96
1:2.00
1:1.00
1:0.50
1:0.25
1:0.125
1:0.0634
1:0.0317
1:0.0158
1:0.0079
1:0.0040
1:0.0020
1:0.0010
1:0.0005
1:0.0003
1:0.0001
1:0.00006
1:0.00003
1:0.00002
1:0.00001
1:0.000005
1:0.000003
1:0.000001
1:0.0000005
1:0.0000003
1:0.0000001
1:0.00000005
1:0.00000003
1:0.00000001
1:0.000000005
1:0.000000003
1:0.000000001
1:0.0000000005
1:0.0000000003
1:0.0000000001
1:0.00000000005
1:0.00000000003
1:0.00000000001
1:0.000000000005
1:0.000000000003
1:0.000000000001
1:0.0000000000005
1:0.0000000000003
1:0.0000000000001
1:0.00000000000005
1:0.00000000000003
1:0.00000000000001
1:0.000000000000005
1:0.000000000000003
1:0.000000000000001
1:0.0000000000000005
1:0.0000000000000003
1:0.0000000000000001
1:0.00000000000000005
1:0.00000000000000003
1:0.00000000000000001
1:0.000000000000000005
1:0.000000000000000003
1:0.000000000000000001
1:0.0000000000000000005
1:0.0000000000000000003
1:0.0000000000000000001
1:0.00000000000000000005
1:0.00000000000000000003
1:0.00000000000000000001
1:0.000000000000000000005
1:0.000000000000000000003
1:0.000000000000000000001
1:0.0000000000000000000005
1:0.0000000000000000000003
1:0.0000000000000000000001
1:0.00000000000000000000005
1:0.00000000000000000000003
1:0.00000000000000000000001
1:0.000000000000000000000005
1:0.000000000000000000000003
1:0.000000000000000000000001
1:0.0000000000000000000000005
1:0.0000000000000000000000003
1:0.0000000000000000000000001
1:0.00000000000000000000000005
1:0.00000000000000000000000003
1:0.00000000000000000000000001
1:0.000000000000000000000000005
1:0.000000000000000000000000003
1:0.000000000000000000000000001
1:0.0000000000000000000000000005
1:0.0000000000000000000000000003
1:0.0000000000000000000000000001
1:0.00000000000000000000000000005
1:0.00000000000000000000000000003
1:0.00000000000000000000000000001
1:0.000000000000000000000000000005
1:0.000000000000000000000000000003
1:0.000000000000000000000000000001
1:0.0000000000000000000000000000005
1:0.0000000000000000000000000000003
1:0.0000000000000000000000000000001
1:0.00000000000000000000000000000005
1:0.00000000000000000000000000000003
1:0.00000000000000000000000000000001
1:0.000000000000000000000000000000005
1:0.000000000000000000000000000000003
1:0.000000000000000000000000000000001
1:0.0000000000000000000000000000000005
1:0.0000000000000000000000000000000003
1:0.0000000000000000000000000000000001
1:0.00000000000000000000000000000000005
1:0.00000000000000000000000000000000003
1:0.00000000000000000000000000000000001
1:0.000000000000000000000000000000000005
1:0.000000000000000000000000000000000003
1:0.000000000000000000000000000000000001
1:0.0000000000000000000000000000000000005
1:0.0000000000000000000000000000000000003
1:0.0000000000000000000000000000000000001
1:0.00000000000000000000000000000000000005
1:0.00000000000000000000000000000000000003
1:0.00000000000000000000000000000000000001
1:0.000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000005
1:0.00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003
1:0.00000

■ 18. To Measure Azimuth of Any Line on Map (fig. 17).—*a.* Required, to find the grid azimuth of the line from the CR (crossroads) at A to the house at B. Extend the line AB until it intersects the 349 grid line. Lay a protractor on the map with its center at this intersection and the straight portion lying along the 349 grid line. Read the grid azimuth of AB. This azimuth is seen to be 137°.

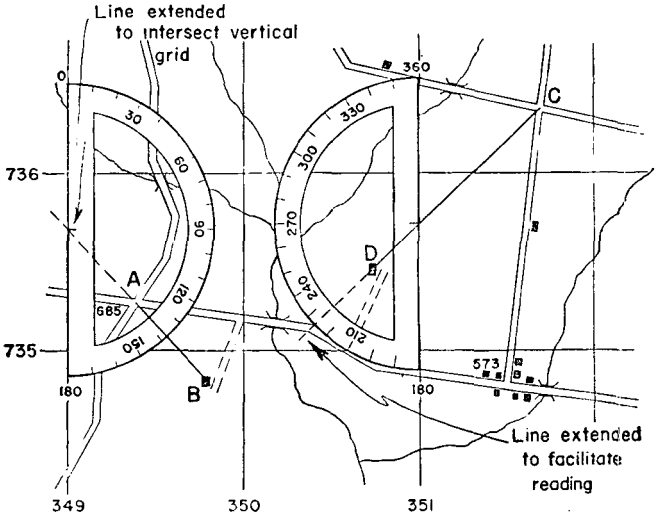
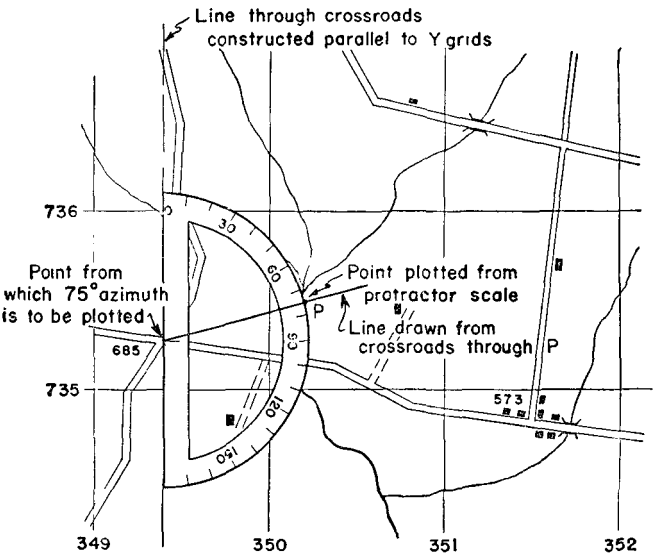


Figure 17.—Using protractor to measure map azimuth. Azimuth of line *AB* is 137°; of *CD* is 226°.

b. Required, to find the grid azimuth of the line from the CR at C to house at D. Extend the line CD a sufficient distance so that it will extend beyond the edge of the protractor. Lay the protractor on the map with its center at the intersection of CD with the 351 grid line and the straight portion lying along the 351 grid line. Since the azimuth of the line is greater than 180°, the scale reading from 180° to 360° will be used to determine the azimuth of CD. This azimuth is 226°.

■ 19. To Plot on Map Line With Given Azimuth (fig. 18).—Required, to plot from CR (crossroads) 685 a line with a grid azimuth of 75°. Construct a line through the CR parallel to the north-south grid. Lay a protractor on the map with its base on the line and its center at the CR. Plot the point P at the 75° reading on the outer scale of the protractor. Remove the protractor and draw a line from the CR through P.

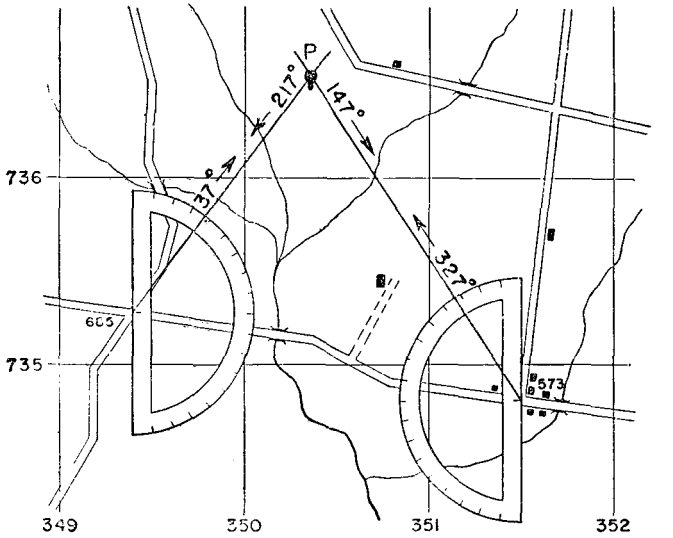


Azimuth of 75° plotted from crossroads 685.

Figure 18.—Plotting azimuths.

■ 20. Locating Point by Intersection and Resection.—*a. General.*—Sometimes it will be necessary for patrol leaders or other military personnel to determine map position of points or objects located either in enemy or other inaccessible territory. Also it may be necessary to find their own map position from inaccessible but visible points that are shown on the map. Figure 19 shows how both these operations can be accomplished.

b. Intersection.—Required, to find map position of an enemy gun that has been spotted at the point P (fig. 19) on the ground. Both CR 685 and RJ 573 are in our territory and the enemy gun is visible from both of these points. By means of a prismatic compass, the magnetic azimuth was taken from CR 685 to the gun at P. Reduced to grid azi-



Where azimuths from road junctions to gun are known, their plotting gives location of the gun. Where azimuths from gun to road junctions are known, they can be converted to back azimuth and gun position plotted as before.

FIGURE 19.—Locating points by intersection and resection.

muth, it was 37°. This grid azimuth was then plotted from CR 685 as shown. Likewise, the magnetic azimuth from RJ 573 to P was taken and reduced to grid azimuth. The grid azimuth was 327°. This azimuth was then plotted from RJ 573. The intersection of these plotted azimuths gives the map position of the gun at P which can be checked by additional similar observations. Observation points should be selected such that the plotted azimuths cross at as near

a 90° angle as possible so that the point of intersection is definite.

c. Resection (fig. 19).—(1) Required, someone at P to find map position of gun at P. This gun is in our territory but no landmarks or other easily identified terrain features are close enough to permit location from these points. However, CR 685 and RJ 573 are visible from P and are also shown on the map. The azimuths from P are read to both road intersections. These azimuths are then converted to grid back azimuths and plotted as before, giving the map position of the gun.

(2) Note that in using these two systems no measurement of distance is required. Location of position is determined merely by reading two angles and plotting two lines.

SECTION V

LOCATION BY COORDINATES

■ 21. GENERAL.—In military operations it is frequently necessary to refer to points on the ground or terrain features in short, convenient, unmistakable terms. The easiest way to accomplish this is to designate the point when given on a map by its name or number. Military maps often show names or numbers of all important locally known features. Hills, road junctions, and crossroads are often given numbers, usually in terms of their elevation in feet above sea level, thus serving the dual purpose of designating the feature and also giving its elevation. But it is not possible to number or name all features of military value on a map. Also it is often difficult to find such points on the map even when they are named or numbered. Thus some simple method or system for describing the position of a point or a place on a map is essential for quick and accurate identification. The use of coordinates has been adopted to serve this purpose. There are several types of coordinate systems but the polar and the military grid are the two types most used and ones with which all officers and enlisted men must be familiar.

■ 22. POLAR COORDINATES.—This system consists of locating a feature by giving its distance and direction from a nearby

landmark, the name and location of which is known or shown on the map. Polar coordinates are commonly used in designating points located with a compass in the field and in designating positions on maps not equipped with the military

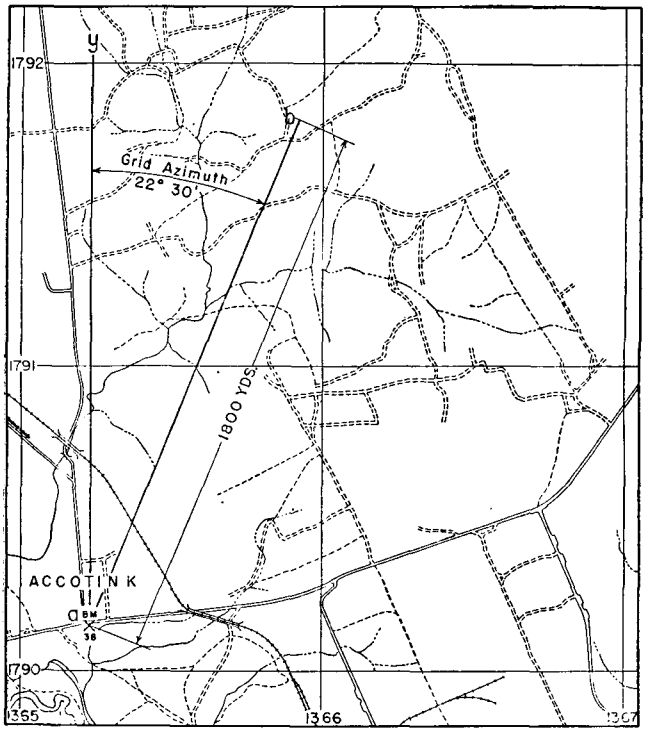


FIGURE 20.—Polar coordinates of b from BM 38, Accotink (village), distance 1,800 yards, on grid azimuth 22°30'.

grid. They are also frequently used in connection with ordinary field sketches. The landmark and selected direction must be clearly described in addition to stating the distance and angle. Polar coordinates are commonly used by reconnaissance patrols sent out to locate enemy installations. The

information brought or sent back by such patrols is usually in the form of a sketch. This sketch gives the distance and a magnetic azimuth to the enemy locations from point of observation of the patrol. Distance is estimated and azimuth read with the compass carried by the patrol leader. From these sketches it is possible to plot the position of these enemy installations on a map. Magnetic azimuths are changed to grid azimuths as stated in paragraph 15, and distance plotted along this azimuth line from the stated point of observation of the patrol. For example (see fig. 20), a patrol sends back information that an enemy position is located at b, an estimated distance of 1,800 yards on a magnetic azimuth of 31°30′ from BM 38 located in Accotink village. On this map, the magnetic north being greater by 9° than grid north, company headquarters, on receiving this information, changes the magnetic azimuth of 31°30′ to a grid azimuth of 22°30′. It then can plot the enemy position (point b) at a distance of 1,800 yards to scale from BM 38 in Accotink village along this grid azimuth as indicated in figure 20.

■ 23. MILITARY GRID.—*a. General.*—To make the reading of military maps easy, grids are printed on the map. The grid is simply a set of numbered north and south lines showing distance in thousands of yards east of the origin, and a set of numbered east and west lines showing distances in thousands of yards north of the same reference point. On a large-scale map (for example, 1:20,000 (par. 5)) these lines are 1,000 yards apart. On the medium-scale map (par. 5) the lines are 5,000 yards apart.

b. Location by grid coordinates.—Points are designated by coordinates simply by the intersection of the north-south grid lines (vertical lines) with the east-west grid lines (horizontal lines). Thus, in figure 21, location of the point A is indicated by the intersection of the 198 grid line and 262 grid line; the coordinates of the point therefore are (198–262). Note that distance east of origin is called the X-coordinate and is read first; and that distance north of origin is called the Y-coordinate and is read last. Beginners often make the error of reading the wrong coordinate first. One way to avoid this is to remember the key phrase "READ-

RIGHT-UP." It often may be necessary to designate points which do not fall at the intersection of grid lines. For example, it is required to find the coordinates of point B in figure 21. If it is assumed that the sides of the grid square are further subdivided into 10 equal parts, it is seen that the point B is 8 of these parts east and 7 of the parts north of the southwest corner of the square in which B is located. The coordinates of the point B are therefore written (197.8–263.7). Often sufficiently close determination can be made by estima-

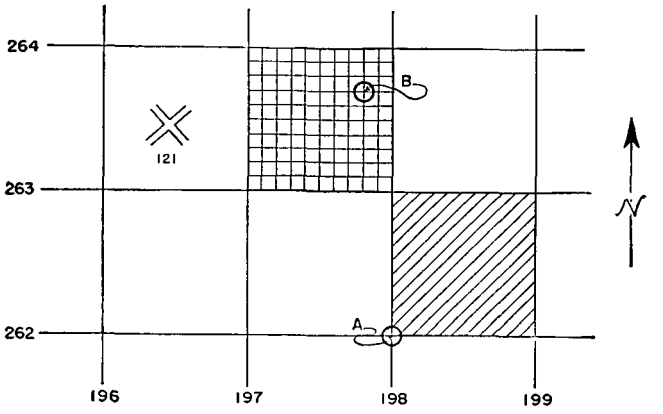


FIGURE 21.—Coordinates.

tion. For example, CR (crossroads) 121 could be located by inspection at (196.4–263.4). Since on all commonly used large-scale maps the grid square measures 1,000 yards on a side, a reading to tenths (one decimal place) gives a location to the nearest 100 yards. A reading of hundredths (two decimal places) gives an accuracy within 10 yards. When the grid numbers have more than two digits, it is customary to drop off all but the last two digits. Thus, the coordinates of point B above may be written (97.8–63.7), or if greater accuracy is desired (97.80–63.70).

c. Location by grid squares.—When a point is easily identified such as a numbered cross road or a town, it is necessary merely to refer to the southwest corner of the grid square in

which it is located. For example, in figure 21 crossroads 121 could be designated as CR 121 (96–63).

■ 24. COORDINATE SCALE.—*a. General.*—In paragraph 23*b*, the coordinates of point B were found by subdividing each side of the square (197–263) into 10 parts. This operation is used

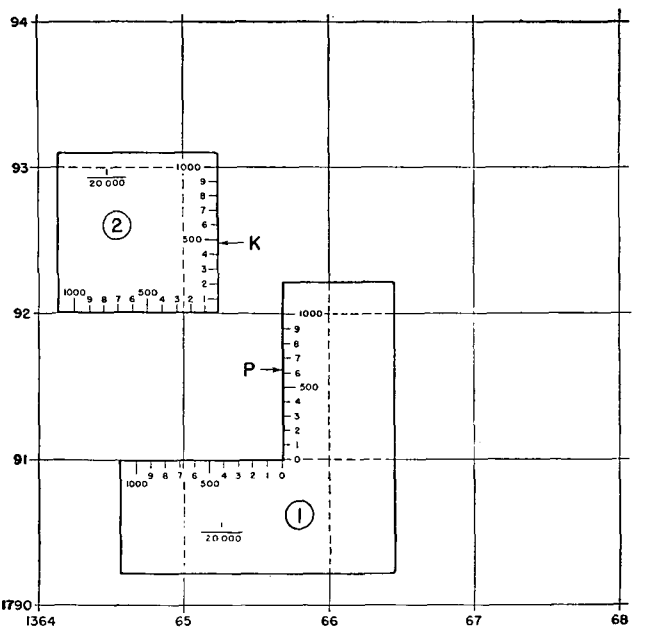


FIGURE 22.—Plotting point with coordinate scale.

only for explanation and is too long and tedious for normal use. A grid coordinate scale or card as shown in ① and ②, figure 22, permits finding these coordinates rapidly and easily. These cards may be made of cardboard, metal, or celluloid. For large-scale maps having grids 1,000 yards apart, lay off on the interior edges 1,000 yards to the scale of the map. Beginning at the vertex divide each 1,000 yards into 10 equal parts. This may be done by means of the graphical scale

printed on the map. For medium-scale maps having grids 5,000 yards apart, lay off on the inner edges 5,000 yards to the scale of the map, and subdivide each 1,000 yard division into

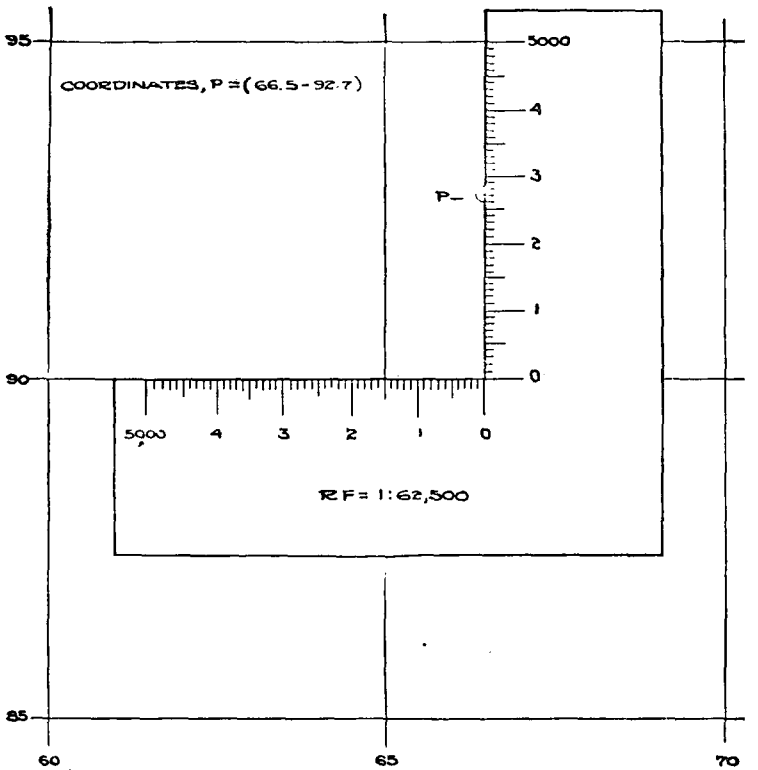


FIGURE 23.—To read grid coordinates of point on map (1:62,500) with 5,000-yard grid by means of coordinate scale. (Not reproduced to scale.)

10 equal parts as described above (fig. 23). The L-shaped type is more convenient to use. However, the rectangular type (① and ②, fig. 22) may be readily improvised by use of any square piece of cardboard or heavy paper.

b. To read coordinates of any point on map using coordinate scale.—Required, to find coordinates of point P (fig. 22). First identify the square in which P lies and write the coordinates of the lower left (southwest) corner of the square thus (1,365–1,791) or, dropping off the first two digits as described in paragraph 23*b*, it could be written (65–91). Now place the coordinate scale with its horizontal (east–west) edge on the 1,791 grid line. Keeping this edge on the 1,791 grid line, slide the scale along until its north-south scale passes through the point P. The decimal portion of the X-coordinate is read on the horizontal (east–west) scale, where it is cut by the west boundary of the square (in this case the 1,365 grid line). The decimal portion of the Y-coordinate is read on the vertical (north-south) scale, at the point P. These readings are then filled in at the proper places after the coordinates already written down. Reading to the nearest 100 yards, the coordinates of P are (1,365.7–1,791.6) or (65.7–91.6). Reading to the nearest 10 yards the coordinates are (65.68–91.62). The coordinates of K are (65.25–92.48). Similarly for the medium scale map shown in figure 23 the coordinates of the point P are (66.5–92.7).

c. To plot on a map any point whose coordinates are given.—This process is the reverse of determining the coordinates of a point. For example, in figure 22 let us assume that it is required to plot the position of the point P whose coordinates are (1,365.68–1,791.62). Place the coordinate scale on the map as shown in position ① in figure 22. The position of P can be marked at once with a pin or sharp pencil.

SECTION VI

ELEVATION AND RELIEF

25. GENERAL.—*a. Ground form and elevation.*—Up to this point the map has been regarded as a representation of a flat surface and only the horizontal position of features indicated thereon has been considered. A map to be of the greatest practical value must convey to the user a definite impression of ground forms (hills, ridges, and valleys) known as relief. This brings up the important subject of elevations.

By elevation is meant the vertical distance of any specified point on the earth's surface above a selected reference plane, which for most maps is mean sea level.

b. Means of representing relief and elevation.—Since a map is a plane surface, some type of conventional sign must be used in order to represent relief and elevation. On most modern topographical maps, this is accomplished by the use of contours. Other methods such as hachures (par. 28) and

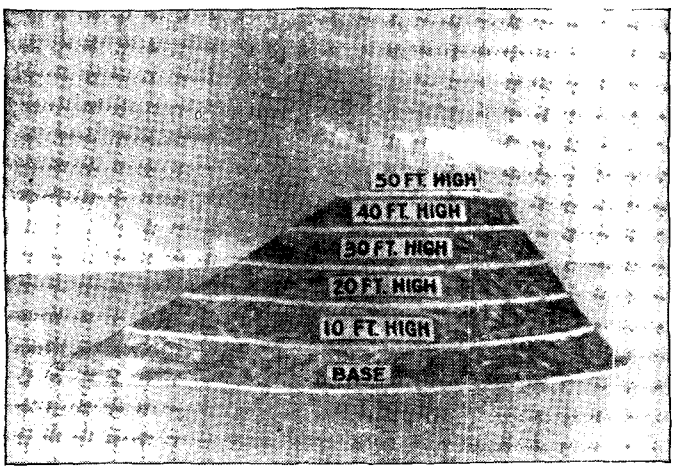


FIGURE 24.—Side view of hill.

hill and valley shading are used but contouring is the most common and practical method.

26. CONTOURS.—*a. General.*—Contours are the conventional signs drawn on a map to show the different ground forms. After practice with contours the map reader cannot only visualize shapes of hills, mountains, and valleys, but can also find elevation of points and determine slope and visibility along given lines. A contour is a line drawn on a map which represents an imaginary line on the ground all points of which are at the same elevation. Figure 24 represents a hill in the middle of the ocean. The seashore line itself would be the base or zero contour. If the sea should rise 10 feet

the new seashore line would mark the 10-foot contour. Similarly the next higher contour line would be marked for each rise in elevation of 10 feet. Figure 24 shows the successive increases in sea level which indicate contours. Figure 25 gives an oblique view of this same hill. From directly above, the hill would appear as in figure 26. Figures 24, 25, and 26 are photographs. Consequently, wiping out the picture of the hill itself, it would appear on a map as in figure 27 when indicated by contours alone.

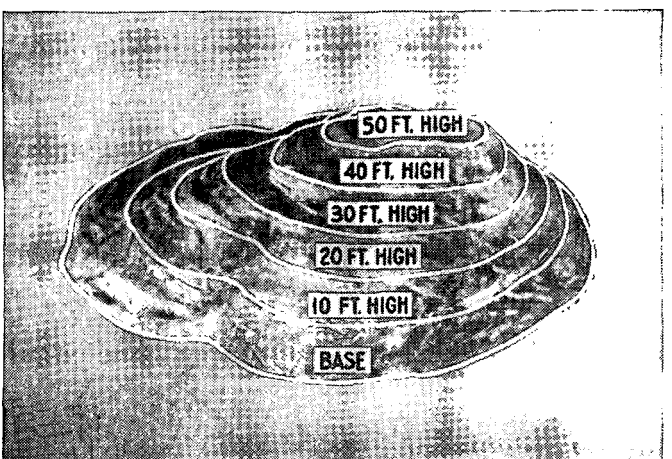


FIGURE 25.—Oblique view of hill.

b. Characteristics.—Figure 28 represents a number of more common ground forms as they are shown by contours. Looking at this figure it should be noted that—

(1) Contours have a characteristic wavy appearance.

(2) Elevation of contours above the reference plane (mean sea level) is shown by numbers usually in feet.

(3) At A, B, and C are contours which are closed curves, indicating either hilltops or depressions. Since the contour numbers increase as these points are approached it is apparent that A, B, and C are actually on hilltops.

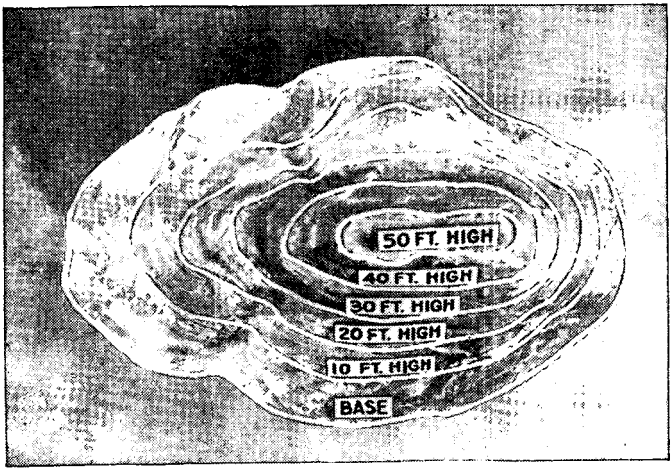


FIGURE 26.—Top view of hill.

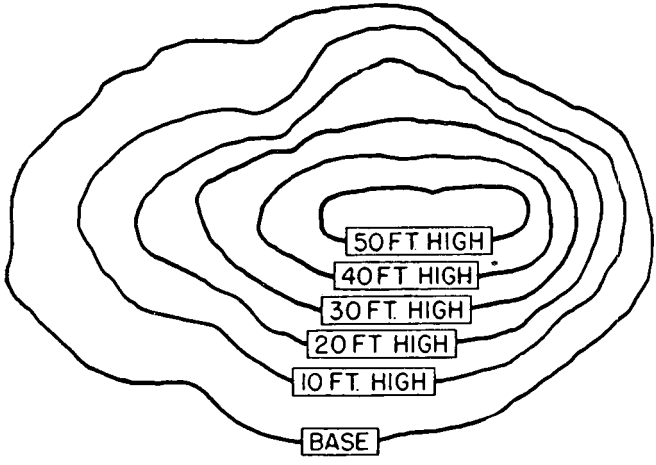


FIGURE 27.—Hill shown by contours.

(4) Contour at A, being nearly circular, indicates the top of a peak or knob, whereas the elongated contour at C indicates the crest of a sharp ridge.

(5) Though all contours are closed curves, most of those shown do not close within the limits of the map sheet. The 200-foot contour runs off the sheet at D–D and closes just

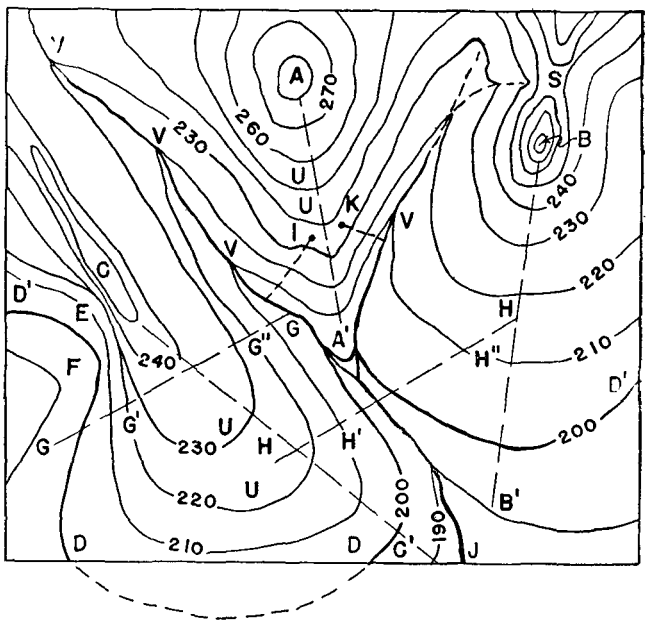


FIGURE 28.—Characteristics of contours.

outside, as indicated by the broken line. It runs off again at D'–D' and closes beyond limits of the sheet.

(6) On the line AA' there is a uniform slope. This is indicated by the equally spaced contours. On the line BB' there is a concave (sway-back) slope since the contours are close together at the top and farther apart at the bottom. On the line CC' there is a convex (humpback) slope. At B there is a steep slope while at B' there is a gentle slope.

The representation of these slopes by means of profiles is further illustrated in figure 29. (For construction of profiles see paragraph 31.)

(7) Contours do not touch each other except at E, which indicates a vertical cliff.

(8) At the points marked V is seen the characteristic V-shape of valley or streamline contours, and at those points marked U, the U-shape of ridge contours. The closed ends of the V's point upstream and those of the U's downhill.

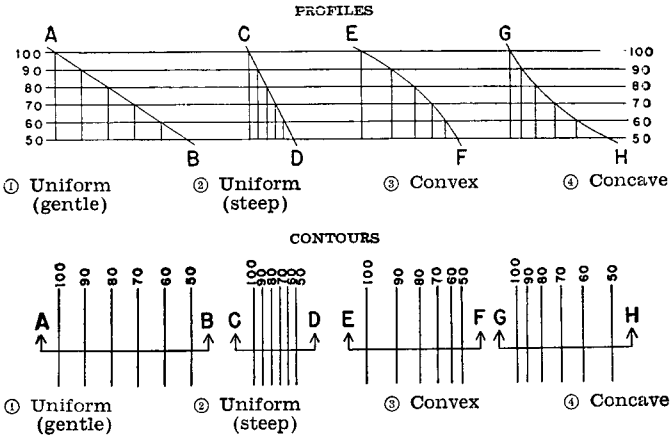


FIGURE 29.—Representation of slope by contours.

(9) At A' is shown the characteristic M-shape appearance of the contour at a Y-stream junction.

(10) Rain falling at I runs down the slope normal to the contours, entering the drainage line near G, and ultimately leaving the area by the main stream at J. The line of the spur AA' is the divide between the two tributary streams. Rain falling at K, just east of the divide, flows into the eastern tributary. The divide between any two adjacent valleys is easily traced out.

(11) Point S is a saddle, a depression or low point in a ridge or line of hills. Note the characteristic shape of the contours. Saddles occur frequently.

(12) Adjacent contours in a water-worn terrain resemble each other. This is the same as saying that changes in the form of the ground are gradual. This characteristic may be noted at many places, as on the ridge lines at AA′ and BB′.

c. Summary.—Briefly summarized, contour characteristics previously discussed and illustrated are—

(1) A contour is a line on a map joining points of equal elevation.

(2) Contours are spaced at uniform vertical intervals.

(3) A small closed contour indicates a hilltop or a depression when so marked by the conventional sign (see fig. 3).

(4) Every contour is a continuous closed curve, on or off the map.

(5) Spacing of contours indicates steepness of slopes. This spacing also indicates nature of slope, whether uniform, concave, or convex.

(6) Contours do not touch or cross each other, except in the unusual case of cliffs.

(7) Valleys are usually characterized by V-shaped contours, and ridges by U-shaped contours.

(8) Adjacent contours resemble each other.

d. Logical.—(1) Figure 30 shows the method by which a map maker draws contours on a map when he is given the drainage net and the elevations for certain critical points. Drawing of logical contours is valuable practice in gaining ability to visualize ground forms shown by contours on topographic maps.

(2) The information shown in figure 30① has been obtained by a field survey or other means. This information consists of the courses of the stream lines and elevations of selected critical points and forms the framework upon which the contour map is drawn. Consider the stream line in the lower right portion of ② running from elevation 97 to elevation 133. Elevations 100, 110, 120, and 130 are marked on this stream line by interpolation. V-marks pointing upstream are used to mark such elevations on a stream line. All other stream lines are treated in a similar manner. Contour locations are marked on the ridge lines in a similar manner, except that straight marks normal to the ridge line are used.

Marks of equal elevation are then joined producing contours as shown in ③.

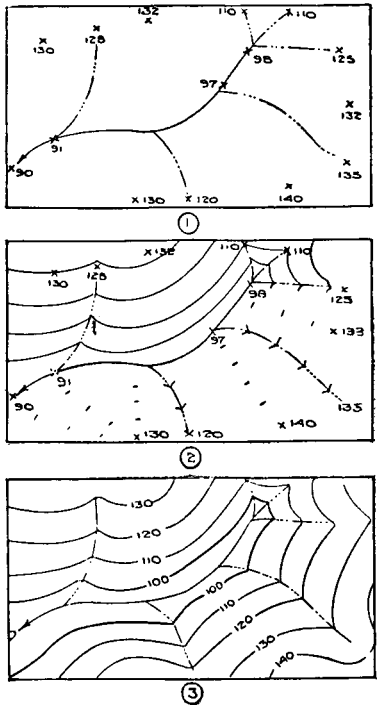


FIGURE 30.—Method of drawing contours by interpolation on drainage net where elevations are given.

■ 27. DETERMINING ELEVATION FROM CONTOURS.—Often the map reader will be concerned with some point on a map which may happen to be located between two contours, and it will be necessary to know the elevation of the point in question. If any point such as B (fig. 31) lies directly upon a contour, its elevation is of course that marked on the contour, or 580 feet in this case. But suppose the point X is not directly upon a contour. It lies between contours 580 and 590. Its

elevation is therefore something between these two figures. If a line is drawn through X perpendicular to the adjacent contours, it will cross them at A and B. Then the elevation of A is evidently 590 feet and the elevation of B 580, because these points lie upon the contours so marked. Assuming the ground falls uniformly from A to B, without making any measurement of the distance BX, it can be judged by eye that it is a little more than half and a little less than two-thirds of the distance AB. It may be said without any great

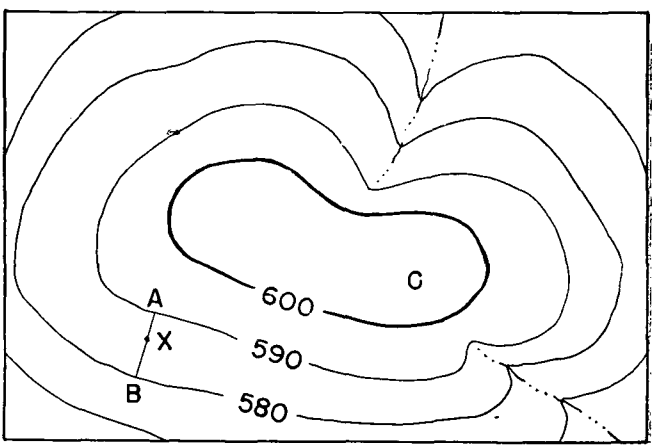


FIGURE 31.—Determining elevation from contours.

error that it is 0.6 of AB. The difference of elevation of A and B is 10 feet. Hence the elevation of X is 580 plus 0.6 of 10 feet or 586 feet, giving an error probably less than 1 foot. This determination is close enough for the map reader. It is not necessary to draw such a line as AB or to measure a distance such as BX. If the point Y is taken it can be said by merely looking at it that its elevation is 588 feet. In case the point in question lies on the top of a hill such as C, only an approximation is possible. The elevation of C is greater than 600 but not as much as 610 since the 610 contour is not shown. Often the exact elevation of the highest points on hills will be given.

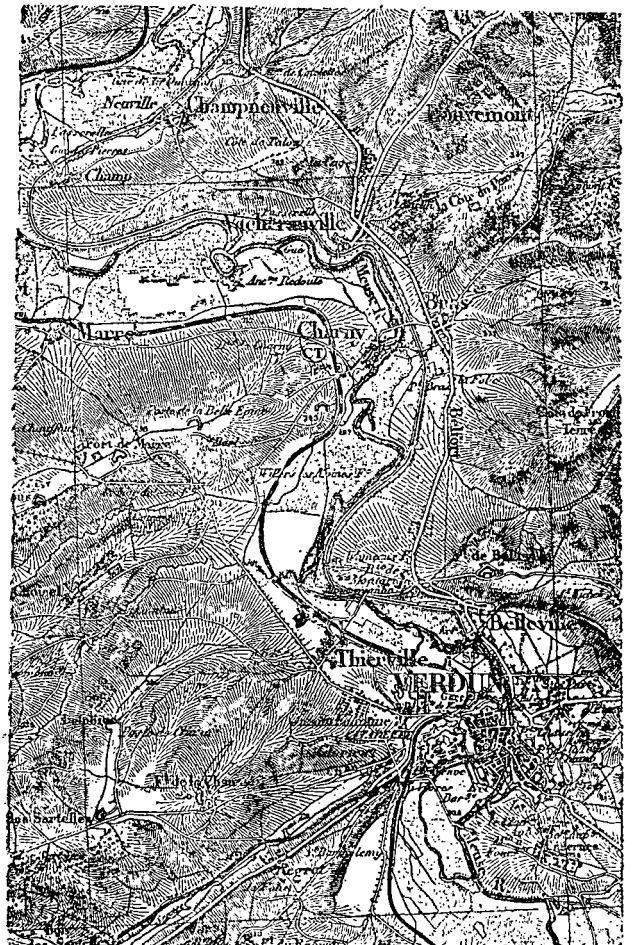


FIGURE 32.—Hachure map.

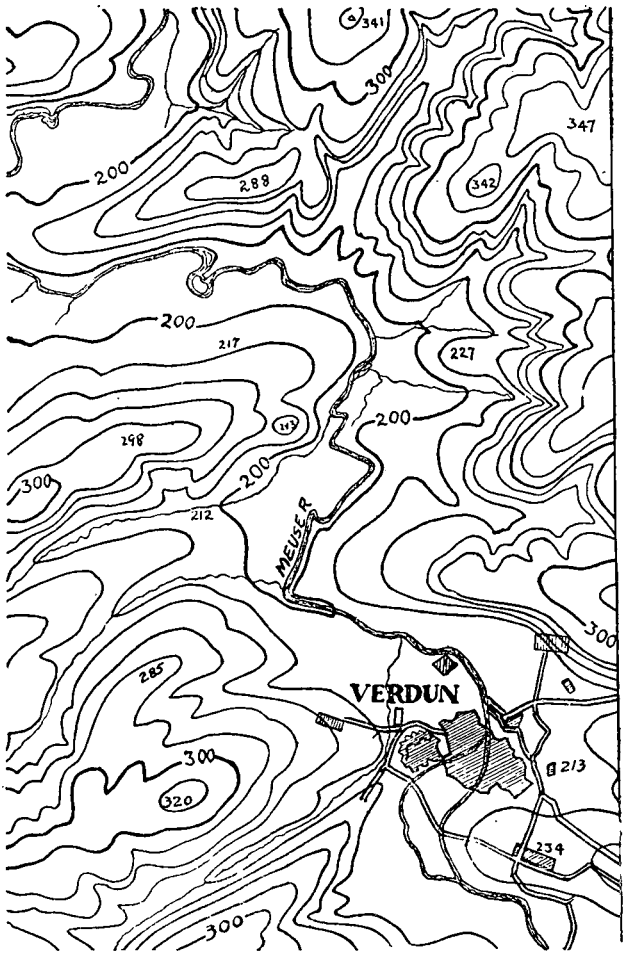


FIGURE 33.—Contour map of same area as hachure map in figure 32.

■ 28. HACHURES.—Frequently on foreign maps, a method of representing elevations called hachuring is used instead of contouring. Hachures consist of short lines running directly down the slopes of hills, that is, they show the direction that water would flow downhill. Hence, hachures are at right angles to contours. Steepness of the slope is indicated by thickness and spacing of the lines; steep slopes are shown by heavily inked lines very close together, while lightly shaded lines wide apart show gentle slopes, and level areas are left without any lines whatever. Hilltops, ridges, valleys, and various slopes are easily recognized from hachures but specific elevations cannot be determined accurately unless given in figures. The contour method is better for military purposes. Figures 32 and 33 show the comparison between a hachured and a contoured map.

■ 29. RIDGE LINING AND STREAM LINING.—*a. Purpose.*—In order to emphasize the basic structure or master lines of the terrain of a given area, a system known as ridge lining and stream lining is often used. On a map or an aerial photograph thus ridge lined or stream lined, the great mass of detail which may tend to confuse may be neglected for the moment, and those basic structures such as stream systems, ridge lines, and key features can be emphasized. Three steps may be followed in this process.

b. Stream lines.—Study the map or aerial photograph and select the main streams and their tributaries. Emphasize them, preferably by drawing over them in blue, and thus cause the drainage system to stand out.

c. Ridge lines.—Draw a line down the main ridges. This should be done preferably in brown so as not to obscure features lying under the lines. Then select the minor ridges and trace their ridge lines in a similar manner. The number of minor ridges to be included will depend upon the emphasis desired. In drawing ridge lines it is not normal to carry them all the way to the stream. A good system is to stop at the beginning of the flood plane as shown by the increase in space between contours. It will be noted that the tendency at first is to mark isolated ridges, whereas the ridge lines should form a connected structure. If all the ridge lines in

an area are drawn, it usually will be found that they join together into a systematic branching structure like the fingers of a hand or the backbone and smaller bones of a fish. This structure is similar also to the branches of streams; in fact

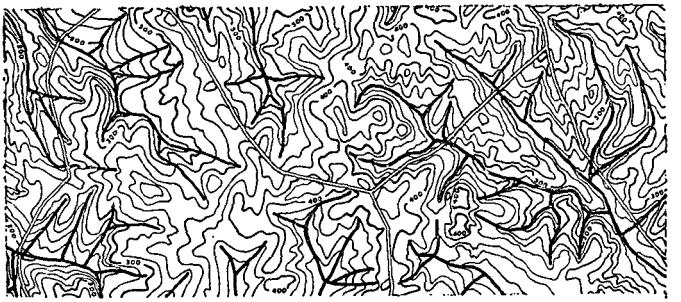


FIGURE 34.—Contoured map with stream lining.

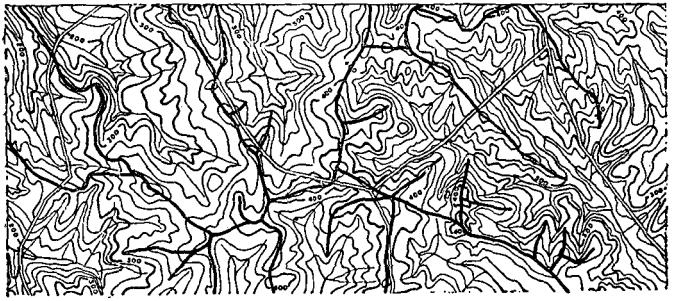


FIGURE 35.—Contoured map with ridge lining.

the branches are fingers of the two systems fitted into each other. Ridge lines do not cross streams. Figure 34 shows a portion of a contour map which has been stream lined; figure 35 shows this same area after it has been ridge lined. Note how the main drainage system and the main ridge lines stand out.

d. Emphasized contours on contoured maps.—Certain contours may be emphasized by use of thicker lines, and it is customary to do this at regular intervals to facilitate the reading of contour maps; for example, on map in figure 1 (back of manual), thicker lines are used at 100-foot intervals. Likewise, commanding elevations may be brought out by coloring the map area between selected contours.

■ 30. SLOPE AND GRADE.—*a. General.*—Slopes and grades are important to the map reader since they affect selection of

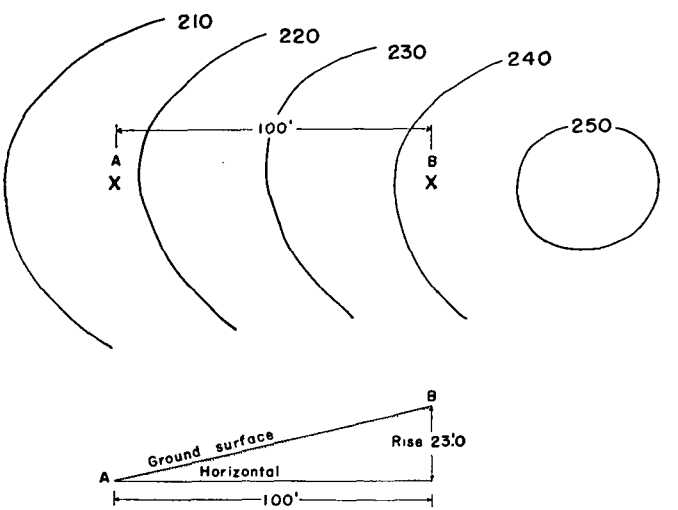


FIGURE 36.—Determination of slope.

routes of travel whether by road or open country, and siting or location of all military works and weapons. In paragraph 26*b* it was learned that the spacing of contours indicates the slope of the ground. A step further is to determine from a study of contours on maps the amount of slope and express it numerically. There are several methods of expressing

slopes of ground surfaces. The method of expressing slope by percent is the principal one and the only one that will be described in this manual.

b. Slope in percent.—A slope of 1 percent is one in which 1 foot of vertical height is ascended or descended in traveling 100 feet of horizontal distance. A slope of 10 percent is one in which 10 feet are ascended or descended in traveling 100 feet. Thus in figure 36 where AB represents a slope, if the horizontal distance from A to B is 100 feet, and difference of elevation is 23 (or 242—219) feet, the slope of AB$=\frac{23}{100}=23$ percent. An upward slope is plus, a downward slope minus, that is, the slope from A to B is plus 23 percent, but from B to A is minus 23 percent.

c. Grade.—The slope of road and railroad lines is referred to as grade, and may be computed in a manner similar to that described in *b* above.

■ 31. PROFILE.—*a. General.*—The most satisfactory way of showing the slope of any line on a map is by drawing its profile. A profile between two points is the line (usually irregular) of intersection of an imaginary vertical plane cutting the earth's surface between these two points. For example, in figure 37 imagine a vertical plane passed from above through the earth between the points A and B, and the front half of the hills and ridges removed, just as a cook passes a knife through a cake and removes half. The outline of the surface of the remaining half would be its profile as represented in figure 37②. It has already been seen in figure 29 how profiles may be used to illustrate the different types of slopes indicated by the spacing of contours. Profiles are also a means of determining the visibility or the defilade of points or areas from any selected point on a map. Visibility is discussed in paragraph 32.

b. To draw profile between two points.—Figure 37① represents a portion of a contoured map. It is desired to construct the profile of the ground represented by the map between the points A and B. Proceed as follows:

(1) Connect points A and B by a straight line and assume that a vertical plane is passed through this line.

(2) Take a piece of cross section paper or any paper which has parallel lines equally spaced; cut or fold the paper along one of these lines.

(3) Refer to map and determine the highest and lowest elevation along the line AB; number the spaces on the paper

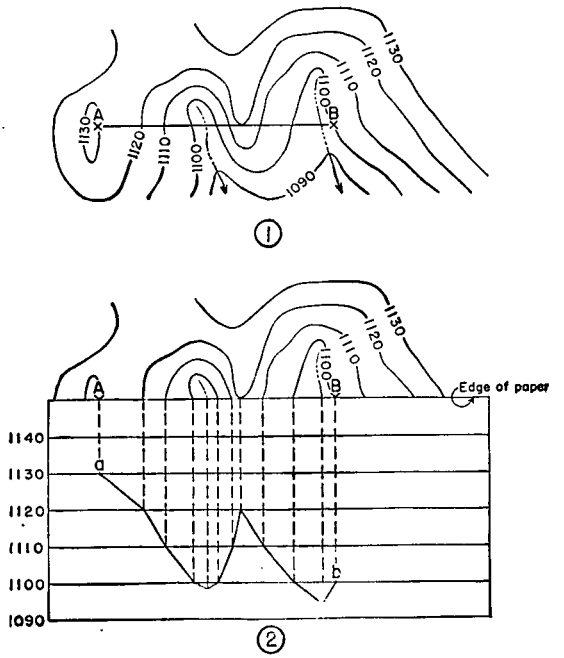


FIGURE 37.—Construction of a profile.

to correspond with the elevations on the map beginning with the highest elevation toward the top edge of the paper (fig. 37②).

(4) Place top edge of the paper along the line AB and where the edge cuts each contour, drop perpendiculars to the line on the paper corresponding to the elevation of the contour being considered.

(5) Connect the points of intersection of the perpendiculars with the lines of the paper. This will represent the profile except between adjacent contours of the same elevation which require the determination of intermediate elevations.

(6) Where the line crosses a crest or a depression an elevation number on the map is sometimes found to assist in completing the profile. Where such elevation numbers are missing, interpolate necessary elevations from the spacing of the contours, using the method described in paragraph 27.

(7) When a profile is desired of an irregular line on the map, such as a road or trench, divide it into a series of sections approximately straight and plot as directed above, turning the paper at each angle to make a continuous profile.

c. Vertical scale.—Profiles usually have an exaggerated vertical scale in comparison with the horizontal scale which ordinarily is the same as that of the map as shown in figure 37②. In the figure, the lines on the paper could represent 10-foot elevations as indicated, or they could represent 5-foot elevations, thus further exaggerating the profile as desired. For constructing profiles, use of cross section paper will be found most convenient since the vertical lines assist in dropping the perpendiculars to the horizontal lines representing the contour elevations.

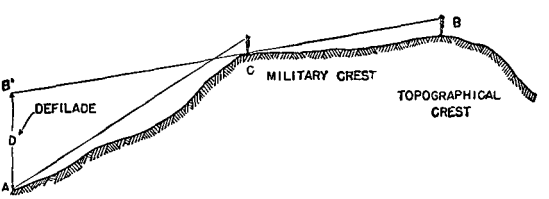


FIGURE 38.—Defilade.

■ 32. VISIBILITY.—*a. General.*—One of the important uses of maps for military purposes is to determine whether a point, a route of travel, or an area is visible from a given point or position. The extent of the area visible affects selection of targets, siting of weapons, and location of defiladed area or dead space (fig. 38). There are various methods of solving visibility problems, but only the ones more commonly used will be covered in this manual.

b. Inspection.—Many problems of visibility may be solved by inspecting the map, and determining from the contours the ground slope represented. The representation of ground slopes by contours is described and illustrated in paragraph 26*b*. For example, in figure 29 it is evident by

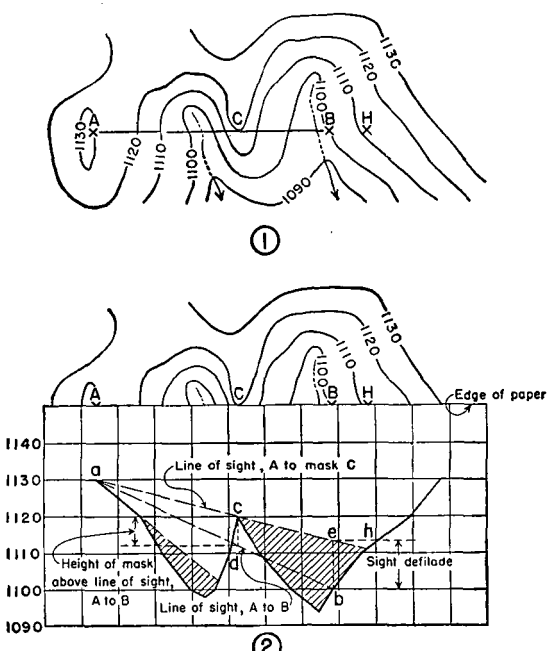


FIGURE 39.—Determination of visibility by profile method.

inspection that an observer at E cannot see the ground at F, this being a convex or humpback slope, while an observer at G can see the ground at H, this being a concave or sway-back slope.

c. Profile.—In paragraph 31 it was learned how to construct a profile between two points such as AB on figure 37. Suppose it is required to use the profile method to

determine what points along the line AB are visible from an observer at A. Construct a profile along the line AB as described in paragraph 31. It is evident in figure 39 that

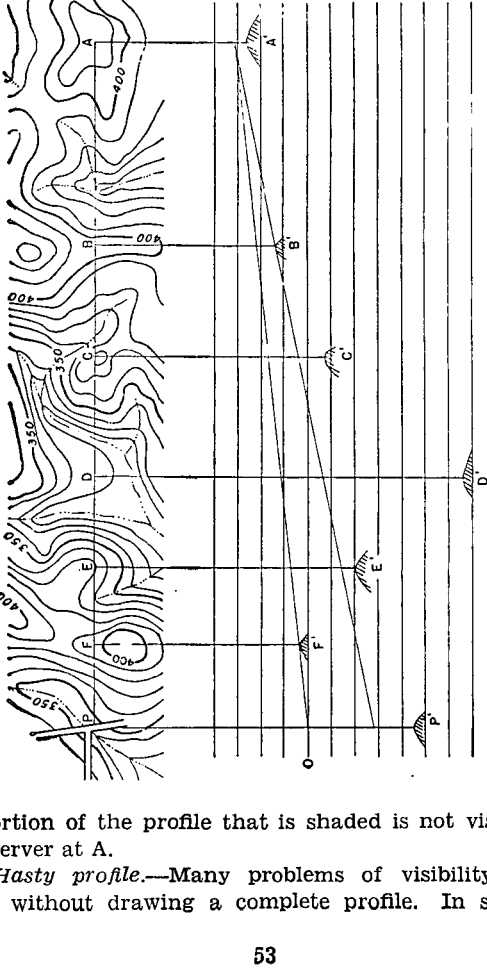


FIGURE 40.—Determination of visibility by hasty profile method.

the portion of the profile that is shaded is not visible from an observer at A.

d. Hasty profile.—Many problems of visibility may be solved without drawing a complete profile. In such cases

only the critical points which may affect the visibility are plotted, such points being first determined by inspection. These points would be the position of the observer's eye, the probable masks (hills or ridges), and the point where visibility is to be determined. This is illustrated in figure 40 which represents a portion of a contoured map. It is required to determine what an observer can see along the line AP from various points along this line, assuming trees and other vegetation do not interfere. It is evident that while at A the observer can see only point B and point F. From B he can see A, C, E, and F, but is unable to see points D and P. This can be continued for other points.

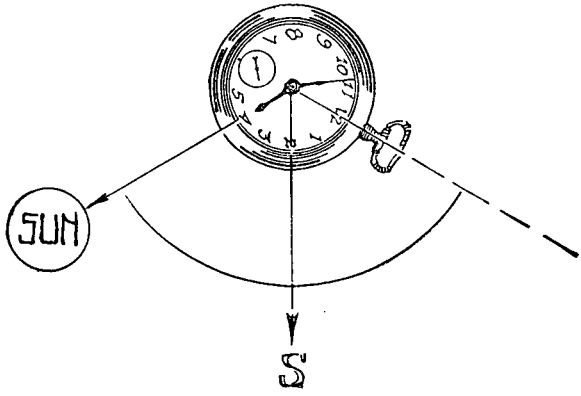
SECTION VII

MAP READING IN THE FIELD

■ 33. GENERAL.—All Army personnel should keep in mind the importance of being able to read maps accurately and quickly in the field. Many disastrous mistakes have resulted from a lack of ability to read maps. To be able to read a map properly in the field, the student should be familiar with all material covered in the preceding sections. He should keep in mind that the map and aerial photograph are often the only means available for studying distant or inaccessible areas. He should always take his map into the field with him and constantly refer to it. He should keep his movements plotted on it, especially when operating over unfamiliar territory, and verify his location at every opportunity. He should practice until it is possible for him to secure a clear and accurate picture of the ground from the information given on the map. In addition to material in preceding sections, a few aids to his map reading ability are orientation, use of compass, determination of distance, and names by which ordinary features of the ground are known. A brief description of each of these follows.

■ 34. ORIENTATION.—*a. General.*—A person is said to have oriented himself when he stands on the ground and knows the cardinal directions north, south, east, and west. A person is oriented with respect to a map when he knows his position on that map, and a map is oriented when in a nori-

zontal position its north point actually points north. Every stream, road, or other feature on the map is then parallel to its true position on the ground, making it comparatively simple to pick out on the ground objects represented on the map. One who is responsible for guiding by map must know his position on it by constant reference to the map. Normally a map reader can keep himself and his map oriented by observing familiar landmarks. When such marks are not



Point hour hand at sun; south is half-way between hour hand and 12 on the dial.

FIGURE 41.—Method of determining direction by watch and sun.

available, the sun, stars, and compass may be used. Figure 41 shows an approximate method of finding south by use of the sun and an ordinary watch showing correct time. Figure 42 shows a method of finding the North Star by use of the pointer stars in the Big Dipper.

b. Method of map orientation.—(1) *Inspection.*—Figure 43 shows how a map may be oriented by carefully observing road system and features in immediate vicinity. It will be noted that the map has been rotated horizontally until the road on the map parallels the road on the ground, care being used to see that positions of nearby ground features are in similar relation to their corresponding conventional signs as shown on the map. This is the most practical method for ordinary

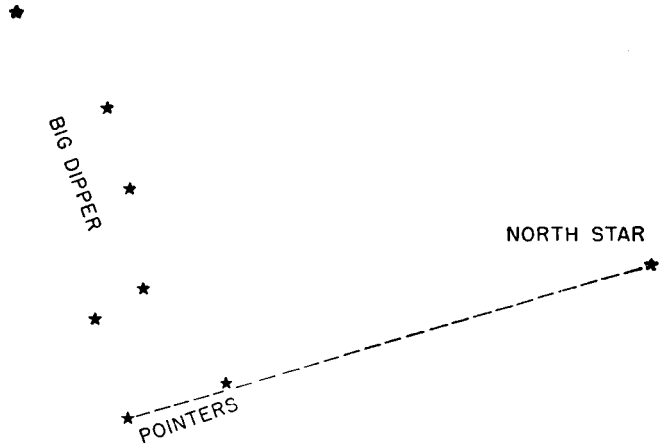


FIGURE 42.—Determining north by use of Big Dipper and North Star.

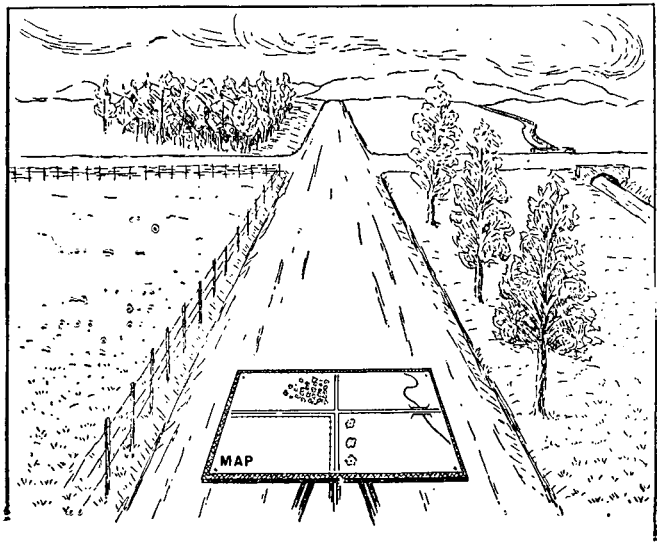


FIGURE 43.—Orienting map by inspection.

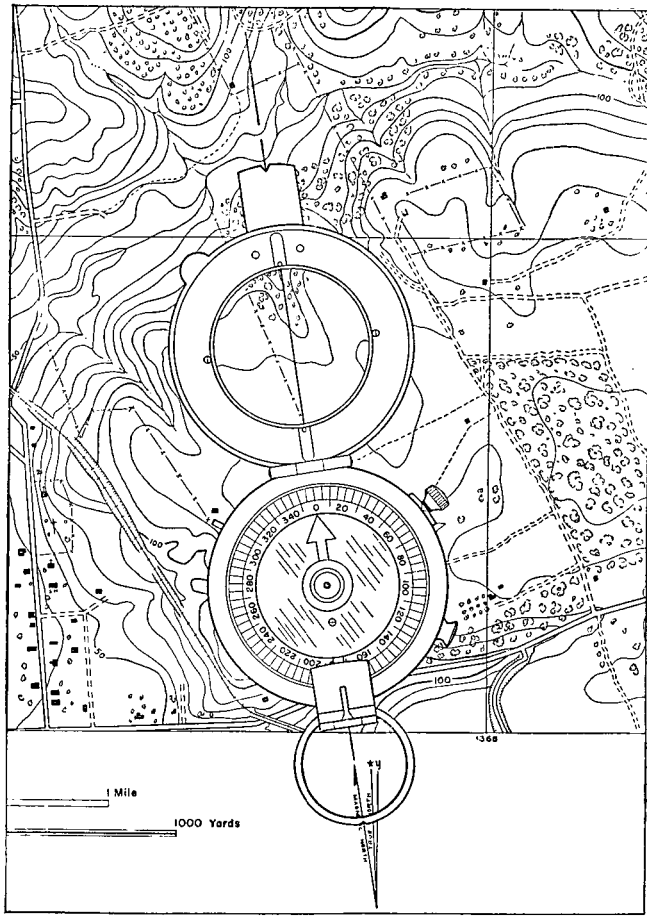


FIGURE 44.—Orientation of map by compass.

purposes and may be used as a rough check on more accurate methods.

(2) *Compass.*—Magnetic north is shown on most maps and is also indicated in the field by the north end of the compass needle. Figure 44 illustrates use of this method. Either

prolong magnetic north line or draw a line parallel to it. Then place compass on map with north point of compass case on this line. Rotate map horizontally until north end of needle coincides with north point of the case. Map is now oriented.

(3) *By means of a distant point when observer's position is known.*—A third method of orientation where a compass is not available and where there are no nearby features suit-

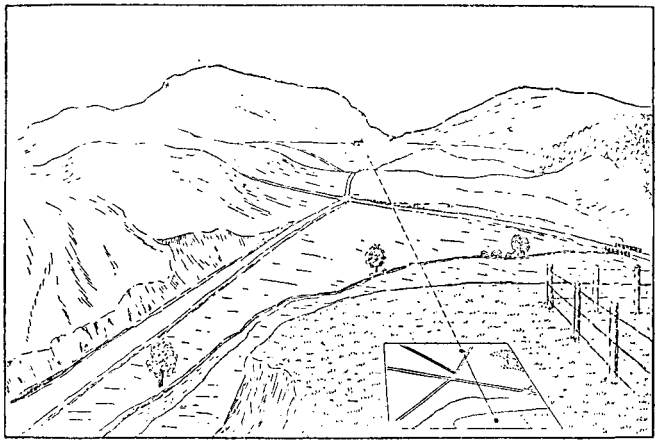


FIGURE 45.—Orienting map by means of distant point.

able for orientation by inspection is illustrated in figure 45. Place a pin at observer's position on map. This may be found by reference to the fence corner (fig. 45). Place another pin on the map location of some well-defined point such as the church. Holding map horizontal, sight at church on the ground along the line of pins. Map is now oriented. A more precise orientation is secured if more than one point can be used. Once the map is oriented, approximate map location of a target or other point may be determined as follows: keeping map in oriented position, sight over pin at observer's position toward designated point and place a pin on line of

sight. From a study of the map or by estimation or measurement of the distance, fix location of the point.

■ 35. FINDING OBSERVER'S POSITION ON MAP.—*a. Inspection.*—If approximate location on a map is known, all the observer has to do is study visible terrain for distinctive features and his position can be found by identifying these features on the map. This procedure is greatly simplified if the map is oriented to the ground. Figure 46 is an example of this method.

b. Striding or estimation of distance when along road, railroad, etc.—This method is illustrated in figure 47. Briefly, the method is to identify on the ground the nearest road bend, road junction, bridge, etc., which appears on the map, such as B in figure 47. The distance to this point is either estimated or measured by striding and position on map is obtained by laying off distance AB to scale of map as indicated in the sketch.

c. Resection from two known points.—This method is illustrated in figure 48. First, orient map accurately. Look over terrain and select two distant visible features on the ground, B and C, which can be located and identified on the map, b and c. Features selected should be so located that lines radiating from observer to them form an angle of as near 90° as possible. Place a pin in b, lay a straightedge (ruler or pencil) against the pin, turn it until it points at B. Draw a ray on the map from the pin toward observer's position. Repeat the same operation with point c. Intersection of the two lines is observer's location on map. Care must be exercised that map remains oriented during entire procedure. If three points are used instead of two, observer's location will probably be more accurate.

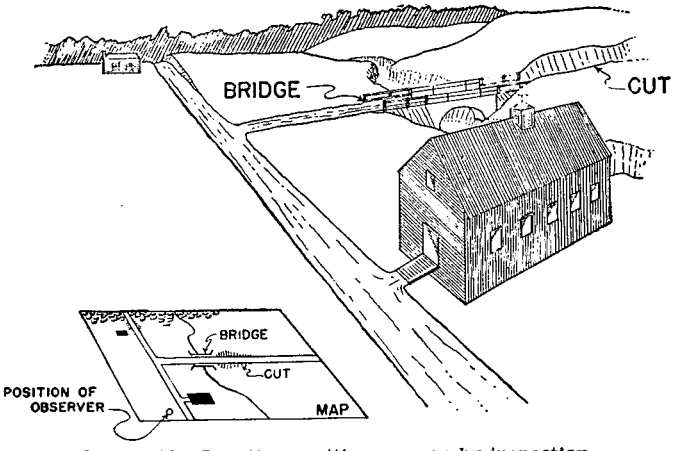


FIGURE 46.—Locating position on map by inspection.

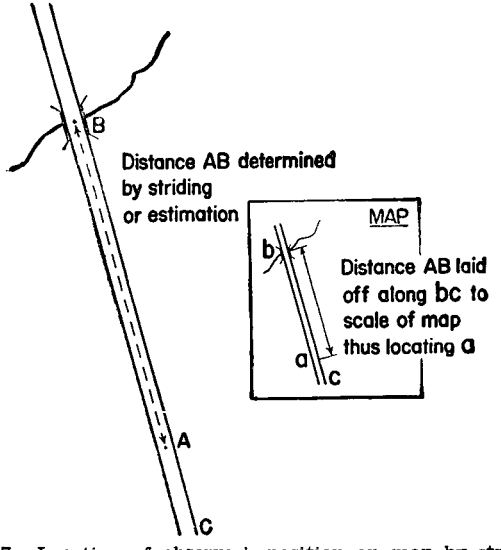


FIGURE 47.—Location of observer's position on map by striding or estimating distance when along road.

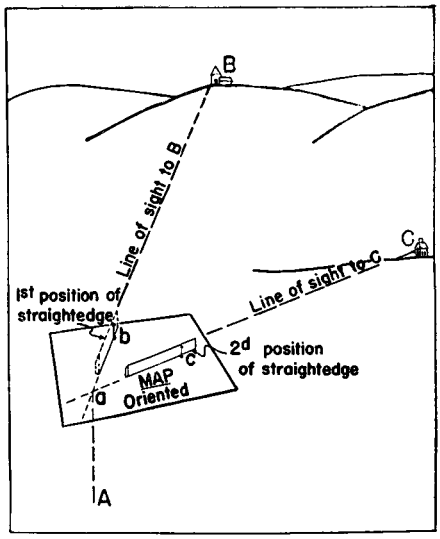


FIGURE 48.—Location of observer's position on map by resection from two distant points (graphic method).

■ 36. MILITARY TERMS FOR TERRAIN FEATURES.—In addition to usual standard terrain terms such as hill, ridge, valley, etc., certain other words are used to describe features of military importance. The most common of these are shown in figure 49.

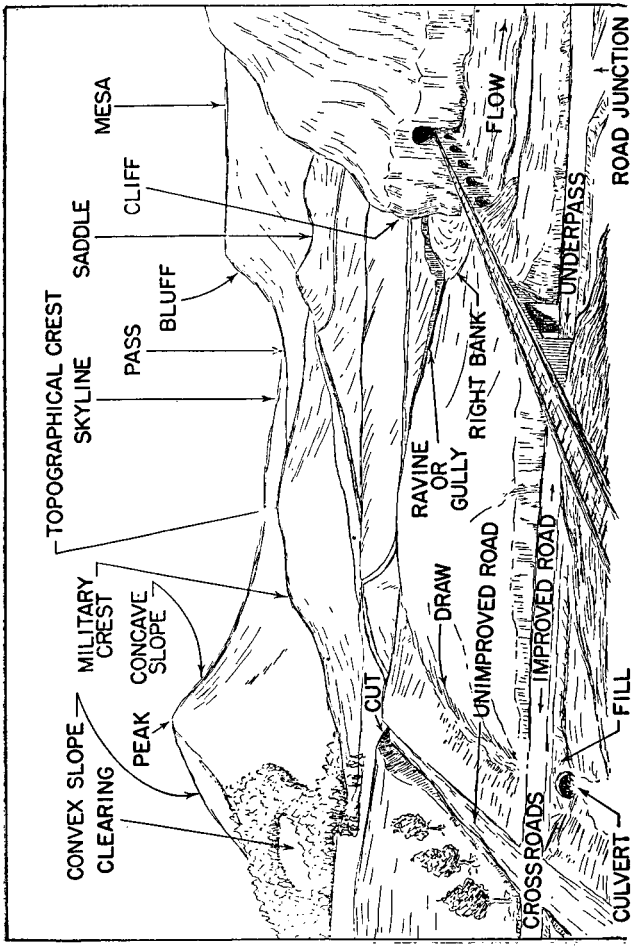


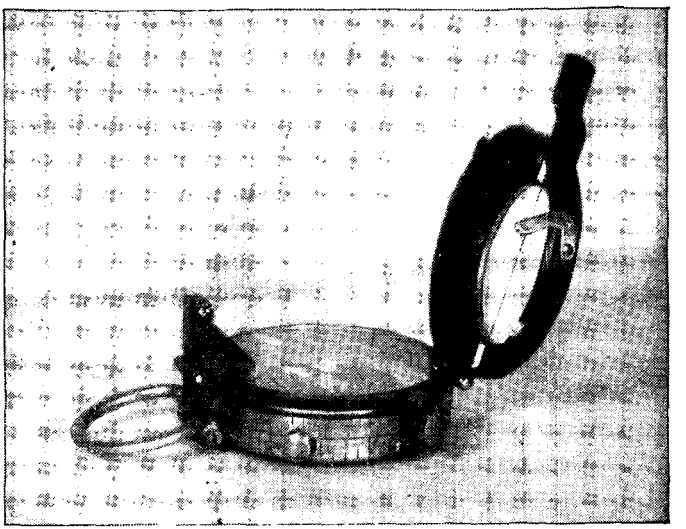
FIGURE 49.—Military features of terrain.

■ 37. DISTANCE.—There are many means of measuring distance. When time is not essential or conditions not unfavorable, pacing or even taping may be used. Along roads measurement of distance by speedometer mileage will be very common. For dismounted troops and for objects off route of travel for motorized troops, distances normally will be estimated by eye. All personnel should practice until they acquire reasonable skill in estimation by eye. However in some conditions, for example, night patroling or marching over broken terrain, all such methods are impracticable. For such operations two other methods may be used. In one, the leader can scale off the distance he must travel on his map and then locate and identify some prominent terrain feature at the end of his march. He has then merely to keep going until he comes to this feature. In the second method, he can reduce distance to time. Since the normal marching rate is 1 mile in 20 minutes, this reduction is very simple. If he is sent down the road a distance of 2 miles, he has merely to walk for 40 minutes and he should be near or at his destination.

■ 38. COMPASS.—*a. Types.*—The three types of compass issued in the service are prismatic, lensatic, and watch. The watch compass shown in figure 8 is being replaced by the lensatic compass. Descriptions of the other two types are given below.

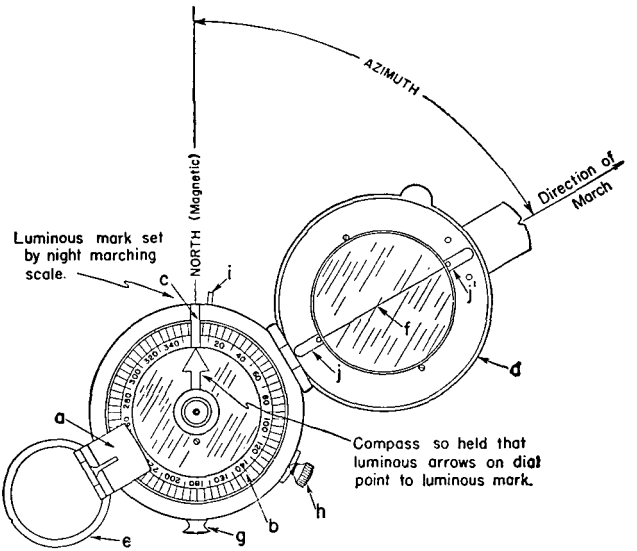
(1) *Prismatic.*—The prismatic compass is shown in figure 50② showing the more important parts labeled. It consists of a case containing a magnetic dial (b) balanced on a pivot, a hinged cover (d) with a glass window, a holding ring (e) and an eyepiece (a) containing a prism for reading graduations on the dial. The dial has two scales, the outer scale to be read through the prism or eyepiece and the inner to be read directly. Both scales are graduated from 0° to 360°. The north point is indicated by an arrow of luminous paint. The glass cover has an etched line (f) which may be used like a front sight, and the eyepiece (a) has a slot that may be used as a rear sight. In case the window in this cover is broken, a horsehair or a fine wire can be threaded through and stretched between the two holes in the cover provided for that purpose. Closing the lid operates a lever (g) which raises the dial to protect the compass from injury when not

in use. To lower the dial push clamp (g) forward with the thumb. A second glass protects the face of the dial when the lid is raised. On it is painted a luminous movable index which is used to set angles from the line of sight or north point. This glass can be revolved by unlocking the set screw (h) and turning the corrugated brass ring so that the movable index points at any angle from the line of sight. It can then be set at this angle by tightening the set screw (h). A rubber washer is fixed to the bottom of the case to prevent slipping when laid on smooth objects. The compass is carried in a stout leather case with a belt loop. The outside of the brass case is marked with two scales, one to read azimuths, and the other to read compass directions. Figure 52 shows one use of this outside scale. The compass is affected by presence of iron, steel, or electricity, and will not give accurate readings near an automobile, tank, fieldpiece, machine gun, or power line. A steel helmet, rifle, or pistol on the person of



① Photographic view.

FIGURE 50.—Prismatic compass.



a. Eyepiece
b. Compass card or dial (with luminous arrow)
c. Movable index mark on crystal (luminous)
d. Hinged cover
e. Holding ring
f Etched front sight cover
g. Clamping knob for compass card
h. Index locking screw
i. Dampening plunger
j-j' Luminous marks on cover

② Parts labeled.

FIGURE 50.—Prismatic compass—Continued.

the observer may influence the needle and make readings inaccurate.

(2) *Lensatic.*—Figure 51 shows two views of a lensatic compass. It functions in much the same manner as the prismatic compass. The hinged eyepiece is a narrow piece of metal containing a magnifying lens in the larger circular opening. When the eyepiece is tilted so that it is aimed at the forward part of the compass face, the observer is able to see both the scale and a distant point at the same time. It should be noted that the face has two scales, the outer

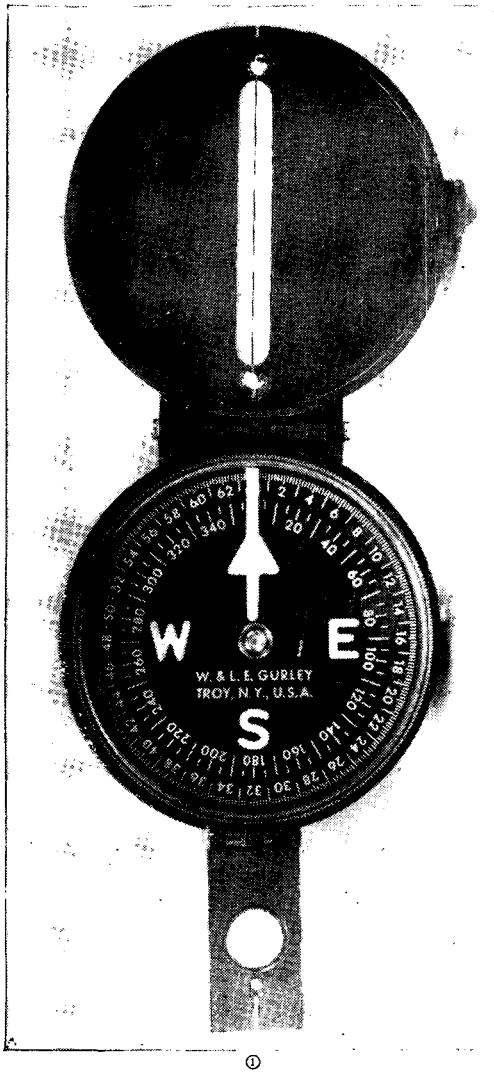


FIGURE 51.—Lensatic compass.

②

FIGURE 51.—Lensatic compass—Continued.

one showing mils, and the inner one showing degrees. The compass is made of light aluminum and is designed so that it may be carried in a pocket.

b. Measuring azimuth with prismatic compass.—To read the azimuth to any point proceed as follows (fig. 50②):

(1) Raise cover (d) and eyepiece (a) vertically, and lower needle dial at (g).

(2) Hold compass horizontally in front of the eye and pointing in the direction of object azimuth of which is desired. In doing this utilize every possible means for holding compass and eye steady. Methods used are somewhat similar to those used for sighting a rifle. A good method is to rest

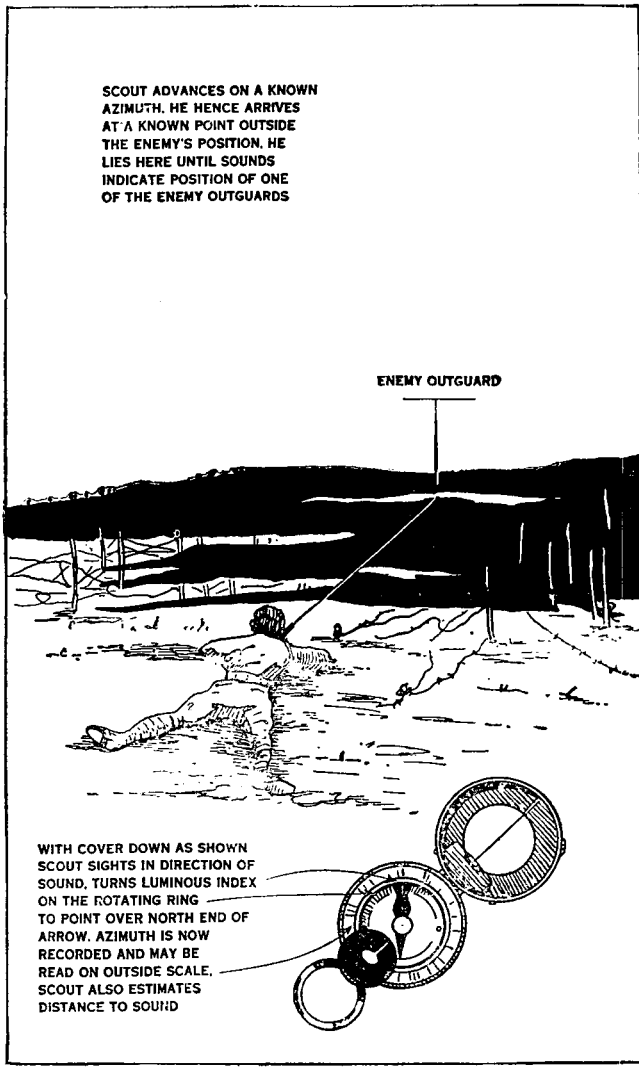


FIGURE 52.—Use of compass dial.

head, wrist, and body against a good substantial tree or other nonmetallic object. A prone or sitting position similar to that assumed for firing a rifle is also suitable. The dial may be dampened by operating the plunger (i) with index finger of left hand.

(3) Sighting through slot in eyepiece, line up object with etched line (f) in cover. Hold compass steady until dial comes to rest. Read azimuth indicated on dial as seen through eyepiece. This will be the magnetic azimuth of the line from observer to object.

c. Marching by compass.—(1) *Day.*—Often troops are ordered either to march or attack cross country according to given azimuths. Such troops might include patrols or individuals on scouting or messenger missions. Patrol leaders or unit commanders may compute from a map azimuths of various legs of their routes to prevent getting lost. Map azimuths must then be converted to magnetic azimuths before they can be used with the compass. Having determined this magnetic azimuth, the leader holds his compass steady and turns it until required azimuth is read on the dial (fig. 53). He then sights along axis of the compass as described in *b*(3) above and selects a house, tree, rock, or other easily recognizable feature of the landscape on this line of sight. He then marches toward this selected feature until he reaches it or loses sight of it. He then takes another sight as described above and selects a new feature. This is repeated until he reaches his destination. Note that the compass is used to select successive features on the line of march and is not used when actually marching.

(2) *Night.*—For marching at night, movable index (c), luminous marks (j–j') on inside of cover, and azimuth scale on outside of case are used (fig. 50②). To march on given azimuth at night, set movable index at desired azimuth, rotate compass until needle points at movable index, and then select some feature on the skyline that is on the axis of the compass. March toward this selected feature. The axis of the compass can be determined by means of the luminous marks (j–j'). Setting the compass must be done in the light, usually by flashlight, screened from observation. On

very dark nights where the skyline is not visible, it may be necessary to send one man ahead to the limit of visibility, line him up on desired azimuth, and then walk toward him, repeating this as often as is necessary.

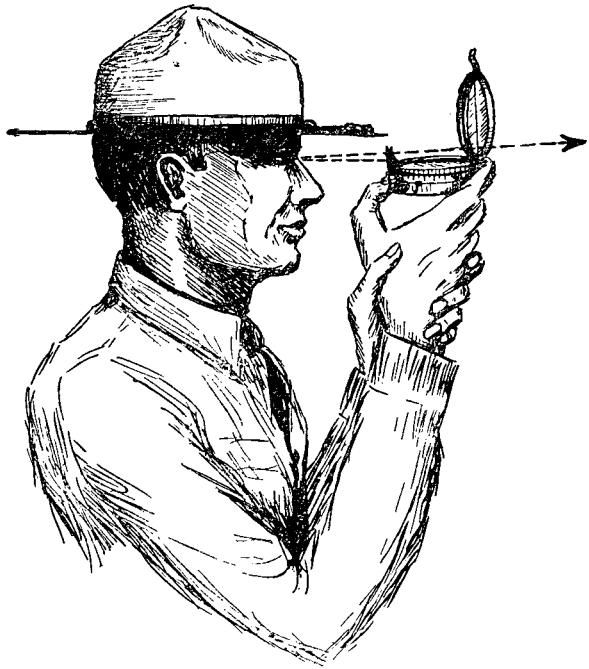


FIGURE 53.—Prismatic compass open and in position for measuring azimuth in daylight.

SECTION VIII

AERIAL PHOTOGRAPH READING

■ 39. GENERAL.—*a. Importance.*—Aerial photographs are used for many different purposes in connection with military operations. In this manual they are considered primarily in conjunction with or as substitutes for topographic maps. The

ideal situation is to have an accurate topographical map and a recent aerial photograph of the same area. During the first few days or even weeks in a new theater of operations there is a great possibility that the only up-to-date information of the terrain available would be that obtained from aerial photographs. They would be used in determining distances and directions, and in selecting routes in much the same manner as ordinary topographic maps.

b. Types.—(1) Vertical photographs are those made when axis of the camera is kept as nearly vertical as possible.

(2) Oblique photographs are those made when axis of the camera is deliberately tipped from the vertical.

(3) Composite aerial photographs are made with cameras having one principal lens and two or more surrounding and oblique lenses. The several resulting photographs are corrected or transformed in printing so as to permit assembly as verticals with the same scale.

c. Marginal data on aerial photographs.—(1) As aids in reading and use, aerial photographs used for photomaps will have information along the black strip at the bottom, reading from left to right, as follows:

(*a*) An arrow one-half inch in length in the lower left hand corner of the negative indicating north, with letter N superimposed over center of shaft.

(*b*) Name of locality or nearest locality.

(*c*) Approximate military grid coordinates of center of photograph.

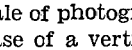
(*d*) Scale of photograph expressed as a representative fraction in case of a vertical, altitude above ground in feet and focal length of camera in case of an oblique.

(*e*) Hour.

(*f*) Date arranged in the following order: day, in figures; month, in letters; and year, in figures.

(*g*) Designation of squadron.

(*h*) Serial number of negative. In additon to a north point, the following is the legend on a vertical:



Saranac, N. Y.—(321–437)—1:20,000—(2:00 P.M.)—(24–Aug–40)—97th—M5. (See fig. 62.)

(2) Mosaics and wide coverage photographs may have in addition to that listed above the following information:

(*a*) Marginal information similar to that shown on maps such as the graphic scale in yards.

(*b*) Some system of grids, preferably the atlas grid described in paragraph 44.

(*c*) Names of important features such as towns, streams, mountains, highways, etc.

■ 40. OBLIQUE.—Normally in making obliques the photographs are taken over the side of the cockpit with the camera.

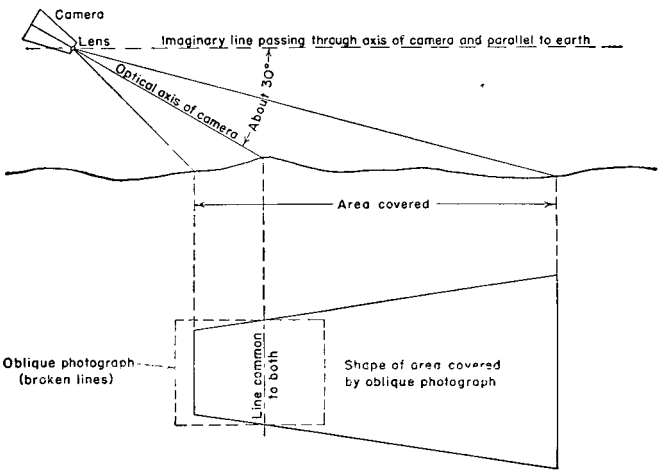


FIGURE 54.—Relative shape of area covered by oblique photograph compared to photograph itself.

intentionally tilted at an angle which will vary according to the mission, but is usually about 30° below the horizontal as shown in figure 54. This procedure gives what is known as a low oblique (fig. 55). Obliques which include the horizon are termed high obliques (fig. 56). Figure 54 also shows the relative shape of the area covered by an oblique photograph as compared to the photograph itself. Note the actual photograph is a rectangular print whereas the area covered by the photograph has the shape of a trapezoid and is much larger. Distances on oblique photographs cannot be scaled

①

FIGURE 55.—Low oblique.

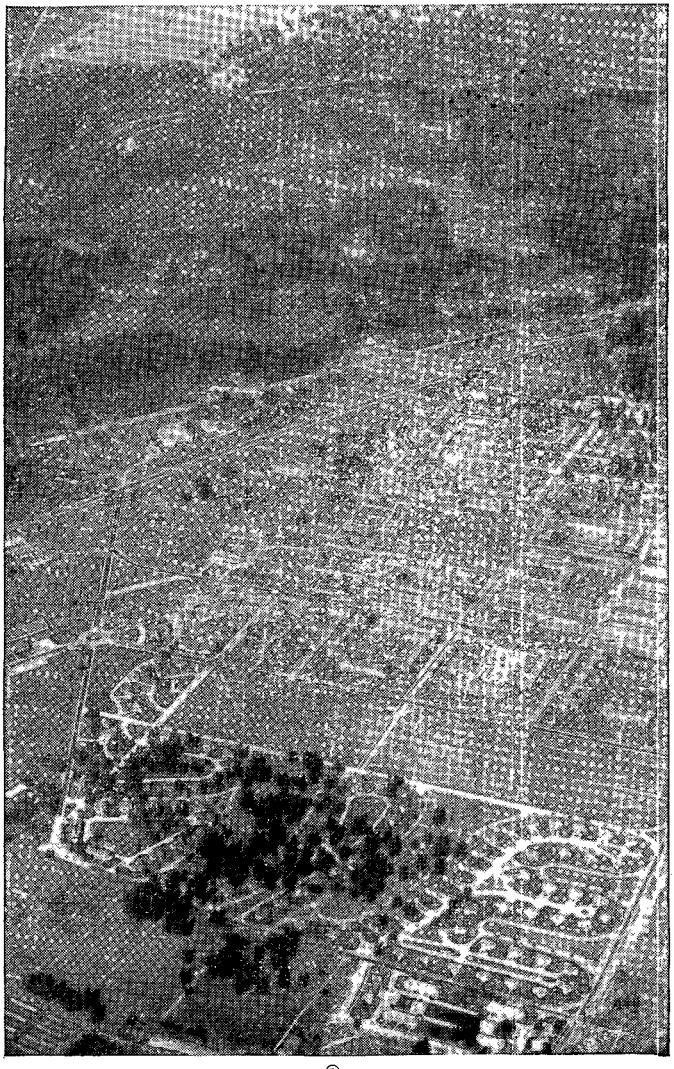


FIGURE 55.—Low oblique—Continued.

FIGURE 56.—High oblique.

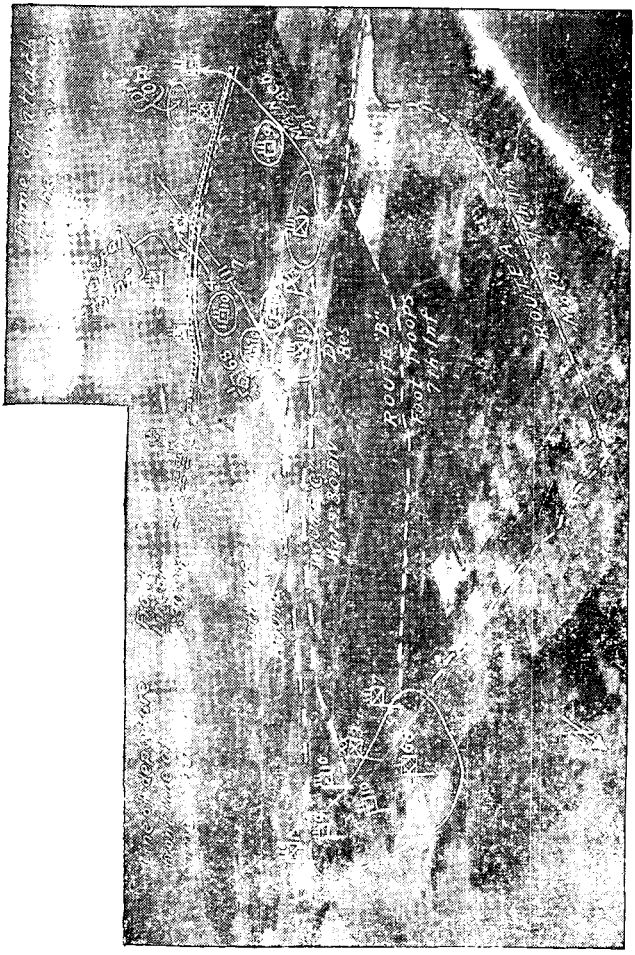
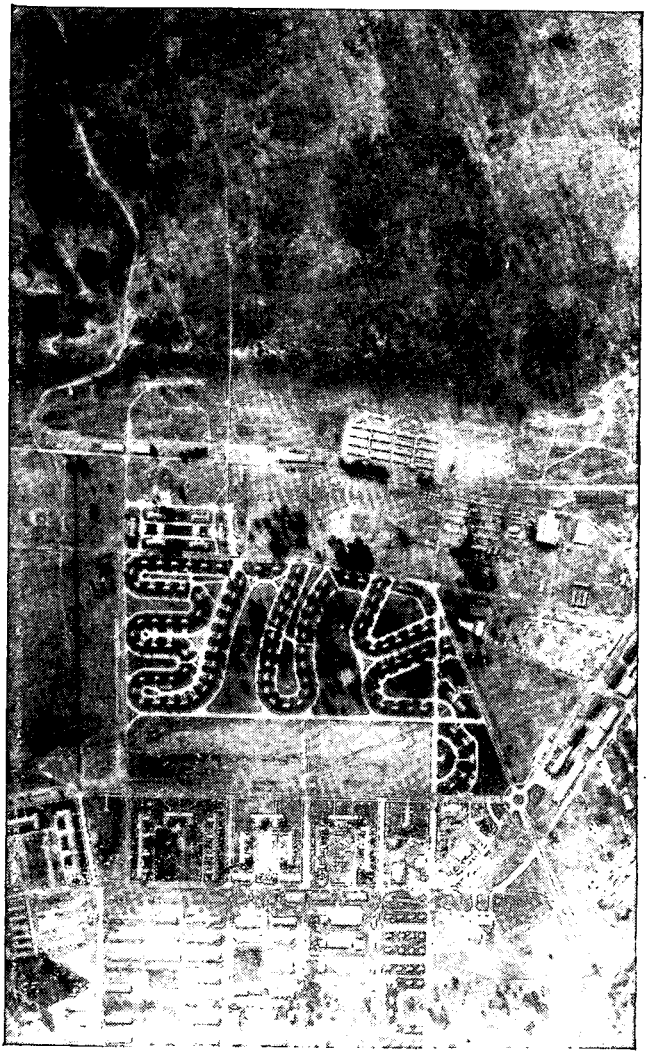


FIGURE 57.—Oblique photograph used as map substitute to accompany oral field order.

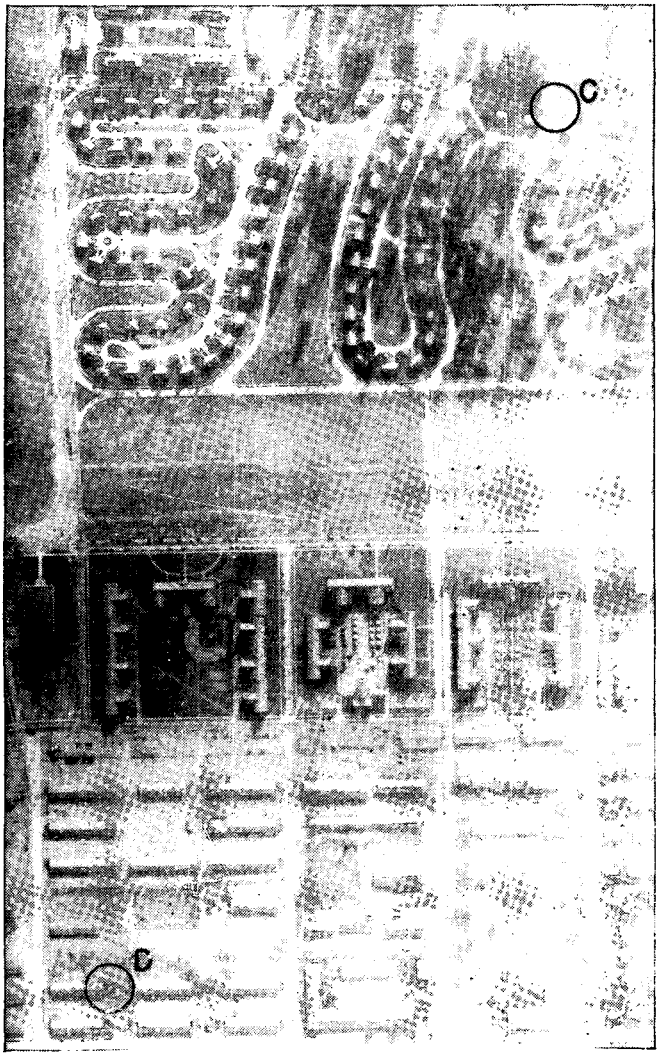
accurately. However, since the oblique picture is taken from a viewpoint similar to that of an observer on a high hill, terrain features have a more normal appearance than they do in a vertical; this characteristic makes them more useful for the study of hills, valleys, buildings, roads, etc. They can also be used to accompany operations or field orders. As shown in figure 57 it is possible to show the line of departure, routes from bivouac to assault positions, assembly positions, boundaries between units, objectives, and information of the enemy.

■ 41. VERTICAL.—Vertical photographs are usually taken through an opening in the floor of the airplane cockpit perpendicular to the surface of the earth. Each photograph covers a comparatively small ground area and shows the area somewhat as it would appear on a detailed map or sketch of similar scale. Figure 58 shows photographs taken from different altitudes of the same general area. Scale (RF) of each is given below it. Obliques of the area are shown in figure 55. Comparison of the areas covered for different scales should be made the subject of careful study. Figure 1 (back of manual) has these same areas outlined in heavy black lines. Learning to read a vertical photograph is similar to learning to read a map. It consists in being able to recognize familiar objects on the landscape from their appearance on the photograph, to orient the photograph, to determine its scale, and to determine distance and direction. A photograph however is not as easy to read as a map. Important features on a map are emphasized and always are shown in the same manner. On a photograph important features such as roads, railroads, bridges, and streams may appear less important than a great amount of unimportant detail, or may be completely hidden by trees or shadows. Dissimilar objects such as roads, railroads, and canals may look alike, and the same objects may appear to be different on various photographs or even on different parts of the same photograph. Also, a single vertical photograph unlike a topographic map contains no definite information of ground forms and elevations. Hills, ridges, and depressions are difficult to visualize unless an analysis of the drainage system within the area is made. Even

① Scale, 1:22,480.
FIGURE 58.—Vertical photograph.



⊙ Scale, 1:16,000 (approximate).
FIGURE 58.—Vertical photograph—Continued.



③ Scale, 1:7,813.
FIGURE 58.—Vertical photograph—Continued.

when this is done relative elevations are not apparent on the photograph. On the other hand, an aerial photograph is very valuable for the reasons that it—

a. Possesses in pictorial form a wealth of detail which no map can equal.

b. Can be prepared for use in a short time, much quicker than making a new map.

c. Is up to date.

d. Can be made of any area, even those inaccessible to ground mapping parties.

■ 42. IDENTIFYING TERRAIN FEATURES.—*a.* Identifying features of terrain on photographs requires a certain amount of practice which is best gained by actually comparing the photograph with the ground. When this is not possible, the next best method is to compare photographs with a good map of the same area. Actual identification of objects on an aerial photograph or on a mosaic is effected through one or more of the following means:

(1) Shape of object.

(2) Its tone, or relative colors from white through various shades of grey to black.

(3) Shadow it casts.

(4) Apparent or relative size.

b. In identifying features always hold the picture so the shadows are falling toward the body. Figure 59 shows several ground features numbered to correspond to the numbers of the subparagraphs below containing their description. When reading the description, look at figure 59 and note how reasons given for each identification apply.

(1) Plowed field looks light in the photograph because it reflects a relatively large amount of light.

(2) Meadow looks darker largely due to the shadows of the grass. The meadow is said to have more texture than the field. The difference between the meadow and the field is similar to the difference between satin and plush velvet. Although both are the same color, the plush looks darker due to the shadows of the hairs which stand erect, but it can be made to look lighter when smoothed down.

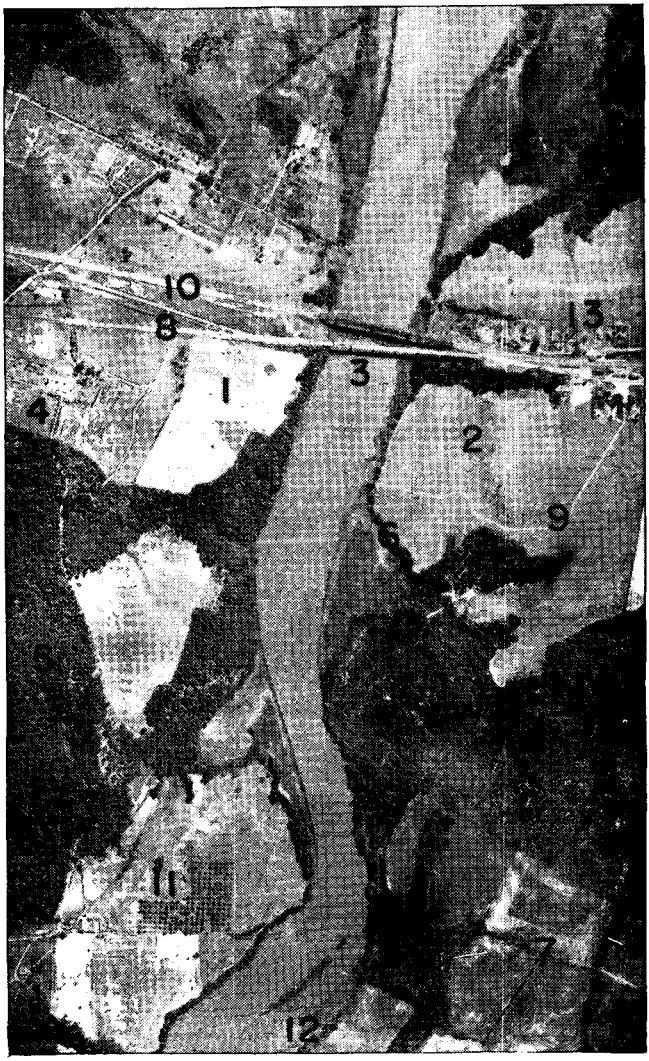


FIGURE 59.—Identification of terrain features.

(3) Bridge looks lighter than the water. It can be identified by its size, shape, and its shadow on the stream.

(4) Building can be identified by its size, shape, difference in appearance of the two roof slopes, and by its shadow. The shadow looks darker than the building.

(5) Woods appear relatively dark because of deep shadows of the trees. They have much texture and reflect little light.

(6) A stream can be identified by its meandering course. Even through open fields some trees or bushes usually grow along its banks. In a dense wood it will appear as a thinning out of the surrounding growth. The water looks very light or dark, depending upon the relative positions of sun, camera, and water.

(7) Fence lines are identified by difference in texture between fields they separate and usually look dark in the photograph because of shadows of bushes growing along them.

(8) Roads are identified by their straight lines, uniform width, and the fact that their surfaces are usually smooth and reflect much light. (Modern open asphalt texture surfaces will appear darker than other road surfaces.)

(9) Trails are also light but are more variable and narrow in width and more crooked than roads.

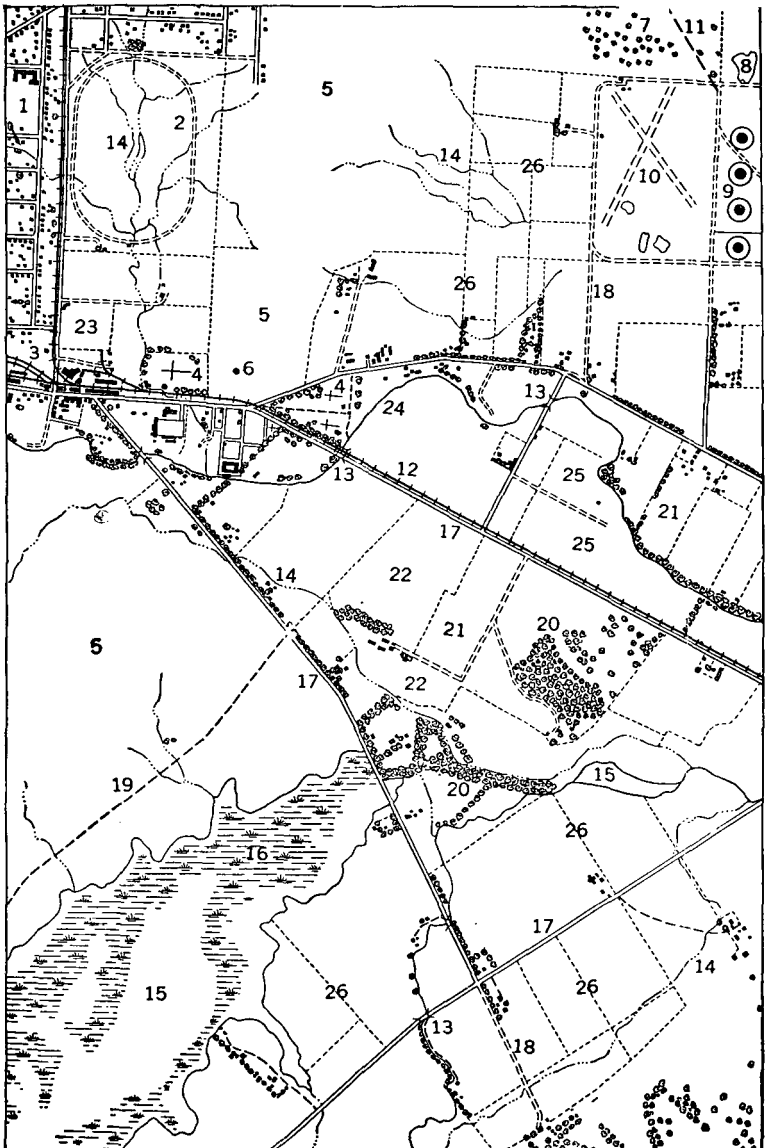
(10) Railroads have more gradual curves, are straighter, and darker in appearance than most roads.

(11) Orchard is identified by its shape and by the straight and regular rows of trees. Shadows of equal length show the trees are all of about the same height.

(12) Mud flats along the stream look darker than the water and have lighter spots in them due to pools of water.

(13) Cluster of buildings shows this is a village.

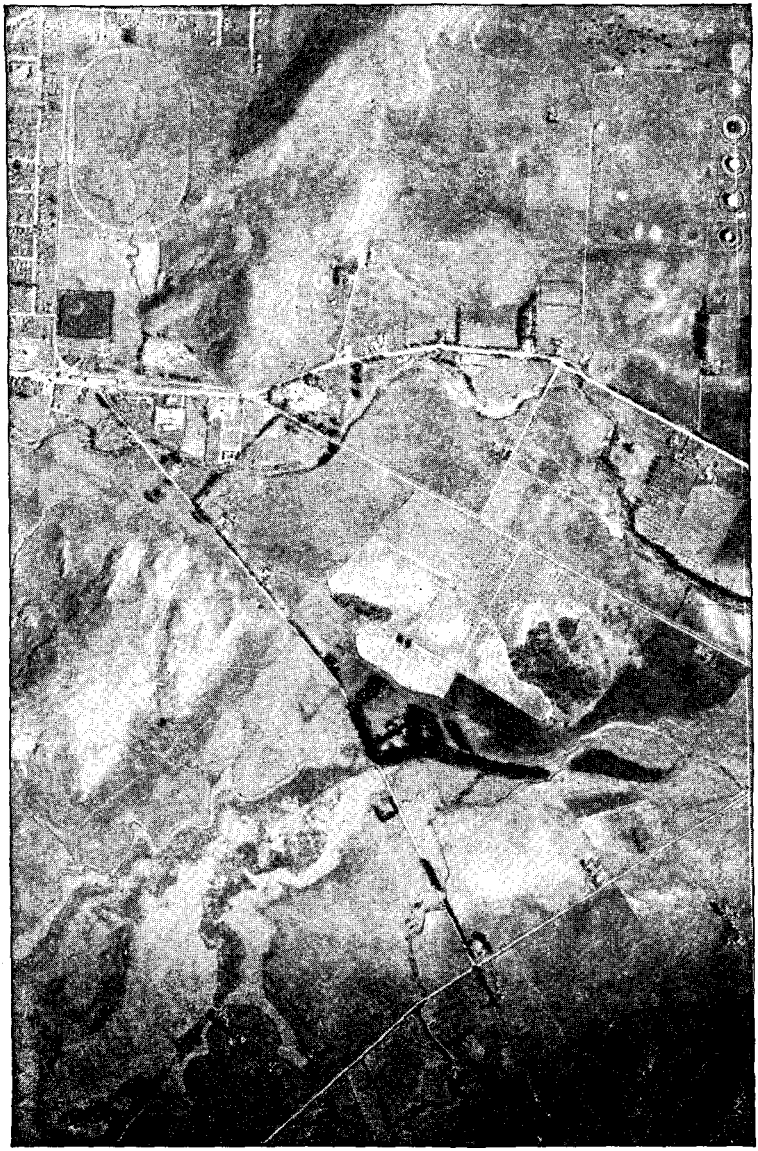
c. A careful study of figure 60 combined with a study of figure 58①, ②, and ③ compared with the map (fig. 1, back of manual) should make the student reasonably proficient in interpreting aerial photographs. It should be remembered that the pictorial effect of aerial photographs is influenced by shadow. In order that this effect will aid rather than hinder the student, he should place the photograph on a table between himself and a lamp, window, or other source of light, shifting it to avoid the glare from its surface and so that shadows on the photograph fall toward him. In this position



1. City; 2. Race track of fair grounds; 3. Railroad yards; 4. Cemetery; 5. Topography with low brush on hillside; 6. Concrete water tank; 7. Scattered wood; 8. Pond; 9. Oil tanks; 10. Airport with runways; 11. Oil pipe line; 12. Railroad; 13. Bridges; 14. Intermittent drainage; 15. Lake; 16. Marshes; 17. First class roads; 18. Secondary roads; 19. Trail; 20. Woods; 21. Orchards; 22. Vineyards; 23. Baseball park; 24. Streams; 25. Pasture; 26. Cultivated fields.

① Vertical aerial photograph.

FIGURE 60.—Interpretation of photographic detail.



② Map of area shown on photograph.

FIGURE 60.—Interpretation of photographic detail—Continued.

objects will have their normal appearance. If the photograph is reversed, that is, placed so that the shadows fall away from the student, actual hollows may appear as hills and trees as holes in the ground.

■ 43. ORIENTATION.—*a. With map.*—(1) When the photograph is used in conjunction with a map it should be oriented with the map. Maps are printed with the north of the map at the top and all lettering, grids, etc., are added on that basis. However, no attempt is made to take photographs to fit this scheme. Photographs may be received without any lettering or direction arrow for orientation. Consequently it may be necessary to study the photograph and identify objects to use in orienting it. When objects shown on the map are found on the photograph it is a simple matter to orient the photograph with respect to the map. Road systems and streams are useful for this purpose. A magnetic north line should then be drawn on the photograph parallel to that on the map.

(2) Another method of drawing the magnetic north line on a photograph is to select two points on the photo that can also be easily identified on the map. The points should be fairly far apart, and the line joining them should pass close to the center of the photograph (points A and B, fig. 58①). Measure on map azimuth of line joining these points. Convert this azimuth to magnetic azimuth. In figure 1 (back of manual) magnetic azimuth of the line A to B is 328°30′. Lay protractor on the photograph (fig. 61) with center of protractor at A and line AB cutting the 328°30′ reading. The base line of the protractor is now lying on magnetic north and south line with north toward the 360° reading. A line with N arrow is drawn parallel to this where desired on the photograph. Further details of this process are given in FM 21–26.

b. With ground.—A photograph may be oriented with the ground by placing some well-defined line as a road on the photograph parallel with the same line visible on the ground. This is similar to the orientation of the map described in paragraph 34b. The same method is used in locating

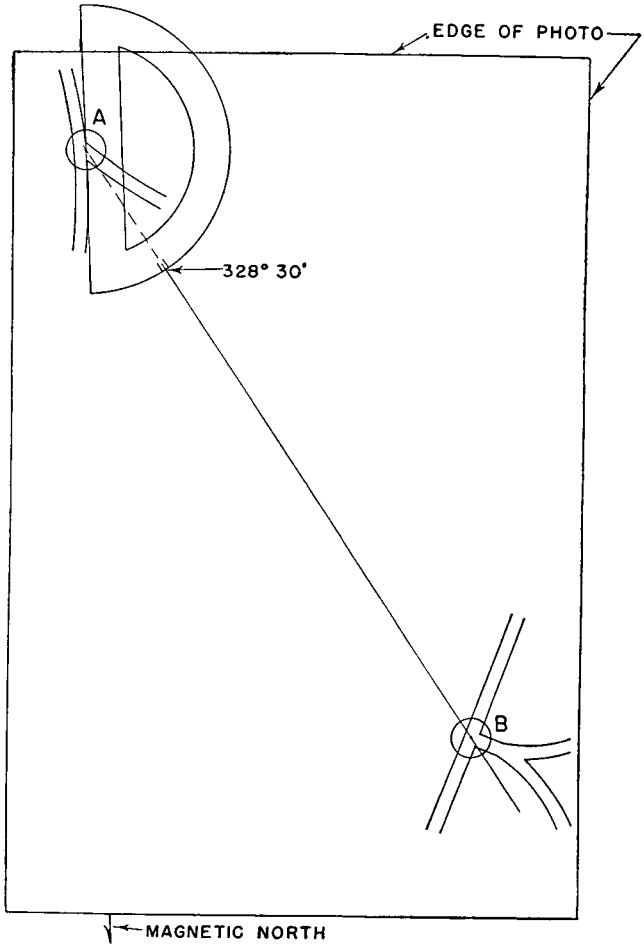


FIGURE 61.—Determining magnetic north on a photograph.

observer's position on a photograph as is used on a map (see par. 35).

c. By shadow.—There may be times when an observer in the field finds it impossible to orient a vertical aerial photograph by either of the above two methods. A third method of rough orientation by use of shadows can be used. In the northern hemisphere shadows fall to the northwest in the morning and to the northeast in the afternoon. Assume the photograph is taken between the usual hours for aerial photography, that is, 10:00 A.M. to 2:00 P.M. The photograph is laid on the ground with the shadows pointing slightly west of north if the photograph was taken in the morning or slightly east of north if taken in the afternoon. The photograph is then approximately oriented. If the exposure is before 10:00 A.M. or after 2:00 P.M., the photograph must be turned west or east of north a correspondingly greater distance.

■ 44. ATLAS GRID.—Because of variations in scale, other inaccuracies, and difficulty of locating grid lines, the military grid is not used on photographs or uncontroled photomaps. The atlas grid is used instead with grid lines always 1.8 inches apart regardless of the scale. With this interval, on a 1:20,000 photograph the grid lines are about 1,000 yards apart. The lines are numbered from the bottom up, and lettered from left to right. Starting at the left edge, the first line is A, the second B, etc. Starting at the bottom the first line is 1, second 2, etc. Therefore, the origin of coordinates at the lower left-hand corner of the photograph is (A.0–1.0) (fig. 62). Points can be located accurately by decimals of the grid interval. For instance, the decimal coordinates of point P would be written (C.5–4.2).

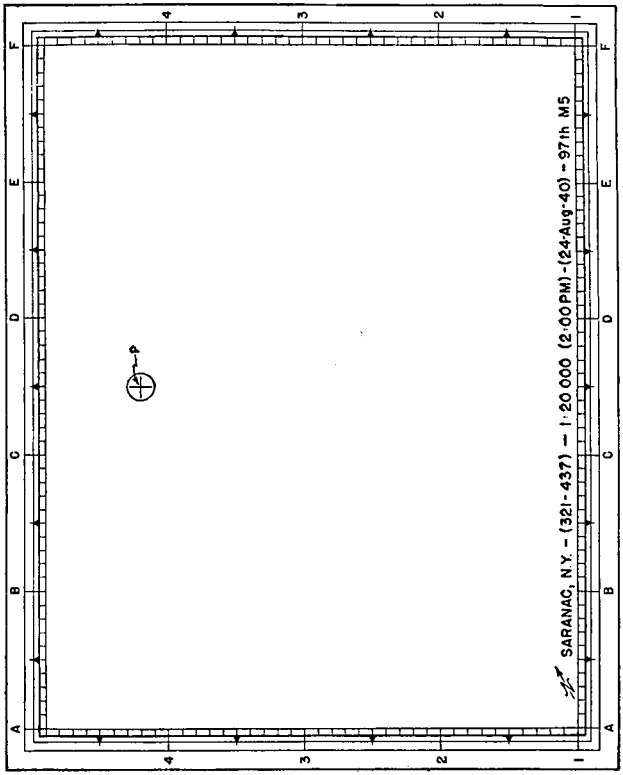


FIGURE 62.—Atlas grid and marginal data.

■ 45. SCALE.—Customarily photographs intended to be used as substitutes for maps will be marked as shown in paragraph 39c. However, they may be received without complete information as, for example, with the scale omitted. In this case the scale must be determined by some other method.

a. By focal length and altitude.—In certain instances, the focal length and altitude at exposure may be shown. This information would appear in the marginal data as follows: (12''-20,000'). This means that the picture was taken with

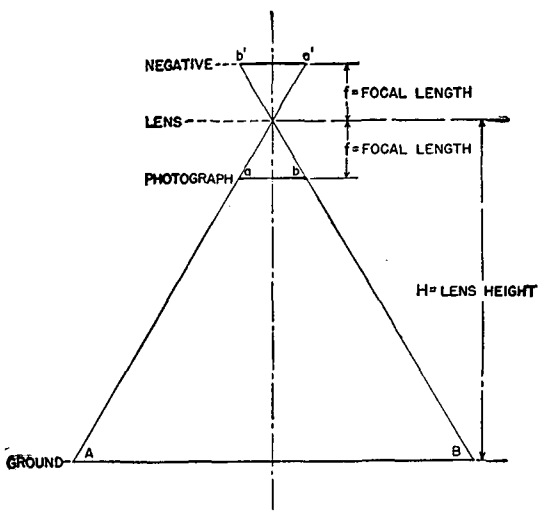


FIGURE 63.—Diagram showing relation of scale, focal length, and lens height.

a camera focal length of which was 12 inches and was 20,000 feet above the ground at time of exposure. By inspection of figure 63 it may be seen that there is a direct relation between focal length of the camera, height of the plane, ground distance AB and corresponding distance ab on the photograph or

$$\frac{f}{H} = \frac{ab}{AB} = RF.$$

If the focal length is 1 foot (12 inches) and the altitude of the plane is 20,000 feet, then the scale of the photograph will be $\frac{1}{20,000}$ or RF=1:20,000. If the focal length had been 6 inches, then the scale would have been $\frac{6/12}{20,000}=\frac{1/2}{20,000}=\frac{1}{40,000}$ or RF=1:40,000. Hence the general expression or formula is:

$$RF=\frac{\text{focal length in feet}}{\text{height of plane in feet}}$$

In some cases the altitude given is the elevation above sea level, and not the elevation above the ground. If the average ground elevation is much above sea level, allowance must be made for this by reducing the plane's height by the elevation of the ground. For instance, in the example given just above, if the elevation of the ground had been 2,000 feet and the altitude given had been the elevation above sea level, the RF would have been actually $\frac{1/2}{20,000-2,000}=\frac{1}{36,000}$ or 1:36,000 instead of 1:40,000.

b. By comparison with map or ground distance.—The average scale of the photograph may be computed by comparison of the distance between two points on the photograph with corresponding distance between the same points on the ground or on a map. For best results the points chosen should be located on the photograph so that straight lines joining them pass fairly near to the center and well across the face of the photograph. For accurate determination see FM 21–26. If required to find the scale of the photograph in figure 58① by comparison with the map in figure 1 (back of manual), select two points such as A and B, that are easily recognizable both on the photograph and on the map. Measure the distance between them both on the photograph and on the map. In this case the map distance is 5.62 inches which on the ground would be 5.62×20,000=112,400 inches since the scale of the map is 1:20,000. Assume the distance between points A and B on the photograph is 5.0 inches. Since it is known that the distance on the ground is 112,400 inches then the RF of the photo is $\frac{5}{112,400}=\frac{1}{22,480}$ or 1:22,480.

Now suppose it is required to find the scale of the photograph in figure 58③ by comparison with the map in figure 1 (back of manual). Select two points such as C and D that can be easily identified both on the photograph and on the map. Proceed as above and in this case the map distance is 2.09 inches which would be $2.09 \times 20{,}000 = 41{,}800$ inches on the ground. Measure the distance CD on the photograph. Assume it is 5.35 inches. Therefore the RF of the photograph is $\frac{5.35}{41{,}800} = \frac{1}{7{,}813}$ or 1:7,813. Note that in both examples, points were selected so that lines connecting them passed close to the center of the picture and that the points were far apart, practically in opposite corners.

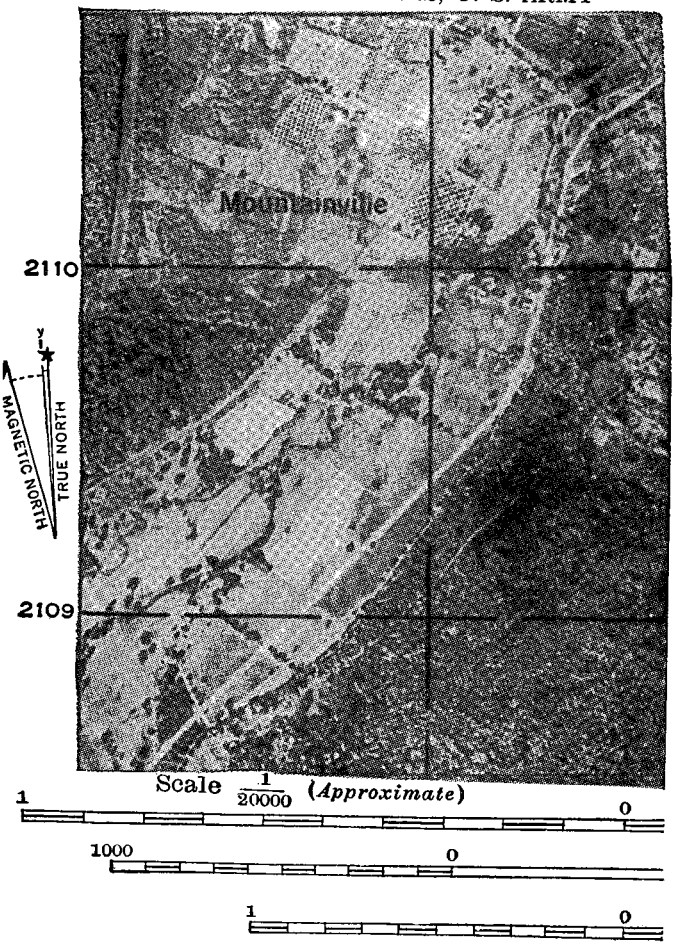
■ 46. MOSAIC.—A mosaic consists of several overlapping vertical photographs joined together. When these photographs are oriented with respect to each other by matching detail in the overlap or along the border, the result is an uncontrolled mosaic which gives a good pictorial effect of the ground but may contain considerable errors in scale and direction. When the several photographs are oriented by means of points along the line of flight and adjusted on previously selected ground points, the result is a controlled mosaic. The controlled mosaic is more accurate and for many purposes is as useful as a map. When several photographs taken from a single airplane flight are joined, the result is a strip mosaic. Strip mosaics are commonly used in the early stages of combat as they are quickly made and give a fairly accurate representation of a more or less extended but narrow section of the terrain.

■ 47. PHOTOMAP.—The term photomap is used as a general term to denote reproductions of vertical aerial photographs, composites, or aerial mosaics. On maps and aerial photographs or photomaps for military usage, roads, railroads, towns, streams, wooded and open areas, and relief are of main interest. Relief is not apparent on any photographs unless there is an overlapping pair that can be seen stereoscopically or unless the photograph is ridge lined and stream lined as described in paragraph 29. Figure 64 is a reproduction of a photomap of about the type which may be expected in the

PHOTO MAP

WAR DEPARTMENT

CORPS OF ENGINEERS, U. S. ARMY



WEST POINT AND VICINITY

FIGURE 64.—Photomap.

field. Although at first glance this photomap appears somewhat indistinct and blurred, those important features referred to above can be seen easily. For example, there is a fairly open valley running from the lower left-hand corner to the upper right-hand corner. There is a stream meandering up the center of this valley. A main highway with several secondary roads runs along its southeastern edge. A railroad, readily identified by means of its long tangents and gradual curves, runs along the northwestern edge of the valley. Several orchards in the vicinity of the town of Mountainville can be picked out. Thus it may be seen that the works of man and changes in wooded and cleared areas are easily seen on a photomap. These are the factors that tend to make a map out of date. The relief as shown on old maps will still be accurate as the ground forms change very slowly. Therefore an up-to-date photomap with any topographic map, whether up to date or not, will give reliable information to the map reader.

■ 48. STEREOVISION.—*a. General.*—The ordinary photograph, as mentioned in paragraph 41, has a flat appearance, which makes it difficult to distinguish between hills and valleys. If two overlapping photographs, known as a stereopair, are viewed either with the naked eyes or with some type of stereoscopic instrument, the effect of depth or relief will be seen and ability had to recognize the actual ground forms. This type of study gives valuable training in understanding and reading both single vertical photographs and photomaps. Consequently, all military personnel should learn and practice stereovision. There are several methods that will assist in acquiring this ability and each individual should experiment until he finds the method that gives him the best results. This ability comes very quickly to most; others will have to use patience and perseverance to obtain it. Experience with large groups of men reveals that anyone with good enough eyes to be in the Army can acquire the ability to see stereoscopically. Stereo studies properly done put no strain on the eyes, and some oculists even prescribe similar exercises to strengthen the eyes. However, when using magnifying spectacles, they should be removed from the eyes before looking up from the photographs.

b. Anaglyph.—Beginners in stereo studies often have difficulty in getting the effect of relief by means of aerial photographs. A simple method of illustrating stereovision is by means of the anaglyph. The anaglyph consists of two different photographs of the same area printed on the same sheet but slightly offset. One is printed in red and the other in blue or green. Relief can be seen when this anaglyph is viewed through a pair of colored spectacles. If the spectacles are reversed or the print is turned upside down, the relief is reversed and ridges will appear as valleys and valleys as ridges. The anaglyph has no practical military value and is used as a quick aid to beginners to illustrate the effects to be obtained by practice in stereovision. For an illustration of an anaglyph see TM 5–230.

APPENDIX

LIST OF REFERENCES

■ 1. MAPS AND MAPPING.—*a.* General publications covering coordination of military maps and mapping:

AR 300–15, Military Maps and Mapping.
FM 30–20, Military Intelligence, Military Maps.
FM 30–21, Military Intelligence, Role of Aerial Photography.

b. Publications of a general nature pertaining to maps and mapping:

FM 21–26, Advanced Map and Aerial Photograph Reading. (Now published as TM 2180–5.)
FM 21–30, Conventional Signs.
FM 21–35, Sketching.

■ 2. CORPS OF ENGINEERS.—Publications pertaining to Corps of Engineers in performance of their mapping duties:

FM 5–5, Engineer Troops.
TM 5–230, Topographic Drafting.
TM 5–235, Surveying.
TM 5–236, Surveying Tables.
TM 5–240, Aerial Photographic Mapping. (Now published as TR 190–27.)
TM 5–245, Map Reproduction in the Field. (Now published as TM 2180–37.)
TM 5–300, Symbols for Seacoast Defense, Fire-Control Maps, Diagrams, and Structures. (Now published as TR 1050–5.)

■ 3. OTHER ARMS.—Publications pertaining to duties of other arms in reference to military maps and mapping:

FM 1–30, Air Navigation.
FM 1–35, Aerial Photography.
TM 1–220, Aerial Photography.
TM 6–200, Field Artillery Survey.

	Paragraphs	Pages
Aerial photographs:		
Atlas grid	44	88
Identifying features	42	81
Marginal data	39	70
Oblique	40	72
Orientation	43	86
Type	39	70
Vertical	41	77
Anaglyphs	48	94
Atlas grid	44	88
Azimuth:		
Back	15	20
Grid	15	20
Measuring	18	26
Magnetic	15	20
Plotting	19	27
Type	15	20
Bearing	16	24
Compass:		
Lensatic	38	63
Measuring azimuths	38	63
Prismatic	38	63
Type	38	63
Use at night	38	63
Watch	11	15
Contours	26	36
Characteristics	26	36
Determining elevations	27	42
Emphasizing	29	46
Logical	26	36
Conventional signs	6	3
Coordinates	21	29
Grid	23	31
Polar	22	29
Scale	24	33
Declination	14	19
Grid	14	19
Magnetic	14	19
Use	14	19
Direction	11	15
Angular	12	15
Base	13	17
Distance	9–37	12, 63
Along irregular lines	9	12
Between two points	9	12
Conversion of march time to	10	14
Elevation:		
Determination from contours	27	42
Means of representing	25	35
Finding position by:		
Inspection	35	59
Resection	35	59
Striding or estimation	35	59
Grades	30	48

	Paragraphs	Pages
Ground forms:		
Representation by hachures	28	46
Representation by contours	26	36
Ridge lining and stream lining	29	46
Hachures	28	46
Location:		
Coordinates	21	29
Intersection	20	27
Position on map	34	54
Resection	20	27
Maps:		
Battle	4	2
Classification	5	2
Scale	8	11
Substitutes	4, 41, 46, 47	2, 77, 92
Map orientation:		
Compass	34	54
Distant points	34	54
Inspection	34	54
Map reading	33	54
Military symbols	7	7
Mosaics	46	92
Oblique	40	72
Orientation of maps. *See* Map orientation.		
Photomaps	47	92
Profiles:		
Drawing	31	49
Hasty	32	51
Vertical scale	31	51
Rates of march	10	14
Relief:		
Contours	26	36
Ridge lining and stream lining	29	46
Representative fraction	8	11
Resection	35	59
Ridge lining and stream lining	29	46
Scales:		
Map:		
Coordinates	24	33
Graphic	8	11
Photograph:		
Focal length and altitude	45	90
Map or ground distance	45	90
Slopes	30	48
Stereovision	48	94
Anaglyphs	48	94
Terrain features, military terms	36	61
Time measurement:		
Distance to march time	10	14
March time to distance	10	14
Vertical photographs	41	77
Visibility:		
Hasty profile	32	51
Inspection	32	51
Profile	32	51

WAR DEPARTMENT
CORPS OF ENGINEERS, U. S. ARMY

GRID ZONE "G"

(Allyn) (Gig Harbor) (Tacoma) 1:125000

SHELTON & U. S. HY. 36 MI.
GIG HARBOR 21 MI.
HOME 2 MI

PT DEFIANCE 4 MI.
CITY CENTER 3.8 MI.

122°45' 47°15' R1E 40' 35' R2E 122°30' 47°15'

2820 2815 T20N 2810 2805 T19N 2800 2795000 T18N

CARR INLET

PUGET SOUND

DRAYTON PASSAGE

PITT PASSAGE

BALCH PASSAGE

PASSAGE

CORMORANT PASSAGE

NISQUALLY REACH

Wyckoff Shoal

Toliva Shoal

Still Harbor

Filuce Bay

Hale Passage

Amsterdam Bay

Carson Bay

East Oro Bay

Oro Bay

Thompson Cove

Henderson Bay

Nisqually Flats

Titlow Lagoon

Chambers

Sequalichew Lake

Steilacoom Lake

Mud Lake

Lake Louise

Gravelly Lake

Clover Park

Lake City

Tacoma

Steilacoom

Tillicum

Fircrest

Fircrest Golf Club

Regent Park School

Belmarlow

Day I

Hope

Fox Pt

Toy Pt

Gibson Pt

Sunset Beach

New Tacoma Cem

Meadow Park Golf Club

Calvary Cem

Pitt I

Mahnckes Pt

McNEIL ISLAND

FEDERAL PENITENTIARY

Gertrude I

Hyde Pt

McDERMOTT LT

Eagle I

Otso Pt

DRAYTON LT

Yoman

Yoman Pt

Gordon Pt

Kerton Island

Sandy Pt

ANDERSON ISLAND

Treble Pt

Cole Pt

Vega

Tatsolo Pt

Lyle Pt

Prison Wharf

Proposed Cable Area

Cable Area

Anderson Island Ferry Dock

Steilacoom Ferry

6th Ave Ferry

Du Pont Dock

Longbranch 1.5 mi.

Olympia 7 mi.

Tacoma 6.4 mi.

Tacoma City Center 8.5 mi.

Olympia 13 mi.

Yelm 7 mi.

McKenna 3 mi.

Loveland 5.9 mi.

Tenino 1:62500
(Chehalis 1:125000)

(Olympia)

(Yelm 1:62500)
(Chehalis 1:125000)

(Tacoma South 1:62500)
(Eatonville 1:125000)

Tanwax Lake 1:62500
(Eatonville 1:125000)

Prepared under the direction of the Chief of Engineers, U. S. Army, 1939.
Control by U. S. Coast and Geodetic Survey, 1924 and 1935, U. S. Geological Survey, 1912 and 1934 and 29th Engineers, U. S. Army, 1937-38.
Topography by 29th Engineers, U. S. Army, 1939, using multiplex aero projectors. T-3 A (five-lens) photography by 91st Observation Squadron, Air Corps, U. S. Army, 1938.
Polyconic Projection, North American Datum 1927.

Scale 1/62500

1 0 1 2 3 4 Miles

1000 500 0 1000 2000 3000 4000 5000 6000 7000 Yards

1500 0 3000 6000 9000 12000 15000 18000 Feet

1 0 1 2 3 4 5 Kilometers

Contour interval 20 feet
Datum is mean sea level (1929 Adj.)

FIVE THOUSAND YARD GRID COMPUTED FROM "GRID SYSTEM FOR PROGRESSIVE MAPS IN THE U. S." ZONE G, U. S. C. & G. S. SPECIAL PUBLICATION NO 59
(THE LAST THREE DIGITS OF THE GRID NUMBERS ARE OMITTED.)

NOTE: OFFICERS USING THIS MAP WILL MARK HEREON CORRECTIONS AND ADDITIONS WHICH COME TO THEIR ATTENTION AND MAIL DIRECT TO "THE CHIEF OF ENGINEERS, WASHINGTON, D. C."

ARMY MAP SERVICE, U. S. ARMY, WASHINGTON, D. C., 200137

GRID NORTH 24°03' MAGNETIC NORTH 1°12'

APPROX. MEAN DECLINATION 1937
ANNUAL MAG. CHANGE 2' DECREASE

ROUTES USUALLY TRAVELED
HARD IMPERVIOUS SURFACES
OTHER SURFACE IMPROVEMENTS
1939
U. S. ROUTE
STATE ROUTE

FIG. 1

FIGURE 2. MEDIUM SCALE MAP

Woods

Cut-over areas

GRID ZONE "G"

FIG. 58

FIG. 62

FIG. 61

FIG. 57

Sequallitchew Lake

Hamer Marsh

Edmond Marsh

Mac Kay Marsh

Wright Marsh

Shannon Marsh

Strickland Lake

Pond Lake

Grant Lake

Sellers Lake

Hanna Lake

Bell Marsh

Spring

Dupont

Green Park

Davis Hill

Bell Hill

Mead Hill

Bare Hill

Beal Hill

Crossland Hill

Foster Hill

Bracken Hill

Holman Hill

Travis Hill

Goodman Hill

Elwood Hill

Donovan Hill

Harlow Hill

Crook Hill

Hale Hill

Ware Hill

Boyd Hill

Kelly Hill

Swift Hill

Newman Hill

Sanders Hill

Carr Hill

Evans Hill

WOODS

CAMPBELL WOODS

GORDAN WOODS

CRAMER WOODS

BELL WOODS

DAVIS WOODS

ARGONNE FOREST

RESERVATION BOUNDARY

PACIFIC HIGHWAY

STEILACOOM 3.0 MI.

TACOMA 14.4 MI.

DUPONT STEILACOOM ROAD

SMITH ENGINEER BLUFF ROAD

PUMPING PLANT

4TH OF JULY HISTORICAL MONUMENT

WATER SUPPLY

Dupont Sch

Federal Prison Camp

WATER TANKS

2806 2805 2804 2803 2802 2801 2800 2799

863 864 865 866 867 868

2798000 863000

39′ 38′ 37′ 122°36′ 47°07′ 06′ 05′ 47°04′

Scale 1/20000

1 0 1 Mile

1000 0 1000 2000 Yards

1 0 1 Kilometer

Contour interval 20 feet

Datum is mean sea level (1929 Gen. Adj.)

ONE THOUSAND YARD GRID COMPUTED FROM "GRID SYSTEM FOR PROGRESSIVE MAPS IN THE U. S." ZONE G. U. S. C. & G. S. SPECIAL PUBLICATION NO. 59

NOTE: OFFICERS USING THIS MAP WILL MARK HEREON CORRECTIONS AND ADDITIONS WHICH COME TO THEIR ATTENTION AND MAIL DIRECT TO "THE CHIEF OF ENGINEERS, WASHINGTON, D. C."

FIGURE 1. LARGE SCALE MAP

Prepared under the direction of the Chief of Engineers, U. S. Army, 1939.
Control by U. S. Coast and Geodetic Survey, 1924 to 1935, U. S. Geological Survey, 1912 to 1934 and 29th Engineers, U. S. Army, 1937-38.
Topography by 29th Engineers, U. S. Army, 1939, using Multiplex Aero Projectors.
T3-A (5 lens) photography by 91st Observation Squadron, Air Corps, U. S. Army, 1938.
Polyconic Projection, North American Datum 1927.

ROUTES USUALLY TRAVELED

HARD IMPERVIOUS SURFACES

OTHER SURFACE IMPROVEMENTS

1940

3 U. S. ROUTE

73 STATE ROUTE

Y

23°58′

1°12′

GRID NORTH

MAGNETIC NORTH

APPROX. MEAN DECLINATION 1937

ANNUAL MAG. CHANGE 2′ DECREASE

ARMY MAP SERVICE, U. S. ARMY, WASHINGTON, D. C., 200137

MHI
Copy 3

FM 21-26

WAR DEPARTMENT

BASIC FIELD MANUAL

ADVANCED MAP AND AERIAL PHOTOGRAPH READING

September 17, 1941

FM 21-26

BASIC FIELD MANUAL

ADVANCED MAP AND AERIAL PHOTOGRAPH READING

Prepared under direction of the
Chief of Engineers

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1941

For sale by the Superintendent of Documents, Washington, D. C.

WAR DEPARTMENT,
WASHINGTON, September 17, 1941.

FM 21–26, Advanced Map and Aerial Photograph Reading, is published for the information and guidance of all concerned.

[A. G. 062.11 (5–15–41).]

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
Chief of Staff.

OFFICIAL:

E. S. ADAMS,
Major General,
The Adjutant General.

DISTRIBUTION:

D (3); B 1, 2, 4, 6, 7, 17 (2); R 1–7, 10, 17 (5); Bn 1 (10), 2–7, 11, 17 (5), 9, 10 (2); C 2, 5–7, 17 (10), 1, 3, 4, 9–11 (5).

(For explanation of symbols see FM 21–6.)

TABLE OF CONTENTS

		Paragraphs	Page
SECTION I.	General	1–9	1
II.	Distance	10–15	10
III.	Direction, orientation, and location	16–28	20
IV.	Coordinates	29–38	41
V.	Elevation and relief	39–48	61
VI.	Slope, profile, and visibility	49–60	73
VII.	Aerial photographs	61–75	87
VIII.	Identification of terrain features on single photograph	76–88	113
IX.	Stereovision and examination	89–93	129
X.	Preparation of aerial photographs for use as map substitute	94–114	148
XI.	Photomaps	115–120	175
INDEX			183

BASIC FIELD MANUAL

ADVANCED MAP AND AERIAL PHOTOGRAPH READING

(This manual supersedes TM 2180–5, September 28, 1938.)

SECTION I

GENERAL

■ 1. PURPOSE.—The purpose of this manual is to provide a text on map and aerial photograph reading for training of military personnel already familiar with basic elements covered by FM 21–25 or who require more detailed instruction than is furnished by FM 21–25.

■ 2. SCOPE.—Sections I to VI, inclusive, cover an exposition of factors and methods employed in map reading. Sections VII to XI, inclusive, provide an extension of these factors and methods into the related field of aerial photograph reading. The large-scale aerial photograph, within its characteristic limitations, is the logical complement of the small-scale map. Knowledge of the characteristics of aerial photographs and proficiency in the basic art of map reading are prerequisites to proficiency in aerial photograph reading.

■ 3. DEFINITION.—A map is a conventional representation of a portion of the surface of the earth as a plane surface. Since a spherical surface cannot be reproduced as a plane with absolute accuracy, the representation is approximate only, with characteristics dependent upon the projection employed.

■ 4. PROJECTION.—*a. Shape of earth.*—Theoretically, the earth is an oblate spheroid in shape; a figure formed by rotating an ellipse around its shorter axis. Because of the continents and islands, the actual surface is slightly irregular. The distance from the center of the earth to a point at sea level on the Equator is 3,963.3 statute miles and the distance from the center of the earth to either of the poles at sea level is 3,950 statute miles. This difference is so slight that the earth may be mentally pictured as a round ball

or sphere which rotates on a line or axis passing through its center. The imaginary intersections of this axis with the surface of the earth are called the North and South Poles. Circles on the earth's surface, cut by imaginary planes passing through the poles, are called meridians of longitude (fig. 1). Circles cut by imaginary planes at right angles to the axis are callel parallels of latitude. The parallel midway between the poles is called the Equator and

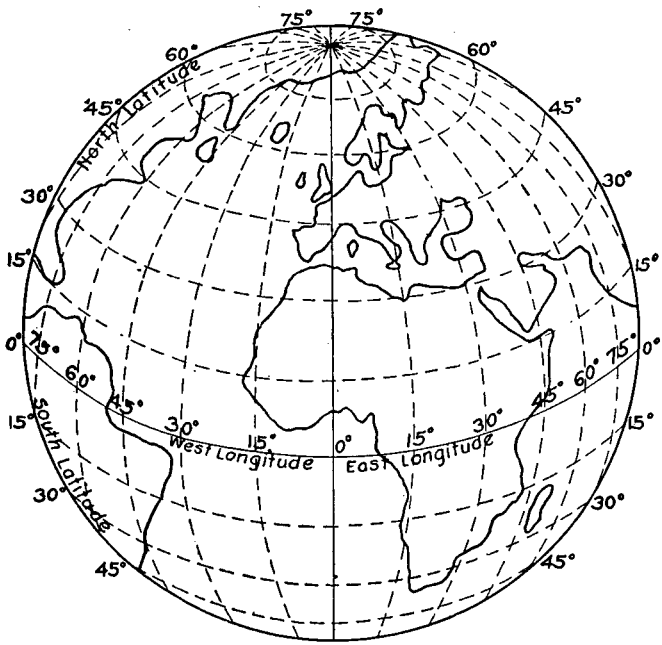


FIGURE 1.—Globe showing meridians and parallels.

divides the earth into the Northern and Southern Hemispheres.

b. Latitude and longitude.—Latitude is expressed by the number of degrees north or south of the Equator, the Equator being 0° and the poles 90°. Points in the Northern Hemisphere have north latitude and in the Southern Hemisphere, south latitude. The meridian of longitude through the

Greenwich Observatory, London, England, has been adopted as 0°. Longitude is measured east or west of the Greenwich meridian to 180°. All points in North and South America have west longitude. (See fig. 1.)

c. Projection.—A map is a representation of a portion of the earth's surface on a plane, and since the earth is a spheroid whose surface is incapable of development as a plane, it is obvious that a map cannot depict a portion of the earth's surface exactly. It is customary in constructing maps to project the portion of the earth's surface under consideration to a surface which is capable of being developed into a plane. A system of developed lines designed for the purpose of constructing a map on a plane surface is called a projection. There have been many kinds of projections devised, all of which may be classified either as equal area, conformal, azimuthal, perspective, or some compromise between these. For further explanation of projection, see TM 5–230.

d. Mercator's projection.—There are several projections based upon a cylinder tangent to the earth along the Equator. That invented by Mercator and known by his name has the latitude scale distorted to equal the stretching in longitude that takes place in developing the sphere upon the cylinder. This distortion is zero at the Equator and infinite at the poles. Due to the rapid distortion when nearing the poles, Arctic land areas such as Greenland are greatly out of proportion. Mercator's projection is used in instrumental navigation, and is the standard projection for hydrographic charts (U. S. Navy), Navy air navigation charts, and Army long distance air navigation charts of small scale.

e. Polyconic projection (fig. 2).—The system adopted for the production of military maps is known as the polyconic projection. On the polyconic projection each parallel of latitude is the developed base of a right cone tangent to the spheroid along that parallel of latitude. Each parallel therefore is a circle whose radius is an element of its tangent cone and whose center is on the axis of the spheroid prolonged. Therefore the radii of no two parallels of latitude, north or south, can be the same. They actually vary between a point at the pole to infinity at the Equator. The result is that parallels of latitude on a polyconic projection are equally spaced along the central meridian of the projection (map),

but this spacing increases rapidly toward the east and west edges. The north-south distortion consequent to this would be prohibitive for military maps on wide projections. In order to avoid this, it is customary to lay out a separate projection for the construction of each standard map sheet, using the central meridian of the map as the central meridian of the projection so that the error or distortion of the projection is limited to the width of a single sheet, in which it is infinitesimal. From this description, it is clear that the characteristics of the polyconic projection are true distances along its parallels of latitude, true distances along its central meridian, and exaggerated distances along all other longitude lines, increasing with the distance toward the east and west edges. Within a projection the size of the United States, the distortion along the Pacific coast would be around 20 percent in a north-south direction.

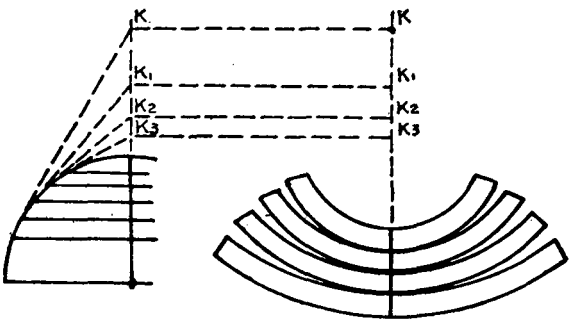


FIGURE 2.—Development of polyconic projection.

■ 5. CLASSIFICATION OF MAPS.—*a. General.*—AR 300–15 prescribes the classification of maps and the specifications for their preparation. Maps used in the theater of operations will consist of those available at the outbreak of hostilities and of those produced thereafter. These maps vary from crude, small-scale planimetric maps to accurate, large-scale topographic maps, and may include various special purpose maps, such as road maps, railroad maps, aeronautical charts, etc. Only in stabilized situations or in a few isolated areas will large-scale maps suitable for tactical operations of small units be found.

b. Types.—Military maps are classified generally according to scale. The general types are—

(1) *Small.*—Maps of small scale varying from 1: 1,000,000 to 1: 7,000,000 are needed for general planning and for strategical studies by the commanders of large units. Various types of general maps are employed for these purposes.

(2) *Intermediate.*—Maps of intermediate scale, normally from 1: 200,000 to 1: 500,000, are required for planning operations, including movements, concentration, and supply of troops. The "Strategic Map of the United States," 1: 500,000, is designed for these uses. Maps of a scale of about 1: 250,000 are particularly applicable to movements of armored forces and as maps of maneuver areas.

(3) *Medium.*—Maps of medium scale, normally from 1: 50,000 to 1: 125,000, are needed for strategical, tactical, and administrative studies by units ranging in size from the corps to the regiment. The United States Geological Survey map, scale 1: 62,500, with wooded areas and road classifications added, has been found suitable for these purposes. This scale is used by the War Department for map production in strategic areas. While not suitable for all purposes, the scale of 1: 62,500 has been found to be the most advantageous for recording topographic detail for future use. During campaign, these maps may be used at this scale or they may be enlarged or reduced according to existing areas.

(4) *Large.*—Maps of large scale, normally not greater than 1: 20,000, are intended for the tactical and technical battle needs of the Field Artillery and of the Infantry. The battle map or map substitute will be furnished for these purposes.

c. Reference.—For a detailed classification of maps by type, see FM 30–20.

■ 6. TRAINING WITH MAPS.—*a. Varied use.*—Any project or operation which involves coordination of movement and employment of groups of men and equipment requires use of a map or map substitute. In peacetime, this may be a sketch indicating a meeting place for a hunting party or an elaborate map of a major railroad system. No organization, with the exception of those involving transportation, utilizes maps more than military forces; and if the variety of types of maps is considered, even the above exception would not apply.

b. Military use.—All arms and services will have occasions to use maps and map substitutes in their respective operations. Modern methods of transportation and warfare demand rapid interpretation of maps by personnel of all units. Lack of time for study in the field necessitates thorough aptitude in map and aerial photograph reading, and the consequent ability to obtain hastily a clear picture of areas represented.

c. Aerial photographs.—Ability to read aerial photographs is required of all military personnel. Usually the nearest thing to a large-scale map in any theater of operations will be aerial photographs in some form. Aerial photographs made under war conditions cannot be expected to depict clearly certain obvious information that is shown in manuals for training in use of aerial photographs. Lack of familiarity with aerial photographs will leave a unit commander with little or no knowledge of valuable information upon which he must make his estimate of the situation.

d. Types of maps used in training.—Equipment used in training should be identical with that used in combat. Nevertheless many troop commanders have been extremely reluctant to use anything except large-scale finished maps in conducting operations. Many junior officers and men become slaves to color maps and contour lines. Initial operations may be with maps of scale 1:200,000 to 1:500,000, or even road maps. The next map available will be some form of photomap, probably a lithographic reproduction of a controlled or uncontrolled mosaic. The large-scale map can be expected only in stabilized situations or for limited areas. The emphasis in training must be placed on such maps, photomaps, or other air photographs as will be available in war. For map restrictions governing training activities, see section IX, FM 30–20.

e. Training in use of maps.—Training in the use of maps and aerial photographs should be planned to include both classroom and field work. The amount of each type of training depends upon the thoroughness contemplated and the size of class. For a small group to receive instruction in the most elementary map and aerial photograph reading, the training should consist of practically all field work. With larger classes and more advanced training, the proportional amount of classroom work increases. In the class-

room, written texts may be used in conjunction with moving pictures (TF–12) or film strips. Film strips with accompanying scripts on map reading (film strip 5–1) and on aerial photography (film strip 5–2) to be shown in 35-mm projectors may be obtained through the corps area or through the Chief Signal Officer, Washington, D. C. FM 21–6 should be consulted to determine what other new publications and aids to training have been prepared or revised in planning any course of instruction.

■ 7. CONVENTIONAL SIGNS.—Conventional signs must be learned just as new words are learned. FM 21–30 or FM 21–25 should be consulted and the conventional signs associated mentally with the objects which they represent.

a. Authorized symbols.—Data are shown on standard and special maps as far as practicable by means of the conventional symbols and type prescribed in FM 21–30. Explanation of the meaning of special symbols should appear in marginal notes.

b. Size of symbols.—In general, symbols resemble the objects which they represent and vary in size with the scale of the map. On small-scale maps, comparatively few objects can be represented and the symbols are reduced to their most elementary form. As the scale is increased, more objects can be represented and more of the symbols can be drawn to the relative shape and size of the object represented.

c. Lettering (type).—The relative size and importance of the feature named are indicated by the size of the type and by the use of capitals and of lower case letters with capital initials. Vertical roman type indicates civil divisions; slant roman type, natural water features; vertical gothic, natural land features; and slant gothic, works of man. Lettering is arranged to be read by the map user from a position at the bottom of the map (south border) or from the right-hand side (east border) since north is usually at the top of the map.

d. Color scheme.—Certain maps may appear in five colors:

(1) Black for the works of man and for the grid.
(2) Brown for contours.
(3) Blue for water and water-covered swamps.
(4) Green for woods and other vegetation.
(5) Red to indicate road information.

■ 8. MARGINAL INFORMATION.—Maps published by the Army and by other Government agencies show along the margin certain information which is of aid in filing the maps, in interpreting them, and in determining their accuracy. The data listed below are usually printed on the margins of all such maps. (See FM 21–30.)

a. Geographic index number of the map and the location in the geographic index of the quadrangle shown on the map sheet. Directions concerning the use of the geographic index system are contained in AR 300–15.

b. Descriptive title, giving the name of the State or States within which the area represented is located and the name of the area or the map quadrangle.

c. Representative fraction of the map and three graphical scales, one in feet or yards, one in meters, and one in miles. (Only one graphical scale is required on maps not intended for lithographing.)

d. True meridian, magnetic meridian (and variation with date and rate of change), and grid meridian.

e. An explanation of any symbol used which is not prescribed in FM 21–30.

f. Contour interval, when contoured.

g. Name of organization which reproduced map.

h. Date of reproduction or revision.

i. Names of organizations executing the surveys and topography upon which the map is based and date of their execution. If the map has been compiled from other maps, source of compilation is also shown.

j. Name of projection used.

k. Horizontal datum. (If no horizontal datum is given, the latitude and longitude of at least one point shown on the map and easily identified on the ground and the method of its determination should be given.)

l. Vertical datum.

m. Zone and system of military grid. Assume continental system if no reference to system is given.

n. If the area represented lies in the overlap of two grid zones, a reference to the grid of the second zone.

o. Designations of the geographic grid lines. These may be ticks only or both ticks and crosses.

p. Designations of military grid lines.

q. Names of adjoining map sheets.

r. An index of adjoining map sheets.

s. Name designation.

NOTE.—Frequently maps are prepared for temporary or local uses and are not intended to be included in any mapping system. Such maps may be encountered by students at service schools or by those pursuing extension courses. Much of the above listed marginal information is not required on such maps and is therefore omitted. This is true of the Gettysburg map used at the Command and General Staff School, which bears a local grid system with its projection based on the town of Gettysburg.

■ 9. GOVERNMENT MAPPING AGENCIES.—In addition to the maps described in paragraph 5, which are published by the War Department and by the United States Geological Survey and which have been adopted as standard for use of the military forces, maps are issued by various Government agencies as follows:

a. Soil survey maps.—These maps are published by the Department of Agriculture on the scale of 1 inch equals 1 mile. They show roads, drainage, towns, and, by symbols and colors, the various classes of soils within the area.

b. Post route maps.—These maps are made by the Post Office Department for the designation of postal routes and are primarily for internal administration in that department.

c. Coast and Geodetic Survey charts.—These charts are intended for the use of navigators on the coast and are published on various scales ranging from 1:5,000 to 1:40,000 for harbor charts and from 1:80,000 to 1:100,000 for coast charts. They show the depth of the water, aids to navigation, and a narrow strip of topography from 1 to 5 miles in width along the shores.

d. Lake survey charts.—These charts are intended for the use of navigators on the Great Lakes and adjacent waters and are published on various scales ranging from 1:5,000 for small harbors to 1:1,200,000 for the general chart of all the lakes. The charts likewise show the depth of the water, aids to navigation, and a narrow strip of topography from 1 to 5 miles in width along the shores.

e. General Land Office maps.—Maps of this bureau are comprised of the following: *Township plots* showing land division and area of tracts; *maps of States* having public land showing land survey lines and United States reservations; *general maps of the United States* showing sources of obtaining land, civil and public land boundaries, and progress of land surveys.

f. International Boundary Commission: United States and Canada.—These maps cover a strip of territory from ½ to 2½ miles in width on each side of the boundary between the United States and Canada, from the Arctic Ocean to Mount St. Elias, from the Pacific Ocean to Lake Superior, and from the head of the St. Lawrence River to the Atlantic Ocean. From Mount St. Elias to Cape Muzon, the boundary maps include practically all the territory between the boundary line and the Pacific Ocean. The scales used are: 1:6,000, 1:12,000, 1:24,000, 1:62,500, and 1:250,000, depending on the locality. The contour intervals range from 5 to 250 feet and the maps are complete in cultural features and relief.

g. United States Forest Service maps.—The United States Forest Service prepares maps of areas included within the national forest boundaries and adjacent thereto. The maps are compiled from all sources, governmental and private, supplemented by United States Forest Service surveys. They are intended primarily for administrative purposes in the United States Forest Service. Besides the topography and culture, they frequently carry detailed classification of vegetation. The publication scales are ¼ inch, ½ inch, and 1 inch to the mile.

SECTION II

DISTANCE

■ 10. LINEAR MEASURE.—*a.* In different countries, various units are used to measure distance. In England the mile is used, in France the kilometer, in Russia the verst, etc. In the United States, the English system of miles is generally used although the metric system is sometimes employed. The American military map reader should therefore be familiar with both English and metric linear measure and be able to express any distance in either unit.

b. The common units of English linear measure are—

12 inches = 1 foot
3 feet = 1 yard
1,760 yards = 1 mile

c. The common units of metric linear measure are—

10 millimeters = 1 centimeter
100 centimeters = 1 meter
1,000 meters = 1 kilometer

d. A distance expressed in English units can be changed into metric units or, if it is expressed in metric units, it can be changed into English units by use of the following relations:

1 meter=almost exactly 39.37 inches or 1.094 yards
1 kilometer=about .62 mile or 1,094 yards

Example 1: A distance on the ground measures 3,300 yards. How many meters does it measure? *Solution:* 3,300÷1.094=3,016 meters (approximately).

Example 2: A distance on the ground measures 2.5 kilometers. How many miles does it measure? *Solution:* 2.5×.62=1.55 miles.

■ 11. SCALES OF MAPS.—Every distance on a map must bear a fixed relation to the corresponding distance on the ground. This fixed relation is called the "scale." Due to the fact that the rise and fall of the ground cannot be shown on the map except by conventional signs (contours and hachures), distances are always measured and written as horizontal distances except when otherwise stated. The vertical distance due to the rise and fall of the ground is called "elevation." For the conventional methods of indicating scales, see FM 21–25.

■ 12. METHODS OF DISTANCE MEASUREMENT.—*a. Graphic scale.*—The measurement of distance on a map by means of the graphic scale is discussed in FM 21–25.

b. By use of map measurer (fig. 3).—The map measurer is an instrument specially designed for quickly measuring distances or lines on a map. It consists of a dial case, handle, and a small wheel or roller. A moving pointer indicates on the dial the distance traveled by the wheel rolling along the line to be measured. Unless the map measurer is graduated to the particular scale of the map being used, it is necessary to convert the units shown on the dial of the instrument to the required units of ground distance. To measure distance with a map measurer, proceed as follows:

(1) Turn the small roller at the side of the dial case opposite the handle to set indicator of map measurer at zero.

(2) Set the roller at one of the given points and, holding

the handle vertical, roll along the line to be measured to the second point.

(3) Under the pointer, read the distance on the divisions on the dial corresponding to the RF of the map.

(4) When there is no scale corresponding to the RF of the map, read the one marked 1: 10,000 and multiply by the denominator of the RF divided by 10,000.

(5) Some dials are divided to read the map distance in inches or centimeters. In this case convert as directed in c (4) and (5) below.

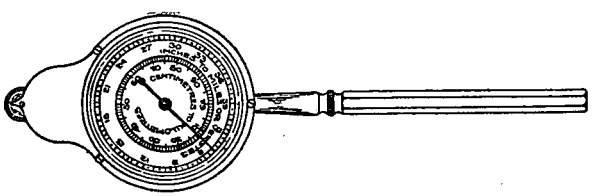


FIGURE 3.—Map measurer.

c. By use of representative fraction and engineer's scale.— The measurement of distance by means of a linear scale necessitates the conversion of the distance (in inches) on the map to the desired units on the ground. On maps of standard scales this is usually done by means of the representative fraction. In order to facilitate the computations which are involved, an engineer's scale should be selected because such a scale is subdivided in accordance with the decimal system. The measurement of the distance between two points on a map is made by proceeding as follows (fig. 4):

(1) Select the edge of the engineer's scale marked 10 (that is, subdivided into tenths of an inch).

(2) Lay the edge on the two points and slide until the zero coincides with one point.

(3) Read the distance on the scale in inches, tenths, and hundredths opposite the other point.

(4) Multiply this distance by the denominator of the representative fraction. This will give the number of inches on the ground between the two points.

(5) To secure the distance in feet, yards, or miles, divide by 12 for feet, 36 for yards, or 63,360 for miles.

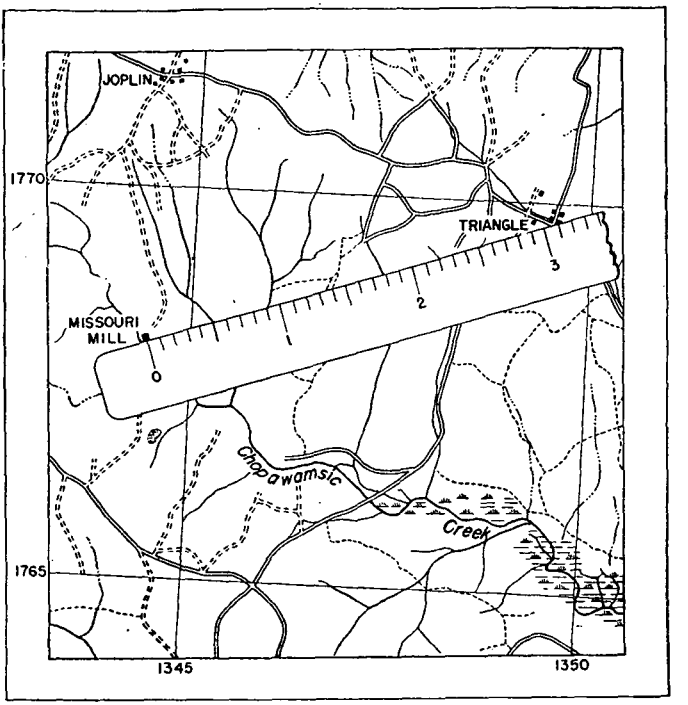
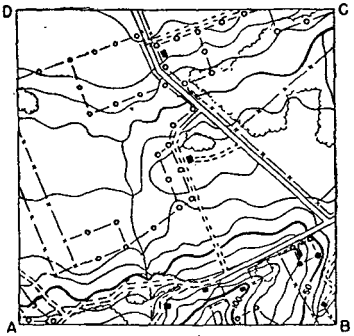


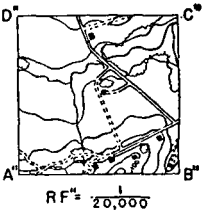
FIGURE 4.—Measurement of distance on a map by means of an engineer's scale.

(6) When the denominator of the representative fraction is the same as the number stamped on the middle of an edge of the engineer's scale, or is that number with additional ciphers, the ground distance in inches may be read directly on this edge of the scale, giving careful attention to correct placing of the decimal point.

(7) To measure an irregular line such as a road or stream, divide it into approximately straight sections. Measure each as indicated above. The sum is the required distance.

Example: Figure 4 shows a portion of a map to a scale of 1: 62,500. It is desired to find the distance on the ground between MISSOURI MILL and the road junction at TRIANGLE. Lay the edge of the engineer's scale divided





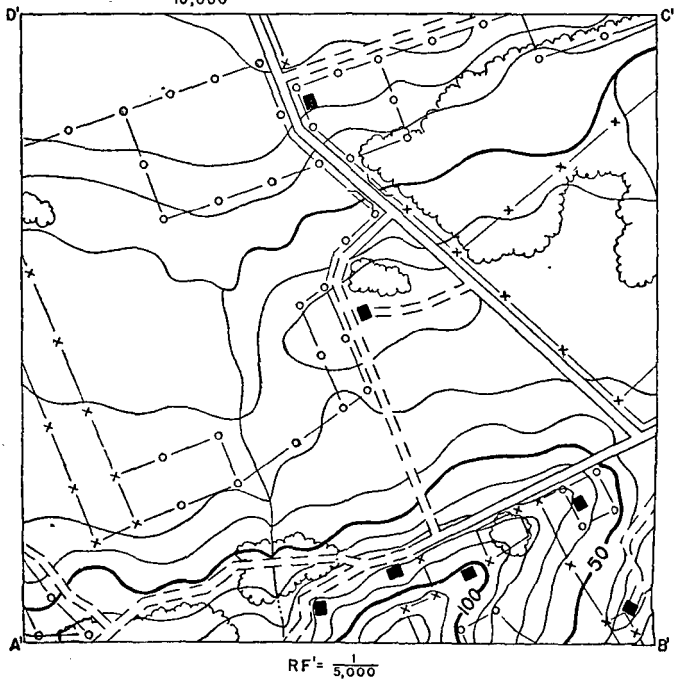


FIGURE 5.—Relation between distances and areas on maps of different scale. (Scales of maps shown above have been reduced in printing.)

into tenths of an inch along the two points. It may be seen that the map distance is 3.07 inches. The distance on the ground is 3.07 times 62,500 or 191,875 inches. This is 15,990 feet or 5,330 yards or 3.03 miles.

■ 13. RELATION BETWEEN DISTANCES AND AREAS ON MAPS OF DIFFERENT SCALE.—Figure 5 shows at a reduced scale an identical area of ground represented on maps of three different scales; that is, 1: 5,000, 1: 10,000, and 1: 20,000. *A*, *B*, *C*, and *D* are points on the ground. *A'B'* on a map of scale 1: 5,000 is just twice as long as *AB* on a map of scale 1: 10,000. The area of the map *A'B'C'D'* at scale 1: 5,000 is just four times the size of the same area at scale 1: 10,000. Conversely, *A''B''* on a map of scale 1: 20,000 is just one-half as long as *AB* on a map of scale 1: 10,000 and the area *A''B''C''D''* is one-fourth the size of *ABCD*. These relationships may be stated as follows:

a. Distances.—Distances on different maps vary directly as the representative fractions of the maps and inversely as the denominators of their respective fractions, thus (fig. 5):

$$\frac{AB}{A'B'}=\frac{RF}{RF'}=\frac{\frac{1}{10{,}000}}{\frac{1}{5{,}000}}=\frac{5{,}000}{10{,}000}=\frac{1}{2}$$

b. Areas.—Areas on different maps vary directly as the squares of the representative fractions of the maps and inversely as the squares of the denominators of their respective fractions, thus (fig. 5):

$$\frac{ABCD}{A'B'C'D'}=\frac{(RF)^2}{(RF')^2}=\frac{\left(\frac{1}{10{,}000}\right)^2}{\left(\frac{1}{5{,}000}\right)^2}=\frac{(5{,}000)^2}{(10{,}000)^2}=\frac{1}{4}$$

■ 14. DETERMINATION OF SCALE OF MAP AND CONSTRUCTION OF GRAPHIC SCALE.—It is important that the user of a map be able to determine the RF of a map when in the field and readily construct a suitable graphic scale for use in the event that the scale data are missing from the map. The procedure is as follows:

a. Determination of scale.—The scale of a map may be determined from known distance on the ground, or from scaled distance on another map of known scale.

(1) *By measurement of distance between two points on ground.*—(*a*) Locate two objects on the ground which can be identified on the map, such as bridges, houses, etc.

(*b*) Estimate, stride, or measure on the ground in some manner, the distance between the selected points, and convert into inches. (The method of measuring should depend on accuracy required, time available, etc.)

(*c*) Measure in inches the distance on the map between the two points selected.

(*d*) Determine the scale from the relation—

$$\text{RF}=\frac{\text{distance on map in inches}}{\text{distance on ground in inches}}$$

This expression, when reduced to a fraction the numerator of which is unity, becomes

$$\text{RF}=\frac{1}{\left(\frac{\text{distance on ground in inches}}{\text{distance on map in inches}}\right)}$$

NOTE.—Distances may be expressed in any unit of measurement provided the same is used for both map and ground distances.

Example: Map distance between two points=3 inches; ground distance between corresponding points=5,208.3 yards.

$$\text{RF}=\frac{1}{\left(\frac{5{,}208.3\times 36 \text{ inches}}{3 \text{ inches}}\right)}=\frac{1}{62{,}500}$$

(2) *By measurement between two points on map of known scale.*—(*a*) Locate two objects on map of known scale which can be identified on the map the scale of which is to be determined.

(*b*) Scale from both maps the distances between the points in the same unit of measurement (inches).

(*c*) Determine the scale of the map by one of the two methods given below:

1. Convert distance on map of known scale to distance on the ground, and solve as in (1) above.
2. Determine scale from the relation—

$$\frac{\text{RF of the map}}{\text{RF of map of known scale}}=\frac{\text{distance on the map}}{\text{distance on the map of known scale}}$$

Example: Distance between two points on the map of unknown scale=8 inches.

Distance between corresponding points on a map of 1:20,000 scale=4 inches.

$$\frac{RF}{\frac{1}{20,000}}=\frac{8}{4}$$

$$RF=\frac{8}{4}\times\frac{1}{20,000}=\frac{1}{20,000\times\left(\frac{4}{8}\right)}=\frac{1}{10,000}$$

It is seen from the above that the denominator of the RF of the map (10,000) is obtained by multiplying the denominator of the RF of the map of known scale (20,000) by the distance measured on that map (4) and dividing by the distance measured on the map the scale of which is sought (8).

b. To construct scale (fig. 6).—(1) Suppose it is desired to construct a graphic scale to read to 1,000 yards for use on a map whose RF has been determined as 1:10,000. The procedure is as follows:

(*a*) 1,000 yards on the ground=36,000 inches. 36,000 inches at scale 1:10,000=$\frac{36,000}{10,000}$=3.6 inches on map, or since 1 inch on the map=10,000 inches on the ground, then 36,000 inches on the ground=$\frac{36,000}{10,000}$=3.6 inches on the map.

(*b*) Lay off the line *ab* (fig. 6)=3.6 inches, using the engineer's scale.

(*c*) Lay off at any acute angle the line *ab'* representing 10 convenient equal divisions of the engineer's scale. Draw the line *bb'* and through each division of the line *ab'* draw lines parallel to *bb'*, to cut the line *ab*, dividing it into 10 equal parts of 100 yards each. Use the left division as the scale extension and further subdivide it in a similar manner into five equal parts of 20 yards each. Mark the graduation as shown in the figure. Show the RF of the scale and the linear unit represented by it.

(2) Another method not so accurate as the above but simpler and quite satisfactory for practical purposes is to compute the length of one 100-yard graduation (or any other suitable division) of the primary scale and then apply that as many times as necessary along a line, as *ab* in figure 6. For example, in the case of the map whose RF was determined as

1:2,769, the length of a 100-yard interval of the scale would be $\frac{3,600}{2,769}$=1.3 inches, approximately. Point off this distance as many times as 100-yard graduations are required for the primary scale, subdividing the left interval as the extension.

■ 15. TIME-DISTANCE SCALES.—In solving tactical problems or in planning military operations on maps, time-distance scales frequently prove time-saving devices of great usefulness. A time-distance scale is a scale whose graduations are

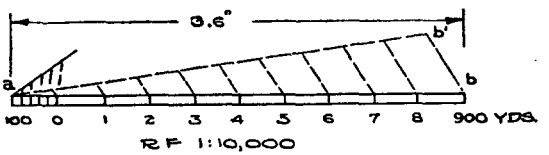


FIGURE 6.—Construction of graphic scale.

time intervals of distance to the scale of the map at a given rate of movement (fig. 7). Suppose that a time-distance scale graduated in hours and minutes of time at a given marching rate, is desired for use on a topographic map 1:62,500. To construct such a scale, the procedure is as follows:

a. (1) In 1 hour, infantry marches 2½ miles or 2½×63,360=158,400 inches.

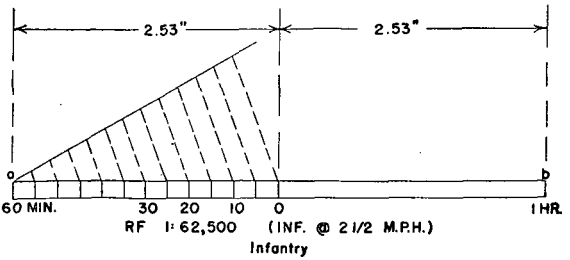
(2) 158,400 inches on the ground=$\frac{158,400}{62,500}$=2.53 inches on a map whose scale is 1:62,500.

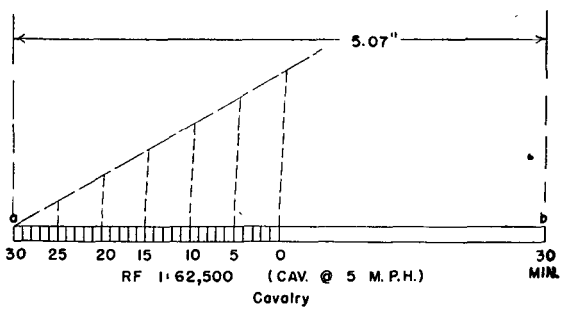
(3) On a suitable strip of paper along a straight line *ab* (fig. 7), lay off as many 1-hour intervals of 2.53 inches each as may be desired in the scale. Subdivide the left interval on the scale extension into 1-minute, 5-minute (used in fig. 7), or 10-minute graduations, depending on the least reading desired; mark the graduations appropriately. On the scale, indicate the RF of the map to which the scale applies and the marching rate to which constructed.

b. (1) In 1 hour, cavalry marches 5 miles or 5×63,360=316,800 inches.

(2) 316,800 inches on the ground=$\frac{316,800}{62,500}$=5.07 inches.

The construction of the scale is similar to that described and illustrated in figure 7.





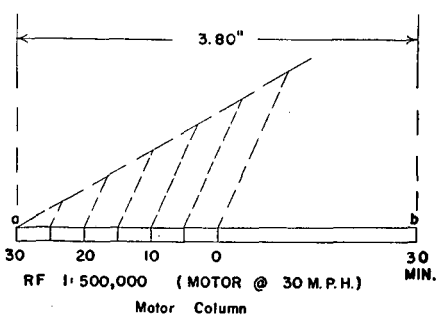


FIGURE 7.—Time-distance scales.

c. (1) In 1 hour, a motor column marches 30 miles or $30 \times 63{,}360 = 1{,}900{,}800$ inches.

(2) 1,900,800 inches on the ground $= \frac{1{,}900{,}800}{62{,}500} = 30.41$ inches on the map.

This shows why operations for units with such rates of march would ordinarily be planned on smaller scale maps. Hence the time-distance scale for a motor column is shown in figure 7 for a 1:500,000 map, making a 1-hour march equal 3.80 inches on the map.

SECTION III

DIRECTION, ORIENTATION, AND LOCATION

■ **16. DIRECTION ANGLES.**—Distance and direction may be used to locate a point or object on the ground or on a map with respect to an occupied or known point. The distance may be measured, paced, or estimated, depending upon the required degree of accuracy. For military purposes direction is always expressed in terms of an angle from some fixed or easily established base direction line.

■ **17. UNITS OF ANGULAR MEASUREMENT.**—The value of an angle may be expressed in degrees, minutes, and seconds; or in mils.

a. Degrees, minutes, and seconds.

A circle $= 360°$
$1° = 60$ minutes.
1 minute $= 60$ seconds.

b. Mils.—A mil is the angle subtended by an arc of 1 unit on a radius of 1,000 units or, in other words, an angle the tangent of which is approximately 1/1,000. The arbitrary value of the mil adopted by the United States Army is 1/6,400 of a circle.

c. Conversion factors.

$1° = 17.8$ mils approximately.
1 mil $= 0.056°$ approximately.
$= 3$ minutes 22.2 seconds.
$= 0.056 \times$ mils.
Mils $= 17.8 \times$ degrees.

■ **18. BASE DIRECTIONS.**—The characteristics of the three base directions are given in table I.

TABLE I.—*Characteristics of base directions*

Designation	Base	Departure from true north	Variations	When used
True north	True meridian	No departure	No variation	In conjunction with geographic map and for permanent records. NOTE.—All directions are assumed based on true north unless otherwise stated.
Magnetic north	Magnetic meridian	Termed magnetic declination and varies in the United States from 25° east in Washington State to 22° west in Maine.	Annual change has been as much as 6 minutes in some localities.	In conjunction with the magnetic compass in the field.
Grid north	True center meridian of the zone of the grid.	Termed gisement and increases to a maximum of approximately 3° at the edge of the grid zone.	No variation	In conjunction with maps on which the military grid is printed.

■ 19. DECLINATION.—Declination is the difference in direction between true north and either magnetic north or grid north. Hence there are two declinations, magnetic declination and grid declination or gisement.

a. Magnetic.—Due to the difference in position between the true and magnetic poles and the inequality of magnetic distribution throughout the earth, there will always be, except in very limited localities, an angle between true north and magnetic north. This angle is called the magnetic declination. When the needle points east of true north, the

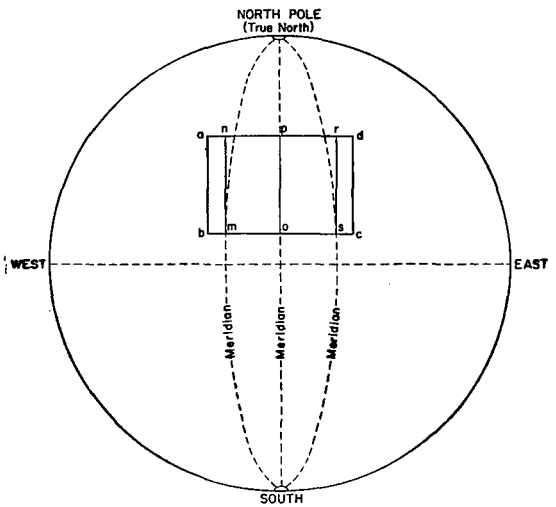


FIGURE 8.—Diagram illustrating reason for grid declination.

magnetic declination is east; when west of true north, the magnetic declination is west. Lines joining points on the surface of the earth where magnetic north and true north are the same direction so that there is no magnetic declination are called agonic lines.

Lines joining points having the same declination are called isogonic lines. The magnetic declination in the United States varies from 25° east in the State of Washington to 22° west in Maine. Isogonic lines run across the United States in a general north and south direction but are very irregular, in some instances doubling back on themselves

(fig. 9). The magnetic declination at any one locality is subject to change, the amount of which can be predicted from past records. This change in some localities in the United States is as much as 4 minutes annually. Magnetic declination and annual magnetic change are shown on maps of the United States published every 5 years by the Coast and Geodetic Survey. Every standard map should show in diagrammatic form the average relation of magnetic and true north for the area of the sheet at a stated date; also the annual magnetic change and whether increasing or decreasing.

b. Grid.—Grid declination is the fixed difference in direction between true north and grid north. Because of the fact that the meridians converge to meet at the pole while all the north-south grid lines (*Y* lines) of the same grid zone are parallel to one another (see par. 34 for an explanation of the military grid system), there is a deviation between true north and grid north except along the central meridian of the grid zone. This deviation is called grid declination or gisement and reaches a maximum of 3° at the edge of the grid zone. It is illustrated in figure 8 which shows a sketch of the projection of the earth with *abcd* representing the area of a map on which the line *op* is the projection of the central meridian of the grid zone. The north-south grid lines are straight lines parallel to *op*. The projections of all meridians other than *op* are curved converging lines which deviate in direction from the direction of the north-south grid lines. This deviation is designated as west grid declination for all points west of the central meridian, as at point *m*, and as east grid declination for all points east of the central meridian, as at point *s*. The declination is determined by finding the angle that the *Y*-grid line makes with true north at the point in question. Although the grid declination varies at different points on a map, this variation on the tactical map is so slight that the average grid declination for the area may be used as the actual grid declination at any point on the map sheet without introducing an appreciable error. Every standard map should show in diagrammatic form the average grid declination for the area represented by the map.

FIGURE 9.—Lines of equal magnetic declination and of equal annual change in United States for 1935.
(For figure see back of manual.)

■ 20. DIRECTION OF ANGULAR MEASUREMENTS.—The characteristics of the methods used to express the direction of angular measurements are given in the following table:

TABLE II.—*Characteristics of methods of expressing directions of angular measurements*

Designation	Units of angular measurement used	Base direction	Direction of measurement
Azimuths	Degrees or mils	True, magnetic, or grid north, unless otherwise stated (south may be used).	Clockwise.
Bearings	Degrees	True or magnetic north and south; whichever used is designated.	Direction which gives smallest arc (must not exceed 90°) is used and is designated.

For military purpose, directions should normally be expressed as azimuths measured from true, magnetic, or grid north.

■ 21. RELATIONSHIP BETWEEN TRUE, MAGNETIC, AND GRID AZIMUTHS AND BEARINGS.—This relationship is shown in figure 10.

Example:

Line *BA:*

Azimuth	60°.
Magnetic azimuth	66°40′.
Grid azimuth	57°35′.
Bearing	N. 60° E.
Magnetic bearing	N. 66°40′ E.
Back azimuth	240°.

Line *AB:*

Azimuth	240°.
Magnetic azimuth	246°40′.
Grid azimuth	237°35′.
Bearing	S. 60° W.
Magnetic bearing	S. 66°40′ W.
Back azimuth	60°.

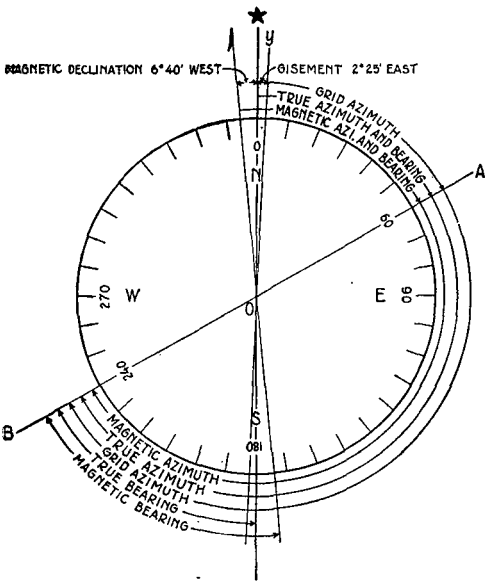


FIGURE 10.—Relationship between true, magnetic, and grid azimuths and bearings.

■ 22. MAGNETIC COMPASS.—There are three types of magnetic compasses used by the Army, varying chiefly in scales and sights. Below is a brief description of each; for a more complete description of the compass and its use, see FM 21–25.

a. Watch compass.—The watch compass has a movable needle, a fixed dial graduated in bearings, and has no sighting device.

b. Prismatic compass.—The prismatic compass has a circular magnetic floating dial, prismatic eyepiece, and a north point painted in luminous paint in the case. One of the two dial graduations is read through the prism and the other is read direct. Each scale is graduated from 0° to 360°. The forward sight is a hair line on the glass in the top of the case.

c. Lensatic compass.—The lensatic compass functions in much the same manner as the prismatic compass. It contains a magnifying lens fixed in a hinged eyepiece. The face has two scales, one graduated in degrees, the other in mils.

■ 23. LOCAL MAGNETIC ATTRACTION.—In addition to the compass variation caused by magnetic declination, the magnetic compass is affected by the presence of iron and electrical fields of magnetism. Consequently, great care should be taken not to approach such local magnetic attraction within a distance which will cause the magnetized compass needle to deviate while making observations to determine direction. The rifle, pistol, and helmet must be laid aside when reading the compass. The following are the minimum safe distances for visible masses of iron and electrical fields of magnetism:

	Yards
High tension power lines	150
Heavy gun	60
Field gun and telegraph wires	40
Barbed wire	10

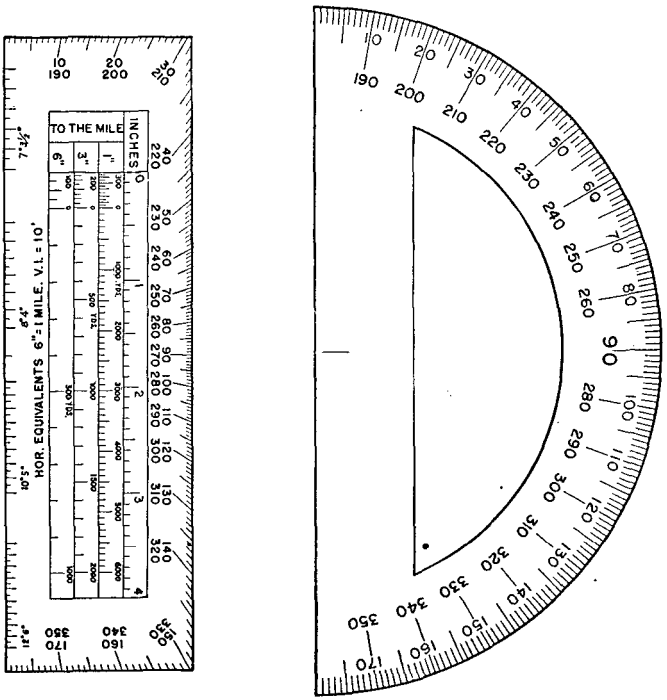
■ 24. PROTRACTOR.—*a. Relationship between semicircular and rectangular protractors.*—In figure 11 it will be noted on each protractor that two scales are shown, one reading from 0° to 180° and the other from 180° to 360°. With both scales, each protractor can be used to read the full circle in degrees. Inasmuch as both the semicircular and the rectangular protractors are used in the same manner, the method of using the less familiar type only is given.

b. Use of rectangular protractor (fig. 12).—Assuming the *Y*-grid lines are available on the map and the angle which magnetic north makes with grid north is shown on the map margin to be the sum of the magnetic declination 6°21′ and gisement 2°35′ or 8°56′, to lay off the magnetic azimuth of a line *AB* the procedure is as follows:

(1) Join the points *A* and *B* by a fine, lightly drawn line and prolong until it crosses the nearest *Y*-grid line and extends beyond the edges of the protractor.

(2) By inspection, the azimuth is seen to be less than 180° and therefore should be measured on the outside or lesser azimuth circle (0° to 180°) of the protractor with the protractor placed on the east side of the direction line.

(3) Place the protractor along the intersected grid line 65 and shift it until the index coincides with the point where *AB* prolonged crosses the grid line. About this point as a pivot, turn off an angle of 8°56′ (or 9° in practice, since the difference is unmeasurable) counterclockwise. The index



① Rectangular. ② Semicircular.

FIGURE 11.—Military protractors.

edge of the protractor is now on the magnetic meridian. The value of the azimuth angle sought is read 61°00′ at the point on the outside azimuth "circle," where the line *AB* prolonged cuts the edge of the protractor.

(4) Suppose, however, the problem is to measure the magnetic azimuth of the line *BA*, which is the back azimuth of the line *AB* and differs from it by 180°. By inspection this is seen to be greater than 180°, requiring use of the inner "circle" of graduations (180° to 360°) with the position of the protractor on the opposite side of the grid line. The procedure is similar to that just described except the protractor is placed on the west side of the 65 grid line, the angle 8°56′ is turned off counterclockwise from the south end of the pro-

tractor, and the angle of 241°0′ is read on the inner "circle" where *BA* prolonged crossed the graduated edge of the protractor.

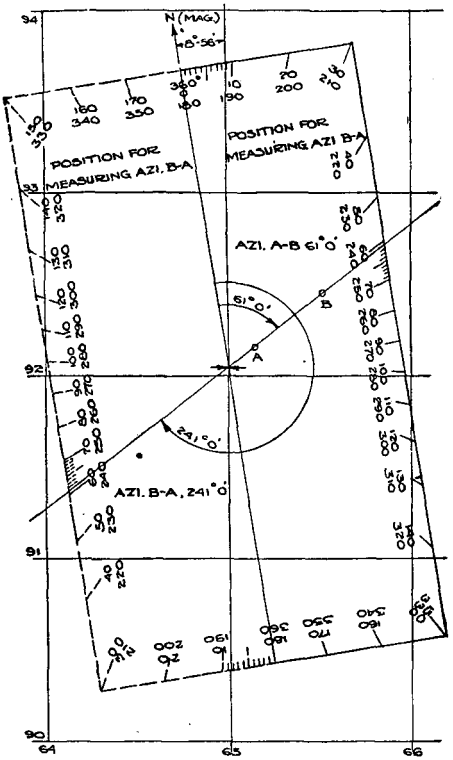


FIGURE 12.—Use of rectangular protractor.

■ 25. DETERMINATION OF DIRECTION BY FIELD EXPEDIENTS.—*a. By aid of watch and sun* (fig. 13).—North can be determined with an error of less than 8° if the sun is visible and a watch showing approximately the correct sun time is available. Point the hour hand, watch held face up, at the sun. This is facilitated by casting the shadow of a vertical pencil across the face of the watch and by then bringing the hour hand into this shadow. A line drawn from the center of the dial

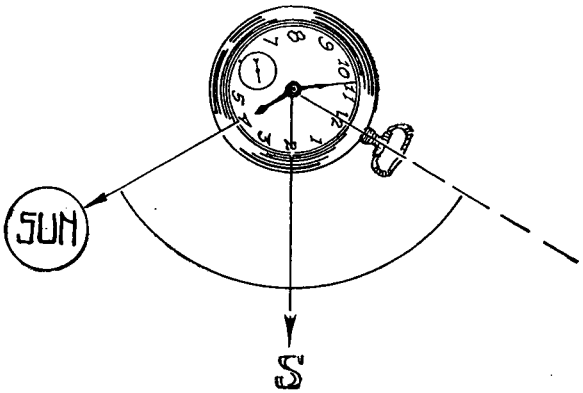
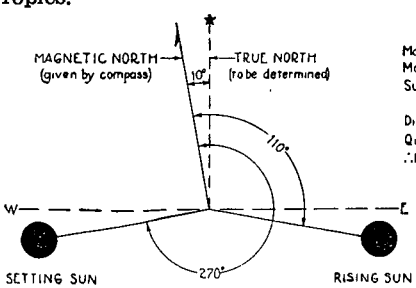


FIGURE 13.—Determination of north by watch and sun.

to a point halfway on the smaller arc between the hour hand and the 12 of the watch will point south. In the Southern Hemisphere the watch must be held face down and this line will point north. This method is difficult to use when the sun is very high in the heavens and is of little or no use in the Tropics.



COMPUTATIONS

Mag. azi. of rising sun	110°
Mag. azi. of setting sun	+270°
Sum	380°
	−360°
Difference	20°
Quotient (÷2)	10°

∴Magnetic Declination is 10° West

FIGURE 14.—Determination of north by rising and setting of sun.

b. By rising and setting of celestial body (fig. 14).—Observe the magnetic azimuth of the sun, a planet, or a bright star at rising and setting on the same day or at setting on one day and rising the next. Add these two azimuths together. Take the difference between this sum and 360°. One-half of this difference is the declination of your compass—east, if the sum of the azimuths is less than 360°; west, if it is greater.

In using this method the observations are best taken when the object is just above the true horizon, or at a gradient of zero. This can usually be done if a high point is chosen for observation. If this cannot be done, be careful to take both observations with the object at the same gradient, as determined with a clinometer. This is most important with the sun. Under the least favorable conditions an inequality of 1° in the gradients at the time of observation on the sun may introduce an error of ½° in the result. In using a star, choose one which rises nearly east from the point of observation. If this is done the inequality of a degree in the gradients will be immaterial. Both observations need not be made at the

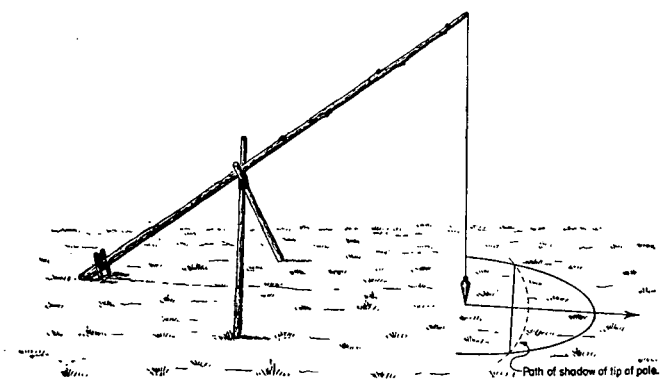


FIGURE 15.—North by sun and plumb line.

same point, but should not be more than 10 miles apart in east and west or north and south directions.

c. By aid of sun and plumb line (fig. 15).—On a level piece of ground, lean a pole toward the north and rest it in a crotch made by two sticks, as shown. Suspend a weight from the end of the pole so that it nearly touches the ground; then, about an hour before noon, attach a string to a peg driven directly under the weight and, with a sharpened stick attached to the other end of the string, describe an arc with a radius equal to the distance from the peg to the shadow of the tip of the pole. Drive a peg on the arc where the shadow of the tip of the pole rested. About an hour after noon, watch the shadow of the tip as it approaches the east-

ern side of the arc and drive another peg where it crosses. By means of a tape or string, find the middle point of the straight line joining the last two pegs mentioned. A straight line joining this middle point and the peg under the weight will, for all practical purposes, be true north.

d. By means of North Star (Polaris).—Ursa Major (Big Dipper) shown in the upper portion of figure 16 is the easiest constellation to distinguish and provides the best

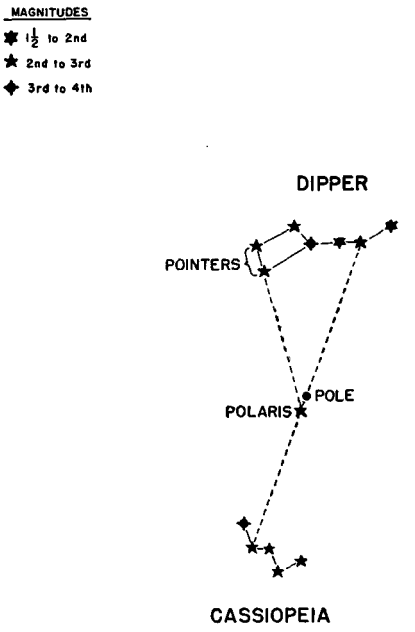


FIGURE 16.—Determination of north by North Star.

means for locating the North Star. The two "pointers," or the stars forming the lip of the dipper, point to the North Star (Polaris) at all times as the Dipper appears to circle the pole. On the opposite side of Polaris and at about the same distance from it is the constellation of Cassiopeia. Its form is that of the letter "W." The great importance which attaches to the North Star is that it is never more than 2° away from the point where the axis of the earth, if extended,

would pierce the heavens. It therefore appears to the eye to be always in the same place. An observation of the North Star to determine true north, when the Dipper and Cassiopeia are above and below the North Star, will give the declination of the compass to within the least reading of the compass.

■ 26. ORIENTATION.—*a. Definition.*—A map is oriented when, in a horizontal position, its north point points north and all lines of the map are parallel to the corresponding lines

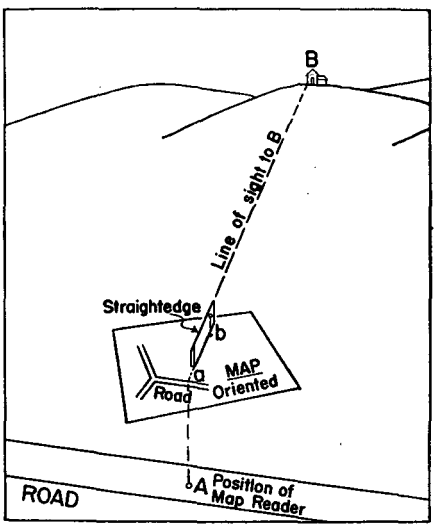


FIGURE 17.—Location of one's position on map by resection when along road (graphic method).

of the ground. A map reader is oriented when he knows his position on an oriented map and the cardinal directions on the ground. A map will be of small use in the field unless its possessor can orient himself readily. It follows that ready command of the simpler methods of practical orientation is of prime importance to the student of map reading.

b. Methods of orientation.—Primary methods of orientation by inspection, with a compass, and by sighting on a distant point (given in FM 21–25) should be known to ad-

vanced students and are not repeated here. Several methods of orientation by resection are given below.

c. Location of one's position along road or similar feature by resection.—The position may be determined graphically or may be plotted by means of a protractor after a compass has been used to give direction. The first method is the speedier and is most commonly employed when the determination of position is undertaken in the field.

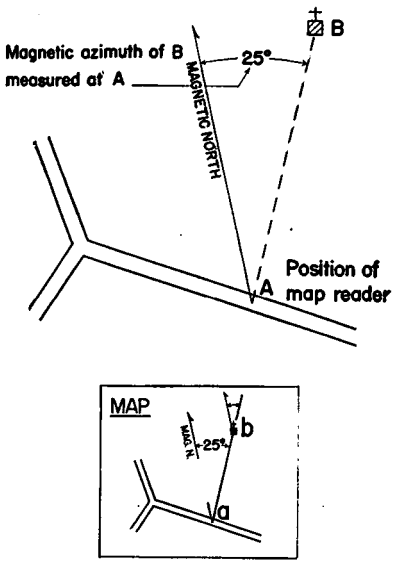


FIGURE 18.—Location of one's position on map by resection when along road, using compass and protractor.

(1) *Graphic method* (fig. 17).—Proceed as follows:

(*a*) Identify a convenient visible object *B* on the ground which appears on the map at *b*.

(*b*) Rest the map in a horizontal position on some nearby convenient support, such as a fence post, stone, or fold in the terrain, from which *B* is visible, and set a pin in the map at *b*.

(*c*) Orient the map.

(*d*) Without moving the map, hold a straightedge against the pin at *b* and aline its edge with the object *B* on the terrain.

(*e*) Draw a line through *b* along the straightedge and prolong it to intersection with the road at *a*. This intersection is the point sought.

(2) *By means of compass and protractor* (fig. 18).—Proceed as follows:

(*a*) Identify a convenient visible object *B* on the ground whose position *b* appears on the map.

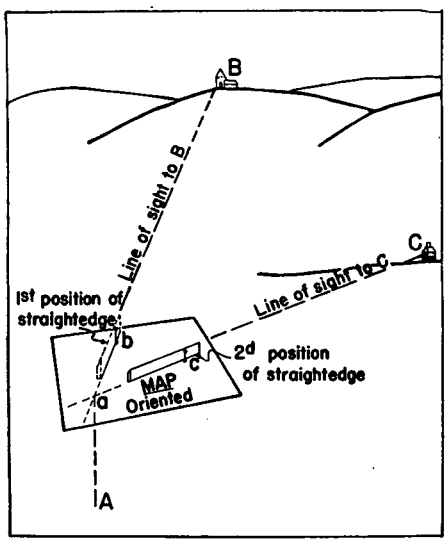


FIGURE 19.—Location of one's position on map by resection from two distant points (graphic method).

(*b*) With the compass, sight *B* and read the magnetic azimuth.

(*c*) On the map with the protractor lay off this azimuth through *b* and prolong the line until it intersects the road at *a*, which is the position sought.

NOTE.—When azimuths are read from observer to a known position, either the azimuth or back azimuth may be used in plotting the direction line through the known position.

d. Location of one's position by resection from two distant points.—This method of locating a position is useful when no well-defined feature, such as a road, is in the vicinity. The position may be determined graphically or may be plotted by means of a protractor after directions have been read by a compass. The first method is speedier and is most commonly employed when the determination of position is undertaken in the field.

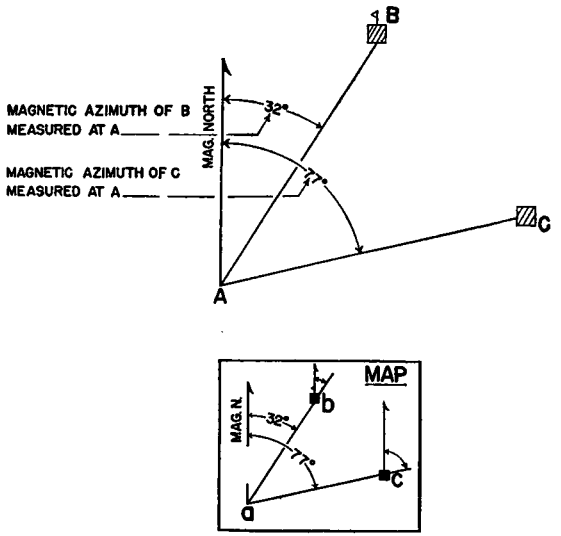


FIGURE 20.—Location of one's position on map by resection from two distant points, using compass and protractor.

(1) *Graphic method* (fig. 19).—Proceed as follows:

(*a*) Select two visible objects on the terrain, as *B* and *C*, whose positions *b* and *c* appear on the map, so situated that lines radiating from observer to objects form an angle of 30° to 150° at the observer.

(*b*) Rest the map in a horizontal position on some nearby convenient support, such as a fence post, stone, or convenient fold in the terrain, from which the objects *B* and *C* on the terrain are visible and set pins through their respective map positions, *b* and *c*.

(*c*) In this position, orient the map.

(*d*) Without moving the map, sight *B* and *C* successively on the terrain along a straightedge held against the pins through the corresponding points *b* and *c*, respectively. Along the straightedge, draw lines through *b* and *c* and prolong these lines to intersection at *a*, which is the point sought.

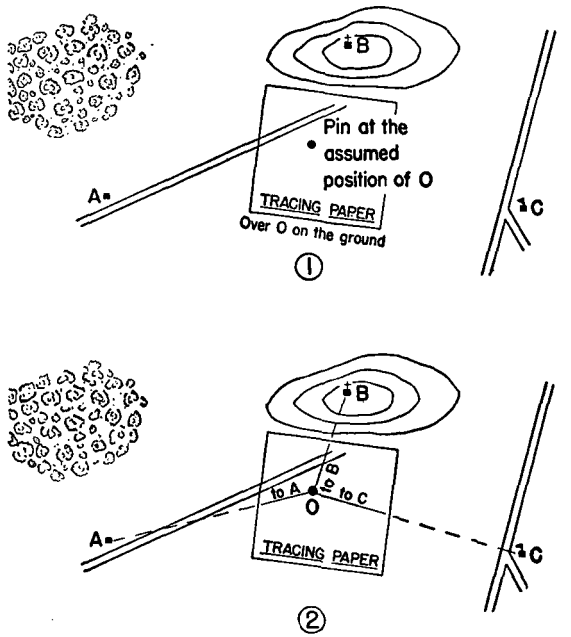


FIGURE 21.—Location of one's position on a map by resection from three distant points (tracing paper method).

(2) *By means of compass and protractor* (fig. 20).—Proceed as follows:

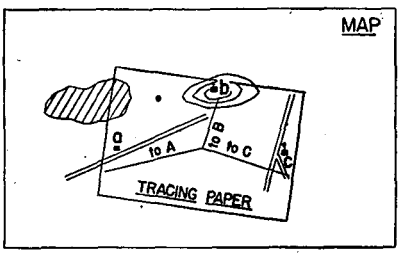
(*a*) Select two visible objects on the terrain, as *B* and *C*, the positions of which, *b* and *c*, can be identified on the map and which are so situated that lines radiating from observer to object make an angle of 30° to 150° at the observer.

(*b*) With the compass sight the objects on the landscape successively, reading the magnetic azimuth to each.

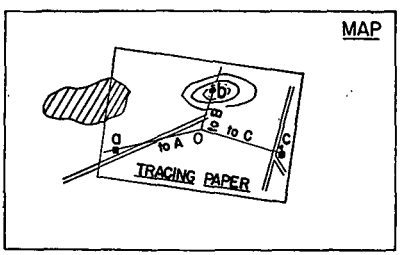
(*c*) Draw magnetic north guide lines through the map position of each object, *b* and *c*, and with the protractor lay off the respective magnetic azimuths.

(*d*) Prolong the azimuth lines through the points *b* and *c* until they intersect.

(*e*) The intersection of these lines at *a* is the map position sought.



③



④

FIGURE 21.—Location of one's position on a map by resection from three distant points (tracing paper method)—Continued.

e. Location of one's position by resection from three distant points (tracing paper method) (fig. 21).—This method is useful on unoriented maps when the observer is without a compass in indefinite terrain of which only distant prominent features are recognizable or when local attraction due to presence of ore bodies or other material renders the magnetic needle useless.

(1) Select three visible objects on the terrain such as *A*, *B*, and *C*, so distributed that radial lines drawn from observer to each point will yield good angles of intersection (about 30° to 150°) at *O*, the position occupied by the observer (fig. 21①).

(2) Place a piece of tracing paper on a flat surface, supported on a convenient fence post, rock, or on the ground,

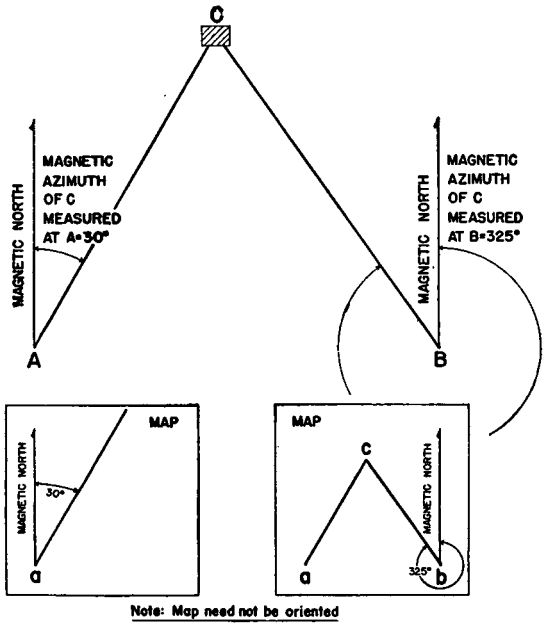


FIGURE 22.—Location on map of distant point by intersection, using compass and protractor.

and set a pin in it at any convenient assumed position of the observer at *O*.

(3) Place any suitable straightedge against the pin, sight along its edge successively to each object, *A*, *B*, and *C*, on the terrain and draw radial lines along the straightedge toward each object (fig. 21②).

(4) Remove the tracing paper and superimpose it over the map (fig. 21③), shifting it about until the three radial

lines pass through the conventional signs *a*, *b*, and *c* on the map which correspond to the three objects sighted on the ground (fig. 21④).

(5) In this position, prick the map through the original pinhole *o* on the tracing. The point thus located on the map is the position of the map reader.

■ 27. LOCATION OF DISTANT POINT BY INTERSECTION.—*a. With compass and protractor.*—It is frequently desirable to locate or post on a map distant or inaccessible objects on the terrain

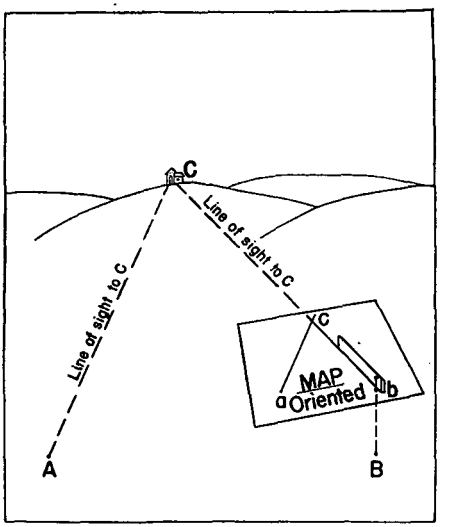


FIGURE 23.—Location on map of distant point by intersection (graphic method).

which do not appear on the map in hand. This may be conveniently done by intersecting lines from two occupied points of known position on the map. Assume that the location of an object *C* shown in figure 22 is desired on a map. In order to locate the position of *C*, one must occupy successively two positions, such as *A* and *B*, from which the object *C* is visible and read the magnetic azimuth of *C* from *A* and *B*, respectively. By aid of a protractor, these azimuths are plotted through the corresponding positions *a* and *b* on the map.

The direction lines prolonged will intersect at *c* on the map, the position sought. Many points may be thus located on the map from two occupied positions.

b. Graphic method (fig. 23).—The observer occupies in succession the positions *A* and *B* on the ground. In each position he rests the map horizontally on some nearby convenient support and sets a pin in the corresponding map positions *a* and *b*, respectively. In each position the map may be oriented with a compass, by inspection, or by alining the positions *a* and *b* on the map with the corresponding objects *A* and *B* on the ground. The last method is the most accurate. At each occupied position a straightedge is placed against the pin in the corresponding position on the oriented map, the object *C*, the position of which is sought, is sighted along the straightedge and a direction line drawn thereto. This results in two such direction lines, one from each occupied position, the intersection of which gives the map position *c* of the object *C*. The results may be checked by a direction line from a third position of the observer.

■ 28. TRAVERSE.—*a.* A series of lines of known distance and direction is called a traverse. An approach route to an assembly area, designated with distances and directions from point to point, would form a traverse.

b. In locating on the terrain objects which do not appear on the map and which cannot be intersected, or in exploring unfamiliar terrain equipped with a compass, the method of traversing is useful. This consists of starting from a known point and following observed compass courses from point to point, measuring distances. These course lines and distances, when plotted to scale on the map, show graphically the course followed and the map location of any desired point on the traverse. Where the distance to the point sought is great and the intervening terrain is rough, it is not practicable to attempt its location by means of a simple straight course. In such cases the traverse would consist of a meander of many straight course lines and angles making changes of direction as influenced by the intervening terrain but ultimately terminating at the point sought. Scouts use this method in registering on a map the route they follow.

SECTION IV

COORDINATES

■ 29. SYSTEMS OF COORDINATES.—*a.* In order to express absolute or relative positions of points, either on a map or on the terrain, one or more of four different systems of coordinates may be selected. Each system has its appropriate use. The names of these systems are as follows:

(1) Polar coordinates.

(2) Rectangular coordinates.

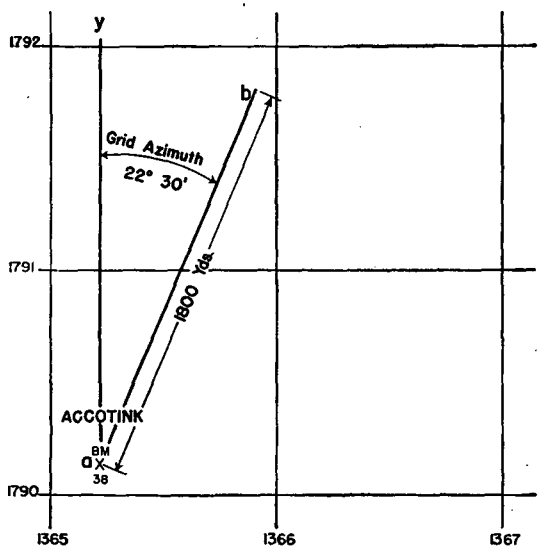


FIGURE 24.—Polar coordinates: BM 38, Accotink (village), distance 1,800 yards, on grid azimuth 22°30'.

(3) Geographic coordinates.

(4) Grid coordinates.

b. Rectangular and polar coordinates are classified as relative coordinates because they are determined by reference to base points (and directions) local to some map and selected by some individual. Thus an indefinite number of polar or rectangular coordinates may be assigned to a single point.

Geographic and grid coordinates are termed absolute coordinates because each is determined by reference to a permanently fixed base point and direction which have been officially adopted for that purpose. Thus only one set of geographic coordinates or, for any grid zone, only one set of grid coordinates can be assigned any point and this set of coordinates is not affected by the selection of map.

■ 30. POLAR COORDINATES.—Polar coordinates are used in designating points located with a compass in the field and in designating positions on maps not equipped with the military grid. They consist of an angle from a known base direction and a distance from a known base position. The base position is the origin of coordinates. It may be a fixed landmark, a survey monument, or any other position easily identified on the map and on the ground. The base direction may be true, magnetic, or grid north or south. The angle may be expressed as azimuth or bearing, the distance in any convenient distance unit. The base position or origin should be fully described.

Examples: Walla Walla quadrangle, BM 1224, on main road 2 miles westerly from Waitsburg, S. 22°45′ W. magnetic (1920) 4.62 miles.

Battle map, Fort Belvoir, 1:20,000 (1935), BM 38, Accotink (village), distance 500 yards N. 30° W. magnetic.

Battle map, Fort Belvoir, 1:20,000 (1935), BM 38, Accotink (village), distance 1,800 yards, on grid azimuth 22°30′. The point so designated is marked *b* in figure 24. The base position, BM 38, is marked *a*, the distance from the base position is the line *ab*, the base direction (grid north) is *ay*, and the angle from the base direction is *yab*.

In dealing locally with many points common to a single map sheet, the sheet reference may be omitted.

a. To plot position of point, polar coordinates of which are given.—(1) Locate on the map the landmark or other base position (origin) given.

(2) Through the base position draw a guide line parallel to the base direction.

(3) With a protractor, point off from the guide line radially about the base position the given angle (azimuth or bearing).

(4) Through the point thus established and the base position (origin) draw a guide line.

(5) Along this guide line from the base position lay off the given distance to scale.

b. To determine polar coordinates of map position with respect to given position and given direction.—(1) Locate on the map the given base position and through it draw a guide line parallel to the base direction.

(2) Draw another guide line through the base position and the point whose polar coordinates are sought.

(3) With the protractor, measure the angle (azimuth or bearing) which the direction line established in (2) above makes with the base direction line established in (1) above.

(4) With a suitable scale at the RF of the map, measure the distance from the base position to the point the coordinates of which are sought.

■ 31. RECTANGULAR COORDINATES.—Rectangular coordinates are used in designating points on ungridded maps without the aid of a protractor. They consist of two distances measured at right angles from a base position. The base position (origin) should be a landmark, survey monument, or other well-established position. The base position, distances, and directions should be fully stated, thus:

Walla Walla quadrangle, NE. cor. T. G. N., R. 36 E., thence due east 811.7 yards, thence due north 409.2 yards.

Battle map, Fort Belvoir, 1:20,000 (1935), BM 38, Accotink (village), 1,500 yards east (magnetic), 1,100 yards north (magnetic. The point so designated is marked *c* in figure 25. The base position, BM 38, is marked *a*, the base direction (magnetic north) is *am*, the direction of the line *ab* (grid east) makes a right angle with the line *am*, and the respective distances are *ab* and *ac*.

a. To plot map position, rectangular coordinates of which are given.—(1) Locate on the map the base position (origin) given.

(2) Through the base position draw a guide line parallel to the base direction.

(3) Through the base position draw a guide line at right angles to the base direction.

(4) From the base position along these lines point off to scale the respective distances in the respective directions as given.

(5) Treat these distances as the adjacent sides of a rectangle; complete the rectangle (other two sides) with construction lines. The intersection of these two construction lines is the point sought.

b. To determine rectangular coordinates of map position with respect to given base position and direction.—(1) Identify on the map the given point and the given base position.

(2) Through the base position draw a guide line parallel to the base direction.

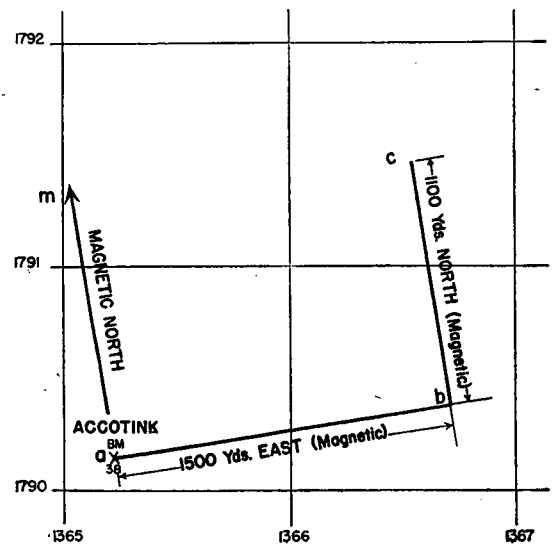


FIGURE 25.—Rectangular coordinates: BM 38, Accotink (village), distance 1,500 yards east magnetic, 1,100 yards north magnetic.

(3) Through the base position draw a guide line at right angles to the base direction.

(4) Through the given point drop perpendiculars to the lines established in (2) and (3) above.

(5) From the base position scale the distance along the guide lines of (2) and (3) above to the respective perpendiculars. These distances are the rectangular coordinates sought.

■ 32. GEOGRAPHIC COORDINATES.—The system of latitude and longitude lines projected on a map represents the geographic or spherical grid covering the earth. In this system the base position (or origin) is the intersection of the meridian of Greenwich, known as the prime meridian, with the Equator. The base direction is true north (or south). Distance on the spheroid (earth) is reckoned in units of degrees, minutes, and seconds of latitude up to 90° north or south of the Equator, and in degrees, minutes, and seconds of longitude up to 180°, east or west of the prime meridian. The location of any point on the surface of the earth is defined in terms

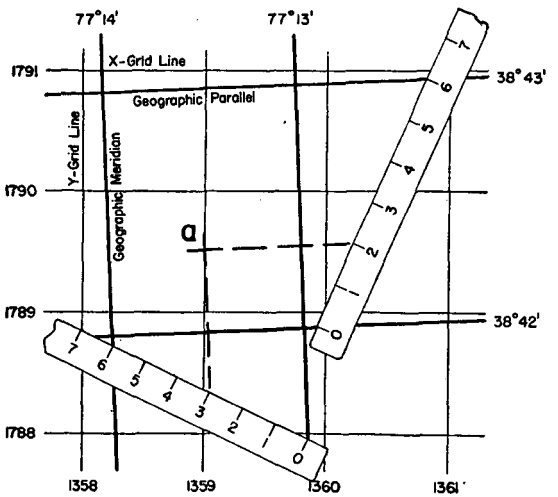


FIGURE 26.—Geographic coordinates: latitude 38°42'20" N., longitude 77°13'30" W.

of the parallel of latitude and the meridian of longitude which intersect at the point, thus, latitude 38°32'20" N., longitude 77°34'30" W. The latitude and longitude of a point constitute its geographical or spherical coordinates. However, meridians of longitude converge at the poles. Therefore, units of longitude decrease in units of linear distance from a maximum at the Equator to zero at the poles. Since the sphere cannot be developed as a plane, other variations are introduced in maps by the chracteristics of pro-

jections used in map construction. While units of latitude and longitude can be converted to distances in meters, yards, miles, etc., by computation or use of tables, the spherical units would not occur, except by fortunate coincidence, in rational multiples of the linear unit. Lines of the spherical grid are necessarily curves or projections of curved lines and vary with latitude and projection. Such variations from straight lines and true distances within the scope of a sheet of the terrain or the tactical map are negligible. For practical map-reading purposes they may be disregarded and the spherical grid may be treated graphically in all respects as a rectangular grid. The 5-minute lines of the geographic grid appear in full or by border registration on topographic sheets. The 1-minute lines of the geographic grid appear registered on some large-scale maps by border ticks and grid intersections. Geographic coordinates are used in designating positions in large indefinite areas, in unmapped areas, and on geographic (ungridded) maps.

a. To plot positions of point, geographical coordinates of which are given.—(1) Identify on the map the two lines of the geographic grid, both of latitude and longitude, which fall nearest to and on each side of the position to be plotted. This may be readily done by inspection of the map in comparison with the given coordinates. In case the lines of the grid do not appear in full on the map, draw in the lines by joining the border ticks and grid intersections. In either case the point sought falls somewhere within the quadrangle whose sides are lines (arcs) of known latitude and longitude. For a battle map (1: 20,000), this is a 1-minute quadrangle (60 seconds by 60 seconds). For a topographic sheet, this is a 5-minute quadrangle (300 seconds by 300 seconds).

(2) The problem then reduces itself to the mechanical operation of dividing the quadrangle into seconds of longitude and seconds of latitude, pointing off the seconds place required by each coordinate. One of these points will fall on the meridian of longitude which passes through the point sought. The other will fall on the parallel of latitude which passes through the point sought. The significant parallel of latitude and meridian of longitude are now struck in as guide lines. Their intersection is the point sought.

(3) Points on the significant parallel of latitude and meridian of longitude are readily located with the engineer's scale

used as a diagonal scale of proportional parts between the available grid lines. For the 1-minute grid the scale should be placed across the lines at any angle so that 60 convenient divisions span the distance. For the 5-minute grid 300 divisions of the scale should span the distance between lines. In each case each division of the scale indicates a second of latitude or longitude, depending upon which coordinate is being plotted.

(4) Figure 26 illustrates the location of a point *a*, the geographic coordinates of which are latitude 38°42′20″ N., longitude 77°13′30″ W.

b. To determine geographic coordinates of map positions.—(1) By inspection of the map, identify the grid quadrangle in which the point lies, drawing in the sides of the quadrangle when the grid appears registered only. The value in degrees and minutes of the meridians of longitude and parallels of latitude which form this quadrangle appears in print on the borders of the map. The problem, then, is to determine the position of the point within the quadrangle in seconds of latitude and seconds of longitude.

(2) Use the engineer's scale as a scale of proportional parts as described in *a*(3) above to establish the seconds lines within the significant quadrangle, except in each case (the two positions of the scale, one for latitude and one for longitude, respectively) the scale should pass through the point whose coordinates are desired. The number of seconds sought may now be read directly from the edge of the scale at the point in the direction of increasing grid values within the grid quadrangle. This added to the recorded value in degrees and minutes of the side of the significant quadrangle lowest in value yields the coordinate sought in degrees, minutes, and seconds.

■ 33. GRID COORDINATES.—*a. General.*—(1) In order to provide a standardized system of rectangular coordinates which are easy to read, the military grid is printed upon the map. The grid is composed of a set of parallel grid north and south lines showing distances in thousands of yards grid east of the origin, and a set of grid east and west lines showing distances in thousands of yards grid north of the origin of coordinates for the grid zone. The distance of any point grid east of the origin is called the *X*-coordinate. The distance

of any point north of the origin is called the *Y*-coordinate. In writing coordinates the *X*-coordinate is written first and the *Y*-coordinate last, with a dash between, and the whole inclosed within parentheses. Thus in figure 27 point *A* is located at (198–262). The coordinates are read in the same manner as they are written. In locating a point the key phrase "READ—RIGHT—UP" should be remembered.

(2) Coordinates are written and read to 1,000 yards and decimal parts thereof. In figure 27 the coordinates of point *B* are (197.8–263.7).

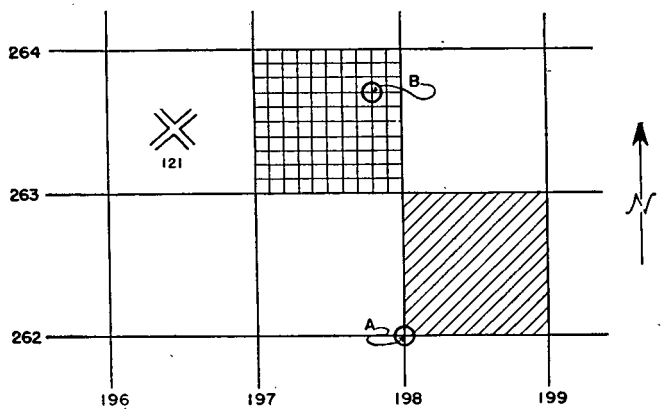


FIGURE 27.—Coordinates.

(3) It is customary to drop all but the last two digits; hence the coordinates of point *B* may be written or read (97.8–63.7).

(4) When a point is easily identified and only one of such exists within the grid square, it is necessary merely to refer to the southwest corner of the grid square in which it is located. For example, in figure 27 crossroads 121 could be designated as "CR 121 (96–63)."

b. Coordinate scale.—The use of the coordinate scale in reading or plotting the coordinates of a print on a map is explained in detail in FM 21–25.

c. Coordinates with engineer's scale.—The engineer's scale or any other suitably graduated scale may be used conveniently as a scale of proportional parts to plot a point within

the significant grid square. Let it be required, for instance, to plot a point *N*, the coordinates of which are (25.35–76.60) (fig. 28). Select any 10 equal subdivisions on the scale such that their total length is equal to or slightly greater than the grid interval on the map. Lay the scale on the map in position ① shown in figure 28 so that the zero is on the 25,000 grid line and the 10 is on the 26,000 grid line. Mark on the map the point *a* at 3.5 on the ruler. Slide the scale down to position ② and again mark on the map the point *a'* at 3.5 on the scale. Draw the line *aa'*. Now place the scale on the map in position ③ so that the zero is on the 76,000 line and

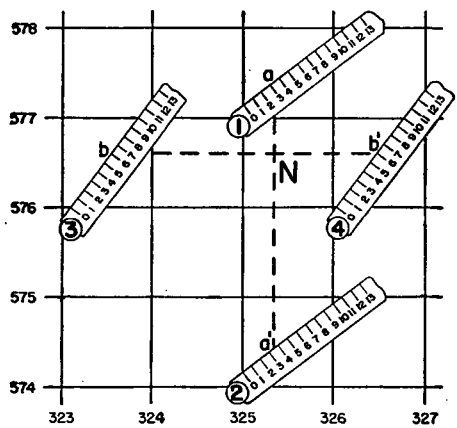


FIGURE 28.—To plot position of point (25.35–76.60) with engineer's scale on terrain map (1: 20,000) having 1,000-yard grid. (Not reproduced to scale.)

the 10 is on the 77,000 line. Mark on the map the point *b* at 6.0 on the scale. Slide the ruler to the right to position ④ and again mark on the map the position *b'* at 6.0 on the scale. Draw the line *bb'*. The intersection of the lines *aa'* and *bb'* is the plotted point *N* required. If desired, the subdivisions may be further subdivided into 10 equal parts, as on the engineer's scale, to give the position of the point by grid lines of 10-yard intervals. It can be seen that reading coordinates with the engineer's scale is accomplished in the same manner. (See fig. 29.)

■ 34. MILITARY GRID SYSTEM.—*a.* The standardized system of rectangular coordinates discussed in paragraph 33 is the grid system devised for use on military maps in order to avoid the difficulties and inconveniences inherent to the spherical grid. A rectangular grid superimposed on a polyconic projection of the whole continental United States would prove no more useful than a map on that projection and for the same reasons. Distances on the rectangular grid would vary prohibitively from true ground distances in the distorted areas near the edges of the map. However, by limiting the width of the projection to about 9° of longitude, the maximum distortion along the edge of the projection never exceeds 2.57 yards per 1,000 yards, or about ¼ of 1 percent, an error of

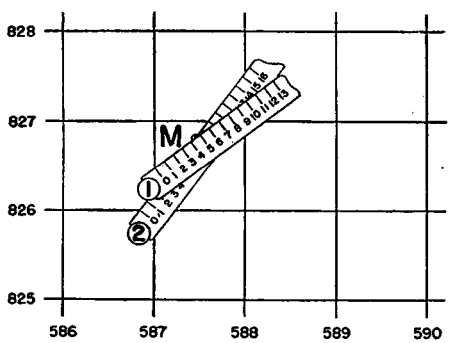


FIGURE 29.—To read grid coordinates of point (87.45–26.80), on terrain map (1: 20,000 scale) having 1,000-yard grid, with engineer's scale.

no military consequence, since the changes in dimensions of an ordinary map sheet due to weather conditions may exceed that amount.

b. For the purposes of superimposing the rectangular grid, the northern half of the continental Western Hemisphere has been divided into seven zones, each 9° of longitude wide. Each zone is a separate polyconic projection. When the military grid system was first established it extended from 28° N. latitude to 49° N. latitude. This system, known as the continental system, was sufficient for continental United States only. Later, in order to take care of Panama and the Caribbean area, the equatorial system, extending from

7° N. to 28° N., was set up. These two systems have different *Y* origins, and hence any point in this area will have the same *X*-coordinate in both systems but different *Y*-coordinates. All grids are identical in structure but each has a separate origin 8° of longitude distant from its neighbor.

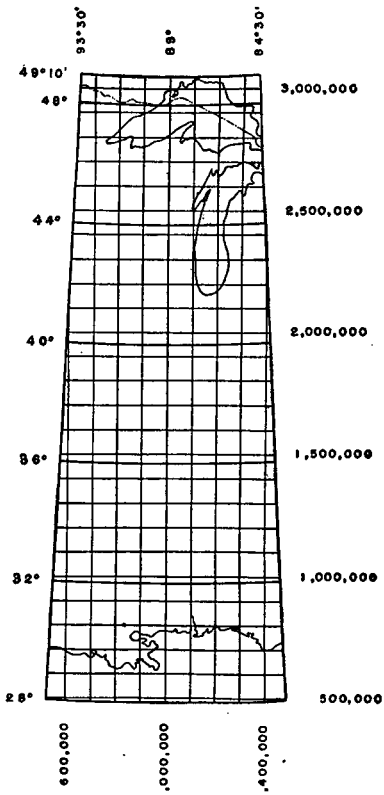


FIGURE 30.—Special military map of continental system grid zone C.

The grids therefore overlap 1° of longitude along the borders, with a net width of 8° of longitude between the central meridians of the overlaps. These zones are designated by a letter in accordance with the following table, that portion

TABLE III.—*Grid zone systems in northern half of continental Western Hemisphere*

Zone	Limiting meridian of zones	Origin of coordinates X	Grid values assigned to origin X yards	Equatorial system		Continental system	
				Origin of coordinates Y	Grid values assigned to origin Y yards	Origin of coordinates Y	Grid values assigned to origin Y yards
A	68°30′ W., 77°30′ W	73° W	1,000,000	Equator	Zero	40°30′ N	2,000,000
B	76°30′ W., 85°30′ W	81° W	1,000,000	do	do	40°30′ N	2,000,000
C	84°30′ W., 93°30′ W	89° W	1,000,000	do	do	40°30′ N	2,000,000
D	92°30′ W., 101°30′ W	97° W	1,000,000	do	do	40°30′ N	2,000,000
E	100°30′ W., 109°30′ W	105° W	1,000,000	do	do	40°30′ N	2,000,000
F	108°30′ W., 117°30′ W	113° W	1,000,000	do	do	40°30′ N	2,000,000
G	116°30′ W., 125°30′ W	121° W	1,000,000	do	do	40°30′ N	2,000,000

of the State of Maine falling to the east of longitude 68°30′ being included in zone A.

c. The limits of the grid zones are shown in table III and illustrated in figure 31. The zone letter appears on all maps containing grids. In designating points by grid coordinates,

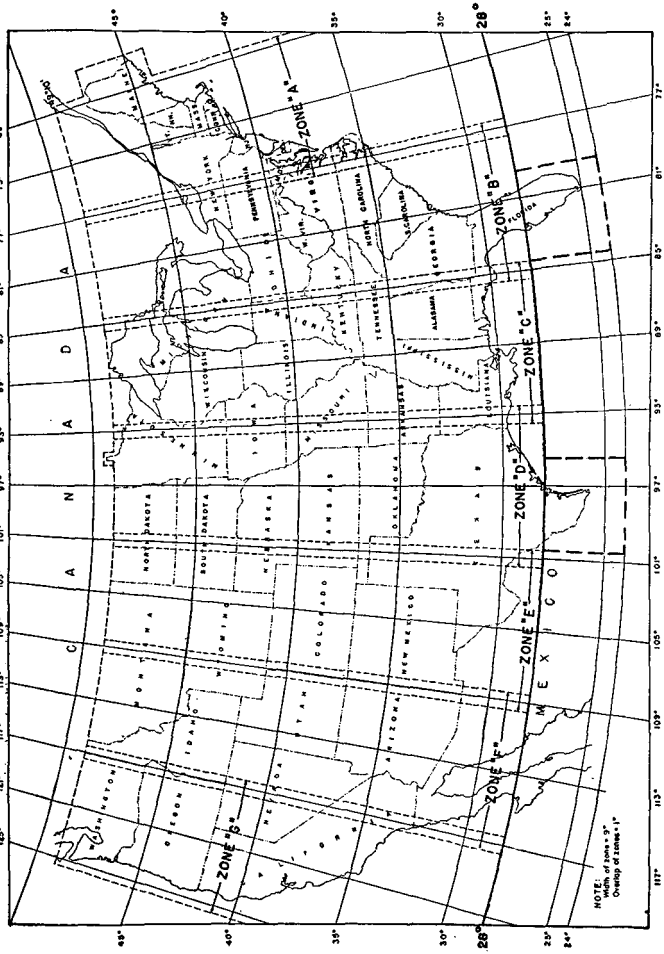


FIGURE 31.—Designation of military grid systems.

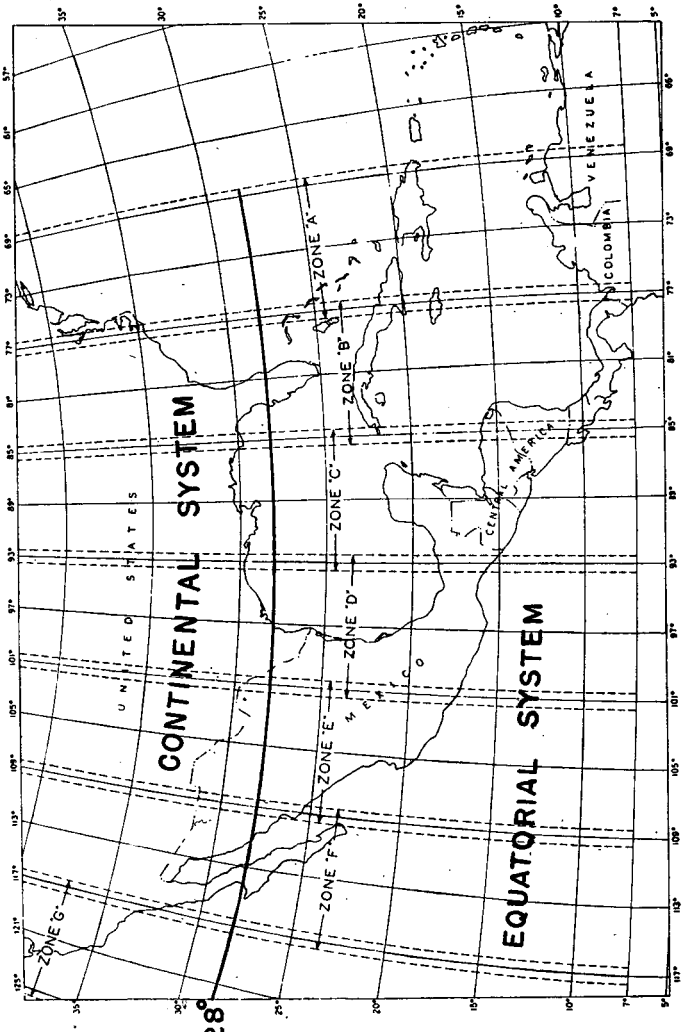


FIGURE 31.—Designation of military grid systems—Continued.

the name of the map sheet and not the zone letter should be used as primary reference.

■ 35. CONTINENTAL SYSTEM.—*a.* In each zone the intersection of its central meridian with the parallel of latitude 40°30′ is selected as the origin of coordinates designated by *O*. The central meridian is chosen as the *Y*-axis and a right line tangent to latitude 40°30′ at *O* is chosen as the *X*-axis. In terms of yards, the grid coordinates of all 5-minute intersections of latitude and longitude within the whole grid zone are computed with respect to these axes and the origin *O*. The coordinates of intersections in all other quadrants, except the first, involve some negative quantities which are undesirable for simplicity. In order to make positive all coordinates which appear on military maps embraced within the zone, the computed values are transferred to a new origin *O′* exactly 1,000,000 yards grid west and 2,000,000 yards grid south of the origin *O*. This is effected by simply adding 1,000,000 yards to all computed *X*-coordinates and 2,000,000 yards to all computed *Y*-coordinates. It is the point *O′* and axes *O′–X* and *O′–Y* to which all grids and grid values appearing on all military maps are related. The original origin *O* has no further significance. This scheme is shown in figure 30 and table III, and the rectangular grid system illustrated therein is referred to as the military grid system.

b. Since the grids for all zones are identical in structure, only one set of original computations suffices for all zones simply by changing in the tables the longitude values successively through 8°, 16°, 24°, etc., of longitude, respectively. (See Special Publication 59, U. S. Coast and Geodetic Survey.)

c. The military grid appears registered on gridded maps in two series of parallel lines at right angles to each other. On sheets of the terrain map (1: 20,000), these lines form 1,000-yard squares. On sheets of the tactical map (1: 62,500), these lines form 5,000-yard squares. The central meridian of the overlap between adjacent grid zones is the dividing line between the zones. Any map which falls within the 1° overlap between grid zones always shows in solid black lines the grid of the zone to which the map pertains. The grid of the adjacent overlapping zone may also appear registered by means of grid intersections (small crosses) on the face of the sheet and ticks around the border lines. The scheme is useful in effecting

transition of data from one zone to another. The lines of the overlapping zone when needed may be struck in by simply joining the registration points. Since the grid lines of each zone are all parallel to the central meridian of the zone and since meridians converge to the poles, the lines of overlapping grids will always cross at distinct angles.

d. The distance of each north and south grid line, grid east of the zero point or origin of coordinates, is marked in thousands of yards along the south border of a gridded map. The distance of each east and west grid line, grid north of the zero point or origin, is marked in thousands of yards along the west border of a gridded map. The numbers which identify the north and south grid line and the east and west grid line which intersect at or nearest to the southwest corner of a gridded map are written out in full in yards. In marking all other grid lines, the digits common to the sheet may be omitted. When the grid of an overlapping zone appears registered by ticks and grid intersection on a map, the ticks of the north and south and east and west grid lines, respectively, which intersect at or nearest to the southeast corner, are marked in full to yards. No other grid lines of the overlapping zone are marked.

e. By agreement with the War Department, sheets of the topographical atlas of the United States Geological Survey adopted as tactical maps will have the 5,000-yard grid registered by ticks along the borders.

NOTE.—The above methods of showing grids on a map are followed by the Corps of Engineers in the reproduction of all gridded maps. There are maps in common use for school purposes, such as the Gettysburg map, on which only a local grid system is used. The reader should not confuse such a grid with the military grid system.

■ 36. EQUATORIAL SYSTEM.—*a.* The equatorial system, using the same zones as the continental system, has the latitudinal origin at the Equator, and covers the area between the 7° N. and 28° N. parallels. The system is otherwise similar to the continental system. Tables and methods of computation for the equatorial system are found in Corps of Engineers publication "Grid System for Military Maps for 7° to 28° North Latitude."

b. In the overlapped areas below 28° N. in Texas and Florida, care must be taken not to confuse the two grid systems. In the absence of other data, it may be assumed

that the continental system is used within the limits shown on figure 31②.

■ 37. DETERMINATION OF UNKNOWN DIRECTIONS, DISTANCES, OR COORDINATES.—*a. To determine distance between two points, grid coordinates of which are given.*—(1) *Graphically.*—Plot

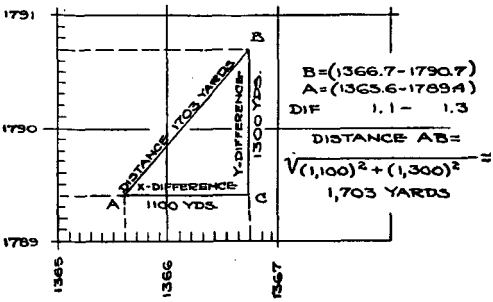


FIGURE 32.—Distance between two points on map by solution of right triangle.

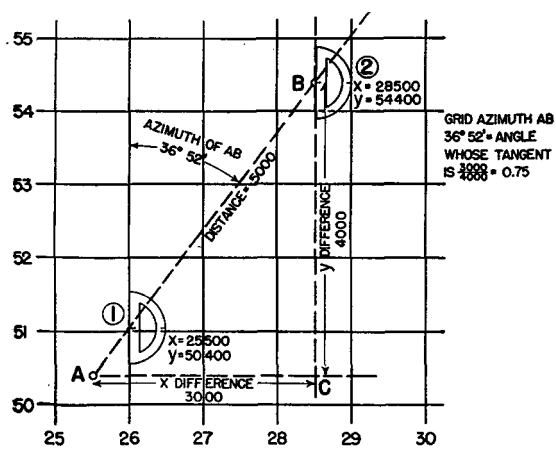


FIGURE 33.—Determination of grid azimuth of line on gridded map.

the positions of the two points on the map. If no map is available, plot the relative position of the points to scale on an improvised grid. In either case, scale directly the distance between the plotted points.

(2) *By solving right triangle* (fig. 32).—The distance between the two points is the hypotenuse of a right triangle whose legs are the differences, respectively, between the *X*- and *Y*-coordinates of the two points. The distance in yards is therefore the square root of the sum of the squares of *X* difference and *Y* difference. The method is completely illustrated in figure 32.

b. To determine grid azimuth of line between two points, grid coordinates of which are known (fig. 33).—(1) *From map.*—Plot the position of the two points *A* and *B* on the map or plot the relative position of the points on an improvised grid to scale as shown in figure 33. Join the plotted positions by a straight line and prolong if necessary to intersect a north-sound grid line. With a protractor, as shown in figure 33①, measure the angle from the north-south grid line clockwise to the straight line indicating the significant direction, bearing in mind that a line has two directions differing in azimuth by 180°.

(2) *By plotting right triangle.*—Plot to scale on plain or cross-section paper or the gridded map the right triangle whose legs are the *X*-difference and the *Y*-difference of the given coordinates of the respective points which may be represented by *A* and *B* in figure 33. In the triangle *ABC* so formed, *CB* is the base or grid north direction. With the protractor at *B* (fig. 33②), measure clockwise the angle from *CB* prolonged either to *AB* prolonged or to *BA*, depending upon which azimuth (differing by 180°) is required.

(3) *By trigonometric functions* (fig. 33).—(*a*) The grid azimuth sought is, by inspection of the figure, seen to be equal to the angle *ABC*, whose tangent is

$$AC/BC=\frac{X\text{-difference}}{Y\text{-difference}}=3{,}000/4{,}000=0.75$$

(*b*) From a table of natural tangents this corresponds to the angle 36° 52′, which is the grid azimuth of the line in the first quadrant.

(*c*) In the SE quadrant subtract this angle from 180°, in the SW quadrant add to 180°, and in the NW quadrant subtract from 360°.

(*d*) The method is useful when the points fall on separate sheets or the map is distorted.

c. Determination of coordinates of point when distance and directions are given from point with known grid coordinates.—

When the distance between two points is comparatively great or lie on sheets of a different scale, the coordinates of one are established mathematically from the one with known coordinates as follows:

(1) Convert direction into bearings using grid north (see par. 21).

(2) Look up sine and cosine of the angle and multiply by the distance.

(3) The sine multiplied by the distance will give the east or west distance to be added algebraically to the first coordinate given; an east bearing is plus; a west bearing is minus.

(4) The cosine multiplied by the distance will give north or south distance to be added algebraically to the last coordinate given; a north bearing is plus; a south bearing is minus.

(5) *Example* (fig. 34).

Given: Coordinates of point *a* (898–252).
Direction of line from *a* to *b*=magnetic azimuth 317° 28′.
Grid declination 9°31′.
Distance 9,720 yards.

Required: Coordinates of point *b*.

Solution: Grid azimuth=317°28′ plus 9°31′=326°59′.
Bearing=360° minus 326°59′=N. 33°01′ W.
From tables of natural trigonometric functions—
Sine 33°01′=0.54488.
Cosine 33°01′=0.83851.
0.54488 times 9,720=5,296 yards.
0.83851 times 9,720=8,150 yards.
Coordinates (898–252 mean 898,000 yards east of basic origin and 252,000 yards north of basic origin.
Since the bearing of the line is N. 33°01′ W. (IV or NW quadrant).
898,000—5,296=892,704 yards.
252,000+8,150=260,150 yards.
Hence coordinates of point *b* are (892.7–260.2).

d. To superimpose grid on map from point with known grid coordinates (fig. 35).—Establish, by some means previously

mentioned, the grid north on the map. Draw lines *N—S* and *E—W* through the known point. Along these lines scale off the desired grid spaces. Extreme care should be exercised in establishing a grid from one point to insure accuracy.

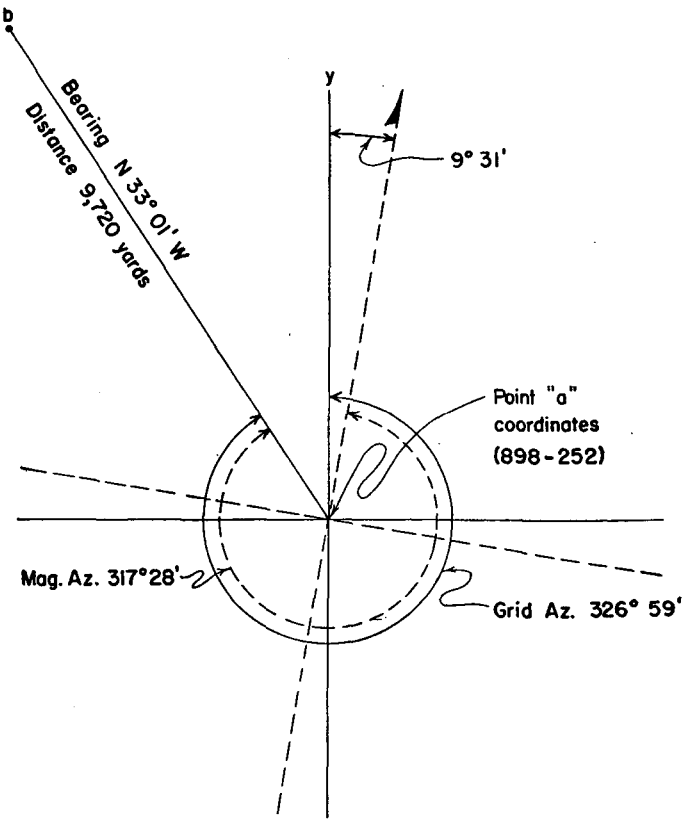


FIGURE 34.—Grid coordinates from known point.

When some other point of known coordinates exists on the map a check should be made with it.

■ 38. CONSTRUCTION OF MILITARY GRID FROM GEOGRAPHIC COORDINATES.—For transformation of geographic coordinates

to grid coordinates, or vice versa, see United States Coast and Geodetic Survey Special Publication No. 59 and "Grid System for Military Maps for 7° to 28° North Latitude"; paragraph 61, TM 5–230; and paragraph 117*f*, TM 5–235.

SECTION V

ELEVATION AND RELIEF

■ 39. ELEVATION.—Elevation is the measure of vertical distance from a known datum plane. For most maps the datum

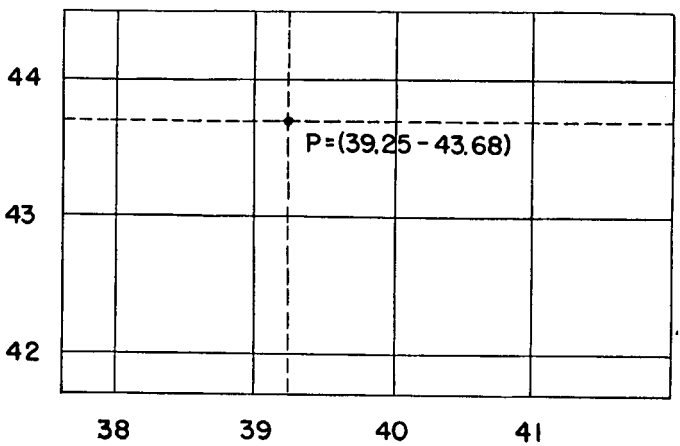


FIGURE 35.—To superimpose a grid on a map from a point with known coordinates.

is mean sea level and zero elevation. Elevation is expressed in feet above or below mean sea level. When above mean sea level, elevation is plus; when below mean sea level, elevation is minus. Where no indication is given the elevations are always taken as plus.

■ 40. RELIEF.—*a.* The variation in the height of the earth's surface, as ridges, valleys, etc., is termed "relief." As the exact nature of the terrain has a marked influence on military operations, it is important that the military commander of every unit familiarize himself with the "lay of the land" in which he is operating. This familiarity cannot always be

obtained by actual reconnaissance beforehand but often must be gained solely by study of topographic maps. The map, then, must convey to the map reader a definite impression of the ground forms. The ability to comprehend relief from the map requires an understanding of the way in which the various ground forms have been produced by nature.

b. There is a considerable degree of regularity and system in ground forms, due to erosion. Not all the water from heavy rains can seep into the soil; much of it runs off. At one point a little stream begins; as it flows downward another joins it; soon several unite into a fair-sized creek, which rushes along, carrying its burden of soil into the main valley, whence the river may carry it into the sea. This simple process, continued for ages, has sufficed to carve the surface of the earth into the form we find today.

c. Since most of our present ground forms are the result of erosion, it is evident that the drainage scheme of an area is the key to its topography. On maps where streams are indicated and on aerial photographs, this key is in evidence; converging streams show a general slope to a valley; diverging fingers of streams portray a crest or ridge. The drainage net and ridge lines constitute the "master lines" of the terrain. Points of change in horizontal or vertical direction of these lines are known as "critical points." Getting the "lay of the land" consists of grasping the significance of these master lines. The method adopted for showing relief on a map must be one which will convey to the map reader an immediate conception of the drainage and ridge lines of the system of relief.

■ 41. METHODS OF REPRESENTING RELIEF.—Since the map is flat, special conventional signs are necessary to show relief. The most common methods used on maps are as follows:

a. Hachures (fig. 36).—A method frequently used to indicate relief in a general way is by the use of hachures. It is particularly useful when the available data are inadequate for the more accurate representation of relief by contours, or when the purpose of the map does not justify the more complicated and time consuming methods. This method of representing relief has been adopted for the Strategic Map of the United States (scale 1:500,000) and will be frequently found on large as well as small scale foreign maps. Hachures

are short parallel or slightly divergent lines drawn in the direction of slopes, closely spaced on steep slopes, wide apart on gentle slopes, and convergent toward the tops of ridges and hills. The resulting shadow effect gives an excellent pictorial representation of hilltops, ridges, and valleys, and enables the map reader to gain a fair conception of the relative slopes of various parts of the terrain.

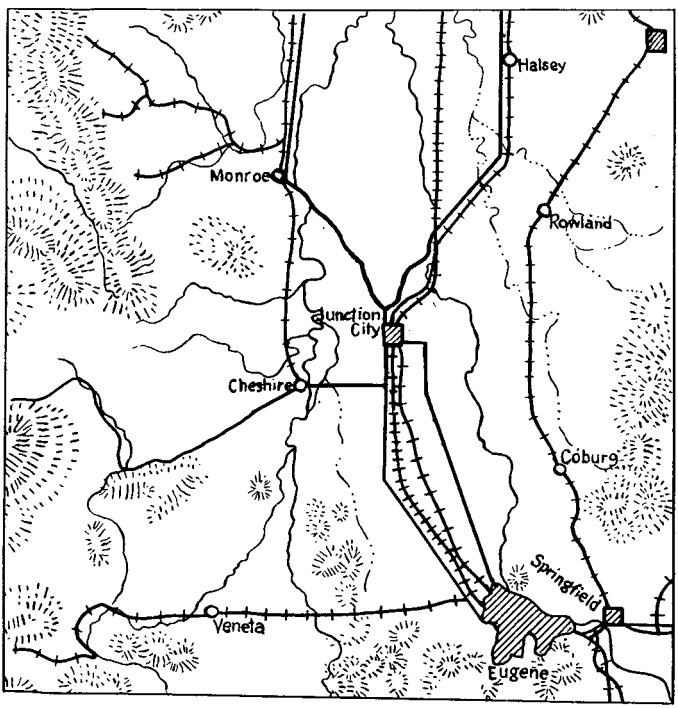


FIGURE 36.—Relief by hachures.

b. Color-layer system.—Color-layer systems of relief representation consist of using different colors or different tones of the same color to distinguish different zones of elevation. These resulting color bands are bounded by contours which are usually shown on the map. Contours falling within color zones are usually omitted. A key to the color system showing

the succession of colors and the elevation zones to which they pertain is given on the map margin. The colors of the elevation gradient should be selected to produce a harmonious effect but there should be sufficient contrast between the colors to insure ease of reading. This method is used on aerial navigation charts published by the Army. The color gradient used on these maps is shown in FM 21–30.

c. Contours.—A contour line represents an imaginary line on the ground, every part of which is at the same elevation usually applied to mean sea level. Such a line could be drawn at any altitude but in mapping only the contours at regular intervals of altitude are shown. The line of the seacoast itself is on the zero contour line if mean sea level is assumed to be the zero datum plane. If the sea should rise 20 feet above mean sea level, the new seacoast line would then be on the 20-foot contour line. Contour lines show the shapes of the hills, mountains, and valleys, as well as their altitudes. Successive contour lines that are far apart on the map indicate a gentle slope; lines that are close together indicate a steep slope; and lines that run together indicate a cliff. Contour lines never cross except in the case of an overhanging cliff. The sketch in figure 37① represents a river valley that lies between two hills. In the foreground is the sea, with a bay that is partly inclosed by a hooked sand bar. On each side of the valley is a terrace into which small streams have cut narrow gullies. The hill on the right has a rounded summit and gently sloping spurs separated by ravines. The spurs are truncated at their lower ends by a sea cliff. The hill at the left terminates abruptly at the valley in a steep scarp from which it slopes gradually away and forms an inclined tableland that is traversed by a few shallow gullies. The manner in which contour lines express altitude, form, and grade is shown in figure 37②. Each feature shown in figure 37① is represented on the contour map (fig. 37②) directly beneath its position in figure 37①.

d. Depth curves.—A contour showing points of equal elevation below the level of any body of water is called a depth curve. These curves will indicate depths below a certain datum, usually mean low water level for the body of water concerned. The vertical interval is frequently expressed in fathoms (6 feet).

■ 42. CHARACTERISTICS OF CONTOURS.—In order to appreciate the representation of relief and elevation differences by contours, study must be given to the basic characteristics of them. FM 21–25 describes very thoroughly these characteristics. Briefly, it may be observed that contours on a map—

a. Are wavy in appearance.

b. Are usually V-shaped in narrow valleys and U-shaped on noses of hills.

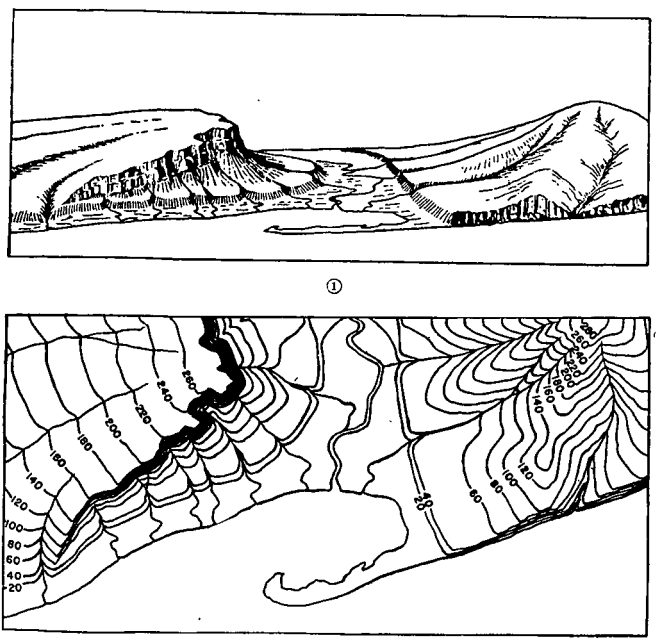


FIGURE 37.—Relief by contours.

c. Always close, on or off the map.

d. Are at right angles to the lines of steepest slope.

e. Are spaced directly as the variation of the slope; close on steep slopes, far apart on gentle slopes.

f. Are roughly parallel to the adjacent contour lines. Figure 38 shows the relation of profile to contours.

■ 43. CONTOUR INTERVAL.—*a.* The contour interval, or the vertical distance in feet between one contour and the next, is stated as marginal information, usually under the scale, at the bottom of each map. This interval differs according to the topography of the area mapped and the scale of the

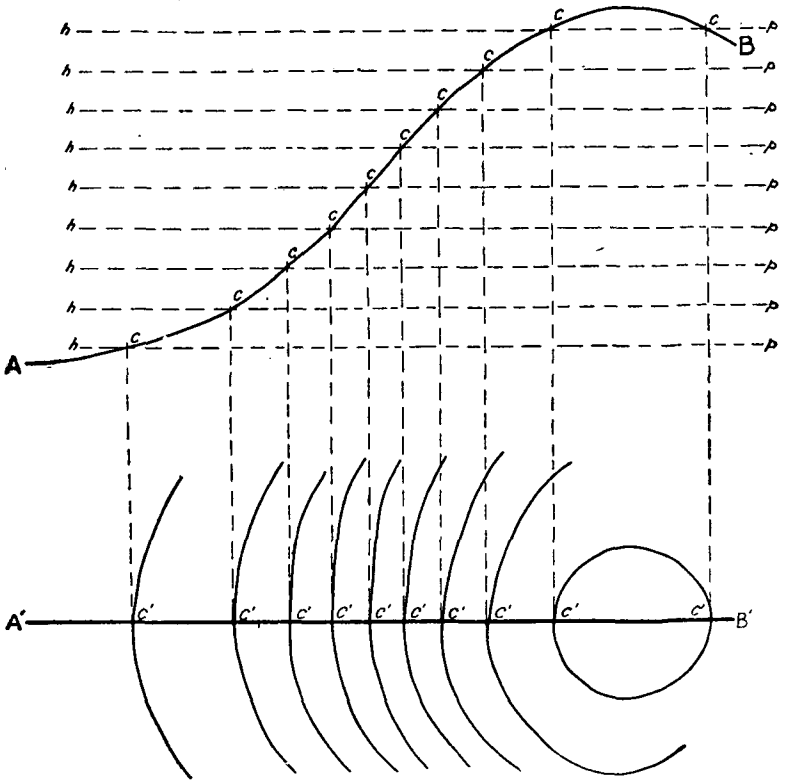


FIGURE 38.—Relation of profile to contours.

map; in a flat country it may be as small as 1 foot; in a mountainous region it may be as great as 250 feet.

b. For military use it is necessary that the various sheets of a map of any given area have a common scale and contour interval or intervals that match. In order that peacetime

practice throughout the United States be consistent, the War Department (AR 300–15) and the United States Geological Survey have adopted the following contour intervals for standard quadrangle maps. The intervals in general conform to contour intervals found on most existing topographic maps.

(1) Contour intervals of 5, 25, 50, or 100 feet in the States which lie all or mostly west of longitude 103° as follows: Washington, Oregon, California, Idaho, Nevada, Utah, Arizona, Montana, Wyoming, Colorado and New Mexico.

(2) Contour intervals of 5, 10, 20, 40, or 100 feet in the States which lie all or mostly east of longitude 103°. The 5-foot contour interval is used only on large-scale maps of limited areas.

c. On most maps every fifth contour line is made heavier than the others and is accompanied by figures showing the altitude at convenient intervals.

■ 44. ELEVATIONS OF IMPORTANT FEATURES.—The elevations of important features such as road junctions, summits, and surfaces of lakes, called spot heights, and those of bench marks are given on the map in figures to the nearest foot. More exact altitudes of bench marks are published in bulletins that are issued by the Geological Survey and the Coast and Geodetic Survey. On coastal charts the datum is mean low water.

■ 45. INTERPRETATION OF RELIEF BY CONTOURS AND MARKED POINTS OF ELEVATION.—*a.* Further understanding of the means of representing and interpreting relief and elevation on maps may be obtained from a study of the sketch represented in figure 39. This shows a section of a map contoured with a vertical interval of 20 feet.

b. The numbers along the edge of the sketch represent the respective elevations of the contours above mean sea level. By following the several contours across the sketch the elevations of various points may be determined. By study of the contour net as a whole the relief of the ground may be interpreted quickly by the practiced map reader. Thus the closed contours at points *X*, *Y*, and *Z* indicate hilltops. The numbers indicate that these hills are at elevations of 1,110, 1,130, and 1,105 feet, respectively. In speaking of unnamed hills on a topographical map, they are referred to by use of

their elevation; for example, hills *Y* and *Z* would be designated hill 1,130 and hill 1,105, respectively.

c. A further study of the sketch will indicate how the various terrain features are recognized. Point *K* represents a saddle between hills *X* and *Y*. It is also the watershed between the head of the stream system at *P* and the slope toward the bottom of the sketch from point *A*. The elevation of point *K* is approximately 1,030 feet (being between the 1,020- and 1,040-foot contours). Point *N* between hills *Y* and *Z* represents a saddle at an approximate elevation of 1,090

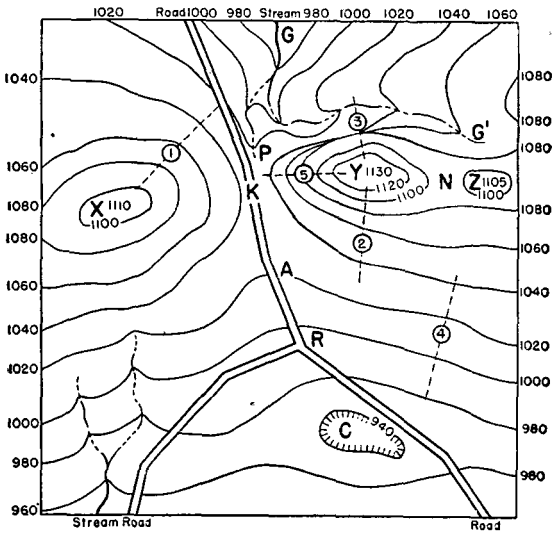


FIGURE 39.—Interpretation of relief.

feet. Along the dotted line ①, the uniform spacing of the contours and their distance apart indicate a uniform, gentle slope. Along the dotted line ②, the spacing of the contours is irregular, indicating varying slopes. Along the dotted line ③, the slope is steep, terminating in a cliff where the contour lines meet each other. Along the dotted line ④, the contours, being almost straight, nearly parallel and quite far apart, represent a very gently sloping plane surface. Along the nose indicated by the dotted line ⑤, the contours

are U-shaped with the botton of each U pointing down hill. Where the contours cross the stream valley G–G', they run up the valley on one side of the stream, turn in a sharp V and run back down on the other side; the bottom of the V formed at the stream crossing points up stream in contradistinction to the U's of the contours on the shoulder of the ridge at ⑤.

d. Since on maps, road junctions usually are given a number corresponding to their elevations above sea level, the road junction at *R*, about halfway between contours 980 and 1,000, would be designated *RJ* (road junction) 990. Crossroads are designated *CR* (followed by the elevation in the same way).

■ 46. APPROXIMATE CONTOURS AND FORM LINES.—*a. Approximate contours.*—When it has not been possible for the topographer to locate accurately contours for a map, they are shown to be approximate only by the use of broken lines.

b. Form lines.—Form lines are similar to contours in that they are drawn at right angles to the direction of steepest slope. However, form lines have no fixed interval and do not indicate elevations. Their purpose is to show the configuration of the ground.

■ 47. LOGICAL CONTOURING.—*a.* In mapping, contouring may be done by the topographer in the field by one of several methods:

(1) He may actually run out the location of the contours on the ground. This method is applicable to large-scale maps when great accuracy is desired and the expenditure of time and labor is economically justified.

(2) He may run out enough contours to define the ground forms and interpolate between them by eye.

(3) He may run out only stream and ridge lines, getting elevations on these lines at each change of slope or ground form. Such elevations defining the ground forms are known as "critical elevations." The contours may then be sketched in the field by eye between critical elevations. This method is the cheapest, quickest, and most commonly used.

b. Logical contouring may best be explained by an illustrative example. In figure 40① critical elevations have been measured by the topographer. The problem is to interpolate

10-foot contours so that the ground forms depicted will be logical.

(1) First, along the main stream, interpolate the elevations of all stream junctions not shown by assuming that the stream has a uniform slope between critical points. For example, there is a stream junction of unknown elevation

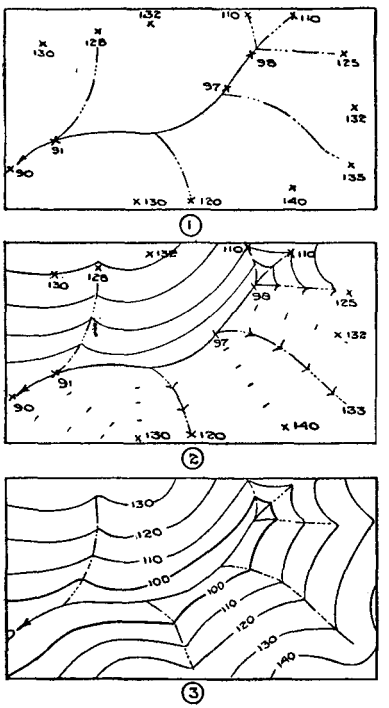


FIGURE 40.—Method of drawing contours by interpolation on drainage net where elevations are given.

between elevations of the stream of 91 and 97 feet, respectively. Between these two points the stream rises 6 feet. Because the stream junction, the elevation of which is sought, is approximately half the distance measured along the stream between elevations 91 and 97, it is assumed that the stream

has risen to that point only one-half of 6, or 3 feet. The elevation sought is therefore 94 feet.

(2) In this way, interpolate elevations which are multiples of 10 feet on all the streams. These are the points where contours cross the stream and are shown as V-shaped marks pointed upstream as in figure 40②.

(3) By interpolation between critical elevations determine where 10-foot contours round the ridges and indicate by lightly drawn U's. Since hills are normally rounded at top and slope off gradually at the bottom with the steepest rise on the slope of the hill (fig. 38), contours will have slightly closer spacing on the rise than at the crest or bottom.

(4) By building up one ground form at a time, connect the V's and U's with smooth contours as shown in figure 40③. Each spur between two streams in the illustration should be drawn in separately.

(5) Every fifth contour (starting from 0) should be made heavier than the rest and should have the elevation written on it.

c. The contours should be sketched while in the field. However, if enemy action or other cause makes this impossible, contours may be interpolated in the office, preferably with the aid of aerial photographs and a stereoscope, provided that critical points have been adequately determined.

■ 48. DETERMINATION OF ELEVATION.—*a.* In the discussion in paragraph 45, approximate elevations of specific points on the map were determined roughly by inspection. Where more accurate elevations are desired, some means of interpolation between contours becomes necessary. In the following procedure the refinement is for theoretical purposes only. Any interpolation from contours is an approximation upon which undue refinement may be misleading.

b. Refer to the margin of the map. To determine the elevation of any specific point, proceed as follows (fig. 41):

(1) If the point falls on a heavy contour, it is only necessary to follow that contour until the elevation appears and read it. For example, the elevation of the point *B* in the figure is read directly as 1,300 feet.

(2) If the point falls on a light contour, the elevation is found by reference to the adjacent heavy numbered contour

lines and interpolating. For example, the elevation of the point *A* is 1,260 feet.

(3) When the point lies between two contours as at *C* in figure 41—

(*a*) Find the elevation of the nearest contour line.

(*b*) Measure the shortest distance between the two adjacent contours along a line passing through the point *C*.

(*c*) Measure the distance along this line from the point in question to the nearest contour.

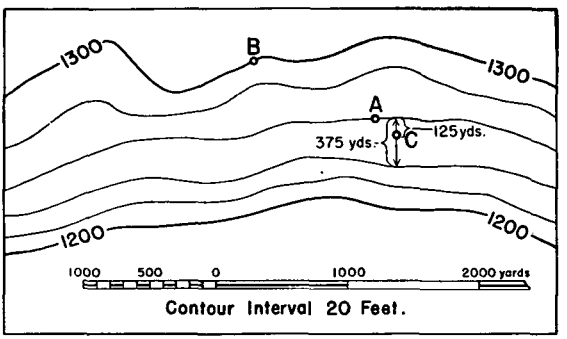


FIGURE 41.—Determination of elevation on contoured map.

(*d*) Solve the following equation:

$$\frac{\text{Distance from point to nearest contour}}{\text{Distance between contours}} \times \text{contour interval} = \text{difference in elevation between point in question and the nearest contour.}$$

Since the distance between adjacent contours at this place is 375 yards and since *C* is 125 yards from the nearest contour (the 1,260 contour), entering the equation given above,

$$\frac{125}{375} \times 20 \text{ feet} = 6\tfrac{2}{3} \text{ feet.}$$

Taking the nearest whole number of feet (7), the elevation at point *C* is 7 feet less than the elevation of the nearest contour, or 1,260—7=1,253 feet. If the nearest contour is of lower elevation than the point in question, the difference in elevation must of course be added.

(4) When a point, the elevation of which is required, lies within a closed contour forming the top of a hill or the bottom of a depression, only an approximation of its actual elevation is possible.

SECTION VI

SLOPE, PROFILE, AND VISIBILITY

■ 49. SLOPE.—The inclination of the land surface relative to a horizontal plane is the slope, and slope is a function of two factors—horizontal distance and vertical distance. Two points are therefore necessary to determine these factors. The vertical distance is the difference in elevation of the points and on a contoured map may be interpolated from the contours. The horizontal distance is scaled from the face of the map. Along a straight line it is the scaled length of the straight line. Along a meandering stream, irregular road, or broken line, it is the scaled length of the meander line or other irregular distance under consideration. Both horizontal and vertical distance must be expressed by the same units, preferably feet. Slope may be computed or measured and expressed in terms of percent, mils, degrees, or as gradient. The slope of roads, railroads, embankments, and cuts is referred to as grade. While the most commonly used method of expressing slope is by percent, the advanced map reader should be familiar with other methods.

■ 50. SLOPE IN PERCENT.—Percent is the most convenient and commonly used method of expressing slope. A slope of 1 percent is a slope which rises vertically a distance of one unit in a horizontal distance of 100 units or one which has this rate of rise (fig. 43). A 2-percent slope rises two units, a 3-percent slope rises three units, and so on, in a horizontal distance of 100 units. The value in percent of any slope is the number of units which it rises vertically in a horizontal distance of 100 units. Thus a rise of 26.8 feet in a horizontal distance of 100 feet is a slope of 26.8 percent (fig. 42).

■ 51. SLOPE IN MILS.—The mil is a unit of angular measurement. A true mil is an angle which subtends an arc of unity at a radius of 1,000 units (fig. 43). A 2-mil slope subtends an arc of two units, a 3-mil slope subtends an arc of three units, and so on, at a 1,000-unit radius. The value of slope in mils

is therefore a function of the angle of slope. The vertical rise of a mil slope is not exactly equal to the subtended arc, the vertical rise of a slope of 2 mils is not exactly twice the vertical rise of a slope of 1 mil, and the variation increases with the angle of slope. However, for slopes up to 350 mils,

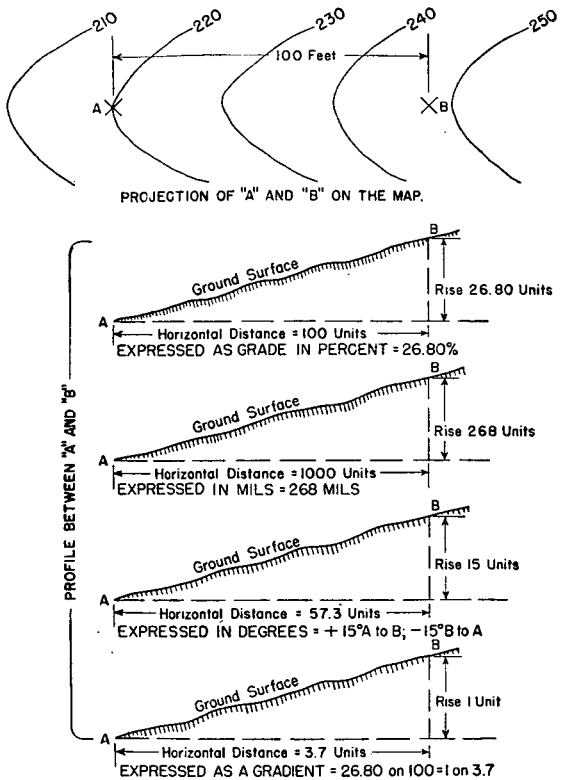


FIGURE 42.—Determination and expression of slope between two points *A* and *B* on map.

the variations are inappreciable and may be disregarded for average purposes. Thus a slope which rises 268 units in a horizontal distance of 1,000 units is a slope of 268 mils (fig. 42). Slopes may be measured with instruments graduated

in the arbitrary mil which is $\frac{1}{6400}$ of a circle. For ordinary slopes the results would not differ appreciably from the value in true mils, of which the circle contains approximately 6,283.

■ 52. SLOPE IN DEGREES.—Many instruments for measuring slope are graduated in degrees. The degree is a unit of angular measurement and is $\frac{1}{360}$ of the circle. A degree is an angle which subtends an arc of unity at a radius of approximately 57.3 units (fig. 43). A 2° slope subtends an arc of two units, a 3° slope subtends an arc of three units, and so on, at a 57.3-unit radius. The value of slope expressed in degrees is therefore a function of the angle of slope (fig. 42). The vertical rise of a degree slope is not exactly equal to the subtended arc, a slope of 2° is not exactly twice the vertical rise of a 1° slope, and the variation increases with the angle of slope. However, for slopes up to 20° the variations are negligible and may be disregarded.

■ 53. GRADIENT.—The gradient is the unit usually used in the measurement of steep slopes. It is the ratio of vertical to horizontal or of horizontal to vertical distance (fig. 42). The manner of expressing this ratio has not been standardized. Two methods are in common use as follows: A gradient of 1 on 3.7 and a gradient of 3.7 to 1.

■ 54. SLOPE BETWEEN TWO POINTS ON MAP.—*a.* Subtract the elevation of the initial point from the elevation of second point to determine the difference in elevation or vertical rise.

b. Scale from the map the horizontal distance between the two points along the line whose slope is to be determined and express in the same units of measurement, preferably feet.

c. Compute the value of slope from the appropriate one of the following formulas:

(1) Percent $= \frac{\text{difference in elevation} \times 100}{\text{horizontal distance}}$

(2) Mils $= \frac{\text{difference in elevation} \times 1{,}000}{\text{horizontal distance}}$

(3) Degrees $= \frac{\text{difference in elevation} \times 57.3}{\text{horizontal distance}}$

(4) Gradient $= \frac{\text{difference in elevation}}{\text{horizontal distance}}$ expressed as a fraction reduced to simplest terms.

■ 55. CONVERSION OF SLOPE EXPRESSION UNITS.—*a*. Unit degree, percent, and mil slopes are illustrated in figure 43. If arc and tangent are assumed to be equal, it is apparent that the relation may be expressed as follows:

$$\text{Degree: percent: mil: } \frac{1}{57.3} : \frac{1}{100} : \frac{1}{1{,}000}$$

or,

$$57.3° = 100 \text{ percent} = 1{,}000 \text{ mils}$$

Hence,

(1) $1° = 100/57.3 = 1.75$ percent, or
$1{,}000/57.3 = 17.5$ mils.

(2) 1 percent $= 57.3/100 = 0.57°$, or
$1{,}000/100 = 10$ mils.

(3) 1 mil $= 57.3/1{,}000 = 0.057°$, or
$100/1{,}000 = 0.1$ percent.

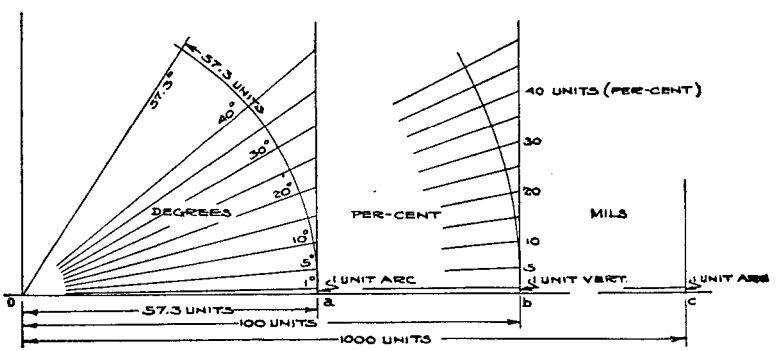


FIGURE 43.—Relation of units of slope.

b. The relations thus expressed, while suitable for conversion of angles up to 20°, are decreasingly accurate as the angle of slope increases, due to the fact that the assumption of equality of arc and tangent becomes increasingly erroneous as the angle increases. The amount of error inherent in this method of conversion for various slope angles is shown as follows:

Angle of slope		Actual percent of slope	Percent of slope computed by conversion factor
Degrees	Mils		
1	17.5	1.75	1.75
5	87.3	8.75	8.73
10	174.5	17.63	17.45
20	349	36.40	34.90
30	523.5	57.74	52.35
45	785	100.00	78.53
57.3	1,000	155.77	100.00

■ 56. AVERAGE SLOPES.—In determining slopes by the methods and formulas described, it should be remembered that the result expresses the slope of an inclined plane surface, whereas the actual surface of the intervening ground may vary quite irregularly up and down. It is therefore customary to refer to slopes thus determined between points over broken terrain or irregular surfaces as "average slopes."

■ 57. PROFILE.—The most satisfactory way of showing the slope of the ground is by making a profile. A profile is a cross section of a specific slope or hill cut by the intersection of the earth's surface by an imaginary vertical plane (fig. 38).

a. Profile from contoured map.—Figure 44① represents a portion of a contoured map. It is desired to construct the profile of the ground represented by the map between the points *A* and *B*. Proceed as follows:

(1) Connect the points *A* and *B* by a straight line and assume that a vertical plane is passed through the line *AB*.

(2) Use a piece of ruled paper which has parallel lines equally spaced; cut or fold the paper along one of these lines.

(3) Refer to the map and determine the highest and lowest elevation along the line *AB*; number the lines on the paper to correspond with the elevations on the map beginning with the highest elevation near the top edge of the paper (fig. 44②).

(4) Place the top edge of the paper along the line *AB* and, where the edge intersects each contour, drop a perpendicular to the horizontal line on the paper corresponding to the elevation of the contour being considered. Proceed in the same

manner with each contour. The profile is then formed by drawing a line between the points of intersection of the perpendiculars with the horizontal lines on the paper. Or, use another piece of paper having a straight edge. Place the straightedge along the line *AB* and make tick marks along the edge of the paper where it intersects each contour. Draw a vertical control line on the first piece of paper which has horizontal ruled lines. Move the paper with tick marks up

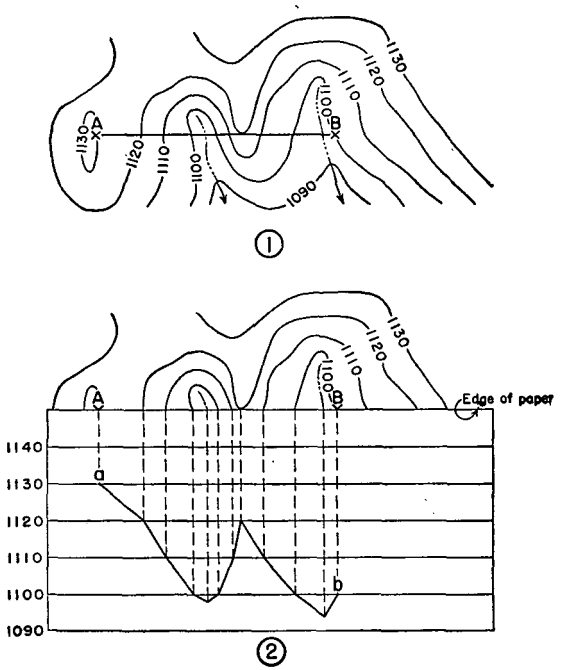


FIGURE 44.—Construction of profile.

and down the vertical control line, keeping the same tick mark on the control line. Place a point on each horizontal line where the tick mark with corresponding elevation intersects it. The profile is then formed by drawing a line between these points. The profile is then complete except between adjacent contours of the same elevation which require the determination of intermediate elevations.

(5) When the line crosses spurs or valleys, examine the map on both sides of the line, estimate the length of the crestline connecting the two adjacent contours and estimate the ratio of this line which lies on each side of the profile line. Compute the desired elevation, using the ratio of these two lengths to the contour interval. Where the line crosses a contour "circle" which forms a knob or depression, an elevation is sometimes found in this area which is of assistance in completing the profile.

(6) If a profile is desired of an irregular line on the map, such as a road or trench, divide the line into a series of sections approximately straight and plot as directed above, turning the paper at each angle to make a continuous profile.

b. Exaggeration.—For the purpose of clarity, profiles are usually exaggerated vertically in comparison with the horizontal, which for convenience is ordinarily the same as that of the map used (fig. 44②). Any selected horizontal or vertical scale may be used depending upon the material on hand and the information desired. In figure 44②, the horizontal profile lines represent 10-foot intervals; they could represent 5-foot intervals, thus further exaggerating the profile. The use of cross section paper will be found most convenient for constructing profiles, as the vertical lines aid in dropping perpendiculars to the horizontal lines.

■ 58. VISIBILITY.—A contoured map can be used to determine whether or not a point, a route of travel, or an area is visible from a given point. Because of inaccuracies inherent to map construction, it is unsafe to conclude that one given point can be seen from another given point if a profile, made from a map and between the points, shows the objective point to be only barely visible. One of the important uses made of maps by a military commander is to conceal lines of march or troop positions from an enemy's observation station. He and his staff officers are thus solving problems of visibility; by inspection of the shape, location, and elevation of map contours, they are determining approximately whether or not certain points can be seen from other points shown on the map. To be a successful troop leader, every officer and noncommissioned officer should be able to solve map visibility problems with reasonable accuracy and rapidity. Frequently the desired information can be obtained by inspection, but when

this is not possible some graphical or mathematical method should be used. The most common are the profile, similar triangle, and graphical methods. The profile method is more laborious than the others, but it is the best because of the completeness and clarity of its results, especially in determining visible areas. The similar triangle method can be used to abbreviate the profile method in many cases, especially in determining the visibility of points, short lines, and small

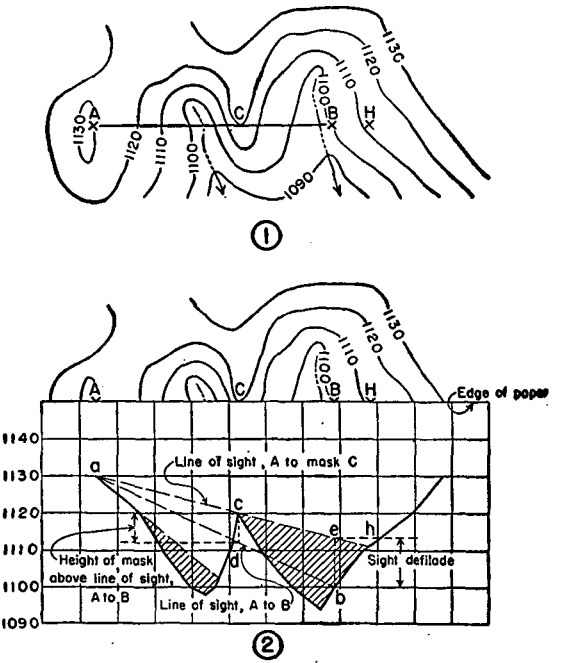


FIGURE 45.—Determination of visibility by profile method.

areas. The graphical method is convenient for checking up visibility along a line without drawing a profile. The extent to which visibility may be determined from a map depends upon the contour interval. The unrepresented variations in relief are of minor character if the contour interval is small. If the contour interval is large, unrepresented ground features may have an important influence.

a. Inspection method.—The following rules may be helpfully applied in determining by inspection the intervisibility of two points shown on a map:

(1) The points, if on opposite sides of a valley and located well above the intervening ground, are intervisible.

(2) If between two points there is a feature represented higher than both, they are not intervisible.

(3) If between the two points a feature is represented which is higher than one of the points, the points may or may not be intervisible.

(4) If the slope of the ground between the two points is convex, they are not intervisible.

(5) If the slope of the ground between the two points is concave, they are probably intervisible.

(6) When the ground between the two points is level, their intervisibility depends upon the presence of vegetation and works of man.

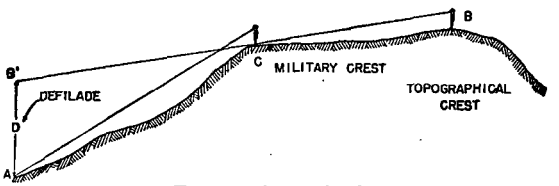


FIGURE 46.—Defilade.

b. Profile method.—(1) Figure 45① represents a portion of a contoured map. It is desired to determine whether or not *B* is visible from *A*. By use of cross section paper, construct a profile along the line *AB* as described in paragraph 57 (fig. 45②). Draw a line *ac* representing the line of sight from *A* tangent to the crest at *C*. This line strikes the ground at *h*. Therefore that portion of the ground between *C* and *H*, including *B*, is not visible from *A*.

(2) It may be noted that in the above example points *A* and *B* were both selected at ground level. Had it been desired to determine whether a man at *A*, eyes 5 feet above the ground, could see a truck 8 feet high at *B*, it would have been necessary to plot *a* in the profile (fig. 45②) with an elevation of 1,135 feet and *b* with an elevation of 1,108 feet. The result would be similar to that illustrated in figure 46. However the map reader will seldom be concerned with

the eye level of a man in a standing position. In combat the available map will probably be uncontoured or of such a scale that 5 feet would make little difference. Also the observer near combat operations will probably observe from as near ground level as possible.

c. Defilade.—In figure 46, *B* represents the topographical crest, that is, the highest crest of a hill; and *C* represents the military crest, that is, the highest crest from which the entire lower part of the hill can be observed. If an observer at *B* is unable to see an object at *A*, due to an intervening hill, spur, wood, or other terrain feature, the object at *A* is said to be "sight defiladed." The intervening defilading feature is called the "mask." In figure 46, the crest at *C* interferes with the view of the foreground from the top of the hill; thus the military crest forms a mask for the topographical crest. The amount which the foreground at *A* is defiladed is equal to the vertical distance *AB'* from *A* to the prolongation of the line "observer-mask." Thus in figure 45, the distance *be*, which scales 13 feet, represents the defilade at *B* caused by the mask *C* when viewed from *A*. The term "height of mask" means the height of a mask above the line of sight between two objects at that point. In figure 45, *cd*, which scales 8 feet, represents the height of mask. Defilade problems like visibility problems may also be solved by a number of graphical and analytical methods.

d. Hasty profile.—The elementary example of defilade above may be mentally expanded to cover many cases of visibility. In a war of movement and aerial observation, terrestrial or captive balloon observation, the consequent visibility problems tend to decrease in importance. The advanced map reader may make some type of hasty profile based on the method employed in figure 47 showing the observer at *A*.

e. Defiladed areas.—From any point as an origin, a line on a map can be extended in any given direction. A profile or partial profile of the terrain passed over by this line can be drawn. Such a profile makes it possible for us to ascertain just what portions of the terrain over which the line passes are visible and just what portions are not visible from the point from which our line was extended. Carrying this factor further and by making a number of profiles, each corresponding to one of a number of lines radiating from a given point, we are able to calculate just what portions (areas) of the

terrain are and are not visible from any given point. Suppose *X* (fig. 48①) represents the plotted location on a contoured map of an observation station. It is desired to determine the areas to the east of *X* that can be observed and the areas that are defiladed. To solve this problem, first draw from *X* a number of radiating lines such as *XY*, *XY*^{1}, *XY*^{2}, and *XY*^{5}, so that the lines cover or include as much of the area in front of *X* as is desired. Afterward, construct a profile corresponding to each of these lines. Three such profiles, *XY*, *XY*^{2}, and *XY*^{5}, are shown in figure 48②. Next, determine on the

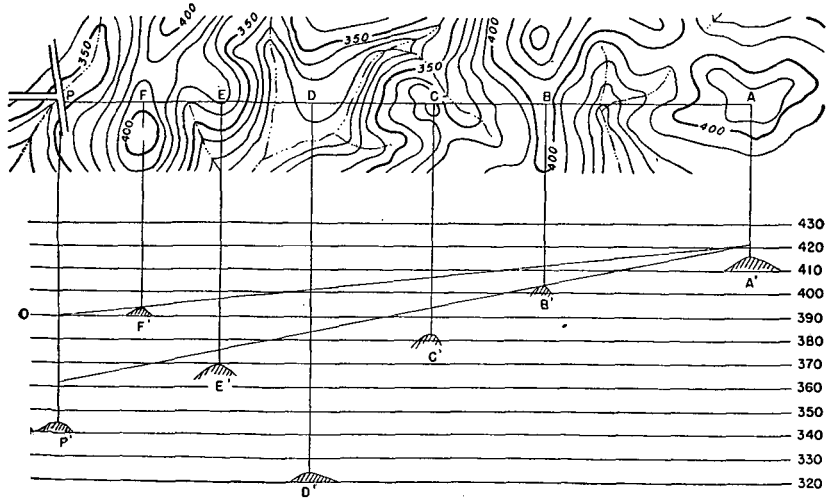


FIGURE 47.—Determination of visibility by hasty profile method.

profiles the parts of each that are defiladed. This may be done by simply drawing lines from *X* to the various crests indicated on the profiles; as in figure 48② *Y*, we see, by prolonging lines from *X* which just touch the tops of the various crests in front of *X*, that those parts of the line *XY* between *a* and *b* and between *e* and *f* are defiladed; similarly, in figure 48② *Y*^{2}, that $a^2 b^2$, $c^2 d^2$, and $e^2 f^2$ are defiladed; also in figure 48② *Y*^{5}, that $a^5 b^5$, $c^5 d^5$, and $e^5 f^5$ are defiladed. If, after solving a number of these profiles, we now plot on

our map the exact locations of the limiting points of the defiladed positions of each line and then afterward join these points as in figure 48①, we can connect up areas such as those shown by the shaded lines in figure 48①. It is then known that all shaded areas, such as those shown in this figure, are not visible from the observation point at *X*.

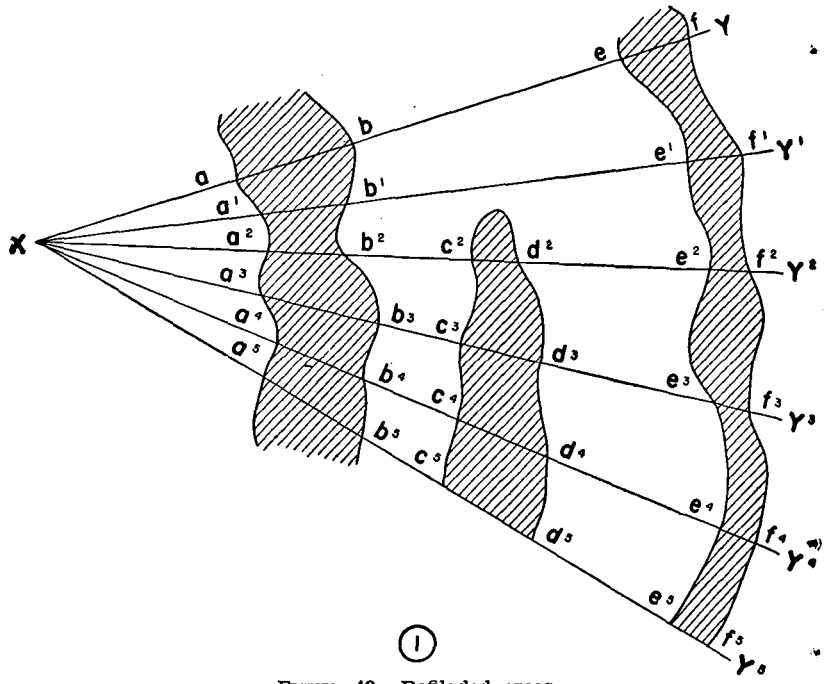


FIGURE 48.—Defiladed areas.

f. Foliage.—In solving problems of visibility, there often appears an intervening woods that may or may not interfere with the visibility. Any group of trees that may possibly defilade one object from another must be carefully considered.

■ 59. VISIBILITY DIAGRAMS (fig. 49).—Visibility diagrams indicate which portions of the ground are visible and which are invisible to an observer at some definite observation post. They

are also a practical aid in identifiying objects from an observation post when a good map is available. The determination by means of a map of the visibility of areas from a given point has been explained in paragraph 58, but personal reconnaissance is also necessary, because trees, hedges, and other objects not shown on the map may considerably affect the view. In constructing a visibility diagram, one should identify on the map the observation post and select a reference object. A line should be drawn joining the two and marked 0°. Lines are then set off at about 10° intervals on both sides of the

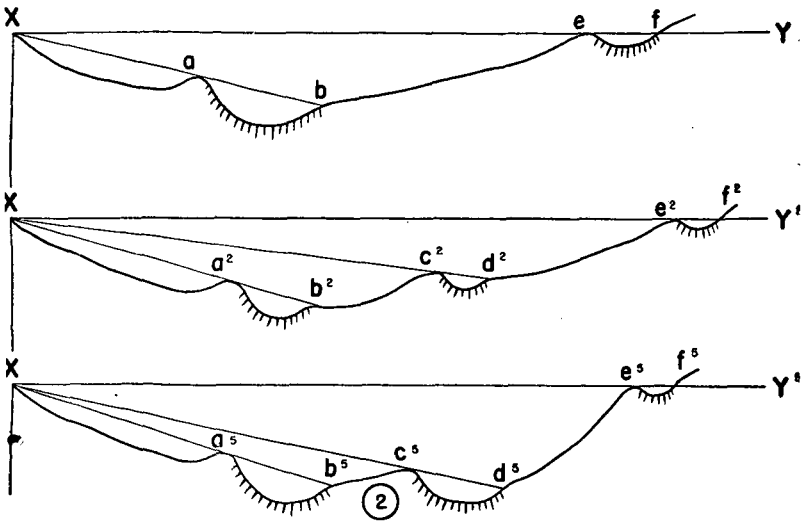


FIGURE 48.—Defiladed areas—Continued.

zero line radiating from the observation post. These serve as lines of sight to be investigated. Next study the features, mark on the map those which interfere with the view, and then determine those areas which are invisible from the observer's position.

■ 60. CURVATURE AND REFRACTION.—In computing intervisibility of points on a map by the methods described herein, the ground is assumed to be flat like the map and the light rays undeflected. Errors resulting from these assumptions are

negligible in average problems on local terrain. However, the earth is a spheroid, and distant light rays are bent from their path by passage through the atmosphere near the earth. The

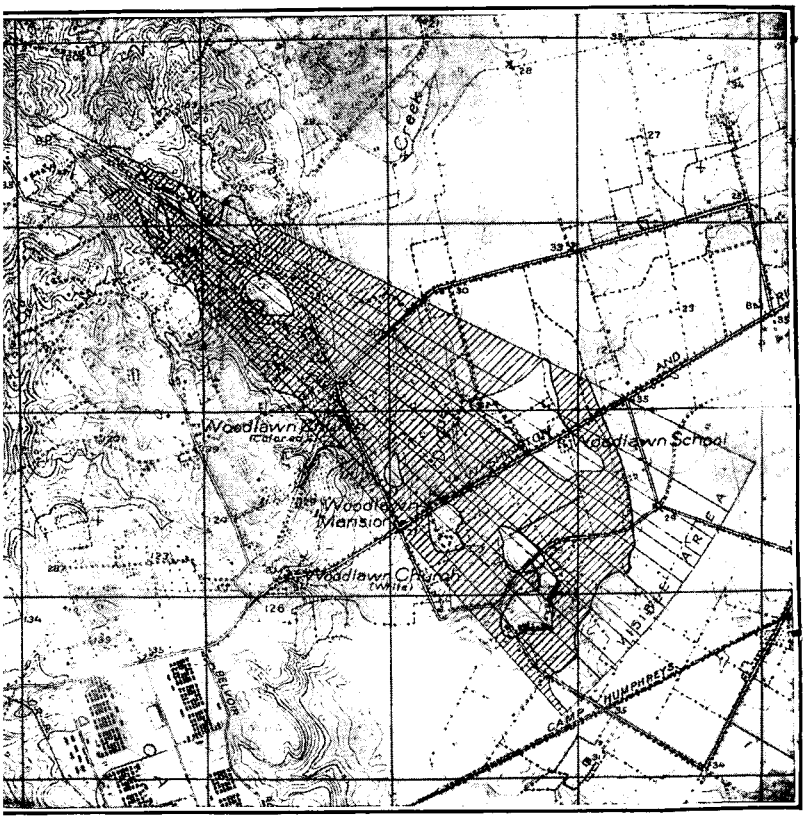


FIGURE 49.—Visibility diagram.

combined effects of curvature and refraction become appreciable at distances greater than 1 or 2 miles and should be duly considered when accurate results are desired.

SECTION VII

AERIAL PHOTOGRAPHS

■ **61. AERIAL PHOTOGRAPHS.**—*a.* An aerial photograph is a perspective picture, with either a vertical or an oblique viewpoint, taken from any kind of an aircraft. Except for color values and a certain capacity of the eyes to perceive differences in relief, the aerial photograph conveys the same impression in image as received by the human eye from the same viewpoint. Since the average person is unaccustomed to the vertical viewpoint, the images of familiar objects on photographs may at first appear strange and unassociated with the objects represented. The difficulties presented in interpretation of vertical aerial photographs appear to be no greater than those ordinarily encountered in learning to read conventional military maps and are overcome in the same way.

b. The vertical aerial photograph is a valuable instrument for conveying topographic information for the following reasons:

(1) It possesses in pictorial effect a wealth of detail which no map can equal.

(2) It possesses accuracy of form.

(3) With freedom of flight, an aerial photograph may be prepared in a short time.

(4) It may be reproduced in quantity by lithography.

(5) It may be made of an area otherwise inaccessible because of either physical or military reasons.

c. The vertical photograph is inferior to a map in respect to the following features:

(1) Important military features which are emphasized on a map are sometimes obscured or hidden by the other detail.

(2) Neither absolute position nor absolute elevation can be obtained.

(3) Relative relief is not readily apparent.

(4) Displacements of position caused by relief and camera tilt usually do not permit the accurate determination of either distance or direction.

(5) Because of a lack of contrast in tone, it is difficult to read in poor light.

(6) Marginal data furnished on maps are generally lacking.

d. A large portion of the area of the United States has never been mapped. Of the area mapped, a large percentage is considered inadequately mapped because of having been mapped more than 40 years ago or to scales unsuitable for military use. The preparation of military maps under service conditions involves factors of both time and space. In consequence, it may require a period of some length before a satisfactory map can be prepared covering territory which has not been adequately mapped. On the other hand, a film may be exposed in an aerial camera over either enemy or friendly territory, the negative developed, and the photograph printed in the course of a few hours. In consequence, the value of the aerial photograph as a means for supplying topographic information before maps can be made available, or before existing maps can be revised, is readily apparent. However, because of its limitations, the aerial photograph does not constitute an ideal map, and its best use is either as a map substitute or as a map supplement. The ideal situation would include the availability of the most accurate topographic map possible, supplemented by the most recent aerial photographs.

■ 62. TYPES OF AERIAL PHOTOGRAPHS.—*a.* Aerial photographs used for military purposes are made with the Air Corps cameras listed in the following table:

TABLE IV.—*Characteristics of photographs made with U. S. Army Air Corps cameras*

Camera	Focal length in inches	Photograph size in inches	Width covered by single photograph in miles at scales of—			Flying altitudes in feet for scales of—			Flight line spacing in miles to give an overlap equivalent to 50-percent overlap on 7- x 9-inch photograph			Purpose
			1:10,000	1:20,000	1:40,000	1:10,000	1:20,000	1:40,000	1:10,000	1:20,000	1:40,000	
K-3B	8.25	7 x 9 or 9 x 9	1.42	2.84	5.68	6,875	13,750	[1] 27,500	0.71	1.42	2.84	A fully automatic aircraft camera for reconnaissance, photographic mapping, and spotting missions.
K-3B	12	7 x 9 or 9 x 9	1.42	2.84	5.68	10,000	20,000	[1] 40,000	.71	1.42	2.84	Do.
K-7C	24	9 x 18	2.84	5.68	11.36	20,000	[1] 40,000	[1] 80,000	1.42	2.84	5.68	An aircraft camera for high altitude, large-scale, spotting and reconnaissance mapping.
K-12	13.5	8 x 10	1.58	3.6	6.32	11,250	22,500	[1] 45,000	0.79	1.58	3.16	An aircraft camera, single lens, with between-lens shutter to take aerial photographs at night.

[1] Impractical flying altitudes due to airplane limits or bumpy air.

TABLE IV.—*Characteristics of photographs made with U. S. Army Air Corps cameras*—Continued

Camera	Focal length in inches	Photograph size in inches	Width covered by single photograph in miles at scales of—			Flying altitudes in feet for scales of—			Flight line spacing in miles to give an overlap equivalent to 50-percent overlap on 7-x 9-inch photograph			Purpose
			1:10,000	1:20,000	1:40,000	1:10,000	1:20,000	1:40,000	1:10,000	1:20,000	1:40,000	
T-3A (five lens).	5.9	Center, 5.4 x 5.4; composite, 32 x 32, approximately.	5.1	10.2	20.4	4,920	9,840	19,680	4.05	8.11	16.22	An aircraft five-lens camera covering a total included angle of 140° for tactical reconnaissance, mapping survey, and rough mosaics.
T-5	6	9 x 9	1.42	2.84	5.68	5,000	10,000	20,000	0.71	1.42	2.84	An aircraft camera designed for precise topographic surveying and to be used with photogrammetric equipment.

b. The photographs made with the cameras listed in *a* above are classified as follows:

(1) *Plain verticals* (fig 50).—(*a*) The term "plain vertical photograph" is applied to all those obtained by pointing a single-lens camera at time of exposure so that the optical axis is as nearly vertical as possible. Plain verticals are made with Air Corps K-type cameras. Since the camera film is practically horizontal, features on the ground are registered on a vertical photograph in perspective with little or no distortion in

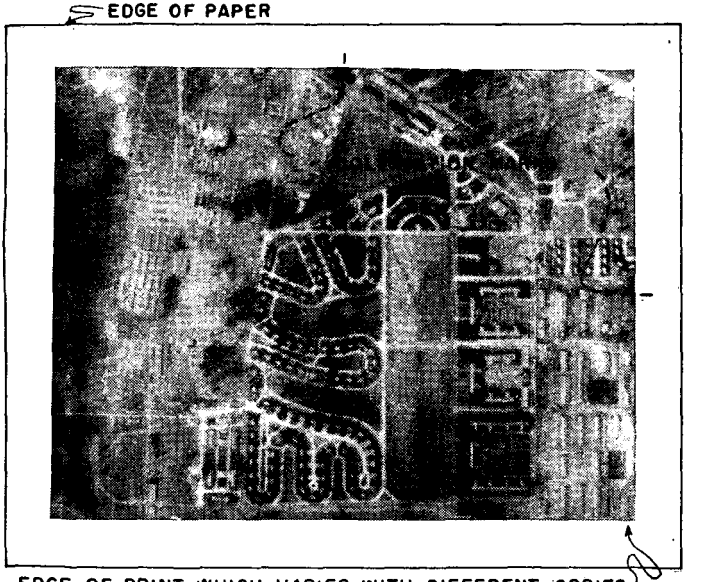


FIGURE 50.—Plain vertical made with Air Corps K-type camera.

their relative shapes and sizes. This is the most useful type of photograph for general military purposes and is the one commonly referred to as an aerial photograph.

(*b*) The neat lines as shown on the vertical in figure 50 are not always the same on photographs made from the same negative. In order to facilitate accurate location of points on vertical photographs, ticks or collimation marks are registered in the center of the four sides of the negative at the time

of exposure by means of a templet in the camera. The method of measuring from these collimation marks is given in paragraph 104*b*.

(2) *Obliques.*—Oblique aerial photographs are obtained by intentionally tilting the optical axis of the camera from the vertical. The oblique photograph is a rectangle, while the area of ground photographed is a trapezoid (fig. 51).
In making obliques the optical axis of the camera is usually held inclined about 30° to the horizontal (fig. 51) at a comparatively low altitude and such obliques are termed "low obliques." Those exposed so as to include the image of the

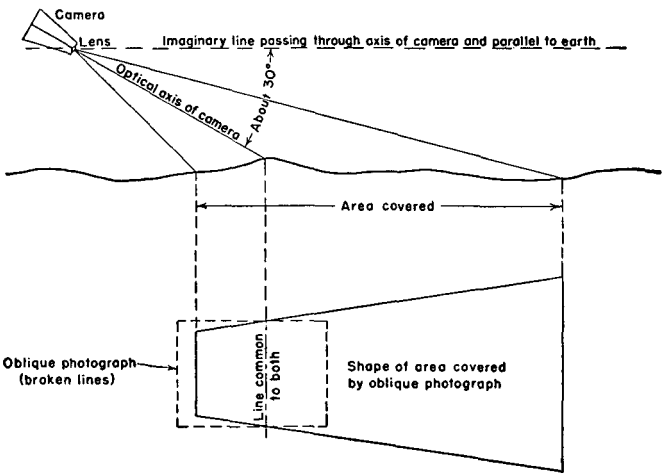


FIGURE 51.—Relative shape of area covered by oblique photograph compared to photograph itself.

horizon are termed "high obliques." Obliques are useful in emphasizing ground forms, in studying vertical dimensions of terrain features or works of man, or in interpreting detail not easily distinguished on vertical photographs when the clarity of perspective is desirable. Obliques cannot be accurately scaled. An oblique may be regarded as a highly improved and economical substitute for a panoramic sketch.

(3) *Composites.*—A composite photograph is one made by joining several photographs transformed to a common plane which have been taken at a single-camera position. Vertical

composites are made with the Air Corps T–3A type multiple-lens camera. This camera has one central chamber, the optical axis of which is held in a vertical position at exposure, and four peripheral chambers, the lenses of which

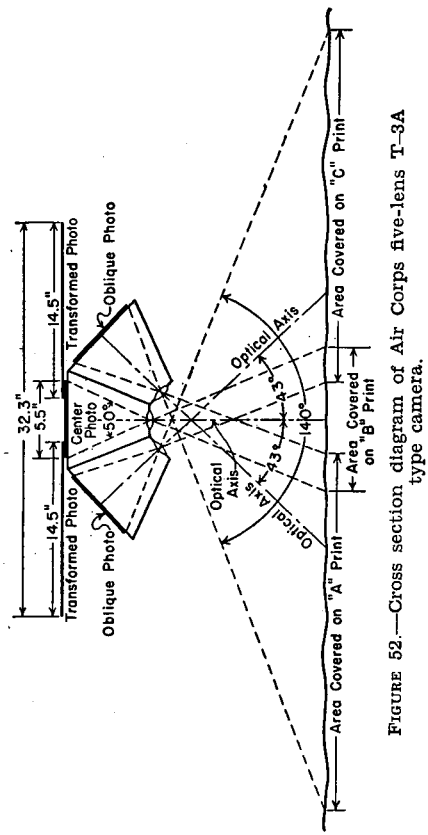


FIGURE 52.—Cross section diagram of Air Corps five-lens T–3A type camera.

are inclined at an angle of 43° with the central lens (fig. 52). The camera has a focal length of 150 millimeters (approximately 6 inches). The result of a single exposure with this camera is one plain vertical photograph which trims to 5.4 by 5.4 inches and four obliques (called wing photographs)

which are transformed to the plane of the center photograph, joined to it, and mounted to produce a single photograph in the shape of a Maltese cross approximately 32 by 32 inches (fig. 53). The transformation of the wing photographs to the plane of the center photograph is effected by means of a transforming printer which projects the wing negatives

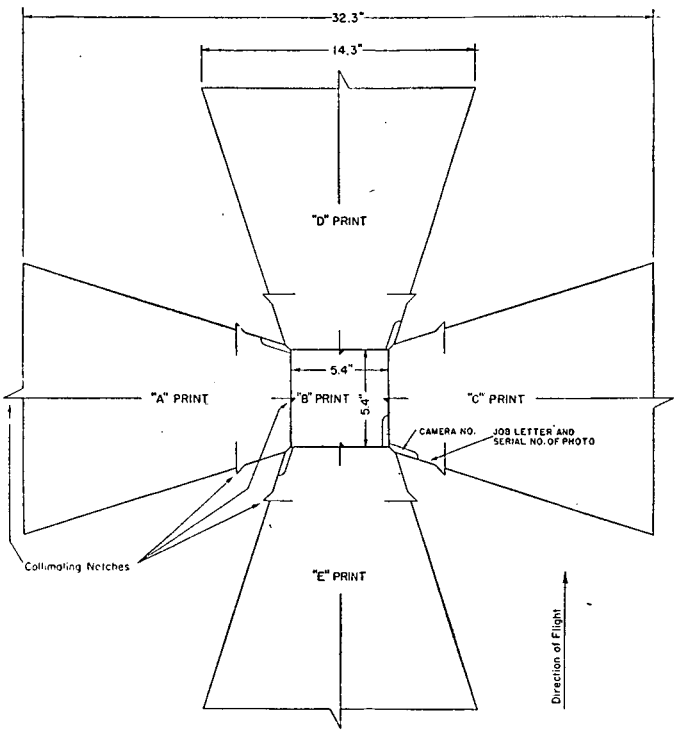


FIGURE 53.—Diagram of composite photograph made with Air Corps five-lens T-3A type camera.

to print paper which is inclined at an angle corresponding to the lens inclination in the T-3A camera (fig. 91). The term "contact prints" applies to photographs made from negatives before their transformation. Thus the contact prints of all five chambers of the T-3A camera measure 5.5

by 5.5 inches. Due to the wide angular scope of 140° and the short focal length of the T–3A camera, a single photograph from a relatively low altitude will cover an area of great width. For example, a single picture at 18,000 feet altitude gives a picture approximately 18 by 18 miles in dimension. It is this feature which makes this camera particularly adaptable to military mapping and to exploiting the detail of a large expanse of terrain from a single photograph. It has also been found possible to make a nine-lens composite (fig. 93) by taking two pictures with T–3A cameras with the vertical axis of the pictures skewed at 45° in respect to one another, thus using the wing photographs of one composite to fill the voids of the other. A photograph of a large area can be produced much more quickly by this method than by the construction of a mosaic.

■ 63. PIN POINTS.—Two or more stereoscopic photographs of an isolated object or spot constitute a pin point. Airdromes, supply depots, dumps, road crossings, bridges, or other bottlenecks on lines of communication requiring detailed study are suitable objects for pin point photographs.

■ 64. STRIPS (fig. 54).—Successive overlapping photographs made from an airplane flying a selected course line or direction constitute a photographic strip. Vertical photographs are usually taken in such strips with a constant overlap of approximately 60 percent between successive pictures forming the strip. A strip made in order to secure information regarding the condition of, or activity along, a more or less extended but narrow section of terrain, such as along a road, a railroad, a stream, an avenue of approach, a zone of action, or a stabilized front line, is called a "reconnaissance strip." When the several photographs of a single strip are joined together or mounted to form a mosaic, the result is a "strip mosaic." Strip mosaics may be either controlled or uncontrolled.

■ 65. MOSAICS.—*a. Uncontrolled mosaic.*—A mosaic is formed by joining several overlapping vertical photographs taken at different camera positions. When several photographs are oriented by matching the detail along their borders, the result is an "uncontrolled mosaic," which gives a good pictorial effect of the ground but will contain serious errors of scale

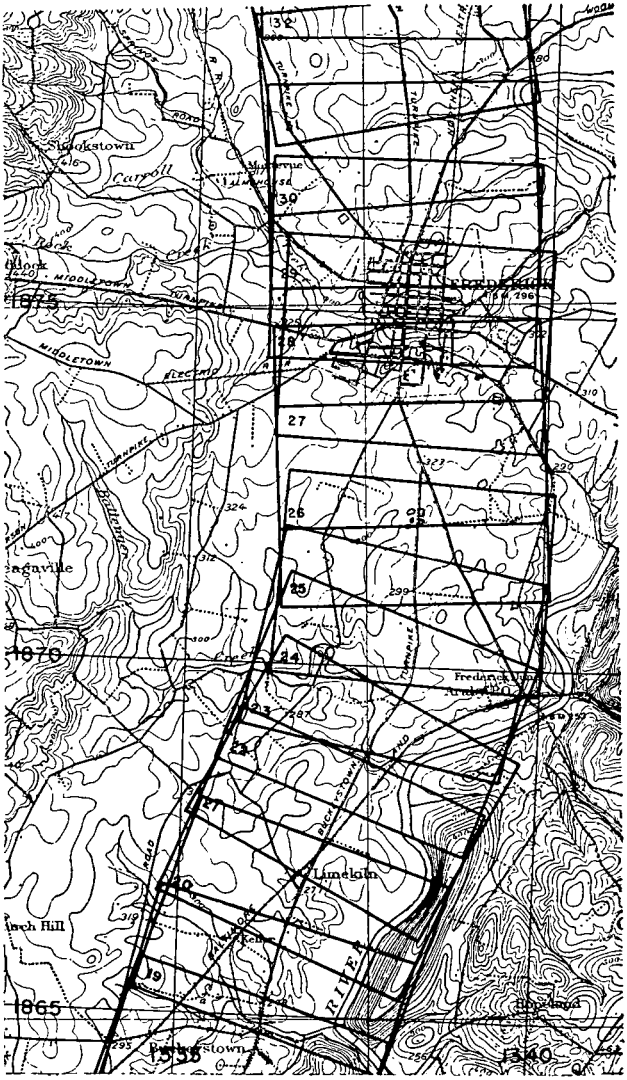


FIGURE 54.—Section of index map showing strip of K-type aerial photographs plotted on map of 1: 62,500 scale.

and azimuth. While care in matching the photographs will assist in approaching accuracy, the only way that scale accuracy can be obtained is by having recognizable control on the ground.

b. Controlled mosaics.—By adjustment of vertical photographs to plotted portions of ground control points and by various other modifications of the photographs as obtained directly from the camera, errors of scale and direction inherent to single photographs and uncontrolled mosaics may be greatly reduced. If the individual prints are prepared by contact printing directly from the aerial camera negatives, they may vary considerably in over-all or average scale due to changes in plane altitude and ground elevation between successive photographs. In the preparation of controlled mosaics from such prints it is customary to determine the average scale of all the photographs by reference to ground control data and to assemble the mosaic on a control plot prepared at that scale. The technique of this operation is described in paragraph 101, TM 5–230. The variation in scale of the individual prints from the average scale of all the prints used, as well as local scale errors caused by camera tilt, will result in mismatching of detail where the prints are joined. The controlled mosaic, therefore, is frequently less pleasing in appearance than the uncontrolled mosaic; however, it is much more reliable for the measurement of distances and direction. If equipment and time are available the individual prints may be reduced or enlarged to the same scale and, in addition, the tilt errors partially or completely removed. These processes are referred to as ratioing and rectifying. If sufficient data as to ground elevation are available, local scale errors caused by variation of ground elevation within the scope of each individual print may be reduced by rephotographing each print in two or more sections. This process is called "pyramiding." Mosaics which are prepared from ratioed, rectified, and pyramided prints approach the accuracy of the best maps in representation of distances and directions. Because of the time involved in these processes as well as the necessity of obtaining extensive ground control data, the highly accurate controlled mosaic will seldom be encountered during initial stages of combat.

■ 66. PRINT PAPER.—Photographs may be printed on either glossy, matte, or semimatte paper of single or double weight. Unfortunately print paper shrinks in the processes of development, sometimes to a most disconcerting extent. Glossy paper gives clearest definition of detail but will receive marks or notations only in ink. Light matte paper shrinks badly and lacks sharpness of detail but will receive either pencil or ink marks. Doubleweight semimatte paper of best quality has low shrinkage, will receive pencil marks, may be used unmounted, and has clearer definition of detail than matte paper of the same weight. Changes in temperature and moisture cause glazed print paper to curl up and become refractory. In general, all prints intended for extensive use should be mounted on manila or similar paper with rubber cement. Photographs used on mapping projects are mounted on heavy cardboard or on thin metal sheets in order to reduce their shrinkage.

■ 67. PICTURE POINTS.—In studying one or more aerial photographs it is sometimes desirable that one be able to identify readily selected points of detail. Points thus chosen are marked on the photographs by small circles about 0.2 inch in diameter. They are known as "picture points." By marking points in this manner adjacent detail is not obscured.

■ 68. OVERLAYS.—Not only is it difficult to mark on the face of a glossy photograph, but marks on the face of any photograph tend to clutter it up, obscure important detail, and diminish its usefulness. Yet it is sometimes desirable that positions of objects be emphasized or that military information such as that representing the disposition of troops, organization of ground, enemy or friendly works, supply and circulation activities, and other information shown graphically on special military maps be recorded by some means without unnecessarily damaging the print. This has been satisfactorily solved by means of overlays of high-transparency paper. A light, tough, almost colorless tracing vellum is most suitable for this work, yet any kind of transparent tracing paper which will take pencil and ink marks will answer the purpose. The tracing should be cut to fit the photograph and then carefully registered to the photograph (fig. 55). This may be done by tracing in the neat line in full or only

at the four corners, by tracing in the border ticks and the center cross, or by any convenient combination of these. The serial number of the photograph should always be traced in. Significant marginal information on the photograph should also appear on the margin of the overlay as far as consistent. The overlay should be fastened to the photograph along one edge by a little mucilage or, better still, by means of two ordinary paper clips. This will enable the overlay to be lifted at one edge for direct examination of detail without disturbing the relation of the overlay to photograph. (All

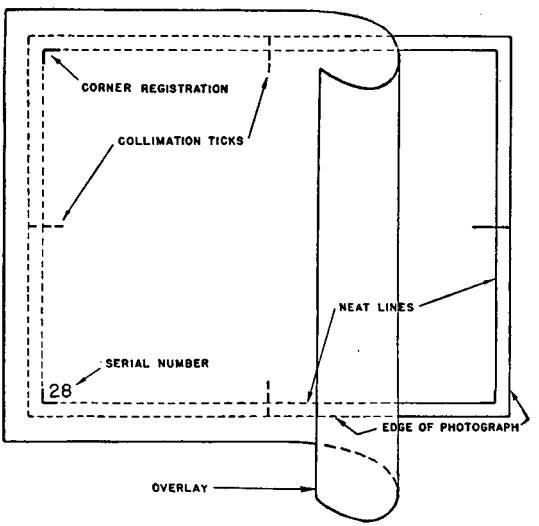


FIGURE 55.—Registered overlay.

photographs destined for extensive use should first be mounted with rubber cement on a sheet of stiff manila or similar paper cut slightly larger than the photograph and the overlay tacked to the mount as described above.)

■ 69. CONVERSION TO LINE MAP.—*a. Methods.*—It is sometimes desirable to convert a photograph to a line map. By doing so, unnecessary detail can be eliminated on the one hand and on the other hand important military features can be emphasized through their representation by conventional map symbols.

This can be done in two ways: either by tracing on a sheet of transparent overlay the topographical detail desired, or by bleaching the photograph. The latter method is seldom used.

b. Tracings.—A tracing of the detail of a good vertical photograph of average terrain in which the features are represented by map symbols in the conventional way and supplemented by useful marginal information, such as the magnetic north point and scale, becomes for practical military purposes an uncontoured map of the area photographed at the scale of the photograph. In this way every detail on the face of a photograph is preserved unblemished and yet the information recorded stands out emphatically. The original tracing may be used as a map or the tracing may be used to reproduce the map in quantity by any of the authorized reproduction processes.

■ 70. To Index and Plot.—On receipt of one or more photographs of an area of which some sort of a map is available, examination and study of the photographs are facilitated by first outlining on the map the area or areas covered by the photograph or photographs as indicated in figure 54. This is best done by determining the scale of the photographs and using the relation to scale of map to construct a templet of tracing paper or other suitable transparent material which represents the dimensions of the photograph to the scale of the map. Thus a templet outlining the ground covered in a photograph having a scope of 7,000 by 9,000 feet on a map having an RF of 1: 20,000 would measure

$$\frac{7{,}000\times 12}{20{,}000} \text{ by } \frac{9{,}000\times 12}{20{,}000} \text{ or } 4.2 \text{ by } 5.4 \text{ inches.}$$

If transparent material is not available, the templet may be made from opaque material by constructing a frame inclosing a cut-out area having the scope of the photograph to the scale of the map. The templet is placed on the map and shifted about until its outline includes the details shown on the photograph. The area covered on the map is then outlined by marking around the templet. The serial number of the photograph is entered in the outline. The process is repeated for any number of photographs in hand. The result is an index sheet of the photographs showing com-

prehensively the relation of the photographs to one another and to the area.

■ 71. CARE OF AERIAL PHOTOGRAPHS.—Unmounted aerial photographs should always be filed flat and kept weighted down when exposed to changes in temperature. Never place them near a radiator, stove, or other heating device, as the photographs will curl up tightly and set in that shape. Never roll up the photographs for any purpose. When in the field, protect them from moisture as much as practicable. A heavy manila envelope is suitable for this purpose and is a convenient container.

■ 72. SOURCES OF ERROR.—Were it possible to photograph an area of perfectly flat terrain from a perfectly level plat-

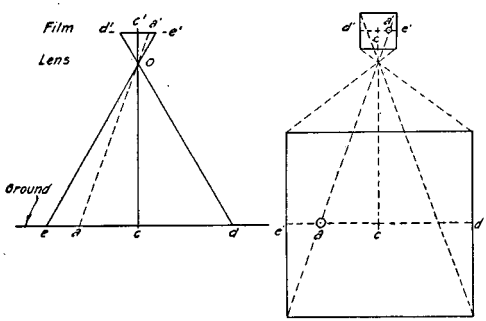
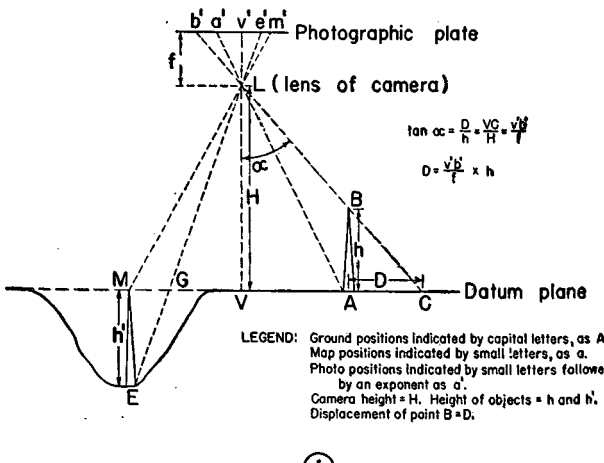


FIGURE 56.—Relation of image on photograph to object on ground under ideal conditions of level ground and camera.

form at a desired elevation, the result would be a perfect map in all planimetric detail, assuming the camera registered a true image. This may be verified by examination of figure 56. Any image *a'* would appear on the negative in the same relation to all other images on the photograph as the object *a* on the ground bears to all other objects on the ground, and similar relation would obtain between the lines *d'e' and de.* The ground is seldom, if ever, perfectly level, and it is impracticable to fly an airplane continuously in any selected horizontal plane. Air currents and variations of air density cause the airplane to tilt about either axis and rise and fall in elevation. Distortions are also caused

by the camera lens, the shutter speed in a rapidly moving airplane, the roughness of the film, the departure of the film from the focal plane (warping of the film), and temperature and moisture changes of the film and the print paper, which may result in errors in the photographic record of the terrain. By careful photography, with good instruments and good materials at elevations of 5,000 feet or higher, all errors of sources other than tilt and relief may be neglected in practical military uses of aerial photographs. At elevations lower than 5,000 feet the aggregate effect of such errors may be very material.



①

FIGURE 57.—Diagram showing displacement of position on aerial photographs caused by relief.

■ 73. EFFECT OF RELIEF.—*a.* In making a map, all topographic detail is in effect projected vertically upon a horizontal plane. This results in such detail being relatively correctly located so as to permit accurate measurements of direction and distance. Reference to figure 56 will indicate that only one point *c* is projected vertically from the earth to the photograph. The remainder of the photograph is a conic rather than a vertical projection. The effect of such a conic projection is illustrated in figure 57①. In this figure, *L* represents a camera lens with

the negative of a plain vertical photograph the focal distance f above it. The line LV is vertical to the earth at point V, therefore the image of V or v' is called the plumb point of

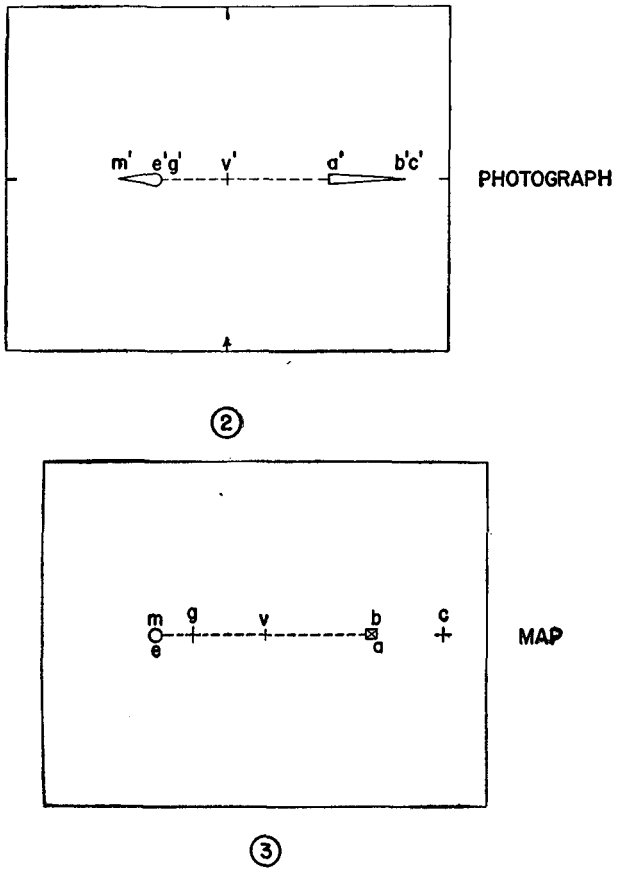


FIGURE 57.—Diagram showing displacement of position on aerial photographs caused by relief—Continued.

the negative. Since in this case the optical axis of the camera is assumed to be held truly vertical, v' is also the principal point of the negative as well as the plumb point. The dis-

tance *LV* is equal to the height of the camera lens above the ground and is designated *H*. If we consider the monument *AB* having its base in the datum plane passing through the point *V* and having a height of *h*, it is apparent from the rays of the camera, indicated by broken lines, that whereas the base of the monument point *A* will appear at *a'* on the negative, the top point *B* will appear at *b'* or in the same position on the negative that the point *C* in the datum plane of *V* would appear. The apparent displacement of *B* is in consequence the distance *D*. The displacement on the negative is the distance *a'b'* and is outward from the plumb point *v'*. In the same figure it may be observed that the image of the point *E*, which is below the datum plane passing through the point *V*, is displaced inward toward *v'* to *e'*. Errors due to relief are present to some extent in all photographs of natural terrain. They cannot be eliminated by rephotographic processes and remain present in all reductions, enlargements, or transformations. In figure 57② is shown in full scale the resulting photograph of the objects shown in figure 57①, and in figure 57③, for the purpose of comparison, their vertical projection as they would be represented upon a map.

b. In figure 57① the triangles *LVC*, *BAC*, and *Lv'b'* are similar right triangles. Consequently the following equations obtain:

$$\tan \alpha = \frac{VC}{H} = \frac{D}{h} = \frac{v'b'}{f} \qquad (1)$$

Therefore

$$D = h \tan \alpha \qquad (2)$$

and

$$D = h\frac{v'b'}{f} \qquad (3)$$

c. From the above discussion it is apparent that—

(1) All displacements due to the elevation of a point above or below the datum plane are radial from the plumb point *v'*.

(2) Since tan α increases as the horizontal distance of the observed point from the point *V* increases, from equation (2), we know that displacements are greater at the outer edges of the photograph.

(3) Similarly since tan α increases as the elevation of the camera above the ground decreases, from equation (2), we know that displacements increase as the camera lens height *H* is decreased. For this reason it is usual when photographs

are to be used as a map to photograph terrain of average relief from heights of not less than 10,000 feet.

(4) Since in figure 57① displacements are radial from the plumb point v', the directions of only those lines which pass through that point can be accurately measured. Errors in

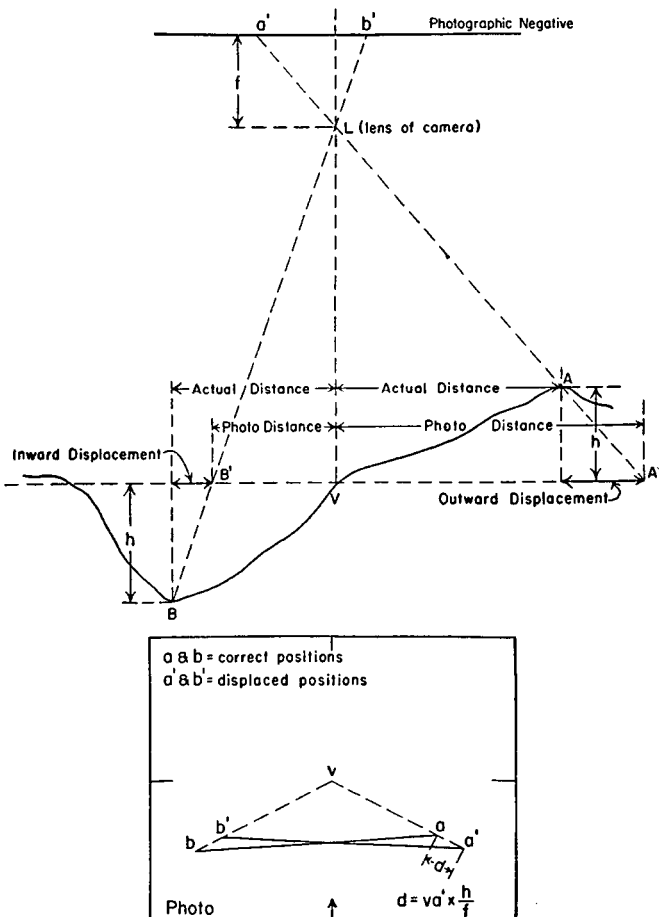


FIGURE 58.—Diagram showing errors in direction caused by relief.

the direction of other lines on the photograph can be caused by relief as illustrated in figure 58. The points *A* and *B* shown in this figure in profile are shown on the photograph (not to scale) displaced to *a'* and *b'*, respectively, because of relief, their true positions being plotted at *a* and *b*, respec-

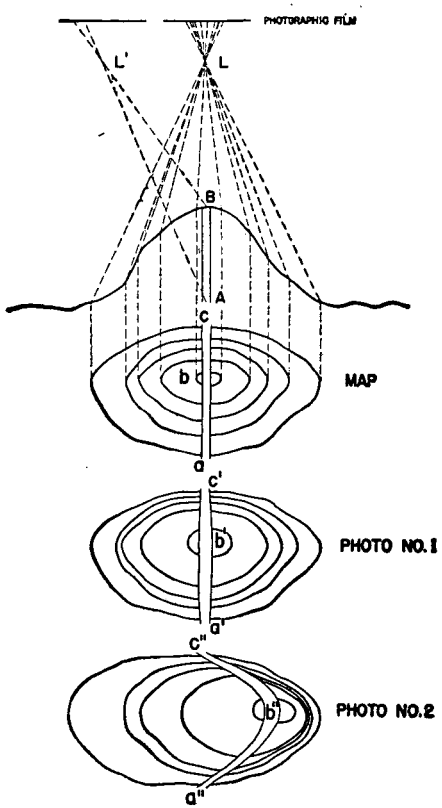


FIGURE 59.—Diagram showing effect of relief upon scale.

tively. The direction line between *A* and *B* (or *ab*) is therefore incorrectly shown on the photograph as *a'b'*.

(5) In figure 57① while *h* equals *h'* and *MV* equals *VA*, *e'm'* does not equal *a'b'*. It can therefore be stated that the scale

of all parts of a photograph of terrain having relief will not be the same. Those objects or features on high ground will be shown at a larger scale than those on lower ground. This is illustrated in figure 59 which shows the appearances of a hill when represented by a vertical projection on a map (Map), when photographed from directly above (Photo No. 1) and when photographed from a point to one side (Photo No. 2). The lens positions L and L' may be considered to be consecutive positions and the hill to appear in the overlap of the two pictures of the same strip. The difference in the appearance of the road *ca* is shown. Obviously such images in the overlap of successive photographs cannot be "matched" successfully as, for example, in the preparation of a mosaic. Since the images of two objects in the overlap area of successive photographs of rolling country are displaced in different degree and almost opposite direction, two photographs of such terrain cannot be accurately oriented by merely matching detail.

d. Since the distance $v'b'$ (fig. 57①) and f (the focal length of the camera) are known or measurable, the actual displacement of an object such as point B in figure 57① may be determined from formula (3), *b* above, when its height h above the datum plane passing through the point V is known.

■ 74. EFFECT OF TILT.—*a*. Because of the instability of an airplane, so far no means have been discovered of maintaining the camera in a truly vertical position at the instant of exposure. Level bubbles are used to indicate the tilt of the camera both in the direction of flight (sometimes defined as tip) and in the transverse direction. However, the bubbles are affected by centrifugal force as well as by gravity when the airplane is skidding, and their reactions are too slow to record sudden deviations from the horizontal. The effect of tilt is illustrated in figure 60. In this figure a section of theoretically level terrain is represented as being photographed with a camera having its lens position at L. The camera, instead of being truly vertical with its axis as the line vLV and the negative in a horizontal position, is tilted about L by an amount equal to the angle θ, and the camera axis takes the position $p'LP$. The principal or center point of the tilted negative is p'. The line from the lens vertical to the ground LV when extended upward intersects the tilted negative at

v', the plumb point. The plumb point of the untilted negative *v* is also its principal or center point. The plane of the tilted negative passes through the plane of the untilted negative along a trace called the "axis of tilt." The middle point of the axis of tilt, point *i'*, is called the "isocenter." Since both *Lp' and Lv* equal the focal length of the camera, triangles *Lp'i'* and *Lvi'* are similar right triangles. If the angle θ is a small angle, *i'v* may be said to equal *i'v'* in length. Consequently *p'i* is equal to *i'v'* and the isocenter *i'* is midway between the plumb point *v'* and the principal point *p'*. Assume that points *A* and *B* are points on the ground forming two of the four corners of a rectangle. Their images appear on the tilted negative at *a'* and *b'*, respectively, and on the untilted negative at *a* and *b*, respectively. On the depressed side of the negative the image of the point *A* is displaced inwardly to *a'* along a line passing through the isocenter *i'*. On the elevated side of the negative the image of the point *B* is displaced outwardly along a line passing through the isocenter *i'*. Thus the area *abcd* registered on the untilted negative as a rectangle is registered on the tilted negative as the trapezoid *a'b'c'd'*. It may be noted that the axis of tilt is common to both the tilted and the untilted negatives. It is the line of unchanged scale on the tilted negative. It is obvious that as the angle of tilt θ decreases, points *p'*, *i'*, and *v'* approach coincidence. When the tlit is slight the distances *p'i' and v'i'* become inappreciable at the scale of the negative. This same relation holds true for the corresponding photograph which is shown by a broken line at the same focal distance below the lens *L*. However, in the photograph the point *A* would be registered on the elevated side, for which the angle of tilt θ is given a positive (+) value. On the other side of the photograph the tilt would be considered negative in sign.

b. It is also to be observed that the angles at *i'* formed by the lines radiating from *i'* to *a*, *b*, *c*, and *d*, respectively, remain unchanged by tilt. The scale of a tilted negative decreases progressively from *i'* outwardly in the direction of tilt on the depressed side and increases progressively outwardly in the direction of tilt on the elevated side. Therefore, lines parallel to the axis of tilt are lines of uniform scale but the scales of no two such lines are the same. For the

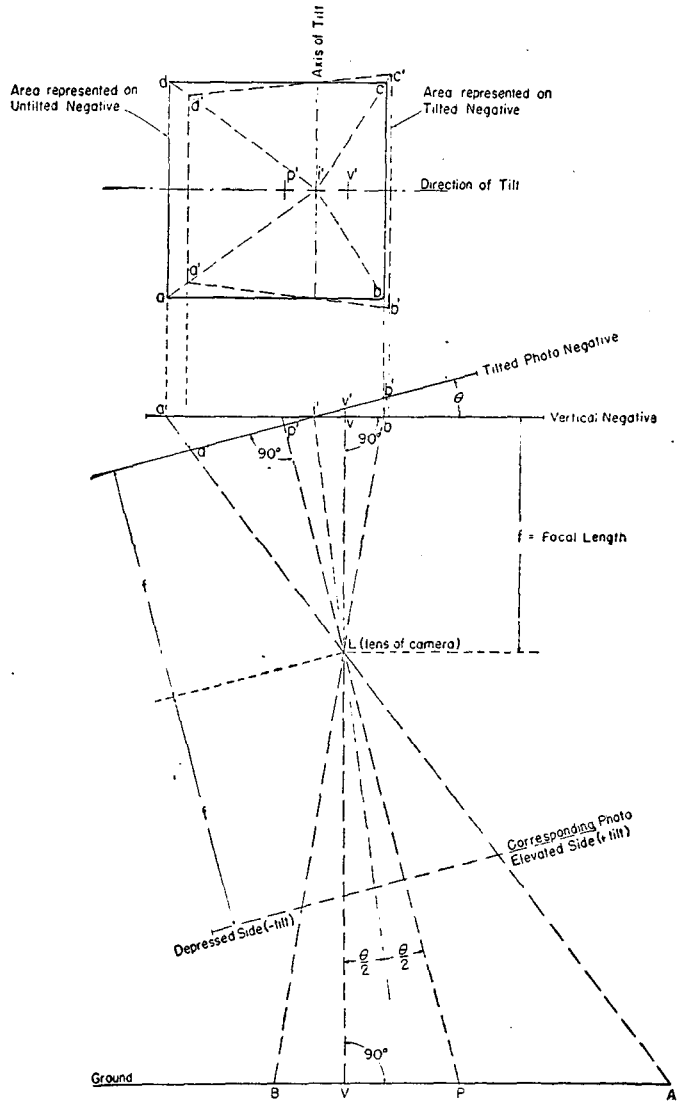


FIGURE 60.—Diagram showing effect of tilt.

same reason diagonal lines joining points unequally distant from *i'* are not lines of uniform scale and do not represent true direction.

c. The displacement due to tilt of casual points and directions is illustrated in figure 61. The images of the ground points *W*, *X*, *Y*, and *Z* are registered at *w'*, *x'*, *y'*, and *z'*, respectively, on the tilted photograph negative, whereas the correct positions of the points would have been shown on an untilted photograph at *w*, *x*, *y*, and *z*, respectively. The displacements of position and direction are apparent.

■ 75. COMBINED EFFECT OF RELIEF AND TILT.—Many puzzling discrepancies are sometimes found on close examination between the map and the vertical photograph, but when understood they will rarely present insuperable difficulties to the map and photograph reader. It has been seen that taken separately the effects of tilt and relief follow simple rules. However, it is their combined effect which is the cause of errors appearing on aerial photographs. These may be cumulative (fig. 62) or may be compensating. The displacements due to relief are radial along a line passing through the plumb point, and those due to tilt are radial along a line passing through the isocenter. The correction of the combined effect is simplified, however, in that these two points approach coincidence at the principal or center point of the photograph with decrease in the angle of tilt. It is therefore possible to assume in the case of slightly tilted photographs that for all practical purposes both displacements are radial along a line passing through the principal or center point. This assumption is made use of in the radial line method of restitution explained in paragraph 113. It does not obtain when the amount of tilt exceeds 3°. However, extensive tests have indicated that few photographs made by experienced aviators in favorable weather are tilted in excess of 3° and that the majority of the photographs are tilted less than 1°. In plain vertical photographs of average tilt taken over gently rolling or fairly flat terrain, the combined effect of errors of relief and tilt over the center half is negligible for ordinary use as a map substitute (precise measurements excepted) and is rarely prohibitive in the marginal portion. Such photographs if tilted in excess of 5° or containing a relief range in excess of 500 feet are

unsuitable for general use as contemplated herein because distances and angles measured on the photograph, as is ordinarily done on a map, will be appreciably inaccurate.

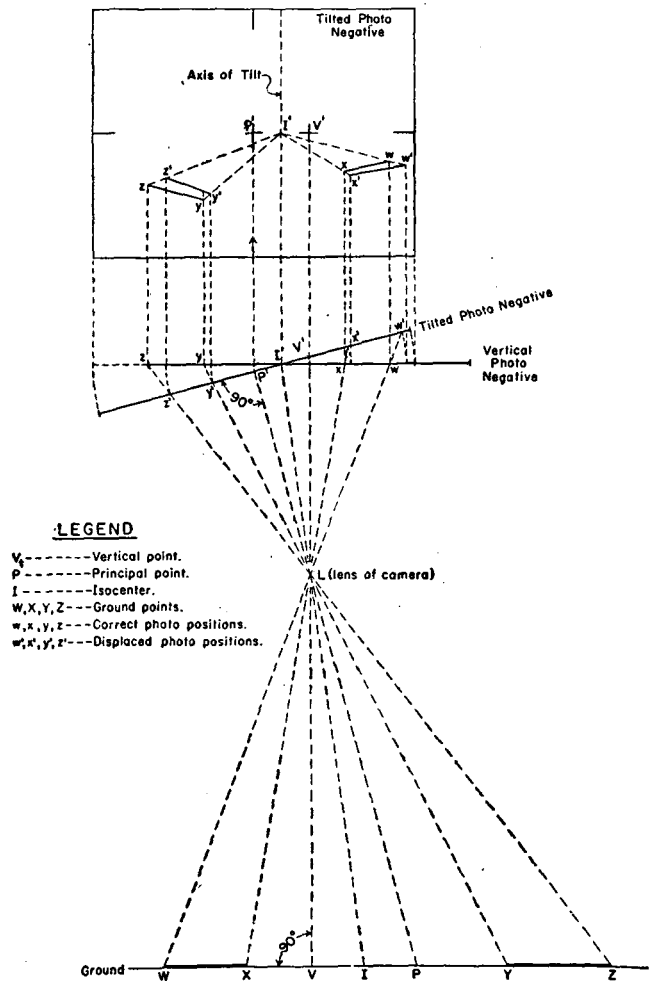


FIGURE 61.—Diagram showing displacement of position on aerial photographs caused by tilt.

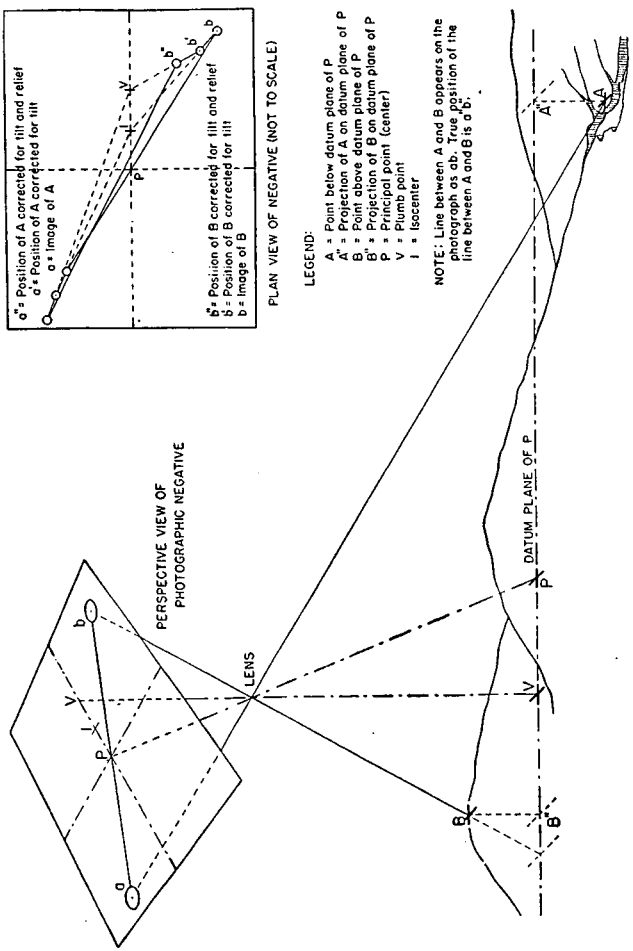


FIGURE 62.—Diagram showing displacement of position on aerial photographs caused by combined effect of relief and tilt.

SECTION VIII

IDENTIFICATION OF TERRAIN FEATURES ON SINGLE PHOTOGRAPH

■ 76. GENERAL.—*a. Topographical identification.*—Topographical identification is the art of identifying visible features of terrain from their images on a photograph, or in deducing the existence of hidden features by their characteristic effects on images of visible features. For instance, roads, railroads, houses, woods, brush, orchards, cultivated lands, etc., are easily identified, and in general closely resemble the conventional signs by which they are represented on maps. On the other hand, the existence of a small stream in heavy woods is inferred by the irregular variation in the density of the woods and association with visible parts of the local drainage net. Likewise, the existence of an invisible stream may be inferred by the narrow irregular band of brush or trees through cultivated lands, or the existence of a fence or land subdivision from a straight hedge line. Successful identification implies familiarity with the characteristics of vertical images and intelligent association of visible effects with hidden causes.

b. Tactical interpretation.—Tactical interpretation of aerial photographs is an art highly developed by the staff intelligence personnel of all armies during the World War. It is properly a specialty of the intelligence sections of staffs; is an advanced phase of aerial photograph reading; and implies tactical experience and knowledge. For treatment of this subject, see FM 30–21.

■ 77. MARGINAL DATA.—As aids in reading and use, aerial photographs to be used individually will have information along the black strip at the bottom, reading from left to right as follows:

a. An arrow ½ inch in length in the lower left corner of the negative indicating north, with letter N superimposed over the center of the shaft.

b. Name of locality or nearest locality.

c. Approximate military grid coordinates of the center of the photograph.

d. Scale of the photograph expressed as a representative fraction, in case of a vertical; altitude above the ground in feet and focal length of camera, in case of an oblique.

e. Hour.

f. Date arranged in the following order: day, in figures; month, in letters; and year, in figures.

g. Designation of squadron.

h. Serial number of negative. For example, the following is the legend on a vertical:

Saranac, N. Y.–(321–437)–1:20,000–(2:00 PM)–(24–Aug–40)–97th–M5.

■ 78. ORIENTATION.—The pictorial effect of an aerial photograph is influenced by shadow. In order that this effect will aid rather than hinder the interpretation of the photograph, the lighting conditions as they occurred in nature at the time that the photograph was taken should be simulated. To do this the photograph should be oriented so that the rays of light from a window or an artificial source strike the photograph from the same general direction as did the sun's rays on the ground. If this is not done, the effect of the light is contrary to that of nature and high ground appears to be a depression and vice versa, to the confusion of the interpreter (fig. 63).

■ 79. IDENTIFICATION OF OBJECTS.—The identification of objects on an aerial photograph or a mosaic is effected through four means as follows:

a. Shape of object.

b. Relative size of object.

c. Tone, or shade of gray, in which object appears.

d. Shadow which object casts.

■ 80. SHAPE.—On a photograph taken from the ground or on an oblique, objects appear in profile as is customary for the eye to view them. On a vertical photograph they appear in plan. A knowledge of their characteristic appearance is best gained by comparison of the photographic image with the object on the ground or with the map symbol representing it.

■ 81. RELATIVE SIZE.—The relative size of an object is a valuable aid in reading photographs. A truck on a road

gives an idea of the road width; outlying residential houses may be compared to warehouses, etc.; and in many parts where farming is intensive, the size of farm blocks offer a means for comparing sizes of objects.

■ 82. TONE.—The shade of gray in which an object appears is known as the tone of the image. It is due almost entirely to the amount of light which is reflected by the object to the camera. The more light reflected by the surface of an object toward the camera, the whiter it appears on the photograph. A surface which reflects no light toward the camera appears black on the photograph. The amount of light reflected depends on the nature and texture of the surface and the angle at which it reflects light toward the camera. Therefore the tone of an object on two consecutive photographs of a strip will vary because the reflection of the sun's rays on the two photographs will not be at the same angle. Because of the preponderant effect of texture, the tone of objects will often appear much lighter or darker than the color would appear to warrant. The following tone effects should be understood:

a. A smooth surface is a good reflector of light and appears white when the camera is in that position which catches the reflected rays of the sun. However if the light is not reflected to the camera, a smooth surface will be dark. The image of smooth water, which is an example of such a surface, is found sometimes to appear to be light and sometimes dark depending upon the angle at which the sun's rays fall upon it.

b. The majority of natural surfaces reflect light in all directions and appear intermediate in tone because some of the reflected light finds its way to the camera.

c. Since not all reflecting surfaces, for example, roofs and sides of slopes, are level, there may be some, no matter what the position of the sun, which will reflect the light and appear white.

d. Rough surfaces reflect light at many different angles in an amount depending upon the nature of the object. Their tone is usually an intermediate one. Roads, unless tarred or oiled, are by nature good reflectors of light and possess a surface sufficiently rough in texture to reflect light through a wide range in position of the sun. As a result, roads almost invariably show as a light line.

e. Any change in the texture of a portion of an object is evident on an aerial photograph through a resulting difference in tone when compared with the other portions. Thus the trampling of a field of grass by walking across it alters the reflection of light and registers a difference in tone on a photograph.

①

FIGURE. 63.—Effect of shadow upon perception of relief. The two illustrations are an identical photograph differing by 180° in orientation.

■ 83. SHADOW.—The effect of shadow is a most important consideration in the interpretation of vertical aerial photographs and mosaics. The shape of an object is often more discernible by the shadow it casts than by either its image or its tone. This is because its vertical dimensions shown by the shadow may be more characteristic than its horizontal

dimensions which are shown by the image; or its tone may blend into the surrounding landscape while its shadow may stand out in contrast. The effect of shadow is an index to valuable military information such as the approximate height, the number of spans and type of a bridge, the height of trees, the shape and height of buildings, and the depth of cuts,

②

FIGURE 63.—Effect of shadow upon perception of relief. The two illustrations are an identical photograph differing by 180° in orientation—Continued.

pits, and quarries. A shadow will sometimes make the general character of relief discernible but, as has already been mentioned, if the photograph is not held so that the direction of the shadows coincides with the observer's sense of direction of the source of the light, the effect is reversed and a depression will appear to be an elevation. This is illustrated in figure 63.

① Summer.

FIGURE 64.—Effect of season.

② Winter.

FIGURE 64.—Effect of season—Continued.

■ 84. PHOTOGRAPHY.—In order to reduce the length of shadows, photography is usually undertaken when the sun is 3 hours or more above the horizon. Light may be diffused by excessive moisture or dust in the atmosphere, resulting in lack of definition in the prints. Intense light produces sharp definition of detail and sharp shadow contrasts. The high-angle sun around noon produces the least shadow effect, and photographs taken around noon are best suited for study of detail through forest canopies and for depicting exact outlines. The low-angle sun, morning or afternoon, produces the greatest shadow effect. Low-lying solid cloud masses effectively prohibit high-altitude photography, and broken clouds seriously interfere by producing white spots on pictures and cloud shadows on the terrain.

■ 85. EFFECT OF SEASON (fig. 64 ① and ②).—Seasonal changes produce corresponding characteristic changes in the physical appearance of terrain on aerial photographs. In summer, deciduous forests show impenetrable expanses of luxuriant treetops, resembling the effect produced by the conventional signs used on some topographical maps. Lesser detail of the terrain is largely hidden. The line of demarcation between forest and open areas is sharply and exactly defined. In winter, deciduous forests on large-scale photographs show a confusion of tree skeletons through which the light penetrates to reveal roads, trails, drainage, and relief with good effect. The line of demarcation between forested and open terrain is not so clear, however, as on small-scale photographs; the tangle of tree trunks and limbs imparts a blurred appearance to the terrain. The appearance of grass and farm land on aerial photographs changes with the seasonal state of culture. Streams in the wet season are broad and may cover extensive back-water areas in flood. The same streams in the dry season may show dry beds or insignificant threads of water. Snow in winter may completely blanket an area which is normally rich in detail.

■ 86. TOPOGRAPHICAL FEATURES.—*a.* Woods on aerial photographs appear as dark masses of irregular outline. The exact shape, size, and density are much more clearly and accurately shown than on the average topographical map. The seasonal characteristics are reflected in the photographs.

In winter photographs of deciduous forests, the leafy canopy is absent, exposing substantially all ground detail which would be wholly or partially obscured in summer photographs of the same forests. Evergreen forests show dark and dense in all seasons (fig. 65 ① and ③).

① Woods, improved and unimproved roads, gravel (or borrow) pit in left foreground.

FIGURE 65.

b. Brush appears similar to light woods but may be distinguished by its sparse character and lack of height (fig. 65②).

c. Bodies of water have a characteristic appearance appreciably lighter or darker than the surrounding land, de-

pending upon the amount of reflection from the surface when the photograph was made (fig. 65③).

d. Streams appear in characteristic wavy traces and show presence of water by darker or lighter lines. In woods, the exact location of small streams may be difficult if not im-

③ Stream partly obscured by woods.

FIGURE 65—Continued.

possible to determine except by reference to a map or inspection of the ground. The visible evidences of such streams are breaks or variations in density of the forest canopy (fig. 65②, ⑤, and ⑦).

e. Cultivated fields show clearly as rectangles or irregular figures of definite shapes and shades. The nature of the

crop usually cannot be determined from the face of small-scale photographs but may be recognized on large-scale photographs. Grain in shocks is conspicuously shown by regularly spaced dots in a lighter background. Fields from which crops have been harvested show light areas. Fields

③ Cultivated fields, woods, orchard, and river.
FIGURE 65—Continued.

with heavy standing crops and grasslands show dark areas. On large-scale photographs they present rough surface appearances. Plowed fields show distinct shading (fig. 65③ and ④).

f. Fences, on large-scale photographs, are distinguished by shadows of the fence posts. On small-scale photographs,

fences are inferred from hedge lines, section lines, outlines of cultivated lands, and the characteristics of paths, trails, and roads (fig. 65⑥).

g. Roads show up in general as light lines or narrow bands—the more used the lighter the appearance. Improved roads

⑥ Railroad, including main line, branch line, siding, and railroad cut.

FIGURE 65—Continued.

show regularity in width, long tangents, and easy curves. The hard surface is clean-cut in outline and may show dark along the middle from the oil drips of automobiles, and light along each edge. Unimproved roads are of irregular width and trace, and may contain sharp turns. Evidence of condi-

tion of road surface is usually apparent from blemishes, shadows, and color variations (fig. 65① and ⑦).

h. Railroads show straighter, darker traces than highways, have fewer changes of direction, long easy curves, and heavy cuts and fills (fig. 65④ and ⑤).

⑤ Railroad bridge over a small stream (at left), overpass (at right).

FIGURE 65—Continued.

i. Small bridges may be looked for at all lesser stream crossings and may be identified by the narrowing of roadbed and shadows cast.

j. Buildings show as indistinct roof images and are sometimes difficult to distinguish from blemishes on prints. The

decisive evidence of the presence of a building is provided by its shadow. Groups of buildings may be blurred by the collective shadow effect. The shape of the shadow is an index of the type and size of the building. The building site is usually the terminus of a road or path (fig. 65③ and ⑥).

⑥ Improved and unimproved roads, trails, and paths.

FIGURE 65—Continued.

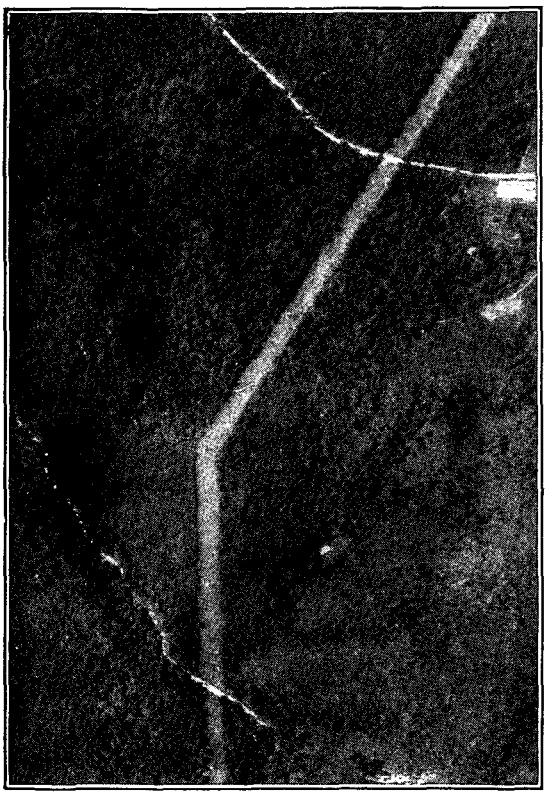
k. Villages and towns are easily distinguished and appear much the same as they do on maps.

l. Trails and paths appear as irregular white bands, lightness and width indicating degree of use (fig. 65⑥).

m. Works of man appear in straight lines, in geometrical form, in unnatural regularity, and relation (fig. 65⑦).

n. Natural features occur in irregular lines, without precision of form and relation.

■ 87. MILITARY FEATURES.—Military works and activities produce characteristic images and terrain effects which make aerial photographs one of the most important sources of



© Slashing for high tension electric power line, stream, and road.

FIGURE 65—Continued.

combat intelligence. FM 30–21 covers this highly important subject.

■ 88. RELIEF.—Single vertical photographs afford only certain clues in regard to relief. Figure 66 represents an untrimmed

vertical photograph from the B (central) chamber of a T–3A camera. Compare this photograph with a sketch of the same area shown in figure 67. The most important clues are those afforded by streams and ponds which indicate low ground. Other clues indicating relief are the alinement

FIGURE 66.—Photograph made with B (central) chamber of Air Corps five-lens T–3A type camera.

and grading of roads and the shadows cast on and by slopes; these, especially the latter, may be very misleading. Direct evidence of relief can be obtained only by stereo examination of an overlapping pair of aerial photographs.

SECTION IX

STEREOVISION AND EXAMINATION

■ 89. STEREOVISION.—*a. General.*—The ordinary vertical photograph has a flat appearance, which makes it difficult to distinguish between hills and valleys. If two overlapping vertical photographs are viewed either with the naked eyes or

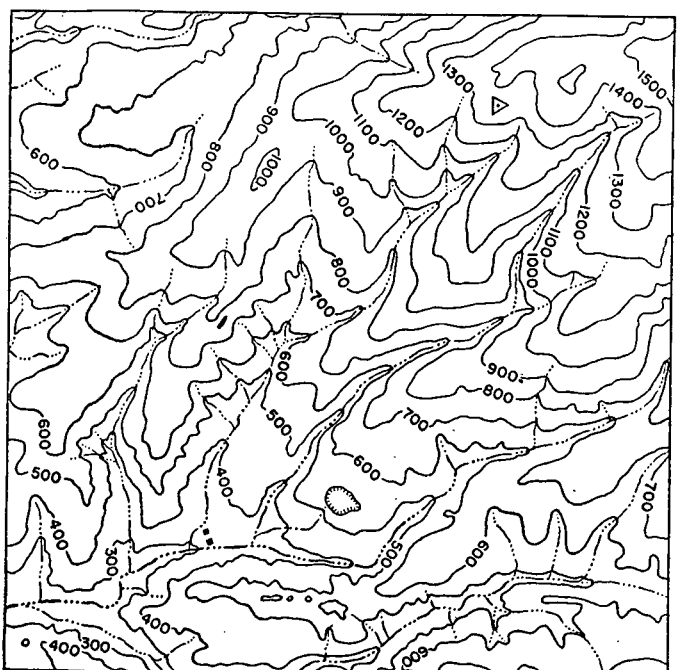


FIGURE 67.—Sketch of area shown in figure 66, representing relief (other detail omitted).

with some type of stereoscopic instrument, the observer will get the effect of depth or relief. This type of study gives valuable training in the understanding and reading of single vertical photographs and photomaps. There are several methods which will assist in acquiring this ability and each individual should experiment until he finds the method which

gives the best results. This ability comes very quickly to most men; others will have to use patience and perseverance to obtain it. Experience with large groups of men reveals that anyone with eyes good enough to be in the Army can acquire the ability to see stereoscopically. Stereo studies properly done put no strain on the eyes, and some oculists even prescribe similar exercises to strengthen the eyes. However, when magnifying spectacles are used, they should be removed from the eyes before looking up from the photographs.

b. Stereogram.—A pair of small pictures, geometric figures, or portions of two overlapping aerial photographs arranged for stereovision is called a stereogram. Figure 68 shows four simple stereograms; figures 69 and 70 show portions of aerial photographs arranged as stereograms.

c. Stereo-pair.—Two vertical photographs of an object or group of objects taken from the same elevation from two different camera positions and with an overlap of not less than 60 percent nor more than 75 percent are known as a stereo-pair (see fig. 72).

d. Stereo-triplet.—Three verticals such that the entire area of the center picture is overlapped by the other two is called a stereo-triplet. For methods of mounting, tilting, marking, etc., see FM 30–21.

e. Anaglyph.—An anaglyph is a form of stereogram on which a picture is formed by almost superimposing an image in red over one in blue to secure stereo or perspective effect when observed through an anaglyphoscope—spectacles with one blue and one red lens. Several methods of indicating perspective relief of the terrain are in use. With aerial photographs available, the simplest method is the overprinting in two colors of a stereo-pair. Another method, the anaglyph of the contoured map, is the result of an expensive and time-consuming process. The polaroid anaglyph is still another form of portraying three dimensions. The anaglyph, as a rule, gives less detail than a stereo-pair of the same scale. However, the anaglyph is of great value in stereo instruction. For an illustration of an anaglyph, see TM 5–230.

■ 90. STEREOVISION EXERCISES.—*a. Preliminary exercises.*—Experience has shown that the best method of quickly ac-

quiring the ability to see photographs stereoscopically either with the naked eyes or with an instrument is to practice certain preliminary exercises. Figure 71 illustrates a simple device which can be quickly and easily prepared by the student for use in these exercises. Cut two pieces of white cardboard each 5 inches long by 3 inches wide. At the exact center of each piece of cardboard describe a circle exactly 1½ inches in diameter. Number these pieces of cardboard 1 and 2, respectively. On card No. 2 draw a smaller circle exactly ⅜ of an inch in diameter, with its center 1⅛ inches to the left of the center of the large circle. Draw a cross ⅜ by ⅜ inch with its intersection 1⅛ inches to the right of the center of the large circle. Label the reverse of card No. 1 as No. 4, and the reverse of card No. 2 as No. 3, and draw a line on each as illustrated in figure 71. Now cut out the large circle from each card. Do *not* cut out the small circle on card No. 2. Sit in a chair and look across the room at a fairly distant wall. Hold card No. 1 about 6 inches in front of the eyes, with the hole directly in front of the bridge of the nose. Look at the wall, through the hole, with both eyes open. Note that there are apparently two distinct holes in the card. This is the first step of stereovision. Take card No. 2. This card is like No. 1 except that it has a circle printed on one side of the hole and a cross on the other side. The method of using this card is exactly the same as No. 1. However, when you see the two holes you will also see between them the circle with the cross inside. Concentrate your eyes on the image. Twist the card and notice how the cross moves with relation to the circle. You will note that if the cross moves up, the circle moves down and vice versa. The holes may appear to be slightly overlapping at some times; at other times the circle and the hole may appear to be floating in the holes entirely off the card. Try holding a strip of paper between the two holes with the images of the circle and the cross on the strip. While you are seeing the hole double, move the paper nearer and farther from the eyes. Watch what happens to the image. When you can see these images, and thus see double, you have accomplished the necessary muscular control to read a stereogram. Practice with this card until you can see these images without effort. When you have acquired skill with No. 2, go on to Nos. 3 and 4. These are used together, No. 3 on the left, No. 4 on the right.

Place the two cards together with the black lines matched and hold them against the nose with the holes in the same position as if they were glasses. The holes should be the same distance apart as your eyes. The distance is normally about 2.6 inches, center to center. Looking through the holes, focus on a distant object. Now move the cards in the direction of this object until they are about a foot from the eyes. You will now see three holes with the object viewed in the center hole. Remember during this that the eyes *must* remain focused on the distant object. When the three holes are seen, the eyes are in the proper position for stereovision. The images of the three holes appear although you are not looking at them. You are looking at the distant object. This is similar to lining up your sights on the target range. You are focusing at the front sight but you see both the bull's-eye and rear sight. Practice at this exercise will enable the three holes to be seen without first focusing on a distant object. This means that you have acquired sufficient muscular control over your eyes to see stereoscopically.

b. Fusion exercises.—The next step is practice in fusing two pictures. In figure 68 the drawings can be fused as follows. Focus the eyes on a distant object. Without changing the focus, bring figure 68 in front of the eyes and about 6 to 10 inches away. As you continue to gaze at the drawing the dots will merge until apparently you have one dot on one figure. You will still get three images but the center one is the important one on which you should fix your attention disregarding the other two outside images. Now see what effect you get with the pair of dots below on figure 68.

c. Exercises for perception of relief.—Figure 68 shows two views each of two geometric figures. Using the same methods as in *b* above, fuse the first pair of drawings, which should cause you to see a square pit with a pyramid sticking up out of the bottom. In other words, instead of a flat geometric drawing, you are seeing a three-dimensional picture. Fuse the other pair of drawings and observe the results.

d. Study of stereograms.—Figures 69 and 70 are stereograms. To see these properly, use the same methods as prescribed above. First, fuse the square points marked *A* in figure 69. You will again get three images, but the center one is the one on which to focus, and is the one on which relief will be visible. If you have difficulty seeing this center image clearly,

hold a piece of cardboard vertically up to the nose so that it is perpendicular to the pictures and one edge of the cardboard lies on the line dividing the two pictures of the stereogram. This will eliminate the two outside images and leave only the center image. Focus on this, and the trees and buildings will appear to stand up high above the page. Practice with figures 69 and 70.

e. Cross-eyed stereovision. — While the great majority of people can see stereoscopically by the method described above, there are a few who may be able to see better by using another method. The difference lies in the fact that in the parallel vision system described above, the right eye looks at the right picture and the left eye at the left picture. In this second method, the right eye looks at the left picture and the left eye at the right picture or in other words with the eyes crossed. In using the stereograms, the relief will be reversed with this method. The hills will look like valleys and the valleys like hills. Therefore, for study of overlapping pairs, the right and left pictures should be placed on the left and right, respectively. This will give the stereo observer using the cross-eyed method the proper effect of relief.

■ 91. STEREOSCOPES.—*a. Types.*—The stereoscopes used for the interpretation of aerial photographs may be classified as mirror, lens, or prism types. The mirror stereoscope (fig. 74) possesses the advantage of a large field of view and is considered to be the most adaptable for general military use. The lens stereoscope (fig. 75), although affording only a limited field of view, has the advantage of permitting the introduction of magnification. The prism stereoscope (fig. 76), which is larger and more expensive than either of the other two types, possesses the advantage of permitting a wide separation of the two overlapping photographs and is therefore particularly suitable for examining T–3A photographs. The instrument illustrated has a magnification of 2 power.

b. Improvised stereoscopes.—A suitable stereoscope for interpreting detail on aerial photographs may be improvised by means of two magnifying glasses of equal power (fig. 77). One glass may be held in each hand and stereoscopic fusion obtained by looking through the inner half of each lens. For more prolonged inspection the glasses may either be

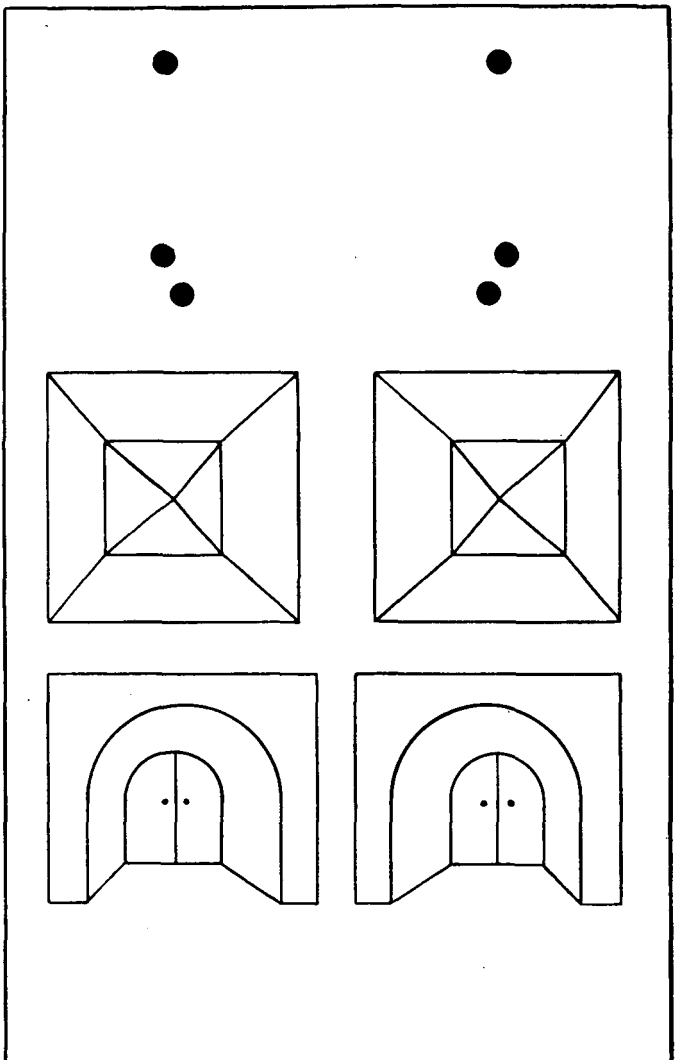


FIGURE 68.—Simple stereograms.

supported on an improvised stand or, if of appropriate size, may be mounted in a spectacle frame. Cellulose tape may be used to hold the glasses to the frame. A pair of strong

FIGURE 69.—Stereogram.

reading glasses will serve as a spectacle stereoscope but will permit only a small separation of the pair of photographs with a corresponding reduction of the effective overlap area.

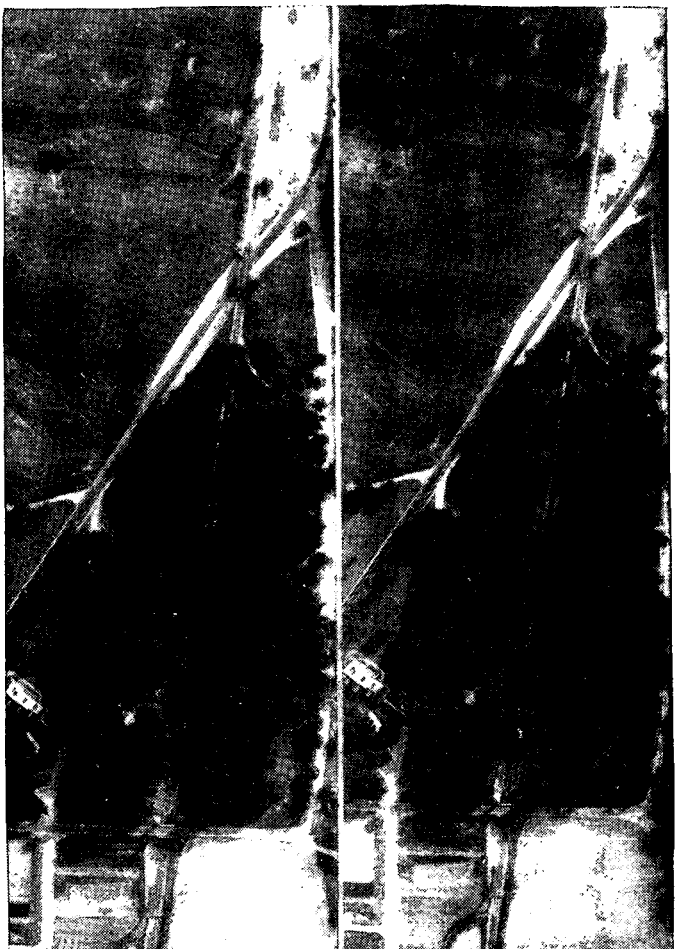
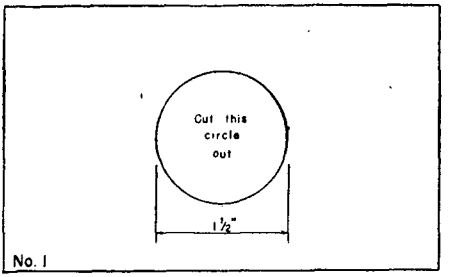
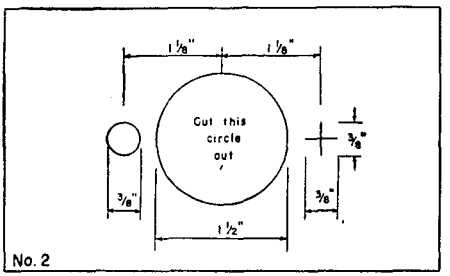
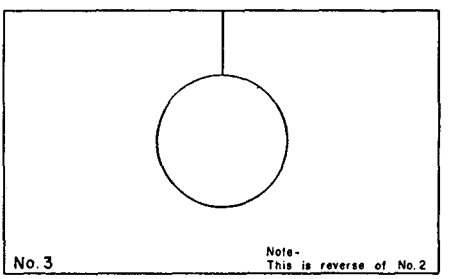


FIGURE 70.—Another view of a stereogram.







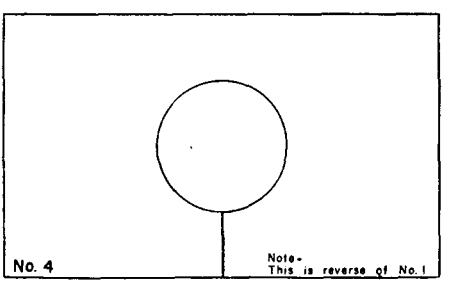


FIGURE 71.—Illustration of cards for use in stereovision exercises.

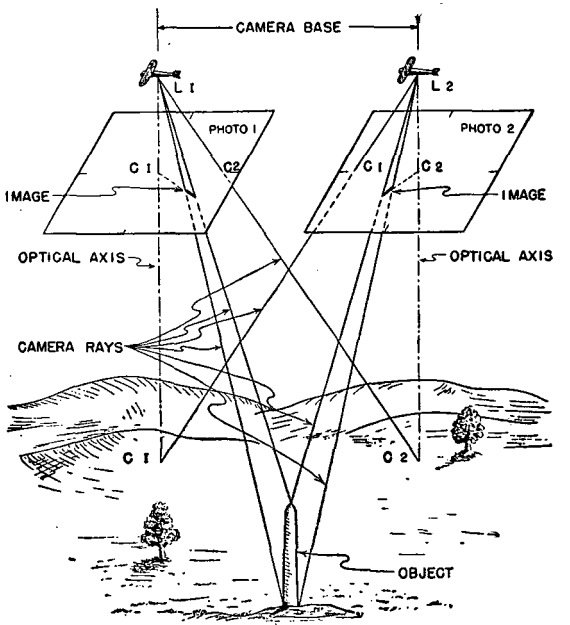


FIGURE 72.—Diagram of a stereo-pair of aerial photographs.

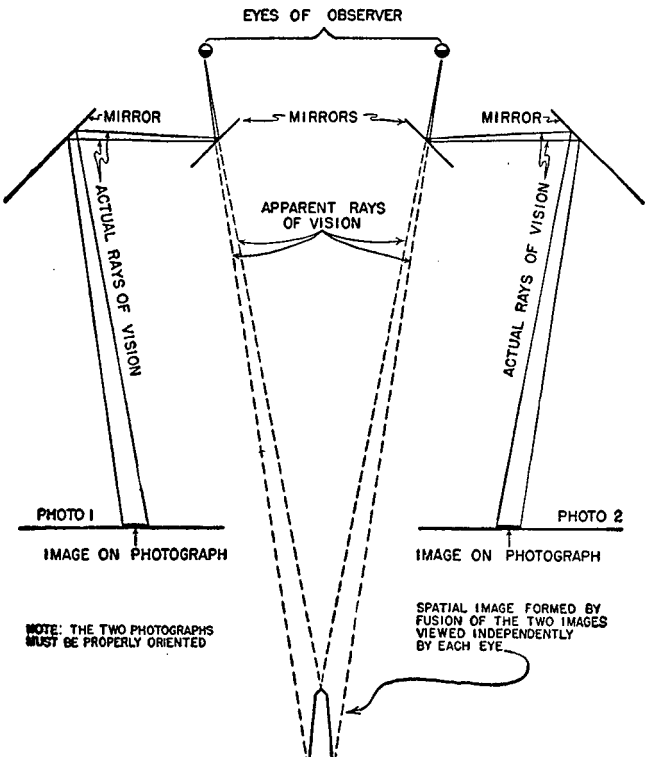


FIGURE 73.—Diagram showing stereo perception.

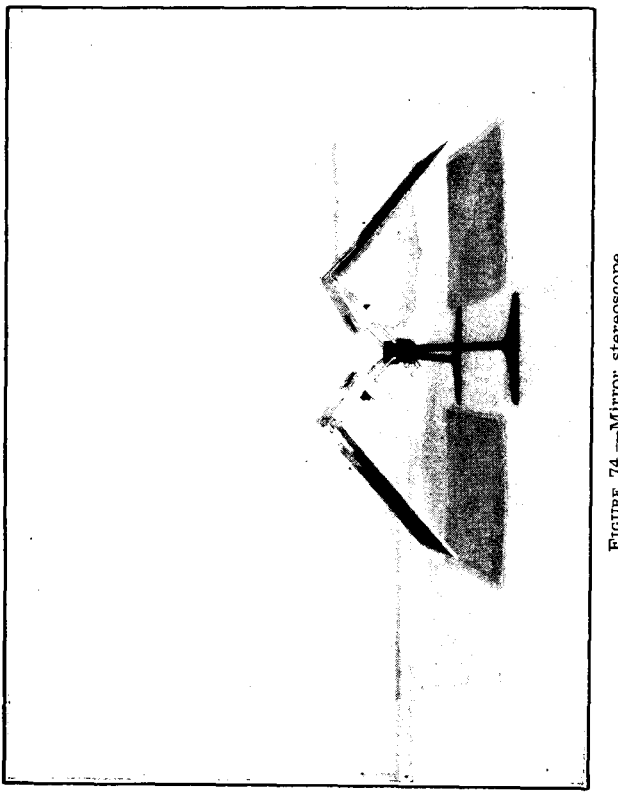


FIGURE 74.—Mirror stereoscope.

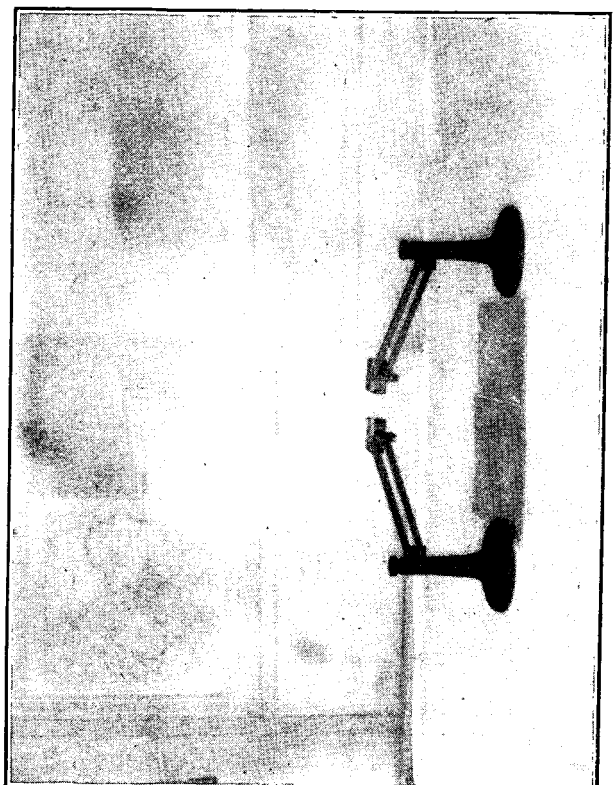


FIGURE 75.—Lens stereoscope.

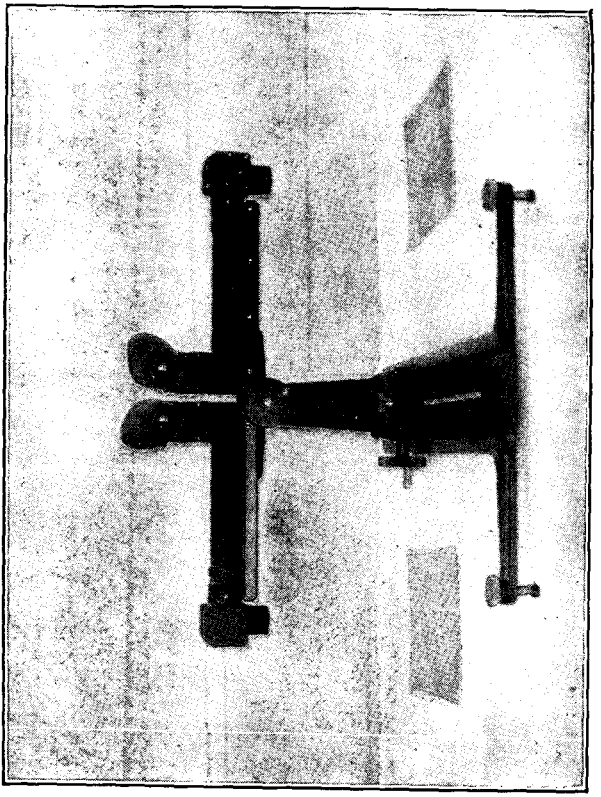


FIGURE 76.—Prism stereoscope.

■ 92. STEREO EXAMINATION OF AERIAL PHOTOGRAPH.—*a. General.*—(1) Appreciation of relative distances is based fundamentally on the slightly different view of various objects presented by each of the two eyes. A person with one eye or a person with only one eye open cannot perceive relative distance any more than a person can perceive depth looking at a single vertical photograph. Under such conditions, distance is sensed only through experience.

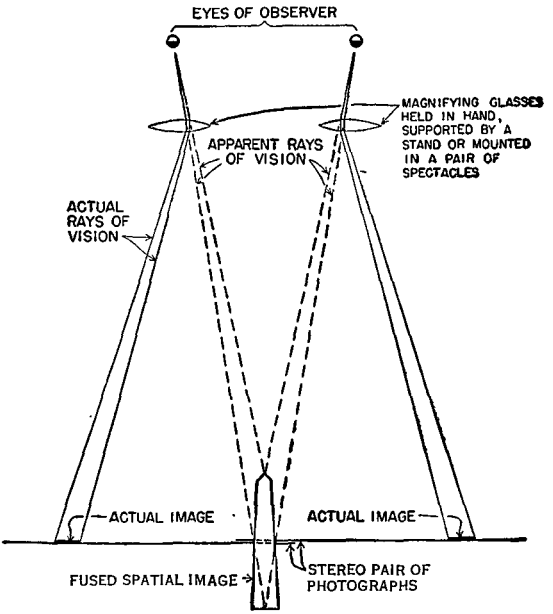
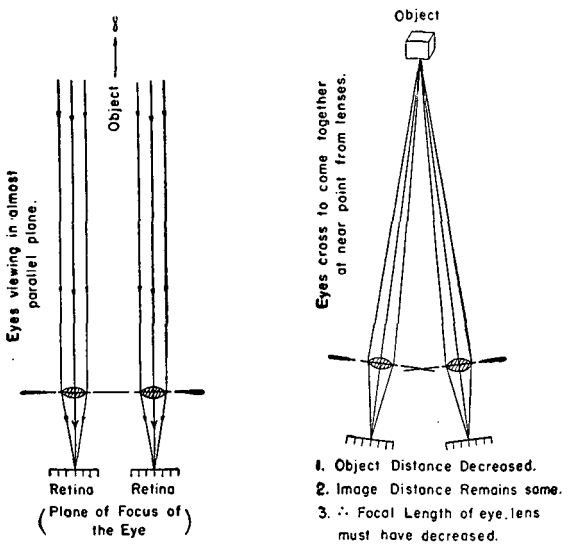


FIGURE 77.—Diagram showing stereo examination by means of improvised lens stereoscope.

(2) Unaided eyes viewing a distant object (fig. 78①) have their lines of vision almost parallel. As the object comes nearer (fig. 78②), the focal length of the eyelens decreases and depth perception is better. If each eye looks straight ahead with line of vision parallel, and the eyelenses are kept at a short focal length, the two images (fig. 78③) will fuse, the result being the same as in figure 78②. This latter

process usually requires training of the eyes, while with little training stereovision can be obtained with the use of spectacles (fig. 78④).

(3) If two vertical photographs of an object or a group of objects are taken to the same scale from two different camera positions as in figure 72, and each picture is viewed by one eye to the exclusion of the other but both pictures viewed simultaneously (fig. 73), the appreciation of distance is then possible because a different view is presented to each



① Unaided eyes viewing distant object.

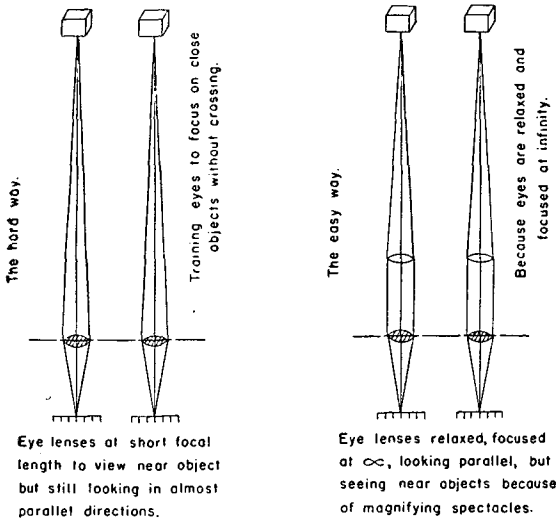
② Unaided eyes viewing very near object.

FIGURE 78.—Stereovision.

of the two eyes as is the case in ordinary vision. In order that a combined or "fused" image may be obtained, certain conditions must be satisfied in the arrangement and in the viewing of the two photographs. These are briefly as follows:

(*a*) Both eyes of the observer should be of equal power or corrected by optical aids, and the two photographs should be equally distinct and equally illuminated.

(*b*) The pictures should be so arranged with respect to each other and to the eyes of the observer that exposure conditions are restored. The distance between the centers of the two photographs corresponds to the base between camera positions, and the positions of the eyes correspond to the positions of the camera lens. The eyes must be parallel not only to the line joining the centers of the photo-



③ Stereoscopic viewing—training to see stereoscopically with unaided eye.

④ Stereoscopic viewing—training to see stereoscopically with spectacles which decrease focal length of eyelens.

FIGURE 78.—Stereovision—Continued.

graphs but also to a line on each photograph drawn between points of detail marking the two corresponding center points. The stereograms shown in figures 69 and 70 are the overlapping portions of two such vertical photographs. They have been mounted side by side in the proper relation with each other to secure stereovision. Any pair of overlapping vertical photos (taken at approximately the same elevation), if arranged in this same manner, can be read stereoscopically.

b. Method.—(1) Place one photo on top of the other so that overlapping detail common to both roughly coincides (fig. 79).

(2) Next note the position of an imaginary line joining their approximate centers. The eye base of the observer must be parallel to this line of centers. Turn the photographs as a unit until the condition is satisfied.

(3) Now separate the photos along the line joining the centers (fig. 80), moving the one on the right to the right and viewing it with the right eye, and the one on the left toward the left and viewing it with the left eye. The exact orientation of the photographs with respect to each other can be obtained by keeping detail, such as roads or streams, which appear in the overlap area parallel to each other. For example, take a road that appears on both photographs. Rotate one photo until the image of the road on this photo is parallel to its image on the other photo. The distance that two objects appearing in the overlap area have to be separated depends on whether the photos are to be examined by the naked eye or by some stereoscopic instrument. For beginners with the unaided eye, this separation of detail should be not more than 1¾ inches. With practice after the steroscopic effect is obtained, the photographs can be gradually separated until a large portion of the overlapping area can be seen. If the study is made first with the right-hand photograph overlapped on top of the left and then with the left-hand photograph placed on top of the right, the entire overlapping area of a 9- by 9-inch stereo-pair with 60 percent overlap can be studied stereoscopically with the unaided eye.

c. Procedure of using stereoscope.—The following procedure should be observed when making a stereo examination of aerial photographs (see also sec. VII, TM 5–230):

(1) Orient the stereo-pair in the direction of flight so that the overlapping detail common to both is roughly in coincidence (fig. 79).

(2) Place the photographs under the stereoscope so that the left print (taken by the camera on the left of the overlap area) is observed by the left eye and the right print by the right eye.

(3) Shift the photographs so as to bring an imaginary line drawn between the center points parallel to the eye base and

in prolongation with one another in the center of the field of view of the stereoscope.

(4) Without changing the relative position of the imaginary lines drawn through the center points, bring together or separate the photographs until stereo conditions of fusion are best fulfilled (fig. 80).

■ 93. FAULTY STEREO EFFECTS.—*a. Faulty stereo orientation.*— Faulty orientation of a stereo-pair with respect to the eye base introduces false parallax difference and lack of correspondence. These make it difficult to fuse detail and cause a diminution of relief.

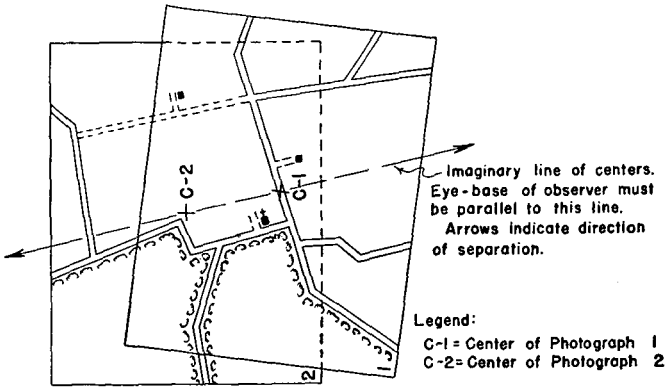


FIGURE 79.—First step in arranging photographs for stereo study (detail in overlap area matched).

b. Tilted photographs.—Photographs which are tilted cannot be brought into accurate correspondence as described in paragraph 92 and sometimes must be shifted as the field of view of the observer is moved from point to point. Distortion of relief results from such a condition.

c. Pseudoscopic effect.—If the position of two photographs forming a stereo-pair is reversed so that the left print (taken by the camera on the left side of the overlap) is viewed by the right eye and the right print by the left eye, the impression of relief is reversed; that is, the point of lowest elevation is reconstructed nearest to the eye and appears to be of high-

est elevation. Practical use may be made of this factor in that drainage lines may be traced by making them appear as ridge lines.

SECTION X

PREPARATION OF AERIAL PHOTOGRAPHS FOR USE AS MAP SUBSTITUTE

■ 94. GENERAL.—In order to make a photograph or groups of photographs sufficiently accurate and detailed for most efficient use, certain mechanical operations must be effected. Certain inaccuracies inherent in a single photograph may

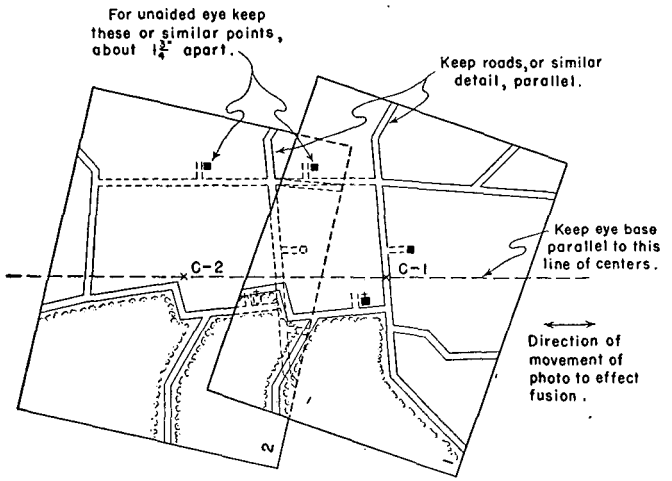


FIGURE 80.—Photographs arranged for stereo study.

be overcome in the compilation and finishing of a group, and with the aid of machines, stereo-pairs may be accurately contoured. By these processes the value of photographs as map substitutes or photomaps is greatly enhanced.

■ 95. SCALE.—An important difference between military maps and vertical photographs used as maps lies in the choice of scales. Military maps conform to a prescribed range of standard scales expressing the relation of ground to map in simple terms. The horizontal scale is uniform throughout the map. On the other hand, the scales of vertical photo-

graphs are dependent principally upon the variable and uncertain factors of lens height, camera tilt, and relief of the ground in the photographic field at the moment of exposure. The scale of a vertical photograph, therefore, not only changes on the several photographs of an overlapping series but is also not uniform on a single photograph. If the degree of scale variation is small the resulting errors become inappreciable, and probably no greater than those which result from average measurements made on a map in the field with the relatively crude instruments used in map reading.

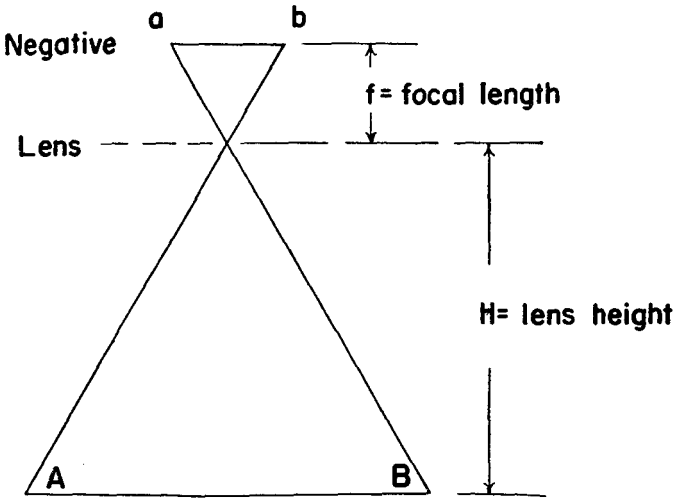


FIGURE 81.—Determination of scale from height.

■ 96. DETERMINATION OF SCALE.—*a. By lens height.*—By inspection of figure 81 it may be seen that, if the ground is assumed to be a plane surface, any distance on the negative, such as *ab*, bears a relation to the corresponding distance on the ground *AB* equal to f/H where f is the focal length of the camera and H is the height of the camera lens above the ground (both f and H being expressed in the same unit of measurement). Hence:

$$RF = \frac{f}{H}$$

Since the altimeter of the airplane usually expresses the elevation above sea level in place of H, the expression H_α—E may be substituted, H_α being the altimeter elevation above

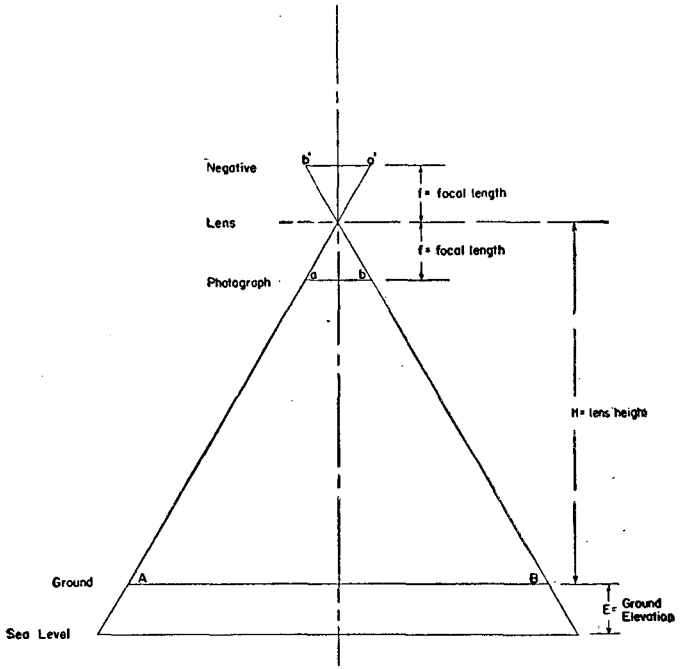


FIGURE 82.—Diagram showing relation of scale, focal length, and lens height.

sea level and E the average elevation of the terrain shown in the photograph (fig. 82). We may accordingly write

$$RF = \frac{f \text{ in feet}}{H_\alpha \text{ in feet} - E \text{ in feet}}$$

Example:

Focal length of camera is 6 inches or $\frac{6}{12}$ feet.
Altitude of the airplane is 10,000 feet above sea level.
Elevation of the ground is 1,000 feet above sea level.

$$RF = \frac{\frac{6}{12}}{10{,}000 - 1{,}000} = \frac{1}{18{,}000}$$

It is usual for a request for aerial photographs to state the scale desired. The flying altitude of the airplane is determined from this formula.

b. By comparison with map or ground.—(1) In *a* above it was stated that the scale of an aerial photograph is equal to the quotient of the focal length of the camera divided by the height of the camera lens. The scale determined by this formula would be the true scale of the entire photograph under the conditions of absolutely accurate altimeter records, complete absence of tilt, and perfectly level terrain. However, altimeter records are often appreciably affected by local

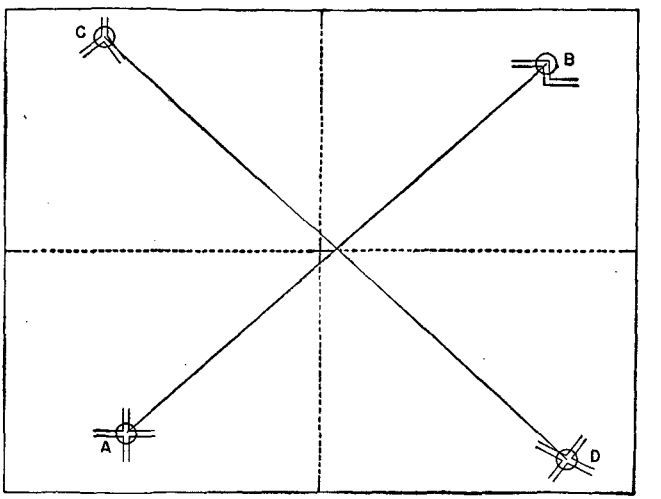


FIGURE 83.—Diagram showing proper location of scale lines.

atmospheric conditions, and the effects of tilt and relief will usually cause some scale variation within the limits of the photograph. For this reason, scale can be determined more accurately by comparing distances measured on the photograph with corresponding distances either on a map or on the ground. Such distances should be between points which are well defined both on the photograph and on the map (or ground). When it is desired to apply the scale to the entire photograph, the distances measured on the photo-

graph should represent the average scale of the photograph. In the discussion which follows, the selected distances are termed "scale lines."

(2) In order to represent the average scale of the photograph, a scale line should extend well across the face of the photograph (fig. 83). Since the effect of tilt is assumed to be radial along a line passing through the center of the photograph and because of its effect in compensating on opposite sides of the photograph, the scale line should pass near to its center. In order that the scale determination will not be affected unduly by relief, care should be taken that there is not a pronounced difference in relief between the points at the ends of the scale line. With the scale line thus determined, its RF can be solved in the same manner as given for maps in paragraph 14; the RF of the scale line being roughly the RF of the photograph.

(3) *Ground.*—The distance between the identified points is measured. Then:

$$\text{RF of the scale line} = \frac{\text{photo distance in inches}}{\text{ground distance in inches}}$$

Ordinarily it should prove convenient and satisfactory to select two points on a straight stretch of a highway and use the distance along the highway as the scale line in the computation of the RF of the photograph.

(4) *Map.*—(*a*) The most simple method of determining the RF of a scale line from a map of known RF is by converting the distance on the map to the equivalent distance on the ground and proceeding as in (3) above.

(*b*) A more rapid method of determining the RF of a scale line is by the direct formula:

$$\text{RF of scale line} = \frac{\text{photo distance in inches}}{\text{map distance in inches}} \times \text{RF of map}$$

(*c*) Although for terrain of low relief one such well-chosen scale line will often suffice, it is preferable that the average scale of the photograph be determined from two or more scale lines, the value assigned to the denominator of the RF of the photograph being the average of the denominators of the computed RF's of each scale line. Thus we may write

$$\text{Average RF of the photo} = \frac{1}{\text{mean of the denominators of the RF's of the scale lines}}$$

Example:

Distance *AB* on photo=8 inches
Distance *AB* on map=6 inches
Distance *CD* on photo=9 inches
Distance *CD* on map=6.65 inches
RF of map is 1:20,000

Using scale line *AB*

$$\text{RF}=\frac{8}{6\times 20{,}000}=\frac{1}{15{,}000}$$

Using scale line *CD*

$$\text{RF}=\frac{9}{6.65\times 20{,}000}=\frac{1}{14{,}778}$$

Average RF of the photo $=\frac{1}{\frac{1}{2}(15{,}000+14{,}778)}=\frac{1}{14{,}889}$

For ordinary purposes a 1:15,000 scale will serve in measuring distances on the photograph.

■ 97. SCOPE.—The area covered by an aerial photograph can be calculated readily by either of the following methods:

a. By the ratio $\frac{\text{ground distance}}{\text{photo distance}}=\frac{H}{f}$ (*H* and *f* being expressed in the same units of length)

Therefore the ground scope of any photograph $=w\frac{H}{f}\times l\frac{H}{f}$

where w=width of the photograph
l=length of the photograph
H=height of camera lens
f=focal length of camera

For K–3B type photographs (f=12 inches, w=7 inches, l=9 inches)

$$\text{Scope}=\frac{7}{12}\times\frac{12}{12}\times H\times\frac{9}{12}\times\frac{12}{12}\times H=\frac{7}{12}H\times\frac{9}{12}H \text{ square feet}$$

For T–3 type photographs (f=6 inches, l=w=32 inches)

$$\text{Scope}=\frac{32}{12}\times\frac{12H}{6}\times\frac{32}{12}\times\frac{12H}{6}=\frac{16}{3}H\times\frac{16}{3}H \text{ square feet}$$

Thus at a height of 12,000 feet the scope of these photographs is as follows:

For the K–3B type, scope $=\frac{7}{12}12{,}000\times\frac{9}{12}12{,}000=7{,}000\times 9{,}000$ square feet=2.26 square miles.

For the T–3A type, scope=64,000×64,000 square feet=146.9 square miles (overall).

b. By the ratio, $RF=\frac{\text{photo distance}}{\text{ground distance}}$

Therefore scope$=\frac{w}{RF}\times\frac{l}{RF}$

where w=width of the photograph
l=length of the photograph

Example:

For a K–3B photograph having an RF of $\frac{1}{12,000}$

$$\text{Scope}=\frac{7\ (12,000)}{12}\times\frac{9\ (12,000)}{12}$$

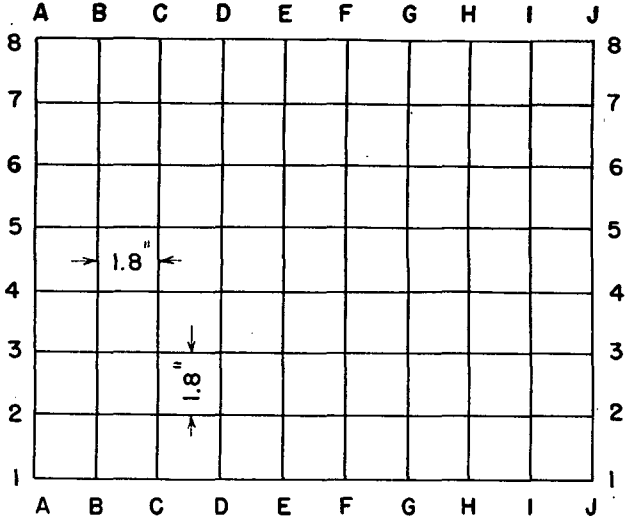
$$=7,000\times9,000 \text{ square feet}=2.26 \text{ square miles}$$

■ 98. GRAPHIC SCALE.—The preparation of a photograph for use as a map may include the construction of a graphic scale in yards or other appropriate units. When given, or having determined, the RF of the photograph, the graphic scale is constructed by the methods employed in constructing such scales for maps or sketches (see sec. II). On mounted photographs the scale so constructed should be placed on the lower margin of the mount, and if desired may extend entirely across the mount. On unmounted photographs, it should usually be placed on the back of the print in order not to obscure unnecessarily the detail on the face of the print. See paragraph 105 for the atlas grid.

■ 99. TO TRANSFER DETAIL OR CHANGE SCALE.—*a. By photography.*—Photographs may be enlarged or reduced by rephotographing when the necessary facilities are available. The resulting prints are usually not as good as the originals, and enlargements lose definition of detail.

b. By rectangular grid (fig. 84).—For average military purposes the detail of a vertical photograph may be roughly enlarged, reduced, or transferred by means of a special rectangular grid on the photograph. To transfer by this method at a changed scale proceed as follows:

(1) Fit a transparent overlay to the photograph and lay out on it a rectangular grid to a scale which is some fractional part of 1.8 inches (atlas grid, par. 105).



ENLARGEMENT
Scale 1:10,000

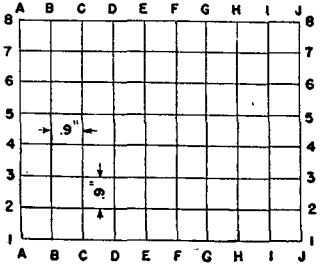


PHOTO
Scale 1:20,000

FIGURE 84.—Change of scale by rectangular grid method.

(2) Trace through on the overlay the topographical detail which it is desired to transfer.

(3) Lay out the atlas grid on a suitable sheet of paper at the new selected scale.

(4) Copy from the photograph overlay to the changed scale overlay (or map), square by square, the detail appearing therein in its proper relation to the square.

(5) For more accurate detail, construct a grid card for each scale. With these cards, important features may be much more accurately located.

Caution: It is to be understood that the above methods for changing scale merely result in copying or reproducing the detail as it appears on the photograph and in no sense should be considered as methods of rectification or elimination of inherent errors.

■ 100. DISTANCE.—Having determined the RF of a vertical photograph intended for use as a map and having constructed a graphical scale of yards for use on it, the photograph reader is ready to scale distances as required. The methods used in the measurement of horizontal distances on maps explained in section II or some elementary text, are also applicable to vertical photographs used as maps. It should suffice to state that the paper strip and graphic scale method is probably the most universal and satisfactory general method. The engineer's scale and the map measurer each serve in their respective fields of usefulness.

■ 101. DIRECTION.—*a.* It has been stated that in a vertical photograph which is of average rolling or fairly flat terrain and which has a small angle of tilt, the combined effect of errors over the center half of the photograph is entirely negligible for ordinary use as a map and is rarely prohibitive even in the marginal areas. Therefore, for normal military uses, direction angles and azimuths on a photograph have the same significance as they do on maps, and may be measured and laid out with the protractor exactly as is done with maps. The methods of measuring angles and directions on maps in section III apply.

b. In order to lay out or measure directions on a photograph with the facility with which this can be done on a map, it is obviously necessary to equip the photograph with

the magnetic north, true north, or grid north line. When practicable and desirable, all three of these are shown. Magnetic north, however, is the most suitable base direction for

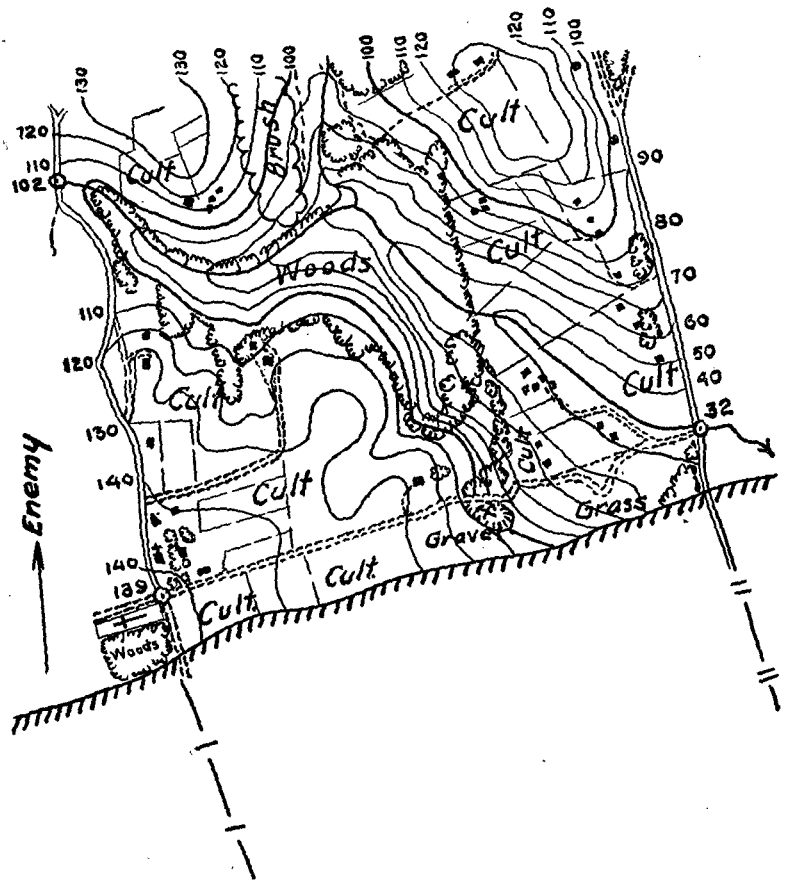


FIGURE 85.—Overlay of section of contoured aerial photograph.

photographs intended as substitutes for military maps and is the most available base direction for photographs of unmapped country. The magnetic north line may be traced

on the photograph negative with a stylus to print in black lines for reproduction in quantity.

■ 102. ELEVATION.—The determination of elevations by the use of a formula such as was developed in paragraph 73*b* is theoretically possible. The accuracy of results secured from the use of such a formula is dependent upon the accuracy of measurements on the face of the photographs, the reliability of corresponding map and ground positions, the determination of the lens height and elevation of the ground plumb point, and the assumption that the effect of tilt is negligible. Possible error introduced from these sources cannot be discounted in the evaluation of the character of the results. The most practical method of determining elevations is by trigonometric leveling. In order that elevations may be determined accurately direct from aerial photographs, photogrammetric equipment must be employed.

■ 103. CONTOURS.—*a.* In unusual situations it may be desired to contour a photograph in the field. This may be done by copying contours onto the photograph from an existing contoured map of the area, or by interpolating logical contours from selected spot elevations determined on the ground. Contouring should be done with the aid of a stereoscope.

b. To contour accurately an aerial photograph it is necessary to have numerous ground control points, and the drawing of the contour lines must be done with the aid of a stereo-comparagraph or some similar instrument. When these and other photogrammetric instruments are used, contouring is done by trained personnel. Engineer topographic organizations prepare accurate large-scale topographic maps, solely from photographs taken on planned flights over large areas upon which ground control has been established.

c. Ridge and streamlining may be accomplished in the field on a photograph or stereo-pair, as an aid to interpretation of relief. After this has been done, contouring may be accomplished as described in *a* above and then placed on an overlay (fig. 85).

■ 104. LOCATION OF MAGNETIC NORTH ON PHOTOGRAPH.—*a. When map showing magnetic north is available* (fig. 86).—Select two points identifiable both on the photograph and on the map and so located that the line joining them passes

through or near the center of the photograph. The direction of such a line will be little if at all affected by relief and tilt. By means of a protractor, determine from the map the magnetic azimuth of the line joining the points selected. From the corresponding line on the photograph, shown in figure 86 as *AB*, turn off counterclockwise an angle equal to the magnetic azimuth measured on the map to *AM*. This establishes on the photograph the magnetic base corresponding to that shown on the map.

b. By means of compass.—Orient the photograph by corresponding points on the photograph and on the ground.

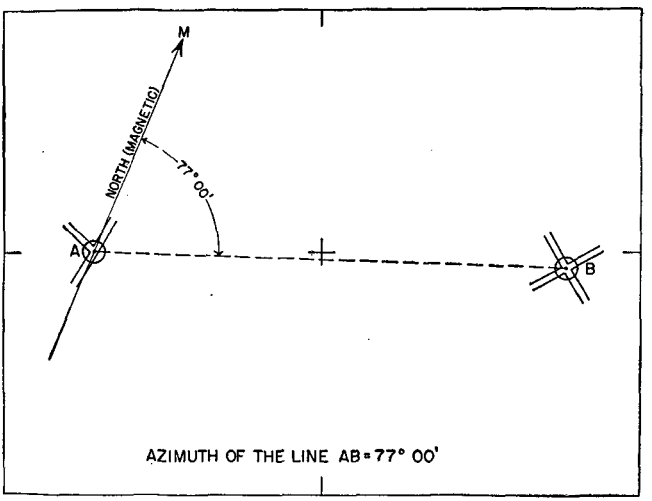


FIGURE 86.—Diagram showing method of locating magnetic north line on photograph.

Place a compass on the photograph and draw a line on the photograph parallel to the direction of magnetic north indicated by the compass needle.

■ 105. ATLAS GRID (fig. 87).—*a.* Because of variation in scale, other inaccuracies, and the difficulty of locating grid lines, the military grid is not used on single photographs or uncontrolled mosaics. Instead of the military grid, the atlas grid is used. The grid lines of the atlas grid are always 1.8 inches

apart regardless of the scale. With this interval, on a 1: 20,000 photo, the grid lines are about 1,000 yards apart. The lines are numbered from the bottom up and lettered from left to right. Thus the origin of the coordinates is at the lower left corner of the photo; numbers 1, 2, etc., upward; letters *A*, *B*, etc., to the right; the coordinates of the origin being (*A*.0—1.0).

b. To superimpose atlas grid on photograph.—In the process of reproduction, the edges of a photograph may vary

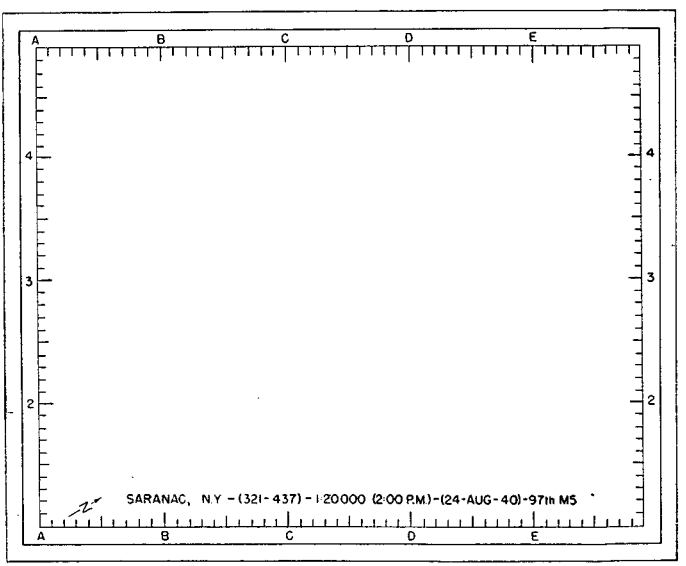


FIGURE 87.—Atlas grid and marginal data.

and successive prints may differ. In order to provide an accurate origin from which to measure, collimation marks are registered at the center of the four sides of a vertical photograph (par. 62*b*(1)(*b*)). To superimpose an accurate atlas grid on a photograph, the true edges must be established from the collimation marks, and the grid lines then spaced 1.8 inches apart beginning at the intersection of the true edges at the lower left corner of the photograph. Thus on a 9- by 9-inch print the true edges would be 4½ inches from

a line drawn between the opposite collimation marks, and the 1.8-inch grid would be laid off along these true edges. Figure 87 represents a 7- by 9-inch photograph which is not quite full size. If the photo were exactly 9 inches wide the *F*-coordinate line would exist. It must be borne in mind that the atlas grid has no definite limits as to the total area covered by it.

■ 106. MILITARY GRID.—*a. General.*—While the military grid is not used on single photographs or uncontrolled mosaics, it is highly desirable on controlled mosaics and photomaps made from them. Because of the inherent characteristics of mosaics, the military grid when superimposed upon them is only approximate. If a gridded map of the photographed area is available, the military grid may be transferred without difficulty to the mosaic by proceeding as follows:

(1) Three points, *A, B,* and *C* are selected on the photograph (fig. 86) which can be readily identified on the map. For greatest accuracy, the points selected should be well-spaced around the central area of the photograph.

(2) Determine the average scale of the photograph by the comparison of map and photograph distances as explained in paragraph 95. In this case the average scale is assumed to be

$$1 \text{ inch} = 434 \text{ yards or}$$

$$\text{RF} = \frac{1}{15{,}624}$$

(3) Determine the grid coordinates of *A, B,* and *C* from the map. These are as follows:

$$A = (1359.35\text{–}1789.52)$$
$$B = (1361.35\text{–}1790.16)$$
$$C = (1360.88\text{–}1788.00)$$

(4) To determine the position of the 1790 *X* (or east-west) grid line, determine the distance from the two points nearest that grid line.

In this case the distance from *A* to the 1790 grid line is 1,790,000—1,789,520=480 yards (measured north), and the distance from *B* to the 1790 grid line is 1,790,160—1,790,000= 160 yards (measured south).

Draw arcs from points *A* and *B*, respectively, as shown with these distances as radii.

FIGURE 88.—Method of superimposing military grid on aerial photograph or mosaic.

(5) To determine the position of the 1361 north-south grid line, determine its distance from two points, in this case *B* and *C*. The distance from *B* to the 1361 grid line is 635 yards measured west, and the distance from *C* to the 1361 grid line is 120 yards measured east.

Draw arcs from points *B* and *C*, respectively, as shown with these distances as radii.

(6) Draw the remaining grid lines parallel to the two already obtained at a distance corresponding to 1,000 yards on the photograph, or

$$\frac{1{,}000}{434}=2.3 \text{ inches}$$

(7) Number the grid lines properly and indicate the direction of magnetic north. Before inking, compare the photograph grid critically for any discrepancies which clearly cannot be attributed to relief or tilt displacements.

(8) Although three points, such as *A, B, C,* are preferable, two points, as *A* and *B,* would suffice for transferring the grid. In this case the procedure for establishing the grid base line is the same, but the 61 north-south grid line is established by drawing line 61 tangent to its arc about *B* (635 yards) and intersecting line 90 at right angles.

(9) The grid may be superimposed roughly by drawing the lines on the photograph through images which correspond to objects or features through which the grid lines on the map pass.

b. Reproduction.—To reproduce a gridded mosaic, in quantity, either draw the grid on the mosaic in black ink and then photograph it or else fit the film negative to the back of the photograph over an illuminated glass plate, carefully register it, cut the grid through the film coating with a stylus, and print from the original negative.

■ 107. ORIENTATION.—*a.* In the field, the photograph, when equipped with a graphic scale and magnetic north point, may be oriented according to the several methods prescribed for maps. All images on the oriented photograph are correct as to direction from a point near the center of the photograph, but serious discrepancies may exist in the outer portion of the photograph where great difference in relief exists. Therefore, use of the outer areas of the photograph should be

avoided where possible and resort made to an overlapping photograph which shows the area under consideration nearer to its center.

b. A rough means of determining north on certain photographs, which is not possible on maps, is by the use of shadows. At noon, in the Northern Hemisphere and out of the Tropics, the shadows will appear on the north side of the objects. The accuracy depends upon the proximity of the noon hour when the photograph was taken and the length of the shadow. For more details on the path of the sun, see paragraph 25.

■ 108. RESTITUTION.—It should be realized at this stage that vertical aerial photographs cannot be accurate maps in fact unless a variety of impossible or impracticable conditions is satisfied. These conditions would include perfectly level terrain, a perfectly level stationary camera platform, a mechanically perfect camera, and a perfect camera lens, film, print paper, and weather. It has been shown that good vertical photographs of terrain of small relief approximate the characteristics of a map. However, it is desirable that the photograph reader be able to use, either in conjunction with maps or as substitutes for maps, photographs which contain tilt or obliquity and relief. He should be able to plot the map positions of images recorded on such photographs and know how to transform the detail from the oblique to the horizontal when desired for correcting or posting existing maps. Restitution is the process of determining the true positions of objects the images of which appear distorted or displaced on aerial photographs. Some useful methods of restitution are described in the following paragraphs. Each method has its limitations. Some of those described do not correct displacements due to relief and serve only to rectify the photograph. More complete details using actual photographs are given in paragraphs 97 and 98, TM 5–230.

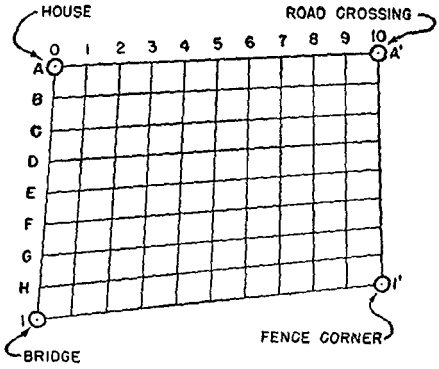
■ 109. RECTIFICATION OF AREAS BY GRID METHOD.—*a. Purpose.*—The grid method of enlarging, reducing, or reproducing an aerial photograph or map is described in paragraph 99. Homologous grids also may be employed as a rough expedient to rectify slightly tilted photographs. This method is not applicable to oblique photographs nor will it eliminate the effect of displacements of position caused by relief.

b. Procedure.—In order to rectify a photograph, select four well-distributed points, such as *A, A', I,* and *I'* in figure 89①, about the margin of the photograph which can be identified on a map. Crossroads, road junctions, important buildings, bridges, or other well-defined locations are suitable. Join the four points on both the photograph and the map by straight lines to form a four-sided homologous figure on each. Divide the opposite sides of the two figures into the same number of equal parts from ½ to 1 inch in length. Joining the divisions laid off, draw on both the photograph and on the map, grids which serve to subdivide the respective areas into the same number of small homologous figures. Finally copy in homologous relation the detail appearing in each grid subdivision of the photograph in the corresponding subdivision of the map.

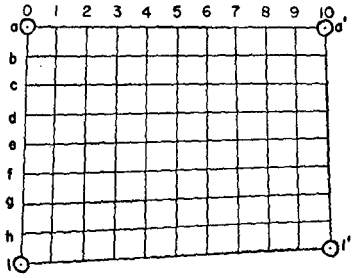
■ 110. RECTIFICATION OF AREAS BY TRIANGULAR DIVISION METHOD.—*a. Purpose.*—This method may be used to rectify either a tilted or an oblique photograph. It is based upon the theory that straight lines on the map appear as straight lines on the photograph. It will not eliminate the effect of displacements of position caused by relief.

b. Procedure.—(1) *When only four control points are available.*—Select four points, such as *A, B, C,* and *D* in figure 90, on the photograph which can be identified on the map and so distributed as to include the area under consideration. Join these points with straight lines to form a four-sided figure such that the opposite sides, when extended, will meet in points *F* and *G* at a convenient distance. If these points fall off the photograph, either they must be extended onto another piece of paper or an overlay of a large sheet of tracing paper must be used. Draw the diagonals *AC* and *BD*. Through their intersection *O* draw lines *FH* and *GI* from *F* and *G*, respectively. It may be observed that in addition to the four control points originally selected, there are now five more points on the photograph, *F, G, H, I,* and *O*, the map positions of which are fixed. The figure *ABCD* has been subdivided into four smaller four-sided figures. Draw diagonals in each of these and continue the process until the "controlled" subdivision of the area results in triangles of suitable size, usually of about ½-inch sides. Using the corresponding points *a, b, c,* and *d* on the map or on an overlay traced

from the map, proceed similarly to produce the same number of homologous triangles. Finally, copy in the triangles of the map figure the corresponding detail as it appears in homologous relation in the corresponding triangles of the photograph figure.



① PHOTOGRAPH



② MAP

FIGURE 89.—Grid method of restitution.

(2) *When more than four points of control are available.*— When more than four points of control are available the method is simpler and can be done in less space. On an overlay, trace from the map a large number of well-distributed control points, such as *a*, *b*, *c*, *d*, *e*, etc., in figure 91, which can

be identified readily on the photograph. Proceed to join by lines, these points as they appear on the map and the photograph, respectively, producing homologous figures. Using diagonals as necessary, carry the subdivisions further to pro-

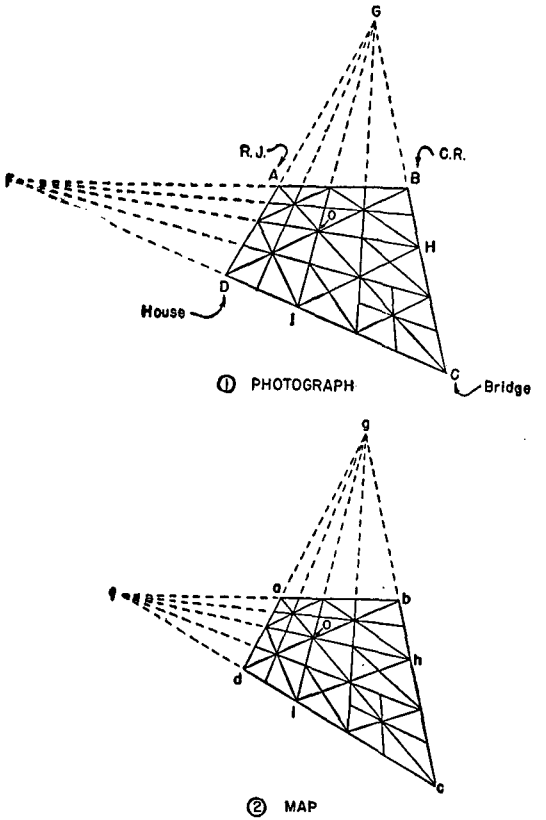
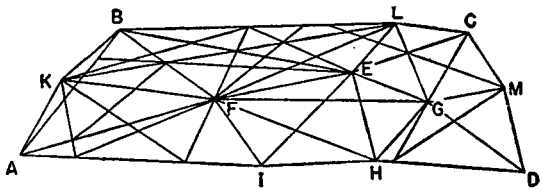


FIGURE 90.—Triangular division method of restitution with four control points.

duce triangles small enough for the desired accuracy without causing undue congestion. Proceed to copy the detail from the photograph triangles to the corresponding map triangles.

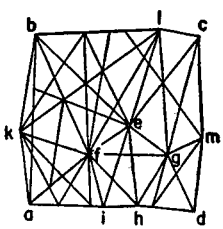
Figure 91 illustrates the mechanics of the method in its application to the rectification of an oblique photograph.

■ 111. LOCATION OF POINT BY TRACING PAPER METHOD OF RESECTION.—*a. Purpose.*—The method of resection by means of a piece of tracing paper may be used to plot roughly the map position of a limited number of points appearing on a vertical photograph.



OBLIQUE PHOTOGRAPH

To avoid congestion subdivisions not carried to smallest possible.



MAP

FIGURE 91.—Triangular division method of restitution where more than four control points are available.

b. Procedure (fig. 92).—Identify on the photo at least three points (preferably five) that appear on the map. Mark on a sheet of tracing paper the position of these points and of the point to be located on the map. This is done most readily by tacking the photograph over the tracing paper and with a pin pricking through each point. On the tracing paper,

draw rays from the point *P*, the location of which is desired, to each of the known points. Place the tracing paper on the map so that the ray to each of the known points passes through the map location of the corresponding point. The point, the location of which is desired, is then in its relative position to the known points. Its position may be pricked onto the map.

c. Limitations.—This method cannot be properly termed restitution because errors of tilt and relief in the photograph are in no way corrected unless the point, the location of which is desired, chances to fall, in their respective cases, either on the isocenter or the plumb point of the photograph. However, the error of location can sometimes be reduced by selecting more than the minimum of three known points. Thus five known points may be selected and it may not be possible to cause all five rays to pass through the respective map positions at one time. If four rays can be made to do so, the other ray may be deemed in error and disregarded.

■ 112. LOCATION OF POINT BY PAPER STRIP METHOD.—*a. Purpose.*—This method may be used to determine the map location of a few points on an aerial photograph. It may be employed with both tilted and oblique photographs. It will not eliminate the effect of displacements of position caused by relief. It is especially useful in bringing maps up to date by locating on the maps features which did not exist at the time that the area was surveyed. It is not necessary that the map and photograph be of the same scale.

b. Procedure (fig. 93).—Assume that it is desired to determine the map location of the cross road at *Y* and the house at *X*, respectively, on an aerial photograph.

(1) Select as control, four points readily identifiable on both the photograph and the map (*A, B, C, D*) and join them by lines as shown. In general the points, the locations of which are desired, should be within or near this quadrilateral.

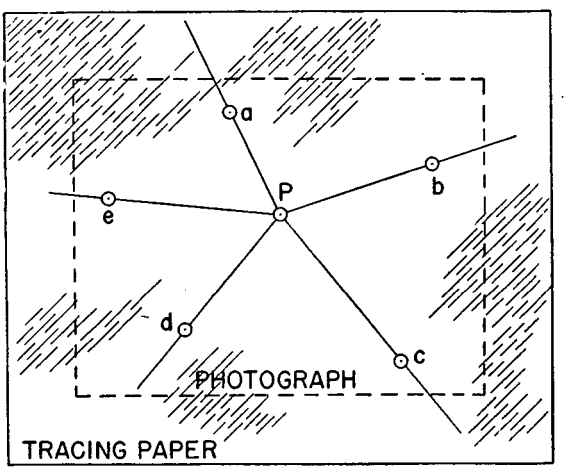
(2) Draw the diagonals *AC* and *BD*.

(3) From any two of the four control points on the photographs, as *A* and *C*, draw rays through the points *X* and *Y*. Select the ray centers to give good intersections at the desired points.

(4) Place a paper strip as in figure 93① and mark on the paper strip *e*, *f*, and *g* (points where the lines of the figure cross the strip) and *x* and *y* where the rays to *X* and *Y*, respectively, cross it.

(5) Place the paper strip as in figure 93② so that *e*, *f*, and *g* fall on their respective lines from *A*, and mark on the map the points *x* and *y* as determined by the marks on the paper strip.

(6) Draw rays on the map from *A* through *X* and *Y*.



①

FIGURE 92.—Location of point on map by tracing paper method of resection.

(7) Similarly place another strip on the reverse side of the paper over the photograph as in figure 93③, marking the position of the five rays from *C*.

(8) Place this second strip on the map as in figure 93④, mark on the map the points *x'* and *y'*, and draw the rays *Cx'* and *Cy'*. The intersections *X'* and *Y'* give the locations on the map of the points *X* and *Y* on the photograph.

■ 113. LOCATION OF POINT BY RADIAL LINE METHOD.—*a. Purpose.*—It will be recalled that in paragraph 75 it was stated that for practical purposes the combined effect of relief

and tilt in slightly tilted photographs is assumed to cause displacements along a radial line passing through the principal point (center) of the photograph. Use is made of this assumption to provide a method for determining accurately the map position of a point appearing in the overlap of two

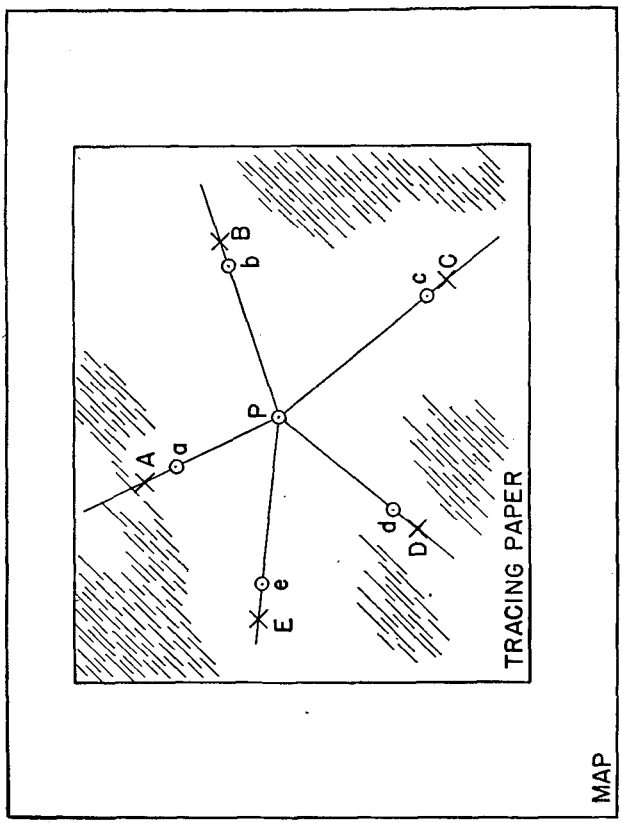


FIGURE 92.—Location of point on map by tracing paper method of resection—Continued.

aerial photographs taken at different camera positions. This method of restitution is the only one which will correct for both relief and tilt. When the tilt is small (3° or less) the assumption that displacements are radial along a line pass-

ing through the principal point is within the bounds of plotting accuracy. The method fails, however, in the presence of excessive tilt and cannot be used with oblique photographs. It is not necessary that the two photographs used are of the same scale. However, if the point sought falls on

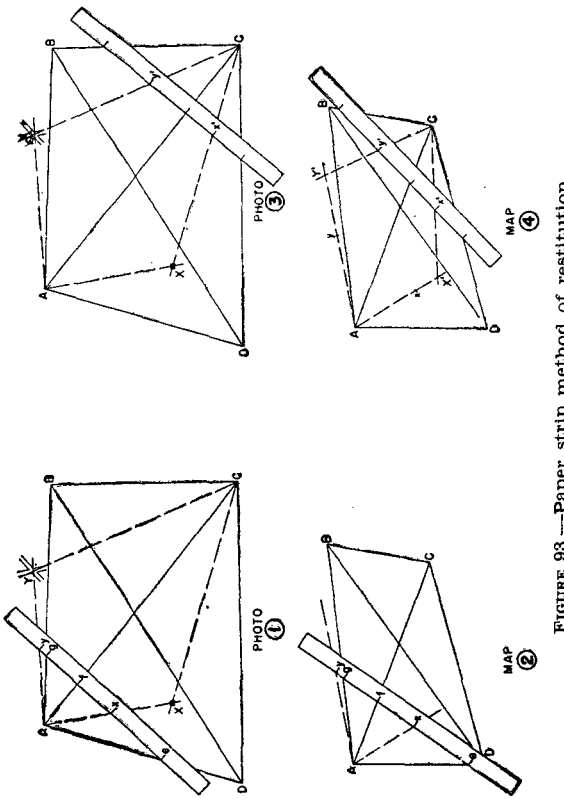


FIGURE 93.—Paper strip method of restitution.

or near the line joining the centers of the two photographs, the method fails because of the lack of a good angle of intersection.

b. Procedure (fig. 94).—Let it be assumed that it is desired to locate on a map an object *A* which appears on two overlapping vertical photographs. Proceed as follows:

(1) Identify on the map and on each of the two photographs, three points which will serve to orient the photograph with respect to the map. A different set of points may be selected for each photograph or the same identical points, as *X*, *Y*, and *Z* shown in figure 94①. The points selected should be well out from the center of each photograph and so distributed that the rays drawn from them to the center of each photograph provide good three-point resection. Points grouped too closely cause acute intersection angles between the rays drawn to the center of the photograph and make accurate work difficult.

(2) Inclose the three points selected on the photograph and the map in small triangles. Inclose the object *A* to be located on the map in a small circle on each photograph.

(3) Place a piece of vellum over the map and mark on the vellum the map positions of the points *X*, *Y*, and *Z* (fig. 94①).

(4) Locate on each photograph (marked Nos. 1 and 2) the principal point (center) and mark this with a cross C_1 and C_2, respectively. Draw rays from the photograph positions of *X*, marked X_1 and X_2, respectively, *Y*, *Z*, and *A* to C_1 and C_2, respectively (fig. 94② and ③).

(5) Place the vellum over photograph No. 1 and orient it so that the points *X*, *Y*, and *Z* marked on the vellum will fall on the rays drawn on the photograph through the images of those points (X_1, Y_1, and Z_1). Trace on the vellum the ray drawn through the object A_1 (fig. 94④).

NOTE.—In doing this we have in effect located on the vellum by resection the position of C_1 and the direction of the position of *A* with respect to C_1. Any displacement of A_1 due to relief or tilt is radial along this line.

(6) Next place the vellum over photograph No. 2 and orient it so that the points *X*, *Y*, and *Z* marked on the vellum again will fall on the rays drawn on the photograph through the images of those points X_2, Y_2, and Z_2. Trace on the vellum the ray drawn through the object A_2 (fig. 94⑤).

(7) The intersection of the two rays through the objects A_1 and A_2, respectively, as traced on the vellum, plots the position of *A* to the scale of the map. The vellum may again be placed over the map and oriented so that the positions of points *X*, *Y*, and *Z* on the vellum and on the map are superimposed one above the other (fig. 94⑥). The position of *A* may then be pricked onto the map.

■ 114. RECTIFICATION BY PHOTOGRAPHY (fig. 95).—By means of the Air Corps transforming printer, tilted and oblique photographs may be projected through the required angle so as to bring the photograph into a horizontal or any desired plane.

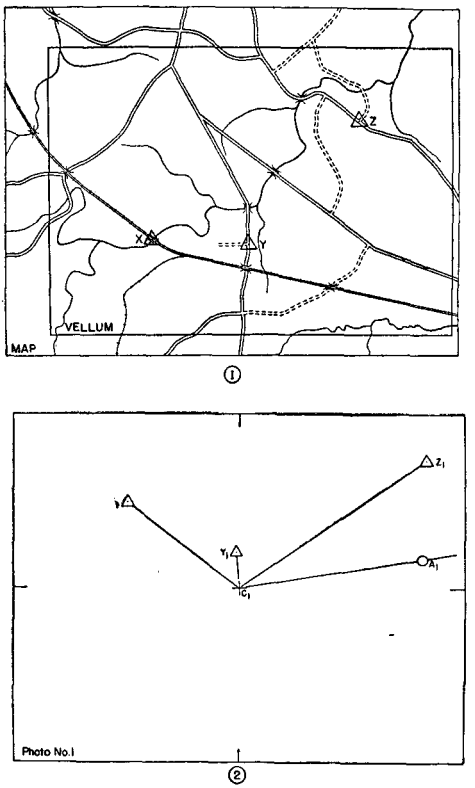


FIGURE 94.—Radial line method of restitution.

This process of rectification of the photograph does not correct for the effects of relief. As previously stated, during the transformation, images lose definition to a varying degree depending upon the amount of enlarging.

SECTION XI

PHOTOMAPS

■ **115. GENERAL.**—A photomap is a single photograph, composite, or mosaic which has been prepared by the addition of grid, marginal and place-name data, and produced in quan-

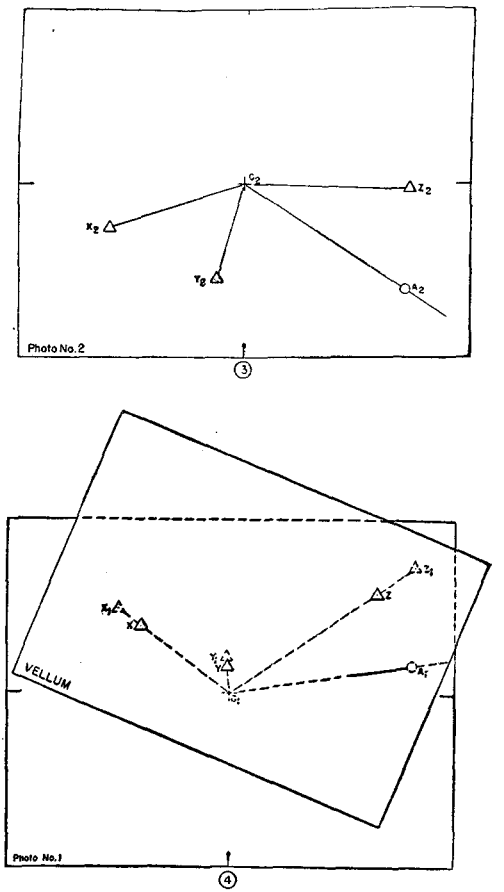


FIGURE 94.—Radial line method of restitution—Continued.

tity by contact printing or lithography. When time for preparation and available information permit, these data will be in the same form and as complete as for standard maps.

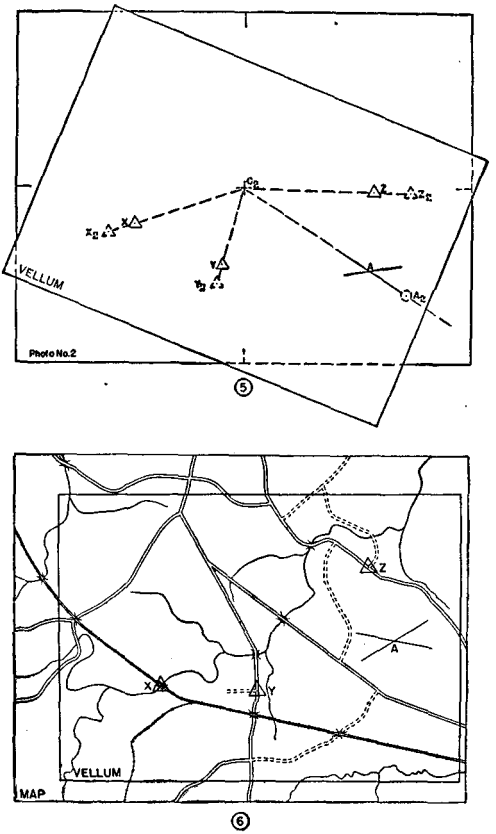


FIGURE 94.—Radial line method of restitution—Continued.

Since the photomap, however, finds its greatest use in providing information quickly, quite frequently much of the data usually found on a map will be missing.

■ 116. TYPES OF PHOTOMAPS.—The types of photomaps most frequently encountered are as follows:

a. Reproduced single lens photographs.—These photographs may be either verticals or obliques (fig. 96) and may be prepared by lithography or by contact printing, at the same scale as taken or by enlargement or reduction. Because of the wide area coverage, the T–5 (wide angle) photograph, print size 9 by 9 inches, provides an excellent source for the preparation of a hasty photomap. Normally the photograph will be taken at 20,000 feet above ground level (scale 1/40,000) and will be enlarged to 1/20,000.

b. Reproduced composites (fig. 97).—The tandem T–3A composite, utilized extensively for mapping photography, is

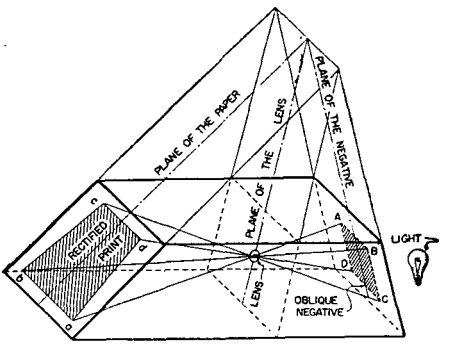


FIGURE 95.—Diagram of transforming printer.

frequently converted to a photomap by enlargement and reproduction of the center or "heart." As a rule, a square section of the center of the composite, measuring about 9 by 9 inches, is used.

c. Reproduced mosaics (fig. 98).—The usual form of photomap is prepared by reproduction of a controlled or uncontrolled mosaic, constructed as indicated in paragraph 65. This type of photomap may be made up in as many sheets as required to cover a given area, providing continuity between adjacent sheets in the same manner as a series of map sheets.

■ 117. MARGINAL DATA.—Marginal data for the reproduced individual photograph will be that given in paragraph 77.

FIGURE 96.—Single oblique used as photomap.

Photomaps which are made from mosaics and certain wide coverage photographs may have, in addition, the following information:

a. Marginal information similar to that shown on maps, such as the graphic scale in yards.

b. Some system of grids, usually the atlas grid described photograph figure.

FIGURE 97.—Tandem T–3A composite.

c. Names of towns, streams, mountains, highways, and other important features.

■ 118. CARE IN USE OF PHOTOMAPS.—Photomap users will make their own estimates of the reliability of the information portrayed by examination of the marginal information and by consideration of the basic materials used in their preparation. The date of the aerial photography gives an indication

FIGURE 98.—Reproduced mosaic.

of the probable accuracy of portrayal of cultural features as they now exist. If the photomap is a simple reproduction of a single photograph or composite, it will be understood that the indicated scale is approximate and that over-all scale errors due to tilt and relief displacements will exist. Photomaps from mosaics will be indicated as "controlled" or "uncontrolled." Photomaps made from uncontrolled mosaics are important primarily because of their pictorial value, and should not be considered as accurate for the determination of distances and directions. If the area is relatively flat and the photographs have been taken at fairly constant elevation with little tilt, even the uncontrolled mosaic will approach the dimensional and directional accuracy of the best maps. A photomap from a controlled mosaic may be accepted as reasonably accurate for measurement of distances and directions, despite the fact that image displacements at the junctions of the individual prints will be apparent. When the photomap has been prepared from a mosaic of high accuracy, as explained in paragraph 65*b*, the legend will so state. Such photomaps may be accepted with the same degree of confidence as a first class planimetric map of the same scale.

■ 119. AIDS IN USE OF PHOTOMAPS.—Photomaps reproduced in quantity by photolithography lose some of the clarity, sharpness, and contrast of the original copy. Even in poor reproductions, however, the principal features of the terrain can be discerned by careful study and through the application of general knowledge of terrain characteristics. It will assist the map reader considerably to trace out the drainage system, accentuating the stream lines with a sharp blue pencil, avoiding, at the same time, the obliteration of essential details. In the same manner, the permanent ridge lines may be traced in brown lines, thus enabling the map reader to grasp at a glance the major features of the terrain.

■ 120. METHODS OF REPRODUCTION.—Photomaps are reproduced in quantity by contact printing, by continuous tone lithography, or by halftone lithography. The contact process produces the best results, but is much more expensive and time consuming than lithography. Furthermore, rapid contact printing of large size photomaps requires equipment which is too bulky for field use. In the continuous tone

lithographic process, much of the contrast of tone which appears in the original photograph or mosaic is lost. As a result, many small features become merged into the background and are difficult or impossible to discern. When the original photography has been satisfactory, the best results in quantity reproduction are obtained by halftone photolithography. Reading glass examination of a photomap reproduced by this process, will disclose that the individual images are made up of a series of dots, the darker the object, the denser the dots. Most of the original tone contrast of the photograph is retained. However, in the halftone process also, some details of the landscape such as individual bushes, small houses, etc., may be too small to create a sufficiently distinct dot pattern to render them recognizable. Another feature to be observed in the study of photomaps from mosaics is the changes in tone and contrast between the adjacent sections of the separate photographs used in the preparation of the mosaic. Because of changes in exposure conditions, as well as variations in printing of individual photographs, marked differences in the tone of adjacent sections of the mosaic frequently occur. Such differences in tone should be recognized readily and should not be misinterpreted as actual changes in landscape texture.

INDEX

	Paragraph	Page
Aerial photographs:		
Atlas grid	105	159
Care	71	101
Compared to map	61	87
Contours	103	158
Conversion to map	69	99
Definition	61	87
Direction	101	156
Distance	100	156
Elevation	102	158
Identification	76, 79	113, 114
Index and plot	70	100
Interpretation	76	113
Military features	87	127
Military grid	106	161
Orientation	78, 107	114, 163
Pin points	63	95
Relative size of objects	81	114
Relief	75, 88, 89	110, 127, 129
Reproduced	116	177
Scale	95, 96	148, 149
Change	99	154
Graphic	98	154
Scope	97	153
Season, effect	85	120
Shadow	83	116
Shape of objects	80	114
Strips	64	95
Texture of ground surface, effects	82	115
Tilted	73–75, 93	102, 147
Tone	82	115
Topographical features	86	120
Tracing	69	99
Training	6	5
Types and characteristics	62	88
Altitude related to photograph scale	62	88
Anaglyph	89	129
Anaglyphoscope	89	129
Angles:		
Direction	16	20
Measurement	17, 24	20, 26
Annual change	18, 19	20, 22
Area:		
Defiladed	58	79
Mapped in United States	61	87
Atlas grid	105	159
Axis of earth	4	1
Azimuth	20, 21	24
Determination	37	57

	Paragraph	Page
Back azimuth	21	24
Base directions	18	20
Bearings	20, 21	24
Bleaching	69	99
Cameras, types for aerial photographs	62	88
Cassiopeia	25	28
Change, annual	18, 19	20, 22
Charts, navigation	4, 41	1, 62
Coast and Geodetic Survey charts	9	9
Collimation marks	62, 105	88, 159
Color-layer system (relief)	41	62
Color maps	6, 7	5, 7
Compass, magnetic	22	25
Composites	62	88
Reproduced	116	177
Concealment	58	79
Contoured maps, training	6	5
Contours:		
Approximate	46	69
Characteristics	42	65
Definition	41	62
Depth curves	41	62
Interval, defined	43	66
Logical	47	69
Marginal data	8	8
On aerial photograph	103	158
Controlled mosaics	65	95
Conventional signs	7	7
Relief	41	62
Conversion factors, angles	17	20
Coordinates	29	41
Determination	37	57
Geographical	32	45
Grid	33	47
Polar	30	42
Rectangular	31	43
Spherical	32	45
Crest, military and topographical	58	79
Curvature of earth	60	85
Declination, grid and magnetic	19	22
Deflade	58	79
Degree (angular measure)	17	20
Departure	18	20
Depth curves	41	62
Designation, directional	18	20
Dipper, Big	25	28
Direction:		
Angular measurement	20	24
Base	18	20
Determination by field expedients	25	28
Determination of unknown	37	57
Expression	16	20
On aerial photograph	101	156
Distance	10	10
Determination of unknown	37	57
On aerial photograph	100	156

	Paragraph	Page
Earth:		
Curvature	60	85
Size and shape	4	1
Elevation	39	61
Determination from contours	48	71
Of important features	44	67
On aerial photographs	102	158
Engineer's scale	12, 32, 33	11, 45, 47
Equator	4	1
Field expedients for determination of direction	25	28
Flight line spacing	62	88
Focal length of cameras	62	88
Foliage	58	79
General Land Office maps	9	9
Geographic:		
Coordinates	32	45
Grid	8, 32	8, 45
Index	8	8
Gisement	19	22
Graphic scale:		
Construction	14	15
Marginal data	8	8
Grid:		
Atlas	105	159
Geographic	8, 32	8, 45
Meridian	8	8
Method of rectification	109	164
Military	8, 34, 106	8, 50, 161
Construction	38	60
North	18, 19	20, 22
Rectangular	34	50
Change scale by	99	154
System	34	50
Continental	35	55
Equatorial	36	56
To superimpose on map	37	57
Zones	34, 35	50, 55
Ground forms	40	61
Hachures	41	62
Height:		
Lens	96, 97	149, 153
Related to scale of photograph	62	88
Hemisphere	4, 34	1, 50
Identification, photograph	76	113
Of objects on photographs	79	114
Index:		
Adjoining map	8	8
Geographic	8	8
Of aerial photographs	70	100
International Boundary Commission: United States and Canada (maps)	9	9

	Paragraph	Page
Interpretation, aerial photographs	76	113
Isogonic lines	19	22
Lake survey charts	9	9
Latitude	4, 32	1, 45
Lens height	96, 97	149, 153
Lensatic compass	22	25
Lettering	7	7
Linear measure	10	10
Lines:		
Contour	41	62
Form	46	69
Isogonic	19	22
Master	40	61
Ridge and stream	40	61
Local magnetic attraction	23	26
Location:		
Distant point	27	39
One's position	26	32
Longitude	4, 32	1, 45
Magnetic:		
Attraction, local	23	26
Azimuth	21	24
Field	23	26
Meridian	8, 18	8, 20
North	18, 19, 24	20, 22, 26
Map:		
Battle	5	4
Classification	5	4
Compared to aerial photograph	61	87
Definition	3	1
Marginal information	8	8
Measurer	12	11
Military use	6	5
Orientation	26	32
Scales	11	11
Titles	8	8
Topographic	5	4
Training with	6	5
Types	5	4
Used in training	6	5
Map substitute	94	148
Scale	95	148
March scale (time-distance)	15	18
Marginal information	8	8
Aerial photograph	77	113
Photomap	117	177
Mask	58	79
Measure:		
Angular	17	20
Linear	10	10
Measurer, map	12	11
Meridian	4	1
Central	19, 35	22, 55
Mil (angular measure)	17	20

	Paragraph	Page
Military:		
Crest	58	79
Features on aerial photographs	87	127
Grid	8, 106	8, 161
Minute (angular measure)	17	20
Mosaics	65	95
Reproduced	116	177
Multiple-lens camera	62	88
Navigation charts	4, 41	1, 62
North:		
Grid	18, 19	20, 22
Magnetic	18, 19	20, 22
Location on aerial photograph	104	158
On aerial photograph	101	156
Star	25	28
True	18, 19	20, 22
Obliques	62	88
Rectification by photography	114	174
Orientation	26	32
Aerial photographs	78, 107	114, 163
Distant point	27	39
Maps	26	32
Methods	26	32
One's position	26	32
Overlays	68	98
Paper, print	66	98
Parallel of latitude	4	1
Perception, stereoscopic	89	129
Photogrammetric instruments	103	158
Photograph. (*See* Aerial photographs.)		
Photography	84	120
Rectification by	114	174
Photomap:		
Aids in use	119	181
Care in use	118	179
Definition	115	175
Marginal data	117	177
Reproduction	120	181
Training with	6	5
Types	116	177
Picture points	67	98
Pin points	63	95
Plain verticals (photograph)	62	88
Plumb line, direction with	25	28
Point:		
Picture	67	98
Pin	63	95
Polar coordinates	30	42
Polaris	25	28
Polaroid anaglyph	89	129
Poles:		
Magnetic	19	22
North and South	4	1
Position, location on map	26	32
Post route maps	9	9
Print paper	66	98
Prismatic compass	22	25

	Paragraph	Page
Profile	57	77
Definition and construction	57	77
Exaggeration	57	77
From contours	57	77
Hasty	58	79
Method of visibility	58	79
Projection	4	1
Classification	4	1
Definition	4	1
Mercator's	4	1
Polyconic	4	1
Protractor	24	26
Pseudoscopic effect	93	147
RF. (*See* Representatives fraction.)		
Radial line, restitution	113	170
Rectangular:		
Coordinates	31	43
Grid	34	50
Protractor, use	24	26
Rectification:		
Aerial photographs	109, 110	164, 165
By photography	114	174
Refraction of light	60	85
Relief	40	61
Aerial photographs	75, 88, 89	107, 127, 129
Interpretation	45	67
Stereo effect	73	102
Representative fraction (RF)	8	8
Determination of scale with	14, 96	15, 149
Use with engineer's scale	12	11
Use with map measurer	12	11
Reproduction (photograph)	106, 116, 120	161, 177, 181
Resection, location of point	111	168
Restitution	108	164
Paper strip method	112	169
Scale	11	11
Aerial photograph	95, 96	148, 149
Change	99	154
Graphic	98	154
Area and distance relation	13	15
Coordinate	33	47
Definition	11	11
Determination, map	14	15
Engineer's	12, 32, 33	11, 45, 47
Graphic	12	11
Construction	14	15
Marginal data	8	8
Standard map	5	4
Time-distance	15	18
Sea level	4, 39	1, 61
Season, effect of	85	120

	Paragraph	Page
Seconds (angular measure)	17	20
Shadow (in photographs)	78, 79, 93	114, 147
Shapes of objects	80	114
Signs, conventional	7	7
For relief	41	62
Size, relative on photographs	81	114
Slope:		
Average	56	77
Between two points	54	75
Conversion of units	55	76
Definition and expression	49	73
Degrees	52	75
Gradient	53	75
Mils	51	73
Percent	50	73
Soil survey maps	9	9
Sources of error (photograph)	72	101
Spherical coordinates	32	45
Standard maps	5	4
Stereo:		
Effects, faulty	93	147
Effects of relief	73	102
Examination	89, 92	129, 143
Fusion	89	129
Pair	89	129
Triplet	89	129
Stereo-comparagraph	103	158
Stereogram	89	129
Stereoscopes	91	133
Contouring with	103	158
Strips, photographic	64	95
Sun, direction by	25	28
Symbols	7	7
Not used on map	8	8
Relief	41	62
T-type camera	62	88
Tactical interpretation, aerial photographs	76	113
Terrain	40	61
Master lines	40	61
Texture (aerial photographs)	82	115
Tilted photographs	93	147
Effect	74, 75	107, 110
Time-distance scales	15	18
Tone (aerial photographs)	82	115
Topographic—		
Crest	58	79
Features (aerial photographs)	86	120
Identification (aerial photographs)	76	113
Maps	5	4
Traverse	28	40
Truth azimuth	21	24
Meridian	8, 18	8, 20
North	18, 19	20, 22

	Paragraph	Page
Uncontrolled mosaics	65	95
Ursa Major (Big Dipper)	25	28
United States Forest Service maps	9	9
Vertical:		
Composite	62	88
Datum	8	8
Interval, contours	43	66
Photograph	62	88
Visibility	58	79
Diagram	59	84
Vision, stereo	89	129
Watch, to find direction	25	28
Watch compass	22	25
X-coordinates, origin	34	50
X-lines	33	47
Y-coordinates, origin	34	50
Y-lines	19, 33	22, 47
Application in problem	24	26

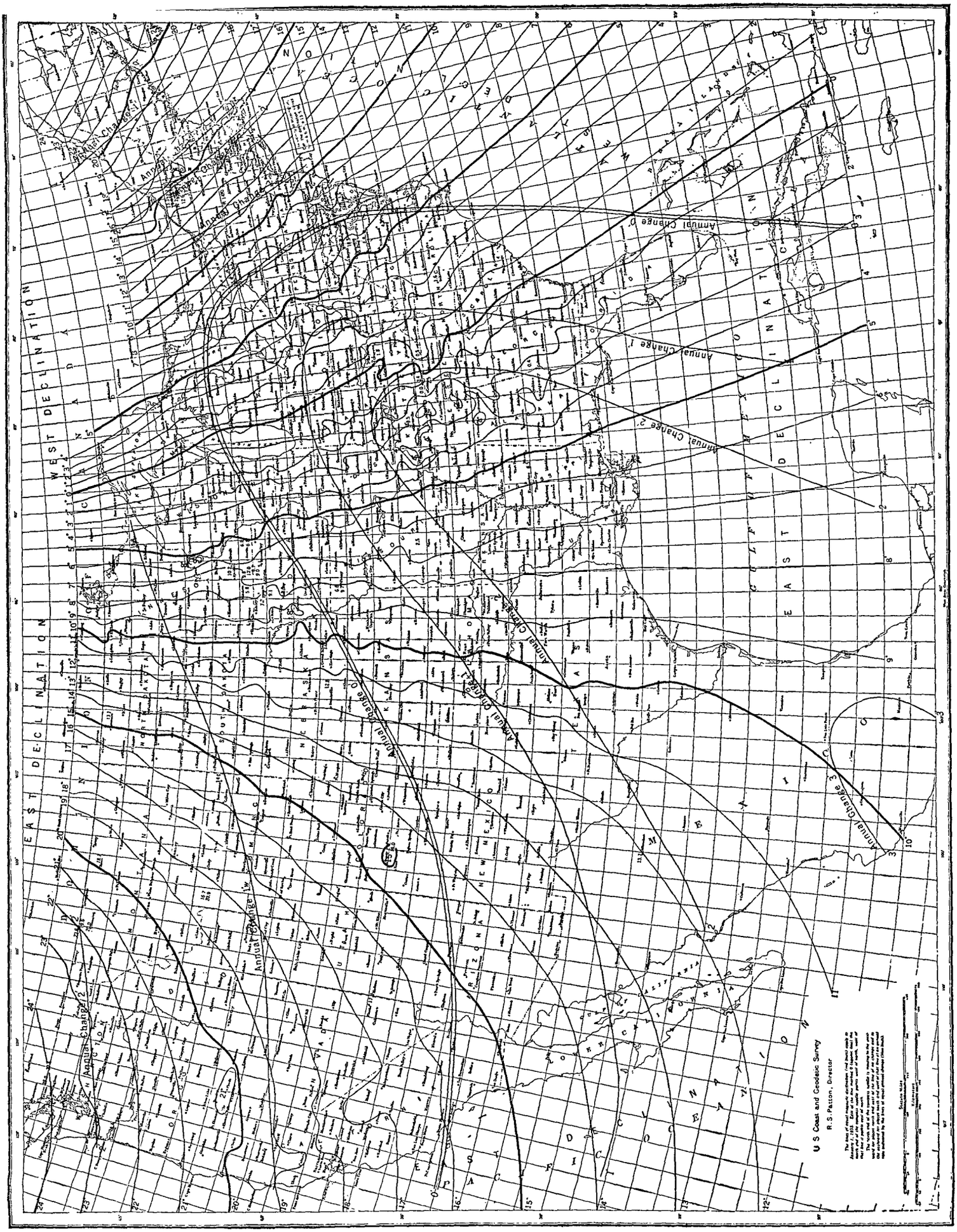


FIGURE 9.—Lines of equal magnetic declination and of equal annual change in United States for 1935.

406669°—41. (Fol. p. 190.)

MHI
Copy 3
COPY
Superseded by
27 Mar 72

FM 30-10

DEPARTMENT OF THE ARMY FIELD MANUAL

TERRAIN INTELLIGENCE

PROPERTY OF
QUARTERMASTER SCHOOL LIBRARY
U. S. ARMY QUARTERMASTER SCHOOL
FORT LEE, VA. 23801

LOGISTICS LIBRARY BR, ALMC

HEADQUARTERS, DEPARTMENT OF THE ARMY
OCTOBER 1967

FIELD MANUAL
No. 30–10

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, D.C., *24 October 1967*

TERRAIN INTELLIGENCE

CHAPTER 1.	INTRODUCTION		1–3	3
2.	CONCEPTS AND RESPONSIBILITIES			
Section I.	Nature of terrain intelligence		4–7	4
II.	Responsibilities		8–11	5
CHAPTER 3.	PRODUCTION OF TERRAIN INTELLIGENCE			
Section I.	Intelligence cycle		12–16	7
II.	Sources and agencies		17–23	8
CHAPTER 4.	WEATHER AND CLIMATE			
Section I.	Weather		24–39	13
II.	Climate		40–47	28
III.	Operations in extreme climates		48–50	35
CHAPTER 5.	NATURAL TERRAIN FEATURES			
Section I.	Significance		51, 52	44
II.	Landforms		53–61	45
III.	Drainage		62–69	64
IV.	Nearshore oceanography		70–75	73
V.	Surface materials		76–81	80
VI.	Vegetation		82–91	84
CHAPTER 6.	MANMADE TERRAIN FEATURES			
Section I.	Significance		92, 93	93
II.	Lines of communication		94–103	93
III.	Petroleum and natural gas		104–108	100
IV.	Mines, quarries, and pits		109–112	102
V.	Airfields		113–115	105
VI.	Water terminals		116–118	107
VII.	Hydraulic structures		119–121	109
VIII.	Urban areas and buildings		122–128	112
IX.	Nonurban areas		129–131	117
CHAPTER 7.	MILITARY ASPECTS OF THE TERRAIN			
Section I.	Military use of terrain		132–139	120
Ii.	Special operations		140, 141	126
III.	Water supply		142–147	127
CHAPTER 8.	TERRAIN STUDIES			
Section I.	Basic features		148–153	132
II.	Terrain and climate		154–156	134
III.	Military aspects		157–166	137
IV.	Coastal hydrography		167, 168	139
CHAPTER 9.	TRAFFICABILITY		169–178	142
APPENDIX A.	REFERENCES			148
B.	OUTLINE FOR TERRAIN STUDIES			150
C.	SAMPLE TERRAIN STUDY			153
D.	SAMPLE CLIMATIC STUDY			161
E.	NATURAL TERRAIN FEATURES			170
F.	DEPARTMENT OF DEFENSE INTELLIGENCE INFORMATION REPORT FORMS 1396 AND 1396C			171
INDEX				173

*This manual supersedes FM 30–10, 28 October 1959.

CHAPTER 1

INTRODUCTION

1. Purpose and Scope

a. This manual serves as a guide in the production and use of terrain intelligence. It shows how terrain and weather are evaluated in military planning and how terrain influences combat. The manual also serves as a guide in understanding the purpose, scope, limitations, and applications of terrain analysis. The manual provides information concerning the acquisition and use of terrain intelligence at unit level in a theater of operations.

b. This manual covers basic characteristics of the natural and manmade features of an area and their effect on military operations. It defines terrain intelligence and explains the intelligence process of collection, evaluation, interpretation of information, and dissemination of the finished intelligence. It discusses some of the sources of terrain information, including their relative value and use. Guidance is furnished for the preparation of the terrain study. The material presented herein is applicable to both nuclear and nonnuclear warfare.

2. Changes and Comments

Users of this manual are encouraged to submit recommended changes or comments to improve it. Comments should be keyed to the specific page, paragraph, and line of the text in which the change is recommended. Reasons should be provided for each comment to insure understanding and complete evaluation. Comments should be forwarded to the Commandant, U.S. Army Engineer School, Fort Belvoir, Va., 22060.

3. Relation to Other Manuals

The material presented in this manual is related to material in FM 5–30, FM 30–5, and TM 5–545. Other manuals of the FM 30- series cover specialized intelligence activities. FM 100–5, FM 100–15, and FM 101–5 cover intelligence in general staff activities and in the plans and operations of large units. Field manuals of the 5-series contain detailed information on the operation of engineer troop units and their intelligence functions.

CHAPTER 2

CONCEPTS AND RESPONSIBILITIES

Section I. NATURE OF TERRAIN INTELLIGENCE

4. Definitions

a. Terrain is part of the surface of the earth, including natural and manmade features. Both its natural and manmade features affect military operations.

b. Terrain intelligence is processed information on the military significance of the natural and manmade characteristics of an area.

c. Terrain analysis is the process of interpreting a geographical area to determine the effect of the natural and manmade features on military operations. It includes the influence of weather and climate on those features.

d. A terrain study is an analysis and interpretation of natural and manmade features of an area, their effects on military operations, and the effects of weather and climate on these features.

e. A terrain estimate is that portion of an analysis of the area of operations concerned with the military aspects of the terrain, and the effects of the characteristics of terrain on enemy and friendly courses of action, including the possible use of nuclear weapons.

5. Purpose

The purpose of terrain intelligence is to obtain data about the terrain, weather, and climate, thereby assisting the commander in making decisions and the troops in attaining their missions. In planning an operation, the commander and his staff analyze the effects that the terrain and weather conditions will have upon the activities of both friendly and enemy forces. The commander must make the most effective use of the terrain assigned to his unit. If he is furnished with adequate terrain intelligence, he will be able to exploit the advantages of the terrain and avoid or minimize its unfavorable aspects. By the proper utilization of terrain, a numerically inferior force may achieve combat superiority over a larger enemy force. The compilation of terrain intelligence is not limited to enemy areas. It also covers the area occupied by the friendly force and also the adjacent terrain.

6. Classifications

a. Mission. Terrain intelligence is classified according to the mission and level of the command at which it is used. These categories are considered broadly as strategic and tactical or operational. Terrain intelligence is one element in the intelligence requirements of a commander. Engineers have considerable interest in terrain because they are trained and equipped to make terrain studies and to conduct field reconnaissance.

b. Strategic. Strategic terrain intelligence is concerned with large-scale plans and may include the military capabilities of nations. Strategic intelligence is produced continuously and requires the compilation and interpretation of information by highly specialized personnel. Included in strategic intelligence are descriptions and analyses of beaches, water terminals, inland waterways, urban areas, and major terrain features; transportation and communication systems; soils, rock types, underground installations, climate and weather, vegetation, state of ground, and hydrography.

c. Operational. Operational terrain intelligence is produced for use in planning and conducting tactical or other operations. It is based upon information secured locally or provided by higher headquarters and is concerned pri-

marily with the effects of weather and terrain upon the particular operations of the unit. Route reconnaissance reports are of greatest importance in providing current information about routes of communication.

d. Objectives. The difference in the type of terrain intelligence required by strategic and tactical planners reflects their objectives. The strategic planner may consider an entire country or continent, while the tactical planner is concerned only with the terrain in the area of his operations. Where the strategic planner often studies problems that may arise some years ahead and applies terrain intelligence in a wide variety of hypothetical situations, the tactical planner is primarily engaged with problems that currently involve his unit, although he will study the terrain in his entire area of possible operation.

7. Applications

a. Planning. Terrain intelligence is essential to the commander in order to plan strategic and tactical operations. Detailed and reliable terrain intelligence is required for all logistical plans, particularly those prepared for special operations or for operations under extremes of climate. Special studies, prepared from a logistical viewpoint, are essential in planning operations in mountains, jungles, or deserts, in snow and extreme cold, and for airborne and amphibious operations.

b. Problems. Research and development agencies are concerned with the problems resulting from adverse climate, weather, and terrain. Terrain intelligence is necessary to determine the requirements for new means of transportation, types of shelter and construction, weapons, and clothing. It is a basic requirement in the development of new equipment and in the maintenance and modification of existing equipment.

c. Needs. Current and accurate terrain intelligence is required by topographic engineer agencies for use in preparing or revising military maps. Civil Affairs operations depend on accurate terrain intelligence, particularly concerning matters of economic and political impact on tactics and logistics.

Section II. RESPONSIBILITIES

8. Department of Defense

a. Defense Intelligence Agency (DIA). The Defense Intelligence Agency (DIA) is an agency of the Department of Defense (DOD) and under the direction, authority, and control of the Secretary of Defense. It is administered by a director, a deputy director and a chief of staff at the headquarters which has such subordinate units, facilities, and activities as are specifically assigned to the Agency by the Secretary of Defense or by the Joint Chiefs of Staff acting under the authority and direction of the Secretary of Defense. DIA is responsible for—

(1) The organization, direction, management, and control of all DOD intelligence resources assigned to or included within DIA.

(2) Review and coordination of those DOD intelligence functions retained by or assigned to the military departments. Overall guidance for the conduct and management of such functions is subject to review, approval, and promulgation by the Secretary of Defense.

(3) Obtaining the maximum economy and efficiency in the allocation and management of DOD intelligence resources. This includes analysis of those DOD intelligence activities and facilities which can be fully integrated or collocated with non-DOD intelligence organizations.

(4) Responding directly to priority requests levied upon the DIA by the United States Intelligence Board (USIB) and satisfying the intelligence requirements of the major components of the DOD.

b. Assistant Chief of Staff for Intelligence (ACSI). The Under Secretary of the Army is the DA's responsible officer for its intelligence, counterintelligence, and communications security in international affairs. The intelligence and counterintelligence activities of the United

States Army are the responsibility of the Assistant Chief of Staff for Intelligence (ACSI). His duties include directing the Army mapping and geodesy program and the military geographic intelligence program. He also has the responsibility for coordinating those activities with Army components of unified and specified commands.

c. Chief of Engineers. Under the program direction of the Assistant Chief of Staff for Intelligence, the Chief of Engineers is responsible for—

(1) Providing direct support to the Assistant Chief of Staff for Intelligence in mapping and geodesy activities.
(2) Providing technical supervision and coordination of worldwide geographic intelligence activities.
(3) Providing and directing assigned elements engaged in mapping, geodesy, military intelligence, and related services, to include maintenance of the Department of Defense (DOD) master worldwide mapping and geodesy library and the DOD World Geodetic System.

9. Command

Commanders at all levels are responsible for the production of intelligence, including terrain intelligence. A commander must insure that he and his staff are aware of the effects of weather and terrain on their mission. He must know and utilize the capabilities for producing terrain intelligence that exist within his command or in outside agencies and insure that his command gathers pertinent information on the weather and terrain, and transmits this to all units requiring it. To do this properly, his command must be trained in the basic skills of terrain analysis. At theater level terrain intelligence is more detailed than the intelligence compiled at national level, and the production of theater intelligence may be assigned to a unit formed for that sole function. At field army and lower levels, combat terrain intelligence is the principal concern, becoming increasingly detailed and localized at successively subordinate levels.

10. Intelligence Officer

The terrain intelligence that a commander needs to make a sound decision and an effective plan must be provided by the unit intelligence officer. As a part of his intelligence report, the intelligence officer makes an analysis of the area of operations normally based upon a terrain study. The intelligence officer must plan and coordinate the collection of terrain information and the production, maintenance, and dissemination of terrain intelligence. Concurrently, he should keep the officer responsible for the preparation of terrain studies informed of the planning that is in progress or in prospect, so that the required terrain information may be secured and compiled.

11. Engineer

Under the general staff supervision of G2 the staff engineer, or the senior engineer commander in the event a staff engineer is not authorized, carries out the terrain intelligence functions. He produces and maintains terrain studies based upon terrain analyses. This involves—

a. Determining the requirements for terrain information, based upon requests from G2.

b. Collecting and evaluating terrain information.

c. Assembling terrain intelligence into a terrain study. He provides technical interpretation of the terrain covering such factors of military significance as obstacles, routes, and avenues of approach, cover and concealment, landforms, hydrology, crosscountry movement, and related subjects. He also disseminates terrain studies and technically evaluated information.

CHAPTER 3

PRODUCTION OF TERRAIN INTELLIGENCE

Section I. INTELLIGENCE CYCLE

12. Phases

The intelligence cycle described in FM 30–5 is also followed in the production of terrain intelligence. The activities associated with intelligence operations follow a four-step cycle, oriented on the commander's mission. The four steps are—

a. Planning the collection effort and preparing orders.

b. Collecting the information.

c. Processing the collected information.

d. Disseminating and using the resulting intelligence.

13. The Collection Effort

a. Direction. Terrain intelligence is directed by the responsible intelligence officer in the name of the commander. This direction involves—

(1) Determination of intelligence requirements.
(2) Preparation of a collection plan.
(3) Issuance of orders and requests to appropriate collection agencies.
(4) Continuous check on the production activities of the collection agencies.

b. Steps. Five successive steps are involved in direction—

(1) Determination of the information requirements.
(2) Analysis of the requirements to determine indications that would answer the questions presented.
(3) Translation of these indications into orders and requests for information pertaining to specific activities, localities, characteristics, or conditions.
(4) Selection of collection agencies to be employed and issuance of the necessary orders and requests.
(5) Followup.

14. Collecting

Collecting is the systematic exploitation of sources of information and the reporting of the information thus obtained to the proper intelligence agencies. A source is the person, thing, or activity from which information is obtained. An agency is any individual or organization which collects or processes information. Sources of terrain information and collection agencies are discussed in paragraphs 17 through 23.

15. Processing Sequence

a. Processing is the step in the intelligence cycle whereby information becomes intelligence.

b. Recording involves the reduction of information to writing or other graphical form of presentation and the grouping of related items to facilitate study and comparison.

c. Evaluation is the appraisal of an item of information to determine its pertinence, the reliability of the source or agency, and the accuracy of the information.

d. Interpretation is the result of critical judgment involving analysis, integration, and deduction. Analysis is the sifting and sorting of evaluated information to isolate significant elements with respect to the mission and operations. Integration is the combination of the elements isolated in analysis with other known information to form a logical picture of enemy activities or the influence of the characteristics of the area on the mission of the command. Deduction is the acquisition of a meaning from

the hypothesis developed, tested, and considered valid.

16. Dissemination and Use

Terrain intelligence is disseminated to commanders and staffs as one element of the overall intelligence report. Dissemination may be accomplished by means of briefings, conferences, messages, or such intelligence documents as the estimate, summary, periodic report, an analysis of area of operations, annex, maps, photointerpretation reports, and climatic summaries. The information and intelligence are instruments in detecting enemy targets and developing effective combat power. The means and methods selected for dissemination depend upon the detail, pertinence, and urgency of the information and intelligence as well as its intended use. Consideration is given to the needs of the user, his resources for using the material, and the capabilities of available communications.

Section II. SOURCES AND AGENCIES

17. Maps and Terrain Models

a. Maps. Maps are a basic source of terrain information. They are intelligence documents, not supply items. Accordingly, the intelligence officer usually is responsible for staff supervision over military maps and survey activities. The classification of US maps by type and scale is explained in AR 117–5. Foreign maps, or those copied from maps that were prepared by foreign agencies, often vary from US standards and procedures. Reliability information is indicated in the margin of US produced topographic maps. Foreign maps may not provide this. Portions of one map sheet may be fully reliable and yet other parts of the same sheet may be based on obsolete data. The use of a map must be regulated by an estimate of the probable changes in manmade features that have occurred since the date of the latest revision. All personnel must be impressed with the importance of reporting errors, changes, and omissions in existing maps, so that new editions may incorporate the necessary corrections. Maps prepared for a special purpose may not be reliable for information that is not related to that purpose. A railway map, for example, may be quite accurate in presenting railway information, but may be unreliable for data shown on roads or other features. Special maps and overlays may be prepared for a specific military purpose or to show only particular characteristics of the terrain.

(1) Soil maps are prepared primarily for agricultural purposes to show the potentialities of the soil for crop production. This type of map shows soils of various types, indicating their degree of acidity, nutrients, suitability for certain crops, and similar information. Engineering soil maps indicate the qualities of soil construction or vehicle movement. Agricultural soil maps may be used for engineering purposes after they have been interpreted according to engineering nomenclature and requirements.

(2) Geologic sketch maps indicate the geology of an area. Outcrop maps show the bedrock that is exposed. Bedrock maps show the surface of the bedrock as it would appear if the overlying soils were removed. These maps are useful in locating sites for major structures and in finding sources of rock for construction purposes when the overburden has been described.

(3) Communication maps include those that show the system of lines and sequence of stations of railways, provide automobile route information, and indicate navigable waterways and the routes and stops of airlines. These really could be considered transportation maps.

(4) Relief maps show differences in elevation by the use of various tints and shading patterns. A plastic relief map is a standard topographic map printed on a plastic and molded into a three-dimensional form with a 2:1 exaggeration in the relief. Because of the shrinkage characteristics inherent in

plastic materials, there is considerable distortion of the features shown on this type of map. For example, some stream lines may appear not coincident with valley bottoms.

(5) Pictomaps are maps on which the photographic imagery of a standard photomosaic has been converted into interpretable colors and symbols. Desert sands, swamps, jungle, glaciers, and extra terrestrial topography are some of the features that are ideally portrayed on a pictomap. Shadows of map features are emphasized on the pictomap. They accurately delineate many cultural features, and they lend a three-dimensional effect to buildings and vegetation. This effect symbolizes and establishes relative heights of these cultural features. The pictomap is an excellent source for terrain information.

(6) Other special maps show the distribution of major vegetation types and show depth of depressions for use in mountain and winter operations; water supply sources and distribution systems; structure of town and city plans; conditions affecting cross-country movement; and similar detailed information that can be presented most effectively in graphic form.

b. Terrain Models. A terrain model is a three-dimensional graphic representation of an area showing the conformation of the ground to scale. Usually it is colored to emphasize various physical features, and the vertical scale is exaggerated to convey relief. Terrain models may be made for use in strategic or tactical planning, assault landings, airborne landings, and aerial target delineation.

18. Photographs and Remote-Sensor Imagery

a. General Features. Aerial and ground photographs provide an accurate visual record of the terrain. They furnish information that is not readily available or immediately apparent by ground reconnaissance or by visual observation from the air, especially of enemy-held areas.

Photographs preserve information in a permanent form, so that it is available for later study and comparison. Remote-sensor imagery includes infrared photography and side-looking airborne radar. It provides imagery records of terrain, vegetation, and cultural features that may be obscured by atmospheric, natural, or artificial cover.

b. Advantages. Properly interpreted, aerial and ground photography and airborne infrared and radar imagery will furnish detailed information concerning:

(1) The identification of vegetation soils and rocks.

(2) Both surface and subsurface drainage characteristics. Indications of surface drainage can be located, marked, and evaluated through detailed stereo study. In some cases, subsurface drainage can be predicted in general terms, such as, "well-drained" or "poorly drained."

(3) Suitability of terrain for construction of airfields, roads, and underground installations, based upon topography, drainage, soils, and engineering materials. General characteristics can be given, such as"flat plain, predominantly fine-grained soils, well-drained, forest cover, deposits of gravel suitable for borrow."

(4) Suitability of terrain for cross-country movement and airborne and air-mobile operations. Photographs and photomaps can be used advantageously in studying and rating areas as to their suitability for movement, based on the evaluation of relief, slopes, drainage, soils, and vegetation. General characteristics may be determined, such as "flat plain, grass-covered, silty soils, hedgerows, poor drainage."

(5) Aerial and ground photographs, interpreted by skilled personnel, can give highly detailed information about all types of manmade features, from artificial obstacles to large industrial complexes.

(6) Photographs depict up-to-date terrain features. Maps depict only what the

mapmaker saw at the time the mapping information was gathered.

c. Limitations. The amount of information that can be derived from interpretation of photography is limited by adverse weather and by densely forested terrain. Aerial photographs may not provide detailed factual information concerning the engineering properties of soil, vehicle type and trafficability relationships, and quantitative data for materials and other items. This type of information usually can be obtained only through field sampling and laboratory testing procedures or by comparison with information from reconnaissance reports, geological surveys, and similar sources. It is important that information obtained from aerial and ground photographs should be correlated with information from other sources, such as maps, personal reconnaissance, and reports from intelligence agencies.

d. Requirements. There should be sufficient aerial photograph coverage made to enable the interpreter to determine the extent of local conditions and the expected variations. Usually vertical coverage is best for measurements, although oblique photographs are more useful for certain purposes, such as in the study of dense forest areas. Scales of 1:5,000 to 1:20,000 are desirable for detailed terrain analysis. Photographs in this range provide good area coverage and stereoscopic perception of relief. They show such details as major gully characteristics, and the outstanding terrain features.

(1) Photographs with scales smaller than 1:30,000 provide excellent area coverage in the broadest sense. Major physiographic details are easily seen and studied; relief must be great, however, before stereovision is practicable because only major relief forms are clearly differentiated at these scales, and small details are lost. Major gullies can be plotted, for example, but in some cases their characteristics cannot be determined. As a rule, landforms can be delineated only when there is a great contrast in pattern. Slopes associated with landforms at times cannot be seen or distinguished. While such manmade features as roads, railroads, bridges, and buildings can be identified, the interpreter may have difficulty in determining their structural details. Colored film is frequently the most effective for identifying vegetation. The best scale depends on the data needed. Vegetation can also be identified from differences in tone on black and white aerial photographs.

(2) Stereopairs, vectographs, and anaglyphs are particularly useful in making terrain studies. A stereopair consists of two photographs of the same terrain taken from different positions. Usually they are taken from a position vertically above the area being photographed with about 60 percent of each photo (called the overlap) common to both photographs. Examination with a stereoscope gives an exaggerated third-dimensional view of the terrain included in the overlap. A vectograph is a print or transparency in which the two photographs of the stereoscopic pair are rendered in terms of degree of polarization presenting a stereoscopic image when viewed through Polaroid spectacles. An anaglyph is a picture combining two images of the same object, recorded from different points of view, as images of the right and left eye, one image in one color being superimposed upon the second image in a contrasting color. Viewed through a pair of light filters, the anaglyph produces a stereoscopic effect.

(3) Controlled mosaics of an area provide an accurate map from which measurements of distances can be obtained. The amount of detail useful for terrain analysis will depend upon the scale of the mosaic.

19. Books and Periodicals

Valuable terrain information can be found in a wide variety of books and periodicals. These include trade journals, economic atlases, tide tables, pilots' handbooks, tourist guides, and similar publications. Unpublished syste-

matic records covering meteorological, hydrological, and similar scientific data prepared by government agencies, engineering firms, private societies, and individuals also contribute valuable terrain information. Although utilized chiefly for terrain studies made by higher headquarters, material of this type, when locally available, can be of considerable value to lower echelons.

20. Intelligence Reports

Strategic intelligence studies prepared by Department of Defense agencies provide detailed terrain information concerning major geographical areas. Such studies include—

a. National Intelligence Survey (NIS). This is a series of documents covering the countries of the world, presenting a digest of the basic intelligence required for strategic planning and for the operations of major units. Each survey describes in detail the terrain characteristics of a specific area or nation supported by descriptive material, maps, charts, tables, and with reliability ratings assigned to all data.

b. Engineer Intelligence Studies (EIS). These are no longer published, but the EIS files are still an important source. These documents describe in detail those natural and manmade features of an area that affect the capabilities of military forces, particularly with reference to engineer operations. They were produced by the Office, Chief of Engineers.

c. Lines of Communication (LOC). These studies, prepared on either medium scale maps or single, small-scale foldup sheets, contain an analysis of transportation facilities with information on railroads, inland waterways, highways, airfields, pipelines, ports, and beaches.

d. Terrain Studies. These contain area intelligence depicted on medium and small scale maps with accompanying textual and graphic material. They are for strategic planning, and describe principal terrain characteristics, major aspects of land, water and air movement, and key installations.

e. Special Reports on Military Geography. These are designed primarily for strategic planning and generally directed towards analysis of a major aspect of military geography such as cross-country movement, amphibious operations, and airborne operations.

f. Engineer Reconnaissance Reports. Reports that summarize data obtained by reconnaissance are a major source of terrain information. They are of particular value in providing current, detailed information about lines of communication and availability of natural construction materials.

21. Captured Enemy Documents

Maps and other intelligence documents captured from the enemy often are of great value as sources of terrain information. Usually, enemy-prepared military maps and terrain studies of enemy territory will be more up to date and detailed than our own. The processing of captured enemy documents is described in FM 30–15.

22. Interrogation

Interrogation personnel should be kept informed of the terrain information that is required by intelligence officers. Useful information about the area held by enemy forces frequently can be obtained from prisoners of war, deserters, liberated civilians, refugees, escapees, evadees, cooperative enemy nationals, and self-surrendered and apprehended enemy espionage agents.

23. Collection Agencies

a. Units. Collection agencies include intelligence personnel, troop units, and special information services. FM 30–5 discusses the types and capabilities of these agencies. All units within a command may be employed by the intelligence officer to secure terrain information. In addition, he may request higher headquarters to use their units and facilities to secure information he requires.

b. Troops. Reconnaissance missions to secure terrain information may be assigned to combat or combat support units. Such missions may be accomplished by units specifically organized for reconnaissance or by other units assigned reconnaissance missions in addition to their normal activities.

c. Aircraft. In addition to ground reconnaissance, aircraft may be employed to secure information about the terrain. Although it may be limited by adverse weather or enemy air defense, air reconnaissance is the fastest

means of gathering terrain information and, at times, may be the most practical means of reconnoitering enemy territory. Information on objects such as trees, structures, and communication lines is of great importance for airmobile and air landing operations. Army aviation has the capability to conduct air reconnaissance missions, but additional support may be requested through intelligence channels for reconnaissance flights to be accomplished by the Air Force.

d. Specialized Agencies. An engineer terrain detachment usually is assigned to each corps. The detachment is composed of personnel in various fields of engineering and the natural earth sciences who prepare special terrain studies, evaluate all types of terrain information, and serve as consultants to agencies faced with technical problems. Terrain information may be provided by personnel whose normal duties are not primarily concerned with terrain intelligence. These include military intelligence personnel of the MI battalion, field army, and MI detachments at corps. Civil Affairs staffs acquire terrain intelligence in considerable detail, particularly in the areas of agriculture, forestry and fishing, transportation, and other economic functions. Civil Affairs area studies and surveys are sources of information and intelligence.

CHAPTER 4

WEATHER AND CLIMATE

Section I. WEATHER

24. Definition

Weather comprises the day-to-day changes in atmospheric conditions. The physical properties and conditions of the atmosphere that must be measured or observed to describe the state of the weather are termed the weather elements.

25. Air Temperature

a. Measuring. Air temperature is the degree of hotness or coldness of freely circulating air as measured by a thermometer that is shielded from the sun. The thermometer is calibrated by using the melting point of ice and the boiling point of water at sea level as standard references. In most English-speaking countries, the Fahrenheit scale is used, with the melting point of ice designated as 32°F above zero and the boiling point of water as 212°F above zero. Countries using the metric system employ the centigrade (Celsius) scale, with the freezing point of water designated as 0° C and the boiling point, 100° C. In the United States, surface air temperatures are indicated in degrees Fahrenheit and upper air temperatures in degrees centigrade. Temperatures may be converted from one of these scales to the other by use of the following formulas:

$C = \frac{5}{9}\ (F - 32°)$ Example: Change 77° F to C.
Multiply 77° F − 32° by $\frac{5}{9}$, which equals 25° C.

$F = \frac{9}{5} \times °C + 32°$ Example: Change 25° C to F.
Multiply 25° C by $\frac{9}{5}$ and add 32°, which equals 77° F.

b. Recording. Temperature data may be recorded in the following forms:

(1) *Mean daily maximum temperature.* The average of the daily maximum temperatures for a month.
(2) *Mean daily minimum temperature.* The average of the daily minimum temperatures for a month.
(3) *Mean daily temperature.* Average of daily maximum and minimum temperatures for any specific day.
(4) *Mean monthly temperature.* Average of daily mean temperatures for any specific month.
(5) *Mean annual temperature.* Average of daily mean temperatures for any specific year.
(6) *Mean annual range.* Difference between the mean monthly temperatures of the warmest and coldest months.
(7) *Diurnal variation.* Difference between the maximum and minimum temperatures occurring in a day.
(8) *Normal values, or long-term mean.* The average of temperature values for the entire period of record. These values usually are used to evaluate the climate.
(9) *Extreme values.* Absolute maximum or absolute minimum or extreme values.

(10) *Length of freezing period.* Number of days with minimum temperature below freezing.

c. Use of Data. Monthly daily maximum and mean daily minimum temperatures usually are employed to provide a general definition of the type of climate, and the mean annual range to indicate its variability. Extreme values show the limits which must be anticipated in the climate being considered. Temperatures also are recorded at various altitudes above the ground level in order to provide data for estimating certain types of nuclear-weapon effects.

26. Atmospheric Pressure

a. Definition. Atmospheric pressure is the force exerted per unit of area by the weight of the atmosphere from the level of measurement to the top of the atmosphere. At sea level this pressure is approximately 6.66 kilograms per 6.45 square centimeter or 14.7 pounds per square inch. Mean sea level is used as a reference for surface weather observations, and pressure measurements are shown on weather maps and climatic charts as if the entire surface of the earth were at sea level. Atmospheric pressures are recorded at various altitudes to provide data for estimating nuclear-weapon effects.

b. Measurement. The standard device for measuring atmospheric pressure is a mercurial barometer which balances the weight of the atmosphere with a column of mercury. The standard atmospheric sea-level pressure is equal to that exerted by a 760 millimeter (29.29 inch) column of mercury at 32°F. and at standard gravity. For some scientific purposes, it is desirable to indicate atmospheric pressure in units of pressure (weight per unit of area) rather than in units of length(centimeters or inches). In the metric systems, a bar is the unit of measure. The millibar (1/1000 of a bar) is used in meteorology to designate the value of atmospheric pressure. The standard sea level pressure is 1013.2 millibars. One millibar equals .0762 centimeters or 0.03 inches of mercury. Most weather stations today observe pressure on an aneroid barometer, calibrated in both millibars or inches or millimeters of mercury. Barometer readings significantly below 760 millimeters usually indicate low-pressure areas and those significantly above 760 millimeters usually indicate high-pressure areas. In general, cold air, being heavy and dense, causes high barometric pressures, while hot air, which is light and thin, causes low pressures. High-pressure systems usually are associated with fair, dry weather; low-pressure systems, with unsettled, cloudy conditions.

27. Winds

a. Description. Wind is air in motion and results from differences in atmospheric pressure. A wind is described by its direction and speed. The direction of a wind is the direction from which it is blowing. A wind coming from the north, for example is termed a north wind. As reported in observations, wind direction is determined with reference to true north and is expressed to the nearest 10 degrees. Thus, a direction of 090 degrees (a wind from due east) would be reported as 09. Wind velocities are reported by the Air Weather Service in knots. A table of wind speeds and their specifications is given (table 1) to aid in estimating speeds. Over irregular terrain, a wind does not move with a steady force or direction, but as a succession of gusts and lulls of variable speed and direction. These eddy currents, caused by friction between air and terrain, are called gusts or turbulence. Turbulence also results from unequal heating of the earth's surface, the cooler air of adjacent areas rushing in to replace the rising warm air from heated areas. Usually the turbulence produced by surface friction is intensified on a sunny afternoon.

b. Systems. Local pressure and wind systems are created by valleys, mountains, and land masses that change the weather characteristics of areas. Since land masses absorb and radiate heat more rapidly than water masses, the land is heated more than the sea during the day and cools more at night. In coastal areas, warm air over the land rises to a higher altitude and then moves horizontally out to sea. To replace this warm air, the colder air over the water moves on to the land, creating the so-called sea breeze. The circulation is reversed at night, so that the surface air moves from the land to the sea, resulting in a land breeze.

Table 1. Weather Map Scale of Wind Velocity

Descriptive item	Knots	Meters/seconds	Specifications
Calm	less than 1	0–0.2	Calm; smoke rises vertically.
Light air	1–3	0.3–1.5	Direction of wind shown by smoke drift but not by wind vanes.
Light breeze	4–6	1.6–3.3	Wind felt on face; leaves rustle.
Gentle breeze	7–10	3.4–5.4	Leaves and small twigs in constant motion; wind extends light flag.
Moderate breeze	11–16	5.5–7.9	Raises dust and loose paper; small branches are moved.
Fresh breeze	17–21	8.0–10.7	Small trees in leaf begin to sway; crested wavelets form on inland waters.
Strong breeze	22–27	10.8–13.8	Large branches in motion; whistling heard in telegraph wires; umbrellas used with difficulty.
Near gale	28–33	13.9–17.1	Whole trees in motion; inconvenience felt when walking against wind.
Gale	34–40	17.2–20.7	Breaks twigs off trees; generally impedes progress.
Strong gale	41–47	20.8–24.4	Slight structural damage occurs (chimney pots, slates and shingles removed).
Storm	48–55	24.5–28.4	Seldom experienced inland; trees uprooted; considerable structural damage occurs.
Violent storm	56–63	28.5–32.6	Very rarely experienced; accompanied by widespread damage.
Hurricane	64 and over	32.7 and over	

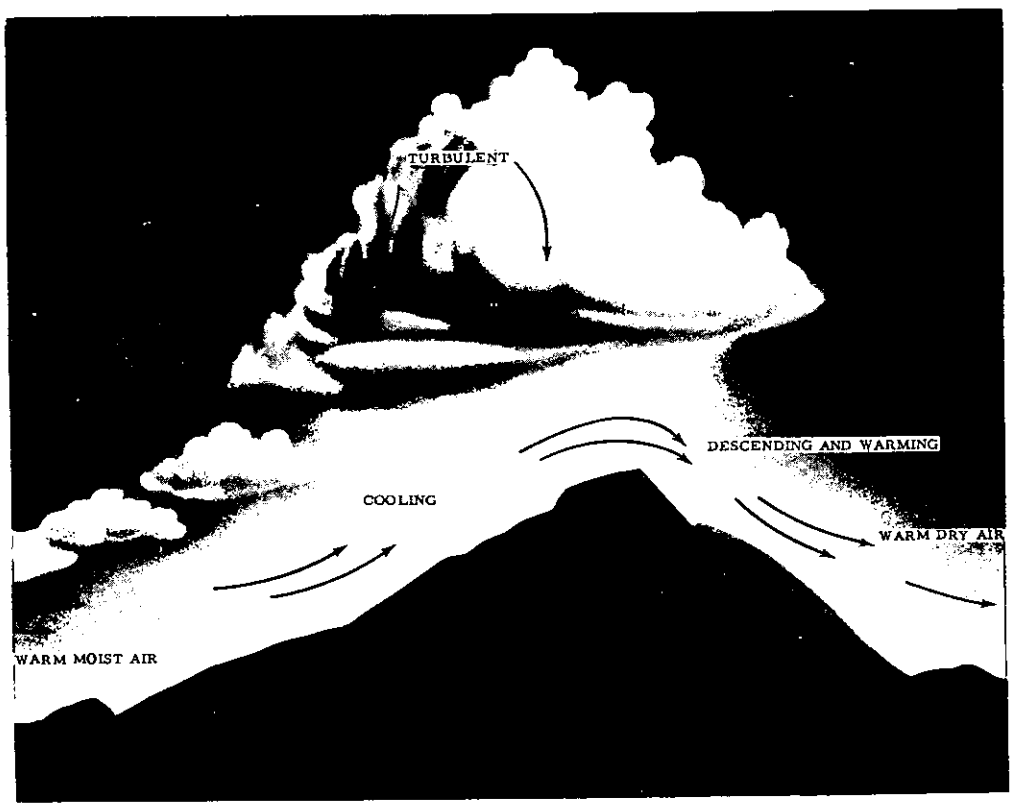


Figure 1. Chinook or foehn effect.

c. Vally Wind. Heated by the daytime sun, the air in contact with a mountain slope becomes lighter than the surrounding air and rises up the slope, being replaced by denser, colder air. This air movement is called a valley wind because it appears to be flowing up from the valley. At night the air in contact with the slope becomes colder and more dense, sinking down along the slope to create a mountain breeze that seems to flow out of the mountain. Mountain breezes generally are stronger than valley winds, especially in the winter.

d. Chinook. A chinook (North America) or foehn (Europe) (fig. 1) is a phenomenon that occurs in winter and spring on the lee or downwind side of mountain ranges over which there flows a steady crosswind of moisture-laden air. As the air rises over the windward side of the mountains it expands and cools rapidly, producing clouds and precipitation. As the air moves down the lee side of the mountain range it compresses and warms. As a result, there are warm, dry winds on the lee side of the mountains.

e. Fall and Gravity. Fall and gravity winds are caused by the descent of downslope air through the action of gravity. They are typical of the Greenland coast, which is essentially a high plateau sloping abruptly to the sea along an irregular coastline cut by many fiords. The central plateau area remains ice-covered throughout the year, developing extremely cold air masses which frequently drain off through the fiords to the sea and attain a near-hurricane speed. At sea level the winds remain relatively cold and very dry. Similar winds are the bora, which drain off the southern Alps and the Balkan Plateau into the Adriatic Sea, and the mistral of the Rhone Valley in France.

f. Monsoon. A monsoon wind is any seasonally changing or reversing wind. It is strongest and steadiest on the southern and eastern sides of Asia. It blows outward from high-pressure centers overland toward the sea in winter and inward toward low-pressure overland in summer. In most regions, the summer monsoon season is generally characterized by extensive cloudiness and frequent precipitation. The winter monsoon season is characterized by dry air and infrequent cloudiness except where the monsoon winds pick up moisture by moving over warm seas before striking an island or peninsular coastline.

28. Humidity

a. Vapor. Water vapor is the most important constituent of the atmosphere that determines weather phenomena. Although the oceans are the primary source, a limited amount of water vapor also is furnished to the atmosphere from lakes and rivers, snow, ice fields, and vegetation. The percentage of water vapor by volume in the air may vary from practically zero in deserts to 4 or 5 percent in humid tropical areas.

b. Amount. Humidity is the term used to describe the amount of water vapor in the air. The amount that the air actually contains compared with what it could hold at a given temperature and pressure is termed the relative humidity. When a specific air mass holds all the moisture that it can at a given temperature, it is described as having a relative humidity of 100 percent.

c. Dew Point. The dew point is that temperature at which the air becomes saturated. The higher the dew point, the greater amount of water vapor the air can hold. The closer the dew point temperature is to the actual temperature, the greater the likelihood of condensation. Condensation results when the capacity of the atmosphere to hold water is reduced by cooling, so that the water vapor in the air is changed to visible moisture such as fog or clouds.

29. Clouds

a. Classification. Clouds are masses of condensed moisture suspended in air in the form of minute water droplets. They are classified according to their form or appearance and by the physical processes producing them. The Air Weather Service reports the type of clouds present, the heights of the cloud bases and cloud tops, the amount of cloudiness, and the direction in which the clouds are moving. Cloud amounts are reported in terms of the fraction of the sky that is covered by clouds (fig. 2). The following terms are used:

(1) *Clear.* No clouds, or less than 0.1 of the sky covered.

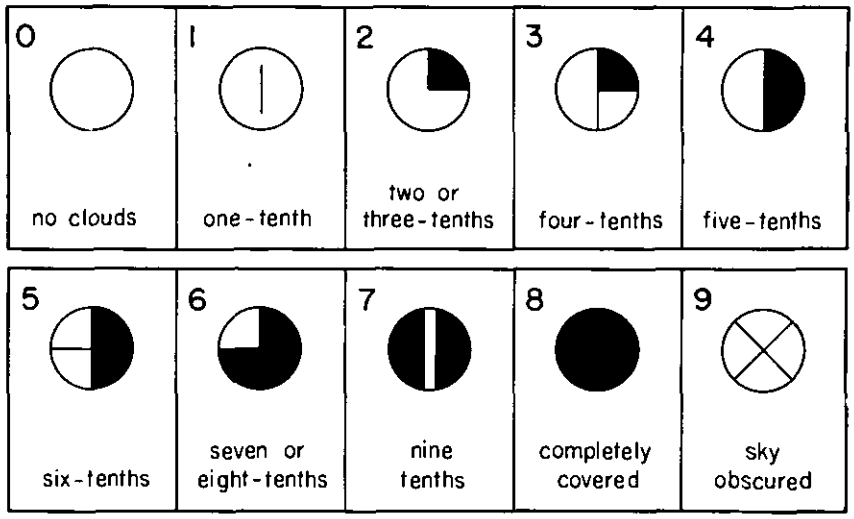


Figure 2. Cloud cover symbols.

(2) *Scattered.* 0.1 to 0.5 of the sky covered.
(3) *Broken.* 0.6 to 0.9 of the sky covered.
(4) *Overcast.* More than 0.9 of the sky covered.

b. Heights. Cloud heights are reported in meters above the ground. The heights of clouds below 1,500 meters (5,000 feet) are reported to the nearest 30 meters (100 feet); clouds from 1,500 to 3,000 meters (5,000 to 10,000 feet) are reported to the nearest 150 meters (500 feet), and clouds above 3,000 meters (10,000 feet) to the nearest 300 meters (1,000 feet). A ceiling is defined as the lowest layer of clouds that is reported as broken or overcast and not classified as thin. Heights of clouds are reported in meters or feet above the point of observation.

c. Direction. Cloud direction is the direction toward which the cloud bases are moving. It is reported according to the eight points of the compass.

d. Appearance. According to their appearance, clouds are either cumiliform or stratiform. Cumiliform clouds are formed by rising currents in unstable air. Stratiform clouds result from the cooling of air in stable layers.

(1) Cumiliform clouds are dense with vertical development. The upper surface of a cumiliform cloud is dome-shaped, while the base is nearly horizontal. Usually clouds of this type are separate from each other and rarely cover the entire sky. The precipitation from cumiliform clouds generally is showery in nature.

(2) Stratiform clouds usually occur in layers that may extend from horizon to horizon, without the vertical development of cumiliform clouds. Precipitation from this type of cloud usually is in the form of light continuous rain, drizzle, or snow.

e. Groupings. Clouds may be grouped into four families (fig. 3)—

(1) *High.* Cirrus, cirrostratus, cirrocumulus.
(2) *Middle.* Altostratus, altocumulus.
(3) *Low.* Stratus, nimbostratus, stratocumulus.
(4) *Vertical development.* Cumulonimbus for an example.

f. High Clouds. High clouds usually occur at heights of from 6,000 to 12,000 meters (20,000 to 40,000 feet), although they may be found at much lower altitudes in polar regions. They are composed of ice crystals. The characteristics of the major cloud types in this group are as follows:

(1) *Cirrus.* This is a delicate white fibrous cloud that often appears bright yellow or red from the reflection of light from a rising or setting sun. Cirrus

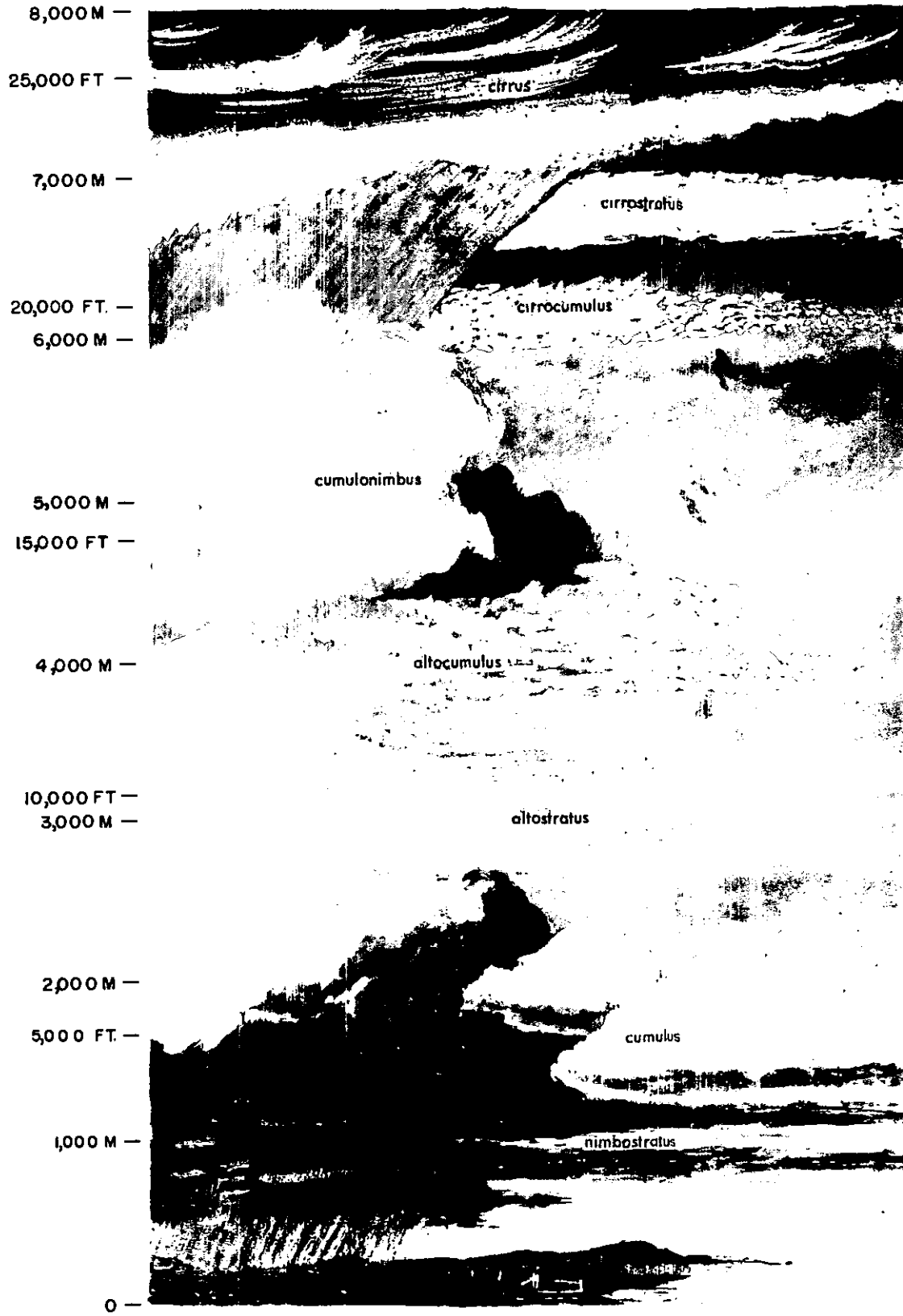


Figure 3. Major cloud types.

clouds may appear as isolated tufts, featherlike plumes, or streaks with upturned ends often referred to as mare's tails. Because of. their thinness, cirrus clouds do not blur the outlines of the sun or moon, and usually do not make an appreciable change in the appearance of the sky.

(2) *Cirrostratus.* These are thin, whitish veils of clouds that give the sky a milky look. Usually they can be distinguished from cirrus clouds by the halo which light from the sun or moon produces in them.

(3) *Cirrocumulus.* Clouds of this type consist of patches of small, rounded masses or white flakes arranged in groups or lines.

g. Middle Clouds. Middle clouds usually occur at altitudes of 1,800 to 6,000 (6,000 to 20,000 feet) meters in the lower limit of this range in the colder seasons, and at altitudes near the upper limit in the warmer seasons. The major types are—

(1) *Altostratus.* Clouds of this type appear as a veil of gray or bluish fibrous clouds, the thinner forms resembling the thicker forms of cirrostratus. Altostratus clouds are associated with smooth or stable air layers, and occasionally they produce light rain or snow.

(2) *Altocumulus.* This cloud type can appear as a layer or in patches, is white or gray in color, and the cloud elements appear as rounded masses or rolls. They occur in a variety of forms, and may exist at several levels at the same time.

h. Low Clouds. Low clouds usually have bases below 1,800 meters (6,000 feet) and include the following types:

(1) *Stratus.* These form a low layer resembling fog, although they do not rest upon the surface. They give the sky a hazy appearance. The base of this cloud is usually rather uniform in height but it often occurs in the form of ragged patches or cloud fragments. Layers of stratus clouds may cover hundreds of thousands of square miles. Usually they are thin, and range in thickness from a few hundred feet to several thousand feet. Frequently, stratus clouds are accompanied by fog, haze, or smoke between their bases and the ground. Visibility is very poor under stratus clouds, and precipitation from them usually is in the form of light snow or drizzle.

(2) *Nimbostratus.* Clouds of this type form a low, dark gray layer. Precipitation usually is in the form of continuous rain or snow of variable intensity. Because of its thickness, sometimes more than 4,500 meters (15,000 feet), the nimbostratus is frequently classified as a cloud of vertical development.

(3) *Stratocumulus.* This type of cloud forms a lower layer of patches of rounded masses or rolls. The base of the stratocumulus usually is higher and rougher than the stratus clouds. Frequently these clouds change into the stratus type.

i. Vertical. Vertical development clouds cannot be classified according to height, since they extend through all the levels assigned to other cloud groups. The bases vary from 150 to 3,000 meters (500 feet to 10,000 feet) or higher, while the tops may vary from 450 meters (1,500 feet) to more than 12,000 meters (40,000 feet). They all occur in relatively unstable air and frequently are associated with strong vertical currents and intense turbulence. In this category are the following:

(1) *Cumulus.* Clouds of the cumulus type are dense, with vertical development. The base is horizontal and uniform in height above the earth, with a top that is domed or cauliflower-like in shape. Cumulus clouds appear white when they reflect sunlight toward the observer, but when viewed from directly underneath or when they are between the observer and the sun, they may appear dark with bright edges. Over land, cumulus clouds tend to develop during the warming of the day, dissipating at night when the

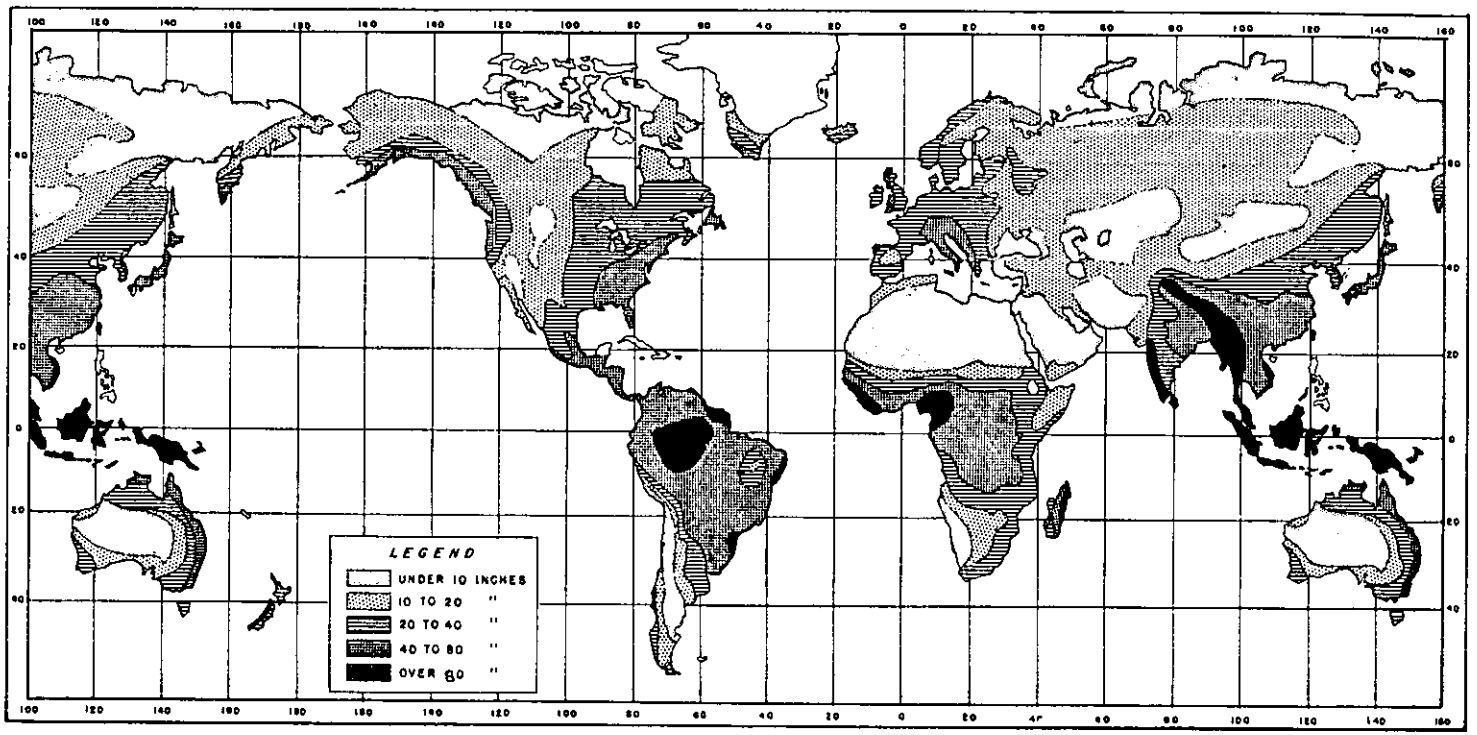


Figure 4. World rainfall.

earth's surface cools. Over water, cumulus clouds tend to develop at night as the water surface remains warm while the air mass cools slightly.

(2) *Cumulonimbus.* Clouds of this type are heavy masses which extend to great heights. Their upper portions resemble mountains or towers capped with a fibrous texture. They develop only in unstable air. Cumulonimbus clouds are distinguished from cumulus clouds chiefly by the veil of ice crystal clouds which surrounds their upper portions. Thunderstorms, squalls, turbulence, and hail are characteristic of cumulonimbus clouds.

30. Precipitation

a. Description. Precipitation (fig. 4) is visible moisture that falls from the atmosphere, such as rain, sleet, snow, hail, drizzle, or combinations of these. As an air mass rises, its ability to hold moisture decreases and clouds form. When the cloud droplets become too large to remain in suspension, rain occurs or if the air temperature is below freezing, snow is formed. Sleet is frozen rain formed by droplets passing through a layer of below-freezing air. Hail consists of rounded particles composed of layers of ice falling from cumulonimbus clouds with strong updrafts. Raindrops are carried to high altitudes and frozen into ice pellets. They then fall and are carried up again by the updraft until the weight of the pellet is greater than the force of the updraft, whereupon it falls to earth. Freezing rain falls from the air in liquid form but freezes upon contact with objects on the surface that are at a temperature below the freezing point. The ice formed on these surfaces is called glaze. Air Weather Service observations include information on the form of precipitation and its character, intensity, and amount.

b. Character. The character of precipitation refers to its duration and to changes in its intensity. It is reported as continuous, intermittent, or showery. Continuous precipitation is that in which the intensity increases or decreases gradually. Intermittent precipitation is characterized by a gradual change in intensity, but ceases and recommences at least once an hour. Showery precipitation is marked by rapid changes in intensity and by starting and stopping abruptly. The intensity of precipitation is determined on the basis of its rate of fall. It is described as follows:

(1) *Very light.* Scattered drops or flakes which do not completely wet an exposed surface, regardless of duration.

(2) *Light.* Not more than 0.25 millimeter (0.01 inch) in 6 minutes.

(3) *Moderate.* 0.26 to 0.75 millimeter (0.01 to 0.03 inch) in 6 minutes.

(4) *Heavy.* More than 0.75 millimeter (0.03 inch) in 6 minutes.

c. Intensity. The intensity of snow and drizzle is determined on the basis of the reductions in visibility which result, as follows:

(1) *Very light.* Scattered drops or flakes which do not completely wet an exposed surface, regardless of duration. Negligible effect on visibility.

(2) *Light.* Visibility 1 kilometer (5/8 statute mile) or more.

(3) *Moderate.* Visibility less than 1 kilometer (5/8 statute mile), but not less than 1/2 kilometer (5/16 statute mile).

(4) *Heavy.* Visibility less than 1/2 kilometer (5/16 statute mile).

d. Amount. The amount of precipitation is expressed in terms of the vertical depth of water (or melted equivalent in the case of snow or other solid forms) accumulated within a specified time on a horizontal surface. This is expressed to the nearest 0.25 millimeter (0.01 inch). A depth of less than 0.13 millimeters (0.005 inch) is called a trace. In the case of snow, both the actual depth and the equivalent in water are required. Snow depth is measured to the nearest whole inch, and less than 1.3 centimeters (0.5 inch) is termed a trace. The water equivalent of snow is determined by melting a representative sample and measuring the resulting depth of water. As an average figure, 25 centimeters (10 inches) of snow are considered to be equivalent to 2.5 centimeters (1 inch) of water, although this is subject to wide variation. The depth of snow is of concern in estimating the trafficability and the water equivalent is significant for

problems involving water supply, flood prediction, stream flow, and drainage.

31. Fog

Fog is defined as a mass of minute water droplets suspended in the atmosphere at the surface of the earth that reduces horizontal visibility. It is formed by the condensation of water vapor in the air. The most favorable conditions for the formation of fog are an abundance of water vapor, high relative humidity, and a light surface wind. A light wind tends to thicken fog. Increasing wind speeds will usually cause fog to lift or to dissipate. Fog usually is more prevalent in coastal areas than inland because there is more water vapor in the atmosphere. Inland fogs may be very persistent in industrial regions. In most areas of the world, fog occurs more frequently during the colder seasons of the year than it does in the warmer seasons.

32. Storms

a. Thunderstorms. A thunderstorm is a local storm accompanied by thunder, strong gusts of wind, heavy rain, and sometimes hail, usually lasting for no more than an hour or two. A thunderstorm is cellular, each of its many cells having violent up and down drafts in close proximity. The overall mass has a characteristic frontal zone with violent cool winds racing inward toward the storm in spite of its forward motion. When a thunderstorm reaches its mature stage and the rain begins, a downdraft starts in the lower and middle levels of the storm. This large body of descending air causes strong, gusty surface winds that move out ahead of the main storm area, often resulting in a radical, abrupt change in wind speed and direction termed the first gust. In general, the strongest thunderstorm winds occur on the forward side of the storm where the downdraft first reaches the surface. These winds ascend upward at various rates, depending on the intensity and size of the storm. The actual storm has layers conducive to icing and hail formation depending on the altitudes obtained by updrafts and so on. The speed of a thunderstorm wind may reach 80 to 120 kilometers (50 to 75 miles) per hour for a short time.

b. Tornadoes. Tornadoes are circular whirlpools of air which range in size from about 30 meters to .8 kilometer (100 feet to one-half mile) in diameter. A tornado appears as a rotating funnel-shaped cloud extending toward the ground from the base of a cumulonimbus. The low pressure and the high wind speeds encountered in the center of the tornado are very destructive. The paths of tornadoes over the ground usually are only a few miles long and the tornadoes move at speeds of 40 to 90 kilometers (25 to 55 miles) per hour. Although the maximum wind speeds associated with tornadoes never have been measured directly, property damage and other effects indicate that they may exceed 800 kilometers (500 miles) per hour. When they occur over water, tornadoes are termed *waterspouts.*

c. Tropical Cyclones. A tropical cyclone is a low-pressure system of cyclonic winds that forms over tropical water areas (fig. 5). Cyclones of great intensity are called hurricanes in the Atlantic and Eastern Pacific Oceans, typhoons in the Western Pacific Ocean, cyclones in the Indian Ocean, and *willi willi* in Australia. The average life span of a tropical cyclone is 6 days, although some last only a few hours and others as long as 2 weeks. Tropical cyclones of hurricane intensity are characterized by extremely strong and gusty surface winds, with speeds of 117 to more than 240 kilometers (73 to more than 150 miles) per hour; continuous intense rain in the central area, and a relatively calm area near the center known as the eye. These storms vary in size from 80 to 800 kilometers (50 to 500 miles) in diameter. The precipitation associated with tropical cyclones is extremely heavy. They are frequently accompanied by violent thunderstorms, with the heaviest rainfall usually occurring some distance ahead of the eye of the moving cyclone. Abnormally high tides are a common companion of hurricanes and are responsible for a great amount of damage.

33. Weather Forecasts

a. Factors. A weather forecast is a prediction of the weather conditions expected to occur at a place, within an area or along a route at a specified future time. The accuracy and reliability of weather forecasts depend upon a number of factors, including the climatic characteristics of the forecast area, the amount

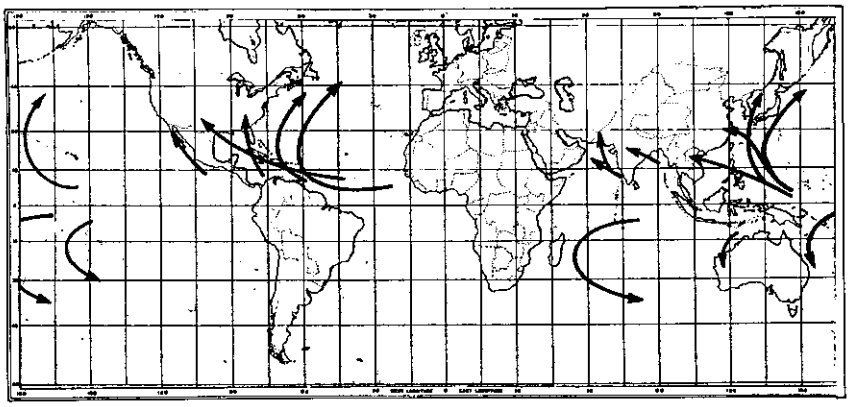


Figure 5. Tropical cyclones.

of weather data available, the reliability of weather communications facilities, the length of the forecast period, and the experience of the forecaster. Other factors being equal, the reliability of forecasts generally decreases as the length of the forecast period increases.

b. Format. Weather forecasts may be presented in coded (numerical), graphical (pictorial), or written (plain language) format. Normally, weather forecasts for use by Army units will be issued in plain language form. Because forecasts are subject to sudden change, they are usually transmitted by electrical means. Abbreviations are used extensively. The abbreviations used in weather messages are contained in AR 320–50 and in the Federal Aviation Agency (FAA) publication, *Contractions.*

c. Sources. Weather forecasts and special studies are provided by agencies of the Air Weather Service of the Air Force. Air Weather Service is found on all Air Force bases and on many Army bases that have Army aviation units. Division and lower units receive weather forecasts from either attached personnel of Air Weather Service or from higher headquarters.

d. Short-Period Forecasts. These forecasts cover a period up to 48 hours in advance of issue, giving detailed values of the weather elements expected to occur during the period and the time of anticipated weather changes. They are sufficiently reliable for use in detailed short-range planning.

e. Medium-Period Forecasts. This class covers a period of 3 to 5 days, and extended-period forecasts cover periods in excess of 5 days. They are less detailed and specific than short-period forecasts. Usually the weather information is expressed in terms of departure from normal conditions and is suitable only for preliminary planning purposes.

f. Severe Weather Forecasts. These provide warnings of weather conditions that will create unusual difficulties. Examples of severe weather include tropical cyclones, thunderstorms, strong and gusty surface winds, heavy precipitation, and extremes of temperature. The Air Weather Service furnishes such warnings when requested by commanders, based upon the needs of their particular unit or installation. The weather conditions that will be critical vary with the type of unit or installation. For example, one unit may require warnings of winds in excess of 15 to 20 knots, but another may not be adversely affected by wind until the speed reaches 35 to 40 knots or more.

34. Weather Intelligence

a. Dissemination. Timeliness is the critical factor in disseminating weather reports and forecasts. Normally they are transmitted by radio or teletype. Weather information is incorporated in such documents as the intelligence estimate, periodic intelligence report, analysis of area of operations, and the intelligence summary.

b. Responsibility of Intelligence Officer. The intelligence officer at corps and lower levels is responsible for determining the weather information requirements and submitting them to

the Air Weather Service personnel. He informs subordinate units of the weather data required by the Air Weather Service and instructs them in the procedure for collecting and forwarding the data. He disseminates the received weather information and coordinates with G3/S3 in the weather training of subordinate units.

c. Requirements. Weather requirements are of two types—those established by the Army and passed to the Air Weather Service for action, and those established by the Air Weather Service and passed to the Army for action. The intelligence officer coordinates all activities directed toward satisfying these requirements. At division and higher levels this coordination is effected through the Air Force Staff Weather Officer, a special staff officer at those echelons. Below division, the intelligence officer requests Air Weather Service support through intelligence channels. Army weather requirements may include climatic information to be used in the planning phase of an entire campaign or operation, weather forecasts, reports of current weather, and weather summaries. Under conditions of nuclear warfare, timely and accurate weather data, particularly that concerning upper air wind speeds and direction, is essential in fallout predictions. Fallout predictions are required both for friendly and enemy employment of nuclear weapons.

d. Requests. Requests for specific weather information received by the intelligence officer are evaluated to determine whether or not the information can be secured by organic agencies before they are forwarded to the Air Weather Service. In all cases, before forwarding the request the intelligence officer insures that requests from various units do not overlap and that they cannot be fulfilled from information already available.

e. Information Sources. Weather data required by the Air Weather Service from Army units may be secured by artillery meteorological sections, Chemical Corps units, Army aviation, and forward combat troops. Artillery meteorological sections are capable of making winds-aloft observations and of determining upper air pressure, temperature, and humidity. In addition, they measure and report data for fallout prediction and use by the Air Weather Service. This information is transmitted every 3 hours. Chemical Corps smoke battalions can furnish information concerning surface winds and temperature. The pilots of Army aircraft are capable of reporting weather conditions within their area of flight operations. Forward combat units can provide weather data obtained by visual observation, and if required, they may be equipped with instruments for obtaining additional weather data.

f. Interpretation. An intelligence officer does not merely disseminate verbatim the weather forecast received from higher headquarters. He must interpret it in relation to particular operations. He also receives interpretations from such special staff officers as the chemical officer (toxic chemical interpretations and interpretations relative to fallout predictions and travel of fallout clouds), the aviation officer, and the Staff Weather Officer. The weather information that he transmits to the command must be presented in its most usable form, with the operational aspects of the data indicated whenever applicable.

35. Effects of Temperature

a. Temperature. Periods of freezing temperatures will increase the trafficability of some soils, while with others it may create ice sheets on roads, making movement more difficult. Thawing temperatures may make frozen soils difficult to traverse and may damage roads with poor foundations. The ability of projectiles to penetrate the earth is decreased by frozen soil, but freezing increases the casualty effect of contact-fuzed shells. Melting snows may cause floods and in mountain areas result in avalanches.

b. Inversions. Temperature inversions create an exception to the normal decrease in temperature that occurs with increases in altitude. In a temperature inversion, the air nearest the ground is colder than the overlying air. The lower air remains stable. Dust and smoke remain near the ground, reducing visibility and air purity. Inversion conditions are favorable to either enemy or friendly employment of toxic chemical or biological agents. Radar beams may also be refracted or ducted due to inversions.

c. Site Selection. In selecting sites to provide protection against low temperatures in the

northern hemisphere, preference should be given to the southwesterly slopes of hills and mountains, where the temperature usually is higher than on other slopes. Cold air flows downslope and remains pocketed in inclosed drainage areas or is dammed by forests or other barriers. These cold air pockets have the lowest temperature of the terrain, and often are characterized by freezing or fog when adjacent areas are frost-free or clear. In areas of frequent calm or near calm conditions such cold air drainage areas should not be selected for troop bivouacs or for such facilities as motor pools and hospitals. In hot climates, caution is required in utilizing cold air pockets, since they are likely areas for the formation of ground fog and excessive humidity. In windy areas, on the other hand, these pockets provide shelter from the chilling effects of the wind. Areas susceptible to cold air drainage can be readily located by ground reconnaissance or from topographic maps by visualizing the flow of cold and dense air over the terrain. In general, concave land surfaces facilitate the accumulation of cold air, and convex surfaces favor drainage of air from the surface. Toxic chemical and biological aerosols also tend to collect in depressions and low places. In areas where heating is required, careful selection of the terrain in locating bivouacs and other installations will save fuel. If temperature data are available for various possible sites, or can be estimated by altitude factors and terrain configuration, fuel requirements may be closely ascertained. Toxic chemical agents vaporize more rapidly in high ambient temperatures than in low ambient temperatures. The effects of weather on toxic chemical and biological agents, and on radiological contamination, are discussed in FM 3–5 and TM 3–240. Temperature has no significant effects upon the intensity of blast or the thermal radiation of nuclear weapons.

36. Winds

a. Description. In arid or semiarid areas, strong winds frequently raise large clouds of dust and sand which greatly reduce observation. Similar effects result in snow-covered regions, where blowing snow may reduce visibility over wide areas. Observation aircraft may be grounded entirely during such periods. The speed and direction of the wind are prime considerations in areas contaminated by toxic chemical agents, biological agents, and radiological fallout. Winds of 5 to 16 kilometers (3 to 10 miles) per hour provide the most favorable conditions for the employment of contaminating agents. Winds below or above that range cause a loss of effectiveness in the use of gas, smoke, chemicals, radioactive clouds, and mists. The direction of the wind must be considered for the protection of friendly troops. In areas characterized by great turbulence and variable winds the use of contaminating agents is highly dangerous.

b. Projectiles. Winds tend to deflect projectiles from their normal paths, particularly when they are fired at long ranges. The effect that wind will have on a projectile increases with an increase in the velocity of the wind and the size of the projectile. To obtain accuracy in artillery fires, the direction and velocity of the wind must be known in order to apply compensating corrections to firing data. Winds also affect the efficiency of sound-ranging equipment.

c. Parachute Landings. Parachute landings are feasible in winds up to 25 kilometers (15 miles) per hour. At higher velocities, the wind tends to scatter troop concentrations, to foul equipment, and increase the number of casualties from landing accidents. Strong winds also increase the time that parachutists must remain in the air, as well as the time required to secure equipment and prepare for combat after landing.

d. Amphibious. Strong winds hinder amphibious operations by creating high seas which will prevent landing craft from landing or retracting.

e. Nuclear. Wind speed and direction have no influence upon the blast or thermal radiation effects of nuclear weapons, nor upon the range of the initial nuclear radiation. Winds at all atmospheric levels are significant factors, however, in determining the location of radiological fallout resulting from the surface, subsurface or airburst of a nuclear weapon. Contaminated dirt and debris carried upon the column and cloud will be deposited downwind.

f. Aerosols. The effectiveness of toxic chemical and biological agent aerosols is influenced

by the direction and speed of the wind. Such aerosols are dissipated rapidly in high winds. The use of toxic chemical agents in vapor form is most effective on clear or partially clear nights when the air usually is most stable.

g. Radar. Strong winds can damage radar antennas or even prevent use of the radar.

37. Effects of Humidity

a. Ballistics. The effects of humidity upon ballistics are important because of the relationship of humidity and density. The amount of water vapor in the air affects the trajectory of projectiles by the influence that it has upon air temperature and density. Humidity also has an effect upon the distance that sounds travel, thus affecting sound-ranging operations. Humidity does not seriously decrease the effectiveness of most toxic agents and may increase the effectiveness of some, such as blister gas. The effectiveness of some biological agent aerosols may tend to be increased by moisture in the air since living organisms are affected adversely by dry air and direct sunlight.

b. Smoke. In the use of a screening smoke, a humidity of 90 percent will have twice the obscuring effect of a humidity of 40 percent. With this increase in relative humidity, only one-fourth of the amount of smoke-producing material need be used.

c. Nuclear. Humidity has no influence upon the blast effect or nuclear radiation of a nuclear weapon and no direct effect upon thermal radiation intensities. It will affect target vulnerability to a degree, because it will determine the moisture content of clothing, structures, equipment, and vegetation and their susceptibility to ignition. This effect is pronounced, however, only when a very high or very low relative humidity has prevailed over a long period.

38. Cloudiness

a. Effects. Daytime cloudiness reduces the amount of heat received from the sun at the earth's surface, slowing down the drying of roads and affecting the trafficability of soils. Extensive night cloudiness prevents the loss of heat from the earth's surface due to radiational cooling and results in higher nighttime temperatures. Cloudiness chiefly affects air operations by limiting aerial observation and reconnaissance. Dense clouds above the camera level may reduce light intensity to the point that photography becomes difficult or impossible. A high, thin layer of clouds, on the other hand, may eliminate ground shadows and thus improve the quality of aerial photographs. In cloudy areas, close combat air support may be prohibited or restricted to aircraft equipped with suitable navigation instruments.

b. Searchlights. Low-lying clouds may be used to advantage by reflecting searchlight beams to illuminate the ground surface. Any considerable degree of night cloudiness reduces the amount of moonlight that reaches the ground. If the fullest utilization of twilight periods is desired, the extent of cloud cover must be considered.

c. Nuclear. Clouds have no influence upon the blast effect of nuclear weapons that are burst below them, nor do they affect nuclear radiation, but they may affect the intensity of thermal radiation reaching a target. If a weapon is burst above or within a continuous cloud layer over the target, a large portion or all of the thermal radiation may be attenuated, with a serious loss of effect. The amount of loss will depend upon the thickness and continuity of the cloud layer and the position of the burst with respect to it. If a weapon is burst below a continuous or nearly continuous cloud layer, some of the thermal energy may be reflected from the cloud layer downward on the target area, enhancing the total thermal effect.

39. Rainfall

a. Amount. When planning extended operations, the average amount of precipitation occurring in the proposed area must be considered. An area with 50 centimeters (20 inches) or less of rainfall in a year normally will not have adequate supplies of water for military purposes. Rainfall of 50 to 200 centimeters (20 to 80 inches) a year presents no serious problems in operations, other than those that occur in rainy seasons through localized flooding and poor soil trafficability. Annual rainfall in excess of 200 centimeters (80 inches) generally hinders normal operations during the seasons that the greater amount of this rainfall occurs. The seasonal and daily cycle of precipitation (fig. 6) affects the scheduling of military activities. Seasonal distribu-

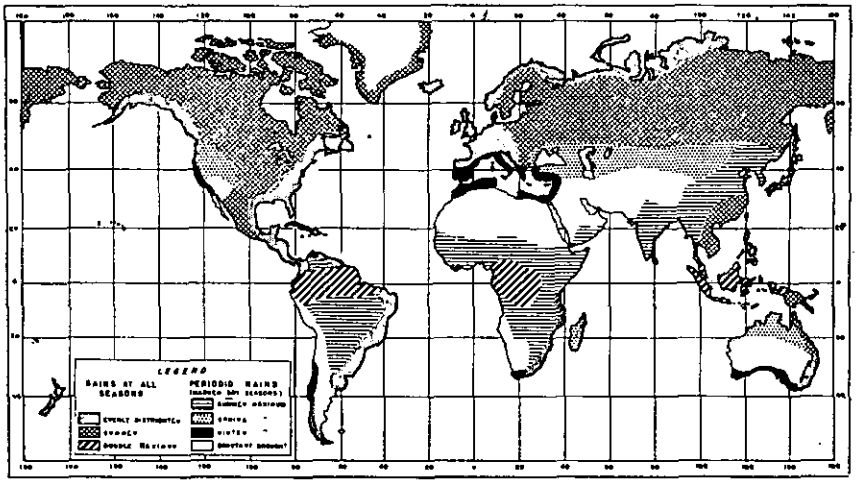


Figure 6. Seasonal distribution of rainfall.

tion may be uniform throughout the year or it may occur in distinct wet and dry periods. In the monsoon areas of southeast Asia, for example, the rains come suddenly and with such violent downpours that some military operations must cease almost entirely, and plans must be revised. During rainy seasons in most tropical or semitropical areas, there usually are predictable periods of maximum rainfall occurring at certain times of the day which must be considered when planning construction work or tactical activities. The maximum rate of precipitation expressed in inches per day or hour may also be critical in designing culverts or other facilities for draining excess water.

b. Trafficability. Precipitation affects soil trafficability and hence cross-country movement. In areas of seasonal precipitation, the cross-country movement characteristics of an area may change drastically each season. Seasonal floods may swell or flood streams, making fording and bridging operations difficult or impossible. Snow and sleet hamper movement on roads in winter, often making them impassable in mountainous areas. The snow that accumulates in mountains during the winter months frequently affords a water supply throughout the year to lower, drier regions.

c. Visibility. Precipitation usually has an adverse effect on visibility and observation, although rain sometimes may wash excessive impurities from the air. Rain and snow aid concealment, and may facilitate surprise attacks. Operation of listening and sound-ranging posts is often limited by precipitation.

d. Neutralization. Rain and snow normally reduce the effectiveness of toxic chemical and biological agents. Heavy or lasting rain washes away these agents and may neutralize them. Snow may cover liquid toxic agents so that little vapor or contamination hazard appears until the snow melts. Heavy precipitation will tend to dilute the concentration of biological agent aerosols.

e. Communication. Precipitation may have an adverse effect upon communications, reducing the range of field wire circuits and producing radar "clutter" which tends to obscure target echoes.

f. Nuclear. Precipitation has a significant influence upon the blast effect of a nuclear weapon, but no effect upon initial nuclear radiation. It affects the range of thermal intensity to the degree that it reduces visibility. Buildings, equipment, debris, vegetation, and other normally flammable elements will require higher thermal intensities for ignition, and the spread of primary or secondary fires will be limited. Residual radiation may be affected. If the radioactive particles formed in an airburst are ingested into rain-bearing clouds, the nuclear cloud (if it does not rise above the rain-bearing clouds) will become so mixed with the rain cloud that it will become an integral part of the rain-producing system. The radio-

active material will be deposited with the rain over a large area. Heavy rain over an area would wash away some of the material from a contaminating burst, either air, surface or subsurface, possibly concentrating it in other areas where there are watercourses, low ground, drainage system, or flat undrained areas.

Section II CLIMATE

40. Definition

a. Elements. Climate (fig. 7) refers to the general variation and pattern of the primary climatic elements which include temperature, precipitation, humidity, winds, and air pressure. It is a composite or generalization of the day-to-day weather at a given place or area over a long period of time. The strength and direction of winds, amount of precipitation, and average temperatures (figs. 8 and 9) that will prevail in an area can be approximated, based upon statistics compiled for previous years. These climatic elements may be described by graphs or charts in terms of means, ranges, average maximums and minimums, extremes, and frequencies of occurrence.

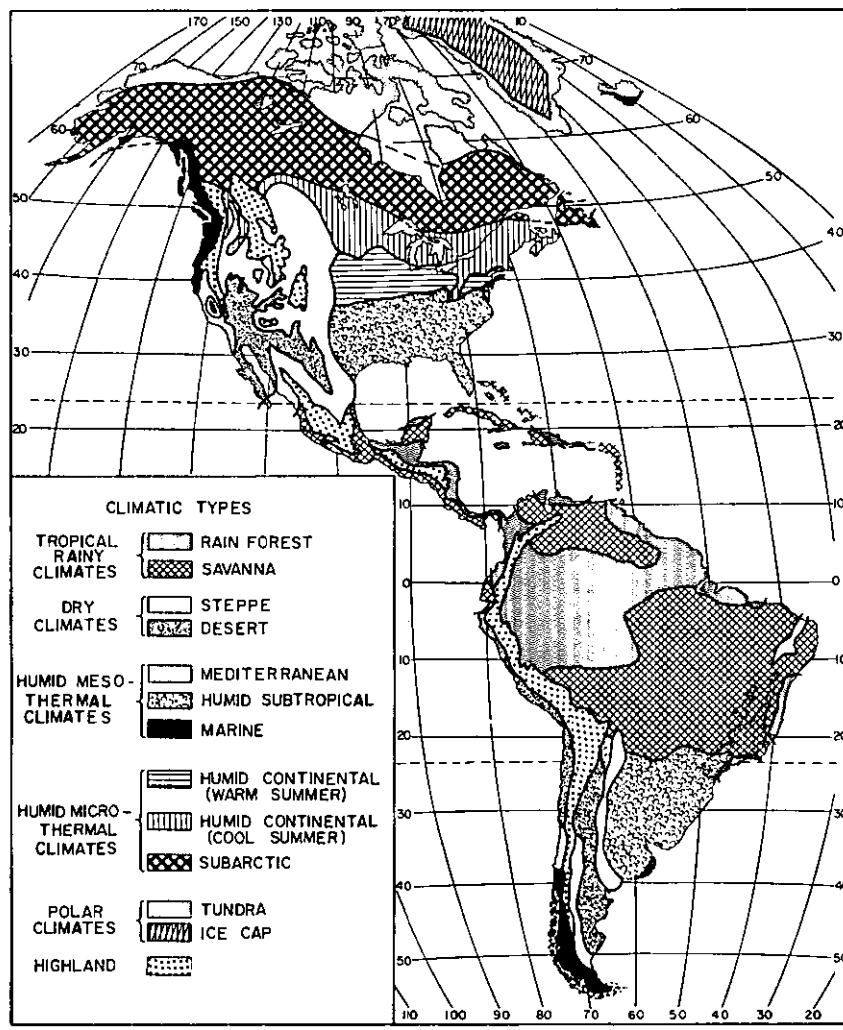


Figure 7. Major climate regions.

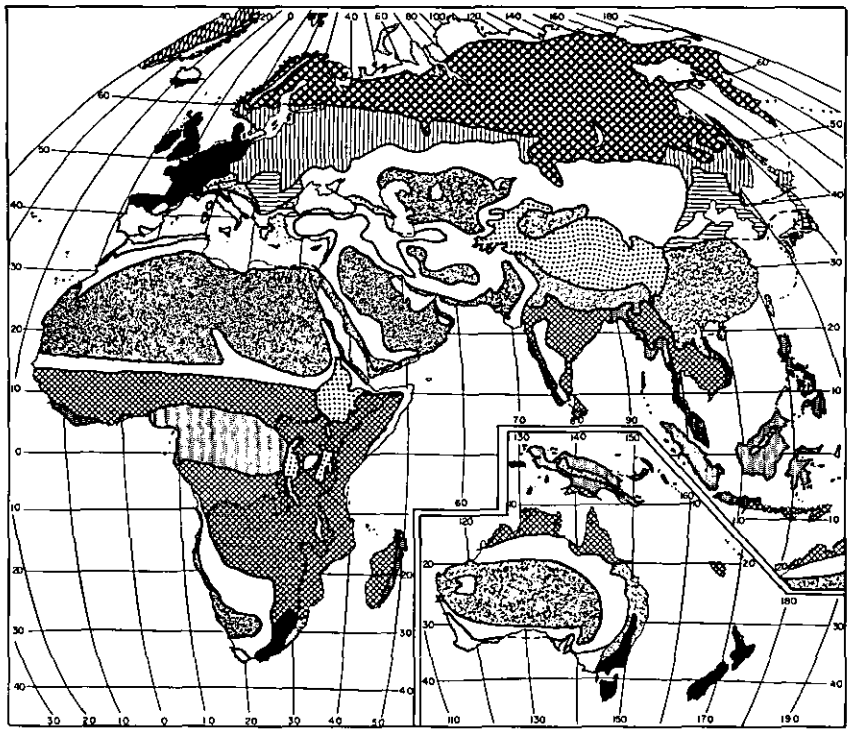


Figure 7—Continued.

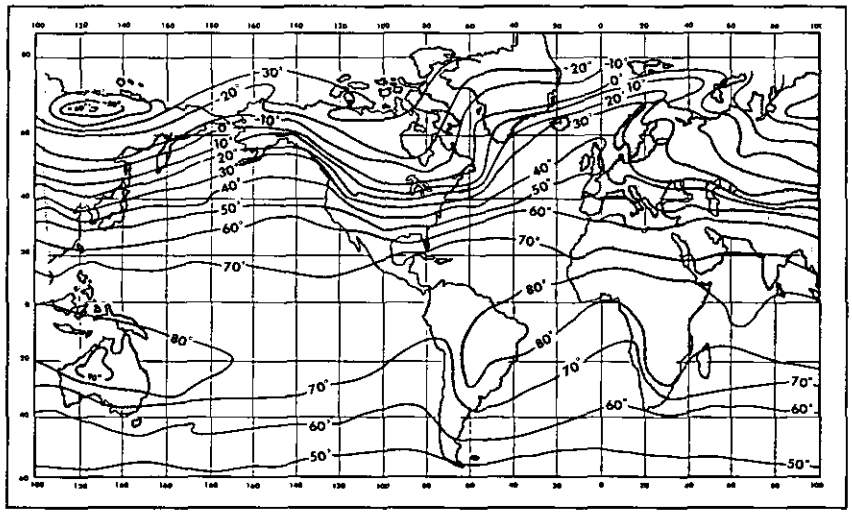


Figure 8. World temperatures in January.

b. Terrain. Although the heat transmitted by the sun to the earth is the dominant factor in weather and climate, terrain has a major effect upon the climate in many regions. High mountains can block the movement of air masses and act as climatic divides. Terrain can also effect differences in climate between land and ocean areas, where the land has higher summer temperatures and lower winter temperatures than the adjacent body of water. Local terrain influences may also be highly significant in military operations. The ground configuration often strongly affects the pattern of occurrence of fog, surface winds, and other

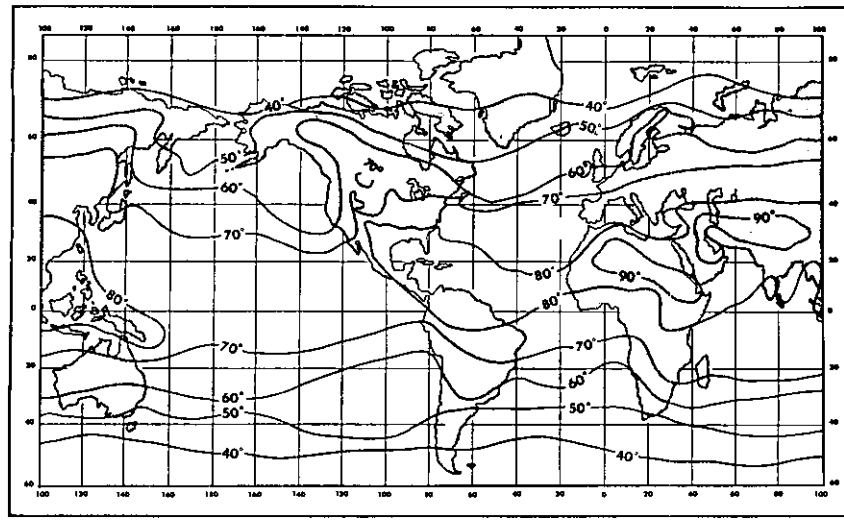


Figure 9. World temperatures in July.

conditions. Information about these local conditions frequently can be obtained only by the analysis of topographic maps, ground reconnaissance, and the interrogation of inhabitants.

c. Plants. The influence of climate on the growth of plants is a predominant factor in their distribution, and the relation between soil formation and climate is so close that the pattern displayed by a soil map will provide an indication of the climatic conditions.

41. Tropical Rainy Climates

a. Rain Forest Climate. The tropical rain forest climate occurs in a belt generally extending from 5° to 8° on either side of the Equator. In some regions, such as the Amazon Basin and the Congo Basin, the air is always hot and damp, there are frequent torrential rains of short duration, and the winds are feeble or absent for long periods of time. This climatic type is also found on windward coasts, where, between latitudes of 5° and 25°, easterly trade winds blow almost constantly over hills or mountains. The cooling of these winds as they rise over the barriers produces an extremely heavy rainfall. This occurs, for example, in portions of Hawaii, the Philippines, the eastern coasts of Central America, Brazil, Madagascar (Malagasy), and most of the islands in the southern Pacific Ocean. In this type of climate, the rays of the sun are nearly vertical most of the time, so that days and nights are practically equal in length throughout the year. Night temperatures usually are a few degrees lower than daytime temperatures. There are no clearly marked seasons. Relative humidity is high at all times, and cloudy weather prevails. There are heavy rains on at least 4 or 5 days each week during the rainiest months, with the greatest amounts during the periods when the sun is most directly overhead. The rains are torrential, often accompanied by thunder and lightning. Ordinarily the rain begins in the afternoon, when the heated air is rising most rapidly, and ends before nightfall, although occasionally a light rain will continue into the night.

b. Savanna Climate. The tropical savanna climate occurs generally in the regions from 5° to 15° on either side of the Equator, between the dry climates and the tropical rain forest regions. Instead of the dense forests typical of the tropical rain forest climate, the savanna regions have more open forests and large areas covered with tall grasses. Savanna regions have high temperatures, with annual ranges (difference between mean temperature of the warmest and coldest months of the year) varying between 5° and 15° F. The total amount of rainfall is less than that of the tropical rain forest climate. There are distinct wet and dry seasons, and usually the rainy season begins and ends with squalls and violent thunderstorms. During the rainy season, periods of intensely hot sunshine also alternate with

brief, violent deluges of rain. The amount of rainfall varies considerably, so that there are years of drought and years of flood. In the dry season the weather resembles that of desert regions, with very little rainfall. Trees lose their leaves, many small streams are dry, and the soil becomes hard and cracked. Visibility is greatly reduced by dust and the smoke from grass fires.

c. Monsoon. In certain parts of southern and southeastern Asia, the climate is greatly influenced by monsoon winds. The wet and dry seasons coincide respectively with the onshore and offshore winds.

42. Dry Climates

a. Description. Dry climates are those in which the evaporation rate exceeds the precipitation rate. The dry climates are located on the leeward interior portions of continents. There are two subdivisions: the arid or desert type, and the semiarid or steppe type. In general, the steppe is a transitional region surrounding the desert and separating it from the humid regions. Dry climates are characterized by extreme seasonal temperatures with large annual ranges. Daily ranges also are high. Humidity is relatively low, averaging from 12 to 30 percent around the middle of the day. Generally the skies are clear and cloudless. Because vegetation is meager, the barren surface of the dry earth becomes very hot during the day and cools rapidly at night. The vegetation offers little friction to the moving air, and accordingly, strong, persistent winds are typical of desert regions.

b. Low-Latitude Desert Climates. These occur in the vicinity of 20° to 25° north or south, with the average positions of their extreme margins at approximately 15° and 30°. The Sahara and Australian Deserts are typical examples of this type of climate. In these desert regions, rainfall is not only small in amount, but erratic and uncertain. However, infrequent heavy showers may turn dry streambeds into raging torrents. Often there is no rainfall for several years, and the skies are almost always clear and cloudless.

c. Low-Latitude Steppes. These are semiarid, having a short period of rain-bearing winds and storms each year. Precipitation, however, is meager and erratic. Steppe regions on the poleward sides of deserts have almost all their annual rainfall in the cool season. Those adjoining savannas on the equatorward sides of deserts generally have a brief period of relatively heavy rains during the time when the sun is highest.

d. Middle-Latitude Dry Climates. These occur within the deep interiors of continents, in the regions surrounded by mountains or plateaus that block the humid maritime air masses. Rainfall is meager and undependable, as in the low-latitude deserts, but there is also a season of severe cold. In winter there may be a small amount of snow, frequently accompanied by strong winds. The temperature and weather characteristics are similar to those of humid continental climates in comparable latitudes, except that there is less rainfall. The area immediately to the east and west of the Caspian Sea is a typical example of this climate.

e. Middle-Latitude Desert Climate. This climate is characterized by lower temperatures and precipitation than low-latitude desert climates. This climate occurs in the basinlike, low-altitude areas, surrounded by high-land rims, that exist in some continental interiors. The Great Basin of the U.S. and the Turkestan Basin of Asia have this type of climate. Summer temperatures are high. Middle-latitude steppes occupy intermediate locations between deserts and humid climates. They have small amounts of rainfall, which is usually unpredictable in amount or time of occurrence.

43. Humid Mesothermal Climates

a. Description. These climates are characterized by moderate temperatures that occur in a seasonal rhythm. They are divided into three general categories—Mediterranean climate, humid subtropical climate and marine west coast climate.

b. Mediterranean Climate. This climate has hot, dry summers and mild winters, during which most of the annual precipitation occurs. Annual rainfall usually ranges from 38 to 64 centimeters (15 to 25 inches). In the winter months, the average temperature is usually between 40° and 50°F.; in the summer, it ranges generally from 70° to 80° F. This type

of climate occurs in five regions—the borderlands of the Mediterranean Sea, central and coastal Southern California, central Chile, the southern tip of South Africa, and parts of southern Australia. Coastal areas often have a modified type of Mediterranean climate, with cool summers accentuated in some areas by the cool ocean currents offshore. There is apt to be a cool daily breeze along the seacoast and for a short distance inland. Relative humidity is high. Fogs are frequent, but usually are dissipated by the heat of the sun in the early morning hours. Winters are mild and frost infrequent, and the annual change in temperature at some locations is uncommonly small. Summer days in Mediterranean climates are warm to hot, with bright sunshine, low relative humidity, and nearly cloudless skies. Daily weather becomes erratic and unpredictable in autumn. The winds are less regular and there is occasional rain. Temperatures remain relatively high. Winters are mild and warm, with occasional frosts and relatively abundant rainfall.

c. Humid Subtropical Climate. This climate occurs in regions located on the eastern sides of continents, generally from about latitude 25° poleward (north or south) to 35° or 40°. This type of climate is found, for example, in the American Gulf States. Temperatures are similar to those of the Mediterranean climate, with less contrast between regions on the coast and those located inland. Rainfall ranges from 75 to 165 centimeters (30 to 65 inches) a year at most locations. In the summer, humidity is high, temperatures average from about 75° to 80°F. in the hottest month, and there are frequent thundershowers. Nights are hot and sultry. There is no drought season, but normally there is less rain in winter than in summer. Severe tropical cyclones occur most frequently in the late summer and early fall. Winters are relatively mild in this type climate. Temperatures in the cool months usually average between 40° and 55°F. with the midday temperature around 55° to 60°F. and the night temperature from 35° to 45°F. The high humidity, however, makes the nights chilly and uncomfortable. Snow may fall occasionally, but it does not remain for more than 2 or 3 days. Daytime temperatures may be raised above 60° or 70°F. by the arrival of a tropical air mass, then be reduced by a subsequent polar wind as much as 30° F. in 24 hours, resulting in a severe freeze.

d. Marine West Coast Climate. This climate occurs on the western or windward sides of continents, poleward from about 40° latitude, and results from onshore westerly winds that blow over the land from adjoining oceans. It borders the Mediterranean type on its equatorward margins, extends into the higher middle latitudes and ends at the subarctic or tundra climate. Where mountains are closely parallel to the west coast, as in Scandinavia, this type of climate is confined to a relatively narrow region on seaward side of the highlands. In parts of western Europe, where there are extensive lowlands, the effects of the ocean conditions have an influence on the climate for many miles inland. Summers are cool with occasional hot days but no severe or prolonged heat waves. Rainfall is fairly abundant. Winters are mild, particularly in western Europe, where a great mass of warm water known as the North Atlantic Drift lies offshore. Cloudy skies and a humid atmosphere are prevalent. There are frequent severe frosts. The midday temperatures of most winter days are relatively high. During unusually cold periods, temperatures may remain below freezing for several days. The winter season is marked by severe storms, fogs, and mist. Where the western coasts are bordered by mountain ranges, as in Norway and Chile, precipitation may reach a total of 250 to 380 centimeters (100 to 150 inches) a year. In areas consisting predominantly of lowlands, rainfall usually averages from 50 to 90 centimeters (20 to 35 inches) a year and may fall steadily for several days at a time. In mountainous regions, such as the Cascade Range or the Scandinavian Highlands, snowfall is very heavy. The marine west coast climate is cloudy, and has mist or fog for at least 40 days a year at many locations.

44. Humid Microthermal Climates

a. Types. The humid microthermal climate occurs in the Northern Hemisphere northward from the subtropical climatic regions and in leeward interior locations. Latitudinal spread is from about 40° N to 60° or 65° N. It has colder winters than the mesothermal type, with larger annual changes of temperature,

longer frost seasons and snow cover that lasts for considerable periods. Humid continental and subarctic are the principal types of microthermal climate.

b. Humid Continental Climates. These climates border the marine west coast climatic regions. Where there are mountain barriers, as in North America, the change between the two types of climate is abrupt, but it is very gradual where there are no barriers, as in the lowlands of western Europe. Seasonal differences are extreme, with very cold winters and warm to hot summers. Along the seaboard, the summer heat is oppressive and sultry because of the higher humidity, and the winter cold is more raw and penetrating than in the drier interior regions. Along the interior margins, humid continental climates border upon the dry climates and have subhumid characteristics. The prairies of North America and interior Eurasia are examples of such climatic regions. In these areas, the maximum rainfall usually occurs in late spring and early summer, rather than at the time of greatest heat. In winter, regions with a humid continental type of climate normally have a permanent snow cover that lasts from a few weeks to several months. Summer rains usually occur in sharp showers accompanied by thunder and lightning. Winter in the prairie regions is characterized by frequent changes in weather conditions, with occasional blizzards, known as burans. A blizzard is marked by violent gales, drifting snow, and extreme cold. Although there may be no precipitation falling, the air is filled to a height of several hundred feet by swirling masses of dry, finely pulverized snow. Afternoon thunderstorms frequently occur during summer in prairie regions.

c. Southern Margins. Regions on the southern margins of microthermal climates have long, hot, and humid summers lasting from 150 to 200 days between the periods of frost. Winters are cold, with frequent intervals of mild, rainy weather.

d. Winter. Winter is the dominant season on the poleward side of regions with this type of climate. Summers are relatively short, usually comprising a period of about 5 months. Temperature changes of as much as 40° F. in 24 hours are common in spring and autumn.

e. Subarctic Climate. This climate occurs in latitudes of 50° to 60° in the Northern Hemisphere. The Eurasian region extends from Finland and Sweden to the Pacific coast of Siberia, and in North America, the subarctic stretches from Alaska to Labrador and Newfoundland. Long, extremely cold winters and very brief summers characterize this type of climate. Winter quickly follows summer, with only a short period of autumn intervening. A large part of these regions are frozen to a considerable depth, with only a few feet of the upper part thawing out in the summer. There is little precipitation in subarctic regions. No more than 40 centimeters (15 inches) a year falls over the greater part of the Siberian area. In most of subarctic Canada the precipitation is less than 50 centimeters (20 inches) annually. Precipitation exceeds 50 centimeters (20 inches) chiefly along the oceanic margins of Eurasia and North America.

45. Polar Climates

a. Location. The poleward limit of forest growth usually is considered the dividing line between polar climates and those of intermediate latitudes coinciding with a line (isotherm) connecting points having a temperature of 50°F. for the warmest month. A mean annual temperature of 32°F. or below is also a distinguishing feature of polar climates. In the Southern Hemisphere, the only large land area with a polar climate is the Antarctic continent. In the Northern Hemisphere, this climatic region includes the Arctic Sea, the borderlands of Eurasia and North America, with the island groups that are north of these continents, and ice-covered Greenland. The Arctic is almost a landlocked sea and the Antarctic is a seagirt land with important climatic differences between them. The climate has fewer wide variations in the Antarctic because it is a single land mass surrounded by oceans with a uniform temperature.

b. Temperature. Polar climates have the lowest mean annual and summer temperatures and although the sun remains above the horizon for 6 months of the year, the rays are too oblique to raise the temperature significantly. Much of the energy from the sun is reflected by snow and ice, and is consumed in melting the snow cover and evaporating the

water. As a result neither the land surface nor the air adjacent to it becomes warm.

c. Precipitation. Precipitation averages less than 25 centimeters (10 inches) a year over large parts of the polar land areas. Because of the low evaporation and small amount of melting, permanent ice fields several thousand feet thick have accumulated on Greenland and the Antarctic continent.

46. Tundra and Icecap

a. Tundra. Polar climates usually are divided into two types—icecap and tundra. Icecap climates are those where the average temperature of all months is below 32° F., vegetation will not grow, and a permanent snow-and-ice cover prevails (figs. 10 and 11). When one or more months in the warm season have an average temperature above 32°F. but below 50°F., the ground is free from snow for a short period and low sparse vegetation is possible. This climate is designated as tundra. It is less rigorous than that of the icecap regions. The warmest month isotherms of 50°F. on the equatorward side and 32°F. on the poleward side are considered to be the boundaries. Over land areas, tundra climate is confined largely to the Northern Hemisphere. Ocean prevails in those Antarctic areas where the tundra climate normally would be found. Summers warm enough to develop a tundra climate occur only in the most northerly fringes of the Antarctic and on certain small islands of the region. The most extensive tundra areas are on the Arctic Sea margins of Eurasia and North America. Long, cold winters and brief, cool summers characterize the tundra climate.

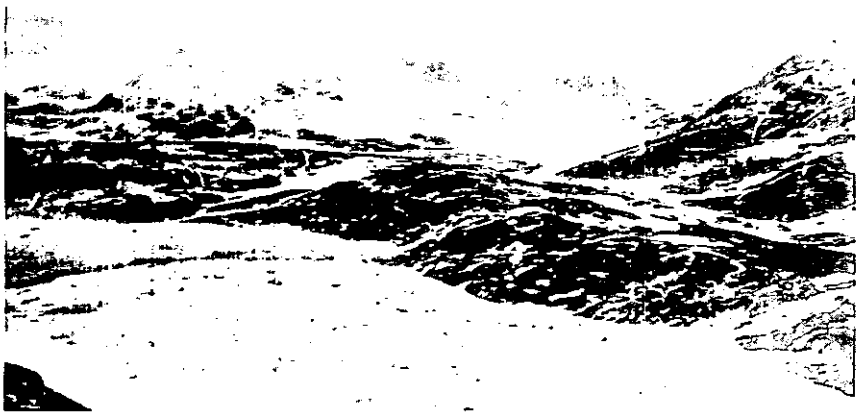


Figure 10. Arctic terrain.

b. Temperatures. Average temperatures usually are above freezing only for from 2 to 4 months of the year, and killing frosts may occur at any time. Fog is prevalent along the coast, frequently lasting for days at a time. Snow cover disappears for 1 or 2 months during the summer season, and the lakes usually are free from ice. Drainage is poor because of the permafrost, resulting in many bogs and swamps. Summer temperatures do not differ greatly in the various tundra regions. There is, however, a considerable variation in winter temperatures. Average temperatures in the Arctic coastal areas of Siberia average about −35° to −40°F. in January and February, with even lower temperatures inland. Along the Arctic borders of North America, the temperature for comparable periods is higher, and winters are less severe.

c. Precipitation. Annual precipitation normally does not exceed 25 cm to 30 cm (10–12 inches) in the tundra regions, although larger amounts are received in parts of eastern Canada, particularly in Labrador. Usually the most precipitation occurs in summer and autumn, the warmest seasons. Most of it is in the form of rain, with occasional snow. The winter snow is dry and powdery, forming a compact cover.

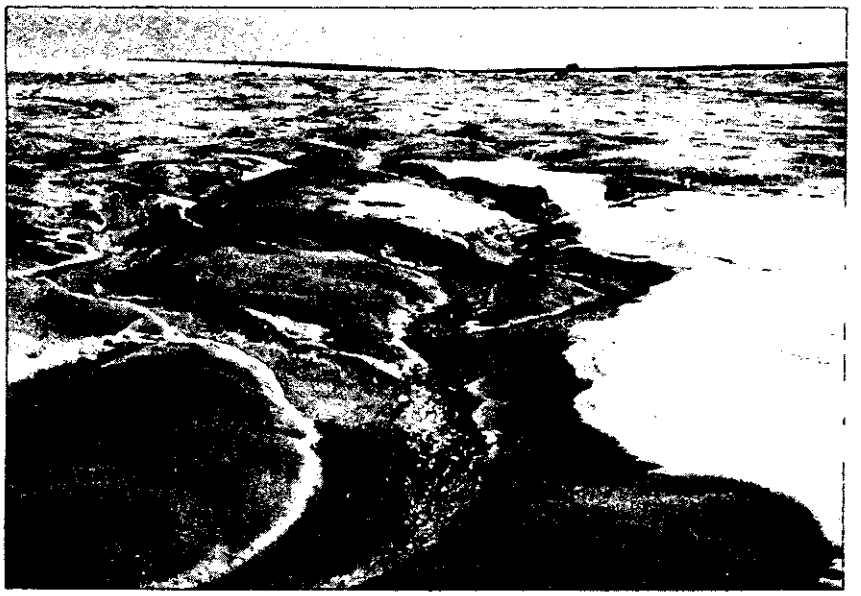


Figure 11. Arctic tundra, showing warm-weather drainage.

Often it is accompanied by strong blizzard winds which pile up the snow on the lee sides of hills and in depressions, sweeping exposed surfaces bare. There is no vegetation to break the force of the wind and to hold the snow cover.

d. Icecap. This climate characterizes the permanent continental ice sheets of Greenland and Antarctica and the ocean in the vicinity of the North Pole. The average winter-month temperatures range from −35° to −45°F. Storms or violent winds do not occur as frequently in the inner portions of the icecaps as in other climatic regions, but in some marginal areas there are extreme gales caused by the precipitous descent of cold air from the continental ice plateau.

47. Climatic Studies

a. Records. Climatic studies are based upon the records of past weather in a given area compiled over a long period of time. They are used in preliminary planning to provide an estimate of the climatic averages that may be expected during the period of the proposed operations. These studies are of particular value in developing new equipment and in anticipating logistical problems. Special climatic studies may be prepared covering winds, rainfall, tides, sea conditions, state of ground, and similar aspects of a specified area. Such studies have been made, for example, to provide data for use in determining—

(1) Location of camps, training areas, depots, and landing fields.
(2) Coastal areas most suitable for amphibious operations.
(3) Operations of aircraft over certain mountainous areas.
(4) Smoke behavior in specified localities.
(5) Seasonal fuel requirements by weight, quantity, and type.

b. Requests. Requests for climatic studies should be made as far in advance as possible, and should provide all pertinent information, including mission, area and time, operational limits, flexibility permitted, and the form of presentation.

Section III. OPERATIONS IN EXTREME CLIMATES

48. Desert Regions

a. Weather. High summer temperatures are normal in desert areas; the summer maximum may reach 120° to 130°F. During daylight hours the thermal action may be so violent that planes cannot operate safely at lower alti-

tudes. The variation between day and night temperatures is great, the temperature often dropping below the freezing point in winter. These sudden changes in temperature occasionally give rise to winds of hurricane force that carry large quantities of dust and sand. Under these conditions, visibility is very poor and movement may be impossible. Climatic conditions in desert areas also increase maintenance requirements of mechanized units. Rain is infrequent in desert regions, usually averaging less than 25 centimeters (10 inches) a year, but it may come in sudden downpours. Water sources are few, and frequently are polluted and brackish. Usually water for military forces must be transported by tank truck, rail, or pipeline from sources outside the desert area. Winds blow almost constantly in the desert, frequently limiting the use of smoke and other chemical weapons. Minefields may be made useless by the blowing dust and sand. The wind either blows away the sand, exposing the mines, or deposits large quantities of it on the minefield, preventing detonation of the mines. In heavy dust and sandstorms, the operations of mechanized units are similar to those conducted at night.

b. Natural Features. There are few landmarks in a sandy desert region. The most prominent features are the huge dunes created by sandstorms (fig. 12). Usually the surface of a sand dune is packed firmly by the wind for a depth of about 5 centimeters (2 inches). This surface will support considerable weight, but detours may be necessary because many of the dunes are high, with steep slopes. Areas of loose sand impede movement on foot or by wheeled vehicles, but tracked vehicles are able to operate in shallow sand. In flat, hard-surfaced areas, roads and trails are not necessary and all types of vehicles can move cross-country. Salt marshes, dry lakes, and wadis (dry streambeds) occur along coastal areas or inland in depressions. Wadis and dry lakes are impassable when wet and contain a powdery silt when they are dry which may cause vehicles to bog down.

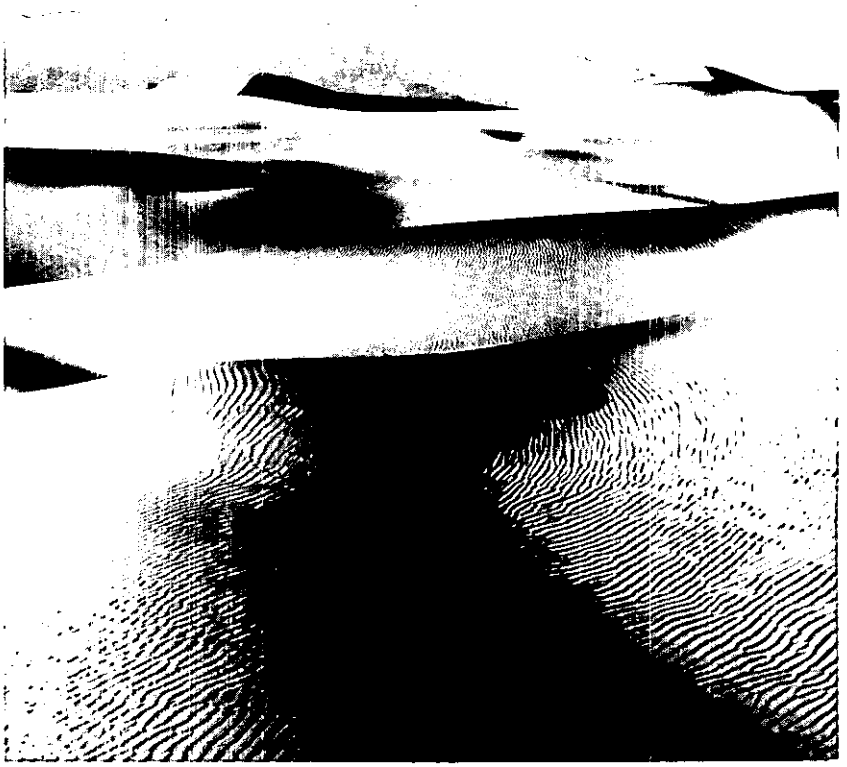


Figure 12. Sand dunes (Death Valley, California).

c. Manmade Features. Well-defined roads are scarce in desert regions, although there usually are trails between water sources. Occasionally flash floods may cut the routes for short periods of time. Dust and sand storms may prevent traffic through lack of visibility and maintenance difficulties. A surfaced main supply route is essential and usually must be constructed. Road location is difficult and time-consuming, requiring extensive map study and area reconnaissance. Buildings must be strong enough to withstand the frequent high winds and constructed tightly to reduce the infiltration of blowing sand and dust. Field fortifications in sand require adequate strengthening, with a maximum use of sandbags. In rocky deserts, field works can be installed only with great difficulty. Field fortifications are easy to dig in sandy deserts, but they must be revetted, and may be filled quickly with drifting sand.

d. Military Aspects.

(1) *Key terrain features.* In desert operations, terrain features usually are not major objectives, since the possession of a particular piece of ground seldom contributes materially to the destruction of the enemy force. Oases and other water sources are always critical, however, because an adequate water supply is a fundamental requirement of military operations in arid or semiarid regions.

(2) *Observation and fields of fire.* The brilliant sunlight of desert areas reflected from the light colored ground surface creates a glare. An observer with the sun to his back may see well, but the glare greatly reduces visibility when he faces toward the sun. He loses his depth perception and will confuse objects which are in shadows or haze. On hot days, a shimmering haze may nullify ground observation at ranges of 450 meters (500 yards) or less, depending on local conditions. An optical phenomenon encountered in desert regions is the mirage, an effect produced by layers of air of varying density across which the observer sees reflections, usually inverted, of some distant object or objects. These occur frequently in summer and are evident in a wide arc which increases as the sun becomes higher in the sky. The effect of a mirage generally is the distortion of objects, particularly in the vertical dimension. This has an adverse effect upon observation, making it particularly difficult to identify vehicles. Distances in deserts are underestimated. Shadows on the light-colored terrain can be seen for miles but tend to distort distant objects. Moonlight in desert areas is much brighter than in other regions and nights usually are very clear, with the haze and glare eliminated. Observation at night may be better than during some periods of the day. In open terrain, sound- and flash-ranging are particularly effective. Artillery observers, however, may find few positions that will allow a commanding view of the terrain. The ability of a weapon to fire effectively in the desert usually is limited only by the range of the weapon and the ability of the observer to adjust fire. There is little vegetation or relief to mask weapons.

(3) *Cover and concealment.* Cover from enemy fire may be afforded by sand dunes, hills, and other irregularities in the desert terrain. Concealment is hard to obtain, since the vegetation is sparse. Camouflage is used more extensively in desert areas than in normal terrain, and reliance must be placed upon artificial means. Camouflage from air or ground observation is extremely difficult to achieve. The movement of troops during daylight is greatly restricted due to the lack of concealment and cover from air attack and troops must be widely dispersed.

(4) *Obstacles.* There are relatively few major obstacles to movement in most desert regions. Although the road net is limited, cross-country movement may be good, varying with the type of surface materials.

(5) *Nuclear weapons.* The ease of dispersion in desert areas avoids a concen-

tration of troops that could provide a profitable target for nuclear weapons. Suitable targets are provided, however, by airfields, communication centers, and supply installations.

(6) *Toxic chemical and biological agents.* Two characteristics of desert regions which limit the employment of toxic chemical agents are the sparseness of vegetation and the extreme variations in ambient temperature. Toxic agents present storage problems because of the wide temperature ranges and the extreme conditions existing during the day. Effective use of toxic chemical agents usually is limited to night. The direct sunlight and dry air which characterize desert regions may present unfavorable environmental conditions for some biological agent aerosols.

(7) *Screening smokes.* Under desert conditions when the winds are still, large-area smoke screening is of considerable importance because of the normal lack of adequate natural concealment and cover.

49. Tropical Regions

a. Weather. Excessive heat and humidity except in tropical deserts characterize tropical regions throughout the year. In the rain forest type of climate, there is little seasonal variation in temperature. The weather is marked by sudden changes, with torrential rains that end abruptly to be followed at once by bright sunshine. Humidity tends to remain high because the vegetation checks evaporation. Although monsoon areas have a dry season, the total rainfall is so great that rain forest vegetation is dominant. High temperatures prevail in the tropical savanna regions, which have distinct wet and dry seasons; but in most of these areas, grass is the predominate vegetation. Both rainfall and relative humidity are high in the wet season, and rainfall is rare and relative humidity ranges from low to high.

b. Natural Features. Military operations in tropical regions are influenced chiefly by the rain forest vegetation. In some areas, such as the Amazon Basin of South America, and in central and west Africa, the rain forest consists of several stories of trees, the foliage of which forms a dense canopy, preventing sunlight from reaching the forest floor, and thus precluding dense undergrowth. In other areas, such as in Southeast Asia and some islands in the Pacific Ocean, where a monsoon climate prevails, the rain forest has a canopy only partly continuous and a dense undergrowth. Rain forest is commonly called "jungle," but the term "jungle" is not recognized as a vegetation type. Terrain covered by the rain forest varies from mountain ranges to low, swampy plains. In Southeast Asia, the Pacific Islands, and parts of Latin America, the rain forest covers irregular terrain. Other rain forest areas, such as those in central Africa and South America, generally are low and level. Some coastal portions of rain forest areas are characterized by mangrove swamps or by open beaches lined with bamboo or coconut groves. Beyond the shoreline there may be paddy fields or pineapple, coconut, sugar cane, or rubber planations. Between these and the rain forest there may be low-lying foothills covered with brush or tall grass. Streams are numerous in rain forest areas, but they are generally muddy and subject to sudden floods. In wet seasons an entire area of flat rain forest may become a continuous swamp. In mountainous areas streams that normally are shallow become torrential shortly after a heavy rain. The characteristics of rain forest terrain and its effects upon military operations are discussed in FM 31–30.

c. Manmade Features. There are few roads or trails in rain forest areas. Usually roads must be constructed, and the use of these is limited to light trucks or light tracked vehicles. Except for coral in some coastal areas, there is a lack of materials suitable for road construction. The dense vegetation, unstable soils, and poor drainage make roadbuilding difficult. To establish and maintain a road net of even minimum standards calls for greater engineer effort than in other types of terrain. Navigable waterways often provide the most efficient routes of communication, although they are highly vulnerable to ambush. Bridges suitable for military loads rarely exist in jungle regions. The construction of bridges is complicated by the frequency and intensity of flash floods, the tendency of some jungle

streams to shift their courses, and the rapid decay of wooden structural members. Engineers must be prepared to repair or replace bridges rapidly at short notice. Aerial trams are useful because of the deep cuts made by jungle streams in hilly or mountainous terrain. Towns and villages in jungle regions rarely provide suitable facilities for military installations. Usually settlements are avoided for hygienic reasons. Excellent anchorages may be found along many tropical coasts, but there are very few water terminals sufficiently developed to be of any value in military operations.

d. Key Terrain Features. In jungle areas, the key terrain features generally are those that provide control of trails, navigable waterways, and beaches suitable for amphibious landings. Possession of the edges of an area of high rain forest could provide observation points, thus giving advantages similar to those derived from the possession of high ground.

e. Observation and Fields of Fire.

(1) *Observation.* In rain forest, the dense vegetation often limits observation to short distances. Usually the canopy in a primary rain forest, which consists of a virgin growth of mature trees, is so thick that it cuts off most sunlight, and visibility is limited to about 20 or 30 meters (20 or 30 yards). Visibility may be limited about 5 meters (5 yards) or less in the secondary forest, which is composed of a second growth that develops when the original forest has been burned off or cut. Rain, clouds, and the steamy exhalation from wet areas also tend to reduce visibility. Because of the limited visibility and the lack of conspicuous landmarks, it is often difficult to locate a ground position from a map. Camouflage from close ground observation is of the greatest importance in the rain forest. In most areas, however, there is less need for artificial camouflage against air observation. Whenever possible, the natural overhead is preserved, since any break in the normally uniform tree canopy is readily noticeable from the air. Because observation is limited, tactical units must employ narrow frontages, reduced distances and intervals between elements, increased patrol activity, and a larger number of liaison parties than required in more open terrain. The difficulties of observation greatly restrict the employment of supporting arms and weapons. Artillery forward observer teams on the ground usually cannot see the burst and must adjust fire by sound spotting and sound sensing methods. Aerial forward observers may be utilized with a higher degree of reliability. Data based on maps or photomaps can be used only to a limited extent.

(2) *Fields of fire.* Since natural fields of fire generally are limited to about 5 or 10 meters (5 or 10 yards), lanes must be cleared. Where the undergrowth is heavy, several days of labor will be required to clear 90-meter (100-yard) fire lanes around a position. In order to avoid revealing weapon positions, a fire lane in dense vegetation usually is in the form of a tunnel from 1 to 3.5 meters (1 to 4 yards) wide, with the overhanging foliage left intact. In rain forest, the most effective weapons are those that can be supplied easily with ammunition and are readily transportable over difficult terrain. Suitable weapons include mortars, machineguns, automatic rifles, and grenades. Armored vehicles cannot move through rain forest unless routes have been prepared. Usually the movement of tanks is limited to beaches, coconut groves, clearings, and improved trails. The principal value of tanks is in the use of their flamethrowers, direct fire weapons, and crushing weight in the destruction of enemy field fortifications. Tanks are highly vulnerable to ambush and close in attack in rain forest terrain. Because the heavy vegetation reduces the ef-

fective bursting radius of artillery shells, weapons of 105-mm or higher calibers must be employed to blast away jungle undergrowth and destroy enemy positions. Artillery pieces should be capable of high-angle fire and should be drawn by tractors or transported by helicopters. Engineer equipment must be available for the improvement of trails, construction of firing positions, and clearing of fields of fire. In some mountainous areas, only pack artillery may be practicable. Air forces are effective in close tactical support of ground elements, but their utility for tactical bombing is less than in other types of terrain. Armed helicopters are used extensively in close support of ground forces.

f. Cover and Concealment. Rain forest provides concealment from air and ground observation and may furnish some cover from small arms fire. The amount of cover given by slit trenches and other field fortifications is often limited by the high water table, which prevents excavating more than a few feet below the surface of the ground.

g. Avenues of Approach. Cross-country movement in rain forest is slow and difficult. Troops may have to cut their way through continuous thick undergrowth or make lengthy detours to avoid impassable swamps. On most trails, troops must move in a column of files, and the average rate of movement rarely exceeds 1.5 km per hour. Usually foot movement may be made most easily on ridges, where the vegetation is more open and the better drainage results in less muddy surfaces. Except for small, fast streams with traversable beds, movement is poorest along the banks of rivers, because of the dense vegetation, mud, swamps, and tributary streams. Even in comparatively dry weather, mud slows down vehicular traffic in the jungles. It may be necessary to supplement motorized transport by the use of helicopters and carrying parties. Jungle roads and trails rapidly disappear unless they are in constant use. Accordingly, maps showing these features seldom are reliable. Air photographs of jungle terrain rarely reveal more than the treetops.

h. Communications. Visual signaling is seldom effective in the rain forest because of the dense growth. The use of messengers is slow and may be hazardous. Wire circuits are hard to install and maintain. The range of radio sets may be greatly reduced by the vegetation, resulting in ranges from 40 to 70 percent less than those considered normal in open or lightly wooded terrain.

i. Toxic Chemical and Biological Agents. Both the weather and terrain conditions in rain forest areas are favorable for the employment of chemical and biological agents. Where the overhead canopy is very dense, however, sprays from aircraft usually are only moderately effective against personnel. The large-scale use of defoliants will increase the fields of fire of weapons, and provide increased observation.

50. Arctic and Subartic Regions

a. Weather. Severe changes in weather are common in arctic and subarctic regions. These changes include shifting periods of severe frosts, mild weather, sudden freezing, snowstorms, strong winds, and dense fogs. Reliable and timely weather forecasts are essential to guard against damage to equipment and installations and to gain any tactical advantages that may be possible by exploiting changes in weather conditions. Arctic operations frequently are hindered by strong winds, which usually occur more often along the coast than in the interior. Wind speeds in excess of 128 kilometers (80 miles) per hour have been recorded at coastal stations. Winds blow continually, and in most areas there are no hills, mountains, or other natural barriers to provide protection. Blowing snow constitutes a serios hazard to flying operations. Winds of 16 to 24 kilometers (10 to 15 miles) per hour will raise the snow several feet off the ground, obscuring such surface objects as rocks and runway markers. The short days and long nights of winter reduce the amount of daylight available for tactical operations and work activities. Nights often are bright because of the illumination of the moon, stars, aurora borealis, and reflections from the snow, so that night movements are possible. The short summer nights permit military operations through the 24-hour period.

b. Natural Features. Following a heavy snowfall, landmarks and other objects become covered, making orientation difficult. Gullies and ditches are filled and obscured so that movement is made more hazardous. The freezing of swamps and lakes may convert obstacles into avenues of approach for the enemy. Warmer temperatures in spring will create thaws and mud in the subarctic, causing rivers and streams to overflow. In mountainous or hilly country, landslides can be expected in the spring, as the result of boulders and smaller rock formations expanding from the warmth of the thawing temperatures.

c. Manmade Features. In the subarctic, routes of communication and transportation are affected by every heavy snowfall and traffic may come to a halt. Strong winds cause snowdrifts requiring a constant clearing of routes, and transportation is slowed greatly by ice and sleet. To avoid these drifts, roads may be routed through woods, where drifts seldom occur, or along the crest of high ground where the snow usually is less deep. In extremely cold temperatures, railroad operation is restricted. Blocked tracks and derailments are frequent; switches often are frozen; snow and rock slides, washouts, and frost heaving damage the lines; and the ice caused by water seepage must be cleared from tunnels before they can be used. Excavation is difficult in either frozen or thawed ground. In frozen ground, handtools are ineffective. Explosives are effective, but they must be employed in quantities greater than required in other terrain. Gravel is easier to excavate than soil, because it has better drainage and accordingly does not freeze as solidly. Foxholes, trenches, breastworks, and emplacements may be provided by digging into the snow or through it into the underlying ground. Snow trenches usually need revetting. In very deep snow, tunnels may be dug to provide concealment. They furnish cover from small arms fire, but do not give protection from artillery fires. The spring thaws in subarctic climates must be considered when planning structures and fortifications. Bunkers, trenches, and other field fortifications must be designed and sited so as to insure good drainage. In the thawing period, roads in low-lying areas and bridges are apt to be washed out. Floating ice will destroy or damage bridges of temporary construction. Runways and landing strips will require considerable maintenance. Airfields that have been improperly designed and constructed may become wholly inoperative for extended periods.

d. Observation and Fields of Fire.

(1) *Observation.* Arctic air is exceptionally transparent, providing visibility over long distances. There is a lack of contrast between objects, however, particularly when they are covered by a layer of new snow. Observation in the Arctic is restricted chiefly by fog, blowing snow, and local smoke. The latter is a serious problem only in the vicinity of larger settlements, where it often accompanies the shallow radiation fogs of winter. A radiation fog results from the radiational cooling of air near the surface of the ground on calm, clear nights. Depth perception is adversely affected by arctic conditions, principally by the extremely clear, dry air, the lack of color differences, and the diffusing effect of light on the crystalline surface of the snow and ice. A hazardous phenomenon that reduces visibility to near zero is the whiteout. When this condition exists, the horizon, shadows, and clouds are not discernible, and only very dark objects can be seen. The amount of light reflected from a snowcovered surface is much greater than that reflected from a darker surface, and accordingly the sun provides greater illumination in the Arctic than in other regions. When the sun is shining, sufficient light is reflected from the snow almost to eliminate shadows except in polar areas where the shadows are quite long when the sun is shining. This causes a lack of contrast, making it difficult for the observer to distinguish the outlines of objects even at short distances. The landscape may appear as a featureless grayish-white field. Dark mountains in the distance may be recognized but a crevasse immediately in front of a mountain may be undetected because of the absence

of contrast. There is good illumination from a full moon, and even the stars create considerable illumination. Only during periods of heavy overcast does the arctic night approach the darkness of other regions. A fog condition peculiar to the arctic climate is ice fog. This is composed of minute ice crystals instead of the water droplets of ordinary fog. Ice fog forms in very cold, still air in a shallow layer next to the ground. It is almost always present at temperatures of −45°F to −50°F in the vicinity of a source of water vapor and remains as long as these conditions persist. Where the smoke from building chimneys contributes water vapor to cold, still air, ice fog may form at temperatures as high as −20°F. When the temperature increases rather than decreases with height through a layer of air, it is termed an inversion. The strong temperature inversions present over the Arctic during winter cause several phenomena that affect observation. Sound tends to carry great distances. Light rays are bent as they pass through the inversion at low angles, often causing objects beyond the horizon to appear above it. This effect, termed looming, is a form of mirage.

(2) *Fields of fire.* The fields of fire of automatic weapons are subject to the effects of wind and snow and the final protective line fires may be rendered ineffective by snow drifts. Impact bursts of high trajectory light artillery, mortar, and hand grenade fires are rendered relatively ineffective by the cushioning effect of deep snow; heavy artillery, however, remains highly effective. The employment of proximity or mechanically timed air bursts and overhead fire usually is advisable. Because of the lack of identifying objects and landmarks on snow-covered terrain, the adjustment of fire is difficult. Registration fire with air observation and by sound and flash is hampered, since the snow obscures projectiles and bursts. A round bursting on impact in deep snow appears as a small white splash, making sensing extremely difficult. Because of the cushioning effects of the snow, mines may fail to detonate. The clear air and snow cover may increase the thermal radiation effect of nuclear detonations in flat terrain and snow shelters will be vulnerable to blast effects. Heavy snow and hard-to-maneuver terrain will slow troops in traversing areas contaminated by induced and residual nuclear radiation. When used in deep snow, impact-detonating chemical ammunition burns in the snow and the chemical agent tends to be smothered by the snow. Toxic chemical munitions produce less vapor concentration because of the low temperature and the smothering effect of the snow. On the other hand, low temperatures increase the persistency of toxic chemical agents in both vapor and liquid form. Decay of biological agents is not as rapid in arctic areas as it is in temperate or tropical areas.

e. Cover and Concealment. The snow-covered terrain offers few features that provide adequate concealment and cover. Tracks in the snow are almost impossible to hide, and dirt on fresh snow can be observed at a great distance. Due to the high visibility, effective camouflage is difficult. Because of the difficulties of concealment, night movements are frequently advisable.

f. Obstacles. During the winter months, the lakes, swamps, and rivers are frozen over and cannot be employed as natural obstacles. Artificial obstacles may be devised by freezing large masses of snow or icecrete (a dense frozen mixture of water, sand, and sometimes, gravel) into desired shapes, or by icing deep drifts. Roadblocks may be made by icing a section of the road, preferably one which the enemy must approach on an upgrade. Tank traps may be devised by cutting the ice on a lake or river, then allowing it to refreeze slightly.

g. Avenues of Approach. Winter is generally the best time to travel in the Arctic and sub-

arctic, since the lakes, streams, and muskeg areas are frozen over. Frozen rivers and water ways often become the best routes of advance and lines of communications during the winter months. In general, most vehicles are immobilized in snow from 1 to 1.5 meters (3 to 5 feet) deep. The consistency of the snow, whether it is dry and loose, moist, or packed, affects the mobility of vehicles to a great extent. Tracked vehicles usually can move at low speeds in packed snow that is no more than 1 meter (3 feet) deep. After a packed snow trail has been formed by the passage of several heavy vehicles, normal speeds may be maintained. A thaw or the passage of a great many vehicles on a relatively warm day will melt the snow surface, resulting in a coating of glare ice. The road then becomes practically impassable to tracked vehicles unless ice cleats are installed on the tracks or the road is sanded. Foot movements are slow in 50 centimeters (20 inches) of snow and impossible in more than 100 centimeters (40 inches) deep without the use of snowshoes and skis. Hard-packed snow, however, is not difficult for troops to negotiate. With reasonable care lakes and streams may be crossed by vehicles in winter. The ice first must be checked for thin spots, cracks, and pressure ridges. During the spring thaws, movement in ice and snow across tundra is difficult and dangerous and cross-country movement is practically impossible. After the snow cover has melted from the ground, both wheeled and tracked vehicles can move relatively freely on it as long as the surface remains frozen. This layer of ground that thaws in the summer and freezes again in the winter is termed the active layer. As soon as the active layer has melted, the tundra cannot support heavy concentrated loads and ordinary vehicles will bog down. Even special-purpose vehicles become roadbound during the thaw period and cannot move across the tundra.

CHAPTER 5

NATURAL TERRAIN FEATURES

Section I. SIGNIFICANCE

51. Definitions

a. Topography. Topography refers to the physical features, both natural and manmade, of the earth's surface. In terrain analysis, the following categories of topographical features are considered: relief, drainage, surface materials, vegetation, special physical phenomena, and manmade (cultural) features. Terrain refers to a consideration of topography in terms of military significance. Weathering and erosion play a major role in shaping natural features (fig. 13). Weathering comprises the effects of the weather elements and erosion includes the action of running water, waves, moving ice and snow, and wind upon rock and soil.

b. Landforms. Landforms are the physical expression of the land surface. The principal groups of landforms are plains, plateaus, hills, and mountains. Within each of these groups there are surface features of a smaller size, such as flat lowlands and valleys. Each type results from the interaction of earth processes in a region with given conditions as to climate and as to kind and structure of rock. The indications of relative elevations given are to afford specific definitions for the purposes of this manual. Other distinctions may be found in other references. A complete study of a landform includes determination of its size, shape, arrangement, surface configuration, and relationship to the surrounding area.

c. Relief. Relief refers to the irregularities of the land surface. Local relief indicates the difference in elevation between the highest and lowest points in a limited area and the size of this area depends upon the purpose for which the surface is being considered. In terrain studies, it is usually five square miles. Relief features are the individual forms of the land surface, such as hills or ridges and major relief features are plains, plateaus, hills and mountains. Minor relief features include:

(1) *High ground*—swells, knolls, mounds, knobs, hummocks, hillocks, spurs, ridges, buttes, mesas, and dunes.

Figure 13. Landforms caused by erosion in arid climate (a) Pinnacle. (b) Butte (Grand Canyon, Arizona).

(2) *Depressions*—gullies, draws, gulches, wadis, ravines, gorges, arroyos, canyons, and basins.
(3) *Breaks in high ground*—saddles, notches, cols, passes, cuts, and gaps.
(4) *Special features*—alluvial fans, talus slopes, talus cones, and boulder fields.

52. Military Operations

a. Influences. Terrain influences strategy and tactics. What aspects of the terrain are most important at any given time will depend upon the particular requirements of the command concerned. Logistic requirements, for example, may emphasize the importance of communication centers, routes and rail nets, and waterways. The tactics of a large-scale campaign may be dictated chiefly by the barriers imposed by major rivers and lakes, mountains, forests, or swamps.

b. Attack. In the attack, the correct use of terrain increases fire effect and diminishes losses. Dominant terrain forms the framework of the system of observation, which in turn directly determines the effectiveness of supporting weapons, the disposition and control of the attacking forces, the selection of objectives, and protective measures. Broken terrain, dense woods, built-up areas, and abrupt changes in elevation hinder the offensive employment of armor but afford cover and concealment for infantry. Open, rolling terrain, although providing little cover and concealment for infantry, is suitable for rapid advances by armored formations. Soil trafficability may be a determining factor in selecting type of attack or an avenue of approach.

c. Defense. The nature of the terrain is a major factor influencing the commander when deciding upon position defense or a mobile defense. When the terrain restricts the ability of an attacking enemy to maneuver and provides natural lines of resistance, a position defense may be desirable and of course, terrain that facilitates maneuver by defending forces will favor a mobile type of defense. In selecting the key areas for defense, the commander depends largely upon a terrain study. In addition, a terrain study frequently will give valuable indications of probable enemy assembly areas, field and air defense, artillery positions, observation posts, and avenues of approach.

d. Retrograde. In retrograde, good observation and fields of fire permit engagement of the enemy at long ranges. Natural and artificial obstacles are exploited to strengthen defenses, protect exposed flanks, and impede the enemy advance. Concealment and cover are essential for assembly areas and routes of movement. Road nets are exploited to expedite the movement of friendly forces and to facilitate control, and are denied to the enemy for the same reasons. The effects of weather on the terrain influence observation, trafficability, control, and the performance of troops and equipment.

e. Nuclear. The maximum effects of a nuclear weapon are subject to many variables, depending on how the weapon is employed. Blast and thermal effects would extend to a greater distance in open terrain, but the missile effect and thermal fires obtained with a certain height of burst could create many adverse conditions, such as tree blowdown, induced radiation, and immediate residual radiation.

Section II. LANDFORMS

53. Plains

a. Definitions. As a landform group, plains are generally flat to rolling areas with uplands or interstream areas less than 150 meters (500 feet) above adjacent valley bottoms. A dissected plain is one with a surface that is interrupted by erosional features, and an undissected plain is one with a smooth uninterrupted surface.

b. General Characteristics. Plains may be situated at any elevation. Some are thousands of feet above sea level and others are at sea level. Some are rough and rolling and others are flat. Because of their low degree of local relief, plains generally have low angles of slope. In temperate climates, this characteristic makes them favorable for transportation routes. Where there is monsoon weather or a tropical climate, however, more reliable routes may be provided by higher terrain. The details of relief include uplands and lowlands, ridges

and valleys, and hills and hollows, all within local ranges of elevation of 150 meters (500 feet) or less.

c. *Classification.* Plains are classified as—

(1) *Flat.* Local relief of less than 15 meters (50 feet).

Figure 14. Coastal plain formed by volcanic lava (Hawaii).

Figure 15. Outer delta features (Moses Point, Alaska).

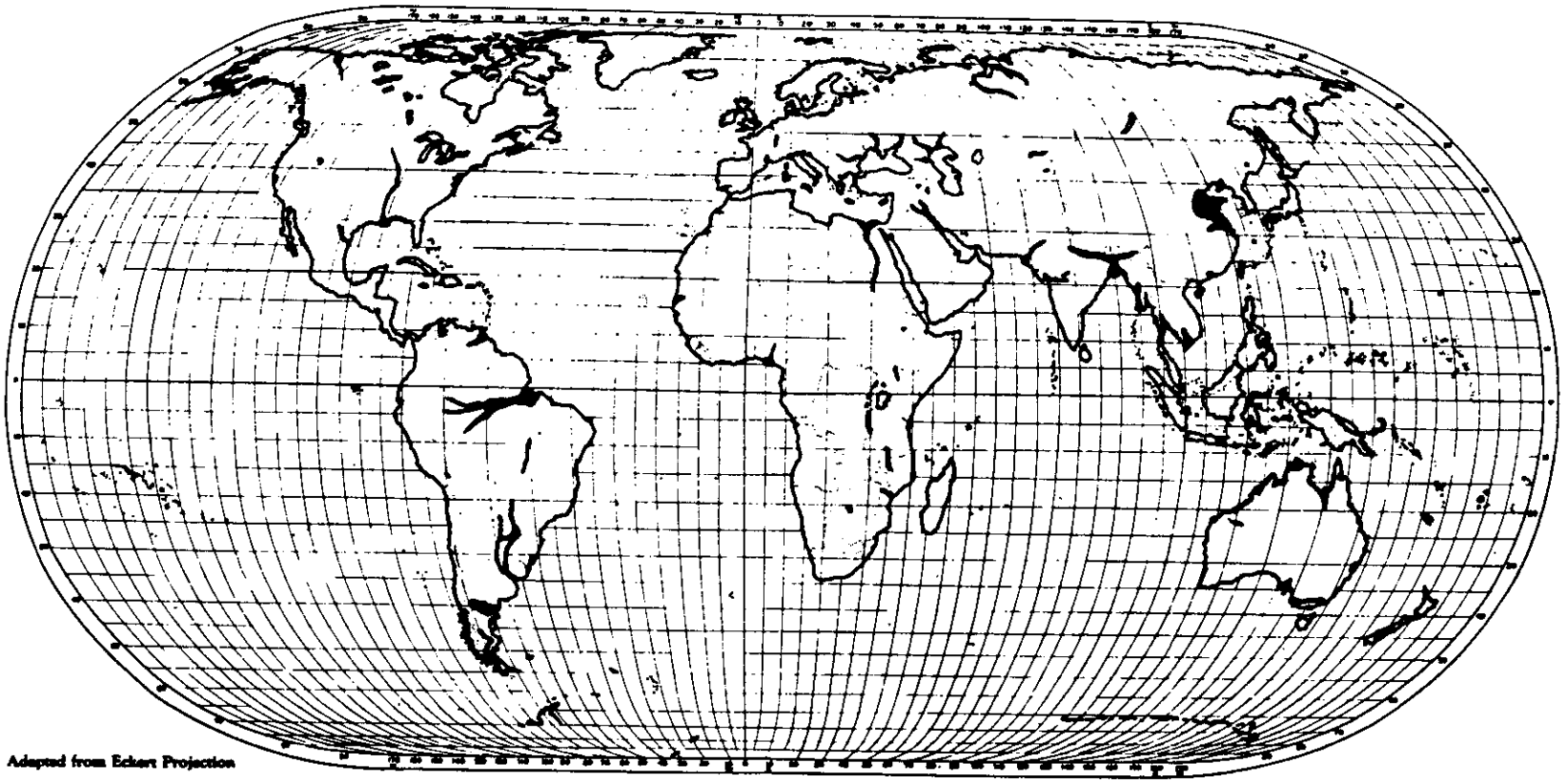


Figure 16. Flood plain, terrace, and delta deposits of the world.

(2) *Undulating.* Local relief of 15 to 45 meters (50 to 150 feet).
(3) *Rolling.* Local relief of 45 to 90 meters (150 to 300 feet).
(4) *Roughly dissected.* Local relief of 90 to 150 meters (300 to 500 feet).
(5) *Slope.* In terms of slope, plains are considered smooth when they have large areas with a slope of less than 2 percent, and rough when there are large areas with a slope of more than 2 percent or many small areas with steep slopes.

d. Coastal Plains. These are generally low and featureless (fig. 14). Frequently they have shallow valleys formed by streams that originate inland. Swamps usually are numerous. Cuestaform coastal plains are characterized by long, low ridges alternating with lowlands in bands several miles wide and many miles long generally parallel to the coast. The ridges on this type plain are usually asymmetrical, the steeper slope being inland.

e. Delta Plains. These plains, which are formed by sediments deposited at the mouths of streams and rivers, are usually low and marshy, with a local relief of less than 15 meters (50 feet) (fig. 15). The features of greatest relief are the natural levees, which are low, broad banks of alluvium on either side of the stream channels. For protection against stream overflow, artificial levees may be built near the stream on top of the natural levees.

f. Flood Plains (fig. 16). These, also called

Figure 17. Meandering river, showing flood plain and oxbow lakes.

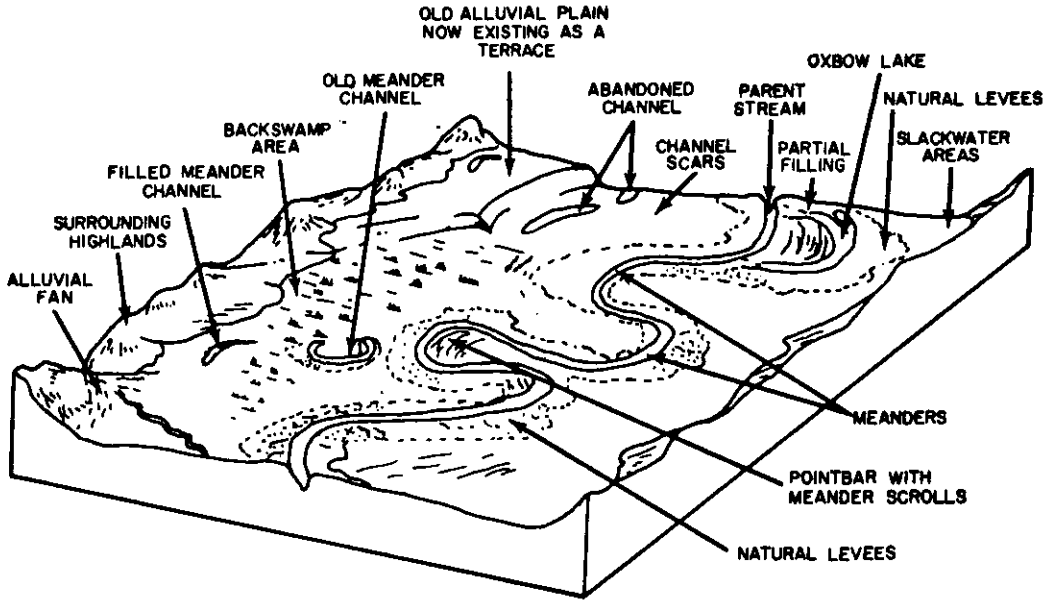


Figure 18. Flood plain with evidence of pre-existing meander.

alluvial plains, are formed by weathered and eroded material deposited by streams upon the floors of their valleys. The flood plain usually is poorly drained, and may contain marshes, swamps, lakes, and former stream channels. Unless protected by levees, it may become partly or completely covered by water in times of flood. The surface is flat, the levees alternating with swamp areas. Meandering rivers and crescent-shaped (oxbow) lakes are characteristic of this type plain (fig. 17 and 18). The silts and clays deposited on flood plains make productive soils, and this type plain is used extensively for agriculture.

g. Piedmont Plains. These are alluvial plains formed by mountain streams with steep gradients that deposit a sediment, consisting largely of gravel and sand, at the point where the stream enters the lowlands. This type of plain is found in arid and semiarid regions with meager vegetation and torrential rains. Although the plain may appear level, actually it slopes away from the mountain base. Many piedmont alluvial plains are covered only with shrubs or sparse grasses. Those with fine soils are high in mineral plant foods and, if irrigation water is available, they are suitable for agriculture.

h. Glacial Plains. These (fig. 19 and 20) are classified as either ice scoured or drift plains.

(1) Ice-scoured plains are level to gently rolling areas composed largely of bare rock. They are characterized by rounded rock hills and broad open valleys and basins with comparatively low local relief. Over the valley floors there may be a thin covering of glacial debris which serves as an anchorage for shallow-rooted trees, chiefly conifers. There are numerous falls, rapids, and lakes. Some small shallow lakes become filled with remains of marsh vegetation, such as sphagnum moss, creating bogs of the type called muskeg in Canada.

(2) Drift plains consist largely of boulders, gravel, sand, or clay in layers of varying thickness on top of other strata of rock and soil. The principal characteristic is a gently undulating surface which includes broad, low hills, or swells, and wide, shallow depressions, or swales. Commonly the local relief is less than 30 meters (100 feet). Large areas of drift plains are essentially flat, with poorly developed natural drainage. Although soils are generally heterogeneous mixtures,

Figure 19. Glacial plain (Moose Jaw, Saskatchewan, Canada).

areas of impervious clays are common. After heavy rains, ponds several acres in extent may form; and unless artifically drained, the water may stand until it evaporates. In some localities there are hills of clayey till called drumlins (fig. 21) that occasionally reach heights of more than 30 meters (100 feet) and may be a mile long. Streams in this type of plain may be interrupted by swamps, lakes, falls, or rapids.

i. Lacustrine Plains. These are formed by sediment settling on lake bottoms. Subsequently the lake was drained by natural forces, or evaporated because of a major change in climate. They are level and often contain salty or alkaline lakes. Generally they are characterized by poor drainage and alkaline soils.

j. Loess Plains. These are formed by windblown particles of silt, called loess, which have been deposited over large areas, forming a smooth, gently sloping surface. The ability of loess to stand in vertical walls results in steep escarpments along gullies, stream valleys, and artificial cuts (fig. 22).

k. Karst Plains. These (fig. 23) are a type of erosional plain developed on limestone. They have a pitted surface along with exposed bedding plain edges (pinnacles) tilted through the surface. The pitting is formed from subsurface collapsing due to the solvent action of underground water. Between the depressions there are low, irregular ridges or hillocks. Numerous caverns are formed beneath the surface of a karst plain, and there are also large underground streams which may issue at the surface as springs of considerable volume.

54. Plateaus

a. Description. A plateau is commonly bordered by an escarpment or steep slope on at least one side. The plateau surface may be cut by deep, narrow stream valleys, but the interstream areas are mostly broad and nearly level. Tabular uplands with a local relief of more than 150 meters (500 feet) may be considered plateaus. They vary greatly in configuration, but most have broad flat surfaces high above sea level, and are deeply trenched by narrow valleys. Depending upon the stage of the erosion cycle, the valleys that dissect the plateau may be widely spaced early in the cycle or very closely spaced late in the cycle (fig. 24). Most large plateaus are in regions with arid or semiarid climates. Plateaus may be classified into three major types:

(1) *Intermountain* (fig. 25). Surrounded or nearly surrounded by mountains.

(2) *Piedmont.* Lying between mountains and plains, or between mountains and the sea.

(3) *Continental* (fig. 26). Rising abruptly from bordering lowlands or the sea on most or all margins; usually without conspicuous mountain rims.

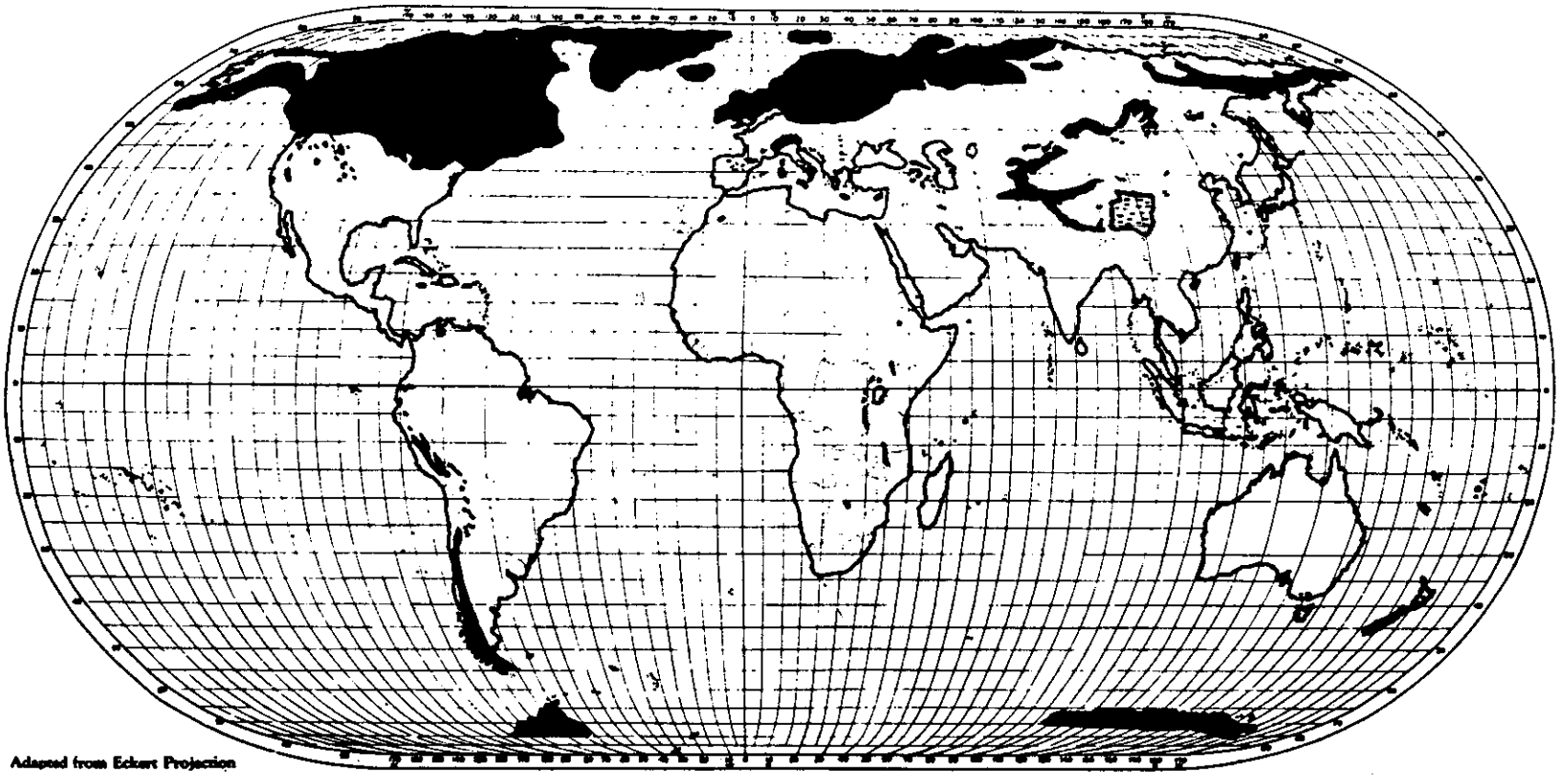


Figure 20. Glaciated areas of the world.

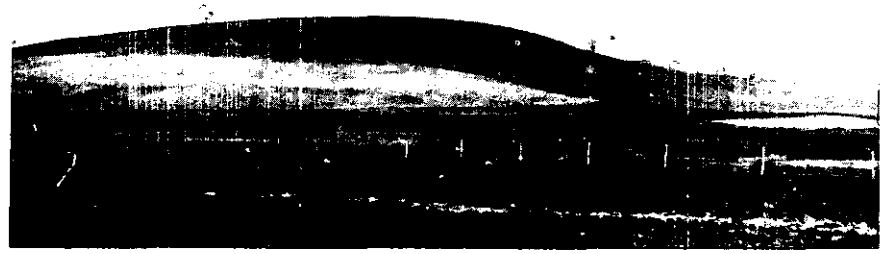


Figure 21. Drumlin (New York).

b. Climates. In arid climates, streams usually flow in canyons cut into the plateau, the typical canyon having a narrow bottom offering little space for a roadway. The stream is seldom navigable and follows a steep, boulder-strewn course interrupted by rapids and falls. Sudden and extensive changes in stream level are common. Canyons usually are too deep to be crossed easily and too wide to be bridged economically. They rarely provide a transportation route and are a difficult obstacle to movement. Areas between the streams usually are flat or rolling uplands, some of vast extent. Areas of interior drainage called bolsons exist on some plateaus. The streams empty into these, resulting in level areas that may contain large salt lakes or salt marshes. Plateaus in humid climates tend to be more dissected by stream erosion than those in arid climates. Broad divides with rounded and irregular uplands are common.

c. Ice Plateaus. The vast sheets of ice that cover most of Greenland and Antarctica may be regarded as great plateaus. Greenland is an intermontane plateau, surrounded by a fringe of mountains. In most of Antarctica, the ice rises in a sheer wall, then slopes up rapidly to a fairly level interior with an average elevation of about 1,830 meters (6,000 feet), the maximum elevation of 3,050 meters (10,000 feet) being found in regions inland from the Pacific coast. In general, the surfaces of an ice plateau are flat or have parallel ridges a few feet in height which result primarily from the wind and drifting snow.

(1) *Marginal features of Greenland.* The highland or mountainous rim and the higher summer temperatures of Greenland produce marginal features which are different from those of Antarctica. The ice is confined by the highlands, melting some distance inland on the southern and western margins. Where ice does not discharge into the sea, it protrudes through gaps in the bordering highlands (fig. 27). Irregular icebergs form, drifting into the Atlantic Ocean during the spring months.

(2) *Marginal features of Antarctica.* The marginal ice of Antarctica is thin and traversed by deep cracks. Except in a few localities where it is retained by the fringing mountains, the ice overruns the land margins, so that the exact position of the continental shoreline is not known. The edge of the ice is marked by sheer cliffs. From these cliffs giant icebergs split off along crevasses as a result of undercutting by waves and the buoyant effect of sea water. Some of these are tens of square miles in area. The icebergs disintegrate by melting and disperse as masses of floe and drift ice which fringe the continent for many miles.

55. Military Effects of Plains and Plateaus

a. Variety. Although plains and plateaus are characterized by relatively low relief compared to hills and mountains, they present a wide variety of topographical conditions. Since each type of plain or plateau differs in its features and effects, one can only generalize about their influences on military operations.

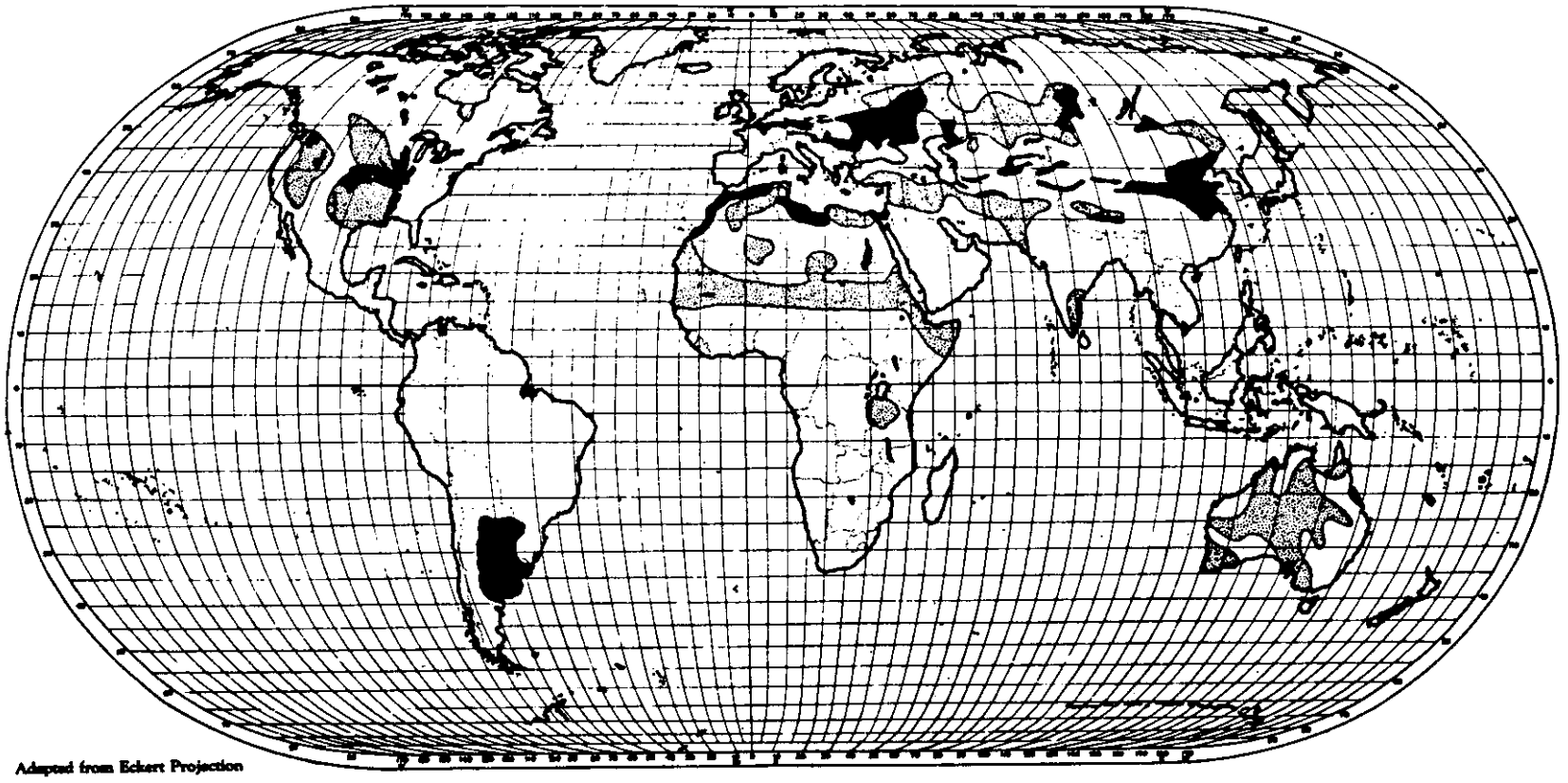


Figure 22. Loess deposits of the world.

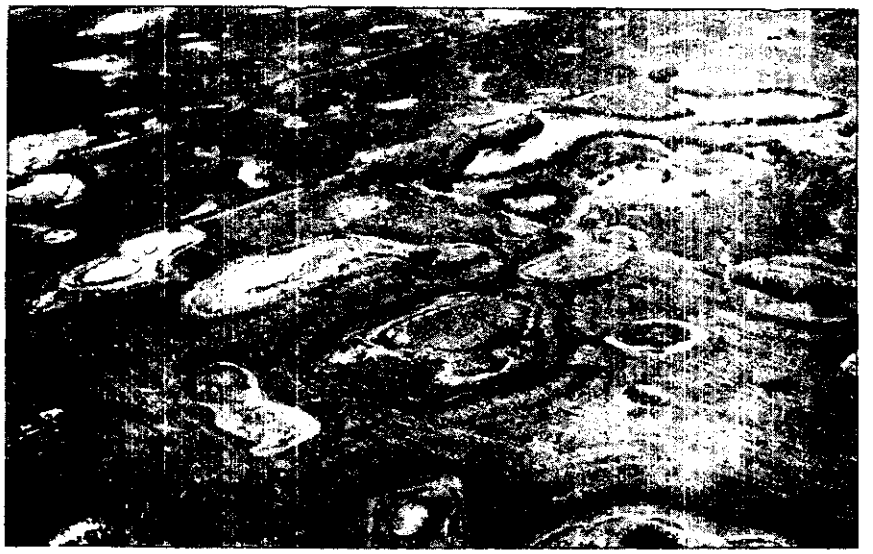


Figure 23. Karst plain (Canada).

Figure 24. Plateau dissected by stream (Deschutes River, Oregon).

b. Movement.

(1) *Coastal plains.* In general, the topography of coastal plains offers no major obstacle to the cross-country movement of tracked vehicles, although there may be areas that are difficult or impracticable because of unfavorable soil conditions and dense vegetation in areas of medium to heavy rainfall. Movement along an indented shore usually is difficult because the terrain is separated into compartments by streams and estuaries. Cross-country movement in-

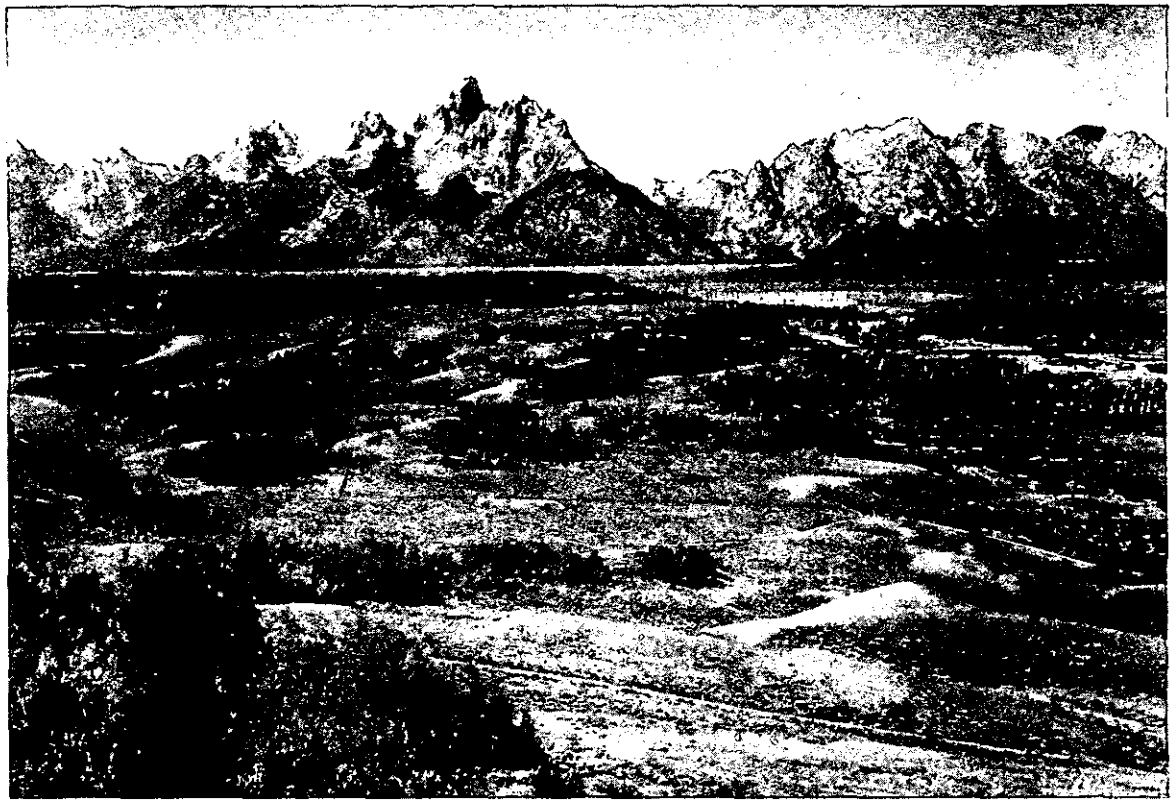


Figure 25. Intermountain plateau (Jackson Hole, Wyoming).

land may be limited to narrow areas bordered by water. In such terrain, attacks may require amphibious support. Coasts with beach ridges hinder an advance inland because vehicles must cross poorly drained areas between relatively stable sand ridges. Terrain of this type impedes the adequate dispersal of troops and supplies.

(2) *Delta plains.* On delta plains cross-country movement usually is hindered by marshy ground, shifting streams with loose sand and mud bottoms, and thick vegetation. Soils are better drained in the inner regions of the delta. Normally the natural levees of streams provide the highest, best-drained, and most trafficable parts of the delta. Movement on the low-lying grounds of delta plains is always threatened by the possibility that the enemy will destroy dikes or levees and flood the area. The use of waterways as avenues of approach by the enemy must not be overlooked.

(3) *Alluvial Plains.* The stream valleys in alluvial plains generally provide corridors through areas of greater relief. In dry weather, the cross-country movement conditions usually are excellent, except for such obstacles as streams and local areas of unfavorable soil or dense vegetation. In wet weather or during floods movement may be limited to small areas of higher, better-drained ground, such as levees. Alluvial terraces are above flood levels and may be well-drained, but they are commonly isolated by steep slopes. It is not unusual for a stream to meander from one side of its valley to the other. If the valley slopes are steep, such meandering may eliminate vehicular movement up or down the valley.

(4) *Glacial plains.* The topography of

Figure 26. Eroded continental plateau (Grand Canyon, Arizona).

glacial plains usually presents no insurmountable obstacles to movement. Large boulders may be obstacles in some area. In regions containing large areas of soft ground, lakes, or marshes, movement in the rainy season may be greatly hindered by mud (fig. 28).

(5) *Lacustrine plains.* No topographic obstacles to movement are offered by the level surface of lacustrine plains (old lake beds). During wet weather, however, the fine soils may be slow-drying and become nontrafficable (fig. 29).

(6) *Loess plains.* Loess is a fine-grained, yellowish-brown silt deposited by the wind. In dry weather, movement conditions on loess plains are good, except where escarpments and ravines

Figure 27. Tongues of icecap descending toward fiord (Greenland).

are encountered. Ground conditions may become very poor in wet weather, making cross-country movement impracticable.

(7) *Karst plains.* Movement on karst plains, a limestone region, is limited chiefly by the sinkholes, which may have steep slopes and contain swamps and ponds. In wet weather the clayey residual soil overlying the limestone may limit movement in some areas. Karst regions vary greatly in their characteristics—from a plain with an occasional sinkhole to a surface so pitted and broken as to make even dismounted movement very difficult. Knowledge of the erosional development is necessary to evaluate such an area properly.

c. Observation. The degree of observation available on coastal plains is normally good along the coastline, but inland the flat country and forest cover usually offer few observation points. Observation is limited on delta plains because the low, level ground generally is covered thickly by vegetation. On alluvial plains, observation from the valley bottoms usually is poor, but the bordering regions provide commanding views into the valleys. Where vegetation does not interfere, it may be good on the more level portions of these plains. Vegetation also determines the amount of observation that may be secured in lacustrine, loess, and karst plains.

d. Cover and Concealment. Coastal plains provide few areas with sufficient cover and concealment for larger units. Except for the levees, there are also few topographic features on delta plains that will conceal or protect troop bodies of any size. Little cover and concealment are available on alluvial plains, except for that provided along terraced scarps, river banks, and levees. On glacial plains, cover is lacking in the more level parts, but there may be some limited cover and concealment provided by knobby and forested areas. The sinkholes of karst plains also provide a moderate degree of concealment and cover.

e. Construction.

(1) *Coastal plains.* Although generally there is no hard rock on coastal plains, sand and gravel are abundant on beaches and along streams. The ground of coastal plains is excavated easily, but the depth of excavation usually is limited by the high water table. Long and straight road aline-

Figure 28. Glacial boulders (Yosemite National Park).

ments normally can be obtained. There are many suitable sites for airfields, particularly along the marine terraces.

(2) *Delta plains.* Abundant sand and fine binder material may be obtained on delta plains, but gravel is scarce. There are no exposed hard-rock formations or bedrock. Generally the location of airfields and roads must be confined to the levees. Structural foundations not built upon levees are unreliable, and may settle due to the low, poorly-drained ground with a threat of periodic flooding. Drainage always is a serious problem because the levees prevent the return of surface water to the river, and the high water table limits underground return. Accordingly, drainage and pumping systems may be required.

(3) *Alluvial plains.* Rock is scarce in flood plains except where it may crop out along the scarps of terraces. Sand, gravel, and binder material are abundant along stream channels and the terrace scarps. Terraces also may provide suitable sites for bunkers and underground installations. Excavations in flood plains are limited by the high water table, but these plains and terraces if well-drained are suitable for the construction of roads and airfields.

(4) *Glacial plains.* Sand and gravel are

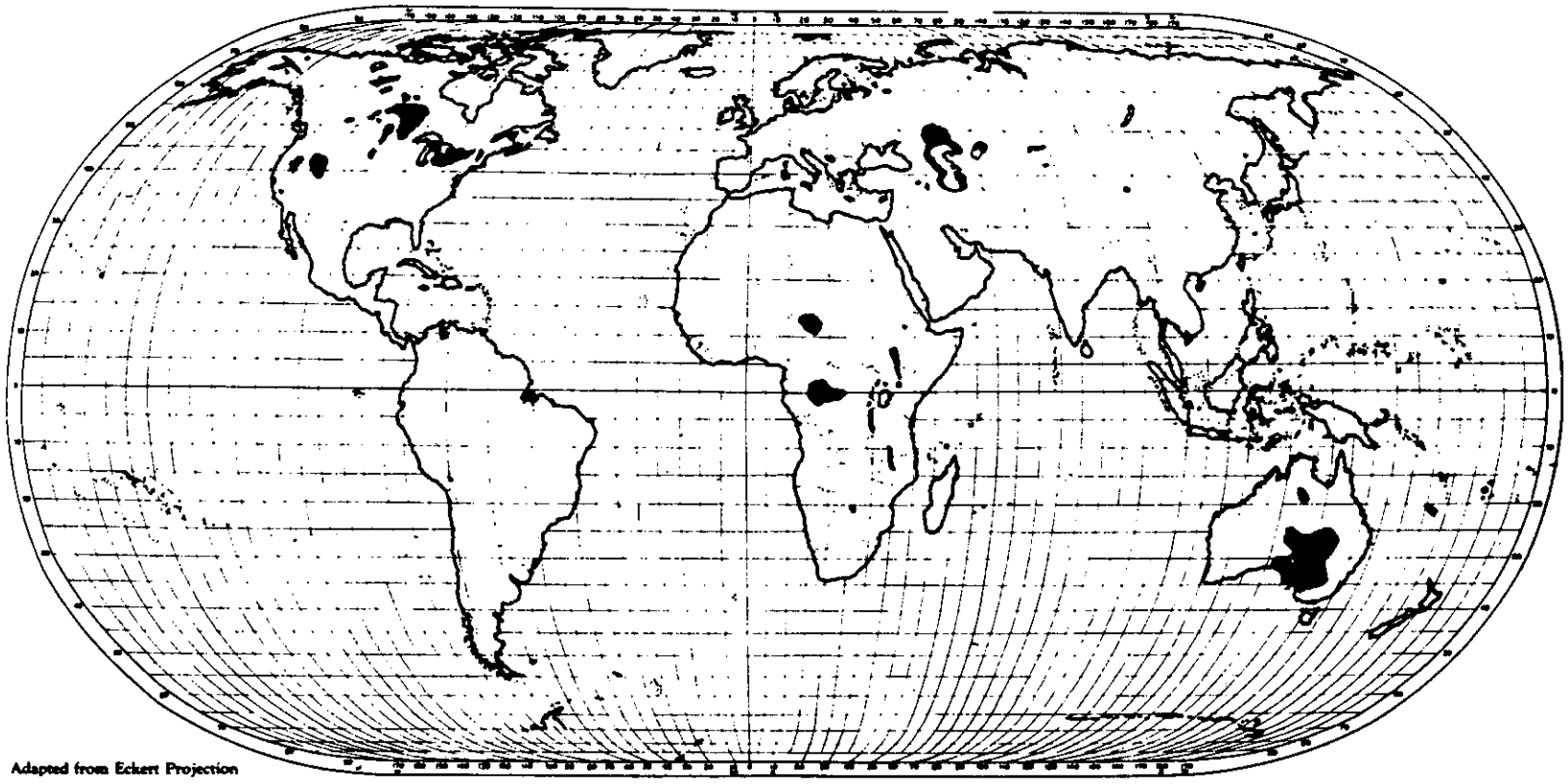


Figure 29. Lake bed and related deposits of the world.

widely distributed on glacial plains, and rock usually is abundant. On till plains, boulders may provide building stone, but there is bedrock only in a few locations, such as in deep valleys where the overlying till has been cut through. Wet ground and weak soils may create foundation problems where the drainage is not good.

(5) *Lacustrine plains.* Except at the marginal slopes, where sand, gravel, and rock may be obtainable, lacustrine plains usually can provide only clay and fine sand for construction purposes. The fine-grained soil makes a poor foundation for structures, particularly in humid climates. Lacustrine plains provide level sites for airfields with few natural obstructions and allow unrestricted road alinements.

(6) *Loess plains.* Loess plains are a poor source of gravel or rock, except where there are underlying deposits. Foundations require stabilization and in cold climates the loess may heave. In dry climates, thick loess deposits are easily excavated and are well suited for underground installations. Many good airfield sites and road alinements usually are available.

(7) *Karst plains.* Large quantities of limestone for building stone and crushed rock may be obtained on karst plains. Sand and gravel usually are lacking. Excavation often is difficult because of the irregular rock surface, with deep clay-filled pits, and the high pinnacles of rock that lie beneath the residual soil. Grading usually requires the excavation of rock. There is always a possibility of foundation subsidence.

56. Information Requirements — Plains and Plateaus

a. Plains.

(1) Extent of area covered by plain.

(2) Surface (elevation, slope, kind of surface).

(3) Major interruptions (hills, mountains, river valleys).

(4) Minor interruptions (gullies, sinks, levees).

b. Plateaus.

(1) Area covered by plateau.

(2) Surface (elevation, slope, surface, relief features).

(3) Major interruptions (hills, mountains, canyons, valleys).

(4) Margins (mountains above plateau, abrupt descending cliffs).

57. Mountains

a. Description. As a landform group, mountains are rugged areas with crests that are, in general, more than 600 meters (2,000 feet) above adjacent lowlands. They are commonly distinguished from other major relief features by the predominance of slopes and their overall massiveness. In terms of local relief, mountains may be classified as low when they have a local relief of 900 meters (3,000 feet) or less, and high when their height exceeds that figure. According to their size and arrangement, mountain features may be classified as peaks, ranges, chains, and cordilleras.

b. Peaks. A peak is a conical high mass, that rises above its surroundings. Ordinarily a peak is a feature of minor order upon a range, but as in the case of an isolated volcanic cone, one peak may stand alone and comprise the entire mountain mass.

c. Ranges. A range is an arrangement, usually linear, of many peaks, ridges, and their valleys. The term ordinarily applies to mountains that have a general unity of form, structure, and geologic age.

d. Mountain Chain. A mountain chain consists of several associated ranges, usually more or less parallel, having unity of position, form or structure, but separated by trenches or basins.

e. Cordillera. A cordillera is a large regional grouping of mountain chains.

58. Mountain Features

a. Relief. Mountains are distinguished from hills by their greater relief, more rugged contours, and more complicated surface patterns. The average slope of large mountains seldom is more than 20° to 25° from the horizontal, and only a few have slopes of more than 35° near the summit. Even walls that seem vertical seldom have slopes that average more than 70°.

b. Valleys. Except where they have reached grade level and meander in flat alluvial valleys, mountain streams have high gradients and flows of high velocity. The rapid downward cutting action of the stream may uncover bedrock of unequal hardness, so that falls and rapids develop. Some streams, in cutting through bedrock of unequal resistance, erode valleys which are broad at their headwaters, then narrow to gorges, and subsequently open out again downstream. Valleys formed by glacial action have wide rounded bottoms and steep sides. They have U-shaped profiles, in contrast to the V-shaped profile of a stream eroded valley. The walls are steep and rugged. Most glaciated valleys have one or more basins in which impounded drainage creates lakes, ponds, or marshes.

c. Divides. Between the mountain valleys there are uplands formed by remnants of the original elevation. Rainfall on these uplands separates according to the surface slopes and descends by numerous rivulets into adjacent valleys, modeling the uplands as it flows. The uplands are called divides. When they separate the drainage destined for opposite sides of a continent they are termed continental divides.

d. Foothills and Spurs. The lowest and least massive features of mountain uplands are the foothills and spurs that fringe the principal highlands. Foothills are hills located at the base of higher mountains or hills. A spur is a ridge projecting laterally from the main crest of a hill or mountain.

e. Passes. The erosion by streams or glaciers creates saddle shaped notches, or passes, in a mountain barrier. The term pass is applied to any type of natural passageway through high, difficult terrain.

59. Hills

As a broad landform group, hills are rough areas with crests generally from 150 to 600 meters (500 to 2,000 feet) above adjacent lowlands. They usually contain a predominance of moderate slopes. Hills may be classified as low when they have local relief of from 150 to 300 meters (500 to 1,000 feet), and high, when the local relief is from 300 to 600 meters (1,000 to 2,000 feet). Some very rough hills may appear mountainous in relation to adjacent plains, and locally may be called mountains, but they are not properly of a size or nature to merit the term. Mature hill lands may be almost entirely a succession of hills, valleys, and narrow ridges, with level land occupying less than five percent of the total area. Hill regions in an early stage of erosion may include some fairly level, plateaulike uplands separated by steep-sided valleys. Those in a more advanced erosional stage may have broad open valleys and reduced slopes that are suitable for agriculture. Because some of the slopes in hill regions are steep and untillable, they have retained their forest cover and have streams with steep gradients that are capable of developing waterpower.

60. Military Effects of Hills and Mountains

a. Key Terrain Features. In both attack and defense, the key terrain features may include the heights which dominate valleys, the routes of communications, passes and valleys which permit cross-country movement through the mountains, and aircraft landing areas. Dominating heights which may be used by the enemy for observation of avenues of approach must be controlled.

b. Observation and Fields of Fire.

(1) *Observation.* In hilly and mountainous areas, observation may be restricted. In most cases, commanding heights provide only partial observation of adjacent valleys and slopes. Foothills and spurs extending into a valley obscure observation along the valley.

(2) *Fields of fire.* Mountains and hills place some restrictions upon the em-

ployment of supporting weapons. Armor loses much of its mobility because it cannot move across country. Occasionally tanks can be used in small numbers against limited objectives, but their action often is confined to providing direct fire support. Artillery is effective, but the limited visibility in mountainous terrain restricts observation and adjustment of fire. Terrain features may also reduce the effectiveness of air defense artillery by making radar siting difficult and reducing the target acquisition range of the system. Survey and fire control are hampered, and more time is required for artillery to displace. There is difficulty in finding gun positions that do not have too much defilade. The heavier crew-served weapons of the infantry and their ammunition are difficult to carry over the rugged terrain. Mortars and recoilless rifles are effective and are favored for operations in mountains and hill regions. Deep valleys and ravines afford a degree of protection from the blast effect of nuclear weapons when the axis of the valley or ravine points well away from ground zero. When it does not, there is little or no shielding effect, and blast damage may be increased because the blast is canalized. Deep valleys and ravines afford substantial protection from thermal and nuclear radiation to troops, materiel, and buildings located within the shaded portions. In terrain characterized by deep valleys and ravines, however, blast effects of nuclear weapons may cause serious avalanches and rock slides. Concentrations of toxic chemical agent aerosols are extremely hard to achieve on marked downward slopes. Toxic chemical agents and biological agent clouds tend to flow over rolling terrain and down valleys, to remain in hollows and on low ground and in depressions, but to go around obstacles. Local winds, coming down valleys at night or up valleys in the daytime, may deflect the clouds or reverse the forecast flow; likewise they may produce favorable conditions for cloud travel.

c. Cover and Concealment. The rugged topography of mountains offers abundant cover and concealment, although movement across slopes or crests above the timberline will be exposed. Sounds carry from valley bottoms to hilltops, but within the valley, sounds are muffled by ground forms and streams.

d. Obstacles. Major obstacles to movement include steep, high ridges and ranges, high valley routes and escarpments, sloping cliffs and terrace faces. Minor obstacles include stream embankments, valley terraces and benches, spurs, talus, and debris-choked valleys, and presence of boulders.

e. Avenues of Approach. Hills and mountains parallel to the axis of advance offer flank protection, but limit lateral movement. When perpendicular to the axis, they are an obstacle to the attacker and an aid to the defender. Mountain roads must be improved because the roads are generally narrow, have steep grades, and poor surfaces. Sharp turns may prevent the use of trailers. Roads in valleys or along defiles require that the adjacent high ground be secured to insure control of the roads. Mountain roads are subject to slides and may be blocked by snow. Those on the crest of ridges may be exposed to enemy observation. Roads in defiles may be flooded and may also have large boulders. The best sites for military roads in mountain areas are normally on the sides of slopes.

f. Communications. Hills and mountains contain dead spaces that often limit the range and effectiveness of radios, although these restrictions usually can be overcome by the use of relay sets. Wire laying is difficult, and visual signals are not always dependable and often can be seen by the enemy.

g. Air Support. The hazards in mountainous regions place limitations upon the use of low-flying combat aviation. Targets are difficult to locate and in many cases close air-support strikes must be controlled by aerial FAC's (Forward Air Controllers) or by indirect

means, since the functions of tactical air-control parties are hindered by the terrain and weather.

h. Combat. Combat in mountains and hilly areas usually consists of a series of independent actions to seize and hold key terrain, strike communication lines, and protect friendly routes of supply and evacuation. Infantry plays the dominant role, since it is not roadbound and can close with the enemy under any condition of terrain. Commanding positions in mountain terrain are often rocky ridges or eminences with little or no soil. If the importance of the position justifies the time and effort required, trenches, emplacements, and galleries can be cut into the solid rock. Parapets and breastworks of cobbles and boulders are effective against small arms, but they are vulnerable to artillery fire. Log breastworks and protective shelters may be built if timber stands are conveniently located. Mines and obstacles find their most important use in obstructing movement on roads and trails and through defiles. Roadblocks are effective because of the difficulty of bypassing them. Mountain terrain favors the defender because available obstacles enable him to use minimum troops to deny the attacker the use of existing routes. He can force deployment of major enemy units and the expenditure of large amounts of mortar and artillery ammunition, and can inflict the maximum punishment from protected positions.

i. Construction. Hard rocks suitable for construction purposes are readily obtained in hills and mountains. Sand is scarce, but gravel may be secured in the lower stretches of streams where they approach the foot of the mountains or flow through hills. There are few suitable locations for airfields because of the difficulty of excavation in rock, the obstructed and limited approaches, the poor accessibility, and the turbulent air currents. Highways, railways, and tunnels are vulnerable in these areas. Geologic data may be useful in indicating rock conditions favorable to initiating rock slides by bombing or artillery fire to block enemy lines of communication. Geological information will also assist in selecting sites for gun emplacements and other fortifications, in estimating the probable effect of fire on rock fragmentation, and determining the possible ricochet effects of projectiles. The soil usually is thin or stony, with underlying bedrock, so that it is difficult to construct field fortifications. Geologic study will assist in selecting areas where excavations may be made and in choosing the required explosives and equipment.

61. Information Requirements — Hills and Mountains

a. Extent and Type of Mountains or Hills.

b. Ridge Crests.

(1) Location and orientation.

(2) Elevations (typical, highest, lowest).

(3) Height above adjacent valley flats (average, highest, lowest).

(4) Pattern (long straight, parallel ridges; branchlike and crooked ridges; clusters of knobs and peaks).

(5) Skyline (flat-topped and broad, or knifelike).

c. Slopes.

(1) Shape (convex, concave).

(2) Angle, in percent or degrees (near crest, middle, near base).

(3) Minor relief features (rough lava, boulder fields and gullies).

d. Valley Flats.

(1) Location.

(2) Width (of main and tributary valleys; average, widest, narrowest for both categories).

(3) Pattern (long, straight, and parallel valleys or branchlike and crooked valleys).

(4) Transverse profile (degree of slope near center and margin of valley).

(5) Longitudinal profile (degree of slope near mouth and head of valley).

(6) Terraces (benchlands) along borders of valley flats (number of terrace steps, width, continuity, elevation of steps one above another, slope between terrace levels).

(7) Stream channels within valley (straight or meandering, bordered by bluffs, gentle downslopes, or natural levees).

e. Intermontane Basins.

(1) Location.

(2) Width (average, widest, narrowest).

(3) Shape (round, oval, long and narrow, irregular).

(4) Flat bottom lands (extent and location).

(5) Terraces (benchland) about borders of flat bottom lands (number of terrace steps, width, continuity, elevation of steps above one another, slope between terrace levels).

f. Passes.

(1) Location.

(2) Elevations (average, lowest, highest).

(3) Number of passes (distance between passes).

(4) Gradients (near head of pass, downslope).

(5) When closed by ice and snow.

(6) Character of defile formed by pass and approaches (width, length, character of slopes).

(7) Routes over each pass.

Section III. DRAINAGE

62. Effects of Drainage

a. Description. The water features of an area comprise its drainage. They include streams and canals; drainage and irrigation ditches; lakes, marshes, and swamps; artificial bodies of standing water such as reservoirs and ponds, as well as such subsurface outlets as springs and wells. The character of these drainage features is determined by precipitation, relief, surface runoff and ground-water flow, and various manmade improvements. Vegetation has a major influence upon drainage. Dense grass and tree growth on slopes tend to slow up and absorb a considerable amount of the runoff, but slopes with few trees and sparse vegetation permit rapid runoff and the formation of channels by erosion.

b. Catchment. A catchment basin or catchment area is the total area drained by a stream or system of streams. All water features within this area are related and are considered as a whole. The limits of the drainage basin are marked by the topographic divide which separates it from neighboring drainage systems. The amount of water reaching the stream, reservoir, or lake depends upon the size of the area, the amount of precipitation, and evaporation and transpiration. The rate of evaporation depends upon the temperature, vapor pressure, wind, and solar radiation.

c. Patterns. Drainage patterns (fig. 30) reflect the subsurface structure. They are of three major types—dendritic, trellis, and radial defined as follows:

(1) A *dendritic* drainage pattern is a treelike arrangement of streams found most frequently in an area underlain by homogeneous rock.

(2) The *trellis* pattern results from the influence of tilted alternating strata of weak and resistant rocks. The resistant strata separate each stream, producing the overall trellis effect.

(3) The *radial* pattern has streams that radiate from a central dome that lies within a relatively flat area.

63. Rivers and Streams

a. Perennial Stream. A perennial stream flows throughout the year. The regular flow may result from a spring lake or a glacier at the head which furnishes a constant supply of water, from direct precipitation of fairly constant quality, or because the beds are deep enough to be permanently below the fluctuating upper level of the ground water or water table.

b. Intermittent Stream. An intermittent stream originates in a source of water that fails periodically and is particularly common

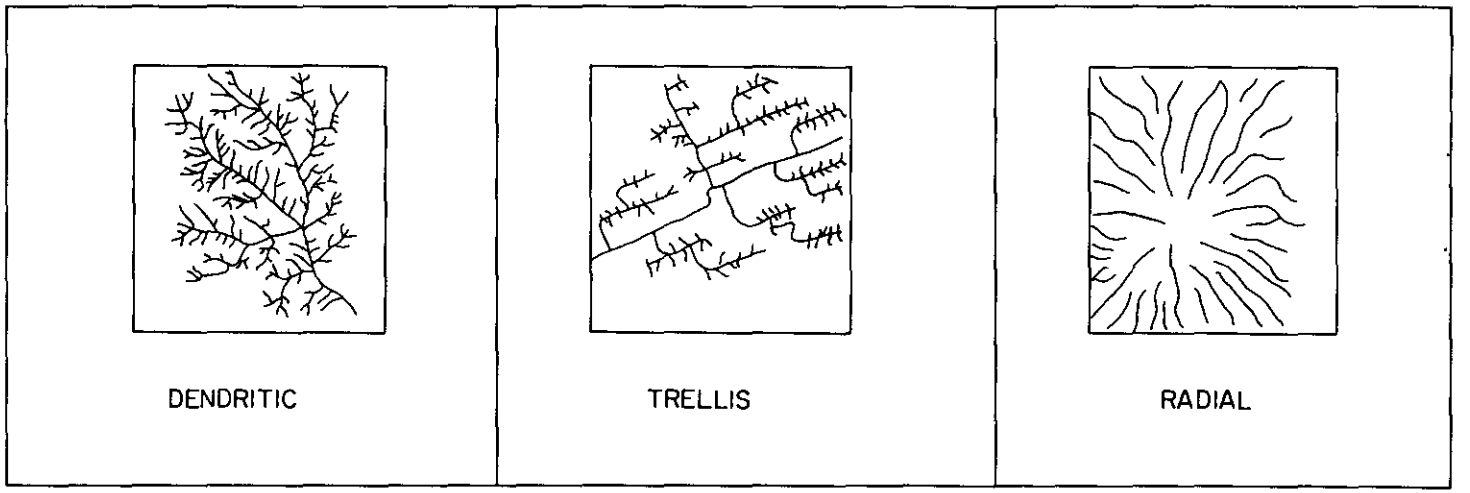


Figure 30. Drainage patterns.

in semiarid regions with seasonal rain or snowfall. Some streams are intermittent because they depend for supply upon the water table and do not have beds deep enough to be independent of fluctuations in the table.

c. Ephemeral Stream. An ephemeral stream is temporary, depending upon infrequent rainfall for supply.

d. Bottoms. Rivers and streams deepen their beds by erosion of the underlying rock. As stream erosion continues, the velocity of the current decreases, with a resulting decrease in down-cutting potential. Eventually, the cutting potential is balanced by the sediment load carried by the stream. Subsequently, unless there is a change in the topography of the catchment basin, the stream alternates between build-up and cutting down. Differences in the load carried by the water at different points, in velocity caused by changes in grade, and in the degree of hardness of the rock make the beds uneven, producing gorges, cataracts, rapids, and potholes. Where streams have a high velocity and flow over loose materials, the bottoms commonly are rocky. In slow-moving water, fine material such as silt and clay is deposited, and the bottoms will be muddy.

e. Banks. As down-cutting potential decreases, side-cutting begins and the river widens its bed or develops a curving course. As a rule, these curves will have steep banks on the outside and gentle, low banks on the inside. The conformation will vary with the composition of the bank, the velocity of the stream, and the kind of materials transported by the stream. Swift streams in rough relief commonly cut deep channels with low banks.

f. Flooding. Some streams flood annually and others infrequently. Floods may be caused by rapidly melting snow, by excessive precipitation and runoff, by ice jams, or by any combination of these. When a river is in flood, the velocity of water is greater than normal, with the fastest current in the main channel.

g. Desert Drainage. Arid climates have long dry periods with infrequent precipitation. Desert streams for this reason are irregular in volume and duration of flow. Large areas of many deserts do not have streams flowing out of their immediate vicinity because the drainage net is centralized in interior basins. There may be separate basins at different elevations in each desert. Many large streams flow into desert lakes that have no outlet, or disappear through evaporation and seepage into porous surface material. Some streams encountered in deserts originate in humid regions, flow across the arid land, and then continue their course in another adjoining humid area. When precipitation occurs in desert areas, it is likely to be in cloudbursts that generate a tremendous runoff as the water rushes down. Sheltered dry washes or wadis may become extremely dangerous locations for bivouacs, gun positions, and installations during these brief but violent floods.

64. Lakes

Some lakes are formed by glacial action creating a depression which subsequently fills with water, by the damming of a river by ice or a moraine, or by water filling a natural depression as a glacier recedes. A stream may be formed into a lake because of interference with its natural course by a lava flow, dam, or avalanche. Coastal lagoons frequently are formed by the deposition of silt or sand at the mouth of a river. The crater of an extinct volcano often collects water and becomes a lake basin. Salt lakes occur when a lake is so poorly drained that the minerals in the water remain while the water evaporates. In limestone country, lakes caused by the filling of depressions of dissolved rocks are common.

65. Marshes and Swamps

a. Description. A swamp (fig. 31) is an area of saturated ground dominated by trees and shrubs. A marsh (fig. 32) is an area of saturated ground dominated by grasslike aquatic plants. A bog is an area of soft, wet, spongy ground consisting of peat which supports mosses, low shrubs, and in some cases poorly developed trees.

b. Formation. Swamps, marshes, and bogs are formed by the overflow of rivers, dams, flooding by tides, a lack of balance between rainfall and runoff or seepage, impervious subsoil in level areas, or the spread of vegetation in lakes, particularly in oxbow lakes. They may

Figure 31. Swamp (Okefenokee Refuge, Georgia).

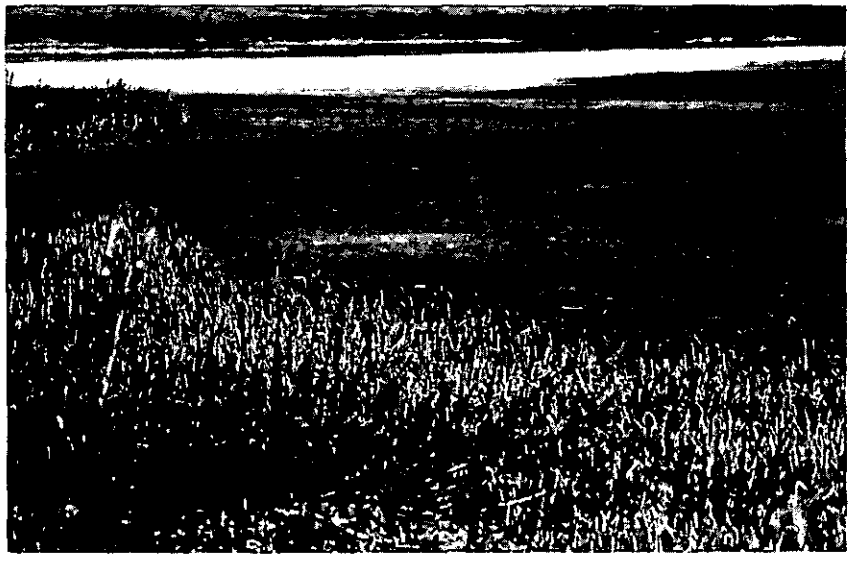


Figure 32. Marsh (Foxholm, North Dakota).

be numerous on delta and flood plains, where surface water is not readily drained. Extensive marshes and swamps are encountered on the plains of humid areas. In glaciated regions, marshes, bogs, and swamps are common.

66. Glaciers

a. Description. A glacier is a thick mass of ice that moves slowly on a land surface. Glaciers depend on the receipt of an annual amount of snow, and form only where there is a carryover of snow from one season to the next. Abundant precipitation is more important than extreme cold. The ice is formed by the crushing of snow flakes from the weight of new snowfalls and shortly altered to a loose aggregate of rounded

granules of ice. With deeper burial these granules are deformed, locally melted and refrozen and recrystallized, to produce a solid mass of interlocking ice crystals. There are two types of glaciers: *valley glaciers* and *continental glaciers.*

b. Valley Glacier. A valley glacier (fig. 33) begins in the summit areas of the high mountains. Patches of snow are converted into icefields. Those icefields at the heads of former stream valleys may eventually become thick enough so that the ice begins to move downward following pre-existing stream valleys. As the glacier moves down the valley, rock fragments become plucked from the walls and become frozen tightly in the sides and bottom of the ice. These fragments abrade the walls like a giant rasp. This abrasion scratches and polishes the walls and straightens out the valley by grinding away irregularities on opposite sides. Narrow "V" stream valleys are reamed out into much more even "U" shaped valleys.

c. Ice Front. The lower end of a glacier, or the ice front, stands at that point where the supply of ice from up the valley is just equal to the loss through melting and evaporation. If supply is greater than loss, the ice front moves down the valley; if loss exceeds supply, the ice front retreats.

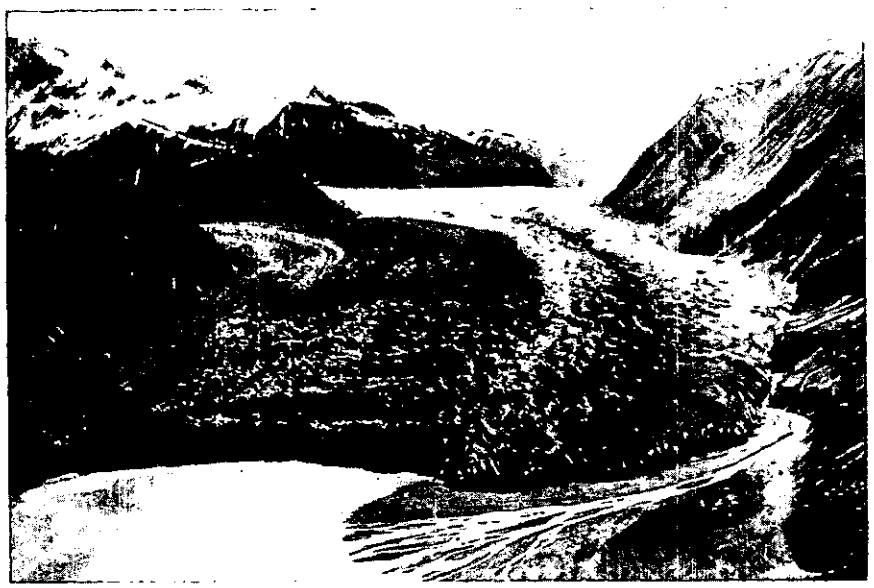


Figure 33. Valley glacier (Alaskan coast. Kame terrace and outwash plain in right foreground).

d. Debris. Rock debris carried in or on the glacier may be dumped at the ice front when the ice melts. This material, called *till,* consists of an unsorted mixture of rock powder, pebbles, cobblestone, and boulders. If the ice front remains stationary for a period of time, a ridge of till, extending across the valley, is formed. This ridge is termed an *end moraine.*

e. Continental Glaciers. Continental glaciers, such as those covering most of Greenland and Antarctica, begin in one or more central areas of snow accumulation. The ice starts to move outward when it becomes so thick that the pull of gravity on the mass exceeds the strength of the ice. No slope is required and in many cases the centers of accumulation lie at low elevations. Continental glaciers make extensive deposits dumped directly from the ice. End moraines mark positions at which the glacier edge stood for some time. They are long ridges or belts of low hills that extend across the country for many miles. Large areas on the glaciated side of the end moraines commonly receive a sheet of till plastered on the underlying rock. This *ground moraine* or *till sheet* was left behind as the heavily loaded ice sheet melted away.

f. Meltwater. Streams of meltwater leaving an ice sheet may flow down valleys that lead away from the glacial front. The material pre-

viously left from frozen ice is deposited along the stream valleys in the form of *valley trains*. Where the land surface slopes evenly away from the edge of the ice sheet, meltwater streams may spread over the countryside in branching, braided patterns forming widespread *outwash plains*. Outwash plains are composed of relatively well-sorted, evenly bedded sand and gravel which may be many feet thick and cover many square miles.

67. Ground Water

a. Hydrologic Cycle (fig. 34). Water evaporated from the ocean is condensed into clouds, from which it falls to the earth as rain, snow, sleet, or hail. Part of this water runs off into lakes and streams, or is retained by the soil, passing into underlying rock formations. Moving through openings in the rocks, the water issues at the surface as springs, streams, and lakes. Ultimately all the water that is precipitated returns to the atmosphere by evaporation from water surface or from the foliage of vegetation. Some also is released from foliage by transpiration, the process by which a plant transmits water through its tissues, discharging water vapor from its foliage. Although this hydrologic cycle is irregular and may extend over a period of years, no water is lost permanently from circulation, but a stage of the cycle may be bypassed or interrupted. Rain falling upon a heavily forested area, for example, may return directly to the atmosphere by evaporation without going through other stages of the normal natural process.

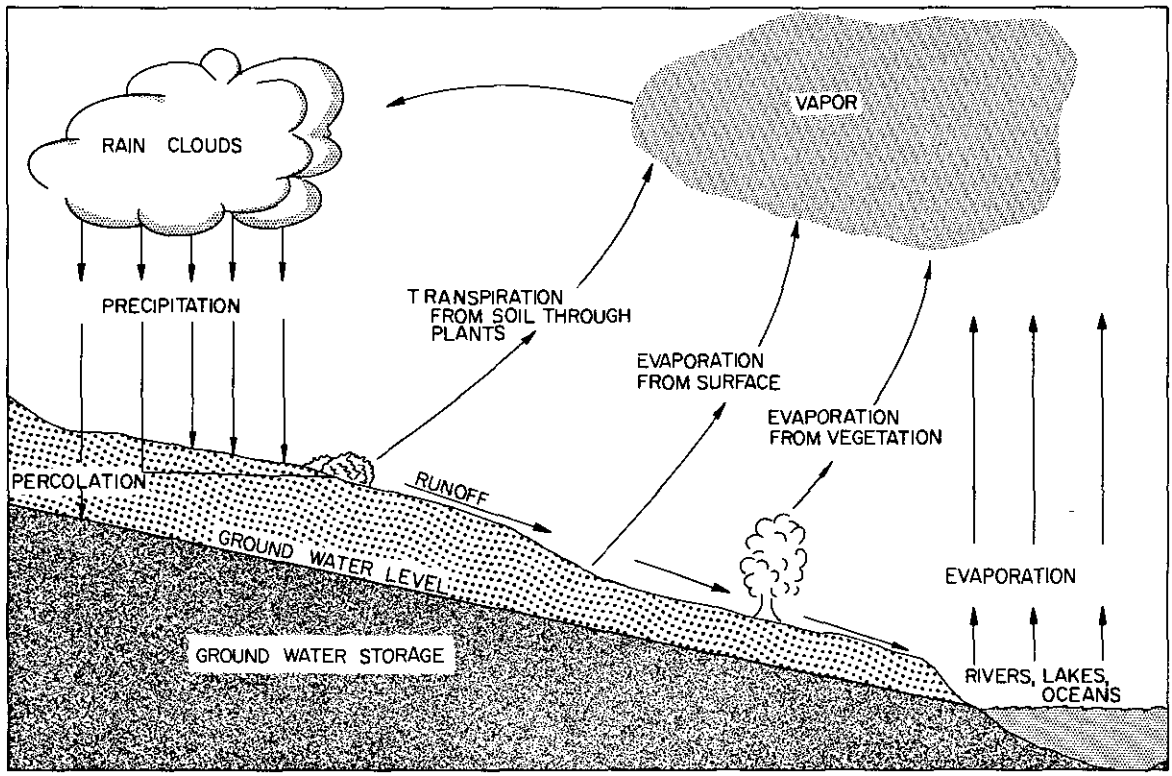


Figure 34. The hydrologic cycle.

b. Water Table. When water fills the pores and crevices of the underlying rock, a zone of saturation results. This is ground water and the top of the saturated zone is the groundwater table, or simply, the water table (fig. 35). The depth of the water table beneath the surface varies according to topography, structure of the rock formations, amount of rainfall, and nature of the pore spaces in the soil or rock. Water stored below the water table is the source of supply for springs and wells. If the water table intersects the land surface, as it may on the sides of valleys, the water will flow or seep out as gravity springs or seeps.

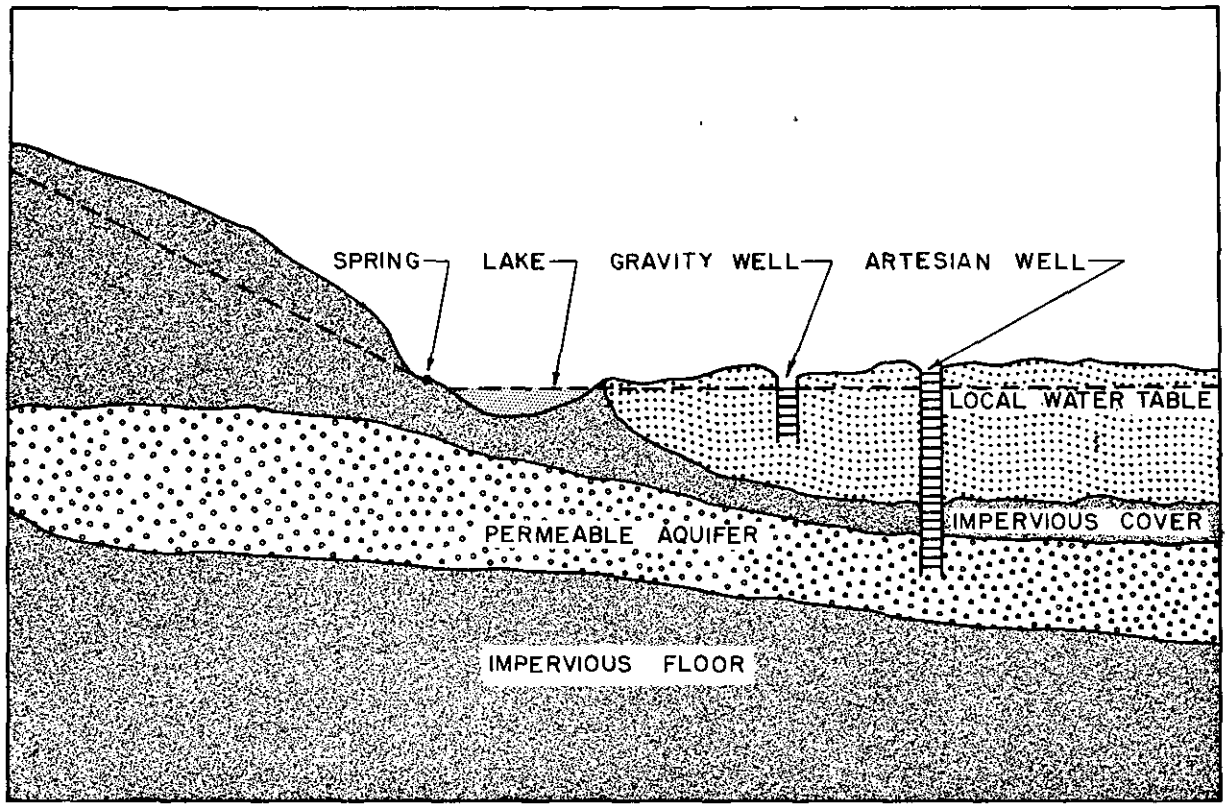


Figure 35. Water sources.

c. Springs and Seeps. Subsurface water issuing at the surface as a spring has a distinct current, flowing continuously or intermittently from a localized area. Water issuing as a seep emerges slowly over a large area, without a noticeable current. Springs and seeps are of two principal kinds; gravity and artesian.

(1) *Gravity springs.* Gravity springs and seeps are those in which the subsurface water flows by gravity from a higher point of intake to lower point of issue. This may occur where the water table comes near or intersects the surface of the ground, usually around the margins of depressions, along the slopes of valleys, and at the foot of alluvial fans. Another type occurs along an exposed contact between the overlying pervious stratum and an underlying impervious stratum. They may appear at almost any elevation along a slope.

(2) *Artesian springs.* Artesian springs occur where confined subsurface water acting under the influence of pressure from a higher water level is forced to the surface of the ground. Fissures in the rock, fault zones, and, in some cases, solution channels may serve as avenues along which water can move to the surface. The water is generally under much hydrostatic pressure, and therefore rises in the spring. Because of this rise, the spring or well is classified as artesian. A well with enough pressure to bring the water above ground is called a flowing artesian well. If the water rises only to an intermediate level, it is a nonflowing artesian well.

d. Circulation. Ground water is not static but moves slowly through openings in the rock and soil toward points of discharge. The rate of movement is controlled by gravity or hydrostatic pressure (the pressure exerted by water at a higher level) and by the capacity of the rock or soil to transmit water, termed its permeability. Climate governs the amount of

water that will be contributed to the surface. The amount that will be absorbed depends upon the amount of pore space, or the porosity of the ground.

68. Hydrological Effects on Military Operations

a. Rivers. Wide, deep rivers with valleys that offer concealment may provide good defensive areas. The employment of a river as a forward edge of battle area (FEBA), however, may also result in a frontage too wide for effective defense and with many covered areas that interfere with observation and fields of fire. Marshy terrain and ditches or tributaries interfere with lateral communications and the movement of reserves.

b. River Line. In the attack of a river line, the initial objectives are key terrain features that could permit the enemy to bring effective small-arms fire on the crossing area. Next are features that allow the enemy to deliver observed artillery fire, and, finally, those areas on the enemy side of the river that are required to accommodate the troops, equipment, and installations necessary to prevent the enemy from delivering effective sustained artillery fire. A river or stream may be a temporary obstacle to cross-country movement, but it slows down advancing forces only until it is bridged or assault boats can be brought to the site or a crossing by helicopter is effected. The effectiveness of a river as an obstacle increases with its width, depth, and velocity. Rivers more than 150 meters (500 feet) in width are major obstacles.

c. River Floods. Floods may cause long traffic interruptions particularly by damaging temporary bridges. A flood may immobilize a theater of operations unless an adequate system of stream-gaging stations and flood-warning agencies has been established for all key rivers. Streams in mountainous areas are characterized by a high velocity with considerable variation in their flow. While they may be effective obstacles during flood periods, they usually are so low in dry seasons that their beds may offer routes of approach rather than obstacles to movement. Such streams, however, are likely to have beds so rocky as to eliminate vehicular movement.

d. Lakes. Usually lakes are obstacles to movement because few are narrow enough to be bridged. They must be bypassed or crossed in amphibious vehicles or boats and where they exist in chains or large groups, as in glaciated areas, they become major obstacles (fig. 36). The narrow land corridors separating the lakes canalize troop movements and limit maneuver, rendering troops highly vulnerable to attack. A series of interconnected lakes may provide an extensive communication system and may also include navigable rivers and canals as in Finland. An ice cover that is 1 meter (3 feet) or more in thickness will support heavy loads. Roads across frozen lakes may be prepared by clearing away the snow.

Figure 36. Arctic lake region (Northwest Canada).

e. Marches and Swamps. Normally movement through a swamp or marsh is usually limited to causeways, but many vehicles are now used in swamps in what is known as a riverine operation. These may be key terrain features that could be seized by airborne, airmobile, or mechanized forces prior to a large-scale movement. Mud and peat bottoms usually prevent cross-country movement. Special engineer floating and portable bridging equipment may be necessary to supplement other means of traversing a swampy area or to cross or bypass a gap in a causeway. Snow roads may be built over swamps by removing the snow and then pouring water over the cleared surface until a frozen surface is obtained.

69. Information Requirements — Drainage

Major drainage areas are shown on maps of appropriate size accompanying some terrain studies. Textual notes are provided if the important facts cannot be shown adequately on a map. Detailed information on features of military significance along a stream or portions of it may be shown on a strip map or annotated photomosaic. Information may include—

a. Rivers and Streams.

(1) Name or other identification, and location.

(2) Channel characteristics (form (fig. 37), length, profile, gradient of stream bed).

(3) Bottom characteristics (composition, depth, firmness, unusual conditions).

(4) Flow characteristics.

(*a*) Measurements and periods of occurrence at low, high, and mean water of depth, width, volume of discharge, and velocity (minimum, maximum, and mean).

(*b*) Special phenomena (crosscurrents, undertows, eddies, floods); periods; area covered; destructive effects. Tidal effects at low, high, and mean tides.

(5) Physical and chemical characteristics of water (turbidity, color, odor, taste, temperature, chemical composition, bacterial pollution, seasonal variations).

(6) Bank characteristics (composition, stability, height, and slope).

(7) Regulatory structures (levees and dams).

(8) Islands, bars, shoals, and rapids (name, size, surface roughness, elevation, and pattern).

(9) Ice (earliest, latest, and mean freezing and breakup dates, extent of frozen surface; thickness of ice; carrying capacity; and frequency and location of ice jams).

(10) Kind and prevalence of animal and vegetable life.

(11) Type and location of crossings.

(12) Utilization of watercourse (for water supply, irrigation, disposal of waste).

(13) Accessibility for military water supply (relation of road nets to potential water points, off-road approaches, intake problems).

b. Lakes.

(1) Name or other identification, and location.

(2) Length, width, depth and surface area at low, high, and mean water; periods of occurrence of each.

(3) Gage locations and periods of record, zero gage elevations, mean and extreme gage heights and periods of occurrence.

(4) Shore characteristics (composition, stability, height, and slope).

(5) Physical and chemical characteristics of water (turbidity, color, odor, taste, temperature, chemical composition, bacterial pollution, seasonal variation).

(6) Bottom characteristics (composition, depth, and firmness of material, unusual bottom conditions, profiles).

(7) Regulatory structures.

(8) Islands, bars, and shoals (name, size, surface roughness, elevation, and pattern).

Figure 37. Characteristic braided stream drainage pattern (Canada).

(9) Ice (earliest, latest and mean freezing and breakup dates; extent of frozen surface; type and thickness of ice; and carrying capacity).

(10) Kind and prevalence of animal and vegetable life.

(11) Type and location of crossings.

(12) Utilization of water body (for water supply, irrigation, disposal of waste).

(13) Accessibility for military water supply (relation of road nets to potential water points, off-road approaches intake problems).

c. Marshes and Swamps.

(1) Information in *b* above, as applicable.

(2) Seasonal variations (months when variations in extent and wetness are greatest and least).

(3) Cross-country movement under various seasonal conditions.

(4) Existing or potential causeways.

(5) Special conditions (quicksand, permafrost).

Section IV. NEARSHORE OCEANOGRAPHY

70. Beaches

a. Description. A beach is defined as the area extending from the shoreline inland to a marked change in physiographic form or material, or to the line of permanent vegetation (coastline). In amphibious operations, it is considered that portion of the shoreline designated for landing a tactical organization. Beaches are characterized according to their predominant surface material, such as sand, silt, cobble, pebble, boulder, or by combinations of these materials, such as sand and pebble. Mud beaches are common, but silt is not usually found in beach form, occurring more commonly in underwater banks and shoals. In general, beaches are long and continuous on low-lying coasts, or on shores with soft rock formations, and where there is an abundant supply of material deposited by streams. Along hard-rock coasts and on those not well supplied with stream-carried material, beaches are short and discontinuous, and are usually separated by bold headlands or rock outcrops (fig. 38).

b. Width. The width of a beach is subject to considerable change. Where there are seasonal variations in wave attack and the supply of material, beaches may disappear or be greatly damaged when the wave attack is heaviest. Beaches formed principally by streams usually show marked seasonal variations in width, and are widest during the period of least rainfall. Beach widths are most nearly constant when the beaches are protected by groins or similar structures.

Figure 38. Characteristic coastline, hard-rock terrain (Brazil).

c. Slope. The slope of a beach is determined chiefly by the size of the beach material and the intensity of wave attack. Beaches of fine sand that are not subject to intense wave action commonly have slopes ranging from 1 on 5 to 1 on 60. Coarse material under light wave attack results in beach slopes from 1 on 5 to 1 on 10. The band of wave uprush on a beach is a good indication of the slope. On air photographs it may appear as a dark band lying just landward of the waterline. A wide uprush band indicates a flatter slope than a narrow band. On gravel beaches, however, uprush bands are always narrow, and usually do not appear clearly on aerial photographs.

d. Firmness. There is a wide variation in firmness between different beaches and different parts of the same beach. Beaches are most firm when damp and when the material size is small. Dry sand usually is soft, except when the material size is small. Pebble, cobble, and boulder beaches are firm as far as bearing strength is concerned but are loose, making it difficult for tracked vehicles to cross them. Silt and clay are invariably soft, but combinations of mud and sand provide a hard surface. As a rule, exposed beaches are firmer than similar beaches in sheltered locations.

e. Vegetation. Vegetation immediately in rear of a beach is an indication of stability. Such areas are firmer than other parts of the beach and always lie above the limit of wave uprush. There is no vegetation on gravel beaches, but beaches composed of gravel and sand in combination may have a vegetation cover.

f. Assault Landing. Assault landing is based upon the potential of the beach and hinterland to permit the initial landing and the logistical support for the operation. Attack transport ships (APA) and attack cargo ships (AKA), which have a loaded draft of 8 meters (27 ft) and 7.3 meters (24 ft), respectively, require landing crafts for unloading. A landing ship tank (LST) requires a maximum draft of 4 meters (13 ft), a landing craft medium (LCM) 1.5 meters (5 ft), and a landing craft, utility (LCU) 2 meters (6.5 ft). Additional aid in landing supplies and personnel include mobile pier sites such as the Spud Barge pier, bridging and engineer equipment required to prepare the terrain for landing.

g. Fresh Water. Fresh water is seldom available on undeveloped beaches, although it may be obtained from nearby streams or in completely inclosed pools or lagoons that lie immediately behind the beach. Streams or rivers with steep gradients that cross the beach will provide fresh water at sites above the highest reach of the tide.

71. Terrain Adjacent to Beaches

a. Ridges. Beach ridges are mounds of beach material heaped up by wave action along the upper limit of wave uprush as single ridges or as a series of approximately parallel ridges extending some distance inland. Commonly these ridges reach from 1 to 2.5 meters (3 to 8 feet) above mean high tide, but individual ridges may be as high as 9 meters (30 feet). High ridges are found only in exposed locations, and are signs of occasionally severe storm wave action. Ridges occur only when there is an abundant supply of material on or in back of the beach. In some locations belts of beach ridges extend for 2 or 3 kilometers (a mile or two) inland, with a vertical difference in elevation of only a meter (few feet). Usually these areas are covered with grass or low bushes.

b. Dunes. Dunes are formed by windblown sand carried inland from the beach and deposited as irregular hills or mounds. The sand is of fine to medium size. Dunes may reach heights of 90 meters (300 feet), although commonly they do not exceed 30 meters (100 feet) in height. Where there is vegetation, low bushes, and grass the dunes are fairly firm and can be crossed by light vehicles. Fresh water may be obtained from wells sunk in depression between dunes (fig. 39).

72. Underwater Topography

a. Description. An examination of the terrain as shown in photographs, topographic maps, and hydrographic charts will indicate the probable characteristics of the hydrography. If the land behind the beach is flat and sandy or marshy, the sea bottom close inshore also will be fairly flat. A beach located on a long stretch of regular coastline normally will have one or more sandbars offshore. Large rock outcrops along the beach or close inland indicate that there are probably similar outcrops under-

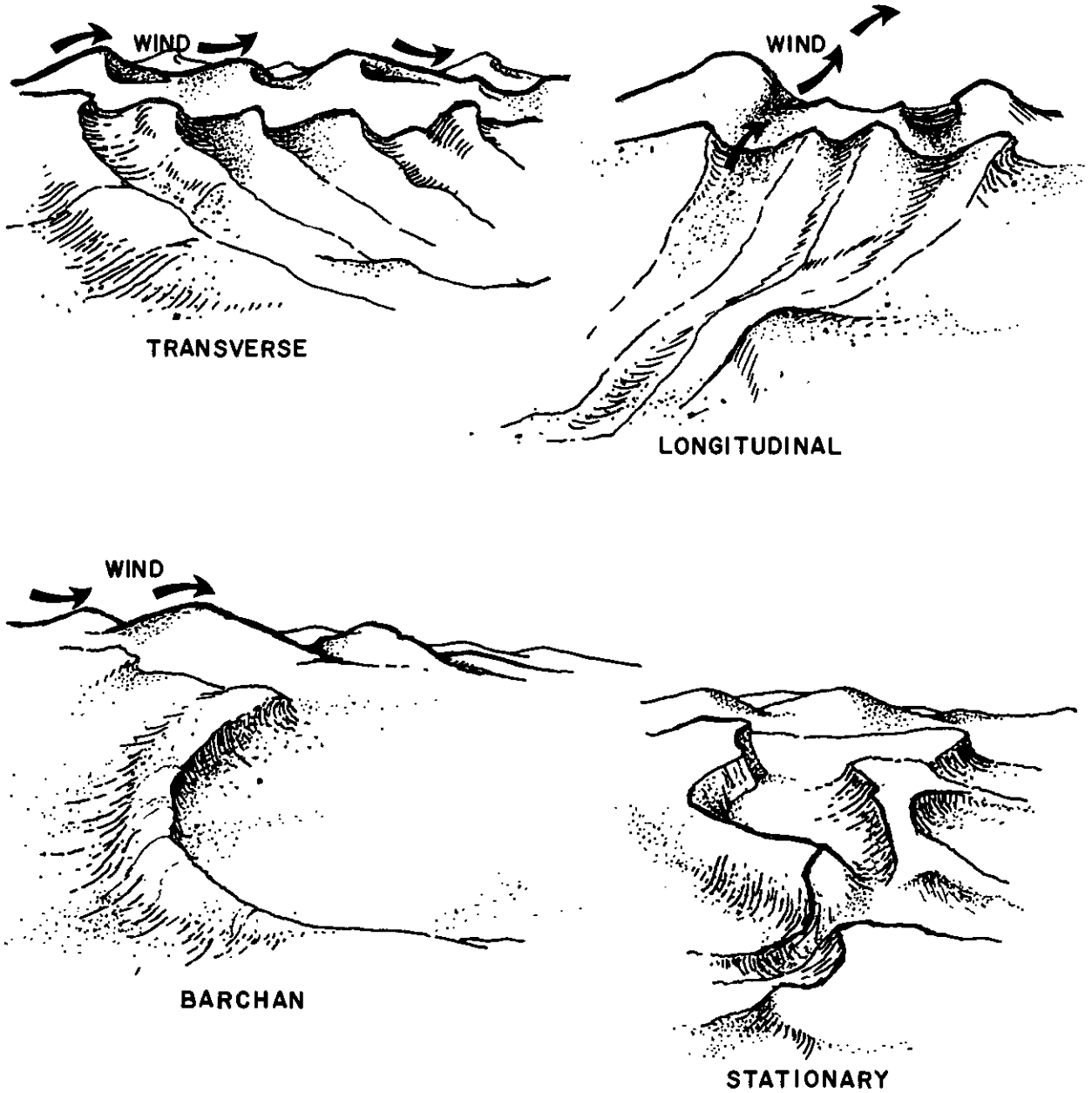


Figure 39. Windblown stationary dunes.

water near the shore. Beaches backed by cliffs or steeply rising hills generally will have a fairly steep underwater gradient. The form of the beach also indicates the underwater contours. A wide, flat beach is an indication of a gently sloping bottom offshore, and a sharp narrow beach suggests a steep slope. Sand beaches have flat to steep slopes, and beaches of gravel, cobble, or boulders are usually steep. It must be remembered, however, that the entire beach profile is changeable, varying with the wave conditions that act upon it. Short concave or pocket beaches (fig. 40) flanked by well-developed headlands are the most constant in their form.

b. Bottoms. The characteristics of the materials that comprise the nearshore bottom are significant in relation to their suitability for the movement of men, vehicles, and landing craft. Bearing strength and smoothness of grad-

Figure 40. Concave beach.

uations are the most important factors. Sand, sand and shell, and gravel bottoms are ideal for landing operations. They are firm and usually quite smooth, although bank, bar, and shoal formations are common. Sand and mud mixtures may be either firm or soft, but they usually are smooth. Mixtures with a high percentage of sand are firm, the firmness decreasing as the sand content is reduced. This type of bottom often has soft spots that may prove hazardous. Mud bottoms are generally avoided, since they are soft, smooth, and slippery. An exception is the case of a thin mud cover overlying a rock bottom, where the rock provides an underlying formation that will give a satisfactory bearing surface if the mud is not more than a meter thick. Clay bottoms are unsatisfactory, since they are soft and slippery and have little strength.

73. Coral Reefs

a. Description. Reef-building corals are marine animals that remove lime from sea water and deposit it around their living bodies, making hard structures of many types. They do not flourish at temperatures much under 75° F. Consequently coral reefs are found only in tropical waters. Since corals cannot move, securing microscopic food from water moving around them, they are usually found near the edge of reefs, along channels, and out from headlands. They cannot form opposite muddy streams or those with a heavy discharge. If the water movement in coral areas is swift enough, rounded coral heads will predominate, and in more quiet water there usually is an open growth of branching corals. Reef corals cannot stand exposure to the air for more than a few hours, so that their upward growth is limited by the level of mean low water. They belong to one of three types—fringing reefs, barrier reefs, or atoll reefs (fig. 41).

b. Fringing. A fringing reef is attached to the shore. If the wave attack is weak, there will be a gently sloping beach of coral sand. Strong wave attack results in steep gravel, cobble, and boulder beaches. On most fringing reefs there are boat channels about 0.3 to 4.5 meters (1 to 15 feet) deeper than the rest of the reef-flat, from 10 to 45 meters (10 to 50 yards) or more wide, and more than a mile in length. These run approximately parallel to the land, opening into breaks in the reef, and providing convenient waterways for small craft.

c. Barriers. Barrier reefs are located roughly parallel to the coastline at some distance offshore. Whether or not a craft can cross a barrier reef depends upon the depth of the coral below water. Usually the coral surface is about 15 centimeters (6 inches) above mean low water, but it may be deeper. Walking upon the reef is dangerous, since the reef-flat is seldom above water and the holes between coral colonies are irregularly spaced, deep, and lined by jagged coral. At low water, extensions of the reef into the lagoon behind it may create compartments that hinder or prevent the free movement of craft along the reef.

d. Atoll. Atoll reefs (fig. 42) are more or

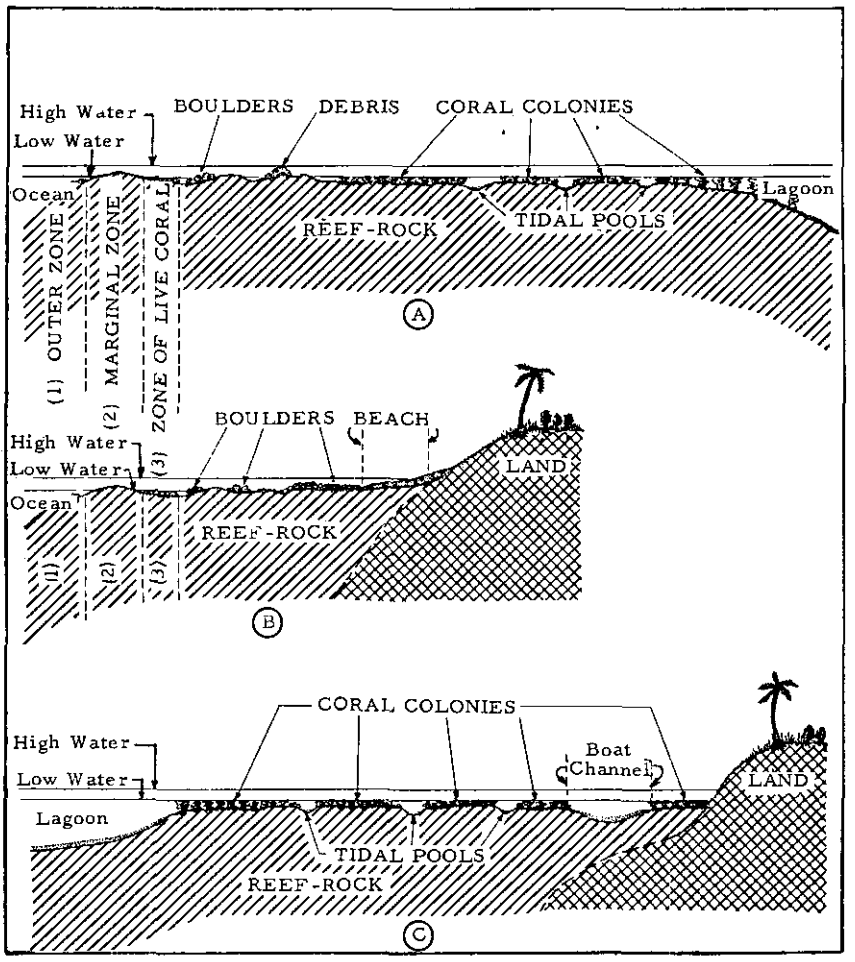


Figure 41. Barrier and fringing reefs—diagrammatic cross-sections.
(A) Wide barrier reef.
(B) Narrow exposed fringing reef.
(C) Protected fringing reef. (Not drawn to scale.)

less rings of coral inclosing circular lagoons. The marginal zone of the reef is a strip from 25 to 70 meters (25 to 75 yards) wide, across which a belt of surf moves with the rise and fall of the tide. If the outer, seaward slope of the reef is steep, there is a clear approach for landing craft. A gentle slope will have coral heads growing just outside, making an approach dangerous. At high tide it may be possible to cross the marginal zone by boat. Reef islands usually are located on higher parts of an atoll reef. Typically these islands are surrounded or partly surrounded by a beach 3 to 15 meters (10 to 50 feet) or more wide, consisting of coral sand and organic debris. Reef islands are seldom more than 3 to 4.5 meters (10 to 15 feet) higher than the reef-flat, and their interiors usually are flat and featureless. From the viewpoint of landing operations, the most unfavorable feature is the high, surf-covered marginal zone. Surf intensity is less on the leeward side. On the lagoon side by entering through channels or breaks in the reef, craft may land on the sand beach at high water. Crossing the reef-flat at low tide is impracticable.

74. Military Considerations

a. Coastlines. A concave coastline is formed by a projection of water (bay or gulf) extending into the coast. From the flanks, converging fires may be brought upon landing forces. The convex type of shoreline includes gently outcurving shores, points, capes, and peninsulas. Supporting fires may be placed on the defender

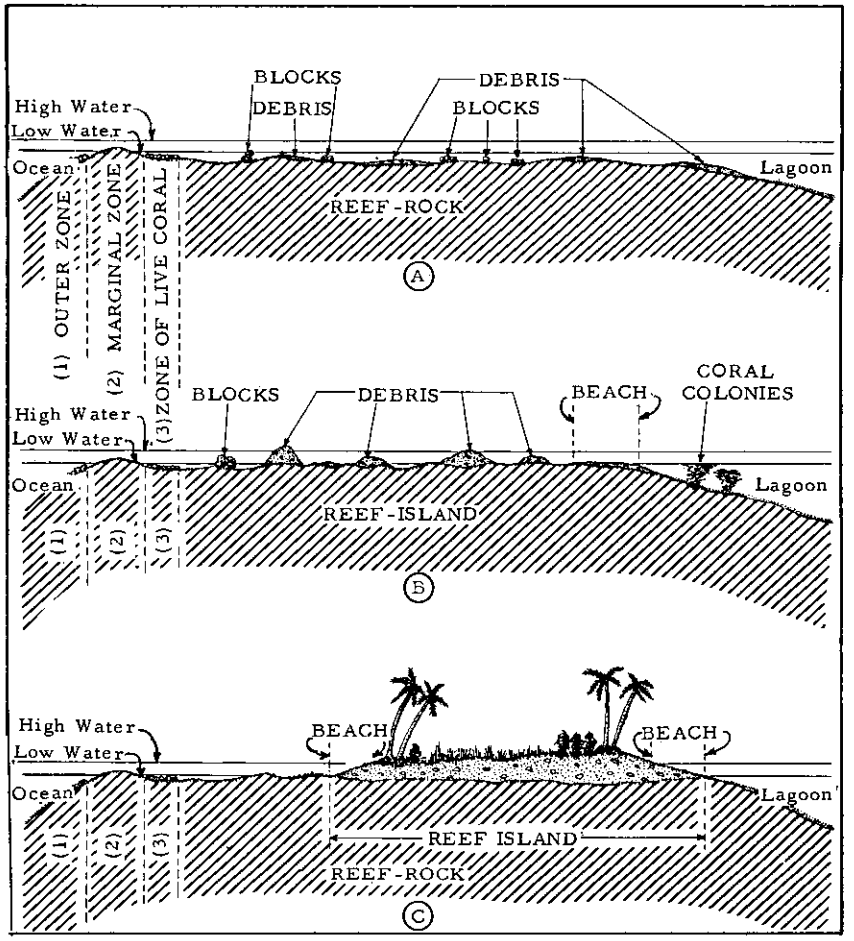


Figure 42. Atoll reefs—diagrammatic cross section.
(A) Open reef area.
(B) Area of impermanent debris accumulation.
(C) Reef-island area. (Not drawn to scale.)

from his flanks and, occasionally, from his rear. His routes of withdrawal or reinforcement are restricted. It is difficult for the defender to organize his fires and to secure extensive fields of fire. Convex shorelines are more exposed to currents, winds, and surf and are often steep and rocky, making landing difficult. A straight shoreline has no prominent indentations or promontories. It offers no decisive advantage either in attack or defense. Very few coastlines, however, are so straight that provide no positions for flanking fires. An irregular coastline is a complex of concave and convex shorelines.

b. Reefs. Barrier and atoll reefs may be obstacles at a distance from the landing beach. A fringing reef forms a nearshore obstacle, normally with a rough tablelike surface, that extends seaward from the shoreline at a level slightly above or below the water. A wide fringing reef provides an area well suited to the organization of defensive smallarms fires.

c. Offshore Islands. Frequently shorelines are protected by groups of small islands lying so close to the mainland that they form a complicated system of waterways immediately offshore. Routes of approach to the mainland through the islands may be tortuous and restricted, making an approaching landing force highly vulnerable throughout its shoreward movement. These islands may be neutralized with nuclear weapons or may be isolated and reduced in detail by successive minor landings preceding the main amphibious attack. Once

secured, they provide the attacker with favorable artillery positions to support the landing.

75. Information Requirements — Landing Areas

Terrain studies made for planning amphibious operations are very detailed. Normally they are based upon the complete data that is provided by special studies and major sources. In general, the following items represent the fundamental information requirements relative to a proposed landing area:

a. Location.

(1) For a beach 3 kilometers (2 miles) or more in length, the latitude and longitude of its limits; for a beach less than 3 kilometers (2 miles) long, the center of the landing area is given.

(2) Nearness to objective of the operations, if known, and to developed areas such as water terminals, harbors, and adjacent beaches.

b. Sea Approach.

(1) Landmarks, both natural and man-made.

(2) Hydrography (nearshore and offshore depths; flats (tidal or other), character of the material and its bearing strength; length of and depths over reefs, bars, shoals, or other natural obstructions; anchorage areas and their conditions; character of nearshore bottom material).

(3) Tides and currents (tidal rise and fall, local peculiarities, direction and magnitudes of currents; neaps and springs).

(4) Winds (strength, direction, effect on tidal heights and surf, local peculiarities).

(5) Waves and surf (height and period of offshore waves; intensity).

c. Beach.

(1) Material (type and size, firmness, variability with weather or season, subsurface material).

(2) Gradient (note particularly scarps and ledges).

(3) Beach structures (groins, bulkheads, jetties, submerged remains of former structures).

(4) Rivers and streams (variability in beach character where rivers cross beach; river channels).

(5) Effects of weather and duration of darkness and daylight.

(6) Local use of beach.

(7) Sources of fresh water on or near beach (both potable and nonpotable).

d. Terrain Inland or on Flanks.

(1) Topography (topographic features, waterways, swamps or marshes, vegetation, location and size of possible dump or assembly areas).

(2) Exits (existing exits by roads or trails; cross-country exits; roads, with details of width, surface, construction; railways, tramways).

(3) Aircraft landing sites within a 16- to 24-kilometer (10- to 15-mile) distance from beach (dimensions, surface, topography).

(4) Utilities (communications, electricity, water supply, transportation).

(5) Helicopter landing sites.

Section V. SURFACE MATERIALS

76. Types of Soils

a. Composition. Soil is defined as the unconsolidated material that overlies bedrock. Soil is made of disintegrated rock, in the form of sand or clay, and humus, the disintegrated remains of past vegetation. Detailed information about soils, their engineering properties, and testing techniques is contained in TM 5—541. Some essentials of soils trafficability are given in chapter 9. For field identification and classification, soils may be grouped into five principal types: gravel, sand, silt, clay,

and organic matter. These types seldom exist separately but are found in mixtures of various proportions, each type contributing its characteristics to the mixture.

b. Gravel. Gravel consists of angular to rounded, bulky mineral particles ranging in size from about 0.6 to 8 centimeters (¼ inch to 3 inches) in diameter. It is classified as coarse or fine; well or poorly graded; and angular, flat, or rounded. Next to solid bedrock, well-graded and compacted gravel is the most stable natural foundation material. Gravel is easy to drain, easy to compact when well graded, affected little by moisture, and not subject to frost action.

c. Sand. Sand consists of mineral grains ranging from about 6 millimeters (¼ inch) down to about 0.08 millimeters (.003 inch) in diameter. It is classified according to size and gradation as coarse, medium, or fine; and as being angular or rounded. Well-graded angular sand is desirable for concrete aggregate and for foundation material. It is easy to drain, little affected by moisture, and ordinarily not by frost action. Sand provides an excellent road subgrade material when it is confined. Care is required, however, to distinguish between a fine sand and silt.

d. Silt. Silt consists of natural mineral grains ranging from about 0.08 millimeters (.603 inch) to about .005 millimeters (.0002 inch) in diameter. It lacks plasticity and possesses little or no cohesion when dry. The term rock flour is commonly used to describe inorganic silts of glacial origin. All silts are treacherous for trafficability and as a foundation material. Because of its inherent instability, slight disturbances in the presence of water, such as traffic vibrations transmitted to a wet silt subgrade, will cause the silt to become soft or to change to a "quick" condition. When ground water or seepage is present, silts exposed to frost action are subject to intensive ice accumulation and consequent heaving. Silts are difficult to compact and drain.

e. Clay. Clay generally consists of particles smaller than 0.005 millimeters (.0002 inch), microscopic in size. Its plasticity and adhesiveness are outstanding characteristics. Depending upon the proportion of coarser grains, clays vary from lean clays (low plasticity) to fat clays (high plasticity). Many clays which are brittle or stiff in their undisturbed state become soft and plastic upon being worked.

77. Soil Maps

a. Contents. Soil maps or overlays indicate the predominant soils in given areas, identifying them according to their engineering characteristics. Such maps may be constructed from air photographs or ground reconnaissance or made from existing soil and geologic maps and reports with the classifications expressed in engineering terms. Agricultural soil maps can be large enough to provide detail for tactical planning, but often the designated soil type applies only to the surface soil. These maps should indicate the following properties of soils:

(1) Permeability.

(2) Stability under stress.

(3) Bearing capacity.

(4) Important variations of (2) and (3) above with changing moisture content.

b. Coverage. For strategical planning, soil maps should cover the area of the study. A large amount of general information may be presented, because detailed plans may not be firm and the future weather conditions uncertain. The information includes the effects of weather upon the soils. The reliability of the information must be clearly indicated.

c. Planning. Soil maps for tactical planning cover a smaller area than do strategical soil maps. They are of a larger scale and contain more precise, detailed information. Greater accuracy is possible because more details are known about the proposed operations. Reconnaissance and patrol reports make it possible to check the ground, and weather forecasts are available to indicate what the prevailing weather will be. The information contained on such maps is useful in determining—

(1) Areas critical to cross-country movement as they affect both advances and counterattacks.

(2) Stretches of road liable to failure under heavy traffic.

(3) Suitable and unsuitable areas for airfields, field fortifications, and other installations.

(4) Areas with soil conditions that are unsuitable for tank and vehicle parks.

(5) Difficult areas for field and air defense artillery deployment.

(6) River bank conditions for bridge foundations and crossing operations.

d. Rear Areas. In planning rear area activities, soil maps are useful for determining road conditions. In order to stand up under heavy traffic during periods of frost and thaw, a road must have a well-drained subsoil foundation. A knowledge of the soils in an area will reveal which stretches of road will be most susceptible to breakdown during a thaw, providing a guide to selecting the best supply routes and indicating portions of the road where precautions must be observed. When supplemented by an aerial reconnaissance, soil maps are a valuable aid in highway location and relocation. They indicate the soil areas with desirable or undesirable engineering characteristics and also show the nearest sources of materials for road construction and maintenance. The information about soil conditions given by a soil map is invaluable in selecting sites for airfields, storage installations, ammunition dumps, and vehicle parks. Preliminary study of the map prevents unnecessary field reconnaissance.

78. Military Aspects of Soils

a. Weather. The actual identity of the type of soil in any area is of little practical value unless the soil is also evaluated in relation to the existing or predicted weather. In general, the major soil types have the following characteristics:

b. Gravel. Weather has little or no effect on the trafficability of a gravel soil which is excellent for tracked vehicles. It it is not mixed with other soil, however, the loose particles may roll under pressure, hampering the movement of wheeled vehicles.

c. Sand. When wet enough to become compacted, or when mixed with clay, sand gives excellent trafficability. Very dry, soft, or loose sand is an obstacle to vehicles, particularly on slopes.

d. Silt. When dry, silt provides excellent trafficability, although it is very dusty. Silt absorbs water quickly and turns to a deep, soft mud when wet, imposing a definite obstacle to movement. It dries quickly after a rain, soon becoming trafficable again.

e. Clay. When thoroughly dry, clay provides a hard surface with excellent trafficability, but it is seldom dry except in arid climates. Although clay absorbs water very slowly during a rain, it also takes a long time to dry. Wet clay is very sticky and slippery. Slopes with a clay surface are difficult or impassable, and deep ruts form rapidly on level ground. A combination of silt and clay makes a particularly poor surface when wet.

f. Special Soil Conditions. If a soil has underlying bedrock near the surface, it will become thoroughly saturated after a rain. The water cannot drain away, making the surface untrafficable.

g. Manmade Effects. Soil under cultivation because it has been worked is softer and absorbs water more quickly than other soils and may therefore have poorer trafficability. Usually the presence of irrigation structures indicates that the soil is soft and contains water and the soil generally will have poor trafficability. The types of crops cultivated in an area provide indications as to the nature of the soil. Since gravelly soils are especially suitable for fruit orchards, for example, the presence of extensive orchards, especially on flat areas, may indicate that the soil has a high gravel content. Many cultivated plants have specific soil and water requirements, giving a clue to the soil and drainage of the area.

h. Nuclear Weapons. Soil composition and density affect the amount of damage by shock that will result from a surface or subsurface burst. Propagation of the shock wave is poorest in light, loamy soils and best in plastic, wet clay. The pressures transmitted by the blast may be 50 times greater than those transmitted through sandy clay. The size and shapes of craters produced by a surface or subsurface burst, their effectiveness as obstacles and the

intensity and decay rate of induced radiation in the soil are also affected by the soil composition and density.

79. Information Requirements—Soils

In a terrain study, soil information usually is presented in tabular form, with the data keyed to a soil map or overlay. It covers—

a. Extent of each dominant soil type.

b. Depth of each type in areas indicated.

c. Surface texture (fine or coarse).

d. Parent material.

e. Description of material.

f. Properties when wet, dry, or frozen, including suitability for specified military vehicles under various conditions, bearing capacity for structure foundations, and permeability when wet.

g. Variations from dominant soil type in specified areas.

h. Areas of permafrost, permanent ice and snow.

i. Seasonal state of the ground (dry, wet, flooded, frozen, snowcovered) by seasons, months, or shorter periods. Effects of each state on cross-country movement, construction, excavation, cover and concealment, and other military aspects.

80. Rock

a. Classification. Rock may be defined as the firm and coherent or consolidated material of the earth's crust. Bedrock is solid undisturbed rock either exposed at the surface or underlying the soil. Igneous rock is formed by cooling and solidification from a molten or partly molten state; sedimentary rock, from material accumulated as a deposit from water or the air, and metamorphic rock, by the recrystallization of igneous or sedimentary rock under the influence of heat, pressure, or both. The information, characteristics, and uses of rock are explained in TM 5–545.

b. Underground Installations. Underground installations require rock and soil that are easily worked and locations that are accessible to transportation and power facilities. Plains, terraces, and alluvial fans usually are best for bunker type installations. The most favorable terrain for tunnels normally is found on plateaus, escarpments, high hills, and mountains with steep bare-rock surfaces. Large bunkers require deep, well-drained soils, with the water table at least 4.5 to 6 meters (15 to 20 feet) below the surface. They should be protected against surface-water flooding, especially if they are located on low plains. Military tunnels may be constructed for tactical, communication, storage, and shelter purposes, including—

(1) Undermining of enemy positions and countermining.

(2) Galleries for water supply.

(3) Fortifications (headquarters, gun emplacement, ammunition storage, defensive installations).

(4) Underground factories and hangars.

c. Tunneling.

(1) *Construction.* Before tunneling operations are initiated, a geologist should evaluate the proposed site. Tunnel type installations are favored by high, steep slopes of exposed bedrock. The tunnel is kept dry by placing the lowest levels above the water table and by constructing it in rocks that have a minimum of fissures, joints, and faults that would permit seepage and flooding. The size of the chambers depends upon the stability of the rock. The thickness of natural cover required to give adequate protection depends upon the type of rock and soil, degree of soundness of the rock, absence of joints and fissures, and the size and shape of the underground openings.

(2) *New methods.* In Viet Nam extensive hand-dug tunnels and tunnel complexes have been found. They are used as hiding places, caches for food and weapons, headquarters, and protection against air attack and artillery fire. They have concealed entrances and exits, camouflaged bunk-

ers, trap doors, and dead ends to confuse the attacker. One trap door may lead to a short change-of-direction tunnel and another door to a second change of direction, and a third door to the main tunnel. There are also multilevel complexes with storage and hiding rooms at lower levels. Some of these have air or water locks as "firewalls" to prevent blast, fragments, gas or smoke from passing from one section to another. The entrances are camouflaged and booby-trapped.

81. Information Requirements—Rock

Terrain studies of an area will be concerned chiefly with the availability of unexploited natural deposits suitable for the construction of roads, protective works, airfields, and underground shelters. The particular information that will be required depends upon the purpose of the study. Requirements may include—

a. Rock Deposits.

(1) Location and extent of deposit.

(2) Type and properties of the material.

(3) Suitability for construction use (as aggregate, binder, surfacing, ballast, riprap, masonry construction material).

(4) Accessibility.

b. Underground Shelters.

(1) Existing areas (mines, caves, underground manmade installations). Characteristics. Special constructions.

(2) Areas suitable for development (rock structure, comparative advantages and disadvantages of indicated locations).

Section VI. VEGETATION

82. Broad Classification of Plants

Vegetation may be classified in four broad categories—trees, shrubs, grasses, and cultivated vegetation. The type of vegetation in an area gives an indication of the climatic conditions, soil type, drainage, and water supply. Seasonal seepage or a rise in the ground-water supply often is indicated by vegetation such as reeds, sedges, cottonwoods, and willows, which thrive wherever seepage occurs. Similarly, arid conditions are also indicated by characteristic desert vegetation. TM 5-545 describes the indications typical of various plant species.

83. Trees

a. Definitions. Trees are defined as perennial woody plants at least 10 feet in height, with single stems and definite crown shapes. A forest is an extensive area covered by trees growing in a close formation, so close that in most cases their crowns touch. Smaller areas covered by trees may be termed woods, groves, or woodlots. In the terminology used on U.S. Army maps, any perennial vegetation high enough to conceal troops or thick enough to be a serious obstacle to free passage is classified as woods or brushwood. Commonly, a deep woods is considered as one that is large enough to provide ample concealed maneuver space for large units deployed in depth. This would include a woods that would conceal both the assault and reserve echelons of a brigade in the attack. A shallow woods is one that is not large enough to conceal elements of this size. Dense woods are those where the growth is thick enough to interfere with visibility sufficiently to limit the maneuver of troops.

b. Characteristics. In temperate regions, trees are commonly found at elevations of not more than 2,440 meters (8,000 feet) above sea level. A good forest climate is one with a warm, rainy vegetative season, a continually moist subsoil, and low wind velocity. The growth of trees is greatly influenced by the temperature of the air and soil; even the hardiest conifers require a mean warm month temperature of at least 50° F.

c. Classification. Trees are classified as either deciduous or evergreen (fig. 43). Deciduous trees drop all their leaves seasonally, but evergreen trees retain their leaves throughout the

year. Trees are also either needleleaf or broadleaf. In the middle latitudes, needleleaf trees are predominantly evergreen, and broadleaf trees are predominantly deciduous. In the humid tropic, nearly all trees are evergreen because the climate remains uniform throughout the year. Almost all deciduous forests are located in the Northern Hemisphere. The important dimensions of trees in a wooded area are the diameter of the tree stems at breast height, the average height of the trees, and the average height above ground of the lowest branches.

Figure 43. Mixed vegetation, showing (a) evergreen trees, (b) deciduous trees, (c) brush, and (d) sedges (Northern Manitoba).

84. Low-Latitude Forests

In the low latitudes, tropical rain forests, swamp forests, and moss forests are the principal types.

a. Tropical Rain. In the tropics, rain forests (selva) blanket many square miles of moist low lands in regions where rainfall is heavy and well distributed throughout the year, with no marked dry season. The Amazon Basin and West Central Africa are the two largest areas of tropical rain forest, although it is also found along many rainy coasts and on tropical islands. This type of forest covers more than one-tenth of the earth's total land surface and comprises nearly one-half of the total forest areas of the world. The rain forest consists of broadleaf trees of many species that form a canopy thick enough to shut off most sunlight. The trees are commonly from 30 to 45 meters (100 to 150 feet) in heights, with large diameters, smooth trunks, and few lower branches. *Lianas*, rope-like plants that entwine themselves around trunks and branches, are common. Usually the undergrowth is not dense, although it restricts observation. In the deepest shade, there is usually only a thick mat of ferns or herbs that offers no obstacle to movement. Typical jungle conditions, with thick and impenetrable undergrowth, are characteristic chiefly of sections where light reaches the forest floor, as one precipitous wet slopes, along rivers and coasts, and in abandoned agricultural clearings.

b. Tropical Swamp (fig. 44). This forest occurs in low terrain near or in swampy regions. Mangrove swamp forests (fig. 45) cover large areas along tropical salt-water coasts, presenting an almost impenetrable barrier to movement. This type of forest is found in the soft mud around river mouths, deltas, and inlets, along shallow bays on small islands, and upstream as far as the tidal influence is felt. Mangrove forests include several kinds of trees, all with thick buttressed roots that extend as high as 3 meters (10 feet) above the ground. These spread outward becoming interlaced in a network that makes movement by foot almost impossible and prohibits any type of vehicular movement. Nipa palms, which generally grow in or near mangrove swamps, also present almost impassable barriers (fig. 46).

c. Moss. This forest is found in the higher latitudes just above the rain forest areas, chiefly at altitudes of 915 meters (3,000 feet)

or higher on the tops of tropical mountains wherever high humidity and cloudiness are persistent. The trees are small with long overhanging branches. Moss grows on the branches, tree trunks, and ground, where it is intermingled with ferns and vines to form a blanket that conceals the earth. This moss often covers chasms and ravines, making them appear to be level terrain. The moss forest accordingly is hazardous to movement. It is dark and gloomy and so dense that very little sunlight penetrates the canopy. Visibility is extremely limited.

Figure 44. Swamp forest (air view) (Sanibel National Wildlife Refuge, Florida).

Figure 45. Mangrove swamp (Malay Peninsula).

85. Middle-Latitude Forests

a. Types. The principal forest types in the middle latitudes include Mediterranean scrub forests, broadleaf forests, and needleleaf forests.

b. Mediterranean Scrub. These consist of broadleaf evergreen trees adapted to regions with long, hot periods of summer drought. They are found in the borderlands of the Mediterranean Sea, as well as in California, Chile, southern Australia, and the Capetown region of Africa. These areas are subtropical, with mild, rainy winters and long, dry, hot sum-

Figure 46. Nipa palms (Northern New Guinea).

mers. This type of forest consists of low trees and woody shrubs. Where climate and soil conditions are most favorable, the virgin forest is composed of low, widely spaced trees with massive trunks and gnarled branches. Between the trees the ground is completely or partially covered by a pale, dusty bush and shrub vegetation resembling the soil in color. Cork oaks and olive trees are typical of this type of forest.

c. Broadleaf. Most of the temperate broadleaf forest is composed of deciduous trees with a seasonal leaf fall, such as oak, hickory, maple, ash, elm, walnut, beech, and poplar. Along the humid subtropical margins of the middle latitudes, principally in southern Japan, New Zealand, and southeastern Australia, there are evergreen broadleaf forests that resemble rain forests, with dense undergrowth and heavy vines. Temperate broadleaf forests vary widely in composition, the dominant tree species differing from one region to another. In some areas there are many conifers among them and the forest may be described as *mixed.*

d. Needleleaf. Needleleaf trees are almost exclusively evergreen. The growth and discard of the needles is a continuous process not confined to any particular period or season. Usually the needleleaf forests occupy the colder continental locations on the poleward side of the broadleaf forests. In areas of poor sandy soils, or on steep mountain slopes where soils are thin or rocky and temperatures are lower, needleleaf trees may supplant broadleaf trees even in the middle latitudes. South of the great belts of subarctic needleleaf trees there are large areas of needleleaf trees that provide valuable timber such as the forests of the Pacific Coast, western Canada, and Alaska. The southern pine forests in the Atlantic and Gulf Coastal Plains of the United States also are major sources of timber.

86. High-Latitude Forests

A wide belt of needleleaf forests extends from coast to coast in the subartic regions of Eurasia and North America below the treeless tundra regions. This Eurasian forest is the largest continuous forest area in the world. Needleleaf trees such as fir, spruce, larch, and pine predominate, although in the swamp areas

there are some broad leaf trees such as aspen, willow, birch, or mountain ash. The area has short, cool summers and long, dry, cold winters so that growth is slow, and few trees are more than 0.45 meter (1½ feet) in diameter. There are numerous large swamps and marshes covered with moss, and containing such trees as balsam and spruce. These areas usually rapidly become impassable after precipitation or during a thaw.

87. Shrubs

a. Description. Shrubs are woody plants usually less than 3 meters (10 feet) high with more than 1 stem. They include a variety of trees that have had their growth stunted because of soil or climatic conditions. Scrub growth includes cactus, stunted shrubs, sagebrush, mesquite, and similar plants found most frequently in arid or semiarid areas. Shrubs comprise the undergrowth in the open forests of middle latitudes. In many arid and semiarid areas they are the dominant vegetation. They are prevalent in the subarctic and in large, burned-over or cutover areas in humid regions.

b. Classifications. Shrubs, like trees, are either deciduous or evergreen, needleleaf or broadleaf. In the middle latitudes, most broadleaf shrubs are deciduous, and all needleleaf shrubs are evergreen. In the humid tropics, nearly all shrubs are evergreen. Most arid regions of both low and middle latitudes have some vegetation, both deciduous and evergreen, although it is sparse (fig. 47). It may consist of low bunch grass with widely spaced bushes or fleshy, water-storing plants such as the cacti. Most commonly, the vegetation comprises sagebrush and similar scrub growth. Perennial shrubs of the desert areas grow far apart, with considerable areas of bare soil in between due to the low rainfall. The rate of growth is very slow.

Figure 47. Characteristic desert vegetation (Arizona).

88. Grasses

a. Kinds. Grasses include all kinds of nonwoody plants. A grassland is an extensive area where the natural vegetation consists primarily of grass. In low latitudes, grasslands often are termed savannas; in middle latitudes, prairies (tall grass) and steppes (short grass). Grasslands in wet or poorly drained areas commonly are called meadows. For terrain intelligence

purposes, grass more than (1 meter) 3 feet high is considered tall, and below that height, short.

b. Tropical Grasslands (Savanna). In areas with heavy seasonal rains and a distinct dry season, the grasslands or savanna are composed mostly of tall, very coarse grasses that grow in tufts separated by intervals of bare soil. If there are trees, they usually are species that can withstand seasonal drought and they grow mostly in clumps in the grasslands or along the margins of streams. Savanna grass grows rapidly at the beginning of the rainy season, reaching heights of 1 to 3.5 meters (4 to 12 feet) in a few months. When dry, the blades become brown, stiff, and harsh in texture, burning very readily. The grasses usually diminish in height with decrease in the annual rainfall, and trees become fewer until under semiarid conditions nearly treeless steppes, composed of shorter grasses, are prevalent. Low-latitude savannas are usually located between desert and forest regions.

c. Prairie. The prairie type of grass occurs most frequently in areas where the soil remains moist for a depth of 75 centimeters (30 inches) or more. The prairies are covered with tall, luxuriant, and relatively deep-rooted grasses that grow to heights of from 30 to 90 centimeters (1 to 3 feet). Over most prairie regions, rainfall varies between 50 to 100 centimeters (20 and 40 inches) annually. Usually there is a large variety of flowering plants in spring and summer. The principal prairie regions include parts of central United States and the prairie provinces of Canada; the Argentine Pampa, Uruguay, and southeastern Brazil; the plains of the Danube in Hungary and Rumania; and parts of Manchuria and southern Russia.

d. Steppe. A steppe is an area of short, shallow-rooted grasses typical of semiarid regions where the depth of moist soil is less than 60 centimeters (2 feet). In common usage, the word steppe is used to describe all the drier, short-grass grasslands, both in tropical and middle latitudes. Some of the steppe grasses lie in a soft, fine mat on the ground, while others stand as hard, wiry tufts. Thorny shrubs and low, coarse bushes may dominate the steppe in some sections. Cacti and other succulent plants may be numerous. Steppe vegetation develops typically in regions that receive less than 50 centimeters (20 inches) of rainfall a year, with a hot summer and a cold, dry winter.

89. Cultivated Vegetation

a. Field Crops. Field crops constitute the predominant class of cultivated vegetation. Vine crops and orchards are common but not widespread, and tree plantations are found only in relatively few areas. The size of cultivated areas ranges from paddy fields covering a quarter of an acre to vast wheat fields. In a densely populated area, where all arable land is cultivated, each parcel will be used for the crop that brings the highest yield, making it possible to predict the nature of the soils from information about the predominant crops. Rice, for example, requires fine-textured soils. Other crops generally must have firm, well-drained land.

b. Orchards. An area of orchards or plantations usually consists of rows of evenly spaced trees, showing evidence of planned planting that can be distinguished on an aerial photograph. Usually such an area is free from underbrush and vines.

c. Rice Fields. Rice fields usually are flooded areas surrounded by dikes or walls approximately ½ or 1 meter (1½ to 3½ feet) in height and ½ to 1½ meters (1½ to 4½ feet) wide. When flooded for planting, the depth to the bottom mud ranges from 15 to 90 centimeters (6 inches to 3 feet).

90. Military Aspects

a. Key Terrain. Woods provide concealment and cover for assembly areas and during the approach march. Forests and heavy vegetation, however, increase the difficulty of maneuver in advancing to attack and in launching the assault. The attacker may have little or no information about the roads, trails, and topography in the area not under his control, due to the difficulty of securing detailed terrain intelligence without actual reconnaissance. Wooded and heavily vegetated areas provide cover and concealment for organized positions, shelter for reserve formations, and an obstacle to the attacking forces. Usually the defender

is able to make a detailed reconnaissance of the area, so that he is familiar with the roads, trails, and other features of the terrain. Infantry weapons form the basis of the defense, due to the difficulty of securing observed artillery fire in heavily wooded areas.

b. Observation and Fields of Fire.

(1) *Observation.* The height and density of the trees and other vegetation largely determine the amount of ground observation that can be obtained. To secure an adequate field of view from an observation post, it may be necessary to clear away vegetation at the risk of losing concealment. The effects of cultivated crops upon observation vary with seasonal conditions. In two or three weeks a cornfield may be covered with high stalks that limit observation. Later in the season, this corn may be harvested in a day, allowing observation again.

(2) *Fields of fire.* Lanes may be cut through vegetation to provide fields of fire, but it is seldom practical to cut lanes that extend far enough to provide long-range observed fires. Extensive clearing indicates the location of weapon positions to the enemy. The extent of clearing that is practicable will depend upon the amount of vegetation, its density, and the length of time that the positions will be occupied. Indirect fire is less affected by vegetation than direct fire. Mortars require little more than overhead clearance. Artillery weapons require more clearance than mortars, but high angle fire may be employed to avoid extensive cutting and clearing. Air defense artillery can be employed effectively in forests and areas of heavy vegetation when clearance requirements are met. Forests and heavy vegetation may be set on fire as a tactical weapon, particularly during dry season. Wooded areas and those covered with heavy vegetation tend to increase the persistence of gas and smoke, particularly during wet seasons or periods of high humidity. The influence of forests and heavy vegetation upon nuclear weapons effects varies with the amount of overhead cover, density of growth, kind of trees, nature of the tree crowns, undergrowth, and the litter on the forest floor. Trees in leaf offer a high degree of protection from thermal radiation if the cover is sufficiently continuous, but protection from initial nuclear radiation is insignificant.

c. Cover and Concealment. Thick forests of deciduous trees in leaf give excellent concealment from air observation when troops observe proper precautions in camouflage and movement. Evergreen forests will provide concealment throughout the year, changing color very slightly from season to season. Deciduous trees lose their leaves, reducing concealment, and change color, which increase the difficulty of natural camouflage. Usually undergrowth and small trees growing closely together give better concealment from ground observation than a stand of larger trees. Unless the undergrowth is high, however, it will provide little concealment from aerial observation. The amount of concealment and cover provided by cultivated crops depends largely upon seasonal conditions. Disruption of the agricultural pattern is readily apparent to aerial observers and in aerial photographs.

d. Obstacles. Fire lanes and certain types of vegetation often canalize movement through forest areas. This is true, for example when lines of trees border streams. Normally, no serious obstacle to movement is offered by shrubs and grasses, but visibility can be reduced in high grasses, with the added danger of reptiles to foot soldiers. Small grain crops hold soil nearly as well as grasses, so that movement is better in such areas than in those planted with row crops. Some parts of vineyards present a tangled maze of poles and wires that constitute a definite obstacle to vehicles and dismounted troops. The terraces and retaining walls on hillsides are also obstacles. Wheeled vehicles and some tracked vehicles are unable to cross flooded paddy fields, although they can negotiate them when the fields have been drained and the soil is thoroughly dry. In some cases even dried paddy fields remain

a serious obstacle to movement because some vehicles are unable to negotiate the dikes surrounding the fields.

e. Avenues of Approach. In most wooded areas, individual trees large enough to stop a tank are seldom so close together that they cannot be bypassed. Closely-spaced trees usually are of relatively small diameters and can be pushed over by a tank. The smaller trees and undergrowth, however, may be so dense that when they are pushed over the resulting mass of pileup vegetation will stop the tank. In most cases, wooded areas slow down the movement of tanks, and a guide may be required to lead each vehicle. Cutover portions of wooded areas usually contain stumps hidden in tall grass or weeds that are serious obstacles to armor. Trees that can stop a wheeled vehicle usually are too closely spaced to be bypassed. The pileup effect from pushing over vegetation is greater for wheeled vehicles than for tanks. Trailed loads are difficult to tow through wooded areas. Woods slow down the movement of dismounted troops. Some types of vegetation, such as mangroves or dense jungle, are frequently impenetrable until routes are cleared.

*f. Construction.*The usefulness of trees for timber is determined by their height and diameter, and by the nature of the wood as hard, soft, or fibrous. Deciduous trees generally are hardwoods. Needleleaf trees are softwoods that usually are easily worked, although some species are fibrous and difficult to saw. When a forest area must be cleared of trees prior to a construction project, a study of the ground will indicate the density and depth of the root systems. Where a forest is closely underlain by hardpan or rock, tree roots branch and remain near the surface, making them easy to uproot. In soil that is firm, with deep underlying rock, trees tend to form large taproots extending to a considerable depth, making them difficult to remove. Trees in inundated, marshy, and muskeg areas have thick widespreading and shallow root systems near the surface of the ground. In northern regions where permafrost occurs, its effect on the root systems of trees is similar to that of hardpan or rock. Where the permafrost is near the surface, the roots branch and lie close to the surface. Deeper taproots are developed where the permafrost is far below the surface.

91. Information Requirements—Vegetation

As far as practicable, information about the vegetation in an area is presented in the form of a map overlay that clearly indicates and identifies the major vegetation types by the use of color and symbols. The accompanying text briefly summarizes the additional information of military significance that cannot be shown adequately on the map. Pertinent information may include the following:

a. Forests.

(1) Name or other identification.

(2) Plant associations.

(3) Principal species (names, proportion in percent, density or average spacing, height range).

(4) Undergrowth species.

(5) Canopy: structure (continuous, open, broken) and seasonality (color, defoliation).

(6) Duff (partly decayed vegetable matter on the forest floor): abundance and nature of fallen trees, logs, and so on.

(7) Exploitation practices (normal cutting, overcutting, undercutting).

(8) Operational aspects (suitability for cover, concealment, blowdown susceptibility, camouflage, and fuel).

(9) Principal tree species.

(*a*) Name (English and botanical).

(*b*) Height (average).

(*c*) Growth form (triangular, linear, and ovate).

(*d*) Diameter (average).

(*e*) Leaves (broadleaf or needleleaf).

(*f*) Period of defoliation.

(*g*) Roots (structure, size, toughness).

(*h*) Suitability for construction.

(*i*) Special features (toxicity, thorniness, edibility).

(*j*) Indicator significance relation to

regional and local climates, kind and state of ground, and ground water, salinity, permafrost, depth and duration of snow cover, human activity).

b. Shrubs.

(1) Location and areal extent.

(2) Name or other identification.

(3) Principal species (names, proportion in percent, density or average spacing, height range).

(4) Foliage—density and seasonality (color, defoliation).

(5) Operational aspects (susceptibility to mass conflagration).

(6) Principal shrub species (for each). (Same information as for tree species.)

c. Grasses.

(1) Location and area extent.

(2) Identification.

(3) Principal species (names, proportion in percent, density, height range).

(4) Seasonality (dates of growth, color).

(5) Operational aspects (susceptibility to mass conflagration).

(6) Principal species (for each).

(*a*) Name (English and botanical).

(*b*) Date of maturity, height.

(*c*) Life span.

(*d*) Growth habit (sod or bunch).

(*e*) Suitability as forage.

(*f*) Special factors (toxicity, irritancy).

(*g*) Indicator significance.

d. Cultivated Crops (general).

(1) Location and areal extent.

(2) Name or other identification.

(3) Principal crops (names, proportion in percent, density or spacing height range; if applicable, months planted, cultivated, and harvested; crop rotation practices).

(4) Canopy, foliage, or stand (as applicable: structure, color, defoliation, density, rates of growth).

(5) Types of farming (irrigated, dry, and so on).

(6) Special factors associated with crops (irrigation ditches, flooding, terraces, hedgerows, dikes, and stone or other types of fences).

(7) Operational aspects (susceptibility to mass conflagration).

(8) Principal crops.

(*a*) Tree and shrub crops (same information as for tree species; in addition, months that the crops are harvested).

(*b*) Grass and grain crops (same information as for tree species; in addition, months of planting and harvesting).

CHAPTER 6

MANMADE TERRAIN FEATURES

Section I. SIGNIFICANCE

92. Definition

Manmade features include all the changes in the natural environment made by man in the course of living on the earth and using its resources. Major manmade features are cities, defensive works, transportation and communication facilities, and similar features that have significant effects upon the military operations. Others are such features as cemeteries, hedgerows, and buildings, which affect only local operations.

93. Military Aspects

In preparing terrain studies, manmade features must be evaluated to determine their effect upon the military aspects of proposed operations. Recommendations may be made to destroy certain features or to retain them for future use after the operation has been completed. Usually each major manmade feature is the subject of a detailed study by military intelligence personnel.

Section II. LINES OF COMMUNICATION

94. Importance

The lines of communication of an area consist of all the roads, railways, and waterways over which troops or supplies can be moved. The importance of particular features will depend upon the unit and the type of operations. The ability of an army to carry out its mission depends greatly upon its lines of communication. One of the primary considerations in planning large-scale operations is the extent and general nature of the transportation network. Planners must consider the advantages and disadvantages of the entire pattern of transportation facilities. An area with a dense transportation network, for example, is favorable for major offensives. One that is criss-crossed with canals and railroads, but possesses few roads, will limit the use of wheeled vehicles and the maneuver of armor and motorized infantry. Railroads extending along the axis of advance will assume greater importance than those perpendicular to the axis, and the direction of major highways and waterways assumes equal significance.

95. Roads and Routes

a. Description. The term roads includes all types of roads and tracks, but pack trails and foot paths are not included. Bridges, ferries, snowsheds, and similar structures and facilities that provide continuity of movement and protection for the way are also considered as integral parts of the road system. An adequate road system is a fundamental requirement in the conduct of any major military operation. Terrain studies must provide information about the roads which exist in the area under consideration and should indicate any major repair or rehabilitation required on existing roads, or where now roads will be needed to support a proposed operation. Roads in the combat zone usually need meet only minimum standards, but those in rear areas, especially in the vicinity of water terminals, airfields, supply installations, and those used as MSR's must be well-surfaced and capable of carrying heavy vehicle traffic without excessive maintenance. Operations on a wide front and the employment of nuclear weapons will require

a large number of secondary roads in both forward and rear areas. The information presented in a terrain study should indicate the minimum maintenance and construction requirements that may be anticipated during a planned operation. Continual maintenance of road net is essential. In addition to the severe punishment given to roads by large volumes of heavy traffic, important bridges, intersections, and narrow defiles are primary targets for enemy bombardment. The maintenance of unnecessary roads must be avoided, and the construction of new roads held to a minimum.

b. Route Types. Routes usually are classified as follows:

(1) *All-weather route (Type X).* Any route which with reasonable maintenance is passable throughout the year to a volume of traffic never appreciably less than its maximum capacity. The roads which make up this type of route have a waterproof surface, adequate drainage, and are only slightly affected by precipitation or temperature fluctuations. At no time is it closed to traffic by weather effects other than snow blockage. In this route class are roads paved with concrete, bituminous surfacing, brick, or paving stone.

(2) *All-weather route (Type Y) (Limited traffic due to weather).* Any route which with reasonable maintenance can be kept open in all weather, but sometimes only to traffic considerably less than maximum capacity. The roads which form this type of route do not usually have waterproof surfaces and are considerably affected by precipitation or temperature fluctuations. Traffic may be halted completely for short periods. Heavy use during adverse weather conditions may cause complete collapse of the surface. Crushed rock or waterbound macadam, gravel, stabilized soil, or sand-clay, are typical roads in this route class.

(3) *Fair-weather route (Type Z).* A route which quickly becomes impassable in adverse weather and cannot be kept open by maintenance short of major construction. This type of route is so seriously affected by weather that traffic may be brought to a halt for long periods. In this route class are roads of natural or stabilized soil, sand-clay, shell, cinders, laterite, and other lightly metalled or light aggregate surfaces.

c. Location and Use. Military routes are classified also as follows:

(1) *Axial route.* Axial route is part of military road net work, and it leads toward the front and is generally perpendicular thereto. When designated as the principal traffic artery of a division or higher unit, such a route is termed a main supply route (MSR). When designated the principal traffic artery of a brigade or battalion, such a road is termed a supply route (SR).

(2) *Lateral route.* A route which generally parallels the front and leads into and across axial routes.

(3) *Reserved route.* A controlled route allocated exclusively to a command or unit, or intended to meet a particular requirement.

(4) *Supervised route.* A route over which control is exercised by means of traffic control posts, traffic patrols, or both.

(5) *Dispatch route.* A route over which full control, both priority and regulation of traffic, is exercised.

d. Adverse Terrain. Swamps, bogs, and lowlands such as delta areas may create special problems of drainage and ditching, necessitate added support to the roadbed and require the construction of many bridges. Rugged topography may result in steep grades and sharp curves, tunneling, bridging, cuts, and sidehill locations in laying out new roads. Sidehill locations, in turn, may require retaining walls, cribbing, and snowsheds to give protection against earth, rock, or snow slides. In the desert, sand fences and special crews and equip-

ment to keep the roads clear of drifting sands may be required. Arctic terrain requires special techniques to build and maintain roads on permafrost and periodically frozen ground.

e. Weather and Climate. Sustained periods of freezing, heavy snowfalls, and similar extreme weather conditions may seriously affect the use, maintenance, and construction of roads. Protection must be provided against snow drifts, and provisions made to remove the snow and to repair damage due to frost heave and frost boils. Excessive rainfall may result in washouts and flooding in low areas and cause earth and rock slides in rugged terrain. Continuous wet weather may make unsurfaced roads impassable. In dry periods, dust control becomes an important factor on unsurfaced roads.

f. Design and Construction. Terrain studies should include an engineering evaluation of the structural soundness of all roads in an area under consideration. If the initial design did not provide for the increased loads and speeds that would accompany military use or if the road was improperly constructed originally, it may prove a serious obstacle to movement. Repairs and excessive maintenance may be required because of an unstable subgrade; inadequate drainage of the subgrade, surface, or slopes; sharp curves, and loose or unsealed wearing surfaces that result in saturated roadbeds.

g. Poor Maintenance. Poor maintenance of a road is shown by clogged culverts and ditches, potholed, bumpy, and rutted surfaces, soft and uneven shoulders, and badly worn and cracked pavements. Studies should indicate where these conditions exist and the maintenance that would be required to bring the roads up to minimum military standards.

h. Trafficability. The various types of soils affect trafficability differently. For example sandstone affords excellent trafficability when it is dry but is reduced to good trafficability when wet; trafficability on a clay surface is rated as fair when dry and impassable when wet.

96. Information Requirements — Roads

a. Information about roads is recorded on map overlays that show the alinement of the significant roads, with the location of associated bridges, tunnels, ferries, fords, and critical points such as rockslide areas. Ordinarily the local system of route numbers is used, but if no system exists that is satisfactory for terrain intelligence purposes, an arbitrary system is used to identify the main and secondary roads.

b. Information about individual roads usually includes the following:

(1) Name and route number.

(2) Terminal points; intermediate localities on the road; distances between major points.

(3) Terrain (elevations, irregularities, slopes, drainage, soils).

(4) Length and width.

(5) General condition (necessary repairs and improvements, with nature and location).

(6) Surface material (by sections, if there are changes in type of surface along the route).

(7) Ratings of alinement, drainage, foundation, and surface.

(8) Roadbed (width of traveled way; type and width of shoulders).

(9) Maximum grade.

(10) Sharpest curvature.

(11) Significant cuts and fills.

(12) Clearance (minimum vertical and horizontal clearances, with nature of restrictions).

(13) Bridges (load capacity, general condition).

(14) Tunnels (length, widths, clearances, condition).

(15) Fords and ferries (type, general characteristics, condition).

(16) Critical points; location and characteristics of possible bypass routes or detours around bottlenecks.

(17) Location and characteristics of routes that provide maximum protection from ground or air attacks.

(18) Snow (critical areas, snow fencing, snow removal equipment).

97. Bridges

a. Importance. Road and railway bridges are vulnerable points on a line of communication. Timely preservation, destruction, or repair of a bridge may be the key to an effective defense or to successful penetration of an enemy area. A bridge seized intact has great value in offensive operations, since even a small bridge facilitates the movement of combat troops across a river or stream. Information about bridge types and their classification is contained in **TM 5–312** and **FM 5–36.**

b. Sites. Because of the time and labor involved, new bridges are erected only when an existing bridge, ford, or detour cannot be used. Terrain suitable for a bridge site should meet the following requirements:

(1) Satisfactory river conditions, with no fast currents or great depths.

(2) Site readily accessible from the road it serves.

(3) Firm, well-drained approaches, preferably above flood level.

(4) For floating bridges, a riverbed free from snags, rocks, and shoals to a minimum depth of three feet and firm enough to hold anchors and to support trestles. Banks should be from two to six feet above water level to minimize excessive abutment preparation.

(5) Firm, stable banks of suitable height. Large differences in bank height require excessive grading. Low banks may be subject to a rising river level that will flood the bridge site.

(6) Adequate, well-drained working areas close to the site including a bivouac for the working party, space for construction materials, and turnarounds and parking places for vehicles and heavy mobile equipment.

(7) Areas close to the site, near or alongside the approach roads, where vehicles can park off the road and under cover while awaiting their turn to cross.

98. Information Requirements — Bridges

a. Detailed information about bridges cannot be obtained from topographic maps, but indications on air photographs usually will permit an approximate determination of the width, clearance, and height above water of a bridge. Details such as the condition, capacity, and structure of a bridge should be obtained by engineer reconnaissance. Reconnaissance procedures are described in **TM 5–312** and **FM 5–36.** Basic information requirements for a bridge should include a summary of its structural characteristics, its critical dimensions (length, usable width, overhead clearance), an estimate of capacity, and general condition.

b. Detailed information includes the following:

(1) Type, number of lanes and width of each, number of spans and length of each length of panels, arrangement of spans.

(2) Height above riverbed, overhead clearance for vehicles, class.

(3) Stream data: width, depth, velocity of current, direction of flow, type of bottom, estimated bearing capacity of bottom, height, slope, and nature of banks.

(4) Description, dimensions, and condition of access roads and approaches.

(5) Type, dimension, and condition of abutments, stringers, flooring, girders, and other structural elements.

(6) If damaged or wrecked—

(*a*) Structural details of bridge in its original form.

(*b*) Nature and extent of damage; position of debris; details regarding any salvageable materials.

(*c*) What loads, if any, can still cross the bridge.

(*d*) If not suitable for use, information about alternate sites.

99. Railways

a. Property. The term railway includes all

fixed property belonging to a line, such as land, permanent way, bridges, tunnels, and other structures. Railways assume increased military importance in areas where the soils are generally untrafficable, roads are poor, and rail transportation facilities are extensive. Frequently, railways can be used as substitute roads for vehicles. Most railway bridges will carry tanks without reinforcement. The basic elements of a railroad include motive power, rolling stock; trackage; yards, terminals, regulating stations, and railheads; transshipment points; water and fuel stations; maintenance and repair facilities; and signal communication facilities.

b. Yard. A yard is an area containing a system of interconnected tracks and is used for making up trains, storing cars, and general maintenance activities.

c. Railhead. A railhead is the point at which supplies destined for a particular unit, installation, or area are transferred from rail to another type of transportation, usually trucks.

d. Regulation. A regulating station is an installation on a military railway line at which the movement of supplies and personnel is controlled. Its facilities include a yard, open and covered storage, and usually, temporary housing and messing facilities for transient personnel.

e. Construction. The development and extent of a railway system largely reflect the topography of the region that it traverses. In desert regions, for example, a single railroad may extend in a straight line across vast barren wastes. In hill regions and mountain areas, the railways run through valleys, with short lines leading off into other terrain. On plains, railways will have few curves but may be subject to the effects of poor drainage conditions. Generally, railways tend to follow rivers because of the more uniform grades, the availability of straight routes, and the concentration of resources, industries, and population centers along the waterway. The terrain characteristics of an area can be determined to a considerable degree by a study of the railway routes, since the rail lines almost invariably follow the topography that offers the fewest obstacles.

f. Military Use. Railways are desirable for extended military operations. Their capabilities are of primary concern and are the subject of continuing studies by personnel at the highest levels. Detailed intelligence about the railways in an area of operations is produced by specialists of transportation and engineer units. Railways are highly vulnerable to enemy attack, particularly to sabotage and guerrilla operations. Keeping a railroad line in operation requires trained security forces and extensive protective measures.

100. Evaluation of Railways

In evaluating a railway for terrain intelligence purposes, consideration should be given to the effects of adverse terrain, weather and climate, and the overall design and construction of the system. The following factors should be considered:

a. Adverse Terrain. Railways passing over swamps, bogs, and delta terrain may encounter special problems of drainage, ditching, and roadbed maintenance. In mountainous areas, steep grades, sharp curves, and tunnels are common. Because of sidehill locations and deep cuts, there should be protection against earth, rock, and snow slides. In desert, drifting sand is a problem and provisions should be made to remove it.

b. Adverse Weather and Climate. Severe winter conditions seriously retard operation and maintenance of railways, requiring protection against drifting snow, provisions for snow removal, and repairs because of damage caused by frost heave. Excessive rainfall may result in washouts and flooding in low areas and cause earth and rock slides in rugged terrain.

c. Design. A railway may prove inadequate because the initial design did not provide for the increased loads and speeds or heavier volume of traffic needed. As a result, a railway might require either considerable reconstruction and repair or extensive maintenance. Among the more common defects are an unstable subgrade, lack of adequate drainage, light rail, poor ballast, and untreated ties. Improper maintenance is evidenced by such con-

ditions as an uneven roadbed, improperly tamped ties, loose fastenings, badly worn rail, or uncleared drains.

101. Information Requirements — Railways

Railway information should be recorded on a map or overlay that shows the true alinement of all rail lines; their trackage, gage, and status; and the location of selected bridges, tunnels, and ferries. A convenient system of line numbers is used based on a standard reference or arbitrarily selected. Fundamental information about railways should include the following:

a. Total mileage.

b. Terminals and details of main lines.

c. Mileage by gage and locations of changes.

d. Number of tracks.

e. Maximum grade and minimum radius of curvature.

f. Location and length of passing tracks.

g. Type and weight of rail.

h. Permissible loads; capacity of bridges.

i. Yards and terminals (location, type, capacity).

j. Details of servicing facilities and other installations.

k. Operating factors (cars per train; speed; number of daily trains each way).

l. Bridges and tunnels (bridge data to include length, number of tracks, spans by type and length, height of structure; tunnel data to include length, number of tracks, and lining).

m. Rail ferries (location, type, capacity).

n. Electrification (location, type).

o. Transshipment points.

p. Individual rail line details—

(1) Name.

(2) Terminals, intermediate stations, length of each stretch.

(3) Obstructions (demolitions, washouts, blocked tunnels).

(4) Gage.

(5) Number of tracks.

(6) Weight of rails.

(7) Maximum grade and minimum radius of curvature with location of each.

(8) Ties, ballast.

(9) Sidings and passing tracks (location, lengths, switches).

(10) Tunnels (locations, clearances).

(11) Overhead structures and vertical clearances.

(12) Drainage facilities, including culverts.

(13) Bridge data.

(14) Operating and servicing facilities (location, availability of fuel and water and ice; signal, traffic control, and dispatching facilities).

(15) Availability of trained and dependable personnel.

(16) Transshipment points.

q. Equipment.

(1) Present condition, and interchangeability with equipment of other countries.

(2) Motive power (type, size, weight, tractive effort, wheel arrangement, type and height of couplings).

(3) Rolling stock (type, number, car dimensions, capacity, weight).

(4) Rail cars self-propelled and trailer-type, total by type, size, capacity.

(5) Work cranes (total by type, size, capacity).

(6) Snow plows (total by type, size).

(7) Armored equipment (total by type, size).

(8) Repair shops (location, types of equipment repaired, capacity by type, number of personnel employed).

102. Inland Waterways

a. Definition. The term inland waterway is

applied to those rivers, canals, lakes, and inland seas of a country which are used as avenues of transport. It includes all the fixed structures which affect the movement of vessels carrying passengers or freight. Types of inland waterways include inland lakes and land-locked seas, rivers, and ship and barge canals, and the intracoastal waterways, usually running parallel to the coastline of a land mass and sheltered enough to permit the navigation of small vessels.

b. Classification. Inland waterways can be classified according to their depths as follows:

(1) *Very shallow.* Depths less than 1.4 meters (4½ feet).

(2) *Medium.* Depths between 1.4 and 2 meters (4½ and 6½ feet).

(3) *Deep.* Depths greater than 2 meters (6½ feet).

c. Advantages. Inland waterways provide an economical form of transportation for bulk supplies, freeing faster modes for shipments of a higher priority. Frequently, large or very heavy items that cannot be handled by truck and rail can be shipped by waterway. One of the major uses of waterways in an active theater is the transportation of supplies for the rehabilitation of the economy in liberated areas, thus reducing the demands upon military transportation facilities.

d. Limitations. Unless icebreaking operations can be conducted, traffic is halted completely during a freezing period. The thaw following a freezeup may cause floods, and periods of drought may result in insufficient water for the movement of vessels. The locks, bridges, cuts, dams, and other facilities are vulnerable to enemy action. Retreating enemy troops usually drop rail or road bridges into the waterway; damage locks and levees; obstruct channels with ships and barges; drain canals; and destroy, dismantle, or move essential equipment. Waterway transport is slow. It is also inflexible, since new waterways cannot be constructed during military operations. The depths of rivers and streams used as waterways fluctuate with maximum and minimum rainfall. Streams with fairly direct courses commonly are interrupted by falls and rapids. Streams of low and uniform gradients usually meander. Their channels shift constantly, depositing sandbars, which are a menace to navigation.

103. Information Requirements — Waterways

Inland waterway information should be recorded on a map or overlay that shows the true alinement of the navigable waterways, the location of all locks, dams, aqueduct bridges, tunnels, and major landing facilities, and the location of specific structures which limit the vertical and horizontal clearances on each navigable reach. The local names are used to identify waterways and structures whenever feasible. Detailed information requirements should include the following:

a. Developed Waterways.

(1) Geographical location (name, origin, terminus, length).

(2) Restricting widths and depths of channel.

(3) Frequency, duration, and effects of seasonal changes (floods, low water, droughts, excessive currents, normal freezeup and opening dates).

(4) Location, description, and restrictive effects of structures (locks, safety gates, dams, bridges, ferry crossings, aqueducts, tunnels, cable crossings).

(5) Speed and fluctuation of current.

(6) Name and location of waterway ports, including length of alongside wharfage and depths, and data on mechanical handling, storage, clearance and ship repair facilities.

(7) Maintenance requirements.

(8) Craft (number, type, cargo capacities).

(9) Communication facilities.

(10) Availability of labor force.

b. Navigable Rivers. In addition to the items listed in *a* above, the following additional information may be required:

(1) Physical characteristics of the river

(bottom, banks, feedwater streams, and important tributaries).

(2) Navigational hazards, such as falls, rapids, and sandbars.

(3) Navigational aids, location, and type (buoys, lights, range markers, radar, foghorns).

(4) Changes in channel.

(5) Dredging requirements.

Section III. PETROLEUM AND NATURAL GAS

104. Location

a. Source. Oil is found only in the stratified sedimentary rocks and sands of ancient sedimentary basin areas. Because of geologic upheavals in past ages, today's oilfields may be found along the foot of mountain chains or in lowland or offshore areas. Petroleum, gas, and water are commonly found together.

b. Gas. Natural gas is found alone, as well as with petroleum. Gas from oil wells is commonly entrained with natural gasoline and is known as wet gas. When economically feasible, wet gas is piped to an absorption plant, where the gasoline is extracted. Gas from gas wells ordinarily is relatively free of natural gasoline and is known as dry gas. If sufficiently free of other unwanted gases and impurities, dry gas may be fed directly into pipelines for distribution.

105. Installations

a. Derricks are commonly the most distinguishing features of an oil or gas field. A derrick is required to position and handle the long sections of drill pipe and other equipment used in the well when drilling for oil. Depending on the type, the cost of moving or future needs, a derrick may or may not be left in place indefinitely following the completion of the well. Where a continuing need exists, the drilling derricks may be replaced with smaller derricks or gin poles. A producing oil well is characterized by a pump or by a "Christmas tree," so called because of its tree-like appearance. A pump is used where the subterranean gas pressure is too low to force oil to the surface. A Christmas tree is used where the underground gas pressure is sufficient to force oil to the surface. It consists of a system of pipes, valves, and gages capping a well for controlling the flow of crude oil and gas.

b. Refineries are located near either producing oil fields or distribution centers in major consuming areas. Adequate all-weather transportation and an abundance of cooling water are essential. Tall, cylindrical distillation or "cracking" towers are the most prominent features at refineries. Other equipment includes large furnaces, cooling towers, electric power plants or substations, and intricate piping systems. Tankage for storing crude oil charge stocks and semirefined and refined products is also required. Refinery capacities are usually rated in barrels per day (42 U.S. gallons per barrel) or metric tons per year of crude oil run to stills (crude oil started through the refining processes). A reliable rule of thumb for converting barrels per day to metric tons per year is to multiply the number of barrels per day by 50. Metric tons per year are divided by 50 to yield barrel-per-day figures. Crude oil for refinery fuel or lost otherwise amounts to about 7 to 10 percent of refinery capacity.

106. Distribution

a. Systems. A bulk distribution system for petroleum products may include ship-to-shore and dockside loading and unloading facilities, bulk storage tank farms, pipelines, pumping stations, bulk delivery points or pipeheads, warehouses, open storage areas, canning and drumming facilities and testing laboratories. Ocean-going tankers, tank barges, railroad tank cars, and tank trucks are also included in integrated distribution systems. For terrain intelligence purposes, pipelines and storage facilities are the most significant features of a distribution system.

b. Pipelines. Pipelines commonly consist of piping, pumping equipment, and regulating tankage. Other supporting equipment may include tele-communications facilities, cleaning

devices and trays for removal of unwanted condensates or contaminants, control and heating devices. The capacity of a pipeline is expressed as a quantity of liquid capable of being transported per unit of time, ordinarily in the number of barrels, metric tons, or cubic meters per day. The quantity of fuel actually transported, usually will not exceed about 85 percent of the pipeline capacity.

c. Military Pipelines. Military pipelines are used chiefly to transport jet fuel and gasoline. Occasionally they are used also to transport diesel fuel and kerosene. Commonly, 15-cm (6-inch) pipe is used; 20-cm (8-inch) pipe is employed for ship unloading or trunk lines. The pipeline follows the most direct level route, within six to nine meters (20–30 feet) of all-weather roads, so as to facilitate construction, partrol, repair, and security of the line. Cross-country cutoffs are used where roads wind excessively. A military pipeline is diverted around difficult terrain, such as marshes, swamps, or land that is subject to periodic flooding. It also avoids populated areas and military installations that have a high element of hazard, such as ammunition dumps. Base terminals are located in rear areas, at or near theater ports of embarkation or other tanker unloading points, but pipehead terminals are located at the forward end of a military pipeline, moving forward with the army supply point to support the advancing forces.

d. Civilian Pipelines. Civilian pipelines are important for potential military support. They are generally permanently installed cross-country along the most economical route. These pipelines may range from about 10 cm (4 inches) to more than 100 cm (40 inches) in diameter. Pipe of extremely large diameter is ordinarily used only for natural gas or crude oil. Pipelines for crude oil are much more common than those for refined products, although use of the latter is rapidly growing. Crude oil pipelines can be converted for handling refined products. This is a costly and time-consuming undertaking, particularly if aviation-grade fuels are to be transported.

e. Tanks. Bulk petroleum and refined products are stored in tanks which differ greatly in size, shape, and construction, according to the function of the tanks and the nature of the product stored. The tanks may be completely above ground, partly or entirely buried. Tanks above ground are surrounded by dikes or low walls to form catch basins and to prevent the occurrence or spread of fires if the tanks are ruptured or overflow. Tanks are buried or partly buried for reason of safety, to reduce evaporation losses, for concealment, or to reduce their vulnerability to military attack. A group of storage tanks is called a tank farm. Tank farms vary greatly in size; some comprise major storage complexes, with storage capacities of millions of barrels. Ordinarily, the tanks are interconnected by an assembly of pipes and valves called a manifold, which permits the movement of products. Because of their vulnerability to air attack, and to nuclear attack, military tanks farms are limited to a total capacity of no more than 250,000 barrels. Military storage tanks are made of steel or aluminum and have capacities up to 10,000 barrels. Portable fabric tanks also are used in military operations at forward supply points and at beachheads.

107. Military Importance

a. Targets. The petroleum and natural gas resources of a country or region are valuable assets to its economy, and the degree of self-sufficiency in military fuels is fundamental to its conventional military capabilities. Accordingly, refineries, terminal facilities, distribution systems, and storage installations are primary targets for air attack and are major objectives. Major oil producing areas and refineries, key pipelines, storage facilities, and marine terminals may be the principal objectives of a campaign to seize them for our use or deny them to the enemy. The most militarily significant natural gas facilities are pipelines, which could be readily converted for handling petroleum products for military support.

b. Planning. Because military planners are interested in the availability of fuel for military use, avoiding possible disturbance to local economics, the typical normal operating conditions with respect to petroleum facilities are important. Included are seasonal variations in the supply and demand for petroleum products, and the principal consumers and their needs. Manufacturing and civil transport

fuel requirements, as well as agricultural consumption by tractors and irrigating systems are militarily significant in modern planning.

108. Information Requirements — Petroleum and Natural Gas

The location and extent of petroleum and gas facilities should be recorded on a topographic map of suitable scale. A numbering system is established to identify the petroleum and the gas pipelines, producing fields, plants, and storage facilities. A separate series of numbers is used for each pipeline. Such pipeline facilities as pumping stations and tank farms are numbered serially, beginning from a designated initial point on the line. Local names may be used for individual installations. Basic information should include the following:

a. General.

(1) Location and type of raw material (oil, oil shale, natural gas); character of crude oil; well logs; and a geologic column which designates the producing formations and the depth to producing horizons.

(2) Reserves of raw material in million barrels, metric tons, or million cubic feet (cubic meters).

(3) Administrative, maintenance, and repair facilities.

(4) Security and safety provisions.

(5) Physical condition of installations and equipment; required major repairs or improvements.

(6) Availability of trained and reliable personnel.

(7) Principal consumers.

b. Refineries.

(1) Location and owner/operator.

(2) Capacity.

(3) Details of construction; type of equipment.

(4) Nature and quality of products produced.

c. Pipelines.

(1) Name, if any; location of lines; material transported.

(2) Terminals.

(3) Number and diameter of pipes; delivery capacity of system at present and under normal conditions; content of pipeline when full.

(4) Facilities at base terminal (if a water terminal, method of loading from tankers).

(5) Storage facilities at terminals and along pipelines; capacity of each installation.

(6) Pumping stations (location, capacity, equipment).

d. Storage.

(1) Location: geographic coordinates; topography; adjacent landmarks.

(2) Surface tanks: types and number; dimensions; protection (revetments, blast walls).

(3) Buried tanks; number; dimensions.

(4) Pump houses: location; number; dimensions; capacity.

(5) Connecting pipelines and distributing systems.

(6) Stocks (location and type).

Section IV. MINES, QUARRIES, AND PITS

109. Mines

a. Mineral Resources. The important mineral resources of a country include metallic ores such as iron, copper, zinc, lead, tin, silver, gold, and uranium; mineral deposits, principally sulfur, phosphate rock, gypsum, graphite, asbestos, and bauxite; and solid fuels, chiefly coal, lignite, and peat. Terrain studies list each significant mineral, covering in detail the estimated quantities available and the methods and facilities employed to mine, process, and distribute each type of mineral. Mineral deposits are exploited either from the surface of the ground or from underground shafts and tunnels, the method depending upon the depth

of the deposit below the surface. A typical underground mine consists of a vertical shaft, horizontal passages opening out of the shaft, and passages driven from above (winzes) connecting the levels. Openings branching off from the levels, where the ore is actually extracted, are called stopes. Supports in mine working usually are made of timber treated with preservatives or of reinforced concrete, steel, brick, or stone. Pillars of ore may be left as supports, finally being mined when the workings are vacated. Where ore beds lie close to the surface, the mineral may be removed from open pits after stripping off the overlying earth and rock. This is strip mining, the coal or other mineral being removed by power shovels.

b. Placer. Placer mining involves the removal of the unconsolidated rock material that lies above bedrock by hand, hydraulic nozzles or dredges, and subsequent separation of the ore from waste by panning and sluicing. It is widely employed to mine gold.

c. Open-pit. In open-pit mining, an excavation is made. In the case of deep pits, the sides usually are cut into steps or benches. Access to the below-ground-level site may be obtained by arranging these benches in spiral form, by cutting inclined approaches, or by sinking a shaft connected to the mine by an adit or tunnel (fig. 48).

Figure 48. Open-pit copper mine.

d. Glory-Hole. In glory-hole mining, the excavation is funnel-shaped, and a vertical passage (raise) driven from below connects with an underground haulage level. The ore slides down this passage into the haulage level for removal.

e. Military Considerations. The ability of any nation to support a war depends upon its mineral resources and enemy mines are accordingly a major objective for air attack. The seizure or defense of important mines may also be the mission of troop units of any size. Mines provide concealment and cover, but their use as shelter for troops may be hazardous and is seldom practicable. Most mines will not withstand the effects of heavy surface bombardment. Coal mines are especially unsuitable for troops or storage. Coal is structurally unstable

and requires extensive supports even in ordinary mining operations. Many varieties of coal give off a gas known as fire damp or marsh gas. This is highly flammable and highly explosive when mixed with air. Coal dust and air also form an explosive mixture. Some mines, particularly salt mines, may be utilized for the storage of supplies and equipment. Adit mines, with their horizontal or slightly inclined entries, are more suitable than vertical-shaft mines for underground storage. The latter type may present drainage problems and offers more difficulties in transporting loads into and out of the mine. To prevent their use by the enemy, mines can be flooded or destroyed with explosives. The possibility of mines being used as headquarters for guerrillas must be considered, and inactive mines in a tactical area should be blocked, destroyed, or otherwise secured against occupancy.

110. Information Requirements — Mines

The information about a mine required for a terrain study will depend upon the purpose. Such information as the following usually is required:

a. Location and name of mine.

b. Product (Mineral extracted, quality, quantity, underground and in reserves).

c. Extraction methods (deep, placer, strip, special methods).

d. Details of layout and operation.

(1) Pits, shafts, galleries, wells.

(2) Hand and mechanical labor involved.

(3) Above ground structures, plant, and equipment.

(4) Refining processes.

(5) Storage facilities.

(6) Transportation facilities.

(7) Utilities (ventilation, electric power, lighting, water, firefighting).

e. Physical condition of installations and equipment.

f. Safety and security features.

g. Availability of labor.

h. Any major repairs needed for operation.

i. Access road and turn around availability.

111. Quarries and Pits

a. Quarries. A quarry is a site providing rock that is suitable in quality, quantity, and size for construction purposes. A hardrock quarry furnishes rock such as granite, limestone, or sandstone, which must be drilled and blasted in quarrying and which must be crushed for some uses. Igneous and metamorphic rocks are generally considered hard rocks. A soft-rock quarry furnishes material that can be removed readily by earthmoving equipment. Soft coral, caliche, shale, chalk, and tuff are materials of this type. Sedimentary rocks are generally considered soft. Quarries are generally the open-faced type, with the vertical surface of the rock exposed. Depending upon local conditions, they may be developed by the single or multiple bench method. A single-bench quarry has the entire floor on one level, the height of the bench worked in one operation varying from 2 to 30 meters (8 to 100 feet). A multiple-bench quarry is one having a series of ledges or terraces resembling steps.

b. Pits. A pit is a site where earth or rock particles suitable for engineer construction may be obtained in quantity. A borrow pit is a site providing soil suitable for fills, surfacing, or blending that can be removed with earthmoving equipment. A gravel pit consists predominantly of particles of gravel size. Unsorted gravel from pits is used extensively for surfacing secondary roads, in base courses for pavements for roads, taxiways, and runways, and as aggregate in concrete and bituminous operations. An alluvial gravel pit derives its name from the origin of the deposit, since the material is stream-deposited. The gravel obtained from these pits usually is very clean and free from clay and humus. It is therefore particularly desirable for concrete and bituminous work. A bank or hill gravel pit produces a clayey gravel or clayey sandy gravel. These materials are very desirable for surfacing work because of their binding qualities.

c. Military Considerations. Pits and quarries are important chiefly as sources of materials for engineering construction. They may be local objectives in tactical operations, if plans require extensive engineering development of

the area. Individual pits and quarries usually can be bypassed by advancing forces, but an area containing a number of them may present difficulties to the movement of larger units and will tend to analyze movements. Flooded quarries are a particularly hazardous obstacle. Pits and quarries provide a varying degree of cover for troops. They may also furnish defiladed locations for artillery and missile positions.

112. Information Requirements — Quarries and Pits

a. Quarries.

(1) Location.

(2) Nature of stone.

(3) Actual and potential capacity in uncrushed stone.

(4) Capacity of crushing machinery in stone of various sizes.

(5) Details of machinery.

(6) Loading facilities

(7) Amount of crushed stone that can be hauled away in a day, considering the manner of loading, number of trucks that can be loaded at one time, access road, and turnarounds.

b. Pits.

(1) Location.

(2) Nature of source.

(3) Nature of raw materials; quality, quantity.

(4) Amount, depth, and type of overburden.

(5) Drainage; ground-water level; standing water.

(6) Utilities available (electricity, water).

(7) Equipment available.

(8) Method of extraction (hand labor, machinery, dredging).

(9) Method of cleaning and sorting.

(10) Daily production capacity.

(11) Transportation routes; access roads; surfaces of roads.

Section V. AIRFIELDS

113. Size, Form, and Components

a. Description. Airfields range in size and function from short landing strips consisting of little more than a cleared area suitable for light liaison planes or helicopters to large permanent air bases with many complex supporting installations. The simplest form of operational airfield consists essentially of a runway, usually oriented in the direction of prevailing winds; one or more perimeter taxiways, with warmup aprons located where they join the ends of the runway; and hardstands to accommodate one or more groups of aircraft. The runway may or may not be surfaced. In addition, there will be a minimum of other facilities, such as access and service roads, fuel storage, ordnance storage, and a control tower. The particular characteristics will depend upon the type of aircraft that will use the field.

b. Tactical Airfield. A tactical airfield in a theater of operations includes the following major elements:

(1) Landing strips.

(2) A system of hardstands and runways.

(3) Warmup aprons close to one or both ends of the runway.

(4) Operation facilities, including control tower and operations and briefing rooms.

(5) Fuel storage and dispensing facilities.

(6) Ammunition storage facilities.

(7) General supply storage facilities.

(8) Repair and maintenance facilities for aircraft, accessories, and automotive vehicles.

(9) Roads, walkways, communications, firefighting unit, and other service facilities.

(10) Security and safety installations.

114. Terrain

a. Location. The general location of a pro-

posed airfield is indicated by the Air Force commander or the Army aviation officer, as appropriate, while the exact site is chosen in coordination with the engineer after a careful evaluation of the terrain.

b. Selection. In selecting a site, the following factors should be considered:

(1) Adequate dimensions to meet operational requirements, with room for future expansion.

(2) Accessibility to supply routes and communication facilities.

(3) Obstructions along flightways and approaches, including critical topographical features, such as high hills or mountains. High tension wires, roads, and railroads crossing the flight way near the runway are dangerous mental and physical hazards to pilots.

(4) Meteorological conditions (wind, rainfall, fog, snow, frost action).

(5) Drainage.

(6) Topography. A site with favorable topography is one located on high ground with sufficient slope for natural cross drainage as well as longitudinal drainage and a reasonably smooth surface requiring little earthmoving.

(7) Clearing, grubbing, and stripping required. A large open area surrounded by sufficient covered areas to conceal all activities is ideal. Ground cover in areas adjacent to the flight strip is especially desirable to provide natural concealment for parked aircraft, dumps, and bivouac and other installations.

(8) Soil characteristics. The type of soil determines the type of equipment required for construction, drainage, effects of adverse weather, and the subgrade bearing capacity that can be obtained.

(9) Availability of gravel, sand, coral, or other materials for excavation.

(10) Water supply. Large quantities of water are required in both the construction and operation of airfields.

(11) Camouflage requirements. A desirable site is one that avoids identifying landmarks and affords cover for installations and aircraft at dispersed locations.

115. Information Requirements — Airfields

Based on available reports and files, detailed studies of particular airfields in local areas will be prepared by intelligence personnel. Pertinent information to be included in a terrain study should include the following:

a. Location (map coordinates, elevation, distance and direction from nearest city or town, principal landmarks, name if any).

b. Category (emergency landing strip, refueling and rearming strip, fighter field, bomber field, heliport, and civilian secondary airport).

c. Characteristics of site (type of terrain, character of soils, special aspects of weather and terrain differing from country-wide or regional conditions).

d. Detailed layout (sketch) of runways, taxiways, parking and service areas.

e. Runways.

(1) Identification.

(2) Length of runway and overrun; extensibility.

(3) Width of runway, overrun, shoulders.

(4) Type and depth of surfacing and base.

(5) Type and adequacy of drainage (ditches, subsurface drains).

(6) Load capacity (in pounds, or kilograms or aircraft type).

(7) Gradient.

(8) Present condition.

f. Taxiways and parking (dimensions, type and depth of surface material and base, load capacity, condition).

g. Detailed description of operation area; improvements planned or under construction.

h. Facilities.

(1) Buildings (type, material, dimensions).
(2) Maintenance and repair (number and extent of buildings and numbers and types of equipment used for airfield maintenance.
(3) Fueling (number and capacity of tanks, above or below ground).
(4) Electricity supply.
(5) Water supply.

i. Related transportation (railroad, road, water; details about type, location, and capacities of transportation facilities available).

j. Airfield construction sites.
(1) Topography.
(2) Wind (direction, intensity of prevailing wind; local peculiarities).
(3) Rainfall (average by months; wet seasons; intensity, duration, and frequency of rainfall).
(4) Other aspects (temperature variations, storms, fog, and ground haze).
(5) Availability of local construction materials.
(6) Water supply.
(7) Clearing and grading required.
(8) Drainage conditions and required improvements.
(9) Soil classification.
(10) Flight obstructions.
(11) Frost heaving, permafrost, flooding, extremely strong winds bear directly on airfield site construction and maintenance.

Section VI. WATER TERMINALS

116. Ports

Water terminals (ports) may range in size from beaches suitable only for landing craft to giant complexes extending along many miles of coastline. They usually constitute key terrain features and primary objectives in military operations. FM 55–51 gives detailed information about the organization and operations of water terminals. Normally, major water terminals (fig. 49) are characterized by deep harbors protected from storms and free from ice in the winter months. The rail and road networks of the area usually extend from the terminals inland to developed portions of the country. Large terminals are often surrounded by commercial, industrial, and shipbuilding areas.

117. Military Significance

a. Vulnerability. Large water terminals are highly vulnerable to attack by nuclear weapons. When the enemy has a nuclear weapon capability, logistical support is provided through a number of dispersed small terminals, often little more than beaches developed to meet minimum requirements. Terrain studies should include an evaluation of all suitable locations for such terminals, indicating their physical characteristics, relative usefulness, and estimated capacities. A large-scale amphibious operation may include a number of separate secondary landings to secure beaches that are suitable for dispersed logistical terminals.

b. Evaluation. Information about established water terminals usually is contained in terrain studies prepared at the highest echelons, which form the basis for studies used in specific operations. The existing water terminals are evaluated as to their usefulness and their present physical condition. If an enemy-held terminal is to be used by friendly forces after its seizure, particular attention is given to the essential structures and facilities that should be spared from destruction, if practicable, during the preliminary bombardment and assault.

118. Information Requirements — Water Terminals

The information about a water terminal which is most essential in preparing a terrain study will depend upon the features that are of the greatest concern in a specific operation. Detailed information requirements for water terminals are contained in FM 55–8. Information required may include—

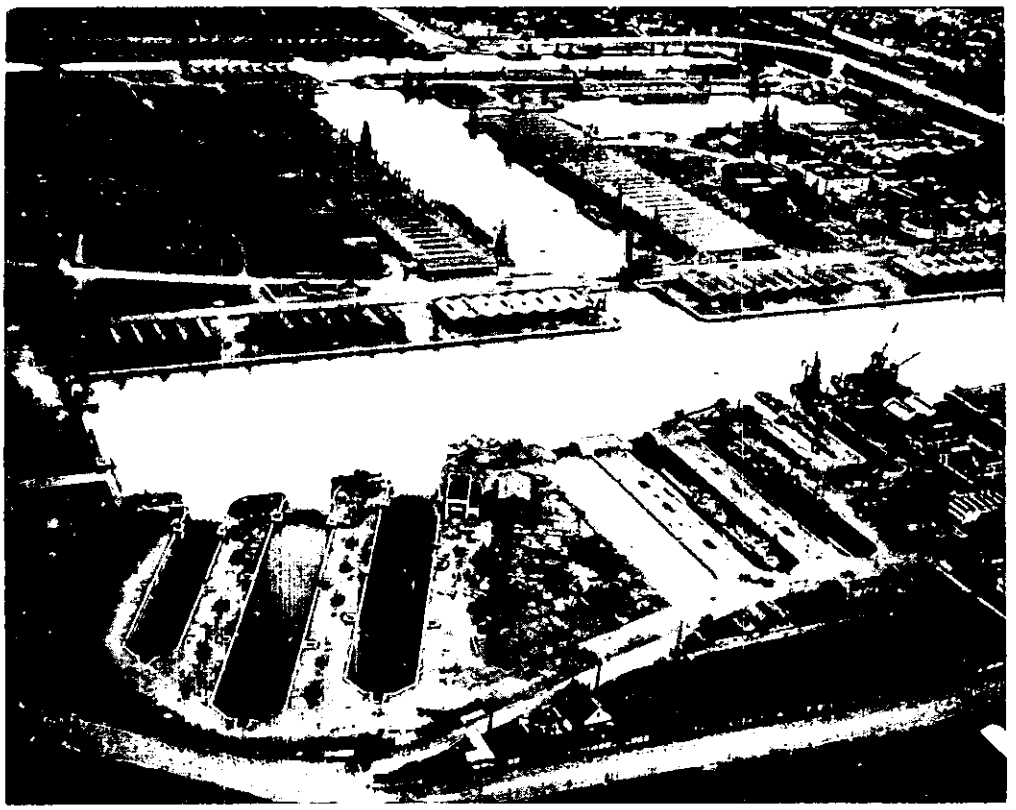


Figure 49. Typical large water terminal (port).

a. Name, location by map references and coordinates.

b. General characteristics (open roadstead, partly inclosed bay, landlocked harbor, sheltered area behind a barrier reef, and river).

c. Entrance and approach channels (controlling depth, length, width).

d. Breakwaters (position, length, construction).

e. Description of harbor.

(1) Type.

(2) Harbor and channel depths.

(3) Extent of silting.

(4) Nature and frequency of maintenance dredging.

(5) Location and nature of anchorages.

(6) Underwater obstructions.

(7) Pilotage information.

f. Bridges regarded as shipping obstructions (location, type, horizontal and vertical clearances at mean low water).

g. Hydrographic and weather conditions.

h. Adjacent beaches usable by landing craft (location, length, type, gradient, and accessibility).

i. Cargo-handling facilities.

(1) Wharves, piers, and quays (type, function, structural features, cargo-handling machinery, road and railroad connections, utilities, mooring facilities).

(2) Wet docks and semitidal basins.

(3) Mechanical handling facilities.

(4) Harbor-service craft (type, function, number).

j. Repair facilities.

(1) Repair yards.

(2) Graving docks.

(3) Floating docks.

(4) Marine railways.

k. Storage facilities.

(1) Location, type of commodities stored, type of constructions, capacity, transportation connections, fire protection, special handling equipment.

(2) Cold storage facilities (temperature, daily ice making capacity).

(3) Grain storage facilities.

(4) Bulk liquid storage (capacities in barrels).

(5) Open storage (location of suitable areas, rail and road connections, approximate capacity).

(6) Petroleum and coal storage (location, type, capacity, bunkering facilities).

(7) Special storage facilities for explosives and ammunition.

l. Clearance facilities (rail lines, highways, inland waterways, pipe lines).

m. Water supply (availability, quality, method and rate of supply).

n. Electric power and lighting (availability, source, and characteristics of current).

o. Capacity of the terminal as a whole, under both normal and present conditions.

p. Data needed for major repairs and improvements; vacant areas available for expansion.

q. Availability of trained, reliable personnel.

Section VII. HYDRAULIC STRUCTURES

119. Types

a. Flood Control. The principal structure employed in flood control is the artificial levee, an embankment built along a river course to prevent flooding of the adjacent country during high water. It may be 6 meters (20 feet) or more in height, and usually is made by packing layers of earth upon a foundation, with grass planted on top of the levee to hold the soil. The levee may be faced with concrete. Usually an artificial levee is constructed some feet in rear of the river banks to provide a wider channel during flood periods.

b. Dams. Earth dams for reservoirs frequently are built of layers of homogeneous material with a center core of puddled clay or other impermeable material. Usually the inner surface is paved with stone or concrete as a precaution against erosion, and the outer surface is covered with grass to bind the surface and to protect it against the weather. Dams across rivers and deep ravines, or where there is considerable width and height, usually are made of stone masonry or concrete. They are built either straight across the river or in the form of an arc, the convex side fronting the stream (fig. 50).

c. Reservoirs. A reservoir is a wholly or partly artificial lake used for water storage. Types of reservoirs include those for flood control, irrigation, recreation, power production, and navigation. Reservoirs are utilized for municipal water supply systems, on rivers to aid in flood control, on canals to maintain the water level for navigation, and in hydroelectric installations to insure a constant water supply. The reservoir may have a lining of clay or other impervious material to prevent water seepage. The embankments or retaining walls may be of earth, loose rock, or masonry. Distributing reservoirs in municipal water systems sometimes are built of masonry or reinforced concrete. They serve to take care of fluctuations in demand and as a reserve in case of interruptions at the source. In reservoirs with earth embankments, overflow is provided for by a *waste weir* or canal, to carry off sur-

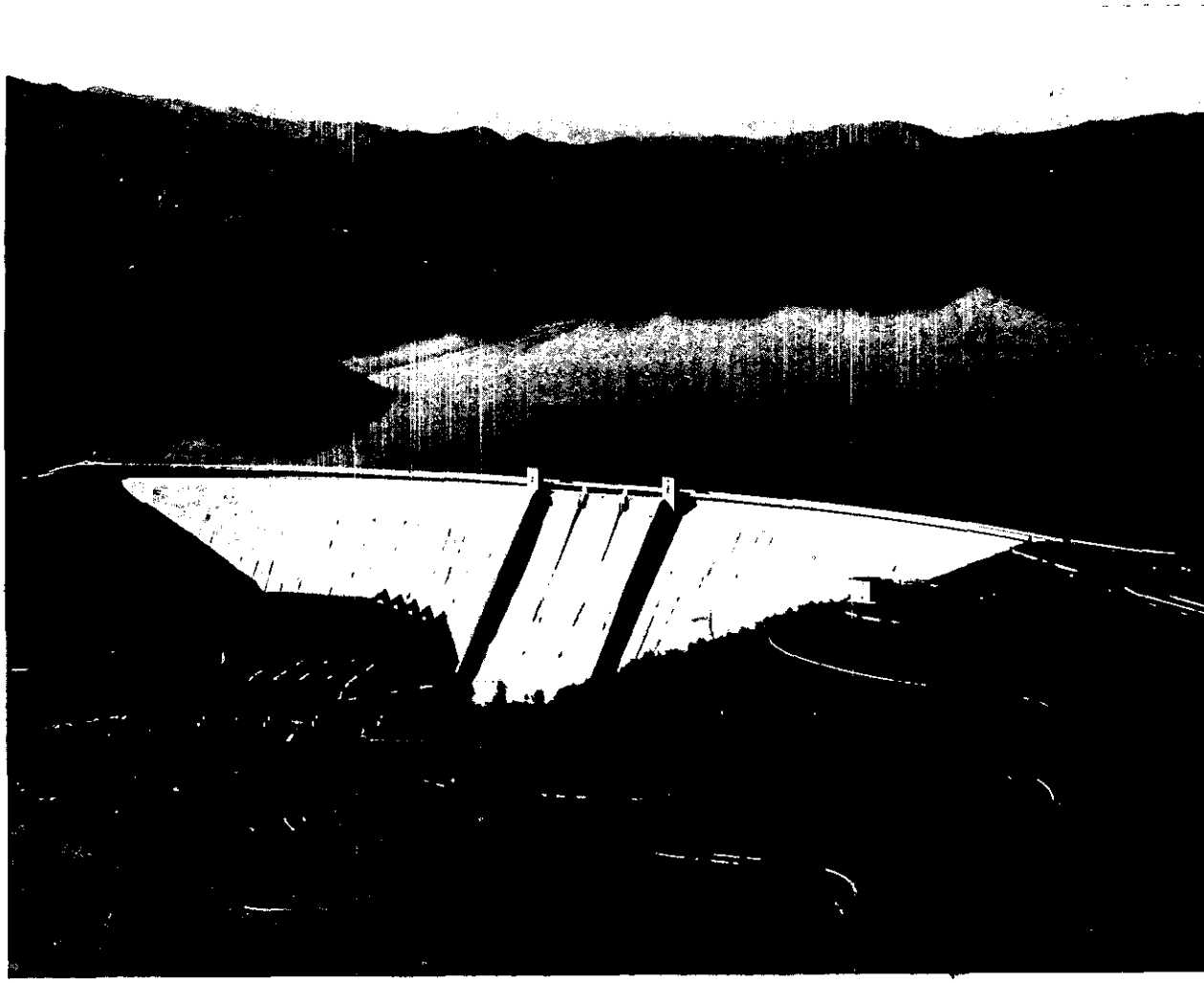


Figure 50. Downstream face of Shasta Dam (California).

plus water. When the reservoir is formed by a masonry dam across a river, the surplus water may be allowed to flow over the top, or spillways may be provided (fig. 51).

d. Locks. The dominant feature of developed waterways is the canal lock. A lock is an enclosed stretch of water with a gate at each end used to raise or lower vessels from one water level to another. When a vessel is to pass from a low level to a higher one, the water in the lock is lowered until it is level with that in which the ship is floating. The vessel is moved into the lock and the gate is closed. Water is then allowed to enter the lock until it reaches the higher level, and then the gate at the other end is opened and the vessel passes through. This procedure is reversed when the vessel goes from a higher to a lower level. Many locks have an intermediate set of gates so that only part of the lock is used for smaller vessels. Usually the water passes through culverts built into the lock walls and is controlled by sluice gates powered by hydraulic or electric power. Lock gates are made of either steel or wood. A pair of gates meets in the center of the lock entrance. When closed, the gates form an arc with the convex side toward the pressure of the water. The lift of a canal lock may be 12 meters (40 feet) or more.

e. Polders. Areas with an extensive network of canals, drainage ditches, and levees may create a major problem in operations. The most notable of these areas are the polders of Belgium and The Netherlands, which have

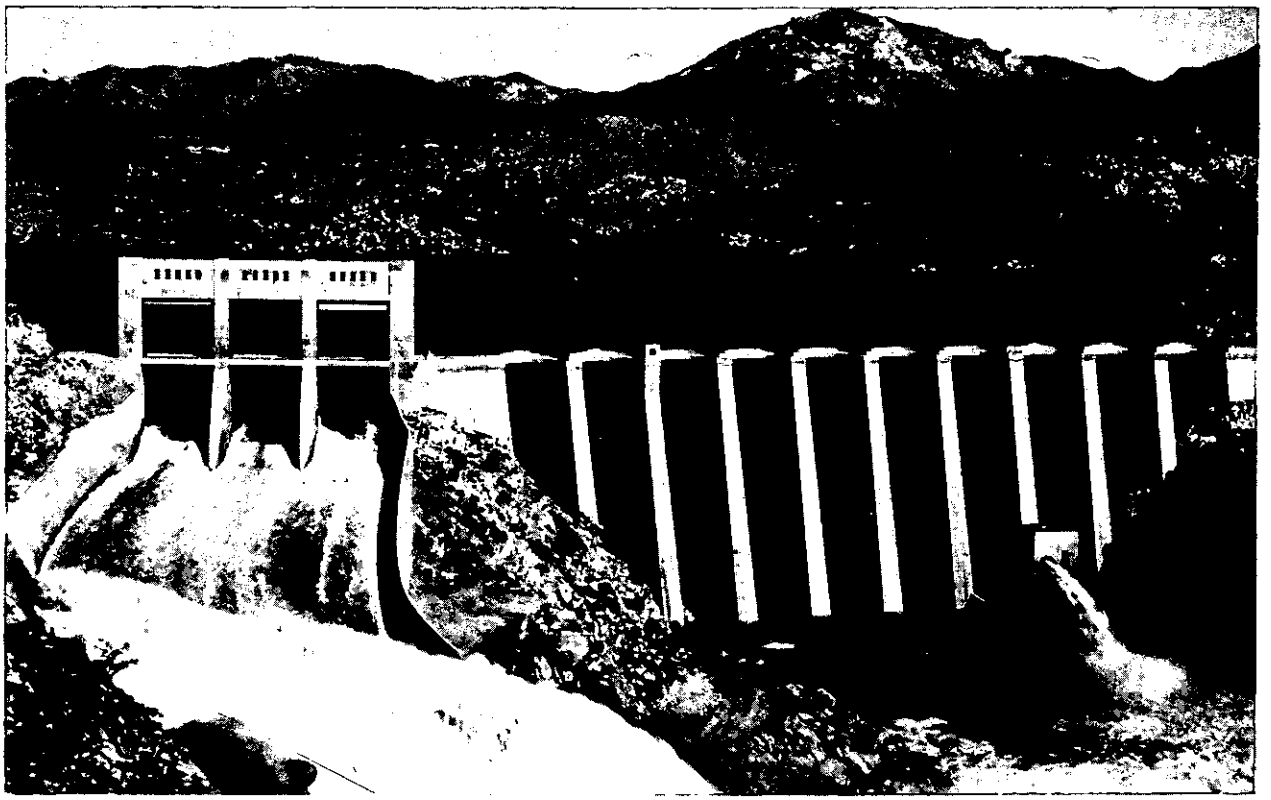


Figure 51. Spillway, storage dam (Bartlett Dam, Arizona).

been reclaimed from the sea by artificial levees called dikes. The terrain is traversed by numerous canals and basins that drain the excess water and serve as navigation routes. The surplus water empties into the sea at low tide. In places where the water courses lead from the interior to the sea, they may be caused to overflow, creating a practically impassable obstacle to movement. In the interior, the polders greatly limit the landing areas suitable for airborne and airmobile forces. When the dikes are destroyed, the cultivated areas are inundated. In these areas tanks and vehicles bog down, there is no cover for infantry, and the water is too shallow for boats.

120. Military Importance

The military importance of hydraulic structures arises from the extensive flooding that may be caused by their destruction. Vast areas may be inundated by the destruction of a large dam or the artificial levees along a major river. Releasing the waters of even a small dam may flood sections of roads and railways or increase the width and velocity of a stream so that crossing operations are impeded. Hydraulic structures in enemy territory may be destroyed by aerial bombardment so as to cause these effects, so they may be seized by airborne forces before the enemy can demolish them. Hydraulic structures are vulnerable to sabotage and guerrilla action. Those in territory under friendly control must be carefully guarded and subject to strict security precautions.

121. Information Requirements — Hydraulic Structures

The type of information that is required concerning a particular hydraulic structure will depend upon whether plans call for its defense, seizure, destruction, or reconstruction. Usually technical specialists are employed to prepare detailed studies of each structure that is being considered. In general, basic information includes—

a. Location and name.

b. Function: navigation, power, flood control, irrigation, water supply.

c. Construction features: design type, materials, height, width, mechanical equipment, capacity.

d. Extent and nature of repairs necessary.

e. Security requirements.

f. Effects of destruction upon the surrounding area.

Section VIII. URBAN AREAS AND BUILDINGS

122. Urban Areas

a. Description. An urban area is defined as a concentration of structures, facilities, and population which forms the economic and cultural focus for some larger area. Usually the inhabitants do not depend upon agricultural activities for their basic economy. A city or town may have a number of functions that make it significant. It may be primarily industrial, commercial, or recreational; the headquarters of government institutions; a port or railway center; or the location of an important cultural feature, such as a cathedral, university, or historical landmark. A large urban area usually has a metropolitan area that includes various surrounding settlements or suburbs whose daily economic and social life is connected with or influenced by the city. Intelligence concerning an urban area covers its general description and importance; physical characteristics; external communication; services and utilities; and major industries, including storage facilities.

b. Topography. The topography and geology of the urban area and its environs are significant elements in the terrain study. Topography exerts a major influence upon the size and pattern of the populated area; the location of external communications; the possibility of inundation or other natural disaster; and the defense that can be made against possible land, waterborne, and air attacks. The development pattern of an urban area is the physical adjustment of the area to its topography, as influenced by past events, current economic forces, and social trends.

c. Construction. The elements comprising an urban area may be classified according to the predominant construction and function of the buildings and other structures. Where no gaps exist between buildings, as in the business districts of larger towns and cities, this is described as block type construction. Detached and semi-detached building areas are those where the buildings are spaced relatively close together, as they are in low- and middle-cost housing areas. Isolated housing areas are found on the approaches to towns and cities where individual or small groups of homes are located in the midst of large open areas. This is typical of the suburbs of the average city.

d. Functional Areas. Normally a city includes separate areas largely devoted to one type of use. The major functional areas may be distinguished as follows:

(1) Industrial areas comprise a grouping of individual plants and loft buildings, with associated storage and transportation facilities, devoted to manufacturing activities.

(2) Commercial areas are composed of a concentration of retail and wholesale establishments, financial institutions, office buildings, hotels, garages, public buildings, and light manufacturing plants.

(3) Residential areas consist predominantly of dwellings with interspersed shopping centers; churches; schools; and fire, police, telephone, and power stations.

(4) Transportation and storage areas contain the terminal, transshipment, storage and repair facilities and service buildings associated with general movement by rail, water, road, pipeline, or railway.

(5) Governmental-institutional areas include the grounds, structures, and facilities related to governmental administrative offices, hospitals, schools, colleges, homes for the aged or orphans, sanitariums, monasteries, penal or research institutions and similar establishments which usually

form distinctive and generally extensive areas.

(6) Military areas contain structures and facilities for billeting, quartering, defense, hospitalization, storage, and repair, which are devoted exclusively to military use.

(7) Open areas comprise land not occupied by buildings and not assigned to any industrial, transportation, business or residential activity. Developed open areas include cultivated land, parks, recreation areas, and cemeteries. Undeveloped open areas include swamps, woods, beaches, and other vacant land.

123. Military Considerations

a. Use of Urban Area. The decision to bypass or to seize and occupy an urban area depends upon the mission of the unit concerned. Cities and towns may be important objectives because they represent centers of population, transportation, manufacture, and supply. Port cities and railroad centers are given a priority status as targets and objectives in both tactical and strategical planning. Unless the mission requires otherwise, a city or town usually is bypassed and isolated, since it is an obstacle that canalizes and impedes both attacking and counterattacking forces. Urban areas are vulnerable to destruction by air or artillery bombardment and may be neutralized by chemical, biological, or radiological contamination. Fires started by nuclear weapons or incendiaries may make them untenable. Combat within built-up areas is described in detail in FM 31–50.

b. Limited Observation and Fields of Fire. Because the opposing troops usually are close to each other, effective close support by artillery and combat aviation is limited. The available cover is rigid and set in straight lines, so that all movement in the open usually can be observed unless it is concealed by smoke, dust, or darkness. Smoke may be used to provide concealment, limit observation, and achieve deception and surprise. In a built-up area, smoke remains effective longer than in open areas. It is usually difficult to observe and locate enemy weapon positions because of the dust caused by the impact of projectiles and explosive charges and the smoke from explosions and fires.

c. Increased Cover and Concealment. Weapons and troops may be concealed in built-up areas, and ample cover is usually available against small-arms fire. Cover from air and artillery bombardment, however, is provided only in buildings of particularly substantial construction.

d. Movement. The mobility and maneuverability of infantry, artillery, and armor are greatly limited in built-up areas. Vehicular traffic is canalized, and extremely vulnerable to ambush and the close-range direct fires of enemy weapons.

e. Communications. It is difficult to maintain efficient communications in built-up areas. Normally control must be decentralized to small-unit commanders. Tall buildings and those with steel frames may interfere with radio communication. Reliance usually must be placed upon wire and foot messengers.

f. Attack. Detailed information concerning the enemy, his defenses, the terrain surrounding the urban area that is under his control, and the layout of the built-up area is essential to the commander in making plans and decisions for an attack. Particular emphasis is placed upon determining the location of covered approaches to the urban area, the location of public utility plants and their security measures and the location and nature of all obstacles. The objective of the attacking force is to seize the entire urban area. Within the area the objectives for individual units include key installations such as railroad stations, telephone exchanges, and the public utility plants, which are often organized as centers of enemy resistance. The attack on an urban area begins with the seizure or terrain features which dominate approaches to the city, followed by the seizure of buildings on the near edge to reduce or eliminate the defender's observation and direct fire upon the approaches. The last phase is a systematic advance through the area until it is fully secured.

g. Defense. Urban areas favor the defense. Whether or not a city or town is organized for

defense depends upon its size, relation to the general defensive position, and the amount of cover it offers for occupying forces. Cities, towns, and villages constructed of flammable materials provide little protection and may become a hazard to the defender, and buildings of solid masonry can be developed into well-fortified defensive positions or centers of resistance. Cellars, sewers, subway tunnels, thick masonry walls, and reinforced concrete floors and roofs provide cover for the defender during heavy bombardments. A heavy aerial or artillery bombardment of a city before an attack actually may serve to strengthen its defenses. The fallen rubble may give the defender increased protection, and may make the streets impassable for armor.

124. Information Requirements—Urban Areas

Information about an urban area requires the compilation of many factors, each devoted to a particular aspect of the area, such as the transportation services, utilities, billeting facilities, or industries. A terrain study should include annotated maps, plans, and photographs, with an accompanying text giving that which cannot be shown graphically. Information that should be included under each category is outlined below. The scope of the information that is presented is limited by the purpose for which the study is being prepared. The text should include information in the following categories, as pertinent:

a. Description.

(1) Name and location (geographic and grid coordinates).

(2) Population (number and trend, significant ethnic and religious segments).

(3) Principal function (communications and industry).

b. Physical Characteristics.

(1) Topography and geology of area and environs.

(2) General cross-country movement of environs.

(3) Climate (mean temperatures and rainfall).

(4) Landmarks (natural and manmade).

(5) Extent of built-up areas (present boundaries, recent additions, probable future expansion).

(6) Functional areas.

c. Structures.

(1) Characteristics of predominant types of buildings (height, number of stories, principal construction materials).

(2) Structure density (ratio of roof coverage to gross ground area; as warranted, ratio of roof coverage to ground area within each of the functional areas).

(3) Principal buildings.

d. Susceptibility to Fire and Shock.

e. Damaged or Destroyed Areas (delineation and general character).

f. Significant Ethnic and Religious Groupings (delineation and general character of the areas occupied).

g. Streets.

(1) Surface, condition, and pattern.

(2) Prevailing widths (to curb and building to building).

(3) Names and alinement of through routes and principal streets.

(4) Location and characteristics of bridges, tunnels, and ferries.

h. External Communications.

(1) *Roads.* Identification of the roads that enter the urban area, the routes that bypass it, and the road distances to the nearest important town on each route should be shown on maps. In the text, the importance of the roads as avenues of movement to and from the town should be discussed. Annotations on city maps should locate and identify highway structures, ferries, and road service facilities.

(2) *Railways.* Maps should show the railways that enter or bypass the urban area, with distances to the nearest

important towns. Text should discuss the importance of the railways as transportation arteries. Annotations on city maps should locate and identify railway structures and crossings (bridges, tunnels, and ferries) and such railway structures as passenger and freight stations, yards and sidings, repair shops, turntables, and "y" track.

(3) *Inland waterways.* Identification of each navigable water route (river, lake or canal) which borders or passes through the urban area and the waterway distance to the nearest upstream or downstream port should appear on maps. The importance of the waterway should be discussed in the text. Annotations on city maps should locate and identify important waterway structures. Information on shipyards is included with that on the industries of the urban area.

(4) *Airfields.* The location of each airfield and seaplane station which serves the urban area should be shown on city maps or, if beyond the limits of the city, on topographic maps. Text should indicate the adequacy of the existing air service, list each commercial airline which serves the area, and provide information on the frequency of service. Information about airfield classification is presented in TM 5–330.

i. Urban Services and Facilities.

(1) Water supply.
- (*a*) Sources (name, location, type, capacity).
- (*b*) Treatment plants (number, type, capacity, and location).
- (*c*) Storage (name, location, type, capacity).
- (*d*) Method of distribution.
- (*e*) Consumption (in terms of minimum and average requirements per person per day, whether any rationing is practiced and during what periods, annual consumption).

(2) Sewage disposal (sanitary, storm, industrial waste).
- (*a*) Collection methods (type, adequacy).
- (*b*) Treatment plants (type, location).
- (*c*) Disposal methods (including location of dumps or incinerating plants).

(3) Garbage and trash disposal.
- (*a*) Collection methods.
- (*b*) Treatment plants (type, location).
- (*c*) Disposal methods (including location of dumps, incinerators, and processing plants producing fertilizer).

(4) Major hospitals.
- (*a*) Name, location, and specialization, if any.
- (*b*) Bed capacity.
- (*c*) Age and condition.

(5) Electricity.
- (*a*) Sources (name, type, location, installed capacity).
- (*b*) Substations (name, type, location, capacity).
- (*c*) Distribution current characteristics.
- (*d*) Number of consumers.
- (*e*) Yearly consumption.

(6) Gas.
- (*a*) Type.
- (*b*) Sources (name, location, capacity).
- (*c*) Storage (type, location, capacity).
- (*d*) Extent of distribution.
- (*e*) Number of consumers.
- (*f*) Yearly consumption.

(7) Storage.
- (*a*) Open (large open areas within or adjoining the town suitable for use as open storage and supply dumps).
- (*b*) Covered (warehouses and sheds).
- (*c*) Cold (refrigerated storage; ice plants with cold-storage facilities).
- (*d*) POL (number of tanks or reservoirs at each location; capacities in U. S. barrels).

(*e*) Explosives (magazine and bulk-storage facilities; types and quantities of explosives stored).

(8) Ice-manufacturing plants (name, location, capacity).

(9) Billeting and accommodation. (Total capacity for billeting and accommodation in military barracks, hotels, public buildings, school and institutional buildings, and other structures; total capacity of bakery and laundry establishments; availability of baths and swimming pools suitable for troop use. Location, capacity, and type of each structure.)

(10) Internal transit system (type, extent, location of main terminal, and maintenance facilities).

(11) Fire protection (organization and manpower of fire department; quantity and type of equipment).

(12) City government (type, personalities, location of facilities).

(13) Civil defense (organization and manpower; quantity and type of equipment).

(14) Industry.

(*a*) Major industrial activity (for each industry, the type, number of plants, number of employees, and importance).

(*b*) Significant manufacturing plants.

125. Buildings

a. Construction. The design and construction of buildings are influenced by climate, available materials, function, and the cultural development of the native inhabitants. In areas with a tropical climate and primitive agriculture, for example, buildings usually are only crude huts made of woven grass, sticks, and mud. Buildings in desert oases are made of clay with thick walls, so that they are cool in summer and fairly warm in winter. In dry climates, where suitable timber is scarce, a wooden structure is a rarity and buildings are constructed from stone, adobe clay, or turf. Where there are cold winters, buildings will be solidly constructed of stone and wood.

b. Military Considerations. The military significance of a building or group of buildings depends upon the purposes of the study. A building may have value as an obstacle, a defensive strongpoint, or as a possible storage, headquarters, medical, or maintenance installation. The structural features of buildings comprise the predominant materials used, size and height, fire resistance, and architectural design. Brick, stone, and masonry buildings, when demolished, create rubble that may make formidable obstacles, or may provide concealment and cover for troops. Flimsy wooden buildings are highly flammable and may be remunerative targets for incendiary shells and bombs. Since the fires are an obstacle to an attacker, they may be employed as a weapon by the defender. The height and number of stories in a building are significant features when selecting observation points. Buildings used in the community may be adapted for military uses. These include garages and other repair facilities, stadiums, theaters, auditoriums, warehouses, transportation terminals, and schools. Wherever possible, structures of religious or artistic importance are usually designated before an operation by civil affairs/military government agencies, and their employment for military purposes is prohibited. Buildings made of solid masonry, concrete, and steel may be organized into defensive strongpoints. Substantial structures with deep basements provide varying degrees of cover from air or artillery attack. The protection against nuclear effects offered by buildings varies according to the type of construction, flammability, distance from ground zero, and many other factors. Personnel in buildings will be protected from the thermal radiation effects of a nuclear weapon and will receive some degree of protection from nuclear radiation effects. Casualties from secondary blast effects are caused largely by falling walls and ceilings and flying glass.

126. Information Requirements—Buildings

a. Location and function (residence, store, warehouse, factory, school, government headquarters, and communication center).

b. Structural features (materials, founda-

tions, roof, bearing capacity of floors, exits, and basement).

c. Layout and capacity (floor plans, areas, cubages).

d. Utilities.

e. Possible military uses.

f. Security features (estimated capability for withstanding bombardment by conventional and nuclear weapons).

g. Needed repairs or improvements for military use.

127. Utilities

a. Special Studies. Detailed intelligence about the utilities of an urban area is necessary in order to plan its utilization for military purposes. In addition, civil affairs may require specific, detailed information and intelligence for special purposes. Special studies by technical personnel should be prepared covering each of the following:

(1) Water supply.
(2) Sewage disposal.
(3) Electric power.
(4) Illuminating gas.
(5) Public transportation system
(6) Communications.
(7) Fire protection.
(8) Trash and garbage disposal.

b. Use of Special Studies. Intelligence studies covering utilities form the basis for estimating requirements for operating and maintenance personnel, the equipment and replacement parts needed for repairs and operation, and the amount of military equipment that must be provided to supplement the existing utility installations. These studies also furnish a guide to selecting the most profitable targets for air attack. The destruction of key utilities is given a high priority in planning aerial bombardments, since a breakdown in these services results in disorganization of the enemy defenses and is highly damaging to civilian morale.

128. Information Requirements—Utilities

The amount and type of information about the utilities of an urban area that is required will depend upon the purpose for which the area is being considered. If it is intended to develop a city into a major logistical base, complete information concerning the capacity, state of repair, and operating methods of each utility will be nceessary. The capability to supply minimum civilian needs as well as military requirements must be evaluated. General surveys of utilities should include the following information about each service or installation—

a. Physical condition.

b. Adequacy for normal load.

c. Portion of present capacity that could be diverted to military use.

d. Repairs, essential for military utilization.

e. Safety and security provisions.

f. Availability of skilled, reliable, civilian personnel.

g. General efficiency and dependability of the plant or system.

Section IX. NONURBAN AREAS

129. Types

a. Farmstead. Populated areas outside towns and cities usually consist of farmsteads and small settlements. A farmstead is the dwelling and adjacent buildings associated with an individual farm. The characteristics of a farmstead reflect the climate of the area and the type of agriculture.

b. Tropical Climate. In rainy tropical climates, most of the inhabitants dwell along streams and waterways, the settlements being located on the bluffs, which are well-drained and exposed to the river breezes. The large rubber, coconut, or banana plantations are usually near the ocean or on the banks of navigable rivers, since roads and railways are few and difficult to maintain. Nonurban areas in dry subtropical climates are dominated by large cattle and sheep ranches, with individ-

ual farmsteads separated by miles of grazing land. In semiarid tropical climates, the native agriculture is largely pastoral, and the relatively few settlements consists of huts surrounded by mud walls or fences of thorny brush. Subarctic villages seldom consist of more than a dozen dwellings, with as much as 50 to 65 kilometers (30 to 40 miles) between settled areas.

c. Temperate Climate. In temperate climates, the buildings of a farmstead are detached from each other, while in areas with extremely cold winters the house, barn, and other outbuildings commonly are under one roof. The outbuildings of a farmstead in the tropics normally are few and small, because the animals remain outdoors all year. Small villages in the middle latitudes often consist of houses built in rows along the sides of a road or clustered around an open square, and in tropical climates the houses of a village usually are dispersed without any regular pattern.

130. Military Significance

a. In general, the same considerations that are pertinent to an urban area also apply to nonurban areas. Small settlements may be critical when they dominate routes of communication at fords, bridges, railway lines, or defiles (fig. 52). Villages that are small in size may have considerable military significance because of a particular industry, mine, or other unique economic feature. They may be local markets and distribution centers serving a wide area and representing an important enemy source of foodstuffs and other supplies. A village with a small local population may be a resort area or the site of a university or similar large institution, capable of providing quarters and other facilities for large numbers of troops.

b. In tactical operations, it is occasionally necessary to secure or destroy small villages that have no direct military value but are used to provide concealment, supplies, and other support to guerrillas. The civilian inhabitants may have to be relocated in other settlements under military control. The buildings of a farmstead furnish quarters for troops and shelter for storage and maintenance facilities. Stone buildings may be suitable for weapons emplacements and defensive strongpoints. Nearly all rural dwellings are within a short distance of a reliable source of water. Cross-country movement frequently is hampered by obstacles such as stone fences, retaining walls, irrigation ditches, and paddy fields. Features such as high fences, hedgerows, embankments, and ditches may offer limited cover and concealment to individuals and small groups.

131. Information Requirements—Nonurban Areas

The particular information about a farmstead or small village that is required will depend largely upon the mission of the unit concerned. Basic information requirements should include—

a. Location; relation to local terrain features.

b. Size (area, population, pattern of streets or roads).

c. Facilities for quarters, maintenance and repair installations.

d. Predominant construction materials.

e. Utilities.

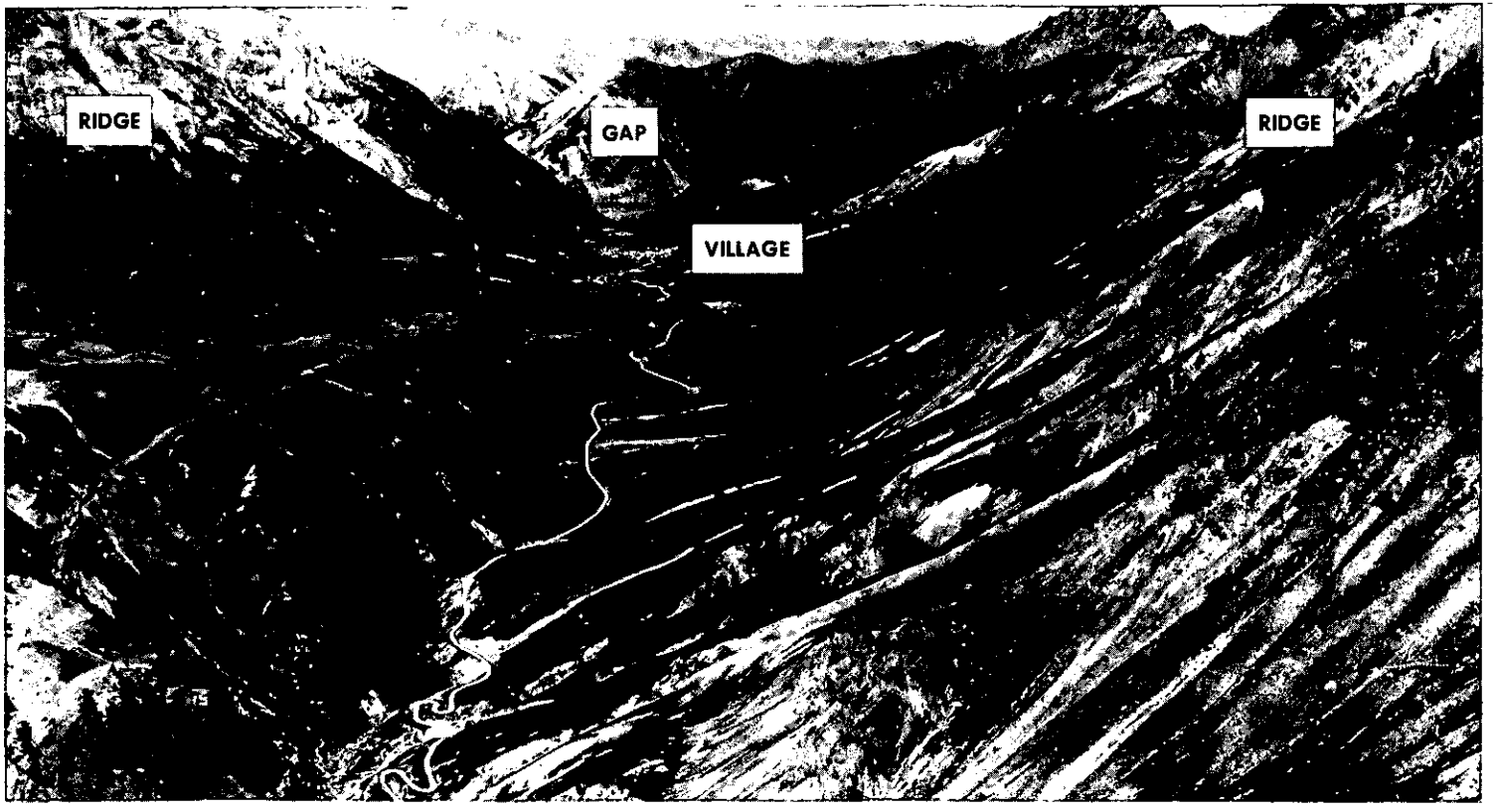


Figure 52. Small settlement dominating a main route of communication.

CHAPTER 7

MILITARY ASPECTS OF THE TERRAIN

Section I. MILITARY USE OF TERRAIN

132. Commander's Considerations

In conducting an operation, the commander must determine how the terrain can be used most effectively by his forces, how it may affect the enemy's capabilities, and how it may be exploited to interfere with the enemy. With the assistance of his staff, he considers the weather conditions, relief and drainage, vegetation, surface materials, and manmade features and their effects upon—

a. Key terrain.

b. Observation and fields of fire.

c. Cover and concealment.

d. Obstacles.

e. Avenues of approach.

f. Communications.

133. Key Terrain

The relative importance of various aspects of the terrain varies with the mission, the type of operation, the size and composition of the forces involved, and their weapons and equipment. Detailed intelligence concerning terrain features normally increases as the size of the unit diminishes. The commander of a field army, for example, may be concerned about the effects that an extensive mountain range will have upon a proposed campaign. A corps commander might be interested only in one mountain of the range, while the commander of a brigade would concentrate upon a particular group of foothills in his area. When making a systematic study of the military aspects of an area, it is sometimes divided into natural subareas, or, if there are no suitable natural boundaries, into subareas based upon the tactical plan. The military aspects of the terrain then are evaluated by each subarea from both the friendly and enemy points of view.

134. Observation and Fields of Fire

a. Observation. Observation is the direct examination of terrain and military activities. It includes examination from ground and air by unaided vision or assisted by optical and infrared devices and detection by photographs, radar, and sonic devices. In general, observation refers to the ability of a force to see the enemy under specified conditions of weather and terrain. The best terrain for observation is that which permits both long-range observation into enemy-held areas and close-in observation of the hostile forward elements. Usually long-range observation is found near the topographical crest and close-in observation is obtained from a location near the military crest. Fog, smoke, precipitation, heat refraction, darkness, manmade and natural features, and vegetation may limit or deny observation. They must be evaluated in determining the extent and type of observation that will be available to enemy and friendly forces. The highest point on the terrain does not always provide the best observation, since variations in relief often create blind spots in the field of vision. The selection of observation points should be based upon reconnaissance, topographic profiles, or examination of aerial photographs.

b. Fields of Fire. A field of fire is an area that a weapon or group of weapons can cover effectively with fire from a given position. The

natural terrain must be evaluated according to its suitability for flat-trajectory weapons, high-trajectory weapons, rockets, and guided missiles, including those with nuclear capabilities. The ideal field of fire for flat-trajectory weapons is flat or gently sloping terrain on which an enemy can be seen with no protection for him within the effective ranges of the waepons. Broken terrain creates dead spots and furnishes cover and concealment for the enemy. Open terrain providing good fields of fire permits a unit to defend a wide front. Broken terrain makes it necessary to provide more troops and weapons to defend a given frontage. The field of fire of high-trajectory weapons is limited only by very steep reverse slopes that the weapons cannot reach and by masks which permit the enemy to occupy positions in defilade. Fields of fire can be improved by cutting or burning vegetation, demolishing buildings, and cutting lanes through woods.

135. Cover and Concealment

a. Evaluation of Terrain. Terrain is evaluated to insure the maximum use of concealment and cover. Terrain under enemy control is also studied, to determine how his concealment and cover can be destroyed. In the attack, concealed and covered routes into the enemy position are sought to gain surprise and to reduce casualties. In the defense, concealment and cover are utilized not only to protect individual positions, but also to hide the general trace of the defenses, so that the attacking troops may be vulnerable to surprise by the location of defense positions and weapons fires. When evaluating terrain for the cover that it will provide, the characteristics of all the weapons used by the enemy must be considered. This includes their ranges, types of fire, and the relative quantities of each type of weapon available to him.

b. Cover. Topography is the major factor influencing cover. Valleys, mountains, gullies, ravines, hills, and similar features provide cover from flat-trajectory weapons. Individuals and small units may secure cover from such terrain features as ditches, riverbanks, folds in the ground, shell craters, buildings, walls, railroad embankments and cuts, and highway fills. Cover from high-angle weapons usually is difficult to obtain. Caves, buildings of exceptionally strong construction, and the steep slopes of hills and mountains may offer some degree of cover, depending upon the capabilities of the weapons employed by the enemy. Nuclear thermal radiation travels by line of sight, so that it will be masked by hills, banks of ravines, and gullies. The extent of protection thus provided will depend upon the height of the explosion. A nuclear blast wave curves around obstacles and is less affected by relief features.

c. Concealment. Terrain features that offer cover also provide concealment. The greater the irregularity of the terrain, the more concealment it will furnish from ground observation. Lower echelons are concerned with the concealment of men, vehicles, weapons, and emplacements; higher echelons, with the concealment of headquarters, supply dumps, airfields, and other major installations.

136. Obstacles

a. Types. According to their effects, obstacles may be classified as antipersonnel obstacles, antimechanized obstacles, underwater obstacles, and obstacles to the landing of aircraft. Natural obstacles comprise such features as unfordable streams, swamps, deep snow, cliffs, steep slopes, thick woods and undergrowth, flooded areas, boulder-strewn areas, lakes, mountains, and nontrafficable soils. Artificial obstacles include those prepared to delay or stop military movement, such as contaminated areas, minefields, trenches, antitank ditches or barriers, roadblocks, blown bridges, road craters, deliberately flooded areas, wire entanglements, and various types of beach and underwater obstacles. They also include man-made features that were not originally designed as obstacles to military movement, such as canals, levees, quarries, or reservoirs.

b. Employment. The employment of obstacles is integrated with the overall scheme of maneuver and fire support. Both natural and artificial obstacles are utilized to channel, direct, restrict, delay, or stop an opposing force. Instructions for the employment of obstacles usually are included as a barrier annex to the operation order of divisions or higher echelons.

FM 31–10 discusses the use of obstacles and the requirements of barrier plans.

c. Barriers. A barrier plan provides for the most effective employment of obstacles to impede enemy movement along favorable routes of approach, divert advancing enemy forces towards routes favorable to defense or compel the enemy to concentrate or disperse. Artificial obstacles must not be located where they would interfere with the proposed movements of friendly forces or with counterattack plans. They may be placed in considerable depth, so as to provide time for counterattacking troops to meet an enemy threat, and to force the enemy to expend time and strength at each barrier. To be fully effective, artificial obstacles must be kept under observation at all times, and must be augmented by fire or explosives. Whenever possible, obstacles are sited so that they are under friendly observation but defiladed from enemy observation. Local unit commanders are responsible for constructing obstacles for the close-in defense of their positions. Advice and technical assistance is provided by engineers, who also construct and install obstacles which require special skill and equipment. The use of toxic chemical and biological agents and radiological contamination to supplement barriers or as obstacles, makes it possible to deny or restrict areas by contamination, to canalize enemy maneuver, or to contaminate enemy field fortifications so that they are untenable. Additional information about the employment of these agents is contained in FM 3–5, FM 21–40, and FM 100–5.

d. Effects. The effects of natural terrain features as obstacles to military movement are discussed in chapter 6. Artificial obstacles are described in FM 5–15 and FM 31–10. The location and extent of both natural and artificial obstacles must be considered by a commander in making his plans. He must decide how they will affect his mission. The tactical effect of an obstacle depends upon the type of operation, the weapons and equipment employed, and the size of the forces involved. A terrain feature that is a major obstacle for a company may be a minor obstacle to a brigade and no obstacle at all to a division.

e. Location. Obstacles may either help or hinder a unit, depending upon their location and nature. For example, a deep creek lying across the axis of advance will slow up an attacker, but will provide defending forces with an advantage, since it delays advancing troops and exposes them to fire. Similarly, heavy woods in front of a position may provide infantry with a concealed route of approach but act as an obstacle to the movement of supporting tanks. In general, obstacles perpendicular to the axis of advance favor a defending force, while those parallel to the axis may give the attacker an advantage by protecting his flanks, although they will also limit lateral movement and his ability to maneuver.

f. Offense. In offensive operations, obstacles influence the choice of objectives, the avenues of approach to an objective, and the time and formation of an attack. Obstacles may be employed to contribute to flank security, impede counterattack, provide additional protection for a section of the front that is not strongly manned, or assist in enemy entrapment.

g. Defense. Obstacles are employed in the defense to channel, direct, delay, or stop the movement of an approaching force. They may be used to delay the initial enemy advance toward the front and flanks of a position, delay the movements of enemy penetrating or enveloping forces, or canalize enemy penetrations into avenues of approach where they can be defeated, or destroyed.

137. Avenues of Approach

a. To a Terrain Feature or an Objective. This is an area of terrain which provides a suitable, relatively easy route of movement for a force of a particular size and type. An avenue of approach should provide—

(1) Ease of movement toward the objective.

(2) Concealment and cover from the defender's observation and fire.

(3) Favorable observation and fields of fire for the attacker.

(4) Adequate maneuver room for the attacking force.

b. Suitability and Ease of Movement. The suitability and ease of movement of an avenue of approach depend upon—

(1) The routes of communication.
(2) Soil trafficability.
(3) Concealment and cover.
(4) Observation and fields of fire.
(5) Obstacles.
(6) Relationship of terrain corridors and cross compartments.

c. Multiple Use. In some types of operations, in which maneuver is very limited by either weather or terrain, an avenue of approach may in itself be a key terrain feature. For example, in rugged mountainous terrain, one road along a valley may be the only route of supply and at the same time the most favorable avenue for approach for the major element of the attacking force. A river in the jungle may be the only transportation route, and thus a key terrain feature, an avenue of approach, and an obstacle.

d. In Attack. Usually an attack is directed toward securing dominating terrain early in the action. The avenue of approach that is most favorable for accomplishing this mission normally is assigned to the forces making the main attack. Whenever possible, the avenues of approach that are selected are those that avoid areas most strongly held by the enemy. In planning an attack, a study is made of the avenues of approach that might be used by the enemy for counterattacks and for reinforcing and supplying his forces. These avenues can be determined by an analysis of the terrain in its relation to the location of enemy reserves and supply routes.

e. In Defense. In planning the organization of defense positions, the terrain is evaluated to determine the avenues of approach that are most likely to be used by the enemy. These normally will be the avenues that lead toward key terrain features, provide good observation, fields of fire, concealment and cover, and either avoid or exploit obstacles. Defense positions are sited to deny such avenues of approach to the enemy. The avenues of approach that can be used by friendly forces in counterattacks also are evaluated.

138. Compartments

The effects of relief and drainage upon avenues of approach are considered in terms of compartments. A terrain compartment is an area bounded on at least two opposite sides by terrain features such as woods, ridges, or villages that limit observation and observed fire into the area from points outside the area. A terrain compartment includes not only the area enclosed but the limiting features as well. Delimiting lines are imaginary lines drawn along limiting features from which ground observetion into a compartment is limited. In compartments formed by woods and villages, these lines run at some point within the edge of the woods or village, depending upon the density of the woods, or the number and density of the buildings. Compartments are classified according to the direction of movement of the forces operating in them. They are termed corridors (fig. 53) when the longer dimension of the compartment lies generally in the direction of movement, or leads toward the objective, and cross compartments (fig. 54) when the longer axis is perpendicular or oblique to the direction of movement. Compartments are also classified as simple or complex (figs. 55 and 56). A complex compartment is one having a smaller compartment or compartments lying within it. This is the type most often encountered.

139. Corridors

Corridors, or ridges that form their limiting features, provide favorable routes of approach for an advancing force because the defender's lateral organization and fields of flat-trajectory fire are obstructed by the limiting features, which also decrease his ability to obtain mutual support between units and limit his observation. To the attacker, a corridor offers two types of approach: valley approach and ridge approach.

a. Valley Approach. Although a valley approach may provide concealment and cover, the military crest of the limiting features on each side must be controlled to deny enemy observation and direct fire into the valley. The best axis of advance is the one that offers the most favorable conditions of observation, cross-country movement, fields of fire, concealment, and cover. Often the most favorable route is along the slopes of a ridge below the military crest rather than along the valley floor. A valley approach should never be used when the enemy controls dominant flank ob-

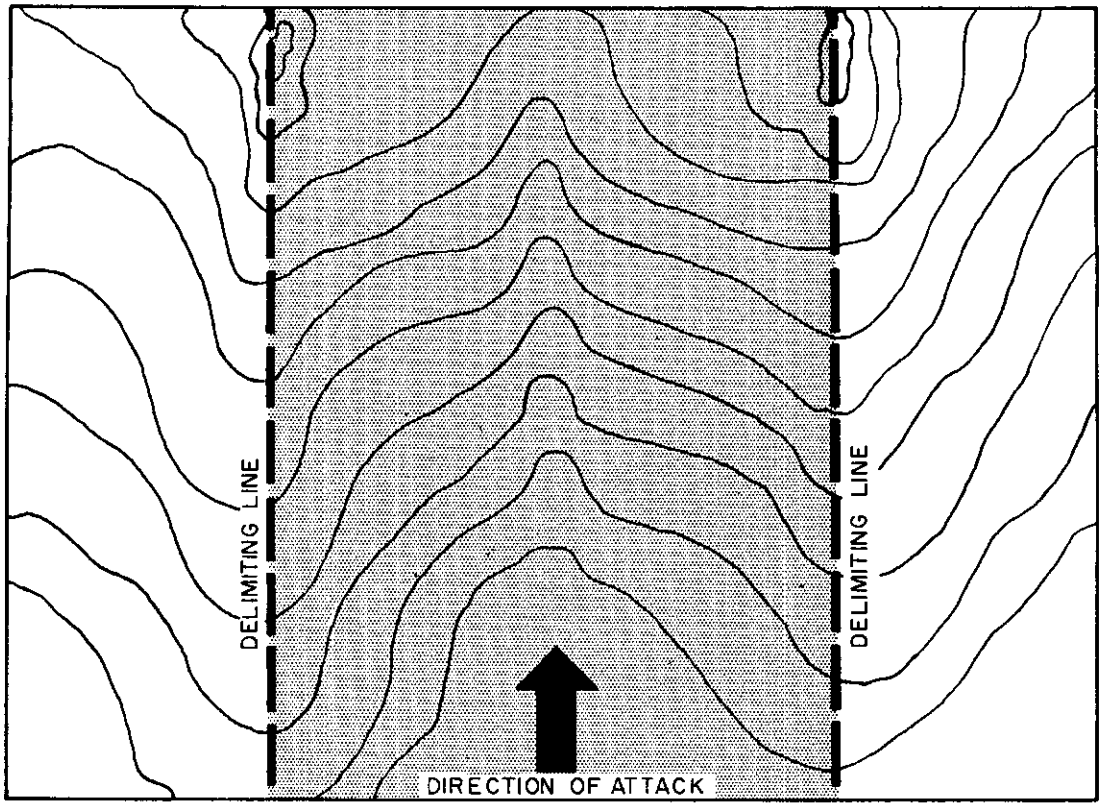


Figure 53. Terrain corridor.

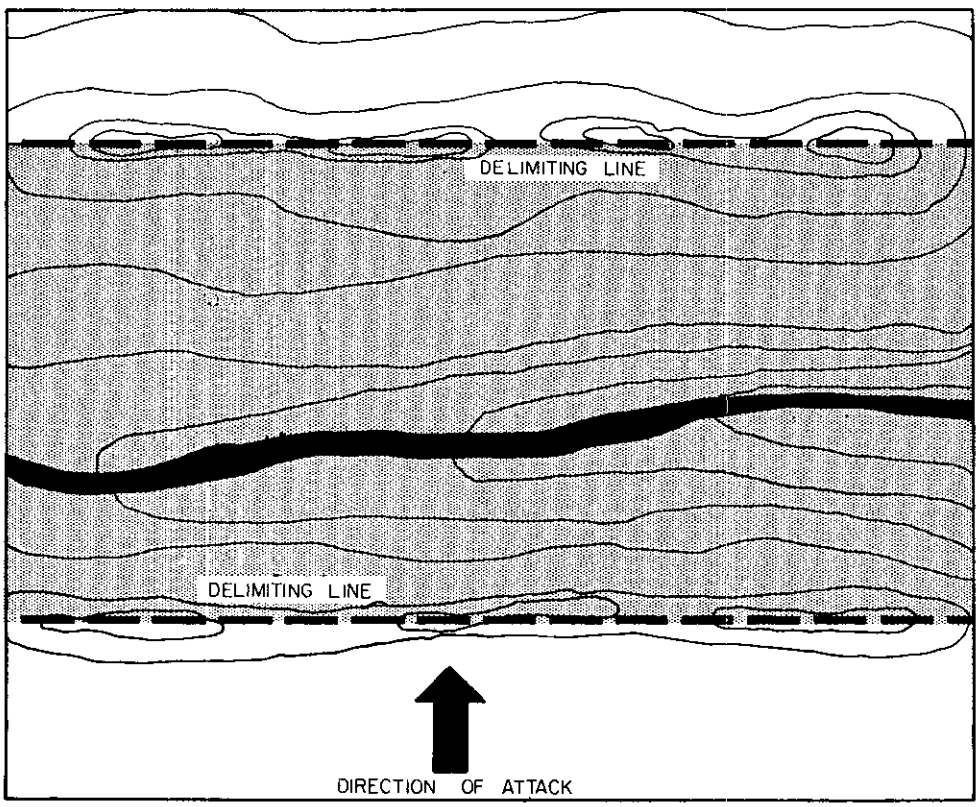


Figure 54. Cross compartment.

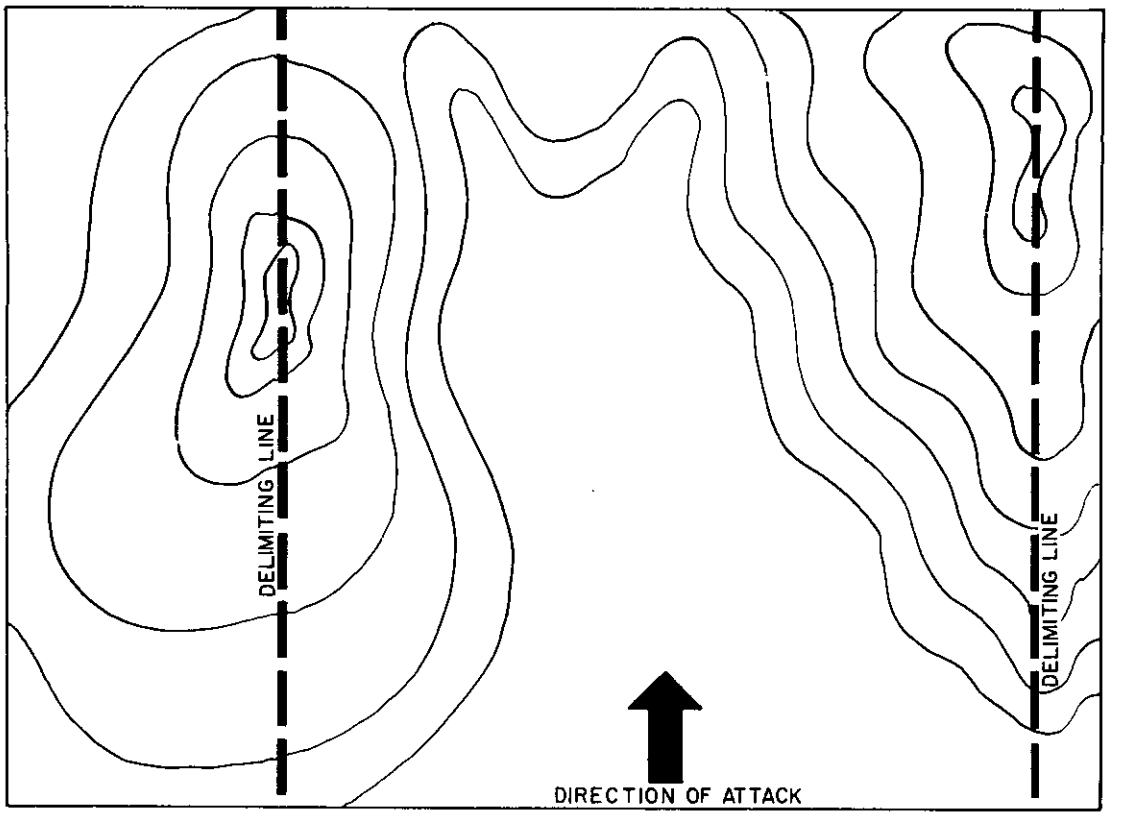


Figure 55. Simple compartment.

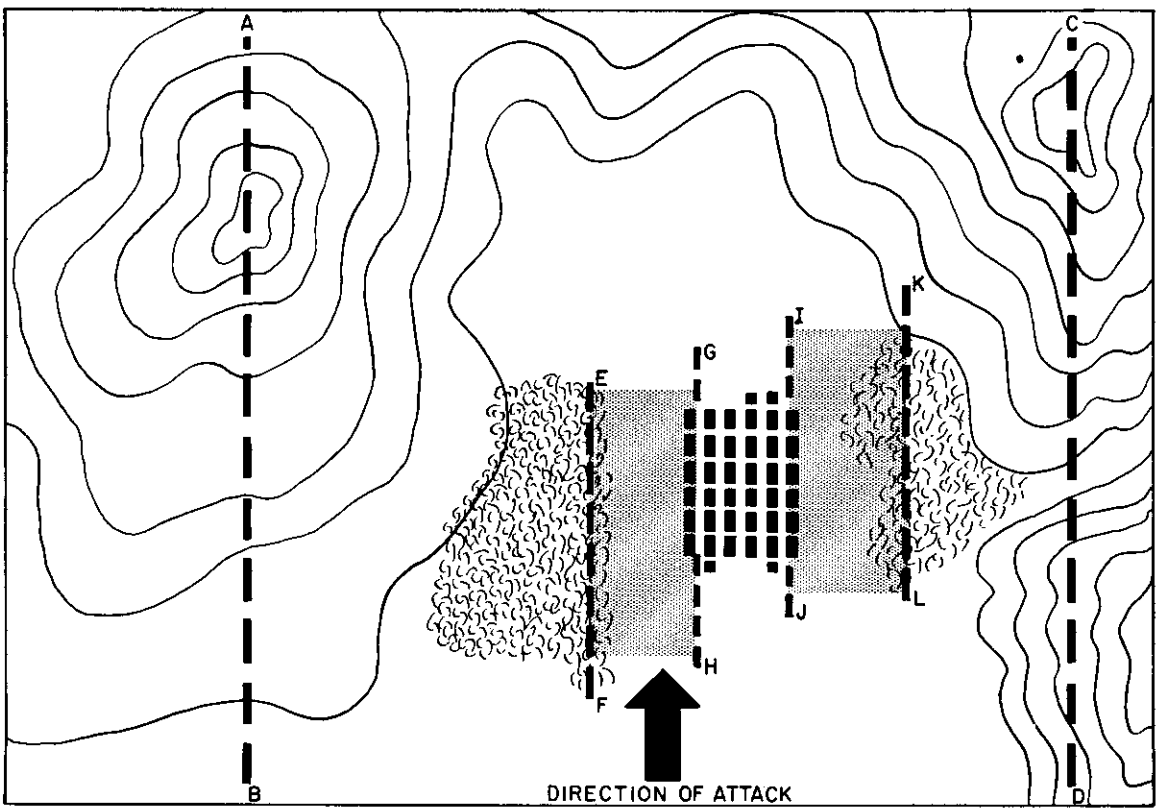


Figure 56. Complex compartments.

servation into the valley, where there are numerous obstacles, and the soils have poor trafficability characteristics.

b. Ridge Approach. The suitability of a ridge for an avenue of approach depends upon its width and shape, the size and frontage of the unit concerned, the distance to adjacent ridges and their elevations, and the capabilities of the enemy weapons. A ridge approach places the axis of advance along dominant observation, but offers little protection from enemy fire directed at the ridge. Usually the best axis of advance in a ridge approach is slightly below the topographical crest, with sufficient forces deployed to control the crest.

c. Cross Compartments. Cross compartments provide the defender with the most favorable terrain for obtaining maximum observation and fields of fire. Mutual support between units, both laterally and in depth, is available and cross compartments also provide the defender with successive defensive or delaying positions. The concealment or cover provided by each limiting feature permits the defender to shift his reserves to meet or to counter threats to his position.

Section II. SPECIAL OPERATIONS

140. Amphibious Operations

a. Detailed Studies. Amphibious operations require detailed studies of hydrography, weather, and terrain. A technical discussion of the requirements and preparation of these studies is beyond the scope of this manual. They are covered in FM 60–30, FM 110–101, and FM 110–115, which also describe the characteristics, tactics, and techniques of amphibious operations. The discussion in this paragraph supplements information in paragraphs 70 through 75.

b. Weather Effects. All phases of an amphibious operation are directly influenced by weather conditions. Weather affects the tides, beaching and unloading conditions, speeds of vessels, air support, and visibility. Poor weather conditions may provide cover for the amphibious force, but favorable weather is essential for the actual landing and during the initial buildup that follows, because excessive sea and swell jeopardize the entire operation.

c. Location. The ideal beach for an amphibious landing is one near a strategic location, with no obstructions seaward; deep water close nearshore; a firm bottom; minimum variation in tides, currents, or surf. The beach terrain should be gently rising, relatively clear, with a firm surface that has adequate drainage. Adequate exits from the beach area should be available. Flat or gently rising terrain, backed by a coastal range high enough to mask the landing area, is the most desirable for landing operations. Ideal conditions are rarely found, and so suitable areas must be evaluated to determine those that come nearest to the optimum requirements.

d. Coastal Plain. A landing on a wide coastal plain provides unrestricted maneuver room usually free from enemy observation and a subsequent advance from the beach can be made in any direction. Boundaries and objectives are hard to locate on this type of terrain, however, and there are few prominent registration points for artillery, naval gunfire, and aerial bombardment. Usually there is no good defensive terrain on the flanks of the beachhead, so that more troops are required to protect the flanks.

e. Coastal Ridge. Terrain which rises evenly to a considerable distance back from the beach gives the defender excellent observation and fields of fire. More commonly, the coastal area remains flat for some distance and then rises abruptly to a coastal ridge.

f. Sand Dunes. Ground that is sharply broken by extensive sand dunes or a low coastal plateau provides the attacker with concealment from enemy observation. The small compartments and corridors limit the range of defensive fires. Direction and control may be extremely difficult.

g. Mountains. Mountains located directly on the sea usually limit the number of beaches large enough to accommodate a landing force of effective size. Where steep ground is lightly defended or neglected by the enemy, a lightly equipped force may seize it and gain surprise. Airborne or airmobile troops may be used to block the movement of enemy reserves to the

landing area, or to secure passes through the mountains and thus prevent the enemy from interfering with the amphibious landing.

141. Airborne-Airmobile Operations

a. Basic Factors. The characteristics, tactics, and techniques of airborne operations are discussed in FM 17–36 and FM 57–10. Airborne forces are capable of crossing such terrain barriers as inland seas, mountains, and jungles that represent serious obstacles to the movement of other troops. Usually airborne assaults are made on terrain that is relatively undefended, to secure initial surprise. Weather has greater restrictive effects upon airborne operations than upon ground operations. Adverse weather may cause postponement or delay in initiating an operation, and prevent adequate reinforcement or supply by air. In addition to terrain studies covering landing and drop-zone areas, special studies may be required to determine the most favorable routes for linkup between airborne forces and friendly ground units.

b. Terrain Requirements. One of the principal factors influencing the selection of a landing area for airborne forces is the terrain. The area chosen must provide adequate space to permit defense in depth; room for maneuver; a safe landing for troops, supplies, and equipment; and protection for critical installations. Airborne troops can land on any terrain that is relatively free from obstacles. Unobstructed areas are required for the landing and recovery of heavy equipment dropped by parachute. Assault aircraft can land on any relatively level and unobstructed terrain that has suitable trafficability. Other fixed-wing transport aircraft require suitable airfields or prepared landing strips. Rotary-wing and other aircraft with vertical takeoff and landing characteristics can land in areas that are otherwise accessible only to parachute units.

c. Drop Areas. The selection of drop areas for the delivery of supplies by parachute requires a consideration of the following:

(1) *Length.* The required length of the area depends upon the type of plane being used. Normally an area 460 meters (500 yards) long is a minimum requirement.

(2) *Width.* A width of 180 meters (200 yards) is minimum. The pilot must have a reasonable amount of room so that he may fly to the right or left of the center of the area, allowing for the drift of his plane under the influence of surface winds.

(3) *Surface conditions.* The type of soil must be considered in relation to the effect that it will have upon the falling loads. A hard surface may cause the bundles to break open upon landing. Soil that is muddy or swampy may cause the dropped loads to bury themselves upon landing, making recovery difficult or impossible.

(4) *Topography.* A clear and level area is desirable. Drop zones on a steep slope or mountainside cause the bundles to scatter, tumble, and break open. A mountain or hill top usually has turbulent winds that reduce drop accuracy and make the drift of bundles unpredictable.

(5) *Access.* A desirable drop zone has an adjacent road, or terrain adjoining the area, that offers good access for vehicles, so that the dropped supplies can be recovered and transported conveniently.

Section III. WATER SUPPLY

142. Importance

An adequate supply of water for drinking, sanitation, construction, and vehicle operation is one of the fundamental needs. In arid and semiarid regions, water supply affects plans and operations. Entire campaigns in desert lands may be conducted solely to secure water sources or to deny them to an enemy. All feasible sources and methods for developing them must be considered when making plans for the water supply of troops and installations. Development data are obtained from reconnaissance, map study, reports or runoff and rainfall average, and geological surveys. Water

sources are located by a study of maps, aerial photographs, water resources data, and intelligence reports, then verified by field reconnaissance if feasible. Detailed information concerning water supply is contained in TM 5–700.

143. Sources

a. Basic Considerations. Water may be obtained from wells, streams, springs, lakes, and municipal or other supplies that are already developed. Water for permanent and semipermanent installations also may be secured from the distillation of sea water or the drainage from building roofs. Investigations to select a water source must consider the quantity and quality of the water, and the conditions at the proposed sites from which the water supply would be secured.

b. Quantity. The quantity of water available in an area depends chiefly upon the climate. In temperate and tropical regions with less than 60 centimeters (25 inches) of annual precipitation, most streams become dry in drought periods. Streams usually flow throughout the year in temperate regions with more than 60 centimeters (25 inches) of annual rainfall and in tropical regions where the rainfall exceeds 90 to 100 centimeters (35 to 40 inches). Seasonal variations may reduce the flow of water below the required amount or result in water points being flooded by seasonal high water periods. The seasonal characteristics of water sources should be obtained from local inhabitants. Terrain studies usually indicate alternate water sources for use in case the primary sources dry up, become flooded, or cannot be used because of enemy action.

c. Quality. Color, turbidity, odor, taste, mineral content, and contamination determine the quality of water. TM 5–700 gives methods for estimating these characteristics and describes the use of standard test kits. The quality of water will vary according to the source and the season, the kind and amount of bacteria present, and the presence of dissolved matter or sediment. Streams in inhabited regions commonly are polluted, with the sediment greatest during flood stages. Streams fed by lakes and springs, with a uniform flow, are usually clear and vary less in the quality of water than do those fed mainly by surface runoff. Water in large lakes generally is of excellent quality, the purity increasing with the distance from shore. Very shallow lakes and small ponds are usually polluted.

d. Site Requirements. The ease with which a water source can be developed, operated, and maintained is determined largely by the location and the routes of communication. The design of the collecting system and the difficulties of development, operations, and maintenance are partially influenced by site conditions, topography, soils and vegetation. A military water point should be located as close as possible to a main route without interfering with traffic. An all-weather access road should lead to the place of storage, with a turnaround or separate exit, and an all-weather off-road parking area for trucks waiting to be filled. In locating the water point, attention is given to concealment and cover, possible nearby targets which may attract enemy fire, drainage, road connections, condition of the banks and the bed if surface water is being drawn, and the means required to develop the source. Existing water supply systems are used when carefully checked by engineers and medical authorities. Purification units may have to be installed. The possibility of contamination by enemy agents also must be considered.

144. Surface Water

a. Regional Variations. Surface water sources are generally more accessible and adequate in plains and plateaus than in mountains. Large amounts of good quality water normally can be obtained in coastal, valley, or alluvial and glacial plains. Although large quantities also can be secured in delta plains, the water may be brackish or salty. Supplies of water are scarce and difficult to obtain on lacustrine, loess, volcanic, and karst plains. In the plains of arid regions, water usually cannot be obtained in the quantities required by a modern army. Much of the water that is available is highly mineralized. In the plains and plateaus of humid tropical regions, surface water is abundant, but it is generally polluted by bacteria and requires treatment. Perennial surface water supplies are difficult to obtain in Arctic regions. In summer, water is abundant but often polluted. In winter it can be obtained

from beneath the ice in the larger lakes and streams, but its quality is poor because of a high organic content.

b. Springs and Seeps. There are two types of springs or seeps: those originating at the base of steep slopes where the topography breaks abruptly, and those caused by faulting. The first type is found along the edges of a valley, and has a perennial flow and fresh, cold water. The second type is caused by the fracture or displacement of confining clay or rock layers above an artesian water-bearing formation (aquifer), thus forcing the water in the artesian zone to the surface. Springs of this type often are thermal, and may contain excessive amounts of minerals. Frequently the depth of a source of water can be estimated by the temperature of the water; the hotter the water, the deeper the source. Spring water is generally clear, cool, and low in organic impurities, but may be hard because of a high dissolved mineral content. In regions where seasonal rainfall varies greatly, the spring flow often decreases during long periods of dry weather. The heavy infiltration of surface water causes some springs to become turbid, and may produce contamination.

c. Streams. Streams are the most common source of surface water supply. Streamflow may vary with precipitation, temperature, and the amount of vegetation. Turbidity and mineral content vary with the flow and with watershed conditions. Since large flows produce high dilution, many such streams may be suitable sources of water supply although they receive raw or partially treated sewage. However, water from such streams must be settled, filtered, and chlorinated before use.

d. Lakes. Ordinarily, lakes are a satisfactory source of water supply. The water level and average yield in small lakes may vary. Many lakes receive sewage flow, have a high content of dissolved minerals, and may have considerable vegetative growth or contain vegetable or animal organisms. These can usually be removed by purification processes.

145. Ground Water

a. Source. Ground water is obtained without difficulty from unconsolidated or poorly consolidated materials in alluvial valleys and plains, streams and coastal terraces, alluvial fans, glacial outwash plains, and alluvial basins in mountainous regions. Areas of sedimentary and permeable igneous rocks also may have fair to excellent aquifers, although they do not usually provide as much ground water as areas composed of unconsolidated materials. Aquifers of this type underlie coastal plains, inland sedimentary plains and basins, karst and volcanic plains and plateaus. Large amounts of good-quality ground water may be obtained at shallow depths from the alluvial plains of valleys and coasts, and in somewhat greater depths in their terraces. Large quantities may also be secured from shallow wells in delta plains, although it is apt to be brackish or salty. Aquifers underlying the surface of inland sedimentary plains and basins also provide adequate amounts of water. Often these formations lie with a few hundred feet of the surface. Those at greater depths yield very hard water which may be too highly mineralized to be drinkable. Abundant quantities of good-quality water generally can be obtained from shallow to deep wells in glacial plains. In loess plains and plateaus, small amounts of water may be secured from shallow wells, but these supplies are apt to fluctuate seasonally. Water from wells usually is clear and low in organic impurity, but it may be high in dissolved mineral content.

b. Plains. Large springs are the best sources of water in karst plains and plateaus. Wells may produce large amounts if they tap underground streams. To estimate the possible yield of proposed wells, information is sought about existing wells that tap similar water-bearing formations in the vicinity. The siting and drilling of wells is difficult because the areas of permeability and the solution cavities in limestone cannot be easily predicted. Shallow wells in low-lying lava plains normally produce large quantities of ground water. In lava uplands, where water is more difficult to find and wells are harder to develop, careful prospecting is necessary to obtain adequate supplies. In wells near the seacoast, excessive withdrawal of fresh water may lower the water table, allowing infiltration of salt water which ruins the well and the surrounding aquifer. Springs and wells near the base of volcanic cones may yield fair quantities of water, but elsewhere in volcanic cones the ground water is too far below

the surface for drilling to be practicable.

c. Climate. Plains and plateaus in arid climates generally yield small, highly mineralized quantities of ground water. In semiarid climates, following a severe drought, there frequently is a flow of subsurface water under an apparently dry streambed that may yield considerable amounts of excellent water. Ground water is abundant in the plains of humid tropical regions, but usually it is polluted by bacteria. In arctic and subarctic plains, wells and springs fed by ground water above the permafrost are dependable only in summer; some of the sources freeze in winter, and subterranean channels and outlets may shift in location during the seasons. Wells that penetrate aquifers within or below the permafrost, however, are good sources of perennial supply.

d. Hills. Adequate supplies of ground water are hard to obtain in hills and mountains composed of gneiss, granite, and granitelike rocks. They may contain springs and shallow wells that will yield water in small amounts.

e. Military Use. Both large- and small-diameter wells are used for military installations. Large-diameter wells usually are dug by hand, in diameters up to 15 meters (50 feet). They may be used as reservoirs, the water level falling during periods of withdrawal and being replenished from subterranean flow during periods of light demand. Small-diameter wells, normally, made by driving, jetting, boring, or drilling, do not provide storage. Deep wells are drilled by percussion rigs or rotary equipment. The amount of water obtained from deep wells will depend upon local conditions. They are less subject than shallow wells to seasonal fluctuation, contamination, and pollution. Information about wells and well-drilling is in TM 5–297.

146. Water Supply Systems

a. Types. There are 3 basic types of water supply and distribution systems—

(1) *Gravity.* The storage reservoirs of gravity distribution systems usually are located high enough to develop the required pressure and flow. Sometimes the storage tanks are filled by gravity from springs located at a higher level, but ordinarily they are filled by pumps.

(2) *Direct pumping.* In direct pumping systems, ordinarily there are no elevated storage tanks. The water is pumped into the distribution system from ground storage reservoirs or wells at a rate depending on demand.

(3) *Combination.* Primary mains are supplied by both gravity and direct pumping in combination systems.

b. Parts. The essential parts of a water supply system are—

(1) *Headworks,* usually a reservoir formed by a dam.

(2) *Conduit,* sometimes an open canal or an aqueduct, but more commonly made of wood, iron, or steel that is watertight to prevent contamination and losses by evaporation, absorption, and changes in temperature.

(3) *Distributing* system, which connects with the plumbing in buildings. Large mains carry the water from the source to service pipes, which take it to individual buildings and other outlets.

147. Information Requirements — Water Supply

Special water supply studies are made by engineers, assisted by geologists and hydrologists. The information required in terrain intelligence studies includes the following—

a. General.

(1) Normal level of water table and variations.

(2) Yield of springs and wells, and variations.

(3) Potability and contaminations.

(4) Underground flow in dry watercourses.

b. Surface Supplies.

(1) Total drainage area.

(2) Rainfall and runoff data.

(3) Sources and kinds of possible contamination, including sewage or industrial wastes.

(4) Chemical and bacteriological analyses.

c. Wells.

(1) Rainfall data.

(2) Reports of available well logs and test data.

(3) Physical, chemical, and bacteriological analyses.

d. Existing Water Supply System.

(1) Source of supply.
(2) Quantity provided; ultimate capacity.
(3) Treatment methods.
(4) Distance from supply to proposed military user point.
(5) Pressures.
(6) Chemical and bacteriological analyses.

CHAPTER 8

TERRAIN STUDIES

Section I. BASIC FEATURES

148. Description

a. Preparation. A terrain study is an intelligence product which presents an analysis and interpretation of the natural and manmade characteristics of an area and their effects on military operations. It is a compilation of only that information which has a direct bearing on some existing requirement. This study is prepared at all echelons to provide the intelligence officer with an analysis of the terrain for use in preparing the analysis of area of operations that forms part of his overall intelligence estimate for the commander, and for use by other staff elements for planning and conduct of operations. The preparation of an analysis of area of operations is discussed in FM 30–5. Above army level, terrain studies are prepared primarily, to assist the commander and his staff. At lower levels, terrain studies are intended chiefly for use in tactical operations and include more details of the terrain and its effects.

b. Topics. Special studies devoted exclusively to certain terrain features or effects may be prepared to meet the requirements of a particular plan or operation. These are produced by technical personnel or teams, and include, but are not limited to, studies concerning—

(1) Construction problems.
(2) Movement.
(3) State of ground.
(4) Water resources.
(5) Lines of communication.
(6) Site selection.
(7) Coast and landing beaches.
(8) Inundation.
(9) Urban areas.
(10) Barriers.
(11) Defenses.
(12) Airborne landing areas.
(13) Soils.
(14) Rock types.
(15) Drainage.
(16) Climate.
(17) Surface configuration.
(18) Inland waterways.
(19) Other military aspects.

149. Prerequisite Information

Before initiating the study, one must know the area to be covered, the mission and type of operation, the specific information required, and the time period to be considered. Terrain intelligence is produced continuously at all echelons. The preparing unit maintains a file of intelligence data, drawing upon it for pertinent matter when he is directed to make a terrain study. Additional information is obtained from the sources and agencies discussed in chapter 3.

150. Format

a. Content. A specific terrain study will not cover every item in outline, but only those items applicable to the operation being planned. Used in this manner, the terrain study form insures uniformity of presentation yet permits the flexibility imposed by terrain analysis.

b. Primary Requirement. The primary requirement for a terrain study at army, corps, or division level is that it must present the intelligence in a form that can be easily utilized by field units. The study must be concise, presenting only pertinent information. Written description should be kept to a minimum. Intelligence should be presented graphically whenever possible.

c. Automation. The intelligence portion of

the Tactical Operations System (TOS) automatic data systems within the Army in the field (ADSAF–75) is an information processing system which uses automatic data processing equipment as a tool for battlefield commanders to help them exercise command and control of their forces and make effective and timely decisions. The computer center accepts information from various sources, including that from forward observers as well as from other computer centers. This information is automatically assembled, sorted, evaluated, and stored by the computer. This computer drives an automatic, constantly up-dated map display which provides the commander with a view of his entire operation. The map includes symbols representing the size, type, and location of all forces, both friendly and enemy, as well as the terrain features, supply dumps, and other intelligence information necessary for the effective evaluation and direction of the operation. This computer center consists of a central processor, memory units, and auxiliary equipment. It also has an automatic communications switching capability which permits contact with all units having an organic intelligence section and a primary intelligence collection mission. In addition, it has operating and monitoring controls for the system.

151. Compilation

a. Format. The format suggested for the terrain study consists of three parts: text, a terrain study map, and a regional description section. A fourth major paragraph, "Analysis of Area of Operations," is prepared by the intelligence officer. The scope of this paragraph is described in FM 30–5. The text follows the sequence of the sample terrain study (app. C). It presents the terrain intelligence called for in the applicable section of the form Tables and charts are used to simplify, amplify, and clarify the presentation. The text should be as concise as possible.

b. Map. Wherever possible, terrain intelligence should be presented on a terrain study map, based on a topographic map of appropriate scale. A map scale of 1:50,000 is usually utilized for brigades and divisions. Corps and army headquarters usually do not require a scale larger than 1:250,000. The terrain intelligence is overprinted on the topographic map (printed in gray monochrome) or is an overlay to the map. Appropriate symbols are used to present items of terrain intelligence. Conditions for movement are portrayed by designated movement colors.

c. Regions. Terrain features exist in certain patterns or combinations, which create distinctive terrain regions. Usually the area of study encompasses several terrain regions. The regional description section of the terrain study gives the user an understanding of the terrain by explaining the combined effect of the terrain features in the regions. This section consists of a sketch map delineating the terrain regions and of brief descriptions summarizing the terrain intelligence for each region. It may be printed on the back of the terrain study map. The information presented in the regional description section enables the user to evaluate the factors influencing movement and to interpret changes in movement which might be caused by changes in weather.

152. Reproduction

Reproduction of terrain studies should be done by the fastest, cheapest, and easiest method. Only as many as necessary for primary users should be made. The engineer topographic battalion assigned to army has the capabilities for map reproduction. The battalion can draft and reproduce in bulk the terrain study map mentioned in paragraph 151. It can also perform the other printing and drafting necessary for the reproduction of terrain studies. The engineer topographic company assigned to corps has basically the same capabilities as the topographic battalion in the type of work it can do, but is limited in volume and equipment. A division has no organic topographic units. Terrain studies are produced by means of duplicators which can produce a map-size paper. The type and quality of terrain studies are limited only by the degree of skill and imagination on the part of the personnel who are responsible for this function.

153. Dissemination

The Engineer or Engineer Terrain Detachment, or G2 Staff Engineer Officer, disseminates the completed terrain study to the G2 and other interested staff elements. The G2 utilizes the terrain study according to the tac-

tical situation and presents the resulting terrain estimate to the commander. If necessary, the terrain study is disseminated to subordinate and adjacent units. The terrain study is also disseminated through engineer channels. Copies are sent to lower echelons to assist them in planning and preparing their own terrain studies. A copy is sent to higher engineer headquarters, and another is sent through enginner channels to the Office of the Chief of Engineers.

Section II. TERRAIN AND CLIMATE

154. Basic Factors Affecting Terrain

The basic factors for a terrain analysis are discussed under item 2 of the terrain study (app C). The factors discussed are climate, topography, and when applicable, coastal hydrography. Although climate and oceanographic aspects of coastal hydrography are not elements of terrain, they have a direct influence on the usefulness of an area for military activities. Appendix C compiles the terrain intelligence that is pertinent to the area of the planned operation. The extent of the area will vary with the echelon performing the compilation. Terrain studies at higher echelons may present fairly extensive descriptions for planning purposes, but terrain studies at lower echelons, having a more definite direction and limit as to area, time, and purpose, restrict their descriptions to the intelligence applicable to the operation planned.

155. Climate

a. Elements. The elements of the climate discussed in a terrain study include visibility, temperature, precipitation, humidity, winds, clouds, and electrical disturbances. Not all must be discussed in every terrain study, because the factors selected depend on the area, time, and type of operation planned. The area of operations influences the description of the climate. The climate of a large area may be described in general terms, whereas a description of a small area will be quite specific. The importance of certain elements of climate depends upon the area. The time that an operation commences determines the type of intelligence presented. Climatic data must be used if the starting date is more than a week or two in the future. (Weather forecasts will be used in the terrain estimate for 5 days or less.) The type of operations planned determines the pertinent elements of climatic information to be furnished. Planning of airborne operations, amphibious operations, and other special operations requires knowledge of weather elements not usually required in normal ground operations. These considerations are discussed in greater detail in manuals pertaining to airborne and amphibious operations.

b. Factors. The methods of describing various factors of climate are discussed below.

(1) *Visibility.* Certain fixed data are best presented graphically. Times of sunrise, sunset, moonrise, moonset, BMNT, EENT, and phases of the moon are best presented on a chart to indicate periods of degree of visibility. Such a chart is included in the sample terrain study. Where pertinent, tide movements can also be presented on this chart. Other deterring influences on visibility, such as fog, smoke, dust, or snowstorms, are discussed in the text.

(2) *Temperature.* This information is generally presented in tabular form. Temperature predictions based solely on climatic studies cannot forecast the expected temperatures, but can describe the range of temperatures that can be expected in a particular location by either of two methods. By the first method, the mean temperature, the mean maximum and mean minimum, and the absolute maximum and absolute minimum temperatures which can be expected for the period can be indicated. The mean temperature alone has little significance since it gives no indication of the range of the temperature variation. The second method is to tabulate the number of days of the period that the temperature can be expected to exceed or

fall below stated temperatures. Temperature effects on other terrain features should be described adequately when significant, such as effect on soil trafficability and freezing or thawing of water bodies.

(3) *Precipitation.* This information, based on climatic studies, can state the type and amount of precipitation encountered during a particular period; the number of days within that period on which certain amounts of precipitation can be expected; and the variability of precipitation from year to year. A statement of the total amount of precipitation that can be expected over a period of time has little significance in itself, since a 3-inch rainfall means one thing when spread over 30 days and a totally different thing when concentrated in 1 day during the 30-day period. The effect of precipitation on other terrain features, particularly water bodies and the trafficability of soils, should be described.

(4) *Winds.* Wind data based on climatic research present the direction, intensities, and duration that can be expected over a period of time. These facts are best expressed graphically by means of a wind rose or may be referenced to the Weather Map Scale of Wind Velocity. Wind rose data may be secured from AWS when specifically required by a commander. The effect of wind on surface materials and on waves is described when pertinent.

(5) *Humidity.* Exact descriptions of humidity are not usually necessary, but the effects of humidity on operations is described when significant. The description should consider fog conditions and the effect of humidity in reducing the efficiency of personnel or in creating problems of storage and maintenance of supplies and equipment.

(6) *Clouds.* Data based on climatic records signify the approximate number of days during a specific period that a certain degree of cloud cover can be expected. There is also a statement as to what time of the day or night certain cloud coverage can be expected. Related conditions such as storms and fog are also described when applicable.

(7) *Electrical disturbances.* This subject is discussed only when it has an important effect on proposed operations. The type of disturbance, its period of occurrence and duration, and its effect on planned operations are described in the text when pertinent.

156. Natural and Manmade Features

a. Relief. Relief is described in the text and symbolized on the map to highlight significant relief features, but not to repeat the detail of a topographic map. The general picture of the relief of an area may be indicated by ridge and stream lining, which accentuates the major ridges and drainage patterns. This consists of emphasizing the streams by drawing over them with a blue pencil and emphasizing ridges with brown pencil. Ridge lining or stream lining can be used separately, if desired, but the combination of the two is more effective. Ridge and stream lining emphasizes the compartmentation of an area, but does not show relative elevations or slope (fig. 57). Another method is to emphasize the principal contours of an area. This is done by tracing over certain critical contour lines with a heavy black pencil or by using different colored pencils to indicate different elevations. This method has the advantage of not obscuring details on the map (fig. 58). Sharp slopes, such as embankments, steep riverbanks, and cliffs are indicated by a red movement symbol when traverse appears to be impracticable. In certain cases, an area may be cut by numerous draws and gullies which are significant but are not shown on topographic maps because their depths are less than the contour interval. These draws and gullies are symbolized on the map. The effect on movement is discussed under "movement" and illustrated graphically by movement symbols.

b. Drainage and Hydrography. Since drain-

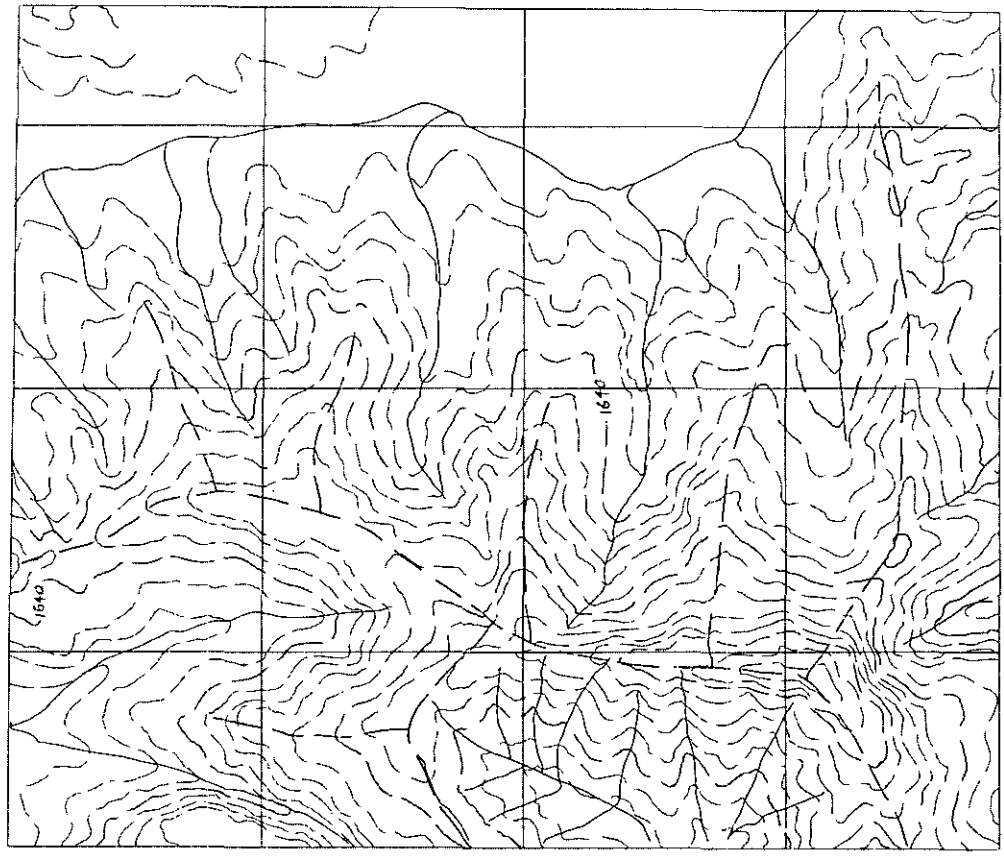


Figure 57. Ridge and stream lining.

age features are subject to change at least seasonally, it is important that the terrain study describe the present condition of the drainage features. The degree of detail in the description is usually determined by the echelon at which the study is prepared and the primary purpose of the study itself. A higher echelon indicates only the major features on the terrain study map, but lower echelon study covering a smaller area can indicate the minor drainage features and give detailed descriptions of them.

c. Vegetation. Forests are indicated graphically. The type of trees, deciduous and evergreen, the density of the forest, and the range of trunk diameters are noted on the map. The text describes other significant vegetation in the area and the effect of weather on the vegetation. Vegetation may be discussed under concealment, fields of fire, obstacles, and any other pertinent aspects of the terrain.

d. Surface Materials. Higher echelon terrain studies usually include a soils map. At army and lower headquarters, this will not usually be feasible. A description of the types of surface materials is included in the surface material section of the study. The effect of surface materials on cross-country movement is an important factor of the terrain study and is described graphically in that section. Surface materials are also discussed in the sections on construction sites and construction materials.

e. Manmade Features. The terrain study describes those manmade terrain features which have particular significance or which require more detailed description to be of value. The more common manmade features are discussed below.

(1) The road-bridge-bypass system is described because of its influence on vehicular movement. A higher echelon study may describe graphically only the primary roads whereas a division study usually describes the secondary

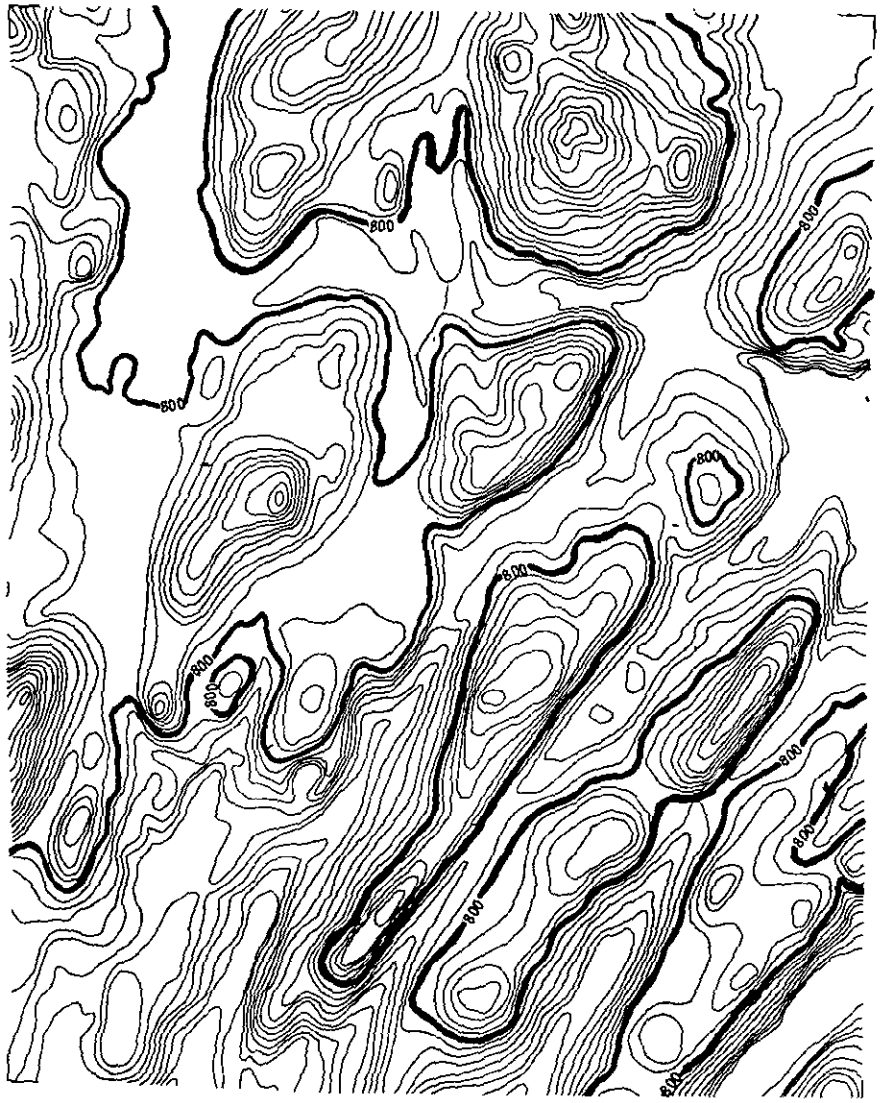


Figure 58. Contour emphasis.

and tertiary systems as well. Important bridges and bypass sites are indicated. (See DIA, AP-1-335-3-1-65 -ADMIN and DIAM 57-5 for route classification symbols.)

(2) Airfields of all types are described. Their locations are shown on the map by standard topographic symbols and an indication is given as to their size and condition. Further details are given in a table.

(3) Principal cities and towns are indicated on the terrain study map, and are listed further in a table.

(4) Railroads are shown on the terrain study map, with detailed information in a table.

(5) Hydrologic structures of all types are described, with detailed information in a table.

Section III. MILITARY ASPECTS

157. Operations

Determining the military aspects of the terrain for an operation requires a knowledge of the terrain and of the operation planned.

Not having complete knowledge of any specific military operation, the person preparing the terrain study should describe the military aspects in terms of generalized operations. The intelligence officer using the study will interpret them in terms of the operation being planned. This is particularly true of key terrain features and avenues of approach. Descriptions of the aspects of terrain vary with the echelon. At army level, descriptions are general; at division level they are more detailed and specific.

158. Key Terrain Features

The determination of key terrain features requires a knowledge of the terrain, the objective, and the plan of operations. As a rule the person making this study may not have a complete knowledge of the plan of operations, and therefore, he must determine those features that have a controlling effect on the surrounding terrain and list them as probable key terrain features for consideration by the user. The description of these features includes a discussion of their significance.

159. Observation and Fields of Fire

a. Observation. The description of observation includes an evaluation of the ground and air observation in the area, and a brief discussion of the terrain features in that area that affect observation. Periods of visibility are described by a visibility chart in the weather and climate section. The effect of the terrain on observation by special devices such as radar, infared equipment, and sound-ranging devices is described when applicable. The description of observation is generally included in the text. A lower echelon study map may indicate the location of individual observation points.

b. Fields of Fire. The description of fields of fire in the terrain study is included in the text, and is primarily concerned with flat-trajectory fire. The description includes a general evaluation and a discussion of the terrain features that affect fields of fire. Features which limit or restrict fields of fire are described in detail. Terrain features that create special problems in the use of high-trajectory weapons are described when they exist. (Areas of marsh or volcanic ash that smother explosive shells are examples of such features.) The possible effect of terrain on nuclear actions is described when pertinent.

160. Cover and Concealment

This includes a discussion of the problem of constructing installations to provide cover, such as foxholes, bunkers, and underground installations. The means available for providing cover from nuclear action is discussed when applicable. Concealment is described in the text with reference to pertinent terrain features such as forests which are portrayed graphically. The amount of concealment and to what extent various type units can utilize it are discussed.

161. Obstacles

The description of obstacles includes a description of the general hindering characteristics of the terrain and a description of specific obstacles. The explanation of the general obstructive elements of the terrain is an overall description and includes terrain features which are unimportant singly, but which constitute obstacles cumulatively, such as systems of irrigation or drainage ditches, terraces, and hedgerows. These are described in the text and indicated graphically by movement symbols. Specific obstacles, such as rivers or escarpments, are described individually. Obstacles that are known to be impracticable for crossing by personnel or equipment are outlined by red hachuring.

162. Avenues of Approach

The determination of avenues of approach involves a summation of all other military aspects as they affect the mission of a particular force. Fixing the avenue of approach involves a tactical decision which is beyond the scope of the engineer intelligence officer. His role in the preparation of a terrain study is to present information on the available avenues of approach for consideration by the G2 and the commander. This information is included in the text. It includes a description of the avenues of approach and a brief discussion of their advantages and disadvantages.

163. Movement

The description of cross-country movement

conditions is the most important and detailed of the descriptions of military aspects of the terrain. The description of movement in the text is devoted to a general evaluation of conditions for movement in the area and a discussion of the terrain features and weather conditions which affect movement. Movement is shown graphically on the terrain study map by color symbols which represent an evaluation of movement conditions. The effect of all terrain features is considered in the text on movement evaluation. The specific meaning of symbols as applied to the area of study is explained in the margin of appropriate classification symbols. A more complete discussion of areas of poor or doubtful movement than is possible on the terrain study map is contained in the regional description section, to enable the commander to determine conditions under which movement is possible through the area.

164. Construction Materials

The description of construction materials presents information on the availability of construction materials in the area of operations. It includes data on the presence of developed and undeveloped sources of rock, sand, gravel, and aggregate, and of stocks of lumber, steel, and other construction materials. It is not a detailed report, but presents general data on the availability of materials for construction in the area. Availability of building materials is discussed generally under military aspects of the terrain. Detailed reports on the sources of construction materials are prepared separately as required by engineer units.

165. Suitability of Sites for Construction

The description of construction sites includes a discussion of sites for roads, airfields, and other surface and underground installations. This description should be suited to the needs of the echelon for which the study is prepared. The description does not indicate specific sites, but describes the general suitability of the area for various types of construction. Building sites are discussed generally in the text. Detailed reports on appropriate sites for specific construction projects are prepared separately as required.

166. Water Supply

The description of water supply enumerates the sources of water available in the area and evaluates their suitability for use by the troops. It includes a discussion of natural water sources and water supply systems. When pertinent, the water requirements of the civilian population are discussed. Water supply is discussed in the text.

Section IV. COASTAL HYDROGRAPHY

167. Describing Coastal Hydrography

a. Presentation. Descriptions of coastal hydrography are of interest primarily for amphibious operations. They differ from overland operations only in the method of transportation and types of routes by which they arrive at the area of operations. The terrain study for an amphibious operation includes: text, terrain study map, and tables. These are the same elements which are in the land-operation study, but the terrain study for an amphibious operation must also include a means for presenting detailed intelligence about the landing area. This is done by extending the three elements of presentation mentioned above to include descriptions of the landing area, and by use of a fourth element, the beach profile diagram. Application of this method of description to coastal hydrography is discussed below.

b. Text. The text describes the features of coastal hydrography, such as sea approaches, beach area, sea and surf, and tides. The description is coordinated with the graphic presentation. The effect of other terrain features on coastal hydrographic conditions is also described, and includes the effect of inland surface materials on beach composition.

c. Terrain Study Map. The terrain study map shows potential amphibious landing areas. Since the terrain study map may be of too small a scale to be of value as a description of the landing area, it is generally used to depict the configuration of the coast line, location and length of the beaches, and location of exits from the beaches.

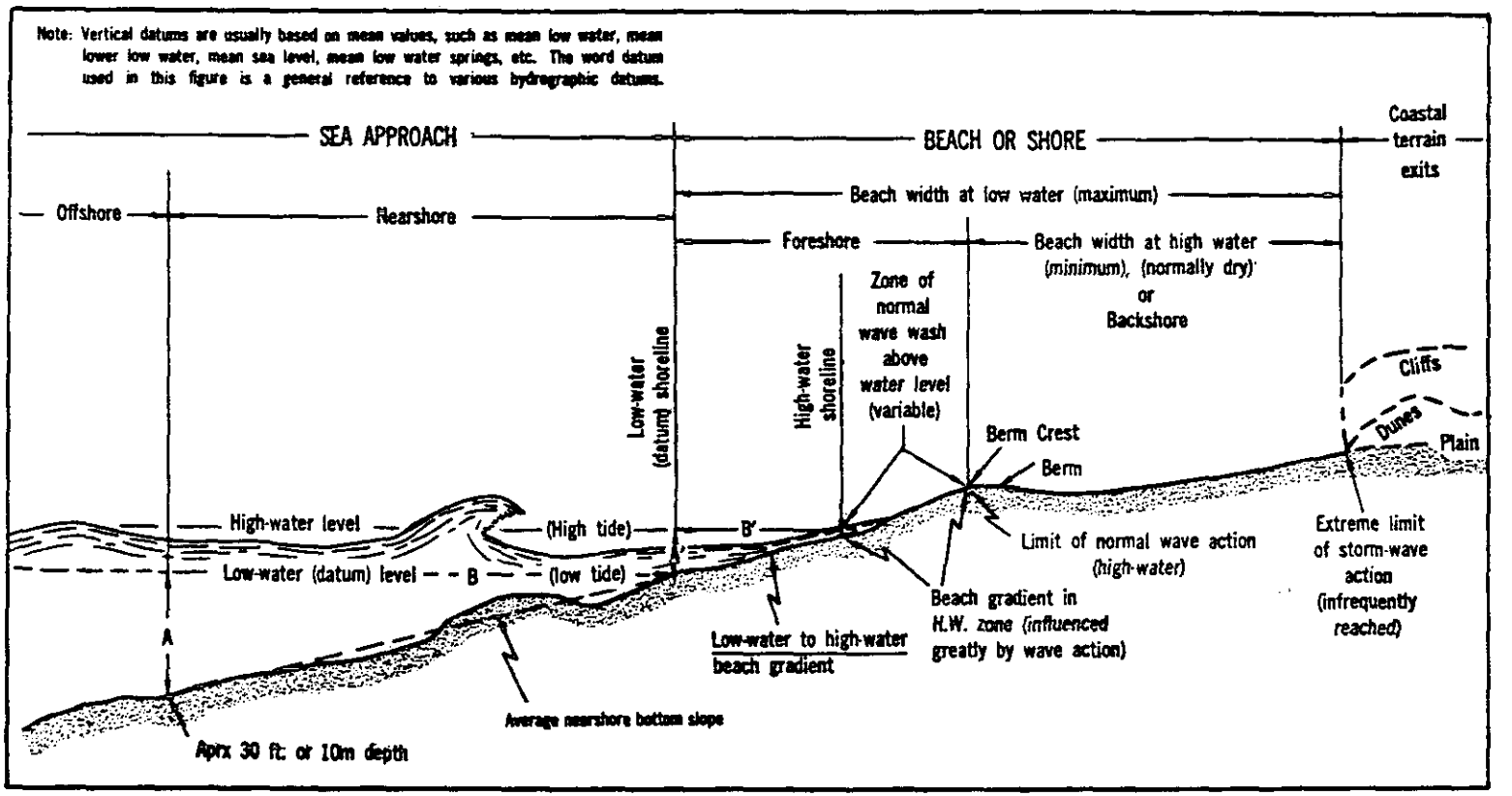


Figure 59. General beach profile diagram (tidal sea).

d. Description. A description of both the hydrographic and terrain conditions for each landing area is included in a table.

e. Beach Profile Diagram. The beach profile diagram (fig. 59) is a large scale sketch of the offshore and nearshore area, the shore, and the coastal terrain (hinterland). The water levels at high tide and low tide are shown in the offshore, nearshore, and foreshore areas. In addition, the beach widths at high water level and low water level and some of the coastal terrain are shown. A profile of the area to the rear of the beach, showing landmarks visible from the sea, is included if deemed necessary as a navigation aid for landing craft. Other data may be included if it is pertinent to the operation.

168. Sea Approaches

a. Offshore Approaches. The offshore approaches are usually of interest only to naval forces and therefore are not described in the terrain study. When description is necessary, a hydrographic chart may be utilized.

b. Nearshore Approaches. The nearshore approaches are of primary interest to landing forces and, as such, require a detailed description. The description should present a general evaluation of the nearshore area, and describe bottom conditions and the effect of sea, swell, breakers, surf, tides and currents. Also described are any special phenomena such as sea vegetation thick enough to be classed as an obstacle, ice conditions, unusual or tricky currents. The landing area map presents a graphic description of the nearshore area. The general relief of the area is described by contours based on the hydrographic chart datum plane. Obstacles are located on the map and any special features are identified by special symbols. Representative profiles, as necessary, describe the gradient of the nearshore area.

c. Beaches and Beach Exits. The text presents a general description of the beach area, covering such items as the capacity of the beach, its composition and trafficability, and the capacity of beach exits. The terrain study map describes the general configuration of the coast, the location and length of the beaches, and the beach exits. The regional description deals with the beaches as part of topographic regions. The landing-area map presents a detailed graphic description of the beaches. It portrays the dimensions of the beaches and the location of obstacles areas, and describes the beach exits. The colors used in the landing-area map conform to the color key used in all movement maps. The water tint usually extends to the high water shoreline, or at time to mean sea level, depending upon the mapping agency. One or more profiles are used to describe the beach gradient. If necessary, the area to the rear of the beach is included to indicate the position of landmarks as seen from seaward.

d. Sea and Swell. Sea is defined as waves caused by local winds, whereas swell refers to wind-generated waves that have advanced beyond the region of generation. The direction of sea is that of the local wind, whereas the direction of swell is independent of, but may coincide with the local wind. Both sea and swell may be present at the same time. Sea and swell must be described in the text, with roses that show the frequency of various height categories by direction.

e. Breakers and Surf. Surf is the disturbed water area extending from the outer breaker line to the limit of uprush on the beach. Breakers are waves that shoal over a reef or on a shore. Hazards to landing increase with increasing breaker height, and vary with period of waves, type of breakers, and the direction of breaker approach onto the beach. Breakers and surf are described by the text, and breaker roses show frequency by direction of specified breaker height ranges.

f. Tides. Tide information is presented graphically. Curves portray times of high and low tides, and can be incorporated into the visibility chart. A chart showing the tides during the period of the study is included in the margin of the landing-area map for predicting the heights of the water at any given time. Special tidal conditions and tidal currents are described in the study text.

CHAPTER 9

TRAFFICABILITY

169. Estimating Soils Trafficability

The purpose of this chapter is to assist intelligence and reconnaissance personnel to determine the trafficability of soils to support cross-country movement of military vehicles. Increased emphasis on the military concept of dispersion, which requires cross-country movement has increased the requirement for information on soil trafficability. Most information on trafficability pertains to military vehicles operating on various unfrozen soils in the temperate zones. The procedures for measurement of soil trafficability can also be applied to unfrozen soils that have been subjected to freeze-thaw cycles. An estimate of trafficability can be made with the aid of this chapter if something is known of the general weather conditions, the topography and the soils of the area.

170. Weather and Climate

Information about the weather and climate is available from meteorological records, and climatology textbooks, and by interrogation of prisoners. Only two general conditions of weather apply to trafficability estimates, the dry period and the wet period.

a. Trafficability During Dry Period. During a dry period all soils usually are passable unless the area is low-lying and poorly drained or is kept wet by underground springs. Sand in a dry state is less trafficable than in a wetter condition (with the exception of quicksand).

b. Trafficability During Wet Period. When moisture is added to a soil its strength is changed. Different soils are affected differently by moisture. During a wet period, all soils with the exception of clean sands and gravels provide poor trafficability. The relative trafficability ratings of soil types under set conditions are given in figure 60. This figure is explained in paragraph 178.

171. Topography

The effects of slopes on soil requirements for vehicle performance can be shown in quantitative units when actual measurements of the cone index (para 174*d*) can be made, but in estimates of trafficability only general statements concerning slopes are feasible. Slopes require better soil traction conditions for vehicle movement than does level terrain of a similar soil type. Other factors pertaining to trafficability that must be kept in mind are that ridges are generally more trafficable than the adjacent valley, that downhill travel is easier than uphill travel, and that low tire pressure increases traction. During the dry season, sand slopes of approximately 30 percent are impassable. Fine-grained soils and sands with fines which are poorly drained may be trafficable up to a 45 percent slope. During the wet season a 30 percent slope is the maximum that should be tried on any type soil.

172. Soils Maps

Two types of soils maps exist. One type classifies the soils according to the Unified Soil Classification System (USCS), as used in determining trafficability. The second type of soils map employs the agricultural system of soil classification (ASSC). This type is not used by the military. It is mentioned here to avoid confusing it with the USCS. Soils are formed by the action of the following factors: parent material, climate, age, chemical action, topography, and vegetation. A trained analyst can estimate the soil types by using a geologic map, providing he has a general knowledge of the climate, the topography, and the vegetation of the area.

173. Aerial Photographs

The full utilization of aerial photos in estimating trafficability is presently being studied. At present the following information pertaining to trafficability is obtained from aerial photographs.

a. Topography. Aerial photographs are a good source of topographic information. Estimates of elevations and slopes can be made from stereopairs by properly instructed personnel. Accurate elevations and slopes can be obtained by trained operators using mechanical equipment such as Multiplex and Kelch plotters.

b. Soils and Moisture Conditions. In the present stage of development, the techniques for identifying soils from airphotos are so complex that only well-trained technicians can employ them to their fullest extent. However, certain general facts may be used to advantage by personnel with a minimum of training. For instance, orchards usually are planted in well-drained, sandy soils; vertical cuts are an evidence of deep loessial (silty) soils; tile drains in agricultural areas indicate the presence of poorly drained soils, probably silts and clays. On a given photo, light color tones generally signify higher elevations, sandier soils, and lower moisture contents than do dark color tones. The same color tone does not always indicate the same soil conditions even on the same photo. Color tone may have entirely different significance on two separate photos. Also, natural tones are apt to be obscured and modified by tones created by vegetation (natural and cultivated), plowed fields, and shadows of clouds.

c. Vegetation. Dense grass, especially if wet, will cause slipperiness. Tall grass will often restrict visibility. Heavier vegetation such as brush and trees will decrease trafficability if the vehicles must push aside this vegetation as they advance. The presence of vegetation in sands usually stabilizes the soil, thus increasing its trafficability. Decaying vegetation including the roots, found especially in the northern latitudes, adds to the support of the soil if the soil is weak. The limited testing that has been done shows that if the mat of partially decayed vegetation is 6 or more inches thick it will support 40 to 50 passes of very light vehicles such as the M29 amphibious cargo carrier. Heavier vehicles will break through after 2 or 3 passes.

d. Obstacles. A complete assessment of the trafficability of a given area must include an evaluation of obstacles such as forests, rivers, boulders, ditches, hedgerows, steep slopes and cliffs, and embankments. Aerial photographs are valuable in identifying these features.

174. Trafficability Terms

a. Trafficability. The capacity of a soil to withstand traffic of military vehicles.

b. Bearing Capacity. The ability of a soil to support a vehicle without excessive settlement of the vehicle. California Bearing Ratio is used in denoting design values.

c. Traction Capacity. Ability of a soil to resist the vehicle tread thrust required for steering and propulsion.

d. Cone Index. A numerical indication of the carrying ability (resistance to penetration by wheels and tracks of vehicles) of a soil. An index of the shearing resistance of soil obtained with the cone penetrometer; a dimensionless number representing resistance to penetration into the soil of a 30° cone with a ½-sq in. base area (actually load in pounds on cone base area in square inches). TM 5–530 discusses this in detail.

e. Remolding. The changing or working of a soil by traffic, or by a remolding test. Remolding may have a beneficial, neutral, or detrimental effect on soil strength.

f. Remolding Index. The ratio of remolded soil strength to original strength, determined in accordance with procedures described in TM 5–530.

g. Rating Cone Index. The measured cone index multiplied by the remolding index; it expresses the soil-strength rating of an area.

h. Critical Layer. The soil layer in which the rating cone index is considered a significant measure of trafficability, or the layer of soil which is regarded as being most pertinent to establishing relationship between soil strength and vehicle performance. Its depth varies with the weight and type of vehicle and the soil

profile, but it is normally the layer lying 6 or 12 inches below the surface.

i. Vehicle Cone Index. The index assigned to a given vehicle that indicates the minimum soil strength in terms of rating cone index required to permit 50 passes of the vehicle.

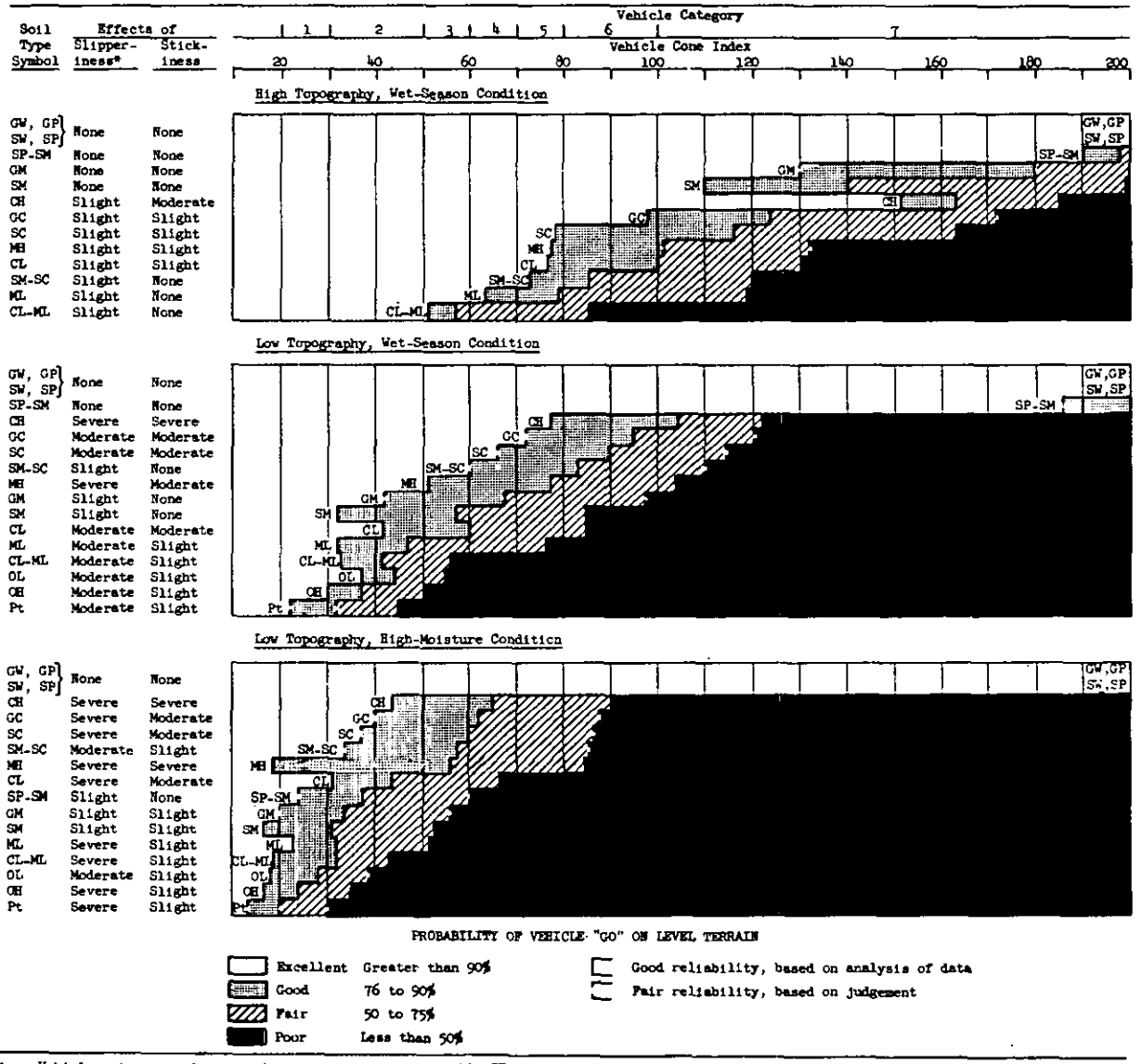
j. Stickiness. The ability of a soil to adhere to vehicles, wheels, and tracks.

k. Slipperiness. Low traction capacity of a soil's surface due to its lubrication by water or mud.

l. Mobility Index. A dimensionless number which results from a consideration of certain vehicle characteristics.

m. Maximum Tractive Effort. The maximum continuous towing force or pull a vehicle can exert expressed as a ratio or percentage of its own weight.

n. Fine-Grained Soil. A soil of which more than 50 percent of the grains, by weight, will pass a No. 200 sieve (Unified Soils Classification System (USCS)).



Note: Vehicle category and cone index range are given on table II.

* Applies only to wheeled vehicles without traction devices.

Figure 60. Soil trafficability classification (USCS).

o. Coarse-Grained Soil. A soil of which 50 percent or more of the grains, by weight, will be retained on a No. 200 sieve.

p. Sand with Fines, Poorly Drained. A sand in which water content greatly influences the trafficability characteristics. These soils react to traffic in a manner similar to fine-grained soils. They usually contain 7 percent or more of material passing the No. 200 sieve, and little or no gravel.

175. Soil Trafficability Table

a. Soil Type Symbols. The soil type symbols used on figure 60 are those employed in the Unified Soil Classification System (USCS). The symbols are given on the extreme left of the figure and also in the graphic portion. The duplication aids in the reading of the graphs. These letter symbols are explained in table 2. Hyphenated letters indicate a mixture of types of soils.

Table 2. Soils Symbols

Symbols	
GW	gravel-sand mixtures, little or no fines.
GP	gravel-sand mixtures, little or no fines.
SW	gravelly sands, little or no fines.
SP	gravelly sands, little or no fines.
CH	inorganic clays of high plasticity, fat clays.
GC	gravel-sand-clay mixtures.
SC	sand-clay mixtures.
CL	gravelly clays, sandy clays, inorganic clays of low to medium plasticity, lean clays, and silty clays.
GM	gravel-sand-silt mixtures.
SM	sand-silt mixtures.
ML	low plasticity silts.
MH	inorganic silts, micaceous or diatomaceous fine sandy or silty soils and elastic silts.
OL	organic silts and organic silty clays of low plasticity.
OH	organic clays of medium to high plasticity and organic silts.

Peat, muck, and swamp soils are not classified in the above list because such soils are almost always impassible except for light amphibious-type vehicles.

b. Strength Measurements. The probable ranges of the cone index (CI), the remolding index (RI), the rating cone index (RCI), and the mean rating cone index are given on figure 60 for those desiring this technical information. For most trafficability purposes this information may be folded out of view to simplify the reading of the remainder of the trafficability chart. Information on the strength measurements is given in TM 5–530.

176. Slipperiness and Stickiness

The information on figure 60 pertaining to stickiness and slipperiness is self-explanatory. The following is general information on each of these two factors.

a. Stickiness. No instrument for measuring the effects of stickiness on the performance of vehicles has been devised. Stickiness will occur in all fine-grained soils when they are comparatively wet. The greater the plasticity of soil, the more severe are the effects of stickiness. In general, stickiness will have adverse effect on the speed and facility of travel and steering of all vehicles. It will immobilize small tracked vehicles like the M29 weasel, but will not stop the larger and more powerful military vehicles. Removal of fenders will reduce stickiness effects on some vehicles.

b. Slipperiness. Like stickiness, the effects of slipperiness cannot be measured quantitatively. Soils which are covered with water or a layer of soft plastic soil usually are slippery and often cause steering difficulty, especially to rubber-tired vehicles. They can often immobilize vehicles, especially when slipperiness is associated with low bearing capacity. Slipperiness effects assume greater significance on slopes. Sometimes slopes whose soil strength is adequate may not be passable because of slipperiness. The use of chains on rubber-tired vehicles usually will be of benefit in slippery conditions.

177. Vehicle Categories

Military vehicles are divided into seven categories according to a cone index range as shown in table 3. These vehicle categories, 1 through 7, are shown at the top of figure 60.

a. Vehicle Cone Index. This index is shown directly below the vehicle category range on figure 60. It is helpful in showing the trafficability of vehicles below category 1 and subdivides each of the seven vehicle categories, especially category 7.

Table 3. Vehicle Categories

Category	Vehicle cone index range	Vehicles
1	20–29	The M29 weasel, M76 Otter, and Canadian snowmobile are the only known standard vehicles in this category.
2	30–49	Engineer and high-speed tractors with comparatively wide tracks and low contact pressures.
3	50–59	The tractors with average contact pressures, the tanks with comparatively low contact pressures and some trailed vehicles with very low contact pressures.
4	60–69	Most medium tanks, tractors with high contact pressures, and all wheel-drive trucks and trailed vehicles with low contact pressures.
5	70–79	Most all-wheel-drive trucks, a great number of trailed vehicles, and heavy tanks.
6	80–99	A great number of all-wheel-drive and rear-wheel-drive trucks, and trailed vehicles intended primarily for highway use.
7	100 or greater	Rear-wheel-drive vehicles and others that generally are not expected to operate off roads, especially in wet soils.

b. Graphic Portion of Figure 60. The legend for the shading of the three graphic portions of figure 60 is given at the bottom part of the figure. The white indicates excellent trafficability, the stippled good, the striped fair, and the black indicates poor to intrafficable soil. The topography and soil conditions are shown in the following three graphs in figure 60.

(1) High topography, (higher areas of the terrain) wet-season condition.
(2) Low topography, (low areas of the terrain) wet-season condition (saturated).
(3) Low topography, high-moisture condition (wet, but below saturation point).

178. Use of Figure 60

a. Mission. You have a rear-wheel drive truck with which to deliver supplies cross country to another area. You have the following information:

(1) Vehicle cone index: 85
(2) Topography: level high topography
(3) Type of soil: clayey sands (SC)

b. Question. Is this trip feasible from the standpoint of trafficability?

c. Procedure in Determining Trafficability.

(1) You know that the vehicle cone index of the truck is 85. Table 3 shows the vehicle to be in category 6. The vehicle cone index range (80–99) to the right of the category in table 3 and the written description under *vehicles* verify the category of your truck.
(2) Locate vehicle category 6 at the top of figure 60.
(3) Find the vehicle cone index 85. The number 85 must be interpolated on the vehicle cone index line in the space between 80 to 100.
(4) Find the soil type SC. This is given under *Soil type symbol* in the left column of the figure, and more conveniently on the graphic portion of the figure.
(5) From the 85 (interpolated) on the vehicle cone index, move downward on the high topography, wet-season condition graphic rectangle to the area marked SC. This area is stippled. Your legend at the bottom of figure shows that the trafficability for your vehicle is *good* in this area. Therefore, the trip is feasible from the standpoint of trafficability. The marking around the soil type area on the figure indicates that the trafficability interpretation on the chart has good reliability, as you may note in the legend. (Good reliability, based on analysis of data.)

d. Trafficability for Same Truck and Soil Type on Low Topography, Wet-Season Condition. From the 85 (interpolated) on the vehicle cone index, move downward into the *low topography, wet-season condition* graphic rectangle to soil type SC. Note that the trafficability is *good*, as indicated by the stippling. Reliability of this trafficability interpretation is fair, based on judgment.

e. Trafficability for the Same Truck and

Same Soil Type on Low Topography, High Moisture Condition. From the 85 (interpolated) on the vehicle cone index, move downward into the *low topography, high-moisture condition* graphic rectangle to soil type SC. Note that the trafficability is only *fair*. Had the vehicle cone index been a few points higher, the trafficability would have been *poor*. The black on this graphic chart indicates poor trafficability and is a warning to "stay off."

APPENDIX A

REFERENCES

1. Field Manuals

FM 3–10	Employment of Chemical and Biological Agents.
FM 3–12	Operational Aspects of Radiological Defense.
FM 5–15	Field Fortifications.
FM 5–20	Camouflage, Basic Principles and Field Camouflage.
FM 5–29	Passage of Mass Obstacles.
FM 5–30	Engineer Intelligence.
FM 5–35	Engineer's Reference and Logistical Data.
FM 5–36	Route Reconnaissance and Classification.
FM 17–36	Divisional Armored and Air Cavalry Units.
FM 21–40	Small Unit Procedures in Chemical, Biological and Radiological (CBR) Operations.
FM 30–5	Combat Intelligence, C–1.
(C)FM 30–10A	Special Applications of Terrain Intelligence (U).
(C)FM 30–15	Intelligence Interrogations (U).
FM 30–16	Technical Intelligence.
FM 31–10	Barriers and Denial Operations.
FM 31–25	Desert Operations.
FM 31–30	Jungle Training and Operations.
FM 31–50	Combat in Fortified and Built-Up Areas.
FM 31–60	River-Crossing Operations.
FM 31–70	Basic Cold Weather Manual.
FM 31–71	Northern Operations.
FM 31–72	Mountain Operations.
FM 55–8	Transportation Intelligence.
FM 57–10	Army Forces in Joint Airborne Operations.
FM 57–35	Airmobile Operations.
FM 60–30	Embarkation and Loading—Amphibious.
FM 100–5	Field Service Regulation—Operations, C–1.
FM 100–15	Field Service Regulations—Larger Units.
FM 101–5	Staff Officers' Field Manual—Staff Organization and Procedure.
FM 101–10–1	Staff Officers' Field Manual—Organization, Technical, and Logistical Data.

2. Technical Manuals

TM 3–240	Field Behavior of Chemical, Biological and Radiological Agents.
TM 5–248	Foreign Maps.
TM 5–249	Terrain Models and Relief Map Making.
TM 5–297	Well Drilling Operations.
TM 5–312	Military Fixed Bridges.
TM 5–330	Planning, Site Selection and Design of Roads, Airfields and Heliports in the Theater of Operations.

TM 5–332	Pits and Quarries.
TM 5–343	Military Petroleum Pipeline Systems.
TM 5–530	Materials Testing.
TM 5–541	Control of Soils in Military Construction.
TM 5–545	Geology.
TM 5–700	Field Water Supply.
TM 30–245	Photographic Interpretation Handbook.
TM 30–246	Tactical Interpretation of Air Photos.

3. Army Regulations

AR 117–5	Military Mapping and Geodesy.
AR 320–50	Authorized Abbreviations and Brevity Codes.

APPENDIX B

OUTLINE FOR TERRAIN STUDIES

1. Purpose and Limiting Considerations

State the purpose and limiting considerations under which the study is being prepared. This statement should include the scope of the study in area, time, and subject matter, and any information on the tactical situation, mission, or method of operations that is pertinent to the study.

2. General Description of the Terrain

a. Synopsis. State briefly the impact of the terrain on military operations.

b. Climatic Conditions. Describe predicted meteorological conditions for the period, based on climatic data. Present climatic data graphically whenever possible. The requirements of the study will determine the exact information presented and the manner of presentation.

(1) *Temperature.* Climatic data—give frequency of occurrence of temperatures during period.

(2) *Precipitation.* Climatic data—state frequency of occurrence of precipitation by type and amount.

(3) *Winds.* Climatic data—give frequency of occurrence of winds of certain velocities and direction. Use wind rose.

(4) *Visibility.* Present graphically data on times of sunrise, sunset, twilight, moonrise, and moonset. Describe effect of fogs, mist, haze, and other influences on visibility. State expected visibility by distance when applicable.

(5) *Cloudiness.* Describe when applicable and separate from precipitation and visibility. Climatic data—give data of frequency of occurrence and time of occurrence of various cloud conditions.

(6) *Humidity.* Describe only when significant. Describe effect when combined with other weather elements, such as oppressive heat or wind chill.

(7) *Electrical disturbances.* Describe only when significant.

c. Topography. If pertinent, describe the following characteristics by written or graphic means. Recommend the use of a topographic map overprint to emphasize particular characteristics.

(1) *Relief and drainage systems.* Use ridge and stream lining, contour emphasis, hilltopping, or relief shading to outline the ridge and valley systems. Use numbers, words, or standard symbols to indicate critical relief or drainage conditions.

(2) *Vegetation.* Indicate location, type, and size of trees, density of planting, existence of undergrowth, and the location, type, and density of other significant vegetation.

(3) *Surface materials.* Indicate the type and distribution of soils, subsoils, and bare rock in the area. Indicate their trafficability under various weather conditions.

(4) *Manmade features.* Describe fully the significant manmade features. Include roads, railroads, bridges, tunnels, towns, important buildings, fortifications, or airfields when pertinent.

(5) *Special features.* Describe significant special features such as earthquake zones or active volcanoes.

d. Coastal Hydrography. Describe when applicable. Use graphic means whenever possible.

(1) *Sea approaches.* Describe nature of approaches, bottom conditions, ob-

stacles, gradients, and coastal structures. Use landing-area map to present information graphically.

(2) *Beaches.* Describe dimensions, trafficability, and beach exits. Use land-area map to present information graphically.

(3) *Tides and currents.* Describe expected time of occurrence and stage of tides. Present graphically. Describe currents by direction, velocity and duration.

(4) *Sea and surf.* Describe height of sea. Describe type of surf, width of surf band, height of surf, and expected duration.

3. Military Aspects of the Terrain

From an analysis of the factors of climate, topography, and coastal hydrography, determine the following military aspects and describe them by written or graphic means. Use of an overlay to the basic topographic map is recommended.

a. Tactical Aspects of the Terrain. The following aspects are those basic to all tactical operations.

(1) *Observation.* Determine the effect of the terrain factors on observation from the ground, from the air, and by means of electric or sonic devices when applicable.

(2) *Fields of fire.* Determine the effect of the terrain factors on the ability of flat- and high-trajectory weapons to deliver projectiles to a target. Consider nuclear weapons when applicable.

(3) *Concealment.* Determine the capability of the terrain to provide concealment for men, equipment, and installations. Consider the effect of terrain on concealment by artificial means.

(4) *Cover.* Determine the capability of the terrain to provide cover for men, equipment, and installations. Consider the problem of cover from flat-trajectory, high-trajectory, and nuclear weapons when applicable.

(5) *Obstacles.* Determine the capability of the terrain to delay the advance of military forces or impede military operations. Consider both natural and manmade obstacles.

(6) *Movement.* From an analysis of soils trafficability, natural and manmade obstacles, and existing routes of movement, determine the ability of troops and equipment to move through an area. Use standard color code to describe movement conditions. Use specific terms of movement whenever possible; i.e.—vehicular, cross-country, and foot.

(7) *Key terrain features.* From an analysis of the terrain and of friendly and enemy methods of operations, indicate those terrain features which appear to be critical, such as a dominant height, a highway, a communication center, or an airfield.

(8) *Avenues of approach.* From an analysis of all terrain factors affecting capabilities to move men and materiel, determine the avenues of approach to the objective. Consider existing routes of movement, possibilities of cross-country movement, and amphibious or airborne or airmobile operations when applicable.

b. Engineering Aspects of the Terrain. Determination of the following military aspects is essential to planning the engineer phase of operations. Include these items in written or graphic form as overprints or overlays.

(1) *Construction sites.* From an analysis of surface material and other terrain factors, determine areas suitable for construction of roads, airfields, buildings, underground installations, surface defensive installations, or others.

(2) *Construction materials.* From an analysis of surface materials and other terrain factors, determine the probable location of rock, gravel, sand, or other natural construction material.

(3) *Water supply.* From an analysis of the drainage system and subsurface formations, determine the probable location of potable water and water suitable for construction use.

4. Maps and Charts (as appropriate)

a. Topographic.

b. Trafficability.

c. Landing (where applicable).

d. Special maps (when needed).

(1) *Geological.*
(2) *Soils.*
(3) *Hydrographic charts.*
(4) *Town plans.*
(5) *Road.*
(6) *Joint operations graphic.*

APPENDIX C

SAMPLE TERRAIN STUDY

Headquarters 15th Army
Western Germany
January 1945

1. PURPOSE AND LIMITING CONSIDERATIONS

a. Purpose. This terrain study considers the area to the south and east of COLOGNE, Germany, for February and March. General boundaries for the zone are the towns of JULICH on the ROER RIVER (3145) and ZULPICH (3418), and the RHINE RIVER north and south of COLOGNE as shown on inclosure 1 (fig. 61). Elements of Fifteenth Army, consisting of armored and infantry units, are located west of the ROER RIVER and presumably will operate in the area with the general mission of advancing northeastward to the RHINE RIVER.

b. Limiting Consideration. Information presented is based on data obtained from maps, intelligence documents, climatic study, and interrogation. Ground reconnaissance has not been made, nor have the effects of bombing been considered.

2. GENERAL DESCRIPTION OF THE TERRAIN

a. Synopsis. The area during this period of the year provides favorable conditions for military operations. It is highly populated mixed farm and industrial region. Construction sites and materials are available and the communication system is excellent. Movement across the RHINE RIVER is canalized at BONN and COLOGNE. Obstacles are the ROER and ERFT RIVERS and the VILLE RIDGE. Conditions influencing movement are sensitive to precipitation.

b. Climate Conditions. See inclosures 2, 3, and 4 (figs. 61-64).

(1) *Temperatures* will present problems to the effective operation of troops in the field. Inclosures 2, 3, and 4 give compiled temperature data.

(2) *Precipitation* in some form normally occurs every second day. Wet soils are common. Snowfalls ordinarily do not exceed 9 to 11 centimeters (6 or 7 inches). Ice, if present, is thin and will not support a man.

(3) *Wind* direction and velocity are given by the wind roses in inclosures 3 and 4. Winds from the east are usually accompanied by severe temperature drops.

(4) *Visibility* factors are listed in inclosures 2, 3, 4 and 5. Fog occurs rarely at this time of year, despite the high relative humidity. The high frequency of moderate to fresh winds favors the formation of low clouds rather than fog.

c. *Topography.*

(1) *Relief* is low and gently rolling with only two exceptions: the southwestern portion of the map (HOHE VENN) has steep wooded hills and highlands dissected by deep valleys; and a low hilly ridge, hereafter known as the VILLE RIDGE, exists between the ERFT RIVER and the RHINE RIVER. This area is discussed in detail on the back of the map and later in this study.

(2) *Drainage.* Streams cross the region generally from southeast to northwest. The ROER RIVER is approximately 80 feet wide, with no fords, and *can be flooded by release of water impounded in dams to the south.* The ERFT RIVER, or canal, meanders through several channels in its flood plain. These channels average 6 to 9 meters (20 to 30 feet) in width and .6 to 1.5 meters (2 to 5 feet) in depth. In many places, the river channels are flanked by marshy flats which are drained through numerous deep ditches.

(3) *Vegetation.* The area is largely devoted to agriculture and pasture but scattered forests do exist, and these are delineated on the map with notes as to density, type, and approximate boll size. Trails and unimproved roads allow restricted passage even through the dense forests. At this period of the year, the ground will be fallow or in low cover crop which will increase its trafficability. Trees are scattered throughout the numerous mine pits in the area.

(4) *Surface materials.* The region is generally covered by a loamy soil tending toward sandy soil in the south. In the VILLE RIDGE area, the original soils have been stripped off during mining, exposing sandstone and shale. Stream valleys are composed of fine grained silts in the northern reaches and change to sandy material upstream to the south. The soil immediately west of the RHINE RIVER is composed of sandy well-drained material. Surface materials are discussed further on the back of the movement map.

(5) *Manmade features.* The manmade features studied include roads, railways, bridges, airfields, towns, and strip mines.

(*a*) An excellent network of roads exists. Only the primary system, that with a route classification (FM 5–36) of X is shown on the map. In addition, secondary roads of general route classification connect many of the villages. Free egress from roads for cross-country movement is possible in most places.

(*b*) Rail communication, as shown on the map, is very good. As a a supplement to the standard-gage system, considerable narrow-gage lines exist, particularly in the VILLE RIDGE region. Marshalling yards are located at DUREN, BONN, and COLOGNE. The tunnel on the double-tracked route between DUREN and COLOGNE is a vulnerable point, but may be bypassed through alternate routes.

(*c*) The classification of bridges along the primary-road system is 65. Important bridges are indicated on the map with the classification noted if lower than the general class. Bridges on the secondary-road system have a general classification of 55.

(*d*) This area contains a large municipal airfield capable of handling heavy-cargo aircraft. These have been marked on the map. Also shown are three landing strips which can be used by assault aircraft. Sections of primary roads and autobahns may be utilized for light Army aircraft strips.

(*e*) Most urban areas are well built-up with stone and masonry buildings. Streets, except for boulevards or freeways, are narrow, and may permit only one-way traffic to trucks and tanks. All but the larger cities may be bypassed easily.

3. MILITARY ASPECTS OF THE TERRAIN

a. Tactical Aspects.

(1) *Observation.* Observation throughout the area is generally good, although there are small areas of defilade. The VILLE RIDGE affords excellent observation of the lowlands to the east and west. The HOHE VENN area provides good points for observation of the ROER RIVER valley. Small hills afford tactical observation in the plains section. Aerial observation will be excellent, except where woods obscure the ground.

(2) *Fields of fire.* The area provides generally good fields of fire for all weapons with two exceptions. The broken terrain of the VILLE RIDGE and the HOHE VENN limits fields of fire for flat-trajectory weapons within the ridge masses themselves. However, flat-trajectory weapons situated on these ridges can command their lowland approaches very effectively.

(3) *Concealment.* The mixed forested areas give good concealment from both air and ground observation. The broadleaf forests are bare of leaves during February and March and offer only limited concealment. Farming practices in this part of Germany are such that little concealment is possible in the winter cover crops, but the many farm buildings and small villages afford good concealment for small units.

(4) *Cover.* Principal cover is offered by the stone structures that make up the cities and farm communities. In the VILLE RIDGE area, some cover can be found in the mine tunnels.

(5) *Obstacles.*

(*a*) The ROER RIVER under normal conditions will offer only minor problems to an assault crossing. Opening or destroying the ROER DAM will flood the ROER VALLEY. If this is done, it will take at least a week for the ROER RIVER to recede, and 2 to 3 weeks for soils trafficability to return to normal.

(*b*) The ERFT VALLEY, with its drained swamps and many canals, will restrict movement to roads in most areas. The river channels themselves are not a serious obstacle to infantry; however, a long thaw, which is quite possible in March, or an unseasonal rain can make them unfordable to foot troops. There are also lignite pits west of Koln along Erft River.

(*c*) Wooded areas may restrict vehicular movement to narrow unimproved roads but are passable for infantry under normal conditions.

(*d*) The VILLE RIDGE forms an obstacle of major importance to vehicular and foot movement. It may be easily defended against

a superior force, affording the defender excellent observation and concealment in its woods and extensive mine workings.

(6) *Movement.* This is indicated on the movement map (fig. 61). The area as a whole provides very good movement during dry weather, and fair to doubtful movement during periods of heavy precipitation.

(7) *Key terrain features.*

(*a*) The VILLE RIDGE dominates the lowlands to the east and west of the hill mass. Routes crossing the VILLE RIDGE are restricted to the roads because of the extensive pits, quarries, and spoil heaps left by coal-mining operations.

(*b*) The HOHE VENN highlands southwest of DUREN overlook the adjacent ROER RIVER valley. In this region heavy forests and steep slopes restrict vehicular traffic to the roads.

(8) *Avenues of approach.* The main highways from the ROER RIVER toward COLOGNE offer good avenues af approach from the southwest, and represent the bet routes for breaching the VILLE RIDGE. The *best* avenues of approach would be to the north of JULICH-COLOGNE highway where the VILLE RIDGE may be flanked and cut off. The secondary road and rail net is adequate for support of an armored attack. The VILLE RIDGE may be flanked from the south in the vicinity of BONN, but here armored operations will be somewhat restricted and canalized by dense forests, and by the constriction of the corridor between the VILLE RIDGE and the RHINE RIVER.

b. Engineering Aspects of the Terrain.

(1) *Construction sites.* With the exception of the mining dumps, the southwestern highlands, and the river flood plains, the area is well suited for the construction of roads, airfields, cantonments, depots, and other military surface structures. The land is level and open, the communication net is excellent, and the soil has good stability and bearing capacity. The HOHE VENN highland is better suited for underground facilities than the plains area. Solid sandstone layers are useful as floors and roofs here, and ground water will not be as troublesome as in the flatlands.

(2) *Construction materials.*

(*a*) *Natural materials.* Quarries and gravel banks are available for stone and aggregate at many places. The terraces along the RHINE and ROER RIVERS are good sources of gravel and sand, while sandstone suitable for construction purposes can be quarried west of ZULPICH. Broken rock consisting of sandstone, shale, and soil is piled in the VILLE RIDGE dumps, and west of DUREN. Forests supply adequate quantities of standing timber to cover any foreseeable needs. Small local sawmills may be useful in cutting the timber for use.

(*b*) *Manufactured materials.* The heavy industrial buildings in the VILLE RIDGE and COLOGNE areas are good sources of construction steel, lumber, and similar materials needed by engineers. In addition, a large network of mine railroads exists throughout the pits and may be utilized for material.

(3) *Water supply.* An adequate field water supply may be obtained from the streams and wells of the area. Civilian water supply on farms is obtained from wells, and in cities through municipal distribution plants and systems which draw water from the major rivers. Emergency water supplies may be drawn from these sources.

5 Inclosures:

Inclosure 1. Movement map of Cologne area (fig. 61).
Inclosure 2. Climate conditions Cologne, Germany, for February and March.
Inclosure 3. Climatic data for Cologne area for February (fig. 62).
Inclosure 4. Climatic data for Cologne area for March (fig. 63).
Inclosure 5. Ephemeris for Cologne area for February and March (fig. 64).

Figure 61. Movement map of Cologne area.

Figure 61—Reverse.

(Located in back of manual)

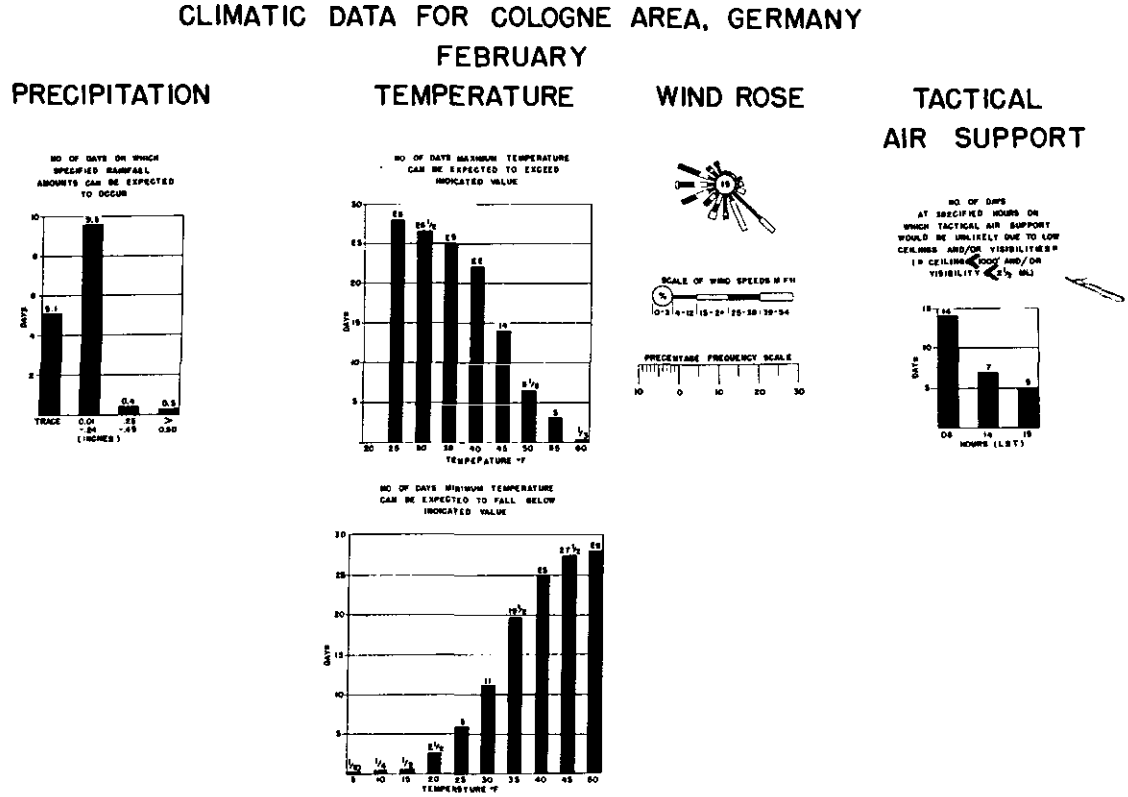


Figure 62. Climatic data for Cologne area for February (Inclosure 3 to app D).

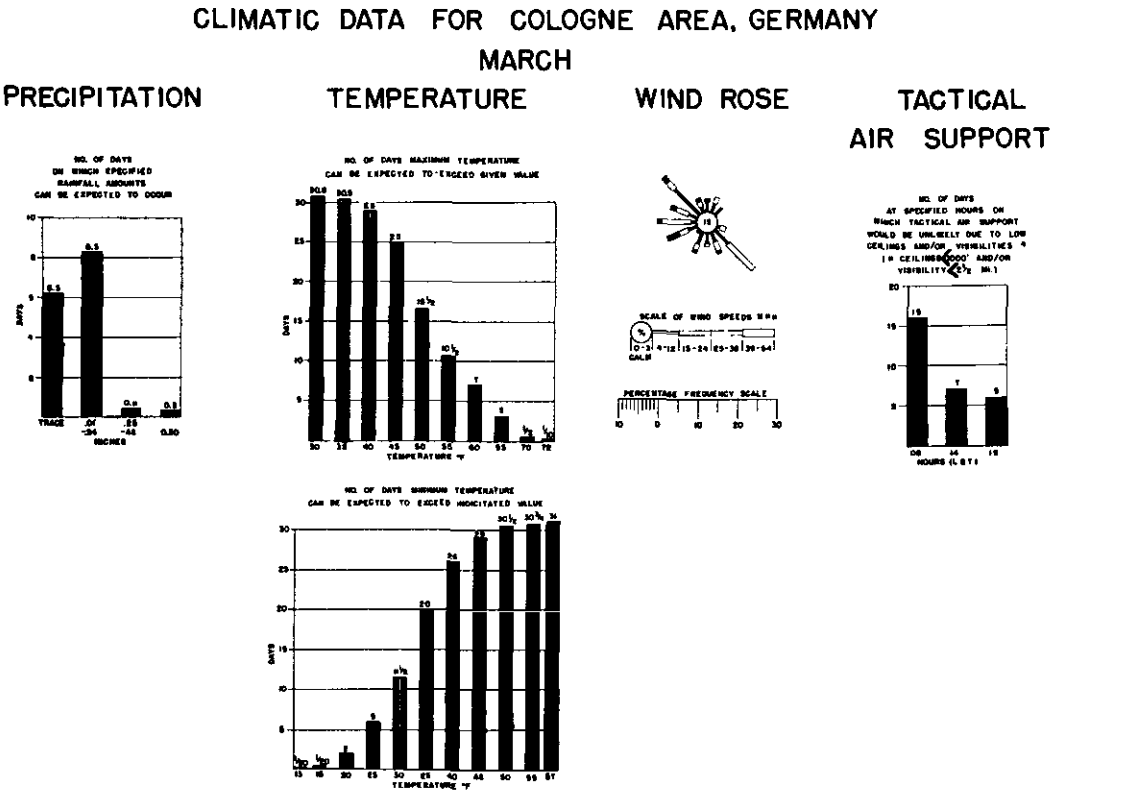


Figure 63. Climatic data for Cologne area for March (Inclosure 4 to app D).

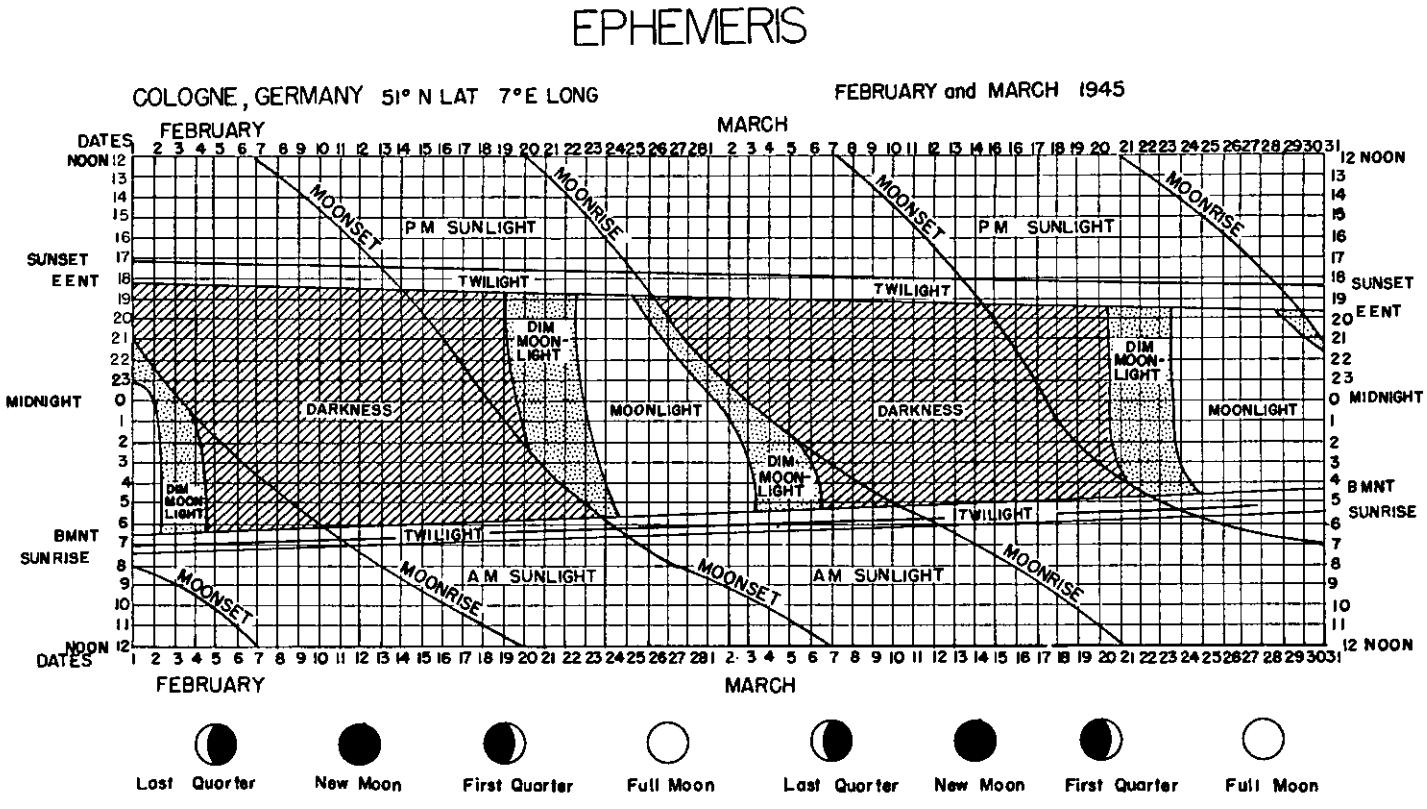


Figure 64. Ephemeris for Cologne for February and March (Inclosure 5 to app D).

Inclosure 2. Climatic Conditions, Cologne, Germany, for February and March

	Feb	Mar
Temperature (°F.):		
Mean maximum	43	49
Mean minimum	33	37
Absolute maximum	66	72
Absolute minimum	0	13
Number of days with:		
Minimum—32°F	10	6
Maximum—32°F	2	0.4
Precipitation (CM):		
Mean	4.09	4.39
Maximum	11.88	10.31
Minimum	0.4	.7
Maximum in 24 hours	3.15	2.06
Mean number of days with:		
Snowfall 0.01CM	6.4	5.9
Snow on ground	5.3	2.0
Fog	1.2	1.4
Wet soil	14.2	13.2
Clear skies	3.2	3.1
Partly cloudy skies	14.7	19.1
Cloudy skies	10.3	8.8
Mean relative humidity (%):		
0700 LST	84	82.
1400 LST	74	67.
1900 LST	82	76

APPENDIX D

SAMPLE CLIMATIC STUDY

General

This study is divided into four parts, each having a different operational aspect: amphibious, airborne, airmobile, and overland in two differing climatic regions. The studies and accompanying data do not refer to any exact geographic locations, but are offered only as a guide for format and content.

a. Information Sources. Source material for such studies is usually drawn from climatic summaries on file at the Climatic Center, Headquarters Air Weather Service, from the National Intelligence Survey (NIS) sources, and from weather summaries on file at the U.S. Weather Bureau or Congressional Libraries. In the field, information of a climatic nature may be obtained from local Air Weather Service detachments or a national meteorological service office. The climatic study is designed to provide a first estimate of weather factors affecting military operations and should not be regarded as an operational forecast which normally is supplied by other Air Weather Service detachments.

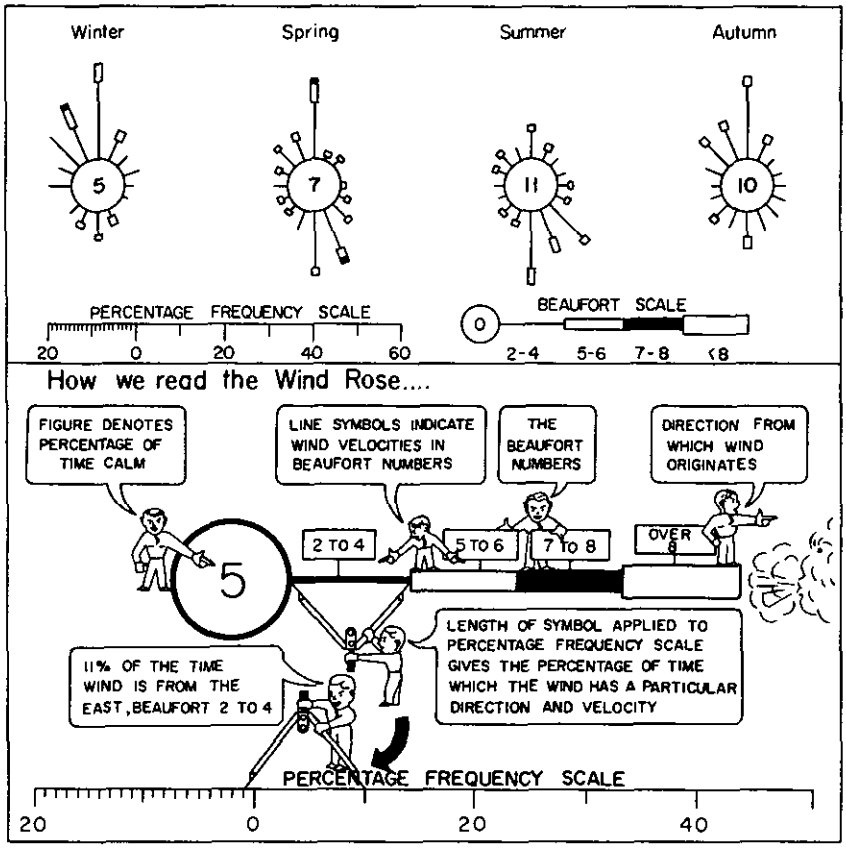


Figure 65. How to read a wind rose.

b. Wind Rose. The agency requesting climatic data from Air Weather Service should specify whether the wind speed data is desired in kilometers, miles, or knots per hour. Wind speed data is shown in compact form by means of a wind rose. The method used to read a wind rose is shown in figure 65. The wind rose makes use of the Beaufort scale, which is a wind scale in which the force of the wind is indicated by numbers with corresponding descriptive terms. These terms are commonly used by the U.S. Weather Bureau (table 1, chap. 4).

Part I

Climatic Factors Affecting an Overland Operation in the Region Surrounding OBJECTIVE ONE During May

In terms of general climate, OBJECTIVE ONE area has a maritime-type climate, characterized by cool, humid winters and mild, comparatively dry summers. The month of May represents a portion of the transition period between these two characteristic seasons.

In the absence of meteorological information for the exact location involved, combined data from adjacent areas, both north and south, were considered to be representative of the climate of OBJECTIVE ONE area and are presented as appendix material in tabular (table D–1) and graphical (fig. 66) form.

Table D–1. Overland Operation OBJECTIVE ONE—May

Temperature (°F.):	
Mean Maximum	62
Mean	50
Mean minimum	38
Recorded Extremes	77 to 31
Mean Number of Days with:	
Fog	1
Thunderstorms	0
Rain	8

Temperature during May is usually conducive to moderate to strenuous activity. Normally, temperature averages approximately 50° F., with a moderate diurnal and monthly range. Minimum temperatures, especially during the first portion of the month, in valley areas or close to the ground surface are frequently in the mid 30's during early morning hours.

Rainfall is light, averaging 5 to 6 centimeters (2 to 2½ inches) for the month. This amount, well distributed in time (the maximum reported for any 24-hour period is 2.5 centimeters (1½ inches)), should not create problems associated with soil moisture and would be sufficient to minimize dust conditions. Snow accumulations on the mountains and passes east of the area melt at this time and provide a source of fresh water for the local streams. Flooding of these streams is unusual.

Relative Humidity is high throughout the day, averaging 80 percent to 85 percent. Diurnally, the variation is relatively small, 10 percent to 20 percent. Although relative humidities average quite high, the incidence of fog and other forms of restricted visibilities is quite low; about 5 percent of the time the visibility is less than 4 kilometers (2½ miles).

Cloud cover and visibilities are well suited for tactical air support.*

Winds are primarily from a westerly direction, southwest through northwest, with an average speed of 7 to 10 knots. Approximately 25 percent of the time the winds are less than 3 knots.

* Minimum ceiling and visibility requirements depend upon the type of support and the equipment involved, and upon the type of terrain over which this support must operate.

CLIMATIC DATA FOR OBJECTIVE ONE

MAY

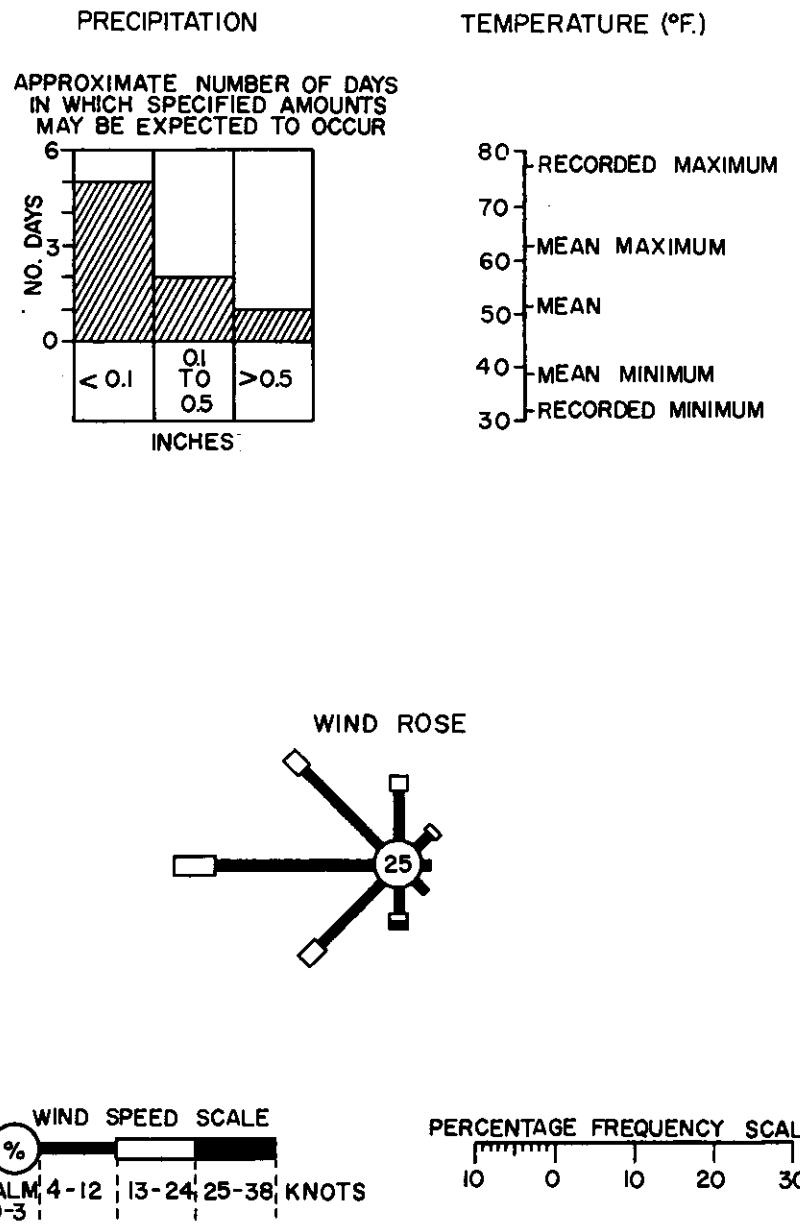


Figure 66. Climatic data for OBJECTIVE ONE—May.

Part II

Climatic Factors Affecting an Amphibious Landing on OBJECTIVE TWO During May or June

Complete meteorological observations on the island were made only during a brief period during World War II. Plantation records for longer periods of record have been used in arriving at precipitation estimates. Climatic data are presented as appendix material (table D–2 and figs. 67 and 68).

Table D–2. Amphibious Operations OBJECTIVE TWO Island—May and June

	May	June
Temperature (°F.):		
Mean Maximum	88	90
Mean	81	82
Mean Minimum	75	76
Recorded Extremes	93 to 73	95 to 74
Mean Number of Days with:		
Thunderstorms	8	6
Precipitation	17	12
1.3 centimeters— 0.5 inch	12	9
4.8 centimeters— 0.6 to 1.9 inches	4	2
5 centimeters— 2.0 inches	1	1

Climatically, OBJECTIVE TWO Island has all the typical tropical characteristics with heavy, shower-type rainfall and a small diurnal and seasonal temperature range. Since the island is affected by the monsoon wind, the May-June period is one of transition, during which winds are normally light and variable.

Temperature conditions are not conducive to human activity, and the daily range of temperatures is insufficient to alleviate this human discomfort at night. The mean temperature is approximately 80° F., with a maximum daily range of about 20 Fahrenheit degrees.

Humidity is constantly high and coupled with the warm temperatures creates problems of material storage and supply, in addition to adding to human discomfort. Mean relative humidity is approximately 80 percent, with only slight variation diurnally.

Visibility is seldom restricted by weather factors except during brief periods of heavy shower activity; however, dense vegetation limits ground visibility severely unless some form of clearing has taken place.

Precipitation is of the brief, heavy shower-type that usually occurs during the afternoon on an average of 1 out of 2 days. Thunderstorms are quite frequent, with an average of 8 storms per month. Although total precipitation is highly variable from year to year, it is more than adequate to keep soils moist, support heavy vegetation, and present vehicular transport problems. Maximum precipitation in 24 hours reported for the island during this period was 18 centimeters (7.2 inches) during May.

Winds are light and variable, except during heavy showers; however, during June the southeast monsoon is being established and southeast winds become more predominant. In the forested areas, winds are usually very light or calm, but along coastal strips they average about 5 knots. Typhoon winds are not considered a threat to operations this early in the season.

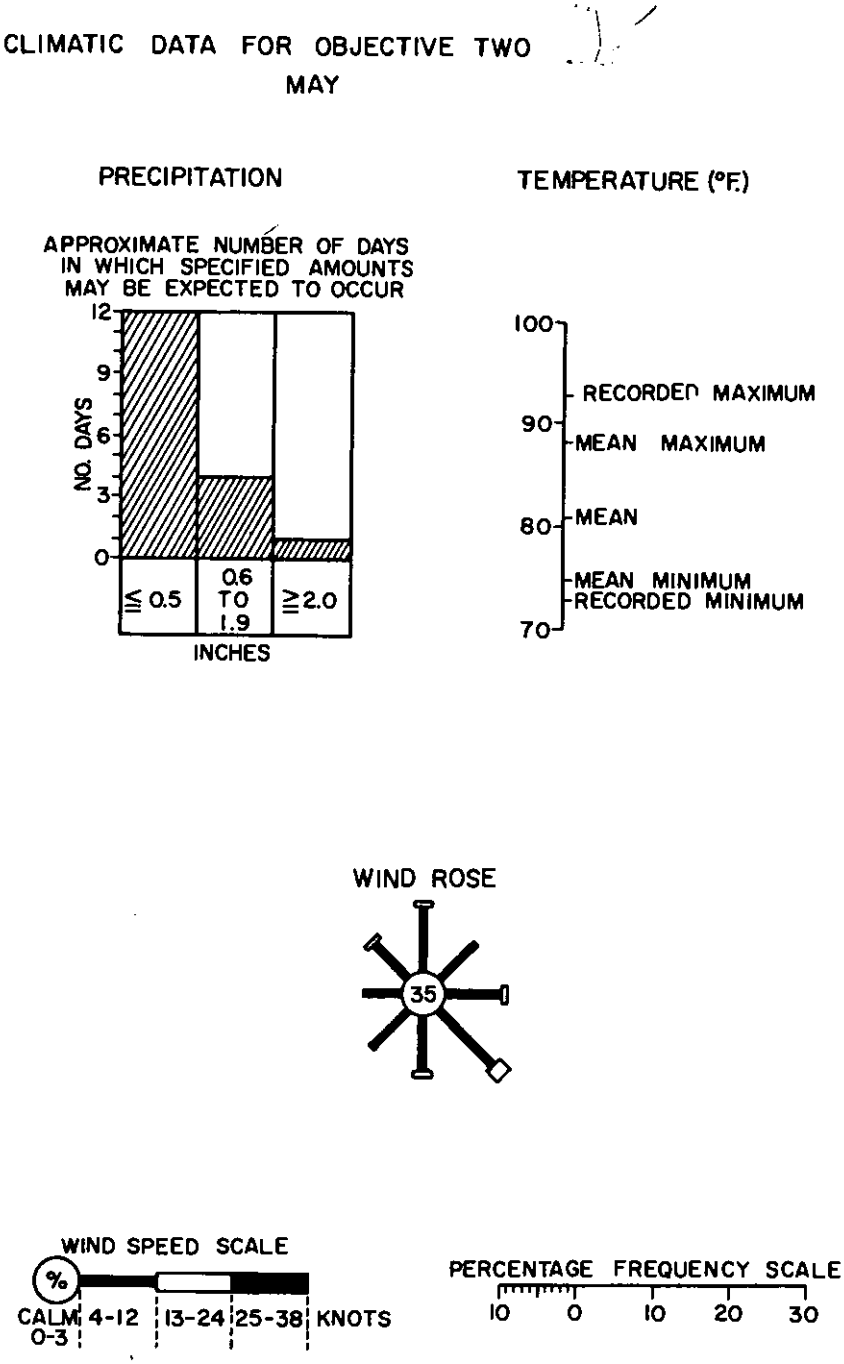


Figure 67. Climatic data for OBJECTIVE TWO—May.

Part III

Climatic Factors Affecting an Airborne-Airmobile Operation in the Vicinity of OBJECTIVE THREE During September

For the purposes of this report, it was assumed that paratroop operations would be carried out only with a ceiling value equal to or greater than 305 meters (1,000 feet), visibility equal to or greater than 4 kilometers (2½ miles), and wind speed less than 13 knots. On this basis, favorable weather occurs most frequently during the midafternoon. Unfavorable

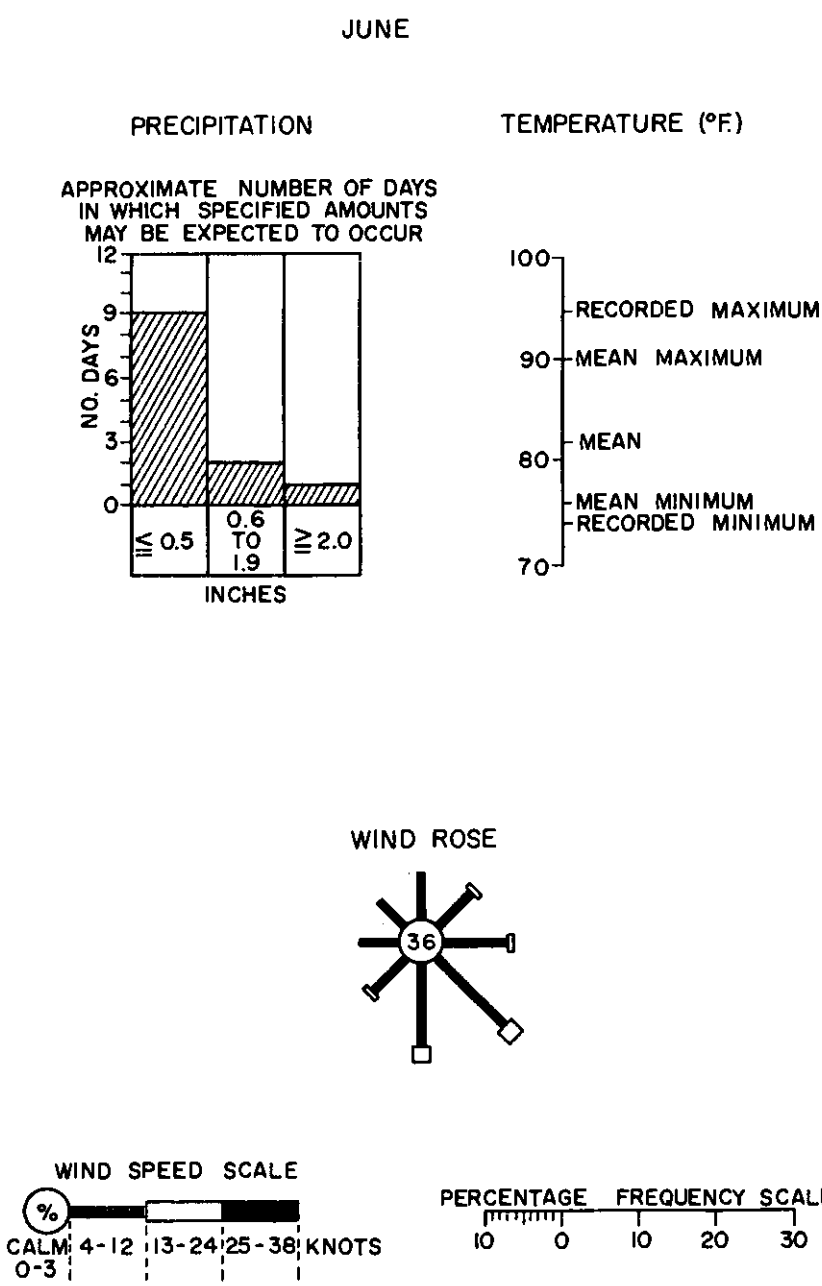


Figure 68. Climatic data for OBJECTIVE TWO—June.

conditions increase gradually until early morning hours when adverse weather occurs approximately 25 percent of the time. Tactical air support, depending upon the type needed and equipment utilized, should be able to operate 70 percent to 80 percent of the daylight hours (table D–3 and fig. 69) .

Table D–3. Airborne Operation OBJECTIVE THREE—September

	September
Temperature (°F.):	
Mean Maximum	67
Mean	58
Mean Minimum	50
Recorded Extremes	87 to 38
Mean Number of Days with:	
Thunderstorms	3
Precipitation	19
2.54 millimeters (0.1 inch)	9
2.54 to 12.70 millimeters (0.1 to 0.5 inch)	6
12.70 millimeters (0.5 inch)	4
Precentage Frequency, by Hour, of Weather Favorable for Paradrop Operations (Ceiling 305 meters (1,000 ft.)), Visibility 4 kilometers (2½ miles, Wind 13 ft.)	
0800 LST 74%	
1400 LST 96%	
1900 LST 91%	

Temperatures are not extreme during this period and should not present problems of human comfort. The extreme range of temperature is large, but normal temperatures are quite moderate with mean maximum of 67° F. and a mean minimum of 50° F.

Precipitation, in the form of drizzle, light rain, or showers, occurs on the average of 2 days out of 3, giving an average September rainfall amount of approximately 6.35 centimeters (2½ inches). Heavy rainfall is infrequent, but when it occurs, poorly drained areas become flooded and trafficability problems are intensified.

Fog restricts visibility to less than 800 meters (one-half mile) on 1 day of 10, most often during the early morning hours. During the afternoon and early evening the possibility of restricted vision caused by air pollutant is even less.

Winds are most frequently from the northwest (see wind rose), with about 10 percent of the observations showing wind speeds greater than 13 knots. Diurnal variations in wind strength or direction appear negligible in this particular area.

Part IV

Climatic Factors Affecting an Overland Operation in the Vicinity of OBJECTIVE FOUR During February

Climatically, the objective area has a marine climate, which implies mild, cloudy, and humid weather (table D–4 and fig. 70).

Table D–4. Overland Operation OBJECTIVE FOUR —February

	February
Temperature (°F.):	
Mean Maximum	45
Mean	38
Mean Minimum	32
Recorded Extremes	64 to 10
Mean Number of Days with:	
Precipitation	16
2.54 millimeters (0.1 inch)	8
2.54 to 12.70 millimeters (0.1 to 0.5 inch)	5
12.70 millimeters (0.5 inch)	3
Snowfall	5
Snow on ground	5
Mean Relative Humidity (%)	
0700 LST	85
1400 LST	71
1900 LST	80

Temperatures usually are not severe, as a result of the moderating effect of the water on the migratory air masses. However, alternate freezing and thawing of the normally water-soaked soil surface is common, creating problems of vehicular movement due to rapid deterioration of natural surfaces.

Precipitation in the form of rain, drizzle, and/or snow occurs on approximately one-half of the days during the month. Snowfall is usually small in amount, but is apt to be wet, heavy, and clinging; possibly resulting in destruction of overhead wires and some vegetation. Snow cover is usually shortlived, being destroyed by the frequent warmer rains. Soils are usually water soaked; only during exceptionally cold winters does the ground freeze to any depth.

Fog occurs on 4 to 5 days during the month and is usually quite dense, persistent, and widespread, restricting visibility to several hundred meters and precluding any tactical air support. Cloud cover is usually present, but

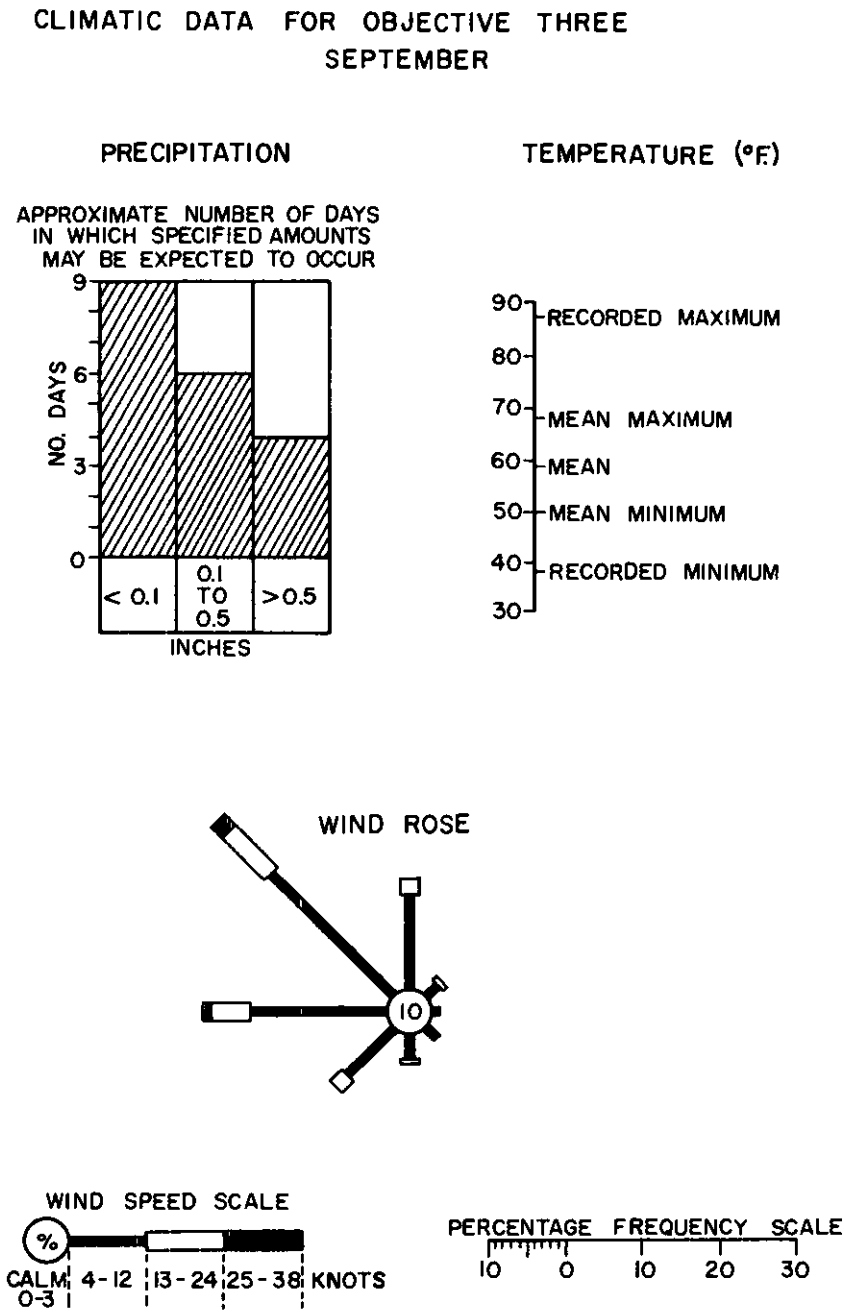


Figure 69. Climatic data Objective Three—September.

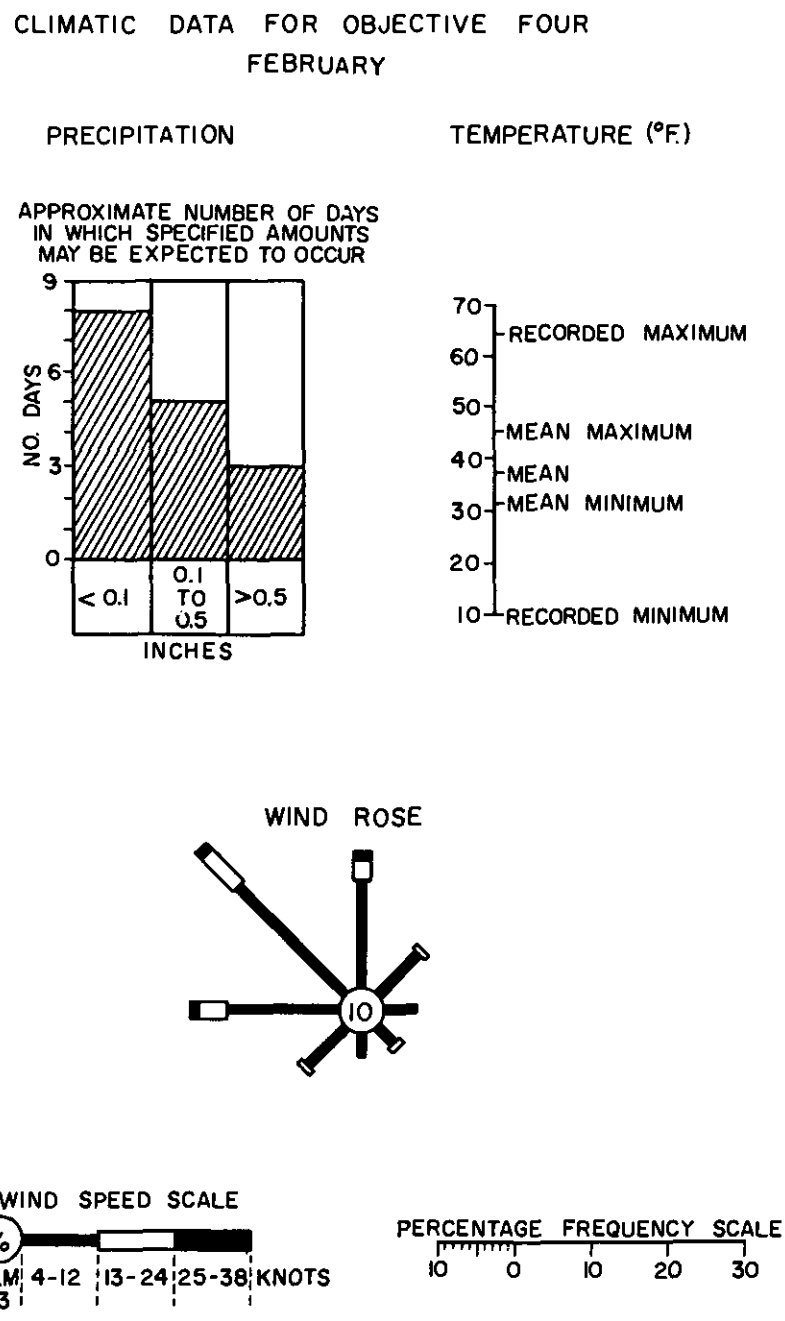


Figure 70. Climatic data for OBJECTIVE FOUR—February.

normally the effective ceiling is about 610 meters (2,000 feet).

Winds are predominately from a northwestern direction, light to moderate in force with infrequent gale-force winds associated with strong frontal passages.

APPENDIX E

NATURAL TERRAIN FEATURES

The natural terrain features shown in A, B, and C, figure 71 will serve as a guide to producers and users of terrain studies. A few of the terrain features identified on the figure may be known in some regions under different names because of local usage.

APPENDIX F

DEPARTMENT OF DEFENSE INTELLIGENCE INFORMATION REPORT FORMS 1396 AND 1396C

Department of Defense intelligence information will be reported on DD Form 1396 and DD Form 1396c. These forms are available through regular supply channels.

INDEX

	Paragraph	Page
Aerial photographs	173	143
Aerosols	36*f*	25
Agencies, intelligence	23	11
Air support	60*g*	62
Air temperature	25	13
Air Weather Service	30*a*, 34*e*	21, 24
Airborne operations	141	127
Airfields	113, 114	105
Airmobile operations	141	127
All weather route	95*b*	94
Alluvial plains	55	52
Altocumulus clouds	29*g*(2)	19
Altostratus clouds	29*g*(1)	19
Amphibious operations	140	126
Anaglyph	18*d*(2)	10
Antarctica	54*c*(2)	52
Arctic regions	50	40
Assault landing	70*f*	75
Atmospheric pressure	26	14
Atolls	73*d*	77
Avenues of approach	49*g*, 50*g*, 60*e*, 90*e*, 95*c*(1), 137, 162	40, 42, 62, 91, 94, 122, 138
Barrier reefs	73*c*	77
Barriers	136*c*	122
Beach profile	167*e*	141
Beaches	70, 71, 168*c*	73, 75, 141
Bearing capacity of soils	174*b*	143
Biological agents	48*d*(6), 49*i*	38, 40
Boulders	55*b*(4)	55
Bridges	97	96
Broadleaf forest	84*c*	85
Buildings	122, 125*b*	112, 116
Catchment basin	62*b*	64
Chain, mountain	57*d*	60
Chemical agents	48*d*(6), 49*i*	38, 40
Chief of engineers	8*c*	6
Chinook wind	27*d*	16
Cirrocumulus clouds	29*f*(3)	19
Cirrostratus clouds	29*f*(2)	19
Cirrus clouds	29*f*(1)	17
City areas	122*d*	112
Civilian oil pipelines	106*d*	101
Clay	76*e*	81
Climate, effects of	54*b*, 155, 170	52, 134, 142
Climate, examples:		
Continental	44*b*	33
Desert	42*b*	31
Dry	42	31
Humid	44*b*	33
Marine west coast	43*d*	32
Mediterranean	43*b*	31
Mesothermal	43	31
Microthermal	44	32
Middle latitude	42*d*	31
Polar	45	33
Savanna	41*b*	30
Subarctic	44*e*	33
Subtropical	43*c*	32
Tropical	41	30
Climate and terrain	40*b*	29
Climatic study:		
Preparing	47	35
Sample	App D	161
Cloud cover symbols	29	16
Cloudiness	38	26
Clouds	29, 38, 155*b*(6)	16, 26, 135
Coastal plains	53*d*, 55*e*(1), 140*d*	48, 57, 126
Coastal ridge	140*e*	126
Coast lines	74*a*	78
Collection agencies, intelligence	23	11
Collection effort, intelligence	13	7
Communication, lines	20*c*, 49*h*, 60*f*, 94, 123*e*	11, 40, 62, 93, 113
Communication maps	17*a*(3)	8
Compartments	138	123
Cone index, vehicle	174	143
Construction:		
Effects of vegetation	90*f*	91
In hills and mountains	60*i*	63
Materials	164, 165	139
Problems	55, 122*c*	52, 112
Continental climate	44*b*	33
Contour emphasis	156	135
Coral reefs	73	77
Cordillera	57*e*	60
Corridors	139	123
Cover and concealment	48*d*(3), 49*f*, 50*e*, 60*c*, 90*c*, 123*c*, 135, 160	37, 40, 42, 62, 90, 113, 121, 138
Crops, field	89*a*,	89
Cross-country movement	163	138
Cycle, intelligence	12	7
Cyclones, tropical	32*c*	22

	Paragraph	Page
Dams	119*b*	109
Deciduous trees	83*c*	84
Defense Intelligence Agency	8*a*	5
Delta plains	53*e*	48
Desert climates	42*b*	31
Desert drainage	63*g*	66
Deserts	48	35
Determining trafficability	178*c*	146
Dew point	28*c*	16
Dispatch route	95*c*(5)	94
Dissemination of intelligence	16	8
Distribution of rainfall	39	26
Divides, mountain	58*c*	61
Documents, enemy	21	11
Drainage	62, 156*b*	64, 135
Drift plains	53*h*(2)	49
Drop areas	141*c*	127
Drumlins	53*h*(2)	49
Dry climates	42	31
Dunes	71*b*, 140*f*	75, 126
Engineer:		
Intelligence functions	11	6
Intelligence Studies	20*b*	11
Terrain Detachment	153	133
Ephemeral streams	63*c*	66
Estimate, terrain	4*e*	4
Evaluation of railways	100	97
Evergreen trees	83*c*	84
Example of climatic study	App D	161
Example of terrain study	App C	153
Extreme climates	41, 42*b*, 45	30, 31, 33
Fair weather route	95*b*(3)	94
Fields of fire	48*d*(2), 49*e*(1), 50*d*(2), 60*b*(2), 90*b*(2), 134, 159*b*	37, 39, 42, 61, 90, 120, 138
Flood control	119*a*	109
Flood plains	53*f*	48
Foehn effect	27*d*	16
Fog	31	22
Foothills	58*d*	61
Forecasts, weather	33	22
Forests	84, 85, 86	85, 86, 87
Glaciers	66	67
Glacial plains	53*h*, 55*e*(4)	49, 58
Glory-hole mining	109*d*	103
Grasses	88	88
Gravel	76*b*	81
Gravity springs	67*c*(1)	70
Greenland, marginal features	54*c*(1)	52
Ground water	67, 145	69, 129
High-latitude forests	86	87
Hills	59, 145*d*	61, 130
Humidity	28, 37, 44*b*, 155*b*(5)	16, 26, 33, 135
Hydraulic structures	119	109
Hydrography	156*b*	135
Hydrologic circle	67*a*	69
Ice front	66*c*	68
Ice cap	46	34
Index, cone vehicle	174	143
Information requirements, terrain:		
Airborne	141*b*	127
Airfields	115	106
Airmobile	141*b*	127
Bridges	98	96
Buildings	126	116
Drainage	69	72
Hills and mountains	61	63
Hydraulic structures	121	111
Inland waterways	103	99
Landing areas	75	80
Mines	110	104
Non-urban areas	131	118
Petroleum and gas	108	102
Plains and plateaus	56	60
Quarries and pits	112	105
Railways	101	98
Roads	96	95
Rock	81	84
Soils	79	83
Urban areas	124	114
Utilities	128	117
Vegetation	91	91
Water supply	147	130
Water terminals	118	107
Inland waterways	102	98
Intelligence:		
Collection	13	7
Cycle	12–16	7, 8
Dissemination	7*a*, 16	5, 8
Officer	10	6
Processing	15	7
Reports	20	11
Strategic	6b	4
Weather	34	23
Intermittent streams	63*b*	64
Interrogation of prisoners	22	11
Jungles	49	38
Karst plains	53*k*, 55*c*(7)	50, 60
Key terrain	48*d*, 49*d*, 60*a*, 90*a*, 133, 158	37, 39, 61, 89, 120, 138
Lacustrine plains	53*i*, 55*e*(5)	50, 60
Lakes	64, 68*d*, 144*d*	66, 71, 129
Landforms	51*b*, 53	44, 45
Lateral route	95*c*(2)	94
Lines of communication	20*c*, 49*h*, 60*f*, 94, 123*e*	11, 40, 62, 93, 113
Locks	119*d*	110
Loess plains	53*i*, 55*e*(6)	50, 60
Low-latitude forests	84	85

	Paragraph	Page
Mangrove swamp	84*b*	85
Manmade terrain features	92	93
Maps	17, 172	8, 142
Marine west coast climate	43*d*	32
Marshes and swamps	65, 68*e*	66, 72
Maximum tractive effort	174*m*	144
Meandering river	53*f*	48
Mediterranean climate	43*b*	31
Mediterranean scrub	85*b*	86
Melt water	66*f*	68
Mesothermal climate	43	31
Microthermal climate	44	32
Middle-latitude climate	42*d*	31
Middle-latitude forests	85	86
Military aspects:		
Bridges	98	96
Buildings	126	116
Coastlines	74*a*	78
Drainage	69	72
Hills and mountains	60, 61	61, 63
Hydraulic structures	120, 121	111
Hydrology	68	71
Inland waterways	103	99
Jungles	49	38
Landing areas	75	80
Mines	109*e*	103
Nonurban areas	130, 131	118
Petroleum and gas	108	102
Plains and plateaus	55, 56	52, 60
Quarries and pits	112	105
Railways	101	98
Reefs	74*b*	79
Roads	96	95
Rock	81	84
Soils	78*a*, 79	82, 83
Terrain	52, 132	45, 120
Tunnels	80*c*	83
Urban areas	123, 124	113, 114
Utilities	128	117
Vegetation	90, 91	89, 91
Water supply	147	130
Water terminals	117, 118	107
Military pipelines	106*c*	101
Military use of railroads	99*f*	97
Mines	109	102
Mobility index	174*l*	143
Models, terrain	17	8
Monsoon	27*f*	16
Moss	84*c*	85
Mountains	57, 58, 140*g*	60, 61, 126
National Intelligence Survey	20*a*	11
Natural gas	104	100
Needleleaf forest	85*d*	87
Nimbostratus clouds	29*h*(2)	19
Nipa palms	84*b*	85
Nonurban areas	129	117
Nuclear weapons	37*c*, 78*h*	26, 83
Observation and fields of fire	48*d*(2), 49*e*(1), 50*d*(1), 55*c* 60*b*, 90*b*, 123*b*, 134, 159*a*	37, 39, 41, 57, 61, 90 113, 120, 138
Obstacles	48*d*(4), 50*f* 60*d*, 90*d*, 136, 161, 173*d*	37, 42, 62, 90, 121, 138, 143
Oil, military importance	107	101
Oil distribution	106	100
Oil fields	105	100
Oil pipelines	106*b*	100
Oil tanks	106*e*	101
Open-pit mines	109*c*	103
Orchards	89*b*	89
Passes, mountain	58*e*	61
Peaks	57*b*	60
Perennial stream	63*a*	64
Petroleum and natural gas	104	100
Photographs	18	9
Pictomaps	17*a*(5)	9
Piedmont plains	53*g*	49
Pipelines, military oil	106	100
Pits	111*b*	104
Placer mines	109*b*	103
Plains	53, 55, 145*b*	45, 52, 129
Planning	132	120
Plants	82	84
Plateaus	54, 55	50, 52
Polar climate	45	33
Polders	119*e*	110
Ports	116	107
Prairie	88*c*	89
Precipitation	30, 155*b*(3)	21, 135
Pressure, atmospheric	26	14
Production of terrain intelligence	12	7
Quarries	111*a*	104
Railways	99, 100	96, 97
Rain, tropical	84*a*	85
Rain forest	41*a*	30
Rainfall	30, 39*a*	21, 26
Ranges, mountain	57*c*	60
Rating cone index	174*g*	143
Reconnaissance reports	20*f*	11
Reefs	73, 74	77, 78
Relief	51*c*, 156*a*	44, 135
Remolding index	174*f*	143
Remote-sensor imagery	18	9
Reports, intelligence	20	11
Reserved route	95*c*(3)	94
Reservoirs	119*c*	109
Rice fields	89*c*	89
Ridge and stream lining	156	135
Ridge approach	139*b*	126
Rivers	63, 68	64, 71
Rock	80	83

	Paragraph	Page
Routes and roads	95	93
Sample terrain study	App. C	153
Sand	76*c*	81
Sand dunes	48*b*	36
Savanna	88*b*	89
Savanna climate	41*b*	30
Screening smokes	48*d*(7)	38
Scrub, Mediterranean	85*b*	86
Sea approaches	168	141
Seeps and springs	67*c*, 144*b*	70, 129
Shrubs	87	88
Silt	76*d*	81
Slipperiness	174*k*, 176*b*	144, 145
Soils	76, 78, 169, 173*b*, 174, 175	80, 82, 142, 143, 145
Soil maps	17*a*(1), 77, 172	8, 81, 142
Soil trafficability table	175	145
Soil-type symbols (table 2)	175*a*	145
Special operations	140	126
Springs, artesian	67*c*(2)	70
Springs, gravity	67*c*(1)	70
Springs and seeps	67*c*, 144*b*	70, 129
Steppes	42*c* 88*d*	31, 89
Stereopairs	18*d*(2)	10
Stickiness, soil	174*j*, 176*a*	144, 145
Storms	32	22
Stratocumulus clouds	29*h*(3)	19
Stratus clouds	29*h*(1)	19
Streams	63, 144*c*	64, 129
Studies:		
Climatic	App D	161
Terrain	App C	153
Subarctic regions	44*e*, 50	33, 40
Subtropical climate	43*c*	32
Supervised route	95*c*(4)	94
Surf	168*e*	141
Swamp, tropical	84*b*	85
Swamps and marshes	65, 68*e*	66, 72
Temperature	35, 155*b*(2)	24, 134
Terrain	4, 6, 52, 114, 132, 136*d*	4, 45, 105, 120, 122
Terrain models	17	8
Terrain studies	148, App. C	132, 153
Thunderstorms	32*a*	22
Tides	168*f*	141
Topography	51, 72, 122*b* 141*c*(4), 171, 173*a*	44, 75, 112, 127, 142, 143
Tornadoes	32*b*	22
Traction capacity of soils	174*d*	143
Trafficability	169	142
Trees	83	84
Tropical climate	41	30
Tropical cyclones	32*c*	22
Tropical grasslands	88*b*	89
Tropical rainy climates	41	30
Tropical regions	49	38
Tropical swamp	84*b*	85
Tundra	46	34
Tunnels	80*c*	83
Underground installations	80*b*	83
Underwater topography	72	75
Urban areas	122	112
Utilities	127	117
Valley approach	139*a*	123
Valley wind	27*c*	16
Valleys, kinds	58*b*	61
Vectographs	18*d*(2)	10
Vegetation	82, 89, 156*c* 173	84, 89, 136, 143
Vehicle categories (table 3)		146
Vehicle cone index	174*i*, 177*a*	144, 145
Velocity, wind (table 1)		15
Visibility	155*b*(1)	134
Volcanic lava	53*d*	48
Water, sources and supply	142, 143, 146, 166	127, 128, 130, 139
Water table	67*b*	69
Water terminals	116	107
Waterways, inland	102	98
Weather	24, 170	13, 142
Weather forecasts	33, 34*f*	22, 24
Weather intelligence	34	23
Weather requests	34*d*	24
Wells	145*e*	130
Wind velocity (table 1)		15
Winds	27, 36, 155*b*(4)	14, 25 135
World rainfall	30	21
World temperature	40	28

By Order of the Secretary of the Army:

HAROLD K. JOHNSON,
General, United States Army,
Chief of Staff.

Official:

KENNETH G. WICKHAM,
Major General, United States Army,
The Adjutant General.

Distribution:

To be distributed in accordance with DA Form 12–11 requirements for terrain intelligence.

☆ U.S. GOVERNMENT PRINTING OFFICE: 1967–0 273–544

MOVEMENT MAP COLOGNE AREA

This sample movement map is not to scale

Sample Movement Color Key

- Good movement under all conditions.
- Good movement in dry weather, fair during wet weather.
- air movement under ll conditions.
- Fair movement in dry weather; poor to doubtful in wet weather
- Poor movement under all conditions.
- Extremely poor movement under all conditions.
- Green hachures indicate passable routes through areas of poor movement.
- Red hachures indicate impracticable obstacles.

Specific Movement Key

- Mountains and steep hills generally wooded. Travel restricted to the few existing roads. — 1
- Gently sloping and level land; slopes less than 10% sandy or gravelly soil; good movement in all but worst weather. — 2A
- Gently sloping and level land; slopes less than 10% loamy or clayey soil; good movement in dry weather, hampered by mud in wet weather. — 2B
- Gently sloping and level land, urban area. Traffic restricted to streets. — 2C
- Wooded areas. Density, type and thickness of trees given on map and these factors determine practicability of passage. — 3
- Drained swamps and flood plains; many canals and ditches. Disruption of canal drainage causes flooding. Generally untrafficable. — 4A
- Mine pits and spoil heaps. Untrafficable because of steep slopes and holes. — 4B
- Swamps. Impracticable. — 5

LEGEND

- Woods
- Railway, multiple track (with tunnel)
- Railway, single track
- Landing strip, light aircraft
- Highway, autobahn, route class 40 ft. × 65 T
- Highway, primary, route class 20 ft. × 55 T
- Highway, state, route class 20 ft. × 55 T
- Bridge, railroad or highway
- Stream, canal, and river
- Airfield, large municipal
- Escarpment and mining pits

GN

X° or Z mils

Y° or M mils

Approx. mean declination 19__ for Center of sheet

ANNUAL MAGNETIC CHANGE __° (E or W)

Scale 1:100,000

1 0 1 2 3 4 5 6 7 Miles

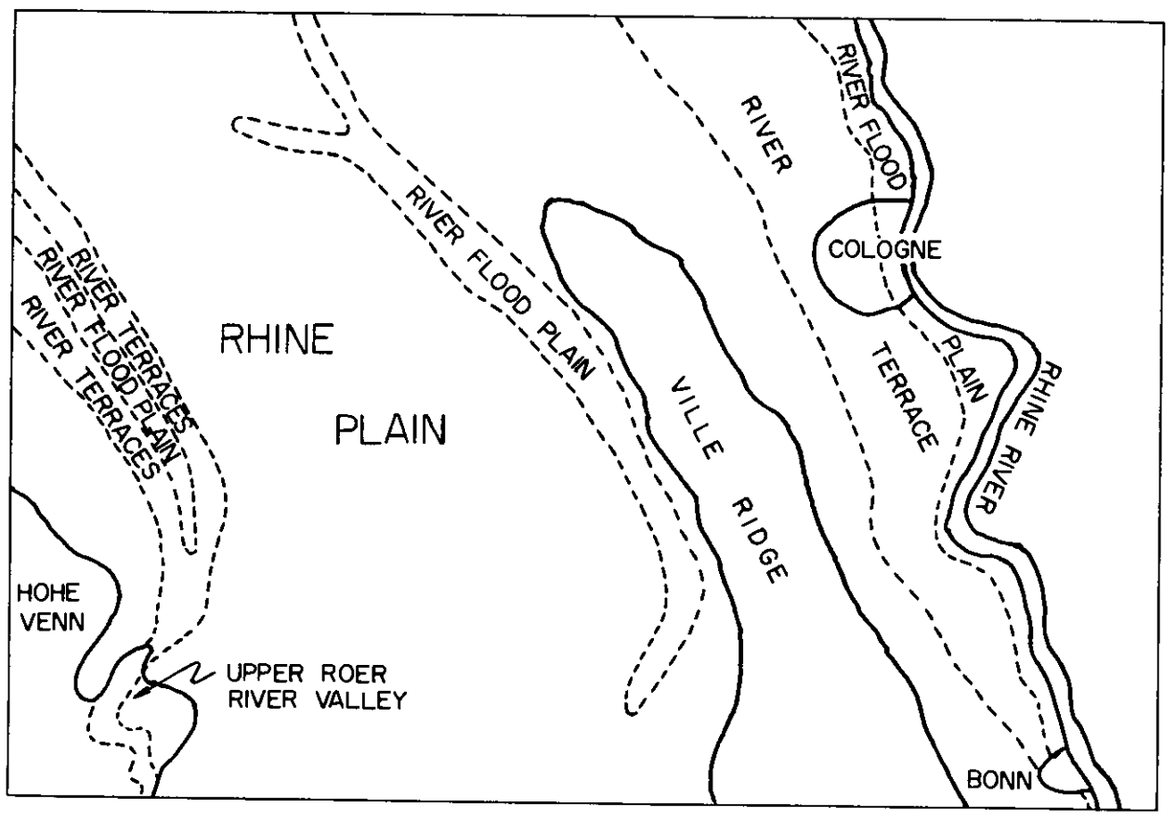
1000 0 1000 2000 3000 4000 5000 6000 7000 8000 Meters

1000 0 1000 2000 3000 4000 5000 6000 7000 8000 Yards

Contour Interval 50 Feet

Prepared by The Engineer School, Fort Belvoir, 1959. Map keyed to Germany 1:100,000 AMS, S-1 and R-1, 1952, to which reference is made for marginal information. Comments concerning field usability are requested by The Department of Training Publications, The Engineer School, Fort Belvoir, Virginia. For illustrative purposes, bridge classification information has been purposely omitted from this map. Route classification information has been added to the legend under "roads".

Figure 61. Movement Map of Cologne area.



HOHE VENN HIGHLAND

The HOHE VENN HIGHLAND shown on the map is the northern tip of a much larger forested plateau to the southwest. It has two principal landforms . . . a dissected upland and the upper ROER RIVER valley system.

Upland

This upland is made up of flattened sandstone hills 300–500 feet high with steep wooded slopes usually above 25 percent. Bluffs are common. Some of the flattened hilltops are open and are used for farming and pasturage. Principal soil type is loam. Cross-country movement is good in the open areas, but steep sandstone-shouldered ravines are frequent barriers. Trails and roads provide occasional passage from the open hilltops through defiles to the lowland valleys. In this area, sandstone may be quarried. Towns are small and scattered, and construction sites for facilities are limited. Road and rail communication is poor as compared to the lowland plains.

Upper ROER RIVER Valley

This valley system is rather narrow with steep wooded sides and occasional escarpments. The valley floor does not exceed one-half mile in width but is made up of sandy gravel; cross-country movement is good under most conditions. The ROER RIVER is approximately 80 feet wide in this vicinity, with a stream velocity of 4-8 ft/sec. Two large dams several miles upstream control its flow and much of the valley floor may be flooded by release of the impounded water. Traffic into and out of the valley is restricted to roads, but a railroad follows the river route into the city of DUREN.

VILLE RIDGE

The VILLE RIDGE is a long (25 miles), narrow (3-5 miles), southward rising promontory with summits 100 to 250 feet above the surrounding countryside. Surface soil type is clay loam with sand loam along the flanks of the ridge, but the overburden is rarely in sight due to extensive surface coal mining. The mine pits, dumps, and spoil heaps, and the great number of industrial buildings effectively limit vehicular movement to roads. Scattered mixed and broadleaf forests are found throughout the ridge and are indicated on the map. Crushed rock is available in the mine dumps. Several coal-driven power generating stations are located here. The ridge area is unfit for airfield sites because of mines, industrial towers, buildings, woods, and so on.

RHINE PLAIN

The RHINE PLAIN consists of three related areas; (1) flood plains of the lower ROER, ERFT, and RHINE RIVERS; (2) the terraces along these rivers; (3) the prairie lands between the rivers.

Flood Plains

The flood plains of the ROER and ERFT RIVERS are quite flat and are dissected by many ditches and drainage channels. They have complex soils of silts and very fine sands; a high water table makes them difficult to traverse during wet periods. Portions of the flood plains are drained swamps with considerable organic material in the soil. Traffic is restricted to the road system by these factors, but foot troops will encounter only minor difficulty. The flood plain of the RHINE RIVER is quite narrow, as the river terraces closely approach the river on the west bank between BONN and COLOGNE. The RHINE RIVER here is 900-1400 feet wide, has a 2-4 ft/sec. velocity and is 20-40 feet in depth.

River Terraces

River terraces are poorly developed along the ROER and ERFT RIVERS, but reach a grand scale along the RHINE RIVER where four or five terraces can be found. They are composed of sandy or occasionally loamy soil, and are up to four miles wide along the west bank. Cross-country movement is good to excellent in most weather. Slopes between terraces are usually less than 10 percent, while the terraces themselves are practically level. One boggy spot (5) is shown between COLOGNE and BONN, but others, all of very small size, may be present on the southwestern outskirts of COLOGNE. Terrace slopes along the ROER and RHINE RIVERS are good sources for gravel aggregate.

Prairie Lands

These are extensive areas of very gently rolling topography mostly taken up with farmland. The land between the ROER and ERFT RIVERS, and that north of the JULICH-COLOGNE highway are examples of prairie lands. Soils are sand loam to clay loam, rather thick, and are the weathered product of loess deposits. Sandy areas are found, and are due partly to glacial outwash, and partly to the lithology of the underlying rock. Cross-country movement over prairie land is good in fair weather, but hampered by mud to a degree dependent upon the sand content of the soil. Scattered wooded areas which usually possess soils of the same loamy nature are delineated on the map. Prairie lands are well suited for most types of military surface construction.

GENERAL WEATHER-MOVEMENT RELATIONS

Although February and March are months low in total precipitation, weather conditions cause soil to retain a high moisture content. Alternate freezing at night and thawing during the day prevents normal drainage. Freezing is seldom intense enough or of such a duration to facilitate movement. The snow cover normally does not exceed six or seven inches at any one time, which will not hinder tracked vehicles but may necessitate the use of chains on wheeled vehicles. Good cross-country movement may be counted on for no more than eight or nine days per month in the prairie lands during this period of the year.

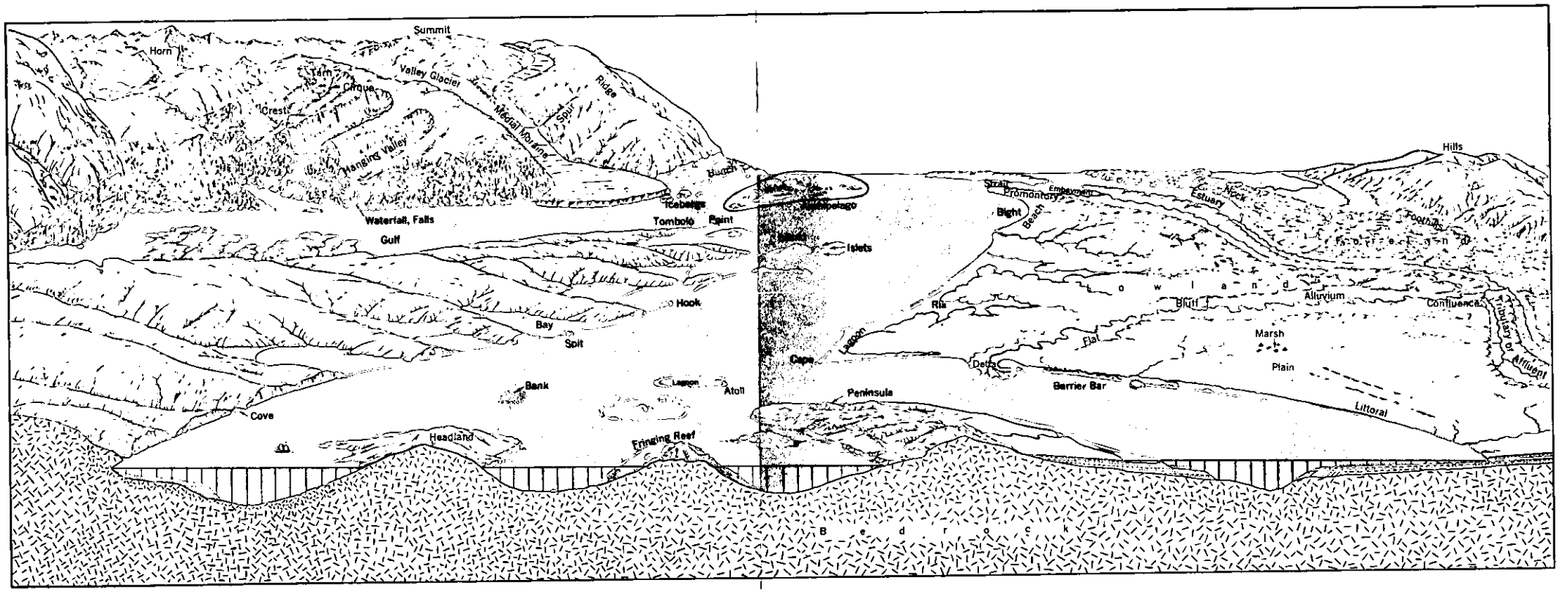
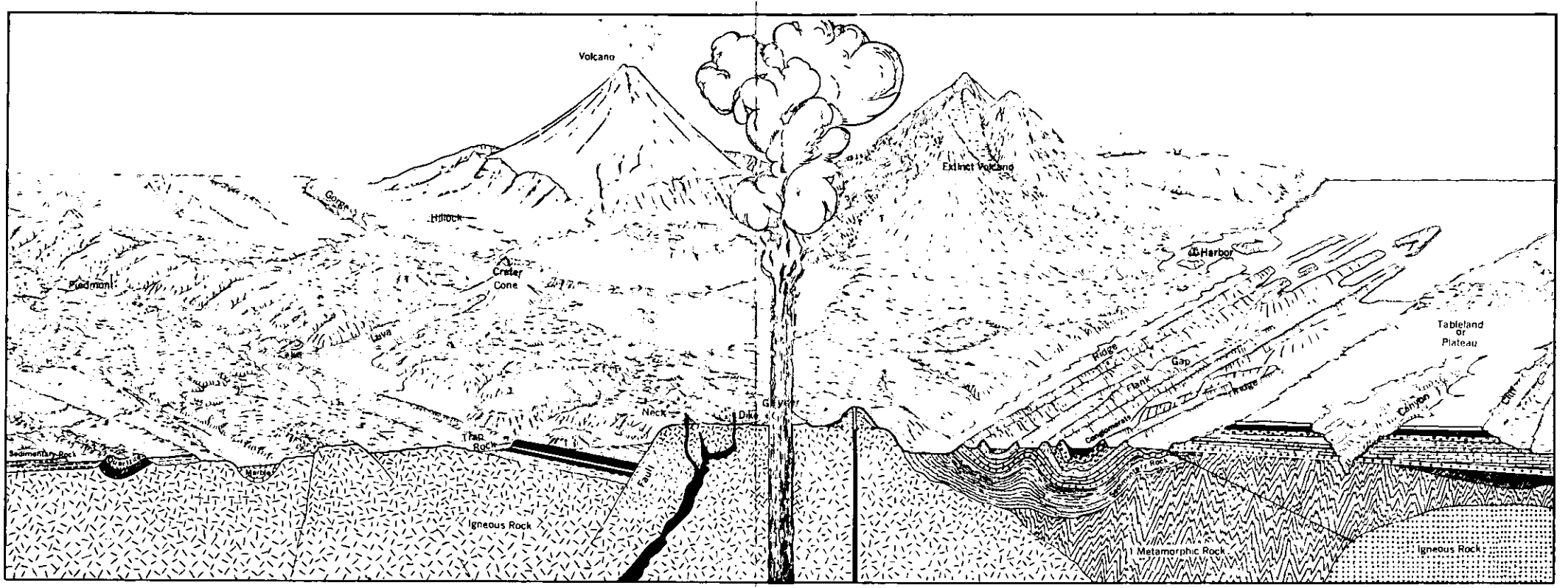
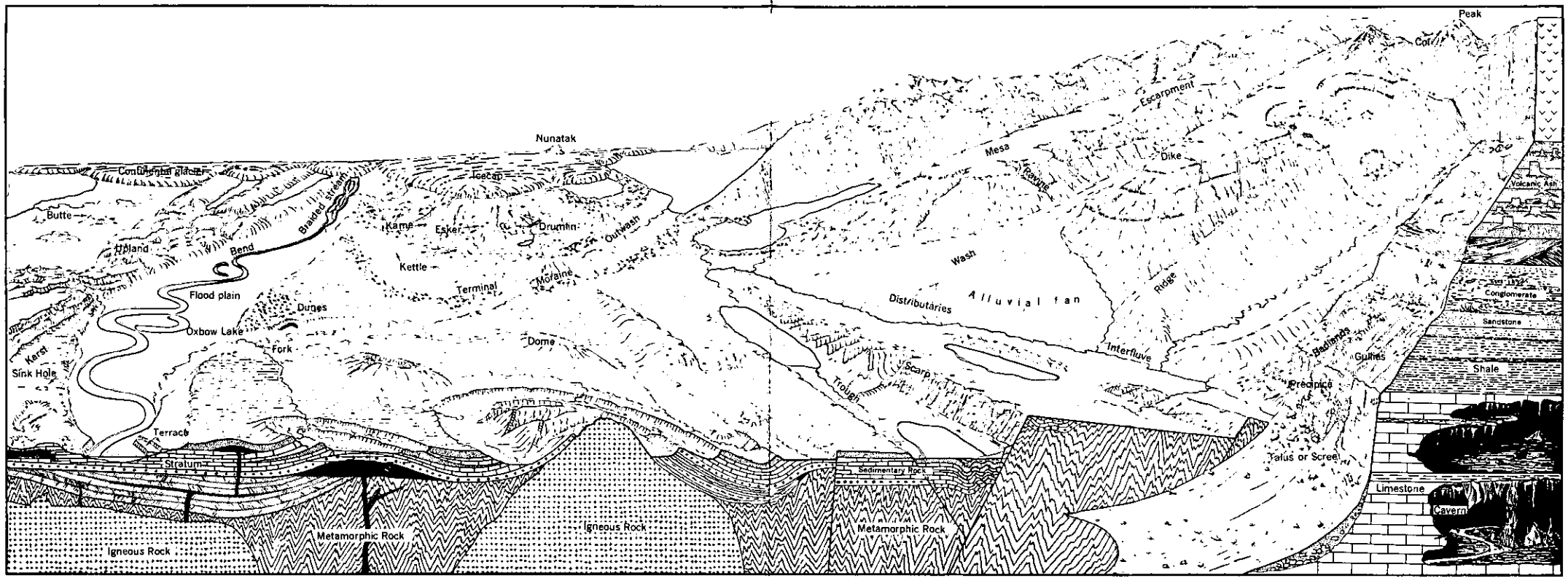


Figure 71. Natural terrain features.



B

Figure 71.—Continued



c

Figure 71.—Continued

REF ID:A56932

~~RESTRICTED~~ ~~CONFIDENTIAL~~

TM32-220

DEPARTMENT OF THE ARMY TECHNICAL MANUAL

BASIC CRYPTOGRAPHY

Accounts taken from WFF's home

DEPARTMENT OF THE ARMY • APRIL 1950

~~RESTRICTED~~

558.2

~~CONFIDENTIAL~~

Declassified and approved for release by NSA on 01-17-2014 pursuant to E.O. 13526

REF ID:A56932

WARNING

Authority for release of this document to a foreign government must be secured from the Director of Intelligence, GSUSA.

When this document is released to a foreign government, it is released subject to the following conditions: This information is furnished with the understanding that it will not be released to another nation without specific approval of the United States of America, Department of the Army; that it will not be used for other than military purposes; that individual or corporation rights originating in the information whether patented or not will be respected; and that the information will be afforded substantially the same degree of security as afforded by the United States of America, Department of the Army.

30 April 1959

This document is re-graded ~~"CONFIDENTIAL"~~ UP of DOD Directive 5200.1 dated 8 July 1957, and by authority of the Director, National Security Agency.

Paul S. Willard
Colonel, AGC
Adjutant General

~~CONFIDE~~ REF ID:A56932

~~RESTRICTED~~

DEPARTMENT OF THE ARMY TECHNICAL MANUAL

TM 32-220

This manual supersedes TM 11-484, 20 March 1945, and TM 11-485, 8 June 1944

BASIC CRYPTOGRAPHY

DEPARTMENT OF THE ARMY • APRIL 1950

United States Government Printing Office
Washington : 1950

~~RESTRICTED~~

REF ID:A56932

DEPARTMENT OF THE ARMY
WASHINGTON 25, D. C., *5 April 1950*

TM 32-220 is published for the information and guidance of all concerned.

[AG 300.7 (2 Sep 49)]

BY ORDER OF THE SECRETARY OF THE ARMY:

OFFICIAL:
EDWARD F. WITSELL
Major General, USA
The Adjutant General

J. LAWTON COLLINS
Chief of Staff, United States Army

DISTRIBUTION:

GSUSA (1); Tech Sv (2); Arm & Sv Bd (1); AFF (10); OS Maj Comd (5); Basic Comd (1); MDW (1); A (ZI) (25), (Overseas) (10); CHQ (10); D (2); B (5); Bn 11 (5); FC (1); USMA (10); Sch (2); PMS&T (2); Tng Ctr (2); SPECIAL DISTRIBUTION.

For explanation of distribution formula, see SR 310-90-1.

REF ID:A56932

CONTENTS

	Paragraphs	Page
PART ONE. ELEMENTARY MILITARY CRYPTOGRAPHY.		
CHAPTER 1. INTRODUCTION.		
Section I. General	1–2	1
II. Terminology	3–9	3
III. Two classes of cryptographic systems	10–12	8
IV. Security and time elements in cryptographic systems	13–18	9
CHAPTER 2. ELEMENTARY TRANSPOSITION SYSTEMS.		
Section I. Simple monoliteral transposition methods	19–26	18
II. Columnar transposition methods	27–30	26
III. Miscellaneous transposition methods	31–34	30
CHAPTER 3. ELEMENTARY SUBSTITUTION SYSTEMS.		
Section I. General	35–40	33
II. Monoalphabetic substitution systems	41–44	37
III. Types of mixed cipher alphabets	45–51	40
IV. Monoalphabetic substitution with variants	52–55	46
V. Polyalphabetic substitution systems	56–60	48
VI. Cipher disks and square tables	61–63	54
VII. Observation on cipher systems	64–67	60
CHAPTER 4. ELEMENTARY CODE SYSTEMS.		
Section I. General	68–71	63
II. Code groups	72–74	66
III. One-part and two-part codes	75–76	69
IV. Enciphered code	77–78	72
CHAPTER 5. COMPARISON OF CODE AND CIPHER SYSTEMS	79–80	74
6. CORRECTION OF ERRORS	81–82	79
7. FUNDAMENTAL RULES FOR SAFEGUARDING CRYPTOGRAMS	83–84	83
PART TWO. ADVANCED MILITARY CRYPTOGRAPHY.		
CHAPTER 8. TRANSPOSITION SYSTEMS.		
Section I. Monophase transposition systems	85–91	87
II. Polyphase transposition systems	92–94	99
III. True double transposition	95–96	102
IV. Grilles and other types of matrices	97–106	106
V. Miscellaneous transposition systems	107–110	121

REF ID:A56932

		Paragraphs	Page
CHAPTER 9. SUBSTITUTION SYSTEMS.			
Section I.	Polygraphic systems	111–113	124
II.	Matrix digraphic substitution	114–119	133
III.	Complex substitution systems	120–127	143
CHAPTER 10. REPETITIVE AND COMBINED SYSTEMS.			
Section I.	Repetitive systems	128–131	151
II.	Combined systems	132–140	153
CHAPTER 11. CIPHER DEVICES AND CIPHER MACHINES.			
Section I.	Cipher devices	141–145	164
II.	Cipher machines	146–152	168
CHAPTER 12. CODE SYSTEMS.			
Section I.	General	153–154	174
II.	Enciphered code	155–163	175

REF ID:A56932

This manual supersedes TM 11-484, 20 March 1945, and TM 11-485, 8 June 1944

PART ONE
ELEMENTARY MILITARY CRYPTOGRAPHY
CHAPTER 1
INTRODUCTION

Section I. GENERAL

1. Scope

This manual consists of two parts as follows:

a. Part one is an introduction to the elementary principles of military cryptography. In this part a few typical examples of cipher systems and code systems are presented; the procedure in cryptographing and decryptographing by means of the systems is shown in detail; methods of preparing keys suitable for use in connection with them are illustrated; errors and their correction are discussed; and finally, a few of the most important precautions to be observed in safeguarding systems and cryptograms from enemy cryptanalysts are set forth. Only such considerations as apply to military cryptography are included.

b. Part two develops the principles established in part one and treats of the more advanced systems. Following the presentation sequence of part one, transposition systems are discussed first, then substitution systems. Considerable attention is devoted to combined substitution and transposition methods. Following this is a description of a limited number of cipher devices and machines, together with a discussion of their present-day limitations. Finally, code systems are discussed briefly with special emphasis upon enciphered code systems.

2. Developments in Cryptography

a. Cryptography is by no means a static art or science and viewpoints are always undergoing change; what is regarded as wholly impracticable today may, through some unforeseen improvement in technique, become feasible tomorrow, and it is unwise to condemn a system too hastily. For example, before World War I, and indeed for the first 2 years of that conflict, the use of codebooks in the theater of operations was

REF ID:A56932

regarded as wholly impracticable.[1] Colonel Hitt in his *Manual for the Solution of Military Ciphers,* published in 1916, stated:

> The necessity for exact expression of ideas practically excludes the use of cod. for military work, although it is possible that a special tactical code might be useful for preparation of tactical orders.

Also, in an official British Army *Manual of Cryptography* prepared in 1914 is found the following statement:

> Codes will first be considered, but as they do not fulfill the conditions required of a means of secret communication in the field, they need not be dealt with here at length.

In the 1935 edition of this text the foregoing quotations were immediately succeeded by the following comment:

> It need only be pointed out in this connection that today code methods predominate in the secret communication systems of the military, naval, and diplomatic services of practically all the large nations of the world. Nevertheless, it is likely that within the next decade or two the pendulum may once more swing over to the other position and cipher methods may again come to the fore, especially if mechanical and electrical cipher machines are perfected so that their operation becomes practicable for general use. It is for this reason, if for no other, that the cryptographer who desires to keep abreast of progress must devote considerable attention to the more complicated cipher methods of the past and present time, for with the introduction of mechanical and electrical devices the complexities and difficulties of these hand-operated methods may be eliminated.

In preparing the revision of this text in 1943, the author found it necessary to say that the forecast he made in 1935 in regard to the rebirth of cipher methods had been fully justified by the present trend, which is in a direction away from code and toward cipher methods, because of important advances made in the field of mechanical and electrical cryptographic mechanisms.

b. Modern electrical communication methods and instrumentalities are finding an increasing need for applications of cryptographic theory and practice to their efficient operation. For example, in very recent years there has developed a distinct need for secure methods and means for distorting voice communications by telephone or radiophone, and for distorting facsimile transmissions by wire or radiotelegraphy. Teleprinter services permitting direct cryptographic intercommunication by machines operated from a typewriter keyboard make it desirable to have means whereby, although the keyboard is operated to correspond to plaintext characters, the latter are instantaneously and automatically enciphered in transmission and the received signals are instantaneously and automatically deciphered upon reception at the receiving end. Thus the printing mechanism at the receiving station records the original

[1] See, in this connection, Friedman, William F., *American Army Field Codes in the American Expeditionary Forces During the First World War,* Signal Security Service Publication, OCSigO, War Department, Washington, 1942.

REF ID:A56932

plain-text characters set up on the keyboard at the sending station but interception of the signals passing over the line or by radio would yield only cipher text.

c. It is difficult to foresee the specific cryptographic methods which might some day be useful in connection with developments of the foregoing nature. Progress in the electrical and electronic fields exercises an important effect upon developments in the cryptographic field. Methods which today appear to yield a high degree of cryptographic security but which are impractical for hand operation a few years from now, may be readily mechanized and become highly practical. On the other hand, methods which today do provide a high degree of security may, a few years from now, become obsolete because high-speed electrical analytical machines have been devised for their rapid solution. Consequently, if among the many and more or less complex methods set forth herein certain ones appear to fall outside the realm of what is today considered practicable, it should be remembered that the purpose in describing them is to present various basic cryptographic principles, and not to set forth methods that may with a high degree of probability be encountered in military cryptography in the immediate future.

Section II. TERMINOLOGY

3. Basic Definitions

In a study of military cryptography as employed in the U. S. Army, the following definitions will be useful:

a. SIGNAL COMMUNICATIONS. Any means of transmitting messages in plain or encrypted text other than by direct conversation or mail. A commander uses signal communications to receive reports of hostile dispositions and activities, to receive reports of the progress and needs of subordinate and neighboring friendly units, to send orders to subordinate units, to receive orders from superior units, and to send to higher and adjacent units information necessary for the coordinated action of the whole command.

b. AGENCY OF SIGNAL COMMUNICATION. The organization, teams, and personnel necessary to perform operational duties pertaining to signal communications.

c. MESSAGE. Used in its broadest sense in Department of the Army and other official publications, the term "message" includes all instructions, reports, orders, documents, photographs, maps, or other information, transmitted by means of signal communication. In this manual, however, the term "message" implies instructions, reports, orders, and similar communications usually transmitted by electrical means.

d. MEANS OF SIGNAL COMMUNICATION. A medium (including equipment) used by an agency for transmitting messages. There are two

REF ID:A56932

dozen or more different means; the most important, so far as this manua is concerned, are—

(1) *Wire:*
Telephone.
Telegraph.
Teletypewriter.
Facsimile (picture or photo transmission).

(2) *Radio:*
Radiotelephone.
Radiotelegraph.
Radio teletypewriter.
Radio facsimile.

e. WRITER. The person who actually prepares and signs the message blank. The writer may be the originator or his officially designated representative.

f. ORIGINATOR. The authority who orders the message written and sent. The commander may delegate this authority to one or more subordinates. Officers assigned as members of a unit's general staff are assumed to have been so designated.

g. TIME OF ORIGIN. The time shown on a message by the writer to indicate the hour and minute when he completed its writing.

h. ADDRESSEE. The authority (organization, office, or person) to whom a message is directed by the originator.

i. MESSAGE CENTER. That signal communication agency of a headquarters, or echelon thereof, which is charged with the receipt, routing and delivery of all official messages except: those which are transmitted directly from the originator to the addressee by means of a personal agent, or telephone or teletypewriter provided for his personal use; mail handled by military or civil postal services, and purely local messages.

j. COMMUNICATIONS CENTER. One or more agencies of signal communication equipped to receive, route, and transmit official messages. A communications center may be established at a point fixed or mobile.

4. Cryptology and Secret Communication

a. Secrecy of intercommunication in military operations is of the utmost importance. Need for it has been recognized from the earliest days of organized warfare. That branch of knowledge which treats the production, use and solution of the means and methods of secret[2] communications is called *cryptology.*

[2] Throughout this manual the term "secret" will be used in its ordinary sense as given in the dictionary. Whenever the designation is used in the more restricted sense of the security classification as defined in AR 380–5, it will be so indicated. There are in current use the classifications, *Restricted, Confidential, Secret,* and *Top Secret,* listed in ascending order of degree.

REF ID:A56932

b. Intercommunication may be conducted by any means susceptible of ultimate interpretation by one of the five senses, but those most commonly used are visual or auditory. Aside from the use of simple visual and auditory signals for intercommunication over relatively short distances, the usual method of intercommunication involves, at one stage or another, the act of *writing, speaking* over a telephone, or of *drawing* or *taking a picture.*

c. To preserve secrecy of intercommunication by telephone, there are means and methods of disguising the electrical currents in telephony so that the messages or conversations can be understood only by persons provided with the proper equipment. The same thing is true of secrecy in the electrical transmission of pictures, drawings, maps, etc. However, this manual is concerned only with secrecy of intercommunication by means of messages conveying in written words the thoughts, orders, reports, etc., of the originator to the addressee.

d. Writing may be either *visible* or *invisible.* In the former, the characters are inscribed with ordinary writing materials and can be seen with the naked eye; in the latter, the characters are inscribed by means or methods which make the writing invisible to the naked eye. Invisible writing is done with certain chemicals called *invisible, sympathetic,* or *secret inks* which have the property of either being initially invisible to the naked eye or becoming so after a short time. In order to make writing done with secret inks visible, special processes must usually be applied. There are also methods of producing writings which is invisible because the characters are of microscopic size. These methods usually require either special photographic apparatus or very delicate mechanical instruments called micropantographs, by means of which ordinary writing may be copied in extremely reduced size. Magnifying lenses must be used to make such writing visible to the naked eye.

e. Invisible writing and visible writing prepared in a form unintelligible in the language in which it is written, constitute *secret writing.* Both of these forms of secret writing have their uses in military communications, but this manual deals only with visible secret writing.

5. Plain Text and Encrypted Text

a. A visible message which conveys an intelligible meaning in the language in which it is written, with no hidden meaning, is said to be in *plain text.* A message in plain text is called a *plain-text message,* a *clear-text message,* or a *message in clear.*

b. A visible message which conveys no intelligible meaning in any language is said to be in *encrypted text.* Such a message is termed a *cryptogram.*

c. A visible message may convey an intelligible meaning which may not be the real meaning intended. To quote a simple example of a mes-

REF ID:A56932

sage containing a secret or hidden meaning, prepared with the intention of escaping suppression by censors in war time, the sentence "Son born today" may mean "Three transports left today." Messages of this type are in encrypted text and are said to be in *open code.* Although occasionally useful in espionage and counter-espionage, secret communication systems of this sort are impractical for field military use, and will not be dealt with further in this manual.

d. The term "correspondents" is used in this manual to designate persons who exchange messages with each other. Between the originator and the addressee there may be persons who actually write and handle the messages, who convert the plain texts into cryptograms, or who reconvert the cryptograms into plain texts. The originator and the addressee may also do this work but in the U. S. Army such work is usually done by special personnel who act as agents of the correspondents.

e. The term "enemy" is used in this manual to designate all persons who obtain messages or copies of messages not intended for them.

6. Cryptography, Cryptographing, and Decryptographing

a. Cryptography is that branch of cryptology which treats of various means and methods for rendering plain text unintelligible and reconverting unintelligible text into plain text or the application thereof.

b. To *cryptograph*[3] (*encrypt*) is to convert a plain-text message into a cryptogram by following certain rules agreed upon in advance by correspondents, or furnished them or their agents by higher authority. The process of *cryptographing* a message produces a *cryptogram.*

c. To *decryptograph* (*decrypt*) is to reconvert a cryptogram into the equivalent plain-text message *by a direct reversal of the cryptographing process;* that is, by applying to the cryptogram the key used in cryptographing the plain text.

d. A person skilled in the art of cryptographing and decryptographing, or one who has a part in making a cryptographic system is called a *cryptographer;* a clerk who cryptographs and decryptographs, or who assists in such work, is called a cryptographic clerk.

7. Codes, Ciphers, and Enciphered Code

a. Cryptographing and decryptographing are accomplished by means collectively designated as *codes* and *ciphers.* Such means are used for either or both of two purposes: (1) secrecy, and (2) economy or brevity. Secrecy usually is far more important in military cryptography than economy or brevity. In ciphers or *cipher systems* cryptograms are produced by applying the cryptographic treatment to *individual letters* of the plain-text messages, whereas in codes or *code systems* cryptograms are produced by applying the cryptographic treatment to entire words,

[3] Compare the terms *"cryptography," "cryptogram,"* and *"cryptograph"* with the terms *"telegraphy," "telegram,"* and *"telegraph."*

REF ID:A56932

phrases, and sentences of the plain-text messages. The specialized meanings of the terms *code* and *cipher* are explained in detail later.

b. A cryptogram produced by means of a cipher system is said to be *in cipher* and is called a *cipher message,* or sometimes simply a *cipher.* Such act or operation of cryptographing is called *enciphering,* and the enciphered version of the plain text, as well as the act or process itself, is often referred to as the *encipherment.* The cryptographic clerk who performs the process serves as an *encipherer.* The corresponding terms applicable to the decryptographing of cipher messages are *deciphering, decipherment,* and *decipherer.* A clerk who serves both as an encipherer and decipherer of messages is called a *cipher clerk.*

c. A *cipher device* is an apparatus or a simple mechanism for literal encipherment and decipherment, usually manually powered; a *cipher machine* is an apparatus or complex mechanism for literal encipherment and decipherment, usually requiring an external power source.

d. A cryptogram produced by means of a code system is said to be *in code* and is called a *code message,* or sometimes simply a *code.* The text of the cryptogram is referred to as *code text.* This act or operation of cryptographing is called *encoding,* and the encoded version of the plain text, as well as the act or process itself is referred to as the *encodement.* The clerk who performs the process serves as an *encoder.* The corresponding terms applicable to the decryptographing of code messages are *decoding, decodement,* and *decoder.* A cryptographic clerk who serves both as an encoder and decoder of messages is called a *code clerk.*

e. Sometimes, for special purposes, the code text of a cryptogram undergoes a further step in concealment involving an enciphering process, thus producing what is called a cryptogram in *enciphered code,* or an *enciphered-code message. Encoded cipher,* the cipher text of a cryptogram which subsequently undergoes encodement, is also possible but rare.

f. In U. S. Army tables of organization and other publications, cipher clerks and code clerks are cryptographic technicians. They are specifically trained to encipher, decipher, encode, and decode messages, using authorized means, equipment, and procedures.

8. General System and Specific Key

a. The total of all the basic, invariable rules followed in cryptographing a message according to a given method, together with all the agreements, conventions or private understandings drawn up between the correspondents or their authorized agents or furnished them by higher authority, constitute the *general cryptographic system.*

b. In the general cryptographic system usually a number, a group of letters selected at random, a word, a phrase, or a sentence, is used as a key. The element selected governs the manner in which a cipher device or a cipher machine is prepared for the encipherment or decipherment

REF ID:A56932

of a specific message, or it controls the steps followed in cryptographing a specific message. This element—usually of a variable nature and changeable at the will of the correspondents, or prearranged for them or for their agents by higher authority—is the *specific key*. The specific key may also involve the use of a set of specially prepared tables, a special document, or even a book.

c. Hereafter, the general cryptographic system will be referred to as the *system,* and the specific key, as the *key.*

9. Cryptanalytics and Cryptanalysis

a. In theory, any cryptographic system except one can be broken down if enough time and skill are devoted to it, and if the volume of traffic is large enough. This can be done even if the general cryptographic system and the specific key are unknown at the start. The exception is the "one time" system in which the key is used only once and in itself must have no systematic construction, derivation, or meaning. In military operations theoretical rules must usually give way to practical considerations. How the theoretical rule in this case is affected by practical considerations will be taken up in subsequent portions of this manual.

b. That branch of cryptology which deals with the principles, methods, and means employed in the solution or *analysis* of cryptograms is called *cryptanalytics.*

c. The steps and operations performed in applying the principles of cryptanalytics constitute *cryptanalysis.* To cryptanalyze a cryptogram is to *solve* it by cryptanalysis.

d. A person skilled in the art of cryptanalysis is called a *cryptanalyst,* and a clerk who assists in such works is called a *cryptanalytic technician.*

Section III. TWO CLASSES OF CRYPTOGRAPHIC SYSTEMS

10. Transposition and Substitution

a. Technically there are only two distinct types of treatment which may be applied to plain text to convert it into secret text, yielding two different *classes* of cryptograms. In the first, called *transposition,* the *elements* or *units* of the plain text, whether one is dealing with individual letters or groups of letters, syllables, whole words, phrases and sentences, retain their original identities and merely undergo some change in their relative positions or sequences so that the message becomes unintelligible. In the second, called *substitution,* the elements of the plain text retain their original positions or sequences but are replaced by other elements with different values or meanings.

b. It is possible to cryptograph a message by a substitution method and then to apply a transposition method to the substitution text, or vice

REF ID:A56932

versa. Such combined transposition-substitution methods do not form a third category of methods. They are occasionally encountered in military cryptography, but the types of combinations that are sufficiently simple to be practicable for field use are very restricted.

11. Letter, Syllable, and Word Methods

Under each of the two principal classes of cryptograms as outlined in the preceding paragraph, a further classification can be made with respect to the nature of the *textual elements* or *units* with which the cryptographic process deals. These textual units are (1) individual letters, or groups of letters in regular sets, and (2) complete words. Methods which deal with the first type of units are called *letter methods,* including, when such is the case, *syllable methods;* those which deal with the second type of units are called *word methods.*

12. Cipher Systems and Code Systems

It is necessary to indicate that the classification into letter, syllable, and word methods is more or less arbitrary or artificial in nature, and is established for purpose of convenience only. No sharp line of demarcation can be drawn in every case, for occasionally a given system may combine methods of treating single letters, groups of letters, syllables, whole words, phrases and sentences. When in a single system the cryptographic treatment is applied to textual units of regular length, usually single letters or pairs, and is only exceptionally applied to textual units of irregular length, the system is called a *cipher system.* Likewise, when in a single system the cryptographic treatment is applied to textual units of irregular length, usually whole words, phrases, and sentences, and is only exceptionally applied to single letters, pairs, or groups of letters and syllables, the method is called a *code system* because it generally involves the use of a code book.

Section IV. SECURITY AND TIME ELEMENTS IN CRYPTOGRAPHIC SYSTEMS

13. Interception, Radio Direction Finding, and Radio Position Finding

a. Messages transmitted by electrical means can be heard and copied by persons who are not the correspondents or their authorized agents. Messages transmitted by radio can be manually copied or automatically recorded by suitably adjusted radio apparatus located within range of the transmitter. Some messages transmitted over wire lines can likewise be

REF ID:A56932

manually copied or automatically recorded by special apparatus suited for the purpose. Correspondents have no way of knowing whether or not radio transmissions are being copied by the enemy, since the unauthorized copying does not interfere in the slightest degree with signals being transmitted. Interception of wire traffic is much more difficult than of radio, mainly because the equipment must be located very near the wire line, or connected directly to it. The act of listening-in and copying or recording electrically-transmitted messages by persons other than the correspondents or their authorized agents is called *interception.* The purpose of interception is to obtain copies of messages transmitted and, by studying them, to obtain information. In time of war, it must be assumed that the enemy will intercept all messages transmitted by any signal communication agency susceptible of interception.

b. It is also possible to determine, with a fair degree of accuracy, the direction of a radio transmitter from a given location and, by establishing the direction from two or more locations, it is possible to determine the geographical location of the transmitter. The science which deals with the means and methods of determining the direction in which a radio transmitter lies is called *radio direction finding;* the method of determining the geographical location of a radio transmitter, by the use of two or more direction-finding installations, is called *radio position finding.*

c. Messages may be transmitted by signals with special apparatus which distort, disguise, or completely hide the signals themselves, so that the processes of interception and recording the signals are very difficult, and intercept personnel may not even be aware of the existence of such signals. All such methods of transmitting messages fall in the class designated in this manual as *systems of secret signaling.* Signaling by means of so-called "black light," that is, invisible or infra-red light waves, falls into this category. Methods of disguising or distorting voice or picture transmissions (par. 2*c*) require more or less highly-specialized apparatus for the interception of the signals and their interpretation or recording in recognizable form. As a rule, the signals of practically all systems of secret signaling can be intercepted and recorded in a form suitable to making the signals understood by one of the senses, usually visual or auditory. Ordinarily, this requires special apparatus but can sometimes be done without the specific apparatus used in forming or sending the signals, or the "key" used in their distortion, or disguise.

14. Traffic Analysis and Cryptanalysis

a. A great deal of information of military value can be obtained by studying signal communications without solving the crytographed messages constituting the traffic. The procedure and the methods used have yielded results of sufficient importance to warrant the application of a

REF ID:A56932

special term to this field of study; namely, *traffic analysis*[4], which is the study of signal communications and intercepted or monitored traffic for the purpose of gathering military information without recourse to cryptanalysis.

b. In general terms, traffic analysis is the careful inspection and study of signal communications for the purpose of penetrating camouflage superimposed upon the communication network for purposes of security. Specifically, traffic analysis reconstructs radio communication networks by: (1) noting volume, direction, and routing of messages; (2) correlating transmission frequencies and schedules used among and within the various networks; (3) determining directions in which transmitters lie, by means of radio direction finding; (4) locating transmitters geographically, by radio position finding; (5) developing the system of assigning and changing radio call signs; (6) studying all items that constitute "conversations" or "chat" exchanged among operators on radio channel.

c. From a correlation of general and specific information derived from these procedures, traffic analysis is able not only to ascertain the geographic location and disposition of troops and military units (technically called "order of battle") and important troop movements, but also to predict with a fair degree of reliability the areas and extent of immediately pending or future activities. Traffic analysis procedures are followed to obtain information of value concerning the enemy, and to determine what information concerning our own forces is made available to the enemy through our own signal communications.

d. These very important results are obtained without actually reading the texts of the intercepted messages; the solution and translation of messages are the functions of cryptanalysis and not traffic analysis. However, the cryptanalyst is frequently able to make good use of bits of information disclosed by traffic analysis such as faults noted in message routing and errors in cryptography causing messages to be duplicated or canceled. Cryptanalysis can provide important information for traffic analysis, since the solution of messages often yields data on impending changes in signal communication plans, operating frequencies and schedules, etc. It also yields data on specific channels, networks, or circuits which are most productive of intelligence, so that effective control and direction of intercept agencies for maximum results can be achieved.

e. In addition to (1) traffic analysis and (2) cryptanalysis as means of obtaining information relating to communications, further data may be obtained (3) by the use of secret agents for espionage, (4) by the capture and interrogation of prisoners, (5) by the capture of headquarters or command posts with records more or less intact, and (6) by treason or carelessness on the part of personnel who handle communications. Of

[4] Which may be abbreviated *tranalysis.*

REF ID:A56932

these six main sources, traffic analysis and cryptanalysis are the most valuable. The amount of vital information they furnish cannot be accurately estimated as it fluctuates with time, place, circumstances, equipment, and personnel. For most effective operation, the results of both cryptanalysis and traffic analysis can be fitted together to yield a unified picture of the communications scheme. Therefore, if all transmitting stations can be located quickly and if all communications can be intercepted and solved, extremely valuable information concerning strength, disposition of forces, and proposed moves will be continually available.

f. The facts set forth above are applicable to our own forces as well as the enemy's.

g. The process of intercepting and copying our own or friendly radio and wire transmissions for the purpose of detecting and correcting violations of regulations is called *monitoring;* it provides increased protection of our own signal communications.

15. Communication Intelligence and Communication Security

a. Communication intelligence is evaluated information concerning the enemy, derived principally from a study of his signal communications. The main components of communication intelligence are as follows:

(1) Interception of signals or messages and forwarding raw traffic to communication intelligence centers for study.

(2) Traffic analysis, including radio direction finding and radio position finding. (Evaluated information from this source is often called *traffic intelligence.*)

(3) Cryptanalysis or solution (and translation, when necessary) of the texts of the messages.

(4) Evaluation of data, that is, analysis of results obtained from the preceding steps and their correlation, collation, and comparison with results obtained from other sources of information.

b. Communication security is the protection resulting from all measures designed to deny to unauthorized persons information of value which may be derived from communications. The main components of communication are as follows:

(1) *Physical security,* that component of communication security which results from all measures necessary to safeguard classified communication equipment, and material from access thereto by unauthorized persons.

(2) *Cryptosecurity,* that component of communication security which results from the provision of technically sound *cryptosystems*[5] and their proper use.

[5] *Cryptosystems* may be categorized as literal and nonliteral. This manual is concerned solely with *literal* or *cryptographic* systems.

REF ID:A56932

(3) *Transmission security,* that component of communication security which results from all measures designed to protect transmissions from interception and traffic analysis.

c. Further details on the subject of communication security will be found in JANAP 122(A) Joint Communications Instructions.

16. Time Needed for Cryptanalysis and its Dependent Factors

a. In military operations time is a vital element. The influence or effect that analysis of military cryptograms may have on the tactical situation depends on various time factors.

b. Of these factors, the following are the most important:

(1) The length of time necessary to transmit intercepted enemy cryptograms to solving headquarters. This factor is negligible only when signal communication agencies are properly and specifically organized to perform this function.

(2) The length of time required to organize raw materials, to make traffic analysis studies and to solve the cryptograms, and the time required to make copies, tabulate, and record data.

(3) The nature of information disclosed by traffic analysis studies and solved cryptograms; whether it is of immediate or operational importance in impending action, or whether it is of historical interest only in connection with past action.

(4) The length of time necessary to transmit information to the organization or bureau responsible for evaluating the information. Only after information has been evaluated does it become *military intelligence.*

(5) The length of time necessary to transmit resulting military intelligence to the agency or agencies responsible for tactical operations, and the length of time necessary for the agency to prepare orders for the action determined by the intelligence and to transmit them to the combat units concerned. The last sentence under (1) above applies here also.

c. Of the factors mentioned in *b* above, the only one of direct interest in this manual is the length of time required to solve the cryptograms. This is subject to great variation, dependent upon other factors, of which the following are the most important:

(1) *The degree of cryptographic security* in the system. The degree of security depends upon the technical soundness of the system itself. Technical soundness, in turn, determines the resistance to analysis which the system offers. Cryptographic systems vary widely in technical soundness, but this manual does not attempt to demonstrate such variation.

REF ID:A56932

(2) The adequacy and technical soundness of regulations drawn up by designers of the cryptographic system for the guidance of cryptographic technicians who are its actual users.

(3) The extent to which cryptographic technicians follow these regulations and procedures. Security of a good cryptographic system can be almost completely destroyed by a few cryptographic technicians who fail to observe the regulations, are careless in their observance, in sheer ignorance commit serious violations of cryptographic security, *or adopt bad technical habits.* As a result, these technicians jeopardize not only their own lives but the lives of thousands of their comrades.

(4) The volume of cryptographic text available for study. As a rule, the greater the volume of text, the more easily and speedily it can be solved. A single cryptogram in a given system may present an almost hopeless task for the cryptanalyst, but if many cryptograms of the same system or in the same or closely related specific keys are available for study, the solution may be reached in a very short time.

(5) The number, skill, and efficiency of organization and cooperation of signal intelligence units assigned to the work. Cryptanalytic headquarters are organized in units of ascending size, ranging from a few persons in the forward echelons to many persons in the rear echelons. Such organization avoids duplication of effort and, especially in forward areas where spot intelligence is most useful, makes possible the quick interpretation of cryptograms in already solved systems. In all these units, proper organization of highly skilled workers is essential for efficient operation.

(6) The amount and character of information and intelligence available to the cryptanalytic headquarters. Isolated cryptograms exchanged between a restricted, small group of correspondents, about whom and whose business no information is available, may resist the efforts of even a highly organized, skilled cryptanalytic office indefinitely. If, however, a certain amount of such information is obtained, the situation may be entirely changed. In military operations usually a great deal of collateral information is available, from sources indicated in paragraph 14*e*. As a rule, a fair amount of more or less definite information concerning specific cryptograms is at hand, such as proper names of persons and places, and events in the immediate past or future. Although the exchange of information between intelligence and cryptanalytic staffs is very important, the collection of information derived from an intensive study of already solved traffic is equally as important because it yields extremely

REF ID:A56932

valuable *cryptanalytic intelligence* which greatly facilitates the solution of new cryptograms from the same sources.

17. Degree of Crytographic Security Required of a System for Military Use

The ideal cryptographic system for military purposes would be a *single, all-purpose* system which would be practicable for use not only by the largest fixed headquarters but also by the smallest troop unit in the combat area, and which would also present such a great degree of cryptographic security that, no matter how much traffic became available, all in the same key, the cryptograms composing this traffic would resist solution indefinitely. Such an ideal system however, is beyond the realm of possibility so far as present methods of cryptographic communication are concerned; in fact, a multiplicity of systems must be employed, each more or less specifically designed for a particular purpose. Of each such system, *the best that can be expected is that the degree of security be great enough to delay solution by the enemy for such a length of time that when the solution is finally reached the information thus obtained has lost all its "short term," immediate, or operational value, and much of its "long term," research, or historical value.*

18. Fundamental Practical Requirements of a Cryptographic System for Military Use

a. Military cryptograms must meet certain fundamental requirements of a practical nature because of definite limiting conditions in present military signal communication means and methods.

b. These requirements are (1) reliability, (2) security, (3) rapidity, (4) flexibility, and (5) economy. Their relative importance is in the order named.

c. Reliability is of first importance. Reliability, as applied to a cryptographic system or device, means that the cryptograms produced by the sending or originating office will be decryptographed promptly, accurately, and without ambiguity by the receiving office; that the cryptographic system, whether a book, machine, or device, will be on hand and in good working order, available for instant use; and that when used it can be expected to be operative as long as needed. Simplicity is implied in reliability; usually, the more simple the system, the more reliable it is. Security is the protection afforded by a sound cryptographic system; rapidity, the speed with which messages can be cryptographed and decryptographed, usually expressed in words or 5-letter groups per minute. The conflicting requirements of *security* and *rapidity* vary according to circumstances. Signal communication personnel must be governed by general principles, subject to existing circumstances, rather than by rigid

REF ID:A56932

regulations. Maximum security at all times should be the goal, but in messages exchanged among the higher headquarters some speed may be sacrificed to meet greater security requirements, while in messages exchanged among the lower headquarters security must often give way to greater speed requirements. For this reason various cryptographic systems must be available to meet varying types of situations. As to flexibility, a cryptographic system specifically adapted for a particular usage cannot serve as an all-purpose system. A codebook designed for front-line use can hardly serve the needs of a high headquarters in the rear; nor can a cryptographic system designed for use by a high headquarters serve the needs of a small combat unit. As to economy, the simpler the operations involved, the shorter will be the texts produced, the amount of time required to produce the cryptographic material, use it, and transmit the messages; and the greater will be the economy.

d. Specific requirements which should be met by a cryptographic system for general military use are set forth below.

(1) Cryptograms must be in a form suitable for transmission by standard telegraphic equipment and methods. This requirement generally eliminates all systems except those which produce cryptograms composed of characters readily transmitted by a telegraphic system employing either the Morse or the teleprinter alphabet. Cryptographic systems using Arabic numerals are not so desirable as those using letters because the Morse signals for numbers are longer, except when "cut" numbers are used, and are more difficult for the average American telegraph or radio operator to handle. Systems which produce cryptograms composed of mixtures of letters and figures, or of letters, figures, and punctuation signs, and which must be transmitted by Morse telegraphy are unsuited for practical usage. However, where such intermixtures are produced automatically by the cryptographic mechanism and are transmitted, received, and deciphered automatically, as certain teleprinter enciphering systems, their use is permissible. In order to be suitable for economical Morse telegraphic transmission, the cryptographic text must be capable of being arranged in regular sets of characters for these reasons: first, it promotes accuracy in telegraphic transmission (since an operator knows he must receive a definite number of characters in each group, no more and no less); and secondly, cryptanalysis is usually made more difficult when the length of the words, phrases, and sentences of the plain text is not apparent. The usual grouping is in sets of five characters, although occasionally other groupings may be made in special circumstances. Such grouping is not necessary in teleprinter encipherment systems.

REF ID: A56932

(2) Regular channels of signal communication can carry only a limited volume of traffic. Their most efficient operation demands that the smallest number of characters actually necessary to convey a given message be transmitted. Therefore, the cryptographic text should be no longer than its equivalent clear text. In an exceptional case, the cryptographic text may be longer than the equivalent clear text, but a system in which the cryptographic text is twice the length of the equivalent clear text is useful only if it is of outstanding merit and suitable for certain restricted or special use. No system in which the cryptographic text is more than twice the length of the equivalent clear text is practicable for military usage. Most of the cryptographic systems in current use produce cryptograms which correspond in length with that of the original plain-text message or are somewhat shorter.

(3) General requirements of reliability and speed are that the operations of cryptographing and decryptographing be relatively simple and rapid. For use in the combat zone, operations must be capable of being performed under difficult field conditions and must not require the remembering and application of a long series of steps or rules. They must be such as to reduce the mental strain on the operator to a minimum. Complex processes requiring several distinct steps are not suited to use in the combat zone, but occasionally systems involving only two steps, if each step is simple and rapid, may be practicable for military usage.

(4) Cipher devices or machines for field use must be light in weight, rugged in construction, and simple in operations, requiring the services of only one operator. Requirements to be met by high-speed cipher machines are too complex to be described in this manual.

(5) The system must be such that errors, which invariably occur in cryptographic communications, can be corrected easily and rapidly by cryptographic technicians. A system is impractical if frequently it is necessary to call for a repetition of the whole transmission, or for a rechecking of the original cryptographing.

e. Only a few of the systems which fulfill at least several of the foregoing practical requirements are included in this manual.

REF ID:A56932

CHAPTER 2
ELEMENTARY TRANSPOSITION SYSTEMS

Section 1. SIMPLE MONOLITERAL TRANSPOSITION METHODS

19. Transposition Ciphers in General

Transposition ciphers are like "jig-saw puzzles" in that all the pieces of which the whole original is composed are present but are merely disarranged. The pieces into which the picture forming the basis of a jig-saw puzzle may be divided are irregular in size and shape, but the pieces into which the plain text forming the basis of a transposition cipher may be divided must be much more regular, for the sake of practicability. They must be either single letters or pairs of letters, or sets of letters in regular groupings, or, in an exceptional case, whole words. Most transposition methods however, deal with individual letters and are therefore termed "monoliteral methods." The other methods are termed "polyliteral methods."

20. Geometric Designs

a. Practically all monoliteral or polyliteral transposition ciphers involve the use of a design or geometric figure, such as a square, rectangle, triangle, trapezoid, etc., in which the letters of the plain text are first *inscribed* or written according to a previously agreed-upon direction of writing and then *transcribed* or rewritten according to another and different, previously agreed-upon direction to form the text of the cryptogram. In nearly all cases the specific key consists in (1) using designs of a specific nature and dimensions, and (2) varying the direction or manner of inscription or transcription, or both.

b. In working with transposition ciphers or, for that matter, most types of ciphers, cross-section paper will be found very convenient. Cross-section paper with ¼-inch squares is most suitable. For brevity in reference, the individual small squares of such cross-section paper will hereafter be called *cells.*

21. Route Transpositions

a. Suppose the correspondents agree to use the method of monoliteral transposition known as *route transposition.* The message is inscribed

REF ID:A56932

within a rectangle in the usual manner of writing, that is, from left to right and in consecutive lines from top to bottom. If one or more cells are vacant at the end, *nulls* or *dummy* letters—letters having no significance—are inserted as "fillers" to complete the rectangle. Then, to form the cipher text, the letters in the design are taken out of the design and rewritten or transcribed by following or tracing one of many different routes. It is possible for each route to have a different starting point, and normally it is one of the four corners of the rectangle. A few typical routes are illustrated in figure 1 where, for the sake of ease in following the route, the plain-text message is assumed to be merely the sequence of letters A B C ... X.

(A) Simple horizontal:

(1)	(2)	(3)	(4)
ABCDEF	FEDCBA	STUVWX	XWVUTS
GHIJKL	LKJIHG	MNOPQR	RQPONM
MNOPQR	RQPONM	GHIJKL	LKJIHG
STUVWX	XWVUTS	ABCDEF	FEDCBA

(B) Simple vertical:

(1)	(2)	(3)	(4)
AEIMQU	UQMIEA	DHLPTX	XTPLHD
BFJNRV	VRNJFB	CGKOSW	WSOKGC
CGKOSW	WSOKGC	BFJNRV	VRNJFB
DHLPTX	XTPLHD	AEIMQU	UQMIEA

(C) Alternate horizontal:

(1)	(2)	(3)	(4)
ABCDEF	FEDCBA	XWVUTS	STUVWX
LKJIHG	GHIJKL	MNOPQR	RQPONM
MNOPQR	RQPONM	LKJIHG	GHIJKL
XWVUTS	STUVWX	ABCDEF	FEDCBA

(D) Alternate vertical:

(1)	(2)	(3)	(4)
AHIPQX	XQPIHA	DELMTU	UTMLED
BGJORW	WROJGB	CFKNSV	VSNKFC
CFKNSV	VSNKFC	BGJORW	WROJGB
DELMTU	UTMLED	AHIPQX	XQPIHA

Figure 1

(E) Simple diagonal:

(1)	(2)	(3)	(4)
ABDGHO	OKGDBA	GKOSVX	XVSOKG
CEHLPS	SPLHEC	DHLPTW	WTPLHD
FIMQTV	VTQMIF	BEIMQU	UQMIEB
JNRUWX	XWURNJ	ACFJNR	RNJFCA

(5)	(6)	(7)	(8)
ACFJNR	RNJFCA	JNRUWX	XWURNJ
BEIMQU	UQMIEB	FIMQTV	VTQMIF
DHLPTW	WTPLHD	CEHLPS	SPLHEC
GKOSVX	XVSOKG	ABDGKO	OKGDBA

(F) Alternate diagonal:

(1)	(2)	(3)	(4)
ABFGNO	ONGFBA	GNOUVX	XVUONG
CEHMPU	UPMHEC	FHMPTW	WTPMHF
DILQTV	VTQLID	BEILQS	SQLIEB
JKRSWX	XWSRKJ	ACDJKR	RKJDCA

(5)	(6)	(7)	(8)
ACDJKR	RKJDCA	JKRSWX	XWSRKJ
BEILQS	SQLIEB	DILQTV	VTQLID
FHMPTW	WTPMHF	CEHMPU	UPMHEC
GNOUVX	XVUONG	ABFGNO	ONGFBA

(G) Spiral, clockwise:

(1)	(2)	(3)	(4)
ABCDEF	LMNOPA	DEFGHI	IJKLMN
PQRSTG	KVWXQB	CRSTUJ	HUVWXO
OXWVUH	JUTSRC	BQXWVK	GTSRQP
NMLKJI	IHGFED	APONML	FEDCBA

(H) Spiral counterclockwise:

(1)	(2)	(3)	(4)
APONML	FEDCBA	NMLKJI	IHGFED
BQXWVK	GTSRQP	OXWVUH	JUTSRC
CRSTUJ	HUVWXO	PQRSTG	KVWXQB
DEFGHI	IJKLMN	ABCDEF	LMNOPA

Figure 1—Continued.

REF ID:A56932

b. It is apparent that instead of following the normal direction of writing, that is, from left to right and from the top downwards, the letters of the plain text may be inscribed according to any one of the routes agreed upon, and then transcribed to form the cipher text by taking the letters from the rectangle in the normal manner, that is, in this case from left to right, and from the top downwards, or *by following any other route of transposition.*

22. Example of Encipherment and Decipherment by Monoliteral Route Transposition

a. Now take a special example of encipherment by monoliteral route transposition. Use the message ATTACK HAS BEEN POSTPONED UNTIL TOMORROW TWO AM, and employ a relatively complicated method. Suppose that the general system agreed upon is the one being described, and that the specific key consists of the following elements:

(1) Using a completely filled rectangle of seven columns;
(2) Inscribing the letters of the plain text within the rectangle by following route (F) (3) of figure 1;
(3) Transcribing the thus inscribed letters (to form the cipher text) by following route (E) (6) of figure 1.

Since the message contains a total of 40 letters, and it has been agreed to use a completely filled rectangle of seven columns, it is necessary to add two nulls to make the total number of letters a multiple of seven. A rectangle of seven columns of cells and six lines of cells is therefore prepared. The design is then filled in as shown in figure 2.

b. To decryptograph such a cryptogram the process is merely reversed. First, the total number of letters in the cipher text must be found. Since

S	L	T	T	W	L	T
O	T	I	O	W	O	M
H	P	P	T	M	O	A
K	A	N	O	N	O	R
T	C	S	E	N	U	R
A	T	A	B	E	E	D

Cryptogram:

TMLAO WROWT ROMOT DUNTI LENOP
TSEEN POBSA HACKT TA

Figure 2

REF ID:A56932

it is 42, and since a completely filled rectangle of seven columns has been agreed upon, a design consisting of seven columns and six rows is outlined on cross-section paper. The cipher text is then inscribed according to route (E) (6) of figure 1, and after this has been completed the plaintext letters are read according to route (F) (3), figure 1. It is apparent that it is necessary to remember a relatively long series of rules, and even when the cryptographing has been accomplished correctly the degree of security is very low. Note how obviously the whole word UNTIL manifests itself in the cipher text. Parts of other words can also be seen. The degree of security remains very low despite the variability afforded by the dimensions of the rectangle, the method of inscription and transcription and their starting points.

23. Use of Nulls in Transposition

a. It will be noted that the two nulls selected as fillers to complete the rectangle in the preceding example were the letters L and T. These were chosen rather than such letters as J, K, Q, X, or Z, for a reason which is important to note. Since transposition ciphers of this type involve merely a rearrangement of the letters, without any change whatever in their identities, it follows that the natural or normal frequencies of letters of plain text remain unchanged. Now, the letters of every alphabetic language have characteristic frequencies, as a result of which certain clues are afforded in cryptanalysis. The presence, in transposition ciphers, of letters of very low frequency (in English), such as J, K, Q, X, or Z, is very unusual and therefore if these are employed merely as fillers they may afford clues as to the real number of letters in the plain text, the starting or finishing points of the real text, etc. For this reason it is best to insert as fillers in transposition ciphers letters of medium or high frequency, such as E, T, R, I, N, O, A, S, D, L, or C, for these will not afford any clues to solution. Nulls, when employed for the purpose of making cryptanalysis more difficult, may also be inserted in specific positions as prearranged, or they may be inserted at random if the system permits. This is true of other cryptographic systems, but as a general rule the use of nulls, especially in cipher systems, is to be discouraged. Very often they add little if any security, and thus merely increase the length of the cryptographic text without any compensating advantages.

b. Whenever it is necessary to add nulls in order to complete a transposition message in any respect, or for any reason whatsoever, they must be added *before* the transposition process is applied and not afterward; otherwise it will be difficult or even impossible for the decryptographing clerk to read the message. This is especially true when the service regulations require that the final group in a cryptogram be a complete group, containing exactly as many letters as all other groups in the message.

REF ID:A56932

24. Special Cases of Route Transposition

a. The oldest and simplest transposition method known, that called reversed writing, is a special case of one of the routes shown in figure 1. Here the text is written in the opposite direction from the normal; for example, BRIDGE DESTROYED is written EGDIRB DEYORTSED. The variability of the scheme, that is, the *specific key,* consists of the fact that the reversal may be applied to groups of fixed length, to whole words, to sentences, or to the whole text. The security of simple reversed writing may be somewhat increased by disguising the original word lengths, by which is meant a destruction of the normal, or natural word limits by combining a part of one word with a part of the next to form either *false words* or groups of regular length.

b. Some examples of reversed writing follow. Let the message be: BRIDGE DESTROYED AT ELEVEN PM.

(1) Reversing only the words and retaining original word lengths:
Cipher: **EGDIRB DEYORTSED TA NEVELE MP**

(2) Reversing only the words and regrouping into false word lengths:
Cipher: **EG DIRB DEYORT SEDTA NEVE LEMP**

(3) Reversing the whole text and regrouping into fives:
Cipher: **MPNEV ELETA DEYOR TSEDE GDIRB**

(4) Reversing the whole text, regrouping into fives, and inserting a null in every fifth position:
Cipher: **MPNER VELEO TADEB YORTH SEDEA GDIRB**

c. A second very simple type of transposition, that known as *vertical writing,* is a special case of another of the routes shown in figure 1.

The message BRIDGE DESTROYED is written in two vertical columns, and the cipher text is taken from the horizontal pairs thus formed. The message becomes:

BSRTI RDOGY EEDDE

BS
RT
IR
DO
GY
EE
DD
E

Figure 3.

When the plain text is inscribed in pairs of letters in vertical writing and then the cipher text is taken by transcribing the columns, a slightly different result is obtained. Using the plain text message BRIDGE DESTROYED, the cipher becomes:

BIGDS RYDRD EETOE

BR
ID
GE
DE
ST
RO
YE
D

Figure 4.

REF ID:A56932

This type of transposition is sometimes called the *rail-fence* cipher because it can be produced by writing the message in the following form:

B I G D S R Y D
R D E E T O E

which yields the same cipher result as before.

25. Remarks on Monoliteral Route Transposition

Reversed writing and vertical writing of the types indicated yield extremely simple cryptograms. In practice they are sometimes used in connection with other more or less simple cryptographing methods to increase their security. The cryptographic security of the other methods thus far indicated is also very low, despite the apparently large degree of variability they afford. The reason is that the route to be followed in the inscription or transcription process is definitely fixed under each type of route. In other types of transposition soon to be discussed, a much wider latitude for variation in the route is afforded by the use of key words to control or to guide these processes. Geometric designs are also used in these types of transposition, and key words determine the dimensions of the design, or else, if only one key word is used, it determines one dimension, the other being determined by the length of the text. Examples given in their proper place will serve to illustrate the processes.

26. Key Words and Numerical Keys

a. It is often necessary, in performing certain cryptographic operations, to employ a *numerical key,* which may consist of a relatively long sequence of numbers difficult or impossible for the average cipher clerk to memorize. To avoid making it necessary that such sequences of numbers be carried on the person in written form, a dangerous procedure, cryptographers have devised very simple methods of deriving such sequences from words, phrases, or sentences, which can usually be remembered much more easily than can unintelligible, relatively long sequences of numbers. One of the simplest methods is to assign numerical values to the letters of the key in accordance with their relative positions in the ordinary alphabet. Such a key is called a *derived numerical key.* This method of assigning the numbers is very flexible and varies with different uses to which numerical keys are put. For purposes of transposition, the method shown below is very satisfactory.

b. Let the prearranged key word be the word CARBUNCLE. Since the word contains the letter A, which comes first in the alphabet, the number 1 is written under this letter in the key word. Thus:

C A R B U N C L E
1

REF ID:A56932

The next letter of the normal alphabet that occurs in the key word is B, which is assigned the number 2. The letter C, which occurs twice in the key word, is assigned the number 3 for its first occurrence, the number 4 for its second occurrence, and so on. The final result is:

Basic key word: C-A-R-B-U-N-C-L-E
Derived numerical key: 3-1-8-2-9-7-4-6-5

c. The method may, of course, be applied to phrases or to sentences, so that a very long numerical key, impossible ordinarily to remember, may be so derived at will from an easily remembered *key text.*

d. It is advisable to make note of a few points valuable in connection with the choice of key text:

(1) It should be such as can be easily remembered. Often a key composed of two or more short words is better than one consisting of a single long word. Thus, the whole sentence WHEN DO WE EAT would be better than the single word EXTRAORDINARY.

(2) It should consist of one or more *simple,* familiar words admitting of but *one* spelling. A word such as REINFORCEMENT is inadvisable because the spelling REENFORCEMENT is also admissible. It goes almost without saying the use of words suitable for "spelling bees," even though they may be familiar, everyday words as DEFINITELY, SEPARATELY, REPETITION, etc., is likewise inadvisable.

(3) It should contain as many different letters as possible, in no systematic sequence. Words with several repeated letters, such as ELEMENT, BANANA, MISSISSIPPI, etc., form poor key words.

(4) It should present no associations with the special situation in which it is used, so as not to be easily guessed by the enemy. For example, to use personal or geographic names associated with a region in the theater of operations is bad practice. The key word GETTYSBURG employed in a cryptogram originating in the vicinity of Gettysburg would be bad practice. Or to use for this purpose words of common military usage, such as BATTALION, REGIMENT, ARTILLERY, SIGNAL CORPS, MACHINE GUN, etc., is likewise bad practice.

e. It is convenient to designate key text in letters as a *literal key.* As noted, a literal key may consist of a single letter, a single word, a phrase, a sentence, whole paragraph, or even a book. The method of deriving a numerical key from a literal key given in *b* above is only one of a number of methods, but it is the most commonly employed. It is also subject to variation in detail. But, so far as the cryptanalyst is concerned, just how the numerical key is derived from a specific literal key is usually of interest to him only if this knowledge will assist in subsequent solutions

REF ID:A56932

of cryptograms prepared according to the same basic system. Often the cryptanalyst is wholly unconcerned as to whether a literal or a numerical key has been used in connection with cryptographing of the messages, and he may frequently be unaware of the fact that a literal key has been used as the basis for deriving a numerical key.

Section II. COLUMNAR TRANSPOSITION METHODS

27. Columnar Transposition with Completely Filled Rectangles

a. One of the most common types of transposition involving the use of a key word or a derived numerical key is that known as *keyed* or *variable-key columnar transposition.* In this type the letters are usually written in a geometric design, most often a rectangle, by inscribing them in the ordinary manner, that is, in horizontal lines from left to right and from the top downwards, and then the letters are transcribed by "reading" the columns in the sequence determined by the numerical key. If the text does not contain a sufficient number of letters to fill the last line completely, as many nulls as are necessary to do so are added at the end. Figure 5 is an example of cryptographing by this method.

Key word: L - I - B - E - R - T - Y
Numerical key: 4 - 3 - 1 - 2 - 5 - 6 - 7

R	E	P	O	R	T	L
O	C	A	T	I	O	N
O	F	S	E	C	O	N
D	B	A	T	T	A	L
I	O	N	C	O	M	M
A	N	D	P	O	S	T
T	O	D	A	Y	D	N

Note. The letters D and N in the final two cells are nulls, inserted to complete the rectangle.

Cryptogram:

PASAN DDOTE TCPAE CFBON OROOD IATRI CTOOY
TOOAM SDLNN LMTN

Figure 5.

REF ID:A56932

b. To decryptograph such a cryptogram, a rectangle with the proper number of cells, determined by the length of the message and the length of the key, must first be prepared. In the foregoing example, since the cipher text consists of 49 letters and the key consists of 7 letters or num-

Cryptogram:

PASAN DDOTE TCPAE CFBON OROOD IATRI CTOOY TOOAM SDLNN LMTN

4-3-1-2-5-6-7

(a)

4-3-1-2-5-6-7

		P				
		A				
		S				
		A				
		N				
		D				
		D				

(b)

4-3-1-2-5-6-7

R	E	P	O	R	T	L
O	C	A	T	I	O	N
O	F	S	E	C	O	N
D	B	A	T	T	A	L
I	O	N	C	O	M	M
A	N	D	P	O	S	T
T	O	D	A	Y	D*	N*

(c)

*The letters D and N are recognized as nulls.

Figure 6.

REF ID:A56932

bers, the rectangle shown in (a) of figure 6 is prepared and then the columns (of cells) are filled in numerical order. An early stage in the decryptographing is represented in (b) of figure 6. It is only after the process has been finished that the complete message reappears, as shown in (c) of figure 6.

c. The method indicated above may vary considerably by changing (1) the key word, (2) the route followed in inscribing the letters of the plain text, and (3) the route followed in transcribing them to form the cipher text. A change in key daily, or oftener, is possible; or, by drawing up a whole list of daily keys for a given period, automatic change in key can be provided for without indicating in the cryptograms the applicable key. It is also possible to prepare a long list of suitable keys and to designate each key by an *indicator* inserted in the cryptogram in a prearranged position. Indicators may be words, numbers, groups of letters, or single letters. For example, each key in a list of 500 may be indicated by a single pair of letters inserted at the beginning, at the end, or at any prearranged position of the cryptogram. This procedure has a disadvantage, however: if an error occurs at the particular position of the cryptogram containing the indicator, the decryptographing is made difficult if not impossible. For this reason indicators, if used, are often inserted in at least two positions in the cryptogram, usually at or near the beginning and end.

d. The letters of the plain text may be inscribed in the rectangle according to any one of the routes indicated in figure 1. If the transcribing process is accomplished by reading whole columns or whole rows, according to a prearranged plan which follows a route perpendicular to the inscribing route (except in the case of spiral inscription), the decryptographing process is simple. Only certain of the simpler combinations of inscription and transcription are suitable for military use, the most practicable being those illustrated in figures 5 and 6.

28. Columnar Transposition with Incompletely Filled Rectangles

a. The degree of cryptographic security of columnar transposition is much increased if the rectangle is *not completely filled.* It is impossible to go into the reasons for this increased security without demonstrating solutions; suffice it to say that the solution will be more difficult than would be suspected if one or more cells are vacant in the last row of the rectangle. An example of cryptographing and decryptographing is shown in figure 7.

b. To decryptograph such a cryptogram one must first count the number of letters in the text and then outline on cross-section paper a rectangle which will exactly contain the message, crossing off the cells which must remain vacant. In the foregoing example, the text contains 30 letters and, since the key contains 7 letters, the outlined rectangle is as

REF ID:A56932

shown in figure 8 of (a). From the complete rectangle $7 \times 5 = 35$ cells, 5 cells must remain vacant at the end.

c. The cipher text is then inserted in key-number order, the result of inserting the first two groups of the text being shown in (b), figure 8. It is only after the process has been finished that the complete message becomes apparent.

Message:

REQUEST IMMEDIATE REENFORCEMENTS

Key word: P – R – O – D – U – C – T
Numerical key: 4 – 5 – 3 – 2 – 7 – 1 – 6

R	E	Q	U	E	S	T
I	M	M	E	D	I	A
T	E	R	E	E	N	F
O	R	C	E	M	E	N
T	S					

Cryptogram:

SINEU EEEQM RCRIT OTEME RSTAF NEDEM

Figure 7.

Cryptogram:

SINEU EEEQM RCRIT OTEME RSTAF NEDEM

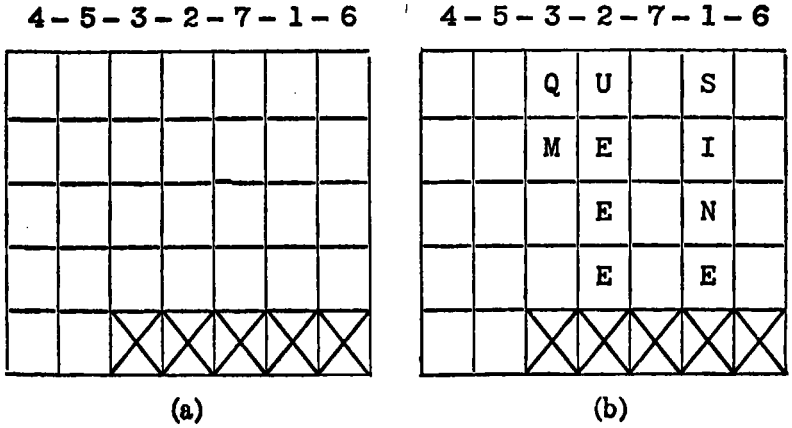


Figure 8.

REF ID:A56932

29. Modification of Columnar Method

A variation of the columnar procedure, but one that produces exactly the same results, may be found useful. First, write the message in groups corresponding to the length of the key. Thus, using the same key and message as in paragraph 28, the following is obtained:

```
4-5-3-2-7-1-6 | 4-5-3-2-7-1-6 | 4-5-3-2-7-1-6 | 4-5-3-2-7-1
R E Q U E S T | I M M E D I A | T E R E E N F | O R C E M E
4-5
T S
```

The letters are then taken from the groups and are transcribed in groups of five, all letters marked 1 being taken first, then all those marked 2, and so on. Thus, the first two cipher text groups are SINEU EEEQM, and the complete text is identical with that produced in figure 7.

30. Addition of Nulls to Complete a Final Group

The example given in the preceding case happened to contain 30 letters, a number that is an exact multiple of five. Thus, the final group in the cryptogram automatically became a complete group. For accuracy, the final group of every message should be complete; therefore, if the number of letters in the text of a message is not a multiple of five, it should be made so by the addition of nulls, *before* the transposition process is applied (see par. 23*b*).

Section III. MISCELLANEOUS TRANSPOSITION METHODS

31. Transposition Systems Employing Special Designs

a. Triangles, trapezoids, and other polygons are among the many designs used to produce transposition ciphers. Most of them, however, are impractical for wide military use but are used occasionally by secret agents.

b. A grille is a common transposition device of some practical importance. There are several types and one of the most common is that known as the *rotating* grille. It is usually made of a square sheet of cross-section paper from which cells have been cut in definite but apparently irregular positions. The grille is superimposed on another sheet of cross-section paper of the same dimensions and the letters of the message are written in the cells exposed by the perforations. Usually the grille is then given a 90° turn clockwise or counterclockwise, as agreed, and the fresh cells exposed by the perforations are filled with the next few letters of the text. If the grille has been prepared properly it is possible to give it four turns of 90° each, at the end of which all the cells on the under sheet of cross-section paper are occupied by letters. The grille is then removed and the letters of the sheet underneath it are transcribed in accordance with some prearranged route to form the cipher text. Natur-

REF ID:A56932

ally, the correspondents must have identical grilles and every step must be definitely prearranged. Although it is possible to construct grilles with many different arrangements of perforations, the necessity for carrying the device on the person, and the many agreements and understandings necessary for its successful operation make the method hardly suitable for field military use. Furthermore, practical difficulties connected with the preparation and distribution of many grilles would make it almost inevitable that several messages would be enciphered by the same grille. The degree of cryptographic security afforded by them is not so great as may be suspected; sometimes single messages of fair length may be solved.

32. Polyliteral and Word Transposition

a. Thus far only individual letters, as units for the transposition process have been discussed. It is possible to use pairs of letters, sets of three or more letters, or entire words as units; procedures are the same in monoliteral and polyliteral transpositions. Sometimes more complicated routes may be followed in transposition; for example, a route may be a prearranged succession of moves made by a knight in chess. It is usually necessary to have at hand a printed form showing the complete route, and this makes these methods impractical for field use. They may, however, be used in special cases.

b. The cipher system used by the Federal Army in the Civil War represents a good example of word transposition. In the earliest form in which this cipher was used by the Federals only one route was used, which consisted in writing the text in six columns, going up the sixth, down the first, up the fifth, down the second, up the fourth, and down the third. Arbitrary words were substituted for proper names, nulls were introduced at regular positions, and words even often misspelled for further obscurity. For example, the word "operation" was often spelled as two words: "opera," and "shun." Later, many additional routes were provided, relatively long lists of arbitrary equivalents for names, numbers, dates, common military terms, etc., were added, and the whole system was made considerably more complicated. While the security afforded by this system was probably ample for those days, it would hardly be sufficient today to permit its use even in cases where a delay of only a few hours is required. Furthermore, if long lists of arbitrary equivalents must be handled, the system presents all the disadvantages of a poor cipher system with but few of the advantages offered by a good code system.

33. Single and Double Transposition Methods

In single transposition methods the letters go through only one transposition from plain text to cipher text. It is possible to take the letters

REF ID:A56932

resulting from a first transposition and apply a second transposition to them; cryptograms so prepared often present a very great degree of security. Triple and quadruple transposition is possible but wholly impracticable for common use. Only a very limited number of double transposition methods are practicable for military use, but the degree of security afforded by certain of them is much greater than that afforded by certain much more complicated substitution methods.

34. Factors Concerning Use of Transposition Systems

a. The transposition methods described above provide a wide range of cryptographic security; in some there is very little security, in others there is a great deal. All transposition systems usually present important advantages in speed and simplicity. These advantages have led to attempts to increase security in some manner or other; double transposition schemes, rotating grilles, and other more complicated methods have consequently been developed. In only certain types are written memoranda or devices required. Very often the entire cryptographing process in even very complex methods may be easily memorized by persons of very good intelligence, such as secret agents. For these reasons transposition systems are often useful in espionage and counterespionage activities.

b. But transposition ciphers for military usage present three very serious disadvantages. In the first place, the methods are such that they do not allow any latitude for errors in handling. Often if a single letter is omitted or added, as not infrequently happens in telegraphic transmission, the whole message becomes difficult if not impossible to decryptograph. In the second place, if two or more messages prepared in the same key and *containing exactly the same number of letters* are available for study, no matter how complicated the method employed, the cryptograms can be solved, and the key recovered, and applied to other cryptograms in the same key but with different numbers of letters. In military cryptography it is not unusual, in cases of heavy traffic, to have as many as 100 or 200 messages transmitted on the same day, all in the same key. Control from a central headquarters of the exact message length would obviously be impossible. The chances, therefore, that the enemy may actually intercept and find several messages of identical length are not negligible. Thus, a transposition method presenting an extremely high degree of cryptographic security when only a few messages are to be cryptographed fails seriously when employed for heavy traffic. Finally, in certain cases, where the double transposition produces a great degree of security, it is almost inevitable that a poorly trained or careless cryptographic clerk will fail to perform both steps correctly. Not only messages prepared by one poor or careless operator, but all other messages, even though correctly prepared, are thus laid open to solution.

REF ID:A56932

CHAPTER 3
ELEMENTARY SUBSTITUTION SYSTEMS

Section I. GENERAL

35. Fundamental Nature of Substitution Methods, Cipher Systems and Code Systems

Methods now to be described differ from those above in that elements or textual units composing the original plain text retain their relative positions, but not their identities, and are replaced by other elements or textual units so that the external form of the writing is cryptographic in nature. For this reason these methods are called *substitution methods.* They may deal with individual letters, pairs of letters, sets of letters in regular groups, syllables, whole words, phrases, and sentences. Substitution methods may accordingly be subdivided into *letter methods, syllable methods,* and *word methods,* as in the case of transposition methods; but such a classification is a rather arbitrary one and is not based on the nature, form, or external appearance of the cryptographic text. For example, a substitution method dealing with single letters of the plain text may not involve their replacement by other single letters. In some cases whole words may be used to replace single letters. Outwardly, such a cryptogram gives the appearance of dealing with words, but its internal nature is quite clear: single-letter substitution has been effected. The classification indicated is, nevertheless, a useful one. When the cryptographic process involves the treatment of individual letters or pairs of letters, and only exceptionally the treatment of syllables or whole words, the method is known as a *substitution cipher system;* and when the process involves the treatment of whole words, phrases, or sentences, and only exceptionally the treatment of individual letters, groups of letters, or syllables, the method is known as a *code system,* because it usually necessitates the use of a *code book.*

36. Nature of Alphabets

a. The simplest kind of substitution cipher is that which is known in literature as Julius Caesar's Cipher, but which, as a matter of fact, was a favorite long before his day. In this cipher each letter of the text of a message is replaced by the letter standing the third to the right of it in the ordinary alphabet; the letter A is replaced by D, the letter B by E, and so on. The word CAB becomes converted into FDE which is cipher.

REF ID:A56932

b. The English language is written by means of 26 simple characters called *letters* which, taken together and considered as a *sequence of symbols,* constitute the *alphabet* of the language. Not all systems of writing are of this nature. Chinese writing is composed of about 44,000 complex characters, each representing one sense of a word. Whereas English words are composite or polysyllabic and may consist of one to eight or more syllables, Chinese words are all monosyllables and each monosyllable is a word. Written languages of the majority of other civilized peoples of today are, however, alphabetic and polysyllabic in construction, so that principles discussed here apply to all of them.

c. The letters composing the English alphabet used today are the results of a long period of evolution, the complete history of which may never fully be known. They are conventional symbols representing *elementary sounds,* and any other simple symbols, so long as the sounds which they represent are agreed upon by those concerned, will serve the purpose equally well. If taught from early childhood that the symbols $, *, and @ represent the sounds "Ay," "Bee," and "See," respectively, the combination @$* would still be pronounced CAB, and would, of course, have exactly the same meaning as before; or suppose that two persons have agreed to change the sound values of the letters, F, G, and H, and after long practice have become accustomed to pronouncing them as "Ay," "Bee," and "See," respectively. They would then write the "word" HFG, pronounce it CAB, and see nothing strange whatever in the matter. But to others not party to their arrangements HFG constitutes cipher. The combination of sounds called for by this combination of symbols is perfectly intelligible to the two who have adopted the new sound values for those symbols and therefore pronounce HFG as CAB, but HFG is utterly unpronounceable and wholly unintelligible to others who are reading it according to their own long established sound-symbol basis. It would be stated that there is no such word as HFG, which would mean merely that the particular combination of sounds represented by this combination of letters has not been adopted by convention to represent a thing or an idea in the English language. Thus it is seen that, in order for the written words of a language to be pronounceable and intelligible to all who speak that language, it is necessary, first, that the sound values of the letters or symbols be universally understood and agreed upon and, secondly, that the particular combination of sounds denoted by the letters should have been adopted to represent a thing or an idea. Spoken plain language consists of vocables; that is, combinations and permutations of elementary speech-sounds which have by long usage come to be adopted and recognized as representing definite things and ideas. Written plain language consists of *words;* that is, combinations and permutations of simple symbols, called letters, which represent visually and call forth vocally the elementary speech-sounds of which the spoken language is composed.

REF ID:A56932

d. It is clear also that in order to write a polysyllabic language with facility it is necessary to establish and to maintain by common agreement or convention, equivalency between *two* sets of elements, first, a set of elementary sounds and, second, a set of elementary symbols to represent the sounds. When this is done the result is what is called an *alphabet,* a word derived from the names of the first two letters of the Greek alphabet, "alpha" and "beta."

e. Theoretically, in an ideal alphabet each symbol or letter would denote only one elementary sound, and each elementary sound would invariably be represented by the same symbol. But such an alphabet would be far too difficult for the average person to use. It has been conservatively estimated that a minimum of 100 characters would be necessary for English alone. Attempts toward producing and introducing into usage a practical, scientific alphabet have been made, one being that of the Simplified Spelling Board in 1928, which advocated a revised alphabet of 42 characters. Were such an alphabet adopted into current usage, in books, letters, telegrams, etc., the flexibility of cryptographic systems would be infinitely extended and the difficulties set in the path of the enemy cryptanalysts vastly increased. The chances for its adoption in the near future are, however, quite small. Because of the continually changing nature of every living language, it is doubtful whether an original perfect alphabet could, over any long period of time, remain so and serve to indicate with great precision the exact sounds which it was originally designed to represent.

37. Normal Alphabets and Cipher Alphabets

a. In the study of cryptography the dual nature of the alphabet becomes apparent. It consists of two parts or components, (1) an arbitrarily arranged sequence of symbols.

b. The ***normal alphabet*** for any language is one in which these two components are the ordinary sequences that have been definitely fixed by long usage or convention. The dual nature of our normal or everyday alphabet is often lost sight of. When we write A, B, C, . . . we really mean:

Sequence of sounds:	"Ay"	"Bee"	"See"	. . . .
Sequence of symbols:	A	B	C	. . . .

Normal alphabets of different languages vary considerably in the number of characters composing them and the arrangement or sequence of the characters. The English, Dutch, and German alphabets each have 26, the French 25, the Italian 21, Spanish 27 (including the digraphs *ch* and *ll*), Russian 31. The Japanese language has a syllabary consisting of 72 syllabic sounds, to express which 48 characters are employed.

c. A ***cipher alphabet*** or a ***substitution alphabet,*** as it is sometimes called, is one in which the elementary speech-sounds are represented by

REF ID:A56932

characters other than those representing them in the normal alphabet. These characters may be letters, figures, signs, symbols, or combinations of them.

d. A more technical definition of a familiar cipher may now be given: When the plain text of a message is converted into encrypted text by the use of one or more cipher alphabets, the resultant cryptogram constitutes a *substitution cipher.*

38. Two Components of an Alphabet

It is convenient to designate that component of a cipher alphabet constituting the sequence of speech-sounds the *plain component,* and the component constituting the sequence of symbols the *cipher component.* If the plain component is omitted in a cipher alphabet, the latter is understood to be the normal sequence. For brevity and clarity, a letter of the plain text, or of the plain component of a cipher alphabet, is designated by suffixing a small letter "p" to it: A_p means A of the plain text, or of the plain component of a cipher alphabet. Similarly, a letter of the cipher text, or of the cipher component of a cipher alphabet, will be designated by suffixing a small letter "c" to it: X_c means X of the cipher text, or of the cipher component of a cipher alphabet. The expression $A_p = X_c$ means that A of the plain text, or A of the plain component of a cipher alphabet, is represented by X in the cipher text, or by X in the cipher component of a cipher alphabet.

39. Standard and Mixed Cipher Alphabets

In the arrangement or sequence of letters forming its cipher component, cipher alphabets are of two kinds:

a. Standard cipher alphabets, in which the sequence of letters in the cipher component is the same as the normal, but reversed in direction or shifted from its normal point of coincidence with the plain component.

b. Mixed cipher alphabets, in which the sequence of letters or characters in the cipher component is no longer the same as the normal in its entirety.

40. Enciphering and Deciphering Alphabets

All cipher alphabets may be classified on the basis of their arrangement as *enciphering* or *deciphering* alphabets. An enciphering alphabet is one in which the sequence of letters in the plain component coincides with the normal sequence, and is arranged in that manner for convenience in encipherment. In a deciphering alphabet the sequence of letters in the cipher component coincides with the normal, for convenience in deciphering. For example, in figure 9, (a) shows a mixed cipher alphabet arranged as an enciphering alphabet; (b) shows the corresponding

REF ID:A56932

deciphering alphabet. An enciphering alphabet and its corresponding alphabet present a *verse and inverse* relationship to each other. To invert a deciphering alphabet is to write the corresponding enciphering alphabet; to invert an enciphering alphabet is to write the corresponding deciphering alphabet.

Enciphering Alphabet

(a)
Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: JKQVXZWESTRNUIOLGAPHCMYBDF

Deciphering Alphabet

(b)
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: RXUYHZQTNABPVLOSCKIJMDGEWF

Figure 9.

Section II. MONOALPHABETIC SUBSTITUTION SYSTEMS

41. Single-Alphabet Substitution

If a message is enciphered, letter-for-letter, by using one cipher alphabet which has been drawn up for the purpose, the resulting cryptogram is said to be enciphered by a single alphabet and to be a single-alphabet, or *monoalphabetic,* substitution cipher. More complex ciphers may use several alphabets in the enciphering of a single message. When two or more cipher alphabets are used, the resulting cryptogram is said to be a *polyalphabetic* cipher.

42. Standard Alphabet Ciphers

a. Standard cipher alphabets are of two sorts:

(1) *Direct standard,* in which cipher component is the normal sequence but shifted to the right or left of its point of coincidence in the normal alphabet. Example:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: QRSTUVWXYZABCDEFGHIJKLMNOP

It is obvious that the cipher component can be applied to the plain component at any one of 26 points of coincidence, but since the alphabet that results from one of these applications coincides exactly with the normal alphabet, a series of only 25 (direct standard) cipher alphabets results from the shifting of the cipher component.

REF ID:A56932

(2) *Reversed standard,* in which the cipher component is also the normal sequence but runs in the opposite direction from the normal. Example:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: QPONMLKJIHGFEDCBAZYXWVUTSR

Here the cipher component can be applied to the plain component at any of 26 points of coincidence, each yielding a different cipher alphabet. There is in this case, therefore, a series of 26 (reversed standard) cipher alphabets.

b. It is often convenient to refer to or designate one of a series of cipher alphabets without ambiguity or circumlocution. The usual method is to indicate the particular alphabet to which reference is made by citing a pair of equivalents in that alphabet. For example, the reversed alphabet above, one of a series of 26 related alphabets, may be designated as that in which $L_p = F_c$ or $W_p = U_c$. But the most common basis of reference is the letter which represents the first or initial letter of the plain component, usually A_p. Thus, the key for the cipher alphabet just referred to, as well as that preceding it, is $A_p = Q_c$, and it is said that the key letter for the cipher alphabet is Q_c.

43. Reciprocal Alphabets

a. The cipher alphabet in paragraph 42*a* (2) is also a *reciprocal alphabet;* that is, the equivalents show reciprocity and are reversible or reciprocal in pairs. For example, in the alphabet referred to, $A_p = Q_c$ and $Q_p = A_c$; $B_p = P_c$ *and* $P_p = B_c$, etc. The reciprocity exists throughout the alphabet and is a result of the method by which it was formed.

b. A series of related reciprocal alphabets may be derived by juxtaposing at all possible points of coincidence two components which are identical but progress in opposite directions. This holds regardless of whether the components are composed of an even or an odd number of elements. The reciprocal alphabet (par. 42*a* (2)) is one of such a series of 26 alphabets.

c. A single or isolated reciprocal alphabet may be produced in one of two ways:

(1) By constructing a complete reciprocal alphabet by arbitrary or random assignments of values in pairs. That is, if A_p is made K_c, then K_p is made A_c; if B_p is made R_c, then R_p is made B_c, and so on. If the two components thus constructed are slid against each other no additional reciprocal alphabets will be produced.

(2) By juxtaposing a sequence comprising an *even* number of elements against the same sequence shifted exactly half way to the right (or left), as seen below;

REF ID:A56932

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

d. A reciprocal alphabet is an inverse alphabet, since it may serve either as an enciphering or deciphering alphabet.

44. Procedure in Encipherment and Decipherment

a. When a message is enciphered monoalphabetically, that is, by means of a single cipher alphabet, letters of the text are replaced by the equivalents in the cipher alphabet selected by prearrangement. Example:

Message: THREE MACHINE GUNS CAPTURED.
Enciphering Alphabet: Reversed Standard, $A_p = D_c$
Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: DCBAZYXWVUTSRQPONMLKJIHGFE
Letter-for-letter encipherment:

THREE MACHINE GUNS CAPTURED
KWMZZ RDBWVQZ XJQL BDOKJMZA

The cipher text is then grouped in fives and the indicator letter D[6] inserted as the initial letter of the first group (or any other prearranged group).

Cryptogram:

DKWMZ ZRDBW VQZXJ QLBDO KJMZA

Figure 10.

b. The procedure in decipherment is merely the reverse of that in encipherment. The initial letter of the message, D, indicates $A_p = D_c$ in the cipher alphabet. The deciphering alphabet is therefore as follows:

Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: DCBAZYXWVUTSRQPONMLKJIHGFE
The message deciphers thus:
Cipher: (D) KWMZ ZRDBW VQZXJ QLBDO KJMZA
Plain: THRE EMACH INEGU NSCAP TURED

The deciphering clerk rewrites the text in word lengths:

THREE MACHINE GUNS CAPTURED

c. When a mixed alphabet is used, the enciphering and deciphering processes are the same as those described under *a* and *b* above. For speed in cryptographing, the cipher alphabet is prepared in the form of an enciphering alphabet, and for speed in decryptographing, in the form of a deciphering alphabet.

[6] If this or any such similar convention has been agreed upon by the correspondents.

REF ID:A56932

Section III. TYPES OF MIXED CIPHER ALPHABETS

45. Systematically Mixed Cipher Alphabets

It will be recalled that in a mixed cipher alphabet the sequence of letters or characters in the cipher component does not correspond to the normal sequence. There are various methods of mixing up the letters of the cipher component, and those which are based upon a scheme that is systematic in its nature are very useful because they make possible the derivation of one or more mixed sequences from any easily remembered word or phrase, and thus do not necessitate the carrying of written memoranda. They are called *systematically mixed cipher alphabets.*

46. Key-word Mixed Alphabets

a. One of the simplest types of systematically mixed cipher alphabets is the *key-word mixed alphabet.* The cipher alphabet consists of a key word or phrase (with repeated letters, if present, omitted after their first occurrence), followed by the letters of the alphabet in their normal sequence (with letters already occurring in the key, of course, omitted). Example, with GOVERNMENT the key word:

Enciphering alphabet....
Plain: ABCDEFGHIJKLMNOPQRTSUVWXYZ
Cipher: GOVERNMTABCDFHIJKLPQSUWXYZ

b. Mixed alphabets formed by including all repeated letters of the key word or key phrase were common in Edgar Allan Poe's day but are impractical because they make decipherment difficult.

Enciphering alphabet....
Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: NOWISTHETIMEFORALLGOODMENT

Deciphering alphabet....
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: P VHMSGD QKAB OEF C
L J RWYN I
X T Z
U

The average cipher clerk would have considerable difficulty in decryptographing a cipher group such as TOOET, each letter of which has three or more equivalents, and from which the plain-text words (N) INTH, ..FT THI (S), IT THI . . . , etc., can be formed on decipherment.

c. An example of a key-word mixed alphabet is shown in figure 9, where, in its enciphering form, the cipher component presents to the experienced eye the skeleton of the key upon which the alphabet is based: WESTERN UNION TELEGRAPH COMPANY. Any easily remembered word, phrase, or sentence may be used. The starting point of the sequence, when used as a cipher component, may be indicated in the usual manner. For example, in the alphabet referred to, the

REF ID:A56932

alphabet key is $A_p = J_c$. Two or more correspondents using the prearranged key, WESTERN UNION TELEGRAPH COMPANY, would obtain the same disarranged sequence; when this sequence is to form the cipher component of a cipher alphabet, the prearranged key letter $A_p = J_c$ would result in giving each correspondent exactly the same cipher alphabet. The key words or phrases need not consist of any definite number of letters, but it is advisable to use for keys such words or phrases as will most thoroughly disarrange the normal sequence. (See, in this connection, par. 26.) A key-word mixed alphabet will manifest the key word or parts of it only when the alphabet is in the form of an enciphering alphabet. Note that alphabet (b) of figure 9 no longer gives any external evidence of having been derived from the phrase WESTERN UNION TELEGRAPH COMPANY.

47. Transposition-mixed Alphabets

a. It is possible to disarrange the sequence even more thoroughly by applying a simple method of transposition to the key-word sequence as if it were a message. An example is illustrated in figure 11.

Key word:

TELPHONY

(a) Simple columnar transposition:

TELPHONY
ABCDFGIJ
KMQRSUVW
XZ

Mixed sequence:

TAKXEBMZLCQPDRHFSOGUNIVYJW

(b) Numerical key, columnar transposition:

7-1-3-6-2-5-4-8
T E L P H O N Y
A B C D F G I J
K M Q R S U V W
X Z

Mixed sequence:

EBMZHFSLCQNIVOGUPDRTAKXYJW

Figure 11.

b. The last two systematically mixed cipher alphabets are *transposition-mixed alphabets.* Almost any of the methods of transposition described in sections IV and V of this chapter may be applied to them.

REF ID:A56932

48. Decimation Method of Forming Mixed Alphabets

Another simple method of forming a mixed alphabet is the *decimation method.* In this method, letters in the normal alphabet, or in a key-word mixed alphabet, are "counted off" according to a selected odd interval. As each letter is decimated—that is, eliminated from the basic alphabet by counting off—it is entered in a separate list to form the sequence of the mixed alphabet. For example, to form a mixed alphabet by this method from an alphabet based on the key phrase SING A SONG OF SIX PENCE with 7 the interval selected, proceed as follows:

a. Key-word (or basic) alphabet:

SINGAOFXPECBDHJKLMQRTUVWYZ

b. When the letters are counted off by 7's from left to right, F will be the first letter arrived at, H the second, T the third:

S I N G A O F X P E C B D H J K L M Q R T U V W Y Z
1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7

Fig. B

These letters are entered in a separate list (F first, H second, T third, etc.) and eliminated from the key-word alphabet.

c. When the end of the key-word alphabet is reached, return to the beginning, skipping the letters already eliminated:

S I N G A O F X P E C B D H J K L M Q R T U V W Y Z
6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5

Fig. C

d. Mixed alphabet.

FHTIEMZPQNDWCVBSLXAGOKYJRU

49. Random-Mixed Alphabets

Practical considerations, of course, set a limit to the complexities that may be introduced in constructing systematically mixed alphabets. Beyond a certain point there is no object in further mixing. The greatest amount of mixing by systematic processes will give no more security than that resulting from mixing the alphabet by random selection, such as by putting the 26 letters in a box, thoroughly shaking them up, and then drawing the letters out one at a time. Whenever the laws of chance operate in the construction of a mixed alphabet, a thorough disarrangement is bound to be produced. Random-mixed alphabets give more cryptographic security than do the less complicated systematically mixed alphabets because they afford no clues to positions of letters, given the

REF ID:A56932

positions of a few of them. Their chief disadvantage is that they must be reduced to writing, since they cannot readily be remembered, nor can they be reproduced at will from an easily remembered key word.

50. Number of Single Alphabets Available from a Basic Alphabet

It is obvious that the cipher component of a cipher alphabet may be shifted or slid against the plain component at 26 points of contact so as to produce a series of different enciphering alphabets. For example, the mixed sequences given under (b) of figure 11, when used as a cipher component, yields the following two of a series of 26 cipher alphabets:

Enciphering Alphabets

(1)
Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: EBMZHFSLCQNIVOGUPDRTAKXYJW

(2)
Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: WEBMZHFSLCQNIVOGUPDRTAKXYJ

The message DAILY REPORT NOT RECEIVED YET would be enciphered by the first alphabet as:

Plain: DAILY REPOR TNOTR ECEIV EDYET
Cipher: ZECIJ DHUGD TOGTD HMHCK HZJHT

and by the second alphabet as:

Plain: DAILY REPOR TNOTR ECEIV EDYET
Cipher: MWLNY PZGOP RVORP ZBZLA ZMYZR

Externally the two cryptograms seem different except in length. The two enciphering alphabets present the same sequence in the cipher component, but this entirely disappears in the corresponding deciphering alphabets, which are as follows:

Deciphering Alphabets

(1)
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: UBIRAFOELYVHCKNQJSGTPMZWXD

(2)
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: VCJSBGPFMZWIDLORKTHUQNAXYE

It is possible to write the same message in 25 different external forms, each using a different cipher alphabet of a series derivable from a basic sequence. The basic sequence or alphabet in such a case is often called a *primary sequence* or a *primary alphabet;* derived alphabets are called *secondary alphabets.* In producing secondary alphabets the basic sequence must be juxtaposed and slid against itself, or against the normal sequence, or against another mixed sequence. In all cases secondary alphabets form a series of alphabets that are interrelated and

REF ID:A56932

that either directly or indirectly manifest relationships which are important from a cryptanalytic point of view. It should be clear now that by means of a single, prearranged, secret word it is possible for two correspondents to send a whole set of messages all in different mixed alphabet, or to use a different alphabet for each of 26 consecutive days.

51. Miscellaneous Types of Cipher Alphabets

a. The cipher alphabets shown thus far have used only letters, but alphabets in which the cipher component consists of figures, or groups of figures, are not uncommon in military cryptography. Cipher alphabets using signs and symbols are not suitable for military cryptography because they can neither be telegraphed nor telephoned with any degree of accuracy, speed, or facility. Since there are but ten digits it is obvious that, in order to represent a complete alphabet in figure ciphers, combinations of at least two digits are necessary. The simplest kind of such an alphabet is that in which $A_p = 01$, $B_p = 02$, . . . $Z_p = 26$.

	1	2	3	4	5	6	7	8	9	0
1	A	B	C	D	E	F	G	H	I	J
2	K	L	M	N	O	P	Q	R	S	T
3	U	V	W	X	Y	Z	.	,	:	;

Figure 12.

b. Instead of a simple alphabet of the preceding type, it is possible to use a simple diagram of the type shown in figure 12. Here the digits at the side and top of the rectangle are used to designate, according to the coordinate system, the cell occupied by each letter and punctuation mark within the rectangle. When used for such purposes, the figures (or letters) constituting coordinate elements are referred to as ***row and column indicators***. It is usually necessary to agree beforehand upon which indicator will be given as the first half of the equivalent for a letter, the row indicator or the column indicator, in order to avoid ambiguity or error. In all of the systems to be described here, the row indicator will always form the first half of an equivalent. Accordingly in figure 12, the letter $A_p = 11$, $B_p = 12$, and so forth.

c. A variation of the foregoing diagram is exemplified in figure 13. Here, letters of the alphabet are inserted in the 25 cells of a large square, I and J being written together in one cell. Then a key word of five letters is applied to the top of the large square and the same or a different key word is applied to the side of the square to form column and row indicators. In figure 13, for example, S_p = TI; W_p = EH; etc.

REF ID:A56932

(2)

(1)		W	H	I	T	E
	W	A	B	C	D	E
	H	F	G	H	I–J	K
	I	L	M	N	O	P
	T	Q	R	S	T	U
	E	V	W	X	Y	Z

Figure 13.

The message RAIDERS HAVE GONE is enciphered thus:

Plain: R A I D E R S H A V E G O N E
Cipher: TH WW HT WT WE TH TI HI WW EW WE HH IT II WE

The cryptogram is then transmitted in groups of five letters:

Cryptogram: THWWH TWTWE THTIH IWWEW WEHHI TIIWE

d. In these two systems just described,

(1) The letters of the alphabet within the square or rectangle may be fixed in a mixed sequence, either systematically or random-mixed sequences being possible.

(2) The column and row indicators may be the same, or different; when letters are used they may form a key word or they may not; the key words, if formed, may be identical or nonidentical.

e. When letters are used as column and row indicators, they may be selected so as to result in producing cipher text that resembles "made-up words," that is, words composed of regular alternations of vowels and consonants. For example, if in figure 13 the row indicators consisted of the vowels A E I O U in this sequence from the top down, and the column indicators consisted of the consonants B C D F G in this sequence from left to right, the word RAIDS would be enciphered as OCABE FAFOD, which very closely resembles code of the type formerly called artificial code language. Such a system may be called a *false,* or *pseudo-code* system.[7]

[7] Prior to 1934, International Telegraph Regulations required code words of five letters to contain at least one vowel and code words of ten letters to contain at least three vowels. The Madrid Conference held in 1932 amended these regulations to permit the use of code groups containing any combination of letters. These unrestricted code groups were authorized for use after 1 January 1934.

REF ID:A56932

Section IV. MONOALPHABETIC SUBSTITUTION WITH VARIANTS

52. Purpose of Providing Variant Values

The individual letters composing ordinary intelligible plain text are used with varying frequencies; some, such as (in English) E, T, R, I, and N, are used much more often than others, such as J, K, Q, X, and Z. In fact, each letter has a *characteristic frequency* by means of which definite clues are afforded in the solution of simple substitution ciphers. This has led cryptographers to devise methods for disguising, suppressing, or eliminating the characteristic frequencies manifested by the letters of cryptograms produced by simple monoalphabetic substitution. One such method is that in which the letters of the plain component of the cipher alphabet are assigned two or more equivalents in the cipher component and they are, for this reason, called *variant values*. In some cases the letters of the plain component receive numbers of variant values, or variants, in proportion to their normal frequencies; in other cases, all the letters receive equal numbers of variant values, determined by the total number available.

53. Figure Ciphers with Variant Values

a. The use of figures in pairs as substitution equivalents makes available a total of 100 different pairs, those from 00 to 99. They may all be used in a complete system, or only certain ones may be selected, as prearranged.

b. One of the most common varieties of ciphers using all the pairs of digits is that in which the alphabet is reduced to 25 letters (by making I and J interchangeable or by eliminating a letter such as Q), and each letter is assigned four values which may be used at will. The assignment of values may be based upon a key word of four letters, each of which designates the starting points of a *normal sequence* of 25 numbers. An example is shown in figure 14, wherein the key word is TRIP. This means that in the first set of numbers, 01 to 25, the first number, 01, is assigned to the letter T; in the second set, from 26 to 50, the first number, 26, is assigned to the letter R; in the third set, from 51 to 75, the first number, 51, is assigned to the letter I; finally, in the last set, from 76 to 00, the first number, 76, is assigned to the letter P.

The letter A_p may be represented by any one of four equivalents, 08, 35, 68, and 87; the letter B_p by 09, 36, 69, 88; and so on. The equivalent used in any particular instance is selected at random, so that the word CAB may be represented in cipher by any one of a total of 64 combinations, such as 10–08–09, 70–35–09, 37–08–69, etc. In the final cryptogram

REF ID:A56932

the figures may be run together in groups of five. The cipher group 10080, on deciphering, would be split up into 10–08–0.

A—08 35 68 87	I–J—16 43 51 95	S—25 27 60 79
B—09 36 69 88	K—17 44 52 96	T—01 28 61 80
C—10 37 70 89	L—18 45 53 97	U—02 29 62 81
D—11 38 71 90	M—19 46 54 98	V—03 30 63 82
E—12 39 72 91	N—20 47 55 99	W—04 31 64 83
F—13 40 73 92	O—21 48 56 00	X—05 32 65 84
G—14 41 74 93	P—22 49 57 76	Y—06 33 66 85
H—15 42 75 94	Q—23 50 58 77	Z—07 34 67 86
	R—24 26 59 78	

Figure 14.

c. In this case, within each set of 25 the numbers progress serially, each set being treated as a ring or circle. It is of course possible to mix the sequence to destroy this serial progression, thus giving four mixed alphabets which can be used at random.

d. Another variation is to assign each letter a set of numbers in accordance with its relative frequency in ordinary English, so that each of the most frequently used letters such as E, T, R, I, and N will have perhaps seven or eight different equivalents, whereas letters of low frequency such as J, K, Q, X, and Z will each have but one equivalent.

54. Use of Rectangles to Provide Variant Values

a. Instead of drawing up alphabets as in figure 14, it is possible to use the diagram shown in figure 12, but with several variant digits as row indicators instead of a single digit for each row. For example, the row indicators may be of the following arrangements:

1–6–7	1–2–3	1–2–3	5–4–3
2–5–8	4–5–6	8–9–4	6–9–2
3–4–9	7–8–9	7–6–5	7–8–1, etc.

Thus, if the first arrangement is used, A_p would have the equivalents 11, 61, 71; B_p, 12, 62, 72; etc. The word RUN might be represented by any one of 27 different combinations, such as 28–31–24, 28–91–54, etc.

b. A variation of the foregoing system is that in which, by use of a diagram of the type shown in figure 13, a number of different letters are applied to each row and column, or 2-figure numbers may be used for this purpose. In this case a series of as many as 50 pairs of digits may be used as row indicators, and another series of 50 pairs as the column indicators.

c. The use of variants lends itself to application in a pseudo-code system such as described in paragraph 51*e*. It presents many possibilities for

REF ID:A56932

variation, with or without key words, with one or more alphabets distributed within the square or rectangle, with alphabets extended to include figures, punctuation signs, common syllables and words, etc. Some times pseudo-code is encountered when the groups of a numerical cipher system (or a figure-code system) are converted into letters, in order to make the cryptographic text conform to certain telegraph regulations and thus have the message accorded a more favorable rate of charge (sec. II, ch. 4). Thus, a group such as 0125784256 might be converted into the group BAFOSULAFE. If the conversion table is irregular in its construction and is kept secret, this adds an encipherment step to the system.

55. Disadvantages of Monoalphabetic Substitution with Variants

The obvious disadvantage of all such methods discussed in the preceding paragraph is that the cryptographic text is exactly twice as long as the original plain text. Furthermore, there is no compensating advantage from the standpoint of cryptographic security. When methods are such that the cipher equivalents are passed through another process which returns the cipher text to a length identical with that of the equivalent plain text, they are usually too complicated, too slow, and too subject to error to be practical. They are often the result of combining substitution and transposition processes in one system. Methods which substitute three or more characters for one letter of the original text are not at all practical for military cryptography.

Section V. POLYALPHABETIC SUBSTITUTION SYSTEMS

56. Monoalphabetic and Polyalphabetic Substitution

a. In the substitution methods thus far discussed it has been noted that only one cipher alphabet is used in the encipherment of a message, and that as a class they constitute the type of system designated as monoalphabetic substitution. It is true that in certain of the systems monoalphabetic substitution with variant equivalents takes place, there are two or more complete alphabets involved and that these systems may, therefore, with apparently good reason be designated as polyalphabetic substitution. This designation, however, will be seen to be somewhat inaccurate when cases of *true polyalphabetic substitution* come to be studied. The real or essential difference between the two systems may best be made clear by setting forth the primary object in each case.

b. In monoalphabetic substitution with variant values, the object of having different sets of equivalents is to suppress so far as possible by *simple* methods the characteristic frequencies of letters. One such method consists in merely providing one or more different values as cipher

REF ID:A56932

equivalents of the same plain-text letter, or a few different values as equivalents of some of the high-frequency letters. Now there are certain conditions inherent in the method itself, conditions which cannot here be indicated, that result in producing in the cryptograms certain definite clues leading to the rapid establishment, in cryptanalysis, of the equivalence of different variant values. Furthermore, in these systems the varying or alternative equivalents for plain-text letters are subject to the free choice and caprice of the encipherer. If he is careful and conscientious in the work he will actually make use of all the variant values afforded by the system; but if he is slip-shod and hurried in his work, he will use the same equivalent repeatedly rather than take pains and time to refer to his charts, tables, or diagrams to find variants. The result is that the cryptograms based upon these methods are open to easy solution, even when the basic methods are such as would make a solution difficult without the interception of carelessly enciphered messages. What is necessary is a system in which there is established a definite procedure for automatically shifting or changing the cipher alphabets employed in the encipherment of a single message; a method which within certain limits is beyond the momentary whims of cipher clerks, and which to a higher degree makes difficult the establishment of the equivalency of different cipher values. These are the objects of true polyalphabetic substitution systems. The number of such systems is large. Therefore, it will be possible to describe only a few of the more common or typical examples of methods practicable for military use.

c. The three methods (a) simple monoalphabetic substitution, (b) monoalphabetic substitution with variants, and (c) true polyalphabetic substitution, are attended by the following consequences in the plain text cipher relationship, a careful study of which will help to understand their similarities and differences:

(1) Encipherment—

In method (a) each plain-text letter is represented by one and always the same cipher equivalent.

In method (b) and method (c), each plain-text letter is represented by two or more different cipher equivalents, but in method (b) the variations are subject only to the whim of the encipherer, whereas in method (c) the identities of the cipher letters are determined by the positions they occupy in the text.

(2) Decipherment—

In method (a) and method (b), each cipher equivalent represents one and always the same plain-text letter.

In method (c) one and the same cipher equivalent represents two or more different plain-text letters, the identities of which are determined by the positions they occupy in the text.

REF ID:A56932

57. Example of Polyalphabetic Substitution

a. A simple example may be used to illustrate what is meant by true polyalphabetic substitution. Suppose that two correspondents agree upon a numerical key, for example, 74030274, each digit of which means that the plain-text letter to which the digit applies as a key number is to be replaced by the letter that stands a corresponding number of places to the right of it in the normal alphabet. For example, if R is to be enciphered by key number 7, it is to be replaced by Y. The numerical key is written under the letters of the plain-text letter for letter, and is repeated until the whole text is covered. Let the message be REENFORCEMENTS BEING RUSHED. The encipherment of a message is shown in figure 15. For convenience in counting forward (to the right) to find cipher equivalents, a normal alphabet is given at the top of the figure.

Normal alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: REENFORCEMENTS BEING RUSHED
Key: 74030274740302 74740 302747
Cipher: YIEQFQYGLQEQTU IIPRG UUUOIK
The text is then transmitted in *five-letter groups.*
Cryptogram: YIEQF QYGLQ EQTUI IPRGU UUOIK

Figure 15.

b. To decipher such a cryptogram, the clerk writes the numerical key over the cipher letters and then counts backward (to the left) in the normal alphabet as many places as indicated by the key number standing over each letter. Thus:

Normal alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Key: 74030 27474 03027 47403 02747
Cipher: YIEQF QYGLQ EQTUI IPRGU UUOIK
Plain: REENF ORCEM ENTSB EINGR USHED
Message: REENFORCEMENTS BEING RUSHED

Figure 16.

58. Systematizing the Work

The work of encipherment may be materially shortened by systematizing the procedure. Instead of having to write the key over and over again in order to cover the text completely, the text may be written in sets of letters corresponding in length to the length of the key. Thus the text may be written underneath a single appearance of the key in successive short horizontal lines, leaving space between the lines for the insertion of cipher equivalents, as shown in figure 17a. Instead of enciphering the letters

7 4 0 3 0 2 7 4
R E E N F O R C
E M E N T S B E
I N G R U S H E
D

Figure 17a.

REF ID:A56932

by individual, repeated countings, two strips of paper bearing normal alphabets may be juxtaposed in the proper relative positions to encipher a whole *column* of letters at one setting of the strips. Thus, for the first column, with the key number 7, the strips are juxtaposed so that the first letter in the column, viz., R (which is to be represented by the seventh letter to the right of it, and is therefore to be enciphered by Y of the lower strip) is directly above Y, as follows:

Plain:
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ

The equivalents for the rest of the letters of the first column may now be rewritten down in their proper places, reference being made to the alphabet strips to see what the cipher letters should be: $E_p = L_c$; $I_p = P_c$; $D_p = K_c$. For the second column the two alphabet strips are in these relative positions:

Plain:
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ

The cipher equivalents for the second column are: $E_p = I_c$; $M_p = Q_c$; $N_p = R_c$. The process is continued in this manner until all the columns have been enciphered, as shown in figure 17b.

7 4 0 3 0 2 7 4
R E E N F O R C Y I E Q F Q Y G
E M E N T S B E L Q E Q T U I I
I N G R U S H E P R G U U U O I
D K

Figure 17b.

The cipher text is then transcribed in groups of five letters, reading the successive lines in the normal manner, that is, from left to right and from the top downwards, yielding the groups YIEQF, QYGLQ, etc. It is

REF ID:A56932

no more difficult to encipher a message by this systematized procedure than by the longer and slower method of writing the text out in long lines and repeating the key over and over again. What is more important is that the shortened procedure promotes accuracy in encipherment. A few seconds careful checking of the relative positions in which the two alphabet strips are set is all that is required but this checking is very necessary, for if that is wrong all the cipher letters in that column to which this setting applies will be in error.

59. Using Key Words to Indicate Number, Identity, and Sequence of Cipher Alphabets Employed

a. If reference is made to the two settings of alphabet strips in paragraph 58, it will be noted that in the first setting $A_p = H_c$, in the second $A_p = E_c$. If the eight settings of the strips are studied it will be found that the letters which A_p represents successively are H, E, A, D, A, C, H, and E, giving the word HEADACHE. These settings, when first presented in the foregoing description, correspond merely to the numerical key 74030274, but this numerical key is also expressible in terms of letters, which when put together properly spell a word. This is only another way of showing that key words may be employed in this type of substitution as in those previously described. Key words of various lengths and composition may be used, consisting of single words, long phrases, or sentences. In general, the longer the key the greater is the degree of cryptographic security. The method as a whole is often referred to as the *repeating key method.*

b. The number of elements in the key—that is, the number of letters or figures composing it—determines the number of alphabets to be employed. The identity of each element of the key, the specific letter or figure it happens to be, determines specifically which of a set of cipher alphabets pertaining to the whole system will be used. And the specific sequence or relative order of the elements of the key determines specifically the sequence with which the cipher alphabets are employed within the encipherment. The total number of cipher alphabets pertaining to or composing the system may be limited or unlimited. When they are produced as a result of the sliding of two basic or primary alphabets against each other, the number is limited to 26 in the English alphabet.

c. A brief notation for indicating or designating a specific key letter is to suffix the subscript "k" to it, just as the subscripts "p" and "c" are suffixed to letters to indicate letters of the plain text or cipher text, respectively. When the key letter occurs in an equation, it can be enclosed within parentheses to avoid ambiguity. Thus, $B_p\ (D_k) = E_c$ means that plain-text letter B when enciphered by key letter D (in a certain alphabet system) yields the cipher letter E.

REF ID:A56932

60. Use of Other Types of Alphabets

a. It has been noted that in the case of monoalphabetic ciphers, alphabets of various types may be employed. This is likewise true of polyalphabetic ciphers. Instead of using two alphabet strips bearing the normal alphabetic sequence to determine the cipher equivalent of a letter enciphered by a given key number or key letter, one may use a pair of strips, one of which bears the normal direct, the other the normal reversed sequence. In the former case one is dealing with direct standard, in the latter, with reversed standard alphabets.

b. Polyalphabetic substitution with direct or reversed standard alphabets does not result in nearly so great a degree of cryptographic security as that resulting from the simple artifice of providing mixed alphabets for the strips. All sorts of mixed alphabets may be used. One of the strips may bear the normal direct or reversed sequence; the other a mixed sequence. Both strips may bear identical mixed sequences proceeding in the same direction, or in opposite directions. Finally, both strips may bear different mixed sequences.

c. In all cases, except where reciprocal alphabets are produced, it is essential that the correspondents agree upon the sequence or strip from which the plain and the cipher letters respectively will be taken, that is, it is necessary to indicate which sequence constitutes the plain component, which the cipher component. If this is not done, two correspondents will have difficulty in deciphering one another's messages. Also, as noted above, it is necessary to agree as to which letter the key letter is to be set against. The usual method is to agree that the initial letter of the plain component, usually A_p, will be set opposite the key letter, though other conventions are possible.

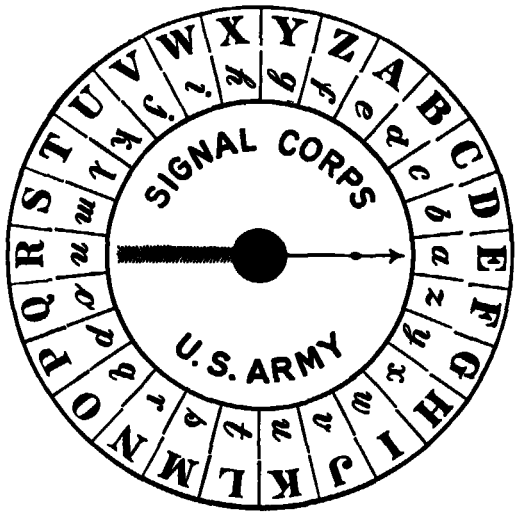
d. The sequences on the strips may be permanent or invariable, but naturally the degree of cryptographic security in this case is considerably lower than if they can be changed easily at the will of the correspondents and by prearrangement. It is possible that a secret word may serve as the basis not only for the key for shifting the strips, but also for the mixing of the alphabetic sequences. For example, two correspondents may agree to use the key CENTRAL AMERICA; to use the first part as the basis for constructing the mixed plain component; the second part, for constructing the cipher component; and to use the whole phrase as the key for enciphering the message. All the methods of constructing systematically mixed alphabets as described in section III of this chapter are applicable.

REF ID:A56932

Section VI. CIPHER DISKS AND SQUARE TABLES

61. Cipher Disks

a. In the foregoing section it was noted that the separate alphabets employed in the encipherment are produced by the use of only two strips of paper bearing the normal alphabet. Such strips are often referred to as *sliding alphabets,* because they can be shifted or slid against each other in any one of 26 points of contact or coincidence. Exactly the same results, so far as cipher equivalents are concerned, can be obtained by the use of other devices. First, there are the so-called cipher wheels or cipher disks in which an alphabet is written on the periphery of a *rotating* disk, the circumference of which is divided into 26 equal segments, and this disk is made to revolve concentrically upon a similar but slightly larger *fixed disk.* Figure 18 shows the now obsolete U. S. Army Cipher Disk, which is of this simple type. Here the alphabetic sequences are printed on glossy celluloid, are permanent, and admit of no variation. The use of unglazed celluloid upon which blank segments appear would permit of writing letters and erasing them as often as desirable. Thus, quick and easy change of alphabets would be possible.



To encipher a message, the key letter or the first letter of the key word or phrase is set opposite "a." Let us assume it to be "E." The cipher letters to be written are those opposite the text letter when "a" on the circle is set opposite "E" on the card. For example, "send powder" would be written "MARBPQIBAN." To use a key word or phrase, each letter is used in turn to encipher one letter only. When the last letter of the key word is used, repeat until all letters of the message are enciphered. Numbers when enciphered with the disk must be spelled out.

Figure 18.

REF ID:A56932

b. The cipher alphabets produced by the cipher disk shown in the figure are merely reversed standard alphabets, the same as are produced by the use of sliding strips of paper, and by the use of certain tables which are discussed below. The method of employing the disk needs no discussion. It may serve in monoalphabetic or polyalphabetic substitution with a key word or key number.

62. Square Tables

a. Tables known in the literature of cryptography under various names, such as "Vigenère Table", "Square Table", "Quadricular Table", "Pythagorean Table", "Cipher Square", "Cipher Chart", etc., are often employed in polyalphabetic substitution. All the results produced by their use can be duplicated by the employment of sliding alphabets or revolving disks. The modern form of the Vigenère Table is shown in figure 19. Such a table may be used in various ways, differing from one another in minor details. The most common method is to consider the top line of the table as containing the plain-text letters, the first column at the left as containing the key letters. Then each successive horizontal line con-

Plain-Text Letter

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 19. The Vigenère Table.

REF ID:A56932

tains the cipher equivalents for the plain-text sequence ABC . . . Z enciphered by the key letter which stands at its left in the first column. Thus, the cipher alphabet corresponding to key letter D is the sequence of letters in the fourth horizontal line under the plain-text line, where $A_p = D_c$, $B_p = E_c$, etc. It will be easy to remember, in using such a table, that the equivalent of a given plain-text letter, T_p, for example, enciphered by a given key letter, O_k, lies at the intersection of the vertical column headed by T, and the horizontal row begun by O. In this case $T_p\ (O_k) = H_c$. The same result will be found on referring to sliding, direct standard alphabets.

b. Minor modifications of the Vigenère Table are encountered. If the top line is made a reversed normal sequence, leaving the interior of the table unchanged, or if the successive horizontal rows are made to contain the reversed normal sequence, leaving the top row (plain text) unchanged, then the results given by using the table are the same as those given by using the obsolete cipher disk shown in figure 18. Again, the same general results can be obtained by using a set of alphabets in tabular form known under the names of Porta's Table and Napoleon's Table, which is shown in figure 20.

AB	A	B	C	D	E	F	G	H	I	J	K	L	M
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CD	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
						etc.							
WX	A	B	C	D	E	F	G	H	I	J	K	L	M
	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
YZ	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	N

Figure 20.

In this table the alphabets are all reciprocal, for example, $G_p\ (W_k) = V_c$, $V_p\ (W_k) = G_c$. Reciprocal alphabets when arranged in this form are sometimes called *complementary alphabets.* Note that in each alphabet either of two letters may serve as key letter indifferently: $G_p\ (W_k)$ or $G_p\ (X_k) = V_c$.

c. Another modification of the basic table, and one that employs numbers instead of letters as cipher equivalents is shown in figure 21. Since many more than 26 different equivalents are available (100 pairs of digits from 00 to 99, it is possible to insert many plain-text elements in

REF ID:A56932

*	a	b	c	d	e	f	g	h	i	*
a	10	11	12	13	14	15	16	17	18	a
b	11	12	13	14	15	16	17	18	19	b
c	12	13	14	15	16	17	18	19	20	c
d	13	14	15	16	17	18	19	20	21	d
e	14	15	16	17	18	19	20	21	22	e
f	15	16	17	18	19	20	21	22	23	f
g	16	17	18	19	20	21	22	23	24	g
h	17	18	19	20	21	22	23	24	25	h
i	18	19	20	21	22	23	24	25	26	i
j	19	20	21	22	23	24	25	26	27	j
k	20	21	22	23	24	25	26	27	28	k
l	21	22	23	24	25	26	27	28	29	l
m	22	23	24	25	26	27	28	29	30	m
n	23	24	25	26	27	28	29	30	31	n
o	24	25	26	27	28	29	30	31	32	n
p	25	26	27	28	29	30	31	32	33	p
q	26	27	28	29	30	31	32	33	34	q
r	27	28	29	30	31	32	33	34	35	r
s	28	29	30	31	32	33	34	35	36	s
t	29	30	31	32	33	34	35	36	37	t
u	30	31	32	33	34	35	36	37	38	u
v	31	32	33	34	35	36	37	38	39	v
w	32	33	34	35	36	37	38	39	40	w
x	33	34	35	36	37	38	39	40	41	x
y	34	35	36	37	38	39	40	41	42	y
z	35	36	37	38	39	40	41	42	43	z
*	a	b	c	d	e	f	g	h	i	*

*	j	k	l	m	n	o	p	q	r	*
a	19	20	21	22	23	24	25	26	27	a
b	20	21	22	23	24	25	26	27	28	b
c	21	22	23	24	25	26	27	28	29	c
d	22	23	24	25	26	27	28	29	30	d
e	23	24	25	26	27	28	29	30	31	e
f	24	25	26	27	28	29	30	31	32	f
g	25	26	27	28	29	30	31	32	33	g
h	26	27	28	29	30	31	32	33	34	h
i	27	28	29	30	31	32	33	34	35	i
j	28	29	30	31	32	33	34	35	36	j
k	29	30	31	32	33	34	35	36	37	k
l	30	31	32	33	34	35	36	37	38	l
m	31	32	33	34	35	36	37	38	39	m
n	32	33	34	35	36	37	38	39	40	n
o	33	34	35	36	37	38	39	40	41	o
p	34	35	36	37	38	39	40	41	42	p
q	35	36	37	38	39	40	41	42	43	q
r	36	37	38	39	40	41	42	43	44	r
s	37	38	39	40	41	42	43	44	45	s
t	38	39	40	41	42	43	44	45	10	t
u	39	40	41	42	43	44	45	10	11	u
v	40	41	42	43	44	45	10	11	12	v
w	41	42	43	44	45	10	11	12	13	w
x	42	43	44	45	10	11	12	13	14	x
y	43	44	45	10	11	12	13	14	15	y
z	44	45	10	11	12	13	14	15	16	z
*	j	k	l	m	n	o	p	q	r	*

*	s	t	u	v	w	x	y	z	*
a	28	29	30	31	32	33	34	35	a
b	29	30	31	32	33	34	35	36	b
c	30	31	32	33	34	35	36	37	c
d	31	32	33	34	35	36	37	38	d
e	32	33	34	35	36	37	38	39	e
f	33	34	35	36	37	38	39	40	f
g	34	35	36	37	38	39	40	41	g
h	35	36	37	38	39	40	41	42	h
i	36	37	38	39	40	41	42	43	i
j	37	38	39	40	41	42	43	44	j
k	38	39	40	41	42	43	44	45	k
l	39	40	41	42	43	44	45	10	l
m	40	41	42	43	44	45	10	11	m
n	41	42	43	44	45	10	11	12	n
o	42	43	44	45	10	11	12	13	o
p	43	44	45	10	11	12	13	14	p
q	44	45	10	11	12	13	14	15	q
r	45	10	11	12	13	14	15	16	r
s	10	11	12	13	14	15	16	17	s
t	11	12	13	14	15	16	17	18	t
u	12	13	14	15	16	17	18	19	u
v	13	14	15	16	17	18	19	20	v
w	14	15	16	17	18	19	20	21	w
x	15	16	17	18	19	20	21	22	x
y	16	17	18	19	20	21	22	23	y
z	17	18	19	20	21	22	23	24	z
*	s	t	u	v	w	x	y	z	*

*	0	1	2	3	4	5	6	7	8	9	*
a	36	37	38	39	40	41	42	43	44	45	a
b	37	38	39	40	41	42	43	44	45	10	b
c	38	39	40	41	42	43	44	45	10	11	c
d	39	40	41	42	43	44	45	10	11	12	d
e	40	41	42	43	44	45	10	11	12	13	e
f	41	42	43	44	45	10	11	12	13	14	f
g	42	43	44	45	10	11	12	13	14	15	g
h	43	44	45	10	11	12	13	14	15	16	h
i	44	45	10	11	12	13	14	15	16	17	i
j	45	10	11	12	13	14	15	16	17	18	j
k	10	11	12	13	14	15	16	17	18	19	k
l	11	12	13	14	15	16	17	18	19	20	l
m	12	13	14	15	16	17	18	19	20	21	m
n	13	14	15	16	17	18	19	20	21	22	n
o	14	15	16	17	18	19	20	21	22	23	o
p	15	16	17	18	19	20	21	22	23	24	p
q	16	17	18	19	20	21	22	23	24	25	q
r	17	18	19	20	21	22	23	24	25	26	r
s	18	19	20	21	22	23	24	25	26	27	s
t	19	20	21	22	23	24	25	26	27	28	t
u	20	21	22	23	24	25	26	27	28	29	u
v	21	22	23	24	25	26	27	28	29	30	v
w	22	23	24	25	26	27	28	29	30	31	w
x	23	24	25	26	27	28	29	30	31	32	x
y	24	25	26	27	28	29	30	31	32	33	y
z	25	26	27	28	29	30	31	32	33	34	z
*	0	1	2	3	4	5	6	7	8	9	*

Figure 21.

REF ID:A56932

the top line of the table in addition to the 26 letters. For example, one could have the 10 digits; a few common double-letter combinations, such as DD, LL, RR, SS; a few of the most frequently used pairs of letters, such as TH, ER, IN, or even such common syllables as ENT, ING, and ION.

63. Square Tables Employing Mixed Alphabets

a. In the tables thus far shown the alphabets have been direct or reversed standard sequences, but just as mixed sequences may be written upon sliding strips and revolving disks, so can mixed alphabets appear in tabular form. The table shown in figure 22, based upon the key word sequence derived from the word LEAVENWORTH, is an example that is equivalent to the use of a strip bearing the same key word sequence sliding against another strip bearing the normal alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z
E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L
A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E
V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	W	S	U	X	Y	Z	L	E	A
N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V
W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N
O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W
R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O
T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R
H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T
B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H
C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B
D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C
F	G	I	J	K	M	P	W	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D
G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F
I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G
J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I
K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J
M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K
P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M
Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P
S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q
U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S
X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U
Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X
Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y

Figure 22.

The usual method of using such a table is the same as that in the preceding cases. The only difference is that the key letters must now be sought in a mixed sequence, whereas in the preceding tables they were located in normal direct or reversed sequences. Example, using figure 22: $C_p\ (S_k) = X_c$.

REF ID:A56932

Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z
U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q
E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U
S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E
T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S
I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T
O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I
N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O
A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N
B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A
L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B
Y	C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L
C	D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y
D	F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C
F	G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D
G	H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F
H	J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G
J	K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H
K	M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J
M	P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K
P	R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M
R	V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P
V	W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R
W	X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V
X	Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W
Z	Q	U	E	S	T	I	O	N	A	B	L	Y	C	D	F	G	H	J	K	M	P	R	V	W	X

Figure 23.

b. Figure 23 illustrates a case in which a mixed alphabet is sliding against itself. The usual method of employing such a table is exactly the same as that explained before. The only difference is that both the plain-text letters and the key letters must be looked for in mixed sequences. Example, using figure 23: $U_p\ (R_k) = V_c$.

c. It has been indicated that the basis of reference in most cryptographic operations involving key words is the letter A_p. In employing sliding alphabets it is usual to set the key letter as located in the cipher component opposite the letter A as located in the plain component. But, as shown in paragraphs 42*b* and 60*c*, the key letter as located in the cipher component is usually set opposite the initial letter of the plain component. In all examples preceding that in figure 23, the key letter has been A. In figure 23, since the plain component is also a mixed sequence and its initial letter is Q, the sliding alphabets are set against each other so that the given key letter in the cipher component is opposite Q in the plain component. Thus, to duplicate the results given by the use of figure 23 in finding the value of $U_p\ (R_k)$, it is necessary to set the sliding strips in the following relative positions:

Plain: QUESTIONABLYCDFGHJKMNPRVWXZQUESTIONABLYCDEFGHJKM
Cipher: QUESTIONABLYCDFGHJKMNPRVWXZ

REF ID:A56932

Here it is seen that U_p $(R_k) = V_c$, which is identical with the result obtained from the use of the table. There are other ways of using the table, however, each having a correspondingly modified method of employing sliding strips in order to obtain identical results.

Section VII. OBSERVATIONS ON CIPHER SYSTEMS

64. More Complex Substitution Systems

a. The substitution systems discussed above are all based on relatively simple methods. They can all be solved rapidly. More complicated systems have been devised, however, and are used in certain situations. They are briefly described in this section.

b. Virtually all systems based upon the principle of a repeating key can be solved because of certain cyclic or periodic phenomena, which the use of a repeating key exhibits externally or internally in the cryptograms. There are methods for preventing the external manifestation in the cryptograms of these phenomena, or their suppression and disguise if present internally. In some, the principle is to make the elements of a fixed or invariable-length key apply to variable or irregular-length groupings of the plain text so that no cyclic phenomena are exhibited by the cryptograms. In others, the principle is to apply irregular lengths of the key, or a variable-length key to regular and fixed groupings of the plain text, with the same object in view. In still other methods, both principles are combined, or the key itself is of such a nature that it does not repeat itself. This may be brought about by constructing or establishing a nonrepeating key, or by employing the key in a special manner. Systems in which the successive letters of the cipher text or successive letters of the plain text after the initial letter serve as successive key-letters are also used with the object of avoiding or eliminating periodicity.

c. In the majority of the methods described the encipherment deals with single letters, and is therefore ***monographic*** in nature. There are, however, certain methods in which encipherment is by pairs of letters, called ***digraphic substitution,*** or by sets of three letters, called ***trigraphic substitution. Polygraphic substitution methods,*** as they are called, have for their object the suppression, so far as possible, of the characteristic frequencies of individual letters, by means of which solution may be reached. The methods may employ extensive tables, small squares, rectangles, and other designs, or sets of sliding or rotating alphabets. The ***Playfair Cipher,*** which was for many years a standard field cipher in the British Army and was for a short time during World War I employed by the U. S. Army, is an example of digraphic substitution.

REF ID:A56932

65. Combined Substitution-Transposition Systems

In paragraph 10*b*, reference was made to the possibility of combining within a single system both transposition and substitution methods; that is, of first enciphering by a method of one type and then taking the resulting cipher text and passing it through an encipherment of the other type. The usual order is first to substitute and then to transpose, but the reverse of this order of procedure is also possible. In some methods, quite complex, there may be a first substitution, then a transposition, and finally a substitution again. Despite the fact that three steps are involved, certain of these systems may be practical for military use under special conditions where speed is not as important as security. These cannot be described in this manual.

66. Cipher Devices and Cipher Machines

a. Only a little practical experience with any of the methods described is necessary to convince one that on the whole they are slow, more or less cumbersome, and subject to errors that often delay or make impossible the decryptographing of messages. Furthermore, from the point of view of cryptographic security, when employed in regular voluminous traffic they leave much to be desired. Consequently, cryptographers, both experienced and inexperienced, have been led to attempt to devise apparatus which will not only facilitate cryptographing and decryptographing, but will also increase the degree of cryptographic security. Small instruments constructed for this purpose, operated by hand, are called *cipher devices.* Scores of them have been devised, but only a few are sufficiently practicable for field use, and still fewer are of such construction that they produce cryptograms of unusual security. Among the better examples of such cryptographs is one which was for some years (1922–42) employed in the U. S. Army under the name of *Cipher Device, Type M–94.* Modern security requirements made such a device obsolete, however, and it has been replaced by a better one, the Converter M-209 ( ) (TM 11–380).

b. There are larger cryptographic machines which are much more nearly automatic in nature and can therefore be operated at a much greater rate of speed. These are usually equipped with typewriter keyboards which can be manipulated with considerable speed; the machine may also print the results of the enciphering or deciphering operations. Sometimes they are equipped with electrical transmitters and can thus serve not only to encipher and decipher messages but also to transmit them automatically. A mechanism of the latter nature is usually in the form of a modified printing telegraph machine, or else it consists of an auxiliary piece of apparatus used in conjunction with the teleprinter.

REF ID:A56932

Such apparatus can obviously be practicably employed only among the larger headquarters where traffic is sufficiently heavy to warrant its use.

67. Disadvantages and Limitations of Cipher Systems

Except for certain electrically operated cipher machines equipped with a typewriter keyboard, most cryptographic methods using "manual" or "pencil and paper" cipher systems are unsatisfactory for military purposes. Practically all such systems can be solved by enemy cryptanalysts, and those suitable for use in the theater of operations offer fewer obstacles to solution than systems suitable for use in the rear areas. Cipher systems are not economical in time units required in electrical transmission; the best that they can do is to produce cryptograms no longer than the original plain text. For use within small tactical units in the forward areas there are other cryptographic methods which offer advantages of speed, simplicity, and brevity and which, properly used, afford sufficient cryptographic security. These are often preferred over cipher methods in the forward echelons of the combat zone. These methods involve the use of lists of groups of letters or figures to which arbitrary meanings have been assigned. They are called "field codes," "prearranged-message codes," "brevity codes," "voice codes," "jargon codes," etc. Codes will be discussed in the succeeding sections of this manual.

REF ID:A56932

CHAPTER 4
ELEMENTARY CODE SYSTEMS

Section I. GENERAL

68. Difference Between Code and Cipher Systems as Methods of Cryptography

A code system is a more or less highly specialized form of substitution. The basic principle underlying substitution cipher systems is the replacement of the individual letter in the plain text of a message by other letters, figures, or symbols. Occasionally the replacement or substitution process is applied to groups of letters, and when this is done the groups are usually of definite, or regular length. In cipher systems the units with which the cryptographic treatment deals are the smallest of which plain text can be composed. The basic principle underlying code systems, however, is the replacement of entire words, long phrases, or complete sentences constituting the plain text of a message by arbitrarily selected equivalents having little or no relation to the elements they replace. These equivalents may be other words, groups of letters, groups of figures, or combinations. It is only exceptionally that the replacement or substitution process is applied to elements smaller than whole words, and when this is done the elements are single letters, groups of letters, or syllables. In code systems the units with which the cryptographic treatment deals are aggregates of smaller units—individual letters combined in various groups of irregular length; that is, words, phrases, sentences.

69. Code Books and Codes

a. If it were possible to memorize a long list of words, phrases, and sentences, together with the arbitrary equivalents called *code groups* assigned to represent them, there would be no need of having written or printed code books. In a code book, the words, phrases, and sentences are listed in a systematic manner and accompanied by their code equivalents. Correspondents must possess identical copies of the document in order to communicate with one another. An ordinary dictionary may, and often does serve the purpose of code communication, so far as single words are concerned, but as a rule a specially prepared document containing the words, phrases, and sentences, suited to particular types of correspondence, is used. Such documents are called, in the United States

REF ID:A56932

and in Great Britain, *code books* or, simply, *codes.* In other countries they are called *repertories, word books, cipher dictionaries, enciphering and deciphering tables, etc.,* although the term "code" is becoming prevalent throughout the world.

b. There are various types of codes each suited to particular types of correspondence. Some are large books used for general business or social correspondence; others are intended for particular industries—for example, rubber, sugar, steel, and automobile—and contain highly specialized technical vocabularies. Most large commercial firms have their own *private codes,* constructed especially for their use. This manual however, is concerned only with codes suitable for military communication. While the resemblances between the ordinary commercial codes and the usual military codes are marked, their primary purposes are different. Code is used in commercial communications principally to effect economy in cost of communicating, secrecy being of secondary importance. In modern military signal communications code is used to effect secrecy, brevity, and speed, especially in front-line signal communications. However, in lengthy administrative messages, the economy afforded by a properly constructed code is important.

70. Brevity Afforded by Code Systems

a. Messages cryptographed by means of a code book are secure only when the code book is kept secret. There are, however, code systems in which secrecy is not a factor. Such systems are intended for brevity or, in transmission by commercial telegraph, for economy. Code books afford a means for abbreviating or condensing the writing necessary to convey information. A single, comparatively short group of code characters may represent a whole word of as many as 15 or more letters, a long phrase, or a complete sentence. Thus, as a rule, the text of a code message is much shorter than the plain text, and therefore costs less to send. Naturally, the *condensing power* of a code book varies with the extensiveness of its *vocabulary,* since in a small book there can be listed only the most common words and only a few phrases and sentences; whereas, in a large book practically all the words likely to be used in telegraphic communication, and many common phrases and sentences may be included. When a code book is used to condense text only for purposes of economy, it is called a *nonsecret code.* Examples of such codes are the ordinary commercial codes sold in book stores. A code book may combine the features of economy and secrecy, in which case the book itself must be safeguarded from the enemy as a *secret code.*

b. In addition to money saving, code systems save time and labor in transmission and reception, as the number of characters handled in code systems is smaller than in cipher systems. The saving of time is an

REF ID:A56932

important factor in front line communications where speed is essential and sometimes outweighs security considerations.

c. In military cryptography, the greatest degree of condensation is afforded by "prearranged-message codes," "brevity codes," and the like. A *prearranged-message code* is a tactical code adapted to the use of units requiring special or technical vocabularies; it is composed almost exclusively of groups representing complete or nearly complete messages and is intended for shortening messages and concealing their content. A *brevity code* has for its sole purpose the shortening of messages. A *field code* is primarily a small tactical code which contains a large number of code groups representing words and a few common short phrases, from which sentences can be composed; a *syllabary,* which is a list of code groups representing individual letters, combinations of letters, or syllables, is usually provided for spelling out words or proper names, not present in the vocabulary; *numerical tables,* or lists of code groups representing numbers, dates, and amounts, are also included. A *jargon code* is another name for a simple, very short code in which bona fide dictionary words, baptismal names of persons, the names of rivers, lakes, etc., are used as code groups. A *voice code* is used for transmission by the small radio-telephone sets used in combat areas and may be a prearranged-message code, a brevity code, or a jargon code. Other names used to designate such codes are *combat code,* and *operations code.*

71. Operation of Encoding and Decoding

These two terms apply to the cryptographing and decryptographing respectively, of messages by means of a code. In encoding a message, a code clerk merely replaces the various words, phrases, sentences, and numbers of plain text by their code equivalents. The code text is built up from code units each representing the longest possible plain-text unit the code book affords. For example, if the sentence ENEMY FORCE ESTIMATED AT ONE BATTALION ENCOUNTERED ONE MILE SOUTH-EAST OF ROCK CREEK CHURCH is to be encoded, and the code book lists the phrase ENEMY FORCE ESTIMATED AT, the code group representing this phrase would be used rather than separate code groups representing the individual words ENEMY, FORCE, ESTIMATED, and AT, all of which might also be present in the code. The process of decoding is the reverse of that of encoding. Each code group is looked up in the code book, its meaning found and written down. Where the errors in transmission are few, the process is rapid; but even a small number of errors in a message may obscure the meaning or render a message unintelligible.

REF ID:A56932

Section II. CODE GROUPS

72. Composition of Code Groups

a. The elements of which code groups are composed may be of one or more of the following types:

(1) *Bona fide words*—real words taken from the dictionaries of one or more languages. The usual languages employed as sources for code words of this type are Dutch, English, French, German, Italian, Latin, Portuguese, and Spanish.

(2) *Artificial words*—groups of letters having no real meaning, constructed more or less systematically by arrangements of vowels and consonants so as to give these groupings the appearance and pronounceability of bona fide words.

(3) Groups of letters presenting no appearance of bona fide or artificial words and resembling cipher groups.

(4) Groups of arabic figures.

b. For special purposes, code groups composed of intermixtures of letters and figures within groups may be used. Call signs for radio stations, such as W2KA and W5AZZ, are examples of such intermixtures often used in radio call-sign codes. In certain highly specialized naval or military codes, the intermixture of letters and figures is sometimes necessary. Such intermixtures, however, are either not accepted or, if accepted, are charged for at a greatly increased rate when they appear in messages transmitted by commercial communications agencies.

c. A code may contain two or more parallel sets of code groups of different types. For example, in many commercial codes and in some military and naval codes, there is one series of code groups of the bona fide or artificial word type and another series of the figure-group type, both applying to the same series of words, phrases, and sentences of the code. There are several reasons for this. In most parts of the world where italic or roman letters are used for writing, letters possess greater advantages in accuracy of reading and handling by telegraph personnel. This is necessary for correct transmission and reception of messages. However, in some parts of the world—for example, Turkey, Russia, China—telegraph personnel, except in the large cities, are unfamiliar with the English alphabet and hence many errors in transmission arise. But arabic digits are almost universally recognized and used, so that for communications between obscure ports and small cities in foreign countries, figure groups are preferred over letter groups. There are certain methods of condensing code groups composed of figures into still smaller groups composed of letters by means of *condensers,* so that many firms use figure groups for such purposes in expensive transmissions. Finally, in certain methods of enciphering code messages for the sake of greater

REF ID:A56932

secrecy, figure groups often form the basis for the encipherment more readily than do letter groups.

d. Prior to 1 January 1934, in practically all modern codes constructed by experts, letter code groups were of the artificial-word type. On that date new rules in international communication became effective,[8] permitting the use of letter code groups without restriction in their formation, as class (3) in *a* above. It is probable that almost all of the codes published subsequently to the above date will contain letter code groups of the unrestricted type.[9]

e. The greatest advantage possessed by letter groups over figure groups lies in the availability of a far greater number of permutations, or interchanges, of letter groups, because there are 26 letters which may be permuted to form letter code groups, whereas there are only 10 digits which may be permuted to form figure groups. If code groups of five elements are used, then there are available 26^5, or 11,881,376 groups of five letters, and only 10^5, or 100,000 groups of five figures. Now since the number of permutations of 26 letters taken in groups of five is so great, only permutations conforming to special types may be selected for use, and there will still remain a sufficient number of code groups for even the largest codes. Certain types of code groups are selected so that possible error in telegraphic transmission can be reduced to a minimum. If the code groups have been constructed scientifically it is possible to correct such errors quickly without having the message repeated.

73. Length of Code Groups

The length of code groups used, whether the groups consist of two, three, four, or five elements, depends upon the size of the code. This applies almost exclusively to field military or naval codes, where transmission is through a governmental agency; in commercial messages or in governmental communications transmitted over privately-operated lines, five-letter or five-figure groups are used almost exclusively because of the regulations adopted by the International Telegraph Conferences and by commercial telegraph and cable companies. As a general rule in the transmission of code and cipher messages, each group of five letters is counted as one word regardless of the number and arrangement of vowels; each group of five figures is counted as one word.

74. Permutation Tables of Two-Letter Differential

a. Code groups of modern codes are constructed by use of tables which permit more or less automatic and systematic construction in the form desired. These are called *permutation tables.* Because they may be used

[8] See Telegraph Regulations, International Telecommunication Convention, Madrid, 1932.

[9] For a treatise on the development of codes see "The History of Codes and Code Language, the International Telegraph Regulations pertaining thereto, and the bearing of this history on the Cortina Report," by Major William F. Friedman, Sig.-Res., Government Printing Office, 1928.

REF ID:A56932

to correct most errors made in transmission or writing, such tables are usually included in the code book and are called *mutilation tables, garble tables, error-detector charts, etc.* Before the invention of permutation tables, code as a system of communication was not wholly reliable. Scientifically constructed tables, however, include a feature (see *b* below) which has remedied this fault to a great extent.

b. To make an error in a group of five letters is not unusual on the part of the average telegraph or radio operator. If a difference of only one letter distinguishes one code group from another in the same code, as ABABA and ABABE, then serious errors may be introduced in the meaning of a message, or the message may be made unintelligible by only a few transmission errors. If, however, every code group in the code book is distinguished from all other code groups in the same code by a difference of at least *two* letters, then there would have to be two errors in a single group and these two errors would have to produce a code group actually present in the code before a wrong meaning would be conveyed. This principle of making code groups within the same code differ from each other by a minimum of two letters is called the *two-letter differential.* It is most easily incorporated in code groups by constructing the permutation table to this end. The differential may be the absolute difference in the identities of two letters or the relative positions occupied by them. For example, BACOF, and BACUG differ from each other in the identities of the final pair of letters; considered as a *combination* of letters, the two groups present a two-letter difference. The two groups BACOF and BOCAF, however, differ in the relative positions occupied by two of their letters, but considered as a permutation of letters, these two groups as well as the two groups BACOF and BACUG, present a two-letter difference. In short, when at least two corresponding letters in a pair of code groups differ in their identities, the two code groups are said to present a 2-letter difference. Errors arising from the exchange of position of two letters, without a change in their identities, are referred to as errors of *transposition.* They are not unusual but fortunately, as a rule, they involve only letters which are either adjacent or alternate. For example, in the pair of groups BACOF and BOCAF there is a transposition of the alternate-letter type. In recent codes, attempts have been made to devise permutation tables which will eliminate one of the two members of every pair of groups which differ from each other by the mere transposition of two adjacent or alternate letters. Codes using groups based upon a permutation table will show the table and explain how to use it in correcting the usual mutilations of groups.

c. The use of the two-letter differential reduces the possibilities for constructing letter-code groups from 26^5 (11,881,376) to 26^4 (456,976), but, considering the advantages, the sacrifice is worthwhile.

d. Permutation tables for the construction of figure-code groups are similar in nature and purpose to tables for the construction of letter-code

REF ID:A56932

groups. However, because of the more limited number of characters available for permutations, the maximum number of 2-figure difference groups possible in a 5-figure code is 10^4, or 10,000.

Section III. ONE-PART AND TWO-PART CODES

75. Arrangement of Contents of Codes

a. In their construction or arrangement, codes are generally of two types:

(1) *One-part,* or alphabetical codes. The plain-text groups are arranged in alphabetical order accompanied by their code groups in alphabetical or numerical order. Such a code serves for decoding as well as for encoding.

(2) *Two-part,* or randomized codes. The plain-text groups are arranged in alphabetical order accompanied by their code groups in a nonalphabetical order. The code groups are assigned to the plain-text groups at random by drawing the code groups out of a box in which they have been thoroughly mixed, or by some other manner in which the element of chance operates. Such a list can serve only for encoding. For decoding, another list must be provided in which the code groups are arranged in alphabetical or numerical order and are accompanied by their meanings as given in the encoding section. For this reason a two-part code is often called a *cross-reference code.* The following brief extracts from typical one-part and two-part codes illustrate the difference between them:

One-part code.		Two-part code.			
		Encoding Section		Decoding Section	
ABABD	A	GAJVY	A	ABABD	Obstructed
ABACF	Abaft	TOGTY	Abaft	ABACF	Term
ABAHK	Abandon	FEHIL	Abandon	ABAHK	Zero
ABAJL	. . . . it	BAYLT	. . . . it	ABAJL	If it has not
ABALN	Abandoned	ZYZYZ	Abandoned	ABALN	To be sent by
ABAMP	. . . . by	NYSYZ	. . . . by	ABAMP	Acceding
ABAWZ	Abandoning	IFWUZ	Abandoning	ABAWZ	Building
ABBAD	Abandonment	RUMGO	Abandonment	ABBAD	Do not attempt
----------	----------	----------	----------	----------	----------
----------	----------	----------	----------	----------	----------
ZYZYZ	Zero	ABAHK	Zero	ZYZYZ	Abandoned

b. Between the two extremes are codes which have features of both; that is, complete sections may be arranged in random sequence, but within each section the contents are arranged in some systematic or logical order. This is true, however, only of some of the older codes. In modern types, the two-part construction is more common.

REF ID:A56932

c. When a strict alphabetical arrangement is used in the sequence of the phrases, the code is said to be a *strictly alphabetical code;* when the phrases are listed under separate headings based upon the principal word or idea in the whole expression, the code is said to be a *caption code.* The following extracts will serve to illustrate the two types:

Caption code	*Strictly alphabetical*
Assistance	Assistance
Give *assistance*	Assistance for
Require *assistance*	Assistance from
No *assistance* required	Assistance has been sent
Assistance has been sent	Assistance to
Assistance for	Assistant
Assistance from	Assisted
Assistance to	.....
Assistant	Give
Assisted	Give assistance
etc.	.....
	No
	No assistance required
	.....
	Require
	Require assistance

d. More precise and economical encoding is possible with a caption code than with an alphabetical code. With the caption code it is easier to assemble an extended variety of expressions and shades of meaning under specific headings than with the alphabetical code. On the other hand, the use of a caption code involves more time and labor in encoding, especially by untrained or unskilled personnel, than the use of an alphabetical code. Where the phraseology of communication is standardized or stereotypic, the most common expressions may be listed in an alphabetical code as readily as in a caption code. In both types of codes there may be tabulated material, such as tables of numbers, dates, equipment, geographical or personal designations, either forming isolated sections in the code or inserted in the vocabulary under appropriate headings.

e. Two-part codes are used by many governments for their secret diplomatic, military, and naval communications because the advantages they offer over one-part codes are greater than their disadvantages. The disadvantages are: a two-part code is harder to handle than a one-part code because it is at least twice as large in content, since each code group and each plain-text element must appear twice; the cost of printing is approximately double; the amount of labor in compiling a two-part code is nearly four times greater because of the necessity for preparing the accurate cross-reference arrangement which is its basic principle.

REF ID:A56932

76. Purposes of Two-Part Type of Code

a. The two-part code is a comparatively recent development in code systems. Its purposes are greater secrecy, and greater accuracy.

b. In a one-part code the plain-text groups progress from A to Z in a regular alphabetical sequence, accompanied by their code groups, also in a regular alphabetical or numerical sequence. If the word ABAFT is represented by a code group whose initial letter is A, or whose initial number is 1, then the word ABANDON will be represented by a group whose initial letter is also A, or whose initial number is also 1. In other words, the enemy cryptanalysts have definite clues to follow in breaking down the code because of the parallelism of the two sequences; the determination of the value of one code group affords definite clues to the value of many other code groups. In a two-part code, however, the word ABAFT might be represented by a group whose initial letter is T, or whose initial number is 8, and the word ABANDON might be represented by a code group whose initial letter is F, or whose initial number is 3. In other words, the two sequences are not alike in progression; hence the determination of the value of one code group will give no clues to the value of any other group.

c. In considering the greater accuracy of a two-part code over a one-part code, the following pair of phrases (in a hypothetical one-part code) are given as an example:

WOVAM	Will be ready to attack
WOVEN	Will not be ready to attack

Such an arrangement is subject to two sources of error. A code clerk working under great difficulties, in a hurry, may accidentally write down WOVAM instead of WOVEN as a result of the contiguity of the two sets of letters which are similar in appearance and are so close together on the page that his eye may take the group from the wrong line. Again, on account of the similarity in sound, his ear may deceive him into writing WOVEN when he should have written WOVAM. Now the meaning of the one group is the exact opposite of the meaning of the other and, since either meaning may fit in correctly with the context of the message, the error may remain undiscovered for some time, thus causing serious inconvenience or, in the case of combat, actual loss of life. Furthermore, although the making of two errors in a single group is rather unusual in transmission or reception, yet it does happen and, in such a case as the above, would not be detected. This is especially true in connection with tabular material such as lists of numbers, dates, and names, in which the context often fails to yield clues to the correction of garbles or errors, or to give conclusive evidence of the presence of an error. But in a two-part code such errors are improbable. In the first source of error mentioned above, the code clerk would be very much less

REF ID:A56932

likely to confuse two entirely different groups of letters; in the second source, if two errors are made in the transmission or reception, and if these errors involve two letters producing a group which actually has a meaning in the code, this meaning is so unlikely to fit in correctly with the context that its probability of occurrence may be negligible. Thus, if this sort of error does happen, the meaning of the group fails to fit in with the context and at once indicates an error. Knowledge of such an error, even if it is impossible to correct it, is more preferable than ignorance of its existence, with a possible action based upon incorrect decodement.

Section IV. ENCIPHERED CODE

77. Purposes of Enciphered Code

a. Sometimes the code groups of a code message undergo a further process of encipherment. The resulting cryptogram constitutes an *enciphered code message.*

b. It is desirable to use enciphered code in two instances:

(1) When the basic code has had wide distribution and the message might fall into unauthorized hands. Commercial codes sold in bookstores, and even special codes distributed widely throughout governmental offices, illustrate the type of code to which this added safety factor should be applied.

(2) When increased security is necessary for highly classified communications. Although the basic code book may already be secret, further encipherment would greatly delay the solution of the code if it fell into the hands of enemy cryptanalysts.

c. It has already been stated that code messages may be solved by cryptanalytic principles without possession of the code. The length of time required for the process varies widely, and is dependent upon the conditions under which the work is done (see ch. 1). To increase the length of time required for solution, as in secret codes, the code text of the messages resulting from the use of the code is passed through a cipher process so that the messages will be in different keys, thus delaying the assembling and study of data, which is necessary to the solution.

78. Types of Encipherment

a. Both of the two general classes of cipher methods, transposition and substitution, may be used in enciphering code. The increased degree of secrecy because of encipherment depends entirely upon the nature of the system applied.

b. Transposition systems involving a rearrangement of complete groups may be employed where the degree of increased security does not

REF ID:A56932

have to be of a high order, and where the original form of the groups must be retained even after encipherment. Transposition systems in which the order of the letters within groups is changed may also be employed. For example, a numerical key may indicate the transposed order of the letters of the code groups, so that a group such as XDFGY will become DFYXG.

c. Substitution systems of many sorts may be employed, ranging from simple monoalphabetic to the most complex types of substitution with cipher machinery. Tables of alphabets are often used. In some systems, a simple transposition process may be combined with a simple substitution process.

d. A favorite method in one-part codes having both letter-code and figure-code groups is that in which the letter-code group standing at a prearranged interval before or after the letter-code group representing the actual word or phrase intended to be conveyed is substituted. The interval may remain fixed within a single message, or it may vary according to some predetermined key. Numerical code groups make the use of large intervals practicable.

e. In modern practice, the most common methods of enciphering figure-code groups are those using addition or subtraction, with a *key book* containing arbitrary groups of figures. When such methods are properly used, they yield a high degree of security. The highest degree of security is attained when such a key book is used *only once.*

REF ID:A56932

CHAPTER 5
COMPARISON OF CODE AND CIPHER SYSTEMS

79. Advantages and Disadvantages of Each Type of System

a. From the viewpoint of purely military cryptography, a comparison of the advantages and disadvantages of each method can be made only between systems suitable for each of the following three general categories:

(1) High-security, or "high-grade," systems for cryptographic intercommunication among the largest military units and the highest echelons of command.

(2) Medium-security, or "medium-grade," systems for cryptographic intercommunication among the intermediate units and echelons of command.

(3) Low-security, or "low-grade," systems for cryptographic intercommunication among the small units and the lowest echelons of command.

b. The principal factors to be taken into account in comparing code and cipher methods in cryptographic communication are reliability, security, rapidity, flexibility, and economy.

(1) *Reliability.* Reliable cipher machines made possible by modern engineering and cryptographic techniques satisfy all or a majority of these factors to a great degree, and such machines are now used in the U. S. Army for these high-grade systems. Although the machines are complex, their reliability can be assured by having properly trained personnel to operate and maintain them. Accuracy is also one of the elements of reliability and a good cipher machine can yield a higher degree of accuracy or completeness of text in cryptographic communication than can a code system. A mistake in one or two code groups may obscure, alter, or render unintelligible the meaning of a whole message, but in cipher systems, often wrong letters may be corrected, or missing letters may be supplied, by the context. It must be remembered, however, that in some cipher systems a single error of a fundamental type, such as using the wrong key or the wrong "setting," may prevent the deciphering of the message.

(2) *Security.* If reliability were the only or the most important factor, code would be preferable to cipher for all echelons of

REF ID:A56932

command, because the simplicity of a code book is to be preferred to the complexity of a large cipher machine. But unenciphered code is not sufficiently secure for the communications of the highest echelons and headquarters. If encipherment must be added as a second step in the cryptographic process, it practically destroys the simplicity features of a code system; unless the enciphering method is fairly complex, it adds little security. In a properly designed cipher machine, embodying sound cryptographic principles based upon a thorough knowledge of cryptanalytic principles, the single-step-encipherment process can yield cryptograms of very great security. In a good code system, however, the solution of one or even of several messages does not entail the immediate breakdown of the entire system, with the consequent ability to read all messages, as is usually the case in a cipher system.[10] Codebooks, of course, can be rendered useless by compromise. Actual possession for a long period of time is not necessary; methods of rapid photography may be applied and a book of several hundred pages copied in a few minutes.

(3) *Rapidity.* The speed with which a cipher machine equipped with a typewriter keyboard can be operated leaves even simple, unenciphered code far behind in the matter of rapidity.

(4) *Flexibility.* Complete flexibility would permit cryptographing the originator's own language without change necessitated by the limitations that exist in all but the most extensive codebooks. Thus, a cipher machine is much more flexible than a code and can be used for all sorts of messages; whereas, in a code containing words, phrases, and sentences prepared for a specific type of communication, rewording the original text as written by the originator is often necessary, if the words, phrases, and sentences in the codebook are to be used; otherwise the original wording must be encoded word by word, or even syllable by syllable.

(5) *Economy.* Whether expressed in terms of money or manpower, cipher systems are more economical than code systems for high-echelon communications. Code text is usually shorter than the equivalent plain text, because it is condensed or abbreviated, but a single clerk operating a rapid cipher machine

[10] A good cipher system may be compared to a library housed in a large structure of many rooms with all doors and all windows securely locked. If an intruder can force an entry into the structure, he will find a master key which will open all the locks and give him access to *all* the books in the library. A good code system (especially a two-part code) may be compared to a library housed in a similar structure, but no two locks are alike and no master key is available or can be made. Therefore, the lock on *each* door must be worked at patiently as a separate problem. Thus, although the intruder may force his way into one room, this gives him access to only a small part of the library; in order to read all the books, he must force his way into each room, which takes much time, since each lock presents a separate and special problem.

REF ID:A56932

can turn out 10 to 15 times as much work as one operating a code system; furthermore, codes must be prepared, printed, and distributed. These steps take much time and labor and are often performed under considerable difficulty. A continuously operative code compilation section must be maintained to replace codes as fast as they become compromised by continued use, or by capture. The handling of the manuscript and proofs in printing entails the necessity of ever watchful secrecy; and finally, the prompt and thorough distribution of codes to all who must use them is sometimes very difficult, especially where the distribution must be made over an extensive territory. Therefore, for high-echelon cryptographing communications, ciphers are more economical than codes, but the economy factor is least important.

c. It is clear that high-grade systems should include all or as many as possible of the five factors listed in *b* above; moreover, the advantages afforded by good cipher machines make cipher systems more desirable than code systems for the high-grade cryptographic systems required by high-echelon cryptographic intercommunication. In addition, secondary or "back-up" systems must be provided so that in case of machine or power failure, there will be available some means for cryptographic communication. Finally, emergency systems must be provided for cryptographic communication when neither apparatus nor codebooks can be employed.

d. Medium-grade cryptographic systems for intercommunication among intermediate echelon commands must meet almost the same severe requirements as systems for intercommunication among high-echelon commands. Here again, cipher machines are preferable to code. The machines may not be so large or complex, but if the same basic cryptographic system is employed by both the high-grade and the medium-grade machine, many advantages are noted. The problems of manufacture, maintenance, instruction of personnel in the operation of the system, distribution of keying data, etc., are simpler if they are basically the same for both types of machines. Moreover, it is possible for a message from an intermediate command to be deciphered by a high-echelon command, and vice versa, without using a second cryptographic system. For these reasons, cipher machines are widely used in the U. S. Army for medium-grade cryptographic communication and, in addition, certain manual systems requiring simple types of apparatus are also used. These may serve also as the secondary or "back-up" systems required for the high-echelon cryptographic communications.

e. (1) Even in the so-called "low-grade" systems, cipher machines are serving the purposes for which field codes were formerly supplied. Converter M–209–( ) is a small, mechanical cipher machine widely used in the U. S. Army for communications

REF ID:A56932

within the small combat units. If properly used, it yields cryptograms of considerable security. It is a complicated device; it has no keyboard, and is slow in operation. Despite its reduced size and weight, this device is not convenient for use in front-line areas, nor is it suitable for use in voice communication by small radio-telephone equipments such as the "walky-talky" or "handy-talky" sets.

(2) Manual or hand-operated cipher systems are also unsuitable for such purposes. The processes of enciphering and deciphering by means of such systems require very close mental attention to avoid errors; the more secure methods are hopelessly slow and the faster ones are not secure, in comparison with the security that a small, frequently-changed *two-part* code yields.

(3) Practical experience indicates that in messages of very small tactical units, in certain types of air-to-air or air-to-ground communications, and in certain forms of messages where the subject matter is highly stereotypic, as in weather reports and fire-control observations, code is often preferred over cipher. In all these cases, speed must give way to security; size and weight of equipment are important factors; simplicity of operation under battle conditions is vital, which eliminates methods requiring much training and concentrated attention. Also, if code is properly prepared, one or two code groups may express a command or a report that would require many groups of cipher text. Small codes meet the requirements in all these respects, and for this reason, code is still used to some extent in the U. S. Army, especially in the forward areas.

80. Fundamental Assumption of Military Cryptography

It has been seen that every good cryptographic system combines two more or less separate and distinct elements: a basic or unchangeable method or process, which is termed the general system; and a specific or variable factor which controls the steps under the general system and is termed the specific key. The secrecy of any military cryptographic system must be entirely dependent upon the specific key because it *must be assumed that the enemy is in full possession of all the details concerning the general system.* This assumption is warranted by the whole history of military cryptography and is based upon the two following considerations which all experienced cryptanalysts regard as valid. In the first place, in military cryptography there are more prolific sources from which to obtain information concerning cryptographic methods than there are in the isolated methods used by private individuals. In fact, by one means or another, the enemy can sooner or later come into possession of full information regarding the general cryptographic system. In the

REF ID:A56932

second place, within a very short time the number of messages available for study becomes so great, and the inevitable blunders in the handling of communications have become so numerous that a solution by detailed study can always be made by the enemy, with a consequent disclosure of the general system. If a cryptographic system adopted for military use were such that messages in that system could be solved easily without the specific keys applicable to the messages once the underlying methods became known, the entire system would have to be changed, a new system devised, and thousands of persons in the military service trained in its operation. This, of course, would be impracticable. It is assumed that the enemy has knowledge of the general cryptographic system, its cipher devices, instruments, or machines. Only cryptographic documents which are given a limited distribution can be kept secret from the enemy, but they can be kept secret only for a variable length of time before they must be changed. These changes, as a rule, do not affect their method of usage. In cipher sytems, the specific key must be susceptible of easy and rapid changes by prearrangement between correspondents. In systems for use by secret agents or very small military parties in the theater of operations, the key may be an easily remembered word, phrase, sentence, or number; it must not require the carrying of written notes on the person. In systems for use by commanders of large and intermediate or even small headquarters in the theater of operations, the specific key may be in the form of written memoranda, paper tapes, and the like. Generally, the specific key must be the same throughout a given period of time for all the members of an intercommunicating network, or at least only a very limited number of specific keys must be in simultaneous effect; otherwise confusion and delay are inevitable. As a consequence of this requirement, the enemy may intercept a good many messages all in the same specific key. A cryptographic system for military use must conform to all requirements of practicability set forth in section IV, chapter 1, and to the foregoing section concerning the specific key; this system must be such that it is practically impossible for the enemy to solve any message quickly enough to make the information obtained of real or immediate value in the tactical situation, even though he is in full knowledge of the general method of the system, possesses the cipher device or apparatus, if used, and may have available for study 1,000 or more cryptograms sent on the same day. There is no single cryptographic system yet known which fully meets all these requirements, and in order to provide the necessary degree of security for a large army several different types of ciphers and cipher machines, as well as small codes for front line use, must be employed simultaneously.

REF ID:A56932

CHAPTER 6
CORRECTION OF ERRORS

81. Sources of Error in Cryptography

Errors, mutilations, and garbles are some of the names applied to the inaccuracies that occur in cryptographic communication. They are so common and so troublesome that commanders who, for the most part, already regard cryptographic processes as hopelessly slow and cumbersome, often become much prejudiced against their use in active operations. Therefore, instruction in the correction of errors is an essential part of the training of personnel assigned to cryptographic work. Training and experience will reduce the time necessary to correct the most common types of errors, which may be traced to the following sources:

a. Cryptographing and decryptographing, including the simple process of copying by hand or by typewriter.

b. Transmission and reception by all means of signal communication other than those in which the cryptograms are physically carried from origin to destination.

82. Practical Suggestions for Eliminating Errors

a. Errors in cryptographing and decryptographing can be much reduced though not wholly eliminated, by systematizing the work so far as possible and *invariably* checking it. Great care must be exercised in the formation of letters in writing, and roman capitals should always be used. If copied messages are checked for correctness by two operators, one reading the letters to the other, a phonetic alphabet must be used in order to prevent misunderstandings. In forward areas it is impossible to provide suitable or convenient quarters for personnel engaged in cryptographic work, but in rear areas and at the larger headquarters this personnel will work much more efficiently in a quiet, well ventilated office. To check the accuracy of cryptographic work it is always advisable, when possible, that an operator other than the original cryptographic clerk decryptograph the message. In checking his own work, an operator should actually decryptograph it—not merely check his cryptographing—because it is a psychological fact that persons have a tendency to repeat an error unconsciously. The most serious errors in cryptographic work leading to difficulties and delays in decryptographing are not the mere mistakes in the writing down of letters, but are errors of a fundamental nature which the operator says, when it comes back to him, "I don't see how I could

REF ID:A56932

have made it." Checking by actually decryptographing will usually eliminate such errors. At the destination, the *final copy* of a decryptographed message should invariably be checked against the *original* work sheets before being turned over to the addressee, and again preferably, by another operator. It is easy to omit the word NOT from a decoded message and to fail to note the omission, if the same operator merely reads over the decryptographed message. Here, again, psychological factors are involved, and clerks who are disposed to transpose letters and words, an unconscious habit of a peculiar psychological origin, must be especially careful in their work.

b. Carelessness in the writing of system and message indicators, or failure to insert them in their proper places in the message, will usually make prompt decryptographing of the received message difficult or impossible. They should be written with the greatest of care.

c. If an incoming message is partially or wholly unreadable, an attempt should be made to find the error in the faulty message. Often a message can be decryptographed by a simple expedient such as applying the key for the day preceding or following and correct date, or applying the daily key for a classification higher or lower and the correct classification. If, however, the garbled text still resists all efforts of correction, a procedure (service) message should be sent. The length of time one should continue with the attempt to break the faulty message before sending a service will depend upon the classification and precedence of the message, transmission problems involved, time required to complete service, etc.

d. The procedure in preparing and handling service messages dealing with errors in cryptographic messages is quite involved, in order not to compromise the cryptographic system or give clues as to the contents of the faulty message. Instructions covering the procedure to be followed in such servicing are issued from time to time and should be carefully followed.

e. The most important precaution to be observed, in order to avoid the transmission of messages which cannot be promptly decryptographed at the receiving end, is the rigid adherence to all instructions set forth in documents describing the cryptographic operations to be followed. Misunderstanding or ambiguity is rarely found in *properly prepared* documents detailing cryptographic operations, and a careful study and observance of the instructions will result in the preparation of messages without fundamental errors.

f. To be efficient in cryptographic work requires, in addition to the usual qualities of carefulness, accuracy, and attention to detail, the possession of certain psychological characteristics peculiar to the work. If absent, these characteristics as a rule cannot be developed, but if present they can be intensified and made more efficient by constant practice and experience. It is therefore advisable to select personnel for cryptographic work as for any other specialized work, to train them carefully, and

REF ID:A56932

retain them as long as possible; the longer they remain in this work the less likely they are to repeat the errors with which the work abounds and the more likely they are to render highly efficient service.

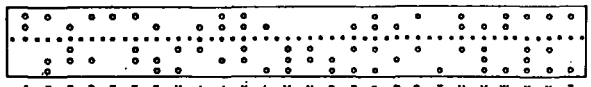
g. Errors in transmission and reception are frequently made, especially in transmission by radio, because of interference, atmospheric disturbances, and the like. Cryptographic clerks should be familiar with the Morse and Bandot alphabets and the most common errors of wire and radio transmission methods, so as to be able to refer an error to its probable origin or to find clues for the correction of badly garbled groups when all other means fail. The following tables will be found useful:

Most common errors in Morse transmission

International Morse alphabet (used in radio, cables, and outside United States)			American Morse alphabet (used in the United States, except for radio)		
Letters and figures	Alphabet	Frequent errors	Letters and figures	Alphabet	Frequent errors
A	• —	i, m, t, et	A	• —	i, t, et
B	— • • •	d, ts	B	— • • •	d, h, ts
C	— • — •	f, k, j, r, nn	C	• • •	s, z, ie
D	— • •	b, s, l, ti	D	— • •	b, ti
E	•	t, a, i	E	•	t
F	• • — •	q, r, in	F	• — •	r, q, en
G	— — •	m, n, o, q, me	G	— — •	n, c, me
H	• • • •	s, v, b, se	H	• • • •	s, p, z, y, es
I	• •	a, n, s	I	• •	a, o, e
J	• — — —	w, o, eo, am	J	— • — •	c, k, ke
K	— • —	a, n, d, o, ta	K	— • —	j, n, ta
L	• — • •	x, r, d, ed	L	——	t, n
M	— —	a, n, i, tt	M	— —	n, a, tt
N	— •	i, m, t, te	N	— •	o, t, te
O	— — —	g, k, m, w, mt	O	• •	n, i, ee
P	• — — •	j, w, g, l, r, an	P	• • • • •	h, s
Q	— — • —	g, k, o, x, z, ma	Q	• • — •	f, g, u, in
R	• — •	a, n, f, g, s, l, w	R	• — •	s, i, ei
S	• • •	h, d, i, r, u, v	S	• • •	h, r, i
T	—	a, e, n	T	—	l, e, n
U	• • —	a, s, v, it	U	• • —	v, a, w, it
V	• • • —	h, u, x, st	V	• • • —	u, st
W	• — —	a, m, o, r, u, at	W	• — —	f, a, u, m, at
X	— • • —	d, v, u, k, y, tu	X	— • •	l, y, f, al
Y	— • — —	x, w, k, c, nm	Y	• • •	h, ii
Z	— — • •	b, d, g, q, mi	Z	• • • •	h, c, se
1	• — — — —	0, 2	1	• — — — •	p
2	• • — — —	1, 3	2	• • — — • •	3
3	• • • — —	2, 4	3	• • • — •	4
4	• • • • —	3, 5	4	• • • • —	3
5	• • • • •	4, 6	5	— — —	
6	— • • • •	5, 7	6	• • • • • •	p
7	— — • • •	6, 8	7	— — • •	
8	— — — • •	7, 9	8	— • • • •	
9	— — — — •	8, 0	9	— • • —	x
0	— — — — —	9	0	——	L

REF ID:A56932

TELETYPEWRITER GARBLE TABLE



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
GAIN OF 1ST PULSE	-	?	(	$	3	!	FIG	6	7	,	(	2	/	)	?	!	!	:	Bell	"	7	LTR	2	/	6	"	UC
	A	B	K	D	E	F	FIG	Y	U	J	K	W	X	F	B	Q	Q	J	S	Z	U	LTR	W	X	Y	Z	LC
GAIN OF 2ND PULSE	-	FIG	:	.	-	(	B	Ø	8	.	(	)	:	:	B	Ø	!	4	7	)	7	:	2	LTR	!	2	UC
	A	FIG	C	J	A	K	G	P	I	J	K	L	V	C	G	P	Q	R	U	L	U	V	W	LTR	Q	W	LC
GAIN OF 3RD PULSE	?	/	:	!	Bell	!	:	£	8	(	(	Ø	.	.	.	Ø	!	:	Bell	£	7	:	!	/	6	6	UC
	U	X	C	F	S	F	V	H	I	K	K	P	M	N	M	P	Q	C	S	H	U	V	Q	X	Y	Y	LC
GAIN OF 4TH PULSE	.	?	:	$	$	!	8	.	:	.	(	8	.	.	9	:	LTR	4	!	9	(	:	FIG	/	/	?	UC
	J	B	G	D	D	F	G	M	G	J	K	G	M	N	O	V	LTR	R	F	O	K	V	FIG	X	X	B	LC
GAIN OF 5TH PULSE	2	?	:	?	"	/	8	£	Ø	FIG	LTR	)	.	.	9	Ø	!	8	6	5	!	:	2	/	6	"	UC
	W	B	V	B	Z	X	G	H	P	FIG	LTR	L	M	M	O	P	Q	G	Y	T	Q	V	W	X	Y	Z	LC
LOSS OF 1ST PULSE	LF	9	:	CR	Blnk	,	8	£	8	4	:	)	.	.	9	Ø	Ø	4	SPC	5	8	:	)	.	£	5	UC
	LF	O	C	CR	Blnk	N	G	H	I	R	C	L	M	N	O	P	P	R	SPC	T	I	V	L	M	H	T	LC
LOSS OF 2ND PULSE	3	?	,	$	3	!	9	£	SPC	$	!	5	.	,	9	£	6	CR	Bell	.5	Bell	.	"	/	6	"	UC
	E	B	N	D	E	F	O	H	SPC	O	F	T	M	N	O	H	Y	CR	S	T	S	M	Z	X	Y	Z	LC
LOSS OF 3RD PULSE	-	?	4	$	3	$	8	5	LF	.	.	)	9	CR	9	)	2	4	3	5	-	8	2	?	"	"	UC
	A	B	R	D	E	D	G	T	LF	J	J	L	O	CR	O	L	W	R	E	T	A	G	W	B	Z	Z	LC
LOSS OF 4TH PULSE	-	"	8	3	3	Bell	)	£	8	-	7	)	£	SPC	5	Ø	!	LF	Bell	5	7	Ø	2	6	6	"	UC
	A	Z	I	E	E	S	L	H	I	A	U	L	H	SPC	T	P	Q	LF	S	T	U	P	W	Y	Y	Z	LC
LOSS OF 5TH PULSE	-	8	:	$	3	!	4	SPC	8	.	(	LF	.	.	CR	8	7	4	Bell	Blnk	7	:	-	!	Bell	3	UC
	A	D	C	D	E	F	R	SPC	I	J	K	LF	N	N	CR	I	U	R	S	Blnk	U	G	A	F	S	E	LC

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

AT THE TOP AND BOTTOM OF THE CHART ARE THE LETTERS ORIGINALLY TRANSMITTED. IN THE SQUARES ARE THE CHARACTERS WHICH WOULD BE RECEIVED WITH GAIN OR LOSS OF PULSE DEPENDING UPON WHETHER MACHINE IS IN "UC" (UPPER CASE) OR "LC" (LOWER CASE).

REF ID:A56932

CHAPTER 7

FUNDAMENTAL RULES FOR SAFEGUARDING CRYPTOGRAMS

83. General

The rules given in this chapter are to be considered as a general guide only. Under actual operating conditions much is dependent upon special situations, and the specific cryptographic systems employed. Therefore, the particular rules and regulations currently in effect always will take precedence over those stated herein.

84. Fundamental Rules of Cryptographic Security

a. Failure to observe the fundamental rules of cryptographic security often makes possible the solution of cryptographic systems by enemy cryptanalysts. These rules apply to the originators of messages to be cryptographed as well as to cryptographic personnel. Detailed instructions for the writers of such messages are outside the scope of this manual. It is, however, desirable to indicate the following points:

(1) Stereotypic phraseology must be avoided, especially at the beginning and ending of a message. *The known or suspected presence of stereotypic phraseology constitutes the basis of many methods employed in cryptanalysis;* in some cases, indeed, the only possible method of solution makes use of the presence of stereotypic phraseologies, or, as they are often called, *cribs.* Operating instructions for currently authorized cryptosystems prescribe the application of measures which effectively reduce the dangers of stereotypic phraseology to the security of those systems; however, as an added precaution, routine reports of all kinds should be sent by agencies of signal communication not susceptible to interception.

(2) Special care must be taken to see that the messages are clear and concise. If a message is ambiguous or incomplete, unnecessary confusion results and the accuracy of the cryptographic operation is brought into question.

(3) Messages should be shortened by the deletion of unnecessary words. Conjunctions, prepositions, repetitions of words, and, especially, punctuation should be reduced to a minimum. When punctuation is necessary, it should be spelled out, either in full or in abbreviated form. Numbers should also be spelled out.

REF ID:A56932

Where letters of the alphabet must be used, as in certain symbols designating types of equipment, it may be necessary to represent these letters by their authorized phonetic equivalents, where it is essential that there be no possibility of error. Such spelling out however, should be reduced to a minimum.

(4) Authorized abbreviations should be used whenever practicable.

(5) Regulations regarding the manner of indicating addresses and signatures should be carefully followed.

(6) Regulations governing the security classification of messages (Top Secret, Confidential, Restricted) must be observed at all times.

b. Much of the success which attends the efforts of cryptanalysts is based upon ignorance and carelessness on the part of cryptographic personnel. Rarely are cryptographic blunders the result of willful violation of instructions; but if cryptographic personnel realize, that, by carelessness or ignorance, their own lives and those of thousands of their comrades are jeopardized, they will be more attentive to rules set up for their guidance. The most important of these rules are as follows:

(1) *Questionable messages.* Never cryptograph a message which, in the opinion of the cryptographer, violates any of the provisions or regulatons relating to the drafting of messages, until the question has been referred to and passed by someone with authority to change the message.

(2) *Mixing plain and cryptographic text.* Never allow cryptographic text with its equivalent plain language to appear in a cryptogram, and never mix plain and cryptographic text, *except in messages where such mixtures are specifically permitted.* This includes punctuation and abbreviations of any description. Such messages afford valuable clues to the enemy. If a message is to be cryptographed at all, it should be completely cryptographed.

(3) *Text of messages.*

(*a*) Never repeat in the clear the identical text of a message once sent in cryptographic form, or repeat in cryptographic form the text of a message once sent in the clear. Anything which will enable an alert enemy to compare a given piece of plain text with a cryptogram that supposedly contains this plain text is highly dangerous to the safety of the cryptographic system. Where information must be given out for publicity, or where information is handled by many persons, the plain-text version should be very carefully *paraphrased* before distribution, to minimize the data an enemy might obtain from an accurate comparison of the cryptographic text with the equivalent, original plain text. To paraphrase a message means to rewrite it so as to change its original wording as much as possible without changing the meaning of the mes-

REF ID:A56932

sage. This is done by altering the positions of sentences in the message, by altering the positions of subject, predicate, and modifying phrases or clauses in the sentence, and by altering as much as possible the diction by the use of synonyms and synonymous expressions. In this process, deletion rather than expansion of the wording of the message is preferable, because if an ordinary message is paraphrased simply by expanding it along its original lines, an expert can easily reduce the paraphrased message to its lowest terms, and the resultant wording will be practically the original message. It is very important to eliminate repeated words or proper names, if at all possible, by the use of carefully selected pronouns; by the use of the words "former," "latter," "first-mentioned," "second-mentioned"; or by other means. After carefully paraphrasing, the message can be sent in the other key or code.

(*b*) Never send the literal plain text or a paraphrased version of the plain text of a message which has been or will be transmitted in cryptographed form except as specifically provided in appropriate regulations.

(4) *Keys.* Never repeat in a different key or system, without paraphrasing, a cryptographed message which has once been transmitted, unless specifically authorized by the appropriate authority.

(5) *New cipher keys.* Never transmit a new cipher key by means of a message cryptographed in an old key.

(6) *Addresses or signatures.* Never place cryptographed addresses or signatures at the beginning or end of the cryptographed text. Bury them in the body of the message.

(7) *Identifying information.* Include in the address of a cryptographed message only the minimum information necessary for the message to reach the headquarters for which it is intended.

(8) *Replies.* Never reply to a cryptographed message in the clear.

(9) *Short titles.* Never use short titles as system or message indicators in cryptographed messages.

(10) *Dummy letters and padding.* Never use dummy letters or padding unless their use is specifically authorized.

(11) *System indicator.* Never encipher, encode, or disguise in any way the system indicator, unless specifically authorized.

(12) *Notations.* Never place on the cryptographed copy of a message any notations about the system or the subject matter of the message.

(13) *Work tables.* Never allow unnecessary materials such as books, documents, or papers to be on the work table during the process of cryptographing and decryptographing.

REF ID:A56932

(14) *Filing messages.* Never file cryptographic messages and their equivalent plain text together. Work sheets must be destroyed by burning.

(15) *Check for accuracy.* Cryptographed messages should be checked for accuracy by decryptographing the message before transmission. Whenever practicable, this should be done by a cryptographer other than the one who originally cryptographed the message.

(16) *Safeguarding material.* Observe all rules of physical security established to safeguard the cryptographic material and message translations. Utmost care should be taken to prevent the loss or unauthorized sight of the codes or lists of cipher keys in use. It is possible to photograph an entire code in two or three hours. Mere continued possession of the cryptographic material is, therefore, no absolute guaranty that it has not been compromised by photography or some other method of reproduction. The only absolute assurance of its not having been compromised is that it has *never* left the possession of the person into whose care it has been entrusted or the safe in which it is kept when not in use. Even if knowledge that a code or cipher has been compromised follows immediately after such compromise, the amount of time and the difficulties involved in notifying all concerned and distributing new cryptographic material are so great that serious damage is caused by the delay and interruption in communication, not to speak of the danger resulting from the enemy's reading the most recent messages in the compromised system.

(17) *Reporting compromise.* Finally, it must be realized that the compromise or capture of cryptographic material is a most serious matter. If there is any reason to suspect that such material or related documents have been compromised, higher authority should be notified by the fastest means possible. Not only is such material available to the enemy for reading current and old messages, but also the cryptanalytic data afforded thereby become most useful in working on similar systems to replace the compromised one. The failure to notify higher authority promptly, if compromise is suspected, may jeopardize the lives of thousands of soldiers and is therefore more serious than permitting compromise to take place, if it could have been avoided. Regulations for reporting compromise should be carefully observed at all times.

REF ID:A56932

PART TWO
ADVANCED MILITARY CRYPTOGRAPHY

CHAPTER 8
TRANSPOSITION SYSTEMS

Section I. MONOPHASE TRANSPOSITION SYSTEMS

85. Transposition Systems Employing Geometric Designs

In part one brief mention was made of the use of geometric designs and figures other than rectangles in producing transposition ciphers. It was stated that triangles, trapezoids, and polygons of various symmetrical shapes can be employed. Figures of these types form connecting links between the methods that use simple rectangular designs and the more complicated methods that use figures in which transposition takes place along diagonals.

86. Trapezoidal Designs

a. A trapezoid or, more accurately, a truncated triangle, of prearranged dimensions as regards the number of cells (which in this case are rhombs into which it is to be partitioned, is constructed. There will be left on one side of the design a series of small triangles which are not to be used for inscribing letters, and are therefore crossed off in the design, as shown in figure 24. Only two agreements are necessary in order to fix the dimensions of the design: a keyword or keyphrase to determine the number of cells at the base of the design, and an understanding as to the height of the design expressed in number of cells. The successive horizontal rows of cells will decrease by one in number from bottom to top of the design. In figure 24, the keyphrase NO CANDY FOR ISSUE is used as a basis for deriving a numerical key of 15 elements, and it is assumed that by prearrangement it was agreed that the height of the design should be eight cells. Therefore, the bottom row has 15 cells, the next one upwards, 14, the next, 13, and so on, to the last, with 8 cells. The inscription may follow any route agreed upon; in the example, it follows the normal manner of writing. The transcription follows the numerical key order, yielding this cryptogram:

REF ID:A56932

ODAIK AEDME HPODV ITEIP NHUET BOBRO
HDTFS EISNI ETBEF BCBTM ESHGA RTORD
IRERE AWARR ERTNS IEPVR VASEO FTEDL
NA

b. Decryptographing is merely the reverse of cryptographing, there being no difficulties provided that the design has been correctly constructed. For this purpose cross-section paper will be found useful. The analysis of such a cryptogram is somewhat complicated by the presence of columns having varying numbers of letters; it may be further complicated by following complex routes in inscription. It is also possible

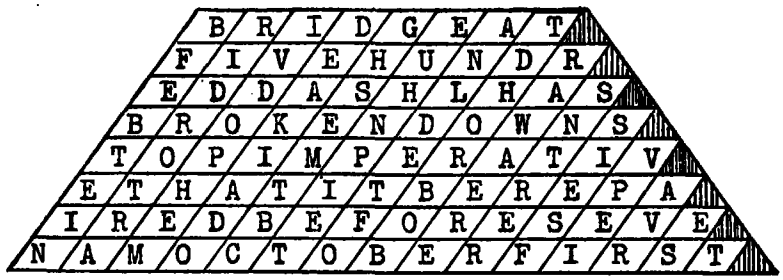


Figure 24.

to follow a numerical key in the inscription of the plain text in horizontal lines; this additional procedure would further complicate and delay solution.

87. Triangular Designs

a. The simplest way of drawing up a triangle for cryptographing is to take cross-section paper, draw a square the side of which is equal to the length agreed upon as expressed in the number of cells, and then draw a diagonal cutting the large square into two equal triangles. This is shown in figure 25, where the length agreed upon is nine, that is, nine cells per side. The letters of the plain text are inscribed in accordance with any prearranged route, the one illustrated in figure 26 being a simple method wherein the letters are inscribed in horizontal lines in the normal manner. When so inscribed, the letters in the diagram will form $2n - 1$ columns where n is the number of cells forming one of the sides of the square from which the triange has been constructed. The total number of letters that can be inscribed within

REF ID:A56932

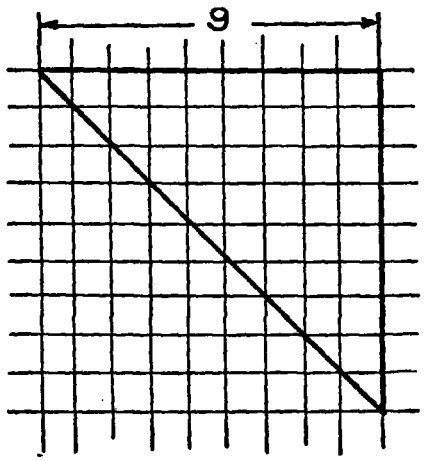


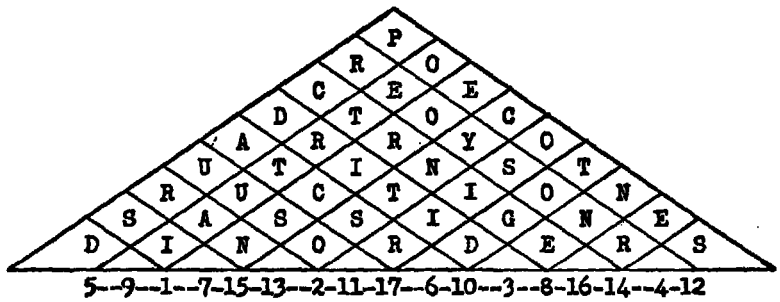
Figure 25.

the triangle is the sum of $n + (n - 1) + (n - 2 + (n - 3) + \ldots + 1$. For a triangle based upon a side of 9 cells, the sum is $9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 = 45$. The letters may then be transcribed to form the cryptogram by following another route, or by following a derived numerical key applied to the base of the triangle. A simple method of deriving a key of $2n - 1$ elements from a key of n elements or letters is exemplified herewith. Let the key be DIAGONALS, a word of nine letters. Extend this key to $2n - 1$ places by repetition, and then assign numerical values as usual:

$n = 9$; $\qquad 2n - 1 = 17$

	1-2-3-4—5—6-7—8—9-10-11-12-13-14-15-16-17
Keyword:	D I A G O N A L S D I A G O N A L
Numerical key:	5-9-1-7-15-13-2-11-17—6-10—3—8-16-14—4-12

This numerical key is the one that has been employed in enciphering the message in Figure 26.

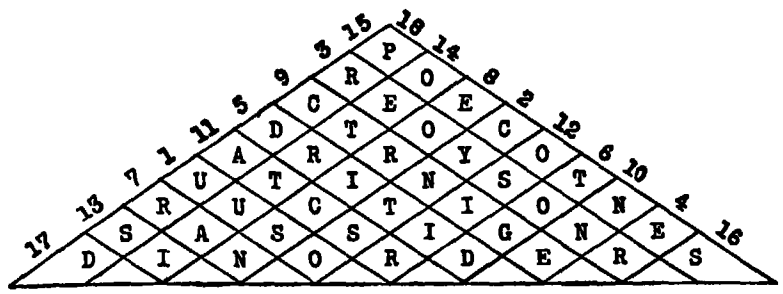


Cryptogram:

RICRC OCSGE DOONI UAOOE
SEYID RTISS DTSNR AUNTN
PERTR

Figure 26.

REF ID:A56932



Cryptogram:

UUSOC YNTSO REOYS ONRER
DRITI DTOGD RANEO RICSN
CTRNI GENNE ATCSR OSIIR
SOIET RTUAI POECO TNESS
DPRCD AURSD

Figure 27.

b. By a slight change in procedure it is possible to encipher a message and produce a text which, for the sake of accuracy in special cases, is double the original length, but which is self-checking. Suppose that instead of applying a single numerical key to the base of the triangle, a double-length key is applied to the legs, as shown in figure 27. Here the key is TRIANGLES, extended to double length by simple repetition, as follows:

	1—2-3-4—5-6-7-8—9-10-11-12-13-14-15-16-17-18
Keyword:	T R I A N G L E S T R I A N G L E S
Numerical key:	17-13-7-1-11-5-9-3-15-18-14—8—2-12—6-10—4-16

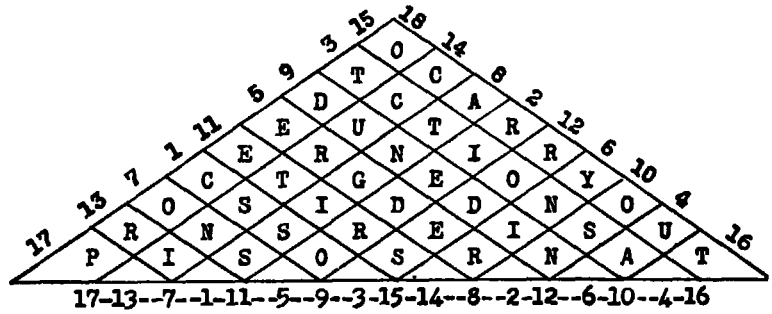
This key is applied to the legs of the triangle beginning at the lower left-hand corner. The transcription then follows key-number order, which results in doubling the length of the message but the repeated letters are scattered throughout the whole message. In decryptographing such a message the clerk merely omits the second occurrence of a letter if it agrees (in identity) with its first appearance in the text.

c. Many variations in inscription and transcription can be employed in the case of triangles as well as trapezoids. Some of the variations in the case of triangles are shown in figure 28.

88. Diagonal Methods

a. A method involving diagonal transposition which is reported to have been employed by the French Army in World War I is now to be described. A numerical key is derived from a fairly long word or phrase, and a rectangle is constructed, as in figure 29. The text is inscribed in this rectangle in normal fashion, nulls being employed, if necessary, to complete the last line of the rectangle.

REF ID:A56932



Inscription: Up left side, down right, alternately.

Transcription: (a) In rows from the base line, left to right and right to left, alternately, upwards:

PISOS RNATU SIERS etc.

(b) In diagonals from right leg, in key-number order:

RIEDR OUAYN etc.

(c) In rows from left leg, in key-number order:

CTGEO YTCEU etc.

(d) From columns in key-number order:

CNROI TUGRU etc.

Figure 28.

Message: ENEMY BATTERY LOCATED AT WOODS 1,000 YARDS SOUTHEAST OF MUMMASBURG HEAVY ARTILLERY STOP THEY ARE FIRING AT RATE OF THREE ROUNDS PER MINUTE FOR THE BATTERY X WILLS, MAJ.

Keyphrase: MIDNIGHT RIDE OF PAUL REVERE.

Enciphering diagram:

M	I	D	N	I	G	H	T	R	I	D	E	O	F	P	A	U	L	R	E	V	E	R	E
15	11	2	16	12	9	10	22	19	13	3	4	17	8	18	1	23	14	20	5	24	6	21	7
E	N	E	M	Y	B	A	T	T	E	R	Y	L	O	C	A	T	E	D	A	T	W	O	O
D	S	O	N	E	T	H	O	U	S	A	N	D	Y	A	R	D	S	S	O	U	T	H	E
A	S	T	O	F	M	U	M	M	A	S	B	U	R	G	H	E	A	V	Y	A	R	T	I
L	L	E	R	Y	S	T	O	P	T	H	E	Y	A	R	E	F	I	R	I	N	G	A	T
R	A	T	E	O	F	T	H	R	E	E	R	O	U	N	D	S	P	E	R	M	I	N	U
T	E	F	O	R	T	H	E	B	A	T	T	E	R	Y	X	W	I	L	L	S	M	A	J

Cryptogram:

ADARR SESAR NUANX YAAPH HAURA UWYPW
RHEDO TETFS HETBE RTOIL TGIMO EITJO
YRURB TMSFT AHUTT NSLAE YEFYO RESTE
AESII EDLRT MNORE OLDYO ECAGR YTUMR
BDSVE LOHTN ATOMO ETEFS TANM

Figure 29.

REF ID:A56932

b. The correspondents agree beforehand upon several diagonals which run from left to right, and from right to left and which intersect, thus cutting up the design quite thoroughly. In figure 29 let these selected diagonals be those indicated by the numbers from 1 to 6, inclusive, the odd ones indicating diagonals running from left to right. In the transcription, the letters along the indicated diagonals are first set down in groups of five, proceeding in key-number order. Correspondents must also agree beforehand as to whether a letter which lies at the intersection of two diagonals will be taken both times it is encountered or taken only once and, if so, whether on its first or second appearance. After all these letters have been written down, one then proceeds with the remaining letters in the usual columnar manner, omitting the letters which have already been taken. The cryptographing process will become clear upon the study of the example in figure 29.

89. Interrupted Keyword Transposition

a. This method of transposition is a development of a more simple method wherein the transposition follows a numerical key. The latter must first be described. A keyword or keyphrase of fair length is selected and a numerical key derived from it. Let this key be the phrase UNIFORMITY OF METHOD.

Keyphrase: U N I F O R M I T Y O F M E T H O D
Numerical key: 17-10-6-3-11-14-8-7-15-18-12-4-9-2-16-5-13-1

The plain text is then written out in horizontal lines corresponding to the length of the key; then transposition is effected *within each row,* according to the sequence of numbers applicable, as shown in figure 30.

Message: ADMINISTRATIVE ORDERS MUST BE COMPLETED AND READY TO ACCOMPANY FIELD ORDERS NOT LATER THAN 5:00 P.M. THIS DATE.

Enciphering diagram:

17-10-6-3-11-14-8-7-15-18-12-4-9-2-16-5-13-1

A D M I N I S T R A T I V E O R D E
R S M U S T B E C O M P L E T E D A
N D R E A D Y T O A C C O M P A N Y
F I E L D O R D E R S N O T L A T E
R T H A N F I V E P M T H I S D A T
E

Cryptogram:

EEIIR MTSVD NTDIR OAAAE UPEME BLSSM
DTCTR OYMEC ARTYO DACND OPNAE TLNAE
DROID STOEL FRTIA TDHVI HTNMA FESRP
E

Figure 30.

REF ID:A56932

b. In the foregoing case the encipherment takes place only by transposition within rows, but it is possible to complicate the method by transposing, in addition, the rows as a whole, employing the same key or only a portion of it, as much as is required. Thus, if the message contained 18 rows of 18 letters each, then the transposition of rows could be effected according to key-number order, the last row being taken first (since the number 1 of the numerical key happens in this case to be at the end of the numerical key), the 14th row being taken second (since the number 2 of the numerical key is the 14th number), and so on. Where the message does not contain as many complete rows as there are numbers in the key, the transposition takes place in key-number order nevertheless, the rows being taken in the numerical order of the numbers present. Using the same key and message as in the foregoing case, the encipherment would be as shown in figure 31.

Enciphering diagram:

```
      17-10-6-3-11-14-8-7-15-18-12-4-9-2-16-5-13-1
17:   A  D M I  N  I S T  R  A  T I V E  O R  D E
10:   R  S M U  S  T B E  C  O  M P L E  T E  D A
 6:   N  D R E  A  D Y T  O  A  C C O M  P A  N Y
 3:   F  I E L  D  O R D  E  R  S N O T  L A  T E
11:   R  T H A  N  F I V  E  P  M T H I  S D  A T
14:   E
```

Cryptogram:

```
ETLNA EDROI DSTOE LFRYM ECART YODAC
NDOPN AAEUP EMEBL SSMDT CTROT IATDH
VIHTN MAFES RPEEE IIRMT SVDNT DIROA
A
```

Figure 31

c. From the preceding method it is but a step to the method of interrupted key transposition now to be described. Instead of writing the text in regular-length groups corresponding to the length of the key, it is written out in irregular groups the lengths of which vary according to some prearranged plan. For example, note the basis of the variable grouping in figure 32, which uses the same message and key as in *a* above.

d. This method may be combined with that shown in *b* above, thus further complicating the system. In decryptographing such a message it is best to use cross-section paper, block out the cells to be occupied by letters in the deciphering diagram, and indicate the key numbers applicable to each line. This will facilitate the process materially and help eliminate errors.

REF ID:A56932

Enciphering diagram:

17	10	6	3	11	14	8	7	15	18	12	4	9	2	16	5	13	1
A	D	M	I	N	I	S	T	R	A	T	I	V	E	O	R	D	E
R	S	M	U	S	T	B	E	C	O	M	P	L	E	T	E	D	A
N	D	R	E	A	D	Y	T	O	A	C	C	O	M	P	A	N	Y
F	I	E	L	D	O	R	D	E	R	S	N	O	T	L	A	T	E
R	T	H	A	N	F	I	V	E	P	M	T	H	I	S	D	A	T
E																	

17	10	6	3	11	14	8	7	15	18	12	4	9	2	16	5	13	1
A	D	M	I	N	I	S	T	R	A	T	I	V	E	O	R	D	E
R	S	M	U	S	T	B	E	C	O	M	P	L	E	.	.	.	.
T	E	D	A	.	.	.	.	.	.	.	.	.	.	.	.	.	.
N	D	R	E	A	D	Y	T	O	A	C	C	.	.	.	.	.	.
O	M	P	A	N	Y	F	I	E	L	D	O	R	D	E	R	.	.
S	N	O	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
T	L	A	T	E	R	T	H	.	.	.	.	.	.	.	.	.	.
A	N	F	I	V	E	P	.	.	.	.	.	.	.	.	.	.	.
M	T	H	I	S	D	A	T	E	(L	C	E	P)*	.	.	.	.	.

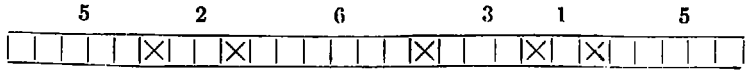
(*The four final letters LCEP are nulls, to complete the row.)

Cryptogram (columnar transposition in key-number sequence):

EEEDI UAEAT IIIPC OERRM MDRPO AFHTE
TIHTS BYFTP AVLRP DSEDM NLNTN SANEV
STMCD CDITD YREDR COEEO EARTN OSTAM
AOALL

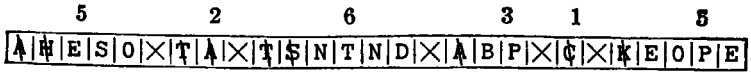
Figure 32.

e. Another method of interrupted transposition is that which employs a rather long sequence of digits to control the interruption. In order to avoid the necessity of carrying around such a written sequence, it is possible to agree upon a number whose reciprocal when converted by actual division into its equivalent decimal number will give a long series of digits. For example, the reciprocal of 7, or 1/7, yields a repeating sequence of *six* digits: 142857142857 . . .; the reciprocal of 49, 1/49, yields a repeating sequence of 42 digits, etc. Zeros, when they appear, are omitted from the sequence. Suppose the number 19 is agreed upon, the reciprocal of which yields the sequence (0)52631578947368421. On cross-section paper mark off sets of cells corresponding in number to the successive digits. Thus:



Let the message be ATTACK HAS BEEN POSTPONED.

Encipherment:



Cryptogram:

AHESO TATSN TNDAB PCKEO PE

REF ID:A56932

f. To decryptograph such a message, the cryptogram is written down in a series of cross-section cells, which are then blocked off in sets according to the numerical key:

5	2	6	3	1	5
A H E S O X T A X T S N T N D X A B P X C X K E O P E					

Taking the letters in consecutive order out of the successive sets, and crossing them off the series at the same time as they are being written down to construct the plain text, the message is found to begin with the following two words:

5	2	6	3	1	5
A H E S O X T A X T S N T N D X A B P X C X K E O P E					

ATTACK HAS . . .

g. Preparatory to cryptographing, it is necessary to find the length of the message to be enciphered and then to mark off as many cells as will be required for encipherment. Nulls are used to fill in cells that are not occupied after enciphering the whole message. The secrecy of the method depends, of course, upon the reciprocal selected, but there is no reason why any fraction that will yield a long series of digits cannot be employed. If the selection of key numbers were restricted to reciprocals, the secrecy would be more limited in scope than is actually necessitated by the method itself.

90. Permutation Method

a. An old method, known in literature as the *aerial telegraphy method,*[1] forms the basis of this system. A set of permutations of 3 4, . . . 9 digits is agreed upon and these permutations are listed in a definite series. As an example, let these permutations be made of the digits 1 to 5, selecting only four of the possible 120. Suppose those selected are the following, set down in successive lines of the diagram in figure 33a:

Permutation

2 3 1 5 4	2	3	1	5	4
3 2 5 1 4	3	2	5	1	4
1 5 3 2 4	1	5	3	2	4
4 3 1 5 2	4	3	1	5	2

Figure 33a.

[1] So named because it was first devised and employed in messages transmitted by a system of semaphore signaling in practical usage in Europe before the electrical telegraph was invented.

REF ID:A56932

The letters of the plain text, taken in sets of fives, are distributed within the sections of the diagram in accordance with the permutations indicated above the sections and also at the left. Thus, the first five letters of the text, supposing them to be the initial letters of the word RECOMMENDATIONS, are inserted in the following positions:

Permutation

2 3 1 5 4	2	3	1	5	4
	E	C	R	M	O

The next five letters are inscribed in the second line of the diagram in the sections indicated by the permutation above and at the left of the line. Thus:

Permutation

2 3 1 5 4	2	3	1	5	4
	E	C	R	M	O
3 2 5 1 4	3	2	5	1	4
	N	E	A	M	D

This process is continued for each line and for as many lines as there are permutations indicated at the left. In the foregoing case, after twenty letters have been inserted, one inserts a second set of five letters again on the first line, placing the letters of this second set immediately to the right of those of the first set, respectively in key-number order. The succeeding lines are treated in similar fashion until the whole message has been enciphered. The following example will illustrate the process:

Message: RECOMMENDATIONS FOR LOCATION OF NEW BALLOON POSITIONS MUST BE SUBMITTED BEFORE 12TH AIRDROME COMPANY CHANGES COMMAND POST TOMORROW.

Enciphering diagram:

Permutation

2 3 1 5 4	2	3	1	5	4
	EASEOM	CTIDMA	RCOTRM	MOIECD	OITBEN
3 2 5 1 4	3	2	5	1	4
	NOSRPS	ESNOMO	ANUTNT	MNOFOP	DFMEAT
1 5 3 2 4	1	5	3	2	4
	TESWYO	SLSTNR	OBBLHO	IWTECM	NAEFAR
4 3 1 5 2	4	3	1	5	2
	LNIRCB*	ROMISC*	FLUHGO	OPTDOD*	OOBAEW

* The letters B, C, and D are nulls, to complete the figure.

Figure 33b.

REF ID:A56932

The letters of the cipher text are taken from the diagram according to any prearranged route, the most simple being to transcribe the lines of letters in groups of fives, thus:

EASEO MCTID MARCO TRMNO IECDO ITBEN
NOSRP SESNO MOANU TNTMN OFOPD FMEAT
TESWY OSLST NROBB LHOIW TECMN AEFAR
LNIRC BROME SCFLU HGOOP TDODO OBAEW

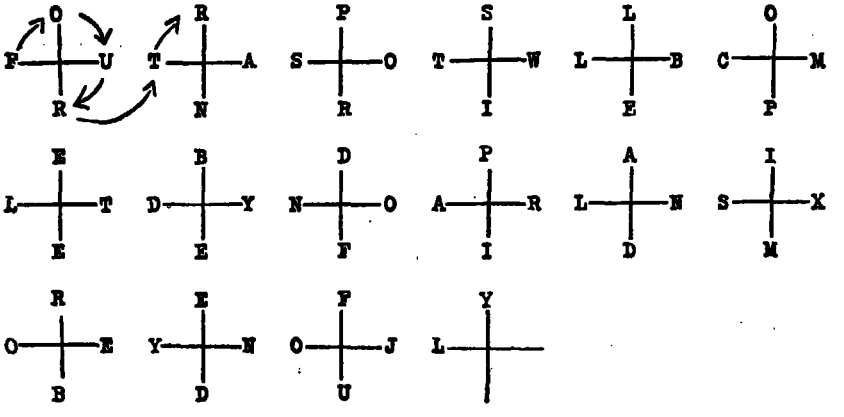
b. The foregoing method when employed in its most simple form does not yield cryptograms of even a moderate degree of security; but if the method of inscription and transcription is varied and made more complex, the degree of security may be increased quite noticeably. It is possible to use longer permutations, based on sets of 6, 7, 8, or 9 digits, but in every case the successive permutations must be prearranged as regards both their exact composition and their order or arrangement in the diagram.

91. Transposition Method Using Special Figures

a. The method now to be described is useful only in special cases where the correspondence is restricted to brief communications between a very limited number of persons. It is necessary to agree in advance on certain particulars, as will be seen. Let the message to be enciphered be the following:

FOUR TRANSPORTS WILL BE COMPLETED BY END OF APRIL AND SIX MORE BY END OF JULY.

Note the following figures and encipherment:



Cryptogram:

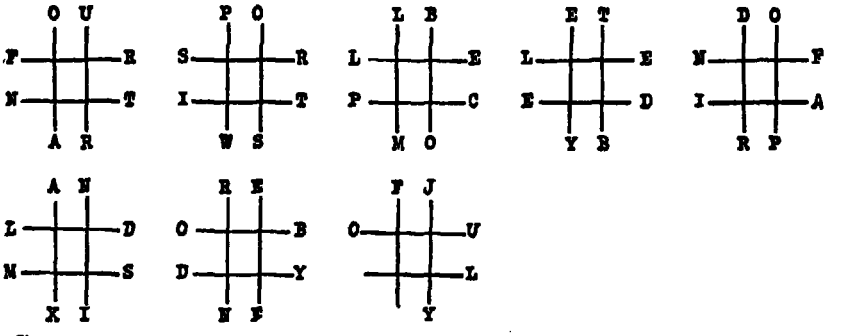
ORPSL OFUTA SOTWL BCMRN RIEPE BDPAI
LTDYN OARLN SXEEF IDMRE FYOEY NOJLB
DU

Figure 34.

REF ID:A56932

b. It will be noted that it is essential to agree in advance not only upon the nature of the figure but also upon the *number* of figures per line.

c. The next series is a modification of the preceding. The same message will be employed, with a double-cross figure, five figures per line.

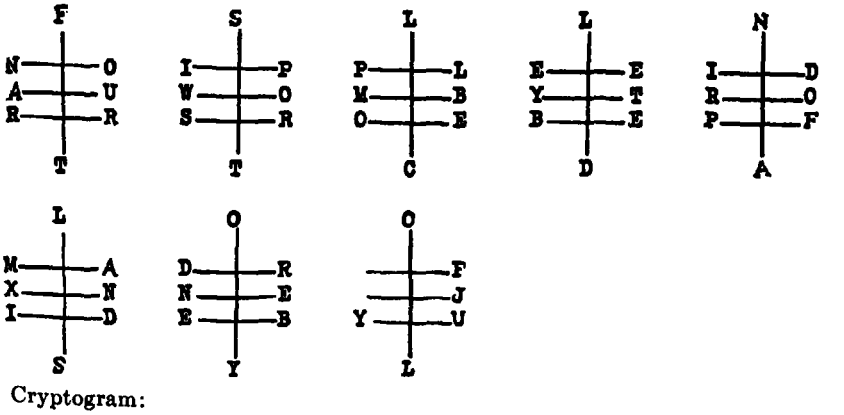


Cryptogram:

OUPOL BETDO FRSRL ELENF NTITP CEDIA
ARWSM OYBRP ANREF JLDOB OUMSD YLXIN
EY

Figure 35.

d. Still another series may be formed, as follows:



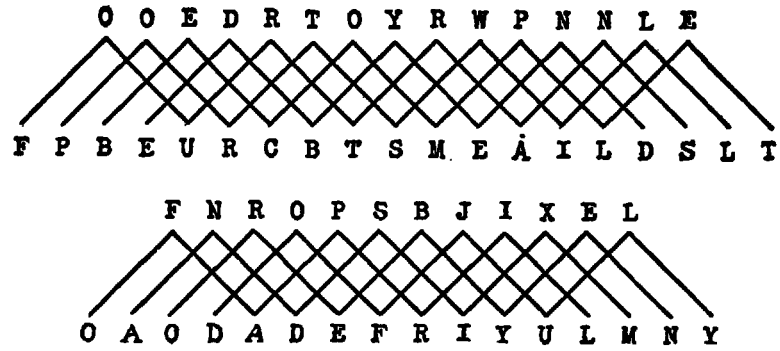
Cryptogram:

FSLLN NOIPP LEEID AUWOM BYTRO RRSRO
EBEPF TTCDA LOOMA DRFXN NEJID EBYUS
YL

Figure 36.

e. A figure of different form than the preceding forms the basis of the next type.

REF ID:A56932



Cryptogram:

OOEDR TOYRW PNNLE FPBEU RCBTS
MEAIL DSLTF NROPS BJIXE LOAOD
ADEFR IYULM NY

Figure 37.

f. From the foregoing examples, it is obvious that many other figures may be used for effective transpositions of this kind, such as stars of varying numbers of points, polygons of various symmetrical shapes, etc. It is merely necessary to agree upon the figures, the number of figures per line, the starting points of the inscription and transcription processes.

g. The method lends itself readily to combination with simple monoalphabetic substitution, yielding cryptograms of a rather high degree of security.

Section II. POLYPHASE TRANSPOSITION SYSTEMS

92. Polyphase Transposition Methods in General

a. In paragraph 33, brief mention was made of transposition systems in which two or more processes of rearrangement are involved. It was stated that only a very limited number of such transposition methods are practicable for military use, but that the degree of security afforded by them is considerably greater than that afforded by certain much more complicated substitution methods. The methods referred to are those which involve two or more successive transpositions, and merely for purposes of brevity in reference they will here be called *polyphase transposition methods* to distinguish them from the single monophase methods thus far described.

b. It is obvious that a polyphase transposition method may involve 2, 3, . . . successive transpositions of the letters of the plain text. To describe these methods in general terms, one may indicate that the letters resulting from a first transposition, designated as the T–1

REF ID:A56932

transposition, form the basis of a second, or T–2 transposition. If the process is continued, there may be T–3, T–4 . . . transpositions, and each may involve the use of a geometric figure or design. For convenience, the design involved in accomplishing the T–1 transposition may be designated as the D–1 design; that involved in accomplishing the T–2 transposition as the D–2 design, etc. However, it may as well be stated at this point, that so far as military cryptography is concerned, methods which involve more than D–2 and T–2 elements are entirely impractical and often those which involve no more than D–2 and T–2 elements are also impracticable for such use.

93. True and False Polyphase Transpositions

a. It is possible to perform two or more transpositions with the letters of a text and yet the final cryptogram will be no more difficult to solve than if only a single transposition had been effected. The equivalent of this in the case of substitution ciphers is to encipher a monoalphabetic cryptogram by means of a second single alphabet; the final result is still a monoalphabetic substitution cipher. Likewise, if a message had been enciphered by a simple form of route transposition and a second and similar or approximately similar form of simple route transposition is again applied to the text of the first transposition, the final text is still that of a monophase transposition cipher. Again, two transpositions may be accomplished without really affecting a more thorough scrambling of the letters composing the original text. Examples will serve to clarify the differences between false and true polyphase transposition.

b. Note the following simple columnar transposition cipher prepared according to the method described in paragraph *27*:

Message: DELIVER ALL AMMUNITION TO 4TH DIVISION DUMP

Keyword: SCHEDULE = S C H E D U L E / 7-1-5-3-2-8-6-4

Enciphering rectangle:

7	1	5	3	2	8	6	4
D	E	L	I	V	E	R	A
L	L	A	M	M	U	N	I
T	I	O	N	T	O	F	O
U	R	T	H	D	I	V	I
S	I	O	N	D	U	M	P

D–1

Cryptogram (T–1):

ELIRI VMTDD IMNHN AIOIP LAOTO RNFVM
DLTUS EUOIU

Figure 38.

REF ID:A56932

In producing the foregoing cryptogram only the columns were transposed. Suppose that by prearrangement, using the keyword BREAK (derived numerical key = 2–5–3–1–4), the horizontal lines of the foregoing enciphering rectangle were also to be transposed. For example, let the horizontal lines of the rectangle D–1 be transposed immediately before taking the letters out of the columns of the design (in key-number order) to form the cipher text. Thus:

2	D	E	L	I	V	E	R	A
5	L	L	A	M	M	U	N	I
3	T	I	O	N	T	O	F	O
1	U	R	T	H	D	I	V	I
4	S	I	O	N	D	U	M	P

D–1

7	1	5	3	2	8	6	4
U	R	T	H	D	I	V	I
D	E	L	I	V	E	R	A
T	I	O	N	T	O	F	O
S	I	O	N	D	U	M	P
L	L	A	M	M	U	N	I

D–2

Cryptogram (T–2):

REIIL DVTDM HINNM IAOPI TLOOA VRFMN
UDTSL IEOUU

Figure 39.

c. The foregoing, however, is not a case of true polyphase or so-called *double* transposition. The same final result may be accomplished in a way which will at first glance appear quite different but is in reality one that accomplishes the same two operations by combining them in one operation. Let the message be inscribed as before, but this time with both numerical keys applied to the top and side of the rectangle. Then let another rectangle of the same dimensions, but with numbers in straight sequence instead of key-number sequence, be set alongside it. Thus:

	7	1	5	3	2	8	6	4
2	D	E	L	I	V	E	R	A
5	L	L	A	M	M	U	N	I
3	T	I	O	N	T	O	F	O
1	U	R	T	H	D	I	V	I
4	S	I	O	N	D	U	M	P

D–1

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								

D–2

Figure 40.

Each letter D–1 is now transferred to that cell in D–2 which is indicated by the row and column indicators of the letter in D–1. For example, the first letter, D, of D–1, has the indicators 2–7 and it is placed in

REF ID:A56932

the 2–7 cell in D–2; the second letter of D–1, which is E, is placed in the 2–1 cell of D–2, and so on. The final result is as follows:

	7	1	5	3	2	8	6	4
2	D	E	L	I	V	E	R	A
5	L	L	A	M	M	U	N	I
3	T	I	O	N	T	O	F	O
1	U	R	T	H	D	I	V	I
4	S	I	O	N	D	U	M	P

D–1

	1	2	3	4	5	6	7	8
1	R	D	H	I	T	V	U	I
2	E	V	I	A	L	R	D	E
3	I	T	N	O	O	F	T	O
4	I	D	N	P	O	M	S	U
5	L	M	M	I	A	N	L	U

D–2

Figure 41.

It will be seen that if the columns of D–2 are now read downwards in straight order from left to right the final cryptogram is identical with that obtained in figure 39: REIIL DVTDM, etc.

d. The foregoing cipher, often called the Nihilist Cipher, is referred to in some of the older literature as a double transposition cipher because it involves a transposition of both columns and rows; and indeed as described in *b* above it seems to involve a double process. It is, however, not an example of true double transposition. When the mechanism of this cipher is compared with that now to be described, the great difference in the cryptographic security of the two methods will become apparent.

94. True Double Transposition

In the form of the false double transposition described above, it is only entire columns and entire rows that are transposed. The disarrangement of the letters is after all not very thorough. In true double transposition this is no longer the case, for here the letters of columns and rows become so thoroughly rearranged that the final text presents a complete scrambling almost as though the letters of the message had been tossed into a hat and then drawn out at random.

Section III. TRUE DOUBLE TRANSPOSITION

95. True Double Transposition of the Columnar Type

a. It is by what is apparently a simple modification of certain of the columnar methods already described that an exceedingly good true double transposition can be effected. Let a numerical key be derived from a keyword in the usual manner and let the message be written out under this key to form a rectangle in the usual manner for columnar transposition. The length of the message itself determines the exact dimensions of the rectangle thus formed, and whether or not it is completely or incompletely filled.

REF ID:A56932

b. In its most effective form the double transposition is based upon an incompletely filled rectangle; that is, one in which one or more cells in the last line remain unfilled. An example of the method now follows: Let the keyword be INTERNATIONAL; the message to be enciphered, as follows:

OUR ATTACK SLOWING UP IN FRONT OF HILL 1000 YARDS SOUTHEAST OF GOLDENVILLE STOP REQUEST PROMPT REENFORCEMENT.

Keyword: I N T E R N A T I O N A L
Derived numerical key: 4-7-12-3-11-8-1-13-5-10-9-2-6

4	7	12	3	11	8	1	13	5	10	9	2	6
O	U	R	A	T	T	A	C	K	S	L	O	W
I	N	G	U	P	I	N	F	R	O	N	T	O
F	H	I	L	L	O	N	E	T	H	O	U	S
A	N	D	Y	A	R	D	S	S	O	U	T	H
E	A	S	T	O	F	G	O	L	D	E	N	V
I	L	L	E	S	T	O	P	R	E	Q	U	E
S	T	P	R	O	M	P	T	R	E	E	N	F
O	R	C	E	M	E	N	T					

D-1

4	7	12	3	11	8	1	13	5	10	9	2	6
A	N	N	D	G	O	P	N	O	T	U	T	N
U	N											

D-2

Figure 42a.

REF ID:A56932

The first, or D–1, rectangle is inscribed in the usual manner of simple numerical key columnar transposition. It is shown as D–1 in the accompanying figure. *The letters of T–1 transposition* are then inscribed in the second, or D–2, rectangle *in the normal manner of writing,* that is, from left to right and from the top downwards. This is shown in D–2 of figure 42a for the first two columns of D–1 (in numerical key order) after transfer of their letters into D–2. The letters of the remaining columns of D–1 are transferred in the same manner into D–2, yielding the following rectangle:

4	7	12	3	11	8	1	13	5	10	9	2	6
A	N	N	D	G	O	P	N	O	T	U	T	N
U	N	A	U	L	Y	T	E	R	E	O	I	F
A	E	I	S	O	K	R	T	S	L	R	R	W
O	S	H	V	E	F	U	N	H	N	A	L	T
R	T	I	O	R	F	T	M	E	L	N	O	U
E	Q	E	S	O	H	O	D	E	E	T	P	L
A	O	S	O	M	R	G	I	D	S	L	P	C
C	F	E	S	O	P	T	T					

Figure 42b.

For the T–2 text the letters are transcribed from the D–2 rectangle, reading down the columns in key-number order, and grouping the letters in fives. The cryptogram is as follows:

PTRUT OGTTI RLOPP DUSVO SOSAU AOREA
CORSH EEDNF WTULC NNEST QOFOY KFFHR
PUORA NTLTE LNLES GLOER OMONA IHIES
ENETN MDIT

e. In paragraph 29 a variation of the simple columnar key method of transposition was described. If the process therein indicated is repeated, double transposition is effected. The following example will serve to illustrate the method, using the same message and key as were used in the paragraph 29:

Message: REQUEST IMMEDIATE REENFORCEMENTS

Keyword: P R O D U C T
Derived numerical key: 4–5–3–2–7–1–6

REF ID:A56932

Encipherment:

```
     4-5-3-2-7-1-6  4-5-3-2-7-1-6  4-5-3-2-7-1-6
Text: R E Q U E S T  I M M E D I A  T E R E E N F
T-1: S I N E U E E  E Q M R C R I  T O T E M E R
T-2: E R E E E R E  F N M T A S E  T S E I Q O T

     4-5-3-2-7-1-6  4-5
     O R C E M E N  T S
     S T A F N E D  E M
     M E I R D U C  M N
```

Cryptogram:

```
EREEE REFNM TASET SEIQO TMEIR
DUCMN
```

d. In some respects this modified method is simpler for the novice to perform correctly than is that employing rectangles. Experience has shown that many inexpert cryptographic clerks fail to perform the two transpositions correctly when D–1 and D–2 rectangles are employed in the work.

96. General Remarks on True Polyphase Transposition

a. The cryptographic security of the true double transposition method deserves discussion. Careful study of a cryptogram enciphered by the double transposition method set forth in paragraph 95 *b* and *c* will indicate that an extremely thorough scrambling of the letters is indeed brought about by the method. Basically, its principle is the splitting up of the adjacent or successive letters constituting the plain text by *two* sets of "cuts", the second of which is in a direction that is perpendicular to the first, with the individual "cuts" of both sets arranged in a variable and irregular order. It is well adapted for a regular and voluminous exchange of cryptograms between correspondents, because even if many messages in the same key are intercepted, *so long as no two messages are identical in length,* they can only be cryptanalyzed after considerable effort.

b. Triple and quadruple transpositions of the same nature are possible but not practical for serious usage. Theoretically, a continuation or repetition of the tranposition process will ultimately bring about a condition wherein the D–n rectangle is identical with the D–1 rectangle; in other words, after a certain number of transpositions the rectangle produced by a repetition of the *cryptographing* process results finally in *decryptographing* the message. Exactly how many repetitive transpositions intervene in such cases is extremely variable and depends upon factors lying outside the scope of this text.

REF ID:A56932

c. In the example of cryptographing given in paragraph 95*b*, the D–1 and D–2 rectangles are identical in dimensions, and identical numerical keys are applied to effect the T–1 and T–2 transpositions. It is obvious, however, that it is not necessary to maintain these identities; D–1 and D–2 rectangles of different dimensions may readily be employed, and even if it is agreed to have the dimensions identical, the numerical keys for the two transpositions may be different. Furthermore, it is possible to add other variable elements. (1) The direction or manner of inscribing the letters in the D–1 rectangle may be varied; (2) the direction of reading off or taking the letters out of the D–1 rectangle in effecting the T–1 transposition, that is, in transferring them into the D–2 rectangle, may be varied; (3) the direction of inscribing these letters in the D–2 rectangle may be varied; (4) the direction of reading off or taking the letters out of the D–2 rectangle in effecting the T–2 transposition may be varied.

d. The solution of cryptograms enciphered upon the double transposition principle is often made possible by the presence of certain plain-text combinations, such as QU and CH (in German). For this reason, careful cryptographers substitute a single letter for such combinations, as decided upon by preagreement. For example, in one case the letter Q was invariably used as a substitute for the compound CH, with good effect.

Section IV. GRILLES AND OTHER TYPES OF MATRICES

97. Type of Cryptographic Grilles

Broadly speaking, cryptographic grilles[2] are sheets of paper, cardboard, or thin metal in which perforations have been made for the uncovering of spaces in which letters (or groups of letters, syllables, entire words) may be written on another sheet of paper upon which the grille is superimposed. This latter sheet, usually made also of cross-section paper, will hereafter be designated for purposes of brevity in reference as the *grille grid,* or *grid.* Its external dimensions are the same as those of the grille. Grilles are of several types depending upon their construction and manner of employment. They will be treated here under the titles of (1) simple grilles, (2) revolving grilles, (3) nonperforated grilles, and (4) "post card" grilles.

98. Simple Grilles

a. These consist usually of a square in which holes or apertures have been cut in prearranged positions. When the grille is superimposed upon

[2] Also often called "stencils." The general term *matrix* (plural, *matrices*) is very useful in referring to a geometric figure or diagram used for transposition purposes. Other terms in common use are *cage, frame, box,* etc.

REF ID:A56932

the grid, these apertures disclose cells on the grid, in which cells letters, groups of letters, syllables, or entire words may be inscribed. An example is shown in figure 43. The four sides of the obverse surface of the grille are designated by the figures 1, 2, 3, 4; the four sides of the reverse surface, by the figures 5, 6, 7, 8. These figures are employed to indicate the position of the grille upon the grid in encipherment.

b. (1) In cryptographing a message the grille is placed upon the grid, in one of the eight possible positions: Obverse surface up, with figure 1, 2, 3, or 4 at the top left; or reverse surface up, with

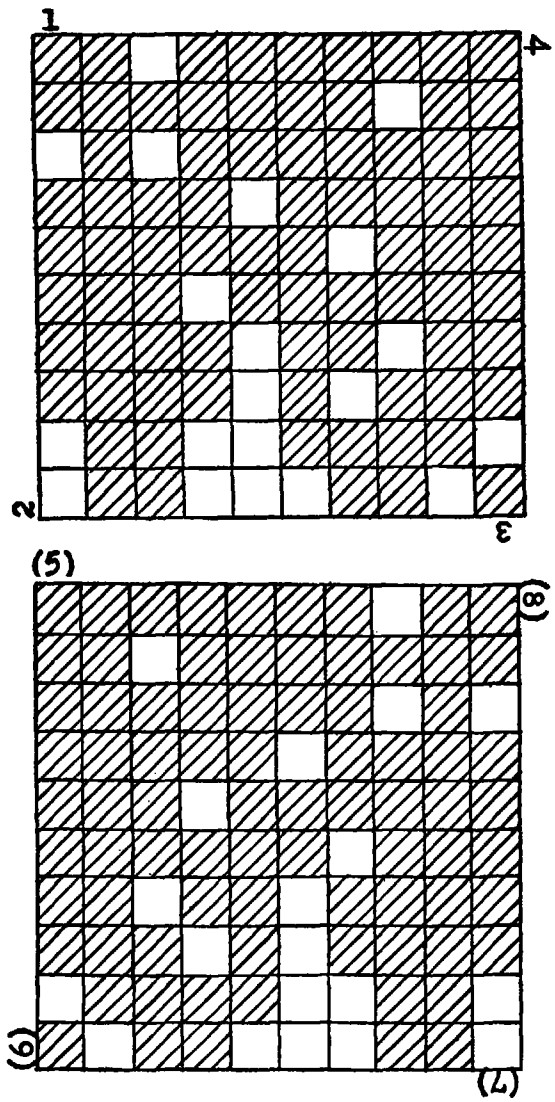


Figure 43.

REF ID:A56932

figure 5, 6, 7, or 8 at the top left. The letters of the plain text are then inscribed in the cells disclosed by the apertures, following any prearranged route. In figure 44, the normal manner of writing, from left to right, and from the top downwards, has been followed in the inscription, the message being ALL DESTROYERS OUTSIDE.

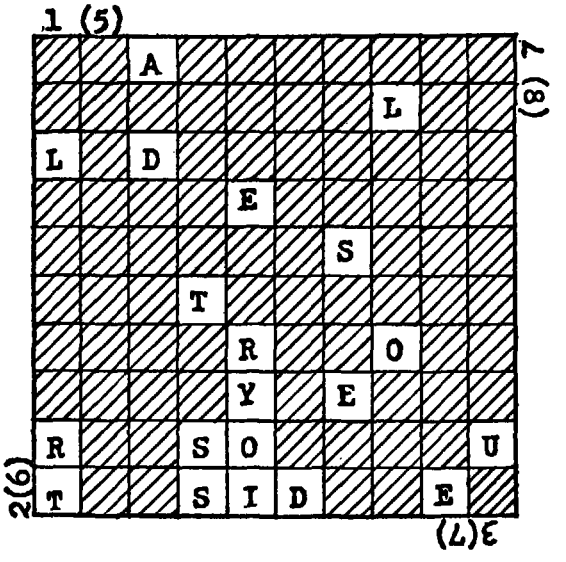


Figure 44.

(2) The transcription process now follows. The cipher text is written down, the letters being taken by following any prearranged route, which must be perpendicular to the route of inscription, otherwise the letters will follow in plain-text order. In the following, the route is by columns from left to right.

Cryptogram:

LRTAD TSSER YOIDS ELOEU

(3) If the number of letters of the plain-text message exceeds the number of cells disclosed by one placement of the grille, the letters given by this placement are written down (in cryptographic order), and then the grille is placed in the next position on a fresh grid; the process is continued in this manner until the entire message has been cryptographed. The several sections of the cipher letters resulting from the placements of the grille on successive grids merely follow each other in the final cryptogram. In this manner of employment it is only necessary for the correspondents to agree upon the initial position of the grille and its successive positions or placements.

REF ID:A56932

c. It is obvious that by the use of a simple grille the letters of a message to be cryptographed may be distributed within an enveloping message consisting mostly of "dummy" text, inserted for purposes of enabling the message to escape suppression in censorship. For example, suppose the grille shown in figure 43 is employed in position 1 and the message to be conveyed is ALL DESTROYERS OUTSIDE. The letters of this message are inscribed in their proper places on the grid, exactly as shown in figure 44. An "open" or disguising text is now to be composed; the latter serving as an envelope or "cover" for the letters of the secret text, which remain in the positions in which they fall on the grid. The open or disguising text, in other words, is built around or superimposed on the secret text. Note how this is done in figure 45, with an apparently innocent message reading:

I HAVE WORKED VERY WELL ALL DAY, TRYING TO GET EVERYTHING STRAIGHTENED UP BEFORE GOING ON MY NEXT TRIP SOUTH, BUT INSIDE TEN DAYS . . .

1 (5)

I	H	A	V	E	W	O	R	K	E	4 (8)
D	V	E	R	Y	W	E	L	L	A	
L	L	D	A	Y	T	R	Y	I	N	
G	T	O	G	E	T	E	V	E	R	
Y	T	H	I	N	G	S	T	R	A	
I	G	H	T	E	N	E	D	U	P	
B	E	F	O	R	E	G	O	I	N	
G	O	N	M	Y	N	E	X	T	T	
R	I	P	S	O	U	T	H	B	U	
T	I	N	S	I	D	E	T	E	N	

2 (6) 3 (7)

Figure 45.

d. The foregoing method naturally requires the transmission of considerably more text than is actually necessary for conveying the message intended. Where questions of censorship are not involved, the method is therefore impractical. A modification of the method suggests itself in the use of a transparent sheet of paper superimposed upon a square or other figure in which the individual cells are irregularly numbered and the inscription process follows the sequence of numbers. An example is shown in figure 46, using the message ROCK CREEK BRIDGE WILL BE DESTROYED WHEN TAIL HAS CROSSED.

REF ID:A56932

16	3	25	21	39	44	7	15
6	37	29	41	1	11	45	31
23	18	43	10	24	20	28	14
34	12	8	42	48	4	33	38
2	35	47	30	5	46	26	17
27	19	13	32	22	40	36	9

a

W	C	T	E	H	O	E	E
R	I	E	S	R	R	S	W
E	L	R	B	S	B	Y	G
N	I	E	C	D	K	E	L
O	T	E	D	C	S	R	I
O	L	D	H	D	A	A	K

b

Figure 46.

The transcription may now follow any prearranged route. The normal method of reading would produce the cryptogram beginning WCTEH OEERI, etc. It is obvious that the correspondents must possess designs with identically numbered cells.[3]

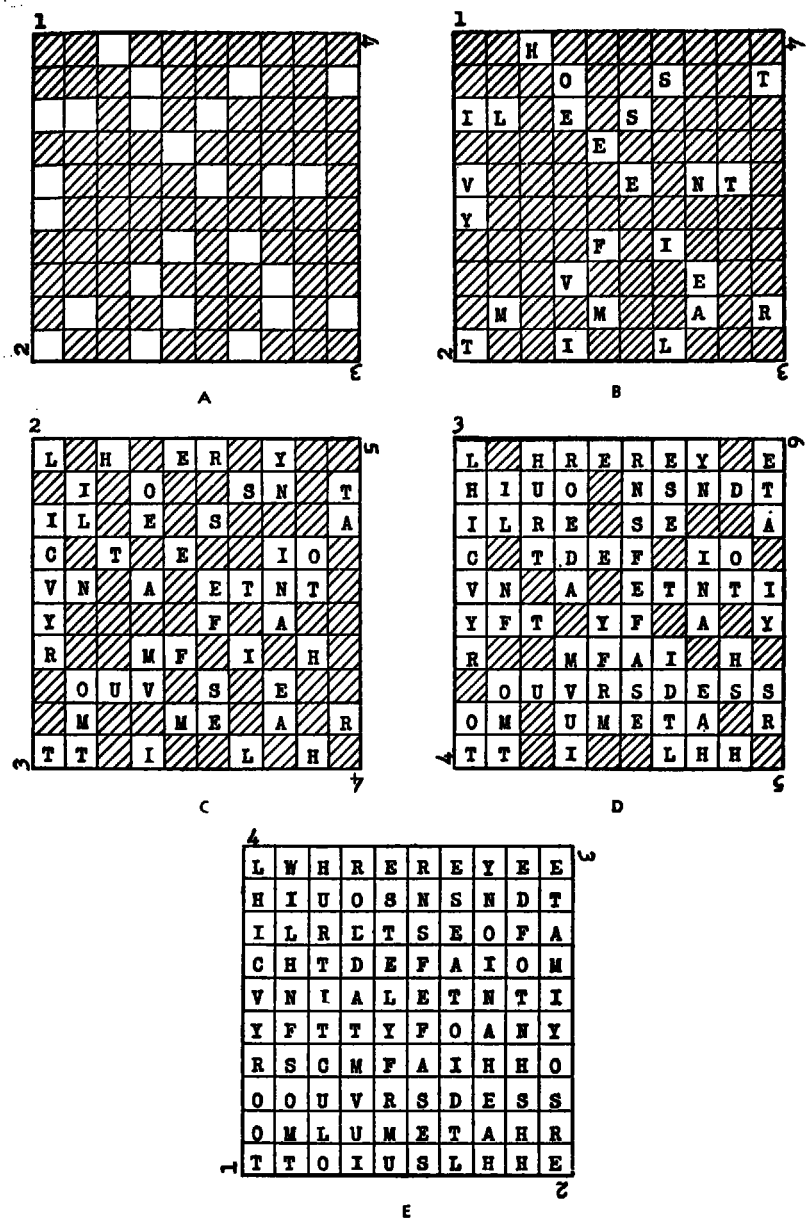
99. Revolving Grilles

a. In this type of grille (see fig. 47a) the apertures are also formed by perforating a sheet of cross-section paper according to prearrangement, but these apertures are so distributed that when the grille is turned four times successively through angles of 90° and set in four *grille positions* on the grid, all the cells on the grid are disclosed in turn. (The preparation of such grilles is discussed in par. 103.) If letters are inserted in the cells so disclosed, then after a complete revolution of the grille every one of the cells of the grid will contain a letter and thus the grid will be completely filled. For this reason such a grille is also called a *self-filling,* or an *automatic-completion* grille. The secrecy of messages enciphered by its means is dependent upon the distribution or position of the apertures, the sequence of grille positions on the grid, that is, whether in the order 1, 2, 3, 4 clockwise; or 1, 3, 4, 2 etc.), and the route followed in inscribing and transcribing the letters in the cells of the grid. For each position of the grille, one-fourth the total number of letters of the text is inscribed; hence it is convenient to refer to "sections" of the text, it being understood that each section consists of one-fourth the total number of letters.

b. There are two possible procedures so far as the inscription-transcription sequence is concerned. (1) The letters of the plain text may be inscribed in the cells of the grid through the apertures disclosed by the grille and then, when the grid has been completely filled, the grille removed, and the letters transcribed from the grid according to a prearranged route; or, (2) the letters of the plain text may first be inscribed in the cells of the grid according to a prearranged route and then the grille applied to the completely-filled grid to give the sequence of letters

[3] The system employed by the French Army in 1886 was of the nature here described.

REF ID:A56932



Cryptogram:

LHICV YROOT WILHN FSOMT
HURTI TCULO ROEDA TMVUI
ESTEL YFRMU RNSFE FASES
ESEAT OIDTL YNOIN AHEAH
EDFOT NHSHH ETAMI YOSRE

Figure 47.

REF ID:A56932

forming the cipher text of the transcription process. The first method will be described in *c* below; the second in *e* below.

c. Taking the simplest manner of inscribing the letters, that is, from left to right and from the top downwards, the letters of the first section of the text are inscribed in the cells disclosed by the apertures, the grille being in the first position. This is shown in b of figure 47. The grille is then given ¼ turn clockwise, bringing figure 2 to the top left. If the grille has been correctly prepared, none of the cells disclosed in the second grille position on the grid will be occupied by a letter. The letters of the second section are then inscribed, this being shown in c of figure 47. In d and e of figure 47, the results of inscribing the third and fourth sections, respectively, are shown. The letters of the cryptogram are then taken out of the completed grid by following any prearranged route of transcription. The cryptogram below has been transcribed by following down the columns in succession from left to right.

d. To decryptograph such a message, the cipher letters are inscribed columnwise in a grid 10 by 10 (that is, one composed of 100 cells, 10 per side) and then the grille applied to the square in four consecutive positions corresponding to those used in cryptographing. The letters disclosed by each placement of the grille are written down as they appear, section after section.

e. The second manner of employing a revolving grille is merely the reciprocal of the first. The procedure followed in the first method to *decryptograph* a message is followed in the second method to *cryptograph* a message; and the procedure followed in the first method to cryptograph is followed in the second method to decryptograph.

100. Grilles of Other Geometric Forms

Grilles are not limited to square-shaped figures. They may be equilateral triangles, pentagons, hexagons, and so on. Any figure which can be pivoted upon a central point and which when revolved upon this pivot can be placed in a succession of homologous positions over a grid corresponding to the grille will serve equally well. A triangle affords three grille positions, a pentagon, five, and so on.

101. Polyphase Transposition by Grilles

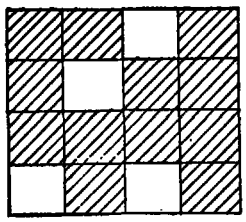
One grille may be employed to inscribe the letters of the message on the grid, and a second, and different, grille employed to transcribe them from the grid to form the final text of the cryptogram. This would constitute a real double transposition method of great complexity. Polyphase transposition by a series of grilles is of course possible.

REF ID:A56932

102. Increasing the Security of Revolving Grilles

a. The total number of letters which a grille will exactly encipher is termed its *capacity.* If the number of letters of a message is always equal to the total capacity of the grille, this information is of great aid in solution by the enemy. For example, a message of 64 letters indicates a grille 8 by 8 with 16 apertures; one of 144 letters, a grille 12 by 12 with 36 apertures, and so on. There are, however, methods of employing a grille so that it will serve to encipher messages the lengths of which are greater or less than the capacity of the grille.

b. When the total number of letters is less than the capacity of the grille, no modification in method of use is necessary. Encipherment of such a message comes to a close when the last plain-text letter has been inscribed. In decryptographing such a message, the recipient must strike out, on the grid upon which he is to inscribe the cipher text, a number of cells corresponding to the difference between the number of letters of the text as received and the total capacity of the grille. The location of the cells to be thus eliminated must be prearranged, and it is best usually to strike them off from the final positions of the grid.



a

15	29	1	30	19	33	5	
42	2	16	43	46	6	20	
17	44	31	18	21	47	34	
3	32	4	45	7	35	8	
25	38	11	39	22	36	9	
50	12	26	51	48	10	23	
27	52	40	28	24	49	37	
13	41	14					

b

Figure 48.

c. When the total number of letters is equal to or greater than the capacity of the grille, a grid of greater capacity than that of the grille can be prepared, on which the grille may be positioned several times, thus forming a large or composite grid composed by the juxtaposition of the several small grids. If there are a few cells in excess of the actual number required, these may be struck off from the large grid at prearranged points, for example, from the last column and row, as shown in b of figure 48. The grille is then placed in its first position in turn on each of the component grids, then in its second position, and so on. An example will serve to illustrate. A message of fifty-two letters is to be

REF ID:A56932

enciphered with the grille shown in a of figure 48, the capacity of which is sixteen letters. The number of letters of the message being greater than three times sixteen, the composite grid must be composed of four small grids containing a total of sixty-four cells. Therefore, twelve of these cells must be eliminated. These are shown in b of figure 48, together with the number indicating the positions occupied by the letters of the text.

103. Construction of Revolving Grilles

a. There are several ways of preparing revolving grilles, of which the one described below is the most simple. All methods make use of cross-section paper.

b. Suppose a revolving grille with a capacity of 100 letters is to be constructed. The cells of a sheet of cross-section paper 10 by 10 are numbered consecutively in *bands* from the outside to the center, in the manner shown in a of figure 49. It will be noted that in each band, if n is the number of cells forming one side of the band, the highest number assigned to the cells in each band is $n - 1$.

c. It will be noted that in each band there is a quadruplication of each digit; the figure 1 appears four times, the figure 2 appears four times, and so on. From each receding band there is to be cut out $(n-1)$ cells: from the outermost band, therefore, nine cells are to be cut out; from the next band, seven; from the next, five; from the next, three; and from the last, one cell. In determining specifically what cells are to be cut out in each band, the only rules to be observed are these: (1) One and only one cell bearing the figure 1 is to be cut out, one and only one cell bearing the figure 2 is to be cut out, and so on; (2) as random a selection as possible is to be made among the cells available for selection for perforation. In b of figure 49 is shown a sample grille prepared in this way.

d. If the side of the grille is composed of an odd number of cells, the innermost band will consist of but one cell. In such case this central cell must not be perforated.

e. It is obvious that millions of differently perforated grilles may be constructed. Grilles of fixed external dimensions may be designated by indicators, as was done by the German Army in 1915 when this system was employed. For example, the FRITZ grille might indicate a 10 by 10 grille, serving to encipher messages of about 100 letters; the ALBERT grille might indicate a 12 by 12 grille, serving to encipher messages of about 144 letters, and so on. Thus, with a set of grilles of various dimensions, all constructed by a central headquarters and distributed to lower units, systematic use of grilles for messages of varying lengths can be afforded.

f. A system for designating the positions of the perforated cells of a grille may be established between correspondents, so that the necessity

REF ID:A56932

for physical transmission of grilles for intercommunication is eliminated. An example of a possible system is that which is based upon the coordinate method of indicating the perforations. The columns from left to right and the rows from bottom to top are designated by the letters A, B, C, . . . Thus, the grille shown in b of figure 49 would have the following formula:

ADG; BBEH; CDJ; DEG; EACH; FFI; GE; HBDHJ; IDG; JABFI.

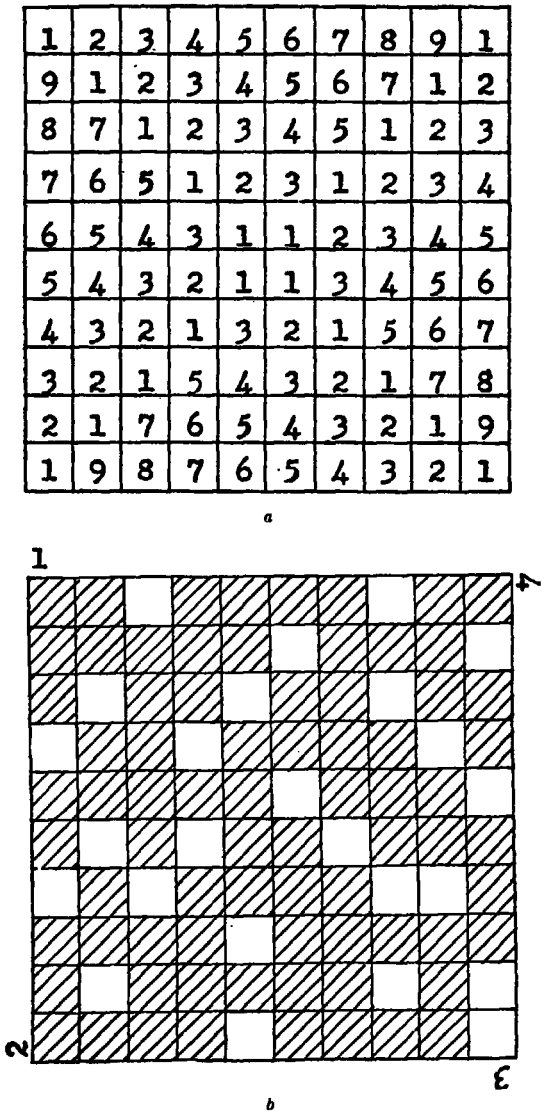


Figure 49.

REF ID:A56932

g. Given the formula, the eight corners of the grille can be labeled in various ways by prearrangement; but the simplest method is that shown in connection with b of figure 49. Then the initial position of the grille can be indicated by the number which appears at the upper left-hand corner when the grille is placed on the grid, ready for use. Thus, position 1 indicates that the grille is in position with the figure 1 at the upper left-hand corner; position 3, with the figure 3 at the upper left-hand corner, etc.

h. The direction of revolving the grille can be clockwise or counterclockwise, so that correspondents must make arrangements beforehand as to which direction is to be followed.

i. Revolving grilles can be constructed so that they have two operating faces, an obverse and a reverse face. They may be termed *revolving-reversible* grilles. The principles of their construction merely involve a modification of those described in connection with ordinary revolving grilles. A revolving-reversible grille will have eight possible placement indicators; usually positions 1 and 5, 2 and 6, and so forth, correspond in this obverse-reverse relationship, as shown in figure 43.

j. The principles of construction described above apply also to grilles of other shapes, such as triangles, pentagons, and so forth.

104. Nonperforated Grilles

a. All the effects of a grille with actual perforations may be obtained by the modified use of a nonperforated grille. Let the cells that would normally be cut out in a grille be indicated merely by crosses thereon, and then on a sheet of cross-section paper let the distribution of letters resulting from each placement of the grille on a grid be indicated by inserting crosses in the appropriate cells, as shown in figure 50.

Grille Grille Position

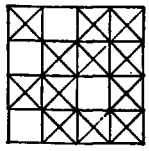


Figure 50a.

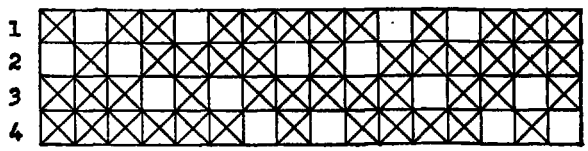


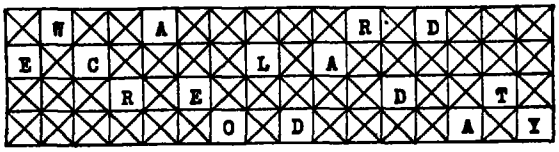
Figure 50b.

b. Note should be made of the fact that in figure 50b the distribution of crosses shown in the third row of cells is the reverse of that shown in the first; the distribution shown in the fourth row is the reverse of that shown in the second. This rule is applicable to all revolving grilles and is of importance in solution.

c. If the letters of the text are now inscribed (normal manner of writing) in the cells not eliminated by crosses, and the letters transcribed

REF ID:A56932

from *columns* to form the cryptogram, the results are the same as though a perforated grille had been employed. Thus:



Cryptogram:

EWCRA EOLDA RDDAT Y

Figure 50c.

d. It is obvious that a numerical key may be applied to effect a columnar transposition in the foregoing method, giving additional security.

e. The method is applicable to grilles of other shapes, such as triangles, pentagons, hexagons, octagons, etc.

f. In figure 50c it is noted that there are many cells that might be occupied by letters but are not. It is obvious that these may be filled with nulls so that the grid is completely filled with letters. Long messages may be enciphered by the superposition of several diagrams of the same dimensions as figure 50c.

105. Rectangular or "Post Card" Grilles

a. The grille shown in figure 51 differs from the ordinary revolving grille in that (1) the apertures are rectangular in shape, and are greater in width, thus permitting of inscribing several letters in the cells disclosed on the grid by each perforation of the grille; and (2) the grille itself admits of but two positions with its obverse side up and two with its reverse side up. In figure 51 the apertures are numbered in succession from top to bottom in four series, each applying to one position of the grille; the numbers in parentheses apply to the apertures when the grille is reversed; the numbers at the corners apply to the four positions in which the grille may be placed upon the grid.

b. One of the ways in which such a grille may be used is to write the first letter of the text at the extreme left of the cell disclosed by aperture 1, the second letter, at the extreme left of the cell disclosed by aperture 2, and so on. The grille is retained in the same position and the 17th letter is written immediately to the right of the 1st, the 18th immediately to the right of the 2d, and so on. Depending upon the width of the aperture, and thus of the cells disclosed on the grid, 2, 3, 4 . . . letters may be inserted in these cells. When all the cells have been filled, the grille may then be placed in the second position, then the third, and finally, the fourth.

REF ID:A56932

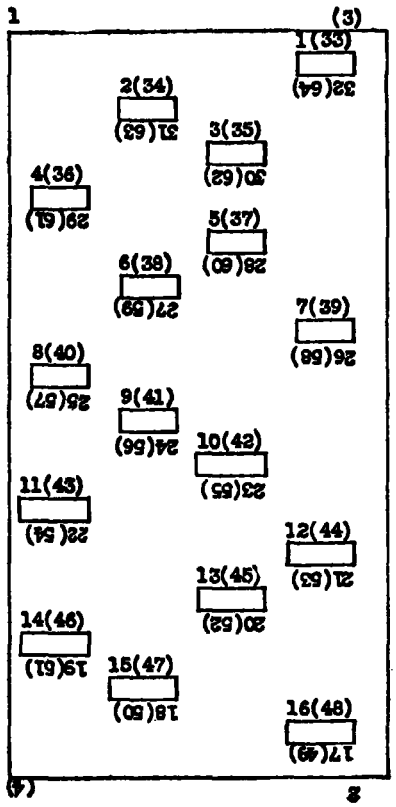


Figure 51.

c. Another way in which the grille may be used is to change the position of the grille after the 16th letter has been inserted, then after the 32d, 48th, and 64th; the 65th letter is then inserted to the right of the 1st, the 81st, to the right of the 17th, and so on until the grid is completed.

d. Whole words may, of course, be inserted in the cells disclosed by the apertures, instead of individual letters, but the security of the latter method is much lower than that of the former.

e. The text of the grid may be transcribed (to form the cryptogram) by following any prearranged route.

f. The successive positions of a post card grille may be prearranged. The order 1, 2, 3, 4 is but one of 24 different sequences in which it may be superimposed upon the grid.

g. A modification of the principles set forth in paragraph 103, dealing with the construction of revolving grilles, is applied in the construction of rectangular or "post card" grilles. Note the manner in which the cells in a of figure 51 are assigned numbers; homologous cells in each band receive the same number. In a of figure 52 there are three bands,

REF ID:A56932

numbered from 1 to 8, 9 to 16, and 17 to 24. Then in each band one and only one cell of the same numbered set of four cells is cut out. For example, if cell 1a is selected for perforation from band 1 (as indicated by the check mark in that cell), then a cross is written in the other three homologous cells, 1b, c, and d, to indicate that they are not available for selection for perforation. Then a cell bearing the number 2 in band 1 is selected, for example, 2c, and at once 2a, b, and d are crossed off as being ineligible for selection, and so on. In c of figure 52 is shown a grille as finally prepared, the nonshaded cells representing apertures.

h. The grille, c of figure 52, is a "six-column" one, that is, the cells form six columns. It is obvious that grilles with any even number of columns of cells are possible. The number of apertures in each band should be equal and this number multiplied by the number of bands and then by 4 should equal the capacity of the grille. In the case of the one shown in c of figure 52, the capacity is 8 by 3 by 4 or 96 cells; this is the same as is obtained merely by multiplying the height (in cells) by the

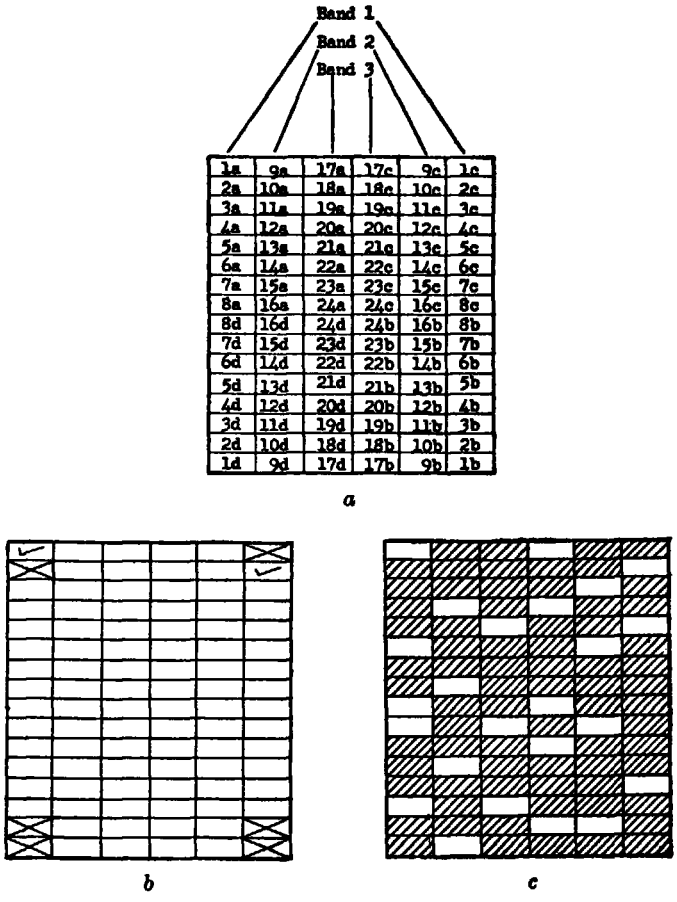


Figure 52.

REF ID:A56932

number of columns, $16 \times 6 = 96$. If four letters are inscribed in each rectangle, the capacity of the grille in terms of letters is 384. The grid in this case would, after completion, present 24 columns of letters, to which a numerical key for a second transposition can be applied in transcription to produce the final text of the cryptogram.

106. Indefinite or Continuous Grilles

a. In his *Manual of Cryptography,* Sacco illustrates a type of grille which he has devised and which has elements of practical importance. An example of such a grille is shown in figure 53. This grille contains 20 columns of cells, and each column contains 5 apertures distributed at random in the column. There are therefore 100 apertures in all, and this is the maximum number of letters which may be enciphered in one position of the grille. The plain text is inscribed vertically, from left to right, using only as many columns as may be necessary to inscribe the complete message. A 25-letter message would require but 5 columns. To form the cryptogram the letters are transcribed *horizontally* from the rows, taking the letters from left to right as they appear in the apertures. If the total number of letters is not a multiple of 5, sufficient nulls are added to make it so. In decryptographing, the total number of letters is divided by 5, this giving the number of columns employed. The cipher text is inscribed from left to right and top downwards in the apertures in the rows of the indicated number of columns and the plain text then reappears in the apertures in the columns, reading downward and from left to right. (It is, of course, not essential that nulls be added in the encipherment to make the length of the cryptogram an exact multiple of 5, for the matter can readily be handled even if this is not done. In decipherment the total number of letters divided by 5 will give the number of complete columns; the remainder left over from the division will give the number of cells occupied by letters in the last column on the right.)

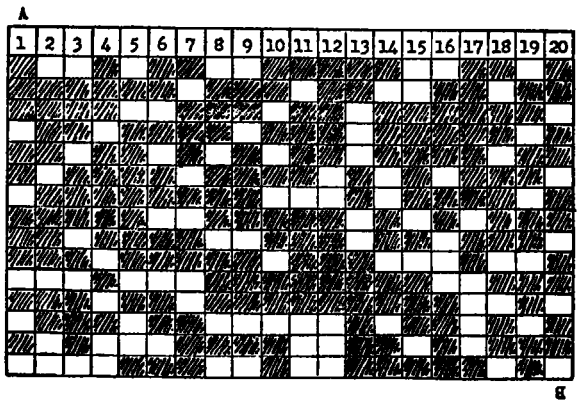


Figure 53a.

REF ID:A56932

b. Such a grille can assume 4 positions, two obverse and two reverse. Arrangements must be made in advance as to the sequence in which the various positions will be employed. That is why the grille shown in figure 53a has the position-designating letter "A" in the upper left-hand corner and the letter "B" (upside down) in the lower right-hand corner. On the obverse side of the grille would be the position-designating letters "C" and "D."

c. Figure 53b shows how a message is enciphered.

Message:

AM RECEIVING HEAVY MACHINE GUN FIRE FROM HILL SIX TWO ZERO.

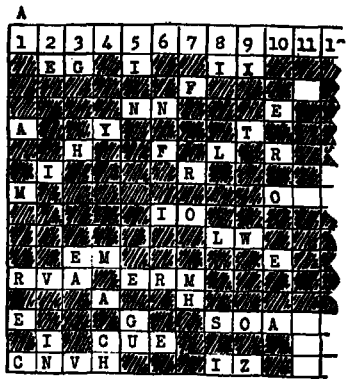


Figure 53b.

Cryptogram:

EGIIX FNNEA YTHFL RIRMO IOLWE MERVA ERMAH EGSOA ICUEC NVHIZ.

(The letters E and A in the 10th column are nulls. Columns 11 to 20 are not used at all, the irregular right-hand edge of the grille merely indicating that this portion of the grille remains vacant.)

Section V. MISCELLANEOUS TRANSPOSITION SYSTEMS

107. Complex Route Transposition

a. In figure 54 a route for inscribing letters within a rectangle is indicated by a sequence of numbers. The initial point may be at any of the four corners of the rectangle, or it may be at any other point, as prearranged. The letters may be inscribed to form the rectangle by following the route indicated and then transcribed from the rectangle to form the cryptogram by following another route; or the letters may be inscribed according to one route and transcribed accordingly to the numerical route indicated.

b. A variation of the foregoing is that illustrated in figure 55, wherein the inscription follows the route shown by the arrows. The initial point

REF ID:A56932

of inscription is indicated by the figure 1, and the final point, by the figure 2.

c. In the foregoing case, the route is a succession of the moves made by the king in the game of chess; it forms the so-called "king's tour", in which the playing piece makes a complete or reentrant journey covering all cells of the chessboard, each cell being traversed only once. A route composed of a succession of moves made by the knight, or the so-called "knight's tour", is also possible, but in order to be practical a grid with the cells numbered in succession would have to be prepared for the correspondents, since millions of different reentrant knight's tours can be constructed[4] on a chessboard of the usual 64 cells.

90	61	60	31	30	1
2	29	32	59	62	89
88	63	58	33	28	3
4	27	34	57	64	87
86	65	56	35	26	5
6	25	36	55	66	85
84	67	54	37	24	7
8	23	38	53	68	83
82	69	52	39	22	9
10	21	40	51	70	81
80	71	50	41	20	11
12	19	42	49	72	79
78	73	48	43	18	13
14	17	44	47	74	77
76	75	46	45	16	15

Figure 54.

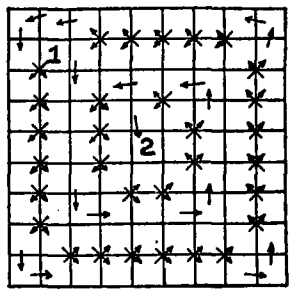


Figure 55.

108. Transposition of Groups of Letters, Syllables, and Words

There is nothing in the previously described methods which precludes the possibility of their application to pairs of letters, sets of three or more letters, or even syllables and whole words. Nor, of course, is their use limited to operations with plain text they may be applied as secondary steps after a substitutive process has been completed (see sec. I, ch. 10).

109. Disguised Transposition Methods

a. The system often encountered in romances and mystery stories, wherein the message to be conveyed is inserted in a series of nonsignificant words constructed with the purpose of avoiding or evading suspicion, is a species of this form of "open" cryptogram involving transposition. The "open" or enveloping, apparently innocent text may be designated as the *external text;* the secret or cryptographic text may be designated as the *internal text.* A complicated example of external or open and internal or secret text is that shown in paragraph 98.

[4] See Ball, W. W. R., Mathematical Recreations and Essays, London, 1928.

REF ID:A56932

b. Little need be said of the method based upon constructing external text the letters of which, at prearranged positions or intervals, spell out the internal text. For example, it may be prearranged that every fourth letter of the external text forms the series of letters for spelling out the internal text, so that only the 4th, 8th, 12th . . . letters of the external text are significant. The same rule may apply to the complete words of the external text, the *n*, *2n*, *3n*, . . . words form the internal text. The preparation of the external text in a suitable form to escape suspicion *is not so easy as might be imagined,* when efficient, experienced, and vigilant censorship is at work. Often the paragraph or passage containing the secret text is sandwiched in between other paragraphs added to pad the letter as a whole with text suitable to form introductory and closing matter to help allay suspicion as to the presence of secret, hidden text.

c. A modification of the foregoing method is that in which the 1st, 3d, 5th, . . . words of a secret message are transmitted at one time or by one agency of communication, and the 2d, 4th, 6th, . . . words of the message are transmitted at another time or by another agency of communication. Numerous variations of this scheme will suggest themselves, but they are not to be considered seriously as practical methods of secret intercommunication.

d. Two correspondents may agree upon a specific size of paper and a special diagram drawn upon this sheet, the lines of which pass through the words or letters of the internal text as they appear in the external text. For example, the legs of an equilateral triangle drawn upon the sheet of paper can serve for this purpose. This method is practicable only when messages can be physically conveyed by messenger, by the postal service, or by telephotographic means. Many variations of this basic scheme may perhaps be encountered in censorship work.

110. Cipher Machines for Effecting Transposition

These may be dismissed with the brief statement that if any exist today they are practically unknown. A few words are devoted to the subject in paragraph 147.

REF ID:A56932

CHAPTER 9
SUBSTITUTION SYSTEMS

Section I. POLYGRAPHIC SYSTEMS

111. General

a. It will be recalled that chapter 3 dealt with the various types of cipher alphabets, simple monoalphabetic substitution, monoalphabetic substitution with variants, the more simple varieties of polyalphabetic substitution, cipher disks, and cipher tables. The following material on substitution is a continuation of the former, a thorough understanding of which is a requisite to the examination of the more complex types of substitution now to be set forth.

b. First it will be advisable to explain several terms which will be used. Substitution methods in general may be described as being *monoliteral* or *polyliteral* in character. In the former there is a strict letter-for-letter replacement, or, to include numerical and symbol methods, there is a "one-to-one" correspondence between the length of the units of the plain text and those of the cipher text, no matter whether the substitution is monoalphabetic or polyalphabetic in character. In polyliteral methods, however, this "one-to-one" correspondence no longer holds. A combination of two letters, or of two figures, or of a letter and a figure, may represent a single letter of the plain text; there is here a "two-to-one" correspondence, two characters of the cipher text representing one of the plain text. The methods described in chapter 3, fall under the latter designation; the cipher equivalents there shown are, properly speaking, bipartite in character. Tripartite cipher equivalents are also encountered. Polyliteral methods, therefore, are said to employ *polypartite alphabets,* of which the bipartite type is by far the most common. Further on in this text, polyliteral methods of greater complexity than those illustrated in chapter 3 will be discussed. Attention now will be directed more particularly to a different type of substitution designated as *monographic* and *polygraphic* substitution.

112. Monographic and Polygraphic Substitution

a. All the methods of substitution heretofore described are monographing in nature, that is, in the enciphering process the individual units subjected to treatment are single letters; there is a letter-for-letter substitution, or, to include numerical and symbol methods, there is, as in the

REF ID:A56932

ENTIAL

case of monoliteral substitution, a "one-to-one" correspondence between units of the plain text and those of the cipher text. In polygraphic substitution, however, *combinations* of letters of the plain text, considered as indivisible compounds, constitute the units for treatment in encipherment. If the units consist of pairs of plain-text letters, the encipherment is pair-for-pair, and is said to be *digraphic* in character; if the units consist of sets of three letters, it is *trigraphic* in character, and so on. There is still a "one-to-one" correspondence involved, but the units in these cases are composite in character and the individual elements composing the units affect the cipher equivalents *jointly*, rather than separately. The basic important factor in true polygraphic substitution is that *all* the letters of the group participate in the determination of the cipher equivalent of the group; the identity of *each* letter of the plain-text group affects the composition of the *whole* cipher group. Thus, in a certain digraphic system AB_p may be enciphered as XP_c, and AC_p, on the other hand, may be enciphered as NK_c; a difference in the identity of but one of the letters of the plain-text pair here produces a difference in the identity of *both* letters of the cipher pair.

b. For practical usage polygraphic substitution is limited to the handling of digraphs and trigraphs, although very occasionally groups of more than three letters may be employed for special purposes.

c. The fundamental purpose of polygraphic substitution is the suppression or rather the elimination of the frequency characteristics of ordinary plain text. It is these frequency characteristics which lead, sooner or later, to the solution of practically all substitution ciphers. When the substitution involves only individual letters in a monoalphabetic system, the cryptogram can be solved very quickly; when it involves individual letters in a polyalphabetic system, the cryptogram can usually be solved, but only after a much longer time and much more study, depending upon the complexity of the method. The basic principle in the solution, however, is to reduce the polyalphabetic text to the terms of monoalphabetic ciphers and then to solve the latter. In true polygraphic substitution on the other hand, the solution does not rest upon the latter basis at all because it is not a question of breaking up a complex text into simpler elements; it rests, as a rule, upon the possibility of analysis on the basis of the frequency of the polygraphic units concerned. If the substitution is digraphic, then the units are pairs of letters and the normal frequencies of plain-text pairs become of first consideration; if the substitution is trigraphic, the units are sets of three letters and the normal frequencies of plain-text trigraphs are involved. In the last two cases the data that can be employed in the solution are meager, and are far from definite or unvarying in their significance, and that is why solution of polygraphic substitution ciphers is often extremely difficult.

d. Just as in typography, when certain combinations of letters, such as fi, fl, and ffi, are mounted on one and the same piece of type, they are

REF ID:A56932

called logotypes or ligatures, so in cryptography, when combinations of two or more letters are to be treated as a unit in a cryptographic process, they may also be called ligatures and can be conveniently indicated as being so by placing a bar across the top of the combination. Thus, $\overline{CO}_p$ represents the digraph CO of the plain text. It will also be convenient to use the Greek letter θ to represent a letter of the alphabet, without indicating its identity. Thus, instead of the circumlocution "any letter of the plain text", the symbol θ_p will be used; and for the expression "any letter of the cipher text", the symbol θ_c will be used. The symbol $\overline{\theta\theta}_p$ then means "any plain-text digraph"; the symbol $\overline{\theta\theta}_c$ "any cipher-text digraph." To refer specifically to the 1st, 2d, 3d . . . member of a ligature, the exponent 1, 2, 3 . . . will be used. Thus, $\theta^2{}_p$ of $\overline{REM}_p$ is the letter E; $\theta^3{}_c$ of $\overline{XRZ}_c$ is Z.

TABLE I

(Showing only a partially filled table)

Initial letter ($\theta^1{}_p$) \ Final Letter ($\theta^2{}_p$)	A	B	C	D	E	F	G	H	I	J	K	. . .	X	Y	Z	
A	FX	CH	XE	YY	ZA	YG	FB	CD	EF	XJ	ZX	. . .	EA	DJ	FH	A
B	NY	DC	NB	ZI	XX	DX						. . .				B
C				AH				AB				. . .		ND		C
D			BB		YA					AY		. . .	BF			D
E	AX					AI						. . .				E
F		AG			NZ			AZ				. . .	AA			F
:	:	:	:	:	:	:	:	:	:	:	:	. . .	:	:	:	:
N		BC		CY								. . .		BA	FE	N
:	:	:	:	:	:	:	:	:	:	:	:	. . .	:	:	:	:
X					AC					AJ		. . .	BE			X
Y	DE						AF					. . .		AD		Y
Z	AE								BD			. . .	AK			Z
	A	B	C	D	E	F	G	H	I	J	K		X	Y	Z	

113. Polygraphic Substitution by Means of Tables

a. The most simple method of effecting polygraphic substitution involves the use of tables similar to that shown in table I. This table merely presents equivalents for digraphs and is to be employed upon the coordinate system, $\theta^1{}_p$ of $\overline{\theta^1\theta^2}_p$ being sought in the column at the left or right, $\theta^2{}_p$ in the row at the top or bottom. The cipher pair, $\overline{\theta^1\theta^2}_c$, is

REF ID:A56932

then found at the intersection of the row and column thus indicated. For example, $\overline{AF}_p = \overline{YG}_c$; $\overline{FH}_p = \overline{AZ}_c$, etc.

b. Table I is reciprocal in nature; that is, $\overline{AF}_p = \overline{YG}_c$ and $\overline{YG}_p = \overline{AF}_c$. Thus, a single table serves for enciphering as well as for deciphering. The word DEFEND would be enciphered as YA NZ CY, and then grouped in fives: YANZC Y . . . . When a final single letter occurs, a null is added in order to make a pair of letters capable of being enciphered by the method. Reciprocity is, however, not an essential factor and for greater security nonreciprocal tables are more advisable. In such cases an enciphering table must have its complementary deciphering table.

c. Until the amount of text enciphered by means of such a table becomes great enough to disclose the cipher equivalents of the most frequently used digraphs, such as EN, ER, RE, TH, ON, etc., cryptograms based upon the table are relatively secure against solution.

d. A simple method for preventing the establishment of the frequencies characterizing these commonly used digraphs and thus eliminating the principal basis for their identification is given in paragraph 134*e*.

e. The factor that contributes most to the relatively high degree of security of the digraphic method described in *a* and *b* above is the absence of symmetry in the table employed; for this table is constructed by random assignment of values and shows no symmetry whatsoever in its arrangement of contents. Hence, even if θ^1_p in a first case of $\overline{\theta^1\theta^2}_p = \overline{\theta^1\theta^2}_c$ is identical with θ^1_p in a second case, $\overline{\theta^1\theta^2}_c$ in the first case is wholly different from $\overline{\theta^1\theta^2}_c$ in the second case. For example, table I shows that $\overline{AC}_p = \overline{XE}_c$ and $\overline{AD}_p = \overline{YY}_c$; the cipher resultants fail to give any hint that the plain-text pairs contain an identical letter.

f. If, however, the latter is not the case and the table exhibits symmetry in its arrangement of contents, solution is somewhat facilitated. Note table II, for example, in which two mixed sequences are employed to form the cipher equivalents. One mixed sequence is based upon the keyphrase WESTINGHOUSE AIR BRAKE; the other, upon the keyphrase GENERAL ELECTRIC COMPANY. The word FIRE would be enciphered as KIQA.

g. A cursory examination of table II shows that when θ^2_p is identical in two cases then θ^2_c is identical in these cases, so that in reality the encipherment is by no means truly digraphic in character. Described in cryptographic terms, the encipherment of θ^1_p is polyalphabetic in character whereas that of θ^2_p is monoalphabetic. A more obvious picture of this condition is brought out in the rearrangement of table II.

h. By a slight modification in arrangement but with no change in basic principle, the encipherment can be made monoalphabetic so far as θ^1_p is concerned, and polyalphabetic so far as θ^2_p is concerned. Note table IV.

REF ID:A56932

TABLE II

θ_1 \ θ_2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	WG	EE	SN	TR	IA	NL	GC	HT	OI	UO	AM	RP	BY	KB	CD	DF	FH	JJ	LK	MQ	PS	QU	VV	XW	YX	ZZ
B	EG	SE	TN	IR	NA	GL	HC	OT	UI	AO	RM	BP	KY	CB	DD	FF	JH	LJ	MK	PQ	QS	VU	XV	YW	ZX	WZ
C	SG	TE	IN	NR	GA	HL	OC	UT	AI	RO	BM	KP	CY	DB	FD	JF	LH	MJ	PK	QQ	VS	XU	YV	ZW	WX	EZ
D	TG	IE	NN	GR	HA	OL	UC	AT	RI	BO	KM	CP	DY	FB	JD	LF	MH	PJ	QK	VQ	XS	YU	ZV	WW	EX	SZ
E	IG	NE	GN	HR	OA	UL	AC	RT	BI	KO	CM	DP	FY	JB	LD	MF	PH	QJ	VK	XQ	YS	ZU	WV	EW	SX	TZ
F	NG	GE	HN	OR	UA	AL	RC	BT	KI	CO	DM	FP	JY	LB	MD	PF	QH	VJ	XK	YQ	ZS	WU	EV	SW	TX	IZ
G	GG	HE	ON	UR	AA	RL	BC	KT	CI	DO	FM	JP	LY	MB	PD	QF	VH	XJ	YK	ZQ	WS	EU	SV	TW	IX	NZ
H	HG	OE	UN	AR	RA	BL	KC	CT	DI	FO	JM	LP	MY	PB	QD	VF	XH	YJ	ZK	WQ	ES	SU	TV	IW	NX	GZ
I	OG	UE	AN	RR	BA	KL	CC	DT	FI	JO	LM	MP	PY	QB	VD	XF	YH	ZJ	WK	EQ	SS	TU	IV	NW	GX	HZ
J	UG	AE	RN	BR	KA	CL	DC	FT	JI	LO	MM	PP	QY	VB	XD	YF	ZH	WJ	EK	SQ	TS	IU	NV	GW	HX	OZ
K	AG	RE	BN	KR	CA	DL	FC	JT	LI	MO	PM	QP	VY	XB	YD	ZF	WH	EJ	SK	TQ	IS	NU	GV	HW	OX	UZ
L	RG	BE	KN	CR	DA	FL	JC	LT	MI	PO	QM	VP	XY	YB	ZD	WF	EH	SJ	TK	IQ	NS	GU	HV	OW	UX	AZ
M	BG	KE	CN	DR	FA	JL	LC	MT	PI	QO	VM	XP	YY	ZB	WD	EF	SH	TJ	IK	NQ	GS	HU	OV	UW	AX	RZ
N	KG	CE	DN	FR	JA	LL	MC	PT	QI	VO	XM	YP	ZY	WB	ED	SF	TH	IJ	NK	GQ	HS	OU	UV	AW	RX	BZ
O	CG	DE	FN	JR	LA	ML	PC	QT	VI	XO	YM	ZP	WY	EB	SD	TF	IH	NJ	GK	HQ	OS	UU	AV	RW	BX	KZ
P	DG	FE	JN	LR	MA	PL	QC	VT	XI	YO	ZM	WP	EY	SB	TD	IF	NH	GJ	HK	OQ	US	AU	RV	BW	KX	CZ
Q	FG	JE	LN	MR	PA	QL	VC	XT	YI	ZO	WM	EP	SY	TB	ID	NF	GH	HJ	OK	UQ	AS	RU	BV	KW	CX	DZ
R	JG	LE	MN	PR	QA	VL	XC	YT	ZI	WO	EM	SP	TY	IB	ND	GF	HH	OJ	UK	AQ	RS	BU	KV	CW	DX	FZ
S	LG	ME	PN	QR	VA	XL	YC	ZT	WI	EO	SM	TP	IY	NB	GD	HF	OH	UJ	AK	RQ	BS	KU	CV	DW	FX	JZ
T	MG	PE	QN	VR	XA	YL	ZC	WT	EI	SO	TM	IP	NY	GB	HD	OF	UH	AJ	RK	BQ	KS	CU	DV	FW	JX	LZ
U	PG	QE	VN	XR	YA	ZL	WC	ET	SI	TO	IM	NP	GY	HB	OD	UF	AH	RJ	BK	KQ	CS	DU	FV	JW	LX	MZ
V	QG	VE	XN	YR	ZA	WL	EC	ST	TI	IO	NM	GP	HY	OB	UD	AF	RH	BJ	KK	CQ	DS	FU	JV	LW	MX	PZ
W	VG	XE	YN	ZR	WA	EL	SC	TT	II	NO	GM	HP	OY	UB	AD	RF	BH	KJ	CK	DQ	FS	JU	LV	MW	PX	QZ
X	XG	YE	ZN	WR	EA	SL	TC	IT	NI	GO	HM	OP	UY	AB	RD	BF	KH	CJ	DK	FQ	JS	LU	MV	PW	QX	VZ
Y	YG	ZE	WN	ER	SA	TL	IC	NT	GI	HO	OM	UP	AY	RB	BD	KF	GH	DJ	FK	JQ	LS	MU	PV	QW	VX	XZ
Z	ZG	WE	EN	SR	TA	IL	NC	GT	HI	OO	UM	AP	RY	BB	KD	CF	DH	FJ	JK	LQ	MS	PU	QV	VW	XX	YZ

REF ID:A56932

i. The results given by table III or table IV may be duplicated by using sliding alphabets, as shown in figures 56 and 57. In the former, which corresponds to table III, alphabets I and IV are fixed, II and III are mounted upon the same strip, which is movable. To use these alphabets in encipherment, θ^1_p of $\overline{\theta^1\theta^2}_p$ is located on alphabet II and alphabets II–III are shifted so that θ^1_p is beneath A on alphabet I; θ^2_p is now sought in alphabet I and $\overline{\theta^1\theta^2}_c$ will be found under it on alphabets III and IV, respectively. Thus, for the word FIRE the successive positions of the alphabet strips are as shown below, yielding the cipher resultant KIQA.

$\overline{FI}_p = \overline{KI}_c$

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ.....Fixed alphabet
II—FGHIJKLMNOPQRSTUVWXYZABCDE
III—NGHOUARBKCDFJLMPQVXYZWESTI } .....Movable alphabet
IV—GENRALCTIOMPYBDFHJKQSUVWXZ.....Fixed alphabet

$\overline{RE}_p = \overline{QA}_c$

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ.....Fixed alphabet
II—RSTUVWXYZABCDEFGHIJKLMNOPQ
III—JLMPQVXYZWESTINGHOUARBKCDF } .....Movable alphabet
IV—GENRALCTIOMPYBDFHJKQSUVWXZ.....Fixed alphabet

Figure 56.

TABLE III

θ^1_p \ θ^2_p	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z
B	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W
C	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E
D	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S
E	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T
F	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I
G	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N
H	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G
I	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H
J	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O
K	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U
L	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A
M	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R
N	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B
O	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K
P	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C
Q	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D
R	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F
S	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J
T	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L
U	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M
V	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P
W	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q
X	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V
Y	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X
Z	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y
θ^2_c	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z

REF ID:A56932

j. To correspond with table IV the alphabet strips are arranged as shown in figure 57. Here alphabets I and II are fixed, III and IV are mounted upon the same movable strip. To use these alphabets in encipherment, θ^2_p of $\overline{\theta^1\theta^2}_p$ is located on alphabet IV and alphabets III–IV are shifted so that θ^2_p (I_p) is beneath A on alphabet I; θ^1_p (F_p) is now sought in alphabet I and $\overline{\theta^1\theta^2}_c$ will be found under it on alphabets II and III, respectively. Thus, for the word FIRE, the successive positions of the alphabet strips are as shown below, yielding the cipher resultant NBJU.

$\overline{FI}_p = \overline{NB}_c$

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ.....Fixed alphabet
II—WESTINGHOUARBKCDFJLMPQVXYZ.....Fixed alphabet
III—IOMPYBDFHJKQSUVWXZGENRALCT
IV—IJKLMNOPQRSTUVWXYZABCDEFGH.....Movable alphabet

$\overline{RE}_p = \overline{JU}_c$

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ.....Fixed alphabet
II—WESTINGHOUARBKCDFJLMPQVXYZ.....Fixed alphabet
III—ALCTIOMPYBDFHJKQSUVWXZGENR
IV—EFGHIJKLMNOPQRSTUVWXYZABCD.....Movable alphabet

Figure 57.

TABLE IV

θ^1_p θ^1_c	θ^2_p A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	W	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z
B	E	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G
C	S	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E
D	T	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N
E	I	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R
F	N	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A
G	G	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L
H	H	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C
I	O	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T
J	U	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I
K	A	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O
L	R	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M
M	B	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P
N	K	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y
O	C	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B
P	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D
Q	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F
R	J	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H
S	L	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J
T	M	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K
U	P	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q
V	Q	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S
W	V	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U
X	X	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V
Y	Y	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W
Z	Z	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X

REF ID:A56932

k. Neither table III nor table IV presents the possibilities such tables might afford for digraphic substitution. They may, however, be rearranged so as to give results that will approach more closely to the desired ideal as to nonrelationship between cipher equivalents of plain-text pairs having an identical letter in common. Note that in table V, which is based upon the same primary alphabets as table III and table IV, the cipher equivalents are the same as in the latter tables, but they have been so distributed as to eliminate the undesirable and externally obvious relationship referred to. (In any table of this nature there can be only 676 different pairs of equivalents, since the table presents merely the permutations of the 26 letters taken two at a time. It is the distribution of the pairs which is important.)

l. Table V still shows symmetry in its construction, and a suspicion of its existence formed during the preliminary stages of cryptanalysis would aid materially in hastening final solution.

m. The foregoing tables have all been digraphic in nature, but a kind of false trigraphic substitution may also be accomplished by means of such tables, as illustrated in the accompanying table VI, which is the same as table V with the addition of one more alphabet at the top of the table.

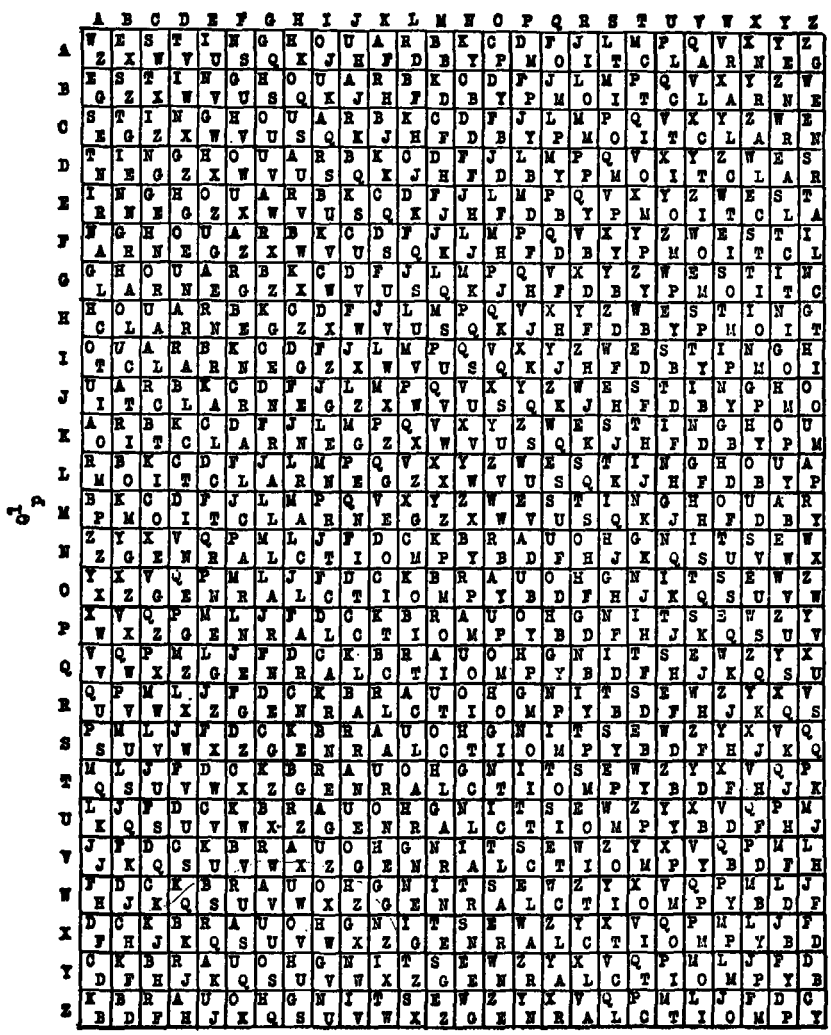
n. In using this table, θ^1_p is located in alphabet I, and its equivalent, θ^1_c, taken from alphabet II; θ^2_p is located in alphabet III, and its equivalent, θ^2_c, taken from alphabet IV; θ^3_c is the letter lying at the intersection of the row indicated by θ^3_p in alphabet I and the column determined by θ^2_p. Thus, FIRE LINES would be enciphered NNZ IEQ KOV. It is obvious, however, that only the encipherment of θ^3_p is polyalphabetic in character; θ^1_p and θ^2_p are enciphered purely monoalphabetically. Various other agreements may be made with respect to the alphabets in which the plain-text letter will be sought in such a table, but the basic cryptographic principles are the same as in the case described.

o. Digraphic tables employing numerical equivalents instead of letter equivalents are, of course, possible but in this case the number of equivalents required, 676, means that combinations of three figures must be used.

REF ID:A56932

TABLE V

σ^2_p



REF ID:A56932

TABLE VI

I.II.	III. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
	IV. R A D I O C P T N F M E B G H J K L Q S U V W X Y Z
A W	G E N R A L C T I O M P Y B D F H J K Q S U V W X Z
B E	E N R A L C T I O M P Y B D F H J K Q S U V W X Z G
C S	N R A L C T I O M P Y B D F H J K Q S U V W X Z G E
D T	R A L C T I O M P Y B D F H J K Q S U V W X Z G E N
E I	A L C T I O M P Y B D F H J K Q S U V W X Z G E N R
F N	L C T I O M P Y B D F H J K Q S U V W X Z G E N R A
G G	C T I O M P Y B D F H J K Q S U V W X Z G E N R A L
H H	T I O M P Y B D F H J K Q S U V W X Z G E N R A L C
I O	I O M P Y B D F H J K Q S U V W X Z G E N R A L C T
J U	O M P Y B D F H J K Q S U V W X Z G E N R A L C T I
K A	M P Y B D F H J K Q S U V W X Z G E N R A L C T I O
L R	P Y B D F H J K Q S U V W X Z G E N R A L C T I O M
M B	Y B D F H J K Q S U V W X Z G E N R A L C T I O M P
N K	B D F H J K Q S U V W X Z G E N R A L C T I O M P Y
O C	D F H J K Q S U V W X Z G E N R A L C T I O M P Y B
P D	F H J K Q S U V W X Z G E N R A L C T I O M P Y B D
Q F	H J K Q S U V W X Z G E N R A L C T I O M P Y B D F
R J	J K Q S U V W X Z G E N R A L C T I O M P Y B D F H
S L	K Q S U V W X Z G E N R A L C T I O M P Y B D F H J
T M	Q S U V W X Z G E N R A L C T I O M P Y B D F H J K
U P	S U V W X Z G E N R A L C T I O M P Y B D F H J K Q
V Q	U V W X Z G E N R A L C T I O M P Y B D F H J K Q S
W V	V W X Z G E N R A L C T I O M P Y B D F H J K Q S U
X X	W X Z G E N R A L C T I O M P Y B D F H J K Q S U V
Y Y	X Z G E N R A L C T I O M P Y B D F H J K Q S U V W
Z Z	Z G E N R A L C T I O M P Y B D F H J K Q S U V W X

Section II. MATRIX[5] DIGRAPHIC SUBSTITUTION

114. Disadvantages of Large Tables

Digraphic substitution by means of tables such as those illustrated in tables I, II, and V is impractical for military use because of the relatively large size that the table takes, and the inconvenience in their production, change, distribution, and handling. Just as it has been noted in section VI, chapter 3, that simple sliding alphabet strips can replace large quadricular tables, so it will be found that small matrices similar to a checkerboard can replace the large quadricular tables in digraphic substitution.

115. Four-Alphabet Matrix

a. The simple or single-alphabet matrix consists of a square 5 by 5, containing 25 cells in which the letters of a 25-element alphabet (I and J

[5] The word *matrix* as herein employed refers to "checkerboard" diagrams smaller than the quadricular tables illustrated in section I. These matrices usually comprise sections of 25 cells each.

REF ID:A56932

being interchangeable) are inserted in any prearranged order. When four such matrix alphabets are arranged in a large square as shown in figure 58, the latter may be employed for digraphic substitution to yield the same cipher results as does the much larger table I. In this square, θ^1_p of $\overline{\theta\theta}_p$ is sought in section 1; θ^2_p, in section 2. Thus, θ^1_p and θ^2_p will always form the northwest-southeast corners of an imaginary rectangle delimited by these two letters as located in these two sections of the square. Then θ^1_c and θ^2_c are, respectively, the letters at the northeast-southwest corners of this same rectangle. Thus, $\overline{TG}_p = \overline{TK}_c$; $\overline{WD}_p = \overline{TX}_c$; $\overline{OR}_p = \overline{PS}_c$; $\overline{UR}_p = \overline{WP}_c$, etc. In decryptographing, θ^1_c and θ^2_c are sought in sections 3 and 4, respectively, and their equivalents, θ^1_p and θ^2_p, noted in sections 1 and 2, respectively. It may, of course, be prearranged that θ^1_p should be sought in the section now labeled 3, θ^2_p, in that labeled 4, whereupon θ^1_c would be located in the section now labeled 1, θ^2_c, in that now labeled 2.

	T	W	E	N	Y	F	O	U	R	T
	K	L	M	O	S	L	M	P	Q	E
Sec. 1 (θ^1_p)	H	V	Z	P	I	K	Y	Z	S	N
	G	U	R	Q	X	I	X	W	V	A
	F	D	C	B	A	H	G	D	C	B
	T	H	I	R	E	F	I	V	E	A
	O	P	Q	S	N	P	Q	R	S	B
Sec. 4 (θ^2_c)	M	Y	Z	U	A	O	Y	Z	T	C
	L	X	W	V	B	N	X	W	U	D
	K	G	F	D	C	M	L	K	H	G

Sec. 3 (θ^1_c) — Sec. 2 (θ^2_p)

Figure 58.

b. It is possible to construct a digraphic substitution matrix that shows reciprocity in its $\overline{\theta\theta}_p = \overline{\theta\theta}_c$ relationship so that if $\overline{AB}_p = \overline{XY}_c$, for example, then $\overline{XY}_p = \overline{AB}_c$. Two conditions are essential to assure reciprocity. These are taken into consideration in the establishment of the $\overline{\theta^1\theta^2}_c$, or deciphering sections, and an example will serve to explain the process.

c. Two enciphering alphabets are first constructed; one in section 1 for θ^1_p, the other in section 2 for θ^2_p, as shown in figure 59a. The alphabet in section 3 is now to be constructed. Any horizontal row of section 1 is taken, for example, the row labeled 1, consisting of the letters BWGRM, and these letters are written on any horizontal row of section

REF ID:A56932

		1	2	3	4	5						
	1	B	W	G	R	M						
	2	N	Y	V	X	E						
Sec. 1 (θ^1_p)	3	S	I	C	T	K						Sec. 3 (θ^1_c)
	4	U	P	L	A	O						
	5	D	Z	F	Q	H						
							C	X	K	P	B	1
							O	M	Y	D	V	2
Sec. 4 (θ^2_c)							S	A	E	W	L	3 Sec. 2 (θ^2_p)
							G	Z	Q	N	R	4
							T	H	I	F	U	5
							1	2	3	4	5	

Figure 59a.

		1	2	3	4	5	5	2	4	1	3	
	1	B	W	G	R	M						
	2	N	Y	V	X	E						
Sec. 1 (θ^1_p)	3	S	I	C	T	K						Sec. 3 (θ^1_c)
	4	U	P	L	A	O	M	W	R	B	G	1
	5	D	Z	F	Q	H						
							C	X	K	P	B	1
							O	M	Y	D	V	2
Sec. 4 (θ^2_c)							S	A	E	W	L	3 Sec. 2 (θ^2_p)
							G	Z	Q	N	R	4
							T	H	I	F	U	5
							1	2	3	4	5	

Figure 59b.

3, in any transposed order, which is immediately written at the top of section 3, as shown in figure 59b.

Row 1 of section 1 was inserted in row 4 of section 3. The reciprocal permutation of 1 4 is 4 1, and therefore row 4 of section 1 must now be inserted in row 1 of section 3, and in the transposed order 5–2–4–1–3, as indicated at the top of section 3. The result is shown in figure 59c. Then

REF ID:A56932

	1	2	3	4	5	5	2	4	1	3	
1	B	W	G	R	M	O	P	A	U	L	4
2	N	Y	V	X	E						
Sec. 1 (θ^1_p) 3	S	I	C	T	K						Sec. 3 (θ^1_c)
4	U	P	L	A	O	M	W	R	B	G	1
5	D	Z	F	Q	H						
						C	X	K	P	B	1
						O	M	Y	D	V	2
Sec. 4 (θ^2_c)						S	A	E	W	L	3 Sec. 2 (θ^2_p)
						G	Z	Q	N	R	4
						T	H	I	F	U	5
						1	2	3	4	5	

Figure 59c.

	1	2	3	4	5	5	2	4	1	3	
1	B	W	G	R	M	O	P	A	U	L	4
2	N	Y	V	X	E	H	Z	Q	D	F	5
Sec. 1 (θ^1_p) 3	S	I	C	T	K	K	I	T	S	C	3 Sec. 3 (θ^1_c)
4	U	P	L	A	O	M	W	R	B	G	1
5	D	Z	F	Q	H	E	Y	X	N	V	2
						C	X	K	P	B	1
						O	M	Y	D	V	2
Sec. 4 (θ^2_c)						S	A	E	W	L	3 Sec. 2 (θ^2_p)
						G	Z	Q	N	R	4
						T	H	I	F	U	5
						1	2	3	4	5	

Figure 59d.

row 2 of section 1 is transferred to another row of section 3, for example, the fifth, and the letters inserted in the already indicated transposed order. Immediately thereafter, in order to continue the reciprocal permutation relationship, row 5 of section 1 becomes row 2 of section 3. This leaves row 3 of section 1 to become also row 3 of section 3, and to be reciprocal to itself. The result is shown in figure 59d, where section 3 is

REF ID:A56932

completely constructed. The foregoing principle of permutation reciprocity applies equally to the rows of section 4. Suppose the permutation 3–5–1–4–2 is decided upon for the rows of section 4. This means that rows 1 and 3 of section 2 become rows 3 and 1 of section 4; rows 2 and 5 of section 2 become 5 and 2 of section 4; row 4 of section 2 becomes row 4 of section 4. As regards the transposed order within the rows of section 4, the following rule applies: The letters forming a complete column from the top of section 3 to the bottom of section 2, whatever their order, must also form a complete column from the top of section 1 to the bottom of section 4. For example, the column designated by the number 5 of section 3 contains the letters OHKMECOSGT; column 5 of section 1 contains five of these letters, MEKOH; therefore, the completed column must contain the letters, COSGT but in the transposed order given by the permutation selected for the rows of section 4, namely, 3–5–1–4–2.

The completed matrix is then as shown in figure 59e, and exhibits reciprocity throughout. Example: $\overline{BB}_p = \overline{LW}_c$, and $\overline{LW}_p = \overline{BB}_c$.

	1	2	3	4	5	5	2	4	1	3	
1	B	W	G	R	M	O	P	A	U	L	4
2	N	Y	V	X	E	H	Z	Q	D	F	5
Sec. 1 (θ^1_p) 3	S	I	C	T	K	K	I	T	S	C	3 Sec. 3 (θ^1_c)
4	U	P	L	A	O	M	W	R	B	G	1
5	D	Z	F	Q	H	E	Y	X	N	V	2
3	W	A	L	E	S	C	X	K	P	B	1
5	F	H	U	I	T	O	M	Y	D	V	2
Sec. 4 (θ^2_c) 1	P	X	B	K	C	S	A	E	W	L	3 Sec. 2 (θ^2_p)
4	N	Z	R	Q	G	G	Z	Q	N	R	4
2	D	M	V	Y	O	T	H	I	F	U	5
	4	2	5	3	1	1	2	3	4	5	

Figure 59e.

d. The total number of reciprocal permutations of five elements is 25, as follows:

Base 12345

(1) 12354	(6) 14325	(11) 21354	(16) 34125	(21) 45312
(2) 12435	(7) 14523	(12) 21435	(17) 35142	(22) 52341
(3) 12543	(8) 15342	(13) 21543	(18) 42315	(23) 52431
(4) 13245	(9) 15432	(14) 32145	(19) 43215	(24) 53241
(5) 13254	(10) 21345	(15) 32154	(20) 42513	(25) 54321

REF ID:A56932

Since the row permutations of sections 2 and 4 are independent, the total number of different four-alphabet matrices as regards row permutations is $25^2 = 625$. Taking into account the column permutations, $5 \times 4 \times 3 \times 2 \times 1$ in number, it is therefore possible to have 625×120 or 75,000 different, four-alphabet matrices of this nature, based upon the same two alphabets in sections 1 and 3. With changes in the latter, the number, of course, becomes very much greater.

116. Two-Alphabet Matrices

a. It is possible to effect digraphic substitution with a matrix consisting of but two sections by a modification in the method of finding equivalents. In the checkerboard shown in figure 60, $\theta^1{}_p$ of $\overline{\theta^1\theta^2}_p$ is located in the square at the left, $\theta^2{}_p$, in the square at the right.

	M	A	N	U	F	A	U	T	O	M	
	C	T	R	I	G	B	I	L	E	S	
$\theta^1{}_p\theta^2{}_c$	B	D	E	H	K	C	D	F	G	H	$\theta^2{}_p\theta^1{}_c$
	L	O	P	Q	S	K	N	P	Q	R	
	V	W	X	Y	Z	V	W	X	Y	Z	

Figure 60.

When $\overline{\theta^1{}_p\theta^2{}_p}$ are at the opposite ends of the diagonal of the imaginary rectangle defined by the letters, $\overline{\theta^1\theta^2}_c$ are at the opposite ends of the other diagonal of the same rectangle, just as in the preceding case. For example, $\overline{AL}_p = \overline{TT}_c$; $\overline{DO}_p = \overline{GA}_c$; $\overline{AT}_p = \overline{TA}_c$; $\overline{EH}_p = \overline{HE}_c$.

b. Reciprocity may be imparted to the two-alphabet matrix by reciprocal permutation of the rows of the squares, no attempt being made to effect any reciprocal permutation of columns. Figure 61 shows such a matrix. Here, for example, $\overline{AW}_p = \overline{OT}_c$ and $\overline{OT}_p = \overline{AW}_c$; $\overline{BA}_p = \overline{DL}_c$ and $\overline{DL}_p = \overline{BA}_c$, etc.

c. In two-alphabet matrices in which one section is directly above the other, reciprocity already exists without special preparations for its

1	M	A	N	U	F	O	S	Q	L	P	4
2	C	T	R	I	G	W	Z	Y	V	X	5
3	B	D	E	H	K	D	K	H	B	E	3
4	L	O	P	Q	S	A	F	U	M	N	1
5	V	W	X	Y	Z	T	G	I	C	R	2

Figure 61.

REF ID:A56932

M	A	N	U	F
C	T	R	I	G
B	D	E	H	K
L	O	P	Q	S
V	W	X	Y	Z
A	U	T	O	M
B	I	L	E	S
C	D	F	G	H
K	N	P	Q	R
V	W	X	Y	Z

Figure 62.

production. In figure 62, $MO_p = UA_c$ and $UA_p = MO_c$; $MA_p = MA_c$ and $MA_c = MA_p$. When both θ^1_p and θ^2_p happen to be in the same column, there is no encipherment[6], a fact which constitutes an important disadvantage of this method. This disadvantage is only slightly less obvious in the preceding cases where the cipher equivalent of such a case of $\overline{\theta^1\theta^2}_p$ consists merely of the plain-text letters in reversed order, yielding $\overline{\theta^2\theta^1}_c$.

117. One-Alphabet Matrices; Playfair Cipher

a. Limiting the matrix to one alphabet and modifying the method of finding equivalents gives the basis for a well-known system called the Playfair Cipher, which was not invented by Lord Lyon Playfair but by Sir Charles Wheatstone. It was used for many years as a field cipher in the British Army. For a short time, 1917–18, it was prescribed as a field cipher for use in the United States Army. The modification in the method of finding cipher equivalents has been found useful in imparting a greater degree of security than that afforded in the preceding types of matrix methods. Figure 63 shows a typical Playfair square. The usual method of encipherment can be best explained by examples given under four categories:

(1) Members of the plain-text pair, θ^1_p and θ^2_p, are at opposite ends of the diagonal of an imaginary rectangle defined by the two letters; the members of the cipher-text pair, θ^1_c and θ^2_c, are at the opposite ends of the other diagonal of this imaginary rectangle. Examples: $\overline{MO}_p = \overline{AI}_c$; $\overline{MI}_p = \overline{UC}_c$; $\overline{LU}_p = \overline{QM}_c$; $\overline{VI}_p = \overline{YC}_c$.

[6] Actually, the plain-text digraph is self-enciphered, in that $\overline{\theta^1\theta^2}_p = \overline{\theta^1\theta^2}_c$.

REF ID:A56932

M	A	N	U	F
C	T	R	I	G
B	D	E	H	K
L	O	P	Q	S
V	W	X	Y	Z

Figure 63.

(2) θ^1_p and θ^2_p are in the same row; the letter immediately to the *right* of θ^1_p forms θ^1_c, the letter immediately to the right of θ^2_p forms θ^2_c. When either θ^1_p or θ^2_p is at the extreme right of the row, the first letter in the row becomes its θ_c. Examples: $\overline{MA_p} = \overline{AN_c}$; $\overline{MU_p} = \overline{AF_c}$; $\overline{AF_p} = \overline{NM_c}$; $\overline{FA_p} = \overline{MN_c}$.

(3) θ^1_p and θ^2_p are in the same column; the letter immediately *below* θ^1_p form θ^1_c, the letter immediately below θ^2_p forms θ^2_c. When either θ^1_p or θ^2_p is at the bottom of the column, the top letter in that column becomes its θ_c. Examples: $\overline{MC_p} = \overline{CB_c}$; $\overline{AW_p} = \overline{TA_c}$; $\overline{WA_p} = \overline{AT_c}$; $\overline{QU_p} = \overline{YI_c}$.

(4) θ^1_p and θ^2_p are identical; they are to be separated by inserting a null, usually the letter X or Q. For example, the word BATTLES would be enciphered thus:

BA TX TL ES
DM RW CO KP

b. The Playfair square is automatically reciprocal so far as encipherments of type (1) above are concerned; but this is not true of encipherments of type (2) or (3).

118. Rectangular Designs

a. It is not essential that matrices for digraphic substitution be in the shape of perfect squares; rectangular designs will serve equally well, with little or no modification in procedure. In four-alphabet and two-alphabet rectangles reciprocity can be produced by following the method indicated in paragraph 115.

b. In figures 64 and 65 are shown two examples of such rectangles, together with illustrations of encipherments. Since the English alphabet consists of 26 letters, a number which can only form an impracticable rectangle 2 by 13, and since the addition of any symbols such as the digits 1, 2, 3 . . . to augment the number of elements to 27, 28, 30, 32, 35, or 36 characters would result in producing cryptograms containing intermixtures of letters and figures, the only practicable scheme is to reduce the alphabet to 24 letters as shown in the figures, where I serves also for J and U also for V.

	1	2	3	4	5	6	6	2	3	1	5	4	
1	T	W	O	H	U	N	Z	M	P	L	Y	Q	4
2	D	R	E	S	I	X	K	B	C	A	G	F	3
3	A	B	C	F	G	K	X	R	E	D	I	S	2
4	L	M	P	Q	Y	Z	N	W	O	T	U	H	1
4	X	R	W	Z	Y	Q	O	N	E	T	H	U	1
3	L	I	K	P	M	G	S	A	D	B	C	F	2
2	B	A	D	F	C	S	G	I	K	L	M	P	3
1	T	N	E	U	H	O	Q	R	W	X	Y	Z	4
	4	2	3	6	5	1	1	2	3	4	5	6	

Sec. 1 (θ^1_p) — Sec. 3 (θ^1_c) — Sec. 4 (θ^2_c) — Sec. 2 (θ^2_p)

Figure 64.

Examples:

Plain: TH ER EA RE BE TT ER CR YP TO GR AM
Cipher: YX BE BK CR ER LX BE RE HC ZX RH IB

	1	2	3	4	2	3	1	4	
1	T	W	O	H	B	C	A	F	4
2	U	N	D	R	Q	Y	P	Z	6
3	E	S	I	X	K	L	G	M	5
4	A	B	C	F	W	O	T	H	1
5	G	K	L	M	S	I	E	X	3
6	P	Q	Y	Z	N	D	U	R	2
5	Q	M	P	R	O	N	E	T	1
2	S	H	U	A	H	U	S	A	2
3	C	D	B	F	D	B	C	F	3
6	Y	W	X	Z	G	I	K	L	4
1	E	O	N	T	M	P	Q	R	5
4	K	G	I	L	W	X	Y	Z	6
	3	1	2	4	1	2	3	4	

Sec. 1 (θ^1_p) — Sec. 3 (θ^1_c) — Sec. 4 (θ^2_c) — Sec. 2 (θ^2_p)

Figure 65.

Examples:

Plain: TH ER EA RE BE TT ER CR YP TO GR AM
Cipher: BS ME MS PR TM FQ ME HN DN BQ XE WE

REF ID:A56932

W	A	S	H	I	N
G	T	O	B	C	D
E	F	J	KA	KE	KI
KO	KU	L	M	P	Q
R	U	V	X	Y	Z

Figure 66.

c. Two-alphabet rectangles are also possible; it is thought unnecessary to demonstrate them by specific examples. The general examples shown in *b* above are considered sufficient.

d. It is possible, however, and it may be practicable to extend the alphabet to 28, 30, or more characters by the subterfuge now to be explained. Suppose one of the letters of the alphabet is omitted from the set of 26 letters, and suppose it is replaced by 2, 3, or more *pairs* of letters, each pair having as one of its members the omitted single letter. Thus, in the case of a one-alphabet Playfair design of rectangular shape, in which the letter K is omitted as a single letter, and the number of characters in the rectangle is made a total of 30 by the addition of five combinations of K with other letters, the rectangle shown in figure 66 may be constructed. An interesting consequence of this modification is that certain irregularities are introduced in the cryptogram, consisting in (1) the occasional replacement of $\overline{\theta^1\theta^2}_p$ by $\overline{\theta^1\theta^2\theta^3}_c$, that is, of a digraph by a trigraph, (2) less frequently, the replacement of $\overline{\theta^1\theta^2\theta^3}_p$ by $\overline{\theta^1\theta^2\theta^3\theta^4}_c$, that is, of a trigraph by a tetragraph, and (3) the appearance of variant values. For example, $\overline{AM}_p = \overline{HKU}_c$; $\overline{GL}_p = \overline{OKO}_c$; $\overline{JK}_p = \overline{KAKE}_c$; $\overline{CK}_p = \overline{BKE}_c$, or $\overline{DKE}_c$, or $\overline{GP}_c$, or $\overline{TP}_c$. So far as the decryptographing is concerned, there would be no difficulty, because the operator always considers any K occurring in the cipher test as invariably forming a ligature with the succeeding letter, taking the pair of letters as a unit. In decryptographing a set of letters, such as $\overline{GP}_c$, he obtains $\overline{CKO}_p$; he disregards the O.

e. As a final note it may be added that it is, of course, possible to insert the letters within a matrix in a less systematic order than that indicated in the various examples. *The letters may be inserted at random or by following the principles of systematically-mixed alphabets, so that no definite sequence is apparent in the matrix.*

119. Combined Alphabetical and Numerical Matrix

a. Figure 67 shows a 4-section matrix which presents a rather interesting feature in that it makes possible the substitution of 3-figure com-

REF ID:A56932

binations for digraphs in a unique manner. To encipher a message one proceeds as usual to find the numerical equivalents of a pair, and then these numbers are added together. Thus:

Plain text:	PR	OC	EE	DI	NG
	275	350	100	075	325
	9	13	24	18	7
Cipher text:	284	363	124	093	332

	A	B	C	D	E	000	025	050	075	100	
	F	G	H	I	K	125	150	175	200	225	
Sec. 1 (θ^1_p)	L	M	N	O	P	250	275	300	325	350	Sec. 3 (θ^1_c)
	Q	R	S	T	U	375	400	425	450	475	
	V	W	X	Y	Z	500	525	550	575	600	
	0	1	2	3	4	V	Q	L	F	A	
	5	6	7	8	9	W	R	M	G	B	
Sec. 4 (θ^2_c)	10	11	12	13	14	X	S	N	H	C	Sec. 2 (θ^2_p)
	15	16	17	18	19	Y	T	O	I	D	
	20	21	22	23	24	Z	U	P	K	E	

Figure 67.

b. To decipher such a cryptogram, take the greatest multiple of 25 contained in the group of three digits; this multiple and its remainder form the elements for determining the plain-text pair in the usual manner. Thus, 284 = 275 + 9 = PR.

Section III. COMPLEX SUBSTITUTION SYSTEMS

120. General

In paragraph 64, brief reference was made to more complex substitution systems. It was stated that there are certain polyalphabetic methods in which periodicity is absent; there are other methods in which the external manifestation of periodicity in cryptograms is prevented, or in which it is suppressed or disguised. Slight hints were then given as to the nature of some of these methods. This and the next two sections give a more detailed description and discussion of the methods indicated, which, as a class, may be designated as *aperiodic* systems, as contrasted with the previously described, more simple *periodic* systems.

REF ID:A56932

121. Continuous or Nonrepeating-Key Systems

a. One of the simplest methods of avoiding periodicity occasioned by the employment of more than one substitution alphabet is to use as the key for the encipherment of one or more messages a series of letters or characters that does not repeat itself. The running text of a book, identical copies of which are in possession of the correspondents, may serve as the key for this purpose. It is only necessary for the correspondents to agree as to the starting point of the key, or to arrange a system of indicating this starting point in the text of the cryptogram. Such a system is called a continuous-key system. Other names applied to it are *nonrepeating, running,* or *indefinite-key* systems. Telephone directories, the Bible, standard reference works, etc., are often used as source books for such keys.

b. Various types of cipher alphabets may be employed in this system, direct or reversed standard alphabets, mixed alphabets drawn up at random, or secondary mixed alphabets resulting from the interaction of two primary sliding mixed components.

c. As an example of the method of cryptographing, suppose the following message is to be enciphered on the continuous key principle, using as the key the text of this subparagraph, beginning AS AN EXAMPLE . . . , and reversed standard alphabets:

HEAVY INTERDICTION FIRE FALLING AT . . . .

Key text:	ASANE XAMPL EOFTH EMETH ODOFC RYPTO . . .
Plain text:	HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram:	TOASG PNTLU BGDAZ QZZLQ KYOUR JLJTV . . .

122. Auto-Key Systems

a. The cipher letters of a cryptogram may serve as keyletters, thus automatically furnishing a key. Suppose, for example, that two correspondents agree to use the word TRUE as an initial key, and suppose the message to be enciphered (with the obsolete U. S. Army cipher disk) is as follows:

HEAVY INTERDICTION FIRE FALLING AT . . . .

The first four letters are enciphered as shown:

Key text:	TRUE
Plain text:	HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram:	MNUJ

The cipher letters MNUJ now form the keyletters for enciphering the next four plain-text letters, YINT, yielding OFHQ. The latter then form the keyletters for enciphering the next four letters, and so on, yielding the following:

REF ID:A56932

SECRET

Key text: TRUEM NUJOF HQKOE IIVWU VQODR LOSGD . . .
Plain text: HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram: MNUJO FHQKO EIIVW UVQOD RLOSG DBMGK . . .

b. Instead of using the cipher letters in sets, as shown, the last cipher letter given by the use of the keyword may become the keyletter for enciphering the plain-text letter; the cipher resultant of the latter then becomes the keyletter for enciphering the following letter, and so on to the end of the message. Thus:

Key text: TRUEJ LDQXT CZRPW OANIA JFAAP EWJDA . . .
Plain text: HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram: MNUJL DQXTC ZRPWO ANIAJ FAAPE WJDAH . . .

c. It is obvious that an initial keyword is not necessary; a single prearranged letter will do.

d. The plain text itself may serve as a key, after an initial group or an initial letter. This is shown in the following example, wherein the text of the message itself, after the prearranged initial keyword TRUE, forms the key text:

Key text: TRUEH EAVYI NTERD ICTIO NFIRE FALLI . . .
Plain text: HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram: MNUJJ WNCUR KLCYV UPOAX JAIGT XNFLP . . .

e. Although reversed standard alphabets have been used in all the foregoing examples, it is obvious that various types of alphabets may be employed, as prearranged.

f. The following method, although it may at first appear to be quite different, is in reality identical with those just described. A mixed sequence is prepared and its elements numbered in sequence. Let the mixed sequence be derived from the keyword PERMUTABLY:

6	3	7	5	9	8	1	2	4	10
P	E	R	M	U	T	A	B	L	Y
C	D	F	G	H	I	J	K	N	O
Q	S	V	W	X	Z				

A J B K E D S L N M G W P C Q R F V T I Z U H X Y O
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Let the message be the same as before, and let the first letter be its own cipher equivalent. Each cipher letter from that point on is produced in turn by finding the sum of the numerical equivalents of the preceding cipher letter and the plain-text letter to be enciphered. When this total exceeds 26, the latter amount is deducted and the letter equivalent of the remainder is taken for the cipher letter. Thus:

REF ID:A56932

Key text:	0	23	2	3	21	20	14	23	16	21	11	17	11	25	18	12	12
Plain text:	H	E	A	V	Y	I	N	T	E	R	D	I	C	T	I	O	N
Numerical value:	23	5	1	18	25	20	9	19	5	16	6	20	14	19	20	26	9
Keyed value:		28	3	21	46	40	23	42	21	37	17	37	25	44	38	38	21
(less 26 or 52 if necessary):	23	2	3	21	20	14	23	16	21	11	17	11	25	18	12	12	21
Cipher text:	H	J	B	Z	I	C	H	R	Z	G	F	G	Y	V	W	W	Z
Key text:	21	12	6	22	1	18	19	1	9	3	12	23	24				
Plain text:	F	I	R	E	F	A	L	L	I	N	G	A	T				
Numerical value:	17	20	16	5	17	1	8	8	20	9	11	1	19				
Keyed value:	38	32	22	27	18	19	27	9	29	12	23	24	43				
(less 26 or 52 if necessary):	12	6	22	1	18	19	1	9	3	12	23	24	17				
Cipher text:	W	D	U	A	V	T	A	N	B	W	H	X	F				

g. In the foregoing example the successive cipher letters form the successive keyletters; but, as noted in *d* above, the successive plain-text letters may serve as the successive keyletters.

h. The same results can be obtained by the use of sliding strips bearing the mixed alphabet. Study the following diagram showing the successive positions of the movable strip and compare the results with those obtained in *f* above.

Plain	Cipher	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y
H	H	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U
E	J	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A
A	B	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J
V	Z	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I
Y	I	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T
I	C	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P
N	H	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U
T	R	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q
E	Z	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I
R	G	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M
D	F	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R
I	G	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M
C	Y	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X
T	V	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F
I	W	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G
O	W	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G
N	Z	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I
F	W	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G
I	D	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E
R	U	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z
E	A	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O
F	V	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F
A	T	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V
L	A	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O
L	N	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L
I	B	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J
N	W	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G
G	H	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U
A	X	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H
T	F	F	V	T	I	Z	U	H	X	Y	O	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R

REF ID:A56932

i. One serious objection to such autokey systems is that the results of errors are cumulative; one error affects all the succeeding letters, and if several errors are made, the messages are difficult to decryptograph. It is possible that this disadvantage can be minimized by the use of automatic cipher devices suitably constructed to accomplish the encipherment with speed and accuracy.

123. Progressive-Alphabet Systems

a. The special characteristic of these systems is that the members of a whole set of cipher alphabets are employed one after the other in progression and in a definite sequence. These systems are periodic in nature and the length of the period is usually equal to the total number of different cipher alphabets employed in the system. The sequence in which the various cipher alphabets are used may or may not change with each message; if it does, this constitutes an additional element of secrecy.

b. To illustrate what is meant by a progressive system a simple example will be given, employing the obsolete U. S. Army Cipher Disk. Starting with the disk so that $A_p = A_c$ (or with any other prearranged initial setting), the first letter of the message is enciphered; the revolving alphabet is then moved one step clockwise (or counter-clockwise) and the second letter is enciphered, and so on. After 26 letters have been enciphered, the disk has returned to its initial starting point and a second cycle begins (if the message is longer than 26 letters). Thus, the period in this case is 26 letters. It is obvious that the displacement of the revolving disk may occur after every 2, 3, 4 . . . . letters, as prearranged, in which case the period increases correspondingly in length. The displacement may, however, be more complicated than this, and may occur after a constantly varying number of letters has been enciphered, whereupon periodicity is suppressed.

c. Two sliding mixed components may be employed, producing a set of 26 secondary mixed alphabets.

d. Another variation is more complicated. Suppose the correspondents draw up a set of 100 random-mixed cipher alphabets, each accompanied by a designating number from 00 to 99, and a set of numerical keys composed of randomized sequences of numbers from 00 to 99. Each such numerical key is designated by an indicator of some sort. To encipher a message, a key sequence is selected and the cryptogram is prepared by means of the sequence of alphabets indicated by the key sequence. If the message is 100 or less letters in length, the alphabets do not repeat; if it is more than 100 letters long, either the sequence of alphabets may repeat or else a new sequence is selected, as prearranged. It is possible to operate the system by means of indicators inserted in the text of the cryptogram.

REF ID:A56932

124. Interrupted or Variable-Key Systems

In certain of the foregoing systems it was noted that periodicity is entirely avoided by the use of a key which is so long that it does not repeat itself; often such a system is referred to as operating in connection with an *indefinite, infinite,* or *unlimited* key as contrasted with one that operates in connection with a *definite, finite,* or *limited* key. But periodicity may also be avoided by special manipulation of a limited key. Several such methods are explained below.

125. Suppressing Periodicity by Encipherment of Variable-Length Groupings of the Plain Text

a. A keyword, though limited in length, may nevertheless be applied to variable or invariable-length sections of the plain text. When, for example, each letter of the key serves to encipher a single letter of the plain text, the encipherment is said to be *invariable* or *fixed* in this respect. The same is true even if a single letter of the key serves to encipher regular sets of letters of the plain text; for example, each letter of the key may serve to encipher 2, 3, 4 . . . . letters of the text. In these cases periodicity would be manifested externally by the cryptograms, providing there is a sufficient amount of text to be examined. But if each letter of the key serves to encipher *irregular* or variable-length groupings of the plain text, then periodicity cannot appear except under rather remote contingencies. Suppose, for example, that so simple a scheme as letting each letter of the key serve to encipher a *complete word* of the text is used; since words are of irregular lengths and there is little or no regularity whatever in the sequence of words with respect only to their lengths, periodicity cannot appear. An example of encipherment will be useful.

b. In the following example the simple cipher disk (direct sequence sliding against reversed sequence) is used, with the key word DEBARK, to encipher the following message, according to the scheme described above. Study it carefully.

```
Key:          D     E      B       A    R    K
Plain text:   COLLECT ALL STRAGGLERS STOP SEND THEM
Cipher:       BPSSZBK ETT JIKBVVQXKJ IHML ZNEO RDGY

Key:          D    E   B
Plain text:   FORWARD AT ONCE
Cipher:       YPMHDMA EL NOZX

Cryptogram:   BPSSZ BKETT JIKBV VQXKJ IHMLZ NEORD
              GYYPM HDMAE LNOZX
```

c. Instead of enciphering according to natural word lengths, the irregular groupings of the text may be regulated by other agreements. For

REF ID:A56932

example, suppose that it is agreed that every keyletter will encipher a number of letters corresponding to the numerical value of the keyletter in the normal alphabet. The foregoing example then becomes as follows:

```
Key:          D     E   B  A          R
Plain text:   COLL ECTAL LS T RAGGLERSSTOPSENDTH
Cipher:       BPSS ACLET QJ H ARLLGNAZZYDCZNEOYK

Key:             K       D
Plain text:   EMFORWARDAT ONCE
Cipher:       GYFWTOKTHKR PQBZ

Cryptogram:   BPSSA CLETQ JHARL LGNAZ ZYDCZ NEOYK
              GYFWT OKTHK RPQBZ
```

d. The foregoing example employed reversed standard alphabets, but mixed alphabets of all types may readily be used.

e. If the keyword is short, and the message long, periodicity may creep in despite the irregular groupings in the encipherment. Sufficient evidence may even be obtained to lead to a disclosure of the length of the key. But if the key consists of a long word, or of a complete phrase or sentence, the text would have to be very long in order that sufficient evidences of periodicity be found to make possible the determinaton of the length of the key.

126. Suppressing Periodicity by Encipherment by Variable-Length Groupings of the Key

a. In paragraph 125*b* periodicity was suppressed by enciphering variable-length groupings of the text; in this paragraph it will be shown how periodicity may be suppressed by enciphering by variable-length groupings of the key. The method consists in *interrupting* the key.

b. Given a keyword, it can become a variable-length key by interrupting it according to some prearranged plan, so that it becomes equivalent to a series of keys of different lengths. Thus, the single keyword UNPREPAREDNESS may be expanded to a sequence of irregular lengths, such as UNPREP/UNP/UNPREPAR/UNPR/UNPREPARE/UNPREPAREDN/U/UNPRE, etc. Various schemes for indicating or determining the interruptions may be adopted. For example, suppose it may be agreed that the interruption will take place immediately after and every time that the letter R occurs in the plain text. The key would then be interrupted as shown in the following example:

```
Key:          UNPUN UNPRE PARED UNPRE UNPRU NP . . .
Plain text:   OURFR ONTLI NESAR ENOWR EPORT ED . . .
```

c. It is possible to apply an interrupted key to variable-length groupings of the plain text. In illustrating this method, an indicator, the letter

REF ID:A56932

X, will be inserted in the plain text to show when the interruption takes place. The plain text is enciphered by natural word lengths.

```
Key:         U     N     U     N     P     U
Plain text:  OUR FRONTX LINES ARE NOWX REPORTED
```

d. It is also possible to interrupt the key regularly, cutting it up into equal length sections as, for example, with the keyword EXTINGUISHER: EXT/XTI/TIN/ING/NGU/GUI/UIS/ISH/SHE/HER. Each set of three keyletters may serve to encipher a set of three plain-text letters. But it is possible to make each set of three keyletters apply to more than three plain-text letters, or to irregular groupings of plain-text letters. For example, suppose a numerical key be derived from the keyword:

```
E  X  T  I  N  G U  I  S  H  E  R
1-12-10—5—7—3-11—6—9—4—2—8
```

Let this numerical sequence determine how many letters will be enciphered by each grouping of the key. The example below will illustrate (reversed standard alphabets are used):

```
Numbers:      1        12          10          5
Key:          E XTIXTIXTIXTI TINTINTINT INGIN
Plain text:   C OLLECTALLSTR AGGLERSSTO PSEND
Cipher:       C JIXTRPXIXFAR TCHIEWBQUF TVCVK

Numbers:         7      3      11
Key:          NGUNGUN GUI UISUISU
Plain text:   THEMFOR WAR DATONCE
Cipher:       UZQBBGW KUR RIZGVQQ

Cryptogram:   CJIXT RPXIX FARTC HIEWB QUFTV
              CVKUZ QBBGW KURRI ZGVQQ
```

e. Another simple method of prearranging the interruption of a keyword or of plain text is to employ the sequence of numbers given by reducing an incommensurate fraction to decimals. For example, the fraction 1/7 yields the sequence 142857142857 . . . This fraction may be represented by the indicator letter H given as the initial letter of the cryptogram.

127. Cipher Devices in Which Periodicity Is Avoided

There are certain cipher devices which operate in such a manner that periodicity is avoided or suppressed. Some of them are discussed in section I, chapter 11. Among them one of the most interesting is that invented by Sir Charles Wheatstone in 1867. As a rule, however, cipher devices, by their very nature, can hardly avoid being cyclic in operation, thus causing periodicity to be exhibited in the cryptograms.

REF ID:A56932

CHAPTER 10
REPETITIVE AND COMBINED SYSTEMS

Section I. REPETITIVE SYSTEMS

128. Superencipherment

a. When, for purposes of augmenting the degree of cryptographic security, the plain text of a message undergoes a first or primary encipherment and the resulting cipher text then undergoes a second or secondary encipherment, the system as a whole is often referred to as one involving superencipherment. If the two or more processes are well selected, the objective is actually reached, and the resulting cryptograms present a relatively great degree of cryptographic security; but sometimes this is not accomplished and the augmented security is of a purely illusory character. The final cryptographic security may, in fact, be no greater in degree than if a single encipherment had been effected, and in unusual cases it may even be less than before.

b. It is impossible to describe all the combinations that might be employed; only a very few typical cases can here be treated, and these will be selected with a view to illustrating general principles. It is possible to pass a message through 2, 3, . . . successive processes of substitution; or through 2, 3, . . . successive processes of transposition; or substitution may be followed by transposition or vice versa. An example of each type will be given.

c. It will be convenient to adopt the symbol C to represent the cipher text produced by any unspecified process of encipherment. The symbols C_1, C_2, C_3, . . . , will then represent the successive texts produced by successive processes in superencipherment. The subscript letter *s* or *t* may be prefixed to the C to indicate that a given process is one of substitution or of transposition. Thus, the steps in a system where a first substitution is followed by a second substitution can be represented symbolically by $sC_1 \rightarrow sC_2$. In a similar manner, $tC_1 \rightarrow tC_2$ represents double transposition. The symbol $sC_1 \rightarrow tC_2$ means that the text from a first process of substitution undergoes transposition as a second process.

129. Repetitive Transposition Systems

These have been dealt with in Chapter 8, Sections II and III, and need no further discussion at this point. It was there shown that properly

REF ID:A56932

selected transposition methods, when repetitive in character, can produce cryptograms of very great security.

130. Repetitive Monoalphabetic Substitution Systems

Suppose a message undergoes a primary encipherment by means of a single-mixed, nonreciprocal alphabet, and the primary cipher text undergoes a secondary encipherment by means of the same or a *different* mixed alphabet. The resulting cryptogram is still monoalphabetic in character, and presents very little, if any, augmentation in the degree of security (depending upon the type of alphabet employed). Here an entirely illusory increase in security is involved and an ineffectual complexity is introduced; the process may indeed be repeated indefinitely without producing the desired result. This is because the fundamental nature of monoalphabetic substitution has not been taken into consideration in the attempts at superencipherment; $sC_1 \rightarrow sC_2 \rightarrow sC_3 \ldots$, still remains monoalphabetic in character.

131. Repetitive Polyalphabetic Substitution Systems

a. If the primary encipherment is by means of the repeating-key principle, with standard alphabets, and the secondary encipherment is similar in character, with similar alphabets, and a key of similar length, the final cryptogram presents no increase in security at all. Thus, if the key BCDE is used in the primary encipherment (Vigenère Method) and the key FGHI is used in the secondary encipherment, the final result is the same as though the key GIKM had been used in a single encipherment.

b. If mixed alphabets are used, and if those of the primary and the secondary encipherment belong to the same series of secondary alphabets resulting from the sliding of two primary sequences against each other, the results are similar in character to those described in *a* above. They are identical with those that would be obtained by an equivalent single encipherment by the appropriate secondary alphabets.

c. If the key for the secondary encipherment is of a different length from that for the primary encipherment, the results are, however, somewhat different, in that the period of the resultant cryptogram becomes the least common multiple of the two key lengths. For example, if the length of the key for the primary encipherment is 4, that for the secondary 6, the result is the same as though a key of 12 elements had been employed in a single encipherment. This can be demonstrated as follows, using the keys 4–1–2–3 and 5–2–6–1–4–3:

4 1 2 3 4 1 2 3 4 1 2 3	4 1 2 3 4 1 2 3 4 1 2 3	4 1 2 3 . . .
5 2 6 1 4 3 5 2 6 1 4 3	5 2 6 1 4 3 5 2 6 1 4 3	5 2 6 1 . . .
9 3 8 4 8 4 7 5 10 2 6 6	9 3 8 4 8 4 7 5 10 2 6 6	9 3 8 4 . . .

REF ID:A56932

d. The degree of cryptographic security is, without doubt, increased by such a method. If the key lengths are properly selected, that is, if they present no common multiple less than their product, the method may give cryptograms of great security. For example, two keys that are 17 and 16 characters in length would give a cryptogram that is equivalent in period to that of a cryptogram enciphered once by a key 17×16, or 272 elements in length. The fundamental principle of an excellent, though complicated, printing telegraph cipher system is this very principle.

Section II. COMBINED SYSTEMS

132. Combined Monoalphabetic and Polyalphabetic Substitution Systems

a. If a message undergoes a primary encipherment by the repeating-key method, using standard alphabets, and the primary cipher text then undergoes a secondary encipherment by means of a single-mixed alphabet, the degree of cryptographic security is increased to the same extent that it would be if the original message had undergone the same primary encipherment with secondary alphabets resulting from the sliding of a mixed primary sequence against the normal sequence. This increase in security is not very great.

b. The same is true if the primary encipherment is monoalphabetic and the secondary encipherment is polyalphabetic by the method described.

c. In general, this also applies to other types of polyalphabetic and monoalphabetic combinations. The increase in security is not very great, and is, indeed, much less than the uninitiated suspect.

133. Combined Substitution-Transposition in General

Combinations of substitution and transposition methods can take many different forms, and only a few examples can be illustrated herein. It is possible of course, to apply substitution first, then transposition, or transposition first, then substitution. The most commonly encountered systems, however, are of the former type, that is $s\mathrm{C}_1 \rightarrow t\mathrm{C}_2$. Furthermore, it can be stated that as a rule practicable systems in which both processes are combined use methods that are relatively simple in themselves, but are so selected as to produce cryptograms of great security as a result of the combination. To give a very rough analogy, in certain combinations the effect is much more than equivalent to the simple addition of complexities of the order X and Y, giving $X+Y$; it is more of the order XY, or even X^2Y^2.

REF ID:A56932

134. Monoalphabetic and Polyalphabetic Substitution Combined with Transposition

a. A message may undergo simple monoalphabetic substitution or complex polyalphabetic substitution and the resulting text passed through a simple transposition. Obviously, either standard or mixed alphabets may be employed for the substitution phase and for the transposition phase any one of the simple varieties of geometric-design methods may be applied.

b. As an example, note the following simple combination, using the message ALL ACTION AT LANDING BEACH HAS CEASED. 1st step: sC_1 (monoalphabetic, by mixed alphabet):

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: TDRAMOBNILPEZYXWVUSQKJHGFC

Message: ALLAC TIONA TLAND INGBE ACHHA SCEAS ED
Cipher: TEETR QIXYT QETYA IYBDM TRNNT SRMTS MA

2d step: tC_2 (as prearranged between correspondents):

TEETRQIX (For the inscription; a rectangle of eight columns.)
YTQETYAI
YBDMTRNN (For the transcription; counterclockwise route beginning
TSRMTSMA at lower right hand corner.)

Cryptogram: ANIXI QRTEE TYYTS RMTSM NAYTE QTBDM TR

c. A simple subterfuge often adopted between correspondents is to write the substitution text backwards to form the final cryptogram (a case of simple reversed writing).

d. An extremely simple and yet effective transposition method (when its presence is not suspected) sometimes employed as a preliminary to substitution is that in which the text of a message is first divided into halves; the second being placed under the first as in rail-fence writing. Thus:

P O E D O O T F M A K T O
R C E T P R O E B R A I N

Then encipherment by simple monoalphabetic methods may be effected and the cipher text taken from the two separate lines. Thus, if a standard alphabet one letter in advance were used, the text would be as follows:

Q P F E P P U G N B L U P
S D F U Q S P F C S B J O

Cryptogram: QPFEP PUGNB LUPSD FUQSP FCSBJ O

REF ID:A56932

e. A simple variation of the foregoing method which is frequently effective with true digraphic methods of substitution is to write θ^2_p under θ^1_p and then encipher the sets of juxtaposed $\overline{\theta^1\theta^1}_p$ letters digraphically, then the sets of juxtaposed $\overline{\theta^2\theta^2}_p$ letters. Thus, let the message be WILL RETURN AT ONCE; it would be written down as follows:[7]

WLRTRAOC
ILEUNTNE

Then the following pairs would be enciphered: $\overline{WL}_p$, $\overline{RT}_p$, $\overline{RA}_p$, $\overline{OC}_p$, $\overline{IL}_p$, etc. The foregoing message enciphered in this manner by means of the Playfair Square shown in figure 63, for example, yields the following cryptogram:

Plain text: WL RT RA OC IL EU NT NE
Cipher: VO IR TN LT CQ HN AR RP
Cryptogram: VOIRT NLTCQ HNARR P

f. Naturally the transposition process may involve groups of letters; a simple type of disarrangement is to reverse the order of the letters in 5-letter groups, or within 5-letter groups a transposition such as 3–2–1–4–5 or 2–1–5–3–4 (any of 120 different arrangements) is possible.

g. Columnar transposition methods lend themselves especially well to combination with substitution methods. An excellent example will be considered under the next section.

135. Polyliteral Substitution Combined with Transposition

In paragraph 111*b* the essential nature of polyliteral substitution as contrasted with monoliteral substitution was discussed. Polyliteral methods make use of polypartite alphabets in which the cipher equivalents are composed of two or more parts. This being the case it is a natural extension of cryptographic processes to *separate* these parts or to distribute them throughout the cipher text so that the components or, so to speak, fractional parts of the cipher equivalents are thoroughly disarranged and distributed evenly or irregularly throughout the text.

136. Fractionating Systems

a. A simple example will first be shown. Let the following bipartite cipher alphabet be drawn up by assigning numerical equivalents from 01 to 26 in mixed sequence to the letters of the normal sequence. Thus:

[7] In preparing the text for encipherment, the clerk must bear in mind that if the normal Playfair system is to be used no doublets can be enciphered. The message WE WILL LEAVE . . would be arranged thus:

WXILXEV
EWLXLAE

REF ID:A56932

A	B	C	D	E	F	G	H	I	J	K	L	M
02	11	06	12	13	05	10	14	09	15	16	17	01

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
03	18	19	20	08	21	07	04	22	23	24	25	26

Each letter is represented by a combination of two digits; in preparing the message for cryptographing, the two digits comprising the cipher equivalent of a letter are written one below the other, thus:

Plain text: ONE PLANE REPORTED LOST

Cipher θ^1_c: 101 11001 01110011 1120

Cipher θ^2_c: 833 97233 83988732 7817

By recombining the single digits in pairs, reading from horizontal lines, and writing down the pairs in unchanged numerical form, one obtains the following:

10 11 10 01 01 11 00 11 11 20
83 39 72 33 83 98 87 32 78 17

b. The foregoing cipher text can be transmitted in 5-figure groups, or it can be reconverted into letters by one means or another, but some difficulties are encountered in the latter case because every one of 100 different pairs of digits has to be provided for, thus necessitating a 2-letter substitution, which would make the cipher text twice as long as the plain text.

c. In the methods to follow presently, these difficulties are avoided by a simple modification. This modification consists in the employment of true *polyfid cipher alphabets,* that is, polypartite alphabets in which the plain component is the normal sequence and the cipher component consists of a sequence of equivalents composed of all the permutations of 2, 3, 4, . . . symbols taken in definite groups. For example, a *bifid alphabet*[8] composed of permutations of five digits taken two at a time can be constructed, yielding a set of 25 equivalents for a 25-letter alphabet (I and J being usually considered as one letter). A *trifid alphabet* of 27 equivalents can be constructed from *all* the permutations of the digits 1, 2, 3, taken three at a time; an extra character must, however, be added to represent the 27th element of the alphabet. It is convenient to represent the parts of a bifid equivalent by the symbols θ^1_c and θ^2_c, the parts of a trifid equivalent, by the symbols θ^1_c, θ^2_c and θ^3_c.

[8] Such an alphabet should be clearly differentiated from a *biliteral alphabet.* In the latter, two and only two elements are employed, in groups of fives, yielding 25 or 32 permutations. The Biliteral Cipher of Sir Francis Bacon and the Baudot Alphabet of modern printing telegraph systems are based upon alphabets that are typical examples of biliteral alphabets. The designation *digraphic alphabet* will be applied to one in which the cipher equivalents are composed of any number of symbols, *n,* taken simply in groups of two, these symbols not being permuted in systematic fashion to produce a complete set of 2^n equivalents.

REF ID:A56932

d. Polyfid cipher alphabets may be systematically-mixed alphabets based upon keywords and keyphrases. For example, note how the following bifid alphabet is derived from the keyphrase XYLOPHONIC BEDLAM:

X	Y	L	O	P	H	N	I	C	B	E	D	A
11	12	13	14	15	21	22	23	24	25	31	32	33

M	F	G	K	Q	R	S	T	U	V	W	Z
34	35	41	42	43	44	45	51	52	53	54	55

The same principle may be applied to trifid alphabets, employing the permutations of the three digits 1, 2, and 3, taken in groups of three.

e. Note the following bifid alphabet and the example of its use in enciphering a message:

A	B	C	D	E	F	G	H	I-J	K	L	M
12	31	21	32	33	15	25	34	24	35	41	11

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	42	43	44	23	45	22	14	51	52	53	54	55

Message: ONE PLANE REPORTED LOST

Cipher θ^1_c: 413 44113 23442233 4442

Cipher θ^2_c: 233 31233 33323232 1252

The bifid elements, θ^1_c and θ^2_c, are now recombined horizontally in pairs and the pairs are reconverted into letter equivalents of the basic alphabet which, for the sake of convenience, is here arranged in the form of a deciphering alphabet:

11	12	13	14	15	21	22	23	24	25	31	32	33
M	A	N	U	F	C	T	R	I	G	B	D	E

34	35	41	42	43	44	45	51	52	53	54	55
H	K	L	O	P	Q	S	V	W	X	Y	Z

Cryptogram: LHLNR QTEQO REAEE DDDAW

f. It will be noted that there are four basic steps involved in the foregoing encipherment: (1) A process of decomposition, substitutive in character, in which each θ_p is replaced by a bipartite θ_c, composed of two parts, θ^1_c and θ^2_c, according to a bifid alphabet; (2) a process of separation, transpositive in character, in which each θ^1_c is separated from the θ^2_c with which it was originally associated; (3) a process of recombination, also transpositive in character, in which each θ^1_c is combined with a θ^2_c with which it was not originally associated; and finally (4) a process of recomposition, substitutive in character, in which each new θ^1_c θ^2_c combination is given a letter value according to a bifid alphabet. In the foregoing example (*e* above), the alphabet for the recomposition was the same as that for the decomposition; this,

REF ID:A56932

of course, is not an inherent necessity of the system; the decomposition and recomposition alphabets may be entirely different. This is shown in the example in paragraph 137*d*.

137. Comparison of Foregoing Fractionating System with Certain Digraphic Systems

a. The method described in paragraph 136*e* can be identified with some of the digraphic substitution systems discussed in chapter 9, section I.

b. Take the message of paragraph 136*e* and let a slight modification in the method of recombining θ^1_c and θ^2_c be made. Specifically, let the first halves and the second halves of the bifid equivalents of the plain-text letters be combined in the following manner, using the bifid alphabet of paragraph 136*e*:

Message: ONE PLANE REPORTED LOST

ON	EP	LA	NE	RE	PO	RT	ED
41=L	34=H	41=L	13=N	23=R	44=Q	22=T	33=E
23=R	33=E	12=A	33=E	33=E	32=D	32=D	32=D

LO	ST
44=Q	42=O
12=A	52=W

Cryptogram: LRHEL ANERE QDTDE DQAOW

If the cryptogram given in paragraph 136*e* were split in the middle into two sections, and the letters taken alternately, the result would be identical with that obtained in this subparagraph. The identification referred to in *a* above is demonstrated in *c* below.

c. Note the two alphabet matrix shown in figure 68. If the same message is now enciphered by its means, a cryptogram identical with that obtained in *b* above will be obtained. Thus:

M	A	N	U	F
C	T	R	I	G
B	D	E	H	K
L	O	P	Q	S
V	W	X	Y	Z

M	C	B	L	V
A	T	D	O	W
N	R	E	P	X
U	I	H	Q	Y
F	G	K	S	Z

Message:

ONE PLANE REPORTED LOST

Substitution of pairs:

$ON_p = LR_c$; $EP_p = HE_c$; $LA_p = LA_c$; $NE_p = NE_c$; $RE_p = RE_c$; etc.

Cryptogram:

LRHEL ANERE etc.

Figure 68.

REF ID:A56932

d. In the example in paragraph 136*e*, the same bifid alphabet was used for the recomposition as for the decomposition. Instead of converting the combined θ^1_e θ^2_e elements into letters by means of the original bifid alphabet, suppose a second bifid alphabet specifically drawn up for this recomposition is at hand (see par. 136*f*). Thus:

11=A	21=B	31=C	41=K	51=V
12=U	22=I	32=D	42=N	52=W
13=T	23=L	33=F	43=P	53=X
14=0	24=E	34=G	44=Q	54=Y
15=M	25=S	35=H	45=R	55=Z

The encipherment of the message is then as follows:

Message: ONE PLANE REPORTED LOST.

Alphabet for decomposition		*Alphabet for recomposition*	
A=12	N=13	11=A	34=G
B=31	0=42	12=U	35=H
C=21	P=43	13=T	41=K
D=32	Q=44	14=0	42=N
E=33	R=23	15=M	43=P
F=15	S=45	21=B	44=Q
G=25	T=22	22=I-J	45=R
H=34	U=14	23=L	51=V
I-J=24	V=51	24=E	52=W
K=35	W=52	25=S	53=X
L=41	X=53	31=C	54=Y
M=11	Y=54	32=D	55=Z
	Z=55	33=F	

Encipherment:

ON	EP	LA	NE	RE	PO	RT	ED
41=K	34=G	41=K	13=T	23=L	44=Q	22=I	33=F
23=L	33=F	12=U	33=F	33=F	32=D	32=D	32=D

LO	ST
44=Q	42=N
12=U	52=W

Cryptogram: KLGFK UTFLF QDIDF DQUNW

e. Now encipher the same plain-text message by means of the four-alphabet matrix shown in figure 69. The results are as follows:

Message: ONE PLANE REPORTED LOST.

Plain text: ON EP LA NE RE PO RT ED LO ST

Cipher pairs: KL GF KU TF LF QD ID FD QU NW

Cryptogram: KLGFK UTFLF QDIDF DQUNW

The results are identical with those obtained in *d* above.

REF ID:A56932

M A N U F C T R I G B D E H K L O P Q S V W X Y Z	A U T O M B I L E S C D F G H K N P Q R V W X Y Z
A B C K V U I D N W T L F P X O E G Q Y M S H R Z	M C B L V A T D O W N R E P X U I H Q Y F G K S Z

Figure 69.

f. If the successive letters of the cryptogram of *b* above are enciphered monoalphabetically by means of the following alphabet, the results again coincide with those obtained in *d* and *e* above.

Alphabet

C_1: A B C D E F G H I-J K L M N O P Q R S T U V W X Y Z
C_2: U C B D F M S G E H K A T N P Q L R I O V W X Y Z

First cryptogram: LRHEL ANERE QDTDE DQAOW
Final cryptogram: KLGFK UTFLF QDIDF DQUNW

138. Fractionating Systems as Forms of Combined Substitution and Transposition

In studying the various types of substitution discussed in chapter 9, section II, it was not apparent, and no hint was given, that these systems combine both substitution and transposition methods into a single method. But the analysis presented in paragraph 137 shows clearly that there is a kind of transposition involved in digraphic methods involving the use of matrices.

139. Fractionation and Recombination within Regular or Variable Groupings of Fractional Elements

a. This method is an extension or modification of that illustrated in paragraph 136*e*. Let the text be written out in groups of 3, 4, 5, . . . letters, as prearranged between the correspondents. Suppose groupings of five letters are agreed upon; a bifid alphabet (that in par. 136*e*) is used for substitution; thus:

Message: ONEPL ANERE PORTE DLOST
41344 11323 44223 34442
23331 23333 32323 21252

REF ID:A56932

Then, let the recombinations be effected *within* the groups horizontally. Thus, for the first group the recombinations are 41, 34, 42, 33, and 31. The entire message is as follows:

41.34.4	11.32.3	44.22.3	34.44.2
2.33.31	2.33.33	3.23.23	2.12.52

Recomposition (using the same bifid alphabet as was used for the decomposition) yields the cryptogram:

LHOEB MDDEE QTERR HQTAW

b. As indicated, other groupings may be employed. Furthermore, a different bifid alphabet for the recomposition may be used than was employed for the original substitution or decomposition. It is also clear that sequences of variable-length groupings may also be employed, as determined by a subsidiary key.

c. Trifid alphabets also lend themselves to these methods. Note the following example:

Alphabet for decomposition			*Alphabet for recomposition*		
A=222	J=312	S=131	111=I	211=U	311=V
B=322	K=112	T=122	112=K	212=N	312=J
C=121	L=231	U=211	113=W	213=H	313=$\overline{\text{ZB}}$
D=133	M=323	V=311	121=C	221=X	321=E
E=321	N=212	W=113	122=T	222=A	322=B
F=123	O=333	X=221	123=F	223=Y	323=M
G=332	P=233	Y=223	131=S	231=L	331=Q
H=213	Q=331	Z=132	132=$\overline{\text{ZA}}$	232=R	332=G
I=111	R=232	?=313	133=D	233=P	333=O

Message: H A S A I R P L A N E R E T U R N E D Y E T ?

H	A	S	A	I	R	P	L	A	N	E	R	E	T	U	R	N	E	D	Y	E	T	?
2	2	1.2	1		2	2	2.2	2		3	2	3.1	2		2	2	3.1	2		3	1	3
1.2	3	2.1			3.3	3	2.1			2.3	2	2.1			3.1	2	3.2			2	2	1
3	2.1	2	1		2	3.1	2	2		1	2.1	2	1		2	2.1	3	3		1	2	3

Cipher text[9]: XUR$\overline{\text{ZA}}$C AYGFT MTBKC YFFAD $\overline{\text{ZB}}$XF
Final cryptogram: XURZA CAYGF TMTBK CYFFA DZBXF

[9] The reason for the regrouping shown in the final cryptogram requires a consideration of the fact that a trifid alphabet involves the use of 27 characters. Since our alphabet contains but 26 letters, either an extra symbol would have to be used (which is impractical) or some subterfuge must be adopted to circumvent the difficulty. This has been done in this case by using $\overline{\text{ZA}}$ and $\overline{\text{ZB}}$ to represent two of the permutations in the recomposition alphabet. In decryptographing, when the clerk encounters the letter Z in the text, it must be followed either by A or by B; according to the alphabet here used, ZA represents permutation 132, and ZB represents permutation 313. In order not to introduce a break in the regulation 5-letter groupings of cipher text, the final cryptogram is regrouped strictly into fives.

REF ID:A56932

d. Bifid and trifid alphabets may be combined within a single system with appropriate groupings, but such combinations may be considered as rather impracticable for military usage.

140. Fractionation Combined with Columnar Transposition

a. An excellent system of combined substitution-transposition that has stood the test of practical, war-time usage is that now to be described. Let a 36-character bipartite alphabet square be drawn up, and a message enciphered, as follows:

	M	O	N	T	H	S
W	H	8	A	1	I	9
I	L	C	3	0	U	M
N	B	2	P	Y	N	D
T	4	E	5	F	6	G
E	7	J	Ø	K	Q	R
R	S	T	V	W	X	Z

(Key for internal alphabet: HAIL COLUMBIA HAPPY LAND. Digits are inserted immediately after each letter from A to J, A being followed by 1, B, 2, etc.)

Message:

ADVANCE PROGRESSING SATISFACTORILY OVER 400 PRISONERS AND 5-75 MM GUNS CAPTURED. SECOND OBJECTIVE REACHED AT 5:15 P. M.

Substitution:

A	D	V	A	N	C	E	P	R	O	G	R	E	S	S
WN	NS	RN	WN	NH	IO	TO	NN	ES	IT	TS	ES	TO	RM	RM
I	N	G	S	A	T	I	S	F	A	C	T	O	R	I
WH	NH	TS	RM	WN	RO	WH	RM	TT	WN	IO	RO	IT	ES	WH
L	Y	O	V	E	R	4	ø	ø	P	R	I	S	O	N
IM	NT	IT	RN	TO	ES	TM	EN	EN	NN	ES	WH	RM	IT	NH
E	R	S	A	N	D	5	7	5	M	M	G	U	N	S
TO	ES	RM	WN	NH	NS	TN	EM	TN	IS	IS	TS	IH	NH	RM
C	A	P	T	U	R	E	D	S	E	C	O	N	D	O
IO	WN	NN	RO	IH	ES	TO	NS	RM	TO	IO	IT	NH	NS	IT
B	J	E	C	T	I	V	E	R	E	A	C	H	E	D
NM	EO	TO	IO	RO	WH	RN	TO	ES	TO	WN	IO	WM	TO	NS
A	T	5	1	5	P	M								
WN	RO	TN	WT	TN	NN	IS								

The C_1 text is now inscribed in a rectangle of predetermined dimensions. Transposition rectangle (columnar, based on key HAIL COLUMBIA HAPPY LAND) (see figure 70).

b. One of the important advantages of this type of cipher is that it affords accuracy in transmission since the text is composed of a

REF ID:A56932

H	A	I	L	C	O	L	U	M	B	I	A	H	A	P	P	Y	L	A	N	D
8	1	10	12	6	17	13	20	15	5	11	2	9	3	18	19	21	14	4	16	7
W	N	N	S	R	N	W	N	N	H	I	O	T	O	N	N	E	S	I	T	T
S	E	S	T	O	R	M	R	M	W	H	N	H	T	S	R	M	W	N	R	O
W	H	R	M	T	T	W	N	I	O	R	O	I	T	E	S	W	H	I	M	N
T	I	T	R	N	T	O	E	S	T	M	E	N	E	N	N	N	E	S	W	H
R	M	I	T	N	H	T	O	E	S	R	M	W	N	N	H	N	S	T	N	E
M	T	N	I	S	I	S	T	S	I	H	N	H	R	M	I	O	W	N	N	N
R	O	I	H	E	S	T	O	N	S	R	M	T	O	I	O	I	T	N	H	N
S	I	T	N	M	E	O	T	O	I	O	R	O	W	H	R	N	T	O	E	S
T	O	W	N	I	O	W	M	T	O	N	S	W	N	R	O	T	N	W	T	T
N	N	N	I	S																

Cryptogram:

NEHIM TOION ONOEM NMRSO TTENR OWNIN
ISTNN OWHWO TSISI OROTN NSEMI STONH
ENNST WSWTR MRSTN THINW HTOWN SRTIN
ITWNI HRMRH RONST MRTIH NNIWM WOTST
OWSWH ESWTT NNMIS ESNOT TRMWN NHETN
RTTHI SEONS ENNMI HRNRS NHIOR ONRNE
OTOTM EMWNN OINT

Figure 70.

limited number of letters. In fact, if the horizontal and vertical coordinates of the cipher square are the same letters, then the cryptographic text is composed of permutations of but six different letters, thus aiding very materially in correct reception. Indeed, it is even possible to reconstruct completely a message that has been so badly garbled that only half of it is present. This cipher system was used with considerable success by the Germany Army in 1917–18, and was known to the Allies as the ADFGVX Cipher, because these were the letters used as horizontal and vertical coordinates of the cipher square, and consequently the cipher text consisted solely of these six letters.

c. The cipher text of the foregoing message is, of course, twice as long as the plain text, but it can be reduced to exactly the original plain-text length by combining the distributed or transposed θ^1_c and θ^2_c elements in pairs, referring to the original (or a different) polypartite square, and recomposing the pairs into letters. In this case, the horizontal and vertical coordinates must be identical in order to permit of finding equivalents for all possible pairs.

REF ID:A56932

CHAPTER 11

CIPHER DEVICES AND CIPHER MACHINES

Section I. CIPHER DEVICES

141. General

The cipher systems previously described by no means exhaust the category of complex systems, but it is impossible to describe them all. Furthermore, each one presents innumerable possibilities for modification in minor respects and for combination with other methods. In the paragraphs to follow, the principles upon which certain of the more simple cipher devices have been based are described.

142. Wheatstone Cipher[10]

a. The device is a little more than four inches in diameter, and consists of a dial with two hands, as shown in figure 71. The dial is composed of two independent circles of letters. In the outer circle the letters progress clockwise in normal alphabetic sequence, but there is an extra character between the Z and the A, making a total of 27 characters. Some of the spaces also have digits inscribed in them, for enciphering numbers. In the inner circle the letters are arranged in mixed alphabetic sequence and are inscribed either on a surface which permits of erasure, or on a detachable cardboard circle which can be removed and replaced by another circle bearing a different sequence. In figure 71 this inner sequence is a systematically mixed sequence derived from the keyword FRANCE, as follows:

1	2	3	4	5	6
F	R	A	N	C	E
B	D	G	H	I	J
K	L	M	O	P	Q
S	T	U	V	W	X
Y	Z				

F B K S Y R D L T Z A G M U N H O V C I P W E J Q X

[10] Credit for the invention of the device and system described in this paragraph belongs not to Sir Charles Wheatstone, as has until recently been thought, but to an American, Decius Wadsworth, who in 1817 constructed a device identical in principle with that described on pp. 342–347 of *The Scientific Papers of Sir Charles Wheatstone*, published by the Physical Society of London in 1879. The Wheatstone device used a 27-element outer alphabet (26 letters

REF ID:A56932

b. The two hands are pivoted concentrically, as are the hour and minute hands of a clock. Now, in a clock, the minute hand makes a complete revolution, while the hour hand makes only $\frac{1}{12}$ of a complete revolution; the action in the case of this device, however, is somewhat different. The short hand is free to move independently of the long one, although the motion of the latter affects the former. Since the outer circle has 27 spaces and the inner one only 26, by a simple mechanical contrivance each complete revolution of the long hand causes the short hand to make $1\frac{1}{26}$ revolutions, thus causing the short hand to point one place in advance of where it pointed at the end of the preceding revolution of the long hand. For example, when the long hand is over B of the outer circle and the short hand points to R of the inner circle, if the long hand is pushed clockwise around the dial, making a complete revolution, the short hand will also make a complete revolution clockwise plus one space, thus pointing to D.

c. To encipher a message, the long hand and the short hand are set to prearranged initial positions. It is usual to agree that the plain-text letters will be sought in the outer circle of letters, their cipher equivalents in the inner circle; and that the long hand is invariably to be moved in the same direction, usually clockwise.

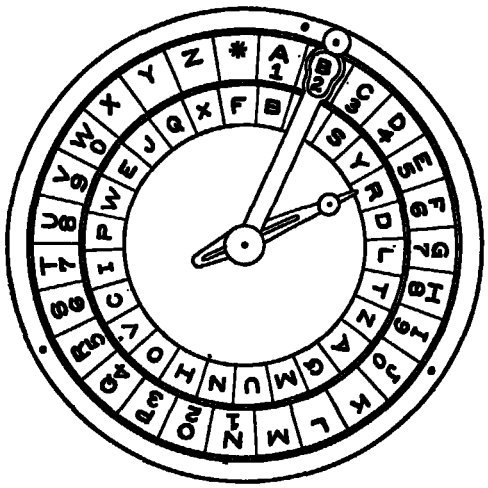


Figure 71.

Suppose the message to be enciphered is SEND AMMUNITION FORWARD. The long hand is moved clockwise until it is directly

and a word-separator), and a 26-element inner alphabet; the Wadsworth device used a 33-element outer alphabet (26 letters and the digits 2–8, inclusive), and a 26-element inner alphabet. Also, whereas in the Wheatstone device only the cipher component could be varied, in the Wadsworth device both components could be varied according to identical or non-identical mixed sequences.

REF ID:A56932

over S on the outer sequence. The letter to which the short hand points is the cipher equivalent of S and is written down. Then the long hand is moved clockwise to a position over E, the letter to which the short hand points is noted and written down. When a double letter occurs in the plain text, as in the case of the double M of AMMUNITION, some infrequently used letter, such as Q, must be substituted for the second occurrence of the letter. To decipher a message, the hands are returned to their initial prearranged position, and then the long hand is moved clockwise until the short hand points to the first cipher letter; the long hand is then directly over the plain-text letter. The process is continued until all the letters have been deciphered.

d. A consideration of the foregoing details shows that the encipherment of a message depends upon a combination of the following variables:

(1) The sequence of letters in the outer circle. In the case just considered, this sequence must be regarded as a known sequence, since it consists merely of the normal alphabet plus one character.
(2) The sequence of letters in the inner circle.
(3) The initial juxtaposition of the two sequences.
(4) The exact composition of the text to be enciphered, since this will determine the number of revolutions of the long hand required to encipher a given number of letters of the message.

e. It is obvious that if the outer alphabet is made a mixed alphabet, as well as the inner, both being different, the cryptograms will be made the more secure against cryptanalysis.

f. The same results as are obtained by using the device can be obtained by using sliding strips of paper, providing the operator will bear in mind that every time a θ_p on the plain component is situated to the left of the preceding θ_p, he must displace the cipher component one interval to the left, if the correspondents have agreed upon a clockwise movement of the long hand, or to the right, if they have agreed upon a counterclockwise movement of the long hand.

143. Jefferson Cipher

a. Credit for the invention of the cipher system and device now to be described belongs to Thomas Jefferson,[11] the original inventor,

[11] The late John M. Manly, Ph. D., formerly Captain, Military Intelligence Division, U. S. A., discovered, in 1922, a description of the device among Jefferson's Papers in the Library of Congress (vol. 232, item 41575, Jefferson's Papers). For a photographic reproduction of this historically interesting item, see pp. 189–91 of *Articles on Cryptography and Cryptanalysis Reprinted From The Signal Corps Bulletin*, Signal Security Service Publication, OCSigO, Washington, 1942.

REF ID:A56932

although it was independently invented many years later (1891) by a French cryptographer, Commandant Bazeries, and still later (1914) by Captain Parker Hitt, U. S. Army (now Colonel, U. S. Army, Ret.). Because it was first described in print (1901) by Bazeries, the principle upon which the cipher system is based is usually referred to in the literature as the Bazeries principle; for the sake of historical accuracy, however, it is herein called the Jeffersonian principle.

b. The basis of this principle is the use of a set of 20 (or more, if desired) mixed alphabets arranged in a sequence that can readily be changed; these can be used in the encipherment of a whole set of 20 letters with one and the same displacement of the alphabets. Successive encipherments are accomplished with different displacements of the alphabets.

c. Whereas Jefferson contemplated a device using a total of 36 different alphabets mounted on revolvable disks, the one Bazeries described used only 20 alphabets mounted in the same manner.

144. The Obsolete U. S. Army Cipher Device, Type M–94

a. This cipher device is based upon the Jeffersonian principle, using 25 mixed alphabets on small aluminum disks. It was widely employed in the U. S. military service and to a more limited extent in other U. S. services until 1942, when it was superseded by better devices.

b. In using the device, the 25 disks were first arranged according to the key for the day (the disks bearing the identifying numbers 1–25, and also the letters B–Z), and then the first twenty-five letters of the plain text were set up along a guide rule. The cipher text consisted of *any* one of the other rows, which would be taken off in five groups of five letters each. This process continued until the entire message was enciphered. To decryptograph, it was merely necessary for the deciphering clerk to set up along the guide rule of the device (properly arranged according to the daily key) the first twenty-five letters of the cipher text, and then by inspection find the one and only one row of letters that constituted plain text, which process would be repeated until the entire message was deciphered.

145. Strip Cipher Systems

a. A modification of the Jeffersonian principle which has found merit in practical cryptography is the strip cipher system. This is nothing more than a series of printed, random-alphabet strips to take the place of the disks of the cylindrical devices. These strips, bearing identifying numbers, slide freely in a strip board which may be made of metal, wood, or plastic. The strips are simpler to produce and more economical to replace than metal disks.

REF ID:A56932

b. It is possible to incorporate modifications of the basic idea of the Jeffersonian principle in using strip systems. For instance, there may be a daily selection of strips from a set consisting of a much larger number; or there may be different sets of strips for messages in the various security classifications; or different sets of strips may be issued to different groups of holders, etc.

Section II. CIPHER MACHINES

146. Importance of Cipher Machines in Modern Cryptographic Communication

The remarks made in paragraph 2 regarding the present trends in the art, are believed to be sufficient to give a clear idea of the importance of a knowledge of the uses and limitations of cipher machines as adjuncts to modern cryptographic communications. However, in this text only observations of a general character can be made, leaving for a future text an exposition of detailed principles involved in the construction and operation of a few typical cipher machines. More and more attention is today being devoted to this phase of cryptography and to a large extent cipher machines have replaced code systems even in lower headquarters, except for small, special-purpose codes.

147. Transposition-Cipher Machines

These are rarely encountered; the files of United States patents disclose but two examples and so far as is known no actual machines have been constructed conforming to the specifications covered therein. It may be said that substitution methods lend themselves so much more readily to automatic encipherment than do transposition methods that the possibilities for the construction of cipher machines for effecting transpositions are almost completely overlooked. Basically it would seem that a machine for effecting transposition would have to include some means for "storing up" the letters until all the plain text has been "fed into the machine," whereupon the transposing process is begun and the letters are finally brought out in what externally appears to be a randomized order. It is conceivable that a machine might be devised in which the disarrangement of the letters is a function merely of the number of letters comprising the message; daily changes in the randomizing machinery could be provided for by resetting the elements controlling the process.

148. Substitution-Cipher Machines

a. The substitution principle lends itself very readily to the construction of cipher machines for effecting it. The cipher devices described in the

REF ID:A56932

preceding section, as well as the simpler varieties making use merely of two or more superimposed, concentric disks are in the nature of hand-operated substitution-cipher mechanisms that are difficult to use, cannot be employed for rapid or automatic cryptographic manipulations, and are quite markedly susceptible to errors in their operation. For a long time these defects have been recognized and many men have striven to produce and to perfect devices more automatic in their functioning. However, the would-be inventors have not, as a rule, realized the complexity of the problems confronting them; nor have they approached these problems with the necessary and thorough knowledge of both theoretical and practical cryptography, with its many limitations, and theoretical as well as practical cryptanalysis, with its wide possibilities for the exercise of human ingenuity. However, when the problem of developing and producing a good cipher machine is attacked by a competent cryptographic and cryptanalytic engineering staff, highly efficient cipher machines can be developed. At this writing some very excellent machines are now in actual use for practical secret communications.

b. It is obvious that automatic devices of this nature should be equipped with a keyboard of some kind, resembling or duplicating that of an ordinary typewriter. Furthermore, for rapid manipulation these machines must be actuated by mechanisms affording speed in operation, such as electric or spring motors, compressed air, electromagnets, etc.

149. Machines Affording Only Monoalphabetic Substitution

Little need be said of those machines in which the ordinary keys of the keyboard are merely covered with removable caps bearing other letters or characters. They yield only the simplest type of substitution cipher known and have little to recommend them. Even when the mechanism is such that a whole series of alphabets can be brought into play, if the encipherment is monoalphabetic for a succession of 20 or more letters before the alphabet changes, the degree of cryptographic security is relatively low, especially if the various alphabets are interrelated as a result of their derivation from a limited number of primary components.

150. Machines Affording Polyalphabetic Substitution

a. In recent years there have been placed upon the commercial market several cipher machines of more than ordinary interest, but they cannot be described here in detail. In some of them the number of secondary alphabets is quite limited, but the method of their employment, or rather the manner in which the mechanism operates to bring the cipher alphabets into play is so ingenious that the solution of cryptograms prepared by means of the machine is exceedingly difficult. This point should be clearly recognized and understood: *other things being equal, the manner*

REF ID:A56932

of shifting about or varying the cipher alphabets contributes more to cryptographic security than does the number of alphabets involved, or their type. For example, it is quite possible to employ 26 direct-standard alphabets in such an irregular sequence as to yield greater security than is afforded by the use of 1,000 or more mixed alphabets in a regular or an easily-ascertained method. The importance of this point is not generally recognized by inventors.

b. One of the serious limitations upon the development of good cipher machines is that the number of letters in our alphabet, 26, does not lend itself well to mechanical or mathematical manipulation, because it has but the factors 1, 2, and 13; nor is it a perfect square. If the alphabet consisted of 25, 27, or 36 characters, much more could be done. The addition of figures or symbols to the 26-letter alphabet introduces the serious practical difficulty that the cryptograms will contain characters other than letters and the cost of transmitting intermixtures of letters, figures, and symbols by Morse telegraphy is prohibitive. Subterfuges of one sort or another, employed to circumvent this difficulty, are usually impractical and expensive.

151. The Converter M–209

a. This machine, widely used for low-echelon U. S. Army communications, is a small, compact, hand-operated, tape-printing, mechanical cipher machine, weighing 6 pounds, with dimensions 7¼" x 5$^{7}/_{16}$" x 3½". The cryptographic principle of this machine embodies polyalphabetic substitution, employing a complex mechanical arrangement to generate a long running key which is used in conjunction with reversed standard alphabets for the primary components. Despite the period of 101,405,850 before the keying cycle repeats, nevertheless a high degree of security can be imparted to messages enciphered by means of this converter *only* if the machine is properly used according to authorized instructions and if the messages are drafted with proper regard for security.

b. Space does not permit the inclusion of details of operation, etc., of this machine. However, full instructions as to its use, maintenance, and repair will be found in TM 11–380, "Converter M–209, M–209–A, M–209–B (Cipher)".

152. Advantages and Disadvantages of Cipher Machines

a. The principles underlying the various machines which have thus far been developed are so diverse and complex that no description of them can be undertaken in this text. However, a few remarks of a general character, dealing with the advantages and disadvantages of cipher machines in military communications today, are deemed pertinent.

REF ID:A56932

b. Until a few years ago, code methods were predominant in military cryptography within the United States Army but the reverse is now the case. This important change has been the result of advances made within comparatively recent years in the design and construction of cryptographic systems and apparatus. It may be useful to compare code methods in general with methods based upon cipher devices and cipher machines in general to note the advantages and disadvantages of each category of methods.

c. (1) When designed for keyboard operation and equipped with a standard typewriter keyboard, cipher machines afford much more speed in encipherment and decipherment than do any "hand-operated" cryptographic methods, including codes and certain types of cipher devices. Comparative speed tests gave the following data recently:

Number of groups or words per minute

Method*	Cryptographing	Decryptographing
1	4.04 (4-letter or 4-figure groups)	6.00
2	1.94 (4-letter or 4-figure groups)	2.26
3	1.75 (5-letter groups)	1.78
4	2.74 (5-letter groups)	3.98
5	3.14 (5-letter groups)	3.54
6	30.00 (5-letter groups)	25.00

*Method 1—A 2-part code of 6,000 groups unenciphered.
Method 2—The same code enciphered by a secure system.
Method 3—The obsolete U. S. Army Cipher Device, Type M–94.
Method 4—A small electrical cryptographic machine giving lamp indications but not provided with a typewriter keyboard.
Method 5—The Converter, M–209.
Method 6—An electrical cryptographic machine producing a printed record and provided with a keyboard.

(2) When properly designed, cipher machines and certain types of "hand-operated" cryptographs afford greater guarantees of cryptographic security than do code methods or hand-operated "pencil and paper" cipher systems, because machines can accurately, speedily, and tirelessly perform far more complex cryptographic operations than can possibly be performed even by the most skillful cryptographers working with code books and cipher tables, or with hand-operated cipher systems.

(3) Though the initial cost of a cipher machine may compare unfavorably with the initial cost of a code book, the over-all cost of maintaining cryptographic security by means of cipher machines is probably less than that in the case of code systems. Good machines designed by technically qualified experts afford a multiplicity of keying arrangements; once distributed there

REF ID:A56932

is no necessity for recalling "old editions" and substituting "new editions," as is the case with code books. Therefore, the labor costs incident to the necessity for repeated preparation, printing, and distribution of code books, together with the labor costs incident to the necessity for repeated accounting operations, correspondence exchanges relative to issue, receipt, etc., in the end overbalance the higher initial cost of cipher machines. In this connection it should be stated that merely the cost of printing an edition of 200 copies of a large 2-part code is well over $25,000. This does not include the cost of the labor involved in the compilation of the code, nor of that involved in preparing, printing, and binding cipher tables for superencipherment, etc.

(4) The security of a cryptographic system involving the use of a properly designed cipher device or cipher machine is not wholly dissipated by the capture or compromise of the machine or device itself, as is the case with a code book.

(5) On the other hand, it must be admitted that, as a general rule, the solution of a very few cryptograms by long and laborious cryptanalysis makes it possible, in the case of a cipher machine, to decryptograph more or less readily many or all other cryptograms enciphered by the same machine with the same (or in certain cases) different "settings," keys, or elements; whereas in the case of a large 2-part code the solution of a few code messages can hardly be accomplished at all, and practical analysis of the code must await the accumulation of a large amount of traffic. Even should the plain text of one or two code messages be obtained by theft or capture, this would not permit the prompt decoding of subsequent messages in the same code; whereas this may be possible in the case of cipher messages.

(6) Again, cipher machines are, as a rule, complicated and delicate mechanisms. They require considerable technical skill for their proper operation by cryptographic clerks, skill which may not always be possessed by such personnel. What is perhaps more important, complicated cipher machines require the skill and services of special personnel for their proper maintenance and repair. They usually require electric current for operation, which may not always be available.

(7) If the cipher machine employed is at all complicated to set up for enciphering and deciphering, errors are easy to make and sometimes call for costly or laborious exchanges of service messages relative to their correction. However, this may be a doubtful point because complex superenciphered code is just as subject to errors as is a complex cipher machine.

REF ID:A56932

(8) As regards administrative communications, cipher cannot compete with code from the point of view of condensation or abbreviation. A cipher message is always at least as long as the original plain-text message, whereas a code message prepared by means of a large code specially compiled to give a high degree of condensation is usually much shorter than the equivalent original plain-text message. This arises, of course, from the fact that in well-constructed code books single groups of 4 or 5 characters may represent long phrases or even whole sentences.

(9) As a rule, cipher devices or machines cannot readily be operated under all sorts of weather conditions. In very damp or in rainy climates, machinery failures are quite common, and it is difficult to keep delicate machines in regular service. Moreover, in hot, humid climates no machines can long survive the disastrous corrosive effects of moisture, vegetable growths, etc., whereas printed matter is hardly affected by these elements. Finally, under field conditions, while a code book can be manipulated outdoors in all sorts of weather, in rain, sleet, or snow, in high altitudes where the temperature is very low, or in the tropics where it is very hot and humid, a cipher machine, especially if electrical, often cannot be operated with success for more than a few minutes or, at most, a few hours.

REF ID:A56932

CHAPTER 12
CODE SYSTEMS

Section I. GENERAL

153. General

a. Chapter 4 was devoted to a general consideration of code systems and enciphered code. It was there indicated that code systems are systems of substitution where the elements of the substitutive process, comprising letters, syllables, words, phrases, and sentences, are so numerous that it is impossible to memorize them or to reconstruct them at will when necessary, so that printed books containing these elements and their code equivalents must be at hand in order to cryptograph or decryptograph messages. The various types of code groups were indicated, together with methods for their construction by means of permutation tables. One-part and two-part codes were briefly discussed. Finally, a few words were added for the purpose of indicating various types of enciphering code for greater cryptographic security.

b. Practical cryptography must take cognizance of the fact that the texts of governmental as well as commercial and social telegrams must conform to certain standard forms and practices. A subsequent text will go into these matters but at this moment it is only necessary to indicate that international telegraph regulations in the past have exercised an important influence upon the structure of code groups and upon the selection of cryptographic systems for their encipherment.

c. In the subsequent paragraphs, when reference is made to ***numerical code groups,*** or ***number-code groups,*** or ***figure-code groups,*** it will be understood that the code groups are composed of digits; when reference is made to ***alphabetical code groups,*** or ***letter-code groups,*** or ***letter groups,*** it will be understood that the code groups are composed of letters of the alphabet; and when reference is made to ***mixed code groups,*** or ***mixed groups,*** it will be understood that the code groups are composed of intermixtures of letters and digits.

154. Intermixtures of Code-Text and Other Kinds of Text

a. Only in commercial code messages is the practice of mixing plain text and code text common in modern communications. In governmental code messages, military, naval, or diplomatic, such intermixtures are today so rare that their presence in telegrams indicates abysmal ignorance

REF ID:A56932

of some of the fundamental rules of cryptographic security. Because the plain-text words give definite clues to the meaning of the adjacent code groups, even though the former may apparently convey no intelligibility in themselves (such words as *and, but, by, comma, for, in, period, stop, that, the,* etc.), their presence constitutes a fatal danger, and no cryptographer who is aware of this danger will countenance such intermixtures.

b. It often happens that correspondents employ a code which makes no provision for encoding proper names or unusual words not included in the vocabulary of the code book. Rather than leave the unencodable text in plain language in the message, *since its appearance will surely lead to clues to unauthorized reading of the message,* the correspondents encipher such words and proper names by means of any prearranged cipher system. Also, in some cases, when the code is limited in its vocabulary and the various inflections of words are not represented, the correspondents may suffix the proper inflections ("ed," "ing," "tion," etc.) in cipher. This procedure, however, is not to be recommended, because it considerably reduces the cryptographic security of the whole system.

c. Sometimes correspondents make use of two or more codes within the same message. This is occasionally the case when they are making use of a general or commercial code which does not have all the special expressions necessary for their business, the latter expressions being contained in a small private code. Sometimes, however, the intermixture of code text from several codes is done for the purposes of secrecy, though it is, as a rule, a rather poor subterfuge.

Section II. ENCIPHERED CODE

155. General

a. The purposes of enciphering code have already been explained together with brief indications of methods. The superimposition of a good cipher system upon the code text of a message is a safe and practical method of cryptography for governmental use, where more rapid machine methods are not available.

b. In the subsequent paragraphs, for brevity and ease in reference, the term *placode*[12] will be employed to designate the actual or unenciphered code groups representing the plain-text elements; the term is derived by telescoping the words *plain* and *code.* On the other hand, the term *encicode*[12] will be employed to designate the final product of the superencipherment; it is likewise derived by telescoping the words *enciphered* and *code.*

[12] Pronounced "play-code" and "en-sigh'-code."

REF ID:A56932

c. The terms *superenciphered code, superencipherment,* or (British) *reciphered code* and *recipherment* all apply to code text which undergoes a subsequent process of encipherment.

d. The terms *indicator system* and *indicator* are very important in connection with all cryptographic procedures but especially so in connection with enciphering systems as applied to code. The indicator gives information relative to the proper tables to use, or the proper point to begin in such tables, etc. Further information in this regard will be given in subsequent paragraphs.

156. General Types of Methods of Superencipherment

Both transposition and substitution methods may be applied to superencipher code. There are arithmetical methods which at first glance appear to constitute a third category of superencipherment methods since they involve mathematical processes apparently resembling neither transposition nor substitution. However, deeper study will lead to the conclusion that these arithmetical methods are substitutive in character.

157. Transposition Methods

a. Transposition methods wherein whole code groups or series of them are shifted about according to some key are not frequently encountered. Transposition methods applied strictly within the code groups, by rearrainging or shifting about the letters or figures composing them, have been used to a limited extent for a number of years. Prior to January 1, 1934, transposition processes for producing encicode messages, that is, for superenciphering code, were practically never employed in commercial or governmental practice because they destroyed the regular vowel-consonant structure of code groups so that they no longer conformed to the requirements of the international telegraph regulations referred to in paragraph 153*b*. However, the restrictions in this respect were lifted on the date indicated and it may be expected that transposition processes for superenciphering code will be encountered much more frequently than in the past.

b. One of the most commonly used transposition methods for this purpose is simple keyed-columnar transposition, either with special matrices, designs, or forms having nulls and blanks, or without these features. The system as a whole, however, is very subject to error and requires high-grade personnel for its practical operation. It is, of course, wholly unsuited for practical military usage, though it can be employed for other purposes. Solution of such a system if well constructed is a very difficult matter, especially if the basic code book is not known,

REF ID:A56932

158. Substitution Methods

a. GENERAL. All of the methods of substitution applicable in the case of cipher systems are available for use in superenciphering code.

b. MONOALPHABETIC METHODS. It is, of course, easy to draw up one or more single-mixed alphabets. When the code book is in possession of the enemy cryptanalysts and the original or placode groups are therefore at hand, this method does not yield any security, for reasons not necessary here to indicate. Even when the actual code book is not known, but it is known that it is one of a set of commerical codes having groups of the 2-letter difference type, the reconstruction of the cipher alphabets is not difficult.

c. POLYALPHABETIC METHODS.

(1) A very simple polyalphabetic method is to have 5 alphabets which are used in succession; or there may be a series of sets of 5 alphabets, the individual set to be used being determined by indicators inserted in the message itself.

(2) Any sort of polyalphabetic method may be used. For example, the repeating-key method, the running or continuous-key method, the interrupted-key method, etc., can be applied. Digraphic methods may also be used; also, combinations of digraphic and monographic methods are frequent.

(3) Tables of various sorts are often employed. For example, using a table applicable to code groups of 5 figures, a table giving pronounceable combinations of letters for the combinations of digits may result in converting a group such as 75152 into the letter group KOBAL. Tables for substituting combinations of letters into other combinations of letters are, of course, equally feasible. The substitution may be strictly digraphic, combining two 5-letter or 5-figure groups into a series of 10 digraphs; or it may be a combination of trigraphic and digraphic substitution, each 5-character group being split up into a 3-character and a 2-character combination. Other combinations are, of course, also possible.

(4) In all the foregoing methods the chief objection is that the advantage of the 2-letter differential feature is more or less dissipated by the encipherment, but this is true of every substitutive method that is superimposed on code.

(5) The disadvantage referred to in the preceding subparagraph is absent in those cases in which the encipherment operates merely to substitute other code groups of the same book for the message code groups. The most common methods of this type make use of the figure-code groups, the latter being manipulated in various ways to change them and the resulting groups then

REF ID:A56932

being given their letter-code equivalents. Some of these methods are explained below.

159. Arithmetical Methods

These are the most important of the various methods of superenciphering code, and must be dealt with in somewhat greater detail than the foregoing methods. There are several different types of treatment, each of which will be briefly discussed in the subsequent subparagraphs.

160. Single or Fixed Additives

a. If the code groups are numerical, the addition of an arbitrarily selected number to each code group in the code message constitutes a simple form of superencipherment. It may be varied by prearrangement between correspondents, simply by changing the fixed number as frequently as may be deemed necessary, or by some easily arranged system of change. The group of digits composing the number which is added to the placode values is commonly termed an *additive group*, or, more often, an *additive*, or sometimes simply an *adder*. In decipherment, the additive is merely removed from the received encicode groups by subtraction, leaving the placode groups, which can then be decoded by reference to the code book. Often the date or some number derivable from the date is employed as the additive but usually the number is simply an arbitrarily composed group of digits. Because the same number is employed throughout the encipherment of the entire code message, such an additive is called a *fixed additive*.

b. Methods such as the foregoing are particularly weak cryptographically if the basic code book and the code groups embody limitations in construction. For example, should it be employed in connection with a code having only 3,000 groups numbered consecutively from 0000 to 2999, then the initial digits of the groups are limited to the three digits 0, 1, and 2; the application of a fixed additive can therefore produce only three different digits as the initial digits of the encicode text. This phenomenon would, of course, soon lead to the determination of the initial digits of the placode groups.

c. One rather simple scheme involving the use of fixed additives in the case of codes having alphabetical as well as numerical code groups is to apply the fixed additive to the numerical code groups representing the plain-text words or phrases and then take the alphabetical code groups corresponding to the sums as the final encicode groups. In codes of this type the additives may be rather large numbers and the process of finding the alphabetical code groups corresponding to the sums is very easy. But in codes wherein only alphabetical code groups are listed, that is, no figure-code or numerical groups are also given, the additives employed must naturally be rather small numbers. It would be extremely

REF ID:A56932

laborious to count 573 groups forward, for example. In cases such as these additives limited to numbers from 1 to 20 or 30 are common.

d. (1) Instead of *adding* a fixed number in encipherment, the latter may be subtracted, in which case, in decipherment, the fixed number must be added to the encicode groups as received. Such a group may be termed a *subtractive group,* or *subtractor,* because subtraction is the process used in encipherment; in decipherment the group becomes, of course, an additive.

(2) Addition and subtraction of a fixed numerical group may be alternated within the same message, according to some simple subsidiary key; for example, a series of additive groups corresponding to the keyword BAD might, by prearrangement, consist of the numbers 200, 100, 400. These might be used in repetitive manner. Or the correspondents might agree to use these key numbers alternatively in additive and subtractive manner, such as +200, −100, +400, −200, +100, −400, +200, −100, etc.

e. Addition without "carrying," or *noncarrying addition,* is just as simple as *normal addition,* that is, addition with "carrying"; and subtraction without "borrowing," or *nonborrowing subtraction,* is just as simple as *normal subtraction,* that is, subtraction with "borrowing." It is merely necessary that the correspondents agree in advance on this point and apply the process consistently throughout a message. In practice, however, it is more common to perform these processes without "carrying" or "borrowing," *so that the operations can be performed from left to right as in normal writing.* Following is an example which will make the matter clear.

Example A

(a) Example of *"noncarrying" addition* in encipherment:

(1) Placode	5517	3082	9015	6710	9541
(2) Fixed group for addition	5678	5678	5678	5678	5678
(3) Encicode	0185	8650	4683	1388	4119

(b) In decipherment, *"nonborrowing" subtraction* is applied:

(1) Encicode	0185	8650	4683	1388	4119
(2) Fixed group for subtraction	5678	5678	5678	5678	5678
(3) Placode	5517	3082	9015	6710	9541

(c) Note that in the *decipherment* process the *encicode* serves as the *minuend,* the additive used in the encipherment serves as the *subtrahend,* and the placode is the *remainder.*

f. In the foregoing example the additive remains the same throughout the superencipherment but it is obvious that this is only the simplest sort of an arrangement. A *series of different additives* may readily be employed, as will be explained later.

REF ID:A56932

g. (1) *Cryptographic procedure.* It is, however, possible to make the cryptographic procedure the same in both encipherment and decipherment, by proper changes in method. *They can both be made either additive or subtractive in nature, thus requiring the learning of but a single process.* Two methods will be explained below.

(2) *Both processes additive.* If in encipherment an additive process is used, and if in decipherment the *complement* of the additive employed in encipherment is then *added* to the encicode groups, the decipherment also becomes an additive process. For example, the complement of the group 5678, on a basis of 10, is 5432. Note the following:

Example B

(a) Example of "noncarrying" addition in encipherment:

(1) Placode	5517	3082	9015	6710	9541
(2) Fixed group for addition	5678	5678	5678	5678	5678
(3) Encicode	0185	8650	4683	1388	4119

(b) In decipherment, using the complement of the additive used in encipherment, *addition* reproduces the placode:

(1) Encicode	0185	8650	4683	1388	4119
(2) Complement of fixed group	5432	5432	5432	5432	5432
(3) Placode	5517	3082	9015	6710	9541

(3) *Both processes subtractive.* By a very simple change in procedure it is possible to apply subtraction in *both* encipherment and decipherment, using the *same* numerical groups as *subtractors,* thus making it necessary to learn only one process. If the additive, instead of being in the second line of the three lines shown in the foregoing examples, is placed on the first line, and a subtraction process applied, the proper results are obtained *regardless of whether encipherment or decipherment is involved.* Note the following example:

Example C

(a) Example of "nonborrowing" subtraction in encipherment and decipherment:

(1) Fixed group	5678	5678	5678	5678	5678
(2) Placode	5517	3082	9015	6710	9541
(3) Encicode	0161	2696	6663	9968	6137

(b) Decipherment (*subtraction also*):

(1) Fixed group	5678	5678	5678	5678	5678
(2) Encicode	0161	2696	6663	9968	6137
(3) Placode	5517	3082	9015	6710	9541

REF ID:A56932

(c) Note that in the *encipherment* process the keying group serves as the *minuend*, the *placode* as the *subtrahend*, whereupon the *remainder* becomes the *encicode;* in the *decipherment* process the keying group again serves as the *minuend*, the *encicode* as the *subtrahend*, whereupon the *remainder* becomes the *placode*.

(4) *Explanation.* The explanation involves a consideration of the nature of the processes themselves when looked at from the point of view of simple algebra. Note the following, where the symble x denotes placode, y denotes the fixed group, and z denotes encicode:

In example A (a)..... $x+y=z$
Transposing..... $x=z-y$
That is..... $z-y=x$

It is seen here that y must be *subtracted* from z in order to recover x and in order that x may be a positive quantity. Thus, this method involves both addition and subtraction.

But in example C (a)..... $y-x=z$
Transposing..... $y-z=x$,

which is exactly what is done in Example C (b). Hence it is seen that in the case of this second method only subtraction is involved, *in both processes.*

h. The method illustrated in Example C is becoming more common, because of its simplicity and ease in manipulation. It is termed the *subtractor method* and the numerical groups employed as keying groups are called *subtractors.* In paragraph 162 more will be said about this method.

161. Repeating or Recurring-Key Additives and Subtractors

a. In the foregoing examples the number which was added or subtracted in encipherment was always the same but this need not, of course, be true. It is possible to employ a *sequence* of numbers for addition or subtraction, the sequence being agreed upon in advance or it may be easily derivable from a key phrase, etc. Thus, suppose the placode message is the same as in the previous examples and that the repeating key is 432809721 and that this key is employed according to the subtractor method explained in paragraph 160*g* (3). Note the following:

(a) Encipherment:

(1) Repeating key.....	4328	0972	1432	8097	2143
(2) Placode.....	5517	3082	9015	6710	9541
(3) Encicode.....	9811	7990	2427	2387	3602

(b) Decipherment:

(1) Repeating key.....	4328	0972	1432	8097	2143
(2) Encicode.....	9811	7990	2427	2387	3602
(3) Placode.....	5517	3082	9015	6710	9541

REF ID:A56932

b. It is important to note that such a key as the foregoing must be of a length that does not contain a factor in common with the length of the code groups involved in the encipherment, for if it does contain a common factor the period will be abbreviated. For example, in the foregoing case, since the repeating key contains 9 digits and the code groups 4 digits, the length of the enciphering period is 9 groups, that is, two identical placode groups must be at least 9 groups apart before they will produce identical encicode groups. But if the keying sequence were 10 digits in length this phenomenon of cyclic repetition could happen if the identical placode groups were but 5 groups apart, since the common factor 2 cuts the potential keying length in half; and if the keying sequence were 12 digits in length the period would be but 3 groups. In this connection see also paragraph 131 *c.*

162. Nonrepeating Additives and Subtractors

a. When special tables are employed as the source of the adders or subtractors for superenciphering code, a much more secure system is provided. The tables may be contained in a book or document called a *keybook,* an *additive book,* or a *subtractor book.* On each page of such a book groups of numbers are regularly disposed in rows and columns on the page. By applying identifying symbols called *indicators* to the pages, as well as to the rows and the columns on each page of the keybook, it is possible to provide for the safe superencipherment of a large volume of traffic. All correspondents must, of course, be provided with the same basic code book and the same keybook. In employing the keybook the *indicators* tell the recipient of a message what groups were used; that is, where to begin in the decipherment of the encicode. A page from a typical keybook of this sort is shown in figure 72.

b. It should be noted that whether the arbitrary numerical groups in the keybook are employed as *adders* or as *subtractors* has nothing to do with the nature of the groups themselves: the latter may be used either way, provided consistency is observed and the correspondents agree as to whether the groups will be employed throughout the messages in the additive manner (in encipherment) illustrated in Example A (a) in paragraph 160*e,* or in the subtractor manner illustrated in Example C (a), in paragraph 160*g.* In figure 72 are shown two sets of 100 4-digit groups, disposed in numbered blocks each containing 10 columns and 10 rows of groups. To designate a group as the initial one to be employed in encipherment, or decipherment, it is merely necessary to give the block number, the row number and the column number of the group. For example, 0116 is the indicator for the group 8790. It is usual to take the successive groups in the normal order of reading, that is, from left to right and from the top downwards, although any other order of reading may be agreed upon between correspondents. The book from which this

REF ID:A56932

BLOCK 00

	1	2	3	4	5	6	7	8	9	0
1	0378	9197	3260	3607	2699	9053	9733	1844	6622	4213
2	7185	0135	6091	2387	4957	3113	7284	0750	3501	1945
3	5037	3365	1294	8261	2149	0718	3678	2510	7238	5268
4	8004	5199	3859	1293	5311	3550	9915	0512	1518	3776
5	9282	6893	4229	9736	0927	1418	1930	9864	0090	8974
6	7259	9399	0769	3144	9801	1378	4732	5134	1435	5282
7	2878	9963	7943	4519	3404	9810	0190	4467	7069	5348
8	1620	5879	0218	1064	9560	5732	6661	0883	1883	2619
9	3868	1905	2500	6654	0824	3710	3875	6332	1503	7259
0	4319	3298	7819	8721	1549	6630	6301	5701	3586	1907

BLOCK 01

	1	2	3	4	5	6	7	8	9	0
1	9328	1135	3871	1549	0839	8790	1771	8251	3274	1173
2	2297	9550	5033	0102	6817	5597	0847	4038	1200	2949
3	3640	3984	3299	1181	3811	8844	2500	4557	4133	0487
4	1456	9614	5520	8372	1941	2417	1098	4039	3943	8282
5	1751	4254	8479	8647	2684	5511	8680	4660	3858	4266
6	3643	0445	4673	6178	5250	4310	9580	0481	1005	4100
7	5875	0710	7652	5415	6851	6001	9668	2109	8471	3276
8	4555	9772	0128	2171	6835	3142	9514	1478	9746	7625
9	0183	2959	3757	7481	4398	4586	8143	8049	7478	8417
0	5072	4405	4128	9068	5023	4374	7741	6373	9454	7733

Figure 72.

REF ID:A56932

example was taken consisted of 50 pages each containing 200 groups, making 10,000 in all. The groups themselves, of course, consist merely of digits selected *at random* when the keybook is in preparation.

c. Referring back to the method illustrated in Example B in paragraph 160*g* (2), in which addition is employed in both encipherment and decipherment, it was noted that in decipherment the *complement* of the additive employed in encipherment must be used in order to recover the placode. This principle serves as the basis for preparing keybooks in which half the contents are additives, the other half, their complements. By proper manipulation of indicators it is possible to use any given page of the arbitrary groups for encipherment, whereupon a specific page (containing the complements) must be used for decipherment. This method obviously requires considerable care in preparing the keybooks, so as to insure that complementary pages are present and are properly indicated; it also involves much more care to insure that the groups on complementary pages are accurate, although there are mechanical methods of preparing series of complements of this type.

d. If a keybook for an additive or a subtractor system is used *once and only once,* security of an absolute order is imparted to the messages *even if the basic code book is known to and possessed by the enemy.* It is not even necessary to use indicators except where a question may arise as to the serial order of one of two or more messages arriving at about the same time. In such a case the system is referred to as a *one-time system* and the keybook is called a *one-time pad* because the pages are usually fastened securely in the form of a tablet or pad and are destroyed as soon as it is certain that the recipient of a message has properly deciphered and decoded it. The disadvantages of such a system are two in number, both very serious. In the first place the production and distribution of the pads present very difficult problems in composition, printing, assembly of sheets, etc. For voluminous correspondence many pads are necessary and the mere question of the production, timely distribution, and proper safekeeping of the pads is a serious one. In the second place, a system such as this is suitable for *only two correspondents* and even in this case there usually must be two pads, one for incoming, the other for outgoing messages, otherwise it will occasionally or frequently happen that both correspondents will use the same series of additives or subtractors.

e. The foregoing difficulties make it desirable to modify the system so that while its security may not be absolute it can be employed by a larger number of correspondents, cutting down on the number of pads required and permitting of intercommunication among all correspondents. For such use, indicators are absolutely essential in order to facilitate the prompt decipherment of messages received from several different correspondents.

REF ID:A56932

f. The security of a scheme such as the foregoing is dependent upon the manner in which the indicators are treated in the cryptographing processes. If the indicators are given *in clear,* that is, without disguise of one sort or another, it becomes possible to study a series of encicode messages and perhaps to solve them, even without possession of the code. On the other hand, if the indicators are themselves disguised by enciphering them according to a well-designed method, the system as a whole becomes very secure and may, indeed, be made impregnable against attack for a very long time.

163. Observations on Arithmetical Methods

a. It can be perceived by this time that the foregoing arithmetical methods are, in reality, substitution methods. Where a fixed group is added or subtracted from the placode group this is easy to see. For example, if the fixed additive is 3089 and the placode group is 8752, the encicode group is 1731. This is the same as saying that a 4-alphabet system is involved, and the alphabets are as follows:

Placode.....		1	2	3	4	5	6	7	8	9	0	
Alphabet No.	1	4	5	6	7	8	9	0	1	2	3	"Cipher"
	2	1	2	3	4	5	6	7	8	9	0	
	3	9	0	1	2	3	4	5	6	7	8	
	4	0	1	2	3	4	5	6	7	8	9	

Note that merely a simple cyclic displacement of values is involved in the process, the amount of displacement being governed by the particular digit in each position of the additive group. What this amounts to, in cryptographic terms, is a four-alphabet encipherment using direct standard alphabets, where the "normal alphabet" is 1 2 3 4 5 6 7 8 9 0. The process could be made more difficult by employing "mixed alphabets" of course, but then the feature of speed, which is now possible (in view of early training in addition, whereby the mental arithmetic involved becomes second nature), would be lost, since constant reference would have to be made to enciphering and deciphering tables.

b. It becomes clear that when a series of different additives or subtractors is used, as when a keybook is employed, then the number of alphabets involved corresponds to the number of digits employed. Thus, despite the fact that the encipherment process is here one that involves merely the numerical equivalents of direct standard alphabets, the system can have great cryptographic security, depending upon (1) how long the keying sequence is, that is, the number of groups comprising the additive or subtractor series; (2) the composition of this keying sequence, that is, whether it consists of random digits or is systematic in its construction; and (3) whether this sequence or parts of it are used only once or several times. The last-mentioned factor is the most

REF ID:A56932

important of the three, for if the keying sequence or parts of it are used but once or a very limited number of times, say 2 or 3, its recovery by cryptanalytic processes is difficult or impossible and therefore even if the sequence is systematic in its construction this fact might not become known. However, as a rule the additives or subtractors are merely digits selected by a purely random means, such as drawing them out of a box, or equivalent means. The length of the sequence is guided only by the amount of traffic to be superenciphered; for a voluminous traffic, keybooks containing thousands of groups are necessary, even with a good indicator system, and even then the books must be changed at frequent intervals.

c. Arithmetical methods are favored above most other methods of superencipherment because of their simplicity and relatively better speed of operation than in the case of alphabetical methods. The speed factor is, of course, attributable to the fact that practically everybody can add (or subtract) rapidly and accurately when single digits are involved, and although very similar processes could be applied in cryptographic processes involving letters of the alphabet, the operations of addition or subtraction would proceed very much more slowly because early training does not devote any time to arithmetical processes involving letters. For example, every child learns that "8 plus 5 equals 13" but none learns that "H plus E equals M."

d. However, these arithmetical methods have two serious disadvantages. First, there is the disadvantage that the final encicode text is composed of numbers. The latter are not only more subject to errors in telegraphic handling than are letters, but also it is more difficult to correct garbled groups when figures are involved than when letters are involved. These disadvantages are, it must be admitted, more serious in American practice, when emphasis in training is laid upon the telegraphic transmission of letters and not figures, than they are in other practices; they may not hold in regard to countries where the emphasis in training is in the other direction, figures being preferred to letters. Second, the physical procedures involved in the preparation, reproduction, distribution, and accounting of the necessary keybooks of adders or subtractors are tedious, costly, and time consuming. Where provision must be made for voluminous intercommunication among many units and for relatively long periods of time, these matters constitute a difficult if not impossible problem for the compiling agency.

☆ U. S. GOVERNMENT PRINTING OFFICE: 1950—874180

ATP 2-22.9

Open-Source Intelligence

July 2012

DISTRIBUTION RESTRICTION: Unlimited Distribution

Headquarters, Department of the Army

***ATP 2-22.9**

Army Techniques Publication
No. 2-22.9 (FMI 2-22.9)

Headquarters
Department of the Army
Washington, DC, 10 July 2012

Open-Source Intelligence

Contents

		Page
	PREFACE	**iv**
	INTRODUCTION	**v**
Chapter 1	**OPEN-SOURCE INTELLIGENCE (OSINT) FUNDAMENTALS**	**1-1**
	Definition and Terms	1-1
	Characteristics	1-1
	The Intelligence Warfighting Function	1-2
	The Intelligence Process	1-3
	The Planning Requirements and Assessing Collection Process	1-4
	The Military Decisionmaking Process	1-4
	Intelligence Preparation of the Battlefield	1-5
Chapter 2	**PLANNING AND PREPARATION OF THE OSINT MISSION**	**2-1**
	Section I – Planning OSINT Activities	**2-1**
	Define the Operational Environment	2-1
	Describe Environmental Effects on Operations	2-2
	Evaluate the Threat	2-2
	Determine Threat Courses of Action	2-2
	Section II – Preparation of OSINT Activities	**2-2**
	OSINT Exploitation	2-3
	Preparation Considerations	2-4
	Section III – Planning and Preparation Considerations	**2-7**
	Open-Source Reliability	2-7
	Open-Source Information Content Credibility	2-8
	Compliance	2-8

DISTRIBUTION RESTRICTION: Unlimited Distribution

.

*This publication supersedes FMI 2-22.9, 5 December 2006.

Operations Security 2-8
Classification 2-9
Coordination 2-9
Deception and Bias 2-9
Copyright and Intellectual Property 2-9
Linguist Requirements 2-10
Machine Foreign Language Translation Systems 2-11
Section IV – Manning the OSINT Section 2-13
OSINT Section Duties 2-13
OSINT Section at the Brigade Combat Team Level 2-13
Task Organization Considerations 2-15

Chapter 3 COLLECTING OSINT 3-1
Collecting Publicly Available Information 3-1
Research 3-3

Chapter 4 PRODUCING OSINT 4-1
Categories of Intelligence Products 4-1
Evaluate Information 4-2
Process Information 4-5
Report and Disseminate Information 4-10
Reporting and Dissemination Considerations 4-12

Appendix A LEGAL RESTRICTIONS AND REGULATORY LIMITATIONS A-1

Appendix B CYBERSPACE INTERNET AWARENESS B-1

Appendix C BASIC AND ADVANCED INTERNET SEARCH TECHNIQUES C-1

Appendix D OSINT CONTRIBUTIONS D-1

Appendix E OSINT ORGANIZATIONS E-4

Appendix F OPEN-SOURCE RESOURCES 1

GLOSSARY Glossary-1

REFERENCES References-1

INDEX Index-1

Figures

Figure 1-1. The intelligence process 1-3
Figure 2-1. Brigade combat team's OSINT section 2-14
Figure 3-1. Process for collecting publicly available information 3-2

Tables

Table 2-1. Open-source reliability ratings 2-8
Table 2-2. Open-source content credibility ratings 2-8
Table 3-1. Open-source media, components, and elements 3-5
Table 4-1. Categories of intelligence products 4-1
Table 4-2. Comparison of communication types 4-3
Table 4-3. Level, factors, and elements of media control 4-7
Table 4-4. Hierarchy of media power 4-8
Table C-1. Boolean logic operators, connectors, and delimiters C-3
Table C-2. Truncating and shortening uniform resource locators C-6
Table E-1. Open Source Academy curriculum E-5
Table F-1. Military open-source training and resources 1

Preface

ATP 2-22.9 establishes a common understanding, foundational concepts, and methods of use for Army open-source intelligence (OSINT). ATP 2-22.9 highlights the characterization of OSINT as an intelligence discipline, its interrelationship with other intelligence disciplines, and its applicability to unified land operations.

This Army techniques publication—

- Provides fundamental principles and terminology for Army units that conduct OSINT exploitation.
- Discusses tactics, techniques, and procedures (TTP) for Army units that conduct OSINT exploitation.
- Provides a catalyst for renewing and emphasizing Army awareness of the value of publicly available information and open sources.
- Establishes a common understanding of OSINT.
- Develops systematic approaches to plan, prepare, collect, and produce intelligence from publicly available information from open sources.

The target audience for this Army techniques publication is Army units at the division level and below conducting OSINT exploitation.

Defined terms are identified in the text. Definitions for which this publication is the proponent are printed in boldface. These terms and their definitions will be incorporated into the next revision of FM 1-02. For other definitions in the text, the term is italicized, and the number of the proponent publication follows the definition. Terms for which this publication is the proponent are indicated with an asterisk in the glossary.

"OSINT personnel" applies to intelligence and nonintelligence Active Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve personnel who engage in missions involving publicly available information and open sources.

AR 381-10 defines a *U.S. person* as—

- A U.S. citizen.
- A U.S. permanent resident alien.
- An unincorporated association substantially composed of U.S. citizens or permanent resident aliens.
- A corporation or subsidiary incorporated in the United States that is not directed or controlled by a foreign government.

The following are presumed to be *non-U.S. persons*:

- A person or organization outside of the United States.
- A person not a citizen or permanent resident alien of the United States.

The use or mention of the name of any commercial or private organization or its associated trademark or services by the Army does not express or imply an endorsement of the sponsor or its products and services by the Army.

This publication applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve unless otherwise stated.

Headquarters, U.S. Army Training and Doctrine Command, is the proponent for this publication. The preparing agency is the U.S. Army Intelligence Center of Excellence (USAICoE), Fort Huachuca, AZ. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: Commander, USAICoE, ATTN: ATZS-CDI-D (ATP 2-22.9), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017.

Introduction

Since before the advent of the satellite and other advanced technological means of gathering information, military professionals have planned, prepared, collected, and produced intelligence from publicly available information and open sources to gain knowledge and understanding of foreign lands, peoples, potential threats, and armies.

Open sources possess much of the information needed to understand the physical and human factors of the operational environment of unified land operations. Physical and human factors of a given operational environment can be addressed utilizing publicly available information to satisfy information and intelligence requirements and provide increased situational awareness interrelated with the application of technical or classified resources.

The world is being reinvented by open sources. Publicly available information can be used by a variety of individuals to expand a broad spectrum of objectives. The significance and relevance of open-source intelligence (OSINT) serve as an economy of force, provide an additional leverage capability, and cue technical or classified assets to refine and validate both information and intelligence.

As an intelligence discipline, OSINT is judged by its contribution to the intelligence warfighting function in support of other warfighting functions and unified land operations.

Chapter 1

Open-Source Intelligence (OSINT) Fundamentals

Pioneer and reformative directives led to the passing of legislation that affected the U.S. intelligence community and its application of publicly available information. The National Security Act of 1992 began the reformation of the U.S. intelligence community resulting in the establishment of the Open Source Office and subsequently the Director of National Intelligence (DNI) Open Source Center (OSC) in 2005. This chapter describes the fundamentals of open-source intelligence (OSINT).

DEFINITION AND TERMS

1-1. *Open-source intelligence* is the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement (FM 2-0). OSINT also applies to the intelligence produced by that discipline.

1-2. OSINT is also intelligence developed from the overt collection and analysis of publicly available and open-source information not under the direct control of the U.S. Government. OSINT is derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to intelligence requirements. Two important related terms are open source and publicly available information:

- **Open source** is any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure. Open-source information can be publicly available but not all publicly available information is open source. Open sources refer to publicly available information medium and are not limited to physical persons.
- **Publicly available information** is data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

***Note*.** All OSINT operations conducted by intelligence personnel must comply with the legal restrictions as outlined in Executive Order (EO) 12333, DOD 5240.1-R, DODD 3115.12, JP 2-0, and AR 381-10.

1-3. OSINT collection is normally accomplished through monitoring, data-mining, and research. Open-source production supports all-source intelligence and the continuing activities of the intelligence process (generate intelligence knowledge, analyze, assess, and disseminate), as prescribed in FM 2-0. Like other intelligence disciplines, OSINT is developed based on the commander's intelligence requirements.

CHARACTERISTICS

1-4. The following characteristics address the role of OSINT in unified land operations:

- **Provides the foundation.** Open-source information provides the majority of the necessary background information on any area of operations (AO). This foundation is obtained through

open-source media components that provide worldview awareness of international events and perceptions of non-U.S. societies. This foundation is an essential part of the continuing activity of *generate intelligence knowledge*.

- **Answers requirements.** The availability, depth, and range of publicly available information enables organizations to satisfy intelligence and information requirements without the use or support of specialized human or technical means of collection.
- **Enhances collection.** Open-source research supports surveillance and reconnaissance activities by answering intelligence and information requirements. It also provides information (such as biographies, cultural information, geospatial information, and technical data) that enhances and uses more technical means of collection.
- **Enhances production.** As part of a multidiscipline intelligence effort, the use and integration of publicly available information and open sources ensure commanders have the benefit of all sources of available information to make informative decisions.

THE INTELLIGENCE WARFIGHTING FUNCTION

1-5. The intelligence warfighting function is composed of four distinct Army tactical tasks (ARTs):

- Intelligence support to force generation (ART 2.1).
- Support to situational understanding (ART 2.2).
- Perform intelligence, surveillance, and reconnaissance (ART 2.3).
- Support to targeting and information superiority (ART 2.4).

1-6. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding of the operational environment, enemy, terrain, weather, and civil considerations (FM 1-02). As a continuous process, the intelligence warfighting function involves analyzing information from all sources and conducting operations to develop the situation. OSINT supports each of these ARTs.

1-7. Publicly available information is used to—

- Support situational understanding of the threat and operational environment.
- Obtain information about threat characteristics, terrain, weather, and civil considerations.
- Generate intelligence knowledge before receipt of mission to provide relevant knowledge of the operational environment.
- Rapidly provide succinct answers to satisfy the commander's intelligence requirements during intelligence overwatch.
- Develop a baseline of knowledge and understanding concerning potential threat actions or intentions within specific operational environments in support of the commander's ongoing intelligence requirements.
- Generate intelligence knowledge as the basis for Army integrating functions such as intelligence preparation of the battlefield (IPB). IPB is designed to support the staff estimate and the military decisionmaking process (MDMP). Most intelligence requirements are generated as a result of the IPB process and its interrelation with MDMP.
- Support situation development—a process for analyzing information and producing current intelligence concerning portions of the mission variables of enemy, terrain and weather, and civil considerations within the AO before and during operations (see FM 2-0). Situation development—
  - Assists the G-2/S-2 in determining threat intentions and objectives.
  - Confirms or denies courses of action (COAs).
  - Provides an estimate of threat combat effectiveness.
- Support information collection. Planning requirements and assessing collection analyzes information requirements and intelligence gaps and assists in determining which asset or combination of assets are to be used to satisfy the requirements.

1-8. For more detailed information on the intelligence warfighting function, see FM 2-0. For examples of how OSINT is used to support other intelligence disciplines and operational tasks, see appendix D.

THE INTELLIGENCE PROCESS

1-9. The intelligence process consists of four steps (plan, prepare, collect, and produce) and four continuing activities (analyze, generate intelligence knowledge, assess, and disseminate). Just as the activities of the operations process (plan, prepare, execute, and assess) overlap and recur as the mission demands, so do the steps of the intelligence process. The continuing activities occur continuously throughout the intelligence process and are guided by the commander's input.

1-10. The four continuing activities plus the commander's input drive, shape, and develop the intelligence process. The intelligence process provides a common model for intelligence professionals to use to guide their thoughts, discussions, plans, and assessments. The intelligence process results in knowledge and products about the threat, terrain and weather, and civil considerations.

1-11. OSINT enhances and supports the intelligence process and enables the operations process, as described in FM 2-0. The intelligence process enables the systematic execution of Army OSINT exploitation, as well as the integration with various organizations (such as joint, interagency, intergovernmental, and multinational). Figure 1-1 illustrates the intelligence process. (For more information on the intelligence process, see FM 2-0.)

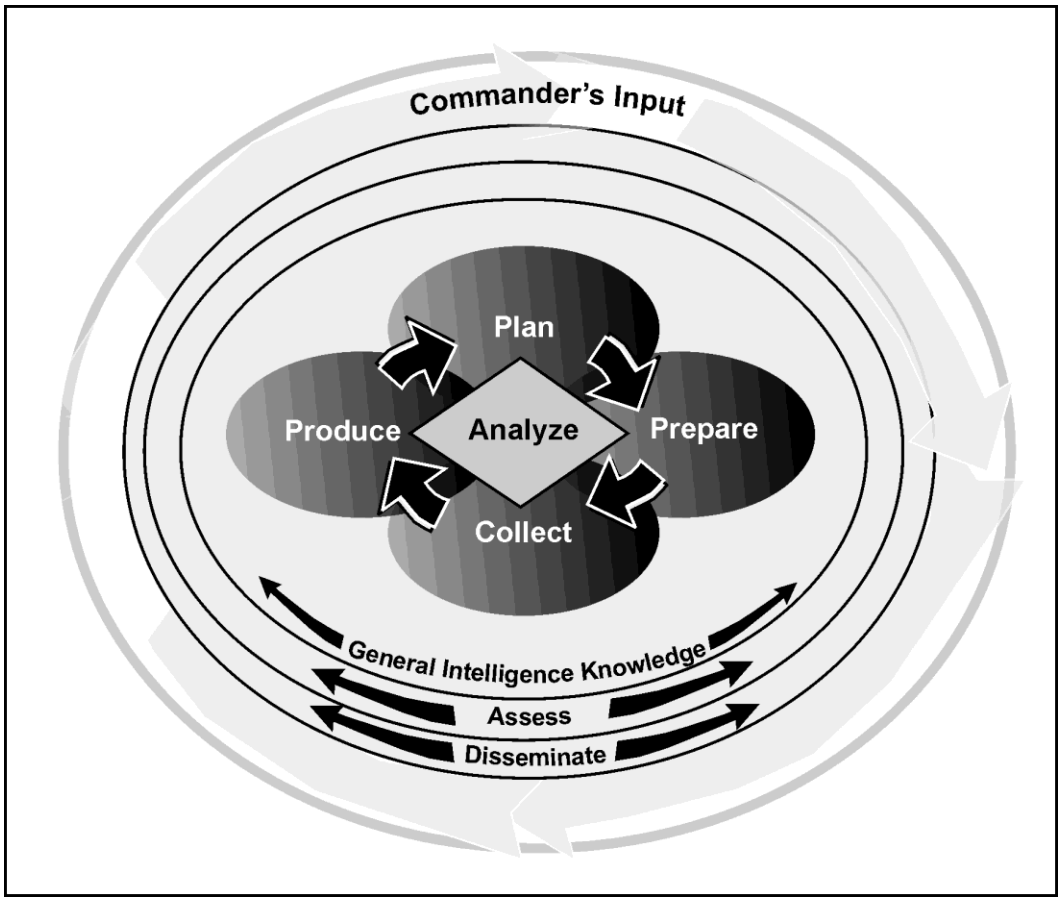


Figure 1-1. The intelligence process

THE PLANNING REQUIREMENTS AND ASSESSING COLLECTION PROCESS

1-12. Information collection informs decisionmaking for the commander and enables the application of combat power and assessment of its effects. *Information collection* is an activity that synchronizes and integrates the planning and operation of sensors, assets, as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations (FM 3-55). This is an integrated intelligence and operations function. For Army forces, this activity is a combined arms operation that focuses on priority intelligence requirements (PIRs) while answering the commander's critical information requirements (CCIRs).

1-13. Information collected from multiple sources and analyzed becomes intelligence that provides answers to commanders' information requirements concerning the enemy and other adversaries, climate, weather, terrain, and population. Developing these requirements is the function of information collection:

- A *commander's critical information requirement* is an information requirement identified by the commander as being critical to facilitating timely decisionmaking. The two key elements are friendly force information requirements and priority intelligence requirements (JP 3-0).
- A *priority intelligence requirement* is an intelligence requirement, stated as a priority for intelligence support, which the commander and staff need to understand the adversary or the operational environment (JP 2-0).
- A *friendly force information requirement* is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0).

1-14. The *planning requirements and assessing collection* process involves six continuous, nondiscrete activities. These activities and subordinate steps are not necessarily sequential and often overlap. The planning requirements and assessing collection process supports the staff planning and operations processes throughout unified land operations.

THE MILITARY DECISIONMAKING PROCESS

1-15. Upon receipt of the mission, commanders and staffs begin the MDMP. The *military decisionmaking process* is an iterative planning methodology that integrates the activities of the commander, staff, subordinate headquarters, and other partners to understand the situation and mission; develop and compare courses of action; decide on a course of action that best accomplishes the mission; and produce an operation plan or order for execution (FM 5-0).

1-16. During the second step of the of the MDMP, mission analysis, commanders and staffs analyze the relationships among the mission variables—mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC)—seeking to gain a greater understanding of the—

- Operational environment, including enemies and civil considerations.
- Desired end state of the higher headquarters.
- Mission and how it is nested with those of the higher headquarters.
- Forces and resources available to accomplish the mission and associated tasks.

1-17. Within the MDMP, OSINT assists in enabling the planning staff to update estimates and initial assessments by using publicly available information and open sources. Major intelligence contributions to mission analysis occur because of IPB. (For more information on the MDMP, see FM 5-0.)

Note. Nonintelligence staff can also research publicly available information to prepare functional area-specific estimates, papers, briefings, plans, and orders in support of the MDMP.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

1-18. *Intelligence preparation of the battlefield* is a systematic process of analyzing and visualizing the portions of the mission variables of threat, terrain, weather, and civil considerations in a specific area of interest and for a specific mission. By applying intelligence preparation of the battlefield, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space (FM 2-01.3).

1-19. IPB was originally designed to support the MDMP and troop leading procedures, but it can also be incorporated into other problem-solving models like design and red teaming. OSINT plays a significant and integral part during IPB in satisfying intelligence and information requirements indicated during the MDMP in support of unified land operations. The indicators that can be satisfied using OSINT during IPB include but are not limited to—

- Population.
- Propaganda.
- Commodities.
- Environment.

1-20. IPB is used primarily by commanders and staffs as a guide to evaluate specific datasets in order to gain an understanding of a defined operational environment. Prior to operations, an examination of national, multination partner, joint, and higher echelon databases is required to determine if the information requested is already available. As operations commence, new intelligence and information requirements are further identified as a result of battlefield changes. Publicly available information and open sources, when produced and properly integrated in support of the all-source intelligence effort, can be used to satisfy intelligence and information requirements. (For more information on IPB and indicators, see FM 2-01.3.)

Chapter 2

Planning and Preparation of the OSINT Mission

Directly or indirectly, publicly available information and open sources form the foundation for all intelligence when conducting operations. This foundation comes from open-source media components that provide worldview awareness of international events and perceptions of non-U.S. societies. This awareness prompts commanders to visualize a plan. Planning occurs when intelligence and information requirements are identified and means are developed as to how they will be satisfied. Effective OSINT mission planning and preparation are conducted during the Army force generation (ARFORGEN) train/ready force pool to enable the ease of transition to combat operations. (See FM 7-0 for more information on ARFORGEN.)

SECTION I – PLANNING OSINT ACTIVITIES

2-1. The *plan* step of the intelligence process consists of the activities that identify pertinent information requirements and develop the means for satisfying those requirements and meeting the commander's desired end state. As an aspect of intelligence readiness, planning for OSINT exploitation begins before a unit receives an official order or tasking as part of the *generate intelligence knowledge* continuing activity of the intelligence process.

2-2. The focus of OSINT research prior to deployment is determined and directed by the commander's guidance. Sustained and proactive open-source research using basic and advanced Internet search techniques plays a critical role in understanding AOs through foundational knowledge required for unit readiness and effective planning. Research during planning for possible missions provides insight into how nontraditional military forces, foreign military forces, and transnational threats have operated in similar AOs. Prior to deployment, organizations with dedicated OSINT missions can also be resourced to satisfy intelligence and information requirements. (See appendix E.)

2-3. After a unit receives a mission, the focus of OSINT research is further refined based on the AO in which the unit operates. OSINT supports the continuous assessment of unified land operations during planning. Effective research and planning ensure commanders receive timely, relevant, and accurate intelligence and information to accomplish assigned missions and tasks. The MDMP and IPB driven by the intelligence process frame the planning of OSINT exploitation. OSINT is integrated into planning through the four steps of the IPB process:

- Define the operational environment.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine threat COAs.

DEFINE THE OPERATIONAL ENVIRONMENT

2-4. When assessing the conditions, circumstances, and influences in the AO and area of interest, the intelligence staff examines all characteristics of the operational environment. There are preexisting publicly available inputs that can be used to identify significant variables when analyzing the terrain, weather, threat, and

civil considerations. At the end of step one of the IPB process, publicly available information and open sources can be used to support the development of the AO assessment and area of interest assessment.

DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS

2-5. When analyzing the environmental effects on threat and friendly operations, publicly available information and open sources can be used to describe the—

- Physical environment (terrestrial, air, maritime, space, and information domains).
- Weather.
- Civil considerations.
- Threat.

2-6. Combine the evaluation of the effects of terrain, weather, and civil considerations into a product that best suits the commander's requirements. At the end of the second step of IPB, publicly available information and open sources can be used to better inform the commander of possible threat COAs and products and assessments to support the remainder of the IPB process.

EVALUATE THE THREAT

2-7. Step three of the IPB process is to evaluate each of the significant threats in the AO. If the staff fails to determine all the threat factions involved or their capabilities or equipment, or to understand their doctrine and tactics, techniques, and procedures (TTP), as well as their history, the staff will lack the intelligence needed for planning. At the end of step three of IPB, publicly available information and open sources can provide the majority of the information required to identify threat characteristics, as well as provide possible information needed to update threat models.

DETERMINE THREAT COURSES OF ACTION

2-8. Step four of the IPB process is to identify, develop, and determine likely threat COAs that can influence accomplishment of the friendly mission. The end state of step four is to replicate the set of COAs available to the threat commander and to identify those areas and activities that, when observed, discern which COA the threat commander has chosen. At the end of step four of IPB, publicly available information and open sources can be used to determine indicators adopted by the threat commander.

SECTION II – PREPARATION OF OSINT ACTIVITIES

2-9. The reliance on classified databases has often left Soldiers uninformed and ill-prepared to capitalize on the huge reservoir of unclassified information from publicly available information and open sources, as the following quote describes:

> *OSINT was fairly new to us and once the term was understood we placed a signals intelligence analyst in charge of OSINT. At the tactical level, it seemed to be effective after the fact. There were three successful attacks against coalition forces aircraft in a specific area. We couldn't figure out the "how" and 5Ws [who, what, when, where, why] but our OSINT analyst found a downed aircraft video on the Internet that helped us identify the ingress and egress routes used during the attack that led to a "no fly" area and successful area denial missions in our area of operation.*
>
> All-Source Intelligence Analyst, Combat Aviation Brigade
> Operation Iraqi Freedom 2008-2009,

OSINT EXPLOITATION

2-10. When preparing to conduct OSINT exploitation, the areas primarily focused on are—

- Public speaking forums.
- Public documents.
- Public broadcasts.
- Internet Web sites.

PUBLIC SPEAKING FORUMS

2-11. Acquiring information at public speaking forums requires close coordination to ensure that any overt acquisition is integrated and synchronized with the information collection plan and does not violate laws prohibiting the unauthorized collecting of information for intelligence purposes. (See appendix A for further information on U.S. persons.)

2-12. Before gathering OSINT information at public speaking forums—

- Coordinate with key staff sections, such as the G-2X/S-2X, G-7/S-7, G-9/S-9, public affairs officer (PAO), and staff judge advocate (SJA), prior to conducting surveillance.
- Identify additional force protection personnel and equipment requirements.
- Identify the procedure for emplacement and recovery of audio and video processing equipment.

2-13. The operation order (OPORD), TTP, or unit standard operating procedures (SOPs) should describe how the unit that is tasked with the public speaking forum mission requests, allocates, and manages funds to purchase digital camera and audio recording equipment along with the computer hardware and software to play and store video-related data.

PUBLIC DOCUMENTS

2-14. Organizations within an AO conduct document collection missions. Once collected, documents are analyzed and the information is disseminated throughout the intelligence community. Before executing any OSINT exploitation related to collecting public documents, it is important to—

- Coordinate document collection, processing, and analysis activities across echelons.
- Identify the procedure to deploy, maintain, recover, and transfer hardcopy, analog, and digital media processing and communications equipment.
- Identify academic and commercial-off-the-shelf (COTS) information services that are already available for open-source acquisition, processing, and production.

2-15. The OPORD, TTP, or unit SOPs should describe how the unit requests, allocates, and manages funds for—

- Document collection and processing services.
- Purchasing books, dictionaries, images, maps, newspapers, periodicals, recorded audio and video items, computer hardware, digital cameras, and scanning equipment.
- The cost of subscribing to newspapers, periodicals, and other readable materials.

2-16. For more detailed information on public documents and document exploitation, see TC 2-91.8.

PUBLIC BROADCASTS

2-17. The DNI OSC collects, processes, and reports international and regional broadcasts. This enables deployed organizations to collect and process information from local broadcasts that are of command interest. Before exploiting OSINT related to public broadcasts, it is important to—

- Coordinate broadcast collection, processing, and production activities with those of the OSC.
- Identify the procedure to deploy, maintain, recover, and transfer radio and television digital media storage devices and content processing and communications systems.

- Identify Internet collection and processing resources to collect on television or radio station-specific Web casts.

2-18. The OPORD, unit SOPs, or TTP should describe how the unit tasked with public broadcast missions requests, allocates, and manages funds to purchase antenna and computer equipment, machine translation services or software, and subscribes to regional and international satellite radio and television broadcast service providers.

INTERNET WEB SITES

2-19. Information collected, processed, and produced from Internet Web sites supports unified land operations. Before exploiting OSINT related to Internet Web sites—

- Coordinate Internet collection, processing, and analysis activities across echelons.
- Identify the procedure to deploy, maintain, recover, and transfer computers and associated communications and data storage systems.
- Coordinate with G-6/S-6 for access to the INTELINK-U network or approved commercial Internet service providers that support open-source acquisition, processing, storage, and dissemination requirements.
- Coordinate with G-6/S-6 to develop a list of authorized U.S. and non-U.S. Internet Web sites for official government use, open-source research, and non-U.S. Internet Web sites restricted to selected authorized personnel engaged in OSINT exploitation.
- Identify academic and COTS information services that are already available for open-source information acquisition, processing, and production.

2-20. The OPORD, unit SOPs, or TTP should describe how the unit tasked with Internet research missions requests, allocates, and manages funds to purchase digitized documents, geospatial information, computer hardware and software applications, as well any subscriptions to academic and commercial online databases, newspapers, periodicals, and references.

PREPARATION CONSIDERATIONS

2-21. Preparing for OSINT exploitation also includes—

- Establishing an OSINT architecture.
- Prioritizing tasks and requests.
- Task-organizing assets.
- Deploying assets.
- Assessing completed operations.

ESTABLISHING AN OSINT ARCHITECTURE

2-22. OSINT contributes to establishing an intelligence architecture, specifically ART 2.2.2, *Establish Intelligence Architecture*. Establishing an intelligence architecture comprises complex and technical issues that include sensors, data flow, hardware, software, communications, communications security materials, network classification, technicians, database access, liaison officers, training, and funding. A well-defined and -designed intelligence architecture can offset or mitigate structural, organizational, or personnel limitations. This architecture provides the best possible understanding of the threat, terrain and weather, and civil considerations. An established OSINT architecture incorporates data flow, hardware, software, communications security components, and databases that include—

- **Conducting intelligence reach.** *Intelligence reach* is a process by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command (FM 2-0).
- **Developing and maintaining automated intelligence networks.** This task entails providing information systems that connect assets, units, echelons, agencies, and multinational partners for

intelligence, collaborative analysis and production, dissemination, and intelligence reach. It uses existing automated information systems, and, when necessary, creates operationally specific networks.

- **Establishing and maintaining access.** This task entails establishing, providing, and maintaining access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments for Army forces, joint forces, national agencies, and multinational organizations.
- **Creating and maintaining databases.** This task entails creating and maintaining unclassified and classified databases. Its purpose is to establish interoperable and collaborative environments for Army forces, joint forces, national agencies, and multinational organizations. This task facilitates intelligence analysis, reporting, production, dissemination, sustainment, and intelligence reach.

Operational and Technical Open-Source Databases

2-23. OSINT exploitation requires access to databases and Internet capabilities to facilitate processing, storage, retrieval, and exchange of publicly available information. These databases are resident on local area networks (LANs), the World Wide Web (WWW), and the Deep Web (see appendix C for additional information). To support unified land operations, OSINT personnel use evaluated and analyzed publicly available information and open sources to populate information databases such as—

- **Operational information databases**, which support the correlation of orders, requests, collection statuses, processing resources, and graphics.
- **Technical information databases**, which support collection operations and consist of unprocessed text, audio files, video files, translations, and transcripts.

Open-Source Collection Acquisition Requirement–Management System

2-24. The primary open-source requirements management operational information and technical information database is the Open-source Collection Acquisition Requirement-Management System (OSCAR-MS). OSCAR-MS is a Web-based service sponsored by the Office of the Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS) to provide the National Open Source Enterprise (NOSE) with an application for managing open-source collection requirements. OSCAR-MS links OSINT providers and consumers within the intelligence community down to the brigade combat team (BCT) level. Personnel at the BCT level access OSCAR-MS via the SECRET Internet Protocol Router Network (SIPRNET) in order to submit requests for information to the Department of the Army Intelligence Information Services (DA IIS) request for information portal. The goal of the OSCAR-MS is to automate and streamline ad hoc open-source collection requirements by—

- Providing useful metrics to understand OSINT requirements.
- Allowing the digital indexing and tagging of submitted and completed open-source products to be searchable in the Library of National Intelligence.
- Providing for local control of administrative data such as unit account management, local data tables, and local formats.
- Allowing simple and flexible formats that employ database auto-population.
- Using complete English instead of acronyms, computer codes, and other nonintuitive shortcuts.
- Allowing linkages between requirements, products, and evaluations.
- Enabling integration of open-source users for collaboration between agencies.
- Reducing requirement duplication through customers directly contributing to existing requirements.

2-25. For more detailed information on OSCAR-MS or to submit OSINT requirements, contact the U.S. Army Intelligence and Security Command (INSCOM) DA IIS at https://www.intelink.gov/sharepoint/default.aspx.

PRIORITIZING TASKS AND REQUESTS

2-26. The G-2/S-2 and G-3/S-3 staffs use commander guidance and primary intelligence requirements to complete the information collection plan. The plan is used to assign tasks to subordinate units or submit requests to supporting intelligence organizations to achieve the desired information collection objectives. Embodied in the information collection plan, these tasks describe how the unit—

- Requests collection and production support from joint, interagency, intergovernmental, and multinational organizations.
- Task-organizes and deploys organic, attached, and contracted collection, processing, and production assets.
- Conducts remote, split-based, or distributed collection, processing, and production.
- Requests and manages U.S. and non-U.S. linguists based on priority for support, mission-specific skills, knowledge requirements (such as language, dialect, and skill level), clearance level, and category.

2-27. When developing information collection tasks for subordinate units, the G-2/S-2 and G-3/S-3 staffs use the task and purpose construct for developing task statements to account for—

- *Who* is to execute the task?
- *What* is the task?
- *When* will the task begin?
- *Where* will the task occur?

TASK-ORGANIZING ASSETS

2-28. With the exception of the Asian Studies Detachment (ASD) that maintains an organic table of distribution and allowances (TDA) with the government of Japan in support of U.S. Pacific Command (USPACOM), the Army does not have a TDA or base table of organization and equipment for OSINT personnel or units when preparing to conduct OSINT exploitation.

DEPLOYING ASSETS

2-29. Deployment of publicly available assets—

- Supports the scheme of maneuver.
- Supports the commander's intent.
- Complies with unit SOPs.

2-30. The deployment of assets generally requires a secure position, with network connectivity to the Internet, in proximity to supporting sustainment, protection, and communications resources.

ASSESSING COMPLETED OPERATIONS

2-31. Typical guidelines used to assess operations are—

- Monitoring operations.
- Correlating and screening reports.
- Disseminating and providing a feedback mechanism.
- Cueing.

2-32. See paragraph 2-67 for an explanation of these guidelines.

SECTION III – PLANNING AND PREPARATION CONSIDERATIONS

2-33. Planning and preparation considerations when planning for OSINT exploitation include—

- Open-source reliability.
- Open-source information content credibility.
- Compliance.
- Operations security (OPSEC).
- Classification.
- Coordination.
- Deception and bias.
- Copyright and intellectual property.
- Linguist requirements.
- Machine foreign language translation (MFLT) systems.

OPEN-SOURCE RELIABILITY

2-34. The types of sources used to evaluate information are—

- Primary sources.
- Secondary sources.

2-35. A *primary source* refers to a document or physical object that was written or created during the time under study. These sources are present during an experience or time period and offer an inside view of a particular event. Primary sources—

- Are generally categorized by content.
- Is either public or private.
- Is also referred to as an original source or evidence.
- In fact, are usually fragmentary, ambiguous, and difficult to analyze. The information contained in primary sources is also subject to obsolete meanings of familiar words.

2-36. Some types of primary sources include—

- Original documents (excerpts or translations) such as diaries, constitutions, research journals, speeches, manuscripts, letters, oral interviews, news film footage, autobiographies, and official records.
- Creative works such as poetry, drama, novels, music, and art.
- Relics or artifacts such as pottery, furniture, clothing, artifacts, and buildings.
- Personal narratives and memoirs.
- Person of direct knowledge.

2-37. A *secondary source* interprets, analyzes, cites, and builds upon primary sources. Secondary sources may contain pictures, quotes, or graphics from primary sources. Some types of secondary sources include publications such as—

- Journals that interpret findings.
- Textbooks.
- Magazine articles.
- Commentaries.
- Histories.
- Criticisms.
- Encyclopedias.

Note. Primary and secondary sources are oftentimes difficult to distinguish as both are subjective in nature. Primary sources are not necessarily more of an authority or better than secondary sources. For any source, primary or secondary, it is important for OSINT personnel to evaluate the report for deception and bias.

2-38. Open-source reliability ratings range from **A** (reliable) to **F** (cannot be judged) as shown in table 2-1. A first-time source used in the creation of OSINT is given a source rating of **F**. An **F** rating does not mean the source is unreliable, but OSINT personnel have no previous experience with the source upon which to base a determination.

Table 2-1. Open-source reliability ratings

A	***Reliable***	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	***Usually reliable***	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
C	***Fairly reliable***	**Doubt** of authenticity, trustworthiness, or competency, but has provided valid information in the past.
D	***Not usually reliable***	**Significant doubt** about authenticity, trustworthiness, or competency, but has provided valid information in the past.
E	***Unreliable***	**Lacking** authenticity, trustworthiness, and competency; history of invalid information.
F	***Cannot be judged***	**No basis** exists for evaluating the reliability of the source.

OPEN-SOURCE INFORMATION CONTENT CREDIBILITY

2-39. Similar to open-source reliability, credibility ratings range from **one** (confirmed) to **eight** (cannot be judged) as shown in table 2-2. If the information is received from a first-time source, it is given a rating of **eight** and, like the reliability ratings scale, does not mean the information is not credible but that OSINT personnel have no means to verify the information.

Table 2-2. Open-source content credibility ratings

1	***Confirmed***	**Confirmed** by other independent sources; logical in itself; consistent with other information on the subject.
2	***Probably true***	**Not confirmed**; logical in itself; consistent with other information on the subject.
3	***Possibly true***	**Not confirmed**; reasonably logical in itself; agrees with some other information on the subject.
4	***Doubtfully true***	**Not confirmed**; possible but not logical; no other information on the subject.
5	***Improbable***	**Not confirmed**; not logical in itself; contradicted by other information on the subject.
6	***Misinformation***	**Unintentionally false**; not logical in itself; contradicted by other information on the subject; confirmed by other independent sources.
7	***Deception***	**Deliberately false**; contradicted by other information on the subject; confirmed by other independent sources.
8	***Cannot be judged***	**No basis** exists for evaluating the validity of the information.

COMPLIANCE

2-40. In accordance with EO 12333, DOD 5240.1-R, and AR 381-10, procedure 2, Army intelligence activities may collect publicly available information on U.S. persons only when it is necessary to fulfill an assigned function. (For more information on intelligence oversight, see appendix A.)

OPERATIONS SECURITY

2-41. OSINT could unintentionally provide present and future indicators of U.S. military operations. Information generally available to the public can reveal the existence of, and sometimes details about classified or sensitive information that can be used to neutralize or exploit military operations. Intelligence organizations

must determine the level of contact with open sources and the collection or acquisition technique that could affect Army operations.

CLASSIFICATION

2-42. AR 380-5 states that intelligence producers "must be wary of applying so much security that they are unable to provide a useful product to consumers." This is an appropriate warning for OSINT personnel where concern for OPSEC can undermine the ability to disseminate inherently unclassified information. Examples of unclassified information being over-classified are—

- Reported information found in a foreign newspaper.
- Message from a foreign official attending an international conference.

2-43. AR 380-5 directs that Army personnel will not apply classification or other security markings to an article or portion of an article that has appeared in a newspaper, magazine, or other public medium. Final analysis of OSINT may require additional restrictions and be deemed *controlled unclassified information* or *sensitive but unclassified information*.

COORDINATION

2-44. During planning, the G-2/S-2 and G-3/S-3 staff must ensure that OSINT missions and tasks are synchronized with the scheme of maneuver. Acquiring open-source information may compromise the operations of other intelligence disciplines or tactical units. Open-source acquisition that is not synchronized may also result in the tasking of multiple assets and the improper utilization of forces and equipment, adversely affecting the ability of nonintelligence organizations, such as civil affairs, military police, and public affairs, to accomplish assigned missions and tasks. Conversely, overt contact with an open source by nonintelligence organizations can compromise OSINT missions and tasks and lead to the loss of intelligence.

DECEPTION AND BIAS

2-45. Deception and bias is a concern in OSINT exploitation. OSINT exploitation does not normally acquire information by direct observation of activities and conditions within the AO. OSINT exploitation relies mainly on secondary sources to acquire and disseminate information. Secondary sources, such as government press offices, commercial news organizations, and nongovernmental organizations spokespersons, can intentionally or unintentionally add, delete, modify, or otherwise filter the information made to the general public. These sources may also convey one message in English with the intent to sway U.S. or international perspectives and a different non-English message for local populace consumption. It is important to know the background of open sources and the purpose of the public information in order to distinguish objectives, factual information, identify bias, or highlight deception efforts against the reader and the overall operation.

COPYRIGHT AND INTELLECTUAL PROPERTY

2-46. *Copyright* is a form of protection, for published and unpublished works, provided by Title 17, United States Code (USC), to authors of "original works of authorship," including literary, dramatic, musical, and artistic works. Intellectual property is considered any creation of the mind and includes, but is not limited to—

- Musical works and compositions.
- Artistic displays.
- Discoveries.
- Inventions.
- Words or phrases.
- Symbols and designs.

2-47. It is illegal to violate the rights provided by the copyright law to the owner of copyright. One major limitation is the doctrine of fair use, which is given a statutory basis in Section 107 of the 1976 Copyright Act. According to the U.S. Copyright Office, "fair use" of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship, or research is not an infringement of copyright. The four factors in determining fair use are the—

- Purpose and character of the use.
- Nature of the copyrighted work.
- Amount and substantiality of the portion used in relation to the copyrighted work as a whole.
- Effect of the use upon the potential market for or value of the copyrighted work.

2-48. AR 27-60 prescribes policies and procedures for the acquisition, protection, transfer, patent usage, copyrights, and trademarks of intellectual property. Army policy recognizes the rights of copyright owners consistent with Army missions and worldwide commitments. OSINT personnel will not produce or distribute copyrighted works without the permission of the copyright owner unless such use is authorized under U.S. copyright law. There is also a requirement for OSINT personnel to forward to the Service SJA for approval and waiver of notice to the copyright holder, if necessary, for OPSEC. (For more information on copyright laws and applicability, see the International Copyright Relations of the United States at http://www.copyright.gov or the local SJA office.)

LINGUIST REQUIREMENTS

2-49. The ability to gather and analyze foreign materials is critical in OSINT exploitation. The effective use and employment of linguists, both civilian and military, facilitates this activity. The areas of the highest criticality of required foreign language skills and knowledge proficiency are—

- **Transcription.** Both listening and writing proficiency in the source language are essential for an accurate transcript. A transcript is extremely important when English language skills of the OSINT personnel are inadequate for authoritative or direct translation from audio or video into English text.
- **Translation.** Bilingual competence is a prerequisite for translations. Linguists must be able to—
  - Read and comprehend the source language.
  - Write comprehensibly in English.
  - Choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.
- **Interpretation.** Bilingual competence is a prerequisite for interpretation. Linguists must be able to—
  - Hear and comprehend the source language.
  - Speak comprehensibly in English.
  - Choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.

Note. Interpretation is a specific skill in which not all linguists are trained.

2-50. To effectively plan and employ linguists, commanders and staffs must understand the Army linguist proficiency evaluation system. Evaluation and reevalution of linguist proficiency is covered in detail in AR 11-6, chapter 5. Language testing is required for all Army personnel, in a language-dependent military occupational specialty (MOS) or Army occupational code (AOC), who have received foreign language training. Other Army personnel who have knowledge of a foreign language are encouraged to take the proficiency test and may work as linguists.

2-51. The Army uses the Defense Language Proficiency Test (DLPT) to measure the proficiency level in a specific language. The DLPT is an indication of foreign language capability, but it is not the definitive evaluation of an individual's ability to perform linguist support.

2-52. The Army uses Interagency Language Roundtable (ILR) descriptions of the proficiency levels for the skills of speaking, listening, reading, and writing a foreign language. Detailed descriptions of these levels are available at http://www.govtilr.org. The plus-level designators, shown as a "+" symbol, are used to designate when a linguist is above a base level, but not yet to the capability of the next level. The six base levels of proficiency as established by the DLPT are—

- **Level 0 (no proficiency).** The Soldier has no functional foreign language ability. Level 0+ is the minimum standard for special-forces personnel and indicates a memorized proficiency only.
- **Level 1 (elementary proficiency).** The Soldier has limited control of the foreign language skill area to meet limited practical needs and elementary foreign language requirements.
- **Level 2 (limited working proficiency).** The linguist is sufficiently skilled to be able to satisfy routine foreign language demands and limited work requirements.
- **Level 3 (general professional proficiency).** The linguist is capable of performing most general, technical, formal, and informal foreign language tasks on a practical, social, and professional level.
- **Level 4 (advanced professional proficiency).** The linguist is capable of performing advanced professional foreign language tasks fluently and accurately on all levels.
- **Level 5 (functionally native proficiency).** The linguist is functionally equivalent to an articulate and well-educated native in all foreign language skills; the linguist reflects the cultural standards of the country where the foreign language is natively spoken.

2-53. The above proficiency base levels designate proficiency in any of the four language skills—listening, reading, speaking, and writing. The DLPT only evaluates reading and listening skills (for example, 2+/3, or 3/1+). Currently, these tests do not evaluate linguists above the 3-proficiency level. The current Army standard to be considered a qualified linguist is a level 2. Oral proficiency interviews evaluate speaking proficiency and may be used to provide a listening score. These interviews may provide an evaluation all the way up to the 5-proficiency level.

2-54. Along with proficiency and fluency, OSINT personnel must consider the biases and cultural backgrounds of civilian interpreters when analyzing non-English open-source information. When planning to utilize linguists, commanders must identify requirements by category. Linguist screening categories are—

- **Category I.** Linguists must at least have advanced professional proficiency in the target language, a level 4 as measured by the ILR and general working proficiency (ILR 2+) in English. They may be locally hired or from a region outside the AO. They do not require a security clearance.
- **Category II.** Linguists are U.S. citizens granted access to a Secret clearance by the designated U.S. Government personnel security authority. They must at least have advanced professional proficiency in the target language (ILR 4) and general working proficiency (ILR 2+) in English.
- **Category III.** Linguists are U.S. citizens granted Top Secret (TS)/Sensitive Compartmented Information (SCI) or an interim TS/SCI clearance by the designated U.S. Government personnel security authority. They must meet a minimum of ILR 3 in both the target language and English.

MACHINE FOREIGN LANGUAGE TRANSLATION SYSTEMS

2-55. Developing a reliable and proficient linguist requires a great deal of time, both for training and gaining experience. This extended timeline often results in shortages of linguist personnel. To fill personnel vacancies throughout Army units and to meet language requirements and demands, MFLT systems are used. When employed properly, MFLT systems can provide an increased capability for translation in support of unified land operations.

2-56. Reliable MFLT capability exists to translate media broadcasts into English and there is readily available software to translate Internet sources into English as well. There are limited speech-to-speech (S2S) capabilities in use.

FOREIGN MEDIA MONITORING

2-57. Media monitoring systems like the BBN Broadcast Monitoring System™ (BMS™) create a continuous searchable archive of international television broadcasts. These systems automatically transcribe the real-time audio stream and translate it into English. Both the transcript and translation are searchable and synchronized to the video, providing powerful capabilities for effective retrieval and precise playback of the video based on its speech content. With this system, intelligence analysts can sift through vast collections of news content in other languages quickly and efficiently.

2-58. These systems provide real-time transcription and translation of broadcast television news, allowing English speakers to rapidly triage non-English television content, be alerted when new content that matches a profile is captured by the system, and work closely with human linguists and cultural experts to create actionable high-quality translations of extracted content.

2-59. The interface allows users to quickly search for specific spoken content in the video archive through keyword queries in English or the source language. Search terms are highlighted in the results, which show an image thumbnail, the transcript segment in the original language, and an English translation. Clicking on a result begins playback of the segment.

2-60. Users interact with the system from any personal computer (PC) or laptop via a common high-speed Internet connection. The only required client software is Microsoft® Internet Explorer and Windows Media® Player.

2-61. The BBN BMS™ continuously captures, encodes, analyzes, and stores live video streams in an automatically maintained, dynamic cache containing 30 days of recorded audio or video. As the video plays back, the system highlights the spoken words in both the original language and the translation. The transcript is enriched by highlighting the names of people, locations, and organizations, and by separating the speakers in the audio file. Users can jump to any point in the cache and begin playback.

2-62. Users can extract video segments or still photos for sharing, presentation, and collaboration. Demonstration compact discs (CDs) contain extracted segments that preserve the highlighting and synchronization of video, transcript, and translation during playback.

2-63. The BBN BMS™ currently translates—

- Modern Standard Arabic.
- Mandarin Chinese.
- Western Hemisphere Spanish.
- Persian Farsi.
- North American English.
- United Kingdom English.
- French.
- Bahasa Indonesian.
- Hindi.
- Urdu.

2-64. The BBN BMS™ does not require any hardware setup, software installation, or onsite administration or maintenance by the customer.

SPEECH-TO-SPEECH

2-65. Army and Marine units continue to attempt to integrate available COTS S2S translation devices into predeployment training and military operations while deployed. The primary tactical use for these devices has been language translation within security operations conducted in and among a general population of non-English speaking people.

SECTION IV – MANNING THE OSINT SECTION

2-66. OSINT personnel that comprise the OSINT section within the intelligence staff section can consist of both intelligence and nonintelligence individuals with the technical competence, creativity, forethought, cultural knowledge, and social awareness to exploit open sources effectively. The designation of OSINT personnel to satisfy requirements, missions, and tasks is generally identified by commanders and task-organized through organic assets (intelligence personnel, nonintelligence personnel, U.S. and non-U.S. contractor personnel, or linguists) in support of unified land operations.

OSINT SECTION DUTIES

2-67. The duties of the OSINT section are to—

- **Monitor operations.** This ensures responsiveness to the current situation and to anticipate future acquisition, processing, reporting, and synchronization requirements.
- **Correlate reports.** Reports (written, verbally, or graphically) should correlate classified reports through OSINT validation.
- **Screen reports.** Information is screened in accordance with the CCIRs and commander's guidance to ensure that pertinent and relevant information is not overlooked and the information is reduced to a workable size. Screening should encompass the elements of timeliness, completeness, and relevance to satisfy intelligence requirements.
- **Disseminate intelligence and information.** Satisfied OSINT requirements are disseminated to customers in the form of useable products and reports.
- **Cue.** Effective cueing by OSINT to more technical information collection assets, such as human intelligence (HUMINT) and counterintelligence (CI) improves the overall information collection effort by keeping organizations abreast of emerging unclassified information and opportunities as well as enabling the use of a multidiscipline approach to confirm or deny information by another information source, collection organization, or production activity.
- **Provide feedback.** An established feedback mechanism is required to the supported commander or customer on the status of intelligence and information requirements.

OSINT SECTION AT THE BRIGADE COMBAT TEAM LEVEL

2-68. Each combatant command may have a task-organized OSINT cell or section to some varying degree in scope and personnel. At the tactical level of operations, it is commonplace for commanders to create OSINT cells from organic intelligence personnel to satisfy intelligence requirements.

2-69. The following quote illustrates how task organization of organic personnel within the common ground station (CGS) can assist in satisfying intelligence and information requirements using the Nonsecure Internet Protocol Routing Network (NIPRNET) and various electronic devices, such as an amplitude modulation and frequency modulation (AM/FM) radio, video cassette recorder (VCR), and digital video disc (DVD) player, to ensure the success of their BCT to perform information collection at the tactical operations center (TOC):

With their CGS team, four to five interpreters, and a steady flow of radio, television, and newspaper reports, the open-source intelligence team produced a daily rollup with analysis. Their office consisted of one television with local and international cable, one laptop connected to the NIPRNET, AM/FM radio, and the daily newspaper. Also, the team acquired a VCR and DVD player to study confiscated propaganda and other media. They understand the importance of local reporting to the success of the BCT campaign and have made it a point to conduct thorough research on topics of local importance. Their product was studied and further analyzed by the (information collection) analysis team at the BCT TOC prior to submission to the BCT S-2 and dissemination to battalions or division.

Military Intelligence Company Commander, 3ID,
Operation Iraqi Freedom 2004—2005

2-70. As displayed in figure 2-1, personnel comprising the OSINT section at the BCT level include—

- Section leader.
- Requirements manager.
- Situation development analyst.
- Target development analyst.

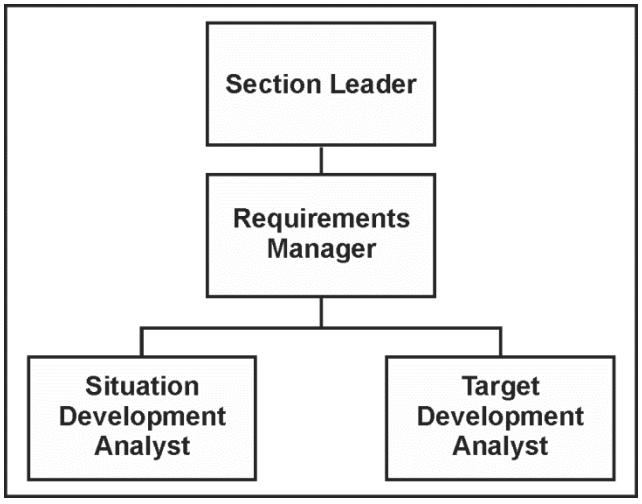


Figure 2-1. Brigade combat team's OSINT section

SECTION LEADER

2-71. The section leader—

- Is the primary liaison and coordinator with the BCT S-2.
- Provides supervisory and managerial capacity oversight.
- Sets the priority of tasks.
- Monitors ongoing intelligence support required by the BCT S-2.
- Ensures that all OSINT products are included in the planning for current and future operations.

REQUIREMENTS MANAGER

2-72. The requirements manager—

- Ensures that situation development and target development support the overall efforts of the section.
- Verifies the availability of collection assets.
- Performs quality control for situation development and target development products.
- Supervises the receipt, analysis, and dissemination of OSINT products.

SITUATION DEVELOPMENT ANALYST

2-73. The situation development analyst—

- Monitors publicly available information and open sources in order to ensure the most accurate common operational picture.
- Analyzes information and produces current intelligence about the operational environment, enemy, terrain, and civil considerations before and during operations.
- Refines information received on threat intentions, objectives, combat effectiveness, and potential missions.
- Confirms or denies threat COAs based on publicly available indicators.
- Provides information to better understand the local population in areas that include, but are not limited to—
  - Tribal affiliations.
  - Political beliefs.
  - Religious tenets.
  - Key leaders.
  - Support groups.
  - Income sources.

TARGET DEVELOPMENT ANALYST

2-74. The target development analyst—

- Identifies the components, elements, and characteristics of specific targets, both lethal and nonlethal.
- Identifies civil and other non-target considerations within the AO.
- Provides publicly available information on threat capabilities and limitations.

TASK ORGANIZATION CONSIDERATIONS

2-75. When task-organizing the OSINT section to satisfy intelligence and information requirements, units must consider—

- Mission command.
- Acquisition.
- Collecting and processing.
- Production.
- Computer systems.

MISSION COMMAND

2-76. Dedicated mission command personnel are needed in order to provide management and oversight of OSINT exploitation to ensure continued synchronization with maneuver elements, tasks, and requests.

ACQUISITION

2-77. Due to the volumes of publicly available information, acquisition through established information collection activities and systems are necessary in order to ensure that open-source information is not lost or misplaced that could provide essential and necessary mission-related information. Publicly available information acquired from open sources should be reported in accordance with established unit SOPs.

COLLECTING AND PROCESSING

2-78. OSINT properly integrated into overall collection plans during operations are used to satisfy CCIRs. In order to access the full array of domestic and foreign publicly available information, the processing of materials oftentimes requires OSINT support to personnel operating in the areas of document exploitation (DOCEX).

Note. Personnel engaging in the collecting and processing of information involving these aspects will require an understanding of those items and materials that are commonplace and those that could possess intelligence value. They must further be versed in the additional regulations for Director, National Security Agency (DIRNSA) oversight. Unless foreign publicly available information and open sources are collected and subsequently processed into a suitable form, the information will lose intelligence value.

PRODUCTION

2-79. Production of actionable and timely publicly available information through open sources is vital in OSINT exploitation. Research methods, Internet techniques (basic and advanced), and other associated tools are utilized to retrieve, integrate, evaluate, analyze, and interpret information into OSINT. Research information and finalized metadata as products are stored in databases accessible to other intelligence and nonintelligence personnel that have vested OSINT exploitation requirements.

COMPUTER SYSTEMS

2-80. OSINT personnel conducting OSINT exploitation need to have software allocated to the appropriate task. The necessary unfettered exploitation suite includes such programs as Analyst Notebook, Portable Document Format (PDF) Maker, and Text Chart.

Chapter 3

Collecting OSINT

Due to the unclassified nature of publicly available information, those engaging in OSINT collection activities can begin researching background information on their assigned area of responsibility long before the issuance of an official military deployment order while generating intelligence knowledge. IPB, an integrating process for Army forces, is the mechanism identifying intelligence and information requirements that can be satisfied utilizing publicly available information and open sources.

COLLECTING PUBLICLY AVAILABLE INFORMATION

3-1. Publicly available information and open-source research, applied as an economy of force, is an effective means of assimilating authoritative and detailed information on the mission variables (METT-TC) and operational variables (political, military, economic, social, information, infrastructure, physical environment, time [PMESII-PT]). The compilation of unanswered intelligence and information requirements determined at the conclusion of the MDMP and IPB are exercised through the commander's input. Commander's input—

- Is expressed in the terms of describe, visualize, and direct.
- Is the cornerstone of guidance used by OSINT personnel.
- Validates intelligence and information requirements.

3-2. Commander's input is expressed as CCIRs and categorized as friendly force information requirements (FFIRs) and PIRs. Continuous research and processing methods, coupled with the commander's input and intelligence and information requirements, OSINT personnel collect publicly available information for exploitation. The *collect* step of the intelligence process involves collecting, processing, and reporting information in response to information collection tasks. Collected information is the foundation of intelligence databases, intelligence production, and situational awareness.

3-3. OSINT is integrated into planning through the continuous process of IPB. Personnel engaging in OSINT exploitation must initiate collection and requests for information to satisfy CCIRs to the level of detail required. Collecting open-source information comprises four steps, as shown in figure 3-1 on page 3-2:

- Identify information and intelligence requirements.
- Categorize intelligence requirements by type.
- Identify source to collect the information.
- Determine collection technique.

IDENTIFY INFORMATION AND INTELLIGENCE REQUIREMENTS

3-4. Intelligence and information gaps are identified during the IPB process. These gaps should be developed and framed around the mission and operational variables in order to ensure the commander receives the information needed to support all lines of operations or lines of effort. As information and intelligence are received, OSINT personnel update IPB products and inform the commander of any relevant changes. OSINT needs clearly stated information and intelligence requirements to effectively focus

acquisition and production and should be incorporated into collection plans in order to satisfy these requirements.

Note. OSINT cannot eliminate all the unknown aspects or uncertainties that concern commanders and staffs. The G-2/S-2 must be prepared to fill gaps with reasonable assumptions; once gaps are filled, the G-2/S-2 must begin developing databases at the unit level in order to have information readily available. This reduces the number of new requests for information from subordinate units or organizations.

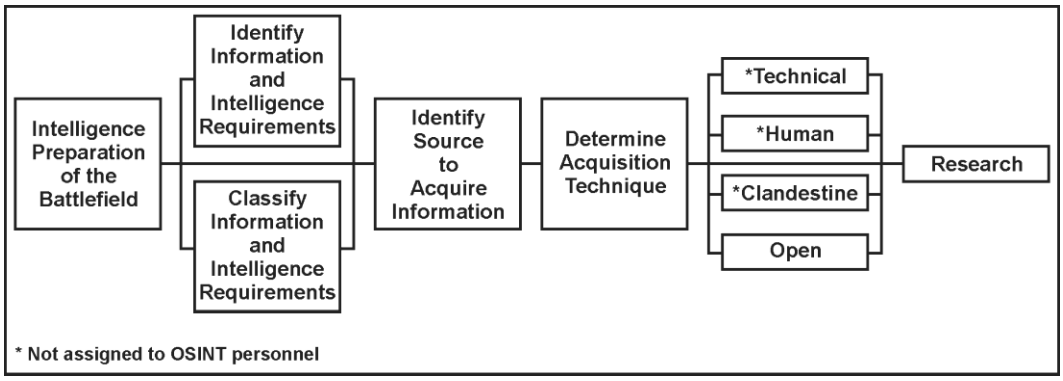


Figure 3-1. Process for collecting publicly available information

CATEGORIZE INTELLIGENCE REQUIREMENTS BY TYPE

3-5. Intelligence requirements that need to be satisfied can extend beyond the scope of OSINT, resulting in gaps. OSINT is subject to information and intelligence gaps that need to be satisfied using other appropriate methods to close those gaps.

3-6. IPB is used to classify intelligence and information requirements by type based on mission analysis and friendly COAs. OSINT personnel provide input during this step. Two important related terms that work in concert with OSINT are private information and publicly available information:

- **Private information** comprises data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. Intelligence requirements that require private information are not assigned to OSINT sections. There are two subcategories of private information:
  - ***Controlled unclassified information*** requires the application of controls and protective measures, for a variety of reasons (that is, *sensitive but unclassified* or *for official use only*).
  - ***Classified information*** requires protection against unauthorized disclosure and is marked to indicate its classified status when produced or disseminated.
- **Publicly available information** comprises data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

Note. The amount of classified information produced on any one topic can be limited and taken out of context if viewed from a solely classified perspective. OSINT validation is necessary when dealing with a large amount of classified information. OSINT validation is used when classified sources are unavailable or to confirm or support preexisting classified sources. This strengthens the credibility of OSINT products in support of all-source intelligence. OSINT validation provides the ability to cue other assets thus enhancing the accuracy and precision of gained intelligence.

IDENTIFY SOURCE TO COLLECT INFORMATION

3-7. Identifying the source is part of planning requirements and assessing collection plans. The two types of sources used to collect information are confidential sources and open sources:

- **Confidential sources** comprise any persons, groups, or systems that provide information with the expectation that the information, relationship, or both are protected against public disclosure. Information and intelligence requirements that require confidential sources are not assigned to OSINT sections.
- **Open sources** comprise any person or group that provides information without the expectation of copyright or privacy—the information, the relationship, or both is not protected against public disclosure. Open sources include but are not limited to—
  - ***Academia.*** Courseware, dissertations, lectures, presentations, research papers, and studies in both hardcopy and softcopy covering subjects and topics on economics, geography (physical, cultural, and political-military), international relations, regional security, and science and technology.
  - ***Government agencies and nongovernmental organizations.*** Databases, posted information, and printed reports on a wide variety of economic, environmental, geographic, humanitarian, security, and science and technology issues.
  - ***Commercial and public information services.*** Broadcasted, posted, and printed news on current international, regional, and local topics.
  - ***Libraries and research centers.*** Printed documents and digital databases on a range of topics.
  - ***Individuals and groups.*** Handwritten, painted, posted, printed, and broadcasted information on subjects and topics on art, graffiti, leaflets, posters, tattoos, and Web sites.
  - ***Gray literature.*** Materials and information that are found using advanced Internet search techniques on the Deep Web consisting of technical reports, scientific research papers, and white papers.

DETERMINE COLLECTION TECHNIQUE

3-8. Collection implies gathering, by a variety of means, raw data and information from which finalized intelligence is then created or synthesized, and disseminated. Collected information is analyzed and incorporated into all-source and other intelligence discipline products. These products are disseminated per unit SOPs, OPORDs, other established feedback mechanism, or intelligence architecture. These techniques confirm the presence of planned targets and provide a baseline of activity and information on sources within the AO for further development and future validation. When gathering information, the utilized technique includes specific information requests, objectives, priorities, timeframe of expected activity, latest (or earliest) time the information is of value (LTIOV), and reporting instructions.

3-9. Open-source information that satisfies a CCIR is disseminated as quickly as possible to the commander and other staff personnel per unit SOPs or OPORDs. OSINT can use unintrusive collection techniques to cue more technical collection assets. Collection techniques, depending on operation complexities, can enhance the chances of satisfying intelligence and information requirements.

3-10. Open-source acquisition of information and intelligence requirements are assigned to OSINT personnel. Open-source collection includes the acquisition of material in the public domain. The extent to which open-source collection yields valuable information varies greatly with the nature of the target and the subject involved. The information might be collected by individuals who buy books and journals, observe military parades, or record television and radio programs.

RESEARCH

3-11. After determining the collection technique, OSINT personnel conduct research to satisfy intelligence and information requirements.

3-12. Research—

- Leads to the population of information and intelligence databases. These databases enable OSINT personnel to accurately respond to changes within the AO by providing requested information to satisfy requirements.
- Is used to gather information that contributes to providing an understanding of a problem and organizing the results comprehensively.
- Is used to generate intelligence knowledge before and during deployments.

3-13. Two types of research methods that can be used are—

- **Field research.** Personnel from academic, governmental, intergovernmental, and nongovernmental organizations acquire data from primary sources, as well as retrieve data and information from secondary sources. Field research—
  - Consists of participant observation, data collection, and survey research.
  - Is typically conducted at the operational and strategic levels when time is not a factor in the development of information and intelligence of the operational variables (PMESII-PT) to provide commanders situational awareness.
- **Practical research.** Intelligence personnel retrieve existing data and information from secondary sources. Practical research—
  - Is typically conducted at the tactical level when time is a factor in the development of information and intelligence of the mission variables (METT-TC) in providing commanders situational awareness.
  - Is primarily used among intelligence personnel that engage in OSINT exploitation.

3-14. All research begins with the determination of a research question and the development of a research plan.

DETERMINE RESEARCH QUESTION

3-15. Research begins with the determination of a research question expressed in the form of CCIRs regarding a given topic. In OSINT exploitation, the research question can be based on the mission variables (METT-TC) and operational variables (PMESII-PT). The research question is refined through the development of information and intelligence requirements to be satisfied. Those requirements that are not satisfied are included in the planning requirements and assessing collection plan where more technical means of collection can be utilized.

DEVELOP RESEARCH PLAN

3-16. Different facets of a question may be expressed as information and intelligence requirements. These requirements form the basis for the research plan. A research plan can use both field research and practical research. The plan consists of—

- Identification of information sources (both primary and secondary).
- Description of how to access those sources.
- Format for compiling the data.
- Research methodology.
- Dissemination format.

IMPLEMENT RESEARCH PLAN

3-17. Utilizing open-source media—the means of sending, receiving, and recording information—components, and associated elements (see table 3-1), OSINT personnel implement a research plan. The primary media used to implement a research plan include—

- Public speaking forums.
- Public documents.
- Public broadcasts.
- Internet Web sites.

Note. The table does not illustrate an all-inclusive list of open-source media types but rather the categories of open-source media to consider when collecting open-source information.

Table 3-1. Open-source media, components, and elements

Media	*Components*	*Elements*	
Public Speaking	Speaker	• Sponsor • Relationship	• Message
	Format	• Conference • Debate • Demonstration • Speeches	• Lecture • Rally • Loud speakers • Talk shows
	Audience	• Location	• Composition
Public Documents	Graphic	• Drawing • Engraving • Painting • Graffiti	• Photograph • Print • Posters
	Recorded	• Compact data storage device • Digital video disk	• Hard disk • Tape
	Printed	• Book • Brochure • Newspapers • Magazines • Government releases • “Dumpster diving” • Annuals	• Periodical • Pamphlet • Report • Novelties • Non-government releases • Leaflets • Business cards
Public Broadcasts	Radio	• Low frequency AM radio • Medium frequency AM radio • Short wave radio	• VHF FM radio • Satellite radio • Standard wave radio
	Television	• Ku band satellite television • VHF and UHF terrestrial television • Advertisements • Motion pictures	
Internet Web Sites	Communications	• Chat • E-mail • News; newsgroup	• Web cam • Web cast • Web log
	Databases	• Commerce • Education	• Government • Military organizations
	Information (Web page content)	• Commerce • Education	• Government • Military organizations
	Services	• Dictionary • Directory • Downloads • Financial	• Geospatial • Search and URL lookup • Technical support • Translation

AM	amplitude modulation	URL	uniform resource locator
FM	frequency modulation	VHF	very high frequency
UHF	ultrahigh frequency		

Public Speaking Forums

3-18. OSINT personnel conduct research by attending public speaking forums such as conferences, lectures, public meetings, working groups, debates, and demonstrations. Attending these and similar events are opportunities to build relationships with nonmilitary professionals and organizations. Intelligence personnel require a thorough understanding of the local culture and laws to ensure any collection activities are unintrusive and do not violate local customs or laws, such as the Chatham House Rule. It is recommended to have the SJA's oversight during such collection missions to ensure compliance with AR 381-10, procedure 10. OSINT personnel require situational awareness and cultural understanding that is typically done by establishing both military and nonmilitary relationships with attendees, identifying any modifications of a speaker's message, and identifying personnel of interest attending the event.

3-19. OSINT personnel engaging in open-source exploitation, utilize public speaking forums typically in operational environments dominated by either stability operations or counterinsurgency operations where the level of violence is low.

Note. The Chatham House Rule states, "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speakers, nor any other participants, may be revealed." Questioning the invocation of the Chatham House Rule should be inquired before the engagement begins. An invoked Chatham House Rule changes the characterization of the source from an open to a confidential source and may demand collection restrictions to ensure compliance with intelligence oversight limitations. (See appendix A.)

Public Documents

3-20. When acquiring public documents, OSINT personnel must be aware of the local environment and use a technique that is unintrusive and appropriate for the situation. These techniques include but are not limited to—

- Photographing and copying documents available in public forums such as town halls, libraries, and museums.
- Finding discarded documents in a public area such as streets, markets, and restrooms.
- Photographing documents in public areas such as banners, graffiti, and posters.
- Purchasing documents directly from street vendors, newspaper stands, book stores, and publishers.
- Purchasing documents through a third party such as a wholesale distributor or book club.
- Receiving documents upon request without charge from the author, conferences, trade fairs, direct mail advertising.

Public Broadcasts

3-21. Regional bureaus of the DNI OSC collect on regional and international broadcast networks in accordance with open-source information and intelligence requirements. Coverage of regional and international broadcasts enables OSINT personnel and organizations to use assets from already identified sources. The four techniques used to acquire information of public broadcasts are—

- **Spectrum search.** Searching the entire spectrum to detect, identify, and locate all emitters to confirm overall activity. This search provides an overview of the amount and types of activities and where they are located in the spectrum.
- **Band search.** Searching a particular segment of the spectrum to confirm overall activity. By limiting the size of the search band, the asset can improve the odds of acquiring a signal.
- **Frequency search.** Searching for radio or television frequencies.
- **Program search.** Searching for radio or television programs. Programs vary by type, content characteristics, and media format. Program surveillance verifies and expands upon initial results.

Note. For best results, OSINT personnel should use these techniques in combination rather than independently to generate intelligence knowledge. The selection of the techniques depends on the mission, the number of personnel, and capabilities.

3-22. For detailed information on collecting information from public broadcasts, see the DNI OSC.

Internet Web Sites

3-23. The four steps to acquire information on Internet Web sites are—

- Plan Internet search.
- Conduct Internet search.
- Refine Internet search.
- Record results.

3-24. For more detailed information on research using Internet Web sites, see appendix C.

Chapter 4

Producing OSINT

The Army operates in diverse environments around the world. This diversity requires proper use of publicly available information and open sources in the production of OSINT. Given the volume of existing publicly available information and the unpredictability of requests for information and intelligence requirements, OSINT personnel engaging in open-source exploitation must be fluidly aware of and flexible when producing OSINT. Effective production ensures that commanders and subordinates receive timely, relevant, and accurate intelligence. OSINT personnel produce OSINT by evaluating, analyzing, reporting, and disseminating intelligence as assessments, studies, and estimates.

CATEGORIES OF INTELLIGENCE PRODUCTS

4-1. After receiving a mission through the MDMP and commander's intent—expressed in terms of *describe*, *visualize*, and *direct*—intelligence and information requirements are identified. Personnel engaging in OSINT exploitation typically gather and receive information, perform research, and report and disseminate information in accordance with the categories of intelligence products. (See table 4-1.) OSINT products are categorized by intended use and purpose. Categories can overlap and some publicly available and open-source information can be used in more than one product. (For more detailed information on the categories of intelligence products, see FM 2-0.)

Table 4-1. Categories of intelligence products

Indications and Warning
Indications and warning are intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve an threat to the United States, U.S. ally, or U.S. citizens abroad. It includes forewarning of hostile actions or intentions against the United States, its activities, overseas forces, or allied/coalition nations (JP 2-0).
Current Intelligence
Current intelligence supports ongoing operations; it involves the integration of time-sensitive, all-source intelligence and information into concise, accurate, and objective reporting on the area of operations (AO) and current threat situation. One of the most important forms of current intelligence is the threat situation portion of the common operational picture. The intelligence officer is responsible for producing current intelligence for the unit. In addition to the current situation, current intelligence should provide projections of the threat's anticipated actions and their implications on the friendly operation. (See JP 2-0.)
General Military Intelligence
General military intelligence is intelligence concerning (1) military capabilities of foreign countries or organizations or (2) topics affecting potential U.S. or multinational military operations relating to armed forces capabilities, including threat characteristics, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness and area terrain intelligence… (excludes scientific and technical intelligence (JP 2-0). This broad category of intelligence is normally associated with long-term planning at the national level. ***Note.*** This definition was shortened for brevity. The complete definition is available in JP 2-0.

Table 4-1. Categories of intelligence products (continued)

Target Intelligence
Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance (JP 3-60). Target intelligence is the analysis of threat units, dispositions, facilities, and systems to identify and nominate specific assets or vulnerabilities for attack, reattack, or exploitation. It consists of target development and combat assessment. Target development is the systematic evaluation and analysis of target systems, system components, and component elements to identify high-value targets for potential engagement through lethal or nonlethal means. Combat assessments provide a timely and accurate estimate of the effects of the application of military force (lethal or nonlethal) and mission command warfare on targets and target systems based on predetermined objectives.
Scientific and Technical Intelligence
Scientific and technical intelligence is the product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information. Scientific and technical intelligence covers foreign developments in basic and applied research and in applied engineering techniques and scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the related research and development, and the production methods employed for their manufacture (JP 2-01).
Counterintelligence
Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities (EO 12333). Counterintelligence analyzes the threats posed by foreign intelligence and security services, and international terrorist organizations, and the intelligence activities of non-state actors such as organized crime, terrorist groups, and drug traffickers.
Estimative
Intelligence that identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations (JP 2-0). Estimates provide forecasts on how a situation may develop and the implications of planning and executing military operations. Estimative intelligence goes beyond descriptions of threat capabilities or reporting of threat activity and tries to forecast the unknown based on an analysis of known facts using techniques such as pattern analysis, inference, and statistical probability.

EVALUATE INFORMATION

4-2. Open sources are overt and unclassified. Due to these aspects of publicly available information and open sources, deception, bias, and disinformation are of particular concern when evaluating sources of information during OSINT exploitation. Information is evaluated in terms of—

- Communications.
- Information reliability and credibility.

COMMUNICATIONS

4-3. A simple communications model is typically two-way and consists of six parts:

- Intended message.
- Speaker (sender).
- Speaker's encoded message.
- Listener (receiver).
- Listener's decoded message.
- Perceived message.

4-4. The speaker and listener each have different perspectives and aspects of communications (as shown in table 4-2 on page 4-4). There are great challenges facing communicators as the message becomes encoded by the speaker and decoded by the listener.

4-5. Communications during public speaking engagements are often difficult to evaluate given the myriad of elements that can prevent a successfully transmitted message. Given the multiple elements taken simultaneously, public speaking events are subjective and can be misunderstood.

4-6. The speaker has an intended message through a verbal, nonverbal, vocal, or visual media channel or combination thereof. Within communications, the areas typically involved in preventing the true intent of the message are the sending method, environment, and receiving method. Having an understanding of these areas generally yields a greater success rate between the speaker and listener.

4-7. Verbal communication begins with a speaker imparting or interchanging thoughts, opinions, or information. This communication can be either positive or negative. The typical speaker has a communication type:

- Passive.
- Aggressive.
- Passive-aggressive.
- Assertive.

4-8. Speakers communicate verbally and nonverbally based on their beliefs, emotions, or goals. These types of communication are indicated in table 4-2 on page 4-4. It is important to understand the differences in communication styles, how they are interpreted by an audience in order to effectively communicate the message intended and avoid misunderstandings. Evaluating information acquired through public speaking venues can be challenging based on these factors. Using the table to compare these types of communication can assist collection personnel in determining the influences surrounding communicators and predicting how the messages may be perceived. Table 4-2 illustrates and provides a guideline to assist in determining the type of displayed behavior, beliefs, emotions, and goals.

Note. Table 4-2 is not intended to stand alone but used in support of all-source intelligence. Publicly available information and open sources are used to develop personality and characteristic traits of an individual. These traits include previous speeches, lectures, sermons, or statements that are used to determine a baseline of anticipated behavior and responses. There are external influences that can positively or negatively affect an individual. These external influences include but are not limited to consequences of disputing a superior's opinion, the atmosphere or setting (such as academic, religious, or political), or an impromptu public interview using a question and answer format.

INFORMATION RELIABILITY AND CREDIBILITY

4-9. OSINT personnel evaluate information with respect to reliability and credibility. It is important to evaluate the reliability of open sources in order to distinguish objective, factual information; bias; or deception. The rating is based on the subjective judgment of the evaluator and the accuracy of previous information produced by the same source.

4-10. OSINT personnel must assess the reliability and the credibility of the information independently of each other to avoid bias. The three types of sources used to evaluate and analyze received information are—

- **Primary sources.** Have direct access to the information and conveys the information directly and completely.
- **Secondary sources.** Conveys information through intermediary sources using the vernacular and summarizes or paraphrases information.
- **Authoritative sources.** Accurately reports information from the leader, government, or ruling party.

Note. Secondary and authoritative sources, such as government press offices, commercial news organizations, political campaign staffs, research center publications, newspapers, periodicals, databases, and libraries, can intentionally or unintentionally add, delete, modify, or filter the information made available to the public.

Table 4-2. Comparison of communication types

	Passive	*Aggressive*	*Passive-Aggressive*	*Assertive*
Behavior	• Keeps quiet. • Does not say what is actually felt, needed, or wanted. • Frequently puts oneself down. • Apologizes when expressing oneself. • Denies feelings of disagreements or indifferences.	• Expresses feelings and wants as though any other view is unreasonable or stupid. • Dismisses, ignores, or insults the needs, wants, and opinions of others.	• Fails to meet the expectations of others through 'deniable' means (such as forgetting or delays). • Denies personal responsibility for actions.	• Expresses needs, wants, and feelings directly and honestly. • Does not assume correctness or everyone feels similar. • Allows others to hold other views without dismissal or insults.
Nonverbal Communication	• Minimizes oneself. • Looks down, hunches shoulders, avoids eye contact. • Speaks softly.	• Enlarges oneself and appears threatening. • Eye contact is fixed and penetrating. • Voice is loud, perhaps shouting.	• Typically mimics the passive style.	• Body is relaxed, and movements are casual. • Eye contact is frequent but not glaring.
Beliefs	• Others' needs are more important. • Others have more rights. • Others' contributions are more valuable.	• Personal needs are more important and more justified than others'. • Others have no personal rights. • Personal contributions are more valuable.	• Entitled to get own way, even after making commitments to others. • Not responsible for personal actions.	• Everyone's needs are equally important. • Everyone has equal rights to be expressive. • Everyone has valuable contributions. • Responsible for personal behavior.
Emotions	• Fears rejection. • Feels helpless, frustration, and anger. • Bears resentment toward others' mistreatment. • Has reduced self-respect.	• Angry or powerful at the time of victory. • Feels remorse, guilt, or self-hatred for hurting others.	• Fears assertiveness. • Resents the demands of others. • Fears of being confronted.	• Feels positive about oneself and the treatment of others. • High level of self-esteem.
Goals	• Avoids conflict. • Pleases others at any expense. • Gives others control.	• Wins at any expense to others. • Gets control over others.	• Gets personal way without having to take responsibility.	• Self-respect is kept by everyone. • Expresses oneself without having to win all the time. • No one controls anyone else.

4-11. Nonauthoritative sources lack reliability and trustworthiness and seldom stand apart from authoritative sources. The information provided by nonauthoritative sources generally does not support topics agreed upon as being true and reliable in academia. Nonauthoritative sources also make finding additional in-depth information difficult to locate.

4-12. Nonauthoritative sources are generally unavailable and inaccessible by the public. Nonauthoritative sources are uncorroborated by multiple public sources of information. Examples of nonauthoritative sources include but is not limited to—

- Unreviewed documents from self-published Web repositories such as blogs, Wikipedia, political sites, and commercial advertising.
- Material received via uncorroborated e-mail, hearsay, or statements solely in oral form.
- Informal personal communications such as letters to the editor and opinion essays.

4-13. When evaluating sources of information to determine reliability and credibility consider—

- **Identity.** *Who* produced the information (for example a student, teacher, political organization, or reporter)?
- **Authority.** *How* much does the source know about the information?
- **Motive.** *Why* was the information published?
- **Access.** Did the source have direct access to the event or information?
- **Timeliness.** *What* is the date of the information?
- **Internal and external consistency.** Does the information contradict governmental policies among local citizens?

PROCESS INFORMATION

4-14. *Process* is an information management activity: to raise the meaning of information from data to knowledge (FM 6-0). The function of processing, although not a component of the intelligence process, is a critical element in the analyzing and producing of OSINT. Publicly available information answers intelligence and information requirements. Based on the type of information received, it must be processed before being reported and disseminated as finalized OSINT. Intelligence personnel transform publicly available information and open sources into a form suitable for processing by—

- Digitizing.
- Transcribing and translating.

DIGITIZING

4-15. OSINT personnel create a digital record of documents by scanning or taking digital photographs. Pertinent information about the document must be annotated to ensure accountability and traceability. Digitization enables the dissemination of the document to external databases and organizations, as well as enables the use of machine translation tools to screen documents for keywords, names, and phrases.

TRANSCRIBING AND TRANSLATING

4-16. A *transcript* refers to a written verbatim, native language rendering of the spoken words in an audio or video recording. Both listening and writing proficiency in the source language are essential for an accurate transcript. The transcript includes descriptions of the activity, background, and conditions that the transcriber hears in the audio and observes in the video. The linguist uses online dictionaries, gazetteers, working aids, and software to improve the transcript. Once completed, the transcription is sent to a quality control linguist.

4-17. A *translation* is not verbatim but an approximation of the literal and implied meaning of the foreign language. The linguist must be able to read and comprehend the source language, write comprehensibly in English, and choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.

4-18. During processing, a linguist creates either an extract, a summary, or a full translation of the original document or transcript into a standardized format established by unit SOPs. The linguist uses online dictionaries, gazetteers, working aids, and software to improve the translation. Once completed, the translation is sent to a quality control linguist.

4-19. Linguists perform quality control reviews of each transcription and translation to ensure both quality and consistency with established unit SOPs. A U.S. Government or military linguist should review all information that a non-U.S. Government linguist processes with exceptions involving long-term multinational partners of the United States and U.S. contractors with the requisite skills and the confidence of the command. Linguistic quality control is an important facet to process foreign publicly available information. Each transcription and translation undergoes two levels of review:

- **Quality control.** During quality control, a qualified linguist ensures that the transcription or translation is accurate, complete, free of bias, and in accordance with reporting and dissemination standards. The U.S. linguist returns the transcript or translation for correction, adds or corrects missed content, or corrects minor format errors. Upon completion of quality control, the transcription or translation is available for processing.
- **Quality assurance.** During quality assurance, a qualified U.S. linguist or OSINT analyst reviews the transcript or translation to ensure that it contains all required information and reads naturally in English. Once reviewed, the completed transcription or translation is saved to internal databases to be processed for reporting and dissemination.

ANALYSIS OF MEDIA SOURCES

4-20. Analysis of the media is the systematic comparison of the content, behavior, patterns, and trends of organic media organizations and sources of a country. Analysis of the media as an activity was developed and based on methods and experience gained during OSINT exploitation against authoritarian political systems during the World War II and Cold War eras where media was government-controlled. Publicly available information and open sources must be analyzed for proper inclusion in OSINT processing. OSINT personnel weigh media analysis against set criterion. These criterions assist OSINT personnel to discern facts, indicators, patterns, and trends in information and relationships. This involves inductive or deductive reasoning to understand the meaning of past events and predict future actions.

4-21. Comparison of trends in the content of individual media with shifts in official policy suggests that some media continues to mirror the dominant policy line. By establishing a track record for media that is vulnerable to external and internal pressure to follow the central policy line, OSINT personnel can identify potential policy shifts. Comparison of *what is said* and *what is not said* against the background of *what others are saying* and *what has been said before* is the core of media source analysis.

4-22. Media source analysis is also important in semi-controlled and independent media environments. In media environments where both official and nonofficial media are present, official media may be pressured to follow the central policy line. Analyzing media in these environments must encompass both the journalist and commentator level. It is important to establish the track record of such individuals to discover access to insider information from parts of the government or being used by officials to float policies.

Note. Differences in content between media outlets controlled by different official elites can reveal policy and leadership disputes. For example, a report on a speech by the President covered by government-controlled media may reveal differences from reports covering the same speech in either a semi-controlled or independent media environment.

4-23. The three aspects of media source analysis are—

- Media control.
- Media structure.
- Media content.

Media Control

4-24. Analyzing media environments in terms of media control requires awareness by intelligence personnel of how different elements of the media act, influence, and are of intelligence value. Careful examination of the differences in how media is handled in different types of environments can provide insight into domestic and foreign government strategies. Media environments are categorized as—

- **Government-controlled.**
  - Control over the media is centralized.
  - The dominant element of control is the government and higher tiers of political leadership.
  - Governments use censorship mechanisms to exercise control over media content prior to dissemination of information.
- **Semi-controlled.**
  - Control over the media is semi-centralized.
  - Governments exercise and promote self-censorship by pressuring media managers and journalists prior to dissemination of information.
- **Independent.**
  - Control over the media is decentralized.
  - Governments may regulate allocation of broadcast frequencies, morality in content, ownership in media markets, and occasionally apply political pressure against media or journalists.
  - Economic factors, norms of the journalist profession, the preferences of people who manage media, and the qualities of individual journalists who report or comment on the news all influence or control media content.

4-25. All media environments are controlled to some degree and therefore easier to perform media source analysis. The challenge for OSINT personnel is to determine the level, factors, and elements (see table 4-3) that elites, institutions, or individuals exercise control, how much power each possesses, and what areas are of interest to satisfy intelligence and information requirements.

Table 4-3. Level, factors, and elements of media control

Level	*Factor*	*Elements*
Political	The laws and norms governing operations of the media, officials, and the distribution of power	• Top leadership consensus • Top leaders individually • Institutions
Journalist	The degree of freedom afforded to the media by the political system that is subordinated from media executives, to media managers, and to individual journalists	• Board of directors of media companies • Individual directors • Influential shareholders • Managing editors • Department editors • Program producers • Anchors • Individual journalist
Individual	The laws and norms governing the appearance and behavior of individuals in the media	• Group of subjects or participants • Individual subject or participant

Media Structure

4-26. Media structure encompasses attributes of media material. There are structural elements that affect the meaning and significance of the content of the item and are often as important as the content itself. Analysis of these elements uncovers insights into the points of view of personnel in government-controlled, semi-controlled, and independent environments to establish the structure of media elements.

4-27. The media structural elements are—

- Selection, omission, and slant.
- Hierarchy of power.
- Format.
- Media type.
- Prominence.
- Dissemination.
- Timing.

Selection, Omission, and Slant

4-28. Selection of media items is a fundamental editorial decision at the core of news reporting. Selection includes media manager decisions about which stories are covered, which stories are not covered, and which slant (viewpoint), images, and information should be included, emphasized, deemphasized, or omitted in a news item.

Hierarchy of Power

4-29. All political systems involve a hierarchy of power (see table 4-4) that logically follows official statements issued by elements in corresponding hierarchy of authoritativeness. Authoritativeness is the likelihood that the views expressed in the statement represent the dominant viewpoint within the political system. The hierarchy is obvious at the political level—a statement by the prime minister trumps a statement by a minister. In other cases, the hierarchy may not be so obvious—a speech by the party chairman is more authoritative than the head of state.

Table 4-4. Hierarchy of media power

Information Type	*Purpose*	*Example*
Reports	Inform the viewer, listener, or reader	Authoritative or nonauthoritative based on track record
Commentary and editorials	State a position or opinion and persuade the viewer, listener, or reader	**Commentators** Authoritative: • Know pseudonym of top leader • Known advisor to Prime Minister • Associated with major party • Contributor to a major paper **Editors** Authoritative: • Ruling party's leaders or large donors • Large segment of political or financial elite • Large numbers of voters or small campaign contributors • Small segment of voters or population with special interests or radical views • Local officials and citizens
Official Statement	Declaration of policy or position by an officer or an executive body of the government or ruling party	Authoritative: • President • Secretary of State • State Department spokesperson

Format

4-30. Format consists of how media is produced and disseminated for public consumption. Format can be in the form of a live news report, a live interview, or a prerecorded report or interview that gives individuals more opportunity to influence the context delivered to consumers.

Media Type

4-31. Television is the medium with the largest potential audience in media environments and has a significant impact in shaping the impressions of the general viewing public. Television has replaced radio as the main source of news except in media environments where poverty prevents mass access to television. Fewer people may get information from newspapers and Internet news Web sites, but these people may be richer, better educated, and more influential than the general television audience. Specialized print publications and Internet Web sites reach a still smaller audience, but the audience will likely include officials and experts who that have influence on policy debates and outcomes.

Prominence

4-32. Questions to consider pertaining to prominence of media stories are—

- Does the story appear on the front page of newspapers or on the homepage of news Web sites?
- How much space is the story given?
- In what order does the story appear in the news broadcast?
- Is it featured in the opening previews of the newscast?
- How frequently is the story rebroadcast on subsequent newscasts or bulletins?
- How much airtime did it get?

Dissemination

4-33. Attention to patterns of dissemination of leader statements is important in government-controlled media environments. Leaders communicate publicly in a variety of ways such as formal policy statements, formal interviews, and impromptu remarks. By comparing the volume of media attention given to a statement, determination is made to whether the statement was intended to be taken as a pronouncement of established policy or merely as an ad hoc, uncoordinated expression prompted by narrow contextual or temporal conditions.

Timing

4-34. OSINT personnel have traditionally paid close attention to the timing of the appearance of information in the media as the information corresponds to the news cycle. A news cycle is the process and timing by which different types of media sources obtain information, incorporate or turn the information into a product, and make the product available to the public.

Media Content

4-35. Understanding the significance of media content can enhance the value of media source analysis. Media content encompasses the elements of—

- Manifest content.
- Latent content.

Manifest Content

4-36. Manifest content is the actual words, images, and sounds conveyed by open sources. One of the most important forms of media source analysis involves the careful comparison of the content of authoritative official statements to identify the policies or intentions represented. Governments, political entities, and actors use statements and information released to the media to strengthen, support, and promote policies.

4-37. Manifest content analysis of authoritative public statements is an effective tool to discern leadership intentions and attitudes. Manifest content, in order to be effective, consists of the following:

- **Esoteric communications** or "reading between the lines" are public statements whose surface meaning (manifest content) does not reveal the real purpose, meaning, or significance (latent content) of the author. Esoteric communication is particularly evident in political systems with strong taboos against public contention or in cases where sensitive issues are at stake. Esoteric communication is more formalized in some media environments than in others but is common in all political communications.
- **Multimedia content** analysis considers elements of content beyond the words used such as facial expressions, voice inflections of leaders giving a speeches or while being interviewed, or the reading of a script by a news broadcaster all provide indicators about the views of a subject or topic. These indicators assist to determine whether a statement was seriously considered, intended to be humorous, or simply impromptu.
- **Historical or past behavior** of open sources must be considered. Influences such as media outlet, journalist, newsmaker, or news broadcaster are factors beyond immediate control. Other issues such as time pressures, deadlines, or technical malfunctions, may also affect the content or context of public information. Analysts' judgments about source behavior must be made with careful consideration of previous behavior.

Latent Content

4-38. Latent content refers to the hidden meaning of a thought. Latent content can reveal patterns about the views and actions of the media controllers. These patterns and rules come from the unstated content that provides the underlying meaning of media content and behavior. When a pattern of content is changed, inference of a change in the viewpoint of the controller or a change in the balance of power among different controlling elements has occurred.

REPORT AND DISSEMINATE INFORMATION

4-39. Intelligence and information requirements satisfied through publicly available information and open sources should be immediately reported and disseminated in accordance with unit SOPs that are generally centered on intelligence requirements, information criticality, and information sensitivity.

Note. Staff personnel not directly assigned to the OSINT section also acquire information that is incorporated within the running estimate of each staff element. Close cooperation between these individuals fosters a supportive environment about *what* and *how* to report information of potential operational or intelligence value through the proper channels.

4-40. Finalized OSINT serves no purpose unless it is timely, accurate, and properly disseminated to commanders and customers in a useable form. Reporting and disseminating a finalized OSINT product that satisfies intelligence and information requirements include but are not limited to—

- Single discipline or multidiscipline estimates or assessments.
- Statements of facts.
- Evaluations of threat capabilities and limitations.
- The threat's likely COAs.

REPORTING GUIDELINES AND METHODS

4-41. Effective dissemination creates a mechanism of feedback in order to assess usefulness and predict or assess future intelligence and information requirements. The objective in reporting and disseminating intelligence and information is to provide relevancy to support conducting (planning, preparing, executing, and assessing) operations.

4-42. The basic guidelines in preparing products for reporting and disseminating information are—

- **Timely.** Information should be reported to affected units without delay for the sole purpose of ensuring the correct format.
- **Relevant.** Information must contribute to the answering of intelligence requirements. Relevant information reduces collection, organization, and transmission times.
- **Complete.** Prescribed formats and SOPs ensure completeness of transmitted information.

4-43. The three reporting methods used to convey intelligence and information are—

- **Written.** Methods include formats (spot reports), tactical reports (TACREPs), or information intelligence reports (IIRs).
- **Graphic.** Web-based report dissemination is an effective technique to ensure the widest awareness of written and graphical information across echelons. OSINT personnel can collaborate and provide statuses of intelligence requirements through Web sites. Information can also be uploaded to various databases to support future open-source missions and operations.
- **Verbal and voice.** The most common way to disseminate intelligence and information verbally is through a military briefing. Based on the criticality, sensitivity, and timeliness of the information, ad hoc and impromptu verbal communication methods are the most efficient to deliver information to commanders.

SECURITY DOMAINS

4-44. OSINT is disseminated via security domains. A security domain is an application or collection of applications that share the same authentication or authorization. A security domain determines the overall classification of an enclave of servers, computers, or networks. Networks are separated by classification in order to prevent the compromise of information. OSINT organizations can exchange publicly available information on unclassified and classified networks across echelons between Army and other armed forces as well as joint organizations and federal, state, and local government agencies.

4-45. The replication of Web sites and databases from unclassified networks to classified networks ensure publicly available information, open sources, and finalized OSINT products are reported and disseminated to intelligence and nonintelligence personnel to support unified land operations. The establishment of an effective OSINT architecture involves the proper utilization of the three primary security domains:

- Joint Worldwide Intelligence Communications System (JWICS).
- SIPRNET.
- NIPRNET.

Joint Worldwide Intelligence Communications System

4-46. JWICS is a system of interconnected computer networks used by various U.S. Government departments to transmit TS/SCI over the transmission control protocol/Internet protocol (TCP/IP) suite in a secure environment. JWICS supports the synchronization of OSINT exploitation, dissemination of OSINT and supporting metadata, and collaboration between deployed and supporting intelligence personnel.

SECRET Internet Protocol Router Network

4-47. SIPRNET is a system of interconnected computer networks used by various U.S. Government departments to transmit classified information over the TCP/IP in a secure environment. SIPRNET is the principal mission-command data network at the tactical level. The network allows access to OSINT services and products through various databases, as well as gives intelligence and nonintelligence personnel the ability to collaborate, view, submit, and track OSINT intelligence and information requirements.

Nonsecure Internet Protocol Router Network

4-48. NIPRNET is used by various U.S. Government departments to exchange information up to the sensitive but unclassified level. NIPRNET is configured to provide access to Internet-based capabilities across all DOD components. It is the domain most commonly used to conduct open-source research and produce OSINT.

REPORTING AND DISSEMINATION CONSIDERATIONS

4-49. When reporting and disseminating OSINT products, considerations include but are not limited to—

- **Classification.** When creating products from raw information, write-to-release at the lowest classification level to facilitate the widest distribution of the intelligence. Use tearline report formats to facilitate the separation of classified and unclassified information for users operating on communications networks of differing security levels. Organizations with original classification authority or personnel with derivative classification responsibilities must provide subordinate organizations and personnel with a security classification guide or guidance for information and intelligence derived from publicly available information and open sources in accordance with the policy and procedures in AR 380-5.
- **Feedback-mechanism development.** E-mail, postal addresses, rating systems, and survey forms are mechanisms that OSINT personnel can use in order to understand the information requirements for customers.
- **Intellectual property identification.** Identify intellectual property that an author or an organization has copyrighted, patented, or trademarked taken to preserve rights to the information. OSINT exploitation does not involve the selling, importing, or exporting of intellectual property. OSINT personnel engaging in exploitation should cite all sources used in reported and disseminated products. When uncertain, OSINT personnel should contact the supporting SJA office before reporting and disseminating a finalized OSINT product.
- **Use of existing dissemination methods, when and if possible.** Creating new dissemination methods can at times complicate existing dissemination methods.
- **Analytical pitfalls.** Analysts need to be cognizant that there are pitfalls when reporting and disseminating OSINT. The errors, referred to as fallacies (omission and assumption), are usually committed accidentally although sometimes they are deliberately used to persuade, convince, or deceive. Analysts must also be aware of hasty generalization, false cause, misuse of analogies and languages, biases (cultural, personal, organizational, cognitive), and hindsight. (For more information on analytical pitfalls, see TC 2-33.4.)

Appendix A

Legal Restrictions and Regulatory Limitations

Publicly available information and open sources cover a wide array of areas. Exploring, assessing, and collecting publicly available information and open sources has the potential to adversely affect organizations that execute OSINT missions. In some regards, OSINT missions could involve information either gathered against or delivered by U.S. persons. Given the scope of OSINT and its applicability within the intelligence community, having a firm awareness of intelligence oversight and its regulatory applications is necessary.

EXECUTIVE ORDER 12333

A-1. All OSINT exploitation conducted by intelligence and nonintelligence personnel must comply with the legal restrictions, policies, and guidelines outlined in EO 12333 and other associated regulations, instructions, or directives.

A-2. EO 12333 states the goal of the national intelligence effort is to provide the President and the National Security Council the necessary information on which to base decisions concerning the conduct and development of foreign defense, economic policy, and protection of U.S. national interests.

A-3. EO 12333 originated from operations that DOD intelligence units conducted against U.S. persons involved in the Civil Rights and anti-Vietnam War movements. DOD intelligence personnel used overt and covert means to collect information on the political positions of U.S. persons, retained the information in a nationwide database, and disseminated the information to law enforcement authorities.

A-4. The purpose of EO 12333 is to enhance human and technical collection techniques, the acquisition of foreign intelligence, and the countering of international terrorist activities conducted by foreign powers especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers. Accurate and timely information about the capabilities, intentions, and activities of foreign powers, organizations, and subordinate agents is essential to informed national defense decisions. Collection of such information is a priority objective, pursued in a vigorous, innovative, and responsible manner that is consistent with the U.S. Constitution and applicable laws and principles.

INTERPRETATION AND IMPLEMENTATION

A-5. AR 381-10 interprets and implements EO 12333 and DOD 5240.1-R. AR 381-10 enables the intelligence community to perform authorized intelligence functions in a manner that protects the constitutional rights of U.S. persons. The regulation does not authorize intelligence activity. An Army intelligence unit or organization must have the mission to conduct any intelligence activity directed against U.S. persons. In accordance with the Posse Comitatus Act (Section 1385, Title 18, USC), the regulation does not apply to Army intelligence units or organizations when engaged in civil disturbance or law enforcement activities without prior approval by the Secretary of Defense.

ASSIGNED FUNCTIONS

A-6. Based on EO 12333, the assigned intelligence functions of the Army are to—

- Collect, produce, and disseminate military-related foreign intelligence as required for execution of responsibility of the Secretary of Defense.
- Conduct programs and missions necessary to fulfill departmental foreign intelligence requirements.
- Conduct activities in support of DOD components outside the United States in coordination with the Central Intelligence Agency (CIA) and within the United States in coordination with the Federal Bureau of investigation (FBI) pursuant to procedures agreed upon by the Secretary of Defense and the Attorney General.
- Protect the security of DOD installations to include its activities, property, information, and employed U.S. persons by appropriate means.
- Cooperate with appropriate law enforcement agencies to protect employed U.S. persons, information, property, and facilities of any agency within the intelligence community.
- Participate with law enforcement agencies to investigate or prevent clandestine intelligence activities by foreign powers or international terrorists.
- Provide specialized equipment, technical knowledge, or assistance to U.S. persons for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies.

ARMY REGULATION 381-10

A-7. AR 381-10 enables any Army component to perform intelligence functions in a manner that protects the constitutional rights of U.S. persons. It also provides guidance on collection techniques used to obtain information for foreign intelligence and CI purposes. Intelligence activity is not authorized by this regulation.

COLLECTION OF U.S. PERSON INFORMATION

A-8. Collection, in this context, is the gathering or receiving information by intelligence personnel in the course of official duties with the intent to use or retain the information for intelligence purposes. Action must be taken to demonstrate intended use of the collected information such as producing an intelligence information report, incident report, or adding the information to an intelligence database.

A-9. There must be a link between the collection of the U.S. person information and the intelligence agency assigned mission. This link is particularly important when dealing with publicly available information, open-source information, and information data exploitation.

A-10. Army intelligence components may collect U.S. person information by lawful means but must be limited to the least intrusive means feasible and shall not violate the law (see DOD 5240.1-R). These least intrusive collection means must be attempted before utilizing more intrusive collection means such as—

- Acquisition from publicly available sources or with the consent of the U.S. person of interest.
- If proven unfeasible or inefficient, acquisition from cooperating sources.
- If proven unfeasible or inefficient, acquisition from other lawful means that do not require a warrant or Attorney General approval.
- If proven unfeasible or inefficient, an approval request for the use of techniques requiring a warrant or Attorney General approval.

A-11. Within the United States, Army intelligence components may collect foreign intelligence concerning U.S. persons by overt means when the following conditions are met:

- The foreign intelligence sought is significant and does not concern the domestic activity of the U.S. person.
- The foreign intelligence cannot be reasonably obtained by overt means.

- Collection has been coordinated with the FBI in order to prevent the disruption of current operations.

A-12. The following considerations apply to the collection of U.S. person information from the Internet:

- Army intelligence components must use government computers to access the Internet for official government business unless otherwise authorized.
- IP addresses, uniform resource locators (URLs), and e-mail addresses that are not associated with a U.S. person may be acquired, retained, and processed by Army intelligence components without making an effort to determine association with a U.S. person as long as the component does not engage in analysis focused upon specific addresses.

A-13. AR 381-10 does not authorize the collection of any information relating to a U.S. person solely because of personal lawful advocacy of measures opposed to government policy as embodied in the First Amendment to the U.S. Constitution. The First Amendment states that Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

RETENTION OF U.S. PERSON INFORMATION

A-14. *Retention* refers only to maintaining information about U.S. persons that the Army intelligence component can retrieve by the person's name or other personal identifying data. AR 381-10, procedure 3, describes the kinds of U.S. person information that an Army intelligence component may knowingly retain without the individual's consent.

A-15. AR 381-10 authorizes the retention of U.S. person information under the following criteria:

- Information properly collected in accordance with AR 381-10, procedure 2.
- Army intelligence components acquired the information incidental to an otherwise authorized collection activity, and retained the information if it—
  - Could have been collected intentionally under the provisions of AR 381-10, procedure 2.
  - Is necessary to understand or assess foreign intelligence or CI.
  - Is foreign intelligence or CI collected from authorized electronic surveillance.

Note. *Electronic surveillance* refers to the acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

  - Is incidental to authorized collection and may indicate involvement in activities that may violate federal, state, local, or foreign law.
- Information relating to functions of other Army activities, DOD components, or non-DOD agencies. The information pertains solely to the functions and responsibilities of other activities, components or agencies, and is retained only as necessary to transmit the information to that agency. The transmittal is filed and destroyed under general correspondence records management. Army intelligence components will not retain the information in intelligence databases or repositories.

A-16. *Temporary retention* refers to the authorization for Army intelligence components to retain information up to 90 days, solely to determine if the information is, in fact, retainable under this regulation. The 90-day period starts upon receipt of the information.

A-17. *Other information* retained by Army intelligence components must be reported for oversight purposes and for necessary subsequent proceedings.

A-18. Access to U.S. person information retained in intelligence files, databases, and repositories is limited to those with a need to know the information. U.S. person information in intelligence files, databases, and

repositories is retained in accordance with disposition criteria in AR 25-400-2. Intelligence components will review intelligence files and databases annually. Intelligence components will specifically review U.S. person information to ensure its retention is still necessary to an assigned function. This ensures U.S. person information is not held beyond established disposition criteria, is retained for an authorized function, and was not retained in violation of this regulation. This does not apply to the Investigative Records Repository or other authorized long-term records holding areas.

DISSEMINATION OF U.S. PERSON INFORMATION

A-19. *Disseminate*, an information management activity, refers to communicating relevant information of any kind from one person or place to another in a usable form by any means to improve understanding or to initiate or govern action (FM 6-0). In other words, dissemination is the delivery of intelligence to users in a suitable form with application of the intelligence to appropriate missions, tasks, and functions. AR 381-10, procedure 4, governs the types of information regarding U.S. persons that Army intelligence organizations may disseminate without the person's consent outside the component which collected and retained the information.

QUESTIONABLE INTELLIGENCE ACTIVITY

A-20. Questionable intelligence activity occurs when intelligence operations potentially violate—

- Laws.
- EOs.
- Presidential directives.
- DOD or Army policies.

A-21. Intelligence personnel should report questionable intelligence activity through the chain of command, the inspector general, or directly to the Assistant to the Secretary of Defense for Intelligence Oversight in accordance with AR 381-10. The following are examples of questionable intelligence activity on improper collecting, retaining, or disseminating of U.S. person information:

- Collecting and gathering information about U.S. domestic groups not connected with a foreign power or international terrorism.
- Producing and disseminating intelligence threat assessments containing U.S. person information without a clear explanation of the intelligence purpose for which the information was collected.
- Collecting and gathering U.S. person information for force protection purposes without determining if the intelligence function is authorized.
- Collecting and gathering U.S. person information from open sources without a logical connection to the mission of the unit.

A-22. AR 381-10 directs intelligence organizations to refer questions concerning the interpretation of the instructions on collection, retention, and dissemination of U.S. person information to the local SJA's office.

ASSISTANT DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE FOR OPEN SOURCE

A-23. The responsibilities of the ADDNI/OS include—

- Exercising the integration, evaluation, and oversight for the NOSE.
- Providing strategic oversight of and guides strategic involvement of OSINT.
- Chairing the National Open Source Committee (NOSC) and Open Source Board of Advisors.
- Overseeing the DNI OSC and the distributed NOSE.
- Ensuring the integration of the open-source collection management strategy.
- Developing oversight of the NOSE.
- Overseeing interagency sharing of open-source information.

INTELLIGENCE COMMUNITY

A-24. The responsibilities of the intelligence community include—

- Developing programmatic oversight and evaluation to be centralized under the ADDNI/OS.
- Supporting all intelligence disciplines.
- Establishing appropriate source and information validation and verification procedures of all open-source exploitation efforts.
- Developing metrics for overall open-source activities.
- Making all open-source information, products, and services available throughout the intelligence community.

NATIONAL OPEN-SOURCE COMMITTEE

A-25. The NOSC provides guidance to the NOSE. The responsibilities of the NOSC include—

- Developing appropriate operational standards for source or information verification, tradecraft, and training.
- Developing science and technology standards for metadata tagging and storage.

DIRECTOR OF NATIONAL INTELLIGENCE OPEN-SOURCE CENTER

A-26. The DNI OSC serves to advance the exploitation of open-source information through acquisition, procurement, analysis, and dissemination of products and services. The responsibilities of the DNI OSC include—

- Facilitating open-source exploitation for U.S. Government partners and customers.
- Securing appropriate licensing agreements for open-source customers.
- Developing open-source programs.
- Training personnel to properly exploit open-source information in accordance with security practices.

Appendix B

Cyberspace Internet Awareness

Intelligence and nonintelligence personnel conducting open-source research must be aware of the digital operational environment by minimizing and reducing cyber "footprints," practicing effective cyber OPSEC, utilizing safe online surfing techniques and habits, and understanding that embedded metadata can be contained in documents.

CYBERSPACE SITUATIONAL AWARENESS AND CYBER SECURITY

B-1. More than any other intelligence discipline, research involving publicly available information and open sources could unintentionally reveal CCIRs. Open-source research sometimes requires access to Internet Web sites that block browsing sessions originating from *.mil* or *.gov* sources. In the areas of computer information assurance and Internet security, internet awareness is needed in order to be effective, aggressive, and to successfully conduct open-source research and exploitation. Unjustified Internet Web-site restrictions have the potential to severely impede acquiring and the subsequent processing, reporting, and disseminating of publicly available information and open sources.

B-2. Awareness is the beginning of effective cyber security. Computers transmit machine specifications such as operating system, type of version of each enabled program, security levels, a history of Web sites visited, cookie information, user preferences, IP addresses, enabled languages, and referring URL when searching the Internet. Visitors are frequently redirected to alternate Web sites based on search criterion, location, language, and time the search is conducted.

B-3. The Internet is described as a "network of networks" due to the hundreds of thousands of interconnected networks consisting of millions of computers. Computers and users connected to the Internet are identified by a system-specific IP address that designates location. The IP address serves as the address where transferred information and datum is delivered. The concern therein rests in the understanding that while visiting nonstandard or questionable Internet Web sites in accordance with official duties, sensitive unit information could inadvertently be revealed.

B-4. *Cyberspace* is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, embedded processors, and controllers (JP 1-02). The Army operates in and through the cyberspace domain, using and managing the electromagnetic spectrum as a holistic and integrated part of unified land operations. Personnel engaging in OSINT exploitation need to understand the cyberspace environment in order to develop and identify outcomes-based, integration-focused, and resource-informed solutions for cyber situational awareness concerns.

B-5. *Cyber situational awareness* is the knowledge of friendly, neutral, and threat relevant information regarding activities in and through cyberspace and the electromagnetic spectrum (FM 1-02). Cyberspace and cyber security involve increasing cyber situational awareness by—

- Identifying threat operations to determine the effect on friendly operations and countermeasures.
- Determining how to use cyberspace to gain support from friendly and neutral entities.
- Determining how to gain, maintain, and exploit technical and operational advantages.

B-6. There are OPSEC and computer security risks to searching and interacting with Internet Web sites. Searching the Internet can compromise OPSEC by leaving "digital footprints" on visited Web sites. "Surfing" on Internet Web sites can compromise computer security by exposing the computer and network to malicious software (such as viruses, worms, and Trojan Horses) or unauthorized access. Intelligence personnel must be vigilant to potential threats, use only authorized hardware and software, and comply with established unit operations security measures.

B-7. URL information from the previous Web site visited is frequently an OPSEC issue and it identifies characteristics and interests of the user. While necessary for an effective research, the use of specific and focused search terms have potential OPSEC implications.

Cyber Security Example

If the user enters the search terms [bradley us army], the referring URL from the Google hit list would be: http://www.google.com/search?hl=en&q=bradley+us+army. This tells the visited site that the user is searching in English (hl=en) for information on Army General of the Army Omar N. Bradley or the U.S. Army's Bradley infantry fighting vehicle.

B-8. All actions on a Web site are logged and saved. The information is saved and linked to what is referred to as *cookie data*. User actions include but are not limited to—

- Words typed in search parameter fields.
- Drop-down menu choices.
- Check boxes.
- Web site movement patterns such as changing domain name or Web site address.

B-9. On many Web sites, information that the user provides or fills in becomes part of the Web site and is searchable. Key information to avoid sharing includes but is not limited to—

- Military plans.
- Operations.
- Exercises.
- Maps and charts.
- Locations.
- Schedules.
- Equipment vulnerabilities, capabilities, and shortfalls.
- Names and related numbers:
  - Telephone numbers.
  - Birth dates.
  - Identification numbers.

B-10. Traditional and irregular threats are disruptive in nature and use the cyberspace domain to conduct operations against the Army. These threats are innovative, networked, and technologically adept. These threats capitalize on emerging technologies to establish and maintain a cultural and social advantage leveraging areas, to include but not limited to mission command, recruiting, logistics, fund raising and laundering, IO, and propaganda.

B-11. When engaged in OSINT exploitation utilizing computer systems and Internet usage, cyberspace awareness assessments should be developed and cover areas including but not limited to network vulnerabilities, network threats (physical and virtual), and future risks.

B-12. For more detailed information about cyber security threats and tips see the U.S. Computer Security Readiness Team's Web.

Appendix C

Basic and Advanced Internet Search Techniques

The ability to search the Internet is an essential skill for open-source research and acquisition. The Internet, considered a reconnaissance and surveillance research tool, provides access to Web sites and databases that hold a wide range of information on current, planned, and potential areas of operation. The exponential growth in computer technology and the Internet has placed more publicly available information and processing power at the fingertips of Soldiers than ever before. A body of knowledge on culture, economics, geography, military affairs, and politics that was once inaccessible to some degree, now rest in the hands of high school and college students—future leaders of the Army.

THE WORLD WIDE WEB AND DEEP WEB

C-1. The Internet is a dynamic information environment consisting of stationary and moving virtual and target Web sites containing a mixture of old and new content. There are numerous virtual databases that grow at exponential rates. Keeping pace with technology is an enduring challenge for personnel that engage in OSINT exploitation utilizing the WWW and Deep Web.

WORLD WIDE WEB

C-2. The WWW is indexed by standard search engines. Standard search engines are typically incapable of accessing or retrieving the type of information necessary for conducting effective open-source research. The total amount of Internet information is estimated to be over 7,500 terabytes and continues to increase. Of this amount, customary search engines on the Internet are estimated to index only one-quarter of the information. Considered a very large amount of information, it only represents a fraction of the amount of open-source information available during research utilizing publicly available information. The other three-quarters (or roughly 5,625 terabytes) are contained on what is called the Deep Web.

THE DEEP WEB

C-3. The *Deep Web* refers to content that is not part of the traditional WWW. This content is estimated to be more than twice the content saved and accessible on the traditional WWW. The content and information contained on the Deep Web is designed around Web-based databases. Unlike the WWW, the Deep Web is not indexed. Nonstatic Web sites and databases located on the Deep Web cannot be accessed or indexed by traditional search engines. The Deep Web offers a tremendous amount of resources. Deep Web resources could fall into one or more of the following:

- **Dynamic content.** Web pages that are returned in response to a submitted query.
- **Unlinked content.** Web pages that are not linked to other Web pages that prevent standard Web crawling programs from accessing the content.
- **Private Web content.** Web pages without backlinks or inlinks.
- **Limited access content.** Web sites that limit access to information.
- **Nonhypertext markup language content.** Textual content encoded in multimedia files that are not handled by search engines.

SEARCH ENGINES

C-4. Search engines are the primary tools that personnel engaging in OSINT activities use when conducting research of publicly available information through open sources. OSINT personnel use search engines and search terms to locate text, images, and information on thousands of Web sites. Technically, search engines are actually searching through the index of Web sites. Commercial and government search engines vary in what parameters are searched, how searches are processed, and how search results are displayed. Most search engines use programs called *web crawlers* to build indexed databases. A web crawler searches Internet Web sites and files and saves the results in a database.

C-5. Most search engines use relevancy formulas to display results in a specific order with a brief description and hyperlink to the reference Internet file. Relevancy formulas evaluate how well the query matches the request. Relevancy formulas are significant to the user as search engines evolve and will not all yield similar results. The placement of keywords yield different results if rearranged due to more emphasis placed on one word over another. As search engines have evolved, some have become adept at finding specific types of information, such as statistical, financial, and news, more effectively. To overcome this specialization, software engineers have developed metasearch engines that allow the user to query more than one search engine at a time.

Search Engines

If a particular search engine cannot accommodate phrases in quotation marks or other types of Boolean functions, then the metasearch engine eliminates that function from the search. The resulting search then becomes too broad and less useful than a well-formatted search using a specialized search engine.

C-6. With an understanding of how search engines work, intelligence personnel—

- Conduct initial searches using unique keywords and combinations.
- Apply Boolean logic to improve search parameters.
- Conduct follow-on searches using natural language.

SEARCH BY KEYWORD

C-7. In keyword-based searches, OSINT personnel should consider what keywords are unique to the information being researched. Keywords should be balanced to yield relevant results without an over abundance of irrelevant information. Common words to be avoided include—

- A.
- An.
- And.
- The.

C-8. These words should be avoided in search terms unless part of the title of a book or article. Most search engines ignore common words. For example, if looking for information about Russian and Chinese tank sales to Iraq, do not use *tank* as the only keyword in the search. Instead, use additional defining words such as "Russian Chinese tank sales Iraq."

BOOLEAN LOGIC OPERATORS, CONNECTORS, AND DELIMITERS

C-9. When searching the Internet, the vast data available can be searched according to the rules of computer database searches. The logical relationship between search terms is referred to as *Boolean logic*. This method of searching provides options for constructing logical relationships among search terms using local operators, connectors, and delimiters.

C-10. Boolean logic operators, connectors, and delimiters assist intelligence personnel in establishing relationships between keywords to improve search activities.

Example of Using Boolean Logic Operators

Applying the following example, using the operators (see table C-1), the search engine searches for *Russian* and *tank* together when placed within parentheses—for example, *(Russian tank)*—and to exclude Chinese tank sales from the search result, use *(Russian tank) NOT (Chinese tank) sale Iraq* in the search. Intelligence personnel can also use a *NEAR* search when the relationship and the distance between the terms are well established. For example, if intelligence personnel are looking for incidents of tank sales in Baghdad and news articles normally place the name of the location within five words of *tank sales* in the title of the body of the article then use *tank sales NEAR/5* in the search.

Table C-1. Boolean logic operators, connectors, and delimiters

Function	*Boolean*	*Example*
Must be present *	AND	Chemical AND weapon chemical *weapon
Must not be present	NOT	Africa NOT Sudan
May be present	OR	Chemical OR biological
Complete phrase	* *	*Chinese tank sales to Iraq*
Nested	( )	(Shining Path)
Near**	NEAR	"White House" NEAR "airspace incursion"
Wildcards	Word* or *word	Gun* (gunpowder)

Note. Boolean searches may not work on all search engines. Using the "Advanced Search" option is available on many web browsers. Advanced search pages include fields to fill in such as "Find web pages that contain all these words;" "this exact wording or phrase;" or "Do not show pages including any of these words."

SEARCH IN NATURAL LANGUAGE

C-11. An alternative to using a keyword search is the *natural language* question format as most of the major search engines allow this capability. OSINT personnel obtain the best results when the question contains good keywords. One of the major downsides to this technique is the large number of results. If the needed information is not found in the results of the first few pages the question should be refined to initiate a new search using different parameters.

INTERNET WEB SITES

C-12. The four steps used to exploit publicly available information and open sources on Internet Web sites are—

- Plan Internet search.
- Conduct Internet search.
- Refine Internet search.
- Record results.

PLAN INTERNET SEARCH

C-13. OSINT personnel use an understanding of intelligence and information requirements to plan Internet searches. Intelligence and information requirements help to determine what information to search for, where to search, and provides the focus and initial keywords used in the search. After determining the focus and keywords, OSINT personnel use Internet browsers and search engines to connect to a previously identified Internet Web site.

Keyword Searches

If a unit is planning a humanitarian assistance operation in a particular country, intelligence requirements may be to locate refugee concentrations in that country. The task for an OSINT cell could include to locate—

- Humanitarian relief organizations operating food distribution centers.
- Population centers in the country.
- Concentrations of militia forces.
- Areas of militia operations within in the last 30 days.

Useful search terms would include—

- Refugee.
- Humanitarian relief.
- Militia.
- Water sources.
- Food distribution.

Locating possible indicators of where refugees may or may not concentrate include—

- Nongovernmental organization aid centers.
- Food.
- Water.
- Hostile militia forces.

Based on intelligence requirements, the search objective is to locate refugee concentrations based on the position of supplies and militia forces in the country.

CONDUCT INTERNET SEARCH

C-14. OSINT personnel conduct an initial search of likely sources using related terms or subject matter for the research question. The initial search is the first of potentially many subsequent searches for data and information that is retrieved and recorded in accordance with the research plan. Once retrieved, the information is integrated into the appropriate digital or analog database. OSINT personnel should avoid the temptation of using only one search engine as each has strengths and weaknesses. Organizational standards, research experience, and peer recommendations typically guide the selection of which search engine to use.

Note. If the information is not identified using multiple search engines within 30 minutes, it is possible that the information does not exist on the Internet, has not been indexed, or is not in a retrievable format.

REFINE INTERNET SEARCH

C-15. Typically, the first few pages of search results are the most relevant. Based on these pages, OSINT personnel exploit the initial search results for relevancy and accuracy for follow-on searches to determine if the results satisfied the intelligence or information requirement. Initial Internet searches can yield undesired results to satisfy intelligence and information requirements. OSINT personnel typically use measures to refine Internet results, including but not limited to—

- Reordering search terms.
- Adjusting upper or lower case.
- Searching within results.
- Searching in the cache and archive.
- Web site domains.
- Changing spelling and grammar.
- Using keyword variants.
- Searching by field.
- Truncating the URL.

Reorder Search Terms

C-16. Search engines may place a higher value on the first word or words in a multiple word or phrase search string. For example, changing the word order from *devices explosive* to *explosive devices* may yield different search results.

Change Spelling and Grammar

C-17. Search engines attempt to match the exact spelling of the words in the search string. There are search engines that recognize alternate spellings or prompt the user to correct common misspellings. For example, changing the spelling of a word from the American-English *center* to the British-English *centre* may yield different results. Boolean logic can also be used in order to circumvent potential spelling mistakes. Additionally, changing the spelling of a transliterated name generates different results that may be useful depending upon the objective of the search, such as the spelling variations of the name—

- *Al-Qaeda*.
- *al-Qaida*.
- *al-Qa'ida*.
- *el-Qaida.*
- *al Qaeda.*

Adjust Upper or Lower Case

C-18. Search engines may or may not support case sensitive searches. Some search engines attempt to match the word exactly as entered in the search. Most searches should be all lowercase letters. When looking for the name of a person, geographical location, title, or other normally capitalized word, use a case sensitive search engine. For example, changing the case of a word such as *java* to *JAVA* changes the results from coffee Web sites to software program Web sites.

Use Keyword Variants

C-19. OSINT personnel use terms that are culturally or geographically common. Using variants of a keyword such as changing *policeman* to *cop*, *bobby*, *gendarme*, *carabiniere*, *policía*, *politzei*, or other forms may improve search results.

Search Within Results

C-20. If the initial or follow-on search produces good but still unsatisfactory results, OSINT personnel can search within these results to produce a higher probability of finding the desired results. Most search engines display an option such as *search within these results* or *similar pages* to assist the user.

Search by Field

C-21. In a field search, OSINT personnel look for keywords within the URL as opposed to searching the Internet. This is typically done when the search engine returned a large number of results. While capabilities vary by search engine, some of the common field search operators are—

- **Anchor.** Searches for Web sites with a specified hyperlink.
- **Domain.** Searches for specific domains.
- **Like.** Searches for Web sites similar or related in some way to specified URLs.
- **Link.** Searches for specific hyperlinks embedded in a Web site.
- **Text.** Searches for specific text in the body of the Web site.
- **URL.** Searches for specific text in complete Web site addresses.

Search in Cache and Archive

C-22. Sometimes a search or an attempt to search with results returns a URL that matches exactly the search objective but when accessed the Web site is no longer active. If the search engine captures data as well as the URL locator, select the cached link to access the original data. OSINT personnel can also search an Internet archive Web site, such as www.archive.org, for the content. OSINT personnel need to have awareness that this information is historical and not subject to update by original creators.

Truncate the Uniform Resource Locator

C-23. Based on the topic of the information or intelligence requirement, OSINT personnel can manually search within the results by truncating the URL to a Web site. OSINT personnel work backwards from the original search result to the Web site containing the desired information or database by deleting the end segments of the URL at the forward slash. See manually truncating a URL example in table C-2.

C-24. There are also URL shortening assistance Web sites that redirect a user from a short URL (such as in the second part of table C-2) to a much longer URL serving as the actual address of the Web site. These are often used in social media services like Twitter due to the character restrictions placed on users.

Table C-2. Truncating and shortening uniform resource locators

Manually Truncating a Uniform Resource Locator (URL)	
Example URL to truncate	http://www.website.com/default.aspx?utm_source=twitter&utm_medium=social-media
Delete all but the main part of the Web site address	http://www.website.com/
Shortening URLs Using Shortening Assistance	
Example URL to paste into shortening assistance Web site	http://www.amazon.com/Kindle-Wireless-Reading-Display-Globally/dp/B003FSUDM4/ref=amb_link_353259562_2?pf_rd_m=ATVPDKIK X0DER&pf_rd_s=center-10&pf_rd_r=11EYKTN682A79T370AM3&pf_rd_t=201&pf_rd_p=1270985982&pf_rd_i=B002Y27P3M
The shortening Web site produces the example URL to use in social media settings or in e-mail	http://tinyurl.com/KindleWireless

Web Site Domains

C-25. Domain names on the Internet are identifying labels and are used in various networking contexts. They are used as simple identification labels to indicate ownership or control of a resource. With the millions of URLs on WWW, intelligence personnel are faced with a myriad of Web sites that may or may not produce or maintain the information presented in that domain. Certain domains, such as those listed in table C-3, are consistently reliable as being administered and authored by those types of organizations.

Note. OSINT personnel exploiting publicly available information and open sources must not take *.org*, *.info*, or *.net* extensions as necessarily produced by a bona fide organization for that domain.

Table C-3. Common Web site domains

Domain	*Description*
.aero	Reserved for members of the air transport industry
.biz	Restricted to businesses
.com	Unrestricted top-level domain intended for commercial content
.coop	Reserved for cooperative associations
.edu	Reserved for postsecondary institutions accredited by an agency on the U.S. Department of Education's list of Nationally Recognized Accrediting Agencies
.gov	Reserved exclusively for the U.S. Government
.info	Unrestricted top-level domain
.int	Used only for registering organizations established by international treaties between governments
.jobs	Reserved for human resource managers
.mil	Reserved exclusively for the U.S. military
.museum	Reserved for museums
.name	Reserved for individuals
.net	Reserved for networking technological individuals
.org	Intended for noncommercial use but open to all communities
.pro	Restricted to credentialed professionals and related entities

OPEN-SOURCE DATABASES, SOFTWARE, AND TOOLS

C-26. There are numerous COTS software applications, tools, and databases that are searchable using query words for research. Search engines used for research include but are not limited to—

- **Google Scholar.** Google Scholar provides a simple way to broadly search for scholarly literature. From one place, searches expand across many disciplines and sources that include articles, theses, books, and abstracts. Google Scholar helps locate relevant work across the world of scholarly research.
- **Spokeo.** Spokeo specializes in organizing people-related information (names, addresses, phone numbers) from phone books, social networks, marketing lists, business Web sites, and other public sources. Spokeo uses algorithms to piece together data into coherent profiles.
- **Blog Pulse.** BlogPulse is an automated trend discovery system for blogs by applying machine-learning and natural language processing techniques.
- **Pipl.** Pipl query engine helps locate Deep Web pages that cannot be found on regular or standard search engines. Pipl uses advanced language-analysis and ranking algorithms to retrieve the most relevant information about an individual.
- **Monitter.** Monitter is a browser-based Twitter search engine. Monitter displays three constantly updated keyword searches parallel to each other in your browser.
- **Maltego.** Maltego is a forensic application that offers data-mining and gathering of information into packaged representations. Maltego allows the identification of key relationships between information and identify previously unknown relationships.

GOOGLE TOOLS

C-27. Google tools assist in exploiting publicly available information and open sources through—

- Query words.
- Query types.
- Query modifiers.

QUERY WORDS

C-28. Google supports several advanced Boolean logic operators, which are query words that have special meaning to Google. Typically query types and query modifiers, when applied by operators, modify the parameters and results of search engines.

QUERY TYPES

C-29. Four categories covering most Web-search queries include—

- **Cache.** If other words are included in the query, Google highlights those words within the cached document. For example, [cache:www.google.com web] shows the cached content with the word "web" highlighted.
- **Link.** The query [link:] lists Web pages that have links to the specified Web page. For example, [link:www.google.com] lists Web pages that have links pointing to the Google homepage.
- **Related.** The query [related:] lists Web pages that are similar to a specified Web page. For example, [related:www.google.com] lists Web pages that are similar to the Google homepage.
- **Info.** The query [info:] presents some information that Google has about that Web page. For example, [info:www.google.com] shows information about the Google homepage.

QUERY MODIFIERS

C-30. Research using a specific search query can be modified using the following modifiers:

- **Site.** If [site:] is included in the query, the results are restricted to those Web sites in the given domain. For example, [help site:www.google.com] finds pages about *help* within www.google.com. [help site:com] finds pages about *help* within *.com* URLs.
- **Allintitle.** If a query starts with [allintitle:], the results are restricted to those Web sites with all of the query words in the title. For example, [allintitle: google search] returns only documents that have both *google* and *search* in the title.
- **Intitle.** If [intitle:] is included in the query, the results are restricted to documents containing that word in the title. For example, [intitle:google search] returns documents that have the word *google* in their title, and have the word *search* anywhere in the document (title or not). Putting [intitle:] in front of every word in the query is equivalent to putting [allintitle:] at the front of the query: [intitle:google intitle:search] is the same as [allintitle: google search].
- **Allinurl.** If a query starts with [allinurl:], the results are restricted to those Web sites with all of the query words in the URL. For example, [allinurl: google search] returns only documents that have both *google* and *search* in the URL.
- **Inurl.** If [inurl:] is included in the query, the results are restricted to those documents containing that word in the URL. For example, [inurl:google search] returns documents that have the word *google* in their URLs, and have the word *search* anywhere in the document (URL or not). Putting "inurl:" in front of every word in the query is equivalent to putting "allinurl:" at the front of the query: [inurl:google inurl:search] is the same as [allinurl: google search].

INTERNATIONAL INTERNET WEB SITES

The number of non-English-language users on the WWW and Deep Web are increasingly surpassing English users. This international reach results in the creation of foreign Web sites with specific country

codes. OSINT personnel must be aware of the origin of foreign Web sites and the potential vulnerabilities inherent in accessing these Web sites.

INTERNET SEARCH TECHNIQUE CONSIDERATIONS

C-31. When conducting Internet basic and advanced searches, technique areas that should be considered are—

- **COTS software.** When utilizing COTS tools and software, OSINT personnel must consider the tools and software utilized in accordance with unit SOPs, guidelines and policies.
- **Cataloging and archiving.** Due to the nature of Internet Web sites and the lack of control restrictions, Web sites can be removed from the WWW without prior notice.
- **Authorship.** Open-source products can oftentimes be authored through anonymity.
- **Identified Web sites and portals.** Familiarization of publicly available information generally results in standardized Web sites and portals used for research. Web sites and portals are subjective in nature due to the biases and perceptions of the Web site administrator or designer.
- **Off-line browsers.** Due to the volatile and unpredictability of Web sites, effective use of off-line browsers can enhance Internet research.

INTERNET AND OPERATIONS SECURITY VULNERABILITIES

C-32. The intent of OSINT is to exploit publicly available information and open sources without revealing user or organizational identities. Exploiting publicly available information and open sources is typically anonymous and conducted with a low risk of potential OPSEC compromise. There are inherent threats when conducting research on the WWW and Deep Web. Open-source research can compromise OPSEC and reveal user identification and the location of the computer systems through IP addresses. Any number of system disruption tools can render open-source collection activities ineffective. These include but are not limited to—

- **Viruses.** Computer codes that attach to computer programs. Once attached, viruses infect other computer systems through replication.
- **Trojan horses.** Computer programs that prevent user-activated commands.
- **Worms.** Self-contained computer programs that infect computers through replication. Worms create traffic on Web sites with the objective of decreasing visibility by conducting denial of service attacks.

Note. OSINT personnel should consult with organic unit's S-6/G-6 and information assurance personnel for current threats and guidelines to ensure that operating systems and browsers are using the most current security patches, antivirus, and antispyware protection software.

Appendix D

OSINT Contributions

The vignettes and discussions in this appendix illustrate how integrated OSINT supports or contributes to—

- Unified land operations and associated missions and tasks.
- Other intelligence disciplines.
- Other functions, such as site exploitation (SE) and source vetting.

The examples provided do not constitute a comprehensive list.

SUPPORT TO TARGETING, COUNTERINSURGENCY, AND IMPROVISED EXPLOSIVE DEVICE DEFEAT OPERATIONS

D-1. As a result of target development, OSINT contributes to the products such as target lists, target folders, target briefs, and exploitation requirements. The following vignette describes one situation where OSINT contributes to targeting. (For more information on targeting see FM 3-60.)

Example of OSINT Contributions to Targeting

The United States is going to war against Country X. The United States has an objective to limit the counterstrike capabilities of Country X. There is a significant military stockpile that Country X purposely collocated by a religious center. Should the United States destroy the stockpile knowing there is a great chance that the symbolic religious center will be destroyed as collateral damage?

OSINT can support this objective by providing information such as—

- What is the religious background of the population living near the religious center?
- Is the religious center culturally significant?
- Is it an historical landmark?
- What is the makeup of the congregation?
- What are the normal times that people congregate?
- What are the technical descriptions of the equipment in the stockpile?

D-2. In support of counterinsurgency operations, publicly available information is valuable for understanding the operational environment. It is often more useful than any other discipline for understanding public attitudes and public support during counterinsurgency operations. Publicly available information is also an important means of determining the effectiveness of inform and influence activities among the local populace. Monitoring public media benefits counterinsurgency operations. If possible, monitoring should occur at every echelon in support of PIRs. Each echelon should monitor the media that contain information relevant to operations at that echelon. For instance, at the corps level, major news networks should be monitored; in contrast, at the tactical level, local newspapers or radio stations may be more important. (For additional information on counterinsurgency operations, see FM 3-24.)

D-3. In support of improvised explosive device (IED) defeat operations, publicly available information can be used to—

- Collect and monitor IED-related information discussed during events that are open to the public or occur in public areas.
- Collect and monitor IED-related information that is located in any recorded public document (such as newspapers, magazines, leaflets, brochures, posters).
- Collect and monitor IED-related information that is broadcast for general public consumption to all receivers or terminals within a computer, radio, or television network.
- Monitor threat or IED-related Internet Web sites that may provide indications and warning of threat intentions, capabilities, activities, and responsible entities for a specific incident.

D-4. See FM 3-90.119 for more information on combined arms IED defeat operations.

SUPPORT TO OTHER INTELLIGENCE DISCIPLINES

D-5. Publicly available information and open sources developed as finalized OSINT can also support other intelligence disciplines.

HUMAN INTELLIGENCE

D-6. OSINT supports HUMINT collection operations by providing open-source materials to the appropriate J/G/S-2X and intelligence community agencies and liaison officers. These materials include but are not limited to—

- Maps.
- Charts.
- Phone directories.
- Business directories.
- Newspapers.
- Video and audio media (including tapes and CDs).

D-7. For further information on HUMINT collector operations see FM 2-22.3.

SIGNALS INTELLIGENCE AND GEOSPATIAL INTELLIGENCE

D-8. The following vignette describes a specific situation where OSINT directly contributes to signals intelligence (SIGINT) and geospatial intelligence (GEOINT).

Example of OSINT Contributions to SIGINT

The signals officer for Unit C is preparing an assessment based on an upcoming operation. The signals officer does not have access to classified systems. Unit C is preparing to conduct operations in an area where the media is state-controlled by a totalitarian government.

OSINT can support the signals officer by providing information such as—

- The identification of locally televised channels along with supporting components and systems.
- Web sites used to communicate to the local populace.

Example of OSINT Contributions to GEOINT

During mission planning, Engineer D is observing the potential effects of building a new rail system. The rail system will bisect an agricultural community located along a primary irrigation path. There is an increased potential that the rail system will disrupt and cause damage to the irrigation canals. There are time constraints preventing the request of satellite imagery in order to provide an overhead view of the area for assessment. If the rail system damages the irrigation canals, the results will more than likely destroy relationships established between unit leadership and tribal leaders.

OSINT can support imagery intelligence (IMINT) by providing information such as Google Earth and other COTS imagery to identify alternative waterways, future irrigation draining areas, and water paths in the event of flooding.

TECHNICAL INTELLIGENCE AND COUNTERINTELLIGENCE

D-9. Publicly available information supports technical intelligence (TECHINT) efforts in significant ways. Although adversaries and potential threats attempt to closely protect capabilities and vulnerabilities as well as intent, the inevitable results of technological advances, such as the Internet and Google Earth, provide exploitation opportunities into even the most secretive nations and organizations. (For further information on TECHINT, see TC 2-22.4.)

D-10. In support of CI, publicly available information can be used to obtain information that satisfies PIRs or other standing CI collection requirements. The collectors of Army OSINT are the military intelligence brigades. Military intelligence Soldiers receive OSINT training at their schools, as applicable. Upon arrival at permanent duty stations, unit training should include OSINT training relevant to duty assignments. (For more information on CI, see FM 2-22.2.)

Appendix E

OSINT Organizations

OSINT expands the entire breath of the intelligence community from the national level to the tactical level of operations. U.S. Government organizations, such as DOD, law enforcement agencies, and others that collect, acquire, exploit, analyze, disseminate, or utilize OSINT as a customer include—

- Defense Open Source Council (DOSC).
- INSCOM.
- DA IIS.
- DNI OSC.
- Open Source Academy.
- ASD.
- FBI.
- Federal Research Division (FRD), Library of Congress.

DEFENSE OPEN SOURCE COUNCIL

E-1. The DOSC is the primary governance mechanism for DOD OSINT. It serves as a forum for the coordination and facilitation of OSINT activities and programs for all Services and combatant commands. The DOSC advices and reports to the Under Secretary of Defense for Intelligence (USD[I]) on OSINT issues and recommends initiatives to improve the effectiveness and efficiency of OSINT programs, activities, and systems of the DOD. The responsibilities of the DOSC include but are not limited to—

- The coordination of activities and the resolution of OSINT programs and activities.
- The prioritization of OSINT requirements.

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

E-2. INSCOM conducts multidiscipline and all-source intelligence operations to include collection, analysis, production, and dissemination; knowledge management for the Army intelligence enterprise; as well as delivers specialized quick reaction capabilities, advanced skills training, and linguist support for deploying forces to enable battle command to support unified land operations.

E-3. INSCOM regionally supports each of the geographic combatant commands through subordinate regionally focused multifunctional military intelligence brigades. Each brigade manages intelligence requirements (to include OSINT) and provides support to Army tactical units deploying to or operating within a unified combatant command's area of responsibility or operational environment. Each multifunctional brigade has the capability to produce OSINT, generate requests to higher agencies, and answer collection requirements submitted by subordinate units at the tactical level through OSCAR-MS.

DEPARTMENT OF THE ARMY INTELLIGENCE INFORMATION SERVICE

E-4. DA IIS provides a broad spectrum of intelligence support functions to Army and intelligence community customers. DA IIS is the primary OSINT information and dissemination proponent for the Army. DA IIS is an element of Army G-2, Intelligence Information Management Directorate (DAMI-IM) and operational control is assigned to the INSCOM G-3. DA IIS is the primary intelligence information dissemination office for the Army. DA IIS provides a broad spectrum of intelligence support functions to Army and intelligence community customers, including Army Open-Source Collections Requirements Management.

E-5. The mission of the DA IIS is to coordinate, disseminate, and validate the strategic-level requests for open-source requirements Army-wide under the direction of the Army G-2. This is done by providing information sharing services across the intelligence community. The DA IIS is a voting member of the Office of the Director of National Intelligence (ODNI) NOSC Collection Requirements Management (CRM) subcommittee. DA IIS is the Army proponent office for OSINT. As such it addresses all aspects of OSINT policy, training, operational support, collection, production, analysis, and dissemination.

DIRECTOR OF NATIONAL INTELLIGENCE OPEN SOURCE CENTER

E-6. The DNI OSC supports the NOSE as directed by the ADDNI/OS. The OSC is an organization within the intelligence community, U.S. Government, private sector, and academia.

E-7. The operations of the OSC are driven by standing open-source requirements contained in the OSC's annually reviewed and approved information collection plans. The OSC maintains a worldwide network of multilingual regional experts that respond to intelligence and information requirements using publicly available information and open sources such as radio, television, newspapers, news agencies, databases, and the Internet. The OSC monitors open sources in more than 160 countries in over 80 languages and acquires open-source data worldwide for organizations across DOD, U.S. government agencies, and local law enforcement departments.

E-8. OSC services and tools facilitate OSINT efforts of agencies and offices throughout the U.S. Government and intelligence community by enabling the creation, management, and dissemination of unclassified products. The effectiveness and adaptability of OSC tools are—

- Highly developed for open-source exploitation and product creation.
- Designed to support and provide resources to a decentralized customer-base mainly through the Internet and readily available, purchased COTS content.
- Consistent with intelligence community security, technical, and metadata standards.

E-9. The OSC analyzes the content and behavior of media and Internet Web sites of nations and other international actors of significant policy interest to the U.S. Government.

OPEN SOURCE ACADEMY

E-10. The Open Source Academy is a leading provider of open-source tradecraft training. As intelligence consumers place a greater value on OSINT, open-source specialists throughout the U.S. Government are turning to Open Source Academy courses (see table E-1) to build open-source skills and to stay abreast of evolving OSINT technologies. The Open Source Academy is building relationships with community leaders across the intelligence community to develop a comprehensive approach to instilling open-source tradecraft skills. The academy hosts participants expanding across DOD, federal agencies, as well as local law enforcement departments.

Table E-1. Open Source Academy curriculum

• Introduction to the Field • Library Resources and Research Techniques • Media Analysis	• Visual Persuasion Methodology Advanced Googling • Audience Resonance Methodology

• Newcomer's Basic Desktop • Open-source Research and Analysis • Orientation to the Open Source Center • OS 101: Open-source Fundamentals • OS 201: Open-source 201 • Open-source Intelligence (OSINT) and the Other Intelligences • Overview of the Open Source Center Collection Requirements Process • Security and Privacy Issues for Internet Users • Smart Research—Partnering with the Library • Temporary Duty Workshop • Tools and Data Sources	• Classification Workshop • Community Digital Audio Video Enterprise (DAVE) System • Creating Multi-media Products • DAVE Executive Overview • Disseminations • Essentials of Open-source Analysis • Field Management • Fundamentals of Open Source Center Textual Production and Operations (PROPS) • Geospatial Analysis: An Introduction • Hidden Universes of Information on the Internet • High-end Workstation Block II 101 • High-end Workstation Block II 201

U.S. ARMY ASIAN STUDIES DETACHMENT

E-11. The ASD is the oldest, largest, and one of the most well-established OSINT activities in DOD that demonstrates the characteristics of sustained OSINT exploitation. The ASD collects, analyzes, exploits, processes, and reports short-to-mid-term analyses of publicly available information on military capabilities, force protection threats, and other operational-level intelligence information on countries, forces, and nonstate actors of interest in the USPACOM area of responsibility. Such requirements include the capabilities, disposition, and readiness of military forces in China, North Korea, and the Russian Far East, as well as defense-related topics throughout South and Southeast Asia. The ASD serves as a model for combatant command-level OSINT exploitation. The ASD workforce consists of Department of the Army Civilians and Army Reserve and National Guard Soldiers who serve as mission managers and editorial staff and Government of Japan-funded foreign nationals who perform all of the collection, analysis, translation, reporting, library, and graphics support functions.

E-12. The mission of the ASD is to collect, analyze, exploit, and report foreign OSINT in response to USPACOM and U.S. Army Pacific taskings and other national-level intelligence requirements. ASD's OSINT collectors, analysts, and reporters accomplish their wide-scope mission through the exploitation of print and Internet media materials.

E-13. ASD personnel extract and compile information into analytical products answering specific taskings received via the OSCAR-MS. The ASD synthesizes and cites open-source references in open-source intelligence report format similar to research papers or essays. ASD's current operations section provides a suite of daily media summary products containing press articles responding to more immediate and time-sensitive requirements for foreign media reflections of U.S. activities and other topics of interest. The services and tools that the ASD provide include but are not limited to—

- OSINT products responding to OSCAR-MS requirements.
- Analytical open-source intelligence reports.
- Daily force protection/situational awareness reports (FPSARs).
- Daily area surrounding Japan open-source intelligence reports (ASJORs).
- Daily situational reports (SITREPs).
- Weekly China and Taiwan Military photos reports.
- Ad hoc reporting as requested by customer in OSCAR-MS.
- OSINT product distribution on NIPRNET, SIPRNET, and JWICS.
- Map collection.
- Media summary reports.

FEDERAL BUREAU OF INVESTIGATION

E-14. The FBI is an agency of the Department of Justice that serves as both a federal criminal investigative body and an internal intelligence agency. The FBI has investigative jurisdiction over violations of more than 200 categories of federal crime.

E-15. The main missions of the FBI are to protect and defend the United States against terrorist and foreign intelligence threats and to uphold and enforce criminal laws. This is done by focusing on specific categories that include but are not limited to—

- Bank robbery.
- Robbery and extortion affecting interstate commerce.
- Drugs.
- Conspiracy.
- Sexual exploitation of minors.
- Mail fraud.
- Bank fraud.
- Fraud by wire, radio, or television.
- Illegal gambling businesses.

E-16. The FBI uses publicly available information through open sources in the areas of counterterrorism, CI, cybercrime, information technology, and forensics. Within the mission scope of the FBI, the services and tools provided include but are not limited to—

- Law enforcement bulletins.
- Crime mapping.
- Statistics (cybercrime, white-collar crime, and violent crime).

FEDERAL RESEARCH DIVISION, LIBRARY OF CONGRESS

E-17. The FRD was organized during World War II to collect and conduct research on captured aeronautical and technical reports on German and Japanese forces. These collections provided insight to future U.S. defensive posture developments and subsequently assisted in the intelligence effort leading to the defeat of the Axis powers.

E-18. The mission of the FRD is to provide directed research and analysis on domestic and international subjects to agencies of the U.S. Government, the District of Columbia, and authorized federal contractors. The FRD conducts open-source research for the U.S. Library of Congress. The services and tools that the FRD provide include but are not limited to—

- Primary research material, including document delivery.
- Foreign language abstracting and translation.
- Annotated bibliographies.
- Organizational and legislative histories.
- Studies and reports.
- Books.
- Military legal resources.
- Country studies.
- Country profiles.
- Terrorism and criminal studies and assessments.

Appendix F

Open-Source Resources

Intelligence personnel have access to vast amounts of information during research. Understanding and awareness of where to begin to look for specific information can be the largest obstacle analysts encounter. The tables in this appendix list some starting reference points for obtaining information that can be developed and produced into finalized OSINT. Table F-1 lists open-source training and resources that are specifically military.

Table F-1. Military open-source training and resources

Intelligence Knowledge Network (IKN):	
IKN is a knowledge management tool that enables intelligence Soldiers worldwide to communicate, collaborate, and investigate. IKN— • Hosts discussion forums. • Serves as a single point of entry to get to U.S. Army Intelligence Center of Excellence (USAICoE) and other intelligence community Web sites. • Hosts a variety of public and private Web applications that support the intelligence community.	
University of Military Intelligence (UMI):	
UMI is the distance learning arm of the military intelligence schoolhouse. From the UMI Web site, military intelligence professionals can access— • Self-paced and reachback training. • The Cultural, Foreign Language Integration Center. • Military intelligence training resources.	
Army Knowledge Online (AKO) Intelligence:	
AKO Intelligence features— • The Intelligence Collaboration Center. • Knowledge Center (documents, FMs, TCs, ATTPs, and others). • Training, agencies, policy, doctrine, and links to other intelligence-related Web sites.	
AKO Open-Source Program:	
AKO Army Open-Source Program features Open-Source— • Events. • Discussion forums. • Links of interest.	• Intelligence products. • Handbooks.
Military Intelligence Library:	***Available via the IKN and Warfighter Forum homepage***
Military Intelligence Library Reference Center includes many databases and resources, such as— • Journals and magazines. • Forms and publications. • Resource guide.	• Historical documents. • Cultural field readings. • Military Intelligence Foreign Language Training Center (MIFLTC).

Table F-1. Military open-source training and resources (continued)

DA IIS Country Research Portal: ***Available via the DA IIS portal from the AKO homepage***
The Department of the Army Intelligence Information Service (DA IIS) Country Research portal has road-mapped and data-mined networks resulting in a one-stop-shop for intelligence information. Some of the links on this Web site include— • Open-source documents such as Early Bird, Terrorism Daily Update, Baghdad Mosquito, Basra Bugle, and others. • Intelligence community. • Combatant commands. • Analyst references. • Foundry program. ***Note.*** Data is accessible through multiple networks to ensure that intelligence consumers have all required information necessary for mission success.
Intelink-U:
Intelink-U is the designated network of the Department of National Intelligence (DNI) for intelligence collaboration. The Intelink-U is— • Managed by the Intelink Management Office. • A joint-use, remotely accessed, and operationally-implemented information service that is used to access and process unclassified, publicly accessible information only. • Provides a protected environment to exchange authorized unclassified, unclassified for official use only, and sensitive but unclassified information among personnel of the DOD. ***Note.*** Access to Intelink-U services is implemented through multiple virtual private networks.
Joint Military Intelligence Training Center:
Armies of the World
Armed Forces of the World ***Note.*** Requires account log in to access the page. Combined Arms Research Library
Center for Army Lessons Learned (CALL)
CALL
Military Operations in Urban Terrain (MOUT)
MOUT
Military Service Intelligence Organizations
U.S. Army Intelligence and Security Command (INSCOM) Office of Naval Intelligence Air Force Intelligence, Surveillance, and Reconnaissance (ISR) Agency Marine Corps Intelligence Activity
Unified Command Intelligence Organizations
U.S. Central Command U.S. European Command U.S. Pacific Command U.S. Southern Command U.S. Africa Command U.S. Air Force Space Command U.S. Special Operations Command U.S. Strategic Command U.S. Transportation Command

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

2X	human intelligence and counterintelligence staff element
ADDNI/OS	assistant deputy to the Director of National Intelligence for Open-source
AM	amplitude modulation
AO	area of operations
AR	Army regulation
ART	Army tactical tasks
ATP	Army techniques publication
ATTP	Army tactics, techniques, and procedures
BCT	brigade combat team
CCIR	commander's critical information requirement
CI	counterintelligence
CIA	Central Intelligence Agency
COA	course of action
CONUS	continental United States
COTS	commercial-off-the-shelf
CRM	collection requirements management
DA	Department of the Army
DA IIS	Department of the Army Intelligence Information Service
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOSC	Defense Open Source Council
DVD	digital video device
EO	executive order
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FFIR	friendly force information requirement
FM	field manual
FMI	field manual interim
FRD	Federal Research Division
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal

G-7	assistant chief of staff, inform and influence activities
G-9	assistant chief of staff, civil affairs operations
GEOINT	geospatial intelligence
HVT	high-value target
ICD	intelligence community directive
IED	improvised explosive device
IIR	intelligence information report
ILR	Interagency Language Roundtable
INSCOM	United States Army Intelligence and Security Command
IO	information operations
IP	Internet protocol
IPB	intelligence preparation of the battlefield
ISP	Internet service provider
JP	joint publication
JWICS	Joint Worldwide Intelligence Communcations System
MDMP	military decisionmaking process
METT-TC	mission, threat, terrain and weather, troops and support available, time available, and civil considerations (mission variables)
MFLT	machine foreign language translation
mm	millimeter
NIPRNET	Nonsecure Internet Protocol Router Network
NOSC	National Open Source Committee
NOSE	National Open Source Enterprise
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OPSEC	operations security
OSC	Open Source Center
OSCAR-MS	open-source collection acquisition requirement management system
OSINT	open-source intelligence
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
S-2	intelligence staff officer
S-3	operations staff officer
S-6	signal staff officer
S-7	inform and influence activities staff officer
S-9	civil affairs operations staff officer
SCI	sensitive compartmented information
SIPRNET	SECRET Internet Protocol Router Network
SOP	standard operating procedure
TCP/IP	transmission control protocol/Internet protocol

TTP	tactics, techniques, and procedures
URL	uniform resource locator
U.S.	United States
USC	United States Code
WWW	World Wide Web

SECTION II – TERMS

esoteric communications

Public statements whose surface meaning (manifest content) does not reveal the real purpose, meaning, or significance (latent content) of the author.

media source analysis

The systematic comparison of the content, behavior, patterns, and trends of organic media organizations and sources of a country.

open source

Any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure.

open-source intelligence

The discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (FM 2-0)

private information

Data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization.

publicly available information

Data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

References

REQUIRED PUBLICATIONS

These documents must be available to the intended user of this publication.

FM 1-02. *Operational Terms and Graphics.* 21 September 2004.

RELATED PUBLICATIONS

These sources contain relevant supplemental information.

AR 11-6. *Army Foreign Language Program*. 31 August 2009.

AR 25-400-2. *The Army Records Information Management System (ARIMS).* 2 October 2007.

AR 27-60. *Intellectual Property*. 1 June 1993.

AR 190-13. *The Army Physical Security Program*. 25 February 2011.

AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

AR 380-67. *Department of the Army Personnel Security Program*. 9 September 1988.

AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.

AR 530-1. *Operations Security (OPSEC).* 19 April 2007.

ATTP 2-91.6. *Tactics, Techniques, and Procedures for Intelligence Support to Site Exploitation.* 27 December 2010.

Carnegie Mellon Software Engineering Institute.

Chatham House.

Department of the Army Intelligence Information Services.

DOD 5240.1-R. *DoD Intelligence Activities.* 1 December 1982.

DODD 5100.20. *National Security Agency/Central Security Service (NSA/CSS).* 26 January 2010.

DODD 3115.12. *Open Source Intelligence (OSINT).* 24 August 2010.

EO 12333. *United States Intelligence Activities.* 4 December 1981.

FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace.* 15 October 2009.

FM 2-19.4. *Brigade Combat Team Intelligence Operations*. 25 November 2008.

FM 2-22.2. *Counterintelligence.* 21 October 2010.

FM 2-22.3. *Human Intelligence Collector Operations*. 6 September 2006.

FM 3-24. *Counterinsurgency*. 15 December 2006.

FM 3-55. *Information Collection*. 14 December 2011.

FM 3-60. *The Targeting Process.* 26 November 2010.

FM 3-90.119. *Combined Arms Improvised Explosive Device Defeat Operations.* 21 September 2007.

FM 5-0. *The Operations Process*. 26 March 2010.

FM 6-0. *Mission Command.* 13 September 2011.

FM 7-0. *Training Units and Developing Leaders for Full Spectrum Operations*. 23 February 2011.

FM 7-15. *The Army Universal Task List.* 27 February 2009.

JP 1-02. *Department of Defense Dictionary of Associated Terms*. 8 November 2010.

JP 2-0. *Joint Intelligence.* 22 June 2007.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 7 October 2004.

JP 3-0. *Joint Operations.* 17 September 2006.

JP 3-35. *Deployment and Redeployment Operations*. 7 May 2007.

JP 3-59. *Meteorological and Oceanic Operations*. 24 September 2008.

JP 3-60. *Joint Targeting*. 13 April 2007.

JP 4-0. *Joint Logistics.* 18 July 2008.

JP 5-0. *Doctrine for Planning Joint Operations*. 20 January 2005.

Lanicci, John M. "Integrating Weather Exploitation into Air and Space Power Doctrine." *Air Power 12, No. 2*. Summer 1998: 52-63.

Library of Congress, Federal Research Division.

Open Source Center.

TC 2-22.4. *Technical Intelligence.* 19 November 2009.

TC 2-33.4. *Intelligence Analysis*. 1 July 2009.

TC 2-91.8. *Document and Media Exploitation.* 6 August 2010.

U.S. Computer Security Readiness Team.

Title 17 USC. *Copyrights*.

Title 18 USC. *Crimes and Criminal Procedure*.

PRESCRIBED FORMS

None.

REFERENCED FORMS

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

Index

Entries are by paragraph number.

A

analysis, 1-2
  intelligence, 2-22
  Internet, 2-19
  media, 4-20
  mission, 1-16, 3-6
  public documents, 2-14
  requirements for, 2-72

C

Chatham House Rule. *See* public speaking forums.

collection, 1-3, 1-7, 3-2
  and analysis, 1-2
  confidential sources, 3-7
  document, 2-14
  foreign media monitoring, 2-57
  information, 1-12
  linguist requirements, 2-49
  machine foreign language translation systems, 2-55
  open sources, 3-7
  technique, 3-8
  U.S. person information, 2-40

cyberspace
  cyber situational awareness, B-6
  defined, B-5

D

databases, 3-12, C-26
  operational information, 2-23
  technical information, 2-23

dissemination
  considerations, 4-49
  digitization, 4-15
  guidelines, 4-42
  media, 4-33
  methods, 4-43
  standards, 4-19
  U.S. person information, A-19

I

information
  collection, 1-12
  evaluate, 4-2
  operations security, 2-41
  publicly available, 1-2, 1-7, 3-1, 4-2
  reliability and credibility, 4-9
  report and disseminate, 4-39

intelligence products, 4-1

Internet
  Boolean logic, C-9, C-29
  cookie data, B-9
  Deep Web, C-3
  international Web sites, C-32
  operations security vulnerabilities, C-35
  publicly available information, C-12
  search engines, C-4
  search, C-15
  truncate the uniform resource locator, C-23
  Web site domains, C-25
  Web sites, 2-19, 3-23
  World Wide Web, C-2

L

legal restrictions
  AR 27-60, 2-48
  AR 381-10, A-7
  copyright, 2-46
  Executive Order 12333, A-1
  fair use, 2-47
  intellectual property, 2-46
  Intelligence Community Directive 300, A-23
  Intelligence Community Directive 301, A-23

M

MDMP, 1-15

media
  analysis, 4-20
  content, 4-35
  control, 4-24
  structure, 4-26

military decisionmaking process. *See* MDMP.

O

open source, 1-1

open-source
  credibility, 2-39
  reliability, 2-34

open-source intelligence. *See* OSINT.

OSINT, 1-1
  and the intelligence process, 1-11
  characteristics, 1-4
  contributions to counterinsurgency operations, D-1
  contributions to GEOINT, D-9
  contributions to HUMINT, D-6
  contributions to improvised explosive device defeat operations, D-1
  contributions to intelligence preparation of the battlefield, 1-18
  contributions to SIGINT, D-9
  contributions to site exploitation, D-12
  contributions to source vetting, D-12
  contributions to targeting operations, D-1
  coordination, 2-44
  deception and bias, 2-45
  defined, 1-1
  exploitation, 2-11, 2-21
  personnel, 2-66
  planning, 2-1
  private information, 3-6
  publicly available information, 3-6

OSINT organizations
  Asian Studies Detachment, 2-28, E-13
  Assistant Deputy Director of National Intelligence for Open Source, A-25
  Defense Open Source Council, E-1
  Department of the Army Intelligence Information Service, E-4

Entries are by paragraph number.

Director of National Intelligence Open Source Center, A-28, E-8
Federal Bureau of Investigation, E-16
Federal Research Division, Library of Congress, E-20
U.S. Army Intelligence and Security Command, E-2
National Open-Source Committee, A-27
Open Source Academy, E-12

P

public broadcasts, 2-17, 3-21
public documents, 2-14, 3-20
public speaking forums, 2-11, 3-18
Chatham House Rule, 3-18

R

requirement
commander's criticial information, 1-13, 3-2
friendly force information, 1-13, 3-2
priority intelligence, 1-13, 3-2
intelligence, 3-5
priority intelligence, 3-2
research, 3-11
field research, 3-13
open-source, 3-1
plan, 3-16
practical, 3-13
question, 3-15

S

security domains, 4-44
Joint Worldwide Intelligence Communications System, 4-46
Nonsecure Internet Protocol Router Network, 4-48
SECRET Internet Protocol Router Network, 4-47
sources
analysis of the media, 4-20
authoritative, 4-10
confidential, 3-7
credibility ratings, 2-39
nonauthoritative, 4-11
open, 1-1, 3-7
primary, 2-35
reliability ratings, 2-38
secondary, 2-37

T

threat
courses of action, 2-8
evaluate, 2-7

U

U.S. person information
collection of 2-40, A-8
dissemination of, A-19
retention of, A-14

ATP 2-22.9
10 July 2012

By order of the Secretary of the Army:

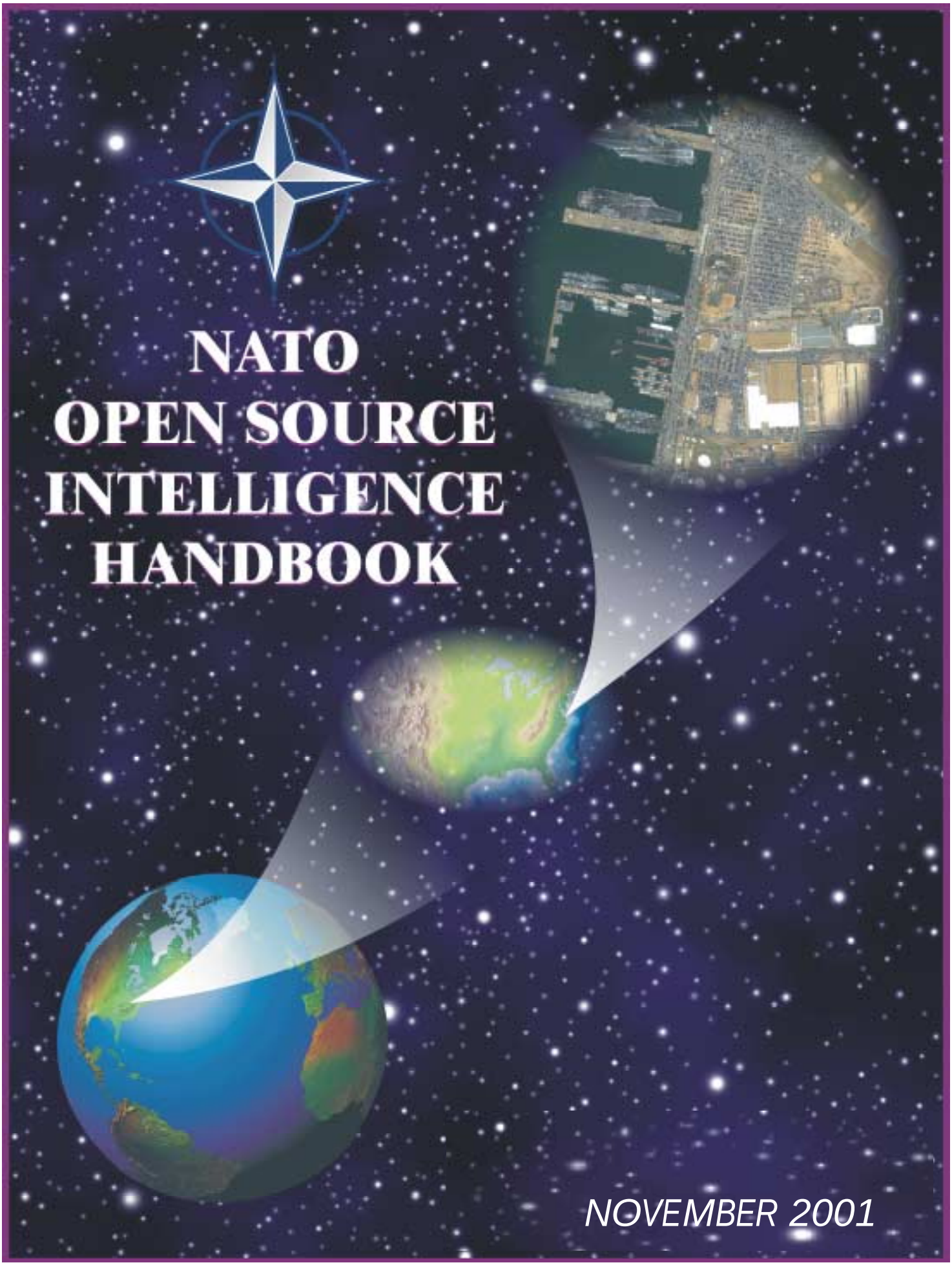
RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

DISTRIBUTION:

Unlimited Distribution; Not to be distributed; electronic media only.


NATO
OPEN SOURCE
INTELLIGENCE
HANDBOOK
NOVEMBER 2001

This Page Is Intentionally Left Blank

PREFACE

This publication provides preliminary joint and coalition training information on the subject of Open Source Intelligence (OSINT). It discusses the fundamentals of OSINT support to both the all-source intelligence process, and to the unclassified intelligence requirements of operators, logisticians, and civilian organizations participating in joint and coalition operations. The focus is on relevant information that can be obtained legally and ethically from the public and private sector, and that is not classified in its origin or processing. The information may become classified in relation to the commander's intent or its association with classified information when it is rightly blended into all-source intelligence reports.

This publication has been prepared under my direction as the Supreme Allied Commander, Atlantic, in collaboration with staff from the Supreme Allied Commander, Europe (SACEUR). This publication has benefited greatly from the continued collaboration between my staff and the staff of Open Source Solutions Inc. With the publication of this document and its companions, the *Intelligence Exploitation of the Internet* and the *NATO OSINT Reader*, commanders and their staffs will have basic guidance for the development of OSINT.

The increasingly robust array of open sources available to all staffs enable commanders at all levels to attempt to satisfy their information requirements themselves rather than immediately directing Requests for Information (RFIs) elsewhere. This manual outlines a systematic approach to OSINT exploitation.

This information is relevant to all NATO commands, task forces, member nations, civil-military committees and working groups, and such other organizations that may be planning or engaged in combined joint operations.

W. F. KERNAN
General, U.S. Army

This Page Is Intentionally Left Blank

Table of Contents

EXECUTIVE SUMMARY **V**
CHAPTER I **1**
OPEN SOURCE INTELLIGENCE AND JOINT OR COALITION OPERATION **1**
Introduction 1
Definitions 2
21st Century Information Operations 3

CHAPTER II **5**
PRIVATE SECTOR INFORMATION OFFERINGS **5**
SECTION A. SOURCES **5**
Traditional Media Sources 5
Commercial Online Premium Sources 6
Other Forms of Commercial Online Information 8
Grey Literature 8
Overt Human Experts and Observer 9
Commercial Imagery 9
Defining Source Access Requirements (Dangers of Pay-per-View) 11
SECTION B. SOFTWARE **12**
Software Hierarchy 12
SECTION C. SERVICES **13**
Collection Services 13
Processing Services 13
Analysis & Production Services 13
Services Examples 14

CHAPTER III **15**
THE OPEN SOURCE INTELLIGENCE CYCLE **15**
SECTION A. OSINT PLANNING AND DIRECTION **15**
Overview 15
Organizations and Responsibilities 15
Requirements Definition 16
Evaluation and Feedback 17
SECTION B. COLLECTION **17**
Overview 17
Knowing Who Knows 19
Collection Discipline 19
Collection Issues 20
Nuances of Open Source Collection 21
SECTION C. PROCESSING AND EXPLOITATION **23**
Overview 23
Analysis 23
Web-Site Authentication and Source Analysis 24
SECTION D. SEARCHING ANONYMOUSLY ON THE WEB **27**
Overview 27
Leaving a Footprint 28
Traffic analysis 28

Contact with others 29
SECTION E. PRODUCTION 29
Overview 29
Reports 29
Link Tables 31
Distance Learning 31
Expert Forums 32
SECTION F. DISSEMINATION AND EVALUATION 33
Overview 33
Dissemination Methods 34
Virtual Intelligence Community 34

CHAPTER IV 36
OSINT AND THE EMERGING FUTURE INTELLIGENCE ARCHITECTURE OF NATO 36
SECTION A. BLENDING OSINT INTO THE ALL-SOURCE PROCESS 36
Overview 36
Direction 38
Collection 39
Processing 41
Dissemination 42

APPENDIX A: GENERAL REFERENCE LINK TABLE 43
APPENDIX B: TRAINING LINK TABLE 45
APPENDIX C: CATEGORIES OF MISPERCEPTION AND BIAS 46
APPENDIX D: LIST OF ABBREVIATIONS 48
FEEDBACK 49

EXECUTIVE SUMMARY

COMMANDER'S OVERVIEW

Open Source Intelligence (OSINT) in Joint and Coalition Operations

Open Source Intelligence, or OSINT, is unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question. It provides a very robust foundation for other intelligence disciplines. When applied in a systematic fashion, OSINT products can reduce the demands on classified intelligence collection resources by limiting requests for information only to those questions that cannot be answered by open sources.

Open information sources are not the exclusive domain of intelligence staffs. Intelligence should never seek to limit access to open sources. Rather, intelligence should facilitate the use of open sources by all staff elements that require access to relevant, reliable information. Intelligence staffs should concentrate on the application of proven intelligence processes to the exploitation of open sources to improve its all-source intelligence products. Familiarity with available open sources will place intelligence staffs in the position of guiding and advising other staff elements in their own exploitation of open sources.

Open Source Intelligence and Joint or Coalition Operations

OSINT is a vital component of NATO's future vision. Through its concentration upon unclassified open sources of information, OSINT provides the means with which to develop valid and reliable intelligence products that can be shared with non-NATO elements of international operations. Experience in the Balkans, and the increasing importance of the Partnership for Peace and Mediterranean Dialogue members in security dialogue, illustrates the need to develop information sources that enable broader engagement with these vital partners.

Private Sector Information Offerings

The Internet is now the default C4I architecture for virtually the entire world. The principle exceptions are most militaries and intelligence organizations. The Internet facilitates commerce, provides entertainment and supports ever increasing amounts of human interaction. To exclude the information flow carried by the Internet is to exclude the greatest emerging data source available. While the Internet is a source of much knowledge, all information gleaned from it must be assessed for its source, bias and reliability.

As a source of reliable information, the Internet must be approached with great caution. As a means with which to gain access to quality commercial sources of validated information, the Internet is unbeatable.

A vision of open source exploitation must not be limited exclusively to electronic sources. Traditional print, hardcopy images and other analog sources continue to provide a wealth of data of continuing relevance to NATO intelligence.

The Open Source Intelligence Cycle

As the range of NATO information needs varies depending upon mission requirements, it is virtually impossible to maintain a viable collection of open source materials that address all information needs instantly. The focus should be on the collection of sources, not information. With knowledge of relevant and reliable sources of open source information, an intelligence staff can quickly devote collection energy and analytical expertise to develop tailored OSINT products to the mission need.

OSINT and the Emerging Future Intelligence Architecture of NATO

OSINT is an essential building block for all intelligence disciplines. Open sources have always played a role in classified intelligence production. In the NATO context, a robust OSINT capability greatly increases the range of information sources available to intelligence staffs to address intelligence needs.

Nations are capable of tasking classified intelligence sources to address intelligence gaps. Lacking organic intelligence collection assets, NATO intelligence staffs are unable to task classified collection. Rather than immediately directed a Request For Information (RFI) to a national intelligence centre, a robust OSINT capability enables intelligence staffs to address many intelligence needs with internal resources.

While unable to replace classified intelligence production, OSINT is able to compliment an all-source intelligence production process with essential support including tip-offs, context, validation and cover for information sanitation.

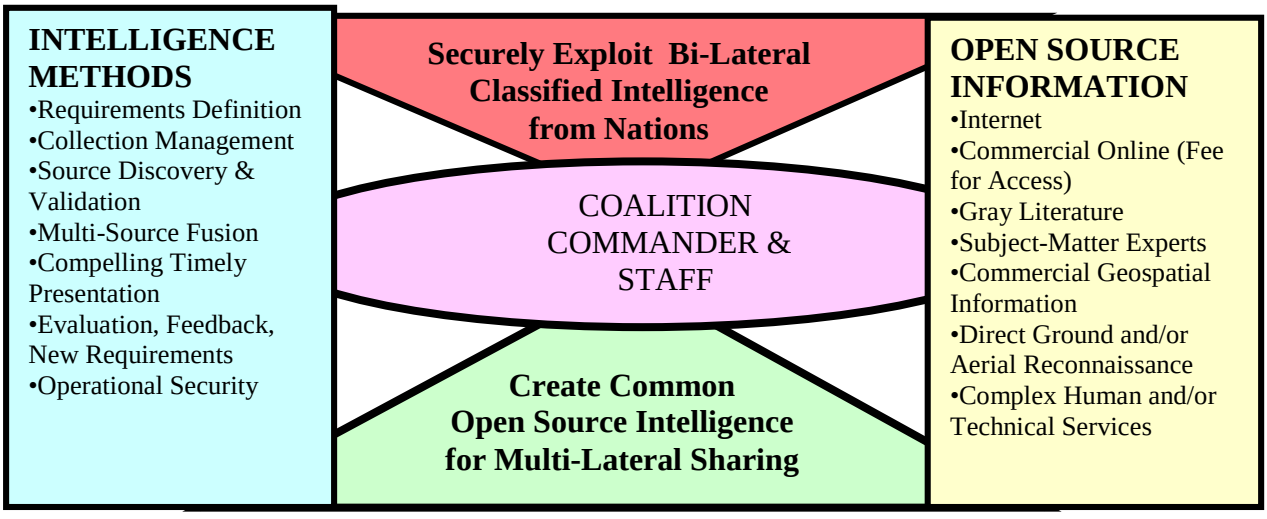
CHAPTER I
OPEN SOURCE INTELLIGENCE AND JOINT OR COALITION OPERATIONS

"OSINT is not a substitute for satellites, spies, or existing organic military and civilian intelligence capabilities. It is, however, a foundation—a very strong foundation—for planning and executing coalition operations across the spectrum from humanitarian assistance to total war. OSINT provides strategic historical and cultural insights; it provides operationally helpful information about infrastructure and current conditions; and it provides tactically vital commercial geospatial information that is not available from national capabilities. In coalition operations, OSINT is both the foundation for civil-military cooperation, and the framework for classified bilateral intelligence-sharing."

Introduction

OSINT is distinct from academic, business or journalistic research in that it represents the application of the proven process of national intelligence to a global diversity of sources, with the intent of producing *tailored* intelligence for the commander. OSINT is also unique, within a coalition operations context, in that it simultaneously provides a multi-lateral foundation for establishing a common view of the shared Area of Operations (AOO), while also providing a context within which a wide-variety of bi-lateral classified intelligence sharing arrangements can be exploited. Figure 1 illustrates these relationships.

Figure 1 - Relationship between Open Source and Classified Information Operations



OSINT is valuable to NATO member nations and to individual Partner nations in that it can be used to provide a common understanding of the AOO across all elements of its military forces and its civilian and non-governmental organization (NGO) counterparts. Elements of the forces not authorized access to the full range of classified information, often including such vital components, as military police, logistics elements, engineers, and the public affairs staff, can be made more effective through the utilization of tailored OSINT. At the same time, external parties with whom coordination is critical, but who are also not authorized access to classified information, can receive tailored OSINT that is helpful to a shared understanding of the AOO and the challenges facing the coalition and all its elements. Figure 2 illustrates this idea.

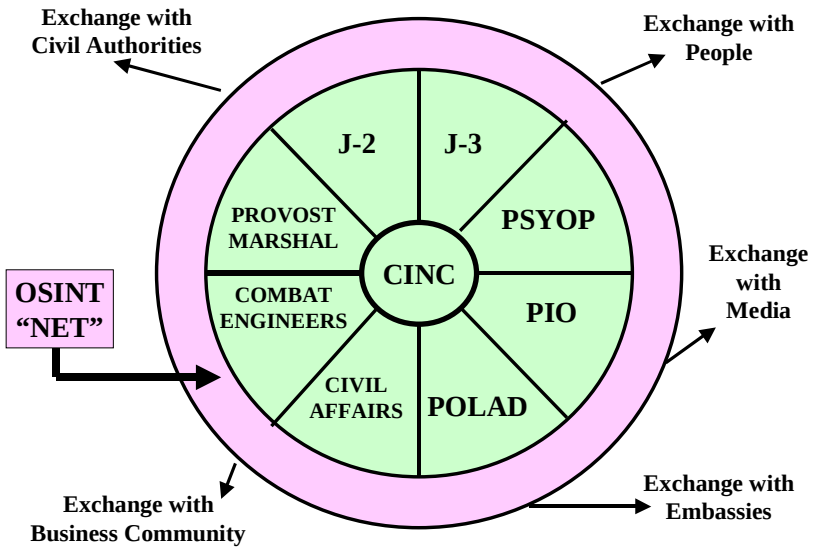


Figure 2 - Utility of OSINT Net for Internal and External Information Exchanges

Definitions

There are four distinct categories of open information and intelligence.

Open Source Data (OSD). Data is the raw print, broadcast, oral debriefing or other form of information from a primary source. It can be a photograph, a tape recording, a commercial satellite image, or a personal letter from an individual.

Open Source Information (OSIF). OSIF is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is *generic* information that is usually *widely disseminated*. Newspapers, books, broadcast, and general daily reports are part of the OSIF world.

Open Source Intelligence (OSINT). OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a *select*

audience, generally the commander and their immediate staff, in order to address a *specific* question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and *creates intelligence*.

Validated OSINT (OSINT-V). OSINT-V is information to which a very high degree of certainty can be attributed. It can be produced by an all-source intelligence professional, with access to classified intelligence sources, whether working for a nation or for a coalition staff. It can also come from an assured open source to which no question can be raised concerning its validity (images of an aircraft arriving at an airport that are broadcast over the media).

21st Century Information Operations

OSINT is an essential contextual and foundation element for classified intelligence operations. Overt human sources can help target and validate clandestine human intelligence (HUMINT) sources. Overt broadcast information can be used to better understand covertly collected signals intelligence (SIGINT). Commercial geospatial information, especially wide-area surveillance imagery, can be used to significantly enhance the value of the more narrowly focused covert imagery intelligence (IMINT) capabilities. OSINT can also make contributions to the emerging discipline of Measurements and Signatures Intelligence (MASINT), to Counter-intelligence (CI), and to Operations Security (OPSEC).

OSINT is the major new "force" in 21st Century Information Operations (IO). OSINT is not "new" in that Nations and organizations have always understood the value of legal travelers, direct observation, structured reading, and legal purchases of information services. What *is* new about OSINT is the confluence of three distinct trends: first, the proliferation of the Internet as a tool for disseminating and sharing overt information; second, the consequent and related "information explosion" in which published knowledge is growing exponentially; and third, the collapse of many formerly denied areas.

OSINT is important to coalition commanders and their staffs for another reason: emerging threats, and the lower end of the spectrum of conflict, increasingly demand out-of-area operations and engagement in operations for which classified intelligence support is not readily available. Out of area operations such as humanitarian assistance and disaster relief operations in the countries of Africa or elsewhere along the NATO periphery, are all characterized by complex information needs related to infrastructure, demographics, health, and other matters not traditionally addressed by classified intelligence collection operations.

OSINT is vital to government operations, and especially to coalition operations, for one additional reason: the changing nature of command & control in the 21st Century. In the past, nations and even coalitions relied heavily on a top-down "chain of command" that relied on closed sources to direct generally unilateral actions with short-term time frames. Today, as non-governmental organizations come to the fore and are often the predominant factors in many of the operations that the military must support, the dynamics of both command & control and information have changed.

Within NATO, operations must be planned and executed in a multi-cultural fashion, with bottom-up consensus often being the most effective means of arriving at sustainable decisions. This is particularly true with the vital role played by non-NATO troop contributing nations. Under these circumstances, a common view of the

operating area, formed with the help of validated OSINT is often the most effective means of delivering decision-support.

The remainder of this manual will discuss private sector information offerings, the open source intelligence cycle, and the integration of OSINT into the NATO and prospective PfP coalition operations. OSINT will be a core element of the NATO Future Intelligence Architecture.

Special Note on Operational Security

The most common objection to the use of open sources of information, apart from the general lack of knowledge and funding with which to exploit open sources, relates to Operational Security (OPSEC). This topic is fully discussed within Chapter III. The Open Source Intelligence Cycle makes full provision for OPSEC at every stage, and ample methods exist to conceal the commander's intent, the source of the inquiry, and other sensitive aspects of open source exploitation.

CHAPTER II
PRIVATE SECTOR INFORMATION OFFERINGS

The four pillars to an OSINT strategy are sources, software, services and analysis. The private sector can address all four to some degree. Analysis is the key enabling skill that is essential to the successful integration of OSINT into an all-source intelligence product. While some analysis of open sources can and should be acquired from private sources, those analytical skills necessary to integrate open source derived intelligence must be grown and nurtured within intelligence staffs. Analysis will be discussed further in Chapter III. This chapter is intended to expose the wider audience to the range of OSINT-related products that the private sector are optimized to provide.

SECTION A. SOURCES

Traditional Media Sources

To many, media sources were the only open sources that were familiar prior to the onset of the Internet. These include traditional foreign print and broadcast media, radio and TV as well as the current array of electronically available products. For current intelligence purposes, media sources remain the core capability necessary for an OSINT effort and are available from a variety of providers. Direct wire-service feeds are available. Commercial online premium sources discussed below all provide an array of media sources on a fee for service basis.

While not private sector information providers, the U.S. Foreign Broadcast Information Service (FBIS) and the British Broadcasting Corporation (BBC) Monitoring Service each provide excellent near real-time translation of foreign media sources. In addition, an array of media analysis products supplement the direct listing of foreign broadcasts and provide useful insight into the general character of foreign media reporting on particular issues.

Internet

The Internet has, since 1994, literally exploded on to the world scene and changed forever the manner in which individuals might carry out global research. According to Dr. Vinton Cerf, acknowledged by many to be one of the founders of the Internet, it will grow from 400 million users in November 2000, to an estimated 3.5 billion users by the year 2015.

Apart from this exponential increase in the number of human beings using the Internet, other experts project a double or triple order of magnitude increase in the use of the Internet to connect devices, from geospatial locators in vehicles, to temperature detectors in soda machines, to usage monitors in doorways. The Internet is at the very beginning of its development as a global grid of enormous value to coalition operators, logisticians, and intelligence professionals.

Figure 3 - Internet users by continent (1999)

The Internet has been over-sold in the past. A study by the Community Open Source Program Office (COSPO) within the U.S. Intelligence Community concluded in 1994 that the Internet only contained roughly 450 useful substantive sites, and that 99% of the Internet was not content of intelligence value, but rather pornography, opinion, and advertising. This earlier evaluation of the intelligence potential of the Internet no longer reflects the extensive content that is now available. Some suggest that over 250,000 databases are now available within the "deep web", a great many of which are of potential intelligence value.

While the Internet has grown substantially in value since 1994, the intelligence professional must be very cautious about both over-reliance on the Internet, and about the source bias of materials found there. In general, Internet sources are rarely dated, formatted, paginated, edited, filtered, or stable, even when addressing substantive topics.

The Internet is an "easy out" for operators and other consumers of intelligence. It is an attractive option for commanders and staff in a hurry. If intelligence professionals do not demonstrate that they monitor and exploit the Internet, and/or if intelligence professionals make it too difficult for consumers to obtain usable all-source intelligence, the Internet represents a "threat" to the existing intelligence process. Increasingly, intelligence professionals must act to place information that is widely available on the Internet into its proper context – either confirming its validity or disputing the information based on classified collateral reporting.

In general, the Internet today provides two benefits to the coalition professional: first, as a means of rapidly communicating with counterparts around the world, primarily to exchange unclassified information and professional insights; and second, as a means of rapidly accessing both free and premium (fee paid for access) information sources. However, the Internet also has its dangers. Electronic mail and attached documents comprise a permanent record in cyber-space, and the sender has little control over subsequent dissemination and exploitation.

OSINT Professional Note: A number of advanced search tools are available that complement the variety of search engines that are freely available on the Internet. OSINT managers should remain abreast of developments in the field of Internet tools and integrate appropriate tools, as they become available, into their OSINT process. An example, its basic form available free or in an advanced version at a small cost, is a meta-search engine that combines the best features of multiple search engines, while also permitting subsequent searches for new information (remembering what has already been seen). Download this program from www.copernic.com.

Commercial Online Premium Sources

There are numerous commercial online premium sources, that is, sources that charge either a subscription fee or a usage fee for access to their information. It is essential that every professional understand the availability and the value of commercial online premium sources. They represent decades worth of editorial selection,

authentication, formatting, indexing, abstracting, and presentation management. In general, source material obtained through a commercial online premium service has been created by a reputable commercial enterprise subject to scrutiny and the judgment of the marketplace. In Figure 4, we discuss the three best known to governments and corporations. There are many others, some unique to Europe or Asia. Each professional is urged to consult his or her librarian or his or her OSINT collection manager to gain a better understanding of what their options are for high-quality commercial information relevant to their action responsibilities.

In general, and in part because of the high cost of mistakes or unnecessary retrievals, all commercial online premium services should be searched by those staff with sufficient training on the database and a thorough understanding of its pricing structure. Even commands with flat-fee pricing should be aware that their next contract will be increased in price based on actual usage during the current flat-fee period. Alternatively, an option is to gain access to commercial sources via the services of a professional librarian or commercial information broker. Most professional information brokers, such as those belonging to the Association of Independent Information Brokers (AIIB), specialize in either LEXIS-NEXIS or DIALOG. There are distinct advantages in contracting a searcher who has detailed familiarity with the very arcane search command characteristics of these two services. In the case of Factiva this is less vital but can still make a big difference in both the success of the searchers, and the cost of the searches.

FACTIVA	LEXIS-NEXIS	DIALOG
www.factiva.com	www.lexis-nexis.com	www.dialog.com
Best web-based user interface, easiest means of searching all available publications. Archive of publications varies but typically provides several years worth of historical file. Includes Jane's Information Group material as well as BBC transcripts. Does not include FBIS information.	Two separate channels, one focused on legal sources including public records (primarily in the United States but very helpful in tracing real estate, aircraft, and water craft including international ships), the other focused on news sources but offering archive access, i.e. ability to reach back several years or more on any topic.	A very large collection of various commercial offerings that can be searched "by the file". Especially valuable for access to conference proceedings, academic and policy journals, dissertations, book reviews, and the Social Science Citation Index (SSCI). The latter is ideal for finding and ranking individual experts, to include identification of their official address.
Flat fee or actual cost pricing.	Flat fee, actual cost, or pay as you go credit card pricing.	Flat fee, actual cost, or pay as you go credit card pricing.

Figure 4 - Leading Commercial Online Premium Sources

OSINT Professional Note: Always ask for search results in electronic form, these files can more easily be shared. Copy the results into a Word document. Add pagination. Add a title page and a blank table of contents page. Sort the items into larger categories (e.g. Political, Military, Economic) and label the categories as "Heading 1". Then go through the document label each individual headline as "Heading 2". These headings are choices in the style bar at the upper left that generally says "Normal". Finally, go to the Table of Contents and use the Insert, Index and Tables, Table of Contents choices to insert a table of contents. If desired, use the Replace function to find and make bold all of the original search terms.

Other Forms of Commercial Online Information

There is a vast range of commercial sources available through direct subscription, both on the Internet and in the form of hard copy or CD-ROM publications. Table 1 below identifies just a few sources of common interest to military commanders and their staff. There are many more than those listed here. SACLANT has undertaken to develop and maintain a common NATO inventory of open sources and access points to which RFIs can be directed. This can be found on MCCIS at www.saclant.nato.int/intel. Work continues to progress on a concept of operations for establishing broad NATO access to such sources at the most competitive prices possible.

Source Type or Function	Source Name and URL
Broadcast Monitoring	BBC Monitoring http://news.monitor.bbc.co.uk/
Broadcast Monitoring	FBIS/NTIS World News Connection http://wnc.fedworld.gov/ntis/home.html
Commercial Imagery	Autometric http://www.autometric.com/AUTO/SERVICES/GIS
Current Awareness (Conferences)	British Library Proceedings http://www.bl.uk/services/bsds/dsc/infoserv.html#inside_conf
Current Awareness (Journals)	ISI Current Contents http://www.isinet.com/
Current Awareness (Regional)	Oxford Analytica http://www.oxan.com/
Defense Monitoring	Janes Information Group http://www.janes.com/geopol/geoset.html
Defense Monitoring	Periscope http://www.periscope1.com
Defense Monitoring (NATO)	Orders of Battle Inc. http://orbat.com
Directories of Experts	Gale Research http://www.gale.com/
Foreign Affairs Discussions	Columbia U. Int'l Affairs Online www.ciaonet.org
Foreign Affairs Monitoring	Country Watch.com www.countrywatch.com
Global Risk Monitoring	Political Risk Service (Country Studies) www.prsgroup.com
Maps & Charts	East View Cartographic http://www.cartographic.com

Table 1 - Examples of specialized commercial information

Grey Literature

Grey literature is that information that is both legally and ethically available, but only from specialized channels or through direct local access. It is generally understood as that information whose distribution is not controlled by commercial publishers, and/or that information that is not published, distributed, catalogued or acquired through commercial booksellers and subscription agencies. Grey literature includes working

papers, pre-prints, technical reports and technical standards documents, dissertations, data sets, and commercial imagery. Producers of grey literature include: non-profit and educational organizations; commercial enterprises creating documents for internal use as well as for clients and suppliers; local, state, and national government agencies producing materials for internal use as well as for citizens and vendors, and; a wide variety of informal and formal associations, societies, and clubs. Examples include university yearbooks, yacht club registries, corporate trip reports, and personal notes from public events that are posted to a public bulletin board.

Overt Human Experts and Observers

The ultimate open source is a human expert or human observer with direct experience. In many places of the world, Africa, for example, it is not possible to obtain published information on specific locations or conditions. For many topics, even those with great quantities of published information, it is not possible to find exactly what is needed even when the time and money is available to collect, process, and analyze all available published information. The human expert is often the most efficient and the most inexpensive means of creating new open source intelligence that is responsive to a specific requirement from the commander or his staff.

The identification and interviewing of those with direct on-the-ground experience is also a valuable means of ascertaining "ground truth." It merits comment that official communications from organizations, and most media reporting, tend to rely on second-hand reports. Unless the information is meticulously sourced and from a very trusted source, expert judgment or observation more often than not it will be less reliable than direct human expert judgment or observation.

OSINT Professional Note: There are essentially four ways to get to expert humans. The most effective means is through citation analysis using the *Social Science Citation Index* (SSCI) or the *Science Citation Index* (SCI). These can both be accessed at www.isinet.com/isi. This generally requires a specialist searcher with access to DIALOG for the SSCI or to the Scientific and Technical Network (STN) for the SCI. The second means is through professional associations such as listed in the *International Directory of Associations* published by Gale Research, or as found through a copernic.com search of the Internet. The third means is by doing a Factiva.com search and identifying experts or "talking heads" that have been quoted in the media on that topic. Last, and often the least efficient, is through a labor-intensive series of telephone calls to various known government agencies or official points of contact. As a general rule, it is best to do a comprehensive professional search for international experts with the most current knowledge, rather than relying on the in-house focal points or whomever might be casually known to in-house points of contact.

Commercial Imagery

The commercial imagery industry continues to mature with the launching in recent years of a number of satellites that offer militarily significant capabilities. One-meter

resolution electro-optical imagery available to the private sector is not only possible now but also likely to be *de rigueur* in the future. Table 2 illustrates some of the military applications of 1-m commercial imagery. By 2003, at least eleven private companies expect to have high-resolution commercial remote sensing satellites in orbit. Their products will be available to whoever has a credit card. While this will bring new capabilities to friend and foe alike, commercial imagery provides unique opportunities for NATO as well. Unbridled by security constraints, which limit the use of imagery derived from military satellites, commercial imagery acquired by NATO can be freely distributed within the constraints of copyright agreements with the original provider. This provides a host of options regarding cooperation with broader coalition partners who do not have access to NATO classified information.

Target *(note a)*	**Detection** *(note b)*	**General ID** *(note c)*	**Precise ID** *(note d)*	**Description** *(note e)*	**Technical Analysis**
Troop units	**6.0**	**2.0**	**1.20**	**0.30**	**0.150**
Vehicles	**1.5**	**0.6**	**0.30**	**0.06**	**0.045**
Aircraft	**4.5**	**1.5**	**1.00**	**0.15**	**0.045**
Airfield facilities	**6.0**	**4.5**	**3.00**	**0.30**	**0.150**
Nuclear weapons components	**2.5**	**1.5**	**0.30**	**0.03**	**0.015**
Missile sites (SSM/SAM)	**3.0**	**1.5**	**0.60**	**0.30**	**0.045**
Rockets and artillery	**1.0**	**0.6**	**0.15**	**0.05**	**0.045**
Surface ships	**7.5-15.0**	**4.5**	**0.60**	**0.30**	**0.045**
Surfaced submarines	**7.5-30.0**	**4.5-6.0**	**1.50**	**1.00**	**0.030**
Roads	**6.0-9.0**	**6.0**	**1.80**	**0.60**	**0.400**
Bridges	**6.0**	**4.5**	**1.50**	**1.0**	**0.300**
Communications					
Radar	**3.0**	**1.0**	**0.30**	**0.15**	**0.015**
Radio	**3.0**	**1.5**	**0.30**	**0.15**	**0.015**
Command and control HQs	**3.0**	**1.5**	**1.00**	**0.15**	**0.090**
Supply dumps	**1.5-3.0**	**0.6**	**0.30**	**0.03**	**0.030**
Land minefields	**3.0-9.0**	**6.0**	**1.00**	**0.30**	**--**
Urban areas	**60.0**	**30.0**	**3.00**	**3.00**	**0.750**
Coasts, landing beaches	**15.0-30.0**	**4.5**	**3.00**	**1.50**	**0.150**
Ports and harbors	**30.0**	**15.0**	**6.00**	**3.00**	**0.300**
Railroad yards and shops	**15.0-30.0**	**15.0**	**6.00**	**1.50**	**0.400**
Terrain	**--**	**90.0**	**4.50**	**1.50**	**0.750**

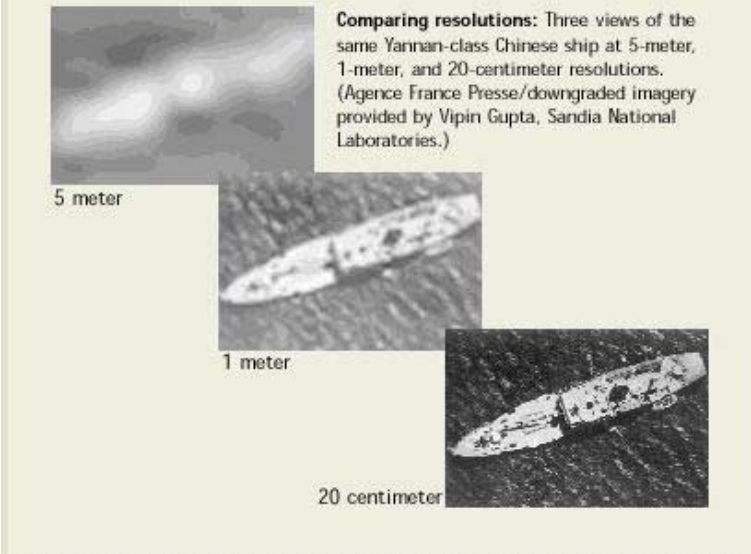
Notes:

a. The table indicates the minimum resolution in meters at which the target can be detected, identified, described, or analyzed. No source specifies which definition of resolution (pixel-size or white-dot) is used, but the table is internally consistent.
b. Detection: location of a class of units, object, or activity of military interest.
c. General identification: determination of general target type.
d. Precise identification: discrimination within a target type of known types.
e. Description: size/dimension, configuration/layout, components construction, equipment count, etc.
f. Technical Analysis: detailed analysis of specific equipment.

Table 2 - Approximate Ground Resolution in Metres for Target Detection, Identification, Description and Analysis

Source: Yahya A. Dehqanzada and Ann M. Florini. *Secrets for Sale: How Commercial Satellite Imagery Will Change the World*. Washington D.C.: Carnegie Endowment for International Peace, 2000.

The individual satellites are currently limited by poor revisit times to specific targets. This factor is mitigated by the growing "virtual constellation" of commercial remote sensing satellites that is comprised of the collective resources of all of the available private companies. The Western European Union (WEU) satellite center has grown its capability through the concept of exploitation of all available commercial resources rather than restricting to merely European sources.



Comparing resolutions: Three views of the same Yannan-class Chinese ship at 5-meter, 1-meter, and 20-centimeter resolutions. (Agence France Presse/downgraded imagery provided by Vipin Gupta, Sandia National Laboratories.)

Figure 5 - Comparative imagery resolutions

In addition to electro-optical sensors, Synthetic Aperture Radar (SAR) imagery capability is improving significantly. SAR imagery relies upon the analysis of a signal transmitted in the microwave part of the electromagnetic spectrum and the interpretation of its return signal. Unlike electro-optical systems, these sensors are not limited to daylight operations. Because they have an active sensor, they can image a target in day or night, in any weather, through clouds and smoke.

While current systems are capable of 8-meter resolution, the next few years will see commercial SAR satellites providing 1-meter resolution. These systems will be able to provide a dependable source of militarily significant commercial imagery to NATO forces as well as to our adversaries.

A number of NATO nations purchase commercial imagery to support their own national imagery requirements. In many cases, these images can be redistributed freely. While NATO commands are able to purchase commercial imagery themselves, national sources of imagery should be consulted, as part of any collection effort, to ensure that commercial imagery needs cannot be addressed through existing sources.

The "virtual constellation" of commercial remote sensing satellites will ultimately be able to provide a target revisit schedule that will increase its reliability as a source of imagery. Until that time, the vast archive of commercial remote sensing images remains a rich source of historical data that can be acquired fast and at low cost. Historical data is optimized for mission planning, mapping and humanitarian support operations when detailed knowledge of infrastructure is essential.

Defining Source Access Requirements (Dangers of Pay-per-View)

It is a relatively easy endeavor to identify private information sources that can support the information needs of an OSINT programme. With the proliferation of restricted and open access Intranets, there are great pressures to place all information acquired onto web-based dissemination systems.

While single copy licenses to information

sources are typically attractively priced, multiple user licenses increase in price. License costs are generally a factor of the number of users that have access to the information. To place information directly onto servers without the knowledge and consent of the information provider is a violation of copyright laws.

An option to reduce costs is to determine the information needs of the organization based on communities of interests. Some information is required by all staff and merits a general site license. Other information is of interest to a more restricted audience. Lloyd's shipping data, for example, may be of general interest to a wider audience but of job specific interest to a select group of analysts. The purchase of a limited site license and the use of restricted access within the Command's Intranet will greatly reduce license costs yet still provide the information in the most effective manner. Finally, ad hoc information requirements may be addressed with the acquisition of single copies of key information sources.

As a general rule, there are few information sources that are required by all members of a staff. Restricting access to some sources will increase the range of open sources that are available for purchase within an organization's OSINT budget. Careful planning and the identification of the logical communities of interest for individual open sources is a reasonable approach to manage scarce resources.

SECTION B. SOFTWARE

Software Hierarchy

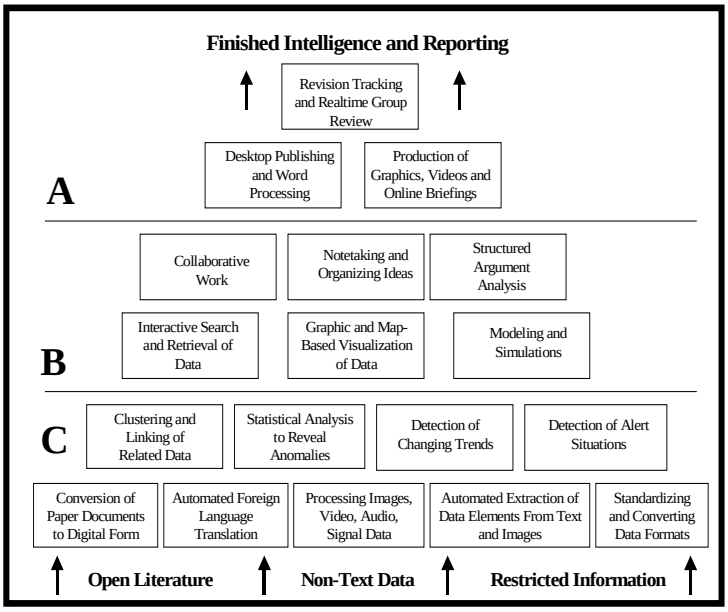


Figure 6 - OSINT Software Hierarchy

Above is an illustration of the eighteen distinct software functionalities that have been identified as being necessary for the optimal processing of open sources of information by any analyst—these would comprise the desktop "toolkit."

Section A functionalities include publishing and production management functionalities. Section B functionalities combine

collaborative work tools with data visualization and manipulation tools with thinking tools: modeling and simulation and structured argument analysis. Section C functionalities combine tools for the automated pre-processing of data once it is digital, and with tools for converting hard copy and multi-lingual or multi-media information into a single digital standard.

Unfortunately, the state of the software industry in general, and of desktop software in particular, is such that today it is not possible to integrate all of these functionalities at an affordable cost. A major obstacle to progress is the existing industry practice of concealing and constantly changing Application Program Interfaces (API). This means that third party software producers desiring to have their offerings work with another major product, must undertake lengthy and often expensive negotiations in order to be shown the proprietary API. Software today is still not "plug and play", and it is unlikely to become fully intergratable "out of the box" until standards of stability and transparency for API are established.

Having said this, it is possible to identify several software packages of some value to the open source intelligence analyst or the action officer working with open source intelligence.

SECTION C. SERVICES

Collection Services

Collection services include online collection (searchers that specialize in Internet, deep web and premium commercial online source exploitation); off-line grey literature or document acquisition; telephone surveys and electoral or other forms of polling; private investigations and human intervention services ("boots on the ground"); and aerial surveillance or reconnaissance services.

Processing Services

Processing services include data conversion from hard-copy or analog to digital, indexing and abstracting of hard-copy or soft-copy textual data or images, interpretation and annotation of imagery or signals, database construction and stuffing, and complex modeling & simulation projects with the best ones including geospatial and time-based visualizations.

When integrated with well-planned open source collection and the right analytical expertise, complex processing services can yield substantial dividends by compressing large amounts of data into manageable tailored products that address specific intelligence requirements.

Analysis & Production Services

A wide variety of commercial and academic organizations offer diverse analysis and production services. As a general rule, the best value is found through the hiring of single individual experts with no overhead, rather than through broad contracts with organizations that then adds a substantial fee for their considerable overhead expenses.

The very best value results when niche collection, niche processing, and niche analysis services can be "mixed and matched" to obtain precisely the desired results. The very worst value comes when an organization is hired because of a convenient contract, they do not have a niche expert, and choose to dedicate an

analyst that does not bring sufficient experience or skill to the task.

Industry leaders can best be identified with reference to citation analysis and familiarity with their product set. This is best accomplished through the identification of other organizations with similar intelligence problems and exchanging information concerning those validated information vendors that they employ. Web-site analysis is another tool, which can be applied to vet the capabilities of a potential information vendor.

Services Examples

Data Conversion	ACS Defense www.acsdefense.com
Database Construction & Stuffing	ORACLE www.oracle.com
Document Acquisition	British Library Document Centre http://www.bl.uk/services/bsds/dsc/
Human Intervention	The Arkin Group www.thearkingroup.com
Imagery Interpretation & Annotation	Boeing Autometric www.autometric.com
Indexing & Abstracting	Access International http://www.accessinn.com/
International Studies Analysis	Monterey Institute of International Studies www.miis.edu
Modeling & Simulation	Boeing Autometric www.autometric.com
Online Collection	Association of Independent Information Professionals www.aiip.org
Open Source Intelligence Portal (meta-service)	Open Source Solutions Inc. www.oss.net
Private Investigation	Intelynx (Geneva) www.intelynx.ch
Scientific & Technical Analysis	CENTRA www.centratechnology.com
Signals Processing	Zeta Associates Incorporated www.zai.com
Telephone Surveys (Primary Research)	Risa Sacks & Associates www.rsacksinfo.com

Table 3 - OSINT Related Services

As a general rule, there are no "portal" companies that serve as honest brokers for helping governments "mix and match" best in class niche providers at the most economical cost.

CHAPTER III
THE OPEN SOURCE INTELLIGENCE CYCLE

SECTION A. OSINT PLANNING AND DIRECTION

Overview

Whether one is going after open source data, information, or intelligence, there is a proven process of intelligence, the intelligence cycle that will yield good value when applied. The open source intelligence process is about discovery, discrimination, distillation, and dissemination—the 4 Ds (Figure 7). This analytical approach is applied to the traditional single source intelligence cycle. A good understanding of the open source intelligence cycle makes it possible to access and harness private sector knowledge using only legal and ethical means, generally at a very low cost in comparison to covert technical or clandestine human collection. Since many requirements that are urgent for the commander and their staff may not qualify for nor be appropriate for secret collection methods, the open source intelligence cycle is in fact *vital* to NATO planning and operations. As will be seen in the following discussion, OSINT is an emerging discipline and the emphasis will often be on informal coordination rather than formal tasking.

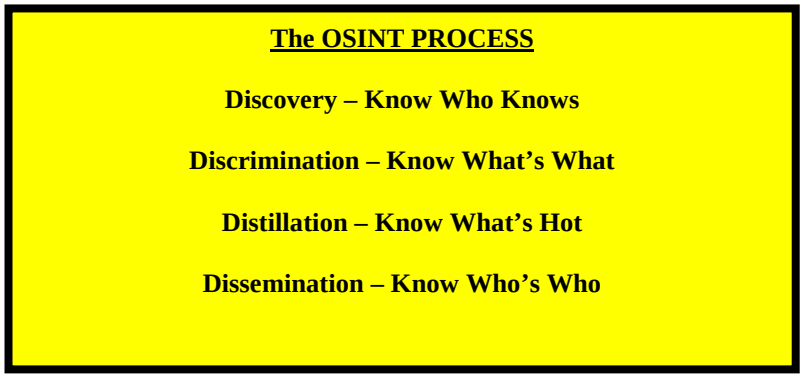


Figure 7 - The OSINT Process

Organizations and Responsibilities

The commander is ultimately responsible for establishing the Essential Elements of Information (EEI) and for applying the resources necessary to satisfy them. Open source intelligence is *not* necessarily the responsibility of, or available from, national-level intelligence organizations. While the intelligence staff typically acts as the staff principal for OSINT activities, other staffs are frequently well placed to both collect open sources and to facilitate the further development of sources on behalf of the Command. The subordinate commanders for Civil Affairs, Public Relations, Military Police, and Combat Engineering may often be the best channels for seeking out OSINT, and can comprise an informal advisory council to the commander.

OSINT sources include, but are not restricted to:

- **National-Level Intelligence Organizations**. Although they are not responsible for satisfying the commander's needs for OSINT, national-level intelligence organizations may have relevant open source information that can be provided. Some countries, such as The Netherlands, United Kingdom, Denmark and Norway, are exceptionally competent in this area and have fully integrated OSINT into their all-source collection and production environments. Others may have selected units that can be called upon, but have not yet mastered this discipline.

- **Diplomatic Missions**. The established diplomatic missions of the various member nations are often the best source of OSINT, at little cost, if they are approached by one of their nationals acting in an official capacity on behalf of the commander. Such missions are under no direct obligation to respond, but informal coordination may yield good results.

- **Chambers of Commerce**. Many of the member nations have Chambers of Commerce and these often have established small communities that bring the general managers and key business executives from their national firms in any given country together. On an informal basis, with clear disclosure of the commander's interest, useful OSINT may be acquired. This is particularly true in deployed areas.

- **Non-Governmental Organizations**. The International Committee of the Red Cross (ICRC), Doctors Without Borders, and the many elements of the United Nations as well as the many international relief and charity organizations, have deep direct knowledge that can be drawn upon through informal coordination.

- **Religious Organizations**. Many Non-Article 5 Operations have very substantial human mass migration and ethnic conflict aspects as witnessed during Operation Allied Force. These issues are often best understood by religious organizations. Organizations such as The Papal Nuncio and the local Opus Dei, the B'nai Brith, the Islamic World Foundation, and other equivalent religious organizations are an essential source of overt information and expert perceptions

Requirements Definition

The greatest challenge for the commander will be the establishment and maintenance of a rigorous and disciplined process for defining the requirements to be addressed through open sources. The common attitudes of "tell me everything about everything" or "if I have to tell you what I need to know you are not doing your job" represent unworkable direction.

Commanders and their staff must carefully evaluate the specific information needs in the context of their concerns and their plans and intentions, and they must articulate, in the narrowest possible way, precisely what they want to know and why. The commander's operational intent is as vital to the intelligence professional as it is to the operations professional. Only by understanding the context and direction of the commander's requirements, can a truly focused and flexible collection effort be undertaken.

OSINT is the most fundamental and fastest means of satisfying basic informational

needs, including needs for historical background, current context and general geospatial information. Each commander should distinguish between their tailored intelligence requirements in support of their future planning and the basic information requirements that will permit operational and logistics and other special staff planning (e.g. Civil Affairs) to go forward. OSINT is highly relevant to both kinds of intelligence support.

Evaluation and Feedback

Planning and direction is a continuous process. The commander and their staff must digest, evaluate, *and provide feedback on* all received intelligence, whether open or classified. As open source intelligence is received and reviewed, it must be shared with staff principals and subordinate commanders, evaluated, and the results of the evaluation passed directly to the staff element responsible for coordinating OSINT support to the commander.

SECTION B. COLLECTION

Overview

The heart of intelligence collection is research – it is the matching of validated intelligence requirements to available sources with the aim of producing a product that answers a valid need. Once an intelligence need has been identified, open sources should be reviewed by intelligence staffs to determine if that intelligence need can be satisfied through those resources organic to the intelligence staffs, those resources that the staff can access, if an RFI to nations is required, or if a combination of these approaches is required.

Collection requires the translation of an intelligence need into an intelligence requirement – an action plan to answer that need. A collection strategy is developed to tap available sources. Optimal sources are selected and the information is collected. This generic collection approach is equally applicable to classified sources as it is to open sources.

In the NATO context, OSINT is a contributing source to an all-source intelligence effort. Open sources are used to compliment the existing classified intelligence and can be collected on a specific area. OSINT-derived products are created to answer a specific intelligence need to which open sources are best optimized. While RFIs from intelligence users typically generate collection efforts, Table 4 illustrates the three types of producer generated intelligence collection and production requirements.

These three categories outline the way in which an internally directed OSINT

Analyst-driven	**Based on knowledge of customer and issues**
Events-driven	**In response to time-sensitive relevant events**
Scheduled	**Periodic activities to document and update target status**

Table 4: Types of Producer-Generated Intelligence Collection and Production Requirements

Source: Arthur S. Hulnick. "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach." Intelligence and National Security, Vol. 1,No. 2, (May 1986)

collection strategy should be developed. Only those products that support the intelligence staff's mission should be produced. The range of open information that is available both freely and commercially will swamp the analytical capacity of any intelligence staff regardless of size. Therefore, effective management must include the avoidance of production without a specific purpose. While not advocating a "make work" approach to intelligence, producer-generated collection builds skills, evaluates sources and increases capabilities necessary to address future RFIs and production requirements.

An analyst is often best placed to determine what product is required to address the past needs of the intelligence user. Proactive collection and management to make effective use of emerging information should be encouraged. This could include the tailoring of a newly available public report that addresses an established intelligence need into a format of use to an intelligence user.

Rapidly changing events can drive the production of new products. A military coup or an environmental crisis could presage increased NATO interest in an area of non-traditional interest. In the absence of national intelligence production shared with NATO, open source collection may be the best means with which to begin to build an intelligence picture for the command.

Less dramatic changes to the international environment may also require open source collection. Seasonal changes in a particular region may lead to population migration. These periods are known well in advance and lend themselves to scheduled production of necessary intelligence products.

Chapter II reviewed private sector information offerings. Chapter III focuses on the methods to be applied by any NATO unit to exploit those offerings, while not recommending any specific source, software, or service. What is important is that every NATO unit is conscious of the overall process, the alternative means for obtaining and exploiting OSINT, and the value of OSINT as part of the all-source intelligence cycle. Figure 8 below is provided a high-level view of the elements of the OSINT collection process.

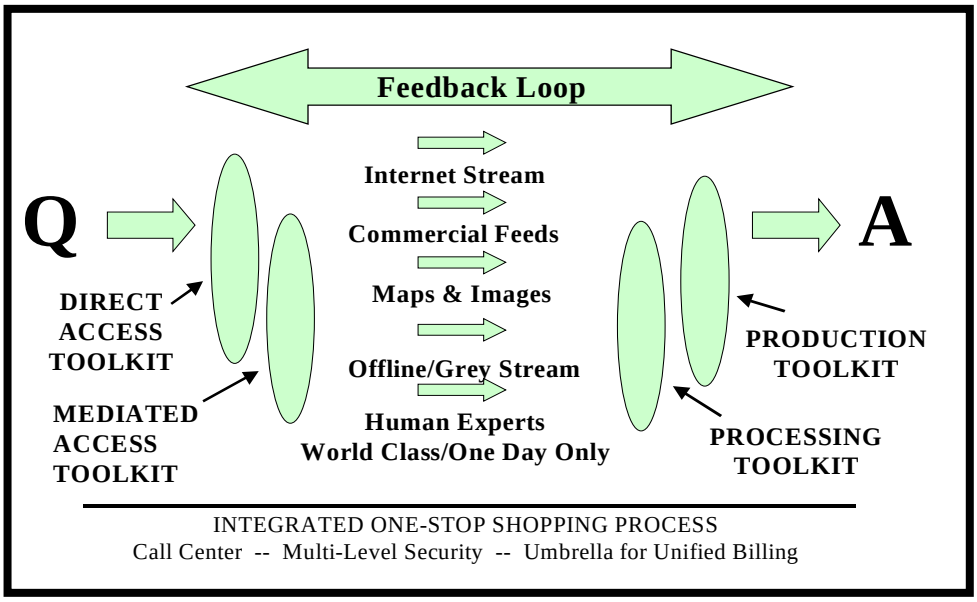


Figure 8 - OSINT Collection Process

Knowing Who Knows

During periods of stability as well as crisis, it is incumbent upon intelligence staffs to establish and nurture sources that will help satisfy information requirements. It is vital that the OSINT professional, known in some governments as Open Source Officers (OSO), focuses initially on "knowing who knows" – the ability to rapidly identify subject matter experts on topics of direct relevance to the commander's mission and to seek information from them.

An approach favoured by some is the concept of collecting sources not information. While the array of available open sources is staggering, the ability to focus collection quickly on an emerging issue of intelligence interest is the key capability. Rather than having a stale open source product to draw upon, the ability to rapidly direct collection on an issue, identify the leading experts on the field and either draw upon their most recent work or contact them directly is the most effective use of an OSINT capability.

Therefore, a standing collection priority should include a preliminary inventory of subject-matter experts (SME) within the parent commands and its subordinate, adjacent, and higher commands, but should then extend further, throughout the parent government and into the national private sector. The business community with its international chambers of commerce, the academic community with its various professional associations, and the non-governmental organizations including the peace institutes resident in many countries, are all vital points of reference.

The command OSO is, in essence, an information attaché to each of these elements, and must always act with the highest standards of overt decorum and propriety. This must include a firm grasp of both the private sector's rights and obligations with respect to copyright and the protection of intellectual property, and NATO's concerns with regard to OPSEC.

Collection Discipline

There is no faster way for an OSO to lose his commander's respect than to try to do too much, and end up taking too long to produce simple answers. Time management, and a very disciplined approach to the art and science of OSINT collection, is the key to every success.

The ever-increasing array of open sources provides a rich environment for unbridled research. OSINT managers must ensure that their staffs are aware of the degree of detail required for each OSINT product being prepared. The Internet and commercial premium online sources are seductive to the analyst. Within any OSINT effort, time spent in collection is always at the expense of analysis. The desire to continue with the

OSINT Professional Note: A recommended timetable for a standard OSINT collection and analysis task is provided below:

15 Minutes	Requirements Definition. Ensure an understanding of commander's intent.
30 Minutes	Internet Collection. Use search tools, rapidly identify top ten sites and review.
15 Minutes	Internet Table. Create Internet Table for future use and for customer's reference.
60 Minutes	Commercial Collection. Use fee sources, identify top 20 items for exploitation.
60 Minutes	Analysis. Read, understand, evaluate, and structure collected information.
60 Minutes	Production. Carefully create an analytical summary, table of contents, and slides.
4 Hours	Total time required to create any OSINT report using only internal resources.

collection and acquisition of open sources at the expense of their evaluation and presentation as an analytical product reduces the effectiveness of the OSINT contribution to the all-source effort. In few other fields is the mantra that "perfection is the enemy of good enough" more appropriate than it is for open source collection. Collection efforts can be reduced if time spent in the evaluation of the reliability and objectivity of specific open sources does not have to be replicated each time an analyst begins a project. OSINT managers should ensure that their staff maintains a dynamic compilation of the open sources that they exploit for specific issues. This reference aid will serve as the starting point for subsequent analytical tasks.

Collection Issues

There are several collection issues that always surface whenever commanders and staff first consider OSINT as a structured discipline. These include OPSEC, Copyright Compliance, Foreign Language Shortfalls, and External Networking.

Operations Security

- OPSEC is easily achievable in the OSINT environment through two measures: first, the concealment of the origin of the search through the use of trusted intermediaries; and second, the utilization of normal commercial Non-Disclosure Agreements (NDA) when necessary to protect direct discussions of a commander's concerns and intentions.

- In general, most OSINT inquiries will be amply protected by existing processes, but when appropriate, a trusted local national with information broker skills can be hired (or a Reservist utilized) to distance the inquiry from the command. It is a misconception to believe that any discussion with OSINT providers must be itself open.

- The private sector is accustomed to protecting proprietary and commercially confidential discussions. A standard private sector NDA is just as a good as a government secrecy agreement, with the added advantage that the private sector partner has a financial motivation for honoring the NDA—they want more business and discretion is part of what they are selling.

Copyright Compliance.

- In the past, many governments have felt that copyright compliance did not apply to their official needs, and some governments have resorted to the classification of open source information as a means of concealing their routine violation of private sector intellectual property rights

- It is now essential for all governments, and for all NATO elements, to learn how to properly comply with applicable copyright provisions. This is important for two reasons:

  - To maintain the highest standards of legal and ethical behavior among all NATO elements;

  - More often than not, OSINT must be shared with external private sector parties (e.g. humanitarian assistance organizations) or used as a means of exchange (pooling information on Kosovo, for example). Thus copyright compliance is a vital means of maintain future *flexibility* in the exploitation of the OSINT available.

Foreign Language Shortfalls.

- Despite the multi-cultural and multi-lingual nature of the NATO alliance, many out-of-area contingencies require

foreign language skills that are not readily available with the NATO force, or that can be identified quickly and provided with security clearances.

- Over time it is vital that each commander identifies foreign language skills as well as shortfalls and that these be consolidated and evaluated as part of the larger NATO Future Intelligence Architecture plan.

- Understanding international terrorism, insurgency, and violent internal political opposition movements, to take one example, requires competency in a number of foreign languages to include: Arabic, Catelan, Danish, Dari, Dutch, English, Farsi, Finnish, French, German, Indonesian, Irish, Italian, Japanese, Korean, Kurdish, Kurmanji, Norwegian, Pashto, Polish, Portuguese, Russian, Serbian, Spanish, Swedish, Tamil, Turkish and Urdu.

- Many of the required capabilities are within the competence of national intelligence organizations but these capabilities are unlikely to be made available to NATO commands for the exploitation of OSINT.

External Networking.

- There are four obstacles to external networking relevant to NATO competency in OSINT.

- First, there is a lack of knowledge about who the real experts are on various regional and topical issues.

- Second, there is a fear of revealing the question as an official inquiry—in some countries; there are even prohibitions against direct contacts between intelligence personnel and private sector experts.

- Third, there is the lack of funding for compensating subject-matter-experts—everything must be done on a barter or exchange of favors or information basis.

- Fourth and finally, the existing command & control, communications, computing, and intelligence (C^4I) architectures tend to prohibit routine access to the Internet, and often make it difficult if not impossible to migrate unclassified information from the Internet into classified databases.

All of these obstacles can be overcome. A major outcome of the new NATO OSINT initiative will be the definition and resolution of each of these obstacles.

Nuances of Open Source Collection

The Internet, although it will never be a completely trustworthy source for information, has become the *de facto* C^4I backbone for everyone other than the military. It is essential that our intelligence, operations and logistics staffs develop new doctrine and new methods for fully exploiting the data sources and the human experts that are easily accessible through this medium. As NATO deals with more and more non-traditional threats and more and more out-of-area as well as civil stability scenarios, OSINT will become a much more important element of the all-source intelligence solution. It is vital that every NATO commander and relevant staff member begin now to understand and plan for their OSINT needs.

Training in open source exploitation is relevant not only to the intelligence professionals, but also to all relevant staff

members who need access to open sources of information. OSINT is not the exclusive purview of the intelligence profession. The intelligence professionals should be available to reinforce the commander and their staff, but as a general rule, if a staff principal can answer his own information requirement exclusively through those open sources available to him, then that staff principal that should manage his own collection effort.

Intelligence staffs should enable all staff elements to access relevant open sources as directly as possible. Intelligence staffs should serve to facilitate the flow of OSINT and open source material while providing source evaluation and guidance. Applying this process will enable many potential RFIs to be self-satisfied and thus not submitted. A robust OSINT programme can reduce the number of unnecessary RFIs that bog-down the all-source intelligence staff with information requests that can otherwise be satisfied.

While each commander will have their preferred means of managing OSINT, what is required is that they have a formal point of contact for OSINT matters, an established process, and that they ensure that OSINT is fully integrated into every aspect of their command & staff operations.

The Internet, despite its current and projected growth, is primarily a vehicle for open collaboration, rather than a repository of knowledge. Commercial online sources such as Factiva, DIALOG, LEXIS-NEXIS, STN and Questel-Orbit have huge repositories of information that have been professional selected, evaluated, indexed, abstracted, structured, and made available in a very stable format with authoritative sourcing, formatting, and dating.

In many cases, the information provided through these services have been “peer reviewed” – an exhaustive evaluation process by established leaders in the field of study to ensure the accuracy of the information and the rigor of the research. The Internet is not a substitute for premium fee-for-service commercial online databases, and it is vital that no NATO element falls prey to this illusion.

Each commercial service, as discussed briefly in Chapter II, has its own strengths and weaknesses. A robust OSINT capability should include the understanding of and the means to exploit each service accordingly. Some are best for current news, others for legal records, and others for access to conference proceedings and dissertations.

According to some OSINT experts, only a fraction of known knowledge is available online, either through the Internet or through the commercial online databases. Grey literature, the limited edition publications that are not available through normal commercial channels, comprises a vital "middle ground" between online knowledge and human expertise capable of creating new knowledge in real time. Therefore the NATO OSINT process includes the inventory and evaluation of grey literature sources, and the development of a strategy, a budget, and a process for assuring that grey literature sources are fully integrated into the NATO future intelligence architecture.

Finally, there is the human element. As OSINT doctrine is developed, it would be helpful to think of three distinct forms of overt HUMINT support to NATO. First and foremost are internal subject-matter-experts. These are scattered across commands and within various elements of the member nations’ governments. Second are the private sector experts who have achieved a favorable reputation based on their proven record of accomplishments and publications. Thirdly, there are "local knowledge" experts, including legal travelers and local residents that are rarely exploited by resident defense attachés for lack of time or funding with which to reimburse individuals for their time and expense.

New means must be found for defining

which local knowledge and local observation is needed, and for combining direct observation by qualified NATO personnel, with out-sourced overt collection and production.

SECTION C. PROCESSING AND EXPLOITATION

Overview

After the vital role played during the collection portion of the intelligence cycle, when "knowing who knows" and being able to "mix and match" niche providers of varying pieces of the OSINT solution is essential, it is in the processing and exploitation portion of the cycle that the OSO really makes a mark.

Open sources, just like clandestine or covert sources, require the application of human judgment in order to sort out the important from the unimportant, the timely from the dated, the relevant from the irrelevant, the trusted from the untrusted. As so much of OSINT is *not* in digital form, hands-on human translation and evaluation are the most important part of processing and exploitation.

Without a dedicated set of automation tools to facilitate the processing of open source information, OSINT production will continue to be reliant upon *ad hoc* software solutions and rigorous analytical effort.

Analysis

When working from open sources, there is considerable danger for the analyst to be susceptible to unwanted biases and deception from open source authors. While it is never wise, nor an acceptable practice, to attribute as fact intelligence solely because it was received from a national intelligence agency, in those cases, the analyst is able to make certain judgments regarding how that agency managed its information prior to releasing its report. This is not always true for open sources. It is essential that the analyst remain mindful of and determine the origin of the information that has been gathered and the degree of trust that can be assigned to it. Appendix C provides a list of some common misperceptions and biases.

In the production of OSINT reports, it is crucial that the reader be aware of what is known and what is being speculated about. The analyst should always be careful to distinguish between information and fact. If the original source material is not provided

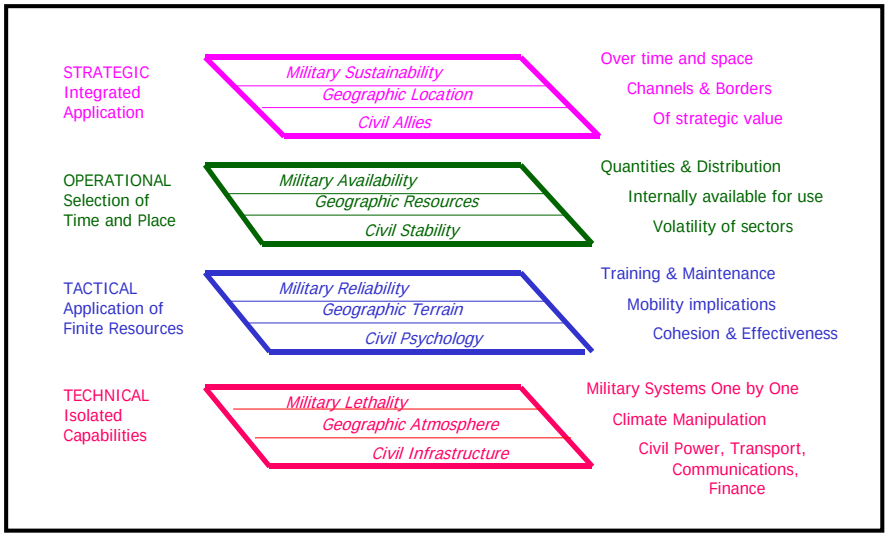


Figure 9 - Levels of Analysis Model

in full text, it is important to make reference to it and provide an assessment of the source's credibility.

If at all possible, the original sourcing information should never be separated from the open source reporting. A complete description of where the open source information was acquired, the identification of the source, the timing of both the production of the open source information and the timing of its acquisition—these all comprise fully half the value of an OSINT product. Without the sourcing pedigree, the open source substance must be considered suspect and of minimal value to the all-source intelligence analysts or the operations or policy consumers being supported.

It is also helpful when processing open source (or classified) information manually to have in mind a clear model of analysis that distinguishes between military, civil, and geographic information, and also between the levels of analysis—strategic, operational, tactical, and technical—for the threat *changes* depending on the level of analysis. This also helps the analyst to recognize gaps in their collected information, and the relationship between different types of information. One such model is provided in Figure 10 above for illustrative purposes.

Web Site Authentication and Source Analysis

Content on the Internet continues to grow at logarithmic rates. The Internet has become an essential enabling element for commerce. It is also facilitating other forms of human interaction across borders which two decades ago were unimaginable. The intelligence value of information found on the Internet is extremely variable. The dangers of creating misleading analysis through the bleeding of unevaluated biased information into the all-source intelligence picture are ever present. Therefore, the OSINT analyst must take steps with each open source to evaluate its reliability. The standard criteria for evaluation of web-sites are as follows:

Accuracy.

- Is the information that is provided consistently accurate based on other sources? The OSINT analyst is able to compare information provided from the web-site with validated all-source intelligence. Benchmarking open sources against validated all-source intelligence assists in assessing the likely accuracy of other information contained on the web-site to be used to address intelligence gaps.

Credibility & Authority.

- Does the web-site clearly identify itself? Is there merely an E-mail address or a full name, address and telephone number. *Sam Spade* (www.samspade.org) is a web service that provides various online tools to validate a web-site. These include diggers that trace routes used by the web-site. (See Web-site Analysis Guide on the following page).

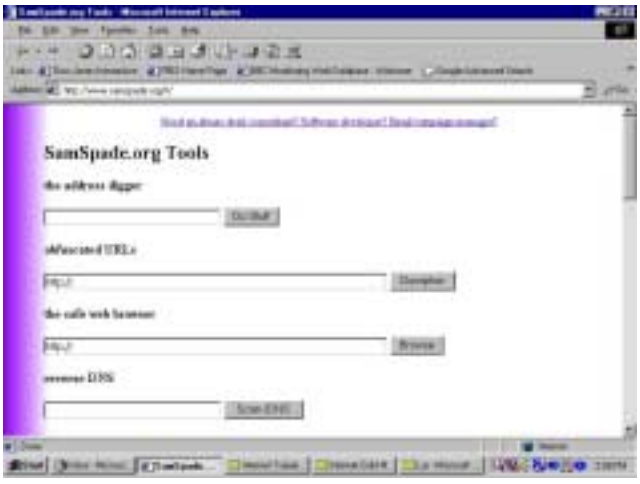


Figure 10 - Web analysis tools

- Does the web-site demonstrate a degree of influence? Do other media cite that web-site in their reporting? Has the web-site been attacked electronically or in official government statements?

- The use of free web-hosts such as Geocities.com or Cybercafe.com often suggest limited financial support for the web-site and a lack of authority in its message.

- Hit-meters/Counters that note the number of times the web-site has been visited can also provide some limited indication as to the influence of the web-site. Thought these can be misleading and should only be used as an element of an assessment of a site's authority.

Currency.

- Does the web-site provide information that is timely or are its pages dated? Some dated information can still be relevant for less dynamic topics (e.g. trade statistics) but may be misleading in tracking current events (e.g. presence of insurgent activity).

Objectivity.

- Does the web-site correspond to a known advocacy group? Does the site represent individuals or an organization? Does that site claim to speak for the organization? Is that site the main web-site or a satellite web-site that represents only a sub-element of the organization.

- To whom does the web-site link? Many sites provide a list of relevant links. These attempt to direct visitors to a community of interests that share similar interests or views. An evaluation of those links can further illuminate the views of the web-site authors.

Relevancy.

- Is the information contained on the web-site relevant to the question at hand? Many web-sites provide information related to a particular topic but do little to add to the understanding of the issue. Information provided can often be interesting but not relevant to the OSINT analyst.

WEB SITE EVALUATION CHECKLIST

Each Internet Website of potential intelligence value must be evaluated as to its suitability for intelligence exploitation *before* it is cited in OSINT reports or used as collateral information in classified reporting. The essential questions remain: who, what, where, when and why?

1. WHO? Examine the URL first. In the page scan for names, and "about" links.

What type of domain is it? (.com / .org / .edu / .gov / .mil / country code) – Is this appropriate for the material presented?
Might it be a personal page? (use of ~ in URL often suggests this)

Who wrote it? **Look for e-mail contact.**
Credentials? **Search on author's name.**
Check source code as webpage's author is often embedded in the code.

Who is the owner of the host server? **Use WHOIS and DNS LOOKUP tools at www.samspade.org to determine the registered owner of the website and evaluate this information. Does this match earlier information gathered?**

What do others say? **Search to see if others cite the author or the web-site.**
Who links to it? **In Google or AltaVista, enter the search string (*link:webaddress)* to find who links to the site. Evaluate the community of interests.**

Opinions of it? What do others think of this website?
Found in any reliable directories? **Determine if the website is contained within reliable web directories or web portals for the topic.**

2. WHAT?

Is the material presented authentic, with sources and dates?
Is data unaltered from its original source?
Note: Little value can be attached to information that is either undated or unsourced.

3. WHERE?

Where does the information originate? **Use www.samspade.org to conduct a TRACEROUTE search. TRACEROUTE will determine the path between your computer and the server hosting the information.**
Is the server located where the author purports to reside? Why or why not?

4. WHEN?

How current is the information provided? **Look for a last updated statement or dates on references.**
How often is the information maintained? Should it contain more recent information?

5. WHY?

What's the page's aim, intent?
Why was it created?
Who sponsor's the page? **Look for an "About us" entry.**

Source: Developed from material created by Joe Barker and maintained on server: www.lib.berkeley.edu.

SECTION D. SEARCHING ANONYMOUSLY ON THE WEB

Overview

While much of the OSINT cycle can be conducted openly, a robust OSINT programme should include a capability to work anonymously on the Internet. Despite the fact that all information on the web is freely available to anyone with a PC and an Internet connection, there are security dangers in searching for it.

All Internet traffic is subject to monitoring at virtually any point by elements external to your organization. It would be of little surprise that NATO was interested in insurgencies in the Balkans and Internet searches on this topic would seem natural from Alliance web addresses. Specific searches on individual leaders of insurgent groups would reveal a heightened interest and potentially reveal intentions. This sort of activity should be protected.

Being anonymous on the web may not necessarily involve deception. It is quite possible to surf the web without openly identifying your identity, purpose or intentions. This is simply a case of "I won't tell you unless you ask."

Before you even start surfing anonymously make sure you don't leave your Internet connection open to attack. You may take all the precautions necessary to hide your intentions and identity whilst surfing, but, without precautions, all the sites that you have visited and all the information you have downloaded is stored on your PC is available via your open connection, then you are vulnerable.

There is an argument for the use a firewall to stop hackers at the front door, but remember that there hasn't been a firewall yet that wasn't eventually cracked. The very expensive firewalls do a good job but it is

Elementary steps to create and maintain an anonymous WEB-Presence

Disable anything that records your activity.

If using MS Internet Explorer:

- **Turn off the cookies**
- **Clean out the history folders, and**
- **Routinely remove cached files.**

Use removable storage media to save any downloaded files to.

Only use your Internet PC for surfing. Do not use the word processor for business or personal letters.

Make sure all your connection details are anonymous.

Ensure the set up of your system is as standard as possible.

Figure 11 - Maintaining an anonymous presence

unlikely that you would want to spend so much money for a simple Internet connection. Besides if you wanted to remain anonymous on the Internet an expensive firewall is not the way to do it. It would highlight the fact that you had something to hide. The same argument applies to the cheaper firewalls. Because they are cheap they are also vulnerable. Hackers know how to get in and often see areas with firewalls as a challenge. One of the best means of security is to remain anonymous and look just like everyone else. By doing this, if a hacker chooses to attack your Internet connection whilst you are online, they would find nothing. The hacker would probably then get bored and never bother you again.

Leaving a Footprint

When you surf the Internet you cannot fail to leave a footprint. A footprint is an electronic signature that identifies you as a unique identity on the Internet during your current session. Most Internet Service Providers (ISPs) now issue a new signature to you each time you log on to surf. But whilst you are surfing during a session after log on, every site you visit retains your electronic signature. If you are trying to find information on a sensitive subject it is possible to carry out an analysis of the sites you visit and the subjects you are searching for. It would be sensible to log off and on again a number of times during a sensitive search.

Although an ISP may provide you with a new signature, part of that signature will identify the ISP. If your organization is large and has its own ISP this will identify your organization. It is always better to go through a civilian ISP whenever possible.

It is possible to use a number of different ISPs. These days there are a huge number of free ISPs available. Each country has its own list of free ISPs and details of these can be obtained via the Internet. It is possible to hide the country from which you are searching from by dialing up an ISP in another country and beginning your search from there. It is almost impossible for a hacker to identify which country your call originated from because Telecoms companies take their personal privacy obligations very seriously.

There is one thing that may identify your country of origin and that is the date and time of your search. When you surf, the date and time of your PC is stamped on the search as part of the electronic signature. If this does not match your ISP time it may indicate that you are trying to hide something, so make sure your PCs time is set to the time zone of the country of the ISP you are using.

Traffic analysis

Every web site has the capability to log the number of visitors to its site and the electronic signature of the visitor. Whilst you may be able to hide your identity, you cannot hide the fact that you have visited the site. If the number of visitors to a significant site increases dramatically then this may be an indicator that there is new or renewed interest in the subject of the site. Such a site may be set up deliberately to identify interest, for example an obscure terrorist related site.

The way to combat this is to ensure that trained personnel, in a central location do all sensitive searches. This will ensure that searches are done quickly and without repetition. The security education of all personnel who have access to the Internet is also a very important factor.

Contact with Others

There may be occasions when you may want to communicate with others to solicit information. In most cases it is beneficial to explain who you are and ask for help or information. There may be other occasions when you may not want others to know exactly who you are or whom you work for. The reasons for this must be decided on a case-by-case basis. It is reasonably easy to create an anonymous persona on the web but the following points should be noted.

It is better to employ discretion rather than deception when soliciting information on the web. This will be less publicly embarrassing later and will make an explanation of your action more reasonable.

An anonymous persona should only be used for occasional requests for information. Any development of a relationship using the Internet should be discouraged. This is the field of other specialists and without proper control can lead to embarrassment.

SECTION E. PRODUCTION

Overview

The four main elements of OSINT production are listed in Figure 12. As

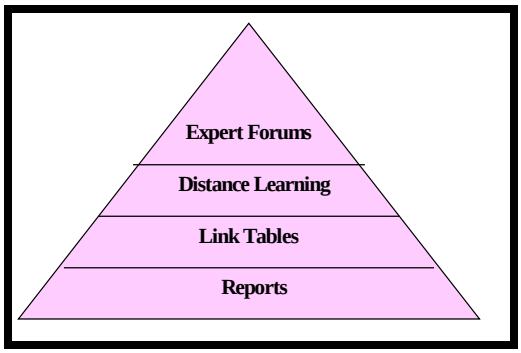


Figure 12 - OSINT Production Elements

opposed to other intelligence disciplines, OSINT relies upon outward engagement beyond the institutional confines of the intelligence staffs. Engagement is essential to the successful exploitation of open sources. This requires knowledge and understanding of information outside of intelligence channels in order to locate and exploit the best sources of information relevant to an intelligence problem and engage them in a meaningful exchange.

OSINT's four production elements will be explained within this section. While the degree of complexity will vary depending upon the intelligence requirement, those four elements will all remain applicable.

A major difference between the OSINT process and the traditional all-source intelligence process exists in how "reports" are treated. In the traditional classified intelligence process, reports are the end of the process—in the OSINT process; they are the beginning, one of four key elements in the *interactive* and *consumer-oriented* process of OSINT support.

Reports

In Chapter One, a distinction was drawn between OSIF, data that has been collated together and is of generic interest, and usually broadcast or widely disseminated and OSINT, information that has been deliberated discovered, discriminated, distilled, and disseminated to a specific consumer in order to answer a specific intelligence need.

NATO OSINT specialists will have occasion to do both kinds, but must be very clear in their own mind, when doing a report, as to whether it is an information report for general broadcast, or an intelligence report for a specific operational purpose.

A report should have an analytical summary. This is value-added expertise from a trained NATO professional who has first screened and integrated multiple elements into an underlying framework, and then devised an executive summary that can stand on its own.

Generally a Report, e.g. a report on Kosovo, will have more than one section, for instance, sections on political, military, insurgents, health, police, and external assistance. Each section should in turn have a short summary, no more than a paragraph in length. The section summaries can be used to create the overall report summary, but should be further distilled and not simply strung together.

Within each section (or linked to each section summary if done in a web-based format) should be between one and five key items of raw information—whether a transcript from a news conference, or a wire service release, or a commercial image, or an extract from a foreign military map.

A major difference between OSINT and other clandestine or covert sources is that OSINT strives to provide concurrently both analytical value and direct access to raw materials. OSINT sources rarely require protection. Text-based products can be stored and disseminated easily by electronic means.

By providing the consumer (the commander, the operator, the logistician, or the all-source intelligence analyst) with direct convenient access to the best of the raw materials, the OSINT analyst is enabling the consumer to dig deeper if they chose to while satisfying the initial RFI.

Reports should always show, on the first page, the date and hour at which collection (not production) was cut off, and the time period in days and/or hours that the report covers. Reports can be organized by source (Internet, Commercial Online, Grey Literature, and Experts) or by topic. They should always identify the author and if appropriate the reviewer of the Report, and provide complete contact information so that readers may quickly ask follow-up questions of the originator.

COUNTRY (e.g. Sri Lanka)

TOPIC (e.g. Economy)

DATE OF INFORMATION (e.g. 26 March 2001, 1500EST)

ANALYTICAL SUMMARY (new value-added analytic summary)

RAW INFORMATION 1 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 2 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 3 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 4 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 5 (best of 20 read sources from 200 screened sources)

Figure 13 - Representative report structure

Link Tables

Internet search engines, even recommended meta-search engines, have severe limitations. By some accounts, any one search engine will cover only 10-15% of the visible web, and even all the search engines working together will overlook what is known as the "deep web." The deep web consists of complex sites with many levels, many free and some by subscription, where search engines are simply ineffective. While some tools such as the affordable software programme *Lexibot* are available to assist in collection from the "deep web", considerable time is spent in the identification and analysis of open sources relevant to the information requirement. For this reason, a major aspect of the OSINT support process is the skilled creation of Internet Link Tables that serve as a ready reference for the commander or staff officer who desires to rapidly scan external information sources without necessarily requesting a report. This browsing endeavor can often help the commander or staff principal reflect on their requirements and better articulate their next demands for finished OSINT. An Internet Link Table should generally be in the form of a Table, such as is illustrated In Table 5 above. By using the Word Table feature, this allows the sorting of the information based on either the Rank or Weight assigned to the site, the URL or title of the site, or the description category of the site. Over time, as various NATO components cooperate and share Link Tables with other allies forces such as the various regional Joint Intelligence Centers, a very comprehensive directory of web resources, one that is tailored to NATO's needs, should emerge.

Ranking	Link	Source
10	http://allafrica.com/libya/	**All Africa News – Libya –** Up-to-date news on Libya, in English and in French.
10	http://memory.loc.gov/frd/cs/lytoc.html	**Library of Congress Libya Country Study** – Excellent, in-depth country study
10	http://members.aol.com/LibyaPage/	**Libya Resources on the Internet –** Excellent, comprehensive site, includes news, Qadhafi info, maps and satellite photos, military and intel, etc.
10	http://www.un.int/libya/	**The Permanent Mission of Libya to the UN** Website **–** Includes press releases & statements, ambassador's remarks and links.
10	http://www.nfsl-libya.com/	**The National Front for the Salvation of Libya** - The NFSL is an opposition movement against the dictatorial regime of Qadhafi in Libya, and was formed in October 1981.
8	http://www.libyamazigh.org/	**Libyan Amazigh** site. Contains info on Libya's Amazigh (Berber) culture, language and history.
8	http://www.libyaonline.com/index.html	**Libya Online** Website – Contains basic facts about Libya, tourism, business, arts, literature and sports.

Table 5 - Example of Internet Link Table

Distance Learning

The Internet, while rendering a major service to those who would like to share information efficiently and also interact inexpensively with diverse people all over the world, has also reduced the productivity of even experienced personnel. Constant interruptions and distractions through diversions to less important information are

core factors. For this reason, there is an urgent need for Distance Learning modules on all countries and topics that are of interest to NATO. The objective is to ensure that all new personnel, and especially new action officers, have an online resource that can serve as a sophisticated turnover file and reference point. This is also a place where unclassified biographic information can be made available, and where annual reviews of each country or topic can be placed.

The U.S. Pacific command initiative known as the Virtual Information Center is an good example of this process. It can be accessed at www.vic-info.org.

Figure 14 - Homepage of US PACOM OSINT Centre

Expert Forums

A number of software programs exist with which to manage a variety of Expert Forums, including private teams with their own newsletters, calendars, and automated email alerts whenever new information is posted. One of the most popular is the Alta Vista Forum. One of the newest, with powerful security features, is offered by Groove Inc. (www.groove.net) and represents the emerging shift in communications and computing power away from centralized server farms toward what is known as "peer to peer" edge units.

Expert Forums can be internal, external, or some combination of the two. Once experts have been identified, they may be invited to join the Expert Forum sponsored by any NATO element. This should be done with the understanding that they will contribute their time and insights on an occasional basis, in return for being granted access to the OSINT being produced by the NATO element sponsoring the Expert Forum. Such a forum can also be a place where individual experts "audition" for short-term consulting contracts and where the biographies of available efforts can be made available for anonymous review by potential NATO employers.

Expert Forums should consist of several parts, all of them of potentially great value to the NATO OSINT process. First, while it is possible to register anonymously for a forum, the greatest value comes from an open registration that includes a photo, biographic note, and complete contact information. Second, the forum will quickly self-organize, with a variety of topics to which an individual can not only contribute observations, but to which they can upload documents, images, even video. The flexibility and scalability of these forums cannot be overstated—but they do have one major flaw: at this time, it is not possible to apply visualization or other technologies to the varied contents of a forum—each item must be copied down to a master database first.

Soon the technology will be available to index and abstract all information contributed to a forum, at which time the best of all worlds will be available: distributed experts able to cast a wide net, and a centralized "banking" function for information freely contributed by various parties. Third, the forum permits the rapid organization of private working groups, and offers calendar, newsletter, and other

coordination features. Fourth and last, the forums can provide an automatic email alert to any member whenever new information is posted to a topic of interest to them, relieving them of the need to constantly check the forum site.

SECTION F. DISSEMINATION AND EVALUATION

Overview

The major difference between OSINT and the other intelligence disciplines is that the latter are inherently classified: OSINT can be shared with *anybody* that the commander deems appropriate, without having to request security or political clearances.

This makes it extraordinarily valuable in non-article V operations as well as in dealing with civil sector coalition partners—including NGO that traditionally distrust the military in general and intelligence professionals in particular. OSINT has become even more valuable in the 21st Century, as there has been a major change in the over-all C^4I paradigm.

As NATO continues to evolve and transform itself in response to the many new challenges, the importance of OSINT will continue to evolve. These new challenges include non-traditional non-military challenges requiring coordinated action with non-governmental and humanitarian relief organizations.

OSINT appears to offer a very substantial advantage as a prime intelligence source and method with which to achieve consensus and a common understanding of the shared area of operations.

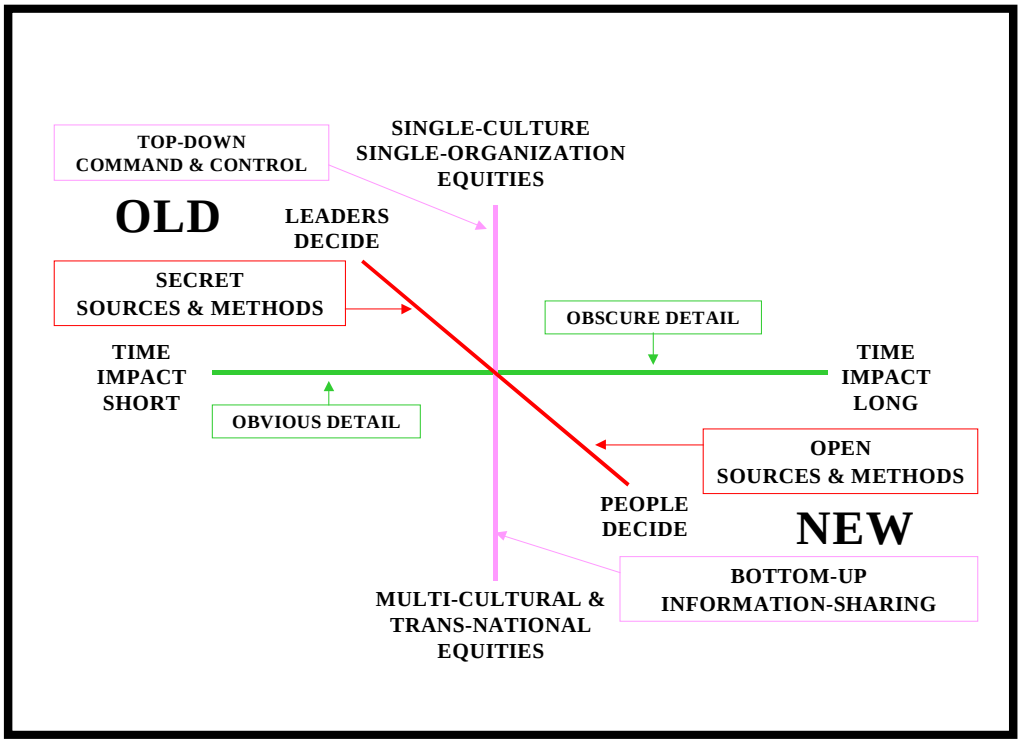


Figure 15 - Emerging Paradigm for Information Sharing

Dissemination Methods

Once open source information has been developed into OSINT, it can be disseminated via the NATO WAN in a "push" mode, or it can be "pulled" off on demand.

The limitations placed on its dissemination are based on the security policies of the organization producing it. While some OSINT products may be shared openly, others may provide details of interests or intentions and should therefore be restricted in their dissemination. The dissemination policy should be driven by the mission requirements. The approach should nonetheless be flexible to fully leverage the ability that the production of OSINT products provides for the engagement of non-NATO elements in security discussions or the development and dissemination of a common view of the operating area.

Within the NATO Intelligence Architecture, options exist for the dissemination of OSINT products via the classified NATO WAN or directly through the Internet. The advantages of the NATO WAN are the direct access afforded to the operations and policy staffs at all levels, including deployed units, as well as the security afforded by the use of a classified system. The principal disadvantage of the NATO WAN for OSINT dissemination is the necessary separation of the products from their source material. Without a direct linkage between an OSINT product and the sources of information, the recipient is less able to drill deeper for additional information, reach the original author, or further evaluate the original sources of the information.

Another option is the use of a Virtual Private Network (VPN). A VPN is a restricted community of interest that communicates on the Internet but use security safeguards to limit the access from others who are not members. By using a VPN, OSINT products can be accessed safely and with working links directly to the original source material. Link tables can also be maintained that enables the rapid collection of information. Other OSINT centres within NATO member countries have direct access to the Internet; few have access to the NATO WAN. A VPN provides the means with which to exchange OSINT products with other OSINT centres across NATO. Finally, the use of a VPN provides the means with which to disseminate OSINT products with non-NATO elements such as NGOs and other international organizations as mission requirements demand.

For these reasons, exploring the feasibility and desirability of a VPN to support the NATO OSINT Initiative remains a priority. SACLANT has begun a trial VPN with the U.S. Open Source Information System (OSIS) to examine the viability of linking NATO OSINT production centres with U.S. OSINT holdings.

Virtual Intelligence Community

The NATO OSINT initiative is the first major multi-national OSINT initiative ever undertaken. While there is much still to learn from those member nations that adopted OSINT as an independent discipline in the 1990's, as well as from the emerging business intelligence community (such as represented by the Society of Competitive Intelligence Professionals at www.scip.org), it is NATO that is leading in the establishment of formal doctrine and tables of organization and equipment specifically earmarked for OSINT. It is helpful, in contemplating this activity, to understand that there is a substantial but still fragmented community of interests with whom NATO could co-develop many OSINT initiatives. This community is illustrated in Figure 16.

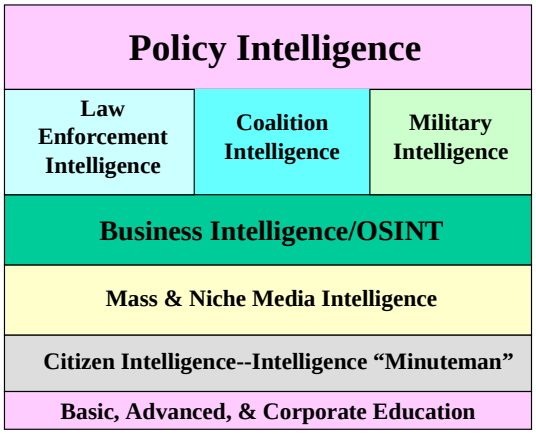


Figure 16 - Elements of a virtual intelligence community

As commanders and their staff evaluate their needs for OSINT, and new methods as well as budget deficiencies, SCs and subordinate commands should seek to establish a constant process of interactive liaison with each of the elements of the "virtual intelligence community" shown here. In this fashion, NATO intelligence could benefit from a greater OSINT effort that cuts across bureaucratic and cultural boundaries, and leads to improved cost efficiencies and new forms of information sharing.

CHAPTER IV
OSINT AND THE EMERGING FUTURE INTELLIGENCE ARCHITECTURE OF NATO

SECTION A. BLENDING OSINT INTO THE ALL-SOURCE PROCESS

Overview

Apart from the importance of OSINT as a means of establishing consensus and a common view with external parties about the shared area of operations, OSINT is absolutely vital to the all-source intelligence process. OSINT provides the historical background information, the current political, economic, social, demographic, technical, natural, and geographic context for operations, critical personality information, and access to a wide variety of tactically useful information about infrastructure, terrain, and indigenous matters. The relationship between OSINT, the traditional collection disciplines, and all-source analysis is shown in Figure 17.

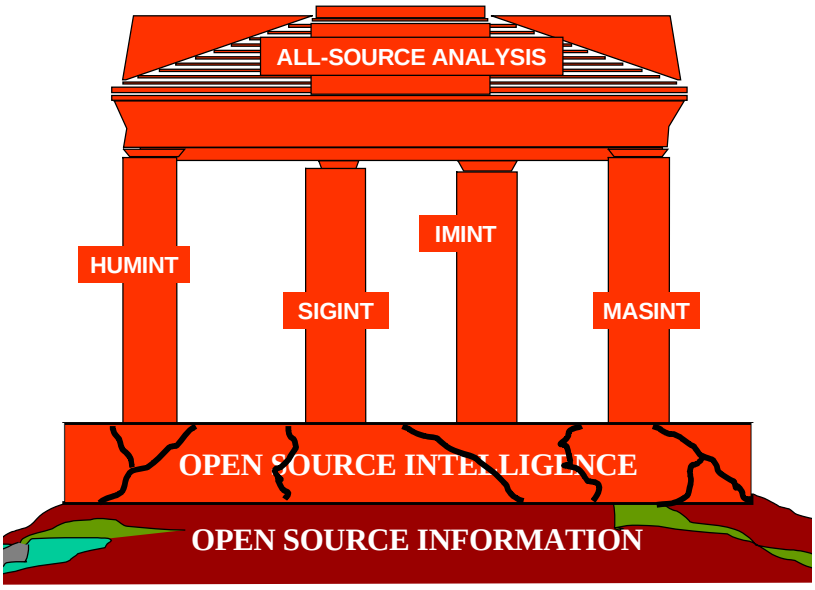


Figure 17 - Open Source - All-Source relationship

Cracks are shown in the OSINT foundation to emphasize that this vital element of the all-source intelligence process has been too long neglected. Following the publication of the Alliance's Strategic Concept in April 1999, OSINT is even more important. NATO, along with other international organizations, is now striving to understand ethnic conflict, water and food scarcity, mass migrations, the collapse of public health across entire continents, transnational crime, and all of the small wars—and the potential threat of large wars—that remain a traditional responsibility. OSINT can and should be integrated into every aspect of the all-source process, from collection through production.

Nations and NATO commands differ fundamentally in their approaches towards OSINT. Both begin with intelligence needs that lead to the generation of intelligence requirements. The approaches diverge at that point. While nations may use OSINT to guide classified collection, NATO rarely has classified collection means beyond the tactical level and those assets are largely restricted to theatres in which forces are already deployed.

NATO commands can use OSINT-V to satisfy intelligence gaps for a large number of its intelligence needs. While nations are able to turn to classified intelligence collection, NATO can and should use the OSINT process described as the first step in its collection process. Too often, NATO commands have defaulted to sending RFIs to nations rather than seeking first to address their intelligence requirements themselves. The range of open sources now within reach of NATO intelligence staffs provides other options.

The new Strategic Concept articulated a vision for the Alliance that is largely focused on non-traditional operating areas and transnational threats. The intelligence services of the NATO member countries are also struggling to deal with a similar problem set. These areas and interests, while not well covered by traditional intelligence production are well addressed in open sources. Rather than relying solely upon nations for intelligence products, NATO intelligence staffs should develop their own network of open sources as the starting point for the compilation of their intelligence assessments.

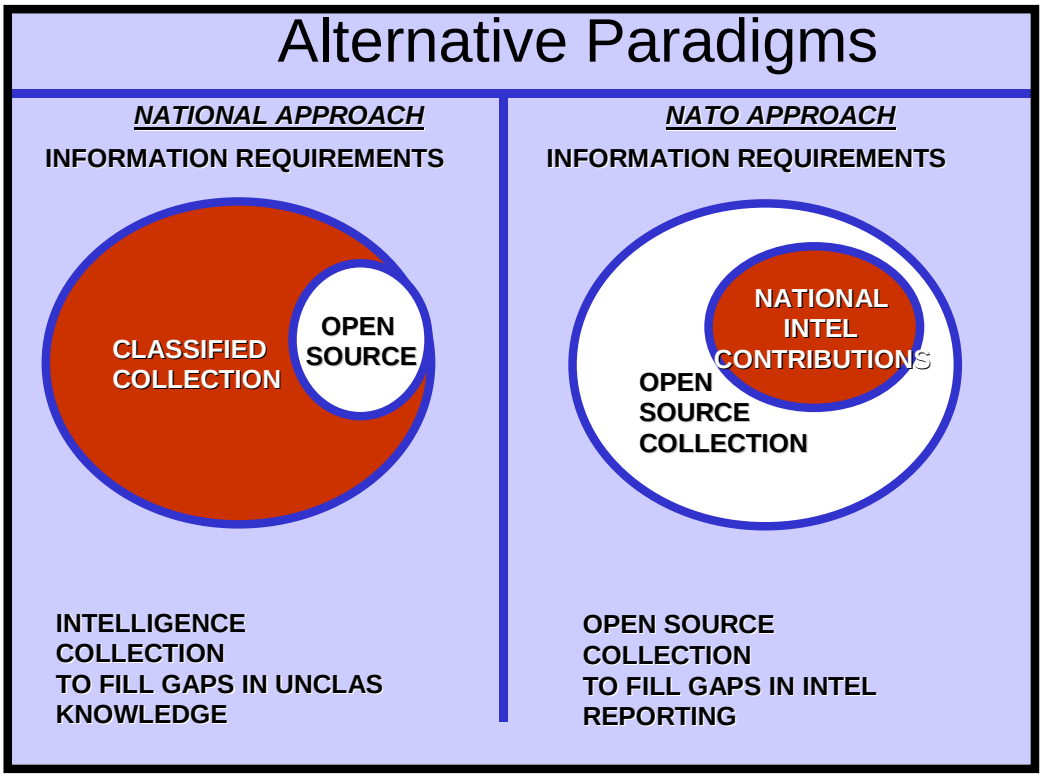


Figure 18 - Alternative Paradigms between NATO and National OSINT Approaches

Direction

Open information sources are as easy for NATO leadership to access as they are for their intelligence staffs. No longer are intelligence staffs in a position to regulate the flow of relevant information to the commander or his staff. Virtually all decision-makers make regular use of open sources to varying degrees. Knowledge of those sources routinely consulted by the staff principals is an important means with which to stay ahead of their intelligence needs.

Rather than attempting to stem the use of open sources by the commander or his staff, an effective OSINT effort facilitates it. Intelligence staffs at both Strategic Commands (SCs) have access to specialized information retrieval tools and commercial sources. In addition, both SCs are in a position to provide training and advice on the effective retrieval of information from open sources. An OSINT process should include the provision of validated information sources for each issue that affects the command. The provision of Link Tables as well as quality assessments of other information sources is an essential OSINT product.

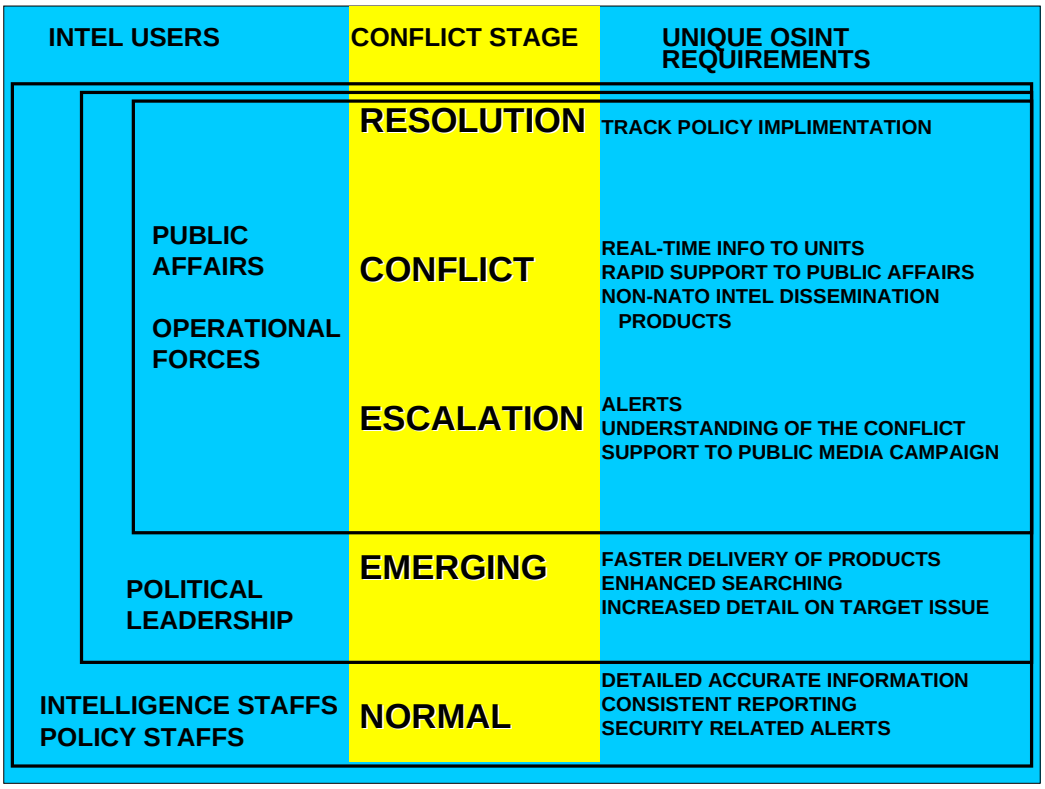


Figure 19 – Unique OSINT Requirements across the Conflict Spectrum

Typically, informed decision-makers make reasoned requests for intelligence. While not always the case, this statement generally holds true. With an appreciation for what is widely known, intelligence users will tend to restrict their requests to that information which they do not already have available to them.

OSINT can support the direction phase of an

all-source intelligence effort through discovery of an issue or providing context with which to understand issues.

The intelligence problem varies depending on the nature of the issue being addressed, which elements of the staff are engaged and what degree of information is required. Figure 19 shows a representative range of information products that a robust OSINT capability can provide.

Assuming an OSINT capability is in place in advance of a crisis, it is likely that the leadership will have had access to quality open source products prior to the onset of mission requirements. In that case informed RFIs can be expected. If there is no familiarity with the issue, decision-makers can be directed to either established OSINT products or open sources of information that can be made available through access to an information portal such as a VPN of another network. Finally, an OSINT collection effort can be initiated to quickly produce relevant background information. This immediate OSINT effort will quickly establish what is easily known about the subject and guide the priorities for classified collection and all-source production.

Collection

Within the intelligence cycle, the collection phase includes the translation of the intelligence need into a collection requirement, the definition of a collection strategy, the selection of the collection sources and the actual information collection. Open sources should be the first recourse in the collection process. OSINT saves money in reducing unnecessary classified collection. In a NATO context, it saves time as RFIs to nations require sufficient lead-time for them to be properly addressed.

While open source information is not free, the costs pale in comparison to those of the classified collection disciplines. If open sources can be collected to produce an OSINT product that addresses completely or to a large degree the intelligence need, classified collection resources can be more effectively deployed elsewhere.

While nations have classified collection capabilities, these are expensive and must always be used wisely. NATO has no tasking authority over national intelligence collection capabilities. Its reliance upon intelligence contributions from nations makes it incumbent upon its intelligence staffs to know what can be known without technical collection.

Open sources have always been used by intelligence organizations. Open sources have typically been referred to as *collateral reporting*. In fact, all single source intelligence disciplines refer to information provided by another intelligence discipline as *collateral reporting*.

However, when this collateral reporting is maintained with a systematic disciplined approach as discussed in this OSINT Manual, the “collateral” grows in its own utility. Instead of being acquired once and used by one intelligence element, it is acquired once and applied across a broader range of the intelligence process from streamlining collection to increasing dissemination.

OSINT’s four main contributions to classified collection are: tip-off for classified sources; targeting of those sources; context and validation to better understand material collected from classified sources, and; providing plausible cover to protect the classified source.

Tip-off.

- Open sources are particularly well suited to providing *tippers* for other collection disciplines. The reduction in the number of denied areas since the end of the Cold War and the advent of cheap international transportation options have enabled greater media access than ever before. Internet NEWSGROUPS, wire services and other traditional print and broadcast media are all within the reach of anyone.

- The Internet remains a primary means with which to gain access to these sources. While traditional print and broadcast media are restricted in the amount of information that they can provide, the Internet has provided virtually limitless dissemination capabilities for information producers. Rather than the editor's selection of stories, the Internet provides the means with which to gain access to all stories filed with all of the wire services depending on the degree of access that is purchased.

- A number of services provide news alerts that are either free of charge or low cost. Non-traditional sources of information include those who witness important events and who post messages on the Internet about what they have seen. While prone to disinformation, this is another source of information that must be evaluated like all others. Those who witness an event and publish on-line or forward emails to their communities of interest can provide the first indication of an event even before media publication.

Targeting.

- While OSINT will often be able to address elements of an intelligence problem quickly and efficiently, OSINT will never invalidate the need for classified collection capabilities.

- When intelligence gaps can be addressed without the need to task classified collection sources overall demand upon limited collection resources decreases. This permits concentration of effort on those issues that can only be discovered through classified collection.

- This model of complementary collection permits both open and classified sources to be optimized for a particular intelligence problem, while at the same time, affording the all-source analyst the ability to use the classified collection products to validate the OSINT products.

Context/Validation.

- Supplemental open source reporting can provide the means with which to place classified reporting into context. Classified reporting, particularly current intelligence reporting, often fails to provide the necessary background information with which to tailor the information to the needs of the recipient or to explain the nuances of the situation.

- While imagery can provide knowledge of ships alongside piers, additional information from open sources can provide an understanding of the cargo that the port handles or the schedule of the ship. Similarly, UN reporting on agriculture production shortfalls in a particular country will give insight into population movements detected with national technical means.

Plausible Cover.

- OSINT is particularly useful in protecting classified sources and methods. The discovery of an open source that corroborates classified

Figure 20 - Commercial imagery of San Diego naval base

reporting may increase the releasability of the initial information by providing a plausible alternate source. This also has applicability to the staffing of requests for the sanitation of classified reporting.

- A thorough understanding of information that is available in unclassified channels facilitates the discovery of plausible alternate sources to classified intelligence reporting. This ultimately increases the ability of intelligence staffs to release intelligence information to non-NATO elements within missions.

Processing

The objective of intelligence processing is the creation of an intelligence product that is value-added, actionable information tailored to a specific user. All-source analysis with its fusion of all relevant and validated sources of information remains the best means to convey intelligence to the user. This process includes both classified and OSINT reporting as appropriate. In most cases, NATO will serve as one element of an international crisis response. Experience has shown that these operations likely include the leading of a broader coalition alongside non-NATO troop contributing nations (NNTCNS). The processing of intelligence products to support the information needs of both the NATO-led force and the international response elements is greatly enhanced with a robust OSINT capability.

Intelligence products can be prepared with a tear-line – classified intelligence restricted in its dissemination above the line and sanitized information that can be more broadly disseminated below the line.

OSINT–V products can be produced specifically tailored for the broader coalition audience but validated by the all-source process. During actual operations, the need to disseminate to non-NATO elements includes not only their operational forces, but also their political liaison elements at NATO headquarters in Brussels.

Figure 21 - Nature of international operations

The maintenance of information sources that can be disseminated outside of NATO channels can often prove essential to both establishing a common view of the operating area and initiating an exchange with other entities that can contribute to the understanding of an issue.

Dissemination

As stated earlier, OSINT is itself optimized for dissemination through VPNs. This enables ready access to the original source material, direct interaction with other related open sources and access to other OSINT producers.

The dissemination of OSINT products as stand-alone intelligence products on classified systems should also be encouraged. OSINT as either stand alone products or as collateral reporting adds to the body of knowledge on a particular issue. Intelligence staffs at all levels should be able to benefit from the effort put into their production. It is rare that all subordinate commands will have access to every intelligence system. Thus, efforts should be made to ensure that products are available on all intelligence dissemination systems as security constraints permit.

Typically, the lower the classification of an intelligence product the wider is its uses. If decision-makers are able to leave their offices with an intelligence product, it is more likely that it will receive undisturbed attention. OSINT products provide the means to place high quality low-classification or unclassified products in the hands of intelligence users. This is only possible if they are disseminated on systems typically used to deliver other forms of intelligence.

The objectives of a robust OSINT capability should be to increase the range of information available to intelligence users and to facilitate interaction with non-NATO elements as appropriate. The dissemination options developed should seek to achieve these two objectives.

APPENDIX A: GENERAL REFERENCE LINK TABLE

Maps:

World Ports	http://www.world-ports.com/
United Nations	http://www.un.org/peace/kosovo/pages/kosovo1.shtml
CIA World Factbook	http://www.odci.gov/cia/publications/factbook/indexgeo.html
Quick Maps	http://www.theodora.com/maps/abc_world_maps.html
CNN Video Select	http://europe.cnn.com/video/netshow/
The Place For Maps	http://www.maps.com/?AID=41160&PID=186662
Map Quest	http://www.mapquest.com/
Expidia.com	http://www.expedia.com/pub/Agent
Media Maps.com	http://media.maps.com

News:

NBC Daily	http://www.nbc.com/
Bloomberg	http://www.bloomberg.com
MSNBC	http://www.msnbc.com
CNN Videoselect	http://europe.cnn.com
Fox News	http://www.foxnews.com
BBC Monitoring	http://news.monitor.bbc.co.uk/
BBC NEWS	http://news.bbc.co.uk/
CBS NEWS	http://www.cbs.com/daytime/bb/show_update/update.shtml
CNBC Dow Jones Business Video	http://cnbcdowjones.com/msnbc
CNET Today	http://news.cnet.com
ABC News	http://abc.go.com
CNN	http://www.cnn.com
The Sunday Times	http://www.information-britain,co.uk/news.sundaytimes.htm"
News Now 1401	http://www.newsnow.co.uk/
MSN News	http://www.msn.com
Real Radio	http://realguide.real.com/tuner/?
ABCNews	http://abcnews.go.com/
Business Journal	http://business.netscape.com/business/main.tmpl
Fox News	http://www.foxnews.com/
International News	http://www.internationalnews.com/
AJR News Link	http://ajr.newslink.org/
ITN News British	http://www.itn.co.uk/
The World News	http://www.theworld.org/
Out There News	http://www.megastories.com/index.shtml
CNN International	http://europe.cnn.com/CNNI/
The Times	http://www.thetimes.co.uk/
LA Times	http://www.latimes.com/
Jerusalem Post	http://www.jpost.com/
Belfast News	http://www.belfasttelegraph.co.uk/index.shtml
The Washington Post	http://www.washingtonpost.com/
South China Morning Post	http://www.scmp.com/
The Japan Times	http://www.japantimes.co.jp/
Yahoo	http://www.yahoo.com
The CNET Channel	http://channel.cnet.com/Channel/Intro/index.htm
The Wall Street	http://interactive.wsj.com/ie4intro/index.htm

Conflict:

United Nations High Commission For Refugees	http://www.unhcr.org
Weapons Of Mass Destruction	http://www.fas.org/irp/threat/wmd_state.htm
Terrorism Research	http://www.terrorism.com/index.shtml

Counter Terrorism	**http://www.state.gov/www/global/terrorism/**
Intelligence Net	**http://www.intellnet.com**
Federation of American Scientist	**http://www.fas.org**
War Information	**http://www.psycom.net/iwar.1.html**
China's Military Developments	**http://www.commw.org**
Kosovo Info	**http://perso.respublica.fr/infokosovo/**
Institute for Global Communications	**http://www.igc.org**
Anti War Home Page	**http://www.nonviolence.org/archivedsites/iraq/**
Missle, Threats & Response	**http://www.cdiss.org/tempor1.htm**
Modern Day Piracy	**http://www.geocities.com/Tokyo/Garden/5213/modern.htm**
KORB Marine Links	**http://www.pg.gda.pl/~korab/kor_lnk.html**
Piracy Centre	**http://www.iccwbo.org/ccs/menu_imb_piracy.asp**
The Panama Canal	**http://www.pancanal.com/eng/index.html**
Royal Australian Navy Sites	**http://www.navy.gov.au/html/links.htm**
Royal Navy Association	**http://www.royal-naval-association.co.uk/page6.htm**

Regional Information:

CIA World Factbook	**http://www.odci.gov/cia/publications/factbook/indexgeo.html**
Geo Spatial Information	**http://www.geoplace.com/**
Geographic Learning Site	**http://geography.state.gov/htmls/plugin.html**
Association For Geographical Information	**http://www.agi.org.uk/**
Salam Iran	**http://www.salamiran.org/IranInfo/General/Geography/**
Limes Geo review	**http://www.limesonline.com/doc.navigation**

Reference:

Britannica	**http://britannica.com/**
Dictionary	**http://Dictionary.com**
Every Rule	**http://Everyrule.com**
FBIS	**http://199.221.15.211/**
Central Intelligence Agency	**http://www.cia.gov/**
Indian Naval Review	**http://www.janes.com/defence/naval_forces/gallery**
Bureau for International Narcotics and Law Enforcement Affairs	**http://www.state.gov/www/global/narcotics_law/**
Archive Site for State Department information	**http://www.state.gov/index.html**
Naval Technology	**http://www.naval-technology.com/index.html**
Janes Naval Forces	**http://www.janes.com/defence/naval_forces/index.shtml**
Encyclopedia	**http://Libraryspot.com**
World Fact Book	**http://Worldfactbook.com**
The Intelligence Community	**http://www.odci.gov/ic/**
One World	**http://www.oneworld.net/**
Yahoo	**http://www.yahoo.com**
Lloyds List	**http://www.lloydslist.com**
Ask Oxford	**http://www.askoxford.com/**
(WMD) Weapons Of Mass Destruction	**http://www.fas.org/irp/threat/wmd_state.htm**
Incident Response	**http://www.llnl.gov/nai/rdiv/rdiv.html**
Conference For Middle East Peace	**http://www.cmep.com/**

APPENDIX B: TRAINING LINK TABLE

Below are a few of the essential references that are available online. Please note that the NATO guide *Intelligence Exploitation of the Internet* is also available online at the SACLANT Intelligence homepage on the NATO WAN. This publication is regularly updated with the best resources available to guide in the use search strategies and tools to exploit open sources available on the Internet. The Open Source Intelligence Proceedings include over 5,000 pages from over 500 international authorities including the (then) Director General of the International Red Cross and many other European and Asian experts, and comprise the "information commons" on the state of the art for open source intelligence.

OSINT Presentation to SHAPE/PfP Flags	http://www.oss.net/Papers/white/SHAPE.ppt
Information & Intelligence Bibliography	http://www.oss.net/Papers/white/23-BibliographyAnnotated.rtf
Eight Self-Paced OSINT Lesson Plans	http://www.oss.net/DispFrame.html?Papers/training/index.html
Creating an OSINT Cell (DIA Report)	http://www.oss.net/DispFrame.html?Papers/white/DIAReport.html
Business Intelligence Primer (1994)	http://www.oss.net/DispFrame.html?Papers/white/THETHEORYANDPRACTICEOFCOMPETITORINTELLIGENCE.html
Open Source Intelligence Proceedings	http://www.oss.net/Proceed.html
Index to OSINT Proceedings	http://www.oss.net/Papers/white/index.rtf
OSINT and the Military	http://www.oss.net/Proceedings/95Vol1/aab0aw.html
Canadian Intelligence Studies	http://www.sfu.ca/igs/CASIS/
Come Back Alive "Ground Truth"	www.comebackalive.com/df/index.htm
Future of Intelligence	www.future-intel.it
History of Intelligence	http://intelligence-history.wiso.uni-erlangen.de
Intelligence Resource Program	http://www.fas.org/irp/index.html
Links to International Media	http://www.esperanto.se/kiosk/index.html
Literature of Intelligence	http://intellit.muskingum.edu
Open Directory Project	http://dmoz.org/
Strategic Intelligence	http://www.loyola.edu/dept/politics/intel.html
Form for Evaluating the Value of Web Pages	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/EvalForm.pdf
Internet Training Course by Russ Haynal	http://navigators.com/fbis.html
Berkeley University Tutorial for Finding Information on the Internet	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/FindInfo.html
Search Techniques for the Invisible Web	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html#Table
Techniques for “Searching Upstream”	http://websearch.about.com/library/weekly/aa061101a.htm?once=true&

APPENDIX C: CATEGORIES OF MISPERCEPTION AND BIAS

Evoked-Set Reasoning: That information and concern, which dominates one's thinking based on prior experience. One tends to uncritically relate new information to past or current dominant concerns.

Prematurely Formed Views: These spring from a desire for simplicity and stability, and lead to premature closure in the consideration of a problem.

Presumption that Support for One Hypothesis Disconfirms Others: Evidence that is consistent with one's preexisting beliefs is allowed to disconfirm other views. Rapid closure in the consideration of an issue is a problem.

Inappropriate Analogies: Perception that an event is analogous to past events based on inadequate consideration of concepts or facts or irrelevant criteria. Bias of "Representativeness".

Superficial Lessons From History: Uncritical analysis of concepts or event, superficial causality, over-generalization of obvious factors, inappropriate extrapolation from past success or failure.

Presumption of Unitary Action by Organizations: Perception that behavior of others is more planned, centralized, and coordinated than it really is. Dismisses accident and chaos. Ignores misperceptions of others. Fundamental attribution error possibly caused by cultural bias.

Organizational parochialism: Selective focus or rigid adherence to prior judgments based on organizational norms or loyalties. Can result from functional specialization. Groupthink or stereotypical thinking.

Excessive Secrecy (Compartmentation): Over-narrow reliance on selected evidence. Based on concern for operational security. Narrows consideration of alternative views. Can result from or caused organizational parochialism.

Lack of Empathy: Undeveloped capacity to understand others' perception of their world, their conception of their role in that world, and their definition of their interests. Difference in cognitive contexts.

Mirror-Imaging: Perceiving others as one perceives oneself. Basis is ethnocentrism. Facilitated by closed systems and parochialism.

Ignorance: Lack of knowledge. Can result from prior-limited priorities or lack of curiosity, perhaps based on ethnocentrism, parochialism, and denial of reality, rational-actor hypothesis (see next entry).

Rational-Actor Hypothesis: Assumption that others will act in a "rational" manner based on one's own rational reference. Results from ethnocentrism, mirror imaging, or ignorance.

Denial of Rationality: Attribution of irrationality to others who are perceived to act outside the bounds of one's own standards of behavior or decision making. Opposite of rational-actor hypothesis. Can result from ignorance, mirror imaging, parochialism, or ethnocentrism.

Proportionality Bias: Expectation that the adversary will expend efforts proportionate to the ends he seeks. Interference about the intentions of others from costs and consequences of actions they initiate.

Willful Disregard of New Evidence: Rejection of information that conflicts with already-held beliefs. Results from prior commitments, and/or excessive pursuit of consistency.

Image and Self-Image: Perception of what has been, is, will be, or should be (image as subset of belief system). Both inward-directed (self-image) and outward-directed (image). Both often influenced by self-absorption and ethnocentrism.

Defensive Avoidance: Refusal to perceive and understand extremely threatening stimuli. Need to avoid painful choices. Leads to wishful thinking.

Overconfidence in Subjective Estimates: Optimistic bias in assessment. Can result from premature or rapid closure of consideration, or ignorance.

Wishful Thinking (Pollyanna Complex): Hyper-credulity. Excessive optimism born of smugness and overconfidence.

Best-Case Analysis: Optimistic assessment based on cognitive predisposition and general beliefs of how others are likely to behave, or in support of personal or organizational interests or policy preferences.

Conservatism in Probability Estimation: In a desire to avoid risk, tendency to avoid estimating extremely high or extremely low probabilities. Routine thinking. Inclination to judge new phenomena in light of past experience, to miss essentially novel situational elements, or failure to reexamine established tenets. Tendency to seek confirmation of prior held beliefs.

Worst-Case Analysis (Cassandra Complex): Excessive skepticism. Reflects pessimism and extreme caution, based on predilection (cognitive predisposition), adverse past experience, or on support of personal or organizational interest or policy preferences.

Source: Lisa Krizan. *Intelligence Essential for Everyone*. Washington D.C. Joint Military Intelligence College, June 1999.

APPENDIX D. LIST OF ABBREVIATIONS

AIIB – Association of Independent Information Brokers
AOO - Area of Operations
API - Application Program Interfaces
BBC - British Broadcasting Corporation
COSPO - Community Open Source Program Office
EEI - Essential Elements of Information
FBIS - Foreign Broadcast Information Service
ICRC - The International Committee of the Red Cross
ISPs - Internet Service Providers
MCCIS – Maritime Command and Control Information System
NATO - North Atlantic Treaty Organization
NDA - Non-Disclosure Agreements
NGO - Non-Governmental Organization
NNTCNS - Non-NATO troop contributing nations
OPSEC - Operational Security
OSIF - Open Source Information
OSINT - Open Source Intelligence
OSO - Open Source Officers
PfP - Partnership for Peace
RFI - Requests for Information
SACEUR - Supreme Allied Commander, Europe
SACLANT - Supreme Allied Commander, Atlantic
SAR - Synthetic Aperture Radar
SC - Strategic Commands
SCI - Science Citation Index
SME - Subject-Matter Experts
SSCI - Social Science Citation Index
STN - Scientific and Technical Network
UN - United Nations
VPN- Virtual Private Network
WEU - Western European Union

FEEDBACK

This manual is intended to be a living document. It represents the first attempt by NATO to place OSINT within the broader context of intelligence efforts. The intention is to subject this publication to regular review and updating to reflect new sources and methods for open source exploitation.

As such, feedback is welcome in any form. Comments, amendments, additions or errors can be reported either with the form below or via email to rsc@saclant.nato.int.

Name: _____

Parent Command: _____

Telephone number: _____

Email address: _____

Comment:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Fax to: HC-310
SACLANT Intelligence Branch
Norfolk, VA
757-445-3572

Joint Military Intelligence Training Center

October 1996

Open Source Intelligence: Professional Handbook

FORWARD

1. **PURPOSE.** *Open Source Intelligence: Professional Handbook*, is published to ensure the dissemination of useful information which is vital to successful intelligence support to the military commander, and highly pertinent to law enforcement and economic intelligence operations, but which may not yet be doctrinally available.

2. **SCOPE.** This publication constitutes material that was producted under contract to the Defense Intelligence Agency, Joint Military Intelligence Training Center, by OPEN SOURCE SOLUTIONS, Inc., using copyrighted OSS Inc. materials. The material has been edited by OSS to develop a single integrated publication which can be used as both a primer and an operational guide to acquiring and exploiting open source information as part of the all-source intelligence process. Open source information is often described as the "source of first resort," and may be the *only* source available to the commander and staff when initially considering an expeditionary contingency. The information contained herein does not necessarily reflect the views, nor should any endorsement or approval be implied by the Department of Defense or the Defense Intelligence Agency, or any other government organization or authority.

3. **COPYRIGHT AND DISSEMINATION.** This publication may be reproduced without restriction by any agency of the US government. It may not be used by others without prior permission of the copyright holder, OPEN SOURCE SOLUTIONS, Inc., 11005 Langton Arms Ct, Oakton VA 22124.

OPEN SOURCE INTELLIGENCE: PROFESSIONAL HANDBOOK 1.1

CONTENTS

	INTRODUCTION	001

Chapter 1. OVERVIEW OF OPEN SOURCES & SERVICES

Paragraph		Page
1001	Purpose of the Chapter	004
1002	Definitions	004
1003	Brief History of U.S. OSINT	005
1004	OSINT & All-Source Analysis	006
1005	Knowledge Terrain: The Information Continuum	007
1006	OSINT and The Military I	008
1007	OSINT and The Military II	009
1008	Militarily Useful OSINT: Two Examples	010
1009	Representative Open Sources I	011
1010	Representative Open Sources II	011
1011	Representative Open Services I	012
1012	Representative Open Services II	013
1013	Intelligence in the Age of Information	014
1014	Changing Role of the Analyst I	015
1015	Changing Role of the Analyst II	015
1016	Changing Role of the Analyst III	016
1017	Changing Role of the Analyst IV	016
1018	Overt Human Networks: Some First Steps	017
1019	OSINT Among Selected Allies	018
1020	OSINT in Asia	019
1021	OSINT in Europe	019
1022	OSINT Within DIA I	020
1023	OSINT Within DIA II	021
1024	OSINT Within DIA III	021
1025	OSINT and the All-Source Product	022

Chapter 2. ACCESS: Intelligence in the Age of Information

Paragraph		Page
2001	Purpose of the Chapter	024
2002	Definitions	024
2003	New "Rules of the Game"	025

2004	Four Information Categories	026
2005	Information Value	027
2006	Open Sources	027
2007	Collection Investment Strategies	028
2008	Windows of Opportunity	029
2009	Collection Management	030
2010	Four Major Consumer Groups	031
2011	Intelligence Production	031
2012	Target Categories	032
2013	Types of Overt Human Sources	033
2014	OSINT As A Resource Saver	034
2015	National Information Strategy	035
2016	Optimizing OSINT	036

Chapter 3. INTERNATIONAL OPEN SOURCES AND SERVICES

Paragraph		Page
3001	Purpose of the Chapter	037
3002	American Online Services	037
3003	Foreign Online Services	038
3004	Information Brokers	039
3005	Grey Literature	040
3006	Document Acquisition	040
3007	International Experts I	041
3008	International Experts II	042
3009	International Directories	042
3010	Jane's Information Group	043
3011	Oxford Analytica	044
3012	Eastview Publications	045
3013	SPOT Image Corporation	045
3014	Universities	046
3015	Knowledge Age	047
3016	Conclusion	048

Chapter 4. THE INTERNET AS A TOOL FOR ALL-SOURCE ANALYSIS

Paragraph		Page
4001	Purpose of the Chapter	049
4002	Introduction: What Is The Internet	049
4003	Where Are We Today?	050
4004	How Representative Is The Internet?	051
4005	Lists: Versatile Low-Tech Tools	052

4006	USENET and Its Newsgroups	052
4007	Conferencing Systems	053
4008	CAUTION: Some Problem Areas	054
4009	How On-Line Communities Form	055
4010	On-Line Communities, Virtual Contacts	055
4011	Structuring Knowledge: Tools and Trends	056
4012	The World-Wide Web	057
4013	Where the Web Has Been, and Where It's Headed	058
4014	Finding Information on the Web	059
4015	"Intranetting"	059
4016	Practical Example #1: Indications and Warning (I&W)	060
4017	Practical Example #2: Cultural Context	061
4018	Practical Example #3: Basic Research	061
4019	Practical Example #4: Science and Technology Collection	062
4020	Practical Example #5: Spotting and Assessment	062
4021	Second Caution: Mischief in Cyberspace	063
4022	Putting It All Together	064
4023	Anticipating Coming Changes	065
4024	Conclusion: A Work in Progress	065

Chapter 5. OPEN SOURCES AND MILITARY CAPABILITIES

Paragraph		Page
5001	Purpose of the Chapter	067
5002	Model for Integrated All-Source Analysis	067
5003	General Utility of OSINT	068
5004	Strategic Intelligence	069
5005	Operational Intelligence	070
5006	Tactical Intelligence	070
5007	Technical Intelligence	071
5008	Commercial Imagery for 1:50:000 Maps	072
5009	Commercial Imagery for Mission Rehearsal	072
5010	Order of Battle Information	072
5011	Historical and Estimative Analysis	073
5012	Networks of Experts	074
5013	Expeditionary Factors Study	075
5014	Strategic Generalizations	075
5015	Commission on Intelligence	076
5016	Conclusion	077

Chapter 6: Open Sources and Operational Security--The Dark Side

Paragraph		Page
6001	Purpose of the Chapter	078
6002	General Considerations	078
6003	Open Sources and Radio Interception	079
6004	Open Sources and Telephone Interception	080
6005	Open Sources and Eavesdropping	081
6006	Open Sources and Undercover Operations	082
6007	Open Sources and Interrogations	082
6008	Open Sources and Direct Research	083
6009	Open Sources and Executions	084
6010	Open Sources and Explosives	085
6011	Open Sources and Radio Detonation of Bombs	085
6012	Open Sources and Vehicular Enhancements	086
6013	Open Sources and Tactical Communications Jamming	087
6014	Open Sources and Bank Card Forgery	087
6015	Open Sources and "Legal" Offshore Passports	088
6016	Open Sources and Offshore Corporations	089
6017	Open Sources and Choosing A Criminal Specialty	090
6018	Conclusion: The Dark Side of Open Sources	091

Chapter 7 CONCLUSION: COLLECTING AND PROCESSING OPEN SOURCE

Paragraph		Page
7001	Purpose of the Chapter	092
7002	Community Open Source Program Office	092
7003	Open Source Information System	093
7004	Defense Intelligence Agency Open Source Program	094
7005	Defense Intelligence Agency Open Source Intelligence Center	094
7006	Marine Corps Intelligence Activity	095
7007	Expeditionary Factors Study	095
7008	Marine Corps Reserve	096
7009	Additional Open Source Training Opportunities	097

APPENDICES

Appendix		Page
A	White Paper on "Open Source Intelligence: What Is It? Why Is It Important to the Military?"	099
B-1	Talking Points on "Private Enterprise Intelligence: Its Potential Contribution to National Security"	110
B-2	Complete Paper on "Private Enterprise Intelligence: Its Potential Contribution to National Security"	113
B-3	Glossary of Open Source Acronyms	145
B-4	Core Open Source References	146
C	White Paper on "ACCESS: Theory and Practice of Intelligence in the Age of Information	147
D	Concise Directory of Selected International Open Sources & Services	165
E-1	Internet: Self-Guided Tour	174
E-2	Internet: Intelligence-Oriented List of Useful Internet Sites	181
E-3	Internet: Intelligence Sites from *PC Magazine*'s Top 100 Web Sites	190
E-4	Internet: How to Find an Interesting Mailinglist	193
F-1	Expeditionary Environment R&A Framework & Model 1990	201
F-2	Mission Area Factors Summary	252
G	Open Source OPSEC: Selected References and Information	302
H	Expeditionary Factors Study: List of Countries	306

INTRODUCTION

This handbook is based almost entirely on six of the eight lessons comprising the Open Source Training Course funded by the Defense Intelligence Agency (DIA). It has been prepared by the staff of the Navy-Marine Corps Intelligence Center as a means for consolidating the course materials in a form which could be most useful to the Marine Air Ground Task Force (MAGTF). All Marines will benefit from this DIA-funded initiative, which is the first organized course of instruction on open source intelligence available in the entire U.S. Intelligence Community. This material is provided to the Fleet Marine Force as an interim measure, pending the availability, possibly in 1997 or 1998, or more formal training materials from the(U.S. Intelligence) Community Open Source Program Office.

Chapter 1, OVERVIEW OF OPEN SOURCES & SERVICES, presents a broad overview of open sources and services which are important to the all-source intelligence analyst. Included in this chapter is a definition of open source and a distinction between data, information, and intelligence; a brief discussion of the history of open source intelligence as a sub-discipline within the all-source intelligence process; a review of why open sources are important to military intelligence; examples of open sources and services which are not now commonly integrated into all-source analysis; and a discussion of open source exploitation within DIA (Defense Intelligence Agency) and in a number of allied intelligence communities. This chapter concludes with a discussion of the changing role of the analyst; and how each analyst can take specific steps to improve their personal exploitation of open sources in support of the all-source intelligence process.

Chapter 2, ACCESS: INTELLIGENCE IN THE AGE OF INFORMATION, presents a more in-depth look at why open sources are critical to the all-source analysis endeavor, and how all-source analysts can optimize their exploitation of open source information. Included in this overview is a review of definitions distinguishing between data, information, and intelligence; discussions of how the art of intelligence is changing in the face of the "information explosion", the four kinds of information categories that an all-source analysts can consider accessing, and the three elements of information value; a discussion of the nine levels of open source information; an examination of possible collection management strategies which integrate open sources into the all-source collection management task and exploit windows of opportunity in which material is available in open sources just prior to being classified or censored; discussion of the four major consumer groups and their intelligence productions needs in relation to open sources; an examination of the four "warrior classes" and how open sources apply to intelligence analysis of each; discussion of the four types of overt human sources the analyst will encounter; an examination of how open source intelligence (OSINT) can help conserve scarce classified resources, and how a national information strategy can increase the amount of open source information available to the defense intelligence community; and concluding comments on optimizing OSINT in the all-source analysis process.

Chapter 3, INTERNATIONAL OPEN SOURCES AND SERVICES, provides an orientation to international open sources and services which are available to the all-source analyst. Although much of the open source world is not yet easily accessible to analysts because of security and procurement constraints, the Commission on Intelligence report of 1 March 1996 has defined such access as "critical", and recommended that dramatically improved analyst access to open sources be a top priority for the Director of Central Intelligence and a top priority for funding. This orientation discusses electronic access, the identification and acquisition of "grey literature", the identification and exploitation of international experts, and several examples of world-class international open source capabilities including Jane's Information Group and SPOT Image Corporation.

Chapter 4, THE INTERNET AS A TOOL FOR ALL-SOURCE ANALYSIS, presents a very broad overview of the global capability known as "The Internet" or "the Net". The Internet is a global communications medium that permits extraordinary flexibility in communicating with a wide variety of people from all walks of life, in receiving free information from many sources (some of dubious authenticity), and in obtaining access to distributed databases, many multi-media in nature, all over the world. This chapter will discuss in general terms the utility of the Internet to the all-source analyst, with special attention to the use of electronic mail, newsgroups, lists, and conferencing systems. It also discusses some of the dangers of the Internet, including the problems of "noise" and "flame wars", as well as the almost total lack of privacy and discretion. The last half of the chapter will focus on the most productive element of the Internet, the World Wide Web, and will provide five practical examples of how to exploit the Internet in support of the all-source analysis endeavor.

Chapter 5, OPEN SOURCES AND MILITARY CAPABILITIES, focuses on the practical application of open sources to military intelligence analysis requirements. The chapter begins by introducing a model for integrated all-source analysis which illustrates the critical importance of geographic and civil factors in evaluating the threat at each of the levels of analysis. While open sources are useful in conducting research and developing intelligence estimates about military capabilities in isolation, open sources are most useful to the military intelligence analyst when used to develop a broader analytical model. The general utility of open sources for military intelligence analysis, and the specific utility of open sources at the strategic, operational, tactical, and technical levels of analysis will be discussed. Next the chapter examines specific private sector capabilities for collecting and processing open source information. Commercial imagery, private sector order of battle information, and networks of experts available for consultation will be reviewed in general terms. Finally this chapter introduces the student to the Expeditionary Factors study developed by the Marine Corps Intelligence Activity, and used for this handbook because it is the only current and authoritative intelligence analysis product which relies exclusively on open sources, is unclassified in its final form, and covers a broad range of mission area factors for eighty countries specifically chosen because of the likelihood that a Marine Air Ground Task Force will be engaged in non-combatant or combatant missions in the countries

Chapter 6, OPEN SOURCES AND OPERATIONAL SECURITY--THE DARK SIDE, documents the premise that everything needed for the planning and execution of criminal or terrorist activity can be found in open sources. Indeed, an entire industry exists which is devoted to the publication of such material. In addition, equipment designed for one purpose and legally available can be used in terrorist or criminal activity. From both a military and a law enforcement point of view, it is critical to understand that even our most poorly-funded and least organized opponents can gain access to relatively sophisticated intelligence collection tools as well as tools of destruction.

Chapter 7, CONCLUSION: COLLECTING AND PROCESSING OPEN SOURCE, wraps up the handbook by providing information about three official U.S. government channels for obtaining open source intelligence: the Community Open Source Program Office and its global Open Source Information System; the Defense Intelligence Agency Open Source Program and the (planned) Defense Intelligence Agency Open Source Intelligence Center; and--especially important for Marines--the Marine Corps Intelligence Activity and the Expeditionary Factors Study. The Chapter concludes with a brief discussion of the usefulness of the Marine Corps Reserve as a source of existing and new open source exploitation experts, and some recommendations on additional open source training opportunities.

The APPENDICES provide both additional background information, and explicit references and points of contact which can be used to acquire open source intelligence in support of the commander and the staff. Appendix A, a White Paper on "Open Source Intelligence: What Is It? Why Is It Important to the Military?" was commissioned by the French Ministry of Defense and used (in translation) to begin the process of creating a French open source intelligence capability. Appendix B, consisting of both talking points and a formal paper on "Private Enterprise Intelligence: Its Potential Contribution to National Security" was developed as an invited paper for the annual open conference on Canadian intelligence. Included in Appendix B are a number of direct points of contact and key references useful in starting an open source intelligence program. Appendix C, a White Paper on "ACCESS: Theory and Practice of Intelligence in the Age of Information", was also commissioned by the French, and represents a somewhat abstract but still useful discussion of open source intelligence as a supporting discipline. Appendix D is a Concise Directory of Selected International Open Sources & Services which was prepared for the Defense Intelligence Agency, and remains both current and useful. Appendix E is a series of papers prepared for the Defense Intelligence Agency and serving as primers on exploiting the Internet, with over 100 pertinent intelligence-oriented sites and lists being identified in detail. Appendix F is a combination of a model (the original Expeditionary Environment Research & Analysis Framework & Model 1990) and strategic generalizations from the first Marine Corps Intelligence Activity study, *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World*. Appendix G provides key references documenting what is available to terrorists and criminals which should be of concern to the military professional from an operations security viewpoint. Finally, Appendix H provides a list of the 80 countries examined in the current MCIA study, *Expeditionary Force Mission Factor Intelligence Analysis Requirements Study* dated 15 September 1994.

Chapter 1

OVERVIEW OF OPEN SOURCES & SERVICES

1001. Purpose of the Chapter

The purpose of this chapter is to present a broad overview of open sources and services which are important to the all-source intelligence analyst.

Included in this chapter will be a definition of open source and a distinction between data, information, and intelligence; a brief discussion of the history of open source intelligence as a sub-discipline of the all-source intelligence process; a review of why open sources are important to military intelligence; examples of open sources and services which are not now commonly integrated into all-source analysis; and a discussion of open source exploitation within DIA (Defense Intelligence Agency) and in a number of allied intelligence communities.

This chapter concludes with a discussion of the changing role of the analyst; and how each analyst can take specific steps to improve their personal exploitation of open sources in support of the all-source intelligence process.

Appendices A and B are provided for background information. This initial chapter serves as the introductory element of the handbook.

1002. Definitions

It is important for the professional intelligence analyst to remember that the final intelligence product is supposed to represent a refined process which integrates requirements analysis (defining what the customer needs to know), collection management, source validation, analytical integration, and presentation.

For the purposes of this handbook, the following definitions are provided:

-- *Data* is the raw print, image, or signal. Data can be classified, as in a technical intelligence signal intercept, or unclassified, as in a report from the Foreign Broadcast Information Service (FBIS) on a public television report. Please note that open source data includes commercial imagery such as is available from SPOT Image Corporation.

-- *Information* is data that has been collated, processed, in order to produce a report that is of generic interest. Information can be multi-media, with integrated graphics and imagery, or simply a print report including interpretation of imagery.

-- *Intelligence* in this context is used to distinguish those products which tailor information in order to support a specific decision by a specific customer.

Nowhere is it written that "intelligence" must be classified. A good intelligence product can be based exclusively on open sources, or only on signals intercepts--it is of course likely that the best intelligence will be "all-source" in nature, integrating an open source foundation with unique value-added insights from classified sources.

The *official* definition of *open source information*, established in Director of Central Intelligence Directive 2/12 (effective 1 March 1994) is: "publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation), as well as other unclassified information that has limited public distribution or access". The latter is referred to as "grey literature" and includes non-proprietary information from companies and other organizations.

1003. Brief History of U.S. OSINT

The Office of Strategic Services (OSS), when first formed, was intended to serve primarily as a coordinator of information, and was initially constructed around a Research and Analysis Branch which relied almost exclusively on open sources. In fact, when the OSS later had significant but scarce clandestine collection capabilities, they utilized *The New York Times* to prepare "secret" reports to satisfy many of their customers' requirements which did not merit the risk or expense of clandestine collection.[1]

Over time, and after the Central Intelligence Agency (CIA) was created by the National Security Act of 1947, the responsibility for open source collection became fragmented between the federal departments, such as the Departments of State, Defense, and Commerce; and selected elements of the CIA which specialized in open source collection. The two most important, still existing today as elements of the CIA, are the Foreign Broadcast Information Service (FBIS), and the National Collection Division (NCD). The former monitors foreign print and broadcast media; the latter works with private sector parties to obtain unclassified information. Today the Community Open Source Program Office (COSPO) coordinates open source investments across the entire U.S. intelligence community. Most other organizations including the Defense Intelligence Agency (DIA) utilize External Research & Analysis (ER&A) funds to contract for open source collection and analysis from the private sector--however, these funds have been severely reduced in the 1990's as fiscal cut-backs and the desire to keep U.S. government personnel on board have led to great reductions in contracting for external (i.e. open source) assistance.

---

[1] Mile Copeland, *Without Cloak or Dagger: The Truth About the New Espionage* (Simon & Schuster, 1974), pages 47-48. Testifying to Congress in 1947, Allen Dulles himself stated "...in time of peace the bulk of intelligence can be obtained through overt channels...these overt, normal, and aboveboard means would supply us with over 80 percent, I should estimate, of the information required for the guidance of our national policy." As quoted in Peter Grose, *Gentleman Spy* (Houghton Mifflin, 1994).

In recent years, the *"information explosion"*, together with major political upheavals within formerly denied areas, have made a vast quantity of open source information available to the public and to the intelligence community. Latin American investigative reporting, processed by Department of Energy laboratories, has been used by the U.S. Southern Operations Command to support Drug Enforcement Administration (DEA) interdiction operations; open source information is playing a critical role in countering proliferation, and in understanding transnational crime and especially financial crime.

Today, within the intelligence community and within Congress, there are differing views on the degree to which the intelligence community should collect and exploit open sources. Most observers, however, agree that the U.S. Intelligence Community should *not* be the focal point for open source collection *per se*, but that it *should* maintain a core capability to exploit private sector capabilities and to integrate global all source information into the all-source collection and production process. In practical terms, this means that *intelligence consumers are expected to manage and fund their own open source collection and production endeavors.*

1004. OSINT & All-Source Analysis

Open Source Intelligence, or OSINT, is an important part of the all-source intelligence process which includes clandestine Human Intelligence (HUMINT), Imagery Intelligence (IMINT), and Signals Intelligence (SIGINT). There are other important sub-disciplines, such as Measurements and Signatures Intelligence (MASINT) which analysts must understand and integrate to produce the best-possible intelligence.

Dr. Joseph Nye, then (1994) Chairman of the National Intelligence Council, used the jig-saw puzzle analogy to explain the relationship between OSINT and the classified disciplines. He likened open sources to the outer pieces of the puzzle, without which you can neither begin nor complete the puzzle. Classified sources, however, were essential to fill in the hardest to understand middle of the puzzle, and to complete the picture.

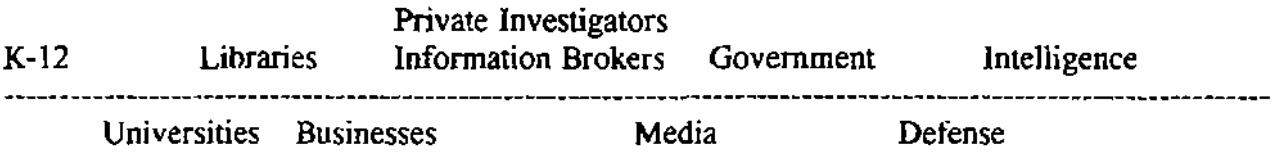
Mr. Paul Wallner, a member of the DIA Senior Executive Service, and the first Open Source Coordinator for the Director of Central Intelligence, described OSINT as "the source of first resort". His original conception was later adapted by a private sector commentator into the more dramatic phrase, "do not send a spy where a schoolboy can go'> Both drive home the point that open sources should be used to the fullest possible extent before risking and expending the more precious classified capabilities.

Dr. Joseph Markowitz, the current Director of COSPO, in addition to publishing the *Community Open Source Strategic Plan* (February 1995), has studied the utility of open sources in relation to traditional and emerging target sets, and concluded that open sources offer their greatest value as gap-fillers and initial orientations against Tier 4 Countries. Tier 4 Countries are those Third World countries which have not rated coverage by scarce classified capabilities, but to which the military must often deploy.

In brief, open sources are not a substitute for classified capabilities, but they can provide a valuable foundation and context for rapid orientation of the analyst and the consumer, and for the establishment of collection requirements which take full advantage of the unique access provided by classified sources. Analysts must be careful about relying exclusively on classified sources, especially against Tier 4 countries, because often the narrow range of classified sources may mislead the analyst into accepting a narrow interpretation of events.

1005. Knowledge Terrain: The Information Continuum

The figure below illustrates the "information continuum" which comprises the knowledge terrain of the private sector within which each all-source analyst must learn to navigate if they are to make the most effective use of classified as well as open sources. Appendix B has more detail on private enterprise intelligence capabilities.



Schools and Universities are a source of both labor (student as well as faculty), and data. Mercyhurst College, for instance, which has the only undergraduate degree in the USA focused on producing trained intelligence analysts, has its students using open sources to produce newsletters on narcotics and other topics of interest to law enforcement agencies. Universities across the country--and around the world--serve as "centers of excellence" in various areas of interest to intelligence community analysts. Knowing how to access and exploit such distributed capabilities can save the analyst time, save the community money, and improve support to the consumer. *Libraries* offer similar opportunities, including the Special Libraries maintained by major multinational corporations and international non-governmental organizations.

Businesses maintain a great deal of information, much of it unpublished but available for the asking, on both conditions in the countries in which the do business, as well as about key personalities. During the war in Southwest Asia, it was businesses which provided the most critical information about Iraqi command & control systems, including the detailed plans for his installed communications and computing infrastructure.

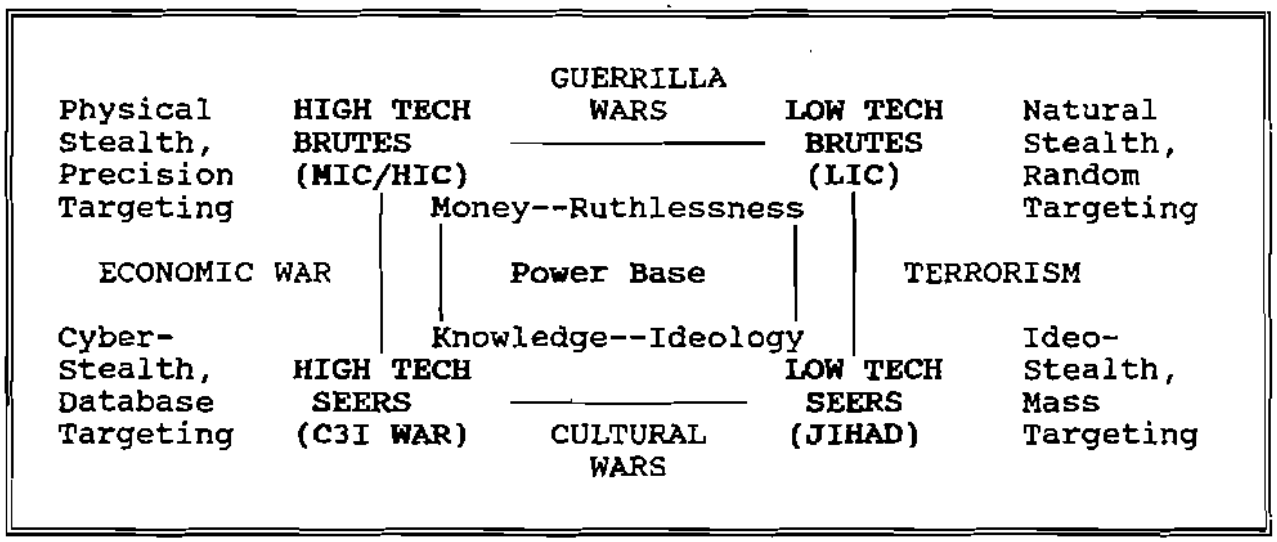
Private Investigators and Information Brokers spend their careers at someone else's expense developing expertise in certain areas and research methods. The *Burwell Directory of Information Brokers*, for instance, has specialists worldwide indexed by topic, country, and language fluency. They constitute a "ready reserve" for the intelligence analyst.

Few people realize that *media reporters* publish less than 10% of what they know, and are often happy to accommodate requests for information "on background". Although direct

contact by the analyst may not be appropriate, the analyst can use services such as LEXIS-NEXIS to identify experts in the media (e.g. the stringers covering Burundi or Somalia) and then task appropriate agencies with interviewing these experts along specific lines. Finally, analysts should catalogue their *counterparts* in other agencies and governments.

1006. OSINT and the Military I

The figure below illustrates the four warrior classes which confront both the military and law enforcement, and helps us understand that the intelligence challenges facing the military in the 21st Century require greater and distinct capabilities than those from the Cold War.



It is significant that our entire defense establishment, and our entire intelligence community, have been optimized over forty years to deal with just one of these warrior classes, the high-tech brute. The other three warrior classes represent significant intelligence challenges--the criminal, for instance, represents a "low-slow singleton" target which does not move high enough or fast enough, or emit enough of a signature, to be detectible by most of our space-borne early warning systems. The economic and computer warriors, the high-tech seers, represent both problems of jurisdiction, and problems of collection.

This training does not address policy, doctrine, or acquisition issues. The point of this chart is to both illustrate the challenges confronting intelligence analysts as they adjust to new targets; and also to make the point that open sources are--fortunately--both plentiful and pertinent when attempting to understand the three increasingly threatening warrior classes.

The information explosion has been a mixed blessing. Although a great deal of information about virtually every topic is available for purchase if not for free, the validity and utility of much of the information is questionable, and requires both heavy screening--

much of which cannot be done by machines--as well as translation and interpretation. All-source analysts today are trained to use classified tools and methods, and do not have optimal access to open source experts and databases.

Open source exploitation by DIA and the U.S. intelligence community is certain to improve, as this chapter concludes, because of the value of unclassified intelligence in support of unilateral information-based warfare, coalition operations, joint civilian-military operations, and support to law enforcement operations.

This chapter does not recommend that all-source analysts spend less time on classified sources and more time on open sources, but rather that they leverage private sector collection and production capabilities in order to optimize the collection management of classified capabilities.

1007. OSINT and the Military II

OSINT can be very important at each of the four levels of intelligence analysis. Appendix A provides additional discussion

At the strategic level, analysts have found that a careful review of open sources, even from societies subject to censorship, can provide a sound understanding of political plans and intentions. Open sources are especially helpful in forecasting cultural turmoil and providing warning of revolution or upheaval. Also at the strategic level, open sources are very useful for developing the *encyclopedic generalizations* needed to develop theater capabilities for multiple contingencies. Finally, open sources are very helpful in orienting both troops and the public.

At the operational level, open sources can help force planning as well as the coordination of joint and coalition operations. It is open sources, for instance, which have established that the average temperature for expeditionary operations in the Third World is 80°, with high humidity. Since most aircraft are designed for "warm"days rather than "hot" days, this means that their range and lift are significantly reduced.

At the tactical level, open sources have proven valuable in obtaining commercial imagery and related products, including 1:50,000 combat charts with contour lines, for Third World areas for which the Defense Imagery Agency does not have digital data or ready maps.[2] Analysts requiring imagery and tactical maps to support a commander should not

---

[2] Of 69 countries established in 1990 by the USMC as being "high probability" deployment areas, DMA had no data or maps for 22 of the countries; old maps for the ports and capital cities only of another 37; and very old maps for the remaining ten countries such as Cuba, North Korea, and Jamaica. *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (MCCDC, March 1991).

hesitate to request commercial imagery. Commercial imagery products also include multi-spectral imagery sensitive to heat differences, and automated three-dimensional "fly-by" videos of approaches to airfields and landing areas.

At the technical level, open sources are very important to developing information-based warfare capabilities and plans for attack; they are also useful in establishing realistic mobility estimates and weapons range and intervisibility (line of sight) needs.

1008. Militarily Useful OSINT: Two Examples

Two examples are offered here of how useful OSINT can be, either as the foundation for a classified collection effort, or "in a pinch" when classified offerings are non-existent and unlikely to be quickly forthcoming. The first example, Somalia, was developed in support of a Marine Corps Wargame in which LtGen Zinni requested a post-mortem on his performance in Somalia. The individual invited to serve as the United Nations Commander for this wargame requested and received the following products via overnight mail:

-- From Jane's Information Group, a one page map of Somalia clearly demarcating the nine clan areas; a one page order of battle for each clan including key artillery and mobility systems; and a compendium of one paragraph summaries with citations of every major article about Somalia published in any Jane's publication in the previous two years.

-- From Oxford Analytica, twenty-two two-page summaries "suitable for a President or Prime Minister" covering U.S. foreign policy toward Somalia; UN operations in Somalia, and US operations in Somalia.

-- From *The Economist* Intelligence Unit, a country study which, while shallow, had valuable insights regarding both the limitations and the fragility of the infrastructure.

Subsequently, in a second example, Burundi, the Commission on Intelligence requested and received, through overnight mail, products similar to the above from Jane's Information Group and Oxford Analytica, and in addition:

-- From Eastview Publications, a list of all immediately available Soviet maps of Burundi, with their scale and price.

-- From LEXIS-NEXIS, a listing of the top 25 journalists reporting on Burundi.

-- From the Institute of Scientific Information, a listing of the top 10 academic knowledgeable about all aspects of Burundi.

Subsequently, it was determined that complete coverage of Burundi was available from SPOT Image Corporation, data already collected and stored, from which both 1:50,000 combat charts with contour lines, and landing point fly-by simulations could be created.

1009. Representative Open Sources I

Contract information for all of the references and organizations discussed in this handbook is provided in Appendix D. Most libraries will not have these references or access to these organizations--asking them to subscribe or develop support contracts is something anyone can do to improve your entire organization's access to key open sources.

The British Library specializes in monitoring international publications, and does especially well with respect to Africa and Asia, and conferences about both scientific & technical topics, and general topics including military matters. They are an especially good source now for examining the contents of conference *Proceedings*, and offer their products in CD-ROM.

Oxford Analytica is unique for having a global network of almost 1,000 overt human experts on-call to prepare concise forecasts and situation reports suitable "for Presidents, Prime Ministers, and you". They specialize in political-economic reporting.

A number of **directories** can help the analyst rapidly identify experts, many of whom are not likely to charge for quick informal inquiries.

-- Specializing in **electronic access** is the book *Find It Fast: How to Uncover Expert Information on Any Subject.*

-- For rapid identification of predominantly **academic experts**, the *Social Science Citation Index* and the *Science Citation Index* are unmatched--they are particularly useful in that they provide the expert's address, prior publications, and list of citations by others, establishing their peer recognition as authorities.

-- **Government authorities** world-wide can be identified, with their full titles, addresses, and voice and fax numbers, through *Worldwide Government Directories*. Also available from the same organization is a biographic reference, *Profiles of World Government Leaders*.

-- Finally, the best private sector **information brokers** world-wide, with complete contact information and indexes identifying their topical and language strengths, can be found through the *Burwell Directory of International Information Brokers.*

1010. Representative Open Sources II

International research sponsored by other governments, international non-governmental organizations, multinational corporations, and universities has been poorly documented in the past; now a new service, *ResearchBase*, is available which allows analysts to determine if there are projects underway which can be built upon rather than duplicated.

The **Internet** is--like the information explosion which it represents--a mixed blessing. Internet resources are in constant motion, and no search path can be duplicated from one day to the next. However, a number of entrepreneurs are beginning to offer useful guides. Among the three best are the *Clearinghouse for Subject-Oriented Internet Resources*; the *Guide to Network Resource Tools*; and *netguide*.

Info-South is an example of how universities can provide distributed database and media monitoring services to analysts. This service provides english-language translations of key Latin American newspapers, and also biographic profiles of Latin American leaders.

Business community information can be accessed through the Special Libraries Association, over 15,000 corporate librarians, through the publication *Inside Information: Profiles of Association Libraries and Information Centers*.

Maps are always very useful, both to the analyst developing the all-source product, and to the consumer, who often does not know where to go once DMA tells them no maps are available. The following two sources are helpful:

-- **Eastview Publications** can rapidly identify and obtain maps of the Third World, generally down to the 1:250,000 level but sometimes better, which were created by the Soviet Union.

-- **SPOT Image Corporation** has most of the world digitized at the 10 meter scale, and from this scale can create 1:50,000 combat charts with contour lines, targeting packages for precision munitions, and three-dimensional "fly-by" visualizations of landing site approaches.

Unclassified **photographs** can add value to intelligence reports; the archive of DoD photographs is now available through the National Technical Information Service (NTIS); a vast collection of international photographs is available from United Press International.

1011. Representative Open Services 1

One of the most important changes in the open source world pertinent to the analyst is not the dramatic increase in the availability of raw data, but rather the significant improvement in the variety and capabilities of open services able to provide value-added collection, processing, and production.

Unlike direct acquisition requests for sources, these services generally have to be contracted for by the organization before they can be exploited; once a contract is established, however, individual analysts can then obtain direct support on demand.

Academic Journal Monitoring by Uncover Reveal or the Institute for Scientific Information allows analysts to receive tables of contents--via fax or email--for various

journals of interest, from which articles can be selected for acquisition.

Commercial online searches can be carried out directly by the providers, such as LEXIS-NEXIS or DIALOG, or through intermediaries such as NERAC. The former tend to be more efficient at exploiting their own databases, the latter has the advantage of charging a fixed price per year.

Daily current awareness profiles are a very good way of following the international media. The profiles generate daily lists of key articles, which can then be ordered if of interest. Besides LEXIS-NEXIS and DIALOG, the two most popular services are *Heads Up* from Individual, Inc., and *NewsEdge* from Desktop Data.

Document Acquisition world-wide is something private sector organizations do very well. Instead of burdening an Embassy with finding an obscure but essential document, organizations such as FIND/SVP can be relied upon.

Environmental information, of increasing importance to some intelligence consumers, depends heavily on commercial imagery as well as databases of environmental research. CIESIN (Consortium for International Earth Science Information Network) is among the leaders in this area.

European Economic Research is a specialty of Fuld & Company--specific research projects might be best conducted through a preliminary open source effort such a private sector company, followed by classified tasking.

1012. Representative Open Services II

Grey literature refers to publicly available (non-proprietary) documents printed in very limited numbers and generally not available outside the country of publication. ACCESS International, and Eastview Publications, are among the best in this area.

Infrastructure surveys, including "ground truth" photography and surveying, can be done by some private sector organizations which employ former SAS (Special Air Service) personnel traveling discreetly under tourist or business cover. E2G, a British company, is one of the few that is openly available. In the US, BDM Federal specializes in remote infrastructure surveys, using legally obtained open sources.

International **investigations**, including economic surveys and technical acquisition projects, can be carried out by private firms such as Kroll Associates or Parvus-Jericho.

Refugee debriefings world-wide can be a gold-mine of raw intelligence. Organizations such as Rapport Research & Analysis, based in the UK, specialize in organizing teams of trained military interrogator-translators in any language, and then conducting debriefings in the major international cities where refugees are legally accessible.

Third World economic analysis can be contracted to such firms as SIS International, which had created a network of host-country business research organizations with special strengths in Asia and Africa.

Telephone Surveys are often a very low-cost means of creating new knowledge and obtaining a rapid sense of where a specific topic stands among leading authorities in the field. Telephone research is a special skill-set which includes a sound understanding of how professional associations around the world are organized and can be exploited. Risa Sacks Associates is one of the top US firms with this unique capability.

Trade database creation is a specialty of the Monterey Institute of International Studies, which is already very well known to the intelligence community for its use of graduate students fluent in Arabic, Russian, and other hard languages to create their proliferation database.

Special comment: in the open source world, niche providers outside the beltway are generally more capable, and cheaper, than large corporations based in Washington, D.C.

1013. Intelligence in the Age of Information

The two major differences between intelligence during the Cold War and intelligence today are as follows:

-- During the Cold War, the enemy was a well-known conventional power with nuclear capabilities, and the threat was relatively static over forty years. This led to the creation of an intelligence community optimized to do repetitive classified collection against a denied area, with a strong focus on major weapons systems with strong electronic and heat signatures. Today, as addressed by the earlier discussion of the four warrior classes, the threat is much more diverse, and consists of many smaller groups that are more difficult to identify, track, and analyze.

-- During the Cold War, the necessary information for intelligence analysis was generally not available through public sources; today much of what is needed to satisfy intelligence consumers is available from open sources, and the intelligence community is often in competition with open sources reaching the consumer directly.

Today, analysts must be responsive to their consumer's desires for intelligence reports that are short, fast, and often unclassified, for the latter can then be shared with Congressional staff and media as well as the public, and thereby help to influence policy change. *It is the consumer, not the analyst, who should make the decisions regarding preferred length, level of classification, and time permitted for report preparation.*

Classified information, which cannot be duplicated by open sources, represents a unique value-added capability--it will be most successful if it builds on open sources, rather

than competing with open sources or--worse--ignoring open sources and finding itself out of context and under-priced by "good enough" open source intelligence.

The most successful all-source analysts will develop methods of harnessing distributed experts and data in the open source world; do "just in time" analysis and production that supports specific decisions being faced by their consumers each day; stay close to the consumer to monitor and add value to the flood of open source reaching the consumer directly; and will master the art of integrating unclassified and classified products so as to give the consumer added power through more disseminable open source intelligence, and added confidence through the unique value-added insights that only classified all-source intelligence can provide.

1014. Changing Role of the Analyst I

The traditional all-source analyst has generally been focused in the task of monitoring and integrating classified intelligence (HUMINT, SIGINT, and IMINT) reaching their classified workstation, and has relied only to a very limited extent on the full range of open sources and services available through the private sector. At the same time, because of time, resource, and security constraints, the analyst has generally not interacted on a regular basis with either their private sector subject-matter counterparts, or their customers.

There is a growing belief that the role of the analyst must change in this decade, moving away from a relatively isolated emphasis on processing hard-copy and electronic intelligence into "products" that are then passed anonymously to a generic set of consumers through an impersonal broadcast, and toward a much more active--a much more interactive--role as a manager of people and resources.

Specifically, since no analyst can hope to master both the flood of classified and the flood of unclassified information, some envision the "reinvented" *analyst as a manager of a network of overt sources which serve as a foundation (not a substitute) for all-source collection and production.* Such a network, maintained by distributed centers of excellence in the private sector, at no expense to the government, could serve as a filter of subject-matter open sources, provide "tiger teams" for short periods to develop surge knowledge bases (e.g. Somalia, Rwanda), and help the analyst frame key questions which cannot be provided by open sources and must be tasked to classified capabilities.

1015. Changing Role of the Analyst II

At the same time, in order to manage and mobilize such a network of overt sources, the *analyst as a manager of resources* must emerge--an analyst that knows who the top experts are, and has the authority to hire them "on demand" for very specific and relatively inexpensive direct support tasks.

Although the intelligence community has received very fine support from a number of

major beltway corporations, these corporations have constituted an "outer ring" of institutionalized capabilities with the same limitations as the intelligence community itself.

The envisioned change in the role of the analyst brings with it the possibility of more direct analyst control over external research & analysis, with more analyst authority over day-to-day direct support contracts with individual experts rather than anonymous institutions.

The significant advantage of this approach is that the community pays only for what it uses, when it is used--this allows the analyst to take advantage of experts whose overhead--whose lifetime of acquired expertise--has been funded by someone else, someone other than the U.S. taxpayer.

1016. Changing Role of the Analyst III

Given the vast amounts of open sources that reach the consumer, there is increased interest in developing analysts able to serve as a *manager of consumer relations*, with three specific objectives:

-- to win the consumers confidence on a day to day basis, and

-- to ensure that the consumer is receiving appropriate decision support daily; and

-- to monitor and exploit the open sources reaching the consumer.

It is very important for analysts to understand that consumers have and value their own open source connections, and they have and like to pay attention to their own departmental analysts.

The analyst, by developing a very close and constant relationship with their consumer, can not only gain access to the open sources that reach the consumer and do not reach the intelligence community--but can help the consumer avoid being taken in by open sources that might at first glance appear authoritative but which can--with the insights gained from all-source collection and analysis--be called into question.

1017. Changing Role of the Analyst IV

The professional intelligence analyst will always be different from scholars, journalists, and other expert commentators because only the professional intelligence analyst will have access to classified intelligence sources and classified intelligence tools.

The professional intelligence analyst that ignores open sources and relies exclusively on classified data for their raw input will not be competitive. In contrast to open sources, which represent the "information explosion" with all its pluses and minuses, the classified sources tend to be very finely focused and to produce narrow slices of information which

have to be melded and integrated. If you fail to use open sources to provide the context for analysis as well as the foundation for estimative intelligence. you will in all likelihood either miss the mark, or miss important tip-offs suggesting the need for classified tasking.

Open source information, therefore, should be seen as a pre-amble to fulfilling the analyst's ultimate responsibility as a *manager of classified capabilities* which lead to the production and delivery of an all-source product.

The role of open source information in the final product is important. At the Central Intelligence Agency, the general rule of thumb is that open source data comprises 40% of the final all-source intelligence product. Within the Defense Intelligence Agency, the general percentage, according to one graduate thesis survey, is 30%. In Canada, according to Mr. Ward Elcock, the director of the Canadian Security and Intelligence Service, open sources comprise 80% of the final all-source product.

What this means is that open sources are both a critical element in targeting classified capabilities, and also a critical element in explaining classified information in an all-source context.

Open sources are also very helpful when the analyst has classified sources which cannot be shared by the consumer with a specific audience (e.g. international organizations or the press)but which confirm the accuracy and utility of specific open source reports over others. Although the fact that the intelligence community lends its authority to specific open sources differentiates those sources at the time, this is sometimes the only way to provide intelligence in support of certain requirements.

1018. Overt Human Networks: Some First Steps

Most analysts know who their counterparts are at the other major intelligence agencies, and in the Joint Intelligence Centers (or, for law enforcement missions, the Regional Intelligence Centers). However, most analysts have not been afforded the time or given the incentive to identify and exploit their subject-matter counterparts in the private sector, and have perhaps also been concerned about the security implications of such contacts.

The analyst interested in evaluating the potential of the private sector to enhance their performance as an all-source analyst can take several steps in turn, with increasing management involvement, to achieve a unique status as a "hub" for both open and classified sources pertinent to their area of interest.

First, without engaging in any direct contacts of possible security concern, the analyst can inventory the private sector's capabilities in their area of interest, and rapidly establish a listing of key people--academics, journalists, business experts--who have something to contribute. At the same time, the analyst can inventory the availability of geographic information for their area of responsibility—as a former Director of the Marine Corps

Intelligence Center told the Council of Defense Intelligence Producers in 1992, "I don't care how much order of battle data you give me, if I cannot plot it on a (1:50,000) map, it is useless to me."

Jane's Information Group, which publishes both *Jane's Intelligence Review* and the *SENTINEL* series of *Country Reports*, also has an online database, and the capability to prepare special reports containing the 80% of the information they have about a country, but cannot publish for a variety of reasons including source protection.

Once the analyst has a good sense of who the top people are that might be of service as a personal network of overt sources, a few of these can be selected, and a specific plan proposed to management which seeks to fund individual familiarization meetings, possibly an exchange of unclassified data, and contingency arrangements for on-call support when required by a contingency.

Sponsorship of inter-agency subject-matter conferences, including an unclassified day with external experts, is a good way for the analyst to position themselves as focal points for voluntary information sharing.

1019. OSINT Among Selected Allies

In general, other intelligence communities are not any better off than the U.S. intelligence community with respect to open source exploitation. However, a number of them illustrate how improvements might be made in our own future endeavors.

Canada has gone on record publicly, stating that 80% of its all-source product comes from open sources; Canada is also a leader in doing unclassified strategic intelligence production which is receiving wide circulation and praise because it can be shared.

Israel has perfected the utilization of host-country information brokers, and exploitation of local laws such as the U.S. Freedom of Information Act, to obtain great quantities of information at almost no cost.

The United Kingdom, influenced by the open source movement within the U.S. intelligence community, has leaped ahead with the first public tender (Request for Comments) for an Open Source Information Center for the Ministry of Defence.

The United Kingdom Open Source Information Center is especially important because it could serve as a model for the United States of America, the other partners in the North Atlantic Treaty Organization, and the United Nation. An initiative to develop a center of expertise at the Joint Analysis Center (Molesworth) would be especially useful as a vehicle for linking United Kingdom and U.S. open source acquisition programs in the military arena.

1020. OSINT In Asia

In Asia there are several examples of strong approaches to open sources as a foundation for both national security and national competitiveness.

Australia, and specifically the Defence Intelligence Organization, has collected a significant amount of open source information on Papua New Guinea, the Spratley Islands, and other areas of interest to the U.S. Pacific Command, but they have no focal point for open source burden sharing.

Japan relies heavily on its private sector, notably the trading companies, for its open source collection, with a stated daily collection of 6,000 newsprint-size pages. Japan has also perfected "dissemination trees" in which each major organization collecting open sources from other countries--whether in the government or in the private sector--has roughly sixty other organizations to which copies are immediately routed.

Singapore relies primarily on open sources, and focuses heavily on economic intelligence. As a major banking center in its own right--and the likely base for those who choose to leave Hong Kong once it is turned over to the Republic of China, Singapore understands the value of providing its business community with a robust information environment. The National Computer Board (NCB) has representatives in every government department and is rapidly integrating all government databases. They will do the banks next--focusing on encyclopedic marketing information--and then elements of the private sector on a voluntary basis.

Taiwan has not been adequately studied, but it should be high on our list of countries to be observed because in Singapore, Taiwan is considered the "model" for open source collection.

1021. OSINT in Europe

France is actively orchestrating economic intelligence collection and education. In 1993, after the publication of the book *Friendly Spies*, and coincident with the privatization of a number of key French companies, the Prime Minister directed increased focus on the utility of open sources of intelligence. A conference was sponsored in October 1993 at which General Heinrich, then Director of Military Intelligence, and several other authorities including the leading U.S. advocate for open sources, made presentations to 300 leaders from across France on the subject of reinventing intelligence and using open sources. The government continues to play a strong role in organizing economic and information strategies, and in encouraging economic intelligence education.

The Netherlands has reorganized its collection to make open sources co-equal with technical and clandestine collection; uses a task force approach to analysis that beings with open sources; and optimizing its exploitation of the Internet by having specialists do

centralized discovery of Internet resources, while analysts do the decentralized exploitation of the resources once specifically identified.

Sweden, although small, has optimized its performance in science & technology by coordinating government, business, and academic collection of open sources through an informal committee called the Swedish Open Source Coordination Forum. The Swedish government is considering the "privatization" of the existing scientific & technical attache service, motivated largely by the need to decrease government spending. Swedish scientific & technical attaches have been aggressive about patrolling the Internet in search of both data and points of contact.

1022. OSINT Within DIA 1

The Program Manager for Open Source Intelligence within the Defense Intelligence Agency is Ms. Alice Cranor, whose contact information is provided here. She serves as the DIA representative to the Open Source Council, which is the advisory body formed to support the Community Open Source Program Office (COSPO). Each agency and service has a single representative to the Council. In addition to an agency-level focal point, every branch within DIA has an OSINT focal point.

The only survey to date of open source intelligence exploitation within DIA was completed in August 1995. "Open Source Intelligence: An Examination of Its Exploitation in the Defense Intelligence Community", by Major Robert Simmons, USA, is a Joint Military Intelligence College thesis which surveyed all analysts in DIA and its two production elements, the Armed Forces Medical Center and the Missile and Space Intelligence Center.

Maj Simmons' findings are shown here:

-- Less than 30% input from open sources

-- Such open sources as are used come through SAFE from FBIS

-- Most analysts do not have Internet access

-- Most analysts rarely discuss issues with external experts

-- Most analysts are not aware of other open source resources

-- Most analysts are generally satisfied with their level of access to open sources

Maj Simmons' concludes that the analytical components of DIA are generally "ill-prepared and ill-supported to make full use of any information outside of the small, restrictive and limited domain of classified intelligence sources. The cultural attitude at DIA generally reinforce(s) using classified information as the first and last stop in the analytical process and

open sources are used rarely to fill the gaps. The result is an intelligence product limited in its scope and overly expensive."

1023. OSINT Within DIA II

Although the thesis results are negative with respect to existing DIA practices, and funding constraints do not appear to offer significant relief in terms of new initiatives to exploit open sources in support of military intelligence, there has been a significant increase within DIA of appreciation for the potential of open sources.

Maj Simmons' thesis concludes with these findings:

-- Tier 3 and 4 countries, where there is a very high probability of U.S. military involvement in contingencies, are not covered by established classified collection priorities.

Almost all of the countries of concern to the Marine Corps, as defined in the *Expeditionary Force Mission Factor Intelligence Analysis Requirements Study* (Marine Corps Intelligence Activity, 15 September 1994), are Tier 3 and 4 countries. In addition to a lack of encyclopedic intelligence, there also exist severe shortfalls in mapping, charting, & geodesy (MC&G) data needed to produce 1:50,000 combat charts for combined arms coordination and ground maneuver. Fortunately, commercial imagery, including 10-meter resolution imagery from SPOT Image Corporation, is capable of providing 1:50,000 maps with contour lines within hours or days--HOWEVER such commercial products still require assistance from classified capabilities orchestrated through the Defense Mapping Agency in order to integrate "ground truth" precision points needed to ensure the accuracy of the maps, as they are to be used for coordinating combined arms fires.[3]

1024. OSINT Within DIA III

Continuing with the conclusions from Maj Simmons' thesis:

---

[3] Two major surveys have been done in recent years of MC&G short-falls in the Third World. The first was done by the Special Operations Command (J-2) in 1987-1988; and the second, focusing specifically on expeditionary contingencies, was done by the new Marine Corps Intelligence Center (now Activity). The Marine Corps Study, published as *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (Marine Corps Combat Development Command, March 1990), found that of the 69 countries of concern to the Marine Corps, there were no combat charts at all for any portion of 22 of the countries; old combat charts for ports and capital cities only--not for maneuver areas--for another 37 countries; and very old combat charts for the remaining ten countries where higher priorities has permitted full coverage at one time--countries such as Cuba and North Korea.

-- OSINT is often the only resort in the early stages of a crisis, and critical in support of rapid-response planning for deployment--it should be noted that commercial imagery and 1:50,000 combat charts with contour lines from commercial imagery can be obtained within hours or days of demand.

-- Private sector publications such as those produced by Jane's Information Group often provide defense intelligence analysts with their first tip-offs on weapons modifications and sales.

-- Open sources serve as valuable tip-offs about national leaders' intentions, since actions are often justified in advance to their public through the press.

-- The majority of Third World terrorist information is obtained from FBIS and wire services (proliferation specialists say the same thing)

-- OSINT is essential when unclassified products are needed for coalition operations or briefings to uncleared Congressional members and staff.

What is the bottom line here: improved exploitation of OSINT as part of the all-source product is not going to be driven by top-down directives, but rather through bottom-up initiatives. Every analyst must understand the value of open sources, and the range of open sources and services available to support their subject-matter production requirements. Through a concerted effort by all analysts to request funding for access to open sources and services, defense intelligence will gradually be revitalized.

1025. OSINT and the All-Source Product

Concluding in this vein, recognizing that the analyst is the focal point for change in how we prepare the all-source product, this chapter suggests that each analyst must:

-- Strive to understand the information continuum and how private sector subject-matter experts and databases can provide direct support to the all-source process;

-- Develop a personal "map" of open source experts of possible value, including complete contact information. This is something which can be done without direct contact, as a pre-amble to securing management and security approvals for interaction.

-- Submit specific proposals to management for employing specific experts in specific ways to enhance the all-source intelligence product; and finally,

-- Work with security to establish comfortable ground rules for both planned and spontaneous contacts and unclassified information exchanges with external experts who will rarely have--or accept--security clearances.

The intelligence analyst is the critical linch-pin for reinventing the intelligence process and fully integrating open sources as a foundation for the all-source product. Those analysts that fully understand open sources, and develop proposals for exploiting open sources, will find themselves able to manage networks of overt open sources, able to justify and to manage modest resources to mobilize those open sources on demand; able to significantly improve their management of consumer relations and their exploitation of open sources reaching the consumer directly; and able to dramatically improve their management of classified capabilities, both in collection and production.

Open sources are <u>not</u> a substitute for classified sources--they are an essential and valuable foundation for making the most of our scarce classified capabilities.

Chapter 2

ACCESS: INTELLIGENCE IN THE AGE OF INFORMATION

2001. Purpose of the Chapter

The purpose of this chapter is to present a more in-depth look at why open sources are critical to the all-source analysis endeavor, and how all-source analysts can optimize their exploitation of open source information.

Included in this overview will be: definitions distinguishing between data, information, and intelligence; discussions of how the art of intelligence is changing in the face of the "information explosion", the four kinds of information categories that an all-source analysts can consider accessing, and the three elements of information value; a discussion of the nine levels of open source information; an examination of possible collection management strategies which integrate open sources into the all-source collection management task and exploit windows of opportunity in which material is available in open sources just prior to being classified or censored; discussion of the four major consumer groups and their intelligence productions needs in relation to open sources; an examination of the four "warrior classes" and how open sources apply to intelligence analysis of each; discussion of the four types of overt human sources the analyst will encounter; an examination of how open source intelligence (OSINT) can help conserve scarce classified resources, and how a national information strategy can increase the amount of open source information available to the defense intelligence community; and concluding comments on optimizing OSINT in the all-source analysis process.

2002. Definitions

For the purposes of this chapter, the following definitions are reviewed. This is a review of definitions provided in Chapter 1.

-- **Data** is the raw print, image, or signal. Data can be classified, as in a technical intelligence signal intercept, or unclassified, as in a report from the Foreign Broadcast Information Service (FBIS) on a public television report. Please note that open source data includes commercial imagery such as is available from SPOT Image Corporation, and from which 1:50,000 combat charts with contour lines can be quickly constructed.

-- **Information** is data that has been collated, processed, in order to produce a report that is of generic interest. Information can be multi-media, with integrated graphics and imagery, or simply a print report including interpretation of imagery.

-- **Intelligence** in this context is used to distinguish those products which tailor information in order to support a specific decision by a specific customer.

These definitions are important because the analyst will often deal with consumers and with questions where the best answer is an unclassified answer. The all-source analyst must avoid falling victim to the concept that only a classified answer has authority. The fact that the all-source analyst has access to classified information is what lends a special credibility to their selection of an open source and their provision to the consumer of an unclassified answer.

Intelligence consumers have important political and public responsibilities which frequently require candid discussions of "the threat" or "the situation" with individuals who are not authorized access to classified information. To the extent that the all-source analyst can provide the consumer with credible unclassified intelligence, the analyst will be facilitating the intelligence consumer's policy tasks.

2003. New "Rules of the Game"

As the defense intelligence community moves away from focusing almost exclusively on the former Soviet Union and "denied area" intelligence, the all-source analyst is faced with requirements from new consumers, about threats and situations in the past which previously did not warrant all-source collection and production. Examples of such old but now more important intelligence problems include proliferation, terrorism, transnational crime, environmental threats, and economic intelligence.

Here are four new "rules of the game":

-- The National Foreign Intelligence Board has stated for the record that open sources comprise 40% of the all-source product, at a cost of less than 1% of the National Foreign Intelligence Program. For some intelligence problems, such as proliferation, and for some allied intelligence services such as the Canadian Security and Intelligence Service, open sources comprise 80% of the all-source product.

-- The private sector has most of the real experts for those problems which are not traditional intelligence concerns. The Vice President has spoken about the need to "harness the distributed intelligence of the Nation". The all-source analyst needs to identify and exploit experts in the private sector and experts in allied governments.

-- Although electronic sources are fashionable, and most defense intelligence analysts rely almost exclusively on open sources collected by the Foreign Broadcast Information Service and delivered to their desktop workstation by the Secure Analysts File Environment (SAFE), in fact most open sources are in hard-copy, in a foreign language, and not available on the library shelves. Analysts must consciously define their open source requirements and set in motion the process to acquire the necessary open source material.

-- Analysts can no longer afford to do "just in case" collection and production. The demands on analysts are so extensive--almost overwhelming--that only a "just in time"

approach will permit them to satisfy consumers. This is especially true because information changes so quickly, that old archived information is usually overtaken by events. Analysts will do better going out to distributed databases at the last possible minute, and then integrating recent classified collection into their all-source product.

2004. Four Information Categories

The all-source analyst should understand that there are four information categories, and the relative cost and degree of difficulty for exploiting each category.

-- Open Source Information is legally and ethically available, at a low cost. The analyst that fully exploits open source information to establish a foundation for their all-source product can generally improve their understanding of the problem and its context at a low cost, and can often reduce requirements for classified collection.

-- Open Proprietary Information, can be legally and ethically obtained, but require a moderate cost to commission reverse engineering studies to extract the information from the product. This is a good alternative to riskier and higher cost espionage intended to steal the information from within the target organization. Examples: buying a French missile to study the missile guidance software and hardware; buying Russian imagery to calculate their overhead technical capabilities.

-- Closed Proprietary Information is only available from within the secure areas of the target organization, and requires espionage, at high cost, to obtain. Some intelligence services use private sector investigative agencies to obtain such information, under the guise of industrial espionage--a form of false flag operation. Examples: stealing source code for major computer applications; stealing designs for delicate machinery used to create scientific & technical instruments.

-- Classified information, collected by spies and satellites, is very expensive, and in the cast of Human Intelligence (HUMINT), often very risky. It does, however, have a very special value to the all-source analyst as its accuracy and reliability is high--this is especially the case with Signals Intelligence (SIGINT) products.

As analysts are thinking about an intelligence problem, they can benefit by drawing four circles around the problem definition. The outer circle, the largest, is the open source information domain. The analyst can annotate what open sources might offer insights to the problem. The next two circles moving inwards are open proprietary information and closed proprietary information. Finally, the smallest circle, classified information, can be annotated to show what precise and specific collection could help the analyst complete the intelligence puzzle. Using this method will help optimize the contribution of low-cost open sources while focusing demands on classified capabilities.

2005. Information Value

Here we want to consider the three elements which--taken together--comprise the value of information. Each is important because each can help the all-source analyst think about their collection management and production processes.

The raw content, a specific document, is often easy to obtain once it has been identified, but not so easy to identify. Any analyst who has ordered a commercial online search and received a listing of thousands of documents, with no means of sorting through them to determine relevance to the problem, will understand how difficult it can be to identify exactly the right document. Resources are scarce, and it is not cost effective to collect all possible documents and then review all personally. Analysts need to work closely with librarians and other open source collectors to refine the inquiry as much as possible. *Often, the best way of refining the inquiry is to consult a private sector expert--such as a defense industry expert--who is fully familiar with available content.*

The context within which specific content can and should be evaluated is often overlooked. For lack of both background and time, the analyst may not realize that specific cultural or political conditions give the content a meaning different from that which it might have in a U.S. context. *Again, consultation with a private sector expert--perhaps including a reputable journalist or a businessman resident in the area of interest--is often the best means of rapidly coming up to speed on context.*

Finally, we have timeliness. Analysts need to be sensitive to the fact that Foreign Broadcast Information Service reporting, while it contains value-added commentary, often arrives two to three weeks after it has been published. Internet news sources and commercial online services are more timely. "Near real time" media monitoring may not always be necessary, but analysts should consciously evaluate the timeliness with which they are receiving open source (and classified) information, and take steps to improve timeliness when it is important to the accuracy and relevance of their all-source intelligence production for the intelligence consumer.

2006. Open Sources

Here we briefly review nine levels of open source information. Future chapters in this course provide more detailed examination of sources such as the Internet.

The Internet is largely "free" once access is obtained, but analysts have to remember that "you get what you pay for". The reliability of Internet sources varies widely, and exploration of the Internet is very labor intensive, and can be misleading. For instance, analysts accessing the Internet through America Online or Compuserve need to know that they are seeing only those Internet sites pre-approved by their service provider.

Commercial online services are very useful, but represent the tip of the knowledge

iceberg. It is also critical for analysts to understand that commercial online services have different kinds of access and are not equivalent to one another. A CIA study found that of all the journals of interest to their analysts, one fifth were accessible through LEXIS-NEXIS (generally trade publications), one fifth through DIALOG (generally academic publications), one fifth through other online services (such as specialty scientific & technical publications), and *two fifths were not online* (such as Third World publications). Therefore, a collection strategy which mixes and integrates the different online services with hard-copy document acquisition is most likely to be successful.

Limited access electronic databases, such as are maintained by universities, industrial associations, or businesses, can over time be identified, and access gained through formal or informal contact. *Here again, overt human contacts are your best means of identifying pertinent databases that are not in the public domain but are accessible.*

Published literature and "grey literature " (limited edition publications) are the more commonly recognized mainstay of the open source world. *Do not overlook foreign language materials.* The *Burwell Directory of Information Brokers* will help the analyst identify professional searchers who speak a foreign language and are familiar with specific topics such as aerospace or nuclear proliferation.

Speeches and briefings are often overlooked as critical sources of "tip-off" on changes in policies and capabilities. In addition to LEXIS-NEXIS searches for media reports on such speeches, organizations such as The British Library carry conference *Proceedings*. Finally, direct interviews and sponsored external research complete the list.

2007. Collection Investment Strategies

Realistically, the analyst is largely dependent on classified information that reaches their desktop workstation or their desk in hard-copy, and on such open source information that reaches them through SAFE. The analyst is also constrained by security and procurement processes that limit their ability to directly access external open sources including overt human experts.

Over time, we can expect progress in developing more direct access options for the analyst. In the interim, analysts can engage in several collection investment strategies where they allocate their time as a means of optimizing open source contributions to the all-source product.

First, analysts--in their role as collection managers--should pay heed to the words of Mr. Paul Wallner, the first Open Source Coordinator (and a member of the DIA senior executive service), who says that "open source should be the source of first resort". By focusing first on what is available through open sources, analysts will more quickly come up to speed on both content and context.

Second, analysts--in their role as resource managers--must recognize that it takes time to develop new forms of access, and that when they identify promising open sources which can contribute to the all-source intelligence production process, they should document their findings and make a business case for allocating funds to maintain access to such sources. Generally such resource planning must occur a year in advance of funds being obligated.

One investment strategy--initially addressing only how an analyst spends their time but ultimately suggesting how dollars might be allocated--would have the analyst spend twenty percent of their time identifying and analyzing open source information. It is important to note that because of the broadness of the open source environment, and the facility with which open sources can be exploited, a 20% investment of time or dollars yields dividends in excess of the investment, on the order of 50% of better of the contribution to the all-source product.

OSINT is well-suited to be the foundation for classified collection management through its provision of encyclopedic and contextual knowledge. However, classified sources must be used, and the analyst must create an integrated all-source product.

2008. Windows of Opportunity

One of the interesting realities about scientific & technical intelligence which has been noticed by expert analysts over time is that often, critical information is published in open sources for a time before it is suddenly classified.

"Secrecy" is in reality an administrative classification of information. Analysts should be alert to precedent knowledge as a foundation for targeting classified capabilities against programs that have suddenly become classified. Censorship is in fact an excellent "tip-off" that a body of knowledge is now being exploited for military purposes.

Pre-publication opportunities for collecting knowledge directly from overt human sources are especially valuable, since "secrecy" tends to be imposed on written information rather than inherent knowledge. If an analyst cannot obtain approval for direct access to foreign scientists and observers, the analyst might consider developing an external research contract with key academics whose foreign travel and attendance at conferences can be funded. There will be significant regulatory guidance on what is permitted, and close coordination with established HUMINT agencies will be required, but the analyst can serve as a catalyst for targeting specific kinds of knowledge before it is published.

Pre-recognition of emerging knowledge areas is also a worthwhile analytical focus. Using citation analysis and bibliometric studies from such unique sources as the Institute for Scientific Information is a very good means of rapidly identifying clusters of knowledge experts and new trends in their relationships to one another. Bio-technology, for instance, could be anticipated by an analyst observing increased cross citations between biologists and computer scientists.

In the final analysis, *there is no substitute for peer contact*. Analysts must strive to identify, get to know, and interact professionally with their counterparts in the private sector, for these individuals are funded full-time by their institutions to follow the topic the analyst is interested in, and can often provide short-cuts and direct access to information that would otherwise take weeks or months to identify and exploit.

2009. Collection Management

There are a number of influences on how classified collection capabilities are actually managed, and analysts need to be aware of the relative priorities and the inevitable gaps in coverage.

Tier One and Tier Two targets (e.g. Russia, China, Germany) will generally receive solid coverage but occasionally require emphasis or follow-up. It is important to note that just because a target is receiving a Tier One or Tier Two priority, this does not mean that classified sources are providing comprehensive coverage. Open sources can provide invaluable additional information including contextual knowledge.

Tier Three and Tier Four targets (e.g. Somalia, Burundi, Haiti) will generally not receive in-depth coverage, and the analyst will have to be very specific about their requirements. It is possible to request a temporary increase in priority for an important "gap" in knowledge about the target. Open sources can be especially helpful in providing "tip-off" information and contextual information which will help the analyst make a case for a temporary increase in priority against a specific aspect of the target.

"Needs-driven" intelligence production, which is to say production that responds to direct requests from the intelligence consumer, is under scrutiny from Congressional staff because they are presuming that such requests are being communicated outside the existing priorities management system. Analysts need to exercise care and have the support of their managers when fulfilling "opportunity analysis" requests. Here, however, open sources will often provide a cheap and quick means of giving the consumer "good enough" intelligence without tasking classified capabilities.

Traditionally, consumers talk to analysts, analysts talk to collectors, and collectors talk to or examine sources. This is the "linear" paradigm for collection management. Increasingly, as open sources become more useful to intelligence consumers, and security obstacles are gradually eliminated, a new paradigm is utilized, the "diamond paradigm". This means that consumers, analysts, collectors, and open sources can and should talk directly to one another, as a means of improving communications, avoiding misunderstandings, and getting "real time" answers from the source to the consumer.

The bottom line for analysts in the open source world: the more overt human sources you can develop in your field of expertise, the more ACCESS you will have to useful OSINT.

2010. Four Major Consumer Groups

In developing their research plans and thinking about how to craft their all-source products, analysts can benefit from an understanding of the four major intelligence consumer groups, each of which has a different "level of analysis" interest.

At the strategic level, departmental consumers are concerned with strategic generalizations and with the plans & intentions of their counterpart leaders across the board, in all regions. For example, if an analyst were to examine all of the countries where the contingency employment of U.S. troops is likely in the next few years, they might find that all of the countries less one or two are characterized by very high temperatures and humidity. This is an important strategic generalization because it impacts on aviation capabilities by reducing the amount of lift and the range of aircraft. Departmental planners can thus benefit from understanding that their "average" aviation capability in most contingencies will be less is assumed by doctrine.

At the regional level, theater commanders and their staff need regional generalizations and detailed mobility studies. For example, very few operational staffs will focus on port clearances (the deepest ship draft), the location of the five fathom line (critical to naval gunfire support), or the distance of the Embassy from the five fathom line (which determines if CH-46's can get there and back without Forward Area Refueling Points). Analysts able to draw out such generalizations will be able to provide a regional intelligence model that is very useful. Most of this information is available from open sources.

At the tactical level, mission area specifics and demographic and cultural studies are helpful. Most of this information is available from open sources, and in the case of demographic and cultural information, is often available only from open sources.

At the technical level, in addition to mission area specifics, it is helpful to develop realistic assessments of the degree to which both friendly and enemy capabilities are supportable by their respective logistics and intelligence capabilities.

There is no "schoolbook" solution for how to shape an intelligence analysis product in relation to the likely consumer, but if analysts are sensitive to the "level of analysis" that their consumer requires, they can provide intelligence products which are more meaningful and which reduce the burden on the consumer to sift through products.

2011. Intelligence Production

Continuing our discussion of the "level of analysis", here we can see that open sources have a great deal to contribute to the all-source product at each level.

At the strategic level, much of the information about military sustainability, including the availability of fuel, water, and rations, can be obtained through analysis of open sources.

The analyst that understands history and geography can exploit open sources to establish a good sense of how geographic location and civil allies might influence plans and intentions.

At the operational level, open sources are not only vital, but often more pertinent than classified sources when studying military availability, geographic resources, and civil instability. Jane's Information Group is regularly credited by analysts with providing "tip-offs" on new weapons acquisitions. A sound understanding of geographic resources can help analysts interpret various scenarios, some of which may not be supportable (or may be driven by) a lack of resources such as oil. Civil instability is especially understandable through open sources. One Department of State analyst, studying the possibilities for instability in Iran in the event of the leader's death, found that clandestine sources tended to reflect the biases of the sources, all former officers under the Shah, and that local newspapers, despite censorship, were provided the most accurate sense of the situation. *Foreign language skill is essential to derive the fullest possible benefit from open sources.*

At the tactical level, while military reliability (troop training, equipment maintenance) is best established through classified sources, open sources offer a great deal. Here it is important to understand that organizations like Jane's Information Group have a great deal of information about military reliability that they do not publish, but which is available on demand. Geographic terrain, particularly for the bulk of the Third World for which the Defense Mapping Agency does not have data, can be studied through commercial imagery. Very few people in Washington realize that 10 meter commercial imagery is adequate for the production of 1:50,000 combat charts with contour lines, as well as simulated three-dimensional fly-bys. SPOT Image Corporation can provide these products for anywhere on earth within 24-72 hours.

Finally, at the technical level, open sources are especially useful in evaluating the civil infrastructure, including the telecommunications, power, and financial networks.

2012. Target Categories

Each area of operations is likely to have a mix of four different kinds of "warrior class" which must be studied. These distinctions are provided in order to help the analyst broaden their effort beyond standard order of battle information, and to emphasize the utility of open sources in understanding non-traditional capabilities.

The traditional opponent which the U.S. has prepared for is the "high-tech muscle" warrior, represented by most of the Western allies and such major powers as Russia and China. This also includes powers such as Iraq which have invested heavily in expensive and sophisticated mobility and weapons systems. Existing classified collection capabilities are best suited for studying this warrior class, as the military systems generally emit heat or have clearly recognizable electronic signatures.

The next most understood warrior class, the "low-tech muscle" warrior, is generally associated with low intensity conflict scenarios. This warrior class is very difficult to track using existing classified capabilities because it represents the "low slow singleton" problem. This class of warrior utilizes single human couriers, Cessnas, and unsophisticated means of communications which do not lend themselves to interception. Surprisingly, open sources turn out to be useful against this class of warrior. The best example of a "success story" is found in the Southern Operations Command, which worked with the Los Alamos National Laboratory to obtain, translate, and study Latin American newspaper articles about drug activities in Latin America. SOUTHCOM discovered that Latin American investigative journalists are very good and provided complex reporting on the relationships between drug cartel members, the supply routes, the arrival of precursor chemicals, and a wide variety of other useful information.

The least understood warrior class is the "low-tech brain" represented by Islamic fundamentalism, for example. This is a warrior class for which open sources are the only viable means of understanding its plans and intentions. However, the open source materials to be mastered are so voluminous, and almost always in a foreign language, so that this becomes a very labor-intensive activity. Against this kind of problem, overt human experts in the private sector often offer the shortest route to insights.

Finally, the "high-tech brain" warrior class, now very popular as we think about both information warfare and economic warfare....here open sources play a very important role. Examples include hackers, electronic bank robbers, and industrial spies.

2013. Types of Overt Human Sources

The purpose of this chapter is not to over-generalize or to categorize all human sources into four groups, but rather to stimulate analyst consideration of what biases and accesses might be represented by any particular overt human source whose written or verbal work they are integrating into the all-source product. These generalizations are offered for discussion purposes only!

These categorizations are drawn from a French source with a strong background in clandestine intelligence, who has spoken publicly on open source intelligence methods.

"Ivory Tower" academics, irrespective of their cultural backgrounds, tend to quote one another and to focus on abstract aspects of a problem in isolation from political and economic realities.

"Band-Wagon" journalists, always following the latest story, have a tendency to write about whatever the latest trend is, whatever the latest "spin" is on a story.

"Mainstream" operators are bound by their institutional or political loyalties to cite the conventional wisdom.

"Up and coming" leaders are the best source for tip-offs on emerging trends and plans and intentions, because they are change agents and more likely to put forth innovative and controversial ideas.

In evaluating the range of open sources that can be collected and integrated into an all-source product, the analyst might wish to consider each open source document with respect to the above four categories, and then to search for open source materials from those categories that are not yet represented. In this fashion, a "collage" of opinion can be charted which is more likely to offer insights, and to provide a solid context for the integration of classified intercepts and other classified materials.

2014. OSINT As A Resource Saver

Apart from its value as "content", as part of the all-source solution, open sources offer significant savings when they are used to avoid waste and unnecessary tasking of classified intelligence capabilities. It is sensible to avoid sending a spy where a schoolchild can go. It is also sensible to understand that intelligence products which limit themselves to classified sources are likely to miss important contextual knowledge and perhaps suffer from serious misperceptions.

Open sources can be the foundation for establishing a more efficient and more focused classified collection management plan. Open sources can be a means of satisfying intelligence consumers with "good enough" answers that avoid tasking classified systems at all. Open sources can be supportive of classified collection targeting, by helping the analyst identify specific human, communications, and organizational targets so that classified capabilities can be "pin-pointed".

Mr. Keith Hall, Director of the Community Management Staff, coined the term "ASK-INT" when he was a member of the professional staff of the Senate Select Committee on Intelligence. Too often, he noted, classified capabilities were tasked to obtain information that could be had for the price of a telephone call. Naturally there will be times when the analyst does not wish to reveal interest in a topic, but there are means for asking open source questions through contracted private sector parties at a lower cost than would be incurred when assigning the question to classified capabilities.

In the signals intelligence arena, open sources have proven to be extraordinarily useful in monitoring conditions across entire nations and in specific areas of interest such as the political and economic arena. For example, analysts tracking regional newspaper stories and editorials can form very accurate impressions about stability and changes in political power. Open sources also provide very valuable information about telecommunications networks (for example, the exact location and nature of power plants, telephone switching stations, and satellite downlinks) which can be used to target classified capabilities.

In the imagery arena, commercial imagery is now available at 10 meters resolution from SPOT Image Corporation, and 2 meter resolution from the Russians. A variety of other commercial imagery providers are emerging, some offering 1 meter resolution imagery capabilities. Low cost commercial imagery, and maps, are a very important resource saver.

2015. National Information Strategy

The national and defense intelligence communities are part of a much larger information continuum, discussed in Chapter 001. One of the challenges facing our Nation as it enters the Age of Information is that of fully exploiting open sources, and ensuring that the broadest possible range of open sources are available to the national and defense intelligence analyst.

The Defense Information Infrastructure (DII), the National Information Infrastructure (NII), and the Global Information Infrastructure (GII) are part of an innovative and comprehensive effort by the current administration to develop increased connectivity across all sectors of the information continuum.

As the Vice President of the United States of America has noted on many occasions, the NII seeks to "harness the distributed intelligence of the Nation". What this really means to the professional intelligence analyst is that new means are being developed which will allow the analyst to access distributed centers of excellence where overt human experts and unclassified electronic databases are maintained. This is helpful to the intelligence community because it enables exploitation of expertise that has been funded by the private sector.

Still lacking for the intelligence analyst is an inventory of such centers of excellence as they apply to the needs of the various functional area specialists. In the interim, each analyst must attempt to identify such centers on their own, and to then work with the library and other collection channels to develop regular access.

An opportunity exists for analysts to take the initiative in developing international unclassified burden-sharing agreements with their counterparts in allied intelligence agencies. Australia has unclassified information on the South Pacific, France and Italy on Africa, and so on. Creative exchanges of unclassified information could be helpful.

Finally, it is important to stress that the existing electronic infrastructure for accessing open source information is not secure. Analysts need to recognize that Internet transactions can be monitored, that viruses are rampant outside the TEMPEST environment afforded by the intelligence community, and that there are many security hazards, both in terms of monitoring and in terms of destructive software, in the open source world. A national information strategy will begin the process of making it safe to work in cyberspace.

2016. Optimizing OSINT

The purpose of intelligence is to inform the policy-maker and the commander.

In developing their collection management and intelligence production plans, the analyst should consider the following paraphrase from the Navy Wing Commander who led the lead flight over Baghdad during the Gulf War:

> *"If it is 80% accurate, on time, and I can share it, this is a lot more useful to me that a compendium of Top Secret CODEWORD information that is too much, too late, and needs a safe and three security officers to move it around the battlefield."*
>
> Navy Wing Commander
> Technology Initiatives Wargame 1992
> Naval War College, Newport RI

In striving to satisfy an ever-growing demand for intelligence, about an always expanding range of topics, the analyst will have to adopt the traditional public administration principle of "satisficing", working to provide the intelligence consumer with "good enough" intelligence. Just as "better" is the enemy of "good enough", excessive reliance on classified capabilities which are already over-tasked, can be counter-productive to the task of informing the intelligence consumer.

In the chaos of the 21st century, the distributed centers of excellence in the private sector which collect and process open source information, are the analyst's first line of defense--as Mr. Paul Wallner has noted, "the source of first resort".

Ultimately the all-source analyst is responsible for thinking in context and ensuring that the policy-maker and the commander receive the best possible intelligence product. Open sources are not a substitute for classified sources--they are a contextual and encyclopedic foundation for thinking about the problem. Open sources are the means by which the all-source analyst extracts the greatest possible return from classified sources.

In the Age of Information, "intelligence" is defined less by whether it is classified or unclassified, and more by whether it is on time, on target, and useful to the consumer.

Chapter 3

INTERNATIONAL OPEN SOURCES AND SERVICES

3001. Purpose of the Chapter

The purpose of this chapter is to provide an orientation to international open sources and services which are available to the all-source analyst. Although much of the open source world is not yet easily accessible to analysts because of security and procurement constraints, the Commission on Intelligence report of 1 March 1996 has defined such access as "critical", and recommended that dramatically improved analyst access to open sources be a top priority for the Director of Central Intelligence and a top priority for funding.

This orientation will discuss electronic access, the identification and acquisition of "grey literature", the identification and exploitation of international experts, and several examples of world-class international open source capabilities including Jane's Information Group and SPOT Image Corporation.

Appendix D provides a concise directory (including complete contact information) for all international open sources & services discussed in this chapter. There are many, many more international sources available to the analyst which can be readily identified either through traditional library research, or through direct contact with international experts who can tell the analyst what sources they have found most useful for specific topics. The References are good starting points for additional direction.

3002. American Online Services

Most people unfamiliar with the world of open sources think of America Online and COMPUSERVE when they think of "online services".

In fact, "real" commercial online services, the kinds used by professional information brokers and specialists world-wide to do serious research, are completely different in nature and operation.

LEXIS-NEXIS and DIALOG are the two premier U.S. commercial online services. They each offer, for specific subscription and access fees, a wide range of electronic libraries. Access can be as cheap as $20 for a quick search, or $70-100 an hour for a complex search. It is best to work with an expert searcher to save money.

It is very important to understand that these two services are complementary and that searching one of them by themselves will not produce the best possible online search results. In the early 1990's a survey was conducted of all analysts in the Central Intelligence Agency, and each was asked to list journals of importance to them. The survey found that one fifth of the journals were available through LEXIS-NEXIS, one fifth through DIALOG, one fifth in

CD-ROM or electronic form, and two fifths were not available online.

American online services, although they have shown significant improvement in the past few years, are still primarily a source of English-language materials from the mainstream of the Western hemisphere, and specifically the United States and the United Kingdom.

America Online and COMPUSERVE are the equivalent of the corner drugstore when compared to the far more robust and extensive holdings of LEXIS-NEXIS and DIALOG "libraries". They do, however, offer very fine interfaces to the world of newsgroups as available on the Internet, and they also offer a number of organized conferences (such as the Military Forum in COMPUSERVE). Most people think of these services, available for around $25 a month, as cheap, but in fact that is only the basic access cost--once the per hour online charges are added, those who spend a lot of time browsing can find themselves spending $200 a month. Direct access to the Internet, including free NEWSNET services, is available for $20 a month from numerous services such as UUNET, Capital Area Internet Services, and DIGEX.

3003. Foreign Online Services

The world of foreign online services is more complex, and for the analyst concerned with international matters, often more rewarding. Unfortunately, these services are not routinely available to the U.S. intelligence analyst today. They are, with the increased emphasis on open sources brought about by the Commission on Intelligence, likely to be made available if requested by the analysts. Their fees are comparable to US services.

The Derwent World Patents Index (DWPA) is the most comprehensive database of inventions published worldwide. Every week more than 20,000 patent documents from 40 countries are processed into patent families, that is, groupings of patent documents from different countries covering the same invention. Each record has an English language abstract, is fully indexed, and is online. Selected technical drawings are included in the online holdings. Generally comprehensive coverage of all technology dates from 1974.

Questel/Orbit is an international online service specializing in patent, trademark, scientific, chemical, business, and news information. It was the first company world-wide to provide access to patent drawings online. Its holdings include materials from the European Patent Office, Japan Patent Information Organization, and the U.S. Patent Office. This service also focuses on international trademarks, and on scientific & technical research, breakthroughs, and products.

STN International, standing for (the Scientific and Technical Information Network) is an online search service providing direct access to over 190 scientific, technical, business, and patent databases. STN is operated jointly by the Japan Information Center of Science and Technology in Asia, by FIZ-Karlsruhe in Germany, and by CAS in North America.

GaleNet is the new online service from one of the most prominent and reliable publishers of international directories such as the *Encyclopedia of Associations*, the *Guide to Internet Databases*, the *Gale Directory of Databases*, and the *Research Centers and Services Directory*.

International Thomson Publishing does not offer its basic references online, but it does offer a free online search service which is useful, allowing simple searches by author, title, or other user-defined search criteria. Among the titles they publish are *Geographic Information Systems: A Guide to the Technology* (1991).

3004. Information Brokers

What is an information broker? The short answer is: the information broker is and can be an analyst's best friend. This is an individual who specializes in discovering, evaluating, and distilling information available from public sources, in order to answer a specific question from a customer. They generally charge between $70 and $120 an hour inclusive of search fees (they are expert at keeping the online cost down, but their offline expertise is valuable), plus between $15 and $60 for individual document delivery. Generally online searches identify the existence of specific documents, which must then be located in a library, copied, and faxed to the buyer.

Perhaps most importantly to the analyst, information brokers tend to specialize in specific scientific and technical, or industrial areas, and so over time they build up an in-depth knowledge of open sources and methods which can be of invaluable assistance to the analyst working a short-fused problem set. This is important: a good information broker can save the analysts days if not weeks of preliminary research.

The *Burwell World Directory of Information Brokers* is available in both hard and soft copy, and is indexed by subject matter as well as by foreign language expertise. Ordering information is provided in the hand-out.

Information brokers differ from all-source analysts in two important ways:

First, they specialize in discovering, evaluating, and distilling information for a client, but they do not conduct the kind of analysis and estimative forecasting that a typical intelligence community analyst is expected to perform; and

Second, they deal only with unclassified public sources which are legally and ethically available.

Having said that, there is much that analysts can learn from information brokers. Two books, for which complete ordering information is provided in Appendix D, are especially recommended:

Reva Basch, *Secrets of the Super Searchers: The Accumulated Wisdom of 23 of the World's Top Online Searchers*; and

Sue Rugge and Alfred Glossbrenner, *The Information Broker's Handbook*.

3005. Grey Literature

A major obstacle to U.S. understanding of foreign events, foreign cultures, and foreign plans and intentions is the fact that most of what is published about these foreign targets is in a foreign language and generally published in limited editions which are not readily identifiable, translatable, and reportable by existing U.S. intelligence capabilities.

"Grey Literature" is a growing field of interest, as experts worldwide begin to focus on the importance of "niche" information. Because grey literature is not "mainstream" and is often not electronic, the challenge of identifying and obtaining just the right piece of information requires the employment of expert intermediaries.

Examples of grey literature include trade show information, conference proceedings, unpublished "pre-prints" or works in progress, local area telephone directories, university yearbooks, and mailing lists for specific industries or countries.

Information brokers remain one of the best paths to grey literature because these information brokers specialize in selected areas and by virtue of their constant focus, are aware of new publications as they emerge, and are also in contact with key people in foreign industries and governments who can help them obtain selected materials not on the public market but still legally available in limited numbers. The *Burwell World Directory of Information Brokers* is unique for having an index identifying individual brokers based on their foreign language, foreign database, and foreign residence knowledge.

Professional associations, including U.S. associations, are a very rich source of leads and often will provide original source materials at no cost. At a minimum, professional associations can help analysts quickly identify authoritative individuals in specific countries who can be approached with a question or request.

Finally, international experts who are not information brokers and may not be associated with any professional association, are key players in linking analysts to exactly the right information. Two means of identifying such experts will be discussed momentarily.

3006. Document Acquisition

Before looking at international experts, it is useful to examine several services which specialize in document acquisition. The most prominent of these, with offices world-wide, is FIND/SVP, where SVP stands for the French-language phrase "if you please". FIND/SVP

has a major office in New York, and operates both a "quick find" service that will locate two or three relevant articles upon telephone request, and a more in-depth strategic research arm.

CISTI is the Canada Institute for Scientific and Technical Information; it provides world-wide scientific, technical, and medical information services, and also provides at no cost online, the CISTI Online Catalogue. One of the special features of CISTI is its collection of conference proceedings and serial reports.

Disclosure, Inc. has teamed up with American Business Information to provide access to high quality mailing lists and company financial and credit reports. Although publicly traded companies have the most information available, privately owned companies also have financial statements and credit reports, and primary research through industry experts (such as the editors of trade newsletters) can uncover more information. They also have a world-wide presence and can respond to document acquisition requests in their area of expertise.

Genuine Article is the document delivery service offered by the Institute of Scientific Information, which is unique for having a global citation analysis database in both science and social science. Citation analysis is a uniquely valuable analytical tool. The references tell the analyst who has cited or is cited by any major article in academic, scientific & technical, and international business literature. This allows the analyst to determine several things: taking a known relevant work, to determine who has done the latest work in this area, identifying them through their citation of the relevant work; taking a known author, rapidly establish the author's peer standing and influence through citations by others; or taking a specific area of inquiry, quickly cluster the different expert groups through their citations of one another.

Uncover Reveal is an online periodical article delivery service and a current awareness alerting service. It indexes nearly 17,000 English language periodicals in its database. There is no charge for searching the database; articles ordered can be delivered by fax, often within one hour.

3007. International Experts I

Analysts forced to rely on "umbrella" support contracts with a few specific intelligence industrial base companies will often find that these companies are simply one bureaucracy removed from the government, and do not have the flexible access to international experts that is needed.

One solution for analysts is to use in-house access to commercial online services such as LEXIS-NEXIS and DIALOG, to identify international experts.

In two different exercises, one on Somalia for the Marine Corps and one on Burundi for the Commission on Intelligence, LEXIS-NEXIS proved superb at identifying the top twenty-five journalists whose by-lines suggested they were expert on the country on which

they were reporting. Such individuals could be easily contacted for background information and insights on emerging trends. It is worth noting that journalists publish less than ten percent of what they know, and often have an understanding of personalities and motivations that they can share off-line but could never publish.

At the same time, using commercial online sources to search for quoted experts is a fast means of locating key individuals whose expertise has already been evaluated and is now relied on by journalists. Their knowledge will be different from that of the journalists.

Finally, since both LEXIS-NEXIS and DIALOG carry the transcripts of Cable News Network and other major international broadcast media such as the British Broadcasting Network, it is also possible to identify the "world-class" experts that are routinely called upon to comment on air.

3008. International Experts II

A second and deeper means of identifying experts is to work through the capabilities provided by the Institute of Scientific Information, and its unique proprietary publications and databases.

Both the *Social Science Citation Index* and the *Science Citation Index* were created to perform a unique service which is not available from any other source: they identify who has cited whom up to date (generally up to within three months). This allows an analyst to take a known work that is directly pertinent, and by examining who has quoted that work, to quickly identify those who are publishing in the field today.

Perhaps even more importantly, the Institute of Scientific Information is able to perform bibliometric analysis on all of this data, and cluster papers according to their influence. "Bibliometric" refers to the study of citation patterns and their meaning, rather than to content analysis. In effect, individual papers can be evaluated based on the degree to which they were considered relevant by others, and at the same time the relationships between different authors and schools of knowledge can be plotted using clustering techniques.

Finally, complete addresses and contact information are available for each author, enabling an analyst to quickly establish direct contact with an individual whose publications and peer citation establishes them as a high-value subject matter expert.

3009. International Directories

There are many international directories, but a few stand out. Ordering information for all of these are contained in Appendix D.

The *Encyclopedia of Associations* is a unique tool for it identifies key professionals in

every scientific and technical endeavor, and often permits direct contact with individuals who would otherwise be constrained by corporate non-disclosure terms.

The *Worldwide Directory of Government Officials*, updated frequently, is a comprehensive source for complete names, titles, telephone numbers, and even fax numbers for government officials from defense, intelligence, and all other government departments.

The *Research Centers Directory* and the *Directory of Publications and Broadcast Media* are examples of useful tools for getting in touch with key people.

A number of excellent references, all listed in the hand-out, are published by The Reference Press, Inc., and these include directories of key contacts in the various geographical regions of the world.

Finally, the International Supplement to The National Directory of Addresses and Telephone Numbers.

It merits comment that even without any directories at all, an analyst willing to use directory assistance, including international directory assistance, should ,in the space of four telephone calls, be able to identify somebody with knowledge useful to the problem at hand. An example: an analyst interested in environmental conditions in an area not covered by any directory, could call directory assistance in that country, ask for any listing beginning with the word "environment" in the local language, and within four telephone calls probably identify someone who is moderately familiar with exactly the information desired.

The bottom line: if you are persistent, the telephone really can help you reach out and touch someone.

3010. Jane's Information Group

Jane's Information Group has long been a primary source for many military intelligence analysts. In his thesis on *Open Source Intelligence: An Examination of Its Exploitation in the Defense Intelligence Community*, then Major (now LtCol) Robert M. Simmons found that many analysts relied on Jane's for tip-offs about new weapons developments and technology transfers.

Among the more obvious benefits from Jane's Information Group are its widely admired publications, *International Defense Review*, *Jane's Intelligence Review*, and of course its entire series of handbooks on different weapons and mobility systems, now available in both hard and soft copy, including a CD-ROM version with illustrations.

Less well known, but still popular, are the Sentinel Country Series, which very few people realize is based on the original analysis model developed by the Marine Corps Intelligence Activity in association with Marine Corps warfighters, and provided to Jane's as

an incentive to meet the demand for an unclassified country study. Jane's also publishes a series of extremely detailed reports on defense budgets world-wide.

Not-so-obvious capabilities which every analyst needs to understand are the following:

First, under special arrangements, the full range of information available through Jane's can be obtained online; this can include information on training and maintenance which has not been published and will not be published.

Second, Jane's can undertake special studies on demand, and utilize its special access as well as its in-house store of knowledge to produce useful "proprietary" reports which can serve as the foundation for follow-on all-source studies.

Finally, Jane's has a global network of experts who have spent years studying specific countries and are intimately familiar with specific defense personalities including field commanders. Under appropriate conditions, analysts can arrange to be put in touch with the pertinent Jane's expert, who can then become the analyst's "running buddy" for a specific analysis project.

3011. Oxford Analytica

Oxford Analytica, whose complete range of products is now available to the analyst through the Open Source Information System (OSIS), is believed by many to be the world's best private intelligence agency in the purest sense of the word.

Founded by an American, Dr. David Young, Oxford Analytica was inspired by Dr. Young's experience as the private secretary to Dr. Henry Kissinger when both served on the National Security Staff under President Richard Nixon.

The organization combines a fifteen person "watch team" which is organized by region and reads all the wires each day, with the Dons of Oxford who are rotated through a morning meeting each day, always asking three questions:

-- What's right in the news that needs to be expanded for our clients?

-- What's wrong in the news that needs to be correct for our clients?

-- What "weak signals" are emerging which require a forecast for our clients?

Upon concluding that a special report is required, Oxford Analytica then commissions either a resident Don from Oxford, or one of over 1,000 experts world-wide. In most cases, the experts have direct access to key decision makers and can obtain authoritative insights through a telephone call.

The final unique element of the Oxford Analytica program, strongly influenced by Dr. Young's experience in serving the President of the United States, is that no report is allowed to be over two pages long, and all reports are required to be complete within four hours of commission--as Oxford Analytica is proud of noting, their material is tailored "for Presidents, Prime Ministers, and you".

3012. Eastview Publications

Eastview Publications, a popular provider of services to the Foreign Broadcast Information Service, is representative of the kinds of niche providers that have emerged with the "information explosion" and the opening of formerly denied areas.

It is the foremost provider to the world of military maps from the former Soviet Union, and distinguished itself during the Commission on Intelligence benchmark exercise on open sources by providing, overnight, a listing of all Soviet maps available for Burundi--maps that did not exist in the U.S. inventory and could not have been created by the U.S. for days if not weeks.

Eastview Publications is also a premier source for Russian grey literature, and through its office in Moscow is able to respond to a wide variety of requirements.

Another example of private sector capabilities focused on Russia and Eastern Europe is that of Access International, based in Albuquerque, New Mexico. This organization, managed by Ms. Marjorie Hlava, a distinguished leader of many key U.S. information associations including the American Society for Information Science and the Association of Independent Information Professionals, produces a CD-ROM in both Russian and English on major Russian information sources including legal and technical sources.

In the scientific and technical arena, Information International Associates, closely associated with the Department of Energy Laboratories, the Defense Technical Information Center, and the National Technical Information Service, is one of the best access intermediaries for international information. Ms. Bonnie Carroll, its President, has been a leader in professional organizations such as the National Federation of Indexing and Abstracting Services and others.

The above are only a small sampling of the kinds of capabilities that can help the analyst exploit international sources. Many others exist--for instance, *THIRD WORLD RESOURCES* is a quarterly review of resources from and about the Third World. Ordering information is contained in the hand-out.

3013. SPOT Image Corporation

During the Gulf War, it took just over sixty days to collect the mapping, charting, & geodesy data that was required for both the targeting of precision munitions, and the creation

of 1:50,000 combat charts with contour lines. As U.S. forces are confronted with a variety of contingencies in the Third World--in areas which have not traditionally been high on the U.S. intelligence collection priority list--they are finding that the lack of maps is a critical encyclopedic intelligence shortfall.

Fortunately, the private sector is in a position to make a major contribution in this area. Ten meter imagery from the SPOT Image Corporation, for instance, can be both multi-spectral and panchromatic, and is suitable for creating both 1:50,000 combat charts with contour lines, and three-dimensional mission rehearsal programs. The Air Force also finds it adequate for the targeting of precision munitions.

What SPOT imagery cannot do is provide the "ground truth" precision points needed to ensure accuracy for combined arms operations, and especially for the coordination of artillery and air strikes. This precision is now provided by the National Reconnaissance Office, and can also be provided by human assets on the ground with Global Positioning Satellite Receivers--each SPOT image requires roughly eight precision points (e.g. a precise location for an intersection visible from space), and each country had from 60 to 200 wide area images which comprise its coverage.

The Defense Mapping Agency has made great strides in the past few years in recognizing the value of commercial imagery, and is now in a position to integrate 5 and 10 meter commercial imagery for broad areas, 1 meter imagery for urban detail, and NRO or GPS precision points.

It merits comment that SPOT imagery is the source for project EAGLE VISION, which combine real-time downlinks from SPOT satellites with mission rehearsal software. This project, sponsored by the Air Force Chief of Staff, was used in Aviano, Italy to prepare air crews for flights to Bosnia, and was credited with doubling sortie effectiveness. Commercial imagery is low-cost in comparison to national imagery. in large part because it has a much lower resolution (10 meters versus under 1 meter) and in part because it does not have the security costs associated with national imagery. A normal procurement for a wide area is on the order of $3,000 to $5,000; individual "snap-shots" can be had for as low as $450, and SPOT advertises sales of imagery at $1.50 a square mile.

3014. Universities

Universities, both U.S. and international, comprise a "virtual intelligence community" of great value to the intelligence analyst. Among their unique features are the fact that they focus exclusively on knowledge collection and processing, and that they do so at the expense of someone other than the U.S. taxpayer. University faculty, university student bodies, and university databases are all available to the intelligence analyst at either no cost, or at the nominal cost associated with access to an existing system.

Here are four examples of exceptional facilities of direct utility to intelligence analysts; contact information for each of them is provided in the hand-out:

-- Monterey Institute of International Studies. They have created and they continue to maintain a database on the proliferation of nuclear weapons, utilizing graduate students with native fluency in Russian, Chinese, Korean, Vietnamese, and other languages. They capability is so extraordinary that they have become the foundation for all-source enhancements within the Nonproliferation Center.

-- Mercyhurst College. This small college in Erie, Pennsylvania is unique because it offers the only program in the United States which grants an undergraduate degree in intelligence and research analysis. Founded and managed by Mr. Robert Heibel, a thirty-year veteran of the Federal Bureau of Investigation, this program requires its students to produce regular newsletters, relying only on open sources, about international narcotics, transnational crime, and other key issues. Students in this program are in very high demand as interns throughout the intelligence community.

-- University of Michigan. They operate a "clearinghouse for subject-oriented Internet resources", including resources for aerospace engineering and government sources of business and economic information.

-- Rice University. They operate an Economic Bulletin Board Service which provides a number of useful files including press releases from the U.S. Trade Representative, defense conversion information, East European trade leads, and so on.

3015. Knowledge Age

Knowledge Age, an intended pun, is intended to highlight the fact that knowledge gets old quickly, and to sensitize the analyst to the fact that there are degrees of currency in knowledge which can be very important.

Books are generally ten years old by the time they are published, and many of them started as graduate theses. Magazine articles were generally commissioned and researched ten months before being published. Even newspaper articles, all but the most sensational, were directed by editors and researched by reported up to ten days before publication. On the Internet, where time moves quickly, clips may be ten hours old.

The point here is that knowledge which has been published is old knowledge.

Where the analyst can get ahead of the curve, and develop insights not yet available to the general public, is by going after unpublished knowledge. By identifying and getting in touch with international experts, the analyst creates the opportunity to ask for tailored new knowledge which is based on unpublished "works in progress".

The analyst should also become sensitive to the existence of "barter networks", and knowledge networks, in which the elite in a particular area of inquiry routinely exchanges insights and information months if not years before publishing. The goal of the analyst should be to establish themselves as a member of this elite, and to use their own unclassified knowledge and their access to unique unclassified information collected at government expense, as their "membership fee" into this broader network of international experts who comprise the analyst's de facto "virtual intelligence community".

3016. Conclusion

There are no hard figures, and in any case the figures will vary from subject to subject and crisis to crisis, but informed judgement is fairly consistent on this point: 80% of what the analyst should know, in the ideal, is not in the USA, is not in English, and is not in electronic form.

The leveraging of international sources is essential for the analyst intent of obtaining a fresh perspective and good "tip-off" value. International open sources and services should be the foundation for a strong all-source analysis program.

Chapter 4

THE INTERNET AS A TOOL FOR ALL-SOURCE ANALYSIS

4001. Purpose of the Chapter

The purpose of this chapter, developed by Dr. Ross Stapleton-Grey, a former civilian intelligence analyst widely known for his Internet skills, is to present a very broad overview of the global capability known as "The Internet" or "the Net".

The Internet is a global communications medium that permits extraordinary flexibility in communicating with a wide variety of people from all walks of life, in receiving free information from many sources, some of dubious authenticity, and in obtaining access to distributed databases, many multi-media in nature, all over the world.

This chapter will discuss in general terms the utility of the Internet to the all-source analyst, with special attention to the use of electronic mail, newsgroups, lists, and conferencing systems.

We will discuss some of the dangers of the Internet, including the problems of noise and flame wars, as well as the almost total lack of privacy and discretion.

The last half of the chapter will focus on the most productive element of the Internet, the World Wide Web, and will provide five practical examples of how to exploit the Internet in support of the all-source analysis endeavor.

The Internet is a work in progress--it is changing every day at an astonishing rate. Some have characterized it as "the Library of Congress with all the books on the floor". It has its uses, but using it also has its limitations.

This course includes five hand-outs intended to facilitate self-study and hands-on exploration of the Internet's utility as one of the sources for information in support of the all-source analysis endeavor, as well as a source of continuing professional education for the intelligence analyst.

4002. Introduction: What Is the Internet?

The Internet is a "network of networks" based on standard protocols which have been established by common consensus among international experts. It is unique in that it is not controlled by any governmental body, and is a relatively autonomous, almost anarchistic, system that works because of its common standards.

It began in the 1970's as a Defense Advanced Research Projects Agency (DARPA) testbed to meet Department of Defense research needs and to develop internetworking

technology. It was divested in 1986 to other agencies in the U.S. government, notably the National Science Foundation, with participation from the Department of Energy and the National Aeronautics and Space Administration. The National Science Foundation initially funded regional and national back-bone service providers, and then switched its funding support to end users--this led to the development of commercial service providers. In 1994 U.S. government funding for the Internet ended.

Internet protocols (the standards which allow any computer to join "the Net" from anywhere in the world)won the competition as a general-purpose technology for constructing networks. It's not the most elegant system, and the Internet has a great many faults that other networking schemes avoid (it is still missing a lot of security features), but it is an open protocol, that is, the standards were developed in an open forum. It is now part of every commercial on-line service and computer company's planning because it has become the world's general-purpose digital information carrier.

Most people think of the Internet as a large electronic mail environment. This is its most common use. However, from an analysis point of view it is much more important in its capacity as a global network of distributed databases maintained at the expense of different universities, companies, and individuals. The Internet is an electronic library, with many public spaces and some private spaces.

Commercial services now include data maintenance, data discovery, and--the foundation for future exchanges of content--digital cash. Today, in the absence of wide spread digital cash capabilities, the Internet is largely a direct marketing network, but in the near future it could become the primary vehicle for organizing the exchange of goods and services. The Internet Society is a non profit activity that coordinates Internet standards, but it does not "control" the Internet.

4013. Where Are We Today?

The Internet is evolving from an academic luxury to a commercial necessity. Today, although the exact numbers are in dispute, we see at least 30 million individual users and over 40 thousand host networks which can be accessed via the Internet.

The Internet continues to grow at geometric rates. Local Internet access providers are finding that they can barely keep up with demand and service is often poor because of the speed with which large numbers of customers sign up daily.

The Internet was fairly closed to users outside government and the universities for much of its history. Big changes occurred when the National Science Foundation (NSF) took steps to turn it from an experimental, research effort, to a commercialized service. The NSF stopped funding networks, and started providing end users (such as schools) with funding to buy network services, establishing the first competitive markets for Internet services. Growth has been enormous ever since the NSF established regional networks (such as SURANET in

the Washington D.C. area) and especially since most of the restrictions (such as NSF's "Acceptable Use Policy" for its networks that required traffic be noncommercial research and academic in nature) were removed.

Today over 50% of the Internet sites are commercial in nature, with research organizations including universities comprising another 29%.

There is less "content" than one might expect. One authority, Dr. Joseph Markowitz, Director of the Community Open Source Program Office, notes in his primary briefing on open sources that "content" comprises just one percent of the Internet, with electronic mail, advertising, and other uses occupying 99% of that capability.

"The Internet is like the Library of Congress,
but with all the books strewn randomly on the floor."

This popular quotation, in several variations, has been around for years, but no one, including Dr. Vint Cerf, founder of the Internet and most recent President of The Internet Society, knows just who first thought of the analogy--but it is a good one!

4004. How Representative Is the Internet?

There are three ways to understand the character of the Internet.

In global political terms, it is dominated by the United States of America, which has more users, more hosts, and more bandwidth than the rest of the world taken together. Western Europe is a very weak second to the USA. The major online service providers, American OnLine and Compuserve, are U.S. companies with a global membership.

In most countries, only a relatively small number of prominent scientists or wealthy users are able to access the Internet, and many of them are restricted by local telecommunications limitations to a very low baud rate and a short access time. This represents the technical character of the Internet. In much of Africa, Asia, and Latin America, for instance, technical constraints are severe.

The Internet became a popular phenomenon around 1994, and exploded on the commercial markets in 1995. Online services all established connections to the Internet, so many of those users can be considered to be "on the Internet." However, it is very important for online service customers, such as those using America Online and Compuserve, to understand that the access they receive to the Internet from these services may be constrained-- Internet search tools such as Web Crawler will "see" only those Internet sites that have been registered by the managers of the online services. Analysts using the Internet need to understand what "hidden limits" might be placed on their searches and the search results by such constraints.

Examining the Internet at a personal level, the overwhelming majority of users around the globe, i.e. factoring in all countries, is comprised of research scientists. Within the USA, on the other hand, the largest group is individuals for whom the convenience and low cost of electronic mail and conferencing has become a major attraction. A third kind of user, the organizational user, is being provided with Internet access as a means of reducing organizational communications costs and increasing informal coordination among members of the organization.

4005. Lists: Versatile Low-Tech Tools

Electronic mail is the single most familiar tool on the Internet. Distribution lists are a first step beyond simple point-to-point E-mail. Analysts can quickly create their own individual "broadcast" groups that permit them to share information or ask questions of their counterparts world-wide.

Automated Lists, known as "Listservs" can be moderated or open. Such lists maintain a constantly changing directory of interested parties, and re-broadcast any messages sent to them to all current members of the list. Membership can be restricted, or open

Electronic mail is the lowest common denominator, since it can be used from virtually any platform (including dumb terminals) and doesn't need to be real-time. Usually one or more individuals interested in an issue or topic will create a distribution list as their set of correspondents grows beyond a few dozen. Some mailing lists may have thousands of subscribers.

Three examples of listservs of interest to the all source analyst are the Open Source List, maintained by the U.S. Army's 434th Military Intelligence Detachment (Strategic); the C4I List maintained by the Naval Postgraduate School, and the Information Warfare List, maintained by Dr. Fred Cohen, an international authority on information warfare who has served as a principal investigator for many defense and intelligence projects. Information on subscribing to all three lists is provided in Appendix E-2.

If you cannot find a list that meets your needs, consider starting your own--you could create one within the classified environment, and another within the open source environment. If you do not wish to be burdened with the maintenance, consider contracting this task out to a related center of excellence, such as a university with a strong program in your regional or functional area of interest.

A complete discussion of listservs and how to find and use them is provided as Appendix E-4.

4006. USENET and Its Newsgroups

USENET is a collection of thousands of newsgroups. Newsgroups are much like

E-mail distribution lists, focused on specific topics and with an emphasis on current events. Internet hosts pass each other USENET "feeds". USENET is not be confused with the larger Internet, something which happens frequently among new users.

USENET newsgroups are similar to bulletin boards, but require special newsreader programs to access the material. Instead of having mail arrive in the user's mailbox, the user accesses postings being held on a server, which is something like using a bulletin board system over a network.

Analysts contracting for an online service should note that in those instances where the basic membership only covers a few hours a month, and there are additional charges for any more time on line, it can become very expensive to do news reading online. One simple way to reduce costs is to utilize the "capture" feature in the communications software, and set for screen scrolling when entering the news area. This will allow for off-line reading as well as cutting and printing, and reduce online time to a minimum.

Here are three examples of pertinent newsgroups; a listing of typical headlines from each is contained at the end of Appendix E-1:

<soc.culture.kuwait>
<alt.current-events.bosnia>
<alt.politics.org.us>

Newsreader programs are generally provided by the same service through which you obtain access to the internet. They are all generally similar.

4007. Conferencing Systems

Conferencing systems are organized discussions, and are hosted on a server or servers which allow authorized participants, those who have password access to the system, to create conferences and within conferences, topics. All other users then have the option of reading entries, contributing their own entries, or "forgetting" the conference or topic by marking it as not being of interest.

Both Compuserve and America Online can be thought of as conferencing systems that "grew up;" when they first began members could only exchange information with other members, using both E-mail and public postings. As the Internet began to become an attractive resource, there was a great deal of pressure on the online systems to tie their services to the Internet, or risk loss of their members to ones that did. Some of the conferencing systems police their content, as Prodigy (to ensure that it's "family friendly") and America Online (which calls its rules its "terms of service") do. The online services do face some policy dilemmas, though: the Stratton Oakmont legal case ruled that because Prodigy censored some members' postings they could be held liable for not censoring libelous postings.

An examples of a Compuserve conference of possible interest is the Military Forum, which you reach--if you are a Compuserve subscriber, by typing "GO MILFORUM". Compuserve provides a number of other services of possible interest to analysts, including "GO MAGELLAN", where maps of current hot spots are available in GIF format, free, and other maps are available for a fee; "GO MAGDB", a large collection of journal articles; and "GO ENS", where ENS stands for Executive News Service, and permits you to establish a profile that selects articles of interest for your personal mailbox.

In the Whole Earth Electronic Link, possibly the most well-known and respected conference system ever built, topics 268 and 288 in the Whole Earth Review conference focus on open sources of intelligence and the reinvention of intelligence. Like most conference systems, monthly subscription fees are required to gain access.

4008. CAUTION: Some Problem Areas

Lists, newsgroups or conferences are contributed to and seen by hundreds to hundreds of thousands. The "noise to signal ratio" on the Internet is very high. If one subscribes to too many lists, or becomes too well known, they can be flooded with information. Although there are some sophisticated tools available today to help filter incoming information, one crude technique is to maintain several electronic identities, including an "unlisted" identity for personal friends. Another technique is to file everything. and then search for specific items of interest within this more limited (but still large) pool of information.

Another problem on the Net is that of "flames" and "flamers". Information on lists, USENET, conferences comes from broad communities of individuals. Although closely moderated lists may produce a high ratio of "wheat" to "chaff", many unmoderated discussions collapse under the weight of a few disruptive sources. "Flame wars" (harassing postings, name calling, and generally disruptive noise) are also common. Some contentious political and ethical discussions (such as on abortion, religion, race, etc.) are guaranteed "flame" generators. Analysts examining newsgroups and posting pertaining to the Middle East or the Balkan region are likely to find diverse and strong opinions, and have some difficulty sorting usable information from personal opinion.

It is important to understand that virtually anyone could be posting the materials found on the Internet, and that it will often be hard to ascertain the credibility of the source. Tools exist to explore "who is" a particular poster, and very good biographical information can often be obtained--as provided by the source themself.

Search tools and online services have their own limitations. Some Web search tools are best for thoroughness, others for new material, others for finding related information that does not have the actual key words. Searching the Net through an online service rather than a direct access provider will severely limit your results because online service providers impose censorship and access restrictions.

Everything about the Net is open for scrutiny by anonymous lurkers who can watch everything you post without revealing their presence, and in some cases arrange (illegally, or by abusing their authorized access as service providers) to monitor your private electronic mail. Internet users need to understand that there really is no such thing as private mail--an electronic message is forever, and might be seen by anyone!

4009. How On-Line Communities Form

It only takes two people to form an online community and share information. Word of mouth and existing personal relationships can quickly expand such communities. The practice of forwarding electronic mail to others is a very low-cost way of sharing information, and leads to widening communities. Broadcasting messages to lists of known interested parties also strengthens communities.

Users with common interests join (or create) lists and newsgroups. Their public postings are advertisements for communication, and users respond to each others' postings. Lists can be attract participants with very specific interests, e.g., C4I.

"Face to Face" communications are an essential aspect of online credibility and sustainability. At some point individuals will want to meet professionally, and this may strengthen or weaken the willingness to invest time online.

Given the face to face rapport, however, and a desire to share information, online communications quickly proves to be better than voice (you can send and forget electronic mail or have it cheaply translated enroute), it is cheaper than voice, and it provided an automatic record of exchanges.

Whether or not a professional and official email address is provided to the analyst, a personal email address through a commercial service provider is a good investment, both for personal communications with relatives and friends who are increasingly turning to the Internet as a primary communications channel, and for professional browsing in the open source world, where a great deal of information can be legally and ethically examined and downloaded without revealing your interest or your organizational affiliation. Analysts must ensure they follow approved procedures when integrating open source digital information into their all-source digital environment. The easiest and safest means is to keep external open source material in printed form, and to scan or keyboard pertinent passages. The alternative is to provide a diskette or send an electronic file to the authorized security point of transfer. Do not take chances with open source digital data!

4010. On-Line Communities, Virtual Contacts

The Internet community has literally exploded in the 1990's, and one can quickly find an online community for just about any topic. Not only are there

many, many pre-existing communities, but the conferencing systems spawn new ad hoc communities every day to deal with current events.

Such communities are a first step in identifying experts who can then be cultivated directly through "off line" personal electronic mail or more formal communications. An analyst can quickly build a "short list" of key people whose commentary can be observed and evaluated from a distance, as a "lurker", before ever introducing one's self. Networking informal sources to get a "head start" on an analysis issue is one of the best possible uses of the Internet. Remember, these communities of experts have spent decades of cumulative time becoming expert in specific areas, and they are usually going to be more familiar than the analyst with other experts and open sources of information about the topic or issue. They can provide a "first cut" that might otherwise take weeks of expensive library research.

There is an Internet culture, and there are standards of behavior. Although, as the New Yorker cartoon of two dogs dramatizes, "on the Internet, no one knows you are a dog", in fact first impressions matter and people will quickly form an opinion as to whether you are abusing their time, contributing to the discussion, or being stupid. Building trust on the Net takes patience, maturity, and a willingness to make constructive contributions to whatever discussions are important to you.

The Internet is today largely a barter or gift economy. At one meeting of international hackers, it was generally agreed that for every piece of information they each contributed to the Net, they generally got 100 pieces back, of which 10 were useful--hence a 10 to 1 noise ratio, but also a 10 to 1 return on investment.

Analysts who are cruising the Internet for information need to be aware of and comply with whatever official constraints may apply. If in doubt, don't post--just lurk and download, use the Internet as a cheap background briefing. The analyst also has the option of using the Internet, together with other traditional research tools such as the *Social Science Citation Index* and the *Science Citation Index* published by the Institute for Scientific Information, to identify possible direct contacts for official approval.

4011. Structuring Knowledge: Tools and Trends

Gopher was the first, popular tool for moving beyond lists and searching for information. The command, used at the prompt with the name of the site which must be known in advance, allows the analyst to access embedded menus and to select items to be downloaded. The Veronica search engine was created to search across a multitude of poorly documented Gopher sites. As gopher sites are now almost extinct, this is mentioned primarily as background.

WAIS was, until the World Wide Web, developed, the Rolls Royce of search engines, and for the first time provided a reliable means of both weighing the relevance of the found

files, and also of refining searches by commanding it to look for other documents "like" documents already in hand and found to be valuable.

Today, the two most popular tools are Netscape and the Web-Crawler. However, tools for the Internet are literally "exploding". Besides WebBrowser and the Microsoft Internet Explorer, the most impressive new tool, not yet widely used by the average individual, is Alta Vista, from Digital Equipment Corporation. Where the four programs return between 20 to 2000 "hits" on the name "Bill Gates", Alta Vista powers through the entire Internet and identifies 80,000 hits! Directions for using each of the above programs are found in the first student hand-out, together with other useful information for exploring the Web. Two of the hand-outs list specific sites of value to the intelligence analyst.

The Internet has always had an information organization problem, since very few people have ever been paid to create catalogs or indexes, there are few standards for online citations, and a great many documents and resources have just been dumped onto Internet sites with little regard for documenting their origin, validity, or even date of creation (much less expiration). Although commercial providers can be expected to offer value-added discovery and discrimination tools of increasing sophistication, it is difficult today to replicate a search, and most experienced navigators find that their best aid is a logbook in which they keep meticulous track of their wanderings in cyberspace. "Bookmarks" are citations of Web sites that a user can save, allowing them to find their way back later--the bookmarks are saved locally, and constitute a personal "map" of key terrain in cyberspace. Organize your hard drive and save the good stuff. Use your electronic mail program, such as PINE, to maintain electronic files with copies of messages from key contacts sorted by topic or area of expertise.

4012. The World Wide Web

The World Wide Web is a true multi-media environment which moves well beyond Gopher's linking of documents and sites, to allow true "hypertext" and "hyper-linking" of images to sounds, sounds to text, documents to other documents, and sites to other sites.

Readers can jump from the middle of a document to some supporting or related document, navigating the Web just like they might move through a library, pulling a reference volume off the shelf upon encountering an unfamiliar term. The Mosaic browser made the Web extremely easy to use, and the work that went into Mosaic was used to create the Netscape browser, which led to the creation of a billion dollar company.

The biggest problem with the Web today is that because it is multi-media, it is a band-width hog, and the demand for access is overwhelming most service providers. There will probably be a slow-down in the Internet in 1996, because a new performance plateau is achieved by the industry.

Users of the Web environment also require a special kind of Internet access, called SLIP, rather than the normal electronic mail and gopher text capability.

Appendix E-1 contains details instructions on how to explore the Web, and how to use different tools.

Here are four examples of useful Web sites. The first is a site dedicated to providing information about different countries; the second focuses on open sources and methods, and includes a full year of its newsletter; the third is a current news service focused strictly on the intelligence profession; and the last is the main access point to all federal government databases and bulletin boards that are accessible to the public.

<www.embassy.org>
<www.oss.net/oss>
<www.awpi.com:80/IntelWeb/>
<www.fedworld.gov>

4013. Where the Web Has Been, and Where It's Headed

The Web relies on Hypertext Markup Language (HTML), which in turn is an open and evolving document creation standard that will permit new applications to work on any standard document.

While running a Web site is technically demanding, many companies are now providing Web space (called a Home Page) for users, just like management companies buy and rent space in commercial buildings. Individuals have the option of hiring a "virtual" server" and obtaining their own domain name, such as "ANALYST.COM".

Security is an issue. Many Web servers do support secure connections, so a user can be sure that the information passing between his or her browser and the server is confidential important when passing credit card information, or other sensitive personal information. Password access can be complicated, so today most home pages and web servers are "wide open".

The next step will be for widely accepted commercial transaction standards to emerge; when this happens we're likely to see it happen quickly, just as point of sale (POS) devices (e.g., credit card swipe readers) have appeared at most retail stores. Digital cash, called by some "cyber-cash", is likely to be commonly available by 1997.

Popular Web sites attract thousands of users per day, and many include advertising graphics on their sites, being paid by the number of "hits" or "page views" they guarantee advertisers. Several companies provide auditing services to verify how much visibility sites provide advertisers.

The Web is likely to make virtual consulting by individual a real possibility, and permit many experts to establish part-time or full-time "cottage industries" selling their expertise to people all over the world in return for digital cash. This is like to cause a number of governments great concern, and may lead to a "virtual taxation" regime--the latter, will however, be very difficult to impose in a world where many encryption alternatives are available.

The professional analyst should think of the Web as a virtual collection environment, where Web sites can be established, and good content provided, as a means of drawing out expertise and collecting both fact and opinion about the topic in question.

4014. Finding Information on the Web

Like the earlier favorite Gopher, searching for things has led to the creation of special search sites. Some sites are important clearinghouses for links to other sites
Several very powerful full-text search sites have been established.

Four examples, each fully described in Appendix E-1, are listed here.

Yahoo:	<http://www.yahoo.com>
Alta Vista:	<http://altavista.digital.com>
InfoSeek:	<http://www.infoseek.com>
Open Text:	<http://www.opentext.com>

Analysts must naturally be concerned that any search they make might reveal a classified interest, but in reality, most analyst is responding to current events and the analyst can find security in obscurity. Everyone else is searching the same sites at the same time. As long as the analyst is searching and not posting, a very reasonable degree of discretion can be assumed.

The appendices corresponding to this chapter are your best guide to finding information on the Web, and contain a great deal of information which could not possibly be communicated in this short one-hour course.

Explore the Net, and keep a log-book. The Web discovery tools also provide "bookmark" features which allow you to keep a list of especially valuable sites to which you can return regularly.

4015. "Intranetting"

Many companies are concerned about security and create their own internal networks, hiding behind firewalls, which are ostensibly "total" breaks between the internal system and the external Internet.

Intranetting is an important consideration to note, because while such information won't be accessible to the public at large, sources and contacts met through the Internet may themselves have access. An analyst can thus obtain access in only two ways: by being an authorized internal user of the system in question, or by going through a personal intermediary, an authorized liaison, who can conduct internal searches and then transfer to the analyst the resulting data.

Examples of two intelligence community "intranets" are INTELINK and OSIS.

INTELINK is a classified Internet; that is, the Intelligence Community has built a secure copy of the Internet for sharing information, with the ease and efficiency enabled by use of World Wide Web servers and browsers, but in a classified setting. In this case, the "firewall" is an air gap, with no direct connections to the global unsecure parent.

OSIS, standing for "Open Source Information System", is a "virtual private network", where several intelligence agencies use the Internet itself for sharing unclassified information more easily, but software, in the form of firewalls and filters, keeps this traffic apart from the rest of the Internet.

Some of the best information available is hidden from the Internet in private intranet environments. This includes both university and corporate data. Analysts need to identify centers of excellence and then explore how they might obtain authorized access to the available data even if it is not directly accessible through the Internet.

The whole area of "intranetting" demonstrates the critical importance of personal networks--the analyst that identifies and cultivates a network of experts will find that the personal contacts can identify and gain access to data regardless of whether it would have been identified through an Internet search--and the Internet will often be the vehicle used for communicating with those experts, and receiving file transfers from them.

4016. Practical Example #1: Indications and Warning

In each of these four cases, information was quickly shared over the Internet, though in several of the cases the information was also traveling through more traditional means.

Researchers at a Swedish university have published a two-volume set of excerpts from network traffic around the Tiananmen Square incidents, including notes calling for protests at Chinese diplomatic facilities in the West, and information passed out of China via fax and phone (and carried by hand) and resent through E-mail. An analyst following Chinese newsgroups is very likely to have been alerted to these events prior to official reports from the U.S. Embassy or other collection capabilities.

Similarly, details of the situation in Moscow during the coup attempt against Gorbachev and Yeltsin were broadcast over the Internet (Yeltsin used a fax to get his statements to the Western press, however, and Gorbachev taped a statement about his detention using his VCR).

The Intel Pentium problem demonstrated the Internet's power as a consumer awareness channel: the bug that Intel considered minor (it only affected the work of serious mathematical processors) was blown up into a major public relations issue. It did however have significant financial ramifications for Intel stock. Similarly, other corporate or technical news can be studied for tip-offs.

Mathematicians have been using the Internet for the past several years to coordinate attacks on complex factoring and other problems, and their achievements have been widely announced via the Internet as solutions are found. On the other hand (and reminding us of the need for caution) the bogus "cold fusion" research was also spread via the Internet, attracting far more attention than it merited.

4017. Practical Example #2: Cultural Context

The Internet is a rich resource of information on distant countries and cultures. Because it's an open channel for information from virtually anyone with access to E-mail, it can become choked with both information and disinformation, but it's hard not to be able to find something on virtually any topic.

At the very end of your first hand-out you will find some extracted lists of messages and files pertaining to Kuwait, Bosnia, and the United Nations.

In combination, newsgroups, listservs, and web sites provide a rich background about current events and historical context. These passive sources of information--passive in the sense that you can "lurk", also permit analysts to rapidly identify articulate individuals to whom "off-line" questions can be posed, saving the analyst significant research time by providing a local perspective and a sense of a situation that would otherwise require hours of reading and might never result in the kind of insight that can be obtained from someone who is heavily involved in the issues under consideration.

4018. Practical Example #3: Basic Research

While the Internet covers a broad spectrum of exotic information, it's also a good repository for basic information.

Some of the first information resources were library card catalogs (catalog databases were simply connected up to allow searching via the Internet); any other product that could be placed on a disk or CD-ROM might also be placed on a Web host.

Appendix E-2 lists a wide variety of sites especially pertinent to intelligence analysts. Appendix E-3 focuses on popular web sites covering computer resources, news. government, and reference. Examples from both lists are shown here.

MILNET: Open Source Military Information Database
Military Intelligence: 20th Special Forces Group
CIA Country Reports
Department of State Country Reports
CNN Interactive
Reuters NewsMedia
Library of Congress
Britannica Online

4019. Practical Example #4: Science and Technology Collection

Virtually every area of interest can be found through the web and listservs. Every analyst with an S&T aspect to their work should consider searching for selected sites and also subscribing to selected listservs in their areas of interest.

Appendix E-2 lists a number of sites associated with weapons transfers and information warfare, some shown here.

High Energy Weapons Archive
Germ Warfare
Code Names and Numbers for Weapons
IW Database
Defense Information Systems Agency--Information Security
Computer Security Institute

Appendix E-3 lists a starting point for scientific and technical information, elements of which are shown here.

Biographical Information
Directory of Scientific Institutions
Electronic Journals

4020. Practical Example #5: Spotting and Assessment

The Internet is both open and public, and capable of allowing private communication. As users interact on mailing lists, newsgroups and conferences, they are seen (or read) by others. Estimates are that roughly 90% of the members of most conferences or newsgroups are "lurkers," that is, only read, and never contribute materials of their own. But a visible poster may attract private E-mail, volunteering information that the sender would like known, but wouldn't be comfortable posting directly.

You can often bait the hook, by offering (sincerely) to exchange information that you are authorized to share without violating copyrights. Sometimes your personal impressions as a professional analyst, and copies of articles that you have published in the unclassified literature, are enough to attract your counter-parts into dialogue.

Occasionally you may find yourself dealing with an electronic walk-in, someone who is volunteering information which appears credible and which may also be subjecting the individual in question to some risk if discovered. Such cases should be brought to the immediate attention of HUMINT and counterintelligence through established channels, not to give them up, but to ensure that the analyst has a full range of HUMINT and CI assistance in developing the source or--in some cases--turning over the source to a clandestine case officer.

Analysts who find names and backgrounds of interest always have the option of requesting security traces through channels. Working with HUMINT professionals can be a rewarding way of furthering any analyst's understanding of the network of human experts available to support the all-source project. Analysts can help the HUMINT discipline by identifying high-value targets for clandestine recruitment, and as the same time receive HUMINT assistance and cooperation in developing approved overt human sources, for whom funds can be budgeted.

4021. Second Caution: Mischief in Cyberspace

Because of the "faceless" nature of the Internet, it's possible to make mischief, from harassment to propaganda on a grand scale. "Astroturf" and "whisper campaigns" are where a few individuals (or even a single individual) can create numerous postings, attributed to a great many more people, in an effort to create a seeming consensus toward an issue or candidate.

"Spamming" occurs when an individual sends numerous and inappropriate postings to large audiences, through numerous mailing lists or newsgroups. This is at best annoying, and can, at worst, severely disrupt recipients' systems, choking their Internet connections or incurring significant costs if they have to pay by the volume of information received.

Because there are few if any restrictions on the collection of information from Internet search tools, and one should presume that, unless encryption is used, communications over the Internet can be at least noted, if not intercepted, one should be concerned about traffic analysis (on the other hand, if one owns a search tool site, one can readily gauge what issues Internet users find interesting!).

Trojan horses and viruses are malicious code that could be placed in resources made available on the Internet; while troublesome, they can be easily avoided by scanning any downloaded software, or limiting collection to text only. Analysts need to be aware that

icons are now also known to be active, and executable code can in fact be imported when importing "non-executable" data and graphics.

4022. Pulling It All Together

This one-hour introduction to the Internet as a tool for all-source analysis has provided you with an overview of various tools and sources you can find on the Internet.

Here we show a sequence of steps which an analyst can pursue to exploit the Internet in support of a specific project.

Step 1.	Search for Background
Step 2.	Identify Experts
Step 3.	Identify Lists and Newsgroups
Step 4.	Send Some Electronic Mail
Step 5.	Post Some Queries on Conferences
Step 6.	Establish a List or Web Site
Step 7.	Host a "Face to Face" Working Lunch
Step 8.	Contribute Unclassified Information
Step 9.	Develop Collaborative Relationships

An initial Web search can readily identify background documents. Together with a search of newsgroups and listservs, a number of experts commentators can be identified through their public postings.

Depending on the sensitivity of the query, the analyst can then take an active role by sending selected electronic mail or posting some general queries. Analysts should be mindful of Net protocols and the general expectation of the barter environment which characterizes the Internet--a sense of professional sharing and the expectation of exchanged favors.

At a more sophisticated level, analysts can work with appropriate infrastructure personnel to create a list or web site focused on their specific interests. This can serve as a magnet for individuals world-wide. In the early stages of the list or web site, it is useful to "salt" it with an introductory document that is deliberately loaded with "hot" words or keywords. Also, it is important to note that direct contact with the more popular clearinghouses can ensure that the site is properly listed and described.

Finally, the analyst can use the Internet to keep in touch with specific individuals, to coordinate face to face meetings, and generally to develop collaborative relationships with private sector peers eager to share unclassified information.

4023. Anticipating Coming Changes

Electronic commerce, as it arrives, will limit some formerly open resources (as people begin to charge what they'd had to previously give out for free) but will also help to fund efforts (such as cataloging) that are sorely needed, and will let others feel comfortable putting new resources online. As the volume of materials become such that most information needs can be met via the Internet (one-stop shopping) such catalogs and directories will become critical.

Since human searching is a chokepoint (there's only so much one person can scan through), we'll see tools for automating searches, or even turning them over to software "agents" to do the heavy lifting of browsing through hundreds or thousands of sites in search of relevant materials.

We've already seen some restrictions on Internet content, such as bans on "indecent" content. Some countries have much stricter restrictions on speech than the US, but the Internet, as a global system, will challenge attempts at censure. Access will continue to expand, especially to let travelers more easily access the Internet when away from home or office.

Some things, however, will NOT change. Analysts will continue to encounter a world of knowledge in which most of the information they really need is in hard-copy, is in a foreign language, and is somewhere else. In all these cases, it will be people who can help the analyst discover key data, discriminate between good and bad data, and distill masses of data into raw information which can then be considered by the analyst as part of the all-source intelligence process.

4024. Conclusion: A Work in Progress

Not only has the Internet changed dramatically over the last several years, the rate of change appears to be increasing. Commercialization is likely to cause further bends in the curve, as it will suddenly become possible for easy electronic sales of information, creating incentives both for companies to put resources online, and for others to create indexes and catalogs to those resources. Low cost global access and virtual conferencing are a rapidly approaching reality.

The Internet isn't the sum of all the world's information, but it is a good jumping off point, and grants easy access to potential sources and experts worldwide. It can also provide new avenues of access to traditional intelligence sources, e.g., as a spotting and assessment tool. It certainly allows activities that would have been impossible previously because of time and distance (such as convening a panel of experts on a fast-breaking topic), and will only improve in that regard as most potential participants in such activities get online themselves.

The analyst's access to both raw data and alternative perspectives is growing quickly because of the Internet; analysis will never be the same. However, the process of analysis has not changed--in evaluating the potential contributions of the Internet to the all-source analysis process, the analyst must remember security, remember source authentication, and remember completeness.

Chapter 5

OPEN SOURCES AND MILITARY CAPABILITIES

5001. Purpose of the Chapter

This chapter focuses on the practical application of open sources to military intelligence analysis requirements.

We will begin by introducing a model for integrated all-source analysis which illustrates the critical importance of geographic and civil factors in evaluating the threat at each of the levels of analysis. While open sources are useful in conducting research and developing intelligence estimates about military capabilities in isolation, open sources are most useful to the military intelligence analyst when used to develop a broader analytical model.

The general utility of open sources for military intelligence analysis, and the specific utility of open sources at the strategic, operational, tactical, and technical levels of analysis will be discussed.

Next we will look at specific private sector capabilities for collecting and processing open source information. Commercial imagery, private sector order of battle information, and networks of experts available for consultation will be reviewed in general terms.

Finally this chapter introduces the student to the Expeditionary Factors study developed by the Marine Corps Intelligence Activity, and used for this class because it is the only current and authoritative intelligence analysis product which relies exclusively on open sources, is unclassified in its final form, and covers a broad range of mission area factors for eighty countries specifically chosen because of the likelihood that a Marine Air Ground Task Force will be engaged in non-combatant or combatant missions in the countries

There are three Appendices associated with this chapter--Appendix A, which was introduced in Chapter 1, and Appendices F-1 and F-2.

5002. Model for Integrated All-Source Analysis

The four levels of analysis first popularized and thoroughly explained by Edward N. Luttwak in his book, *STRATEGY: The Logic of War and Peace* (Belknap, 1987), are most easily understood with an illustration. The Marine Corps Intelligence Center expanded this model by distinguishing between military, geographic, and civil factors. The third hand-out is a complete description of the model, including a summary illustration on page v.

When the model was first developed, a specific Middle Eastern country was used by the Marine Corps, in consultation with DIA, CIA, and NSA analysts responsible for that

country. to test assumptions. Their tank warfare capability. traditionally assessed as a high threat. proved on examination through the four levels of analysis, to be a high threat only at the technical level, because the country had an inventory of T-72 tanks, the best tanks that money could buy at the time. At the tactical level of analysis, the threat dropped to low because the tanks were not being maintained, in fact were being cannibalized for parts, and the troops were not trained. At the operational level, the tank threat increased to medium because there were a significant number of tanks available around the country. Finally, at the strategic level of analysis,the tank threat again dropped to low because it was not possible for the country to sustain tank operations for very long.

This analytical model becomes even more useful when we introduce the three analysis domains--military, geographic, and civil--and consider how the three domains interact at each level of analysis. At the strategic level, military sustainability, geographic location, and civil allies are the essential elements of employable power. At the operational level, military availability. geographic resources, and civil instability bear on the regional influence of the target country. At the tactical level, military reliability, geographic terrain, and civil psychology come together to determine battlefield dynamics. Finally, at the technical level, military lethality (and accuracy), geographic atmosphere--specifically temperature--and civil infrastructure including communications and computing systems, help determine the balance of power.

In short, the threat varies depending on the level of analysis. Open sources provide both raw information, and a general context, for this more complex form of analysis.

5003. General Utility of OSINT

There are three major ways in which open sources are very useful to the defense intelligence analyst:

First, open sources are very quickly and cheaply available, and even when the full weight of the traditional classified capabilities are being brought to bear, will offer the analyst--and the supported policy maker or commander--a rapid orientation useful for planning purposes.

For example, in one case where U.S. forces were being directed to deploy quickly to a remote area of Turkey, it was an open source reference which quickly identified the nearest airfields and their runway, navigation, and bunkerage capabilities.

In many cases, open sources may be the only available source for a significant period of time. As military operations other than war, and unanticipated contingencies, tend to occur in Third World countries that are Tier 3 or Tier 4 in terms of standing intelligence priorities, it will often be the case that the military intelligence analyst and the operating forces will be forced to rely exclusively on commercial imagery, private sector news broadcasts, and direct contact with overt human experts, in order to produce intelligence.

The second area where open sources have a significant value is with respect to collection management. By providing a rapid and inexpensive orientation, a "first cut" on what is known and what is not known, open sources has enable the analyst to develop a collection management strategy which avoids wasting precious classified resources of essential elements of information which can be handled by open sources, and which focuses the clandestine and technical capabilities on "the hard stuff".

Finally, open sources are very helpful when conducting joint or coalition operations, including support to law enforcement, where there are constraints on the sharing of classified intelligence, and it is considered prudent to avoid sharing sensitive intelligence and the means by which the intelligence was obtained.

5004. Strategic Intelligence

At the strategic level, military sustainability, geographic location, and civil allies are critical elements of national power. Much of the information needed at this level is in fact available through open sources.

In the indications & warning arena, open sources can--through the technique of content analysis and comparisons of content over time--provide very reliable gauges of national intent. In fact, the Office of Strategic Services and its original Research & Analysis Branch made the analysis of open sources an art form--by studying what the German leaders were telling their own people through the public media, the OSS was able to develop estimative intelligence.

Open sources are also critical in two areas traditionally not within the normal scope of classified systems--demographic intelligence and cultural intelligence. Today, as organizations such as the U.S. Information Agency begin to apply intelligence methods to open sources, and adopt a collection and reporting role in these areas (as was recently recommended to their oversight body, the U.S. Commission on Public Diplomacy--the analyst may find that one of their most important sources for partially analyzed open source information is the traditional consumer of intelligence.

Strategic generalizations are not yet a well developed aspect of national intelligence support to acquisition, but as the concluding chapters will demonstrate, a potentially important means of money and improving system performance. To take just one example: if aircraft are built to a standard "warm" day, and the "real world" of contingencies is in fact a "hot" world, then by definition our forces will be using aviation resources which can fly half as far and carry half as much as advertised when operating at the "optimal" temperature. When European truck manufacturers adopt a strict policy of never selling a vehicle weighing over thirty tons to a Third World county, the viability of some of our heavier ground combat vehicles must be called into question.

At the strategic level open sources are helpful in understanding the context for security assistance programs, and in developing support for specific programs from the public, the press, and the policy community.

5005. Operational Intelligence

At the operational level, military availability, geographic resources, and civil instability influence the regional effectiveness of individual countries.

It is very helpful for an analyst to develop regional generalizations, to establish an understanding of order of battle averages, and of geographic and civil constraints characteristic of the region. Third World operations are inherently different from the European theater operations against a Soviet threat for which most U.S. mobility and weapons systems were designed--the analyst that understand both the limitations of our own systems in the Third World, and the possible advantages which accrue to those fighting on their home ground with equipment designed for their home ground, will probably produce more useful intelligence products.

Open sources are especially valuable to the theater commander and those supporting the theater and its Joint Intelligence Center because most contingencies will not warrant major collection campaigns from classified sources. This is true both in the planning phrase, and in the execution phase when it is necessary to coordinate logistics and other matters with joint and coalition partners. At the operational level, where the greatest mixture of allied and U.S. services is to be found, and there is a greater involvement of civilian agencies from both the U.S. and other countries, secrecy can be an impediment to understanding and consensus, and open sources can have a corresponding simplicity which increases cooperation and improves coordination.

As the theater staff plans the allocation of resources, a sound understanding of the region and the capabilities of all parties to the operation, largely gathered through open sources, can help determine what should be left on the pier, what additional capabilities are needed from the national level, and what to expect or request for allies.

5006. Tactical Intelligence

At the tactical level, military reliability, geographic terrain, and civil psychology are essential determinants of battlefield success.

At this level, where combined arms coordination at the 1:50,000 scale is essential to the art of maneuver and the control of precision munitions, commercial imagery is often the only available source which can be brought to bear. National collection capabilities are not well-suited for wide area surveillance, they were designed for point targets, and will naturally be much in demand for the development of target intelligence.

Commercial imagery, notably SPOT imagery at the 10 meter level of resolution (meaning you can see an object ten meters wide on the ground), is not only fully suitable for the creation of 1:50,000 combat charts with contour lines, but has also proven to be more than acceptable to the U.S. Air Force as the foundation for targeting precision munitions, and as the source for digital elevation data used to create sophisticated simulations for mission rehearsals and other needs.

It is important to note that commercial imagery requires the addition of "ground truth" points to orient the image and establish precise geo-spacial accuracy. Such precision is obtainable in two ways: through the integration of precision points (e.g. key intersections) obtained from the National Reconnaissance Office through the Defense Mapping Agency, or through Global Positioning Satellite (GPS) recordings taken by human assets actually on the ground.

Open sources are very useful in emerging target areas which have not been heavily covered by classified capabilities. The Director of the Non-Proliferation Center, for instance, has stated publicly as much as 80% of his final intelligence products are based on open sources; in counter-narcotics operations, open sources--including investigative journalism in Latin American newspapers--has proven to be accurate and comprehensive....so much so that the U.S. Southern Command enlisted the Department of Energy laboratories (Los Alamos and Sandia) to collect and process open source information from Latin America, with the result that tactical interdiction operations were mounted. This story is told in *SHARING THE SECRETS: Open Source Intelligence and the War on Drugs.*

5007. Technical Intelligence

At the technical level, military lethality (including accuracy), geographic atmosphere, and civil infrastructure are important determinants of battlefield success.

As was discovered during the Gulf War, open sources are the best and often the only source of information needed to "map" the target area's C4I infrastructure, and develop information warfare operations.

Open sources are also the backbone for planning logistics operations and mobility systems, since information about airheads, ports, rail and road networks, and related support systems are all a matter of public record. There is however, an aspect of the open source world that is not obvious at first: much of what is counted as "open" source is in fact grey literature, limited edition literature in a foreign language. Collecting and processing open source information is not necessarily easy!

Finally, open sources are the foundation for long-term intelligence efforts against scientific and weapons research. Unclassified civilian research, and publications by civilians employed in defense-related industries, have long been a critical foundation for intelligence in support of major acquisition programs. In fact, one tip-off for intelligence analysts is the

disappearance from a literature of a particular expert, or a particular line of inquiry.

5008. Commercial Imagery for 1:50,000 Maps

A ten meter image from SPOT Image Corporation can be processed to integrate both the standard military grid lines, and the contour lines that most people do not realize is achievable from SPOT panchromatic coverage.

It is especially important for analysts to understand that this commercial system has been in operation for over a decade, and that virtually the entire world has been imaged, with most images being less than five years old and in ground station archives--this imagery is available within 24 hours.

Source imagery is not enough by itself, as was mentioned earlier. Additional processing is required to establish elevation points and precision points, and additional time is needed to produce the 1:50,000 combat charts necessary for combined arms operations and especially infantry patrolling....but the source imagery, traditionally the stumbling block when attempting to use national systems to obtain wide area coverage in a crisis, is no longer the obstacle to producing maps.

By combining SPOT wide area coverage with NRO precision points, under the management of the Defense Mapping Agency, we can have 1:50,000 maps right now.

5009. Commercial Imagery for Mission Rehearsal

The same commercial imagery that is used to produce 1:50,000 combat charts can also produce superb three-dimensional simulations and perspectives that can be used to study beach approaches, potential landing zones, and nape of the earth flight corridors.

5010. Order of Battle Information

The former Soviet Union and the People's Republic of China are probably the only two countries where the U.S. intelligence community could state with certainty that it possessed more accurate information about the order of battle than was available from open sources. Perhaps this is even true of other denied areas such as North Korea and Cuba.

Yet when it comes to virtually any other country, the information collected and processed by Jane's Information Group, publisher of the Jane's series of books and CD-ROMS which cover all types of mobility and weapons systems, is the world standard. In fact, in a graduate thesis by (then) Major Robert M. Simmons, titled "Open Source Intelligence: An Examination of Its Exploitation in the Defense Intelligence Community", our own military intelligence analysts are quoted as saying "reference publications such as Jane's often provide first indications of weapons modifications and sales" (page 112).

The Jane's series of references books and CD-ROMS is now also available online by special subscription, and the material is kept current by a global network of overt human assets as well as extraordinarily good relations between Jane's and most Ministries of Defense. Analysts need to know that as good as the Jane's publications are, only 20% of the information known to Jane's is actually made public. "Confidential" reports on training, morale, and other issues can be obtained by special arrangement.

Jane's is also helpful in understanding the order of battle for non-traditional information. Jane's has provided orders of battle for the warring clans in Somalia, and is considering providing a similar service with respect to transnational criminal organizations.

Another private sector service that can be helpful to analysts attempting to understand Third World or non-traditional orders of battle (e.g. of revolutionary groups) is offered by Rapport Research & Analysis, representative of a small number of elite organizations, most with Special Air Service or similar backgrounds, who specialize in making available highly trained interrogator-translators who are able to canvass refugee and exile communities to identify sources and then systematically develop the needed information as well as leads to in-country sources of potential value.

5011. Historical and Estimative Analysis

In the age of distributed information, the concept of "central intelligence" is difficult to implement, and even unnecessary. While a central coordinating authority, and bodies of trained analysts with clearances, are both needed, there is now a very robust "virtual intelligence community" which can be harnessed to develop significant amounts of historical and estimative analysis based solely on open sources.

Oxford Analytica, a U.S. owned company based in Oxford, England, is the best private intelligence agency in the world, and its excellence is based strictly on analysis. Founded by Mr. David Young, who worked with Dr. Henry Kissinger when the latter was National Security Advisor to the President, Oxford Analytica specializes in producing daily regional reports which concisely address three questions: what's right in the news that needs elaboration? what's wrong in the news that needs correction? and what weak signals are we seeing that merit scrutiny and an estimate?

This organization covers the world. For Somalia, to take one example, over a period of two years they produced over twenty two page reports on UN operations in Somalia, US foreign policy toward Somalia, and US operations in Somalia.

How does this "best in class" organization work? They start by having a fifteen person team, organized by region and function, review all news wires and major periodicals on a day to day basis. They then bring in the Dons of Oxford in small groups rotated regularly, and draw on the expertise resident at Oxford University—in effect they have harnessed the centuries of accumulated experience, and integrated that experience into their

daily operations. Then, when special reports are desired, they have a global network of 1,000 experts, culled down from 2,500, to whom they can turn at any time with a request for a two-page report which integrates personal calls to key decision-makers, and is drafted at a level suitable for a President, Prime Minister....or you, the analyst preparing intelligence products for policy-makers and commanders.

5012. Networks of Experts

The most significant difference between elementary and advanced analysis is that the first draws primarily on published information, and the second draws primarily on direct contact with world class experts.

Most published information is out of date by the time it is published. In addition, the intelligence community, which specializes in secrets, is not trained, equipped, and organized to collect open source materials. The result, well documented in the thesis by Major Simmons cited earlier, is that analysts have very limited access to the broad capabilities in the private sector. Advanced analysis requires recourse to a network of expert colleagues in the private sector who can serve as a collection filter, and quickly identify key documents, comment authoritatively on emerging trends, and generally help the advanced analyst to fully exploit open sources, while also adding the unique value that is inherent in all-source analysis.

LEXIS-NEXIS and DIALOG, the two major online news services, are recommended to analysts not for the massive volume of printed information they can provide, but for something far more subtle: the identification of journalists and sources who--through their by-lines or their being cited, might aid the analyst in leap-frogging over old published information and into the future.

Complementing the online services is the Institute of Scientific Information, and its two major publications, the *Social Science Citation Index* and the *Science Citation Index*. These are unique databases, available both in hardcopy and online, because they allow the analyst to take an older work known to be relevant, and to quickly identify, right up to the current week, who has cited the older work. In essence, the analyst can quickly reach the most current and authoritative experts on any topic through this capability, with the added advantage that frequency of citation conveys a sense of peer evaluation.

Professional associations and associations of retired military personnel are mentioned simply to highlight the fact that the entire world is full of knowledgeable people, most of whom would be happy to respond to questions. Finding the right person and asking the right question is becoming more important than "keeping up with traffic".

5013. Expeditionary Factors Study

The *Expeditionary Factors* study sponsored by the Marine Corps Intelligence Activity and carried out by PRC under contract, is a second generation effort, and current as of 1994. It is a showcase for OSINT, as it is the only high-level intelligence community product that relies exclusively on open sources, and is published in an unclassified form (For Official Use Only).

The first generation study was completed in 1990, and was called *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World*. Copies of the original analysis model, and of the strategic generalizations chapter from the original study (this chapter was inadvertently overlooked in the follow-on study and thus was not updated), are included as hand-outs.

The other unique aspect of the Marine Corps study was its focus on countries which the Marine Corps felt has the "highest probability" of requiring entry by U.S. forces, rather than on the traditional "worst case" priorities focus. The original list of countries, approved by the Marine Corps flag officer community, was comprised of 69 countries. The current list includes 80 countries, almost all of them in the Third World.

The Marine Corps approach, besides focusing on open sources and an unclassified product, was also unique in that warfighters--operators--were asked to define low, medium, and high degrees of difficulty for each mission area, and this was then converted into a five point scale that can be graphically depicted.

This three-volume hard-copy set, also available on CD-ROM, is an excellent ready reference for planning, and is available. To obtain ordering information, call or fax the numbers shown here.

5014. Strategic Generalizations

Having introduced the *Expeditionary Factors* study, we now turn to some of the strategic generalizations which emerged from its predecessor and remain constant today.

The expeditionary environment is complex and lethal. Experienced infantry, modern armor, sophisticated artillery, night/all weather aviation, and integrated air defense systems are all too often characteristic of the "Third World".

The "cultural terrain" is steep, with 40 of the original 69 countries speaking Arabic or a primary language other than English, French, or Spanish, and most practicing Islam or an eastern or trivial religion.

The aviation temperature is uniformly hot, with a sustained heat index of over 80 degrees, which automatically reduces both lift and range of aviation platforms significantly.

There is an equal mix of mountains, deserts, jungle, and urban terrain. We must be ready for all four. Cross-country mobility was non-existent in 60% of the countries and severely constrained in another 20%. When combined with an average bridge loading capability of no more than 30 tons (not in the study but well-known as the civilian limit for truck weight), this suggests real difficulty for existing concepts of ground maneuver.

Average line of sight distance was under 1,000 meters, with only eight of the 69 countries offering stand-off engagement ranges of over 2,000 meters. In the absence of carrier aviation, the Navy's standard guns are no match for the coastal artillery and missiles of many of these countries.

There were no 1:50,000 maps for 22 of the countries, and old maps for ports and capital cities only of another 37 of the countries.

Finally, between half the countries having no usable ports, and most capital cities with their Embassies being beyond the round-trip range of a CH-46 flying from the five fathom line, Non-Combatant Evacuation Operations presented real challenges.

5015. Commission on Intelligence

Open sources are gradually being accepted as an important part of the all-source production process, but there are still many obstacles to its full integration into national and defense intelligence.

The Commission on Intelligence, popularly known as the Aspin or Brown Commission, was created by Congress to thoroughly evaluate the U.S. intelligence community. One of the closed hearings held by the Commission, on 3 August 1996, addressed open sources. Among the four individuals testifying were the National Security Advisor to the President, Dr. Anthony Lake and the founder of OPEN SOURCE SOLUTIONS, Inc., Mr. Robert Steele.

At the end of the session, a Thursday afternoon, General Lew Allen, USAF (Ret), challenged Mr. Steele to join in a benchmark exercise testing private sector capabilities against those of the entire Intelligence Community. Burundi was chosen as the target, and a deadline was set for 1000 the following Monday.

The Commission was surprised by the results. In short order, they received order of battle information on tribes from Jane's Information Group; strategic commentary from Oxford Analytica; a list of available Russian maps down to the 1:250,000 level from Eastview Publications; a list of authoritative journalists from LEXIS-NEXIS; and a list of expert academics and others from the Institute of Scientific Information. Later, not part of the initial response, it was determined that SPOT imagery was available for all of Burundi and could be used to produce 1:50,000 combat charts and mission simulation programs.

As a direct result of this benchmark exercise, the Commission included in its final report an extraordinarily detailed and strong statement on the importance of open sources. The Commission noted that OSINT has limitations, but went on to state that the Intelligence Community has been "inexplicably slow" to provide analysts with access to open sources; that the Commission views such access as "critical" to the all-source analysis process; and that the Commission believes that open source access should be a top priority for the Director of Central Intelligence and a top priority for funding.

5016. Conclusion

Commercial imagery is a useful example of how open sources can support and enhance national intelligence capabilities:

-- 10 meter commercial imagery provides cheap and fast wide-area coverage, and has the added advantage that most of the world has already been overflown and generally cloud-free imagery are already stored in the ground stations;

-- 1 meter commercial imagery--if U.S. policy and a lack of funding does not derail private sector efforts to create this new capability--can provide urban detail and a closer focus on key targets while avoiding an order of magnitude increase in the cost of maps which would accompany any attempt to use 1 meter for the whole world (not to mention the delay in collection); and finally

-- Classified imagery from the National Reconnaissance Office can provide the eight precision points per wide-area image that are necessary to create a 1:50,000 map to our standards of accuracy for combined arms operation.

The Defense Mapping Agency, or the new National Imagery and Mapping Agency, are ideally placed to manage a truly national program in which private sector open sources and classified Intelligence Community capabilities are fully integrated. This is the ultimate value of open source intelligence--as an integral part of the all-source solution.

What should we conclude from all this? First, it is clear that experts and data reside in the private sector, outside the intelligence community, which are vital to understanding and which should be harnessed in support of the all-source intelligence process. Second, these resources represent a potential source of savings to the U.S. taxpayer, since they are maintained at no cost to the taxpayer, are constantly validated by their survival in the marketplace, and--if properly exploited--permit the expensive classified capabilities to be applies more effectively to "the hard stuff". Open sources provide orientation and context. They do not provide the complete answer in most cases, but rather make the other intelligence disciplines more effective.

Chapter 6

OPEN SOURCES AND OPERATIONAL SECURITY--THE DARK SIDE

6001. Purpose of the Chapter

This chapter was developed by Mr. Richard Horowitz, a licensed private investigator and security consultant based in New York. Mr. Horowitz has served in the Israel Defense Forces, attaining the rank of Captain, and is now studying law in New York City.

This chapter is grounded on the premise that everything needed for the planning and execution of criminal or terrorist activity can be found in open sources. Indeed, an entire industry exists which is devoted to the publication of such material. In addition, equipment designed for one purpose and legally available can be used in terrorist or criminal activity.

The total cost of the publications and equipment presented in this "dark side" chapter is available for approximately $1,800. The chapter is based on the "seeing is believing" principle. Each of the items discussed in this chapter can be ordered by using the complete ordering information containing in Appendix G.

From both a military and a law enforcement point of view, it is critical to understand that even our most poorly-funded and least organized opponents can gain access to relatively sophisticated intelligence collection tools as well as tools of destruction.

This chapter--like all other chapters in this handbook--is unclassified. The key point to emphasize is that everything presented is publicly and legally available. Books on intelligence collection, killing methods, offshore money laundering, and any other aspect of criminal operations can be purchased by calling an (800) number and using a credit card. We must all be aware of how such information might be exploited when acquired by persons seeking to harm or take advantage of others, and specifically, to harm members of the MAGTF in garrison or ashore.

6002. General Considerations

It is a fact of life that society contains those who are morally deviant, socially misguided, or worse. It is of similar importance that our society is based on certain freedoms which cannot be taken away. The combination of the two can results in terrorism and crime as we know it today. Underlying the activities of these individuals and groups is a culture which includes recruitment, indoctrination, education, training, planning, preparation, and execution.

This chapter is not a training manual, though many techniques and methods can be recognized from professional government training. The objective is to create an awareness regarding the availability of open sources for terrorist and criminal activity.

Four general considerations are offered as an introduction to this model:

1) The availability of the open sources to criminals and terrorists, and the extent to which such capabilities exist, does not document a threat *per se*. Each individual command and each individual operation must carry out a threat analysis unique to their circumstances.

2) Everything we discuss in this chapter is available to anyhody anywhere. This includes Colombian drug smugglers, Los Angeles gang members, Korean contract employees on a U.S. Army base overseas, and individual "crazies" seeking media attention by causing deaths or damage aboard U.S. military installations.

3) Information that has been available for years in published form is now available through the Internet. Bomb designs are popular in cyberspace. Periodic press reports tell of teenagers injuring themselves trying to construct a bomb they have read about on the Internet. While this problem will arguably increase, it should not obfuscate the reality that the industry which produces the material in hard copy has existed for many years.

4) Although "high-tech" threats attract more media attention, the reality is that low-tech capabilities are often just as effective, cheaper, and easier to develop. A federal officer can be attacked by a doberman with its vocal cords cut out--a low-tech but very effective means of perimeter security. The bomb used to destroy the Federal Building in Oklahoma City was not a complex construction--it was a simple mix in a large amount.

6003. Open Sources and Radio Interception

Intelligence acquisition, or information gathering, is a crucial first step in planning and executing an operation. The next six slides are devoted to various methods of information gathering: electronic monitoring, operational activity, and computer databases.

This split slide shows frequencies for Air Force One on the left, taken from a book by a California hobbyist which is devoted to monitoring the President. Entitled "Monitoring Air Force One," the volume discusses and lists frequencies of the Mystic Star, Echo/Foxtrot, and FM-FDM-SSB systems, along with identified Secret Service code names.

On the right is the cover of a book published in 1986, entitled *Guide to Embassy and Espionage Communications*, which listed thousands of frequencies transmitted from 55 countries, the International Red Cross, Interpol, and the United Nations.

The extent to which frequencies of federal and state agencies that are intercepted and published presents a security problem is not within the scope of this chapter. The range of equipment and information commercially available indicates a problematic potential or at the very least, can be an incentive for subversive groups to attempt to intercept government transmissions.

Commercially available radio scanners can intercept UHF, VHF, and military bands; some have uninterrupted frequency ranges from 30 MHz to 1.2 GHz and are available in desk top or portable versions. Current law requires manufacturers to block cellular telephone frequencies.

Frequency counters-devices that intercept radio transmissions and display their frequencies on a read-out-are also commercially available.

Monitoring Times runs a column which publishes frequencies used by federal agencies that were intercepted by hobbyists. These agencies include the F.B.I., Secret Service, U.S. Customs, and numerous military agencies. After the World Trade Center bombing, the magazine carried an article listing frequencies used by various Port Authority units, the FAA, and local "press disaster" frequencies. Guides to U.S. and allied official frequencies are readily available worldwide--if a hobbyist can track you, so can a criminal!

6004. Open Sources and Telephone Interception

It is illegal to monitor cellular phone conversations (868-896 MHz). Prior to April 1994 however, radio scanners capable of intercepting these frequencies were legally manufactured and sold. Scanners that blocked cellular frequencies were constructed such that they could be easily modified to intercept cellular transmissions.

Scanners manufactured before April 1994 can still be legally owned or sold. Hence, many scanners capable of intercepting cellular calls are accessible and in use.

Some methods of scanner modification:

-- A Massachusetts company advertises that for $40, they will "unlock" your scanner

-- Journals print schematic diagrams showing how to modify the scanner's circuitry;

-- While the new law prohibits the manufacture of frequency converters- a device that will convert 400 MHz interceptions to 800 Mhz interceptions, many are accessible.

-- For those with technical skills- a cellular phone, which needless to say operates on cellular frequencies, can be modified to intercept other cellular calls.

A book entitled *Tune In On Telephone Calls*, listed in your second hand-out, enumerates frequencies and channels used in various types of telephonic transmissions. Its various chapters cover such operational relevant areas as military aircraft VIP phone calls, satellite phone calls, coastal maritime calls, and cellular calls.

In addition to voice and data interception, there is a commercially available device called a tone decoder which converts the frequencies of a touch-tone dialing system to

numbers and displays them on a read-out, in effect allowing easy identification of those being called by the intercepted telephone, as well as read-out of any other information being transmitted through the touch-tone signals, such as codes and account numbers.

Internationally, for instance from Switzerland, more sophisticated equipment is available, and we should assume that surplus or illicitly obtained military equipment is also available to individuals to whom good intercepts are critically important.

6005. Open Sources and Eavesdropping

Numerous books are in print detailing how to tap a phone or bug a room. Some are quite technical. A manual originally published by the U.S. Department of Justice entitled *Electronic Eavesdropping Techniques and Equipment* has been republished under a different title by a commercial publisher, and is listed in your second hand-out. Please note that "old" techniques can be very effective, especially if there is very little emphasis on operational security against civilian opponents!

In April, 1995, U.S. customs officials raided 40 spy shops in 24 cities that were illegally selling eavesdropping equipment smuggled into the United States from two Japanese companies; 11 people were charged with crimes a result. Termed "electronic surreptitious interception device," among the equipment smuggled into the United States and sold by these shops:

-- telephone transmitters with a range of 400 meters

-- bugging transmitters with a range of 1,000 meters

-- ball-point pen transmitters with a range of 200 meters

-- A/C line transmitters-attached to the line, behind the wall outlet and permanently operates on its current-with a range of 200 meters.

From documents filed in court by the U.S. Government, from October 1993 through February 1995 a total of 161 shipments of 4,367 eavesdropping devices took place. The devises had an estimated retail value of $2,972,517.

Companies also publish electronic plans enabling an individual to assemble his own equipment. These schematic diagrams include automobile tracking transmitters, bugging transmitters, telephone transmitters, a transmitter locator, and audio amplifiers.

Bottom line: assume your are "on the air" unless certain the circumstances are secure!

6006. Open Sources and Undercover Operations

Undercover operations is a term used to describe various types of activities designed so that the fact they are taking place is not recognized, or, if recognized, not for what it really is. The general purpose of undercover operations is generally either to affect a change on a target or to gather information about a target.

Manuals for private investigators, as well as training manuals for law enforcement from various countries have made virtually all aspects of undercover operations a matter of public record. There are manuals on undercover operations in general, on developing clandestine human networks, on surveillance, on lockpicking, and even on elicitation and pretext calls, a very common technique for obtaining information.

Books are in print containing prepared scripts for obtaining personal and financial information from people. One book opens with a chapter entitled "Establishing Rapport and Overcoming Objections." Complete citations are in your second hand-out.

This slide shows two illustrations, one from a manual on surveillance techniques, the other from a manual on lockpicking. Complete citations for both are listed in your second hand-out.

Lockpicking tools are legally sold; prices can start from about $25. The law does not criminalize possession of lockpicking tools unless the person possessing the tools "evinces an intent" to use them for burglary. To quote the New York State law:
"A person is guilty of possession of burglar's tools when he possesses any tool, instrument, or other article adapted, designed or commonly used for committing or facilitating offenses involving forcible entry into premises...under circumstances evincing an intent to use or knowledge that some person intends to use the same in the commission of an offense of such character."

It merits comment that with the limited number of known aerial and maritime surveillance platforms that the U.S. Coast Guard has to patrol the drug routes from Latin America to the United States, it would be an easy matter for drug criminals to establish both passive observation posts near airfields and ports, and also active aerial and maritime surveillance capabilities. In brief then, criminals and terrorists who understand the value of intelligence collection, can easily establish significant capabilities which can frustrate official government programs.

6007. Open Sources and Interrogations

Criminals and terrorists have access to professional training and professional interrogators. Even the most reputable firms, such as E2G and Rapport Research in the United Kingdom, both staffed by highly trained former Special Air Service (SAS)

interrogator-translators, will be happy to offer training and perhaps even surveillance and other services to those who come to them with cash and an appropriate cover story.

In the United States, the "Soldier of Fortune" circuit includes many training and exercise schools where useful knowledge can be learned.

This slide listed selected chapter headings from two books readily available on the open market, one on psychological interrogation techniques, the other on physical interrogation techniques.

As transnational crime becomes a greater threat to national security, and the military become more involved in support to law enforcement operations, it merits comment that operational security and "need to know" are just as important in this environment as in any other.

Indeed, one of the distinguishing aspects of transnational criminal operations are their ruthlessness, and the ease with which they can select and coerce civilians to help them on a one-time basis by threatening to kill their loved ones–how many Pacific Coast fisherman do you suppose would refuse to carry one load of drugs if they were assured that it would only be a one-time risk, and that their loved ones were being held under surveillance and would be killed if the fisherman did not cooperate?

6008. Open Sources and Direct Research

Previous chapters have dealt with the rich range of open sources, and how to develop intelligence from open sources, including international sources and the Internet. The point to emphasize is that terrorists and criminals have access to everything in the open source world described by this handbook.

Major criminal and terrorist organizations are fully cognizant of the utility of open sources, and know how to do their homework. They know the power of computerized search & retrieval, and the value of information in support of their operational objectives.

For the purposes we are discussing, the computerized databases which can be accessed by anyone in the public, including criminals and terrorists, can be divided into the following three broad categories:

– Media: available are not only *The New York Times*, *Washington Post*, and *Wall Street Journal*, but numerous local newspapers such as *The Rocky Mountain News* (Denver, CO), *The Commercial Appeal* (Memphis, TN), and *The Times-Picayune* (New Orleans, LA), and foreign newspapers such as *Le Monde*, *The Irish Times*, and *The Prague Post*. Wire services- UPI, AP, Reuters, and the Xinhua News Agency (China), for example, are also accessible.

-- Business and public records: corporate and bankruptcy filings, SEC filings. property ownership, criminal background checks, driver's licenses. Financial news. Companies combine mailing lists of hundreds of marketing companies, resulting in a database which can identify the address of a person or family, or their neighbors. Reverse phone directory-enter name, retrieve a person's phone number, or enter a phone number and retrieve the name of the person.

-- Specialized trade and industry information: databases exist that specialize in information unique to a particular industry or country, generally in the form of periodic newsletters, and are a valuable source of information. This slide lists some of the sources of possible use to criminals planning electronic thefts or money laundering operations, and terrorists planning specific acts.

A classic example of the basic utility of research: on 3 May 1993 a complete report was carried online about the meeting of the Nuclear Regulatory Commission, entitled: "Commission Hears Options for Dealing with Vehicle Bomb Threats". Discussed in detail online: the four options regarding physical barriers surrounding nuclear power plants.

6009. Open Sources and Executions

This slide is a combination of extracts from two books, one on killing and one on creating silencers.

Literature on killings and executions are graphic and the methods described are real. A six volume work entitled "How To Kill" is representative. Volume One begins with "Chapter One: The Target," complete with an anatomy chart highlighting sensitive parts of the body. Subsequent chapters are devoted to various types of killings. Appendices entitled "The Signs of Death," "Your First," and "A List of Poisons" follow the chapters.

A separate body of literature exists on the use of knives. One book has the topical heading of "anatomical considerations" followed by diagrams entitled bleeders, immobilizers, quick kill, showing the respective spots on the body. The book ends with an appendix entitled "Suggestions for Further Study."

Books describing how to construct silencers from household material exist. Attaching a slightly filled plastic soda bottle or a container of three tennis balls to the barrel of a gun are crude methods. More technical methods requiring metals are detailed. In a chapter entitled "Your Last Chance To Be Legal," one book discusses the various federal forms that need be filed in order to request to manufacture a silencer.

Manuals on improvised weapons show how to install a gun or firing mechanism in, for example, an umbrella, belt buckle, flashlight, briefcase, cigarette lighter, or tobacco pipe.

The same publisher selling books on how to kill supplies a book on how to dispose of dead bodies, including a technique on removing a bullet from a body without leaving evidence.

Full citations to all the books cited in this chapter are contained in Appendix G.

6010. Open Sources and Explosives

This slide is also a combination of several diagrams to illustrate the nature of the information that is available in open sources about creating and using explosives.

Improvised explosives, and bomb design, are topics with the most published literature. Numerous books in a "cook book" form describe how to mix readily available chemicals into explosives. Mixing soap flakes with gasoline so as to allow the gasoline to stick to its target instead of dripping off before igniting is discussed in a book and in a video on making explosives.

Separate books exist on how to make C4 and Semtex.

While these books generally have a disclaimer that the information contained therein is for educational purposes only, a book entitled "Professional Standards for Preparing, Handling, and Using Explosives" is available from the publisher.

From a catalogue:

DEATHTRAP! The Video: There is no better way to learn about improvised explosive booby traps used by international terrorists than to watch live, on-camera demonstrations of their construction, deployment and detonation. DEATHTRAP! The Video is a chilling seminar in just that - how terrorists modify innocent everyday items to conceal insidious explosive booby traps designed for maximum shock and lethality. You'll see ingeniously disguised devices made out of books, music cassettes, mugs, portable tape players, foot powder cans, alarm clocks, videocassettes, mousetraps, and more, all triggered by simple electrical, chemical, or mechanical means.

The video costs $29.95 and runs for 35 minutes.

A wide variety of related books are also available, for instance on bridge demolition.

6011. Open Sources and Radio Detonation of Bombs

Apart from simple explosives, it merits comment that sophisticated devices for detonating explosives from a distance are readily available to criminals and terrorists.

Bombs can be detonated by remote control, through radio detonation. The chip needed for production of the detonating tone retails under $20.00.

A book entitled *Improvised Radio Detonation Techniques* describes how to modify various types of radio equipment into detonation transmitters. This slide lists devices afforded a chapter in the book, along with relevant information regarding their modification.

In March, 1994, this book was among numerous other books found in a storage locker of a man suspected in the package bomb that killed five people in upstate New York. In a similar incident, on February 10, 1995, the Associated Press released a report of a high school student's locker booby-trapped with a set of firecrackers wired to a circuit board and capable of being detonated by radio control.

Radio detonation, including that of car bombs, is a major problem worldwide:

-- In May 1992, the Mafia killed Judge Giovanni Falcone and three bodyguards with a car bomb detonated by remote control while they were driving along a Sicilian highway.

-- A March 1994 article in the Current Digest of the Soviet Press entitled "Who's Getting Killed In Moscow, and How" cited the problem of remote control detonation.

-- In January 1995, a group that manufactured radio detonated bombs was arrested in St. Petersburg. Constructed for $60 and sold for $1,500, the bombs came with a six month guarantee.

According to the Intelligence Newsletter of March 16, 1995, Egypt spent $18 million in 1994 on equipment to detect car bombs and to jam their detonation frequencies.

6012. Open Sources and Vehicular Enhancements

Evasion is a significant concern after executing an operation. There are a number of enhancements that can be made to vehicles, enhancements which can increase chances of evasion if detected and pursued. Some possible enhancements are listed in this slide.

There is a thriving small industry specializing in the production of armored cars for civilians. Publications such as *The ROBB Report* routinely advertise all manner of armored vehicles for sale--vehicles which to all outward appearances, are simply a normal car.

In addition to enhancements to the individual vehicle, skill at evasive driving is crucial in case operatives are detected. One manual on evasive driving illustrates evasive techniques on city or country roads, and in chase situations, along with automobile security modifications such as an oil slick or smoke screen generator. In case the driver does not successfully evade the pursuer, techniques for knocking the pursuer off the road are described. The manual has a chapter entitled "Suggested Training Schedule."

This is a good point in the chapter to emphasize that criminals and terrorists are very aware of the fact that they pursue very high-risk, high-gain occupations, and have a great deal to gain from proper preparation. Their preparations are all the more difficult to deal with because by definition they are camouflaged as civilians and do not wear uniforms or follow any recognized rules of engagement. Establishing their technical capabilities and their "order of battle" thus calls for entirely different collection methodologies.

6013. Open Sources and Tactical Communications Jamming

Military forces rely heavily on command & control, and on combined arms operations. Military patrols in support of law enforcement operations are relying on artillery and other forms of reinforcement as they venture out "on point". It therefore becomes important to understand that criminals and terrorists are capable of executing tactical communications jamming operations.

Although radio jamming is illegal, *Improvised Radio Jamming Techniques* is a technical book describing the construction of a jamming station, allowing an operative to jam radio transmissions of government agencies as part of an operation or during the evasion stages.

Chapters in the book include:

-- Intercept Equipment Selection
-- Covert Antenna Systems
-- Intercept Operations
-- Police Radio Operational Procedures
-- High-Risk Frequency Detection Techniques
-- Jamming Equipment Deployment
-- Operational Security

6014. Open Sources and Bank Card Forgery

Central to criminal and terrorist operational security is the creation of a new identity, or a variety of identities that frustrate the efforts of law enforcement officials to track their international and domestic movements. The methods of creating a new identity in various books range from obtaining a new public image to physically disappearing and altering one's identity. Some books on creating a new identity focus on obtaining public records under a new name. Chapters are devoted to social security cards, driver's license, credit cards, and bank statements.

Other books exist on how to produce counterfeit identification documents. One book contains chapters such as The Forger's Kit, Forgery Techniques, and Quality Control, and discusses the "False Identification Crime Control Act of 1982" which prohibits selling fake I.D. by mail. The book continues: "It's still possible for the forger to buy the various

materials needed to produce fake I.D." and provides names and address and several companies.

A separate book exists devoted to counterfeiting currency. Chapters include "Basic Printing Techniques Used in Counterfeiting," " Purchasing Equipment and Supplies," and "Passing Counterfeit Currency."

Worldwide contacts, and world-wide mail drops, area readily available to criminals and terrorists. Companies publish booklets listing lawyers, bankers, and accountants in numerous countries ready to take a call from someone in need, together with lists of thousands of companies providing voice, fax, and correspondence forwarding services.

These are the traditional methods. Today, "cyber-theft", and direct anonymous access to bank accounts, as well as the complete concealment of international financial transactions through encryption and anonymous remailers, is becoming the major foundation for global criminal activity. One good reference is *Electronic Fund Transfer Systems Fraud*, published by Paladin Press (ISBN 0-87364-490-5).

6015. Open Sources and "Legal" Offshore Passports

Companies will, for a fee, arrange a legal passport and citizenship for their client, from a country not the person's country of birth.

Below is the fee scale from a company based in Amsterdam which specializes in passports and citizenship from Latin American and Caribbean countries--a legal citizenship with can be obtained within 90 days of submitting the company's application.

Dominican Republic	$19,500 for 1-4 individual orders
Venezuela	$21,900 for 1-4 individual orders
Panama	$20,900 for 1-4 individual orders
Ecuador	$23,900 for 1-4 individual orders

The application requests information such as the applicant's name, date and country of birth, height, eye color, visible scars, existing citizenship, profession, and mother's maiden name.

Along with the application, one need submit:

-- the signature and photo page of the applicant's current passport
-- copy of a birth certificate
-- three color negatives in three different sets of clothing
-- affidavit of good conduct from a licensed attorney or local police clearance
-- six thumbprints
-- six signatures on a white sheet of paper

-- a personal character reference or bank reference

The company's material explains that one need not visit his new country but can remain a "citizen living abroad," and contains a chart indicating countries that can be entered without a visa with your new passport.

The company can arrange a diplomatic passports "to some," for a fee of $55,000.

A midwest American company offers "genuine" passports and driver's licenses from countries that no longer exist, such as Burma, Rhodesia, Dutch Guiana, and the Republic of Zanzibar. The company portrays these passports as "emergency passports," in case terrorists hijack a plane and the American traveller would not want to identify himself as such. The application requires only a name and credit card number.

A U.S. Government "Passport Agent's Manual" has been acquired and republished by a commercial publisher. The manual is a useful guide for avoiding obvious mistakes.

6016. Open Sources and Offshore Corporations

In addition to arranging second passports and citizenship, companies exist that will establish shell companies for their client, generally offshore.

One British company specializes in establishing companies in the Bahamas, Belize, the British Virgin Islands, Delaware, Gibraltar, and Panama. The company's promotional material contains a chapter on each country, reviewing the requirements regarding:

-- capital and shares
-- directors and shareholders
-- meetings
-- accounting
-- corporate seals
-- company name
-- registered agent, office, and domicile

The application form requests only the name of the company to be established, the names and nationalities of the shareholders and directors, the objective of the company, and the applicant's name and address.

A Hong Kong company will also form a company in numerous localities around the world, from the Cayman Islands in the Caribbean to the Isle of Man located in the Irish Sea. The company's specialty however is Hong Kong "shelf companies"- corporations ready for purchase.

The Hong Kong company provides a list of over one hundred shelf companies incorporated in Hong Kong. Company names were chosen, apparently with the intent of attracting American buyers. These shelf companies were incorporated in 1993-94, allowing the company's purchaser to give the impression that the company had been in business years before the purchaser took control.

The application form requests only the names, business occupations, nationalities, and passport numbers of the company's officers and directors, along with information on the purchaser's bank account. For the client's benefit, the Hong Kong company includes educational material on how to arrange letters of credit through the client's new offshore company.

6017. Open Sources and Choosing a Criminal Specialty

Similar to books on individual methods and techniques, books are available on crime as a profession. For example, a book entitled *Drug Smuggling* contains information on how to find a drug source, what type of airplane is suitable for smuggling, and how to launder money. It closes with a discussion on dealing with law enforcement and a chart detailing federal and state drug laws, shown in this slide.

A book entitled *Successful Armed Robbery* written by an inmate in a federal penitentiary, contains the following chapter headings:

-- The Selection Process
-- Strategic Production-Planning
-- Factors Affecting Your Success
-- Self-Caused Failure

This book contains diagrams of various types of parking lots and illustrations on how to approach and assault the driver of a car.

Hit Man; A Technical Manual for Independent Contractors covers the entire range of activity for the planning and execution of a contract murder. Topics range from surveilling the target to psychological approaches to the job. From a chapter entitled "Finding Employment, What To Charge, Who To Avoid": "Prices vary according to risk involved, social or political prominence of the victim, difficulty of the assignment, and other factors. A federal judge recently brought the price of $250,000, according to one example provided. A county sheriff might bring $75,000 to $100,000."

A related book entitled *How To Hide Anything* is available to criminals and terrorists. It contains numerous diagrams illustrating the construction of hiding compartments for objects or people an indoor and outdoor settings, and can be used to create hiding places for contraband, documentation of illegal exchanges, and special illegal technical equipment.

The list goes on. There is a market in information about how to be a criminal or terrorist, and there are established concepts, doctrines, and information about organization, methods, and equipment which is readily available world-wide.

6018. Conclusion: The Dark Side of Open Sources

This chapter has reviewed the open source knowledge available to criminals and terrorists which, when properly utilized, can make the military mission and the mission of law enforcement more difficult.

In particular, this chapter has sought to emphasize that operational security and the "need to know" are important aspects of success against a well-trained and well-equipped criminal or terrorist organization which understands the value of intelligence collection.

Criminals and terrorists can intercept radio and telephone conversations; they can exploit eavesdropping devices and execute tactical signal intelligence collection operations. They know how to conduct undercover operations, how to interrogate captured prisoners, and how to do direct research using open sources.

Individuals can be effective at executions and in the use of explosives. Radio detonation of explosives through a variety of remote devices is easily understood and readily carried out.

In the escape and evasion phase, criminals and terrorists can exploit armored vehicles equipped with oil slick and other devices for delaying pursuit, and can also execute tactical jamming operations which may allow them cut off and surround their military or law enforcement pursuer before back-up forces can be mobilized.

In conducting transnational criminal and terrorist activities, these individuals can avail themselves of false credit cards, new identities including legal passports possibly obtained through false supporting documentation, and related corporate and letter of credit documentation.

Over all, this chapter has sought to communicate the degree to which information about various criminal professions is available in the open source world, allowing for knowledge about how to conduct many different kinds of crimes and illegal activities to pass from one generation of criminals to another.

Criminals and terrorists can think and read--open sources are as useful to them as they are to intelligence professionals and the operational commanders they support.

Chapter 7

CONCLUSION: COLLECTING AND PROCESSING OPEN SOURCE

7001. Purpose of the Chapter

This final chapter wraps up the handbook by providing information about three official U.S. government channels for obtaining open source intelligence: the Community Open Source Program Office and its global Open Source Information System; the Defense Intelligence Agency Open Source Program and the (planned) Defense Intelligence Agency Open Source Intelligence Center; and--especially important for Marines--the Marine Corps Intelligence Activity and the Expeditionary Factors Study. The Chapter concludes with a brief discussion of the usefulness of the Marine Corps Reserve as a source of existing and new open source exploitation experts, and some recommendations on additional open source training opportunities.

7002. Community Open Source Program Office

The Community Open Source Program Office (COSPO) was established effective 1 March 1994 by DCID 2/12, which superceeded the earlier establishment on 1 June 1992 of the Open Source Coordinator. The requirement for an Open Source Coordinator first emerged in 1992 as a result of the findings of the Open Source Task Force, one of eleven task forces that Congress required the Director of Central Intelligence to establish as part of his confirmation process. Although all elements of the Intelligence Community have used External Research & Analysis (ER&A) funds to contract for academic and technical research, and the Foreign Broadcast Information Service (FBIS) of the Central Intelligence Agency has been responsible for monitoring foreign print media as well as radio and television broadcasts, the task force concluded that a focal point would be helpful to the DCI.

According to DCID 2/12, "The COSPO is responsible for the definition and defense of the Open Source Program in the planning cycle, and for providing guidance and oversight to the program in the execution cycle. The Office, with Community departmental open source program managers, develops an optimum allocation of resources across the Community in the execution year, subject to ratification by the Open Source Steering Committee. ... the objectives of COSPO are to:

a. Oversee a process for coordinating responsive actions to satisfy user needs.

b. Provide advocacy and defense of departmental development and operational efforts.

c. Ensure funds for critical open source activities.

d. Oversee a process for identifying and prioritizing open source substantive requirements."

COSPO functions include strategic planning, program formulation and representation, initiative and innovation sponsorship, operational services of common concern, systems architecture, development of services of common concern, and open source advocacy and representation.

Speaking publicly to the annual international conference on open source intelligence, in 1995 Dr. Joseph Markowitz, the Director of COSPO, stated that roughly 40% of the all-source product funded within the National Foreign Intelligence Program comes from open sources, at a cost to the program of only 1% of the total budget. Experts generally agree that the percentage of the open source contribution will vary from zero to 100 percent depending on the problem, and than an average of 40-60% is readily certifiable. Somewhat unexpectedly, open source receives great credit against terrorism and proliferation, and is said to account for as much as 80% of the all source product in those two reporting areas.

7003. Open Source Information System

The Open Source Information System (OSIS) is the principal means by which COSPO is seeking to enhance analyst access to open sources. However, as it is limited at this time to information available in electronic form, it must be regarded as a very positive but only partial solution.

OSIS is an electronic network which provides both access to and sharing of unclassified U.S. Government and other open source information about Intelligence Community (IC) agencies and selected other organizations with similar information requirements.

OSIS is being installed at the various Joint Intelligence Centers, and should one day be accessible to any Marine Corps intelligence professional afloat or ashore. Examples of the information available in OSIS include:

-- Jane's Electronic Library of 24 titles providing up-to-date information on military equipment, weapon systems, and defense products worldwide

-- IC ROSE, a database service providing fulltext articles from hundreds of periodicals on a wide range of subjects

-- FBIS products online, including the Daily Reports, S&T Perspectives, Trends, and Pacific Rim Economic Review

-- Oxford Analytica Regional Daily Reports (Strategic Political and Economic Intelligence)

-- DTED, the Defense Mapping Agency's online Digital Terrain Elevation Data map collection providing worldwide coverage

-- CIRC, a database of over ten million titles on scientific and technical topics, including patents, standards, military equipment, and systems

-- a Conference Database of upcoming symposia, congresses, conventions, etcetera, in the areas of science, technology, engineering, politics, and economics

-- Unclassified library holdings of several OSIS member agencies including DIA

OSIS also offers specialized tools, such as the National Air Intelligence Center's SYSTRAN machine translation capabilities to support real time translations of non-English language information located on World Wide Web sites.

7004. Defense Intelligence Agency Open Source Program

The Program Manager for Open Source Intelligence within the Defense Intelligence Agency is Ms. Alice Cranor, whose contact information is provided here. She serves as the DIA representative to the Open Source Council, which is the advisory body formed to support the Community Open Source Program Office (COSPO). Each agency and service has a single representative to the Council. In addition to an agency-level focal point, every branch within DIA has an OSINT focal point.

Ms. Cranor, whose office code is PO1-3, can be reached by voice at (202) 373-4005, via facsimile at (202) 373-8971, or via email at <AFcraat@dia.osis.gov>.

MAGTF OSINT requirements should be discussed with the appropriate DIA Branch OSINT focal point to ensure that existing DIA capabilities for accessing OSINT on that topic are not overlooked.

7005. Defense Intelligence Agency Open Source Intelligence Center

As of August 1996, a new initiative is under discussion, to create a DIA OSINT Center funded at $10 million a year, and consisting of an EAGLE VISION ground station (to receive commercial imagery directly from commercial satellites), close to $3 million a year to buy commercial imagery not obtainable through Defense Mapping Agency funding, and $4 million a year to fund roughly 4,000 man-days of individual international expert support for the entire defense intelligence community. Although not yet approved, this initiative has been favorably discussed by the Director of DIA with Congressional staff, and funding is anticipated. MAGTFs should be developing their open source requirements and submitting them through appropriate channels to ensure that a fair share of these resources are devoted to expeditionary intelligence requirements.

7006. Marine Corps Intelligence Activity

The Marine Corps Intelligence Activity (MCIA) has from its inception understood and valued open source intelligence. Today the primary expression of Marine Corps emphasis on the value of open source is the Expeditionary Factors Study, discussed below. In addition, MCIA has a Mapping, Charting, & Geodesy section which is able to acquire and exploit commercial imagery in support of MAGTF requirements, and all analysts are aware of the value of open sources for fulfilling expeditionary intelligence requirements.

The MCIA Librarian, Ms. Barbara Necoba, is the focal point for Marine Corps OSINT requirements.

7007. Expeditionary Factors Study

In 1988, when the Marine Corps Intelligence Activity (MCIA) was first established, the first Director (a Colonel) and his civilian Special Assistant/Deputy Director discovered that much of what was needed by the Warfighting Center, the acquisition program managers, and senior staff at Headquarters Marine Corps, was not available through classified databases and classified intelligence products. In close consultation with the Fleet Marine Force, MCIA established an agreed upon list of 67 countries and two island groups against which to develop encyclopedic intelligence. Working closely with the Warfighting Center, a wide variety of mission area factors were agreed upon, and defined by the operators in terms of five levels of difficulty. Under the supervision of the Special Assistant/Deputy Director, a contractor was hired to prepare Overview of Planning and Programming Factors for Expeditionary Operations in the Third World. This three-volume product was approved by the Commanding General of the Marine Corps Combat Development Command for dissemination in March 1991, and represents the Marine Corps' ground breaking effort to create a useful intelligence product using only open sources.

Subsequently Marine Corps flag officers were consulted and agreed on a new list of 80 countries, and the study was repeated, now titled Expeditionary Force Mission Factor Intelligence Analysis Requirements Study (ExFac Study), and this new expanded study was published 15 September 1994 in both hard-copy and as a CD-ROM database. There are over 100 copies of this unique resources available throughout the Marine Corps, with one set in the library of the Navy Marine Corps Intelligence Training Center.

The following mission area factors are covered for each of 80 countries (Appendix H contains a list of the countries):

Drug Threat	Ground Order of Battle
Terrorism	Air Order of Battle
Gray Arms & Technology Transfer	Naval Order of Battle
Nuclear, Biological, & Chemical	Ongoing Conflicts
U.S. Equities	Culture

Weather	General Geographic Conditions
Coastal Characteristics	-- Cross-Country Mobility
Mapping. Charting, & Geodesy	-- Intervisibility
Airfields	-- Operational Elevation
Ports	Key Installations
Noncombatant Evacuation Logistics	Communication Infrastructure
Highways/Railways	Medical Operations

Examining the results contained in this study leads some very useful "strategic generalizations" which can help planners better prepare for expeditionary operations. For instance, the Marine Corps aviation day is hot, over 80 degrees on average, with relatively high humidity. Fewer than 50% of the ports in the this Marine Corps environment are suitable for pierside offload, requiring instream offload even when unopposed. Intervisibility (line of sight) distance in much of the Marine Corps world is heavily constrained, and cross-country mobility is almost non-existent. It should be stressed that this unclassified intelligence product is for orientation and ready reference purposes, it should not be used as the basis for planning and conducting military operations--it provides context and is intended to aid in requirements analysis and collection management of the traditional disciplines.

Every MAGTF should have at least one copy of this study, available in both hard-copy (three volumes) and CD-ROM. To obtain a copy, communicate with Mr. Steve Foster, Deputy Director, MCIA, at (703) 784-6140.

7008. Marine Corps Reserve

The Marine Corps Reserve represents a very significant source of open source expertise. Many Marine Corps Reserve personnel have achieved considerable stature as civilian experts in various regional and subject matter areas. Many have worked overseas as civilians, and acquired foreign language and foreign culture expertise which may not be a matter of record but which qualify them as "virtual" Foreign Area Officers.

MAGTFs should consider initiatives to identify specific Marine Corps Reserve personnel competent in languages and countries of direct interest to the MAGTF, so as to hold these Reservists as "hip pocket" augmentation unit for specific contingencies. As a general rule, the reservists who are most talented and most competent will not be available for "make work" active duty assignments or Individual Mobilization Augmentee billets, but would be available for 15-30 assignments in their country of interest.

Such reservists can be requested and funded apart from the normal Marine Corps Reserve funding process, by requesting General Defense Intelligence Program (GDIP) Reserve Augmentation funding from HQMC. When requesting orders for such reservists, ensure that the request specifies that a) liberal civilian grooming and attire authorized; b) non-reporting orders; and c) special conveyance authorized. The first permits the Reservists to blend in as civilians as they "walk the ground" legally; the second avoids any unnecessary

contact with the U.S. Embassy and precludes the Reservists from being co-opted for administrative duties by the local defense attache; and the third permits them to take in-country tours with guides, as well as hire canoes, donkeys, and other conveyances requiring an indigenous driver.

7009. Additional Open Source Training Opportunities

There is only one significant private sector source of open source intelligence training expertise, and that is OPEN SOURCE SOLUTIONS, Inc., the non-profit educational corporation dedicated to studying and teaching open source intelligence. This organization offers three significant additional open source training opportunities:

a) Annual Conference. Each year in mid-September, OSS, Inc. offers a 3.5 day conference on open sources, systems, and services. This conference, the only one of its kind, attracts between 600-800 international representatives (although 50% of the audience is from the U.S. government), and includes the Open Source Coordinators for all of the major European nations as well as many Asian and African nations. For information about the conference send electronic mail to <OSS96@oss.net> (change year as appropriate); send a facsimile request to (703) 242-1711, or call (703) 242-1700 and leave a complete mailing address.

b) Newsletter. *OSS NOTICES* is the only newsletter in the world dedicated exclusively to open source intelligence, and it draws on a substantial range of other publications to report each month, in 30-40 pages without advertising, on open sources, systems, and methods. Each month's issue has a theme, including six regional themes a year. To review past issues, visit <http://www.oss.net/oss>, email <oss@oss.net> with a request for a sample copy, or fax (703) 242-1711 with a request and complete mailing address.

c) References. OSS, Inc., which is now entering its fifth year as the leading advocate and student of open source practices, publishes a two volume *Proceedings* from each of its annual conferences, and these are available for purchase. Especially recommended is the set from 1995, which consists of *Open Source Intelligence: Selected Readings* (Volume I) and *OSS '95: The Conference* (Volume II).

The Community Open Source Program Office has in August 1995 released a Request for Proposal for a series of training lessons oriented toward the Open Source Information System, and these will be available no earlier than 1998 and perhaps later.

Any questions? Mr. Robert D. Steele, President of OPEN SOURCE SOLUTIONS, Inc., and a former Marine, is prepared to support any MAGTF in any clime and place. Communicate with him at <ceo@oss.net>, voice: (703) 242-1700, or fax: (703) 242-1711.

APPENDICES

		Page
A	White Paper on "Open Source Intelligence: What Is It? Why Is It Important to the Military?"	099
B-1	Talking Points on "Private Enterprise Intelligence: Its Potential Contribution to National Security"	110
B-2	Complete Paper on "Private Enterprise Intelligence: Its Potential Contribution to National Security"	113
B-3	Glossary	145
B-5	Core Open Source References	146
C	White Paper on "ACCESS: Theory and Practice of Intelligence in the Age of Information	147
D	Concise Directory of Selected International Open Sources & Services	165
E-1	Internet: Self-Guided Tour	174
E-2	Internet: Intelligence-Oriented List of Useful Internet Sites	181
E-3	Internet: Intelligence-Related Sites from *PC Magazine*	190
E-4	Internet: How to Find an Interesting Mailinglist	193
F-1	Expeditionary Environment Research & Analysis Framework & Model	201
F-2	Mission Area Factors Summary	252
G	OSINT OPSEC: Selected References and Information	302
H	Expeditionary Factors Study: List of Countries	306

APPENDIX A

Open Source Intelligence: What Is It? Why Is It Important to the Military?

Robert D. Steele, President
OPEN SOURCE SOLUTIONS, Inc.

Introduction

This White Paper defines Open Source Intelligence (OSCINT) and its relevance in meeting the needs of the military (both commanders and defense policy-makers).

OSCINT is intelligence derived from public information--tailored intelligence which is based on information which can be obtained legally and ethically from public sources.

This White Paper suggests that OSCINT is a both force multiplier and a resource multiplier. OSCINT provides a practical political and military advantage which complements the advantage provided by traditional intelligence, it is available at low cost, and it cannot be ignored.

First the paper describes and discusses the utility of OSCINT in general terms, and at the strategic, operational, tactical and technical levels of warfare, including a single practical example at each level. The paper then describes the "information continuum" within which a range of open sources, systems, and services can be obtained which are relevant to military needs. Finally, the paper provides a brief discussion of the status of the open source intelligence programs in the United States, The Netherlands, and Sweden, and concludes with a concise discussion of opportunities and risks inherent in the use of OSCINT to meet military requirements, and of several practical steps that can be taken to exploit OSCINT in support of military strategy, operations, tactics, and technical acquisition and countermeasures.

The official definition of OSCINT by the U.S. Intelligence Community:

> By Open Source we refer to publicly available information appearing in print or electronic form. Open Source information may be transmitted through radio, television, and newspapers, or it may be distributed by commercial databases, electronic mail networks, or portable electronic media such as CD-ROM's. it may be disseminated to a broad public, as are the mass media, or to a more select audience, such as gray literature, which includes conference proceedings, company shareholder reports, and local telephone directories. Whatever form it takes, Open Source involves no information that is: classified at its origin; is subject to proprietary constraints (other than copyright); is the product of sensitive contacts with U.S. or foreign persons; or is acquired

through clandestine or covert means.[1]

The official definition is limited in its understanding to standard commercial sources of traditional information, and excludes, to take one important example, SPOT imagery. It also fails to take into account the importance of unpublished materials including electronic information and human knowledge which can be accessed legally and ethically.

The official approach to OSCINT is also limited in that the existing information-handling architectures for intelligence processing, including dissemination to the commander, are all classified, and there is a very limited capability for routing unclassified information efficiently, even assuming it can be obtained. In most communities, there appears to be a reluctance to assume primary responsibility for the collection and processing of OSCINT, which is why military operators in two countries (the United States and the United Kingdom) are examining means of acquiring and exploiting OSCINT directly, bypassing the intelligence community in order to give action officers at the policy level, and commanders at the operational level, direct access to OSCINT.

Experienced intelligence professionals have found that while OSCINT is not a substitute for traditional intelligence disciplines, including Human Intelligence, Imagery Intelligence, and Signals Intelligence. However, OSCINT does offer three major advantages for planning and conducting military operations:

-- When encountering requirements for military operations in the Third World or in support of humanitarian assistance and counter-terrorist operations for which intelligence collection priorities have not been high. OSCINT is frequently the only discipline able to respond rapidly (to include commercial imagery), and it provides the commander and his staff with a rapid orientation adequate for both developing initial planning packages; and for establishing collection requirements for the traditional intelligence disciplines.

-- OSCINT is also a means of achieving significant savings, in that many essential elements of information required by the commander and his staff can be acquired from commercial sources at a lower cost, in less time, than from classified capabilities, with the added advantages that OSCINT is often more up to date, and requires no political risk in its acquisition. *This permits classified intelligence capabilities to be focused quickly and effectively on mission-critical gaps, and avoids depleting or mis-directing these scarce resources—"do not send a spy where a schoolboy can go".*

-- Finally, OSCINT, whether it precedes or follows traditional intelligence collection, can protect national intelligence sources and methods by serving as the foundation for

---

[1] Although the original intelligence community report was classified SECRET, the definition and extensive commentary appeared in an unclassified document, *United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations (Working Group Draft Dated 6 January 1992)*, and portions, including the definition, were subsequently reprinted in *OSS NOTICES* Volume 2 Issue 9 (30 November 1994).

intelligence support to joint and coalition operations where it is not possible, or desirable, to reveal the capabilities and limitations of the traditional intelligence community.

Open Source Intelligence and the Military

The availability and utility of OSCINT depends upon, and will vary, depending on the specific area of operations under consideration, and on two other factors: the level of warfare, and the point on the spectrum of conflict, from presence to general war, where the intelligence will be applied.

In general terms, OSCINT has significant potential as a source of intelligence support in terms of indications & warning, policy development, contingency planning, security assistance, weapon acquisition (design and countermeasures), joint and coalition operations, and tactical operations against new priorities such as proliferation. Finally, OSCINT is vital as a means of rapidly orienting the commander and serving as the foundation for collection management within the traditional intelligence disciplines.

At the strategic level:

-- OSCINT can provide indications & warning of both hostile intent, and opportunities for military advantage. Content analysis of multiple open sources such as regional newspapers from the Middle East, are often if not always more reliable foundations for estimating stability and instability, than reports from clandestine sources with a limited range of access and a personal perspective that biases their reporting.[2] OSCINT is especially valuable with respect to cultural and demographic intelligence, areas not generally well-covered by traditional civilian and military intelligence collection and analysis capabilities.

-- OSCINT can also provide very important geographic and civil generalizations which can significantly affect major military acquisition and design decisions. For instance, most countries build their aircraft for optimal performance on a "standard aviation day" which is defined in terms of warm (60°-70°F) conditions and balanced humidity. The military commander that is responsible for expeditionary operations to the Third World will find themselves utilizing aircraft which carry half as much half as far because the standard aviation day in the Third World is hot (over 80°F with high humidity). If aircraft cannot be designed for optimal performance on a hot day, then the military commander can at least ensure that doctrinal publications reflect accurate load and lift capabilities for the true expeditionary conditions to be encountered.

-- OSCINT can provide unclassified threat intelligence which can be used to educate

---

[2] This point was made publicly by Dr. Stephen Fairbanks, the Iranian Analyst for the U.S. Department of State's Intelligence and Research Bureau, in the presence of his superior, Dr. Jennifer Sims, Deputy Assistant Secretary of State for Intelligence Coordination.

and mobilize public and political support for military needs including policy development.

At the operational level:

– OSCINT can provide the geographic and civil generalizations required for regional force planning and force employment. In particular, OSCINT has establish credible regional generalization regarding the capabilities of air, ground, and sea forces to be encountered by the commander; geographic generalizations with respect to cross-country mobility, average line of sight distances, temperatures, and water availability; and civil generalizations such as bridge-loading, port clearance, airhead bunkerage; and civil communications and computing resources. OSCINT provides a time-sensitive solution to questions the theater commander will have about civil infrastructure, political cliques and personalities, and economic or financial factors affecting operational employment of forces, and is therefore especially helpful to contingency planning which must be pursued without adequate support from traditional intelligence capabilities.

-- OSCINT is especially useful to the theater commander for the coordination of joint and coalition operations where traditional classified intelligence capabilities are either not available (e.g. in much of the Third World where lower priorities have restricted coverage), or cannot be shared with foreign elements.

At the tactical level:

-- OSCINT has been shown to be highly pertinent and effective against new priorities, including counter-proliferation, counter-terrorism, and peacekeeping operations. This is true for both conventional military operations focused on overt interdiction, and clandestine or covert "direct action" by special operations forces.[3]

-- OSCINT is a critical resource for the military commander who requires maps and digital targeting information for Third World area for which current geographic information is not available from government sources, whether classified or unclassified. In combination, SPOT and other commercial imagery resources can provide the commander with up to date maps containing all airfields, roads, and bridges; and soon containing contour lines as well,

---

[3] At a Canadian intelligence conference 27-29 October 1994, both the Director of the Canadian Security and Intelligence Service, Mr. Ward Elcock; and Dr. Paula Scalingi of the Los Alamos National Laboratory in the United States, stated that OSCINT provides over 80% of the input to the final all-source product; in Dr. Scalingi's case, this was with specific reference to intelligence support for counter-proliferation. Dr. Gordon Oehler, Director of the U.S. Intelligence Community's Nonproliferation Center, has made similar comments on several public occasions.

for expeditionary operations.[4]

At the technical level:

-- OSCINT about civil communications and computing capabilities in the area of operations will be very important to the commander. As information warfare and information peacekeeping become critical mission areas, and all opponents achieve some capabilities to conduct electronic warfare, the commander will need to use OSCINT both to understand how to degrade the performance of civil capabilities being used by opponents, and to consider exploitation of civil capabilities to maintain joint and coalition communications.

-- OSCINT will provide most of what the commander needs to plan and coordinate joint and combined air, sea, and land operations in the expeditionary environment, with specific reference to strategic airlift and sealift operations involving civil aircraft, air traffic control and air defense planning for civil platforms, and fueling and other logistical considerations.

The Information Continuum

There are three ways of understanding the robust nature of the private sector's potential contribution to military intelligence needs. The first is by examining in general terms this continuum.

		Private Investigators		
Schools	Libraries	Information Brokers	Government	Intelligence
Universities	Businesses	Media	Defense	

Each of these nine sectors of the global or national information community maintains a cadre of human experts as well as a range of both hard-copy and electronic information. Much of what is known to them, or stored by them, is not available through commercial online services. Following a specific example from each sector:

---

[4] SPOT is going to 5-meter resolution imagery in the very near future. In the U.S. Space Imaging, Inc., a subsidiary of Lockheed, has announced plans to provide 1:2,500 meter synoptic resolution imagery, within a year. These commercial capabilities will be critical to expeditionary operations in the Third World because of the lack of current maps. One U.S. study, *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (Marine Corps Combat Development Command, March 1991), determined that for the 69 countries of concern to the Marine Corps, there were no 1:50,000 combat charts for 22 of the countries, old 1:50,000 charts for ports and capital cities only in the case of another 37 countries, and very old 1:50,000 complete coverage for another ten countries.

-- Language schools can rapidly identify individuals by location and nationality who have received training in the home country language and are target country nationals (e.g. Somalis studying French in Paris): these individuals can be contacted and offered part-time employment as translators.

-- Universities utilize their existing infrastructures and a regular supply of cheap intellectual labor to maintain important and authoritative databases. The Monterey Institute of International Studies, for instance, maintains the best database on the proliferation of nuclear materials, and utilizes graduate students fluent in Russian, Chinese, Arabic, and other languages to cover a wide range of multi-lingual publications, and to maintain an electronic database, at very low cost.

-- Libraries can be used, either as needed or in a deliberate fashion, to serve as repositories for "just in case" archiving of political-military, economic, and other materials pertaining to specific countries. This allows the government to share the cost of archiving with other library sponsors, and in many cases avoid the cost all-together.

-- Businesses have enormous repositories of market research, including communications and logistics research, on countries throughout the world where they have made or plan to make an investment. Businesses are also acutely familiar with the political corruption, climate conditions, and other factors which affect operational efficiency in specific locations. Two unique examples of business dedicated to meeting private intelligence needs are Oxford Analytica, with its network of 750 overt agents world-wide, and *The Economist* Intelligence Unit.

-- Information brokers can be identified who specialize in particular scientific & technical topics or regions of the world. This permits more efficient search & retrieval by exploiting capabilities whose "learning curve" has been funded by others. In addition, information brokers can be identified with specific language capabilities, and employed to do rapid exploitation of captured or acquired documents.

-- Journalists responsible for specific areas of the world, including journalists specializing in military, aerospace, and insurgency matters, rarely publish ten per cent of what they know, and they never publish their sources. They can, however, be engaged to prepare special reports, and to provide background information on specific personalities of importance to planned military operations. This need not be done secretly or through direct recruitment; it can be done discreetly as a private commercial transaction. Media organizations, such as Jane's Information Group, acknowledge that they publish less than 20% of what they know, in some cases to protect sources--they are however willing to do tailored confidential reports drawing on their complete range of sources.

-- Governments, including provincial and state governments, frequently have experts in agriculture or other trade-related fields who are familiar with specific areas of operation and the logistics as well as the key personalities. Embassies have personnel whose reporting

does not fully communicate what they know. Bringing key government personnel together for a week can quickly establish a foundation for collection management which the commander could not normally achieve through analysis of raw information.

-- Other intelligence organizations, including the "information and research" elements of the Vatican, the United Nations, and the International Red Cross, have global networks of reporting sources, including sources with special linguistic and regional skill, that can be drawn upon.

The third way of understanding the robust capability of the private sector is to consider the range of information services that are offered which are directly pertinent to military intelligence needs. These are listed in three columns:

Direct Observation	Document Acquisition	Telephone Surveys
Commercial Online Searching	Document Translation	Market Research
Current Awareness	Broadcast Translation	*Recruited Agents*
Experts On Demand	Multi-Expert Research	*Industrial Espionage*

Recruited agents and industrial espionage are not considered legal nor ethical within the private sector, but there are very competent organizations that openly offer such services, to include route reconnaissance and target identification services in third countries. In each of the above categories, it is highly likely that a private sector partner can collect, process, translate, and deliver open sources of intelligence able to make an important contribution to the commander's needs for information--and to do so in a cost-effective fashion which could not be duplicated by defense attaches or traditional military intelligence collection brigades.

The third way to understand the utility of the private sector for military intelligence needs is to take a case study, such as Somalia. In the absence of internally-available intelligence information, the fastest means of establishing an encyclopedic foundation for further collection management, and the fastest means of providing the commander with at least some useful information pending responses from the traditional intelligence disciplines, it by seeking out private sector experts and private sector databases. A leading scholar, a leading businessman recently returned from a tour as General Manager in Somalia, a leading journalists, and perhaps an information broker specializing in African information could be brought together and could quickly identify human, hard-copy, and electronic sources--including sources of digital geographic information--of immediate utility.

In one specific instance, supporting a wargame on Somalia, an individual playing the role of the United Nations commander was able to overcome the inadequacies of the U.S. intelligence community by making three telephone calls. Overnight, in Express Mail, at a *pro forma* cost of about $5,000, the individual received:

– From Jane's Information Group, a spiral-bound volume containing a map of Somalia clearly marking the nine clan areas; a one-page order of battle for each clan (at a time when most intelligence analysts were thinking only of the old Somali army); and a one-paragraph precis with full citation for each article about Somalia published in any of the Jane's publications (including the excellent *Jane's Intelligence Review*) in the past two years. This constituted a superb orientation for both planning and collection management.

– From Oxford Analytica, twenty two-page reports suitable for Presidents and Prime Ministers, covering three topical areas: United Nations operations in Somalia, U.S. foreign policy toward Somalia; and U.S. operations related to Somalia. Again, a superb orientation on strategy and policy, in concise and immediately-usable form.

– From *The Economist* Intelligence Unit, a copy of the appropriate country risk report, which included important summary information on the logistics difficulties that would be encountered, including the limitations of both the port and the airfields for strategic entry.

Commentary on Representative National Approaches to OSCINT

Although OSCINT has always been part of the national and military intelligence process, in recent decades increased emphasis on technical systems and secret collection have tended to sharply reduce the amount of funding and the number of personnel dedicated to collecting and processing publicly available information. At the same time, the "information explosion" or "information revolution" has dramatically increased both the quality and quantity of the information available in the public sector. Today the commander can take a weather map of Bosnia off of the Internet, or exchange email with volunteer observation and listening posts in Bosnia.

Unfortunately, the reality today is that most intelligence communities are trained, equipped, and organized to collect and process secrets. OSCINT capabilities in both the civilian and military sectors of government have both atrophied where they existed, and also failed to keep up with the growth of private sector OSCINT capabilities.

– United States of America. The National Foreign Intelligence Board was recently briefed to the effect that while 99% of the $28-35 billion dollars a year budget is spent on classified collection and processing, and only 1% is spent on OSCINT, OSCINT provides 40% of the all-source product. In one interview, the Deputy Director for Science & Technology of the Central Intelligence Agency stated that this latter figure was actually 70%. The major element of the U.S. intelligence community program is the Foreign Broadcast Information Service, which is under severe criticism for its continued emphasis on print

media exploitation, and its inability to master a wider range of open sources. In an attempt to gain control over the modest distributed resources being applied to OSCINT, the Director of Central Intelligence created the Community Open Source Program Office. This office is about to release a strategic plan for OSCINT, but it is limited to improving internal community access to open sources already collected. The Department of Defense program. for which the National Air Intelligence Center is the executive agent, builds on the existing scientific & technical intelligence document acquisition and translation program. The Department of Energy Laboratories, and especially Sandia and Los Alamos, constitute a major OSCINT resource which is being exploited by some military consumers of intelligence, such as the U.S. Southern Command, but which is not under the control of the intelligence community. Some very modest individual initiatives have taken place within the military services, the most advanced of which is the publication, in draft form by the Army, of an open source primer for military intelligence officers. At this time the U.S. military does not have timely broad access to a full range of open sources.[5]

-- The Netherlands. Various open sources, including the *Intelligence Newsletter* out of Paris, and *OSS NOTICES* in the United States, have reported that the foreign and military intelligence agencies have been integrated. Within the new national intelligence agency. a special Open Source Coordinator has been appointed, and a task force approach is being taken to intelligence collection and analysis. Every task force has an open source intelligence specialist. and all requirements for intelligence must first be examined and if possible satisfied through OSCINT before tasking of clandestine or technical capabilities is permitted. More recently, the intelligence elements of the individual military services were integrated into a joint military organization reporting to the Prime Minister.

-- Sweden. This country is most interesting because is has a unique consortium within which to formally orchestrate the activities of government intelligence, the business intelligence community, and the university research community. Swedish scientific & technical attaches have been noted to regularly exploit the Internet, and there is discussion within Lund University of the need for an Open Source Intelligence Center™ to meet the combined needs of the government, business, and university communities in Sweden.

Advantages and Disadvantages of Open Source Intelligence

-- Advantages include the fact that OSCINT has virtually unlimited potential on any topic; is of relatively low cost because expertise is maintained at someone else's expense; is generally up to date; and can be shared with anyone.

---

[5] The extraordinary relevance of Department of Energy OSCINT capabilities in support of military operations are described in *SHARING THE SECRETS: Open Source Intelligence and the War on Drugs* (OSS Inc. Limited Edition, 1994). The Army paper, prepared by the 434th Military Intelligence Detachment, Strategic, is titled *Open Source Intelligence Resources for the Military Intelligence Officer* (Fort Huachuca, November 1994).

-- Disadvantages include the possibility of revealing military plans and intentions (security can be provided by laundering the question through trusted intermediaries); the time and cost associated with searching for exactly the right information within the hugh volumes of public information; and the temptation to accept an open source at face value when it could be disinformation or simply inaccurate.

Obstacles to Military Exploitation of Open Sources

There are three obstacles to military exploitation of OSCINT:

-- Organizationally, the military relies on a classified intelligence community for its "intelligence", and does not have an alternate structure established to obtain OSCINT. Among the most important problems created by this reliance are those of funding: there are no well-established programs for contracting directly with the private sector for OSCINT.

-- Culturally, there is a strong attitude, primarily within the intelligence community but to an extent within the operational community, that information achieves a special value only if it is classified. This is in part a result of a cultural inclination to treat knowledge as power, and to withhold knowledge from others as a means of protecting one's power. This attitude is the equivalent of the calvary ignoring the tank and the machine gun. The "openness" paradigm has thoroughly defeated the secrecy paradigm, and those organizations which focus on protecting secrets rather than exploiting publicly available information, will find themselves "starving" for knowledge.

-- Technically, because of the historical focus on training, equipping, and organizing forces for unilateral and conventional military operations, with the added assumption that all "intelligence" will come through classified and well-established channels, the existing command & control architecture, including communications, computing, and intelligence elements, is not designed to rapidly interface with joint and coalition forces, with special forces and direct action clandestine teams, and with the vast array of private sector and non-military government elements which can provide OSCINT to the commander.

Opportunities for Advantage

The Director of Military Intelligence (DMI) for any nation has essentially three opportunities to improve national capabilities to collect, process, and disseminate OSCINT to commanders and military policy-makers:

-- Existing library resources are poorly-funded and organized for the purpose of "just in time" archiving of information. Library resources, both within the intelligence community

and outside the intelligence community, must be recognized as the "source of first resort"[6] Commanders and policy-makers must restore funding for library operations, including the cost of subscribing to external online services and out-sourced research, while at the same time redirect the libraries toward "just in time" decision-support to specific consumers, and away from "just in case" generic collection and processing.

-- Existing military intelligence analysts must be given the training, fiscal authority, and commander's guidance necessary to convert them from narrow specialists focusing on the analysis of classified information, to managers of networks of overt human experts and related electronic and hard-copy databases. At the same time, analysts must be re-oriented so that their primary focus is on day to day interaction with the commander and other consumers of military intelligence, and on day to day collection management founded upon open source exploitation, rather than the existing focus on producing classified reports in isolation from the consumer.

-- Existing commanders, in consultation with the DMI, must recognize that it is impossible for the DMI to satisfy their intelligence requirements related to a wide range of new priorities, with existing classified military intelligence capabilities. The entire structure of military intelligence must be recast to permit rapid maneuver throughout the private sector's knowledge terrain, and the rapid collection, processing, and dissemination of mission-critical OSCINT to the commander at every level of operations (strategic, operational, tactical, and technical) and in "every clime and place".

Role of the Military Reserve

The military reserve constitute a national resource which has enormous potential. A simple example will serve to make the point. For every country of interest, a cadre of five military intelligence reservists could be formed, and given a responsibility to monitor pertinent foreign language periodicals and publications (which would be provided them on subscription), and to prepare weekly OSCINT summaries. These same individuals should be afforded direct access to the Internet and commercial online databases, and serve as direct reinforcements on demand to the active duty military intelligence analysts responsible for the same areas of interest. Funds should also be provided for the five person cadre to spend thirty days each in the country of interest, unencumbered by administrative duties. In this way, when a contingency requirement emerges, the responsible commander can activate the appropriate cadre (or cadres in the case of a theater commander).

---

[6] This important phrase was developed by Mr. Paul Wallner, the first (and last) Open Source Coordinator in the Office of the Director of Central Intelligence in the United States. Mr. Wallner, a member of the Senior Executive Service (flag rank) served for many years in the Defense Intelligence Agency and has been a strong advocate for improving OSCINT support to the commander. Today he serves as Deputy to the first Director of Community Open Source Program Office, Dr. Joseph Markowitz.

APPENDIX B-1

PRIVATE ENTERPRISE INTELLIGENCE: ITS POTENTIAL CONTRIBUTION TO NATIONAL SECURITY[7]

Talking Points

Concepts

Threat: No longer mono-lithic, mono-culture.

Four warrior classes--high-tech brute, low-tech brute, low-tech seer, high-tech seer. Community was built to deal with high-tech brute, is not ready for the other three.

Must distinguish between data (raw print, image, signal), information (collated data of generic interest, including 95% of the intelligence community's production), and intelligence, which is information tailored to support a specific decision by a specific person at a specific time.

Context

Joe Nye's jigsaw puzzle analogy--OSCINT provides context and orientation, and larger share of the puzzle than before.

Information continuum (K-12, universities, libraries, business, private investigators and information brokers, media, government, defense, intelligence) is robust and ready to provide low cost responsive intelligence on many topics today.

Virtual intelligence community in U.S. is a $500 billion per year industry, and *someone else pays the overhead.*

OSCINT is a means of achieving savings which permit reinvestment in improved clandestine and technical collection. *Don't send a spy where a schoolboy can go!*

---

[7] These talking points were prepared by Mr. Robert D. Steele, President of OPEN SOURCE SOLUTIONS, Inc., for presentation to a Canadian intelligence conference, "Intelligence Analysis and Assessment: The Producer/Policy-Maker Relationship in a Changing World, 27-29 October 1994, Ottawa, Canada.

Challenge

Integrated analysis--integrating geographic and civil factors and striving for strategic and operational generalizations and forecasting, not just tactical and technical specifics about military capabilities--requires an order of magnitude increase in the exploitation of open sources.

90% of what the policy maker reads and listens to is not only unclassified, it is unanalyzed. Open sources reaching the consumer reflect a wide variety of competing influences and perspectives--the community is not helping the policy maker make sense of the babble.

"Just in time" intelligence support means just in time collection as well as production. Linear paradigm (consumer to analyst to collector to source, and back up) is dead. New paradigm is the diamond paradigm, where all four talk to each other at one time or another.

Must resolve the dilemma of whether intelligence is about secrets, or about informing policy. 80% of what is needed to inform policy is unclassified, and unclassified intelligence is much more useful politically.

Change

We used to promote analysts for mastering classified data in isolation from open sources, collectors, and consumers. This will no longer be the case.

The analyst of tomorrow will be a manager of a network of overt human sources who serve as distributed filters of unclassified information, and provide "on demand" guidance as to the most pertinent sources and data.

The analyst of tomorrow will be a partial extrovert skilled at "recruiting" the consumer and maintaining direct personal relations with the consumer.

The analyst of tomorrow will be both a resource manager and a collection manager, able to draw from open sources to the fullest extend possible, while tasking clandestine and technical sources as needed.

Country

The intelligence community cannot reinvent itself in isolation. To harness the distributed intelligence of the Nation and optimize its exploitation of open sources, the intelligence community--the Nation--requires a national information strategy.

That strategy should enable connectivity across the information continuum; nurturing and exploitation of distributed centers of excellence focused on content; coordination of information technology research & development; and establishment of Nation-wide standards of communications & computing security.

In the information age, only smart nations will prosper and survive. The intelligence community is a vital but not a sole source of national intelligence. The smart nation must integrated classified government capabilities with unclassified private sector capabilities to create a new form of national intelligence.

APPENDIX B-2

PRIVATE ENTERPRISE INTELLIGENCE: ITS POTENTIAL CONTRIBUTION TO NATIONAL SECURITY

Losing Our Way 114
OSCINT and the Changing Threat 118
OSCINT and Changing Definitions of National Security 122
OSCINT and the Consumer 124
The Strategic Context of Private Enterprise Intelligence 126
Operational Concepts, Policies, and Practices 131
Private Enterprise Intelligence--Tactical Opportunities 134
Conclusion 143

Appendix B-3: Glossary 145
Appendix b-4: Core Open Source References 146

Figure 1: The Four Warrior Classes and Implied Intelligence Challenges 118
Figure 2: Competing Influences on the Policy-Maker 124
Figure 3: The "Information Continuum" or "Virtual Intelligence Community" 129
Figure 4: Basic "Intelligence" Capabilities in the Non-Profit Arena 135
Figure 5: Core Business/Economic Intelligence Capabilities 138
Figure 6: More Intrusive Private Intelligence Capabilities 141

PRIVATE ENTERPRISE INTELLIGENCE: ITS POTENTIAL CONTRIBUTION TO NATIONAL SECURITY

Robert David Steele[e]

95% de l'information dont une entreprise a besoin peut s'acquirir par des moyens honorables.

Henry Stiller, Director General
Histen Riller, Societe Civile

ABSTRACT: In an era when both the nature of the threat and the definition of national security have undergone radical redefinition, it is essential that the intelligence and security services understand what their consumers have recognized for many years: private enterprise intelligence capabilities are robust, diverse, responsive, and relatively inexpensive. As we all strive to "reinvent" our intelligence and security services, the potential contribution of the private sector must be understood and integrated into our final design. At the strategic level, the private sector provides the context for classified and technical collection; at the operational level, the private sector is well ahead of the government in pursuing new concepts for intelligence dominance; and at the tactical level, the private sector now offers open sources and services which can meet roughly 80% of the needs of traditional and emerging intelligence consumers.

Losing Our Way

Too often we in the intelligence community forget our roots and abandon our private sector allies. Spies existed before Christ, but most of them were actually legal travelers and

---

[e] *Mr. Steele is President of OPEN SOURCE SOLUTIONS, Inc., a non-profit educational association established to assist governments and private sector organizations in understanding and capitalizing upon private enterprise intelligence capabilities, generally known as "open source intelligence" (OSCINT). In 1992 he was named one of the "Microtimes 100: industry leaders and unsung heros who made a difference in the computer industry in 1992 and helped create the future". In 1993 he was featured by Alvin and Heidi Toffler as "The Rival Store" in their chapter on "The Future of the Spy", in War and Anti-War: Survival at the Dawn of the 21st Century. Mr. Steele is a veteran of the clandestine service of the United States of America, has helped manage overhead satellite programs, and was the founding Deputy Director of the Marine Corps Intelligence Center, where he developed many of his findings on the relative utility of OSCINT as a substitute or complement to the traditional intelligence collection disciplines.*

discreet merchants. Tea was stolen from China, and porcelain from England, by merchants.[9] More recently Japan, China, and Taipei have demonstrated profitable and cost-effective private intelligence capabilities. France and Israel excel at government support to the private sector, but I speculate that soon it will be the private sector that is conducting most of the espionage as well as the open source intelligence (OSCINT) collection in these two countries.[10]

The Anglo-Saxon intelligence communities lost their way in the late 1950's, largely because of over-reliance on the American intelligence budget as a safety net, with the unfortunate result that the American tendencies to ignore counter-intelligence and cultural intelligence, and to rely on technical panaceas and bean counting, infected the other services and skewed the manner in which our respective intelligence services trained, equipped, and organized for sustained warfare against "the threat".

Among the worst of the American influences on Anglo-Saxon intelligence were its obsessive focus on the Soviet Union as the only enemy worthy of total attention; and the

---

[9] The "privatization of intelligence" is a concept—indeed a sub-discipline--which owes a great deal to Dr. Stefan Dedijer of Lund University in Sweden. His contributions were honored with a book dedicated to him, by Jon Sigurdson and Yael Tagerud, *The Intelligent Corporation: The Privatization of Intelligence* (Taylor Graham, 1992). Most recently, aided by one of his more promising disciples, Ms. Katarina Svensson, Ph.L., he published *Technical Attaches and Sweden's Innovation Intelligence* (Lund University, April 1994). It is not my task here to provide citations to the literature critical of classical intelligence, but I do wish to acknowledge the lasting influence of Mr. Loch K. Johnson, whose article "Seven Sins of Strategic Intelligence", *World Affairs* Volume 146 Number 2 (Fall 1983), and subsequent book, *A Season of Inquiry: The Senate Intelligence Investigation* (The University Press of Kentucky, 1985), set the stage for the critical exploration of alternative sources & methods. In the final note I provide several references focused strictly on private enterprise sources and methods.

[10] I consider the Swedes to be the "stealth Japanese" of the Anglo-Saxon intelligence world, and also--with the Dutch--to have the most potential for creating the first Anglo-Saxon "intelligent Nation". Outside the Anglo-Saxon world I look to India, Viet-Nam, and Saudi Arabia to set new standards of excellence in government and private sector intelligence endeavors, and in fact speculate that they have already enjoyed significant successes. The dark side of private enterprise intelligence is represented by the criminal gangs--where the Colombians have been relatively unsophisticated, but omni-present in shadowing every U.S. frigate and aerial observation aircraft, I see the Russian, Vietnamese, Korean, and Japanese criminal organizations as cohesive, well-funded, and highly sophisticated. They represent a major threat which law enforcement will not be able to handle without a radical redefinition of both the responsibilities of national intelligence, and the support obligations of national defense.

American "solution" for poorly managed human intelligence (HUMINT) against the Soviets[11], an extremely expensive and deceptively ineffective technical collection empire which had the unanticipated impact of precluding American HUMINT from developing into a serious clandestine service. A side effect of the American resort to extremely expensive and highly classified[12] imagery intelligence (IMINT) and signals intelligence (SIGINT) overhead collection systems was the abandonment of the robust, diverse, responsive, and relatively inexpensive capabilities of the private sector.[13]

---

[11] In the aftermath of World War II, the Americans displayed their distressingly usual tendency to take the easy way, and attempted to penetrate the Soviet Union using emigres and others from organizations which had already been thoroughly penetrated by Soviet intelligence. When all of these "agents" were captured and executed, rather than doing some serious soul-searching and then creating a more serious illegals capability, the Americans turned to the U-2 and its follow-on satellites as an "acceptable" alternative to traditional spycraft. Now we find ourselves facing a wide range of threats which are not amenable to technical penetration, while we are simultaneously handicapped by the absence of a clandestine service worthy of the name.

[12] Americans (among others) have developed the art of secrecy as a means of concealing ineffectiveness, inefficiency, and irrelevance. Although the technical disciplines, both imagery and signals, have much to offer our communities, the reality is that we process less than 10% of what we collect, and we disseminate roughly 10% of what we process (*ergo* we disseminate 1% of what we collect), and it is highly questionable as to whether the technical disciplines provide the return on investment that they should in comparison with either clandestine intelligence or open source intelligence. My detailed comments on the costs of secrecy is contained in my invited *Testimony and Comments on Executive Order 12356, "National Security Information"*, to the Presidential Inter-Agency Task Force on National Security Information, Department of Justice, 9 June 1994. For a related comment, consider the statement of Rodley B. McDaniel, then Executive Secretary of the U.S. National Security Council and a former Senior Director (White House) of the Crisis Management Center. Speaking to a senior executive service class at Harvard University, he stated: "Everybody who's a real practitioner, and I'm sure you're not all naive in this regard, realizes that there are two uses to which classification is put: the legitimate desire to protect secrets, and protection of bureaucratic turf. As a practitioner of the real world, it's about 90 bureaucratic turf; 10 legitimate protection of secrets as far as I'm concerned." As reported in Thomas P. Croakley (ed.), *C³I: Issues of Command and Control* (National Defense University, 1991), page 68.

[13] It was an enormous shock to me, while serving as the senior civilian responsible for the establishment of a new $20 million intelligence production center, the Marine Corps Intelligence Center, to discover that the $2 million per year we earmarked for a Top Secret Sensitive Compartmented Information (TS/SCI) computer system with direct access to data from the Central Intelligence Agency (CIA), National Security Agency (NSA), and Defense Intelligence Agency (DIA) proved to be virtually worthless. The analysts kept coming in

It is instructive. in thinking back to the early days of the Office of Strategic Services (OSS), to consider how very important the academics from the private sector were to the development of our analysis methods, and how very important open sources were to our strategic intelligence efforts. The anecdote about the price of oranges in Paris as an indicator of the effectiveness of our bombing attacks on the railroad bridges leading to Paris is a classic. In a more humorous and yet deadly serious vein, consider the story told by Miles Copeland, about how the OSS handled the innumerable requests from the Department of State and the Pentagon which did not merit clandestine collection.

The OSS put two men in a room with *The New York Times*. Anything that could be answered from this open source was typed up, stamped secret, and disseminated as the result of a highly compartmented human intelligence operation--and one which was ostensibly very expensive, hence justifying requests for additional funds. The information itself was not fabricated, only the purported methods of acquiring it.[14]

---

saying "there's nothing there but Soviet missile silo data, the Third World 'data fill' has not been done". I subsequently discovered that I could meet 80% of the intelligence requirements of the Marine Corps through the use of open sources, as a cost of roughly $20,000 a year expended in subscriptions to LEXIS/NEXIS, EasyNet, Jane's Information Group. and several other private enterprise information services. Our first major product. for which I served as Study Director, was an unclassified review of 69 countries of interest to the Marine Corps. Titled *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (Marine Corps Combat Development Command, March 1990). this product was unique for relying strictly on unclassified sources, and was embraced by the operational community because it a) asked them to define beforehand what they considered to be the key factors as well as the distinctions between high. medium, and low degrees of difficulty for each factor; and b) it could be easily shared with pilots and platoon commanders as well as coalition partners and the press. It was this experience that led to the subsequent Congressional interest and my launching of a public campaign--while still a government employee and with the approval of my General Officer--to radically realign resources between open and traditional sources of intelligence.

[14] Miles Copeland, *Without Cloak or Dagger: The Truth About the New Espionage* (Simon and Schuster, 1974), pp. 47-48. It was with great amusement that I listened to four recently retired KGB officers, speaking at OSS '93 on the topic of "Soviet Exploitation of U.S. Open Sources During the Cold War". To a packed room, they described how often "Centre" would catch them in the act of using open sources as a substitute for successful agent operations, and how open sources were in fact a mainstay of their Cold War scientific & technical collection efforts. Second International Symposium on "National Security & National Competitiveness: Open Source Solutions", Washington, D.C., 2-4 November 1993. The officers speaking were Colonel Vladimir B. Barkovsky. Ph.D. (former Deputy Director, KGB Science & technology Institute); Colonel Yuri I. Modin, Ph. D. (former Deputy Director. Research Institute on Intelligence Problems): Colonel Vsevelod I. Gapon (former

OSCINT has maintained a modest role within the larger intelligence communities, and a more central role within the smaller intelligence communities, but the reality is that the Anglo-Saxon intelligence communities of today exploit less than 10% of what is available from the private sector.

It is our task to explore the larger strategic context within which private enterprise intelligence can make a contribution to national security; to understand operational concepts from private enterprise intelligence which can and should be adopted by the traditional government intelligence services; and finally, to inventory, at this point in time, some of the specific private enterprise intelligence capabilities which can be used by the government to achieve both tactical results and sustained savings.

OSCINT and the Changing Threat

Others participating in this conference have addressed the changing threat and changing intelligence agenda, but I wish to outline here an intellectual construct which influenced my early appreciation of how poorly our intelligence community exploits private sector intelligence capabilities, and how relevant OSCINT is to the threats that have always been with us, but which are receiving a more appropriate degree of interest today.

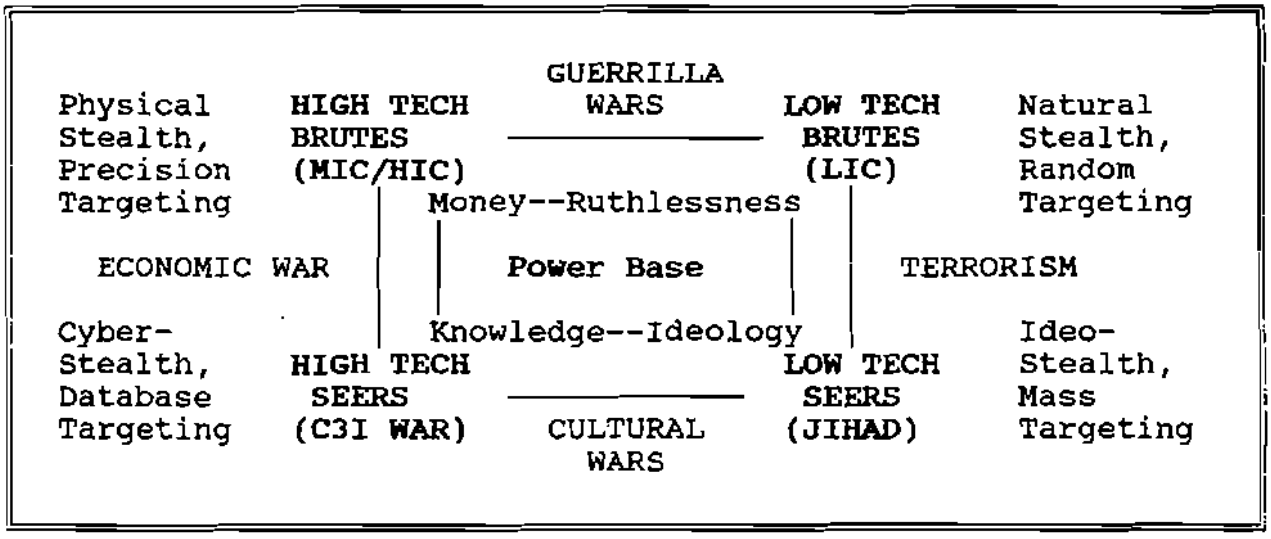


Figure 1: The Four Warrior Classes and Implied Intelligence Challenges[15]

Deputy Chief of Division, KGB); and Colonel Yuri H. Totrov (former KGB Section Chief for Counterintelligence, Central Intelligence Agency Affairs).

[15] This graphic is from my article "The Transformation of War and the Future of the Corps" in *INTELLIGENCE: Selected Readings--Book One* (Marine Corps Command & Staff College, AY 1992-1993). It is my privilege to continue serving the Marine Corps as Adjunct

While there are obviously variations to these four categories (for instance, some international criminals now use very sophisticated Swiss encryption and communications devices, as well as computer Van Eck emissions capture devices), these four categories helped me focus on the original threat--the high tech brute or conventional military opponent --while also keeping sight of the three major emerging threat categories.

What I perceive in this matrix is two fundamental aspects of national security and national intelligence:

a) First, since the National Security Act of 1947 which created the U.S. intelligence community, all that has followed has led to an intelligence community trained, equipped, and organized to deal with a single monolithic "high-tech brute", the Soviet Union, and very poorly trained, equipped, and organized to deal with smaller high-tech brutes, such as Iraq, or the other three major categories of threat. In particular, national intelligence capabilities in support of both international and domestic law enforcement, and economic competitiveness, are mediocre to non-existent.[16] We do not have the long-term ethnic human penetrations we need against international criminal organizations, nor do we have the kind of tactical SIGINT capabilities, or even air-breathing tactical IMINT, that would be helpful in coping with this robust international cancer.[17] We find that cultural movements baffler our

---

Faculty for Intelligence. My thinking was stimulated by Martin Van Crevald during his tenure as a Visiting Professor at Command & Staff College, and by his book *The Transformation of War* (Free Press, 1991).

[16] For a detailed critique of the existing U.S. intelligence community, a critique which draws on my years of service both in the Central Intelligence Agency as well as the Marine Corps, including participation in all of the post-mortems on intelligence failures in the Gulf War as well as Marine Corps support to the Department of Defense "reinvention of intelligence" initiatives undertaken by then Assistant Secretary of Defense for Command and Control, Communications, Computing, and Intelligence, Mr. Dwayne Andrews, see "A Critical Evaluation of U.S. National Intelligence Capabilities" in the *International Journal of Intelligence and Counterintelligence* (Volume 6, Number 2, Summer 1993). More recently I have summed up four years of critical commentary in "Reinventing Intelligence: Holy Grail or Mission Impossible?", in the *International Journal of Intelligence and Counterintelligence* (Volume 7, Number 2, Summer 1994).

[17] Until recently, very few traditional intelligence analysts were aware of the existence of the International Association of Law Enforcement Analysts (IALEA). This organization represents a first step in transferring some of the methods of analysis developed by the traditional intelligence community into the law enforcement arena. They can be reached at Post Office Box 52-2924, Miami, Florida, 33152, Voice: (305) 653-3010, Facsimile: (305) 716-3218. When I participated in reviews of intelligence effectiveness against low intensity conflict targets, one of the most critical deficiencies was the fact that our systems could not deal with "low slow singleton" targets. A major deficiency within the military is its

indications & warning (I&W) system because they do not use point to point communications but rely instead on couriers, the pulpit, and broadcast television to indirectly mobilize action elements from within the masses.[18] We do not have an electronic counter-intelligence capability worthy of the name, nor have we established the most basic economic counter-intelligence capabilities.[19]

b) Second, and this stems from a personal awaking inspired by the failure of our Marine Corps Intelligence Center's $10 million classified intelligence computing system and related classified databases, when contrasted with a $20,000 a year expenditure on private enterprise information sources and services, it is clear to me that OSCINT can meet 80% of our needs for intelligence against the emerging threats, and that OSCINT must be the foundation upon which we completely restructure our classified capabilities.

Now, there is going to be a natural tendency on the part of the "old boys" to say that OSCINT is all well and good, but not for critical national security issues. I have heard this from the best of them, including flag officers in England and France. I have also heard from flag officers in the U.S. and England, and officers in other countries, that they are fed up with classified intelligence that is relatively useless to their day to day needs, and highly interested in streamlining and improving their direct access to private enterprise information

---

propensity to procure "fast movers" (jets) with very limited loiter times over the target area, at the same time that they decline to invest in the necessary "sensor to shooter" collection and connectivity so that these expensive toys can be effective against low slow singletons targets.

[18] One of the finer pieces of journalism I have encountered was a superb series, each article taking up an unheard of full newsprint page or more, in *The Washington Post*. On Monday 2 August 1993 they published "Islamic Warriors: Radical Movements Thrive on Loose Structure, Strict Ideology", and a sidebar article, "Militarized Hezbollah Follows Lead on Iran". On Tuesday 3 August 1993 they published "Islamic Warriors: Global Network Provides Money, Haven", with a sidebar article on "A New Strain of Terrorism: Groups are Fast, Loose, Hard to Find".

[19] Many of my thoughts on information warfare, and information peacekeeping, are contained in my lecture "War and Peace in the Age of Information", presented by invitation to the Naval Postgraduate School at Montery, California, as a Superintendent's Guest Lecture on 17 August 1994. Among other controversial elements, this lecture outlines how I would completely neutralize U.S. military and civil capabilities through electronic attacks on ten specific targets. More recently my friend Winn Schwartau has published a superb book, *INFORMATION WARFARE: Chaos on the Electronic Superhighway* (Thunder's Mouth Press, 1994), a detailed review of the specific capabilities and threats associated with personal, corporate, and global information warfare.

sources.[20]

Let me offer just two short proofs. In 1991 over 100 senior officers, including ten Colonels from the Marine Corps (an unheard of investment for a single event from this

---

[20] For a current critique of the U.S. intelligence community by a prominent consumer, see former Secretary of State George P. Shultz's *Turmoil and Triumph: My Years as Secretary of State* (Charles Scribner's Sons, 1993), pp. 50, 297, 307, 312, 425, 492, 493, 595, 619 *passim.* One Marine Corps general officer has stated that he used to talk about intelligence being broken, until he realized that this implied it existed--in his view, national intelligence simply does not "exist" when it comes to supporting expeditionary military operations. I am fully familiar with the open source intelligence capabilities of the U.S. intelligence community, and in fact served as the Marine Corps member of the Open Source Intelligence Council until my resignation from the Corps on 1 April 1993. The Foreign Broadcast Information Service (FBIS) and the excellent scientific & technical intelligence capabilities developed by the National Air Intelligence Center (NAIC), the National Maritime Intelligence Center (NMIC), and the National Ground Intelligence Center (NGIC) all merit respect. Unfortunately, the U.S. intelligence community spends less than 1% of its budget on open sources (while admitting that open sources provide 40% of the all-source product), and is in my judgement tapping less than 10% of the private sector's capabilities. Among the obstacles to improved OSCINT are an archaic security system, a culture that thrives on secrecy rather than results, and a procurement system that makes it very easy to spend millions on hardware, while making it virtually impossible to subscribe to LEXIS/NEXIS or pay a consultant a quick $1,000. I am totally committed to protecting and improving the U.S. national intelligence community, and attempting to preserve its present level of funding, but in the absence of radical realignments among the disciplines and between collection versus distributed analysis, the community is in for some rough years. The first community attempt at defining its open source intelligence strategy was so disappointing, without reference to past studies or known experts, that I was obliged, as a Marine Corps civilian, to produce *United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations: Working Group Draft Dated 6 January 1992* (Headquarters, U.S. Marine Corps, 11 January 1994). The intelligence community finally appointed an Open Source Coordinator, Mr. Paul Wallner, to whom I am indebted for his integrity in supporting our private sector advocacy of open source intelligence developments; more recently Dr. Joseph Markowitz has been appointed Director of the Community Open Source Program Office (COSPO), with Mr. Wallner as the Deputy for this much-expanded effort. I have a very high regard for both of these gentlemen--but they are not being given the inter-agency authority and resource control they require to truly make OSCINT "the source of first resort", as Mr. Wallner has correctly defined it. I do not believe the U.S. intelligence community will truly restructure until it faces the real threat of a 50% (fifty percent) cut in its budget over five years, a threat which may well materialize in 1994 as an outcome of the newly established Warner Commission (formally known as the Commission on the Roles and Capabilities of the United States Intelligence Community).

austere Corps). met at the Naval War College in Newport for Technology Initiatives Game 1991. This game was a first effort to scrub Admiral Jerry Tuttle's COPERNICUS program. and included an Intelligence Cell. Here is a paraphrase of what the Navy Wing Commander (Captain, O-6) who led the lead flight into Baghdad said:

> *If it is 85% accurate, on time, and I can share it, that is a lot more useful to me than a compendium of Top Secret/Codeword information that is too much, too late, and needs a safe and three security officers to move it around the battlefield.*[21]

We in the intelligence community must be mindful of the acceleration of the operational tempo, and the fact that our consumers are not stupid. They are growing impatient with the ability of the intelligence community to "keep up". In the Gulf War the classified imagery cycle took eight days from articulation of the requirement to deliver of the imagery. The operational planning cycle was three to five days. Classified imagery was not only poorly suited for wide area surveillance, but it was always too late to be really useful. By contrast, you now have real-time imagery delivery from SPOT, and commercial synoptic one-meter imagery is a year or two away from reality. CNN is blanketing the battlefield, and although it is often wrong, it influences policy and operations. Commercial online services and international executive investigative services are offering astute consumers a degree of tailored intelligence support which is not available from the intelligence community for anyone other than the President or Prime Minister.

More recently, we have the instructive example of OSCINT in the war on drugs. Without belaboring the point, as an entire book will be coming out shortly on this topic, Los Alamos National Laboratory has demonstrated that for $100,000, using only OSCINT, it can do better at estimating global drug production and movement than an equivalent effort by the U.S. national intelligence community, at a cost of $12-15 million dollars.[22]

OSCINT and Changing Definitions of National Security

With the globalization of demographic and ideological movements, as well as the globalization of crime and the economy, the intelligence community is finding itself hard-

---

[21] Marine Corps Trip Report, Technology Initiatives Wargame 1991, Naval War College, 21-25 October 1991, disseminated by Assistant Chief of Staff, Command and Control, Communications and Computer, Intelligence and Interoperabillity, Ltr C4I2R dtd 3 January 1992.

[22] Dr. James Holden-Rhodes, *SHARING THE SECRETS: Open Source Intelligence and the War on Drugs* (forthcoming), extract from Chapter 5. This book has been selected for distribution at OSS '94, and 1,000 copies will be especially printed by OSS, Inc. one year in advance of the book's release to the public by the prospective publisher.

pressed to meet the needs of its consumers for intelligence about areas which have traditionally been excluded from its charter, such as strategic economic intelligence assessments which must of necessity draw on comparative domestic economic information: or support to law enforcement in its increasingly dangerous efforts to contain very powerful and very ruthless international criminal organizations with solid ethnic cohesion.[23]

It was instructive to me, in January 1994, to hear Ms. Ellen Seidman, Special Assistant to the President of the United States, discuss her responsibilities on the National Economic Council, and her perceptions of both intelligence and normal governmental information processes. In brief, she found the intelligence community irrelevant to her mandate because in the U.S. the intelligence community is not permitted to develop strategic assessments about domestic matters, even economic competitiveness matters. At the same time, Ms. Seidman expressed frustration with the normal governmental information processes, such as represented by the Federal Reserve Board and the Departments of Commerce, Treasury, and Labor, because the latter do not have any concept of how to collect. process, and disseminate intelligence. They don't "do" collection management. or critical analysis, or forecasting. or indications & warning. at the level of sophistication which our intelligence communities have developed over time.[24]

As we reinvent intelligence, there is clearly a need to reconsider not only our sources and methods, but the range of inquiry and the broadness of the consumer base. In my judgement the intelligence community must find a new balance between supporting more consumers with non-traditional requirements including domestic information requirements, while also relying on open sources and private enterprises to fulfill most of the encyclopedic intelligence requirements. The intelligence community. cannot, however, centralize its management of OSCINT, nor can it even presume to control what reaches the consumer. There is a strategic approach which must be taken to integrate government intelligence with private enterprise intelligence.

---

[23] Mr. John Petersen, President of the Arlington Institute (and former staff member of the National Security Council) defines national security in this way: "The Nation's security is no more than the total of the individuals' perceived sense of security (at home and abroad)." He uses a matrix from "Here to There" and "Peace to War" to show the broadening of national security concerns to include "Here" and "Peace" as major areas where both our defense community, and our intelligence community, are not prepared. Personal communications.

[24] Ms. Seidman was speaking to the Open Source Intelligence Lunch Club in Washington, D.C. on 11 January 1994. Her remarks were reported in ***OSS NOTICES*** Issue 94-001 dated 21 February 1994, page 10.

OSCINT and the Consumer

As we consider how best to integrate OSCINT capabilities from the private sector with both old and new classified intelligence capabilities, we must remain acutely conscious of the realities which characterize our consumer's acceptance and exploitation of information.

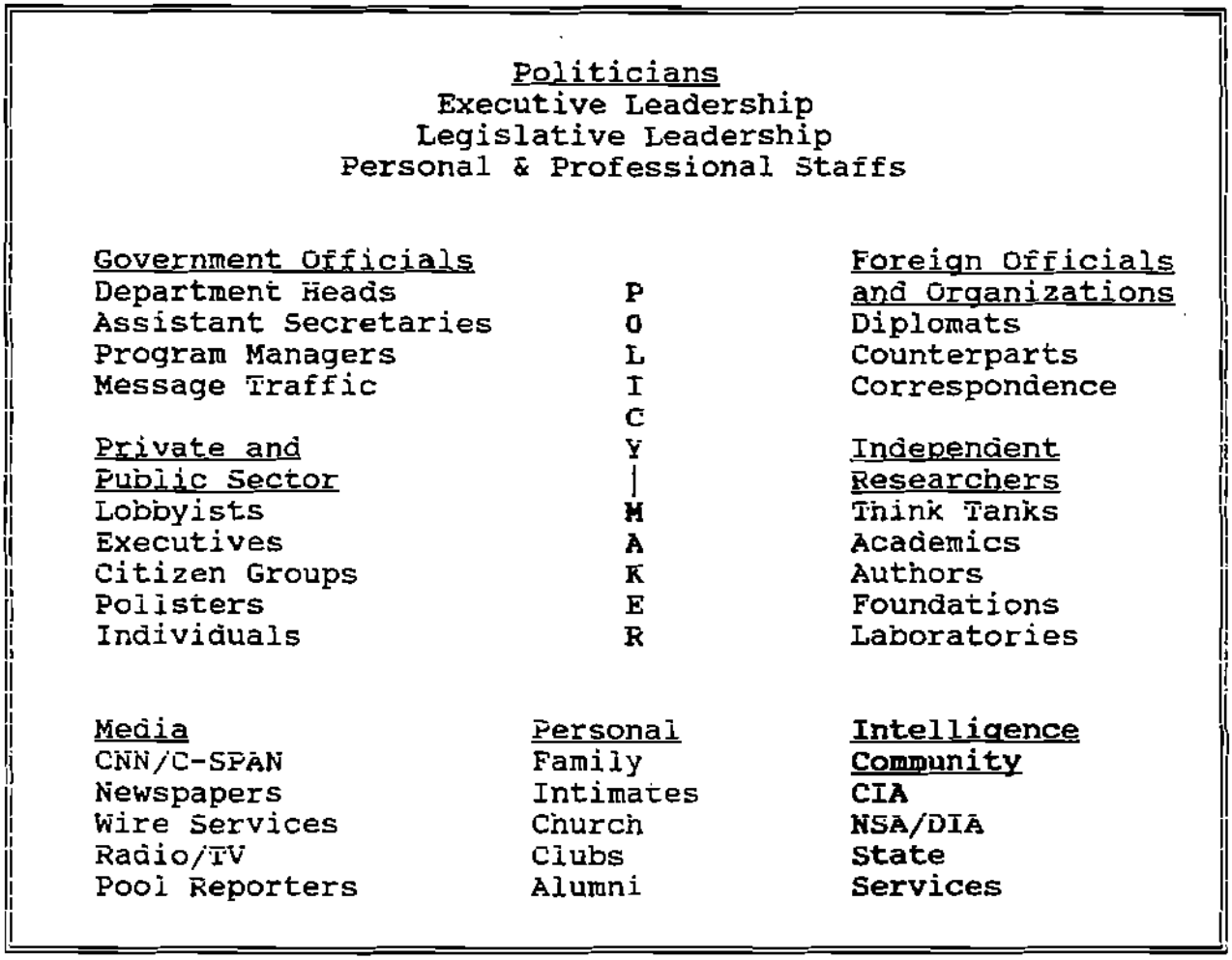


Figure 2. Competing Influences on the Policy-Maker

Consider the above figure, a graphic depiction of the range of "open sources" reaching the consumer each day, independent of the intelligence community:[25]

---

[25] This chart is reproduced from "A Critical Evaluation....", *supra* note 8, and in turn taken from the CIA "Intelligence Successes & Failures Course" which I understand has been discontinued. Dr. Jack Davis, Senior Intelligence Service, was for many years the keeper of the flame for "real world analysis", and the only senior officer willing to stand up to those who would politicize intelligence analysis and pretend that going through the motions constituted real intelligence. Others whose integrity and vision merit recognition including

a) Ninety percent of what the consumer reads and listens to is not only unclassified, but also unanalyzed and unrelated to the classified information sent to them.

b) There is no penalty to the consumer for ignoring classified information.

c) Classified information often comes with so much security baggage as to be an untenable contender for the policy-level consumer's attention (and the executive assistants do not have the codeword clearances, so even the consumer's filtering mechanism is of no help in flagging "useful" codeword material).

d) Unclassified material, even if inaccurate, if it fits the consumer's worldview or agenda, is immediately useful as something which can be disseminated to the press, the public, or Parliamentary personalities.

One of the most important changes the intelligence community can make, one which both addresses the potential as well as the hazards of unbridled open sources reaching the consumer directly, is to develop a much more extensive network of analyst-operators assigned to specific consumers and attending directly to their daily needs. Only through day to day interaction, and physical co-location, will such intelligence community representatives be able to a) monitor the OSCINT reaching the consumer, b) earn the consumer's trust and confidence; and c) properly channel requirements for timely action by the classified world, and d) "pull" exactly the right intelligence from the classified world in such a way as to be directly pertinent to the consumer's needs of the moment.[26]

---

the instructors for the Harvard "Intelligence Policy Seminar", notably Drs. Ernest May and Richard Neustadt, and in recent years, including the course I attended, Dr. Gregory Treverton (now Vice Chairman, National Intelligence Council). Mr. Doug MacEachin, the current Deputy Director for Intelligence (DDI) is a superb officer laboring under enormous constraints to improve intelligence analysis--as he has commented to a meeting of the Security Affairs Support Association, in paraphrase, "it is hard to do serious analysis when you have a bunch of 19-year olds on two year rotations". The entire concept of what constitutes the "value-added" role of national intelligence needs redefinition.

[26] The best article I have seen on how best to do intelligence analysis within the kind of competitive environment provided by OSCINT from private enterprises is that of Mr. Andrew Shepard, a senior analyst now on detail to the Community Management Staff (CMS). His "Intelligence Analysis in the Year 2002: A Concept of Operations", was published in the *Proceedings* (Volume I) of the First International Symposium on "National Security & National Competitiveness: Open Source Solutions" (McLean, Virginia, 1-3 December 1992), and is beginning to have an impact outside the United States. The paper was first presented at the Symposium on Advanced Information Processing and Analysis (Reston, Virginia, 24-26 March 1992). Mr. Shepard capably articulates how on-site intelligence analysts can fulfill three major roles in direct support of the consumer: real time validation and review of

The Strategic Context of Private Enterprise Intelligence

When we lost our way in the late 1950's, and fell in love with technology and the simplicity of a world with only one "main enemy", we built ourselves a cement bunker with no windows. In their time, satellites were like an oasis in the desert. However, in the past twenty years private enterprise information collection, processing, and dissemination alternatives have exploded--unfortunately, for those within the bunker, with its bad air and depleting supplies, it is difficult to notice such changes. It is a tribute to the organizers of this conference, and those behind them, that OSCINT is receiving a full and proper hearing in Canada.

The strategic context of private enterprise intelligence is a fundamental starting point for the reinvention of intelligence. There is no more promising aspect of our profession than that offered by the private sector. While we must assuredly pursue improvements in both clandestine and technical collection sources and methods, OSCINT--the private sector--must of necessity serve as both the "stopgap" measure by which we meet requirements for which our community is not trained, equipped, and organized; and also the benchmark against which we evaluate the value of clandestine and technical capabilities applied to new targets.

In the tactical section which concludes this paper I provide examples of specific private enterprise information-intelligence capabilities from each of the above. At this, the strategic level, I wish to make three points:

a) First, the consumer is now in charge, and acutely conscious of the advantages which OSCINT provides, not only in terms of responsive information at a very low cost, but in terms of political advantage....OSCINT can be shared with the press and Parliament, and therefore is much more politically potent than a secret report which cannot be shared.

b) Second, this is the age of distributed information. It is simply no longer possible to centralize control over collection, storage, processing, and dissemination. I have stated publicly my view that the "Central" Intelligence Agency is not long for this world--that is not to say that we do not require its capabilities, simply that the way in which it is now organized and managed is so ineffective and inconsistent with the realities of today, that it must inevitably join the mammoths in the tar pit.[77]

OSCINT reaching the consumer independent of the intelligence community: real-time retrieval from intelligence community databases of that information which can be tailored to support an imminent decision by the consumer; and collection management tailored to the needs of the consumer rather than the circumstances of the collectors.

[77] My most detailed statement on where I see the U.S. intelligence community developing, to include the dissolution of the Central Intelligence Agency (and the establishment of a separate Clandestine Services Agency) is contained in ***OSS NOTICES***

c) Third, it is simply not advisable, for both political and financial reasons, to render classified intelligence support to private enterprise with any consistency, or with an assured return on investment. In coming to this conclusion I draw on my participation in a special workshop within the Harvard Executive Program on Intelligence Policy (1991).[28] There is no question but that classified economic espionage is required to "illuminate the playing field" for the governmental policy maker. However, given the fragmentation of ownership, management, and employment of most international firms, defining a strictly American or strictly Canadian firm meriting the expenditure of taxpayer funds for classified intelligence becomes problematical. What I found most interesting, though, in thinking about this issue with my classmates, was my personal conclusion that the single best thing the government can do for national competitiveness is to nurture the growth of what Lee Felsenstein calls the

---

Volume 2, Issue 6, 30 August 1994). Among the highlights: dissolution of the Central Intelligence Agency; establishment of a separate Clandestine Services Agency (CSA) under total non-official cover; conversion of the Directorate of Intelligence into the cadre for an inter-agency series of intelligence centers under the oversight of the National Intelligence Council; creation of Deputy Directors of Classified Intelligence for Research & Development, and for Communications & Computing; integration of the National Reconnaissance Office (NRO) with the Defense Mapping Agency (DMA) to create a Defense Mapping & Reconnaissance Agency which contracts out 75% of its collection and production; expansion of the National Security Agency (NSA) charter to include monitoring of unencrypted cyber-space data and the establishment of a clandestine capability for inserting alternative transmitters into sites using unbreakable encryption; and expansion of the Defense Intelligence Agency (DIA) to manage a totally integrated Intelligence Corps which provides the military intelligence personnel to all military elements from the forward-most tactical element through the Joint Intelligence Centers (JIC) and into the Pentagon. A superb book on emerging governance principles for distributed networks is that of Kevin Kelly (editor of *WIRED Magazine*), *OUT OF CONTROL: The Rise of Neo-Biological Civilization* (Addison-Wesley, 1994). One of the concepts which Kelly articulates is that of "hive mind". In my own work I am pursuing ideas once articulated by Teilhard de Chardin and Quincy Wright, among others, with respect to what constitutes an "intelligent nation". I envision a "virtual intelligence community" which is 100 times larger and more encompassing than the existing intelligence communities; while such a community must by definition be "out of control", it is in fact far more effective and responsive to the needs of our consumers than the existing government intelligence communities (and their non-intelligence uninformative counterpart agencies).

[28] This course, sponsored by the Central Intelligence Agency, brings together approximately thirty general officers and their senior civilian counterparts, each at a point where they are about to manage the entirety of their organization's intelligence resources. As the second civilian in the very small Marine Corps intelligence pond, I benefitted from this opportunity around eight years earlier than I might have in a larger organization.

"information commons" of open source multi-media data.[29]

Let me expand on this concept for a moment. Our own Deputy Assistant Secretary of Defense for Intelligence and Security, Mr. Keith Hall, has stated clearly that while intelligence must of necessity rely on OSCINT for context, that intelligence is intended to collect secrets not available "by other means", and that OSCINT falls firmly within the category of "other means".[30] What we have here is a dilemma. On the one hand, we want the intelligence community to focus on secrets. On the other hand we have to keep the policy-maker informed, and find that 80% of the time OSCINT is better at informing policy than are secrets. What I believe we need is a new strategic definition of what constitutes "national intelligence"--our definition must provide for a distinction between classified governmental intelligence and unclassified private enterprise intelligence, while also providing for the integration of both under the national intelligence umbrella.

The isolation of the intelligence community from its consumers, and the arrogance of the intelligence community in presuming that it knows best who its consumers should be, and that it knows best whether secrets are better than open sources in any given instance, must be brought to an end.

In essence, it is not enough for the government to simply understand and take advantage of private enterprise intelligence. It is essential that the government have a national information strategy, and that it nurture what I call distributed centers of excellence. It is not enough to expect that the private sector will undertake the necessary collection and processing that is required--government must actively encourage, without controlling, such endeavors, and constantly monitor the state of its national information continuum.[31]

---

[29] Lee works at the Interval Research Corporation in Palo Alto, California, and can be reached at (415) 354-0857, fax (415) 354-0872, email <lee@interval.com>. Interval is Paul Allen's attempt to create a modern Xerox Parc.

[30] Mr. Hall provided his first public address on the relationship between intelligence and open sources to the Open Source Intelligence Lunch Club in Washington, D.C., on 9 August 1994. Mr. Hall, whose rich experience at the tactical level in military intelligence and at the Office of Management and Budget as well as on the Senate Select Committee for Intelligence makes him one of the most qualified senior leaders in our community, was the originator of the term "ASK-INT", and has over the past decade challenged intelligence collectors to determine if the information they want to use expensive methods to collect might not in fact be available for the asking.

[31] In the United States, the National Information Infrastructure (NII) was until recently focused strictly on connectivity. It was with some gratification that I finally heard him speak of the need to harness the "distributed intelligence of the Nation", a phrase I used in my address to OSS '94. He used this phrase when announcing the GII in Brazil, and again at the Public Interest Summit in Washington, D.C. on 29 March 1994.

Below I illustrate what I call the "information continuum". It is very important to note that the intelligence community is but one ninth of that continuum, and that existing security and procurement practices assure the complete isolation of the intelligence community from the other eight sectors. If one regards the intelligence community as the pinnacle of the national information continuum, then the most interesting aspect of reinvention is that associated with new responsibilities for the community--instead of simply collecting information and processing it in a centralized way, the community must now begin the process of nurturing distributed networks which are unwitting or benignly witting, and most assuredly not "under control".

What I call the "information continuum" is the knowledge terrain within which government intelligence and corporate intelligence must operate:

K-12	Libraries	Private Investigators Information Brokers	Government	Intelligence
Universities	Businesses	Media	Defense	

Figure 3: The "Information Continuum" or "Virtual Intelligence Community"

It consists of our elementary and secondary schools, our universities, our libraries, all businesses and their information repositories, private investigators and information brokers, the media including the trade journal and scientific & technical media, governments down to the state and local level, all defense and law enforcement organizations, and the official and usually secret intelligence communities. I call these the nine sectors of the information continuum.

IF we can harness this distributed power, then we can create a "virtual intelligence community" far more capable than the isolated communities now in existence.

The good news is that this continuum provides a low-cost, flexible, and responsive "virtual research department" of extraordinary power and value. The bad news is that very few people know how to navigate this terrain, or how to break down the iron curtains between sectors, the bamboo curtains between industries, the plastic curtains between individuals.

In order to bridge the gap between what we have in the "real" intelligence community today, and what we might have in the "virtual" intelligence community of tomorrow, a national information strategy is an essential pre-requisite. Whether through legislation or through administrative fiat, there must be a concerted effort on the part of the government to harness the "distributed intelligence of the Nation".

In addition to the connectivity that comes with the National Information Infrastructure (NII) and its international extension, the Global Information Infrastructure (GII), three other elements are required to fully harness private enterprise intelligence:

a) There must be, fully independent from the intelligence community[32], a National Information Foundation (NIF), modeled after the National Science Foundation (NSF), which nurtures distributed centers of excellence without attempting to control them or their content.

b) Expenditures for information research and development (both tools and content) must be coordinated to avoid duplicative or counter-productive investments (e.g. every major bank commissioning a separate market survey on Indonesia, or development of a desktop analysts' workstation).

c) Communications & computing security must be assured through national standards, testing & certification laboratories, due diligence legislation, and national education.[33]

In brief then, while the private sector provides a very robust foundation for reinventing intelligence, and private enterprise intelligence can today be exploited well beyond what the intelligence community is doing, only a national program and a national strategy which explicitly recognizes the distributed nature of private enterprise intelligence, and seeks to harness it, will yield the optimal value for national security and national competitiveness.

---

[32] There is no avoiding the fact that most private enterprises, be they commercial or academic, will simply not trust the intelligence community to "manage" or "control" their databases or their activities. The best way to harness the distributed power of the private sector is to create a National Information Foundation (or Institute) which is non-regulatory and distributes funds (rather than centralizes information) to "centers of excellence" chosen because of their focus on specific regions or topics of interest to the government. This would be a non-intrusive means of orchestrating capabilities. OSS, Inc. is in the process of obtaining from every U.S. Senator and Representative their nominations for centers of excellence in their respective States and Districts, as a pre-amble to publishing the first national inventory of centers of national intelligence excellence in the private sector.

[33] Although I have had very good relations with major hacker groups since 1992, when they recognized me for "hacking the intelligence bureaucracy", it was not until this past year that I realized that absolute private security was an essential pre-condition to complete openness. In order to engender the kind of open exchanges that are needed in a distributed intelligence system, it is essential that individuals feel that they a) know who is on the other end with some certainty; b) will receive the original document without modification; and c) can rely on a digital cash payment being transferred if that is part of the exchange. It was this realization that led me to oppose the Clipper Chip, and to testify to the NII Security Committee on 15 July 1994.

Operational Concepts, Policies, and Practices

At the operational level, which deals with top-level guidance of over-all intelligence efforts, rather than the specific research tasks common to the tactical level, I want to highlight some core concepts where I believe that the private sector is ahead of the intelligence community.[34]

Decision-Support is the only acceptable mission for intelligence. One must carefully distinguish between *data*, which is the raw text, image, or signal; *information*, which is collated data of generic interest, such as newspapers or research reports; and *intelligence*, which is information that has been tailored to support a specific decision by a specific person about a specific topic at a specific time and place.[35]

Collecting Secrets is not difficult if you focus on collecting them before they become secrets. The weakest link, and the cheapest and easiest to exploit, is the grey literature and human infrastructure responsible for doing research just before someone decides to label something proprietary or classified.[36]

Cast a Wide Net. The French steel industry worked very hard at competitor intelligence against other steel industries, and completely overlooked the plastics industry.

---

[34] Both the operational concepts and the tactical specifics which follow were developed for my keynote presentation to the Association for Global Strategic Information (AGSI) in Heidelberg on 14 June 1994. That speech, oriented toward strategic planners and senior executives in international business, was printed as "ACCESS: Theory and Practice of Competitor Intelligence", *Journals of AGSI* (July 1994). Both sections have been revised, to include alteration of some of the tactical elements, in order to be more meaningful to a government intelligence community audience.

[35] When I first began developing new concepts for analysis in order to make the very austere Marine Corps Intelligence Center as effective as possible, I undertook a review of all CIA and DIA production available to the Marine Corps from the preceding year. I was intrigued to discover that almost nothing produced by either of these two organization actually supported any specific decision. It was all classified information of generic interest, and of a broadcast nature. I also found that almost all the production focused on a specific topic, weapons system, or country, rather than producing strategic generalizations helpful to long-term assessments and the formulations of strategic plans.

[36] For a detailed articulation of my theory and practice of OSCINT, see "ACCESS: Theory and Practice of Intelligence in the Age of Information". This was prepared for a foreign government which is among the most advanced in exploiting legal and open sources and methods in support of its national competitiveness. The paper was published in Volume I of the *Proceedings* of the Second International Symposium on "National Security & National Competitiveness: Open Source Solutions" (Washington, D.C., 2-4 November 1994).

which was busy developing steel substitutes.[37]

Openness versus Secrecy. The openness paradigm has won. The example of the nuclear industry, based on secrecy and not very progressive, is instructive when compared with the openness of the electronics industry, where competing engineers compare their approaches over coffee.[38]

Just in Time versus Just in Case. Paul Evan Peters, Executive Director of the Coalition for Networked Information, makes the point that in the age of distributed information easily accessible through electronic connectivity, it makes no sense to store volumes of out-of-date information when you can reach out and get exactly what you need in the way of current information on a "just in time" basis.

Leverage Everyone Else's Overhead. An expansion of the above concept is that of avoiding the enormous costs of attempting to maintain, with limited sustainability, in-house experts and in-house archives on everything. The private sector contains many superb information and intelligence capabilities where the resident expertise, and the existing databases, are maintained at someone else's expense. The intelligence community must do a much better job of exploiting such centers of excellence. *The most important contribution these external elements can make is not as a substitute for in-house analysis and the final production of an integrated classified product, but rather as self-sustaining information filters and on-demand experts able to rapidly identify the latest and best multi-media information pertinent to a specific decision area--information that can then be rapidly acquired, evaluated, and integrated.*[39]

---

[37] I heard this marvelous anecdote from Mr. Herve Serieyx, Vice President of the Institute for European Leadership, as included in his address to the French information industry congress, IDT '93, in Paris during the month of June 1993.

[38] Mr. John Perry Barlow, Co-Founder of the Electronic Frontier Foundation, articulated this contrast during his address to OSS '92.

[39] Early on in my OSCINT advocacy days, I suddenly realized that too many of my former colleagues were confusing my advocacy of OSCINT as a foundation for all-source intelligence with a view--which I do not support--that OSCINT can do it all or can substitute for clandestine and technical collection. I am fond of the analogy that Dr. Joseph Nye uses (he was until recently the Chairman of the U.S. National Intelligence Council). Dr. Nye talks about the intelligence problem as a jig-saw puzzle, and of open sources as the outer pieces of the puzzle, without which one can neither begin nor complete the puzzle. Clandestine and technical collection comprise the inner pieces. Dr. Nye would probably agree with my proposition that open sources have become a larger part of the solution in recent years--he might be reluctant to agree with my proposition that one often does not need the classified pieces in order to make a decision, and that in fact the maintenance of operational momentum is often is direct contradiction to the intelligence community's

Diamond versus Linear Paradigm. The old paradigm for information acquisition is the linear model, where the consumer goes to the analyst who goes to the collector who goes to the source, and then back up the chain the answer goes. This paradigm is not only too slow, it is not workable when you have a fast-moving topic with lots of nuances that are difficult to communicate to intermediaries. The new paradigm is the diamond paradigm, where the consumer talks to the analyst, the collector, and on many occasions the source, in order to ensure there is a timely and accurate meeting of the right minds[40]

CIO = Corporate Intelligence Officer. The last person corporations should appoint to the CIO position is the oldest information systems expert. They are technicians and do not have the slightest understanding of corporate strategy and the needs of senior executives for real-time *content* displayed in meaningful ways. The CIO position should not only be responsible for ensuring that the entire corporation--every employee--serves as part of the collection network, but also for ensuring that the information in hand is exploited, and that the corporation has the broadest possible network of external collection and processing capabilities on demand. The CIO should be the intelligence community's primary point of contact for legitimately and openly exchanging unclassified information.

Information Value: content + context + time. Corporations and banks have a wealth of information that is rotting away unused rather than being bartered or made available to one another as a means of increasing the competitiveness of an industry or a country. If

---

propensity to delay and delay in the hopes of getting a perfect answer. In forming my judgement on what best meets the need of my military commanders, I am influenced not only by many discussions with officers at the Warfighting Center of the Marine Corps, but also by Brigadier Richard E. Simpkin's excellent book, *Race to the Swift: Thoughts on Twenty-First Century Warfare* (Brassey's, 1985).

[40] I developed this concept while considering how relationships have changed between consumers, analysts, case officers, and clandestine agents. Those that do not actually understand the capabilities and limitations of clandestine intelligence frequently fall victim to the myths of clandestinity, and fail to understand that both agents and case officers are human. Too often, an agent will fabricate information or take information from open sources and pretend it comes from a "third cousin working for the Foreign Minister" to avoid any appearance of diminished access, and too often, a case officer will accept a fabricated answer either for lack of time to validate the information, or out of naivete. The number of case officers that do not read the local press or understand the local language at a level of competence sufficient to detect nuances and dissembling is distressing. Now, with so many open sources and so many experts being brought "on line" through the Internet and other means, it is my view that the role of the analyst is changing dramatically. Instead of evaluating analysts on the basis of their ability to master a limited amount of classified data, we must now begin training our intelligence analysts, and evaluating them, on the basis of their ability to identify and exploit an almost infinite range of external human sources.

one understands that stripping information of time and context allows it to be bartered without losing a competitive advantage, while gaining additional information in the process. then the way is open to operational-level agreements which will increase an individual firms competitiveness as part of a larger consortium. The intelligence community should be the catalyst for a national program to inventory existing information that is in storage or available through private enterprise collection networks, and then devising means of accelerating the transfer of basic information to the information commons.[41]

Information-Driven Actions are better than mission-driven actions. Many corporations as well as government organizations appear to be mired in old organizational practices where a business unit is given a specific series of tasks to accomplish, and is then expected to accomplish those tasks over and over again without reference to the external environment or other elements of the corporation.

Corporate Hive. Every employee is a collector, producer, and consumer of intelligence. Drivers of delivery vehicles, service technicians, those responsible for cold calls on customers, all should receive special training in observation and elicitation, and should have easy to use channels and processes for reporting what they see and hear. At the national level, the concept of "national hive" merits pursuit.[42]

In brief, then, we must think of each organization within the information continuum as an information network, with each citizen-employee being in turn responsible for exploiting those external information networks that they come in contact with--quite literally, <u>everyone</u> becomes a collection and producer of intelligence.

<u>Private Enterprise Intelligence--Tactical Opportunities</u>

Now here are some tactical specifics--these are representative examples of capabilities that you could be using today--if you are not, you simply are not getting the best private intelligence possible.

---

[41] This concept of value probably owes something to a number of readings in cybernetics, but no single reading stands out. It was articulated in my paper on "ACCESS:....", *supra* note 25.

[42] See Kevin Kelly, *supra* note 16, *passim*. Kelly's book will be hard going for the average intelligence officer, but at the management level it is well worth the effort. The concept of gaining control over a $500 billion a year private enterprise intelligence continuum by <u>giving up control</u> of the fraction of intelligence resources necessary to nurture distributed centers of excellence is one that will be difficult to accept for the current generation of senior intelligence managers, but one that will inevitably be implemented within the next five to six years by the incoming leadership.

I want to stress that reliance on a single provider of private enterprise intelligence and information services is no better than having an in-house capability--the greatest returns on your investments in tactical intelligence will come when you have the ability to "mix and match" sources and services from across the entire information continuum, hiring the very best experts on very narrow topics for only as long as needed, but with the assurance that the information they provide is first-hand, in-depth, and not only current, but in fact ahead of the published record.

It is also important to note that the non-profit arena, and particularly libraries, are discovering that they can exploit existing infrastructure, and cheap student labor, to compete with commercial online services. Across the information continuum, capabilities and limitations are in flux, with new and lower cost capabilities emerging every day.

INTERNET	Tony Rutkowski Internet Society (703) 648-9888	Brewster Kahle WAIS, Inc. (415) 327-9247	Chris Berendes Internet Navigator (202) 543-1527
UNIVERSITIES	Geoffrey Fox Syracuse "InfoMall" (315) 443-1722	U. of Michigan Clearinghouse <lou@umich.edu>	Economic BBS Rice University (313) 764-9366
LIBRARIES	Brenda Bailey Uncover Reveal (303) 758-3030	David Bender Special Libraries A. (202) 234-4700	Charles E. Bailey Jr Lib.-Oriented Lists (713) 743-9804

Figure 4: Basic "Intelligence" Capabilities in the Non-Profit Arena

Tony Rutkowski, Executive Director of the Internet Society, also oversees publication of a professional journal loaded with information about resources on the Internet, and understands better than most the technical issues associated with making global information available to any business. I am a member of the Board of Advisors of the Internet Society, and one of the things I am encouraging is a new focus on distributed content--on establishing a structured understanding of what comprises the "virtual library" or "virtual university" which is connected by Internet links.

Brewster Kahle, formerly with Thinking Machines, is the genius that invented the Wide Area Information Server (WAIS), which is now a standard for rapidly searching the entire Internet for weighted (relevancy ranked) full text documents. Brewster can tell you what businesses are doing to take advantage of the Internet, including their collection and search strategies. WAIS, and now the World Wide Web, enable an intelligence organization to constantly assess what is available on the Internet for any given topic, and to rapidly access

specific documents *and specific subject-matter experts.*[43]

Chris Berendes is a Master Inter-naut whose specific expertise is seeking out scientific & technical information of business value from all over the Internet.

One comment on the Internet: it eats people. It is much better to have a single Internet specialist, or to contract out searches, otherwise employees run the risk of either becoming hopelessly lost, or hopelessly addicted to wandering in cyberspace.

Geoffrey Fox is the man behind Syracuse University's "InfoMall". This is a good example of a university recognizing that it can substitute support to business for declining students as a source of revenue. He provides multi-media "intelligence" to businesses.[44] It is

---

[43] The economics of information, and the protocols associated with "tapping into" distributed expertise, are in great flux. Among those who are well-established within the Internet community, there is an understood barter economy as well as understood rules of behavior which preclude blatant exploitation (or even imposition of traffic upon) acknowledged experts. One of the most inconvenient things to happen to me is to have been listed in a new book, *E-Mail Addresses of the Rich and Famous.* While I am neither rich nor famous, my status as a former spy led to my being exploited by the publishers of this book, with the result that I must now deal with inquiries from people who have nothing better to do than send electronic mail to people they do not know. My rule of thumb is that I will give serious inquiries one free response--after that I charge $200 an hour. Once small digital cash exchanges become a matter of routine on the Internet, I anticipate much more *ad hoc* consulting and self-publishing. One of the reasons that TELTECH and BEST America are doing so well is that they provide three essential services: they pre-screen experts for quality; they obtain non-disclosure agreements; and they handle billing and compensation. The private sector can be expected to develop many more clearinghouses and "expert on demand" capabilities meeting the needs of the intelligence community.

[44] Although intelligence communities have in the past exploited their universities, largely through directed contracts funded, in the United States, by "External Research & Analysis" (ER&A) funds, with the fiscal decline these funds have been among the first to be cut, a strategic error on the part of intelligence community management. It is far more productive to cut vertical slices of classified programs than to further distance the intelligence community from private enterprise intelligence capabilities. At the Advanced Information Processing and Analysis Steering Group (Intelligence Research and Development Council) Symposium in March 1993, one senior intelligence community officer lamented the fact that 80% of the information technology dollars go to maintenance, and that the installed base is dragging the whole program down. That is precisely the problem--the community needs to transition from an era of large centralized installed bases, and into an era where a core of dedicated analysts with the finest possible tools exploit private enterprise intelligence capabilities to the fullest extent possible--and only if the private sector cannot to meet the consumer's needs, should a

also a good example of how shared computing resources, and part-time university talent, can meet needs which the business and government communities might not be able to afford on a "full-time" or dedicated basis.

University of Michigan Clearinghouse for subject-oriented Internet resources is a classic example of graduate students doing something useful for the business community. Among the directories they have prepared are ones for aerospace engineering, government sources of business and economic information, and so on.

Economic Bulletin Board Service operated by the University of Michigan provides a number of useful files including statistical information, press releases from the U.S. Trade Representative, defense conversion information, East European trades leads, and so on.

I am convinced that universities, especially now that they are confronted with declining student populations, have a very important role to play in the provision of practical tactical intelligence support to corporations and governments. Adopt a university in order to harness the brainpower of their graduate students, and the connectivity and power of their electronic resources.

Brenda Bailey at Uncover Reveal is the tip of the Colorado library association that may put some of the commercial online services out of business. They are using existing library overhead to index and abstract, and then supporting their library services through on-demand faxing of materials for which fees are charged. Here is a simple example of their service: they distribute, at no cost via the Internet, the tables of contents of the journals they process. Any intelligence community analyst can receive, for free, exactly those tables of contents that are of interest to them--and they can either order copies of articles of interest from their government library, or--perhaps more efficiently, at a nominal cost from the University of Colorado.

Special Libraries Association takes care of the many corporate and academic special libraries, and in essence nurtures a wealth of information that is not mainstream but is very much at the heart of our national competitiveness. They are the private intelligence service for esoteric issues. They have been in existence for over 84 years, and specialize in helping librarians tap into international corporate libraries and other specialty collections.[45] The

---

revitalized clandestine or technical intelligence capability be called upon.

[45] One of the things that most impressed me during my March 1994 visit to Singapore, where I was welcomed by the National Computer Board (27 years olds with 140+ Intelligence Quotients, acting as a very effective shadow government), was their strategic plan to link government databases in the near future, *followed shortly by the linking of banks and private enterprise databases*. Obviously proprietary information and multi-level security issues will have to be sorted out, but I fully expect Singapore to be among the first three

Canadian equivalent of this organization should be an integral part of the national strategy for harnessing the enormous power resident in corporate libraries and databases.

Corporate and other private libraries are a critical national resource, and there should be a national program which facilitates "inter-library loan" sharing, as well as digitization of materials of common interest. My friend Paul Strassmann developed the concept of Corporate Information Management (CIM).[46] CIM means "one time data entry, corporate wide access". I have extended this concept to include National Information Management (NIM) and Global Information Management (GIM), and am convinced that the next major advance in the intelligence field will be the development of robust unclassified burden-sharing arrangements between governments and their private sector partners, and between governments acting on behalf of their private sectors....and of course in the private sector there are already numerous strategic alliances for information sharing.

Library-Oriented Lists on the Internet were put together by Charles E. Bailey, Jr. He is Assistant Director for Systems, University Libraries, University of Houston. He is Co-Editor of *Advances in Library Automation and Networking*, and Editor-in-Chief of *The Public Access Computer Systems review*. He understands the role libraries have to play in national competitiveness, and the importance of networking.

BASIC PRIVATE INTELLIGENCE	David Young Oxford Analytica +(44 865) 244-442	WONG Chiu-Yin *Economist* Intel Unit (212) 554-0600	Joseph Casitore FIND/SVP (212) 645-4500
ADVANCED PRIVATE INTELLIGENCE	Ruth Stanat SIS International (914) 639-1934	Herb Meyer RWI, Inc. (206) 378-3910	Dick Klavens SCIP (215) 896-4859
PRIVATE INTEL CONSUMERS AND EXPERTS	Olga Staios LEXIS/NEXIS (513) 865-7312	TELTECH Experts on Demand (612) 829-9000	BEST America Experts on Demand (410) 563-2378

"smart nation-states" in the world.

[46] Mr. Paul Strassmann is perhaps best known for his recent service as Director of Defense Information in the U.S., where he managed the world's largest information empire. Previously he has served in a number of executive positions, including Chief Information Officer of the Xerox Corporation. Among his recent books pertinent to the creation of national information architectures are *Information PayOff: The Transformation of Work in the Electronic Age* (Free Press, 1985), *The Business Value of Computers* (The Information Economics Press, 1990), and *The Politics of Information Management: Policy Guidelines* (forthcoming).

Figure 5: Core Business/Economic Intelligence Capabilities

David Young founded Oxford Analytica, and this is, in my judgement, the finest global intelligence service that is open and private. He was a National Security Council staffer with Kissinger, and decided he could do better than what CIA was providing to the President. He enlisted the Don's of Oxford, and now provides the business community with daily intelligence and special reports that have earned praise from the World Bank and others. *Oxford Analytica runs 750 legal, overt human assets world-wide, trimmed down from an original 2,500 contract assets.*[47]

WONG Chiu-Yin runs *The Economist* Intelligence Unit, based in New York. They provide intelligence reports and special consultations to businesses world-wide, and there is a good reason why they are called an Intelligence Unit.

Joe Casitore is the Vice President for New Business Development at FIND/SVP in New York. This international firm will obtain any published document, including what we call gray literature (documents published in limited numbers by private parties, but not classified or proprietary). FIND/SVP also runs an "ask any question" service that is mainstay of the private intelligence business, and it has a strategic research division.

Ruth Stanat represents the best of the new private intelligence breed. She has an international company with correspondents all over, and she does a very fine job of both market research, and forecasting. Together with Herb Meyer and Kirk Tyson in Chicago, Ruth is among the best in the privatization of intelligence. David Young is my hero because he has a network of 750 agents worldwide, and does intelligence every day about every topic; Ruth does research on demand, but I believe she is a great deal more competent and more trustworthy than most private detectives and more globally tuned in than many information brokers. Ruth is also the author of the excellent book *The Intelligent Corporation: Creating*

---

[47] Every morning, the staff of Oxford Analytica meets, bringing together its area officers (one for each major region) with a changing mix of Dons. The area officers come to the morning meeting after a lengthy review of all over-night wires and news services. In collaboration with the Dons, they ask and answer three questions: a) where is the news wrong, and must be corrected for our clients? b) where is the news right, and must be elaborated upon with technical or other detail for our clients? and c) what weak signals are we starting to detect, that might allow us to make a useful forecast of coming changes for our clients? After deciding what issues to address that day, a limited number of their world-wide human network are mobilized. A typical example: a Chilean economist, friends with the Minister of Trade, is asked for a report. Within four hours he provides a two page report suitable for a President or Prime Minister, based on direct sourcing to those in positions of power. The World Bank complimented Oxford Analytica in writing, for being the only private enterprise to correctly forecast economic developments in Russia when it was transitioning from Gorbachev to Yeltsin.

a Shared Network for Information and Profit.

Herb Meyer is a good example of a "private spy" (in the new sense of legal open intelligence, not the old sense of industrial espionage). He was editor of *Fortune*, then Vice Chairman of the National Intelligence Council, and is now CEO of Real World Intelligence. Inc. He is the author of author of *Real World Intelligence: Organized Information for Executives*. Herb is a success story, and has translated lessons learned in the classified intelligence community into a competitive advantage in the private sector.

Dick Klavens is the President of the Society of Competitor Intelligence Professionals (SCIP). These are the people around the world whose specific job it is to collect, process, and disseminate corporate intelligence. They are the "in-house" managers of corporate-wide collection plans, cross-business unit intelligence sharing, and--when needed--the hiring of external information brokers, telephone surveyors, and the occasional (rare) private investigator. Their annual symposium, together with that of the Association for Global Strategic Information (AGSI). and that of the Association of Information and Dissemination Centers (ASIDIC), as well as my own, are "must attend" events for anyone who wishes to be follow the latest open sources & methods in the information age.[48]

LEXIS/NEXIS, besides being a good all-around tool for research, is a good way of identifying experts and finding those journalists and professionals who are thinking about publishing the latest developments in specialized areas of interest.

TELTECH Experts on Demand are part of the private intelligence community, but they can also tell you about their customers. They have 3,000 technical experts on call. and can put a customer in touch with one over the telephone, with the result that "real-time intelligence" is produced when needed.

BEST America is similar to TELTECH, only they have 40,000 experts on line, and specialize in the life sciences. Pharmaceutical companies pay serious money to be able to reach out and tap into very narrow expertise on a moment's notice and with the assurance of total discretion.

---

[48] SCIP's symposium, including a number of excellent pre-conference tutorials, is generally held each April, and moves from city to city and attracts 500-700 participants. SCIP is actively expanding its international membership. AGSI meets in Europe and attracts 50-100 corporate strategic planners and business intelligence specialists. ASIDIC meets twice annually in the U.S. and attracts 50-100 of the leaders of the U.S. information industry. I consider ASIDIC to be the elite information industry association. The OSS symposium, the only symposium in the world where spys, hackers, information brokers, and corporate buyers of information services come together, is held in early November each year, always in Washington, D.C., and attracted 629 people in 1992 and 808 in 1993.

I want to emphasize the value of external experts. This is important because anything that is printed is by definition out of date. Books are seven to ten years out of date, articles are 7-10 months out of date, and even daily newspapers stories are a few days old. In the age of information, when speed is a factor in competitiveness, you can get ahead of the mainstream by using experts to create information and give it to you before it is published. Any research which does not commission original thinking and include some telephone surveys with real people is not optimized for advantage. Getting to the best expert on a topic, rather than relying on a generalist searching the literature, is the only way to ensure your research is current.

The external experts are especially important as uncompensated filters and evaluators. They spend their lives, at someone else's expense, monitoring their respective areas of expertise. In addition to providing their own expertise, they can quickly guide an intelligence community analyst to exactly the right materials, which can then be acquired for independent evaluation and integration into an all-source product.

PRIVATE INVESTIGATORS	Kroll Associates (New York) (212) 319-0044	Fairfax Group (Washington, D.C.) (703) 207-0600	Parvus-Jerico (USA-Bermuda) (301) 589-4949
INFORMATION BROKERS	Reva Basch Aubergine Info. Svc (510) 527-5770	Seena Sharp Sharp Information (310) 379-5179	Helen Burwell B. Enterprises, Inc. (214) 732-0160
CLASSICAL INTELLIGENCE	Rapport Research & Analysis (U.K.) +44 71 355 5020	Aerobureau/STARS (703) SKY-NEWS	OSS, Inc. V: (703) 242-1700 F: (703) 242-1711

Figure 6: More Intrusive Private Intelligence Capabilities

Kroll Associates (New York) has received favorable publicity as a leader in offering trade secret protection and related private intelligence services. Across the private investigative and "executive services" community, they are the one constant when credible, reliable, international capabilities are discussed.

Fairfax Group (Washington, D.C.) provides a range of services from financial investigations of takeover targets to debugging of offices and handling of ransom negotiations for executives.

Parvus-Jerico (USA-Bermuda) is run by Jerry Burke, former Executive Director of the President's Foreign Intelligence Advisory Board in the U.S.A., and does especially well in the Caribbean and Latin America.

Reva Basch. Author/editor of *Secrets of the Super Searchers*, this lady is widely

regarded as the god-mother of online searchers. A founding member of the Association of Independent Information Producers (AIIP), Reva is respected everywhere--she also has a very strong commitment to ethical guidelines, and believes (and proves every day) that the best private intelligence can be acquired legally and ethically at relatively low cost.

Seena Sharp is one of those hard-core New York sharpies transported to California, with a great sense of humor and the ability to do whatever it takes (legally) to get you what you want. She also is one of the founding members of the AIIP.

Helen Burwell is the best organized of the independent information brokers, and publishes the *Burwell Directory of Independent Information Brokers*. She knows everyone, knows their strengths and their weaknesses. At my suggestion she recently surveyed all independent brokers for their foreign language and foreign database/resident experiences, and her directory now opens windows into the foreign environment.

Information brokers are very special people. Most companies make the mistake of using a single broker, when in fact there is an entire range of brokers who specialize in very specific areas. Helen's directory is the perfect window into this marvelous global community of very talented people.

In the classical intelligence arena, there are a few people in the Anglo-Saxon community (I am not yet familiar with the Asian and Latin communities) who conduct classical intelligence operations on a for-hire basis. The three I have selected are simply representative.

Rapport Research & Analysis has strong roots in the SAS and British intelligence community, and specializes in using ethnic cut-out career agents to securely handle tailored networks in any country. They are also capable of developing rapid-response teams of linguistically qualified interrogators and debriefers who can exploit resident immigrant populations to quickly develop both operational leads and positive intelligence on other countries, organizations, and personalities.

Aerobureau Corporation has a very nice air-breathing surveillance aircraft and a program to provide "Strategic Television Airmobile Reports via Satellite" (STARS). The four-engine aircraft includes a remote-controlled drone that can take videos over denied or dangerous areas. Although focused on imagery, they could also be equipped with rapid-response signals equipment, to include fax and telex intercepts.

OPEN SOURCE SOLUTIONS, Inc. is an umbrella organization which specializes in knowing who is "best-in-class" for any given requirement at any given time. It provides open sources, systems, and services that are legal, ethical, discreet, responsive, and relatively inexpensive. This can include everything from simple on-line searches to complex telephone surveys, from document acquisition to human network development to real time imagery delivery. The whole point of a clearinghouse is to relieve the customer of the burden of

finding the correct private enterprise intelligence capability, while also "laundering" the customer's requirement by concealing its origin and context, and providing the customer with a quality-control guarantee. Founded originally as a non-profit organization to push U.S. policy, OSS, Inc. has responded to international demand by repositioning itself as a for-profit capable of delivering any open source, system, or service.

Conclusion

In the information age, "intelligence" is less a matter of penetrating secrets, and more a matter of separating useful information from the flood of open information that is available legally and cheaply, *in order to provide "just in time" decision-support to the consumer.*

In a period of rapidly changing and emerging threats, when fiscal resources for national intelligence are in decline, open sources are proving to be far more capable and responsive than any intelligence analyst would ever have expected, and cost a fraction of their classified counter-part disciplines.

The private sector is a Nation's first line of defense, and also its first line for collection and processing. It is the private sector which offers the cheapest and fastest indications & warning, current intelligence, and even estimative intelligence capabilities.

The concept of "central" intelligence will simply not survive. "National intelligence" must be redefined, and the intelligence community reinvented, in order to harness the distributed intelligence of the Nation, while permitting the intelligence community to conserve its scarce resources. The intelligence community must focus on satisfying a broader range of consumers, on outsourcing collection and analysis to the maximum extent possible, *and on developing clandestine and technical collection capabilities that are truly discreet and able to achieve results without exposure.*

National intelligence communities cannot remain isolated entities relying solely on in-house capabilities funded by the tax-payer. Without a national information strategy, and national vehicles for harnessing the distributed private enterprise intelligence capabilities of the nation (and of other nations), national intelligence communities are at risk of both a 50% cut in their budgets (or worse), and relegation to an obscure role as special action teams restricted to *in extremis* tasking.

The bottom line, however, remains the consumer of intelligence. Today's consumer is sophisticated and constantly exposed to the wide variety of private enterprise intelligence capabilities. Today's consumer is also beset-by fiscal constraints, and it will not take the consumer long to realize that there may be some advantages to "raiding" the intelligence community's budget in order to "distribute" intelligence resources among the consumers themselves. If the intelligence community does not master OSCINT and provide the consumer with a "value-added" contribution in relation to OSCINT, then the day is going to come when the consumer will testify to Parliament that they do not read classified

intelligence, they do not want classified intelligence, or are not willing to pay for classified intelligence. On that day, intelligence as we know it will die.

It is our burden and our privilege to work together to ensure that from the ashes arises a new form of national intelligence, a national intelligence which fully integrates and harnesses the distributed capabilities of each Nation, and serves as the foundation for national security & national competitiveness. Together, in combination, the unclassified capabilities of private enterprise intelligence and those of classified government intelligence can form a "virtual intelligence community" without equal, a virtual intelligence community able to simultaneously inform policy-makers, business, the academy, and citizens.

APPENDIX B-3

GLOSSARY

AGSI	Association for Global Strategic Information
AIIP	Association of Independent Information Professionals
ASIDIC	Association of Information and Dissemination Centers
C3I	Command & Control, Communications, and Intelligence
C4I2	C4I and Interoperability
CIA	Central Intelligence Agency
CIM	Corporate Information Management
CIO	Corporate Intelligence Officer (vice Corporate Information Officer)
CNN	Cable News Network
DIA	Defense Intelligence Agency
DMA	Defense Mapping Agency
FBIS	Foreign Broadcast Information Service
FIND/SVP	FIND/S'Il Vous Plait
GII	Global Information Infrastructure
GIM	Global Information Management
HIC	High Intensity Conflict
HUMINT	Human Intelligence (Clandestine. Not Covert or Overt)
IMINT	Imagery Intelligence
K-12	Kindergarten-12th Grade
LIC	Low Intensity Conflict
MASINT	Measurements and Signatures Intelligence
MIC	Mid-Intensity Conflict
NAIC	National Air Intelligence Center
NGIC	National Ground Intelligence Center
NFAIS	National Federation of Abstracting and Information Services
NIF	National Information Foundation
NII	National Information Infrastructure
NIM	National Information Management
NMIC	National Maritime Intelligence Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSF	National Science Foundation
OOTW	Operations Other Than War
OSCINT	Open Source Intelligence (includes imagery and signals)
OSS	Office of Strategic Services
OSS, Inc.	OPEN SOURCE SOLUTIONS, Incorporated
SCIP	Society of Competitor Intelligence Professionals
SIGINT	Signals Intelligence
STARS	Strategic Television Airmobile Reports via Satellite
WAIS	Wide Area Information Service

APPENDIX B-4

CORE OPEN SOURCE REFERENCES

NOTE: These are simply a representative sampling. Much of the information is now either in digital form (online, CD-ROM) or published in frequently updated periodicals and directories. ***OSS NOTICES*** provides monthly notification of new meta-sources.

Arnold, Steve. *Internet 2000, The Path to the Total Network* (Infonortics, 1994)

Basch, Reva. *Secrets of the Super Searchers: The Accumulated Wisdon of 23 of the World's Top Online Searchers* (Eight Bit Books, 1993)

Bernhardt, Douglas. *Perfectly Legal Competitor Intelligence: How to Get It, Use It, and Profit From It* (Financial Times/Pittman Publishing, 1994)

Bibliography of Business/Competitive and Benchmarking Literature (Washington Researchers, Ltd. 1994)

Burwell, Helen. *The Burwell Directory of Information Brokers* (Burwell Enterprises, 1994)

Coleman, Edwin J. and Ronald A. Morse. *DATA: Whre It is and How to Get It: The 1993 Directory of Business, Environment, and Energy Data Sources* (Coleman/Moore Associates, Ltd., 1993)

Dedijer, Stevan. *A Heteroglossary for Business Intelligence and Security Innovation* (Lund University, August 1993)

Dedijer, Stevan and Katarina Svensson. *Technical Attaches and Sweden's Innovation Intelligence* (Lund Unviersity, April 1994)

Elias, Arthur W. *The NFAIS Yearbook of the Information Inudstry: 1993* (Learned Information, Inc., 1993.

Frey, Donnalyn and Rich Adams. *!%@:: A Directory of Electronic Mail Addressing and Networks* (O'Reilly Associates, 1993)

From the Top: Profiles of U.S. and Canadian Corporate Libraries and Information Centers (Special Library Association, 1994)

Holden-Rhodes, James. *SHARING THE SECRETS: Open Source Intelligence and the War on Drugs* (OSS, Inc., forthcoming)

Inside Information: Profiles of Association Libraries and Information Centers (Special Libraries Association, 1994)

INTERNET PASSPORT: NorthWestNet's Guide to Our World Online (NorthWestNet, 1993)

Global Perspectives on Competive Intelligence (Society of Competive Intelligence Professionals, 1993)

Orenstein, Ruth. *Fulltext Sources Online* (Bibliodata, 1994)

Rosell, Steven S. *et al. Governing in an Information Society* (The Medidian International Institute, date?)

Rosetto, Louis. *netguide* (1-800-345-8112, 1993)

Rugge, Sue and Alfred Gloassbrenner. *The Information Broker's Handbook* (Windcrest/McGraw Hill, 1992)

Tompkins, Alan, *et al. Open Source Intelligence Resources for the Military Intelligence Officer* (434th Military Intelligence Deatchment, forthcoming)

APPENDIX C

ACCESS:
Theory and Practice of Intelligence in the Age of Information

Robert D. Steele, President
OPEN SOURCE SOLUTIONS, Inc.

95% de l'information dont une entreprise a besoin peut s'acquirir par des moyens honorables.

Henry Stiller, Director General
Histen Riller, Societe Civile

Executive Summary

Point #1: In the Age of Information, "intelligence" is less a matter of penetrating secrets, and more a matter of separating useful information from the flood of open information that is available legally and cheaply: *electronic sources are especially useful.*

Point #2: In combination, the economic and political cost of industrial espionage, or penetrations of other governments to divine "plans and intentions", are insupportable when contrasted with the benefits of open source intelligence (OSCINT).

Point #3: The concept of "central" intelligence cannot survive in the Age of Information. By focusing on OSCINT, a Nation can mobilize each of its knowledge sectors, and turn the entire Nation into a "virtual" intelligence agency with far greater collection. processing, and action capabilities than are provided by the existing bureaucracies dedicated to national and defense intelligence.

Point #4: Comprehensive national knowledge strategies must provide for connectivity, content, culture, coin, and C4 security: the "Five C's".

Table of Contents

1 Background. What is the issue; changed "rules of the game"; national information continuum; four information categories; three characteristics of value; speed as the foundation of security; hard copy versus electronic information.

2. Discussion. Role of intelligence and "virtual" intelligence; information as a substitute for capital and labor; possible investment strategy for information; political and economic cost of espionage; pre-publication/pre-secret windows of opportunity; speed advantages of open source exploitation.

3. Information Requirements and Player Identification. Priority versus gaps-driven collection; four major consumer groups of intelligence; refining the gaps-driven requirements process; model for consumer-oriented production; four major target groups for intelligence; four kinds of players in the open source arena.

4. Sources of Information and Methodology. Five distinguishing aspects of information sources; essential reorientation of intelligence toward open sources; privatization of intelligence; five elements of a national knowledge strategy.

5. Industrial Espionage, Sanctions, and Proscribed Information. U.S. views of Japanese and French; general attitudes about industrial espionage; sanctions; proscribed (prioprietary) information.

6. Analysis. Rules of the game have changed; competitive advantage has shifted from secrecy to openess; new "order of battle" needed for national intelligence; national knowledge strategy is a critical initiative; strategic opportunity for competitive advantage exists.

7. Action Requirements. Reinvent national intelligence; realign resources; establish a national information requirements council; establish open source focal points within United States and other countries.

8. References. Resume and selected publications; other works of importance; date of information.

1. **Background**

What is the issue? The issue of access has enormous importance for both the national security and the national competitiveness of any Nation.

> *The issue for the client is: how does a Nation achieve national security and national competitiveness in the Age of Information, and what does this mean to existing national policies on intelligence organization and the expenditure of public and private funds for information collection, processing, and dissemination activities.*

Changed "Rules of the Game. An understanding of the "sources and methods" which comprise "access" in the Age of Information is absolutely vital for top-level decision makers in both government and the private sector. Top-level decision-makers must understand that the "rules of the game" have changed, and that competitive advantage in the

Age of Information is dependent on the laws of cybernetics, not the laws of physics. Under the laws of physics, secrecy and the restriction of knowledge provided a temporary advantage. In cybernetics, openness and flexibility win.

Most great nations spend on the order of $20 billion to $30 billion a year on "intelligence", which is traditionally comprised of clandestine human intelligence, and technical collection of imagery and signals.

National Information Continuum. At the same time, most great nations have an "information continuum" (illustrated below) whose endeavors and products are going to waste...the capabilities of these elements of the national information continuum are not being exploited! This continuum represents, in a typical great nation, a $100 billion per year capability that is lying fallow.

K-12 Libraries PI/IB Government Intelligence

Universities Business Media Defense

Figure 1A. The National Information Continuum--Nine Sectors

NOTE: The above is an original representation that has been current in the literature for over a year. It is different from the more practical Sector Breakout because it reflects a focus on elements of the information continuum which do not--at this time--contribute significantly to national and defense research endeavors.

Four Information Categories. There are four "information categories" in the access arena. They are:

a. Open source or public information: within intelligence communities, this is known as open source intelligence or OSCINT. "Grey literature", literature which is unclassified and not proprietary, but produced in limited quantities for limited purposes, is included as an element of OSCINT. Open (unclassified) electronic information, such as that available through the INTERNET and related file servers and newsgroups, is also included in OSCINT. *The vast majority of scientific & technical intelligence is available through OSCINT, to include 600 scientific & technical journals that appear only in electronic form.*

b. Open proprietary information, discernable through open source investigation. This includes the reverse engineering of legitimately acquired products, and legally conducted "competitor intelligence". (Note: competitor intelligence is the globally accepted term for legal research efforts by businesses studying their competitor's products, organizations, and related matters.)

c. Closed proprietary information, available only through industrial espionage or

clandestine and technical penetrations of regulatory agencies.

d. Classified information, available only through clandestine human intelligence or technical (imagery or signals) intelligence.

Open Sources	Proprietary (Open)	Classified
Grey Literature	Proprietary (Closed)	

Figure 1B. The Four Information Categories

Three Characteristics of Value. The value of information is derived from three characteristics of the information: its substance or content; the context within which it is being considered by others; and the timing with which it is received.

> *The single most significant step an organization can take to increase the value of the information it is acquiring is to increase the speed with which the information is acquired and acted upon. This is also the most inexpensive step--but only if top management is willing to accept significant changes in doctrine and procedure.*

Speed as the Foundation for Security. The speed with which information moves and achieves value depends less on the information itself (the externality) and more on the degree to which the participating organizations are organized and aware of their requirements (the internality). Organizations are drowning in information because they have not learned to swim. They are not trained, equipped, or organized to collect, process, disseminate, and act upon information. The most important employees, the ones with the contextual understanding of the situation, are normally not empowered to act on information, and normally do not receive intelligence products.

Imbuing a national infrastructure with "speed" really means that a complete change is required in the way in which organizations relate to one another, and in the way in which managers relate to front line workers or action officers. The beauty of working with open sources is that it eliminates, in a single stroke, all of the political and legal, as well as the economic, constraints that characterize the sharing of classified information. We have been trying to water the desert with oil, instead of water.

Hard Copy versus Electronic Information. Finally, in discussing issues of access, it is important to understand the relative value of hard copy versus electronic information. Although hard-copy information far outweighs electronic sources in quantity, and particularly in relation to Third World sources, the electronic world is where "up and coming" technologists as well as "up and coming" leaders are communicating their most signficicant thoughts.

The electronic world is especially useful because it allows an enormous amount of research to be conducted from a single location, and also allows relatively anonymous browsing through other computers or commercially available databases. Hard-copy is an important secondary source, especially when investigating Third World and non-technical issues.

Third World Hard Copy "Cyberspace"

First/Second World Hard Copy INTERNET

Figure 1C. Hard Copy versus Electronic Information

2. Discussion

Role of Intelligence and "Virtual" Intelligence. There is no issue more important to a Nation in the Age of Information than that of the role of intelligence--not only of the role of the traditional national intelligence services, but also of the non-traditional "virtual" intelligence services which are represented by the other elements of the national information continuum.

> *A proper perspective on this matter, at the highest levels of both the government and the private sector, represents at least a $100 billion a year value. This is enormously important, not only because it will be the major policy area affecting the future of the Nation, but because it is relatively easy to achieve by realigning and coordinating existing capabilities and funds.*

Information as a Substitute for Capital and Labor. In the Age of Information, when information is the "first order" commodity, and information is a substitute for time, space, capital, and labor, the implications of this discussion are enormous. The fate of the Nation depends on a proper appreciation of this issue, and on adequate coordination between government and private sector leaders responsible for elements of the information continuum.

Possible Investment Strategy for Information. The four "information categories" in the access arena can be evaluated as follows:

-- Open source: 80% of what is required for sound decision-making, at 20% of the cost, in 20% of the time (relative to industrial espionage or classified collection). The value of open source information cannot be exaggerated.

-- Proprietary (open): 5% of what is required, for an additional 10% cost increment.

-- Proprietary (closed): 5% of what is required, for an additional 20% cost increment.

-- Classified: 10% of what is required, for an additional 50% cost increment.

|----------OSCINT (80%)----------|

PROPRIETARY (10%)
CLASSIFIED (10%)

Figure 2A. Possible Investment Strategy for Information

Political and Economic Cost of Espionage. It merits comment that industrial espionage in particular, but clandestine and technical intelligence as well, reflects a political risk, or a potential political cost, that is easily triple the economic cost--industrial espionage and classified penetrations are not only twice as costly as open source exploitation, they are also twice as likely to "explode" in the face of their sponsor.

Pre-Publication/Pre-Secret Windows of Opportunity. In the area of open source information, or open source intelligence (OSCINT). it is very important that decision-makers understand the levels of access in terms of time
--time is the vital aspect of cybernetics, and is the critical factor in national competitiveness:

Published sources are available to mass audiences at the same time--books are generally provided to the public years after they were actually written; articles generally months after they were written; and newspaper reporting days or weeks after being drafted..

"Grey literature" is available to specialized audiences at the same time. and to non-members after a period of time.

"Work in progress" in available to peer review groups and to specially equipped "outsiders".

"Pre-publication intelligence" is available to specially equipped outsiders who take the trouble to identify and cultivate selected sources of public information. This area is the "center of gravity" for those who seek to "reinvent" national intelligence.

Speed Advantages of Open Source Exploitation. There are two reasons why open source intelligence (OSCINT) is a vital area of concentration: the first is that most applied technology, including proprietary or classified technology, begins with open publications about its sub-elements, and it is often possible to piece together very good intelligence reports "at the source" while avoiding the risk of industrial espionage or clandestine operations against foreign targets. The second reason is that every "dual-use" technology to which export controls are eventually applied spends at least two years, and sometimes up to ten years, in "beta" development. The Department of Commerce, which has the lead in classifying dual-use technology, is generally two years behind actual market developments; this is particularly true in the software arena. Thus, the best time to capture a "secret" or a restricted technology, is during the two year "beta" window before it becomes a secret or is

restricted.

Real-Time Mind Link Beta Testing Traditional Sources

Work in Progress Gray Literature

Figure 2B. Speed Advantages in Open Source Exploitation

Refining one's open source intelligence (OSCINT) intelligence process to collect information in the pre-publication stage, by identifying and keeping in touch with key experts who provide advance looks at "works in progress", adds a further six months to a year of competitive advantage. *Electronic searching is the single most vital tool in identifying these experts "in time".*

3. Information Requirements and Player Identification

There are three ways of looking at the information playing field: by focusing on the four consumer groups for national intelligence; by focusing on the four warrior classes of the future; and by focusing on the sources of information. Each will be discussed in turn, together with a means of executing gaps-driven collection and consumer-oriented production.

Priority versus Gaps-Driven Collection. The information requirements arena is traditionally one which intelligence communities have not mastered. Too often they collect what is collectable, or obviously protected, and they rarely produce intelligence that is tailored to a specific customer or delivered "just in time". Information requirements are typically driven by gross priorities (e.g. the Soviets are priority one, the Chinese priority two), rather than by "gaps" or real requirements. This often means that Third World encyclopedic intelligence (most of which is unclassified), and economic or demographic intelligence vital to penetrating foreign markets, does not receive the attention it requires.

Four Major Consumer Groups of Intelligence. There are four specific groups of information customers that every intelligence organization should be serving, but generally does not, because it focuses on the very highest levels of government rather than on the subordinate levels where policy is actually created and actions are taken on a day to day basis.

a. Departmental planners and programmers, in every Department of government, not only in the national security arena, require both strategic generalizations (rather than a flood of detailed reports about tiny parts of many problems), and political-military information heavily laden with information about "plans and intentions".

b. Regional planners and programmers, including Ambassadors and Assistant Secretaries of every Department of government, require regional generalizations and very detailed mobility and market information. This is the customer group most likely to take

advantage of intelligence which focuses on opportunities for advantage, opportunities to prevent disaster or establish commercial gains before anyone else realizes there is a threat or an opportunity to be contested.

c. Ambassadors and corporate general managers in specific countries require both detail about the physical capabilities of their opponents or competitors, and very detailed evaluations of sustainability, availability, reliability, and or accuracy of competitor products. In the economic arena, intelligence about demographics and culture is more easily obtained, and more valuable, than internal corporate information about competing products. If you understand the BUYER's requirements, you do not need to collect every detail about competing SELLER's capabilities. This point merits elaboration: competitive advantage comes from satisfying the buyer, not from beating the opposing seller. It is far more important to understand every detail about what the buyer wants to buy, than attempting to understand opposing solutions.

d. System designers and project managers, and those at the most senior levels who make acquisition and investment decisions, generally receive adequate intelligence about technical details, but do not receive good intelligence (intelligence which is generally unclassified) about whether the system is really worth acquiring in terms of cost-value, competing means of meeting the requirement, cost of sustainability, and so on. For instance, most advanced nations have invested billions of dollars in fast-moving sophisticated systems and failed to establish the necessary communications and computer support to actually make those systems effective in the field.

System Designers Regional Planners

General Managers Department Planners

Figure 3A. Four Major Consumer Groups for Intelligence

Refining the Gaps-Driven Requirements Process. The greatest flaw in a priority-driven requirements process is that it is divorced from the day to day needs of the policy and action-level consumer. Priority-driven collection tends to err on the side of repetitive and "vacuum cleaner" collection against the highest priorities, and to completely disregard both encyclopedic and current intelligence requirements for targets which may be of a lesser priority in the "grand strategy" arena, but of vital interest at the operational and tactical levels. A gap-driven information requirements process will take its requirements each day (rather than through monthly or quarterly "priorities validation" meetings), both from the consumer of intelligence ("here is what I need to know tomorrow") and from the analyst ("here are the things I did not know in producing this report").

Model for Consumer-Oriented Production. The existing production model, at least in the United States, is based on "stove-pipe" production which is rarely as "all-source" as it could be (e.g. the National Security Agency produces reports drawn largely from signals

intelligence), and is also severely deficient because it focuses on specific countries, topics, or weapons systems--i.e. the production is defined by the target, not by the needs of the consumer. Below is illustrated a superior line of consumer-oriented products, most of which would be unclassified and whose contents would be primarily drawn from open sources of intelligence.

BASIC PRODUCTION: COUNTRY PROFILES. Integrate executive summaries for each of the four consumer groups, with brief encyclopedic intelligence summaries of each of the key industrial, geographic, and civil factors.

STRATEGIC PRODUCTION. Tailored products that focus on establishing *strategic generalizations* pertinent to specific mission areas (e.g. aircraft, automobiles, textiles), specific regions, and specific timeframes (generally long-term).

OPERATIONAL PRODUCTION. Tailored products focused on *regional generalizations* with a special emphasis on industrial areas within the region, on seasonal differences (whether terrain or trade), and on leadership character and demographics.

TACTICAL PRODUCTION.. For each industrial area (or industry area) both generalizations and specifics country by country, with emphasis on terrain, climatic, and civil constraints. It is only at this level that a consumer should have to deal with the level of detail which now characterizes most intelligence community products.

TECHNICAL PRODUCTION. Get away from system-specific production, and move instead toward industry-area production with regional and timeframe sub-sets. Focus on support to cost-benefit and trade-off decisions, not on the system in isolation.

Figure 3B. Model for Consumer-Oriented Production

Four Major Target Groups for Intelligence. There are four specific targets for information and intelligence activities; each of these target groups must be completely understood if a Nation is to maintain both its national security and its national competitiveness. Each target group has a different source of power, and a different way of training, organizing, and equipping itself for battle. Each requires a different intelligence approach and in essence a different kind of intelligence community. The traditional intelligence officer will not be competent against all four of the target sets--four different kinds of intelligence organizations must be trained, equipped, and organized for their specific target set.

a. The High-Tech Brute, similar to the United States of America, is that group which relies on expensive technical capabilities and hugh logistics trains. In industrial terms. this is the capital-intensive player.

b. The Low-Tech Brute, such as the narcotics trafficker or the Italian crime family. represents a "needle in the haystack" problem. In industrial terms, this is the labor-intensive player.

c. The High-Tech Seer, such as highly skilled and knowledgeable computer engineers. is comprised of both conglomerations of skilled individuals engaging in economic warfare, and single individuals, "hackers", able to penetrate advanced computer and telecommunications networks. In idnustrial terms, this is the brain-intensive player.

d. The Low-Tech Seer, such as the Islamic Fundamentalists, or Asian gangs in the United States, are those whose "weapons" are of a cultural or demographic kind, whose "command and control" system is comprised of the television and the pulpit--very difficult for a Western intelligence service to understand and address. In industrial terms, this is the labor union.

In each of these cases, using electronic sources of news and information provides a significant competitive advantage in terms of time, scope of review, and depth of understanding.

High-Tech Brute	High-Tech Seer
High-Tech Brute	Low-Tech Seer

Figure 3C. Four Major Target Groups for Intelligence

Four Kinds of Players in the Open Source Arena. The diagram in the "Background" section clearly identified the nine constituencies in the access arena. Naturally there are sub-constituencies (e.g. government is divided at the federal level into legislative, executive, and judicial, and also into federal, state, and local; media is divided into mainstream national papers, regional papers, niche journals, and technical newsletters).

In general terms, there are four kinds of players:

-- Those who talk to one another but are not influential, are divorced from practical military or commercial applications: the "ivory tower" academics. Spend 10% of your resources on this group.

-- Those who are influential but do not quote one another and contribute nothing substantial: the "bandwagon" journalists. Spend 10% of your resources on this group.

-- Those who are both connected to one another and influential--this constitutes the "mainstream" of current thinking. The downside of the mainstream is that is tends to reflect conventional wisdom rather than innovative or revolutionary thinking. Spend 20% on this group.

-- Those--and they are a small group--that are neither connected nor influential, but who are in fact the "up and coming" leaders in their disciplines. It is this group which not only represents the greatest potential value for a Nation, but which is the least protected! The only obstacle to exploiting this group is internal, it is bureaucratic! Spend 60% on this group. Although intelligence organizations are accustomed to thinking of this group as a source of "sleeper" agents, in fact it should be thought of as a source of "avant garde" thinking which is not only of enormous importance to international competitiveness and domestic security, but predominantly unclassified.

Mainstream (20%)	Up and Coming (60%)
Bandwagon (10%)	Ivory Tower (10%)

Figure 3D. Four Kinds of Players in the Open Source Arena

4. Sources of Information and Methodology

Five Distinguishing Aspects of Information Sources. Sources of information can be classified by medium, location, discipline, language, and level of classification.

The most pervasive medium is hard-copy information. However, most of the hard-copy information is of relatively low grade, and often not worth the expense of acquisition. Never-the-less, it cannot be ignored. Spend 20% of your resources on the hard-copy medium.

The next major medium is micro-fiche; although many organizations are phasing out their micro-fiche holdings, this remains an important medium, particularly in the patent and archival worlds. Spend 10% on this medium.

Electronic information is available through online services as well as offline products. It is important to emphasize that electronic information includes imagery (SPOT, LANDSAT) as well as signals (foreign radio and television broadcasts, unencrypted cellular telephones, facsimiles, and telex transmissions). It is also important to note that, despite the fact that electronic information is a relatively small arena of interest in relation to hard-copy and microfiche, it is "exploding" and already dominates many of the most advanced disciplines as the "medium of choice. For instance, this medium contains over 600 scientific journals online that do not appear in hard-copy at all. *The electronic medium is the battleground where strategic advantage can be gained at relatively low cost and with no political risk--it is open, it is pervasive, and it is not being exploited by other countries as well as it could be--*

this is a very important area. Spend 40% of your resources on this medium.

The most subtle storage medium is the human brain. No intelligence service will ever master the data entry or data collection problem. The most important capability any intelligence service can develop is that of establishing real-time mind-links between the customer and the best available source. The "intelligence minuteman" concept. first articulated in December 1992 at the First International Symposium on "National Security & National Competitiveness: Open Source Solutions", is the wave of the future. Spend 30% of your resources on this medium. Note that this medium provides real-time access to the other mediums--the human expert responsive to tasking can rapidly collect, process, and disseminate essential information from the other mediums, on demand.

It is important to note that in the Age of Information technology has made possible a radical shift in why and when one acquires information. It is now possible to train, equip, and organize collectors of information for "just in time" collection instead of "just in case" collection. Hard copy and microfiche were the dominant storage mediums under the old "just in case" paradigm. Electronic information, and direct access to an enormous global pool of oven human asseets are the dominant access mechanisms under the new paradigm.

The location of the information is both geographic and physical. Some information cannot be obtained without a personal visit to its location. Most information can be obtained remotely. through a telephone call or correspondence, and payment if necessary to the appropriate person.

> *A single researcher skilled at remote data acquisition for a particular region is more valuable than 100 clandestine case officers spread over ten countries. Physically the information might be part of a central filing system or a personal filing system. 80% of the time the information will be part of a personal filing system, which reiterates the critical importance of developing human paths to the information.*

Professional disciplines (e.g. physics, electro-optics) are the most global and well-organized structures through which to acquire information. Penetrating a professional association with global links is far more useful than penetrating a single government's nuclear facility, to take one example. Again, professional associations provide the human links and paths toward virtually any information--they are also the most likely to publish information before it becomes classified. It is futile to train intelligence professionals to pretend to be scientists. It is much more useful and cost-effective to provide existing scientists with the finest communication tools and travel budgets possible--they will absorb far more, and be able to report far more, than a few case officers working with a few agents of limited access.

Language skills cannot be ignored. English, French, Spanish, Japanese, Chinese, and Arabic are the most important languages, followed by Russian, Punjabi, Hindu, and Hebrew. Any international intelligence or information service which does not have at least 100 people

fluent in each of the most important languages, and at least 20 people fluent in each of the minor languages listed above, is not serious. Language translation programs (e.g. Global Link) are important aids, and can be used to reduce the time of translation for a typical document from eight hours to three. The importance of linguistic and cultural nuances should not be underestimated. The language of the consumer should be the language of production, even if this involves extraordinary cost.

Level of classification (in governments generally Confidential, Secret, Top Secret, and Codeword; in business generally Proprietary, Trade Secret, Executive Only) is the most misunderstood and over-rated basis for selecting information. Enormous amounts of money are wasted, and significant political risk is undertaken, to obtain information that is classified "secret" or "proprietary". This is a fundamental mistake which reflects a lack of understanding about how knowledge works in society, a lack of understanding of current trends in information sources and methods.

MEDIUM DISCIPLINE CLASSIFICATION

LOCATION LANGUAGE

Figure 4A. Five Distinguishing Aspects of Information Sources

Essential Reorientation of Intelligence Toward Open Sources. The methods used to obtain information should be appropriate to the sector of information generation that is being studied. Each of the nine sectors has information producers. Each nation has representatives of their own in sectors of their own. For instance, your own journalists are frequently the best means of approaching foreign journalists, and of monitoring the production and the human sources being used by foreign journalists.

The fundamental flaw in the "methods" of most intelligence agencies is that they attempt to acquire all information using their own personnel and clandestine or technical methods. Instead, they should leverage the other sectors of the information continuum, and establish a "virtual" intelligence community that is comprehensive. By focusing on open information and the open exploitation of individuals in all sectors, a Nation with a $10 billion intelligence budget can leverage another $90 billion in existing independent but exploitable "virtual" intelligence capabilities whose "overhead" costs are not being paid by the government. The electronic medium is the "lever that can move the world" and give the intelligence professional enormous access.

Privatization of Intelligence

The most fundamental change in "methods", besides moving away from investments in clandestine and technical intelligence capabilities, and toward investments in open source intelligence, is that of the privatization of intelligence. It is more efficient, most cost-effective, indeed, more discreet, to

utilize ad hoc private collectors and processors of information, than it is to use existing bureaucracies, including existing intelligence agencies and existing Embassies or local corporate offices overseas.

Five Elements of a National Knowledge Strategy. This focus on openness is extremely important because it means that the fruits of this open source intelligence effort can be shared directly with industry, the press, and the legislature, without the slightest political risk. For those who do not understand how "open" information can provide a competitive advantage, consider only how disorganized everyone else is--the first Nation to establish a national knowledge strategy which harnesses the full power of their information continuum will achieve an enormous competitive advantage as we enter the Age of Information. A national knowledge strategy is comprised for five elements:

a. CONNECTIVITY. Provide leading representatives within each sector with the telecomputing tools they require to keep in touch with their counterparts in all other countries, and with one another. At the same time, provide government and corporate intelligence analysts with the same tools, and provide everyone with incentives to communicate with one another.

b. CONTENT. Provide incentives to all parties to maximize the amount of information that they put "online"; the government can increase online information by testing new economic models (for instance, the "compound interest" model instead of the "single sale" model for compensating authors) and making appropriate adjustments to copyright and patent law. This is a two-way concept. It is not only important to increase the amount of foreign language material that is captured, translated, and placed online, but it is equally important that great emphasis be placed on exporting national intellectual products which have been fully and accurately translated into major foreign languages such as English, Japanese, and Chinese. In the Age of Information, "gunboat diplomacy" has been replaced by intellectual influence. The quality of a nation's intellectual output, and the degree to which it is made useable by others, will have a dramatic impact on the strategic position of the Nation.

c. CULTURE. Recognize the importance of accelerating the integration of ethnic populations and economically impoverished citizens. In particular, those ethnic groups which speak and read fluently the language of their adopted country, and the language of their former country, are priceless national assets which can be used as interpreters and translators.

d. COIN. A typical major nation wastes on the order of $2 billion a year just on end-user fiddling with personal computer hardware and software combinations. If all redundant and contradictory research & development were brought under control, just in the information technology arena, a typical major nation would probably save on the order of $10-20 billion a year.

e. C4 SECURITY. Every nation, and particularly the advanced nations of Europe

and the Anglo-Saxon world, is extremely vulnerable to the interruption of command & control, communications, and computing services.
Virtually every major antenna system, including the downlinks from the satellites, is completely unprotected. No nation has established a serious C4 security posture that recognized the degree to which government, military, and economic communications depend on a very vulnerable civil infrastructure. No nation has established an effective "cyberspace order of battle". This is the "Pearl Harbor" of the Age of Information, waiting to happen.

CONNECTIVITY CULTURE C4 SECURITY

CONTENT COIN (R&D)

Figure 4B. The Five Elements of a National Knowledge Strategy

5. Industrial Espionage, Sanctions, and Proscribed Information

U.S. Views of Japanese and French. There is a very strong perception within the United States that the Japanese view economic competition as "war", and that the French, while not necessarily viewing economic competition as war, are willing to engage in "unethical" measures including direct support from government intelligence agencies to specific Frnech companies. The book Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets, while discredited in some circles, has done enormous damage to French interests in the U.S. The running joke about Air France seats being "bugged", very common in U.S. business circles, is a good sign of how deeply this book has penetrated the "psyche" of the U.S. business community.

General Attitudes About Industrial Espionage. Most U.S. companies do not have a full appreciation of how easily others can penetrate their organizaations, and most do not engage in significant industrial espionage. For instance, most U.S. companies have absolutely no computer security and no measures to protect their computers from external penetration. They are completely unaware of the ease with which computer screens and computer emissions can be captured from a van parked outside their building. There is a general sense among U.S. firms that industial espionage is "not worth it". There are two exceptions to this: the first is the hiring of executives and key employees from competitor firms, and the second is bribery, but only overseas.

Sanctions. The Toshiba case is a good example of the sanctions that might be imposed is specific instances when there is a public knowledge of violation, but in general the U.S. government will not publicize or act on cases of industrial espionage.

Proscribed (Prioprietary) Information. There is a strong trend in the United States toward openness. This is true of the government, where many "secrets" and many secret technologies are about to be declassified, and also of industry, where there is a growing understanding that the restriction of information imposes internal costs that may not be

warranted. In the case of specific chemical formulas or other "protectable" secrets, this may not be so, but in the case of general engineering practices, targeted markets, and so on, the general focus is on openness and staying ahead of the competition, rather than on protecting secrets.

6. Analysis

The client is better able to evaluate the applicability of this new theory and practice of intelligence to their needs, but on balance one must conclude:

"Rules of the Game" Have Changed. The Age of Information has redefined our concepts of war and peace, of national security and national competitiveness. The "rules of the game" have changed, and there has been a reordering of both power and the sources of power. Information is now a commodity, and the most important resource to any Nation.

Competitive Advantage Has Shifted From Secrecy to Openness. The Age of Information has destroyed the ability of individuals, organizations, and governments to control information or restrict the dissemination of information. It is virtually impossible to keep a "secret" in this day and age. Hence, the competitive advantage has shifted from those able to conduct research in secret, to those able to RAPIDLY exploit the efforts of others through openly available information collected "just in time".

New "Order of Battle" Needed for National Intelligence. The Age of Information requires a new "order of battle" philosophy within national governments and their major corporate sectors. The degree to which individual minds can be linked across sectors now becomes more important than the number of tanks one has--existing conventional forces can be immobilized, and existing industrial processes can be superceded, by relatively modest applications of knowledge. *The rapid development of competent electronic search & retrieval specialists, and particularly specialists in scientific & technical databases and newsgroups, as well as cultural matters, should be a national priority.*

National Knowledge Strategy is a Critical Initiative. Although there are several nations, including Japan, Sweden, Israel, and Taiwan (and their tribal villages world-wide) which are generally ahead of all others in their national knowledge activities, no nation has actually developed a national knowledge strategy nor harnessed the potential of its nine sectors in the information continuum--a continuum that constitute a "virtual" intelligence community of enormous power.

Strategic Opportunity for Competitive Advantage Exists. A strategic opportunity for competitive advantage exists. In my judgement there is about a two to five year window within which an organized national effort can reap enormous dividends. After that time many organizations will both realize the power of open information and start developing their own collection capabilities more fully, and public encryption will be widespread, introducing a "Tower of Babel" effect into the "electronic English" information commons that is just

beginning to appear.

7. Action Requirements

a. Reinvent National Intelligence. Each nation has an enormous store of non-traditional intelligence and information capabilities outside of government that are rarely called upon. Consider the potential of these non-traditional sources, and develop plans for the total mobilization of the nation's intellectual power.

b. Realign Resources. Roughly 80% of the existing intelligence budget could be realigned to open source intelligence (OSCINT) collection, processing, and dissemination, in close cooperation with the other elements of the national information continuum, who might be inspired to effect their own realignments once they see the government in a leadership role.

CLASSIFIED INTELLIGENCE			**10%**
PROPRIETARY INTELLIGENCE			**10%**
OPEN SOURCE INTELLIGENCE			**80%**
Human Sources		30%	24%
-- "Up and Coming"	60%		24%
-- Mainstream	20%		08%
-- Bandwagon	10%		04%
-- Ivory Tower	10%		04%
Hard Copy		20%	16%
Microfiche		10%	08%
Electronic		40%	32%

NOTE: Column one percentages are 100% of subheading percentage in column two, while column two percentages are 100% of column three subheading. The percentages in column three are actual percentages of the total budget.

Figure 7A. Notional National Intelligence Resource Realignments

c. Establish a National Information Requirements Council. Identify an organization able to coordinate demands for information with global collection activities and impose the common sense guideline of exploiting open sources as "the source of first resort". This has the interesting ramification of also making much more of what we need to know obtainable through private sector capabilities rather than government capabilties.

d. Establish Open Source Focal Points Within United States and Other Countries. Within the United States, contract with two separate organizations: the first should serve as a complement to the Embassy and as a rapid-response local representative for the national intelligence council. It's role should be one of requirements management, oversight, and product packaging. The second organization should actually carry out all the research through sub-contracted collection and production, with value-added quality control. Similar arrangements can be made in other countries, perhaps by building on the established SVP network.

8. References

A resume and a list of selected personal publications are attached. The *Proceedings* of the First International Symposium on "National Security & National Competitiveness: Open Source Solutions", are the sole existing foundation for a national intelligence restructuring of this magnitude. A copy of both volumes is provided as part of this report, together with copies of more recent articles, speeches, and testimony bearing on this issue.

Other works of importance include: Jon Sigurdsom and Yael Tagerud (eds), *The Intelligent Corporation: The Privatization of Intelligence* (Taylor Graham, 1992); Alvin Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Little, Brown, forthcoming), see especially the chapters on knowledge warriors and the future of the spy. Winn Schwartau, *Information Warfare: How to Wage and Win War in Cyberspace* (Interpact, forthcoming); James Holden-Rhodes, *Sharing the Secrets: Open Source Intelligence and the War on Drugs* (Sandia National Laboratory, forthcoming)

9. Date of Information. 17 September 1993

APPENDIX D

CONCISE DIRECTORY OF SELECTED INTERNATIONAL OPEN SOURCES & SERVICES

DOI: 1 March 1996

Prepared by Robert D. Steele
Based on Research As Published in *OSS NOTICES* 1992-1996

ACCESS INNOVATIONS, INC.

Ms. Marjorie Hlava, President
Post Office Box 40130
Albuquerque, NM 87196
Voice: (505) 265-3591
Fax: (505) 256-1080

Ms. Hlava has been past president of the major information associations in the USA including the American Society for Information Science and the Association of Independent Information Producers.

BDM FEDERAL

Mr. Tom Price III
Principal Staff Member
1501 BDM Way
McLean, VA 22101-3204
Voice: (703) 848-5203
Fax: (703) 848-6683

The National Security & Technology Applications Division is under the leadership of LtGen C. Norman Wood, USAF (Ret), former Director of the Intelligence Community Staff, and specialized in OSINT support to U.S. intelligence.

BRITISH LIBRARY, THE

Mr. Mike Curston
Document Supply Centre
Boston Spa, Wetherby
West yorkshire LS23 7BQ
UNITED KINGDOM
Voice: (44 937) 546-333
Fax: (44 937) 546-061

Something like the U.S. Library of Congress, but better organized and focused on solid business practices. Known world-wide for its access to obscure sources and especially for its access to conference proceedings. Produces CD-ROMS, others aids.

BURWELL ENTERPRISES

Ms. Joanne Pauline
Marketing Director
3724 FM 1960W, Suite 214
Houston, TX 77068
Voice: (713) 486-3500 x 2353
Fax: (713) 920-7086

Ms. Helen Burwell is the publisher of the *Burwell Directory of International Information Brokers*, and recently added an index to this work which identifies brokers who speak a foreign language, and are familiar with in-country databases.

CIESIN (CONSORTIUM FOR INTERNATIONAL EARTH SCIENCE NETWORK)

Mr. Robert J. Coullahan

Director of Government & International Programs
1747 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
Voice: (202) 775-6606
Fax: (202) 775-6622

This organization is a non-profit and one of the best sources of meta-data: data about environmental information, including imagery and seismic data, held by others around the world. Excellent advisors.

CISTI

The Canada Institute for Scientific and Technical Information, originally focused on meeting the needs of Canada, has expanded in recent years to offer its services to the North American customer base. Their online catalogue is available free at <http://www.cisti.nrc.ca/cisti/serlist.html>. For more information contact Document Delivery Services, CISTI, National Research Council, Ottawa, Ontario K1A OS2, Canada. Voice: (613) 993-9251, facsimile (613) 952-8243. Email: <cisti.docdel@nrc.ca>.

CLEARINGHOUSE FOR SUBJECT-ORIENTED INTERNET RESOURCES

University of Michigan

60 subject-matter guides including:

- Aerospace Engineering
- Archives on the Internet
- Government Sources of Business & Economic Information
- Neurosciences Internet Resource Guide
- U.S. technology Public Policy

Example of university resources being applied for the common good.

<gopher.lib.umich.edu>, look for "What's New and Featured resources", go to "Clearinghouse". Or anonymous ftp to <una.hh.lib.umich.edu path:/inetdirstaks>. If you have trouble, email <lou@umich.edu>.

Derwent World Patents Index

Available through DIALOG, Questel/Orbit, and STN. Communicate with Derwent Publications, Ltd., Derwent House, 14 Great Queen Street, London WC2B 5DF, United Kingdom. Voice: (44 171) 344-2800 or in the USA (703) 790-0400. Web: <http://193.128.218.44/products/>.

DIALOG (Knight-Ridder)

Mr. David Brown, Team Leader
Government Team, Suite 500
1901 North Moore Street
Arlington, VA 22209
Voice: (703) 908-2383
Fax: (703) 524-1680

One of the two leading commercial online services--it is very important to understand that both DIALOG and LEXIS-NEXIS are required to "hit" 2/5ths of the available online information, and that the other 3/5ths require additional research.

Directory of Publications and Broadcast Media

Available from Gale Research for $295. ISBN 0-8103-7188X. Formerly titled the *Directory of Directories*, this is a recommended starting point for virtually any search.

Disclosure, Inc.

Disclosure, Inc., 5161 River Road, Building 60, Bethesda, MD 20816. Web: <http://www.disclosure.com/>.

E2G (UK)

Mr. William Owen, Managing Director
2nd Floor, 1 Northumberland Avenue
Trafalgar Square
London WC2 N5BW ENGLAND
Voice: (44 171) 487-3626
Fax: (44 171) 487-3817

Former Special Air Service and other British special forces personnel are available through this organization to conduct route reconnaissance, develop military maps, and provide other pre-landing support services.

EASTVIEW PUBLICATIONS

Manager
Gray Literature Acquisitions
3020 Harbor Lane N
Minneanapolis, MN 55447
Voice: (612) 500-0961
Fax: (612) 559-2931

This organization is one of the best in the world at acquiring "grey literature", with a strong specialization in Russian and East European literature. They are also the foremost source of Third World maps, including tactical maps, created by USSR.

Encyclopedia of Associations

Available from Gale Research for $250. ISBN 0-8103-7421-8.

FIND IT FAST: HOW TO UNCOVER EXPERT INFORMATION ON ANY SUBJECT

Robert Beckman, Author
Harper Collins, Publisher
$13, Cost
(800) 427-7372

As described--an essential handbook for the analyst interested in exploiting the open source world.

FIND/SVP

Mr. Joseph Cositore, Vice President
625 Avenue of the Americas
New York City, NY 10011-2002
Voice: (212) 645-4500
Fax: (212) 645-7681

FIND/SVP ("SVP" in French stands for "if you please") specializes in obtaining any article, any document, through a world-wide network of franchises. It does almost no analysis, just acquisition.

FULD & COMPANY

Mr. Leonard Fuld, President
80 Trowbridge Street
Cambridge, MA 02138
Voice: (617) 492-5900
Fax: (617) 492-7108

Publisher or *The New Competitor Intelligence*, a handbook for business intelligence specialists. Includes resource listing--strongest of Europe.

GaleNet

GaleNet can be used by anyone with an Internet connection, either dial-up or direct, and a graphical World-Wide-Web browser. The Web site offers a demonstration area. OSS tested their site by accessing the *Encyclopedia of Associations*, using the word "information", and found 138 associations that have "information" in the keyword search field. To arrange for a demonstration of GaleNet at your site, or for more information, please call the National Field Sales Manager, Mr. Tim Brandner, at (510) 671-5379, or send email to <Tim brandner@gale.com>.

Genuine Article

A service of the Institute of Scientific Information. Contact Mr. Frank Spiecker, 3501 Market Street, Philadelphia, PA 19104. Voice: (215) 386-0100 extension 1374; Facsimile: (215) 386) 6362. Web: <http://www.isinet.com/>.

GUIDE TO NETWORK RESOURCE TOOLS

by European Academic & Research Network
Free of charge online
Go to <listserv@earncc.bitnet>
Send command <GET NETTOOLS PS> (for postcript) or
Send command <GET NETTOOLS MEMO> (for plaintext)
Covers Archie, Astra, Bitftp, Gopher, Listserv, Netnews, Netserv, Trickle, WAIS, Whois, and World-Wide-Web

As described.

INDIVIDUAL, INC.

Director, New Business
8 New England Executive Park West
Burlington, MA 01803
Voice: (617) 273-6000
Fax: (617) 273-6060

This is one of the finest "current awareness" services, providing a one page listing of "hits" on your profile by fax or email, with full-text available immediately through automated order.

Information Broker's Handbook

By Sue Rugge and Alfred Glossbrenner. Published by Windcrest/McGraw-Hill, 1992. ISBN 0-8306-3797-4. $30.95, order through local bookstores.

INFOSOUTH

University of Miami
(800) 752-9567

Translations of Latin American press. biographies on Latin American leaders.

INSIDE INFORMATION: PROFILES OF ASSOCIATION LIBRARIES AND INFORMATION CENTERS

Special Libraries Association
Mr. Kevin Heffner, Director
Fund Development
1700 Eighteenth Street, N.W.
Washington, D.C. 20009
Voice: (202) 234-4700 ext. 631
Fax: (202) 265-9317

This is the international organization that serves over 15,000 librarians in charge of small specialized libraries for associations, corporations, or other special interests. This is an essential networking vehicle for reaching limited edition publications, especially in economic and financial arena.

International Thomson Publishing

Their Web site is located at <http://www.thompson.com>. To receive a catalog you can write to them at 7625 Empire Drive, Florence, Kentucky 41042, call voice (800) 865-5840, facsimile (606) 647-5013, or send email to <americas-info@list.thomson.com>

JANE'S INFORMATION GROUP

Mr. Robert Loughman
Sales Consultant
1340 Braddock Place, Suite 300
Alexandria, VA 22314
Voice: (703)683-3700x202
Fax: (703) 836-0297

The Jane's periodicals, database, and *SENTINEL* Country Series are "best in class" for military information. Jane's is also available online. It is important to know that Jane's only publishes 20% of what it knows, ask for unpublished info.

KROLL ASSOCIATES

Mr. Thomas Fedorek, Managing Director
900 Third Avenue
New York, NY 10022
Voice: (212) 593-1000
Fax: (212) 593-2631

This is by all press and other accounts the world's best investigative firm, able to obtain scientific & technical information as well as other nominally sensitive information, using legal & ethical means.

LEXIS-NEXIS

Mr. Jeff Krattenmaker
Government Information Services
9393 Springboro Pike, P.O. Box 933
Dayton, OH 45401-0933
Voice: (513) 865-1877
Fax: (513) 865-7902

Together with DIALOG, one of the top two commercial online services, but perhaps best suited to be the "first stop". followed by DIALOG and other region-specific online services. "Government-friendly" and responsive.

Mercyhurst College

Mr. Robert Heibel, Program Director, Research/Intelligence Analyst Program. Mercyhurst College, Department of History, Erie, Pennsylvania 16546. Voice: (814) 824-2117, fax: (814) 824-2219.

MONTEREY INSTITUTE OF INTERNATIONAL STUDIES

Dr. Christopher Fitz
Senior Manager
PNS, 425 Van Buren Street
Monterey, CA 93940
Voice: (408) 647-4193
Fax: (408) 647-3519

Uses graduate students fluent in Arabic, Russian, Vietnamese, and Korean, and other languages, to monitor media and maintain world's best unclassified database on proliferation--used by CIA's NPC.

NERAC

Manager, New Business
One Technology Drive
Tolland, CT 06084-3900
Voice: (203) 872-7000
Fax: (203) 875-1749

Combines DIALOG and university experts to offer an annual "fixed price" research service that many businesses find to be responsive and cost-effective.

netguide

"TV Guide" of cyberspace
Covers 60,000 bulletin boards
9,000 networks, 500 libraries,
all commercial online services
384 pages, $19.00, (800) 345-8112

As described--there are increasing numbers of such guides, most at higher prices. This is a good starting point.

***NEWSEDGE* FROM DESKTOP DATA**

Ms. Emily Elliott, Assistant Marketing Manager
Financial Markets
1601 Trapelo Road
Waltham, MA 02154
Voice: (617) 672-2425
Fax: (617) 890-1565

This unique service combines the normal current awareness service with the ability to deliver data directly into existing local area networks & database structures.

OXFORD ANALYTICA

Mr. Robin Porteus
Director of Client Services
5 Alfred Street
Oxford OX1 4EH
UNITED KINGDOM
Voice: (44 1865) 261-600
Fax: (44 1865) 242-018

Founded by Mr. David Young, who served on the National Security Council with Dr. Henry Kissinger, this is the best international window into political and economic reporting. Combines the Dons of Oxford and 1000 experts worldwide, with a 24-hour media monitoring service.

PARVUS-JERICHO

Mr. Gerard Burke, Chairman
8403 Colesville Road
Suite 610
Silver Spring, MD 20910
Voice: (301) 589-4949
Fax: (301) 589-0007

After Kroll Associates, one of the best international investigative organizations. Mr. Burke served previously as the Executive Director of the President's Foreign Intelligence Advisory Board, and can support community needs.

Questel/Orbit

Communicate with them at Questel/Orbit, Inc., France Telecom Group, 8000 Westpark Drive, McLean, VA 22102, voice (703) 442-0900, or facsimile (703) 898-4632.

RAPPORT RESEARCH & ANALYSIS (UK)

Mr. Charles Pettifer, Director
Mr. Kevin Dodd, Director
11 Berkeley Street
Mayfair, London W1X 6BU ENGLAND
Voice: (44 171) 355-5020
Fax: (44 171) 355-5021

This organization can provide trained debriefers fluent in any language to any place in the world. Especially good at canvassing refugee and emigre communities for raw intelligence.

RESEARCHBASE

Mr. Frank J. Vega, President
Post Office Box 187
Arlington, VA 22210
Voice: (703) 271-5988
Fax: (703) 271-5989

This very low-cost ($500) database is an essential means of saving money by avoiding redundant research in all major international relations areas. Tap into existing research for starters!

Research Centers Directory

Sometimes titled *Research Centers and Services Directory*. Available from Gale Research for $400 (two volumes). ISBN 0-8103-7353X.

Rice University

Call (313) 764-9366 to obtain information on gaining access to the Economic Bulletin Board Service (BBS).

RISA SACKS ASSOCIATES

Ms. Risa Sacks, President
3838 14th Avenue
Oakland, CA 94602
Voice: (510) 530-6154
Fax: (510) 531-9086

Telephone surveys and telephone "discovery" of key elements of information is an art, and Ms. Risa Sacks is acknowledged by her peers as one of the best in the USA.

SCIENCE CITATION INDEX, SOCIAL SCIENCE CITATION INDEX

Institute for Scientific Information

Frank Spiecker
3501 Market St.
Philadelphia, PA 19104
Voice: (215) 386-0100 ext.1374
Fax: (215) 386-6362

This organization combines a citation database that will identify the latest articles based on known earlier publications, and also identify emerging technologies as well as key experts.

Secrets of the Super Searchers

By Reva Basch, 1993. Order directly from Eight Bit Books, 462 Danbury Road, Wilton, CT 06897-2126. ISBN 0-910965-12-9. $39.95 plus shipping & handling.

SIS INTERNATIONAL RESEARCH

Ms. Ruth Stanat, President
490 South Main Street
New City, NY 10956
Voice: (914) 639-1934
Fax: (914) 639-6936

Complements Fuld & Company with special strengths in Latin America and Asia; primarily a business/marketing research organization.

SPOT IMAGE CORPORATION

Mr. Clark Nelson, Director of Communications
1897 Preston White Drive
Reston, VA 22091
Voice: (703) 715-3100
Fax: (703) 648-1813

They have, in hand, 10 meter resolution panchromatic and multispectral imagery for almost the entire world, and can produce both combat charts and simulations quickly.

STN International

STN Service Center, c/o Chemical Abstracts Service, 2540 Olentangy River Road, Columbus, OH 43210. Voice: (800) 848-6533, facsimile (614) 447-3798. Email: <help@cas.org>.

The Reference Press, Inc.

Among its offerings are a variety of directories and guides to international business sources and information for Latin America, Canada, Europe, Asia Pacific, and Russia. For a catalog call (512) 454-7778 or fax (512) 454-9401.

WORLDWIDE GOVERNMENT DIRECTORIES

Mr. Jonathan Hixon, Publisher
7979 Old Georgetown Road, #900
Bethesda, MD 20814
Voice: (301) 718-8770

Mr. Keith Hall invented the term "ASK-INT". This is the directory. They also publish government and military

Fax: (301) 718-8494

biographies for leaders worldwide.

UNCOVER REVEAL

Uncover Company
3801 East Florida
Suite 200
Denver, CO 80210
Voice: (303) 758-3030
Email: <mwhitaker@carl.org>

Building on the University of Colorado's existing infrastructure, they will deliver for a nominal cost to your email or fax the tables of contents of all journals you wish, as they are published--then you can order articles from any source.

UNITED PRESS INTERNATIONAL

Ms. Alison Myers
Director of Business Development
UPI Photo Network
Voice: (202) 898-8248
Fax: (202) 371-8247

A picture can be worth a thousand words. Analysts interested in using visual images to improve the intelligence consumer's absorption of the intelligence product's content can call on this resource.

University of Michigan

Send electronic mail to <lou@umich.edu> to obtain information on gaining access to the electronic clearinghouse.

APPENDIX E-1

Internet: Self-Guided Tour

by Dr. Ross Stapleton-Grey <director@embassy.org>

1. Philosophy
2. Strategies
3. Useful Tools
4. Starting Points
5. Print and Other Resources
6. USENET Illustration

Philosophy

The Internet is a steadily changing thing. What's there today will almost certainly be different tomorrow, either for the better, or for the worse! This poses a challenge when useful resources disappear, whether because they've been abandoned, or simply moved with no apparent forwarding address. On the other hand, hosts of new resources are being created every day... faster than they're being cataloged. The Internet has been described as "a wonderfully rich library, but all the books are lying in heaps on the floor."

The last few years have seen a number of wonderful navigational aids created, including powerful search engines, and comprehensive catalog sites for Web page creators to register their resources. But there will always be a place for serendipity, and certainly it helps to have a network of contacts and colleagues to pass along leads.

Strategies

The best strategy in looking for information via the Internet is to cast a broad net: Web sites will lead to others, or cite newsgroups or mailing lists, or vice versa, and human contacts made through the Internet can pass along useful nuggets.

All of the major Web browsers support "bookmarking," i.e., saving pointers to particularly useful or interesting destinations once you've found them (placing them on your "hotlist"). A helpful strategy is to bookmark all of the initial tools--query sites, or especially rich indexes--you might need, along with other sites you'll need to check regularly.

Useful Tools

The following are useful tools for the Internet (and especially, World Wide Web)

navigator. They can also be thought of as starting points: the skilled Internet navigator will make use of any number of search and catalog sites, to access familiar resources, or to launch off into undiscovered territory with a few search keywords.

Alta Vista - http://altavista.digital.com

One of the newest search engines, established by Digital Equipment Corporation (DEC), a major mid-range system manufacturer, as a technology demonstrator and a means to attract an audience. The service claims to index 8 billion words from some 16 million Web pages, and to continuously update its contents, retiring old materials no longer found, and adding new pages when encountered (some indexes don't--or can't--retire old pages, and may return links that lead to nowhere).

Alta Vista is the most impressive raw search engine for the World Wide Web thus far created. In addition to simple queries, one can structure complex searches, with weighted terms, and all of the usual Boolean search qualifiers. But the search tool has also been designed to meet the specific needs of Web navigators: one can search by date of the document (critical when what's needed is current information, and not some aging Web page with last year's news), and for URLs (Web page "universal resource locators," the "http:www.etc..."). The latter allows for neat tricks: check Alta Vista's help menus for directions on how to search for all of the Web pages that reference a certain other page, or how to find all of the pages mentioning certain terms, but which are not at some given address.

In addition to searching for Web pages, Alta Vista can search the most recent traffic in many of the USENET news groups.

Yahoo - http://www.yahoo.com

The most significant index in the Web's first major growth spurt, and the first comprehensive index of sites. Having one's Web site registered in Yahoo was (and is) a necessity. Yahoo involves human cataloging (submitters request where they would like to be filed, but Yahoo staff implement all linking), as opposed to the full-text indexers like Alta Vista. Where Alta Vista is an excellent tool to pull in anything and everything matching a given set of keywords, Yahoo's strength is in its organization. It would be extremely difficult to compile an exhaustive list of organizations in a given field by sifting through the mixed page of Web pages returned by Alta Vista; Yahoo will have a well-ordered index of companies divided and subdivided up according to a logical hierarchical structure. On the other hand, while Alta Vista vacuums up and indexes anything it can find on the Web, Yahoo is only as thorough as submitters and catalogers make it.

Yahoo also has an arrangement with Reuters to provide current newswire material through its site. The "Xtra" pages provide breaking items (a dozen or so per category) in Politics, News and World News, Business, Internet and Computers, and a half dozen other

areas.
http://webcrawler.com

An early full-text indexing tool, bought by America OnLine for more than a million dollars. It's included here largely for historical reasons, as other tools like Alta Vista seem to be eclipsing it. Webcrawler also has the annoying feature that it retains everything ever put in its index: pointers to Web pages that have been deleted long ago will still be found, and will give the user the famous "404 - URL Not Found" error when the link is followed.

A number of other services provide searching of extensive amounts of the World Wide Web, including OpenText (http://www.opentext.com) and Infoseek (http://www.infoseek.com).

Starting Points

All of the search tools mentioned previously are excellent starting points. In addition to those, the following sites are rich indexes to their various areas:

NewsPage - http://www.newspage.com

NewsPage is a valuable site for industry information, including the telecommunications, energy, pharmaceutical and other industries. The site pools press releases and other news from a variety of other online services, and organizes them by category. While the site bases some of its revenues on advertising, it also charges premium subscription fees for some of its articles, and for use of a search facility.

Online Newspapers - various

Numerous "physical" news papers such as the Detroit News, San Francisco Chronicle, and New York Times have created Web versions to allow readers greater access to their stories, and to complement the print versions.

The Detroit News Web site (which was launched, coincidentally, as the print paper was in the middle of a union strike, and which has provided news on the strike as an editorial soapbox for the paper) is a good example of a Web site's use of a structured presentation: each day's format is identical, even if the content changes, providing a familiar layout. The Detroit News Website is at http://detnews.com.

Other good jumping off points to online newspapers:

Yahoo's newspaper index:

http://www.yahoo.com/Business_and_Economy/Companies/Media/Newspapers/

The Newspaper Association of America homepage : http://www.infi.net/naa/hot.html

The White House - http://www.whitehouse.gov

In addition to holding information on the White House, the Executive Office of the President, and the texts of presidential and vice presidential speeches, the White House Web site is the "site of sites" for the Federal Executive Branch. White House staff have taken considerable care to encourage Federal agencies to provide Web addresses, and the site indexes all of the major cabinet offices and a great many of the other agencies, bureaus and programs.

The WELL's War Conference, IW sites -
http://www.well.com/conf/war/iwsites.html

Participants in the War conference on the WELL (a large online conferencing system based in Northern California but with users worldwide) have compiled an extensive reference of Web sites of interest to the "Information Warrior" (largely of defense, economic security and
intelligence related sites). Some of the sites included on the list (a small sampling):

The White House's Information Infrastructure Task Force - http://www.iitf.doc.gov
Office of the Secretary of Defense - http://enterprise.osd.mil
US Air Force - http://www.afin.af.mil
Air Force 38th E&I Wing - http://www.eiw38.af.mil/cshome.html
Central Intelligence Agency - http://www.odci.gov/cia
Intelligence Community - http://www.odci.gov/ic

Electronic Embassy - http://www.embassy.org

The Electronic Embassy Web site is an index to information, including Web homepages where available, from the foreign embassy community in Washington D.C.

All of the above ought to be considered merely starting points, and most lead quickly to many other resources. The White House site is an exhaustive list of Federal agencies, while the Electronic Embassy is a quick shortcut to find the State Department, foreign affairs committees of the Congress, or the United Nations.

The more the Internet begins to parallel the "real world," that is, as having a Web site becomes the rule for companies, and not just the innovative exception, traditional clearinghouses will have a role to play. The Software Publishers Association (http://www.spa.org), for example, has long been an advocacy organization for the software industry, with a large number of the most significant software producers as members. The SPA Web site, extending its member services onto the Internet, provides a lengthy index to all of its members, with pointers to their own Web sites.

There are excellent "theme" pages created by individuals, compiling exhaustive lists of known resources on the Web under a given topic area. These might range from Feminist Activist resources (Sarah Stapleton-Gray's page at IGC - http://www.igc.org/women/feminist.html) to anything and everything related to telecommunications organizations, technologies and policy (Jeff MacKie-Mason's page at the University of Michigan, http://www.spp.umich.edu/telecom-info.html). While one could try to compile a list of these lists (and to some extent such a thing has been done with Yahoo). spending even a small amount of time "surfing" the Web is guaranteed to turn up such useful references, which can then be bookmarked.

Print and Other Resources

The nature of the Internet is such that virtually any print resource, and certainly any that attempts to document an exhaustive list of anything, be it USENET newsgroups or "the best Web sites for...," becomes obsolete in a manner of months. That said, there are some fairly useful books on various aspects of the Internet and the World Wide Web, which can give a good feel for the tools and the Internet's content, while recognizing that any given list of Web sites will have changed even as the book went to the printers.

The O'Reilly and Associates series of books are essential reading for the nuts and bolts of how the Internet works. *The Whole Internet User's Guide and Catalog* is a basic primer, with extensive (but, of course, fast-aging) lists of useful sites, mailing lists and newsgroups. *Managing Internet Services* provides extensive information on the technical details of Gopher, Majordomo (mailing list software) and the World Wide Web--not for the novice but providing for a complete understanding of how all of these features actually work.

HTML Sourcebook, by Ian S. Graham (John Wiley & Sons, publisher) is a good overview of how to create pages for the World Wide Web, again providing good insight into how the Internet supports the Web, and how Web sites work. The book provides walk-throughs of several actual sites, dissecting them to show how the Web can be used to deliver information, query users using forms, etc.

Members of the Internet Society receive its "On The Internet," a bi-monthly magazine on Internet issues and features. Individual membership in the Society is $35 per year. ISOC may be reached at:

The Internet Society
12020 Sunrise Valley Drive, Suite 210
Reston VA 22091
(703) 648-9888

ISOC also has a Web site:
http://www.isoc.org as does its
DC area chapter:
http://www.dcisoc.org

USENET Illustration

NOTE: For each of these, the first column is the message number. the second column shows the number of replies, if any, followed by the message title and the poster's userid.

From soc.culture.kuwait:

97	+	(FWD) BAHRAIN: Amnesty Int'l Appeal	socakh@pmail.ldc.lu.se
98	+	TEST -- ignore -- TEST --	Furqan (truth@reality.com
99	+ 2	(Fwd) Bahrain News/more	socakh@pmail.ldc.lu.se
100	+	Test!! Please ignore	Badran (badran@kuwait.net
101	+	Online Zakat Payment	Sohail Mohammed (zakat@di
102	+ 3	My visit to Kuwait	Lee Cooper (leec@kuwait.n
103	+ 2	WANTED: STAMPS.....PLEASE,...,.PLEA	Carol (carol@cam.org)
104	+ 2	Immigrate To C A N A D A	lfrank@interlink.net
105	+	WWW Islamic Server: What's New!	Muslim Student Associatio
106	+	Canada - employment opportunities	Colin R. Singer (csinger@
107	+	-How can we benefit from the Internet?	Al-Sirat Al-Mustaqeem Mag
108	+ 3	"I love you" in many languages Re: Ple	Gaspar Rodriguez (grodrig
109	+	Telethon for Islamic Centre for Kingst	Thomas (Aalim Zakee) Feve
110	+ 3	SMITH	Sbostic@loveits.com
111	+	Ramadhan Radio 107.4 FM. London	m.asghar@ic.ac.uk
112	+ 2	arranged marriages	Shoba Narayan (shoba@i-20

From alt.current-events.bosnia:

113	+	"Vise-parlamentarizam" -- metod veleiz	Y Rapido (rapido@eskimo.c
114	+ 3	Wars for Succesion of Yugoslavia / WEB	d.d. chukurov (ddc@bellco
115	+	Yugoslav Daily Survey. 2/2	d.d. chukurov (ddc@bellco
116	+	Serbia Today, 2/2	d.d. chukurov (ddc@bellco
117	+	Yugo Wars - Stay Informed - Visit : g	d.d. chukurov (ddc@bellco
118	+ 2	Michael Axelrod strikes again	Frank Hendrix (Frank@accl
119	+ 7	Army witch hunts	RICHARD CASTROP (RCASTROP
120	+	Yugo Wars - Stay Informed - Visit : Vu	Barry S. Marjanovich (bsm
121	+ 3	appeal	barala@vossnet.co.uk
122	+	The three religius groups Moslem, east	Ben (smillieb@the.link.ca
123	+	Novi "bogovi" - "Hrvatska domovna" 12/	BorPet (borpet@aol.com)
124	+	idea: low-tech approach to safely remo	JGizdavic (jgizdavic@aol.
125	+	Bosnain to English dictionary	JGizdavic (jgizdavic@aol.
126	+	Serbia Today (After SREBRENICA)	Barry S. Marjanovich (bsm
127	+	Britain, Rose, SAS Stab-in-the-Back--t	Y Rapido (rapido@eskimo.c
128	+	YUGOSLAV WEEKLY SURVEY, 2/2	D.D. Chukurov (ddc@nyquis

From alt.politics.org.un:

97	+	6	WAR ON THE FED waged by Utah's Patriot	Tony Kimball (alk@pobox.c
98	+		UN Daily Highlights: 29 Jan, 1996 (Rev	Shawn H (c626193@mizzou1.
99	+		United Nations Update: 30 Jan, 1996	Shawn H (c626193@mizzou1.
100	+	6	Steve Forbes as a Phony Candidate	root (root@tailor.roman.o
101	+		United Nations Association of the Unit	Shawn H (c626193@mizzou1.
102	+	6	GORE CLINTON OUT	Fresh816 (fresh816@aol.co
103	+		United Nations Update: 31 Jan, 1996	Shawn H (c626193@mizzou1.
104	+	2	U.S. Public Support for U.N. Growing (	Rodney L. Cornelius (CORN
105	+	3	Slick Willie as a Phony Candidate	Mark O. Wilson (Mark.O.WI
106	+		U.S. Must Pay U.N. Dues says Defense W	Al Banner (ac590@FreeNet.
107	+		----Gen X Presidential Forum!!!	Mike Lee (mlee@harvard.ed
108	+	3	New site: Electronic Field Trip to th	Nancy K (nancyk@bga.com)
109	+	2	Setting the Record Straight (The UN I	Nancy K (nancyk@bga.com)
110	+		What is next for Michael New?	Archibald E. Roberts, LtC
111	+		United Nations Update: 1 Feb. 1996	Shawn H (c626193@mizzou1.
112	+	3	Michael New	Boulder Weekly (bweditor@

APPENDIX E-2

Intelligence-Oriented List of Useful Internet Sites

From the Staff of OSS, Inc. <oss@oss.net>

NOTE: The material which follows focuses primarily on World-Wide Web (www) sites because that is the overwhelmingly most productive environment. Gopher sites (menus providing access to text) and File Transfer Protocol (FTP) sites are still available but declining so quickly as to hardly be worth citing. Also, it is important to do your own searches for sites and to regularly update your lists. The Net is growing geometrically, and sites emerge (or die) every day. The sites listed below are simply illustrative, and by no means comprehensive. Besides regular searches of the www, analysts should subscribe to ListServs in their areas of interest--these deliver documents directly to an email address, and also allow for analysts to contribute commentary to the list for rebroadcast to others.

Top Guns

http://www.oss.net/oss/

The home page of OPEN SOURCE SOLUTIONS, Inc., a non-profit educational corporation that serves as an international clearinghouse for information about open sources, systems, and services, this site provides past issues of *OSS NOTICES* for free, and is soon to offer, also for free, digital copies of the two volume *Proceedings* from each of the annual conferences on open sources which have taken place since 1992. This site offers direct links to a number of other open source vendors and pertinent sites for open source intelligence.

http://www.tiac.net/users/jardines/434mid.html

These heavy-duty reservists, the 434th Military Intelligence Detachment (Strategic), created the first-ever *Open Source Intelligence Resources for the Military Intelligence Officer*, and kicked off an Army-wide effort that is now leading joint concepts and doctrine on the integration of open source intelligence into the all-source collection and production process.

http://www.awpi.com:80/IntelWeb/

The home page of *Intelligence Watch Report*, a daily electronic clipping service for intelligence-related news, and the only service of its kind focused strictly on national intelligence. Benefits from correspondents in Europe, Russia, and Asia.

http://www.fedworld.gov/

FedWorld, the central point of access to the entire U.S. government, very ably

developed and maintained by the National Technical Information Service. a self-sustaining activity of the Department of Commerce.

United States Government

http://www.whitehouse.gov/	The White House
http://www.loc.gov/	The Library of Congress
http://thomas.loc.gov/	U.S. Legislation OnLine.

United States Intelligence

http://www.odci.gov	Central Intelligence Agency
http://www.nsa.gov:8080/	National Security Agency
http://www.fbi.gov/	Federal Bureau of Investigation
http://www.ustreas.gov/treasury/bureaus/usss/usss.html	U.S. Secret Service
http://www.fas.org/pub/gen/fas/irp/nro/index.html	National Reconnaissance Office
http://www.awpi.com/IntelWeb/US/NCC/index.html	National Counterintelligence Center

United States Military

http://www.dtic.mil/defenselink/osd/index.html	OSD
http://www.dtic.mil/defenselink/osd/index.html	Joint Chiefs of Staff
http://www.army.mil/	U.S. Army
http://www.dot.gov/dotinfo/uscg/	U.S. Army Reserve
http://www.dtic.mil/airforcelink/	U.S. Air Force
http://www.dtic.mil/airforcelink/	U.S. Navy
http://www.navy.mil/navresfor/	U.S. Naval Reserve
http://www.hqmc.usmc.mil/	U..S. Marine Corps
http://www.dot.gov/dotinfo/uscg/	U.S. Coast Guard
http://www.dtic.dla.mil/c3i/	OSD C3I
http://www.dtic.dla.mil/dtiw/	Defense Technical Information Center

http://www.onestep.com:80/milnet/
MILNET: Open Source Military Information Database

http://www.dtic.dla.mil/defenselink/pubs/pentagon/index.html
The Pentagon
gopher://marvel.loc.gov:70/11/federal/fedinfo/byagency/military/
US DOD Gopher Sites

http://www.dtic.mil/airforcelink/pa/factsheets/Air_Force_Reserve.html
USAF Reserve

http://pages.prodigy.com/AL/20sfga/mid20sfga.html
Military Intelligence: 20th Special Forces Group

United States Unified Commands

http://www.dtic.mil/defenselink/factfile/chapter1/eucom.html	U.S. European Command
http://www.dtic.mil/defenselink/factfile/chapter1/pacom.html	U.S. Pacific Command
http://www.dtic.mil/defenselink/factfile/chapter1/pacom.html	U.S. Atlantic Command
http://www.dtic.mil/defenselink/factfile/chapter1/southcom.html	U.S. Southern Command
http://www.dtic.mil/defenselink/factfile/chapter1/centcom.html	U.S. Central Command
http://www.dtic.mil/defenselink/factfile/chapter1/spacecom.html	U.S. Space Command
http://www.dtic.mil/defenselink/factfile/chapter1/socom.html	U.S. SpecOps Command
http://infosphere.safb.af.mil/TRANSCOM/	U.S. TransCom
http://www.dtic.mil/defenselink/factfile/chapter1/stratcom.html	U.S. StratCom

Related U.S. Sites

http://huachuca-usaic.army.mil/	USAIC/Schoolhouse
http://www.dtic.dla.mil/dtiw/	Defense Technical Information Web

gopher://UMSLVMA.UMSL.EDU:70/11/LIBRARY/GOVDOCS//BNOTES
U.S. State Department Country Reports

http://www.esd.ornl.gov/doe-labs/doe-labs.html
(U.S. Department of Energy National Laboratories & Programs)

http://dosfan.lib.uic.edu/
(Department of State Foreign Affairs Network)

Associations & Organizations

http://www.cais.com/NMIA/HomePage.html"	National Military Intelligence Association
http://www.cais.com/zhi/OPSHomePage.html	Operations Security Professionals Society
http://www.loyola.edu/politics/intel.html	Loyola Page on Strategic Intelligence
http://www.acsp.uic.edu/oicj/pubs/	Office of International Criminal Justice
http://www.cdi.org/	Center for Defense Information
http://nsi.org/	National Security Institute
http://www.eff.org/govt.html	Electronic Frontier Foundation

More Related Publications

http://www.jedefense.com/jed.html	Journal of Electronic Defense

http://ursula.blythe.org/NameBase NameBase News
http://www.worldmedia.com/caq/ Covert Action - Home Page
http://www.awpi.com/IntelWeb/US/S-GB/index.html
Secrecy & Government Bulletin

Cyber War

http://www.tcst.com/~tighe/ Mike Tighe's Cryptology Home Page
http://www.psycom.net/iwar.1.html Information Warfare, I-War, Cyberwar
http://www.disa.mil/ciss/itso.html DISA - Information Security
http://all.net/ InfoSec
http://freeside.com/phrack.html Phrack - underground hacker magazine
http://www.gocsi.com/ Computer Security Institute
http://dubhe.cc.nps.navy.mil/~budden/ IW - US Navy
http://www.cse.dnd.ca/~formis/ IW - Resources

http://www.csto.arpa.mil/ResearchAreas/Defensive_Information_Warfare.html
IW database

http://carmen.artsci.washington.edu/propaganda/contents.htm
Propaganda - Disinformation Warfare

http://www.monmouth.army.mil/peoiew/peoiew.html
Intelligence and Electronic Warfare

Foreign Countries - US Sources

gopher://UMSLVMA.UMSL.EDU/11/LIBRARY/GOVDOCS/ARMYAHBS
US Army - Foreign Intelligence Agencies

gopher://UMSLVMA.UMSL.EDU:70/11/LIBRARY/GOVDOCS//BNOTES
US State Dept.: Report by Country

gopher://UMSLVMA.UMSL.EDU:70/11/LIBRARY/GOVDOCS//WF93/WFLATEST
US CIA: Report by Country

http://www.ncsa.uiuc.edu/SDG/Experimental/soviet.exhibit/soviet.archive.html
Library of Congress Soviet Archives Exhibit

Foreign Countries

http://watserv1.uwaterloo.ca/~brobinso/cse.html
The Unofficial Communications Security Establishment Webpage

http://www.reading.ac.uk:80/SecInt/
Great Britain - SECURITY AND INTELLIGENCE

http://www.awpi.com/IntelWeb/Palestine/index.html
Palestinian Intelligence Community

http://www.primenet.com/~lion/j.html#issue
USSR - The Third World Countries & US

gopher://infx.infor.com:4600/11.browse/ESPIONAGE
ESPIONAGE - publications

http://www.odci.gov/mapspub/index.html
CIA Maps & Publications

On-line Search

http://webcom.com/%7Epinknoiz/covert/ciabasesearch.html	CIABASE On-line
http://www.btg.com/janes/	BTG Jane's EIS - on-line
http://www.janes.com/janes.html	Jane's Information
http://www.mayhem.net/Crime/	Crime Archives
ftp://wiretap.spies.com/	Directory of Wiretaps
ftp://ftp.lglobal.com/pub/foreignc/	The Foreign Correspondent:

http://world.std.com/~mmoore
INVESTIGATIVE DATABASE: Boston, MA

http://www.delve.com/consort.html
The Consortium - Investigative Reports

telnet://ursula.blythe.org
NAMEBASE telnet version - telnet gateway required. Log in as "namebase"

http://ursula.blythe.org/NameBase/bookindx.html
NAMEBASE - Web version

Military Intelligence - Non-Governmental Resources

http://www.infomanage.com/international/intelligence/default.html
Intelligence Resources

http://www.cdi.org/
Center for Defense Information

http://www.tscm.com/
TSCM.COM Counterintelligence Home Page

http://www.interlog.com/~vabiro/
Counter-Terrorism

http://www.interport.net/~sagal/ajax.html
AJAX MILITARY, INTELLIGENCE & LAW ENFORCEMENT AGENCY ACCESS

http://www.acsp.uic.edu/oicj/pubs/
Office of The International Criminal Justice

http://www.essential.org/nautilus/
Nautilus Institute for Security and Sustainable Development

http://www.fas.org/pub/gen/fas/
Federation of American Scientists Home Page</A>

http://www.usdoj.gov/ojp/rol/docs/home.html
Rule of Law Online

http://www.webcom.com/%7epinknoiz/politics.html
Political Investigations

http://www.interaccess.com/trc/tsa.html
Technical Services Agency

http://www.rssi.ru/
Russian Space Science

http://www.peak.org/~danneng/decision/int-law.html
War Crime Laws

United States Military & Defense Laboratory Servers

http://www.arc.umn.edu/html/ahpcrc.htm
Army High Performance Computing Research Center

http://www.arpa.mil/
Advanced Research Projects Agency

http://bradbury.nrl.navy.mil/general/bmdo.html
Ballistic Missile Defense Organization Test Data Centers

http://www.dtic.dla.mil:80/lablink/
(U.S. Department of Defense Laboratory System

http://www.nrl.navy.mil/
The Naval Research Laboratory

http://www.rl.af.mil:8001/
(USAF Rome Laboratory for C41 Technology

Weapons and Their Transfers

Gopher://csf.colorado.edu:70/11/peace/pubs
General information

http://www.atcon.com/stores/armament/index.htm
Armament Technology

http://www.pal.xgw.fi/hew/
The High Energy Weapons Archive

http://nuke.handheld.com/
Nuke Home Page

http://neutrino.nuc.berkeley.edu/neutronics/todd.html
Todd's Atomic Homepage

http://www.earthlink.net/~bkonop/GermIncidents2.html
GERM WARFARE

http://www.opcw.nl/guide.htm
The Chemical Weapons Convention

http://www.aber.ac.uk/~ctj94/
Bombs 'n' Bullets

http://www.umcc.umich.edu/~schnars/texte/fore-cod.htm
Code Names and Numbers for Weapons

Law Enforcement

http://www.ustreas.gov/treasury/bureaus/atf/atf.html
Bureau of Alcohol, Tobacco and Firearms

http://gopher.usdoj.gov/bureaus/bop.html

Federal Bureau of Prisons

http://www.ustreas.gov/treasury/bureaus/fincen/fincen.html
Financial Crimes Enforcement Network

http://www.ustreas.gov/treasury/bureaus/fletc/fletc.html
Federal Law Enforcement Training Center

http://gopher.usdoj.gov/bureaus/usm.html
U.S. Marshals Service

http://nletc.aspensys.com:83/nletchome.html
National Law Enforcement Technology Center

http://www.ustreas.gov/treasury/bureaus/usss/usss.html
Secret Service

http://www.gate.net/~customs/
U.S. Customs Service Office of Investigation

Commercial Intelligence & Industrial Espionage

http://w3.lanter.net/NEWR/	NEAL E. WILSON RESEARCH
http://infomanage.com/icr	Asia Business Intelligence
http://www.webcom.com/~thames/spy/	MIND YOUR OWN BUSINESS
http://www.jax-inter.net/ispy/	Somers & Associates
http://www.ipn.net/	Information Professionals Network

Security Resources & Services

http://nsi.org/	Security Resource Net
http://www.ozemail.com.au/~hotsec/index.html	HTSCORP Home Page
http://www.fsk.ethz.ch/D-REOK/fsk/defs_intn.html	International Security Network
http://www.t8000.com/eci/brief.htm	Cellular Surveillance Systems
http://chelsea.ios.com/~glenz/	Corporate Security - Sigma Group
http://www.canadamalls.com/provider/horvath.html	The Spy Depot
http://www.w2.com/docs2/z/spyshop.html	THE SPY SHOP
http://www.hometeam.com/apex.shtml	Apex Home Page
http://www.trcone.com/tsa.html	The Codex Home Page
http://www.ozemail.com.au/~hotsec/hitec.htm	HI TECH Securities Services
http://www.iapps.org/	Bodyguard Home Page
http://www.best.com/~cntrspy/	Bodyguard
http://www.shadow.net/~trinfo/	TR Information Services
http://www.wta.com/giin/	Global Investigations & Information

http://www.tiac.net/users/cgb/din	Detective Information Network
http://www.mja.net/pub/continen/	Continental Investigative Service
http://www.integctr.com/	Integrity Center: Risk Management
http://lainet3.lainet.com/factfind/	Investigative Resources
http://www.tecs.com/irrs	Investigators Resource and Referral

http://www.yahoo.com/Business/Products_and_Services/Security/
Yahoo - Security < /A > < br >

http://www.yahoo.com/Business/Corporations/Investigative_Services/
Yahoo - Investigative Services

International

http://www.ifs.univie.ac.at/~pr2gq1/uno
United Nations Crime Prevention & Criminal Justice

http://daedalus.dra.hmg.gb/
Defence Research Agency, United Kingdom

http://www.dreo.dnd.ca/
Defense Research Establishment, Ottawa, Canada

http://www.nato.int
North Atlantic Treaty Organization

Usenet Groups

news:alt.politics.org.cia
news:alt.politics.org.fbi
news:alt.politics.org.nsa
news:alt.conspiracy.amer51
news:sci.crypt"
news:talk.politics.crypto

APPENDIX E-3

Intelligence (Related) Sites from *PC Magazine*'s Top 100 Web Sites

Selected by the Staff of OSS, Inc. <oss@oss.net>

NOTE: The sites listed below are drawn from "Web Sites 100: PC Labs Rates the Top 100", in *PC Magazine* Volume 15, Number 3 (6 February 1996). The quickest way to explore all of these sites is through the online version of the story, available at <http://wwkw.pcmag.com>, where the list will also be constantly updated.

Computer Resources

BrowserWatch http://www.ski.mskcc.org/browserwatch/

The best place to follow emerging Internet browser tools.

O'Reilly and Associates http://www.ora.com

Publishers of such respected books as *Computer Crime: A CrimeFighter's Handbook*, this organization is a good place to identify educational materials for all aspects of Internet research.

News & Sports

CNN Interactive http://www.cnn.com

Includes a video vault as well as a keyword search tool for past CNN stories. Could be the ideal source for downloading film and sound "snapshots" for a multi-media briefing.

Electronic Telegraph http://www.telegraph.co.uk/

The respected London newspaper.

Reuters NewMedia http://www.yahoo.com/headlines/current/news

Rapid bare-bones reporting, strictly text-based.

Time Magazine http://www.pathfinder.com/time

Everything you would expect, including *Time Daily*, late-breaking news.

USA Today http://www.usatoday.com

Retains its graphical excellence. Includes cyber-listings.

Government & Politics

FedWorld Information Network http://www.fedworld.gov/

Access to over 130 government bulletin boards as well as many government Web and gopher sites.

GPO Gate http://ssdc.ucsd.edu/gpo

Includes full-text of major GPO publications such as the *Federal Register*, *Congressional Record*, Senate and House calendars, and the United States Code.

The Library of Congress http://www.loc.gov

Includes THOMAS, a Web version of the *Congressional Record*, and other Capitol Hill publications. Often mis-represented as providing access to 70 million actual documents, what it really provides is access to the listing of such documents. It does have some full text material.

The United Nations http://www.un.org

Marginal in terms of substance, but some conference updates, news releases, and Security Council information.

Reference

Britannica On-Line http://www.eb.com

Costs money ($25 registration, $150 per year). Includes same content as bound edition, articles not yet in print, *Britannica Book of the Year*, and *Webster's Dictionary*.

CityNet http://www.city.net

While not a comprehensive guide, it does cover sites from Scotland to Africa, and is an interesting illustration of the kind of beach surveys and city maps that might one day be available to arriving military forces accessing the Internet from their landing platforms.

Science, Technology, & Medicine http://www.asap.unimelb.edu.au/hstm/hstm_ove.htm

Historical in nature, part of the Virtual Library, includes biographical information,

documents on every area of technology, a directory of scientific institutions, and electronic journals.

APPENDIX E-4

HOW TO FIND AN INTERESTING MAILINGLIST

Arno Wouters - Arno.Wouters@phil.ruu.nl
(with minor modifications by OSS, Inc. staff)

Last update: 5 February 1994

This document is available by email from "listserv@vm1.nodak.edu" with "GET NEW-LIST WOUTERS" or by anonymous ftp from "vm1.nodak.edu" as "new-list.wouters" in the directory "new-list".

(In compiling this information I have made ample use of Marty Hoag's "Some lists of list" (as of 05/01/92) which is retrievable from NEW- LIST as "LISTSOF LISTS")

TABLE OF CONTENTS

GENERAL INFORMATION ABOUT MAILINGLISTS
TWO NOTES ON ADDRESSES
SOURCES
TOOLS and METHODS
The LISTSERV "List of lists"
The SRI NISC "interest-groups" list of lists
The USENET lists of newsgroups and mailing lists
The Dartmouth SIGLIST
The "Directory of Scholarly Electronic Conferences" (ACADLIST)
NEW-LIST
LIST SEARCHES ON THE INTERNET

GENERAL INFORMATION ABOUT MAILINGLISTS

A mailing list is a computer program that distributes messages among a list of subscribers. This program has an email-address (listname@domain). Mail sent to this address is distributed automatically to all the subscribers.

There are two types of mailing lists: manually maintained lists and automated lists.

(1) In its manual form the list of subscribers is maintained by a person, the list administrator. To subscribe to such a list one should ask the list administrator to add you to the list. Typically the administrator can be reached at listname-request@domain.

(2) An automated list is maintained by a program (a so-called mailserver). To (un)subscribe to an automated list one should send a message to the mailserver. Usually.

this is the command "SUB listname Yourfirstname Yourlastname" to subscribe and "SIGNOFF listname" to sign off (substitute the appropriate names and leave off the quotes!).

A mailserver is a program that interprets the lines in a message as a series of commands to act on, for example to mail a file or to add a person to a mailing list. To learn how to handle a mailserver one should send a one line message containing the command "help" (no quotes!) to the mailserver's address. (In some rare cases, the mailserver needs an empty message with "help" in the subject).

LISTSERV is the name of the single most important mailserver on Bitnet. It provides three kinds of services: (1) mailing list management, (2) file archives, and (3) address registration. A userguide is available from LISTSERV@EARNCC.BITNET by sending it the command GET LSVGUIDE MEMO. The command HELP can be sent to any Listserv. It will give you a short list of commands. "INFO REFCARD" returns a longer list, "INFO GEN" a manual. Typically, if a list's address is LIST@NODE.BITNET the list is maintained by LISTSERV@NODE.BITNET. Alternatively, if LISTSERV@NODE.BITNET maintains a list named LIST the list's address is LIST@NODE.BITNET.

There are also Unix versions of Listserv that work on the Internet. Don't expect these versions to function exactly like the traditional Listserv.

IMPORTANT: One should carefully distinguish between the address of the list and the address of the administrator/mailserver. Never send requests/commands for (un)subscription to the list! Such a message would bother all the participants, but it would not help you to get on/off the list. Note, that the list administrator is often just that: one of the computer people who maintains the list, but is not himself a subscriber. Alternatively, a mailserver will only react to mail that is addressed to the mailserver's address, not to the address of the lists it maintains.

Type of list	Address of list	Requests/commands
Manually	listname@domain	listname-request@domain
LISTSERVed	listname@node.BITNET	LISTSERV@node.BITNET

TWO NOTES ON ADDRESSES

Internet addresses have the format user@domain (for example John.Doe@phil.ruu.nl). Bitnet uses the format user@bitnetnode (for example JDOE@HNYKUN51). To send mail from Internet to Bitnet append ".BITNET" to the Bitnet address (e.g. JDOE@HNYKUN51.BITNET). To send mail from BITNET to Internet one could use the Internet address without any changes.

Janet users in the United Kingdom should reverse the order of the Internet domainnames and Internet users outside the UK should reverse the order of Janet domainnames.

There are several lists of lists available. The main ones are:

-- the Listserv "list of lists" on Bitnet;
-- the Internet "interest-groups" list;
-- two lists of Usenet newsgroups;
-- the Usenet list of "Publicly Accessible Mailing Lists" on Internet and UUCP networks;
-- a combined list of Bitnet and Internet lists from Dartmouth (SIGLIST):
-- the "Directory of Scholarly Electronic Conferences" (ACADLIST), an annotated list of mailing lists, newsgroups, newsletters, electronic journals etc. that are of interest to academics;

Another important sources is:

-- NEW-LIST, a Listserved mailing list and archive for announcements of new lists. In addition, the NEW-LIST archive contains copies of both the Listserv and the "interest-groups" lists of lists in a searchable format.

NOTE: The WAIS based "lists" database on CIC-net has been dissolved.

TOOLS and METHODS

Basically, there are two methods to access these sources:

(1) on line searches

(2) retrieve a list and search through it at home (electronically or after printing).

As most lists are long, the first method is often the preferred one.

Internet tools for on line retrieval: gopher, WAIS, telnet (one tool would suffice, gopher is the preferred one for lists).

Listserv databases can be searched interactively from VAX/VMS and from VM/SP CMS systems. Other users should submit batch jobs by email. Send an "INFO DATABASE" to an appropriate Listserv for more information.

Tools for retrieving files: anonymous ftp (Internet only) and email. Make sure you have enough disk space available, since most lists are VERY long.

Tools for searching the retrieved files include your favorite word processor, GREP commands, hypercard etc.

The LISTSERV "List of lists"

The Listserv list of lists contains one line descriptions of Listserved lists on Bitnet. Most (but not all) Listservs will get you a copy after submitting the command "LIST GLOBAL". Most servers would also allow for the command "LIST GLOBAL /string" (e.g. "LIST GLOBAL /philos") to get those lists which have "string" in their description.

The SRI NISC "interest-groups" list of lists

This is a list with descriptions of special interest group mailing lists available on the Internet, compiled by Steven Bjork. New versions of this list are typically issued on a quarterly basis.

The file "interest-groups" (over 1.2 MB!) is available: by anonymous ftp from sri.com in the directory "netinfo", or by email from mail-server@sri.com ("send interest-groups").

A hardcopy, indexed version is available from Prentice Hall under the title *Internet: Mailing Lists* (ISBN 0-13-327941-3).

The USENET lists of newsgroups and mailing lists

David Lawrence maintains two lists of newsgroups on Usenet. The "List of Active Newsgroups" lists the regular Usenet newsgroups. The Usenet software also allows the transport of hierarchies of newsgroups not part of the "traditional" Usenet (bionet, alt-groups, bit.listserv etc.). These groups are listed in the list of "Alternative Newsgroup Hierarchies". Both lists contain one line descriptions.

Stephanie da Silva maintains the list of "Publicly Accessible Mailing Lists". This is a list of mailing lists available primarily through the Internet and the UUCP network. The list includes short descriptions of the purpose of the lists.

These lists are distributed via the Usenet newsgroups news.lists and news.answers (monthly updates). News.answers is archived at many sites. The files are named "active-newsgroups", "alt-hierarchies" and "mailing-lists". They can also be obtained from the MIT Usenet archive: by anonymous ftp from rtfm.mit.edu in "/pub/usenet/news.answers" or via email from "mail-server@rtfm.mit.edu". The appropriate commands are:

send usenet/news.answers/active-newsgroups/*

send usenet/news.answers/alt-hierarchies/*

send usenet/news.answers/mail/mailing-lists/*

The Dartmouth SIGLIST

David Avery from Dartmouth maintains a combined edited list (over 500 KB!) of Listserved and manually maintained lists on both Bitnet and Internet. The list includes short descriptions of the purpose of the lists and is sorted by category (computing, science, humanities etc.). It is updated monthly. Dartmouth provides several versions of the list. They also provide several applications (MacIntosh Hypercard, MSDOS, VM/CMS, VAX/VMS and Unix) that present the list in a nice format and facilitate searches.

SIGLIST is available:

-- by anonymous ftp from DARTCMS1.DARTMOUTH.EDU in directory SIGLISTS.

-- by email from LISTSERV@DARTCMS1.BITNET ("INDEX SIGLISTS" for a list of files and "GET READ ME" for more information)

The "Directory of Scholarly Electronic Conferences" (ACADLIST)

From the README file: "This directory contains descriptions of electronic conferences (e-conferences) on topics of interest to scholars. E-conference is the umbrella term that includes discussion lists, interest groups, e-journals, e-newsletters, Usenet newsgroups, forums, etc. We have used our own judgment in deciding what is of scholarly interest, and accept any advice or argument about our decisions."

ACADLIST (from Kent State University) is an annotated list. The entries are placed into categories according to the academic subject area of the e-conference. ACADLIST consists of 8 separate text files. Please note that the first four files contain several subject areas arranged in alphabetical order. FILE1 is titled: "Anthropology-Education", this means that it contains all the subject areas that fall alphabetically between A and E! The list is also available as a two file HYPERCARD stack and as a one file MS WORD document (MAC version!).

ACADLIST is available:

-- by anonymous ftp from KSUVXA.KENT.EDU in the directory "library" (get "acadlist.readme" for more information).

-- by email from LISTSERV@KENTVM.BITNET ("GET ACADLIST README"

for more information).

NEW-LIST

The NEW-LIST mailing list at LISTSERV@NDSUVM1.BITNET provides announcements of new mailing lists. To subscribe send the command "SUB NEW-LIST Yourfirstname Yourlastname" to the LISTSERV. The mailing list is gatewayed to Usenet as the newsgroup "bit.listserv.new-list". The NEW-LIST archive is the principal source for list searches. It contains three databases in a searchable format:

-- lists: the LISTSERV list of lists
-- intgroup: the Internet "interest-groups" list
-- new-list: the archived contributions to the NEW-LIST mailing list.

From Marty Hoag's "Some lists of lists":

For example, to search of both these databases for lists on "bicycles" you would send the statements

```
 //DBlook  JOB  Echo=No
Database Search DD=Rules
//Rules DD *
Select bicycle in lists
index
Select bicycle in intgroup
index
Select bicycle in new-list
index
/*
```

in the text/body of the mail to LISTSERV@VM1.NoDak.EDU or on BITNET just LISTSERV@NDSUVM1 . These statements would search the global LISTSERV list of lists ("in lists"), and the local copy of the SRI-NIC Interest Groups ("in intgroup"), and the archives of the "new-list" list ("in new-list")."

To get more information subsequently submit the following job (substitute "list-number(s)" by the numbers of the lists of interest found in the first job, separated by spaces):

```
// JOB Echo=No
Database Search DD=Rules
//Rules DD *
Select bicycle in lists
```

index
print list-number(s)
Select bicycle in intgroup
index
print list-number(s)
Select bicycle in new-list
index
print list-number(s)
/*

Send LISTSERV the command INFO DATABASE for more information.

LIST SEARCHES ON THE INTERNET

Many sites provide a searchable version of one or more lists of lists via gopher. To find them, connect via gopher to a Veronica-server (usually, you'll get there by choosing something like "Other gopher and information servers" in your main menu) and search for "-t7 list lists" "-t7 mailing lists" and/or "-t7 interest groups". The "-t7" addition assures that you'll get searchable versions only. A search for "list lists" will give you about 20 links, "interest groups" about 30, "mailing lists" more then 100, and "lists" more then 4,000. However, this method has several drawbacks. The most important one is that you can never be sure that the lists are regularly updated. There are sites that provide a version of February 1992! Another is that many of those links point to the ghosts of once existing databases (e.g. to lists.src or mailing-lists.src). The Lund University Library Services (Sweden) provides a searchable WAIS-based version of ACADLIST ("academic email conf.src"). There are several ways to access this database:

-- By means of your own WAIS client
-- There are more then 60 gophers linked to this database (use Veronica to find one).
-- Several gopher sites provide a general gateway to WAIS (e.g. the gopherhome in Minnesota).
-- Telnet to one of the following servers: quake.think.com (login: wais). nnsc.nsf.net (login: wais), swais.cwis.uci.edu (login: swais), sunsite.unc.edu (login: swais), or info.funet.fi (login: info)

ADDITION (15 May 1993)

The Association of Research Libraries publishes a hardcopy "Directory of Electronic Journals, Newsletters and Academic Discussion Lists" (ISSN: 1057-1337)" edited by Diana Kovacs and Michael Strangelove. This directory is derived from network-accessible files. The section on scholarly discussion lists and interest groups is derived from ACADLIST mentioned above. The section on journals and newsletters is derived from Strangelove's "Directory of Electronic Journals and Newsletters". This directory is available from several

sources, e.g. from LISTSERV@UOTTAWA.BITNET by sending the commands "get Ejourn11 Directory" and "get Ejourn12 Directory". To order the ARL directory contact Gloria Haws, Publications Manager of the Association of Research Libraries, email: osap@cni.org. The price of one copy is USD 42 plus postage, shipping and handling charges.

EXPEDITIONARY ENVIRONMENT RESEARCH & ANALYSIS FRAMEWORK & MODEL 1990

(DRAFT CONCEPT UNDER DEVELOPMENT)

USMC INTELLIGENCE CENTER
MARINE CORPS COMBAT DEVELOPMENT COMMAND
QUANTICO, VIRGINIA
(703) 640-3177/2268 GRAY 980-6109/10

CONTENTS

Brief.....Tab A
Military Capabilities.....Tab B
Operational Geography.....Tab C
Civil Factors.....Tab D
Insurgency Template & Framework Application.....Tab E

21 MAY 1990

OBJECTIVES & PURPOSE OF THE MODEL & SUPPORTING FRAMEWORK

- TO DEVELOP A GENERIC THREAT MODEL USEFUL TO MARINE CORPS PLANNERS & PROGRAMMERS USING THE CONCEPT BASED REQUIREMENTS SYSTEM (CBRS)

- TO DEVELOP A VALIDATED ANALYTICAL FRAMEWORK WHICH IDENTIFIES "CENTERS OF GRAVITY" AND KEY PLANNING & PROGRAMMING FACTORS ABOUT MILITARY CAPABILITIES AND PHYSICAL & HUMAN CONDITIONS AGAINST WHICH INTELLIGENCE ASSESSMENTS SHOULD BE DEVELOPED.

- SET THE STAGE FOR APPLYING THE FRAMEWORK TO COUNTRIES OF INTEREST TO THE MARINE CORPS IN ORDER TO DEVELOP A GENERIC UNCLASSIFIED INTELLIGENCE MODEL OF WHAT CAPABILITIES AND CONDITIONS WILL BE ENCOUNTERED BY THE MARINE CORPS IN THEIR MOST LIKELY AREAS OF OPERATION.

JUSTIFICATION FOR DEVELOPMENT OF A GENERIC FRAMEWORK

- USE OF THE SOVIET/WARSAW PACT AS THE ONLY "WORST-CASE" SCENARIO IS NO LONGER ACCEPTABLE

- THERE ARE ALTERNATIVE "WORST CASE" SCENARIOS IN THE THIRD WORLD WHICH MUST BE CONSIDERED

- IT IS NOT POSSIBLE TO DEVELOP A DETAILED REVIEW OF ALL COUNTRIES, OR ALL THIRD WORLD COUNTRIES, FOR EACH CBRS REQUIREMENT

- WHAT IS NEEDED IS A GENERIC MODEL BASED ON INTELLIGENCE ABOUT FACTORS WHICH PLANNERS & PROGRAMMERS HAVE IDENTIFIED AS IMPORTANT, AND IS:

  -- BASED ON COUNTRY-SPECIFIC REVIEWS FROM WHICH GENERALIZATIONS USEFUL TO CBRS CAN BE DRAWN;

  -- SPECIFIC ENOUGH AT THE UNCLASSIFIED LEVEL TO ENABLE PLANNERS & PROGRAMMERS TO DO ESTIMATES OR EVALUATIONS OF REQUIRED OPERATIONAL CAPABILITIES

  -- GENERAL ENOUGH SO THAT DETAILED & CLASSIFIED COUNTRY-SPECIFIC TECHNICAL ANALYSIS CAN "FIT" INTO AN OVER-ALL PACKAGE USEFUL TO MISSION AREA PLANNERS & PROGRAMMERS

EXPEDITIONARY ENVIRONMENT RESEARCH & ANALYSIS FRAMEWORK 1990

CONDITIONS & CAPABILITIES	HIGH	MEDIUM	LOW
MILITARY CAPABILITY			
OPS GEOGRAPHY			
CIVIL COMPLEXITY			

- FRAMEWORK DESIGN BASED ON COMBINATION OF NOIC BASELINE FOR NAVAL THREAT, IPB PROCESS, ORIGINAL WORK AND WARFIGHTING CENTER CONCEPTS AND PLANS AND MAA CRITERIA.

- AS ANALYTICAL FRAMEWORK DEVELOPS, MUST DEFINE WHAT IS TO BE MEASURED, HOW ("OBSERVABLES") FACTORS CAN BE MEASURED, AND, BASED ON INPUT FROM PLANNERS & PROGRAMMERS, WHY (JUSTIFICATION) FOR DIVIDING LINES BETWEEN "HIGH", "MEDIUM", AND "LOW" THRESHHOLDS FOR EACH FACTOR.

- FRAMEWORK WILL BE VALIDATED THROUGH COUNTRY-SPECIFIC ANALYSIS; VALIDATION WILL LEAD TO SPECIFIC TRUEISMS, GENERIC GENERALITIES, AND DEVELOPMENT OF NEW AND PERHAPS UNANTICIPATED GENERALITIES & SPECIFICS

WHAT THE FRAMEWORK DOES NOT DO

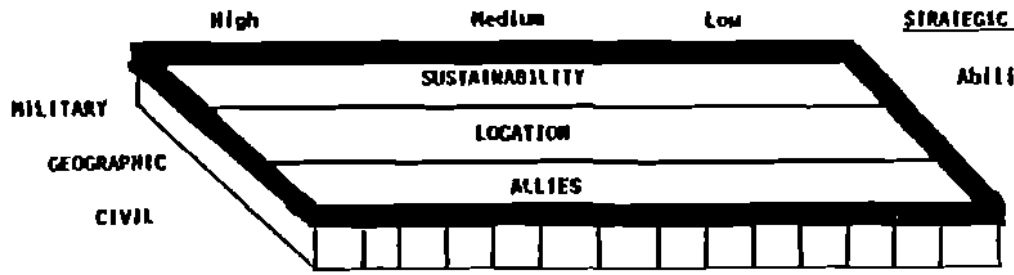
- THE FRAMEWORK DOES NOT PROVIDE CLASSIFIED TECHNICAL INTELLIGENCE PERTINENT TO SPECIFIC COUNTRIES, FACTORS, OR SYSTEMS TO BE EVALUATED

- THE FRAMEWORK DOES NOT PROVIDE "NET ASSESSMENTS" (COMPARISONS & JUDGEMENTS OF FRIENDLY VERSUS ENEMY CAPABILITIES & CONSTRAINTS)

- THE FRAMEWORK DOES NOT PRESCRIBE FRIENDLY REQUIREMENTS OR TACTICAL & OPERATIONAL CAPABILITIES TO BE CONSIDERED BY MISSION AREA PLANNERS & PROGRAMMERS

- THE FRAMEWORK IS NOT "FROZEN" AND WILL BE CONSTANTLY REVISED AS COUNTRIES, FACTORS, AND ACTUAL CONDITIONS & CAPABILITIES CHANGE, PROVIDING PLANNERS & PROGAMMERS WITH A "LIVING DOCUMENT"

CONCEPT OF OPERATIONS FOR INTEGRATED INTELLIGENCE ANALYSIS

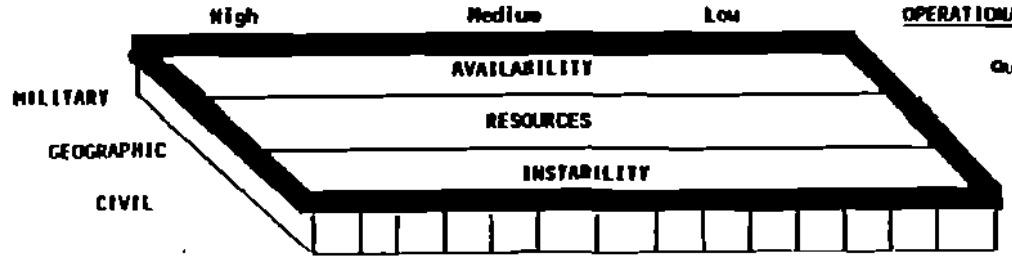


STRATEGIC LEVEL - Integrated Application of all national sources of power

Ability to sustain operations over time & space

Strategic geo-political location or source of materials

External relationships of strategic import

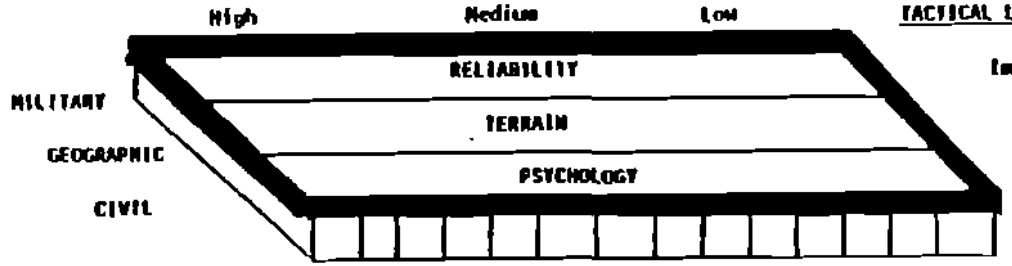


OPERATIONAL LEVEL - Selection of time, space, and nature of engagements

Quantities of military power available for commitment

Internal natural resources .ording self-sustainment

Internal precipitants & preconditions of volatility

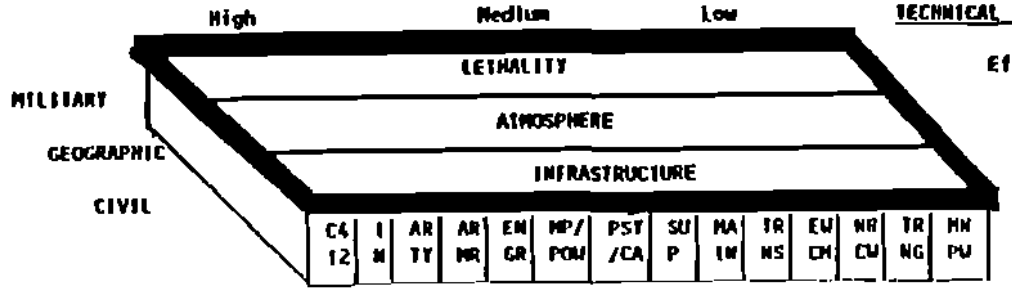


TACTICAL LEVEL - Application of finite power at fixed time & place

Impact of training & maintenance on existing capabilities

Internal geographic conditions affecting mobility

Internal group dynamics affecting cohesion & operations



TECHNICAL LEVEL - System-specific capabilities assessed in isolation

Effectiveness of specific capabilities assuming no constraints

Internal climate affecting system performance

Civilian structures enabling or blocking system use

MISSION AREA ANALYSIS SLICE - Vertical & Horizontal looks

Vertical: through each level of warfare

Horizontal: in relation to geographic & civil factors

EXPEDITIONARY ENVIRONMENT - TERMS OF REFERENCE

Level of Warfare

Strategic	Integrated application of all national sources of power
Operational	Selection of time, space, and nature of tactical engagements in order to attain strategic objectives - theater level
Tactical	Application of finite combat power at fixed time & place
Technical	System-specific capabilities independent of external conditions

Military Capability

Sustainability	Ability to bring to sustain military operations over time & space
Availability	Quantities of military power available for commitment
Reliability	Impact of training & maintenance on existing capabilities
Lethality	Effectiveness of specific capabilities assuming no constraints

Geographic Condition

Location	Strategic geo-political location or source of minerals
Resources	Internal natural resources affording self-sustainment
Terrain	Internal geographic conditions affecting mobility
Atmosphere	Internal atmospheric conditions affecting system performance

Civil Complexity

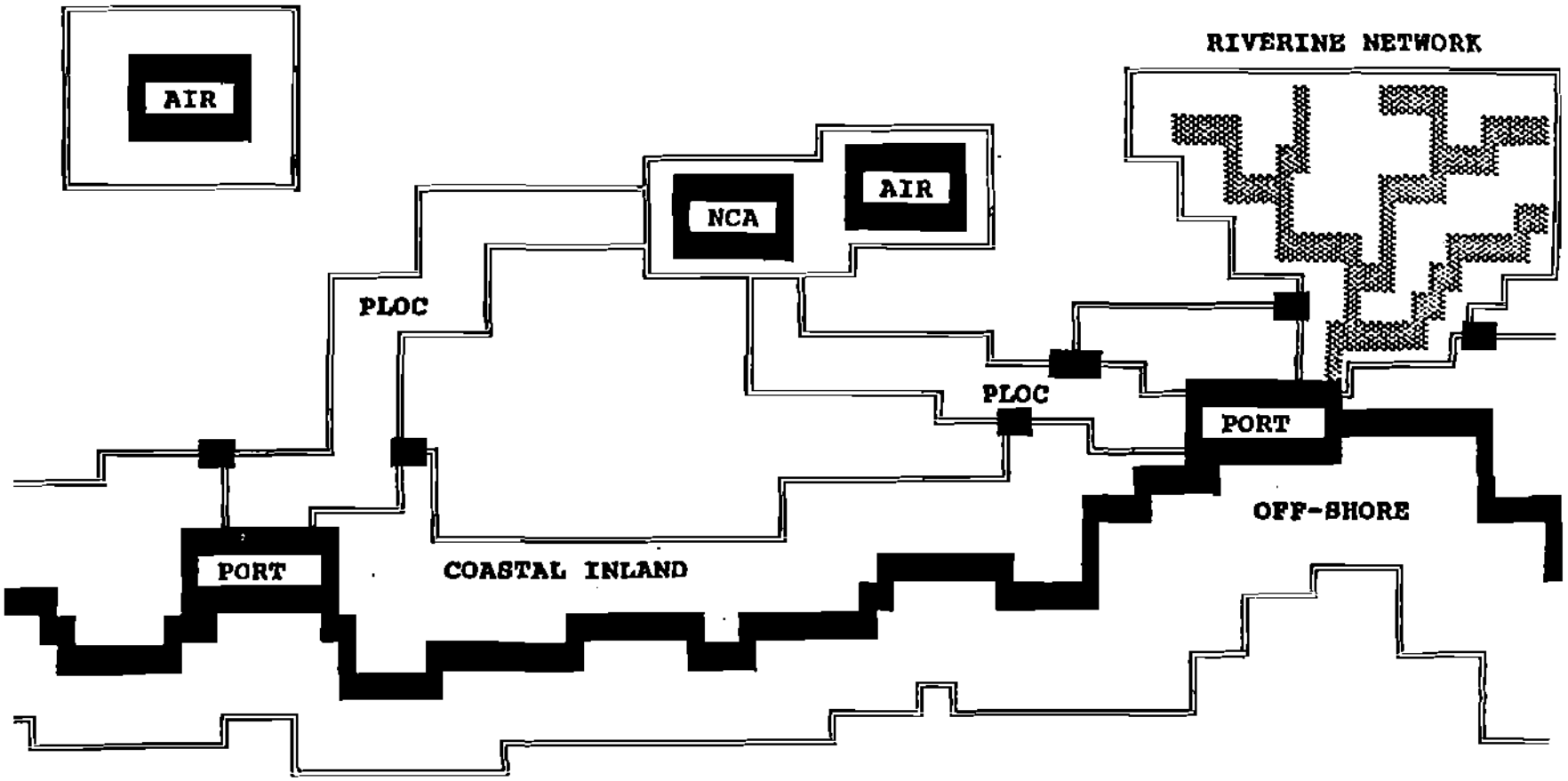
Allies	External relationships of strategic importance
Instability	Internal conditions affecting regime/insurgent effectiveness
Psychology	Internal group dynamics affecting national cohesion
Infrastructure	Internal structures affecting national capabilities

Areas of Operation

Off-Shore	From 25 NM off-shore to high-water mark
Inland Coast	From high-water mark to 50 K inland
PLOC	Primary Line of Communication from Port to NCA + 30 K each side
NCA	National Capital Area + nearest strategic airhead + 30 K around
Internal	Riverine networks, other concentrations of people, military, or key infrastructure nodes

ILLUSTRATION OF EXPEDITIONARY AREAS OF OPERATION

(Method of Delimiting Analysis Problem)



OFF-SHORE:	25 NM TO HIGH-WATER MARK
COASTAL INLAND:	HIGH-WATER MARK TO 50 K INLAND
PLOC:	PRIMARY LINE OF COMMUNICATION FROM PORT TO NCA + 30 K EACH SIDE
NCA:	NATIONAL CAPITAL AREA + NEAREST STRATEGIC AIR HEAD + 30 K ALL ROUND
INTERNAL:	RIVERINE NETWORKS, OTHER STRATEGIC AIR HEADS OR CONCENTRATIONS OF PEOPLE, MILITARY, OR KEY INFRASTRUCTURE NODES

EXPEDITIONARY ENVIRONMENT RESEARCH & ANALYSIS FRAMEWORK 1990
(Early Generalizations)

CONDITIONS & CAPABILITIES	HIGH	MEDIUM	LOW
MILITARY CAPABILITY	Fully integrated high-tech military infrastructure with mobile deep-strike cababilities incl atk air, arty, & SSM followed by mech combined arms force capable of sustained ops	Defined military infrastructure with emerging air-ground strategy. Capable of uncoordinated air & ground attacks, hasty & deliberate defenses, limited reinforcements, withdrawal/delay	Fragmented military infrastructure based on old or poorly defined technologies. Capable of hasty defense and delaying tactics.
OPERATIONAL GEOGRAPHY	Trails, dirt roads in highly forested mountain region over 9000 ft, snowing, temperature below freezing, visibility less than 1000 M	Constrained landing sites, single egress to single land roads in rolling hills w/ scattered trees, to small city. Airfield avail for tacops	Airfield suitable for strategic air transport, rural plain, 40 ft draft port with multiple cranes, piers, and electric power
CIVIL COMPLEXITY	Regional power with allies, fanatical religion, strong international media and propaganda capability, global intel organization, independent energy/food	Garrison state with grass roots support or fragemented unarmed opposition, major urbanization, widespread disease or famine, sufficient water, food, energy	Rural/urban opposition w/local base, limited nat'l intel capability, small elite w/o mass spt, urban/rural mix, no safehaven

NEXT STEPS IN THE DEVELOPMENT OF THE GENERIC FRAMEWORK

- USMC INTELLIGENCE CENTER MUST INITIALLY APPLY ROUGH FRAMEWORK WHICH NOW EXISTS TO A SINGLE COUNTRY TO DETERMINE:
  - -- AVAILABILITY & RELIABILITY OF INFORMATION
  - -- RELEVANCE OF CHOSEN CRITERIA
  - -- IDENTIFICATION OF ADDITIONAL OR ALTERNATIVE CRITERIA
- REFINE FRAMEWORK BASED ON COUNTRY-SPECIFIC ANALYSES.
- DO SUFFICIENT INTERATIONS TO ESTABLISH REPETITIVE PATTERNS AND VALID GENERALIZATIONS.
- RESULTS WILL ESTABLISH "ACCEPTABLE GENERALITIES" WHICH WILL DEFINE THE EXPEDITIONARY ENVIRONMENT MODEL WHILE ACCOMODATING REGIONAL DISTINCTIONS AND COUNTRY-UNIQUE CONDITIONS.

PROCESS FOR DELPHIC USE OF RESEARCH & ANALYSIS FRAMEWORK

FACTOR	HIGH	MEDIUM	LOW
ARTILLERY	SP or towed, with rockets & missiles, NBC, range 30K+	SP or towed, with some missiles, bio-chem, <30K range	Towed artillery with <30K range and/or mortars
MOUNTAINS	High steep slope range with heavy trees cover or low range w/o cover	Low mountain range with scattered trees	Small rolling hills with light scattered trees
OPPOSITION - ORGANIZED - POPULAR	International Opposition with Popular Sympathy	National Opposition with Grass Roots Spt	Rural or Urban Opposition with Only Local Base

- Discuss each factor & description
- Refine descriptions to distinguish between levels
- Categorize level of country for each factor
- Provide one or two bullets justifying each catagorization
- Identify an "observable" for each bullet
- Identify data base or data source for each observable
- Identify collection/processing/production gap if appropriate
- State whether factor is moving higher or lower
- Identify any other factors bearing on categorization

EXAMPLE

LIBYA: POLITICAL-LEGAL/Opposition

- Rated both high and low
- High because of Egypt and Chad
- Low because of Islamic fundamentalists but relative control
- Number of incidents or denunciations by Egypt & Chad can be plotted
- Public references to Islamic fundamentalists can be plotted
- Need automated scanning/extraction of open source print/voice media
- Need improved clandestine HUMINT reporting as well as emigre debriefing

MILITARY CAPABILITIES SHAPING THE EXPEDITIONARY ENVIRONMENT

Executive Summary

- Military capabilities shaping the expeditionary environment should be considered in each of five dimensions:

  -- Ground Overview
  -- C4I2
  -- Combat Support
  -- Combat Service Support
  -- Readiness & Other Factors
  -- Military Manning
  -- Aviation Overview (2)
  -- EW
  -- NBC

- The threat within each dimension can be related to the lethality, range, effectiveness, and sustainability of each capability. For this reason some of the capabilities (e.g. combat arms) will depend on the degree to which other capabilities (e.g. training) are present.

- Examples of a "high", "medium", and "low" environment:

  -- High: A fully integrated high-tech military infrastructure based on an air-ground combined arms strategy utilizing state-of-the-art technologies. Envision a highly mobile, deep-strike capability utilizing ground attack aircraft, long range artillery or SSM's deploying non-persistent CW agents followed by a mechanized combined arms ground force attack to quickly neutralize and destroy opposing forces.

  -- Medium: A defined military infrastructure with an emerging air-ground strategy utilizing current technologies but attempting high-tech systems integration. Envision an enemy capable of uncoordinated air and ground attacks, hasty and deliberate defenses, limited reinforcements, withdrawal and delaying tactics.

  -- Low: A fragmented military infrastructure with segregated military capabilities based on obsolete or ill-defined technologies. Envision an enemy capable of hasty defense and delaying tactics only.

OVERVIEW OF GROUND FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
INFANTRY	Mechanized, division-sized combined arms capable with ALP	Mobile trained Rgmts or Bns with some combined arms	Bn-sized forces with limited mobility & spt
ARTILLERY	SP or towed, with rockets & missiles, NBC, range 30K+	SP or towed, with some missiles, bio-chem, <30K range	Towed artillery with <30K range and/or mortars
ARMOR	T-72MI or T-80/64B equivalent with advanced armor (R/A)	M-60, T-62E/Mod 55 equivalent with 3rd gen. armor	M-48/T-54/IFV equivalents or less
C4I2	Integrated strategic & tactical C4I2 using full RF spectrum	Terrestial RF and landlines, limited encryption & intel	Single-channel radio, limited encryption/intel
SUPPORT	Full-range engineers, complete military police/PSYOP-CA units,	Limited engineers, some military police and PSYOP-CA	Countermobility engineering, no dedicated MP/PSYOP
SERVICE SUPPORT	Able to move, supply, & maintain a division beyond its borders	Can move, supply, & maintain rgmts & bns within borders	Some resupply & limited maint. capability
LEADERSHIP, TRAINING, & READINESS	Corps+ leaders, troops experienced, well-trained, fully ready	Div level leaders, some troop training partially ready	Regt lev leaders, no or infrequent training, not rdy
MILITARY MANNING	Foreign advisors, full reserve, PM/elite units	Foreign contractors, partial reserves, some PM/elite units	Constabulary or pro forma reserve w/o SOF

C4I2 FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
COMMAND & CONTROL & COMMUNICATIONS	Integrated automated C4 btw NCA & ground/ air hqs; national/alt. CP, full RF & SATCOM, encryption all levels	Limited C4 automation w/reliance on land-lines & terrestial RF w/strategic encryp-tion, tac. ops codes	No integration or automation of C4, use single channel radios (e.g. HF), offline encry/clear
COMPUTING	Mainframe & high performance distributed processing, ADP tools	Limited use of stand alone workstations, basic PC packages	Manual data process-ing and report production
INTELLIGENCE & INTEROPERABILITY	Multi-discipline collection capability w/all-source analysis at national & tactical levels	Strategic intel from allies, some SIGINT, IMINT, HUMINT collec-tion, limited inte-gration	Limited strategic intel from allies, national HUMINT, tactical SIGINT, no/ limited IMINT

COMBAT SUPPORT FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
ANTI-TANK	PGM, atk helo, self-propelled AT, arty/air deliverable mines	SP AT, RR, arty/air deliverable mines	Crew served or shoulder launched AT weapons
ENGINEERS	Heavy equipment, can do mobility/countermobil., survivability, gen eng.	Few heavy assets, can do minefields & obstacles, demolit.	Manual minefield & obstacle construc. & clearing
MILITARY POLICE	Dedicated organized MP units able to handle mass refugee/POW groups	Limited organized MP units able to handle routine matters	No dedicated MP units; law enforcement by infantry
PSYOP & CIVIL AFFAIRS	Dedicated organized PSYOP/CA units with organic equipment	Limited organized PSYOP/CA specialists detailed to infantry	No organized PSYOP or CA capabilities

COMBAT SERVICE SUPPORT FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
SUPPLY	Self-sufficient, can sustain combat ops for over 6 months, to include external ops	Self-sustaining up to 6 months, rely on allies for supplies	Self-sustaining for less than 30 days, rely on allies/raids
MAINTENANCE	Unit, intermediate, & depot-level	Unit & intermediate (DS & GS units), external depot spt	Unit level only. Dependent on external manning & facilities
TRANSPORTATION	Modern assets, fast response, not reliant on commercial assets	Good rail & roads, limited air, partial use of commercial	Primitive or limited transport, slow response, commercial

READINESS & OTHER FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
LEADERSHIP	Combat experience, Corps-level staffs, professional schools	Ops/exercises done, div-level staffs, few foreign advisors	Regiment-level staffs, rely on foreign advisors
TRAINING	Training at division level or higher, 3-5 days per month	Training at rgmt or lower level, 1-3 days per month	Infrequent training at/below 1 day per month
READINESS	All equipment receives preventive maintenance from trained personnel	Most equipment in ready status, is repaired as needed	Generally poor maintenance, most equipment deficient

MILITARY MANNING FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
FOREIGN ADVISORS	In-country, providing R&D or intel support, of manning equipment	Intel & operational advisory role, MTTs, liaison/oversight	Temporary travel in-country for MTT or supply purposes
CONTRACTORS	Fully responsible for manning and/or maint. of critical systems	Responsible for maintenance & testing of key systems	Temporary travel in-country for installation/repair
RESERVES	Organized trained reserve able to fill range of combat needs	Organized coastal, constabulary, or specialty units	No organized units or regular training
PM/SOF/ELITE	Trained & specially equipped units with unique status	Organized units with special roles and loyalties	No organized PM, SOF, or elite units

OVERVIEW OF AVIATION FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
AIR SURVEILLANCE WEAPONS SUPPORT	Full integrated air defense net, with digital automation	2nd/3rd generation Soviet/Western IAD	Limited IAD netting with landline links
FIGHTER AIRCRAFT (FIXED & VSTOL)	4th generation Soviet / Western full LD/SD capability	3rd generation Soviet /Western limited LD/SD cap	Early jets with limited scramble, no sustained CAP
STRIKE AIRCRAFT (FIXED & VSTOL)	All-weather medium & long-range, NBC capable	Marginal all-weather medium/long range without NBC	Day only, VFR delivery
HELICOPTERS (BOTH ATTACK & TRANSPORT)	4th gen. attack & transport	3rd gen. attack & transport, limited assets	No military assets, limited commercial assets
SURFACE TO AIR MISSILES	4th Gen Soviet/Western Strategic / Tactical Improved IR	3rd Gen Soviet/West Strategic/Tactical	Hand Held Tactical IR Only
ANTI-AIRCRAFT ARTILLERY	4th Gen Soviet/West Radar associated Mobile	3rd Gen Soviet/West limited radar restricted mobile	Small arms Optical sighting Manual operations
AIR TO AIR MISSILES	4th Gen Soviet/West Dual Mode True All-Aspect	3rd Gen Soviet/West Limited All-Aspect	Early IR/SAR Rear Quarter

OVERVIEW OF AVIATION FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
RECONNAISSANCE	Long-range dedicated platform with real-time links	Medium/long-range multi-role platform w/NRT links	Low mission priority with no NRT links
AIRBORNE EARLY WARNING/CONTROLLER (AEW)	Long-range/extended loiter time, multi-mission, digital links	Single mission ops w/limited coverage, voice links	No capability
TACTICAL ELECTRONIC WARFARE (TACEW)	Dedicated platform ESM/ECM, both fixed wing & rotor	Self-protection only or helo platforms only for ECM	No capability
TRAINING & READINESS	Simulators, live fire & free play; sustain support all levels	Limited training & live fire; foreign support at depot	Less than 10 hours flight/month; rely on foreign support

NBC FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
NUCLEAR	Stockpiled nuclear weapons or proven capability to build	Advanced R&D effort, component acquisition, prototypes	No nuclear capability or capacity to develop
CHEMICAL	Indigenous production, full spectrum, prior utilization	Stockpiles of major agent, indigenous or foreign production	Foreign procurement, non-persistent, limited stocks
BIOLOGICAL	Indigenous production, full spectrum of toxic & infectuous agents	Microbiology R&D, some infectuous agents in stock	Foreign procurement would be needed, no agents in stock
DELIVERY	Full range of air & missile/artillery delivery systems	Artillery & mortar delivery, some air (rotary) delivery	No tested delivery system

EW FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH	MEDIUM	LOW
EW SUPPORT MEASURES (ESM)	Automated netted COMINT & ELINT w/DF, capable against full spectrum & w/full proc/rpt	Manual collection & DF against some comms & non-comms signals	Limited or no collection
ELECTRONIC COUNTER MEASURES (ECM)	Mobile programmable jamming/deception, full spectrum, active & passive, varied tech.	Capable of jamming & deception within specific frequency ranges	Limited or no jamming/deception capability (can do ICD obvious jamming)
ELECTRONIC COUNTER-COUNTER MEASURES (ECCM)	Fully developed and exercised system of preventive & remedial measures/equipment	Some doctrine & equipment	Non-existent system or limited to operator training

OPERATIONAL GEOGRAPHY SHAPING THE EXPEDITIONARY ENVIRONMENT

Executive Summary

- Operational geography shaping the expeditionary environment should be considered in each of six dimensions:

  - -- Basic Topography
  - -- Assault Hydrography
  - -- Operational Infrastructure
  - -- Ground Assault Conditions
  - -- Aeronautical Conditions
  - -- Basic Weather

- The threat within each dimension can be related to the degree to which topographical and/or weather conditions constrain operational mobility, firepower, and/or sustainability.

- Examples of a "high", "medium", and "low" environment for these factors is offered below:

  - -- High: Trails, dirt roads in a highly forested mountain region over 9000 ft, snowing, temperature at 0, visibility less than 1000 meters, with objective too far inland to permit sea-launched assault and naval gunfire support.

  - -- Medium: Single amphibious landing vehicle sites with egress to single lane hard surface roads and rail roads, small rolling hills with moderate scattered trees, to a small city. Airfield suitable for sustained tactical air transport operations.

  - -- Low: Airfield suitable for sustained strategic air transport. Rural plain, 40 ft draft port facility that has multiple cranes, piers and electric power.

OPERATIONAL GEOGRAPHY SHAPING THE EXPEDITIONARY ENVIRONMENT

BASIC TOPOGRAPHY	GROUND ASSAULT	ASSAULT HYDROGRAPHY	AERONAUTICAL CONDITIONS	OPERATIONAL INFRASTRUCTURE	BASIC WEATHER
Surface Configuration	Cover	Beaches	Ops Elevation	Port Access	Temperat.
Surface Vegetation	Concealment	NGF (5 fathom line)	Aerial Visibility	Port Utility	Windspeed
Surface Materials	Inter-Visibility	Surf Conditions	Aerial Ceiling	Air Terminals	Precipit.
Surface Hydrology	Landing Zones	Approach Conditions		Road/Rail Net	Humidity
Man-made Features	Drop Zones	Riverine Network		Bridges	Light Data

BASIC TOPOGRAPHY FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
SURFACE CONFIGURATION	High steep slopes of >40%, ranges with ravines & embankments	Low ranges with small ditches and scattered outcrops	Small rolling hills with valeys and flat areas
SURFACE VEGETATION	Double & triple canopy with heavy dense trees and dense undergrowth	Single canopy with mix of vegetation and open bare ground	Shrubs & grasses on flat plains including cactus or eleph. gr.
SURFACE MATERIALS	Wet clay, silt, large gravel or drifing loose sand, sebkhas & wadis	Moist sand, small gravel or loose unsettled sand	Dry silt, clay, small gravel or flat hard plain w/o sebkhas
SURFACE HYDROLOGY	Lakes, swamps, rivers, and/or glaciers; boats required for crossings	Streams, canals, small rivers; fording equipment needed	Seasonal streams, creeks, no major water obstacles
MANMADE FEATURES	Urban areas, major oil fields, major bridges or tunnels/pipelines	Sururban or village areas, minor power facilities, bridges	Predominantly rural, minor bridges and/or tunnels, few obstacl.

GROUND ASSAULT CONDITIONS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
COVER	Flat plains and wide open areas	Moderate scattered trees on rolling hills	Densely wooded areas within low mountain range
CONCEALMENT	75% or more canopy closure	40-74% canopy closure	0-39% canopy closure
INTER-VISIBILITY	Average line of sight distance in AO is less than 1000 meters	Average line of sight in AO is 1000 to 3000 meters	Average line of sight in AO is over 3000 meters
LANDING ZONES	Slope of available LZ/HLZ greater than five degrees	Slope of available LZ/HLZ 3-5 degrees	Slope of available LZ/HLZ <3 degrees
DROP ZONES	Few or very small clearings with no ground access/exits	Small playing field size clearings with limited exits	Large open fields with many exits & access to LOCs

ASSAULT HYDROGRAPHY CONDITIONS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
BEACHES	Limited or not avail, with restricted or channeled egress	Sufficient to allow single LCAC or few LAV, multiple egress	Multiple sites for full LAV waves, multiple egress
NAVAL GUN FIRE	5 fathom line more than 16K meters offshore	5 fathom line is >8K <16K meters offshore	5 fathom line is less than 8K meters offshore
SURF CONDITIONS	>3.5 ft. swells, >4.0 ft. surf, underlying current >3 kts	2-3 ft. swells, 2-4 ft. surf, under-current 2-3 kts	0-1 ft. swells, 0-1 ft. surf, under-current < 2 kts.
APPROACH CONDITIONS	>15 ft. tidal range, or slope <1:5 and/or silty/muddy bottom	>5' <15' tidal range and/or slope >1:5 <1:10, sand	<5' tidal range, or slope >1:5 and/ or hard bottom
RIVERINE NETWORK	Major river complex with tributaries >6' deep and ocean access	Defined network w/ streams >3' <6' deep, mostly inland	Seasonal streams <3' deep

AERONAUTICAL CONDITIONS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
ELEVATION	Over 9000 ft	4000-9000 ft	Less than 4000 ft
AERIAL VISIBILITY	Less than 2 NM	>2 <5 NM	Over 5 NM
AERIAL CEILING	Less than 1000 ft	3-5K ft +/-	Over 10K ft +/-

OPERATIONAL INFRASTRUCTURE CONDITIONS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
PORT ACCESS	Less than 34' draft (tactical assault)	35-40' draft (gray shipping)	Over 40' draft (black shipping)
PORT UTILITY	No cranes or piers	At least one crane or pier per port	Multiple cranes & piers, electric power available
AIR TERMINALS	Not good for tactical transport ops, no ground control	Suitable for fully loaded tactical transport ops	Suitable for strategic airlift
AIRHEAD UTILITY	One or no ramps	Two to five ramps, some fuel storage and bunker areas	Five or more ramps suitable for C-5, good fuel/ammo site
ROAD/RAIL NETWORK	Trails, dirt roads, very limited or no railroad	Hard surface single lane roads, single track RR	Major highways, extensive RR
BRIDGES	Many primitive or old bridges of low or unknown load bearing	Mix of steel/cement bridges w/load bearing <20 tons	Modern steel & cement bridges with >20 ton capability

BASIC WEATHER FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITIONS	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
TEMPERATURE	>80 <32 F	32-50 or 65-80 F	51-64 F
WIND SPEED	>30 knots	13-30 knots	<13 knots
PRECIPITATION	1"/hour or 2"/12 hrs; 2" snow/hour or 6" snow/12 hrs	.5-1"/hour or 1"/ 12 hrs; 1-2" snow/ hr or 3-6"/12 hrs	0-.5"/hour or .5"/ 12 hrs; 0-1" snow/hr 0-3"/12 hrs
HUMIDITY	60-100%	31-59%	12-30%
LIGHT DATA	4-6 hrs daylight	6-10 hrs daylight	>10 hrs daylight

CIVIL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

Executive Summary

- Civil factors shaping the expeditionary environment should be considered in each of five dimensions:

  -- Political
  -- Psychological
  -- Economic
  -- Infrastructure
  -- Natural Resources

- The complexity of the factors, increasing the difficulty facing the tactical commander, can be related to the area of influence of each factor: International = HIGH, National = Medium, Local/Urban = LOW.

- The relevance of the factors to expeditionary operations can be established by determining whether the factor must be considered in relation to short-term missions under 7 days (e.g. a NEO), mid-term missions over 7 but under 30 days (e.g. humanitarian assistance) and longer-term missions over 30 days (e.g. internal security).

- Examples of a "high", "medium", and "low" environment for these factors is offered below:

  -- High: Regional power with allies, fanatical religion, strong international media and propaganda capability, global intelligence organization, and independent energy & food supplies.

  -- Medium: Garrison state with grass roots support or fragmented unarmed opposition, major urbanization, widespread disease or famine, sufficient water, food, energy.

  -- Low: Rural/urban opposition with local base, limited national intelligence capability, small elite without mass support, balanced mix of urban & rural populations, secure borders offering no safehaven.

CIVIL FACTORS - TERMS OF REFERENCE

Civil Dimensions

Political.....	**Focus on political relationships between groups and individuals, including external allies and internal opposition groups; and on basic capabilities and legal environment maintaining government control of political process.**
Psychological.....	**Focus on the ideological and cultural nature of the population and the degree to which individual behavior undermines or supports the nation-state. Assesses role of religion & language as divisive or cohesive factors, group divisions & customs, national myths, and other issues associated with individual education & rebellion.**
Economic.....	**Focus on ability of state to fulfill its functions and allocate resources, with emphasis on the stability of the consumer market, the role of the military as a dominant group, the general stregth of the economy, and the degree to which capital is available and research & development sponsored for future economic power.**
Infrastructure.....	**Focus on the technical and demographic resources of the nation-state including basic issues regarding population distribution, disease, communications, public works, public transportation, and electronic computing resources.**
Natural Resources.....	**Focus on natural resources including water, food, energy, and mineral wealth, as well as related issues which contribute to conflicts, such as contiguous hostile areas, land tenure practices, and production base constraints.**

CIVIL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

POLITICAL	PSYCHOLOGICAL	ECONOMIC	INFRASTRUCTURE	NATURAL RESOURCES
Allies	Religion & Language	Strikes & Riots	Key Facilities & No Fire Areas	Contiguous Hostile Area
Opposition	Group Divisions, Customs/Taboos	Black Market, Corruption, & Mil/Pol Crime	Urbanization & Population Issues	Water Supply
Intelligence	Myth/Identity, Media Themes, & View of USA	Unemployment & Inflation	Disease & Public Health Resources	Food Supply
Government	Education	Basic Civilian Staples/Supply	Public Voice/Print Media & Telecommunications	Energy Supply
Human Rights	Intellectuals	Garrison State	Public Works (Power & Water)	Strategic Minerals & Raw Materials
Public Form, Franchise, & Opinion	Censorship	Foreign Capital & Capital Flight	Public Transportation Assets	Production Base
Legal Codes	Violence	R&D Program	Electronic Computing & Storage	Land Tenure

POLITICAL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
ALLIES	Major hostile power or several regional powers	Major regional power or scattered minor supporters	No major ally in region nor Sov/PRC interest
OPPOSITION - ORGANIZED - POPULAR	International Opposition with Popular Sympathy	National Opposition with Grass Roots Spt	Rural or Urban Opposition with Only Local Base
INTELLIGENCE - STRUCTURED - PROFESSIONAL	International Intelligence with Global Assets	National Intelligence with Rural/Urban Assets	Limited Intelligence with Capital City Base
GOVERNMENT - STRUCTURED - RESPONSIVE	Fully capable sovereign government	Nationally capable government with limited int'l role	Parochial or unformed state w/limited powers
HUMAN RIGHTS	Violent repression w/o oversight of police &/or military	Limited repression w/some political oversight/pressure	Firm commitment to human rights, broad public pressure
PUBLIC FRANCHISE & OPINION - LEGITIMACY	Unrestricted citizen base with protected rights	Partial franchise with popular majority	Very restricted elite without majority support
LEGAL CODES - EXISTENCE - EFFECTIVE	Religious or primitive codes or patron power	Legal or religious codes partially or arbitrarity used	Established legal system with working courts

* Includes gender mix and stratification of population by class, race, [illegible], or religion.

PSYCHOLOGICAL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
RELIGION & LANGUAGE	Intense national religion or varied opposed religions; "hard" language	Major religion or mass movement with active role; Western language	Western or varied religions of no real influence; Eng/Frnch/Spnsh
GROUP DIVISIONS, CUSTOMS, AND TABOOS	Major fragmentation of society with conflicting mores	Major minority element not fully integrated	No significant socio-economic fragmentation
MYTH/IDENTITY, MEDIA THEMES, & VIEW OF USA	Cohesive national myth system, with xenophobic nature	Strong national identity and sense of history	Limited or fragmented myth system/identity
EDUCATION - PUBLIC - QUALITY	No public schools and a primitive illiterate public	Partial public education, literate urban population	Public education and literate population
INTELLECTUALS - EXISTENCE - COMMITMENT	Strong intellectual community firmly committed to state	Isolated community of intellectuals including exiles	Fragmented or unformed community of intellectuals
CENSORSHIP - SCOPE - DEGREE	Total censorship of all media and all topics	Censorship of political topics or select groups	Limited or no censorship
VIOLENCE - PRE-DISPOSED - EXTENT	Cultural pre-disposition and history of violence	Elite history of unchecked violence	No significant pre-disposition or history

ECONOMIC FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
REBELLION (RIOTS, STRIKES, DEMONSTRATIONS)	Frequent and sustained public riots & strikes	Occasional violent rebellion or many demonstrations	Limited and generally peaceful gatherings
BLACK MARKET & CORRUPTION & MIL/POLICE CRIME	Thoroughly corrupt society, bribes for basic transactions	Limited elite corruption, some bribes necesary	Limited elite corruption, no major monopolies
INFLATION & UNEMPLOYMENT - RATE	Rapid rate of inflation and high unemployment	Fluctuating rates of inflation and unemployment	Steady or limited inflation and unemployment
BASIC CIVILIAN STAPLES/SUPPLY - TYPE/EXTENT	Major shortages of basic staples and household items	Shortages of convenience items & minor luxuries	Full range of staples and consumer goods
GARRISON STATE - MONOPOLY - ISOLATED	Dictatorship or entrenched military controlling economy	"Benevolent" or professional military elite	Militia or home guard with limited role
FOREIGN CAPITAL & CAPITAL FLIGHT	Most elite funds withdrawn and no foreign credit	Steady capital flight, high rates of loan interest	Modest capital flight, steady foreign loans
R&D PROGRAM - FUNDED - QUALITY	National R&D program with high-tech goals	Private industry R&D in some areas	No significant R&D program

INFRASTRUCTURE FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
KEY FACILITIES & NO FIRE AREAS	Regionally important facilities, many no fire areas	Nationally vital facilities, some no fire areas	No major facilities requiring control, minor no fire areas
POPULATION ISSUES - URBANIZATION - DISPLACEMENT	Excessive and unsupportable urbanization	Major urbanization with limited or sporadic services	Balanced mix of urban & rural populations
DISEASE & HEALTH - SCOPE - ADDRESSED	Uncontrolled famine and/or disease such as AIDS/schistosom.	Major disease such as schistosomaisis and public program	No major disease or famine and/or good public plan
PUBLIC COMMS - VOICE/PRINT MEDIA - TELECOMMUNICATION	Int'l media & propaganda, int'l telecommunications	National media and propaganda capability	Primitive media & limited nat'l telecommunications
PUBLIC WORKS - POWER - WATER	No established public works system	Partial public works and/or frequent breakdown	Established and functional public works system
PUBLIC TRANSPORTATION ASSETS	Major transport fleets with int'l infrastructure	Substantial ground transport fleet w/ national network	Some urban assets w/generally poor roads or rails
ELECTRONIC COMPUTING & STORAGE	National network of electronic data entry & management assets	Strong program of data management in primary industry	Limited or old data storage and management tools

NATURAL RESOURCE FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CONDITION	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
EXTERNAL THREAT - CONTIGUOUS - MAJOR POWER	Major hostile power on border	Minor or neutral power on border allowing safehaven	Secure borders offering no safehaven
WATER SUPPLY - LOCAL - RELIABLE	Importer of water or scarce water resources	Sufficient natural water for basic needs	Major rivers and lakes with good water works
FOOD SUPPLY - LOCAL - RELIABLE	Importer of basic foods	Nationally self-sufficient in basic foods	International supplier of major edible commodity
ENERGY SUPPLY - LOCAL - RELIABLE	International supplier of oil or electricity	National reserves of energy, partial exploitation	Importer of oil and/or electric power, coal
STRATEGIC MINERALS & RAW MATERIALS	International supplier of major minerals/materials	National reserves of basic minerals and materials	Importer of basic minerals and materials
PRODUCTION BASE - SINGLE/MULTIPLE - EXPLOITED	Over-reliance on single sector and/or weak market	Strong single sector with good distribution	Balanced mix of production (both indus. & agri.)
LAND TENURE - DISTRIBUTED - EFFECTIVE	Well distributed and exploited land holdings	Limited land tenure, strong share-cropping	Restrictive land tenure, serf-like labor conditions

"SO WHAT" TEST FOR CIVIL FACTORS

NOTE: Unlike military conditions and operational geography, the relevance of civil factors to normal MAGTF planning & programming activities may not be as apparent. Although the Small Wars Manual and other doctrinal publication recognize the importance of psychological and civil affairs, and the are clearly defined intelligence requirements associated with these functions as well as engineering, motor transport, and so on, the above matrix sought to bring together the various "civil" factors as a means of integrating them in the intelligence estimates process and highlighting the co-equal status of civil factors when planning for stability operations and limited objective operations.

Political

Allies	**Potential for intervention and/or mobilization of regional or international opinion**
Opposition	**Potential of existing groups (both armed and unarmed) for assisting or opposing MARFOR**

Intelligence	**Potential of intelligence & security services for assisting or opposing MARFOR operations, both internally and through covert actions & propaganda activities outside the AO (including against domestic U.S. public)**
Government	**Potential for assisting or opposing MARFOR**

Human Rights	**Establishes degree to which individuals have been repressed, and possible need for remedial programs; includes degree to which entrepreneurship present & successful**
Franchise	**Insights into nature of public's political personality, degree to which public opinion can aid or hamper MARFOR and/or government**
Legal Codes	**Foundation of internal order**

Psychological

Religion & Language	**Degree of difficulty for MARFOR intel, PAO, and engineers; includes religious codes and language conventions which MARFOR must understand**
Group Divisions, Customs/Taboos	**Degree to which certain groups must be monitored and MARFOR behavior adjusted**
Myth/Identity, Media Themes, & View of USA	**Provides MARFOR with estimate of cohesiveness of population, understanding of popular propaganda themes, and attitudes toward USA**
Education	**Establishes degree of popular literacy in relation to MARFOR public information program and public understanding of issues**
Intellectuals	**Establishes location & nature of key leaders of public opinion and degree to which they might oppose/support MARFOR ops**
Censorship	**Establishes degree to which public has been misinformed, and degree to which MARFOR must undertake remedial public information program**
Violence	**Establishes degree to which local population is culturally pre-disposed to violence, and alerts MARFOR to potential volatility**

Economic

Rebellion	Degree to which population supports insurgents and/or might impact MARFOR ops
Black Market, Corruption, & Mil/Pol Crime	Orients MARFOR to local "norms" (including need for MARFOR discretionary funds) as well as general dislocation of economy and degree to which local forces are regarded as "predators"
Inflation & Unemployment	Degree to which economic dislocation exists that may interfere with long-term MARFOR ops
Basic Civilian Staples/Supply	Degree to which civilians lack staples for diet or consumer goods which MARFOR must provide, or which MARFOR can draw upon in lieu of external resupply
Garrison State	Degree to which AO is militarized
Foreign Capital & Capital Flight	Presence or absence of foreign equities and/or flight of internal capital may complicate conditions for MARFOR
R&D Program	Identifies degree to which military R&D might threaten MARFOR, and general health of local R&D effort as it supports prosperity

Infrastructure

Key Facilities & No Fire Areas	**Identifies key facilities requiring MARFOR protection and possibly operation, and key sites (archives, monuments, etcetera) that constrain MARFOR ops**
Population Issues	**Establishes concentrations of people that MARFOR must deal with, and potential for displaced persons, refugees, and groups requiring MARFOR control or support**

Disease & Public Health Resources	**Identifies major diseases dangerous to individual Marines, degree to which local health resources are present or absent, extent to which MARFOR must provide medical reinforcements**
Public Comms (Voice/Print Media & Telecomms)	**Identifies degree to which existing local media outlets can be mobilized to meet MARFOR public information requirements; also availability of commercial telecommunications to be controlled, monitored, or exploited**

Public Works	**Degree to which public utilities (power & water) can be relied upon or must be managed by MARFOR engineers; identification of key nodes to be controlled or protected**
Public Transport	**Degree to which civilian transportation assets can be used to support or oppose mid-term MARFOR stability ops (actual infrastructure covered in Operational Geography)**

Natural Resources

Contiguous Hostile Areas	Establishes whether or not safehaven areas are available for opposing forces, and whether direct overland logistics resupply is possible. Identifies expanded AO.
Water Supply	Identifies degree to which water supply might constrain MARFOR as well as local elements, and whether engineer support will be needed to assure water for MARFOR and/or civilians
Food Supply	Identifies degree to which food supply might constrain local elements, and whether engineer spport and imported staples will be required for civilians
Energy Supply	Identifies degree to which energy supply might constrain MARFOR as well as local elements, and whether engineer support will be needed to assure energy for MARFOR and/or civilians
Strategic Minerals & Raw Materials	Identifies presence or absence of minerals & & raw materials critical to production of war supplies as well as national economy
Production Base	Identifies income-producing areas or lack of alternatives which may constrain long-term stability & undermine internal security
Land Tenure	Orients MARFOR regarding existing land distribution/exploitation practices which may stimulate long-term hostility in rural area and/or require civilian assistance

INSURGENCY FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

Executive Summary

- Insurgency factors shaping the expeditionary environment all fall within existing factors under the military and civilian elements of the framework for expeditionary analysis. However, in recognition of their importance, and the efforts of the Army-Air Force Center for Low Intensity Conflict, this section builds on the results of the "Indicators Templating" Study, and presents a tailored framework for drawing high-level generalizations about insurgency factors.

- The five matrices extracted from the Study and then refined or expanded include:

  -- Insurgent Military Capabilities
  -- Insurgent Civil Factors
  -- Insurgent Event Data
  -- Host Country Military Capabilities
  -- Host Country Civil Factors

- Examples of a "high", "medium", and "low" environment for these factors is offered below:

  -- High:

  -- Medium:

  -- Low:

INSURGENCY FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

INSURGENT MILITARY CAPABILITIES	HOST COUNTRY MILITARY CAPABILITIES	INSURGENT CIVIL FACTORS	HOST COUNTRY CIVIL FACTORS	INSURGENT EVENT DATA
Commitment to Terrorism	Leadership	Overt Political Mobilization	Police Operations	Bombings
Capability for Terrorism	Military Intelligence	Covert Political Mobilization	Civilian Intelligence Operations	Kidnapping & Assassination
Safe-Haven or Controlled Territory	Troop Discipline & Behavior	Propaganda	Civil-Military Relations	Civil Disobedience
Steady Flow of Weapons & Trained G's	Use of Popular Militia	Civil Acquisition	Unified Management	Strikes & Riots
Established Military Organization	Force Structure	Funding Mechanism	Psychological Operations	International Media Events
Acquisition of Crew-Served Wpns & Vehicles	Strategy	Indoctrination Mechanism	Political Environment	Conventional Military Ops
Established C4I2 Networks	Tactics	Admin & Logs Mechanisms	Administrative & Legal Reforms	International Legal Activity

INSURGENT MILITARY CAPABILITIES SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
COMMITMENT TO TERRORISM	Leaders & followers commited to global campaign of terrorism	National program of terrorism against selected targets	Only occasional resort to terrorism as method of ops
CAPABILITY FOR TERRORISM	International support network and freedom of movement	Limited ability to conduct terrorist acts away from home	Limited to local acts of terrorism
SAFE-HAVEN OR CONTROLLED TERRITORY	Multiple controlled areas and/or adjacent countries offering S/H	Mixed rural-urban controlled area &/or single S/H country	Small rural area or no regular control, free night passage
STEADY FLOW OF WEAPONS & TRAINED G'S	Regular deliveries of arms, established training areas	Occasional shipment of arms, foreign & informal training	Sporadic & limited arms deliveries, no regular training
ESTABLISHED MILITARY ORGANIZATION	National military command & regional command structure	Informal coordination among separate regional mil. ldrs.	Popular leaders of small bands or cells with no staff
ACQUISITION OF CREW-SERVED WPNS & VEHICLES	Regular pipeline for introduction of larger wpns & mil. vehicles	Shoulder-held SAMs & heavy MG, Mortars, use commercial veh.	Limited to small arms, grenades; walk & use animals
ESTABLISHED C4I2 NETWORKS	National & regional radio & informant networks w/security	Some mobile radio equipment, crude intelligence nets	Limited to personal & commercial comms, personal obsvtn.

HOST COUNTRY MILITARY CAPABILITIES SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
LEADERSHIP	Opportunistic & corrupt leaders w/o scrupples	Trained officers, no/untrained NCOS, conscripted troops	Highly professional military sensitive to popular concerns
MILITARY INTELLIGENCE	Only informal sources & no standard methods for intel processing	Provincial networks under informal control	Organized networks & data handling techniques
TROOP DISCIPLINE & BEHAVIOR	Conscripted troops of different ethnic or regional origin	Untrained troops inclined to violent repression	Trained disciplined troops sensitive to popular concerns
USE OF POPULAR MILITIA	Marginal militia not integrated into military structure	Organized militia independent of regular military	Organized militia fully integrated into regular struc.
FORCE STRUCTURE	Paramilitary force without counter-insurgency training	Military ground force, limited air, some CI training	Complete combined arms force including SO/CI forces
STRATEGY	Top-level refusal to adopt national civil-military strategy	Limited commitment to partial strategy for CI operations	National political & military commitment to CI strategy
TACTICS	Troop leaders refuse to adopt appropriate tactics (e.g. night)	Some troop leaders experiment with & adopt CI tactics	Full understanding & commitment to CI tactics in military

INSURGENT CIVIL FACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
OVERT POLITICAL MOBILIZATION	Full range of front organizations & ties, int'l representation	One or more front organizations, some political support	Exist as faction within established pol/labor group
COVERT POLITICAL MOBILIZATION	International covert network for channeling funds & information	National covert network, limited int'l connections	Covert cells in select rural/urban areas
PROPAGANDA	High-profile int'l network able to feed video/print material	Organized media strategy & manning, some production	Staged local events with verbal briefs for media
CIVIL ACQUISITION	Full capability to acquire & distribute equip, clothes, food	One-time or ad hoc procurement of items in bulk	Occasional thefts to obtain specific needed items
FUNDING MECHANISM	Int'l financial net with regular flow of funds from supporters	National protection racket or other stable funding	Occasional thefts or reliance on local contributions
INDOCTRINATION MECHANISM	Established ideology & political/economic program w/training	Populist program w/simplistic goals but no training	No established program or indoctrination
ADMIN & LOGS MECHANISMS	Organized files & property control, accountability	Personal files & oversight, some coordination	Limited or no record keeping & accountability

HOST COUNTRY CI[illegible] ACTORS SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
POLICE OPERATIONS	Personal or para-military police w/o public peace role	Organized police w/limited ability to ensure peace	Integated national police force fully committed to peace
CIVILIAN INTELLIGENCE OPERATIONS	Opportunistic, corrupt, or limited civilian intelligence org.	Urban/rural-based civilian intel with personal networks	National integrated civilian intel with sources & methods
CIVIL-MILITARY RELATIONS	Completely autonomous military independent of civilian control	Working relations btw civil authority & military forces	Military fully subordinate & supportive of civil.
UNIFIED MANAGEMENT	Autonomous or disorganized agencies unable to coord.	Organized military w/police cooperation in some areas	Fully integrated civil-military ops across host country
PSYCHOLOGICAL OPERATIONS	Government unwilling to sponsor PSYOP or lacking in credibility	Limited topic or duration PSYOP if external assist.	Full PSYOP program with quality effort & good media access
POLITICAL ENVIRONMENT	Government does not appeal to populace, lacks legitimacy	Government neutral, military or security forces unpopular	Government and its forces appeal to populace
ADMINISTRATIVE & LEGAL REFORMS	Civil or military refusal to compromise or sponsor reforms	Limited admin & legal reforms w/o full enforcement	Fully enforced reforms w/strong military support

INSURGENT EVENT DATA SHAPING THE EXPEDITIONARY ENVIRONMENT

CAPABILITY	HIGH COMPLEXITY	MEDIUM COMPLEXITY	LOW COMPLEXITY
BOMBINGS	Deliberate & frequent bombings of key infra-structure nodes	Occasional major bombing campaigns throughout country	Random bombings for effect on public & private property
KIDNAPPING & ASSASSINATION	Routine kidnappings for funds & routine assassination of pols.	Occasional kid-napping for effect, selected assassins.	Random kidnappings or assassinations
CIVIL DISOBEDIENCE	Strong labor/school support, large public shows of solidarity	Occasional major demonstrations w/o violence	Infrequent public demonstrations, limited turnouts
STRIKES & RIOTS	Regular strikes & riots paralyzing the economy	Occasional strikes or riots affecting areas or industries	Infrequent strikes or riots limited in scope & duration
INTERNATIONAL MEDIA EVENTS	Daily or weekly events staged for or communi-cated to int'l media	Monthly int'l media events, or advance notice of ops	Occasional local events of limited interest to media
CONVENTIONAL MILITARY OPS	Established campaign of national scope with artillery support	Regional campaign with good C4I2, mortars, SAMS	"Hit & Run" tactics only, reliance on escape vice arms
INTERNATIONAL LEGAL ACTIVITY	Established territory & controlled populace, attempted recognition	Routine appeals to int'l organizations for observer status	No basis for legal recognition, no real attempts

APPENDIX F-2

Mission Area Factors Summary

A. TERMS OF REFERENCE INTRODUCTION

Mission area factors were developed by the Marine Air-Ground Task Force (MAGTF) Integration Section, Proponency and Requirements Branch of the MAGTF Warfighting Center to show the various threats and conditions that may be encountered by warfighters when operating in the countries of the expeditionary environment. The following charts depict the mission area factors and outline the criteria for levels of difficulty (thresholds) within each factor.

MISSION AREA FACTORS: THREAT

MISSION AREA FACTORS THREAT	CRITERIA LEVELS OF DIFFICULTY					
Drugs	Low		Medium			High
Terrorism	Low	Medium -			Medium +	High
Grey Arms/Tech Transfer	Low		Medium			High
Consolidated Threat	Negligible	1 of 3			2 of 3	All 3
General Ground OOB						
Infantry	Draft/No TR	Draft/TR	PM/No Exp	PM	Reg/TR	Reg/Exp
Armor	None	M-48/T-54/LAV	M-60,AA	T-62E/MOD 55	T-72M1	T-80/64B
Artillery	None	Mortars	How/SP	>30K Range/ FASCAM/TGM	>30K Range/NBC	BLOC
General Air OOB						
Air OOB	None	DC-3/Props	Day/VFR Jets	Early Radar	3d Gen Radar	BLOC
Close Air	None	Props	Day Jet Atk	Early Smart	STD-OFF PGM	NT/AW
AAW(IAD)	None	Early AAA	Hand-Held SAMs	EW Radar	3d Gen SAMs	BLOC
General Naval OOB						
Naval OOB	None	Small Surface	DEST/FRIG	ASUW/Air/ASW	F/W Carrier	NT/AW
S/S Msls	None	HE	Multi Warhead HE/BC	High/Flex Trajectories	Countermeasures	BLOC
Patrol Craft	None	Speed Boats	Sm Gun Boats	Lg Gun Boats	ASUW/Amlair	BLOC
NBC	None	Chem Weap/ No Delivery	Chem Weap/ With Delivery	Chem Weap/ Used	Chem/Bio Used	Nuc/Chem Avail
Ongoing Conflicts	No Conflicts					Conflicts

MISSION AREA FACTORS: ENVIRONMENT

MISSION AREA FACTORS ENVIRONMENT	CRITERIA LEVELS OF DIFFICULTY					
U.S. Equities	Low		Medium			High
Culture						
Language	English	Spanish/French		Arabic		All Others
Religion	Christian	Christian Orthodox		Eastern/Tribal/Islam		Islam
Weather	Dry/Warm	Wet/Warm	Mixed	Dry/Hot	Wet/Hot	Wet/Cold
Gen Geo Cond	Urban	Desert		Jungle		Mountainous
OP Elevation	<2000 Ft	<4000 Ft	<6000 Ft	>6000 Ft	>9000 Ft	>12000 Ft
Cross-Country Mob	Generally Suited			Partially Suited		Generally Unsuited
Intervisibility (LOS)	>2000 Meters			1000-2000 Meters		<1000 Meters
Hydrography- NGF	Good	Fair		Poor		Unsatisfactory
Hydrography- Coastal Threat	US NGF Advantage			US NGF and Threat Equal		Threat Advantage

MISSION AREA FACTORS: LOGISTICS

MISSION AREA FACTORS LOGISTICS	CRITERIA LEVELS OF DIFFICULTY					
MC&G Coverage	1:50 New	1:50 Old	Some 1:50	MSI Avail	1:250 New	None
Airfields	>1/C-5	1/C-5	>5/C-130	2-4/C-130	1/C-130	None
Ports	Wide Harbor/ >50' Depth	Wide Harbor/ >40' Depth	>40' Depth	35-39' Depth	25-34' Depth	None
Key Installations	None	Few Sites	Multi Sites	Pipeline	Oil Field	NBC
MEU Response Time	<2 Days	>2 - <4 Days		>4 - <6 Days		>6 Days
NEO						
Embassy Staff	<25	<50	<100	<250	<500	>500
Evacuees	None	<100	<200	<300	>300	>500 *
Inland Obj	Coastal	<100 NM	<300 NM	>300 NM	>600 NM	>999 NM

* For purposes of this study, 500 evacuees was used as a threshold. Anything above 500 would probably require consideration of other options, i.e., evacuation by airlift or sealift.

These mission area factors define the critical conditions, situations, threats, and logistical constraints which, when taken together with the countries identified, show various levels or thresholds of difficulty for conducting military operations. This product repesents a totally new approach to intelligence for warfighters because it evaluates and classifies countries in relationship to mission area factors and levels of difficulty assigned by warfighters themselves. The mission area factors do not represent a "fixed" list but constitute a "snapshot" based on their initial development in 1989 and 1990. The way in which thresholds between levels of difficulty for each factor are defined can be expected to change over time. Our intent at this stage has been to inform, to provice a useful reference that does not need to be locked up, and to establish and introductory baseline from which more detailed and precise factors and thresholds of difficulty can be developed.

The following charts provide a consolidated overview of seleted mission area factors for those countries which represent the greatest combination of threat, terrain, and logistic challenges to the MAGTF Such countries would be good candidates as models for the testing of USMC scenarios.

MISSION AREA FACTORS OVERVIEW - THREAT

REGION	COUNTRY	DRUGS	TERROR	GRAY ARMS	GND	AIR	NAV	NBC
WESTERN HEMISPHERE	CUBA	●	●	●	●	●	●	●
	MEXICO	●	●	●	●	●	●	○
MIDDLE EAST/ SOUTHWEST ASIA	IRAN	●	●	●	●	●	●	●
	IRAQ	○	●	●	●	●	●	●
	LIBYA	○	●	●	●	●	●	●
	SYRIA	●	●	●	●	●	●	◒
AFRICA	SOUTH AFRICA	○	◒	●	●	●	●	●
ASIA/PACIFIC	INDIA	●	●	●	●	●	●	●
	INDONESIA	●	○	○	●	●	●	●
	JAPAN	○	●	●	●	●	●	◒
	NORTH KOREA	○	●	●	●	●	●	◒
	PAKISTAN	●	●	◒	●	●	●	●
	PRC	●	○	●	●	●	●	●
	THAILAND	●	○	○	●	●	●	●
	VIETNAM	○	●	●	●	●	●	●
EUROPE/ MED	GREECE	●	●	●	●	●	●	○
	ITALY	○	●	●	●	●	●	○
	TURKEY	●	●	●	●	●	●	○

● ◒ ○ — INCREASING INVOLVEMENT

MISSION AREA FACTORS OVERVIEW - ENVIRONMENT AND LOGISTICS

REGION	COUNTRY	CULT	WX	TERR	NGF	MCLG	FAC	LIFT	MED
MIDDLE EAST/ SOUTHWEST ASIA	IRAQ	●	●	●	●	●	●	○	●
	NORTH YEMEN	●	●	●	◒	●	●	◒	●
	OMAN	●	●	●	◒	●	●	○	●
	SAUDI ARABIA	●	●	●	●	●	◒	○	●
AFRICA	MADAGASCAR	●	●	●	●	●	●	●	◒
	SOMALIA	●	●	○	◒	●	●	●	●
	SUDAN	●	●	●	◒	●	●	●	●
	UGANDA	○	◒	●	●	●	●	●	●
	ZAIRE	◒	●	●	○	●	●	●	●
ASIA/ PACIFIC	AFGHANISTAN	●	◒	●	●	●	●	●	●
	BANGLADESH	●	●	●	◒	●	●	●	●
	BURMA	●	●	●	◒	●	●	●	◒
	PAKISTAN	●	●	◒	●	●	●	◒	●
	PRC	●	◒	●	●	●	◒	●	●
	THAILAND	●	●	●	◒	●	●	◒	●

● ◒ ○ — INCREASING DIFFICULTY

B. CRITERIA AND SUMMARY ASSESSMENTS

The following pages will address each of the mission area factors separately and further describe the criteria by which levels of difficulty were established. These discussions will also include a summary assessment (taken from Volume I) of how individual factors impact on the 69 countries which presently comprise the expeditionary environment.

DRUG THREAT

CRITERIA FOR LEVELS OF DIFFICULTY

HIGH:

- Major drug producing and/or processing countries
- Heavy involvement in support functions for drug trafficking.

MEDIUM:

- Minor drug producing and/or processing countries
- Primary involvement is in one or more of the following:
  - Money laundering
  - Drug transshipment
  - Supply of precursor chemicals

LOW

- Drugs are of little significance.

Using this criteria, countries were classified into the three threat categories through research of the data sources. These sources included, but were not limited to the following:

(1) Annual Report of the Organized Crime Drug Enforcement Task Force Program, Fiscal Year 1988

(2) Defense Science Board Summer Study 1987, Detection and Neutralization of Illegal Drugs and Terrorist Devices, October 1987.

(3) U.S. Department of State, Bureau of International Narcotics Control, Strategy Report, March 1989.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The "war on drugs" is developing into a real war and **Latin America** in particular offers a "target rich environment" where Marine Corps forces can expect to be on call to assist law enforcement agencies.

In **Asia**, the "**Golden Triangle**" where **Burma, Thailand, and Laos** share a border is the center of the heroin trade, and this area should also see an increase in joint military-law enforcement activity in the future.

The top three drug trafficking countries were consiered to be **Colombia, Peru, and Burma**. Overviews of those countries are as follows:

(1) **Colombia** is the center of **South American** cocaine trafficking, the world's largest producer of marijuana, and the world's third largest producer of coca. This country has destroyed more than 90 percent of the cannabis growing in traditional northern areas, but traffickers have planted extensively in the San Lucas Mountains and south in Cauca. Marijuana tonnage increased in 1988 despite an aggressive eradication campaign. Coca cultivation increased above the 1987 level although eradication of 230 hectares was conducted manually. Despite police efforts to harrass the **Medellin** cartel and other trafficking groups, large amounts of cocaine continued to flow to the U.S.; almost 20 metric tons were seized by U.S. Customs. Overall enforcement remains hampered by a judicial system that has been intimidated by violence. Drug profits flow into and out of **Colombia**, but money laundering per se is not a major activity.

(2) **Peru** is the world's largest producer of coca with between 97,000 to 124,000 metric tons harvested in 1988. In addition, it converts much of its coca into coca paste and is a primary supplier of this substance to Colombian cocaine refineries. Enforcement in the **Upper Huallaga Valley**, the major growing zone for coca remains quite hazardous.

(3) **Burma** is the world's largest producer of opium with between 1,065 to 1,500 metric tons harvested in 1988. Political turmoil in the country has grounded its large-scale aerial eradication program until an effective Government is seated in **Rangoon**. Traffickers capitalized on diminished enforcement efforts to smuggle large quantities of opium and heroin with little interference. The prospect for the future is grim: with highly favorable climatic conditions and the suspension of programs to destroy crops or seize shipments of drugs or precursor chemicals from **China**, **Thailand**, and **India**, traffickers may harvest and move annually as much as 1,400 metric tons of opium to heroin refiners in **Southeast Asia**.

The following matrix shows the expeditionary environment countries that are most involved in drug production and trafficking:

MOST SIGNIFICANT DRUG COUNTRIES TYPES OF THREAT

	DRUG PRODUCTION	DRUG PROCESSING	PRECURSOR CHEMICALS	MONEY LAUNDERING	TRANSIT POINT
WESTERN HEMISPHERE					
ARGENTINA		X	X	X	X
BOLIVIA	X	X			
BRAZIL	X	X	X		X
COLOMBIA	X	X	X		
ECUADOR	X		X		X
JAMAICA	X				X
MEXICO	X				X
PANAMA			X	X	X
PERU	X	X			
MIDDLE EAST					
IRAN	X				X
ASIA					
AFGHANISTAN	X				
BURMA	X				
LAOS	X				
PAKISTAN	X				
THAILAND	X	X	X		

PLANNING AND PROGRAMMING IMPLICATIONS

In fighting the "war on drugs", the most common form of military assistance is expected to be wide-area surveillance and interdiction. This challenge will tax to the utmost Marine Corps reconnaissance, intelligence, and communications assets. The nature of the target being sought, generally a single nondescript platform integrated among many legitimate aircraft or ocean-going vessels, will require development of close working relationships and fast-reaction capabilities responsive to civilian intelligence and law enforcement leads. The requirements for liaison to law enforcement agencies could become as demanding, and as frustrating, as the present requirements for liaison to various remote threater staffs; Command and Control, Communications, Computers, Intelligence, and Interoperability (C4I2) requirements and capabilities will "Make or Break" Marine Corps forces assigned a role in the war on drugs.

TERRORISM THREAT

CRITERIA FOR LEVELS OF DIFFICULTY

HIGH: Countries found to have a significant association with terrorism, either through state-sponsored terrorism, organizational terrorism, or insurgent terrorism, or a combination of the three.

MEDIUM TO HIGH: Countries which have had past association and still maintain a residual involvement in terrorism, but to a lesser degree than high threat countries.

LOW TO MEDIUM: Countries largely characterized by internal revolutionary activity and related incidents where terrorism plays a role.

LOW: Countries with little or no association with terrorism.

Based on this criteria, countries were classified into the four categories through research of the reference material. This included, but was not limited to the following publications:

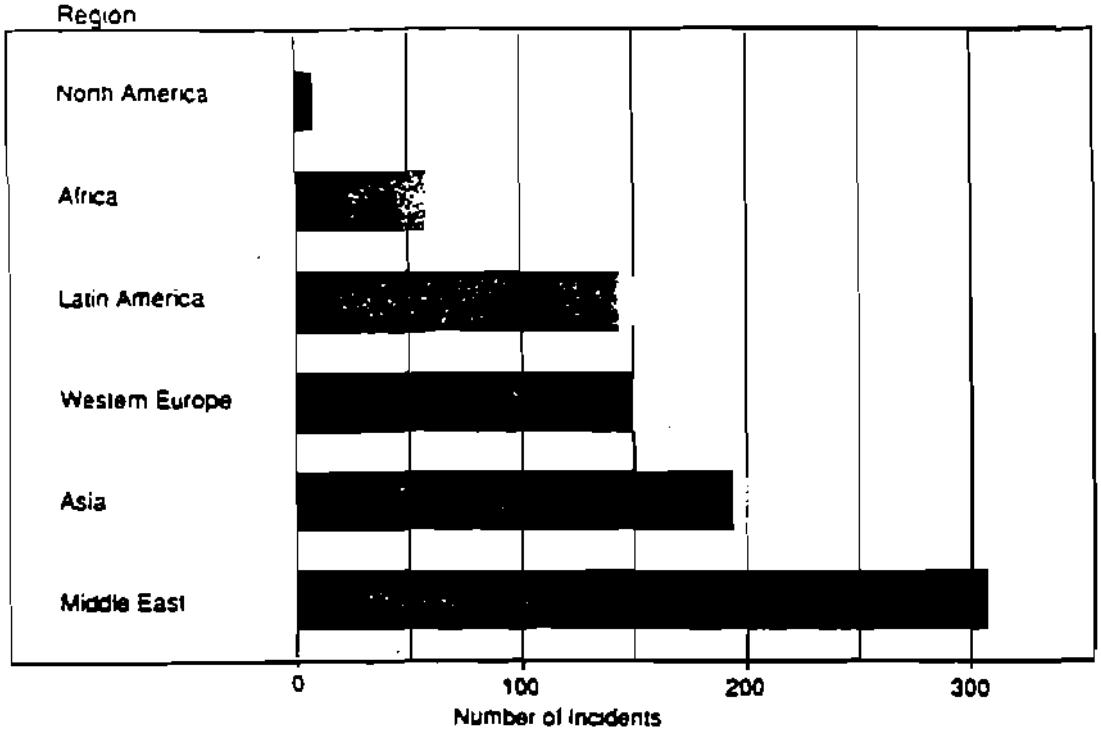
(1) Patterns of Global Terrorism: 1988, Department of State Publication 9705, Office of the Secretary of State Ambassador-at-Large for Counterterrorism, March 1989.

(2) Terrorist Group Profiles, U.S. Government Printing Office, November 1988.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The level of international terrorist activity worldwide increased by three percent in 1988 with 856 incidents as compared with 832 in 1987. As shown in the following chart, the **Middle East** continued to be the region most affected, incurring 313 attacks or 36 percent of the total worldwide. When **Middle East** spillover attacks are added, **Middle East**-inspired terrorist incidents account for 41 percent of the total. **Asia**, primarily due to terrorist attacks by **Afghanistan** against targets in **Pakistan**, held second place with 195 incidents or 22 percent of the total.

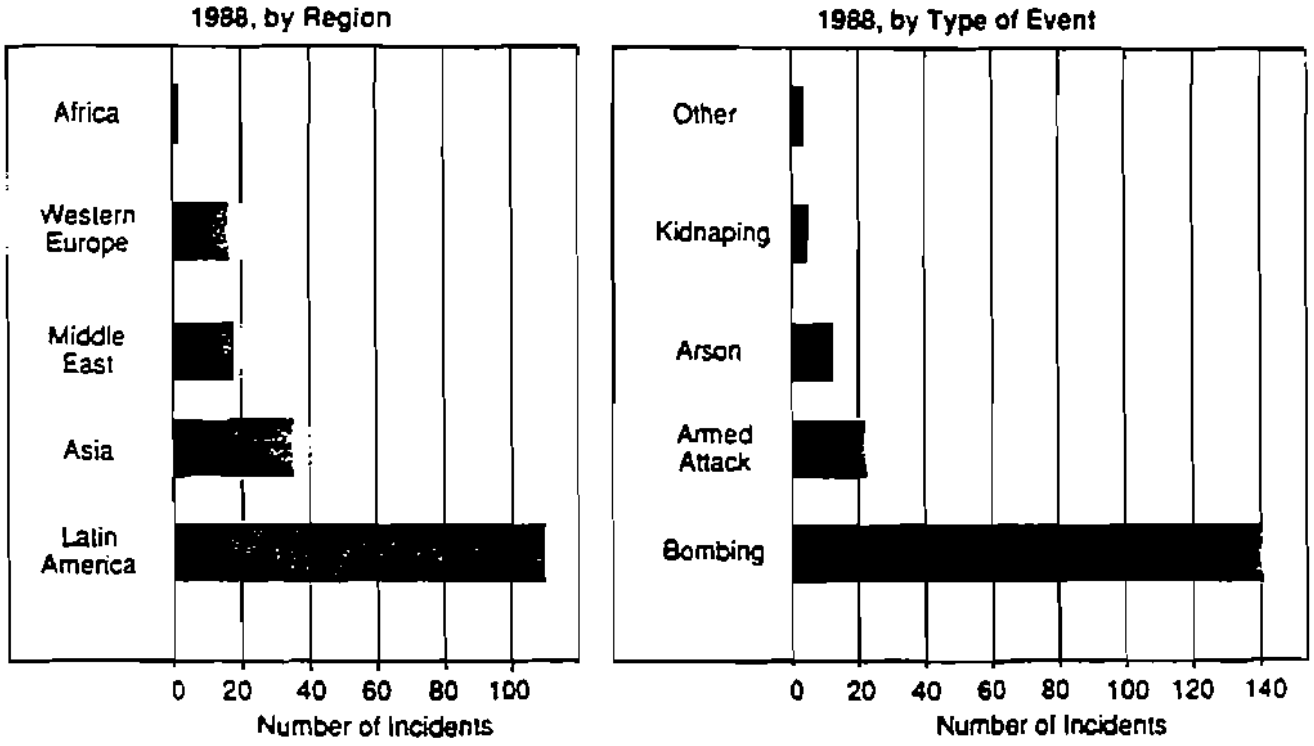
INTERNATIONAL TERRORIST INCIDENTS, 1988



As illustrated in the next two charts, the U.S. sustained a substantial number of attacks and casualties abroad in 1988, indicating that it remains a primary target for international terrorists. The number of anti-U.S. incidents increased in all regions, rising from 149 in 1987 to 185 in 1988, and resulting in 192 persons killed and 49 injured. Latin America was the locus of 60 percent of the incidents against U.S. citizens and property. About 20 percent of the anti-U.S. incidents took place in **Asia** while 10 percent were in the **Middle East** and 9 percent in Western Europe.

In 1988, 48 percent of the terrorist attacks involved bombings. Armed attacks came next with 29 percent followed by arson at 15 percent. Terrorists decreased their use of kidnappings as a method in 1988, with only 4 percent of the total. Of the 32 kidnapping incidents worldwide, 12 took place in Latin America. This was a change from 1987 when most of the kidnappings occurred in the **Middle East**.

ANTI-U.S. TERRORIST ATTACKS



PLANNING AND PROGRAMMING IMPLICATIONS

Terrorism is an unpredictable global threat. **Latin America** is the location of the greatest number of terrorist events, while the **Middle East** contains the greatest numer of terrorist training camps and other targetable facilities. Terrorists do not have rules of engagement, and they generally cannot be detected until after they have struck. MAGTFs must plan for perimeter security measures able to deal with the unexpected. As with drugs, preemptive raids could become more common in the 1990's. Also worth consideration is the possibility of a new method of operation developing between Joint Special Operations Forces (SOFs) and MAGTFs. In concept there is much to be said for the use of SOFs to "find and secure" hostages in place, with MAGTF elements being used to execute a hostile NEO on call. The ability to lift, deliver, and evacuate battalion-sized forces from over-the-horizon and into complex urban environments will be essential for this kind of mission.

GRAY ARMS AND TECHNOLOGY TRANSFER THREAT

CRITERIA FOR LEVELS OF DIFFICULTY

HIGH: Countries found to be sources of gray market arms and technology sales to unstable and potential hostile Third World buyers.

MEDIUM: Countries which have acted as transit sites or transshipment points for gray arms and technology sales.

LOW: Countries with no known association with gray arms and technology transfer.

DEFINITION:

Sales of military and military-related goods that fall between black market sales and open legitimate transactions comprise the gray market. Such grayness originates in the nature of the item being transferred, or in the character of the transaction, or both. In addition to basic weapons transfers, various products fall into the gray zone when they have both civilian and military applications, and if they are being shipped to countries eligible to receive them for civilian but not military use. Computers are good example, as well as communications equipment, unarmed cargo planes, air traffic control radars, and off-road vehicles. A company that ships such equipment to **South Africa** or another embargoed country, knowing it is intended for military use is engaged in gray-market arms trafficking.

Based on this methodology, countries were classified into the three categories through a rigorous review of the source data. Reference material included:

(1) World Military Expenditures and Arms Transfers 1988, U.S. Arms Control and Disarmament Agency

(2) Arms Transfers and the Third World: Trends and Developments, Army-Air Force Center for Low Intensity Conflict, Langley Air Force Base, Virginia, July 1988.

(3) Stockholm International Peace Research Institute (SIPRI) Yearbook 1989, 1988 and 1987

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart depicts the countries associated with gray arms sales and technology transfer. It is interesting to note that almost 60 percent of the source countries listed are in **Europe** while about 30 percent are in **Asia**

Great Britain, France, Italy, and **West Germany** have proven their technological prowess on the international market. **Japan** has used high technology in home electronics, computers, and semiconductors to gain its current position as an industry leader. **Israel**, has a significant emerging technological capability.

Individuals and companies operating in countries such as **France, Israel,** and **Japan** serve as either sources of arms for the Third World or as conduits through which **China, North Korea, Vietnam, Iran,** and **Iraq** illegally acquire restricted **U.S.** technology. In turn, these countries, as a routine policy, distribute arms and restricted technology to revolutionary groups and terrorists.

During the period 1981 to 1987, 502 individuals and companies were cited in 156 cases arising from violations of the 1976 Arms Export Control Act. However, it is suspected that many of the less visible brokers, financiers, middlemen, and fixers who specialize in convert arms transactions escaped detection.

COUNTRIES INVOLVED IN GRAY ARMS AND TECHNOLOGY TRANSFER

SOURCES	TRANSIT POINTS	BUYERS
BELGIUM	BELGIUM	AFGHANISTAN
CHINA	BULGARIA	ALGERIA
FINLAND	CHINA	ANGOLA
FRANCE	CUBA	BANGLADESH
INDIA	CYPRUS	COLOMBIA
ISRAEL	GREECE	CUBA
ITALY	HONG KONG	IRAN
JAPAN	ITALY	IRAQ
NETHERLANDS	MEXICO	KENYA
NORTH KOREA	NETHERLANDS	LIBYA
PANAMA	PANAMA	MALAYSIA
SCOTLAND	PORTUGAL	NICARAGUA
SWEDEN	SINGAPORE	NORTH KOREA
TURKEY	SOUTH AFRICA	SOMALIA
UNITED KINGDOM	SOUTH YEMEN	SOUTH AFRICA
VIETNAM	SYRIA	SOUTH YEMEN
WEST GERMANY		SUDAN
		UGANDA
		VIETNAM

PLANNING AND PROGRAMMING IMPLICATIONS

The sale of arms and technology to the Third World by more developed nations is of an increasing concern to the U.S. Questionable sales of restricted systems and material to unstable Third World countries are occurring largely through third party transfers. Such transfers often involve at least one Third World transit point. Panama for example, is a major transshipment site for computer technology enroute from the U.S. to Eastern Europe. Included in this threat is the proliferation of nuclear, biological, and chemical weapons and manufacturing capabilities, as well as the marketing of "Blue" (allied) weapons systems which cannot be countered without adverse impact on friendly forces. Many of the industrialized countries of Europe as well as emerging Third World countries are showing growth in arms and technology sales in the international market. While efforts are being made by cooperating countries to prevent illegal or questionable sales, they are frequently unsuccessful. Involved countries may not be aware of impending sales or may disagree with a U.S. view against a sale. Furthermore, U.S. attempts to define and restrict "dual-use" technology are frequently years behind industry development, so that such technologies are usually available during their early production. Finally, some private companies and individuals are willing to violate the laws and sell to any interested party for a profit. Gray arms trafficking and technology theft may generate requirements for the employment of Marine forces to destroy arms factories and storage depots, neutralize terrorist stocks of bio-chemical weapons, or confiscate stolen materials.

CONSOLIDATED THREAT OVERVIEW

CRITERIA FOR LEVELS OF DIFFICULTY

The most difficult countries are in the "all 3" category which indicates involvement with drugs, terrorism, and gray arms/technology transfer. Progressively lower levels of difficulty are shown by country involvement in "2 of 3", "1 of 3" or "negligible" association with these threats.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices show the involvement of expeditionary environment countries in the three threat areas of drugs, terrorism, and gray arms/technology transfers. In the **Western Hemisphere, Cuba, Mexico, and Panama** were the high-threat countries with involvement in all three areas. Eight other countries, or 50 percent of the countries addressed in this region, were associated with both drugs and terrorism.

In the **Middle East/Southwest Asia, Syria** was the highest threat country, followed by **Iran, Lebanon, South Yemen, Egypt, and Libya.**

Africa was the lowest overall threat. Only **Angola, Kenya, and South Africa** were identified with one threat area.

In **Asia, India** presented the greatest threat with involvement in all areas, while six other countries were identified with two of three areas and six countries with one of three areas.

In **Europe/Mediterranean, Greece** and **Turkey** were both high-threat countries followed by **Italy** with involvement in terrorism and gray arms/technology transfer.

CONSOLIDATED THREAT OVERVIEW

	NEGLIGIBLE	1 OF 3	2 OF 3	ALL
WESTERN HEMISPHERE	GRENADA	DOM REP (D)	COLOMBIA (D,T)	CUBA
	SURINAM	HAITI (D)	COSTA RICA (D,T)	MEXICO
		JAMAICA (D)	EL SALVADOR (D,T)	PANAMA
			GUATEMALA (D,T)	
			HONDURAS (D,T)	
			NICARAGUA (D,T)	
			PERU (D,T)	
			VENEZUELA(D,T)	
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN	EGYPT (D)	IRAN (D,T)	SYRIA
	IRAQ	LIBYA (T)	LEBANON (D,T)	
	KUWAIT		SOUTH YEMEN (T,G)	
	NORTH YEMEN			
	OMAN			
	QATAR			
	SAUDI ARABIA			
	UAE			

KEY D Drugs
T Terror
G Gray Arms/Technology Transfer

CONSOLIDATED THREAT OVERVIEW

	NEGLIGIBLE	1 OF 3	2 OF 3	ALL
AFRICA	ALGERIA	ANGOLA (T)		
	DJIBOUTI	KENYA (D)		
	ETHIOPIA	SOUTH AFRICA (G)		
	LIBERIA			
	MADAGASCAR			
	NAMIBIA			
	SOMALIA			
	SUDAN			
	TUNISIA			
	UGANDA			
	ZAIRE			
	ZIMBABWE			
ASIA/ PACIFIC	BANGLADESH	BURMA (D)	AFGHANISTAN (D,T)	INDIA
	PAPUA N. G.	INDONESIA (D)	NORTH KOREA (T,G)	
	SOUTH KOREA	JAPAN (T)	PAKISTAN (D,T)	
	S. PACIFIC IS.	MALAYSIA (D)	PHILIPPINES (D,T)	
	SPRATLY IS.	SRI LANKA (T)	PRC (D,G)	
		THAILAND (D)	VIETNAM (T,G)	
EUROPE/ MED	DENMARK		ITALY (T,G)	GREECE
	NORWAY			TURKEY
	YUGOSLAVIA			

KEY: D Drugs
T Terror
G Gray Arms/Technology Transfer

PLANNING AND PROGRAMMING IMPLICATIONS

Drug trafficking, terrorism, and gray arms trade are likely to be national security issues in the next decade. MAGTFs, operating as integral components of the balanced fleet, may have to respond to crisis situations in a variety of ways to protect the national interest. These may range from providing security or peacekeeping forces to conducting retaliatory strikes against threat forces. Marines must continually evaluate the threat as well as their operational concepts, doctrine, force structure, and acquisitions to ensure the maximum preparedness for potential contingency operations. Drugs, terrorism, and gray arms "targets" and scenarios require a different force structure, different organization and equipment, and different concepts and capabilities in C4I2. Force planners must also focus on the unique challenges of Third World environments and logistics requirements where Marine forces must operate without being able to turn on the conventional warfare "pipeline."

GENERAL GROUND ORDER OF BATTLE

CRITERIA FOR LEVELS OF DIFFICULTY

General Ground OOB	LEVELS OF DIFFICULTY (CAPABILITY) →					
	A	B	C	D	E	F
Infantry	Draft/No TR	Draft/TR	PMN/No Exp	PM	Reg/TR	Reg/Exp
Armor	None	M-48/T-54/LAV	M-60, AA	T-62/MOD 55	T-72M1	T-80/64B
Artillery	None	Mortars	How/SP	>30 Range/ FASCAM/TGM	>30 Range/NBC	BLOC

The expeditionary environment countries were broken into six approximately equal groups based on an assigned total capability value. The groups ranged from "A" with the least general ground Order of Battle (OOB) capability to "F" with the greatest. The total capability value was obtained by assigning points to the various infantry, armor and artillery capabilities, with the most significant capabilities (e.g., Reg/Exp, T-80/64B, BLOC) receiving the most points. Army size and quality (an assessment of training, leadership, combat experience, and general efficiency) were also factored into the total capability value. Volume II, Study Supporting Material, Section 13, General Gound Order of Battle contains more detailed information on this process including the exact point values assigned and the calculations made for each country. The references used as source material for this assessment are as follows:

(1) The Military Balance, 1988 - 1989
(2) Defense and Foreign Affairs Handbook, 1989
(3) World Armies, Second Edition by John Keegan, 1983

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices show the general ground OOB capabilities for expeditionary environment countries. Most countries in the **Western Hemisphere** had either small or small-to-medium capabilites. The countries with the most significant resources were **Cuba, Nicaragua, Colombia,** and **Mexico**.

In the **Middle East/Southwest Asia**, the countries which stood out with the largest capabilities were Egypt, Iran, Iraq, Syria, Libya, and **Saudi Arabia**.

GENERAL GROUND OOB CAPABILTIES

INCREASING CAPABILITY →

WESTERN HEMISPHERE	COSTA RICA	DOM. REP	EL SALVADOR	COLOMBIA	CUBA	
	GRENADA	HAITI	GUATEMALA	MEXICO	NICARAGUA	
	HONDURAS	PANAMA	PERU			
	JAMAICA	VENEZUELA				
	SURINAM					
MIDDLE EAST/ SOUTHWEST ASIA	KUWAIT	BAHRAIN	LEBANON	SAUDI ARABIA	LIBYA	EGYPT
		QATAR	NORTH YEMEN			IRAN
			OMAN			IRAQ
			SOUTH YEMEN			SYRIA
			UAE			

The most impressive ground OOB capabilities in **Africa** were found in the countries of **Algeria** and **Ethiopia**, followed by **Angola, Somalia, South Africa, Sudan and Uganda.**

In **Asia**, the countries of **India, North Korea, the Peoples' Republic of China**, and **Vietnam** were identified to have the largest capabilities not only in the region, but in the entire expeditionary environment. They were followed by **Pakistan, South Korea, Burma, Indonesia, Japan**, and **Thailand.**

In **Europe, Turkey** had the largest ground OOB followed by **Greece, Italy**, and **Yugoslavia.**

GENERAL GROUND OOB CAPABILTIES

INCREASING CAPABILITY →

AFRICA	DJIBOUTI	KENYA	MADAGASCAR	ANGOLA	ALGERIA	
	NAMIBIA	LIBERIA	ZAIRE	SOMALIA	ETHIOPIA	
		TUNISIA	ZIMBABWE	SOUTH AFRICA		
				SUDAN		
				UGANDA		
ASIA/ PACIFIC	PAPUA N. G.	SRI LANKA		AFGHANISTAN	BURMA	INDIA
	S. PACIFIC IS.			BANGLADESH	INDONESIA	NORTH KOREA
	SPRATLY IS.			MALAYSIA	JAPAN	PAKISTAN
				PHILIPPINES	THAILAND	PRC
						SOUTH KOREA
						VIETNAM
EUROPE/ MED		NORWAY	DENMARK		GREECE	TURKEY
					ITALY	
					YUGOSLAVIA	

PLANNING AND PROGRAMMING IMPLICATIONS

Besides Soviet proxies with advanced weapons systems, the conventional threat includes Third World countries using non-Soviet systems sold to them by allied or nominally friendly countries, and relatively sophisticated systems developed by Third World regional powers. The non-Soviet systems complicate our electronic warfare planning, signal intelligence, and communications; for in some instances we cannot jam them without jamming ourselves, and because of shared frequency spectrums.

The expeditionary environment is complex and lethal. The MAGTF can expect to meet trained and experienced infantry, modern armor, relatively sophisticated artillery including scatterable mines, as well as smart or stand-off munitions. Some countries have sophisticated surface-to-surface missiles and other advanced coastal defense systems.

An overview assessment of capabilities indicates that a MEU could conduct successful operations in countries with a small ground OOB. Depending on intelligence and threat country force dispostions, a MEU could also conduct successful raid-type operations against the larger and stronger countries. Such missions as Noncombatant Evacuation Operations (NEO) and other limited objective operations could be conducted with a reasonable chance of success provided there was adequate preparation and naval support. In deciding how to train, equip, and organize Marine Corps forces our planners much constantly evaluate trade-offs between our own capabilities limited by our forward deployed amphibious character and the small size of our forces afloat, and the fully equipped, trained, and generally well organized forces we might confront.

GENERAL AIR ORDER OF BATTLE

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY (CAPABILITY) →					
	A	B	C	D	E	F
General Air OOB						
Air OOB	None	DC-3/Props	Day/VFR Jets	Early Radar	3d Gen Radar	BLOC
Close Air	None	Props	Day Jet Atk	Early Smart	STD-OFF PGM	NT/AW
AAW (IAD)	None	Early AAA	Hand-Held SAMs	EW Radar	3d Gen SAMs	BLOC

The expeditionary environment countries were divided into six approximately equal groups based on an assigned total capability value. The groups ranged from "A" with the least general air OOB capability to "F" with the greatest. The total capability value was obtained by assigning points to the various air OOB, close air support, and Antiair Warfare (AAW)/Integrated Air Defense (IAD) capabilities, with the most significant capabilities (e.g., BLOC, 3d generation radar, Night Time/All Weather (NT/AW), Stand-Off-Precision Guided Munitions (STD-OFF PGM), 3d generation Surface-to-Air Missiles (SAMs)) receiving the most points. Air Force size and quality (an assessment of training, leadership, combat experience, and general efficiency) were also factored into the total capability value. Volume II, Study Supporting Material, Section 14, General Air Order of Battle contains more detailed information on this process including the exact point values assigned and the calculations made for each country. The references used as source material for this assessment are as follows:

(1) Defense and Foreign Affairs Handbook, 1989
(2) Jane's All the World's Aircraft, 1988 - 1989
(3) Jane's Land Based Air Defense Systems, 1989 - 1990
(4) Jane's Weapon Systems, 1988 - 1989
(5) Jane's Weapon Systems 1987 - 1988

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices depict the general air OOB capabilities for expeditionary environment countries. Most countries in the **Western Hemisphere** are grouped in the lowest three categories. In this region, the countries with the most significant aviation resources were **Cuba, Nicaragua, and Peru.**

From a global perspective, **Egypt, Iran, Iraq, and Syria** stood out with the strongest aviation and air defense assets. Other countries in the **Middle East/Southwest Asia** with large capabilities were **Libya, Saudi Arabia, and South Yemen.**

GENERAL AIR OOB CAPABILITIES

INCREASING CAPABILITIES →

WESTERN HEMISPHERE	COSTA RICA	DOM REP	COLOMBIA	NICARAGUA	CUBA	
	GRENADA	GUATEMALA	EL SALVADOR	PERU		
	JAMAICA	HAITI	MEXICO			
	PANAMA	HONDURAS	VENEZUELA			
	SURINAM					
MIDDLE EAST/ SOUTHWEST ASIA		BAHRAIN	OMAN	KUWAIT	LIBYA	EGYPT
		LEBANON	QATAR	NORTH YEMEN	SAUDI ARABIA	IRAN
			UAE		SOUTH YEMEN	IRAQ
						SYRIA

In **Africa**, the most impressive air OOB countries were **Algeria, Angola,** and **South Africa.**

The most extensive aviation capabilities in **Asia/Pacific** were found in the countries of **India, Japan, North Korea,** and the **People's Republic of China.** They were followed by **Afghanistan, South Korea,** and **Vietnam.**

In **Europe/Mediterranean, Italy, Turkey,** and **Yugoslavia** had the strongest air OOB followed by **Greece, Norway,** and **Denmark.**

GENERAL AIR OOB CAPABILITIES

INCREASING CAPABILITIES →

AFRICA	DJIBOUTI	KENYA	SOMALIA	ETHIOPIA	ALGERIA	
	LIBERIA	UGANDA	SUDAN	MADAGASCAR	ANGOLA	
	NAMIBIA	ZAIRE	TUNISIA	ZIMBABWE	SOUTH AFRICA	
ASIA/ PACIFIC	PAPUA N. G.	BURMA	BANGLADESH	INDONESIA	AFGHANISTAN	INDIA
	S. PACIFIC IS.	SRI LANKA	PHILIPPINES	MALAYSIA	SOUTH KOREA	JAPAN
	SPRATLY IS.			PAKISTAN	VIETNAM	NORTH KOREA
				THAILAND		PRC
EUROPE/ MED				DENMARK	GREECE	ITALY
					NORWAY	TURKEY
						YUGOSLAVIA

PLANNING AND PROGRAMMING IMPLICATIONS

The expeditionary environment in the air is as complex and lethal as that on the ground. The MAGTF can expect to encounter threat aircraft with some night or all-weather capability, as well as smart or stand-off munitions. Iraq, for example, employs MiG-29 aircraft which are kept operationally ready through the assistance of on-site Soviet advisors. Threat integrated air defense systems may include three dimensional long-range radars able to detect stealthy airborne platforms. In this regard, Libya employs an air defense system known as "SENEZH" which is modeled after Soviet equipment and doctrine. China has a relatively sophisticated network of air defense radars which provides surveillance and control, and an early warning system for the detection of hostile missiles. Threat air defense systems may also employ a variety of advanced and strategicallly placed SAMs. Syria, for example, has some of the most modern Soviet provided SAMs as well as 50,000 personnel in a separate air defense command.

An examination of aviation and air defense capabilities of expeditionary environment countries indicates that a MEU could expect to conduct successful air operations against most lower capability countries. Depending on a variety of factors, such as the operational condition of threat aircraft and air defense weapons, unit locations, and detection capabilities, a MEU could also conduct operations effectively against many of the stronger countries. Given our critical reliance on vertical lift as a primary means of expeditionary mobility, Marine Corps planners must make more provision for the suppression of air defense, survivability of lift aircraft, and availability of close air support for all MAGTF missions with special emphasis on stability operations and low-intensity conflict requirements.

GENERAL NAVAL ORDER OF BATTLE

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY (CAPABILITY) →					
	A	B	C	D	E	F
General Naval OOB						
Naval OOB	None	Small Surface	DEST/FRIG	ASUW/Air/ASW	F/W Carrier	NT/AW
S/S Msls	None	ME	Multi Warhead ME/BC	High/Flex Trajectories	Countermeasures	BLOC
Patrol Craft	None	Speedy Boats	Sm Gun Boats	Lg Gun Boats	ASUW/Antiair	BLOC

The expeditionary environment countries were divided into six approximately equal groups based on an assigned total capability value. The groups ranged from "A" with the least general naval OOB capability to "F" with the greatest. The total capability value was obtained by assigning points to the various naval OOB, surface-to-surface missile, and patrol craft capabilities, with the most significant capabilities (e.g., NT/AW, Fixed Wing Carrier, Bloc, Countermeasures, Antisurface Warfare (ASUW)/Antiair) receiving the most points. The Navy size and quality (an assessment of training, leadership, combat experience, and general efficiency) were also factored into the total capability value. Volume II, Study Supporting Material , Section 15, General Naval Order of Battle contains more detailed information on this process including the exact point values assigned and the calculations made for each country. The references used as source material for this assessment are as follows:

(1) Jane's Fighting Ships, 1988 - 1989
(2) Jane's Weapon Systems, 1987 - 1988
(3) Defense and Foreign Affairs Handbook 1989
(4) A Quick and Dirty Guide to War by James Dunnigan and Austin Bay, Updated Edition, dated 1986

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices show the general naval OOB capabilities for expeditionary environment countries. In the **Western Hemisphere, Cuba** was identified as having the greatest naval capability, followed by **Colombia, Mexico, Peru,** and **Venezuela.**

In the **Middle East/Southwest Asia, Egypt** stood out with the most well-equipped naval force followed by **Iran, Iraq, Libya,** and **Syria.**

GENERAL NAVAL OOB CAPABILITIES

INCREASING CAPABILITIES →

WESTERN HEMISPHERE	GRENADA	COSTA RICA	DOM REP	COLOMBIA	CUBA	
	SURINAM	GUATEMALA	EL SALVADOR	MEXICO		
		HAITI	NICARAGUA	PERU		
		HONDURAS		VENEZUELA		
		JAMAICA				
		PANAMA				
MIDDLE EAST/ SOUTHWEST ASIA	LEBANON		BAHRAIN	SAUDI ARABIA	IRAN	EGYPT
			KUWAIT	SOUTH YEMEN	IRAQ	
			NORTH YEMEN		LIBYA	
			OMAN		SYRIA	
			QATAR			
			UAE			

In **Africa** the primary naval forces were found in **Algeria, Ethiopia,** and **South Africa** followed by **Angola, Kenya,** and **Somalia.**

Both **Asia/Pacific** and **Europe Mediterranean** have a high proportion of countries with a strong naval force. In **Asia,** the countries of **India, Indonesia, Japan, North Korea, Pakistan,** the **People's Republic** of China, and **South Korea** were predominate, while in **Europe, Italy, Turkey** and **Yugoslavia** had the most extensive capabilities.

GENERAL NAVAL OOB CAPABILITIES

INCREASING CAPABILITIES →

AFRICA	DJIBOUTI	MADAGASCAR	TUNISIA	ANGOLA	ALGERIA	
	LIBERIA	SUDAN		KENYA	ETHIOPIA	
	NAMIBIA	ZAIRE		SOMALIA	SOUTH AFRICA	
	UGANDA					
	ZIMBABWE					
ASIA/ PACIFIC	AFGHANISTAN	PAPUA N. G.	BURMA	MALAYSIA	BANGLADESH	INDIA
	S. PACIFIC IS.	SRI LANKA	PHILIPPINES		THAILAND	INDONESIA
	SPRATLY IS.				VIETNAM	JAPAN
						NORTH KOREA
						PAKISTAN
						PRC
						SOUTH KOREA
EUROPE/ MED				DENMARK	GREECE	ITALY
				NORWAY		TURKEY
						YUGOSLAVIA

PLANNING AND PROGRAMMING IMPLICATIONS

The expeditionary environment at sea could present some serious challenges for an Amphibious Task Force (ATF) enroute to, or operating in an objective area. India, for example has two fixed wing aircraft carriers (Ex -U.K.), five destroyers, twenty-one frigates, and six corvettes equipped with Surface-toSurface Missiles (SSMs), SAMs, guns, torpedos, antisubmarine mortars, countermeasures, and radars. Another example of an expeditionery environment country with a strong naval capability is Italy. It has two light aircraft carriers (one can accommodate VSTOL aircraft and helicopters, and one can handle helicopters only), two cruisers, six destroyers, sixteen frigates, and nineteen corvettes all equipped with modern weapons and supporting systems.

A review of the naval capabilities of expeditionary environment countries indicates that those countries depicted in the three most difficult categories would represent a formidable threat to a MEU-sized ATF. Limited objective operations in these countries should be planned to take greatest advantage of intelligence, naval support, and the element of surprise. Marine Corps planners should also pursue continued close coordination with the Navy to focus on the shortfalls in amphibious lift, shallow-water anti-submarine and mine warfare, over-the-horizon delivery, and the suppresion of coastal missiles.

NUCLEAR, BIOLOGICAL, AND CHEMICAL ORDER OF BATTLE

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY (CAPABILITY) →					
	A	B	C	D	E	F
NBC	None	Chem/Weap/ No Delivery	Chem Weap With Delivery	Chem Weap/ Used	Chem/Bio Used	Nuc/Chem Avail

E - Countries possessing nuclear and chemical weapons

E - Countries which have used chemical and biological weapons

D - Countries which have used chemical weapons

C - Countries suspected to have chemical weapons with a delivery capability

B - Countries suspected to have chemical weapons but without a means of delivery

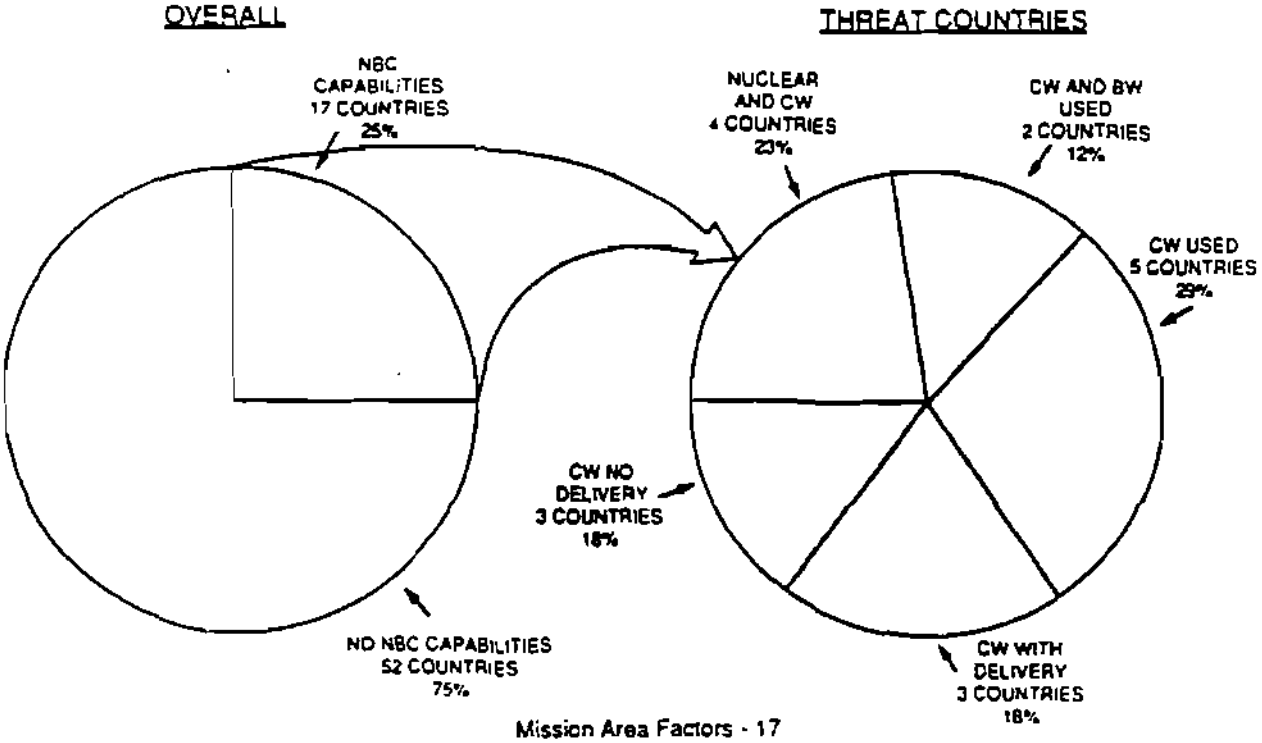
A - Countries believed not to have an NBC weapons capability

Countries in the various categories were identified through a thorough review of open source literature. References most useful to this assessment were the SIPRI Yearbooks, 1989, 1988, and 1987.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying graphics address the expeditionary environment countries which were found to possess varying types and quantities of NBC weapons.

DISTRIBUTION OF EXPEDITIONARY ENVIRONMENT COUNTRIES BASED ON NBC CAPABILITIES



Mission Area Factors - 17

There were 4 countries, (**South Africa, India, Pakistan,** and the **PRC**) thought to possess nuclear and chemical weapons and constitute the greatest threat.

At the next level of threat, there were 2 countries, **Iraq** and **Vietnam**, accused of using both chemical and biological weapons.

Next, there were 5 countries reported to have used chemical weapons only. These countries are **Cuba, Iran, Libya, Indonesia,** and **Thailand.**

The last two categories of threat were the countries with chemical weapons and delivery means, and those with chemical weapons but without a reported means of delivery. Each of these categories had 3 countries. **Egypt, Syria,** and **North Korea** were reported to have chemical weapons with delivery means while **Burma, Japan,** and **South Korea** were thought to have only possession.

NBC THREAT OVERVIEW

	CHEMICAL WEAPONS NO DELIVERY	CHEMICAL WEAPONS WITH DELIVERY	CHEMICAL WEAPONS USED	CHEMICAL WEAPONS AND BIOLOGICAL WEAPONS USED	NUCLEAR AND CHEMICAL WEAPONS
WESTERN HEMISPHERE			CUBA		
MIDDLE EAST/ SOUTHWEST ASIA		EGYPT	IRAN	IRAQ	
		SYRIA	LIBYA		
AFRICA					SOUTH AFRICA
ASIA/PACIFIC	BURMA	NORTH KOREA	INDONESIA	VIETNAM	INDIA
	JAPAN		THAILAND		PAKISTAN
	SOUTH KOREA				PRC

PLANNING AND PROGRAMMING IMPLICATIONS

The NBC threat must be factored into Service capabilities planning and programming. There are countries, particularly in the **Middle East** and **Asia**, that have used bio-chemical weapons and can be expected to use them again. There are increasing numbers of countries that have stocks of bio-chemical weapons, and other countries working to maintain or develop nuclear capabilities. Perhaps most threatening, as NBC technology and weapons proliferate, the opportunities for nongovernmental groups to steal working weapons and active bio-chemical agents increases dramatically. The next decade may well see a large metropolitan area held hostage to the threat of covertly emplaced and remotely detonated bio-chemical or nuclear weapons.

Some MAGTFs, for example those assigned contingency missions in the **Middle East** and selected countries in **Asia**, must continue to plan for and stock equipment needed to fight in a contaminated environment. All MAGTFs should be prepared to execute raids to seize and neutralize NBC weapons under development or in transit.

However, it would be imprudent to over-emphasize this threat, which appears in only 25% of the countries of concern to the Marine Corps. One strategy of possible value would be to carefully tailor a single MAGTF and develop MEU (NBC) training and equipping cycles just as we have for MEU (SOC).

ONGOING CONFLICTS

CRITERIA FOR LEVELS OF DIFFICULTY

Through a review of the source material, conflicts locations throughout the world were identified. These conflicts fell into five categories: regional conflicts, civil wars, insurgencies, drug related conflicts, and conflicts involving government instability and repression. In many of the situations, various levels of violence and disorder have occurred in the past and threaten to break out again. In other cases fighting occurs continuously or intermittently at the present time. All countries were evaluated for their involvement in conflict situations. Volume II, Study Supporting Material, Section 5, Existing Ongoing Conflicts provides a description of ongoing conflicts in the countries of interest. When research identified conflicts in countries outside the expeditionary environment, they were also described. The following references were used as the principal basis for this assessment:

(1) Defense and Foreign Affairs Handbook, 1989
(2) A Quick and Dirty Guide to War, by James F. Dunnigan and Austin Bay, 1986
(3) The Statesman's Yearbook, 1989 - 1990
(4) World Almanac and Book of Facts, 1989
(5) Zones of Conflict: An Atlas of Future Wars, by John Keagan and Andrew Wheatcraft, 1988
(6) Countries of the World and Their Leaders Yearbook, 1989
(7) The World in Conflict, by John Laffin, 1989
(8) Brassey's War Annual 2, A Guide to Contemporary Wars and Conflicts, by John Laffin, 1986

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows a regional breakdown of conflict locations and the types of conflict involved. In the **Western Hemisphere** there have been various levels of violence and disorder in **El Salvador, Guatemala, Honduras,** and **Nicaragua** caused by insurgents. Drug related violence, often combined with terrorism and insurgency, is a major problem in **Colombia** and **Peru.**

In the **Middle East,** regional disputes have prevailed in recent years dominated largely by the **Iran-Iraq** War and **Syrian** intervention in **Lebanon. Syria** would like to take advantage of the civil war in **Lebanon** to expand its borders. The territorial issue between **Israel** and the Palistinians is also highly volitile and the possibility of escalated conflict is a major concern. Now, a new confrontation in this region has erupted between **Iraq** and its Arab neighbors, as well as the **U.S.** and most other countries of the world, over the **Iraqi** seizure of **Kuwait.** Only **Libya,** the Palestine Liberation Organization (PLO), and to a certain degree **Jordan** and **Sudan** seem to side with **Iraq.** This confrontation has potential to be the largest conflict in recent years.

In **Africa,** there are a range of conflicts from the civil wars in **Angola, Liberia** and **Mozambique,** to the insurgent violence in **Ethiopia,** to the disorder and bloodshed in **South Africa** over apartheid. In this region, many countries can be characterized by government instability, frequent violence, economic underdevelopment, and acute poverty. The crisis-torn west **African** country of **Liberia** is an example of an ongoing conflict with poor prospects for resolution in the immediate future. To protect **U.S.** interests, a **MEU** was recently committed in this country to conduct noncombatant evacuation operations and maintain order around the **U.S.** Embassy. In **Ethiopia,** civil war and starvation continue to prevail, while a corrupt and unstable Marxist regime struggles to remain in power. As the **South African** Government continues to support its policy of apartheid and black **African** groups fight among themselves, there is potential for serious consequences in this country.

In **Asia** and the **Pacific,** a major share of the 12 conflicts countries are involved in insurgencies and/or drug related violence. Countries such as **Afghanistan, Cambodia,** and the **Philippines** all have active guerrilla forces trying to overthrow their governments. The "Golden Triangle" where **Burma, Thailand,** and **Laos** share a border, is the center of the region's heroin trade as well as frequent clashes between drug traffickers and government authorities. Countries such as **North Korea** have stocks of chemical weapons, and other countries (**PRC, India,** and **Pakistan**) are working to expand an already developed arsenal of nuclear weapons. Given the rate at which NBC weapons are proliferating in this region, it is quite likely they will eventually fall into the hands of extremist or terrorist groups.

While **Europe** and the **Mediterranean** presently have no active conflicts, there is significant ethnic unrest along with political and economic turmoil in a number of countries that could form the basis for open conflict. Although Poland now has free elections and a non-Communist government, severe economic problems persist and there could be a resurgence of hostility from the people if conditions do not rapidly improve. The longstanding disputes between **Greece** and **Turkey** could easily reemerge as they did in 1987. If this should occur over an issue such as the oil rights under the Aegean Sea, it could lead to a war between these two countries which would have serious impact on **Europe** as well as the **U.S.**

CONFLICTS LOCATIONS

WESTERN HEMISPHERE	MIDDLE EAST	AFRICA	ASIA	EUROPE
COLOMBIA (D)	IRAN (R)	ANGOLA (CW)	AFGHANISTAN (I)	POLAND (I/R)
EL SALVADOR (I)	IRAQ (R)	CHAD (R)	BURMA (D)	TURKEY/GREECE (R)
GUATEMALA (I)	ISRAEL (R)	LIBERIA (CW)	CAMBODIA (I)	
GUYANA (R)	LEBANON (CW)	LIBYA (R)	CHINA (R)	
HAITI (I/R)	OMAN (I)	ETHIOPIA (I)	INDONESIA (I)	
HONDURAS (I)	SYRIA (R)	MOZAMBIQUE (CW)	KOREA (N/S) (R)	
NICARAGUA (I)		NAMIBIA (I)	LAOS (D)	
PANAMA (R)		SOUTH AFRICA (I)	MALAYSIA (I)	
PERU (D)		SUDAN (CW)	PAKISTAN (R)	
		WESTERN SAHARA (R)	PHILIPPINES (I)	
		ZAIRE (I/R)	THAILAND (D)	
		ZIMBABWE (I)	S. CHINA SEA (R)	

KEY: R- REGIONAL CW - CIVIL WAR I - INSURGENCY D - DRUGS I/R - INSTABILITY/REPRESSION

PLANNING AND PROGRAMMING IMPLICATIONS

The expeditionary environment is a violent one with numerous existing conflicts and high likelihood of increased instability in the future. The emerging threat of the 1990's is predominantly nongovernmental, nonconventional, dynamic or random, nonlinear, and without rules of engagement or known doctrine. This threat is also difficult to guard against because our national intelligence community does not have an "indications and warnings" capability against these "type"threats, while the emerging enemy, by contrast, has a virtually unlimited source of drug addicts and related criminals that can be mobilized to compromise our own operational security. The emerging threat has added "worst case" scenarios for which MAGTFs must prepare, including the threat of nonconventional attacks, such as bio-chemical attacks against concentrations of U.S. citizens overseas. In view of the diversity of threats it may confront in the future, MAGTFs must train, equip, and organize to be prepared for operations across the spectrum of conflict, while being more thoughtful about what specific roles and missions a single MAGTF can realistically undertake by itself and/or as the vanguard of follow-on forces.

U.S. EQUITIES OVERSEAS

CRITERIA FOR LEVELS OF DIFFICULTY

HIGH - Countries with substantial U.S. equities.

MEDIUM - Countries with moderate U.S. equities.

LOW - Countries with few U.S. equities.

For purposes of this assessment, U.S. equities in the countries of interest included:

- Direct investment
- Trade (imports and exports)
- Economic and military aid
- U.S. citizens in residence
- Strategic and tactical equities (e.g., strategic location, U.S. bases, special cooperation)

In the process of determining overall U.S. equities, the following two step methodology was used:

(1) The monetary values of U.S. direct investment, exports, imports, and U.S. aid for each country were combined and applied to the U.S. $ Equities scale below. The number of U.S. citizens living in each country was applied to the U.S. Citizen Equity scale:

U.S. $ EQUITY	
BIL $S	RATING
>10.00	6
5.00 - 10.00	5
2.50 - 4.99	4
1.00 - 2.49	3
.50 - .99	2
>0 - .49	1
0	0

U.S. CITIZEN EQUITY	
NO. CIT.	RATING
>10,000	6
5,000 - 10,000	5
2,500 - 4,999	4
1,000 - 2,499	3
500 - 999	2
>0 - 499	1
0	0

(2) The U.S. dollar equity rating and U.S. citizen equity rating were added together and applied to the following overall U.S. equity scale:

OVERALL U.S. EQUITY		
HIGH	-	9-12
MEDIUM	-	5-8
LOW	-	0-4

Volume II, Study Supporting Material, Section 6, U.S. Equities Overseas contains a description of strategic and tactical equities in the respective countries as well as the data for U.S. military and citizen equities on which the ratings were based. The following references were used as source material for this assessment:

(1) U.S. Department of State, Country Reports on Economic Policy and Trade Practices, 1989
(2) Defense and Foreign Affairs Handbook, 1989
(3) Countries of the World and Their Leaders Yearbook 1989, Gale Research, Inc.
(4) Central Intelligence Agency, The World Factbook, 1988
(5) U.S. Department of State, Background Notes and Post Reports, 1987 - 1989.
(6) U.S. Department of Commerce, Statistical Abstract, 1989.
(7) Consular Affairs Office, U.S. Department of State, Numbers of U.S.Citizens Living in Countries of Interest, 21 - 22 February 1990

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows a regional distribution of countries by their level of U.S. equity. In the **Western Hemisphere, Mexico** had the highest ranking with significantly more dollar equity (25.9 billion) and U.S. citizens (322,250) than other countries. It was followed by **Venezuela, Panama** and **Colombia**, all with over 5 billion in trade and investment, and over 11,000 U.S. citizens. Overall in this region, just under half the countries (7 of 16) fell into the high category while the remainder were about evenly distributed between medium and low.

In the **Middle East/Southwest Asia, Saudi Arabia** had by far the largest U.S. equity with over 10 billion in dollar value and 21,600 U.S. citizens. It was followed by **Egypt** (3 billion dollar equity and 11,210 U.S. citizens). The other countries in this region fell into the low category except for **Kuwait** and **North Yemen** which were rated as medium.

In **Africa**, two thirds of the countries (10 of 15) were rated in the low category. **Algeria, Kenya, Liberia**, and **Zaire** were classified medium and only **South Africa** with 3.5 billion dollar equity and 9,400 U.S. citizens was rated high.

In **Asia/Pacific** region, **Japan** surpassed all other countries with almost 122 billion in dollar equity and 41,000 U.S. citizens. The next closest countries in the high rating were **South Korea** (27 billion dollars and 10,250 U.S. citizens) and the **Philippines** (6 billion and 120,090 U.S. citizens). Besides the 6 countries in the high category, 4 countries including **India** and **Pakistan** were rated medium, and the remainder were low.

In **Europe** and the **Mediterranean, Italy** had the highest rating with 25.6 billion in dollar equity and 92,269 U.S. citizens. It was followed by **Greece** and **Norway** in the high category. The remaining three countries, **Turkey, Denmark** and **Yugoslavia** received a medium classification.

U.S. EQUITY OVERSEAS

	LOW	MEDIUM	HIGH
WESTERN HEMISPHERE	CUBA EL SALVADOR GRENADA NICARAGUA SURINAM	GUATEMALA HAITI HONDURAS JAMAICA	COLOMBIA COSTA RICA DOM REP MEXICO PANAMA PERU VENEZUELA
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN IRAN IRAQ LEBANON LIBYA OMAN SOUTH YEMEN SYRIA	KUWAIT NORTH YEMEN	EGYPT SAUDI ARABIA UAE
AFRICA	ANGOLA DJIBOUTI ETHIOPIA MADAGASCAR NAMIBIA SOMALIA SUDAN TUNISIA UGANDA ZIMBABWE	ALGERIA KENYA LIBERIA ZAIRE	SOUTH AFRICA
ASIA/PACIFIC	AFGHANISTAN BANGLADESH BURMA NORTH KOREA SOUTH PACIFIC IS SPRATLY IS SRI LANKA VIETNAM	INDIA MALAYSIA PAKISTAN PAPUA NEW GUINEA	INDONESIA JAPAN PHILIPPINES PRC SOUTH KOREA THAILAND
EUROPE/MED		DENMARK TURKEY YUGOSLAVIA	GREECE ITALY NORWAY

PLANNING AND PROGRAMMING IMPLICATIONS

With existing conflicts in the expeditionary environment and high likelihood of increased instability in the future, U.S. investments and U.S. citizens no longer enjoy the relative immunity from local violence which characterized earlier decades. The increasing lethality of both Third World governments and nonconventional groups places at risk assets and strategic choke points that in the past could only have been attacked by a major power. The deliberate sinking of a major U.S. vessel in both the Panama Canal and Suez Canal is a threat difficult to defend against. As such threats begin to concern policy-makers, the prospects for the employment of U.S. forces in preemptive attacks will increase. To effectively meet the difficult challenges of the future, Marines must sharpen their abilities for rapid crisis-action planning and be ready to "fight smart" when the time comes to execute a mission.

CULTURAL FACTORS: LANGUAGE AND RELIGION

CRITERIA FOR LEVELS OF DIFFICULTY

Cultral	LEVELS OF DIFFICULTY →			
	A	B	C	D
Language	English	Spanish/French	Arabic	All Others
Religion	Christian	Christian Orthodox	Eastern/Tribal/Islam	Islam

D - Countries with hard languages other than those specified below combined with the religion of Islam.

C - Countries with the Arabic language combined with Eastern, Tribal, or Islamic religions

B - Countries with Spanish, French, and other predominately **European** languages combined with the Christian Orthodox religion

A - Countries with the English language combined with the Christian religion

Note - In cases where a country did not match a precise level as specified above, an intermediary level between the language and religion was selected, e.g. **Liberia** with the English language and traditional religion was rated B.

Volume II, Study Supporting Material, Section 17, Cultural Factors: Language and Religion provides tables showing a cultural factors assessment for each country as well as a listing of religions and primary and secondary languages. The references used as source material for this assessment are as follows:

(1) Special Assistant, USMC Intelligence Center letter 3811 IN 06 of 26 October 1989, Marine Corps Expeditionary Environment Language Requirements
(2) Countries of the World, 1989, Gale Research Inc.,
(3) World Almanac and Book of Facts, 1989, Published by Pharos Books, a Scripps Howard Company

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts depict the distribution of 69 expeditionary environment countries by culture: language and religion. Almost 60 percent of the countries fall into the two most difficult cultural categories (C and D).

The regions with the hardest languages and the most distant religions were the **Middle East/Southwest Asia** (Iran most difficult), **Africa** (**Ethiopia** and **Somalia** most difficult), and **Asia/Pacific** (**Afghanistan, Bangladesh, Indonesia,** and **Pakistan** most difficult). The **Western Hemisphere** and **Europe/Mediterranean** (with the exception of **Turkey** and **Yugoslavia**) were found to have a much closer language and religion association with the U.S.

CULTURAL FACTORS: LANGUAGE AND RELIGION

FACTORS	A	B	C	D
LANGUAGE	ENGLISH	SPANISH/FRENCH *	ARABIC	ALL OTHERS
RELIGION	CHRISTIAN	CHRISTIAN ORTHODOX	EASTERN/ TRIBAL/ISLAM	ISLAM
NUMBER OF EXPEDITIONARY ENVIRONMENT COUNTRIES	6	22	30	7

* ALSO INCLUDES GREEK, ITALIAN, DUTCH, PORTUGUESE, DANISH, NORWEGIAN, AND TURKISH

CULTURAL FACTORS: LANGUAGE AND RELIGION

	A	B	C	D
WESTERN HEMISPHERE	GRENADA JAMAICA	COLOMBIA COSTA RICA CUBA DOMINICAN REPUBLIC EL SALVADOR GUATEMALA HAITI HONDURAS MEXICO NICARAGUA PANAMA PERU SURINAM VENEZUELA		
MIDDLE EAST/ SOUTHWEST ASIA			BAHRAIN EGYPT IRAQ KUWAIT LEBANON LIBYA NORTH YEMEN OMAN QATAR SAUDI ARABIA SOUTH YEMEN SYRIA UAE	IRAN
AFRICA	SOUTH AFRICA UGANDA	ANGOLA LIBERIA ZAIRE ZIMBABWE	ALGERIA DJIBOUTI KENYA MADAGASCAR NAMIBIA SUDAN TUNISIA	ETHIOPIA SOMALIA
ASIA/PACIFIC	PAPUA NEW GUINEA SOUTH PACIFIC ISLANDS		BURMA CHINA INDIA JAPAN MALAYSIA NORTH KOREA PHILIPPINES SOUTH KOREA SRI LANKA THAILAND VIETNAM	AFGHANISTAN BANGLADESH INDONESIA PAKISTAN
EUROPE/MED		DENMARK GREECE ITALY NORWAY	TURKEY YUGOSLAVIA	

PLANNING AND PROGRAMMING IMPLICATIONS

Language and religion are two major elements of the "cultural" terrain within which the MAGTFs must conduct stability operations and limited objective operations. Both require intense interaction with the civilian populace during the operation. The good news is that a MAGTF with strong Spanish and French language skills can operate in 79% of the countries studied, as English, Spanish, or French are established as second languages. Arabic, however, remains a weak point, and is required in fully 30% of the countries of concern. Along with Arabic, an understanding of Islam is critical in 36% of the countries.

Intelligence specialists are not the only ones who need language skills. Low intensity operations require many more Marines in occupational specialties as wide-ranging as military police, engineers, and public affairs to be in language designated billets.

The lack of an active duty PSYOP and Civil Affairs capability may pose a dilemma to MAGTFs needing no-notice support but lacking the authority to mobilize reservists. Religion is an important environmental feature. One product that could be developed by the reserves for contingency use would be a series of distinct Codes of Conduct corresponding to each major religion and related ethnic or racial group likely to be encountered by the MAGTF. Such a series should be no more than one page in length per category, and suitable for issuance to the individual Marine.

CRITICAL WEATHER FACTORS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →					
	A	B	C	D	E	F
Weather	Dry/Warm	Wet/Warm	Mixed	Dry/Hot	Wet/Hot	Wet/Cold

F - • Precipitation of 70 inches or more annually
• Temperature of 40 degrees Fahrenheit or below for extended periods

E - • Precipitation of 70 inches or more annually
• Heat index (combined relative humidity and air temperature) of 80 or above for extended periods

D - • Precipitation of 12 inches or less annually
• Heat index of 80 or above for extended periods

C - • Precipitation between 12 and 70 inches annually
• Wide variations in temperature and rainfall throughout a country

B - • Precipitation of 70 inches or more annually
• Temperatures ranging between 40 degrees Fahrenheit and a heat index of 80

A - • Precipitation of 12 inches or less annually
• Temperatures ranging between 40 degrees Fahrenheit and a heat index of 80

Volume II, Study Supporting Material, Section 18, Critical Weather Factors provides tables which show average temperatures, average relative humidity, and average rainfall by country, as well as a rating of overall weather conditions for each country. The references used as source material for this assessment are as follows:

(1) The Weather Almanac, Gale Research Company, 1981
(2) The Weather Handbook, A Summary of Weather Statistics for Selected Cities Throughout the United States and Around the World, Conway Research, Inc, 1974
(3) The New Book of World Rankings, Facts on File, Inc., 1984
(4) World Facts and Figures, John Wiley and Sons, 1989
(5) Worldmark Encyclopedia of Nations, 1984
(6) World Climate Data, Climatic Data Press, 1972

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows the weather conditions associated with the various regions of the world. For operations in **Latin America** and the **Caribbean**, military forces should be prepared for wet and hot conditions, while in the **Middle East** and **Southwest Asia** dry and hot conditions prevail.

Africa presents a variety of conditions including some of the most challenging. **Asia** and the **Pacific** are primarily wet and hot or to a lesser extent mixed, while **Europe** has the most difficult conditions in **Norway**, followed by mixed or variable situations elsewhere.

Within the expeditionary environment, only one country, **Norway**, had wet and cold conditions which are the most difficult to operate in. There were 33%, or 23 of 69 countries with the next most difficult conditions, wet and hot. Countries such as **Colombia, Panama, Liberia**, and the **Philippines** fall within this category.

The next level of difficulty is dry and hot conditions with 24%, or 16 of 69 countries in the expeditionary environment. Countries such as **Libya** and **Angola** are in this grouping. This is followed by countries with mixed or highly variable conditions. Here there are 33% of the total, or 23 countries, including **Cuba** and **Iran**.

The last two types of weather conditions representing the least operational difficulty are wet/warm with 1% and dry/warm with 8%. Examples of countries with these conditions are **Syria** and **South Africa**.

CRITICAL WEATHER FACTORS

	DRY/WARM	WET/WARM	MIXED	DRY/HOT	WET/HOT	WET/COLD
WESTERN HEMISPHERE	PERU		CUBA DOM. REP. GUATEMALA HAITI MEXICO VENEZUELA		COLOMBIA COSTA RICA EL SALVADOR GRENADA HONDURAS JAMAICA NICARAGUA PANAMA SURINAM	
MIDDLE EAST/ SOUTHWEST ASIA	IRAN SYRIA		LEBANON	BAHRAIN EGYPT IRAQ KUWAIT LIBYA NORTH YEMEN OMAN QATAR SAUDI ARABIA SOUTH YEMEN UAE		
AFRICA	NAMIBIA SOUTH AFRICA		ALGERIA ETHIOPIA KENYA TUNISIA UGANDA ZIMBABWE	ANGOLA DJIBOUTI SOMALIA SUDAN	LIBERIA MADAGASCAR ZAIRE	
ASIA/ PACIFIC		JAPAN	AFGHANISTAN INDIA NORTH KOREA PRC SOUTH KOREA	PAKISTAN	BANGLADESH BURMA INDONESIA MALAYSIA PAPUA N. G. PHILIPPINES S. PACIFIC IS. SPRATLY IS. SRI LANKA THAILAND VIETNAM	
EUROPE/ MED			DENMARK GREECE ITALY TURKEY YUGOSLAVIA			NORWAY

PLANNING AND PROGRAMMING IMPLICATIONS

As indicated by the above figures, the weather in the expeditionary environment is uniformly hot. This suggests that evaluation standards for vertical lift and other systems should be based on "hot" as the norm rather than as the "extreme" condition. **Norway**, and its cold weather conditions is unique among the countries. The cost to the Marine Corps and its MAGTFs in maintaining a cold weather capability for this single contingency may merit review.

GENERAL GEOGRAPHIC CONDITIONS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →			
Gen Geographic Conditions	Urban	Desert	Jungle	Mountainous

The most difficult geographic conditions were mountains, followed by jungle, desert, and urban centers. The predominate condition in each country was determined through a review of the reference material. A country was classifed as "urban" if 70 percent or more of its population were living in urban areas. References used for this assessment included:

(1) Countries of the World and Their Leaders Yearbook, 1989, Gale Research Inc.
(2) The World Almanac and Book of Facts, 1989, Published by Pharos Books, a Scripps Howard Company
(3) The World Factbook, 1988. Directorate of Intelligence, Central Intelligence Agency

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts show a breakdown of country general geographic conditions by regional distribution. In the **Western Hemisphere**, over half the countries have primarily mountainous conditions. Countries such as **Colombia**, **El Salvador**, and **Panama** fall into this most difficult category. Three countries in the region, **Costa Rica**, **Nicaragua**, and **Surinam**, have predominately jungle conditions which are the next most difficult after mountains.

In the **Middle East/Southwest Asia**, almost 60 percent of the countries have desert conditions. These include **Egypt**, **Kuwait**, and **Saudi Arabia**. In this region, **Iran**, **North Yemen**, and **Oman** can be characterized as mountainous. **Bahrain**, **Iraq**, and **Lebanon** have 70 percent or more of their populations living in urban centers.

GENERAL GEOGRAPHIC CONDITIONS REGIONAL DISTRIBUTION

	URBAN	DESERT	JUNGLE	MOUNTAINOUS
WESTERN HEMISPHERE	CUBA		COSTA RICA	COLOMBIA
	MEXICO		NICARAGUA	DOM. REP.
	PERU		SURINAM	EL SALVADOR
	VENEZUELA			GRENADA
				GUATEMALA
				HAITI
				HONDURAS
				JAMAICA
				PANAMA
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN	EGYPT		IRAN
	IRAQ	KUWAIT		NORTH YEMEN
	LEBANON	LIBYA		OMAN
		QATAR		
		SAUDI ARABIA		
		SOUTH YEMEN		
		SYRIA		
		UAE		

Africa was found to have a range of conditions. Eight countries such as **Algeria**, **Somalia**, and **Tunisia** have desert conditions, three have jungle (**Liberia**, **Uganda**, and **Zaire**), and four have mountains (**Ethiopia**, **Madagascar**, **South Africa**, and **Zimbabwe**) as their primary features.

In **Asia/Pacific**, just under half the countries had mainly jungle conditions. Representative countries in this category were **Burma**, **Indonesia**, and **Malaysia**. Mountainous conditions prevailed in almost 40 percent of the countries in this region. Countries such as **Afghanistan**, **North Korea**, **South Korea**, and the **People's Republic of China** were in this caregory.

In **Europe/Mediterranean**, **Greece**, **Norway**, **Turkey**, and **Yugoslavia** presented mountainous conditions while Denmark and Italy had mainly urban populations.

GENERAL GEOGRAPHIC CONDITIONS REGIONAL DISTRIBUTION

	URBAN	DESERT	JUNGLE	MOUNTAINOUS
AFRICA		ALGERIA	LIBERIA	ETHIOPIA
		ANGOLA	UGANDA	MADAGASCAR
		DJIBOUTI	ZAIRE	SOUTH AFRICA
		KENYA		ZIMBABWE
		NAMIBIA		
		SOMALIA		
		SUDAN		
		TUNISIA		
ASIA/ PACIFIC	INDIA	PAKISTAN	BANGLADESH	AFGHANISTAN
	JAPAN		BURMA	NORTH KOREA
			INDONESIA	PAPUA N. G.
			MALAYSIA	PHILIPPINES
			SPRATLY IS	PRC
			SRI LANKA	SOUTH KOREA
			THAILAND	S. PACIFIC IS.
			VIETNAM	
EUROPE/ MED	DENMARK			GREECE
	ITALY			NORWAY
				TURKEY
				YUGOSLAVIA

PLANNING AND PROGRAMMING IMPLICATIONS

The four types of terrain appear with sufficient frequency to require the development of full combined arms capabilities for each: mountains, jungles, deserts, and urban environments. Scenarios corresponding to each of these different environments would be helpful in developing Required Operational Capabilities (ROC).

OPERATIONAL ELEVATION

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →					
	A	B	C	D	E	F
OP Elevation	<2000 Ft	<4000 Ft	<6000 Ft	>6000 Ft	>9000 Ft	>12,000 Ft

F - Elevations greater than 12,000 feet

E - Elevations from 9,001 feet to 12,000 feet

D - Elevations from 6,001 feet to 9,000 feet

C - Elevations from 4,000 feet to 6,000 feet

B - Elevations from 2,000 feet to 3,999 feet

A - Elevations from sea level to 1,999 feet

NOTE: In the process of grading each expeditionary environment country, averages were taken of elevations adjacent to coastal areas, capital cities, key installations, important lines of communications, and other areas where Marines would be likely to operate. Data was obtained from reference material, including atlases, encyclopedias, and almanacs.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrices show the regional distribution of countries by operational elevation. In the Western **Hemisphere**, half the countries had operational elevations between 2,000 and 4,000 feet. The mountainous country of **Peru** was found to have the highest elevations.

In the **Middle East/Southwest Asia**, almost 80 percent of the countries were grouped in the elevation categories of less than 4,000 feet and less than 2,000 feet. **North Yemen, Iran,** and **Saudi Arabia** had the highest elevations

REGIONAL DISTRIBUTION OF COUNTRIES BY OPERATIONAL ELEVATION

	< 2,000 FT	< 4,000 FT	< 6,000 FT	> 6,000 FT	> 9,000 FT	> 12,000 FT
WESTERN HEMISPHERE	CUBA	COSTA RICA	GUATEMALA	COLOMBIA	PERU	
	GRENADA	DOM. REP	NICARAGUA	MEXICO		
	SURINAM	EL SALVADOR				
		HAITI				
		HONDURAS				
		JAMAICA				
		PANAMA				
		VENEZUELA				
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN	IRAQ	IRAN	NORTH YEMEN		
	EGYPT	LEBANON	SAUDI ARABIA			
	KUWAIT	OMAN				
	LIBYA	SOUTH YEMEN				
	QATAR	SYRIA				
	UAE					

In **Africa**, the operational elevations ranged between 2,000 and 9,000 feet for all countries.

Operational elevations in the countries of **Asia/Pacific** ranged across most of the categories with **Papua New Guinea** presenting the most difficult conditions.

In **Europe/Mediterranean, Denmark** had the lowest elevations while **Greece, Norway, Turkey,** and Yugoslavia had the highest.

REGIONAL DISTRIBUTION OF COUNTRIES BY OPERATIONAL ELEVATION

	< 2,000 FT	< 4,000 FT	< 6,000 FT	> 6,000 FT	> 9,000 FT	> 12,000 FT
AFRICA		LIBERIA	ALGERIA	ANGOLA		
		NAMIBIA	DJIBOUTI	ETHIOPIA		
		TUNISIA	SOMALIA	KENYA		
		ZAIRE	SOUTH AFRICA	MADAGASCAR		
			SUDAN			
			UGANDA			
			ZIMBABWE			
ASIA/ PACIFIC	BANGLADESH	INDIA	JAPAN	AFGHANISTAN	PAPUA N. G.	
	BURMA	INDONESIA	PAKISTAN	MALAYSIA		
	SPRATLY IS.	PRC	PHILIPPINES	NORTH KOREA		
	SRI LANKA	S. PACIFIC IS.	SOUTH KOREA			
	THAILAND					
	VIETNAM					
EUROPE/ MED	DENMARK		ITALY	GREECE		
				NORWAY		
				TURKEY		
				YUGOSLAVIA		

The two expeditionary environment countries with the highest elevations are described as follows:

(1) **Papua New Guinea** contains a complex system of mountains extending from the eastern end of the main island to the western boundary with **Indonesia**. Precipitous slopes, knife-sharp ridges, great outcroppings of mountains to heights of almost 15,000 feet, and broad upland valleys at altitudes of 5,000 to 10,000 feet characterize this area.

(2) In **Peru**, the Andes Mountains occupy nearly 27 percent of the land area and represent a formidable natural barrier to transportation and communications between the coast and the interior. The highest mountain, Huascaran, is 22,071 feet above sea level.

PLANNING AND PROGRAMMING IMPLICATIONS

In preparing for all types of conflict situations, the elevations where Marines will be operating should be a foremost consideration. Particularly in helicopter operations, weather conditions, as well as elevation, must be carefully assessed. The vertical lift of Marines, together with their equipment and supplies, over varied terrain to inland locations is a fundamental requirement for most operations and must receive the careful attention of planners in order to be successfully executed.

CROSS - COUNTRY MOBILITY

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY		
	A	B	C
Cross-Country Mobility	Generally Suited	Partially Suited	Generally Unsuited

C - Large portions of a country are unsuitable for cross-country movement of tracked vehicles due to broken terrain, extensive ground cover, marshes, swamps, and/or significant bodies of water. In those countries where the coastal region prevents tracked movement from the beach to the interior, the entire country is categorized as unsuited for tracked movement.

B - Significant parts of a country are suitable for cross-country movement of tracked vehicles. For example, the **Central Luzon** plain of the **Philippines** is trafficable, while most other parts of the country are mountainous and unsuited for tracked movement.

A - Large parts of a country can accommodate the cross-country movement of tracked vehicles. **Algeria**, for example, is primarily desert and suitable for both wheeled and tracked cross-country movement.

Note: Trafficability in this assessment reflects the suitability for cross-country tracked vehicle movement. The factor did not address lines of communications, and existing road, rail, and canal networks. The emphasis was on true cross-country movement.

The analytical judgments in this assessment are based on a review of each country's National Intelligence Survey or its follow-on Army Country Profile and were developed by the USMC Intelligence Center staff.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts illustrate the regional distribution of expeditionary environment countries by suitability for cross-country mobility. Over 60 percent of the countries are generally unsuited for this movement and an additional 20 percent are only partially suited.

In the **Western Hemisphere**, almost 60 percent of the countries were found to be generally unsuited for cross-country movement by tracked vehicles. Countries such as **Colombia, El Salvador, Guatemala**, and Peru have extensive mountain ranges while **Costa Rica, Nicaragua** and **Surnam** have dense tropical forests that preclude vehicular movement. Only in **Cuba, Mexico**, and **Venezuela**, and to a lesser extent **Grenada** can movement be generally accommodated.

GENERAL TRAFFICABILITY/CROSS-COUNTRY MOBILITY

	GENERALLY SUITED	PARTIALLY SUITED	GENERALLY UNSUITED
WESTERN HEMISPHERE	CUBA MEXICO VENEZUELA	GRENADA	COLOMBIA COSTA RICA DOMINCAN REPUBLIC EL SALVADOR GUATEMALA HAITI HONDURAS JAMAICA NICARAGUA PANAMA PERU SURINAM

In the **Middle East/Southwest Asia**, over 40 percent of the countries are generally unsuited for tracked movement. **Iran**, for example, has rugged hills and mountains, and smaller areas of wetlands covering about two-thirds of its area. However, about 60 percent of this region is generally, or at least partially, suited for movement by tracked vehicles. **Egypt** and **Libya** in particular have desert plains which facilitate movement.

Africa was the region with the most countries which could readily accommodate tracked vehicles. Exactly 40 percent of the countries, including **Algeria, Ethiopia,** and **Somalia,** were generally suited for tracked movement while an additional 13 percent (**Madagascar** and **Uganda**) were partially suited. The remaining 47 percent of the countries, including **Angola, South Africa,** and **Sudan,** were generally unsuited due to conditions ranging from forest areas to coastal mountains.

In the **Asia/Pacific** region trafficability presents a serious problem with 13 of 18 countries or 72 percent generally unsuited for tracked movement. The primary impediments to trafficability are dense tropical jungles, numerous wetlands such as swamps and marshes, and periodic heavy rainfall. Only **India** was generally suited and **Afghanistan, Pakistan, the Philippines,** and **South Korea** partially suited for tracked movement in this region.

Of the six **European/Mediterranean** countries considered, four were generally unsuited and two were partially suited for tracked movement. The significant mountain ranges in countries such as **Greece, Turkey,** and **Yugoslavia** were a principal limiting factor in this region.

GENERAL TRAFFICABILITY/CROSS-COUNTRY MOBILITY

	GENERALLY SUITED	PARTIALLY SUITED	GENERALLY UNSUITED
MIDDLE EAST/ SOUTHWEST ASIA	EGYPT LIBYA	BAHRAIN KUWAIT LEBANON QATAR SYRIA UAE	IRAN IRAQ NORTH YEMEN OMAN SAUDI ARABIA SOUTH YEMEN
AFRICA	ALGERIA DJIBOUTI ETHIOPIA KENYA SOMALIA TUNISIA	MADAGASCAR UGANDA	ANGOLA LIBERIA NAMIBIA SOUTH AFRICA SUDAN ZAIRE ZIMBABWE
ASIA/PACIFIC	INDIA	AFGHANISTAN PAKISTAN PHILIPPINES SOUTH KOREA	BANGLADESH BURMA INDONESIA JAPAN MALAYSIA NORTH KOREA PAPUA NEW GUINEA PRC SOUTH PACIFIC IS SPRATLY IS SRI LANKA THAILAND VIETNAM
EUROPE/MED		ITALY TURKEY	DENMARK GREECE NORWAY YUGOSLAVIA

PLANNING AND PROGRAMMING IMPLICATIONS

Marine Corps capabilities which are totally dependent on vehicular transport may need to be reevaluated. It merits comment that a premise which led to these generalizations was that if the coastal region of a country was unsuited, the entire country was assumed to be unsuited because heavy vehicles could not get from their offshore launch point to inland objectives. Maritime Prepositioning Ships (MPS) and strategic airlift deployment alternatives were not considered.

INTERVISIBILITY: AVERAGE LINE OF SIGHT DISTANCE

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →		
	OPTIMUM	RESTRICTED	POOR
Intervisibility (Line Of Sight)	>2,000 Meters	1,000 - 2,000 Meters	<1,000 Meters

POOR - Average Line Of Sight (LOS) distance is less than 1,000 meters

RESTRICTED - Average LOS distance is between 1,000 and 2,000 meters

OPTIMUM - Average LOS distance is between 2,000 and 3,000 meters.

Intervisibility is defined as the LOS distance that direct-fire weapons (armor and antiarmor) of the ground combat element can fire without restrictions to visibility and weapons effectiveness in each of the expeditionary environment countries. The firepower of armor and antiarmor weapons is highly dependent on the terrain. Long-range, flat-trajectory weapons cannot effectively utilize their range in cities, forests, industrial areas, and mountainous regions. In covered and broken terrain, armored forces can employ only a fraction of their firepower and light infantry forces have the advantage. Darkness, poor weather conditions, and obscurants on the battlefield will also have a limiting effect on long-range, direct-fire weapons. The more open the terrain and visibility becomes, the better these weapons can realize their full potential.

After a close examination of the source material in relation to the above criteria, each of the expeditionary environment countries was rated according to its intervisibility. Volume II, Study Supporting Material, Section 22, Intervisibility: Average Line of Sight Distance contains an assessment of the conditions within each country on which the ratings were based. The references used as source material for the assessment are as follows:

(1) Battlefield Central Europe, Danger of Overreliance on Technology by the Armed Forces, Brigadier General Franz Uhle-Wettler, undated.
(2) Zones of Conflict: An Atlas of Future Wars, John Keegan and Andrew Wheatcroft, 1986.
(3) A Quick & Dirty Guide to War, James E. Dunnigan and Austin Bay, 1986.
(4) Atlas of the Third World, George Kurian, 1983.
(5) Hamond World Atlas, 1984, Hammond Inc.
(6) Countries of the World and Their Leaders Yearbook 1989, Gale Research, Inc.
(7) Worldmark Encyclopedia of the Nations, 1984, Worldmark Press Inc.
(8) USMC Intelligence Center document titled Trafficability Narrative.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying matrix shows the regional distribution of countries according to their degree of intervisibility. In the **Western Hemisphere**, over 80 percent of the countries have poor intervisibility where armor and antiarmor weapons cannot be fully employed. Only **Cuba, Mexico,** and **Venezuela** could accommodate better line of sight ranges.

In the **Middle East/Southwest Asia**, more than half the countries had poor intervisibility. The exceptions here were the flat and barren countries of **Egypt, Kuwait, Qatar,** and the **United Arab Emirates**, and to a lesser extent **Iraq** and **Libya** which had better line of sight distances.

In **Africa**, 60 percent of the countries had average line of sight distances less than 1,000 meters. **Kenya** and **Tunisia** could accommodate intervisibility between 1,000 and 2,000 meters while **Algeria, Djibouti, Ethiopia,** and **Somalia** could exceed 2,000 meters.

The great majority of countries in **Asia/Pacific** and **Europe/Mediterranean** fall into the category of poor intervisibility. In the middle category on the matrix, with average line of sight ranges between 1,000 and 2,000 meters were found the **Asian** countries of **India** and **Pakistan** and the **European** country of **Denmark.**

REGIONAL DISTRIBUTION OF COUNTRIES BY INTERVISIBILITY

	> 2,000 METERS	1,000 - 2,000 METERS	< 1,000 METERS
WESTERN HEMISPHERE		CUBA	COLOMBIA
		MEXICO	COSTA RICA
		VENEZUELA	EL SALVADOR
			GRENADA
			GUATEMALA
			HAITI
			HONDURAS
			JAMAICA
			NICARAGUA
			PANAMA
			PERU
			SURINAM
			DOM REP
MIDDLE EAST/ SOUTHWEST ASIA	EGYPT	IRAQ	BAHRAIN
	KUWAIT	LIBYA	IRAN
	QATAR		LEBANON
	UAE		NORTH YEMEN
			OMAN
			SAUDI ARABIA
			SOUTH YEMEN
			SYRIA
AFRICA	ALGERIA	KENYA	ANGOLA
	DJIBOUTI	TUNISIA	LIBERIA
	ETHIOPIA		MADAGASCAR
	SOMALIA		NAMIBIA
			SOUTH AFRICA
			SUDAN
			UGANDA
			ZAIRE
			ZIMBABWE
ASIA/ PACIFIC		INDIA	AFGHANISTAN
		PAKISTAN	BANGLADESH
			BURMA
			INDONESIA
			JAPAN
			MALAYSIA
			NORTH KOREA
			PAPUA N. G.
			PHILIPPINES
			PRC
			SOUTH KOREA
			S. PACIFIC IS.
			SRI LANKA
			THAILAND
			VIETNAM
EUROPE/ NATO		DENMARK	GREECE
			ITALY
			NORWAY
			TURKEY
			YUGOSLAVIA

PLANNING AND PROGRAMMING IMPLICATIONS

An overall assessment of intervisibility in the expeditionary environment indicates that almost three quarters of the countries have average line of sight distances less than 1,000 meters. It was determined that on an average, the engagement range for armor and antiarmor weapons was about 900 meters. This means that most of the countries in the expeditionary environment have terrain, vegetation, and/or other conditions of obscuration which would preclude engagements by these weapons at their maximum ranges. As a result, it may not be cost effective to acquire and maintain a sizeable number of these weapons in the Marine Corps inventory if they cannot be fully utilized. Light infantry forces with a minimum of armor and heavy equipment would appear to be better able to operate in the restricted terrain and visibility conditions that were identified in this assessment. Marine planners must continually evaluate the tradeoffs between forces and weapon systems to select those that can be employed most effectively in the anticipated environment.

HYDROGRAPHY - NAVAL GUNFIRE CONSTRAINTS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →			
Hydrography - NGF Constraints	Good	Fair	Poor	Unsatisfactory

UNSATISFACTORY: Distance of the 5 Fathom Line from the coast is greater than 24,000 meters

POOR: Distance of the 5 Fathom Line from the coast is between 16,001 and 24,000 meters

FAIR: Distance of the 5 Fathom Line from the coast is between 8,001 and 16,000 meters

GOOD: Distance of the 5 Fathom Line from the coast is 8,000 meters or less

This assessment addresses NGF capabilities and the constraints imposed by hydrographic conditions off the coasts of expeditionary environment countries. For purposes of this evaluation, a U.S. Navy destroyer with an 8.8 meter (29 foot) draft and 5-inch 54-caliber guns was chosen as the representative NGF platform. To determine coastal hydrographic conditions, the Defense Mapping Agency's hydrographic charts were examined to identify the closest distance a destroyer could operate offshore of the countries of interest. Because the water depths and conditions along extended coastlines frequently have significant variations, key locations (adjacent to ports, cities, or key lines of communications inland) where an ATF would be likely to operate were selected, and a reading taken of the average distance of the 5 Fathom Line from the coast. (Distances were calculated only to the beach, not to inland targets.) Distances were then compared with the 24,000 meter maximum range of the destroyer's guns and a NGF rating based on the above scale was assigned to each country. Volume II, Study Supporting Material, Section 23, Hydrography - Naval Gunfire Constraints provides a listing of country key locations selected for a reading of the 5 Fathom Line, DMA chart numbers of charts used, the assessed distance of the 5 Fathom Line from the coast, and the overall country ratings. The primary reference used for this assessment was the Department of Defense, Defense Mapping Agency, Catalog of Maps, Charts, and Related Products, Part 2 - Hydrographic Products

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts show a regional breakdown of NGF capabilities affected by hydrography. In the Western Hemisphere, most of the countries have conditions favorable to NGF coverage. Only Surinam had unsatisfactory conditions which would prevent the use of NGF.

NAVAL GUNFIRE CAPABILITIES BY REGION

	GOOD	FAIR	POOR	UNSATISFACTORY
WESTERN HEMISPHERE	COLOMBIA	HONDURAS		SURINAM
	COSTA RICA			
	CUBA			
	DOM. REP.			
	EL SALVADOR			
	GRENADA			
	GUATEMALA			
	HAITI			
	JAMAICA			
	MEXICO			
	NICARAGUA			
	PANAMA			
	PERU			
	VENEZUELA			

In the **Middle East/Southwest Asia**, NGF can be employed to various degrees of effectiveness in all the countries. **Iraq** and **North Yemen** were found not to have the poorest conditions.

In **Africa**, hydrographic conditions were not identified as limiting NGF employment. Only against the inland countries of **Uganda** and **Zimbabwe** was it found not feasible to use NGF.

In **Asia/Pacific** there was determined to be a range of conditions. Due to the offshore constraints involved, NGF could not be effectively employed in **Bangladesh, Burma, North Korea,** and the **People's Republic of China**, as well as the inland country of **Afghanistan**. In other countries in this region, NGF could be delivered with varying degrees of effectiveness.

In **Europe/Mediterranean** offshore hydrographic conditions were found to permit satisfactory NGF coverage in all of the six countries considered.

NAVAL GUNFIRE CAPABILITIES BY REGION

	GOOD	FAIR	POOR	UNSATISFACTORY
MIDDLE EAST/ SOUTHWEST ASIA	KUWAIT	BAHRAIN	IRAQ	
	LEBANON	EGYPT	NORTH YEMEN	
	OMAN	IRAN		
	SOUTH YEMEN	LIBYA		
	SYRIA	QATAR		
		SAUDI ARABIA		
		UAE		
AFRICA	ALGERIA	KENYA		UGANDA
	ANGOLA	MADAGASCAR		ZIMBABWE
	DJIBOUTI	ZAIRE		
	ETHIOPIA			
	LIBERIA			
	NAMIBIA			
	SOMALIA			
	SOUTH AFRICA			
	SUDAN			
	TUNISIA			
ASIA/ PACIFIC	INDONESIA	INDIA	SOUTH KOREA	AFGHANISTAN
	JAPAN	MALAYSIA		BANGLADESH
	PHILIPPINES	PAKISTAN		BURMA
	S. PACIFIC IS.	PAPUA N. G.		NORTH KOREA
	SRI LANKA			PRC
	THAILAND			
	VIETNAM			
	Note: Hydrographic charts were not available for the Spratly Islands			
EUROPE/ MED	DENMARK			
	GREECE			
	ITALY			
	NORWAY			
	TURKEY			
	YUGOSLAVIA			

PLANNING AND PROGRAMMING IMPLICATIONS

The results of this assessment indicate that good NGF coverage is possible in over half of the expeditionary environment countries if a destroyer approaches to its closest point off the beach. However, to execute an Over-The-Horizon (OTH) amphibious assault where the element of suprise is highly important, it is necessary that the NGF platform operate further out to sea and still cover the priority targets ashore. For this type of operation the 24,000 meter range of the 5-inch, 54-caliber gun is no longer satisfactory. To adequately support OTH operations in the future, Marines must encourage and support Navy actions to acquire an NGF weapon with a range of at least 60 nautical miles.

HYDROGRAPHY - COASTAL THREAT CONSTRAINTS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →		
Hydrography - Coastal Threat Constraints	US NGF Advantage	US NGF and Threat Equal	Threat Advantage

THREAT ADVANTAGE: Maximum range of threat coastal defense weapons exceeds 24,000 meters

US NGF AND THREAT EQUAL: Maximum range of threat coastal defense weapons is 24,000 meters

US NGF ADVANTAGE: Maximum range of threat coastal defense weapons is less than 24,000 meters

This assessment considers U.S NGF capabilities as compared to the effectiveness of threat surface-to-surface weapons when used for coastal defense. For purposes of this evaluation, the representative NGF platform was again a destroyer with 5-inch, 54-caliber guns positioned off the coast of expeditionary environment countries. The maximum range of the 5-inch, 54-caliber gun was considered to be 24,000 meters. The methodology for this assessment involved gathering data on surface-to-surface weapons of the countries of interest and comparing the longest range weapon with that of the U.S. destroyer's 5-inch, 54-caliber gun. The above scale was used to assign a rating or level of difficulty to each country.

Volume II, Study Supporting Material, Section 24, Hydrography - Coastal Threat Constraints contains a listing of each country's maximum capability weapon, each weapon's maximum range, and the country ratings which were assigned. The primary data source used for this assessment was Jane's Weapon Systems, 1987 - 88.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts illustrate a regional breakdown of U.S. NGF versus threat coastal defense capabilities. It was found that the coastal threat may pose a major problem, as 44 percent of the countries considered have at least some capability that exceeds the range of the standard 5-inch gun on most Navy combatants.

In the Western Hemisphere, Cuba, Peru, and Venezuela have a firepower advantage, while Honduras and Nicaragua possess a capability equal to U.S. NGF.

U.S. NGF VERSUS THREAT CAPABILITIES BY REGION

	U.S. NGF ADVANTAGE	U.S. NGF AND THREAT EQUAL	THREAT ADVANTAGE
WESTERN HEMISPHERE	COLOMBIA	HONDURAS	CUBA
	COSTA RICA	NICARAGUA	PERU
	DOM. REP.		VENEZUELA
	EL SALVADOR		
	GRENADA		
	GUATEMALA		
	HAITI		
	JAMAICA		
	MEXICO		
	PANAMA		
	SURINAM		

In the **Middle East/Southwest Asia**, over two-thirds of the countries have a firepower advantage over U.S. NGF. It is particularly noteworthy that unstable countries such as **Iran, Iraq,** and **Libya** fall into this category.

In **Africa**, almost half the countries, including **Algeria, Angola, Somalia,** and **Sudan**, can out-gun the 5-inch, 54-caliber weapon.

In **Asia/Pacific**, seven countries have the advantage in firepower, the most notable of which are **North Korea, the People's Republic of China,** and **Vietnam**. **Thailand** was found to have a capability equal to U.S. NGF.

In **Europe** and the **Mediterranean**, all the countries considered except **Denmark** have the advantage against U.S. NGF.

U.S. NGF VERSUS THREAT CAPABILITIES BY REGION

	U.S. NGF ADVANTAGE	U.S. NGF AND THREAT EQUAL	THREAT ADVANTAGE
MIDDLE EAST/ SOUTHWEST ASIA	NORTH YEMEN	BAHRAIN	EGYPT
	QATAR		IRAN
	UAE		IRAQ
			KUWAIT
			LEBANON
			LIBYA
			OMAN
			SAUDI ARABIA
			SOUTH YEMEN
			SYRIA
AFRICA	DJIBOUTI		ALGERIA
	KENYA		ANGOLA
	LIBERIA		ETHIOPIA
	NAMIBIA		MADAGASCAR
	SOUTH AFRICA		SOMALIA
	TUNISIA		SUDAN
	ZAIRE		
ASIA/ PACIFIC	BANGLADESH	THAILAND	INDIA
	BURMA		JAPAN
	INDONESIA		NORTH KOREA
	MALAYSIA		PAKISTAN
	PAPUA N. G.		PRC
	PHILIPPINES		SOUTH KOREA
	S. PACIFIC IS.		VIETNAM
	SPRATLY IS.		
	SRI LANKA		
EUROPE/ MED	DENMARK		GREECE
			ITALY
			NORWAY
			TURKEY
			YUGOSLAVIA

PLANNING AND PROGRAMMING IMPLICATIONS

This asessment has found that many of the expeditionary environment countries have acquired surface-to-surface weapons which, when employed in a coastal defense role, would give them the advantage over the standard U.S. NGF capabilities. The 24,000-meter range of the 5-inch, 54-caliber gun is inadequate to provide the necessary support for amphibious or limited objective operations. To effectively supress enemy coastal defenses and engage inland targets from an Over-The-Horizon (OTH) location a more capable NGF weapon is needed. Marines must encourage and support Navy actions to obtain an enhanced NGF capability that will support expeditionary operations at a range of 60 nautical miles or more.

MAPPING, CHARTING, AND GEODESY SHORTFALLS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →					
	A	B	C	D	E	F
MC&G Coverage	1:50 New	1:50 Old	Some 1:50	MSI Avail	1:250 New	None

F - Countries with no coverage by 1:50,000 or 1:250,000 scale maps or Multispectral Imagery (MSI)

E - Countries with complete coverage by 1:250,000 scale maps (either series 1501 (ground) or 1501A (air)) and map editions all have been produced since 1980. No 1:50,000 scale map coverage or MSI are available.

D - Countries which have current and complete MSI available, but no 1:50,000 scale map coverage

C - Countries with partial coverage by either current or dated 1:50,000 scale maps

B - Countries with complete coverage by 1:50,000 scale maps, most editions of which were produced prior to 1980

A - Countries with complete coverage by 1:50,000 scale maps and all map editions were produced since 1980

Using the above criteria, expeditionary environment countries were classified into the six categories (A through F through research of the data sources. These sources consisted of the following.

(1) Department of Defense, Defense Mapping Agency, Catalog of Maps, Charts, and Related Products.
(2) Telephone conversations with the Earth Observation Satellite Company, Subject: MSI Support for DMA.
(3) Commanding General, Marine Corps Combat Development Command letter 3140 IN 06 dated June 1, 1989, Subject: Marine Corps Concerns--Mapping, Charting, and Geodesy Documents.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts show the distribution of Mapping, Charting, and Geodesy (MC&G) coverage by region. Because there was no countries identified with items E (1:250 New) and F (None) at the upper end of the level of difficulty scale, these items were not addressed further in this assessment.

In the **Western Hemisphere**, only four countries had full coverage by the older 1:50,000 scale maps. These were **Cuba, Dominican Republic, Haiti and Jamaica.** Over 50 percent of the countries had partial coverage with 1:50,000 maps while **Grenada, Mexico, and Surinam** had the less effective MSI available.

DISTRIBUTION OF COUNTRIES BY MC&G COVERAGE

	1:50 NEW	1:50 OLD	SOME 1:50	MSI AVAIL
WESTERN HEMISPHERE		CUBA DOM. REP. HAITI JAMAICA	COLOMBIA COSTA RICA EL SALVADOR GUATEMALA HONDURAS NICARAGUA PANAMA PERU VENEZUELA	GRENADA MEXICO SURINAM

In the **Middle East/Southwest Asia** most of the countries had some 1:50,000 scale map coverage. Only **Bahrain** had full coverage with dated 1:50,000 maps, and **Kuwait** and **North Yemen** had just the MSI available.

In **Africa**, there were no countries with full 1:50,000 scale map coverage. Countries in this region were about equally divided between those with partial coverage by 1:50,000 scale maps and those with MSI. Countries such as **Algeria, Liberia, South Africa**, and **Zimbabwe** had partial 1:50,000 map coverage. Representative countries with only MSI were **Angola, Namibia, Sudan**, and **Uganda**.

In the **Asia/Pacific** region there were only two countries, **North Korea** and **South Korea**, with full coverage by dated 1:50,000 scale maps. The remaining countries were equally divided between the partial 1:50 and the MSI available categories. Nations such as **Afghanistan, Pakistan**, and **Thailand** had the partial 1:50 while **Burma, India**, and **Malaysia** were representative of the MSI available category.

In **Europe** and the **Mediterranean**, the countries of **Greece** and **Turkey** presented the most difficult conditions with only MSI available. **Italy** has partial 1:50 coverage while **Denmark, Norway** and **Yugoslavia** had full coverage with the dated 1:50's.

DISTRIBUTION OF COUNTRIES BY MC&G COVERAGE

	1:50 NEW	1:50 OLD	SOME 1:50	MSI AVAIL
MIDDLE EAST/ SOUTHWEST ASIA		BAHRAIN	EGYPT IRAN IRAQ LEBANON LIBYA OMAN QATAR SAUDI ARABIA SOUTH YEMEN SYRIA UAE	KUWAIT NORTH YEMEN
AFRICA			ALGERIA DJIBOUTI ETHIOPIA LIBERIA SOUTH AFRICA TUNISIA ZAIRE ZIMBABWE	ANGOLA KENYA MADAGASCAR NAMIBIA SOMALIA SUDAN UGANDA
ASIA/PACIFIC		NORTH KOREA SOUTH KOREA	AFGHANISTAN INDONESIA JAPAN PAKISTAN PHILIPPINES PRC THAILAND VIETNAM	BANGLADESH BURMA INDIA MALAYSIA PAPUA N. G. S. PACIFIC IS. SPRATLY IS. SRI LANKA
EUROPE/MED		DENMARK NORWAY YUGOSLAVIA	ITALY	GREECE TURKEY

PLANNING AND PROGRAMMING IMPLICATIONS

This assessment has indicated that there are significant shortfalls in MC&G coverage of expeditionary environment countries. Over 85 percent of the countries have only partial 1:50,000 scale map coverage or MSI. As a result of this situation, MAGTF's employed in many of these countries will not have the maps required to conduct effective ground and air operations. To overcome this deficiency, actions must be taken to ensure that the Defense Mapping Agency directs its available resources toward an aggressive large-scale mapping program of Third World countries to support the range of operations across the spectrum of conflict.

AIRFIELDS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY					
	A	B	C	D	E	F
Airfields	>1/C-5	1/C-5	>5/C-130	2-4/C-130	1/C-130	None

F - Countries with no airfields that are capable of receiving C-130 or larger transport aircraft

E - Countries with only one airfield that can accommodate C-130 or C-141B aircraft. There are no airfields that can receive C-5 aircraft.

D - Countries with two to four airfields that can accommodate C-130 or C-141B aircraft. There are no airfields that can receive C-5 aircraft.

C - Countries with five or more airfields that can accommodate C-130 or C-141B aircraft. There are no airfields that can receive C-5 aircraft.

B - Countries with only one airfield that can receive C-5 aircraft. These countries may have additional airfields that can handle C-141B and C-130 aircraft.

A - Countries with more than one airfield that can receive C-5 aircraft. These countries may also have airfields that can handle only C-141B and C-130 aircraft.

Using the above criteria, in conjunction with a thorough review of source material, the expeditionary environment countries were classified into the six levels of difficulty (A to F). The purpose in this instance was to show the degree of access that a military force might have to a country through its airfields. Volume II, Study Supporting Material Section 26, Airfields contains a listing of the primary airfields in each country, a brief discription of each airfield, and the overall country rating assigned. The principal reference used for source material was the Military Airlift Command, Code DOVF, Airfield Suitability Report, dated August 1, 1989.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows a breakdown of countries by their capability to receive strategic airlift. Overall, nearly 80 percent of the countries have at least one airfield that can receive C-5s. There are more than one C-5 capable airfields in 50 percent of the countries. Some of the airfields, however, are constrained in such ways as runway condition, ramp space, fuel storage, and other support functions.

In the **Western Hemisphere**, all the countries considered have at least one airfield able to receive C-5 aircraft. Particularly noteworthy are **Colombia** with 3 C-5, 4 C-141B, and 2 C-130 capable airfields, and **Honduras** with 3 C-5 and 7 C-130 capable airfields.

In the **Middle East/Southwest Asia** 10 of 14 countries or over 70 percent of the total, have at least one airfield which will accommodate C-5s. **Saudi Arabia** has 9 C-5 capable airfields while **Iran** has 8 and **Egypt** 6. In this region, **Iraq**, **North Yemen**, and **Qatar** all have the least accessibility to airlift with only one C-141B capable airfield.

Africa has the fewest countries with airfields able to handle large transport aircraft. The six countries of **Algeria**, **Angola**, **Madagascar**, **Tunisia**, **Uganda**, and **Djibouti** are all unable to accommodate C-5s.

In **Asia/Pacific**, 11 of 18 countries have more than one airfield that can receive C-5s and 4 of 18 countries have just one airfield with this capability. Only **Afghanistan** and **Burma** are limited to C-141B capable airfields while no airfields for transport aircraft can be found in the **Spratly Islands**.

In **Europe** and the **Mediterranean**, 5 of 6 countries have more than one C-5 capable airfield. Only **Yugoslavia** has the lesser capability of 4 C-141B capable airfields.

AIRFIELDS

	>1/C-5	1/C-5	>5/C-130	2-4/C-130	1/C-130	NONE
WESTERN HEMISPHERE	COLOMBIA	COSTA RICA				
	DOM. REP.	CUBA				
	GUATEMALA	EL SALVADOR				
	HONDURAS	GRENADA				
	JAMAICA	HAITI				
	MEXICO	NICARAGUA				
	PANAMA	PERU				
	VENEZUELA	SURINAM				
MIDDLE EAST/ SOUTHWEST/ ASIA	EGYPT	BAHRAIN		LIBYA	IRAQ	
	IRAN	KUWAIT			NORTH YEMEN	
	OMAN	LEBANON			QATAR	
	SAUDI ARABIA	SOUTH YEMEN				
	UAE	SYRIA				
AFRICA	ETHIOPIA	LIBERIA	ALGERIA	TUNISIA	DJIBOUTI	
	KENYA	NAMIBIA	ANGOLA	UGANDA		
	SOMALIA	SOUTH AFRICA	MADAGASCAR			
	SUDAN	ZIMBABWE				
	ZAIRE					
ASIA/ PACIFIC	INDIA	BANGLADESH		AFGHANISTAN		SPRATLY IS.
	INDONESIA	PAPUA N. G.		BURMA		
	JAPAN	S. PACIFIC IS.				
	MALAYSIA	SRI LANKA				
	NORTH KOREA					
	PAKISTAN					
	PHILIPPINES					
	PRC					
	SOUTH KOREA					
	THAILAND					
	VIETNAM					
EUROPE/ MED	DENMARK		YUGOSLAVIA			
	GREECE					
	ITALY					
	NORWAY					
	TURKEY					

PLANNING AND PROGRAMMING IMPLICATIONS

The information shown here is designed to illustrate the types of airfields available for planning purposes and provide indicators about where accessibility by strategic airlift may be most difficult. It is noteworthy that strategic airlift (the C-5) surfaced as a very viable option for 79 percent of the countries with tactical airlift (the C-130) opening an additional 21 percent of the countries, if third party nations were available as staging areas. Also, in those cases where direct entry into a country through its airfields is constrained, planners will need to consider access via adjacent countries in conjunction with other tactical means of transport such as helicopter and surface lift.

PORTS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →					
	A	B	C	D	E	F
Ports	Wide Harbor/ >50' Depth	Wide Harbor/ >40' Depth	>40' Depth	35-39' Depth	25-34' Depth	None

F - Countries with no major ports.

E - Countries having at least one major port with a large, medium, or small harbor, and channel and anchorage depths of between 25 and 34 feet.

D - Countries having at least one major port with a large, medium, or small harbor, and channel and anchorage depths of between 35 and 39 feet.

C - Countries having at least one major port with a small harbor, and both channel and anchorage depths exceed 40 feet.

B - Countries having at least one major port with either a large or medium harbor, and both channel and anchorage depths between 40 and 50 feet.

A - Countries having at least one major port with either a large or medium harbor, and both channel and anchorage depths greater than 50 feet.

MAJOR PORT:

- Accommodates vessels over 500 feet in length
- Channel and anchorage depths of 25 feet or more
- Harbor size of large, medium or small

HARBOR SIZE:

- Determined by the DMA World Port Index
- Based on area, facilities and wharf space

Through application of the above criteria to the source material, the countries of interest were classified into the six levels of difficulty (A to F). The purpose here was to show the degree of access that a military force might have to a country through its ports. Volume II, Study Supporting Material, Section 27, Ports contains a listing of the primary ports in each country; identifies the most accessible ports; briefly describes each port; and provides overall level of difficulty country ratings. The following references were used for source material:

(1) Defense Mapping Agency Hydrographic/Topographic Center, World Port Index, Ninth Edition, 1984
(2) Commander in Chief, U.S. Atlantic Fleet and Commanding General, Marine Corps Combat Development Command, TACMEMO PZ005700-1-88, Deployment of the Assault Follow-On Echelon, June 1988

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows a breakdown of countries by their capability to receive strategic sealift. Overall, it was found that 33 of 69 countries or about 48 percent of the total fall into the top three levels of difficulty. There were 10 countries, or 14 percent, which have no acceptable major ports. Such countries as **El Salvador, Somalia, Oman**, and **Bangladesh** were in this most difficult category. A total of 15 countries, or 22 percent of the expeditionary environment were in the second most difficult category where major ports had channel and anchorage depths of only 25 to 34 feet. Representative countries in this category were **Cuba, Nicaragua, Iraq**, and **Libya**. Channel and anchorage depths below 35 feet are highly marginal for the approach and off-load of strategic sealift such as the Maritime Prepositioning Ships (MPS) and other Military Sealift Command (MSC) shipping. MPS ships have drafts up to 33 feet. Certain types of MSC and U.S. Flag Fleet cargo ships have drafts over 40 feet.

From a regional perspective, the **Western Hemisphere** countries had the fewest suitable ports while Europe and the **Mediterranean** had countries with the most capable ports. Other regions had a fairly even distribution across the levels of difficulty.

PORTS

	WIDE/>50'	WIDE/>40'	>40'	35-39'	25-34'	NONE
WESTERN HEMISPHERE			COLOMBIA	JAMAICA	COSTA RICA	EL SALVADOR
			GRENADA	VENEZUELA	CUBA	SURINAM
			MEXICO		DOM. REP.	
			PANAMA		GUATEMALA	
			PERU		HAITI	
					HONDURAS	
					NICARAGUA	
MIDDLE EAST/ SOUTHWEST ASIA	LEBANON		BAHRAIN	QATAR	IRAQ	NORTH YEMEN
	SAUDI ARABIA		EGYPT		LIBYA	OMAN
	UAE		IRAN			
			KUWAIT			
			SOUTH YEMEN			
			SYRIA			
AFRICA	SOUTH AFRICA	ALGERIA	ANGOLA	DJIBOUTI	MADAGASCAR	SOMALIA
			KENYA	ETHIOPIA	NAMIBIA	UGANDA
			LIBERIA	SUDAN	ZAIRE	ZIMBABWE
				TUNISIA		
ASIA/ PACIFIC	JAPAN		INDIA	NORTH KOREA	BURMA	AFGHANISTAN
	SRI LANKA		INDONESIA		PAKISTAN	BANGLADESH
			MALAYSIA		THAILAND	SPRATLY IS.
			PAPUA N. G.			
			PHILIPPINES			
			PRC			
			SOUTH KOREA			
			S. PACIFIC IS.			
			VIETNAM			
EUROPE/ MED	ITALY		DENMARK			
	NORWAY		GREECE			
	YUGOSLAVIA		TURKEY			

PLANNING AND PROGRAMMING IMPLICATIONS

The information shown here is designed to illustrate the types of ports available for planning purposes and provide indicators concerning those countries where accessibility by strategic sealift is most difficult. In the process of rapid mission planning for contingency operations in expeditionary countries, Marine Corps planners must able to examine all avenues of entry, including sea, air, and land and choose the one most effective. Marine Corps wargaming initiatives and other training efforts should be designed to support this process.

KEY INSTALLATIONS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →					
	A	B	C	D	E	F
Key Installations	None	Few Sites	Multi Sites	Pipeline	Oil Field	NBC

F - Countries associated with Nuclear, Biological, and Chemical (NBC) weapon possession and production. These countries have NBC production and storage facilities which could present significant industrial complexity in terms of neutralization.

E - Countries with oil as a significant natural resource. These countries have oil fields, off-shore oil recovery facilities, and supporting industrial capabilities.

D - Countries with numerous industrial complexes together with pipelines for crude oil, refined products, or natural gas.

C - Countries with several basic industrial centers in being or under development and moderately capable transportation and communications systems.

B - Countries having an underdeveloped infrastructure with only a few important facilities such as airfields, ports, and communications sites.

A - No installations of military significance.

Using the above criteria, expeditionary environment countries were classified into the six categories (A through F) through research of the data sources. The purpose here was to show the level of industrial complexity which might be encountered by military forces when operating in a country. Key installations may quickly become priority targets or key objectives when a crisis situation develops. Volume II, Study Supporting Material, Section 28, Key Installations depicts the primary facilities in each country and is the basis for the country ratings assigned. The following references were used for source material:

(1) Foreign Area Studies, The American University, Area Handbook Series, 1979 - 1989
(2) Countries of the World and Their Leaders Yearbook, 1989 Gale Research, Inc.
(3) World Almanac and Book of Facts, 1989.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows the distribution of countries according to their degree of industrial complexity. Overall, there were 17 of the 69 countries, or 25 percent, which were identified as having NBC facilities, the most difficult category. An additional 19 countries or 28 percent, had oil fields and supporting industrial capabilities.

From a regional perspective, the **Western Hemisphere** countries showed a range of key installation categories from **Grenada** and **Surinam** with just a few sites, to **Cuba** with a reported chemical and biological capability.

The **Middle East** countries all had numerous communications and transportation facilities as well as pipelines and oil fields. **Egypt, Iran, Iraq, Libya,** and **Syria** were associated with NBC production or possession.

In **Africa**, there again was a range of countries from **Djibouti** and **Liberia** with just a few less developed facilities to **South Africa** with a reported emerging nuclear capability.

In **Asia** there were ten expeditionary environment countries which reportedly produce or possess various types of NBC weapons. These included **India, North Korea, Pakistan,** and **Vietnam.**

The countries of Europe all had modern communications and transportation facilities, including industrial centers and pipelines. **Greece** and **Norway** had offshore oil extraction facilities.

KEY INSTALLATIONS

	NONE	FEW SITES	MULTIPLE SITES	PIPELINE	OIL FIELD	NBC
WESTERN HEMISPHERE		GRENADA	EL SALVADOR	COSTA RICA	COLOMBIA	CUBA
		SURINAM	HAITI	DOM. REP	GUATEMALA	
			HONDURAS	JAMAICA	MEXICO	
				NICARAGUA	PERU	
				PANAMA	VENEZUELA	
MIDDLE EAST/ SOUTHWEST ASIA				LEBANON	BAHRAIN	EGYPT
				SOUTH YEMEN	KUWAIT	IRAN
					NORTH YEMEN	IRAQ
					OMAN	LIBYA
					QATAR	SYRIA
					SAUDI ARABIA	
					UAE	
AFRICA		DJIBOUTI	ETHIOPIA	KENYA	ALGERIA	SOUTH AFRICA
		LIBERIA	MADAGASCAR	SOMALIA	ANGOLA	
			NAMIBIA	SUDAN	TUNISIA	
			UGANDA	ZAIRE		
			ZIMBABWE			
ASIA/ PACIFIC	SPRATLY IS.	S. PACIFIC IS.	PAPUA N. G.	BANGLADESH	AFGHANISTAN	BURMA
				PHILIPPINES	MALAYSIA	INDIA
				SRI LANKA		INDONESIA
						JAPAN
						NORTH KOREA
						PAKISTAN
						PRC
						SOUTH KOREA
						THAILAND
						VIETNAM
EUROPE/ MED				DENMARK	GREECE	
				ITALY	NORWAY	
				TURKEY		
				YUGOSLAVIA		

PLANNING AND PROGRAMMING IMPLICATIONS

This assessment has indicated that there is a wide diversity of industrial complexity among the countries of interest. Marines must have an understanding of the infrastructure within these countries to be prepared for a range of operations across the spectrum of conflict. Because events frequently unfold very quickly, important facilities in a country can suddenly become key objectives for peacetime contingency or counterterrorist operations. NBC weapons producing facilities may need to be rapidly seized and secured without adverse affect. Ports and airfields may need to be neutralized and then rapidly repaired so they can be used by friendly forces. Noncombat equipment, material, and replacement parts will all be required to complete this process satisfactorily. Marine planners must ensure that equipment acquisition and training actions are taken to achieve the maximum level of readiness for these situations. Marines, and especially their engineers, must know how such facilities are constructed, what key nodes are within the facilities, and how to protect, destroy, or covertly neutralize the facility.

STRATEGIC AND TACTICAL LIFT CAPABILITIES AND CONSTRAINTS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY			
	A	B	C	D
MEU Response Time	<2 Days	>2 - <4 Days	>4 - <6 Days	>6 Days

D - Countries which require more than 6 days deployment time for a sea-based MEU.

C - Countries which require between 4 to 6 days deployment time for a sea-based MEU.

B - Countries which require between 2 and 4 days deployment time for a sea-based MEU.

A - Countries which require less than 2 days deployment time for a sea-based MEU.

GUIDELINES

(1) The focus was on typical response times for forward-deployed MEUs and garrison MEUs on the U.S. east and west coasts. The Air Alert Force (AAF) and two Air Contingency Battalions (ACBs) were recognized as a capability to deploy Marines by strategic airlift to any location in the world within 24 hours. However, because neither the AAF nor the ACBs possess a forcible entry capability, they were not factored into this assessment.

(2) The Atlantic Amphibious Ready Group (ARG) with an embarked MEU normally operates in the Mediterranean Sea. The Pacific ARG with its embarked MEU operates either in the Middle East/Southwest Asia region or the Western Pacific based on intelligence reports and the anticipated threat. An assumption was made that there would be some advance warning of a developing crisis to allow initial movement of the ARGs toward an objective area.

(3) Garrison MEUs at Camp Lejeune and Camp Pendleton both require 72 hours to embark aboard amphibious ships. Once embarked, it would require 3 more days for the Atlantic coast MEU to reach the Caribbean Sea and the Pacific coast MEU to reach the southern part of Mexico.

(4) ARGs, once underway, would maintain a speed of 12 knots.

Using the above methodology in conjunction with the data sources, the countries of interest were placed in the four categories (A through D). The following references were used as the basis for this assessment.

(1) Defense Mapping Agency, Hydrographic/Topgraphic Center, Distance Between Ports, Fifth Edition, 1985.
(2) MAGTF Warfighting Center letter dated 13 November 1989, Subject: Deployment Capabilities Guidelines.
(3) Headquarters U.S. Marine Corps, Marine Air-Ground Task Force Master Plan, dated 7 July 1989.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying charts show the regional distribution of expeditionary environment countries according to their respective sea-based MEU response times. In the **Western Hemisphere**, most of the countries require in excess of 6 days deployment time. Only a portion of **Mexico** and **Cuba** can be reached in less time. This is due to the time necessary for garrison MEUs on the **U.S.** east and west coasts to embark on amphibious ships and sail to these countries. In the **Middle East/Southwest Asia**, however, ARG/MEU arrival times at most countries are less than 2 days. These countries are mainly on the Mediterranean Sea and Persian Gulf littoral and are in proximity to the principal ARG/MEU operating areas. In **Africa**, over half the countries required a response time or more than 6 days. These countries are outside the Mediterranean Sea and the farthest away from the ARG/MEU operating in the Indian Ocean. In **Asia/Pacific**, response times were calculated from a likely ARG/MEU operating area in the **Philippines**. Those countries most distant from the **Philippines** had the longest response times. In **Europe/Mediterranean**, the countries of **Norway** and **Denmark** had the longest response times for the ARG/MEU operating primarily in the Mediterranean Sea.

DISTRIBUTION OF COUNTRIES BY ARG/MEU RESPONSE TIMES

	< 2 DAYS	> 2 < 4 DAYS	> 4 < 6 DAYS	> 6 DAYS
WESTERN HEMISPHERE		NORTH MEXICO	CUBA MID-MEXICO	COLOMBIA COSTA RICA DOM. REP. EL SALVADOR GRENADA GUATEMALA HAITI HONDURAS JAMAICA SOUTH MEXICO NICARAGUA PANAMA PERU SURINAM VENEZUELA
MIDDLE EAST/ SOUTHWEST ASIA	BAHRAIN EGYPT IRAN IRAQ KUWAIT LEBANON LIBYA OMAN QATAR SAUDI ARABIA SYRIA UAE	NORTH YEMEN SOUTH YEMEN		
AFRICA	ALGERIA TUNISIA	DJIBOUTI	KENYA MADAGASCAR SOMALIA	ANGOLA ETHIOPIA LIBERIA NAMIBIA SOUTH AFRICA SUDAN UGANDA ZAIRE ZIMBABWE
ASIA/PACIFIC	COASTAL INDIA COASTAL PAKISTAN PHILIPPINES SPRATLY IS.	INLAND INDIA INDONESIA MALAYSIA INLAND PAKISTAN PAPUA N. GUINEA COASTAL PRC SRI LANKA THAILAND VIETNAM	BANGLADESH BURMA SOUTHERN JAPAN INLAND PRC SOUTH KOREA S. PACIFIC IS. (SOLOMON IS.)	AFGHANISTAN NORTHERN JAPAN NORTH KOREA S. PACIFIC IS. (FIJI, KIRIBATI, VANUATU)
EUROPE/MED	GREECE ITALY TURKEY YUGOSLAVIA		DENMARK	NORWAY

PLANNING AND PROGRAMMING IMPLICATIONS

This assessment has found that 42 percent of the countries have ARG/MEU response times of more than six days. This suggests that the Commandant's recent emphasis on strategic deployment by air merits in-depth planning and programming support. In the area of tactical lift, capabilities such as the Landing Craft Air Cushion (LCAC) will allow a naval expeditionary force to be far offshore and still effectively strike a target. The CH-46 helicopter, however, does not have the extended range to adequately support the OTH assault and a replacement such as the MV-22A Osprey needs to be acquired. By using tactical lift capabilities such as the Advanced Assault Amphibious Vehicle, high-speed LCAC, and extended-range vertical lift, the ATF will have a better opportunity to execute its OTH assault.

NONCOMBATANT EVACUATION LOGISTICS

CRITERIA FOR LEVELS OF DIFFICULTY

	LEVELS OF DIFFICULTY →					
	A	B	C	D	E	F
NEO						
Embassy Staff	<25	<50	<100	<250	<500	>500
Evacuees	None	<100	<200	<300	>300	>500 *
Inland Obj	Coastal	<100 NM	<300 NM	>300 NM	>500 NM	>999 NM

* For purposes of this study, 500 evacuees was used as a threshold. Anything above 500 would probably require consideration of other options, i.e., evacuation by airlift or sealift.

F - U.S. Embassy staff over 500; evacuees over 500; and evacuation site 1,000 nm or more from the coast.

E - U.S. Embassy staff - 250 to 500; evacuees - 300 to 500; and evacuation site 500 to 1,000 nm from the coast.

D - U.S. Embassy staff - 100 to 250; evacuees - 200 to 300; and evacuation site 300 to 500 nm from the coast.

C - U.S. Embassy staff - 50 to 100; evacuees - 100 to 200; and evacuation site 100 to 300 nm from the coast.

B - U.S. Embassy staff - 25 to 50; evacuees - up to 100; and evacuation site up to 100 nm from the coast.

A - U.S. Embassy staff less than 25; no evacuees; and evacuation site located on the coast.

EMBASSY STAFF: This includes the Country Team and supporting units such as the Marine Security Guard. Not included are Foreign Nationals who under some circumstances would require evacuation.

EVACUEES: These are the U.S. citizens (less military personnel and U.S. Embassy staff) in residence.

INLAND OBJECTIVE: The capital of each country was selected as the NEO inland objective (evacuation site). Distances were calculated from a point just off the coast to the capital.

Using the above criteria in conjunction with source material, the countries of interest were assigned a rating (A through F). Because a number of countries did not always match the designated categories for Embassy Staff, Evacuees, and Inland Obj, the highest value for the three categories determined the rating. For example, if the country's evacuees exceeded 500 but the inland objective was less than 200 nm from the coast, an "F" rating was assigned. Volume II, Study Supporting Material, Section 30, Noncombatant Evacuation Logistics contains the data for each country on which the ratings are based. The following references were used as source material:

(1) U.S. Department of State, Statistics on U.S. Embassies in Countries of Interest, 21 February 1990.
(2) U.S. Department of State, Numbers of U.S. Citizens Living in Countries of Interest, 21-22 February 1990.

SUMMARY ASSESSMENT OF IMPACT ON EXPEDITIONARY ENVIRONMENT COUNTRIES

The accompanying chart shows the regional distribution of countries according to noncombatant evacuation logistics. In the **Western Hemisphere**, over 80 percent of the countries fell into the most difficult category due primarily to the large number of potential evacuees.

In the **Middle East/Southwest Asia**, all but two countries were rated in the three most difficult categories. There were 9 of the 16 countries in this region that had more than 500 potential evacuees while 5 countries had distances to their capitals (evacuation points) exceeding the range (70 nautical miles) of the CH-46 medium lift helicopter.

In **Africa**, over half the countries presented the most difficult logistic conditions for NEO. Nine of the 15 countries in this region had evacuation distances greater than the range of the CH-46.

In **Asia/Pacific** a total of 12 countries were in the most difficult category while in **Europe/Mediterranean** all 6 countries were rated most difficult. These two regions had 7 countries where distances to the evacuation point exceeded the range of the CH-46. There were 18 countries in these regions with more than 500 evacuees.

REGIONAL DISTRIBUTION OF COUNTRIES BY NONCOMBATANT EVACUATION LOGISTICS

INCREASING DIFFICULTY →

WESTERN HEMISPHERE			EL SALVADOR	CUBA SURINAM		COLOMBIA COSTA RICA DOM. REP. GRENADA GUATEMALA HAITI HONDURAS JAMAICA MEXICO NICARAGUA PANAMA PERU VENEZUELA
MIDDLE EAST/ SOUTHWEST ASIA	LIBYA SOUTH YEMEN			IRAN IRAQ	QATAR	BAHRAIN EGYPT KUWAIT LEBANON NORTH YEMEN OMAN SAUDI ARABIA SYRIA UAE
AFRICA	ANGOLA	DJIBOUTI	MADAGASCAR NAMIBIA	SOMALIA	ALGERIA UGANDA	ETHIOPIA KENYA LIBERIA SOUTH AFRICA SUDAN TUNISIA ZAIRE ZIMBABWE
ASIA/PACIFIC	SPRATLY IS.	NORTH KOREA VIETNAM	BURMA		AFGHANISTAN S. PACIFIC IS.	BANGLADESH INDIA INDONESIA JAPAN MALAYSIA PAKISTAN PAPUA N. GUINEA PHILIPPINES PRC SOUTH KOREA SRI LANKA THAILAND
EUROPE/MED						DENMARK GREECE ITALY NORWAY TURKEY YUGOSLAVIA

PLANNING AND PROGRAMMING IMPLICATIONS

Despite the emphasis in recent years on the importance of the MAGTF in NEO, the study found that these operations are extremely difficult in 53 of the 69 countries (77%) unless there is a major draw-down of U.S. citizens before the crisis develops, or provisions are made for the use of strategic airlift to evacuate the noncombatants. The existing range and lift capability of the CH-46 cannot support the requirements of the expeditionary environment. In most countries, there are over 100 U.S. citizens in the Embassy, and/or over 200 U.S. citizens in the national capital, and/or the distance of the NEO objective from the offshore platform is greater than 300 nautical miles.

APPENDIX G

OSINT OPSEC: Selected References and Information

NOTE: The complete addresses for all of the publishers are provided at the end of this handout.

OPEN SOURCES AND TELEPHONE INTERCEPTION

Tom Kneitel, *Tune In On Telephone Calls*, CRB Research (1993)
ISBN: 0-939780-19-4

OPEN SOURCES AND RADIO INTERCEPTION

Monitoring Air Force One- 50 page manual. Published without any reference to the identity of its author nor to the place or date of its publication. Purchased in July, 1994, through an ad placed in *Monitoring Times*.

Tom Kneitel, *Guide to Embassy & Espionage Communications*, CRB Research (1986).
ISBN: 0-939780-06-2

Monthly hobbyist magazine: *Monitoring Times*, Brasstown, NC.

OPEN SOURCES AND EAVESDROPPING

Electronic Eavesdropping Techniques and Equipment, prepared for the National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice, by Raymond N. Jones. Republished as *Covert Intelligence: Electronic Eavesdropping* by CRB Research. No date listed.

Electronic plans from - *Portfolio of Schematic Diagrams for Electronic Surveillance*, Mentor Publications, Flushing, NY (1979)

OPEN SOURCES AND UNDERCOVER OPERATIONS

E. Roy Slade and James R. Gutz, *The Pretext Book*, Cloak and Data Press, Houston, TX (1991). Available through: The P.I. Catalogue, (512) 928-8190.

Kingdon Peter Anderson, *Undercover Operations; A Manual for the Private Investigator*,

Paladin Press (1988). ISBN: 0-87364-486-7.

Eddie the Wire, *The Complete Book of Lockpicking*, Loompanics Unlimited (1981). ISBN: 0-915179-06-7.

Burt Rapp, *Shadowing and Surveillance; A Complete Guidebook*, Loompanics Unlimited (1986). ISBN: 0-915179-33-4.

OPEN SOURCES AND INTERROGATIONS

Richard W. Krousher, *Physical Interrogation Techniques*. Loompanics Unlimited, (1985). ISBN: 0-915179-23-7.

No author listed, *Interrogations: Techniques and Tricks to Secure Evidence*, Paladin Press (1991). ISBN: 0-87364-625-8.

OPEN SOURCES AND EXECUTIONS

John Minnery, *How To Kill*, Paladin Press (1973). ISBN: 0-87364-003-9.

George Hayduke, *The Hayduke Silencer Book*, Paladin Press (1989). ISBN: 0-87364-522-7.

John Sanchez, Slash and Thrust, Paladin Press (1980). ISBN: 0-87364-188-4.

J. David Turby, *Zips, Pipes, and Pens; A Manual of Improvised Weapons*, Paladin Press (1992). ISBN: 0-87364-702-5.

OPEN SOURCES AND EXPLOSIVES

Ragnar Benson, *New and Improved C-4*, Paladin Press (1995).

Seymour Lecker, *Homemade Semtex: C-4's Ugly Sister*, Paladin Press (1991). ISBN: 0-87364-617-7.

Thomas Mordechai, *Professional Standards for Preparing, Handling, and Using Explosives*, Paladin Press (1995). ISBN: 0-87364-807-2.

Jo Jo Gonzalez, *Death by Deception; Advanced Improvised Booby Traps*, Paladin Press (1992). ISBN: 0-87364-651-7.

Seymour Lecker, *Improvised Explosives, How To Make Your Own*, Paladin Press (1985).

ISBN: 0-87364-320-8.

No author, *How To Destroy Bridges*, Paladin Press (1988). ISBN: 0-87364-485-9.

OPEN SOURCES AND RADIO DETONATION OF BOMBS

Lawrence W. Meyers, *Improvised Radio Detonation Techniques*, Paladin Press (1988). ISBN: 0-87354-479-4.

OPEN SOURCES AND VEHICULAR ENHANCEMENTS

Ronald George Eriksen, *Getaway; Driving Techniques For Escape and Evasion*, Loompanics Unlimited (1982)

OPEN SOURCES AND TACTICAL COMMUNICATIONS JAMMING

Lawrence W. Myers, *Improvised Radio Jamming Techniques*, Paladin Press (1989). ISBN: 0-87364-520-0.

OPEN SOURCES AND BANK CARD FORGERY

Anonymous, *How To Create A New Identity*, Carol Publishing Group, NY (1991). ISBN: 0-8065-1034-X.

Jack Luger, *Counterfeit I.D. Made Easy*, Loompanics Unlimited (1990). ISBN: 0-915179-90-3.

Thomas Collins, *Counterfeit Currency, How To Really Make Money*, Loompanics Unlimited (1990). ISBN: 1-55950-042-5.

John Sample, *Methods of Disguise*, Loompanics Unlimited (1993). ISBN: 1-55950-096-4.

J.F. Straw, *Around The World Contacts*, Worldwide Investment News, Dalton, GA (1991).

OPEN SOURCES AND LEGAL OFFSHORE PASSPORTS

Passport Agent's Manual, originally published by the U.S. Passport Service, republished by Eden Press, Fountain Valley, CA (no date listed).

OPEN SOURCES AND CHOOSING A CRIMINAL SPECIALTY

K. Hawkeye Gross, *Drug Smuggling: The Forbidden Book*, Paladin Press (1992).
ISBN: 0-87364-685-1.

Harold S. Long. *Successful Armed Robbery*, Loompanics Unlimited (1990).
ISBN: 1-55950-023-9.

Rex Farel, Hit Man; *A Technical Manual for Independent Contractors*, Paladin Press (1992).
ISBN: 0-87364-7.

Michael Connor, *How To Hide Anything*, Paladin Press (1984).
ISBN: 0-87364-289-9.

Ragnar Benson, *Gunrunning for Fun & Profit*, Paladin Press (1986).
ISBN: 0-87364-359-3.

Communicating with the Publishers

Paladin Press
P.O. Box 1307
Boulder, CO 80306
(800) 392-2400

CRB Research Books, Inc.
Box 56
Commack, NY 11725
(800) 656-0056

Loompanics Unlimited
P.O. Box 1197
Port Townsend, WA 98369
Does not have an (800) order line

Eden Press
P.O. Box 8410
Fountain Valley, CA 92728
(800) 338-8484

For those interested in further study of this topic, catalogues are available from each publisher which document the full range of material available to the public.

Communicating with the primary source for this lesson:

Mr. Richard Horowitz
307 West 79th Street
Suite 331
New York, NY 10024
Tel: (212) 362-5199
Fax: (212) 769-6162
RHJDPICPT@Compuserve.com

APPENDIX H

Countries Comprising the Expeditionary Environment

Asia/Pacific	Europe/Mediterranean	Middle East/SW Asia
Bangladesh	Belarus	Afghanistan
Cambodia	Bosnia-Herzegovina	Armenia
China	Croatia	Azerbaijan
Fiji	Czech Republic	Bahrain
Indonesia	Denmark	Georgia
Japan	Estonia	India
Kazakhstan	Greece	Iran
Kiribati	Italy	Iraq
Kyrgystan	Latvia	Israel
Malaysia	Lithuania	Jordan
Myanmar	Macedonia	Kuwait
New Caledonia	Moldova	Lebanon
North Korea	Norway	Oman
Papua New Guinea	Poland	Pakistan
Philippines	Romania	Qatar
Russia	Serbia and Montenegro	Saudi Arabia
Solomon Islands	Slovakia	Syria
South Korea	Slovenia	Tajikistan
Spratly Islands	Turkey	Turkmenistan
Sri Lanka	Ukraine	United Arab Emirates
Thailand		Uzbekistan
Vanuatu		Yemen
Vietnam		

Western Hemisphere	Africa
Argentina	Algeria
Bolivia	Angola
Brazil	Djibouti
Colombia	Egypt
Costa Rica	Ethiopia
Cuba	Ghana
Dominican Republic	Kenya
Ecuador	Liberia
El Salvador	Libya
Grenada	Madagascar
Guatemala	Namibia
Haiti	Nigeria
Honduras	Somalia
Jamica	South Africa
Mexico	Sudan
Nicaragua	Tunisia
Panama	Uganda
Paraguay	Zaire
Peru	Zimbabwe
Suriname	
Uraguay	
Venezuela	

I-INTELLIGENCE

OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK

I-INTELLIGENCE

OPEN SOURCE INTELLIGENCE

TOOLS AND RESOURCES HANDBOOK

2018

Aleksandra Bielska

Natalie Anderson, Vytenis Benetis, Cristina Viehman

Foreword

I am delighted to share the latest version of our OSINT Tools and Resources Handbook. This version is almost three times the size of the last public release in 2016. It reflects the changing intelligence needs of our clients in both the public and private sector, as well as the many areas we have been active in over the past two years.

No list of OSINT tools is perfect, nor is it likely to be complete. Indeed, such is the pace of change that by the time you read this document some of our suggestions may have been surpassed or have ceased to exist. Regrettably, today's tool might also be tomorrow's vulnerability.

To counter the first problem, we have included a list of toolkits provided by other OSINT practitioners working to improve the state-of-the-art. To manage the second, we recommend that all tools be tested in a secure computing environment whenever possible.

Work on the next iteration of the Handbook has already begun. For now, I hope this version contributes to improving your efficiency and effectiveness as a researcher, analyst, investigator or general OSINT practitioner. Please feel free to share it with your colleagues. To encourage its broadest possible dissemination, we are publishing the Handbook under a Creative Commons CC BY License.

I would like to end by thanking my colleagues at i-intelligence for their efforts in compiling the Handbook. Particular credit is due to Aleksandra Bielska who led the project and has coordinated the inputs from different contributors. I am also indebted to Natalie Anderson of Mercyhurst University for her excellent research and for the time spent checking these links. Kris Wheaton and Brad Gleason from Mercyhurst's Department of Intelligence Studies are also thanked for their support.

Finally, I would like to thank our community of followers on Twitter for sharing their recommendations with us, as well as the many practitioners who have suggested new tools to us while participating in our courses.

Chris Pallaris
Director, i-intelligence GmbH

CC BY

Table of Contents

Foreword 2

Search 9
- General Search 9
- Meta Search 11
- Visual Search and Clustering Search Engines 12
- National Search Engines 13
- Code Search 16
- FTP Search 17
- Similar Sites Search 18
- IoT Search Engines 19
- Kids-Friendly Search Engines 20
- Other Specialty Search Engines 21
- Other Search Engines and Tools 23

Social Media 25
- Major Social Networks 25
- Real-Time Search, Social Media Search, and General Social Media Tools 27
- Social Media Tools: Twitter 30
- Social Media Tools: Facebook 35
- Social Media Tools: Google+ 37
- Social Media Tools: Instagram 38
- Social Media Tools: Pinterest 40
- Social Media Tools: Reddit 41
- Social Media Tools: VKontakte 43
- Social Media Tools: Tumblr 44
- Social Media Tools: LinkedIn 45
- Social Media Tools: Snapchat 46
- Social Media Tools: WhatsApp 47
- Social Media Tools: Skype 48
- Social Media Tools: Telegram 49
- Other Instant Messaging and Chat Tools 50
- Dating Apps 51

Blogs, Forums, Discussion Boards, and Q&A Sites 52
- Blog Search 52

Forums and Discussion Boards Search 53
Q&A Sites 54

People Investigations 55
Main People Search Tools and Engines 55
Address & Contact Information Search 58
Public Records 60
Ancestry Research 62
Phone Search 63
E-mail Search / E-mail Check 66
Username Check 70
CV and Resume Search 71
Expert Search 72
Salary Search 74
Creating a Sock Puppet 76

Company Research 77
Main Company Search Tools and Engines 77
Company Research (EU) 80
Company Research (UK) 81
Company Research (US) 84
Company Research (Switzerland) 86
Company Research (Middle East) 87
Company Research (Africa) 88
Company Research (China) 90
Business Registers (EU + EFTA) 91
Business Registers (US) 93
Business Registers (Other) 95
Business Registers Lists and Directories 97
Job Search Resources 99
Company Reviews 101
Patent Research 102
Tenders 104
Charity, NGO, and Nonprofit Research 106

Real Estate Research 108
Real Estate Research 108

Online Marketplaces 111
Classifieds and Online Marketplaces 111

Cryptocurrencies and Financial Information 114
Cryptocurrencies 114

Financial Information 115
Legal Research 116
Legal Research Reources and Tools 116
Researching Countries 119
Country Profiles 119
Researching Terrorism, Crime, and Cybersecurity 120
Researching Terrorism 120
Researching Crime 122
Researching Cybersecurity 123
Researching Stolen Items 125
Researching Stolen Items 125
Researching Human Trafficking 127
Researching Human Trafficking 127
Transportation 131
Airplanes 131
Drones 133
Cars 135
Railways 137
Public Transport 141
Ships 144
Container and Cargo Tracking 146
Web Intelligence 147
Domain and IP Research, Websites Analysis 147
Web History and Website Capture 155
Wifi Search 157
Researching Dark Web 158
Researching Dark Web 158
Events Search 160
Events Search 160
Working with Images 161
Image Search and Reverse Image Search 161
Image Analysis 164
Stock Images 167
Image and Photo Editing 169
OCR Tools 171
Working with Videos 172

Video Search and Reverse Video Search 172
Live Streaming and Webcams 174
Other Video Tools 176
Video Editors 179

Working with Audio 181
Radio 181
Podcasts 183
Other Audio Tools 185

Working with Documents 186
Documents and Slides Search 186
Pastebins 188
Document and Reference Management 189
PDF Management 190
Working with Document Metadata 191

Academic Resources and Grey Literature 192
Academic and Grey Literature Research Tools 192

Lectures, Talks, Conference Presentations, Speeches 196
Lectures, Talks, Conference Presentations, Speeches 196

Books and Reading 198
Books Search and Reading Tools 198

Working with Data and Statistics 201
Data and Statistics 201
Infographics and Data Visualization 206
Dashboard Tools 209
Data Analysis 210
Data Scrapers 212

Working with News 214
News Sources 214
News Digest and Discovery Tools 216
Fact Checking 217

Working with Foreign Language Content 219
Translation Tools 219

Web Monitoring 222
RSS Readers 222
Other RSS Tools 224
Website Monitoring 225
Social Media Monitoring 226

Other Monitoring Tools 227

Data Collation 228
Bookmarking 228
Notetaking 231
Annotation and Highlighting 233
Screenshot and Screen Capture Tools 234

Browsing and Browsers 236
Browsers 236
Startpages 238
Customising New Tab 239
Tab Management 241
Extension Managers 243
Offline Browsing 244
Browsing History 245
Other Browsing Tools 246

Writing and Dissemination 247
Writing and Office Tools 247
Slideshow and Presentation Tools 249
Digital Publishing 251
Newsletter Tools 252
Digital Storytelling 253

Wikis, Websites, and Web Apps 255
Wikis 255
Website Builders 256
App Builders 258

Mind Mapping, Concept Mapping and Idea Generation 259
Mind Mapping, Concept Mapping and Idea Generation Tools 259

Productivity and File Management 261
Main Work Management and Productivity Tools 261
E-mail Management 264
Cloud Storage and File Sharing 266
Web Automation 268

Collaboration and Communication 269
Collaboration and Project Management 269
Communication Tools 273

Other Utility Tools 276
File Converters 276

URL Shorteners and Expanders 278
Keywords Discovery and Research 279
Android Emulators 280
Virtual Machine 281
Date & Time 282
Weather 283
Barcodes 285

Analysis 286
Social Network Analysis 286

Geospatial OSINT 287
Geospatial Research and Mapping Tools 287
Interesting Maps 293

Privacy and Security 295
General Privacy Tools and Resources 295
Secure Browsing 297
Ads and Tracking Blockers 301
Blocking of Currency Miners 302
Private Search Engines and Private Searching 303
Secure OS 304
Backup Tools 305
Secure Communication Tools 306
E-mail Security 307
Phone Security 309
Password Management and Secure Login 310
Encryption Tools 311
Secure File Sharing 313
VPN Services 314
VPN Texting 316
Proxy Tools 317
Antivirus Software 318
Other Security Tools 319
Copyright and Takedowns 320
Researching Leaks 321

Research and Recon Tools 322
Research and Data Recon Tools 322

OSINT Tools Lists 324
OSINT Tools Lists 324

Search

General Search

Tool	Link
Aol	http://search.aol.com
Ask	http://www.ask.com
Baidu	http://www.baidu.com
Bing	http://www.bing.com
Deeperweb	http://deeperweb.com
Dothop	http://dothop.com
DuckDuckGo	https://duckduckgo.com
Ecosia	https://www.ecosia.org
entireweb	https://www.entireweb.com
Factbites	http://www.factbites.com
Gigablast	http://gigablast.com
Goodsearch	http://www.goodsearch.com
Google Advanced Search	https://www.google.com/advanced_search
Google Search	http://www.google.com
Jive Search	https://www.jivesearch.com
Lycos	http://www.lycos.com
MyWebSearch	http://home.mywebsearch.com
SurfCanyon	http://www.surfcanyon.com
Teoma	http://www.teoma.com
Wolfram Alpha	http://www.wolframalpha.com
Yahoo! Search	http://www.yahoo.com

Yandex	https://www.yandex.com

Meta Search

Tool	Link
All-in-One	http://all-io.net
AllTheInternet	http://www.alltheinternet.com
Bing vs. Google	http://bvsg.org
Dogpile	http://www.dogpile.com
eLocalFinder	http://www.elocalfinder.com/HSearch.aspx
Etools	http://www.etools.ch
Excite	http://msxml.excite.com
FaganFinder	http://www.faganfinder.com/engines
Findsmarter	http://www.findsmarter.com
Info.com	http://www.info.com
Infospace	http://www.infospace.com
Instya	http://www.instya.com
iZito	http://www.izito.com
Nextaris	http://www.nextaris.com
Metabear	http://www.metabear.com
Monster Crawler	http://www.monstercrawler.com
Myallsearch	http://www.myallsearch.com
opentext	http://fqs.opentext.com/web.htm
Search	https://www.search.com
Sputtr	http://www.sputtr.com
SonicRun	http://www.sonicrun.com
Trovando	http://www.trovando.it
WebCrawler	http://www.webcrawler.com
Zapmeta	http://www.zapmeta.com

Visual Search and Clustering Search Engines

Tool	Link
Answer The Public	https://answerthepublic.com
Carrot2	http://search.carrot2.org
Cluuz	http://www.cluuz.com
Exalead	http://www.exalead.com
iSEEK	http://iseek.com
Yippy	http://yippy.com

National Search Engines

Tool	Link
1ste Keuze (Netherlands)	http://www.eerstekeuze.nl
360 so (China)	https://www.so.com
AEIOU (Portugal)	http://www.aeiou.pt
Alleba (Philippines)	http://www.alleba.com
AnoKato (Greece)	http://www.ano-kato.com
AONDE (Brazil)	http://www.aonde.com
Apali! (Spain)	http://www.apali.com
Arabo (Algeria)	http://www.arabo.com
Arama (Turkey)	http://www.arama.com
Baidu (China)	http://www.baidu.com
Baidu In English	http://baiduinenglish.com
Daum (South Korea)	http://www.daum.net
Deusu (Germany)	https://deusu.de
Dive3000 (Italy)	http://www.dive3000.com/search
Editus.lu (Luxembourg)	https://www.editus.lu
Eniro (Sweden)	http://www.eniro.se
FineLib (Nigeria)	http://www.finelib.com
Finna (Finland)	https://www.finna.fi
Fireball (Germany)	https://fireball.de
Freenet.de (Germany)	http://suche.freenet.de
Goo (Japan)	http://www.goo.ne.jp
Gooru (Poland)	http://www.gooru.pl
Hao123 (China)	https://www.hao123.com
Iranmehr (Iran)	http://www.iranmehr.com

Jamasp (Iran)	http://www.jamasp.ir
KacMac (Syria)	http://www.kacmac.com
Kvasir (Norway)	http://www.kvasir.no
Leit (Iceland)	http://leit.is
Libero (Italy)	http://arianna.libero.it
Lycos.fr (France)	http://www.lycos.fr
Makupalat (Finland)	https://www.finna.fi
Maven Search (Israel)	http://www.mavensearch.com
MetaGer (Germany)	https://metager.de
Mojeek (United Kingdom)	https://www.mojeek.co.uk
Mozbot (France)	https://www.mozbot.com
Najdsi (Slovenia)	http://www.najdi.si
Nate (South Korea)	http://www.nate.com
Naver (South Korea)	http://www.naver.com
Onet.pl (Poland)	http://www.onet.pl
Orange (France)	http://www.orange.fr
Parseek (Iran)	http://www.parseek.com
Pipilika (Bangladesh)	https://www.pipilika.com
Raftaar (India)	https://www.raftaar.in
Raziskovalec (Slovenia)	http://www.raziskovalec.com
Rismoon (Iran)	http://www.rismoon.com
Rootle (Russia)	http://www.rootle.ru
SAPO (Portugal)	http://www.sapo.pt
Search.bg (Bulgaria)	http://www.search.bg
Search.ch (Switzerland)	http://www.search.ch
Search Engine Colossus	http://searchenginecolossus.com
Search Lotto (United Kingdom)	https://www.searchlotto.co.uk
Seznam (Czech Republic)	https://www.seznam.cz
Shamrock (Ireland)	http://www.ireland-information.com/engine
Sina (China)	Https://www.sina.com.cn
Sogou (China)	https://www.sogou.com
Surf (Slovakia)	http://www.surf.sk

Walla (Israel)	http://www.walla.co.il
Yam (Taiwan)	http://search.yam.com
Yandex (Russia)	http://www.yandex.com
Yoodle (Switzerland)	http://www.yoodle.ch
Yooz (Iran)	https://yooz.ir
Vinden (Netherlands)	https://www.vinden.nl
Qq.com (China)	http://www.qq.com
Zoznam (Slovakia)	https://www.zoznam.sk

Code Search

Tool	Link
NerdyData	https://search.nerdydata.com
Google Code Search	https://code.google.com
PublicWWW	https://publicwww.com
Programmable Web	https://www.programmableweb.com
SearchCode	https://searchcode.com

FTP Search

Tool	Link
Archie	http://archie.icm.edu.pl/archie_eng.html
Filemare	https://filemare.com
Global File Search	http://globalfilesearch.com
Global File Search	http://globalfilesearch.net
MMNT	http://www.mmnt.ru
NAPALM FTP Indexer	http://www.searchftps.net

Similar Sites Search

Tool	Link
Find Similar Sites	http://www.findsimilarsites.com
Google Similar Pages	https://chrome.google.com/webstore/detail/google-similar-pages/pjnfggphgdjblhfjaphkjhfpiiekbbej
SimilarPages	http://www.similarpages.com
SimilarSites	http://www.similarsites.com
SimilarSiteSearch	http://www.similarsitesearch.com
SitesLike	http://www.siteslike.com

IoT Search Engines

Tool	Link
Internet of Things Scanner	https://iotscanner.bullguard.com
Shodan	https://www.shodan.io
Thingful	https://www.thingful.net
ZoomEye	https://www.zoomeye.org

Kids-Friendly Search Engines

Tool	Link
Fact Monster	https://www.factmonster.com
KidsClick	http://www.kidsclick.org
KidRex	http://www.kidrex.org
Topmarks	https://www.topmarks.co.uk

Other Specialty Search Engines

Tool	Link
Athlinks	https://www.athlinks.com
Biznar	http://biznar.com
Blade Search	https://bladesearch.com
CiteSeerX	http://citeseer.ist.psu.edu
crunchbase	https://www.crunchbase.com
Datasheet Library	http://www.datasheetlib.com
Digle	https://www.digle.com
Economic Search Engine	http://ese.rfe.org
FluidDATA	https://fluid.bitplatter.com
Google Custom Search	http://www.google.com/cse
Harmari	https://www.harmari.com/search/unified
Instant Logo Search	http://instantlogosearch.com
Internet Archive	https://archive.org/
Lableb	https://lableb.com
moocha	https://www.moocha.io
Open Hub	https://www.openhub.net
Qwikia	http://www.qwika.com
Rebbutter.me	http://rebutter.me
ShareDir	https://sharedir.com
Sweet Search	https://www.sweetsearch.com
SymbolHound	http://symbolhound.com
Think Tank Search	https://guides.library.harvard.edu/hks/think_tank_search
WikiVisually	https://wikivisually.com
WorldWideScience.org	http://worldwidescience.org

Yamli	http://www.yamli.com
Yobi 3D	https://www.yobi3d.com
Zanran	http://zanran.com

Other Search Engines and Tools

Tool	Link
2lingual Search	http://www.2lingual.com
Advangle	http://advangle.com
Answer the Public	https://answerthepublic.com
AOL Search Database	https://search-id.com
Banana SLUG	http://www.bananaslug.com
BOOL	https://chrome.google.com/webstore/detail/bool/cfpmoigmhcehoegokjllchipdiindpkc
Context Menu Search	https://chrome.google.com/webstore/detail/context-menu-search/ocpcmghnefmdhljkoiapafejjohldoga
Custom Search	https://inteltechniques.com/OSINT/user.html
Impersonal.me	http://www.impersonal.me
European Search Engines, Directories and Lists	http://www.searchenginesoftheworld.com/search_engines_of_europe/
Fast Advanced Google Search	https://chrome.google.com/webstore/detail/fast-advanced-google-sear/idijdjdcncjcgmeiipcnkpjedhgepalk?hl=en
Faster Google Search	https://chrome.google.com/webstore/detail/faster-google-search/fmhiafgdfaglfbaaefbbolaholfhkmjc?hl=en
Google Correlate	https://www.google.com/trends/correlate
Google Search Filter	https://chrome.google.com/webstore/detail/google-search-filter/eidhkmnbiahhgbgpjpiimdogfidfikgf?hl=en
Google Similar Pages	https://chrome.google.com/webstore/detail/google-similar-pages/pjnfggphgdjblhfjaphkjhfpiiekbbej
Infinite Scroll	https://chrome.google.com/webstore/detail/infinite-scroll-for-googl/acjdmkdcbbhokaleofmalpcnnkpgphpb?hl=en-US
I Search From	https://isearchfrom.com

Klug Suchen	http://www.klug-suchen.de
Million Short	https://millionshort.com
Net Data Directory	http://netdatadirectory.org
Neuskool	http://neuskool.com
pagodo	https://github.com/opsdisk/pagodo
Polycola	http://www.polycola.com
RESULTER	https://chrome.google.com/webstore/detail/resulter-google-search-sh/chojfhfgbdaeokblbdeahgbijodikdpk
Result Preview	https://chrome.google.com/webstore/detail/result-preview/geogklgaaafmfijgfninjjbcinicfafb
Ruin My Search History	http://ruinmysearchhistory.com
SCANNER-INURLBR	https://github.com/googleinurl/SCANNER-INURLBR
Search by Image	https://chrome.google.com/webstore/detail/search-by-image-by-google/dajedkncpodkggklbegccjpmnglmnflm/related?hl=en
Search Engine Colossus	http://www.searchenginecolossus.com
Search Engines of the World	https://www.searchenginesoftheworld.com
Search Preview	https://chrome.google.com/webstore/detail/search-preview/majhgbekihmliceijipbdccgicepmmei
Search the current site	https://chrome.google.com/webstore/detail/search-the-current-site/jliolpcnkmolaaecncdfeofombdekjcp
Secret Search Engine Labs	http://www.secretsearchenginelabs.com
Selection Search	https://chrome.google.com/webstore/detail/selection-search/gipnlpdeieaidmmeaichnddnmjmcakoe
Sensebot	http://sensebot.com
Suchmaschinen Datenbank	http://www.suchmaschinen-datenbank.de
tracerT	https://github.com/GeneralTesler/tracerT
wiby	https://wiby.me

Social Media

Major Social Networks

Tool	Link
Draugiem (Latvia)	https://www.draugiem.lv
Facebook	http://www.facebook.com
Facenama (Iran)	http://facenama.com
Fediverse	https://fediverse.party
Flickr	https://www.flickr.com
Google+	https://plus.google.com
Instagram	https://www.instagram.com
kik	https://www.kik.com
Linkedin	https://www.linkedin.com
Mastodon	https://mastodon.social
Meetup.com	https://www.meetup.com
Mixi (Japan)	https://mixi.jp
Odnoklassniki (Russia)	http://ok.ru
Periscope	https://www.pscp.tv
Pinterest	http://www.pinterest.com
Qzone (China)	http://qzone.qq.com
Reddit	https://www.reddit.com
Snapchat	https://www.snapchat.com
Swarm	https://www.swarmapp.com
Taringa (Latin America)	http://www.taringa.net
Tinder	https://www.gotinder.com

Tumblr	https://www.tumblr.com
Twitter	https://twitter.com
VKontakte	https://vk.com
Weibo (China)	http://weibo.com
Xing	https://www.xing.com
YouTube	https://www.youtube.com

Real-Time Search, Social Media Search, and General Social Media Tools

Tool	Link
360 social.me	https://www.360social.me
Agora pulse	https://www.agorapulse.com
AIDR	http://aidr.qcri.org
Audiense	https://www.audiense.com
Bloopish	http://bloopish.com
Brand24	https://brand24.com
Brandwatch	https://www.brandwatch.com
Buffer	https://buffer.com
Buzzsumo	http://buzzsumo.com
CrowdTangle Link Checker	https://chrome.google.com/webstore/detail/crowdtangle-link-checker/klakndphagmmfkpelfkgjbkimjihpmkh
Custom Communities Search	https://inteltechniques.com/osint/communities.html
Custom Social Networks Search	https://inteltechniques.com/osint/social.networks.html
Cyfe	http://www.cyfe.com
Falcon	https://www.falcon.io
Flumes	http://flumes.com
Gaddr	https://gaddr.me
Geocreepy	http://www.geocreepy.com || https://n0where.net/creepy
Geofeedia	https://geofeedia.com
Hootsuite	http://hootsuite.com
HowSociable	http://www.howsociable.com
Hashtatit	http://www.hashatit.com

Keybase	https://keybase.io
Keyhole	http://keyhole.co
Klear	http://klear.com
Kred	http://kred.com
ManyContacts Mail Check	https://www.manycontacts.com/en/mail-check
Mention	https://mention.com
MustBePresent	http://mustbepresent.com
netlytic	https://netlytic.org
Netvibes	http://www.netvibes.com
NUVI	https://www.nuvi.com
OpinionCrawl	http://www.opinioncrawl.com
Profilr	https://www.profilr.social/search/jsmith
Pulsar	https://www.pulsarplatform.com
Rival IQ	https://www.rivaliq.com
RSS Social Analyzer	https://chrome.google.com/webstore/detail/rss-social-analyzer/ncmajlpbfckecekfamgfkmckbpihjfdn?hl=en
Samdesk	https://www.samdesk.io
Sendible	https://www.sendible.com
Smaller Social Networks Search	https://inteltechniques.com/osint/smaller.social.networks.html
SocialBakers	http://www.socialbakers.com
SocialBlade	http://socialblade.com
Social DownORNot	http://social.downornot.com
Socialhome	https://socialhome.network
Social Media Monitoring Solutions	http://wiki.kenburbary.com/social-meda-monitoring-wiki
Social Mention	http://socialmention.com
Social Sear.ch	http://www.socialsear.ch
Social Searcher	http://www.social-searcher.com
SproutSocial	https://sproutsocial.com
Storyful Multisearch	https://chrome.google.com/webstore/detail/storyful-multisearch/hkglibabhninbjmaccpajiakojeacnaf?hl=en
Tagboard	https://tagboard.com
Trackur	http://www.trackur.com

UnionMetrics	https://unionmetrics.com
UVRX	http://www.uvrx.com/social.html
Visibrain	https://www.visibrain.com
Webometric	http://lexiurl.wlv.ac.uk
Zoho Social	https://www.zoho.com/social/social-media-monitoring.html

Social Media Tools: Twitter

Tool	Link
AccountAnalysis	https://accountanalysis.lucahammer.com
AllDeletedTweets From Politicians	https://politwoops.com/countries
AllMyTweets	https://www.allmytweets.net/connect
audiense	https://audiense.com
Backtweets	http://backtweets.com
Birdwatcher	https://n0where.net/twitter-osint-framework
Blue Nod	http://bluenod.com
Botcheck.me	https://botcheck.me
Botometer	https://botometer.iuni.iu.edu
Burrrd	https://burrrd.com
BU-TCAT	http://www.bu.edu/com/research/bu-tcat/#left-sidebar
Charm	http://charm.benapps.net
Chorus	http://chorusanalytics.co.uk/chorus/request_download.php
Commun.it	http://commun.it
COSMOS	http://socialdatalab.net/software
Custom Twitter Tools	https://inteltechniques.com/menu.html
Deadbird	https://keitharm.me/project/deadbird
Discover Text	https://discovertext.com
DMI-TCAT	https://github.com/digitalmethodsinitiative/dmi-tcat
doesfollow	https://doesfollow.com
Download Twitter Video	http://www.downloadtwittervideo.com
Echosec	https://app.echosec.net
Fake Follower Check	https://fakers.statuspeople.com

First Tweet	http://ctrlq.org/first
FlipFeed	https://flipfeed.media.mit.edu
Foller.me	http://foller.me
Followerwonk	http://followerwonk.com
Followthehashtag	http://www.followthehashtag.com
GeoSocial Footprint	http://geosocialfootprint.com
Geotweet	http://geotweet.altervista.org
GetTwitterID	http://gettwitterid.com
Gigatweeter	http://gigatweeter.com
HappyGrumpy	https://www.happygrumpy.com
Hashtagify	http://hashtagify.me
Hashtags.org	http://www.hashtags.org
InTweets	http://intweets.com
Jooicer	https://jooicer.com
Keyhole	http://keyhole.co
Klear	https://klear.com
Lakako	https://www.lakako.com/twitter
Lazqa	http://www.lazqa.com
ManageFlitter	http://manageflitter.com
MentionMapp	http://mentionmapp.com
My Twitter ID	http://mytwitterid.com
nowTweets	http://nowtweets.com
OneMillionTweetMap	http://onemilliontweetmap.com
Quarter tweets	http://qtrtweets.com/twitter
Queryfeed	https://queryfeed.net
RiteTag	https://ritetag.com
SaveVideo	http://savevideo.me
Sentiment140	http://www.twittersentiment.appspot.com
Silver Bird	https://chrome.google.com/webstore/detail/silver-bird/encaiiljifbdbjlphpgpiimidegddhic?hl=en
Sleeping Time	http://sleepingtime.org
SnapBird	http://snapbird.org
Social Bearing	http://www.socialbearing.com

Social Rank First Follower	http://socialrank.com/firstfollower
SocioViz	http://socioviz.net
Spoonbill	https://spoonbill.io
tagboard	https://tagboard.com
Tagdef	https://tagdef.com
TAGS	https://tags.hawksey.info
Thread Reader	https://threadreaderapp.com
Tinfoleak	https://tinfoleak.com
Treeverse	https://chrome.google.com/webstore/detail/treeverse/aahmjdadniahaicebomlagekkcnlcila
Trends24	http://trends24.in
TrendsMap	http://trendsmap.com
Twayback Machine	http://staringispolite.github.io/twayback-machine
Twazzup	http://www.twazzup.com
twbirthday	http://twbirthday.com
TwChat	http://twchat.com
TWDOWN	https://twdown.net
TweepDiff	http://tweepdiff.com
Tweeple Search	https://tweeplesearch.com
Tweepsect	http://tweepsect.com
Tweepsmap	http://tweepsmap.com
Tweet Archiver	https://chrome.google.com/webstore/detail/twitter-archiver/pkanpfekacaojdncfgbjadedbggbbphi?hl=en
TweetArchivist	http://www.tweetarchivist.com
Tweetbeaver	https://tweetbeaver.com
Tweet Chat	http://www.tweetchat.com
TweetDeck	https://www.tweetdeck.com
TweeterID	https://tweeterid.com
TweetMap	http://mapd.csail.mit.edu/tweetmap
TweetMap	https://www.mapd.com/demos/tweetmap
Tweet Mapper	https://keitharm.me/projects/tweet
Tweetpaths	http://www.tweetpaths.com
TweetPsych	http://tweetpsych.com

Tweetreach	http://tweetreach.com
Tweets_analyzer	https://github.com/x0rz/tweets_analyzer
TweetStats	http://www.tweetstats.com
Tweet Tag	http://www.tweet-tag.com
TweetTunnel	http://tweettunnel.com
Twellow	http://www.twellow.com
Tweriod	http://www.tweriod.com
Twiangulate	http://www.twiangulate.com
Twicsy	http://twicsy.com
Twilert	http://www.twilert.com
Twime	http://www.twimemachine.com
Twint	https://github.com/haccer/twint
Twimap	https://twimap.com
Twipho	http://www.twipho.net
TwiSSR	http://www.twissr.com
Twitonomy	http://www.twitonomy.com
TwitRSS	https://twitrss.me
Twitter Account Details	http://www.twitteraccountsdetails.com
Twitter Advanced Search	https://twitter.com/search-advanced?lang=en
Twitter Audit	https://www.twitteraudit.com
Twitter BFTD	https://github.com/misterch0c/twitterBFTD
Twitter Chat Schedule	http://tweetreports.com/twitter-chat-schedule
Twitter Counter	http://twittercounter.com
Twitterfall	http://twitterfall.com
Twitter List Copy	http://projects.noahliebman.net/listcopy/index.php
Twitter Search	http://search.twitter.com
Twitter Search Tools	https://inteltechniques.com/menu.html
Twlets	http://www.twlets.com
Twopcharts	http://twopcharts.com
twoogel	http://twoogel.com
twXplorer	https://twxplorer.knightlab.com
TWUBS Twitter Chat	http://twubs.com/twitter-chats

unfollowgram	https://unfollowgram.com
Video Downloader for Twitter	http://www.downloadtwittervideo.com
Warble	https://warble.co

Social Media Tools: Facebook

Tool	Link
Agora Pulse	http://barometer.agorapulse.com
Aware Online Facebook Graph Search	https://www.aware-online.com/tips-voor-osint/facebook-graph-search/
Bulk Facebook ID Finder	http://seotoolstation.com/bulk-facebook-id-finder
Commun.it	http://commun.it
Custom Facebook Tools	https://inteltechniques.com/osint/facebook.html
Deturl.com Video Download	http://deturl.com/www.youtube.com/watch?v=uqnqLrakxY8
DownFacebook	http://www.downfacebook.com
Dredown	http://www.dredown.com
Expand All Facebook Comments	http://com.hemiola.com/2015/08/29/expand-all
ExtractFace	http://le-tools.com/ExtractFace.html#download
Facebook Like Checker	http://www.fblikecheck.com
Facebook Livemap	https://www.facebook.com/livemap
Facebook People Search	https://www.facebook.com/people-search.php
Facebook Search	https://search.fb.com
Facebook Search Tool	http://netbootcamp.org/facebook.html
Facebook Search Tools	https://inteltechniques.com/osint/facebook.html
Facebook Video Downloader	http://fbdown.net
Fanpage Karma	http://www.fanpagekarma.com
FB DOWN	https://www.fbdown.net
FB Scan Tool	http://pitoolbox.com.au/facebook-tool

Fb-sleep-stats	https://github.com/sqren/fb-sleep-stats
Find my Facebook ID	http://findmyfbid.com
Graph Tips	http://graph.tips
LikeAlyzer	http://likealyzer.com
Lookup-ID.com	https://lookup-id.com
peoplefindThor	https://www.peoplefindthor.dk
SaveVideo	http://savevideo.me
SearchIsBack	https://searchisback.com
Signal	https://signal.fb.com
Socialider Facebook Search	https://www.socialider.com/fbsearch
Social Fixer for Facebook	https://chrome.google.com/webstore/detail/social-fixer-for-facebook/ifmhoabcaeehkljcfclfiieohkohdgbb?hl=en
Socialsearching	http://socialsearching.info/#/fb
Socmint Tools	http://socmint.tools
StalkFace	https://stalkface.com
stalkscan	https://stalkscan.com
Wallfux	https://www.wallflux.com
Who posted what?	https://whopostedwhat.com
Wolfram Alpha Facebook Report	http://www.wolframalpha.com/input/?i=facebook+report
YouTube Comment Scraper	http://ytcomments.klostermann.ca
Zesty Facebook Search	http://zesty.ca/facebook

Social Media Tools: Google+

Tool	Link
CircleCount	http://www.circlecount.com
Google Plus Search	http://googleplussearch.chromefans.org
Lakako	https://www.lakako.com/google-plus
PlusFeed	http://plusfeed.frosas.net

Social Media Tools: Instagram

Tool	Link
Blocked and Banned Instagram Hashtag Search	http://thedatapack.com/tools/blocked-hashtag-search
Chrome IG Story	https://chrome.google.com/webstore/detail/chrome-ig-story/bojgejgifofondahckoaahkilneffhmf
Commun.it	https://commun.it
Custom Instagram Search Tools	https://inteltechniques.com/osint/instagram.html
DownloadGram	https://downloadgram.com
Find Instagram User ID	https://codeofaninja.com/tools/find-instagram-user-id
gramrix	https://gramrix.com
Hashtagify	http://hashtagify.me
Helper Tools for Instagram	https://chrome.google.com/webstore/detail/helper-tools-for-instagra/hcdbfckhdcpepllecbkaaojfgipnpbpb
Iconosquare	http://iconosquare.com
ImgToon	https://imgtoon.com
Ink361	http://ink361.com
Instagram User ID Finder	https://www.otzberg.net/iguserid/index.php
Instagram Search Tool	http://netbootcamp.org/instagram.html
Instagram User ID	http://www.ershad7.com/InstagramUserID
InstaLooter	https://github.com/althonos/InstaLooter
INSTATAGZ	http://instatagz.com
Instidy	http://instidy.com
Keyhole	http://keyhole.co
Lakako	https://www.lakako.com
Mininsta	http://mininsta.net
mulpix	https://mulpix.com

Mundimago Search People	http://www.mundimago.com/profile/search
Picbear	http://picbear.com
Picodash	https://www.picodash.com
Pictame	http://www.pictame.com
SnapMap	https://snapmap.knightlab.com
Social Rank	https://www.socialrank.com
Someture	http://someture.com
tailwind	https://www.tailwindapp.com
Tofo.me	https://tofo.me
Vibbi Instagram Web Viewer	https://vibbi.com/viewer
Webstagram	https://web.stagram.com/search
Websta	http://websta.me
Worldcam	http://worldc.am
Yooying	https://www.yooying.com

Social Media Tools: Pinterest

Tool	Link
Pingroupie	http://pingroupie.com
Pinterest Guest	https://addons.mozilla.org/en-US/firefox/addon/pinterest-guest
tailwind	https://www.tailwindapp.com

Social Media Tools: Reddit

Tool	Link
Ceddit	https://ceddit.com/r/all
Imgur	http://imgur.com
Karma Decay	http://karmadecay.com
Metareddit	http://metareddit.com
Mostly Harmless	http://kerrick.github.io/Mostly-Harmless/#features
Reddit All Comments Viewer Secure	https://chrome.google.com/webstore/detail/reddit-all-comments-viewe/hgpgeobpjpchpmkecjppgcnekmbibgbi?hl=en-GB
Reddit Archive	http://www.redditarchive.com
Reddit List	http://redditlist.com
Reddit Investigator	http://www.redditinvestigator.com
Reddit Metrics	http://redditmetrics.com
Reddit Suite	https://chrome.google.com/webstore/detail/reddit-enhancement-suite/kbmfpngjjgdllneeigpgjifpgocmfgmb
Reddit User Analyser	https://atomiks.github.io/reddit-user-analyser
Reddit Watch	https://redditwatch.com
Redective	http://redective.com
Reditr	http://reditr.com
Reeddit	https://reedditapp.com
ReSavr	https://www.resavr.com
Savvit.io	http://savvit.io
SnoopSnoo	http://snoopsnoo.com
Subreddits	http://subreddits.org

TopIAmA	https://www.topiama.com
uforio	http://uforio.com
Un-Delete Reddit Comments	https://chrome.google.com/webstore/detail/un-delete-reddit-comments/goelkfmlebeihlnanaindammeonplnhi

Social Media Tools: VKontakte

Tool	Link
Дезертир	http://vk.com/app3046467
Barkov.net	http://vk.barkov.net
Find Face	http://findface.ru
Report Tree	http://dcpu.ru/vk_repost_tree.php
Social Stats	http://socialstats.ru
SnRadar	http://snradar.azurewebsites.net
Spotlight	http://spotlight.svezet.ru
Target Hunter	https://targethunter.net
Target Log	http://targetolog.com
VK5	http://vk5.city4me.com
VK Community Search	http://vk.com/communities
VK Parser	http://vkparser.ru
VK People Search	http://vk.com/people
VK to RSS Appspot	http://vk-to-rss.appspot.com
vMetaDate	https://gist.github.com/cryptolok/8a023875b47e20bc5e64ba8e27294261

Social Media Tools: Tumblr

Tool	Link
Searchlr	http://searchlr.net
Tumblr Originals	http://studiomoh.com/fun/tumblr_originals
Tumblr Search	http://www.tumblr.com/search

Social Media Tools: LinkedIn

Tool	Link
Custom LinkedIn Search by Country	https://inteltechniques.com/osint/linkedin.country.html
Dux-Soup	http://www.dux-soup.com
Find Anyone's Email	https://chrome.google.com/webstore/detail/find-anyones-email-contac/jjdemeiffadmmjhkbbpglgnlgeafomjo
FTL	https://chrome.google.com/webstore/detail/ftl/lkpekgkhmldknbcgjicjkomphkhhdkjj?hl=en-GB
Linkedin2username	https://github.com/initstring/linkedin2username
LinkedIn Guest Browser	https://addons.mozilla.org/en-US/firefox/addon/linkedin-guest-browser
raven	https://github.com/0x09AL/raven
ScrapedIn	https://github.com/dchrastil/ScrapedIn
socilab	http://socilab.com
the-endorser	https://github.com/eth0izzle/the-endorser

Social Media Tools: Snapchat

Tool	Link
FindMySnap	http://findmysnap.com
snapdex	https://www.snapdex.com
Snap Map	https://map.snapchat.com
Snap VIP	https://snapvip.io
Somechater	http://somechater.com

Social Media Tools: WhatsApp

Tool	Link
WhatsAllApp	https://github.com/LoranKloeze/WhatsAllApp
WhatsApp Fake Chat	http://www.fakewhats.com/generator
whatsfoto	https://github.com/zoutepopcorn/whatsfoto

Social Media Tools: Skype

Tool	Link
CyberHub Resolver	http://cyber-hub.net/resolver.php
Web Resolver	https://webresolver.nl

Social Media Tools: Telegram

Tool	Link
Save-telegram-chat-history	https://github.com/pigpagnet/save-telegram-chat-history
Telegram Channels Catalog	https://tchannels.me
Telegram Search	http://tsear.ch

Other Instant Messaging and Chat Tools

Tool	Link
Botbot.me	https://botbot.me
icq	https://icq.com/people
IRC Search	http://irc.netsplit.de/channels/search.php
ircsnapshot	https://github.com/bwall/ircsnapshot
mibbit	http://mibbit.com

Dating Apps

Tool	Link
Dating Apps and Sites for Investigators by Emmanuelle Welch	https://start.me/p/VRxaj5/dating-apps-and-sites-for-investigators

Blogs, Forums, Discussion Boards, and Q&A Sites

Blog Search

Tool	Link
Bloghunt	https://bloghunt.me
BlogSeacrhEngine	http://www.blogsearchengine.org
NetworkedBlogs	http://www.networkedblogs.com
Notey	https://www.notey.com
Twingly	http://www.twingly.com
Webhose.io	https://webhose.io

Forums and Discussion Boards Search

Tool	Link
BoardReader	http://boardreader.com
Delphi Forums	http://www.delphiforums.com
Facebook Groups	https://www.facebook.com
Foren User	http://www.forenuser.de
Google Groups	https://groups.google.com
Hoood.de	http://www.hoood.de
Linkedin Groups	http://www.linkedin.com
Ning	http://www.ning.com
Xing Groups	https://www.xing.com/communities
Webhose.io	https://webhose.io
Yahoo Groups	https://groups.yahoo.com

Q&A Sites

Tool	Link
Answers.com	http://www.answers.com
Ask	http://www.ask.com
Ask.fm	https://ask.fm
eHow	http://www.ehow.com
gutefrage	https://www.gutefrage.net
Quora	http://www.quora.com
StackExchange	http://stackexchange.com
Yahoo Answers	http://answers.yahoo.com

People Investigations

Main People Search Tools and Engines

Tool	Link
411 (US)	http://www.411.com
Addresses (US)	http://www.addresses.com
Alumni.net	http://www.alumni.net
AnyWho (US)	https://www.anywho.com/whitepages
Classmates	http://www.classmates.com
CrunchBase	http://www.crunchbase.com
Custom Person Search Tool	https://inteltechniques.com/osint/person.html
Data.com Connect	https://connect.data.com
dataScrape	https://github.com/khayes-r7/dataScrape
Discoverly	https://chrome.google.com/webstore/detail/discoverly-for-gmail-link/dijhcpbkalfgkcebgoncjmfpbamihgaf || https://discover.ly
Gaddr	https://gaddr.me
facesearch	http://facesaerch.com
FTL	https://chrome.google.com/webstore/detail/fullcontact-for-gmail/cnaibnehbbinoohhjafknihmlopdhhip
GPSies	https://www.gpsies.com/trackList.do
Gravatar	http://en.gravatar.com
Hey Press (Search for Journalists)	https://www.hey.press
HowManyOfMe	http://howmanyofme.com/search
HIRETUAL	https://chrome.google.com/webstore/detail/hiretual-10x-faster-talen/jeablngoapekimaeoeclgcefdcpjhjcg

Intelius (US)	https://www.intelius.com
Itools	http://itools.com/search/people-search || http://itools.com/tool/wink-people-search
John Doe (US)	https://johndoe.com
Keybase	https://keybase.io
LittleSis	https://littlesis.org
LookUp	http://www.lookup.com
LookUpUK	http://www.lookupuk.com
ManyContacts Mail Check	https://www.manycontacts.com/en/mail-check
MarketVisual	http://www.marketvisual.com
NameScan	https://namescan.io
Neighbor Report	https://neighbor.report
Nextdoor	https://nextdoor.com
Nuwber	https://nuwber.com
Nuwber	https://nuwber.co.no
peekyou	https://www.peekyou.com
Peoplefinders (US)	https://www.peoplefinders.com
People Looker (US)	https://www.peoplelooker.com
People Search	http://netbootcamp.org/peoplesearch.html
People Search (Australia)	http://www.peoplesearch.com.au
PeopleSmart (US)	https://www.peoplesmart.com
PersonLookup.com	http://www.personlookup.com
FastPeopleSearch (US)	https://www.fastpeoplesearch.com
PimEye	https://pimeyes.com/en
pipl	https://pipl.com
Profile Engine	http://profileengine.com
Profilr	https://www.profilr.social/search/jsmith
Recruit'em	http://recruitin.net
Research.com (US)	https://www.research.com
Reverse Genie	http://www.reversegenie.com
Skimleads	http://skimleads.com
Skipease (US)	http://www.skipease.com
Smugmug	https://www.smugmug.com/search

Snitch.name	http://www.snitch.name
Snoop Station (US)	http://snoopstation.com
Social catfish	https://socialcatfish.com
Speedy Hunt (US)	https://speedyhunt.com
Spokeo	http://www.spokeo.com
Spytox (US)	https://www.spytox.com
Strava	https://labs.strava.com/heatmap
TalentBin	https://www.talentbin.com
TruePeopleSearch (US)	https://www.truepeoplesearch.com
ufind.me	http://ufind.name
UserSearch	https://usersearch.org
USSEARCH (US)	https://www.ussearch.com
WebMii	http://www.webmii.com
Yasni	http://www.yasni.com
Zoominfo	http://www.zoominfo.com

Address & Contact Information Search

Tool	Link
118172	https://www.118712.fr
192 (UK)	http://www.192.com
411 (US)	http://www.411.com
Addresses (US)	http://www.addresses.com
Address Search (US)	http://www.addresssearch.com
AnyWho (US)	https://www.anywho.com/yellow-pages
Australia Lookup	http://www.australialookup.com
BeenVerified (US)	https://www.beenverified.com
Canada411(Canada)	http://www.canada411.ca
Data 24-7	https://www.data24-7.com
Find People Search (US)	http://www.findpeoplesearch.com
HomeMetry	https://homemetry.com
Infobel	http://www.infobel.com/en/world
John Doe (US)	https://johndoe.com
PeopleSmart (US)	https://www.peoplesmart.com
FastPeopleSearch (US)	https://www.fastpeoplesearch.com
SearchBug (US)	http://www.searchbug.com
Spytox (US)	https://www.spytox.com
That'sThem	https://thatsthem.com
TruePeopleSearch (US)	https://www.truepeoplesearch.com
USSearch (US)	https://www.ussearch.com
Verispy (US)	https://www.verispy.com/people-search
White Pages	http://www.whitepages.com
whowhere	http://www.whowhere.com

Zabasearch	http://www.zabasearch.com

Public Records

Tool	Link
Advanced Background Checks (US)	https://www.advancedbackgroundchecks.com
Australia Public Records	http://australiapublicrecord.com
Birth Database	http://www.birthdatabase.com
Black Book Online (US)	https://www.blackbookonline.info
BRBPub.com	http://www.brbpub.com
Crime Reports (US)	https://www.crimereports.com
Criminal Searches (US)	https://www.criminalsearches.com
Cubib (US)	http://cubib.com
DOBSEARCH	https://www.dobsearch.com
Family Watchdog (US)	https://www.familywatchdog.us
Federal Bureau of Prisons - Inmate Locator (US)	http://www.bop.gov/inmateloc
Felon Spy (US)	http://www.felonspy.com
Find A Grave (US)	https://www.findagrave.com
Find People Search (US)	https://findpeoplesearch.com
Fold3 (US Military Records)	http://www.fold3.com
Free Public Records Directory (US)	http://publicrecords.onlinesearches.com
golookup (US)	https://golookup.com
GOVDATACA (Canada)	https://govdataca.com
Grave Info (US)	http://www.graveinfo.com
Inmate Locator (US)	http://www.theinmatelocator.com
Inmate Locator (US)	https://www.bop.gov/inmateloc
Intelius (US)	https://www.intelius.com
Interment (Cemetery Records)	http://www.interment.net/data/search.htm

Instant Checkmate	https://www.instantcheckmate.com
Investigative Dashboard Search	https://data.occrp.org
Legacy.com (US)	http://www.legacy.com
Melissa (US)	http://melissadata.com
NETR ONLINE (US)	https://publicrecords.netronline.com
NSOPW (US)	https://www.nsopw.gov/en/Search/Verification
Orbituaries Australia	http://oa.anu.edu.au
Peoplefinder (US)	https://www.peoplefinders.com
Political MoneyLine (US)	http://www.politicalmoneyline.com
Public Info Directory (US)	https://publicrecords.directory
Public Records (Australia)	https://www.publicrecords.com.au
Radaris	http://radaris.com
RecordsPedia	http://recordspedia.com
Reunion (US)	http://www.reunion.com
SCRA Website (US)	https://scra.dmdc.osd.mil/scra/#/home
Sorted by Birth Date	http://sortedbybirthdate.com
Speedy Hunt	https://speedyhunt.com
SSN Validator	https://www.ssnvalidator.com
UniCourt	https://unicourt.com
USSEARCH (US)	https://www.ussearch.com
Voter Registration Records (US)	https://voterrecords.com

Ancestry Research

Tool	Link
Ancestor Hunt	http://ancestorhunt.com
Ancestry	http://www.ancestry.com
Family Search	https://familysearch.org
FamilyTreeNow	http://www.familytreenow.com
Find my past	https://search.findmypast.com/search-world-records
Forebears	http://forebears.io
FreeBMD	https://www.freebmd.org.uk
Genealogy	https://www.genealogy.com
Genealogy Bank	http://www.genealogybank.com
Genealogy in Time	http://www.genealogyintime.com
Genealogy Links	http://www.genealogylinks.net
Locate Family	https://www.locatefamily.com
Mocavo	https://www.findmypast.com/mocavo-info
The National Archives UK	http://www.nationalarchives.gov.uk
Rootsweb	http://home.rootsweb.ancestry.com
Search for Ancestors	http://www.searchforancestors.com
Sorted By Name	http://sortedbyname.com

Phone Search

Tool	Link
411 (US)	https://www.411.com/reverse-phone
Abc telefonos	http://www.abctelefonos.com
Addresses (US)	http://www.addresses.com
AnyWho (US)	https://www.anywho.com/reverse-lookup
Australia Lookup	http://www.australialookup.com
Blacklist Checker	https://imei24.com/blacklist_check
Bmobile.in	https://bmobile.in
British Phone Book	http://www.britishphonebook.com
BT Phone Book	https://www.thephonebook.bt.com
CallerID Service	https://secure.calleridservice.com
CallerID Test	https://www.calleridtest.com
CallerSmart	https://www.callersmart.com
Carrier Lookup	https://www.carrierlookup.com
Carrier Lookup Service	http://freecarrierlookup.com
CellRevealer	https://cellrevealer.com
CountryCode	https://countrycode.org
Custom Telephone Search	https://inteltechniques.com/OSINT/telephone.html
FastPeopleSearch (US)	https://www.fastpeoplesearch.com
Fone Finder	http://www.fonefinder.net
Free Carrier Lookup (US)	https://freecarrierlookup.com
golookup	https://golookup.com
IMEI24	https://imei24.com
International Numbering Plans	https://www.numberingplans.com

International White and Yellow Pages	http://www.wayp.com
Ivycall	http://www.ivycall.com
John Doe (US)	https://johndoe.com
Keecall (US)	http://www.keecall.us
Leaked Source	https://leakedsource.ru
MailTester	http://mailtester.com/testmail.php
MrNumber (US)	http://mrnumber.com/1-888-742-0000
nextcaller	https://nextcaller.com
Number Guru	https://www.numberguru.com
NumberVille	https://numberville.com
numberway	https://www.numberway.com
numpi	https://numpi.com
NumSpy	https://bhattsameer.github.io/numspy
peoplebyname	http://www.peoplebyname.com
People Call	https://www.peoplecall.com
Peoplefinders (US)	https://www.peoplefinders.com
People Looker (US)	https://www.peoplelooker.com
PeopleSmart (US)	https://www.peoplesmart.com
Phone Book of the World	http://pbof.com
phoneowner	https://phoneowner.com
PhoneSearchFree (US)	https://www.phonesearchfree.com
Phone Tools	https://inteltechniques.com/osint/telephone.html
PhoneValidator	https://www.phonevalidator.com
Open Cnam	https://www.opencnam.com
Reverse Genie (US)	http://www.reversegenie.com/phone.php
SearchYellowDirectory	http://www.searchyellowdirectory.com
Snusbase	https://snusbase.com
Social catfish: Reverse Phone Lookup	https://socialcatfish.com/reverse-phone-lookup
Speedy Hunt	https://speedyhunt.com
Spy Dialer (US)	https://www.spydialer.com
Spy on Caller	http://spyoncaller.net

Spytox (US)	https://www.spytox.com
Sync.me	https://sync.me
Telefonbuch	http://www.telefonbuch.com
TextMagic Free Carrier Lookup	https://www.textmagic.com/free-tools/carrier-lookup
That's Them: Reverse Phone Lookup	https://thatsthem.com/reverse-phone-lookup
Truecaller	https://www.truecaller.com
TruePeopleSearch (US)	https://www.truepeoplesearch.com
Twilio	https://www.twilio.com/lookup
USPhoneBook	https://www.usphonebook.com
USSEARCH (US)	https://www.ussearch.com
Whocalld	https://whocalld.com
Vigilante	https://www.vigilante.pw
Zonzoo	http://zonzoo.nl

E-mail Search / E-mail Check

Tool	Link
411 (US)	http://www.411.com
Ashley Madison Hack	https://ashley.cynic.al
BotScout	https://botscout.com/search.htm
BreachAlarm	https://breachalarm.com
BriteVerify Email Verification	http://www.briteverify.co.uk
Cellular Email Assumptions	https://inteltechniques.com/osint/cellperm.html
Clearbit Connect	https://chrome.google.com/webstore/detail/clearbit-connect-supercha/pmnhcgfcafcnkbengdcanjablaabjplo?hl=en
Custom Email Search Tools	https://inteltechniques.com/osint/menu.email.html
DomainBigData	https://domainbigdata.com
Email4Corporations	https://sites.google.com/site/emails4corporations/home
Email Address Validator	http://www.email-validator.net
Email Assumptions	https://inteltechniques.com/osint/email.html
Email Checker	https://email-checker.net
EmailDrop	https://chrome.google.com/webstore/detail/emaildrop-extract-emails/peilgijmhiocdmdeglhiljipigamfbjh
Email Extractor	https://chrome.google.com/webstore/detail/email-extractor/jdianbbpnakhcmfkcckaboohfgnngfcc?hl=en
Email Extractor	http://emailx.discoveryvip.com

Email Extractor Lite	http://eel.surf7.net.my
Email Format	http://email-format.com
Email Generator	http://emailgenerator.io
Email Guesser	http://www.guesser.email
Email Header Analyzer	https://mxtoolbox.com/EmailHeaders.aspx
EmailHippo	https://tools.verifyemailaddress.io
Email Hunter	https://hunter.io
Email Location	http://www.melissadata.com/lookups/email-location.asp
emailmatcher	https://emailmatcher.com
Email Permutator+	http://metricsparrow.com/toolkit/email-permutator
Emails4corporations	https://sites.google.com/site/emails4corporations/home
EmailSearch.org	http://www.email-search.org/search-emails
Email Validator	https://www.email-validator.net
FindThatLead	https://findthatlead.com
Free Email Verifier	http://verify-email.org
Gawker Hack Email Check	https://labs.duo.com/gawker
Github-osint	https://github.com/hackstep/github-osint
Googligan Checker	https://gooligan.checkpoint.com
Gotcha	https://gotcha.pw
Gravatar Email Check	http://en.gravatar.com/site/check
Hacked Emails	https://hacked-emails.com
Have I Been Pwned	https://haveibeenpwned.com
Have I Been Sold	https://haveibeensold.app
headreach	https://headreach.com
HPI Identity Leak Checker	https://sec.hpi.uni-potsdam.de/ilc/search;jsessionid=A94B3A03C67B00F3B0FADB4A8C08E6FA

Hunter	https://hunter.io
Infoga	https://github.com/m4ll0k/infoga
Leaked Source	https://leakedsource.ru
Mail Jagger	https://mailjagger.ga
MailTester	http://mailtester.com/testmail.php
Many Contacts Email Check	https://www.manycontacts.com/en/mail-check
Melissa (US)	http://www.melissadata.com/lookups/emails.asp
OSINTTOOLKIT Email	https://osinttoolkit.github.io/EmailUsername
Peepmail	http://www.samy.pl/peepmail
People Looker (US)	https://www.peoplelooker.com
PeopleSmart (US)	https://www.peoplesmart.com
Pipl	https://pipl.com
Polities	https://www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html
Prospect Linked	https://prospectlinked.com
Public E-mail Records	http://publicemailrecords.com
Read Notify	http://www.readnotify.com
Reverse Genie E-mail	http://www.reversegenie.com/email.php
sellhack	https://sellhack.com
Snusbase	https://snusbase.com
Speedy Hunt	https://speedyhunt.com
SPYDialer	https://www.spydialer.com
Spytox (US)	https://www.spytox.com
TCIPUTILS.com Email Test	http://www.tcpiputils.com/email-test
That'sThem	https://thatsthem.com/reverse-email-lookup
Toofr	https://www.toofr.com
USSEARCH (US)	https://www.ussearch.com

Validate Email Address	https://validateemailaddress.org
Verifalia	http://verifalia.com/validate-email
Verify Email	https://verify-email.org
Verify Email Account	https://es.infobyip.com/verifyemailaccount.php
Verify Email Address	https://tools.verifyemailaddress.io
VoilaNorbert	https://www.voilanorbert.com

Username Check

Tool	Link
Check User Names	http://www.checkusernames.com
Custom User Name Search	https://inteltechniques.com/osint/username.html
Gaddr	https://gaddr.me
Knowem	http://www.Knowem.com
Leaked Source	https://leakedsource.ru
Lullar	http://com.lullar.com
Name Checkr	http://www.namecheckr.com
Name Chk	http://www.namechk.com
Namech_k.sh	https://github.com/HA71/Namechk
Name Vine	https://namevine.com
OSINTTOOLKIT Username	https://osinttoolkit.github.io/EmailUsername
peekyou	https://www.peekyou.com
pipl	https://pipl.com
Snitch.name	http://snitch.name
Snusbase	https://snusbase.com
Speedy Hunt (US)	https://speedyhunt.com
Spokeo	https://www.spokeo.com
Usercard	http://usercard.org
User Search	http://www.usersearch.org
User Sherlock	http://usersherlock.com
Vigilante	https://www.vigilante.pw
WhatsMyName	https://github.com/WebBreacher/WhatsMyName

CV and Resume Search

Tool	Link
Custom Hidden Resume Search	https://inteltechniques.com/osint/hidden.resumes.html
CVGadget	http://www.cvgadget.com
Indeed	https://www.indeed.com
LeadFerret	https://leadferret.com/search
Linkedin	https://www.linkedin.com
MarketVisual	http://www.marketvisual.com
Recruit'em	https://recruitin.net
Visualize.me	http://vizualize.me
XING	https://www.xing.com

Expert Search

Tool	Link
Academia	http://academia.edu
CanLaw	http://www.canlaw.com
expertfile	https://expertfile.com
ExpertiseFinder	http://www.expertisefinder.com
ExpertGuide	http://www.expertguide.com.au
ExpertPages	http://expertpages.com
Experts.com	http://www.experts.com
HARO	http://www.helpareporter.com
GlobalExperts	http://www.theglobalexperts.org
Idealist	http://www.idealist.org
Innocentive	http://www.innocentive.com
Internet Experts	http://www.internetexperts.info
Library of Congress: Ask a Librarian	http://www.loc.gov/rr/askalib
Maven	http://www.maven.co
MuckRack	http://muckrack.com
National Speakers Association	http://www.nsaspeaker.org
Newswise	http://www.newswise.com
Patent Attorneys/Agent Search	https://oedci.uspto.gov/OEDCI
PRNewswire	https://prnmedia.prnewswire.com
ProfNet	http://www.prnewswire.com/profnet
ReseacherID	http://www.researcherid.com
ScholarUniverse	http://www.scholaruniverse.com
SheSource	http://www.womensmediacenter.com/shesource
speakezee	https://www.speakezee.org

Sources	http://www.sources.com
TRExpertWitness	https://www.trexpertwitness.com
Zintro	https://www.zintro.com

Salary Search

Tool	Link
Adecco USA	https://www.adeccousa.com/resources/salary-calculator
AFL-CIO Executive Paywatch	https://aflcio.org/paywatch
CareerBliss	https://www.careerbliss.com/salary
Career Boutique	https://www.careerboutique.com/salary
Career Builder	https://www.careerbuilder.com
Career One Stop	https://www.careeronestop.org/Toolkit/Wages/find-salary.aspx
Glassdoor Salaries	https://www.glassdoor.com/Salaries/index.htm
Equilar	http://www.equilar.com
Indeed Salaries	https://www.indeed.com/salaries
Job Search Intelligence	https://www.jobsearchintelligence.com/etc/jobseekers/salary-calculator.php
Live Career	https://www.livecareer.com/salary
Monster Salary	https://www.monster.com/salary
Payscale	https://www.payscale.com/research/US/Country=United_States/Salary
Paysa	https://www.paysa.com/salaries-list/company
Pay Wizard	https://paywizard.org/main/salary/calculator#
RAPS.org	https://www.raps.org/careers/salary-calculator
Salary.com	https://www.salary.com
Salary Expert	https://www.salaryexpert.com

Simply Hired Salary Estimator	https://www.simplyhired.com/salaries
Salary List	http://www.salarylist.com
United States Department of Labor	https://www.bls.gov/ooh
US Experteer	https://us.experteer.com/salary_calculator
Wall Street Oasis Salary Search	https://www.wallstreetoasis.com/wso-company-database/salary

Creating a Sock Puppet

Tool	Link
Behind the Name	https://www.behindthename.com/random
Fake Identity Generator	http://backgroundchecks.org/justdeleteme/fake-identity-generator
Fake Name Generator	https://www.fakenamegenerator.com
Fake Person Generator	https://www.fakepersongenerator.com
Data Fake Generator	http://www.datafakegenerator.com/generador.php
List of Random Names	http://listofrandomnames.com
Name Fake	https://en.namefake.com
Random Name Generator	http://random-name-generator.info/random/?n=10&g=1&st
Sudo App	https://sudoapp.com

Company Research

Main Company Search Tools and Engines

Tool	Link
AIHIT	https://www.aihitdata.com
AllStocksLinks	http://www.allstocks.com/links
AngelList	https://angel.co
Annual Reports	http://www.annualreports.com
Big Red Directory	https://www.bigreddirectory.com
bikudo	https://www.bikudo.com
Bizeurope	http://www.bizeurope.com
Biznar	https://biznar.com
Bizstats	http://www.bizstats.co.uk
Bizstats	http://www.bizstats.com
Bloomberg	http://www.bloomberg.com/research/company/overview/overview.asp
brandchecker	https://brandchecker.com
Business Source	https://www.ebscohost.com/academic/business-source-complete
Bureau Van Dijk	http://www.bvdinfo.com
Buzzfile	http://www.buzzfile.com
Canadian Business Research	https://www.canada.ca/en/services/business/research.html
Canadian Business Resource	http://www.cbr.ca
Cedar Rose	https://www.cedar-rose.com
Checktrade	https://www.checkatrade.com

Comparably	https://www.comparably.com
CompeteShark	http://competeshark.com
Corporate Information	http://www.corporateinformation.com
Corporation Wiki	https://www.corporationwiki.com
CorpWatch	http://www.corpwatch.org
Crunchbase	https://www.crunchbase.com
Data.com Connect	https://connect.data.com
Dun & Bradstreet	https://www.dnb.com
EDGAR Online	http://www.edgar-online.com
Engineering 360	https://www.globalspec.com
Euromonitor	http://www.euromonitor.com
Europages	http://www.europages.co.uk
Ezilon	http://www.ezilon.com
Factiva	https://global.factiva.com
Forbes Global 2000	http://www.forbes.com/global2000/
Fortune Global 500	http://fortune.com/global500
Foursquare	https://foursquare.com
Glassdoor	https://www.glassdoor.com
globalEdge	http://globaledge.msu.edu
Google Finance	https://www.google.com
GuideStar	http://www.guidestar.org
Hoovers	http://www.hoovers.com
HotFrog	https://www.hotfrog.com
Inc. 5000	http://www.inc.com/inc5000
infobel	https://www.infobel.com
Infocif (Spain)	http://www.infocif.es
Info clipper	http://www.info-clipper.com
InstantLogoSearch	http://instantlogosearch.com
iSpionage	https://www.ispionage.com
Investigative Dashboard Search	https://data.occrp.org
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk

Linkedin	https://www.linkedin.com
LittleSis	https://littlesis.org
Mapped in Israel	https://mappedinisrael.com
Manta	https://www.manta.com
MarketLine	http://marketline.com
MarketVisual	http://www.marketvisual.com
Mergent Intellect	http://www.mergentintellect.com
Mergent Online	http://www.mergentonline.com/login.php
Mint Global	https://mintglobal.bvdinfo.com
Morningstar Research	http://library.morningstar.com
Notablist	https://www.notablist.com
orbis directory	https://orbisdirectory.bvdinfo.com
opencorporates	https://opencorporates.com
Owler	https://www.owler.com
Plunkett Research	http://www.plunkettresearchonline.com
The Public Register	http://www.annualreportservice.com
The Public Register	http://www.prars.com/search/alpha/A
Quandl	https://www.quandl.com
Report Linker	https://www.reportlinker.com
Ripoff Report	http://www.ripoffreport.com
Sqoop	https://sqoop.com
Skimleads	http://skimleads.com
SpyFu	https://www.spyfu.com
Startupexplore	https://startupxplore.com/en/startups
ThomasNet	https://www.thomasnet.com
Usercard	http://usercard.org
Vault	http://www.vault.com
Xing	http://www.xing.com
Yahoo Finance	https://finance.yahoo.com
Zauba Corp	https://www.zaubacorp.com
Zoominfo	https://www.zoominfo.com/companies-search

Company Research (EU)

Tool	Link
Bizeurope	http://www.bizeurope.com
Central and Eastern European Business Directory	http://www.ceebd.co.uk/ceebd
Company Registration Round the World	http://www.commercial-register.sg.ch/home/worldwide.html
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
De Telefoongids (Netherlands)	https://www.detelefoongids.nl
Europages	http://www.europages.co.uk
European Business Register	http://www.ebr.org
Ezilon	http://www.ezilon.com
Foursquare	https://foursquare.com
Global Business Register	http://www.globalbusinessregister.com
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
Libreborme	https://libreborme.net
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
opencorporates	https://opencorporates.com
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com
Startupexplore	https://startupxplore.com/en/startups

Company Research (UK)

Tool	Link
Big Red Directory	https://www.bigreddirectory.com
BizDB	http://www.bizdb.co.uk
Bizstats	http://www.bizstats.co.uk
Central and Eastern European Business Directory	http://www.ceebd.co.uk/ceebd
Claims Management Regulation – Authorised Business Register	https://www.claimsregulation.gov.uk/search.aspx
Companies in the UK	https://www.companiesintheuk.co.uk
Company Registration Round the World	http://www.commercial-register.sg.ch/home/worldwide.html
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Cylex (UK)	https://www.cylex-uk.co.uk
ELTO (UK)	https://eld.elto.org.uk
Elucify (UK)	https://www.elucify.com

Employment Tribunal Decisions (UK)	https://www.gov.uk/employment-tribunal-decisions
Europages	http://www.europages.co.uk
European Business Register	http://www.ebr.org
Ezilon	http://www.ezilon.com
Fair Trades	http://www.fairtrades.co.uk
Financial Conduct Authority Search (UK)	https://www.fca.org.uk/search-results?search_term=clone%20firm%20details&start=1&sort_by=dmetaZ
Foursquare	https://foursquare.com
Food Hygiene Ratings (UK)	https://www.scoresonthedoors.org.uk//index.php
Global Business Register	http://www.globalbusinessregister.com
iSpionage	https://www.ispionage.com
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
Kompass	https://www.kompass.com
Kyckrs	https://portal.kyckr.co.uk
Local Heroes	https://www.localheroes.com
My Builder	https://www.mybuilder.com
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
NicEic	http://www.niceic.com
Opening Times (UK)	https://www.opening-times.co.uk
orbis directory	http://orbisdirectory.bvdinfo.com/version-20161014/OrbisDirectory/Companies

opencorporates	https://opencorporates.com
Overseas Company Registers	https://www.gov.uk/government/publications/overseas-registries/overseas-registries
Scoot	http://www.scoot.co.uk
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com
Stall Finder	https://www.stallfinder.com
Tradesmen Corner (UK)	https://www.tradesmencorner.co.uk
Trustatrader	https://www.trustatrader.com
Trust Mark (UK)	https://www.trustmark.org.uk
Trust Pilot (UK)	https://uk.trustpilot.com
UK Companies List	https://www.companieslist.co.uk
UK Data	http://ukdata.com
Yell	https://www.yell.com

Company Research (US)

Tool	Link
Better Business Bureau	http://www.bbb.org
Business Source	https://www.ebscohost.com/academic/business-source-complete
Company Registration Round the World	http://www.commercial-register.sg.ch/home/worldwide.html
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Comparably	https://www.comparably.com
Corporation wiki	https://www.corporationwiki.com
EDGAR Online	http://www.edgar-online.com
Ezilon	http://www.ezilon.com
Foursquare	https://foursquare.com
Glassdoor	https://www.glassdoor.com
Global Business Register	http://www.globalbusinessregister.com
GuideStar	http://www.guidestar.org
Inc. 5000	http://www.inc.com/inc5000
iSpionage	https://www.ispionage.com
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
LinkSV	http://www.linksv.com
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers

Manta	https://www.manta.com
MarketLine	http://marketline.com
Mergent Online	http://www.mergentonline.com
Morning Star	http://www.morningstar.com
orbis directory	https://orbisdirectory.bvdinfo.com
opencorporates	https://opencorporates.com
Owler	https://www.owler.com
PrivCo	https://www.privco.com
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com
Stall Finder	https://www.stallfinder.com
Startupexplore	https://startupxplore.com/en/startups
Vault	http://www.vault.com
Wall street Oasis	https://www.wallstreetoasis.com/wso-company-database

Company Research (Switzerland)

Tool	Link
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
orbis directory	http://orbisdirectory.bvdinfo.com/version-20161014/OrbisDirectory/Companies
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com

Company Research (Middle East)

Tool	Link
Bahrain	*http://www.big.bh/einvestor.web*
Dubai	*https://www.difc.ae/setting-up*
Ezilon	*http://www.ezilon.com*
Israel	*http://www.justice.gov.il/En/Pages/default.aspx*
Jordan	*http://ccd.gov.jo*
Kompass	*https://www.kompass.com*
Kyckr	*https://portal.kyckr.co.uk*
Mapped in Israel	*https://mappedinisrael.com*
National Company Registers	*https://en.wikipedia.org/wiki/List_of_company_registers*
SEMrush	*https://www.semrush.com*
Skimleads	*http://skimleads.com*

Company Research (Africa)

Tool	Link
BCE (Senegal)	http://creationdentreprise.sn/rechercher-une-societe
CCI (Burkina Faso)	http://www.cci.bf/?q=fr/entreprise
CCIMA (Cameroon)	http://www.ccima.cm
Cedar Rose	https://www.cedar-rose.com
CEPICI (Ivory Coast)	https://www.cepici.ci
CIPC	http://www.cipc.co.za/za
Clarified By	https://www.clarifiedby.com
CNRC (Algeria)	https://sidjilcom.cnrc.dz
Companies and Intellectual Property Commission (South Africa)	https://eservices.cipc.co.za
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Directinfo.ma (Marocco)	https://www.directinfo.ma
Ezilon	http://www.ezilon.com
GUFE-RCA	http://gufe-rca.org
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
Nigeria Corporate Affairs Commission	http://new.cac.gov.ng
Registre de commerce de Tunisie	https://www.registre-commerce.tn
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com

South Africa	http://www.cipc.co.za/za

Company Research (China)

Tool	Link
China	https://www.cr.gov.hk
Ezilon	http://www.ezilon.com
Kompass	https://www.kompass.com
Kyckr	https://portal.kyckr.co.uk
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
SEMrush	https://www.semrush.com
Skimleads	http://skimleads.com

Business Registers (EU + EFTA)

Tool	Link
United Kingdom: Authorised Business Register	https://www.claimsregulation.gov.uk/search.aspx
United Kingdom: Companies House	https://www.gov.uk/government/organisations/companies-house
European Business Register	http://www.ebr.org
National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
Austria	http://www.justiz.gv.at/firmenbuch
Belgium	http://www.eurodb.be
Bulgaria	http://www.brra.bg
Cyprus	http://www.mcit.gov.cy/mcit/drcor/drcor.nsf/index_en/index_en?opendocument
Czech Republic	https://www.mfcr.cz
Denmark	https://datacvr.virk.dk/data
Estonia	https://ariregister.rik.ee/mobile/mobile/select
Finland	https://www.prh.fi/en/index.html
France	https://www.infogreffe.fr
France	https://www.inpi.fr
Germany	https://www.unternehmensregister.de/ureg/?submitaction=language&language=en
Greece	http://www.acci.gr/acci/shared/index.jsp?context=101
Hungary	https://www.e-cegjegyzek.hu
Iceland	https://www.rsk.is/english/individuals
Ireland	https://www.statice.is
Italy	http://www.infocamere.it/en/home
Latvia	https://www.ur.gov.lv/lv

Lithuania	http://www.registrucentras.lt/en
Luxembourg	https://www.rcsl.lu/mjrcs/jsp/IndexActionNotSecured.action?time=1525227992196&loop=2
Malta	https://registry.mfsa.com.mt/ROC
Netherlands	https://www.kvk.nl
Poland	https://www.ms.gov.pl/en/about-the-ministry-of-justice
Portugal	http://www.irn.mj.pt/IRN/sections/inicio
Romania	https://e-justice.europa.eu/content_business_registers-104-en.do
Slovakia	http://www.orsr.sk/default.asp?lan=en
Slovenia	https://www.ajpes.si/Iscem
Skimleads	http://skimleads.com
Spain	https://sede.registradores.org/contenido/buyingahouse
Spain	http://www.rmc.es/Home.aspx?lang=en
Sweden	http://www.bolagsverket.se
Norway	https://www.brreg.no
Principality of Lichtenstein	http://www.oera.li/hrweb/ger/firmensuche_afj.htm
Switzerland	https://www.zefix.admin.ch/de/search/entity/welcome
United Kingdom	https://www.gov.uk/government/organisations/companies-house

Business Registers (US)

Tool	Link
Alabama	https://sos.alabama.gov
Alaska	https://www.commerce.alaska.gov/CBP/Main
Arizona	http://www.azcc.gov/divisions/corporations
Arkansas	https://www.sos.arkansas.gov/business-commercial-services-bcs
California	http://www.sos.ca.gov
Colorado	http://www.sos.state.co.us
Connecticut	http://portal.ct.gov/sots
Delaware	https://corp.delaware.gov
Florida	http://www.miamidade.gov/businessexpress/start-register.asp
Georgia	http://sos.ga.gov
Hawaii	https://hbe.ehawaii.gov/BizEx/home.eb;jsessionid=FFFC59E1C1F6E7629F05499018074B2B.lana
Idaho	https://sos.idaho.gov
Indiana	http://www.in.gov/sos/business
Illinois	https://www2.illinois.gov/business
Iowa	https://sos.iowa.gov
Kansas	http://www.kssos.org/business/business.html
Kentucky	https://www.sos.ky.gov/Pages/default.aspx
Louisiana	https://www.sos.la.gov/BusinessServices/Pages/default.aspx
Maine	http://www.state.me.us/sos/cec/corp/index.html
Maryland	http://www.dat.state.md.us/Pages/default.aspx
Massachussets	https://www.mass.gov
Michigan	http://www.michigan.gov/business
Minnesota	https://mblsportal.sos.state.mn.us/Business/Search

Mississippi	http://www.sos.ms.gov/Pages/default.aspx
Missouri	https://www.sos.mo.gov/categories.asp?id=2
Montana	http://sos.mt.gov/business
Nebraska	http://www.nebraska.gov/#business
Nevada	https://nvsos.gov/sosentitysearch/corpsearch.aspx
New Hampshire	http://sos.nh.gov/nhbuslookup.aspx
New Jersey	http://www.nj.gov/treasury/revenue/
New Mexico	http://www.tax.newmexico.gov/default.aspx
New York	https://www.dos.ny.gov/
North Carolina	https://www.sosnc.gov/corporations/
North Dakota	https://apps.nd.gov/sc/busnsrch/busnSearch.htm
Ohio	http://business.ohio.gov
Oklahoma	http://www.state.ok.us/?c=4
Oregon	http://sos.oregon.gov/business/Pages/default.aspx
Pennsylvania	https://www.pa.gov
Rhode Island	http://www.ri.gov/business
South Carolina	http://www.scsos.com/Search%20Business%20Filings
South Dakota	http://sdsos.gov/business-services/default.aspx
Tennessee	https://sos.tn.gov/products/business-services/business-information-search-0
Texas	http://www.sos.state.tx.us/corp/index.shtml
Utah	https://corporations.utah.gov
Vermont	http://www.sec.state.vt.us
Virginia	https://www.scc.virginia.gov/index.aspx
Washington	http://access.wa.gov
West Virginia	https://sos.wv.gov/Pages/default.aspx
Wisconsin	http://www.wisconsin.gov/Pages/home.aspx
Wyoming	http://soswy.state.wy.us/Business/Default.aspx

Business Registers (Other)

Tool	Link
Andorra	https://www.ompa.ad
Aruba	http://www.arubachamber.com
Australia	http://www.asic.gov.au
Bahamas	http://www.bahamas.gov.bs/bahamasweb2/home.nsf/vContentW/99B49574E4044661852570180064 7AFB
Bermuda	http://www.roc.gov.bm
British Virgin Islands	http://www.bvifsc.vg
Canada	http://corporationscanada.ic.gc.ca/eic/site/cd-dgc.nsf/Intro
Colombia	http://www.confecamaras.org.co
Curacao	http://www.ruta-curacao.com
Gilbraltar	http://www.companieshouse.gi
Guernsey	http://www.guernseyregistry.com/homepage
India	http://www.mca.gov.in
Isle of Man	https://www.gov.im/categories/business-and-industries/companies-registry
Jersey	http://www.jerseyfsc.org
Malaysia	http://www.ssm.com.my
New Zealand	https://www.business.govt.nz
Philippines	http://www.sec.gov.ph
San Marino	https://www.cc.sm
Serbia	http://www.apr.gov.rs/Default.aspx?alias=www.apr.gov.rs
Singapore	https://www.acra.gov.sg
Sri Lanka	http://www.drc.gov.lk

Thailand	http://www.dbd.go.th/dbdweb_en/ewt_news.php?nid=3974

Business Registers Lists and Directories

Tool	Link
Business Reference Services	http://www.loc.gov/rr/business/company/directories.html
Central and Eastern European Business Directory	http://www.ceebd.co.uk/ceebd
Company Registration Around the World	http://www.commercial-register.sg.ch/home/worldwide.html
Company Research Resources by Country	http://www.rba.co.uk/sources/registers.htm
Europages	https://www.europages.com
European Business Register	http://www.ebr.org
Federation of International Trade Associations	http://www.fita.org/webindex/browse.cgi/Entering_International_Markets/Trade_Information_Business_Directories/international_Business_Directories/Europe_Trade_Directories/All_Europe_Directories
Global Business Register	http://www.globalbusinessregister.com
Global Edge	https://globaledge.msu.edu/global-resources/company-directories
Investigative Dashboard	https://investigativedashboard.org/databases
Knowledge guide to international company registration	http://www.icaew.com/en/library/subject-gateways/business-management/company-administration/knowledge-guide-international-company-registration
List of Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
Ministry of Economic Development of the Russian Federation	http://www.ved.gov.ru/eng/companies

National Company Registers	https://en.wikipedia.org/wiki/List_of_company_registers
Overseas Company Registers	https://www.gov.uk/government/publications/overseas-registries/overseas-registries
Recoupera	https://recoupera.com/countries-companies-registry
Santander Trade Portal	https://en.portal.santandertrade.com/reach-business-counterparts/business-directories?todo=valider&affichage=&pays_recherche=11&code_secteur=all&tri=#result

Job Search Resources

Tool	Link
Beyond	http://www.beyond.com
CampusCareerCenter	http://www.campuscareercenter.com
CareerBuilder	http://www.careerbuilder.com
College Recruiter	https://www.collegerecruiter.com
Craiglist	http://losangeles.craigslist.org
Dice	http://www.dice.com
Eluta (Canada)	http://www.eluta.ca
Eurojobs	https://www.eurojobs.com
Fish4Jobs	http://www.fish4.co.uk
Gigajob	https://www.gigajob.com
Glassdoor	https://www.glassdoor.com
Headhunter	http://www.headhunter.com
Indeed	http://www.indeed.com
JOBBÖRSE	https://jobboerse.arbeitsagentur.de
JobRobot	https://www.jobrobot.de
Jobs (Germany)	https://www.jobs.de
Jobs (Poland)	http://www.jobs.pl
Jobware (Germany)	https://www.jobware.de
Jobsite (UK)	http://www.jobsite.co.uk
Linkedin	https://www.linkedin.com
Monster	http://www.monster.com
Naukri (India)	http://www.naukri.com
Reed (UK)	http://www.reed.co.uk
Seek (Australia)	http://www.seek.com.au

SimplyHired	http://www.simplyhired.com
Stackoverflow Developer Jobs	https://stackoverflow.com
Stellenanzeigen.de	https://www.stellenanzeigen.de
StepStone	https://www.stepstone.de
whoishiring	https://whoishiring.me
Xing	http://www.xing.com
ZipRecruiter	https://www.ziprecruiter.com

Company Reviews

Tool	Link
CareerBliss Reviews	https://www.careerbliss.com/reviews
Comparably	https://www.comparably.com
Fairygoodbooss	https://fairygodboss.com
Glassdoor	https://www.glassdoor.com
Indeed	https://www.indeed.com/companies
The JobCrowd	https://www.thejobcrowd.com
Jobvoting	https://www.jobvoting.de
Kununu	https://www.kununu.com
LookBeforeYouLeap	http://www.lookbeforeyouleap.net
Meinchef	https://www.meinchef.de
Paysa	https://www.paysa.com
RateMyEmployer	http://www.ratemyemployer.ca
Seek	https://www.seek.com.au/companies
TargetJobs	https://targetjobs.co.uk
Vault	http://www.vault.com

Patent Research

Tool	Link
Advanced Google Patent Search	https://www.google.com/advanced_patent_search
AusPat IP Australia	http://pericles.ipaustralia.gov.au/ols/auspat/welcome.do;jsessionid=GhZjQ0fgjVF4sudf5kQ_8XW5haPebJTu6s55ZIWx6Kh8eh_HzFxk!199765566
Benelux Patent Platform (Belgium, The Netherlands and Luxemburg)	http://mijnoctrooi.rvo.nl/bpp-portal/home
Canada Intellectual Property Office	http://www.ic.gc.ca/opic-cipo/cpd/eng/search/basic.htm l
Common Citation Document FiveIPoffices	http://ccd.fiveipoffices.org/CCD-2.1.6
Danish Patent and Trademark Office	http://www.dkpto.org/online-tools/databases-(free-access).aspx
DPMA Register	https://register.dpma.de/DPMAregister/pat/einsteiger
Espacenet Patent Search (Europe)	https://worldwide.espacenet.com/help?topic=ecla&locale=en_EP&method=handleHelpTopic
European Patent Office	https://register.epo.org/regviewer
Finland Patent Search	https://patent.prh.fi/patinfo/default2.asp?Lng=
Free Patents Online Search	http://www.freepatentsonline.com/search.html
German Patent and Trade Mark Office	https://www.dpma.de/english/search/index.html
Google Patents	https://patents.google.com https://www.google.com/?tbm=pts
GOV.UK Patent Search	https://www.gov.uk/search-for-patent
INPI (France)	https://www.inpi.fr

Israel Patent Authority Database	http://www.ilpatsearch.justice.gov.il/UI/mainpage.aspx
Japan Patent Office	https://www.jpo.go.jp/cgi/linke.cgi?url=/torikumi_e/searchportal_e/classification.htm
Japan Platform for Patent Information	https://www.j-platpat.inpit.go.jp/web/all/top/BTmTopEnglishPage
Korea Intellectual Property Rights Information Service	http://engpat.kipris.or.kr/engpat/searchLogina.do?next=MainSearch
Marcaria Trademark Search	https://trademark-search.marcaria.com
Markenchk	http://www.markenchk.de
Norwegian Industrial Property Office	https://search.patentstyret.no
Office of General Patents (India)	http://ipindia.nic.in
Patent Genius	http://www.patentgenius.com
Patent Search (Spain)	http://consultas2.oepm.es/InvenesWeb/faces/busquedaInternet.jsp
PIZNET	http://www.piznet.de
Swedish Patent and Registration Office	https://www.prv.se/en/patents
Swiss Federal Institute of Intellectual Property	https://www.swissreg.ch/srclient/faces/jsp/start.jsp
UK Intellectual Property Office	https://www.ipo.gov.uk/p-ipsum.htm
United States Patent and Trademark Office (USPTO)	https://www.uspto.gov
USPTO Patent Full-Text and Image Database	http://patft.uspto.gov/netahtml/PTO/search-adv.htm
World Intellectual Property Organization (WIPO)	https://patentscope.wipo.int/search/en/advancedSearch.jsf
World Intellectual Property Organization (WIPO) Hague Express	http://www.wipo.int/designdb/hague/en

Tenders

Tool	Link
APEC Contracting: Tenders and Request for Proposals	https://www.apec.org/Projects/Tenders-and-RFPs
Department of Finance (UK)	https://www.finance-ni.gov.uk/topics/procurement
Development Business	https://www.devbusiness.com/Search/Search.aspx?PreLoadProjects=1
DG Market: Tenders Worldwide	https://www.dgmarket.com
Double Trade	https://www.doubletrade.com
Global Tenders	http://www.globaltenders.com
Infrastructure Civil Works & Construction Tenders	http://www.cwctenders.com
Medical Pharma Healthcare Tenders	http://www.medicaltenders.com/medical_tenders_gcc_countries.htm
Merx (Canada, US)	https://www.merx.com/English/NonMember.asp?WCE=Show&TAB=1&PORTAL=MERX&State=1&hcode=tAF08b5PaGBuUkl43CRDCg%3d%3d
Middle East Tenders Search	http://www.middleeasttenders.com/#20180326108
NSW eTendering	https://tenders.nsw.gov.au
SIMAP Information About European Public Procurement	http://simap.ted.europa.eu
South Australian Tenders & Contracts Website	https://www.tenders.sa.gov.au/tenders/index.do
Tenderio	http://www.tenderio.com
Tenderscope	http://www.tenderscope.com
Tender Link	https://www2.tenderlink.com
Tenders Info	http://www.tendersinfo.com
Tenders Page	https://tenderspage.com

Tenders VIC: Victorian Government Tenders System	https://www.tenders.vic.gov.au/tenders/tender/search/tender-search.do?action=advanced-tender-search-open-tender
The Federation of International Trade Associations	http://www.fita.org/webindex/browse.cgi/Entering_International_Markets/Government_and_Multinational_Procurement/Worldwide_Government_Procurement_Tenders/Europe_Government_Procurement_(Tenders)
Queensland Government Building and Asset Services eTender	https://www.hpw.qld.gov.au/bas/etender
United Nations Development Programme	http://procurement-notices.undp.org/search.cfm
United Nations Global Marketplace	https://www.ungm.org/Public/Notice

Charity, NGO, and Nonprofit Research

Tool	Link
Benefacts (Ireland)	https://benefacts.ie
Benevity Causes Portal	https://causes.benevity.org/causes/search
CAF America	https://cafa.iphiview.com/cafa/givenow/charitydatabasesearch/tabid/464/default.aspx
Charity Commission for England and Wales	https://www.gov.uk/government/organisations/charity-commission
Charity Intelligence	https://www.charityintelligence.ca/research/a-z-charity-listing
Charity Navigator	https://www.charitynavigator.org
Charity Watch	https://www.charitywatch.org
Citizen Audit	https://www.citizenaudit.org
Give.org National Charity Reports	https://give.org/charity-reviews/national
Google Custom Search Engine NGOs Search	https://cse.google.com/cse/home?cx=012681683249965267634:q4g16p05-ao
Government of Canada List of Charities	https://www.canada.ca/en/revenue-agency/services/charities-giving/charities-listings.html
Guide Star	https://www.guidestar.org/NonprofitDirectory.aspx
Illinois Attorney General Charitable Trust Database	http://charitableviewer.ilattorneygeneral.net
IRS Charities & Non-Profits A-Z Site Index	https://www.irs.gov/charities-non-profits/charities-non-profits-a-z-site-index
National Center for Charitable Statistics	http://nccs.urban.org
NYU Libraries NGO, Charity, and Non-Profit Resources	https://guides.nyu.edu/c.php?g=276965&p=1846647

Office of Massachusetts Attorney General Non-Profits & Charities Document Search	http://www.charities.ago.state.ma.us/charities
Open Charities	http://opencharities.org
UK Charity Commission	http://apps.charitycommission.gov.uk/Showcharity/RegisterOfCharities/registerhomepage.aspx
United Nations Department of Economic and Social Affairs NGO Branch	http://esango.un.org/civilsociety/login.do
State of California Department of Justice Charity Research Tool	https://oag.ca.gov/charities/charity-research-tool#Location:Default
Silicon Valley Global Charity Database	https://www.siliconvalleycf.org/ngo
The Chronicle of Philanthropy	https://www.philanthropy.com/data
WANGO Worldwide NGO Directory	http://www.wango.org/resources.aspx?section=ngodir

Real Estate Research

Real Estate Research

Tool	Link
Airbnb	https://www.airbnb.co.uk
Arivify (US)	https://www.arivify.com
Ananz	http://www.ananzi.co.za
Bigger Pockets	https://www.biggerpockets.com/rei
BlueBook International	http://www.bluebook.net
Bret Whissel Amortization Calculator	http://bretwhissel.net/amortization
Carmel Realty Company (CN)	http://www.carmelrealtycompany.cn/real-estate-listings-Carmel.htm
CBRE (Global)	https://www.cbre.us
Central 21 (Global)	https://www.century21.com
Colliers International	https://www2.colliers.com
CouchSurfing	https://www.couchsurfing.com
Digmap Real Estate Tools & Analysis	https://www.digmap.com/solutions/real-estate-analysis
Emporis	https://www.emporis.com
EuroResales	http://www.euroresales.com
FixMyStreet (UK)	https://www.fixmystreet.com
Freddie Mac	http://www.freddiemac.com/research
Funda (NL)	https://www.funda.nl
HomeFacts (US)	https://www.homefacts.com
HomeMetry (US)	https://homemetry.com

HouseShop (UK)	https://www.thehouseshop.com
iLocate (NL)	https://www.ilocate.nl
Institute for Real Estate Management	http://www.irem.org
Jaap (NL)	https://www.jaap.nl
Land.net (US)	http://www.land.net
LondonRentMyHouse	http://www.londonrentmyhouse.com
Loopnet (US)	http://www.loopnet.com
National Association of Realtors Directory of Real Estate Research Centers	https://www.nar.realtor/directories/directory-of-real-estate-research-centers
National Association of Realtors Research Reports	https://www.nar.realtor/research-and-statistics/research-reports
Placester Multiple Listing Service (MLS) Directory (US)	https://placester.com/mls-directory
PadMapper (US)	https://www.padmapper.com
People Looker (US)	https://www.peoplelooker.com
Realestate.com.au (AU)	https://www.realestate.com.au
Real Estate Navigator (US)	https://rehold.com
Realtor	https://www.realtor.com
Redfin (US)	https://www.redfin.com
Rehold (US)	https://rehold.com
Remax Global	https://global.remax.com
RightMove	http://www.rightmove.co.uk
SoldPrice	http://house.speakingsame.com
Sotherby's International Realty	http://www.sothebysrealty.com
SkyscraperPage	http://skyscraperpage.com
Spanish Country Homes (Spain)	http://spanishcountryhomes.com
Street Check (UK)	https://www.streetcheck.co.uk
Total View Real Estate	http://www.totalviewrealestate.com/userguide.php
United Country Real Estate (US)	http://www.unitedcountry.com
US Department of Housing and Urban Development	https://www.hud.gov

World Properties	https://www.worldproperties.com
Zillow (US)	https://www.zillow.com
Zoopla (UK)	https://www.zoopla.co.uk

Online Marketplaces

Classifieds and Online Marketplaces

Tool	Link
2dehands (BE)	https://www.2dehands.be
Alibaba	https://www.alibaba.com
AliExpress	https://www.aliexpress.com
Allegro	https://allegro.pl
Americanas (BR)	https://www.americanas.com.br/hotsite/marketplace-americanas
bedpage	https://www.bedpage.com
Big Commerce Global Marketplaces Index	https://www.bigcommerce.com/blog/global-marketplaces
Bonanza	https://www.bonanza.com
Claz	http://claz.org
Craigslist	https://www.craigslist.org
Depop	https://www.depop.com
ebay	https://www.ebay.com
eBid (Global)	https://www.ebid.net
eCrater	https://www.ecrater.com
Etsy	https://www.etsy.com
Extra (BR, MX)	https://www.extra.com.br/marketplace/venda-no-extra.aspx?origin=ex
FatFingers	http://fatfingers.com
Federal Association of Online Trade Marketplaces Across Europe (DK)	http://bvoh.de/overview-of-online-marketplaces-across-europe

Flipkart (IN)	https://www.flipkart.com
flippity	http://www.flippity.com
Folksy	https://folksy.com
GAME Marketplace (UK)	https://www.help.game.co.uk/hc/en-gb
Goofbay	https://www.hotukdeals.com/deals/goofbay-free-ebay-tools-misspellings-typos-sniper-bargains-1006930
Goofbid	https://www.goofbid.com
Gumtree	https://www.gumtree.com
hotukdeals	https://www.hotukdeals.com
JD (CH)	https://www.jd.com
Jet	https://jet.com
Jingdong Mall (CH)	https://www.jd.com
Jumia (NG)	https://www.jumia.com.ng
Kijiji (Canada)	https://www.kijiji.ca
Lazada (Asia)	https://www.lazada.com
LeoList	https://www.leolist.cc
MarkaVIP (Middle East)	http://markavip.com
Markt.de	https://www.markt.de
Marktplaats	https://www.marktplaats.nl
Mercado Livre (BR, MX)	https://www.mercadolivre.com.br
oodle	https://www.oodle.com
Otto (DE)	https://www.otto.de/unternehmen/en/e-commerce/index.php
OzBargain (AU)	https://www.Ozbargain.com.au
PicClick	https://picclick.com
Privalia (ES, IT, MX, BR)	http://www.privalia.com
Quikr	https://www.quikr.com
Quoka	https://www.quoka.de
Rakuten (JP, DE)	https://www.rakuten.com
Sales Spider	https://www.salespider.com
Search All Junk	http://www.searchalljunk.com
SearchTempest	https://www.searchtempest.com

Shopify	https://www.shopify.com/?utm_source=eCommerce%20platforms&utm_medium=blog&utm_campaign=Pixcblog
Snapdeal (IN)	https://www.snapdeal.com
Speurders	https://www.speurders.nl
Statista Top Real Estate Companies	https://www.statista.com/study/44581/top-100-real-estate-companies
Submarino (BR, MX)	https://www.submarino.com.br
Taobao (CN)	https://www.taobao.com
Tictail	https://tictail.com
TMall (CH)	https://www.tmall.com
Used (Canada)	https://www.used.ca
Willhaben (AT)	http://www.willhaben.at
Zalora (Asia)	https://worldwide.zalora.com
Zibbet	https://www.zibbet.com

Cryptocurrencies and Financial Information

Cryptocurrencies

Tool	Link
Addresswatcher	https://addresswatcher.com
Bitcoin WhosWho	http://bitcoinwhoswho.com
BitRef	https://bitref.com
Blockchain	https://blockchain.info
Block Explorer	https://blockexplorer.com
Blockonomics	https://www.blockonomics.co
Chain Radar	https://chainradar.com
coinbase	https://www.coinbase.com
Crypto Scam Checker	https://fried.com/crypto-scam-checker
Crypto Stack	https://cryptostack.xyz
EtherChain	https://www.etherchain.org
EtherScan	https://etherscan.io
Live Coin Watch	https://www.livecoinwatch.com
Monero Blocks	https://moneroblocks.info
Monero Wallet Hunter	https://www.xmrhunter.com
WalletExplorer	https://www.walletexplorer.com
xmrchain	https://xmrchain.net

Financial Information

Tool	Link
Bin Base	http://www.binbase.com/search.html
Binlist	https://binlist.net
cuitonline	https://www.cuitonline.com
IBAN Check	http://www.tbg5-finance.org/?ibancheck.shtml
IBAN Checker	https://www.iban.com
Search BIN Database	http://www.binbase.com/search.html
TVA Recherche.lu	https://tva-recherche.lu/adresse
VAT Lookup	http://www.vat-lookup.co.uk
VAT Search	http://vat-search.co.uk

Legal Research

Legal Research Reources and Tools

Tool	Link
Asian Legal Information Institute	http://www.asianlii.org
Australian Capital Territory Civil & Administrative Tribunal	http://acat.act.gov.au
Australian Legal Information Institute	http://www.austlii.edu.au
British and Irish Legal Information Institute	http://www.bailii.org
Bundesverfassungsgericht	https://www.bundesverfassungsgericht.de/SiteGlobals/Forms/Suche/Entscheidungensuche_Formular.html
CanLaw (Canada)	https://canlaw.com
CanLII (Canada)	https://www.canlii.org
Cardiff Index to Legal Abbreviations	http://www.legalabbrevs.cardiff.ac.uk
Case Law Database	http://cld.unmict.org
Case Tracker (UK)	http://casetracker.justice.gov.uk
Chambers and Partners	https://www.chambersandpartners.com
Commonwealth Legal Information Institute	http://www.commonlii.org
County-Courts.co.uk	https://county-courts.co.uk
Court Listener	https://www.courtlistener.com
Court News (UK)	http://courtnewsuk.co.uk
Crown Court List (UK)	http://xhibit.justice.gov.uk
Cylaw (Cyprus)	http://www.cylaw.org
De Rechtspraak	https://uitspraken.rechtspraak.nl
Deutsche Justice	http://www.deutschejustiz.de

Droit	http://www.droit.org
DRSP	http://www.drsp.net
Free County Court Records	https://www.blackbookonline.info/USA-County-Court-Records.aspx
Hong Kong Legal Information Institute	http://www.hklii.org
IIJusticia	http://www.iijusticia.edu.ar
Irish Legal Information Initiaitive	https://www.ucc.ie/academic/law/irlii/index.php
ittig	http://www.ittig.cnr.it
Jersey Legal Information Board	https://www.jerseylaw.je
JuraForum	https://www.juraforum.de
Kenya Law	http://kenyalaw.org
Korea Legislation Research Institute	http://www.klri.re.kr
Law Pages	http://www.thelawpages.com
The LAWPHiL Project	https://www.lawphil.net
Law Society (UK)	http://www.lawsociety.org.uk
Law Society of Northern Ireland	https://www.lawsoc-ni.org
Law Society of Scotland	https://www.lawscot.org.uk
Legal Information Institute of India	http://www.liiofindia.org
Legal Tools	http://www.legal-tools.org/en/what-are-the-icc-legal-tools
Legislation.gov.uk	http://www.legislation.gov.uk
Leaxdin	https://www.lexadin.nl/wlg
Lexetius.com	https://lexetius.com
Lexxion	http://www.lexxion.de
Lexum	https://lexum.com
LLRX	https://www.llrx.com
Malawi LII	https://www.malawilii.org
New Zeland Legal Information Institute	http://www.nzlii.org
NYU LIbGuide International Law	http://nyulaw.libguides.com/international-law
OpenJur	https://openjur.de
PACER	https://www.pacer.gov
Pacific Islands Legal Information Institute	http://www.paclii.org

Pinnington Law	https://pinningtonlaw.co.uk
Southern African Legal Information Institute	http://www.saflii.org
Trial International	https://trialinternational.org
UAB Institute of Law and Technology	http://idt.uab.cat
Uganda Legal Information Institute	https://www.ulii.org
UNODC Sherloc	https://www.unodc.org/cld/v3/sherloc
Urteilfinden	http://www.urteilfinden.de
World Legal Information Institute	http://worldlii.org

Researching Countries

Country Profiles

Tool	Link
BBC News Country Profile	http://news.bbc.co.uk/2/hi/country_profiles/default.stm
CIA World Factbook	https://www.cia.gov/library/publications/resources/the-world-factbook/index.html
Country Studies	http://countrystudies.us
Global Edge	https://globaledge.msu.edu
IMUNA Country Profiles	http://www.imuna.org/resources/country-profiles
Kwintessential Country Guides	https://www.kwintessential.co.uk/resources/guides
Library of Congress Country Studies	https://www.loc.gov/collections/country-studies/about-this-collection
Library of Congee Nations	http://www.loc.gov/law/help/guide/nations.php
UN Country Profiles	http://www.un.org/esa/population/publications/countryprofile/profile.htm
UNCTAD Country Profile	http://unctadstat.unctad.org/CountryProfile/en-GB/index.html

Researching Terrorism, Crime, and Cybersecurity

Researching Terrorism

Tool	Link
ALIC Terrorism	https://www.archives.gov/research/alic/reference/terrorism-links.html
Counter Extremism Project	https://www.counterextremism.com
Combating Terrorism Center	https://ctc.usma.edu
Counter Terrorist Trends and Analyses (CTTA)	http://www.rsis.edu.sg/rsis-publication/icpvtr/counter-terrorist-trends-and-analyses-ctta-volume-10-issue-06/#.WyDPZBIzZTZ
Global Counterterrorism Forum	https://www.thegctf.org
Global Terrorism Database	https://www.start.umd.edu/gtd
Global Terrorism Index	https://en.wikipedia.org/wiki/Global_Terrorism_Index#2017
Global Terrorism Research Project	http://gtrp.haverford.edu
International Center for Counter-terrorism	https://icct.nl
Jihadica	http://www.jihadica.com
Online Jihad	https://onlinejihad.net
RAND National Security and Terrorism	https://www.rand.org/topics/national-security-and-terrorism.html
RAND Counterterrorism	https://www.rand.org/topics/counterterrorism.html
Profiles of Individual Radicalization in the United States	http://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus

South Asia Terrorism Portal	http://www.satp.org
START Terrorism Databases and Resources	http://www.start.umd.edu/topics/terrorism-databases-and-resources
Terrorism Analysts	http://www.terrorismanalysts.com
Terrorism & Political Violence Risk Map	https://www.riskadvisory.com/campaigns/terrorism-political-violence-risk-map-2018
Tracking Terrorism	https://www.trackingterrorism.org
UN Office of Counter-Terrorism	http://www.un.org/en/counterterrorism/index.shtml
UN Research Counter-terrorism	http://research.un.org/en/counter-terrorism

Researching Crime

Tool	Link
Crime Data Explorer	https://crime-data-explorer.fr.cloud.gov
CrimeReports	https://www.crimereports.com
Data.Police.UK	https://data.police.uk
Europol	https://www.europol.europa.eu
Eurostat Crime	http://ec.europa.eu/eurostat/web/crime/database
International Crimes Database	http://www.internationalcrimesdatabase.org
Interpol	https://www.interpol.int
Office for National Statistics Guide to Finding Crime Statistics	https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/guidetofindingcrimestatisticsoct2016
UNODC	http://www.unodc.org
WikiCrimes	http://www.wikicrimes.org

Researching Cybersecurity

Tool	Link
BlackHat	http://www.blackhat.com
Center for Internet Security	https://www.cisecurity.org
CNET Security	https://www.cnet.com/topics/security
Common Weakness Enumeration	http://cwe.mitre.org
CSO Online	https://www.csoonline.com
CVE Details	https://www.cvedetails.com
CVE MITRE	http://cve.mitre.org
Dark Reading	https://www.darkreading.com
DShield	https://dshield.org
Exploit Database	https://www.exploit-db.com
Google Safety Center	https://www.google.com/safetycenter
HelpNetSecurity	https://www.helpnetsecurity.com
Information Systems Security Association International	https://issa.site-ym.com
Infosec Island	http://www.infosecisland.com
Infosecurity Magazine	https://www.infosecurity-magazine.com
Krebs On Security	https://krebsonsecurity.com
Linux Security	http://www.linuxsecurity.com
McAfee Labs	https://securingtomorrow.mcafee.com/mcafee-labs
Microsoft Secure	https://www.microsoft.com/en-us/security/default.aspx
Mozilla Security Blogs	https://blog.mozilla.org/security
Naked Security	https://nakedsecurity.sophos.com
Network World Security	https://www.networkworld.com/category/security

NIST	https://csrc.nist.gov
Packet Storm Security	https://packetstormsecurity.com
SANS	https://www.sans.org
SCMagazine	https://www.scmagazine.com
SecuriTeam	http://www.securiteam.com
Security Focus	https://www.securityfocus.com
Security Intelligence	https://securityintelligence.com
Security Mailing List Archive	http://seclists.org
Security Tube	http://www.securitytube.net
Security Week	https://www.securityweek.com
Security Wizardry Radar	http://www.securitywizardry.com/radar.htm
Stay Safe Online	https://staysafeonline.org/resources
Stop Think Connect	https://stopthinkconnect.org
Talos Intelligence	https://www.talosintelligence.com
Threatpost	https://threatpost.com
Tripwire State of Security	https://www.tripwire.com/state-of-security
US-CERT	https://www.us-cert.gov

Researching Stolen Items

Researching Stolen Items

Tool	Link
Art Loss	http://www.artloss.com
BBB Scam Tracker	https://www.bbb.org/scamtracker/us/
Beds Alert	https://www.bedsalert.co.uk/da/155614/Do_you_recognise_stolen_items_recovered_in_nearby_Hertfordshire_.html
Canadian Police Stolen Property Search	http://www.cpic-cipc.ca/index-eng.htm
Comerica Fraud Center	https://www.comerica.com/fraud-center/report-fraud/lost-stolen-cards-checks.html
Culture Crime News	http://news.culturecrime.org
Find Stolen Art	http://www.findstolenart.com/Search.asp?sr=0
Gestohlen.org	http://www.gestohlen.org
Gumtree Lost & Found	https://www.gumtree.com/lost-found-stuff/uk/stolen
HotGunz	http://www.hotgunz.com
Interpol Works of Art Database	https://www.interpol.int/Crime-areas/Works-of-art/Database
It's BEEN NICKED	http://www.itsbeennicked.co.uk
Pawn Alert	http://www.pawnalert.com/search-stolen-database.html
Prey Project	https://www.preyproject.com
Scrap Theft Alert	https://www.scraptheftalert.com/Home/Home.aspx
Securius	https://www.securius.eu/de/datenbank
Stolen and Found	https://stolenandfound.com
Stolen Boats (UK)	http://www.stolenboats.org.uk

stolencamerafinder	http://www.stolencamerafinder.co.uk
Stolen Caravan, Motorhome and Trailer Tent Database	http://www.ukcampsite.co.uk/articles/view.asp?id=108
Stolen Lost Found	http://www.stolenlostfound.org
Stolen Property	http://www.stolen-property.com
Stolen Register	http://www.stolenregister.com/search
Stolen 911	https://stolen911.com
Trace Checker	https://www.tracechecker.com
The Watch Register	http://www.thewatchregister.com
World Museum Community Red Lists Database	http://icom.museum/resources/red-lists-database

Researching Human Trafficking

Researching Human Trafficking

Tool	Link
Allies Against Slavery	http://www.alliesagainstslavery.org
Asia-Europe Foundation	http://www.asef.org
ASTRA Anti-Trafficking Action	https://www.astra.rs
Arc of Hope for Children	https://arkofhopeforchildren.org/child-trafficking/child-trafficking-statistics
Blue Heart International	http://blueheartinternational.org/human-trafficking-in-california
CARIM East - Consortium for Applied Research on International Migration	http://www.carim-east.eu
Caritas	https://www.caritas.org/what-we-do/migration/human-trafficking
Chance	http://chance.amstat.org
Child Protection Hub	https://childhub.org
CNN Freedom Project	http://thecnnfreedomproject.blogs.cnn.com
Commission on Security and Cooperation in Europe	https://www.csce.gov/issue/human-trafficking
Council of the Baltic Sea States	http://www.cbss.org
Counter-Trafficking Data Collaborative (CTDC)	https://www.ctdatacollaborative.org
Department of Homeland Security Blue Campaign	https://www.dhs.gov/blue-campaign/share-resources
ECPAT	http://www.ecpat.org

Eastern Shore Human Trafficking Task Force	http://eshttf.org
End Slavery Now	http://www.endslaverynow.org
Erase Child Trafficking	https://www.erasechildtrafficking.org
Ethics & religious Liberty Commission Human Trafficking Index	https://erlc.com/resource-library/topic-index/human-trafficking
European Commission	http://ec.europa.eu/anti-trafficking
European Court of Auditors Special Report	http://publications.europa.eu/webpub/eca/special-reports/human-trafficking-09-2017/en
European Freedom Network	http://www.europeanfreedomnetwork.org/resources
Europol	https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/trafficking-in-human-beings
Family and Youth Services Bureau	https://www.acf.hhs.gov/fysb/success-story/trafficking-rhy-20170410
Fight Against Trafficking	https://www.fightagainsttrafficking.org/participating-countries
Force 4 Compassion	http://www.f-4-c.org
Free the Slaves	https://www.freetheslaves.net
Free To Shine	https://www.freetoshine.org
Global Centurion	https://www.globalcenturion.org
Global Incident Map	http://human.globalincidentmap.com
Global Modern Slavery Directory	http://www.globalmodernslavery.org
Global Slavery Index	https://www.globalslaveryindex.org
Human Trafficking Center	http://humantraffickingcenter.org
Human Trafficking Flow Map	http://dataviz.du.edu/projects/htc/flow
Human Trafficking Research	http://humantraffickingsearch.org
Human Rights First	https://www.humanrightsfirst.org
Institute for Security & Development Policy	http://isdp.eu
International Human Trafficking Task Force	http://www.ihttf.com
International Labour Organization	http://www.ilo.org/global/topics/forced-labour/lang--en/index.htm

International Labor Rights Forum	https://www.laborrights.org
International Organization for Migration	https://www.iom.int
International Organization for Migration Australia	http://www.iomvienna.at
Interpol	https://www.interpol.int/Crime-areas/Trafficking-in-human-beings/Trafficking-in-human-beings
Kalamazoo Anti-Human Trafficking Coalition	http://www.kahtc.org
Laboratory to Combat Human Trafficking	https://combathumantrafficking.org/category/research-resources
La Strada International	http://lastradainternational.org
Living For Tomorrow	http://www.lft.ee/human-trafficking
Ludwig Boltzmann Institute: Human Rights	http://bim.lbg.ac.at/en/trafficking-human-beings
Maryland Human Trafficking Task Force	http://www.mdhumantrafficking.org
MTV Staying Alive	http://www.mtvstayingalive.org
National Crime Agency	http://www.nationalcrimeagency.gov.uk/publications/national-referral-mechanism-statistics#
National Human Trafficking Hotline	https://humantraffickinghotline.org
National Society for the Prevention of Cruelty to Children	https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/child-trafficking/research-resources
National Runaway Safeline	https://www.1800runaway.org
Nordic Council of Ministers' Office in Estonia	https://www.norden.ee/en/welfare-society/fight-against-human-trafficking
Not for Sale Campaign	https://www.notforsalecampaign.org
Office for Victims of Crime	https://ovc.ncjrs.gov/humantrafficking/resources.html
Office on Trafficking in Persons	https://www.acf.hhs.gov/otip
Ohio Human Trafficking Task Force	http://humantrafficking.ohio.gov
Pearls4Hope	https://www.pearls4hope.com
Polaris Project	https://polarisproject.org/human-trafficking
Ref World	http://www.refworld.org/cgi-bin/texis/vtx/rwmain

Shared Hope International	https://sharedhope.org/the-problem
Silk Road Studies Program	https://www.silkroadstudies.org
Statista	https://www.statista.com/topics/4238/human-trafficking
Stop the Traffik	https://www.stopthetraffik.org/about-human-trafficking/the-scale-of-human-trafficking
South Carolina Human Trafficking Task Force	http://humantrafficking.scag.gov/data-reports
Thorn	https://www.wearethorn.org/child-trafficking-statistics
United Nations Human Rights Office of the High Commissioner	http://www.ohchr.org/EN/PublicationsResources/Pages/Publications.aspx
USAID	https://www.usaid.gov/trafficking
US Department of Defense Combating Trafficking in Persons	http://ctip.defense.gov
US Department of Health and Human Services Office of Refugee Resettlement	https://www.acf.hhs.gov/orr/trafficking-resources
US Department of Justice Office of Justice Programs - Human Trafficking	https://ojp.gov/specialfocus/humantrafficking/publications.htm
US Department of Justice Child Exploitation and Obscenity Section	https://www.justice.gov/criminal-ceos
US Department of State Office to Monitor and Combat Trafficking in Persons	https://www.state.gov/j/tip
VAW net	https://vawnet.org/sc/human-trafficking
Vets 4 Child Rescue	https://vets4childrescue.org/national-human-trafficking-hotline-statistics

Transportation

Airplanes

Tool	Link
ADS-B Exchange	https://www.adsbexchange.com
Aeroseek	http://www.aeroseek.com
Airmap	https://developers.airmap.com
Airliners	http://www.airliners.net
Airport Webcams	http://airportwebcams.net
Aviation Edge	https://aviation-edge.com/airport-database-api
Avaiation Herald	https://www.avherald.com
Aviation Safety	https://aviation-safety.net
Bridgenet Volans Live Display	http://volans.airportnetwork.com/js3d/volanspublicsfo.html
CAA (UK)	http://www.caa.co.uk
Canadian Civil Aircraft Register	http://wwwapps.tc.gc.ca/saf-sec-sur/2/ccarcs-riacc/RchSimp.aspx
Casper Flights	http://casperflights.com
Donner Radar	http://www.donnyradar.co.uk
FlyAriana (Afghanistan)	http://www.flyariana.com
FlightAware (UK)	https://uk.flightaware.com
FlightAware (US)	https://flightaware.com
Flightradar24	https://www.flightradar24.com
Flight Radar (EU)	https://www.flight-radar.eu
Flight Stats	https://www.flightstats.com

Flightwise	http://flightwise.com
FlightView	https://www.flightview.com
Humberside Airport	https://www.humbersideairport.com/live-flight-information
Open Flights	https://openflights.org/data.html
Opensky Network	https://opensky-network.org
Over the North East	http://www.otne.co.uk/eta
PlaneFinder	https://planefinder.net
Plane Spotters	https://www.planespotters.net
Programmable Web Transportation APIs	https://www.programmableweb.com/category/transportation/api
RadarBox	https://www.radarbox24.com
Radar Virtuel	http://www.radarvirtuel.com
Search Airfields	http://www.pilotweb.aero/airfields/search-airfields
Seatguru	https://www.seatguru.com
Stack Exchange Aviation Forum	https://aviation.stackexchange.com
Symphony Public Vue	https://secure.symphonycdm.com/publicvue/Frames.asp
WebTrak5	http://webtrak5.bksv.com
Zhaw Radar	http://radar.zhaw.ch/AirTraffic.html
360 Radar	https://360radar.co.uk

Drones

Tool	Link
Airdata UAV	https://airdata.com
Australian Government Civil Aviation Safety Authority	https://www.casa.gov.au/aircraft/landing-page/flying-drones-australia
Aviation Safety Network	https://aviation-safety.net/database/issue/drones.php
Bard College Center for the Study of the Drone	http://dronecenter.bard.edu/the-drone-database
Drone no-fly zones	https://kadata.kadaster.nl/dronekaart
dronestagram	http://www.dronestagr.am
Drone Regulations	https://www.droneregulations.info
Drone Research Lab	http://droneresearchlab.com
Drone Wars UK	https://dronewars.net/drone-crash-database
DroneZon	https://www.dronezon.com
Event38	https://event38.com
Federal Aviation Administration	https://www.faa.gov/news/updates/?newsId=85548
Federal Aviation Administration UAS Data on a Map	https://faa.maps.arcgis.com/apps/webappviewer/index.html?id=9c2e4406710048e19806ebf6a06754ad
Global Drone Regulations Database	https://droneregulations.info
Google Map Fusion Table	https://fusiontables.googleusercontent.com/embedviz?viz=MAP&q=select+col2+from+1WuTyH62PmUF97oxo6IreT1BL_aw9HJN5pocwmwg&h=false&lat=44.08758502824518&lng=-85.5615234375&z=4&t=1&l=col2&y=1&tmplt=2
Precision Hawk Mapper	http://www.precisionhawk.com/precisionmapper
RAND Corporation	https://www.rand.org/topics/unmanned-aerial-vehicles.html

Skylark Drone Research	http://www.skylarkdroneresearch.com/skylark-drone-research.html
Skyward	https://skyward.io/support/user-guide/airspace/usa/airports
The Conversation: Drones	http://theconversation.com/us/topics/drones-2513
The Drone Database	http://drones.cnas.org/drones
Travel by Drone	http://travelbydrone.com
UAS Vision	https://www.uasvision.com/about
UAViators Humanitarian UAV Network	http://uaviators.org
United States Association Unmanned Aerial Videography	https://uavus.org
Unmanned Aerial Online	https://unmanned-aerial.com

Cars

Tool	Link
AllVehicleData	http://www.allvehicledata.com
AutoCheck	https://www.autocheck.com/vehiclehistory/?siteID=0
AutoDNA	https://www.autodna.com
AutoTrader (RU)	https://autotraveler.ru/en/spravka/vehicle-registration-codes-in-the-world.html#.Wsz3O4jwY2w
Big Rig VIN	http://bigrigvin.com
Car Detective	https://www.cardetective.com/vin-decoder
CarFax	https://www.carfax.com
Check That VIN	https://checkthatvin.com
FaxVIN	https://www.faxvin.com/vin-check
Federal-Mogul Motorparts Finder	https://www.fmmotorparts.com/fmstorefront/federalmogul/en/USD/catalog/partsFinderLicensePlateLookup
Honda Recall Lookup	https://owners.honda.com/service-maintenance/recalls
Interpol Vehicle Crimes	https://www.interpol.int/Crime-areas/Vehicle-crime/Links
Kelley Blue Book	https://www.kbb.com/vehicle-history-report
License Plates of the World	http://www.worldlicenseplates.com
MOT Checker	https://www.ismycar.co.uk/mot-checker
National Highway Traffic Safety Administration	https://vinrcl.safercar.gov/vin
National Motor Vehicle Title Information System	https://www.vehiclehistory.gov
Reverse Genie License Plate Search	http://www.reversegenie.com/plate.php
Saskatchewan VIN search	https://www.sgi.sk.ca/vin
Vehicle History	https://www.vehiclehistory.com

Vehicle Identification Number	https://vehicleidentificationnumber.com
VINCheck	https://www.nicb.org/how-we-help/vincheck
VINCheck.info	http://vincheck.info
VIN decoder	https://www.vindecoderz.com
VINFree Check	https://www.vinfreecheck.com
VIN Place	http://vin.place

Railways

Tool	Link
ACW Railway (US)	http://www.acwr.com/economic-development/rail-maps
Association of American Railroads	https://www.aar.org
Association for Open Data of Public Transportation Secretariat Office (Japan)	http://airport.odpt.org/index-e.html
Archive Freight Rail Works	http://archive.freightrailworks.org
British Columbia Data Catalogue	https://catalogue.data.gov.bc.ca/dataset/railway-track-line
Canadian Rail Research Laboratory	http://carrl.ca
Centre For Railway Research	http://www.crr.iitkgp.ernet.in/crr/index.php
Data.gov (India)	https://data.gov.in/sector/railways
Data.gov (Saudi Arabia)	http://www.data.gov.sa/en/saudi-railways-organization
Data.gov (US)	https://catalog.data.gov/dataset?tags=railroad
Data.deutschebahn	http://data.deutschebahn.com/dataset
Data.vancouver.ca (Canada)	http://data.vancouver.ca/datacatalogue/railway.htm
DB (Germany)	http://www.apps-bahn.de
DB Open Data Portal	http://data.deutschebahn.com

DSB (Denmark)	https://www.dsb.dk
Eurail (EU) Participating Railway Companies	https://www.eurail.com/en/get-inspired/trains-europe/useful-train-information/participating-railway-companies
European Reference Center for Intermodal Freight Transport	http://eurift.eu/index.php
Federal Railroad Administration (US)	https://www.fra.dot.gov/Page/P0001
Indian Railways	https://railways.socialcops.com
International Association of railway Operations	http://www.iaror.org
International Journal of Railway Research	http://ijrare.iust.ac.ir
Interrail Trains Per Country	https://www.interrail.eu/en/plan-your-trip/trains-europe/trains-country
Intermodal Map (EU)	http://www.intermodal-map.com/freie-karte
Keisei Electric Railway Company (Japan)	http://www.keisei.co.jp
Liik Enne Vira Sto (Finland)	https://www.liikennevirasto.fi/web/en/data
Network Rail (UK)	https://www.networkrail.co.uk/who-we-are/transparency-and-ethics/transparency/open-data-feeds
Odakyu Electric Railway Company (Japan)	https://www.odakyu.jp
Office of Rail and Road (UK)	http://orr.gov.uk/about-orr/corporate-data
Open.cCnada	https://open.canada.ca/data/dataset?keywords=railway+networks
Open Data: City and County of Durham	https://opendurham.nc.gov/explore/dataset/durham-railways
Open Data NI	https://www.opendatani.gov.uk/group/transport

Open Data Peel Region (Canada)	http://opendata.peelregion.ca/data-categories/transportation/railways.aspx
Open Data Regina (Canada)	http://open.regina.ca/dataset/railways
Open Data Swiss	https://opendata.swiss/en/organization/schweizerische-bundesbahnen-sbb
Open Data Transport NSW (Australia)	https://opendata.transport.nsw.gov.au/search/type/dataset
Open Railway Map	https://www.openrailwaymap.org
PennDOT Open Data	https://data-pennshare.opendata.arcgis.com
Queensland Government Data	https://data.qld.gov.au/dataset/steam-locomotive-drawings-and-railway-plans
Rail Analysis India	http://railanalysis.in
Raildar FR	http://raildar.fr
Rail Delivery Group	https://www.raildeliverygroup.com/our-services/rail-data.html
Rail Freight Locations (EU)	http://www.railfreightlocations.eu
Rail Net Europe	http://www.rne.eu/downloads
Railway Gazette	http://www.railwaygazette.com
Railway Research	http://www.railway-research.org
Railway Technical Research Institute	http://www.rtri.or.jp/eng
Railway Technology	https://www.railway-technology.com/company-a-z
Rail Webcams	http://railwebcams.net
Spoorkaart	http://spoorkaart.mwnn.nl
Tobu Railway Company (Japan)	http://www.tobu.co.jp/corporation
Trafa Transport Analysis	https://www.trafa.se/en/rail-traffic
Trafi Finnish Transport Safety Agency	https://www.trafi.fi/en/information_services/open_data
Trainline	https://www.thetrainline.com

Transport Focus (UK)	https://www.transportfocus.org.uk/research-publications/rail-research/#?modes=4
UCL Railway Research Group	http://www.ucl.ac.uk/railway-research
UIC (Union Internationale Des Chemins De Fer)	https://uic.org/research
UK Rail Research and Innovation Network	http://www.ukrrin.org.uk
Union Pacific (US)	https://www.up.com/index.htm
US Department of Transportation Railroads	https://www.transportation.gov/railroads
Welsh Railways Research Circle	http://wrrc.org.uk/research.php
World By Map Railways	http://world.bymap.org/Railways.html

Public Transport

Tool	Link
Bay Area Rapid Transit	http://www.bart.gov
Bureau of Transportation Statistics	https://www.bts.gov
Chicago Regional Transportation Authority	http://data.rtachicago.org
Department for Transport NaPTAN (UK)	http://naptan.dft.gov.uk/naptan/process.htm
DIVA-GIS	http://www.diva-gis.org/gdata
Geofabrik Open Street Map	http://download.geofabrik.de
Global BRT Data	https://brtdata.org
Global Roads Data	http://www.ciesin.columbia.edu/confluence/display/roads/Global+Roads+Data
Global Mass Transit Report	http://www.globalmasstransit.net/archive.php?id=2181
Google Maps - Transit	https://maps.google.com/landing/transit/index.html
Koordinates	https://koordinates.com
Livemap24	https://livemap24.com
Mapnificent	https://www.mapnificent.net
New York City Department of Transportation	http://www.nyc.gov/html/dot/html/about/datafeeds.shtml
Open Cycle Map	https://www.opencyclemap.org
Open Data City of New York	https://opendata.cityofnewyork.us/data
Open Data Platform Swiss Public Transport	https://opentransportdata.swiss/en/dataset

Open Data Showroom	http://opendata-showroom.org/en/traffic
Open Data Soft - Navitia	https://navitia.opendatasoft.com/explore/?sort=modified
Open Data Soft - Navitia	https://navitia.opendatasoft.com/page/start
Open Data Swiss	https://opendata.swiss/en
Open Data Transport (Australia)	https://opendata.transport.nsw.gov.au/dataset/public-transport-realtime-vehicle-positions
Open Street Map	https://www.openstreetmap.org
Open Street Map Belgium	http://www.osm.be
Open Street Map Lithuania	https://openmap.lt/#m/7.34/55.00084/23.95463/0/0
Open Street Map Public Transport Wiki	https://wiki.openstreetmap.org/wiki/Public_transport
ÖPNVKarte (OpenBusMap)	http://www.openbusmap.org
Organisation for Economic Co-operation and Development	https://data.oecd.org/transport/passenger-transport.htm
PT Map	https://ptmap.plepe.at
Public Transport Information (UK)	http://www.carlberry.co.uk/rfnsearch.asp
Public Transport Victoria	https://www.ptv.vic.gov.au/getting-around/maps
Thunderforest Maps	https://www.thunderforest.com/maps
Transitfeeds	http://transitfeeds.com
transitland	https://transit.land/playground
TransitWiki	https://www.transitwiki.org/TransitWiki/index.php/Publicly-accessible_public_transportation_data
Transport for London Open Data	https://tfl.gov.uk/info-for/open-data-users
Transports Metropolitans de Barcelona	https://www.tmb.cat/es/home
Transport Scotland	https://www.transport.gov.scot/public-transport
Traveine	http://www.traveline.info
TRAVIC	http://tracker.geops.ch
Queensland Government Data General Transit	https://data.qld.gov.au/dataset/general-transit-feed-specification-gtfs-qconnect

UITP	http://www.uitp.org/data-statistics
Vision Zero View NYC	http://www.vzv.nyc/#
WikiRoutes	https://wikiroutes.info
World Bank	http://www.worldbank.org/en/topic/transport

Ships

Tool	Link
AIS Data Exchange Dispatcher	http://www.aishub.net/ais-dispatcher
AIS Tracker (Russia)	http://en.aistracker.ru/map7.asp
Arundale	http://arundale.com/docs/ais/sp_map.html
BoatInfoWorld	https://www.boatinfoworld.com
Boat Nerd	http://ais.boatnerd.com
Bottenviken Live AIS	http://ais.sk2hg.se
Coast Guard Vessel Search	https://www.st.nmfs.noaa.gov/coast-guard-vessel-search/index
Cruise Mapper	http://www.cruisemapper.com
Cruise Ship Tracker	http://www.cruisin.me/cruise-ship-tracker
Digimap Guernsey	http://www.digimap.gg/marine/ais
FleetMon	https://www.fleetmon.com
Global Fishing Watch	http://globalfishingwatch.org
Gloucester Harbour Trustees	http://gloucesterharbourtrustees.org.uk/ship-positions-marine-traffic
Helcom AIS	http://maps.helcom.fi/website/AISexplorer
ICC Piracy Map	http://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map
Infomarine	http://www.infomarine24.com
International Registries Inc.	https://www.register-iri.com/index.cfm?action=page&page=53
Krooz Cams	http://www.kroooz-cams.com
Landsort AIS	http://www.landsort-ais.se/aism.html
Live Cruise Ship Tracker	https://www.livecruiseshiptracker.com

Live Cruise Ship Tracker	http://www.thecruisevillage.com/live-cruise-ship-tracker.phtml
Maritime Connector	http://maritime-connector.com
Marine Cadastre	https://marinecadastre.gov/ais
Marine Scotland	http://marine.gov.scot/information/ais-shipping-traffic-selected-ports
MarineTraffic	https://www.marinetraffic.com
MarineTraffic	http://www.marinetraffic.org
My Ship Tracking	https://www.myshiptracking.com
Naxos Island	http://www.naxosisland.eu/live_ship_data.html
Open Sea Map	http://map.openseamap.org
Open Sea Map	http://www.openseamap.org
Pocket Mariner	http://pocketmariner.com
Port Hedland Live AIS	http://www.phseafarers.org/live-ship-map-ais.html
Rathlin Weather AIS (United Kingdom)	http://www.rathlinweather.co.uk/AIS
Sandkilen-Helmi AIS	http://www.helmi.se/en/tours-events/ais-live-trace-7227149
Sandy Bay Yacht Club	http://www.sandybay.org/AIS.shtml
Scanner Net	http://www.scannernet.nl/maritiem/live-ais
SCCOOS (United States)	http://sccoos.org
Shipais	http://www.shipais.com
Ship Finder	http://shipfinder.co
Shipping Explorer	http://www.shippingexplorer.net
ShipSpotting	http://www.shipspotting.com
Ship Tracker Shodan	https://shiptracker.shodan.io
Trewillis.co.uk	http://www.trewillis.co.uk
Vessel Finder	https://www.vesselfinder.com
Vessel Tracker	https://www.vesseltracker.com
World Map	https://worldmap.harvard.edu/maps/2892
World Port Index	https://msi.nga.mil/NGAPortal/MSI.portal?_nfpb=true&_pageLabel=msi_portal_page_62&pubCode=0015
2sandnessjo (Norway)	http://www.2sandnessjo.no/shipplotter/gmap/stavanger.htm l

Container and Cargo Tracking

Tool	Link
APL Tracking	https://www.apl.com/wps/portal/apl/etools/tracking
Cargo Loop	http://www.cargoloop.com
Cargo Tracking	http://cargotracking.utopiax.org/containertracking.html
Container Tracking	http://container-tracking.org
FleetMon	https://www.fleetmon.com/services/container-tracker/search
Freight Metrix	http://www.freightmetrics.com.au/Marine/ShipTracking/tabid/483/Default.aspx
Locus Traxx Worldwide	http://www.locustraxx.com
Marine Traffic	https://www.marinetraffic.com/en/ais/home/centerx:5.7/centery:57.9/zoom:2
My Ship Tracking	https://www.myshiptracking.com
Navipedia	http://www.navipedia.net/index.php/Package_and_Container_Tracking
Searates	https://www.searates.com/container/tracking
Track-trace	http://www.track-trace.com
Vessel Finder	https://www.vesselfinder.com
Vessel Tracker	https://www.vesseltracker.com/en/Googleearth.html

Web Intelligence

Domain and IP Research, Websites Analysis

Tool	Link
Accuranker	https://www.accuranker.com
ahrefs	https://ahrefs.com
Alexa	http://www.alexa.com
altdns	https://github.com/infosec-au/altdns
Analyze ID	http://analyzeid.com
APNIC	https://www.apnic.net
aquatone	https://github.com/michenriksen/aquatone
ARIN	https://www.arin.net
Assetnote-poc	https://github.com/infosec-au/assetnote-poc
Backlink Checker	http://smallseotools.com/backlink-checker
BGP	https://bgp.he.net
Bing Webmaster Tools	http://www.bing.com/toolbox/webmaster
Blacklist Check Tool	http://www.blchecktool.com
BlackWidow	http://www.softbytelabs.com/en/BlackWidow
Blue Backlinks	http://bluebacklinks.com
Bluto-Old	https://github.com/darryllane/Bluto-Old
BotScout	https://botscout.com/search.htm
BrightCloud URL or IP Lookup	https://www.brightcloud.com/tools/url-ip-lookup.php
BuiltWith	http://builtwith.com
Censys	https://censys.io
Central Ops	http://centralops.net

certgraph	https://github.com/lanrat/certgraph
Certificate Search	https://crt.sh
clearwebstats	https://www.clearwebstats.com
CloudFail	https://github.com/m0rtem/CloudFail
CloudFlare Watch	http://crimeflare.biz
Complete DNS	https://completedns.com
COMODO SSL Analyzer	https://sslanalyzer.comodoca.com
Copyscape	http://copyscape.com
Crt.sh	https://crt.sh
CQCounter	http://cqcounter.com/whois
Custom Domain Search Tools	https://inteltechniques.com/osint/menu.domain.html
Custom IP Address Search Tools	https://inteltechniques.com/osint/menu.ip.html
CuteStats	https://www.cutestat.com
Cymon	https://cymon.io
Cymru IP to ASN Lookup	https://asn.cymru.com
Daily Changes	http://dailychanges.domaintools.com
DB-IP	https://db-ip.com
Dedicated or Not	http://dedicatedornot.com
Deepviz - search	https://search.deepviz.com
Denic web whois	https://www.denic.de/webwhois
Digital Point	https://tools.digitalpoint.com
Directory of Malicious IPs	http://www.projecthoneypot.org/list_of_ips.php
DNSDumpster	https://dnsdumpster.com
DNS History	http://dnshistory.org
DNSlytics	https://dnslytics.com
dnspop	https://github.com/bitquark/dnspop
dnsrecon	https://github.com/darkoperator/dnsrecon
DNS Root Instances	https://atlas.ripe.net/results/maps/root-instances
DNSSec Analyzer	https://dnssec-analyzer.verisignlabs.com
DNS Spy	https://dnsspy.io
DNSStuff	http://www.dnsstuff.com
DNS Trails	http://dnstrails.com

DNS Trails	https://securitytrails.com/dns-trails
dnstwister	https://dnstwister.report
DNSViz	http://dnsviz.net
Domain Big Data	http://domainbigdata.com
Domain Crawler	http://www.domaincrawler.com
Domain Dossier	http://centralops.net/co/DomainDossier.aspx
Domain History	http://www.domainhistory.net
Domain & IP Addresses	http://netbootcamp.org/websitetool.html
DomainIQ	https://www.domainiq.com
Domain Tools	https://www.domaintools.com
Domain Tools	http://whois.domaintools.com
downdetector	http://downdetector.com
downforeveryoneorjustme	http://downforeveryoneorjustme.com
DShield API	https://isc.sans.edu/api
EasyCounter WHois	https://whois.easycounter.com
Easy whois	https://www.easywhois.com
EURid	https://eurid.eu
Exfiltrated	http://www.exfiltrated.com/querystart.php
Exonera Tor	https://exonerator.torproject.org
Fierce-domain-scanner	https://github.com/davidpepper/fierce-domain-scanner
FindSubDomains	https://findsubdomains.com
Finitimus	https://chrome.google.com/webstore/detail/finitimus/ckdjcgaagfcnndkkknfmncedapdjaokb?utm_source=chrome-ntp-icon
Follow.net	http://follow.net
gdns	https://github.com/hrbrmstr/gdns
Geo IP Tool	https://geoiptool.com
gobuster	https://github.com/OJ/gobuster
GoDaddy WHois	https://ca.godaddy.com/whois
GooHak	https://github.com/1N3/Goohak
GraphyStories	http://app.graphystories.com
Hexillion	http://hexillion.com
HypeStat	https://www.hypestat.com

Icann Whois	https://whois.icann.org
IKnowWhatYouDownload	https://iknowwhatyoudownload.com/en/peer/?ip=198.8.80.192
InfoBylp (Bulk Domain & IP Lookup	https://www.infobyip.com/ipbulklookup.php
Infosniper	http://www.infosniper.net
intoDNS	http://www.intodns.com
IntelliTamper	http://www.softpedia.com/get/Internet/Other-Internet-Related/IntelliTamper.shtml
InterNIC Whois	http://www.internic.net/whois.html
IP 2 Geolocation	http://ip2geolocation.com
IP 2 Location	https://www.ip2location.com
IP Address	https://www.ip-address.org
IP Address Location	http://www.ipaddresslocation.org
Ipapi Bulk IP Address Lookup	https://app.ipapi.co/bulk
IP Checking	http://www.ipchecking.com
IP Chicken	http://www.ipchicken.com
IP Data	https://ipdata.co
IPFingerprints	http://www.ipfingerprints.com
iphostinfo	https://iphostinfo.com
IP Info	http://ipinfo.info
Ipinfo.io	https://ipinfo.io
ipintel	https://ipintel.io
IP Lists by FireHOL	http://iplists.firehol.org
IP Location	https://www.iplocation.net
IP to ASN	https://iptoasn.com
IP Tracker Online	https://www.iptrackeronline.com
IPv6 Locator	http://ipv6locator.net
ipverse	http://ipverse.net
IPVoid	http://www.ipvoid.com
iTools	http://itools.com
iwantmyname	https://iwantmyname.com
IXMaps Explore	https://www.ixmaps.ca/explore.php

JoeSandboxCloud	https://www.joesandbox.com
Jotti	https://virusscan.jotti.org
Kloth	http://www.kloth.net/services
lacnic	http://www.lacnic.net
Leaked Source	https://leakedsource.ru
Linktally	http://linktally.com
Majestic	https://majestic.com
Maltego	https://www.paterva.com/web7
Malware Domain List	http://www.malwaredomainlist.com/mdl.php
MaxMind	https://www.maxmind.com
McAfee Customer URL Ticketing System	https://trustedsource.org/sources/index.pl
mnemonic	https://passivedns.mnemonic.no
moonsearch	http://moonsearch.com
moreofit	http://www.moreofit.com
Mr. LOOQUER	https://mrlooquer.com
MXToolbox	http://origin.mxtoolbox.com || https://mxtoolbox.com
My IP	https://www.myip.ms
Netcraft Site Report	http://toolbar.netcraft.com/site_report?url=undefined#last_reboot
NetStat Agent	http://netstatagent.com
Network Intelligence	https://netintel.net
Network Tools	http://network-tools.com
Nibbler	http://nibbler.silktide.com
NirSoft	http://www.nirsoft.net
Onyphe	https://www.onyphe.io
OpenLinkProfiler	http://www.openlinkprofiler.org/ratelimit/domain.com
Open Site Explorer	https://moz.com/researchtools/ose
OSINT SPY	https://osint-spy.com
PageGlimpse	http://www.pageglimpse.com
Pentest-Tools Find Subdomains	https://pentest-tools.com/information-gathering/find-subdomains-of-domain
Pentest-Tools.com	https://pentest-tools.com/information-gathering/google-hacking

Plagiarism Checker	http://smallseotools.com/plagiarism-checker
PTRArchive	http://ptrarchive.com
pubDB	http://pub-db.com
Quantcast	https://www.quantcast.com
Quick Sprout	https://www.quicksprout.com
RedirectDetective	http://redirectdetective.com
Remote DNS Lookup	https://remote.12dt.com
Reverse DNS Lookup	https://hackertarget.com/reverse-dns-lookup
Reverse IP to Domain Lookup	http://www.ipfingerprints.com/reverseip.php
RIPE NCC	https://www.ripe.net
RiskIQ	https://community.riskiq.com
Risk Neustar	https://www.risk.neustar/resources/tools/ip-geolocation-lookup-tool
Robtex	https://www.robtex.com
SameID	http://sameid.net
SameIP	http://www.sameip.org
Scamvoid	https://www.scamvoid.com
scanless	https://github.com/vesche/scanless
Scans.io	https://scans.io
Security Headers	https://securityheaders.com
SEMrush	https://www.semrush.com
SEO Chat Tools	http://tools.seochat.com
SEO SiteCheckup Sitemap Test	https://seositecheckup.com/tools/sitemap-test
SEOTools for Excel	http://seotoolsforexcel.com
Serpstat	https://serpstat.com
Shodan	https://www.shodan.io
SIDN	https://www.sidn.nl
Similar Web	https://www.similarweb.com
Site Dossier	http://www.sitedossier.com
Siteliner	http://www.siteliner.com
SiteSleuth	https://www.sitesleuth.io

SmallSEOTools	http://smallseotools.com
Snusbase	https://snusbase.com
Software77 Multi-Lookup	http://software77.net/geo-ip/multi-lookup
SpyCraw	https://www.spycraw.com
SpyOnWeb	http://spyonweb.com
StatsCrop	http://www.statscrop.com
Sublist3r	https://github.com/aboul3la/Sublist3r
Sucuri Free Website and Malware Scanner	https://sitecheck.sucuri.net
Symantec WebPulse Site Review Request	https://sitereview.bluecoat.com
Talos Reputation Lookup	https://talosintelligence.com
TCPIPUTILS.com	http://www.tcpiputils.com
Tejji	http://tejji.com
Threat Crowd	https://www.threatcrowd.org
Threatglass	http://www.threatglass.com
Threat Miner	https://www.threatminer.org
Trend Micro Site Safety Center	https://global.sitesafety.trendmicro.com
Timer4Web	https://www.timer4web.com
Tucows domains	https://www.tucowsdomains.com
urlQuery	http://urlquery.net
urlscan	https://urlscan.io
URLVoid	http://www.urlvoid.com
Utrace	http://en.utrace.de
Verisign	http://dnssec-debugger.verisignlabs.com
Viewdns	http://viewdns.info
Vigilante	https://www.vigilante.pw
Virus Total	https://www.virustotal.com
Visual Site Mapper	http://www.visualsitemapper.com
W3bin.com	https://w3bin.com
W3dt	https://w3dt.net
w3snoop	http://webboar.com.w3snoop.com
Wappalyzer	https://wappalyzer.com

Watch Guard Reputation Authority	http://www.reputationauthority.org
Web Filter Lookup	https://fortiguard.com/webfilter
Web Inspector Free Website Malware Scanner	http://app.webinspector.com
WebMeUp	http://webmeup.com
WebPageTest	https://www.webpagetest.org
Website Informer	http://website.informer.com
Website Outlook	http://websiteoutlook.com
webtarantula	http://webtarantula.com
WhatIsMyIPAddress	http://whatismyipaddress.com
Whois	https://www.whois.com
Who.is	https://who.is
Whois Amped	https://whoisamped.com
Whois Arin Online	https://whois.arin.net
Whois.com	https://www.whois.com
WhoIsHostingThis	http://www.whoishostingthis.com
WHOIS ICANN	https://whois.icann.org
WhoisLookup	http://www.puwong.com/whois
WhoisMind	http://www.whoismind.com
WHOis.net	https://whois.net
Whois.Search	https://whois-search.com
Whoisology	https://whoisology.com
WhoIsRequest	http://whoisrequest.com
WhoLinks2Me	http://www.wholinks2me.com
Whoxy	https://www.whoxy.com
Wigle	https://wigle.net
Woorank	https://www.woorank.com
xray	https://github.com/evilsocket/xray
You Get Signal	http://www.yougetsignal.com
Zulu URL Risk Analyzer	https://zulu.zscaler.com

Web History and Website Capture

Tool	Link
Archive.is	http://archive.is
Archive.fo	http://archive.fo
BlackWidow	http://softbytelabs.com/en/BlackWidow
Cached Pages	http://www.cachedpages.com
Cached View	https://cachedview.nl
Common Crawl	http://commoncrawl.org
Convert Web to PDF	https://play.google.com/store/apps /details?id=com.smobileteam.pdf.activity
Go Back in Time	https://chrome.google.com/webstore/detail /go-back-in-time/hgdahcpipmgehmaaankiglanlgljlakj
InstaWeb	http://www.digiset.me/instaweb
Mass archive	https://github.com/motherboardgithub/mass_archive
PageDash	https://www.pagedash.com
Passive Cache	https://addons.mozilla.org/en-US/firefox/addon/passive-cache
PDFMyURL	http://pdfmyurl.com
Print Friendly	https://www.printfriendly.com
Print What You Like	http://www.printwhatyoulike.com
Resurrect Pages	https://addons.mozilla.org/en-US/firefox/addon/resurrect-pages
Save as PDF Add-on	https://pdfcrowd.com/save-as-pdf-addon
Save to Google Drive	https://chrome.google.com/webstore/detail/save-to-google-drive/gmbmikajjgmnabiglmofipeabaddhgne?hl=en
Save Webpage As Word Document	https://chrome.google.com/webstore/detail/save-webpage-as-word-docu/mcebgdgbcbdkgdljffnkkbekldnidbmn

Screenshots.com	http://www.screenshots.com
Time travel	http://timetravel.mementoweb.org
UK Web Archive	http://www.webarchive.org.uk
Wayback Machine	http://archive.org/web/web.php
Wayback Machine Chrome Add-on	https://chrome.google.com/webstore/detail/wayback-machine/fpnmgdkabkmnadcjpehmlllkndpkmiak?hl=en-US
View-page-archive	https://github.com/dessant/view-page-archive
waybackpack	https://github.com/jsvine/waybackpack
Web2PDF	https://www.web2pdfconvert.com
Web2Pdf.	https://www.microsoft.com/en-us/store/p/web2pdf/9nblgggz5phq
Web Cache	https://chrome.google.com/webstore/detail/web-cache/coblegoildgpecccijneplifmeghcgip
WebCitation	http://webcitation.org/query
Webpage to PDF	http://webpagetopdf.com
Webrecorded	https://webrecorder.io

Wifi Search

Tool	Link
Avast Wifi Finder	https://www.avast.com/en-in/wifi-finder
Find Wifi	https://find-wifi.mylnikov.org
Instabridge	https://instabridge.com
Places to Work	https://placestowork.net
Wifi Finder + Map	https://itunes.apple.com/us/app/map-wifi-wi-fi-finder/id946365975?mt=8&ign-mpt=uo%3D8
Wifi Finder Connect Internet	https://itunes.apple.com/us/app/wifi-finder-free-internet/id1011519183?mt=8&ign-mpt=uo%3D8
WifiFreeSpot	http://www.wififreespot.com
Wigle	https://wigle.net
WikiFiox	https://foxnomad.com/2016/04/26/map-wireless-passwords-airports-lounges-around-world-updated-regularly

Researching Dark Web

Researching Dark Web

Tool	Link
DarkNet Stats	https://dnstats.net
Dark Web Map	https://www.hyperiongray.com/dark-web-map
DeepDotWeb	https://www.deepdotweb.com
DeepWeb Sites	https://www.deepweb-sites.com
DeepWebSitesLinks	https://www.deepwebsiteslinks.com
DarkWebNews	https://darkwebnews.com
Docker-onion-nmap	https://github.com/milesrichardson/docker-onion-nmap
Exonera Tor	https://exonerator.torproject.org
Hidden Wikitor	http://hiddenwikitor.com
Hunchly's Hidden Services Report	https://darkweb.hunch.ly
i2P	https://geti2p.net
onioff	https://github.com/k4m4/onioff
Onion Link	http://onion.link
Onionscan	https://onionscan.org
Onion Investiagtor	https://oint.ctrlbox.com
Onion Land Search Engine	https://onionlandsearchengine.com
Onion Search Engine	http://onionsearchengine.com
The Dark Websites	https://www.thedarkwebsites.com
Tor2Web	https://www.tor2web.org
Tor Netwrok Status	https://torstatus.blutmagie.de
Tor Project	https://www.torproject.org

Torscan	http://torscan.io
Zeronet	https://zeronet.io

Events Search

Events Search

Tool	Link
Eventbrite	https://www.eventbrite.com
Meetup	https://www.meetup.com
WhereEvent	http://www.wherevent.com

Working with Images

Image Search and Reverse Image Search

Tool	Link
Baidu Images	http://image.baidu.com
Berify	https://berify.com
Betaface	https://www.betafaceapi.com
Bing Images	http://www.bing.com/images
Camera Trace	http://www.cameratrace.com/trace
CamFind	https://camfindapp.com
CC Search	https://search.creativecommons.org
Current Location	https://current-location.com
DownloadGram	https://downloadgram.com
Explore Places	http://places2.csail.mit.edu/explore.html
facesearch	http://www.facesaerch.com
FindFace	https://findface.ru
Flickr	https://secure.flickr.com
Flickr Hive Mind	http://flickrhivemind.net
Flickr Map	https://www.flickr.com/map
Fotki	http://www.fotki.com
Geograph	https://www.geograph.org
Google Images	https://images.google.com
Gramfeed	http://www.gramfeed.com
Image Net	http://image-net.org

Image Raider	https://www.imageidentify.com
Imgur	https://imgur.com
KarmaDecay	http://karmadecay.com
Lakako	https://www.lakako.com
Loc.alize.us	https://loc.alize.us
Lycos Images	http://search.lycos.com/images
MyPicsMap	http://www.mypicsmap.com
Photo Map	http://photo-map.ru
PhotoTracker	http://phototracker.ru
Picquery	https://www.picquery.com
Picsearch	http://www.picsearch.com
PicTriev	http://www.pictriev.com
PimEye	https://pimeyes.com/en
Places	http://places2.csail.mit.edu
Reverse GIF	https://ezgif.com/reverse
Reverse Image Search	http://www.reverse-image-search.org
Reverse Image Search	http://www.reverse-image-search.com
Reverse Image Search	https://inteltechniques.com/osint/menu.reverse.image.html
Revimg	http://www.revimg.com
RootAbout	http://rootabout.com
SauceNAO	https://saucenao.com
Small SEO Tools: Reverse Image Search	https://smallseotools.com/reverse-image-search
Smugmug	https://www.smugmug.com/search
Social Catfish Reverse Image Search	https://socialcatfish.com/reverse-image-search
Startpage: Images	https://www.startpage.com/eng/pics.html
StolenCameraFinder	http://www.stolencamerafinder.co.uk
TinyEye	https://tineye.com
Twitter Image Search	https://twitter.com/search?q=%3Csearchterm%3E&src=typd&vertical=default&f=images
View Image	https://chrome.google.com/webstore/detail/view-image/jpcmhcelnjdmblfmjabdeclccemkghjk ||

	https://addons.mozilla.org/en-US/firefox/addon/view-image/
Who Stole My Pictures?	https://addons.mozilla.org/en-US/firefox/addon/who-stole-my-pictures
Websta	http://websta.me
Wolfram Language: The Identification Project	https://www.imageidentify.com
Worldcam	http://www.worldc.am
Yahoo Image Search	https://images.search.yahoo.com
Yandex Images	https://www.yandex.com/images

Image Analysis

Tool	Link
AnalogExif	https://sourceforge.net/projects/analogexif
BetaFaceAPI	https://www.betafaceapi.com/demo.html
CameraSummary	https://camerasummary.com
Diffchecker	https://www.diffchecker.com/image-diff
exifdata	http://exifdata.com
Exifer	https://www.thexifer.net
ExifPro	http://www.exifpro.com
Exif Search	http://www.exif-search.com
exiftool	https://sourceforge.net/projects/exiftool
ExifTool by Phil Harvey	http://www.sno.phy.queensu.ca/~phil/exiftool
Exif Viewer	https://chrome.google.com/webstore/detail/exif-viewer/nafpfdcmppffipmhcpkbplhkoiekndck?hl=en
Exif Viewer	https://addons.mozilla.org/en-US/firefox/addon/exif-viewer
Extract Metadata	https://www.extractmetadata.com
Fake Image Detector	https://play.google.com/store/apps/details?id=fake_image_detector.coder.genuine.com.fakeimagedetector&hl=en
FastPreview	https://tn123.org/fastpreview
Find Exif	http://www.findexif.com
Forensically	https://29a.ch/photo-forensics/#level-sweep
FotoForensics	http://www.fotoforensics.com
FourMatch	http://www.fourandsix.com/fourmatch
Fuskr	https://chrome.google.com/webstore/detail/fuskr/glieaboaghdnlglpkekghloldikefofo
Gbimg.org	http://gbimg.org

GeoSetter	http://www.geosetter.de
Ghiro	http://www.getghiro.org
Google Search "View Image" Button	https://chrome.google.com/webstore/detail/google-search-view-image/hgngncnljacgakaiifjcgdnknaglfipo
How Old	https://how-old.net
Image Edited	http://imageedited.com
Image forensic	https://www.imageforensic.org
Image Identification Project	https://www.imageraider.com
Image Search Options	https://addons.mozilla.org/en-US/firefox/addon/image-search-options
Image Verification Assistant	http://reveal-mklab.iti.gr/reveal/index.html
ImgOps	http://imgops.com
ImpulseAdventure	http://www.impulseadventure.com/photo/jpeg-snoop.html
InVID	http://www.invid-project.eu/tools-and-services/invid-verification-plugin
Irfanview	http://www.irfanview.com
izitru	http://www.izitru.com
Java Exif Viewer	https://sourceforge.net/projects/jexifviewer
Jeffrey's Image Metadata Viewer	http://exif.regex.info/exif.cgi
JPEGsnoop	https://github.com/ImpulseAdventure/JPEGsnoop
Let's Enhance	https://letsenhance.io
Logos	http://logos.iti.gr
metapicz	http://metapicz.com/#landing
Photo Detective	https://itunes.apple.com/us/app/photo-detective-pro/id1045128136?mt=8
PhotoMe	http://www.photome.de
Pic2Map	https://www.pic2map.com
Plaghunter	http://www.plaghunter.com
ReadEXIF	https://readexifdata.com
Resemble.js	https://huddle.github.io/Resemble.js
Reveal Image Verification Assistant	http://reveal-mklab.iti.gr/reveal/index.html

RevEye Reverse Image Search	https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaclcjhehbbapnphnmpiklalfhelgf?hl=en
Send to Exif Viewer	https://chrome.google.com/webstore/detail/send-to-exif-viewer/gogiienhpamfmodmlnhdljokkjiapfck?hl=en-US
tawbaware	http://www.tawbaware.com
Veracity (iPhone app)	https://itunes.apple.com/us/app/veracity-image-search/id870153874?mt=8
Verexif	http://www.verexif.com
View Image	https://chrome.google.com/webstore/detail/view-image/jpcmhcelnjdmblfmjabdeclccemkghjk
Web Inspector	https://chrome.google.com/webstore/detail/web-inspector/enibedkmbpadhfofcgjcphipflcbpelf?hl=en
Where is the picture?	https://whereisthepicture.com
Who Stole My Pictures	https://addons.mozilla.org/en-US/firefox/addon/who-stole-my-pictures

Stock Images

Tool	Link
Adobe Stock	https://stock.adobe.com
AlltheFreeStock	http://allthefreestock.com
Burst	https://burst.shopify.com
CC Search Commons	https://ccsearch.creativecommons.org
Clipstill	http://www.clipstill.com
Death to Stock	http://deathtothestockphoto.com
Epicantus	http://epicantus.tumblr.com
Freeimages	http://www.freeimages.com
Freestocks.org	http://freestocks.org
FoodiesFeed	https://www.foodiesfeed.com
Get Refe	http://getrefe.tumblr.com
Getty Images	https://www.gettyimages.com
Gratisography	http://www.gratisography.com
Image Brief	http://www.imagebrief.com
IM Free	http://www.imcreator.com/free
ISO Republic	http://isorepublic.com
iStockphoto	http://www.istockphoto.com
Jay mantri	http://jaymantri.com
Kaboompics	http://kaboompics.com
LibreStock	https://librestock.com
Life of Pix	http://www.lifeofpix.com
Little Visuals	http://littlevisuals.co
MMT	https://mmtstock.com
Moose	https://photos.icons8.com

Morguefile	https://morguefile.com
NegativeSpace	http://negativespace.co
New Old Stock	http://nos.twnsnd.co
Picjumbo	https://picjumbo.com
Picography	https://picography.co
Pixabay	https://pixabay.com
Pexels	https://www.pexels.com
Photobucket	http://photobucket.com
Public Domain Archive	http://publicdomainarchive.com
reshot	https://www.reshot.com
Shot Stash	https://shotstash.com
Shutterstock	http://www.shutterstock.com
skitterphoto	https://skitterphoto.com
SplitShire	https://www.splitshire.com
Startup Stock Photos	http://startupstockphotos.com
StockSnap	https://stocksnap.io
Styled Stock	https://styledstock.co
Superfamous	http://superfamous.com
tookapic	https://stock.tookapic.com
unDraw	https://undraw.co
Unplash	https://unsplash.com

Image and Photo Editing

Tool	Link
AddText+	https://addtext.com
Affinity Photo	https://affinity.serif.com
Annotable	https://itunes.apple.com/us/app/annotable-ultimate-image-annotation/id1099850421?mt=8
Apple Photos	http://www.apple.com/osx/photos
Aviary	https://www.aviary.com
Befunky	https://www.befunky.com
Birme	https://birme.net
Canva	https://www.canva.com
Croppola	http://croppola.com
Ezgif.com	https://ezgif.com
FastSTone	http://www.faststone.org
FlipA Picture	http://flipapicture.com
Fotor	http://www.fotor.com
Foto Flexer	http://fotoflexer.com
Gimp	http://www.gimp.org
Hugin	http://hugin.sourceforge.net
Image Composite Editor	https://research.microsoft.com/en-us/um/redmond/projects/ice/
Image Tricks Lite	https://itunes.apple.com/us/app/image-tricks-lite/id403735824?mt=12
Irfanview	http://www.irfanview.com
LightZone	http://lightzoneproject.org
Lunapic	http://www124.lunapic.com/editor
OnlineImageSplitter	http://www.htmlkit.com/services/is

Paint.NET	http://www.getpaint.net/index.html
Photoscape	http://www.photoscape.org/ps/main/index.php
Photoshop	http://www.photoshop.com
picfull	http://www.picfull.com
PicMoneky	http://www.picmonkey.com
Pixlr	https://pixlr.com
Polarr	https://www.polarr.co
Seashore	http://seashore.sourceforge.net
Social Image Resizer Tool	https://www.internetmarketingninjas.com/seo-tools/favicon-generator-crop-images
SumoPaint	http://www.sumopaint.com
textify	http://textify.it
TinyPNG	https://tinypng.com

OCR Tools

Tool	Link
Free OCR	http://www.free-ocr.com
I2OCR	http://www.i2ocr.com
New OCR	http://www.newocr.com
Online OCR	http://www.onlineocr.net

Working with Videos

Video Search and Reverse Video Search

Tool	Link
360 Daily	http://www.360daily.com
9gag.tv	http://9gag.com/tv
Aol Videos	http://on.aol.com
Bambuser	http://bambuser.com/broadcasts
Berify	https://berify.com
Bing Videos	http://www.bing.com/?scope=video
Crackle	https://www.sonycrackle.com
Custom YouTube Search Tools	https://inteltechniques.com/osint/menu.youtube.html
DailyMotion	http://www.dailymotion.com
DownloadGram	https://downloadgram.com
Download Twitter Video	http://www.downloadtwittervideo.com
Dogpile Video Search	https://www.dogpile.com/?qc=video
D Tube	https://d.tube
Geosearch	http://www.geosearchtool.com
Giphy	https://giphy.com
Google Video Search	https://www.google.com/videohp
Internet Archive: Open Source Videos	https://archive.org/details/opensource_movies
LiveLeak	http://www.liveleak.com
Metacafe	http://www.metacafe.com
Metatube	http://www.metatube.com
MySpace Videos	https://myspace.com/discover/videos

The Open Video Project	https://open-video.org
Reverse Video Search Tools	https://inteltechniques.com/osint/menu.reverse.html
Smugmug	https://www.smugmug.com/search
Snap Map	https://map.snapchat.com
Spaactor	https://www.spaactor.com
Spotter	https://spotter.tech
Startpage Videos	https://www.startpage.com/eng/video.html
TV News Archive	https://archive.org/details/tv
Xplore	http://getxplore.com
Veoh	http://www.veoh.com
Vimeo	https://vimeo.com
Voxalead	http://voxalead.labs.exalead.com
Yahoo Video Search	http://video.search.yahoo.com
Yasiv	http://yasiv.com/youtube
YouTube	https://www.youtube.com
YouTube GeoSearch	http://youtube.github.io/geo-search-tool/search.html

Live Streaming and Webcams

Tool	Link
123webcam	http://123webcam.com
Airport Webcams	http://airportwebcams.net
Bambuser	http://bambuser.com
camvista	http://www.camvista.com
Earthcam	http://www.earthcam.com
Facebook Livemap	https://www.facebook.com/live/map
Flixwagon	http://www.flixwagon.com
Freedocast	http://www.freedocast.com
Insecam	http://www.insecam.org
KeepVid	https://keepvid.com
Krooz Cams	http://www.kroooz-cams.com
Liveleak	https://liveleak.com
Livestream	https://livestream.com
Lookr	https://www.lookr.com
MetaCafe	http://www.metacafe.com
Motorway Cameras	https://www.motorwaycameras.co.uk
OnPeriscope	http://onperiscope.com
OpenStreetCam	https://www.openstreetcam.org
Opentopia	http://www.opentopia.com
Periscope	https://www.periscope.tv
Periscope Map	http://www.periscopemap.live
Periscope Streams	http://onperiscope.com
Perisearch	https://www.perisearch.xyz
PeriViewer	http://periviewer.com

Rail Webcams	http://railwebcams.net
RecPeriscope	http://www.recperiscope.com
Scopedown	http://downloadperiscopevideos.com
See All The Things	https://github.com/baywolf88/seeallthethings
tchannels	https://www.tchannels.tv
Twitch	https://www.twitch.tv
Ustream	http://www.ustream.tv/explore/all
Vaughn Live TV	https://vaughnlive.tv
Vevo	https://www.vevo.com
Vimeo	https://vimeo.com
Webcams Travel	https://www.webcams.travel
WorldCam	https://worldcam.eu
YouNow	https://www.younow.com
YouTube	https://www.youtube.com

Other Video Tools

Tool	Link
Applian	http://applian.com
Avidemux	http://avidemux.sourceforge.net
Clip Converter	https://www.clipconverter.cc
Convertio TS to MP4	https://convertio.co/ts-mp4
Deturl	http://deturl.com
DownFacebook	http://www.downfacebook.com
DownloadHealper	http://www.downloadhelper.net
Download Persicope Videos	http://downloadperiscopevideos.com
Download Subtitle	http://downsub.com
Download Twitter Video	https://www.downloadtwittervideo.com
Downvids.net	http://www.downvids.net
Dredown	http://www.dredown.com
eclips	https://eclips.io
FBDOWN	http://www.fbdown.net
Flash Video Downloader	https://chrome.google.com/webstore/detail/flash-video-downloader/aiimdkdngfcipjohbjenkahhlhccpdbc?hl=de
Format Factory	http://www.pcfreetime.com/formatfactory/index.php
Frame by Frame	https://chrome.google.com/webstore/detail/frame-by-frame-for-youtub/elkadbdicdciddfkdpmaolomehalghio?hl=en-GB
Freemake Video Converter	http://www.freemake.com/free_video_converter/
Free Video Downloader	https://chrome.google.com/webstore/detail/free-video-downloader/ppgadljdflpomdcdacknofppeejgmjdn?hl=de
Handbrake	https://handbrake.fr
hooktube	https://hooktube.com

InVID	http://www.invid-project.eu/tools-and-services/invid-verification-plugin
Invideo for YouTube	https://chrome.google.com/webstore/detail/invideo-for-youtube/iacbjlffnpbhgkgknabhkfmlcpdcigab?
Keep for Chrome	https://chrome.google.com/webstore/detail/keep-for-chrome/ghhhikeonlfpibbaibecmiellnmaikoh
KEEPVID	http://keepvid.com
Logos	http://logos.iti.gr
Montage	https://montage.storyful.com
Orbit Downloader	http://www.orbitdownloader.com
OwlZoom	https://addons.mozilla.org/en-US/firefox/addon/owlzoom-youtube/
Savefrom.net	http://de.savefrom.net
SaveVideo	http://savevideo.me
Softorino YouTube Converter	https://softorino.com/youtube-converter-2
trint	https://trint.com
TubeCHop	http://www.tubechop.com
TWDOWN	https://twdown.net
VDownloader	https://vdownloader.com
Video Downloader Professional	https://chrome.google.com/webstore/detail/video-downloader-professi/elicpjhcidhpjomhibiffojpinpmmpil?hl=de
Video Vault	https://www.bravenewtech.org
VideoVault for Chrome	https://chrome.google.com/webstore/detail/videovault-for-chrome/onoidkfboifjplllldnfnaebfigijckmk
Watch Frame by Frame	http://www.watchframebyframe.com
Y2mate	https://y2mate.com
YooDownload	http://yoodownload.com
Yout	https://yout.com
YouTube Comment Scraper	http://ytcomments.klostermann.ca
YouTube Converter	https://youtubeconvert.cc
YouTube Data Tools	https://tools.digitalmethods.net/netvizz/youtube
YouTube DataViewer	https://www.amnestyusa.org/citizenevidence
Youtube-dl	https://rg3.github.io/youtube-dl
YouTube MP3 Conventer	https://www.ytbmp3.com

YouTube Playlist Analyzer	https://youtube-playlist-analyzer.appspot.com
YouTube Restriction Check	http://polsy.org.uk/stuff/ytrestrict.cgi?ytid=vg7wh_zf2X0
ZamZar TS to MP4	http://www.zamzar.com/convert/ts-to-mp4

Video Editors

Tool	Link
Camtasia	https://www.techsmith.com/video-editor.html
Clip Champ Create	https://clipchamp.com/en/video-editor
DaVinci Resolve	https://www.blackmagicdesign.com/products/davinciresolve
Filmora	https://filmora.wondershare.com
FreeMake	http://www.freemake.com/free_video_converter/?irgwc=1&clickid=wFUzM2U6bT5VXz3zG83eA0TwUkjyvo2GP3k3xA0
Hitfilm Express	https://hitfilm.com/express
iMovie (Mac)	https://www.apple.com/imovie
Kizoa	https://www.kizoa.com/Video-Editor
Lightworks	https://www.lwks.com
Machete	http://www.machetesoft.com
Media 100	https://www.media100.com
Movie Maker Online	http://moviemakeronline.com
NCH Software	http://www.nchsoftware.com/videopad
Online Video Cutter	https://www.wevideo.com
Open Shot Video Editor	https://www.openshot.org
Powtoon	https://www.powtoon.com/home/?
Video Toolbox	http://www.videotoolbox.com
VSCD Free Video Editor	http://www.videosoftdev.com
Wideo	https://wideo.co
WeVideo	https://www.wevideo.com
Windows Movie Maker - Free	https://www.microsoft.com/en-us/store/p/movie-maker-free/9mvfq4lmz6c9

YouTube Video Editor	https://support.google.com/youtube/answer/183851?visit_id=0-636615121384437440-336407512&p=video_editor&hl=en&rd=1

Working with Audio

Radio

Tool	Link
Accuradio	https://www.accuradio.com
AntennaSearch	http://www.antennasearch.com
Antenna Structure Registration Search	http://wireless2.fcc.gov/UlsApp/AsrSearch/asrRegistrationSearch.jsp
Aprs.fi	https://aprs.fi/#!lat=40.51860&lng=-74.34990
ArtSci	http://www.artscipub.com/repeaters
BCC World Service Radio	http://bbcworldservice.radio.net
Broadcastify	http://www.broadcastify.com
Cell Reception	http://www.cellreception.com/towers
City Freq	https://www.cityfreq.com
Digital Frequency Search	https://digitalfrequencysearch.com/index.php
DX Zone	https://www.dxzone.com
HF Underground	https://www.hfunderground.com/board
Home Patrol	http://homepatrol.com
Intercept Radio	http://www.interceptradio.com/bbs
Listenlive	http://www.listenlive.eu
Live365	https://live365.com/listen
Live ATC	https://www.liveatc.net
National Radio Data	http://www.nationalradiodata.com
Police Scanner Info	https://police-scanner.info

Radio.com	https://player.radio.com/station-directory
Radio-locator	https://radio-locator.com
RadioReference	http://www.radioreference.com
Radio Station World	http://radiostationworld.com
Radio Tower	http://radiotower.com
RD Forum	https://www.rdforum.org/index.php
Scanner Master Blog	http://www.scannermasterblog.com/tag/scanner-radio
Streema	https://streema.com
Strong Signals	https://strongsignals.net
TuneIn	https://tunein.com
World Wide DX	https://www.worldwidedx.com/forums/scanning-shortwave-listening.83
Worldwide Radio	http://www.live-radio.net/worldwide.shtml
Zip Scanners	https://www.zipscanners.com/resources/police-scanner-resources-forums-links

Podcasts

Tool	Link
Anchor	https://anchor.fm
Antennapod	http://antennapod.org
BeyondPod	http://www.beyondpod.mobi
Blubrry Podcast Directory	https://create.blubrry.com/resources/blubrry-podcast-directory
Breaker	https://breaker.audio
Castbox	https://castbox.fm
Castro	http://supertop.co/castro
Deepgram	https://www.deepgram.com
Doggcatcher	http://www.doggcatcher.com
Downcast	http://www.downcastapp.com
Edge of the Web Radio	https://edgeofthewebradio.com/seo-podcast
Fyyd	https://fyyd.de
iCatcher! Podcast Player	http://www.joeisanerd.com/apps
iPodder	http://www.ipodder.org
iTunes Podcasts	http://www.apple.com/itunes/podcasts
Listen Notes	https://www.listennotes.com
NPR Podcast Directory	https://www.npr.org/podcasts
Player FM	https://player.fm
Overcast	https://overcast.fm
Pocket Casts	http://www.shiftyjelly.com/pocketcasts
Pocket Casts Voodoo	https://chrome.google.com/webstore/detail/pocket-casts-voodoo/eipnphplecohckkjkgldkmmkgdfbmlek

Podbean	https://www.podbean.com
Podcast App	https://chrome.google.com/webstore/detail/podcast-app/hdpgebcembbojpibjdjbjpnekmabmjmp
Podcast Fast Track	https://podcastfasttrack.com
Podcast Player Prime	https://mybrowseraddon.com/podcast-player.html
Podcast Republic	http://podcastrepublic.net
Podcast Search	http://podcastsearch.david-smith.org
Podcasts	http://www.podcasts.com
Podible	https://podible.co
Podkicker	https://play.google.com/store/apps/details?id=ait.podka&hl=en
podStation Podcast Player	https://chrome.google.com/webstore/detail/podstation-podcast-player/bpcagekijmfcocgjlnnhpdogbplajjfn
PRI SoundWorks	http://www.pri.org/soundworks
Read2me	https://read2me.online
RSSDemon News & Podcast Reader	https://play.google.com/store/apps/details?id=com.meecel.feedreader.RssDemonAd&hl=en
RSS Radio	http://rssrad.io
SmarterPod	https://chrome.google.com/webstore/detail/smarterpod-simple-and-sma/ehlmnfeohfahemdjnakciaheggkojchf
SoundCloud Player	https://chrome.google.com/webstore/detail/soundcloud-player/geamkdoeadoihdcnnkanojmdegppdmkh
SoundCloud Podcasting	https://soundcloud.com/for/podcasting
Spaactor	https://www.spaactor.com
Speaker Podcast Radio	https://www.spreaker.com/download/spreaker-podcast-radio
Stabl	http://www.wearestabl.com
Stitcher	https://www.stitcher.com
The Audacity to Podcast	https://theaudacitytopodcast.com/tap069-top-podcast-directories-and-how-to-get-in-them
tumello	https://tumello.com/search
wecast	http://www.wecastapp.com
Winds	https://getstream.io/winds

Other Audio Tools

Tool	Link
descript	https://www.descript.com
FluidData	https://fluiddata.com
Play.ht	https://play.ht/landing
Rightspeed	https://itunes.apple.com/us/app/rightspeed-the-speed-listening-app/id1104515047?mt=8
Spext	https://www.spext.co
trint	https://trint.com

Working with Documents

Documents and Slides Search

Tool	Link
Ask the EU	https://www.asktheeu.org
Authorstream	http://www.authorstream.com
Court Listener	https://www.courtlistener.com/recap
Custom Document Search by Format	https://inteltechniques.com/osint/docs.format.html
Custom Documents Search Tool	https://inteltechniques.com/osint/docs.html
Declassified and Ratified	http://www.declassifiedandratified.com
DocumentCloud Search	https://www.documentcloud.org/public/search
Edocs-Engine.com	http://www.edocs-engine.com
Find-pdf-doc	http://www.findpdfdoc.com
Free Full PDF	http://www.freefullpdf.com
goofile	https://tools.kali.org/information-gathering/goofile
Hashdoc	https://www.hashdoc.com
Inevstigative Dashboard Search	https://data.occrp.org
Offshore Leak Database	https://offshoreleaks.icij.org
PDF Search Engine	http://www.pdfsearchengine.info
PDFSR	http://pdfsr.com
RECAP	http://archive.recapthelaw.org
Scribd	http://www.scribd.com
SlideSearchEngine	http://www.slidesearchengine.com

SlideShare	http://www.slideshare.net
Slideworld	http://www.slideworld.com
soPDF.com	http://www.sopdf.com

Pastebins

Tool	Link
Custom Pastebin Search	https://inteltechniques.com/osint/menu.pastebins.html
Pastebin	https://pastebin.com
PasteLert	https://andrewmohawk.com/pasteLert
Paste Site Search	http://netbootcamp.org/pastesearch.html

Document and Reference Management

Tool	Link
Colwiz	https://www.colwiz.com
DocumentCloud	https://www.documentcloud.org
Endnote	http://endnote.com
F1000	http://f1000.com
Investigative Dashboard Search	https://data.occrp.org
Mendeley	https://www.mendeley.com
Omnity	https://www.omnity.io
Open Semantic Desktop Search	https://www.opensemanticsearch.org/doc/desktop_search
Overview	https://www.overviewdocs.com
Readcube	https://www.readcube.com
RefME	https://www.refme.com
Zotero	https://www.zotero.org

PDF Management

Tool	Link
CleverPDF	https://www.cleverpdf.com
Foxit Reader	https://www.foxitsoftware.com/products/pdf-reader
ilovepdf	http://www.ilovepdf.com
PDFEscape	https://www.pdfescape.com
PDFExpert	https://pdfexpert.com
PDFx	http://www.metachris.com/pdfx
Smallpdf	http://smallpdf.com
Tabula	http://tabula.technology
Weava Highlighter	https://chrome.google.com/webstore/detail/weava-highlighter-pdf-web/cbnaodkpfinfiipjblikofhlhlcickei
XODO	http://xodo.com
Xpdf	http://www.foolabs.com/xpdf/home.html

Working with Document Metadata

Tool	Link
Doc Scrubber	http://www.brightfort.com/docscrubber.html
ExtractMetadata	http://www.extractmetadata.com
FOCA	https://www.elevenpaths.com/labstools/foca/index.html
Metashield Clean-up-Online	https://metashieldclean-up.elevenpaths.com
OOMetaExtractor	https://archive.codeplex.com/?p=oometaextractor
Pdf-redact-tools	https://github.com/firstlookmedia/pdf-redact-tools
Spiderpig	https://github.com/hatlord/Spiderpig

Academic Resources and Grey Literature

Academic and Grey Literature Research Tools

Tool	Link
Academia	https://www.academia.edu
Academic Index	http://www.academicindex.net
Academic Journals	http://www.academicjournals.org
African Journals Online	http://www.ajol.info
Altmetric	https://www.altmetric.com
American Society of Civil Engineers	http://ascelibrary.org
AMiner	https://aminer.org
Archive	https://archive.org
arXiv	https://arxiv.org
A-Z Library Databases	http://guides.uflib.ufl.edu/az.php
Base	http://www.base-search.net
Beyond Citation	http://www.beyondcitation.org
Bibsonomy	http://www.bibsonomy.org
bioRxiv	https://www.biorxiv.org
Cambridge Journals	http://journals.cambridge.org
Citation Machine	http://www.citationmachine.net
citeulike	http://www.citeulike.org
copac	https://copac.jisc.ac.uk
Core	https://core.ac.uk
deepdyve	https://www.deepdyve.com
Elsevier	https://www.elsevier.com

ERIC	https://eric.ed.gov
EThOS	http://ethos.bl.uk
Etymo	https://etymo.io
Europeana	https://www.europeana.eu
Europe PMC	http://europepmc.org
figshare	https://figshare.com
Focus	https://focus.universite-paris-saclay.fr
The Getty Research Institute	http://www.getty.edu/research/library
Google Scholar	https://scholar.google.com
Google Scholar Button	https://chrome.google.com/webstore/detail/google-scholar-button/ldipcbpaocekfooobnbcddclnhejkcpn
Grey Guide	http://greyguide.isti.cnr.it
Grey Literature (HLWIKI International)	http://hlwiki.slais.ubc.ca/index.php/Grey_literature
Grey Literature – List of Gateways	http://csulb.libguides.com/graylit
Grey Literature Report	http://www.greylit.org
Grey Literature Strategies	http://greylitstrategies.info
GreyNet International	http://www.greynet.org
Hathi Trust Digital Library	https://www.hathitrust.org
HighWire: Free Online Full-text Articles	http://highwire.stanford.edu/lists/freeart.dtl
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp
International Affairs Resources	https://internationalaffairsresources.com
IssueLab	https://www.issuelab.org
Journal Guide	https://www.journalguide.com
Journal Seek	http://journalseek.net
JSTOR	http://www.jstor.org
KFF	https://www.kff.org
Lazy Scholar	http://www.lazyscholar.org
Libguides Community	https://community.libguides.com
Library of Congress	https://www.loc.gov
Mednar	https://mednar.com
Microsoft Academic	https://academic.microsoft.com
National Archives	https://www.archives.gov/research/catalog

NRC Research Press	http://www.nrcresearchpress.com
Open Access Scientific Journals	http://www.pagepress.org
OpenAIRE	https://www.openaire.eu
Open DOAR	http://v2.opendoar.sherpa.ac.uk
Open Grey	http://www.opengrey.eu
Open Knowledge Maps	https://openknowledgemaps.org
Open Syllabus Explorer	http://explorer.opensyllabusproject.org
The Open Syllabus Project	http://opensyllabusproject.org
OSF Preprints	https://osf.io/preprints/discover
OSTI.GOV	https://www.osti.gov
Oxford Journals	http://www.oxfordjournals.org
PAGEPress Publications	https://www.pagepress.org
PhilPapers	https://philpapers.org
PLOS	https://www.plos.org
PQDT Open	https://pqdtopen.proquest.com/search.html
PubMed	http://www.ncbi.nlm.nih.gov/pubmed
PubPeer	https://pubpeer.com
Quertle	https://quertle.com
Quetzal Search	https://www.quetzal-search.info
refseek	https://www.refseek.com
Research Gate	http://www.researchgate.net
REPEC	http://repec.org
Retraction Watch	https://retractionwatch.com
SAGE Journals	http://journals.sagepub.com
ScienceDirect	http://www.sciencedirect.com
ScienceDomain	http://www.sciencedomain.org
Science.gov	https://www.science.gov
Science Publications	http://www.thescipub.com
Science Research	http://www.scienceresearch.com
SCIRP	http://www.scirp.org
Scholar Universe	http://www.scholaruniverse.com
Semantic Scholar	https://www.semanticscholar.org
SOC ARXIV	https://osf.io/preprints/socarxiv

Sparrho	https://www.sparrho.com
Springer	http://link.springer.com
SSRN	https://www.ssrn.com
Sweet Search	https://www.sweetsearch.com
Taylor & Francis Online	http://www.tandfonline.com
TechXtra	http://www.techxtra.ac.uk
Unpaywall	https://chrome.google.com/webstore/detail/unpaywall/iplffkdpngmdjhlpjmppncnlhomiipha?hl=en
Video Lectures	http://videolectures.net
Wiley	http://eu.wiley.com
World Digital Library	http://www.wdl.org
World Science	http://worldwidescience.org
zenodo	https://zenodo.org
Zetoc	http://zetoc.jisc.ac.uk

Lectures, Talks, Conference Presentations, Speeches

Lectures, Talks, Conference Presentations, Speeches

Tool	Link
Academic Earth	https://academicearth.org
All Conferences	http://www.allconferences.com
AutoDesk University	http://au.autodesk.com
American Archive of Public Broadcasting	http://americanarchive.org
Brown University Library	https://library.brown.edu
Cornell University Archive	http://societyhumanities.as.cornell.edu/events-archive
Deepgram	https://www.deepgram.com
Elsevier	https://www.elsevier.com/events/conferences
Findlectures	https://www.findlectures.com
Global Academy for Medical Education	https://www.globalacademycme.com/conferences-archive
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp
iTunes U	https://itunes.apple.com/us/app/itunes-u/id490217893?mt=8
Kennedy Center Lecture Archive	http://kennedy.byu.edu/lectures
Nature.com	https://www.nature.com/natureevents/science
Nursing Network	https://www.nursingnetwork.com/nursing-events
Open University	http://www.open.ac.uk/#
Renal Archive	http://www.renalarchive.org
Royal Society of Chemistry	http://www.rsc.org/event
Speakerdex	https://speakerdex.co

Streaming Media	http://www.streamingmedia.com/conferences
Talks at Google	https://talksat.withgoogle.com
Ted	https://www.ted.com
The Great Courses	https://www.thegreatcourses.com
UCI School of Social Science	https://www.democracy.uci.edu/resources/asia/index.php

Books and Reading

Books Search and Reading Tools

Tool	Link
100 Million Book	http://www.100millionbooks.org
Amazon Cheap Books	http://www.amazon.com/b?tag=mak041-20&linkCode=as2&ie=UTF8&node=2245146011
Audible	http://www.audible.com
Auditus	https://auditus.cc
Bibliomania	http://www.bibliomania.com
Blinkist	https://www.blinkist.com
Bookbub	https://www.bookbub.com
BookClub	https://bookclub.cool
Bookish	https://www.bookish.com
Booklikes	http://booklikes.com
Bookmate	https://bookmate.com
Bookseer	http://bookseer.com
Books on the Knob	http://blog.booksontheknob.org
Bookstr	https://www.bookstr.com
Calibre	http://www.calibre-ebook.com
Daily Cheap Reads	http://www.dailycheapreads.com
Europeana	https://www.europeana.eu
Favobooks	http://favobooks.com
Free Kindle Books	http://freekindlebooks.org
The Getty Research Institute	http://www.getty.edu/research/library

Gnooks	http://www.gnooks.com
Google Books	https://books.google.com
Goodreads	http://www.goodreads.com
Hathi Trust Digital Library	https://www.hathitrust.org
How Long To Read	https://www.howlongtoreadthis.com
I love my Kindle	https://ilmk.wordpress.com
Internet Archive Texts	http://archive.org/details.php?identifier=texts
ISBN Plus	http://isbnplus.com
Jellybooks	https://www.jellybooks.com
Just Free Books	http://www.justfreebooks.info
Keendly	http://keendly.com
KindleNationDay	http://kindlenationdaily.com
KindleWorld	http://kindleworld.blogspot.com
Lendle	http://lendle.me
LibraryThing	https://www.librarything.com
Librivox	https://librivox.org
Loyal Books	http://www.loyalbooks.com
Many Books	http://manybooks.net
Narro	https://www.narro.co
The Online Books Page	http://digital.library.upenn.edu/books/search.html
Open Culture: Free Audiobooks	http://www.openculture.com/freeaudiobooks
OpeningtheBook	http://www.openingthebook.com
Open Library	https://openlibrary.org
Overdrive	https://www.overdrive.com
ParrotRead	http://parrotread.com
Pixel of Ink	http://www.pixelofink.com
Project Gutenberg	http://www.gutenberg.org
Read	https://medium.com/@readapp/introducing-read-for-ios-de4d2799254a#.z3lrigjr7
Reader IQ	http://www.ereaderiq.com
Readgeek	http://www.readgeek.com
Readism	https://chrome.google.com/webstore/detail/readism-article-reading-t/bmiolhceebkeljaikojgcoeefblcihje

Readlax	https://chrome.google.com/webstore/detail/readlax-speed-reading/noggimpgfjnknjbldfibbdnocffdoii
Readwise	https://readwise.io
Reddit: 52 Weeks, 52 Books	https://www.reddit.com/r/52book
Riffle	https://www.rifflebooks.com
SendtoKindle	https://addons.mozilla.org/en-US/firefox/addon/sendtokindle/?src=search
Talk to Books:	https://books.google.com/talktobooks
TasteDive: Books	https://tastedive.com/books
TheBooksProject	http://thebooksproject.co
TheFrugaleReader	http://www.thefrugalereader.com
The Online Books Page	http://digital.library.upenn.edu/books/search.html
Tinderizer	http://tinderizer.com
Toolinbox Klib	https://en.toolinbox.net/Klib
WhatShouldIReadNext	http://www.whatshouldireadnext.com
YourNextRead	http://www.yournextread.com

Working with Data and Statistics

Data and Statistics

Tool	Link
AGOA Data Center	http://agoa.info
AidData	http://aiddata.org
ADB Statistics and Databases	http://www.adb.org/data/statistics
Archeology Data Service	http://archaeologydataservice.ac.uk
AWS Public Datasets	http://aws.amazon.com/datasets
Bank for International Settlements Statistics	http://www.bis.org/statistics/index.htm
Beyond Citation	http://www.beyondcitation.org
BP Statistical Review of World Energy	http://www.bp.com/en/global/corporate/energy-economics/statistical-review-of-world-energy.html
Berkely Library: Data Lab	http://www.lib.berkeley.edu/libraries/data-lab
Bizstats	http://www.bizstats.com
CIA World Factbook	https://www.cia.gov/library/publications/the-world-factbook
Center for International Earth Science Information Network	http://www.ciesin.org
Center for Global Development	https://www.cgdev.org/commitment-development-index-2017
CEPII	http://www.cepii.fr/CEPII/en/welcome.asp
Data 360	http://www.data360.org
Data BASIC	https://databasic.io
Data Catalog	https://catalog.data.gov/dataset
Data Europa	https://data.europa.eu

Data.gov.uk	https://data.gov.uk
Datawrapper	https://www.datawrapper.de
DBPedia	http://wiki.dbpedia.org
DRYAD	https://datadryad.org
EMBL-EBI	https://www.ebi.ac.uk
European Commission Eurobarometer	http://ec.europa.eu/COMMFrontOffice/PublicOpinion
European Union Open Data Portal	http://open-data.europa.eu/en/data
Eurostat	http://ec.europa.eu/eurostat
FAIRsharing.org	https://fairsharing.org
FAOSTAT	http://faostat3.fao.org
FRED	https://fred.stlouisfed.org
Gapminder World	http://www.gapminder.org/data
globalEDGE Database of International Business Statistics	http://globaledge.msu.edu/tools-and-data/dibs
Google Finance	https://www.google.com/finance
Google Fusion Tables	https://support.google.com/fusiontables/answer/2571232
Google Public Data Explorer	http://www.google.com/publicdata/directory
GOVDATA	https://www.govdata.de
Government of Canada Open Data	http://open.canada.ca/en
IHS Piers	https://www.ihs.com/products/piers.html
Human Development Reports	http://hdr.undp.org/en/global-reports
IDEA Databases	https://www.idea.int/data-tools
International Labour Comparisons	http://www.bls.gov/fls/chartbook.htm
International Trade Center	http://www.intracen.org/ByCountry.aspx
ILOSTAT	https://www.ilo.org/ilostat
ILO World Employment and Social Outlook Trends	http://www.ilo.org/global/research/global-reports/weso/sustainable-enterprises-and-jobs-2017/lang--en/index.htm
IMF Data	http://www.imf.org/en/Data
IMF World Economic Outlook Databases	http://www.imf.org/external/ns/cs.aspx?id=28
Index Mundi	http://www.indexmundi.com
International Energy Agency Energy Atlas	http://energyatlas.iea.org

International Energy Agency Statistics	http://www.iea.org/statistics
Junar	http://junar.com
Knoema	https://knoema.com
LandMatrix	http://landmatrix.org
Latinobarometro	http://www.latinobarometro.org
Library, University of Michigan: Statistics and Datasets	http://www.lib.umich.edu/browse/Statistics%20and%20Data%20Sets
Maptia	https://maptia.com
Nation Master	http://www.nationmaster.com/statistics
OECD Aid Database	http://www.oecd.org/dac/stats/data.htm
OECD Data	https://data.oecd.org
OECD Factbook	http://www.oecd-ilibrary.org/economics/oecd-factbook_18147364
OECD Statistics Directorate	http://www.oecd.org/std
OFFSTATS	http://www.offstats.auckland.ac.nz
Open Data Network	http://www.opendatanetwork.com
Open Data Portal	http://www.opendataportal.at
Open Data Portal Munich	https://www.opengov-muenchen.de
Open Data Showroom	http://opendata-showroom.org
Open Government Data	http://opengovernmentdata.org/data
Paul Hensel's General Informational Data	http://www.paulhensel.org/dataintl.html
Pew Research Center	http://www.pewinternet.org/datasets
Population Reference Bureau Data Finder	http://www.prb.org/DataFinder.aspx
PRS Risk Indicators	http://www.prsgroup.com
Public Open Data Soft	https://public.opendatasoft.com/explore/?sort=modified
Quandl	https://www.quandl.com
Re3data.org	https://www.re3data.org
Research Pipeline	http://www.researchpipeline.com
SESRIC Basic Social and Economic Indicators	http://www.sesric.org/baseind.php
SESRIC Databases	http://www.sesric.org/databases-index.php

Statista	http://www.statista.com
Statpedia	https://statpedia.com
The Atlas of Economic Complexity	http://atlas.cid.harvard.edu
The Data and Story Library	http://lib.stat.cmu.edu/DASL
Trading Economics	http://www.tradingeconomics.com
Transparency.org Corruption Perception Index	https://www.transparency.org/news/feature/corruption_perceptions_index_2016
UK Data Service	https://www.ukdataservice.ac.uk
UN COMTRADE Database	http://comtrade.un.org
UNCTAD Country Fact Sheets	http://unctad.org/en/Pages/DIAE/World%20Investment%20Report/Country-Fact-Sheets.aspx
UNCTAD Investment Country Profiles	http://unctad.org/en/Pages/Publications/Investment-country-profiles.aspx
UNCTAD STAT	http://unctadstat.unctad.org
UN Data	http://data.un.org
UNDP's Human Development Index	http://hdr.undp.org/en/data
UNECE	http://w3.unece.org/PXWeb/en
UNESCO Institute for Statistics	http://www.uis.unesco.org
UNIDO Statistical Databases	http://www.unido.org/resources/statistics/statistical-databases.html
UNStats Social Indicators	http://unstats.un.org/unsd/demographic/products/socind
US Census Bureau	https://www.census.gov
Visual Investigative Scenarios	https://vis.occrp.org
Vizala	https://vizala.com
Upsala Conflict Data Program	http://www.pcr.uu.se/research/UCDP
US Data and Statistics	https://www.usa.gov/statistics
WHO Data	http://www.who.int/gho/en
Wikidata	https://www.wikidata.org
World Bank Data Catalog	https://datacatalog.worldbank.org
World Bank Global Consumption Database	http://datatopics.worldbank.org/consumption/home
World Bank Open Data	http://data.worldbank.org
World Bank Doing Business	http://www.doingbusiness.org

World Bank Enterprise Surveys	http://www.enterprisesurveys.org
World Bank Investing Across Borders	http://iab.worldbank.org
World Integrated Trade Solution	http://wits.worldbank.org
WTO Statistics	https://www.wto.org/english/res_e/statis_e/statis_e.htm
Zanran	http://zanran.com

Infographics and Data Visualization

Tool	Link
Adobe Color CC	https://color.adobe.com/create/color-wheel
Aeon	http://www.aeontimeline.com
Arbor.js	http://arborjs.org
BeakerX	http://beakerx.com
Befunky	https://www.befunky.com
Bizint	http://www.bizint.com
Cacoo	https://cacoo.com
Canva	https://www.canva.com
chartblocks	http://www.chartblocks.com
Charted	http://www.charted.co
Chartico	http://chartico.com
Chart.js	http://www.chartjs.org
Circos	http://circos.ca
creately	http://creately.com
Crossfilter	http://square.github.io/crossfilter
csvkit	https://github.com/wireservice/csvkit
DataBasic.io	https://databasic.io
Data Visualization Catalogue	http://datavizcatalogue.com
D3js	https://d3js.org
Datawrapper	https://datawrapper.de
dygraphs	http://dygraphs.com
easely	http://www.easel.ly
Exhibit	http://www.simile-widgets.org/exhibit
Flot	http://www.flotcharts.org

FusionCharts	http://www.fusioncharts.com
Google Developers: Charts	https://developers.google.com/chart
Google Fusion Tables	https://support.google.com/fusiontables/answer/2571232
GraphX	http://spark.apache.org/graphx
Highcharts	http://www.highcharts.com
Hohli	http://charts.hohli.com
Inkscape	https://inkscape.org
Infogr.am	https://infogr.am
Java Infovis Toolkit	http://philogb.github.io/jit
JpGraph	http://jpgraph.net
jqPlot	http://www.jqplot.com
Knoema	https://knoema.com
Leaflet	http://leafletjs.com
Listify	http://listify.okfnlabs.org
Linkuroius	http://linkurio.us
Lucidchart	https://www.lucidchart.com
Neo4j	https://neo4j.com
Nodebox	https://www.nodebox.net
OpenLayers	http://openlayers.org
Palladio	http://hdlab.stanford.edu/palladio
Piktochart	https://piktochart.com
Pixcone	http://www.pixcone.com
Pixxa	http://www.pixxa.com
Plotly	https://plot.ly
Sizzle	https://www.sizzleanalytics.com
SpicyNodes	http://www.spicynodes.org
QlikView	https://www.visualintelligence.co.nz/qlikview
Quadrigram	http://www.quadrigram.com
Raphael	http://dmitrybaranovskiy.github.io/raphael
RAW Graphs	http://app.rawgraphs.io
Shanti Interactive	http://www.viseyes.org
Snappa	https://snappa.io
Statpedia	http://statpedia.com

Tableau	http://www.tableau.com
Tableau Public	https://public.tableau.com
Textures.js	https://riccardoscalco.github.io/textures
Tiki-toki	http://www.tiki-toki.com
Tik-tok	https://datanews.github.io/tik-tok
Timeflow	https://github.com/FlowingMedia/TimeFlow/wiki
Timeglider	http://timeglider.com/widget
Timeline	http://timeline.knightlab.com
Timeline	http://www.simile-widgets.org/timeline
Timeline Maker	https://www.timelinemaker.com
Timetoast	http://www.timetoast.com
Word Art	https://wordart.com
Wordle	http://www.wordle.net
Venngage	https://venngage.com
Visage	https://visage.co
Vis.js	http://visjs.org
Visme	http://www.visme.co
Visual Investigative Scenarios	https://vis.occrp.org
Visualize.me	http://vizualize.me
visually	https://visual.ly
Vortex	http://www.dotmatics.com/products/vortex
ZingChart	http://www.zingchart.com

Dashboard Tools

Tool	Link
Analytics Portfolio	https://analyticsportfolio.com
Chartio	https://chartio.com
Clicdata	http://www.clicdata.com
Cyfe	http://www.cyfe.com
Dashthis	https://dashthis.com
DataDeck	https://www.datadeck.com
Geckoboard	https://www.geckoboard.com
Happy Metrics	https://www.happymetrix.com
Klipfolio	http://www.klipfolio.com
Qlik	http://www.qlik.com
Visually	http://visual.ly

Data Analysis

Tool	Link
Automatic Statistician	https://www.automaticstatistician.com
Auto-WEKA	http://www.cs.ubc.ca/labs/beta/Projects/autoweka
AW Stats	http://www.awstats.org
bigML	https://bigml.com
Cloud Automl	https://cloud.google.com/automl
Countly	https://count.ly/web-analytics
DataCracker	https://www.datacracker.com
Dataiku DSS	https://www.dataiku.com/dss/trynow
Data Kleenr	http://chi2innovations.com/datakleenr
Data Pine	https://www.datapine.com/data-analysis-tools
Data Preparator	http://www.datapreparator.com
DataRobot	https://www.datarobot.com
Data Wrapper	https://www.datawrapper.de
Data Wrangler	http://vis.stanford.edu/wrangler
D3	https://d3js.org
eAnalytics	http://www.eanalytics.de
Exhibit	http://simile-widgets.org/exhibit
Exmerg	http://www.exmerg.com
Google Analytics	https://www.google.com/analytics/?gclid=CjwKEAiAh7WkBRCQj-_zwZvk52ISJADj7z8COo_vM67BKDQAuisEzPwsNZ5Yphpu7Q5x2MirmakiUxoCZ6fw_wcB#?modal_active=none
Google Data Studio	https://www.google.com/analytics/data-studio
Google Fusion Tables	https://support.google.com/fusiontables/answer/2571232
H2O.ai	https://www.h2o.ai

Import.io	https://www.import.io
JavaScript InfoVis Toolkit	http://philogb.github.io/jit
Knime Analytics Platform	https://www.knime.com/knime-analytics-platform
Matomo	https://matomo.org
Microsoft Azure Machine Learning Studio	https://studio.azureml.net
MLBase	http://mlbase.org
MLJAR	https://mljar.com
Mr. Data Converter	https://shancarter.github.io/mr-data-converter
OpenRefine	https://github.com/OpenRefine
Open Web Analytics	http://www.openwebanalytics.com
Orange	https://orange.biolab.si
Paxata	https://www.paxata.com
PDF Tables	https://pdftables.com
Public Open Data Soft	https://public.opendatasoft.com/explore/?sort=modified
Rapid Miner	https://rapidminer.com
R Project	https://www.r-project.org
Scumblr	https://github.com/Netflix/scumblr/wiki
SEM Rush	https://www.semrush.com
Tableau Public	https://public.tableau.com/s
Talend	https://www.talend.com/products/data-preparation#free-desktop
Trifacta	https://www.trifacta.com
Weka	https://www.cs.waikato.ac.nz/ml/weka
Zoho Reports	https://www.zoho.com/reports
Qlik View	http://global.qlik.com/us/landing/go-sm/qlikview/download-qlikview

Data Scrapers

Tool	Link
Agenty	https://www.agenty.com
Beautiful Soup	https://www.crummy.com/software/BeautifulSoup/bs4/doc
Big Data Made Simple	http://bigdata-madesimple.com/top-50-open-source-web-crawlers-for-data-mining
Cola	https://github.com/chineking/cola
Content Bomb	http://www.contentbomb.com
Connotate	https://www.connotate.com
Common Crawl	https://commoncrawl.org
Crawly	http://crawly.diffbot.com
Crawl Monster	https://www.crawlmonster.com
Cyotek WebCopy	https://www.cyotek.com/cyotek-webcopy
Data Miner	https://data-miner.io
Demiurge	https://github.com/matiasb/demiurge
Dexi.io	https://dexi.io
DiffBot	https://www.diffbot.com
FMiner	http://www.fminer.com
Getleft	https://sourceforge.net/projects/getleftdown
Grabby	https://grabby.io
Helium Scraper	http://www.heliumscraper.com/en/index.php?p=home
HTTrack	https://www.httrack.com
Import.io	https://www.import.io
Lassie	https://github.com/michaelhelmick/lassie
Listly	https://listly.io

Mechanical Soup	https://github.com/MechanicalSoup/MechanicalSoup
Octoparse	https://www.octoparse.com
Open Data Tools	http://opendata-tools.org/en/data
OutWit Docs	http://www.outwit.com/products/docs
OutWit Hub	http://www.outwit.com/products/hub
Parsehub	https://www.parsehub.com
Portia	https://scrapinghub.com/portia
Pyspider	https://github.com/binux/pyspider
Reaper	https://reaper.social || https://github.com/ScriptSmith/reaper/blob/master/README.md
Scraper	https://chrome.google.com/webstore/detail/scraper/mbigbapnjcgaffohmbkdlecaccepngjd
Scraper Wiki	https://scraperwiki.com
Scrapy	https://scrapy.org
Screen Scraper	https://www.screen-scraper.com
Sitebulb	https://sitebulb.com
UiPath	https://www.uipath.com/community
Web Harvy	https://www.webharvy.com
Webhose.io	https://webhose.io
Web Scraper	http://webscraper.io
80 Legs	http://80legs.com

Working with News

News Sources

Tool	Link
1st Headlines	http://www.1stheadlines.com
ABYZNewsLinks	http://www.abyznewslinks.com
AllYouCanRead	http://www.allyoucanread.com
AP	http://hosted.ap.org
Associated France Press (AFP)	http://www.afp.com
BBC News	http://www.bbc.co.uk/news
Bing News	http://www.bing.com/news
CNN	http://edition.cnn.com
DailyEarth	http://dailyearth.com
DPA International	http://www.dpa-international.com
The Economist Explorer	https://yvoschaap.com/economist
EMM	http://emm.newsbrief.eu/NewsBrief/clusteredition/en/latest.html
Euronews	http://www.euronews.com
Europe Media Monitor (EMM) NewsExplorer	http://emm.newsexplorer.eu
Factiva	http://www.dowjones.com/factiva
France24	http://www.france24.com
Good Gopher	http://www.goodgopher.com
Google News	https://news.google.com
Google News Print Archive	http://news.google.com/newspapers
HeadlineSpot	http://www.headlinespot.com

Inshorts	https://inshorts.com/en/read
Itar-Tass	http://www.itar-tass.com
Library of Congress – US Newspapers	http://chroniclingamerica.loc.gov/search/titles || http://chroniclingamerica.loc.gov
MagPortal	http://www.magportal.com
NewsBot	https://getnewsbot.com
News Map	http://newsmap.jp
News Now	http://www.newsnow.co.uk
Newseum - Today Front Pages	http://www.newseum.org/todaysfrontpages
NewsLookup	http://www.newslookup.com
Newsography	http://newsography.com
Newspaper Map	http://newspapermap.com
Newspaperindex	http://www.newspaperindex.com
Newspapers.com	http://www.newspapers.com
OnlineNewspapers	http://www.onlinenewspapers.com
Paperboy	http://www.thepaperboy.com
Patch	https://patch.com/map
PR Newswire	http://www.prnewswire.com
Press Reader	http://www.pressreader.com
Reuters	http://www.reuters.com
Silobreaker	http://www.silobreaker.com
storyzy	http://search.storyzy.com
TV News Archive	https://archive.org/details/tv
Wikinews	https://en.wikinews.org
Wikipedia: Current Events	https://en.wikipedia.org/wiki/Portal:Current_events
WorldNews	http://wn.com
World-Newspapers	http://www.world-newspapers.com
Yahoo News	http://news.yahoo.com
YouGotTheNews.com	http://yougotthenews.com

News Digest and Discovery Tools

Tool	Link
10000 Flies	http://www.10000flies.de
anderpink	https://anderspink.com
Banjo	https://ban.jo
Blende	https://launch.blendle.com
FastNews	https://fastnews.me
Flipboard	https://flipboard.com
Hubii	http://hubii.com
inkl	https://www.inkl.com
inshorts	https://www.inshorts.com
[INSIDE]	http://blog.inside.com
News360	https://news360.com
NewsBot	https://getnewsbot.com
News Explorer	https://betamagic.nl/products/newsexplorer.html
Nuzzle	http://nuzzel.com
Populast	http://populast.com
Press Reader	http://www.pressreader.com
Reality Brief	http://www.realitybrief.com
Reeder	http://reederapp.com
SmartNews	https://www.smartnews.com
Spike	http://www.newswhip.com
Superdesk	https://www.superdesk.org
TLDR World News	https://tldrworldnews.com
Topix	http://www.topix.com

Fact Checking

Tool	Link
AfricaCheck	https://africacheck.org
AIDR	http://aidr.qcri.org
Check	https://meedan.com/en/check
Checkdesk	https://meedan.com/en/checkdesk
Chequeado	http://chequeado.com
Citizen Desk	https://www.sourcefabric.org/en/citizendesk
CivikOwl	http://www.civikowl.com
Emergent	http://www.emergent.info
Fact Check	http://www.factcheck.org
Fakespot	https://www.fakespot.com
FirstDraftNews Check	https://chrome.google.com/webstore/detail/firstdraftnewscheck/japockpeaaanknlkhagilkgcledilbfk
Full Fact	https://fullfact.org
Hoaxy	https://hoaxy.iuni.iu.edu
InVID	http://www.invid-project.eu/tools-and-services/invid-verification-plugin
MediaBugs	http://mediabugs.org
Reporterslab Fact Checking	https://reporterslab.org/fact-checking
Snopes	http://www.snopes.com
StopFake	http://www.stopfake.org/en/news
Truly	http://www.truly.media
Trusted News	https://trusted-news.com
TrustServista	https://www.trustservista.com
Urban Legends	https://www.thoughtco.com/urban-legends-4132595

Verificado	https://verificado.mx
Verification Handbook	http://verificationhandbook.com
Verification Junkie	http://verificationjunkie.com
Verification Checklist	https://revealproject.eu/a-roadmap-to-the-truth
Verify Syria	http://www.verify-sy.com/en

Working with Foreign Language Content

Translation Tools

Tool	Link
2lingual	http://www.2lingual.com
Apertium	https://www.apertium.org
Babelfish	https://www.babelfish.com
Bab.la	https://en.bab.la
Bablic	https://www.bablic.com
Babylon	http://translation.babylon.com
Bing Translator	http://www.bing.com/translator
British Slang	http://www.britishslang.co.uk
Deepl Translator	https://www.deepl.com/translator
Dict.cn	http://dict.cn
Dictionary.com: Translation	http://translate.reference.com
FreeTranslation	http://www.freetranslation.com
Free Translator	http://www.free-translator.com
Free Website Translation	http://free-website-translation.com
Frengly	http://frengly.com
Gengo	http://gengo.com
Gizoogle	http://gizoogle.net/textilizer.php
Google Input Tools	https://www.google.com/inputtools/try
Google Translate	https://translate.google.com
Google Translate Extension	https://chrome.google.com/webstore/detail/google-translate/aapbdbdomjkkjkaonfhkkikfgjllcleb?hl=en
IdiomaX Translation	http://www.idiomax.com/online-translator.aspx

imTranslator	http://imtranslator.net/translation
India Typing	http://indiatyping.com/index.php/translations/english-to-hindi-translation
Irish Translator	http://www.whoohoo.co.uk/irish-translator.asp
iTranslate	https://www.itranslate.com
iTranslate Voice	http://itranslatevoice.com
Lexicool Translation	http://www.lexicool.com/translate.asp
Lexilogos	https://www.lexilogos.com
Linguee	http://www.linguee.com
LingvoSoftOnline	http://www.lingvozone.com
Microsoft Translator	http://www.microsoft.com/en-us/translator
Noslang	http://www.noslang.com
OdysseyTranslator	http://odysseytranslator.com
Online Translator	http://www.online-translator.com
Pleco	https://www.pleco.com
PROMT-Online	http://translation2.paralink.com
Reddit/r/translator	https://www.reddit.com/r/translator
Reverso	http://www.reverso.net
Reverso Dictionary	https://dictionary.reverso.net
Sco Translate	http://www.scotranslate.com
Slangit	http://slangit.com
Spanish Dict	http://www.spanishdict.com
South African Slang	http://www.rsa-overseas.com/features/slang.htm
Systran	http://www.systransoft.com
Trans8it	http://transl8it.com
Translate British	https://www.translatebritish.com
Translate.com	https://www.translate.com
Translation2	http://translation2.paralink.com
Unbabel	https://unbabel.com
Urban Dictionary	https://www.urbandictionary.com
Wiktionary	https://www.wiktionary.org
WorldLingo	http://www.worldlingo.com
WorldReference.com	http://www.wordreference.com

Yamli (Arabic Search Engine)	http://www.yamli.com
Yandex Translate	https://translate.yandex.ru

Web Monitoring

RSS Readers

Tool	Link
Awasu	http://www.awasu.com
Cappuccino	http://cappuccinoapp.com
CurioStudio	http://www.curiostudio.com
DiggReader	http://digg.com/login?next=%2Freader
Fedora Reeder	https://www.microsoft.com/en-us/store/p/fedora-reader/9nblgggzm828?ranMID=24542&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-f3VMyJK1Njf8DUSG_atALQ&tduid=(e939f887862d0b3f3ccbf2a2fb27c10c)(256380)(2459594)(TnL5HPStwNw-f3VMyJK1Njf8DUSG_atALQ)()
Feedafever	http://www.feedafever.com
FeedDemon	http://www.feeddemon.com
Feedenlarger	http://feedenlarger.com
Feedly	http://www.feedly.com
FeedReader	http://www.feedreader.com
Netvibes	http://www.netvibes.com
Newsblur	http://newsblur.com
Nextgen Reader	https://www.microsoft.com/en-us/store/p/nextgen-reader/9wzdncrfj262?ranMID=24542&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-RfRFLElSGFCdyaiTXT53gg&tduid=(e939f887862d0b3f3ccbf2a2fb27c10c)(256380)(2459594)(TnL5HPStwNw-RfRFLElSGFCdyaiTXT53gg)()
OmeaReader	http://www.jetbrains.com/omea/reader

Pine	https://pine.blog
QuiteRSS	https://quiterss.org
Royal	http://www.the-sz.com/products/royal
RSS Bridge	https://github.com/RSS-Bridge/rss-bridge
RSS Feed Reader	https://chrome.google.com/webstore/detail/rss-feed-reader/pnjaodmkngahhkoihejjehlcdlnohgmp
RSS for the rest of us	https://github.com/wilderborn/rss-for-the-rest-of-us
RSSOwl	http://www.rssowl.org
Rufus	https://github.com/jtanza/rufus
Telescope	https://itunes.apple.com/us/app/telescope-news-rss-reader/id1353282977?mt=8
Selfoss	http://selfoss.aditu.de
The Old Reader	http://theoldreader.com
ViennaRSS	https://github.com/ViennaRSS/vienna-rss
Winds	https://getstream.io/winds

Other RSS Tools

Tool	Link
Bridge.Leslibres	https://bridge.leslibres.org
Bridge.Suumitsu	https://bridge.suumitsu.eu
Feed Filter Maker	http://feed.janicek.co
Fetch RSS	http://fetchrss.com
Google Alerts	http://www.google.com/alerts
Google-alerts 0.1.5	https://pypi.org/project/google-alerts
Kill the Newsletter	https://www.kill-the-newsletter.com
Pipes	https://www.pipes.digital
Reeder	http://reederapp.com
RSS Bridge	https://github.com/RSS-Bridge/rss-bridge
RSS Micro	http://www.rssmicro.com
RSS Search Hub	http://www.rsssearchhub.com
RSS Subscription Extension	https://chrome.google.com/webstore/detail/rss-subscription-extensio/bmjffnfcokiodbeiamclanljnaheeoke?hl=en
Sage	https://addons.mozilla.org/en-US/firefox/addon/sage/?src=search
siftrss	https://siftrss.com

Website Monitoring

Tool	Link
ChangeDetect	http://www.changedetect.com
ChangeTower	https://changetower.com
Custodee	https://www.custodee.com
deltafeed	http://bitreading.com/deltafeed
Distil Web Monitor	https://chrome.google.com/webstore/detail/distill-web-monitor/inlikjemeeknofckkjolnjbpehgadgge?hl=en-US
Feed43	http://feed43.com
FollowThatPage	http://www.followthatpage.com
OnWebChange	http://onwebchange.com
urlwatch	https://github.com/thp/urlwatch
versionista	http://versionista.com
visualping	https://visualping.io
WatchThatPage	http://www.watchthatpage.com
WebSite Watcher	http://www.aignes.com/index.htm

Social Media Monitoring

Tool	Link
altervista	http://fb2rss.altervista.org
Feed Exileed	http://feed.exileed.com
Mention	https://en.mention.com
Queryfeed	http://www.queryfeed.net
Talkwalker	http://www.talkwalker.com
TwiSSR	http://www.twissr.com

Other Monitoring Tools

Tool	Link
InfoMinder	http://www.infominder.com/webminder
Keendly	http://keendly.com

Data Collation

Bookmarking

Tool	Link
Bibsonomy	http://www.bibsonomy.org
BonzoBox	http://bonzobox.com
Bookmark OS	https://bookmarkos.com
Booky	http://booky.io
ChannelKit	http://channelkit.com
Clipix	https://www.clipix.com
Curabase	https://www.curabase.com
Diigo	https://www.diigo.com
Dragdis	https://dragdis.com
Evernote	http://evernote.com
Dropmark	http://www.dropmark.com
eLink	https://elink.io
Email This	https://www.emailthis.me
FAVable	http://www.favable.com
Google Bookmarks	https://www.google.com/bookmarks
Granary	https://granary.pro
Historious	https://historio.us
Instapaper	http://www.instapaper.com
Juxtapost	http://www.juxtapost.com
Klart	https://klart.co

Larder	https://larder.io
Liner for Pocket	http://getliner.com/liner-for-pocket
Link.fish	https://link.fish
Linkman Pro	http://www.outertech.com/en/bookmarks-favorites
Linkstash	http://www.xrayz.co.uk
LiveBinders	http://www.livebinders.com
Lumio	https://www.lumioapp.com
memomize	http://www.memomize.com
Memonic	http://www.memonic.com
Microsoft OneNote	http://office.microsoft.com/en-us/onenote
mochimarks	https://mochimarks.com
netrostation	https://www.netrostation.com
P2K	https://p2k.co
Papaly	https://papaly.com
Paperwork	https://github.com/twostairs/paperwork
Pinboard	https://pinboard.in
Pearltrees	http://www.pearltrees.com
Pocket	http://getpocket.com
Raindrop	https://raindrop.io
Readibility	http://www.readability.com
Refind	https://refind.com
Save to Google	https://chrome.google.com/webstore/detail/save-to-google/meoeeoaohbmgbocpdpnjklmfmjjagkkf?utm_source=chrome-app-launcher-info-dialog
Scoop.it	http://www.scoop.it
Scrapbook	https://addons.mozilla.org/en-US/firefox/addon/scrapbook
Scrible	http://www.scrible.com
Session Buddy	https://chrome.google.com/webstore/detail/session-buddy/edacconmaakjimmfgnblocblbcdcpbko?hl=en
Sitehoover	http://www.sitehoover.com
Spaaze	http://www.spaaze.com
Stache	http://getstache.com
syncmarx	https://syncmarx.mcleodgaming.com

Thinkery	http://thinkery.me
Trackplanet	https://trackpanel.net
Trello	https://trello.com
Turtl	https://turtlapp.com
Tusk	https://github.com/klauscfhq/tusk
unhoard	https://www.unhoard.io
vookmark	https://vookmark.co
wallabag	https://wallabag.org
Wepware	http://www.wepware.com
Wonderpage	http://www.wonderpage.com
WorldBrain	https://worldbrain.io
Zotero	http://www.zotero.org

Notetaking

Tool	Link
Agenda	https://itunes.apple.com/us/app/agenda-a-new-take-on-notes/id1287445660
Bear Writer	http://www.bear-writer.com
Cherrytree	http://www.giuspen.com/cherrytree
Evernote	https://www.evernote.com
Google Keep	https://keep.google.com
Google Keep for Desktop	http://keepfordesk.xyz
inkdrop	https://www.inkdrop.info
Joplin	http://joplin.cozic.net
Kl1p	http://kl1p.com
Laverna	https://laverna.cc
Listacular	http://www.bloomingsoft.com/listacular
Microsoft OneNote	https://www.onenote.com
Milanote	http://www.milanote.com
Mindful	https://chrome.google.com/webstore/detail/mindful-beta/cieekmjjdkckhpidgaffphlaljdfhhab
Notebook	https://www.zoho.com/notebook
Outliney	https://glamdevelopment.com/outlinely/ios
Pear Note	http://www.usefulfruit.com/pearnote
Scribble	http://scribble.wreally.com
Simplenote	http://simplenote.com
Slite	https://slite.com
somnote	http://somcloud.com/about/somnote
Squid	http://squidnotes.com

Standard Notes	https://standardnotes.org
Thinkery	https://thinkery.me
Tomboy	https://wiki.gnome.org/Apps/Tomboy
Turtl	https://turtlapp.com
Tusk	https://github.com/klauscfhq/tusk
TypeLink	https://typelink.net
Workflowy	https://workflowy.com
wridea	http://wridea.com
Zoho Notebook	https://www.zoho.com/notebook

Annotation and Highlighting

Tool	Link
A.nnotate	http://a.nnotate.com
Beanote	https://chrome.google.com/webstore/detail/beanote-note-taking-on-we/nikccehomlnjkmgmhnieecolhgdafajb
Bounce	https://www.bounceapp.com
Diigo	https://www.diigo.com
Easy Annotate	http://www.easy-annotate.com
Highly	https://www.highly.co
Hypothesis	https://hypothes.is
Liner	http://getliner.com
Note Anywhere	https://chrome.google.com/webstore/detail/note-anywhere/bohahkiiknkelflnjjlipnaeapefmjbh
Pund.it	http://thepund.it
Skitch	https://evernote.com/skitch
Sum It Up	http://rachitgulati.com/sum-it-up
Weava Highlighter	https://chrome.google.com/webstore/detail/weava-highlighter-pdf-web/cbnaodkpfinfiipjblikofhlhlcickei

Screenshot and Screen Capture Tools

Tool	Link
1Click Screenshot	https://chrome.google.com/webstore/detail/1click-screenshot/akgpcdalpfphjmfifkmfbpdmgdmeeaeo?hl=en
Ashampoo Snap 9	https://www.ashampoo.com/en/usd/pin/1724/multimedia-software/Ashampoo-Snap-9
Awesome Screenshot	https://www.awesomescreenshot.com
BrowseShot	https://itunes.apple.com/us/app/browseshot/id615916400?ls=1%20&%20mt=12
Captur	http://cambhlumbulunk.blogspot.com/p/captur.html
Cockos LICEcap	https://www.cockos.com/licecap
EyeWitness	https://github.com/ChrisTruncer/EyeWitness
FastStone	http://www.faststone.org/FSCaptureDetail.htm
FireShot	https://getfireshot.com
Fraps	http://www.fraps.com
Full Page Screen Capture	https://chrome.google.com/webstore/detail/full-page-screen-capture/fdpohaocaechififmbbbbbknoalclacl?hl=en-US
Full Page Screenshot	https://chrome.google.com/webstore/detail/full-page-screenshot/glgomjpomoahpeekneidkinhcfjnnhmb?hl=en
Full Web Page Screenshots	https://addons.mozilla.org/en-US/firefox/addon/fireshot
Greenshot	https://getgreenshot.org
Gyazo	https://gyazo.com
jetScreenshot	http://www.jetscreenshot.com
Jing	https://www.techsmith.com/jing-tool.html
lazyshot	https://github.com/mdhama/lazyshot
LightShot	https://app.prntscr.com
Monosnap	https://monosnap.com

Nimbus	http://nimbus.everhelper.me
Pages 2 Images	http://www.page2images.com
Paparazzi!	https://derailer.org/paparazzi
PickPick	http://ngwin.com/picpick
puush	https://puush.me
qSnap	https://chrome.google.com/webstore/detail/qsnap-screen-capture-scre/bijakfpegjnjmfdoiloebhaemhomjkon
Screengrab	https://addons.mozilla.org/en-US/firefox/addon/screengrab-fix-version/
Screen Master	https://play.google.com/store/apps/details?id=pro.capture.screenshot
Screenshot App	http://screenshotapp.com
Screenshot Captor	http://www.donationcoder.com/software/mouser/popular-apps/screenshot-captor
Screenshot Layer	https://screenshotlayer.com
Screenshot Machine	https://www.screenshotmachine.com
Screenshot Utility	http://screenshot-utility.com
ScreenToGif	http://www.screentogif.com
ShareX	https://getsharex.com
Shrink the Web	https://www.shrinktheweb.com
SiteShoter	http://www.nirsoft.net/utils/web_site_screenshot.html
Snaggy	https://snag.gy
Snagit	https://www.techsmith.com/screen-capture.html
Snapito	https://snapito.com
Snapper	https://github.com/dxa4481/Snapper
Snip&Paste	https://www.snipaste.com
Take Webpage Screenshots Entirerly	https://chrome.google.com/webstore/detail/take-webpage-screenshots/mcbpblocgmgfnpjjppndjkmgjaogfceg?hl=en-US
TinyTake	https://tinytake.com
URL2PNG	https://www.url2png.com
URL Box	https://urlbox.io
Web-Capture	https://web-capture.net
Web Page Saver	https://www.magnetforensics.com/free-tool-web-page-saver
webscreenshot	https://github.com/maaaaz/webscreenshot

Browsing and Browsers

Browsers

Tool	Link
Addap's	https://www.addaps.com
Alloy	http://alloy.simoncaminada.ch
Aloha Browser	https://alohabrowser.com
Basilisk	http://www.basilisk-browser.org
Brave	https://brave.com
CentBrowser	http://www.centbrowser.com
Chrome	https://www.google.com/chrome
Chromium	https://www.chromium.org
Cliqz	https://cliqz.com
Colibri	https://colibri.opqr.co
Comodo Dragon	https://www.comodo.com/home/browsers-toolbars/browser.php
Cocoon	https://getcocoon.com
Coowon	http://coowon.com
Dooble	https://textbrowser.github.io/dooble
Edge	https://www.microsoft.com/en-us/windows/microsoft-edge/microsoft-edge
Firefox	https://www.mozilla.org
Ghost Browser	https://ghostbrowser.com
Iridium	https://iridiumbrowser.de
Konqueror	https://konqueror.org
Links	http://links.twibright.com

Maxthon	http://www.maxthon.com
Midori	http://midori-browser.org
Min	https://minbrowser.github.io/min
Next	http://next-browser.com
Opera	http://www.opera.com
Opera Neon	http://www.opera.com/computer/neon
Pale Moon	https://www.palemoon.org
Qt Web	http://www.qtweb.net
QupZilla	https://www.qupzilla.com
Safari	http://www.apple.com/safari
SeaMonkey	https://www.seamonkey-project.org
Silo	https://www.authentic8.com/overview
Sleipnir	http://www.fenrir-inc.com/jp/sleipnir
SRWare Iron	http://www.srware.net/en/software_srware_iron.php
Torch	http://www.torchbrowser.com
UCBrowser	http://www.ucweb.com
Vivaldi	https://vivaldi.com
Yandex Browser	https://browser.yandex.com/desktop/main

Startpages

Tool	Link
allmyfaves	http://www.allmyfaves.com
ighome	http://www.ighome.com
iloggo	http://iloggo.com
Kadaza	http://www.kadaza.com
Myfav.es	http://myfav.es
My Yahoo	https://my.yahoo.com
Open OOX	https://openoox.com
Protopage	http://www.protopage.com
Start.io	http://start.io
Startme	http://www.startme.com
Symbaloo	http://www.symbaloo.com
uStart.org	http://www.ustart.org
Yourport	http://www.yourport.com
Zenstart	http://www.zenstart.com

Customising New Tab

Tool	Link
Blink	https://addons.mozilla.org/en-GB/firefox/addon/blink
Bookmark Dial	https://addons.mozilla.org/en-GB/firefox/addon/bookmark-dial
Chrome Customize Your New Tab Page	https://chrome.google.com/webstore/category/collection/customize_your_new_tab_page
Custom New Tabs	https://addons.mozilla.org/en-US/firefox/addon/custom-new-tabs
Live Start Page LST	https://addons.mozilla.org/en-US/firefox/addon/live-start-page-lst
Moment	https://addons.mozilla.org/en-US/firefox/addon/moment/?src=search
New MetroTab	https://addons.mozilla.org/en-US/firefox/addon/new-metrotab
New Tab Tools	https://addons.mozilla.org/en-US/firefox/addon/new-tab-tools
Rocket Dashboard	https://chrome.google.com/webstore/detail/rocket-dashboard/plcedaomjjdiihihamfhangiiknamifc?utm_source=website&utm_medium=splash&utm_campaign=temp-splash
SiteLauncher	https://addons.mozilla.org/en-GB/firefox/addon/sitelauncher
Speed Dial New Tab Page	https://addons.mozilla.org/en-US/firefox/addon/fvd-speed-dial
Speed Start	https://addons.mozilla.org/en-GB/firefox/addon/speed-start
Start.me	https://addons.mozilla.org/en-US/firefox/addon/startme
Super Start	https://addons.mozilla.org/en-GB/firefox/addon/super-start

ViewMarks	https://addons.mozilla.org/en-US/firefox/addon/viewmarks

Tab Management

Tool	Link
Bookmark Ninja	https://www.bookmarkninja.com
OneTab	https://chrome.google.com/webstore/detail/onetab/chphlpgkkbolifaimnlloiipkdnihall?hl=en
MySessions	https://addons.mozilla.org/en-US/firefox/addon/my-sessions
Quick Tab	https://chrome.google.com/webstore/detail/quick-tab/bdeifmcaonlafkglbdpbbhkeecjnkipo
Session Buddy	https://chrome.google.com/webstore/detail/session-buddy/edacconmaakjimmfgnblocblbcdcpbko?hl=en
Tabli	https://chrome.google.com/webstore/detail/tabli/igeehkedfibbnhbfponhjjplpkeomghi
TabCloud	https://chrome.google.com/webstore/detail/tabcloud/npecfdijgoblfcgagoijgmgejmcpnhof?hl=en
Tab Hibernation	https://chrome.google.com/webstore/detail/tab-hibernation/pbdpajcdgknpendpmecafmopknefafha?hl=en
TabJump	https://chrome.google.com/webstore/detail/tabjump-intelligent-tab-n/hokofmgcicpnjchllaccgedmmmbbnbmf?hl=en
Tab Manager	https://addons.mozilla.org/en-US/firefox/addon/tab-manager-webextension
Tab Manager	https://addons.mozilla.org/en-US/firefox/addon/tab_manager
Tabs Outliner	https://chrome.google.com/webstore/detail/tabs-outliner/eggkanocgddhmamlbiijnphhppkpkmkl
TabsPlus	https://chrome.google.com/webstore/detail/tabsplus/nikomkkhhpfoeamojhhgpfkpkdlfhfii?hl=en

Tab Session Manager	https://addons.mozilla.org/en-US/firefox/addon/tab-session-manager
Tab Wrangler	https://chrome.google.com/webstore/detail/tab-wrangler/egnjhciaieeiiohknchakcodbpgjnchh?hl=en
The Great Suspender	https://chrome.google.com/webstore/detail/the-great-suspender/klbibkeccnjlkjkiokjodocebajanakg
Toby	https://www.gettoby.com
TooManyTabs	https://chrome.google.com/webstore/detail/toomanytabs-for-chrome/amigcgbheognjmfkaieeeadojiibgbdp?hl=en

Extension Managers

Tool	Link
Addons Manager Hilite	https://addons.mozilla.org/en-US/firefox/addon/addons-manager-hilite/?src=search
Add-ons Manager Context Menu	https://addons.mozilla.org/en-US/firefox/addon/am-context
Custom Chrome	https://chrome.google.com/webstore/detail/custom-chrome-extension-m/balnpimdnhfiodmodckhkgneejophhhm
Extensions Manager (aka Switcher)	https://chrome.google.com/webstore/detail/extensions-manager-aka-sw/lpleipinonnoibneeejgjnoeekmbopbc?hl=en
Extension Manager Extended	https://addons.mozilla.org/en-US/firefox/addon/extension-manager-extended
Extensity	https://chrome.google.com/webstore/detail/extensity/jjmflmamgggndanpgfnpelongoepncg/reviews
My Extensions	https://chrome.google.com/webstore/detail/my-extensions/igejgfmbjjjjplnnlgnbejpkpdajkblm?hl=en
One Click Extensions Manager	https://chrome.google.com/webstore/detail/one-click-extensions-mana/pbgjpgbpljobkekbhnnmlikbbfhbhmem?hl=en
Simple Add-on Manager	https://addons.mozilla.org/en-US/firefox/addon/simple-add-on-manager

Offline Browsing

Tool	Link
A1 Website Download	http://www.microsystools.com/products/website-download
Cyotek WebCopy	http://www.cyotek.com/cyotek-webcopy
gmapcatcher	https://github.com/heldersepu/gmapcatcher
Hooey webprint	http://www.hooeeywebprint.com.s3-website-us-east-1.amazonaws.com/download.html
HTTrack	http://www.httrack.com
Offliberty	http://offliberty.com
Resolver	https://metaproductsrevolver.com
ScrapBook	https://addons.mozilla.org/en-US/firefox/addon/scrapbook
SiteSucker	http://ricks-apps.com/osx/sitesucker/index.html
WebAssistant	http://www.proxy-offline-browser.com/download.html
Website Ripper Copier	http://www.tensons.com/products/websiterippercopier

Browsing History

Tool	Link
Chrome History View	https://www.nirsoft.net/utils/chrome_history_view.html
Falcon	https://chrome.google.com/webstore/detail/falcon/mmifbbohghecjloeklpbinkjpbplfalb?hl=en
Fea KeyLogger	https://chrome.google.com/webstore/detail/fea-keylogger/fgkghpghjcbfcflhoklkcincndlpobja?hl=en
Fiddler	https://www.telerik.com/download/fiddler
History Search	https://historysearch.com
Hunchly	https://www.hunch.ly

Other Browsing Tools

Tool	Link
AutoPagerize	https://chrome.google.com/webstore/detail/autopagerize/igiofjhpmpihnifddepnpngfjhkfenbp
Block Facebook	https://sarimhaq.github.io/block-facebook-website
Downforeveryoneorjustme	http://downforeveryoneorjustme.com
Finitimus	https://chrome.google.com/webstore/detail/finitimus/ckdjcgaagfcnndkknfmncedapdjaokb?utm_source=chrome-ntp-icon
Google When	https://chrome.google.com/webstore/detail/google-when/dgafcidlgmbcehokgdeghmfnbpbfhihh
Panic Button	https://chrome.google.com/webstore/detail/panicbutton/faminaibgiklngmfpfbhmokfmnglamcm
Pawblock	https://www.pawblock.dannyguo.com
Referer Control	https://chrome.google.com/webstore/detail/referer-control/hnkcfpcejkafcihlgbojoidoihckciin?hl=en
SelfControl	http://selfcontrolapp.com
Simple Blocker	https://chrome.google.com/webstore/detail/simple-blocker/akfbkbiialncppkngofjpglbbobjoeoe
User-Agent Switcher for Chrome	https://chrome.google.com/webstore/detail/user-agent-switcher-for-c/djflhoibgkdhkhhcedjiklpkjnoahfmg

Writing and Dissemination

Writing and Office Tools

Tool	Link
Arguman	http://en.arguman.org
bibisco	http://www.bibisco.com
Bibme	http://www.bibme.org
Cite This For Me	https://chrome.google.com/webstore/detail/cite-this-for-me-web-cite/nnnmhgkokpalnmbeighfomegjfkklkle?hl=en
Citationsy	https://citationsy.com
Classeur.io	http://classeur.io
CustomWritings.com: Citation Generator	https://www.customwritings.com/citation_generator.html
FreeOffice	http://www.freeoffice.com
Grammarly	https://chrome.google.com/webstore/detail/grammarly-for-chrome/kbfnbcaeplbcioakkpcpgfkobkghlhen?hl=en
GoogleDocs	https://www.google.com/docs/about
Hemmingway Editor	http://hemingwayapp.com
KingSoft	http://www.kingsoftstore.com
LibreOffice	https://www.libreoffice.org
Manuskript	http://www.theologeek.ch/manuskript
MS Office	https://products.office.com
Office Online	https://chrome.google.com/webstore/detail/office-online/ndjpnladcallmjemlbaebfadecfhkepb/related
Ommwriter	https://ommwriter.com
OmniOutliner	https://www.omnigroup.com/omnioutliner
OnlyOffice	https://www.onlyoffice.com

oStoryBook	http://ostorybook.tuxfamily.org
oTranscribe	http://otranscribe.com
Plume Creator	http://plume-creator.eu
Scrivener	http://literatureandlatte.com/scrivener.php
StoryToolz	http://storytoolz.com
TextExpander	https://smilesoftware.com/textexpander
UltraEdit	http://www.ultraedit.com
Ulysses	https://ulyssesapp.com
wordnik	http://wordnik.com
WriteApp	https://writeapp.me
Write or Die	http://writeordie.com
Writer's Cafe	http://www.writerscafe.co.uk

Slideshow and Presentation Tools

Tool	Link
Canva	https://www.canva.com/create/presentations
Deckset	http://www.decksetapp.com
emaze	https://www.emaze.com
FlowVella	https://flowvella.com
genially	https://www.genial.ly
GoogleDocs	https://docs.google.com
Haiku Deck	https://www.haikudeck.com
Keynote	http://www.apple.com/de/mac/keynote
KingSoft	http://ksosoft.com/product/presentation-free.html
KnowledgeVision	http://www.knowledgevision.com
LibreOffice	https://www.libreoffice.org
Live Slides	https://www.liveslides.com
Mighty Meeting	http://www.mightymeeting.com
MS Office	https://products.office.com
Paste	https://fiftythree.com/paste
Piktochart	https://piktochart.com
Pitch Deck	https://pitchdeck.io
Powtoon	https://www.powtoon.com
presenterswall	http://www.presenterswall.com
Prezent 3D	https://www.prezent3d.com
Prezi	https://prezi.com
Slidebean	https://slidebean.com
Slidedog	http://slidedog.com
SlidePresenter	http://www.slidepresenter.com

SlideRocket	https://www.clearslide.com/product/sliderocket
Slides	https://slides.com
SpeechInMinutes	http://www.speechinminutes.com/
Sway	https://sway.com
WebSlides	https://webslides.tv
vcasmo	http://www.vcasmo.com
Visme	http://www.visme.co
Zoho Docs	https://www.zoho.com/docs/show.html

Digital Publishing

Tool	Link
Canva	https://www.canva.com
Doclayer	https://standaert.net/doclayer
Issuu	https://issuu.com
Lucidpress	https://www.lucidpress.com
Mag.io	http://mag.io
My eBook	http://www.myebook.com
Omeka	http://omeka.org
Scribd	https://www.scribd.com
Yudu	http://yudu.com

Newsletter Tools

Tool	Link
AWeber	http://www.aweber.com
BombBomb	http://bombbomb.com
Campayn	http://campayn.com
Canva	https://www.canva.com
ConstantContact	http://www.constantcontact.com
Freshmail	http://freshmail.com
GetResponse	http://www.getresponse.com
iContact	https://www.icontact.com
MadMimi	https://madmimi.com
Mailchimp	http://mailchimp.com
Mailjet	https://www.mailjet.com
Mailup	http://www.mailup.com
Newsletter Creator for Gmail	https://chrome.google.com/webstore/detail/newsletter-creator-for-gm/cihaednhfbocfdiflmpccekcmjepcnmb
sendinblue	https://www.sendinblue.com
Sendicate	https://www.sendicate.net
Sendloop	https://sendloop.com
Signupto	https://www.signupto.com
TinyLetter	http://tinyletter.com
VerticalResponse	http://www.verticalresponse.com
Vision6	http://www.vision6.com.au

Digital Storytelling

Tool	Link
Adobe Spark	https://spark.adobe.com/
Animatron	https://www.animatron.com
Animoto	https://animoto.com
Atavist	https://atavist.com
Closr	https://www.closr.it
Eko Studio	https://studio.helloeko.com
Juxtapose	https://juxtapose.knightlab.com
Klynt	http://www.klynt.net
MakeBeliefsComix	http://www.makebeliefscomix.com
Metta	http://www.metta.io
Neatline	http://neatline.org
Odyssey	https://cartodb.github.io/odyssey.js
Pageflow	http://pageflow.io
Photodex	http://www.photodex.com
Piclits	http://www.piclits.com/compose_dragdrop.aspx
Racontr	https://racontr.com
RaptMedia	http://www.raptmedia.com
RawShorts	http://www.rawshorts.com
Shorthand Social	https://shorthand.com/social
Soundcite	http://soundcite.knightlab.com
sStory	https://ejfox.github.io/sStory
Steller	https://steller.co
Storify	https://storify.com
Storyboard	http://generator.acmi.net.au/storyboard

Storyform	https://storyform.co
StoryMap	https://storymap.knightlab.com
StoryMaps	http://storymaps.arcgis.com
Sway	https://sway.com
Thinglink	https://www.thinglink.com
Timeline	http://timeline.knightlab.com
Tripline	http://www.tripline.net
Visual Investigative Scenarios	https://vis.occrp.org
Wevideo	https://www.wevideo.com
VideoScribe	http://www.videoscribe.co

Wikis, Websites, and Web Apps

Wikis

Tool	Link
DokuWiki	https://www.dokuwiki.org/dokuwiki
Foswiki	http://foswiki.org
Matterwiki	http://matterwiki.com
MediaWiki	https://www.mediawiki.org/wiki/MediaWiki
Nuclino	https://www.nuclino.com
PmWiki	http://www.pmwiki.org
Scribbleton	http://scribbleton.com
TiddlyWiki	http://tiddlywiki.com
Tiki Wiki	https://info.tiki.org
Torchpad	https://torchpad.com
TWiki	http://twiki.org
Wikia	http://www.wikia.com/Wikia
Wikidot	http://www.wikidot.com
Wikispaces	http://www.wikispaces.com
wikidPad	http://wikidpad.sourceforge.net
Zim	http://zim-wiki.org/downloads.html

Website Builders

Tool	Link
Boldgrid	https://www.boldgrid.com
Duda	https://www.duda.co
eHost	https://www.ehost.com
GoDaddy	https://ca.godaddy.com/websites/website-builder
Google Sites	https://gsuite.google.com/products/sites
IM Creator	http://www.imcreator.com
jimdo	https://www.jimdo.com
LonelyPage	http://www.lonelypage.io
Publishthis.email	https://www.publishthis.email
Sheet2site	https://www.sheet2site.com
Simvoly	https://simvoly.com
Site Builder	https://www.sitebuilder.com
Sitey	https://www.sitey.com
Squarespace	https://www.squarespace.com
Strikingly	https://www.strikingly.com
UCoz	https://www.ucoz.com
UCraft	https://www.ucraft.com
Ukit	https://ukit.com
Voog	https://www.voog.com
Web.com	https://www.web.com
Webnode	https://us.webnode.com
Website Builder	https://www.websitebuilder.com
Webstarts	https://www.webstarts.com
Weebly	https://www.weebly.com

Wix	https://www.wix.com
Wordpress	https://wordpress.com
yola	https://www.yola.com
Zoho	https://www.zoho.com/sites/website-builder.html

App Builders

Tool	Link
Appery.io	https://appery.io
AppsBar	http://www.appsbar.com
AppsBuilder	http://www.apps-builder.com
Apps Geyser	https://www.appsgeyser.com
App Machine	http://www.appmachine.com
AppMakr	http://www.appmakr.com
Appy Pie	https://www.appypie.com
bubble	https://bubble.is
Build Fire	https://buildfire.com
Bizness Apps	https://www.biznessapps.com
ChupaMobile	https://www.chupamobile.com
Game Salad	https://gamesalad.com
Good Barber	https://www.goodbarber.com/native
iBuild App	https://ibuildapp.com
Kony	https://www.kony.com/products/appplatform#download?utm_medium=tpp&utm_source=businessofapps&utm_campaign=19q1-pf-business-of-apps&utm_content=notapp&utm_term=notapp&utm_adgroup=notapp&kash=notapp
Mobile Roadie	https://mobileroadie.com
Shoutem	http://www.shoutem.com
The App Builder	https://www.theappbuilder.com

Mind Mapping, Concept Mapping and Idea Generation

Mind Mapping, Concept Mapping and Idea Generation Tools

Tool	Link
The Brain	http://www.thebrain.com
Bubbl.us	https://bubbl.us
Cmap	https://cmap.ihmc.us
Comapping	http://www.comapping.com
ConceptDraw	http://www.conceptdraw.com
Coogle	https://coggle.it
DebateGraph	https://debategraph.org
Fast Idea Generator	http://diytoolkit.org/tools/fast-idea-generator-2
Freemind	http://freemind.sourceforge.net/wiki/index.php/Main_Page
Freeplane	http://freeplane.sourceforge.net/wiki/index.php/Main_Page
Germ	https://germ.io
GroupMap	http://www.groupmap.com
Ideaphora	http://www.ideaphora.com
iMindMap	https://imindmap.com
iMindQ	https://www.imindq.com
Lucidchart	https://www.lucidchart.com
Mattermap	https://www.mattermap.nl
Mind42	http://mind42.com
Mind Genius	http://www.mindgenius.com
Mindjet	https://www.mindjet.com

Mind Map	https://chrome.google.com/webstore/detail/mindmap/gdaeohpmcenmffofpikllphdhlkkocfa#detail/mindmap/gdaeohpmcenmffofpikllphdhlkkocfa
Mind Mup	https://www.mindmup.com
Mindmeister	https://www.mindmeister.com
Mindomo	https://www.mindomo.com
Org-brain	https://github.com/Kungsgeten/org-brain
Popplet	http://popplet.com
Realtimeboard	https://realtimeboard.com
Scapple	http://literatureandlatte.com/scapple.php
Simple Mind	https://simplemind.eu
Sketchboard	http://sketchboard.io
Slatebox	https://slatebox.com
Spiderscribe	http://www.spiderscribe.net
Stormboard	https://stormboard.com
Text2MindMap	https://tobloef.com/text2mindmap
VUE	http://vue.tufts.edu
Wise Maping	http://www.wisemapping.com
yWorks	http://www.yworks.com/en/products_yed_gallery.html
Xmind	http://www.xmind.net

Productivity and File Management

Main Work Management and Productivity Tools

Tool	Link
2Do	http://www.2doapp.com
Any.do	http://www.any.do
Asana	https://asana.com
Boomerang App	http://www.boomerangapp.com
Dapulse	https://dapulse.com
Dayboard	https://dayboard.co
Droptask	https://www.droptask.com
Flask	http://flask.io
Focus booster	https://www.focusboosterapp.com
Freecamp	https://freedcamp.com
Leechblock	https://addons.mozilla.org/en-US/firefox/addon/leechblock
minimalist	http://www.getminimalist.com
MorningRoutine	http://www.ubicolor.com/morningroutine.html
MyLifeOrganized	http://www.mylifeorganized.net
Noteplan	https://noteplan.co
Pintask	https://pintask.me
PomodoroTechnique	http://pomodorotechnique.com
Producteev	https://www.producteev.com
Quire	https://quire.io
Remember the Milk	https://www.rememberthemilk.com
RescueTime	https://www.rescuetime.com
Restya	http://restya.com

StayFocusd	https://chrome.google.com/webstore/detail/stayfocusd/laankejkbhbdhmipfmgcngdelahlfoji/details
Taskboard	https://taskboard.matthewross.me
TikiTiki	https://ticktick.com
Tinygain	https://tinygain.com
Trello	https://trello.com
Todo.ly	https://todo.ly
Todo	http://todotxt.com
Todoist	https://en.todoist.com
Toggl	https://www.toggl.com
Tomighty	http://www.tomighty.org
Toodledo	https://www.toodledo.com
Workflowy	https://workflowy.com
Wunderlist	https://www.wunderlist.com

Calendars and Scheduling

Tool	Link
Assistant	http://www.assistant.to
Bunchapp	http://bunchapp.io
Calendly	https://calendly.com
Cozi	http://www.cozi.com
Doodle	http://doodle.com
Foogi	http://www.foogi.me
Fruux	https://fruux.com
Meekan	https://meekan.com
Meetin.gs	http://www.meetin.gs
MyMemorizer	http://www.mymemorizer.com
Noteplan	https://noteplan.co
ScheduleOnce	http://www.scheduleonce.com
TeamUp	http://www.teamup.com
Teamweek	https://teamweek.com

E-mail Management

Tool	Link
ActiveInbox	http://www.activeinboxhq.com
Batched Inbox	https://www.batchedinbox.com
Baydin	https://www.baydin.com
BetterGmail	https://addons.mozilla.org/en-US/firefox/addon/better-gmail-2/
Block Sender	https://chrome.google.com/webstore/detail/block-sender/bklnjbfcmglhiaoppcckdodanccbelcg
Boomerang Mail	http://www.boomeranggmail.com
ClearContext	http://www.clearcontext.com
Cleanfox	https://www.cleanfox.io
Complete	https://complete.li
FindBigMail	https://www.findbigmail.com
Followupthen	https://www.followupthen.com
gpum	https://addons.mozilla.org/en-US/firefox/addon/gpum
Hiver	http://hiverhq.com
Integrated gmail	https://addons.mozilla.org/en-US/firefox/addon/integrated-gmail
Mailstore	http://www.mailstore.com
Hubspotsales	https://chrome.google.com/webstore/detail/hubspot-sales/oiiaigjnkhngdbnoookogelabohpglmd?hl=en
Minimalist	https://chrome.google.com/webstore/detail/minimalist-for-everything/bmihblnpomgpjkfddepdpdafhhepdbek
NudgeMail	https://www.nudgemail.com
Rapportive	https://rapportive.com
Sanebox	https://www.sanebox.com
Send for Gmail	https://chrome.google.com/webstore/detail/send-from-gmail-by-google/pgphcomnlaojlmmcjmiddhdapjpbgeoc

Sortd	http://www.sortd.com
TrueNew	https://chrome.google.com/webstore/detail/truenewtm-count-for-gmail/lhgbgmbdabgjdephnmkpmcdkmnpiahlb
Ugly Email	https://uglyemail.com
Unroll.me	https://unroll.me
WiseStamp	https://chrome.google.com/webstore/detail/wisestamp-email-signature/pbcgnkmbeodkmiijjfnliicelkjfcldg

Cloud Storage and File Sharing

Tool	Link
4Shared	http://www.4shared.com
ADrive	http://www.adrive.com
Amazon Cloud drive	https://www.amazon.com/clouddrive/home
Box	https://www.box.com
Boxcryptor	https://www.boxcryptor.com
Cloudapp	http://www.getcloudapp.com
CloudFuze	https://www.cloudfuze.com
CloudHQ	https://www.cloudhq.net
docuvo	https://www.docuvo.com
Dropbox	https://www.dropbox.com
Dropcanvas	http://dropcanvas.com
droplr	https://droplr.com
DropSend	http://www.dropsend.com
Duplicati	http://www.duplicati.com
Egnyte	http://www.egnyte.com
EnCrypted Cloud	https://www.encryptedcloud.com
Ge.TT	http://ge.tt
GoodSync	http://www.goodsync.com
Google Drive	https://www.google.com/intl/nl/drive
Hightail	https://www.hightail.com
hubiC	https://hubic.com
iCloud	https://www.icloud.com
Mediafire	https://www.mediafire.com
Mega	https://mega.nz

Mindbox	https://minbox.com
Mozy	http://mozy.com
Multicloud	https://www.multcloud.com
Onedrive	https://onedrive.live.com
Onehub	https://www.onehub.com
Otixo	http://www.otixo.com
pCloud	https://www.pcloud.com
Sendthisfile	https://www.sendthisfile.com
Sendspace	https://www.sendspace.com
Simple.Savr	https://www.ssavr.com
Spideroak	https://spideroak.com
SugarSync	https://www.sugarsync.com
Syncthing	https://syncthing.net
TransferBigFiles	https://www.transferbigfiles.com
Tresorit	https://tresorit.com
WeTransfer	https://www.wetransfer.com

Web Automation

Tool	Link
Apiant	https://apiant.com
Cloud Work	https://cloudwork.com
IFTTT	https://ifttt.com
Microsoft Flow	https://flow.microsoft.com
Stringify	https://www.stringify.com
Trigger Happy	https://trigger-happy.eu
WeWiredWeb	https://wewiredweb.com
Workflow	https://workflow.is
Zapier	https://zapier.com

Collaboration and Communication

Collaboration and Project Management

Tool	Link
10kinsights	https://www.10000ft.com
92fiveApp	http://92fiveapp.com
5pm	http://www.5pmweb.com
ActionMint	https://www.actionmint.com
ActiveCollab	https://www.activecollab.com
Advanseez	http://www.advanseez.com
Agilewords	http://www.agilewords.com
Airtable	https://airtable.com
AllThings	http://www.allthings.io
Any.do	http://www.any.do
Apollo	http://www.apollohq.com
Asana	https://asana.com
Authorea	https://www.authorea.com
AWW	https://awwapp.com
Azendoo	https://www.azendoo.com
Basecamp	https://basecamp.com
Binfire	https://www.binfire.com
Box	https://www.box.com
Breeze	https://www.breeze.pm
Canvanizer	https://canvanizer.com
Casual	https://casual.pm

Cardboardit	https://cardboardit.com
Cardsmith	http://cardsmith.co
CloudApp	http://www.getcloudapp.com
Collabtive	http://collabtive.o-dyn.de
CollaborateCloud	http://www.collaboratecloud.com
Comindwork	http://www.comindwork.com
Conceptboard	https://conceptboard.com
Confluence	https://www.atlassian.com/software/confluence
CoSketch	http://cosketch.com
Crowdbase	http://crowdbase.com
Deekit	https://www.deekit.com
Draw.to	http://draw.to
eGroupWare	http://www.egroupware.org
Elegantt	https://elegantt.com
Encrypted Cloud	https://www.encryptedcloud.com
Firepad	https://firepad.io
Firesub	https://firesub.com
Flask	http://flask.io
Float	https://www.float.com
Flowdock	https://www.flowdock.com
Flockdraw	http://flockdraw.com
Flow	https://www.getflow.com
Frame	https://frame.io
Freedcamp	https://freedcamp.com
Glasscubes	https://www.glasscubes.com
GQueues	https://www.gqueues.com
Hightail	https://www.hightail.com
hitask	https://hitask.com
Huddle	https://www.huddle.com
Idea Flip	https://ideaflip.com
Infolio	https://infolio.co
KabanTool	http://kanbantool.com
Kanboard	https://kanboard.net

Kerika	http://kerika.com
Loomio	https://www.loomio.org
LumoFlow	https://lumoflow.com
Nozbe	https://nozbe.com
Nutcache	http://www.nutcache.com
meistertask	https://www.meistertask.com
Minute	https://www.getminute.com
Monday	https://monday.com
Mural	https://mural.co
MyKanzen	https://mykanzen.com
OmniGroup	https://www.omnigroup.com
OnlyOffice	https://www.onlyoffice.com
Padlet	https://padlet.com
Piematrix	http://www.piematrix.com
Pinstriped	http://pinstriped.com
PivotalTracker	http://www.pivotaltracker.com
Plan	https://plan.io
Planleaf	http://www.planleaf.com
Planzone	https://www.planzone.com
Podio	https://podio.com
PrimaryPad	http://primarypad.com
ProjectManager	https://www.projectmanager.com
ProjectPlace	https://www.projectplace.com
ProofHub	https://www.proofhub.com
Quip	https://quip.com
Quire	https://quire.io
Realtimeboard	https://realtimeboard.com
Redbooth	https://redbooth.com
Reverb	http://reverbapp.com
ScadaPlan	http://scadaplan.com
SeavusProjectViewer	https://www.seavusprojectviewer.com
Smartsheet	https://www.smartsheet.com
Stackfield	https://www.stackfield.com

Stormboard	https://www.stormboard.com
SyncSpace	http://infinitekind.com/syncspace
Taiga	https://taiga.io
Taskboard	https://taskboard.matthewross.me
táve	https://tave.com
TeamAllocator	http://www.teamallocator.com
Team.fm	https://team.fm
Team Pad	https://www.team-pad.com
TeamWork	https://www.teamwork.com
TeamWorklive	http://www.teamworklive.com
Transparent Business	http://transparentbusiness.com
Trello	https://trello.com
Tuzzit	https://www.tuzzit.com
Twiddla	http://www.twiddla.com
Twoodo	https://www.twoodo.com
updatey	http://updatey.com
Web Whiteboard	http://webwhiteboard.com
Weekdone	https://weekdone.com
wePaste	http://www.wepaste.com
Whiteboard	http://whiteboard.drewwilson.com
Whiteboard Fox	https://whiteboardfox.com
Workfront	https://www.workfront.com
Wrike	https://www.wrike.com
Yammer	https://www.yammer.com
YouTrack	https://www.jetbrains.com/youtrack
Zoho	https://www.zoho.com

Communication Tools

Tool	Link
Adobe Connect	http://www.adobe.com/products/adobeconnect.html
AnyDesk	http://anydesk.com/remote-desktop
AnyMeeting	https://www.anymeeting.com
Auralink	http://auralink.com
Babblebay	http://www.babblebay.com
BeamYourScreen	http://www.beamyourscreen.com
Blackboard	http://www.blackboard.com/online-collaborative-learning/index.aspx
blind	https://us.teamblind.com
Briar	https://briarproject.org
Cisco Spark	https://notes.ciscospark.com
clearvale	https://www.clearvale.com/marketing/en
Digital Samba	http://www.digitalsamba.com
Discourse	http://www.discourse.org
eBLVD	https://www.eblvd.com
Ekiga	http://ekiga.org
FaceFlow	http://www.faceflow.com
Fleep	https://fleep.io
FreeConferenceCall	https://www.freeconferencecall.com
FreeScreenSharing	https://www.freescreensharing.com
Friends	http://moose-team.github.io/friends
Glance	http://ww2.glance.net
GoToMeeting	http://www.gotomeeting.com
Highfive	https://highfive.com

icq	https://icq.com
iLinc	http://www.ilinc.com
Infinite	http://www.infiniteconferencing.com
Intercall	http://www.intercall.com
Jitsi	https://jitsi.org
Join.me	https://www.join.me
Jostle	http://www.jostle.me
KIK	https://www.kik.com
Let's Chat	http://sdelements.github.io/lets-chat
lifesize	http://www.lifesize.com
Line	https://line.me
Linphone	http://www.linphone.org
Live Conference Pro	http://www.liveconferencepro.com
Lucid Meetings	http://www.lucidmeetings.com
Meet Franz	https://meetfranz.com
MeetingOne	https://www.meetingone.com
MeetNotes	https://meetnotes.co
MeWe	https://mewe.com
mikogo	https://www.mikogo.com
mobilimeet	http://mobilimeet.com
MyBB	http://www.mybb.com
PGi iMeet	http://www.pgi.com/imeet
Phorum	http://www.phorum.org
Quicktopic	http://www.quicktopic.com
ReadyTalk	https://www.readytalk.com
RingCentral	http://www.ringcentral.com
Rocket.Chat	https://rocket.chat
screenleap	http://www.screenleap.com
sifonr	http://www.sifonr.com/
Signal	https://signal.org
Skype	http://www.skype.com
Slack	https://slack.com
StartMeeting	https://www.startmeeting.com

Stride	https://www.stride.com
Talky	https://talky.io
Teamviewer	https://www.teamviewer.com
Telegram	https://telegram.org
Tibbr	http://www.tibbr.com
Tixeo	https://www.tixeo.com/en/secure-video-conferencing
Toc	http://toc.im
TrueConf	http://trueconf.com
Twchat	http://twchat.com
Vanilla Forums	http://vanillaforums.org
Veeting rooms	https://www.veeting.com
VeriShow	http://www.verishow.com
Viadesk	http://www.viadesk.com
VideoLink2	https://videolink2.me
Webex	http://www.webex.com
Webinato	http://www.webinato.com
WeChat	https://web.wechat.com
WhatsApp	https://www.whatsapp.com
Zeetings	http://www.zeetings.com
Zoho Meeting	https://www.zoho.com/meeting
Zoom.us	https://zoom.us
Zulip	https://www.zulip.org

Other Utility Tools

File Converters

Tool	Link
Adapter	https://macroplant.com/adapter
Any Video Converter	http://www.any-video-converter.com/products/for_video_free
Apowersoft	https://www.apowersoft.com/free-online-video-converter
Avidemux	http://avidemux.sourceforge.net
Batch Photo	https://www.batchphoto.com/espresso
cloudconvert	https://cloudconvert.com
Clip Convert	https://clipchamp.com/en/video-converter
Cometdocs	https://www.cometdocs.com
Convert Files	http://www.convertfiles.com
Convert Video Online	https://convert-video-online.com
CoolUtils	https://www.coolutils.com/online/Image-Converter
Covertion	https://convertio.co
DVD Video Soft	https://www.dvdvideosoft.com/products/dvd/Free-Image-Convert-and-Resize.htm
Fileshifter	https://fileshifter.io
File Zig Zag	https://www.filezigzag.com
Free File Convert	https://www.freefileconvert.com
Free Make	http://www.freemake.com/free_video_converter
NCH Software	https://www.nchsoftware.com/software/converters.html
Online-Convert	https://www.online-convert.com

PDF Converter	https://www.freepdfconvert.com
PDF Converter	https://smallpdf.com/pdf-converter
PDF Forge	http://www.pdfforge.org/pdfcreator
PIX Converter	https://www.coffeecup.com/pixconverter
Publisher to PDF	https://www.publishertopdf.com
RoboBraille	https://www.robobraille.org
XnConvert	https://www.xnview.com/en/xnconvert
Zamzar	https://www.zamzar.com

URL Shorteners and Expanders

Tool	Link
Bit.do	https://bit.do
bitly	https://bitly.com
CheckShortURL	http://checkshorturl.com
GetLinkInfo	http://www.getlinkinfo.com
unFurlr	https://unfurlr.com
Unshorten	https://unshorten.it
Unshorten.link	https://chrome.google.com/webstore/detail/unshortenlink/gbobdaaeaihkghbokihkofcbndhmbdpd?hl=en
urlex	http://urlex.org
Where Does This Link Go?	http://wheredoesthislinkgo.com

Keywords Discovery and Research

Tool	Link
Google Adwords	http://adwords.google.com
Google Keyword Suggest Tool	http://tools.seochat.com/tools/suggest-tool
Google Trends	https://www.google.com/trends
Keyword Discovery	http://www.keyworddiscovery.com
Keyword Spy	http://www.keywordspy.com
KeywordTool	http://keywordtool.io
One Look Reverse Dictionary	http://www.onelook.com/reverse-dictionary.shtml
Word Tracker	https://www.wordtracker.com
Soovle	http://www.soovle.com
Ubersuggest	http://ubersuggest.org

Android Emulators

Tool	Link
Andyroid	https://www.andyroid.net
BlueStacks	https://www.bluestacks.com
GenyMotion	https://www.genymotion.com
Leapdroid	https://leapdroid.en.softonic.com
NoxPlayer	https://www.bignox.com

Virtual Machine

Tool	Link
Buscador Investiagtive Operating System	https://inteltechniques.com/buscador
Linux KVM	https://www.linux-kvm.org/page/Main_Page
Microsoft VMS	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms
Parallels	https://www.parallels.com
QEMU	https://www.qemu.org
Veertu	https://veertu.com
VirtualBox	https://www.virtualbox.org/wiki/Downloads
VMWare	https://www.vmware.com
VMWare ESXi	https://www.vmware.com/products/esxi-and-esx.html
Windows Hyper-V	https://www.microsoft.com/en-us/cloud-platform/server-virtualization
Windows Virtual PC	https://www.microsoft.com/en-us/download/details.aspx?id=3702
Xenserver	https://xenserver.org

Date & Time

Tool	Link
Coder's Tool Box	https://coderstoolbox.net/unixtimestamp
Earth Date to Martian Solar Longtitude	http://www-mars.lmd.jussieu.fr/mars/time/martian_time.html
EpochConverter	https://www.epochconverter.com
Epoch Timestamp Converter	https://www.unixtimestamp.com/index.php
Every Time Zone	http://everytimezone.com
ExcelJet	https://exceljet.net/formula/convert-time-to-time-zone
NASA's HEASARC Tools	https://heasarc.gsfc.nasa.gov/cgi-bin/Tools/xTime/xTime.pl
Online Conversion	http://www.onlineconversion.com/unix_time.htm
Sonnenverlauf	https://www.sonnenverlauf.de
SunCalc	http://suncalc.net
Sun or Moon Rise (US)	http://aa.usno.navy.mil/data/docs/RS_OneYear.php
timeanddate	https://www.timeanddate.de
Timeanddate	https://www.timeanddate.com/worldclock/converter.html
Time Now	http://www.thetimenow.com
TimeStampConvert	http://www.timestampconvert.com
Time Temperature	https://www.timetemperature.com/time-tools-advanced/time-converter-future-date.php
Time Zone Converter	http://www.timezoneconverter.com/cgi-bin/tzc.tzc
Time Zone Converter	http://www.thetimezoneconverter.com
World Time Buddy	https://www.worldtimebuddy.com
World Time Server	https://www.worldtimeserver.com
WolpframAlpha	http://www.wolframalpha.com

Weather

Tool	Link
AccuWeather Global	https://www.accuweather.com/en/world-weather
Aviation Weather Center	https://www.aviationweather.gov
BBC Weather	https://www.bbc.com/weather
Earth	https://earth.nullschool.net
Global Sailing Weather	http://www.globalsailingweather.com
GreatWeather	http://www.greatweather.co.uk
Intellicast	http://www.intellicast.com
MeteoFrance	http://www.meteofrance.com
MetEye	http://www.bom.gov.au/australia/meteye
Mike's Weather Page	http://spaghettimodels.com
NOOA Weather	http://www.noaa.gov/weather
Open Weather Map	https://openweathermap.org
UK Weather Cams	http://www.ukweathercams.co.uk
Ventusky	https://www.ventusky.com
weatherbase	http://www.weatherbase.com
Weather Underground	https://www.wunderground.com
Weather And Climate	https://weather-and-climate.com
Weather.com	https://weather.com
Weather.gov	https://www.weather.gov
weather.org	http://weather.org
Weatherzone.com	http://www.weatherzone.com.au/world
Wetter.com	https://www.wetter.com
Windy.com	https://www.windy.com/?39.538,-76.352,5
wisuki	http://wisuki.com

World Weather	http://worldweather.wmo.int/en/home.html
World Weather and Climate Extremes Archive	https://wmo.asu.edu
World Weather Online	https://www.worldweatheronline.com/lang/en-us
wunderground	https://www.wunderground.com

Barcodes

Tool	Link
Barcode Link	http://www.barcodelink.net
Barcode Reader	https://online-barcode-reader.inliteresearch.com
Barcode Scanner	https://play.google.com/store/apps/details ?id=com.google.zxing.client.android&hl=en_US
CodeReader	https://www.codereadr.com/
IB Scanner	http://www.ibscanner.com/online-barcode-scanner
Online Barcode Reader	https://www.onlinebarcodereader.com
Online Barcode Reader	https://online-barcode-reader.com
QR and Barcode Reader	https://play.google.com/store/apps/details ?id=com.teacapps.barcodescanner&hl=en_US
QR Code Reader and Scanner	https://itunes.apple.com/us/app/ qr-code-reader-and-scanner/id388175979?mt=8
QR Code Scanner	https://webqr.com
Scandit	https://www.scandit.com
ScanMe	https://www.scan.me
Scan – QR Code, Barcode Reaser	https://itunes.apple.com/us/app/ scan-qr-code-barcode-reader/id411206394?mt=8

Analysis

Social Network Analysis

Tool	Link
Gephi	https://gephi.org
Graph Commons	https://graphcommons.com
IBM Analyst Notebook	https://www.ibm.com/us-en/marketplace/analysts-notebook
ORA	http://www.casos.cs.cmu.edu/projects/ora/software.php
Sentinel Visualizer	http://www.fmsasg.com
SocioViz	http://socioviz.net
Visual Investigative Scenarios	https://vis.occrp.org

Geospatial OSINT

Geospatial Research and Mapping Tools

Tool	Link
ACT Map	http://www.actmapi.act.gov.au
AIRBUS WorldDEM	http://www.intelligence-airbusds.com/worlddem-sampledata
ALOS	http://www.eorc.jaxa.jp/ALOS/en/aw3d30
Animaps	http://www.animaps.com
a.placebetween.us	http://a.placebetween.us
aprs	https://aprs.fi
ArcGIS Online	https://www.arcgis.com
Atlasify	http://www.atlasify.com
Baidu Maps	http://map.baidu.com
Batchgeo	http://batchgeo.com
Batch Geocoding	https://www.doogal.co.uk/BatchGeocoding.php
Batch Reverse Geocoding	https://www.doogal.co.uk/BatchReverseGeocoding.php
Bing Maps	http://www.bing.com/maps
Bing Maps Aerial in Google Earth	http://ge-map-overlays.appspot.com/bing-maps/aerial
Bonding Box Drawing Tool	http://automatingosint.com/blog/geographic-bounding-box-drawing-tool
Carto	https://carto.com
Colorbrewer	http://colorbrewer2.org
Convert Latitude/Longitude to Decimal	https://andrew.hedges.name/experiments/convert_lat_long

Coordinate Conversion	http://www.synnatschke.de/geo-tools/coordinate-converter.php
Corona @ CAST	http://corona.cast.uark.edu
CrimeMapping	https://www.crimemapping.com
CrimeReports	https://www.crimereports.com
CrowdMap	https://crowdmap.com
CTLRQ Address Lookup	https://ctrlq.org/maps/address
Custom Satellite View Tools	https://inteltechniques.com/osint/menu.maps.html
Daum Maps	http://map.daum.net
DIgitalGlobe	http://www.digitalglobe.com || https://discover.digitalglobe.com
DigitalGlobe ImageFinder	https://browse.digitalglobe.com/imagefinder
Diva-GIS	http://www.diva-gis.org
Dominoc925	https://dominoc925-pages.appspot.com/mapplets/cs_mgrs.html
doogal	https://www.doogal.co.uk
dronestagram	http://www.dronestagr.am
DualMaps	http://data.mashedworld.com/dualmaps/map.htm
Earth Data	https://search.earthdata.nasa.gov/search
EarthExplorer	https://earthexplorer.usgs.gov
EarthPoint Convert	http://www.earthpoint.us/Convert.aspx
Earth Resources Observation and Science Center - USCG	https://eros.usgs.gov/find-data
Echosec	https://www.echosec.net
EOLI	https://earth.esa.int/web/guest/eoli
esri	http://www.esri.com
Esri Search	https://esri-es.github.io/arcgis-search
Europe Livemap	http://europe.liveuamap.com
Facebook Live Map	https://www.facebook.com/live
Fallingrain	http://www.fallingrain.com/world/index.html
Follow Your World	https://followyourworld.appspot.com
FreeMap Tools	https://www.freemaptools.com/radius-around-point.htm
Geobytes	http://geobytes.com/FreeServices

GeoHack	https://tools.wmflabs.org/geohack/geohack.php
GeoFabrik	http://www.geofabrik.de
GeoGig	http://geogig.org
Geograph	https://www.geograph.org
Geographic Coordinates Converter	http://www.synnatschke.de/geo-tools/coordinate-converter.php
GeoLocate This!	http://geolocatethis.site
GeoNames	http://www.geonames.org
GeoPlaner	http://www.geoplaner.com
GeoSocial Footprint	http://geosocialfootprint.com
GeoVisual Search	https://search.descarteslabs.com
Global Explorer	https://www.globalxplorer.org
Global Gazetteer	http://www.fallingrain.com/world/index.html
Go KML Maps	http://gokml.net/maps#ll=33.467074,-99.528235&z=10&t=h
Google Earth	http://www.google.com/earth
Google Maps	https://www.google.com/maps
Google Maps Downloader	http://www.allmapsoft.com/gmd
Google Maps Streetview Player	http://brianfolts.com/driver
Google My Maps	https://www.google.com/maps/about/mymaps
Gosur Map	http://www.gosur.com/map
GPSVisualizer	http://www.gpsvisualizer.com
GrassGIS	http://grass.osgeo.org
Here	http://here.com
HibeBikeMap	http://hikebikemap.org
Historic Aerials	https://www.historicaerials.com
Hivemapper	https://hivemapper.com
Hyperlapse	https://github.com/TeehanLax/Hyperlapse.js
Imergis	http://www.imergis.nl
Indian Geo-Platform of ISRO	http://bhuvan.nrsc.gov.in/data/download/index.php
INPE Image Catalog	http://www.dgi.inpe.br/CDSR
Inspire Geoportal	http://inspire-geoportal.ec.europa.eu
InstantAtlas	http://www.instantatlas.com

Instant Google Street View	http://www.instantstreetview.com
Inteltechniques Custom Mapping Tools	https://inteltechniques.com/osint/maps.html
Kartograph	http://kartograph.org
Land Cover	http://landcover.org
Land Information New Zealand	https://data.linz.govt.nz
Landsat Look	https://landsatlook.usgs.gov/viewer.html
Land Viewer	https://eos.com/landviewer
Latlong	https://www.latlong.net
Leaflet	http://leafletjs.com
Libra	https://libra.developmentseed.org
Liveuamap	http://liveuamap.com
MapAList	http://mapalist.com
MapBox	https://www.mapbox.com
Mapchart.net	https://mapchart.net
Map Checking	https://www.mapchecking.com
Map Developers	https://www.mapdevelopers.com
Maperitive	http://maperitive.net
MapHub	https://maphub.net
Mapillary	https://www.mapillary.com
mapkit	https://mapkit.io
Mapline	https://mapline.com
Map Puzzle	http://www.mappuzzle.se
Map Overlays for Google Earth	http://www.mgmaps.com/kml/#view
Mapquest	https://www.mapquest.com
meetways	https://www.meetways.com
MgMaps	http://mgmaps.com/kml/#view
Military Grid Reference System Coordinates	https://dominoc925-pages.appspot.com/mapplets/cs_mgrs.html
Modest Maps	http://modestmaps.com
Movable Type Scripts	http://www.movable-type.co.uk/scripts/latlong-os-gridref.html
MyGeoPosition	http://mygeoposition.com

NASA Earth Observatory	https://earthobservatory.nasa.gov
Naver Maps	https://map.naver.com
NEXRAD Data Archive, Inventory, and Access	https://www.ncdc.noaa.gov/nexradinv
NGA GEOINT	https://github.com/ngageoint
NOAA CLASS	https://www.bou.class.noaa.gov/saa/products/catSearch
NOAA DataViewer	https://coast.noaa.gov/dataviewer
NOAA Digital Coast	https://coast.noaa.gov/digitalcoast
OpenLayers	http://openlayers.org
OpenStreetCam	https://www.openstreetcam.org/map/
OpenStreetMap	http://www.openstreetmap.org
Overpass Turbo	https://overpass-turbo.eu
pattrn	http://pattrn.co
Photo Maps	http://photo-map.ru
Planet Explorer	https://www.planet.com/explorer
Polymaps	http://polymaps.org
Perry Castaneda Library	https://www.lib.utexas.edu/maps
Old Maps Online	http://www.oldmapsonline.org
Open Railway Map	https://www.openrailwaymap.org
Open Street Cam	http://openstreetcam.org
Open Street Map	http://www.openstreetmap.org
QGIS	http://qgis.org
QuickMaps	https://chrome.google.com/webstore/detail/quick-maps/bgbojmobaekecckmomemopckmeipecij
Radiant Earth	https://radiant.earth
Research UN Maps	http://research.un.org/en/maps
SASGIS	http://www.sasgis.org
Scribble Maps	http://scribblemaps.com
Sentinel2Look Viewer	https://landsatlook.usgs.gov/sentinel2
Sentinel Hub Playground	http://apps.sentinel-hub.com/sentinel-playground
StoryMap	https://storymap.knightlab.com
StoryMaps	http://storymaps.arcgis.com/en

Tableau	http://www.tableausoftware.com
TerraPattern	http://www.terrapattern.com
TerraServer	https://www.terraserver.com
Travel by Drone	http://travelbydrone.com
US Naviguide	http://www.usnaviguide.com
ViaMichelin	http://www.viamichelin.com
View in Google Earth	http://www.mgmaps.com/kml/#view
VITO Free Satellite Imagery	http://www.vito-eodata.be/PDF/portal/Application.html
Walking Directions	https://www.foxtons.co.uk/tools/walking_directions.html
WarWire	https://www.warwire.net
Wego.here	https://wego.here.com
Wikimapia	http://wikimapia.org
World Aeronautical Database	http://worldaerodata.com
World Map Creator	http://worldmapcreator.com
WorldMap Harvard	http://worldmap.harvard.edu
Yahoo Maps	https://maps.yahoo.com
Yandex Maps	https://yandex.ru/maps
YourNavigation	http://yournavigation.org
Zeemaps	https://www.zeemaps.com
Zoom Earth	https://zoom.earth

Interesting Maps

Tool	Link
ACLED Dashboard	https://www.acleddata.com/dashboard
ACT Government Incidents Map	http://esa.act.gov.au/community-information/incidents-map
A World of Disputed Territories	http://metrocosm.com/disputed-territories-map.html
Crime Mapping (Police.uk)	https://www.police.uk
Disputed Territories	http://metrocosm.com/disputed-territories-map.html
Global Fishing Watch	http://globalfishingwatch.org/map
Global Incident Map	http://www.globalincidentmap.com
IMB Piracy & Armed Robbery Map	https://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map
Live Piracy Map	http://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map
Live Earthquakes Map	http://quakes.globalincidentmap.com
Mapping the Flow of International Trade	http://www.visualcapitalist.com/interactive-mapping-flow-international-trade
MissileMap	http://nuclearsecrecy.com/missilemap
N2YO.com	http://www.n2yo.com
National Geographic Map Stories	https://www.nationalgeographic.com/maps
Newspaper Map	https://newspapermap.com
Nukemap	http://nuclearsecrecy.com/nukemap
Relief Web Maps	https://reliefweb.int/countries
Risk Map	https://www.riskmap.com
Roadworks	https://roadworks.org
Roman Heritage	http://sites.romaheritage.co.uk

RSOE EDIS Alert Map	http://hisz.rsoe.hu/alertmap/index2.php
Secret Bases	https://www.secret-bases.co.uk/google-earth.htm
Snapchat Map	https://map.snapchat.com
Space Near Us	http://spacenear.us
Strava Global Heatmap	https://www.strava.com/heatmap#7.00/-120.90000/38.36000/hot/all
Tracker.habhub	https://tracker.habhub.org
The True Size Of	https://thetruesize.com
Wifi SPC	https://wifispc.com
World Aero Data	http://worldaerodata.com

Privacy and Security

General Privacy Tools and Resources

Tool	Link
Abine	https://www.abine.com
AccountKiller	https://www.accountkiller.com
Background Checks	http://backgroundchecks.org
BleachBit	https://www.bleachbit.org
CCleaner	https://www.piriform.com/ccleaner
Centralised Place for Privacy Resources	https://themanyhats.club/centralised-place-for-privacy-resources
CleanMyMac	https://macpaw.com/cleanmymac
ClearConsole	https://addons.mozilla.org/en-US/firefox/addon/clear-console
Click&Clean	https://addons.mozilla.org/en-US/firefox/addon/clickclean
deseat	https://www.deseat.me
Dock	https://dock.io
Epic.org Privacy Tools	https://epic.org/privacy/tools.html
Eraser	http://eraser.heidi.ie
GNU PG	https://www.gnupg.org/download/index.html
Guardian Project	https://guardianproject.info
HotCleaner	https://www.hotcleaner.com
justdeleteme	http://justdelete.me
Me and My Shadow	https://myshadow.org
My Data Request	https://mydatarequest.com
MyPermissions	https://mypermissions.com
OptOutPrescreen	https://www.optoutprescreen.com

Peerblock	http://forums.peerblock.com
PixelPrivacy	https://pixelprivacy.com
Pribot	https://pribot.org
Prism Break	https://prism-break.org
Privacy Checker	http://www.privacychecker.nl/en
Privacy Pal	http://www.privacypal.co
Privacy Rights Clearinghouse	https://www.privacyrights.org
Privacy Tools	https://www.privacytools.io
Privazer	http://privazer.com
Opt-Out Doc	https://docs.google.com/spreadsheets/d/1UY9U2CJ8Rnz0CBrNu2iGV3yoG0nLR8mLINcnz44XESI/edit#gid=1864750866
Social Media Leak	https://robinlinus.github.io/socialmedia-leak
TOSBack	https://tosback.org
ToSDR	https://tosdr.org
Verexif	http://www.verexif.com
What Facebook Thinks You Like	https://chrome.google.com/webstore/detail/what-facebook-thinks-you/eoknmaajkanapojcdeccofmeimpddoim?hl=en

Secure Browsing

Tool	Link
Adblock Plus	https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/?src=search
Am I Unique?	https://amiunique.org
anonymoX	https://www.anonymox.net
Avast	https://www.avast.com/en-us/secure-browser
Bitdefender Traffic Light	https://www.bitdefender.co.uk/solutions/trafficlight.html
Blender	https://addons.mozilla.org/en-US/firefox/addon/blender-1
Blur	https://addons.mozilla.org/en-US/firefox/addon/donottrackplus/?src=search
Brave	https://brave.com
Browserleaks	https://browserleaks.com
Browserscope	http://www.browserscope.org
BrowserSpy	http://browserspy.dk
Citrix	https://www.citrix.com/virtualization/secure-browser.html
Click & Clean	https://chrome.google.com/webstore/detail/clickclean/ghgabhipcejejjmhhchfonmamedcbeod?hl=en
Cliqz	https://cliqz.com
Cocoon	https://getcocoon.com
Comodo's Dragon	https://www.comodo.com/home/browsers-toolbars/browser.php
Cookie AutoDelete	https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete/?src=search
Country Flags & IP Whois	https://addons.mozilla.org/en-US/firefox/addon/country-flags-ip-whois/?src=search
Credit Card Nanny	https://chrome.google.com/webstore/detail/credit-card-nanny/lfmmjpapolbaaddobpnlcjkgchmhhoog

Decentraleyes	https://addons.mozilla.org/en-US/firefox/addon/decentraleyes/?src=rating
Disconnect	https://addons.mozilla.org/en-US/firefox/addon/disconnect/?src=featured || https://disconnect.me/disconnect
Doileak	https://www.doileak.com
Epic Privacy Browser	https://www.epicbrowser.com
Ericom	https://www.ericom.com/solutions/browser-isolation
Extension Source Viewer	https://addons.mozilla.org/en-US/firefox/addon/crxviewer/?src=rating
Firefox Lightbeam	https://addons.mozilla.org/en-GB/firefox/addon/lightbeam
Forget Me Not	https://addons.mozilla.org/en-US/firefox/addon/forget_me_not/?src=featured
Freenet	https://freenetproject.org/index.html
Globus	https://globus-vpn-browser.en.softonic.com
Ghostery	https://addons.mozilla.org/en-US/firefox/addon/ghostery/?src=featured
HTTPs Everywhere	https://www.eff.org/https-everywhere
I2P	https://geti2p.net/en
IPLeak	https://www.ipleak.net
Iridium	https://iridiumbrowser.de
KeeFox	https://addons.mozilla.org/en-US/firefox/addon/keefox
Kimetrak	https://addons.mozilla.org/en-US/firefox/addon/kimetrak/?src=search
Link Cleaner	https://addons.mozilla.org/en-US/firefox/addon/link-cleaner
Netcraft Anti-Phishing Extension	https://addons.mozilla.org/en-US/firefox/addon/netcraft-toolbar
NoScript	https://noscript.net
No-Script Suite Lite	https://chrome.google.com/webstore/detail/no-script-suite-lite/ahnanjpbkghcdgmlchbcfoiefnifjeni?hl=en
Panopticlick	https://panopticlick.eff.org
Passport	https://addons.mozilla.org/en-US/firefox/addon/passbolt/?src=featured
Policeman	https://addons.mozilla.org/en-US/firefox/addon/policeman
Privacy Badger	https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/?src=search

Privacy & Security Add-ons	https://addons.mozilla.org/en-US/firefox/extensions/privacy-security
Privacy Tab	https://addons.mozilla.org/en-US/firefox/addon/private-tab/?src=rating
Private Bookmarks	https://addons.mozilla.org/en-US/firefox/addon/webext-private-bookmarks/?src=search
Safe Browser	https://chrome.google.com/webstore/detail/safe-browser/lapbdblogmakkmcnkacalmpoljnofnnj?hl=en
Safe Browsing	https://chrome.google.com/webstore/detail/safe-browsing/ecpnacfdmkfdabpdpbnnacjfdfcldklf?hl=en
Safe Web	https://safeweb.norton.com
Script Safe	https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbdgdf?hl=en
Self-Destructing Cookies	https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies
Simple Blocker	https://chrome.google.com/webstore/detail/simple-blocker/akfbkbiialncppkngofjpglbbobjoeoe
SRWare Iron	http://www.srware.net/en/software_srware_iron.php
SSleuth	https://addons.mozilla.org/en-US/firefox/addon/ssleuth/?src=rating
Sucuri Free Website Malware and Security Scanner	https://sitecheck.sucuri.net
Tor Project	https://www.torproject.org
Trust Wave	https://www.trustwave.com/Products/SecureBrowsing
UBlock Origin	https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/?src=search
UMatrix	https://addons.mozilla.org/en-US/firefox/addon/umatrix
US-CERT	https://www.us-cert.gov/publications/securing-your-web-browser
User-Agent Switcher	https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher-revived/?src=search
Vanilla Cookie Manager	https://chrome.google.com/webstore/detail/vanilla-cookie-manager/gieohaicffldbmiilohhggbidhephnjj?hl=en
Webutation	http://www.webutation.net
What browser am I using?	http://www.whatbrowseramiusing.co
WhatIsMyBrowser	https://www.whatismybrowser.com

WOT	https://www.mywot.com

Ads and Tracking Blockers

Tool	Link
AdblockPlus	https://adblockplus.org
AskBlocker	https://adamlynch.com/askblocker
Blokada	http://blokada.org
Disconnect	https://disconnect.me
Do Not Track	http://donottrack.us
Do Not Track Me Google	https://chrome.google.com/webstore/detail/dont-track-me-google/gdbofhhdmcladcmmfjolgndfkpobecpg?hl=en
Ghostery	https://www.ghostery.com
Nixory	http://nixory.sourceforge.net
No Script	https://noscript.net
Panopticlick	https://panopticlick.eff.org
PixelBlock	https://chrome.google.com/webstore/detail/pixelblock/jmpmfcjnflbcoidlgapblgpgbilinlem?hl=en
Privacy Badger	https://www.eff.org/privacybadger
Trackography	https://trackography.org
uBlock	https://www.ublock.org

Blocking of Currency Miners

Tool	Link
CryptoPrevent Malware Prevention	https://www.foolishit.com/cryptoprevent-malware-prevention/#gsc.tab=0
How-to Geek	https://www.howtogeek.com/334018/how-to-block-cryptocurrency-miners-in-your-web-browser
Malware Bytes	https://www.malwarebytes.com/lp/sem/en/?c=cj&s=2786910&aid=11971602&k=11971602&utm_source=cj&utm_medium=aff&utm_content=11971602&utm_campaign=AFF-CJ_2786910&tracking=cj&x-wts=cj&x-affid=2786910&ADDITIONAL_AFFID=cj-2786910
minerBlock	https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl
No Coin	https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl
NoScript	https://addons.mozilla.org/en-US/firefox/addon/noscript
Opera	https://www.opera.com

Private Search Engines and Private Searching

Tool	Link
Disconnect Search	https://disconnect.me/search
Discrete search	https://www.discretesearch.com
Duck Duck Go	https://duckduckgo.com
Gibiru	http://www.gibiru.com
Lukol	https://www.lukol.com
MetaGer	https://metager.de
Oscobo	https://oscobo.co.uk
peekier	https://peekier.com
Search encrypt	https://www.searchencrypt.com
Searx.me	https://searx.me
Startpage by ixquick	https://www.ixquick.com
Swisscows	https://swisscows.com
Qwant	https://www.qwant.com

Secure OS

Tool	Link
Qubes	https://www.qubes-os.org
Tails	https://tails.boum.org
whonix	https://www.whonix.org

Backup Tools

Tool	Link
Acronis	https://www.acronis.com
BackBlaze	https://www.backblaze.com
Carbonite	https://www.carbonite.com
Crashplan	https://www.crashplan.com
Dropbox	https://www.dropbox.com/?landing=dbv2
Handy Backup	https://www.handybackup.net/backup-website.shtml
IBackup	https://www.ibackup.com
IDrive	https://www.idrive.com
Jungle Disk	https://www.jungledisk.com
Mozy	https://mozy.com/#slide-11
Norton Online backup	https://nobu.backup.com/session/new
OpenDrive	https://www.opendrive.com
SiteGround	https://www.siteground.com/tutorials/getting-started/backup-and-restore-tool
Site Vault	http://www.site-vault.com
Spideroak: One	https://spideroak.com/one
SOS Online Backup	https://www.sosonlinebackup.com

Secure Communication Tools

Tool	Link
Adium	https://adium.im
Chanty	https://www.chanty.com
Chatsecure	https://chatsecure.org
Crypto.cat	https://crypto.cat
Fleep	https://fleep.io
Google Hangouts	https://hangouts.google.com
Go To Meeting	https://www.gotomeeting.com
Hipchat	https://www.stride.com
Join.me	https://www.join.me
Mailbird	https://www.getmailbird.com
Pidgin	https://www.pidgin.im
Realtime Board	https://realtimeboard.com
Signal	https://signal.org
Silent circle	https://www.silentcircle.com
Skype for Business	https://www.skype.com/en/business
Slack	https://slack.com/r/02tltzm1-02tpl6m9
Spideroak: Semaphor	https://spideroak.com/semaphor
Surveilliance Self Defense	https://ssd.eff.org
Syndie	http://syndie.i2p2.de
Telegram	https://telegram.org
Tibbr	http://www.tibbr.com
Unseen.is	https://unseen.is
Workfront	https://www.workfront.com
Yammer	https://www.yammer.com

E-mail Security

Tool	Link
10minutemail	https://10minutemail.com
20minutemail	http://www.20minutemail.com
Anonymouse	http://anonymouse.org
Ashley Madison Hack	https://ashley.cynic.al
BreachAlarm	https://breachalarm.com
Disposable-email-domains	https://github.com/martenson/disposable-email-domains/blob/master/disposable_email_blacklist.conf
Disposable-email-provider-domains	https://gist.github.com/michenriksen/8710649
E4ward	http://e4ward.com
EmailOnDeck	https://www.emailondeck.com
Enigmail	https://www.enigmail.net
Gawker Hack Email Check	https://labs.duo.com/gawker
Gmelius for Inbox by Gmail	https://chrome.google.com/webstore/detail/gmelius-for-inbox-by-gmai/dlbjhjnahgmigifoggidegpakbcjomgg
Googligan Checker	https://gooligan.checkpoint.com
Gotcha	https://gotcha.pw
GPG Tools	https://gpgtools.org
Guerrilla Mail	https://www.guerrillamail.com
Hacked Emails	https://hacked-emails.com
Have I Been Pwned	https://haveibeenpwned.com
Have I Been Sold	https://haveibeensold.app

HPI Identity Leak Checker	https://sec.hpi.uni-potsdam.de/ilc/search;jsessionid=A94B3A03C67B00F3B0FADB4A8C08E6FA
InboxBear	https://inboxbear.com
Leaked Source	https://leakedsource.ru
Lockbin	https://lockbin.com
Mailbox	https://mailbox.org
Mailinator	http://www.mailinator.com
Mailvelope	https://www.mailvelope.com
MyTrashMail	http://mytrashmail.com
Open PGP	https://www.enigmail.net/index.php/en
Pixel Block	https://chrome.google.com/webstore/detail/pixelblock/jmpmfcjnflbcoidlgapblgpgbilinlem
ProtonMail	https://protonmail.com
Psbdmp.ws	https://psbdmp.ws//
Scamdex	http://www.scamdex.com
Sneakemail	https://sneakemail.com
Snusbase	https://snusbase.com
Streak SecureGmail	https://www.streak.com/securegmail
Sudo App	https://sudoapp.com
Tempr.email	https://tempr.email
Thunderbird	https://www.mozilla.org/en-US/thunderbird
TrashMail	https://trashmail.com
Unseen.is	https://unseen.is
Vigilante	https://www.vigilante.pw
ZMail	http://zmail.sourceforge.net

Phone Security

Tool	Link
Hushed	https://hushed.com
Leaked Source	https://leakedsource.ru
Receive SMS	https://receive-sms.com
Receive SMS Online	http://receive-sms-online.com
Receive SMS Online	https://www.receivesmsonline.net
SMS Sellaite	http://sms.sellaite.com
Snusbase	https://snusbase.com
Sudo App	https://sudoapp.com
Vigilante	https://www.vigilante.pw

Password Management and Secure Login

Tool	Link
1Password	https://1password.com
Dashlane	https://www.dashlane.com
KeePass Password Safe	http://keepass.info
Last Pass	https://lastpass.com
Master Password	http://masterpasswordapp.com
Password Alert	https://chrome.google.com/webstore/detail/password-alert/noondiphcddnnabmjcihcjfbhfklnnep
Have I Been Pwned	https://haveibeenpwned.com/Passwords
Spideroak: Encrypt	https://spideroak.com/encryptr
Two Factor Auth	https://twofactorauth.org
Unseen.is	https://unseen.is
What Facebook Thinks You Like	https://chrome.google.com/webstore/detail/what-facebook-thinks-you/eoknmaajkanapojcdeccofmeimpddoim?hl=en
WOT	https://www.mywot.com
ZMail	http://zmail.sourceforge.net

Encryption Tools

Tool	Link
AES Crypt	https://www.aescrypt.com
Axcrypt	https://www.axcrypt.net
BitLocker	https://www.microsoft.com/en-in/download/details.aspx?id=7806
boxcryptor	https://www.boxcryptor.com
CertainSafe	https://certainsafe.com/digital-safety-deposit-box
Challenger	https://encryption-software.de/challenger/en/index.html
Cryptainer LE	https://www.cypherix.com/cryptainerle
CryptoExpert	https://www.cryptoexpert.com
CryptoForge	http://www.cryptoforge.com
Dekart	https://www.dekart.com/free_download
DiskCryptor	https://diskcryptor.net/wiki/Downloads
Encrypted Cloud	https://www.encryptedcloud.com
FileVault	https://support.apple.com/en-us/HT204837
Folder Lock	http://www.newsoftwares.net/folderlock
Intercrypto	https://www.intercrypto.com
Rohos	https://www.rohos.com
Secure IT	https://www.cypherix.com/secureit2000
SecurStick	http://www.withopf.com/tools/securstick
Steganos	https://www.steganos.com/de/steganos-safe-19
Streak SecureGmail	https://www.streak.com/securegmail
Symantec Drive Encryption	https://www.symantec.com/smb
Veracrypt	https://www.veracrypt.fr/en/Home.html

7-Zip	https://www.7-zip.org/download.html

Secure File Sharing

Tool	Link
Box	https://www.box.com
DropBox	https://www.dropbox.com/?landing=dbv2
Drop Send	https://www.dropsend.com
Egnyte	https://www.egnyte.com
Google Drive	https://www.google.com/drive
HighTail	https://www.hightail.com
Just Cloud	http://www.justcloud.com
OneHub	https://www.onehub.com
OpenDrive	https://www.opendrive.com
Securesha	https://securesha.re
Send This File	https://www.sendthisfile.com
Share File	https://www.sharefile.com
Smart Room	https://smartroom.com
Sugar Sync	https://www2.sugarsync.com
4Shared	https://www.4shared.com

VPN Services

Tool	Link
Box PN	https://boxpn.com
CryptoStorm	https://cryptostorm.is/#section5
CyberGhost	https://www.cyberghostvpn.com
ExpressVPN	https://www.expressvpn.com
HideMyAss	https://www.hidemyass.com
Hoxx	https://hoxx.com
Hotspot Shield	https://www.hotspotshield.com
IPVanish	https://www.ipvanish.com
Mullvad	https://mullvad.net
NordVPN	https://nordvpn.com
Overplay	https://www.overplay.net/en/products/vpn
Personal VPN	https://www.personalvpn.com
Pure VPN	https://www.purevpn.com
TorGuard	https://torguard.net
TunnelBear	https://www.tunnelbear.com
Private Internet Access	https://www.privateinternetaccess.com
Speedify	http://speedify.com/desktop-vpn
Strong VPN	https://strongvpn.com/plans.htm
UnoTelly	https://www2.unotelly.com
Viking VPN	https://vikingvpn.com
VPN Unlimited	https://www.vpnunlimitedapp.com
Vypr VPN	https://www.goldenfrog.online/vyprvpn
Windscribe	https://windscribe.com

ZenMate	https://zenmate.com
ZenVPN	https://zenvpn.net/en

VPN Texting

Tool	Link
Check IP	https://www.perfect-privacy.com/check-ip
DNS Leak	https://www.dnsleaktest.com
DNS Leak Test	http://dnsleak.com
Email Leak Test	http://emailipleak.com
IPCheck	http://ip-check.info
IPLeak	https://ipleak.net
IPv6 Leak Test	http://ipv6leak.com

Proxy Tools

Tool	Link
4everproxy	http://www.4everproxy.com
anype	http://www.anype.com
FilterBypass	https://www.filterbypass.me
Hide.me	https://hide.me/en/proxy
HideMyAss Proxy	https://www.hidemyass.com/proxy
Premium Proxy	https://premproxy.com
Proxy4Free	http://www.proxy4free.com
ProxySite	https://www.proxysite.com
Public Proxy Servers	http://www.publicproxyservers.com

Antivirus Software

Tool	Link
Avast Pro Antivirus	https://www.avast.com/en-us/pro-antivirus
AVG Internet Security Unlimited	https://support.avg.com/support_Protection?l=en
BitDefender Antivirus Plus	https://www.bitdefender.com/media/html/2018/cl50off-opt/?pid=50off&cid=aff|c|ir
BullGuard	https://www.bullguard.com/products/bullguard-antivirus.aspx
ESET Internet Security	https://www.eset.com/us/newyear/?ref=AFC-CJ&attr=7603059&pub=12800315&shop=521pxCDDNg
ESET NOD32 Antivirus	https://www.eset.com/us/home/antivirus
F-Secure Anti-Virus	https://www.f-secure.com/en_US/web/home_us/anti-virus
McAfee Antivirus Plus	https://www.mcafee.com/consumer/en-us/promos/sem/l1144/0s/01/01/a/01_sl125.html
McAfee Total Protection	https://www.mcafee.com/consumer/en-us/store/m0/catalog/mtp_521/mcafee-total-protection.html
Norton Antivirus Basic	https://us.norton.com/norton-antivirus
Norton Security Deluxe	https://us.norton.com/norton-security-antivirus
Sohos Home Premium	https://home.sophos.com
Trend Micro Antivirus + Security	https://www.trendmicro.com/en_us/forHome/products/antivirus-plus.html
Webroot SecureAnywhere Antivirus	https://www.webroot.com/us/en/home/products/av

Other Security Tools

Tool	Link
Angry IP Scanner	http://angryip.org
Cymon	https://cymon.io
Defacer	https://defacer.id
ID Ransomware	https://id-ransomware.malwarehunterteam.com
InSpectre	https://www.grc.com/inspectre.htm
jotti	https://virusscan.jotti.org
Malwarebytes Anti-Rootkit Beta	https://www.malwarebytes.com/antirootkit
NoMoreRansom	https://www.nomoreransom.org
Open DNS	https://www.opendns.com/home-internet-security
OSSEC	https://ossec.github.io
Pulsedive	https://pulsedive.com
Security-in-a-box	https://securityinabox.org
Snort	https://www.snort.org
Tech Solidarity	https://techsolidarity.org
ThreatCrowd	https://threatcrowd.org
Threatglass	http://www.threatglass.com
urlquery	https://urlquery.net
Virus Total	https://www.virustotal.com
W3bin	https://w3bin.com
Zone-h	http://www.zone-h.org

Copyright and Takedowns

Tool	Link
Copyscape	https://www.copyscape.com/compare.php
Copyright.gov	https://www.copyright.gov
Copyright Information	http://www.copyrightinformation.org/the-copyright-alert-system
Copywrited.com	https://www.copyrighted.com
DMCA	https://www.dmca.com/Takedowns.aspx
DMCA Pro	http://dmca.pro
Google Webmasters	https://www.google.com/webmasters/#?modal_active=none
Hack Hunter	https://www.hack-hunt.com
Link Killer (Fresh Killer)	http://killer.freshface.cz
Lumen Database	https://lumendatabase.org
Whois Ad-ons	https://addons.mozilla.org/en-US/firefox/search/?q=whois&appver=&platform=
MyVows	https://myows.com
NPPA	https://nppa.org/page/5617
Patent Trademark Laws	http://www.patent-trademark-law.com/copyrights/plagiarism-take-down-stolen-content/cease-desist-dmca-takedown
Plague Hunter	https://www.plaghunter.com
XDMCA Takedown Tool	http://xdmca.com

Researching Leaks

Tool	Link
BalkanLeaks	https://balkanleaks.eu
Cryptome	https://cryptome.org
DataBreaches	https://www.databreaches.net
FindMySnap	http://findmysnap.com
GLOBALLEAKS	https://www.globaleaks.org
OCCRP Data	https://data.occrp.org
Offshore Leaks	https://offshoreleaks.icij.org
Public Library of US Diplomacy	https://search.wikileaks.org/plusd
WELEAKINFO	https://weleakinfo.com
Wikileaks	https://wikileaks.org
Wikileaks Advanced Search	https://search.wikileaks.org/advanced
WikiSpooks	https://wikispooks.com

Research and Recon Tools

Research and Data Recon Tools

Tool	Link
AutOISNT	https://github.com/bharshbarger/AutOSINT
Belati	https://github.com/aancw/Belati
Buscador	https://inteltechniques.com/buscador
dataspoit	https://github.com/DataSploit/dataspoit
FAW Project	https://it.fawproject.com
Inquisitor	https://github.com/penafieljlm/inquisitor
Int-Rec-Pack	https://github.com/NullArray/IntRec-Pack
Intrigue	http://intrigue.io
Maltego	https://www.paterva.com/web7
OSINT Browser	http://osirtbrowser.com
osintstalker	https://github.com/milo2012/osintstalker
OSINT-SPY	https://github.com/SharadKumar97/OSINT-SPY
OSINT Toolkit	https://osinttoolkit.github.io
osrframework	https://github.com/i3visio/osrframework
Paliscope	https://www.paliscope.com
Recon-ng	https://bitbucket.org/LaNMaSteR53/recon-ng
Scumblr	https://github.com/Netflix/Scumblr
Social Recon	https://www.kitploit.com/2018/01/social-recon-investigate-online.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PentestTools+%28PenTest+Tools%29
Spiderfoot	http://www.spiderfoot.net
theharvester	https://github.com/laramies/theHarvester

XRay	https://n0where.net/network-osint-gathering-tool-xray

OSINT Tools Lists

OSINT Tools Lists

Tool	Link
101+ OSINT Resources for Investigators (i-sight)	https://i-sight.com/resources/101-osint-resources-for-investigators
Aware Online Academy OSINT Links	https://aware-online.com/academy/osint-links
Awesome OSINT	https://github.com/jivoi/awesome-osint
Awesome_osint	https://github.com/Ph055a/awesome_osint
Bellingcat OSINT Links	https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit
Bruno Mortier Sources	https://start.me/p/3g0aKK/sources
Bruno Mortier Sources CNTY	https://start.me/p/W2kwBd/sources-cnty
CiberPatrulla	https://ciberpatrulla.com/links
DFIR Training Tool Directory	https://www.dfir.training/index.php/tools/advanced-search
Digital intelligence Research Tools	https://atlas.mindmup.com/digintel/digital_intelligence_training/index.html
Emmanuelle Welch Dating apps and sites for investigators	https://start.me/p/VRxaj5/dating-apps-and-sites-for-investigators
HR Sourcing Toolbox	https://hrsourcingtoolbox.wixsite.com/main
Julia Bayer Verification Toolset	https://start.me/p/ZGAzN7/verification-toolset
inteltechniques Internet Search Links	https://inteltechniques.com/menu.links.html
MidaSearch OSINT Websites	https://midasearch.org/osint-websites
Netbootcamp OSINT Tools	https://netbootcamp.org/osinttools

Onstrat OSINT Starting Points	http://www.onstrat.com/osint/#startingpoints
OSINT Browser Plugins	https://github.com/IVMachiavelli/OSINT-Browser-Plugins
OSINT Framework	http://osintframework.com
OSINT Link	http://osint.link
OSINT Post	https://osintpost.com
OSINT Team Links	https://github.com/IVMachiavelli/OSINT_Team_Links
RBA Business Information Resources	http://www.rba.co.uk/sources
Research Clinic	http://www.researchclinic.net
Reuser OSINT Discovery Toolkit	http://rr.reuser.biz
Startme Open Source Investigative Tools by Malachy Browne	https://start.me/p/gyvaAJ/open-source-investigative-tools
Startme OSINT Technisette	https://start.me/p/m6XQ08/osint || https://start.me/p/nRQNRb/addons
Sprp77 Awesome OSINT	https://drive.google.com/drive/folders/0BwyWDQ59jRVGMFp3UnBfeUEzanM
Toddington Resources	https://www.toddington.com/resources
Tomoko Discovery Tools List	https://tomokodiscovery.com/free-tools-osint-socmint-dark-web-darknet-tor-bitcoin
ToolsInsight	http://www.toolsinsight.com
Uk-osint	http://www.uk-osint.net/addons.html

Contact

Chris Pallaris

Director

i-intelligence

+41 (0) 43 243 3849 | info@i-intelligence.eu

www.i-intelligence.eu | @i_intelligence

governmentattic.org
"Rummaging in the government's attic"

Description of document:	Defense Intelligence Agency (DIA) Style Manual for Intelligence Production, 2016
Requested date:	20-June-2014
Released date:	02-February-2017
Posted date:	13-March-2017
Source of document:	FOIA Request Defense Intelligence Agency ATTN: FAC2A1 (FOIA) 7400 Pentagon Washington, DC 20301-7400 Fax: (301) 394-5356 Email: FOIA@dodiis.mil FOIA Request Online Templates: PDF Microsoft WORD

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-5100

U-17-1066/FAC-2A1 (FOIA)

FEB 02 2017

This responds to your Freedom of Information Act (FOIA) request, dated June 20, 2014, that you submitted to the Defense Intelligence Agency (DIA) for information concerning a copy of the Defense Intelligence Agency Style Manual. I apologize for the delay in responding to your request. DIA continues its efforts to eliminate the large backlog of pending FOIA requests. In order to properly respond, it was necessary to consult with another office within the agency.

A search of DIA's systems of records located one document (234 pages) responsive to your request.

Upon review, I have determined that some portions of the one document (234 pages) must be withheld in part from disclosure pursuant to the FOIA. The withheld portions are exempt from release pursuant to Exemptions 3 of the FOIA, 5 U.S.C. § 552 (b)(3). Exemption 3 applies to information specifically exempted by a statute establishing particular criteria for withholding. The applicable statute is 10 U.S.C. § 424. Statute 10 U.S.C. § 424 protects the identity of DIA employees, the organizational structure of the agency, and any function of DIA

If you are not satisfied with my response to your request, you may contact the DIA FOIA Requester Service Center, as well as our FOIA Public Liaison at 301-394-5587.

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. You may contact OGIS by email at ogis@nara.gov; telephone at 202-741-5770, toll free at 1-877-684-6448 or facsimile at 202-741-5769; or you may mail them at the following address:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road-OGIS
College Park, MD 20740-6001

You may also exercise your right to file an administrative appeal by writing to the address below and referring to case number 0374-2014. Your appeal must be postmarked no later than 90 days after the date of this letter.

Defense Intelligence Agency
7400 Pentagon
ATTN: FAC-2A1 (FOIA)
Washington, D.C. 20301-7400

Sincerely,

Alesia Y. Williams
Chief, FOIA and Declassification Services Office

Enclosure

UNCLASSIFIED

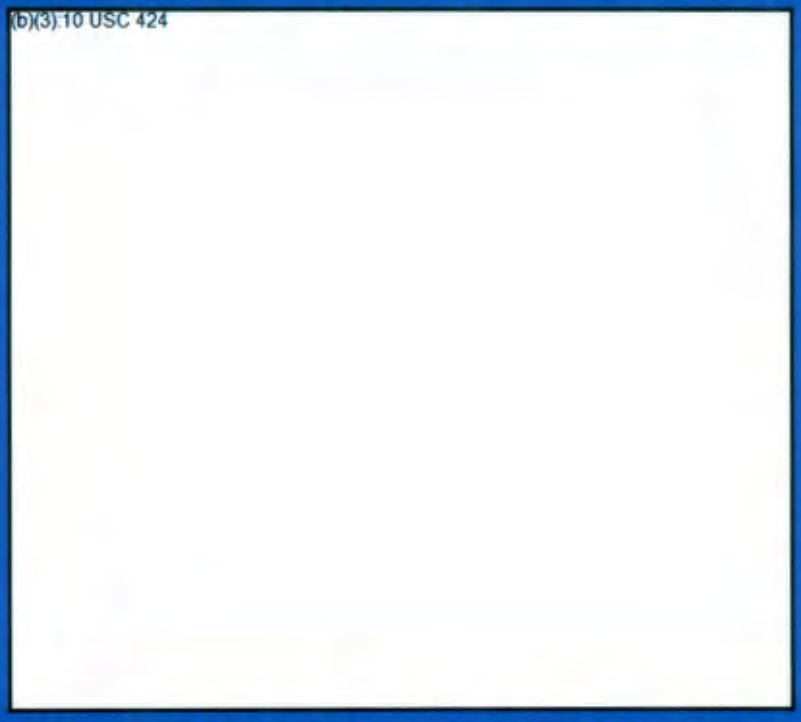
DEFENSE INTELLIGENCE AGENCY

DIA Style Manual
for Intelligence Production

2016

ICOD: 11 December 2015
DIA-01 1309-510

UNCLASSIFIED



DIA Style Manual
for Intelligence Production

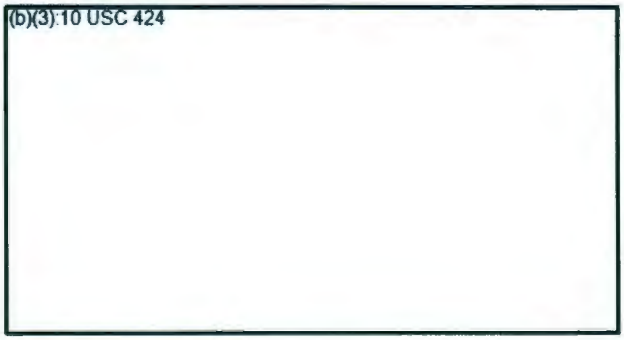
DIA Style Manual for Intelligence Production

Defense Intelligence producers are more than analysts; they are also professional writers. Despite various new media and technological developments, writing is still the principal medium through which the Agency conveys its information, ideas, and concerns to customers. If our written products are to have the impact and inspire the confidence they warrant, they need to be delivered in a well-crafted package.

This manual is the authoritative reference to help us create that package. It sets Agency standards for written intelligence production, minimizing the guesswork on capitalization, numbers, abbreviations, and other style points. Consequently, intelligence producers can focus on crafting effective arguments to support analytic judgments.

The *DIA Style Manual for Intelligence Production* has been in use for decades. The manual's executive agent, the Directorate for Analysis, refines the guidance as Intelligence Community standards develop and the language evolves. The U.S. Government Printing Office *Style Manual* served as the basis for most of the guidance in this manual, and other references provided additional direction, notably *The Gregg Reference Manual.*

As professional analysts, we focus every day on maintaining subject matter expertise, but communicating that expertise requires us to maintain excellent writing skills. DIA must convey a Defense Intelligence message that is concise, precise, and compelling. This manual is a key tool in our arsenal as we execute our mission and ensure we meet the highest possible standards.



CONTENTS

CHAPTER 1: Practical Advice for Writers and Editors

Be Aware of Grammar Rules Versus Superstitions 3
Consider Style and Context 3
Use Short Sentences and Paragraphs 3
Short Sentences 3
Get to the Point in Topic Sentences 4
Focus Headings 4
Limit the Passive Voice 4
Recognizing Passive Voice 4
Activating the Passive 5
Using Passive Voice Effectively 5
Rethink Expletive Constructions 5
Don't Confuse Passive Voice and Past Tense 5
Avoid Nouns That Stifle Verbs 6
Use Qualifiers Judiciously 6
Avoid Cliched Concepts and Jargon 6
Keep Parallel Ideas in Parallel Form 6
Put Modifiers in Their Place 7
Restrictive Modifiers 7
Danglers 7
Avoid Illogical Shifts Within a Sentence 7
Tense 7
Mood 7
Work Toward a Common Goal: Readability 8
Subject or Voice 8
Person 8
Number 8
Tone or Style 8

CHAPTER 2: Abbreviations

To Use or Not To Use 11
When To Introduce an Abbreviation 11
Establishing Abbreviations 12
Forming and Using Abbreviations 12
Capitalization 12
Italics With Abbreviations 13
Periods in Abbreviations 13
Plural and Singular Abbreviations 13
Forming Plurals of Abbreviations 13
Possessives and Abbreviations 14

Prefixes and Suffixes With Abbreviations 14
Hyphenation When Introducing Abbreviations 15
Articles Accompanying Abbreviations 15
A or An? 15
Nix GOx Abbreviations 16
Avoiding Redundancy 16
Country Names 16
Military Rank/Rate 16
U.S. Army Officers/Warrant Officers 16
U.S. Navy and Coast Guard Officers/Warrant Officers 17
U.S. Air Force Officers 17
U.S. Marine Corps Officers/Warrant Officers 17
U.S. Army Enlisted Personnel 18
U.S. Navy and Coast Guard Enlisted Personnel 18
U.S. Air Force Enlisted Personnel 18
U.S. Marine Corps Enlisted Personnel 19
Foreign Military Officers 19
Units of Measure 20
Months and Days 21
Percent and Other Symbols 21
Abbreviation List 22

CHAPTER 3: Capitalization

Beginnings 59
Proper Names 59
Capitalizing Plurals 59
Common Nouns in Proper Names 60
Derivatives of Proper Names 60
Particles With Proper Names 61
Organized Bodies 63
Governmental Bodies 63
Parliament 63
Military Forces 64
U.S. Military Services and Combatant Commands 65
International Organizations 65
Diplomatic and Consular Units 65
The Agency 66
DIA-Specific Capitalization 66
Political Parties and Philosophies 66
Party Names 66

CONTENTS

Philosophies 66
Religious Terms 66
Geographic Terms 67
Nationalities, Tribes, and Other Groups of People 68
Coined Names 68
Titles of Persons 69
The U.S. President 69
Titles and Headings 70
Cross-References 70
Word Equivalents of Abbreviations/Acronyms 70
Emphasis 70
Seasons 70
Military Equipment Designators 70
Military Exercises, Operations, and Special Projects 71
Academic Degrees 71
Chemical Elements and Isotopes 71
Plant and Animal Genus and Species 72

CHAPTER 4: Numbers

Basic Rules 75
Turning Off Superscripting for Ordinal Numbers 76
Other Number Rules 76
Ordinal Numbers 76
Numbers in Tables 77
Numbers at Beginnings of Sentences 77
Metric Units 77
Metric and Nonmetric 78
Measurements 79
Age 79
Dates 79
From, Between, and Dashes 80
Time 80
Years 80
Decades/Centuries 80
Clock Time 81
Money 81
Percentages 81
Times Phrases 81
Ratios, Odds, Returns 81

BE Numbers 82
Geographic Coordinates 82
Mathematical Expressions 82
Numerical Designators 82
Numbers in Proper Names 82
Indefinite and Nonliteral Numbers 83
Millions, Billions, and So Forth 83
Ranges 83
Approximation 83
Commas With Numbers 84
Numbers With x To Stand for by 84
Possessive Case With Numbers 84
Decimals 84
Fractions 84
Mixed Numbers 85
Numbers in Unit Modifiers 85
Numbers Side by Side 85
Singular and Plural Units With Numbers 85
Quantities and Numbers as Subjects 86

CHAPTER 5: Current Usage

Word Choices 89
Among and Between 92
Compose, Comprise, Constitute, Include 96
Data 98
Endemic, Indigenous, Native 99
Instead of, Rather Than, Vice, Versus 102
Leaders, Leadership 103
Not Only … But Also 105
Parliamentarian 106
Predominant, Predominate, Predominantly, Predominately 107
Represent 108
Omitting ***That*** 109
Economy of Words 113
Simple Words 118

CHAPTER 6: Punctuation

Apostrophe 123
For Possessives 123

CONTENTS

Apostrophes and Descriptives 124
For Some Plurals 124
Brackets 125
Square Brackets 125
Angle Brackets 125
Bullets 126
Marking Bulleted Items 126
Presenting Bulleted Items 126
Colon 126
Improper Colon Use 127
Punctuation for Source Reference Citations (Endnotes) in Intelligence Products 127
Serial Comma 128
Comma 128
Watch for Dangling Modifiers 130
Marking Interruptions 130
Beware of Comma Splices 131
Coordinate and Cumulative Adjectives 132
Dashes 133
Em-Dash 133
Dashes and the Hyphen 133
En-Dash 134
Ellipsis 135
Exclamation Point 135
Italics 136
Parentheses 140
Period 140
Question Mark 141
Quotation Marks 141
Double Quotation Marks 141
U.S. Versus British Use of Quotation Marks 142
Spacing Between Colocated Single and Double Quotation Marks 143
Single Quotation Marks 144
Punctuation With Quotation Marks 144
Semicolon 144
Slash 145

CHAPTER 7: Spelling and Compounding

Spelling Rules 149
Geographic Names 149
Diacritical Marks 149

American Versus British Spellings 150
Plurals of Compound Terms 150
Compounding Rules 150
General Rules 150
Separate Words 150
Joined or Hyphenated Words 150
Derivatives 150
Solid Compounds 151
Parts of Speech and Compounding 151
Unit Modifiers 153
Hyphenated 153
A Caution About Modifier Strings 153
Joined 154
Unhyphenated 154
Predicate Adjectives 154
Comparatives and Superlatives 154
Three-Word Modifiers 155
Foreign Phrases 155
Adverbs Ending in *-ly* 155
Suspending Hyphens 156
Proper Nouns 156
Quotation Marks 156
Chemical Terms 156
Letter or Number Elements 156
Common Basic Elements 156
Prefixes and Suffixes 157
Numerical Compounds 158
Other Compounds 159
Using the Spelling and Compounding List 159
Gender Neutrality 160
Spelling and Compounding List 161

APPENDIX: **Metric and English Conversion Factors**

Length/Distance 221
Area 221
Mass 222
Volume 222
Temperature 222

CHAPTER 1: Practical Advice for Writers and Editors

In the dark days and darker nights when England stood alone—and most men save Englishmen despaired of England's life—he mobilized the English language and sent it into battle.

—President John F. Kennedy on Winston Churchill

CHAPTER 1: Practical Advice for Writers and Editors

Unlike the rest of this style manual, which focuses on "house style" issues, this chapter presents practical advice for authors and editors to consider in intelligence-related writing.

Be Aware of Grammar Rules Versus Superstitions

Good writers and editors need to be familiar with foundational grammar rules, such as subject-verb agreement, but they also need to recognize what is and is not a hard-and-fast rule. Many people remember learning that they should not split infinitives or end a sentence with a preposition, but both are "rules" modern usage references largely dismiss.

> The organizers decided to immediately address parking for employees and guests.

Moving the adverb "immediately" anywhere else in this sentence would make the meaning less clear. The natural place for an adverb is directly in front of the word it describes. Bottom line: avoid split infinitives if you prefer, but don't make a sentence awkward or confusing by doing so. The same guidance applies to ending a sentence with a preposition.

Consider Style and Context

Similarly, writers and editors need to recognize an error as opposed to a style or context decision.

- Failing to capitalize a word at the beginning of a sentence is an error, but not capitalizing a person's title when it is separated from the name is a style choice (see Chapter 3).
- Spelling out numbers less than 10 in some cases but using numerals for them in others may appear to be a consistency error, but a closer look may show the presentation is in keeping with style guidance to use numerals for all numbers in a sentence when any are equal to or greater than 10 (see Chapter 4).
- Treating words such as *none* and *majority* as plural may appear to be a subject-verb agreement error, but these words can be treated as either singular or plural, depending on the context (see Chapter 5).

This guide offers numerous examples of preferred presentation and answers many questions that come up in intelligence writing, but it does not cover every situation. For additional guidance, use a good all-around reference on the mechanics of writing, such as *The Gregg Reference Manual*. It contains detailed guidance, with numerous examples, on punctuation, grammar, and usage. However, keep in mind that the *DIA Style Manual for Intelligence Production* takes precedence on style issues, such as capitalization and compounding.

Use Short Sentences and Paragraphs

Studies of writing today advise authors to keep both sentences and paragraphs short—not necessarily because readers can't deal with more complex writing, but because shorter sentences and paragraphs are easier to read and can be understood more quickly.

Traditionally, writers have used a paragraph to show the development of a single thought. For a complex thought, though, the paragraph's length could become quite imposing. Moreover, for a publication with type in columns, paragraphs seem even longer because fewer words fit on a line. There's a real risk, then, that several long paragraphs will resemble a solid block of type.

Short Sentences

Short sentences—fewer than 20 words—make your readers' task easier. Use caution, though; too many short sentences can make your writing choppy. Good writers mix long and short sentences for variety. Just wrap it up when those longer sentences reach about 30 words.

The key is to look for minor changes within the thought of the long paragraph and to break the paragraph at those points. The unity and coherence of the thought aren't likely to suffer. Breaking material into shorter paragraphs is simply a better way of packaging ideas—one that uses white space to show readers minor shifts in organization, helping to speed them through their reading.

Get to the Point in Topic Sentences

When organizing material in intelligence products, keep in mind that the topic sentence (first sentence) is the most important part of a paragraph. The topic sentence should be straightforward, encapsulating the message of the paragraph up front. Don't lead a topic sentence with a dependent clause, especially one that begins with a contrary term, such as *although, despite,* or *however.* Such clauses can impede the reader's ability to absorb the main point. Use subsequent sentences in the paragraph to fill out the story.

Focus Headings

A heading can announce the topic of a section, or it can do more—focusing readers' attention on the main point of the section. Avoid labels like "Background" or "Introduction." Look instead for headings that provide the gist of a section, especially headings that express the point in a way that invites readers to continue reading. Don't try too hard to grab attention, though; cute titles or headings can detract from the professionalism of your presentation.

For long studies, there's another consideration: levels of headings. You have to be wary of the organizational complexity you try to portray with the headings. For the most part, writers of books only occasionally go beyond two levels of headings. Readers are likely to become confused if you try to portray three or four levels of headings throughout a long document.

Make your outline as complex as you need to help you organize the points and subpoints in what you write. However, when you actually write, use headings to highlight only the most important points, and focus readers' attention with the wording of those headings.

Limit the Passive Voice

Passive voice is one of the less desirable features of bureaucratic writing. Passive constructions are more wordy than corresponding active constructions and can generate other wordiness—especially sentences beginning with "It is" and "There are." In addition, passive voice is indirect, reversing the natural order of spoken English, and it lacks the vigor inherent in active voice. Finally, passive constructions often mask the actor. Imagine being told, "Your fate will be decided tomorrow." Your reaction is to demand, "By whom?" Passive voice makes it all too easy for writers to omit the "by" part of a thought, and this evasiveness in particular is a mark of bureaucratic writing.

Recognizing Passive Voice

The natural order for an English sentence—actor-action-acted upon—requires active voice:

The sailor	*rowed*	*the boat*
(actor)	(action)	(acted upon)

A sentence in passive voice reverses that order:

The boat	*was rowed*	*by the sailor.*
(acted upon)	(action)	(actor)

Recognizing these constructions in more complicated sentences still is quite simple; that's why grammar-checking software can locate passive verbs quite well. Only a passive sentence will receive "yes" answers to all of the following tests:

- Is the subject of the sentence acted upon?
- Does the sentence combine a form of *to be* with the past participle of a main verb? The simple forms of *to be* are *is, am, are, was,* and *were.* Compound forms are *will be, is being,* and *has been.* Past participles of main verbs usually end in *-ed* or *-en* (except for irregular verbs such as *shot*). Thus, passive verbs look like these: *is divided, was shaken, has been shot.*

Don't Confuse Passive Voice and Past Tense

Both active and passive forms of a verb can appear in present, past, or even future tenses:

Active: takes, took, will take
Passive: is taken, was taken, will be taken

- If the actor appears in the sentence, is it in the prepositional phrase *by someone or something?* Or, if the actor doesn't appear in the sentence, does the sense of the sentence imply *by someone or something?*

Activating the Passive

Far too often, writers accept passive voice because they can't think how to write in the active voice; in such cases, passive is more accidental than intentional. You can prevent this lack of control in your own writing by learning the following three methods to convert passive voice into active:

- Reverse the object and the subject.

Passive: The greatest area coverage is offered by open-wire lines.
But: Open-wire lines offer the greatest area coverage.

- Delete the past participle main verb, leaving the form of *to be* as the only verb.

Passive: The processing plants are located in the north.
But: The processing plants are in the north.

- Change the verb. For example, *received* is an active counterpart of *was given.*

Passive: About 17,000 people are employed in research institutes.
But: About 17,000 people work in research institutes.

Using Passive Voice Effectively

Is passive voice always wrong? No, of course not. Passive constructions have legitimate uses:

- When the object of the action is more important than the actor.
- When the actor is obvious, unimportant, or unknown.

But be careful! You can stretch those justifications to cover most sentences if you try hard enough. Even when the object of an action is more important than the actor, a verb in passive voice may not be necessary. Notice that the second and third methods for activating the passive do not require you to alter the subject of the sentence. Instead, both of these methods change the verb. A good rule of thumb, then, is to use the passive voice only when you have a strong reason.

Rethink Expletive Constructions

Like passive voice, expletive constructions (*it is, it was, it will be, there are, there were, there will be*) lengthen a sentence, delay the point, mask responsibility, and force the subject to follow the verb. The fix is often simple:

Unemphatic: There was a second explosion that killed three soldiers.
Emphatic: A second explosion killed three soldiers.

Unemphatic: It is probable that voter turnout will be heavy.
Emphatic: Voter turnout probably will be heavy.

Avoid Nouns That Stifle Verbs

Strong writing requires strong verbs, so don't bury verbs inside nouns by attaching *-ion, -tion, -ment, -ance,* and *-ence.*

Weak: Chemical attacks are in violation of the treaty.
Strong: Chemical attacks violate the treaty.

Weak: North Korea has made a commitment to resume talks.
Strong: North Korea has committed to resuming talks.

Use Qualifiers Judiciously

Qualifiers are often necessary for accuracy in intelligence writing, but multiple qualifiers impede clarity. Words that already express a degree of judgment—for instance, *imply, indicate,* and *suggest*—should not be combined with qualifiers such as *may, likely,* and *probably.*

Not: The lull in attacks may indicate the rebels are ready to negotiate.
But: The lull in attacks indicates the rebels are ready to negotiate.
Or: The lull in attacks may mean the rebels are ready to negotiate.

Avoid Cliched Concepts and Jargon

When we discuss cliches, we usually think of overused comparisons like "blind as a bat" or "older than dirt"—phrases most of us know to avoid. However, cliches also can be stale words or phrases that indicate concepts in intelligence writing. Watch out for terms such as "paradigm" or "center of gravity"; they can be the words you need at times, but overuse can turn them into unhelpful catchphrases.

Along similar lines, avoid jargon that is familiar to a particular community but not to your entire audience. If an editor needs a term explained, chances are many other readers will as well.

As you choose the terms for your intelligence papers, be sure the concepts are fresh, accurate, and appropriate. Think twice about using a term just because you've seen it in a number of other papers—it may not be the right wording for your product.

Keep Parallel Ideas in Parallel Form

Parallelism is particularly important for headings and bulleted lists. Readers expect headings to be in parallel form. Parallelism is even more important in lists, since their purpose is to emphasize a pattern of organization.

Readers grasp parallel ideas more quickly when they are in parallel form. Nouns should be parallel with nouns, active verbs with active verbs, infinitive phrases with infinitive phrases, subordinate clauses with subordinate clauses, and so on.

Not: The general's success has resulted from the allegiance of his troops and how he has treated the civilians in his region to gain their acceptance. [Noun paralleled with clause.]
But: The general's success has resulted from the allegiance of his troops and the acceptance of the civilians in his region. [Noun paralleled with noun.]
Not: As a soldier he had been in Japan, fighting in Vietnam, and following his general to the Middle East. [Verb paralleled with participles.]
But: As a soldier he had been in Japan, had fought in Vietnam, and had followed his general to the Middle East. [Verb paralleled with verbs.]

When it will help make the parallelism clear, repeat a preposition, an article, a helping verb, the *to* of an infinitive, or the introductory word of a long phrase.

Not: Overextended police forces have done little to protect farmers threatened by strongmen employed by drug dealers, interdict drug shipments, or destroy processing laboratories.

But: Overextended police forces have done little to protect farmers threatened by strongmen employed by drug dealers, to interdict drug shipments, or to destroy processing laboratories.

Put Modifiers in Their Place

Restrictive Modifiers

Placement of restrictive modifiers such as *almost, every, just, merely, most, nearly, only, primarily,* and *principally* requires care. Look at the effect of placement for *only* in "This plant produces lug nuts."

Only this plant produces lug nuts. [No other plant produces them.]
This plant only produces lug nuts. [The plant doesn't do anything else with them, such as marketing.]
This plant produces only lug nuts. [The plant produces nothing else.]
This plant produces lug nuts only. [The plant produces nothing else.]

As a general rule, put modifiers close to whatever they modify. "Close to" can be before or after the thing modified, so long as the sentence makes sense.

Not: The agreement provided for military equipment which was signed recently.

But: The agreement, which was signed recently, provided for military equipment.

Or: The recently signed agreement provided for military equipment.

Danglers

Pay particular attention to a modifier that begins a sentence. Dangling modifiers can occur anywhere in a sentence but are most common at the beginning. Readers expect an introductory word or phrase modifier to refer to the subject of the sentence. When the modifier cannot logically modify the subject, the modifier "dangles."

Not: When completely filled out and checked, the taxpayer should sign the form.

But: When the form is completely filled out and checked, the taxpayer should sign it.

Or: After completely filling out and checking the form, the taxpayer should sign it.

Note, however, that some introductory phrases express a general truth rather than modifying the subject of the sentence. These introductory phrases do not dangle.

Given the importance of the operation, the staff studied a number of scenarios.
To sum up, we all agree to support the change.

Avoid Illogical Shifts Within a Sentence

Sudden, illogical shifts within a sentence or passage obscure the meaning and hamper reading:

Tense

Not: The farmer was intimidated by threats and cultivates coca leaves. [Shift from past tense to present tense.]

But: The farmer was intimidated by threats and began cultivating coca leaves. [Both verbs in past tense, with the second verb implying a continuing action.]

Mood

Not: Determine the margins for the page, and then you should set tabs. [Shift from imperative mood to indicative mood.]

But: Determine the margins for the page, and then set the tabs. [Both verbs in imperative mood.]

Subject or Voice

Not: The troops hurried up the mountain path, and soon the camp came into their sight. [Subject shifts from *troops* to *camp*.]

But: The troops hurried up the mountain path and soon saw the camp. [One subject only.]

Not: The soldier did not relish a reduction in pay, but confinement to barracks was seen as the harsher punishment. [Subject shifts from *soldier* to *confinement* as active voice shifts to passive voice.]

But: The soldier did not relish a reduction in pay but saw confinement to barracks as the harsher punishment. [One subject only and both verbs active.]

Person

Not: Analysts will find the new library hours a great convenience. You will have greater freedom to arrange your research time. [Shift from third to second person.]

But: Analysts will find the new library hours a great convenience. They will have greater freedom to arrange their research time. [Constant third person.]

Number

Not: The United Nations deserves encouragement. Indeed, they deserve more than that. [If *United Nations* takes a singular verb in the first sentence, it cannot take a plural pronoun reference in the second sentence.]

But: The United Nations deserves encouragement. Indeed, it deserves more than that. [*United Nations* and *it* correspond in number.]

Tone or Style

Not: Analysis of the main obstacles to harmony in the United Nations reveals that a group of nations refuses to play ball with the rest of the world. [Shift from formal to colloquial style.]

But: Analysis of the main obstacles to harmony in the United Nations reveals that a group of nations refuses to cooperate with the rest of the world. [Consistent formal style.]

Work Toward a Common Goal: Readability

Most writers and editors in the Intelligence Community have a common appreciation for the need to produce accurate, concise, clear intelligence for their readers, particularly busy policymakers and warfighters. Neither excessive pride of authorship nor heavyhanded editing helps to achieve that goal. Producers should keep two things in mind:

- All analytic products are the work of the Defense Intelligence Agency, not solely of the analyst or office on the byline. Authors need to recognize that just as senior intelligence officers and other reviewers have a responsibility to ensure the quality of the analytic content, technical editors have a responsibility to ensure the readability and professionalism of the presentation.
- At the same time, editors need to keep their changes focused on readability. Rather than altering the author's voice, editors should keep changes to the minimum necessary to ensure clarity, consistency, conformance with DIA style and Intelligence Community standards, and good grammar and usage. Some products require more editing than others to achieve these objectives, but overediting risks introducing errors and should be avoided.

CHAPTER 2: Abbreviations

Do not use initials for the names of organizations or movements unless you are certain the initials will be readily understood. Write things out. Not everyone knows that MADD means Mothers Against Drunk Driving, and even if everyone did, there are babies being born every minute who will someday encounter the name for the first time. They deserve to see the words, not simply the initials. A good rule is to start your article by writing out names in full, and then, later, when your readers have got their bearings, to shorten them.

—Strunk and White, *The Elements of Style*

CHAPTER 2: Abbreviations

Abbreviations can be acronyms, shortenings, brevity codes, or organizational designators. This chapter treats them all generally as abbreviations.

To Use or Not To Use

Abbreviations can simplify presentation in a document, but too many of them make reading and understanding difficult. Readers are faced with a code known to the writer but unfamiliar or unknown to them—a source of irritation at best, but frequently an obstruction to communication. For this reason you should use abbreviations sparingly and only when you can be sure their meaning is clear for your readers.

Even in tables and graphics, where space is a consideration, avoid abbreviating unless the full terms will not fit. Changes in layout or type point size may preclude using abbreviations.

Common sense dictates these rules:

- Use an abbreviation only if it will simplify a document. Just because an abbreviation exists is not justification for using it. Establishing an abbreviation and then using it only once seldom justifies forcing readers to translate your abbreviations. If you are not going to repeat an abbreviation frequently, do not use it.

  Also, keep in mind that making use of context in a paper may eliminate the need to establish an abbreviation when the abbreviation will not be needed repeatedly. Consider the following example:

  > Infrastructure modifications were evident in the Very Important Military District (VIMD), consistent with the VIMD's high priority in defense planning.

  Establishing "VIMD" appears to be justified: the abbreviation will replace four words (a reasonable saving), and clearly the abbreviation is going to be used again, since it appears again in the same sentence. However, in this case rewording the sentence to make use of the context the sentence already establishes will eliminate the need for establishing the abbreviation:

  > Infrastructure modifications were evident in the Very Important Military District, consistent with that district's high priority in defense planning.

- Limit your use of abbreviations to appropriate places. Avoid using all but the most common abbreviations in key judgments or executive summaries, titles and headings, and tables of contents.
- Avoid using an abbreviation for a person's name. For example, refer to Kim Jong Un on secondary reference as Kim, not KJU.

When To Introduce an Abbreviation

Common wisdom says to introduce an abbreviation with the first occurrence of the corresponding term in a document. Taken literally, this leads to unnecessary abbreviations in key judgments and summaries and frequently results in an abbreviation's being introduced long before its next occurrence.

The best time to introduce an abbreviation is the first time you use the corresponding term in a portion of a document in which the abbreviation will appear frequently.

For example, a product dealing with military capabilities often discusses a force's organization—showing relationships among a number of subordinate entities in the force structure—and then each of the subordinate entities. If the writer introduces abbreviations for the entities in the discussion of the hierarchy, readers may be faced with 10 to 20 abbreviations in a few sentences. Expecting readers to absorb those abbreviations and recognize them later is unreasonable. The writer would do better to introduce each abbreviation in the discussion of the subordinate entity, when the abbreviation will reappear shortly after its introduction.

Occasionally readers are more familiar with an abbreviation than they are with the abbreviated term. For example, in a discussion of special forces, readers are more likely to recognize *SEAL* than the full term *sea/air/land* (which communicates little without further explanation). In such a case, use the abbreviation for clarity.

Establishing Abbreviations

The most common way of introducing an abbreviation is to state the full term and then, immediately after it, to include the abbreviation in parentheses.

A motorized rifle division (MRD) reportedly....
The Federal Aviation Administration (FAA)....

When an abbreviation is better known than the term itself, you may want to reverse their positions, placing the term in parentheses after the abbreviation. This may be the case if the abbreviation is derived from the initial letters of a foreign term rather than the English translation.

The Cuban FAR (Revolutionary Armed Forces)....
During operations in Chechnya, Russia's GRU (General Staff Main Intelligence Directorate) ensured....
Subordinate to Algeria's Ministry of National Defense is its Department of Intelligence and Security, or DRS (*Departement de Renseignement et de Securite*).

Sometimes you may need to establish an abbreviation more than once in a document:

- In a long document, when a large amount of text intervenes between the introduction (and first repeated use) of the abbreviation and later repeated use of the same abbreviation.
- In a collection of articles. Because readers often look at only some of the articles or read them in an order different from that of the publication that collects them, abbreviations do not carry over well from article to article. You will need to establish necessary abbreviations in each article, independent of the use of the same abbreviations in other articles.

Forming and Using Abbreviations

Capitalization

Capitalization in an abbreviation does not indicate that the words of the corresponding term also must be capitalized. Capitalize the initial letters of appropriate words in the related term if they are proper nouns, and use lowercase for the words if they are common nouns.

The aircraft returned to Argut Naval Air Station (NAS).
The aircraft returned to the naval air station (NAS).

Authors frequently become confused about capitalization when they write about operational systems. The test still is whether the term is being used as a proper noun or only as a generic term.

The American Multiple-Launch Rocket System (MLRS) differs from other multiple rocket launchers (MRLs).

Capitalization also is an issue in establishing abbreviations. For years two different systems for establishing abbreviations have existed side by side—a situation that sometimes causes confusion. One system capitalizes only letters for important words, leaving those for unimportant words like *of* in lowercase form. The other system capitalizes all the letters in the abbreviation, whether they stand for important or unimportant words.

- Today the predominant system is to use capitals for all the letters in an abbreviation. If you establish an abbreviation in an intelligence product, use capital letters throughout the abbreviation.

Nevertheless, well-established legacy abbreviations with some lowercase letters, such as *DoD* for the U.S. Department of Defense, are still in use today while similar abbreviations, such as *DOE* for Department of Energy, have all uppercase letters.

Italics With Abbreviations

An abbreviation formed from a foreign term is not italicized, though the foreign term may be. Normally you will not italicize the original language or English translation of names of foreign organizations, institutes, governmental bodies, political parties, educational institutes, corporations, Internet service providers, and the like, because our business—assessing intelligence information dealing with foreign governments and their defense and security organizations—uses numerous foreign terms as a part of our writing. However, if you are providing the original language words to explain the formation of an abbreviation, italics are appropriate for the foreign words.

Russia's Spetsnaz (from *voiska spetsialnogo naznacheniya*, or "troops of special designation") had special missions.

Subordinate to Algeria's Ministry of National Defense is its Department of Intelligence and Security, or DRS (*Departement de Renseignement et de Securite*).

Periods in Abbreviations

Very few abbreviations require periods. The exceptions are the traditional nonmilitary ranks or titles (*Mr., Mrs., Ms., Dr., Prof.*) and *no.* (for "number," to distinguish it from the answer or command *no*). In addition, use periods with *U.S.* The abbreviations *i.e.* ("that is") and *e.g.* ("for example") also require periods; however, many people confuse these abbreviations, so using them is discouraged.

Plural and Singular Abbreviations

Most abbreviations are established in the singular form. Therefore, when you introduce (or use) an abbreviation, pay attention to whether the term is singular or plural. If the term is singular, the abbreviation should be as well; if the term is plural, the abbreviation usually will have to be changed to make it plural.

... earth-penetrator weapons (EPWs).

... within the military regions (MRs).

SA-7 and SA-14 surface-to-air missiles (SAMs) are among the world inventory of shoulder-fired SAMs.

Particularly for military forces, an abbreviation often equates to a plural thing—for example, "ANDSF" for "Afghan national defense and security forces." However, usually the abbreviation itself, after it is established, is singular and requires a singular verb.

Afghan national defense and security forces (ANDSF) continue to improve their ability....

Here the subject *Afghan national defense and security forces* requires a plural verb (*continue*) and a plural pronoun (*their*). Thus, "ANDSF" represents a plural entity. Nevertheless, when *ANDSF* itself is used as a subject, the abbreviation is singular and requires a singular verb and singular pronoun:

However, the ANDSF is not yet prepared to hold its own in....

Forming Plurals of Abbreviations

When an abbreviation ends in an uppercase letter, form the plural by adding a lowercase *s*, without an apostrophe.

ICBMs SAMs MiGs INSs

However, if the abbreviation ends in lowercase letters, form the plural by adding *'s* (apostrophe + lowercase *s*).

cy's

These are rare in general military intelligence writing but sometimes occur in scientific or technical publications. Do not confuse them with plurals of lowercase abbreviations for units of measure, which are not changed to plural form.

not 500 km's *or* 500 kms *but* 500 km

Furthermore, even though an abbreviation may stand for an entity that we know to consist of many people, references to the abbreviation cannot be the pronouns *they* or *their*. This problem occurs frequently in intelligence writing in discussion of a political party or organization (which obviously is a group of people):

Not: The CCP decided to implement their decisions after....
But: The CCP decided to implement its decisions after....

When the abbreviation is used instead as a modifier for a plural noun—for example, in *CCP members*—the abbreviation no longer determines the number, so a plural pronoun reference is appropriate to refer to the plural noun:

The CCP members decided to implement their decisions after....

Because of what they stand for, a few abbreviations are only plural. When it stands for "tactics, techniques, and procedures," *TTP* is one of these. Because *TTP* in this sense is plural, we cannot write "A new TTP proved successful." Instead, we would need to write "A new tactic [or technique, or procedure] proved successful."

Possessives and Abbreviations

As with the terms they represent, most abbreviations can be used in the possessive form. If the abbreviation is being used as a singular possessive, add an apostrophe and a lowercase s. If the application requires a plural possessive, add the apostrophe after the lowercase s that forms the plural of the abbreviation.

Singular possessive: The MRD's leaders....
Plural possessive: The MRDs' leaders....

Generally the adjective form of the abbreviation is preferable; it can be substituted for both the singular and plural possessive forms:

Adjective form: The MRD leaders....

When you introduce an abbreviation, avoid establishing it in its possessive form. Usually you can avoid that situation by using the abbreviation as an adjective, or you can put the abbreviation in a prepositional phrase. However, if you do establish an abbreviation when the words for it are in the possessive form, the abbreviation also needs to appear in the possessive form.

Avoid: The Royal Air Force's (RAF's) aircraft....
Use: The Royal Air Force (RAF) aircraft....
Or: The aircraft of the Royal Air Force (RAF)....

Prefixes and Suffixes With Abbreviations

You can join a prefix or suffix to an abbreviation with a hyphen. Do not capitalize the prefix or suffix unless it indicates a proper noun form.

anti-NATO stance
pro-UN position
CFE-mandated reductions
START-related reforms

However, the participial and negative forms of *MIRV* are formed without hyphens:

a MIRVed ICBM
an unMIRVed version of the ICBM
deploying nonMIRVed missiles

Hyphenation When Introducing Abbreviations

When you need to form a multiple-word compound at the same time you are introducing an abbreviation, hyphenate after the parentheses enclosing the abbreviation.

interference with Global Positioning System (GPS)-related technology

If possible, avoid a construction such as this by restructuring the passage: in this case, for example, with "interference with technology related to the Global Positioning System (GPS)."

Articles Accompanying Abbreviations

Depending on how you use an abbreviation in a sentence, a definite article (*the*) or an indefinite one (*a* or *an*) may need to precede the abbreviation. If you would use *the* in front of the term the abbreviation stands for, you usually will need *the* in front of the abbreviation.

The surface-to-air missile was fired....
The SAM was fired....

The ground-controlled intercept operator chooses....
The GCI operator chooses....

Task Force Marte reported....
TFM reported....

Use of *the* with abbreviations is not a hard-and-fast rule, but be aware of common practice. Particularly for organization names, *the* is used with abbreviations pronounced as individual letters (initialisms) more often than with abbreviations pronounced as words (acronyms), especially multisyllable words. For instance, *the* is generally used with *the CMC* and *the FARC* but not with *AMISOM*, *NATO*, and *ISAF*.

For abbreviations representing Intelligence Community and Defense Intelligence Enterprise agencies and organizations (DIA, NSA, CIA, NGIC, etc.) and the combatant commands (USCENTCOM, etc.), delete *the* from in front of the abbreviation for general intelligence writing, including most correspondence.

DIA estimates....
... coordination with CIA, NSA, and USSTRATCOM.

Deleting *the* from in front of an abbreviation also is appropriate for the abbreviation representing the organization of which the writer is a part. For example, an author who is a member of DIA's Directorate for Analysis (DI) could write something like the following:

When dealing with Defense Intelligence Enterprise organizations, DI will....

Using *a* or *an* with abbreviations is trickier. For an abbreviation, including an acronym or letter/number group, pronounced as a word (such as "HOT" and "IMINT"), use *a* if the abbreviation begins with a consonant sound or an aspirated *h* ("a HOT missile") and *an* if the abbreviation begins with a vowel sound ("an IMINT collector"). For abbreviations for which you pronounce the letters and numbers themselves:

- Use *a* when the group begins with *b*, *c*, *d*, *g*, *j*, *k*, *p*, *q*, *t*, *u*, *v*, *w*, *y*, or *z*: "a DIA employee," "a UN worker."
- Use *an* when the group begins with *a*, *e*, *f*, *h*, *i*, *l*, *m*, *n*, *o*, *r*, *s*, or *x*: "an NSC directive," "an SS-25 missile," "an Su-24 aircraft."

A or An?

When choosing between using *a* or *an* with an abbreviation, consider the abbreviation itself, not an expansion of the abbreviation. For example, for discussion of a frequency-hopping (FH) radar, because we would pronounce the letters of the abbreviation, we would write "an FH radar," as *an* is appropriate before an abbreviation beginning with *f*; we would not choose "a FH radar" even though *a* would be appropriate before "frequency."

Avoiding Redundancy

You have to consider the expansion of an abbreviation when deciding what words can follow it. Be careful to avoid redundancy when you use abbreviations.

AC current = alternating current current
START treaty = Strategic Arms Reduction Treaty treaty
LOC lines = lines of communication lines
AWACS system = airborne warning and control system system
CAC card = common access card card

Nix GOx Abbreviations

Avoid using abbreviations like *GOP* for "government of Pakistan [or Panama, Peru, Paraguay, etc.]" in a finished intelligence product. Abbreviations such as this are useful in message traffic and similar reporting, but they are out of place in finished intelligence products, especially those for senior-level customers.

Country Names

Use what *The World Factbook* calls the conventional short form for a country name (rather than the conventional long form): "China" rather than "People's Republic of China," "North Korea" rather than "Democratic People's Republic of Korea," "South Korea" rather than "Republic of Korea," etc. Congo is a bit more complicated because of the need to distinguish between the two countries. For the Democratic Republic of the Congo, establish the abbreviation "DRC," which *The World Factbook* lists as the conventional short form for the country's name; "Congo (Kinshasa)" also is acceptable. For the Republic of the Congo, *The World Factbook* provides "Congo (Brazzaville)" as the conventional short form.

Spell out most country names, whether you use them as nouns or adjectives—except the United States, the United Kingdom, and the United Arab Emirates. Spell out *United States* and *United Kingdom* (and *United Nations*) when you use them as nouns, but use the abbreviations for the adjective forms. If you need multiple references to the United Arab Emirates, establish *UAE* early in a paper.

The United States sold....
U.S. arms sales....
... contracts involving the United Kingdom.
... UK contracts.

Military Rank/Rate

For members of the U.S. military, use rank/rate abbreviations as the individual Military Services use them. For all militaries, use the abbreviation in front of a name, but spell out the rank in lowercase elsewhere: "Maj Gen Gonzales of the Mexican Air Force plans to visit shortly after his promotion to lieutenant general." Also spell out the rank in plural form: "Captains Arroyo and Valdez."

U.S. Army Officers/Warrant Officers

general of the Army (special)	GA
general (O-10)	GEN
lieutenant general (O-9)	LTG
major general (O-8)	MG
brigadier general (O-7)	BG
colonel (O-6)	COL
lieutenant colonel (O-5)	LTC
major (O-4)	MAJ
captain (O-3)	CPT
first lieutenant (O-2)	1LT
second lieutenant (O-1)	2LT

chief warrant officer 5 (W-5)	CW5
chief warrant officer 4 (W-4)	CW4
chief warrant officer 3 (W-3)	CW3
chief warrant officer 2 (W-2)	CW2
warrant officer 1 (W-1)	WO1

U.S. Navy and Coast Guard Officers/Warrant Officers

fleet admiral (special)	FADM
admiral (O-10)	ADM
vice admiral (O-9)	VADM
rear admiral, upper half (O-8)	RADM
rear admiral, lower half (O-7)	RDML
captain (O-6)	CAPT
commander (O-5)	CDR
lieutenant commander (O-4)	LCDR
lieutenant (O-3)	LT
lieutenant, junior grade (O-2)	LTJG
ensign (O-1)	ENS
chief warrant officer (W-5)	CWO5
chief warrant officer (W-4)	CWO4
chief warrant officer (W-3)	CWO3
chief warrant officer (W-2)	CWO2
warrant officer (W-1) [no longer used]	WO1

U.S. Air Force Officers

general of the Air Force (special)	GOAF
general (O-10)	Gen
lieutenant general (O-9)	Lt Gen
major general (O-8)	Maj Gen
brigadier general (O-7)	Brig Gen
colonel (O-6)	Col
lieutenant colonel (O-5)	Lt Col
major (O-4)	Maj
captain (O-3)	Capt
first lieutenant (O-2)	1st Lt
second lieutenant (O-1)	2nd Lt
[U.S. Air Force does not have warrant officers]	

U.S. Marine Corps Officers/Warrant Officers

general (O-10)	Gen
lieutenant general (O-9)	LtGen
major general (O-8)	MajGen
brigadier general (O-7)	BGen
colonel (O-6)	Col
lieutenant colonel (O-5)	LtCol
major (O-4)	Maj
captain (O-3)	Capt
first lieutenant (O-2)	1stLt
second lieutenant (O-1)	2ndLt
chief warrant officer 5 (W-5)	CWO5
chief warrant officer 4 (W-4)	CWO4

chief warrant officer 3 (W-3)	CWO3
chief warrant officer 2 (W-2)	CWO2
warrant officer 1 (W-1)	WO

U.S. Army Enlisted Personnel

sergeant major of the Army (E-9)	SMA
command sergeant major (E-9)	CSM
sergeant major (E-9)	SGM
first sergeant (E-8)	1SG
master sergeant (E-8)	MSG
sergeant first class (E-7)	SFC
staff sergeant (E-6)	SSG
sergeant (E-5)	SGT
corporal (E-4)	CPL
specialist (E-4)	SPC
private first class (E-3)	PFC
private (E-2)	PV2
private (E-1)	PVT

U.S. Navy and Coast Guard Enlisted Personnel

U.S. Navy and Coast Guard enlisted personnel are identified by paygrade (rate) and occupational specialty (rating). These specialties and their combinations with rates are too numerous to list here. For ratings, see NIPRNET <http://www.navy.mil/navydata/nav_legacy.asp?id=259>. Rates are as follows:

master chief petty officer of the Navy (E-9)	MCPON
master chief petty officer of the Coast Guard (E-9)	MCPOCG
fleet/force/command master chief petty officer (E-9)	FLTCM/FORCM/CMDCM
master chief petty officer (E-9)	MCPO
senior chief petty officer (E-8)	SCPO
chief petty officer (E-7)	CPO
petty officer first class (E-6)	PO1
petty officer second class (E-5)	PO2
petty officer third class (E-4)	PO3
seaman (E-3)	SN
seaman apprentice (E-2)	SA
seaman recruit (E-1)	SR

U.S. Air Force Enlisted Personnel

chief master sergeant of the Air Force (E-9)	CMSAF
command chief master sergeant (E-9)	CCM
first sergeant (E-9)	CMSgt
chief master sergeant (E-9)	CMSgt
first sergeant (E-8)	SMSgt
senior master sergeant (E-8)	SMSgt
first sergeant (E-7)	MSgt
master sergeant (E-7)	MSgt
technical sergeant (E-6)	TSgt
staff sergeant (E-5)	SSgt
senior airman (E-4)	SrA
airman first class (E-3)	A1C
airman (E-2)	Amn
basic airman (E-1)	AB

U.S. Marine Corps Enlisted Personnel

sergeant major of the Marine Corps (E-9)	SgtMajMC
sergeant major (E-9)	SgtMaj
master gunnery sergeant (E-9)	MGySgt
first sergeant (E-8)	1stSgt
master sergeant (E-8)	MSgt
gunnery sergeant (E-7)	GySgt
staff sergeant (E-6)	SSgt
sergeant (E-5)	Sgt
corporal (E-4)	Cpl
lance corporal (E-3)	LCpl
private first class (E-2)	PFC
private (E-1)	Pvt

Foreign Military Officers

For foreign military officers, regardless of branch of service, use the following abbreviations for ranks:

admiral	Adm
admiral (first grade)	Adm (1st Grade)
admiral of the fleet	Adm Flt
admiral (second grade)	Adm (2nd Grade)
air chief marshal	Air CMar
air commander	Air Cdr
air commodore	Air Como
air marshal	Air Mar
air vice marshal	Air VMar
army general	Army Gen
brigadier	Brig
brigadier general	Brig Gen
captain	Capt
captain first rank	Capt 1st Rank
captain second rank	Capt 2nd Rank
chief warrant officer	CWO
colonel	Col
colonel general	Col Gen
colonel major	Col Maj
commander	Cdr
commodore	Como
corps general	Corps Gen
director general	Dir Gen
division general	Div Gen
ensign	Ens
field marshal	Fld Mar
first lieutenant	1st Lt
fleet admiral	Flt Adm
flight lieutenant	Ft Lt
flying officer	FO
general	Gen
general-colonel	Gen-Col
general (first grade)	Gen (1st Grade)

general-lieutenant	Gen Lt
general-lieutenant colonel	Gen-Lt Col
general-major	Gen Maj
general of the air force	Gen AF
general of the army	Gen Army
general (second grade)	Gen (2nd Grade)
group captain	Grp Capt
lieutenant	Lt
lieutenant colonel	Lt Col
lieutenant colonel general	Lt Col Gen
lieutenant commander	LCdr
lieutenant general	Lt Gen
lieutenant junior grade	Ltjg
major	Maj
major general	Maj Gen
marshal	Mar
marshal of aviation	Mar Avn
marshal of the Royal Air Force	Mar RAF
marshal of the Soviet Union	MSU
pilot officer	PO
rear admiral	RAdm
second lieutenant	2nd Lt
senior colonel	Sr Col
senior lieutenant colonel	Sr Lt Col
squadron leader	Sq Ldr
squadron vice admiral	Sq VAdm
staff air marshal	Staff Air Mar
staff air vice marshal	Staff Air VMar
staff brigadier general	Staff Brig Gen
staff general	Staff Gen
staff lieutenant general	Staff Lt Gen
staff major general	Staff Maj Gen
staff rear admiral	Staff RAdm
vice admiral	VAdm
vice marshal	VMar
warrant officer	WO
wing commander	Wg Cdr

Units of Measure

Do not abbreviate a unit of measure used in a general or approximate (dataless) sense.

Ranges are in kilometers.

The opening was several meters wide.

As a general rule, write out the units of measure in text when presenting nouns, but abbreviate the units of measure in the adjective form. In tables, abbreviations are appropriate for all units of measure because of space limitations. Abbreviations for units of measure do not have periods and are not changed to plural form. Unit modifiers involving units of measure require hyphens. (For a full explanation of unit modifiers, see Chapter 7; for complete coverage of number usage, see Chapter 4.)

a 50-km road segment
a section of road that stretched 50 kilometers
a 500-NM range
a 3-cm-diameter pipe

Because of the risk of ambiguity, avoid single-letter abbreviations (*g, h, m, L, t, V, W*).

Change:	a segment of 300 m on Route A
To:	a 300-meter segment on Route A
Or:	a Route A segment of 300 meters

Some offices have preferred to use *mt* or *MT* for metric ton(s). These abbreviations, however, present problems.

- As a prefix, *m* equates to "milli," and t is the symbol for metric ton(s), making *mt* equate to "milli-metric ton(s)," which is somewhat nonsensical.
- In addition, using *mt* or *MT* invites confusion with *Mt*, which equates to "megaton(s)."

For these reasons, we need to use the international symbol of t for metric ton(s), even though this abbreviation has only a single character. Of course, using the words *metric ton* or *metric tons* avoids the abbreviation issue.

Percent and Other Symbols

Do not abbreviate or use the symbol for *percent* except to save space in tables or graphics, where the symbol % may be used if required. However, even in these cases do not abbreviate unless the term will not fit. Similarly, do not use symbols such as ~ (*about* or *roughly*), < (*less than*), or > (*greater than*) unless the spelled-out term will not fit. In tables where symbols are appropriate, minimize clutter by putting symbols in column headings if possible, rather than in individual cells.

Months and Days

Do not abbreviate the names of months and days except to save space in tables and graphics. However, even in these cases do not abbreviate unless the full terms will not fit.

Use the following abbreviations if they are required:

Days		*Months*	
Sunday	Sun	January	Jan
Monday	Mon	February	Feb
Tuesday	Tue	March	Mar
Wednesday	Wed	April	Apr
Thursday	Thu	May	May
Friday	Fri	June	Jun
Saturday	Sat	July	Jul
		August	Aug
		September	Sep
		October	Oct
		November	Nov
		December	Dec

Abbreviation List

The list that follows contains abbreviations for use in DIA intelligence products. This list is included for standardization of preferred usage, to show uppercase and lowercase forms, and to permit marking abbreviations that may be used without being introduced in the text of a product. This list does not preclude use of the *Department of Defense Dictionary of Military and Associated Terms* and Intellipedia's "Acronyms" page, which present many abbreviations not covered here.

The following abbreviation list sometimes shows multiple uses for the same abbreviation, and all of them can be considered "preferred" abbreviations. Common sense, however, indicates that you cannot use the same abbreviation for multiple purposes in the same paper. For example, even though *BW* can stand for either "biological warfare" or "biological weapon," it must not stand for both things in the same piece of writing.

The abbreviation list employs two symbols:

- A superscript dagger symbol (†) marks an abbreviation that should be used instead of the words the abbreviation stands for. Very few abbreviations show this marking.
- An asterisk (*) after an abbreviation indicates that you can use the abbreviation without introducing it if you can be certain that intended users of a product will understand the abbreviation. When you have any doubt about whether your consumers will understand an abbreviation, spell out the term on first use in your publication, even if the abbreviation is marked with an asterisk in the following list.

Caution: Because a production element has been reading numerous bits of information that use an abbreviation and analysts from that element are writing a number of papers using an abbreviation, analysts frequently believe that surely everyone else must be familiar with the abbreviations they commonly see and use. However, for perspective, consider the following: The Free Dictionary, on the Internet at <http://www.thefreedictionary.com>, has an "Acronym Finder" that lists expansions for letter sets, and it includes military expansions among the many possible "translations" for an abbreviation. As of 1 December 2015, this website produced 43 expansions for "PTG," one of which equated to the expansion in our listing; 191 expansions for "SSP," none of them matching the one in our listing; and 105 for "ADA," one of which was the one in our listing. For this reason, we need to be careful when deciding whether to establish an abbreviation. Do not consider an asterisk with an abbreviation to be a license to never establish the abbreviation.

- Correspondence going to high-level customers normally will need to have all abbreviations established. For example, the personnel directly supporting the DIA Command Element usually require that all abbreviations be established for papers going to or through members of the Command Element. High-level customers receive large numbers of documents and have little time to review any of them. They are generalists for many subjects, not subject matter experts. Even though they may have been exposed to abbreviations Defense Intelligence analysts commonly see and use, expecting these high-level customers to remember all the abbreviations analysts are capable of using simply is not realistic.
- As an experienced editor in one of the Agency's scientific and technical intelligence production centers has noted, basic documents produced in the centers frequently go to inexperienced customers as well as to those who might be familiar with abbreviations. Establishing most abbreviations in basic intelligence products, therefore, is both a courtesy and a wise course of action.
- You can never go wrong by establishing an abbreviation, whereas not establishing it may cause problems.

A

Å	angstrom(s)
AA*	antiaircraft
AAB	Abdallah Azzam Brigades
AAA*	antiaircraft artillery
AAH	Asaib Ahl al-Haq
AAI	air-to-air intercept
AAIED	antiarmor improvised explosive device
AAM*	air-to-air missile
AAR	air-to-air refueling
AAS	Ansar al-Sharia
AAS-T	Ansar al-Sharia in Tunisia
AAW	antiair warfare
AB*	airbase [in the proper name of a U.S. OCONUS airbase, Air Base—for example, Incirlik Air Base]
ABCCC	airborne battlefield command and control center
ABM*	antiballistic missile
abn	airborne
ABNCP	airborne command post
AC	alternating current
acft	aircraft
ACI	airborne-controlled intercept
ACIC	Army Counterintelligence Center
ACINT	acoustic intelligence
ACP	alternate command post
ACR	armored cavalry regiment
ACRV	armored command and reconnaissance vehicle; artillery command and reconnaissance vehicle
ACV	air-cushion vehicle; armored combat vehicle
ACW	aircraft warning and control; anticarrier warfare
AD	air defense
ADA	air defense artillery
ADATS	air defense antitank system
ADCC	air defense command center
ADD	air defense district
ADF	automatic direction finding
ADG	degaussing/deperming ship
ADIZ	air defense identification zone
ADOC	air defense operations center
adv	advanced
ADX	air defense exercise
ADZ	air defense zone
AE	ammunition ship
AESA	active electronically scanned array
AEV	armored engineer vehicle
AEW	airborne early warning
AEW&C	airborne early warning and control
AF	stores ship
AFB*	air force base
AFC	automatic frequency control
AFDM	medium auxiliary floating drydock (non-self-propelled)
AFIAA	Air Force Intelligence Analysis Agency
AFIOC	Air Force Information Operations Center
AFISRA	Air Force Intelligence, Surveillance and Reconnaissance Agency
afld	airfield
AFMIC	Armed Forces Medical Intelligence Center [now NCMI—National Center for Medical Intelligence]
AFOSI	Air Force Office of Special Investigations
AFOTEC	Air Force Operational Test and Evaluation Center

AFS	combat stores ship
AFSATCOM	Air Force Satellite Communications System
AFTAC	Air Force Technical Applications Center
AFV	armored fighting vehicle
AG	Australia Group; auxiliary general [ship]
AGB	icebreaker
AGE	experimental auxiliary [ship]
AGI	intelligence collection ship
AGOR	oceanographic research ship
AGOS	ocean surveillance ship
AGS	surveying ship
AGZ	actual ground zero
AH	hospital ship
AI	avian influenza; airborne intercept; air interdiction
AIAI	al-Ittihad al-Islamiya
AICV	armored infantry combat vehicle
AIDS*	acquired immunodeficiency syndrome
AIFV	armored infantry fighting vehicle
AIG	addressee indicator group
AIM	air-intercept missile
AIP	air-independent propulsion/ power; air-independent-powered
AIS	automated information system; Automatic Identification System
AIT	American Institute in Taiwan
AK	cargo ship
aka*	also known as
ALCM*	air-launched cruise missile
ALOC	air line of communication
ALRAAM	air-launched long-range air-to-air missile
AM*	ante meridian (before noon); amplitude modulation
AMB	ambassador
AMC	Air Mobility Command [USAF]
AMEMB	American Embassy [U.S. Embassy preferred]
AMISOM	African Union Mission in Somalia
AMR	antimateriel rifle
AMRAAM	advanced medium-range air-to-air missile
ANA	Afghan National Army
ANC	African National Congress; active noise control
ANCOP	Afghan National Civil Order Police
ANDS	Afghanistan national development strategy
ANP	Afghan National Police
ANDSF	Afghan national defense and security forces [formerly ANSF—Afghan national security forces]
ANZUS	Australia-New Zealand-United States [Treaty]
AO	area of operations; oiler
AOB	air order of battle
AOC	air operations center
AOE	fast combat support ship
AOG	gasoline tanker
AOI	area of interest
AOR	area of responsibility; replenishment oiler
AOS	special liquids tanker
AOT	transport oiler
AP	armor-piercing; ammonium perchlorate; access point; transport [ship]
APC*	armored personnel carrier
APEC	Asia-Pacific Economic Cooperation

APOD	aerial point of debarkation; air point of departure
AQ	al-Qaida
AQAP	al-Qaida in the Arabian Peninsula
AQI	al-Qaida in Iraq [now known as Islamic State of Iraq and the Levant (ISIL)]
AQIM	al-Qaida in the Lands of the Islamic Maghreb
AQIS	al-Qaida in the Indian Subcontinent
AR	repair ship
ARABSAT	Arab Satellite Communications Organization
ARC	armored reconnaissance carrier; cable repairing ship
ARENA	Nationalist Republican Alliance [El Salvador]
ARM	antiradiation missile
ARPV	advanced remotely piloted vehicle
ARS	salvage ship
arty	artillery
ARV	armored recovery vehicle; armored reconnaissance vehicle
AS	submarine tender
ASAP*	as soon as possible
ASARS	advanced synthetic-aperture radar system
ASAT	antisatellite
ASBM	antiship ballistic missile
ASCM*	antiship cruise missile
ASDS	advanced SEAL/swimmer delivery system
ASDV	auxiliary SEAL/swimmer delivery vehicle
ASEAN	Association of Southeast Asian Nations
ASF	African Standby Force
ASG	Abu Sayyaf Group
ASL	above sea level
ASM	air-to-surface missile
ASR	alternate supply route; submarine rescue ship
ASRAAM	advanced short-range air-to-air missile
ASROC	antisubmarine rocket
ASSW	antisurface ship warfare
ASUW	antisurface warfare
ASV	armored support vehicle
ASW*	antisubmarine warfare
AT	antitank; antiterrorism
ATA	auxiliary ocean tug
ATACMS	Army Tactical Missile System
ATBM	antitactical ballistic missile
ATC	air traffic control; mini-armored troop carrier
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives; fleet ocean tug
ATG	antitank gun
ATGM*	antitank guided missile
AT&L	Acquisition, Technology, and Logistics
ATM	asynchronous transfer mode
ATTU	Atlantic-to-the-Urals [region]
ATV	advanced technology vehicle; all-terrain vehicle
AU	African Union
AUV	autonomous underwater vehicle
AV	armored vehicle
AVB	aviation logistic support ship
AVLB	armored-vehicle-launched bridge
AWACS*	airborne warning and control system
AWOL*	absent without leave
AWT	water transport [ship]
AWX	all-weather

AX	miscellaneous auxiliary [ship]
AXT	training ship

B

b	barrel(s)
BACRIM	criminal band [from *banda criminal*]
BAG	battalion artillery group
BAI	battlefield air interdiction
bcm	billion cubic meters
b/d*	barrel(s) per day
BDA	battle damage assessment
bde	brigade
BE*	Basic Encyclopedia
BENELUX	Belgium, Netherlands, Luxembourg
BGN	Board on Geographic Names
b/h	barrel(s) per hour
BICES	Battlefield Information Collection and Exploitation System
BINUB	United Nations Integrated Office in Burundi
BIOS	basic input/output system
bit/s	bit(s) per second
bldg	building
BLOS	beyond line of sight
BLT	battalion landing team
BMD	ballistic missile defense
BMDS	ballistic missile defense system
BMEWS	ballistic missile early warning system
bn	battalion
BOA	broad ocean area
BONUCA	United Nations Peacebuilding Support Office in the Central African Republic
BRAC	Base Realignment and Closure
BRICS	Brazil, Russia, India, China, and South Africa
BTADS	Border Tunneling Activity Detection System
btry	battery
bu	bushel(s)
BVR	beyond visual range
BW	biological warfare; biological weapon
BWC	Biological Weapons Convention

C

C*	Celsius
C2*	command and control
C3*	command, control, and communications
C4*	command, control, communications, and computers
C3CM	command, control, and communication countermeasures
C3I*	command, control, communications, and intelligence
C4I*	command, control, communications, computers, and intelligence
C4ISR*	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAA	combined-arms army
CAC*	common access card
CACM	Central American Common Market
CAG	carrier air group
cal*	caliber
CANUKUS	Canada-United Kingdom-United States

CANUS	Canada-United States
CAP	combat air patrol
CAPCO	[former] Controlled Access Program Coordination Office [see SMP]
CARICOM	Caribbean Community
CAS	close air support
cav	cavalry
CBD	chemical and biological defense
CBM	confidence-building measure
CBR	chemical, biological, and radiological
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and explosives
CBU	cluster bomb unit
CBW	chemical and biological warfare; chemical and biological weapon
CC	command center; command ship
CCB	command and control boat
CCD	camouflage, concealment, and deception; charge-coupled device
CCIR	commander's critical information requirement
CCM	counter-countermeasure
CCMD	combatant command [see COCOM]
CCP	Chinese Communist Party
CCTV	closed-circuit television; China Central Television
CD*	compact disc
CDC	Centers for Disease Control and Prevention
CDCM	coastal defense cruise missile
CDI	Chief of Defence Intelligence [Canada]
CD-R	recordable compact disc
CD-ROM*	compact disc–read-only memory
CD-RW	rewriteable compact disc
CECOM	Communications and Electronics Command
CENTAM	Central America
CEP	circular error probable
CERT	computer emergency response team
CFE	Conventional Armed Forces in Europe
CFV	cavalry fighting vehicle
cg*	centigram(s)
CG	guided-missile cruiser; coast guard [or Coast Guard]
CGN	nuclear-powered guided-missile cruiser
CGS	common ground station
CH	aviation cruiser
CHG	guided-missile aviation cruiser
CHOD	chief of defense
CHOP	change of operational control
CI	counterintelligence
CIA*	Central Intelligence Agency
CIA/CNC	Central Intelligence Agency Crime and Narcotics Center
CIC	combat information center; combat intelligence center
CICA	Conference on Interaction and Confidence-Building Measures in Asia
CIG	Consolidated Intelligence Guidance
CINC	commander in chief
CIOC	Combined Intelligence Operations Center

CIS	Commonwealth of Independent States
CISP	Counterintelligence Support Program
CIWS	close-in weapon system
CJCS*	Chairman of the Joint Chiefs of Staff
CKO	core knowledge online
CL	light cruiser
CLOS	command to line-of-sight
cm*	centimeter(s)
cm2*	square centimeter(s)
cm3*	cubic centimeter(s)
CMC	Central Military Commission [China]
CMF	Cyber Mission Force
CN	counternarcotics
CNA	computer network attack
CNCI	Comprehensive National Cybersecurity Initiative
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations; Chief of Naval Operations
co	company
CO	commanding officer
COA	course of action
COC	combat operations center
COCOM	combatant command (common usage) [*Note*: The *Department of Defense Dictionary of Military and Associated Terms* reserves *COCOM* for the command authority of a combatant command, using *CCMD* as the abbreviation for combatant command.]
CODEL	congressional delegation
COG	combined operations group; center of gravity
COI	community of interest
COIN	counterinsurgency
COLISEUM	Community Online Intelligence System for End Users and Managers
COMEX	communications exercise
COMINT*	communications intelligence
COMPUSEC	computer security
COMSAT	communications satellite
COMSEC*	communications security
CONOPS*	concept of operations
CONPLAN*	contingency plan; concept plan
CONUS*	continental United States
COOP	continuity of operations
COR	Council of Representatives [Iraq]; contracting officer representative
COTS	commercial off-the-shelf
CP	command post
CPA	Comprehensive Peace Agreement [Sudan]
CPU	central processing unit
CPX	command post exercise
CR	collection requirement
CRBM	close-range ballistic missile
CS	combat support
CSAR	combat search and rescue
CSBM	confidence- and security-building measure
CSG	carrier strike group
CSNP	nonpowered causeway section (non-self-propelled)
CSS	combat service support; Central Security Service [NSA—often shown as NSA/CSS]
CSTC-A	Combined Security Transition Command–Afghanistan
CSTO	Collective Security Treaty Organization

CSX	command and staff exercise
CTA	capstone threat assessment
CTBT	Comprehensive Test Ban Treaty
CTFI	counter-threat-finance intelligence
CTOL	conventional takeoff and landing
CV	multipurpose aircraft carrier
CVA	attack aircraft carrier
CVAN	nuclear-powered attack aircraft carrier
CVH	V/STOL aircraft carrier
CVL	light aircraft carrier
CVN	nuclear-powered multipurpose aircraft carrier
CVRT	tracked reconnaissance combat vehicle
CW	chemical warfare; chemical weapon; continuous wave
CWC	Chemical Weapons Convention
CWIED	command-wired improvised explosive device
CY*	calendar year
cy*	copy

D

DAO*	defense attaché office
DARPA	Defense Advanced Research Projects Agency
DATT*	defense attaché
dB*	decibel(s)
dBsm	decibel referenced to 1 square meter
DC	direct current
DCA	Defense Cooperation Agreement
DCHC	Defense Counterintelligence and HUMINT Center [now DIA Directorate for Operations]
DCI	Director of Central Intelligence [position no longer exists]
DCIPS	Defense Civilian Intelligence Personnel System
DCS	Defense Clandestine Service
DD	deputy director; destroyer
D&D	denial and deception
DDG	guided-missile destroyer
DDH	aviation destroyer (ASW)
DDNI/A	Deputy Director of National Intelligence for Analysis
DDNS	dynamic domain name system
DDoS	distributed denial of service
DDR	disarmament, demobilization, and reintegration
DDR&E	Directorate of Defense Research and Engineering; director, Defense Research and Engineering
DE	damage expectancy; directed energy
DEA*	Drug Enforcement Administration
DEFSMAC	Defense Special Missile and Aerospace Center
deg	degree(s)
DepSecDef	U.S. Deputy Secretary of Defense
dept	department
det	detachment
DEW	directed-energy weapon
DEXCOM	Intelligence Community Deputies Executive Committee
DF	direction finding
DGZ	desired ground zero

DHCP	dynamic host configuration protocol
DHKP/C	Revolutionary People's Liberation Party/Front
DHS	Department of Homeland Security
DI	Directorate for Analysis; Director for Analysis
DIA*	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center [now DIA Headquarters]
DIAD	Defense Intelligence Agency directive
DIAI	Defense Intelligence Agency instruction
DIAL	Defense Intelligence Agency Liaison Office
diam	diameter
DIAM	Defense Intelligence Agency manual
DIAP	Defense Intelligence Analysis Program
DIAR	Defense Intelligence Agency regulation
DID	*Defense Intelligence Digest*
DIO	defense intelligence officer; Defence Intelligence Organisation [Australia]
DIS	Defence Intelligence Staff [United Kingdom]
DISA	Defense Information Systems Agency
DISES	Defense Intelligence Senior Executive Service
DISL	Defense Intelligence Senior Level
div	division
DLO	Defense Liaison Office
DMPI	desired mean point of impact
DMS	Defense Message System
DMZ	demilitarized zone [use initial capitalization when spelling out a proper name, such as Korean Demilitarized Zone]
DNA*	deoxyribonucleic acid
DNI	Director of National Intelligence
DOB*	date of birth
DOC	Department of Commerce [or Commerce Department]
DOCEX	document exploitation
DoD*	Department of Defense [or Defense Department]
DoDD	Department of Defense directive
DoDIIS	Department of Defense Intelligence Information System
DoDM	Department of Defense manual
DoDR	Department of Defense regulation
DOE	Department of Energy [or Energy Department]
DOI	date of information; Department of Interior [or Interior Department]
DOJ	Department of Justice [or Justice Department]
DOMEX	document and media exploitation
DOS	Department of State [or State Department]
DoS	denial of service
DOT	Department of Transportation [or Transportation Department]
DOT&E	director of Operational Test and Evaluation
DPI	desired point of impact
DPP	diesel powerplant
DR	director

DRC	Democratic Republic of the Congo
DRFM	digital radiofrequency memory
DSCA	Defense Security Cooperation Agency
DSCS	Defense Satellite Communications System
DSN*	Defense Switched Network
DSP	Defense Support Program
DSRV	deep-submergence rescue vehicle (self-propelled)
DSS	Defense Security Service
DSV	deep-submergence vehicle (self-propelled)
DTA	dynamic threat assessment
DTIP	Disruptive Technology Innovations Partnership
DTO	drug trafficking organization
DTRA	Defense Threat Reduction Agency
DTSA	Defense Technology Security Administration
DUG	deep underground [facility]
DVD*	digital video disc
dwt	deadweight ton(s)
DZ/LZ	drop zone/landing zone

E

EA	electronic attack [formerly ECM—electronic countermeasures]
ECCM	electronic counter-countermeasures [now EP—electronic protection]
ECM	electronic countermeasures [now EA—electronic attack]
ECOWAS	Economic Community of West African States
E&E	escape and evasion
EEI	essential element of information
EEZ	exclusive economic zone
EFP	explosively formed penetrator
EHF	extremely high frequency
EIJ	Egyptian Islamic Jihad
EIU	Economist Intelligence Unit
EKIA	enemy killed in action
ELF	extremely low frequency
ELINT*	electronic intelligence
elm	element
ELN	National Liberation Army [Colombia]
email*	electronic mail
EMCON	emission control
EMINT	emissions intelligence
EMP	electromagnetic pulse
ENDP	exception to National Disclosure Policy
EO	electro-optical; executive order
EOB	electronic order of battle
EOD	explosive ordnance disposal
EORSAT	ELINT ocean reconnaissance satellite
EOSAT	Earth observation satellite
EOW	electro-optical warfare
EP	electronic protection [formerly ECCM—electroniccounter-countermeasures]
EPIC	El Paso Intelligence Center
EPIL	explosively pumped iodine laser
EPL	ELINT Parameter Limits
EPW	earth-penetrator weapon
ER	extended-range

ERP	effective radiated power
ERPAC	Popular Antiterrorist Revolutionary Army of Colombia
ERS	early release of submunitions
ERW	enhanced radiation weapon
ES	electronic warfare support [formerly ESM—electronic support measures]
ESA	European Space Agency
ESDP	European security and defense policy
ESM	electronic support measures [now ES—electronic warfare support]
est*	estimate; estimated
ETA	estimated time of arrival; Basque Fatherland and Liberty
ETF	enhanced tactical fighter
ETIM	East Turkestan Islamic Movement [also called ETIP]
ETIP	East Turkestan Islamic Party [also called ETIM]
ETL	elevate to launch
EU*	European Union
EUFOR	European Union Force
EULEX	European Union Rule of Law Mission
EUTELSAT	European Telecommunications Satellite Organization
EUV	extreme ultraviolet
EW	electronic warfare; early warning
EW/GCI	early warning/ground-controlled intercept
EXCOM	executive committee; Intelligence Community Executive Committee

F

F*	Fahrenheit
FA	field artillery
FAC	forward air controller
FAE	fuel-air explosive
FAI	fuel-air incendiary
FAPSI	Federal Agency for Government Communications and Information [Russia]
FARC	Revolutionary Armed Forces of Colombia
FARDC	Armed Forces of the Democratic Republic of the Congo
FATA	Federally Administered Tribal Areas [Pakistan]
FBI*	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service [see OSC]
FC	fire control
FCC	functional combatant command
FCIP	Foreign Counterintelligence Program
FDA	Food and Drug Administration
FDO	foreign disclosure officer
FEBA	forward edge of the battle area
FEMA	Federal Emergency Management Agency
FEP	fuel enrichment plant
FF	frigate
FFAR	folding-fin aerial rocket
FFG	guided-missile frigate
FFL	corvette
FFT	frigate (reserve training)

FGI	foreign government information
FH	frequency-hopping
FIE	foreign intelligence entity
FIR	far infrared
FIS	foreign instrumentation signal; foreign intelligence service
FISA	Foreign Intelligence Surveillance Act
FISINT	foreign instrumentation signals intelligence
FISS	foreign intelligence and security service
FLIR	forward-looking infrared
FLO/FLO	float-on/float-off
FLOT	forward line of own troops
flt	fleet; flight
FLTSATCOM	Fleet Satellite Communication System
FM*	frequency modulation
FME	foreign materiel exploitation
FMF	Foreign Military Financing
FMLN	Farabundo Marti National Liberation Front
FMP	fuel manufacturing plant
FMS	Foreign Military Sales
FNU*	first name unknown
FOB	forward operating base
FOBS	fractional orbital bombardment system
FOC	full operational capability
FOD	foreign object damage
FOFA	follow-on forces attack
FOIA	Freedom of Information Act
FOT&E	follow-on test and evaluation
14FYC	14 February Youth Coalition
FOV	field of view
FPDD	focused police district development
freq	frequency
FROG*	free rocket over ground
FSB	Federal Security Service [Russia]
FSLN	Sandinista National Liberation Front
FSS	forward storage site
FSTEK	Federal Service for Technical and Export Control [Russia]
FSU	former Soviet Union
FSV	fire-support vehicle
ft*	foot; feet
ft2*	square foot; square feet
ft3*	cubic foot; cubic feet
FTE	full-time equivalent; full-time employee
FTI	fixed-target indicator
ft/min	foot (feet) per minute
FTO	foreign terrorist organization
FTP	file transfer protocol
ftr	fighter
ft/s	foot (feet) per second
FTX	field training exercise
FVEY	Five Eyes (United States, Australia, Canada, New Zealand, United Kingdom) [tetragraph for portion markings; in text, spell out, as in "Five Eyes community"]
FY*	fiscal year
FYDP	Future Years Defense Program
FYI*	for your information

G

g*	gram(s); acceleration of gravity
G7	Group of Seven (major industrial nations): United States, United Kingdom, Canada, France, Germany, Italy, Japan
G8	Group of Seven plus Russia
G20	Group of 20: 19 of the world's largest economies plus the European Union
GAD	guards artillery division
gal*	gallon(s)
GBU	guided bomb unit
GCA	ground-controlled approach
GCC	Gulf Cooperation Council; geographic combatant command
GCCS	Global Command and Control System
GCHQ	Government Communications Headquarters [United Kingdom]
GCI	ground-controlled intercept
GCSS	Global Combat Support System
GCTF	Global Counterterrorism Force
GDIP	General Defense Intelligence Program
GDP*	gross domestic product
GEO	geosynchronous Earth orbit
GEOINT*	geospatial intelligence
GHQ	general headquarters
GHz*	gigahertz
GID	General Intelligence Directorate
GIG	Global Information Grid
GITS	General Intelligence Training System
GIUK	Greenland-Iceland-United Kingdom
GLCM*	ground-launched cruise missile
GLOC	ground line of communication
GLONASS	Global Navigation Satellite System
GMI	general military intelligence
GMRD	guards motorized rifle division
GMT*	Greenwich Mean Time [see Coordinated Universal Time (UTC), also called Zulu in the U.S. military]
GNP	gross national product
GOB	ground order of battle
GOCO	government-owned, contractor-operated
GOSP	gas-oil separation plant
GOSSIP	Geotagged Open-Source Search Intelligence Program
GOTS	government off-the-shelf
GP	general purpose
GPS*	Global Positioning System
grp	group
grt	gross registered ton(s)
GRU	General Staff Main Intelligence Directorate [Russia]
GS	General Staff
GSE	ground support equipment
GSM	Global System for Mobile Communications
GSOMIA	General Security of Military Information Agreement
GSTAR	Global Strategic and Tactical Relay
GTD	guards tank division
GTMO	Guantanamo Bay
GTO	geostationary transfer orbit
GTPP	gas turbine powerplant

H

h*	hour(s)
ha	hectare(s)
HAB	hardened aircraft bunker
HADR	humanitarian assistance and disaster relief
HALO	high altitude, low opening
HAMAS†	Islamic Resistance Movement [*Note*: Because the abbreviation is better known and more commonly used than either the Arabic name on which it is based or its English equivalent, shown here, *HAMAS* generally is used without establishing the abbreviation; showing the English equivalent is acceptable for information but is not necessary.]
HARM	high-speed antiradiation missile
HAS	hardened aircraft shelter
HAWK†	Homing-All-the-Way Killer
HAZMAT*	hazardous materials
HCS	HUMINT Control System
HDBT	hardened and deeply buried target
HDTV*	high-definition television
HE	high explosive
HEAT	high-explosive antitank
HEI	high-explosive incendiary
HEL	high-energy laser
helo	helicopter
HEMP	high-altitude electromagnetic pulse
HEO	highly elliptical orbit
HET	heavy equipment transporter
HEU	highly enriched uranium
HF*	high frequency
HF/DF	high-frequency direction finding
HGV	hypersonic glide vehicle
HHW	higher high water
HIG	Hezb-e-Islami Gulbuddin
HIMARS	High-Mobility Artillery Rocket System
HIV*	human immunodeficiency virus
HLA	helicopter landing area
HLA/DZ	helicopter landing area/drop zone
HLW	higher low water
HLZ	helicopter landing zone
HME	homemade explosive
HMG	heavy machinegun
HMMWV	high-mobility multipurpose wheeled vehicle [preferred: Humvee, not spelled out]
HOB	height of burst
how	howitzer
hp*	horsepower
HPM	high-power microwave
HPP	hydroelectric powerplant
HQ*	headquarters
HQN	Haqqani Network
HSC	Homeland Security Council
HSS	high-speed sealift [vessel]
HSV	high-speed vessel
HUD	head-up display
HUJI	Harakat-ul-Jihad-i-Islami
HUJI-B	Harakat ul-Jihad-i-Islami Bangladesh
HUMINT*	human intelligence
HVAC	heating, ventilation, and air conditioning
HVE	homegrown violent extremist
HVI	high-value individual
HVT	high-value target
hwy*	highway
Hz*	hertz

I

IA	information assurance
IADS	integrated air defense system
IAEA	International Atomic Energy Agency
IAW*	in accordance with
IBERLANT	Iberian-Atlantic [region]; Iberian-Atlantic [Command, NATO; now SOUTHLANT]
IBP	Iraqi Baath Party
IC*	Intelligence Community
ICAO	International Civil Aviation Organization
ICBM*	intercontinental ballistic missile
ICC	International Criminal Court
ICD	Intelligence Community directive; imitative communication deception
ICE	Immigration and Customs Enforcement
ICG	International Contact Group
ICJ	International Court of Justice [commonly called World Court]
ICOD	information cutoff date; intelligence cutoff date
ICR	intelligence collection requirement
ICRC	International Committee of the Red Cross
ICTY	International Criminal Tribunal for the former Yugoslavia
ICV	infantry combat vehicle
IDA	International Development Association
IDF	Israel Defense Forces
IDP	internally displaced person
IEA	International Energy Agency
IEC	Independent Election Commission [Afghanistan]
IED*	improvised explosive device
IFCNR	Implementation and Followup Committee for National Reconciliation [Iraq]
IFF*	identification, friend or foe
IFR	instrument flight rules
IFV	infantry fighting vehicle
IG	inspector general; Islamic Group
I-HAWK†	Improved Homing-All-the-Way Killer
IHEC	Independent High Electoral Commission [Iraq]
IICT	Interagency Intelligence Committee on Terrorism
IIR	intelligence information report; imaging infrared
IJU	Islamic Jihad Union
ILS	instrument landing system
IM	info memo
IMET	International Military Education and Training
IMF	International Monetary Fund
IMINT*	imagery intelligence
IMO	International Maritime Organization
IMSAT	imagery satellite
IMU	Islamic Movement of Uzbekistan; inertial measurement unit
in*	inch(es)
in2*	square inch(es)
in3*	cubic inch(es)
IN	information need
INA	Iraqi National Alliance
IND	improvised nuclear device
indef	indefinite

inf	infantry
INF	intermediate-range nuclear force; Intermediate-Range Nuclear Forces [Treaty]
INFOSEC	information security
INMARSAT	International Mobile Satellite Organization [originally International Maritime Satellite Organization]
INR	[State Department] Bureau of Intelligence and Research
INS	inertial navigation system
INSCOM	Intelligence and Security Command [U.S. Army]
Intel*	intelligence
INTELSAT	International Telecommunications Satellite Organization
Interpol*	International Criminal Police Organization
INTREP	intelligence report
INTSUM	intelligence summary
IO	information operations
IOC*	initial operational capability
IOC	International Olympic Committee
IP*	Internet protocol
IPB	intelligence preparation of the battlespace
IPR	intelligence production requirement
IR	infrared
IRA	Irish Republican Army
IRAM	improvised rocket-assisted munition
IRBM*	intermediate-range ballistic missile
IRCM	infrared countermeasures
IRFNA	inhibited red-fuming nitric acid
IRGC	Islamic Revolutionary Guard Corps [Iran]
IRGC-QF	Islamic Revolutionary Guard Corps–Qods Force [Iran]
IRINT	infrared intelligence
IRKS	INHERENT RESOLVE Kinetic Support
IRST	infrared search and track
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISAF	International Security Assistance Force
ISCI	Islamic Supreme Council of Iraq [formerly SCIRI—Supreme Council for the Islamic Revolution in Iraq]
ISF	Iraqi security forces
ISI	Directorate General for Inter-Services Intelligence [Pakistan]
ISIL*	Islamic State of Iraq and the Levant [widely known in the news media as ISIS (for Islamic State of Iraq and Syria) or simply Islamic State]
I-SLIC	improved semisubmersible infiltration landing craft [improved infiltration boat]
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
ISP	Internet service provider
ISR*	intelligence, surveillance, and reconnaissance
ISTAR	intelligence, surveillance, target acquisition, and reconnaissance
IT*	information technology
ITAR	International Traffic in Arms Regulations
ITAR-TASS	Information Telegraph Agency of Russia

ITSO	International Telecommunications Satellite Organization
ITWA	initial threat warning assessment
IVO	in the vicinity of; in view of
IW	information warfare
I&W	indications and warning
IWG	interagency working group; intelligence working group
IX	unclassified miscellaneous unit [naval]

J

JAC	joint analysis center
JAEIC	Joint Atomic Energy Intelligence Committee
JAG	judge advocate general
JAK	Jund al-Khilafah
JASSM	joint air-to-surface standoff missile
JAT	Jemaah Anshorut Tauhid
JCOFA	joint country force assessment
JCS*	Joint Chiefs of Staff
jct	junction
JCTD	joint capabilities technology demonstration
JDA	joint duty assignment
JDAM	Joint Direct-Attack Munition
JDEC A	Joint Document Exploitation Center–Afghanistan
JEM	Justice and Equality Movement; Jaish-e-Mohammad
JEWC	Joint Electronic Warfare Center
JFCC-ISR	Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance
JFCC-NW	Joint Functional Component Command for Network Warfare
JI	Jemaah Islamiyah
JIACTF	Joint Interagency Cyber Task Force
JIATF South	Joint Interagency Task Force South
JIC	joint intelligence center
JIDA	Joint Improvised-Threat Defeat Agency [formerly JIEDDO]
JIEDDO	[former] Joint Improvised Explosive Device Defeat Organization [now JIDA]
JIOC	joint intelligence operations center
JIOC-A	Joint Intelligence Operations Center–Afghanistan
JIOWC	Joint Information Operations Warfare Command
JIPOE	Joint Intelligence Preparation of the Operational Environment
JMITC	Joint Military Intelligence Training Center
JOC	joint operations center
JOIIS	Joint Operational Intelligence Information System
JP	jet petroleum
JRTN	Jaysh Rijal al-Tariq al-Naqshabandiyah (Army of the Naqshabandiyah Order)
JS	Joint Staff
JSDF	Japan Self-Defense Force
JSF	Joint Strike Fighter
JSOW	Joint Standoff Weapon

JSTARS	Joint Surveillance Target-Attack Radar System
JTF	joint task force
JTF-GNO	Joint Task Force–Global Network Operations
JTIDS	Joint Tactical Information Distribution System
JUD	Jamaat-ud-Dawa
JUIAF	Joint-Use Intelligence Analysis Facility
JUSMAG	Joint U.S. Military Advisory Group
JWAC	Joint Warfare Analysis Center
JWICS*	Joint Worldwide Intelligence Communications System

K

K*	degrees Kelvin [*Note:* used without degree symbol (°) or word degree]
KDP	Kurdistan Democratic Party [Iraq]
KFOR	Kosovo Force
kg*	kilogram(s)
KGK	Kongra-Gel [also called Kurdistan People's Congress; formerly Kurdistan Workers' Party (PKK)]
KH	Kataib Hizballah
kHz*	kilohertz
KIA*	killed in action
KKV	kinetic-kill vehicle
km*	kilometer(s)
km2*	square kilometer(s)
km3*	cubic kilometer(s)
km/h*	kilometer(s) per hour [see also kph]
kn*	knot(s)
kN	kilonewton(s)
KPA	[North] Korean People's Army
kph	kilometer(s) per hour [see also km/h]
KRG	Kurdistan Regional Government [Iraq]
ksi	kips per square inch
kt	kiloton(s)
kV*	kilovolt(s)
kW*	kilowatt(s)
kWh*	kilowatt-hour(s)

L

L*	liter(s)
lab*	laboratory
LAC	Line of Actual Control [de facto boundary between India and China]
LACM*	land-attack cruise missile
LAF	Lebanese Armed Forces
LAN	local area network
LANDSAT*	Land Satellite (commercial multispectral)
LANTIRN	Low-Altitude Navigation and Targeting Infrared for Night
LAR	light artillery rocket
laser†	light amplification by simulated emission of radiation
LASINT	laser intelligence
LAW	light antitank weapon
lb*	pound(s)
LCA	assault landing craft
LCAC	air-cushion landing craft
LCC	amphibious command ship
LCF	launch control facility

LCM	mechanized landing craft [U.S. Navy definition]; medium landing craft [definition commonly used with navies of other countries]
LCMA	air-cushion medium landing craft
LCP	personnel landing craft
LCPA	air-cushion personnel landing craft
LCS	littoral combat ship
LCU	utility landing craft
LCUA	air-cushion utility landing craft
LCVP	landing craft, vehicle, personnel
LDS	launch-detection satellite
LEA	law enforcement agency
LEF	law enforcement force; Law Enforcement Forces [Iran]
LEO	low Earth orbit
LEU	low-enriched uranium
LF*	low frequency
lg	large
LGB	laser-guided bomb
LGM	laser-guided munition
LGW	laser-guided weapon
LHA	amphibious assault ship
LHD	amphibious assault dock
LHW	lower high water
LIC	low-intensity conflict
LIDAR	light detection and ranging
LIFG	Libyan Islamic Fighting Group
LKA	amphibious cargo ship
LLW	lower low water
LNG	liquefied natural gas
LNI	Library of National Intelligence
LNO	liaison officer
LNU*	last name unknown
LO	low-observable
LOC	line of communication; Line of Control
LOCE	Linked Operations Intelligence Centers Europe
LORAN	long-range aid to navigation
LOS	line of sight
LOTS	logistics over the shore
LOX	liquid oxygen
LPA	amphibious transport
LPAR	large phased-array radar
LPD	amphibious transport dock
LPG	liquefied petroleum gas
LPH	amphibious assault ship (helicopter)
LPV	low-profile vehicle
LRA	Long-Range Aviation [Russia]; Lord's Resistance Army
LRAAM	long-range air-to-air missile
LRCM	long-range cruise missile
LSD	dock landing ship
LSDV	swimmer delivery vehicle
LSM	medium landing ship
LSSC	light SEAL/swimmer support craft
LST	tank landing ship
LT	Lashkar-e-Tayyiba
LTBT	Limited Test Ban Treaty
Ltd*	Limited [as part of a firm's proper name]
LTD	laser target designator
LTTE	Liberation Tigers of Tamil Eelam
LWIR	long-wavelength infrared
LZ	landing zone

M

µ	micro [one-millionth]
µm	micrometer(s)
µs	microsecond(s)
m*	meter(s)
m2*	square meter(s)
m3*	cubic meter(s)
MAAG	Military Assistance Advisory Group
MAD	magnetic anomaly detector
MAGTF	Marine Air-Ground Task Force
MANPADS*	man-portable air defense system(s)
MAP	membership action plan [NATO]
MARV	maneuverable reentry vehicle
MASINT	measurement and signature intelligence
MAT	medium assault transport
max	maximum
MB	megabyte(s)
MBT	main battle tank
MCFI	Multinational Coalition Forces–Iraq
MC&G	mapping, charting, and geodesy
MCIA	Marine Corps Intelligence Activity
MCM	mine countermeasures; mine countermeasures ship
MCP	mobile command post
MCS	mine countermeasures support ship
MD	military district
MDA	Missile Defense Agency
MDCI	multidisciplinary counterintelligence
mdm	medium
MEADS	medium extended air defense system
medevac†	medical evacuation [abbreviation accepted as a standard English word]
MEDINT	medical intelligence
MEF	Marine expeditionary force
MEK	Mujahedin-e Khalq
MEL	mobile erector-launcher
MEO	medium Earth orbit
MEPED	Military Equipment Parametrics and Engineering Database
MERCOSUR	Southern Cone Common Market
MERSHIP	merchant ship
MESF	Middle East Stability Force
METSAT	meteorological satellite
MEU	Marine expeditionary unit
MF	medium frequency
MFO	Multinational Force and Observers
mg*	milligram(s)
MGRS	Military Grid Reference System
MHC	coastal minehunter
MHCA	air-cushion coastal minehunter
MHS	minehunting ship
MHWN	mean high water neaps
MHWS	mean high water springs
MHz*	megahertz
mi*	(statute) mile(s)
mi2*	square mile(s)
MIA*	missing in action
MIB	Military Intelligence Board
MIBN	military intelligence battalion
MICV	mechanized infantry combat vehicle
MIDB	Modernized Integrated Database

MiG*	Mikoyan aircraft [formerly Mikoyan-I-Gurevich Design Bureau]
mi/h*	mile(s) per hour [see also mph]
MIJI	meaconing, intrusion, jamming, or interference
MILF	Moro Islamic Liberation Front
MILSATCOM	military satellite communications
MILSTAR	Military Strategic and Tactical Relay [System]
min*	minute(s); minimum
MINURCAT	United Nations Mission in the Central African Republic and Chad
MINURSO	United Nations Mission for the Referendum in Western Sahara
MINUSTAH	United Nations Stabilization Mission in Haiti
MIP	Military Intelligence Program
MIRV*	multiple independently targetable reentry vehicle
MK V SOC	Mk V special operations craft
mL	milliliter(s)
MLLW	mean lower low water
MLRS	Multiple Launch Rocket System
MLWN	mean low water neaps
MLWS	mean low water springs
mm*	millimeter(s)
MM	minelayer
mm2*	square millimeter(s)
mm3*	cubic millimeter(s)
M-MRCA	medium-range multirole combat aircraft
MMW	millimeter wave
MNF	multinational force
MNF-I	Multinational Force–Iraq [became USF-I on 1 January 2010]
MNLF	Moro National Liberation Front
MNU*	middle name unknown
MOA	memorandum of agreement
MOB	main operating base; missile order of battle; mobilization
MOD	Ministry of Defense [preferred: Defense Ministry]
Mod	modification [used in missile designators, such as "CSS-5 Mod 4"]
MODAFL	Ministry of Defense and Armed Forces Logistics [Iran]
MOGAS	motor gasoline
MOIS	Ministry of Intelligence and Security [Iran]
MON	monitor [riverine warfare craft]
MONUC	United Nations Organization Mission in the Democratic Republic of the Congo
mort	mortar
MOU	memorandum of understanding
MOUT	military operations in urban terrain
MOX	mixed oxide
MP	military police; maritime patrol
MPa	megaPascal(s)
MPA	maritime patrol aircraft
MPFA	maritime pre-positioning ship, aviation
MPFC	maritime pre-positioning ship, cargo
MPFD	maritime pre-positioning ship, dock
mph	miles per hour [see also mi/h]
MPLA	Popular Movement for the Liberation of Angola

MR	military region
MRAP	mine-resistant, ambush-protected [vehicle]
MRBM*	medium-range ballistic missile
MRC	motorized rifle company
MRD	motorized rifle division
MRL	multiple rocket launcher
MRR	motorized rifle regiment
MRTT	multirole tanker transport
ms	millisecond(s)
m/s	meter(s) per second
MSB	minesweeping boat
MSC	coastal minesweeper
MSCO	coastal minesweeper (old)
MSD	minesweeper, drone
MSF	fleet minesweeper (steel hull)
MSH	minehunter
MSI	inshore minesweeper
MSIC	Missile and Space Intelligence Center
MSL	mean sea level; minesweeping launch
MSM	river minesweeper
MSP	money service provider
MSR	main supply route
MSS	specialized minesweeper
MSSC	medium SEAL/swimmer support craft
Mt	megaton(s)
MTCR	Missile Technology Control Regime
MTI	moving target indicator
MTU	master terminal unit
MTZ	motorized infantry
MUSIS	Multinational Space-Based Imaging System
M/V	merchant vessel
MW*	megawatt(s)
MW	mine warfare
MWe	megawatt(s) electrical
MWIR	mid-wavelength infrared
MWL	mean water level
MWR	missile warning receiver
MWt	megawatt(s) thermal

N

NA*	not applicable; not available
NAC	North Atlantic Council
NAFTA	North American Free Trade Agreement
NAI	named area of interest
NAM	Nonaligned Movement
NAMRU	Naval Medical Research Unit [U.S.]
NAS*	naval air station
NASA*	National Aeronautics and Space Administration
NASIC	National Air and Space Intelligence Center
NATO*	North Atlantic Treaty Organization
NAVAID	navigation aid
NAVSAT	navigation satellite
NBC	nuclear, biological, and chemical
NCA	national command authority; nuclear command authority
NCIC	National Counterintelligence Center
NCIS	Naval Criminal Investigative Service
NCMI	National Center for Medical Intelligence [formerly AFMIC—Armed Forces Medical Intelligence Center]
NCO*	noncommissioned officer
NCOIC	noncommissioned officer in charge

NCPC	National Counterproliferation Center
NCR	National Capital Region
NCS	National Clandestine Service
NCTC	National Counterterrorism Center
NCW	network-centric warfare
NDP	national disclosure policy
NEO	noncombatant evacuation operation
NFI*	no further information
NFIB	National Foreign Intelligence Board
NFZ	nuclear-free zone
NGA	National Geospatial-Intelligence Agency [formerly DMA (Defense Mapping Agency) and later NIMA (National Imagery and Mapping Agency)]
NGIC	National Ground Intelligence Center
NGL	natural gas liquids
NGO*	nongovernmental organization
NIC	National Intelligence Council
NICB	National Intelligence Collection Board
NIC C	National Intelligence Coordination Center
NIE	national intelligence estimate
NIO	national intelligence officer
NIP	National Intelligence Program
NIPF	National Intelligence Priorities Framework
NIPRNET*	Nonsecure Internet Protocol Router Network
NIR	near-infrared
NIST	National Intelligence Support Team; National Institute of Standards and Technology
NIT	national intelligence topic
NIU	National Intelligence University
NJOIC	National Joint Operations Intelligence Center
NLL	Northern Limit Line [Koreas]
nm	nanometer(s)
NM*	nautical mile(s)
NMD	national missile defense
NMEC	National Media Exploitation Center
NMI*	no middle initial
NMIC	National Maritime Intelligence Center
NMN*	no middle name
no.*	number
NOB	naval order of battle
NORAD	North American Aerospace Defense Command
NPA	New People's Army
NPT	Nonproliferation Treaty
NR	submersible research vehicle (self-propelled)
NRO	National Reconnaissance Office
NRT	near-real-time
ns	nanosecond(s)
NSA*	National Security Agency
NSA/CSS	National Security Agency/ Central Security Service
NSC	National Security Council
NSG	Nuclear Suppliers Group
N-SILC	nonsubmersible infiltration landing craft [small speedboat]
NSIP	NATO Security Investment Program
NSW RHIB	naval special warfare rigid-hull inflatable boat
NTM	national technical means
NTM-A	NATO Training Mission–Afghanistan

NTO	nitrogen tetroxide [N2O4; also shown as dinitrogen tetroxide]
NUCINT	nuclear intelligence
NVD	night-vision device
NVG	night-vision goggles
NWFP	North-West Frontier Province [Pakistan] [now Khyber Pakhtunkhwa]
NWFZ	nuclear-weapons-free zone
NWSS	nuclear weapon storage site

O

OAS	Organization of American States
OB	order of battle
OBE*	overtaken by events
OCA	offensive counterair
OCONUS*	outside the continental United States
OCU	operational conversion unit
ODNI*	Office of the Director of National Intelligence
OECD	Organization for Economic Cooperation and Development
OEF	Operation ENDURING FREEDOM
OHCHR	Office of the High Commissioner for Human Rights
OHR	Office of the High Representative
OIC	officer in charge; Organization of the Islamic Conference
OIF	Operation IRAQI FREEDOM
OJT	on-the-job training
O&M	operations and maintenance
OMG	operational maneuver group
OMLT	operational mentoring and liaison team
OMS	Office of the Martyr Sadr
ONI	Office of Naval Intelligence
ONIR	overhead nonimaging infrared
OOA	out of area
OPCW	Organization for the Prohibition of Chemical Weapons
OPEC*	Organization of Petroleum-Exporting Countries
OPFOR	opposing force(s)
OPI	office of primary interest
OPIR	overhead persistent infrared
OPLAN	operation plan
OPR	office of primary responsibility
OPSEC*	operations security
OPTEMPO*	operational tempo
OPTINT	optical intelligence
OSC	Open Source Center [formerly FBIS—Foreign Broadcast Information Service]
OSCE	Organization for Security and Cooperation in Europe
OSD	Office of the Secretary of Defense
OSINT*	open-source intelligence
OT&E	operational test and evaluation
OTH	over-the-horizon
OTH-B	over-the-horizon backscatter [radar]
OTHR	over-the-horizon radar
OTHT	over-the-horizon targeting
OTU	operational training unit
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
oz*	ounce(s)

P

P5	permanent five members of the UN Security Council (United States, United Kingdom, France, China, Russia)
P5+1	permanent five members of the UN Security Council plus Germany
PA	Palestinian Authority; probability of arrival
PAL	permissive action link
PAP	People's Armed Police [China]
PAR	precision-approach radar; phased-array radar
Patriot†	phased-array tracking radar intercept on target
PAWS	Phased-Array Warning System
PB	patrol boat
PBA	air-cushion patrol boat
PBD	drone patrol boat
PBG	guided-missile patrol boat
PBH	hydrofoil patrol boat
PBR	river patrol craft
PBT	training patrol boat
PBV	postboost vehicle
PC	personal computer; coastal patrol craft
PCF	fast patrol craft
PCFA	fast air-cushion patrol craft
PCFG	fast guided-missile patrol craft
PCFH	fast hydrofoil patrol craft
PCFS	fire-support patrol craft
PCH	hydrofoil patrol craft
PCS	permanent change of station
PD	probability of damage; pulse duration
PDA	personal digital assistant
PDB	President's Daily Brief
PDF	portable document format
PED	personal electronic device
penaid	penetration aid
PFLP	Popular Front for the Liberation of Palestine
PFLP-GC	Popular Front for the Liberation of Palestine–General Command
PFP	Partnership for Peace
PG	patrol combatant
PGG	guided-missile patrol combatant
PGGA	air-cushion guided-missile patrol combatant
PGH	hydrofoil patrol combatant
PGM	precision-guided munition
Ph.D.	doctor of philosophy
PHM	patrol combatant missile (hydrofoil) [hydrofoil guided-missile patrol combatant]
PHOTINT*	photographic intelligence
PIJ	Palestine Islamic Jihad
PIR	passive infrared; priority intelligence requirement
PII	personally identifiable information
PKI	public key infrastructure
PKK	[former] Kurdistan Workers' Party [see KGK]
PKO	peacekeeping operation
PLA	People's Liberation Army [China]
PLF	Palestine Liberation Front
PLO	Palestine Liberation Organization
plt	platoon
p/m	part(s) per million
PM*	post meridian (after noon)

PM	river monitor [naval craft]; perception management
PMO	project management office; program management office
POC*	point of contact
POE	port of entry
POL*	petroleum, oils, and lubricants
Polisario†	Popular Front for the Liberation of Saguia el-Hamra and Rio de Oro
POMCUS	pre-positioning of materiel configured to unit sets
POTUS*	President of the United States
POW*	prisoner of war
PPRC	Palestinian Popular Resistance Committees
PR	production requirement
PRA	Performance Review Authority [DCIPS]
PRF	pulse repetition frequency
PRI	pulse repetition interval
PRT	provincial reconstruction team
PS	large patrol ship
PSG	guided-missile patrol ship
psi*	pound(s) per square inch
PSI	Proliferation Security Initiative
PSP	pierced-steel planking
PST	training patrol ship
PSTN	public switched telephone network
PSYOP	psychological operations
pt*	pint(s)
PT	torpedo boat
PTD	drone torpedo boat
PTF	fast patrol craft
PTG	missile attack boat
PTGA	air-cushion missile attack boat
PTGH	hydrofoil missile attack boat
PTH	hydrofoil torpedo boat
PTT	push to talk
PUG	partially underground
PUK	Patriotic Union of Kurdistan [Iraq]
PV	physical vulnerability
PWHQ	primary war headquarters

Q

Q&A*	question(s) and answer(s)
QC	quality control
QDR	Quadrennial Defense Review
qt*	quart(s)

R

RAD	radiation absorbed dose
radar†	radio detection and ranging
RADCOM	radio communications
RADINT	radar intelligence
RADREL	radio-relay
RAM	radar-absorbing material; random access memory
RC	regional command
RCA	riot-control agent
RC Capital	Regional Command Capital [Afghanistan]
RC East	Regional Command East [Afghanistan]
RCIED	radio-controlled improvised explosive device
RCLR	recoilless rifle
RC North	Regional Command North [Afghanistan]
RCS	radar cross section

RC South	Regional Command South [Afghanistan]
RC West	Regional Command West [Afghanistan]
rd	round(s)
R&D*	research and development
RDA	research, development, and acquisition
RDD	radiological dispersal device
RDF	radio direction finding
rd/min	round(s) per minute
RDT&E	research, development, testing, and evaluation
REC	radioelectronic combat
recon	reconnaissance
ref*	reference
regt	regiment
Ret*	retired [used with rank]
RF	radiofrequency
RFI	request for information
RFID	radiofrequency identification
RFP	request for proposal
RFW	radiofrequency weapon
RGF	remote ground facility
RHAW	radar homing and warning
RHIB	rigid-hulled inflatable boat
RIF	reduction in force
RL	rocket launcher
RM	response memo; risk management
RMR	rock-mass rating
ROE	rules of engagement
RO/RO	roll-on/roll-off
RPG*	rocket-propelled grenade
rpm*	revolution(s) per minute
RPV	remotely piloted vehicle
RRF	rapid-reaction force
RSMA	RESOLUTE SUPPORT Mission Afghanistan
RSP	render-safe procedure
RSS*	Really Simple Syndication
RSTA	reconnaissance, surveillance, and target acquisition
rte	route
RTP	rail transfer point; rail transshipment point
RTU	remote terminal unit; remote telemetry unit
RV	reentry vehicle
RWR	radar warning receiver
rwy	runway

S

s*	second(s)
SACEUR	Supreme Allied Commander, Europe [NATO]
SACLANT	Supreme Allied Command(er), Atlantic [NATO]
SACLOS	semiautomatic command to line-of-sight
SADC	Southern African Development Community
SAFF	safing, arming, fuzing, and firing
SAM*	surface-to-air missile
SAMOB	surface-to-air missile order of battle
SAP	special access program
SAR	search and rescue; synthetic aperture radar
SARS	severe acute respiratory syndrome
SASM	strategic air-to-surface missile
SATCOM	satellite communications
SATNAV	satellite navigation

SATRAN	satellite reconnaissance advance notice
SBIRS	Space-Based Infrared System
SBL	space-based laser
SBR	space-based radar
SCADA	supervisory control and data acquisition
SCI*	sensitive compartmented information
SCIF	sensitive compartmented information facility
SCIRI	Supreme Council for the Islamic Revolution in Iraq [now ISCI—Islamic Supreme Council of Iraq]
SCO	Shanghai Cooperation Organization
SCRM	supply chain risk management
scuba†	self-contained underwater breathing apparatus
SDIA	senior defense intelligence analyst
SDR	source-directed requirement
SDV	SEAL/swimmer delivery vehicle; strategic delivery vehicle
SEAD	suppression of enemy air defenses
SEAL†	sea/air/land
SecDef	[U.S.] Secretary of Defense
SEDENA	Secretariat of National Defense [Mexico—includes Mexico's Army and Air Force]
SEMAR	Secretariat of the Navy [Mexico]
SERE	survival, evasion, resistance, and escape
SERER	survival, evasion, resistance, escape, and recovery
SES	Senior Executive Service
SF	special forces
SFOR	Stabilization Force
SHAPE	Supreme Headquarters Allied Powers, Europe [NATO]
SHF	superhigh frequency
ShLBM	ship-launched ballistic missile
SHORAD	short-range air defense
SI	special intelligence; International System of Units [commonly called the metric system]
SIA	senior intelligence analyst
SIGINT*	signals intelligence
SILC	semisubmersible infiltration landing craft [infiltration boat]
SIM*	subscriber identity module
SINCGARS	single-channel ground and airborne radio system
SIO	senior intelligence officer
SIOP	Single Integrated Operational Plan
SIPRNET*	Secret Internet Protocol Router Network
SITREP	situation report
SL	Sendero Luminoso [or Shining Path]
SLAM	standoff land-attack missile
SLAR	side-looking airborne radar
SLBM*	submarine-launched ballistic missile
SLCM*	sea-launched cruise missile
SLEP	service life extension program
SLF	superlow frequency
SLM/A	Sudanese Liberation Movement/Army
SLOC	sea line of communication
SLV	space launch vehicle
SLWT	side-loadable warping tug
sm	small

SME	subject matter expert
SMEB	significant military exercise brief
SMP	Security Markings Program [formerly CAPCO]
SMS	short message service
SNF	short-range nuclear force; spent nuclear fuel
SNS	social networking site
SOB	space order of battle
SOC	sector operations center
SOC-R	special operations craft, riverine [riverine special operations craft]
SOF	special operations forces
SOFA	status of forces agreement
SOG	special operations group
SOI	Sons of Iraq
SO/LIC	special operations/ low-intensity conflict
sonar†	sound navigation and ranging
SOP	standard operating procedure
SORT	Strategic Offensive Reduction Treaty
SOSI	space object surveillance and identification
SOUTHLANT	Regional Command Southeast Atlantic [NATO; formerly IBERLANT]
SP	self-propelled
SPAAG	self-propelled antiaircraft gun
SPADOC	space defense operations center
SPG	self-propelled gun
SPOD	seaport of debarkation; sea point of departure
SPOT*	Satellite pour l'Observation de la Terre
SPSS	self-propelled semisubmersible [vessel]
sq*	square
sqdn	squadron
SRAM	short-range attack missile
SRBM*	short-range ballistic missile
SRF	Strategic Rocket Forces [Russia]
SRO	sensitive reconnaissance operation
SS	diesel-powered attack submarine
SSA	auxiliary submarine
SSB	ballistic missile submarine; single sideband
SSBN	nuclear-powered ballistic missile submarine
SSC	coastal submarine
SSG	cruise missile attack submarine
SSGN	nuclear-powered cruise missile attack submarine
SSLP	transport submarine
SSM	surface-to-surface missile; midget submarine
SSMOB	surface-to-surface missile order of battle
SSN	nuclear-powered attack submarine
SSP	air-independent-powered attack submarine
SSR	surface-to-surface rocket
SSRP	Sensitive Source Reporting Program
SSS	staff summary sheet; source summary statement
SST	training submarine
SSTR	stability, support, transition, and reconstruction
St*	street; saint

S&T	scientific and technical; science and technology
STANAG	standardization agreement [NATO]
STAR	system threat assessment report
START*	Strategic Arms Reduction Treaty
S&TI	scientific and technical intelligence
STO	special technical operation
STOL	short takeoff and landing
STOVL	short takeoff and vertical landing
STP	Strategic Transition Plan [South Korea]
STSS	space tracking and surveillance system
STU	secure telephone unit
SUBROC	submarine rocket
SUW	surface warfare
SVBIED	suicide vehicle-borne improvised explosive device
SVIED	suicide vest improvised explosive device
SVR	Foreign Intelligence Service [Russia]
SWAPO	Southwest Africa People's Organization
SWC	special warfare craft
SWCL	special warfare craft, light
SWCM	special warfare craft, medium
SWHQ	static war headquarters
SWIR	short-wavelength infrared

T

t*	metric ton(s) (tonne[s])
T2	technology transfer [see also TT]
TA	tank army
TAA	tactical air army
TACAN*	tactical air navigation
TARE	telegraph automation relay equipment
TARM	tactical antiradiation missile
TASM	tactical air-to-surface missile
TASMO	tactical air support for maritime operations
TBA*	to be announced
TBD*	to be determined
TBM	theater ballistic missile; tactical ballistic missile; tunnel-boring machine
TBMD	theater ballistic missile defense
TCM	tactical cruise missile
TCP/IP	transmission control protocol/Internet protocol
TD-2	Taepo Dong 2
TDM	time-division multiplexed
TDMA	time-division multiple access
TDY*	temporary duty
T&E	test and evaluation
TECHINT	technical intelligence
TEL	transporter-erector-launcher
TELAR	transporter-erector-launcher and radar
TELINT	telemetry intelligence
TFG	Transitional Federal Government [Somalia]
TFLIR	targeting forward-looking infrared
TFR	terrain-following radar
tgt	target

THAAD	terminal high-altitude air defense
TIC	toxic industrial chemical
TIDE	Terrorist Identities Datamart Environment
tk	tank
TLAM	Tomahawk land-attack missile
TLAM/C	Tomahawk land-attack missile/conventional
TLAM/N	Tomahawk land-attack missile/nuclear
TLAR	transporter-launcher and radar
TLE	treaty-limited equipment
TMD	theater missile defense
TNF	theater nuclear force
TOA	time of arrival
TO&E	table of organization and equipment
TOR	term of reference
TOT	time on target
TOW†	tube-launched, optically tracked, wire-guided [antitank missile]
tpd	metric ton(s) per day
TPP	thermal powerplant
TR	tank regiment
TRA	temporary restricted area
TRADOC	Training and Doctrine Command [U.S. Army]
TRB	technical reconnaissance bureau
TSA	Transportion Security Administration
TSMO	Threat System Management Office
TT	technology transfer [see also T2]
TTBT	Threshold Test Ban Treaty
TTP	tactics, techniques, and procedures; Tehrik-e Taliban Pakistan
TV*	television
TVD	theater of military operations
TWJWA	al-Tawhid wal-Jihad in West Africa [also known as Movement for Unity and Jihad in West Africa (MUJWA)]

U

UAE	United Arab Emirates
UAV*	unmanned aerial vehicle
UC	under construction
UCAV	unmanned combat aerial vehicle
UCF	uranium conversion facility
UCP	Unified Command Plan
UDMH	unsymmetrical dimethyl hydrazine
UDT	underwater demolition team
UEF	uranium enrichment facility
UF_4	uranium tetrafluoride
UF_6	uranium hexafluoride
UFAC	Underground Facility Analysis Center
UG	underground
UGF	underground facility
UGV	unmanned ground vehicle
UHF*	ultrahigh frequency
UI*	unidentified
UK*	United Kingdom
ULCC	ultralarge crude carrier
ULF*	ultralow frequency
ULV	unmanned launch vehicle
UMOPAR	Rural Mobile Patrol Unit [Bolivia]
UN*	United Nations
UNAMA	United Nations Assistance Mission in Afghanistan
UNAMI	United Nations Assistance Mission for Iraq

UNAMID	African Union–United Nations Hybrid Operation in Darfur
UNASUR	Union of South American Nations
UNC	United Nations Command
UNDOF	United Nations Disengagement Observer Force
UNDP	United Nations Development Program
UNEP	United Nations Environment Program
UNESCO	United Nations Educational, Scientific, and Cultural Organization
UNFICYP	United Nations Peacekeeping Force in Cyprus
UNFPA	United Nations Population Fund
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
UNIDO	United Nations Industrial Development Organization
UNIFIL	United Nations Interim Force in Lebanon
UNIOSIL	United Nations Integrated Office in Sierra Leone
UNIPSIL	United Nations Integrated Peacebuilding Office in Sierra Leone
unk*	unknown
UNMIK	United Nations Interim Administration Mission in Kosovo
UNMIL	United Nations Mission in Liberia
UNMIN	United Nations Mission in Nepal
UNMISS	United Nations Mission in South Sudan
UNMIT	United Nations Integrated Mission in Timor-Leste
UNMOGIP	United Nations Military Observer Group in India and Pakistan
UNOCI	United Nations Operation in Cote d'Ivoire
UNODC	United Nations Office on Drugs and Crime
UNOGBIS	United Nations Peacebuilding Support Office in Guinea-Bissau
UNOMIG	United Nations Observer Mission in Georgia
UNOPS	United Nations Office for Project Services
UNOWA	United Nations Office for West Africa
UNPOS	United Nations Political Office for Somalia
UNRCCA	United Nations Regional Centre for Preventive Diplomacy in Central Africa
UNRWA	United Nations Relief and Works Agency for Palestinian Refugees in the Near East
UNSC	United Nations Security Council
UNSCO	Office of the United Nations Special Coordinator for the Middle East Peace Process
UNSCOL	Office of the United Nations Special Coordinator for Lebanon
UNSCR	United Nations Security Council resolution
UNTSO	United Nations Truce Supervision Organization
URL†	uniform resource locator
U.S.*	United States

USA*	United States of America [United States or U.S. preferred]; United States Army
USAF*	United States Air Force
USAFRICOM*	United States Africa Command
USAID	United States Agency for International Development
USCENTCOM*	United States Central Command
USCG*	United States Coast Guard
USDA	United States Department of Agriculture [or Agriculture Department]
USDAO*	United States Defense Attaché Office
USD(I)	Under Secretary of Defense for Intelligence
USEUCOM*	United States European Command
USF-I	United States Forces–Iraq [formerly MNF-I]
USFK	United States Forces, Korea
USGS	United States Geological Survey
USJFCOM	United States Joint Forces Command
USMC*	United States Marine Corps
USN*	United States Navy
USNORTHCOM*	United States Northern Command
USPACOM*	United States Pacific Command
USPER*	U.S. person
USSOCOM	United States Special Operations Command
USSOUTHCOM*	United States Southern Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
USV	unmanned surface vehicle
USW	undersea warfare
UTC	Coordinated Universal Time [also known as Greenwich Mean Time and as Zulu]
UUV	unmanned underwater vehicle
UW	unconventional warfare
UWB	ultrawideband

V

V*	volt(s)
VBIED	vehicle-borne improvised explosive device
VDS	variable-depth sonar
VDT	video display terminal
VDV	Russian Airborne Troops
VFR	visual flight rules
VGW	variable-geometry wing
VHF*	very-high frequency
VIP*	very important person
VISINT	visual intelligence
VISOB	visual observer
VLCC	very large crude carrier
VLF*	very-low frequency
VN	vulnerability number
VOIED	victim-operated improvised explosive device
VOIP	Voice Over Internet Protocol
VOR*	very-high-frequency omnidirectional range
VORTAC*	colocated VOR and TACAN
VSAT	very-small-aperture terminal
V/STOL	vertical/short takeoff and landing
VTOL	vertical takeoff and landing
VTR	tracked recovery vehicle

W

W prefix for ship designators	[Adding an initial W to an abbreviation for a naval ship or craft indicates a coast guard ship or craft; thus, a WLCU is an LCU (utility landing craft) assigned to a coast guard or coast-guard-like force.]
W*	watt(s)
WAN	wide-area network
WARM	wartime reserve mode
WB	wideband
WFP	World Food Program
Wh	watt-hour(s)
WHO	World Health Organization
WHQ	war headquarters
WIA*	wounded in action
WIG	wing-in-ground effect
WLL	wireless local loop
WMD*	weapons of mass destruction
WRM	war reserve materiel
WRMS	war reserve materiel stock
WSSIC	Weapon and Space Systems Intelligence Committee
WTO	World Trade Organization
WUNM	weapons-usable nuclear material
WWW	World Wide Web

X

XA	executive assistant
xmtr	transmitter
XO	executive officer

Y

yd*	yard(s)
yd2*	square yard(s)
yd3*	cubic yard(s)
yr*	year(s)

Z

Z*	Zulu [see Coordinated Universal Time (UTC); also known as Greenwich Mean Time]
ZIB	Ziyad al-Jarrah Battalions

CHAPTER 3: Capitalization

Social Security is a government program; *social security* might refer to whether you have a date Friday night.

—Bill Walsh, *Yes, I Could Care Less: How to Be a Language Snob Without Being a Jerk*

CHAPTER 3: Capitalization

The trend in American publishing has been to reduce the amount of capitalization in text. Proper nouns still are capitalized, of course, but often words derived from them are printed with lowercase without damage to clarity or significance.

Beginnings

Begin each sentence with a capital letter.

Begin each item in an indented listing with a capital letter. This applies to bulleted lists, lists marked with em- or en-dashes or other symbols in place of bullets, numbered lists, and nonbulleted lists—and it applies whether the items are full sentences, clauses, phrases, or single words.

The rule applies to the following types of indented lists:

- Lists marked with bullets (•), numbers, or other symbols (such as >) that are equivalents of bullets.
- Lists marked with em (—) or en (–) dashes.
- Lists that are indented but that lack initial markings.

Note: This rule generally has not been applied in this style manual so that fragmentary samples can illustrate desired combinations of uppercase and lowercase letters.

Proper Names

Capitalize proper names, also known as proper nouns.

Many authors feel a need to treat a common noun (the type of noun that identifies one or all of the members of a class of persons, places, things, qualities, or actions) as a proper noun (the type of noun that identifies a unique person, place, thing, quality, or action) because the author is writing about the thing or things a common noun represents. For example, an author discussing activities at a forward operating base in Afghanistan may feel a need to capitalize *forward operating base* because that type of thing is the focus of the author's attention. Nevertheless, the noun (or noun phrase) remains a common noun—and should not be capitalized—unless the author uses the name of a specific item from the class (a proper noun), such as *Forward Operating Base Kala Gush*.

Capitalizing Plurals

Capitalize the plural form of a common noun when it follows the proper adjective portion of two or more proper names.

Baltic and Black Seas
Tigris and Euphrates Rivers
Helsinki and Turku Naval Bases
Helmand and Kandahar Provinces

Forward Operating Base Kala Gush
but a forward operating base; three forward operating bases

Ninawa Reconstruction Team
but a provincial reconstruction team; two provincial reconstruction teams

Karbala Provincial Council
but a provincial council; affecting all provincial councils

UN Security Council Resolution 1600
but a UN Security Council resolution; UN Security Council resolutions

Most decisions on capitalizing names are concerned with common nouns that occur as parts of proper names, derivatives of proper names, and particles with names.

Common Nouns in Proper Names

Capitalize common nouns as parts of proper names but *not* when the common noun is separated from the rest of the name by a word or phrase or when the common noun stands for the name of the place or thing.

- The Persian Gulf is an exception because of its prominence in military writing. Thus, we write "the Gulf War," "Gulf states," etc. Use lowercase for *gulf* as a common noun referring to any other gulf—for example, "Operations in the Gulf of Aden have increased because of pirates' activities in the gulf."

Quebec Province; Province of Quebec; Quebec, Canada's separatist province; the province
the Panama Canal; the canal
the Volga River; the river
Volgograd Command Post and Barracks; the command post; the barracks in Volgograd
Gwadar Port; the port
Puerto Quetzal; the port
Target Intelligence Conference; the conference
the Gulf of Aden; the gulf
the English Channel; the channel
Korean Peninsula; the peninsula

Capitalize *treaty* when it is part of the proper noun title or shortened title of a signed treaty; however, use lowercase for the word *treaty* when it is part of the name of an agreement that is not yet signed. Use lowercase for *treaty* when it stands alone for an agreement.

the Conventional Armed Forces in Europe Treaty; the CFE Treaty; the treaty
A conventional forces in Latin America treaty has never been developed.
The treaty was signed in 1973 but was not approved by the legislatures of all participating nations until 1984.
treaty-limited equipment

Use lowercase for *constitution* in most cases; use initial capitalization only when referring to the U.S. Constitution.

Derivatives of Proper Names

Capitalize the proper name portion of names that retain an association with their origin.

Bailey bridge [a bridge type]	Internet websites	neo-Stalinism
Castroite sympathies	Islamization	Patton tank
degrees Celsius	Leninist doctrine	Ponzi scheme
degrees Fahrenheit	Marxism	Trojan horse
Doppler effect	Morse code	World Wide Web

Use lowercase for derivatives of proper names when they have acquired independent meanings. (The U.S. Government Printing Office *Style Manual*, available on NIPRNET, contains a more extensive list.)

anglicize	india ink	pitot tube
angstrom unit	italicize	plaster of paris
arabic numerals	italic type	quisling
arctic clothing	jeep [as vehicle type, not trade name]	quixotic
artesian well	joule	quonset hut
bohemian	macadamized road	roentgen

bowie knife	mach	roman candle
braille	madras cloth	roman numerals
degaussing	manila envelope	roman type
diesel engine	mason jar	sanforize
fuller's earth	mecca [as place of interest, not city]	utopia
gargantuan	molotov cocktail	vaseline
gauss	neon light	venturi tube
german silver	newton	vulcanize
gothic type	pasteurize	watt
herculean task	philistine	website
holland cloth	pitman arm	zeppelin

Capitalize trade names that have not been forced into the generic language. However, unless you know a particular item is the genuine trade article, you'll do better to substitute the generic term.

air-cushion vehicle or hover craft [unless it is a real Hovercraft]
fiberglass [unless it is Owens-Corning Fiberglas]
a copy or photocopy [unless it is a Xerox copy]
a vacuum container [unless it is a real Thermos]
clear thermoplastic sheet [unless it really is Plexiglas]

Use lowercase for international and national currencies, even though a number of them may appear to be based on proper names, such as the euro, the bolivar, and the balboa.

afghani	dollar	peso
balboa	euro	pound
bolivar	franc	ruble
deutsche mark	lira	rupee

Particles With Proper Names

Capitalize *the* or its equivalent in a foreign language when it is part of an official name. When the name is used as an adjective, an uncapitalized *the* may precede it—despite the redundancy for a non-English name.

The Hague; the Second Hague Conference
El Salvador; the El Salvador situation
The Bahamas; the Bahamas Tourist Office
The Gambia; the Gambia mapping project

For many place names, convention calls for a lowercase *the*, especially with names of regions, island groups, rivers, and mountain ranges; place names that are in plural form; and place names that are adjective-noun compounds.

the North Caucasus	the Ural Mountains
the Midwest	the Netherlands
the Spratly Islands	the United States
the Tigris River	the United Kingdom

Do not capitalize *the* when it begins the name of a newspaper or other periodical; the name of a vessel, aircraft, or train; or the name of a firm. This rule applies even though *The* may appear as part of a newspaper's name on its masthead, as part of a vessel's name, or as part of a business's name.

the *Washington Post*
the *Times*
the *Los Angeles* [proper name of a ship]
the Hershey Company

In many European names, *d', de, della, den, du, la, l', van, vander, von,* and so forth normally are not capitalized except at the beginning of a sentence. The convention for the same particles for individuals born in English-speaking countries varies widely; try to find out how the individual capitalizes his or her name, but use the lowercase form if that information is not available.

Arabic Persons' Names. When *al-* is part of a person's name in Arabic, include the *al-* when writing out the individual's full name the first time, as in "DIA judges that Iraqi Prime Minister Haydar al-Abadi will modify the plan." For subsequent references to the same individual, drop the *al-*, as in this secondary reference in the same paper: "Diplomats have noted that Abadi expects the plan to include three phases." Also, note the hyphen with the *al* in "Haydar al-Abadi":

> Intelligence Community (IC) guidance requires first that IC agencies follow spellings of individuals' names as they appear in *The World Factbook* no matter what transliteration practices might indicate. For the many Arabic names that do not appear in *The World Factbook*, IC guidance directs that agencies follow an IC standard for transliteration of Arabic. This standard calls for hyphens to "connect name elements within a name," as in "Abd-al-Rahman" and "Abu-al-Bashar." However, hyphens are not used in names that include *Allah* as part of the name (as in "Abdallah" or "Nasrallah") or names marked by the lineage/family marker *Al* (as in "Al Saud"), though this latter situation is rare and occurs mostly with names of individuals in Gulf Arab royal houses.
>
> *The World Factbook* is available on JWICS at <https://www.cia.us.qlat/DI/Factbook/index.html>.

Arabic Place Names. Presentation of *al* and similar elements associated with place names in Arabic follows different rules—those of the Board on Geographic Names (BGN), which the National Geospatial-Intelligence Agency (NGA) uses for most of the Middle East. For Arabic place names, *al* appears with an uppercase A, and no hyphen joins *Al* to the rest of the name, as in "Al Basrah" and "Al Qanbariyah" in Iraq.

> A further difference exists between the IC standard for presenting Arabic personal names and the BGN's standard for spelling Arabic place names that include *al*. The IC standard for personal names transliterates the definite article *al* as it is *written* in Modern Standard Arabic (MSA)—*alif lam*. The BGN transliterates the definite article *al* in place names as it is *pronounced* in MSA. In MSA pronunciation, *al* is "assimilated" when followed by one of the 14 "sun letters." When preceding the letter *nun*, for example, *al* is pronounced "an"—*alif nun*. Therefore, the BGN renders an Iraqi city as "An Najaf" rather than "Al Najaf." Similar examples are "As Sulaymaniyah," "Ar Ramadi," "Ash Shamiyah," "Ad Diwaniyah," and so forth.
>
> NGA maintains a searchable database of place names using BGN standards on NIPRNET: <http://www.geonames.nga.mil/namesgaz/>. Search this database with "Options" set for "No Diacritics" and "BGN Standard" when you are seeking only BGN-approved spellings of place names.

Arabic Business/Organization Names. For names of businesses or business-related organizations with Arabic portions in their names, follow the presentation style for *al-, al, Al,* or *Al-* as that element appears in the source of the information. Businesses and business-related organizations use a variety of styles for presenting such an element, as company literature, business websites, and business directories demonstrate. If multiple sources show conflicting styles for the same business or organization and you have no way of finding out what the company or organization itself prefers, use *Al-* as the default.

Dresser Al-Rushaid Valve & Instrument Ltd	Dallah al Baraka Group
Ras Al Khaimeh Gas Commission	Dr. Al-Oufi Law Firm

A'amal Al Nashi Transportation Est.
Al-Arabiyah [television network]
Al-Furat [television network]

A M Al Khorafi Est.
Al Jazeera [television network]
Al-Furat [newspaper]

Arabic Names Occurring Within Sentences. When an Arabic name with *al-* as part of the name begins a sentence, the first letter of *al-* must be capitalized. However, when a name with *al-* as part of the name occurs within a sentence, keep the *al-* in its lowercase form. Of course, if *Al* has initial capitalization, as in a place name, the *Al* will have initial capitalization whether it begins a sentence or occurs within the sentence.

Al-Qaida in Iraq had maintained a presence since....
When al-Qaida in Iraq sent fighters into....
Operations in Al Basrah began during....

Arabic Names in Titles or Headings. When an Arabic name with *al-* as part of the name appears in a title or heading, keep the *al-* in lowercase form unless the name begins the title/heading or appears immediately after a colon that connects a subtitle/subheading to a main title/heading:

Al-Qaida in the Arabian Peninsula Resizing Its Forces in the South
A Volatile South: Al-Qaida in the Arabian Peninsula Resizing Its Forces
Iraqi Government Operations Against al-Qaida Fighters

Organized Bodies

Governmental Bodies

Capitalize the proper name of a *national* governmental body as well as the shortened form of the proper name. Use lowercase for generic equivalents of the proper names and for shortened forms of the names of administrative bodies.

the U.S. Congress; the Congress; a congressional delegation
the British Parliament; the Parliament; the British legislature
the Colombian Congress; the Congress; the Colombian legislature; the Colombian parliament
the Icelandic Althing; the Icelandic parliament; the Icelandic legislature
the Ecuadorian National Congress; the Congress; the legislature
the Austrian Federal Assembly; the congress; the parliament
but the Pakistani Ministry of Law and Justice; the ministry
the Mexican National Public Safety Council; the council

Use lowercase for *government* (except *U.S. Government*) or its equivalent and for *administration*.

the U.S. Government; the British government; the government of Italy; the national government; the Brown government; the government; the Obama administration; the administration

For the United States only, use initial capitalization for *Cabinet*.

the U.S. Cabinet; President Obama's Cabinet; the Cabinet

Parliament
Capitalize *Parliament* if it is the actual name of a country's legislature, but use lowercase *parliament* if the legislature actually has a different name. Check *The World Factbook* if you are uncertain about a legislature's proper name.

For the United Kingdom and the Commonwealth of Independent States, capitalize *Commonwealth* as part of the proper name and standing alone as a substitute for the full name.

the British Commonwealth; the Commonwealth; Commonwealth negotiations
the Commonwealth of Independent States; the Commonwealth; Commonwealth military issues

For *subnational* governmental bodies, capitalize only the full proper name; avoid shortened forms that might be confused with shortened forms of national equivalents.

the Commonwealth of Virginia; the commonwealth
the Maryland House of Delegates; the state legislature
the Quebec Parliament; the provincial parliament
the Jerusalem Municipal Council; the municipal council
the Karbala Provincial Council; the council

Military Forces

The names of a nation's military and police forces or services depend on how the nation's forces are structured. Do not assume that a nation's force names mirror those of the United States.

For the United States, capitalize *Armed Forces* when the term appears with the nation's name, but use lowercase if the name is separated from it.

the U.S. Armed Forces; the Armed Forces of the United States; the capabilities of the U.S. Armed Forces
but The capabilities of the armed forces have improved.

For the rest of the world, use lowercase for *armed forces*, unless *armed forces* is part of the proper name.

the Argentine armed forces; the armed forces of Argentina; the armed forces
the Lebanese Armed Forces; the armed forces

Note: This guidance also applies when an acronym is being established for use in subsequent references to the military:

The structure of the Argentine armed forces (AAF)....

Capitalize the full proper name of a military force, military service, or national police force as well as a shortened form of the proper name. Use lowercase for generic terms related to force names and for names of forces that are being considered but that have not yet been developed. Terms such as *army, navy, air force,* and *marines* will be generic labels if a nation's proper names for its forces use other terms or if a nation's military structure is too small to include a developed army, navy, and so on.

the U.S. Army; the Army; Army fighting vehicles [controlled by the U.S. Army]
the U.S. Navy; the Navy; Navy surface ships [controlled by the U.S. Navy]
but naval; naval weapons [generic reference]; naval vessels [generic reference]
the U.S. Marine Corps; the U.S. Marines; the Marines; a Marine; a Marine landing craft [controlled by the U.S. Marines]; a marine amphibious craft [generic reference to a vessel type]; development of marine tactics [generic reference]
the U.S. Air Force; the Air Force; Air Force fixed-wing aircraft and helicopters [controlled by the U.S. Air Force]
the U.S. Coast Guard; the Coast Guard; a Coast Guard rescue vessel [controlled by the U.S. Coast Guard]
the Egyptian Army; the Army; the Egyptian ground forces; army equipment [generic reference to an equipment type]; army, division, or regiment level
the People's Liberation Army; the PLA; the Chinese Army; the Army; Chinese ground forces; the People's Liberation Army Air Force; the Air Force
the French Navy; the Navy; naval units [generic reference]; naval combatants [generic reference]

the Royal Air Force; the Air Force; an Air Force pilot [controlled by the Royal Air Force]
the Syrian Arab Air and Air Defense Forces; the Air and Air Defense Forces; Air Defense units [controlled by the Syrian Air and Air Defense Forces]; air defense guns and missiles [generic reference to weapon types]
the Spanish Guardia Civil [the Spanish form of the proper name]; the Spanish Civil Guard [the English equivalent for the proper name]; Spain's national police; the national police
the Barbados Coast Guard; the Coast Guard; the navy of Barbados
the Jamaica Air Wing; the Air Wing; Jamaica's air force; the air force

The Russian military has six combat arms: the Ground Forces, the Navy, the Air Forces, the Airborne Troops, the Strategic Rocket Forces, and the Space Troops. In this structure, *army* is a generic reference:

the Russian Ground Forces; a Ground Forces unit; the Russian army; an army unit

Use lowercase for shortened forms of individual unit names.

the 1st Army; the army
the 6th Fleet; the fleet
the 1028th Brigade; the brigade
I Corps; the corps

Use lowercase—other than for proper names—for military services as a group, for general references to one kind of service in the plural form, or for the plural form of a military service type for more than one country.

the British military establishment
NATO naval forces; NATO navies
Central European air forces
British-supplied air force, naval, and ground equipment
but Greek and Turkish Navies; British, Indian, and French Air Forces [the plural form of the common noun following the proper adjective portion of two or more proper names]
the armies of the United States and the United Kingdom

U.S. Military Services and Combatant Commands

For the U.S. military, use initial uppercase for *Military Service(s)* but lowercase for *service(s)*, *unified command(s)*, *specified command(s)*, and *combatant command(s)*.

Do not capitalize these terms in connection with the militaries of other countries or for U.S. commands below the combatant command level (except as part of the full name of a command).

International Organizations

Capitalize the full proper name of an international organization and its subelements; use lowercase for shortened forms of the names and for use of the terms in general senses.

the UN General Assembly; the assembly
the International Bank for Reconstruction and Development; the bank
representatives from a number of international banks

Diplomatic and Consular Units

Capitalize the name of a specific embassy, mission, or consulate. Use lowercase for shortened forms of those words and for their use in general senses—except for U.S. diplomatic entities, which should appear with initial capitalization.

the British Embassy in Washington; the embassy
the French Consulate in New York; the consulate

reports from African embassies
members of diplomatic missions
the U.S. Embassy Rome; the Embassy; the U.S. Consulate General Naples; the U.S. Consulate in Naples; the Consulate; the U.S. Mission; a spokesman for the Mission

DIA-Specific Capitalization

This manual is consistent with the DIA *Correspondence Guide* on initial capitalization for several terms used frequently in correspondence and in papers dealing with DIA structural issues related to analysis.

The Agency

Use initial capitalization for *Agency* when it is a substitute for the "Defense Intelligence Agency."

- Use initial capitalization for *Federal* (as in "Federal agencies"), *Government*, and *Nation* for passages dealing with the United States only.
- Capitalize *Directorate*, *Office*, and *Center* when discussing those specific DIA structural elements, but use lowercase for generic senses. Do not capitalize *division*, *branch*, *section*, or *team* unless they are part of the full name of an Agency element.
- Use initial capitalization for *Defense* when referring to the U.S. Defense Intelligence Community: "developments in Defense Intelligence"; "Defense initiatives"; "the Defense Intelligence Enterprise"; "the Defense Intelligence Community."

Political Parties and Philosophies

Party Names

Capitalize the full or shortened name of a political party, but not the word *party* standing alone.

the Chinese Communist Party; the CCP; the Communist Party; the party
the Italian Socialist Party; the Socialist Party; the party

Philosophies

Capitalize words referring to members of organized parties, but use lowercase for words referring to political philosophies and their adherents.

a Socialist; a Communist; a Liberal; a Labourite; a Conservative; a Tory; a Christian Socialist [party members]
a British socialist belonging to the Labour Party
Eurocommunism; noncommunist countries; communist countries; anticommunist movement; a procommunist organization; a communist party called the Socialist Unity Party
liberal parties of Western Europe
but Christian Democrat, Christian Democracy, and Christian Democratic
[The *D* is capitalized as well as the *C* to prevent confusing adherents of Christian Democracy with Christians who adhere to democracy.]

Religious Terms

Capitalize names of religions, specific religious bodies, and terms for religious adherents and their writings.

Christianity
Catholicism
Catholic Church; the Church
the Bible; Biblical text
a Protestant
Judaism
Talmudic scholar
Quranic law
a Muslim
an Islamist
the Musa Qala Shura
but shura members
Ansar al-Sunnah Sharia Council
but sharia law; sharia court; a sharia council

Use lowercase for religious terms used in nonreligious senses.

a bible for intelligence writing
her catholic approaches to English usage

Geographic Terms

Use lowercase for terms denoting direction or position on the Earth.

north	northerly	northern Norway
west	north-northwest	the polar region
southwest	east coast	polar icecap
eastward	southern France	

Capitalize geographic terms for definite regions and geographic features. For political or administrative groupings, capitalize the term for the political/administrative grouping when it is used with a geographic term to form a proper name—for example, *province* in Kandahar Province or *governorate* in Diyala Governorate—but use lowercase for the political or administrative term when it is used generically—for example, in "European countries," "the Maghreb states," "Afghan provinces," and "Iraqi governorates."

the North Atlantic	Korean Peninsula
the West	Gaza Strip
the East	East-West dialogue
the Western Hemisphere	Mediterranean coast
the Middle East	Midwestern states
the Continent [continental Europe]	Western countries
Caribbean Basin	Persian Gulf states; Gulf states
North Pole	Baltic states
Holy Land	former Soviet republics
Equator	Helmand Province
San Andreas Fault	An Najaf Governorate
North and South Poles	South Sudan
	but northern Sudan

For individual studies, particular attention may be focused on a locality, and a name may be coined to distinguish that locality; in such a case, capitalize the coined name. This capitalization does not apply to general references to localities.

the cocaine industry in Peru's Upper Huallaga Valley [designating a particular locality for focused attention]
but farming along the lower Orinoco [a general reference to a locality]

Capitalize geographic terms used to divide the world into groups of countries for intelligence writing.

Middle East; Middle Eastern	Western Europe; West European
North Africa	Eastern Europe; East European
Sub-Saharan Africa	Central Europe; Central European
West Africa	Latin America
East Africa	Middle America
South Asia	Central America
East Asia	*but* southern Afghanistan
Central Asia	central Russia
	northern France

Capitalize the names of the celestial bodies the Sun, the Moon, and the planets (including, of course, the Earth). When the name of one of these bodies is used in a sense not associated with its being a celestial body, use lowercase.

Earth orbit; near-Earth orbit; orbit the Earth; position on the Earth; the Earth's crust;
but digging in the earth [here *earth* is equivalent to *dirt*, not the name of the planet]
Moon landing, moonlight
orbit the Sun, the Sun's rays; sunshine

Use lowercase for descriptive geographic terms.

tropical temperature
arctic conditions; arctic nights
polar exploration

Nationalities, Tribes, and Other Groups of People

Capitalize the names of racial, linguistic, and religious groupings, but use lowercase for terms based on racial origin, color, or local usage. In most cases, lowercase the word *clan*; capitalize it only in the Scottish context when preceding the clan name.

African-American
Indo-European
Jewish
Maori
Native American
Darod clan
Shia; Shiite
Sunni
aborigine
black
white
but Clan MacArthur

Coined Names

Capitalize full proper forms of coined names for military, economic, political, or other groupings. Use lowercase for the shortened forms of the names and for generic references.

the former Warsaw Pact; the pact; pact countries
the North Atlantic Treaty Organization; NATO; the alliance; allies; allied
the European Community; the community
the European Union
the Big Four
the Muslim World; Muslim countries
the Arab World
the former Soviet Bloc; the bloc
Six-Party Talks
the Developing World
the Greens
the Intelligence Community [U.S.]; the community
the Defense Intelligence Community [U.S.]; the community

Capitalize holidays, religious feasts, and names coined to designate historic or political events.

New Year's Day
the New Year
the Feast of the Passover
the Great Leap Forward
the Holocaust
the Battle of the Bulge
the Islamic Revolution
the Great Depression
the Rose Revolution
the New Deal

Capitalize the names of wars, including coined names designating wars, but use lowercase for the word *war* when it stands alone or is used in a generic sense.

World War II
post-World War II
World War I
the Civil War
the Six-Day War; 1967 Arab-Israeli War
the Yom Kippur War; the October War
the Korean War
the Vietnam War
the Iran-Iraq War
the Cold War
the Global War on Terrorism
the first Persian Gulf War; the first Gulf War; the first Iraq War
but the war; in the second world war; during two world wars; a civil war

Titles of Persons

When an individual's title *immediately precedes* the person's name, capitalize the title. However, when the title follows the name, including being in apposition to it, or replaces the name, use lowercase for the title. Do not confuse a description with a title. Similarly, capitalize only valid titles; use lowercase for terms identifying illegitimate actors.

Prime Minister David Cameron; Prime Minister Cameron; the prime minister
Defense Minister Juan Carlos Pinzon; Defense Minister Pinzon; the defense minister; Juan Carlos Pinzon, Colombia's defense minister
a meeting of the defense ministers of all the region's nations
special emissary Habib
al-Qaida emir Zawahiri
Taliban shadow governor Salam

The U.S. President

For U.S. presidents only, capitalize *President* except when using the term in a general sense or in a general reference to a group of U.S. presidents.

President Barack Obama; President Obama; Barack Obama, the U.S. President; the President
but a meeting of all living U.S. presidents; the presidential election

Chief of the Defence Staff Lt Gen Thomas Lawson; the chief of the Defence Staff; Thomas Lawson, the chief of the Defence Staff; the Defence Staff chief; the chief
Chilean Army Commander in Chief Gen Juan Miguel Fuente Alba; Commander in Chief Gen Fuente Alba; the commander in chief; Gen Fuente Alba, the commander in chief of Chile's Army
101st Airborne Division Commander Maj Gen James McConville; Maj Gen James McConville, commander of the 101st Airborne Division; the division commander; the commander
but the Supreme Allied Commander, Europe; the commander
the Chairman, Joint Chiefs of Staff [U.S.]; the chairman; the general

In official correspondence, use initial capitalization for titles of high-level officials, with or without a name.

the Deputy Under Secretary of Defense for Policy
but the workforce development program manager

Capitalize *Acting* if it is part of an official title. Use lowercase for *former*, the prefixes *ex-* and *then-*, and the suffixes *-designate* and *-elect*.

Acting Party Chairman Spelling; the acting party chairman; the acting chairman
former Communist Party General Secretary Gorbachev; former party chief Gorbachev
Prime Minister-elect Fields; the prime minister-elect
then-President Shorter; the then-president

Titles and Headings

For titles of publications (books, journals, magazines, newspapers, newsletters, reports, etc.), articles in publications, television and radio programs, sections, chapters, headings, figures, tables, and headings and subheadings within tables, follow these guidelines:

- Capitalize the first and last word and the first word following an em-dash or colon; nouns, pronouns, verbs (including the *to* of an infinitive), adjectives, adverbs; prepositions and conjunctions longer than three letters; and parts of compounds that would be capitalized standing alone.
- Use lowercase—except for the first or last word or the first after a colon or em-dash—for the articles *a, an,* and *the;* prepositions shorter than four letters (*at, by, for, in, of, on, to,* and so on); conjunctions shorter than four letters (*and, as, but, if, or, nor*); and the second element of a compound numeral.

Spotting Terrorists: What To Look for and Where To Look
Warlords and Other Militant Leaders
Pacific Alliance—The United States and Japan
"Nothing but Trouble: Divisions Within the Party"

Cross-References

In cross-references, use initial capitalization for the common noun portion of numerical or letter designations of chapters, parts, sections, phases, stages, graphics, tables, appendixes, and so on.

covered in Chapter 3
included in Appendix B
expected in Phase 3
(see Figure 13)
detailed in Table 5

Word Equivalents of Abbreviations/Acronyms

The capitals used for an abbreviation—including an acronym—do not necessitate capitals for their word equivalents. If the abbreviation/acronym is for a proper name, use capitals for the words; otherwise, use lowercase.

the Strategic Arms Reduction Treaty (START)
the Intermediate-Range Nuclear Forces (INF) Treaty
a treaty applying to all intermediate-range nuclear force (INF) operations within ground-controlled intercept (GCI) coverage

Emphasis

Avoid using capitals for emphasis. Boldfaced type, italics, and placement (centering or indenting) are more effective, less distracting means to provide emphasis.

Seasons

Use lowercase for the seasons of the year. [*Note: the … of* is not necessary in passages dealing with a season of a specific year: *not* "a conference in the spring of 2007," *but* "a conference in spring 2007."]

a meeting in summer 1999
no later than fall 2008

Military Equipment Designators

Use initial capitalization for the nicknames for aircraft, ships, and other weapon systems, including NATO-designated nicknames for military equipment. Use *class* with the name of a class of ships to indicate that the name is for the entire class, not just the first ship from the class; however, *class* is

optional when context makes clear that a name is for the ship class. Use italics for the proper name (but not the type or class) of an individual ship, aircraft, or spacecraft; do not use italic type for the nation indicator when you include it with the proper name.

Yankee class submarine; two Yankees; Polaris class submarine; Polaris submarine
Sovremennyy class guided-missile destroyer; Sovremennyy destroyer
MiG-29 Fulcrum fighter; L-39 Albatros
AA-10 Alamo air-to-air missiles
Tu-22M Backfire bomber
Ka-25 Hormone helicopter
SA-4 Ganef surface-to-air missile
Scud surface-to-surface missile
Knife Rest radar
Alouette III helicopter
HMS *Ark Royal*; USS *Enterprise*; the *Spirit of St Louis*
the Kiev class aircraft carrier *Admiral Gorshkov*; the *Admiral Gorshkov*; the *Gorshkov* task group
the *Soyuz-3*; the latest Soyuz TMA spacecraft
the Concorde; a Leopard tank

Military Exercises, Operations, and Special Projects

Use all uppercase for codenames or covernames assigned to military exercises, operations, and special projects or programs.

during Exercise SOYUZ-85; the SOYUZ-85 exercise
Exercise ULCHI FOCUS LENS
Operation ENDURING FREEDOM
the STONE'S THROW test project
BYZANTINE HADES information

Academic Degrees

Use initial capitalization for the names of academic degrees, but use lowercase for references to degrees in a general sense.

Doctor of Law; Doctor of Veterinary Medicine; doctor's degree in law; doctorate
Master of Arts in English; Master of Arts in the humanities; master's degree in education
Bachelor of Science in computer science; bachelor's degree
associate's degree in communication applications

Chemical Elements and Isotopes

Show the names of chemical elements and compounds in lowercase as words but with initial uppercase for chemical symbols. (By international agreement, in technical symbology the mass number of an isotope appears in superscript form to the left of the symbol for the element; that is, technically the symbol for uranium-235 is ^{235}U. However, for less technical writing, such as intelligence papers, the more common rendering of the symbol is U-235.)

sodium chloride; NaCl
sodium citrate; $Na_3C_6H_5O_7.2H_2O$
uranium; U; uranium tetrafluoride; UF_4; uranium hexafluoride; UF_6
uranium-235; U-235; uranium-238; U-238

Plant and Animal Genus and Species

Use uppercase for a plant or animal genus and lowercase for the species (even in titles and headings). (Both genus and species also appear in italics.) After the first use of a genus, it can be abbreviated (but it remains uppercase and italic). Higher divisions of plants and animals—phylum, class, order, and family—are capitalized but shown in roman type.

Clostridium botulinum; C. botulinum [on subsequent use]

Giardia lamblia; G. lamblia [on subsequent use]

Escherichia coli; E. coli [on subsequent use]

Anthropoda [phylum]

Mammals; Mammalia [class]; destruction by some sort of mammal [generic reference, not a reference to the class]

Rodentia [order]

Hominidae [family]

CHAPTER 4: Numbers

It is stylistically poor to begin a sentence—or a paragraph—with a numeral *<1997 saw the publication of no fewer than 3,700 mystery novels>*. Some journals, such as *The New Yorker*, would make that sentence begin, *Nineteen ninety-seven saw. . . .* But most writers and editors would probably simply begin the sentence some other way, as by writing, *In 1997, no fewer than 3,700 mystery novels were published.*

—Bryan A. Garner, *A Dictionary of Modern American Usage*

CHAPTER 4: Numbers

Numbers can appear in writing as numerals (numeric symbols, like 1, 2, 3 or I, II, III) or as words or groups of words. Most rules for presenting numbers have to do with determining which form—numerals or words—is more appropriate for a particular situation. This chapter provides a set of basic rules that cover most circumstances and other rules for special situations or factors related to using and presenting numbers.

Writers sometimes try to reduce guidance for using numbers to only two rules: spell out numbers below *x*, but use numerals for numbers *x* and above. As appealing as that logic is in its simplicity, it just does not account for the variety of situations in which writers use numbers in their text and tables. As cumbersome as the rules in this chapter may appear at first, they provide a logical and consistent appearance for numbers in publications.

As *The Chicago Manual of Style* points out, several factors affect whether numbers should appear as numerals or words:

- The size of a number (our most basic rule has to do with whether a number is less than 10 or equal to or greater than 10).
- The kind of entity a number represents (another basic rule deals with units of measure, time, or money).
- Whether a number is exact or indefinite (we treat numbers differently if they are nonliteral or indefinite).
- The context in which a number appears (for example, a number that starts a sentence receives special treatment, and we vary treatment of numbers somewhat when they appear in tables rather than text).

The basic rules and all of the variations of the basic rules are related to these factors.

Basic Rules

1. **Except at the beginning of a sentence, show numbers 10 or greater as numerals.** If a number is the first word of a sentence, however, spell it out.

   The job took 12 workers 30 days.
   Forty-three workers built the bridge.

- We make an exception for a number that is the first "word" of a sentence or sentence fragment in a comments or remarks field in a table. Such a number can appear as a numeral rather than a word. See "Numbers in Tables" below for an illustration of this exception.

2. **Except for units of measurement, time, and money, spell out numbers less than 10.**

   The shipment consisted of three tanks and two armored personnel carriers.

3. **For specific units of measurement, time, and money, use numerals, regardless of whether a number is less than, equal to, or greater than 10.** (Rules related to those types of numbers will be treated in greater detail following these basic rules.)

   In the past 11 years, no new incidents have occurred.
   In the past 3 years, no new incidents have occurred.

4. **When numbers 10 or greater are mixed with numbers less than 10, follow either rule 4a or 4b below for numbers within a sentence.** The rule that applies depends on whether any of the numbers are for measurements, time, or money.

   a. When a sentence contains both numbers less than 10 and numbers equal to or greater than 10, use numerals for all the numbers. The following examples have both numbers less than 10 and numbers equal to or greater than 10, but none of the numbers are for measurements, time, or money.

      The attack involved 60 soldiers, 5 tanks, and 2 helicopters.
      The attack involved five tanks and two helicopters.

In the first example, *5* and *2* are numerals because of the *60* in the same sentence. In the second example, *five* and *two* are words because the sentence does not contain a number 10 or greater.

b. Units of measurement, time, and money—which should appear as numerals—do not affect the other numbers in a sentence and are not affected by them. Those other numbers continue to follow rule 4a above.

> In the past 11 years, only two attacks and seven casualties have occurred.
>
> In the past 11 years, 2 attacks and more than 120 casualties have occurred.
>
> In the past 3 years, 2 attacks and more than 120 casualties have occurred.
>
> In the past 3 years, only two attacks and seven casualties have occurred.

The *11 years* (a measure of time), though greater than 10, does not affect the form of the other numbers in either of the first two sample sentences. In the third sample, the *120* does not affect the *3 years*; the numeral *3* is appropriate simply because it is for a measure of time. In the first sample, *two* and *seven* are words because each of them is less than 10 (and *11 years* has no bearing on the form in which those numbers appear). In the fourth sample, *3 years* has no bearing on the form for the other numbers in the sentence, which are words because both of them are less than 10. In the second and third samples, both *2* and *120* are numerals because of the *120* in each sentence.

Turning Off Superscripting for Ordinal Numbers

Word 2007's default autocorrection settings automatically superscript the endings of ordinal numbers as you type unless you turn this feature off. To turn it off, follow these steps:

1. Click on the "Word Options" selection at the bottom of the drop-down box that appears when you select the round Microsoft Office logo, which is in the upper-left corner of all Word ribbons.
2. Select "Proofing" in the list at the left side of the "Word Options" drop-down box.
3. Select "AutoCorrect Options," near the top of the available selections.
4. Select the "AutoFormat" tab in the drop-down box.
5. Deselect "Ordinals (1st) with superscript" and click on "OK."
6. Select the "AutoFormat As You Type" tab in the drop-down box.
7. Deselect "Ordinals (1st) with superscript" and click on "OK."
8. Click on "OK" in the "Word Options" box to clear it from your screen.

This will prevent Word from putting the endings of ordinal numbers in superscript form as you type. It will not automatically change superscripted ordinals that have been saved in a document, but it will make correcting text easier.

However, spell out a number less than 10 if it is clearly unrelated to the other numbers in a sentence.

> At one hearing, all 15 local members of the group pressed for a 1-week delay to allow members from outside the country to arrive.

Other Number Rules

Ordinal Numbers

Ordinals indicate order in a series: 1st, 2nd, 3rd, 4th, etc. The basic rules generally apply to ordinal as well as cardinal numbers (1, 2, 3, etc.)—except for designators for military units. However, when ordinal and cardinal numbers appear in the same sentence, the basic rules apply to each type of numeral independently: ordinals do not affect cardinals, and cardinals do not affect ordinals.

> The third group contained two items.
>
> The third group contained 12 items.
>
> The 3rd and 10th groups contained three items each.
>
> The 3rd and 10th groups contained 3 and 11 items, respectively.

- Ordinal numbers should appear with the *nd, rd, st,* or *th* portion on the line, rather than in superscript form ("22nd" rather than "22nd").

Military Unit Designators. Except for the exceptions below, present the designators for foreign military units using arabic numerals (rather than roman numerals or words) and in ordinal form (for example, "the 115th Infantry Division" rather than "the 115 Infantry Division"). Use these presentation forms no matter how the foreign military itself presents the designators. Abbreviating the word portion of unit designators is acceptable in tables and graphics when space is a limitation, but write out the words in text.

323rd Fighter Wing
451st Motorized Rifle Division

- Exception 1: Use roman numerals for U.S. Army corps (but not for foreign corps).

XII Corps
XVIII Airborne Corps

- Exception 2: In text, use words for China's Second Artillery Corps.

Numbers in Tables

Except within footnotes to a table, all numbers within a table will be numerals, even if the table contains textual remarks. If a remarks or comments column contains sentences or sentence fragments, those can begin with numerals (see the final portion of the second remarks entry in the following sample). Within footnotes to a table, however, follow the basic rules for numerals in text, and do not begin sentences with numerals.

Wharf Reference	*Months*	*Cargo-Handling Equipment*	*Remarks*
South Pier	Breakbulk 2G	2 mobile jib cranes; [1] portal jib crane	Discharge 680 t/d breakbulk.
North Pier	Container 36-C	2 straddle cranes	Discharge 10,000 t/d container. 30-meter RO/RO ramp planned.[1]

[1] Currently the port has no RO/RO capability. Construction of one ramp here and two at nearby Port Manatil will open the country's Pacific coast to RO/RO shipping.

Numbers at Beginnings of Sentences

If you cannot avoid beginning a sentence with a number, spell it out. That spelled-out number, however, will have no effect on the form (numeral or word) of other numbers in the same sentence; they will continue to follow the basic rules as if the opening number did not exist.

Fifty kilometers away, rising to 3,500 meters, is Mount Finch.
Fifty kilometers away, along a 7-km ridge line, were three guerrilla bases.

Metric Units

In response to U.S. public law, DIA has used metric units for most measurements since 1976. The International System of Units (SI), which we commonly call the metric system, is the standard for scientific disciplines, is used commonly among the Military Services, and is the standard of allies with whom we collaboratively produce products and to whom we release intelligence.

Preferences exist for which units are to be used with which quantities. In addition, some nonmetric units still are appropriate.

- Cubic meters and kilograms are preferred for volume and mass, but liters and metric tons are preferred for fuel capacity and bulk mass (wheat, coal, and others). Bushels, barrels, and barrels per day may be used.
- Use square meters for floor areas within buildings and for other covered structures, including caves, and small open-air storage areas less than 10,000 square meters. Use hectares for large open storage areas (equal to or greater than 10,000 square meters, since 1 hectare equals 10,000 square meters) and cropland (except for small gardens), forests, etc. Use square kilometers for land areas of large political units (urban areas, districts, provinces, states, countries, etc.), for areas of military operations, and for enclosed bodies of water (unless the body of water is so small, as with a pond, that showing square meters is more appropriate).
- Use kilotons and megatons for nuclear weapon yields.
- Weights for standard U.S. bombs usually are given in pounds rather than kilograms—for example, "a 5,000-lb penetrating warhead."
- Use degrees (rather than radians) for azimuth, beamwidth, inclination, reentry angle, and other angles for which degrees customarily have been used.
- For very short distances and very small pressures, use micrometers, not microns.
- Preferred units for radius, range, speed, and altitude vary depending on the applications:
  - Nautical miles and knots or mach continue to be used for naval and aircraft-related parameters and for radius, range, or distance associated with aircraft and ship operations. Showing metric units in addition is not required but sometimes may be appropriate. If altitudes are associated with distances in nautical miles, those altitudes should be in feet.
  - Use nautical miles for ranges of territorial waters and economic zones at sea.
  - Use meters for wave heights (showing feet in parentheses also may be appropriate).
  - Metric units (kilometers and kilometers per hour) should be used where more appropriate, such as when discussing flight activity originally reported in kilometers, when describing radar scopes and other items calibrated in kilometers, when citing data from foreign documents with distances in kilometers, and when reporting estimates originally calculated in metric units. Showing values in nautical miles in addition to values in kilometers is not required; however, key characteristics—maximum range, maximum speed, and others—should be stated in nautical miles and knots as well as in metric units. Altitude capability should be expressed in meters (rather than kilometers).
  - Use kilometers for ballistic missiles and space-related parameters such as range, apogee, and perigee.
  - Use meters for circular error probable (CEP). CEP is a measure of locational accuracy; it represents the radius of a circle into which half of the projectiles—bombs, missile warheads, bullets, etc.—are expected to impact.
  - Use meters per second for velocity and g for acceleration.
  - Use kilometers and kilometers per hour where statute miles and miles per hour customarily would have been used, such as for highway and rail travel, landline distances, and "roadmap" distances between sites. Use meters for altitude for land-related locations.

Metric and Nonmetric

Take particular care within a document not to mix metric and nonmetric units unnecessarily so that readers are left with confusing data. For example, in discussions of air-land operations, do not mix nautical mile data for aircraft and kilometers for units and objects on the ground. If you indicate that a target is 500 kilometers from Airbase X and that the combat radius of the fighter-bombers at that base is 300 nautical miles, can the aircraft reach the target without refueling? Because the units of measure are mixed, the answer is not obvious. In such cases, convert all measurements to metric data or provide both metric and nonmetric measurements for the data customarily expressed in nonmetric units.

- Other nonmetric units still in wide use—such as standard atmosphere, millibar, and roentgen—should be used in contexts for which departure from traditional units would impair communication.

Online Conversion Tools. Such tools are available for many measurement conversions. On the DIA homepage on JWICS, select "Resources," and from there select "Tools" and then "Misc Calculators" and "Metric Converter."

In addition, the appendix provides conversion factors for units of measure commonly used in intelligence products.

Measurements

Use numerals for any number expressing a measurement unless you are stating an indefinite quantity. As a general rule, write out the units of measure in text when presenting nouns, but abbreviate the units of measure in the adjective form: for example, "a section of road that stretched 5 kilometers," but "a 5-km section of road." In tables, abbreviations are appropriate for all units of measure because of space limitations. Never abbreviate the units with an indefinite quantity. Avoid abbreviating units when the result is a single-letter abbreviation ("a 3-meter stream" rather than "a 3-m stream").

The missile exploded 500 kilometers downrange.
The vehicle has an estimated 500-km range without refueling.
Each aperture is protected by a 2-meter shield.
The platoon advanced several hundred kilometers. [*not* "several 100 kilometers," and *not* "several hundred km"]

Age

Use numerals for ages. In many instances, using the terms *age* or *aged* is unnecessary (as in the first three samples below) because context usually will make clear that the numeral is for an individual's age.

The general is 60. [or "60 years old," *not* "60 years of age"]
The general is in his 60s.
The general, 60, is retiring soon. [*not* "aged 60"]
The draft now applies to 17-year-olds.

Dates

Use numerals for days and years. In intelligence products, give dates in military format (day-month-year order); in official correspondence, use traditional format (month-day-year order). Only the day and month are necessary if the year is obvious from context. Ordinal numbers may be used after the month is clearly established. Do not abbreviate the month or year in text, though abbreviating for tables may be appropriate because of space limitations.

India's independence was declared on 15 August 1947. [*not* "15 Aug 47"]
All signers had left by the 22nd.
A class of pilots graduated in June 1989. [*not* "June, 1989"]

For a date in a classified product's classification authority/declassification block, Information Security Oversight Office and Department of Defense guidance requires the date to be all in numerals and in YYYYMMDD form.

Declassify on: 20351117

Time

Use numerals for units of time: seconds, minutes, hours, days, weeks, months, and years. However, if the expression of time is nonliteral or indefinite, use words instead.

The work usually requires 2 hours of labor.
She worked for the company for 7 months and 2 days.
but lasted more than four decades
in a day or two
finish by the eleventh hour

From, Between, and Dashes

Do not combine *from* or *between* with years joined by an en-dash (use *to*, *through*, or *and* instead of the en-dash).

He visited the embassy twice between 2008 and 2009. [*not* "between 2008–09"]
He visited the embassy twice from 2008 to 2009. [*not* "from 2008–09"]

Years

Except in indefinite or nonliteral expressions, use numerals for years.

Pilot candidates study general sciences for 1 year, followed by 2 years of flight training.
but Data for any one year will show that the plan was ineffective.

Also use numerals for fiscal years.

fiscal year 2010	FY 2010–12
FY 2010	from FY 2010 to 2011

For numerals designating a *continuous* period of 2 or more years, use an en-dash to mean "to and including" or "through." Never use an en-dash to join separate years not representing a continuous period; to indicate 2 years without indicating a continuous period, use *and* instead.

He worked at the embassy during 2004–06.
He worked at the embassy during 2006 and 2007.
The first two submarines were launched in 1990 and 1991. [*not* "1990–91"]

Use a slash (or virgule) to show a period occurring partially in one year and partially in another.

production in FY 2010/11
He flew three illegal flights in 2008/09.

Notice that the numerals and slash are run together without spaces around the slash.

Decades/Centuries

For decades, use the numerals of the initial year followed by an s (1980s). You can show centuries the same way (1800s), but ordinal numbers are more common (19th century).

This estimate covers the mid-to-late 1980s.

However, if you are discussing decades or centuries in a general or nonliteral sense, use words instead of numerals.

during three decades	from one century to the next

Clock Time

Use numerals and the 24-hour system.

The managers met at 0745.
The meeting has been postponed to 1725.

Money

Express values in U.S. money with numerals preceded by a dollar sign. Indicating *U.S.$* (or *USD*) is not necessary unless foreign dollars could be understood. If you need to show foreign currency, follow it with the dollar amount in parentheses. Use words, not symbols, when indicating foreign currencies. Hyphenate unit modifiers involving money just as you would other unit modifiers involving numerals. Use the word *dollars* (or *cents* for amounts less than a dollar) when you are giving generalized or indefinite amounts.

The missile system cost the Iranians nearly $500 million.
The military purchased $5 million worth of radio-relay equipment.
The group paid 5 million South Korean won ($4,325) for safe return of the hostage.
The equipment cost the government nearly 100 million pounds (about $156 million). [*not* £100 million]
The company offered its workers a $1.53-per-hour increase in wages.
He called the conference a $50-million boondoggle.
He paid about 40 cents tax on every dollar he earned.
The work cost the firm thousands of dollars.

Percentages

Use numerals with percentages. Write out the word *percent* in text. The percent sign (%) is acceptable in tables and graphics if space is tight, but normally write out *percent* in the text portions of tables and graphics, and especially in footnotes to them.

The plan projects a 5-percent increase by 1990.
He formed a joint venture that was 59 percent Chinese and 41 British.
Agricultural products make up 20 to 25 percent of the country's imports.

Times Phrases

For expressions showing the relationship of a larger quantity to a smaller one (often accompanied by the word *times* or its equivalent), follow the basic rules for numbers less than or equal to or greater than 10 unless a decimal is involved; for such expressions with decimals, use numerals.

five times as large
2.5 times faster
10 times greater

The number of tanks is five times greater than before the war.
Missiles increased to 100 in 1991, 5 times the previous total.

Ratios, Odds, Returns

Use numerals.

The pilot-to-aircraft ratio is 1.2:1.
He had a 50–50 chance of winning.
The measure passed with a 50–to–1 vote.

BE Numbers

For Basic Encyclopedia (BE) numbers, use *BE*, a space, and the number. In a table with "BE Number" as a column heading, show only the number in the column (omitting *BE*).

BE 0254-08342 BE 0254CA8342

Separate a BE number from any associated O-suffix with a slash.

BE 0613DJ0002/DJ003

If such data will appear in a table, use a column heading of "BE Number/O-Suffix."

Geographic Coordinates

Use hyphens between degrees, minutes, and seconds, and leave a space between latitude and longitude. Show all three places for degrees for longitude.

The village was at 60-17-44N 135-20-16E.
The border crossing was at 22-12-17N 015-34-10W. [*not* "15-34-10W"]

Portraying decimal coordinates may imply an accuracy that is not correct and is unnecessary for most intelligence products. Decimal-second accuracy is important for targeting lists and databases of ground features when a high degree of accuracy is necessary for precise locations. For these reasons, decimal coordinates should be reserved for those limited cases for which such accuracy is critical and should not be used with general intelligence publications.

Mathematical Expressions

Use numerals when referring to numbers in mathematical expressions, no matter the size of the number.

multiplied by 3
divided by 4
Data points are rounded to the nearest 10th.
The estimate could be off by a factor of 2 or 3.

Numerical Designators

Use arabic numerals for designators for tables, graphics, footnotes, endnotes, parts of publications, and so forth. (However, appendixes to publications have letter designators: "Appendix A," "Appendix B," etc.)

Table 1 Figure 3
Part 4 Section 5

Numbers in Proper Names

Treat numbers appearing as parts of proper names as they commonly appear for those names; do not apply basic numbers rules to such names.

Three Rivers, Pennsylvania Air Force One
1st Army

Indefinite and Nonliteral Numbers

Do not apply the basic rules to indefinite or nonliteral numbers; instead, spell them out.

a tenfold increase
The project will cost tens of millions.
She addressed several thousand people.
She is famous for eleventh-hour decisions.
He is the number-two man in the regime.

Approximation

Do not use *about, around, approximately,* or any other word of approximation with exact numbers—"approximately 5,600" but not "approximately 5,613."

Terms such as *nearly, about, around,* and *approximately* do not by themselves reflect indefinite expressions. Normally such terms indicate rounding, but a rounded number remains more definite than an indefinite or nonliteral number.

Millions, Billions, and So Forth

Round numbers greater than 999,999 unless an exact number is necessary. Spell out *million, billion,* and so forth and precede the word with a numeral rounded usually to no more than two decimal places.

The population is about 240 million.
More than 12.35 million Americans served in World War II.
The program calls for funding of $5.2 billion.

Ranges

See page 80 under "Years" for en-dashes with ranges of years. Take particular care in joining range numerals (other than years and page references) so readers cannot be confused by the figures shown. En-dashes may be used (though not required) in ranges in the millions and multimillions—but note particularly the placement within money figures in the second sample below.

The march covered 10–15 kilometers. [*or* "10 to 15 kilometers"]
The program will cost $12 million to $14 million. [*or* "$12–14 million," but *not* "$12 to $14 million," which implies "12 dollars to 14 million dollars"]
Gas reserves are estimated at 10–15 billion cubic meters. [*or* "10 to 15 billion cubic meters"]

Do not combine *from* and *between* with numbers joined by an en-dash (use *to, through,* or *and* instead of the en-dash).

Estimates range from 10 to 30. [*not* "from 10–30"]
Bids fell between $10 million and $14 million. [*not* "between $10–14 million"]

For ranges in temperature, show the degree sign and the type of temperature scale only once if the parts of the range appear together, but repeat the sign and scale if other text separates the parts of the range. Note in the following examples that a space should appear between the number for the temperature and the indication of the temperature scale.

average in the high 20 °Celsius (80 °Fahrenheit)
drop to 8 to 12 °Celsius (upper 40 to lower 50 °Fahrenheit)
around 5 °C (low 40 °F)
exceed 30 °C (upper 80 to 90 °F)
rise to near 10 °C (upper 40 °F) in April and reach a high of 20 °C (80 °F) in June

For ranges of inclusive page numbers, show all numbers up to 100 (3–4; 4–12; 54–55). Thereafter, reduce the second number of a set to two digits (253–54; 601–09, 1901–02, 2614–15) unless the hundred or thousand changes (499–501; 2998–3002).

Commas With Numbers

Use commas to separate numerals in the thousands, millions, and so on—except for years, military unit designators, clock time, most serial numbers, fractional portions of decimal numbers, page numbers, and radiofrequencies in the thousands of kilohertz.

There were 1,087,143 casualties.
A force of 20,000 was needed.

but

during 2009
the 1028th Brigade
1400 hours
job number 518225/10
3.1416
3,732.14592
pages 3614 and 3617
1812 kHz [*but* 15,117 kHz and 1,832 MHz]

Numbers With x To Stand for by

When you use *x* to stand for *by* in commonly used numerical expressions, such as equipment designators, run the numerals and the lowercase *x* together without intervening spaces.

4x4
8x8

Possessive Case With Numbers

Numerical expressions including possession require an apostrophe but not an en-dash or hyphen. (Do not be concerned with the argument that inanimate nouns cannot possess things. The form being used is the genitive case, which came to be called the possessive case in the 18th century, and does not involve possession.)

After 5 years' planning, the project was scrapped.
The new regime bought several million dollars' worth of equipment. [*but* "$10 million worth of equipment"]

Decimals

Use numerals for numbers requiring a decimal point. For numbers less than 1.0, precede the decimal point with *0* (except for designations of gun bore or ammunition). Omit zeros from the end of a decimal number unless you are showing an exact measurement.

0.25 centimeter
1.25 centimeters
silver 0.900 fine [exact measurement]
a .22-caliber cartridge

In the samples above, notice that when the numeral for a unit of measure is equal to or less than 1.0, the word for the units—when written out—is singular (0.25 centimeter), but it is plural when the numeral is greater than 1.0 (1.25 centimeters). The same is not true for abbreviated units, however; they appear only in the singular form: 0.25 cm, 1.25 cm, 10.25 cm.

Fractions

Convert fractions to decimals whenever reasonable. Otherwise, write out fractions, with a hyphen in both noun and adjective forms.

0.75 kilometer [preferred over "three-quarters of a kilometer"]
one-half year
a two-thirds majority; a majority of two-thirds
first quarter FY 2009 [note no hyphen in "first quarter"]

Mixed Numbers

Avoid combinations of whole numbers and fractions by converting to decimal quantities whenever reasonable.

5.5 percent [*not* "5 1/2 percent"]

Otherwise, spell out phrases in nonstatistical contexts.

two and a half years ago	a two-and-a-half-year trial period

In statistical contexts, use mixes of whole numbers and fractions (5 1/2, 4 1/4) if converting to decimals is not appropriate.

Numbers in Unit Modifiers

Use hyphens with numerical unit modifiers.

20-km march	23-meter-wide river
105-mm guns	eleventh-hour decision
7-meter limit	two-story building; 10-story building
3-million-member Army	6-percent increase; 6- to 7-percent increase
20-NM range	
one- to two-story structure	

Numbers Side by Side

To avoid confusion, avoid placing cardinal numerals side by side.

Twenty-five divisions were identified by 2006. [*not* "In 2006 25 divisions were identified."]

However, when the second number is part of a unit modifier, the hyphen of the unit modifier prevents misreading, so placement of numbers side by side is acceptable:

14 152-mm guns

Singular and Plural Units With Numbers

When the word for a unit of measure is written out, use the singular form with a number less than or equal to 1.0; use the plural form with numbers, including fractions or decimals, greater than 1.0.

0.75 meter	1 meter
1.25 meters	7 meters

However, when the unit of measure is in its abbreviated form, use only the singular form.

a 0.75-km road segment	a 1-km road segment
a 1.25-km road segment	a 7-km road segment

Quantities and Numbers as Subjects

When a number is the subject of a clause, the number is singular or plural (and takes a corresponding singular or plural verb) depending on whether it designates a quantity (something measured as a unit, as in length, area, volume, mass, temperature, or time) or a number of things (things counted individually).

- Quantities, which are measured, are singular and are the most common numerical subjects.

  Four gallons of milk was all the machine would hold. [*Four gallons* in this passage is a measure of volume and is singular because it represents a single unit.]

- A number of individual things is plural.

  Four gallons of milk were sitting in the dairy case. [The *four gallons* in this passage are being discussed as individual things—four 1-gallon containers of milk—making the subject plural.]

Beware of becoming confused by the seemingly plural nature of the unit of measure (*gallons* in the samples above). Although the measure sounds plural, it designates a unit—a single thing.

Twenty kilometers of track was all the crew could lay in 8 hours.
Nearly 2 million barrels of capacity was destroyed in the first attacks.
Over 2 metric tons of cocaine was seized in the drug raid.

In each of these sentences, the unit of measure sounds plural (*kilometers*, *barrels*, and *metric tons*) but actually indicates the amount of a single thing—length, volume, and mass.

Do not confuse quantities and numbers as subjects with words that express a *portion of a whole*—words such as *percent* or *half* (and other fractions). These words can take either a singular or a plural verb, depending on the sense of the rest of the sentence (or of surrounding sentences):

Thirty percent of the forest was destroyed by yearend. [The *30 percent* is singular in this passage because it is being discussed as a single unit.]
Thirty percent of the trees were loaded onto trucks. [Because the trees would be loaded individually, or perhaps in multiple small groups, this *30 percent of the trees* is plural.]

For further discussion, see *all, any, half (and other fractions), more, most, none, part, percent, percentage, some* in Chapter 5.

CHAPTER 5: Current Usage

UNCLASSIFIE

nauseated/nauseous. It's the difference between sick and sickening. You are made sick (nauseated) by something sickening (nauseous). Never say, "I'm nauseous." Even if it is true, it's not something you should admit.

—Patricia T. O'Conner, *Woe is I: The Grammarphobe's Guide to Better English in Plain English*

UNC ASS

CHAPTER 5: Current Usage

This chapter provides guidance on troublesome words and phrases. Some are frequently confused or misused; some are overused and should be replaced with more vigorous expressions; some show preference for usage among related words or phrases. A thesaurus can be a valuable tool when you are stuck on a word or phrase, but pay attention to the differing shades of meaning among the choices, especially to connotations that may present nuances that make some word choices inappropriate for the passage you are considering.

Word Choices

a, an. The choice between *a* and *an* depends on the initial sound of the next word or abbreviation, not on whether its initial letter is a vowel or consonant.

- With words.
  - Use *a* before a word beginning with a consonant sound or an aspirated *h* (such as "hill," "habitual," "historic").
  - Use *an* when the following word begins with a vowel sound or a silent *h* (such as "honest," "hour," "honor").
- With numerical expressions. When the following expression begins with a numeral, choose between *a* and *an* on the basis of the pronunciation of the numerical term, applying the rules for words above: "a 12-year-old ship"; "an 11-year-old airframe."
- With abbreviations, including acronyms and letter/number groups. The initial sound test still applies.
  - For acronyms pronounced as words (such as "BMEWS," "HOT," "IMINT," "OCONUS"), apply the rules for words above: "a BMEWS installation," "a HOT missile," "an IMINT collector," "an OCONUS military base."
  - For acronyms and other letter/number groups (such as "SS-25") for which you pronounce the letters and numbers themselves, apply the following rules:

    Use *a* when the group begins with *b, c, d, g, j, k, p, q, t, u, v, w, y,* or *z*: "a DIA employee," "a UN worker."

    Use *an* when the group begins with *a, e, f, h, i, l, m, n, o, r, s,* or *x*: "an NSC directive," "an SS-25 missile," "an Su-34 aircraft."
  - When choosing between *a* and *an* with an abbreviation, consider the abbreviation itself, not the expansion of the abbreviation. For example, for discussion of a fuel-air explosive (FAE) device, because we would pronounce the letters of the abbreviation, we would write "an FAE device," since *an* is appropriate before an abbreviation beginning with *f*; we would not choose "a FAE device" even though *a* would be appropriate before "fuel."

ability, capability, capacity. Regarding people, *ability* is the power to do something; *capacity,* like aptitude, is the inherent facility to acquire an ability. A person can acquire ability but already must possess capacity. For people, *capability* refers to having the talent or potential for development. For things, *ability, capacity,* and *capability* are synonymous—all referring to having the potential to be used for a particular purpose. Although some people believe only a person (not a thing) can have an ability, dictionaries do not support this distinction.

about, around. In the sense of approximately, use *about* rather than *around.* In a sentence such as "The unit strength is estimated at about 2,500," the writer does not need both *estimated* and *about.* The sentence can be simplified to "The unit strength is about 2,500" or "The unit strength is estimated at 2,500"; the first choice usually is preferable because the second is in passive voice, but

the second choice is preferable if the writer is conveying that the number is an estimate rather than a generally accepted fact. Do not use any word for approximation with an exact number: "about 5,600" but not "about 5,613." For *about*, see also *as to* and *approximately, about, roughly, some*.

above, below. *Above* is accepted as meaning "previously mentioned" and *below* as "mentioned later." Use of either term to refer to text elsewhere in a document should be infrequent (overuse sounds legalistic), and the references should be clear ("the description above of command bunkers" rather than "the description above") so readers cannot be in doubt about what is being addressed. *Above* is preferable to the legalistic *abovementioned* or *aforementioned*.

absolute. Because the term shows a perfect, complete, unrestricted state, most modifiers and comparisons are illogical: "very absolute," "too absolute," "more absolute." However, *nearly* is an acceptable modifier ("nearly absolute acceptance"). Also see *very*.

access, assess. *Access*, as a noun, is a means of approaching, entering or exiting, or communicating; the ability to do one of these; or the act of doing such a thing. As a verb, especially in relation to computers, to *access* is to obtain entry. *Assess* is a verb dealing with determining value (as for taxation), setting the amount for taxation or special payment, or actually charging such a payment. For sports, to *assess* is to charge with a penalty. Finally—and most important for intelligence writing—to *assess* is to determine the value or significance of something: "We assess that changes in the Army's force structure will result in a more mobile force."

accidental, fortuitous, contingent, incidental, opportune. Related adjectives, these have varied shades of meaning: *Accidental* carries the idea of chance. *Fortuitous* strengthens the sense of chance; it can suggest luck or good fortune, but it does not lose the associated sense that the good fortune was unplanned. (Saying "The president's choice of Stein for prime minister was fortuitous," then, implies that the president's choice came from dumb luck, not brilliant insight.) *Contingent*, in its sense of "accidental," suggests something that may happen but that is uncertain because causal factors, including chance, are unknown. *Incidental* suggests an association that may or may not be accidental. *Opportune* suggests an element of chance mixed with timeliness: being in the right place at the right time.

actual, real, virtual. *Actual* emphasizes fact as it is or has become at the moment, whereas *real* emphasizes fact as it always has been or has been for a long time. *Virtual* means "having the effect but not the form" (as with a "virtual leader" when an actual leader exists).

adapt, adopt. *Adapt* is to adjust oneself or something to a new or changed situation. *Adopt* is to accept or choose a new course of action.

adit, entrance, entryway, entranceway, portal. An *entrance* is an opening allowing entry. An *entryway* is a passage serving as an entrance; this term is preferable to *entranceway*. In general English, a *portal* is a two-dimensional entrance or doorway; an *adit* is an entryway, mostly horizontal, leading into a mine or other underground facility. For intelligence writing related to hardened structures and underground facilities, however, both *portal* and *adit* have more precise engineering definitions; see the Defense Resources and Infrastructure Office's *Lexicon of Hardened Structure Definitions and Terms*, <http://www.dia.ic.gov/intel/world_wide/dird/DIA-13-1110-170_REL_TO_FVEY.html>.

adjacent, contiguous, colocated. In a general sense, *adjacent* and *contiguous* are interchangeable. However, *adjacent* means "close to" or "lying near"; *contiguous* means "touching" or "sharing an edge or boundary." *Colocated* means "placed together"; it is appropriate for two organizations that share a building, facility, or complex, as in "the headquarters of the 32nd Battalion and the 48th Battalion are colocated at Steinmark Barracks."

advance, advanced. As an adjective, *advance* emphasizes precedence in position or time ("advance party," "advance payment"); *advanced* implies having a position forward of or superior to a norm ("advanced thinking," "advanced training"). In "advance planning," *advance* is redundant and should be deleted.

adverse, averse. Both adjectives mean "opposed," but their points of view differ: something *adverse* is opposed or hostile to a subject's will or interests ("The prime minister has been subjected to adverse criticism"); *averse* is opposition or reluctance on the subject's part ("The prime minister is averse to believing his critics").

affect, effect. Except in psychology, *affect* is always a verb and usually means "to influence," "to cause a response," or "to cause a change" in a person or thing. As a verb, *effect* means "to bring about or accomplish" or "to cause to occur."

The government's policy change will affect worker productivity. [The change will influence the workers in a way that will change their productivity.]

The government's policy change is a means to effect increased worker productivity. [The change is a means to bring about increased productivity.]

Effect as a noun refers to a result or consequence—"something brought about by a cause or agent": "Increased productivity was one effect of the government's policy change."

afterward, afterwards. *Afterward* is preferred.

all, all of. Except when a personal pronoun follows, *of* usually is unnecessary: "The change affected all the production facilities" rather than "... all of the production facilities." Beware of sentences that say "all of something did not do something," as such sentences are ambiguous. For example, in "All the regiments did not move forward," does the writer mean that none of the regiments moved forward or that only some did?

all, any, half (and other fractions), more, most, none, part, percent, percentage, some. Each of these words can take either a singular or a plural verb, depending on the sense of the rest of the sentence (or of surrounding sentences). Frequently that sense includes either quantity or number. A reference with a quantity of something requires a singular verb: "Some of the water was leaking." A reference with a number of things requires a plural verb: "Some of the plants are poisonous." In other cases (particularly with *any* and *none*) the verb determination depends on whether the writer has in mind one person or thing (requiring a singular verb) or two or more (requiring a plural verb): "None of the protesters was willing to risk arrest" (*not one* was willing). "None of the protesters were willing to risk arrest" (*not any* were willing).

allegedly, reportedly, reputedly. The three mean "supposedly," but they have slightly different shades of meaning: *Allegedly* carries the sense of "claimed or charged but not proved." *Reportedly* implies that the information has been reported formally. *Reputedly* means "generally considered or estimated but not necessarily claimed openly." See also *qualifiers*.

all ready, already. *All ready* means that everyone or everything is ready; *already* means "before" or "previously."

all right, alright. *All right* is the correct term; *alright* is substandard.

all together, altogether. *All together* means "collectively" or "in unison." *Altogether* means "entirely, completely." *Note:* When *all together* is appropriate, the words in the sentence can be rearranged so that *all* and *together* are separated by other words: "The workers arrived all together" can be changed to "All the workers arrived together."

almost. See *most, mostly* and *only*.

alongside, alongside of. *Alongside* is adequate without *of*.

along with. This phrase (and others such as *as well as, in addition to, like,* and *together with*) frequently follows immediately after a subject of a sentence. The prepositional phrase and its object(s) do not affect whether the verb in the sentence is singular or plural. For example, in "The governor, along with members of his staff, is traveling to the coast," the verb is singular *(is)* because the subject

(governor) is singular and the prepositional phrase *along with members of his staff* has no impact on whether the subject and verb are singular or plural. If, however, a writer were to state that same idea like this—"The governor, and members of his staff, are traveling to the coast"—the verb must be plural *(are)* because the subject is plural *(the governor and members of his staff)*; the presence of commas around *and members of his staff* does not keep the subject from being compound and therefore plural. (Moreover, the commas should be removed.)

a lot, alot. Use *a lot*, as *alot* is not a word.

alternate, alternately, alternative, alternatively. *Alternate* and *alternately* usually refer to occurring successively or by turns. *Alternative* and *alternatively* refer to one from a set of possible courses of action or choices. Although traditionalists would limit alternatives to only two possibilities, use in connection with multiple choices is acceptable.

although, though, even though, while. *Although*, *though*, and *even though* are often interchangeable for the sense of "in spite of the fact that." *Although* is more formal than *though* as a conjunction, but *though* can also serve as an adverb, as in "They raised objections, though." *Even though* emphasizes the sense of "in spite of" or "regardless." *While* has become a common substitute for *although* in informal usage; however, in this sense *while* means "at the same time that," and in writing it should be reserved for sentences requiring a sense of time.

altitude, elevation. Use *altitude* in relation to something in the air—for example, "The missile was ineffective at altitudes below 5,000 meters." *Elevation* is in relation to the ground or sea level—for example, "The facility is at an elevation of 75 meters."

amid, amidst, among, amongst. *Amid* and *among* are preferred.

among, between. [See tone box.]

amount, number. Use *amount* with things involving weight, bulk, or sums—things measured with a total; use *number* with things that must be counted individually: "the amount of water in the mixture," "the amount of the gross national product," "the number of gantry cranes in the port."

ample, enough. Although these commonly are interchanged, *ample* carries a second meaning of "abundant, more than enough." Therefore, phrases such as "more than ample," "barely ample," or "scarcely ample" are nonsensical.

an. See *a, an.*

and/or. This combination with the slash refers to one or the other or both. Avoid its use, especially with more than two alternatives.

any. See *all, any, half (and other fractions), more, most, none, part, percent, percentage, some.*

Among and Between

Between is appropriate when just two entities are involved—for example, "an agreement between France and the United Kingdom." Numerous writers have insisted that *among* always should be used when more than two entities are involved, but current English usage and modern dictionaries do not support this position. When more than two entities are being considered, choosing between *among* and *between* depends on whether the writer is discussing separate entities acting independently or entities considered collectively.

- In "conflicts between the four nations," each nation is considered to be acting independently of the others, with conflict one on one.
- "Conflicts among the four nations" allows for coalitions, including the possibility of the coalitions changing over time.
- In "rockets struck between the entrance to the compound, portal 1, and portal 3," the rockets are considered to have impacted literally between the named points without hitting any of them.
- In "rockets struck among the entrance to the compound, portal 1, and portal 3," the rockets are considered to have impacted in the general area of the named entities and may or may not have struck them.
- If named points or entities define the extent of an area, use *between*, as in "the rockets impacted in the area between the entrance to the compound and portals 1 and 3."

anyone, anybody. Each of these usually is written as one word (except in the sense of "any one of a group"). They take singular verbs and singular pronoun references. If you have trouble remembering that these words are singular, try thinking of them as "any-single-one" and "any-single-body."

apparent, evident. These words share a sense of "obvious" or "open to view" but differ slightly: *apparent* suggests use of reasoning; *evident* suggests a basis of facts or external signs. *Apparent* also means "seeming but not necessarily true." Before a noun that meaning is clear ("her apparent concern"); however, after a form of *to be*, *apparent* can mean either "obvious" or "seeming," so the context needs to be worded to make the meaning clear.

apparently. See *qualifiers*.

approximately, about, roughly, some. Do not use any word of approximation with an exact number: "approximately 5,600" but not "approximately 5,613." See also *about, around*.

apt, liable. Although these words are interchanged in informal usage, their meanings remain distinct. Reserve *apt* for instances in which the subject has a natural tendency: "He is apt to settle the issue without consultation." In this sense, *liable* means "susceptible" and suggests a probability for something unwanted or burdensome: "Temperatures are liable to drop below freezing in higher elevations."

arch-, arched-. *Arch-* can be used with *shaped* in a unit modifier: "an arch-shaped structure." Modifiers in names of structural components use *arched-* ("arched-roof segments"), whereas the name of the completed structure uses *arch-* ("an arch-roofed bunker").

around. See *about, around*.

as, because, for, since. *Because* is the strongest of these conjunctions expressing cause or reason; *since*, the next most strong; and *as*, the weakest. Use caution with *since*, which may be read as meaning "from a specific time." *As* works best with a dependent clause that ends a sentence; a comma precedes it when *as* appears as a conjunction showing a causal relationship. *For*, a coordinating conjunction, shows a causal relationship between independent clauses.

as if, as though, like. Both *as if* and *as though* are acceptable as conjunctions (for example, "The exterior of the building looked as if it had been raked by gunfire"). Either is preferable to *like* for introducing a clause.

as per, as regards. Replace these with *according to, concerning,* or *about*.

assess. See *access, assess*.

as such. *As such* requires an antecedent, as in "Applicants will not be treated as U.S. persons unless identified as such" [identified as U.S. persons]. Avoid using *as such* to mean "therefore"; don't write "As such, we expect a dropoff in applicants."

assure, ensure, insure. Similar in the sense of making certain, these words require different usages. *Assure* refers to a person—setting that person's mind at ease by making him or her certain of something. Use *ensure* for the sense of making a thing certain. Reserve *insure* for guaranteeing life or property from risk.

as to. This phrase should be replaced or deleted. In a sentence such as "She was uncertain as to the proper answer," replace *as to* with *about*. In expressions such as *as to whether, as to where,* or *as to which*, the *as to* is unnecessary.

as well as. See *along with*.

attributive nouns. See *nouns as adjectives*.

average, median, mean. *Average* is that which is midway between two extremes. Common usage has made it synonymous with an arithmetic mean (the result of dividing the sum of a series of figures by the number of figures). *Mean* is a more precise term when you actually want to refer to a mathematical result,

but *average* is acceptable for general usage. A *median* is the middle figure in an arithmetically arranged list of figures; half the numbers are less than the median, and half are greater than the median. Each of the three terms refers to a single figure, so a sentence such as "The tide averages between 2 and 4 meters" should be replaced by "The tide averages 3 meters" or "The mean tide is 3 meters."

averse. See *adverse, averse.*

awhile, a while. *Awhile* is an adverb meaning "for a time"; *while* is a noun meaning "a period of time." Both imply a *short* time. *For* is a part of the sense of *awhile* and should not be used with it. Thus, "stay for a while" is correct, but "stay for awhile" should be "stay awhile."

back of, in back of, behind. Use *behind* in place of *back of* and *in back of.*

bad, badly. *Bad* (the adjective) is correct after linking verbs such as *feel* and *look.*

because. See *as, because, for, since.*

because (reason is). In "The reason is because ...," replace *because* with *that* when the following material is a clause.

begin, commence, start, initiate. *Begin, commence,* and *start* usually are interchangeable; in general senses, *commence* is less desirable than either of the other two because it is more formal. However, *commence* has a stronger sense of initiative—of some person or force initiating an action. *Start* is particularly appropriate when action must begin following a period of inactivity. *Initiate* refers to taking the first steps in a process and does not refer to what follows.

believe. Avoid using "DIA believes." Assessing or judging requires weighing the data; believing does not. By contrast, *believe* can be appropriate when describing what the *subject* of DIA analysis thinks about something: "The defense minister probably believes that the arms purchase will strengthen the military."

below. See *above, below.*

beside, besides. Use *besides* for the senses of "except for" and "in addition to": "No vehicles were present besides one staff car outside the headquarters building." "Besides the commander, the chief of staff also attended." *Beside* means "at the side of." Thus, "No one entered the room beside me" and "No one entered the room besides me" state different things.

between. See *among, between.*

biannual, biennial, bimonthly, biweekly. In standard usage, *biannual* means "happening twice each year" or "semiannual," whereas *biennial* means "happening every second year" or "lasting for 2 years." However, both *biannual* and *biennial* have secondary meanings that can greatly confuse the timeframe. *Bimonthly* means "once in 2 months," and *biweekly* means "once in 2 weeks." Because of the possibility for confusion, writing "occurring every other year," "occurring twice a year," "every 2 weeks," "twice a week," and so on, is safer.

blatant, flagrant. *Blatant* means "unpleasantly noisy" or "offensively conspicuous"—stressing offensiveness and noisiness. *Flagrant* emphasizes wrongdoing or evil intent. Thus, the difference between a "blatant act" and a "flagrant act" is the degree of intent.

blond, blonde, brunet, brunette. *Blond* and *brunet* should be used with either gender; avoid *blonde* and *brunette.*

boat, ship. A *ship* is large and travels the sea lanes. A *boat* is relatively small, stays mostly in shallow or sheltered waters, and can be carried on a ship. *Boat* also is acceptable in reference to a submarine.

border. When identifying the border between two countries, use the noun rather than the adjective form of the countries' names: *Libya-Tunisia border* instead of *Libyan-Tunisian border.*

born, borne. Both of these words are correct spellings for the past participle of the verb *bear.* However, *born* is used only as a passive construction in relation to birth: "She was born in the former Soviet Union." *Borne* is used for the active voice in relation to birth ("She had borne three children before entering politics."), as well as for all other senses of *to bear* ("a vehicle-borne improvised explosive device").

both. In sentences such as "Both sides have reached agreement on the plan," *both* is redundant; use "The two sides have reached agreement...."

boycott, embargo. A *boycott* is a refusal to buy or use a product or service. An *embargo,* a legal restriction on trade, can apply to either buying or selling.

but also. See *not only ... but also.*

cadre, cohort. A *cadre* is a core of trained personnel around which a larger unit is to be built or a member of such a group. A *cohort* can be a united band or group, or it can be a companion or associate. Current usage no longer restricts these terms to just groups rather than individuals.

capability, capacity. See *ability, capability, capacity.*

capital, capitol. *Capitol,* a noun, has only one meaning—the building in which a legislature meets. As a noun, *capital* has to do with wealth or resources, an uppercase letter, or a town or city that is the seat of government; the latter meaning, of course, is the one that generates confusion with *capitol.*

capital standing for nation. In intelligence writing we commonly substitute the name of a nation's capital for the name of the nation and use either to represent the national government. For example, we might write either "The United Kingdom anticipates withdrawing...." or "London anticipates withdrawing...."

- A notable exception is Israel. Avoid using either Tel Aviv or Jerusalem to represent Israel.

casualty. A *casualty* could be injured, captured, missing in action, or killed.

cement, concrete. *Cement* as a powder is a component used in making *concrete.* Concrete is made from aggregate (sand, gravel, and so forth), cement, and water (and possibly additives to enhance the concrete properties). The concrete gains its strength from a chemical reaction between the cement and the water.

censor, censure. To *censor* is to examine and remove objectionable material. To *censure* is to find fault or condemn.

center around. Because it is a point, *center* can be paired with *on, upon, in,* or *at*—but not with *around.*

certain, some. *Certain* means "fixed" or "definite." In some instances it equates more generally to "some." Problems come with the general sense in an expression such as "modifications of certain procedures." This statement begs for an explanation of just what procedures are to be modified. Replacing *certain* with *some* reduces the strength of the expression but does not totally eliminate the need for further explanation. If you do not intend to define which procedures are to be modified, omitting the adjective may be a better choice.

China, Chinese, Taiwan, Taiwanese. *China* and *Chinese* refer to the mainland country and its people. The offshore island is *Taiwan;* its adjective form also is *Taiwan. Chinese* is the noun and adjective for people on Taiwan in general; *Taiwanese* refers only to the indigenous inhabitants of the island. To distinguish the people on Taiwan from those on the mainland, use people "on Taiwan," "from Taiwan," or "of Taiwan."

cite, sight, site. These words sometimes are confused because they are homonyms. *Cite*, a verb, has several meanings: to quote or mention as an authority or example; to officially praise or formally honor, especially for military merit; or to summon before a court. *Sight*, a noun or verb, has to do with seeing. A *site* is a location or setting; in relation to computers and the Internet, *site* also is a variant of the more specific *website*.

claim. To *claim* means to assert that something is the case, typically without providing evidence or proof. *Claimed* can have a slightly negative connotation, so consider whether *stated* or *reported* would work better in context.

clearly. See *qualifiers*.

climactic, climatic. *Climactic* refers to the climax, the highest point. *Climatic* refers to weather.

close proximity. *Proximity* is redundant in this phrase.

cohort. See *cadre, cohort*.

collective nouns. A collective noun—such as *committee, company, enemy, group, team*, and the like—takes a singular verb when the group acts as a whole but a plural verb when its members or parts act separately.

> The committee has decided to recommend banning chemical weapons. [The committee's decision is a collective action.]
>
> The committee have returned to their offices. [Each member must act separately in such a situation.]

The second construction sounds awkward to many ears, though, so a better choice may be to insert a plural noun, as in "The committee members have returned to their offices." Be particularly careful to ensure that the verb connected to a collective noun and any pronoun reference to the same collective noun are either both singular or both plural—as with *have* and *their* in the second example.

colocated. See *adjacent, contiguous, colocated*.

combined, joint. In reference to military exercises, a *combined* exercise involves forces from more than one country; a *joint* exercise involves forces from two or more services of the same country.

commence. See *begin, commence, start, initiate*.

communication, communications, telecommunication, telecommunications. Both the singular and the plural forms are acceptable as modifiers: "the communication system," "the communications system." The singular forms (*communication* and *telecommunication*) are preferable for most uses, especially when the next word in a sentence begins with s ("telecommunication system"). Either form is preferable to *communicational*.

comparatively, relatively. Use these modifiers only when the comparison they refer to is clear. In "There was relatively little debate about the president's proposal," what does *relatively little* really mean?

compare, contrast. *Compare to* points out similarities between inherently dissimilar things; *compare with* points out both similarities and differences. *Contrast with* points out differences.

complement, compliment. *Complement* refers to something that completes. A *compliment* is flattery or praise.

Compose, Comprise, Constitute, Include

Comprise means "to consist of" or "to contain"—the whole comprises the parts. *Compose* means "to constitute or make up"—the parts compose the whole. *Constitute* is interchangeable with *compose*. *Include* is similar to *comprise* in the sense of containing parts; *comprise* should be used when all parts are named and *include* when only some of them are named. Never use *is comprised of* or *are comprised of*.

complex, complicated. Both refer to things with many interrelated parts that are hard to understand or operate. *Complex* emphasizes the number of varying parts, whereas *complicated* emphasizes the elaborate relationship of parts rather than their number.

compose, comprise, constitute, include. [See tone box.]

conceivably. See *qualifiers.*

concept, conception. A *concept* is a general idea or understanding, whereas a *conception* is a particular mental picture or understanding of a concept.

concrete. See *cement, concrete.*

condition. Authors frequently use *condition* in connection with another descriptive term when the other term, or a form of it, can stand by itself. For example, use "The building was damaged" rather than "The building was in a damaged condition" and "He was weak" rather than "He was in a weakened condition."

conduct. Writers overuse *conduct* by combining it with a noun to describe an action when the verb equivalent of the noun will work on its own. For example, change "officials conducted an inspection of the facility" to "officials inspected the facility."

consensus. This is opinion held collectively or generally, not simply by a majority. In *consensus of opinion,* delete *of opinion.*

consequence, effect, implication. A *consequence* is the result of an event that has occurred, but the term implies only a weak causal relationship. An *effect* results from a causative act or agent. An *implication* is a possible future effect or result and is preferable to "potential consequence."

constitute. See *compose, comprise, constitute, include.*

contact. Use of *contact* as a noun equating to "source" is acceptable in intelligence writing (for example, "His contact was a member of the resistance group").

contiguous. See *adjacent, contiguous, colocated.*

contingent. See *accidental, fortuitous, contingent, incidental, opportune.*

continual, continuous, continued, ongoing. *Continual* refers to something that occurs intermittently or repeats at intervals: "Arguments over procedures were continual." *Continuous* refers to something that occurs without interruption in space or time: "Rainfall during the day was continuous." Something *continued* has remained in the same state (persisted), has existed for a long time (lasted), or has begun again after an interruption (resumed). Something *ongoing* is occurring at the moment—in progress or evolving.

continues, remains. Writers overuse these two terms. A sentence such as "Drug trafficking continues to provide most funds for the insurgents" can be stated more directly with "Drug trafficking provides most funds for the insurgents" because the present tense verb *(provides)* establishes that the activity is continuing. Similarly, a sentence such as "The insurgency remains concentrated in the south" can be stated simply as "The insurgency is concentrated in the south."

contrast. See *compare, contrast.*

convince, persuade. Though related, these words differ in application: we *convince* someone of the truth of a statement but *persuade* the person to act in a particular way.

could, may, might. These are low-confidence assessment terms and should be used with care in intelligence writing. Limit *could* to discussions of capability: "The missile could be targeted against the city" (the city is within the missile's range). Use *may* or *might* for judgments or predictions: "The missile may be targeted against the city" (possibly the enemy intends to employ the missile for that purpose). *Might* traditionally expresses a stronger sense of doubt than *may* or a contrary-to-fact hypothetical: "The city might

have been targeted if the rebels had captured more missiles." All three terms include the idea of possibility and should not be accompanied by modifiers such as *possibly* or *conceivably*.

council, counsel. *Council*, a noun, refers to a deliberative assembly, its work, or its members. *Counsel*, either a noun or a verb, refers to advice and the person(s) giving it.

country names. Except when making a point about the full formal name of a nation, use the common English name for a country rather than its formal name—what *The World Factbook* calls the "conventional short form" name rather than the "conventional long form" name. For example, use *Bulgaria* rather than *Republic of Bulgaria*; *China* rather than *People's Republic of China*; *South Korea* rather than *Republic of Korea*; *North Korea* rather than *Democratic People's Republic of Korea*; and so on. (See also *capital standing for nation* and *China, Chinese, Taiwan, Taiwanese.)*

country, nation. Both are neuter and require gender-neutral pronouns (for example, *it* or *its*).

credible, creditable. *Credible* means "believable" or "plausible." *Creditable* means "deserving credit or praise."

crisis. Reserve *crisis* for actual or potential international conflict, not for minor national or international disruptions. A *governmental crisis* is the period between the fall of a parliamentary government and the election of a new one.

> Data
>
> Although for years writers have insisted that *data* can be used only in the plural (because *data* is the plural of *datum* in Latin, the source of the English word), in current usage *data* appears primarily in the singular, in the sense of a body of information, as in "When we receive the data, we can interpret it" or "Little test data is available." Use of *data* as a plural noun still occurs, particularly in scientific or technical writing, though this usage is becoming less common.

current, currently. Analysts frequently include these terms when they do not need them. For example, in "current status," *current* is superfluous, since readers will expect to learn about the current state unless the writer establishes a different timeframe. If the context of a passage indicates that an activity is ongoing, *currently* is superfluous. In "A pilot project currently is testing the system," *is testing* indicates that the pilot project is ongoing, so *currently* is unnecessary and should be deleted.

dangling modifier, dangling participle. See *participles*.

data. [See tone box.]

dates as modifiers. Be careful in using dates as modifiers. "The 1973 Middle East War" is acceptable because it distinguishes a particular war in the region from others in other years. However, "his 1988 death" implies that he has died more than once—an absurdity.

definite, definitive. Although both mean "clearly defined," *definitive* carries the additional meaning of "authoritative and complete."

defuse, diffuse. To *defuse* is to remove the fuze from an explosive device or to reduce tension, hostility, or danger. To *diffuse* is to spread around or scatter.

degenerate, deteriorate. Although both refer to a decline in quality, *degenerate* refers particularly to a loss of worth or virtue, whereas *deteriorate* refers to a wearing away or weakening.

desires, feels, hopes. In intelligence writing, be careful with words that have an emotional connotation, such as *desires*, *feels*, and *hopes*. If the source material does not give an emotional context, try instead more neutral terms, such as *seeks*, *thinks*, or *plans*.

device, devise. The noun *device* refers to an implement that serves a particular purpose, especially a machine to perform a task. Except in its unique senses in law related to property, *devise* is a verb meaning to plan or arrange.

different from. Use this rather than *different than* or *different to.*

dilemma. This applies to a choice between evenly balanced alternatives (normally all are unattractive). Do not use *dilemma* when you mean merely a "predicament" or a "problem."

directional terms. See *east, eastern (and similar directional terms).*

disburse, disperse. To *disburse* is to pay out, as from a fund. To *disperse* is to scatter or spread widely, disseminate, or make disappear.

disclose, divulge, expose, reveal. *Disclose* refers to making public something that has been private. *Divulge* refers to making public something that has been secret. *Expose* refers to making public something reprehensible. *Reveal* implies unveiling something not previously known.

discreet, discrete. Often confused because of the similarity in their spellings and pronunciation, these words have no meanings in common. *Discreet* is "lacking pretension" or "showing a judicious reserve in one's speech or behavior." *Discrete* means "constituting a separate thing" or "consisting of unconnected distinct parts."

disinterested, uninterested. *Disinterested* means impartial. *Uninterested* means not having interest in something.

due to. *Due to* modifies nouns and is normally used after a form of the verb *to be*, as in "The minister's fall was due to a bribery scandal." It works the same way as *attributable to.* Avoid using *due to* to modify verbs ("The minister fell due to a bribery scandal"); try *because of* instead.

during, over. Although one of the lesser meanings for *over* is "throughout the duration of something," this is the primary meaning of *during*, which is preferable for a passage such as "during the past 3 years."

each. As a subject, *each* takes a singular verb and singular pronoun references: "Each has separate duties." However, when *each* follows a plural subject, it does not affect the verb; the verb remains plural to correspond with the plural subject: "The president and the vice president each have separate duties."

east, eastern (and similar directional terms). Indefinite or general directional references end with *-ern:* "In the eastern part of the country." Definite directional references use the shorter form: "on the east bank of the river," "in the east end of town."

economic, economical. *Economic* is an adjective pertaining to finance or production and management of material wealth. *Economical* is an adjective pertaining to prudent or thrifty management—that which is not wasteful.

Endemic, Indigenous, Native

Something that is *endemic* occurs commonly in a place or region or among a particular people. How the thing or person became endemic, whether by birth or creation or movement, is not at issue. A disease can be *endemic in* or *endemic to* a geographic area, but a geographic area cannot be *endemic for* a disease. Someone *indigenous* originates in a place rather than moving into or being brought into it. Something *indigenous* to a locale occurs there naturally, so *indigenous* should not be used to refer to things produced in a locale; instead, refer to domestic production. *Native* emphasizes birth or creation in a particular place, region, or country.

effect. See *affect, effect* and *consequence, effect, implication.*

either ... or, neither ... nor. When both parts of an *either ... or* or *neither ... nor* construction are singular or plural, the corresponding verb is singular or plural, respectively. However, when one element is singular and one plural, the verb corresponds with the number of the nearer part: "Either the president or his advisers want the conflict to continue." You can avoid an awkward (albeit correct) sentence by

ensuring that the plural part of the construction is nearer the verb. Also, if you combine *not* with *either*, the companion construction uses *or*, not *nor*: "The guerrillas were not interested in either the deserted camp or the remains of the shack that has served as its headquarters."

elevation. See *altitude, elevation.*

embargo. See *boycott, embargo.*

emigrate, immigrate. *Emigrate*, to leave a place permanently, usually is followed by *from*: "He emigrated from Germany." *Immigrate*, to come to a place permanently, usually is followed by *to*: "He immigrated to Wisconsin." When a sentence includes the idea of both, *immigrate* can be eliminated: "He emigrated from Germany to Wisconsin."

eminent, imminent. A person who is *eminent* is prominent, of high rank, noteworthy, distinguished, or well known. Something that is *imminent* is impending, about to occur.

employ. See *usage, use, employ, utilize.*

endemic, indigenous, native. [See tone box.]

enemy. See *collective nouns.*

enough. See *ample, enough.*

ensure. See *assure, ensure, insure.*

entrance, entryway, entranceway. See *adit, entrance, entryway, entranceway, portal.*

equal, equivalent. *Equal* emphasizes quantitative likeness: "The weapon inventories of the two countries are nearly equal." *Equivalent* applies to qualitative similarities: "Although their inventories are not equal, the combat capabilities of the two countries are roughly equivalent."

every. See *only.*

everyone, everybody. Although these words have a plural sense, they are singular and require singular verbs and singular pronoun references. If you have trouble remembering that they are singular, try thinking of them as "every-single-one" and "every-single-body."

evident. See *apparent, evident.*

evidently. See *qualifiers.*

execute. Writers overuse *execute* by combining it with a noun to describe an action when the verb equivalent of the noun will work on its own. For example, change "insurgents executed an attack" to "insurgents attacked."

explicit, implicit. *Explicit* refers to something clearly stated rather than implied. *Implicit* is the opposite—something implied, not expressly stated.

explosive, explosives. Use *explosive* for a specific reference to a bursting or propelling charge: "a high-explosive round." Normally use the plural form in an expression such as "explosives storage area."

expose. See *disclose, divulge, expose, reveal.*

extort. To *extort* is to obtain (something) by coercive means; the thing is extorted, not the person who has it. Write "Militants extorted money from villagers" rather than "Militants extorted villagers."

farther, farthest, further, furthest, furthermore. *Farther* and *farthest* refer to physical or literal distance. *Further* and *furthest* are concerned with figurative or notional distance—degree, time, quantity. *Furthermore*, an adverb meaning "moreover" or "in addition," is preferable for a passage such as "Furthermore, the Shia are likely to...."

fewer, fewer than, less, less than. Use *fewer* and *fewer than* with numbers or units counted individually: "fewer gantry cranes," "fewer than seven main battle tanks." Use *less* and *less than* with quantities of things measured with a total (weight, bulk, sums) or conceptually: "less water," "less gross national product," "less enthusiastic," "less than 125 metric tons of stainless steel plates." See also *amount, number.*

financial, fiscal, monetary. *Financial* is the broadest of these terms, though it sometimes refers more specifically to large-scale transactions. *Fiscal* applies to governmental policies and procedures related to money. *Monetary* applies to the money itself—to the coinage and currency or to the policies relating to their circulation.

first, second, third, and so on. Use these terms for reference to a list or sequence rather than *firstly, secondly, thirdly,* and so forth.

flagrant. See *blatant, flagrant.*

flaunt, flout. To *flaunt* is to show off; to *flout* is to show contempt.

flounder, founder. To *flounder* is to struggle clumsily or helplessly, as in confusion. To *founder* is to cave in or sink, as in a ship filling with water and sinking.

foot, feet. Use *foot* with a modifier preceding a noun: "a 6-foot pole." Use *feet* if the modifier follows the noun: "a pole 6 feet long." (However, keep in mind that in most circumstances DIA intelligence products should be using metric units.)

for. See *as, because, for, since.*

forego, forgo. To *forego* is to precede in time or place; to *forgo* is to do without something.

foreword, forward. A *foreword* is a prefatory or introductory note. *Forward* usually is a directional reference for "at or near the front," although it has a number of other meanings. In a publication, a *foreword* is an introduction that comes forward of the main body of the publication.

former, latter. These terms refer to one of a series of two things, not more than two. In referring to parts of a series of three or more things, use terms such as *first* or *last.*

fortuitous. See *accidental, fortuitous, contingent, incidental, opportune.*

for which. See *where, in which, for which.*

from ... to, from ... through. An expression such as "paid from 13 July to 7 August" does not include the final day ("7 August" in this instance). Using *through* rather than *to,* however, would include the final day.

further, furthest, furthermore. See *farther, farthest, further, furthest, furthermore.*

geographic, geographical. Use the simpler *geographic.*

governmental crisis. See *crisis.*

group. See *collective nouns.*

half (and other fractions). See *all, any, half (and other fractions), more, most, none, part, percent, percentage, some.*

hanged, hung. Use *hanged* for the past tense of *hang* when referring to executions. For other senses, use *hung.*

headquarters. *Headquarters* is a plural noun that can take either a singular or plural verb. Use of a plural verb is more common, especially when the emphasis is on location: "The company's headquarters are in Washington, DC." Use of a singular verb is common when the emphasis is on authority: "Corporation headquarters has issued new rules for trading commodities."

helicopter, rotary-wing aircraft. Avoid the wordy *rotary-wing aircraft* when you mean *helicopter*. *Rotary wing* is acceptable in uses such as "rotary-wing UAV."

historic, historical. Although their meanings overlap, common usage restricts *historic* to famous or particularly important events in history and applies *historical* to general events of the past and to things related to history or its study. "Gettysburg, Pennsylvania, was the site of a historic battle." "The president hoped emblems in his office would suggest comparison of him with historical leaders from the nation's past." "She is doing historical research in open sources."

if, whether. In informal usage, either *if* or *whether* can introduce a clause that expresses uncertainty, but for general usage, *whether* is preferable for introducing such a clause. "We cannot confirm if a suitable candidate has been selected" should be written instead as "We cannot confirm whether a suitable candidate has been selected."

immigrate. See *emigrate, immigrate.*

imminent. See *eminent, imminent.*

impact. *Impact* is usually a noun: "The impact of these changes will be clearer in time." As a verb, it means to strike forcefully: "The missile impacted downrange." Avoid using *impact* as a verb to mean "affect": "These changes will impact [affect] all employees."

impending. See *pending, impending.*

implication. See *consequence, effect, implication.*

implicit. See *explicit, implicit.*

imply, infer. To *imply* is to state something indirectly. To *infer* is to draw a conclusion or deduce something.

important, importantly. To introduce a second, more worthy consideration, use *more important* rather than *more importantly*. "Hoarding has decreased; more important, shops now have items that have been unavailable for months."

in addition to. See *along with.*

in back of. See *back of, in back of, behind.*

incident. Reserve *incident* for minor occurrences of momentary importance. "An incident took place last month when traffickers fired on a police outpost." *Incident* is not suitable for a major conflict or catastrophe.

incidental. See *accidental, fortuitous, contingent, incidental, opportune.*

include. See *compose, comprise, constitute, include.*

indigenous. See *endemic, indigenous, native.*

initiate. See *begin, commence, start, initiate.*

in order to. This phrase can often be whittled down to just *to*, especially at the beginning of a sentence. However, *in order to* can be helpful when the sentence contains another infinitive nearby: "The speaker plans to delay in order to reach a wider audience after the holiday."

inside of. See *outside of, inside of.*

Instead of, Rather Than, Vice, Versus

Instead of and *rather than* are synonyms, and either is preferable to *vice* or *versus* as a preposition—"The insurgent fired a rocket-propelled grenade rather than an antitank guided missile at the tank" instead of "The insurgent fired a rocket-propelled grenade vice an antitank guided missile at the tank."

instead of, rather than, vice, versus. [See tone box.]

Insure. See *assure, ensure, insure.*

Interagency. This term is a problem because an "Interagency" does not exist. When *Interagency* is used as a noun, the passage frequently is something like "interaction among DIA, CIA, NGA, and the Interagency"; in this context *Interagency* means, roughly, "other U.S. Government organizations." When the term is used in relation to liaison or coordination, writers generally mean liaison or coordination with DIA's counterparts throughout the Federal Government. No matter how it is used, *Interagency*, as the proper name for some sort of body, lacks a clear definition and should not be used. However, *interagency*—without the initial capitalization—is an acceptable adjective associated with something involving two or more agencies, so "interagency coordination" is fine, but "Interagency coordination" is not. The bottom line: whereas *interagency* is acceptable as an adjective, do not use *Interagency* as a noun.

Leaders, Leadership

Using *leadership* as a collective noun for the leaders of a nation or organization implies that the leaders act as a unit. If the people at the top are not in agreement or are acting independently, especially against each other, *leaders* is the better choice. Change a passage such as "supporting other national leadership" to "supporting other national leaders." In addition, beware of a sentence such as this: "The leadership has shown interest in arms deals that produce kickbacks to line their pockets"; *leadership* cannot take both a singular verb (*has shown*) and a plural pronoun reference (*their*).

in which. See *where, in which, for which.*

in, within. These terms are generally synonymous, but *within* emphasizes being "inside" or "in the inner part of." For this reason, write the more general "an incident in Georgia" rather than "an incident within Georgia" unless you need to emphasize that something is occurring well inside the country.

Islamist, Islamicist, Moslem, Muslim. An *Islamist* is a person following Islamic beliefs, especially one who has Islamic fundamentalist beliefs and holds that they apply to politics as well as to religion; the term applies especially to followers of Islamic revivalist movements. Of *Islamist* and *Islamicist*, *Islamist* is the simpler and preferred term for such a follower of Islam. Of *Moslem* and *Muslim*, *Moslem* is the older spelling but today is considered outdated and possibly offensive; *Muslim* is preferred for an adherent of Islam.

it is, there are (and similar expressions). Avoid beginning a sentence with one of these phrases. They are indirect, delaying the point; are inherently wordy; usually invert the sentence structure; and frequently are connected with passive voice. "It is clear that…." just adds words to "Clearly…." We can change "There are several conclusions that can be drawn from these hypothetical scenarios" to "Several conclusions can be drawn from these hypothetical scenarios" just by deleting *There are* and *that*. Then we can improve the sentence further by correcting the passive voice that the writer used with the inverted sentence structure: "We can draw several conclusions from these hypothetical scenarios."

its. *Its* is the possessive form of *it*. *It's* is the contraction for "it is" or "it has."

-ize. Use caution with words that end in *-ize*, which can be trendy but not widely accepted. Some of these terms, such as *economize*, *jeopardize*, and *terrorize*, are well established and fine to use in formal writing, but avoid new words with the *-ize* suffix, such as *incentivize* and *Afghanize*.

Joint. See *combined, joint.*

Just. See *only.*

last, latest, past. *Last* indicates finality, especially in referring to things that come at the end of a chronology or sequence: "This report is the last he prepared before retiring." *Past* refers to things gone by or in recent time; it is preferable in a passage such as "violence during the past 3 years" because this deals with an occurrence in time recently gone by rather than the end of a grand chronology or sequence. *Latest* can mean only "most recent": "This report is the latest on the subject."

latter. See *former, latter.*

lay, lie. *Lie* is an intransitive verb (the kind that does not take an object) meaning to recline (its most common usage) as well as to occupy a position or to remain in a given condition: "He wants to lie on the beach for a week"; "The paper lies on the desk"; "The facility lies 15 kilometers south of Baghdad." *Lay* is a transitive verb (it requires an object) meaning to place something: "Lay the report on the desk after you read it"; the past tense is *laid*: "She laid her timesheet in the inbox." Most confusion between the two verbs results because *lay* also is the past tense of *lie*: "He lay on the beach for a week"; "The paper lay on the desk."

leaders, leadership. [See tone box.]

less, less than. See *fewer, fewer than, less, less than.*

liable. See *apt, liable.*

likely. Preferred usage for *likely* as an adverb is with a modifier such as *most* or *quite*: "He most likely will decide tomorrow." As an adjective, however, it does not require modification: "He is likely to decide tomorrow."

like, such as. *Like* introduces a comparison: "Hills in this part of the country are low and rounded like those near the coast." *Such as* introduces an example from a group: "hills in the Midwest such as those along the Ohio River." For *like* as a conjunction introducing a clause, see *as if, as though, like*. See also *along with.*

located. An overused term in intelligence writing, *located* often can be omitted: "The factory is located 60 kilometers west of Karachi" can become "The factory is 60 kilometers west of Karachi."

logistic, logistics, logistical. *Logistics* is the noun form. For the adjective, either *logistic* or *logistics* is acceptable, though *logistic* is preferred. Either is preferable to *logistical.*

long term, short term. Use these terms only when the context gives the reader an idea of the timeframe. Otherwise, be more specific, such as "within 5 years." See also *near term.*

loose, lose. *Loose* means not attached, restrained, or confined. *Lose* means mislaying something, not having it anymore, being unable to control something, or failing to win.

majority. Meaning "the greater part of something" or "more than half of a total," *majority* by itself is not synonymous with *most*, which in this sense means "the greatest part." When modifiers such as *great* and *vast* are used with *majority*, the combined sense corresponds with that of *most*, and *most* is an effective substitute. When *majority* refers to a vote total, the term is singular: "The prime minister's majority in parliament for health care was only three votes." However, when it refers to a group of people or things, *majority* is a collective noun that can take either a singular or a plural verb. If the sense is oneness, use a singular verb: "The majority of parliament supports the legislation." If members of the majority are acting as individuals, use a plural verb: "The majority of the members of parliament represent working class districts."

material, materiel. *Material* is any substance from which something is made. *Materiel* refers to arms, ammunition, and equipment.

may. See *could, may, might* and *qualifiers.*

meantime, meanwhile. *Meantime* is usually a noun: "In the meantime, she waited." *Meanwhile* is usually an adverb: "Meanwhile, she waited."

media. *Media* is the plural of *medium* (*mediums* also is an acceptable plural) and usually takes a plural verb. However, when *media* is used with *the*, it is a collective noun equating roughly to "the press" or "the press and other mass communication entities." As a collective noun, *media* can take either a singular or plural verb, depending on whether the collective group is acting as a unit (singular) or as separate parts (plural): "The national media has consistently supported the prime minister, but the local media have begun to demonstrate differences, with some supporting the prime minister and some supporting the opposition."

median, mean. See *average, median, mean.*

merely. See *only.*

methodology. If you mean *method, means,* or *system,* use one of those words rather than *methodology* (the study of the science of methods or a group of procedures or rules for an inquiry or branch of study). For example, change "The oil company has not found an effective methodology for cleaning the spilled oil from the beaches" to "The oil company has not found an effective means for cleaning the spilled oil from the beaches." However, *methodology* is appropriate in "The professor explained his students' methodology for surveying the people's satisfaction with the wage supplement."

Not Only ... But Also

The difficulty in using these correlative conjunctions is maintaining the parallel structure of the pieces that follow them: specifically, the part of speech or grammatical construction following *but also* should parallel the part of speech or construction following *not only*. For example, a noun should parallel a noun; an infinitive, an infinitive; a clause, a clause. Therefore, "The unit not only sent the message to its higher headquarters but also to the main directorate" should be changed to "The unit sent the message not only to its higher headquarters but also to the main directorate." Here "to the main directorate," following *but also*, parallels "to its higher headquarters," following *not only*. The sentence also could be changed so that the parallel pieces are "sent the message to its higher headquarters" and "sent the message to the main directorate." In addition, *also* is optional, especially when the pieces following the correlative conjunctions are short.

might. See *could, may, might* and *qualifiers.*

militate, mitigate. *Militate* means "to have weight or effect" for or against: "The facts militate against your interpretation." *Mitigate* means "to moderate or alleviate": "The new social order will mitigate the suffering of the poor."

monetary. See *financial, fiscal, monetary.*

more. See *all, any, half (and other fractions), more, most, none, part, percent, percentage, some.*

more important. See *important.*

more than one. Although plural in sense, this phrase almost always takes a singular verb: "More than one factor was involved in her decision."

Moslem. See *Islamist, Islamicist, Moslem, Muslim.*

most. See *all, any, half (and other fractions), more, most, none, part, percent, percentage, some; majority;* and *only.*

most important. See *important.*

most, mostly. *Most* is not an appropriate substitute for *almost:* "almost everyone" rather than "most everyone." *Most* rather than *mostly* is the correct word to mean "to the greatest degree": "those most affected" rather than "those mostly affected." *Mostly* means "for the greatest part" or "usually": "The attacks were mostly unplanned."

Muslim. See *Islamist, Islamicist, Moslem, Muslim.*

nation. See *country, nation.*

native. See *endemic, indigenous, native.*

near-, nearly. Use *nearly* rather than *near-* to modify most adjectives—for example, "a nearly complete proposal" rather than "a near-complete proposal." An exception is *near-* in *near-real-time*—"near-real-time detection." Also see *only.*

near term. This expression is open to broad interpretation—does it mean days, weeks, months, even years? When possible, replace "in the near term" with more precise language, such as "in the next 3 to 6 months." See also *long term, short term.*

neither ... nor. See *either ... or, neither ... nor.*

none. See *all, any, half (and other fractions), more, most, none, part, percent, percentage, some.*

not only ... but also. [See tone box.]

> Parliamentarian
>
> This is an expert on parliamentary rules and procedures or a member of a parliament, though "member of parliament" is preferred for that second meaning.

nouns as adjectives. Nouns used as adjectives (*attributive nouns*) are part of standard English usage: for example, "communications intelligence" is preferable to the cumbersome "communicational intelligence." Normally you should not use a noun as an adjective when an adjectival form of the word is available—provided the two words mean the same thing. Often they do not: clearly a "cloud chamber" differs from "a cloudy chamber." In general, stringing a number of attributive nouns together is undesirable; for example, the string "weapon system development and acquisition cost reductions" should be broken up, becoming "cost reductions from weapon system development and acquisition."

number. When *the* precedes *number*, *number* takes a singular verb: "The number of mistakes has decreased." When *a* precedes *number*, *number* takes a plural verb: "A number of mistakes result from carelessness." See also *amount, number.*

obsolete, obsolescent. *Obsolete* means "no longer in use"; *obsolescent* means "becoming outdated or out of use." Thus, something *obsolescent* is becoming *obsolete.*

obviously. See *qualifiers.*

offload. *Unload* is preferable.

off of, out of. *Of* generally is unnecessary when *off* or *out* is used in the sense of motion: "jump off the roof" or "jump out the window," but "move out of the building."

ongoing. See *continual, continuous, continued, ongoing.*

onload. *Load* is preferable.

only. Place *only* close to the word it limits, usually so it adjoins the word. Observe the change in meaning when *only* is shifted within the following sentence:

Only the soldier fired the gun. [No one else fired it.]
The only soldier fired the gun. [No other soldiers were involved with this incident.]
The soldier only fired the gun. [He did nothing else with it or to it; for example, he did not load it.]
The soldier fired only the gun. [He fired nothing else.]
The soldier fired the only gun. [No other gun was associated with this incident.]
The soldier fired the gun only. [He fired nothing else.]

The most common placement problem—one almost all of us commit when we speak—is placing the limiting word in front of a sentence's verb (as in the third sample above). Rarely do we actually

mean to limit the meaning of the verb; usually we intend to limit the meaning of the verb's direct object (as in the fourth sample above).

Similarly, take care with placing *almost, every, just, merely, most, nearly, primarily, principally,* and *scarcely.*

opportune. See *accidental, fortuitous, contingent, incidental, opportune.*

oral, verbal. *Oral* refers to spoken words; *verbal,* to either spoken or written words.

ordinance, ordnance. An *ordinance* is an order, a command, a regulation, or a statute. *Ordnance* is military materiel, cannon or artillery, supplies (particularly explosives) used with the military materiel, or the department responsible for weapons and their supplies. An EOD team is an explosive ordnance disposal team, not an "explosive ordinance disposal" team.

out of. See *off of, out of.*

outside of, inside of. When *outside* is a preposition, *of* is unnecessary: "outside the building," "outside the realm of possibility." The same is true of *inside.*

over. See *during, over.*

pair, pairs. For more than one pair, *pairs* is preferable: "two pairs of antennas."

parliamentarian. [See tone box.]

part. See *all, any, half (and other fractions), more, most, none, part, percent, percentage, some.*

Predominant, Predominate, Predominantly, Predominately

Predominant is an adjective meaning having the greatest importance, influence, or authority, especially for a particular period: "the predominant weapon during the early days of the insurgency." *Predominate* is a verb meaning to prevail, to gain power or authority: "His views predominate in all government decisions." *Predominantly* is the preferred adverb.

participles. The chief usage problem connected with participles is with participial phrases that open sentences. Readers expect a modifier that begins a sentence to refer to the subject of the sentence. When a participial phrase cannot logically modify the subject of the sentence, we say the modifier "dangles"—a dangling participle or dangling modifier. In "Popping up from behind the hill, the tank was fired upon by the helicopter," the participial phrase dangles because it cannot modify the subject *tank.* The sentence should read "Popping up from behind the hill, the helicopter fired on the tank."

past. See *last, latest, past.*

pending, impending. *Pending* means "yet to come" or "not yet settled." *Impending* has a similar basic meaning but also connotes a sense of threat or menace.

people, persons, personnel. *Persons* is applicable to a specific, relatively small number: "He killed 10 persons." *People* is acceptable in this sense as well and is the word of choice for a large number of individuals, whether collectively or individually. *Personnel* is a collective noun referring to employees of an organization or members of a group. It should be avoided as a substitute for *people* or *persons*: "six persons" or "six people" rather than "six personnel exited the building." See also *populace, population* for related usage issues.

percent, percentage. See *all, any, half (and other fractions), more, most, none, part, percent, percentage, some.*

perhaps. See *qualifiers.*

period of time. *Period* almost always conveys a sense of time, so *of time* generally is unnecessary.

persuade. See *convince, persuade.*

populace, population. *Population* refers to all the people in a specific area or to the number of people in a group, class, or race in a specific area. *Populace* refers particularly to the masses—the general public—and

is not a good substitute for *population* in a statement such as "the population of the lower White River valley speaks a variant of French." See also *people, persons, personnel* for related usage issues.

portal. See *adit, entrance, entryway, entranceway, portal.*

portend, presage. *Portend* means "to serve as an omen or warning." *Presage* connotes a feeling or premonition, a presentiment. Therefore, *portend* is preferable for use with something inanimate, such as an event: "An increase in security violations could portend more serious problems within these forces."

possibly. See *qualifiers.*

practical, practicable. *Practical* indicates useful, effective, or sound. *Practicable* applies to things or concepts that are feasible or achievable and cannot apply to persons.

predominant, predominate, predominantly, predominately. [See tone box.]

presage. See *portend.*

preventive, preventative. Use *preventive.*

primarily. See *only.*

principally. See *only.*

principal, principle. *Principal* is an adjective meaning "most important" or a noun referring to a key official or to money. *Principle*, always a noun, refers to a standard of conduct, an essential element, or a general truth.

prioritize. To *prioritize* is to arrange items in order of priority, as in "prioritize work, school, and family." Avoid using *prioritize* with a single item; in that case, try "place a priority on" or "give priority to."

probably. See *qualifiers.*

pronouns for countries or ships. Use the gender-neutral forms *it* or *its.*

proved, proven. *Proved* is the preferred past participle for the verb: "The story has proved false." *Proven* is the preferred adjective: "a proven success."

provided, providing. Either term is acceptable as a conjunction: "You can use this method, provided [providing] your supervisor agrees." Neither should be used when the word *if* expresses a simple possibility: "The ceremony will be canceled if the rain continues."

publically, publicly. Use *publicly.*

purportedly. See *qualifiers.*

purposely, purposefully. *Purposely* means "intentionally." *Purposefully* indicates determination to reach a goal.

quagmire. *Quagmire* raises particular problems in intelligence writing. The standard definition is a difficult, precarious, or entrapping position. However, the word is so strongly associated with Vietnam that readers may question the parallels with that conflict. Try *predicament* or *quandary* instead.

qualifiers. Intelligence analysts must use qualifiers to remain objective and accurate. They should not, however, habitually hide judgments behind words such as *allegedly, apparently, conceivably, evidently, likely, may, might, perhaps, possibly, probably, purportedly, reportedly, reputedly, seemingly,* and *virtually.* Conversely, they should not strengthen judgments based on weak evidence with words such as *obviously, undoubtedly,* and *clearly.* Moreover, multiple qualifiers (for example, *may possibly*) are never justified.

Represent

This means "to depict" or "to symbolize," not "to constitute." "The dotted line represents the department boundary" is proper usage. "South African gold represents most of the world's output" is not.

question as to whether. See *as to.*

quote, quotation. Except in informal usage, *quote* is a verb; *quotation* is the noun. *Quote* should not be used as a noun to replace *quotation* in general writing.

range, vary. In the elements of their meanings for which *range* and *vary* are similar, *range* refers to changing or differing within limits, whereas *vary* refers to changing in succession. "Elevations range between 500 and 1,500 meters above sea level." "Temperatures vary from season to season."

rare, scarce. Both mean "infrequently occurring" or "uncommon." *Rare* connotes high value. *Scarce* connotes that supplies are insufficient.

rather than. See *instead of, rather than, vice, versus.*

real. See *actual, real, virtual.*

rebut, refute. Though these terms are somewhat synonymous, *rebut* means "to offer opposing arguments," whereas *refute* connotes success in winning an argument.

recurrence, reoccurrence. *Recurrence* has the sense of happening repeatedly or periodically, whereas *reoccurrence* suggests simply happening again.

regards. *In regards to* is substandard. Use *in regard to, with regard to, regarding, about,* or *on.*

rein, reign. A *rein* is a strap attached to a bridle, used to control a horse—hence the expressions "take the reins" and "rein in." Do not confuse it with *reign*, which refers to a monarch's rule.

relatively. See *comparatively, relatively.*

reluctant, reticent. *Reluctant* means "unwilling to act." *Reticent* means "uncommunicative" or "reserved."

remains. See *continues, remains.*

reportedly. See *allegedly, reportedly, reputedly* and *qualifiers.*

represent. [See tone box.]

reputedly. See *allegedly, reportedly, reputedly* and *qualifiers.*

respectively. *Respectively* means "one at a time, in the order indicated." It is particularly useful for matching sets of data, as in this example: "Terrorists attacked markets in Baghdad and Basrah with a vehicle-borne improvised explosive device and rocket-propelled gre-

Omitting *That*

Some writers routinely eliminate *that* when it is a relative pronoun introducing a dependent clause. Leaving out *that* generally works well when the dependent clause simply modifies another word in the sentence. For example, in "The building that the team was watching was unoccupied," omitting *that* causes no problem for readers: "The building the team was watching was unoccupied." We might even argue that the sentence is easier to read without *that*. However, when the dependent clause is the direct object of a sentence's verb, omitting *that* may cause momentary problems for some readers. Consider the following versions of the same thought:

> Moderate Muslim clerics emphasize Islam does not condone terrorism.
>
> Moderate Muslim clerics emphasize that Islam does not condone terrorism.

Omitting *that* from the first version of the sentence causes many readers to initially read "Moderate Muslim clerics emphasize Islam." Because the sentence continues and because that initial thought is simplistic (as Muslim clerics of course "emphasize Islam"), those readers quickly reread the beginning of the sentence to look for a clause that clarifies the thought. This momentary disruption does not occur with the second version of the sentence because the relative pronoun *that* is a marker readers have learned to recognize; it alerts readers to look for the clause that follows. Using *that*—rather than leaving it out—provides the marker readers are accustomed to seeing and alerts them to the structure of the sentence.

nades, respectively." Here *respectively* tells readers that the vehicle-borne improvised explosive device attack was against the market in Baghdad, while the rocket-propelled grenade attack was against the market in Basrah. *Respectively* serves little useful purpose if used at the end of a single set of data—"Terrorists attacked markets in Baghdad and Basrah, respectively"—and usually should be deleted.

reticent. See *reluctant, reticent.*

reveal. See *disclose, divulge, expose, reveal.*

rotary-wing aircraft. See *helicopter.*

roughly. See *approximately, about, roughly, some.*

Sahara desert. Because *Sahara* is Arabic for "desert," use simply *Sahara* or *the Sahara.*

sanction. *Sanction* has meanings that are almost in opposition: from approval and encouragement to penalty or coercion. Therefore, use *sanction* only if context will make its meaning clear.

scarce. See *rare, scarce.*

scarcely. See *only.*

second. See *first, second, third, and so on.*

seemingly. See *qualifiers.*

-shape, -shaped. Use *-shaped,* rather than *-shape,* in a unit modifier: "an H-shaped administration building," "an L-shaped lot." Do not combine either *-shape* or *-shaped* with a modifier that already names a shape; for example, change "a square-shaped structure" to "a square structure." In addition, use "irregularly shaped" rather than "irregular-shaped."

ship. See *boat, ship.*

short term. See *long term, short term.*

should. In intelligence writing, limit *should* to cases that carry a sense of obligation or duty. Use *if* to express a condition. Instead of "Should the outer defenses fail, guards will respond," write "If the outer defenses fail, guards will respond."

sight. See *cite, sight, site.*

significant, significantly. These words suffer from overuse in intelligence writing, especially when applied to ordinary activities or momentary changes. The alternative is to state the facts and let their significance speak for itself.

since. See *as, because, for, since.*

site. See *cite, sight, site.*

situation. Authors frequently use *situation* in connection with another descriptive term when the other term, or a form of it, can stand by itself. For example, use "emergency" by itself rather than "emergency situation" and "deteriorating security" rather than "deteriorating security situation."

-size, -sized. Use *-sized* in a phrase such as "medium-sized barrel."

some. See *all, any, half (and other fractions), more, most, none, part, percent, percentage, some; approximately, about, roughly, some;* and *certain, some.*

stalemate. This term may mislead some people because in chess, a stalemate is permanent and cannot be broken. When referring to a predicament that might be resolved eventually, try *impasse* instead.

start. See *begin, commence, start, initiate.*

stationary, stationery. Something *stationary* is still, not capable of moving, or unchanging. *Stationery* refers to paper for writing, or more generally paper and envelopes or office supplies.

such as. See *like, such as.*

suppose, supposed. *Suppose* is the present tense of a verb that means to assume, to believe, or to consider something to be likely. *Supposed* is the past tense and past participle of the same verb. As the past participle, *supposed* is an adjective that means presumed, intended, expected, or permitted: "The missile was supposed to fly at least 250 kilometers, but it failed shortly after launch."

table. As a verb, *table* can mean "to introduce something for consideration" or "to set an issue aside." If you use *table* as a verb, be sure the context is unmistakable, or use a different verb.

Taiwan, Taiwanese. See *China, Chinese, Taiwan, Taiwanese.*

team. See *collective nouns.*

telecommunication, telecommunications. See *communication, communications, telecommunication, telecommunications.*

that, which, who. Use *that* to introduce a restrictive (defining) clause—one with information that is necessary for full identification of the person or thing the clause modifies. "The platoon that was pinned down held its position" implies that although two or more platoons were involved, only one of them was pinned down, so "platoon that was pinned down" clearly defines which platoon is being discussed. Use *which* with a nonrestrictive (nondefining) clause—one with information that is not essential to fully identify the thing the clause modifies. "The platoon, which was pinned down, held its position" indicates only one platoon is being identified; it cannot be confused with any other platoons, so "which was pinned down" is not required to fully identify the platoon under discussion. Notice that a set of commas accompanies the nonrestrictive clause to set it off from the main part of the sentence; these commas are required in standard English usage. Use *who* only when people are involved; *who* can be used with either restrictive or nonrestrictive modifying clauses, so commas are essential to set off the nonrestrictive uses. Do not use *who* to introduce clauses modifying organizations; an organization is a thing, even though it represents a group of people. In some sentences with restrictive clauses, *that* and *who* may be omitted to tighten wording, although their sense will still be present. See also tone box "Omitting *That*."

there are. See *it is, there are (and similar expressions).*

third. See *first, second, third, and so on.*

though. See *although, though, even though, while.*

ties. Use *ties to* rather than *ties with. Relations with* often works as an alternative.

together with. See *along with.*

to include. *To include* has become a bureaucratic way of saying *including*. The infinitive is appropriate in a sentence such as "The Army will expand training to include live-fire exercises." Otherwise, *including* is preferred: "The regime has supplied militias with military equipment, including [not *to include*] rockets."

toward, towards. Use *toward.*

undoubtedly. See *qualifiers.*

uninterested. See *disinterested, uninterested.*

unknown, uncertain, unclear, undetermined. As an adjective, *unknown* can mean both "not known to anyone" and "not part of the writer's/speaker's knowledge." The usage problem for intelligence writing occurs when someone obviously must know whatever is being discussed but the context suggests that no one knows. One solution to this problem is to substitute *uncertain, unclear,* or *undetermined,* though those terms

will not always improve the situation. The preferred fix is to clearly identify that the author does not know, with something like "DIA does not know whether…." or "We do now know whether…." Serious shortfalls in the knowledge base can be addressed in a tone box dealing with intelligence gaps.

usage, use, employ, utilize. In the most basic sense, these terms are interchangeable; *use*, the shortest term, is the best choice except when you need the more specialized connotation of one of the other terms. *Usage* fits for the way a language or its elements are used, interrelated, or pronounced: "She studied usage of French in Canada." *Employ* is particularly applicable for obtaining or maintaining the services of an individual or object: "During World War II, U.S. companies employed many women in manufacturing." *Utilize* is suitable for something's being useful for a new function, including for an unintended purpose: "He utilized a chair to reach the top shelf."

vary. See *range, vary.*

verbal. See *oral, verbal.*

very. As an adverb, *very* means "in or to a high degree" and often is used to intensify adjectives or other adverbs: "very happy," "very annoyed," "very concerned," etc. The problem comes with overuse of *very* for this purpose, especially with terms for which degrees of intensity are questionable. Few people would argue with dropping *very* from a phrase such as "very complete," as something either is or is not "complete." However, what real meaning does *very* add if we write "very nearly complete"? Even if the author has a difference in mind between "nearly complete" and "very nearly complete," are readers likely to understand that difference in intensity? When you see *very* modifying an adjective or another adverb, ask yourself whether *very* adds anything useful or should be deleted.

vice, versus. See *instead of, rather than, vice, versus.*

virtual. See *actual, real, virtual.*

virtually. See *qualifiers.*

way, ways. Use *way*: "She was a long way from home."

weapon, weapons. Both singular and plural forms are acceptable as modifiers, though the singular (*weapon*) is preferred in most instances, especially when using *weapons* would duplicate the s sound in both modifier and word modified: for example, *nuclear weapon storage* rather than *nuclear weapons storage*; *chemical and biological weapon problems* rather than *chemical and biological weapons problems.*

website. See *cite, sight, site.*

where, in which, for which. Because *where* is associated with locations, *in which* and *for which* are better choices than *where* when the context of a passage has nothing to do with a place or places. "In other cases, where U.S. involvement is not a factor, the working group recommends…." would be better written as "In other cases, in which U.S. involvement is not a factor, the working group recommends…." Similarly, "individuals involved in special assignments, where overtime requirements are likely to exist, should…." would be better as "individuals involved in special assignments, for which overtime requirements are likely to exist, should…."

whether. See *if, whether.*

which, who. See *that, which, who.*

while. See *although, though, even though, while.*

with. Avoid using *with* as a conjunction similar to *and*. For example, write "Attention has focused on maritime security, and the president has signed an order to create a coast guard" instead of "Attention has focused on maritime security, with the president signing an order to create a coast guard."

within. See *in, within.*

Economy of Words

Concise wording makes reading easier. The key is compression, not omission. In particular, watch for unnecessarily wordy phrases that have become habitual in our writing. One small connecting word often can do the work of several. In addition, watch for redundancies—eliminating the duplicative idea compresses and sharpens the expression.

For	*Try*
abortive coup attempt	abortive coup
absence of	no
absolutely essential	essential
acute crisis	crisis
adequate enough	adequate
a distance of 14 kilometers	14 kilometers
advance planning	planning
afford an opportunity	let, permit, allow
after the conclusion of	after
aggregate total	total
a large portion of	many, much of
all-time record	record
along the lines of	like, such as
am (is, are) going to	will
a myriad of details	myriad details
appear to be	appear
appointed to the post of	appointed
around the world	worldwide
at a later date	later
at the present time	now, currently, at present
at this point in time	now, currently, at present
back up	back
before long	soon
blue in color [also applies to other colors]	blue [or other named color]
bring an end to	end
built a new	built a
by means of	by, with
by the time	when
close confidant	confidant
close proximity	close, near, proximity
close scrutiny	scrutiny
collaborate together	collaborate
combat environment	war, battlefield
combine together	combine
come in contact with	meet
commented to the effect that	commented that
completely unanimous	unanimous
completely untrue	untrue

For	*Try*
complete monopoly	monopoly
conduct a raid	raid
consensus of opinion	consensus
contingent upon	depends, hinges on
continue to maintain	maintain
continue to remain	remain
cooperate together	cooperate
cost the sum of	cost
cover over	cover
crisis situation	crisis
dates back from (to)	dates from (to)
depart from	leave
despite the fact that	although
destroyed by fire	burned
divide up (off)	divide
due to the fact that	because, since, hence
during such time as	while
during the time that	while
each and every one	each
economic situation	economy
eliminate altogether	eliminate
end product	product
end result	result
entirely absent	absent
entirely complete	complete
entirely eliminated	eliminated
established a new	established
estimated at about	estimated at
famine condition	famine
few in number	few
filled to capacity	filled
final outcome	outcome
final settlement	settlement
firm commitment	commitment
foreign import	import
form a new unit	form a unit
for the amount of	for
for the most part	usually
for the purpose of	for, to
fresh beginning	beginning
full complement of	complement of
future prospect	prospect
galvanize into action	spur, prompt
gave a briefing	briefed

For	*Try*
general public	public
has (have) the ability (capability, capacity) to	can
hope for the future	hope
hour of noon	noon
important essentials	essentials
in addition . . . also	in addition
in an effort to determine	to determine
in a number of cases	some, sometimes
in a position to	can, able to
inasmuch as	because
in a suspicious manner	suspiciously
in case	if
include among them	include
in conjunction with	and, or
in connection with	in, on, about, with
individual persons	individuals
in lieu of	instead
in order that	so
in order to	to
in regard to	regarding, on, about, concerning
in relation to	concerning, regarding, about
in short supply	scarce
insofar as	because, since, as
in terms of	in, for
in the amount of	for
in the city (town) of	in
in the course of	in, during, while
in the event that (of)	if
in the interest of	for
in the interim period between	in the interim
in the majority of instances	usually
in the midst of	amid
in the month of	in
in the near future	soon, shortly
in the process of fighting	fighting, while fighting
in the vicinity of	near, around
in this day and age	today
in 2 years' time	in 2 years
in view of the fact that	since, because, although
join together	join
just recently	recently
large in size	large
last of all	last, finally
launch a new operation	launch an operation, begin
link together	link

For	*Try*
located at	in, at
major breakthrough	breakthrough
make a decision	decide
make arrangements	arrange
make preparations	prepare
many in number	many
may possibly suggest	suggest
meet up with	meet
merge together	merge
more paramount	paramount
more perfect	perfect
most unique	unique
multitude of	many
never before in the past	never before
new discovery	discovery
new initiatives	initiatives
new recruits	recruits
of an indefinite nature	indefinite
of great importance	important
on a few occasions	occasionally
on a regular basis	consistently, regularly
on a timely basis	fast, quickly, rapidly
on condition that	if
one of the last remaining	one of the remaining
one of the purposes (reasons)	one purpose (reason)
on the occasion of	when, for
on the part of	by, for, among
owing to the fact that	because, since, hence
pare down	pare
passing phase	phase
penetrate into	penetrate
personal friend	friend
plan ahead	plan
plan in advance	plan
plethora of	many
pressing for the imposition of a curfew	pressing for a curfew
primarily focused on	focused on
prior to	before
prominent and leading	prominent
provided that	if
provide support to	support
reason is because	reason is
reason why	reason
recalled back	recalled
recur again	recur

For	*Try*
reduce down	reduce
repeat again	repeat
resume again	resume
retain his position	remain
revert back	revert
rise up	rise
separate out	separate
serious crisis	crisis
serve(s) as	is, are
SIGINT reports [or other INT]	SIGINT [or other named INT]
skirt around	skirt
small in size	small
still remains	remains
subsequent to	after, since
substantial portion	much, large part
succeeded in defeating	defeated
succeeded in ending	ended
sworn affidavit	affidavit
take action on	act on
temporary reprieve	reprieve
true facts	facts
under active consideration	being considered
until such time as	until
usual customs	customs
violent explosion	explosion
when and if	if
whether or not	whether
with reference to	on, about, concerning
with regard to	regarding, on, about, concerning
with the exception of	except, except for
with the result that	so
worst ever famine	worst famine

Simple Words

Keep writing simple and direct. In many cases using the following simple words will strengthen the writing and make it easier to read.

For	*Try*
accomplish	do
adequate	enough
advantageous	helpful
advise	report, say, tell
ameliorate	improve, better
approximately	about, nearly, roughly, some
ascertain	learn, find out
assistance	help, aid
attempt	try
citizenry	citizens
commence	begin, start
concerning	about, on
construct	make, build
contradistinction	opposite
customary	usual
deem	think
demonstrate	show
dialogue	conversation, discussion, talks
dispatch	send
dwell	live
effectuate	cause
endeavor	try
evince	show
exacerbate	aggravate, worsen
fabricate	make, build
facilitate	ease, help
finalize	complete, finish, conclude
frequently	often
heretofore	before, until now
impact	effect
implement	carry out, fulfill, do
inaugurate	begin, start
individual flotation device	lifejacket
induce	persuade
initial	first
initiate	begin, start
innumerable	many
materialize	happen, appear
maximum	most, greatest
minimum	least, smallest

For	*Try*
necessitate	force, cause
notwithstanding	although, despite
obfuscate	hide, mask
objective	goal, aim
opine	think, believe
optimum	best
output	product, yield
per	a, each
perceive	believe, see
populace	people
prerogative	privilege
prioritize	rank
procure	get, buy
proliferate	spread
rail infrastructure	railroads
regarding	about, on
request appropriations for	ask for money for, ask for funds for
reside	live
rotary-wing asset	helicopter
spaceborne platform	satellite
stated	said
stockpile	stock
subsequently	later
sufficient consideration	enough thought
terminate	end, finish
transmit	send
transpire	take place
ultimate	final
upon	on
utilize	use
vice	instead of, rather than
virtually	almost
weaponry	weapons
whenever	when

CHAPTER 6: Punctuation

UNCLASSIFIED

What the semicolon's anxious supporters fret about is the tendency of contemporary writers to use a dash instead of a semicolon and thus precipitate the end of the world. The main reason people use the dash is that they know *you can't use it wrongly*—which, for a punctuation mark, is an uncommon virtue.

—Lynn Truss, *Eats, Shoots & Leaves*

UNCLASSIFIED

CHAPTER 6: Punctuation

Punctuation is intended to promote readability. It helps clarify the structure of written material and provides clues for how to read material aloud. Sometimes punctuation is critical for readers' understanding of what an author intended to say.

Apostrophe

For Possessives

The Basic Rule. Form the possessive case of singular nouns, indefinite pronouns, and abbreviations by adding an apostrophe and a lowercase s. For most plural nouns add only an apostrophe; however, for irregular plurals (ones that do not end in s), add an apostrophe and a lowercase s.

boy: the boy's book	boys: those boys' books
woman: the woman's briefcase	women: the women's briefcases
Jones: the elder Jones's papers	Joneses: the Joneses' home
Thai: that Thai's passport	Thai: those Thai's passports
CO: the CO's orders	COs: those COs' orders
Shiite: the Shiite's factory	Shia: those Shia's neighborhood
each other: each other's territory	

The basic rule applies to proper names and abbreviations ending in sibilants (the hissing sound of an *s*, *x*, or *z*). However, leave off the *s* after the apostrophe if the extra sibilant is not normally pronounced.

Gibbons: General Gibbons's tactics	Marx: Marx's manifesto
Juarez: Juarez's troops	Berlioz: Berlioz's music
CBS: CBS's broadcasting	Damascus: Damascus's intentions
HAMAS: HAMAS's activities	*but* the Netherlands' policy
	the Philippines' interest

Some Complexities. One exception is for common nouns ending in *s* or *ce* when followed by a word beginning with *s*: in these cases the possessive of the common noun is formed with only an apostrophe.

for goodness' sake	for convenience' sake

For *corps* (both singular and plural and whether as a common or proper noun), add only an apostrophe.

the corps' barracks	the two corps' mission
11th Corps' field hospital	the Second Artillery Corps' strategic missiles

For compound titles, make the last word—the word closer to the thing possessed— possessive.

the secretary general's speech	the secretaries general's speeches
the commander in chief's decision	the commanders in chief's decisions
the assistant chief of staff's policies	the assistant chiefs of staff's policies

To show joint possession for two or more nouns, make only the last one possessive.

Phil and Dick's collaboration on the Sudan report was a success.

However, to show individual possession, make each noun possessive.

Phil's and Dick's draft reports on Sudan did not agree on two key points.

Follow the form of the original for geographic names; names of firms, organizations, and institutions;

and titles of publications. Of note, most place names today—but not all—do not include apostrophes, and some that did at one time (such as Harper's Ferry in the beginning) no longer have the apostrophe.

Harpers Ferry	Martha's Vineyard
Lloyds Bank; follow Lloyds's lead	Lloyd's insurance; follow Lloyd's lead
Johns Hopkins University	*Reader's Digest*

What we call the possessive case often is used when ownership is not involved. Do not be concerned with the argument that inanimate nouns cannot possess things. The form being used is the genitive case—which came to be called the possessive case in the 18th century—and does not involve possession. These forms are perfectly acceptable.

2 hours' pay	a dollar's worth
the room's furnishings	the airplane's speed
for pity's sake	for old times' sake

Do not use an apostrophe with the possessive form of personal pronouns. Be particularly careful not to confuse the possessive *its* with the contraction *it's* (for "it is" or "it has"). Generally avoid contractions in intelligence writing.

his	ours
hers	yours
its	theirs

Apostrophes and Descriptives

Do not use an apostrophe after the name of a state, country, or most other bodies ending in s, or after words more descriptive than possessive, except when the plural does not end in s.

Massachusetts laws	*but*	children's hospital
Bureau of Ships report		Commission on the Status of Women's headquarters
writers guide		Congress's priorities
officers club		
commanders conference		
dockworkers strike		

For a date, be careful to distinguish between the plural (formed with a lowercase s, as in *1970s*) and the possessive (formed with an apostrophe and a lowercase s for a singular date, as in *1970's*, or with just an apostrophe for the plural possessive, as in *1970s'*). The plural *1970s* refers to the years in that decade (1970 through 1979), whereas the possessive *1970's* refers to something belonging to that year and the plural possessive *1970s'* to something belonging to that decade.

For Some Plurals

Except as noted in the exceptions below, use an apostrophe and a lowercase s to form the plural of an abbreviation that ends in a lowercase letter or to form the plural of a single letter or digit.

cy's	7's and 8's
dotting i's and crossing t's	

- Do not use an apostrophe for the plural for an abbreviation that is treated as a word:

emails	lasers
medevacs	radars
scubas	sonars

- Do not use an apostrophe and a lowercase s for the plural of a unit of measure, as units of measure appear the same for both singular and plural instances.

  67 km (*not* 67 kms) 550 t (*not* 550 t's)

- Do not use an apostrophe for the plural of an abbreviation ending in an uppercase letter or a number.

  ICBMs SS-25s
  MiGs H-IIs

Brackets

Square Brackets

Use square brackets—[ ]—for the following:

- To enclose a parenthetical expression inside a set of parentheses.

  The temperature in the room (20 °Celsius [80 °Fahrenheit]) was the main reason the meeting broke up early.

- To enclose an interpolation, such as an editorial remark, within a direct quotation. However, a parenthetical remark that is part of the original material being quoted and that is within parentheses would remain in parentheses.

  The defense minister stated that he would "resolve the apparent policy shift with him [the prime minister] before the meeting."

If you need to label a mistake, such as a misspelling or wrongly used word, within a direct quotation, you can show *sic* (in roman rather than italic type) within square brackets immediately following the error you are labeling.

The article seemed to be cursed from the start, as its title first appeared as "Elections in Chili [sic] Likely To Topple President."

This interpolation tells readers that you are aware of the mistake and did not introduce it. Use this technique sparingly, however, as readers also may wonder why you felt the need to quote erroneous material. A better alternative, if it is available, is to present the quotation in a way that will allow you to omit the erroneous text.

Angle Brackets

Use angle brackets—< >—for Intelink and Internet URLs (uniform resource locators), email addresses, and account names when you present them in text, but omit angle brackets with live links. This technique was devised to clearly distinguish between punctuation that is part of an electronic address and punctuation for the sentence. It also allows for a break to be made in a URL that is too long to appear on a single line; make such a break at internal punctuation within the URL, and do not add any sort of punctuation at the break in the line. You may have to insert the angle brackets a second time to make them appear in text if Word automatically converts the URL to a hyperlink.

The World Factbook is available on JWICS at <https://www.cia.us.qlat/DI/Factbook/index.html> and on NIPRNET at <https://www.cia.gov/library/publications/the-world-factbook/>.

Angle brackets are unnecessary when referring to a website name, even if ".com" is part of the name.

The group used Twitter to spread word of the demonstration.
The online newspaper *Boston.com* carried a photo of the suspect.

Bullets

Marking Bulleted Items

Use a bullet (•) or caret (>), depending on the product line, to set off each item of an indented list. Using subordinate levels below the bullet level is discouraged. If subbullets are necessary in publications and correspondence, mark each with an en-dash (–), which Word makes available for this type of bullet.

- The first item in a bulleted list.
- The second item in the bulleted list.
  - A subbullet.
  - A second subbullet.
- The third item in the bulleted list.

Keep indentation as formatted in DI's current product line templates for bulleted lists. However, for correspondence, such as info memos, action memos, and response memos, align bullets with the left margin. The left end of the en-dash that marks a subbullet should be aligned on the left with the start of the text for the primary bullets.

Presenting Bulleted Items

For textual products (but not briefing slides), use an initial capital letter for the first word of the material in each bulleted item (or each subbulleted item), and end the material with a period (unless the context calls for different ending punctuation, such as a question mark). Use this form regardless of whether a bulleted item is a word, phrase, or full sentence. Of course, a bulleted item also could have multiple sentences, and these would be punctuated as normal sentences. Most of the formats DIA uses for both substantive products and correspondence call for blank lines before and after each bulleted item.

For briefing slides, DIA uses slightly different presentation. Each bulleted item begins with an initial capital letter, but the bulleted items have no end punctuation unless a bulleted element has multiple sentences; then only the final sentence has no end punctuation.

Colon

Use a colon (:) for the following:

- At the end of a sentence to point to material that summarizes or expands on the thought in the preceding portion of the sentence. Any grammatical unit can follow the colon: a word or phrase, a series of words or phrases, a dependent clause or clauses, or even a sentence or series of sentences.

  The foreign delegation visited three cities in the United States: New York, Chicago, and Los Angeles.

  The general is well qualified to serve as Army commander: he has served 5 years as the vice commander and previously held key leadership posts in each of the military districts.

  If a single sentence follows a colon for this purpose, begin that sentence with a lowercase letter—essentially linking it to the previous sentence, as in the second sample above. However, if a series of sentences follows the colon, begin each of them with a capital letter.

- To introduce a list set off from the rest of the text by indentation (as with the colon in the last example in the box below).
- To introduce some direct quotations. A colon is the normal punctuation mark to introduce a direct quotation when a long quotation is indented as a block to separate it from a paper's body text or after a formal introduction such as "as follows" or "the following."

The prime minister said the following in a speech outside the parliament building on 27 March 2010:

> My government is not responsible for the tragic events of 25 March. Irresponsible individuals rioted, destroyed public property, and endangered all our citizens. The government had no choice except to stop these illegal activities.

Improper Colon Use

Do *not* use a colon between a verb and its objects or between a preposition and its objects, unless the colon sets off an indented list.

Not: The Army wants several U.S. military systems, such as: attack helicopters, Patriot missiles, and Humvees.

But: The Army wants several U.S. military systems: attack helicopters, Patriot missiles, and Humvees.

Or: The Army wants several U.S. military systems, such as attack helicopters, Patriot missiles, and Humvees.

Or: The Army wants several U.S. military systems:

- Attack helicopters.
- Patriot missiles.
- Humvees.

For the introduction to the indented list above, the sentence could have been written like this: "The Army wants several U.S. military systems, such as"; even though this introduction would not be grammatically wrong, the *such as* is unnecessary, as the colon by itself is sufficient to introduce the list that follows.

Punctuation for Source Reference Citations (Endnotes) in Intelligence Products

Placement of Reference Numbers in Text in Relation to Sentence Punctuation. Endnote references in the text of a product are numbered sequentially, beginning with 1, and should be placed as close as reasonably possible after the text to which the number refers—but always at the end of a clause or phrase and after ending punctuation (comma, semicolon, period, and quotation marks). Often the endnote reference number can go at the end of a sentence, as in the first sample below.

... end of sentence.[1] New sentence....

Two days later the so-called Green Revolution began;[2] young members of the People's Progressive Party rioted in the capital.

Although the prime minister insisted that his administration was not responsible for the rioting in the capital,[3] he offered little justification for the brutality of the repressive measures he is believed to have ordered to bring quiet to the city's streets.

Punctuating Multiple Reference Numbers in the Same Location. For writing in academia, authors almost never need multiple footnote or endnote reference numbers in the same location. Instead, they use a single reference number, which corresponds to a footnote or endnote presenting information for the multiple sources. This practice is not practical for DIA's intelligence products, however, because of the coding DIA uses for posting products and because selected endnotes may have to be sanitized for some dissemination. As a result, DIA products sometimes have multiple endnotes in the same location. Multiple reference numbers should be separated with a comma and a space after each reference number.

... end of sentence.[4, 5, 6] New sentence....

Note, however, that other punctuation marks, such as a comma or em-dash (or no punctuation at all), also may be appropriate before a direct quotation, depending on how the quoted material fits into the writer's sentence pattern. For example, the sample above could have been written like this instead:

In a speech outside the parliament building on 27 March 2010, the prime minister said that his administration was

> not responsible for the tragic events of 25 March. Irresponsible individuals rioted, destroyed public property, and endangered all our citizens. The government had no choice except to stop these illegal activities.

(See also page 130 for use of a comma to introduce a short quotation.)

- Between a title and a subtitle.

  "Russia: Outlook for Key Military Reforms"

An em-dash can fulfill this same function, though a colon is more common. Moreover, if you need to join elements associated with a complex title and subtitle, use a colon for one punctuation mark and an em-dash for the other rather than using two colons or two em-dashes.

"Captives: A Month With the Taliban—What They Saw and Heard"

- To show a ratio. If the ratio is used as an adjective, however, use hyphens and *to*.

  Her chances are 15:1.
  but She has a 15-to-1 chance.

Comma

Use a comma (,) for the following:

- To separate two words or figures that otherwise might be misunderstood.

  Of the total, profit from the first sale raised the most concern.
  In 2009, 870 tractors were completed. (*But:* In 2009 only 870 tractors were completed.)

- After every item in a series except the last item. This rule applies whether the items in the series are single words, phrases, or clauses.

  Exports include copper, lead, zinc, and tin.
  Copper, lead, zinc, and tin are exported.

If any item within a series itself requires commas, use semicolons to separate the items of the series. However, the same rule still applies for semicolons for the major parts of the series and for commas within any of the parts.

Three major NATO commands are subordinate to Allied Command Operations, with headquarters in Brunssum, Netherlands; Naples, Italy; and Lisbon, Portugal.

Targeting requires the ability to locate targets; identify them, determine their vulnerability, and evaluate potential weapon effects against them; deliver appropriate weapons to a target; and evaluate the resulting damage.

Serial Comma

Note that DIA uses a comma after the next-to-last item in a series (serial comma). Advocates of "open" punctuation leave out the comma after the next-to-last item in a series of three or more things—a style some popular periodicals employ. Generally, however, this is a disservice to readers. Because items within a series may be compound, if you leave out the comma after the next-to-last item, readers cannot tell when they see *and* or *or* in a series whether that word joins parts of a compound element within the series or whether it precedes the final item of the series. Always providing the comma after the next-to-last item in the series will eliminate the need for rereading to correctly understand the series.

- Before a coordinating conjunction that joins two independent clauses (full sentences). Coordinating conjunctions are *and, or, nor, for, but,* and sometimes *so* and *yet.*

  Traffickers smuggle in both cocaine and marijuana, but domestic marijuana is available in small quantities.

  Note: Do not confuse a coordinating conjunction that joins independent clauses with one that joins verbs in the same clause. No comma is required before *and* in the following sentence:

  He served in the Air Force until 1988 and has worked for DIA since then.

- After a dependent clause that begins a sentence.

  Because they needed funds to expand their operations, the insurgents became involved with drug trafficking.

  A comma usually is not necessary before a dependent clause that ends a sentence, especially a dependent clause that is closely related to the meaning of the main clause. In the following example, for instance, the ending dependent clause explains why the main clause is true.

  The insurgents became involved with drug trafficking because they needed funds to expand their operations.

  However, a dependent clause that follows a sentence's main clause and is not essential to the meaning of the main clause—usually because it provides additional information or departs from the main clause in a new direction—may require a comma at the start.

  Insurgents in the mountains are well protected, whereas those attempting to operate in the lowlands are more vulnerable to interdiction.

- After a dependent clause immediately following a coordinating conjunction that joins two independent clauses. (The coordinating conjunction in the following example is *but.*)

  The Army commander initially claimed that guerrillas had attacked the convoy, but after operational details appeared in the press, he revealed that friendly troops had fired on the trucks.

  Note: Advocates of "close" punctuation also would use a comma between *but* and *after*—at the beginning of the dependent clause that follows the coordinating conjunction—because the dependent clause interrupts the primary flow of thought in the sentence. That way of punctuating the sentence, however, would result in commas on both sides of *but,* which many readers find excessive, so most writers and readers today are more comfortable with the comma at the end of the dependent clause (following *press*) but would not use a comma at the start of the dependent clause (before *after*).

- After a long phrase that begins a sentence. No clear guidance defines *long* for this purpose. The role of the comma is to aid readers—by pointing out where the sentence changes from introduction to main clause—so look at the sentence as readers would. Usually you'll want a comma after an introductory phrase of more than three words. A comma is optional but may aid readability after a short introductory phrase followed by a capitalized word.

  Because of his need for control, he expanded the operations of his organization.
  After his operation he retired from the firm.
  In March, Andorra announced the establishment of a national riverine surveillance system.

- Both before and after a long phrase or clause that occurs between the subject and the verb of a sentence.

  The platoon, having been ordered to prepare to disable the bridge, attached explosive charges to the bridge supports.

  A clause or phrase such as this one between a sentence's subject and verb may interrupt the flow of thought too much and may make a sentence unnecessarily complex. Moving the interrupting clause to the beginning of the sentence (or occasionally to the end) may result in a better sentence.

Watch for Dangling Modifiers

When a sentence includes a modifying phrase or clause but lacks a word the modifier can reasonably modify, the modifier "dangles."

- The most common dangling modifier occurs at the beginning of a sentence. Readers expect a modifier at the start of a sentence to modify the sentence's subject. When that relationship is not reasonable, the modifier dangles.

Consider the following:

> Arriving at the forward operating base after the attack had begun, the perimeter was quickly secured by the company.

This sentence literally says that the perimeter arrived at the forward operating base after the attack had begun. Because that is nonsensical, the opening long modifying phrase dangles. One way to repair the sentence is to put the appropriate term in the subject position:

> Arriving at the forward operating base after the attack had begun, the company quickly secured the perimeter.

Be particularly careful with sentences beginning with *Based on ...*, especially when such a sentence opening is paired with a passive voice construction, like this one:

> Based on the sequence of operations just prior to the failure, the system design is considered to have caused the failure.

This sentence says that the system design based something "on the sequence of operations just prior to the failure." We cannot tell from this sentence who assessed the failure on the basis of the sequence of operations, but we know it was not the system design itself. The sentence needs to be rewritten.

> Having been ordered to prepare to disable the bridge, the platoon attached explosive charges to the bridge supports.

- To set off a nonrestrictive word, phrase, or clause. *Restrictive* material is essential for the definition of whatever it modifies and is not set off from it. *Nonrestrictive* material is not essential for definition of whatever it modifies, interrupts the flow of the sentence, and is separated from the thing modified with a comma or set of commas.

> She briefed on three topics that were of high interest.
>
> She briefed on three topics, which were of high interest.

Marking Interruptions

Three types of punctuation marks can set off interrupters: commas, parentheses, and em-dashes. Choosing among them depends on the amount of emphasis you want to give to the interrupter:

- Commas set off the interrupting material, marking it as nonrestrictive, without affecting the emphasis on the interruption. That is, commas provide standard emphasis.
- Parentheses take emphasis away, making the words set off like a whispered aside.
- Em-dashes add emphasis to the words they set off.

The first of those sentences *implies* that more than three topics existed and says that three of them were high-interest topics. Because *that were of high interest* restricts the definition of *three topics*, the modifier is essential to the meaning and is not set off with a comma. The second sentence *says* three topics existed; no more definition is required, though the sentence adds the nonrestrictive information that the three topics were highly interesting. If the nonrestrictive material had come in the middle of the sentence, it would have needed commas on both sides.

> The supervisor, who was dismissed in 1972, was rehired the next year.

What if more than one supervisor had been fired—one in 1972 and one in 1978? Then *who was dismissed in 1972* would be necessary for the definition of *supervisor* and the sentence would have no commas:

The supervisor who was dismissed in 1972 was rehired the next year.

- To set off a nonrestrictive word, phrase, or clause used in apposition to a noun. An appositive (the material in apposition to the noun) is a special type of interrupter that provides an explanatory equivalent for the noun it follows. Like other interrupters, it can be either restrictive or nonrestrictive, depending on whether the appositive is necessary for understanding the noun it accompanies. Nonrestrictive appositives are set off from the noun for which they are equivalents—usually with a set of commas (though parentheses or em-dashes could be used instead)—whereas no punctuation should be used to set off a restrictive appositive.

  Two of Saddam Husayn's children, Uday and Qusay, died on 22 July 2003 in a firefight with troops from the 101st Airborne in Mosul.

  The appositive *Uday and Qusay* is nonrestrictive because we can understand the main point of the sentence, that two of Saddam's children were killed, without the names of which children died in the firefight.

  Saddam's children Uday and Qusay died on 22 July 2003 in a firefight with troops from the 101st Airborne in Mosul.

  Here the appositive *Uday and Qusay* is restrictive—and not set off with commas—because not all of Saddam's children died in the firefight.

Beware of Comma Splices

A comma splice—a misuse of the comma—occurs when a writer joins two independent clauses with only a comma.

He worked for the company for 20 years, he took a leave of absence from 1952 to 1954.

Few authors in DIA would make that mistake. A more common error introduces a comma splice when a conjunctive adverb comes between the two clauses but the writer uses only a comma before the conjunctive adverb:

He worked for the company for 20 years, however he took a leave of absence from 1952 to 1954.

or

He worked for the company for 20 years, however, he took a leave of absence from 1952 to 1954.

A conjunctive adverb and a comma or commas cannot join two independent clauses in that fashion. Changing the first comma to a semicolon is one way to correct the error.

He worked for the company for 20 years; however, he took a leave of absence from 1952 to 1954.

- To set off a contrasting statement in a sentence.

  Stanley, not Jameson, won the trophy.

  Workers completed construction, but neither on time nor within the budget.

- After a conjunctive adverb unless it is the last word in the sentence. Conjunctive adverbs are words like *however, moreover, nevertheless,* and *therefore*. A conjunctive adverb in the middle of a clause needs commas on both sides; if it is the last word in a sentence, it will be preceded by a comma.

He worked for the company for 20 years. However, from 1952 to 1954 he took a leave of absence.
He worked for the company for 20 years; however, from 1952 to 1954 he took a leave of absence.
He worked for the company for 20 years;
from 1952 to 1954, however, he took a leave of absence.
He worked for the company for 20 years;
from 1952 to 1954 he took a leave of absence, however.

- To separate coordinate adjectives (unless they are joined by *and*).

  It will become a neutral, nonaligned state.

  Coordinate adjectives independently modify a noun or noun phrase. In the sample sentence above, both *neutral* and *nonaligned* modify *state* independently. This is not the case with cumulative adjectives. In "illegal drug trafficking," *illegal* modifies not just *trafficking*, but *drug trafficking*. Therefore, *illegal* and *drug* are not coordinate, so no comma should go between them.

Coordinate and Cumulative Adjectives

Because of the independence of coordinate adjectives, you can check for two characteristics that help distinguish them.

- Coordinate adjectives are reversible; cumulative adjectives are not. You could write *nonaligned, neutral state*, but *drug illegal trafficking* just sounds peculiar.
- *And* fits naturally between coordinate adjectives, but not between cumulative adjectives. You could write *neutral and nonaligned state* but not *illegal and drug trafficking*.

Of course, modifier chains can include both coordinate and cumulative adjectives. Consider the modifiers in the following sentence.

Several short, swift tributary streams crossed the clearing.

Short and *swift* are coordinate adjectives; both modify *tributary streams* separately and are separated by a comma. However, *several* modifies *short, swift tributary streams*, and the *short, swift* combination modifies *tributary streams* (not just *streams*), so no comma comes after *several* or after *swift*.

- To introduce some direct quotations. A comma is the normal punctuation mark to introduce a short direct quotation, separating it from the identification of the speaker.

  The minister said, "We must avoid hostilities."
  "We must avoid hostilities," the minister said.

  However, do not use the comma with a quotation that is only part of a sentence. A sentence that includes a partial quotation requires only punctuation that would be normal for the sentence itself—with nothing besides quotation marks to set off the quoted material.

  The minister said his nation "must avoid hostilities."

  In addition, do not use a comma to set off an indirect quotation. An indirect quotation captures the thought from the original material through a summary or paraphrase but does not directly quote the original.

  The minister said his nation needed to steer clear of fighting a war.

  (See also page 124 for use of a colon to introduce a long quotation indented as a block or a quotation that follows a formal introduction.)

- To indicate that a word or words have been omitted.

  Profit in 2008 was $4 million; in 2010, $10 million.

- To separate an individual's title and an organization's name when *of* and *of the* are not present.

  John Smithson, director, Research Department, Stockton Company....

- To set off a province, state, or country from a city name; *Jr.*, from a person's name; and *Inc, Ltd,* or *SA,* from a corporate name.

  Born in Baltimore, Maryland, Franco Garibaldi, Jr., now directs Recycling, Inc.

- To separate digits in the thousands, millions, and so on—except for years, military unit designators, clock time, most serial numbers, fractional portions of decimal numbers, page numbers, and radiofrequencies in the thousands of kilohertz.

2,973	*but*	during 2009
3,946,834		the 1028th Brigade
		1400 hours
		job number 518225/10
		3,732.14592
		pages 3614 and 3617
		1812 kHz (*but* 15,117 kHz and 1,832 MHz)

Dashes and the Hyphen

Dashes—the em-dash and the en-dash—and the hyphen differ in length. Theoretically a hyphen is half the length of an en-dash, which is half the length of an em-dash. However, various typefaces do not necessarily produce these length relationships exactly. The most we can be sure of is that an em-dash (—) is longer than an en-dash (–), which is longer than a hyphen (-).

More important are the differences in uses for these punctuation marks. This chapter covers em- and en-dashes. Hyphens are used in compounding, which Chapter 7 covers in detail.

All three marks are produced without spaces on either side:

em-dash:	She participated in this attack—as she did in four earlier attacks.
en-dash:	13 December 2009–5 January 2010
hyphen:	self-propelled

Dashes

Em-Dash

Use an em-dash (—) for the following:

- As with commas or parentheses, to set off an interrupter in a sentence. If the interruption ends the sentence, only one dash, at the beginning, sets off the material. When an interrupter occurs inside a sentence, a set of dashes is required. Em-dashes that set off interrupting material emphasize the interrupter. The interrupter could be an appositive that the writer wishes to emphasize, as in the third sample below, or a point that abruptly changes the flow of thought in a sentence, as in the fourth sample.

  He was a key player in upsetting the coup attempt—as he was with two previous attempts.

  In this coup attempt—as with two previous attempts—he was a key player in upsetting the work of the coup plotters.

  Before Saddam Husayn was captured, his two sons who were significant in his regime—Uday and Qusay—died in a firefight with U.S. troops in Mosul.

  Workers completed construction in April—almost half a year later than projected.

Do not use an em-dash as a substitute for a semicolon simply to connect two independent clauses. Clauses connected with an em-dash should have a stronger connection than the following example demonstrates:

The minister traveled to Rome—later he continued to Istanbul.

- As with a colon, at the end of a sentence to point to material that summarizes or expands on the material in the preceding portion of the sentence. A word or phrase, a series of words or phrases, a dependent clause, or an independent clause can follow the dash. Unlike the colon, however, a dash would not precede a series of sentences.

  The foreign delegation visited three cities in the United States—New York, Chicago, and Los Angeles.

- Like a colon, between a title and a subtitle.

  "Russia—Outlook for Key Military Reforms"

A colon is more common for that purpose. However, if you need to join elements associated with a complex title and subtitle, use a colon for one punctuation mark and an em-dash for the other rather than using two colons or two em-dashes.

"Captives: A Month With the Taliban—What They Saw and Heard"

En-Dash

Use an en-dash (–) for the following:

- To connect two parts of continuing or inclusive numbers, whether page references, dates, or time. When continuing numbers are joined in this manner, the range means "to and including" or "through."

pages 1214–33	August–September 2010
1400–1430 hours	13 December 2009–5 January 2010

However, do not use an en-dash (or a hyphen) to replace *to* in "from x to y" or *and* in "between x and y":

not	from 10–12 August	*but*	from 10 to 12 August
	between 2008–10		between 2008 and 2010

- To replace *to* in election results, scores, and directions. This is similar to the use above in continuing or inclusive numbers, but the en-dash no longer occurs in a numerical range.

  The election resulted in a 153–13 vote.
  The game ended in a 2–2 tie.
  The Rome–Naples rail line was flooded 17 kilometers southeast of Rome.

- In place of a hyphen to connect two parts of a compound term when one part of the compound is hyphenated or consists of more than one word. However, as the examples below illustrate, the width difference between a hyphen and an en-dash is not dramatic, so using *to* may be preferable to using an en-dash to connect compound terms when one part is hyphenated.

  first-stage–third-stage operations [better: first-stage to third-stage operations]
  pages 6-3–6-5 [better: pages 6-3 to 6-5]
  post–Operation ENDURING FREEDOM
  Joint Intelligence Operations Center–Afghanistan
  United States Forces–Iraq

Ellipsis

An ellipsis—three spaced periods (. . .)—marks an omission of a word or words within a direct quotation. When a quotation clearly is not a complete sentence, you do not need an ellipsis to show that material has been left out at the beginning or end of the quotation. No ellipsis is needed with the following quotation because *must avoid hostilities* obviously does not constitute a complete sentence:

> The minister said his nation "must avoid hostilities."

However, when your editing results in what appears to be a complete sentence, use an ellipsis at the beginning, end, or both (depending on where you cut material) to show that you have modified the original. Consider the following source paragraph:

> Writing in 1890 about Custer's defeat on the Little Bighorn River in 1876, Charles King described three factors that appeared to have contributed to Custer's mistakes. Dividing his command into columns to converge on the Indian village from different directions was a tactic that had worked for Custer and the 7th U.S. Cavalry at the Battle of Washita River against the Southern Cheyenne in 1868. The terrain Custer's force was passing through toward the Little Bighorn River hid much of the Sioux encampment from sight, making the village appear smaller than it was. Finally, when he saw evidence of heavy activity where he expected the Sioux village to be, Custer interpreted actions taken to get the Indian women and children to safety as a sign that the Indians were rapidly fleeing, justifying an immediate attack.

Using "Custer interpreted actions taken to get the Indian women and children to safety as a sign that the Indians were rapidly fleeing" from that source passage would appear to quote a complete sentence, so the quotation would need an ellipsis at the beginning and one at the end to make clear that the quotation truncates the original:

> In analyzing Custer's mistakes at the Little Bighorn, Charles King indicated that "... Custer interpreted actions taken to get the Indian women and children to safety as a sign that the Indians were rapidly fleeing...." For that reason he attacked without conducting thorough reconnaissance of the battle area. Unfortunately for Custer and the 7th Cavalry, the Sioux were preparing to fight rather than retreating.

This sample also demonstrates the two primary format styles associated with using an ellipsis:

- When an omission occurs inside a sentence or at the beginning, the result looks like the following or like the first ellipsis in the preceding sample.

  > "Tin and lead . . . are the primary exports."

- When an omission occurs at the end of a sentence, use four spaced periods without a space in front of the first period (a period for the sentence plus the three spaced periods for the ellipsis).

  > "Exports are primarily tin and lead.... Imports include copper and zinc."

Exclamation Point

Because of the impartial tone that characterizes intelligence writing, the exclamation point normally is not useful for DIA products.

Italics

Use *italic type* for the following:

- To emphasize a word or words in a passage.

  Do *not* use a colon between a verb and its objects or between a preposition and its objects, unless the colon sets off an indented list.

- For titles of works published separately, including online—titles of books or pamphlets, periodicals (magazines, journals, and newspapers), or works of art (plays, films, radio and television programs, paintings, and sculptures).

  an article in the *Defense Intelligence Digest*
  an issue of the *Washington Post*
  a news story on *Today*
  an opinion piece in *Slate*

  Note: For source reference citations, to simplify the source endnotes, DIA eliminated both italics for titles of works published separately and quotation marks for titles of things published as a part of longer works. Therefore, the guidance above for using italics with document titles, etc., does not apply to source reference citations.

- For foreign words.

  The *adhan* (Islamic call to prayers) issued from the mosque five times a day.

  Foreign terms whose meanings have become commonly understood can be used without translation. However, for a non-English term that may not be understood, show the term in italics and follow it with a translation or explanation in parentheses, as above.

  Do not use italic type or diacritical marks for the following terms, which were "foreign" but which have been brought into English:

ad hoc	cabana(s)
aide-de-camp, aides-de-camp	cafe(s)
aide-memoire [singular and plural]	cafeteria(s)
a la carte	caique(s)
alter ego(s)	caliph(s)
amir(s)	caliphate(s)
angstrom(s)	canape(s)
aperitif(s)	carte blanche, cartes blanches
applique(s)	caudillo(s)
a priori	cause celebre, causes celebres
apropos	chateau(s)
avant-garde	circa
bazaar(s)	cliche(s)
bazaari(s)	communique(s)
Bedouin [singular and plural]	confrere(s)
blase	consomme(s)
blitzkrieg(s)	cortege(s)
bona fide [adjective]	coulee(s)
bona fides [noun, singular and plural]	coup de grace, coups de grace

coup d'etat, coups d'etat
coupe(s)
critique(s)
cum laude
debacle(s)
debris
debut(s)
de facto
de jure
denouement(s)
depot(s)
devotee(s)
eclat(s)
elan
elite(s)
emir(s)
ennui
en rapport
en route
entree(s)
esprit de corps
ex cathedra
exemplar(s)
exemplum, exempla
ex hypothesi
ex libris [singular and plural]
ex nihilo
ex officio
ex parte
ex post facto
facade(s)
fait accompli, faits accomplis
fatwa(s)
faux pas [singular and plural]
fedayee [singular rarely used], fedayeen
felucca(s)
fete(s)
forte(s)
habeas corpus
habitue(s)
hadith(s)
hajj, hajjes
hajji(s)
halal
hawala(s)
imam(s)
in absentia
in extenso
in extremis
in loco parentis
in medias res
in situ
inter alia
inter alios
inter nos
in toto
in vitro
in vivo
ipso facto
ipso jure
jihad(s)
kolkhoz(es)
kosher
laissez faire
machismo [noun]
macho [adjective]
madrassa(s)
melee(s)
metier(s)
modus operandi, modi operandi
modus vivendi, modi vivendi
muezzin(s)
mujahid, mujahideen [If a variation of *mujahideen* appears in a group's name, use the source's spelling.]
mullah(s)
naive
naivete
nee
noblesse oblige
nom de guerre, noms de guerre
nom de plume, noms de plume
nouveau riche, nouveaux riches
obkom(s)
oblast(s)
ombudsman, ombudsmen
par excellence
per capita
per diem
per se
persona non grata
piece de resistance
premiere(s)

prima facie	Shiite, Shia [both noun and adjective]
pro forma	shura(s)
protege(s)	sic
quid pro quo, quid pro quos	sine qua non, sine qua nons
Quran	soiree(s)
Ramadan	status quo
rapporteur(s)	Sunna
rapprochement(s)	Sunni(s)
raykom(s)	tete-a-tete(s)
rayon(s)	ulama (variant of *ulema*)
regime(s)	ulema (plural noun)
risque	verbatim
samizdat(s)	vice versa
seance(s)	vis-a-vis
sharia	zakat
Shiism	

Do not use italic type for the following terms, which were "foreign" but which have been brought into English, but do use diacritical markings as indicated, as these terms have entered English with diacritical markings from the original languages:

attaché	émigré(s)
chargé d'affaires, chargés d'affaires	entrepôt(s)
déjà vu	exposé (s)
démarche(s)	précis [singular and plural]
détente(s)	raison d'être, raisons d'être
	résumé(s)

- For *imeni* ("named after") in names of Russian organizations or institutes.

  the Leningrad Naval Institute *imeni* A.K. Popov

However, do *not* italicize the original language or English translation of names of foreign organizations, institutes, governmental bodies, political parties, educational institutes, corporations, Internet service providers, and the like when a name is being used as if it were an English-language name for a similar type of entity. Because DIA's writing focuses on foreign information, we of course write about numerous foreign organizations, businesses, etc., as a normal part of our production. For most of these foreign proper names, then, we treat them as if they are in English and do not italicize elements of the proper names that are in or translated from a foreign language.

The Russian natural gas company Gazprom	debated in the Bundestag
the Cuban news agency Prensa Latina	the Parti Quebecois
the Buddhist organization Soka Gakkai	the Al-Aqsa Mosque

Nevertheless, if you clearly are providing the foreign language translation for something, show the foreign words in italics even though the subject of the discussion may be a foreign organization, institute, governmental body, political party, educational institute, corporation, Internet service provider, etc.

Gazprom is a contraction from *Gazovaya Promyshlennost*, or "gas industry."

The Gestapo (*Geheime Staatspolizei*, or "Secret State Police") was Nazi Germany's official secret police organization.

Subordinate to Algeria's Ministry of National Defense is its Department of Intelligence and Security, or DRS (*Departement de Renseignement et de Securite*).

In addition, do not italicize the original language or English translation of names of geographic features (mountains, rivers, islands, etc.) or place names.

At the time of the Bay of Pigs invasion, the large island off the southwest coast of Cuba was named the Isla de Pinos (Isle of Pines), but in 1978 it was renamed the Isla de la Juventud (Isle of Youth).

- When citing a letter as a letter, a word as a word, or a phrase as a phrase. That is, these items are italicized when they are being used not for their meanings but as things or terms.

  For the possessive, add an apostrophe and a lowercase *s*.
  Do not confuse the possessive *its* with the contraction *it's*.
  Along with and other phrases such as *as well as, in addition to, like,* and *together with* frequently follow immediately after a subject of a sentence.

- For the proper name (but not the type or class) of a ship, aircraft, or spacecraft.

	seizure of the *Pueblo*	*but*	the Dolgorukiy class SSBN *Yuriy Dolgorukiy*
	the USS *Wisconsin*		the Chinese Shang class SSN
	the *Spirit of St Louis*		the Indian Talwar II class FFG
	launched the *Soyuz-3*		a Soyuz-series space launch vehicle

- For a plant or animal genus and species. The genus also has initial capitalization, though the species does not. After first use of a genus, it can be abbreviated, though it still is uppercase and in italics. Higher divisions of plants and animals—phylum, class, order, and family—have initial capitalization but appear in roman type.

Clostridium botulinum; C. botulinum		*Escherichia coli; E. coli*
but	Anthropoda [phylum]	Mammals; Mammalia [class]
	Rodentia [order]	Hominidae [family]

- To mark the family name with the first use of a person's name (such as one in Spanish) for which the family name may not be obvious. This is not a style for general use in most intelligence products but is intended for special use in products such as military leadership profiles or papers with a protocol function, as this presentation device indicates the name to be used to refer to the person. If only a first name and family name are cited, no italics are required, since the family name then is obvious. Subsequent use of a family name should not continue the italic face.

  One trafficking organization reportedly employed Juan *Carlos* Martinez to pilot several illegal flights. Carlos and a companion, Pedro Rodriguez, also were reported to be dealing with ranchers to establish runways on their properties.

When the format for a product calls for italic type for a portion and you need to use italics for an element within that portion, make that "italic" element roman instead. For example, the following passage might occur in the opening paragraph of a report for which the product format requires the first paragraph to be in italic type; the reference to *Escherichia coli* within the paragraph then appears in roman type (the reverse of italic type):

Dr. Harriet Smith has studied the effects of exposure to pathogenic Escherichia coli *from contaminated food. This research may prove useful for developing foodborne biological agents.*

Parentheses

Use a set of parentheses—( )—for the following:

- As with commas or dashes, to set off an interruption within a sentence. When parentheses are used with an interruption, they reduce the emphasis on it, making it like a whispered aside.

  The country's exports (tin and lead) are not sufficient for a favorable trade balance.
  The country's trade balance suffers from inadequate exports (tin and lead only).

  In the second example above, the final parenthesis precedes the sentence period. If a complete sentence (or sentences) is used parenthetically, the end punctuation goes inside the final parenthesis, as in the following:

  The country's trade balance suffers from inadequate exports. (Only tin and lead were exported in 2009, and those were at low levels.)

  For a parenthetical expression within a parenthetical element, see the rules for using square brackets (page 123).

- To enclose a cross-reference.

  Exports of tin were only slightly greater than those for lead (Figure 2).
  Exports of tin were only slightly greater than those for lead. (See Appendix A.)

- To enclose numbers or letters that mark items in a series within a sentence.

  The Defense Ministry wants to acquire (1) attack helicopters, (2) Patriot missiles, and (3) main battle tanks.

  Note: This example is to illustrate the mechanics of presenting the parenthetical elements; such a simple series normally does not need numbering of its items.

- To enclose translations or explanations, particularly for foreign expressions.

  Memories of the *Anschluss* (Nazi Germany's annexation of Austria) still influence Austrian politics today.
  Subordinate to Algeria's Ministry of National Defense is its Department of Intelligence and Security, or DRS (*Departement de Renseignement et de Securite*).
  Be particularly careful not to confuse the possessive *its* with the contraction *it's* (for "it is" or "it has").

Period

A period brings a reader to a full stop at the end of a sentence. DIA also uses periods for the following:

- For bulleted material as part of a product's body text. For textual products (but not briefing slides), end each bulleted item (or each subbulleted item) with a period (unless the context calls for different ending punctuation, such as a question mark). Use this form regardless of whether a bulleted item is a word, phrase, or full sentence. If a bulleted item has multiple sentences, punctuate these as normal sentences.

  - The first item in a bulleted list.
  - The second item in the bulleted list.
    - A subbullet.
    - A second subbullet.

  For briefing slides, although each bulleted item begins with an initial capital letter, the bulleted items normally have no end punctuation. If a bulleted element has multiple sentences, only the final one has no end punctuation.

- At the end of an in-paragraph heading. In-paragraph headings normally are bolded, and the period that ends such a heading also should be bolded. For example, the following is the beginning of a passage from Chapter 3 of this style manual and uses an in-paragraph heading.

Arabic Persons' Names. When *al-* is part of a person's name in Arabic, include the *al-* when writing out the individual's full name the first time, as in "DIA judges that Iraqi Prime Minister Haydar al-Abadi will modify the plan." For subsequent references to the same individual, drop the *al-*, as in this secondary reference in the same paper: "Diplomats have noted that Abadi expects the plan to include three phases."

DIA normally does *not* use periods for the following:

- With standalone headings. In-paragraph headings end with a period because body text immediately follows on the same line. Standalone headings, however, should have no such ending punctuation. See for example the first-level heading that comes below for "Question Mark." The rare heading that is a question, however, should end with a question mark.
- With table headings and for short comments within a "remarks" or "comments" type of table cell. However, if remarks are sufficiently lengthy or complex to require divisions within the comments, punctuation such as commas, semicolons, or even periods may be needed to separate parts of the table's comment field. Moreover, if periods are needed for one comments-type cell in a table, then use periods for all of that type of table cell in the same table.

Question Mark

Use a question mark (?) for the following:

- At the end of a direct question.

  How can the funds be raised?

  However, do not use a question mark with an indirect question.

  He asked how the money could be raised.

- To show uncertainty or ignorance. In a table this can be done by using a question mark rather than information in a data field. A similar application can be used in text, although such use should be avoided as much as possible.

  The country's first prime minister, Dodson Wainwright (?–1721), began the custom.

- For a title that asks a question.

  "Military for Sale: Can Commercial Ventures Save the Armed Forces?"

Quotation Marks

Double Quotation Marks

Use a set of double quotation marks (" ") for the following:

- To enclose a direct quotation.

  The minister said, "We want to avoid hostilities."

  "At all cost," the minister said, "we want to avoid hostilities."

  "We want to avoid hostilities," the minister said.

  When a long quotation is set off by block indentation within the margins of a page or within a text column, the indentation serves as a set of quotation marks, so none is required unless the passage has internal quoted material. The block-indented passage below is a direct quotation, but the material has no quotation marks because the indentation represents a set of quotation marks. If something within the indented passage had quotation marks in the original, then double quotation marks should appear with that internal quotation.

In a speech outside the parliament building on 27 March 2010, the prime minister said that his administration was

> not responsible for the tragic events of 25 March. Irresponsible individuals rioted, destroyed public property, and endangered all our citizens. The government had no choice except to stop these illegal activities.

U.S. Versus British Use of Quotation Marks

Conventions for using double and single quotation marks differ between U.S. and British publishing. The most striking differences are these:

- British use of double and single quotation marks generally is the reverse of U.S. use.
- The rules for how other punctuation marks appear relative to quotation marks also differ somewhat.

Epigraphs. An epigraph is a quotation related to body text—usually to suggest a theme—but not a part of it; although epigraphs can appear at the beginning of a chapter or section, they are more common at the start of a document. Epigraphs occasionally occur in intelligence products, including in briefings, though by no means are epigraphs usual elements of our products. Wherever it appears in a document, an epigraph is a special type of block quotation. An epigraph generally leaves out some elements of other direct quotations: because epigraphs often quote a well-known source, they usually attribute the quotation to only the person's name or to the person's name and the work in which the original passage occurred, and other documentation is eliminated. Presenting an epigraph in a classified product presents a special formatting problem because putting "(U)" at the start of a quotation from, say, Sun Tzu looks a bit silly. Follow these formatting rules for presenting an epigraph:

- Present the quotation without quotation marks (unless quotation marks are needed within the epigraph).
- Double-space after the quotation to find the line for naming the author, right-justify the author's name or the author's name and the work in which the quotation appears, and precede the author's name with an em-dash.
- To avoid having to show a portion classification marking on the quotation in the epigraph, put the epigraph in a tone box and mark the quotation outside the box in the upper left corner. Generally you will not show a title for the tone box (though one could be used if needed).

UNCLASSIFIED

> Native agents are those of the enemy's country people whom we employ.
>
> —Sun Tzu

UNCLASSIFIED

> Native agents are those of the enemy's country people whom we employ.
>
> —Sun Tzu, *The Art of War*

- To enclose the titles of works that are published as parts of longer works—poems, short stories, songs, articles, notes, essays, headlines, chapter titles, and other parts of a book or periodical. Online works follow this rule as well.

  "Russia: Outlook for Key Military Reforms" was an article in a recent issue of the *Defense Intelligence Digest*.

  Note: For source reference citations, to simplify the source endnotes, DIA eliminated both italics for titles of works published separately and quotation marks for titles of things published as a part of longer works. Therefore, the guidance above for using quotation marks with article titles, etc., does not apply to source reference citations.

Spacing Between Colocated Single and Double Quotation Marks

Occasionally material will require single and double quotation marks to appear in a line together—for example, "a quotation that includes a 'quoted word'"—which looks strange. You can modify this spacing to improve readability by inserting a thin space between the single and double quotation marks. Two ways are available to add the thin space in Word 2007:

Using the Insert Symbol Function

1. Place the cursor where you want the thin space added—between the single and double quotation marks.
2. On Word 2007's Insert ribbon, at the far right side, select Symbol.
3. In the drop box, select More Symbols.
4. In the box that opens, change the font to Arial Unicode MS.
5. In the Character code box type 2009.
6. Choose the Insert button, followed by the Close button.

Using a Keyboard Shortcut

1. Place the cursor where you want the thin space added—between the single and double quotation marks.
2. Type 2009, followed immediately by Alt+x; the 2009 will change into the thin space.

The result should look like this: "a quotation that includes a 'quoted word' "—with a thin space between the single and double quotation marks.

- To set off a word or phrase used in a special sense (a meaning different from the normal sense) or to indicate the standard meaning of a word or phrase.

  The refugees were offered "voluntary" repatriation.
  He invited me for a "working lunch," but I did all the work and he ate all the lunch.
  Do not confuse *its* (the possessive of it) with *it's* (a contraction for "it is" or "it has").

  Use caution when presenting a word or phrase in a special sense. The quotation marks with the term indicate something is unusual about it, but readers must easily understand the special sense of the material. Using this device to be clever may result instead in a failure to communicate.

- To set off words or phrases following terms such as *entitled, named, endorsed, signed, cited as,* or *referred to as* (unless rules for using italics call for italic type instead).

  The document was signed "G. Washington."
  Rome's Leonardo da Vinci International Airport also is referred to as "Fiumicino," the suburb of Rome where the airport is located; failure to know both names can get a driver lost, as road signs for the airport sometimes show one name and sometimes the other.

  However, quotation marks usually are not necessary for expressions following terms such as *known as, called,* or *so-called.*

  The change is not likely to affect the so-called extremist Islamic states.
  Beryllium is known as glucinium in some European countries.
  The system is called profit and loss, but the profits may not be apparent.

  Even after these terms, however, quotation marks may be used to give special emphasis to the quoted or verbatim nature of an expression, especially if irony, sarcasm, or bad grammar is involved.

  The government's antiterrorism battalion nearly eliminated the village with an operation staged under its so-called "pacification" program.

Single Quotation Marks

Use a set of single quotation marks (' ') to enclose quoted material within a quotation that already is marked with double quotation marks. (A quotation within a block-indented quotation would take double rather than single quotation marks.)

He said, "I think you should read 'Russia: Outlook for Key Military Reforms.' "

Some U.S. writers believe they should use only single quotation marks around a single word or short phrase used in a special sense. That convention is true for British use of quotation marks but not for U.S. use. Instead, see the third bulleted guidance above for double quotation marks.

Punctuation With Quotation Marks

Place periods and commas inside quotation marks.

He said, "I think you should read 'Russia: Outlook for Key Military Reforms.' "
"I think you should read 'Russia: Outlook for Key Military Reforms,' " he said.

Place semicolons and colons outside quotation marks.

He said I should read "Russia: Outlook for Key Military Reforms"; he thought it would be good for me.
He said I should read "Russia: Outlook for Key Military Reforms": he thought it would be good for me.

Place a question mark or exclamation point inside quotation marks if the quotation is a question or exclamation; this rule applies whether or not the sentence as a whole is a question or exclamation. However, put the question mark or exclamation point outside quotation marks if the sentence is a question or an exclamation but the quotation is not.

She asked, "Do you remember reading the article?"
The author also wrote "Why Can't Johnny Read?"
Why should I read "Russia: Outlook for Key Military Reforms"?

Semicolon

Use a semicolon (;) for the following:

- To separate the elements in a series when one or more of the series elements itself requires commas. Semicolons generally are not needed if only the last element has internal commas.

  Three major NATO commands are subordinate to Allied Command Operations, with headquarters in Brunssum, Netherlands; Naples, Italy; and Lisbon, Portugal.

  Targeting requires the ability to locate targets; identify them, determine their vulnerability, and evaluate potential weapon effects against them; deliver appropriate weapons to a target; and evaluate the resulting damage.

  Rescue workers focused on building temporary shelters, securing potable water, and gathering blankets, medical supplies, and food.

- To separate two independent clauses closely related in meaning but not joined by a coordinating conjunction.

  He served in the Army until 1988; he has worked for DIA since then.
  He worked for the company for 20 years; from 1952 to 1954, however, he took a leave of absence.

- To separate two independent clauses when the second one is joined to the first with a conjunctive adverb. Common conjunctive adverbs are *first (second, etc.), for example, for instance, furthermore, however, moreover, nevertheless, nonetheless, therefore,* and *thus.*

  He worked for the company for 20 years; however, he took a leave of absence from 1952 to 1954.

Slash

Use a forward slash (/)—also called a virgule—for the following:

- To indicate a period occurring partially in one year and partially in another.

  FY 2010/11

  He flew three illegal flights in 2008/09.

- For two special commonly used representations.

  9/11 24/7

- To represent *per* in an abbreviation.

  km/h rd/min

- To separate alternatives.

  Many factors need to be considered in program/budget decisions.

  Note: In this application the slash is intended to mean "and/or." Thus, the sample above refers to "program decisions or budget decisions or program and budget decisions." However, a caution is necessary here: some writers use this punctuation device to avoid making a decision about what term is correct. In "our goal/objective is," no useful distinction exists between the alternatives, so the writer should pick one rather than demonstrating indecision.

- To indicate a word combination when one or both of the elements in the combination already contain a hyphen.

  The insurgents were armed with Cuban-/Russian-supplied weapons.

  Again the slash equates to "and/or": thus, the sample refers to "Cuban-supplied and/or Russian-supplied weapons." If the writer wants only an "or" or an "and" relationship, then the sentence should be recast:

  The insurgents were armed with Cuban- or Russian-supplied weapons.

  The insurgents were armed with Cuban- and Russian-supplied weapons.

- To indicate azimuthal direction.

  ENE/WSW runway

CHAPTER 7: Spelling and Compounding

In large letters, [a dentist sign] gives this command: Fear Free Dentistry. Maybe these dentists intend to scare people away from free dentistry. Probably, though, they intend to advertise fear-free dentistry. The hyphen changes it to dentistry that is free of fear. (How many customers do you think their omission scares away? Who would want someone that sloppy coming at them with a drill?)

—Mignon Fogarty, *Grammar Girl's Quick and Dirty Tips for Better Writing*

CHAPTER 7: Spelling and Compounding

The spelling and compounding list that makes up the bulk of this chapter combines preferred spellings (when alternative spellings exist) and spellings for compound words in their various functions in a sentence (as nouns, verbs, adjectives, unit modifiers, and so on). These words are combined into a single list with more than 10,000 entries.

The word list can help with the following types of spelling decisions:

- Choosing between alternative spellings. (Should you use *analog* or *analogue?*)
- Determining whether to double the consonant at the end of a word when you add a suffix. (Should you use *canceled* or *cancelled?*)
- Determining whether to use an anglicized spelling of the plural of a Latin word or the Latin spelling. (Should you use *forums* or *fora* as the plural of *forum?*)
- Choosing between possible spellings for a compound word or phrase: as two (or more) words, with a hyphen (or hyphens), or solid as a single word. (Should you use *time consuming, time-consuming,* or *timeconsuming?*)

The following guidance includes points that cannot be covered adequately by entries in a word list. In addition, spelling and compounding rules are provided for users who need to understand the logic applied in the choices in the word list, especially for compounding.

Spelling Rules

Geographic Names

The authority for spellings of place names is the U.S. Board on Geographic Names (BGN). The National Geospatial-Intelligence Agency provides a text-based BGN search function on JWICS at <http://names.nga.ic.gov/namesgaz/> and on NIPRNET at <http://geonames.nga.mil/namesgaz/>. Another useful source is *The World Factbook.*

The National Geospatial-Intelligence Agency's Geographic Names Server reflects foreign place names sanctioned by the BGN. This database provides "Approved" spellings (which generally have diacritics and often special endings for some names), "Variants" (which normally will include a spelling without the diacritical marks), and, when they exist, "Conventional" spellings (which reflect the spelling commonly used in English).

Diacritical Marks

Although diacritical marks appear in the place names on some maps and sometimes in *The World Factbook*, we generally will not use them in text for intelligence publications. Diacritical marks indicate phonetic distinctions, whereas writing for which precise pronunciation is not particularly important normally uses conventional, commonly used spellings instead.

Numerous spellings typically come up in a BGN search for a place name. Check the "Feature Designation" column first; "primary administrative division" generally indicates a province or governorate, and "populated place" indicates a city or town. In the appropriate row, look for either the "Conventional" or the "Approved" spelling.

- If the search result shows a "Conventional" spelling for a place name, we generally will use that spelling. Thus, instead of *Moskva*, the "Approved" spelling, use the "Conventional" name of *Moscow*. Instead of the "Approved" spelling for North Korea's capital—*P'yŏngyang*—use the "Conventional" spelling of *Pyongyang*.
- When an "Approved" spelling has diacritical marks, use that spelling without the diacritics. Thus, instead of *Islamabad*, the "Approved Short" spelling for the capital territory in Pakistan, use *Islamabad*. Do not confuse apostrophes with diacritical marks; retain the apostrophe in place names such as N'Djamena.

When possible, spellings in text and on maps should agree. For example, beware of showing *Rhodes* in text but showing *Rhodos* or *Rhodus* on an accompanying map.

American Versus British Spellings

When American and British spellings of *common* English words differ, use the American spelling. However, when the words are part of a *proper name* for a party, organization, office, etc., use the British spelling, but only within the proper name.

labor relations of the Labour Party
defense intelligence reports from the Australian Defence Intelligence Organisation
Industrialisation Board rulings on industrialization issues

Plurals of Compound Terms

For plurals of compound terms, form the plural on the significant word or words. If no word is significant or all parts are equally significant, form the plural on the last word.

significant word first:	adjutants general, aides-de-camp, courts-martial, goings-on
significant word in middle:	deputy chiefs of staff, assistant surgeons general
significant word last:	major generals, provost marshals, trade unions
both words equally significant:	gentlemen farmers, women writers
no word significant:	also-rans, go-betweens, pick-me-ups

Compounding Rules

Compounding conveys an idea by combining two or more words to form a thought. The result can be separate words in an unconnected sequence, words linked with a hyphen or hyphens, or words joined as a solid, single word. Current language trends lead to closing up many word sets that have become associated in readers' minds through frequent use.

General Rules

Separate Words

One compounding form is to write words in sequence, without joining them or linking them with a hyphen, if this form causes no ambiguity in sense or sound.

blood pressure	real estate
early warning	training ship

Joined or Hyphenated Words

Often words are joined (written solid) or linked with hyphens to express ideas that would not be as clear if the words remained unconnected.

bookkeeping	cross-reference
newsprint	do-gooder
whitewash	right-of-way

Derivatives

Derivatives of a compound usually retain the hyphenated or solid form of the original.

footnote, footnoting	cost-effective, cost-effectiveness
praiseworthy, praiseworthiness	ill-advised, ill-advisedly

Solid Compounds

When two nouns form a compound that has only one primary accent, the compound is written solid, especially when the prefixed noun has only one syllable or when one of the elements loses its original accent.

bathroom	*but*	bomb bay
bookseller		coal mine
pipeline		night shift

Parts of Speech and Compounding

A noun formed from a short verb and an adverb usually is written solid, but it is hyphenated when the solid compound would interfere with comprehension. The verb form usually remains two words.

breakdown (verb: break down)	cut-in (verb: cut in)
buildup (verb: build up)	run-in (verb: run in)
setup (verb: set up)	tie-in (verb: tie in)

Compounds beginning with the following nouns usually are solid.

book (bookstore)	school (schoolteacher)
eye (eyeglasses)	shop (shopworn)
horse (horseplay)	snow (snowbank)
house (housekeeping)	way (wayside)
mill (millcourse)	wood (woodland)
play (plaything)	work (workday)

Compound terms *beginning with cyber* may be written either solid or as multiple separate words, depending on meaning. When cyber terms began appearing in English-language dictionaries, the dictionaries showed solid terms, treating *cyber* as a combining form requiring solid compound words. The *Yahoo! Style Guide*, published in July 2010, treats the terms similarly, indicating that *cyber* usually would be combined with root words except when the root word begins with a capital letter. Typical early dictionary and Yahoo! entries included *cyberattack, cybercrime, cybernetics, cyberphobia, cyberpunk, cyberspace,* and *cyberterrorism.*

- Because of the growing importance of cyber terms for U.S. security operations, Defense Intelligence has a need to consider a multitude of terms dealing with infrastructure, funding, resources, and other aspects of managing intelligence operations related to the cyber realm. Most likely many of these terms will never appear in English-language dictionaries. Consider just one of these terms—how to label intelligence analysts dedicated to cyberintelligence. Should such an analyst be a *cyberanalyst* or a *cyber analyst*? Showing *cyberanalyst* as a solid word would seem to suggest that the analyst exists in cyberspace, an ethereal analyst, like an avatar, rather than a flesh-and-blood analyst. For things or concepts such as this, multiple separate words are more appropriate.
- For this reason, we make a distinction for cyber terms based on meaning:
  - Cyber terms related predominantly to *things inside or integral to the cyber realm*—for which we join *cyber* with the root word to form a solid term: for example, *cyberactivity, cyberattack, cybercrime, cyberoperation, cybersecurity, cyberterrorism, cyberthreat.*
  - Cyber terms related predominantly to *things about the cyber realm or managing it*—for which we keep *cyber* separate, resulting in multiple separate words: for example, *cyber analyst, cyber collection, cyber community, cyber doctrine, cyber offensive and defensive operations.*

Less frequently, *cyber* also may be joined by a hyphen to another word when the combined term is being used as a unit modifier—for example, *cyber-related data*. When in doubt, follow the current trend of joining the terms as a solid word.

Compounds ending in the following usually are solid when the initial word has one syllable. (When the initial word has multiple syllables, the compound is less often solid: spaceborne, *but* satellite-borne, helicopter-borne.)

board (cardboard)
boat (rowboat)
book (textbook)
borne (bloodborne; foodborne; spaceborne; waterborne; *but* tick-borne; vector-borne; food-, water-, and vector-borne)
bound (landbound)
box (gearbox)
boy (lowboy)
craft (aircraft)
field (airfield)
fish (crawfish)
girl (schoolgirl)
grower (foodgrower)
headed (clearheaded)
hearted (halfhearted)
holder (shareholder)
house (boathouse)
keeper (beekeeper)
keeping (bookkeeping)
land (farmland)
light (moonlight)
like (boxlike)
line (pipeline)
load (boatload)
maker (automaker)
making (cementmaking)
man (airman)
mate (teammate)
monger (scaremonger)
over (crossover)
owner (homeowner)
person (salesperson)
piece (fieldpiece)
plane (airplane)
power (airpower)
proof (blastproof)
room (chartroom)
shop (toolshop)
site (damsite)
smith (gunsmith)
stone (lodestone)
store (bookstore)
tight (airtight)
time (halftime)
ward (homeward)
water (bluewater; freshwater [adjective]; groundwater; saltwater; seawater; wastewater; *but* drinking water; fresh water [noun]; surface water; well water [noun and adjective])
way (seaway; waterway)
wide (worldwide)
wise (edgewise)
woman (spokeswoman)
wood (firewood)
work (artwork)
worker (pieceworker)
working (woodworking)
worm (ringworm)
worthy (seaworthy)
writer (speechwriter)
writing (checkwriting)
yard (shipyard)

Write solid the compounds of *any, every, no,* or *some* with *body, thing,* or *where*. When *one* is the second element, write the compound as two words if it means a particular person or thing. Always write *no one* as two words to avoid mispronunciation.

anybody
anything
nowhere
someone

but: Anyone can be in charge, and any one of you can volunteer.

Unit Modifiers

Authors frequently encounter problems with compound modifiers that immediately precede the words they modify. When the words make sense only as a unit, the compound is a unit modifier and usually is written with a hyphen.

- In "short, swift streams," both *short* and *swift* modify streams independently (they are coordinate adjectives), and no hyphen is used to join the modifiers. (There is a comma, however, because the adjectives are coordinate; see comma usage in Chapter 6.)
- In "short tributary streams," *tributary* modifies streams, and *short* modifies *tributary streams*; the adjectives are cumulative, and no special mark is used to join them. Note, however, that each adjective logically *could* modify the noun separately; that is, "short streams" and "tributary streams" both make sense, even if these are not what the writer means.
- In "40-horsepower engine," neither *40* nor *horsepower* logically can modify *engine* by itself; the modifiers make sense only as a unit—hence the term "unit modifier."

A Caution About Modifier Strings

Beware of stringing so many modifiers in front of a noun that your thought becomes difficult to comprehend. For example, "weapon system development and acquisition cost reductions" is hard to understand; the modifier string should be broken up, becoming "cost reductions from weapon system development and acquisition."

Part of the confusion for many authors is that a compound modifier receives different treatment when it follows the word it modifies:

I bought an engine that is rated at *40 horsepower.*
I bought a *40-horsepower engine.*
As a result of the conference, we now have *standards* that are *agreed upon.*
As a result of the conference, we now have *agreed-upon standards.*

Thus, the special treatment for a unit modifier is situational. Users of the word list in this chapter must bear this in mind. *A compound modifier marked* um *in the list and linked with a hyphen retains the hyphen only when it precedes the word it modifies.*

Hyphenated

Unit modifiers immediately preceding the word or words they modify *usually* are hyphenated.

drought-stricken area	state-of-the-art technology
English-speaking nation	U.S.-owned property
fire-tested material	1-inch diameter
lump-sum payment	2-inch-diameter pipe
most-favored-nation clause	4-percent increase

Use a hyphen in a unit modifier with an ordinal number in its literal sense (unless the modifier is a proper noun).

first-stage booster	second-class treatment
fourth-quarter earnings	third-party statement

In addition, use hyphens in unit modifiers containing prepositional phrases.

fly-by-night establishment	quality-of-life incentives
out-of-area operations	under-the-counter sales

Joined

Some unit modifiers are written solid rather than being hyphenated.

aboveground shelter	indepth assessment
airdrop mission	lookdown angle
blackout curtains	mineclearing equipment
breakaway republics	onboard computer
broadband radio	sealane defense
deadweight tons	sweptwing fighter
firsthand experience	understrength division

Unhyphenated

Especially when the compound is a well-established phrase, hyphens sometimes are omitted from a unit modifier, and the modifier is written as separate words.

air defense artillery	ground support aviation
air intercept regiment	hard currency loan
ballistic missile submarine	law enforcement efforts
broad gauge railroad	mine warfare task force
drug trafficking organization	missile support unit
early warning radar	nuclear delivery system
free market system	open pit mining
general purpose vehicle	throw weight equivalent

No hyphens are needed for most compounds that are linked by conjunctions.

command and control echelons	middle or late 1980s
medium and high altitudes	warm but cloudy day

However, improvised compounds that contain conjunctions do use hyphens.

bread-and-butter issues	hard-and-fast rule

Predicate Adjectives

As indicated in the introduction to unit modifiers, compound predicate adjectives usually have no hyphens.

Unit Modifier	*Predicate Adjective*
The attack took place on U.S.-owned property.	The property where the attack took place was U.S. owned.
She gave an indepth assessment.	The assessment she gave was in depth.
We are to get a 4-percent raise.	The raise is to be 4 percent.

The word list in this chapter contains some hyphenated compound adjectives (*adj*); they retain their hyphens when they are predicate adjectives.

The study used all-source intelligence.	The intelligence in the study was all-source.
We watched a combined-arms exercise.	The exercise we watched was combined-arms.

Comparatives and Superlatives

Hyphens usually are omitted from two-word modifiers when the first word is a comparative or superlative.

little-developed country	low-priced model
less developed country	lower priced model
least developed country	lowest priced model

Note that *lower* is the comparative of *low*, with *lowest* the corresponding superlative. However, *lower* also is the opposite of *upper*, which is not a comparative and has no superlative (*uppest?*). In its sense opposing *upper*, *lower* is joined (solid) or linked (with a hyphen) to the other words in a modifier.

uppercase letters	lowercase letters
upper-class neighborhood	lower-class neighborhood
upper-middle-class housing	lower-middle-class housing

Hyphens also are retained in many three-word modifiers that include a comparative or superlative.

higher-than-market price	most-favored-nation clause
less-than-perfect solution	most-sought-after assignment
lighter-than-air craft	

Adverbs Ending in *-ly*

Do not use a hyphen in a two-word unit modifier when the first word is an adverb ending in *-ly*. (Do not confuse adjectives ending in *-ly* with adverbs.)

eagerly awaited moment	*but*	only-child complex
recently designed building		lonely-hearts club
wholly owned subsidiary		

Sometimes a comparative or superlative needs to be combined with the word it precedes to ensure clarity. If we write "older technology mines," the phrase can be misunderstood as indicating "technology mines" that are "older." Adding a hyphen to connect *older* and *technology*—"older-technology mines"—makes clear that we mean mines employing older technology.

Three-Word Modifiers

Do not use hyphens in a three-word unit modifier when the first word is an adverb modifying the second word.

unusually well preserved specimens
very well defined usage

exceptions:
very-high-frequency broadcast
very-low-frequency transmission

However, if the first word of a three-word modifying phrase modifies the other two words as a unit, use a hyphen between those two parts of the unit.

a nearly right-angle corner
a formerly well-known person

Foreign Phrases

Do not use a hyphen in a unit modifier consisting of a phrase of foreign origin.

bona fide transaction	ex officio member
carte blanche policy	per capita tax
ad hoc tasking	

Proper Nouns

Do not use a hyphen or en-dash in a compound proper noun or capitalized coined name used as a unit modifier (unless the basic noun form includes a hyphen or en-dash).

Cold War tension	*but*	Spanish-American heritage
Latin American states		French-English descent
Iraqi Army operations		Franco-Prussian War
World War II period		North American–South American sphere

Quotation Marks

Do not use hyphens in a unit modifier enclosed in quotation marks unless the modifier normally is hyphenated, and do not use quotation marks in lieu of hyphens.

a "spare the rod" approach to parenthood
the "one-man woman" plots of many operas
but a right-to-work law

Chemical Terms

Do not use a hyphen in a unit modifier composed of chemical terms.

carbon monoxide poisoning	methyl bromide solution

Letter or Number Elements

Except in established military equipment designators, do not use a hyphen in a unit modifier with a letter or numeral as its second element.

Annex B maps	*but*	An-22 transport
Article III provisions		MiG-29 fighter
Mod 3 missile		T-80 tank
Number 2 fuel oil		

Common Basic Elements

When two or more hyphenated compounds in a series have a common basic element and this element is omitted in all but the last or first term, retain the hyphens.

2- or 3-year period	*but*	mid- and late 1990s *but* mid-to-late 1990s
8-, 10-, and 16-km segments		early or mid-1990s *but* early-to-mid 1990s
ground- and air-launched missiles		
U.S.-owned and -operated companies		
low- to high-altitude coverage		
medium- to long-range missiles		

Suspending Hyphens

When two or more solid compounds in a series have a common basic element and this element is omitted in all but the last or first term, use a suspending hyphen with the incomplete forms.

first- and secondhand access
low- and midlevel operatives
postearthquake and –tsunami operations

but

oil and gas fields or oilfields and gasfields (not oil and gasfields)

Prefixes and Suffixes

Prefixes (except *ex, self, quasi,* and *vice*) and suffixes (except *free, designate,* and *elect*) usually form a solid compound with a noncapitalized word.

With Prefixes

byproduct
cooperate
counterintelligence
hydroelectric
multipurpose
neofascist
nonferrous

ex-serviceman
self-centered
quasi-military
vice-chairmanship

With Suffixes

clockwise
fourfold
lifelike
northward
forcewide
geocentric
but youth-centric, brigade-centric, etc.

rent-free
minister-designate
President-elect Jones
councilor-elect

However, retain hyphens that appear in proper names.

Directorate General for Inter-Services Intelligence

Except for the short prefixes *co, de, pre,* and *re*—which generally are written solid—use a hyphen to avoid doubling a vowel when adding a prefix or tripling a consonant when adding a suffix.

With Prefixes

anti-insurgent
contra-acting
semi-independent
ultra-ambitious

but cooperate
deescalate
preexisting
reentry

With Suffixes

hull-less
shell-like

but nonnuclear
subbasement

Even for prefixes that normally form solid compounds, use a hyphen if its omission would lead to mispronunciation, cause confusion with a word spelled identically but without a hyphen, or create an illogical compound.

mid-ice
mini-state
under-ice
co-op (*but* cooperate)
multi-ply (several plies)
pre-position (position in advance)
pro-state (in favor of the state)
re-form (form again)

re-present (present again)
un-ionized
non-civil-service position
non-scientific and technical intelligence

Use a hyphen to join duplicated prefixes.

counter-countermeasures	counter-counternarcotics
sub-subcommittee	sub-subparagraph

Use a hyphen to join a prefix or suffix in a compound with a capitalized word.

anti-Castro	Africa-wide
neo-Nazi	Latin America-wide
non-U.S. NATO	Truman-like
pro-British	

exceptions: nonMIRVed, unMIRVed

A prefix (except *un*) normally forming a solid compound often is followed by a hyphen when joined with a two-word or hyphenated compound to form a unit modifier.

anti-guided-missile	*but*	antiballistic missile
non-missile-equipped		superhigh-frequency
non-nuclear-powered		ultrahigh-frequency
post-target-tracking		uncalled-for
semi-land-mobile		unself-conscious

However, do not insert a hyphen after a prefix joined to a solid compound.

antigunrunning	postreentry
nonlifelike	submachinegun
nonoceangoing	ultrarightwing

Numerical Compounds

Use a hyphen between the elements of compound numbers from 21 to 99 when they are spelled out. (In most contexts, the numbers in this range will be presented as numerals, not written out as words; see Chapter 4 for rules on writing numbers as words or numerals.)

twenty-one	ninety-nine
twenty-first	one hundred twenty-one

one thousand four hundred twenty-one

Use a hyphen in an adjective compound with a numerical element first.

two-sided question	8-kg box
the Six-Day War	18-year-old student
.22-caliber cartridge	10- to 20-year period

500-km-range missile

When an adjective numerical compound appears in a listing (such as a table) with the compound following but reading back to the word or words modified, use a hyphen in the compound and use the compound in its singular form.

motor, 3-phase, 60-cycle, 115-volt
belts: 2-inch, 1.25-inch, 0.25-inch

Use a hyphen between elements of a fraction, whether the fraction is a noun or an adjective.

two-thirds of the vote	a two-thirds majority

Other Compounds

Do not use hyphens in a compound title denoting a single civil or military office, but use a hyphen in a double title.

ambassador at large	manager-director
commander in chief	minister-counselor
vice president	secretary-treasurer
but under-secretaryship, vice-presidency	

Except for titles, hyphens appear in some—but not all—noun compounds containing a prepositional phrase.

government-in-exile	*but* next of kin
grant-in-aid	prisoner of war
man-of-war	state of the art
mother-in-law	state of war

Use hyphens in improvised compounds.

first-come, first-served basis	roll-on/roll-off ship
hard-and-fast rule	stick-in-the-mud
know-it-alls	technical know-how

Hyphenate the verb form of compound nouns that are written as two words.

to blue-pencil galley proofs (*but* proof with a blue pencil)
to cold-shoulder an idea (*but* turn a cold shoulder)
to cross-brace a structure (*but* a structure with a cross brace)
to flight-test a missile (*but* a missile in flight test)

Join a single capital letter to a noun or participle with a hyphen.

H-bomb	V-necked
I-beam	X-ray, X-raying
T-shaped	X-ed out
but I band, K band, P band, L band, etc.	

Using the Spelling and Compounding List

The following list contains both preferred spellings and preferred formations for compounds (multiple words, hyphenated words, or solid words).

The following abbreviations appear in the list:

adj (adjective)	masc (masculine)
adv (adverb)	n (noun)
cf (combining form)	pref (prefix)
etc (and so on)	um (unit modifier)
fem (feminine)	v (verb)

Frequently the abbreviations indicate that a compound appears in the form shown only for the specific function or functions shown. For example:

- *fire-resistant (um)* means that the compound is hyphenated as a unit modifier but not, for instance, as a predicate adjective:

  We chose a fire-resistant material.
  The material we chose was fire resistant.

- *low-key (adj)* means that the compound is hyphenated both as an adjective preceding the word modified (like a unit modifier) and as an adjective following the word modified:

  She gave a low-key speech.
  Her speech was low-key.

- *human rights (adj, n)* means the compound is written as separate words in both adjective and noun functions:

  It was a human rights issue.
  Human rights was the issue of the moment.

- *anti-American (etc)* means that the same compounding structure applies to similar compounds, such as *anti-British* or *anti-German* in this case.

- *counter (cf)* means that the compounding structure applies when forming a compound but not when the terms are simply juxtaposed in a sentence:

  The team focused on counterrebel operations.
  The team dug in to counter rebel advances.

Gender Neutrality

Be aware that modern publishing standards call for gender-neutral terms. Even though many terms containing *man* are part of the military lexicon, these terms are not always the best choice. For such terms shown in the following list, consider using them in reference to specific individuals but choosing gender-neutral terms for general reference.

Spelling and Compounding List

Numerical Terms

24/7
3-D
3G, 4G
9/11

A

aberration
able-bodied (um)
able-minded (um)
A-bomb
about-face
above-average (um)
aboveboard
above-cited (um)
abovedeck
aboveground (adj)
above-mentioned (um)
above-named (um)
above-water (um)
above-written (um)
abridgment
absentminded
accessory
accommodate
accursed
across-the-board (um)
acknowledgment
acoustic
acre-foot
active-duty (um)
adapter
addendum, addenda
add-on (adj, n)
address book
ad hoc
adjuster
ad-lib (adj, n, v),
  -bed, -bing
adviser
  advisor (law)
aegis
aerial refueling (adj, n)
aero (cf)
  all one word
afoot
afore (cf)
  all one word
A-frame
African-American
after (cf)
  afterward
  all one word
after-action (um)
ageless
agenda, agendas
age-old (adj)
aging
agreed-upon (um)
agro (cf)
  agroindustrial
  all one word
aid (n, v)
aide (assistant)
aide-de-camp,
  aides-de-camp
aimpoint
airbag
airbase
airblast
air-blasted (um)
airborne
airborne warning and
  control system aircraft
airbrake
air-breathing
airbrush
airburst
aircargo
air-conditioner
air-conditioning
air-cool (v)
air-cooled (um)
air cover
aircraft
air crash
aircrew
air-cushion (um, v)
air defense (adj, n)
air-deliver (v)
air-delivered (um)
air-dried (um)
air-driven (um)
airdrome
airdrop (adj, n, v)
airdroppable
air-dry (v)
airfare
airfield
airflow
airfoil
air-formed (um)
airframe
airfreight
airgap
airhammer
airhole
airhose
air intercept (adj, n)
airlanding
airlane
air-launch (v)
air-launched (um)
airlift
airline
airliner
airlink
airlocked
airmail
airman
airmass
airmobile
airmobility
airpark
airpath
air policing (adj, n)
airport (all meanings)
air-portable (um)
airpower
  but naval and air power
air raid
air-refueling (um)
airscoop
airship (n)
air-ship (v)
air show
airsick
airspace
airspeed
air station
airstream
airstrike
  but naval and air strikes
airstrip
air surveillance
airtight
airtime
air war
airwave

airway
air wing
airworthy
aka
a la carte
alter ego
algae
align
all-aged (um)
all-American (etc)
all-around (um)
all-clear (n, um)
all-day (um)
all-encompassing
all-inclusive (um)
all-knowing
all-out
all ready (prepared)
  already (previous)
all right
all-purpose (um)
all-source (adj)
all-star
all-terrain (um)
alltime (adj)
all time (n)
all together (collectively)
  altogether (completely)
all-weather
allies, allied
  but Allies, Allied
  (WWI and WWII)
alongshore
alongside
alphanumeric
al-Qaida
also-ran
altocumulus
altostratus
alumna, alumnae (fem)
alumnus, alumni (masc)
ambassador at large
amber-colored (um)
ambi (cf)
  all one word
amidships
amino (pref)
  amino acid
  as prefix, one word
amir (*emir* is preferred)
ampere-hour
amperemeter
ampere-second
amphi (pref)
  all one word
ampoule
analogous
analogue
  analog (science, computer)
anchor light
anemia
anesthetic
aneurysm
angio (cf)
  all one word
anglicize
Anglo (cf)
  Anglo-American (etc)
  rest one word
angstrom unit (etc)
anhydr(o) (cf)
  all one word
ankle-deep (um)
annul, -led, ling
annulment
anomalous
anonymous
ante (pref)
  ante bellum (etc)
  ante-Christian (etc)
  antedate
  ante mortem
  rest one word
anteater
antenna, antennas
  antennae (zoology)
antero (cf)
  all one word
anthill
anthra (cf)
  all one word
anthropo (cf)
  all one word
anti (pref)
  antiaircraft
  anti-American (etc)
  antiapartheid
  antiarmor
  anti-arms-control
  antiballistic missile
  antichrist
  anti-cruise-missile
  antiestablishment
  antiextremist
  antigovernment
  anti-guided-missile
  antigunrunning
  anti-icer
  anti-imperial
  anti-inflationary
  anti-infrared
  anti-insurgent
  antijam
  antimissile
  anti-missile-missile (um)
  antinuclear
  anti-nuclear-weapons
  antioccupation
  antipersonnel
  antisatellite
  anti-Semitism
  anti-tactical-ballistic missile
  antitank
  anti-theater-ballistic missile
  antitrust
  antivirus
  rest one word
antro (cf)
  all one word
anybody
anyhow
anyone
anyplace (adv)
anyway (adv)
aorto (cf)
  all one word
apo (pref)
  all one word
A-pole
appall, -ed, -ing
apparatus, apparatuses
appendix, appendixes
applecart
a priori
apropos
aquaculture
aqualung
aquamarine
aquarium, aquariums
arabic numerals
archbishop
archduke
arched-roof (adj)

archenemy
archeo (cf)
all one word
archi (pref)
all one word
archo (cf)
all one word
arch-Protestant (etc)
archrival
arc-over (adj, n)
arctic clothing (etc)
arc-weld (v)
areo (cf)
all one word
aristo (cf)
all one word
arithmo (cf)
all one word
armband
armchair
armor-clad (um)
armor-heavy (um)
armor officer
armored brigade
armored unit
armor-piercing (um)
armorplate
armor-plated (um)
armpit
armrest
arms control
arm's length (adj)
arm-twisting
army-group-level (um)
armywide
Army-wide
around-the-clock (um)
arrester
arrowhead
arrow-shaped (um)
arseno (cf)
all one word
arterio (cf)
all one word
artesian well
arthro (cf)
all one word
artilleryman
artwork
ascendance, -ant
ascent (rise)
assent (consent)
ashcan
ash-colored (um)
ash-gray (um)
ashtray
assembly line
assemblyman
assembly room
associate's degree
astro (cf)
all one word
attaché
atomic energy (adj, n)
at-large (um)
at-sea (um)
attorney at law
attrit
attritted, -ting
audio (cf)
audiofrequency
audiogram
audiosurveillance
audiotape
audiovisual
all one word
auri (cf)
auri-iodide
rest one word
authorship
auto (cf)
auto-objective
autogiro
automaton,
automatons
autopilot
rest one word
automaker
autoworker
avante garde
avatar
awe-inspiring (um)
awhile (adv)
a while (n)
ax
axis, axes
axo (cf)
all one word

B

Baathist
baby boomer
babyface
babysit
bachelor's degree
backache
backbencher
backbite (v)
backbone
backbreaker
back-brief (v)
back burner
back channel (n)
back-channel (adj, v)
back-country (um)
backdate
backdoor (adj)
backdown (adj, n)
backdrop
backface
backfill
backfire
backfit
backflow
background
backhand
backhoe
back-in (adj, n)
backlash
backlist (v)
backlog
backpacker
backpay
backpayment
backpedal (v)
backrest
backroom (adj)
backroad (adj)
backscatter
backseat
backslide
backspace
backspin
backstage
backstop
backstory
backstroke
backswept
backswing
backtalk

backtrack
backtrail
backup (adj, n)
back up (v)
backwall
backward
backwash
backwater
backyard
bagful
baggage room
bagpipe
bag-shaped (um)
Bailey bridge
bailout (adj, n)
bail out (v)
balance-of-payments (adj)
baldfaced
Balkanize
Balkanization
ball bearing
ballistic missile (adj, n)
ballistic missile
  early warning (um)
ball-like
ballpark
ballplayer
ballpoint (adj, n)
ballot box
bandanna
bandsaw
bandstand
bandwagon
bandwidth
bangup (adj, n)
banknote
bankside (stream)
bantamweight
bareback
barebones
barefaced
barefoot
barehanded
bargainer
bark (ship)
barnstormer
barreled, -ing
barrel-roll (v)
barrel-shaped (um)
bartender
baseball
baseball bat
base camp
baseline
  base line (surveying)
baseplate
basi (cf)
  all one word
basis, bases
basketball
bas-relief
bastille
bathrobe
bathroom
bathtub
bathyscaph
battalion
battalion-sized (um)
battleax
battlefront
battleground
battle group
battleline
battle management
battle-scarred (um)
battleship
battlespace
battle-tested (um)
battlewagon
battle-weary (um)
batwing
bazaar
bazaari
beachhead
beadroll
beamwidth
beanbag
beanpole
bean-shaped (um)
bedchamber
bed check
bedclothes
bedcover
bed-down (um)
bedframe
Bedouin
bedpan
bedpost
bed rest
bedridden
bedrock
bedsheet
bedside
bedsore
beekeeper
beeswax
beetle-browed (um)
beforehand
before-mentioned (um)
before-named (um)
bell-bottomed (um)
bellringer
bellwether
bellyache
below-grade (um)
below-ground (um)
below-market (um)
belt-driven (um)
belt-tightening
benchmark (nonliteral)
  bench mark
  (surveying)
benchwarmer
benefited, -ing
benzo (cf)
  all one word
best man
bestseller
beveled, -ing
beyond-visual-range (um)
bi (pref)
  bicentennial
  bifocal
  bi-iliac
  rest one word
biased, -ing
big data
bigmouthed
big-power (adj)
big shot
big-ticket (adj)
billfold
billhook
bio (cf)
  bio-osmosis
  rest one word
bird's-eye (adj)
birdshot
birdwatcher
birdwatching
birthday
birthmark
birthplace

birthrate
birthright
bitmap
bitstock
bitstream
bittersweet
blackball (nonliteral)
black-eyed (um)
blackface
blackguard
blackjack
blacklist
blackmail
black market (adj, n)
black-market (v)
black-marketeer
blackout (adj, n)
blacktop
blase
blasthole
blastmark
blastproof
bleary-eyed (um)
blight-resistant (um)
blind-bomb (v)
blind-flying (um)
blindfold
blindspot
blitzkrieg
bloc (group)
  block (grants)
blockbuster
blog
blood-alcohol (um)
bloodbath
bloodborne
bloodcurdling
blood-drenched (um)
blood-giving (um)
bloodhound
bloodletting
blood pressure
blood-red (um)
bloodshed
bloodshot
bloodstain
bloodstock
bloodstream
bloodsucker
bloodthirsty
bloody-nosed (um)
blowback (adj, n)
blowby (adj, n)
blowdown (adj, n)
blowgun
blowhard (adj, n)
blowhole
blowoff (adj, n)
blowout (adj, n)
blow out (v)
blowpipe
blowtorch
blowup (adj, n)
blow up (v)
blueblood
bluecoat (n)
blue-collar (nonliteral) (adj)
blue-eyed (um)
bluegrass
blue-gray (um)
blue-green (um)
bluejacket
bluenose
blue-pencil (adj, v)
blueprint
blue-ribbon (nonliteral)(adj)
bluestreak (nonliteral)
bluewater
blunderbuss
blunt-edged (um)
blunt-spoken (um)
boardwalk
boatbuilder
boatcrew
boathook
boathouse
boatload
boatswain
boatwright
boatyard
bobcat
bobsled
bodybuilder
bodyguard
bohemian
boildown (adj, n)
boil down (v)
boilerplate
boldface
boltcutter
bolthead
bolthole
bomb bay
bomb blast
bombdrop
bombload
bombmaker
bombmaking
bombproof
bombshell
bombsight (device)
  bomb site (location)
bombthrower
bomb-throwing (um)
bona fides (n, singular and plural)
bone-dry (um)
bone-hard (um)
bonemeal
bone-white (um)
boobytrap, -ped, -ping
bookbinder
bookcase
bookkeeping
book-lined (um)
booklist
booklover
bookmark
bookmobile
bookseller
bookshelf
bookstall
bookstand
bookstore
book-taught (adj)
boomtown
boondoggle
bootblack
boot camp
bootlace
bootleg
bootstrap
border-crossing (um)
borderland
borderline
borehole
boresafe
boresight
born (birth)
  borne (carried)
born-again (n, um)
bottle-fed (um)
bottleneck
bottle-nosed (um)

bottom land
bottom-line (adj)
bottom-up (um)
bouillon (soup)
  bullion (metal)
boulder
bowie knife
bowknot
bowlegged
bowsprit
bowstring
boxcar
boxlike
brachio (cf)
  all one word
brachy (cf)
  all one word
braille
brainchild
brainstorm
brain trust
brainwash
brakedrum
brassworks
breach (gap)
  breech (lower part)
bread-and-butter (adj)
breadbasket
breadcrumb
breadfruit
breadwinner
breakaway (adj, n)
breakbulk
breakdown (adj, n)
break down (v)
break-even (um)
breakfront
break-in (adj, n)
break in (v)
breakneck
breakoff (adj, n)
breakout (adj, n)
break out (v)
breakpoint
breakthrough
breakup (adj, n)
break up (v)
breastbone
breastplate
breathtaking
breechblock
breechloader
breech-loading (um)
breechlock
bribe-free (um)
bribegiver
bribetaker
bric-a-brac
brick-built (um)
brick-colored (um)
bricklayer
brick-red (um)
bridgebuilder
bridgehead
bridgeway
bridgework
briefcase
brier
brigade-centric (adj)
bright-colored (um)
bright-eyed (um)
brilliant-cut (um)
brilliant-green (um)
brinkmanship
broadacre
broad-area (um)
broadax
broadband (adj, n)
broad-based (um)
broad-beamed (um)
broadcast
broadcloth
broad gauge (adj, n)
broadleaf (n)
broad-leaved (um)
broadleg (adj, n)
broadloom
broadminded
broadside
broadsword
broken-down (um)
broken-legged (um)
broncho (cf)
  all one word
bronze-clad (um)
broomstick
brotherhood
brother-in-law
browbeat
brown bag (adj, n)
brown-eyed (um)
brownout (adj, n)
brush holder
brushoff (adj, n)
bucketful
bucket-shaped (um)
bucksaw
buckshot
bugbite
buildingways (singular and plural)
building-block (adj)
buildup (adj, n)
build up (v)
buildout (adj, n)
built-in (um)
built-up (um)
bulkhead
bulldog
bulldoze
bulletproof
bullfight
bullpen
bullring
bull's-eye (nonliteral)
bullwhip
bunghole
bureau, bureaus
burdensharing
burned
burned-out (um)
burned-up (um)
burn-in (adj, n)
burnout (adj, n)
burn-through (adj, n)
burnup (adj, n)
bus, bused, buses,
  busing
busdriver
  but schoolbus driver
busfare
bushwhacker
businesslike
busline
busload
busybody
busywork
butter-yellow (um)
buttondown (adj, n)
buttonhole
buttonhook
butt-weld (v)
buyback (adj, n)
buy-in (adj, n)

buy-out (adj, n)
buzzword
by (cf)
  by-and-by
  byelection
  bylaw
  bypass
  byproduct
  by-the-way (n, um)
  by-your-leave (n, um)
  rest one word

C

cabana
cabdriver
cabfare
cable-laid (um)
cab owner
cabstand
caco (cf)
  all one word
cactus, cactuses
cafe
caffeine
caique
calci (cf)
  all one word
caldron
caliber
caliper
caliph
caliphate
calk
callback (adj, n)
call back (v)
call-in (adj, n)
call-off (adj, n)
callous
callout (adj, n)
call-over (adj, n)
call sign
callup (adj, n)
call up (v)
camelback
camel's-hair (um)
campfire
campground
camshaft
canalside
canape
canceled, -ing
cancellation
candlelit
candlestick
candlewick
can-do (um)
candor
cane-backed (um)
canebrake
canister
cannonball
cannot
canvas (cloth)
  canvass (solicit)
canvas-covered (um)
capful
capital (city)
  capitol (building)
capital-intensive (um)
capscrew
carabao (singular and plural)
carat (gem weight)
  caret (omission mark)
carbarn
car-bomb (adj)
car bomb (n)
car-bomb, -ing (v)
carbureted, -ing
carburetor
carcino (cf)
  all one word
cardboard
cardio (cf)
  cardio-aortic
  rest one word
cardplayer
cardsharp
cardstock
carefree
caretaker
careworn
carfare
car ferry
carjack
carload
cargo(es)
cargo-handling (um)
carhop
caroled, -ing
carotene
carpetbagger
carpet-covered (um)
carpetweaver
carpet-weaving (um)
carpool
carport
carrier-based (um)
carrierborne
carryall (adj, n)
carryback (adj, n)
carry-in (adj, n)
carry-on (adj, n)
carryout (adj, n)
carryover (adj, n)
carry over (v)
carsick
carte blanche
cartwheel
carwash
case-by-case (um)
caseworker
cash-and-carry (adj)
cash-flow (adj)
cashier's check
castaway (n, um)
caster (roller)
  castor (oil)
cast-by (um)
castout (n, um)
Castroite views (etc)
casual (unimportant)
  causal (cause)
catalog, -ed, -ing
catchall
catchphrase
catchup (adj, n)
catch up (v)
catchword
catercorner
caterwauling
catgut
cation
cat-o'nine-tails
cat's-eye (nonliteral)
cat's-paw (nonliteral)
cattle breeder
cattle-raising (um)
cattle ranch
catwalk
caudillo
cause celebre,
  causes celebres
causeway
cavedweller

cave-dwelling (um)
cave-in (adj, n)
caviled, -er, -ing
cease-fire (adj, n)
cease fire (v)
cell phone
cement-covered (um)
cementmaking
census taker
census-taking (um)
center field
center-left
centerline
centermost
centerpiece
centerpole
center-right
centi (cf)
  centimeter-gram-second
  rest one word
centri (cf)
  all one word
centro (cf)
  all one word
cephalo (cf)
  all one word
cerebro (cf)
  cerebro-ocular
  rest one word
cesarean
cesspit
cesspool
chain-driven (um)
chain link
chain of command
chainsmoke (v)
chainsmoker (n)
chairman
chairperson
chair-shaped (um)
chairwoman
chalkboard
chalk-white (um)
chancellery
chancellor
changeable
changeover (adj, n)
change over (v)
channeled, -ing
chaperon
charcoal
charge-coupled (um)
chargé d'affaires,
  chargés d'affaires
chargeout (adj, n)
chartroom
chassis (singular and plural)
château
chat room
cheapskate
checkbook
checkbox
check-clearing
check-in (adj, n)
check in (v)
checklist
checkmark
checkoff (adj, n)
checkout (adj, n)
check out (v)
checkpoint
checkpost
checksheet
checkup (adj, n)
check up (v)
check valve
cheekbone
chemical-weapons-free (um)
chemico (cf)
  all one word
chemo (cf)
  all one word
cherrypick (v)
chickenfeed
chickenpox
chicken yard
chief justice
chief-justiceship
chief mate
chief of staff
  chiefs of staff
childbearing
childbirth
child care
childhood
childlike
chill-cast (um, v)
china shop
chin-high (um)
chinstrap
chiro (cf)
  all one word
chiseled, -ing
chitchat
chloro (cf)
  chlorophyll
  rest one word
chockablock
chock-full (adj)
chocolate-brown (um)
chokepoint
chole (cf)
  all one word
chopstick
chromo (cf)
  all one word
chrono (cf)
  all one word
chuckwagon
churchgoer
cigarette
cigar-shaped (um)
cine (cf)
  all one word
circa
circuit breaker
circum (pref)
  circumarctic
  circumpacific
  rest one word
cirro (cf)
  all one word
cis (pref)
  cisalpine
  cisatlantic
  rest one word
city-born (um)
city-bred (um)
city dweller
cityfolk
cityscape
citywide
civil defense (adj, n)
civil society (adj, n)
clambake
clamor
clampdown (adj, n)
clamshell
class-conscious (um)
claw-footed (um)
clawhammer
claybank
clay-colored (um)

claymore
claypit
clayworks
clean-cut (um)
cleanhanded
cleanout (adj, n)
clean room
clean-shaved (um)
clean-smelling (um)
cleanup (adj, n)
clean up (v)
clear-cut (distinct)
clearcut (forestry) (n, v)
clear-eyed (um)
clearheaded
clearinghouse
clear-sighted (um)
clearup (n)
clear up (v)
clew (nautical)
  clue (other)
cliche
cliffdweller
cliff-dwelling (um)
cliffhanger
cliffside
clifftop
clip art
cloak-and-dagger (adj, n)
clockface
clockwatcher
clockwise
close air support
close-connected (um)
close-cut (um)
closed-circuit (adj)
closed-door (um)
closedown (n)
closed shop
closefisted
close-hold (adj)
close-in (um)
close-knit
closeminded
closemouthed
closeout (adj, n)
close out (v)
close-quarters (um)
closeup (n, um)
close up (v)
cloth-backed (um)
clotheshorse
clothesline
clothespin
cloudbase
cloudburst
cloudcap
cloud-hidden (um)
cloverleaf
cloud cover
cloud-covered (um)
clubfoot
club-shaped (um)
co (pref)
  coauthor
  cochair
  cohost
  co-op
  cooperate
  co-opt
  co-optation
  co-orbital
  co-owner
  coproduction
  rest one word
coal-black (um)
coalboat
coal car
coalfield
coal-fired (um)
coal gas
coalition (generic)
  Coalition (specific
    U.S.-led alliance)
coal-laden (um)
coal loader
coal mine
coal miner
coal-mining (um)
coalpit
coal-slurry (um)
coast guard
coastline
coastside
coathanger
coatrack
coattails
cobweb
coca grower
coca-growing (um)
cocaine
cockeyed
cockfight
cockpit
cocksure
cock-tailed (um)
coconut
codename
codenamed
codeword
coffeebreak
coffee-colored (um)
coffeegrower
coffee-growing (um)
coffeehouse
coffeepot
cofferdam
cogwheel
coin-operated (um)
coke oven
coldblooded
coldbloodedness
cold-chisel (v)
coldcuts
cold-flow (v)
cold-forge (v)
cold-hammer (v)
cold-hammered (um)
coldpack
cold-press (v)
cold-roll (v)
cold-rolled (um)
cold-shoulder (v)
Cold War
cold-work (v)
coli (cf)
  all one word
collarbone
collateral
colocated
colo (cf)
  all one word
colorblind
colorblindness
color-code (v)
colorfast
combatant
combat arms
combat-capable (um)
combated, -ing
combat-ready (um)
combat support (adj, n)
combined-arms (adj)
comeback (adj, n)
come-between (n)
comedown (n)

come-off (adj, n)
come-on (adj, n)
come-out (n)
comeuppance
command and control
commander in chief
commando(s)
command post
commandwide
commingle
commit, -ted, -ting
common law
commonplace
common sense
commonweal
commonwealth
communique
communitywide
companionship
companywide
compel, -led, -ling
compendium,
  compendiums
condominium,
  condominiums
cone-shaped (um)
conference room
confidant (masculine
    and feminine)
  confident (sure)
confidence- and
  security-building (um)
confidence-building (um)
confirmer
confrere
congressman at large
conjurer
connecter
consignor
consomme
consortium, consortiums
consulter
container ship
contra (pref)
  contra-acting
  contradictor
  contraindicate
  contra-ion
  rest one word
control, -lable, -led, -ling
converter
conveyor
cookoff (adj, n)
cookout (adj, n)
cookstove
coolheaded
cooped-up (um)
copilot
copout (n)
cop out (v)
copper-bottomed (um)
copper-colored (um)
copperhead
copper mine
copper miner
copperplate
copper-plated (um)
copperworker
copperworks
copycat
copydesk
copyedit
copyreader
copyright
coral-red (um)
cork-lined (um)
corkscrew
corncob
cornerpost
corn-fed (um)
corn-growing (um)
cornhusk
cornmeal
cornstarch
corpsmember
corral, -led, -ling
cost-effective (adj)
cost-effectiveness
costo (cf)
  all one word
cost-of-living (um)
cost-saving (um)
cotton-growing (um)
cotton mill
cottonmouth (snake)
cottonseed
coulee
councilor (of council)
  counselor (adviser)
counseled, -ing
countdown (adj, n)
counter (cf)
  counteract
  counterattack
  counter checking (banking)
  counter-countermeasures
  counterintelligence
  counter-off
  counternarcotics
    but counter-narcotics-
    trafficking efforts
  counterpropaganda
  counterrebel
  counterregime
  counter septum
  counterterrorism
    but counter-
    terrorism-finance
    efforts (etc)
    rest one word
country-born (um)
country-bred (um)
countryside
country-western
countrywide
coup de grace, coups de grace
coup d'etat, coups d'etat
coupe
coursework
court-martial
courtship
cousin-in-law
coveralls
covername
cover term
coverup (adj, n)
cover up (v)
cowcatcher
cowhand
cowherd
cowhide
cowpath
cowpen
cozy
crackdown (adj, n)
crack down (v)
crackup (adj, n)
craneway
cranio (cf)
  all one word
crankcase
crank-driven (um)
crankshaft

crash-land (v)
crash landing (n)
crawfish
cream-colored (um)
credit card
creditworthiness
creekbed
creekside
crestfallen
crewcut
crewmember
crew-served (um)
crew station
crew training
crimefighter
crimewave
crisis, crises
crisscross
criterion, criteria
critique
crook (cf)
all one word
crop index
crop-year
cross-appeal
crossarm
cross baffle
crossband
crossbar
crossbeam
crossbones
cross-border
cross-brace
crossbred
cross-bridge (v)
cross-channel
cross-check
cross-claim
cross-compound (v)
cross-connect
cross-country (adj)
cross-cultivate (v)
crosscurrent
crosscut, -ting
cross-echelon
cross-examination
cross-examine
cross-eyed (adj)
crossfeed
cross-fertile (um)
cross-fertilize (v)
crossfire
crossflow
cross-grained (um)
crosshair
crosshatch
cross-immunity
cross-index (um)
cross-interrogate (v)
crosslegged
cross-level (v)
cross-license (v)
crossmark
crossmember
cross-national (adj)
crossover (adj, n)
crosspath
cross-pollinate (v)
cross-pressure
cross-purpose (n)
cross-question
crossrange
cross-reaction
cross-refer (v)
cross-reference
crossroad
cross section
cross-sectional (um)
cross-service
cross-stone
cross-sue (v)
crosstalk
cross-target
crosstie
crosstown
crosstrack
cross-train
crossunder (adj, n)
cross-vote
crosswalk
crosswind
crosswise
crossword
crowbar
crowd control
crow's-foot (nonliteral)
crow's-nest (nonliteral)
cruise missile
cryptanalysis
crypto (cf)
crypto-Christian (etc)
rest one word
crystal-clear (um)
crystalline
crystallize
cubbyhole
cudgeled, -ing
cum laude
cumulo (cf)
all one word
cupful
curbside
cure-all (adj, n)
current account (adj, n)
curriculum, curriculums
curveball
custom-built (um)
custom-made (um)
custom-tailored (um)
cut and fill (adj, n)
cutaway
cutback (n)
cut back (v)
cutglass
cut-in (n)
cutoff (n, um)
cutout (n, um)
cutover (adj)
cutrate (adj)
cutthroat
cutting-edge (um)
cut-under (um)
cut-up (n, um)
cyano (cf)
all one word
cyber activist
cyberactivity
cyberactor
cyber adversary
cyberanalysis
cyber analyst
cyberanalytic
cyber arena
cyberattack
cyberattack signature development (etc)
cyber authority
cyber battlefield
cybercafe
cyber campaign
cyber capability
cyberchallenge
cyber coalition
cyber cognitive analytic tools
cyber collection

cyber command
cybercommunication
cyber community
cyber components
cyber concern
cyberconflict
cybercrime
cybercriminals
cyber customer
cyberdata
cyberdefense
cyber deterrence
cyber doctrine
cyber domain
cyberdominance
cyber economy
cybereffort
cyber element
cyber emir
cyber enterprise
cyberentity
cyberenvironment
cyberespionage
cyberevent
cyber expert
cyberexploitation
cyberfirm
cyberforce
cyberfraud
cyber fusion
cyber geographics
cyber geolocation
cyber hardware
cyberhostilities
cyber implications
cyberincident
cyber indications and warning
cyberinformation
(information in the cyber realm)
cyber information
(information about the
cyber infrastructure)
cyber information assurance
cyber infrastructure
cyber initiative
cyberintelligence
cyberintrusion
cyber investment
cyberism
cyber issue
cyberland
cyber law
cyber means
cybermercenaries
cyber mission
cyber modeling
cyber national
signatures
cyber national strategy
cybernetwork
cyber offensive and
defensive operations
cyberoperation
cyber operator
cyber order of battle
cyber organization
cyber pact
cyberpenetration
cyber plan
cyber platform
cyber police
cyber policy
cyber position
cyber posture
cyber power
cyberproduction
cyber-proficient foreign
actors (etc)
cyber program
cyber realm
cyber reconnaissance
cyber-related data (etc)
cyber requirement
cyber research and
development
cyber resources
cyber role
cybersabotage
cyber safeguard
cybersecurity
cyber service
cyber signature
cyber situational
awareness
cyber skills
cyber solution
cyberspace
cyber staff
cyberstrategy
cyber support
cybersystem
cyber target
cyber tactics,
techniques, and
procedures
cyber team
cybertechnique
cyber technology
cyber terminology
cyberterrorism
cyberthreat
cybertool
cyber toolkit
cyber training
cyber unit
cybervisualization
cybervulnerability
cyberwar
cyberwarfare
cyberweapon
cyber word
cyber world
cyber year
cyclo (cf)
all one word
cysto (cf)
all one word
cyto (cf)
all one word
czar

D

dairy farm
damping-off (n, um)
damsite
dancehall
danger line
daredevil
daresay
dark-eyed (um)
darkhorse (nonliteral)
data bank
database
data flow
datalink
data-mine (v)
data-mining (um)
data mining (n)
data point
data print
data-processing (um)
data set
dateline

date stamp (n)
  date-stamp (adj, v)
datum (rarely used), data
daughter-in-law
daybed
daybreak
day care
daydream
day-fly (aviation) (v)
day-flying (um)
daylit
daylong
day school
day shift
daytime
day-to-day (um)
dayworker
D-day
  D-day plus 4
de (pref)
  deactivate
  de-air
  decentralize
  deconflict
  deenergize
  deescalate
  degaussing
  deice
  de-ion
  derail
  rest one word
deadbeat (n)
deaddrop (nonliteral)
dead end
deadeye (n)
deadfall
deadhead
dead heat
dead-in-the-water (um)
deadline
dead load
deadlock
deadweight (adj, n)
deadwood
deaf-mute
deathbed
deathblow
deathlike
death rate
deathtrap
deathwatch
debacle
debarkation
debris
debt service
debut
decadelong
  decades-long
decisionmakers
  but policy and
  decision makers
decisionmaking
deckhand
deep-cut (um)
deep-dive (um)
deep-felt (um)
deep-freeze (um, v)
deep-frying (um)
deepgoing
deep-laid (um)
deep-rooted (um)
deep-sea (adj)
deep-seated (um)
deep-set (um)
deep-space (adj)
deep-strike (um)
deep-underground (um)
deep-voiced (um)
deepwater (um)
de facto
defense
defense-industrial
defuse
degrees Celsius
degrees Fahrenheit
dehydr(o) (cf)
  all one word
déjà vu
dejure
démarche (n)
deliverer
demagogue
demarcation
demi (pref)
  demi-Christian (etc)
  demi-incognito
  rest one word
demonstrator
denial-of-service (um)
denouement
dependent
depot
depth charge
dermato (cf)
  all one word
descendant (adj, n)
desecrater
desert-bred (um)
desktop
détente
deter, -red, -ring
deterrence
deterrent
detractor
deutero (cf)
  all one word
develop, -ed, ing, -ment
developing-country (um)
devilry
devotee
dewclaw
dewlap
dewpoint
dextro (cf)
  all one word
dextrous
di (pref)
  all one word
dia (pref)
  all one word
diagrammed, -ming
diagrammatic
dialed, -ing
dialog box
dialogue (discussion)
dial-up (adj, n)
diamondback
diamond-backed (um)
diamond-shaped (um)
diaphragm
diazo (cf)
  diazo-oxide
  rest one word
die-away (um)
dieback
diecast (adj, v)
die-cut (adj, v)
diehard (adj, n)
diesel-driven (um)
diesel-electric
diesel engine
diesel-powered (um)
diffuser
dike
dimlit

dimout (adj, n)
dingbat
dining room
dinitro (cf)
  dinitro spray
  rest one word
dipstick
direct-connected (um)
directed-energy (adj)
direct-indirect
direction-finding (um)
dirt-cheap (um)
dirt-encrusted (um)
dirty work
dis (pref)
  all one word
disaster relief
discreet (prudent)
  discrete (distinct)
dishcloth
disheveled, -ing
dishwasher
disk
diskjockey
disk-shaped (um)
dispatch
dispel, -led, -ing
distill, -ed, -ing, -ment
distributor
districtwide
ditchdigger
dive-bomb (v)
diverter
division-level (um)
do-all (adj, n)
dockhand
dockside
dockworker
doctorate
doctor's degree
dog-bitten (um)
dogcatcher
dog-ear (v)
dog-eared (adj)
dogfight
dogfood
dogleg
dogma, dogmas
do-gooder
dogsled
dog tag
dog-tired (um)
do-little (adj, n)
domestically produced
do-nothing (adj, n)
doomsday
doorbell
doorframe
doorjamb
doorknob
doormat
doorstop
Doppler effect
dorsi (cf)
  all one word
dorso (cf)
  dorso-occipital
  rest one word
dot-com (adj, n)
double-agent (adj)
double-barreled (um)
double-breasted (um)
double-charge (v)
doublecheck (n, v)
doublechecked (adj)
double-click
double-count (v)
doublecross (nonliteral)
doubledeal, -ing (v)
double-decker
double-duty (adj)
double-edged (um)
double-entendre
doubleheader
double-jointed
double play
double-quick (um)
double space
doubletalk
double time
double-track (adj, v)
doubletree
double-up (um, v)
doweled, -ing
downbeat
downcast
down-covered (um)
downcut
downdraft
down-echelon (adj)
downfall
downfield
downflow
downgrade
downgradient
downgrowth
downhill
down-link
download
downlock (n)
downlook
downpayment
downplay
downpour
downrange
downright
downriver
downrush
downside
downsize
downslope
downspout
downstairs
downstream
downstroke
downswing
downtime
down-to-earth
downtown
downtrend
downtrodden
downturn
downward
downwind
draft age
draftage (allowance)
draft-exempt (um)
dragnet
drainpipe
drawback
drawbridge
drawdown (adj, n)
draw down (v)
drawgear
drawing board
drawing room
drawn-out (um)
drawoff (adj, n)
drawout (adj, n)
drawspan
drawstring
dreamed
dressing room

dressup (adj, n)
driftmeter
drift-mining (um)
drill down
drill-like
drinking water
drip-dry (um, v)
driveaway (adj, n)
drive-by (adj, n)
drive by (v)
drive-in (adj, n)
drive shaft
drive-through (adj, n)
drive-up (adj)
dropaway (adj, n)
drop-down (adj)
dropkick
dropleaf (adj, n)
dropleg
dropoff (adj, n)
drop off (v)
dropout (adj, n)
drop out (v)
drop text
drought
droughtlike
drought-stricken (um)
drug-addicted (um)
drugpusher
drug trafficker
drug trafficking
drumbeat
drumhead
drumstick
drum-up (adj, n)
dryclean
drycleaning
dry-cure (v)
drydock
dry-farm (v)
dry-packed (um, v)
dry rot
dry-rotted (um)
dry-salt (v)
dry-season (adj)
drywash
dual-gauge (um)
dual-hatted (adj)
dual-purpose (um)
dual-track (um)
dual-use (um)
duck-billed (um)
duckblind
duckpond
due date
due-in (n, um)
dueled, -ing
dueout (n, um)
dues-paying (um)
duffelbag
dug-in (um)
dugout (n)
dug-up (um)
dull-edged (um)
dull-looking (um)
dullness
dumbbell
dumbwaiter
dumbfound
dumpsite
duo (cf)
all one word
dustbin
dustcloth
dust-covered (um)
dustpan
duststorm
dutybound
duty-free (um)
dwelt
dyeing (coloring)
dying (death)
dys (pref)
all one word

E

earache
earbud
eardrum
earflap
earful
early-1960s-vintage (adj) (etc)
early-June (etc) (um)
early-model (adj)
early or mid-March (etc)
early- to mid-March figures (etc)
early warning (adj, n)
earmark
earphone
ear-piercing (um)
earplug
earring
earshot
earsplitting
earthfill
earthmover
earthmoving
earthquake
earth-shaking (um)
earthwall
east-central (um)
East European (um)
Eastern Europe (n)
easternmost
eastgoing
east-northeast
east-southeast
eastward
easygoing
eavesdrop
Ebola
edge plane
edgewise
editor in chief
eggbeater
egg-shaped (um)
eggshell
eightfold
eight-ply (um)
eight-wheeler
elan
elbowroom
electro (cf)
electrochemical
electromagnetic
electro-optical
electro-osmosis
electro-ultrafiltration
rest one word
elicited, -ing
elite
ellipsis, ellipses
email
embargo(es)
embarrass
embed
embellish
embryo (cf)
all one word
emigrant (go from)
immigrant (go into)

émigré
emir
emptyhanded
enameled, -ing
encase
encephalo (cf)
all one word
enclose
enclosure
encumber
encumbrance
end-all (adj, n)
end game
end-item (um)
endmost
endnote
endo (cf)
all one word
endorse, -ment
endpoint
end-stage (um)
end-state (um)
end-strength (um)
end-use (um)
end user
endwise
energy-sector (um)
enforce, -ment
engine-driven (um)
engine driver
enginehouse
engineroom
engine shop
engine yard
English-language (etc) (um)
ennui
en rapport
enroll, -ed, -ing, -ment
en route
ensnare
entero (cf)
all one word
entree
entrench
entrepôt
entrust
envelop, -ed, -ing
envelope (n)
epi (pref)
epilogue
rest one word
equaled, -ing
equal rights (adj, n)
equi (cf)
equi-gram-molar
rest one word
equilibrium, equilibriums
equip, -ped, -ping
erratum, errata
erythro (cf)
all one word
escapable
esprit de corps
esthetic
ethno (cf)
all one word
ethnic Uzbek (etc) (adj, n)
Euro (cf)
Euroatlantic
Eurocommunism
Euroloan
Eurozone
but euro (currency)
all one word
evacuee
evenhanded
even-numbered (um)
even-tempered (adj)
eventide
ever-changing (um)
ever-constant (um)
ever-growing (um)
everglade
evergreen
everlasting
evermore
ever-present (um)
ever-ready (um)
every day (each day)
everyday (ordinary)
everyone (all)
every one (distributive)
every time
evildoer
ex cathedra
excel, -led, -ling
excommunicate
exemplar
exhibitor
ex libris (singular and plural)
ex officio
exoatmosphere
exoatmospheric
ex parte
expel, -led, -ling
exposé
ex post facto
ex-FARC (etc)
ex-president (etc)
ex-servicemember (etc)
extoll, -ed, -ing
extra
extra-American
extra-condensed (um)
extraconstitutional
extracurricular
extra-fine (um)
extrahazardous
extrajudicial
extra-large (um)
extralegal
extra-long (um)
extramural
extraordinary
extra-strong (um)
extraterritorial
extravascular
for extra (outside), generally do not hyphenate; for extra (more), use hyphen
eyeball
eyebank
eyebolt
eyebrow
eye-catching (um)
eyeglasses
eyehole
eyelash
eyelid
eye opener
eye-opening (um)
eyeshade
eyesight
eyesore
eyestrain
eyetooth
eyewash
eyewitness
eying

F

facade
facecloth
facedown (adj, n)
face-on (adj, n)
face-off (adj, n)
faceplate
face-saving (um)
face-to-face (um)
faceup (adj, n)
factbook
fact-check (v)
fact checking (n)
factfinding
factsheet
fadeaway (adj, n)
fade-in (adj, n)
fadeout (adj, n)
fail-safe
fainthearted
fairground
fair-haired (um)
fairminded
fairplay
fairytale
fait accompli, faits accompli
fallback (adj, n)
fall-in (adj, n)
falloff (n)
fallout (adj, n)
fallow land
false-bottomed (um)
falsehood
fancy-free (um)
fanfare
fan-jet
fan-shaped (um)
fan-tailed (um)
faraway (n, um)
far cry
far-distant (um)
Far East (n)
  Far Eastern (um)
farfetched
farflung
fargone
far-left (adj)
far-leftist (um)
farm-bred (um)
farmhand
farmland
farmstead
farmworkers
far-off (um)
far-reaching (um)
far-right (adj)
far-rightist (um)
farseeing
far-set (um)
farsighted
farther (distance)
  further (degree)
fastback
fast-breaking (um)
fast-moving (um)
fast track (n)
fast-track (adj, v)
fat-free (um)
father-in-law
fat-soluble (um)
fatwa
faultfinding
faultline
faux pas (singular and plural)
favor
fax
fear-free (um)
fearmongering
featherbed
featherweight
fedayee (singular rarely used),
  fedayeen
fed-up (um)
feebleminded
feedback (n)
feedbag
feedgrain
feedlot
feedstock
fellow (cf)
  fellowship
  fellow traveler
  rest two words
felt-lined (um)
felucca
fence jumper
fencepost
fence-sitter
fence-sitting (um)
ferro (cf)
  ferro-carbon-titanium
  ferro-uranium
  rest one word
fete
fetish
fever-stricken (um)
fiber
fiberboard
fiberglass
fiber-optic (adj)
fiber-optics (n)
fibro (cf)
  fibro-osteoma
  rest one word
field day
field-deploy (v)
fieldglass
fieldgoal
field-grade (adj)
field grade (n)
field-launch (v)
fieldpiece
field-strip (v)
field-test (v)
field training
fierce-looking (um)
fiery-tempered (um)
fighter-bomber
fighter-interceptor
fighter pilot
fig leaf
figurehead
figure-of-eight (um)
figure work (printing)
file clerk
file-hard (um)
file name
fill-in (adj, n)
fillout (adj, n)
fill-up (adj, n)
filmgoer
filmmaker, filmmaking
filmstrip
finback
fine-cut (um, v)
fine-drawn (um)
fine-featured (um)
fine-looking (um)
fine-tune (v)
fine-tuning

finger-cut (um)
fingerprint
fingertip
fin-shaped (um)
fiord (as common noun; as part of name, follow Board on Geographic Names)
firearm
fireball
firebase
firebolt
firebomb
firebrand
firebreak
fire-burnt (um)
fire-control (adj)
fire control (n)
firecracker
firedamp
fire drill (adj, n)
firefight
firefighter
fireguard
fire-hardened (um)
firehose
firepit
fireplace
fireplug
firepower
fireproof
fire-red (um)
fire-resistant (um)
firesafe
fireside
firestorm
fire-support (adj)
fire-tested (um)
firetrap
firetruck
firewall
firewarden
firewood
firm-footed (um)
firm-handed (um)
firm-set (um)
firm-up (adj, n)
first aid (adj, n)
first-ballot (adj)
firstborn
first-class (um)
first-come, first-served
firstcomer
first-echelon (adj)
first-ever (um)
first-generation (adj)
first-half (adj)
firsthand (adj, adv)
firstline (adj)
first-made (um)
first-named (um)
first-quarter (adj)
first-rate (adj)
first-rater
first responder
first-stage (adj)
fishbone
fisheye
fish-fed (um)
fishhook
fish-joint (v)
fishpond
fishtrap
fistfight
fit out, fitting out (v, gerund)
fitting-out (um)
fivefold
five-ply (um)
five-pointed (um)
fixed-wing (um)
flagbearer
flagpole
flagpost
flag-raising (um)
flagship
flag-signal (v)
flagstaff
flak jacket
flame-cut (v)
flameout (n)
flameproof
flamethrower
flammable
flareback (adj, n)
flareout (adj, n)
flareup (adj, n)
flashback (adj, n)
flashbulb
flashcard
flashgun
flashlamp
flashpoint
flatback (bookbinding)
flatbed
flat-bottomed (um)
flatcar
flatfoot
flat-footed
flathead
flatiron
flatout (n, um)
flat-rolled (um)
flattop
flat-topped (um)
flatwoods
fleabite
flea-bitten (um)
fledgling
fleet-footed (um)
fleur-de-lis
flexitime
flier
flightcrew
flight hour
flightline
flightpath
flight test (adj, n)
flight-test, -ed, -ing
flight time
flip-flop
flip-up (adj, n)
floodgate
floodlamp
floodlight
floodlighting
flood plain
floodtide
floodwall
floodwater
floorboard
floorlamp
floor-length
floormat
floor plan
floorspace
floorwalker
flotation
flour mill
floursack
flowchart
flowerbed
flowerpot
flowmeter

flowoff (adj, n)
flowsheet
flowthrough
fluo (cf)
all one word
fluoro (cf)
all one word
flush-cut (um)
flush-decked (um)
fluvio (cf)
all one word
flyaway
flyback
flyball
flyblown
fly-by-night (adj, n)
flycatcher
fly-fish (v)
fly fishing
flying boat
flying fish
flyleaf
flypaper
flytrap
flyweight
flywheel
focus, focuses
focused, -ing
fog-hidden (um)
foghorn
fold-in (adj, n)
foldout
foldup (adj, n)
folklore
folksong
follow-on (adj, n)
followthrough (adj, n)
followup (adj, n)
follow up (v)
foodborne
foodgrain
foodgrower
food-processing (adj)
foodstore
foodstuffs
foolhardy
foolproof
foot-and-mouth (adj)
football
footbath
footbrake
footbridge
foot-candle
foot-dragging
footfall
footgear
foothill
foothold
footlocker
footloose
footnote (n, v)
footnoting
footpad
footpath
footplate
foot-pound
foot-pound-second
footprint
footrace
footrail
footrest
foot-second
foot soldier
footsore
footstep
footstool
foot trail
footwalk
footwall
for (pref)
all one word
forbid, forbade, forbidding
forced labor
force-on-force (adj)
force projection
force protection
forcewide
fore (cf)
fore-and-aft (n, um)
fore-edge
foresee
rest one word
foreign exchange (adj, n)
forest-covered (um)
forest land
forestside
forgettable
forgo (do without)
forego (precede)
foregone conclusion
forklift
fork-tailed (um)
format, -ted, -ting
formfitted
formula, formulas
forsake
forswear, forswore
forte
forthcoming
forthright
forthwith
fortuneteller
forum, forums
forward (ahead)
foreword (preface)
forward-deploy (v)
forward-leaning (um)
forward-looking (um)
foul-looking (um)
foulmouthed
foulup (adj, n)
fountainhead
fourfold
four-footed (um)
four-masted (um)
four-master
four-ply (um)
fourscore
foursome
foursquare
four-star (adj)
fourth-quarter (adj)
four-wheel drive (n)
four-wheel-drive (um)
four-wheeled
foxhole
foxhound
foxtailed
fracto (cf)
all one word
frameup (adj, n)
framework
Francophile
Francophone
freeborn
freedom fighter
free enterprise (adj, n)
free-fall
free-for-all
freehand (drawing)
freehanded
freehold
freelance

freelancer
freeloader
free market (adj, n)
free-market-
  oriented (um)
freemasonry
free port
free-spoken (um)
freestanding (um)
freethinker
freethinking
free trade (adj, n)
freeway (highway)
freewheel (um, v)
freewheeling
free will (n)
freewill (adj)
freeze-dry (v)
freezeout (adj, n)
freezeup (adj, n)
freight car
freight room
fresh-looking (um)
fresh-painted (um)
freshwater (adj)
fresh water (n)
front-end (adj)
frontline
front-loading (um)
front man
fronto (cf)
  fronto-occipital
  fronto-orbital
  rest one word
front page
frontrunner
frontrunning
frontseat
front-wheel (um)
frostbite
frost-free (um)
frost-killed (um)
frostline
frostproof
fruitcake
fruit fly
fruit-growing
frying pan
fueled, fueling
fueler
fuel line
fuel oil
fullback
full-bellied (um)
fullblooded
fuller's earth
fullface
fulfill, -ed, -ing, -ment
full-fledged
full-grown (um)
full load
full-speed (adj, adv)
full-strength (adj, adv)
full-time (adj, adv)
fundraiser
fundraising
fungus, fungi
funneled, -ing
funnel-shaped (um)
fur-clad (um)
furcoat
fur-lined (um)
fur-trimmed (um)
fuse
  fuze (mechanical or electrical)
fuselage
fuseplug

G

gainsay
galact(o) (cf)
  all one word
gallbladder
galley proof (printing)
galvano (cf)
  all one word
gamboled, -ing
game changer
game-changing (um)
game plan
gangboss
gangplank
garrote
gasbomb
gas-driven (um)
gases
gasfield
  but oil and gas fields,
  natural gas field
gas-fired (um)
gas-flow (adj)
gas-heated (um)
gaslamp
gaslight
gaslit
gasline (machine)
  gas line (queue)
gaslock
gas main
gas mask
gasmeter
gastro (cf)
  gastro-omental
  rest one word
gas well
gasworker
gasworks
gatekeeper
gatepost
gauge
Gaullist policies (etc)
gauss
gearbox
gearcase
gear-driven (um)
gear-operated (um)
gearshift
gearwheel
gelatin
gemcutter
gem-set (um)
gemstone
general purpose (adj, n)
genius, geniuses
geo (cf)
  geolocation
  geopolitics
  geotag
  all one word
german silver
germ-free (um)
gerrymander
getaway (adj, n)
getoff (adj, n)
get-together (adj, n)
getup (adj, n)
ghetto(s)
ghostwrite
ghostwriter
gigabyte
gilt-edge (um)
give-and-take (adj, n)
give away (v)
giveaway (adj, n)

glacio (cf)
all one word
glamorous
glamour
glassblower
glasscutter
glassmaking
glassworks
glauco (cf)
all one word
glidepath
glideslope
globetrotting
glosso (cf)
all one word
glove box
gluc(o) (cf)
all one word
glycero (cf)
all one word
glyco (cf)
all one word
go-ahead (adj, n)
goalpost
go-around (adj, n)
goatherd
go-back (adj, n)
go-between (n)
gocart
godchild
goddaughter
godfather
godless
godmother
godparent
godsend
godson
go-fast (adj)
go-getter
go-getting (adj, n)
goings-on
gold-filled (um)
gold-inlaid (um)
goldleaf
gold mine
goldplate
gold-plated (um)
goldsmithing
goodbye
good-faith (adj)
good-for-nothing (n, um)
good-natured (um)
good offices
good-quality (adj)
goodwill
go-off (adj, n)
gooseflesh
gooseneck
goosepimples
gossipmonger
gothic type
government-in-exile
government-owned (um)
governmentwide
grab-all (adj, n)
grab bag
grabhook
grainfield
gram-molecular
gram-negative (um)
gram-positive (um)
grandchild
grandfathered
grandstand
grandstanding
grant aid
grant-in-aid
grapeseed
grapevine
grapho (cf)
all one word
grass-covered (um)
grassroots (nonliteral)
gravedigger
graveled, -ing
graveside
gray
gray arms
gray-haired (um)
gray-market (um, v)
grayout (adj, n)
great-aunt
greatcoat
Greater London (etc)
great-grandchild (etc)
great-power (adj)
great-uncle
greenback (adj, n)
greenbelt (community)
greenhorn
greensand (geology)
greenwood (forest)
green wood (literal)
greyhound
gridiron
ground-attack (um)
ground-based (um)
groundbreaking
groundburst
ground-controlled
intercept
ground crew
ground-effect machine
ground force(s) (adj, n)
groundmass
ground-mobile (um)
ground rules
ground shock
groundspeed
ground station
ground support
groundswell
ground test (adj, n)
ground-test, -ing (v)
ground war
groundwave
groundwater
groundwork
group-connect (v)
groupthink
groveled, -ing
grownup (n, um)
gruesome
guarantee (n, v)
guaranty (n) (law)
guarantor
guardhouse
guard post
guardrail
guerrilla (warfare)
guesswork
guesthouse
guest worker
guided-missile (adj)
guideline
guidepost
guide rail
gun-barrel (adj)
gunblast
guncotton
guncrew
gundeck
gunfight

gunfighting
gunfire
gun-for-hire (um)
gunlock
gunmaking
gun mount
gunplay
gunpoint
gunpowder
gunrack
gunrunner
gunrunning
gunship
gunshot
gun-shy (adj)
gunsight
gunsmith
gunstock
gunwale
gutless
gymno (cf)
all one word
gyneco (cf)
all one word
gypsy
gyro (cf)
gyro horizon
gyro mechanism
rest one word

H

habeas corpus
habitue
hacksaw
hadith
hailstone
hailstorm
hairband
hairbreadth
hairbrush
haircut (n)
hairdo
hairdresser
hairline
hairpin
hairsplitting
hajj(es)
hajji
halal
half-and-half (n, um)
half-afraid
half-alive
halfback (football)
half-baked (um)
half-bound (um)
half brother
half-clear
halfcocked
half-dark
half-day (adj)
half-dozen (adj)
halfhearted
half hour
half-hourly (um)
half-life
half load
half-loaded (um)
half-mast
half measure
half-mile (adj)
half-miler
half-monthly (um)
half moon
half-on (adj, n)
halfpace
halfpenny
half-ripe (adj)
half sister
half-speed (adj)
halfstaff
half-strength (adj)
halftime
halftone (printing)
halftrack
half-true
half-truth
halfway
half-weekly (um)
half-yearly (um)
hallmark
halo(s)
ham-fisted (adj)
ham-handed (adj)
hamstring
hamstrung
hammerhead
hammerlock
hammertoe
handbag
handball
handbill
handbook
hand-bound (um)
handbrake
hand-built (um)
hand-carry (v)
handcart
hand-carve (v)
handclap
handclasp
hand-clean (v)
hand-courier (v)
handcrank
handcuff
hand-cut (v)
hand-fed (v)
handgrenade
handgrip
handguard
handgun
hand-held (um)
hand-high (um)
handhold
handicap, -ped, -ping
hand-in-hand (um)
handkerchief
hand-knit (v)
handlebar
hand-letter (v)
handmade
hand-me-down (adj, n)
handmix (v)
handoff (adj, n)
hand off (v)
handout (adj, n)
hand out (v)
handover (n)
handpick (v)
handpicked
handprint
handrail
handsaw
hand-selected
handset
handshake
hands-off (adj)
hands-on (adj)
handspring
handspun
hand-stamp (v)
handstand
handstitch

hand-tailored (um)
handtool
hand-tooled (um)
handwoven
hand-wringing
handwrite (v)
handwritten
hangdog
hang glider
hangnail
hangout (adj, n)
hangup (adj, n)
happy-go-lucky
hara-kiri
harass
harbormaster
harborside
hard-and-fast
hard-baked (um)
hard-bitten (um)
hard-boiled (um)
hardcase
hard-charging
hardcopy
hardcore
hardcover
hard currency (adj, n)
hard drive (n)
hard-driving (um)
hardhat
hardheaded
hard-hit (um)
hard-hitting (um)
hard line (n)
hardline (adj)
hardliner (n)
hardnose
hardpan
hard-pressed (um)
hard-set (um)
hardship
hardstand
hard-surface (um)
hardtack
hard-target (adj)
hardtop (auto)
hard up
hardware
hardwired
hard-won (um)
hard work
hard-working (um)
has-been (n)
hashmark
hashtag
hatband
hatpin
hatrack
haulback (n)
have-not (adj, n)
haversack
hawkbill
hawk-nosed (um)
hawsepipe
hayloft
haymarket
haystack
haywire
H-bar
H-beam
H-bomb
headache
headachy
headband
headcloth
headcount
headdress
headfirst
headgear
headhunter
headlamp
headlight
headline
headlock
headlong
head of state
head-on (adj, adv)
headphone
headquarters
headrest
headroom
headscarf
headset
headspace
headspring
headstand
headstart
headstock
headstream
headstrong
heads-up (adj, n)
headwaiter
headwaters
headway
headwind
health care (adj, n)
healthful (producing health)
  healthy (in good health)
heartache
heartbeat
heartbreak
heartburn
heartfelt
heartland
heartsick
heartstring
heartthrob
heat-resistant (um)
heat-sensitive (um)
heatstroke
heat-treating (um)
heavy-duty (um)
heavyhanded
heavy-lift (adj)
heavyset
heavy water (n)
heavy-water (adj)
heavy-water-moderated
heavyweight (adj, n)
hecto (cf)
  all one word
hedgehog
hedgehop
height-finding (adj)
heir apparent
helicopter-borne (um)
helio (cf)
  all one word
helix, helices
helpmate
help page
helter-skelter
hema (cf)
  all one word
hemi (pref)
  all one word
hemo (cf)
  all one word
hempseed
henceforth
henceforward
hepato (cf)
  all one word

hepta (cf)
all one word
herculean task (etc)
hereafter
hereby
herefrom
herein
hereof
hereon
hereto
heretofore
herewith
herringbone
hetero (cf)
all one word
hexa (cf)
all one word
H-hour
hiccup
hide-and-seek (adj, n)
hideaway (adj, n)
hidebound
hideout (adj, n)
hi-fi
high-altitude (um)
highball
highborn
highbred
highbrow (nonliteral)
high-caliber (um)
high-class (um)
high-density (um)
high-energy (um)
high-explosive (um)
higher-than-market (um) (etc)
higher-up (n)
highflier (n)
highflying (um)
high frequency (n)
high-frequency (um)
highhanded
high-hat (v)
high-intensity (um)
highlander
high-level (um)
highlight (nonliteral)
high-minded (um)
high point
high-power (um)
high-precision (um)
high-pressure (um, v)
high-priced (um)
high proof
high protein (adj)
high-quality (um)
high-ranking (um)
high-reaching (um)
high-rise
highroad
high school (adj, n)
high seas
high-speed (um)
high-strung (um)
high-tech (um)
high-technology (um)
high-tension (um)
high-up (um)
high-value (um)
high water
high water mark
hijack
hijacker
hillside
hilltop
hill tribe
hindcast
hindleg
hindmost
hindrance
hindquarter
hindsight
hipbone
hip-hop (adj, n)
hippo (cf)
all one word
hipshot
histo (cf)
all one word
hit-and-miss (adj)
hit-and-run (adj)
hitchhiker
hit-or-miss (adj)
Hizballah
hoarfrost
hobbyhorse
hocus-pocus
hodgepodge
hogback
hognose (machine)
hog-nosed (um)
hog's-back (geology)
hogshead
hogsty
hog-tie (v)
hogwash
holdall (adj, n)
holdback (adj, n)
hold-clear (adj, n)
holddown (adj, n)
holdfast (adj, n)
holdoff (adj, n)
holdout (adj, n)
holdover (adj, n)
hold time
holdup
holland cloth
hollow-ground (um)
holo (cf)
all one word
home-baked (um)
home base (n)
home-based (v)
homebody
homebred
homebrew
homebuilder
homebuilding
home buyer
homecoming
home-fed (um)
homefront
homegrown
homeland
homelife
homemade
homeo (cf)
all one word
homeowner
homepage
homeplate
home port (n)
home-port (v)
home rule
homesick
homespun
homestead
homestretch
hometown
homeward
homo (cf)
all one word
homologue
honey-colored

honeycomb
honeydew
honeymoon
honeypot
honeytrap
honorbound
hoodwink
hoofbeat
hoofprint
hook-nosed (um)
hookup (adj, n)
hop point
hopscotch
horehound
hormono (cf)
all one word
hornbill
hornblower
hornpipe
horseback
horseflesh
horsehair
horsehead
horsehide
horsehoof
horsemeat
horseplay
horsepower-hour
horsepox
horserace
horse sense (n)
horseshoe
horsethief
horsetrading (nonliteral)
horsewhip
hostage taker
hostage taking
host country
host name
host nation
hotbed
hotblood
hot-blooded (um)
hot-cold
hotdog
hotfoot
hothead (n)
hotheaded
hothouse
hot-launched
hotline (nonliteral)
hotlink
hot-mix (um)
hotpatch
hotplate
hot-press (v)
hot-pursuit (adj)
hotrod (nonliteral)
hot-roll (v)
hot-rolled (um)
hotspot
hot-swap (v)
hot swap (n)
hotwork (v)
hourglass
housebreaking
housebroken
housebuilder
housebuilding
house call
housecleaner
house-cleaning (adj)
houseguest
household
housekeeping
housetop
housetrailer
housewares
housewarming
housewife
housework
hover craft
however
howsoever
how-to (adj, n)
H-piece
hubcap
hull-less
humanitarian assistance
humankind
human rights (adj, n)
human-source (adj)
humdrum
humpback
Humvee
hunchback
hundredfold
hundredweight
hunger strike
hung-up (um)
hunter-killer (adj, n)
hush-hush
hush money
hushup (adj, n)
hydro (cf)
hydroelectric
hydroplant
hydropower
hydro station
rest one word
hygro (cf)
all one word
hyper (pref)
hyper-Dorian (etc)
hyperlink
rest one word
hypo (cf)
all one word
hypothesis, hypotheses
hypotenuse

I

I band (etc) (adj, n)
I-bar
I-beam
iceberg
iceblind
ice blindness
iceblock
icebound
icebreaker
icecap
ice-clad (um)
ice-cold (um)
ice-covered (um)
ice cream
icefall
icefield
ice fishing
icefloe (island)
iceflow (current)
ice-free
icemaking
icemelt
icepack
ice shelf
ice skate (n)
ice-skate (v)
ice-skating
ice storm
ice water
ID (n, v)

ideo (cf)
  ideounit
  rest one word
I-iron
ill-advised (adj)
ill-advisedly
ill-defined (adj)
ill-fated (adj)
ill health
ill-prepared (adj)
ill-timed (adj)
ill-treat (v)
ill-use (v)
ill will
imam
impaneled, -ing
impel, -led, -ling
imperiled, -ing
import-export
impostor
in (pref/cf)
  inactive (um)
  in-and-out (um)
  inasmuch
  in-being (um)
  incountry (um)
  indepth (um)
  infighting
  inflight (um)
  in-house
  in-law (n)
  inmigration (um)
  inport (um)
  inservice (um)
  inshore
  insofar
  intheater (um)
  rest one word
in absentia
inbox
inch-deep (um)
inch-long (um)
inch-pound
incur, -red, -ring
index, indexes
india ink
indigo(s)
Indo-European (etc)
industrywide
in extenso
in extremis
infantryman
infer, -red, -ring
inferable
inference
information gathering
information sharing
infra (pref)
  infrared
  infra-axillary
  infrastructure
  rest one word
ingenious (skillful)
  ingenuous (simple)
ink-black (um)
inkjet
inkpot
inkspot
inkstain
inkstand
inkwell
in loco parentis
inner circle
inner-city (adj)
ino (cf)
  all one word
input, -ting
insect-borne (um)
insignia
in situ
install, -ed, -ing, -ment
installation
instant-message (adj, v)
instant message (n)
instill, -ed, -ing
intelligence collection
intelligence gathering
intelligence sharing
inter (pref)
  inter-American (etc)
  interchange
  intersperse
  rest one word
inter alia
inter alios
interceptor
interment (burial)
  internment (jail)
intern
Internet
intervener
intifada
in toto
intra (pref)
  intra-atomic (etc)
  intracoastal
  intranet
  rest one word
intransigent (adj, n)
intro (pref)
  all one word
in vitro
in vivo
ipso facto
ipso jure
I-rail
ironclad
ironfisted
iron-free (um)
ironhanded
iron-lined (um)
iron lung
ironmaking
iron-red (um)
ironside
ironworking
ironworks
Islamization
island-born (um)
iso (cf)
  isooctane
  iso-osmosis
  rest one word

J

jackhammer
jack-in-the-box
jackknife
jack-of-all-trades
jackpot
jackrabbit
jackscrew
jackstay
jailbreak
jampacked
jawbone
jawbreaker
jaywalk
J-bolt
jeep (vehicle type, not trade name)
jellybean
jellyroll

jet aircraft
jet airliner
jet bomber
jetliner
jetport
jet-powered (um)
jetprop
jet-propelled (um)
jet propulsion
jet set
jetstream
jetwash
jeweled, -ing, -er
jewel-studded (um)
jigsaw
jihad
jobholder
jobseeker
joint-force (um)
joint-service (um)
joint-use (um)
joint-venture (um)
joule
joulemeter
journeyman
joyride
joystick
judgment
judgeship
jujitsu
jump off (v)
jumpoff (adj, n)
jump-start
jungle-clad (um)
jungle-covered (um)
juniormost
junk mail
junkpile
jury box
jury-fixing (um)
jury-rigged (um)
just-completed (um) (etc)
juxta (cf)
  juxta-articular
  rest one word

K

keelblock
keelhaul
keel-laying (um)
keel line
keepsake
kerato (cf)
  all one word
kerosene
kettledrum
key-activated (adj)
keyhole
keylock
keynote
keypunch
keyring
keyword
kickback (adj, n)
kick-in (adj, n)
kickoff (adj, n)
kickout (adj, n)
kick-start
kidnap-for-ransom (um)
kidnapped, -ping
kidnapper
kilo (pref)
  kilobyte
  kilogram-meter
  kilohertz
  kilovoltampere
  kilowatt-hour
  rest one word
kindhearted
kingbolt
kingmaker
kingpin
kiss-off (adj, n)
knapsack
knee-deep (um)
knee-high (um)
knee-jerk (adj)
kneepad
knifepoint
knockabout (adj, n)
knockdown (adj, n)
knock-kneed (um)
knockoff (adj, n)
knock-on (adj, n)
knockout (adj, n)
knothole
know-all (adj, n)
know-how (adj, n)
know-it-all (adj, n)
knowledgeable
know-little (adj, n)
know-nothing (adj, n)
knucklebone
kolkhoz(es)
kopek
kosher
K-ration
K-term

L

labeled, -ing
labor-intensive (um)
laborsaving
labor union
lackluster
laid-off (um)
laid-up (um)
laissez faire
lakebed
lakefront
lakeshore
lakeside
lameduck (nonliteral)
lampblack
lamppost
lampshade
lampstand
land-attack (adj)
land base
land-based (um)
landborne
landbound
landfall
landfast
landfill
landform
landgrab
landgrabber
land-grant (um)
landholding
landline
landlocked
landlord
landmark
landmass
landmine
land-mobile (um)
landowner

landownership
landowning
land-poor (adj)
landscape
landside
landslide
land tax
landward
lapbelt
laptop
large-scale (adj)
lash-up (adj, n)
lasso(s)
last-cited (um)
last-ditch (adj)
last-minute (adj)
last-named (um)
latchbolt
latchkey
latecomer
late-June (etc) (um)
late-model (adj)
lath (wood)
  lathe (machine)
latter-day (adj)
lattermost
laughingstock
launch crew
launching ways (singular and plural)
launch-on-tactical-warning (adj, n)
launch on tactical warning (v)
launch-on-warning (adj, n)
launch on warning (v)
launch pad
launch site
launch stand
launch weight
laureled
law-abiding (um)
law-and-order (adj)
lawbreaker
lawmaking
lawsuit
layaway (adj, n)
layback (adj, n)
lay-by (n)
laydown (adj, n)
layman
layoff (adj, n)
layout (adj, n)
layover (adj, n)
layperson
layup (adj, n)
lay up (v)
laywoman
L-bar
L-beam
L-block
leader line
lead-filled (um)
lead-gray (um)
lead-in (adj, n)
leadline
lead line (medical, nautical only)
leadoff (adj, n)
leadout (adj, n)
leadtime
lead-up (adj, n)
lead up (v)
leakthrough
lean-to (adj, n)
leapfrog
leap year
leaseback (adj, n)
leasehold
leather-bound (um)
leather-covered (um)
leatherworking
leavetaking
lee shore
leeward
left-bank (v)
left-click (n, v)
left field
left-hand (adj)
left-handed (um)
left-leaning (adj)
leftmost
left-of-center (um)
left-sided (um)
leftwing (adj)
left wing (n)
leftwinger
lend-lease
Leninist doctrine (etc)
lens, lenses
lepto (cf)
  all one word
less developed (etc)
letdown (n, um)
letter bomb
letterhead
letter-perfect (um)
letterpress
letterwriting
letup (n)
let up (v)
leuc(o) (cf)
  all one word
leveled, -ing
leveler
levelheaded
libeled, -ing
liberal-minded (um)
lieutenant colonel
lieutenant governor
lieutenant-governorship
lifebelt
lifeblood
lifeboat
life cycle
lifeguard
life insurance (adj, n)
lifejacket
lifelike
lifeline
lifelong
liferaft
lifering
lifesaver
lifesaving
life-sized (adj)
lifespan
lifestyle
lifetime
lifevest
liftoff (adj, n)
light-armed (um)
light-clad (um)
lighter-than-air (um)
lightface (printing)
light-footed (um)
light-producing (um)
lightship
light water (n)
light-water (adj)
lightweight (adj, n)
light-year
likable

like-minded (um)
limekiln
linchpin
line-of-sight (um)
lineup (adj, n)
line up (v)
linkup (adj, n)
link up (v)
lionhearted
lipread
lipservice
liquefy
liquid-fueled (adj)
liquid-propellant (adj)
liquid-propelled (um)
litho (cf)
  litho-offset
  rest one word
little-known (um)
little-used (um)
livable
live-fire (um)
live load
livestock
live wire
  livewire (nonliteral)
living costs
loadmeter
loadout (adj, n)
loath (adj)
  loathe (v)
lockjaw
locknut
lockon (adj, n)
lock on (v)
lockout (adj, n)
lockstep
lockup (adj, n)
locker room
locus, loci
lodestar
lodestone
lodgment
logbook
loggerheads
login (adj, n)
log in (v)
logjam
logout (adj, n)
log out (v)
logsheet
logo (cf)
  all one word
lone-wolf (um)
long ago (adv, um)
long-awaited (um)
long-bed (truck)
longbow
long-distance (adj)
long-drawn (um)
longfelt
long-haired (um)
longhand (nonliteral)
long-handled (um)
long-lasting (um)
long-lived (um)
long-past (um)
long-pending (um)
longplaying (um)
long-range (um)
long-run (adj)
longstanding (adj)
long-term (adj)
longtime
longwave (radio)
longways
longwinded
look-alike
look angle (n)
lookdown (adj, n)
lookdown-shootdown (adj)
look-in (adj, n)
lookout (adj, n)
lookthrough (adj, n)
lookup (adj, n)
look up (v)
loophole
looseleaf
loose-tongued (um)
lopsided
loudmouthed
loudspeaker (radio)
loud-voiced (um)
louver
low-altitude (um)
lowborn
lowboy
low-built (um)
lowdown (n, um)
low Earth orbit
low-enriched uranium
lowercase (printing)
lower-class (um)
lower-grade (um)
lower-income (um)
lower-level (um)
lower-middle-class (um)
lowermost
low-end (adj)
low-fat (um)
low frequency (n)
low-frequency (um)
low-income (um)
low-intensity (um)
low-key (adj)
lowland (adj, n)
low-level (adj)
low-lying (um)
low-observable
  (adj, n)
low-power (um)
low-pressure (um)
low-priced (um)
low-quality (um)
low-ranking (um)
low-technology (um)
low water
L-shaped
L-square
lukewarm
lumberjack
lumber room
lumberyard
lunchtime
luster
lying-in (adj, n)

M

macadamized road
mach 2 (etc)
machine building (n)
machine-building (um)
machine-finished (um)
machinegun
machine-hour
machine-made (um)
machine shop
machine tool
machine work
machismo (n)
macho (adj)
macro (cf)
  all one word

madam, mesdames
madcap
made-over (um)
made-up (um)
madras cloth
madrassa(s)
magneto (cf)
  magneto-optics
  rest one word
mailbag
mailbox
mail-order (um)
mainframe
mainland
main line (literal)
  mainline (nonliteral)
mainmast
mainsail
mainsheet
mainspring
mainstay
mainstream (nonliteral)
maintop
main yard
major-domo
major-leaguer
major-minor
make-believe (adj, n)
makefast (n)
makeshift
makeup (adj, n)
make-work
making up
mal (cf)
  all one word
malware
manageable
manager-director
man-day
maneater
maneuver
manhandle
manhole
man-hour
manic-depressive
manifold
manila envelope
man in the street
mankind
manmade (adj)
man-of-war
man-portable (um)
manpower
mantel (shelf)
  mantle (cloak)
many-colored (um)
man-year
manyfold
many-sided (um)
mapmaker
mapreading
marijuana
markdown (adj, n)
marketplace
markoff (adj, n)
markshot
markup (adj, n)
marshaled, -ing
marshaler
martial law
marveled, -ing
marvelous
Marxism
mashup (adj, n)
mason jar
mass-casualty (um)
mass-produce (v)
master at arms
mastermind
master of ceremonies
master's degree
masterstroke
masthead
matchhead
matchstick
matrix, matrices
matter-of-fact (adj)
maxi (pref)
  all one word
maximum, maximums
maybe (adv)
May Day (1 May)
  mayday (distress call)
M-day
meager
mealtime
mean-spirited (um)
mean time (astronomical)
  meantime (meanwhile)
meanwhile
measurable
meatpacking
mecca (center of interest, not the city)
mechanico (cf)
  all one word
medaled, -ing
medalist
medieval
medio (cf)
  all one word
medium, media
medium and high altitudes
medium- and high-altitude (adj)
medium-to-high altitude (n)
medium- to high-altitude (adj)
medium-sized (um)
meetingplace
mega (cf)
  megabyte
  megadose
  megaproject
  all one word
megalo (cf)
  all one word
meltdown (n, um)
meltwater
member-state (adj)
member state (n)
memento(s)
memorandum, memorandums
merchant ship
meso (cf)
  all one word
messhall
messkit
mess-up (adj, n)
meta (pref)
  metadata
  metatag
  all one word
metalammonium
metal-clad (um)
metal-coated (um)
metal-cutting (um)
metaled, -ing
metal-lined (um)
metalworker
metalworking

metalworks
meter-amperes
meter-kilogram
meter-kilogram-second
metier
metro (cf)
  all one word
Metro Manila (etc)
Metropolitan Moscow (etc)
  but Moscow
    metropolitan area (etc)
micro (cf)
  microblog
  microorganism
  all one word
mid (cf)
  midair
  mid-American (etc)
  mid-April (etc)
  midday
  mid-decade
  mid-18th century (n) (etc)
  mid-18th-century (adj) (etc)
  mid-1980 (etc)
  mid-1980s (etc)
  mid-1980s-style (adj)
  mid-ice
  midinfrared
  midlevel
  midmorning
  mid-Pacific (etc)
  midrange
  midstage
  midterm
  mid-to-late 1980 (etc)
  midyear
  rest one word
middle age
middle-aged (um)
middle-class (um)
Middle East (adj, n)
  Middle Eastern (adj)
middle ground
middle-income (um)
middleman
middlemost
middle-of-the-roader
middle-sized (um)
middleweight
midi (pref)
  all one word
mild-mannered (um)
mileage
mile-long (adj)
milepost
mile-wide (adj)
Military Departments (U.S.)
military-political (um)
Military Services (U.S.)
militiaman
militia member
millennium, millennia
milli (cf)
  milligram-hour
  rest one word
millimeter wave
millpond
millpost
millrace
millstream
mill wright
minable
mincemeat
mindreader
mindreading
mindset
mineclearing
minefield
minehunter
minehunting
minelayer
minelaying
mineship
minesweeper
minesweeping
minethrower
mine warfare (adj, n)
mineworks
mini (pref)
  miniempire
  mini-state
  rest one word
minimum, minimums
minimum-security (adj)
minister-counselor
minor-leaguer
minutia (rarely used),
  minutiae (plural)
MIRVed
mis (pref)
  all one word
mischiefmaking
missile defense (adj, n)
missile-equipped (um)
missile support (adj, n)
missile suspension (adj, n)
mission-critical (um)
mist-covered (um)
miter
miter box
miter-lock (v)
mixup (n)
mixing room
mizzenmast
mobile erector-launcher
mobile missile (adj, n)
mockup (adj, n)
modeled, -ing
modeler
modus operandi,
  modi operandi
modus vivendi,
  modi vivendi
mold
molehill
molotov cocktail
mollusk
molt
moneybag
moneychanger
money-laundering (um)
moneylender
moneymaking
moneysaving
mono (cf)
  mono-ideistic
  mono-ion
  rest one word
monogrammed, -ming
monsieur, messieurs
monthend
monthlong (adj)
month-old (adj)
moonbeam
moonglow
moonlight
moonrise
moonset
moonshine
moonstruck
mopping-up (um)
mopup (adj, n)
mop up (v)

moratorium,
  moratoriums
moreover
Morse code
mortise
most-favored-nation (um)
most-sought-after (um)
mothball(ed)
moth-eaten (um)
mother-in-law
motherland
mother ship
moto (cf)
  all one word
motorbike
motorboat
motorbus
motorcade
motorcoach
motorcycle
motor-driven (um)
motordrome
motor pool
motorship
motor torpedo boat
mountain-high (um)
mountainside
mountaintop
mouthful
mouthpiece
movable
moviegoer
moviemaking
much-needed (um)
muckrake (v)
muckraker (n)
mudbank
mud-colored (um)
mudflat
mudflow
mudguard
mudhole
mudslinging
muezzin
mujahid, mujahideen
  but follow source's spelling if part of a group name
mullah
multi (cf)
  multifiber
  multifamily
  multi-ply (several plies)
  multipurpose
  multistory
  multiton
  all one word
multiple-launch rocket system
multiple-purpose (adj)
multiple rocket launcher
musclebound
musico (cf)
  all one word
music teacher
mustache
myria (cf)
  all one word
mytho (cf)
  all one word

N

nailhead
nail-studded (um)
naive
naivete
name-calling (um)
name-dropping (um)
nameplate
namesake
nano (cf)
  nanotechnology
  all one word
narco (cf)
  narcotrafficker
  narcotrafficking
  all one word
narrow-band (adj)
narrow-beam (adj)
narrow-body (adj, n)
narrow gauge (adj, n)
narrowminded
nation-state
nationwide
native-born (um)
natural gas (adj, n)
natural gas field
navy-blue (um)
nearby
near-Earth orbit
Near East (n)
  Near Eastern (um)
near-infrared (um)
near miss
near-real time (n)
near-real-time (um)
nearsighted
near success
near-term (um)
neckband
neckbone
neck-deep (um)
neck-high (um)
necktie
needlepoint
needle-sharp (um)
need to know (n)
need-to-know (adj)
ne'er-do-well
neo (cf)
  neofascist
  neo-Greek (etc)
  neo-Nazi (etc)
  rest one word
neon light
nerve-racked (um)
nerve-racking
net-centric (adj)
nettlesome
network
net worth
neuro (cf)
  all one word
never-ending (um)
nevermore
nevertheless
newborn
newcomer
new-fashioned (um)
newfound
new-made (um)
newscast
newscaster
newsclip
news editor
news feed
newsletter
newsmagazine
newsmaking
newspaper
newspeople

newsphoto
newsprint
newsreader
newsreel
newssheet
newsstand
newsstory
newsweekly
newsworthy
newton
next-generation (adj)
next of kin
nickel
nickelplate
nickel-plated (um)
nickeltype
nickname
nightclub
night editor
night-fly (aviation) (v)
night-flying (um)
nightlife
nightlong (um)
night school
night shift
nightstick
nighttime
night-vision (um)
nightworker
nimbostratus
ninefold
nine-lived (um)
nitpick, -ing
nitro (cf)
  nitro-hydro-carbon
  rest one word
no-account (adj, n)
noble-minded (um)
noblesse oblige
nobody
no-confidence (um)
no-fault (adj)
no-first-use (um)
no-fly zone (adj, n)
no-go (adj, n)
no-good (n, um)
no-hitter (n)
noisemaker
noisemaking
no man's land
nom(s) de guerre
nom(s) de plume
non (cf)
  non-air-transportable
  nonaligned
  non-civil-service
  noncommissioned
  noncommunist
  non-Communist Party
  noncontrol
  non-DIA (etc)
  nondivisional
  non-European (etc)
  nonferrous
  non-intelligence-related
  nonlifelike
  nonmilitary
  nonMIRVed
  non-missile-equipped
  non-mission-capable
  nonnegotiable
  nonnuclear
  non-nuclear-weapon state
  non-nuclear-powered
  non-nuclear-related
  nonoceangoing
  nonoil
  non-oil-producing
  nonoperational
  non-party-member
  non-rare-earth
  non-scientific and technical
  non-self-propelled
  non-self-sustaining
  non sequitur (etc)
  nonstate
  nonuse-of-force (adj)
  non-U.S. NATO forces
  as prefix, one word
nonesuch
nonetheless
no-no
  no-no's (plural)
no-nonsense (adj)
noonday
northbound
north-central
northeast
northeastern
north end
northernmost
northgoing
north-northeast
north-northwest
north shore
north-sider
northward
northwest
nosecone
nosedive
nosedown (adj, n)
nose-high (um)
nosering
nose tip
noseup (n, um)
nosewheel
no-show (adj, n)
notebook
note-taking (um)
note paper
noteworthy
notwithstanding
nouveau riche,
  nouveaux riches
no-war/no-peace
nowhere
nuclear-armed (um)
nuclear-capable (um)
nuclear delivery (adj, n)
nuclear-free zone
nuclear power (adj, n)
nuclear-powered (um)
nuclear strike (adj, n)
nuclear-warfighting (um)
nuclear weapons (adj, n)
nuclear-weapons-free zone
nuclear weapon state
nucleo (cf)
  all one word
nucleus, nuclei
number-one (um) (etc)

O

oarlock
oasis, oases
obkom
oblast
occur, -red, -ring
occurrence
oceanborne
oceangoing
oceanside
ocean-spanning (um)
oceanwide
ocher
octo (cf)
  all one word
octopus, octopuses
odd-looking (um)
odd number
odd-numbered (um)
off-and-on (um)
off-balance
off-base (um)
offbeat
off-campus
offcenter (um)
off chance
offcolor (adj)
off day
off-duty (um)
offense
offered, -ing
offguard
offhand
off-hours
officeholder
officeseeker
office-seeking (um)
officeworker
off-limits (um)
offline
offload
offprint
off-putting
off-ramp
off-road
offscreen
off-season
offset
offshoot
offshore
offside
offsite
offstage
off-the-rack (um)
off-the-record (um)
off-the-shelf (um)
off-track
off-white (um)
off year
oftentimes
ohm-ammeter
ohmmeter
oilcan
oilcloth
oil-driven (um)
oil-fed (um)
oilfield
oil-forming (um)
oil-producing (um)
oil-rich
oil sands (adj, n)
oil shale (adj, n)
oil-soaked (um)
oilspill
oil workers
oil well
old-fashioned (um)
old-guard (adj)
old-line (adj)
oldstyle (printing)
oldtime
oleo (cf)
  oleo gear
  oleo oil
  oleo strut
  rest one word
olivewood
Olympics
  Olympic Games, the games
  Summer Olympics
  Winter Olympics
ombudsman, ombudsmen
omni (cf)
  omni-ignorant
  rest one word
on (cf)
  on-again/off-again
  on-and-off (adj, n)
  onbase (adj, n)
  onboard (adj, n)
  on call (n)
  oncall (um)
  on-demand (um)
  ongoing
  onhand (adj, n)
  online (adj, n)
  onscene
  onshore
  onsite (adj, n)
  onstation (adj, n)
  onstream
  rest one word
once-over
one-armed (um)
one-eyed (um)
onefold
one-half (etc)
one-handed (um)
one-man/one-vote
one-on-one
oneness
one-piece (um)
oneself
one-sided
one-sidedness
one-striper
onetime (former)
one-time (single instance) (um)
one-two-three
one-way
on-ramp
on-the-job (um)
onward
open-air (um)
open-armed (um)
open-backed (um)
opencut (mining)
open-door (um)
open-ended (um)
openhanded
open house
openminded
open-ocean (adj)
open pit (adj, n)
open-source (adj)
open source (n)
opt-in (adj, n)
optoelectronics
orbited, ing
orderly room
order-of-battle (um)

ordinance (law)
  ordnance (weapons)
organo (cf)
  all one word
ortho (cf)
  all one word
out (cf)
  out-and-out (um)
  outfight
  out-loud (um)
  outmaneuver
  outmigration
  out-of-area (um)
  out-of-date (um)
  out-of-door(s) (um)
  out-of-state (um)
  out-of-the-way (um)
  as prefix, one word
outbox
outer-city (um)
outermost
outer space
outfit, -ted, -ting
outward-bound (um)
outyear
ovenbaked
ovendried
over (cf)
  overabundance
  overactive
  overage (older) (n, um)
  overage (surplus)
  overall
  overfishing
  overhaul
  overriding
  over-snow vehicle
  over-the-counter (um)
  rest one word
oxcart
oxhide
oxy (cf)
  all one word

P

pacemaker
pace-setting (um)
packhorse
packsaddle
packup (adj, n)
padlock
page-for-page (um)
page proof
page view
painkiller
painstaking
paintball
paintbrush
paintmixer
paintstained (um)
paleo (cf)
  paleo-Christian (etc)
  rest one word
pallbearer
pan (cf)
  Pan-American,
    Pan-Asian,
    Pan-Islamic (etc)
  Pan American Union
  panchromatic
  Panhellenic
  pantheism
  rest one word
paneled, -ing
panic-stricken (um)
panto (cf)
  all one word
paperback
papercutter
papermill
paper-thin (um)
paperweight
para (cf)
  para-anesthesia
  paramilitary
  rest one word
paralleled, -ing
parceled, -ing
parenthesis,
  parentheses
par excellence
parimutuel
part-finished (um)
parti (cf)
  all one word
particle beam weapon
partnership
part owner
part-time (adv, um)
part-timer (n)
part way
party giver
partygoer
party line
partywide
passageway
passcode
passenger car
passer(s)-by
passkey
pass-in-review (adj, n)
passout (adj, n)
passphrase
passport
passthrough (adj, n)
pass through (v)
password
password-protect (v)
past-due (um)
pasteurize
pastureland
pat-down (adj, n)
pathbreaker
pathfinder
patho (cf)
  all one word
patri (cf)
  all one word
patrol, -led, -ling
Patton tank
pawnbroker
payback (adj, n)
paycheck
payday
paydirt
paygrade
payload
payoff (adj, n)
payout (adj, n)
payroll
peacekeeping
peace-loving (um)
peace-building (um)
peacemaking
peacetime
peacoat

pea-green (um)
peakload (n, um)
peanut
pea-sized (um)
peat-roofed (um)
pebble-strewn (um)
peddler
peeloff (adj, n)
peephole
peer-to-peer (adj)
pegleg
penciled, -ing
pendant (n)
  pendent (hanging)
  pendant number (ship)
penknife
penmanship
pen name
pennyworth
penta (cf)
  penta-acetate
  rest one word
pent-up (um)
peptalk
per capita
percent
percentage
percentile
per centum
per diem
perestroyka
peri (pref)
  peri-insular
  rest one word
periled, -ing
permafrost
permit, -ted, -ting
per se
persona non grata
persulfide
pestridden (um)
petaled, -ing
petro (cf)
  petro-occipital (etc)
  rest one word
pharmaco (cf)
  pharmaco-oryctology
  rest one word
pharming
phased-array (adj)
phasedown (adj, n)
phase down (v)
phase-in (adj, n)
phase in (v)
phasemeter
phaseout (adj, n)
phase out (v)
pheno (cf)
  all one word
phenomenon, phenomena
philistine
philo (cf)
  philo-French (etc)
  rest one word
phishing
phono (cf)
  all one word
phony
phospho (cf)
  all one word
photo (cf)
  photo atlas
  photo interpretation
  photo-offset
  photooxidation
  photoreconnaissance
  rest one word
phreno (cf)
  all one word
physico (cf)
  all one word
physio (cf)
  all one word
pianoforte
pickax
picket line
picklock
pick-me-up (adj, n)
pickoff (adj, n)
pickover (adj, n)
pick over (v)
pickpocket
pickup (adj, n)
pick up (v)
picture book
piece goods
piece de resistance
piecemeal
piece rate
piecework
pieceworker
pierside
piezo (cf)
  piezo-oscillator
  rest one word
pigeonhole
piggyback
pikestaff
piledriver
pile-driving (um)
pileup (adj, n)
pilot boat
pilot light
pinball
pinch-hit (v)
pinch-hitter
pinfeather
pinhole
pinhook
pinpoint
pinprick
pinup (adj, n)
pinwheel
pipe bomb
pipedream
pipefitter
pipefitting
pipelayer
pipelaying
pipeline
pipe smoker
pipestem
pipet
pistol-whip (v)
pistonhead
pitch-black (um)
pitchblende
pitch-dark (um)
pitchfork
pitchout (adj, n)
pitchup (adj, n)
pitfall
pitot tube
placecard
placekick
place name
plague-infested (um)
plain-clothed (adj)
plainclothes (um)
plainclothesman
plain-looking (um)
plain-spoken (um)
plaintext

planeload
plane-parallel (um)
planetable (surveying)
plani (cf)
all one word
plano (cf)
all one word
plantlife
plaster of paris
plateau, plateaus
plate glass
plate proof (printing)
plate-roll (v)
plate-rolled (um)
platy (cf)
all one word
play-act (v)
playback (adj, n)
playdown (adj, n)
play down (v)
playground
playlist
playoff (adj, n)
plaything
pledger
pleo (cf)
all one word
pleuro (cf)
all one word
plow
plowhand
plowhorse
plowshare
plug-in (adj, n)
plug in (v)
plus or minus
plus-up
pluto (cf)
all one word
pneumato (cf)
pneumato-hydato-genetic (um)
rest one word
pneumo (cf)
all one word
pocketknife
pocket-sized (um)
pocket-veto (v)
pockmark
pockmarked (um)
podcast
podium, podiums
pointblank
point defense
point man
point person
poison-dipped (um)
polearm
poleax
pole-shaped (um)
polestar
pole-vault (v)
policymaker
policymaking
politico (cf)
politico-orthodox (etc)
rest one word
pollwatcher
poly (cf)
all one word
pommeled, -ing
pontoon (civilian and military)
Ponzi scheme
poor-quality (adj)
poppy farming
poppyfield
poppyseed
pop-up (adj, n)
pop up (v)
pork-barrel (adj)
port call
portfire
portfolio
porthole
portmanteau
portside
post (cf)
postattack
postaudit
post bellum
postblast
postboost
postcard
post-Christian (etc)
post diem
post-free (um)
postgraduate
posthaste
post hospital (military)
posthostilities
post meridiem
postmodern
postmortem
post office
postreentry
post school (military)
poststrike
post-target-tracking
posttest
posttreaty
postwar
as prefix, one word
potash
potato field
potbellied
potboiler
pothole
potlatch
potluck
potpourri
potshot
poultry-raising (um)
pound-foolish (adj)
pound-foot
powder-blue (um)
powder house
powder mill
powder room
power base
power broker
power-driven (um)
powerhouse
powerline
power-operated (um)
powerpack
powerplant
power play
power-projection (um)
power-sharing (um)
powerstation
practice (n, v)
praiseworthiness
praiseworthy
pre (pref)
preattack
predétente
predetermine
preexamine
preexisting
pre-Incan (etc)
preindependence
pre-martial-law (etc)
pre-position (v)
preseries
rest one word

précis (singular and plural)
precision-guided (um)
prefer, -red, -ing
preferable
preference
premier (first in status)
  premiere (first performance)
present-day (um)
president-elect
president pro tempore
press agent
press-forge (v)
press-gang (n, v)
press-made (um)
pressplate
press proof (printing)
presstime
pretense
preter (pref)
  all one word
preventive
price-cutting (um)
price-fixing (um)
pricelist
price-sharing (um)
price-support (um)
pricetag
prima facie
prime minister
prime-minister-
  designate
  but Prime Minister-
  designate Jones (etc)
prime-ministerial
prime-ministership
prime-ministry
prime mover
prime-time (um)
printout (n)
printshop
prisoner of war (n)
prisoner-of-war (um)
private-sector (um)
prizefighter
prizewinner
prizewinning
pro (cf)
  pro-African (etc)
  pro forma
  progovernment
  pro-opposition
  pro rata
  proreform
  proregime
  pro-state
  pro tem
  pro tempore
  prowar
  as prefix, one word
proffer, -ed, -ing
profit-and-loss (um)
profited, -ing
profitmaking
profit-sharing (um)
program, -med, -ming
programmer
programmable
programmatic
prologue
proof of life (n)
proof-of-life (um)
proofread
proofsheet
propel, -led, -ling
propellant (n)
  propellent (adj)
prophecy (n)
  prophesy (v)
propjet
propwash
protector
protege
protester
proto (cf)
  proto-Egyptian (etc)
  rest one word
provincewide
pseudo (cf)
  pseudo-official
  pseudo-owner
  pseudo-peace-loving
  rest one word
psycho (cf)
  psycho-organic
  rest one word
publicity-conscious (um)
publicly
public-minded (um)
public-sector (um)
public-spirited (um)
public works
pullback (adj, n)
pull-down (adj)
pull down (v)
pull-in (adj, n)
pulloff (adj, n)
pull-on (adj, n)
pullout (adj, n)
pull-push (um)
pullthrough (adj, n)
pullup (adj, n)
pulse Doppler
pulsewidth
pummeled, -ing
pump house
pump-priming (adj)
pump station
purebred
pure line (biological)
purse strings
pushbutton
pushcart
pushoff (adj, n)
pushover (adj, n)
push-pull (um)
push-to-talk (adj, n)
pushup (adj, n)
putback (n, um)
putoff (n, um)
put-on (n, um)
putout (n, um)
put-up (n, um)
pyro (cf)
  all one word

Q

Q-boat
Q-fever
quadri (cf)
  quadri-invariant
  rest one word
quality control (adj, n)
quality-of-life (um)
quandary
quarreled, -ing
quarterback
quarter-cut (um)
quarterdeck
quartermaster
quartermaster general
quarter-miler
quarter-phase (um)
quarterstaff

quasi (cf)
  quasi-judicial
  quasi-military
  all hyphenated
queue, queued, queuing
quick-change (um, v)
quick-drawn (um, v)
quickfreeze (um, v)
quicklime
quick-reaction (adj)
quick-response (adj)
quicksand
quickset
quicksilver
quickstep
quick time
quick-witted (um)
quid pro quo(s)
quisling
quixotic
quonset hut
Quran

R

rabble-rouser
racecourse
racehorse
racetrack
racket (all meanings)
radar cross section
radar-imaging (um)
radarscope
radar tracking
radio (cf)
  radio amplifier
  radio antenna
  radio channel
  radio communication(s)
  radio control
  radioelectronic
  radio engineer
  radio engineering
  radiofrequency
  radioisotope
  radio link
  radio navigation
  radio range
  radio receiver
  radio-relay
  radio set
  radio station
  radiotelegraph
  radiotelephone
  radio transmitter
  radio tube
  radio wave
  rest two words
radiumtherapy
radius, radii
radix, radixes
ragtag
railborne
railcar
railguard
railhead
rail line
rail-mobile (um)
rail net
railroad
rail shed
railsplitter
rail spur
rail train
railway
railyard
rainbow
raincheck
raincoat
raindrop
rainfall
rainforest
rainmaking
rainproof
rainshower
rainspout
rainstorm
rainwash
rainwater
raison(s) d'être
Ramadan
ramjet
ramrod
ramshackle
rangefinder
rangehead
rank and file (n)
rank-and-file (adj)
rapid fire
rapid-reaction (um)
rapid transit
rappel, -led, -ling
rapporteur
rapprochement
rare-earth (um)
ratable
rate-cutting (um)
rate-fixing (um)
ratepayer
rate-raising (um)
ratesetting
rat-infested (um)
rat race
rattlesnake
rattrap
raveled, -ing
rawboned
rawhide
razor-sharp (um)
razzle-dazzle
raykom
rayon
re (pref)
  re-cover (cover again)
  re-create (create again)
  re-cross-examination
  redirect
  reengineer
  reentry
  reequip
  reevaluate
  reexport
  re-form (form again)
  re-ice
  reignite
  re-ink
  reman
  re-present (present again)
  reprocess
  re-redirect
  rest one word
reachback (adj, n)
read ahead
reading room
readme file
readout (n)
read-through (adj, n)
ready-built (um)
readymade
ready reference

real estate
real-time (um)
real time (n)
real-world (um)
rear-area (um)
rear end
rear-guard (um)
rearmost
rear service
rear services area
rearview (um)
rebel, -led, -ling
reconnaissance
reconnoiter
recordbreaker
recordbreaking
recordkeeping
recordmaking
recti (cf)
all one word
recto (cf)
all one word
recyclable
red carpet
redeye
red-haired (um)
redhanded
redhead(ed)
red-hot (um)
red line (literal)
redline (nonliteral)
redtape (nonliteral)
reduced-observable (adj, n)
refer, -red, -ring
referable
referendum, referendums
refueled, -ing
refusenik
regionwide
regime protection
reinforce
releasability
religio (cf)
all one word
remodeler
remote control (adj, n)
remote-controlled (adj)
remote-sensing (um)
renaissance
rent-free
repair shop
repairway
reparable
repellant (n)
repellent (adj)
representative at large
representative-elect
requester
research study
research worker
resino (cf)
all one word
responder (electronics)
rest home
restroom
résumé
retro (cf)
retrofire
retrofit
retro-ocular
retro-operative
retrorocket
rest one word
reveled, -er, -ing
reverse-engineer (v)
reverse-engineering
rheo (cf)
all one word
rhino (cf)
all one word
rhizo (cf)
all one word
rhod(o) (cf)
all one word
rhomb(o) (cf)
all one word
ricefield
ricegrowing
riceland
rice water
ridge line
ridgetop
rifleshot
right-angle (um, v)
right-angled (um)
right away
right-click (n, v)
right field
right-hand (adj)
right-handed (um)
rightmost
right-of-way
right-to-work (adj)
rightwing (adj)
right wing (n)
rightwinger
rig-up (adj, n)
rim-deep (um)
rimfire
rimlock
ringbolt
ring-in (adj, n)
ringlead (v)
ringleader
ring-off (adj, n)
ring-shaped (um)
ringside
ringtone
ring-up (adj, n)
ringworm
riot control
ripcord
ripsaw
riptide
rip-up (adj, n)
risque
rivaled, -ing
riverbank
riverbed
riverborne
river bottom
river-crossing (um)
riverflow
river-formed (um)
riverfront
riverhead
riverine
riverside
roadblock
roadbound (um)
roadbuilding
roadhead
roadhog
roadmap
road-mobile (um)
road scraper
road show
roadside
road-test (v)
roadway
road-weary (um)
rockbottom (nonliteral)
rock-climbing (um)

rockfall (n)
rockfill
rockpile
rockslide
rock wool
rod-shaped (um)
roentgen
roentgeno (cf)
all one word
rollabout (adj, n)
rollback (adj, n)
rollcall
roll-fed (v)
rolling-stock (adj)
roll-off (adj, n)
roll-on (adj, n)
roll-on/roll-off (adj, n)
rollout (adj, n)
rollout-to-launch (um)
rollover (adj, n)
rolltop
rollup (adj, n)
roman candle
roman numeral
roman type
roofgarden
rooftop
root-cutting (um)
roothold
rootstock
ropewalk
roughcast (um, v)
rough-cut (um)
roughhewn
roughhouse
roughing-in (um)
rough-legged (um)
roughshod
rough-sketch (v)
roundabout (adj, n)
round-faced (um)
roundhead
round-made (um)
roundnose (tool)
roundout (adj, n)
roundrobin (petition)
roundtable (panel)
round-the-clock (um)
round-topped
round trip (adj, n)
roundup (adj, n)
round up (v)
rowboat
rubberband
rubber-lined (um)
rubber plant
rubber-set (um)
rubberstamp (nonliteral)
rubdown (adj, n)
ruble
rulemaking
rule of law (n)
rule-of-law (um)
rule of thumb
ruling-party (adj)
rumormonger
runabout (n, um)
runaround (adj, n)
runaway (adj, n)
runback (n, um)
runby (n)
rundown (n, um)
run-in (adj, n)
run in (v)
runner(s)-up
running mate
runoff (n, um)
run-on (adj, n)
runout (n, um)
runthrough (n, um)
runup (n, um)
run up (v)
runway
runway-penetrator (um)
rush hour
Russo (cf)
Russo-Chinese (etc)
rest one word
rust-brown (um)
rustproofing
rust-resistant (um)
rust-stained (um)

S

saccharin (n)
saccharine (adj)
saccharo (cf)
all one word
sackcloth
sacro (cf)
all one word
saddlebag
saddlesore
safe-conduct (adj, n)
safecracker
safecracking
safe-deposit (adj)
safeguard
safehaven
safehold
safehouse
safekeeping
sailboat
sailcloth
sailmaking
salable
salesclerk
salesmanship
salespeople
salesperson
sales tax
salt-cured (um)
saltpan
saltpeter
saltpond
saltshaker
saltwater
saltworks
salvo(s)
samizdat
sanatorium, sanatoriums
sandaled, -ing
sandbag
sandbank
sandbar
sandblast
sandblown
sand-buried (um)
sand-cast (um, v)
sand dune
sandglass
sandhill
sandlot
sandpaper
sandpit
sandspit
sandstorm
sandtable
sandy-bottomed (um)
sangfroid
sanitarium, sanitariums
sans serif

sarco (cf)
all one word
satellite-borne (um)
savable
savanna
save-all (adj, n)
savior
sawdust
sawmill
sawtooth
saw-toothed (um)
say-nothing (adj, n)
say-so (n)
S-bend
S-brake
scaleback (adj, n)
scaledown (adj, n)
scaleup (n)
scale up (v)
scalloped, -ing
scandalmongering
scapegoat
scarecrow
scaremonger
scar-faced (um)
scenesetter
schizo (cf)
all one word
school-age (um)
schoolbag
school board
schoolbook
schoolboy
schoolbus
schoolchildren
schoolday
schoolgirl
schoolroom
schoolteacher
but high school teacher
school-trained (um)
schoolwork
schoolyard
school year
scientifico (cf)
all one word
scoreboard
scorecard
scorekeeping
scoresheet
scout car
scrapbook
scrap heap
scrap iron
scrap paper
scratch pad
scratch test
screen name
screenplay
screensaver
screenshot
screenwriter
screwcap
screw-driven (um)
screwdriver
screwhead
screwjack
screw propeller
screw-threaded (um)
screw-turned (um)
screw wheel
scroll bar
scrollwheel
scrubland
scuttlebutt
sea base
sea-based (um)
seabeach
seabed
seaboard
seaborne
seacoast
seacraft
seadrome
seafaring
seafloor
seafood
seafront
seagoing
seakeeping
sea lane
sea level
sealift
sea lines of
communication
sea lion
seam-welded (um)
seance
seaplane
seaport
seapower
seaquake
search and rescue
searchlight
searchplane
seascape
seashell
seashore
seasick
seaside
seatbelt
sea test
sea time (clock)
seawall
seaward
seawater
seaway
sea wing
seaworthiness
seaworthy
second-best
second-class (um)
second-degree (um)
second-generation (um)
second-guess (v)
second-half (adj)
secondhand (adj, adv)
second in command
second-largest (adj)
secondline (adj)
secondmost
second-most-powerful
second-quarter (adj)
second-ranking (um)
second-rate (um)
second-rater
secretary general
secretary-generalship
secretaryship
secretary-treasurer
secret service
secret society
seedbed
seesaw
seismo (cf)
all one word
self (cf)
self-centered
as reflexive pref, use hyphen
self-defense
selfhood
selfless

self-motivated
selfness
self-propelled
selfsame
self-trained
selloff (adj, n)
sellout (adj, n)
semi (pref)
semiannual
semiarid
semi-armor-piercing
semiautomatic
semi-Christian (etc)
semidesert
semi-idleness
semi-indirect
semi-independent
semi-land-mobile
semiofficial
semitrailer
semi-winter-hardy
rest one word
sendoff (adj, n)
sendout (adj, n)
seniormost
senso (cf)
all one word
septi (cf)
all one word
serious-minded (um)
service-connected (um)
serviceman
servicemember
service life
servicewide
servoamplifier
servocontrol
servomechanism
servomotor
servosystem
sesqui (cf)
all one word
set-aside (n, um)
setback (n, um)
set back (v)
setdown (n, um)
set down (v)
set-in (n, um)
set in (v)
setoff (n, um)
set off (v)
set-on (n, um)
setout (n, um)
setpiece
setscrew
settler
set-to (n, um)
setup (n, um)
set up (v)
sevenfold
seven-up (n)
severalfold
sewage (waste)
sewerage (drain system)
shadowbox
shadowboxing
shadowgraph
shadow line
shakedown (adj, n)
shake down (v)
shakeout (adj, n)
shake out (v)
shakeup (adj, n)
shake up (v)
shallow-draft (um)
shamefaced
shameworthy
shantytown
shaped-charge (adj)
shapeup (adj, n)
sharecropper
shareholder
sharia
sharia council
sharia court
sharia law
sharp-angled (um)
sharp-cut (um)
sharp-edged (um)
sharpshooter
sharpshooting
sharp-witted (um)
shaykh
sheep farm
sheepherder
sheepherding
sheepland
sheepshearing
sheepskin
sheetrock
shelf life
shelf plate
shellback
shellburst
shellfire
shellfish
shell game
shellhole
shell-like
shellproof
shellshocked
shelter half
shield-shaped (um)
Shiism
Shia, Shiite (adj, n)
shinbone
shinguard
shipboard
shipborne
shipbreaker
shipbroker
shipbuilder
shipbuilding
ship-day
shipload
shipowner
ship-rigged (um)
shipshape
shipside
shipwreck(ed)
shipyard
shirtband
shirtwaist
shock wave
shoehorn
shoelace
shoestring
shoo-in
shootdown (adj, n)
shoot down (v)
shootoff (adj, n)
shootout
shopkeeping
shoplifter
shoplifting
shop-made (um)
shopowner
shoptalk
shopwindow
shopworn
shore-based (um)
shore boat
shoreland

shore leave
shoreline
shoreside
shortchange (v)
short circuit (n)
short-circuit (v)
short-circuited (adj)
shortcoming
shortcut
shortfall
shorthand (writing)
short-handed (adj)
short-lived (um)
short-range (adj)
shortrun (adj)
short run (n)
shortsighted
shortstop
short-term (adj)
short-to-long (adj)
short ton
shortwave (radio)
shotgun
shotput
shoulder-high (um)
shoveled, -ing
showboat
showboating
showcase
showdown
showman
showoff (adj, n)
showpiece
showplace
showstopper
showthrough (printing) (adj, n)
showup (adj, n)
shredout (n, um)
shriveled, -ing
shura
shutaway (n, um)
shutdown (n, um)
shuteye (adj, n)
shut-in (n, um)
shutoff (n, um)
shutout (n, um)
shuttlecock
sic
sickbay
sickbed
sick leave
sicklist
sidearms
sideband
sideburns
sidecar
side-cut (um)
side effect
sidehill
sidekick
sidelap
side light (literal)
sidelight (nonliteral)
side line (literal)
sideline (nonliteral)
sidenote
sideplate
side road
sidesaddle
sideshow
sideslip
sidesplitting
sidestep
sideswipe
sidetrack
sidetrip
sidewalk
sideward
sideways
sidewinder
sightread
sightreading
sightseeing
signaled, -ing
signalman
signal-processing (um)
signal tower
sign-in (adj, n)
sign in (v)
signoff (adj, n)
sign-on (adj, n)
sign-out (adj, n)
sign out (v)
signpost
signup (adj, n)
sign up (v)
silk screen
silkworm
silo-based (um)
silver-backed (um)
silver-haired (um)
sliverplate
silver-plated (um)
silverpoint (drawing)
silver-tongued (um)
silverware
simple-minded (um)
simulcast
sine qua non(s)
single-breasted (um)
single-decker
single-edged (um)
singlehanded
single-loader
single-minded (um)
single-mindedly (adv)
single-mindedness (n)
single-phase (um)
single-seater
single-track (adj)
single-use (um)
singsong
sinkhole
Sino-Japanese (etc)
siphon
sirocco(s)
S-iron
sister-in-law
sitdown (adj, n)
site map
sit-in (adj, n)
situp (adj, n)
six-cylinder (um)
sixfold
six-ply (um)
six-shooter
six-wheeler
sizable
sizeup (adj, n)
skeptic
ski, skis
skillful
skill set
skindeep
skinflint
skipjack
skullcap
sky-blue (um)
sky-high (um)
skyjack
skyjacker
skylight
skyline
skyrocket
skyscape
skyscraper

skyward
skywave
skywriting
slab-sided (um)
slapdash
slapdown (adj, n)
slaphappy
slapstick
slaveholding
slaveowner
slave trade
Slavo-Hungarian (etc)
sledgehammer
sleepwalking
sleetstorm
slideknot
slide rule
slideshow
slingshot
slipcase
slipcover
slipknot
slip-on (adj, n)
slip proof (printing)
slipproof
slipring
slipsheet
slipshod
slipstream
slip-up (adj, n)
slipway
slowdown (adj, n)
slow-footed (um)
slowgoing (adj)
slow-motion (adj)
slow time
slowup (adj, n)
slow-witted (um)
sluice gate
slumdweller
slumlord
small arms (n)
small-arms (adj)
small-boat (adj)
small business
small businessman
small-caliber (um)
smallpox
small-scale (adj)
smalltalk
smalltown (adj)
small-unit (adj)
smart aleck
smart-alecky (adj)
smart card
smartphone
smart set
smashup (adj, n)
smear culture
smoke-blinded (um)
smokebomb
smoke-dried (um)
smoke-filled (um)
smokepot
smokeproof
smokescreen
smokestack
smolder
smoothbore
smooth-tongued (um)
smooth-working (um)
snackbar
snail mail
snail-paced
snail's pace
snakebite
snake-bitten (um)
snakepit
snap-on (adj, n)
snapout (adj, n)
snapshot
snap-up (um)
sniveled, -ing
snowball
snowbank
snowblind
snow blindness
snow-blocked (um)
snowblower
snowcapped
snowclad (um)
snow cover
snow-covered (um)
snowdrift
snowfall
snowflake
snowline
snowmelt
snow-melting (um)
snowmobile
snowpack
snowplow
snowscape
snowshoe
snowstorm
snowsuit
snow-topped (um)
snow-white (um)
so-and-so
soapbox
soap opera
sober-minded (um)
sob story
so-called (um)
social-networking (adj)
social network (n)
social work
social worker
socio (cf)
  socio-official
  socioeconomic
  rest one word
sod house
softball
soft-boiled (um)
soft coal
softcopy
soft goods
softhearted
soft-pedal (v)
soft-power (um)
soft sell (n)
soft-sell (adj, v)
soft-shelled (um)
soft-soap (nonliteral) (v)
soft-soaped
soft-spoken (um)
soiree
solid-propellant (adj)
solid-state (adj)
somebody
someday
somehow
someone (anyone)
  some one (distributive)
someplace (adv)
something
sometime (adj, adv)
some time (n)
sometimes (adv)
somewhat
somewhere
son-in-law

sonobuoy
soon-to-be (um)
sore point
sorry-looking (um)
so-seeming (um)
so-so
soul-searching (um)
sound-absorbing (um)
sound field
soundingboard
sound-minded (um)
soundoff (adj, n)
soundproof
soundtrack
sound wave
sourfaced
sour grapes
southbound
south-central
southeast
southeast-bound
south end
southernmost
southgoing
southpaw
south side
south-sider
south-southeast
south-southwest
southward
southwest
soybean
space age
space-based (um)
spacebar
spaceborne
spacecraft
spaceflight
space key
space launch
space mine
space plane
spaceship
space station
space suit
space-time
space tracking (adj, n)
space walk
spam
spammer
Spanish-Arab
Spanish-born (um)
Spanish-speaking (um)
spare-parts (um)
spare room
spark plug (literal)
sparkplug (nonliteral)
spearhead
spear phishing
spear-shaped (um)
special forces
special-interest (um)
special operations
special-purpose (um)
specter
spectra (cf)
  all one word
spectrum, spectra
speechwriter
speechwriting
speedboat
speedtrap
speedup (adj, n)
speed up (v)
speed writing
spellbinding
spellbound
spell-check (v)
spell-checker (n)
spendthrift
spent-fuel (adj)
Spetsnaz
spheno (cf)
  spheno-occipital
  rest one word
spider web (n)
spiderweb (um, v)
spillover (adj, n)
spill over (v)
spillway
spinoff (adj, n)
spin off (v)
spinup (adj, n)
spin up (v)
spiraled, -ing
spirituous (liquor)
spitfire
splashdown (adj, n)
splash down (v)
split second
splitup (n, um)
spoilsport
spokesman
spokesperson
spokeswoman
spoon-fed (um)
spoon-shaped (um)
sportsmanlike
spot check (n)
spot-check (v)
spot-checked (um)
spotwelded (um)
spray-washed (um)
spread-eagle (adj, v)
spreadout (n, um)
spread-set (v)
spreadsheet
springboard
spring fever
springhead
springtime
spur line
spyglass
spyhole
spyware
square-bottomed (um)
square-built (um)
square deal
square-headed
square meter
square-rigged (um)
square root
square-set (um)
squeeze-in (adj, n)
squeezeout (adj, n)
squeeze play
S-ray
S-shaped
stackup (adj, n)
stadium, stadiums
staff member
stagecoach
stagehand
stage-manage
stage-managing
stage-struck (um)
staging area
stainless steel
staircase
stairstep
stakeout (n)
stalemate
stalking horse

stanch (v) (stop)
  staunch (adj) (steadfast)
standalone (adj, n)
standard bearer
standard gauge (adj, n)
standard operating procedure
standard time
standby (adj, n)
stand by (v)
standdown (adj, n)
stand down (v)
standfast (adj, n)
stand fast (v)
stand-in (adj, n)
stand in (v)
standoff (adj, n)
stand off (v)
standoffish
standout (adj, n)
stand out (v)
standpat (adj, n)
stand pat (v)
standpipe
standpoint
standstill (adj, n)
stand still (v)
standup (adj, n)
stand up (v)
starboard
star-spangled (um)
startup (adj, n)
start up (v)
state-aided
statehood
state of the art (n)
state-of-the-art (um)
state of the union
state of war (n)
state-of-war (adj)
state-owned
stateroom
state's evidence
stateside
statesman
statesmanlike
stateswoman
statewide
stationary (fixed)
  stationery (paper)
station house
stationmaster
station wagon
stato (cf)
  all one word
statue (sculpture)
  stature (height)
  statute (law)
status quo
statute book
statute mile
stay-at-home (adj, n)
staysail
steamboat
steam-driven (um)
steam engine
steamer-borne (um)
steamer line
steamfitter
steamfitting
steam heat
steamline
steampipe
steamplant
steampower (n)
steam powerplant
steam-propelled (um)
steamroll (v)
steamroller (adj, n)
steamship
steam table
steel-cased (um)
steelclad
steel-framed (um)
steel-hard (um)
steelhead
steelmaking
steel mill
steelplate
steel-producing (um)
steel wool
steelworker
steelworks
steep-rising (um)
steep-walled (um)
stempost
stenciled, -ing
stenciler
steno (cf)
  all one word
stepchild (etc)
stepdown (adj, n)
step-in (adj, n)
stepladder
stepoff (adj, n)
step-on (adj, n)
stepped-up (um)
steppingstone
step-up (adj, n)
step up (v)
stereo (cf)
  all one word
sterncastle
stern-faced (um)
stern-looking (um)
sternmost
sternpost
stern wheel
stern-wheeler
stick-in-the-mud (nonliteral)
stickout (adj, n)
stickpin
stick-to-it-iveness
stickup (adj, n)
stiff-backed (um)
stiff-necked (um)
stillborn
still life
still-lingering (um) (etc)
still-to-be- (um)
stimulus, stimuli
stir-up (adj, n)
stockholder
stockholding
stock-in-trade
stockpile
stockpot
stock-still (um)
stocktaking
stockyard
stokehold
stone-cold (um)
stonecutter
stonecutting
stone-dead (um)
stone-deaf (um)
stonehand (printing)
stonemason
stone proof (printing)
stone wall (n)
stonewall (nonliteral) (v)
stopclock
stopcock
stopgap

stoplight
stopoff (adj, n)
stop off (v)
stopover (adj, n)
stop over (v)
stopwatch
storage room
storefront
storm-swept (um)
storm-tossed (um)
storyboard
storyteller
storytelling
storywriting
stouthearted
stoutheartedness
stovepipe
stowaway (adj, n)
stow away (v)
slowdown (adj, n)
straightaway
straight-backed (um)
straight-cut (um)
straightedge
straight-edged (um)
straight face
straight-faced (um)
straightforward
straight-legged (um)
straight line
straight-lined (um)
straight-out (n, um)
straight time
straight-up (um)
straitjacket
straitlaced
stranglehold
S-trap
straphanger
strap-on (adj)
strap on (v)
strato (cf)
all one word
stratum, strata
straw-built (um)
strawhat
strawman (nonliteral)
straw-roofed (um)
straw vote
streambank
streambed
streamflow
streamline
streamlined
streamside
streetcar
streetsmart
streetwise
stretchout (adj, n)
strikebreaker
strike-in (adj, n)
strikeout (adj, n)
strikeover (adj, n)
strip mine (n)
strip-mine (v)
striptease
strong-arm (adj, v)
strongback (nautical)
strong-backed (um)
strongbox
stronghearted
stronghold
strongman (nonliteral)
strong-minded (um)
strongpoint (military fortification)
strong point (personal forte)
strong-willed (um)
stuckup (n, um)
stumblingblock
stylebook
style guide
style manual
style sheet
stylus, styluses
sub (pref)
subarctic
subbalance
subbasement
subcommittee
sub-Himalayan (etc)
submachinegun
subpolar
subpoena, -ed
sub rosa
Sub-Saharan Africa (n)
Sub-Saharan African (um)
subspecies
substandard
sub-subcommittee
subsystem
rest one word
subject matter expert
subject-object
subter (pref)
all one word
succor
such-and-such
suck-in (adj, n)
sugar beet
sugarcane
sugar-coat (v)
sugar-coated (um)
sugar-cured (um)
sugar mill
sulfa (cf)
all one word
sulfo (cf)
all one word
sulfon (cf)
all one word
sulfureted, -ing
summer school
summertime (season)
sun-baked (um)
sunbath (n)
sunbathe (v)
sunbeam
sunblind
sun blindness
sunburn
sunburst
sun-cured (um)
sundial
sundown
sun-dried (um)
sun-dry (v)
sunglare
sunglass
sunglow
sunlamp
sunlit
Sunna
Sunni
sunray
sunrise
sunset
sunshade
sunshine
sunspot
sunstroke
sun-synchronous (um)
suntan

sunup
super (pref)
  supercharger
  super-Christian (etc)
  superegoist
  superhigh frequency (n)
  superhigh-frequency (um)
  superhighway
  supermarket
  superpower
  supersensitive
  super-superlative
  rest one word
supra (pref)
  supra-auditory
  supra-Christian (etc)
  supranational
  rest one word
sur (pref)
  all one word
sure-fire (um)
sure-footed (um)
sure thing
surface ship (adj, n)
surface water
surveil, -led, -ling
surveillance
survivability
swallow-tailed (um)
swandive
swansong
swapout (adj, n)
swayback (adj, n)
sway-backed (um)
sway-brace (v)
swearing-in (adj, n)
sweatband
sweepback (aviation) (adj, n)
sweepforward (aviation) (adj, n)
sweepstakes
sweepthrough (adj, n)
sweptback (n, um)
sweptforward (n, um)
sweptwing (n, um)
swift-footed (um)
swift-running (um)
swimsuit
swingbar
swing shift
swingstock
swingwing
switchback
switchblade
switchboard
switch box
switchgear
switchplate
switch tower
switchyard
swiveled, -ing
swiveleye
swivel-eyed (um)
swordplay
S-wrench
syllabus, syllabuses
symposium,
  symposiums
sylvan
syn (pref)
  all one word
sync, -ed, -ing
synchrocyclotron
synchromesh
synchrotron
synopsis, synopses
Syro-Arabian (etc)
syrup

T

tableau, tableaus
tablecloth
table-shaped (um)
tablespoon
tabletop
taboo
tailfirst
tailgate
tail-heavy (um)
tailhook
tailormade
tailpipe
tailrace
tailspin
tailstock
tail-up (n, um)
tailwheel
tailwind
take-all (n)
takeaway (adj, n)
take away (v)
takedown (adj, n)
take down (v)
take-home (adj, n)
take home (v)
take-in (adj, n)
take in (v)
takeoff (adj, n)
take off (v)
takeout (adj, n)
take out (v)
takeover (adj, n)
take over (v)
takeup (adj, n)
take up (v)
taleteller
talking-to (n)
tally board
tally room
tank car
tankship
tapdance
tape-record (v)
tape-tied (um)
taproot
tap-tap
targeted, -ing
targetable
targeter
tariff-protected (um)
tarp-covered (um)
tar-paved (um)
tarpot
task force
taskmaster
tasseled, -ing
tattletale
tax collector
tax dodger
tax-exempt (um)
tax form
tax-free (um)
taxi, taxis
taxibus
taxicab
taxied, -ing
taximeter
taxistand
taxpayer
taxpaying
tax-supported (um)
T-beam
T-boat
T-bone

tea-colored (um)
teacup
teakettle
teammate
teamplay
teamplayer
teamwork
teapot
teardown (adj, n)
tear down (v)
teardrop
teargas, -sed (v)
tear gas (adj, n)
tearline
tear-off (adj, n)
tear-out (adj, n)
tear-stained (um)
teaspoon
technique
techno (pref)
  technobabble
  technological
  technophobia
  all one word
technology transfer
teenage (adj)
teenager
teetotaler
tele (cf)
  telecommunication(s)
  all one word
teleo (cf)
  all one word
telltale
telo (cf)
  all one word
temporo (cf)
  temporo-occipital
  rest one word
tender boat
tenderfoot
tender-footed (um)
tenfold
tenpenny (nail)
tentpole
terminus, termini
terra cotta
terra firma
territorywide
test bed
test-fire (v)
test-fly (v)
test-launch (v)
test range
tete-a-tete
tetra (cf)
  all one word
text (n, v)
textbook
text box
text-message (adj, v)
text message (n)
thanksgiving (gratitude)
thatch-roofed (um)
theater
theatergoing
theaterwide
thenceforth
then-ruling (um)
then-troublesome (um) (etc)
theo (cf)
  all one word
theologico (cf)
  all one word
thereabout(s)
thereafter
thereat
thereby
therefore
therefrom
therein
thereof
thereon
thereto
thereupon
therewith
thermo (cf)
  all one word
thesis, theses
thickset (adj, n)
thickskinned
thick-wooded (um)
thick-woven (um)
think tank
thinset (um)
thinskinned
third-class (adj)
third-country (adj)
third-degree (adj)
third-generation (adj)
thirdhand (adj, adv)
third-party (adj)
third-quarter (adj)
third-rate (um)
third-rater
thoroughbred
thoroughfare
thoroughgoing
thought-out (um)
thought-provoking (um)
thousandfold
thralldom
threadbare
threadworn
three-cornered (um)
three-dimensional (adj)
  or 3-D
threefold
three-in-hand
threepenny (nail)
three-piece (um)
three-ply (um)
threescore
threesome
three-square
threshold
throughout
throughput
through road
throwaway (adj, n)
throw away (v)
throwback (adj, n)
throw back (v)
throw-in (adj, n)
throw line
throwoff (adj, n)
throw-on (adj, n)
throwout (adj, n)
throw weight (adj, n)
thrust-pound
thumb drive
thumbmark
thumb-marked (um)
thumbnail
thumbprint
thumbscrew
thumbs-up (adj, n)
thumbtack
thunderbolt
thunderclap
thundercloud
thunderhead
thundershower

thunderstorm
thunderstruck
tick-borne
ticketholder
ticket seller
tidal wave
tideland
tidemark
tidetable
tidewater
tide-worn (um)
tieback (n)
tied, tying
tiedown (adj, n)
tie-in (adj, n)
tie in (v)
tie-on (adj, n)
tiepin
tieup (adj, n)
tie up (v)
tightfisted
tight-fitting (um)
tightlipped
tightrope
tightwad
tightwire
timberjack
timberland
time being
time bomb
timecard
timeclock
time-consuming (um)
timeframe
time-honored (um)
timekeep (v)
timekeeper
timekilling
timelag
timeline
timelock
timeout (adj, n)
timepiece
timesaver
timesaving
time-sensitive (um)
timeserver
time-share
timesheet
timeshift
timeshifting
timeslip
timeslot
timespan
time-stamp (v)
timetable
time-urgent (um)
timewaster
timewasting
timeworn
tinfoil
tinhorn
tin-lined (um)
tinpan
tinplate
tin-plated (um)
tin-roofed (um)
tintype
tip-in (adj, n)
tipoff (adj, n)
tip off (v)
tiptoe
tiptop
tip-up (um)
tiresome
T-iron
titer
tit for tat
titleholder
title-holding (um)
title page
title-winning (um)
T-jetty
to-and-fro
tobacco(s)
tobacco-growing (um)
today
to-do (adj, n)
toecap
toehold
toe-in (adj, n)
toenail
toeprint
toilsome
tollbar
tollbooth
toll bridge
tollgate
toll line
toll road
tolltaker
tommygun
tomorrow
tone box
tone-deaf (um)
toneup (adj, n)
tongue-lash (v)
tongue lashing
tonguetied
tongue twister
tongue-twisting (um)
tonight
ton-kilometer
ton-mile
ton-mileage
toolbag
toolbar
tool-grinding (um)
toolkit
toolshed
toolshop
toolsmith
tool steel
toolwork
toothache
tooth and nail
toothbrush
toothmark
toothpaste
toothpick
toothsome
top brass
topcoat
top cover
top-down (um)
top drawer
topflight (adj)
tophat
top-hatted (um)
topheavy
topknot
top-level (adj)
topline
topliner
topmark
topmast
topmost
topnotch (nonliteral)
topo (cf)
all one word
top-quality (adj)
topsail
top-secret (um)

topside (nautical)
topsoil
topsy-turvy
torchlight
torchlit
tormenter
torpedo boat
torpedo mine
torpedo room
torpedo tube
torquemeter
torsion bar (adj, n)
tossup (adj, n)
totaled, -ing
touch and go
touchback (adj, n)
touchdown (adj, n)
touchpad
touchscreen
touchup (adj, n)
tough-minded (um)
tough-skinned (um)
toward
towaway
toweled, -ing
towhead
to wit
townhall
town meeting
township
townside
townspeople
towpath
towrope
trackball
track-mobile (um)
trackside
tractor-trailer
trade board
tradecraft
trade-in (adj, n)
trade in (v)
trademark
trade name
tradeoff (adj, n)
trade off (v)
trade school
tradesman
tradespeople
tradesperson
tradeswoman
trade union
trade unionism
trade unionist
trade wind
trafficking
T-rail
trailblazer
trailblazing
trailbreaker
trail-marked (um)
trailside
trainborne
traincrew
training camp
training ship
trainload
trainmaster
trainwreck
trainyard
tramcar
tramline
trammeled, -ing
tram rail
tramway
tranquilize(r)
tranquillity
trans (pref)
  transalpine
  transatlantic
  trans-Canadian (etc)
  transcontinental
  transisthmian
  transpacific
  transship
  rest one word
trans fat
transfer, -red, -ring
transferable
transferal
transferor
transited, -ing
transit time
transmit, -ted, -ting
transmittal
transponder (electronics)
transporter-erector-launcher
transshipment
trapdoor
trapshoot
traveled, -ing
traveler
travelog
travel-worn (um)
trawlnet
treasure-filled (um)
treasure house
treasure-laden (um)
treatybound
treatybreaking
treatymaking
treaty-sealed (um)
tree-clad (um)
tree line
tree-lined (um)
tree-ripe (um)
treetop
tree trunk
trellis-covered (um)
trenchcoat
trenchfoot
trenchmouth
tri (cf)
  tricolor
  trifocal
  tri-iodide
  tri-ply (um)
  tripartite
  tripresidency
  triservice
  tristate
  rest one word
tribesman
tribespeople
trim-cut (um)
trinitro (cf)
  all one word
triphammer
triple-edged (um)
triplefold
triple play
tripwire
Trojan horse
trolley
trolley bus
trolley car
trolley line
trooplift
troopship
troop train
troop training (adj, n)
tropo (cf)
  all one word

trouble-free (um)
troublemaking
troubleshooter
troublesome
trouble spot
troweled, -ing
truckborne
truckdriver
but delivery truck driver (etc)
truckline
truckload
truckstop
truck tractor
truck trailer
true-blue (um)
trunkline
try-on (adj, n)
tryout (adj, n)
T-scale (score)
T-shape (n)
T-shaped
T-shirt
T-square
tube-fed
tube-feed (v)
tugboat
tug of war
tuneup (adj, n)
tune up (v)
tunnel-boring (um)
tunneled, -ing
tunneler
tunnel-shaped (um)
turbo (cf)
turbo-ramjet (um)
rest one word
turf-covered (um)
Turko-Greek (etc)
turnabout (adj, n)
turn about (v)
turnaround (adj, n)
turn around (v)
turnback (adj, n)
turn back (v)
turnbuckle
turncoat
turndown (adj, n)
turn down (v)
turned-back (um)
turned-down (um)
turned-in (um)
turned-on (um)
turned-out (um)
turned-over (um)
turn-in (adj, n)
turn in (v)
turnkey
turnoff (adj, n)
turn off (v)
turnout (adj, n)
turn out (v)
turnover (adj, n)
turn over (v)
turnpike
turnscrew
turnstile
turntable
turn-to (n)
turnup (adj, n)
turret deck
turret gun
turret ship
turtleback
twelve-fold
twenty-first
twentyfold
twenty-one
twice-born (um)
twice-told (um)
twice-reviewed
twin boat
twin-engine (adj)
twin-jet (adj)
twin-motor (um)
twin-screw (adj)
two-a-day (um)
two-faced (um)
twofold
two-handed (um)
twopenny (nail)
two-piece (adj)
two-ply (um)
two-seater
two-sided (um)
twosome
two-striper
two-thirds
two-up (adj, n)
two-way (adj)
two-wheeler
typecase
typecast
typeface
typescript
typeset
typesetting
typewrite (v)
typewriting
typo (cf)
all one word
tyro

U

U-boat
U-cut
Uighur
ulama (variant of *ulema*)
ulema
ultra (pref)
ultra-ambitious
ultra-atomic
ultra-English (etc)
ultrahigh frequency (n)
ultrahigh-frequency (adj)
ultrahigh-performance (adj)
ultrahigh-speed (adj)
ultrahigh-voltage (adj)
ultra-large-scale (adj)
ultralow frequency (n)
ultralow-frequency (adj)
ultraorthodox
ultrarightwing
ultrashortwave
ultrasonic
ultraviolet
rest one word
U-magnet
un (pref)
un-American (etc)
unapparent
uncalled-for (um)
undamaged
unheard-of (um)
un-ionized (um)
unMIRVed
unself-conscious
unsent-for (um)
unthought-of (um)
rest one word
under (pref)
underage (deficit) (n)
underage (too young) (adj, n)
under contract

undercover (um)
under cultivation (being tilled)
undercultivation (insufficient)
underdog
undergo
underground
under-ice (adj)
undermanned
under oath
under obligation
under orders
underpriced
under secretary
under-secretaryship
understrength (adj)
under suspicion
under-the-counter (um)
under way
underway (ship)
under-ice (um)
as prefix, one word
uni (cf)
unicellular
unilateral
uni-univalent
rest one word
union-made (um)
union shop
up-anchor (um, v)
up-and-comer
up-and-coming (um)
up and up
upbeat
upcountry
update
up-echelon (adj)
upend (v)
up-front (um)
upgrade
upgradient
upkeep
uplift
up-link
upload
uppercase (printing)
upper-class (um)
upperclassman
uppercrust (adj, n)
uppercut
upper hand
upper-income (um)
upper-middle-class (um)
uppermost
uprange
uprate
upriver
upstairs
upstate
upstream
upswing
uptake
uptight (adj, n)
up-to-date
uptown
uptrend
upturn
upward
upwind
U-rail
used-car (um)
user-friendly (um)
user name
U-shaped
utopia
U-tube
U-turn

V

value added (n)
value-added (um)
valve-grinding (um)
vandriver
vanguard
vanpool
vapor-filled (um)
variable rate mortgage
vaseline
vase-shaped (um)
V-connection
V-curve
vector-borne
V-E Day
veld
V-engine
venthole
venturi tube
veranda
verbatim
vermilion
vertebra, vertebrae
very-high frequency (n)
very-high-frequency (adj)
very-low frequency (n)
very-low-frequency (adj)
vice admiral
vice-admiralty
vice chairman
vice-chairmanship
vice chancellor
vice consul
vice-consulate
vice-consulship
vice governor
vice-governorship
vice minister
vice-ministry
vice-presidency
vice president
vice-president-elect
but Vice President-elect Smith
vice-presidential
vice regent
vice versa
videotape (n, v)
videotape recording
video teleconference
viewfinder
viewpoint
vine-covered (um)
virtuoso, virtuosos
visa, -ed, -ing
vis-a-vis
V-neck
voicemail
voltammeter
volt-ampere
voltmeter
voltohmmeter
volt-second
vortex, vortexes
votable
vote-casting (um)
votegetter
vote-getting (um)
vote-rigging (um)
vowbreaker
V-shaped
V-type
vulcanize

W

wage earner
wage-earning (um)
wage scale
waistband
waistbelt
waistcoat
waist-deep (um)
waist-high (um)
wait-and-see (adj)
waiting list
waiting period
waiting room
waitlist
wake-up (adj, n)
walkaround (adj, n)
walkaway (adj, n)
walkie-talkie
walk-in (adj, n)
walk in (v)
walk-on (adj, n)
walk on (v)
walkout (adj, n)
walk out (v)
walkthrough (adj, n)
walkup (adj, n)
walk up (v)
walled-in (um)
walled-up (um)
wall-like
wallpaper
wallplate
war-disabled (um)
wardship
warfare
warfighting
war game (n)
war-game (adj, v)
wargaming (n)
warhead
warhorse (nonliteral)
warlike
war-made (um)
warmaking
warmblooded
warmed-over (um)
warmonger
warmup (adj, n)
warm up (v)
warpath
war plan
warranter
  warrantor (law)
warranty
warship
war-swept (um)
wartime
war-torn
war-waging (um)
war-wearied (um)
war weariness
war-weary (um)
war-winning (um)
washbasin
washcloth
washdown (adj, n)
washed-out (um)
washed-up (um)
wash-in (adj, n)
washoff (adj, n)
washout (adj, n)
wash out (v)
washrag
washstand
washup (adj, n)
wash up (v)
wastebasket
wastepaper
wastewater
watchband
watchdog
watchlist
watchman
watchstander
watchtower
watchword
waterbag
water-bearing (um)
water body
waterborne
watercolor
water-colored (um)
water-cool (v)
water-cooled (um)
watercourse
watercraft
water-cut
waterdrop
waterfall
water-filled (um)
waterflood
waterflow
waterfog
water-free (um)
waterfront
watergate
waterhead
waterhole
water-laden (um)
water level
waterline
water-lined (um)
waterlog
waterlogged
water main
waterman
watermark (as on
  stationery)
  but high water mark
waterpower
waterproof
waterproofing
water-rot (v)
water-sharing (um)
watershed
waterside
waterski
water-soak (v)
water-soaked (um)
water-soluble (um)
waterspout
waterstain
water table
watertight
waterwall
waterway
waterworks
watt-hour
wattmeter
watt-second
wave band
wave-cut (um)
waveform
waveguide
wave-lashed (um)
wavelength
wavemeter
wave-on (adj, n)
waveoff (adj, n)
wave-swept (um)
wave-worn (um)
wayback (adj, n)
wayfarer

waylaid
waylay
waymark
waypoint
wayside
way station
way-up (adj, n)
weak-eyed (um)
weak-kneed (um)
weakminded
weaponmaking
weapon system(s)
weasel-worded (um)
weatherbeaten
weather-borne (um)
weathercock
weather-hardened (um)
weather map
weather-marked (um)
weatherproof
weatherproofing
weatherstrip
weatherworn
web browser
webcam
webcast
web-crawling
web feed
web forum
web hosting
webinar
webmaster
webpage
web server
website
weed-choked (um)
weekday
weekend
weeklong (adj)
week-old (adj)
weighbridge
weigh-in (adj, n)
welder
well-armed (um)
well-being (n)
well-born (adj)
well-bred (adj)
well-clad (um)
well-deserving (um)
well-doer
well-doing (n, um)
well-drained (um)
well-drilling (um)
well-equipped (um)
well field
well-grown (um)
wellhead
wellhouse
well-informed (um)
well-kept (adj)
well-known (um)
well-looking (um)
well-off (adj)
well-positioned (um)
well-read (adj)
well-regarded (um)
well-set-up (um)
well-settled (um)
well-spoken (adj)
wellspring
well-thought-of (um)
well-thought-out (um)
well-to-do (adj)
well-trained (um)
well-wisher
well-wishing (um)
well-worn (um)
well water (adj, n)
welterweight
W-engine
westbound
west-central (um)
west end
western (direction)
Western (relating to countries of the West)
Western-government-backed (um)
West European (um)
Western Europe (n)
westernmost
west-facing (um)
westgoing
west-northwest
west-southwest
westward
wetland
wharf boat
wharfhand
wharfside
whatever
whatnot (n)
whatsoever
wheatfield
wheatgrower
wheatland
wheat-rich (um)
wheatstalk
wheelbarrow
wheelbase
wheelbox
wheelchair
wheel-cut (um)
wheeler-dealer
wheelhouse
wheelpower
wheelspin
wheelwright
whenever
when-issued (um)
whereabouts
whereafter
whereas
whereat
whereby
wherefore
wherefrom
wherein
whereof
whereon
whereto
whereunder
whereupon
wherever
wherewith
wherewithal
whet (stimulate)
whichever
whimsy
whipcord
whip hand
whiplash
whipsaw
whirlpool
whirlwind
whiskey(s)
whistlestop
white book (diplomatic)
whitecap (nonliteral)
whitecoat (n)
white-collar (nonliteral) (adj)
white flag
white goods

white-hot (um)
white lie
whiteout (um, v)
white paper
whitewash
whoever
wholehearted
wholesale
wholesome
whomsoever
whosoever
wide-angle (adj)
wide-area (adj)
wide-awake (adj)
wideband (adj)
wide-body (adj, n)
wide gauge
widemouthed
wide-open (um)
wide-ranging (um)
wide-scale (adj)
widespread
wide-spreading (um)
widthwise
WiFi
wiki
wild card
wildcat
wild-eyed (um)
wildfire
wild land
wildlife
wild man
willful
willpower
willy-nilly
windbag
windblown
windborne
windbreak
windbreaker
windchill
winddown (n, um)
wind down (v)
windfall
windflow
windjammer
windlass
windmill
window-cleaning (um)
window-dressing (um)
windowpane
windowshopping
windowsill
windpipe
windpower
windproof
windrow
windscreen
windshield
windsock
windspeed
windstop
windstorm
windstream
windswept
windup (n, um)
wind up (v)
windward
windworn
wing flap
wingless
wing-loading (um)
wingnut
wing-shaped (um)
wingspan
wingspread
wingtip
wingwalker
wingwall
winterkill
winterproof
winter-sown (um)
wintertime
winter wheat
wire-caged (um)
wire-cut (um)
wirecutter
wire-haired (um)
wireless
wire line
wirephoto
wirepuller
wiretap
wire-wound (um)
wisecrack
wise guy
wise man
wishbone
witch hunt
withdraw
withhold
within
without
withstand
woeful
wolfhound
wolfpack
woodblock
wood-built (um)
woodcut
wooden-hulled (um)
woodland
wood-lined (um)
woodlot
wood-paneled (um)
woodpile
wood-planing (um)
woodprint
woodpulp
woodshed
woodside
woodstock
wood-walled (um)
woodwork
woodworking
woolen
woolgatherer
woolgathering
wool-lined (um)
woolly
woolshearing
woolworking
wordbook
wordbuilding
word combination
wordcraft
word-for-word (adj, adv)
wordlist
word-of-mouth (adj, adv)
word of mouth (n)
word-perfect (um)
wordplay
word-processing (adj)
word processing (n)
workaday (adj, n)
workaround (adj, n)
workbench
workday
workflow
workforce
workhorse
work hour

working-class (adj)
working-level (adj)
workingman
workingwoman
workload
workman
workmanlike
workmanship
work order
workout (adj, n)
workplace
worksaving
worksheet
work shift
workshoe
workshop
worksite
workspace
workstand
workstation
workstream
worktable
worktime
workup (adj, n)
workweek
workyard
workyear
world-class (adj)
world consciousness
world line
world power
worldview
world-weary (adj)
worldwide
World Wide Web
worndown (um)
wornout (um)
worrywart
worshiped, -er, -ing
worst case
worthwhile
wraparound (adj, n)
wrap-up (adj, n)
wrap up (v)
wristband
wristbone
wristlock
wristwatch
writeback (adj, n)
write-in (adj, n)
write in (v)
writeoff (adj, n)
write off (v)
writeup (adj, n)
write up (v)
wrongdoer
wrong-ended (um)
wrong-minded (um)
wrong-thinking (um)
wrought iron
wrought-up (um)
W-shaped
W-surface
W-type

X

X-body
X-ed
X-ray
X-virus
X-shaped

Y

yardarm
yard-deep (um)
yard-long (um)
yardstick
yard-wide (um)
Y-chromosome
yearbook
yearday
yearend
year-hour (um)
yearlong (um)
year-old
year-round
yellowcake (uranium)
yellow fever
yes-man
yesteryear
Y-joint
Y-level
young-looking (um)
youth-centric (adj)
youthlike
Y-potential
Y-shaped
Y-track
Y-tube

Z

zakat
Z-bar
Z-chromosome
zeppelin
zero(s)
zero-day (adj)
zero-dimensional (um)
zero-emission (adj)
zero-gravity (um)
zero-option (um)
zero-sum (um)
zigzag
zinc-coated (um)
zinc-white (um)

APPENDIX: Metric and English Conversion Factors

Although an appendix is not an essential part of every book, the possibilities and uses of the device are many. Some kinds of material properly relegated to an appendix are explanations and elaborations that are not essential parts of the text but are helpful to a reader seeking further clarification; texts of documents, laws, and so forth, illustrating the text; and long lists, survey questionnaires, or sometimes even charts or tables. The appendix should not be a repository for raw data that the author was unable to work into the text.

—*The Chicago Manual of Style*

APPENDIX: Metric and English Conversion Factors

Conversion factors in boldface are exact. All others are approximate and are given to four significant figures.

Length/Distance

To Convert	*Multiply by*	*To Obtain*
millimeters	0.03937	inches
centimeters	0.3937	inches
meters	3.281	feet
meters	1.094	yards
kilometers	3281	feet
kilometers	0.6214	miles (statute)
kilometers	0.5400	miles (nautical)
inches	**25.4**	millimeters
inches	**2.54**	centimeters
feet	**0.3048**	meters
feet	**0.0003048**	kilometers
yards	**0.9144**	meters
miles (statute)	**1.609344**	kilometers
miles (nautical)	**1.852**	kilometers
miles (statute)	0.8690	miles (nautical)
miles (nautical)	1.151	miles (statute)

Area

To Convert	*Multiply by*	*To Obtain*
square centimeters	0.1550	square inches
square meters	10.76	square feet
square meters	1.196	square yards
square meters	0.0002471	acres
square meters	**0.0001**	hectares
square inches	**6.4516**	square centimeters
square feet	0.09290	square meters
square yards	0.8361	square meters
acres	4047	square meters
acres	0.4047	hectares
hectares	**10,000**	square meters
hectares	2.471	acres

Mass

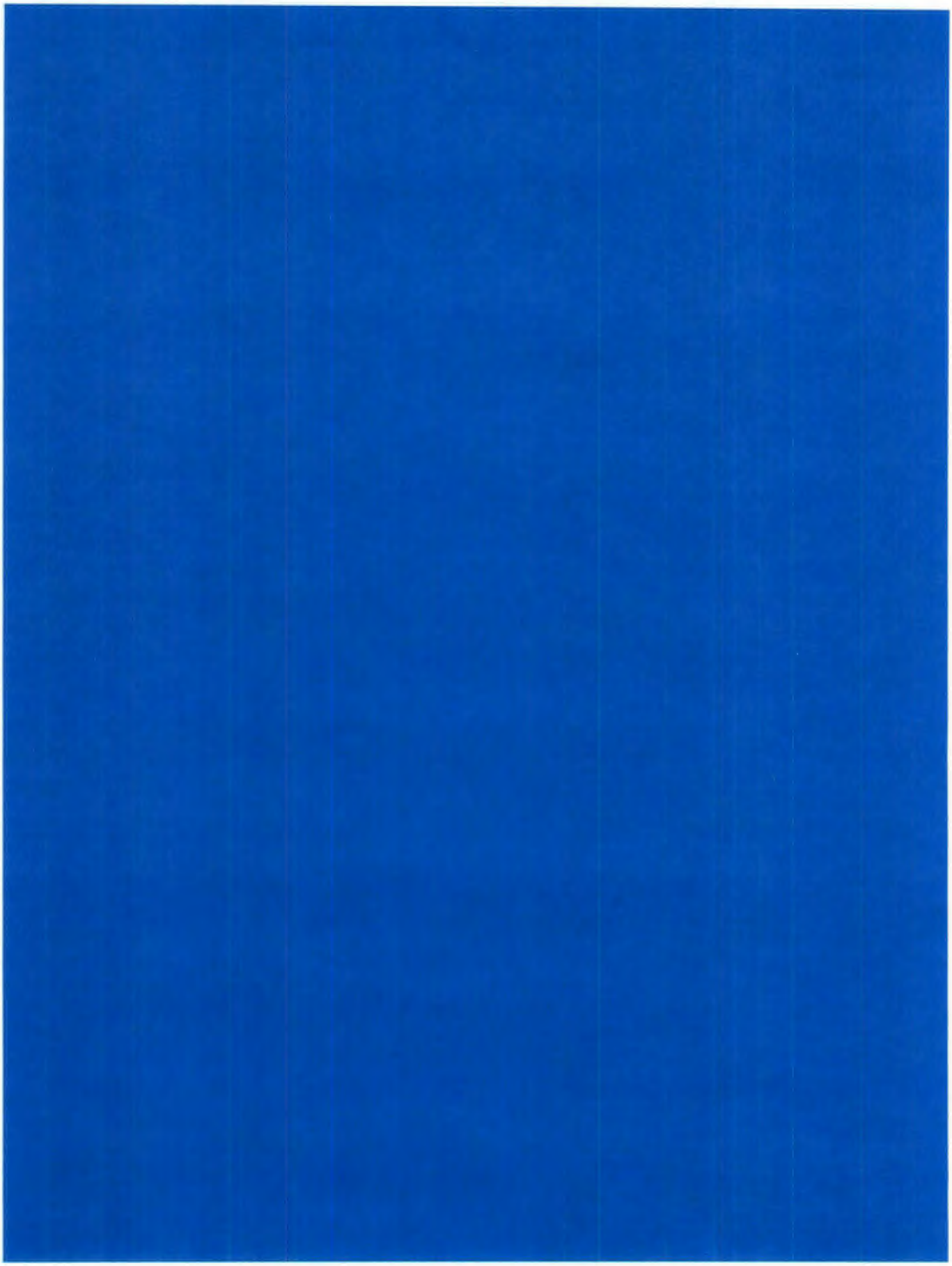
To Convert	*Multiply by*	*To Obtain*
kilograms	2.205	pounds (avoirdupois)
metric tons	1.102	short tons
metric tons	0.9842	long tons
pounds (avoirdupois)	**0.45359237**	kilograms
short tons	0.9072	metric tons
long tons	1.016	metric tons

Volume

To Convert	*Multiply by*	*To Obtain*
liters	0.2642	gallons
liters	0.008386	barrels (U.S. liquid)
liters	0.006290	barrels (POL)
liters	**0.001**	cubic meters
cubic meters	**1000**	liters
cubic meters	264.2	gallons
cubic meters	35.31	cubic feet
cubic meters	8.386	barrels (U.S. liquid)
cubic meters	6.290	barrels (POL)
cubic meters	1.308	cubic yards
gallons	3.785	liters
gallons	0.1337	cubic feet
gallons	0.03175	barrels (U.S. liquid)
gallons	0.02381	barrels (POL)
gallons	0.003785	cubic meters
cubic feet	7.481	gallons
cubic feet	0.2375	barrels (U.S. liquid)
cubic feet	0.1781	barrels (POL)
cubic feet	0.02832	cubic meters
cubic yards	0.7646	cubic meters
barrels (U.S. liquid)	119.2	liters
barrels (U.S. liquid)	**31.5**	gallons
barrels (U.S. liquid)	4.211	cubic feet
barrels (U.S. liquid)	0.1192	cubic meters
barrels (POL)	159.0	liters
barrels (POL)	**42**	gallons
barrels (POL)	5.615	cubic feet
barrels (POL)	0.1590	cubic meters

Temperature

°C = (°F – 32) ÷ 1.8
°F = (°C × 1.8) + 32



UNCLASSIFIED

DEFENSE INTELLIGENCE AGENCY

DIA Style Manual
for Intelligence Production

200 MacDill Blvd., Bldg 6000 | Washington, DC 20340-5100

UNCLASSIFIED

C05757260

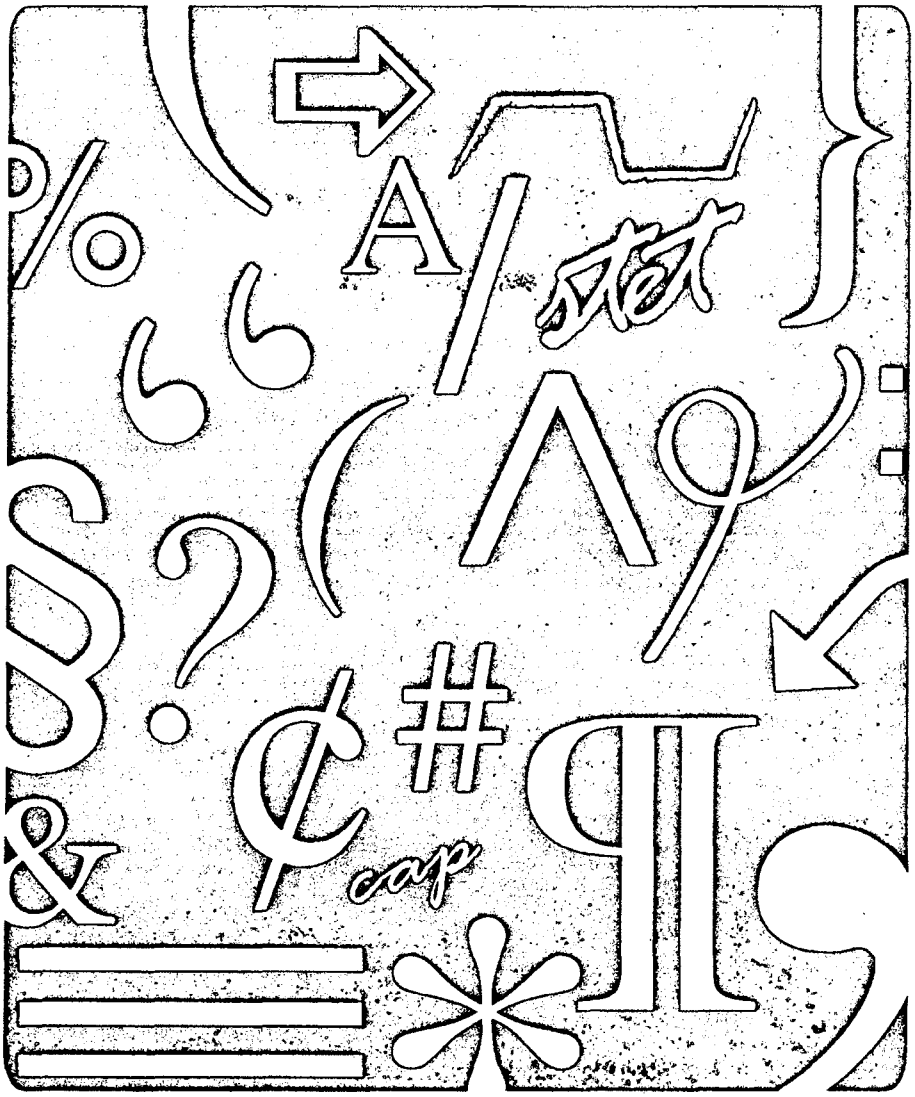
(b)(3)

DIRECTORATE OF INTELLIGENCE

STYLE MANUAL & WRITERS GUIDE

FOR INTELLIGENCE PUBLICATIONS

Eighth Edition, 2011



This style guide was prepared by the DI

APPROVED FOR RELEASE DATE: 28-Feb-2012

C05757260

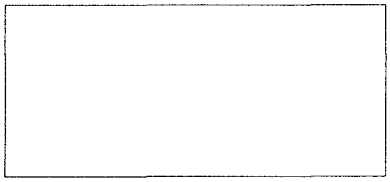
Foreword

Good intelligence depends in large measure on clear, concise writing. The information CIA gathers and the analysis it produces mean little if we cannot convey them effectively. The Directorate of Intelligence and the Agency as a whole have always understood that. Both have been home, from their earliest days, to people who enjoy writing and excel at it.

The *Style Manual and Writers Guide for Intelligence Publications* is an essential reference for the officers of our Directorate. Now in its eighth edition, it reflects an enduring commitment to the highest standards of care and precision.

This guide is designed to be helpful and convenient, sensible in organization, and logical in content. It contains, among other changes, a revised list of accepted acronyms and new tips on word usage. The world is not static. Nor is the language we employ to assess it.

In dealing with foreign policy and national security, our government has many sources of insight on which to draw. The depth of our knowledge, the strength of our thinking, and the power of our words will ensure that our customers, from policymakers to operations officers, continue to rely on the Directorate of Intelligence.



Fran Moore
Director for Intelligence

C05757260

Preface

The eighth edition of the *Style Manual and Writers Guide for Intelligence Publications* provides guidance for English usage and writing style in the Central Intelligence Agency. It incorporates most of the improvements that appeared in previous editions but returns to the organization by chapters of the earliest versions. The chapters on capitalization, numbers, abbreviations, italics, punctuation, spelling, and compound words have numerous headings and subheadings to enable users to find specific subjects quickly within the chapters themselves or through the table of contents. Further subject indexing is provided in chapter 9—the Word Watchers List—which incorporates many of the style rules in abbreviated form; it is similar to the Word Watchers Index in the fourth edition and to the overall organization of more recent editions. The manual also includes a comprehensive Spelling and Compound Words List, as have all previous editions, and an index to the entire manual.

The counsel in this guide is derived from many sources, including the works of Barzun, Bernstein, Copperud, Follett, Fowler, the Morrises, Strunk and White, Gregg, and other recognized arbiters of English usage. It also draws on the stylebooks of press services, newspapers, publishing houses, and past and present CIA offices.

A basic reference for spelling, compounding, and other instructions for all eight editions is the US Government Printing Office's *Style Manual*, the most recent edition of which was issued in 2008. The GPO's authority for spelling and compounding words is *Webster's Third New International Dictionary*, published by G. & C. Merriam Company. That dictionary or the more up-to-date abridgments of it (the latest being *Webster's 11th New Collegiate Dictionary*) are the authorities for the preferred spellings listed in this guide that were not found in the GPO manual.

This guide is for both the creators and the processors of intelligence analysis—for the writers and for the editors of their analyses. It also serves writers and processors of administrative papers. Moreover, it has been used and will continue to be used by teachers and students of writing and publications processing.

The manual is available online in both web browser (HTML) and printer-friendly (PDF) versions; limited quantities are available in hardcopy. The browser version contains active links that take users from one related issue to another; these are indicated with the standard hyperlink convention: underlined text. The browser version may be updated as needed.

C05757260

CONTENTS

FOREWORD iii

PREFACE v

1. CAPITALIZATION 1

1.1. A Few Basic Rules 1
1.2. Proper Nouns 1
1.3. Derivatives of Proper Names 2
1.4. Articles in Place Names 2
1.5. Names of Persons 2
1.5a. Particles in Personal Names, 3
1.5b. Nicknames, 3
1.6. Government Bodies 3
1.7. Military Forces 4
1.8. International Organizations 4
1.9. Diplomatic and Consular Units 4
1.10. Religious Terms 5
1.11. Titles of Religious Leaders 5
1.12. Political Parties and Similar Groups 5
1.13. Political Philosophies 5
1.14. Geographic Terms 6
1.14a. Direction, 6
1.14b. Special Geographic Groupings, 6
1.15. Nationalities, Tribes, and Other Groups of People 7
1.16. Coined Names 8
1.17. Holidays, Religious Feasts, and Historic and Other Significant Events 8
1.18. Trade Names 8
1.19. Titles of Persons 9
1.19a. Before the Name, 9
1.19b. After or in Place of the Name, 9
1.19b1. Head or Assistant Head of State or Government; Royal Heir Apparent, 10
1.19b2. Top Officials, National Government Unit; Principal Members, Legislative and Judicial Branches, 10

C05757260

1.19b3. Officers of Party Organizations in Communist Countries, 10
1.19b4. Top Officials of First-Order Subnational Administrative Divisions, 11
1.19b5. Top Officers in a Military Service, 11
1.19b6. Principal Official of an International Organization, 11
1.19b7. Principal Members of the Diplomatic Corps, 11
1.20. Publications 12
1.20a. Titles in English, 12
1.20b. Shortened Titles, 12
1.20c. Laws and Treaties, 12
1.20d. Foreign Titles, 12
1.21. Graphics, Tables, and Chapters 13
1.22. Cross-References 13
1.23. Indented Bullet or Dash Paragraphs 13
1.24. Miscellany 13
1.24a. Seasons, 13
1.24b. Major Storms, 13

2. NUMBERS 15

2.1. Basic Guidance 15
2.2. Numbers of 10 or More 15
2.3. Numbers Under 10 15
2.4. Mixes of Numbers Above and Below 10 15
2.5. Ordinal Numbers 16
2.6. Indefinite Numbers 16
2.7. Figures of 1,000 or More 16
2.8. Millions and Billions 16
2.9. Numerical Unit Modifiers 17
2.10. Possessives 17
2.11. Ranges of Numbers 17
2.11a. Below the Millions, 17
2.11b. In the Millions, 18
2.12. Numbers in Tables and Graphics and for Pages, Paragraphs, and Footnotes 18
2.13. References to Numbers as Numbers 18
2.14. Numbers in Nonliteral Sense 18
2.15. Decimals 19
2.16. Fractions 19
2.17. Mixed Numbers 19
2.18. Expressions of Value 19
2.18a. US Money, 19
2.18b. Foreign Money, 20
2.19. Percentages and Times Phrases 20
2.19a. Percentage, 20
2.19b. Times Phrases, 20

C05757260

2.20. Expressions of Time 21
2.20a. Ages of Persons, 21
2.20b. Ages of Inanimate Things, 21
2.20c. Dates, 21
2.20d. Years, 22
2.20e. Decades, 22
2.20f. Centuries, 22
2.20g. Clock Time, 23
2.20h. Other Time Expressions, 23
2.21. Units of Measure 23
2.22. Figures With Units of Measure 23
2.23. Other Number Rules 24
2.23a. Numbers Close Together, 24
2.23b. Ratios, Odds, Scores, Returns, 24
2.23c. Indefinite Expressions Using Figures, 24
2.23d. Scientific Notation, 24
Factors for Converting to Metric Units of Measure 25

3. ABBREVIATIONS 27

3.1. General Guidance 27
3.2. First Reference 27
3.3. Well-Known Abbreviations 28
3.4. Foreign Terms 28
3.5. Incomplete or Possessive References 28
3.6. Plural Forms 29
3.7. Military Ranks 29
3.8. Unusual Forms 29
3.8a. MIRVs, 29
3.8b. SALT, MBFR, INF, 30
3.9. Country Names 30
3.9a. US, UK, 30
3.9b. China, 30
3.9c. Miscellaneous Rules, 30
3.10. Titles of Persons 31
3.10a. Civil or Military, 31
3.10b. Complimentary, 31
3.11. Latin Abbreviations 31
3.12. Political Subdivisions 31
3.13. Months and Days 32
3.14. Percent 32
3.15. Units of Measure 32
3.16. Ambiguous Abbreviations 34

C05757260

4. ITALICS 35

4.1. Prominence or Emphasis 35

4.2. Titles 35

4.3. Foreign Words 35

4.3a. Familiar or Anglicized Foreign Words, 35
4.3b. Other Foreign Words, 36
4.3c. Titles of Publications, 36
4.3d. Names of Organizations, 36

4.4. Names of Craft 37

4.5. Cited Letters, Words, and Phrases 37

5. PUNCTUATION 39

5.1. General Principles 39

5.2. Apostrophe 39

5.2a. Possessives, 39
5.2a1. Words That End in an s Sound, 39
5.2a2. Words That Do Not End in an s Sound, 40
5.2a3. Compounds, 40
5.2a4. Combinations Indicating Joint Possession, 40
5.2a5. Geographic, Firm, or Organization Names or Publication Titles, 40
5.2a6. Organized Bodies That End in s, 40
5.2a7. Personal Pronouns, 41
5.2b. Possessives With Persons or Inanimate Bodies, 41
5.2c. Noun or Pronoun Preceding a Gerund, 41
5.2d. Plurals, 41

5.3. Brackets 42

5.3a. Inside Parentheses, 42
5.3b. Editorial Remarks, 42

5.4. Bullets (Ticks) 42

5.5. Colon 42

5.5a. Summaries or Expansions, 42
5.5b. Separation of Clauses, 43
5.5c. Titles and Subtitles, 43
5.5d. Ratios, 43
5.5e. Indented Material, 43

5.6. Comma 43

5.6a. For Comprehension, 43
5.6b. Separation of Coordinate Modifiers, 44
5.6c. With Nonrestrictive Words, 44
5.6d. With Contrasting Statements, 44
5.6e. Serial Comma, 44
5.6f. Compound Sentences, 45
5.6g. Numbers in the Thousands and Higher, 45
5.6h. Introductory Phrases, 45
5.6i. Title of Person and Name of Organization, 46
5.6j. Omission of a Word or Words, 46
5.6k. Before Direct Quotations, 46

C05757260

5.6l. With Geographic, Personal, or Corporate Names, 46
5.7. Dash (or Em Dash) 46
5.7a. Parenthetical Matter, 46
5.7b. Before a Final Summarizing Clause, 47
5.7c. In Place of a Bullet, 47
5.8. Ellipsis 47
5.9. En Dash 47
5.10. Exclamation Point 48
5.11. Hyphen 48
5.12. Parentheses 48
5.12a. With Comments, 48
5.12b. With Cross-References, 48
5.12c. With Numbers or Letters in a Series, 48
5.12d. With Foreign Words, 48
5.13. Period 49
5.14. Question Mark 49
5.14a. To Show Uncertainty, 49
5.14b. In a Title, 49
5.15. Quotation Marks 49
5.15a. Double Quotation Marks, 49
5.15a1. Direct Quotations, 49
5.15a2. Titles That Do Not Merit Italicization, 50
5.15a3. Selected Words or Phrases, 50
5.15b. Single Quotation Marks, 50
5.15c. Punctuation With Quotation Marks, 50
5.15d. Terms Precluding Need for Quotation Marks, 51
5.16. Semicolon 51
5.16a. Series, 51
5.16b. Compound Sentence, 51
5.16c. With Conjunctive Adverbs, 51
5.17. Slash 52
5.17a. To Show a 12-Month Period Occurring in Two Calendar Years, 52
5.17b. To Represent *Per* in Abbreviations, 52
5.17c. To Separate Alternatives, 52
5.17d. To Show Combination in Certain Instances, 52

6. SPELLING 53
6.1. General Principles 53
6.2. Preferred and Difficult Spellings 53
6.3. British Terms 53
6.4. Anglicized Foreign Words 53
6.5. Plural Forms 54
6.5a. *O* Endings, 54
6.5b. Compound Terms, 54
6.5c. Other Difficult Plurals, 54

C05757260

6.6. Endings *-yze*, *-ize*, and *-ise* 54
6.7. Endings *-sede*, *-ceed*, and *-cede* 55
6.8. Endings *-ible* and *-able* 55
6.9. Doubled Consonants 55
6.10. Indefinite Articles 55
6.10a. With Consonants and Vowels, 55
6.10b. With Initials That Begin With a Consonant Sound, 56
6.10c. With Initials That Begin With a Vowel Sound, 56
6.10d. With Acronyms, 56
6.10e. With Abbreviations That Have Variable Pronunciations, 56
6.10f. With Numerical Expressions, 56
6.11. Geographic Names 56
6.12. Names and Titles of Persons and Organizations 57
6.13. Diacritical Marks 57
6.14. Transliteration Guidance 57

7. COMPOUND WORDS 59

7.1. General Rules 59
7.1a. Separate Words, 59
7.1b. Joined or Hyphenated, 59
7.2. Solid Compounds 59
7.2a. Combinations of Nouns, 59
7.2b. Combinations of Verbs and Adverbs, 60
7.2c. Compounds Beginning With Certain Nouns, 60
7.2d. Compounds Ending With Certain Words, 60
7.2e. *Any*, *Every*, *No*, or *Some* Combined With *Body*, *Thing*, *Where*, or *One*, 60
7.2f. Self or Selves, 60
7.2g. Compass Directions, 61
7.3. Unit Modifiers 61
7.3a. Hyphenated, 61
7.3b. Unhyphenated, 61
7.3c. With Ordinal Numbers, 62
7.3d. Predicates, 62
7.3e. Comparatives and Superlatives, 62
7.3f. Adverbs Ending in *-ly*, 63
7.3g. Three-Word Modifiers, 63
7.3h. Foreign Phrases, 63
7.3i. Proper Nouns, 63
7.3j. En Dash in Proper Noun Compounds, 63
7.3k. Quotation Marks, 64
7.3l. Chemical Terms, 64
7.3m. Letter or Number Elements, 64
7.3n. Common Basic Elements, 64

C05757260

7.4. Prefixes and Suffixes 65
7.4a. Unhyphenated, 65
7.4b. Hyphenated, 65
7.4c. Doubled Vowels or Tripled Consonants, 65
7.4d. To Avoid Confusion, 65
7.4e. Duplicated Prefixes, 66
7.4f. Prefixes or Suffixes in Compounds With Capitalized Words, 66
7.4g. Unit Modifier Containing a Multiword Compound, 66
7.5. Numerical Compounds 66
7.5a. Spelled Out, 66
7.5b. Adjective Compounds With Numerical First Element, 67
7.5c. Fractions, 67
7.6. Other Compound Words 67
7.6a. Titles, 67
7.6b. Noun Compounds Containing a Prepositional Phrase, 67
7.6c. Improvised Compounds, 67
7.6d. Verb Forms of Noun Forms Written as Two Words, 67
7.6e. Single Capital Letter Plus a Noun or Participle, 68

8. SPELLING AND COMPOUND WORDS LIST 69

9. WORD WATCHERS LIST 145
9.1. What's in This Chapter? 145
9.2. Who Are the Word Watchers? 145
9.3. Some Helpful Precepts 145

INDEX 177

1. CAPITALIZATION

1.1. A Few Basic Rules

When deciding whether or not to capitalize a word, follow the old maxim: "When in doubt, don't." Do not, for example, capitalize the first letters of the words explaining an uppercase abbreviation unless the term abbreviated is a proper name.

LAN (local area network) USPS (United States Postal Service)

The capitalization of abbreviations themselves is covered in chapter 3. One general rule is to avoid the all-uppercase formulations common in the military for weapon designators (use Scud, *not* SCUD) and for exercises. Lowercase is preferred for acronyms (such as comsat), but be aware of exceptions (notably NATO and SIGINT).

This chapter covers other areas in which uncertainty about capitalization may arise. We assume all users of this manual know that the first letter of a sentence should be capitalized, but a writer may be unsure about what to do if a number begins a sentence—spell it out, even if it is a number normally written as a figure (see sections 2.2 and 2.14), or rephrase the sentence (for example, change *1988 was a significant year for her* to *The year 1988 was significant for her*).

1.2. Proper Nouns

Generally, capitalize a common noun when it forms part of a proper name but not when it is used alone as a substitute for the name of the place or thing or when it becomes separated from the rest of the name by an intervening word or phrase. Certain well-known short forms of specific proper names, however, are exceptions to this rule.

Social Democratic Party, the party
Catholic Church, the church
Harvard University, the university
Quebec Province, Province of Quebec; the province; Quebec, Canada's separatist province
but
the British Commonwealth, the Commonwealth
the Panama (or Suez) Canal, the Canal
the Golan Heights, the Heights
the Persian Gulf, the Gulf
the Horn of Africa, the Horn
the Korean Peninsula, the Peninsula
the Olympic Games, the Games, the Olympics, the Winter (or Summer) Olympics
the Taiwan Strait, the Strait, cross-Strait

A noun common to two or more proper names is capitalized in the plural form when preceded by the proper adjectives in those names.

Montgomery and Prince George's Counties
Harvard and Yale Universities
Red and Black Seas

1.3. Derivatives of Proper Names

Do not capitalize derivatives of proper names used with acquired independent meanings.

anglicized words	italic type
bohemian lifestyle	molotov cocktail
byzantine organization	pasteurized milk
diesel engine	roman type
draconian measures	venetian blinds
but	
Castroite sympathies	Islamization
degrees Celsius	Marxist, Leninist
degrees Fahrenheit	Morse code
Francophone	pulsed Doppler effect
Gaullist policies	Sandinista

1.4. Articles in Place Names

Capitalize the definite article, or its foreign language equivalent, when it is part of an official name. When such a name is used adjectively, an uncapitalized *the* might be used and, despite the redundancy, would precede a capitalized non-English equivalent.

The Bahamas	the Bahamas Tourist Office
El Salvador	the El Salvador situation
The Gambia	the Gambia mapping project
The Hague	the Second Hague Conference

For some country names the definite article is used but is not capitalized because it is not part of the official name (for example, the United Kingdom, the United States, the Vatican) or because the convention has been to use a lowercase *t*, as in:

the Philippines (The proper adjective is Philippine; the people are Filipinos.)

the Netherlands (The proper adjective is Dutch or Netherlands; the people are called the Dutch or the Netherlanders.)[1]

Do not omit the article before a country name in a series if the article is used when the name stands alone.

the United States and *the* Netherlands (*not* the United States and Netherlands)

There is no *the* in *Congo, Seychelles, Sudan,* or *Western Sahara* (*the Sahara* refers to the desert).

1.5. Names of Persons

The spelling of personal names in CIA writing follows transliteration systems generally agreed upon by US Government agencies, unless officials have stated a preference for variant spellings of their names.

[1]Guidance on country names and the nouns and adjectives denoting nationality is given in *The World Factbook,* produced by the CIA and available online [redacted] or in hardcopy from the US Government Printing Office or the National Technical Information Service.

C05757260

1.5a. Particles in Personal Names

In certain personal names, particles such as *al, d', da, de, del, della, den, di, du, l', la, le, van,* and *von* are usually not capitalized unless they begin a sentence.

. . . achieved independence while de Gaulle was President. De Gaulle, however, did . . .

. . . was opposed by the den Uyl government. Den Uyl's policy differed from that of van Agt . . .

In some cases, particles are often dropped when the family name alone is used.

Iraqi Prime Minister Nuri al-Maliki; *but* Maliki stated . . .

Anglicized versions of foreign names vary in the matter of retaining or dropping particles and in the use of capital letters.

1.5b. Nicknames

When a nickname or a descriptive expression replaces a person's first name, capitalize it. If the nickname falls between a person's first and last names, capitalize it and enclose it in quotation marks.

the late revolutionary Che Guevara

Israeli Prime Minister Binyamin "Bibi" Netanyahu

1.6. Government Bodies

Capitalize both the full proper name of a national government body and its shortened form.

the British Parliament, the Parliament, Parliament

the Argentine Congress, the Congress; the Tunisian Chamber of Deputies, the Chamber; *but* the Argentine legislature, the Tunisian legislature, the legislature

the French Senate, the Senate, the upper house

the Cuban Council of Ministers, the Council of Ministers

the British Cabinet, the Cabinet, the Conservative Cabinet, Cabinet member; *but* the Labor shadow cabinet (This example does not apply across the board, especially if the term *cabinet* is used in reference to a body whose formal title does not resemble the English word. If in doubt, use lowercase.)

the Ministry of Economy, the Ministry; a proposed ministry of energy, the proposed ministry, various ministries, several ministries, the economic ministries, the foreign service, the civil service; *but* a Secret Service agent, the Intelligence Community

the Supreme Court

the Central Bank, the Bank

the US Government, the Federal Government (US only; also Federal employee, etc.), the French Government, the French and Italian Governments, the Government of France, the Governments of France and Italy; *but* the government (shortened form always lowercased), the Brown government, the Tory government, the European governments; the executive, legislative, and judicial branches of government; the Obama administration, the administration; the Calderon administration

For a subnational government body, capitalize only the full proper name and avoid shortened forms that might be confused with national equivalents.

the Maryland House of Delegates, the state legislature (*not* the House); the Quebec Parliament, the provincial parliament; the Jerusalem Municipal Council, the council, municipal councils all over Israel

C05757260

1.7. Military Forces

Capitalize the full proper name (or reasonable translations and approximations thereof) of a military force or service as well as the shortened form of that name.

the US Army, the Army
the Egyptian Army, the Army, an Army engineer
Chilean Army, division, or regiment level
the Russian Navy, the Navy, a Navy officer
the People's Liberation Army, the Army, the PLA
the Royal Air Force, the Air Force, the RAF, an Air Force pilot
The Israel Defense Forces, the IDF (*not* the Forces)

This rule does not apply to individual units in the matter of capitalizing the shortened form of the name.

the 3rd Army, the army	the 27th Division, the division
the 7th Fleet, the fleet	The 1028th Brigade, the brigade

Nor does it apply to a reference, other than a proper name, to military services as a group, to a general reference to one kind of service in the plural form, or to any general reference.

the Russian armed forces
the British military establishment
the infantry, the artillery, the submarine forces
US naval forces
the East European air forces
the navies of the Mediterranean NATO members
a navy (army, air force) to be proud of
Russian-supplied air force (naval, ground force) equipment
but
the German and French Air Forces, the Greek and Turkish Navies (specific services referred to by proper names in plural form)

1.8. International Organizations

Capitalize both the full proper name and the shortened form of an international organization and its subelements.

the UN General Assembly, the Assembly
the World Bank, the Bank

1.9. Diplomatic and Consular Units

Capitalize the full or shortened name of a specific embassy, mission, or consulate, but not those words when used generally.

the British Embassy, the Embassy
the British Embassies in Paris and Rome
the US Mission, a spokesman for the Mission
the French Consulate, the Consulate, during Consulate hours

C05757260

but
reports from African embassies
employees skilled in consulate operations
members of diplomatic missions
US embassy guards in the African states

1.10. Religious Terms

Capitalize the names of religions, religious bodies, and the terms for their adherents and writings.

the Bible	Islam	Methodist Church (*but* the church)
Biblical text	a Jew	a Muslim
Catholicism	Judaism	a Protestant
Christianity	the Koran	the Talmud
an Episcopalian	Koranic law	Talmudic scholar

Do not capitalize such terms when they are used in a nonreligious sense.

This style guide, which should be the bible for intelligence writers, attempts to be catholic in its approach to English usage.

1.11. Titles of Religious Leaders

The terms for and titles of religious leaders are capitalized preceding a name and occasionally following the name or when used alone.

Bishop Tutu, the Bishop; *but* appointment of a bishop. (In a political context simply use the name for subsequent reference: *meetings between Tutu and the authorities.*)

Pope Benedict XVI . . . the Pope; *but* election of a pope; future popes; papal, papacy

1.12. Political Parties and Similar Groups

Capitalize the full or shortened name of a political party but not the word *party* standing alone.

the Chinese Communist Party, the party, the CCP
the Italian Socialist Party, the Socialist Party, the PSI
the Christian Democratic Union, the party, the CDU
the British (or Australian or New Zealand) Labor[2] Party, the party, Labor's chances in the election

1.13. Political Philosophies

Capitalize words referring to members of organized parties but not words referring to political philosophies and their adherents.

a Socialist, a Liberal, a Laborite, a Conservative, a Tory, a Social Christian, a Christian Socialist, a Communist (all party members)

A British socialist is likely to be a member of the Labor Party.

The socialist parties of Western Europe include the British Labor Party and the German Social Democratic Party.

[2]Note that, even in proper names, we always use the American spelling for English words spelled differently in the British Commonwealth.

C05757260

Not all liberal European parties have the word *liberal* in their names.

a communist opposition party called the People's Party

The communist[3] countries today are China, Cuba, North Korea, Laos, and Vietnam.

Eurocommunism

but

Christian Democracy, Christian Democrat, Christian Democratic (both the *C* and the *D* are uppercased)

1.14. Geographic Terms

1.14a. Direction

A geographic term used to denote mere direction or position on the earth[4] is not a proper name and is not capitalized.

north, south, east, west, south-central, far north

northerly, eastward, western, far western

east coast, southern France, central Europe

the polar region, polar icecap; the Arctic Circle, the Arctic region (lowercase as descriptive adjective: arctic clothing, conditions, etc.)

Latitude (zero to 90 degrees) and longitude (zero to 180 degrees) continue to describe position on the earth, but context and space limitations allow for differences in format beyond the traditional symbols used to designate degrees, minutes, and seconds (when needed).

Either 55° 45' north latitude, 37° 35' east longitude or 55 45 north latitude, 37 35 east longitude may be used in the text of a paper, as long as use is consistent.

The format 55 45 N 37 35 E is preferred on a map or graphic.

Six digits set solid (554500N) is preferred in a table or matrix with latitude as a header and seven digits set solid (0373500E) with longitude as a header.

1.14b. Special Geographic Groupings

Geographic terms often become part of a proper name for a definite region, geographic feature, or political grouping and are capitalized.

the West, the East, Western countries, East-West dialogue

the Western Hemisphere, the North Pole, the Caribbean Basin, the San Andreas Fault, the Equator

the Continent (meaning continental Europe)

but

the coterminous, or contiguous, United States (meaning the first 48 states) and the continental United States (meaning the first 48 states plus Alaska)

Greater Moscow, Metropolitan Moscow (*but* Moscow metropolitan area)

North and South, capitalized, are often used as abbreviations of the two Koreas or to refer, respectively, to the developed and developing countries, as in "the North-South dialogue."

[3]Communist countries and parties often call themselves "Socialist" or "socialist." In paraphrasing communist statements, put such references in quotation marks. The same applies to *imperialism* and *imperialist* (and to *anti-imperialism* and *anti-imperialist*), which are terms communists use in describing their opponents.

[4]Capitalize *Earth*, *Moon*, and *Sun* only in extraterrestrial contexts. Earth orbit, Moon landing, orbit the Sun; *but* earth's topography, moonlight, sunshine.

C05757260

Some capitalized geographic terms are used to divide the world into groups of countries for purposes of intelligence reporting.

Middle East or Middle Eastern (preferred over Near East, Mideast)
North Africa (occasionally North-Central Africa)
Sub-Saharan Africa
West Africa, East Africa
but
black Africa, southern Africa (South Africa refers only to the republic)
South Asia (sometimes Southwest or Southeast Asia)
East Asia (preferred over Far East)
Oceania (note also North or South Pacific, the Pacific Rim, *but* eastern, western Pacific)
Western Europe, West European
Eastern Europe, East European
Latin America
Middle America
Central America

Some countries fall into more than one category, depending on the context. In some reports, countries logically belonging in a geographic category are grouped separately by some other criterion, such as membership in NATO. The Arab states are often treated as a group in papers on the Middle East. And the terms Middle America and Central America are not synonymous. Be careful, therefore, to explain any such groupings or any deviations from normal geographic categories in a prefatory note or a footnote.

1.15. Nationalities, Tribes, and Other Groups of People

Capitalize the names of racial, linguistic, tribal, ethnic, and religious groupings such as the following. Check *The World Factbook* for specific groupings in a country.

African-American	Colored[6]	Mongol
Amerindian	Creole	Mongoloid
Arab	Indian	Mormon
Aryan	Indo-Chinese	Negro, Negroid
Asian	Indo-European	Nordic
Bedouin (ethnic population)[5]	Jewish	Oriental
Berber	KwaZulu	Polynesian
Bushman	Magyar	Pygmy
Caucasian	Malay	Walloon
Caucasoid	Maori	Zulu

Do not capitalize the following terms based on racial origin, size, and local or other usage. (Some terms of this sort can have offensive connotations and, of course, should never be used.)

aborigine, aboriginal	bushman (general sense)	overseas (as in overseas Chinese)
animist	mestizo	pygmy (general sense)
bedouin (nomadic lifestyle)	mulatto	white
black		

[5]See *bedouin* in chapter 9.

[6]The capitalized term *Colored* is used in reporting on South Africa and (historically) other white-populated areas of Africa. Except in the way it is spelled here (Colored, *not* Coloured) the term conforms to local usage.

C05757260

1.16. Coined Names

A coined name or short form for a military, economic, political, or other grouping is capitalized.

the Alliance, Allied (adjective), and Allies in reference to NATO (uppercasing is needed for clarity; otherwise lowercase)
the Contras
the European Union, the Union, the EU member states
the Free World (use *noncommunist world* in all but historical contexts)
the Group of Eight (G-8)
the Intelligence Community
Nonaligned Movement
Six-Party Talks
but
Camp David accords, Geneva accords, Helsinki accords, Amman accords, Dayton accords, Paris accords
the establishment
fifth column
the occupied territories
Persian Gulf states, the Gulf states
stealth bomber, stealth technology, counterstealth

1.17. Holidays, Religious Feasts, and Historic and Other Significant Events

Many of the examples in this section need capitalization to give them the emphasis or prominence essential to understanding their meaning, especially when they are used out of context.

the Cold War
the Cultural Revolution
D-Day
the Depression
the Feast of the Passover
the Great Leap Forward
the Holocaust
Independence Day
New Year's Day
the October War[7]
the 23rd Party Congress
the Prague Spring
Ramadan
the Renaissance
the Six-Day War[7]
World War II

1.18. Trade Names

Trade names (such as *Velcro, Kleenex,* or *Teflon*) should be capitalized or replaced with a generic term.

air-cushion vehicle (ACV) or hover craft (unless it is a real Hovercraft)
fiberglass (unless it is Owens-Corning Fiberglas)
oxytetracycline (unless the physician specifically prescribed Terramycin)
a photocopy (unless it is known to be a Xerox copy or a Kodak copy)
tracked vehicles (unless they have genuine Caterpillar treads)
a canning jar (unless it is a real Ball or Mason jar)

[7]Capitalize the *W* in *October War* or *Six-Day War* because either term as a whole is a distinguishing coined name, but *1973 Middle East war* or *1967 Arab-Israeli war* is distinguishing enough without the capital *W*. Avoid *Yom Kippur war*, which is slangy. Do not uppercase the *w* in *Korean war*, which was "undeclared"; the same logic applies to *Vietnam war* and *Falklands war*, and a similar convention (if not logic) to *Iran-Iraq war*.

C05757260

Sometimes an acceptable replacement is hard to find. For example, "Ping-Pong diplomacy," the catchphrase once used to describe the exchange of sport and cultural delegations between the United States and China, was probably not entirely accurate even with the trade name uppercased but was certainly preferable to "table tennis diplomacy." Usage eventually pushes bestselling trademarks into the generic language—and in some cases, such as jeep, the generic preceded the trade name. For instance, the following once-capitalized names are now listed in the Merriam-Webster dictionary in lowercase: *celluloid, deep-freeze, dry ice, photostat,* and *zipper.*

1.19. Titles of Persons

1.19a. Before the Name

Capitalize any valid title (or short form of it) immediately preceding a person's name. The plural form of the title preceding more than one name is also capitalized. In front of a title, the prefix *ex* (followed by a hyphen or an en dash) and the adjectives *former* and *then* (neither followed by a hyphen) are not capitalized; neither are the suffixes *designate* and *elect.* Do not confuse a mere description with a title by capitalizing it.

President Sarkozy, Acting President Ghimpu, Defense Minister Barak, First Deputy Premier Shuvalov

Prime Ministers Cameron and Cowen

former Prime Minister Callaghan, then Defense Minister Sharon, ex-President Lopez, ex-Foreign Minister Gromyko, President-elect Salinas, Permanent Representative-designate to the UN Dauth

the late PLO Chairman Arafat (*but* former PLO leader Arafat)

Chief Justice Ramirez, Associate Justice Alberti, Justices Alberti and Ramirez

Bishop Jones, Chairman Smith, Prof. Mary Brown, Professor Brown

Mayor Black, Assistant Principal Jones

First Lady Margarita Zavala de Calderon

party Secretary Brown (uppercase any party top leader's formal title preceding the name), ruling-party Chairman Jones

vice-presidential candidate Gonzalez, pianist Ray Charles

Avoid preceding a name with more than one title. Use the more important one first, and then the other later in the text if necessary or if desired for variation.

onetime Minister of Defense Yazov . . . Marshal Yazov

the late President Pinochet . . . General Pinochet

1.19b. After or in Place of the Name

Generally, a title standing alone is lowercased unless it refers to an incumbent—present or past (but not future). To indicate preeminence or distinction in certain instances, capitalize a common-noun title or shortened title when it follows the name of a person or is used alone in reference to the person to whom the title belongs or belonged. The plural form of such a title is also capitalized as appropriate. So is the word *Acting* if it is a valid part of a capitalized title. Do not capitalize such a title when it refers to the office rather than the individual or when it is used generally.

1.19b1. Head or Assistant Head of State or Government[8]; Royal Heir Apparent

Nicolas Sarkozy, President of France
the President
the Prime Ministers of Italy and France
the Premier-designate, the Vice President–elect
the woman designated as Premier, the man elected Vice President
the former Vice President, an ex-President
the then Secretary General
the Queen of England, the Prince of Wales, the Crown Prince
the former King
but
aspire to be president
destined to be king
a younger head of state
the new chief of state
note also
the First Lady, the First Family (*but* the royal family)

1.19b2. Top Officials, National Government Unit; Principal Members, Legislative and Judicial Branches

David Wright Miliband, Secretary of State for Foreign and Commonwealth Affairs
the Acting Foreign Secretary
the Minister of Foreign Affairs, the Foreign Minister
the Deputy Minister of Foreign Affairs
Minister Without Portfolio
the Chief Justice
the President of the Senate, the President
the Speaker of the House, the Speaker
Bank of Canada Governor Carney
but
a deputy minister of foreign affairs, a first deputy premier
shadow minister, shadow chancellor of the Exchequer, shadow foreign secretary
conferred with cabinet ministers and secretaries of state
the senator, the representative, the congressman, the assemblyman
the member of Parliament (*never* parliamentarian—see chapter 9)
a deputy in the National Assembly
an associate justice
chairman of the Foreign Affairs Committee
the deputy chairman

1.19b3. Officers of Party Organizations in Communist Countries

Cuban Communist Party First Secretary Fidel Castro
Hu Jintao, General Secretary of the Communist Party of China
party General Secretary Hu
the General Secretary, the party General Secretary

[8]Capitalize *Presidential* in any reference to a present or past US President (Presidential vetoes, decisions, proclamations, etc.) but not a reference to a future one (the 2012 presidential election) or to the office generally (presidential powers under the US Constitution). Outside the US context, lowercase *presidential* and other adjectives referring generally to government offices unless they are part of an official name or title: Presidential (Ministerial, Vice-Presidential) Liaison Office(r); *but* presidential action, ambassadorial courtesies, prime-ministerial caliber.

but
Politburo member Ricardo Alarcon
party secretary Juan Almeida
the party secretary responsible for agriculture
a full member or candidate member of the party Politburo
the general secretary of the Italian Communist Party

1.19b4. Top Officials of First-Order Subnational Administrative Divisions

Jean Charest, Premier of Quebec
the Vice Premier of Quebec
the Governor of Connecticut
the Lieutenant Governor of Virginia
the Acting Governor of Maryland
the Armenian Republic First Secretary
but
a capable premier
several state governors
the mayor of Philadelphia

1.19b5. Top Officers in a Military Service

Commander in Chief of the Chilean Army; the Commander in Chief
Chief of Staff, Brazilian Air Force
Deputy Chief of Staff
but
the quartermaster
commander, IV Corps
chief, G-2 (Intelligence Branch), Army Headquarters
the general (military title standing alone not capitalized)

1.19b6. Principal Official of an International Organization

the Secretary General
the current Secretaries General of the UN and the OAS
but
periodic selection of NATO secretaries general

1.19b7. Principal Members of the Diplomatic Corps

the Ambassador, the British Ambassador[9]
the Deputy Chief of Mission
the Minister, the Charge, the Consul General, Minister Plenipotentiary
but
the counselor of embassy, the economic counselor, the first secretary, the US defense attache, the consul, the rank of ambassador, ambassadors at the conference (general use)

[9]There are four levels of ambassadorship. 1) Ambassador-nominee: a person who has been designated by a government as ambassador but for whose appointment the United States has not granted *agrement*. 2) Ambassador-designate: a person whose government has obtained *agrement* for appointment but who has not yet taken up the post. 3) Appointed Ambassador: a person who has presented credentials to the Secretary of State or designee but not to the President. 4) Ambassador: a person who has presented credentials to the President.

C05757260

1.20. Publications

1.20a. Titles in English

Capitalize the first letter of the initial word, that of the final word, and that of any principal word in titles of publications and the like (books, newspapers, magazines, articles, series, reports, speeches, plays, movies, musical compositions, works of art, and historical documents). Principal words include all nouns, pronouns, verbs (including the *to* in an infinitive), adjectives, and adverbs; the preposition *via*, as well as *per* when part of a unit modifier; any other word of more than three letters; the first word following a colon or em dash within a title; and parts of compounds that would be capitalized standing alone (Long-Term, President-Elect, Re-Creation, Follow-On, Trade-Off *but* Balance-of-Payments Problems, Nine-to-Five Schedule, Co-op Formation). If a normally lowercased short word is used in juxtaposition with a capitalized word of like significance, it should also be capitalized (*Buildings In and Near Minneapolis, Construction "On the Cheap"*).

1.20b. Shortened Titles

The above rule is sometimes modified to apply to accepted shortened titles of some publications and historic documents.

article in *The Washington Post*; quoted in the *Post* article
reported in *The Times*; from the London *Times*[10]
Quadripartite Agreement; the Agreement
Balfour Declaration; the Declaration (*but* a British white paper)
the Ruritanian Constitution; the Constitution
but
The 1962 Constitution was a vast improvement over earlier constitutions.
Writers of constitutions (general use) and compilers of style guides are kindred souls.

1.20c. Laws and Treaties

Capitalize the first word and all other important words in the formal titles or distinguishing shortened names of federal, state, or foreign documents. If a descriptive term is used, or if the document is still in draft form, use lowercase. The names of ratified treaties are capitalized when rendered in full. For treaties that have not been ratified, the *t* in treaty should always be lowercase.

Bill of Rights
START Treaty, the treaty, New START Treaty
Treaty of Paris, the treaty
Kyoto treaty

1.20d. Foreign Titles

Capitalization of titles that must be given in a language other than English should conform to the practice in that language.

[10]Always word references to the London *Times* so as to avoid confusion with *The New York Times* and vice versa.

C05757260

1.21. Graphics, Tables, and Chapters

The rule in section 1.20 concerning capitalization of titles of publications and the like also applies to titles of graphics, tables, chapter and part headings, headlines, and the equivalent, but not to annotations (such as arrowed captions or callouts) on a photograph, map, or other graphic—for which only the first letter of the initial word is capitalized. If a number given as a figure begins such a caption the word following it is *not* capitalized.

200-mile limit (*not* 200-Mile limit or 200-mile Limit)

1.22. Cross-References

The common nouns used in numeral or letter designations of chapters, parts, graphics, tables, etc. are not usually parts of titles and are not capitalized in cross-references.

covered in chapter III, volume I
refer to appendix B
(see figure 13)
(detailed in table A-4)
disagrees with section 27

1.23. Indented Bullet or Dash Paragraphs

Capitalize the first letter of each entry in a series of blocks of text indented for emphasis and introduced by a bullet or an em dash.

1.24. Miscellany

1.24a. Seasons[11]

Do not capitalize *spring*, *summer*, *fall* (*autumn*), or *winter*. As a general rule, use the definite article in referring to a season and use *of* before the year.

in the fall of 2009
but
her fall 2009 election triumph

1.24b. Major Storms

Capitalize *hurricane* and *typhoon* as part of a US National Weather Service name for such a storm, as in Hurricane Katrina or Typhoon Morakot. Both terms designate types of cyclones, as does *tornado*, but personalization has not been applied to cyclones, tornadoes, or waterspouts (tornadoes gone to sea). In view of the confusion of nomenclature, be sure of what you are talking about before you write about it.

[11]Avoid seasonal references in any writing about the Southern Hemisphere.

C05757260

§ 2. NUMBERS

2.1. Basic Guidance

Although the reader comprehends figures more readily than numbers spelled out, particularly in technical, scientific, or statistical matter, typographic appearance and other special reasons often call for spelling out numbers rather than using figures.

2.2. Numbers of 10 or More

Except in the first word of a sentence, write numbers of 10 or more in figures, not in spelled-out words.

Her tour covered 11 countries in 16 days.

Sixteen days on the road left him exhausted. (*Better*: He was exhausted after 16 days on the road.)

2.3. Numbers Under 10

Spell out most numbers under 10, but use figures if such numbers are decimals, ages of persons, percentages, specific amounts of money, or numbers used with units of measure other than time.

For five years the county has provided free preschool classes for 5-year-olds.

They visited six countries in Asia, three in Africa, and two in Europe, spending an average of 1.45 days in each country.

He walked 6 kilometers every 2.5 days (*but* every two days).

She spent 8 percent of her time in Europe.

He overspent his daily allowance by an average of $7.

The jet's top speed was Mach 2.2.

2.4. Mixes of Numbers Above and Below 10

Combinations of numbers on either side of 10 follow the basic rules governing numbers set forth above.

The estimate covers the period five to 10 years from now.

He packed two suits, 12 shirts, and three ties.

She had 14 children (three daughters and 11 sons).

The measure lacked three of the 34 votes needed for approval.

The attack involved about 200 troops, 12 tanks, and two aircraft.

C05757260

2.5. Ordinal Numbers

The rules governing cardinal numbers generally apply to ordinal numbers, except that military units are always designated by figures (again, unless the figure unavoidably comes at the beginning of a sentence), and fractions are usually written out.

First Congress	82nd Congress
ninth century	20th century
seventh region	17th region
fifth anniversary	50th anniversary
first grade	11th grade
3rd Army	2nd Infantry Division
323rd Fighter Wing	1028th Brigade
9th Naval District	7th Fleet
VI Corps (Army usage)	XII Corps

2.6. Indefinite Numbers

Except with words such as *about, nearly, more than,* and *approximately,* references to quantities in an indefinite sense usually are not written with figures.

The project will cost the government tens of millions.

He addressed several thousand people.

She answered hundreds of questions.

but

He spent about 30 hours on his trip report and had to wait more than 15 days to be reimbursed for expenses.

2.7. Figures of 1,000 or More

Numbers with more than three digits are written with commas, except for years, radiofrequencies, military unit designators, clock time, most serial numbers, and the fractional portions of decimal numbers.

She had traveled 6,187 kilometers as of 1400 hours.

A force of 20,000 (*never* 20 thousand) troops was needed.

According to some sources, there were 1,076,245 US casualties in World War II.

The station operated on a frequency of 1800 kHz.

He was assigned to the 1028th Brigade.

He picked up job number 518225 10-88.

The exact weight is 3,399.243046 grams.

The next step is to multiply by 3.1416.

2.8. Millions and Billions

Numbers over 999,999 are rounded unless an exact amount must be stated. Spell out *million* or *billion* preceded by a figure rounded usually to no more than two decimal places.

The world population today is more than 6.8 billion.

The US population is about 309 million.

C05757260

The number of Americans dead and wounded in World War II totaled 1,076,245.

More than 16.35 million Americans served in World War II—more than three times the 4.74 million in World War I.

Estimates range between $10 million and $20 million (*not* between $10 and $20 million).

but

The cost is estimated at $10-20 million.

2.9. Numerical Unit Modifiers

Numerical unit modifiers are written with hyphens.

third-level decision
20-kilometer (*or* 20-km) march
eleventh-hour decision
10-room house
20th-century progress
200-million-euro loan
(*but* $200 million sale)
3-million-man army
a 1-cent increase
one- and two-bath apartments
five-year plan[12]
105-millimeter (*preferred* 105-mm) guns
7-meter (*never* 7-m)[13] limit
.45-caliber pistol
50-billion-ruble budget (*but* $50 billion program)
2-million-barrel-per-day
(*or* 2-million-b/d) output
6-percent increase, 6- to 7-percent (*or* 6-to-7-percent) increase (*but* 6 percent short)

2.10. Possessives

Numerical expressions in the possessive case require an apostrophe but not a hyphen.

After five years' planning, the project got under way.

She put 16 days' work into the project.

The new regime bought several million dollars' worth of arms (*but* $20 million worth).

2.11. Ranges of Numbers

2.11a. Below the Millions

In order to prevent typographical error or misreading in ranges of numbers, use prepositions and conjunctions rather than hyphens, except for years, page or paragraph references, and values in the millions.

The march covered 10 to 15 kilometers (*not* 10-15 kilometers).

The league membership is between 15,000 and 20,000 (*not* 15,000-20,000).

Model numbers 847,312 through 873,214 were recalled (*not* 847,312-873,214).

but

This report covers the years 2005-09.

For further information, see pages 12-25.

[12]The hyphen is retained in capitalized forms of this term.

[13]Abbreviations of units of measure, including abbreviations formed by a single letter (such as *m* for *meter*), are acceptable in appropriate circumstances, such as in tables or in texts making frequent references to specific quantities. One exception, however, is a hyphenated modifier with a single-letter abbreviation, such as *7-m* or *20-L*. Such compounds are confusing and should be avoided. Instead, spell them out (7-meter, 20-liter) or change the unit of measure (700-cm, 20,000-mL). Potentially confusing also are the abbreviations m^2 and m^3, which, although proper metric forms, can sometimes be mistaken for footnote references. Spelling out *square meter(s)* or *cubic meter(s)* is preferred, or *sq m* and *cu m* may be used. So may m^2 and m^3 if there is no possibility of ambiguity.

C05757260

In tabular material, especially where space limitations apply, the use of hyphens in ranges of numbers is usually more appropriate.

Do not use combinations of prepositions and hyphens, such as *between 15,000-20,000* and *from 847,312-873,214*, to express a complete range of values. The final example in section 2.11b below shows the only circumstance in which such a combination would be appropriate.

2.11b. In the Millions

Hyphens may be used in ranges of numbers in the millions and multimillions.

> Natural gas reserves are estimated at 20-30 billion cubic feet.
>
> Production rose to 2.0-3.5 million tons annually during the period 1971-75.
>
> The range of estimated construction costs has increased from $500-600 million to $2-3 billion. (Do not repeat the dollar sign in ranges like these. Do not write $500 to $600 million or $2 to $3 billion. Although writing $500 million to $600 million or $2 billion to $3 billion is correct, such phrasing would be awkward in the sentence above.)

2.12. Numbers in Tables and Graphics and for Pages, Paragraphs, and Footnotes

Such numbers—and sometimes those that immediately follow each bullet or "tick" in a series that highlights quantities—are not subject to the general rules for numerals, nor are numeral designators for tables, graphics, volumes, chapters, and other parts of publications. However, the text portions of footnotes and, unless space constraints dictate otherwise, of tables and graphics are governed by the same rules for numerals that are applicable to the main text.

2.13. References to Numbers as Numbers

Any number referred to as a number is given as a figure unless beginning a sentence with such a reference is unavoidable.

> The estimate could be off by a factor of 2 or 3.
>
> The data are rounded to the nearest 5.
>
> Divide by 5 to determine your share.
>
> His lucky number is 7.
>
> *but*
>
> Seven is his lucky number.

2.14. Numbers in Nonliteral Sense

Numbers used in a metaphorical or figurative sense are spelled out without regard for the basic rules covering numbers above and below 10.

> The Minister is famous for eleventh-hour decisions.
>
> Moreover, he is often a hundred percent wrong.
>
> Because he is a shrewd politician he remains number two in the regime instead of number twenty.
>
> There must be a thousand others who could run the Ministry better than he.

C05757260

2.15. Decimals

Numbers with a decimal point are expressed in figures. Decimal numbers of less than 1 should have a zero before the decimal point except for designations of gun bore or ammunition. Zeros are omitted at the end of a decimal number unless exact measurement is indicated.

0.25 meter (note that the unit of measure is singular)
1.25 centimeters
silver 0.900 fine (exact measurement)
.22-caliber cartridge

2.16. Fractions

Fractions referring to reasonably specific quantities are written out, with a hyphen in both noun and adjective forms.

three-fourths (*or* three-quarters) of a kilometer[14]
a two-thirds majority; a majority of two-thirds
one-fifth of the electorate; one-tenth; one-twentieth (*or* a fifth, a tenth, a twentieth)
but
a quarter of a lifetime
the second quarter of 2009, the last three quarters of 2009, earnings for first quarter 2010, first-quarter earnings

2.17. Mixed Numbers

If possible, avoid a combination of a whole number and a fraction by converting the fraction to a decimal quantity.

5.5 percent (or *about 5.5 percent*, if you wish to avoid a suggestion of precision)

In nonstatistical contexts, written-out phrases are preferred.

two and a half (*not* one-half) years ago
two-and-a-half-year trial period (*better in some contexts*: 30-month trial period)

In statistical texts, however, precise reporting may require mixes of whole numbers and fractions (5½ , 4¼).

2.18. Expressions of Value

2.18a. US Money

Values expressed in US money are given in figures preceded by a dollar sign. Ordinarily, there is no need for the initials *US* to precede the dollar sign unless the context could allow the reader to assume that dollars other than US dollars are meant. If this is the case and the dollar amounts appear throughout the text, consider adding a footnote such as "Money values in this paper are in US dollars unless otherwise indicated." The word *dollars* is used in an indefinite expression with no figure given or if some definition of the word is needed—such as the year to which the dollar value applies. The word *cents* is used for amounts less than a dollar.

[14]Fractional quantities such as this one may sound plural but they take a singular verb (three-fourths of a kilometer is too far to walk). The same is true of any quantitative expression in which the emphasis is on its meaning as a single unit of measure—for example, money ($500 is too expensive) and time (two years is too long).

C05757260

Russia spent nearly $50 million to develop the system.

Motorists in Amsterdam pay about US $6.50 for a gallon of gasoline; those in Caracas, however, pay only 12 cents a gallon.

Each unit now costs several hundred dollars.

We estimate the system cost the equivalent of 50-60 billion 1987 dollars.

2.18b. Foreign Money

When values are expressed in foreign money, use figures except for indefinite amounts. Because they are unfamiliar to many readers, do not use symbols for foreign currency.

The Israeli-British talks set the unit price at 1,250 pounds sterling (3,065 Israeli pounds).

The construction costs averaged 5 rubles per capita.

The fare is 1 euro.

A bottle of Japanese beer costs 230 yen in Tokyo.

but

Meals in London will cost a few pounds more (*sterling* is understood).

2.19. Percentages and Times Phrases

Numbers showing the relationship of a smaller to a larger quantity are often expressed in percentages, which are always given in figures (75 percent, 6.2 percent, 1 percent, 0.5 percent).

Numbers showing the relationship of a larger quantity to a smaller one are often accompanied by the word *times* and, unless decimals are used, are governed by the basic rules for numbers on either side of 10 (five times as large, 10 times greater, 50 times more frequently, 2.5 times more powerful, two to three times greater).

2.19a. Percentage

The word *percent* is preferred in ordinary text. The percent sign (%) is acceptable in tables and graphics. Unless space is tight, the text portions of tables and graphics should use the word and not the sign to express percentage. Figures are always used for percentage except at the beginning of a sentence that cannot be reworded.

The current five-year plan projects a 20-percent increase by 2015.

Voter turnout dropped 5.7 percent in the second round.

African-Americans make up 5 percent of the student body.

Be careful to distinguish between percent and percentage point.

The inflation rate, which rose only half a percentage point last year, is expected to go up a full 2 or 3 points to 12 or 13 percent in 2010.

2.19b. Times Phrases

Various ways of expressing proportion with the word *times* are shown below. Note that careful wording is needed to avoid a wrong meaning. Sometimes the message is clearer if expressed in percentage. One can also use the suffix *-fold*, although this is somewhat archaic—and awkward when decimal factors are involved. Never use meaningless expressions such as "four times smaller," which sometimes is written by an author who means to say "one-fourth as large."

The number of tanks increased to five times the prewar level. (This is a 400-percent, or fourfold, increase.)

The number of tanks is five times greater than before the war. (This is a 500-percent, or fivefold, increase.)

The number of tanks increased five times. (The tank count went up on five separate occasions by unspecified amounts.)

There are five times as many tanks as there were before the war. (The present number is 400 percent, or four times, greater than the prewar number; is five times the prewar number; and has undergone a fourfold increase.)

If the suffix is attached to a whole number written solid and unhyphenated, spell the resulting word without a hyphen (fourfold, tenfold, twentyfold, hundredfold). Otherwise use a figure and a hyphen (21-fold, 5.75-fold).[15]

2.20. Expressions of Time

2.20a. Ages of Persons

These are expressed in figures except at the beginning of a sentence and in approximations by decades.

The general is almost 60 (*or* 60 years old, *but not* 60 years of age).

General Manley, 60 (*or* age 60, *but not* aged 60), is retiring at the end of the year.

The general must be in his sixties.

Five-year-olds who will reach their 6th birthday by 31 December are eligible.
(Change sentence to begin: All 5-year-olds.)

2.20b. Ages of Inanimate Things

These are given according to the basic rules for numbers above and below 10.

The program is two years old.

Those 30-year-old submarines are being scrapped.

2.20c. Dates[16]

Intelligence writing follows the military style of stating a date without internal punctuation and with day, month, and year in that order.

The United States declared its independence on 4 July 1776.

Switzerland's Independence Day is celebrated on 1 August.

She graduated in June 1951 (*not* June, 1951).

Both (word inserted to avoid starting the sentence with a figure) 11 and 26 November were holidays in 2009.

The March-April spring vacation period empties college campuses. (Use a hyphen to separate the months.)

It snowed heavily on the night of 20-21 February. (Use a hyphen to separate the days.)

The play had a three-week run (25 April–14 May). (Use an en dash—see section 5.9—to separate these dates.)

The base rights ended on 30 April 2008.

[15]The principal advantage of *fold* is that it sometimes permits a more precise translation of data reported in a foreign (particularly Slavic) language. A 5.75-fold increase, however, can just as easily be expressed as a 575-percent increase, an increase of 5.75 times the previous level, or an increase to 6.75 times the previous level.
[16]See dates as modifiers in chapter 9.

2.20d. Years

Figures designating a continuous period of two or more years are separated by a hyphen meaning "up to and including." For two years, *and* may be used.

The presidencies of John Adams (1797-1801), William McKinley (1897-1901), and Bill Clinton (1993-2001) were the only ones to span two centuries.

She worked here during the period 1961-96.[17]

She worked here in 1961 and 1962.

Do not combine *from* or *between* with a hyphen instead of *to* or *and*. Such combinations (from 1951-77, between 1941-45) are almost always incorrect.

A hyphen may be used to date events that straddle consecutive years representing a continuous period, but do not use one to date related but separate events occurring in two consecutive years.

Training of crewmembers took place during the period 2008-09.

during the winter of 2009-10

during the Argentine summer of 2008-09

Clinton was a US Senator (2001-09) before she became Secretary of State.

The first two submarines were launched in 1960 and 1961 (*not* 1960-61).

Use a slash, not a hyphen, in a combining form designating a 12-month period occurring in two calendar years, such as a fiscal year or an academic year, and state the type of year and, if necessary, the period covered.[18]

The farm made a profit in the 2007/08 crop year (1 July–30 June)[19] but not in 2008/09.

Registrations for the academic year 2010/11 are being accepted.

The report covered actual expenditures during fiscal year 2008/09 and made some projections of FY 2009/10 spending. (The abbreviation FY may be used after the first mention of fiscal year, but do not drop the 20. In this illustration it would be equally clear in the second reference to write simply 2009/10, without the FY or the term it stands for.)

2.20e. Decades

Decades are usually expressed with the figure for the initial year followed by an *s* but not an apostrophe.

All those submarines were constructed in the 1960s (*not* 60s, '60s, or sixties).

Our estimates were intended to cover the early and middle 1990s. Your figures dealt with the middle and late 1980s.

2.20f. Centuries

In certain special contexts, a century may be referred to in a manner similar to that used for decades (the 1800s, the eighteen hundreds), but, in most intelligence writing, ordinal numbers (in the 19th century, 20th-century progress) would be more appropriate.

[17]In an expression such as "during the period 1951-77," inclusion of the words "the period" is suggested. If the subject requires repeated reference to such ranges of years, as in economic reporting, the words might be omitted after the first such use. (He composed mainly for motion pictures during the period 1961-64 and twice returned to that medium in 1967-69 and 1974-75. His film music has been compared to that composed at Warners during 1935-50, the heyday of the Viennese-dominated Hollywood school.) In a text prepared for oral presentation write "from 1951 to (or through) 1977."

[18]In US Government practice the fiscal year is stated not in a combining form but with the calendar year representing the larger portion of the fiscal year. US fiscal year 2009 began on 1 October 2008 and ended on 30 September 2009. (Japan's fiscal year 2009, on the other hand, began on 1 April 2009 and ended on 31 March 2010.)

[19]Note the use of an en dash instead of a hyphen in a timespan joining compound elements; a hyphen would be used if the period were shown as July-June.

2.20g. Clock Time

The time of day is written in the 24-hour system, without internal punctuation.

The managers met at 0845 hours.
The satellite was launched at 1800 EDT (2400 GMT).
The midday break is 1300-1430.
also acceptable
The noon meal was the heaviest of the day.
Many high school students rarely get to bed before midnight.

2.20h. Other Time Expressions

Apart from the situations covered in sections 2.20a through 2.20g, references to time follow the basic rules for numbers above and below 10.

The protest lasted for eight days.
The aircraft were airborne in 11 minutes.
The pulses were seven seconds apart.
Figures are given for three fiscal years.
Some countries structure their economic activities according to five-year plans.
He resigned after his sixth year of service.
Payment is acceptable on the 29th day after the due date.
The Communist regime accounts for just six decades in China's history of more than 40 centuries.

2.21. Units of Measure

The Intelligence Community generally uses the International System of Units (metric system) to express size, specifications, or characteristics of things. Among the acceptable nonmetric units of measure are the kiloton, the nautical mile for sea distances, pounds per square inch (psi), and the knot. Other nonmetric units of measure still in use include barrels (and barrels per day) in reporting on the petroleum industry, the US bushel in reporting on grain production and trade, cubic feet in reporting on natural gas reserves or output, and short tons (*not* metric tons) in reporting on nuclear weapons.

2.22. Figures With Units of Measure

Figures are used with any unit of measure (excluding units of time) unless an indefinite quantity is stated, in which case the unit is never abbreviated. As a general rule, do not abbreviate units of measure unless they occur frequently in a report. *They advanced several hundred kilometers* (*never* several hundred km).

1 gallon	4 bushels	8 acres bushels
3 miles	6 meters	8½ by 11 inches
exceptions		
fourfold	six-story building	three-ply
one gross	tenpenny nail	two dozen

C05757260

2.23. Other Number Rules

2.23a. Numbers Close Together

When a cardinal number ordinarily given as a figure precedes a numerical unit modifier that normally would use a figure, try to reword the sentence. If this is not possible, spell out one figure, preferably the smaller one.

15 six-meter trees (*or* 15 trees 6 meters tall)
twelve 250-kilogram bombs (*or* 12 bombs, each weighing 250 kilograms)

2.23b. Ratios, Odds, Scores, Returns

Use numbers for each of these numerical situations.

Women were outnumbered 17 to 1.
The doctor-to-patient ratio was 1:17.
He had a 50-50 chance of winning.
The New Orleans Saints won Super Bowl XLIV, 31 to 17.
The first vote gave the Democrats 21 seats, the Socialists 9, and the Communists 5.
The measure was approved by a 90-to-3 vote.

2.23c. Indefinite Expressions Using Figures

Illustrated in the following examples are numerical expressions that may be required in certain contexts (such as a direct quotation) but are not recommended. Alternative wording is usually available.

100-odd (*better:* more than 100) species of insects
reserves of 50-plus (*better:* 50 or more) vehicles

2.23d. Scientific Notation

A scientific and technical paper may require exponential expression of quantities in the multimillions: 10^{17} watts/cm^2.

C05757260

Factors for Converting to Metric Units of Measure

To Convert From[a]	To (Abbreviation or Symbol)[b]	Multiply by
acres	hectares[c] (ha)	0.4047
acres	square kilometers (sq km, km^2)	0.004047
acres	square meters (sq m, m^2)	4,046.8564
bushels	cubic meters (cu m, m^3)	0.03524
degrees Fahrenheit	degrees Celsius (°C)	5/9 (after subtracting 32)
feet	centimeters (cm)	30.48
feet	meters (m)	0.3048
feet, cubic	cubic meters (cu m, m^3)	0.02832
feet, square	square meters (sq m, m^2)	0.09290
gallons, UK (imperial)	cubic meters (cu m, m^3)	0.004546
gallons, UK (imperial)	liters (L)	4.5461
gallons, US	cubic meters (cu m, m^3)	0.003785
gallons, US	liters (L)	3.7854
inches	centimeters (cm)	2.54
inches	meters (m)	0.0254
inches, cubic	cubic meters (cu m, m^3)	0.00001639
inches, square	square centimeters (sq cm, cm^2)	6.4516
inches, square	square meters (sq m, m^2)	0.0006452
miles, nautical	kilometers (km)	1.852
miles, nautical	meters (m)	1,852
miles, nautical, square	square kilometers (sq km, km^2)	3.4299
miles, statute	meters (m)	1,609.344
miles, statute	kilometers (km)	1.6093
miles, statute, square	hectares (ha)	258.9988
miles, statute, square	square kilometers (sq km, km^2)	2.5900
ounces, avoirdupois	grams (g)	28.3495
ounces, troy	grams (g)	31.1035
pints, liquid	liters (L)	0.4732
pounds, avoirdupois	kilograms (kg)	0.4536
pounds, troy	grams (g)	373.217
pounds per square inch	kilopascals (kPa)	6.8948
quarts, liquid	liters (L)	0.9464
tons, long	metric tons (t)[d]	1.0160
tons, short	metric tons (t)[d]	0.9072
yards	meter (m)	0.9144
yards, cubic	cubic meters (cu m, m^3)	0.7646
yards, square	square meters (sq m, m^2)	0.8361

[a]This table covers only a selection of the most frequently encountered nonmetric units. More comprehensive conversion tables are available elsewhere (in *The World Factbook*, for example).

[b]See footnote 13 and section 2.22 for words of caution about proper use of abbreviations of metric units. The National Bureau of Standards holds that shortened forms used to represent units of measure should be called symbols, rather than abbreviations, because no periods are used.

[c]It is best to avoid the word *acreage* in the metric age, but it has not really been replaced by *hectarage* in the American vernacular. Try *area* instead.

[d]Not *tonnes*. Avoid abbreviation, however, because the *t*, like other one-letter abbreviations, sometimes gets lost in the shuffle. The best approach for metric tons is to establish early in the text of a paper that tons thereafter means *metric tons* and then just use the four-letter word. Occasionally, *MMT* is used to abbreviate *million metric tons* if frequent repetition warrants.

C05757260

3. ABBREVIATIONS

3.1. General Guidance

Use abbreviations sparingly and only when their meaning is clear. When abbreviations are necessary, use standard forms such as those in the GPO *Style Manual* and *Merriam-Webster's Collegiate Dictionary*, or other forms that have gained acceptance. In CIA usage, periods are usually omitted in all but a few categories of abbreviations, such as academic degrees (B.A., Ph.D.), export/import terms (f.o.b., c.i.f.), and ranks or titles (Gen., Prof., Dr.). (Abbreviations for military ranks are in section 3.7.)

3.2. First Reference

An organization, group, international agreement, unit of measure, weapon system, or the like that is referred to throughout a report is abbreviated after it is spelled out at the first reference, often with its abbreviation following it in parentheses. (In long reports, as a convenience to the reader, repeat the full designation occasionally without respecifying the abbreviation, but continue thereafter to use the abbreviation as before.)

Non-Proliferation Treaty (NPT)

nautical mile (nm)

multiple reentry vehicles (MRVs)

airborne warning and control system (The carriers are AWACS aircraft, never AWACs, as in "one AWAC, two AWACs.")

Omit the parenthetical insertion if the first use of the abbreviation closely follows the spelled-out name or term and the connection between the two is clear. This approach is particularly applicable to long country names that, because of repeated mention, need to be abbreviated after the first reference.

The newer models, with a range of 500 nautical miles, are replacing the 400-nm versions now widely deployed.

The United Arab Emirates is . . . the UAE is . . . a UAE delegation arrived[20]

Sometimes it is appropriate to give an abbreviation first, with the full title or other identification in parentheses, or set off by commas, immediately afterward.

WHO (World Health Organization)

ITAR-TASS, the Russian news agency

Pemex (Petroleos Mexicanos)

[20]Note that some country names, like this one, are plural in construction but take singular verbs. Some country names are compounds, but that form is ignored for both syntactic and adjectival purposes—*Trinidad and Tobago is* (adjective: *Trinidadian*); *Sao Tome and Principe is* (adjective: *Sao Tomean*).

C05757260

3.3. Well-Known Abbreviations

Some abbreviations are widely recognized and need no explanation. Even these, however, should be spelled out if the context suggests a need to do so or if there is any doubt about clarity.

ABM (antiballistic missile)
ANC (African National Congress)
APEC (Asia Pacific Economic Cooperation)
ASEAN (Association of Southeast Asian Nations)
AU (African Union)
AWACS (airborne warning and control system)
BGN (Board on Geographic Names)
BW (biological warfare)
CIA (Central Intelligence Agency)
CPU (central processing unit)
CW (chemical warfare)
DHS (Department of Homeland Security)
DIA (Defense Intelligence Agency)
DNI (Director of National Intelligence)
DOD (Department of Defense)
DOE (Department of Energy)
DOJ (Department of Justice)
EU (European Union)
FBI (Federal Bureau of Investigation)
FY (fiscal year)
GDP (gross domestic product)
GNP (gross national product)
GPS (global positioning system)
IAEA (International Atomic Energy Agency)
IC (US Intelligence Community)
ICBM (intercontinental ballistic missile)
IMF (International Monetary Fund)
IRBM (intermediate-range ballistic missile)
KGB (former Soviet State Security Committee)
LDC (less developed country)
MIRV (multiple independently targetable reentry vehicle)
NAFTA (North American Free Trade Agreement)
NATO (North Atlantic Treaty Organization)
NGA (National Geospatial-Intelligence Agency)
NGO (nongovernmental organization)
NRO (National Reconnaissance Office)
NSA (National Security Agency)
OAS (Organization of American States)
OECD (Organization for Economic Cooperation and Development)
OPEC (Organization of Petroleum Exporting Countries)
PLO (Palestine Liberation Organization)
R&D (research and development)
S&T (science and technology)
SALT (strategic arms limitation talks)
SAM (surface-to-air missile)
SLBM (submarine-launched ballistic missile)
SRBM (short-range ballistic missile)
START (Strategic Arms Reduction Treaty)
UK (United Kingdom)
UN (United Nations)
US (United States)
USSR (Union of Soviet Socialist Republics)
WHO (World Health Organization)
WMD (weapons of mass destruction)
WTO (World Trade Organization)

3.4. Foreign Terms

The name of a foreign institution is spelled out in English, if possible, but the commonly used abbreviation may be used even if it is drawn from the foreign wording.

Struggle of Filipino Democrats (LDP)

3.5. Incomplete or Possessive References

Avoid wording that would put an abbreviation immediately after an incomplete or possessive form of the name abbreviated.

the ban under the Non-Proliferation Treaty (NPT), *not* the Non-Proliferation Treaty's (NPT) ban

the platform of the Liberal Democratic Party (LDP), or the Liberal Democratic Party (LDP) platform, *not* the Liberal Democratic (LDP) platform

C05757260

3.6. Plural Forms

If the logical place to spell out an abbreviation comes when the term is plural, the abbreviation must also be in the plural form, even though the singular is used thereafter.

multiple independently targetable reentry vehicles (MIRVs)

3.7. Military Ranks

These abbreviations for the most commonly used military ranks are used only when they precede proper names, preferably full names. In general usage, the ranks are spelled out in lowercase.

Adm.	admiral
Army Gen.	army general
Brig.	brigadier
Brig. Gen.	brigadier general
Capt.	captain
CWO	chief warrant officer
Col.	colonel
Cdr.	commander
Cpl.	corporal
Ens.	ensign
1st Lt.	first lieutenant
Flt. Adm.	fleet admiral
Gen.	general
Lt.	lieutenant
Lt. Col.	lieutenant colonel
Lt. Cdr.	lieutenant commander
Lt. Gen.	lieutenant general
Lt. (jg)	lieutenant junior grade
Maj.	major
Maj. Gen.	major general
Mar.	marshal
Pvt.	private
Rear Adm.	rear admiral
Ret.	retired
2nd Lt.	second lieutenant
Sgt.	sergeant
Vice Adm.	vice admiral
WO	warrant officer

3.8. Unusual Forms

3.8a. MIRVs

This acronymic abbreviation is almost always plural as a noun; note the lowercase *s*. The term also has a verb form, which in turn has participial and negative forms.

If the Soviets had decided to MIRV all their ICBMs . . .
Producing an unMIRVed version of the ICBM system . . .
Stop deploying non-MIRVed missiles after a certain date . . .

C05757260

3.8b. SALT, MBFR, INF[21]

Sometimes an abbreviation not ending in *s* stands for a plural term, as in *SALT* (strategic arms limitation talks). Note that uppercase is not used in spelling out these terms. The abbreviation *SAL* (strategic arms limitation) is also used and, in context, often is clear enough to preclude any need to spell out. The negotiating rounds at Geneva in the 1970s have generally been abbreviated *SALT I* and *SALT II*. Note that it is redundant to write "SALT talks." This is not the case with "MBFR talks," in which the abbreviation (less familiar than SALT and therefore probably requiring explanation) covers only the purpose of the talks—mutual and balanced force reduction. The same logic applies to "INF talks"—negotiations concerning intermediate-range nuclear forces. It is customary not to use an article with these abbreviations. Although the term that SALT stands for is plural, the abbreviation is construed as singular (SALT *was* a high-priority issue in Brezhnev's foreign policy).

3.9. Country Names

3.9a. US, UK

The preferred style is to use the abbreviation for our own country only in the adjective form (a US initiative, *but* favored by the United States). This is not a rigid rule; the abbreviation may be used in graphics or text where space constraints dictate its use. In general, neither the full name *United States of America* nor the abbreviation *USA* is used.

Our style with respect to references to the United Kingdom of Great Britain and Northern Ireland is flexible to the same degree that it is for the United States. *Britain* or *Great Britain* is often used as the shortened form of the country name, but *the United Kingdom* (note the lowercase *t* in *the*) is preferred. *UK* is acceptable as an adjective or, preceded by the definite article, as a noun, except in cases where "sparing use" obliges us to avoid it. *British* is also an acceptable adjective—according to some authorities, it is the preferred one.

3.9b. China

The full name of the People's Republic of China usually is shortened to *China*, although *PRC* may be used. *Chinese* is the preferred adjective and refers only to the mainland. For what we used to call Nationalist China or the Republic of China, use only *Taiwan*, both as a noun and as an adjective. For variation *Taipei* may be used in either noun or adjective form (for example, the officials in Taipei, or the Taipei authorities), but avoid *Taiwanese* as an adjective referring to the island's administration or its officials (and do not use the term *Taiwanese government*). The terms *Communist China* (and *Chinese Communist*) and *Nationalist China* (and *Chinese Nationalist*) or *Republic of China* should be used only in historical contexts. (See *China*, *Taiwan* in chapter 9.)

3.9c. Miscellaneous Rules

Do not abbreviate when a country is mentioned only once or twice, or when it is included in a series in which other country names are spelled out. Most countries have long official names that have been shortened to forms now preferred by the US Board on Geographic Names. Some examples are Australia (Commonwealth of Australia), Mexico (United Mexican States), and South Africa (Republic of South Africa; this full name would be preferred in some contexts to avoid confusion—for instance, a text on the situation in southern Africa as a whole).

[21]All three of these terms refer to past events and should be used only in a historical context.

C05757260

3.10. Titles of Persons

3.10a. Civil or Military

Most civil or military titles preceding a name are abbreviated if followed by both a given name or initial and a surname. *Senator, Representative, Commodore,* and *Commandant* are never abbreviated. *Doctor* is always abbreviated as a title.

> Prof. Mary Jones, Professor Jones; Gen. J. F. Smith (note space between initials), General Smith
> Representative Henry Brown, Representative Brown
> Dr. Robert Young, Dr. Young

3.10b. Complimentary

Complimentary titles (Mr., Mrs., Ms., M., MM., Messrs., Mlle., Mme.) are also abbreviated at all times but are rarely necessary in intelligence writing. Except in biographic reports, the only title we should use is an official one at the first mention of a person's name. After that, refer to the person by last name or by title, treating males and females alike.

> Foreign Minister Spiknayskaya is expected to take part in the conference only long enough to deliver her government's opening position statement. After her departure the principal negotiator will be Ambassador Faytfirskiy, a protege of the Foreign Minister. He is, in fact, a strong candidate to succeed Spiknayskaya when she retires.

In a biographic report mentioning the spouse or other relatives of a person who is the subject of the report, a complimentary title might be needed to ensure clarity.

> President Amigo's family will accompany her on the visit. Her husband, Luis, is a concert pianist. Mr. Amigo, while politically active, has never run for office.

3.11. Latin Abbreviations

Avoid Latin abbreviations (such as *op. cit., et al.,* and *ibid.*) except in footnotes and bibliographies. For the most part, the abbreviations *e.g.* and *i.e.* can be replaced by *for example* or *for instance* (instead of *e.g.*) and *that is* (instead of *i.e.*)—all three phrases followed by a comma. Likewise, use *namely* or *that is* (followed by a comma) instead of *viz.* Another Latin abbreviation to be avoided is *etc.*, because it is, in general, not appropriate in formal writing. [No doubt, some reader will point out that *etc.* is used many times in this publication. The compiler apologizes for confusing anyone but notes that style guides have a somewhat different set of rules from intelligence reports.] If these abbreviations must be used, they retain the periods and are not italicized. Nor is *versus* italicized, either spelled out (preferred in a title or heading) or abbreviated *(vs.)*.

3.12. Political Subdivisions

As a general rule, do not abbreviate the names of political subdivisions such as provinces, departments, or states (US or foreign). Abbreviation of states of the United States or provinces of Canada is acceptable to distinguish cities of the same names in different jurisdictions if the names are used repeatedly. Most of the time there is no need to use political subdivisions for well-known cities such as Toronto, Montreal, New York, and Washington (the DC is almost never necessary in intelligence contexts). Do distinguish Saint John, New Brunswick, from Saint John's, Newfoundland, if the text does not make clear which one is in question; London, Ontario, from London, England; and Vancouver, Washington, from Vancouver, British Columbia.

C05757260

It is not necessary to put the name of the country after that of any well-known city (Bern, Islamabad, Canberra, Brasilia), even if it is not the capital (Geneva, Karachi, Sydney, Rio de Janeiro). Use country names with cities not well known.

3.13. Months and Days

Do not abbreviate the names of months or days except to save space in tables or graphics.

3.14. Percent

Do not abbreviate *percent* except to save space in tables or graphics, where the symbol (%) may be used.

3.15. Units of Measure

Do not abbreviate a unit of measure used in á general or approximate (dataless) sense. Do not abbreviate or use symbols for one or just a few isolated units of measure[22] within text even when precise quantities are given. But do abbreviate units of measure used throughout the text of a report.

This report includes for each city the temperatures (in degrees Celsius) during the trip; the hottest was Washington's (35 °C).

Ranges are given in kilometers.

The opening was several meters wide.

The system has a capacity of 3,000 Btu.

Standard Symbols for Units of Measure:

A	ampere, angstrom	**kn**	knot (speed)
ac	alternating current	**kt**	kiloton
AF	audiofrequency	**kV**	kilovolt
Ah	ampere-hour	**kVA**	kilovoltampere
A/m	ampere per meter	**kW**	kilowatt
AM	amplitude modulation	**kWh**	kilowatthour
avdp	avoirdupois	**L**	liter
b	bit	**lb**	pound
b/d	barrels per day	**LF**	low frequency
Btu	British thermal unit	**L/s**	liters per second
bu	bushel	**M**	million (3M = 3 million)
C	Celsius (degrees)	**m**	meter
c	cycle (radio)	**m^3**	cubic meters
cL	centileter	**μ**	micro (prefix, one-millionth)
cm	centimeter	**μF**	microfarad
c/m'	cycles per minute	**mA**	milliampere
cu	cubic	**mbar**	millibar
cwt	hundredweight	**mb/d**	million barrels per day
da	deka	**Mc**	megacycle

[22]Note that these abbreviations (symbols) do not have plural forms. Be particularly alert to the fact that the lowercase and uppercase forms of the same letter have different meanings in metric abbreviations (*K, Kelvin*; *k, kilo*; *M, mega*; *m, meter*). Be aware also that a capital *L* now is specified as the abbreviation for *liter*.

C05757260

dag	dekagram
daL	dekaliter
dam	dekameter
dB	decibel
dBu	decibel unit
dBsm	decibels relative to 1 square meter
dc	direct current
dg	decigram
dL	deciliter
dm	decimeter
dwt	deadweight ton
EHF	extremely high frequency
emu	electromagnetic unit
F	Fahrenheit (degree), farad
FM	frequency modulation
ft	foot
G	giga (prefix, 1 billion)
g	gram, acceleration of gravity
gal/min	gallons per minute
gal/s	gallons per second
GHz	gigahertz (gigacycles per second)
h	hour
ha	hectare
HF	high frequency
hg	hectogram
hL	hectoliter
hm	hectometer
hp	horsepower
hph	horsepower-hour
Hz	hertz (cycles per second)
in	inch
J	joule
J/K	joule per kelvin
K	kelvin (degree not used)
k	kilo, thousand (7k = 7,000)
KB	kilobyte
kc	kilocycle
kg	kilogram
kHz	kilohertz (kilocycles per second)
kL	kiloliter
km	kilometer
km²	square kilometers
km/h	kilometer per hour
mc	millicycle
mg	milligram
MHz	megahertz
mHz	millihertz
min	minute
MJ	megajoule
mL	milliliter
mm	millimeter
MMt	million metric tons
mph	miles per hour
Mt	megaton
mV	millivolt
MW	megawatt
mW	milliwatt
n	nano (prefix, one-billionth)
nA	nanoampere
nm	nautical mile
ns	nanosecond
oz	ounce (avoirdupois)
p	pico (prefix, one-trillionth)
pA	picoampere
pH	hydrogen-ion concentration
ps	picoseconds
psi	pounds per square inch
pt	pint
pW	picowatt
qt	quart
quad	quadrillion
rad	radian
rms	root mean square
rpm	revolutions per minute
rps	revolutions per second
s	second
T	tera (prefix, 1 trillion)
ton	US ton (not abbreviated)
UHF	ultrahigh frequency
V	volt
VA	voltampere
VHF	very high frequency
V/m	volt per meter
W	watt
Wh	watthour

C05757260

3.16. Ambiguous Abbreviations

Do not use without explanation (if possible, avoid altogether) an abbreviation that can be construed in different ways. *NA*, for example, has been used in tables to mean *not available* as well as *not applicable*. Current practice is to use *NA* only to mean not available. The absence of an entry is assumed to mean not applicable.

Another ambiguous abbreviation is *MT*, which for some writers stands for *metric tons* (the proper abbreviation for which is *t*), but which others have used to mean *megatons* (correctly abbreviated *Mt*).

Still another source of confusion is the improper *kts* for *knots* (which, if abbreviated at all, should be shortened to *kn*). The *kts* is easily mistaken for *kilotons* (correctly abbreviated *kt*).

Finally, the abbreviation C^3, C_3, $C3$, or any of its confusing forms is discouraged—it is supposed to mean *command, control, and communications* but, in careless use, often does not. The preferred form requires a larger-than-normal superior number—C^3—to distinguish it from the smaller variety used for, say, footnote references.

4. ITALICS

4.1. Prominence or Emphasis

The primary purpose of italic type is to give prominence or emphasis to particular words and phrases; italics should be used sparingly so as not to defeat this purpose.

> All members of the working group except the representative of the Central Intelligence Agency believed that the Ruritanians would choose a *phased* development over the next five years. *CIA held to its position that they would try to complete the project by the end of 2012.*

4.2. Titles

Use italic type for titles of books, periodicals, or works of art (including the performing arts—plays, compositions, broadcasts, films, etc.).

> Philip Caputo's *A Rumor of War*
> Michael Jackson's *Thriller*
> concert opening with *An American in Paris*
> the television medical drama *House*
>
> a subscription to *The New Yorker*
> a showing of da Vinci's *Mona Lisa*
> appearing on *American Idol*
> *Slumdog Millionaire* won the Best Picture Oscar in 2009.

Use quotation marks for titles of articles or other parts within longer works (see section 5.15a2).

> "The Style Invitational" in *The Washington Post*

4.3. Foreign Words

The need for italicizing or translating foreign words in intelligence reports depends on whether the word or phrase has been naturalized into English, has not been anglicized but is reasonably familiar to American readers, is the title of a publication or work of art, is the name of an organization, or is otherwise governed by some special consideration.

4.3a. Familiar or Anglicized Foreign Words

Do not italicize foreign words and phrases that have been naturalized into English. Italicize but do not translate foreign words and expressions that have not been anglicized but are familiar to American readers or are easily understood by virtue of their similarity to English (an English equivalent is preferred unless the foreign expression has a special meaning).[23]

> He served as aide-de-camp to the general.
> His experience as chef de cabinet was a factor in his nomination.
> The speaker was shouted down by crowds chanting, *"Democracia, democracia!"*

[23]See section 6.13 for guidance on the use of diacritical marks in foreign words and phrases.

C05757260

4.3b. Other Foreign Words

When a non-English word not covered by section 4.3a is used in ordinary text, italicize it and follow it with a translation in parentheses. This need not be a literal translation if a freer interpretation or explanation, even an extensive one, would be more helpful to the reader. The translation is not italicized unless it constitutes a title of a publication or work of art.

> The achievement of *enosis* (union)[24] with Greece is the all-consuming goal of one segment of the Cypriot population.
>
> Brandt's *Ostpolitik* (his policy of seeking harmony with the communist world)[24] was a hallmark of his chancellorship.
>
> Austria's memories of the *Anschluss* (annexation by Nazi Germany) in 1938 remain a factor in contemporary politics.
>
> He earned the coveted *agregation* (secondary-level teaching credential) the following year.
>
> Marcel Proust's *A la recherche du temps perdu (In Search of Lost Time)* is required reading for Dr. Reboussin's course in French literature.

4.3c. Titles of Publications

As stated in section 4.2, any book or periodical title is italicized. A title in a foreign language may or may not be translated, depending on the title and the context. If a translation is given, it should be in parentheses and in italics (see the final example in section 4.3b above and note that the capitalization style of the original title follows that of the French-language press, whereas the translation follows English-language style).

No translation is needed for such familiar titles as *Pravda, Trud, Der Spiegel, Le Monde, Izvestiya, L'Osservatore Romano, Paris Match,* and *Kommunist.* Some titles—*People's Daily,* for example—have conventionally been cited only in translated form. For this title sometimes and for other titles almost always, an explanation is more relevant and useful than a translation.

> *People's Daily,* official organ of the Chinese Communist Party

Other titles can go either way. For example, *Krasnaya zvezda (Red Star)* [note that *zvezda* is not capitalized], the newspaper of the Russian armed forces, is sometimes cited in Russian followed by a translation, but just as often the title is given only in translated form. Either way is acceptable as long as that way is used consistently in the issuance in which the publication is cited.

4.3d. Names of Organizations

Whenever possible, use the English translation, rather than the original language, in referring to the name of a foreign organization, government body, political party, educational institution, corporation, or the like. Often, however, there are compelling reasons—including convention, wide recognition, and untranslatability—for giving such a name in the original language. In such cases, do not italicize the name. If a translation is possible, relevant, or unobvious, supply one in parentheses following the foreign-language name. If appropriate, give instead or in addition an explanation of the name or description of the organization.

> the joint Bulgarian-Hungarian building enterprise, Intransmech
>
> the Cuban news agency, Prensa Latina
>
> the Portuguese labor organization Intersyndical
>
> the Buddhist organization Soka Gakkai and its political arm, Komeito
>
> chairwoman of Yayasan Haropan Kita (Our Hope Foundation)

[24] A translation of *enosis* or explanation of *Ostpolitik* would not be necessary in every instance.

C05757260

the Wissenschaftsrat (Science Council)
debated in the Bundestag (or the Bundesrat)
the defunct an-Nahda (Renaissance) Party
the Parti Quebecois
graduate of the Sorbonne
veteran of the Surete
visited the al-Aqsa Mosque in Jerusalem
vote of confidence in the Knesset (parliament)

4.4. Names of Craft

Do not italicize (or enclose in quotation marks) names of ships,[25] aircraft, or spacecraft.

seizure of the Pueblo
launched Soyuz-3
a Yankee-class submarine
the Concorde's noise level

4.5. Cited Letters, Words, and Phrases

This style guide provides numerous illustrations of another use of italic type: the citing of a letter, word, or phrase.

words ending in s
nonabbreviation of *percent*

[25]Do not use feminine pronouns to refer to ships or other craft.

5. PUNCTUATION

5.1. General Principles

Most readers of this style guide already know that punctuation is based on meaning, grammar, syntax, and custom and is used to make writing clear. Even so, there are likely to be selected instances when a writer needs guidance. Such guidance is provided in this chapter. The trend should always be toward reducing the amount of punctuation, but be careful to use phrasing that avoids ambiguity and ensures exact interpretation. The sole aim of the choice and placing of punctuation marks should be to bring out the author's thought more clearly. Omit punctuation marks if they do not aid in reading and prevent misreading.

If you would like more information than is given below, consult the GPO *Style Manual*, the *Gregg Reference Manual*, or *Merriam-Webster's Collegiate Dictionary* for explanation and illustration of punctuation rules that are applicable to intelligence reports..

5.2. Apostrophe

The primary functions of the apostrophe are to show possessive case and, in some cases, to create plural forms. (It is also used to indicate contractions in words such as *can't* and *it's*, but these are not appropriate in written English.)

5.2a. Possessives

The possessive case of most nouns and indefinite pronouns is indicated by some combination of the apostrophe and the letter *s*.

5.2a1. Words That End in an s Sound

If the singular of a word (or acronym or abbreviation) ends in an *s* sound, add an apostrophe and an *s* unless the added sibilant is not present in the word's normal pronunciation; in such cases, add only the apostrophe.

the corps' units	Paris's history[26]
Dickens's novels	PBS's programs
Juarez's troops	the Philippines' outer islands
Nantes' port	the United Arab Emirates' oil
the Netherlands' canals	

[26]To avoid a triple sibilant, exceptions are sometimes made for significant names that already end in a double sibilant; for example, convention favors *Jesus'* and *Moses'*. Another exception is *Achilles' heel*.

If the plural of a word ends in *s*, add only the apostrophe.

the boys' team	the two leaders' rift
The Joneses' address	the Russians' policy[27]

5.2a2. Words That Do Not End in an s *Sound*

If a word (either singular or plural) does not end in an *s* sound, add an apostrophe and an *s*.

the child's shoes	the children's shoes
each other's home	the officer's report
that Thai's[28] passport	those Thai's[28] passports
the woman's book	the women's books

5.2a3. Compounds

In compounds, make only the last word possessive.[29]

commander in chief's decision	secretary general's speech
someone else's hat	Shah of Iran's overthrow

5.2a4. Combinations Indicating Joint Possession

In a combination of two or more nouns for which joint possession is to be indicated, make only the last noun possessive; if individual possession, make both or all nouns possessive.

President Obama and Chancellor Merkel's meeting to discuss Afghanistan and international climate change occurred on 3 November 2009.

Rodgers and Hammerstein's only collaboration specifically for a film was on *State Fair*.

Clint Eastwood's, Hilary Swank's, and Morgan Freeman's Oscars were all for *Million Dollar Baby*.

5.2a5. Geographic, Firm, or Organization Names or Publication Titles

In geographic names, firm names, the names of organizations and institutions, and the titles of publications, follow the generally accepted form.

Consumers Digest	Johns Hopkins University	People's Republic
Court of St. James's	Lloyds (bank)	*Reader's Digest*
Harpers Ferry	Lloyd's (insurance)	Reuters (news agency)

5.2a6. Organized Bodies That End in s

Do not use an apostrophe after names of states or countries and other organized bodies ending in *s*, or after words more descriptive than possessive, except when the plural does not end in *s*.

Kansas law	Weight Watchers meeting	National Organization of
League of Nations mandate	officers club	Women's headquarters
master's degree	teachers college	writers guide

[27]Use of the possessive in a phrase like this is an easy fix for one of the most frequent writing errors, the antecedentless pronoun, as in "the *Russian* policy toward *their* minorities." Change the adjective *Russian* to the possessive noun *Russians'* to give *their* an antecedent. The reference word (usually an antecedent) for a pronoun must be a noun or another pronoun, never an adjective, like *Russian* in the sample phrase. An early CIA style guide writer called the antecedentless pronoun a *moose track*, as in *"There were moose tracks in the snow but none of them could be seen"*—the pronoun *them* does not have a proper antecedent in the noun-turned-adjective *moose*.

[28]Note that *Thai* is both singular and plural.

[29]If the compound is plural (see section 6.5b), use the *of* possessive (section 5.2b) unless the plural is formed in the final word of the compound: decisions of the attorneys general, *but* the general counsels' decisions.

5.2a7. Personal Pronouns

Do not use the apostrophe with the possessive form of personal pronouns.

his	ours	yours
hers	theirs	its (Do not confuse with the contraction *it's* [it is].)

5.2b. Possessives With Persons or Inanimate Bodies

As a general rule, the possessive form made up of an apostrophe and an *s* (the Minister's) is used for nouns denoting persons, and the form combining the preposition *of* and a noun object is applied to organizations or inanimate things (a decision of the Ministry). However, the *s* possessive is commonly used for the inanimate in expressions that indicate time (moment's notice, year's labor, two hours' work, a day's pay) and in other familiar phrases (heaven's sake, heart's content, for pity's sake, for old times' sake).

Which possessive form to use often depends on sound or rhythm: the *s* possessive is more terse than the longer, more sonorous *of* phrase (morning's beauty, beauty of the morning). In some *of* phrases, idiom calls for a sort of possessive redundancy—always for a pronoun (friend of his), usually but not necessarily for a proper noun (friend of John's; friend of John Jones), and optionally for a common noun (friend of the author, friend of the author's).

5.2c. Noun or Pronoun Preceding a Gerund

The possessive case is used for a noun or pronoun preceding a gerund if this syntax is unavoidable (try to rephrase).

> London announced it had no objection to Rome's taking part. (*Better:* London announced it would not object if Rome took part.)
>
> Economy was one reason for George's buying a small car. (*Better:* Economy was one reason George bought a small car.)

5.2d. Plurals

The apostrophe is inserted before a lowercase *s* to form the plurals of single letters and digits and of abbreviations ending with a period. (*Note:* an abbreviation of a unit of measure has neither a period nor a plural form [1 km, 2 km].) It is not inserted before the *s* in the plurals of groups of letters or hyphenated letter-number combinations unless needed to enhance comprehension—for example, if the combination ends with a lowercase letter (SS-N-3a's). It is omitted in the plurals of groups of digits designating decades or centuries.

Boeing 747s	dotted i's
Pershing Ia's (*but* Pershing IIs)	11s and 13s
H-Is and H-IIs (*but* type I's)	Kresta-IIs (*but* Flogger B's)
MiGs	RVs
Ph.D.'s, B.A.'s, M.A.'s[30]	7's and 8's (*but* SS-7s and SS-8s)
the 1980s	SS-N-4s (*but* Mod 2's; all Mods of the SS-11)

[30]Academic degrees are in lowercase when spelled out: doctor of philosophy, doctorate, master of arts, bachelor's degree.

C05757260

To form the plurals of spelled-out numbers, of most words referred to as words, and of words already containing an apostrophe, add just *s* or *es*. But, add *'s* to indicate the plural of words referred to as words if the omission of an apostrophe would cause difficulty in reading.

> One of Theodore M. Bernstein's best style books is *Dos, Don'ts & Maybes of English Usage*, but it fails to point out that most incorrect *due to*'s can be remedied by changing them to *because of*'s. (Note that the 's is not italicized when attached to form the plural forms of the italicized *due to* and *because of* in this example.)

5.3. Brackets

5.3a. Inside Parentheses

Brackets are used to enclose a parenthetical word or expression within a set of parentheses.

> He was well educated (by tutors in Portland [Maine]).

5.3b. Editorial Remarks

Brackets are used to set off such remarks within quoted material.

> The Minister said, "The election [of 3 March] will be reexamined."

5.4. Bullets (Ticks)

Bullets—usually solid circular symbols—are used to introduce a list of two or more items set off within a column of text. They may be used instead of or in combination with *em dashes* (sometimes called *ticks*), as in a series of indented, itemized blocks of text in which some blocks are subsets of more important ones. Never use a single bullet or tick simply for emphasis; rather, use boldface or italic type.

Capitalize the first letter of all material introduced by a bullet or an em dash and end each phrase with a period (or a question mark, if appropriate). Introduce the material with a colon at the end of the introductory sentence or phrase.

The following are examples of bullets used with em dashes:

- This would be a primary bullet phrase (or clause).
- This would be another primary bullet phrase.
  —This would be a secondary phrase subordinate to the bullet phrase above.
  —This would be another secondary phrase.
- This would be the next primary phrase.
  —Phrases pertinent to this phrase would be listed under it like this.
  —And this.
- This would be the last primary bullet phrase.

5.5. Colon

5.5a. Summaries or Expansions

Use a colon before a final clause or phrase that summarizes or expands preceding matter. A single space is used after a colon.

C05757260

Food, clothing, fuel, and building materials: these are the critical items.

The delegation visited four European cities: London, Paris, Dublin, and Rome.

Jones served in three Ministries: Economy; Communications, Power, and Industry; and Agriculture.

5.5b. Separation of Clauses

A colon is used to separate two main clauses if the second amplifies or explains the first. Otherwise, use a semicolon (see section 5.16b).

Railroading is not a variety of outdoor sport: it is a service.

He is well qualified to serve as Foreign Minister: he has held posts in the Ministry since 1995 and has served abroad many times.

5.5c. Titles and Subtitles

Use a colon to separate subtitles from titles.

The Tragic Dynasty: A History of the Romanovs

Editorial Consistency: An Agency Goal

5.5d. Ratios

Figures (not spelled-out words) are always used for ratios, but use hyphens if the ratio is used adjectively.

20:1, *but* a 20-to-1 chance

5.5e. Indented Material

Use a colon to introduce lengthy material set off from the rest of the text by indentation. If the material is a quotation, do not use quotation marks.

5.6. Comma

The comma is the punctuation mark that is both most often used and most often misused. There is a general tendency to use too many commas, but the sin of omission is almost as common as the sin of commission.[31]

5.6a. For Comprehension

Use a comma to separate two words or figures that might otherwise be misunderstood.

Of the total, production was the greatest single item.

To his younger brother, Murray was a paragon whose every action was to be imitated.

Instead of thousands, hundreds were built.

In 2009, 523 units were completed. (*but* In 2009 about 500 units . . .)

[31]One "sin of commission" is the so-called comma splice, in which a comma is used instead of a semicolon or period to denote cessation rather than pause, as in "Rain is forecast, however, we intend to hold the event anyway." The first comma should be a semicolon (or a period, followed by a new sentence), or the two elements of the compound sentence can be "spliced" properly with *but:* "Rain is forecast, but we intend to hold the event anyway."

C05757260

5.6b. Separation of Coordinate Modifiers

Use a comma to separate from each other the parts of a series of coordinate modifying words (the words are coordinate if you can substitute *and* for the comma).

short, swift streams long, slender, brittle stems

Do not use a comma if the modifying words are cumulative (cannot be separated by *and*), rather than coordinate—that is, if one modifies another or a unit of which another is a part.

illegal drug traffic short tributary streams

If the modifying words are neither coordinate nor cumulative, they probably constitute a unit modifier (see section 7.3).

5.6c. With Nonrestrictive Words

Use a comma to set off nonrestrictive (nonessential) words, phrases, or clauses.

The chairman, George Smith, spoke last.

The work was, in fact, completed.

The manager, who was dismissed in 2008, was reappointed in 2009.

His brother, Joseph, was appointed. (He had only one brother.)

Mitchell's novel, *Gone With the Wind*, was a bestseller. (She wrote only one novel.)

Actual production, however, was lower.

Whether the element is nonrestrictive is determined by the intent of the sentence. Note that in the following sentences each of the elements that are nonrestrictive in the sentences above is necessary to the meaning of the sentence in which it appears, is therefore restrictive, and is not set off by commas. Compare these examples with the ones above.

Cochairman Smith spoke last (not Cochairman Jones).

The idea must work in fact as well as in theory.

The manager who was dismissed in 2008 was rehired in 2009. (The *who* clause identifies the particular manager being discussed.)

His brother Joseph was appointed. (He had more than one brother.)

James Michener's novel *Tales of the South Pacific* won the Pulitzer Prize for fiction. (He wrote many other novels, but none of them won Pulitzers.)

However hard they tried, production stayed low for several years.

5.6d. With Contrasting Statements

Use a comma to set off contrasting statements in a sentence.

Obama, not Bush, made the decision.

5.6e. Serial Comma

Use a comma after each element except the last in a series of three or more words, phrases, clauses, letters, or figures used with *and* or *or* (as long as none of the elements in the series is a phrase or clause with internal commas). Opinion is divided about whether to use the serial comma, as the comma after the next to last element in a series is called: many publications, especially newspapers, generally omit it so as to save space but sometimes insert it to avoid ambiguity. The question does not arise if the serial comma is always used. Most authorities on English usage recommend that policy, and it is the rule for CIA publications.

C05757260

Copper, lead, zinc, and tin were mined.

The contestants may dance, play an instrument, or sing.

The data were collected, estimates were made, and conclusions were drawn.

Complete forms A, B, and C by writing 1, 2, or 3.

If one or more of the elements in the series is a phrase or clause with internal commas, use semicolons instead of commas between the elements, rearranging the sentence if necessary to put the series at the end. No matter how short the elements, use the serial semicolon before the *and* or *or*.

The chief exports were brass, which is an alloy; platinum, which is a precious metal; and tin. (*never* Brass, which is an alloy; platinum, which is a precious metal; and tin were the chief exports.) (See also section 5.16a.)

5.6f. Compound Sentences

Use a comma before the coordinating conjunction in a compound sentence (a sentence that contains at least two independent clauses).

He served in the Army until 1996, and then he went to work for the telephone company.

The country imports copper, iron, and lead, but domestic tin is available.

In a simple sentence with a compound predicate do not use a comma before the coordinating conjunction unless it is needed for clarity.

He served in the Army until 1996 and then went to work in a bank.

He went to Russia to study but decided not to stay.

but

He goes to sleep the minute he hits the mattress, and springs out of bed in the morning always eager to begin a new day.

5.6g. Numbers in the Thousands and Higher

Use a comma to separate digits of most numbers in the thousands and unrounded millions.

1,000

3,399.243046

6,201

250,000

5,752,194 (if rounded, 5.75 million, 5.8 million, or 6 million)

5.6h. Introductory Phrases

Use a comma to separate from a main clause an introductory clause or phrase that is long or that might cause confusion without a comma.

Because the corporation derived much of its 2008 income from suburban outlets, it established several new ones in 2009. (*but* After his defeat he retired from public life.)

Use a comma to set off a beginning participial phrase modifying the subject or an absolute phrase before the subject; and, if it contributes to easier reading, an opening adverbial phrase stating a year.

To begin with, Smith worked as an engineer.

In 1986 the tragedy at Chernobyl occurred.

In 1987, Gorbachev formulated his policies of glasnost and perestroika.

Note that, whereas no comma is needed after 1986 in the second example, in the next one, when the year is followed by an *uppercased* word, insertion of a comma aids quick comprehension; such a comma is nevertheless optional.

C05757260

5.6i. Title of Person and Name of Organization

In the absence of the words *of* or *of the*, use a comma to separate a person's title and the name of an organization.

director, Coal Division, Ministry of Mines

5.6j. Omission of a Word or Words

Use a comma to indicate omission of a word or words, unless the construction is clear enough without commas.

In spring and fall there is hiking in the area; in summer, sailing; in winter, skiing. (*but* The data were collected, estimates made, and conclusions drawn.)

5.6k. Before Direct Quotations

Use a comma to separate an introductory phrase from a short direct quotation (for long quotations, use a colon instead).

He said, "Now or never."

5.6l. With Geographic, Personal, or Corporate Names

Use a comma to set off a province, state, or country name from a city name; *Jr.* (but not, say, *III* or *IV*) following a personal name; and sometimes (follow the subject's preference) *Inc.*, *Ltd.*, or *S.A.* after a corporate name. If the setting off occurs in midsentence, a comma must be used after as well as before.[32]

He lives in Vancouver, Washington, but visited Vancouver, British Columbia, for the Winter Olympics in 2010.

John Jones, Jr., heads Dictionaries, Inc., and his son John Jones III runs the Georgetown branch (not his only son, or the name would be set off by commas—see 5.6c).

5.7. Dash (or Em Dash)

The dash (or *em dash*, not to be confused with the *en dash*—see section 5.9) should be used only when it is needed, and not when such punctuation as a comma, a colon, or parentheses would suffice. Excessive use presents a visual barrier to the reader and interrupts the flow of thought. The dash should never be used immediately after a comma, a semicolon, or, except as described in section 5.4, a colon.

5.7a. Parenthetical Matter

The dash is sometimes used to set off parenthetical matter, although a pair of dashes can often be replaced by parentheses and should be if there would otherwise be two pairs of dashes within a sentence. If the dash is used to set off material *at the end of a sentence*, only one dash, at the beginning, is needed. If the material is set off *within the sentence*, only another dash (not a comma or a semicolon) can be used to end the setoff phrase or clause.

He was a key figure in the successes—as well as the problems, both domestic and international—of Japan's trade policies.

He has three sons—Thomas, 29; Richard, 19; and Henry, 16.

[32]Failure to do this results in what usage and style authority Roy Copperud dubs a "one-legged comma." Such an omission can also occur before a setoff clause or phrase.

C05757260

He goes home twice a year—at Christmastime and on his birthday—and he never stays for more than two days. (In this example, the necessary second dash supersedes the comma that would ordinarily divide the two clauses of this compound sentence.)

The report for 2009 (the calendar, not the fiscal, year) led to an angry exchange—unusual for January—in the legislature.

5.7b. Before a Final Summarizing Clause

The dash is often used interchangeably with the colon to introduce a final summarizing clause.

Freedom of speech, freedom of worship, freedom from want, freedom from fear—these are the fundamentals of moral world order.

5.7c. In Place of a Bullet

The dash is sometimes used instead of a bullet to mark the beginning of each part of a block of material (other than quotations) set off by indentation from the rest of the text. If used in this way, it may be called a *tick*. (See section 5.4.)

5.8. Ellipsis

An ellipsis (the omission of words within quoted material) is represented by three spaced periods. When in the middle of a quotation an ellipsis occurs at the end of a sentence, a fourth period (or other punctuation, if appropriate) precedes the spaced periods. When only part of a sentence is quoted, periods to show omission are required only within the quotation, not at the beginning or the end.

The President began his address with the observation that in 1776 "our fathers brought forth a new nation, conceived in liberty and . . . dedicated to the proposition" of equality for everyone.

In his words, "we [cannot] consecrate . . . this ground. The brave men . . . who struggled here . . . have consecrated it. . . . The world . . . can never forget what they did here."

5.9. En Dash

The en dash (not to be confused with the *dash*, or *em dash*) is, in effect, a superhyphen, used to "hyphenate" a compound modifier that includes one or more compound elements. It is effective with capitalized compounds but is less so with lowercase compounds, for which use of multiple hyphens is better, even though the lowercase compound is one not normally hyphenated. (The en dash can usually be avoided by rewording.)

Winston-Salem–Pointe Claire telephone call (*or* call between Winston-Salem and Pointe Claire)

Saudi Arabia–United Arab Emirates border (*or* border between Saudi Arabia and the United Arab Emirates)

Health Department–sponsored program (*or* program sponsored by the Health Department)

post–World War II policies (*or* policies after World War II)

SS-19–type silos (*or* silos of the SS-19 type)

but

Echo-II-class submarine (Use two hyphens, *not* a hyphen and an en dash, because this is a special category. See section 7.6e.)

defense-industry-based engineers (*not* defense industry–based engineers, which is confusing)

also

a vice-president-elect, *but* the Vice President–elect

a prime-minister-designate, *but* the Prime Minister–designate

C05757260

5.10. Exclamation Point

Because intelligence reports are expected to be dispassionate, this punctuation mark should rarely, if ever, be used.

5.11. Hyphen

Use of the hyphen is well illustrated in the chapters on numbers, spelling, and compound words.

5.12. Parentheses

Parentheses are used as shown in 5.12a through 5.12d. (See also section 5.3 on the use of brackets in functions similar to but distinct from those served by parentheses.)

5.12a. With Comments

Use parentheses to set off a word, phrase, clause, or sentence that is inserted by way of comment or explanation within or after a sentence but that is structurally independent of it.

This style guide (unclassified) will be widely disseminated.

He graduated from Stony Brook University (part of the State University of New York system).

Three old destroyers will be scrapped. (All three have been out of commission for some time.)

Note that the placement of the period above depends on whether the parenthetical insertion is part of the sentence that occasioned it or is an independent, complete sentence (see the last two examples above). In the following example, note that the comma follows the parentheses enclosing an insertion made in the middle of a series separated by commas.

He visited Portland (Maine), Philadelphia, and Baltimore.

5.12b. With Cross-References

Use parentheses to enclose cross-references.

Japan's exports have risen steadily for the past 10 years (see figure 3).

. . . *or* (annex A).

. . . *or* (see the table).

. . . *or* (See figure 3.) *as a separate sentence.*

5.12c. With Numbers or Letters in a Series

Use parentheses to enclose numbers or letters that set off parts of a series.

We must set forth (1) our long-term goals, (2) our immediate objectives, and (3) the means at our disposal. (Be sure to use a set of parentheses with each number, not just a single one after it.)

5.12d. With Foreign Words

Use parentheses to enclose translations or explanations—if necessary—of foreign words or to enclose the original language following the English version (see section 4.3).

He referred to the document as an estimate (*otsenka*).

Sagan's best known novel is *Aimez-vous Brahms?* (*Do You Like Brahms?*). [Italicize the translation because it is still a title.]

C05757260

Pointing to the skyline as we neared the capital, he trumpeted the nation's new *grandeza*—even as we passed one of the *favelas* (shantytowns) outside the city.

5.13. Period

The use of the period is so elementary that it hardly needs to be discussed in this guide except to point out that it is not generally used in CIA for abbreviations and that a single space is used between sentences. The placement of the period in its principal function, to terminate a nonexclamatory or noninterrogative sentence, is discussed and illustrated in other parts of this chapter on punctuation—under "Parentheses" and "Quotation Marks," for example. (See section 5.8, which discusses one of the period's sidelines.)

5.14. Question Mark

As with the period, a discussion of the function of the question mark borders on stating the obvious. Note, however, that, apart from its principal function of terminating interrogative sentences, the question mark is used:

5.14a. To Show Uncertainty

A question mark may be used to show uncertainty (or ignorance), as when it is placed next to (or instead of) a figure in a tabulation. Similar application can be made within the text, but this should be kept to a minimum.

The paper was a hodgepodge, trying to deal with poets as diverse as Omar Khayyam (?-1132?) and Geoffrey Chaucer (1340?-1400).

5.14b. In a Title

A question mark may be used as part of an appropriate title.

Moscow and the Eurocommunists: Where Next?
A Credible Nuclear Deterrent?

5.15. Quotation Marks

Quotation marks may be double or single and must always be used in a pair. Single quotation marks never appear in American usage unless double marks are present.

5.15a. Double Quotation Marks

5.15a1. Direct Quotations

Use a set of double quotation marks around a short direct quotation. (If the quotation is long—say, half a dozen lines or more—set it off by indentation within the text column and omit the quotation marks.)

"The President," he said, "will veto the bill."
Who asked, "Why?"
Why label it a "gentlemen's agreement"?
The citation read: "For meritorious service beyond the call of duty."

5.15a2. Titles That Do Not Merit Italicization

Use quotation marks to set off titles of poems, songs, short stories, and other parts of a longer work (see section 4.2).

> Many people consider "Billie Jean" to be the most influential song in Michael Jackson's album *Thriller*.
>
> Who wrote the article "Thermonuclear Processes" in that issue of *Survey*?
>
> Have you read Robert Frost's poem "Fire and Ice"?
>
> "Punctuation" is one of the chapters in the GPO *Style Manual*.

5.15a3. Selected Words or Phrases

Use quotation marks to set off words or phrases—but usually not letters, for which italic type is better—used or cited in a special sense. (For this function, quotation marks are sometimes used interchangeably with italic type.)

> Do not capitalize the s in *socialist* in the phrase "most British socialists join the Labor Party."
>
> The North Korean press put the blame on "US imperialism."
>
> If this is a "working" vacation, why are you lying there doing nothing?
>
> Do not italicize, or use quotation marks for, the *T* in "the inverted-T-shaped building."

Be careful not to overuse or misuse quotation marks. Use them to enclose words used in a special sense (such as communist jargon), but do not use them to apologize for acceptable English words or in an attempt to redeem slang. Never allow the reader to wonder why they were used. For example, the wording "the Russians took a 'pragmatic' approach" is obscure; it probably means "the Russians took what they called a pragmatic approach," but the reader may assume that the quotation marks around pragmatic connote some "special" meaning and may waste time looking for an explanation.

5.15b. Single Quotation Marks

A pair of single quotation marks is used to enclose a quotation within a quotation. But, if a quotation is set off by indentation, rather than by quotation marks, a quotation within it would use double, not single, quotation marks.

> He said, "I used the term 'gentlemen's agreement.'"
>
> He asked, "Why label it a 'gentlemen's agreement'?"
>
> "Remember," she said, "what Grandfather used to advise: 'When other people run, you walk.'"
>
> "Do you remember," she asked, "that Grandfather used to advise: 'When other people run, you walk'?"

5.15c. Punctuation With Quotation Marks

Also illustrated in the examples already given are the positions of various punctuation marks with relation to quotation marks:[33]

- Commas and periods always go inside quotation marks (single or double).
- Semicolons and colons always go outside the final quotation mark.
- Other punctuation marks are placed inside quotation marks at the end of a sentence only if they are part of the matter quoted.

[33]An asterisk or a superior reference number or letter normally follows all punctuation marks except a dash but falls inside a closing parenthesis or bracket if it applies only to the matter within the parentheses or brackets.

C05757260

5.15d. Terms Precluding Need for Quotation Marks

Quotation marks are usually not necessary to enclose expressions following terms such as *known as, called,* or *so-called.*

Aluminum is known as aluminium in Canada.

Your so-called investigating body has not done much investigating.

If this is called profit and loss, when do we start profiting?

They may be used even here, however, to give special emphasis to the quoted or verbatim nature of the expression given, especially if sarcasm or bad grammar is involved:

He criticized what he called the "looks funny" school of editing.

They are following the so-called "where it's at" lifestyle.

Other such terms—*entitled, named, endorsed,* and *signed* or their equivalent—clearly call for either italicizing or enclosing in quotation marks the word or words that follow them.

The card was signed "You know who."

His housemates named him "chief cook and bottle washer."

The word *radar* is an acronym derived from the term "radio detecting and ranging."

5.16. Semicolon

The semicolon can be regarded to some extent as a supercomma because it supersedes the comma in cases where a comma is not clear enough for the function intended.

5.16a. Series

Use a semicolon to separate the elements in a series that falls at the end of a sentence and cannot be separated by commas without risk of making the sentence difficult to understand. If such a series is in midsentence, reword the sentence to put the series at the end. (See section 5.6e.)

The major inputs are iron ore, which comes from Poland; nitric acid, which is imported from the Czech Republic; and nickel, which is furnished in adequate quantities by domestic producers.

The principal legatees were a niece, Jane Wilson; a longtime friend, Samuel Jones; and the city library.

5.16b. Compound Sentence

Use a semicolon to separate the clauses of a compound sentence when a coordinating conjunction is not used.

He received a degree from the University of Vermont in 1976; later he attended Dartmouth College.

A fool babbles continuously; a wise man holds his tongue.

5.16c. With Conjunctive Adverbs

Use a semicolon before an independent second clause introduced by a conjunctive adverb (accordingly, also, consequently, furthermore, hence, however, indeed, moreover, nevertheless, otherwise, so, still, then, therefore, thus, yet).

Some Americans spend millions of dollars for junk food; consequently, the national obesity rate is growing rapidly.

Smith speaks English, French, German, and Russian well; moreover, he understands Persian, Urdu, and Vietnamese.

In monsoon season you should take your umbrella with you; otherwise, you may get soaked.

C05757260

5.17. Slash

The slash (also called diagonal, oblique, shill, slant, solidus, and virgule) should be used sparingly and never in place of a hyphen or dash.

5.17a. To Show a 12-Month Period Occurring in Two Calendar Years

fiscal year 1965/66
marketing year 1973/74
crop year 2005/06
academic year 2009/10

5.17b. To Represent Per *in Abbreviations*

km/h (kilometers per hour)
b/d (barrels per day)

5.17c. To Separate Alternatives

These designs are intended for high-heat and/or high-speed applications. (Usage guides generally discourage *and/or* and encourage one or the other of the two words instead. In this example *and* alone would suffice.)

She sat at her computer for hours in a catatonic/frenzied trance trying to cover every possible contingency of style usage in the Agency. (And in this one, *or* could replace the slash with no confusion of meaning.)

5.17d. To Show Combination in Certain Instances

Russian support was pivotal for this Japanese/US-backed proposal. (Use of an en dash or another hyphen would be awkward.)

Insurgent forces were armed with Cuban/Russian-supplied weapons. (Use of a slash here could indicate either a combination or alternatives, the latter reflecting Moscow's practice of sometimes using surrogates to supply its clients.)

The goal of one-man/one-vote was never forgotten. They campaigned on a one-man/one-vote platform. (Keep the hyphen and slash whether a noun form or an adjective form.)

The group endorsed the Christian Democratic Union/Christian Social Union platform.

C05757260

6. SPELLING

6.1. General Principles

The majority of the words given as examples in this chapter are also found in chapter 8 (Spelling and Compound Words List), where all entries are listed in alphabetical order. A writer seeking the correct spelling or hyphenation of a word or words may find it easiest to look there first.

The GPO *Style Manual* and *Webster's Third New International Dictionary*, published by the G. & C. Merriam Company—or the abridged version, *Merriam-Webster's Collegiate Dictionary*—are the authorities for the guidance provided in this chapter and in chapters 7 (Compound Words) and 8. Where there is a difference, the GPO version usually prevails over Merriam. For a word not given in this style guide, consult first the GPO manual and then the Merriam dictionary. For guidance on the spelling of proper names—geographic, personal, and organizational—see sections 6.11 and 6.12.

6.2. Preferred and Difficult Spellings

Words frequently misspelled and the preferred forms of words with variant spellings are included in the list in chapter 8. Many other such words are dealt with in special categories in this chapter.

6.3. British Terms

When the American and British spellings of common English words differ, the American spelling is always used, even when these common words form part of a proper name usually spelled with British English.

Industrialization (*not* Industrialisation) Board
Labor (*not* Labour) Party
Minister for Defense (*not* Defence)
Programs (*not* Programmes) Chairman

6.4. Anglicized Foreign Words

Many foreign words and phrases have been thoroughly anglicized. Others are not as easily comprehended by American readers and should not be used unless there is no equivalent English expression (for example: *ad hominem*, *passim*). Still other foreign expressions should be avoided because they sound hackneyed (apropos, confrere, faux pas, inter alia, piece de resistance, tete-a-tete). Foreign-derived words sufficiently common or functional to be used (without italic type) can be found in chapter 8.

C05757260

6.5. Plural Forms

6.5a. O Endings

Nouns ending in *o* preceded by a vowel add *s* to form the plural; most nouns ending in *o* preceded by a consonant add *es* to form the plural. Following are selected exceptions.

commandos	magnetos	solos
dynamos	mementos	tobaccos
egos	mestizos	Tornados (aircraft name), *but* tornadoes (common noun)
escudos	octavos	twos
ghettos	provisos	virtuosos
kimonos	salvos	zeros

6.5b. Compound Terms

For the plurals of compound terms, whether hyphenated or not, use the plural form of the significant word or words. If there is no significant word, the plural is formed on the last word.

adjutants general	courts-martial	inspectors general
aides-de-camp	deputy chiefs of staff	major generals
also-rans	directors general	ministers-designate
ambassadors at large	general counsels	passers-by
assistant comptrollers general	gentlemen farmers	pick-me-ups
attorneys general	go-betweens	presidents-elect
brothers-in-law	goings-on	rights-of-way
charges d'affaires	governors general	secretaries general
chiefs of staff	grants-in-aid	trade unions
commanders in chief	hangers-on	under secretaries
consuls general	higher-ups	vice chairmen

6.5c. Other Difficult Plurals

Other words with plural forms that might cause difficulty are listed in chapter 8. If you are unsure of a word's plural, look there.

6.6. Endings *-yze*, *-ize*, and *-lse*

A verb whose last three letters are pronounced like *eyes* is usually spelled in one of three ways. The letter *l* is followed by *-yze* if the verb expresses an idea of loosening or separating. The related noun ends in *-lysis*.

analyze (analysis) paralyze (paralysis)

Most other words in this class end in *-ize*. Common exceptions are the following.

advertise	disguise	incise
advise	enfranchise	merchandise
arise	enterprise	revise
chastise	excise	rise
comprise	exercise	supervise
compromise	exorcise	surmise
despise	franchise	surprise
devise	improvise	televise

C05757260

6.7. Endings *-sede, -ceed,* and *-cede*

A verb with a final syllable that sounds like *seed* is usually spelled in one of three ways. As shown below, only one such word ends in *-sede,* only three end in *-ceed,* and the others end in *-cede.*

supersede	exceed	accede
	proceed	concede
	succeed	intercede
		precede

6.8. Endings *-ible* and *-able*

If you are not sure whether a word ends in *-ible* or *-able,* look it up in chapter 8.

6.9. Doubled Consonants

There is no firm rule about whether to double a single consonant following a single vowel at the end of a word before adding a suffix beginning with a vowel. For one-syllable words the consonant is almost always doubled (rob, robbed, robber, robbing; kiss, kissed, kisses, kissing). For words of more than one syllable the consonant is usually not doubled unless the accent in the derivative falls on a syllable containing the troublesome consonant or its double (*can*cel, *can*celed, *can*celing, *but* cancel*la*tion; re*fer*, re*ferred*, re*fer*ring, *but re*ference).

Inevitably, however, there are exceptions to both the rules stated above. The derivatives of *bus,* for example, break the rule for one-syllable words (bus, bused, buses, busing). The derivatives of *handicap* run counter to the formulation for words of more than one syllable (handicap, handicapped, handicapping). The Merriam dictionary sometimes gives first spelling preference to a doubled-consonant derivative (programmed) but also approves a single-consonant variation (programed).

Spelling preferences in this guide usually accord with the tendency in American (as opposed to British) usage to use a single consonant in most cases where there is a choice. The first order of preference is the GPO choice if there is one; otherwise, our spelling is taken from Merriam. If Merriam gives a choice, the single-consonant version is generally preferred.

6.10. Indefinite Articles

6.10a. With Consonants and Vowels

The indefinite article *a* is used before a consonant and an aspirated *h;* the article *an* is used before a silent *h* and all vowels except *u* pronounced as in *usual* and *o* pronounced as in *one.*

a historical review	a once-over	an honor
a hotel	a union	an hour
a humble man	an herb, *but* a herbicide	an onion

C05757260

6.10b. With Initials That Begin With a Consonant Sound

When a group of initials pronounced as letters begins with *b, c, d, g, j, k, p, q, t, u, v, w, y,* or *z,* each having a consonant sound, use *a.*

a BGN compilation	a DVD player	a TV program
a CIA position	a GPO *Style Manual* chapter	a UPI dispatch
a DC tax form	a PBS special	a VCR tape

6.10c. With Initials That Begin With a Vowel Sound

When a group of initials pronounced as letters begins with *a, e, f, h, i, l, m, n, o, r, s,* or *x,* each having a vowel sound, use *an.*

an FDA recall	an ICBM silo	an NBC program
an HHS report	an MRV system	an SLBM system

6.10d. With Acronyms

When initials form an acronym that is pronounced as a word, the use of *a* or *an* is determined by the sound, according to the guidance given in section 6.10a.

a HAWK missile	a NASA launch	a UN mission
a MIRV system	an NREM sleep	an UNCTAD report

6.10e. With Abbreviations That Have Variable Pronunciations

If pronunciation of an abbreviation is variable or borders on slang, use the article appropriate to sounding the group of initials as letters.

an AAA battalion, *not* a AAA (pronounced "triple A") battalion
an SLBM system, *not* a SLBM (pronounced "slubbum") system
but
because of entrenched Pentagon and State Department usage: a SLCM (pronounced "slikkum") system

6.10f. With Numerical Expressions

The rule on use of *a* or *an* also applies to numerical expressions and letter-number designators.

an 11-year-old	a onetime winner	an VIII classification
a IV-F category	an Su-20 Fitter aircraft	a MiG-21 Fishbed

6.11. Geographic Names

CIA's authority for the spelling of geographic names is the US Board on Geographic Names (BGN). The official repository of standard spellings of all BGN-sanctioned foreign place names is the GEOnet Names Server of the National Geospatial Intelligence Agency (NGA), which can be found online [redacted]

Refer also to maps or other references issued by [redacted] [redacted] or consult a regional specialist [redacted] Such consultation is automatic when a cartographer is preparing a map to accompany the paper in which the place names appear. Be sure that the spellings of place names in the text of the paper agree with those on the map. If the approved spelling is markedly different from a more familiar and recognizable spelling, the

more familiar spelling should be inserted in parentheses after the place name on the map. In the text, however, use the more familiar spelling, with the other version following it in parentheses at the first reference. In a paper on Tunisia, for example: Gulf of Gabes (Khalij Qabis); Menzel Bourguiba (Manzil Bu Ruqaybah) Shipyard.

Follow [redacted] advice in the use of hyphens and apostrophes in transliterations (Anse-d'Hainault, Komsomol'sk, N'Djamena). Diacritical marks used in place names on the map, however, are usually omitted in the text. (See section 6.13.)

6.12. Names and Titles of Persons and Organizations

The DI regional leadership analysts and [redacted] in the Office of Policy Support are the points of contact at CIA for the spelling of foreign personal names. CIA normally follows the Intelligence Community transliteration standards developed under the DNI Foreign Language Program Office. Current standards for personal names exist for Arabic, Hindi/Urdu, Iranian Farsi and Afghan Dari, Korean, and Russian, with an additional set available for Cyrillic Slavic languages (Belarusian, Bulgarian, Macedonian, Serbian Cyrillic, and Ukrainian). Other standards are currently in development.

At times, a prominent foreigner expressly indicates a preference for, or the media or official documents regularly use, a spelling of his or her name that differs from the IC transliteration standard. In such cases, CIA uses the alternative spelling—for example, former President Mohammed Hosni Mubarak of Egypt. For assistance in the spelling of names and titles of foreigners, consult either [redacted] in the Office of Policy Support or the appropriate regional leadership analyst, or, if the person in question is a government leader, refer to *Chiefs of State and Cabinet Members of Foreign Governments*, available online at [redacted]

6.13. Diacritical Marks

Diacritics are used on maps and in *The World Factbook* but not in other intelligence writing.

6.14. Transliteration Guidance

Under the guidance of the DNI Foreign Language Program Office, the Intelligence Community has approved standards for the transliteration into the Latin alphabet of personal names originally rendered in a language that uses another alphabet. The transliteration standards are an agreed-upon set of symbols to represent non-Latin alphabets. They are not meant to be a pronunciation guide, and they assume that the audience does not know the foreign language. They are designed to be easy to apply, readable, and recognizable to the educated English reader. As a result, transliterated names may contain ambiguities (for example, "Samir" may refer to two distinct Arabic names). IC guidelines require that variant transliterations for an individual already encountered be noted in parentheses or footnotes in order to ensure that vital forensic information is not lost.

For transliteration of place and personal names, consult first the authorities named in sections 6.11 and 6.12.

It is mandated that these standards be used in official intelligence reports and finished intelligence products. Other standards may be employed in other cases (for example, technical standards for transcription), although widespread use of the IC standards may help facilitate name retrieval and linkage.

When names of individuals from cultures outside the language in question are encountered (for example, "Hillary Clinton" appearing in Russian Cyrillic), use the established spelling for that person's culture rather than transliteration.

For organizational names, transliterate proper nouns according to the IC standards. Translate common nouns and other words: for example, Al-Nakhl Sugar Company, *not* Sharikat al-Nakhl lil-Sukkar or Palms Sugar Company. For well-known entities, use the established English name and spelling: for example, Arab League.

For terms that are not personal or place names, adhere to the following guidance: use the IC standard for terms not translated into English, as in intifada. Use the dictionary spelling for words in general use in English, as in minaret. If there is a good English translation of a word, use it: pilgrimage, *not* hajj, for example.

C05757260

§ 7. COMPOUND WORDS

7.1. General Rules

When an idea cannot be expressed in a single word, we use a compound—the combination of two or more words—to express the thought. A compound can be created by writing the words in unconnected sequence, by hyphenating them, or by connecting them to form a solid, single word. This chapter summarizes various rules governing the formation of compounds. Chapter 8 lists thousands of compounds, so look there if you need to find the preferred spelling of a particular one.

7.1a. Separate Words

One may write two words in sequence, without connecting them with a hyphen or merging them into a single word, if this formulation causes no ambiguity in sense or difficulty of comprehension.

blood pressure	living costs	real estate
eye opener	music teacher	word combination

7.1b. Joined or Hyphenated

Often, words have to be joined into a solid form or connected with a hyphen to express an idea that would not be as clear if they were not so compounded.

18-year-olds	bookkeeping	need-to-know	right-of-way
afterglow	cross-reference	newsprint	whitewash

Derivatives of a compound usually retain the hyphenated or solid form of the original.

coldbloodedness	footnoting	praiseworthiness	stick-to-it-iveness
cost-effectiveness	ill-advisedly	railroader	X-rayed

7.2. Solid Compounds

7.2a. Combinations of Nouns

When two nouns form a compound that then has a primary accent, it is written solid (joined without a hyphen), especially when the prefixed noun consists of only one syllable or when one of the elements loses its original accent.

bathroom	bookseller	pipeline

C05757260

7.2b. Combinations of Verbs and Adverbs

A noun formed by combining a short verb and an adverb is usually written solid, but it is hyphenated when the solid form risks misinterpretation. The verb (v) forms of such combinations usually remain two words.

buildup (v build up)	giveaway (v give away)	setup (v set up)
cut-in (v cut in)	run-in (v run in)	tie-in (v tie in)

7.2c. Compounds Beginning With Certain Nouns

Compounds beginning with the following nouns are usually solid.

book (bookstore)	house (housekeeping)	shop (shopworn)
eye (eyeglasses)	school (schoolteacher)	work (workday)

7.2d. Compounds Ending With Certain Words

Compounds ending in the following words are usually solid when the prefixed word consists of one syllable, but are less often so written when the prefixed word has several syllables (spaceborne, *but* satellite-borne, helicopter-borne).

boat (rowboat)	man (lobsterman)	time (halftime)
book (textbook)	master (harbormaster)	ward (homeward)
borne (spaceborne)	mistress (choirmistress)	way (seaway)
bound (landbound)	owner (homeowner)	wide (worldwide)
hearted (halfhearted)	person (salesperson)	wise (edgewise)
holder (shareholder)	piece (mouthpiece)	woman (chairwoman)
house (boathouse)	power (airpower)	work (artwork)
keeper (beekeeper)	proof (blastproof)	worker (pieceworker)
light (moonlight)	room (chartroom)	working (woodworking)
like (boxlike)	shop (toolshop)	writer (speechwriter)
maker (steelmaker)	tight (airtight)	yard (shipyard)

7.2e. Any, Every, No, *or* Some *Combined With* Body, Thing, Where, *or* One

Write solid a combination of *any*, *every*, *no*, or *some* and *body*, *thing*, or *where*. When *one* is the second element, write as two words if the meaning is a particular person or thing; to avoid mispronunciation, write *no one* as two words at all times.

anybody everything nowhere someone

but

Some one choice must be made, and any one of you can make it. Will no one volunteer?

7.2f. Self or Selves

Pronouns ending in *self* and *selves* are always solid compounds.

herself	oneself	themselves
itself	ourselves	yourself

C05757260

7.2g. Compass Directions

Write as one word a compass direction consisting of two points, but use a hyphen after the first point when three points are combined.

northeast north-northeast

7.3. Unit Modifiers

A unit modifier functions as an adjective. It contains more than one word but acts on the noun it modifies as a unit. Examples are civil defense plan, wholly owned subsidiary, policymaking level, and most-favored-nation clause. Unit modifiers always precede the word they modify; if a modifier is located elsewhere in the sentence, it cannot be a unit modifier.

Unit modifier: The Secretary of State occupies a policymaking position.
Not a unit modifier: A decision is policy making only if effective.

If the modifiers are coordinate (see section 5.6b) or cumulative—that is, if either word could serve as a single modifier—they do not constitute a unit modifier. In "migrant construction workers," for example, the modifiers are cumulative because *migrant* or *construction* alone could modify *workers*. In "40-horsepower engine," however, neither *40* nor *horsepower* could logically serve as a single modifier. In "carefully prepared report" only the second word could modify *report*. Both of these phrases are unit modifiers.

7.3a. Hyphenated

Unit modifiers immediately preceding the word or words modified are usually hyphenated but sometimes are written as one word.

1-meter-diameter pipe	low-priced model	Six-Day War
4-percent increase	most-favored-nation clause	Third Five-Year Plan
drought-stricken area	number-one priority	UN-initiated talks
English-speaking nation	part-time job	US-owned property
high-level post	policymaking level	value-added tax
longtime friend	rightwing group	well-known name

7.3b. Unhyphenated

When the meaning is clear and readability is not aided, hyphens may be omitted from a compound that precedes the word modified, especially if the compound is an established or familiar phrase. But refrain from an accumulation of modifiers that defies comprehension and impedes readability.

atomic energy program	flight test program	human rights position
ballistic missile submarine	free enterprise system	life insurance company
civil defense plan	ground attack aircraft	natural gas exports
current account deficit	hard currency loan	surface ship deployment

but

no-hyphen rule (readability aided; *no hyphen rule* would be ambiguous)

areas in which ballistic missile submarines normally operate (readable); *not* normal ballistic missile submarine operating areas (difficult to comprehend)

ballistic missile early warning radar (established use)

C05757260

7.3c. With Ordinal Numbers

In general, the omission of hyphens is not recommended in a compound containing an ordinal number used in its literal sense, no matter how familiar and frequent the expression.

first-quarter report	second-half performance
fourth-grade class	third-country involvement
but	
first aid station	Third World delegates

Similarly, in a unit modifier containing a prepositional phrase, comprehension is enhanced if hyphens are used for even the best known expressions.

balance-of-payments problem	right-to-work law
cost-of-living study	under-the-counter sales

No hyphen is required if the compound preceding the word or words modified is already tied together with a conjunction.

cold but sunny day	medium and high altitude
command and control echelons	middle or late 1970s

An improvised compound (euphemism for cliche) such as that in "hard-and-fast rule" or "bread-and-butter issue" is an exception (see section 7.6c).

7.3d. Predicates

A unit modifier must be distinguished from a compound predicate adjective, in which the hyphen is usually omitted.[34]

His future was *still undetermined* while he was a student.
Most of the transactions in that deal were *foreign financed*, and the exchanges were *under the counter*.
The talks were *US initiated*, and the agenda *well prepared*.
The increase was *4 percent* in 2008 and *5 percent* in 2009.
The majority of the population was *English speaking*.
The government has been *socialist leaning* in recent years.

7.3e. Comparatives and Superlatives

The hyphen is usually—although not always—omitted in a two-word unit modifier in which the first word is a comparative or superlative. For clarity's sake, however, it should be retained in certain three-word modifiers.

best liked books	less developed countries	lowest priced model
highest level meeting	lower income group	worst case scenario
but		
bestselling novel (derived from *bestseller*)	lighter-than-air craft	
higher-than-market price	most-favored-nation clause	
lighter-colored paper	most-sought-after tickets	

[34]In this sense, do not confuse a unit modifier with a hyphenated compound formed by adding a prefix or suffix (see sections 7.4b to 7.4g). Such a compound (for example, *self-educated* or *rent-free*) would retain its hyphen in the predicate form. Also, note that entries in chapter 8 labeled *um* (unit modifier) generally conform to section 7.3d, but entries labeled *adj* (adjective) do not. *Was the call local or long-distance? This approach was low-key.*

C05757260

7.3f. Adverbs Ending in -ly

Do not use a hyphen in a two-word unit modifier in which the first word is an adverb ending in *-ly*.

recently designed logo	wholly owned subsidiary
but	
lonely-hearts club	only-child complex

7.3g. Three-Word Modifiers

Do not use hyphens in a three-word unit modifier in which the first word is an adverb modifying the second word.

unusually well preserved specimen	very well defined line	
exceptions		
extremely-low-frequency communications	very-high-frequency broadcasts	very-low-frequency transmissions

If the first word of a three-word unit modifier modifies the other two, the hyphen is used between those two.

a formerly well-known person	a nearly right-angle bend	a virtually self-educated man

7.3h. Foreign Phrases

Do not use a hyphen in a unit modifier consisting of a phrase of foreign origin.

bona fide transaction	ex officio member	per capita tax
carte blanche policy	per diem allowance	prima donna behavior

7.3i. Proper Nouns

Do not use a hyphen in a compound proper noun or in a capitalized coined name used as a unit modifier, in either its basic or derived form.

Cold War tensions	Latin American states
French Revolutionary period	World War II period

Do, however, use one if the proper noun is normally a combined form.

Afro-American program	French-English descent
Franco-Prussian War	Indo-Pakistani relations

This rule does not apply to numerical compounds in an expression such as *Fifth Five-Year Plan*, nor would it apply entirely in an expression incorporating an already-hyphenated coined name (*Six-Day War euphoria*).

7.3j. En Dash in Proper Noun Compounds

In a unit modifier made up of proper adjectives or proper nouns of which one or more is a compound, the en dash is used between the parts.

North American–South American sphere
Dominican Republic–Haiti border
Ulan-Ude–Chita–Ulaanbaatar triangle

C05757260

7.3k. Quotation Marks

Do not use a hyphen in a unit modifier enclosed in quotation marks unless it is normally a hyphenated form, and do not use quotation marks in lieu of hyphens.

a "spare the rod" approach to parenthood
the "one-man woman" plots of many operas
a "damn it all" attitude toward writing style

7.3l. Chemical Terms

The hyphen is not used in a unit modifier composed of chemical terms.

carbon monoxide poisoning

7.3m. Letter or Number Elements

Do not use a hyphen in a unit modifier containing a letter or numeral as its second element (*but* see section 7.6e).

annex B maps	level 4 alert	Proposition 13 backlash
Article III provisions	Mod 3 missile	Type 59 tank
grade A milk	number 2 fuel oil	

This rule does not, however, apply to certain terms established by long usage for military aircraft and naval ships.

An-22	MiG-19	Su-7
Kresta-I	Osa-II	Yak-40

7.3n. Common Basic Elements

When two or more hyphenated compounds have a common basic element and this element is omitted in all but the last or first term, the hyphens are retained.

the British- and French-produced Concorde	two- or three-year period
first-, second-, and third-grade students	US-owned and -operated companies
ground- and air-launched missiles	

but

firsthand and secondhand (*not* first- and secondhand)
twofold or threefold (*not* two or threefold)
oil and gas fields, or oilfields and gasfields (*not* oil and gasfields)
mid- and late 1990s (*but* mid-to-late 1990s)[35]
early or mid-1990s (*but* early-to-mid-1990s,[35] *better:* early-to-middle 1990s)

[35]Use of the hyphenated prefix *mid-* in the examples shown is not incorrect, but the hyphen makes it awkward to combine *mid-* with the other, unhyphenated elements, *early* and *late*. For this reason it is recommended that *middle* rather than *mid-* be used when a combination is involved: middle and late 1990s, early and middle 1990s, early or middle 1990s, early-to-middle 1990s.

C05757260

7.4. Prefixes and Suffixes

7.4a. Unhyphenated

Prefixes other than *ex, self, quasi,* and *vice* and suffixes other than *free, designate,* and *elect* usually form a solid compound with a noncapitalized word.

afterhours	clockwise	multicolor	semiofficial
antedate	counterintelligence	neofascist	subcommittee
antiaircraft	fourfold	nonferrous	transship
biweekly	hydroelectric	northward	ultramodern
byproduct	lifelike	partnership	unofficial

7.4b. Hyphenated[36]

A hyphen is used in compounds formed with the prefixes and suffixes noted as exceptions in the preceding section.

ex-serviceman	rent-free
minister-designate	self-control
President-elect Jones	vice-chairmanship (*but* vice chairman)
quasi-academic	

7.4c. Doubled Vowels or Tripled Consonants

Except after the short prefixes *co, de, pre,* and *re,* which are generally written solid, a hyphen is used to avoid doubling a vowel when adding a prefix or tripling a consonant when adding a suffix.

anti-inflation	hull-less	shell-like	
brass-smith	semi-independent	ultra-atomic	
but			
cooperation	nonnuclear	posttreatment	reestablishment
deemphasize	overreact	preelection	subbasement

7.4d. To Avoid Confusion

A hyphen is used with a prefix that normally forms solid compounds if omission of the hyphen would lead to mispronunciation or cause confusion with a word spelled identically but without a hyphen.

co-op (*but* cooperative)	re-cover (cover again)	re-treat (treat again)
multi-ply (several plies)	re-create (create again)	under-ice
pre-position (position in advance)	re-form (form again)	un-ionized
pro-state	re-present (present again)	

[36]The hyphenated compounds discussed in sections 7.4b through 7.4g are not subject to the rule in section 7.3d and would retain their hyphens in the predicate form.

C05757260

7.4e. Duplicated Prefixes

A hyphen is used to join duplicated prefixes.

counter-countermeasures sub-subcommittee

7.4f. Prefixes or Suffixes in Compounds With Capitalized Words

A hyphen (unless an en dash is called for) is used to join a prefix or a suffix in a compound with a capitalized word.[37]

Africa-wide	neo-Nazi	pro-British
anti-Castro	pre-Renaissance	un-American
exceptions		
nonMIRVed	unMIRVed	
en dash called for		
Latin America–wide	pre–World War II	

7.4g. Unit Modifier Containing a Multiword Compound

A prefix (except *un*) normally forming a solid compound is often followed by a hyphen when joined with a two-word or hyphenated compound to form a unit modifier.

anti-guided-missile	non-nuclear-powered	pre-martial-law
non-missile-equipped	post-target-tracking	semi-land-mobile
but		
antiballistic missile	uncalled-for	unself-conscious

For many of the terms used above to illustrate the rule in this section, rephrasing of the sentence might be preferable to insertion of the extra hyphen.

defense against guided missiles (instead of anti-guided-missile defense)
aircraft not equipped with missiles (instead of non-missile-equipped aircraft)
a system that is partially land mobile (instead of a semi-land-mobile system)

Do not insert a hyphen after a prefix joined to a solid (unhyphenated, one-word) compound.

antigunrunning	nonoceangoing	submachinegun
nonlifelike	postreentry	ultrarightwing

7.5. Numerical Compounds[38]

7.5a. Spelled Out

Use a hyphen between the elements of compound numbers from 21 to 99 when they must be spelled out (bear in mind that figures, rather than spelled-out words, are generally used for numbers of two or more digits).

twenty-one	ninety-nine	one thousand one hundred forty-one
twenty-first	one hundred forty-one	

[37]For similar reasons, retain the hyphen if it is part of an established formal name such as Non-Proliferation Treaty (abbreviated NPT) and Multi-Fiber Arrangement (MFA), even though the spelling differs from our normal style (nonproliferation, multifiber).
[38]See chapter 2.

C05757260

7.5b. Adjective Compounds With Numerical First Element

10- to 20-year period (*or* 10-to-20-year period)
18-year-old student
20th-century progress
3-meter (*never* 3-m) railing
5-to-4 vote
8-kilogram (*or* 8-kg) turkey
but
$20 million loan
eight-time Olympic medalist
medium-to-high altitude
medium-to-high-altitude interceptors
multimillion-dollar loan
the Six-Day War
Third Five-Year Plan

7.5c. Fractions

Use a hyphen between the elements of a fraction whether it is a noun or an adjective.

a two-thirds majority
two-thirds of the legislature

7.6. Other Compound Words

7.6a. Titles

Do not use a hyphen in a compound title denoting a single civil or military office, but do use one in a double title.

ambassador at large
commander in chief
editor in chief
but
under-secretaryship
manager-director
minister-counselor
secretary general
vice-presidency
secretary-treasurer
under secretary
vice president

7.6b. Noun Compounds Containing a Prepositional Phrase

Apart from titles, hyphens are used in some noun compounds containing a prepositional phrase.

government-in-exile
grant-in-aid
but
next of kin
prisoner of war
man-of-war
mother-in-law
state of the art
state of war

7.6c. Improvised Compounds

bread-and-butter issue
classroom full of know-it-alls
first-come-first-served basis
hard-and-fast rule
need-to-know
technical know-how

7.6d. Verb Forms of Noun Forms Written as Two Words

turn a cold shoulder (to cold-shoulder an idea)
proof with blue pencils (to blue-pencil galleys)
missile in flight test (to flight-test a missile)

C05757260

7.6e. Single Capital Letter Plus a Noun or Participle

H-bomb	L-shaped room	T-shaped
I-beam	T-jetty	X-ray

Use hyphens (*not* en dashes) in the compounds designating Russian submarine classes when the compounds are used adjectively.[39] If the meaning is clear, refer to these submarines by the class designator alone.

Yankee-class, Delta-class, Victor-class, etc.
Echo-II-class, Charlie-I-class (two hyphens, *not* hyphen and en dash)
submarines of the Yankee class (no hyphen)
a Delta-class unit, a Delta-II-class unit
Delta and Yankee units (acceptable to omit word *class*)
a Victor tracking a Yankee
Four Yankees, two Delta-IIs, and a Victor have been observed in the submarine yard.
The characteristics of the Delta-I and -II were compared.

The same rules apply essentially to surface ship classes (Komar, Osa) and non-Russian submarine classes (Han, Xia).

[39]In CIA publications the full designator, not just its first letter, is preferred: Delta-class (*not* D-class), Yankee-class (*not* Y-class). Note, however, that the designator is spelled with only the first letter capitalized, not in all capital letters, as seen in military usage. Designators for Russian submarines, according to DIA, are as follows: Akula, Alfa, Bravo, Charlie, Delta, Echo, Foxtrot, Golf, Hotel, India, Juliet, Kilo, Lima, Mike, November, Oscar, Papa, Romeo, Sierra, Tango, Typhoon, Uniform, Victor, Whiskey, Yankee, and Zulu. (All are phonetics except Akula and Typhoon.)

C05757260

§

8. SPELLING AND COMPOUND WORDS LIST

Including inflections, plurals, and other word forms, there are more than 13,000 words listed in this chapter. Many are familiar and are not likely to cause a problem for any writer. Others may be unfamiliar or confusing.[40] Rules for spelling and compounding may be found in chapters 6 and 7, but if you want only to determine the correct spelling or compound form of a word or phrase, you are likely to find your answer below. Note that a word followed by (*s*) (antibiotic[s]) and marked as both *n* and *adj* or *um*, takes the *s* only in the noun form. Similarly, if a word is shown with several inflections (airmail[s], airmailed, airmailing) and is marked as both *n* and *v*, usually only the first form (airmail[s]) is the noun, although sometimes the present participle is also a noun (back[s], backed, backing) or an adjective (wind[s], wound, winding).

adj (adjective)	**masc** (masculine)	**prep** (preposition)
adv (adverb)	**n** (noun or modified noun)	**sing** (singular)
cf (combining form)	**pl** (plural)	**syn** (synonym)
comp (computer term)	**pred** (predicate)	**um** (unit modifier)
fem (feminine)	**pref** (prefix)	**v** (verb)

C05757260

A

aberration(s)

able-bodied (um)

ABM (antiballistic missile) **system**

about-face

above-average (um)

aboveboard

abovedeck

aboveground (um)

above water (pred)

abridgment(s)

absentminded

accede(s), acceded, acceding

access code(s)

accessible

access time(s)

accommodate(s), accommodated, accommodating

accommodation(s)

accords (Amman, Camp David, Dayton, Geneva, Helsinki, Paris)

accoutrement(s)

Achilles' heel(s)

acknowledgment(s)

acoustic (adj)

acoustic(s) (n)

acquiesce(s), acquiesced, acquiescing (takes preposition *in*, not *to*)

across-the-board (um)

active-duty (um)

A.D. (*anno domini*, refers to years since the birth of Christ; see *B.C.*)

adapter(s)

addendum, addenda (pl)

additionally (adv, of addition; do not use for *in addition*)

add-on(s) (n)

ad hoc

adjutants general

ad lib (adv)

ad-lib(s) (n, adj, v), **ad-libbed, ad-libbing**

admissible

advertise(s), advertised, advertising

advertisement(s)

advice (n)

advise(s), advised, advising

adviser(s); advisor (used in the legal field and by others by preference)

advisory

aegis

aesthetic(s) (n, adj)

affect(s), affected, affecting (v, influence; see *effect*)

affection(s) (n, fondness)

affectation(s) (n, insincere attitude)

A-frame(s)

Africa-wide

Afrikaans

after (cf, all one word)
- aftereffect
- afterglow
- afterward

agenda(s)

agents-of-influence

age-old

aging

agitprop

agree(s), agreed, agreeing (*with* a person, *to* a proposal, *on* a plan)

agreed-to (um)

agreed-upon (um)

agribusiness

agro (cf, all one word)
- agroindustrial

aid(s) (n, assistance)

aid(s), aided, aiding (v, assist)

aide(s) (n, assistant)

aide(s)-de-camp

aide-memoire, aides-memoires (pl) (memory jog)

AIDS (acquired immunodeficiency syndrome)

aim point(s)

air and sea ports

C05757260

airbag(s)
airbase(s)
air-based (um)
airblast(s)
airborne warning and control system (AWACS) aircraft
air-breathing
airburst(s)
aircargo(es)
air-condition(s), air-conditioned, air-conditioning
air-conditioner(s)
air cover(s)
aircraft
air crash(es)
aircrew(s)
air-cushion vehicle(s) (ACV[s])
air defense(s) (n, um)
air-dried (um)
airdrop(s), airdropped, airdropping (n, v)
airdroppable
airfield(s)
air fleet(s)
airflow(s)
airframe(s)
air-handling (um)
air intercept(s) (n, um)
airland(s), airlanded, airlanding
air-launched (um)
airlift(s), airlifted, airlifting (n, v)
airlink(s)
airmail(s), airmailed, airmailing (n, v)
airman, airmen (pl)
airmass(es)
airmobile (adj)
airpower
but
naval and air power
air quality (n, um)
air raid(s)
air show(s)
airspace(s)
airspeed(s)
airstrike(s)
but
naval and air strike(s)
airstrip(s)
airtight
air time(s) (broadcast media)
air vent(s)
air war(s)
airwave(s)
airway(s)
airworthy
alias(es)
align(s), aligned, aligning
alignment(s)
all-absorbing (um)
all-around (um)
all-clear(s) (n, um)
all-day
Alliance, Allied, Allies (in reference to NATO, otherwise lowercase)
all-inclusive (um)
all-knowing (um)
allot(s), allotted, allotting
allotment(s)
all-out
all ready (prepared; see *already*)
all right
all-round (um)
all-source (adj)
all-star(s)
all time(s) (n, full time)
alltime (adj)
all together (collectively, in unison; see *altogether*)
all-weather
alongside
a lot (never *alot*, even if you do often see that form elsewhere)
alphanumeric
already (previously; see *all ready*)
also-ran(s)

C05757260

alter ego(s)

alternate(s), alternated, alternating (n, v rotating, following by turns)

alternative(s) (n, adj; pertains to a choice between possibilities)

altogether (completely; see *all together*)

a.m.

alumna, alumnae (pl) (fem)

alumnus, alumni (pl) (masc)

ambassador(s) at large

Ambassador-designate

ambi (cf, all one word)
ambidextrous

American-flag (Liberian-flag, Yemeni-flag) **ship**
but
in a naval context, US flagship

amidships

amino (as prefix, all one word)

amino acid(s)

among (use when the relationship of more than two things is vague or collective)

amorphous

analog(s) (comp)

analogue(s) (all other meanings)

analysis, analyses (pl)

analytic (adj)

analyze(s), analyzed, analyzing

anchorperson(s)

anemia(s)

anesthetic(s) (n, adj)

aneurysm(s)

anglophone (adj)

Anglophone(s) (n)

annul(s), annulled, annulling

annulment(s)

anomalous

antedate(s), antedated, antedating

antenna(s)

antennae (pl, zoology only)

anti (pref, usually one word)
antiaircraft
antiapartheid
antiballistic missile(s) (n, um, ABM)
antibiotic(s) (n, adj)
antichrist(s)
antidefense
antiestablishment
antigunrunning
antimissile
antiradiation
antiradiation-homing (adj)
antiship cruise missile (n)
antitank guided missile(s) (n, ATGM)
antivirus program
antiwar
but
anti-American
anti-arms-control
anti-cruise-missile(s) (n, um)
anti-guided-missile (um)
anti-imperial
anti-inflation
anti-inflationary
anti-insurgent
anti-money-laundering (um)
anti-nuclear-weapons
anti-Semite(s)
anti-Semitic
anti-Semitism
antiship-cruise-missile (um)
anti-submarine-warfare (um)
anti-tactical-ballistic missile(s) (n, ATBM)
anti-tactical-ballistic-missile (um)

antipathy, antipathies (pl)

anybody

anyone

any time

anyway (adv)

APEC (Asia Pacific Economic Cooperation)

apocalypse(s)

appall(s), appalled, appalling

apparatus(es)

appealing

appendix B

appendix(es)

apprehensible

April Fools' Day

a priori

A-priority (or priority A)

Arab-Israeli war

arched-roof (adj)

C05757260

archenemy, archenemies (pl)
archeology
archrival(s)
arch-roofed (um)
archetypal
archetypally
archetype(s)
arise(s), arose, arising, arisen
armor-heavy (um)
arms control(s) (n)
arms-control (um)
arms-exporting (um)
arm's-length (um)
armsmaker(s)
arms-producing (um)
arms-supplying (um)
arm-twisting (n)
army-group-level (um)
armywide
Army-wide
around-the-clock (um)
artificial intelligence
artificial language(s)
artilleryman, artillerymen (pl)
artwork(s)
ascend(s), ascended, ascending
ascendancy, ascendancies (pl)
ascendant
ascent(s) (rise, climb; see *assent*)
ASCII (American Standard Code for Information Interchange)
Asia Pacific Economic Cooperation
but
Asia-Pacific region
assassinate(s), assassinated, assassinating
assassination(s)
assembly line(s)
assemblyman, assemblymen (pl)
assemblywoman, assemblywomen (pl)
assent(s), assented, assenting (consent; see *ascent*)
assistant comptroller(s) general
assure(s), assured, assuring (affirm; see *ensure, insure*)
asylee(s) (person seeking asylum or one given asylum)
ATBM(s) (anti-tactical-ballistic missile)
at-large (um)
atomic energy, atomic energies (pl) (n, um)
at-sea (um)
attache(s)
attorney(s) general
audible
audiocassette(s)
audiosurveillance(s)
audiotape(s)
audiovisual(s) (n, adj)
auger(s) (n, hole-boring tool)
augur(s), augured, auguring (v, predict from signs or omens)
automaker(s)
autoworker(s)
auxiliary, auxiliaries (pl)
AWACS (airborne warning and control system)
avant-garde
a while (n, a period of time)
awhile (adv, for a time)
ayatollah(s)
ax, axes (pl)
axis, axes (pl)

B

B.A. (bachelor of arts)
baby boomer(s)
bachelor's degree(s) (B.A.[s])
back(s), backed, backing (n, v)
backbench(es)
backbencher(s)
backbite(s), backbit, backbiting
backbiter(s)
backbone(s)
back burner(s)

C05757260

back-channel (um)
backdoor (um)
back(s) down, backed down, backing down
backfit(s), backfitted, backfitting (n, v)
background processing
backlash(es)
back pay
backpedal(s), backpedaled, backpedaling
backroad (um)
backroom (um)
backseat(s) (n, um)
backslide(s), backslid, backsliding
backstage
backstop(s), backstopped, backstopping (n, v)
backtrack(s), backtracked, backtracking
back(s) up, backed up, backing up
backup(s) (n, um)
backup system(s)
backward (no s)
backwater(s)
backyard (um)
bagful(s)
Bahamas, The
Bahamian (n, adj)
bail(s) out, bailed out, bailing out
bailout(s) (n, um)
balance-of-payments (adj)
Balkanize(s), Balkanized, Balkanization
ball bearing(s)
ballistic missile (um, of submarines, defense, radar)
ballistic missile early warning (BMEW) radar(s)
ballistic-missile-related (um)
ballistic missile submarine(s) (SSB)
ballpark(s) (n, adj)
Baltic republics/states (not *the Baltics;* citizens are referred to as *Estonians, Latvians,* or *Lithuanians,* not *Balts*)
bandwagon(s)
bandwidth(s)
banknote(s)
bankrupt(s), bankrupted, bankrupting
bar code(s)
barebones (um, nonliteral)
base camp(s)
baseline(s)
basis, bases (pl)
battalion(s)
battlefront(s)
battleground(s)
battle group(s)
battleline(s)
battle management (n, um)
battle readiness
battle-ready (um)
B.C. (before Christ, comes after the number; see *A.D.*)
beam width(s)
Bear G('s) (Russian aircraft)
bedouin (sing, pl)
bed rest
bedrock (n, adj)
behind-the-scenes (adj)
belowground
below-market (um)
belt-tightening (um)
beltway bandit(s)
benchmark(s) (nonliteral)
beneficent
benefit(s), benefited, benefiting (n, v)
Benelux
Berlin Wall (the Wall)
beside (alongside)
besides (except, other than)
best seller(s)
bete noire, betes noires (pl)
better-than-even (um)
biannually (prefer *semiannually*, but *consider* replacing with *twice a year*; see *biennially*)
bias(es), biased, biasing (n, v)
biennially (consider replacing with *once every two years*; see *biannually, semiannually*)
big-power (adj)
big shot(s)
big-ticket (adj)

C05757260

binary system(s)
binational
bipolar
birder
bird's-eye (adj)
birdshot
birdwatch(es), birdwatched, birdwatching
birthdate
birthplace(s)
birthrate(s)
bistatic
bitmap(s), bitmapped, bitmapping (n, v)
bitmapped (um)
biweekly (once every two weeks; see *semiweekly*)
blacklist(s), blacklisted, blacklisting (n, v)
blackmail(s), blackmailed, blackmailing (n, v)
black market(s) (n)
black-market(s), black-marketed, black-marketing (um, v)
black-marketeering (n)
black-marketer(s)
blastmark(s)
blastproof
blind eye(s)
blitzkrieg(s)
bloc(s) (group)
block(s) (form)
blog(s) (n, short for weblog)
blog(s), blogged, blogging
blogger(s)
blond(s) (masc, fem)
bloodbath(s)
bloodletting(s)
bloodlust
blood pressure(s)
bloodshed
bloodthirsty
blowdown(s)
blow(s) out, blew out, blowing out (v)
blowout(s) (n, adj)
blue chip(s) (n)
blue-chip (um)
blue-collar (nonliteral, um)
blue-pencil(s), blue-penciled, blue-penciling (v, um)
blueprint(s)
blue-ribbon (nonliteral, um)
blue-water navy, blue-water navies (pl)
boardroom(s)
boatbuilding
boathouse(s)
boatload(s)
boat people
boatyard(s)
body bag(s)
bodyguard(s)
body politic
Boeing 747(s)
boilerplate
boldface
bomb bay(s)
bombdrop(s)
bomb load(s)
bombmaker(s)
bombmaking
bombproof
bombsight(s)
bombsquad(s)
bona fide (adj)
bona fides (n, sing, pl)
boobytrap(s), boobytrapped, boobytrapping (n, v)
bookkeeper(s)
bookkeeping
bookmark(s), bookmarked, bookmarking (n, v)
bookseller(s)
bookstore(s)
Boolean logic
boot camp(s)
bootleg software
border guard(s) (n, um)
borderland(s)
borderline(s)

C05757260

border post(s)
boresight(s)
born (given birth)
born-again (n, adj)
borne (carried)
bottleneck(s)
bottom line(s) (n)
bottom-line (adj)
bourgeois (adj)
bourgeoisie(s) (n)
boxcar(s)
boxlike
brain child, brain children (pl)
brain trust(s)
brainwash(es), brainwashed, brainwashing
brand name(s) (n, um)
breach(es) (gap; see *breech*)
bread-and-butter (adj)
breadbasket(s)
break(s) down, broke down, breaking down
breakdown(s) (n, um)
break(s) even, broke even, breaking even
break-even (um)
break(s) in, broke in, breaking in
break-in (n)
break(s) out, broke out, breaking out
breakout (n, um)
breakpoint(s)
breakthrough(s)
break(s) up, broke up, breaking up
breakup(s) (n, um)
breathtaking
breech(es) (lower part, part of a gun barrel; see *breach*)
breeding ground(s)
bridgebuilder(s)
bridgehead(s)
bridgeway(s)
bridgework(s)
briefcase(s)
brinkmanship
broadband (n, adj)
broad-based
broadcast(s), broadcast, broadcasting (n, adj, v)
broadcloth(s)
broad gauge(s) (n)
broad-gauge (adj)
broadleg(s) (n, adj)
broadminded
broken-down (um)
brother(s)-in-law
brunet(s) (masc, fem)
brushpass(es)
budget-busting (um)
building block(s) (n)
building-block (adj)
build(s) up, built up, building up
buildup(s) (n)
built-in(s) (n, adj)
built-up (um)
bulletin board(s)
bulletproof
bullheaded
burdensharing
bureau(s)
burgeoning
burka(s)
burn bag(s)
burnout(s) (n)
burnup(s)
bus(es), bused, busing (n, v)
busdriver(s)
busfare(s)
businesslike
busline(s)
busload(s)
busting (used in terms like budget busting and trust busting; hyphenate as a um)
buy-back (um)
buy(s) in, bought in, buying in
buy-in (n, adj)
buy(s) out, bought out, buying out

C05757260

buyout(s) (n, um)

buzzword(s)

BW-agent (um)

by (cf, usually one word)
byelection(s)
bylaw(s)
bypass(es)
byproduct(s)

C

cache(s)

caldron(s)

caliber(s)

caliph(s)

caliphate(s)

call(s) back, called back, calling back

callback(s) (n, um)

call(s) in, called in, calling in

call-in (n, um)

call sign(s)

call(s) up, called up, calling up (n, v)

callous (adj, unfeeling; see *callus*)

callup(s) (n, um)

callus(es) (n, thickening of the skin; see *callous*)

camouflage(s)

cancel(s), canceled, canceling

cancelable

cancellation(s)

candor(s)

canister(s)

cannon (pl **cannon** or **cannons**, depending on usage)[41]

cannot

canoe(s), canoed, canoeing (n, v)

canvas(es) (cloth)

canvas-covered (um)

canvass(es), canvassed, canvassing (solicit)

capital(s) (city, money)

capital-intensive (um)

[41]Use *cannon* if such weapons are referred to collectively (*Cannon were deployed on the surrounding hillsides*) but *cannons* when the weapons are discussed individually. (*Wing-mounted cannons, two on each side, augment the aircraft's firepower.*)

capitol(s) (building)

caplet(s)

carat(s) (unit of weight; see *caret*)

carbarn(s)

car-bomb(s), car-bombed, car-bombing (n, adj, v)

carbon footprint(s)

carbon monoxide

carcinogen(s)

carcinogenic

card-carrying (um)

carefree

caret (insertion mark; see *carat*)

car ferry, car ferries (pl)

cargo(es)

Caribbean

carline(s)

carload(s)

car-mile(s)

carpal tunnel syndrome

carrier-based (um)

carrierborne

carry over, carries over, carried over, carrying over

carryover(s) (n, um)

carte blanche, cartes blanches (pl)

cartel(s) (even with specific name)

cartilage(s)

car wash(es)

case-by-case (adj)

caseload(s)

case officer(s)

caseworker(s)

cash-and-carry (adj)

cash-flow(s) (n, adj)

cashier's check(s)

cash-strapped (um)

cast(s) off, cast off, casting off

castoff(s) (n, um)

casual (informal; see *causal*)

casualties (include persons injured, captured, or missing in action, not just those killed)

C05757260

casus belli (sing, pl)
catalog(s), cataloged, cataloging (n, v)
cataloger(s)
cat-and-mouse (um)
catchall(s) (n, um)
catchphrase(s)
catch(es) up, caught up, catching up
catch-up(s) (n, um)
catchword(s)
cat's-paw(s)
cattle breeder(s)
cattleman, cattlemen (pl)
cattle raiser(s)
cattle-raising (um)
cattle ranch(es)
caudillo(s)
causal (of cause; see *casual*)
cause celebre, causes celebres (pl)
causeway(s)
cave(s) in, caved in, caving in
cave-in(s) (n, um)
CD-ROM(s) (compact disk read-only memory)
cease(s) fire, ceased fire, ceasing fire
cease-fire(s) (n, um)
cell phone
Celsius
cementmaking
census taker(s)
census-taking (um)
center(s), centered, centering (as a verb, is used with *on*, *upon*, *in*, or *at*, but not *around*)
center-left
centerline(s)
centerpiece(s)
centerpole(s)
center-right
centi (cf, all one word)
centri (cf, all one word)
chain(s) of command
chainsmoke(s), chainsmoked, chainsmoking
chainsmoker(s)
chairman, chairmen (pl)
chairperson(s)
chairwoman, chairwomen (pl)
chancellery, chancelleries (pl)
chancellor(s)
chancellor-candidate(s)
chancery, chanceries (pl)
changeable
change(s) over, changed over, changing over
changeover(s) (n, um)
channel(s), channeled, channeling (n, v)
chaperon(s)
charge-coupled
charge(s) d'affaires
chartroom(s)
chassis (sing, pl)
chastise(s), chastised, chastising
chastisement(s)
chateau(s)
chauvinism
checkbook(s)
check-clearing (um)
check(s) in, checked in, checking in
check-in(s) (n, um)
checklist(s)
check(s) out, checked out, checking out
checkout(s) (n, um)
checkpoint(s)
checksheet(s)
check(s) up, checked up, checking up
checkup(s) (n, um)
check valve(s)
checkwriting
chef(s) de cabinet
chemical-weapons-free (um)
chemical-weapons-related (um)
cherrypicker(s)
chief(s) of staff
childcare
childlike
chisel(s), chiseled, chiseling (n, v)

C05757260

chiseler(s)
chitchat(s)
chlorofluorocarbons
chokepoint(s)
church(es), the
but
the Catholic Church
churchgoer(s)
churchgoing
CI (um, counterintelligence)
CIALink
c.i.f. (cost, insurance, and freight)
circa
circuit breaker(s)
citable
City, the (London financial district)
city dweller(s)
citywide
civil defense(s) (n, um)
clamor(s)
clamp(s) down, clamped down, clamping down
clampdown(s) (n)
clean(s) up, cleaned up, cleaning up
cleanup(s) (n, um)
clear-cut (distinct)
clearcut(s), clearcut, clearcutting (n, v, forestry)
clearheaded
clearinghouse(s)
clear(s) up, cleared up, clearing up
cleave(s), cleaved, cleaving
clew(s), clewed, clewing (n, v; nautical; see *clue*)
cliche(s)
climactic (climax, highest point)
climatic (of climate, weather)
clip art
clockwise
closed-circuit (um)
closed-door (adj)
close-hold (adj)
close-in (um)
close-knit (um)
closemouthed
close(s) out, closed out, closing out
closeout(s) (n, um)
close-range (um)
close(s) up, closed up, closing up (v)
closeup(s) (n, um)
cloth-backed (um)
clothbound
clothesline(s)
clue(s), clued, clueing (n, v; meanings other than nautical; see *clew*)
co (pref, usually one word)
coauthor(s), coauthored, coauthoring (n, v)
cochair(s), cochaired, cochairing (n, v)
coexist(s), coexisted, coexisting
cofound(s), cofounded, cofounding
cofounder(s)
cooperate(s), cooperated, cooperating
coorbital
coprocessor(s)
coproduction(s)
but
co-deputy-chair(s)
co-op(s)
co-opt(s), co-opted, co-opting
co-optation(s)
co-owner(s)
co-vice-chair(s)
coalbed(s)
coal-black (um)
coalboat(s)
coal car(s)
coalfield(s)
coal gas(es)
coal-laden (um)
coal mine(s) (n)
coal-mining (um)
coalpit(s)
coal-slurry (um)
coast guard(s)
coastline(s)
coca grower(s), coca growing (n)
coca-growing (um)
cocaine(s)
c.o.d. (cash on delivery)
codename(s)

C05757260

codeword(s)

coffee grower(s) coffee growing (n)

coke oven(s)

coldblooded

coldbloodedness

cold-roll(s), cold-rolled, cold-rolling

cold shoulder(s) (n)

cold-shoulder(s), cold-shouldered, cold-shouldering

Cold War

collapsible

collateral

collocate(s), collocated, collocating (to set in a place or to occur in conjunction with something; see *colocate*)

colloquy, colloquies (pl)

colocate(s), colocated, colocating (to locate together; see *collocate*)

color(s), colored, coloring (n, v)

combat(s), combated, combating (n, v)

combatant(s)

combat-capable (um)

combat-ready (um)

combat support (n, adj)

combined-arms (adj)

combustible(s) (n, adj)

comeback(s)

comedown(s)

come-on(s)

comeuppance(s)

command and control

command, control, and communications (C3)

command, control, communications, computers, and intelligence (C4I)

commander(s) in chief

commando(s)

command post(s)

commingle(s), commingled, commingling

commiserate(s), commiserated, commiserating

commit(s), committed, committing

common law(s) (n)

common-law (adj)

commonplace

common sense (n)

commonsense (adj)

commonwealth(s)

communications system(s)

communique(s)

communitywide

Community-wide (IC)

companywide

compatible

compel(s), compelled, compelling

compendium(s)

complement(s), complemented, complementing (n, v, complete)

compliment(s), complimented, complimenting (n, v, praise)

compose(s), composed, composing (to constitute or to make up; see *comprise*)

comprehensible

comprise(s), comprised, comprising (to contain or to consist of; see *compose*)

compromise(s), compromised, compromising (n, v)

computer-generated (um)

computer literate

concede(s), conceded, conceding

concerted (mutually contrived or agreed upon)

conclave(s) (secret meeting, not just any gathering)

concomitant

cone-shaped (um)

confectionery, confectioneries (pl)

confidant(s) (n, one with whom confidences are shared; see *confident*)

confidence- and security-building (um)

confidence-building (um)

confident (adj, self-assured; see *confidant*)

congressional (non-US)

Congressional (US)

con man

connoisseur(s)

consensus(es) (an opinion held collectively, not simply by a majority)

consensus builder

consensus building (n)

C05757260

consensus-building (um)
consortium(s)
constitution(s) (a state's)
Constitution (a country's)
consul(s) (n, foreign service officer; see *council, counsel*)
consul(s) general
consumer price index(es)
consummate
containership(s)
contemptible
continental shelf, continental shelves (pl)
contra (pref, usually one word)
but
contra-acting
contra-approach
contra-ion
contraband (no s)
control(s), controlled, controlling (n, v)
controllable
converter(s)
convertible(s) (n, adj)
conveyor(s)
coolheaded
coolly
copper mine(s) (n)
copper-plated (um)
copperplate(s)
copperworker(s)
copperworks
cornerstone(s)
corn growing (n)
corollary, corollaries (pl)
corps (sing, pl)
corral(s), corralled, corralling (n, v)
corroborate(s), corroborated, corroborating
cost-cutting (n, um)
cost-effective (adj)
cost-effectiveness (n)
cost-free (adj)
cost-of-living (um)
cost-reduction (um)
council(s) (n, deliberative assembly, its works or membership; see *consul, counsel*)
councilor(s) (council member; see *counselor*)
counsel(s), counseled, counseling (v, n; advice and the person offering it; see *consul, council*)
counselor(s) (adviser; see *councilor*)
counter (cf, usually one word)
counterclockwise
counterintelligence (CI)
counterrevolutionaries
counterstealth
but
counter-countermeasures
country-specific (um)
country-western
countrywide
coup(s) d'etat
coupmaker(s)
course work
courthouse(s)
court-martial(s), court-marshaled, court-marshaling
court(s)-martial (n)
covername(s)
coversheet(s)
cover story, cover stories (pl)
cover(s) up, covered up, covering up
coverup(s) (n, um)
crack (cocaine)
crack(s) down, cracked down, cracking down
crackdown(s) (n, um)
crackhead(s)
cradle-to-grave (um)
crankcase(s)
crank-driven (um)
crankshaft(s)
crash-land(s), crash-landed, crash-landing
crash landing(s) (n)
credence (belief or mental acceptance)
credible (worthy of belief and judged plausible)
credibility (the quality of being believable)
credit card(s) (um)
credit-starved (um)
creditworthiness

C05757260

crewmember(s)
crew-training (um)
crimewave(s)
crisis, crises (pl)
crisscross(es), crisscrossed, crisscrossing (n, adj, v)
criteria (the singular, *criterion*, is rarely used)
critical thinking (adj)
crop-dusting(s) (n)
crop index(es)
crop-year(s)
cross-border (adj)
crossbreed(s)
cross-channel
cross-check(s), cross-checked, cross-checking (n, v)
cross-connect(s), cross-connected, cross-connecting (n, v)
cross-country (adj)
crosscurrent(s)
crosscut(s), crosscut, crosscutting (n, adj, v)
cross-examination(s)
cross-examine(s), cross-examined, cross-examining
crossfire(s)
cross-functional
crosshaul(s), crosshauled, crosshauling
crossline(s) (n, um)
cross-national (um)
crossover(s) (n)
cross-pressure(s)
cross-purposes
crossrange(s)
cross-reference(s), cross-referenced, cross-referencing (n, v)
crossroads
cross section(s) (n)
cross-section(s), cross-sectioned, cross-sectioning (v)
cross-sectional
cross-strait (adj)
cross-target(s)
crosstrading
crosstrained
crosswalk(s)
crosswise
cruise missile(s) (n, um)
cruise-missile-armed (um)
cruise-missile-related (um)
cryptanalysis, cryptanalyses (pl)
crypto (cf, usually one word)
but
crypto-Christian
crystal-clear (um)
crystalline
crystallize(s), crystallized, crystallizing
culminate(s), culminated, culminating (takes the preposition *in*)
Cultural Revolution
cum laude
cure-all(s) (n)
current account(s) (n, um)
current-generation (um)
curriculum(s)
cursor(s)
custom-built (um)
custom-made (um)
cutaway(s)
cutback(s) (n)
cut(s) in, cut in, cutting in
cut-in(s) (n)
cut(s) off, cut off, cutting off
cutoff(s) (n, um)
cutouts (n)
cutover (um, of timberland)
cutrate (adj)
cutting-edge (um)
cutthroat(s) (n, adj)
cyber (cf, usually one word)
cybercrime
cyberjack(s), cyberjacked, cyberjacking
cyberspace
czar(s)
czarist(s)

C05757260

D

dairy farm(s)
dairyman, dairymen (pl)
damsite(s)
dark horse(s) (n)
darkhorse (um, nonliteral)
data (the singular, *datum*, is rarely if ever used)
database(s)
data link(s)
data print(s)
data-processing (um)
data transfer rate(s)
dateline(s)
date stamp(s) (n)
date-stamp(s), date-stamped, date-stamping
daughter(s)-in-law
daylong
day school(s)
day shift(s)
daytime(s)
day-to-day
dayworker(s)
D-day
D-day plus 4
de (pref, all one word)
deemphasize(s), deemphasized, deemphasizing
deemphasis
deenergize(s), deenergized, deenergizing
deescalate(s), deescalated, deescalating
deice(s), deiced, deicing
deaddrop(s) (nonliteral)
dead end(s)
dead heat(s)
dead-in-the-water (um)
deadline(s)
deadload(s)
deadlock(s)
deadpan(s)
deadweight(s) (n, um)
deadwood
dealmaker(s)
dealmaking
deathbed(s)
deathblow(s)
deathlike
death rate(s)
death squad(s)
debris
debt-rescheduling (um)
debt service(s)
decadelong, decades-long (pl)
decadent
decade-old
decisionmaker(s)
decisionmaking
but
economic decision making (it is the decisions that are economic, not the making; hence *decision* and *making* are separated)
deckhand(s)
deductible(s) (n, adj)
deep cover
deep-ocean (adj)
deep-sea (adj)
deep-seated (um)
deep-space (adj)
deep underground
deepwater (um)
de facto
defense(s)
defense attache(s)
defense-industrial (um)
defensible
defuse(s), defused, defusing (to remove a fuse; to deintensify; see *diffuse*)
degrees Celsius (or **Fahrenheit**)
deja vu
de jure
demagogue(s)
demarcation(s)
demarche(s)
denouement(s)

C05757260

deorbit(s), deorbited, deorbiting (n, v)
dependent(s) (n, adj)
deploy(s), deployed, deploying
deprecate(s), deprecated, deprecating (express disapproval of something)
depreciate(s), depreciated, depreciating (besides its applications to prices and values, means to belittle something)
depth charge(s)
deputy chief(s) of staff
Deputy Permanent Representative to the UN
descendant(s) (n, adj)
desiccate(s), desiccated, desiccating
desktop(s)
desperate (distressed; see *disparate*)
despise(s), despised, despising
detente(s)
deter(s), deterred, deterring
deterrence(s)
deterrent(s)
detriment(s)
devastate(s), devastated, devastating
develop(s), developed, developing
development(s)
developed-country (adj)
developing-country (adj)
device(s) (n)
devise(s), devised, devising
devotee(s)
dexterous
diagram(s), diagramed, diagraming
diagrammatic
dialogue(s)
die(s), died, dying
diehard(s) (n, adj)
diesel-driven (um)
diesel-electric
diesel engine(s)
diffuse(s), diffused, diffusing (to spread; see *defuse*)
directed-energy (adj)
direction-finding (um)
director(s) general
disastrous
discernible
discreet (cautious, prudent)
discrete (separate, distinct)
discussible
disequilibrium(s)
disinformation (the deliberate planting of false reports)
disinterested (impartial; see *uninterested*)
disk(s)
disk drive(s)
disparate (different; see *desperate*)
dispatch(es), dispatched, dispatching
dispel(s), dispelled, dispelling
dispersible
dissension
distill(s), distilled, distilling
distillation(s)
distribute(s), distributed, distributing
distribution(s)
distributor(s)
districtwide
divisible
dockworker(s)
doctrinaire
DOD (Department of Defense)
dogfight(s)
doggerel
dogma(s)
dollar-peso exchange rate
dominance
dominant (adj)
dominate(s), dominated, dominating
donor-country (um)
doomsday
Doppler
dossier(s)
dot-com
double agent (n)
double-agent (adj)

C05757260

double-barrel (n, um)
double-barreled (um)
double check(s) (n)
double-check(s), double-checked, double-checking
double-count(s), double-counted, double-counting (um, v)
double cross(es) (n)
double-cross(es), double-crossed, double-crossing
double-crosser(s)
double-dealer(s)
double-dealing (n, um)
double-decker(s)
double-digit (um)
double-duty (um)
double-edged (um)
double-entry (um)
double play(s)
double space(s) (n)
double-space(s), double-spaced, double-spacing
doubletalk
double time
double-track(s), double-tracked, double-tracking (v, um)
down-and-out (um)
dovetail(s), dovetailed, dovetailing
downcast
downdraft(s)
downfall(s)
downflow(s)
downgrade(s), downgraded, downgrading (n, v)
downhill(s) (n, adj, adv)
downline(s)
down-link(s)
download(s), downloaded, downloading (n, v)
downpayment(s)
downplay(s), downplayed, downplaying
downpour(s)
downrange (adv)
downriver (adj, adv)
downside(s)
downsize(s), downsized, downsizing
downstream (adj, adv)
downswing(s)
Down syndrome
downtime(s)
down-to-earth (adj)
downtrend(s)
downturn(s)
downward
downwind
draconian measures
draft(s), drafted, drafting (n, v)
draft age (um)
drawbridge(s)
drawdown(s) (n, um)
drawn-out (um)
dreadlocks
drive-by (n, adj)
drive-in(s) (n, adj)
drive shaft(s)
drive-through(s) (n, adj)
drive(s) up, drove up, driving up
drive-up (um)
drop(s) off, dropped off, dropping off (v)
dropoff (n, um)
drop(s) out, dropped out, dropping out
dropout(s) (n)
drought(s)
droughtlike
drought-stricken (um)
drug czar(s)
drug-free (um)
drug lord(s)
drug money (n, um)
drug mule
drug-producing (um)
drug runner
drug-smuggling (um)
drug traffic
drug trafficker
drug-trafficking (um)

C05757260

dry cleaner(s) (n, um)
drycleaning
drydock(s)
dry-season (um)
dual-purpose (adj)
dual-use (um)
due date(s)
dues-paying (um)
dumpsite(s)
duo (cf, all one word)
dutybound
duty-free (um, adv)
dye(s), dyed, dyeing (coloring)
dysfunction
dysfunctional

E

18-year-olds
e- (cf, usually hyphenated)
e-book(s)
e-business(es)
e-commerce
e-mail(s), e-mailed, e-mailing (n, v)
e-trade(s)
e-trading
e-zine(s)
earful(s)
early-1980s-vintage (um)
early or mid-1990s
early or mid-March
early-model (um)
early-to-mid(dle) 1990s
early-to-mid-March
early warning (um, of radar)
earthmover(s)
earthmoving
east-southeast
eastward
easygoing
economic decision making
economic policy making
edgewise
editor(s) in chief
effect(s), effected, effecting (n, result, outcome; v, bring about, perform; see *affect*)
ego(s)
either (as a subject, takes a singular verb and pronoun)
elan
elbowroom
eldercare
elect (suffix, hyphenated)
President-elect
Senator-elect
election (singular unless the context is plainly plural, as in the last four national elections)
electro (cf, usually one word)
electromagnetic
electrotechnics
but
electro-optics
electro-ultrafiltration
eleventh-hour (adj)
elicit(s), elicited, eliciting (v, to draw out; see *illicit*)
eligible
elite(s) (n, adj)
ellipsis, ellipses (pl)
elusive (hard to capture; see *illusive*)
embargo(es)
embarkation(s)
embarrass(es), embarrassed, embarrassing
embarrassment(s)
embed(s), embedded, embedding
embellish(es), embellished, embellishing
embellishment(s)
emigrant(s) (person moving to a new country; see *immigrant*)
emigrate(s), emigrated, emigrating (leave one's country for a new one; see *immigrate*)
emigre(s) (an emigrant)
eminence grise, eminences grises (pl)
emptyhanded
encase(s), encased, encasing
enclose(s), enclosed, enclosing
enclosure(s)

C05757260

encumber(s), encumbered, encumbering
encumbrance(s)
encyclopedia(s)
end date(s)
endgain(s)
endgame(s)
end item(s)
endorse(s), endorsed, endorsing
endorsement(s)
end point
end run (n)
end-run(s), end-ran, end-running (v)
end use(s) (n)
end-use (adj)
end-use item(s)
end user(s) (n)
end-user (adj)
enforce(s), enforced, enforcing
enforcement(s)
enfranchise(s), enfranchised, enfranchising
engine-driven (um)
engine driver(s)
enginehouse(s)
engineroom(s)
English-speaking (um)
en masse
ennui
enormity, enormities (pl) (great wickedness)
enormousness (n, great size)
enroll(s), enrolled, enrolling
enrollment(s)
en route
ensure(s), ensured, ensuring (guarantee; see *assure, insure*)
enterprise(s)
entrench(es), entrenched, entrenching
entrepot(s)
entrepreneur(s)
entrepreneurial
entrepreneurialism
entrepreneurship
entrust(s), entrusted, entrusting
entry into force
entwine(s), entwined, entwining
envelop(s), enveloped, enveloping
envelope(s) (n)
environmental impact (um)
environmental protection (um)
environmental technology (um)
epilogue(s)
equal(s), equaled, equaling (n, v)
equality, equalities (pl)
equal rights (n, um)
Equator
equilibrium(s)
equip(s), equipped, equipping
equipment
erector-launcher(s)
erratum, errata (pl)
error message(s)
escapable
escudo(s)
esprit de corps
et al. (see section 3.11)
ethno (cf, usually one word)
euro(s) (n, currency)
euro zone (n)
euro-zone (um)
Euro (cf, usually one word)
Eurodollar
Euroloan
Eurotunnel
European Central Bank (ECB)
European Union
evacuee(s)
evenhanded
even-numbered (um)
even-keeled (um)
even-tempered (um)
ever-present (um)
everyday
ex cathedra
ex-serviceman, ex-servicemen (pl)

C05757260

exceed(s), exceeded, exceeding
excel(s), excelled, excelling
exchange rate(s) (n, um)
excise(s), excised, excising (n, v)
ex-civil-servant (n, adj)
excommunicate(s), excommunicated, excommunicating
Executive Order(s) (US President)
exercise(s), exercised, exercising (implement, train; see *exorcise*)
ex-Governor(s)
exhibitor(s)
exhilarate(s), exhilarated, exhilarating
exhort(s), exhorted, exhorting
exhortation(s)
ex officio
exonerate(s), exonerated, exonerating
exoneration(s)
exorbitant
exorcise(s), exorcised, exorcising (purge; see *exercise*)
expediter(s)
expel(s), expelled, expelling
export-control (adj)
expose(s), exposed, exposing (v [two syllables], to lay open)
expose(s) (n [three syllables], an exposure)
ex post facto
expulsion(s)
extant (in existence)
extol(s), extolled, extolling
extra(s) (n)
extra (as pref, usually one word)
extracurricular
extra-heavy (um)
extra-large (um)
extra-long (um)
extramural
extraordinary
extraterritorial
extremely-low-frequency (adj)
eye(s), eyed, eying
eye-catching (um)
eyeglasses
eye opener(s)
eye-opening
eye to eye
eyewitness(es)

F

facade(s)
face-saving (um)
face-to-face (adj, adv)
factbook(s)
factfinding
factsheet(s)
Fahrenheit
fail-safe(s) (n, adj)
fair-haired (um)
fairminded
fair-skinned (um)
fait accompli, faits accomplis (pl)
fall(s) (autumn)
fallback(s) (n, um)
fall guy(s)
fallible
falling-out (n)
falloff(s) (n)
fallout(s) (n, um)
fall wheat
faraway (um)
far cry, far cries (pl)
farfetched
farflung
far-left (adj)
far-leftist (um)
farm bloc(s)
farm-bred (um)
farmland(s)
farmwork
farmworker(s)

C05757260

far-reaching (um)
far-right (adj)
far-rightist (um)
farseeing
farsighted
farther (physical or literal distance; see *further*)
farthest
fast-breaking (um)
fast breeder reactor(s)
fast-moving (um)
fast-food (adj)
father(s)-in-law
fatwa(s)
faultfinding (n, adj)
faultline(s)
favor(s), favored, favoring (n, v)
fax(es), faxed, faxing (n, v)
fearmongering
feasible
featherbedding (n)
fedayeen (sing, fedayee, rare)
federal government(s) (non-US)
Federal Government (US only)
feedback (n)
feedgrain(s)
fellow traveler(s)
fence jumper(s)
fence-mending
fence-sitter(s)
fence-sitting
ferro (cf, usually one word)
but
ferro-carbon-titanium
ferro-uranium
ferryboat(s)
fiasco(es)
fiber(s)
fiberboard(s)
fiberglass
but
trade name Fiberglas
fiber-optic (um)
fiber optics (n)
field day(s)
field-deployed
field grade(s) (n)
field-grade (adj)
fieldpiece(s)
field-test(s), field-tested, field-testing (v)
fifth column(s)
fighter-bomber(s)
fighter-interceptor(s)
fighter pilot(s) (n, um)
fig leaf, fig leaves (pl)
figure 4 (reference)
figure eight(s)
figurehead(s)
file clerk(s)
file name
filmmaker(s)
filmmaking
final assembly area(s)
fine-tune(s), fine-tuned, fine-tuning (v)
finger pointing (n)
fingerprint(s)
firearm(s)
fireball(s)
firebomb(s), firebombed, firebombing
fire control(s) (n)
fire-control (adj)
firecracker(s)
fire drill(s) (n, adj)
firefight(s)
firefighter(s)
firefighting
fire-hardened (um)
firepower
fireproof(s), fireproofed, fireproofing (adj, v)
fire-resistant (um)
firesafe
fire storm(s)
fire-support (adj)
firetruck(s)

C05757260

firewall(s)
firewood
firm-handed (um)
first aid (n, um)
first-ballot (adj)
firstborn
first-class (adj)
first-come-first-served
first-echelon (adj)
first-half (adj)
firsthand (adv, um)
First Family
First Lady, First Ladies (pl)
firstline (adj)
first-quarter (adj)
first-rate (adj)
first-stage (adj)
first-time (adj)
fistfight(s)
fit(s) out, fitted out, fitting out
fitting-out (um)
fivefold
five-pointed (um)
Five-Year Plan (if specific)
fixed-rate (adj)
fixed-wing (adj)
fjord(s)
flagship(s)
but
American flag ship
flameproof(s), flameproofed, flameproofing (adj, v)
flamethrower(s)
flammable (literal)
flare(s) up, flared up, flaring up
flareup(s) (n)
flashpoint(s)
flatbed(s) (n, adj)
flatcar(s)
flatfoot, flatfeet (pl, physical condition of foot); **flatfoots** (pl, policemen)
flat-footed
flaunt(s), flaunted, flaunting (to display ostentatiously; see *flout*)
fledgling(s)
flexibility
flexible
flier(s)
flight control (adj)
flightcrew(s)
flight deck(s)
flight-hour(s)
flightline(s)
flightpath(s)
flight test(s) (n, adj)
flight-test(s), flight-tested, flight-testing (v)
flight time(s)
flip-flop(s), flip-flopped, flip-flopping (n, v)
floodgate(s)
floodlight(s)
flood plain(s)
floodwater(s)
floor-length
floor plan(s)
floorspace(s)
flounder(s), floundered, floundering (to stumble about clumsily; see founder)
flout(s), flouted, flouting (to treat with contempt; see *flaunt*)
flow chart(s)
fluorescent(s) (n, adj)
fluoro (cf, all one word)
flyaway (adj)
flyover(s)
f.o.b. (free on board)
focus(es), focused, focusing (n, v)
fold (suffix, usually one word)
twofold
fourfold
foldout(s)
follow-on(s) (n, um)
followthrough(s) (n, um)
follow-up(s) (n, um)
follow(s) up, followed up, following up (v)

C05757260

foodgrain(s)
food grower(s) (n)
food-processing (um)
foodstore(s)
foodstuff(s)
foolhardiness
foolhardy
foolproof
foot-and-mouth (adj)
footbridge(s)
foot-dragging
foothill(s)
foothold(s)
footnote(s), footnoted, footnoting (n, v)
foot-pound(s)
footprint(s)
foot soldier(s)
footstep(s)
forbear(s), forbore, forborne, forbearing
(v, tolerate; see *forebear*)
forbid(s), forbade, forbidding
force majeure
forebear(s) (n, ancestor; see *forbear*)
forced labor
force-feed, force-fed, force-feeding
forefront(s)
forego(es), forewent, foregone, foregoing
(precede; see *forgo*)
foregone conclusion
foreground(s)
foreign decisionmaking
foreign exchange(s) (n, um)
foreign-government-backed (um)
Foreign Military Sales (a US Government program)
foreign policy making
Foreign Service (US only)
foremost
foresee(s), foresaw, foreseen, foreseeing
foreseeable
forestall(s), forestalled, forestalling
forest-covered (um)
forest land(s)
foreword(s) (prefatory note)
forgettable
forgo(es), forwent, forgone, forgoing
(do without; see *forego*)
forklift(s)
format(s), formatted, formatting (n, v)
formateur(s)
forsake(s), forsook, forsaken, forsaking
forswear(s), forswore, forsworn, forswearing
forte(s)
forthcoming
forthright
forthwith
fortuitous (happens by chance or accident)
fortune-teller(s)
forum(s)
forward (adj, adv, opposite of backward)
forward-based (um)
forward-looking (um)
founder(s), foundered, foundering (to go lame, collapse, sink, fail; see *flounder*)
four-star (adj)
fourth-quarter (adj)
four-wheel drive(s) (n)
four-wheel-drive (um)
framework(s)
Franco-Prussian War
fraught
free (suffix, usually hyphenated)
duty-free
rent-free
but
carefree
freedom fighter(s)
free enterprise(s) (n, um)
free-fall(s)
free-for-all(s)
free hand(s) (n)
freehand (adj, adv)
freelance(s), freelanced, freelancing (n, adj, v)
freelancer(s)

C05757260

free market(s) (n, um)
free-marketeer(s) (n)
free-market-oriented (um)
free port(s)
freer
free-spoken (um)
freestanding
freethinker(s)
freethinking
free trade (n, um)
free-trade-oriented
freeway(s)
freewheeling
free will (n)
freewill (um)
freeze-dry, freeze-dries, freeze-dried, freeze-drying
freight car(s)
French Canadian
but
Italian-American
Chinese-American
French-English
French Revolutionary period
freshwater (um)
frogman, frogmen (pl)
front burner(s)
front-end (adj)
front-load(s), front-loaded, front-loading (v)
frontline(s)
front man, front men (pl)
front page(s)
frontrunner(s)
frontrunning
frontseat(s)
frost-free (um)
frostline(s)
frostproof(s), frostproofed, frostproofing (adj, v)
fruit growing (n)
fuel pump(s)
full-blown
fullblooded
fullface
fulfill(s), fulfilled, fulfilling
fulfillment(s)
full-fledged
full-grown (um)
full load
full-scale (adj)
full-scope (adj)
full-speed (adj)
full-strength (adj)
full-time (adv)
fulsome (adj, offensive to the senses or loathsome; *not* complete or full)
fundraiser(s)
fundraising(s)
funnel(s), funneled, funneling (n, v)
funnel-shaped (um)
further, furthest (generally conveys notion of additional degree, time, or quantity; see *farther*)
fuse(s), fused, fusing (n, v, preferred spelling except for missile and other military applications; see *fuze*)
fuselage(s)
fuze(s), fuzed, fuzing (certain military senses; see *fuse*)
FY 2010

G

gainsay(s), gainsaid, gainsaying
gallbladder(s)
Gambia, The
game plan(s)
gas-canister bomb(s)
gas-driven (um)
gasfield(s)
but
oil and gas fields
gas-fired (um)
gas-flow (adj)
gas-gathering (um)
gas-heated (um)

C05757260

gas-laden (um)
gaslight(s)
gasline(s)
gas main(s)
gas mask(s)
gas oil
gastro (cf, usually one word)
gas well(s)
gasworker(s)
gasworks
gatekeeper(s)
gauge(s)
gazetteer(s)
GDP (gross domestic product)
gearbox(es)
gear-driven (um)
gearshift(s)
gendarme(s)
gendarmerie (collective)
general counsel(s)
general-purpose (adj)
gentlemen farmer(s)
geopolitics
ghetto(s)
ghostwrite(s), ghostwrote, ghostwriting
ghostwriter(s)
gibe(s), gibed, gibing (n, v, taunt or sneer; see *jibe with*)
gigawatt-hour(s)
give-and-take(s) (n)
give(s) away, gave away, giving away (v)
giveaway(s) (n)
glad hand (n)
glad-hand(s), glad-handed, glad-handing (v)
glamorous
glamour
glasnost
glassmaking
globetrotting
glove box(es)
GmbH (German equivalent of the US Inc.)
GNP (gross national product)
go-ahead(s) (n)
go-around(s)
go-between(s) (n)
go-getter(s)
going(s)-on
gold mine(s)
goodbye(s)
good-faith (adj)
good-hearted (um)
good-heartedness
good-humored (um)
good offices
good-quality (adj)
good-to-excellent (um)
goodwill (in economics)
good will (usually literal senses)
go-slow(s)
gossiped-about (um)
gossipmonger(s)
government(s) (when referring to a sovereign state, capitalize in phrases like *Egyptian Government*; lowercase when used alone or with nonsovereign entities; see *Hong Kong government*)
government(s)-in-exile
governmentwide
governor(s) general
grab bag(s)
graded earth runway(s)
grainfield(s)
grainland(s)
grandstanding
grant(s)-in-aid
grapevine(s)
grassroots (nonliteral)
gravesite(s) (n)
gray(s), grayed, graying (adj, v)
gray arms broker(s)
gray arms market(s)
gray-market (um)
great-aunt(s)
Greater London

C05757260

great-grandfather(s)
great-grandmother(s)
Great Himalaya Range
great-power (adj)
great-uncle(s)
greenbelt(s)
green card(s)
greenhouse(s)
grievous
ground attack (adj, of aircraft)
ground-based (um)
groundbreaking(s) (n, adj)
groundburst(s)
ground-controlled (um)
ground crew(s)
ground-effect vehicle(s) (generic for a Hovercraft or similar machine)
ground fire
ground force(s) (n, adj)
ground-launched (um)
ground-mobile (um)
ground rules
ground station(s)
ground support (adj, of equipment)
ground swell(s)
ground test(s) (n, adj)
ground-test(s), ground-tested, ground-testing (v)
ground war(s)
groundwater(s)
groundwave(s)
groundwork
groupthink
growth rate(s)
gruesome
G-7 summit(s)
guarantee(s), guaranteed, guaranteeing (n, v)
guaranty, guaranties (pl) (n, used only in legal sense)
guardhouse(s)
guerrilla(s)
guesswork
guest worker(s)
guidance and control (um)
guided-missile (adj)
guided-missile cruiser
guideline(s)
guide rail(s)
Gulf state(s) (Persian)
Gulf war (Persian understood)
gun-barrel (adj)
gun battle(s)
gunbearer(s)
gun-bore (adj)
gundeck(s)
gunfighting
gunfire
gun(s)-for-hire (n)
gunmaking
gunman, gunmen (pl)
gun mount(s)
gunpoint
gunpowder(s)
gunrunner(s)
gunrunning
gunship(s)
gunshot(s)
gunsight(s)
gun tube(s)
gunsmith(s)
Gypsy, Gypsies (pl)

H

habeas corpus (sing, pl)
Hague, The
hailstone
hailstorm
hairbreadth
hairline
hairsplitting

C05757260

hajj(es) (Muslim pilgrimage)
hajji(s) (Muslim pilgrim; capitalize only if it precedes a person's name)
half brother(s)
half-day (adj)
half-dozen (adj)
halfhearted
half hour
half-hourly (um)
half-life
half load
half-mast
half measure
half-mile (adj)
half-million (adj)
half-monthly (adj)
half moon
half-ripe (um)
half sister(s)
half-speed (adj)
half-step
half-strength (adj)
halftime
halftrack
half-truth
halfway
half-yearly
Halley's comet
hallmark
ham-fisted (adj)
hamstring(s), hamstrung, hamstringing (n, v, adj)
handbook
hand-built (um)
hand-carry(s), hand-carried, hand-carrying
handclasp(s)
handcuff(s)
hand-deliver(s), hand-delivered, hand-delivering (v, adj)
handgrenade(s)
handgun(s)
handheld (adj)
hand-holding
handicap(s), handicapped, handicapping
hand-in-hand
handmade
hand-me-down(s) (n, um)
hand(s) off, handed off, handing off
handoff(s) (n, um)
hand(s) out, handed out, handing out
handout(s) (n, um)
hand(s) over, handed over, handing over
hand-over(s) (n)
handpicked
handrail(s)
handshake(s)
hands-off (adj)
hands-on (adj)
hand-wringing
handwritten
hangers-on
hangup(s)
harass(es), harassed, harassing
harbormaster(s)
hard-and-fast
hardball
hard-charging (um)
hardcopy
hard core (n, adj)
hardcover
hard currency (n, um)
hard drive(s)
hard-driving (um)
hardhat(s)
hardheaded
hard-hit (um)
hard-hitting (um)
hard line(s)
hardline (adj)
hardliner(s)
hard-nosed (adj)
hard-pressed (um)
hardstand(s)

C05757260

hard-target (adj)
hard up
hardware
hardwired (adj)
hard-won (um)
hard work
hardworking (adj)
harebrained
harvesttime
has-been(s)
have-not(s) (n, adj)
H-bomb(s)
headfirst
headlight(s)
headline(s)
headlong
head-on (adj, adv)
headquarter(s), headquartered, headquartering (n, v)
headrest(s)
headroom
headstart(s)
headstrong
heads-up (n, adj)
head-to-head (um)
headwaters
headway(s)
health care (n)
health-care (um)
healthful (producing health)
health worker(s)
healthy (in good health)
heartbeat(s)
heartland(s)
heat-resistant (um)
heat-seeking (um)
heavy bomber(s) (n, um)
heavy bomber base(s)
heavy-duty (adj)
heavyhanded
heavy hitter(s)
heavy-lift (adj)
heavy-set (um)
heavy-water (adj)
heavy-water-moderated (um)
heavyweight (n, um)
hedgehop(s), hedgehopped, hedgehopping
height-finding (adj)
heir(s) apparent
helicopter-borne (um)
hemisphere(s)
but
Western Hemisphere
hemorrhage(s)
Her Majesty's Government
hereafter
hereby
herein
heretofore
herewith
heterogeneous
heyday(s)
hidebound
hideout (n, um)
high-altitude (adj)
highborn
high-caliber (adj)
high-class (adj)
high-density (adj)
high-end (adj)
high-energy (adj)
higher-income
higher-level (um)
higher-paying
higher-ranking
higher-than-market price
higher-ups
highest-altitude (um)
highest-ranking
high-explosive (um)
high fidelity
highflier(s)

C05757260

high-frequency (adj)
high-frequency direction-finding (um)
highhanded
high-intensity (adj)
highland(s) (n, um)
high-level (adj)
high light(s) (literal)
highlight(s) (nonliteral)
high-minded (um)
high point(s) (literal, nonliteral)
high-power (adj)
high-precision (adj)
high-pressure(s), high-pressured, high-pressuring (v, adj)
high-priced (um)
high-priority (adj)
high-profile (adj)
high-protein (adj)
high-quality (adj)
high-ranking (um)
high-resolution (adj)
high-rise (adj)
high school (n, um)
high-speed (adj)
high-strung (um)
high-tech(nology) (adj)
high-tension (adj)
high-value (adj)
high water mark
hijack(s), hijacked, hijacking (n, v)
hijacker(s)
hilltop(s)
hill tribe(s)
hindsight
hit-and-miss (adj)
hit-and-run (adj)
hit list(s)
hit man, hit men (pl)
hit-or-miss (adj)
HIV
HIV-positive (um)
hodgepodge(s)
hold off, held off, holding off
holdout(s)
holdover(s) (n, adj)
hold time(s)
holdup(s)
Holocaust (the)
home base(s)
homebrew(s)
homebuilding
home buyer(s)
homecoming(s)
home front(s)
homegrown
home guard(s)
homeland(s)
homemade
homeowner(s)
home page(s)
home port(s)
home-port(s), home-ported, home-porting
home rule
homesick
homestead(s)
homestretch(es)
hometown(s)
homeward
homogeneous
honeymoon(s)
Hong Kong government
honorbound
hookup(s) (n, adj)
horselaugh(s)
horseman, horsemen (pl)
horseplay
horsepower
horserace(s)
horseshoe(s)
horsetrade(s), horsetraded, horsetrading (n, v, nonliteral)
horsetrader(s) (nonliteral)

C05757260

hostage taker(s)
hostage taking
host-country (adj)
host-government (adj)
host-nation (adj)
hotbed(s)
hot-blooded (um)
hot-button (adj)
hotheaded
hothouse(s)
hotline(s) (nonliteral)
hot-pursuit (adj)
hotspot(s)
hour-long
housebuilding
house call(s)
house-clean(s), house-cleaned, house-cleaning
housecleaner(s)
house-cleaning (um)
houseguest(s)
household(s)
housekeeping
but
safehouse keeper
safehouse keeping
housework
hover craft (unless trade name Hovercraft)
HTML (hypertext markup language)
hull-less
human rights (n, um)
human-rights-related (um)
human-source (adj)
humdrum
HUMINT
hundredfold
hundredweight
hunger strike(s)
hunker(s) down, hunkered down, hunkering down
hush money
hush(es) up, hushed up, hushing up
hushup(s) (n, adj)

hydro (cf, usually one word)
hydroelectric
hydropower
hydrostatic
hyper (pref, usually one word)
hyperinflation
hyperlink(s), hyperlinked, hyperlinking (n, v)
hypertext system(s)
but
hyper-Dorian
hypocrisy
hypothesis, hypotheses (pl)

I

I-beam(s)
Iberian Peninsula
ibid. (see 3.11)
iceberg(s)
icebound
icebreaker(s)
icecap(s)
ice-covered (um)
icefield(s)
ice-free
icemaking
icepack(s)
ice shelf, ice shelves (pl)
ice skate(s) (n)
ice-skate(s), ice-skated, ice-skating
ice storm(s)
idiosyncrasy, idiosyncrasies (pl)
idiosyncratic
idyll(s)
ill-advised (um)
ill-advisedly
ill-at-ease (um)
illegible
ill-equipped (um)
ill health
illicit (n, illegal; see *elicit*)
illicit drug trafficking

C05757260

illiquid
illiquidity
ill-prepared (um)
ill-timed (um)
illusive (deceptive; see *elusive*)
ill will
image-building (um)
image-conscious (adj)
image-enhancing (um)
imam(s)
immersible
immigrant(s) (coming into; see *emigrant*)
impasse(s)
impel(s), impelled, impelling
impending (hint of threat or menace)
imperceptible
imperil(s), imperiled, imperiling
impermissible
impersuadable
impersuasible
implausible
implementer(s)
imply (implies), implied, implying (state something indirectly; see *infer*)
impostor(s)
imprimatur(s)
improvise(s), improvised, improvising
in absentia
inaccessible
inadmissible
inaudible
inbound
in-board (adj)
inbox(es)
Inc.
incise(s), incised, incising
incompatible
incomprehensible
incontrovertible
incorrigible
incorruptible
in-country (adj, adv)
incredible
incur(s), incurred, incurring
indefensible
indelible
Independence Day
in-depth (um)
indestructible
indeterminate
index, indexes (pl); **indices** (pl, scientific only)
indications-and-warning intelligence
indict(s), indicted, indicting (to accuse; see *indite*)
indigestible
indite(s), indited, inditing (to compose; see *indict*)
indivisible
Indo-European
industrialization
industrywide
inedible
ineligible
inequity, inequities (pl) (unfairness; see *iniquity*)
inexhaustible
in extremis
infallible
infantryman, infantrymen (pl)
infeasible
infer(s), inferred, inferring (draw a conclusion or make a deduction; see *imply*)
inferable
inference(s)
infighter(s)
infighting
inflammable (figurative)
inflexible
in-flight (um)
inflow(s)
influence-buying
information processing
infra (pref, usually one word)
but
infra-axillary
infra-esophageal
infra-umbilical

C05757260

INF (intermediate-range nuclear forces) **Treaty**
in-garrison
ingenious (skillful)
ingenuous (without guile)
in group(s)
in-house (adj, adv)
iniquity, iniquities (pl) (sin; see *inequity*)
ink jet(s)
in-law(s)
inner-city (adj)
inner tube(s)
innocuous
innuendo(s)
inoculate(s), inoculated, inoculating
input(s), input, inputting (n, v)
inquire(s), inquired, inquiring
inquiry, inquiries (pl)
inshore
insignia (the singular, *insigne*, is rarely used)
in situ
insofar as
inspector(s) general
install(s), installed, installing
installation(s)
installment(s)
instill(s), instilled, instilling
insure(s), insured, insuring (cover by an insurance policy; see *assure*, *ensure*)
insurgency, insurgencies (pl)
insurgent(s)
intangible(s) (n, adj)
Intelink
intelligence-gathering (um)
intelligentsia
intelligible
integrity
inter (pref, usually one word)
interactive processing
inter alia
but
inter-American
inter-European
intercede(s), interceded, interceding
interceptor(s)
Interests Section (capitalize if US)
interfere(s), interfered, interfering
interleaving
intermediate-range ballistic missile (IRBM)
interment(s) (burial; see *internment*)
intermittent
intern(s)
internally displaced person(s) (IDP)
Internet
internment(s) (detention; see *interment*)
INTERPOL
interrepublic
interruptible
in-theater (adj)
intifada(s)
in toto
intra (pref, usually one word)
but
intra-atomic
intra-German
intransigent (n, adj)
intro (pref, all one word)
invincible
invisible
ipso facto
Iran-Contra
Iran-Iraq war
irascible
IRBM (intermediate-range ballistic missile)
iridescence
ironclad
ironfisted
ironically (involves incongruity between what might be expected and what actually occurs)
iron lung(s)
ironmaking
ironworking
ironworks
irreducible

C05757260

irreplaceable
irrepressible
irresistible
irresponsible
irreversible
Islamization
issues (are resolved, not solved)
iteration(s)
its (possessive of *it*; compare *it's*, the contraction of *it is*; contractions are rarely appropriate in formal writing)

J

jailbreak(s)
jawbone(s), jawboned, jawboning (n, v)
jerry-build(s), jerry-built, jerry-building
jerry-built (um; see *jury-rigged*)
jet aircraft
jet airliner(s)
jet bomber(s)
jetliner(s)
jet-powered (um)
jet-propelled (um)
jet propulsion
jet set(s)
jibe with (informally, be consonant with; see *gibe*)
jihad(s)
jobholder(s)
jobseeker(s)
joint-service (adj)
joint-stock (adj)
joint-venture (adj)
journeyman, journeymen (pl)
judgment(s)
jump(s) off, jumped off, jumping off
jumpoff(s) (n, um)
jump-start(s), jump-started, jump-starting (n, v, adj)
jury-rigged (um; see *jerry-built*)
just-completed (um)
just-in-time (um)

K

kaleidoscopic
keel-laying (um)
kerosene(s)
ketchup(s)
keypad(s)
keyword(s)
kick(s) back, kicked back, kicking back
kickback(s) (n, um)
kick-start(s), kick-started, kick-starting
kidnap(s), kidnapped, kidnapping
kidnapper(s)
kidney stone(s)
killjoy(s)
kill rate(s)
kilobyte(s) (KB)
Kilo-class (um)
kilowatt-hour(s) (kWh)
kimono(s)
kingmaker(s)
kingpin(s)
king-sized (um)
km/h (kilometers per hour)
knee-jerk (um)
know-how
know-it-all(s) (n)
knowledgeable
know-nothing(s) (n, adj)
Korean war
kowtow(s), kowtowed, kowtowing
Kresta-II(s)
kudos (never *kudo*)

C05757260

L

label(s), labeled, labeling
labeler(s)
Labor Day
labor-intensive (um)
laborsaving
labor union(s)
lackluster
laid-back (adj)
laid-off (um)
laid-up (participle)
laissez-faire (n, adj)
lakebed(s)
lakefront(s)
lameduck(s) (nonliteral)
LAN (local area network)
land-attack (adj, of a missile)
land base(s)
land-based (um)
landborne
landbound
land bridge(s)
landfill(s)
landgrab(s)
landholding
landline(s)
landlocked
landlord(s)
landmass(es)
landmine(s)
land-mobile (um)
landowner(s)
landownership
landowning
land-poor (um)
Land Rover(s)
Landsat (US Earth resources satellite)
landslide(s)
land tax(es)
land-use (adj)
landward
landwire(s)
lapdog(s)
large-scale (adj)
largess
last-ditch (adj)
last-minute (adj)
last resort(s) (n)
last-resort (adj)
latecomer(s)
late-model (adj)
late-night (adj)
late-payment (adj)
Latin American country (countries)
latter-day (adj)
launch crew(s)
launch(es), launched, launching on tactical warning
launch-on-tactical-warning (n, um)
launch(es), launched, launching on warning
launch-on-warning (n, um)
launchpad(s)
launch point(s)
launchsite(s)
but
space launch site
launch stand(s)
launch weight(s)
law-abiding (um)
law-and-order (adj)
lawbreaker(s)
lawmaking
lawsuit(s)
lay(s), laid, laid (to put, place, or prepare; always takes a direct object; see *lie*)
layoff(s) (n, adj)
layout(s) (n, adj)
layover(s) (n, adj)
layperson, laypeople (pl)
lay(s) up, laid up, laying up
layup(s) (n, um)

C05757260

LCD(s) (liquid crystal display)
lead-in(s) (n, um)
leading edge(s) (n)
leading-edge (um)
leading-edge (adj)
leadtime(s)
lead(s) up, lead up, leading up
lead-up(s) (n, um)
League of Nations
leakthrough(s)
leapfrog
leap year(s)
leather-bound (um)
leatherworking
lee shore(s)
leeward
left-hand (adj)
left-leaning (adj)
left-of-center (um)
left wing(s) (n)
leftwing (adj)
leftwinger(s)
legible
legman, legmen (pl)
legwork
lend-lease(s)
less (suffix, usually not hyphenated)
dataless
weaponless
but
hull-less
shell-less
less developed (no hyphen)
lesser-known
less-than-even (um)
letter bomb(s)
letter-perfect (um)
letterspacing
letterwriting
let(s) up, let up, letting up
letup(s) (n)
level(s), leveled, leveling
leveler(s)
levelheaded
liaison(s)
license(s)
license plate(s) (n, um)
lie(s), lay, lain (to recline or be situated; never takes a direct object; see *lay*)
lifeblood
lifeboat(s)
life cycle(s) (n, um)
lifeguard(s)
life insurance (n, um)
lifelike
lifeline(s)
lifelong
liferaft(s)
lifesaving
life-size (adj)
lifespan(s)
lifestyle(s)
lifetime(s)
lift(s) off, lifted off, lifting off
liftoff(s) (n)
lighter-than-air craft
lighthearted
light-water (adj, in reference to nuclear power)
light-water-reactor (um)
lightweight(s) (n, adj)
light-year(s)
like (suffix, usually one word)
businesslike
lifelike
but
bell-like
hull-like
likable
likelihood
like-minded (um)
Likud party
linchpin(s)
line-item (adj)
line-of-sight (um)

C05757260

line(s) up, lined up, lining up
lineup(s) (n, um)
line width(s)
link(s) to, linked to, linking to
link(s) up, linked up, linking up
linkup(s) (n, um)
lipservice
liquefy (liquefies), liquefied, liquefying
liquid-propellant (adj)
liquid-propelled (um)
little-known (um)
little-used (um)
livedrop(s) (nonliteral)
live-fire (um)
livewire(s) (nonliteral)
living costs
llano(s)
Lloyd's (insurance)
Lloyds (bank)
loan-sharking (n, um)
loath (adj, reluctant)
loathe(s), loathed, loathing (detest)
locavore(s)
lock(s) on, locked on, locking on
lockon(s) (n, adj)
lock(s) out, locked out, locking out
lockout(s)
locus, loci (pl)
logbook(s)
loggerheads
log(s) in, logged in, logging in
logistic (adj)
logistics (n)
logjam(s)
log(s) off, logged off, logging off
log(s) on, logged on, logging on
London summit(s)
lonely-hearts club(s)
long ago (adv)
long-ago (um)
long-awaited (um)
long-bed(s) (n, adj; truck)
long-delayed (um)
long-distance (adj)
longest-ruling leader(s)
long-lasting (um)
long-lived (um)
long-range (adj)
long run(s) (n)
long-run (adj)
long shot(s) (n)
long-shot (adj)
long-sought (um)
longstanding (adj)
long-term (adj)
longtime (adj)
long-winded
look-alike(s) (n, adj)
lookdown/shootdown (um, of aircraft radar)
lookout(s) (n, um)
loop (as in, *in the loop*)
loophole(s)
loose-knit (um)
looseleaf (adj)
lopsided
loss-making (um)
loudspeaker(s)
low-altitude (adj)
low-cost (adj)
low Earth orbit(s) (n)
low-Earth-orbit (adj)
lowercase(s), lowercased, lowercasing (adj, v)
lower-class (adj)
lower-cost (adj)
lower-echelon (adj)
lower-profile (adj)
lower-grade (adj)
lower-house (adj)
lower-income (adj)
lower-level (adj)
lower-middle-class (adj)

C05757260

low-flying (um)
low-frequency (adj)
low-income (adj)
low-key (adj, adv)
lowland(s) (n, um)
low-level (adj)
low-light (adj)
low-lying (um)
low-observable(s) (n, um)
low-paying (um)
low-power (adj)
low-pressure (adj)
low-priced (um)
low-profile (adj)
low-quality (adj)
Ltd.
lukewarm
lumberyard(s)
lump-sum (um)
lunchtime(s)

M

M.A.('s)
machine-building (um)
machine dependent
machinegun(s)
machine-made (um)
machine readable
machine shop(s)
machine tool(s)
machismo
macho (adj)
macro (cf, all one word)
made-over (um)
made-up (um)
madrasa(s)
magnate(s) (VIP)
magnet(s) (metal attractor)
magneto(s)
mah-jongg
mail merge(s), mail-merged, mail-merging (n, v)
mainframe(s)
mainland(s)
main line(s) (n, literal)
mainline(s), mainlined, mainlining (adj, v, nonliteral)
mainspring(s)
mainstay(s)
mainstream(s) (n, adj)
major generals
make-believe (n, adj)
makeshift
makeup(s) (n, um)
make-work
mal (cf, all one word)
malware
manageable
manager-director(s)
man-day(s)
maneuver(s), maneuvered, maneuvering (n, v)
man-for-man
manhandle(s), manhandled, manhandling
manhole(s)
man-hour(s)
manic-depressive (avoid; prefer *bipolar*)
manifold(s) (n, adj, adv)
man (men) in the street
manmade (um)
man-of-war, men-of-war (pl)
manpack (adj)
man-portable (um)
man-portable air defense system (MANPADS)
manpower
mantel(s) (shelf)
mantle(s) (cloak)
man-year(s)
many-sided (um)
mapmaker(s)
mapreading
maquiladora(s)

C05757260

marijuana
market-oriented (um)
marketplace(s)
marshal(s), marshaled, marshaling
mass-produce(s), mass-produced, mass-producing
masterful (domineering, powerful)
masterly (knowledgeable, skillful)
mastermind(s)
master's degree(s)
master stroke(s)
matrix, matrices (pl)
matter-of-fact (adj)
matter-of-factly (adv)
maxi(s) (n)
maxi (pref, all one word)
maximum(s)
May Day (1 May)
mayday(s) (distress call)
mea culpa
mealtime(s)
mean-spirited (um)
mean time (astronomical)
meantime (meanwhile)
meanwhile
meatpacking
media (always use pl)
media-savvy (um)
Medicaid
Medicare
medieval
medium- and high-altitude (adj)
medium and high altitudes
medium-size(d) (adj)
medium-to-high altitude (n)
medium-to-high-altitude (adj)
meetingplace(s)
mega (cf, usually one word)
megabyte(s) (MB)
megadose(s)
megaproject(s)
member state(s) (n)
member-state (adj)
memento(s)
memoir(s) (personal reminiscence)
memorandum(s)
memorandum(s) of understanding (MOU)
menu driven
merchandise
merchantman, merchantmen (pl)
merchant ship(s)
Mercosur
messhall(s)
messkit(s)
mestizo(s)
metal-coated (um)
metal-cutting (um)
metal-smelting (um)
metalworker(s)
metalworkers union (no apostrophe)
metalworking
metamorphosis, metamorphoses (pl)
metaphor(s) (implied comparison of dissimilar things)
meteorology
meter(s)
Metro Manila
Metropolitan London
Metropolitan Moscow
but
the Moscow metropolitan area
micro (cf, usually one word)
but
micro-organism
mid (cf)
mid- and late 1990s
mid-April
midcareer
midday
mid-decade
mid-18th century (n)
mid-18th-century (adj)
mid-ice
midinfrared
midlevel

C05757260

midmorning
mid-1960s-style (adj)
mid-1989
mid-1990s
mid-Pacific
midpoint(s) (n, adj)
midsixties
midterm(s) (n, adj)
midthirties
mid-to-late 1990s
mid-to-long-term (um)
midyear

middle age(s)

middle-aged (um)

middle class(s) (n)

middle-class (adj)

Middle East (n, adj)

Middle Eastern (adj)

Middle East war

middle ground

middle-income (adj)

middle-level (adj)

middleman, middlemen (pl)

middle-of-the-roader(s)

middle-size(d) (adj)

MiG-21(s)

mild-mannered (um)

mileage(s)

mile-long (um)

milepost(s)

milestone(s)

mile-wide (um)

milieu(s)

militate(s), militated, militating (to have weight or effect, for or against; see *mitigate*)

militiaman, militiamen (pl)

millennium, millennia (pl)

minable

mindreading

mind-set(s)

mineclearing (um)

minefield(s)

minehunter(s)

minehunting

minelayer(s)

minelaying

mineship(s)

minesite(s)

minesweeper(s)

minesweeping

mine warfare (n, um)

mineworks

mini (n)

mini (pref, usually all one word)
miniempire(s)
but
mini-estate

minimum(s)

minimum-security (adj)

minister-counselor(s)

minister(s)-designate

minister-president(s)

minuscule

minutes' (possessive case)

minutiae (the singular, *minutia*, is rarely used)

MIRVs (multiple independently targetable reentry vehicles)

unMIRVed

nonMIRVed

mischief-maker(s)

mischiefmaking

missile-equipped (um)

missile-related (um)

missile support(s) (n, um)

missile suspension(s) (n, um)

Missile Technology Control Regime (MTCR)

Mission (US, to the UN; not to be capitalized for other diplomatic offices, US or otherwise)

misspell(s), misspelled, misspelling

mitigate(s), mitigated, mitigating (to moderate or alleviate; see *militate*)

mixup(s)

mnemonics

mobile-erector-launcher(s) (n)

mobile missile(s) (n, um)

mockup(s) (n)

C05757260

Mod 4
but
modified HY-4

model(s), modeled, modeling

modeler(s)

modem(s)

moderate-to-high (um)

modern-day (um)

modus operandi, modi operandi (pl)

modus vivendi, modi vivendi (pl)

mold(s), molded, molding (n, v)

molotov cocktail(s)

money laundering (n)

money-laundering (um)

money-losing (um)

moneymaker(s)

moneymaking

money market(s)

moneys (preferred plural of money [rather than *monies*]; sounds stilted in most contexts; use cash, funds, and similar everyday words)

moneysaving

monogram(s), monogrammed, monogramming

monologue(s)

monthend

monthlong (adj)

month-old (um)

months-long (adj)

mop(s) up, mopped up, mopping up

mopup (n, um)

moratorium(s)

mosque(s) (the)

most-favored-nation (adj)

most-sought-after (adj)

mothballed

mother(s)-in-law

motherland(s)

mother ship(s)

motor torpedo boat(s)

motorboat(s)

motorcycle(s)

motor-driven (um)

motorized rifle regiment(s)

motorship(s)

MOU (memorandum of understanding)

mountainside(s)

mouthful(s)

mouthpiece(s)

movable

moviemaking

MRV(s) (multiple reentry vehicle)

MTCR (Missile Technology Control Regime)

much-discussed (um)

much-needed (um)

muckrake(s), muckraked, muckraking

muckraker(s) (n)

mudbank(s)

mudflat(s)

mudslinging

Muhammad

mullah(s)

multi (cf, usually one word)
multicolor(ed)
multifiber
multi-ply (adj, several plies)
multitasking
multi-user system(s)
multimillion-dollar (adj)

multiple independently targetable reentry vehicles (MIRVs)

multiple-purpose (adj)

multiple reentry vehicles (MRVs)

multiple-restart (adj)

multiple rocket launcher(s)

multiplex(es), multiplexed, multiplexing

multiplexer(s)

musclebound

music teacher(s)

Muslim(s)

mutually agreed on

C05757260

N

naivete

NAM (Nonaligned Movement)

name-calling (um)

nameplate(s)

Napoleonic code

narco (cf, all one word)
narcoinsurgent
Note: narco (sometimes just *narc*) can also be a separate word. Both the noun and the adjective should be limited to informal use.

narrowband (adj)

narrow-beam (adj)

narrow-body (n, adj, of aircraft)

narrow gauge(s) (n)

narrow-gauge (adj)

narrowminded

nation-building

nation-states

nationwide

native-born (um)

natural gas

natural gas field(s)

nearby

near-Earth orbit

near miss(es)

near-real time (n)

near-real-time (adj)

near-record (adj)

nearsighted

near success(s)

near-term (um)

neck and neck

need-to-know (um)

ne'er-do-well(s)

negligible

neo (cf, usually one word)
neocolonist(s) (n, adj)
neofascist(s) (n, adj)
but
neo-Communist(s) (n, adj)
neo-Nazi(s) (n, adj)

nerve-racking

Netherlands, the

network(s), networked, networking (n, v)

net worth(s)

neuro (cf, all one word)

never-ending (um)

nevertheless

newcomer(s)

newfound

new-generation (adj)

newly industrializing countries (NICs) or economies (NIEs)

newsbroadcast(s)

newscaster(s)

news editor(s)

news-gathering (um)

newsgroup(s)

newsletter(s)

newsmagazine(s)

newsmaking

newspaper(s)

newspaper reporter(s)

newsprint(s)

newsstand(s)

newsweekly, newsweeklies (pl)

news wire(s)

newsworthy

New Year (the)

New Year's Day

next-generation (adj)

next of kin

nightclub(s)

night-flying (um)

night letter(s)

nightlong (um)

night school(s)

night shift(s)

nighttime(s)

night-vision (adj)

nightworker(s)

Nile Delta

C05757260

ninefold

nitpick(s), nitpicked, nitpicking (n, v)

nitpicker(s)

nitpicky

Nobel laureate(s)

Nobel prize(s)

noblesse oblige

nobody, nobodies (pl)

no-confidence (adj)

No Dong(s) (missile)

no-fault (adj)

no-first-strike (adj)

no-first-use (adj)

no-fly zone(s)

noise-free

noisemaker(s)

noisemaking

noisome (offensive and disgusting, like a noisome odor, or harmful)

no man's land(s)

nom(s) de guerre

nom(s) de plume

non (as prefix, usually one word)
- nonaligned
- Nonaligned Movement (NAM)
- Nonaligned summit
- nonattributable
- noncommissioned officer
- noncontrol
- nonferrous
- nonlifelike
- nonMIRVed
- nongovernmental organization (NGO)
- nonnuclear
- nonoceangoing
- nonoil
- nonproliferation
- nonrotating-Earth (um, extraterrestrial context)
- nonuse of force (n)
- nonuse-of-force (adj)
- *but*
- non-CIA
- non-civil-service
- non-European
- non-intelligence-related
- non-interest-bearing (um)
- non-life-threatening (um)
- non-missile-equipped
- non-nuclear-powered
- non-nuclear-related
- non-nuclear-weapon state
- non-oil-producing
- non-party-member(s)
- non-printing character(s)
- Non-Proliferation Treaty (NPT, spell out for first use)
- non-rare-earth

nonetheless

no-no, no-no's (pl)

no-nonsense (adj)

nonplussed

non sequitur(s)

no one

northbound

north-central

northeast

northeastern

north end(s)

Northern Atlantic

north-northeast

North Rhine–Westphalia

north shore(s)

northward

nosecone(s)

nosedive(s)

no-show(s) (n, adj)

notebook(s)

note paper(s)

noteworthy

noticeable

notwithstanding

nouveau riche, nouveaux riches (pl)

novel-writing (um)

no-war/no-peace

now-dominant (um)

nowhere

NPT (Non-Proliferation Treaty; Nuclear Non-Proliferation Treaty, spell out on first use)

nuclear-armed (um)

nuclear-capable (um)

nuclear delivery (n, um)

nuclear-free (um)

Nuclear Non-Proliferation Treaty (NPT, spell out on first use)

C05757260

nuclear power(s) (n, um)
nuclear-powered (um)
nuclear-powered ballistic missile submarine (SSBN)
nuclear-related (um)
nuclear strike(s) (n, um)
nuclear-war-fighting (um)
nuclear weapon(s) (n, um)
nuclear-weapons-free (um)
nuclear-weapon-sized (um)
nuclear-weapons-related (um)
nuclear-weapon state(s)
nucleus, nuclei (pl)
number-one, number-two (um)

O

oasis, oases (pl)
oblast(s)
occasional
occupied territory, occupied territories (pl)
occur(s), occurred, occurring
occurrence(s)
oceanborne
oceangoing
oceanside
oceanwide
octavo(s)
October War
odd number(s)
odd-numbered (um)
off-and-on (um)
off-balance (adj)
off-base (adj)
off-campus (adj)
offcenter (um)
off chance
offcolor (um)
offday(s)
off-duty (adj)
offer(s), offered, offering
offguard
offhand
off-hours
officeholder(s)
officer-in-alias
officers club(s)
officeseeker(s)
office-seeking (um)
officeworker(s)
off-limit
off line (pred)
offline (adj, adv, comp)
off-load(s), offloaded, offloading
off-lying (um)
off-road (adj)
off-season(s)
offset(s), offset, offsetting
offshoot(s)
offshore
off-site (adj, adv)
offstage
off-the-record (um)
off-the-shelf
off-track
but
offtrack betting
off year(s)
oilfield
but
oil and gas fields
oil-processing (um)
oil-producing (um)
oil-rich
oil sands (n, um)
oilseed(s)
oil shale (n, um)
oil slick(s)
oilspill(s)
oil-soaked (um)
oil well(s)
oil workers

C05757260

old-boys network(s)
old-fashioned (um)
old-guard (adj)
old-line (adj)
old-style (adj)
oldtime
Olympic Games
Olympics
  Summer Olympics
  Winter Olympics
ombudsman, ombudsmen (pl)
on-and-off (um)
on-again/off-again
on board (pred)
onboard (adj)
once-impressive
once-over
one-half
one-man (adj)
one-man/one-vote (n, adj)
one-on-one (adj, adv)
oneself
one-sided (um)
one-time (adj, single instance)
onetime (um, former)
one up (adj)
one-up(s), one-upped, one-upping
one-upmanship
one-way
ongoing
on line (pred)
online (adj, comp)
on-screen
onshore
on-site (adj)
on-station (adj)
onstream (um)
on-the-job training
on-time (adj)
OPEC summit(s)
open-air (adj)
open-door (adj)
open-ended (um)
openhanded
open-heart (adj)
open house(s)
open-market (adj)
openminded
open-ocean (adj)
open pit(s) (n, um)
open-sea (adj)
open-source (adj)
opium poppy field(s)
  but
  poppyfield(s)
opium poppy grower(s), opium poppy growing (n)
opium-poppy-growing (um)
optoelectronics
orbit(s), orbited, orbiting (n, v)
orbital
orbiter(s)
order-of-battle (um)
ordinance(s) (law)
ordnance (weapons)
orthodox
ostensible
out (prefix, one word except with *of*)
  outfit(s), outfitted, outfitting
  outfitter(s)
  outmigration(s)
  outnumbered
  out-of-area (um)
  out-of-date (um)
  out-of-pocket (um)
  out-of-touch (um)
  out patient(s) (n, um)
outermost
over (cf, one word)
  Exception: over-snow vehicle(s)
overflow(s), overflowed, overflowing (n, adj, v)
overhead(s) (all senses)
overland radar(s)
overlap(s), overlapping, overlapped
overnight

C05757260

overreaching
overreact(s), overreacted, overreacting
overstaff(s)
overwrite(s), overwrote, overwriting
ozone-depleting (um)

P

pacemaker(s)
pace-setting (um)
Pacific Rim
page proof(s)
painstaking
palate(s) (roof of mouth)
palette(s) (range of colors, paint mixing tray)
palisade(s)
pallet(s) (bed, platform)
pan (cf, one word except with uppercase words, and then uppercase *P*)
panchromatic
pannational
pantheism
Pan-American
Pan-Slavic
pandemic(s)
panic buying
papacy, papacies (pl)
papal
papermaker(s)
papermaking
papermill(s)
paperwork
paragraph 12
parallel(s), paralleled, paralleling (n, v)
parallel processing
paralysis, paralyses (pl)
paralyze(s), paralyzed, paralyzing
paraphernalia
parastatal (state administered)
parcel(s), parceled, parceling (n, v)
parenthesis, parentheses (pl)
par excellence
Paris accords
parkland(s)
particle beam weapon(s)
partisan(s) (n, adj)
part owner(s)
part-time (adv, adj)
part way
party giver(s)
party goer(s)
party line(s)
partywide
passageway(s)
passenger car(s)
passer(s)-by
passport(s)
pass(es) through, passed through, passing through
passthrough(s) (n, adj)
password(s)
past-due (um)
pastureland(s)
pathbreaker(s)
pathfinder(s)
patrol(s), patrolled, patrolling (n, v)
pay(s) back, paid back, paying back
payback(s) (n)
paycheck(s)
payload(s)
pay(s) off, paid off, paying off
payoff(s) (n, um)
payroll(s)
peacekeeping
peace-loving (um)
peacemaking
peace talks
peacetime(s)
pedal(s), pedaled, pedaling (n, v)
pending (yet to come or not yet settled)
peninsulawide
pen name(s)

C05757260

pent-up (um)
peptalk(s)
per capita
percent(s)
percentage(s)
percentile(s)
perceptible
per diem
peremptory
perestroika
permafrost
Permanent Representative(s) to the UN
Permanent Five (in UNSC)
permissible
permit(s), permitted, permitting (n, v)
perquisite(s) (privilege; see *prerequisite*)
per se
Persian Gulf state(s)
Persian Gulf war (Gulf war)
persistent
personal (of the individual)
persona non grata, personae non gratae (pl)
personnel (staff)
perspective(s) (view; see *prospective*)
persuadable
persuasible
petro (cf, usually one word)
  petrodollars
  but
  petro-occipital
phased-array (adj)
phase(s) down, phased down, phasing down
phasedown(s) (n, um)
phase(s) in, phased in, phasing in
phasein(s) (n, um)
phase(s) out, phased out, phasing out
phaseout(s) (n, um)
Ph.D.('s)
phenomenon, phenomena (pl)
Philippines, the (n)
phone-in (um)
photo (cf, usually one word)
  photocopy, photocopies (pl)
  photomap(s)
  photoreconnaissance satellite(s)
  but
  photo atlas(es)
  photo-offset(s)
  photo-oxidation
picayune
picket line(s)
pick-me-ups
pickpocket(s)
pick(s) up, picked up, picking up
pickup (n, um)
picnicking
piece goods
piecemeal
piece rate(s)
piecework(s)
pieceworker(s)
piggyback
piledriver(s)
pinpoint(s), pinpointed, pinpointing (n, v, adj)
pinstripe(s)
pin-striped
pipe bomb(s)
pipedream(s)
pipefitting(s)
pipelaying
pipeline(s)
pipe smoker(s)
place name(s)
plainclothes
plainclothesman, plainclothesmen (pl)
plain-spoken (um)
plaintext
planeload(s)
plantlife
plaster of Paris
plateau(s)
plate glass
plausible
playboy(s)
plea-bargain(s), plea-bargained, plea-bargaining (n, um, v)

C05757260

plenum(s)

PLO Chairman

plowshare(s)

plug-in (n, um)

plus or minus (adj, adv)

p.m.

pock-marked (um)

pointblank

point man, point men (pl)

police (always plural)

policymaker(s)

policymaking (spell as two words when accompanying adjective modifies only policy as in *economic policy making*—but *unauthorized policymaking*)

politicking

politico (cf, usually one word)
but
politico-orthodox

politics (always singular)

pollwatcher(s)

poor-quality (adj)

poppyfield(s)
but
opium poppy field(s)

poppy grower(s), poppy growing (n)

poppy-growing (um)

poppyseed(s)

popular-front (adj)

populate(s), populated, populating

popup(s) (n, um)

pork-barrel (adj)

portentous

porthole(s)

portside

post (pref, usually one word)
postattack
postboost
postcoup
postgraduate
posthaste
postmortem
postreentry
posttest
posttreatment
posttreaty
but
post-9/11 (adj)
post bellum
post-civil-war (um)
post-target-tracking

postcard(s)

potbellied

potboiler(s)

potluck

potpourri(s)

potshot(s)

poultryman, poultrymen (pl)

poultry-raising (um)

poverty-stricken

power base(s)

power breakfast(s)

power broker(s)

power-driven (um)

power-generating (um)

power grab(s)

power grid(s)

powerhouse(s)

powerline(s)

power plant(s)

power play(s)

power-projection (adj)

power sharing (n)

power-sharing (um)

power station(s)

practice(s), practiced, practicing (n, v)

praiseworthiness

praiseworthy

pre (pref, usually one word)
predetente
preelection
preexisting
preindependence
premed (adj)
prewar
but
pre-flight-test (um)
pre-Incan

C05757260

pre-position(s), pre-positioned, pre-positioning (position in advance)
pre-martial-law

precede(s), preceded, preceding (go ahead of)

precedence (priority)

precedents (prior instances)

precis (sing, pl)

precision-guided missile(s) (PGM)

predilection(s)

predominant (adj)

predominate(s), predominated, predominating

preempt(s), preempted, preempting

prefer(s), preferred, preferring

preferable

preference(s)

prerequisite(s) (need; see *perquisite*)

present-day (adj)

presidential (non-US)

Presidential (US; see footnote 8)

presidential guard(s)

president(s)-elect

President-elect (US)

press agent(s)

press-gang(s), press-ganged, press-ganging (n, v)

presstime(s)

prevaricate(s), prevaricated, prevaricating

price-sharing (um)

prima donna behavior

prima facie

prime minister(s)

prime-minister-designate (general sense)
but
the Prime Minister–designate

prime-ministerial

prime-ministership(s)

prime-ministry, prime-ministries (pl)

prime mover(s)

prime-time (adj)

principal (sum of money, chief)

principle(s) (proposition)

printout(s)

printshop(s)

prisoner(s) of war (n)

prisoner-of-war (um)

private-sector (adj)

privilege(s)

prizewinner(s)
but
Nobel Prize winner

prizewinning

pro (as a prefix meaning "in favor of," generally one word)
proactive
proapartheid
profederal
progovernment
proreform
proregime
prowar
but
pro-African
pro-arms-control (um)
pro-free-market (um)
pro-free-trade
pro-ruling-party
Note: When used as part of a Latin phrase, *pro* stands alone and is not hyphenated.
pro forma
pro rata
pro tem
pro tempore

problem solver(s)

problem-solving (um)

proceed(s), proceeded, proceeding (n, v)

processible

producible

production-sharing (um)

proffer(s), proffered, proffering

profit(s), profited, profiting (n, v)

profitable

profit-and-loss (um)

profitmaking

profit-sharing (um)

program(s), programmed, programming (n, v)

programmable

programmatic

programmer(s)

C05757260

prologue(s)
proofread(s), proofread, proofreading
propel(s), propelled, propelling
propellant(s)
prophecy, prophecies (n)
prophesier(s)
prophesy, prophesies, prophesied, prophesying
propjet(s)
prospective (anticipated; see *perspective*)
protege(s)
protester(s)
protocol(s)
prove(s), proved, proving
proved (adj, for energy reserves only)
proven (adj, except energy reserves)
proviso(s)
pseudo (cf, usually one word)
but
pseudo-Messiah
pseudo-official
pseudo-peace-loving
publicity-conscious (um)
public-sector (adj)
public-spirited (um)
public works
pullback(s) (n, um)
pullout(s) (n, um)
pulsed Doppler effect
pulse-Doppler
pulsewidth(s)
pummel(s), pummeled, pummeling
pump house(s)
pump-priming (um)
pump station(s)
purse strings
pushover(s) (n, um)
pushup(s) (n, um)
put-on(s) (n, um)
put-up(s) (n, um)

Q

quality-of-life (um)
quarrel(s), quarreled, quarreling
quarterdeck(s)
quartermaster(s)
quadripartite
quasi (pref, all hyphenated)
Note: quasi can also be a separate adj.
quasi currency board
questionnaire(s)
queue(s)
quick-count polling
quick fix(es)
quick-reaction (adj)
quicksilver (n, adj)
quick time
quick-witted (um)
quid pro quo(s)
quitclaim(s)

R

rabble-rouser(s)
racehorse(s)
racetrack(s)
rack(s), racked, racking (n, v; see *wrack*)
radar-absorbing (um)
radar-cross-section(s)
radar tracking
radio (cf, usually one word)
radioactive
radiobroadcast(s)
radioelectronic(s) (n, adj)
radiofrequency, radiofrequencies
radioisotope(s)
radiotelegraph(s)
radiotelephone(s)
but
radio amplifier(s)
radio antenna(s)
radio-cassette(s)

C05757260

radio channel(s)
radio communication(s)
radio control(s)
radio engineer(s)
radio engineering
radio link(s)
radio navigation
radio range(s)
radio receiver(s)
radio relay(s)
radio set(s)
radio station(s)
radio transmitter(s)
radio tube(s)
radio wave(s)

radius, radii (pl)
rag-tag
railborne
railcar(s)
railhead(s)
rail line(s)
rail-mobile (um)
rail net(s)
railroad(s)
railroader(s)
rail shed(s)
rail spur(s)
rail train(s)
railway(s)
railwayman, railwaymen (pl)
railyard(s)
raincheck(s)
rainfall(s)
rain-fed (um)
rain forest(s) (n)
rainforest (um)
rainmaking
rainproof
rainshower(s)
rainspout(s)
rainstorm(s)
raintight
rainwater
raison(s) d'etre
RAM (random-access memory, read/write memory)
Ramadan
ramjet(s)
ramrod(s)
ramshackle
rangefinder(s)
rangehead(s)
range rate(s) (n)
range-rate (adj)
rank and file (n)
rank-and-file (adj)
rapid fire (n)
rapid-fire (adj)
rapid transit
rapid-reaction (adj)
rapid-response (adj)
rapporteur(s)
rapprochement(s)
rare-earth (um)
rate-cutting (um)
rate-fixing (um)
ratesetting
rat-infested (um)
ratline(s)
rat race(s)
ravels, raveled, raveling
razor-sharp (um)
re (pref, usually one word)
realign(s), realigned, realigning
redirect(s), redirected, redirecting
reemerge(s), reemerged, reemerging
reenter(s), reentered, reentering
reentry, reentries (pl)
reequip(s), reequipped, reequipping
reestablish(es), reestablished, reestablishing
reevaluate(s), reevaluated, reevaluating
reexport(s), reexported, reexporting
reformat(s), reformatted, reformatting
refuel(s), refueled, refueling
reignite(s), reignited, reigniting
reinforce(s), reinforced, reinforcing
reman(s), remanned, remanning
reinstate(s), reinstated, reinstating
reinvent(s), reinvented, reinventing

C05757260

reprocess(s), reprocessed, reprocessing
reuse(s), reused, reusing
but
re-cover(s), re-covered, re-covering (cover again)
re-create(s), re-created, re-creating (create again)
re-cross-examination
re-form(s), re-formed, re-forming (form again)
re-ice(s), re-iced, re-icing
re-ink(s), re-inked, re-inking
re-present(s), re-presented, re-presenting (present again)
re-redirect(s), re-redirected, re-redirecting
re-treat(s), re-treated, re-treating (treat again)

readout(s)

ready-built (um)

readymade

ready reference(s)

real estate (n, um)

realpolitik

real-time (adj)

rear area(s) (n, um)

rear end(s)

rear-guard (adj)

rear service(s)

rear services area

rebel(s), rebelled, rebelling

rebut(s), rebutted, rebutting (to argue to the contrary; see *refute*)

recently designed logo(s)

receptacle(s)

reconnaissance(s)

reconnoiter(s), reconnoitered, reconnoitering

recordbreaking

recordkeeping

recordmaking

red, redder, reddened, reddening

red-blooded (um)

red-carpet (adj)

red-haired (um)

redhanded

redhead(s)

redheaded

red-hot (um)

redound(s), redounded, redounding

red tape(s) (literal)

redtape (nonliteral)

reduced-observable(s) (n, adj)

reducible(s)

refer(s), referred, referring

referable

reference(s), referenced, referencing (n, v)

referendum(s)

reform-minded

refute(s), refuted, refuting (connotes success in winning the argument; see *rebut*)

regionwide

reign(s), reigned, reigning (n, v; to exercise sovereign power)

rein(s), reined, reining (n, v; to guide, to control, or—with *in*—to hold back)

relations with

relevant

reluctant (unwilling to act; see *reticent*)

reminiscent

remit(s), remitted, remitting

remote-control (adj)

remote-controlled

remote-sensing (um)

renaissance(s)
but
the Renaissance

Renaissance man, Renaissance men (pl)

rent-free

repairman, repairmen (pl)

replication(s)

reprehensible

Representative(s) (US Congress)

representative(s) at large

representative(s)-elect

republicwide

requester(s)

research study, research studies (pl)

Resident(s) (diplomatic)

residence(s)

resilience

resilient

C05757260

resistance
resistant
rest cure(s)
rest home(s)
restroom(s)
resume(s), resumed, resuming
reticent (uncommunicative or reserved; see *reluctant*)
retrofire
retrofit(s), retrofitted, retrofitting
retrorocket(s)
Reuters (news agency)
reverse-engineer(s), reverse-engineered, reverse-engineering
reversible
revise(s), revised, revising
Revolutionary Guard (force or members)
ricefield(s)
rice growing (n)
riceland(s)
ridge line(s)
rifleman, riflemen (pl)
right-angled (um)
right away
right-hand (adj)
right-handed (um)
right(s)-of-way
right-to-work (adj)
right turn(s)
right wing(s)
rightwing (adj)
rightwinger(s)
ringleader(s)
ring-shaped (um)
ringside(s)
ringworm
riot-control (adj)
riptide(s)
rise(s), rose, rising (n, v)
risk taker(s)
risk taking
rival(s), rivaled, rivaling
riverbank(s)
riverbed(s)
riverborne
river bottom(s)
river-crossing
riverfront(s)
riverside(s)
roadbed(s)
roadblock(s)
roadbuilding
road-clearing (um)
roadmap(s)
road-mobile (um)
road scraper(s)
road show(s)
roadside(s)
road-test(s), road-tested, road-testing (n, v)
roadway(s)
road-weary (um)
rob(s), robbed, robbing
rockbottom (nonliteral)
rockslide(s)
rock wool
rogue state(s)
rollback(s) (n, um)
rollcall(s)
rolling-stock (adj)
roll-on/roll-off (um, of ships)
Ro/Ro (military) or **ro/ro**
roll(s) out, rolled out, rolling out
rollout (n, um)
rollout-to-launch (um, of weapons)
rollover(s) (n, um)
roll(s) up, rolled up, rolling up
roll-up (n, um)
ROM (read-only memory)
rooftop(s)
rough-and-ready (um)
rough-and-tumble (n, adj)
roughcast (um, v)

C05757260

rough-faced (um)
roughhewn
roughhouse(s), roughhoused, roughhousing (n, v)
roughneck(s) (n, adj)
roughrider(s)
rough-sketch(es), rough-sketched, rough-sketching (n, v)
roundabout(s) (n, um)
roundrobin(s) (petition)
roundtable(s) (panel)
round-the-clock
round-topped
round trip(s) (n, um)
round(s) up, rounded up, rounding up
roundup (n, um)
rubbernecker(s)
rubber plant(s)
rubber stamp(s) (literal, n)
rubberstamp(s), rubberstamped, rubberstamping (nonliteral, n, um, v)
rubber-stamped (literal, um)
rubles' (pl possessive)
rulemaking
rule(s) of thumb
rules-of-origin
ruling-family (adj)
ruling-party (adj)
rumormonger(s)
runaround(s) (n, adj)
runaway(s) (n, adj)
rundown(s) (n, um)
run(s) in, ran in, running in
run-in(s) (n, um)
runner-up, runners-up (pl)
running mate(s)
runoff(s) (n, um)
runthrough(s) (n, um)
run(s) up, ran up, running up
runup(s) (n, um)
runway
rush hour(s)
Russian Far East
rustproofing
rust-resistant (um)

S

saber rattling(s) (n)
saber-rattling (um)
saddle stitch(es) (n)
saddle-stitch(es), saddle-stitched, saddle-stitching
saddle-stitched (um)
safe-conduct(s) (n, adj)
safecracking
safe-deposit (adj)
safeguard(s), safeguarded, safeguarding (n, v)
safe haven(s)
safehouse(s)
safehouse keeper(s)
safehouse keeping
safekeeping
sailboat(s)
sailcloth(s)
sailmaking
salable
salesmanship
salesperson, salespeople (pl)
sales tax(es)
SALT (strategic arms limitation talks)
salt flat(s)
saltwater(s)
salvo(s)
samizdat(s)
samurai
San Andreas Fault
sanatorium(s)
sandbag(s), sandbagged, sandbagging (n, v)
sandbank(s)
sandbar(s)
sandblast(s), sandblasted, sandblasting (n, v)

C05757260

sand dune(s)
Sandinista(s)
sandpaper(s), sandpapered, sandpapering (n, v)
sandstorm(s)
sandy-bottomed (um)
sanguinary (bloodthirsty)
sanguine (ruddy or optimistic and cheerful)
sanitarium(s)
satellite(s)
satellite-borne (um)
sawmill(s)
saw-toothed (um)
say-so (n)
scale(s) up, scaled up, scaling up
scaleup(s) (n)
scale(s) back, scaled back, scaling back
scandalmongering
scapegoat(s)
scaremonger(s)
scareproof
scatterbrained
scene setter(s)
school-age (adj)
school board(s)
schoolbook(s)
schoolboy(s)
schoolbus(es)
schoolchildren
schoolday(s)
schoolgirl(s)
schoolgrounds
schoolhouse(s)
schoolroom(s)
schools of thought
schoolteacher(s)
but
high school teacher
school-trained (um)
schoolwork
schoolyard(s)
school year(s)
scorched-earth (adj)
scoreboard(s)
scorecard(s)
scorekeeping
scot-free
Scotsman, Scotsmen (pl)
scout car(s)
scrapbook(s)
scrap heap(s)
scrap iron
scrap paper(s)
scrapyard(s)
scratch pad(s)
scratch test(s)
screw-driven (um)
screw propeller(s)
screw-threaded (um)
screw wheel(s)
scrubland(s)
scuba
Scud B('s)
scuttlebutt
sea
sea-based (um)
seabed(s)
seaboard(s)
seaborne
seacoast(s)
seacraft
seafaring
seafloor(s)
seafood(s)
seagoing
seakeeping
sea lane(s)
sea-launched cruise missile(s) (SLCM)
sea level
sea life
sealift(s), sealifted, sealifting (n, v)
sea lines of communication (SLOC)
sea lion(s)
seaplane(s)
seaport(s)
seapower
sea route(s)
seashore(s)
seasick

C05757260

seaside(s)
sea test(s), sea tested, sea testing (n, v)
seawall(s)
seaward
seawater
seaway(s)
seaworthy

search-and-destroy (um)

search engine(s)

searchlight(s)

searchplane(s)

seatbelt(s)

second
second-best (um)
second-class (adj)
second-degree (adj)
second-generation (adj)
second-guess(es)
second-guessed
second-guessing (v)
second-half (adj)
second hand(s) (n)
secondhand (adv, adj)
second in command
second-largest (adj)
second-leading (um)
secondmost
but
second-most-powerful (um)
second-quarter (adj)
second-ranking (um)
second-rate
second-rater(s)
second-tier (um)

Second World War

secretary general, secretaries general (pl)

secretary-generalship

secretaryship(s)

secretary-treasurer

secret service(s)

secret society, secret societies (pl)

secretwriting

security decisionmaking

seesaw(s), seesawed, seesawing (n, adj, v)

seize(s), seized, seizing

self (reflexive prefix, use hyphen)

self-motivated

self-trained

selfless

selfsame

sell(s) off, sold off, selling off

selloff(s) (n, adj)

sellout(s) (n, um)

semi (pref, usually one word)
semiannually (twice a year; use in preference to biannually; see also *biennially*)
semiarid
semidesert
semiofficial
semiweekly (twice a week; see *biweekly*)
but
semi-armor-piercing
semi-Christian
semi-idleness
semi-independent
semi-indirect
semi-land-mobile
semi-winter-hardy

Senator(s) (US Congress)

sendoff(s) (n, um)

separate(s), separated, separating

Serbo-Croatian

serious-minded (um)

serviceable

service-connected (um)

serviceman, servicemen (pl)

servicewide

servicewoman, servicewomen (pl)

servomechanism(s)

set(s) back, set back, setting back

setback(s) (n, um)

set(s) down, set down, setting down

setdown(s) (n, um)

set(s) in, set in, setting in

set-in(s) (n, um)

set(s) off, set off, setting off

setoff(s) (n, um)

setpiece(s)

set-to(s) (n, um)

set(s) up, set up, setting up

setup(s) (n, um)

C05757260

sevenfold
severalfold
shadowbox(es), shadowboxed, shadowboxing
shake(s) down, shook down, shaking down
shakedown(s) (n, um)
shake(s) out, shook out, shaking out
shakeout(s) (n, um)
shake(s) up, shook up, shaking up
shakeup(s) (n, um)
shallow-draft (adj)
shamefaced
shameworthy
shantytown(s)
shaped-charge (adj, of warheads)
sharecropper(s)
shareholder(s)
sharia
sharp-angled (um)
sharp-edged (um)
sharpshooting
sharp-witted (um)
shaykh(s)
sheep farm(s)
sheepherder(s)
sheepherding
sheepkeeping
sheepland(s)
sheepshearing
sheepskin(s)
sheet metal(s)
shelf life, shelf lives (pl)
shelf plate(s)
shellburst(s)
shellfish
shell game(s)
shellhole(s)
shell-like
shellproof
shellshocked
sherpa(s)
ship (suffix, usually one word)
partnership(s)
premiership(s)
prime-ministership(s)
shipboard
shipborne
shipbuilder(s)
shipbuilding
ship-day(s)
shipload(s)
shipowner(s)
shipowning
shipshape
shipwreck(s), shipwrecked, shipwrecking (n, v)
shipyard(s)
shock wave(s)
shogun(s)
shoo-in(s)
shoot(s) down, shot down, shooting down
shootdown(s) (n)
shootout(s)
shopkeeping
shoplift(s), shoplifted, shoplifting (n, v)
shopowner(s)
shoptalk
shopworn
shoreland(s)
shore leave(s)
shoreline(s)
shortchange(s), shortchanged, shortchanging
short circuit (n)
short-circuit(s), short-circuited, short-circuiting
short-circuited (um)
shortcoming(s)
shortcut (n, adj, v)
shortfall(s)
shorthand (writing)
short-handed (um)
short-lived (um)
short-range (adj)
short run(s) (n)
shortrun (um)

C05757260

shortsighted
short-term (adj)
short-to-long (adj)
short-to-long-range (adj)
shortwave(s) (n, adj; radio)
shoulder-launched (um)
showcase(s)
showdown(s)
showman, showmen (pl)
showoff(s) (n, um)
showpiece(s)
shura
shut(s) down, shut down, shutting down
shutdown(s) (n, um)
shut(s), shut in, shutting in
shut-in(s) (n, um)
shut(s) off, shut off, shutting off
shutoff(s) (n, um)
shut(s) out, shut out, shutting out
shutout(s) (n, um)
sickbay(s)
sickbed(s)
sick leave
sidearm(s)
sidebar(s)
side effect(s)
side line(s) (literal)
sideline(s), sidelined, sidelining (nonliteral; n, v)
side lobe(s)
side road(s)
side-scan radar
sideshow(s)
sidestep(s), sidestepped, sidestepping (n, v)
sideswipe(s), sideswiped, sideswiping (n, v)
sidetrack(s), sidetracked, sidetracking (n, v)
sidetrip(s)
sidewalk(s)
sideways
siege(s)
sightreading
sightsaving
sightsee(s), sightsaw, sightseeing
sightseer(s)
SIGINT
signal(s), signaled, signaling (n, v)
signaler(s)
signalman, signalmen (pl)
signal-processing (um)
signal tower(s)
sign(s) off, signed off, signing off
signoff(s) (n, um)
sign(s) on, signed on, signing on
sign-on(s) (n, um)
signpost(s), signposted, signposting (n, v)
sign(s) up, signed up, signing up (n, v)
signup(s) (n, um)
silk screen(s), silk screened, silk screening (n, v)
silkworm(s)
silo-based (um)
silver-gray (um)
silver-haired (um)
silver-tongued (um)
silverworker(s)
simon-pure (um)
simple-minded (um)
simple-witted (um)
simulcast(s), simulcast, simulcasting (n, v)
sine qua non(s)
single-handed (um)
single-handedly (adv)
single-minded (um)
single-mindedly (adv)
single-mindedness
single-most-important (um)
single-seat (adj)
single-source (adj)
single-track (adj)
single warhead
Sino- (as prefix)
siphon(s)
sister(s)-in-law
sitdown(s) (n, um)

C05757260

sit(s) in, sat in, sitting in
sit-in(s) (n, um)
Six-Day War
sizable
ski(s), skied, skiing (n, v)
skillful
skindeep
skinhead(s)
skyjack(s), skyjacked, skyjacking
skyjacker(s)
skyjacking(s) (n, adj)
skylight(s)
skyline(s)
skyrocket(s), skyrocketed, skyrocketing (n, v)
skyscraper(s)
skyward
skywriting
slaughterhouse(s)
slaveholding
slaveowner(s)
slave trade
SLBM(s) (submarine-launched ballistic missile)
SLCM(s) (sea-launched cruise missile)
sledge hammer(s)
sleepwalk(s), sleepwalked, sleepwalking (n, v)
sleetstorm(s)
slide rule(s)
slip(s) up, slipped up, slipping up
slip-up(s) (n, um)
SLOC (sea lines of communication)
slowdown(s) (n, um)
slowgoing
slow-motion (adj)
slow-moving (um)
slowpoke(s)
slow time(s)
slowup(s) (n, um)
slow-witted (um)
sluice gate(s)
slumdweller(s)
slumlord(s)
small arms (n)
small-arms (adj)
small business(es)
small businessman, small businessmen (pl)
smallpox
small-scale (adj)
smalltalk
small-time (adj)
small-timer(s)
small-to-moderate (um)
smalltown (um)
small-unit (adj)
smart aleck(s)
smart-alecky (um)
smart-looking (um)
smart set(s)
smashup(s) (n, um)
smear culture(s)
smokebomb(s)
smoke-filled (um)
smokeproof
smokescreen(s)
smokestack(s)
smolder(s), smoldered, smoldering
smoothbore(s) (n, adj)
smooth-tongued (um)
smooth-working (um)
smudge pot(s)
snail-paced
snail's pace
snowball(s)
snowbank(s)
snowbound
snowcapped
snow cover(s)
snow-covered (um)
snowcraft
snowdrift(s)
snowfall(s)
snowline(s)
snowmobile(s)

C05757260

snowshoe(s)
snowstorm(s)
snow-topped (um)
snow-white (um)
soapbox(es)
soap opera(s)
sober-minded (um)
sobersided
sob story, sob stories (pl)
so-called (um)
social work
social worker(s)
socio (cf, usually one word)
socioeconomic
but
socio-official
soft coal
soft copy, soft copies (pl) (n)
soft-copy (adj)
soft drink(s) (n, um)
soft goods
softhearted
soft-pedal(s), soft-pedaled, soft-pedaling (v)
soft-soap(s), soft-soaped, soft-soaping (v, nonliteral)
soft-spoken (um)
software
Solidarity (Poland)
solid-propellant (adj)
solid rocket propellant(s)
solid-state (adj)
solo(s)
somebody (pronoun)
somebody, somebodies (pl) (n)
someday
somehow
someone (anyone)
some one (distributive)
someplace (adv)
something
some time (n, an unspecified time)
sometime (adj, occasional; adv, at an unspecified time)
sometimes (adv, occasionally)
somewhat
somewhere
son(s)-in-law
sonobuoy(s)
soon-to-be- (um, often prefixed)
sore point(s)
sorry-looking (um)
soulmate(s)
soul-searching (um)
sound-absorbing (um)
soundingboard(s)
sound-minded (um)
soundoff(s) (n, um)
soundproof(s), soundproofed, soundproofing (adj, v)
sound wave(s)
sourfaced
sour-natured (um)
sous-sherpa(s)
southbound
south-central
southeast
southeast-bound (um)
south end(s)
south side(s)
south-southeast
southward
southwest
soybean(s)
space age
space-based (um)
spaceborne
spacecraft
spaceflight(s)
space key(s)
space launch site(s) (n, um)
space mine(s)
space plane(s)
spaceship(s)
space station(s)

C05757260

space suit(s)
space tracking (n, um)
space walk(s)
spam(s), spammed, spamming (n, v)
Spanish American
Spanish-born (um)
Spanish-speaking (um)
spare-parts (adj)
spark plug(s)
special envoy(s)
special-forces (adj)
special-interest (adj)
special-purpose (adj)
Special Weapons and Tactics (SWAT)
specter(s)
spectrum, spectra (pl)
speechwriter(s)
speechwriting
speedboat(s)
speedwriting
spellbind(s), spellbound, spellbinding
spellbinder(s)
spell check(s), spell checked, spell checking
spell checker(s)
spendthrift(s)
spent-fuel (adj)
spent nuclear fuel reprocessing plant(s)
spill(s) over, spilled over, spilling over
spillover(s) (n, um)
spillway(s)
spin doctor(s), spin-doctored, spin-doctoring (n, v)
spin control
spin(s) off, spun off, spinning off
spinoff(s) (n, um)
spin(s) up, spun up, spinning up
spinup(s) (n, um)
splash(es) down, splashed down, splashing down
splashdown(s) (n, um)
split second (n)
split-second (adj)
split(s) up, split up, splitting up
splitup(s) (n, um)
spoilsport(s)
spokesperson(s) (spokespeople alt pl)
sports bar(s)
sportsmanlike
spot check(s) (n)
spot-check(s), spot-checked, spot-checking
spreadsheet(s)
spring(s) (season)
springboard(s)
spring fever
springtime(s)
spur line(s)
square-bottomed (um)
square deal(s)
square meter(s)
square root(s)
squeeze play(s)
SRF (Strategic Rocket Forces)
SS-7(s)
SSB(s) (ballistic missile submarine)
SSBN(s) (nuclear-powered ballistic missile submarine)
SS-N-4(s)
S&T (science and technology)
stadium(s)
stage-manage(s), stage-managed, state-managing
stairstep (adj)
stalemate(s), stalemated, stalemating (n, v)
stalking-horse(s)
stanch(es), stanched, stanching (v, stop, especially with regard to a heavy outflow; see *staunch*)
stand(s) alone, stood alone, standing alone
stand-alone(s) (n, adj)
standard bearer(s)
standard gauge(s) (n)
standard-gauge (adj)
standard time(s)
stand(s) by, stood by, standing by
standby(s) (n, um)

C05757260

stand(s) down, stood down, standing down
standdown(s) (n, um)
stand(s) fast, stood fast, standing fast
standfast(s) (n, um)
stand(s) in, stood in, standing in
stand-in(s) (n, um)
standing-room-only (um)
stand(s) off, stood off, standing off
standoff(s) (n, um)
standoffish
stand(s) out, stood out, standing out
standout(s) (n, um)
stand(s) pat, stood pat, standing pat
standpat(s) (n)
standpatter(s)
standpoint(s)
stand(s) still, stood still, standing still
standstill(s) (n, um)
stand(s) up, stood up, standing up
standup(s) (n, um)
starboard
star-spangled (um)
start(s) up, started up, starting up
startup(s) (n, um)
state banking system(s)
state enterprise industrial sector(s)
state enterprise sector(s)
statehood
state of the art (n)
state-of-the-art (adj)
state of the union
state of war (n)
state-of-war (adj)
stateroom(s)
state-run (um)
statesman, statesmen (pl)
statesmanlike
stateswoman, stateswomen (pl)
statewide
stationary (fixed)
stationery, stationeries (pl) (paper)
stationmaster(s)
station wagon(s)
Status of Forces Agreement (SOFA)
status quo
statute book(s)
statute mile(s)
staunch (adj, steadfast; see *stanch*)
stay-at-home(s) (n, adj)
staybehind(s) (n)
stealth
stealth bomber(s)
stealth technology, stealth technologies (pl)
steamboat(s)
steam-driven (um)
steam engine(s)
steamer-borne (um)
steamer line(s)
steamfitting
steam heat
steampipe(s)
steam-propelled (um)
steamroller(s), steamrollered, steamrollering (n, um, v)
steamship(s)
steelhearted
steelmaking
steel mill(s)
steel-producing (um)
steel trading
steel wool
steelworker(s)
steelworks
stepbrother(s)
stepchild, stepchildren (pl)
steppingstone(s)
stepsister(s)
step(s) up, stepped up, stepping up
step-up(s) (n, um)
stick-in-the-mud(s) (nonliteral)
stick-to-it-iveness
stillborn

C05757260

still life(s)
still-lingering (um)
still-to-be- (um, often prefixed)
still-unseated (um)
stimulus, stimuli (pl)
stockholder(s)
stock-in-trade
stock market(s) (n, um)
stockpile(s), stockpiled, stockpiling (n, v)
stockraising
stock-still (um)
stocktaking(s)
stockyard(s)
stone-cold (um)
stonecutting
stone-deaf (um)
stonehearted
stone wall(s) (n)
stonewall(s), stonewalled, stonewalling (v, nonliteral)
stopgap(s)
stoplight(s)
stop(s) off, stopped off, stopping off
stopoff(s) (n, adj)
stop(s) over, stopped over, stopping over
stopover(s) (n, adj)
stopwatch(es)
storefront(s)
storeowner(s)
storm-swept (um)
storytelling(s)
storywriting
stouthearted
stow(s) away, stowed away, stowing away
stowaway(s) (n, um)
straightaway
straight face(s)
straight-faced (um)
straightforward
straight line(s)
straight shooter(s)
straight-shooting (um)
straight-spoken (um)
straight-talker(s)
straight-talking (um)
straitjacket(s)
straitlaced
stranglehold(s)
straphanger(s)
strap(s) on, strapped on, strapping on
strap-on (n, adj)
stratagem(s)
Strategic Rocket Forces (SRF)
stratum, strata (pl)
strawman, strawmen (pl) (nonliteral)
straw vote(s)
streambed(s)
streamline(s), streamlined, streamlining
streetcar(s)
streetsmart (adj)
street smarts (n)
streetwise
stretchout(s) (n, um)
strikebreaker(s)
strike(s) out, struck out, striking out
strikeout(s) (n, um)
strike(s) over, struck over, striking over
strikeover(s) (n, um)
strong-arm(s), strong-armed, strong-arming (um, v)
strongbox(es)
stronghearted
stronghold(s)
strongman, strongmen (pl) (nonliteral)
strong-minded (um)
strong point(s) (personal forte)
strongpoint(s) (military fortification)
strong-willed (um)
stubbornness
stumblingblock(s)
stupid-looking (um)
stylebook(s)

C05757260

style guide(s)

style manual(s)

Su-20(s)

sub (cf, usually one word)
subbalance(s)
subbasement(s)
subbasin(s)
subchaser(s)
subcommittee(s)
subcontinental
submachinegun(s)
submarginal
subpolar
substandard
subsystem(s)
subunit(s)
but
sub-Himalayan
sub rosa
Sub-Saharan
sub-subcommittee(s)

submarine-launched ballistic missile(s) (SLBM)

submit(s), submitted, submitting

subpoena(s)

subtlety, subtleties (pl)

succeed(s), succeeded, succeeding

sudden-death (um)

sugar beet(s)

sugarcane(s)

sugar-coat(s), sugar-coated, sugar-coating

sugar-coated (um)

sugar mill(s)

sulfur (derivatives also spelled with *f*)

summer(s) (season)

summer school(s)

summertime(s)

summit(s) (literal and nonliteral, initial letter not capitalized; example: OPEC summit)

sundown(s)

sun-dried (um)

sunlit

sunstroke(s)

suntan(s), suntanned, suntanning (n, v)

sunup(s)

super (pref, usually one word. Note that *super* can also be a separate word—n, or, informally, adj or adv)
superegoist(s)
superhighway(s)
superpower(s)
supermarket(s)
but
super-Christian
super-high-frequency, super-high-frequencies (pl) (n, adj)
super-superlative(s) (n, adj)

supersede(s), superseded, superseding

supervise(s), supervised, supervising

supra (pref, usually one word)
supranational
suprarenal
but
supra-abdominal
supra-Christian

sure-fire (adj)

sure-footed (um)

sure thing(s)

surface-burst (adj)

surface ship(s) (n, um)

surface-to-air (um)

surge protector(s)

surmise(s), surmised, surmising (n, v)

surprise(s), surprised, surprising (n, v)

surreptitious

surveil(s), surveilled, surveilling

surveillance

susceptible

SWAT (Special Weapons and Tactics)

sweepstake(s)

sweptback(s) (n, um)

sweptwing(s) (n, um)

swing shift(s)

swingwing(s)

switchblade(s)

switchboard(s)

switch box(es)

switch(es) over, switched over, switching over

switchover(s) (n)

switch tower(s)

switchyard(s)

C05757260

syllabus(es)
symposium(s)
synonymous
synopsis, synopses (pl)
synthetic-aperture (adj, of radar)
syrup(s)
system backup(s)
systemwide (adj)

T

table A-4
tableau(s)
taboo(s)
tailgate(s), tailgated, tailgating (n, v)
tailormade
tailpipe(s)
tailspin(s)
Taiwan (n, adj)
take(s) down, took down, taking down
takedown(s) (n, um)
take(s) home, took home, taking home
take-home(s) (n, adj)
take(s) off, took off, taking off
takeoff(s) (n, um)
take(s) out, took out, taking out
takeout(s) (n, um)
take(s) over, took over, taking over
takeover(s) (n, um)
take(s) up, took up, taking up
takeup(s) (n, um)
talebearer(s)
talemonger(s)
taleteller(s)
Taliban (takes singular verb)
tamperproof
tangible(s) (n, adj)
tank(s) (lowercase, even after a proper title—Abrams tank)
tank car(s)
tape deck(s)
tape-record(s), tape-recorded, tape-recording
tape recorder(s)
target(s), targeted, targeting
targetable
targeter(s)
task force(s)
taskmaster(s)
tax collector(s)
tax dodger(s)
tax-exempt (um)
tax form(s)
tax-free (um)
taxi(s)
taxpaying
tax-supported (um)
teachers college (no apostrophe)
teamplay
teamplayer(s)
teamwork
tear(s) down, tore down, tearing down
teardown(s) (n, um)
teargas(es), teargassed, teargassing (n, v, um)
teenage
teenager(s)
tele (cf, all one word)
televise
telltale(s) (n, adj)
tendency, tendencies (pl)
tenfold
terminus, termini (pl)
territorywide
test bed(s)
test case(s)
test-fire(s), test-fired, test-firing
test-fly, test-flies, test-flew, test-flown, test-flying
test-jam(s), test-jammed, test-jamming
test-launch(es), test-launched, test-launching
test range(s)
test site(s)
test stand(s)

C05757260

tete-a-tete(s)
textbook(s)
thanksgiving(s)
but
Thanksgiving Day
thank-you(s) (n)
theater(s)
theatergoing
theaterwide
then Premier
then-ruling (um)
then second deputy minister
then-troublesome (um)
thereafter
thereby
therefor (for it)
therefore (for that reason)
thereunder
thereupon
thesis, theses (pl)
thickheaded
thickskinned
think factory, think factories (pl)
think-piece(s)
think tank(s)
thinskinned
third-class (adj)
third-country (adj)
third-degree (adj)
thirdhand (adv, adj)
third-order (adj)
third-party (adj)
third-quarter (adj)
third-rate (adj)
Third World countries
thoroughbred(s) (n, adj)
thoroughfare(s)
thoroughgoing
thought-provoking (um)
threat-driven (um)
three-dimensional (um)
threefold
threesome(s)
threshold(s)
throughout
throughput(s)
through road(s)
throughway(s)
throw(s) away, threw away, thrown away, throwing away
throwaway(s) (n, um)
throw(s) back, threw back, throwing back
throwback(s) (n, um)
throw line(s)
throw rope(s)
throw weight(s) (n, um)
thumbnail(s)
thunderclap(s)
thunderhead(s)
thundershower(s)
thunderstorm(s)
Tiananmen Square
ticketholder(s)
ticket seller(s)
tidal wave(s)
tideland(s)
tidetable(s)
tidewater(s)
tide-worn (um)
tiebreaker(s)
tie(s) in, tied in, tying in
tie-in(s) (n, um)
tie(s) to, tied to, tying to
tie(s) up, tied up, tying up
tieup(s) (n, um)
tightfisted
tight-knit (um)
tightlipped
tightrope(s)
tightwad(s)
timberland(s)
time (suffix, often solid)

C05757260

daytime
halftime
peacetime
but
full-time
part-time

time being
time bomb(s)
timeclock(s)
time-consuming (um)
time-delay (adj)
time frame(s)
time-honored (um)
timekeeper(s)
timekilling
timelag(s)
timeline(s)
time-out(s) (n)
timepiece(s)
timesaving
time-sensitive (um)
timeserver(s)
time-share(s), time-shared, time-sharing (n, v)
timeslot(s)
timespan(s)
timetable(s)
time-urgent (um)
timewasting
timeworn
tip(s) off, tipped off, tipping off
tipoff(s) (n, um)
tiptoe(s), tiptoed, tiptoeing (n, v)
titleholder(s)
title page(s)
title-winning (um)
T-jetty, T-jetties (pl)
to-do(s) (n)
toehold(s)
toll bridge(s)
tollgate(s)
toll road(s)
Tomahawk-class missile(s)
tone-deaf (um)
tone(s) up, toned up, toning up
toneup(s) (n, um)
tongue-lash(es), tongue-lashed, tongue-lashing (v)
tongue lashing(s) (n)
tonguetied
tongue twister(s)
tongue-twisting (um)
ton-kilometer
toolbuilding
toolfitter(s)
toolkit(s)
toolshop(s)
toolsmith(s)
tool steel
toolwork(s)
tooth and nail
top brass
top drawer(s) (n)
top-drawer (adj)
top-end (adj)
topflight (adj)
topheavy
top-level (adj)
topline(s)
topliner(s)
topmost
topnotch
top-quality (adj)
top-secret (um)
topside (nautical)
topsy-turvy
torchlight(s)
tornado(es)
Tornados (aircraft name)
torpedo boat(s)
torpedo mine(s)
torpedo room(s)
torpedo tube(s)
torsion bar(s) (n, um)

C05757260

tortuous (adj, twisting, devious, highly complex)
torturous (adj, causing torture, cruelly painful)
tossup(s) (n, um)
total(s), totaled, totaling
touch and go
touch(es) down, touched down, touching down
touchdown(s) (n, um)
touch(es) up, touched up, touching up
touchup(s) (n, um)
tough-minded (um)
toward (no s)
to wit
townhall(s)
town meeting(s)
townspeople
traceable
track-and-field (um)
track-mobile (um)
track record(s)
tractor-trailer(s)
tradeable
tradecraft
trade(s) in, traded in, trading in
trade-in(s) (n, um)
trademark(s), trademarked, trademarking (n, v)
trade name(s)
trade(s) off, traded off, trading off
trade-off(s) (n, um)
trade school(s)
tradesperson, tradespersons or tradespeople (pl)
trade union(s)
trade unionism
trade unionist(s)
trade wind(s)
trafficking
trailblazing
trainborne
training camp(s)
training ship(s)
trainload(s)
trainmaster(s)
trainshed(s)
train station(s)
trainyard(s)
tramcar(s)
tramline(s)
tramrail(s)
tramway(s)
tranquilize(s), tranquilized, tranquilizing
tranquilizer(s)
tranquillity
trans (pref, usually one word)
transalpine
transatlantic
transisthmian
transonic
transpacific
transship(s), transshipped, transshipping
transshipment(s)
transuranic
but
trans-Canadian
trans-Siberian
transcendent
transfer(s), transferred, transferring (n, v)
transferable
transferal(s)
transit(s), transited, transiting (n, v)
transmit(s), transmitted, transmitting
transmittal(s)
transmittance(s)
transmitter(s)
transporter-erector-launcher(s) (n)
trapdoor(s)
travel(s), traveled, traveling (n, v)
traveler(s)
traveler's checks
traveltime(s)
travel-worn (um)
treatybound
treatybreaking
treaty-limited
treatymaking
tree line(s)
tree-lined (um)

C05757260

tree-ripe (um)
treetop(s)
tree trunk(s)
tri (cf, usually one word)
tricolor
tripartite
tristate
but
tri-iodide
tri-ply
tribesman, tribesmen (pl)
tribespeople
trigger-happy (um)
triple-edged (um)
triple play(s)
tripwire(s)
Trojan horse(s)
trolley(s)
trolley line(s)
troopship(s)
troop train(s)
troop training (n, um)
trouble-free (um)
troublemaking
troubleshooter(s)
troublesome
trouble spot(s)
truckborne
truckdriver(s)
truck farm(s)
truckline(s)
truckload(s)
truckstop(s)
truck tractor(s)
truck trailer(s)
true-blue (um)
trunkline(s)
trust-building (um)
trust-busting (um)
try out, tries out, tried out, trying out
tryout(s) (n, um)
T-shaped
T-shirt
T-square
Tu-16
tube-feed(s), tube-fed, tube-feeding
tug of war(s)
tune(s) up, tuned up, tuning up
tuneup(s) (n, um)
turbo (cf, usually one word)
but
turbo-ramjet
turn(s) about, turned about, turning about
turnabout(s) (n, um)
turn(s) around, turned around, turning around
turnaround(s) (n, um)
turn(s) back, turned back, turning back
turnback(s) (n, um)
turncoat(s)
turn(s) down, turned down, turning down
turndown(s) (n, um)
turn(s) in, turned in, turning in
turn-in(s) (n, um)
turnkey(s)
turn(s) off, turned off, turning off
turnoff(s) (n, um)
turn(s) out, turned out, turning out
turnout(s) (n, um)
turn(s) over, turned over, turning over
turnover(s) (n, um)
turnpike(s)
turnscrew(s)
turntable(s)
turret deck(s)
turret gun(s)
turret ship(s)
turtleback(s) (n, adj)
20th-century (adj)
twenty-first
twenty-one
twice-reviewed (um)
twin-engine (adj)
twin-engined (um)
twin-jet (adj)
twin-screw (adj)

C05757260

two(s)
two-faced (um)
twofold
two-piece (adj)
two-seater(s)
two-sided (um)
twosome(s)
two-thirds
two-way (adj)
two-wheeler(s)
typecast
typeface(s)
typescript(s)
typesetting
typewriting

U

ultra (pref, usually one word)
ultrahigh
ultraorthodox
ultrarightwing
ultrashortwave
ultrasonic
ultraviolet
but
ultra-ambitious
ultra-atomic
ultra-English
ultra-high-frequency (adj)
ultra-high-speed (adj)
ultra-high-voltage (adj)
ultra-large-scale (adj)

un (pref, usually one word)
unaware (adj)
unawares (adv)
uncalled-for (um)
unheard-of (um)
unMIRVed
unself-conscious
unsent-for (um)
unthought-of (um)
but
un-American
un-ionized

UN
UN Charter
UN-initiated (um)
UN Mission(s)
UN Permanent Representative(s)
UN Special Commission (UNSCOM)
UN Special Representative(s)

under (pref, usually one word)
under age (pred)
underage (um, too young)
under contract
undercover (um)
under cultivation (being tilled)
undercultivation (insufficient cultivation)
undercut(s), undercut, undercutting (n, v)
underdog(s)
undergo(es), underwent, undergone, undergoing
underground(s), undergrounded, undergrounding (n, adj, v)
under-ice (adj)
under oath
under obligation
under orders
underpriced
underrepresented (adj)
underresourced (adj)
underside(s)
under secretary, under secretaries (pl)
under-secretaryship(s)
under strength (pred)
understrength (um)
under suspicion
under-the-counter (um)
under water (pred)
underwater (um)
under way (pred)
underway (um)

uni (cf, usually one word)
unintelligible
uninterested (indifferent; see *disinterested*)
union-made (um)
union shop(s)

up
up-and-comer(s) (n)
up-and-coming (um)
upbeat
upcountry
update(s), updated, updating (n, v)
upend(s), upended, upending
up-front (um)
upgrade(s), upgraded, upgrading (n, v)
uphill

C05757260

upkeep
uplift(s), uplifted, uplifting (n, v)
up-link(s), up-linked, up-linking (n, v)
upload(s), uploaded, uploading (n, v)
uprange
upriver
upstairs
upstream
upswing(s)
uptick(s)
up time(s)
up-to-date
uptown
upturn(s)
upwind

uppercase (printing)
upper-caste (adj)
upper-class (adj)
upperclassman, upperclassmen (pl)
uppercrust (n, um)
upper hand
upper-house (adj)
upper-income (adj)
upper-middle-class (adj)
uppermost
URL(s) (uniform resource locator)
US $3 million
usable
user friendly
userid(s)
upside down
US-owned (um)
U-turn(s)

V

vacillate(s), vacillated, vacillating
value-added (um)
variable rate mortgage(s)
V-E Day
verbatim
vertebra(s)
vertebrae (pl, scientific)
very-high-frequency (adj)
very-low-frequency (adj)
vice admiral(s)
vice-admiralty
vice chair(s)
vice chairman, vice chairmen (pl)
vice chancellor(s)
vice consul(s)
vice-consulate(s)
vice-consulship(s)
vice-marshal(s)
vice minister(s)
vice-ministry, vice-ministries (pl)
vice-presidency, vice-presidencies (pl)
vice president(s)
vice-presidential
vice-president(s)-elect (general sense)
but
Vice President–elect
vice versa
videocassette(s)
videoconferencing
videotape(s), videotaped, videotaping (n, v)
video tape recording(s)
Vietnam war
viewgraph(s)
viewpoint(s)
vilify, vilifies, vilified, vilifying
virtuoso(s)
vis-a-vis
visible
voice-activated (um)
voice mail(s)
Voice of America
volt-ampere(s)
voltmeter(s)
volt-second(s)
vote-casting (um)
votegetter(s)
vote-getting (um)
VRAM (video RAM)

C05757260

VRML (virtual reality modeling language)

W

wage earner(s)
wage-earning (um)
wage scale(s)
wagonload(s)
wait-and-see (adj)
waiting list(s)
waiting period(s)
wake-homing
walkie-talkie(s)
walk(s) in, walked in, walking in
walk-in (n, um)
walk(s) on, walked on, walking on
walk-on(s) (n, um)
walk(s) out, walked out, walking out
walkout(s) (n, um)
walled-in (um)
walled-up (um)
wall-like
wallpaper(s), wallpapered, wallpapering (n, v)
war chest(s) (n)
war crimes (n)
war-crimes (adj)
warfighter(s)
warfighting (n)
war-fighting (um)
war game(s) (n)
war-game(s), war-gamed, war-gaming (adj, v)
wargaming (n)
warhead(s)
warhorse(s) (nonliteral)
warlike
warlord(s)
warmaking
warmonger(s)
warpath(s)
warplane(s)
warplan(s)
warship(s)
wartime(s)
war-torn
war-waging (um)
war-wearied (um)
war weariness
war-weary (um)
war-winning (um)
war zone(s)
ward (suffix, usually one word; no final s)
afterward
homeward
northward
wardheeler(s)
warehouse(s), warehoused, warehousing (n, v)
warmed-over (um)
warm(s) up, warmed up, warming up
warmup(s) (n, um)
washed-out
wash(es) out, washed out, washing out
washout(s) (n, um)
wash(es) up, washed up, washing up
washup(s) (n, um)
wastewater(s)
watchband(s)
watchdog(s)
watchlist(s)
watchman, watchmen (pl)
watchword(s)
water-bearing (um)
water body, water bodies (pl)
waterborne
watercolor(s), watercolored, watercoloring (n, v)
water-cool(s), water-cooled, water-cooling
water-cooled (um)
water-cut (from oil well)
watered-down (um)
waterfall(s)
water-filled (um)
waterflood(s) (of oil wells)

C05757260

waterflow(s)
waterfront(s)
waterhole(s)
water level(s)
waterline(s)
waterlogged
water main(s)
waterman, watermen (pl)
watermark(s) (as on stationery)
but
high water mark(s) (as in floods)
waterpower
waterproof(s), waterproofed, waterproofing (n, adj, v)
water sharing (n)
water-sharing (um)
watershed(s)
waterside(s)
waterski(s), waterskied, waterskiing (n, v)
water-soaked (um)
water-soluble (um)
water table(s)
watertight
water tower(s)
water treatment (adj)
waterway(s)
waterworks
watthour (Wh)
wave band(s)
waveform(s)
wave front(s)
waveguide(s)
wave height(s)
wavelength(s)
wave-swept (um)
way point(s)
way station(s)
weak-kneed (um)
weak-willed (um)
weaponmaking
weapons-grade
weapons of mass destruction (WMD)
weapons-of-mass-destruction (um)
weapons-related (um)
weapon system(s) (preferred), **weapons system(s)**
weatherbeaten
weather-hardened (um)
weather map(s)
weatherproof(s), weatherproofed, weatherproofing (adj, v)
weatherstrip(s), weatherstripped, weatherstripping (n, v)
web browser(s)
webcam(s)
webcast(s)
web index(es)
webmaster(s)
webpage(s)
web server(s)
website(s)
weekday(s)
weekend(s)
weekender(s)
weeklong (adj)
week-old (um)
well-being (n)
well-born (um)
well-bred (um)
well-coordinated (um)
well-done (um)
well-drilling (um)
well field(s)
wellhead(s)
wellhouse(s)
well-informed (um)
well-known (um)
well-looking (um)
well-off (um)
well-prepared (um)
well-read (um)
well-spoken (um)
wellspring(s)

C05757260

well-thought-of (um)
well-thought-out (um)
well-to-do
well-trained (um)
well-wisher(s)
well-worn (um)
westbound
west-central
west end(s)
Western-government-backed (um)
Western Hemisphere
westernmost
westmost
west-northwest
westward
wet(s), wet or wetted, wetting (n, v; of water; see *whet*)
wet, wetter, wettest (adj)
wetland(s)
wheatfield(s)
wheat grower(s) (n)
wheatland(s)
wheat-rich (um)
wheatstalk(s)
wheelbarrow(s)
wheelbase(s)
wheelbox(es)
wheelchair(s)
wheeler-dealer(s)
wheelpower
whereabouts
whereas
whereby
whereupon
wherewithal
whet(s), whetted, whetting (to stimulate; see *wet*)
whipcord(s)
whip hand(s)
whiplash(es)
whirlpool(s)
whistle-blower(s)
whistle-blowing
whistlestop(s)
white book(s) (diplomatic)
whitecap(s) (nonliteral)
white-collar (adj, nonliteral)
white count(s)
white flag(s)
white goods
white lie(s)
white paper(s) (diplomatic)
whitewash(es), whitewashed, whitewashing (n, v)
wholehearted
wholesale
wholesome
wholly owned subsidiary (subsidiaries [pl])
wide (suffix, usually one word)
armywide
nationwide
peninsulawide
but
Africa-wide
Army-wide
wide-angle (adj)
wide-area (adj)
wide-awake (um)
wide-band (adj)
wide-body, wide-bodies (n, adj)
wide gauge(s) (n)
wide-gauge (adj)
wide-open (um)
wide-ranging (um)
wide-scale (adj)
widespread
widthwise
Wi-Fi
wild card(s)
wildlife
willful
willpower
wind (cf, usually one word)
windblown
windborne
windbreak

C05757260

windburn(s)
windchill(s)
windfall(s)
windmill(s)
windpipe(s)
windpower
windproof(s), windproofed, windproofing (adj, v)
windshield(s)
windspeed(s)
windstorm(s)
windswept
windward
but
wind tunnel (n)
wind-tunnel (adj)

window-dress(es), window-dressed, window-dressing

window-dressing (n)

windowsill(s)

wind(s) up, wound up, winding up

windup(s) (n, um)

wine-making (um)

wing flap(s)

wingspan(s)

wingspread

wingtip(s)

winter(s), wintered, wintering (n, v)

winterkill(s)

winterproof(s), winterproofed, winterproofing (adj, v)

winter-sown (um)

wintertime(s)

winter wheat

wireline(s)

wirephoto(s)

wiretap(s), wiretapped, wiretapping (n, v)

wise (suffix, usually one word)
businesswise
clockwise

wisecrack(s)

wise guy(s)

wise man, wise men (pl)

wise-spoken (um)

wish list(s)

witch hunt(s)

withdraw(s), withdrew, withdrawn, withdrawing

withhold(s), withheld, withholding

withstand(s), withstood, withstanding

WMD (weapon[s] of mass destruction)

woodland(s)

woodpulp(s)

woodwork(s)

woodworking (n, adj)

woolgathering

wool-lined (um)

woolshearing

woolworking

wordbook(s)

wordbuilding

word combination(s)

wordcraft

word-for-word (adj, adv)

wordlist(s)

word-of-mouth (adj, adv)

wordplay(s)

word watcher(s)

word wrap, word wrapped, word wrapping

work (cf, usually one word)
workday(s)
workflow(s)
workforce(s)
workhorse(s)
workload(s)
workman, workmen (pl)
workmanlike
workmanship
workout(s)
workplace(s)
workplan(s)
worksaving
worksheet(s)
workshop(s)
worksite(s)
workspace(s)
workstation(s)
workteam(s)
worktime(s)
workup(s)
workweek(s)
workyard(s)
workyear(s)

C05757260

but
work hour(s)
work order(s)
work shift(s)

working-class (adj)
working day(s)
working-level (adj)
workingman, workingmen (pl)
working woman, working women (pl)
worldbeater(s)
world-class (adj)
World Court
world-record-breaking (um)
worldview(s)
World War II period (n)
worldwide
World Wide Web (WWW)
WORM (write-once, read-many)
wornout (um)
worrywart(s)
worship(s), worshiped, worshiping
worshiper(s)
worst case(s) (n, um)
worthwhile
would-be
wrack(s), wracked, wracking (wreck)
wrap(s) up, wrapped up, wrapping up
wrap-up(s) (n, um)
wreak(s), wreaked, wreaking (to cause)
write(s) down, wrote down, writing down
write-down(s) (n, um)
write(s) in, wrote in, writing in
write-in(s) (n, um)
write(s) off, wrote off, writing off
writeoff(s) (n, um)
write protected
writers guide(s)
write(s) up, wrote up, writing up
writeups (n, um)
wrongdoers
wrong-minded (um)
wrong-thinking (um)
wrought iron
WWW (World Wide Web)
Wye River Memorandum
but
Wye accord

X, Y, Z

X-ray(s)
X-shaped
Yak-40(s)
yearbook(s)
yearend
yearlong
year-old
year on year (adv)
year-on-year (adj)
year-round
years' (possessive case)
yellowcake (of uranium)
yellow fever
yes-man, yes-men (pl)
yesterday(s)
yet-determined (um)
yet-to-be
Y-joint(s)
young-looking (um)
youthlike
zero-gravity (adj)
zero(s)
zero-sum (adj)
zigzag(s), zigzagged, zigzagging (n, adj, v)

C05757260

9. WORD WATCHERS LIST

9.1. What's in This Chapter?

The Word Watchers List contains an alphabetized compilation of entries dealing with possibly troublesome words, word types, and word problems. It is intended to help writers and processors of the written word find quickly the answers to questions likely to arise most often in their work. Most of the entries provide answers on the spot. Others direct the user to other entries in this chapter (such references are highlighted in red) or to parts of earlier chapters referred to by section or footnote number.[42]

9.2. Who Are the Word Watchers?

This compilation is meant to provide guidance for writers of intelligence publications as well as writers of intelligence-related administrative papers. All are assumed already to possess the three essentials of intelligence analysis: knowledge, clarity of thought, and good judgment. No writing, however skilled, can conceal deficiencies in these requisites.

9.3. Some Helpful Precepts

Written English is the analysts' and administrators' main vehicle for conveying their studied evaluations to consumers. Mastery of the language adds force, precision, and grace to these presentations. Writers who want to compose English prose devoid of jargon and easy to comprehend should bear in mind these concepts:

- Keep the language crisp and pungent; prefer the forthright to the pompous and ornate.
- Do not stray from the subject; omit the extraneous, no matter how brilliant it may seem or even be.
- Favor the active voice and shun streams of polysyllables and prepositional phrases.
- Keep sentences and paragraphs short, and vary the structure of both.
- Be frugal in the use of adjectives and adverbs; let nouns and verbs show their own power.
- Make sure that subject and verb agree in number; do not be tricked by intervening words.
- Be just as sure that every pronoun has a clearly identifiable antecedent and that the two agree in number and gender.
- Be aware of your reading audience; reserve technical language for technical readers.
- Be objective; write as a reporter or analyst or administrator unless you are entitled to write as a policymaker.

[42]Note that a section number always begins with the number of the chapter in which the section appears—section 7.3, for example, is the 3rd section of chapter 7. Footnotes, however, are numbered in one sequence throughout—from footnote 1 in chapter 1 to footnote 42 in chapter 9.

C05757260

a, an before h	Use *an* when the next word begins with a silent *h* (*an herb*); use *a* when the *h* is pronounced (*a historic occasion*).
aboard, on board	*Aboard* can be an adjective (*the crew is aboard*), an adverb (*they went aboard*), or a preposition (*they are aboard the ship*). The prepositional phrase *on board* can be used adjectively (*they are on board*) or adverbially (*they went on board*) but preferably not prepositionally—avoid *they went on board the ship*.
about, approximately, around	*Around* is acceptable in approximations of time: *around three o'clock*. In other contexts it is a questionable synonym for *about* or *approximately*. Given a choice between those two words, choose *about* most of the time; it saves space and sounds less stuffy. Do not use *about* (or *approximately, around,* or *estimated)* when a figure is stated precisely. Do not say *during the attack,* ***about*** *3,041 troops were killed* if you are sure of the number. If you are not sure, replace the 3,041 figure with *about* (or *an estimated*) *3,000*.
absolutes	Some adjectives convey an absolute: it is the whole thing or nothing. They do accept modifiers that take away their absoluteness—*almost*, for example—but they do not accept limiting modifiers such as *somewhat, totally, more*, and *less*. The Preamble to the US Constitution is out of bounds grammatically when it speaks of *a more perfect Union*, and, as the common saying puts it, a woman cannot be *somewhat pregnant*. Other words in this category are *eternal, fatal, incessant, maximum, minimum, ultimate, unique*, and *universal*. *Absolute maximum* is overkill: *maximum* says it all.
accelerate	See escalate, accelerate, intensify.
acquiesce, agree	*Acquiesce* takes the preposition *in*, not *to* (*acquiesce* ***in*** *the decision*); *to* is used with *agree* (agree ***to*** the plan).
acronyms	Explain them as you would any other abbreviation. But be aware that acronyms do not always seem to follow conventions about capitalization or other matters (*Aramco, NATO, agitprop*). Usually, when an acronym is made up solely from the first letter of the major words in the expanded form, render the acronym in all capitals (*North Atlantic Treaty Organization*, or *NATO*). We write *comsat* when speaking generally of a communications satellite but *Comsat* in reference to the corporation. The term *Landsat* should refer only to the US Earth resources satellite, but *landsat* might be used in a less specific reference.
active voice	In formal writing, prefer the active voice. *Lifeguards clear beaches when forecasters predict storms.* Only if your focus is beach clearing rather than lifeguards would the passive be preferred. *The beaches are cleared when storms are forecast.*
activity	See condition, situation, activity.
additionally	Prefer *in addition* if you must use something.
adverbs	When modifying a verb, adverbs usually go between the auxiliary (or auxiliaries) and the main verb. (*The Prime Minister has finally announced her decision.*)

C05757260

adverse, averse	sound alike, and both express opposition, but *adverse* applies to something working against a person or program (*adverse weather conditions*), and *averse* applies to a person who is against something. (*He is averse to traveling by plane.*)
affect, effect	*Affect* as a verb means to influence, to produce an effect upon. (*The blow on the head affected John's vision.*) *Effect*, as a verb, means to bring about. (*The assailant effected a change in John's vision by striking him on the head.*) *Effect*, as a noun, means result. (*The effect of the blow on John's head was blurred vision.*)
agree	*with* a person, *to* a proposal, *on* a plan. (See acquiesce, agree.)
AIDS	See HIV/AIDS.
all ready, already	are not interchangeable. The first means everybody is set to do something; the second means by or before a specified or implied time. (*Fortunately, the employees are all ready for the 3:00 meeting because it is already 2:45.*)
all right	never *alright*.
all together	See altogether, all together.
already	See all ready, already.
almost	See most, mostly, almost.
along with	See together with.
also	When used as a direct modifier of a negative verb—*he also does not favor import quotas*—*also* sounds awkward and unidiomatic. Do one of three things: move the word to modify the whole sentence or clause (*also, he does not favor import quotas*), replace it (*he does not favor import quotas either* or *moreover, he does not favor import quotas*), or make the verb positive (*he also opposes import quotas*). Be sure, moreover, that *also* is intended to modify the verb directly and not some other word in the sentence; *also*, like *even* and *only*, is a notorious "floating modifier." (See fill-ins.)
alternate, alternative	*Alternate* means rotating, following by turns; *alternative* pertains to a choice between possibilities. *Alternate*, as an adjective, does overlap *alternative* by conveying the idea of a second choice.
altogether, all together	*Altogether* means all told or completely. *All together* means in unison.
always	means on every occasion or forever. Be sure that you do not use *always* when you mean habitually or usually. *The President always leaves his office at noon on Saturday.* Are there no exceptions? (See absolutes.)
ambiguous, ambivalent	Use *ambiguous* if you wish to point out inconclusiveness or lack of clarity in a situation. *Ambivalent* applies to mixed feelings, the simultaneous operation in the mind of two different and usually conflicting desires.
American	is certainly acceptable as a noun meaning a US citizen, but for the adjective describing our country the preferred term is US.
among	See between, among.
amused	See bemused.

C05757260

anathema	means both a curse or denunciation and the thing or person cursed or denounced. In the former case the article and plural are used. *The anathemas of the losers, to pronounce an anathema.* In the latter they usually are not. *He was anathema to his enemies, they were anathema to their enemies.*
and, but, however	may be used at the beginning of a sentence when emphasis is desired, but use this construction sparingly; overuse blunts its effect and leans toward the informal.
and/or	Do not use in DI writing. See section 5.17c.
and so forth	See etc., and so forth.
anticipate, expect	When you *anticipate* an event, you generally make some preparation for it; when you *expect* an event, you simply await developments before acting. *They anticipated a hostile crowd, so they mobilized the National Guard.* Had they *expected* a hostile crowd, they would not have been surprised, but the National Guard would not have been there.
anxious, eager	Both connote a strong interest or desire; use *eager* unless you want to add a dimension of worry or fear.
any	as a pronoun, can take either a singular or a plural verb. *Any* [any one] *of her options is suitable. Are any* [some] *of them practicable?*
apparently	See qualifiers.
appraise, apprise	*Appraise* means to set a value on; *apprise*, to inform. *Apprise*, however, is considered a pretentious word and should be avoided.
approximately	See about, approximately, around.
apt	See likely.
around	See about, approximately, around.
as	in positive comparisons, is followed by another *as*. *She is as clever as her adversary.* Watch out for mismatches. *As good as or better than*, not *as good or better than*. In negative comparisons, *so* may be substituted for the first *as*. *She is not so clever as her adversary.* (See like, as and compare, contrast.)
as far as	Confusion arises with the construction *as far as . . . is concerned.* This is an indissoluble unit; *as far as* by itself is incorrect. *As far as football teams are concerned, I like the Redskins* is correct. *As far as football teams, I like the Redskins* is not.
as noted	See fill-ins.
assure, ensure, insure	*Assure* applies to persons (*to assure a leader of one's loyalty*). It alone has the sense of setting a person's mind at rest. Use *ensure* to mean make certain (*to ensure a nation's security*). *Insure* means to cover with insurance.
as well as	See together with.
as yet	Most of the time *as* can be dropped.
asylee	a permissible word, even though not in many dictionaries, meaning a person seeking asylum or one given asylum.
at the same time	See fill-ins.
augur, auger	*Augur* is a verb meaning to predict from signs or omens. An *auger* is a tool for boring holes.

C05757260

averse	See adverse, averse.
awhile	is not preceded by *for*. *He stayed awhile*; but *he stayed for a while.*
based on, due to, owing to	These word sets are almost always awkward and often introduce dangling phrases: *Due to (or owing to) illness, the meeting was postponed.* You can usually produce something smoother by reworking the sentence: *We had to postpone the meeting because almost everyone was sick.*
basically	See fill-ins.
because	See reason, because.
bedouin	Capitalize *Bedouin* when referring to an ethnic population, as in Jordan (see *The World Factbook*). When referring to a nomadic lifestyle, lowercase is suitable (*the bedouin belief in afreets [powerful evil demons]*).
beef up	Avoid this overused term. (See metaphors.)
before	See prior to, before.
bemused	means confused or bewildered and is not synonymous with *amused.*
between, among	*Between* expresses the relationship of two persons or things (*between the devil and the deep blue sea*); *among*, the relationship of three or more (*The spoils of victory were divided among the four winning parties*). Use *between*, however, if you are considering more than two things in pairs as well as in a group. (*We see major differences between the policies of Country A, Country B, and Country C.*)
biannual, biennial, semiannual	Both *biannual* and *semiannual* mean twice a year; *biennial* means every two years. To avoid confusion between *biannual* and *biennial*, avoid the former and use *semiannual*. Even better, say *twice a year* and *every two years.*
bits, bytes	are considered units of measure and are quantified in figures, not spelled-out words (*a 7-bit byte, 5 bytes of 7 bits each*; but *five 7-bit bytes*—see section 2.23a).
blatant, flagrant	Both words describe glaringly antisocial behavior. *Blatant* denotes the obvious, the offensive, the obtrusive: *a blatant lie*. *Flagrant* carries a stronger overtone of malice; it denotes deliberate, obtrusive wrongdoing. One who willfully violates a pledge commits a *flagrant* act. Both words convey subjectivism in many contexts. (See subjective words.)
bloc	is usually not capitalized, except for references to the former Soviet Bloc.
blog	A *blog* is a type of website, usually maintained in an online journal format, containing commentary, descriptions of events, or other material such as graphics or video. As a verb, *blog* means to maintain or add content to a blog. *Blog* is short for *weblog*, but the longer term is rarely used.
boat, ship	*Boats*, nautically speaking, are usually small craft that can be carried on a *ship*, a larger vessel suitable for crossing the high seas. The exception is a *submarine*, which is most often referred to as a boat. All take the pronoun *it*, not *she*.
both	is redundant in expressions such as *they both agree* or *they both share.* With three, however, *both* might be used: *Both London and Paris agree with Washington that the arrangement is sound.*
both . . . and	Be sure that the material that follows is in balance. *He was deaf to both argument and entreaty*, not *he was both deaf to argument and entreaty.* (See parallelism.)

C05757260

boycott, embargo	A *boycott* is a refusal, usually by an organized group, to buy or use a particular product or service. It is not synonymous with *embargo*, which is a legal restriction on trade.
breach, breech	As a noun, *breach* is a violation, a gap, or a rift in a solid structure. Do not confuse it with *breech*, which is acceptable only in reference to ordnance and to human anatomy.
burgeoning	Originally descriptive of something newly emerging, *burgeoning* has become accepted for something growing and expanding rapidly.
burnish	means to make shiny or lustrous; it is not correct to say someone *burnished his credentials.*
but	See and, but, however.
bytes	See bits, bytes.
cadre	*Cadre* was originally a military term for a group around which a larger unit is formed but now, under the influence of communist terminology, may denote any core group, as well as a member of such a group. Use in a nonmilitary context seems to be dying out as the Cold War era fades further into history. Use an English term if possible. Always add an *s* when the word is plural. (See cohort.)
calculate	See feel.
capital cities	in intelligence writing are generally legitimate stand-ins for the names of national governments. *Moscow's position is clear* is fine, but be sure not to use capital cities when you are referring to the country as a whole. Do not write, for instance, *Moscow is reinforcing its borders.*
casualties	include persons injured, captured, or missing in action as well as those killed in battle. In formulating casualty statistics, be sure to write "killed *or* wounded," not "killed *and* wounded." (See injuries, casualties.)
celebrity copycatting	can lead one up the garden path because those emulated are not always pure of speech. A venerable newscaster persists in mispronouncing *February* (without the first *r* sound) and has misled a whole generation. Another Pied Piper of TV is given to saying "one of those who *is*"—joining many others who are deceived by the *one* and forget that the plural *who* is the subject of the verb (see one). The classic copycat phrase, *at this point in time*, grew out of the Watergate hearings and now is so firmly entrenched that we may never again get people to say *at this time, at present*, or simply *now* (see presently).
center	as a verb is used with *on, upon, in*, or *at*, but not *around. The dispute* ***centers on*** *the fairness of the election.* The dispute can, however, ***revolve around*** *the fairness of the election.*
charisma	is a Greek word denoting divine grace or endowment. Its use should be limited to those rare and gifted persons who attract exceptional devotion from great numbers of followers.

C05757260

China, Taiwan	The full name of the People's Republic of China is usually shortened to *China*. *PRC* may be used. Hong Kong has been a Special Administrative Region of China since July 1997. *Chinese* is the preferred adjective and refers only to the mainland. For what was once called Nationalist China or the Republic of China, use only *Taiwan*, both as noun and as adjective. For variation, *Taipei* may be used in either noun or adjective form (for example, *the officials in Taipei*, or *the Taipei authorities*), but avoid *Taiwanese* as an adjective referring to the island's administration or its officials (and do not use the term *Taiwanese government*). The terms *Communist China* (and *Chinese Communist*) and *Nationalist China* (and *Chinese Nationalist*) or *Republic of China* should be used only in historical contexts.
citizenry	See pretentious words.
clearly	See qualifiers.
climactic, climatic	*Climactic* refers to climax or high point, *climatic* to weather. *The **climactic** moment of the President's trip came at Bonn. The **climatic** changes in the area are being studied.*
clout	is best confined to fights and baseball or golf. It can be used occasionally in the metaphorical sense of influence or power, but it always sounds colloquial. (See colloquialisms.)
cohort	always refers to a group of people. Emphasis is on the trait or traits common to all members. *Cohort* should not be used as a synonym for *comrade* or *comrades*. Mr. X may belong to a cohort, but neither he nor his buddies are cohorts. (Compare cadre.)
colloquialisms	are words or phrases suitable for conversation or other informal situations but not for intelligence writing.
colored	See footnote 6.
combined, joint	When referring to military exercises or operations, a *combined* exercise involves the forces of more than one country, a *joint* exercise two or more services of the same country.
communication(s)	In military/security terminology *communication* usually adds s as an adjective: *communications equipment, communications intelligence*. As a noun it sometimes drops the s: *sea lines of communication* (sometimes abbreviated *SLOCs* and pronounced as an acronym).
communism	See section 1.13 and footnote 3.
comparatively	See relatively, comparatively.
compare, contrast	*Compare to* points out likenesses; *compare with* points out both likenesses and differences; *contrast with* points out only differences. *He **compared** his cabinet **with** Kennedy's.* (He pointed out similarities and differences.) *He **compared** his cabinet **to** Kennedy's.* (He showed how much alike they were—and by implication, how praiseworthy his cabinet was.) *He **contrasted** his cabinet **with** Kennedy's.* (He emphasized the differences.) When using *compared* as a participle, preceding it with *as* will ensure better comprehension and in some cases avoid the appearance of a dangling participle. *This year's output, **as compared with** last year's, is more export oriented.*

C05757260

compel, impel, propel	*Compel* means to force, drive, or constrain; *impel* to urge to action through moral pressure; *propel* to impart motion to.
comprise, compose, include	*Comprise* views a collection as a whole; it means to contain or to consist of. Use *comprise* when referring to all components; use *include* when mentioning only some of them. *The statement comprises all he has to say on the topic. The statement includes a cogent summary of his thoughts.* *Compose* emphasizes the elements of a collection; it means to constitute or to make up. Unless accompanied by a modifier, it, too, refers to all components. *The parts compose the whole. The committee is composed of Sue, Jim, and Andy, among others.* The real problem with *compose/comprise* comes with the passive form. *Compose* in the sense of contain generally requires a passive construction: *is composed of. Comprise* lacks a meaningful passive form, but (partly because *comprise* sounds fancier than *compose*) we try to fill the gap with a parallelism: *is comprised of.* Never use this phrase. Something can be *composed of* a, b, and c. It can *include* a, b, and c. It can *comprise* (be made up of, be composed of) a, b, and c. It can never be *comprised of* a, b, and c.
concern	takes different prepositions for different senses. *He is concerned **with** computers* (he is so occupied or employed). *He is concerned **about** computers* (he is worried about them). When used in the sense of worry, concern sounds limp: *The government of Country A is concerned about US policy.* Focus whenever possible on what the government *calculates*, on what it might do.
concerted	meaning combined, requires a plural subject or object to make sense. Only *we* or *they* (never *I, he, she,* or *it*) can make a "concerted effort."
conclave	is a secret meeting, not just any gathering.
concrete steps	In nonliteral use this phrase raises awkward connotations of literalness. Say *concrete measures* or *specific steps.*
condition, situation, activity	often intrude into sentences for no reason. Good writers will say *the famine is worsening*, not *the famine conditions are worsening. The deteriorating economy* reads better than *the deteriorating economic situation.* Likewise, *the Russian Navy continued its exercises*, not *its exercise activities.*
consensus	is an opinion held collectively, not simply by a majority. Note the spelling: one *c*, three *s*'s.
consider, regard	*Regard*, in the sense of coming to a belief after careful deliberation, is usually followed by *as*; *consider*, in the same sense, is not. *He considered the vote a defeat. He regarded the vote as a defeat.*
consul	See council, counsel, consul.
continual, continuous, continuing, continued	*Continual* applies to something that occurs intermittently or is repeated at intervals, *continuous* to something that is uninterrupted in time or space. *Continuing* can be used in either sense. *Continuing* and *continued* are most often seen in government prose as pallid filler words. When tempted to use either, ask yourself whether there is a more effective word or whether you can do without the adjective. *His continuing efforts . . .* (*persistent efforts? fruitless efforts?* Do you need any adjective at all?)
contractions	are not acceptable in formal writing.
contradistinction	See pretentious words.
contrast	See compare, contrast.

C05757260

convince, persuade	are not interchangeable. A person is *convinced of* a need after he has been *persuaded to* recognize the need. *They convinced him of the importance of his participation and persuaded him to join.* If *convince* is followed by *to*, it usually is incorrect.
could, may, might	In the DI these words are used more or less interchangeably in a predictive mode: *Country A could (may, might) invade Country B.* Strictly speaking, however, they are not predictive at all. They are conditionals, and conditionals carry little analytic weight without the anchor of a limiting condition: *Country A **may** invade country B **if** Country B's leader leaves the scene.* Moreover, the three words are not synonymous. *Could* means *would be able to* and should be confined to statements dealing with capability. *Country A **could** invade Country B **if** it achieved air superiority.* Without a limiting condition, *could* carries the connotation that the capability exists but will not be used. *Country A could invade Country B (but we do not think it will).* Both *may* and *might* deal with possibility. For many, *might* carries an implication of greater uncertainty on the part of the writer. Again, the construction provides little enlightenment unless it offers further analysis. *Country A **may** invade Country B **if** President X gets the support of Country C. Country A **might** invade Country B **if** President X can persuade the legislature to back him.* Note the logical constraints imposed by *may* and *might* when they are properly yoked to a limiting condition. The last two examples not only warn about a possible invasion if certain conditions are satisfied; they also tell the reader by implication that the invasion *will not* occur *unless* the conditions are satisfied. If that is not what we want to say, the sentence needs reworking.
council, counsel, consul	*Council* is a noun that refers to a deliberative assembly, its work, or its membership. *Counsel* may be either a noun or a verb; it applies to advice and the person proffering that advice. *Consul* is the title of an officer in the foreign service.
countries, nations	Even La Belle France and Mother Russia are neuter and, like boats, take neuter pronouns (*it, they*). For information on country names and nationality designators, consult *The World Factbook.* (See footnote 1.)
credence, credibility, credulity	*Credence* means belief or mental acceptance. *Credibility* is the quality of being believable; something is *credible* when it is worthy of belief and judged plausible. One receives information that lends *credibility* to a rumor; one gives *credence* to the rumor upon being convinced that the information is valid. One who gives credence too easily is likely to stray over into *credulity*, which is next to gullibility.
crisis	In international affairs, a *crisis* is a situation involving significant actual or potential conflict. Similarly, in a country's domestic politics, reserve the word for major turning points. *Crisis* should not be used to describe lesser disruptions.
criteria	See data, media, criteria, phenomena.
culminate	takes the preposition *in* and is used intransitively. *The concert **culminated in** a sing-along,* not *a sing-along culminated the concert.*
cyberspace	the electronic medium of computer networks in which online communication occurs.

C05757260

dangling participles	See participles.
data, media, criteria, phenomena	are plural and therefore require plural verbs. The singulars are *datum*, *medium*, and (because they come from Greek rather than Latin) *criterion* and *phenomenon*. *Datum* and *medium* rarely have a place in DI writing, but we do use *criterion* and *phenomenon*. One never satisfies a criteria or observes a phenomena. (Note: *Gregg* points to a few instances when *data* and *media* might appropriately take a singular verb in formal writing; see section 1018. In the DI, you still are safer sticking with a plural verb.) The majority of *-um* nouns, of course, appear most often in the singular form. When pluralizing them, the DI generally uses English rather than Latin endings—for example, *forum(s)*, *curriculum(s)*. See also *Gregg*, section 614, for lists of the preferred pluralizations of foreign words.
dates as modifiers	A date should be used adjectivally only if you are distinguishing one event from another. Thus, the *1973 Middle East war* differentiates that conflict from others in other years. In contrast, *the 1901 assassination of President McKinley* and *the 1991 Iraqi invasion of Kuwait* need to be recast because they refer to unique events. Ending the phrases with *in 1901* and *in 1991*, respectively, would be a quick solution, but more creative choices may be available.
decimate	originally meant to select by lot, and then to kill, one out of every 10 in a group of enemies. Now it is used (and overused) to encompass heavy losses of many kinds. Use it only when referring to people, most often military people, and only when actual deaths are involved. Troops and units can be decimated. By extension, a disease can decimate a population. But buildings, tanks, and crops are damaged or destroyed, not decimated; and government economizing does not, one hopes, decimate the relief rolls.
definitely	See very, definitely.
defuse, diffuse	*Defuse* means to remove a fuse (or *fuze*—see the spelling and compounding list in chapter 8) from a weapon or, nonliterally, to deintensify, as in to *defuse a crisis*. *Diffuse* means to spread around, to scatter.
depart, leave	*Depart* requires a preposition; *leave* does not. *She will **depart from** Dulles today and will **leave** London on Tuesday.*
deploy	applies to military movement—in its narrowest definition, to military movement in preparation for battle. Avoid using it in the service of nonmilitary activity.
deprecate, depreciate	*Deprecate* means to express disapproval of something. Besides its application to prices and values, *depreciate* means to belittle something. If you *depreciate* someone's public-speaking skills, you are saying they do not amount to much; if you *deprecate* a speech, you are criticizing it.
developing countries	See less developed countries.
die	is something we all do, even writers who relegate world leaders to a sort of Immortality Club with phrasing like *the President has taken steps to ensure a peaceful transition if he should die.* Reality can be recognized by inserting *in office* or *before the end of his term*, or even by saying simply *when he dies.*
Dietmen	Avoid this term for members of the Japanese legislature; rather, use *Diet members* or *members of the Diet*.

C05757260

different from	is correct; *different than* is not. *Her opinion is different from his.* Better yet, *differs from.*
diffuse	See defuse, diffuse.
dilemma	involves a choice between two equally unsatisfactory courses of action. It is not the proper word to use when you mean simply a predicament or a troublesome decision. *The general had a dilemma: he had to decide whether to surrender or to face almost certain defeat on the battlefield.*
diplomatic corps	comprises all foreign diplomats assigned to a particular city; it is not synonymous with a country's diplomatic (or foreign) service. *Jones, a member of the British Foreign Service since 1983, is currently dean of the diplomatic corps in Ouagadougou.*
disburse, disperse	*Disburse* refers to the release of funds. *The payroll office disbursed the funds on Friday. Disperse* means to scatter. *The air force dispersed all its aircraft on Friday.*
disclose	See reveal, expose, disclose, divulge.
discreet, discrete	*Discreet* means cautious, prudent. *Discrete* means separate, distinct.
disinformation, misinformation	*Disinformation* refers to the deliberate planting of false reports. *Misinformation* equates in meaning but does not carry the same devious connotation.
disinterested, uninterested	*Disinterested* means impartial, not swayed by self-interest. *He attended the conference as a disinterested observer. Uninterested* connotes indifference. *She was uninterested in the film on management techniques.*
disperse	See disburse, disperse.
divulge	See reveal, expose, disclose, divulge.
domestic, indigenous	These words are synonymous in some senses but not all. Modifying *production*, for example, both define it as homegrown, or related to the country concerned. Modifying *animal*, on the other hand, the words diverge in meaning, *domestic* meaning domesticated or tamed, *indigenous* connoting native to or naturally occurring in the country or region concerned. In a phrase like *domestic political opponents* domestic is unnecessary because political opponents are always domestic unless otherwise stipulated; you may not need *political* either.
downbeat	See upbeat, downbeat.
due to	See based on, due to, owing to.
during	See more than, fewer than, over, under, during, while.
each	As a subject, *each* takes a singular verb and singular related pronouns. *Each has his own duties.* If, however, *each* follows a plural subject, the verb is plural. *The President and the Vice President each have an interest in the outcome.*
eager	See anxious, eager.
East Asia	Prefer to Far East.
East-West	*East-West* relations refers to those between the United States and its allies on one side (the West) and the Soviet Union and its allies on the other (the East) between World War II and the breakup of the Soviet Union in 1991.
economic growth	DI publications do not use the term *negative rate of economic growth.* Say instead that gross domestic product (or gross national product) is declining.

C05757260

effect	See affect, effect.
effectuate	See pretentious words.
either	as a subject, takes a singular verb and pronoun. For *either . . . or* constructions, see neither . . . nor.
election	Singular in most cases: usually there is only one election at a time (*national election, general election, presidential election*). But *presidential and legislative elections, municipal elections in several parts of the country.*
e-mail	a way to transmit messages electronically, or a message or messages so transmitted.
e-ticket	a paperless electronic document used for ticketing passengers, usually on an airline.
e-trade	electronic stock trading.
embargo	See boycott, embargo.
emigrate, immigrate, migrate	*Emigrate* is to leave a place permanently and is usually followed by *from*. *Immigrate* is to come to a place permanently and is usually followed by *to*. *Migrate* embraces both. *The doctor **migrated** in the 1950s. He **emigrated from** Sweden. He **immigrated** to Italy.* When a sentence includes both the place of departure and the place of arrival, *immigrate* is usually omitted. *He **emigrated from** Sweden **to** Italy.*
enormity, enormousness	*Enormity* means great wickedness. *The enormity of his attempts to conceal the facts led to his ouster. Enormousness*, the noun form of *enormous*, means great size.
ensure	See assure, ensure, insure.
enthuse	should not be used. (See colloquialisms.)
enunciate	See pretentious words.
equal, equivalent	*Equal* emphasizes precise quantitative likeness. *The three countries have equal numbers of submarines. Equivalent* applies to two or more things that have a qualitative similarity. *The military capabilities of the three countries are roughly equivalent.*
equally, as	Do not use these two words together in the same sentence (*equally as*) when you are making comparisons. Drop *equally* when you are comparing two persons or groups or two things. *He is as ineffective as his predecessor* (not *equally as ineffective*). Drop *as* when you name only one person or group or one thing in the sentence. *They are equally ineffective.*
equivalent	See equal, equivalent.
escalate, accelerate, intensify	*Escalate* means to increase by successive stages. A confrontation can *escalate* from border skirmishes to raids to invasion to all-out war; pensions can *escalate* with annual cost-of-living increases. Do not use *escalate* when you mean simply accelerate or intensify. *His political problems are escalating* is poor usage.
essentially	See fill-ins.
estimated	See about, approximately, around.
etc., and so forth	Rarely appropriate in DI writing. Enumerating the additional instances is usually more helpful.
eternal	See absolutes.

C05757260

even	a notorious floating modifier when used as an adverb. If it ends up in the wrong place it can distort meaning, and proper placement in a sentence requires care. *Even the Secretary was not disturbed by the threats* (and, if anybody would be, it would be he). *The Secretary was not even disturbed by the threats* (in fact, he was more or less unaffected). *The Secretary was not disturbed even by the threats* (much less by other things).
eventuate	See pretentious words.
evidence	is not a synonym for information or reporting. For the most part, avoid the word and get on with the analysis. Such phrases as *available evidence indicates* are essentially meaningless.
evidently	See qualifiers.
evince	See pretentious words.
exacerbate	Avoid this word; try *weaken*, *worsen*, *heighten*, *intensify*, *widen*, or *deepen* instead. (See pretentious words.)
exile	Except for diplomatic exile, a person is exiled *from* a country, not *to* a country. (See asylee.)
expect	See anticipate, expect.
expose	See reveal, expose, disclose, divulge.
extra words	See verbal overkill.
fake analysis	Phrases like the following betray sloppy thinking and detract from any serious presentation: anything can happen it is not possible to predict further developments are to be expected it is too early to tell it remains to be seen only the future will tell
Far East	See East Asia.
farther, further	*Farther* refers to physical or literal distance; *further* conveys the notion of additional degree, time, or quantity. A person hits a ball *farther*; he pursues a subject *further*.
fatal	See absolutes.
fear	Use only to describe a strong emotion, not a vague concern, an uneasy feeling, or an ill-defined skepticism.
feel	carries tricky emotional overtones. If a piece of analysis says the leaders of another country *feel* a certain way, the policymaking reader may conclude that the writer is identifying with those leaders—and perhaps criticizing the policymaker. You are on safer ground with *calculate* or *estimate*, whose relationship to the policymaker's operational world is unambiguous.
fewer, less	*Fewer* applies to numbers or units considered individually, *less* to quantities taken collectively. *Fewer dollars, less money; fewer months, less time; fewer miles, less distance.*
fewer than	See more than, fewer than, over, under, during, while.

C05757260

fill-ins	Reserve words and phrases like the following for those few occasions when they are really needed: *also, as noted, at the same time, basically, in connection with, indeed, in this context, of course, on the other hand, essentially, significantly, with reference to.* (See verbal overkill and fake analysis.)
finalize	See *-ize* words.
fiscal, monetary	*Fiscal* applies to a budget, *monetary* to currency.
fiscal year	See section 2.20d and footnote 18.
flagrant	See blatant, flagrant.
flammable, inflammable	*Flammable* is the preferred word when you are describing a combustible substance. However, a situation or a temperament is *inflammable*, not *flammable*.
flaunt, flout	*Flaunt* means to display ostentatiously; *flout* means to disobey openly, to treat the rules with contempt. *The starlet flaunted her physical assets in hopes of getting a good role. George flouted community association rules when he built a glass house.*
flounder, founder	As a verb, *flounder* means to stumble about clumsily; *founder* means to go lame (as with horses), to sink (as with boats), to collapse, or to fail utterly.
flout	See flaunt, flout.
forceful, forcible	*Forceful* means vigorous, strong, effective. If you want to connote the exertion of force, use *forcible*.
forego, forgo	*Forego* is to go before in time or place. Instead of using it we would usually write *go before* or *precede*. If you are doing without something, *forgo* the *e*.
foreword, forward	*Foreword* is the name for something written, usually by someone other than the author, to appear at the beginning of an article or book—whose author ordinarily writes the *preface*. Do not confuse with *forward*, which means near, at, or moving toward the front.
forgo	See forego, forgo.
former	See latter, former.
forthcoming	See upcoming, forthcoming, coming.
fortuitous, fortunate	*Fortuitous* describes something that happens by chance or accident. Do not confuse with *fortunate*. A *fortuitous* event can be either fortunate or unfortunate.
fortunately	See subjective words.
forward	See foreword, forward.
founder	See flounder, founder.
fractions	*One-half, one-third*, and the like are used when the fractions are precise. When precision is lacking, use *a half, a third*, and so forth.
Free World	is at best an imprecise designation. Use only in quoted matter.
fulsome	means offensive or loathsome, not complete or full.
further	See farther, further.

C05757260

gender	The English language is steadily acquiring new terms to counter the predominance of masculine forms: *anchor, newscaster, flight attendant, business person, layperson, chairperson, chair, mail carrier, Diet member, member of Congress, firefighter, police officer.* No completely satisfactory substitute yet exists for the pronouns *he, she, his, her,* and *him.* The best solution is to use the plural: *All representatives* (instead of *each representative*) *must cast their ballots* (rather than *his or her ballot*). If this is impractical, stick with *one* or *he or she* until someone comes up with a better idea.
gibe, jibe	A *gibe* is a taunt or sneer. *Jibe* is the act of shifting sails. Informally, to *jibe with* means to agree.
hackneyed phrases	Phrases like the following have been overused to the point of becoming meaningless cliches. Note the number of tired metaphors, and of equally tired adjectives and adverbs, in this list. a likely scenario assume the mantle of office bottom line broad outlines of the case considered judgment dire straits far-reaching implications geared up for action generates further disagreement hammer out a compromise heightened tensions hit the campaign trail keep their options open net effect of the decision nonstarters potential chokepoint refurbish his tarnished image triggered new developments viable alternatives widely held perception
hanged, hung	*Hanged* is the past tense of *hang* when referring to an execution; *hung* is the proper past tense in all other meanings.
hardly	has the force of a negative (*They had hardly any* [not no] *response.*); be careful to avoid an inadvertent double negative (*does not hardly*).
he/him/his	See gender.
historic, historical	*Historic* means famous in history. (*Gettysburg was the scene of a historic battle.*) *Historical* refers to general events of the past. (*She presented a historical review of the Middle East.*)
HIV/AIDS	Use *HIV/AIDS* when discussing the disease in terms of its social, economic, and political impacts. Use *HIV* by itself when discussing the human immunodeficiency virus or HIV prevalence rates. Use *AIDS* by itself when discussing mortality rates or the prevalence of AIDS-related illnesses, which follow HIV infection.
Hong Kong	See China, Taiwan.
hopefully	means with hope. Avoid using the word in the sense of *it is to be hoped, in the hope of,* or *let us hope.* (See subjective words.)
however	See and, but, however.
HTML	abbreviation for hypertext markup language.
hung	See hanged, hung.
hyperlink	a word, phrase, or image in a document that, when clicked on with a computer mouse, will take the user to a point in another document or another place in the same one. Hyperlinks are most common in webpages but can also be found in other hypertext documents.

C05757260

hypertext	a computer-based text retrieval system that enables a user to access particular locations in webpages or other electronic documents by clicking on hyperlinks.
hypertext markup language	a special language used to write pages and sites for the Internet.
immigrate	See emigrate, immigrate, migrate.
impact	Verbs such as *affect* or *hit* are preferable to *impact*. If you do use it as a verb, you should always use it intransitively. A missile does not impact a target; it *impacts* ***on*** a target or ***in*** a target area.
impel	See compel, impel, propel.
impending	See pending, impending.
imply, infer	*Implying* occurs when the writer or the speaker states something indirectly. *Inferring* occurs when the reader or the hearer draws a conclusion on the basis of indirect evidence.
important	When you want to introduce a second and more worthy consideration, use *more important* rather than *more importantly. Retail sales were up last month; more important, interest rates fell for the first time this year.* Similarly, use *most important*, rather than *most importantly*, in a context requiring the superlative. (See relevant, important.)
in addition to	See together with.
incessant	See absolutes.
incident, incidence	*Incident* applies to a minor occurrence or an event of only momentary importance. *A border incident took place yesterday when a small patrol entered the neutral zone. Incident* is not the proper word to use in cases of major conflict or catastrophe. An invasion is not an incident; neither is an earthquake. Be careful also to distinguish between *incidents* (occurrences) of civil unrest and the *incidence* (frequency) of civil unrest.
include	See comprise, compose, include.
in connection with	See fill-ins.
incredible, incredulous	*Incredible* means not believable; *incredulous* means skeptical. *His explanation was incredible; she gave him an incredulous stare.* (See credence, credibility, credulity.)
indeed	See fill-ins.
indicate	denotes a conclusion based on specific information. (*The massing of troops indicates that a battle is imminent.*) Do not use when you mean announce, reveal, say, or the like.
indigenous	See domestic, indigenous.
individual	is not a desirable synonym for person. Use it when you need to make a distinction between one person and a group: *The police are searching for the group or individual responsible.*
infer	See imply, infer.
infinitives	No one insists any more that all split infinitives must be shunned. Do, however, make sure that clarity or the flow of the sentence demands the split. If you are not sure, do not split.
inflammable	See flammable, inflammable.
infrastructure	is a legitimate word, but use it selectively.

C05757260

injuries, casualties	are suffered or sustained, not received or taken. (See casualties.)
in order to	often begins an adverbial phrase in the middle of a sentence, but at the beginning of the sentence you can usually do without the first two words. *He brought his lunch in a bag in order to save money.* But: *To save money, he brought his lunch in a bag.* Be careful of negative verbs followed by phrases beginning with *in order to* or *because of*. *He did not go out to lunch in order to save money* and *He did not go out to lunch because he wanted to save money* are both ambiguous, leading the reader to ask *then why did he go out to lunch?* The problem is usually solved by putting the *in order to* or *because of* phrase at the beginning of the sentence. A better plan is to rephrase and change the negative verb to a positive one with negative connotations. *He avoided restaurant lunches in order to (because he wanted to) save money.*
insure	See assure, ensure, insure.
intensify	See escalate, accelerate, intensify.
inter, intra	*Inter* indicates something that is between or among or together; *intra*, a prefix, means within. *International competition* (competition among nations), *intramural competition* (competition within an institution).
Internet	a communications network that connects computer networks and organizational computer facilities around the world.
interestingly	See hopefully and subjective words.
in terms of	a pretentious and often unnecessary phrase that can usually be deleted along with what it introduces—or at least replaced by *at*, *in*, *for*, or *by*.
in this context	See fill-ins.
intra	See inter, intra.
ironically	involves a sharp contrast between the apparent and the expected. Do not use *ironically* when referring to a trivial oddity. *Ironically, the senator, a professed atheist, goes to church every Sunday* is fine. *Ironically, the senator wears tennis shoes to church* is not.
Islam	the religious faith of Muslims. (See Muslims.)
issues	are resolved, not solved.
its, it's	*Its* is the possessive of the personal pronoun *it*. *It's* is the contraction of *it is*.
-*ize* words	appeal to many misguided writers. Seek synonyms for *conceptualize*, *finalize*, *optimize*, *prioritize*, and their ilk—a recent, particularly egregious example is *rumorize*.
jibe	See gibe, jibe.
joint	See combined, joint.
kind	See type.
kudos	is a Greek word meaning glory. In English it means praise or credit for an outstanding achievement. In both Greek and English it is singular and has no plural. Kudos goes to someone, kudos never go to anyone.
lack	as a transitive verb, is not followed by *for*. *The French do not lack* (omit *for*) *a sense of their grandeur.*
laid, lain	See lay, lie.

C05757260

late	When referring to someone who is deceased use *the* before the word *late. He succeeded the late President Smith*, not *He succeeded late President Smith.*
Latin abbreviations	See section 3.11.
latter, former	Both words refer to one of only two persons or things or collections. In a series of three or more, repeat the subject referred to or, if repetition is a problem, use *last-named* (or *first-named*).
lay, lie	*Lay* means to put, place, or prepare. It always takes a direct object. Both the past tense and the past participle are *laid*. (*The President ordered his aide to lay a wreath at the unknown soldier's tomb. The aide laid the wreath two hours later. Yesterday a wreath was laid by the defense minister.*) *Lie* means to recline or be situated; it never takes a direct object. Confusion arises because the past tense of *lie* is *lay* (the past participle is *lain*). *He lies* (or *lay*, or *has lain*) *down.*
lead, led	*Lead* (rhymes with *reed*) means to go ahead of; *led* is its past tense and participle. *Lead* (rhymes with *red*) is the metal.
leave	See depart, leave.
led	See lead, led.
LDCs	See less developed countries.
lend, loan	Use *lend* when you need a verb; *loan* as a verb is colloquial.
less	See fewer, less.
less developed countries (LDCs)	Developing countries is preferred. (Do not say "lesser developed countries." (See Third World.)
liable	See likely.
lie	See lay, lie.
like, as	Both *like* and *as* can properly be used in making comparisons, but *like*, a preposition, governs nouns, pronouns, and incomplete clauses, while *as*, a conjunction, governs full clauses. *He behaves **like** a child. He behaves as a child **would behave**.* Sometimes you can omit the verb in the clause after *as*. In this case the verb is understood: *When I was a child, I thought as a child [would think].* Leaving out the verb will often produce smoother prose, but you need to ensure that the omission does not sound stilted or foster ambiguity.
likely	As an adverb, *likely* must be preceded by a qualifier like *quite, more, most,* or *very*. (*She will very likely win the election.*) As an adjective, it needs no qualifier. *He is likely to blow the operation* (not *He will likely blow the operation*). *She is a likely candidate.* *Apt* and *liable* sometimes crop up as synonyms for *likely*. Neither, however, has the same predictive connotation. *Apt* suggests a tendency, usually unfortunate: *He is apt to lie at the drop of a hat. Liable* connotes vulnerability rather than probability: *He is liable to arrest.*
likewise	is an adverb, not a conjunction, and cannot properly be used as a substitute for *and*.
links	See relations, ties, links.
loan	See lend, loan.

C05757260

loath, loathe, loathsome	*Loath*, an adjective, means reluctant. *He is loath to break the agreement. Loathe*, a verb, means to dislike intensely. *He loathed the long train ride. Loathsome* means abhorrent or repulsive. *The bloody murder was loathsome.*
logistic	in the sense of moving, quartering, and supplying troops, is the adjective; *logistics* is the noun. *Logistical* is discouraged.
lower	is both the comparative degree of the positive adjective *low* (superlative *lowest*) and the antonym of the positive adjective *upper*, which, like the antonymous *lower*, has no comparative or superlative. This consideration is significant only when deciding whether to put a hyphen after *lower* (as always after upper) in a unit modifier. (See footnote 34.)
majority	means more than 50 percent. *Majority* takes a singular verb when the sense is oneness. *The majority of the Senate supports the measure.* When the individuality of the members is stressed, the verb is plural. *The majority of the Senators are from rural districts.* When no one has achieved a majority, someone still will have a plurality (the group that, while falling short of a majority, is larger than any other). Neither *majority* nor *plurality* can be modified by terms like "one-vote" or "one-seat." (See plurality, consensus, and margin.)
margin	*Margin*, not *majority*, is what you call the number of legislative seats by which the majority exceeds the minority. *The Prime Minister's party, with 220 seats, has a 20-seat margin over the opposition's 200 seats.* (See majority and plurality.)
masterful, masterly	Careful writers distinguish between these adjectives. A *masterful* person is overpowering, overbearing, or imperious; he or she is capable of mastering others. A virtuoso performance is *masterly*, the work of a master artist.
material, materiel	*Material* is any substance from which something is made. *Materiel* refers to equipment, especially military supplies.
may	See could, may, might.
maximum	See absolutes.
meaningful	is a vacuous word that is too often used by analysts to mean significant. *The results of the meeting were meaningful* is meaningless.
meantime, meanwhile	The former serves mainly as a noun. *In the meantime, he waited.* You can express the same idea in fewer words by using *meanwhile. Meanwhile, he waited.*
measures, units of	See sections 2.21, 2.22, and 3.15 as well as the conversion chart on page 25.
media	See data, media, criteria, phenomena.
mercifully	See hopefully and subjective words.
metaphors	are figures of speech used to describe something in terms of something else. Approach them with caution. Even experienced writers, seeking to add a flourish to their prose, sometimes make the mistake of mixing unrelated metaphors in a single sentence. One example will serve as a warning: *This slap on the wrist came on the heels of the President's trip.*
Middle East	is preferred over *Near East* and *Mideast* and, as an adjective form, is as acceptable as *Middle Eastern.*
might	See could, may, might.
migrate	See emigrate, immigrate, migrate.

C05757260

military	as a noun can be singular or plural—be consistent within a paper. If in doubt, consider it plural.
militate	See mitigate, militate.
minimum	See absolutes.
misinformation	See disinformation, misinformation.
mitigate, militate	*Mitigate* means to moderate or alleviate. *He did what he could to mitigate his minister's wrath. Militate* means to have weight or effect, either for or against but more frequently the latter. *The facts militate against his interpretation.*
Mod	is an abbreviation-derived jargon word (capitalized) that is acceptable in formal writing about weapons to designate different versions (models) of a weapon system: *the SS-II Mod 2, all Mods of the SS-11.*
modifiers, floating	See also, even, and only.
momentarily	applies to a fleeting instant; it does not mean *at any moment.*
monetary	See fiscal, monetary.
more than, fewer than, over, under, during, while	*Over* and *under* describe location; use *more than* and *fewer than* with numbers. For time, use *during, from,* or *while* except when the time reference is indefinite or vague. *The system has improved during the past year. Inflation is up 10 percent from a year ago.* But: *Relations between the two nations have improved over time. Living conditions have changed over the centuries.*
most, mostly, almost	*Most* is not a proper substitute for *almost* in formal writing. *Almost every one,* not *most everyone. Most,* not *mostly,* is the correct word when you mean to the greatest degree. *Those most affected,* not *those mostly affected.*
Muhammad, Mohammed	See Muslims.
Muslims	are adherents of Islam. They are followers of the prophet *Muhammad,* not *Mohammed.*
nations	See countries, nations.
naturally	See subjective words.
neither . . . nor	When the elements in a *neither . . . nor* construction are singular, the verb is singular; when they are plural, the verb is plural. When the elements differ in number, the verb is determined by the number of the nearer (or nearest) element. *Neither Bob nor Joe is going to the conference. Neither the French nor the Italians are attending this year. Neither Bob nor his neighbors are planting gardens.*
never	Think before writing that something has *never* happened: are you sure that there has not been even one occurrence in all of history? (See absolutes.)
newly industrializing countries or economies	See Third World.
noisome	means either offensive and disgusting, like a *noisome odor,* or harmful; it has nothing to do with noise.
nonaligned countries	do not belong to alliances of West or East, but they often are not practitioners of neutrality, like Switzerland. Instead, they are advocates or opponents of selective policies of both sides. Most of them are grouped in the Nonaligned Movement.

C05757260

nonconventional, unconventional	*Nonconventional* refers to high-tech weaponry short of nuclear explosives. *Fuel-air bombs are effective nonconventional weapons. Unconventional* means not bound by convention. *Shirley Chisholm was an unconventional woman.*
none	is singular when used in the sense of no one or not one. *None of those delegates was elected party chair.* If *none* applies to more than one person or thing, use a plural verb. *None of those delegates were expected to be nominated.* The object of the *of* phrase following *none* is usually the best indicator of whether *none* is singular or plural. *None of the cake was eaten. None of the cookies were eaten.*
North-South	refers in international politics to relations between industrialized and developing nations. *North* and *South* also can mean the two Koreas.
not only . . . but also	In *not only . . . but also* constructions, be sure that the parts of the sentence are parallel. *He is aware not only of the political consequences but also of the military dangers. He not only is aware of the political consequences but also recognizes the military dangers.* (See parallelism.)
number of	a phrase that is too imprecise in some contexts. *A number of troops were killed.* (If you do not know how many, say *an unknown number.*) *Number of*, when preceded by *the*, usually takes a singular verb. *The number of mistakes is small.* When preceded by *a*, *number of* generally takes a plural verb and means several. *A number of the mistakes were due to carelessness.*
numerical order designators	*First, second, third*, and other designators of numerical order are preferred to *firstly, secondly, thirdly*, and the rest.
obviously	See qualifiers.
of	turns up as an unnecessary hanger-on in conjunction with words like *outside* and *off*. The latter are prepositions in their own right and need no reinforcement. One gets *off* one's high horse or *off* the fence, not *off of* them. *Out of*, on the other hand, cannot do without *of*.
of course	See fill-ins.
offload	Use the less pretentious word *unload*.
offput	is not a word. If you are offended, you are put off.
older, younger	refer to only two persons or things or collections of either; *oldest* and *youngest* are the proper adjectives when more than two are involved.
on	See upon, on.
on board	See aboard, on board.
one	has a way of intruding into a sentence. *The congress was an obstreperous one* reads better as *The congress was obstreperous.* In constructions where *one* is the subject, use a singular verb. *One in every 10 senators is uncommitted.* But beware: *He is one of those who were* (not *was*) *uncommitted*; in this construction, *those who*, not *one*, controls the verb.
only	is a floating modifier that can be attached to almost any word in a sentence. Anchor it carefully to ensure that you are conveying the meaning you want to convey. *Even, primarily*, and *mainly* pose similar challenges. *Only he attended the meeting.* (The others did not show up.) *He only attended the meeting.* (He did not make a speech.) *He attended only the meeting.* (He skipped the dinner.)
on the other hand	See fill-ins.

C05757260

opine	See pretentious words.
opposition, opposed, opponent	*Opposition* takes the preposition *to*, as does *opposed*; *opponent* is followed by *of*.
optimize	See *-ize* words.
oral	See verbal, oral.
organ, organism, organization	An *organ* is a musical instrument, a part of the body, or a medium of communication. An *organism* is a living plant or animal. An *organization* is a society or association or business consisting of people united in some way for a specific purpose. Do not use these three words interchangeably.
over	See more than, fewer than, over, under, during, while.
owing to	See based on, due to, owing to.
parallelism	To make a parallel clear, repeat a preposition, an article, the *to* of the infinitive, or the introductory word of a phrase or clause. *Technology **to boost** production and **to exploit** natural resources.*
parameter, perimeter	*Parameter* is a legitimate word for mathematicians and scientists, but it is easily misused, for example when *dimension* or *characteristic* would be better. Save *parameter* for the times you really mean a limiting factor, especially when the thing limited is abstract rather than concrete. Do not confuse with *perimeter*, which is the outer edge of a physical area; the emphasis is on shape and extent rather than on the limits being set.
parliament	Use only if it is the actual name of the body. Otherwise, use *legislature* or the precise name: *National Assembly, Diet, Congress*.
parliamentarian	A *parliamentarian* is an expert on parliamentary rules and procedures, not a member of parliament. People who pass laws are *legislators*. Or use the specific title of the legislators in question (*senator, delegate*). Refer to a Japanese legislator as a *Diet member*, not a *Dietman*.
participles	must not be left dangling, where they often lead to ambiguity and illogicality. *Turning the corner, the view was much changed* is clearly wrong. The sentence should read: *Turning the corner, he found the view much changed.* General guide: participles are adjectives, so watch what they modify and keep them close by. (A memorable dangler from a travel brochure: *You can see the Statue of Liberty sailing into New York harbor.*)
party	should be applied to a person only in telephone and legal contexts. For guidance on when to capitalize party, see section 1.12.
passive voice	See active voice.
PC	means personal computer.
pending, impending	*Pending* means yet to come or not yet settled; *impending* adds a hint of threat or menace.
people, persons, personnel	The word *people* usually applies to sizable groups imprecisely enumerated (*several thousand people showed up for the demonstration*), *persons* to smaller, usually explicit numbers (*217 persons were interviewed, nine persons were hired*). *Personnel* is a collective noun (usually plural) referring to employees of an organization or to members of the armed services as a group. Do not use it as a substitute for *people* or *persons*. *Many people applied. Three persons remain in the running. All company personnel have to be trained.*
perimeter	See parameter, perimeter.

C05757260

personnel	See people, persons, personnel.
persons	See people, persons, personnel.
persuade	See convince, persuade.
phenomena	See data, media, criteria, phenomena.
plurality	The largest single group (of votes, opinions, and the like) when no one has a majority. (See majority and consensus.)
plurals of *-um* nouns	To pluralize nouns that began life as neuter Latin words (ending in *-um*), the DI generally adds s rather than following the Latin rules: *forums* rather than *fora*, for instance. See *Gregg*, section 614 for lists of the preferred pluralizations of foreign words. For Latin (and Greek) words that appear most commonly in the plural, see data, media, criteria, phenomena.
possible	See probable, possible.
possibly	See could, may, might.
practicable, practical	*Practicable* means capable of being carried out in action; *practical* connotes useful. *It was practicable to build a highway* (it could be done), *but it was not practical* (because it would receive little use).
precipitate, precipitant, precipitous	*Precipitate* applies to rash or hasty human actions. *Precipitant* is used in the same general sense, but with stress on rushing or falling headlong. *Precipitous* refers to physical steepness.
preclude, prevent	Generally, *preclude* applies to events as its object, *prevent* to persons. *The bad weather precludes a departure today. The bad weather prevents me from leaving today.*
predominant, predominate	*Predominant* is the adjective; *predominate* is the verb. *His predominant influence is evident in party pronouncements. His views predominated in party pronouncements.*
preface	See foreword, forward.
presently	means in a short time, not at present, currently, or now.
pressure	As a verb, *press* is preferred.
pretentious words	Avoid words like *apprise*, *citizenry*, *contradistinction*, *effectuate*, *enunciate*, *eventuate*, *evince*, and *opine* and use simpler synonyms.
prevent	See preclude, prevent.
primarily	See only.
principal, principle	*Principal* is an adjective meaning most important, or a noun referring to a leader or to money. *Principle* is a noun only. It means basic truth, rule of conduct, fundamental law; *principled* is its related adjective.
prioritize	See *-ize* words.
prior to, before	*Prior to* is appropriate when a notion of requirement is involved. *The law must be passed prior to 1 July.* Otherwise, *before* is the better word.
pristine	describes something that is in its original condition, or primitive. It should not be used as a synonym for *new* or *clean*.
probable, possible	Analysts, particularly military analysts, are tempted to use *probable* or *possible* when *what probably is* or *what possibly is* is the proper formulation: *the attache saw what probably is a missile*, not *the attache saw a probable missile*. Could the officer have seen an improbable (or impossible!) missile?

C05757260

propel	See compel, impel, propel.
protagonist	the leading or principal character, not necessarily a champion of an idea or course of action. *Chief protagonist* is redundant. (See redundancies.)
proved, proven	*Proved* is preferred as the participle, *proven* as the adjective except for energy contexts such as *proved reserves* or *proved fields.*
purportedly	See qualifiers.
qualifiers	Do not weaken judgments supported by direct evidence by inserting words like *apparently, evidently, seemingly, purportedly.* Conversely, you cannot strengthen judgments based on weak evidence by using words like *obviously, undoubtedly, clearly.* These adverbs are an instance of modifiers that do little or no work. Often you will find adjectives that are open to the same criticism. (See subjective words and the discussion of adjectives and adverbs in section 9.3.)
reason, because	After an opening like *the reason for,* the clause containing the reason should begin with *that,* not *because* or *why. The reason for his failure was that he was ill.* Better still would be *He failed because he was ill.*
rebound	See redound, rebound.
rebut, refute	If you *rebut* a point of view, you argue to the contrary; if you *refute* a point of view, you win the argument. New evidence can sometimes *refute* an earlier report or a piece of intelligence analysis; otherwise, *rebut* is generally the appropriate word in DI writing.
redound, rebound	*Redound* means to have an effect. *The plan redounds to his credit. Rebound* means to bounce back. *The economy rebounded last month.*

C05757260

redundancies are phrases that succumb to repetition. They expose bad habits or, worse, carelessness. The author who writes *It is a true fact that they are offering free gifts* is not watching his words. Below are selected examples observed over the years by the "redundancy police":

accidentally misfired	military troops
adequate enough	mutual cooperation
advance reservation	naval marines
as has been mentioned previously	old adage
both agree	own personal
build a new house	past career
bureaucratic redtape	past history
chief mainstay	personal autograph
church seminarians	personal charisma
close confidant	past custom
close personal friend	personal popularity
combine together	piecemeal on a piece basis
completely surrounded	professional career
consensus of opinion	rally together
could possibly	relocate elsewhere
current status	separate isolation cells
established tradition	separate out
exact same	share together
exile abroad	single greatest
exports beyond their borders	single most
eyewitness at the scene	small cottage
first began	small village
final vestiges	sound logic
foreign imports	still continues
free gift	still remains
future potential	still retains
future prospects	sufficient enough
future successor	sum total
historical monuments	tandem couple
historical past	temporary respite
holy shrine	temporary suspension
in close proximity	thin veneer
interact together	top business magnate
joint coalition	true facts
little booklet	trusted confidant
live studio audience	underlying premise
long litany	unexpected surprise
major crisis	unite together
major milestone	well-known reputation
meet personally	young baby

refute See rebut, refute.

regard See consider, regard.

regime has a disparaging connotation and should not be used when referring to democratically elected governments or, generally, to governments friendly to the United States.

regretfully See subjective words.

regrettably See subjective words.

C05757260

relations, ties, links	*Relations* should be followed by the preposition *with. This country is about to establish relations* ***with*** *that one. Ties* (or *links*) should be followed by *to. That country has ties* (*links*) ***to*** *this one.*
relatively, comparatively	*Relatively* should be used only when the intended comparison can be easily grasped. *He has a relatively heavy workload* has, by itself, little meaning. Relative to what? Last year? Last week? His colleagues? The same stricture applies to *comparatively.* (See compare, contrast.)
relevant, important	*Relevant* refers to something that has a bearing on the matter at hand and should be followed by *to. His speech was relevant* ***to*** *the problem.* Do not use *relevant* when you mean *important.*
reluctant, reticent	*Reluctant* means hesitant, unwilling to act and should not be confused with *reticent*, which means uncommunicative or reserved.
represent	means to depict or symbolize, not constitute. *The red line on the map represents the boundary between France and Germany* is proper usage. *South African gold represents most of the world's output* is not.
reticent	See reluctant, reticent.
reveal, expose, disclose, divulge	*Reveal* implies an unveiling of something not previously known; *expose*, to the making public of something reprehensible; *disclose*, to the making public of something that has been private; *divulge*, to the making public of something that has been secret.
Russian submarines	See section 7.6e for information on Russian submarine designators and footnote 39 for a list of submarine names.
sanction	as a noun, has meanings that are almost in opposition: from approval and encouragement to penalty and coercion. It should therefore be used only when the context makes its meaning clear. As a verb, *sanction* picks up only the approval aspect of the noun.
sanguinary, sanguine	*Sanguinary* means accompanied by carnage or bloodthirsty. *Sanguine* means ruddy or optimistic and cheerful.
seemingly	See qualifiers.
semiannual	See biannual, biennial, semiannual.
shall, will	Grammar purists tell us there are fine distinctions to be made between *shall* and *will.* Today, these distinctions are not closely observed even in serious writing. For devotees of grammatical history, the distinctions are: in the first person, *shall* denotes simple futurity; in the second and third persons, *shall* denotes promise, inevitability, command, or compulsion. *Will* is the other way around. In our publications, use *will.* The same distinctions are true for *should* and *would.*
she/her/hers	See gender.
ship	See boat, ship.
should	Except when used to connote moral obligation, *should* is a fuzzy word. Use more precise language in presenting intelligence judgments. (See shall, will.)
significantly	See fill-ins.
single	See redundancies.
situation	See condition, situation, activity.

C05757260

smartphone	a mobile phone that offers advanced capabilities, often with PC-like functionality.
sort	See type.
spam	unsolicited e-mail, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; as a verb it means to send such junk e-mail.
strategy, tactics	*Strategy* is an overall plan of action, usually military action; *tactics* are specific plans or maneuvers designed to advance strategic goals. *Nuclear weapons can be included in both strategic and tactical planning.*
subjective words	The DI is not in the business of deciding whether something is good or bad; therefore, words like *fortunately* and *unfortunately* should not appear in DI writing. Discerning the subjective overtones sometimes requires a keen ear: *naturally*, for example, may give the reader a sense of being talked down to. *Regretfully, regrettably, mercifully, interestingly*, and other subjective words are vulnerable to the same kind of abuse. Stick with terms that focus on the world of our operational readers: motives and the actions that flow from them, choices, strengths and weaknesses, capabilities and intentions. Most of the time you can find a better way to express the thought. (See hopefully, feel, regime, and upbeat, downbeat.)
surveil	If you must use it, confine it to the military or intelligence sense.
table	As a verb, *table* can mean to put a bill aside. In British usage it can also mean to introduce a bill for consideration. Use the word only when the meaning is unmistakable.
tactics	See strategy, tactics.
Taiwan	See China, Taiwan.
technical terms	For the most part, DI analysts are writing for generalists. Generalists may have deep expertise in specific areas, such as missile technology or a country's tribal politics; nonetheless, the analyst's goal is to do away with the specialist's jargon and to put everything into layman's language. If your audience consists of just a few people who thoroughly understand the subject (or who cannot be trusted to follow the reasoning without jargon to guide them), by all means sprinkle your piece with technical terms. Most of the time, however, write for the nonexpert.
that, which	*That*, as a relative pronoun, introduces clauses containing information necessary for the full comprehension of a sentence. Such defining or restrictive clauses are not set off by commas. *The report that was on the general's desk needed revision* suggests that there were several reports, but only the one on the general's desk needed to be revised. *Which* introduces clauses that are not essential to the meaning of a sentence. These nonrestrictive clauses are set off by commas. *The report, which was on the general's desk, needed revision* suggests that there was a report in need of revision, and it happened to be on the general's desk. The distinction between the two types of clauses is not always easy to make. In crisp prose, *that* can, and probably should, often be deleted. *The information that he needs* goes faster as *the information he needs.* When persons are involved the pronoun is *who*, whether the clause is restrictive or nonrestrictive.

C05757260

there is, there are	Try to avoid using *there is* or *there are* to start a sentence; look for a more illuminating verb than *is*. If you do lead off with such a construction, be sure the number of the verb agrees with the subject that follows. Acceptable but minimally informative: *There is an artillery regiment on the border.* Better: *The government has moved an artillery regiment to the border.* Grammatically correct but hard to comprehend: *There are a headquarters building for each unit and numerous other structures.* Better: *The army has built a headquarters building for each unit as well as numerous other structures.*
Third World	refers to the economically underdeveloped or developing nations in Africa, Asia, and Latin America. These nations are also known as *less developed countries*, or *LDCs*, or, preferably, *developing countries*. Some countries within the Third World are more advanced than the others; they are called *newly industrializing countries*, or *NICs*. Among the NICs are Singapore and South Korea. When a reference to such a grouping embraces "noncountries" such as Hong Kong and Taiwan, the more appropriate term is *newly industrializing economies* (avoid the abbreviation *NIEs*). Note that we capitalize (for clarity) the abbreviations *LDC* and *NIC* but not the literal terms they stand for; however, we do capitalize (for distinction or contrast) certain nonliteral terms like *Third World, Cold War, North-South, East-West,* and, if unavoidable, *Free World.*
this	Often used as a demonstrative pronoun, representing in a single word a situation or a thought expressed earlier. Be sure, however, that *this* has a clear antecedent; if it does not, either rework the sentence to make the antecedent unmistakable (proximity is the best solution), add the appropriate word or words after *this*, or devise a formulation that makes the connection without using *this*.
ties	See relations, ties, links.
together with	is often found immediately after the subject of a sentence. *Together with* phrases do not affect the verb. *Lower productivity, together with higher interest rates, is hurting the economy.* The same is true of *along with, as well as, in addition to,* and *like*.
too	in the sense of *very*, is not acceptable in formal writing; in the sense of *excessively*, however, it is likely to be the best word.
torturous, tortuous	*Torturous* means extremely painful. *Tortuous* means twisting, devious, or highly complex. *Many accidents have occurred on the tortuous mountain road.*
traditions	long-established practices or elements of culture passed down from generation to generation. Do not use to describe practices developed over the past few years.
try	is followed by *to*, not *and*.
type	As a noun, *type* should be followed by *of* in constructions like *that type of plane* or, in the plural, *those types of planes*. Never omit the preposition. The same holds true for *kind* and *sort*.
ultimate	See absolutes.
unconventional	See nonconventional, unconventional.
under	See more than, fewer than, over, under, during, while.
undoubtedly	See qualifiers.

C05757260

unfortunately	See subjective words.
uninterested	See disinterested, uninterested.
unique	See absolutes.
universal	See absolutes.
unprecedented	See absolutes.
upbeat, downbeat	should be confined to use as musical terms. In formal prose they sound overly colloquial and may be value-laden as well. (See subjective words.)
upcoming, forthcoming, coming	When you are looking for an adjective meaning *to take place later*, try *forthcoming* or just *coming* instead of *upcoming*. Better yet, give a clue as to when: tomorrow, next week, next month.
upon, on	In almost all cases you can substitute *on* for *upon* as a preposition (*bearing on the case*), but not as an adverb (*he felt overworked and put upon*).
URL	is the abbreviation for uniform resource locator, a protocol for specifying addresses on the Internet.
US	The preferred adjective for our country is *US*, not American. *United States* (written out) is the preferred noun, but *the US* may be used when repetition or space is a problem. You can also use *Washington* as the noun when it is clear that you are referring to the US Government, not the capital city. Never use *we*, *us*, *our*, or *ours* when referring to the United States. *US* (not *our*) *allies disagree*. The first person plural is reserved in intelligence writing for the analysts/estimators/writers themselves.
usage, use	*Usage* means either a manner of use, as in *rough usage*, or a habitual practice creating a standard, as in *good English usage*.
variety of	takes a plural verb when conveying the sense of several or various. *A variety of sources report high casualties.* When the emphasis is on the singular *variety*, rather than on the plural object of *of*, the verb is singular. *A variety of meals is better than eating the same food all the time.*
verbal, oral	A *verbal* message can be either spoken or written. An *oral* message is always spoken.
verbal overkill	Extra words are burdensome to the reader and should be avoided. Here are some samples of verbal overkill and a simple substitute for each: are in a position to (can) at that point in time (then) at the present time (now) currently in progress (going on) due to the fact that (because) in regard to (about) in the event that (if) in the near future (soon) it is highly likely that (probably) it is possible that (may) never before in the past (never) subsequent to (after) the majority of (most) the manner in which (how) whether or not (whether) (See fill-ins and redundancies.)
very, definitely	Use these and other ambiguous intensifiers sparingly.
viable	denotes the capacity of a newly created organism to maintain a separate existence. It is often mistakenly used when *durable*, *lasting*, *workable*, *effective*, or *practical* is the appropriate adjective.
vicious circle	is correct. Although *vicious cycle* is now seen almost as often, it is not accepted in DI writing.

C05757260

war	See footnote 7 for guidance on capitalization.
whether	*Whether* does not always need *or not. He still has not decided whether to go. She is going whether or not he does.*
which	See that, which.
while	as a conjunction, usually has reference to time. *While the President was out of the country, the Army staged a coup.* It can, with discretion, also be used in the sense of *although* or *but. While he hated force, he recognized the need for order.* Avoid using *while* in the sense of *and.* (See more than, fewer than, over, under, during, while.)
who, whom	Most of the time the issue of whether to use *who* (nominative case) or *whom* (objective case) is straightforward. Subject: *Who* is his boss? Object of a verb: *Whom* did the committee choose? Object of a preposition: *Whom* does she work for? The nominative case in the objective slot, as in *Who did the committee choose?* or *Who does she work for?*, has become acceptable in casual English, spoken or written, but it is not acceptable in formal writing. The main difficulty comes in subordinate clauses, when the syntax sometimes gives *who* and *whoever* an objective cast even though structurally they are nominative. *The voters will pick the candidate who they think will do the best job.* (*Who* is the subject of *will do* in the subordinate clause. Do not be thrown off by the interjection *they think.*) *The voters will turn against whoever they think is responsible for their economic hardships. The voters will turn against whomever they blame for their economic hardships.* (In the first of the last two sentences, it might seem that *whoever* is the object of the preposition *against* and should be replaced with *whomever.* The object of *against,* however, is not a single word but the entire clause *whoever . . . economic hardships.* Thus, *whoever,* the subject of the verb in the subordinate clause, is correct. In the second sentence, *whomever,* the direct object of *blame* in the subordinate clause, is properly in the objective case.)
whose	functions as the possessive of both *who* and *which. Of which,* though grammatically correct, sometimes sounds stilted.
will	See shall, will.
with	Do not use *with* in the conjunctive role of *and.* Sometimes this sort of use has unintended consequences. *They are married* ***and have*** *three children.* (Not: *They are married,* ***with*** *three children.*) *He is married* ***and has*** *a child.* (Not: *He is married* ***with*** *one child.*) Too often, *with* is used to attach an additional thought that would be better treated as an independent clause following an *and* or a semicolon. *Economics and history are his mainstays; knowledge of linguistics is an additional qualification.* (Not: *Economics and history are his mainstays,* ***with*** *knowledge of linguistics an additional qualification.*)
with reference to	See fill-ins.
would	See shall, will.
younger	See older, younger.

C05757260

youth	as the opposite of old age is always singular; when it means young persons (male or female) collectively it is always plural; when the word refers to an individual young male it is, of course, singular, and its plural is *youths*. *The nation's youth were encouraged to enroll. A gang of youths started the riot.* Nowadays, rioting young persons probably include females as well as males, and reports of their activities are more likely to say *youths* rather than *young persons*—a trend that we probably should join until someone comes up with a better unisex term.

C05757260

§ INDEX

A

a, an before h 146
abbreviations 27–34
ambiguous 34
country names 30
China 30
miscellaneous 30
UK 30
US 30
days 32
first reference 27
foreign terms 28
incomplete or possessive references 28
Latin 31
measure, units of 32
military ranks 29
months 32
percent 32
personal titles 31
civil 31
complimentary 31
military 31
plural forms 29
political subdivisions 31
unusual forms 29
INF 30
MBFR 30
MIRVs 29
SALT 30
well-known 28
aboard 146
about 146
absolutes 146
accelerate 156
acquiesce 146
acronyms 146
active voice 146
activity 152
additionally 146
adverbs 146
adverse 147
affect 147
agree 147
AIDS 159
all ready 147
all right 147
all together 147
almost 164
already 147
also 147
alternate 147
alternative 147
altogether 147
always 147
ambiguous 147
ambivalent 147
American 147
among 149
anathema 148
and 148
and/or 148
and so forth 156
anticipate 148
anxious 148
any 148
apparently 148
appraise 148
apprise 148
approximately 146
apt 148
around 146
as 148, 162
as far as 148
as noted 148
assure 148
as well as 148
as yet 148
asylee 148
at the same time 148
auger 148
augur 148
averse 147
awhile 149

B

based on 149
basically 149
because 168
bedouin 149
beef up 149

C05757260

before 167
bemused 149
between 149
biannual 149
biennial 149
bits 149
blatant 149
bloc 149
blog 149
boat 149
both 149
both . . . and 149
boycott 150
breach 150
breech 150
burgeoning 150
burnish 150
but 148
bytes 149

C

cadre 150
calculate 150
capital cities 150
capitalization 1–13
bulleted paragraphs 13
chapters 13
coined names 8
Communist Party officers 10
cross-references 13
diplomatic and consular units 4
diplomatic corps, principal members of 11
first-order subnational administrative divisions, top officials of 11
geographic terms 6
direction 6
geographic groupings, special 6
government bodies 3
graphics 13
head of state or government 10
heir apparent, royal 10
historic events 8
holidays 8
international organizations 4
international organizations, principal officials of 11
judicial branch, principal members of 10
legislative branch, principal members of 10
military forces 4
military service, top officers 11
national government unit, top officials 10
nationalities 7
personal titles 9–11
after or in place of the name 9
before the name 9
persons, names of 2
nicknames 3
personal names, particles in 3
place names, articles in 2
political parties 5
political philosophies 5
proper names, derivatives of 2
proper nouns 1
publications 12
laws and treaties 12
titles, English 12
titles, foreign 12
titles, shortened 12
religious feasts 8
religious leaders, titles of 5
religious terms 5
seasons 13
storms, major 13
tables 13
trade names 8
tribes 7
casualties 150, 161
celebrity copycatting 150
center 150
charisma 150
China 30, 151
citizenry 151
clearly 151
climactic 151
climatic 151
clout 151
cohort 151
colloquialisms 151
colored 151
combined 151
coming 173
communication(s) 151
communism 151
comparatively 170
compare 151
compel 152
compose 152
compound words 59–68
any, *every*, *no*, or *some* combined with *body*, *thing*, *where*, or *one* 60
beginning with certain nouns 60
compass directions 61
ending with certain words 60
improvised 67
joined or hyphenated 59
noun combinations 59

C05757260

numerical 66–67
fractions 67
in adjective compounds 67
spelled out 66
prefixes and suffixes 65–66
compounds with capitalized words 66
doubled vowels 65
duplicated prefixes 66
hyphenated 65
to avoid confusion 65
tripled consonants 65
unit modifier containing a multiword compound 66
unhyphenated 65
prepositional phrase in noun compound 67
self or *selves*, with 60
separate words 59
single capital letter plus a noun or participle 68
solid 59
titles 67
unit modifiers 61–64
adverbs ending in *-ly* 63
chemical terms 64
common basic elements 64
comparatives, superlatives 62
differentiated from predicates 62
en dash with proper noun 63
foreign phrases 63
hyphenated 61
letter or number elements 64
ordinal numbers, with 62
proper nouns 63
quotation marks 64
three-word modifiers 63
unhyphenated 61
verb forms of two-word noun combinations 67
verbs-adverbs combinations 60
comprise 152
concern 152
concerted 152
conclave 152
concrete steps 152
condition 152
consensus 152
consider 152
consul 153
continual 152
continued 152
continuing 152
continuous 152
contractions 152
contradistinction 152
contrast 151
convince 153
could 153
council 153
countries 153
credence 153
credibility 153
credulity 153
crisis 153
criteria 154
culminate 153
cyberspace 153

D

data 154
dates as modifiers 154
decimate 154
definitely 173
defuse 154
depart 154
deploy 154
deprecate 154
depreciate 154
developing countries 154
diagonal (or slash) 52
die 154
Dietmen 154
different from 155
diffuse 154
dilemma 155
diplomatic corps 155
disburse 155
disclose 170
discreet 155
discrete 155
disinformation 155
disinterested 155
disperse 155
divulge 170
domestic 155
downbeat 173
due to 149
during 164

E

each 155
eager 148
East Asia 155
East-West 155
economic growth 155
effect 147
effectuate 156
either 156

C05757260

election 156
e-mail 156
embargo 150
em dash (or dash) 46
emigrate 156
en dash 47
enormity 156
enormousness 156
ensure 148
enthuse 156
enunciate 156
equal 156
equally, as 156
equivalent 156
escalate 156
essentially 156
estimated 156
etc. 156
eternal 156
e-ticket 156
e-trade 156
even 157
eventuate 157
evidence 157
evidently 157
evince 157
exacerbate 157
exile 157
expect 148
expose 170
extra words 157

F

fake analysis 157
Far East 157
farther 157
fatal 157
fear 157
feel 157
fewer 157
fewer than 164
fill-ins 158
finalize 158
fiscal 158
fiscal year 158
flagrant 149
flammable 158
flaunt 158
flounder 158
flout 158
forceful 158
forcible 158
forego 158
foreword 158
forgo 158
former 162
forthcoming 173
fortuitous 158
fortunate 158
fortunately 158
forward 158
founder 158
fractions 158
Free World 158
fulsome 158
further 157

G

gender 159
gibe 159

H

hackneyed phrases 159
hanged 159
hardly 159
he/him/his 159
historic 159
historical 159
HIV/AIDS 159
Hong Kong 159
hopefully 159
however 148
HTML 159
hung 159
hyperlink 159
hypertext 160
hypertext markup language 160

I

immigrate 156
impact 160
impel 152
impending 166
imply 160
important 160, 170
in addition to 160
incessant 160
incidence 160
incident 160
include 152
in connection with 160
incredible 160
incredulous 160

C05757260

indeed 160
indicate 160
indigenous 155
individual 160
infer 160
infinitives 160
inflammable 158
infrastructure 160
injuries 161
in order to 161
insure 148
intensify 156
inter 161
interestingly 161
in terms of 161
Internet 161
in this context 161
intra 161
ironically 161
Islam 161
issues 161
italics 35–37
foreign words 35
anglicized 35
familiar 35
organization names 36–37
other 36
publication titles 36
letters, words, phrases, cited 37
names of craft 37
prominence or emphasis 35
titles 35
it's 161
its 161
***-ize* words 161**

J

jibe 159
joint 151

K

kudos 161

L

lack 161
laid 161
late 162
latter 162
lay 162
LDCs 162
lead 162
leave 154
led 162
lend 162
less 157
less developed countries 162
liable 162
lie 162
like 162
likely 162
likewise 162
links 170
loan 162
loath 163
loathe 163
loathsome 163
logistic 163
lower 163

M

majority 163
margin 163
masterful 163
masterly 163
material 163
materiel 163
maximum 163
may 153
meaningful 163
meantime 163
meanwhile 163
measures, units of 163
media 154
mercifully 163
metaphors 163
Middle East 163
might 153
migrate 156
military 164
militate 164
minimum 164
misinformation 155
mitigate 164
Mod 164
modifiers
floating 164
numerical Unit 17
unit 61
momentarily 164
monetary 158
more than 164
most 164
mostly 164
Muhammad 164
Muslims 164

C05757260

N

nationalities, tribes, and other groups of people 7
nations 153
naturally 164
neither . . . nor 164
never 164
newly industrializing countries or economics 164
noisome 164
nonaligned countries 164
nonconventional 165
none 165
North-South 165
not only . . . but also 165
number of 165
numbers 15–25
1,000 or more 16
10 or more 15
as numbers 18
close together 24
decimals 19
footnotes 18
fractions 19
graphics 18
indefinite 16
indefinite expressions using figures 24
metric units conversion factors 25
millions and billions 16–17
mixed 19
mixed above and below 10 15
money, foreign 20
money, US 19–20
nonliteral sense 18
ordinal 16
pages 18
paragraphs 18
percentages and times phrases 20
possessives 17
ranges 17–18
below the millions 17–18
in the millions 18
ratios, odds, scores, returns 24
scientific notation 24
tables 18
time expressions 21
ages of inanimate things 21
ages of persons 21
centuries 22
clock time 23
dates 21
decades 22
other time expressions 23
years 22
under 10 15
unit modifiers, numerical 17
units of measure 23
units of measure, figures with 23
value expressions 19–20
numerical order designators 165

O

oblique (or slash) 52
of 165
of course 165
offload 165
offput 165
older 165
on 173
one 165
only 165
on the other hand 165
opine 166
opponent 166
opposed 166
opposition 166
optimize 166
oral 173
organ 166
organism 166
organization 166
over 164

P

parallelism 166
parameter 166
parliament 166
parliamentarian 166
participles 166
party 166
passive voice 166
PC 166
pending 166
people 166
perimeter 166
personnel 166
persons 166
persuade 153
phenomena 154
plurality 167
possible 167
possibly 167
practicable 167
practical 167
PRC 151

C05757260

precipitant 167
precipitate 167
precipitous 167
preclude 167
predominant 167
predominate 167
preface 167
presently 167
pressure 167
pretentious words 167
prevent 167
primarily 167
principal 167
principle 167
prioritize 167
prior to 167
pristine 167
probable 167
propel 152
protagonist 168
proved 168
proven 168
publications 12
punctuation 39–52
apostrophe 39–42
brackets 42
editorial remarks 42
inside parentheses 42
bullets 42
colon 42–43
clause separation 43
expansions 42–43
indented material 43
ratios 43
summaries 42–43
titles and subtitles 43
comma 43–46
compound sentences 45
comprehension 43
contrasting statements, setting off 44
coordinate modifiers, separation of 44
corporate names, setting off 46
direct quotation, setting off 46
geographic names, setting off 46
introductory phrases 45
nonrestrictive words, setting off 44
numbers of 1,000 or above 45
personal names, setting off 46
personal title with organizational name 46
serial 44–45
word omission 46
dash 46–47
before summarization 47
instead of bullet 47
parenthetical matter 46–47
ellipsis 47
en dash 47
exclamation point 48
hyphen 48
parentheses 48
comments, setting off 48
cross-references, enclosing 48
foreign words, translations 48
numbers or letters in a series, separating 48
period 49
plurals 41–42
possessives 39–41
compounds 40
firm names 40
geographic terms 40
joint possession 40
noun or pronoun preceding a gerund 41
organization names 40
organized bodies ending in s 40
personal pronouns 41
publication titles 40
with inanimate bodies 41
with persons 41
words ending in s sound 39–40
words not ending in s sound 40
question mark 49
in title 49
uncertainty, showing 49
quotation marks 49–51
double 49
direct quotations 49
unitalicization of titles 50
words or phrases, selected 50
punctuation with 50
single 50
unneeded 51
semicolon 51
compound sentence 51
conjunctive adverbs, with 51
series 51
slash 52
alternatives, to separate 52
combination, showing 52
period occurring in two calendar years 52
per, representation of 52
purportedly 168

Q

qualifiers 168

C05757260

R

reason 168
rebound 168
rebut 168
redound 168
redundancies 169
refute 168
regard 152
regime 169
regretfully 169
regrettably 169
relations 170
relatively 170
relevant 170
reluctant 170
represent 170
reticent 170
reveal 170

S

sanction 170
sanguinary 170
sanguine 170
seemingly 170
semiannual 149
shall 170
she/her/hers 170
shill (or slash) 52
ship 149
should 170
significantly 170
single 170
situation 152
slant (or slash) 52
smartphone 171
solidus (or slash) 52
spam 171
spelling 53–58
British terms 53
consonants, doubled 55
diacritical marks 57
difficult forms 53
endings *-ible, -able* 55
endings *-sede, -ceed, -cede* 55
endings *-yze, -ize, -ise* 54
foreign words, anglicized 53
geographic names 56–57
indefinite articles 55–56
abbreviations having variable pronounciation, before 56
acronyms, before 56
consonants, before 56
initials having consonant sound, before 56
initials having vowel sound, before 56
numerical expressions 56
vowel, before 56
organization names and titles 57
personsonal names and titles 57
plural forms 54
compounds 54
o endings 54
preferred forms 53
transliteration guidance 57–58
spelling and compounding 69–143
strategy 171
subjective words 171
submarines, Russian 170
surveil 171

T

table 171
tactics 171
Taipei 30
Taiwan 30, 151
technical terms 171
that 171
there are 172
there is 172
The World Factbook 2
Third World 172
this 172
ticks (or bullets) 42
ties 170
together with 172
too 172
tortuous 172
torturous 172
traditions 172
try 172
type 172

U

ultimate 172
***-um* nouns, plurals of 167**
unconventional 165
under 164
undoubtedly 172
unfortunately 173
uninterested 155
unique 173
universal 173

C05757260

unprecedented 173
upbeat 173
upcoming 173
upon 173
URL 173
US 173
usage 173
use 173

V

variety of 173
verbal 173
verbal overkill 173
very 173
viable 173
vicious circle 173
virgule (or slash) 52

W

war 174
whether 174
which 171
while 164, 174
who 174
whom 174
whose 174
will 170
with 174
with reference to 174
would 174

X, Y, Z

younger 165
youth 175

FM 34-8-2

INTELLIGENCE OFFICER'S HANDBOOK

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

FIELD MANUAL
No. 34-8-2

Headquarters
Department of the Army
Washington, DC, 1 May 1998

Table of Contents

Page

PREFACE iv

CHAPTER 1 - G2/S2 ROLES AND MISSIONS 1-1
Why You Need This Handbook 1-1
Purpose of This Handbook 1-1

CHAPTER 2 - FORCE PROJECTION 2-1
Force Projection Principles 2-1
Intelligence Readiness 2-2
Indications and Warnings 2-5
Stages of Force Projection Operations 2-6

CHAPTER 3 - MILITARY DECISION-MAKING PROCESS (MDMP) 3-1

CHAPTER 4 - S2 OPERATIONS CHECKLISTS 4-1

APPENDIX A. UNIT INTELLIGENCE TRAINING CHECKLIST A-1
APPENDIX B. INTELLIGENCE PREPARATION OF THE BATTLEFIELD PRODUCTS B-1
APPENDIX C. RECONNAISSANCE AND SURVEILLANCE PLANNING C-1
APPENDIX D. PRIORITY INTELLIGENCE REQUIREMENTS, INFORMATION REQUIREMENTS, AND INDICATORS D-1
APPENDIX E. GRAPHIC REPORT FORMATS E-1
APPENDIX F. TARGETING F-1
APPENDIX G. IEW SYSTEMS G-0
APPENDIX H. MILITARY INTELLIGENCE UNITS AND CAPABILITIES H-1
APPENDIX I. INTELLIGENCE TRANSITION CHECKLIST I-1
APPENDIX J. INTELLIGENCE REFERENCE LIST J-1
APPENDIX K. WEATHER ELEMENTS AND SUPPORT K-1
GLOSSARY Glossary-1
REFERENCES References-1

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

LIST OF TABLES AND FIGURES

Page

Table 1-1. Collection resources 2-1
Table 4-1. Mission checklist 4-2
Table 4-2. N-Hour critical times 4-4
Table 4-3. N-Hour critical actions list. 4-5
Table 4-4. Mission planning sequence. 4-6
Table C-1. G2/S2 R&S responsibilities C-1
Table F-1. Bulk electric power supply F-38
Table K-1. Weather effects from cloud ceilings K-13
Table K-2. Weather effects from reduced visibility K-14
Table K-3. Weather effects from precipitation K-17
Table K-4. Weather and environmental data elements impacting Army systems and operations K-19
Table K-5. Windchill chart K-21
Table K-6. Daily water consumption requirements for three levels of activity K-23
Table K-7. Work time in hot weather operations K-24
Table K-8. WBGT index (light work) K-24
Table K-9. Conversion factors K-25

Figure 2-1. Principles of force projection IEW operations 2-2
Figure B-1. Modified combined obstacles overlay B-2
Figure B-2. Population status overlay B-2
Figure B-3. Key facilities and target overlay B-3
Figure B-4. Logistics sustainability overlay B-4
Figure B-5. Concealment and cover overlay B-5
Figure B-6. Lines of communication overlay B-6
Figure B-7. Doctrinal template - depicts enemy forces according to doctrinal deployment, unconstrained by terrain B-7
Figure B-8. Situation template - depicts deployed enemy forces adjusted for obstacles and terrain B-7
Figure B-9. Decision support template B-8
Figure B-10. Partial BOS synchronization matrix B-9
Figure B-11. Event template - considers COAs of reinforcing or counterattacking forces B-9
Figure B-12. Event template - depicts key events in each threat COA B-10
Figure B-13. Event matrix B-11
Figure B-14. Sample of an ADA-tailored IPB B-12
Figure C-1. R&S planning process C-2

Page

Figure C-2.	R&S planning considerations	C-6
Figure C-3.	Example of a brigade reconnaissance OPORD	C-8
Figure C-4.	R&S overlay with instructions on acetate	C-12
Figure C-5.	R&S tasking matrix	C-15
Figure C-6.	Example of a GSR OPORD	C-17
Figure C-7.	Sample IREMBASS employment OPORD	C-19
Figure C-8.	Sample patrol employment OPORD	C-20
Figure C-9.	Sample debrief format	C-21
Figure E-1.	Graphic INTSUM	E-3
Figure E-2.	Threat unit locations and mission activities (committed)	E-4
Figure E-3.	Threat unit locations and mission activities (uncommitted)	E-5
Figure E-4.	Threat mission capabilities assessment	E-6
Figure E-5.	Threat problem area symbology	E-7
Figure E-6.	Threat air activity symbology	E-8
Figure E-7.	Predicted threat activity timelines	E-9
Figure F-1.	Functions of intelligence support to targeting	F-2
Figure F-2.	Targeting methodology.	F-3
Figure F-3.	Targeting checklist	F-3
Figure F-4.	The targeting process	F-7
Figure F-5.	Example high-payoff target list	F-9
Figure F-6.	Example target selection standards matrix	F-10
Figure F-7.	Example attack guidance matrix	F-13
Figure F-8.	BOS detection capabilities	F-17
Figure F-9.	Intelligence disciplines	F-19
Figure F-10.	Deliver functions and responsibilities	F-22
Figure F-11.	BDA functions	F-27
Figure F-12.	CARVER techniques	F-31
Figure H-1.	MI battalion (heavy division)	H-1
Figure H-2.	MI Battalion (Light, Airborne, Air Assault Division)	H-2
Figure H-3.	Corps MI Brigade	H-3
Figure H-4.	Organization, MI Detachment, Spt Co, SFG	H-4
Figure H-5.	Organization, MI Detachment, Spt Co, SFB	H-4
Figure K-1.	Common weather elements	K-2
Figure K-2.	IPB weather overlay criteria	K-4
Figure K-3.	Example of a weather forecast chart	K-9
Figure K-4.	Example of a weather impacts display chart	K-10
Figure K-5.	Critical weather factors	K-11

PREFACE

This publication is a roles and missions manual for G2/S2 sections. As the companion handbook to FM 34-8, this manual is written for officers serving as the G2 or S2 in combat, CS, and CSS units. It provides guidance for officers and NCOs assigned to G2/S2 sections. G2s should find this handbook a useful MTP when executing intelligence training responsibilities.

The proponent of this publication is the United States Army Intelligence Center and Fort Huachuca, Fort Huachuca, AZ. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, US Army Intelligence Center and Fort Huachuca, ATTN: ATZS-TDL-D, Fort Huachuca, AZ 85613-6000.

This manual does not implement any ISAs. However, it complies with the following STANAGs:

- STANAG 2022, Intelligence Reports, Edition 8.
- STANAG 2077, Order of Battle, Edition 5.
- STANAG 2149, Intelligence Requests, Edition 5.
- STANAG 2844, Counterintelligence Procedures, Edition 2.
- STANAG 2936, Intelligence Doctrine, Edition 2.
- STANAG 6010, Electronic Warfare in the Land Battle, Edition 1.

It also complies with QSTAG 593, Mutual Support Between EW Units; and QSTAG 1034, Intelligence Preparation of the Battlefield.

Unless specifically designated, all references to the intelligence officer at corps, division, brigade, or battalion will be stated as S2.

Acronyms and brevity codes used in this manual are identified only in the glossary.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Chapter 1

G2/S2 ROLES AND MISSIONS

WHY YOU NEED THIS HANDBOOK

The G2/S2 must provide continuous intelligence and information for the commander to conduct operations and minimize risk.

Intelligence is the commander's decisionmaking tool. The commander, who drives intelligence, does so for planning before deployment, while enroute, and during operations and redeployment. The S2/NCO—

- Provides the commander timely and accurate intelligence, IPB, I&W, and vulnerability assessments for force protection, targeting, and BDA.
- Makes decisive predictions on when and where an action will take place.
- Prioritizes IR.
- Integrates with other staff elements on I&S issues.
- Provides the commander with a view of all facets of the battlefield.
- Ensures his staff is trained.

PURPOSE OF THIS HANDBOOK

This manual does not replace the doctrine and TTP contained in the other FM 34-series manuals; it does, however, focus on their application. It also summarizes information that helps the S2 manage and coordinate the CCIR. It provides the S2 the roles and missions required for executing the intelligence support function.

The G2/S2 is the “Top Down”/“Bottom Up” integrator of RISTA operations, which have always been performed at the brigade and battalion levels. Three factors help to redefine traditional R&S planning:

- Top Down reporting.
- Bottom Up reporting.
- Digitization.

Systems and technologies available to units make an integrated approach to managing “top down” and “bottom up” reporting feasible. The ACT serves as the nexus of RISTA operations, digitally linking the brigade S2 with the automated capabilities of the DS MI company, resulting in RISTA operations which blend intelligence, R&S, and TA. (See FM 101-5 for G2/S2 responsibilities and Table 1-1 for RISTA collection resources.)

Table 1-1. Collection resources

IEW	RISTA
SIGINT	Troops in contact
IMINT	Other troops in contact (RAS)
HUMINT	Scouts (aerial & ground)
CI	LRS, SOF
MASINT	Countermortar & CB radars
TECHINT	Gun cameras
	Hand emplaced sensors
	CA, PAO, PSYOP

Chapter 2

FORCE PROJECTION

FORCE PROJECTION PRINCIPLES

Future Army operations will rely more heavily on the force projection of US combat power. There is no single method to support force projection. This chapter identifies key principles and considerations for planning and executing IEW force projection.

Successful force projection of IEW support is based on understanding and applying the key principles shown in Figure 2-1.

Other key force projection components are intelligence readiness and a requirement to define responsibilities each echelon performs down to the lowest tactical level. This chapter discusses—

- Intelligence readiness.
- I&W.
- Stages of force projection operations (minus operations).

Considerations are in a logical order but may not be sequential nor applicable for all force projection missions. Corps and division G2s must provide primary planning support for force projection operations because of their expertise. The S2 at each level identifies—

- Personal knowledge deficiencies (e.g., communications architecture, imagery dissemination systems and methods, ability to identify the staff's shortcomings).

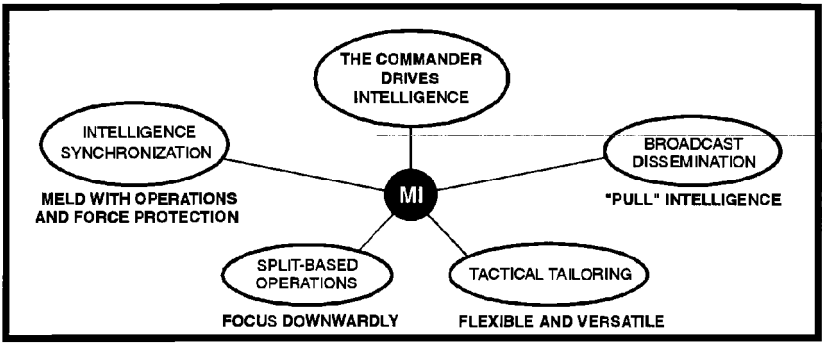


Figure 2-1. Principles of force projection IEW operations.

- Technical limitations (e.g., ASAS, SIDS capability).
- Intelligence gaps with adequate specifics.

INTELLIGENCE READINESS

In a JTF force projection operation, higher echelons will provide intelligence for situation and target development to lower echelons (top down) until the tactical ground force completes entry and secures the lodgment area. The JTF J2 may be reluctant to push everything down through tactical intelligence channels due to the volume of the intelligence information available. The S2 may receive support on a “smart push” basis, and needs to know his requirements to be able to do a “smart pull.”

The most significant change in the evolution of force projection operations is the enhanced information flow through hierarchical and non-hierarchical networks (computer, communications, and personal). The S2 should—

- Review available databases on assigned contingency AIs; conduct IPB on these AIs; and develop appropriate IPB products.
- Be aware of higher HQ SOPs and DIA manuals for specific CM guidance.
- Prepare, practice, and conduct information collection activities as part of in-garrison IO rehearsals.

- Preplan and practice an intelligence "surge" on likely contingency crises.
- Prepare and practice coordination from predeployment through redeployment with personnel from imagery, SIGINT, HUMINT, SWO, CA, PSYOP, and SF units, to include databases and connectivity.
- Ensure the following are a part of the daily operating environment:
  - — RC and other augmentation.
  - — Line numbers and SOPs including a linguist plan with proficiency scores (alert through early entry phases of deployment).
  - — Training (individual and collective).
- Form ad hoc intelligence links and networks early on to meet a developing contingency. Incorporate, request, and receive intelligence from unfamiliar sources (linguists, MI augmentation, other services); exploit NGOs and PVOs once a crisis emerges. Exchange communications protocols with theater and higher HQ and subordinate and lateral units.
- Forward all RIIs to the higher HQ IAW SOPs. The J2, G2, and S2 can focus intelligence downward based on the commander's needs.
- Understand the JTF J2's multiple echelon and broadcast dissemination capability to ensure NRT reporting to all deployed, in transit, or preparing to deploy forces.
- Maintain an intelligence database on the battlefield environment and threats for each contingency. The S2 must state and record the CCIR as PIR, subordinate SOR, and SIR, and include the following:
  - — For the battlefield environment, the commander's approval of the AI, to include separate ground, air, littoral waters, and political AIs.
  - — Maps, terrain, and weather products. Request from National Imagery and Mapping Agency hard copies (unclassified or at the lowest classification). Request authority to declassify these products locally.

— Digitized products (map sheets for ASAS, terrain data, and imagery).

— Physical environmental information. The TERRA BASE program allows S2s to template the effects of terrain on communications and direct fire. During mission analysis, TERRA BASE or other automated terrain products—WINCATS, TOPOSKINNER—provide the S2 a tool to help the commander visualize how terrain can affect friendly and enemy forces. These products can illuminate terrain effects for subordinate commanders in the OPORD brief. [Technique: Use the program at Home Station to develop and sustain proficiency.] The supporting engineer staff officer may also have terrain visualization products.

— Threat or potential threats. The intelligence community, primarily the NGIC, and open sources produce products useful for intelligence readiness. These products can be tailored to best support the commander. (See FM 34-3 for information on intelligence analysis.) INTELLINK will be an S2's primary access to any type of requested strategic intelligence. Examples of strategic level products include—

- Global security forecast.
- Battlefield development plans.
- Automated and hardcopy databases.
- Arms proliferation and military power studies related to the weapons acquisition strategies and the overall military power and potential of selected foreign military forces.
- TECHINT and User Bulletins.
- CIA World Fact Book and DIA country studies.
- Open source studies and articles.
- Other services.

INDICATIONS AND WARNINGS

Theater and national intelligence units monitor regional and global threats to

provide I&W intelligence to the NCA and military commanders. I&W intelligence flows to strategic, operational, and tactical commanders; it prevents surprise, reduces risk, and supports development and refinement of CONPLANs. The S2 must ensure the commander identifies PIR, IR, and targeting requirements for each assigned contingency area. The S2 should—

- Conduct CM and synchronization planning on I&W requirements. Review your unit's collection plan and preplanned SOR for each contingency area. If necessary, refine existing collection plans and SOR.
- Review and modify reporting procedures for I&W contingency areas. This may involve changing intelligence reporting (e.g., increasing reporting on one area and decreasing reporting on another) and message routing addresses and precedence (e.g., FLASH designation).
- Prioritize and forward SOR to higher headquarters.
- Disseminate intelligence and information to the commander, staff, and subordinate units.
- Coordinate for direct dissemination when possible.
- Recommend to the commander whether to maintain or increase unit readiness levels; plan and surge the intelligence effort for the impending operation; or move the unit from its current mission to contingency, branch, or subsequent operations.
- Adjust intelligence readiness steps according to pre-crisis I&W.

STAGES OF FORCE PROJECTION OPERATIONS

REMINDER: All phases of the intelligence cycle are being executed continuously during all stages of force projection.

MOBILIZATION:

Mobilization is a process in which the armed forces augment the AC capability in preparation for war or other national emergencies. It includes activating all or part of the RC assembling and organizing personnel, supplies, and materiel; and certifying the proficiency of individuals and units.

(See FM 100-17 for mobilization process.) In peacetime, AC and RC MI units plan, train, and prepare together to accomplish mobilization and deployment tasks. During the mobilization phase, the S2 should—

- Assist the mobilizing RC unit by preparing and conducting intelligence training and threat update briefings and by disseminating intelligence.
- Identify force requirements for the different types of operations and CONPLANs.
- Employ and adhere to existing procedures.
- If possible, use prior coordinated IMAs to fill gaps created by personnel shortages. These IMAs should already have a working knowledge of your SOPs and understand the mission.
- Monitor intelligence reporting on threat activity and I&W indicators.
- Conduct or coordinate CI and OPSEC training and operations.
- Manage IR and RII from your unit and subordinate units.
- Evaluate reporting.
- Update collection planning.

PREDEPLOYMENT ACTIVITY:

Predeployment activity provides the foundation for subsequent force projection operations.

- I&W will continue throughout force projection operations. The S2 must perform IPB early and continuously. (See FM 33-1, FM 34-130, FM 41-10.)
- Accelerated training will ensure all AC and RC MI units are able to conduct IEW operations. Integrate mobilization and deployment tasks into unit METL and training; emphasize and integrate critical aspects of force projection into battle tasks and planning.
- Focus broadbased knowledge to support CONPLAN refinement (IPB).

- Ensure tactical tailoring or split-based operation planning is based on an existing CONPLAN.

- Establish appropriate relationships; establish higher, lower, and lateral liaisons if they are different.

- Continuously conduct and update CM and IEW synchronization planning.

  — IO synchronization ensures IO are linked to the CCIR and respond in time to influence decisions and operations. IO encompasses more than just MI assets and requires MI support. (See FM 34-40 and FM 100-6.)

— IEW synchronization ensures IEW operations are linked to the CCIR and respond in time to influence decisions and operations. IEW is a subset of IO.

— The commander generates CCIR. CCIR focus on what is critical. They should change as the situation changes. CCIR affect PIR, IR, EEFI, and FFIR.

o Plan imagery coverage for target nomination, validation, and PSA.

o Require from collection assets, timelines for preplanned and dynamic collection requests.

o Plan synchronization through all five steps of the intelligence cycle.

o Ensure each PIR is related to a specific operational decision. (See FM 34-2 and FM 100-6.)

o Prepare an ISM and backward plan so collection production efforts are executed with the operation; deliver focused intelligence to support operational decisions.

o Coordinate with the S3 and signal officer for EW offensive and electronic deception operations, specifically for target nomination, no-fire target criteria, protected frequencies, and synchronized EW effort during all phases of the operation.

o Plan BDA requirements.

o Refine, manage, and update SOR. Monitor and maintain synchronization.

- Anticipate and initiate collection early against long lead-time requirements.

- Ensure CCIR process is continuous and the intelligence cycle and IEW operations remain tied to the commander's decisions and concept of operations.

- Identify collection gaps after you synthesize available information on the AO and coordinate the collection efforts of existing intelligence organizations. (Consider national, EAC, other US forces and services, and HN support.)

- Develop a collection strategy which factors PIR, IR, and METT-TC. Submit RII and other requests for support to adjacent, higher, and HN units. Develop a collection plan which supports all PIR and IR and maintains synchronization.

- Develop your intelligence team:

— *Commander's intelligence support*: The S2 and supporting MI commander form the maneuver commander's intelligence team. ASAS is the primary intelligence processing system supporting this team. A unit may need to augment its S2 staff, to include area experts, TECHINT LNOs, linguists, interrogators, intelligence analysts, and CI agents. Tailor the size and sophistication of the deploying unit's intelligence staff to the mission.

— *ACT*: The DS MI company provides an ACT to support the commander's intelligence team at brigade.

— *Additional attachments*: These could include PSYOP and CA.

— *DISE*: This is a small intelligence support team that provides communications, automated intelligence fusion, and broadcast downlinks in a small package capable of deploying with Army early entry forces.

- Decide whether you will form the DISE from the organic assets of the early entry force or from the corps ACE, supporting EAC MI brigade, or a combination thereof.

- Plan the configuration, which can range from "briefcases" (Mini-DISE) to HMMWVs (DISE vehicular), and are normally staffed by 5 to 12 soldiers, respectively. Build the supporting hardware systems around the Army's ASAS and integrate them with other Army, joint intelligence, and communication capabilities.

- Plan whether the DISE will expand to a full ACE as lodgment operations are completed or will disband once the mission is accomplished.

- Plan situations in which the DISE will go directly to higher headquarters for information without the home base's approval.

- Plan on requirements to support the DISE with 24-hour operations.

— *ISB*: This is the rear element of split-based operations that provides processed and analyzed intelligence to the DISE.

- Plan the automation, communications capacity, and personnel necessary to provide continuous intelligence requirements management, collection, processing, and reporting.

- Plan all procedures for the DISE to "pull" specific intelligence products and reports, obtain status of collection, and "push" the current intelligence picture from the lodgment back to the ARFOR and JTF commanders if not in theater.

— Plan all links to higher intelligence organizations, including the JIC and the elements designed to leverage theater intelligence; focus on support down to the corps and echelons below corps (e.g., the CMISE).

— Coordinate with and understand the capabilities of the JTF to include the NIST if formed.

— Plan to use RC augmentation. Some examples are a mix of CI agents, UAVs, interrogators, and linguists.

- Transportation availability (aircraft or naval vessel) for deployment.

- Sustainability.

- Portability once deployed.

- Disciplined operations. The commander's ability to collect may be affected by nonmilitary decisionmakers. The CINC can contribute to the deploying commander by ensuring at the outset that intelligence is decompartmented and releasable to allied units (if

applicable).

— Review applicable publications (ARs, DA Pamphlets, USSIDs).

— Review SOFAs, ROE, international laws, and other agreements. (Coordinate with SJA on these issues.)

— Review applicable NIMA guidance.

— Establish force deployment priorities based upon METT-T. Sequence initial required forces and capabilities, build-up priorities, and follow-on forces to ensure a sequenced plan, a tailored force, and established command and support relationships. Consider sensors, processors, preprocessors, CI, and HUMINT. Maintain unit integrity.

— Plan communications architecture (build redundancy when possible). Remember to—

  - Plan links to the JTF DISE, if formed, that complements the NIST. (See FM 34-25-3 and FM 34-37).

  - Ensure intelligence links provide the early entry commander vital access to multisource Army and joint intelligence collection assets, processing systems, and databases.

— Ensure collection is synchronized with production, and intelligence is still synchronized with operations (specify reporting procedures and timelines).

— Finalize the IEW OPLAN (terrain and communications deconfliction). Coordinate with the MI commander on his tactical decisionmaking process. Understand the MI commander's SOR that are his specified tasks, implied tasks, task organization, concept of operation (the organization, deployment, allocation, and employment of subordinate MI units), and coordination requirements with forward maneuver units.

— Establish the intelligence crossover point. Estimate the time and establish a measurable criteria to indicate when you have reached that point. Intelligence crossover occurs when enough tactical

collection assets are in theater to reduce the dependency upon strategic

or national assets. (See FM 34-1, Chapter 3.)

- Receive all augmentation and support elements quickly (ACT, DISE) and incorporate them within your unit, SOP, and training.
- Update databases to support the IPB process that will follow. Practice using INTELLINK.
- Support force protection. Intelligence operations—MDCI in particular—identify, locate, and target an enemy's ability to target and affect friendly forces, facilities, and operations. Intelligence support must—
  - — Conduct threat and risk assessment.
  - — Consider elements of fratricide avoidance:
    - Accurate target identification.
    - Collateral weapon effects.
    - Familiarity with supporting units.
    - ROE.
  - — Consider elements of force protection:
    - Information Warfare:
      - OPSEC.
      - Physical destruction.
      - PSYOP.
      - Deception.
      - EW.
    - COMSEC.
    - NBC.

- Personnel security.
- Neutrality maintenance.
- Personal awareness.
- Sniper threat.
- Counterreconnaissance.
- Arms and physical security.

— Using the MDCI process, assess and review friendly vulnerabilities and the threat's ability to exploit them.

- S2s should inform commanders and operators on CI and MDCI analysis.
- Train your MDCI analysts to conduct reverse IPB and think like the enemy S2, to include the enemy's perception of friendly centers of gravity and how he will attack or influence them.
- Incorporate your MDCI analysis into the G2/J2 situation and decision briefings and all planning (especially deception planning).
- Assign CI and MDCI sections appropriate missions and analytical responsibilities, such as rear area threat analysis, and continuously assess effectiveness.

— Identify potential countermeasures to deny the enemy access to friendly critical areas.

— Identify and recommend actions to counter enemy intelligence collection capabilities.

— Implement the following controls to support force projection:

- Establish access to national HUMINT and CI databases, automated links to joint service, coalition, and HN sources to help identify, assess, and develop countermeasures for threats. Develop FLASH precedence reporting procedures.

- Receive and disseminate CI information and specific CI tasks from ASAS and other means such as the CHATS.

- Support further CONPLAN and OPLAN development. MI units continually monitor and update their CONPLANs to reflect the evolving situation, especially during crises.

- Immediately before deployment, update deploying forces with the most recent intelligence on the AO and update your technical databases and situation graphics.

- Develop contingency tailored packages that allow the G2/S2 to place the right force support teams in a deployable posture with an adequate amount of training.

DEPLOYMENT:

Success in force projection operations hinges on the capability of airlift and sealift assets to move forces into the AO. Force protection is more critical during this stage.

- Monitor intelligence reporting on threat activity and I&W indicators. Continuously conduct and update IEW, CM, and synchronization planning.

- Plan enroute updates to eliminate information voids and allow your commander to adjust OPLANs prior to arrival in theater. Request supporting intelligence organizations use SATCOM, broadcast technology, and ADP systems to provide graphic and textual intelligence updates while enroute.

- Continue IPB.

- Provide timely, accurate, and specific infrastructure and weather information. IMETS can provide weather information.

- Use accurate situation development to help the commander understand and reduce risk on the battlefield.

- Use the DST, collection plan, R&S plan, ISM, and SOR to anticipate which decisions the commander and staff will make.

ENTRY OPERATIONS:

During initial entry operations, EAC organizations provide major intelligence support in a "smart push" mode. This support may include departmental, joint, and scalable Army intelligence elements capable of deploying forward. Entry units must continue to "smart pull" the intelligence they need for operations.

- Continue to conduct force protection planning.
- Monitor the buildup of the in-theater capability required to conduct sustained IEW operations and to reduce your total dependence on split-based, "top driven" intelligence from outside the AO. As organic IEW assets flow into the theater, assess their reliability for tactical intelligence. (National and theater organizations will still remain sources of strategic intelligence.) Determine intelligence crossover point.
- Monitor intelligence reporting on threat activity and I&W indicators.
  - — Routinely debrief troops.
  - — Use local nationals employed by or in frequent contact with your force to provide information (area experts must analyze it).
- Ensure liaison personnel and basic communications are in place prior to the scheduled arrival of parent commands.
  - — Deploy HUMINT forces into theater as early as possible.
  - — Contact HN or civil authority. (Contact CA units; see FM 41-10.)
  - — Contact other services.
  - — Contact lateral units.
  - — Coordinate with supporting CI unit for CI support to force protection.
- Emplace ACT, DISE, NIST, and other elements.
  - — Establish security.
  - — Establish communications.

- — Establish analytical capability.
- — Perform IPB.
- — Continue to conduct CM and intelligence synchronization planning. Recommend revised PIR and IR. Refine, manage, and update SOR. Evaluate reporting.
- — Consider space requirements, power, and logistical support for high use or unique items.

- Conduct situation development, target development, and support to targeting. During this stage as combat strength increases, your unit's organic tactical systems will conduct situation and target development (intelligence crossover point).

- Develop measurable criteria to evaluate the results of your collection plan. Reassesses—
  - — "Push" versus "pull" requirements.
  - — Communications architecture.
  - — Reporting procedures and timelines.
  - — Crossover point in intelligence.
  - — Intelligence support to OPLANs and OPORDs, branches, and sequels (to include planning follow-on forces).

WAR TERMINATION AND POSTCONFLICT OPERATIONS:

Upon cessation of hostilities or truce, deployed forces transition to a period of postconflict operations.

Commanders redirect PIR and IR to support units conducting restoration operations (e.g., engineer units conducting infrastructure reconstruction operations, medical and logistics units providing humanitarian relief). The nature of the PIR shifts from assessing threat forces to assessing political, economic, social, religious, and other conditions that affect force protection and the desired end-state; planning residual presence of US forces; and preparing for redeployment of forces.

- Continue to conduct force protection planning.
- Remain open to the possibility that hostilities could resume.
- Monitor intelligence reporting on threat activity and I&W indicators.
- Continue to conduct CM and intelligence synchronization planning. Update collection planning.
- Refine, manage, and update SOR.
- Evaluate reporting.
- Disseminate intelligence.
- Use pre-deployment tactical tailoring procedures to plan a phased redeployment of IEW assets and personnel ensuring continual coverage of the commander's requirements.

REDEPLOYMENT AND RECONSTITUTION:

As the combat power and resources decrease in the AO, force protection and I&W become the focus of the CCIR. This drives the selection of those MI units that must remain deployed and those which may redeploy.

- Monitor intelligence reporting on threat activity and I&W indicators.
- Continue to conduct force protection planning.
- Request intelligence BOS support (theater and national systems) and provide intelligence in support of redeployment and reconstitution (reverse intelligence crossover point).

DEMOBILIZATION:

Demobilization is the process by which MI individuals and units transfer from active to a premobilization or other approved posture. MI units resume intelligence readiness posture. RC MI units transition to peacetime status.

- Monitor intelligence reporting on threat activity and I&W indicators.
- Capture consolidated databases.

- Capture lessons learned via AARs (doctrine and TTP).
- Maintain intelligence readiness (e.g., training).
- Adjust MTOEs and evaluate the need for IMAs.

Chapter 3

MILITARY DECISION-MAKING PROCESS (MDMP)

MDMP in General

- FM 101-5 is the doctrinal source.
- The MDMP is a single, established, and proven analytical technique.
- The commander must follow the one-third/two-thirds planning rule.
- MDMP helps the commander and staff examine a battlefield situation and reach logical decisions.
- The commander can decide to use the complete or abbreviated version.
- Staffs should train on both the complete and abbreviated versions.
- Incomplete execution of the MDMP is a recurring deficiency at the CTCs.

Intelligence in the MDMP

- MDMP is based on continuous IPB, especially initial IPB during mission analysis.
- The commander drives intelligence; IPB is an integrated staff function driven by the commander.
- Train your section to conduct IPB so you can coordinate closely with other staff and BOS representatives.
- You must understand how all the BOS operate and how to integrate intelligence during planning, especially within the targeting process IAW FM 6-20-10.
- "Push" the staff to develop a robust and integrated R&S plan.

Staff Estimates

- FM 101-5 provides a generic staff estimate.
- The generic staff estimate is the base for the commander's operations, personnel, intelligence, logistics, CMO, communications, and special staff estimates.
- These staff estimates are designed to form, analyze, compare, and recommend friendly COAs.
- Staff estimates are continuous, must not be overly time consuming, and do not have to be a written product (time dependent).
- The wargame results and staff estimates help the staff compare COAs.

The Intelligence Estimate

- The purpose, scope, and content of the intelligence estimate changed with draft of FM 101-5.
- The old intelligence estimate was a text-based product derived from IPB that focused on ECOAs, capabilities, strengths, and vulnerabilities.
- This old intelligence estimate is functionally replaced by IPB products.
- A standard staff estimate prepared by the G2/S2 is the new intelligence estimate—it is radically different.
- The new intelligence estimate focuses on the G2/S2's ability to support friendly COAs and is used to compare and approve friendly COAs.

Step 1: Receipt of Mission ■ The mission comes from higher headquarters or is derived from an ongoing mission. ■ On receipt of a new mission, the G3/S3 issues a WARNO to the staff. ■ The staff immediately prepares for mission analysis (SOP preparation). ■ Immediately the commander and staff do a quick initial assessment with emphasis on an initial allocation of available time. ■ The commander issues his initial guidance, and the G3/S3 issues a WARNO to subordinate units.	**Intelligence in Step 1** ■ Collaborate with your higher G2/S2 before and during receipt of mission to facilitate the initial IPB. ■ As part of the initial assessment, look for gaps in your intelligence database and products. ■ Proactively request/prepare terrain products, weather, light, and climatology data; update the MCOO and doctrinal templates; maintain the enemy situation. ■ Focus on the initial time allocation (complete or full MDMP), R&S guidance, and any additional tasks or focus from the commander's initial guidance. ■ Establish/verify an IHL.
Step 2: Mission Analysis 1. Analyze the higher HQ order. (If confused by or you disagree with it, seek immediate clarification or resolution.) 2. Conduct initial IPB. 3. Determine specified, implied, and essential tasks. (It is important to understand specific requirements for each task.) 4. Determine the AI. 5. Review available assets. (The staff must identify additional resources needed to ensure the mission's success.) 6. Determine constraints (normally found in the scheme of maneuver, concept of the operation, and coordinating instructions). 7. Identify critical facts and assumptions. (List all appropriate assumptions from higher; state relevant conditions over which the commander has no control.) 8. Conduct risk assessment. 9. Determine initial CCIR. (Limit to 10 or less.)	**Intelligence in Step 2** ■ Intelligence and intelligence-related products: ❙ AI. ❙ Initial PIR (from the commander.) ❙ Initial OPSEC vulnerabilities and EEFI.***** ❙ MCOO and terrain as described by OCOKA and its effects. ❙ Assumptions (include enemy mission, objectives, threat BOS activities). ❙ Other elements of the battlefield. ❙ Situation templates (unrefined). ❙ Event templates and matrices (unrefined). ❙ Center/centers of gravity. ❙ HVTs. ❙ The IPB portion of the mission analysis brief and associated graphics (OB, weaknesses and peculiarities, activities and capabilities, and COAs). ❙ Collection plan (initial, G2 only).

10. Determine the initial reconnaissance plan. (The resulting R&S annex sets reconnaissance in motion.) 11. Plan use of available time. (The commander and staff refine initial plan for use of available time.) 12. Write the restated mission. Who, what, when, where, and why. 13. Conduct mission analysis briefing. (Given to commander and staff. The briefing is critical to ensure a thorough understanding of planning.) 14. Approve the restated mission. 15. Develop the initial commander's intent. A clear, concise statement of what the force must do regarding the enemy, terrain, and desired end-state. 16. Issue the commander's guidance. This provides additional guidance to focus staff planning. 17. Issue a WARNO. 18. Review facts and assumptions. When facts or assumptions change, the commander and staff must assess their impact.		The R&S plan (initial plan that starts R&S operations) and associated FRAGOs or WARNOs. | Intelligence estimate (initial). ■ These products are used to write Annex B to the OPORD or OPLAN and as the foundation for the DST* later in the MDMP. ■ Based on mission analysis, request information or intelligence based on intelligence gaps. ■ Develop as many ECOAs as time will allow. ■ Your higher HQ OPORD, OPLAN, and/or Annex B will task your unit to perform certain collection or R&S tasks. ■ Start the subsequent steps of CM & intelligence synchronization (FM 34-2) to support the initial collection plan (at a minimum SII, SIR, and SOR). ■ The R&S plan is a coordinated staff effort that must include FS, MEDEVAC, and CONPLANs (e.g., what the brigade does if 2 key scout sections are destroyed). ■ The MI Bn/DS MI Co participates in mission analysis and briefs the collection status and capabilities.
Step 3: COA Development 1. Analyze relative combat power. See FM 34-130 for estimating relative-force ratios. 2. Generate options. Goal is to develop COAs for every feasible ECOA; however, the commander usually limits that option with his guidance. 3. Array initial forces. Identify number of units needed and operational methods; develop a knowledge base to help make decisions. 4. Develop the scheme of maneuver. 5. Assign headquarters. This creates the task organization.	**Intelligence in Step 3** ■ Intelligence and intelligence-related products: | Situation templates (refined and prioritized). | Event templates and matrices (refined). | EWTL (initial).* ■ Ensure the G3/S3 uses the IPB facts, assumptions, and products developed during mission analysis and subsequently refined. ■ Work with the entire staff to ensure that friendly COAs take advantage of the environment and threat situation.*

6. Prepare COA statements and sketches. ■ The G3/S3 uses appropriate media to clearly portray how unit will accomplish the mission (e.g., scheme of maneuver).	■ Key on threat vulnerabilities. ■ Your input is critical in analyzing relative combat power. ■ Do not forget to support deception planning (when appropriate).
Step 4: COA Analysis (Wargme) 1. Gather the tools. 2. List all friendly forces. 3. List known assumptions. 4. List known critical events and DPs; include an HVTL list. 5. Determine evaluation criteria. 6. Select the wargame method. 7. Select a method to record and display results. 8. Wargame the battle and assess results. ■ The wargame is a critical and disciplined process used to visualize the flow of battle. ■ The commander selects the order of comparison of threat to friendly COAs. ■ The staff must evaluate the need for branches and sequels. ■ When technically possible, the staff should capture as much of the wargame on ATCCS as possible; otherwise, use a wargame worksheet or ISM. ■ These wargame results are key to developing DSTs and BOS synch matrix. ■ Use the action, reaction, counteraction method (consider at a minimum maneuver, FS, mobility, counter-mobility, survivability, and IEW). ■ The staff should track force ratios throughout the wargame.	**Intelligence in Step 4** ■ Intelligence and intelligence-related products: ❙ PIR with LTIOV (refined). ❙ HPTs. ❙ Confirmation of the enemy center/ centers of gravity. ❙ Situation templates (final). ❙ Some force protection issues (e.g., NBC vulnerabilities). ❙ EWTL (refined).***** ■ You wear both a "red" and "blue" hat in wargaming. ■ As the enemy commander you project enemy actions or reactions, develop DPs, and project enemy losses. ■ During the wargame you must address all relevant enemy BOS capabilities. ■ As the friendly G2/S2, you identify IR and NAIs; refine the situation template; and participate in the targeting conference. ■ Ensure the G3/S3 honestly portrays friendly capabilities during the wargame.***** ■ Work with entire staff to ensure friendly COAs take advantage of environment and threat situation. ■ Ensure HPTs, AGMs, and TSS support the operation.***** ■ The AGM is approved by the commander and addresses which targets will be attacked, how, when, and the desired effects. ■ TSS are criteria used in deciding whether to pass information as a target nomination.

	■ The MI Bn/DS MI Co commander and collection manager are important players at the wargame.
Step 5: COA Comparison ■ Used to identify COA that has highest probability of success. ■ Staff may use any technique; the decision matrix is the most common. ■ Staff gets its criteria from the commander (e.g., the principles of war or tenets of Army operations).	**Intelligence in Step 5** ■ Intelligence product: ❙ Intelligence estimate (final). ■ Ensure you play a key role during this step.
Step 6: COA Approval ■ If the commander modifies a proposed COA or gives the staff a new COA, staff must wargame that COA.	**Intelligence in Step 6** ■ Intelligence and intelligence-related products: ❙ PIR with LTIOV (approved). ❙ DST (an integrated staff product). ❙ BOS synch matrix.***** ❙ ISM. ❙ Event templates and matrices (final). ❙ The R&S plan (final).***** ❙ Collection plan (refined, G2 only). ■ Start the subsequent steps of CM and intelligence synchronization (FM 34-2) (i.e., development of new SII, SIR, and SOR). ■ If the commander designates you to perform BDA to support one of his decisions, you must thoroughly plan the BDA support and tie that plan into the collection plan.
Step 7: Orders Production ■ Based on the commander's decision and final guidance.	**Intelligence in Step 7** ■ Intelligence and intelligence-related products: ❙ OPORD or OPLAN Annexes B (Intelligence), L (R&S), P (C^2W)*****, Q (OPSEC)*****, S (Deception)*****, and T (EW).*****
***** The G2 participates in developing the products but is not the proponent.	

ACCELERATING THE MDMP:

The MDMP involves three techniques that can be applied in different situations: deliberate, abbreviated, and accelerated. Only the accelerated technique is discussed herein because it is the most difficult to implement. (See CALL Newsletter Update No. 95-12.)

The accelerated technique may be used when one or more of the following conditions apply:

- Commander has a staff available to assist him in developing the plan, but little time to use a more formal process.
- Commander does not have a staff, or the staff is not accessible.

When these conditions apply, the commander must rely primarily on TLP to develop his plan. The accelerated technique assists the commander in developing a tentative plan. Under extreme circumstances, this may be little more than a mental process; nonetheless, the commander can use it to assist him and key staff members (S2/S3/FSO/XO) as he develops his plan.

The accelerated technique follows the basic procedures in the deliberate and abbreviated processes, but the differences are more significant. The major differences between the abbreviated and accelerated techniques involve the commander's guidance and the COA development phase (Figure 3-1). The accelerated technique is characterized by active participation by the commander, and development of one COA that is suitable, feasible, and flexible.

In some situations, the products developed using the accelerated technique may be the same as those developed when using the deliberate or abbreviated technique. Because time is the key factor, the accelerated technique will normally result in the development of a FRAGO.

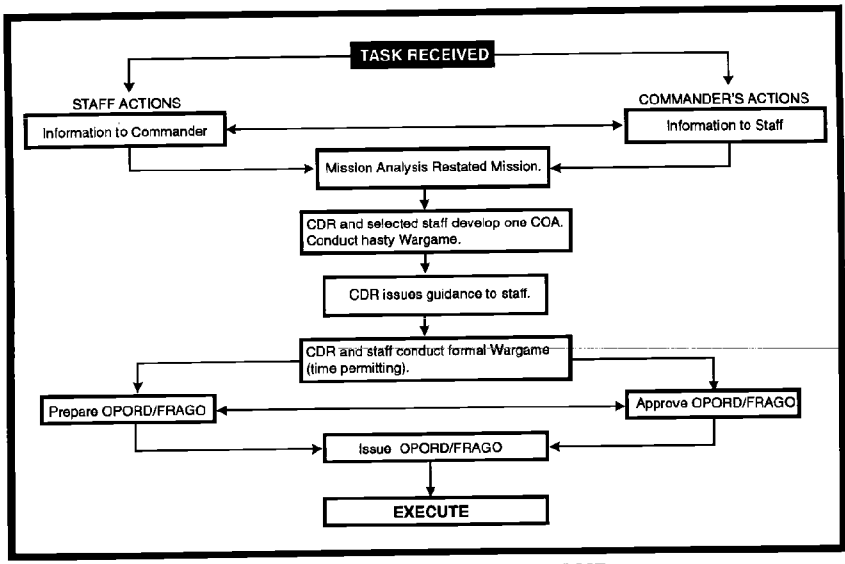


Figure 3-1. Accelerated MDMP.

MISSION ANALYSIS:

ISSUE: The commander and staff must be able to rapidly conduct the mission analysis to determine the restated mission.

DISCUSSION: When using the deliberate or abbreviated technique, the staff conducts a detailed mission analysis to develop the restated mission. As previously stated, resorting to a mental process in lieu of a detailed restated mission is acceptable; however, this should be the exception rather than the norm. The staff may be forced to brief their initial estimates orally, without the use of charts or viewgraphs. Conduct as formal a mission analysis as time allows. During the mission analysis, there are no major differences between the three techniques. There are no techniques that will significantly reduce the amount of time required to conduct the mission analysis. Anticipation, prior preparation, and experience by the staff are the keys to a timely mission analysis process.

TECHNIQUES:

- Commander must get personally involved by supervising and managing the mission analysis process.

- In extreme situations, the staff must be prepared to brief the commander without the use of visual aids.

COA DEVELOPMENT:

ISSUE: When time is severely limited, providing the commander's guidance after the mission analysis may not be the most appropriate time.

DISCUSSION: Instead, the commander may decide to immediately begin personally developing *one* COA with input from selected staff officers. There is probably not time to seek input from every staff officer, so the commander must determine relevant and critical staff officers (e.g., S2, F3, FSO, XO). This team may vary depending on the type of mission. For example:

- In the defense include staff engineer.

- During SASO include CA, PAO, SJA, PSYOP.

- In other situations, include subordinate commanders because of their experience.

This team must then quickly develop a flexible COA to accomplish the mission. The key to success, when using the accelerated technique, is to rapidly develop a base plan with appropriate branches that is flexible, feasible, suitable, and acceptable. *DO NOT WORRY ABOUT DEVELOPING THE PERFECT COA; THERE IS NOT TIME FOR IT*. This is the major distinction between the accelerated technique and the others.

Once the COA is developed, the commander might consider conducting a hasty wargame. In extreme situations, this may be the only opportunity to conduct the wargame process. Next, the commander should begin to quickly develop his guidance to the staff. The accelerated technique is

characterized by an active role of the commander, and very specific guidance to the staff.

TECHNIQUES:

- Focus on developing one COA with branch plans that is flexible, feasible, suitable, and acceptable.

- The commander plays the central role when developing this COA.

COMMANDER'S GUIDANCE:

Once the commander has developed the COA, he must issue guidance to his staff so it can refine and wargame the COA. The commander's guidance to the staff must be directive and specific. The staff's responsibility is to support the commander's plan, not to develop the perfect plan. Well-developed and clearly communicated commander's guidance can be a significant timesaver. The commander's guidance should serve to keep the staff focused by establishing parameters to work within. Commander's guidance must be constantly reviewed and analyzed. As the situation changes and information becomes available, the commander may have to alter his guidance to the staff.

COA ANALYSIS:

ISSUE. The commander and staff must rapidly conduct the COA analysis process.

DISCUSSION: Conducting the wargame process using the accelerated technique is the most difficult of the three processes because only one COA was developed. The purpose of the COA analysis is not to analyze and compare multiple COAs that result in a recommendation to the commander, but to synchronize and integrate the commander's directed COA. This wargame session should focus on refining the branches or contingencies to the base plan and follow the formal wargame process as much as time allows. Focus on the most critical events. You do not have time to wargame the entire operation. When wargaming using the accelerated technique, the commander's involvement is even more important. The staff should use the box technique, focusing on actions at the objective or the engagement area. If time permits, wargame other critical events as well. The staff must work to support the commander's plan. However, as the staff works to refine the plan, it cannot become so biased that it develops a plan that is infeasible and insupportable. If the staff determines that it cannot support the commander's plan, then a new COA must be developed.

TECHNIQUES:

- If time permits, conduct a hasty wargame session during the COA development step. Ensure you identify and develop branches to the base plan.
- Involve the commander. He must supervise the wargame session, actively participate, make decisions, and provide guidance as required.
- Use the box technique, focusing on the most critical event first.

DECISION:

When using the accelerated technique, a decision brief is not required because only one COA was developed. The only decision that may be required is if the developed COA becomes unsuitable, infeasible, or unacceptable. If this occurs, another COA must be developed.

ADVANTAGES:

- Requires less time.
- Facilitates adaptation to a rapidly changing situation.
- Allows commander to compensate for lack of a staff or an experienced staff.

DISADVANTAGES:

- Significantly limits staff initiative and flexibility.
- Very directive, explores only one friendly COA.
- May result in only an oral order or FRAGO.

CHAPTER 4

S2 OPERATIONS CHECKLISTS

Intelligence operations will usually begin with a notice tasking statement. CONPLANs, training, the N-Hour sequence, and the MDMP contribute to mission readiness. The S2 can use the following checklists to monitor intelligence readiness prior to receipt of a mission and subsequently to verify preparations and facilitate mission planning.

The timelines used could apply to any echelon.

- Mission Checklist (Table 4-1).
- N-Hour Critical Times (Table 4-2).
- N-Hour Critical Actions List (Table 4-3).
- Mission Planning Sequence (Table 4-4).
- Reconnaissance Planning (Table 4-5).

Table 4-1. Mission checklist .

Mission Day Minus	ACTION	REMARKS
A-28	Notify attachments to provide updated access rosters prior to A-Day.	
	Provide open access to national and strategic databases.	
	Initiate verification of clearances within battalion.	Include sensitive positions and RTOs.
	Coordinate security briefings for unit personnel.	Include all OPSEC program components and SAEDA program.
	Coordinate contingency AI briefings.	
	Verify access to intelligence databases through division or higher.	Disseminate hard copy products to subordinate units.
	Inspect unit areas and equipment for physical security deficiencies.	Coordinate for support and access. Check equipment compatibility.
	Review section files.	Designate deployable and nondeployable records.
	Obtain current TECHINT/User Bulletins and DIA Top Ten Equipment Acquisition list from 203d MI Bn (TECHINT).	Acquire information on disposition directives from JCS and theater commander.
A-21	Obtain higher HQ access roster.	Update as required throughout mission cycle.
	Coordinate security force requirements with tasked units and MP.	
	Identify linguists in unit or update current file.	Provide list, crosscheck with S1 data.
	Provide updated list of telephone numbers to be cut off at N+2 to the S1.	
A-14	Finalize security plans and instructions.	Check guard/MP patrols.
A-8	Coordinate security requirements for filler personnel.	Barrier material, lighting, container seals, security of vehicle holding area, motor pool, empty barracks.

Table 4-1. Mission checklist (continued).

Mission Day Minus	ACTION	REMARKS
A-8	Prepare DA Form 3964 for classified material transported with deploying elements.	
	Brief MI battalion LNO on duties.	
A-7	Finalize MI battalion personnel and equipment support list.	Ensure copy placed in SDO book.
	Update section alert notification roster.	
	Continually monitor intelligence WATCHCON levels.	
A-4	Check alert rosters in SDO book and completion of all unit OPSEC and SAEDA briefings.	
A-Day	Brief RDC on battalion security plan.	EEFI material, handle accordingly.
	Issue guard instructions.	
	Provide access rosters to rear detachment personnel, higher and supported HQ.	

Table 4-2. N-Hour critical times.

N-Hour	EVENT	REMARKS
N-Hour	Notify and assemble units.	
	Initiate telephone control.	
	Initiate area security plan.	
	List questions for N+2 brief.	
N+1:30	Prepare staff equipment to go to staging area.	
	Verify basic load, load plans.	Maps, batteries, etc.
N+1:45	Depart for N+2 brief location.	
	Distribute updated access roster.	
	Secure battalion conference room.	
N+2:00	Present N+2 briefing.	
	Coordinate with CI to initiate OPSEC plan; inspect battalion area for physical security violations.	
N+3:30	Present the intelligence estimate.	
N+3:45	Confirm transfer of company arms room keys to the rear detachment S2 before departing to staging area.	
	Verify security clearances of attachments through supporting S2.	
N+4:30	Sweep battalion area with CI personnel.	
N+5:00	Impose restrictions on incoming/ outgoing mail.	When given proper authority.
N+6:30	Issue OPORD at staging area.	
N+8:00	Ensure rear detachment is briefed on security.	
	Provide latest intelligence update to commander and staff. Have LNOs, DS MI CDR attend.	

NOTE: Modify times depending on mission requirements and SOPs.

Table 4-3. N-Hour critical actions list.

H-HOUR		ACTION	ACTION OFFICER(S)
	_____	Mission Receipt	
1	_____	WARNO----------	CDR, S2/S3
-	_____	Do IPB----------	S2 (w/asst from ENGR, Terrain, Weather, etc)
2	_____	Mission Analysis	
2	_____	Brief Mission to CDR----------	Coordinating Staff
-	_____	Initial CDR's Guidance	
2	_____	Do COAs----------	CDR, S2/S3
3	_____	Staff IPB & COAs----------	S2, S3
4	_____	Do Staff Estimates----------	Unit Staff
-	_____	COA Analysis (wargaming)----------	CDRs, Unit Staff
5	_____	Select Best COA----------	S3, Selected Staff
6	_____	Do DST----------	S2/S3, FSO, ADA, ENGR, SIG, CHEM
5	_____	Brief DST	
7	_____	Brief Selected COA----------	Selected Staff
-	_____	CDR's Decision	
7	_____	WARNO Scouts/Patrols Recon----------	S2/Asst S2/BICC officer/S3
8	_____	Mission Brief	
8	_____	OPORD Prep/Staff Coord----------	Unit Staff
8	_____	Turn in OPORD Annex	
9	_____	Proof OPORD	
10	_____	Issue Targeting Overlay----------	FSO
11	_____	Brief Scouts/Patrols Recon----------	S2/Asst S2/BICC officer/S3/ENGR/FSO/ADA
12	_____	Execution Matrix----------	S3
13	_____	BOS Synchronization Matrix----------	Unit Staff
14	_____	Maps/Charts Prep----------	Unit Staff
14	_____	CDR's Map Updated----------	S2/S3
15	_____	OPORD Rehearsal----------	XO, S3
16	_____	OPORD Briefing----------	XO
17	_____	Initial Backbrief	
17	_____	TF CDR Brief Higher HQ----------	CDR, S2, S3
17	_____	Co/Bn CDR Backbrief	
18	_____	Rehearsal----------	Unit Staff, CDR
19	_____	Final INTEL Update----------	S2
	_____	LD/LC	

NOTE: These items are not listed in a definite order; some may not occur at all.

Table 4-4. Mission planning sequence .

S2 ACTIONS UPON RECEIPT OF A MISSION:

1. Receive and analyze mission:
   - Receive CDR's guidance and assist in development of CDR's PIR.
   - Understand CDR's intent.

2. Define the battlefield environment:
   - Identify AO and AI.
   - Identify battlefield characteristics that will influence friendly and threat operations.
   - Identify intelligence gaps.
   - Develop preliminary IR.
   - Identify specified and implied intelligence tasks:
     - **Specified:** From OPORD Annex B, R&S Appendix, tasks to subordinate units, MI task organization for combat, coordinating instructions, and collection plan.
     - **Implied:** Mission dependent METT-T.
       M—**Mission** (CDR's intent, PIR, scheme of maneuver).
       E —**Enemy** (OB and IPB to develop collection IR).
       T—**Troops** (Organic and Higher Assets).
       T—**Terrain and Weather** (R&S asset LOS, LOCs, obstacles, weather effects on system's collection ability).
       T—**Time Available** (Plan, Move, Operate, Report).
   - Determine availability of organic/attached/supporting intelligence assets.

3. Request support/information from higher HQ if items/information are not available organically:
   - Maps/Imagery/sketches/blueprints of objectives, NAIs.
   - Collection plan, asset available times and asset tracks.
   - Weather - light data and climatic summary.
   - Enemy OB data.
   - Terrain products (LOC/vegetation/CCM/MCOO/elevation/LOS/hydrology).
   - Higher R&S plan.
   - Determine R&S assets you and higher HQ will control (intelligence architecture).
   - Determine availability, coordinate intelligence support from non-MI systems and organizations (AN/TPQ-36/37, OH-58D, FISTV, AN/TPS-25A, AN/TPS-58B, Engr, Co/teams, Cavalry, chemical units).
   - Obtain SOI; sign and countersign information through unit SIGO.
   - Advise higher of your recommended PIR and expected intelligence gaps.

4. Distribute maps, imagery, and sketches (maintain accountability).

5. Brief staff on abbreviated intelligence estimate to assist their mission planning.

6. Issue WARNO to R&S assets.

7. Describe the battlefield's effects:
   - Analyze terrain.
   - OCOKA factors.
   - Effect on friendly and enemy operations.
   - Analyze weather effects on terrain, troops, equipment, and friendly and enemy operations.

Table 4-4. Mission planning sequence (continued).

8. Assess other characteristics of the battlefield (mission dependent):
   - Politics.
   - Population.
   - Demographics.
   - Social ethnic/Religion.
   - Economic

9. Evaluate threat:
   - Evaluate enemy OB, current disposition and strength, committed and reinforcing units (maneuver, artillery, engineer, ADA, NBC, UW, air, intelligence assets, smoke, E-O sensors) and current significant activities.
   - Evaluate threat capabilities and tactics.
   - Develop/refine intelligence database and threat models.
   - Prepare doctrinal templates.
   - Prepare threat critical event lists.

10. Determine ECOAs:
   - Use doctrinal templates to develop event and situation templates (include all forces that can affect mission completion), AAs and MCs.
   - Identify enemy mission and intent.
   - Determine (in simple terms) how the enemy sees us acting in this operation.
   - Determine how the enemy is currently disposed and what must be accomplished to get from now to his desired end state, given that this ECOA must account for our actions determined in 3 above.
   - Determine enemy concept of the operation and subunit tasks. How will each of the following contribute to accomplishing the intent determined in 2 above:
     - Maneuver.
     - RISTA.
     - FS.
       - Artillery/mortars/rockets.
       - CAS.
       - Aviation.
       - NBC weapons.
       - EA.
     - Air defense - Recommend task organization for MI assets.
   - Identify most likely and most dangerous ECOAs.
   - Identify IR and NAIs for each friendly COA identified; TAIs with S3/FSO for each COA.
   - Develop HPTs for each friendly COA with S3/FSO.
   - Assist in developing HVTs for each ECOA.
   - Integrate EA into targeting.
   - Determine BDA criteria (damage required for each target, a means to determine damage).
   - Finalize and prioritize PIR (obtain CDR's approval).
   - Define indicators and SIR.
   - Send WARNO on threat to subordinate units to facilitate planning.

11. Develop ISM:
   - Tie to PIR/IR (include LTIOV).
   - Include timeline, required decisions, decision criteria, SIR, collection assets.
   - Plan for system cross-cue, back-up coverage.
   - Ensure it answers CDR's requirements for intelligence, targeting, and BDA in time to make decisions.

Table 4-4. Mission planning sequence (continued) .

- Participate in staff wargame of DST and targeting plan (as opposing CDR).
- Never hold MI assets in reserve.

12. Develop R&S plan and overlay to support DST (with support from S3/FSO/ENGR/ ADO) (see **Reconnaissance Planning** below):
- Determine indicators, SIR, NAIs, DPs, TAIs.
- Ensure NAI/TAI support synchronization or R&S plan with fire plan and scheme of maneuver.
- Identify intelligence gaps and request collection support from higher (RII).
- Develop communications plan/reporting schedule.
- Wargame R&S and collection plan.
- Update ISM, R&S, and/or collection plan.
- Receive, consolidate, and deconflict subordinate R&S plans and overlays.
- Consider "Reconnaissance Fundamentals" [Maximum reconnaissance force forward, orient on the location or movement of the reconnaissance objective, report all information rapidly and accurately, retain freedom to maneuver, gain and maintain enemy contact, develop the situation rapidly (FM 17-95).]
- Consider "R&S Principles" [(1) Tell the commanders what they need to know in time for them to act and (2) Do as much as possible ahead of time (FM 34-2-1)].

RECONNAISSANCE PLANNING

While the DMP for reconnaissance operations is conducted in the same manner as for any other combat operation, the following steps will assist the reconnaissance planner in ensuring that the unique features of reconnaissance operations are addressed.

Reconnaissance Mission Analysis

■ Identify Reconnaissance Objectives. Reconnaissance mission analysis must identify the objectives of the unit's reconnaissance effort. These objectives are obtained from—
- PIR.
- DPs.
- HPTs/HVTs.
- Confirming Events. (These are enemy actions and counteractions that confirm an ECOA and are determined by event analysis.)

The reconnaissance planner may determine that some of the above requirements may be accomplished by RFIs to higher HQ, but all of those that are not must become reconnaissance objectives.

■ Identify Reconnaissance AO. Reconnaissance planners identify the area in which reconnaissance forces will be operating, either specified by control measures such as LOAs or CFLs or implied by the location of reconnaissance objectives.

■ Restate Reconnaissance Missions. Once reconnaissance objectives have been determined, the mission for each element of the unit reconnaissance force must be determined from task analysis and stated as a subunit task. The task analysis process—determining specified, implied, and essential reconnaissance tasks and identifying limitations and constraints—is described in FM 101-5. Reconnaissance missions will be determined to be reconnaissance-in-force or zone, area, route, or force-oriented reconnaissance missions.

■ Identify Available Reconnaissance Force. Reconnaissance planners must identify the subunits that are available to execute the unit's reconnaissance effort and their current and projected status.

Table 4-4. Mission planning sequence (continued) .

■ Identify Available Equipment. Reconnaissance planners must identify the equipment available in an FMC status that will be used by elements of the reconnaissance force to accomplish reconnaissance tasks.

RCOA Development

■ Identify Required Reconnaissance Force. Reconnaissance planners must identify the force required to accomplish the unit's reconnaissance objectives. The number and type of elements involved will be based on the following:

- Number, type, location, and sequencing of reconnaissance objectives. Some objectives will require constant surveillance. Some will be time-phased and need only be observed for part of the battle. Some elements of the reconnaissance force will be able to accomplish several reconnaissance objectives.

- Type of reconnaissance mission. A route reconnaissance will require a different element than a reconnaissance-in-force.

- Strength, composition, and disposition of enemy security force. For each element of the reconnaissance force, the decision will have to be made whether it will have to infiltrate or penetrate the enemy security force. Infiltrations dictate stealthy elements and techniques while penetrations will require the correct reconnaissance force ratio.

■ Identify Required Equipment. Each reconnaissance objective will require specific reconnaissance equipment based on the following:

- Proximity of the reconnaissance element to the objective. What is the effective observation range?
- Environmental conditions. What will be the impact of severe weather? Night?
- Signature provided by the target. Does it emit a signal? Heat? Does it need to talk to anyone?

■ Determine the Reconnaissance Scheme. The RCOA must ensure that all reconnaissance objectives are addressed by elements of the reconnaissance force that can provide the read on the objective required by the commander. The reconnaissance force must therefore be in the right place, at the right time, and with the right observation, communications, and force protection equipment. The RCOA must deploy the reconnaissance force in depth to ensure that contact is not lost with moving reconnaissance targets. It must identify reconnaissance objectives that cannot be addressed so that RFIs may be prepared or risk accepted. In developing the RCOA, reconnaissance planners must answer the following questions:

- Are all PIR, HPT, DP, and confirming events addressed as reconnaissance objectives or RFI?
- What role will other BOS/combat operations play in the reconnaissance scheme?
  - FS (to include EA and SEAD for air insertions/extractions).
  - Air defense.
  - Mobility/counter-mobility.
  - CSS.
  - Deception.
  - OPSEC.
- How will this RCOA—
  - Maintain focus on the reconnaissance effort?
  - Gain and **maintain** contact with reconnaissance targets?
  - Provide early warning?
- How will we ensure that reconnaissance operations remain the bde/TF initial main effort?

Table 4-4. Mission planning sequence (continued) .

- What is the reconnaissance force's relationship with security force?
- How far forward will we conduct reconnaissance? Is there a force in front of us? What are the control measures?
- How will fire support be integrated into this RCOA?

■ Determine Task Organization, C^2 Relationships. Once the reconnaissance force and its associated equipment are determined, it must be task organized to accomplish the RCOA in the most efficient manner. The C^2 structure must address unity of effort by identifying the COR. **The COR must have the control structure and authority to direct the reconnaissance force.** Reconnaissance operations often take place over large distances and long periods of time where communications systems are subject to attack. The communications plan will require careful attention to the use of retransmitted teams and redundant systems.

■ Identify Control Measures. While reconnaissance operations require the same positive control measures as any other, some require special attention.
- LOA. This measure identifies the forward edge of the reconnaissance battlespace and is usually associated with a CFL or FSCL.
- BHL. Reconnaissance forces operate throughout the unit's AO, but must be able to coordinate the acceptance of reconnaissance targets entering their battlespace with the unit to their front.
- TF Forward Boundary. In brigade operations there will often be a need to identify a brigade zone forward of the subordinate maneuver TFs.

■ Determine CSS Requirements:
- Resupply: How often, by whom, where, how?
- CasEvac: By whom, how?
- Reconstitution: From where will reconstituted reconnaissance forces come? What are the priorities?

RCOA Analysis and Wargaming

■ Key Events to Wargame During Analysis of an RCOA:
- Infiltration or penetration of the enemy security force.
- Insertion/extraction methods.
- Backup communications plan.
- CasEvac operations.
- Change in reconnaissance objectives based on new information.
- Handover of reconnaissance target leaving reconnaissance unit's LOS or AO.

R&S Ten Keys To Success

1. Commander's intent and **CCIR** drive R&S.
2. Support **R&S** early with integrated staff products.
3. Be adept at abbreviated **IPB** for **Quick** or **Combat Decision Making Process.**
4. S2 focus on the event template to capture the moving enemy.
5. S2 then provides **situation template,** depicting enemy in the engagement area.
6. Use automation tools like **ASAS** to enhance products.
7. Deploy organic R&S assets early and request support from higher. Issue S3 **FRAGO** with S2 graphic overlay.
8. Provide continuous coverage throughout the depth of the battlefield.
9. Use all possible assets from national level to scouts.
10. Evaluate reporting and provide **immediate and continuous feedback** to the commander.

APPENDIX A

UNIT INTELLIGENCE TRAINING CHECKLIST

This checklist will help a newly assigned brigade or battalion S2 maintain technical and tactical intelligence proficiency. Its building-block approach is systematic. The phases are supported by tasks to be completed for certification during the time specified. Some tasks may not apply to a particular echelon of staff.

PHASE I - ORIENTATION PHASE

This phase covers basic orientation to the division and the unit's mission. **This phase should be completed within the first 30 days** . The goal is to quickly acquaint the S2 with an understanding of the battalion, brigade, and division roles within corps, possible missions, and deployment areas.

Initial/Date	Task
_____	Coordinate with and receive briefing from outgoing S2.
_____	Review unit's intelligence library of publications listed in Appendix J.
_____	Read unit METL and latest training brief to determine overall unit missions and status.
_____	Receive unit CDR in-brief.
_____	Talk with unit CDR; ask what are his desires for intelligence and intelligence products. Tailor intelligence to the needs of the CDR.
_____	Visit and receive briefing from ACofS G2, Deputy G2, G2 Operations Chief, G2 Plans Chief, G2 Training Chief.
_____	Meet with subordinate S2's and gain an understanding of—
_____	● Their commander's intelligence priorities.

- Personnel and equipment status.
- Training proficiencies and deficiencies.
- Areas where they need your echelon's help.

Visit MI battalion or DS MI Co commander for unit and equipment briefings, display, and demonstrations.

Study division, brigade, and battalion OPLANs.

Review and evaluate intelligence annex to unit SOPs. (Use FM 34-1, FM 101-5, your SOP, and intelligence annex to the division SOP.) Provide CDR an updated evaluation of the unit intelligence annexes. Develop an SOP if one is missing or outdated.

Receive an organizational and functional briefing from the next higher G2/S2.

Study the CDR's current PIR and IR as developed.

Meet and discuss intelligence missions, products, and training with the—

- Scout platoon leader.
- GSR platoon leader.
- Local division CI team.
- ACT.
- ACE Chief, IPS Chief, and CM Chief.
- EWO.
- Terrain detachment team.

Determine all organic or assigned division intelligence collection assets that may support collection efforts. (See Appendix G.)

Learn to use section's automation equipment and programs.

_____ Learn the connectivity, reporting, and requesting procedures.

_____ Meet with next higher echelon G2/S2 to discuss the CM process.

_____ Review unit's collection plan.

_____ Become knowledgeable of the unit's and division's FSOP, RSOP, and deployment procedures.

_____ Read unit and division history.

_____ Obtain SI access through the SSO and review SCI billets for unit.

_____ Review unit's arms room security SOP.

_____ Inventory all sensitive items in one company.

_____ Review key control program SOP.

_____ Review physical security and crime prevention SOP.

_____ Receive a crime prevention and physical security program briefing from the MP and Directorate of Security.

_____ Become familiar with the S2 section vehicles and generators, as necessary.

_____ Become familiar with the TOC SOP, setup, and multisystem, multiechelon connectivity.

_____ Visit G2 training for intelligence training products.

_____ Test an arms room’s J-SIIDS.

_____ Visit unit staff sections and attached sections from other units (FSO, ADA, NBC, SOCCE, and ENGR).

_____ Develop and implement a detailed internal security inspection program that covers intelligence areas within the unit.

_____ Develop working relationship with higher echelon G2/S2.

_____ Review mission and section METL and battle tasks. Have section members give their assessment of current training level.

PHASE II - FUNDAMENTAL PHASE

This is the most critical phase for the newly assigned S2. The knowledge, insight, and assessments of I&S will establish the foundation for future development. This phase focuses on the IPB process, intelligence production and dissemination, collection operations, and security. **This phase should be completed within 90 days** .

Initial/Date **Task**

_____ Present to unit personnel an officer professional development class on the threat.

_____ Update unit's collection plan as needed; submit revisions to the CDR and forward a copy to higher HQ G2/S2.

_____ Brief the CDR on division and corps IEW assets.

_____ Brief next lower units on division and corps IEW assets.

_____ Inspect unit map program. Identify basic map load and training requirements.

_____ Inspect and evaluate unit training for intelligence tasks, including awareness of AR 381-10.

_____ Determine country and area study requirements from open and classified sources based on contingency and assigned OPLANs.

_____ Begin country studies.

_____ Understand additional duty responsibilities as required:

_____ ● Security manager.
_____ ● Physical security officer.
_____ ● Personnel security officer.
_____ ● Crime prevention officer.
_____ ● Key custodian.
_____ ● Top secret document custodian.
_____ ● Information systems security officer.

_____ Receive briefing and training from unit SIGO on communications procedures and communications equipment PMCS.

_____ Become familiar with capabilities, limitations, and vulnerabilities of unit's equipment (tanks, Bradleys, other assigned, attached, DS systems, or OPCON BOS operating in the unit's battlespace; particularly the TA and information dissemination capabilities).

_____ Update, as needed, the unit's—

_____ ● Arms room SOP.
_____ ● Physical security SOP.
_____ ● Key control SOP.
_____ ● Crime prevention program.

_____ Conduct random unannounced security spot checks. Report the results and any recommendations to the CDR.

_____ Brief CDR on the unit's intelligence estimate.

_____ Brief CDR on the intelligence collection and reporting system from platoon through corps.

_____ Develop, update, and evaluate an S2 section METL and battle tasks.

_____ Be knowledgeable on CTC threat vehicles, E-O devices, doctrine, and tactics. Teach a class on this subject at least once in this phase.

_____ Visit nearest battle simulation center and become familiar with computer operations.

_____ Visit and observe training of primary weapon systems in the division.

_____ Understand current division policy on CONUS and OCONUS transportation of classified material.

_____ Work with commanders. Ask what intelligence they want during FTXs and OPORD briefings.

_____ Know how to read a TACFIRE direction system message. Let FSO know you want to receive these during FTXs and deployments.

_____ Work with FSO to develop and review unit targeting and BDA procedures.

_____ Know unit air LNO. Request BDA and in-flight reports that will bolster reporting.

_____ Obtain recent CTC and applicable CALL. Develop plan to correct any deficiencies.

_____ Obtain inspector general checklist and CIP checklists; conduct internal inspection on all S2 functional areas. Brief CDR on inspection results and solutions.

_____ Review language proficiency requirements; assist S3 in coordinating training. Retain list of unit's capabilities; include unpaid abilities.

_____ Conduct classified materials inventory; learn destruction and verification methods; review destruction and transfer SOPs.

_____ Constantly review clearance requirements, applications, and updates.

PHASE III - DEVELOPMENTAL PHASE

This phase will build and expand on the knowledge gained during Phase II. It will cover the same basic intelligence functions but in greater detail. **This phase should be completed within 180 days.**

Initial/Date	Task
_____	Fully understand the functions of the S2 at the unit's TOC and how S2 functions drive other TOC functions.
_____	Submit REDTRAIN requests through applicable higher S2 to G2 training, as required.
_____	Review threat OB holdings and files. Order update material as required.
_____	Determine available intelligence databases and actually "work the system" to obtain data in support of a CONPLAN. Brief CDR on the results.
_____	Identify gaps of information in battle books, OB holdings and files, and intelligence annexes. Submit RIIs to satisfy intelligence requirements.
_____	Identify S2 and intelligence weaknesses from the last EXEVAL and present a correction plan to the CDR.
_____	Evaluate intelligence training classes and provide written results to the CDR.
_____	Evaluate unit soldier's knowledge of intelligence training tasks and provide a written report to the CDR.
_____	Determine if all ADP systems are accredited. Brief CDR on steps needed to correct any problems.

_____ Demonstrate a thorough understanding of the intelligence reporting system during FTXs.

_____ Act as threat CDR during the wargaming process and TF rehearsals.

_____ Develop an internal S2 section intelligence cross-training program. Have section soldiers teach the classes.

_____ Determine unit's security posture during FTXs and recommend corrective actions to the CDR.

_____ Become familiar with and teach a class on doctrine, tactics, and current vehicles of a CONPLAN threat.

PHASE IV - ADVANCE PHASE

This phase will take the S2 who has mastered the intelligence fundamentals through **the first year,** during which the unit will have participated in the full annual training program.

Initial/Date **Task**

_____ Successfully complete an EXEVAL.

_____ Successfully deploy section and perform S2 operations during a CTC rotation.

_____ Successfully deploy section and perform S2 operations during a BCTP Warfighter Exercise.

_____ Qualify or familiarize yourself on all unit weapon systems.

_____ Update unit's intelligence annex as required.

_____ Research a classified intelligence topic that is relevant to the unit's mission and brief the CDR on the conclusion.

_____ Accurately predict threat actions during FTXs using IPB and all intelligence assets.

_____ Successfully integrate with higher echelon G2/S2.

APPENDIX B

INTELLIGENCE PREPARATION OF THE BATTLEFIELD PRODUCTS

This following examples of various overlays, templates, and matrices are constructed and used during the IPB process to enhance the battlespace visualization of the commander and staff. These samplings are not all-inclusive. Your products will be dictated by your mission statement, resources available to you, and the time allowed.

Figures B-1 through B-6 are terrain overlays. Figures B-7 through B-13 are templates and associated matrices. Figure B-14 is a sample of an ADA-tailored IPB.

The MCOO includes—

- **MCs** and **AAs** stated in terms of concealment and cover, size and deployment type of formation that can move along them (armored battalion in company wedge), speed the formation can reasonably achieve; dismounted, mounted, and aerial routes; trails and passes that will allow column movement if unopposed.

- **Obstacles** in terms of what they are an obstacle to.

- **Key terrain**.

- **Restricted terrain** in terms of what size force can deploy there and what mobility work could be done to "unrestrict" it.

- **Severely restricted** terrain in terms of what will allow a dismounted force to traverse it and at what speed.

- **IVLs**. Without a 1- or 5-meter resolution terrain product, IVLs will have to be determined by historical knowledge or ground reconnaissance.

- **Soils** and **weather analysis** that indicate trafficability and "dig-ability."

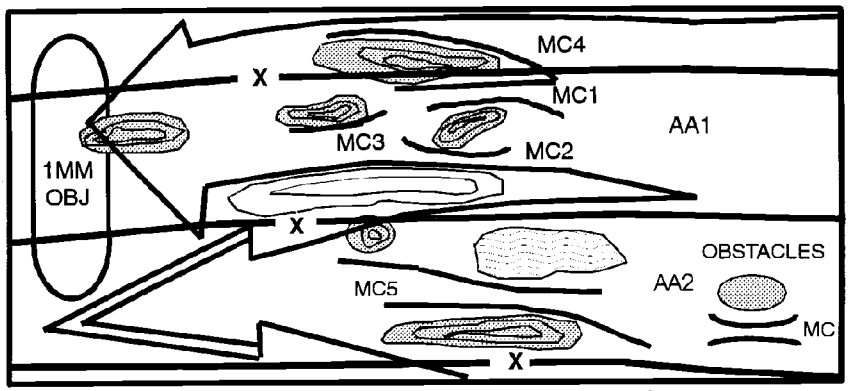


Figure B-1. Modified combined obstacles overlay.

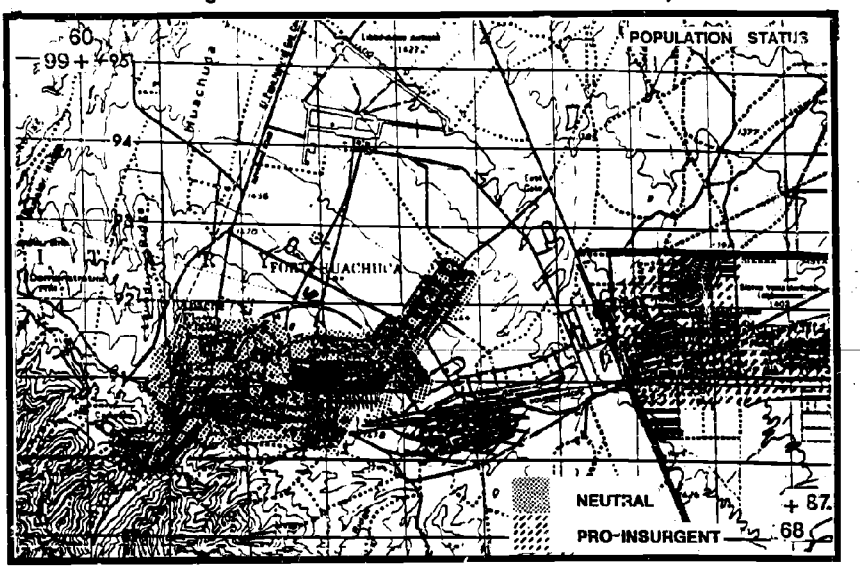


Figure B-2. Population status overlay.

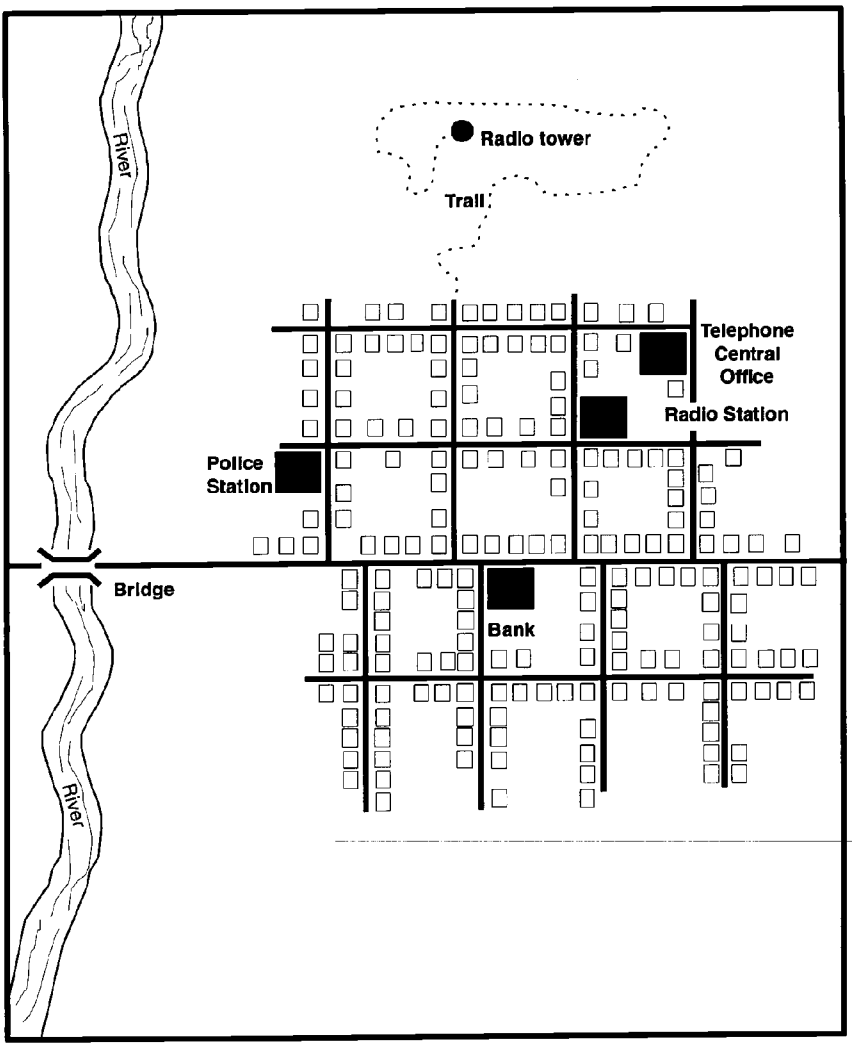


Figure B-3. Key facilities and target overlay.

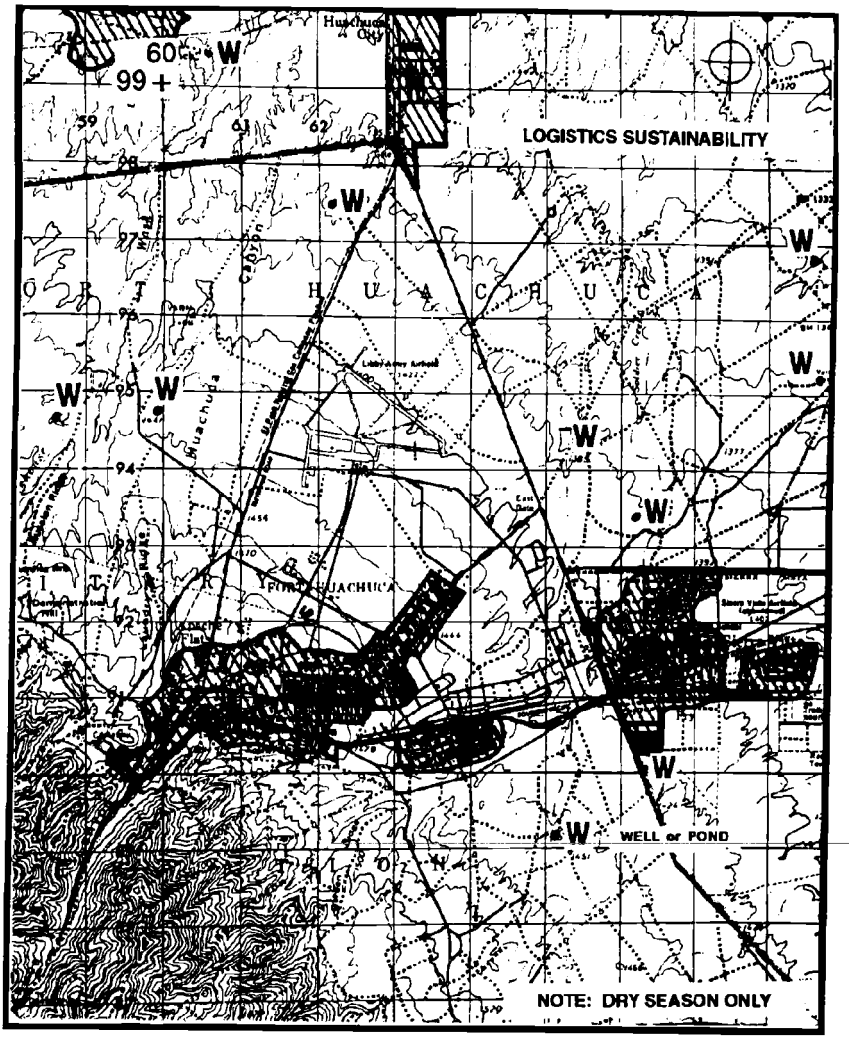


Figure B-4. Logistics sustainability overlay.

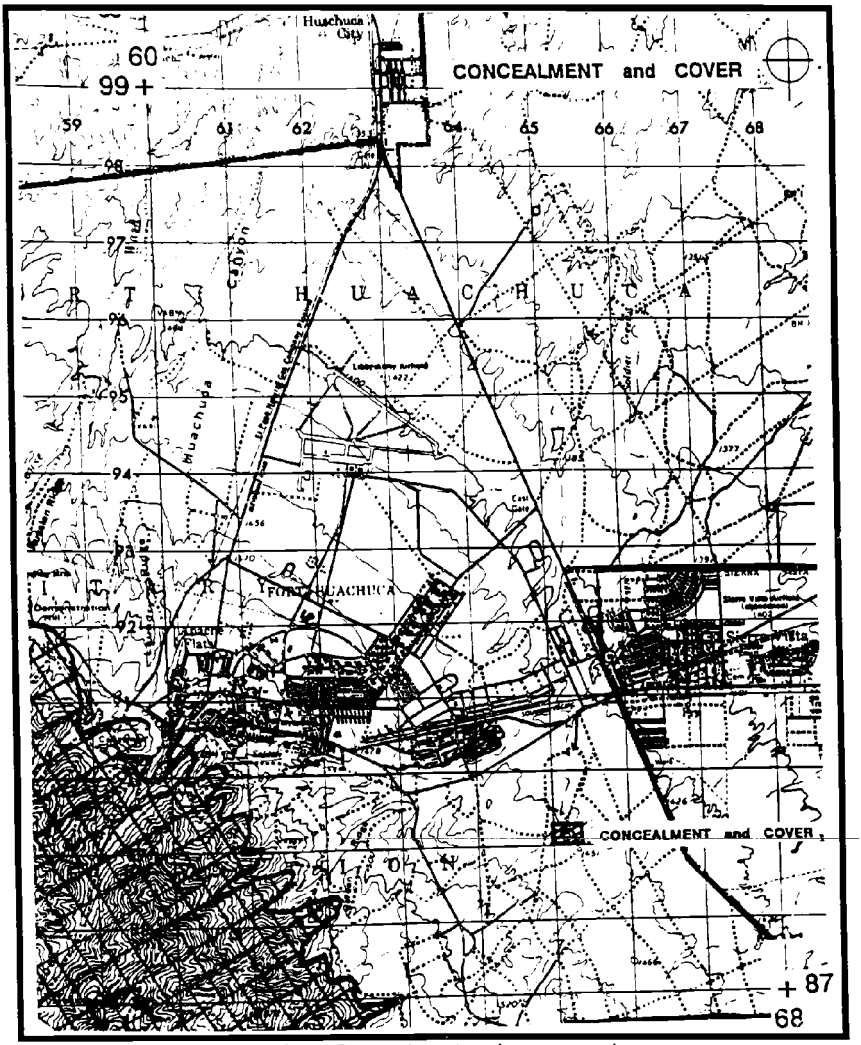


Figure B-5. Concealment and cover overlay.

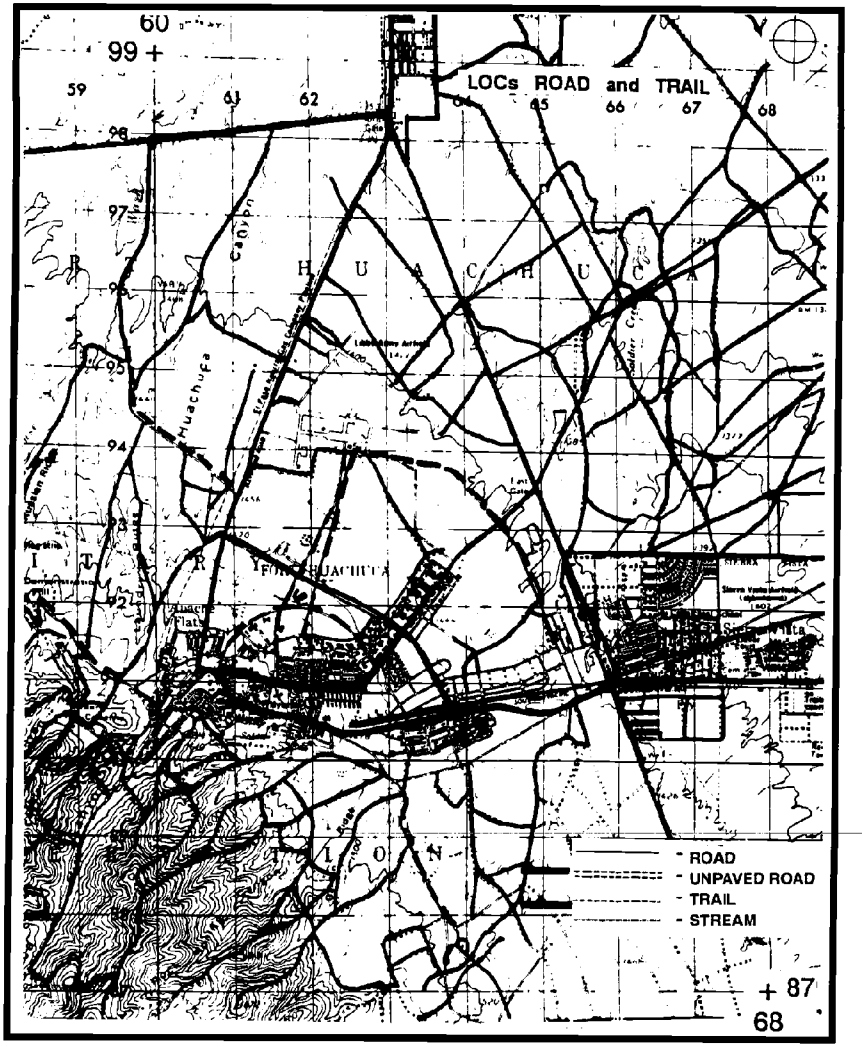


Figure B-6. Lines of communication overlay.

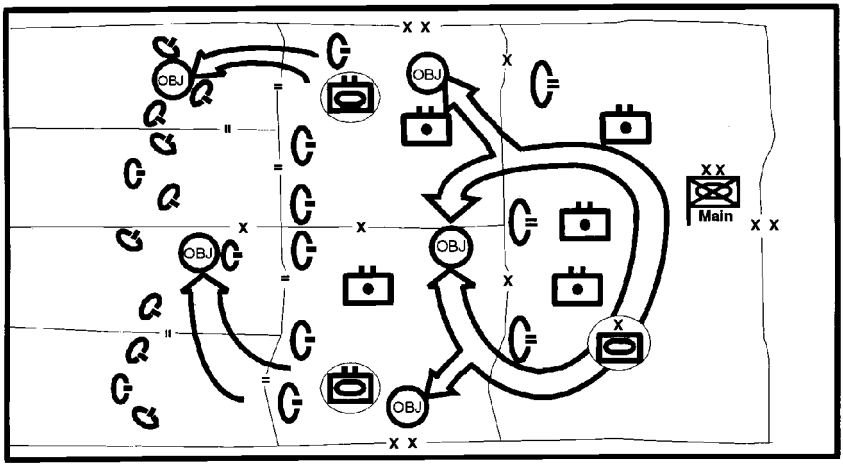


Figure B-7. Doctrinal template - depicts enemy forces according to doctrinal deployment, unconstrained by terrain.

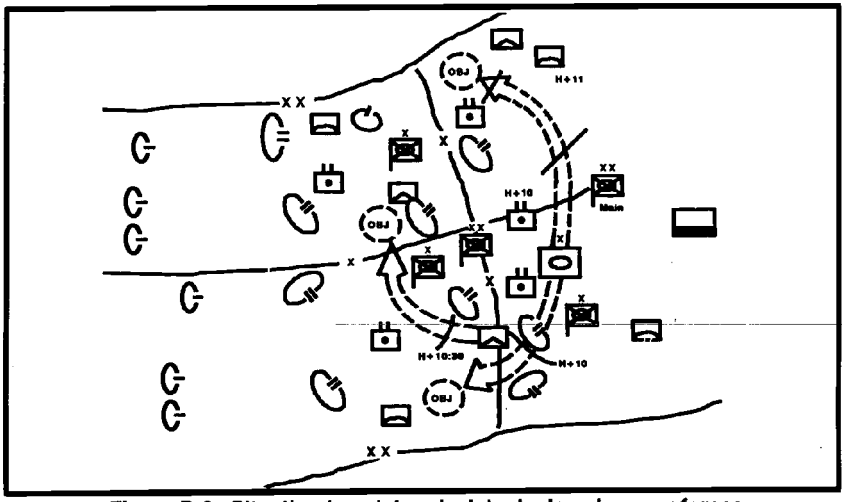


Figure B-8. Situation template - depicts deployed enemy forces adjusted for obstacles and terrain.

The situation template should include the following for mechanized armor-based offense and defense.

In the offense:	**In the defense:**
• Objectives & LOA. • AAs & MCs. • Recon routes, OP & IEW sites. • Firing lines & direct fire range fans. • Formations & deployment lines. • Artillery targets & range fans. • Artillery & ADA position areas. • ADA coverage. • Attack helicopter routes, BPs & range fans. • LZs. • CAS routes. • Situational obstacles. • Chemical agent targets. • Smoke targets	• BPs & direct fire range fans. • Reserve & hide positions. • CATK routes & firing lines. • Counter-SOPs & counterrecon forces. • Recon routes, OP & IEW sites. • Ambush sites. • Artillery targets & range fans. • Artillery & ADA position areas. • ADA coverage. • Attack helicopter routes, BPs & range fans. • Tactical & protective obstacles. • CAS routes. • Situational obstacles. • Chemical agent targets. • Smoke targets.

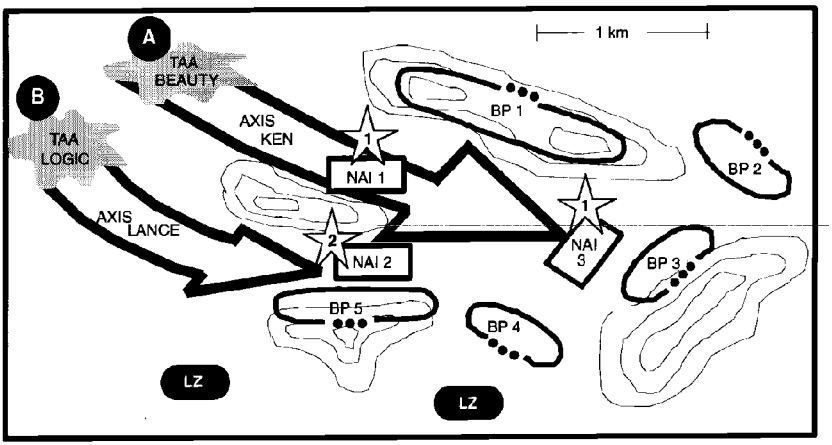


Figure B-9. Decision support template.

DP No.	1	2
Decision Criteria	Insurgent Camp is in NAI 1 or 3.	Insurgent Camp is in NAI 2.
Maneuver	A Co receives 3/B, occupy TAA BEAUTY, O/O movement to CATK along AXIS KEN.	A Co occupies TAA BEAUTY, O/O occupy BPs 1, 2, and 3.
FS	Priority: A, B, C.	Priority: C, B, A.
M-CM-S	1/A/13th Engr to A.	1/A/13th Engr to C.

Figure B-10. Partial BOS synchronization matrix.

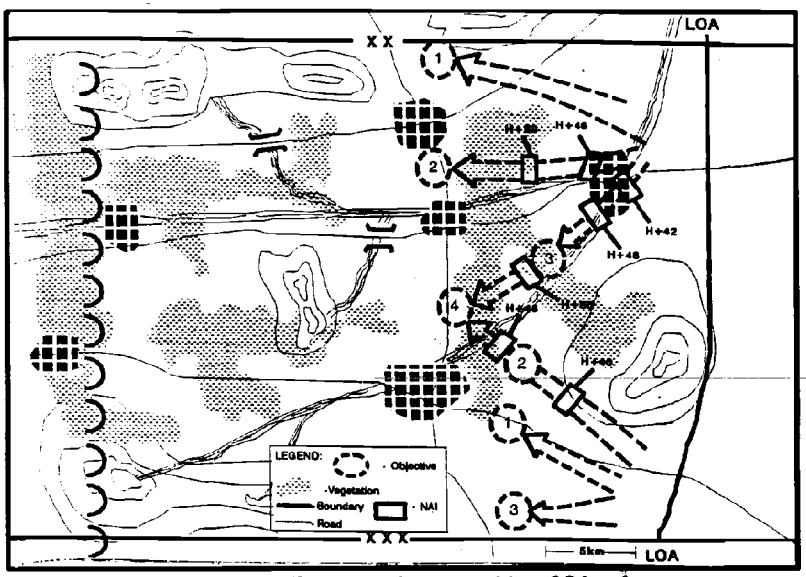


Figure B-11. Event template - considers COAs of reinforcing or counterattacking forces.

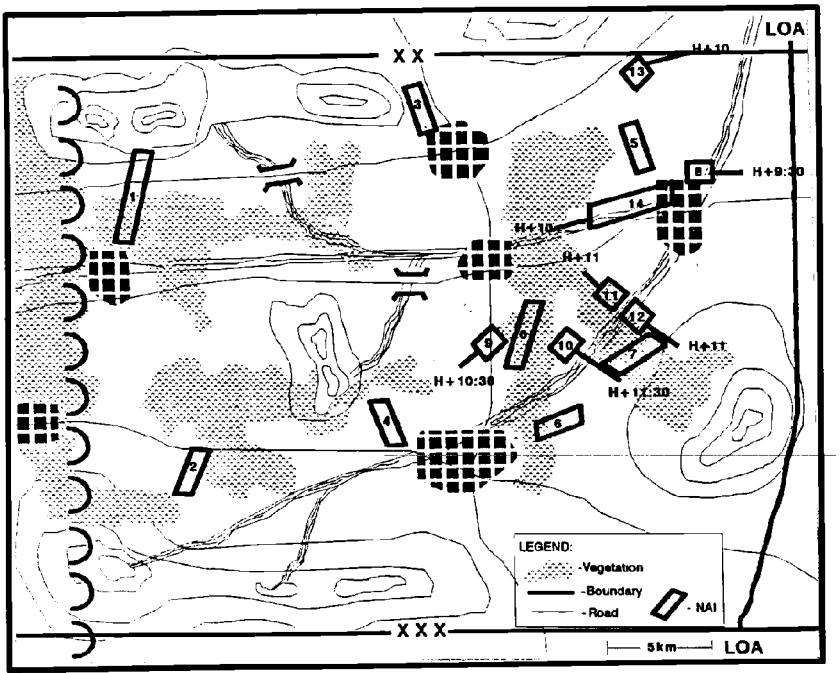


Figure B-12. Event template - depicts key events in each threat COA.

NAI	EST TIME	INDICATORS THAT WOULD HELP CONFIRM COA 1	COA 2	COA 3	OTHER
1	H-15		AASLT Forces		
2	H-15		AASLT Forces		
3	H-15	AASLT Forces		ASSLT Forces	
4	H-15		Infil of LT Inf		
5	H-4		LT Inf ATK NAI 5		
6	H-4	LT Inf ATK NAI 7	LT Inf ATK NAI 6		
7	H-4	LT Inf ATK NAI 8		LT Inf ATK NAI 7	
8	H-4	■Poised to ATK		LT Inf ATK NAI 8	
9	H-4	■Poised to ATK	■Poised to ATK		TD ATKs
10	H-4		■Poised to ATK	■Poised to ATK Abreast	TD ATKs
11	H-6			■Shifts N	
12	H-18				1 or 2 Bdes ATK N
13	H-18				1 or 2 Bdes ATK S
■ Indicates ECOAs.					

Figure B-13. Event matrix.

CONSIDERATIONS FOR AIR IPB

1. DEFINE THE BATTLEFIELD .

- AI for air IPB is significantly larger than ground IPB.
  - – Includes airfields which can range supported unit AO to include those within aerial refueling radius.
  - – AAAs which lead into supported unit's AO.
  - – Three types of air avenues:
    - * F/W Attack = Normally follows ground forces.
    - * F/W Transport = Bombers and R/W lift uses terrain to mask ingress and egress routes.
    - * R/W Attack = Normally follows ground forces.

2. DESCRIBE THE BATTLEFIELD'S EFFECTS . See the following example of weather effects on aviation operations.

TYPE AIR-CRAFT	MINIMUM VIS	WIND-SPEED & DIREC-TION[1]	PRECIPI-TATION	TEMPER-ATURE & HUMIDITY[2]	ILLUMI-NATION
Fixed Wing	2.5 nmi vis 2.5 nmi AGL ceiling in hilly terrain 1.0 nmi AGL in flat terrain	For airborne operations speed must be <13 knots	Severe weather within 3 miles of target will hinder acquisition. Freezing rain greatly limits lift capability	Temp >100 and humidity <80% will degrade payload capability	Little air-to-air or point CAS capability at night except newest F/W
Rotary Wing	1.0 nmi vis 300 ft AGL	For airmobile operations speed must be <13 knots	Same	Same	No CAS without illumina-tion except newest R/W

[1] Strong winds perpendicular to AAA increase difficulty in hitting target.
[2] Amount of degradation differs with type of aircraft.

Figure B-14. Sample of an ADA-tailored IPB.

- Terrain Analysis.
  - Determine impact of geographic factors on the ability of the aircraft to approach, acquire, and engage a target.
  - Predict how an aircraft would most likely approach target or area to deliver ordnance.
  - Locate positions that rotary wing could use for stand-off and/or pop-up attacks.
  - Determine locations of possible LZs, DZs, and the AAAs to these areas.
  - AAAs do not stop at FLOT or FEBA and they do not enter your AO solely from the FLOT or FEBA; watch your flanks and rear.
  - The closer an aircraft is to a target the greater an influence terrain will have on the aircraft and how it is employed.
  - The best method for formulating AAAs is based on fixed factors:
    * Locations of enemy airbase or staging area (known or suspected).
    * Position of friendly targets.
    * Most aircraft will fly a straight-in approach from the airbase to the vicinity of the target.

    Reason: Shorter overall mission time, less fuel needed, more payload or ordnance.
  - Exceptions which cause deviation from this rule:
    * Heavy concentrations of air defense.
    * Major terrain features that can mask the approach of aircraft at low altitudes.
    * Terrain that may force unnecessary exposure.
    * Terrain exceeding the operating ceiling of rotary-wing aircraft.
  - What happens in the vicinity of the target?
    * Most attacking aircraft will drop lower to use terrain masking and minimize early warning and exposure times to associated air defenses.
    * How will the enemy aircraft approach the target (Hi-Hi-Lo, Lo-Hi-Lo, or Lo-Lo-Hi, etc)?
    * To engage the target the pilot must be able to see it (visual, radar, sensor).
    * The pilot must approach his target so he can see it at far enough distance to allow lock-on and engagement by his weapon system.
    * The pilot will maximize his standoff range to increase survivability.
  - How to determine the direction of attack:
    * Know the enemy HPT; what friendly asset he must destroy.
    * Know the location of these assets.
    * Know the location of known or suspected enemy airbases and FARP.

Figure B-14. Sample of an ADA-tailored IPB (continued).

* Determine AAA which could be used by fixed- or rotary-wing aircraft making the attack.
* Determine locations from which stand-off and pop-up rotary-wing attacks are most likely.
* These locations will provide terrain masking for the aircraft to hide behind.
* The location must also provide observation and fields of fire into the target area when the aircraft pops-up.
* This type of location + a masked ingress and egress route = a stand-off or pop-up position.
* Within the vicinity of the target, consider the following:
  _ LOS acquisition of the target.
  – Weapon stand-off capability.
  – Pilot reaction time.
  – Aircraft survivability.
  – Standard tactics.

3. EVALUATE THE THREAT.

- Should address the following:
  – AOB—How many and what type aircraft. (Include different models such as Mi-24 E or F because they all have varying payloads, optics, and weapon systems.)
  – Capabilities of the aircraft in the enemy inventory.
  – Types of ordnance available to the enemy.
    * Guns.
    * Rockets.
    * Tactical ASMs, CBUs, PGM, AAM, NBC, and mines.
  – Capabilities:
    * Range.
    * Guidance (aerial, ground).
    * Release altitude.
  – Doctrine:
    * Raid sizes and composition.
    * Ingress and egress altitude and speed.
    * Delivery profiles.
    * Use of EP and SEAD.
  – C^2:
    * Most non-Western aircraft operate under strict ground control. They are vectored toward a target rather than being sent to an area to seek

Figure B-14. Sample of an ADA-tailored IPB (continued).

targets on their own. The vector is from ground emplaced beacons which normally operate in HF range.
- – Work to template high value C^2 targets:
  - * GCI nodes.
  - * FAC.
  - * RNP.
  - * Beacons.
- – Maintenance and Sortie Generation Capability:
  - * OR rates determine the percentage of aircraft able to fly. OR rate x number of aircraft = the maximum aircraft that can fly at any one time.
  - * The average sortie generation rate for most modern air forces is 2.5 to 3 for first 24-hour period. Second and succeeding day's planning factor is 5% of available number of aircraft.
  - * To get sortie generation rate: number of aircraft x sortie generation rate = number of sorties in a 24-hour period.
  - * To estimate number of sorties in your AO, consider ground situation, enemy main effort, enemy doctrine.

4. DETERMINE THREAT COURSES OF ACTION.

- Enemy air operations are conducted in support of their ground operations. The most important part of determining enemy air COAs is to understand the ground situation and enemy ground COAs.

- With the information and analysis you've done in the first three steps, determine how the enemy will employ his air assets.

- Consider enemy doctrine, AAAs, terrain in the target area, and current weather conditions.

- You must answer the following questions:
  - – When will the enemy commit his air assets?
  - – Where will the enemy commit his air assets (target area)?
  - – What air assets will the enemy commit (number of aircraft)?
  - – How will the aircraft attack in the target area (AAA or delivery profile)?

Figure B-14. Sample of an ADA-tailored IPB (continued).

APPENDIX C

RECONNAISSANCE AND SURVEILLANCE PLANNING

R&S planning is continuous. You must understand the commander's intent for each mission. After mission analysis, the commander should tell you the key information needed before and during the mission. This key information is the commander's PIR and IR. The PIR and IR provide the initial focus to R&S planning. Plan to conduct R&S throughout the depth of the battle in space and time. (See FM 34-2-1.)

G2/S2 R&S RESPONSIBILITIES (Table C-1)

Table C-1. G2/S2 R&S responsibilities.

REQUIREMENT	EFFECTS
Coordinate with higher, flank, forward units.	Better guidance from higher & integration with adjacent units; less redundancy & gaps in coverage.
Identify R&S requirements; rehearse R&S plan.	Success of unit mission.
Supervise & coordinate the command's aerial & ground reconnaissance (include LRRPs).	Better use of survl systems (GSR/REMBASS employment), LRRPs, and tasking UAVs or other aerial assets to answer CDR's PIR.
Brief GSR, REMBASS, and patrol team leaders (plt leaders of every BOS in AO to collect) (e.g., LLVI, LRSD, scouts).	Effectiveness of R&S assets which, in turn, affects success of R&S effort.
Prepare R&S WARNO and OPORD early-on.	Start the reconnaissance effort ASAP.
Update R&S OPORD as info is received.	Effectiveness of R&S effort and unit mission.
Provide R&S plan to higher, lower, and adjacent units.	R&S effectiveness and other unit actions; prevention of negative effects.

EXAMPLE: The primary R&S planning objective is to task subordinate units (all possible assets; e.g., MI, MP, FA, Signal, Engr, FSB) to cover NAIs important to brigade mission or directed by higher HQ. Subordinate units plan the use of available R&S assets to satisfy taskings from the brigade and their own requirements. They strive to complete their plans quickly (using the 1/3, 2/3 rule) so R&S assets have time to prepare and execute the plan. As soon as they are complete, the subordinate unit plans are consolidated at brigade to form the brigade R&S plan. You now have a draft plan that shows when and in what areas to begin R&S planning.

R&S PLANNING PROCESS (Figure C-1)

I. PLANNING PROCESS.

A. Initial Requirements:

1. Did higher HQ provide tasking requirements?
2. Was the commander's PIR and IR stated and included?
3. Did commander provide R&S intent?
4. Did S2 brief the staff on enemy collection capabilities?
5. Were other staff tasks performed?

B. SIR Developed (IPB Driven):

1. Did S2 identify air or ground AA?
2. Did situation and event templates reflect probable or prioritized ECOAs?
3. Was NAI developed in detail? (What is expected? When? Where?)
4. Were collectible indicators at NAIs developed?
5. Were SIR developed from NAIs and indicators?
6. Were reporting requirements developed for priority collection missions to allow the commander time to change plans?

C. Possible Collectors Analyzed:

1. Did S2 coordinate with staff, S2, and G2 to identify all available collection assets?
2. Did S2 analyze asset capabilities to develop collection requirements based on range to target, time available, target characteristics, terrain, weather, enemy (obscurant use), and communication?
3. Did S2 analyze collection redundancy (is it necessary)?

Figure C-1. R&S planning process.

4. Did staff identify support requirements (communication nets, retransmission, FS, NBC reconnaissance support, logistic support, special equipment support)?
5. Did S2 identify gaps in collection?
6. Did S2 back brief S3 or the commander on R&S concept?
7. Were WARNOs sent to appropriate assets?
8. What were timelines?
   a. When was mission received?
   b. What is NLT time for execution?
   c. When was templating done?
   d. When was tentative plan made? Back briefed?
   f. When was initial reporting needed?
   g. Who was in charge of R&D planning?
   h. Who was in charge of counterreconnaissance planning?
   i. What is LTIOV.

II. PREPARATION FOR R&S OPERATIONS.

A. Specific Collection Instructions:

1. What assets could be available? Used? **(See Figure C-4.)**
   a. Scouts.
   b. Patrols.
   c. Forward Observers.
   d. Armor.
   e. Aviation.
   f. Infantry.
   g. EW.
   h. REMBASS.
   i. Chemical.
   j. UAV.
   k. Medical.
   l. CI teams.
   m. GSR.
   n. OPs and LPs.
   o. Signal.
   p. Antitank.
   q. Engineer.
   r. Cavalry.
   s. MP.
   t. ADA.
   u. SOF.
   v. Support units.
   w. GRCS.
   x. Interrogation teams.

2. Did the S2 provide detailed instructions to tasked assets? Did the instructions include—
   a. Who is tasked?
   b. What to look for?
   c. Why to look?
   d. When to look?
   e. Where to look?
   f. What you could expect to see?
   g. How to get there?
   h. Who to coordinate with?

Figure C-1. R&S planning process (continued).

i. Passage of lines and recognition signals?
j. Reporting requirements?
k. Friendly assets in AO?
l. Resupply?
m. Obstacles?
n. MEDEVAC?
o. NBC hazards?

3. Was the collection location appropriate (concealment, collectable)?
4. Were there sufficient control measures included to control assets during mission?
5. Did the S2 request assistance from higher HQ for identified collection gaps?
6. Did the R&S plan cover all collection requirements?
7. Were assets overtasked?
8. Was redundancy appropriate for this mission?

B. Coordination:

1. What is format of plan (collection plan, overlay, matrix)?
2. Were direct or indirect fires or jamming coordinated between staff and S2?
3. Was a CI vulnerability assessment made?
4. Was additional equipment (special) planned for?
5. Were communication nets established to meet reporting needs?
6. Were commanders and staff briefed on plan before execution?
7. Did commander or S3 approve final plan?
8. Did assets know specific requirements (PIR and IR)?
9. Was plan disseminated to all involved or with a need to know (FRAGO, overlay)?
10. Was plan sent to higher HQ?

C. Asset Internal Coordination:

1. Was equipment checked?
2. Were internal procedures clarified?
3. Did coordination between assets occur?
4. Was mission rehearsed?
5. Was plan developed far enough in advance for assets to prepare or rehearse?
6. Was plan developed in time for higher HQ to review?

III. EXECUTION.

A. Continuity of R&S and counterreconnaissance operations:

Figure C-1. R&S planning process (continued).

1. Did unit plan provide for operations when scout or other R&S assets are inoperable?
2. Did unit SOP provide for operations during briefings, debriefings, or rehearsals?
3. Are unit and leaders cross-trained to facilitate substitutions or replacement of scouts?

B. Asset and Unit Response:

1. Did assets depart and set up on time?
2. Did assets use concealment, cover, and camouflage?
3. Were assets able to observe enemy undetected?
4. Was low-level deception used?
5. What were meteorological report requirements?
6. Were enemy locations pinpointed?
7. Was objective reconnoitered?
8. Were obstacles identified and marked?
9. Were routes marked?
10. Did assets submit route/obstacle overlay?
11. Was enemy reconnaissance located?
12. Were counterreconniassance missions performed?
13. Did assets help with C^2 during attack?
14. Did assets help direct or control fires?
15. Was terrain reconnoitered (trafficability reported)?

C. Reporting:

1. Were reports timely, accurate, and concise?
2. Were assets debriefed?

D. Results:

1. Did S2 plot asset reports (track results of plan)?
2. Did S2 identify inadequately tasked or unproductive assets and change tasking (with approval of commander and S3)?
3. Did reports or analysis answer PIR and IR?
4. Was R&S plan updated and recoordinated?
5. Were templates updated?

E. Dissemination:

1. Was commander briefed on answer to PIR?
2. Has commander updated PIR?
3. Did units get intelligence based on priority?
4. Did higher HQ get answers to taskings?
5. Did assets receive feedback on level of success?

Figure C-1. R&S planning process (continued).

OTHER R&S PLANNING CONSIDERATIONS (Figure C-2)

1. General.
   a. Combat information is knowledge of the enemy, weather, and terrain.
   b. R&S collection should answer the commander's PIR and IR.
   c. Every soldier is an important HUMINT collection asset.

2. Analysis of information collected on PIR and IR is an objective process.

3. Determine requirements:
   a. Set priorities. Develop SIR and SOR. Do not let the R&S elements decide what answers the commander's PIR.
   b. Terrain and weather.
   c. Tactical situation (deep, close, rear).
   d. Focus the R&S mission.

4. Develop R&S plan based on the principles of reconnaissance:
   a. Timely information.
   b. Aggressive reconnaissance.
   c. Continuous reconnaissance.
   d. Focus combat power.
   e. Relevant information (focused on PIR and CCIR).
   f. Reconnaissance OPSEC. Coordinate with G3/S3 to establish control measures which deconflict and help protect R&S assets on the battlefield.
   g. Accurate information.
   h. Complementary with operations.
   i. Consideration of threat counterreconnaissance threat.
   j. Destruction of threat reconnaissance elements when detected.
   k. Plan for CasEvac, resupply, and reconstitution for teams in the field.

5. Identify METT-T.

6. Develop communications plan and reporting schedule.

7. Issue WARNO to R&S asset leaders.

8. Coordinate R&S plan with—
   a. Commander and commanders of areas in which teams will operate.
   b. Adjacent and higher G2/S2.

Figure C-2. R&S planning considerations.

c. Unit S1/S3/S4.
d. FSO.
e. SIGO.
f. Engineer LNO.
g. ADA LNO.
h. Chemical Officer.
i. G3/S3 to tie R&S plan into the maneuver plan.

9. Brief R&S team leaders and all other R&S assets.

10. Advise higher and lower S2 of R&S plan.

11. Request support from higher headquarters.

12. Write R&S tasks into paragraph 3 of the OPORD.

13. Evaluate reports, review requirements, and identify intelligence gaps.

14. Analyze reports to deny or confirm your templates; then update templates.

15. Ensure combat information is passed immediately to those elements that can react to it.

16. Update the R&S plan based on known intelligence.

17. Plan for future operations.

18. Maximize use of all available assets.

Figure C-2. R&S planning considerations (continued).

You can now begin adding some detail to the R&S plan. Integrate any requirements from higher HQ. Translate the initial PIR and IR into indicators on which R&S assets can collect. Use the indicators to develop the SIR and SOR. The SIR and SOR ensure assets are collecting specific information that answers the PIR and IR.

Once you have a picture of the coverage required for the R&S effort, prioritize the SIR. Assign a high priority to those SIR that, when answered, will provide the greatest amount of intelligence in the shortest amount of time. After you prioritize the SIR, draft the R&S plan and distribute to the appropriate R&S assets. It is critical that you deploy R&S assets early-on and update them as additional information is received.

TOOLS TO TRACK DEPLOYED R&S ASSETS

Three methods are used to track deployed R&S assets:

- Reconnaissance base OPORD (Figure C-3).
- R&S overlay (Figure C-4).
- R&S tasking matrix (Figure C-5).

Select any method as long as the assets receive clear, specific instructions. Some S2s use all three methods by attaching the R&S overlay and R&S tasking matrix to the reconnaissance order prior to dissemination. When possible, using all three is best because each asset then has a graphic, a matrix, and a written set of instructions.

RECONNAISSANCE ORDER:

The reconnaissance order is the narrative instructions for deployed assets. Figure C-3 is an example of a brigade reconnaissance order.

RECONNAISSANCE ORDER

1. SITUATION.
   a. Enemy forces.
   b. Friendly forces.
   c. Attachments and detachments.
   d. Assumptions (OPLAN only).

2. MISSION. Expressed as task and purpose derived from planning process. Clearly stated reconnaissance objectives.

3. EXECUTION. Commander's intent, derived during planning process:

a. Concept of Operation. State how reconnaissance assets are operating in relation to the parent organization. This scheme must identify if the reconnaissance force is infiltrating or penetrating the enemy's security forces (or both) and how this will occur.

Figure C-3. Example of a brigade reconnaissance OPORD.

(1) Manuever.
(2) FS. (Refer to FS annex if required.)
(a) Scheme of fires that specifies what fires are available and how to get them.
(b) Engagement criteria.
(c) Scheduled fires in support of insertions and extractions.
(3) Mobility and survivability.
(4) Air defense.
(5) C^2W.

b. Tasks to maneuver units. [List all units from task organization into subparagraphs, and only unique items for those units; all other tasks go into d below.] For each of the elements in the reconnaissance force, state the following:
(1) How to get there.
(2) Where to look (NAI for static targets).
(3) What to look for.
(4) When to look for it.
(5) Plan to maintain contact with moving target.
(6) What equipment to bring.
(7) How (what communications systems, how often) to report.
(8) To whom to report:
(a) Brigade reconnaissance teams.
(b) Task forces.
(c) MI company (EW, UAV, other).
(d) ADA battery.
(e) Engineer battalion.
(f) FA battalion.
(g) Chemical company.
(h) MP platoon.
(i) Signal company.
(j) FSB.

c. Tasks to combat support units (if applicable).
(1) Fires (or refer to FS annex).
(a) Air support.
(b) Chemical support.
(c) FA support.
(2) Mobility and survivability. (Refer to mobility and survivability annex if required.)

Figure C-3. Example of a brigade reconnaissance OPORD (continued).

(3) Air defense. (Refer to air defense annex if required.)
(4) C^2W. (Refer to C^2W annex if required; address applicable subcomponents of C^2W: deception, EW, psychological warfare, UAVs.)

d. Coordinating instructions.
(1) Time or condition when OPORD or OPLAN becomes effective.
(2) EEFI.
(a) PIR.
(b) EEFI.
(c) FFIR.
(3) Risk reduction control measures.
(4) Environmental considerations.
(5) Any additional coordinating instructions.
(a) LD or defend NLT _____ .
(b) MOPP level.
(c) Rally points, alternate positions.
(d) Rehearsal time, type, location.
(e) Extraction plan.
(f) PZ and LZ.
(g) Fratricide avoidance measures.
(h) ROE and actions on contact.
(i) IHL.

4. SERVICE SUPPORT. State the concept of logistic support.
a. Support concept.
b. Material and services (resupply location or time and days of supply, emergency resupply, vehicle evacuation).
c. Medical evacuation (CasEvac plan).
d. Personnel (reconstitution plan).
e. Civil-military cooperation. NA.
f. Miscellaneous.

5. COMMAND AND SIGNAL.
a. Command (C^2 structure, report plan).
b. Signal (nets used, retransmission or relay plan).

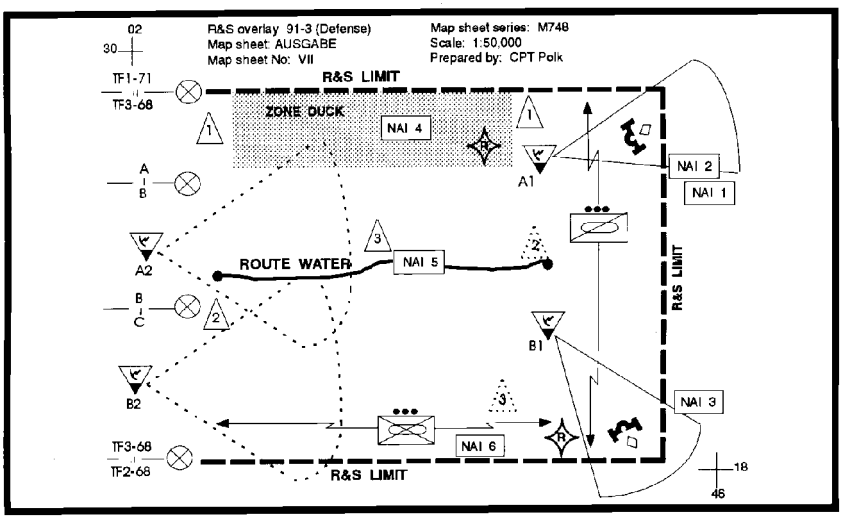
Figure C-3. Example of a brigade reconnaissance OPORD (continued) .

R&S OVERLAY:

The R&S overlay is the R&S plan in graphic format. Its purpose is to show exactly where and when R&S assets are operating. Use FM 101-5-1 for overlay graphics and symbols. Due to various R&S operational techniques and the unique nature of some SASO missions, you will need to construct some new graphics and explain them in your legend (Figure C-4).

The R&S overlay has two parts: (1) The graphic display of deployed or planned deployment of R&S assets, and (2) The marginal data consisting of the legend, administrative data, specific instructions to each asset, and the distribution list. The latter part consists of standard wording found on all overlays. (See top of Figure C-4.)

With digitized systems coming online, the location, heading, range to target, system health, and logistical data will be available NRT in digital, preformatted report format available to the S2/S3/S4 in the TOC, TAC, and ALOC.



INSTRUCTIONS:

SCOUTS: Establish forward screen NLT 1600 at coordinate_____. Target enemy recon (BRDM, BMP, tanks). Coordinate with B Co for route to screen position and GSR team.

REMBASS: Establish two strings vicinity____and____ NLT 1800. Target enemy dismount recon and MR troops infiltrating along forest trails. Coordinate passage with B Co, Scout platoon, and GSR team.

GSR: Establish position A1 vicinity____NLT 1700. Target enemy recon (BDRM, BMP, tanks, dismounted troops). Coordinate with A Co for passage, Scout platoon, and REMBASS team. Establish position A2 on order. Coordinate with B Co for position. Establish position B1 vicinity____ NLT 1700. Target enemy recon. Coordinate with B Co for passage, Scout platoon, and REMBASS team. Establish position B2 on order. Coordinate with C Co for position.

PATROLS: A Co conduct recon and security patrols in Zone Duck. Begin patrols NLT 1830 to 0600. Target enemy dismounted troops, BMP, and BRDMs. Coordinate with GSR team and Scout platoon. C Co establish screen along southern flank NLT 1800. Target enemy recon, BMP, BRDM, tanks. Coordinate with Scout platoon and GSR team.

OP/LP: Position as per battalion R&S SOP.

REPORTS: Report on battalion intelligence net using SALUTE format. Patrol leaders report on intelligence net after each patrol. Report combat information on intelligence or operations net. Assets report using schedule in R&S SOP. React to jamming as per battalion TAC SOP.

DISTRIBUTION: A, B, and C Companies, Scout platoon, GSR team, REMBASS team, S3, FSO, and brigade S2.

Figure C-4. R&S overlay with instructions on acetate.

The key portion of the administrative data contains the written instructions to each R&S asset. The instructions should focus on—

- The required operational timeframes. Give each asset a start and a finish time for each observation or action.

- The target. To answer the PIR, look for specific indicators. Each asset should be told exactly what to look for. Never give broad-based generic mission statements. Specific guidance will promote specific answers.

- Coordinating instructions. All assets at one time or another will move through or near another unit's AO. To keep units from shooting (directly or indirectly) friendly R&S assets, assets and units must coordinate with each other. FSO should restrict fires around R&S assets.

- Reporting requirements. All assets should know when, how often, and what format to use when reporting. Provide frequencies, alternate frequencies, and reactions during jamming, as well as the LTIOV for specific information to be reported.

Initially, the locations for assets are areas in which you recommend that they deploy. After the assets have deployed to the NAI, they report to the S2 or the S3 the actual coordinates from which they can best accomplish their mission. The S2 or the S3 then updates the R&S overlay graphics to show actual locations. Include the following control measures on your R&S overlay:

- Friendly boundaries, R&S limit of responsibility, NAIs, SPs, RPs, and checkpoints.

- Graphics depicting route, area, and zone reconnaissance.

- Primary, alternate, and supplementary positions.

- Sectors of scan for sensors.

R&S TASKING MATRIX:

Another less preferred method of disseminating R&S guidance is the matrix method (Figure C-5).

- **Priority.** The priority number of each mission, which should correspond with the PIR number.
- **NAI.** The NAI number and grid coordinate.
- **START/STOP.** The times for this mission.
- **SIR INSTRUCTIONS.** Explains to the assets exactly what they are looking for (target).
- **TASKINGS.** Lists the actual assets tasked to conduct each mission. An "X" placed under each asset identifies the tasking.
- **COORDINATION.** Tells the assets which units to coordinate with for this mission.
- **REPORTS.** Provides the assets with reporting requirements.

(Classification)

DTG: _____

MISSION: _____

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
PRIORITY	NAI	START / STOP	SI/INSTRUCTIONS	A	B	C	D			SCOUTS	MORTARS	GSR	REMBASS	OTHER	COORDINATION	REPORTS
1	1 2 3	1600 / 2400	When? Where? What type equipment does the recon element have? Do not Engage							X					With B Co for route to screen position. With GSR TM and REMBASS TM.	Per BN R&S SOP.

(Classification)

Figure C-5. R&S tasking matrix.

BRIEFING OPORDs

The following OPORDs are additions to the base reconnaissance OPORD (see Figure C-3). GSR, REMBASS, and patrol employment OPORDs would be issued to the teams by the respective platoon leaders.

GSR EMPLOYMENT:

- Give GSR teams adequate time to prepare and deploy.
- Deploy GSRs for best area coverage.
- Deploy GSRs, with a security force, so they scan an area and provide early warning.
- Plan logistical support.
- Limitations:
  - — Limited to LOS acquisition and gives off detectable signal.
  - — Visibility hindered by heavy precipitation, thick vegetation, and broken terrain.
  - — Limited range and ability to identify except by personnel and wheeled or tracked vehicles.

- Brief team leader using the OPORD format at Figure C-6.

1. SITUATION.

   a. Enemy. Intelligence estimate format.

   b. Friendly.
      (1) Current unit locations.
      (2) Scheme of maneuver.
      (3) Boundaries.
      (4) Objectives.

2. MISSION. Who, what, where, when, and why for this R&S mission. Surveillance of threat antiaircraft from location and time.

3. EXECUTION.

   a. Concept of operation.
      (1) Primary and alternate routes to sites (SPs, PPs, checkpoints, RPs).
      (2) Primary, alternate, and supplementary sites.
      (3) Sectors of scan.
      (4) Operating times.

   b. Coordinating instructions.
      (1) Battalion and brigade R&S plan: patrols, scout routes, times, sizes, LP and OP locations, ground and air cavalry screens, REMBASS, asset replacement plan, NAI redundancy coverage backup plan, etc.
      (2) Link-up plan with security forces.
      (3) Obtain target list from FSO (recommend additional targets).
      (4) Coordinate fire control measures with FSO and plan NFA for team locations.
      (5) Obtain obstacle plan from TF engineer and check routes for obstacles.
      (6) Coordinate with supported commander to tie the R&S site into unit defensive plan or scheme of maneuver.
      (7) Review engagement and disengagement criteria.
      (8) Review actions upon mission completion.

Figure C-6. Example of a GSR OPORD.

4. SERVICE SUPPORT. Coordinate with S4, battalion maintenance officer, SIGO for—

a. Class I (Food).
b. Class III (Fuel).
c. Class IV (Barrier materials) (during prepared defense).
d. Class V (Ammunition).
e. Class IX (Repair parts).
f. Organizational maintenance.

5. COMMAND AND SIGNAL.

a. Signal.
(1) Issue SOI extract.
(2) Review reporting requirements and communications connectivity.
(3) Identify multiple reporting paths and methods.
(4) Review communications check requirements.
(5) Execute COMMEX prior to employment.
(6) Review actions upon EA.

b. Command.
(1) Review chain of command.
(2) Review leaders' locations.

6. SAFETY.

Figure C-6. Example of a GSR OPORD (continued).

IREMBASS EMPLOYMENT:

Brief team leader using the reconnaissance OPORD format (see Figure C-3) with the changes shown in Figure C-7.

1. SITUATION.

2. MISSION. Who, what, where, when, and why for this R&S mission. Monitor NAIs, DPs, routes.

3. EXECUTION.

a. Concept of operation.
   (1) SIR required.
   (2) Team leader recommends sensor mix, emplacement sites, and relay sites.
   (3) Primary and alternate routes and transportation to emplacement sites, PPs, and checkpoints.
   (4) Emplacement method.

b. Coordinating instructions.
   (1) Battalion and brigade R&S plan: patrols, scout routes, times, sizes, LP and OP locations, ground and air cavalry screens, IREMBASS.
   (2) Link-up plan with security forces.
   (3) Obtain target list from FSO (recommend additional targets).
   (4) Coordinate fire control measures with FSO.
   (5) Obtain obstacle plan from TF engineer and check routes for obstacles.
   (6) Review engagement and disengagement criteria.
   (7) Actions upon mission completion.

Figure C-7. Sample IREMBASS employment OPORD.

PATROL EMPLOYMENT:

Brief patrol leader using reconnaissance OPORD format (see Figure C-3) with the changes shown in Figure C-8.

1. SITUATION.

2. MISSION.

3. EXECUTION.

   a. Concept of operation.
      (1) Maneuver.
      (2) Fire support.

   b. Subunit tasks.

   c. Coordinating instructions.
      (1) Actions at the objective.
      (2) Time of departure and return.
      (3) Movement techniques and order of movement.
      (4) Routes.
      (5) PPs.
      (6) RPs and actions at RPs.
      (7) Actions upon enemy contact.
      (8) Actions at danger areas.
      (9) Actions at halts.
      (10) Locations of friendly obstacles, mine fields.
      (11) Rehearsals and inspections.
      (12) Debriefings.
      (13) SIR.

Figure C-8. Sample patrol employment OPORD.

DEBRIEFING Debrief patrols using the sample debriefing format below.

1. Size and composition of team. Team leader, assistant team leader, radio operator, and observers.

2. Mission.

3. SIR.

4. Reporting requirements.

5. Time of departure, method of infiltration, and point of departure.

6. Enemy observed enroute.
   a. Ground activity.
   b. Air activity.
   c. Miscellaneous activity.

7. Routes.
   a. Dismounted.
   b. Vehicle.
   c. Air.

8. Terrain.
   a. Key terrain.
   b. Significant terrain.
   c. Decisive terrain.
   d. Terrain compartment.
   e. Terrain corridor.
   f. Map corrections.

9. Enemy forces and installations.

10. Miscellaneous information.
    a. Lack of animals or strange animal behavior. Did animal reaction to patrol's presence generate alarm? If so, when, where, type of animal, activity that caused the alarm, and nature of alarm.

Figure C-9. Sample debrief format.

b. Mutilated plants.
c. Strange, uncommon insects.
d. Abandoned military equipment, number and type.
(1) Out of fuel.
(2) Unserviceable; estimate reason.
(3) Destroyed or damaged; how.
(4) Operational equipment left intact.

e. Abandoned towns or villages.

11. Results of encounters with enemy forces and local populace.

12. Condition of team including disposition of dead and wounded.

13. All of team's maps or any other identifiable material returned with team. For missing items, describe item and approximate location lost.

14. Conclusions and recommendations.

15. Process CEE, CEM, photographs, and videos taken by teams.

16. Time of exfiltration, method of exfiltration, exfiltration point.

17. Routes of return.
a. Dismounted.
b. Flight.

18. Time of return.

19. Point of return.

20. Enemy observed on return route.

21. What pre-mission intelligence support was provided and not needed? What intelligence support was not provided but needed? What intelligence was provided but turned out to be misleading or erroneous?

Figure C-9. Sample debrief format (continued).

R&S TEN KEYS TO SUCCESS :

1. Know that the commander's intent or CCIR drives R&S.

2. Support R&S early with integrated staff products.

3. Be adept at abbreviated IPB for quick or combat decisionmaking process.

4. Focus on the event template to capture the moving enemy.

5. Provide situation template depicting enemy in the engagement area.

6. Use automation tools like ASAS to enhance products.

7. Deploy organic R&S assets early and request support from higher HQ. Issue S3 FRAGO with S2 graphic overlay.

8. Provide continuous coverage throughout the depth of the battlefield.

9. Use all possible assets from national levels to scouts.

10. Evaluate reporting and provide immediate and continuous feedback to the commander.

APPENDIX D

PRIORITY INTELLIGENCE REQUIREMENTS, INFORMATION REQUIREMENTS, AND INDICATORS

PIR are intelligence requirements associated with a decision that will affect the overall success of the command's mission. PIR may change in order or be replaced entirely.

IR are requirements for intelligence to fill a gap in the command's knowledge and understanding of the battlefield or threat forces. They target specific COAs.

Indicators are positive or negative evidence of threat activity or any AO characteristic which points toward threat vulnerabilities or adoption or rejection by the threat of a particular capability, or which may influence the commander's selection of a COA.

During wargaming, the S2 develops a set of PIR for each friendly COA. Each is linked to a specific enemy action that requires a friendly response (DPs).

PIR are those IR critical to accomplishing the mission. Wargaming will dictate which IR will become PIR as the mission runs its course.

The S2 should nominate PIR for approval ONLY FROM THE LIST OF ALREADY PLANNED AND COORDINATED IR.

EXAMPLE OF A POOR PIR:

"Will the enemy attack? If so, how, when, where, and in what strength?"

- The PIR contains five significantly different questions. Which one is the priority? Unless the S2 gives more guidance, the individual collector must determine which part of this PIR to work.

- The S2 probably knows more about the situation than "the enemy might attack somehow, sometime, somewhere, and in some strength." The PIR as stated might prompt some collection assets to collect known information.

- Even for issues that the S2 does not know, the enemy can only select from a limited range of COAs due, for example, to terrain, weather, policies. If the PIR consider IPB, the S2, through more specific tasking, will minimize the chance that collection assets will look for the enemy where they are not likely to be.

- When the staff wargames, it may find some aspects of this question to be irrelevant to the present situation. For example, the defense may be fully capable of defeating an enemy attack regardless of when they actually attack. Why waste collection assets on a question that does not need to be answered?

EXAMPLE OF A GOOD PIR:

There is no "set" of PIR we can present that will be useful for all tactical situations any more than there is a set of maneuver paragraphs that the S3 can plug into any OPORD. Below are examples of *types* of PIR the S2 presents to the commander for approval. Because intelligence needs change over time, most PIR will be important only during certain times.

Referring to PIR as "timephased" is redundant. They are dynamic just as the battle will be dynamic. Just as there are no standard situation templates or friendly COAs that will serve in all situations, there is no standard set of PIR. Good PIR, however, have some things in common:

- They ask only one question.
- They focus on a specific fact, event, or activity.
- They provide intelligence required to support a single decision.
- They are tied to key decisions that the commander has to make.
- They give an LTIOV.

Examples:

- "Will the enemy defend OBJ JAMES using a forward slope defense?"
- What size force is defending OBJ NACO?"
- Which bridges over the San Pedro River are intact?"

Not all PIR are appropriate as questions, particularly those associated with moving targets or formations. PIR are *requirements* and should be stated as such when appropriate. In addition, PIR for moving targets must include the requirement to continue to maintain contact with the target. Simply locating the target once will not prevent it from surprising the commander later.

Example: "Locate and track the enemy's battalion reserve."

APPENDIX E

GRAPHIC REPORT FORMATS

Intelligence personnel use a variety of formats to request, report, and disseminate information (see FM 34-3). Personnel working in a joint environment should use JCS Pub 6-04.11. The formats assimilate information into automated intelligence support systems, such as the ASAS.

This appendix concentrates on graphic report formats, specifically the graphic INTSUM and the graphic intelligence estimate. The INTSUM is the main focus, but a graphic intelligence estimate is also provided.

GRAPHIC INTELLIGENCE SUMMARY

The graphic INTSUM is used by units at all echelons to rapidly convey threat situation dynamics. The graphic INTSUM is a current depiction of significant threat dispositions, activities, strengths, and weaknesses and an assessment of the most probable ECOA. A current, complete graphic INTSUM will provide for efficient collection and enable the commander to exploit fleeting threat vulnerabilities.

The graphic INTSUM can be maintained on conventional maps of any scale as an overlay or created electronically and disseminated to computer and television screens. For example, army-level organizations may utilize a 1:250,000 map scale and focus on an army or front-level threat, whereas in SASO activities the deployed unit may utilize a map scale of 1:25,000 or smaller and focus on a platoon or company-size threat.

The graphic INTSUM (Figure E-1) may contain 12 components:

- Legend and margin information.
- Area orientation.
- Threat unit locations and mission activities.
- Threat mission capabilities assessment.
- Threat boundaries and front-line trace.
- Threat objectives.
- Threat air activity.
- Threat weaknesses and vulnerabilities.
- Threat strengths and capabilities.
- Threat intentions assessment.

- Friendly commander's intent and PIR.
- Predicted future threat activity.

LEGEND AND MARGIN INFORMATION:

Components include—

- Overall classification of the INTSUM, posted top and bottom, to include a "Classified By" line and declassification instructions.
- Title.
- Issuing headquarters.
- "As Of" DTG. Use either local or Zulu time; this is critical since predicted threat activity will be depicted based upon the "As Of" DTG plus a given number of hours.
- Map reference, to include scale, and at least two coordinate registration marks.
- A symbology key can be added for increased clarity and **must** be included if symbols used are not in FM 101-5-1.
- SASO symbology is not standardized, but there are several symbol methodologies that have been developed. (See MIPB Jan-Mar 94, p 35.)

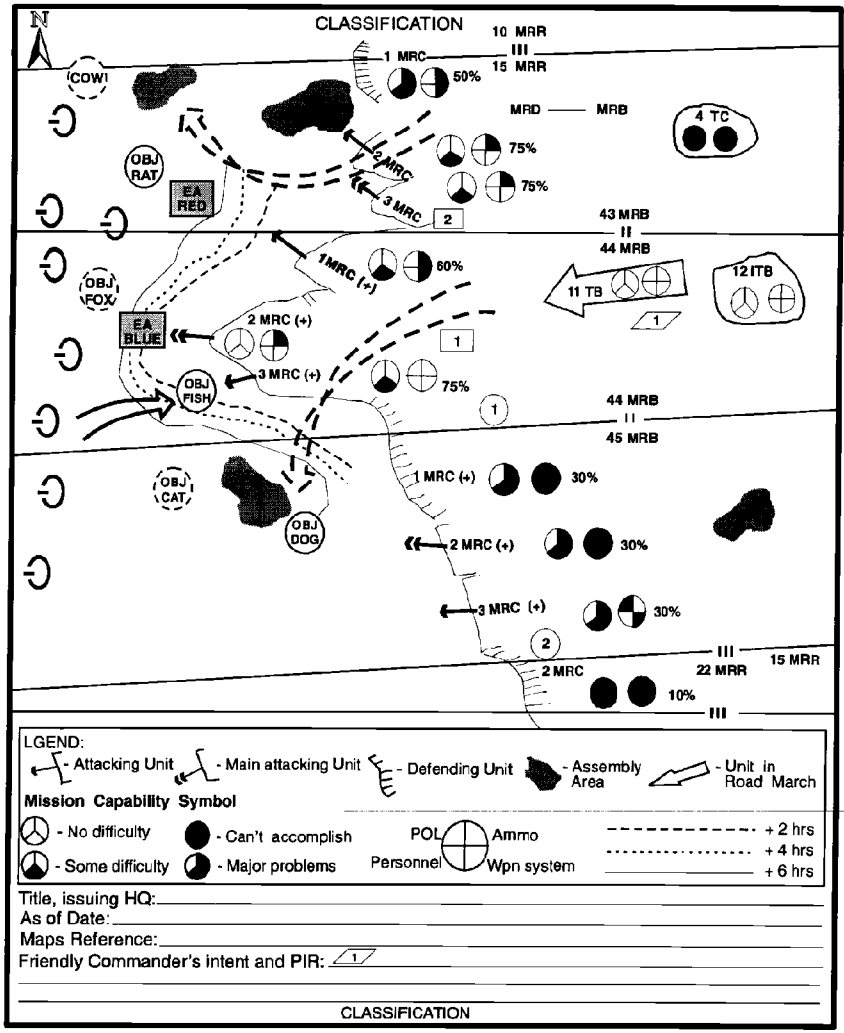


Figure E-1. Graphic INTSUM.

AREA ORIENTATION:

Selected geographic features will be highlighted on the overlay in order to orient the user to the area being displayed. The features selected will depend on the specific AO and type mission in which the friendly unit is involved.

Common features could include cities, rivers, and major relief features. Selected features for some SASO activities may be highlighted on a smaller scale. In an NEO highlighted features could include airports, LOCs, embassies, consulates, and American housing areas, and other features that will play prominently in the operation. Provide only the features necessary for orientation; do not clutter the INTSUM.

THREAT UNIT LOCATIONS AND MISSION ACTIVITIES :

Depict **committed** threat unit locations with a bracket followed by the unit identification. The size of the bracket will indicate the frontage occupied by the unit. The mission of the unit will be shown graphically (Figure E-2).

Depict **uncommitted** threat units with the symbology shown in Figure E-3.

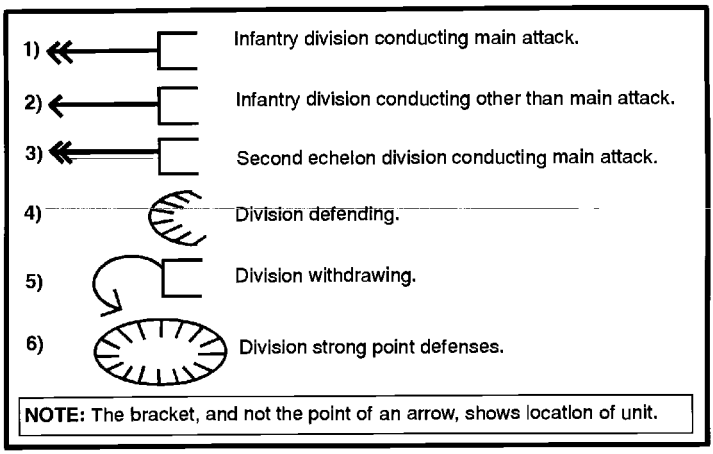


Figure E-2. Threat unit locations and mission activities (committed).

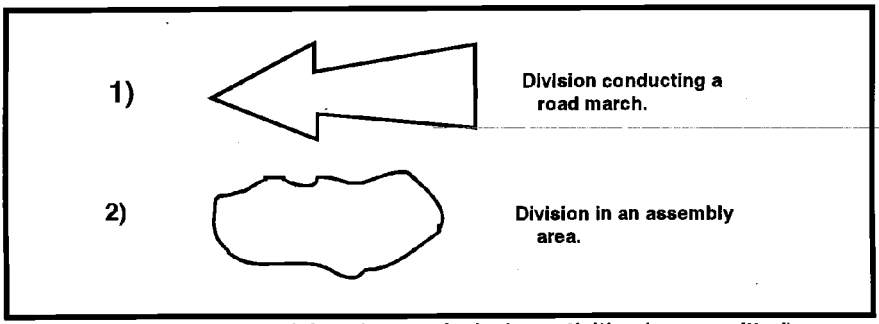


Figure E-3. Threat unit locations and mission activities (uncommitted).

THREAT MISSION CAPABILITIES ASSESSMENT :

Use combat effectiveness graphics to assess and display the capability of a threat unit to perform its mission. Consider all factors, tangible and intangible, in making the assessment; include unit strength, logistics status, maintenance and readiness status, morale, mission, weather, and terrain. Place selected symbols in the vicinity of the unit identification (Figure E-4).

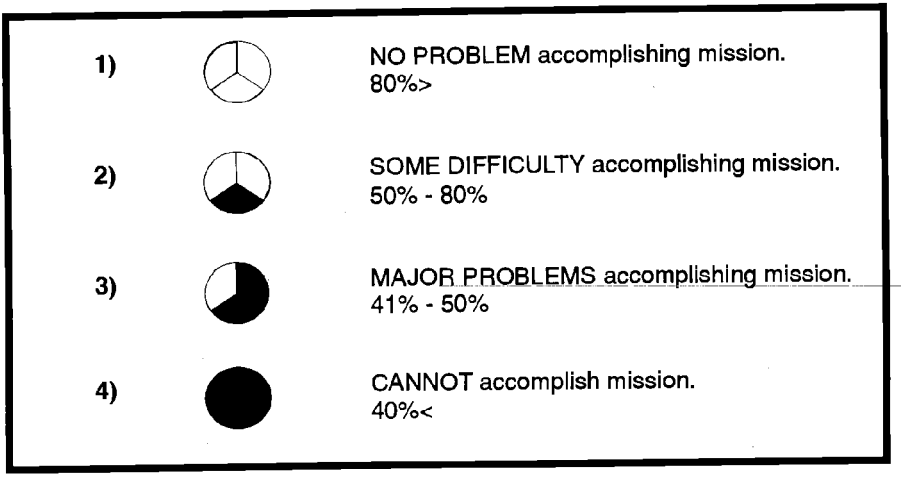


Figure E-4. Threat mission capabilities assessment.

A diminished threat mission capability is due usually to one or more specific problem areas such as damaged or destroyed weapons systems or a lack of ammunition, POL, or replacement personnel. If known, graphically depict these problem areas for each unit immediately next to the threat mission capabilities assessment symbol so the friendly commander can exploit what may be a very crucial, but fleeting, threat vulnerability.

Specific problem areas are indicated by blackening in the appropriate quadrant of the circle. The problem area categories are not static; other problem areas can be selected for display on this symbol as long as the selection is clearly explained in the key. Figure E-5 shows a sample problem area symbol and an example of the problem area symbol used in conjunction with the threat mission capabilities assessment symbol.

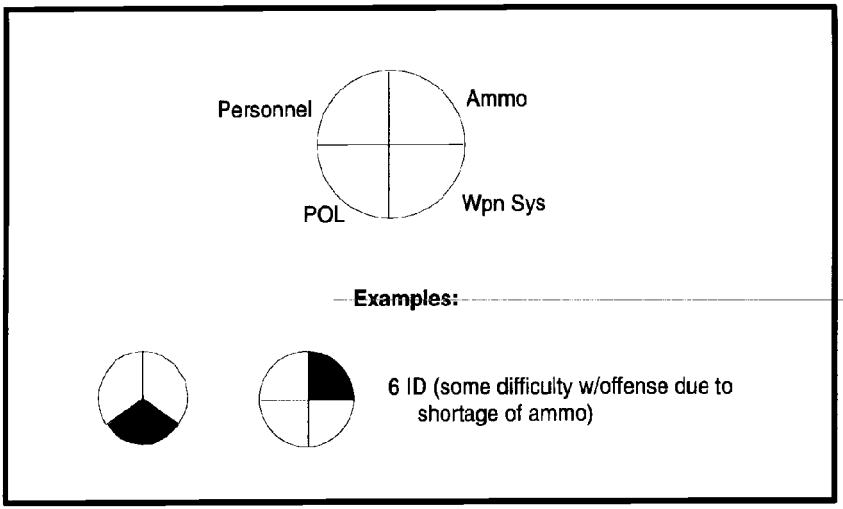


Figure E-5. Threat problem area symbology.

THREAT BOUNDARIES AND FRONT-LINE TRACE:

In conventional military operations, threat boundaries below the division level normally will not be included in the INTSUM. These lower level boundaries are often difficult to delineate and clutter the INTSUM. In some SASO activities, such as support to insurgency and COIN, smaller units will be the rule and must be constantly accounted for on the INTSUM.

The front-line trace will not be shown on the graphic INTSUM. The brackets depicting the frontages of the threat units in contact will suffice for an effective front-line trace. Addition of a front-line trace can be easily confused with the depictions of predicted threat activity.

THREAT OBJECTIVES:

If threat objectives can be discerned, they will be placed on the INTSUM.

THREAT AIR ACTIVITY :

Depict threat air activity on the INTSUM. Use an aircraft symbol with direction of travel and total number of sorties. Some units may opt to break down the sortie count by category, such as fighter (F), bomber (B), and reconnaissance (R). Example: A total sortie count of 12 could be depicted as (12). The same sortie count could also be depicted as (4F/6B/2R). The sortie breakdown should be used only if it will not clutter the INTSUM unnecessarily. Sortie breakdown symbols, such as F, B, and R must also be included (Figure E-6).

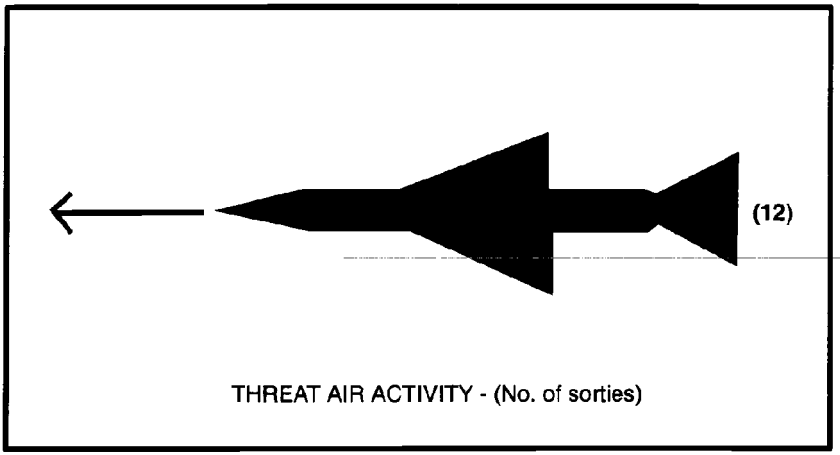


Figure E-6. Threat air activity symbology.

HREAT WEAKNESSES AND VULNERABILITIES:

Show specific weaknesses or vulnerabilities by using a numbered circle on the INTSUM (see Figure E-1). A supporting message could list threat weaknesses and vulnerabilities in narrative form.

THREAT STRENGTHS AND CAPABILITIES :

Show threat strengths and capabilities by using numbered squares (see Figure E-1).

THREAT INTENTIONS ASSESSMENT :

Write an assessment of threat intentions and most probable COA in a concise narrative format; graphically key it to the INTSUM when possible.

FRIENDLY COMMANDER'S INTENT AND PIR :

List the friendly commander's intent and PIR in narrative format on the INTSUM. Graphically key these statements to the overlay.

PREDICTED FUTURE THREAT ACTIVITY :

Draw predicted lines of threat advance or withdrawal and tie them to a timeline to convey as much information about future threat activity as possible (Figure E-7). Predicted lines of advance or withdrawal will be based on the "As Of" time found in the legend and margin information. Remember: Predicted lines are only an aid to planners; current threat situation must be continuously monitored to update the predictions.

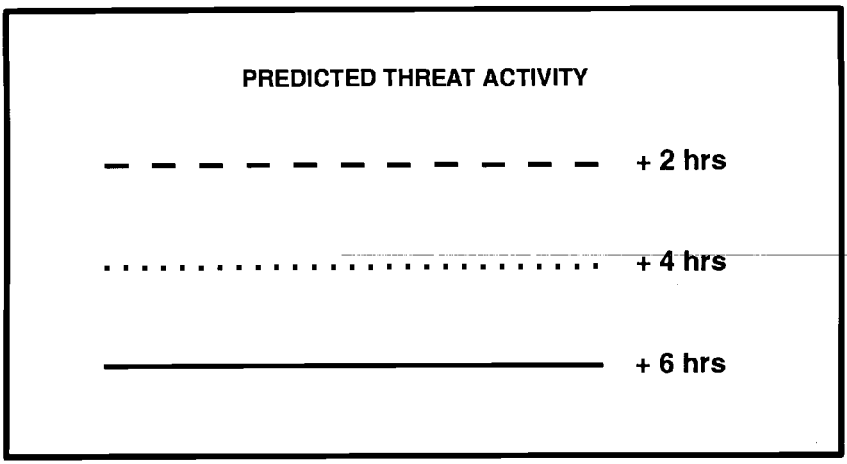


Figure E-7. Predicted threat activity timelines.

APPENDIX F

TARGETING

TARGETING PROCESS

Targeting is the process of selecting targets and matching the appropriate response to them, including operational requirements and capabilities. The purpose of targeting is to disrupt, delay, or limit threat interference with friendly COAs; it requires coordinated interaction between FS operations, intelligence, EW, and plans cells. Targeting is based on the enemy's assets that provide him an advantage (HPTs), friendly scheme of maneuver, and tactical plans. (See FM 6-20-10.)

Target development is one of the six IEW tasks. Mission analysis must precede generating any ECOAs. These ECOAs are the starting point for all other staff actions to wargame against, and to develop follow-on products. The products of the decide function are briefed to the commander. Upon his approval, his decisions are translated into the OPORD with annexes. (See FM 34-130.)

METHODOLOGY

Decisions create the guidelines for the acquisition and engagement of targets. TA and attack are made through a decision cycle. The methodology used to translate the commander's intent into a plan is **DECIDE, DETECT, DELIVER,** and **ASSESS.** Figure F-1 shows the functions of intelligence support to targeting, Figure F-2 shows the targeting methodology, and Figure F-3 is a targeting checklist.

RECEIVE GUIDANCE ON:	• Commander's intent. • HPTs. • Attack criteria. • Lead time between DPs and TAIs. • ROE. • Conditions to establish BDA requirements.
DEVELOP:	• MCOO. • Situation and event templates. • HVTs.
EXPLAIN:	• ECOA as part of wargaming. Based on friendly COA, refine event template; assist in developing HPT list, TSS matrix, and sensor or attack systems matrix.
PRODUCE:	• Collection plan, ISM, and AGM. • SOR.
BRIEF: (Ensure all analysts & collectors understand the CDR's intent.)	• ACE sections (ECOA, HPTL, TSS, and AGM).
COLLECT:	• Information for nomination, validation, and PSA.
DISSEMINATE:	• HPT related information and intelligence to FS immediately. • Pertinent information and BDA per SOP and TTP.
ENSURE:	• Information collection and intelligence production support all FRAGOs.

Figure F-1. Functions of intelligence support to targeting.

DECIDE	DETECT	DELIVER	ASSESS
• Target Development • TVA • HPT and HVT • TSS • Attack Options • Attack Guidance	• Target Detection Means • Detection Procedures • Target Tracking	• Attack • Planned Targets • Targets of Opportunity • Desired Effects • Attack Systems	• Tactical Level • Operational Level • Restrike • Feedback
Tracking your target is applicable during all of these steps.			

Figure F-2. Targeting methodology.

DECIDE:

_____ Do the commander's planning guidance and intent contain enough detail to enable the targeting team to determine—
- — HVTs to nominate as HPTs?
- — Desired effects on each HPT?
- — When to attack each HPT?
- — Any restrictions or constraints?
- — Which HPTs require BDA?

_____ What targeting assets (organic, attached, supporting) are available to detect and attach HPTs?

_____ What detect, deliver, and assess support is needed from higher HQ?

_____ When must requests to higher HQ be submitted to obtain the support when required?

_____ Have target tracking responsibilities been established?

_____ Are systems in place to handoff the detected targets to assets that are capable of tracking them?

_____ What detect, deliver, and assess support is required from subordinate units; when is it required?

Figure F-3. Targeting checklist.

_____ What detect, deliver, and assess support requests have been received from subordinate units; what has been done with them?

_____ Has the AGM been synchronized with the DST and the maneuver and FS plans?

_____ Are all commands using a common datum for locations? If not, are procedures in place to correct differences in data?

DETECT:

_____ Does the collection plan focus on PIR HPTs? (Which includes HPTs designated as PIR?)

_____ What accuracy, timeliness, and validity standards (TSS) are in effect for detection and delivery systems?

_____ Are all TA systems fully employed?

_____ Have backup TA systems been identified for HPTs?

_____ Have responsibilities been assigned to the appropriate unit and/or agency for detecting each HPT?

_____ Are HPTs being tracked?

_____ Have verification procedures using backup systems been established where necessary?

_____ Are TA and BDA requirements distributed properly among systems that can accomplish both?

DELIVER:

_____ Have communications links been established between detection systems, the decisionmaker, and delivery systems?

_____ Have responsibilities been assigned to the appropriate unit and/or agency for attacking each HPT?

_____ Has a backup attack system been identified for each critical HPT? (The primary system may not be available at the time the HPT is verified.)

_____ Have FSCMs or AGMs and clearance procedures been established to facilitate target engagement?

Figure F-3. Targeting checklist (continued).

_____ Have O/O FSCMs or AGMs been established to facilitate future and transition operations?

_____ Have potential fratricide situations been identified; have procedures been established to positively control each situation?

_____ Have responsibilities been assigned to the appropriate unit or agency for tracking specific HPTs and providing BDA on specified HPTs?

_____ What are the procedures to update the HPTL and synchronize the AGM and DST if it becomes necessary to change the scheme of maneuver and FS as the situation changes?

ASSESS:

_____ Are the collection assets linked to specific HPTs still available?

_____ Have the collection asset managers been notified of the attack of a target requiring assessment?

_____ Have assessment asset managers been updated as to the actual target location?

_____ Has all the coordination for the assessment mission, particularly airborne assets, been accomplished?

_____ What is the status of BDA collection?

_____ Has the information from the mission been delivered to the appropriate agency for evaluation?

_____ Has the targeting team reviewed the results of the attack to determine restrike requirements?

_____ Has the target intelligence gathered from the assessment been incorporated into the overall enemy situation development?

Figure F-3. Targeting checklist (continued).

STEP 1 - DECIDE:

DECIDE provides the overall focus and sets priorities for intelligence collection and attack planning (Figure F-4). Targeting priorities must be addressed for each phase or critical event of an operation. The decisions made are reflected in visual products as follows:

- HPTL is a prioritized list of HPTs whose loss to the enemy will contribute to the success of the friendly COA.

- Intelligence collection plan, or R&S plan, answers the commander's PIR, to include those HPTs designated as PIR. The plan, within the availability of additional collection assets, supports the acquisition of more HPTs. Determining the intelligence requirements is the first step in the CM process. (See FMs 34-2 and 34-2-1.)

- TSS matrix addresses accuracy or other specific criteria that must be met before targets can be attacked.

- AGM, approved by the commander, addresses which targets will be attacked, how, when, and the desired effects.

The formats for the HPTLs, TSS, and AGMs are examples only. Targeting personnel must understand all that is involved in building these targeting tools. However, experienced staffs may prefer to develop their own tailored formats.

IPB and Mission Analysis. IPB, including EPB, is a continuous process and starts in the preparation phase. It continues to provide updated as well as new products and supports the targeting process. The intelligence estimate provides key support to target development. MCOOs, doctrinal, situation, event, and DSTs help identify ECOAs, NAIs, TAIs, HVTs.

***TVA and Wargaming*.** The battlefield environment, its effects on combatants, and the threat are considered in IPB analysis to arrive at an intelligence estimate. TVA yields HVTs for a specific ECOA. Target spreadsheets identify the HVTs in relation to a type of operation, and target sheets (see FM 6-20-10, App A) give detailed targeting information for each HVT. This information is used during the IPB and the wargame processes. Both tools are developed by the G2 ASPS.

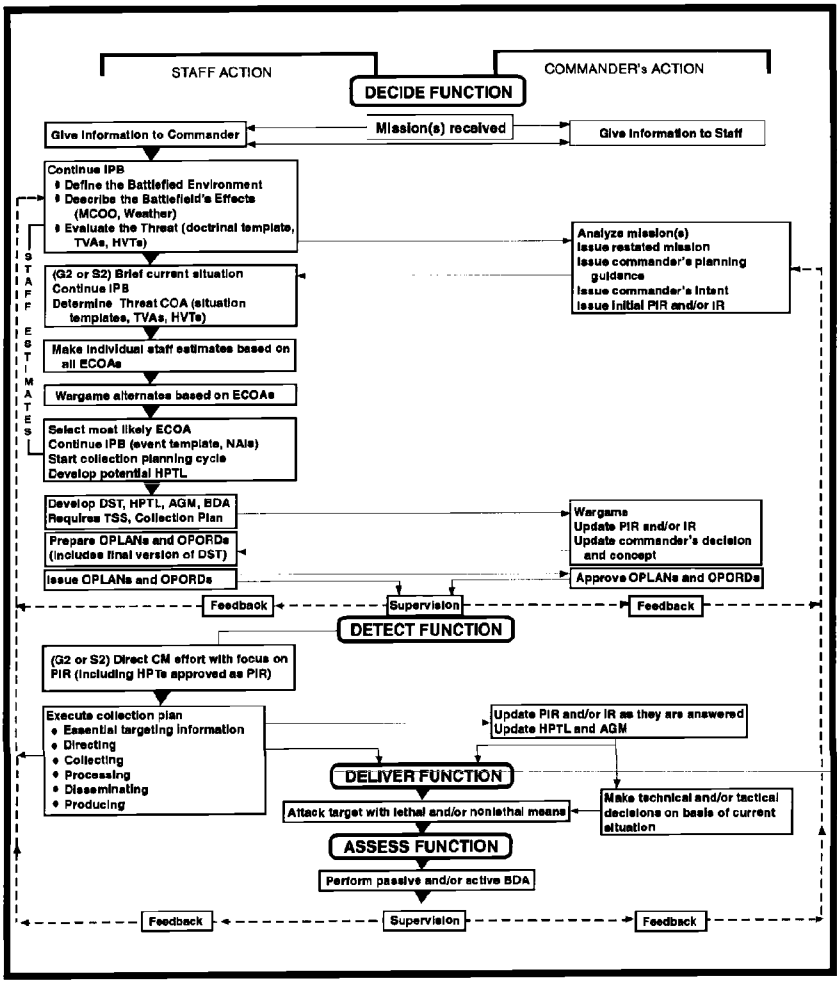


Figure F-4. The targeting process.

TVA, which is a detailed analysis of the enemy in selected COAs, uses the following enemy characteristics:

- Doctrine.
- Tactics.
- Equipment.
- Organizations.
- Expected behavior.

TVA methodology provides a relative ranking of target sets, or categories. It begins when target analysts in the G2/S2 assume the position of enemy commander. The target analyst, in coordination with other staff members, wargames the operation.

During wargaming, alternate friendly COAs are analyzed in terms of their impact on enemy operations and likely responses. The enemy battlefield functions that must be attacked to force the best enemy response are identified. The commander and staff analyze the criticality of friendly battlefield functions on a specific COA. The best places to attack HPTs are identified as TAIs. DPs or decision TPLs are used to ensure that the decision to engage or not to engage occurs at the proper time. Wargaming also identifies HVTs in priority that are critical to the success of the enemy mission. It also identifies the subset of HVTs which are HPTs that must be acquired and attacked for the friendly mission to succeed. HPTs selected are recorded on the DST.

Collection managers evaluate HVTs to determine asset detection capability. HPTs receive priority in the allocation of assets. The FSO determines friendly weapons systems capable of attacking HVTs with lethal fires, and the EWO nominates and coordinates to provide non-lethal fires.

Using the capabilities of the system to attack the targets, the G2/S2 analyzes and synthesizes the threat's response to each attack. Targets should be assigned priorities according to description, signature, degradation, and graphic representation. If targets have the same relative importance, a targeting team must prioritize the targets and seek advice from the FSE targeting analyst and the FAIO. After the targets are prioritized, they are placed on an HPTL (Figure F-5). After the HPTL is approved, the G2 will use it to develop the collection plan.

EVENT OR PHASE:		
PRIORITY	CATEGORY	TARGET

Figure F-5. Example high-payoff target list.

TSS. TSS are criteria applied to enemy activity (acquisitions and battlefield information) used in deciding whether the activity is a target. TSS break nominations into two categories: targets, which meet accuracy and timeliness requirements for attack; and suspected targets, which must be confirmed before any attack.

- HPT. This refers to the designated HPTs which the collection manager is tasked to acquire.
- TIMELINESS. Valid targets are reported to attack systems within the designated timeliness criteria.
- ACCURACY. Valid targets must be reported to the attack system meeting the required TLE criteria. The criteria is the least restrictive TLE considering the capabilities of available attack systems.

Considering these factors, different TSS may exist for a given enemy activity on the basis of different attack systems. For example, an enemy artillery battery may have a 150-meter TLE requirement for attack by cannon artillery and a 1 km requirement for attack helicopters. TSS are developed by the FSE in conjunction with MI personnel. Intelligence analysts use TSS to quickly determine targets from battlefield information and pass the targets to the FSE.

Attack system managers, such as FSEs, FCEs, or FDCs, use TSS to quickly identify targets for attack. Commands can develop *standard* TSS based on anticipated enemy OB and doctrine matched with the normally available attack systems.

The G2/S2 knows the accuracy of acquisition systems, associated TLE, and the expected dwell times of enemy targets. He can then specify whether

information he reports to the attack system manager is a target or a suspected target. Some situations may require the system to identify friendly and neutral from threat before approval to fire is given. HPTs that meet all the criteria should be tracked until they are attacked IAW the AGM. Location of targets that do not meet TSS should be confirmed before they are attacked. The TSS can be depicted in a TSS matrix (Figure F-6).

The matrix lists each system that forwards targets directly to the FSE, FCE, or FDC. The effects of weather and terrain on the collection assets and on enemy equipment are considered. TSS are keyed to the situation. However, the greatest emphasis is on the enemy situation considering deception and the reliability of the source or agency that is reporting.

HPT	TIMELINESS	ACCURACY
COPs	3 hr	150 m
RISTA	30 min	150 m
2S3	30 min	500 m
M-46	30 min	500 m
ADA	15 min	500 m
CPs	3 hr	500 m
Ammunition	6 hr	1 km
Maneuver	1 hr	150 m

Figure F-6. Example target selection standards matrix.

Attack Guidance. Knowing target vulnerabilities and the effect an attack will have on enemy operations allows a staff to propose the most efficient available attack option. Key guidance is whether the commander wishes to disrupt, delay, limit damage, or destroy the enemy. During wargaming, DPs linked to events, areas (NAIs and TAIs), or points on the battlefield are developed. These DPs cue the command decisions and staff actions where tactical decisions are needed.

On the basis of commander's guidance, the targeting team recommends how each target should be engaged in terms of the effects of fire and attack options to use. Effects of fire (see Joint Pub 1-02) can be to **harass, suppress, neutralize,**

or **destroy** the target. The subjective nature of what is meant by these terms means the commander must ensure the targeting team understands his use of them. Applying FS automation system default values further complicates this understanding.

- Harassing fire is designed to disturb the rest of the enemy troops, to curtail movement, and, by threat of losses, to lower morale. The decision to employ harassing fires needs careful consideration. Harassing fire has little real effect on the enemy, subjects gun crews to an additional workload, and increases the threat of counter-battery fires. ROE or the potential for adverse public opinion may prohibit its use. However, harassing fires may be a combat multiplier in some situations. Consider their use in SASO, delaying actions, and economy of force operations.

- Suppressive fire on or about a weapons system degrades its performance below the level needed to fulfill its mission objectives. Suppression lasts only as long as the fires continue. The duration of suppressive fires is either specified in the call for fire or established by SOP. Suppression is used to prevent effective fire on friendly forces. It is typically used to support a specified movement of forces. The FSCOORD needs to ask or calculate the *when* and *how long* questions.

- Neutralization fire is delivered to render the target ineffective or unusable temporarily. Neutralization fire results in enemy personnel or material becoming incapable of interfering with an operation or COA. Key questions the FSCOORD must ask are when and how long does the commander want the target to be neutralized. Most planned missions are neutralization fires.

- Destruction fire is delivered for the sole purpose of destroying material objects. It physically renders the target permanently combat-ineffective unless it is restored, reconstituted, or rebuilt. Setting automated FS default values for destruction of 30 percent does not guarantee achieving the commander's intent. The surviving 70 percent may still influence the operation. Destruction missions are expensive in terms of time and material. **Consider whether neutralization or suppression may be more efficient.**

The decision of what attack system to use is made at the same time as the decision on when to acquire and attack the target. Coordination is required when deciding to attack with two different means (such as EW and combat air operations). Coordination requirements are recorded during the wargame process.

The attack guidance must be approved by the commander and detail the following:

- A prioritized list of HPTs.
- When, how, and desired effects of attack.
- Any special instructions.
- HPTs that require BDA.

This information is developed during the wargame. Attack guidance—

- Applies to planned targets and targets of opportunity.
- May address specific or general target descriptions.
- Is provided to attack system managers via the AGM (Figure F-7).
- May change as the operation progresses.

The AGM must be updated during staff planning meetings and as the enemy situation changes. Consider separate AGMs for each phase of an operation.

PHASE/EVENT: Attack through the security zone				
HPTL	**WHEN**	**HOW**	**EFFECT**	**REMARKS**
COPs	P	GS ARTY	N	PLAN IN INITIAL PREP
RISTA and OPs	P	GS ARTY	N	PLAN IN INITIAL PREP
2S1 and 2S3	P	MLRS	N	PLAN IN INITIAL PREP
2S6, SA9 and SA13	P	GS ARTY	S	SEAD FOR AVN OPS
REGT CP	A	MLRS	N	
RESERVE BN	P	AVN BDE	D	INTENT TO ATTACK RESERVE BN IN EA HOT
LEGEND:	I = IMMEDIATE A = AS ACQUIRED P = PLANNED		S = SUPPRESS N = NEUTRALIZE D = DESTROY	
NOTES: [1]This is only an example of an AGM. Actual matrices are developed on the basis of the situation. [2]An "H" for harassing fires may be included in the EFFECT column during SASO.				

Figure F-7. Example attack guidance matrix.

HPTL. Lists the prioritized HPTs identified during wargaming. They have priority for engagement.

WHEN. Timing the attack of targets is critical to maximizing effects. During wargaming, the optimum time is identified and reflected in the WHEN column. A " **P"** indicates the target should not be engaged now but should be *planned* for future firing (e.g., a preparation, a SEAD program, or a countermobility program) or simply put on file. An **"A"** indicates such targets should be engaged in the sequence received in the headquarters, with respect to the priority noted in the HPTL. An **"I"** indicates the attack

must be *immediate* and is a special case. This designation should be limited to a small percentage of targets and only for the most critical types. Too many immediate targets are disruptive and lower the efficiency of attack systems. Immediate attacks take precedence over all others and are conducted even if attack systems must be diverted from attacks already underway. Examples of important targets include:

- Missile systems capable of NBC attacks.
- Division headquarters.
- NBC weapons storage and support facilities.

MRLS may be considered for immediate attack depending on their demonstrated effectiveness against friendly forces and their tactical employment. The G3/S3 and FSCOORD or FSO must establish procedures within the TOC that allow for immediate attack of targets.

HOW. Links the attack system to the HPT. It is best to identify a primary and backup attack system for attack of HPTs.

EFFECT. Refers to the target attack criteria. The targeting team should specify attack criteria according to the commander's guidance. Target attack criteria should be quantifiable (e.g., percentage of casualties or destroyed elements, time, ordnance, and allocation or application of assets). Also, it can be noted as the number of battery or battalion volleys.

REMARKS. Notes which targets should not be attacked in certain tactical situations (e.g., if the enemy is withdrawing). Examples of how to use this column:

- Accuracy or time constraints.
- Required coordination.
- Limitations on the amount or type of ammunition.
- Any need for BDA.

STEP 2 - DETECT:

DETECT is the next critical function in the targeting process. The G2/S2 is the main figure in directing the effort to detect identified HPTs. To identify who, what, when, and how for TA, the G2/S2 must work closely with the—

- ACE.
- FAIO.
- Targeting officer and FSO.

This process determines accurate, identifiable, and timely requirements for collection systems. The ACE must ensure collection system asset managers understand these requirements.

Information needs for target detection are expressed as PIR and IR. Their priority depends on the importance of the target to the friendly COA and tracking requirements. PIR and IR that support detection of HPTs are incorporated into the overall unit collection plan.

Targets are detected by the maximum use of all available assets. The G2/S2 must focus the intelligence acquisition efforts on the designated HPTs and PIR. Situation development information, through detection and tracking, will be accumulated as collection systems satisfy PIR and IR. The collection manager—

- Considers availability and capabilities of all collection assets within his echelon and those available to subordinate, higher, and adjacent units.
- Considers joint or combined force assets.
- Translates the PIR and IR into SIR and SOR.
- Arranges direct dissemination of targeting information from the collector to the targeting cell or targeting intelligence to the FSE if possible.

Detection Procedures. Use all TA assets effectively and efficiently. Avoid duplication of effort among intelligence available assets unless it is required to confirm target information. At corps and division, the ACE develops and manages the collection plan and ensures that no gaps in planned collection exist. This allows timely combat information to be collected to answer the commander's intelligence and TA requirements. To detect HPTs, give clear and concise

taskings to those TA systems capable of detecting a given target. This information lets analysts develop the enemy situation and identify targets (Figure F-8).

FS personnel provide the G2/S2 with the degree of located accuracy. The accuracy requirements are matched to the TLE of the collection systems. This allows the G2/S2 to develop more detailed TSS. NAIs and TAIs identified are matched with the most capable detection system available. If the target type and its associated signatures (e.g., electronic, visual, thermal) are known, the most capable collection asset can be directed against the target. The asset can be placed in the best position according to estimates of when and where the enemy target will be located.

Assets are positioned based on friendly estimates of where the enemy target is located. Information needed to detect targets are expressed in PIR and IR, which are incorporated into the collection plan. The collection manager translates the PIR and IR into SIR.

The collection manager considers the availability of all collection assets at all echelons. When a target is detected, the information is passed to the FAIO to determine if it is an HPT, its priority, and if it meets the TSS. To ensure that target information is passed quickly, the FAIO should be located in the ACE with communications to the FSE. Once an HPT is discovered, the FAIOs coordinate with their respective G2s/S2s and pass the targets directly to the FSE. If the commander approves the target, it is then passed to a firing unit. Mobile HPTs must be detected and tracked to maintain a current target location. Target tracking is inherent to detection.

BOS	TARGET ACQUISITION MEANS
INTELLIGENCE	SIGINT/EW, IMINT, HUMINT, TECHINT, MASINT systems.
MANEUVER	Patrols, scouts, units in contact, air/ground cavalry/air units.
FS	TAB, AN/TPQ-36/37 radars, FOs, AFSOs, COLTs.
AD	ADA scouts, ADA system's acquisition radars.
MOBILITY, COUNTER-MOBILITY, SURVIVABILITY	Engineer and NBC reconnaissance.
CSS	Truck drivers, base cluster recon/counterrecon patrols.
C^2	MIJI reports.
AIR FORCE	Joint STARS, AWACS.

Figure F-8. BOS detection capabilities.

As the assets collect information for target development, the information is forwarded to ACE intelligence analysts who use the information to perform situation and target development. Once a target specified for attack is identified, the analysts pass it to the FSE. The FSE executes the attack guidance against the target. Coordination between the intelligence staff and the FSE is essential to ensure that the targets are passed to an attack system that will engage the target.

The FAIOs can coordinate with the G2 and FSE to pass HPTs and other targets directly to the FCE at the division artillery TOC or, if approved by the maneuver commander, directly to a firing unit. The result is an efficient attack of targets which have been designated in advance for attack.

When the FAIO gets intelligence information which warrants attack, he notifies the FSE. This allows the FAIO to focus on intelligence analysis and the FSE to manage the control of fires. The targeting officer at the maneuver brigade and the S2 at the battalion perform FAIO functions.

Tracking priorities are based on the commander's concept of the operation and targeting priorities. Tracking is executed through the collection plan. Not all targets will be tracked. Because many critical targets move frequently or constantly, these HPTs require tracking.

Synchronization of Intelligence Collection. While conducting operations, the G2/S2 monitors execution of the collection plan. He uses an ISM to synchronize the intelligence system in order to give answers to PIR in time to affect the decisions they support. As HPTs are identified, he informs the appropriate FSE and cross-cues collection assets to support BDA as needed.

During delivery, NRT collectors and observers are cued to continue tracking targets during their engagement. Planned or cued BDA collection and reporting help determine if the engagement produced the desired effects. If not, continued tracking supports immediate reengagement.

To facilitate hand-off of target and tracking responsibilities, the G2/S2 coordinates with higher and subordinate units. Requirements for intelligence in a given area can then be directed to the unit responsible for that area. Operational graphics are useful when tracking particular threat units or HPTs. Passing responsibility for the target as it crosses the graphic ensures that it is not lost in crossing.

Synchronization continues during the CM process. The G2/S2 uses the products of the targeting process to develop SIR and SOR that synchronize the collection effort with command DPs. He plans and allocates time for collection, processing, and dissemination.

During execution the collection manager monitors the collection and reporting to ensure synchronization. He prompts asset managers to meet timelines, cross-cueing, and retasking as necessary to keep intelligence operations synchronized with command operations.

IEW Systems. The collection manager at each echelon gives appropriate IEW agencies missions through the collection plan and ISM. The intelligence analyst directly supports the collection manager. To properly synthesize information being received from forward units and collection systems intelligence analysts must understand their capabilities and limitations.

Figure F-9 explains the intelligence disciplines that provide targeting information through collection.

DISCIPLINE	FUNCTION
SIGINT/EW	• Friendly SIGINT/EW systems search for, intercept, and locate threat electronic signals emanating from radios, radars, and beacons. • Signatures are caused by electronics associated with the particular C^2 functions of the target. • Signatures identify signals based on characteristics of the signal or content of any messages intercepted. • The signals are then associated with an adversary's OB. • Electronic systems organic to tactical and operational (corps and theater) EW units can locate threat radio, radar, beacon, and C^2 system emissions using DF equipment. • DF efforts have inherent considerations that affect target accuracy such as DF system accuracy, terrain, and distance to target.
IMINT	• Imagery assets can be located in the AEB of the corps MI Bde, GRCS, and GS and DS companies of the Div MI Bn TUAV when fielded. • TUAV is organic to the DS Co of a heavy division. • TUAV is organic to the GS Co in a light infantry division. • FCE is assigned to the GS Co. • Predator UAV and Joint-STARS are USAF assets. They include airborne and ground-based IMINT sensors such as photo, TV, infrared, and MTI radar. • Targets have visual and infrared signatures that can be imaged. • Imagery analysts study results of IMINT missions to determine the presence, location, and assessed damage to threat targets. These films and devices can detect thermal signatures produced by equipment (engines, heaters, or any device producing or absorbing heat). These devices can also differentiate camouflaged equipment and structures. • Mounted sensors in UAVs provide TA capability which can locate threat elements unseen by ground observers and

Figure F-9. Intelligence disciplines.

	can successfully direct engagement of the targets. SLAR can detect the movement of vehicles beyond visual range of ground observers. • Imagery and intelligence analysts look for the threat's patterns of activity or intentions produced from IMINT systems. • Patterns of movement (numbers, direction, times) are analyzed and synthesized with other combat information to determine a threat commander's intentions. • Imagery can be requested from national and theater systems to support area studies and operations. • Imagery can also be used for training in garrison and at CTCs.
HUMINT	• HUMINT is produced by LRSUs, CI teams that are positioned throughout the depth of the battlefield, and interrogation teams that may be at maneuver battalions and higher. • Interrogation of threat prisoners can be focused on the detection of HVT and HPTs. • Interrogators should receive lists of intelligence interests and the commander's PIR. • Giving current HPTLs to the interrogators allows them to focus their efforts on locating these targets while gleaning additional information for situation development. • LRSUs are another HUMINT source. They may be tasked to determine the presence or absence of threat activity within the NAIs developed during the IPB process. • Keying these NAIs to HPTs allows the LRSUs to contribute significantly to the target detection process. • Information gained from LRSUs is real or NRT and can result in immediate engagement. • Due to extensive preparation and support requirements, LRSUs should be planned early and used IAW its doctrine (e.g., depth, target selection, insertion techniques). • CI teams detect subversion, espionage, and terrorist threats to friendly forces, and can also work with the local population to gather items of intelligence interest. • SOF may be tasked through SOCCE assigned at brigade, division, or Corps.

Figure F-9. Intelligence disciplines (continued).

TECHINT	• The TECHINT system is made up of two parts: S&TI and battlefield TECHINT. • S&TI supports strategic level of war intelligence. • Battlefield TECHINT supports operational and tactical levels of war intelligence. • TECHINT aids the commander by providing products that either identify or counter an adversary's monetary technological advantage. • TECHINT is an integral part of all-source intelligence because it involves everyone from individual soldiers to the policy makers. • Foreign material is photographed or captured and exploited for information, capabilities, limitations, and vulnerabilities. • The 203d MI Battalion operates the CMEC for the Army, or forms the Army's component of JCMEC or CCMEC. • Teams are sent from the battalion down to ECB units. • The G2, G3, TECHINT commander, and MI commander comprise the battlefield TECHINT team. • The commanders execute the staff's directives to collect materials for the TECHINT teams to exploit.
MASINT	• A MASINT sensor collects energy emitted by or reflected from an object or event for the purpose of identification and characterization. • Enemy weapon systems have physical characteristics and distinct performance identifiers when used. • Dynamic targets and events are primary candidates for MASINT exploitation by the MI force projection brigades. • These sources create energy emissions across the EM spectrum which carry information about its characteristics and performance via waves or particles. • This information is the signature collected by MASINT sensors; it can be used when developing threat assessments, OBs, IPB, and targeting materials. • MASINT data becomes invaluable during the rapid reprogramming of *smart* weapons and sensors or when changing tactics.

Figure F-9. Intelligence disciplines (continued).

STEP 3 - DELIVER:

DELIVER executes the target attack guidance and supports the commander's battle plan once the HPTs have been located and identified (Figure F-10).

ATTACK OF TARGETS MUST:	■ Satisfy attack guidance developed in *decide* function. ■ Require two categories of decisions—*tactical* and *technical*.
TACTICAL DECISIONS DETERMINE:	■ Desired effect, degree of damage, or both. ■ Attack system to be used. ■ Time of attack. This is determined IAW type of target: Planned target or target of opportunity. ; **PLANNED TARGET:** –Some targets will not appear as anticipated. –Target attack takes place only when the forecasted enemy activity occurs in projected time or place. Detection & tracking of activities associated with target becomes trigger for target attack.
TARGETING TEAM:	
G2 RESPONSIBILITIES:	■ Verifies enemy activity as the planned target to be attacked. ■ Validates target by conducting final check of reliability of source & accuracy (time & location) of target. Passes target to FSE. ■ Current operations officer checks legality of target in terms of the ROE.
FSE RESPONSIBILITIES:	■ Determines if attack systems planned are available & still best systems for attack. ■ Coordinates with higher/lower/adjacent units, other services, allies & HN (important where potential fratricide situations are identified).

Figure F-10. Deliver functions and responsibilities.

	■ Issues fire mission request to appropriate executing units. ■ Informs G2 of target attack. G2 alerts appropriate system responsible for BDA (when applicable). ; **TARGETS OF OPPORTUNITY:** –Are processed the same as planned HPTs. –Those not on HPTL are first evaluated to determine when or if they should be attacked. ■ Decision to attack follows attack guidance & is based on— •Activity of the target. •Dwell time. •Target payoff compared to other targets currently being processed for engagement. –If decision is made to attack immediately, target is processed further. –Availability & capabilities of attack system to engage targets are assessed. –If target exceeds availability or capabilities, send target to higher HQ for immediate attack. –If decision is to defer attack, continue tracking; determine DPs for attack, and modify collection taskings as appropriate.
TECHNICAL DECISIONS (DETERMINED BASED ON TACTICAL DECISIONS):	■ Precise delivery means. ■ Number and type of munitions. ■ Unit to conduct the attack. ■ Response time of the attacking unit. ■ Results in physical attack of targets by lethal and/or nonlethal means. ■ FS cell directs attack system to attack target once tactical decisions have been made. ■ FS cell provides attack system manager with—

Figure F-10. Deliver functions and responsibilities (continued) .

	•Selected time of attack. •Effects desired IAW previous discussion. •Any special restraints or requests for particular munitions types. ■ Attack system manager (FSCOORD, ALO, AVN BDE, LNO, NGLO) determines if his system can meet requirements. If cannot, he notifies FS cell. Some reasons for not being able to meet requirements include— •System not available at specified time. •Required munitions not available. •Target out of range. ■ FS cell must decide if selected system should attack under different criteria or if a different system should be used.
TARGETS OF OPPORTUNITY ARE ATTACKED BASED ON:	■ The target's activity. ■ Estimated assembly area activity.
DESIRED EFFECTS: **DISRUPT** **DELAY** **LIMIT**	■ Planned Targets: •Verify enemy activity as that planned to be attacked. •Reaffirm decision to attack. •Issue the fire mission request (through FS cell) to appropriate executing units. ■ Targets of Opportunity: •Targeting team must decide payoff and availability of attack systems and munitions.
ATTACK SYSTEM:	■ Planned Targets: •Decision made during *decide* function. •Determine system availability & capability. •Targeting team must determine best system available to attack target if system not available or capable.

Figure F-10. Deliver functions and responsibilities (continued).

	■ Targets of Opportunity: •Targeting team must determine attack system, subject to maneuver commander's approval. •Consider all available attack systems. •Attacking targets should optimize capabilities of— –Light and heavy ground forces. –Attack helicopters. –FA. –Mortars. –Naval gun fire. –Combat air operations (CAS and air interdiction). –Offensive EW. •Consider availability & capabilities of each resource using the following: –Desired effects on the target. –Payoff of the target. –Degree of risk to use asset against target. –Impact on friendly operations. •Target attack must be coordinated among two or more attack systems. •Engaging a target by lethal means, along with jamming or monitoring, may be of greater benefit than simply firing at the target.

Figure F-10. Deliver functions and responsibilities (continued).

STEP 4 - ASSESS:

Combat assessment is the determination of the effectiveness of force employment during military operations. It is composed of three elements:

- BDA, which is the timely and accurate estimate of damage resulting from the application of lethal or nonlethal military force against a target.
- MEA, which is an assessment of the military force in terms of weapon systems and munitions effectiveness.

- Reattack recommendation.

In combination, BDA and MEA inform the commander of effects against targets and target sets. Based on this, the threat's ability to make and sustain war and centers of gravity are continuously estimated. During the review of the effects of the campaign, restrike recommendations are proposed or executed. BDA pertains to the results of attacks on targets designated by the commander. Producing BDA is primarily an intelligence responsibility, but requires coordination with operational elements. BDA requirements must be translated into PIR. It accomplishes the following:

- At the tactical level, commanders use BDA to get a series of timely and accurate snapshots of their effect on the enemy. It provides commanders an estimate of the enemy's combat effectiveness, capabilities, and intentions. This helps commanders determine when or if their targeting effort is accomplishing their objectives.

- BDA helps to determine if restrike is necessary. Commanders use BDA to allocate or redirect attack systems to make the best use of available combat power.

The G3 through the targeting team conducts MEA concurrently and interactively with BDA as a function of combat assessment. MEA is used as the basis for recommending changes to increase effectiveness in—

- Methodology.
- Tactics.
- Weapon systems.
- Munitions.
- Weapon delivery parameters.

The G3 develops MEA by determining the effectiveness of tactics, weapons systems, and munitions. Munitions effect on targets can be calculated by obtaining rounds fired on specific targets by artillery assets. The targeting team may generate modified commander's guidance concerning—

- UBL.
- RSR.
- CSR.

The need for BDA for specific HPTs is determined during the **decide** function. Record BDA on the AGM and intelligence collection plan. The resources used for BDA are the same resources used for target development and TA. An asset used for BDA may not be available for target development and TA. The ACE receives, processes, and disseminates to the targeting team the results of attack, which are analyzed in terms of desired effects.

The targeting team must keep the following BDA principles in mind:

- BDA must measure things that are important to commanders, not make important the things that are easily measurable.
- BDA must be objective. When a G2/S2 receives a BDA product from another echelon, he should verify the conclusions (time permitting). G2s/S2s at all echelons must strive to identify and resolve discrepancies among the BDA analysts at different headquarters.
- The degree of reliability and credibility of the assessment relies largely upon collection resources. The quantity and quality of collection assets influence whether the assessment is highly reliable (concrete, quantifiable, and precise) or has low reliability (best guess). The best BDAs use more than one collection discipline to verify each conclusion.

Each BDA has three assessment components (Figure F-11). Each requires different sensors, analytical elements, and timelines. They are not necessarily subcomponents of each BDA report. (See FM 6-20-10, Appendix D.)

COMPONENTS	DESCRIPTION
PDA	• Qualitative physical damage from munitions blast, fragmentation, and fire. • Based on observed or interpreted damage.

FDA	• Effects of military force to degrade or destroy capability of target to perform mission. • Assessment based on all-source intelligence. • Includes an estimate of time to reconstitute or replace target. • Temporary assessment compared to a TSA used for specific missions.
TSA	• The overall impact of the full spectrum of military operations on an entire target system's capability. • Can be applied against an adversary's combat effectiveness. • May address significant subdivisions of a target. • A more permanent assessment.

Figure F-11. BDA functions.

BDA is more than determining the number of casualties or the amount of equipment destroyed. The targeting team can use other information, such as—

- Whether the targets are moving or hardening in response to the attack.
- Changes in deception efforts and techniques.
- Increased communication efforts as the result of jamming.
- Whether the damage achieved is affecting the enemy's combat effectiveness as expected.

BDA may also be passive by compiling information regarding a particular target or area (e.g., the cessation of fires from an area). If BDA is to be made, the targeting team must give intelligence acquisition systems adequate warning for sensors to be directed at the target at the proper time. BDA results may change plans and earlier decisions. The targeting team must periodically update the decisions made during the **decide** function concerning—

- IPB products
- HPTLs.
- TSS.
- AGMs.
- Intelligence collection plans.
- OPLANs.

Based on BDA and MEA, the G2/G3 consider the level to which operational

objectives have been achieved and make recommendations to the commander. Reattack and other recommendations should address operational objectives relative to the—

- Target.
- Target critical elements.
- Target systems.
- Enemy combat force strengths.

BDA key players are the commander, operations officer, FSO, AAO, ALO, and S2. The S2 integrates intelligence and operational data. In coordination with the G3, the G2/S2—

- Recommends HPTs.
- Develops and recommends IR to include those for targeting and BDA. Some requirements become PIR.
- Coordinates with the G3/S3, AAO, and FSO to develop a fully coordinated targeting and BDA plan.
- Develops a synchronized collection plan to answer the commander's IR and tracks and maintains BDA charts and files.
- Tasks or requests collection support from the appropriate unit or agency to collect information required to satisfy the commander's targeting objectives and BDA reporting requirements.
- Establishes procedures to ensure reports from FOs, scouts, troops in contact, pilots, and AVTRs are quickly made available for BDA analysis.
- Matches BDA reporting requirements against the commander's objectives to determine targeting effort drain; develops and maintains historical BDA databases, and disseminates hard and soft copy intelligence and BDA results.
- Uses the results of BDA and combat assessment to determine the need to develop further threat COAs.
  - — Determines priority for collection assets between the targeting effort and

the BDA supporting requirements.

— Determines and updates enemy capabilities based upon results of the targeting effort.

SASO CONSIDERATIONS

Target development and targeting are difficult in an SASO environment. Although the principles of the targeting process still apply in SASO, consider the following:

- ROE tend to be more restrictive than in conventional combat situations. Everyone involved in the targeting process must completely understand the ROE.
- Identification of HVTs, threat intentions, threat locations, and weapons systems is slow to develop and may not be able to be acted upon when fully developed.
- Because of the nature of the threat (usually a relatively small, unconventional enemy may constitute a significant threat to US forces) determination of HVTs (specifically, what constitutes an HVT) is extremely difficult. Thus, it is difficult to develop precise time, location, and rates of march for a threat force.
- "Targets," which blend into the population, are often less visible than conventional targets.
- When identified, targets present less of a window of opportunity in which to react, decreasing decision time.
- Because of considerations of the HN population, targeting must be precise. Selecting the right weapons system for the right target is paramount.
- Interaction and coordination with nontraditional elements and agencies may be required. This may include private organizations, NGOs, other federal agencies, civil agencies, allies or coalition forces, and HN forces.

CARVER TECHNIQUE

ARSOF uses CARVER factors to assess mission, validity, and requirements. They are also used in technical appreciation and target analysis.

The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are given a numerical value, which represents the desirability of attacking the target. The values are then placed in a decision matrix. After CARVER values for each target or component are assigned, the sum of the values indicates the highest value target or component to be attacked within the limits of the statement of requirements and commander's intent. Figure F-12 explains the CARVER techniques.

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
Criticality	•Means target value. •Primary consideration in targeting. •Target is critical when its destruction or damage has major impact on military, political, or economic operations. •Consider targets within a system in relation to other elements of the target system. •Value of target will change as situation develops. •Target requires use of time-sensitive methods which respond to changing situation. **EXAMPLE:** When one has few locomotives, railroad bridges may be less critical as targets; however, safeguarding bridges may be critical to maneuvering conventional forces requiring use of such bridges.	•Time—How rapidly will impact of target attack affect operations? •Quality—What % of output, production, or service will be curtailed by target damage? •Surrogates—What will be effect on output, production, and service? •Relativity—How many targets? What are their positions? How is their relative value determined? What will be affected in the system or complex stream?	•Immediate halt; target cannot function without it. •Halt within 1 day, or 66%. •Halt within 1 week, or 33%. •Halt within 10 days, or 10%. •No significant affect. *Refers to time or %; curtailment in output, production, or service.	9 to 10 7 to 8 5 to 6 3 to 4 1 to 2

Figure F-12. CARVER techniques.

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
Accessibility	•Target is accessible when operations element can reach the target with sufficient personnel and equipment to accomplish mission. •Entails identifying & studying critical paths the operational element must take to achieve objectives & measuring those things that aid or impede access. •You must be able to reach target AND remain there for extended periods. •Basic steps identifying accessibility: –Infiltration from staging base to target. –Movement from point of entry to target/objective. –Movement to target's critical element. –Exfiltration.	•Active & passive EWS. •Detection devices. •AD capabilities within target area. •Road & rail transportation systems. •Type terrain & its use. •Concealment & cover. •Population density. •Other natural or synthetic obstacles & barriers. •Current & climatic weather conditions. •Analysis along each critical path to target should measure time it would take for action element to bypass, neutralize, or penetrate barriers/ obstacles. •Measured by relative ease or difficulty of movement for operational element & likelihood of detection. Consider using standoff weapons in such evaluations.	•Easily accessible standoff weapons can be employed. •Inside a perimeter fence but outdoors. •Inside a building but on ground floor. •Inside a building but on second floor or in a basement; climbing or lowering is required. •Not accessible or inaccessible without extreme difficulty.	9 to 10 7 to 8 5 to 6 3 to 4 1 to 2

Figure F-12. CARVER techniques (continued).

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
Recuperability	•Measured in time—How long will it take to replace, repair, or bypass destruction of or damage to the target? •Varies with sources and type of targeted components and availability of spare parts availability.	•Onhand equipment such as railroad cranes, dry docks, and cannibalization. •Restoration and substitution through redundancies. •Onhand spares. •Equivalent OB equipment sets that backup critical equipment or components; effects of economic embargoes and labor unrest.	Replacement, repair, or substitution requires— •1 month or more. •1 week to 1 month. •72 hours to 1 week. •24 to 72 hours. •Same day replacement, repair, or substitution.	9 to 10 7 to 8 5 to 6 3 to 4 1 to 2
Vulnerability	•Target is vulnerable if operational element has means & expertise to successfully attack the target. •Scale of critical component needs to be compared with capability of attacking element to destroy or damage it. •Attacking element may tend to— –Choose special components. –Do permanent damage.	•Depends on— –Nature and construction of the target. –Amount of damage required. –Assets available, (e.g., personnel, expertise, motivation, weapons, explosives, and equipment.)	•Vulnerable to long-range laser target designation, small arms fire, or charges of 5 lbs or less. •Vulnerable to light antiarmor weapons fire or charges of 5 to 10 lbs.	9 to 10 7 to 8

Figure F-12. CARVER techniques (continued).

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
	–Maximize effects through use of onsite materials. –Cause the target to self-destruct.		•Vulnerable to medium antiarmor weapons fire, bulk charges of 10 to 30 lbs, or very careful placement of smaller charges.	5 to 6
			•Vulnerable to heavy antiarmor fire, bulk charges of 30 to 50 lbs, or requires special weapons.	3 to 4
			•Invulnerable to all but the most extreme target-ting measures.	1 to 2
Effect	•Measure of possible military, political, economic, psychological & sociological impacts at target & beyond. •Closely related to the measure of target criticality. •Type & magnitude of given effects desired will help planners select targets & target components.	•Primary effect of destruction of 2 adjacent long-range radar sites in EWS may be to open hole in system that is of sufficient size & duration to permit attacker to launch a successful air or missile nuclear strike against defender.	•Overwhelmingly positive effects; no significant negative effects.	9 to 10
			•Moderately positive effects; few significant negative effects.	7 to 8
			•No significant effects; neutral.	5 to 6
			•Moderately negative effects; few significant positive effects.	3 to 4

Figure F-12. CARVER techniques (continued).

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
	•Addresses all significant effects, whether desired or not, that may result once selected target component is attacked. •Traditionally, this element addressed effect on local population; now there are broader considerations. •Frequently neutral at tactical level.	•Can include— –Triggering of counter-measures. –Support of negation of PSYOP themes. –Unemploy-ment. –Reprisals against civilian popu-lace. –Collateral damage to other targets. •Possible effects can be specula-tive & thus should be labeled. •Effects of same attack may be different at tactical, opera-tional & strategic levels. **EXAMPLE:** Destruction of a substation may not affect local power but cuts off power to adjacent region.	•Overwhelmingly negative effects; no significant positive effects.	1 to 2

Figure F-12. CARVER techniques (continued).

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
Recognizability	•Target's recognizability is degree to which it can be recognized by an operational element or intel collection & recon assets under varying conditions. •Weather impacts visibility. •Rain, snow & ground fog may obscure observation. •Road segments with sparse vegetation & adjacent high ground provide excellent conditions for good observation. •Distance, light & season must also be considered.	•Site & complexity of target. •Existence of distinctive target signatures. •Presence of masking or camouflage. •Technical sophistication & training of attackers.	•Target is clearly recognizable under all conditions & from a distance; requires little or no training. •Target is easily recognizable at small-arms range & requires small amount of training. •Target is difficult to recognize at night or in bad weather, or might be confused with other targets or components; requires some training. •Target is difficult to recognize at night or in bad weather, even within small-arms range; it is easily confused with other targets or components; requires extensive training. •Target cannot be recognized under any conditions, except by experts.	9 to 10 7 to 8 5 to 6 3 to 4 1 to 2

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE

Figure F-12. CARVER techniques (continued).

CARVER factors and their assigned values are used to construct a CARVER matrix. Table F-1 is a tool for rating the desirability of potential targets and allocating attack resources.

- List the potential targets in the left column.
- For strategic level analysis, list the enemy's systems or subsystems (electric power supply, rail system).
- For tactical level analysis, list the complexes or components of the subsystems or complexes selected for attack by your higher HQ.
- As each potential target is evaluated for each CARVER factor, enter the appropriate value into the matrix.
- Once all the potential targets have been evaluated, add the values for each potential target.
- The sums represent the relative desirability of each potential target; this constitutes a prioritized list of targets.
- Attack those targets with the highest totals first.
- If additional men or munitions are available, allocate these resources to the remaining potential targets in descending numerical order.
- This allocation scheme will maximize the use of limited resources.

The S2 can use the CARVER matrix to present operation planners with a variety of attack options. With the matrix, he can discuss the strengths and weaknesses of each COA against the target. Having arrived at conclusions through the rigorous evaluation process, the S2 can comfortably defend his choices.

Table F-1. Bulk electric power supply.

POTENTIAL TARGETS	C	A	R	V	E	R	TOTAL
Fuel Tanks	8	9	3	8	5	6	41
Fuel Pumps	8	6	2	10	5	3	34
Boilers	6	2	10	4	5	4	31
Turbines	8	6	10	7	5	9	45
Generators	4	6	10	7	5	9	41
Condenser	8	8	5	2	5	4	34
Feed Pumps	3	8	5	8	5	6	33
Water Pumps	3	8	5	8	5	4	33
Generator Step up Transformer	10	10	10	9	5	9	53

APPENDIX G

IEW SYSTEMS

QUICKFIX (AN/ALQ-151(V1)) Advanced QUICKFIX (AN/ALQ-151(V2))

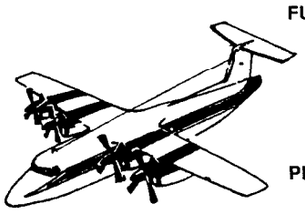
FUNCTION: VHF DF intercept, VHF EA, VHF DF (nets w/TRAILBLAZER for DF). Component of IEWCS AF/VHF/UHF ES

PRIME MOVER: EH-60A, EH-60L (BLACKHAWK)

UNIT AND QTY: HVY DIV: 3 Systems 3 Flt Plt, Avn Bde; LT DIV: 3 Systems, 3 Flt Plt, Avn Bde; AASLT DIV: 3 Systems, 3 Flt Plt, HHOC, MI Bn; ABN DIV: 3 Systems, 3 Flt Plt, Cbt Avn Sqdn; ACR: 3 Systems, 3 Flt Plt, Cbt Avn Sqdn

INTEL APPLICATION: COMINT

Airborne Reconnaissance Low (ARL)



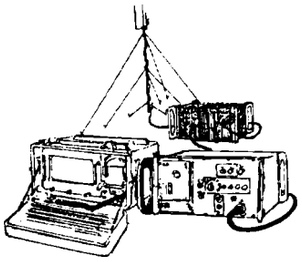
FUNCTION: Ground processing station, ACT 101 remote rcv sets, TACLINK video rcv sets, FLIR system, daylight imaging systems, infrared line scanner, radio intercept/DF systems; interoperates w/ASAS & CTT

PRIME MOVER: DHC-7 arrives ready for immediate employment

UNIT AND QTY: Select Brigades

INTEL APPLICATION: COMINT/IMINT

Commander's Tactical Terminal (CTT), AN/TSC-125



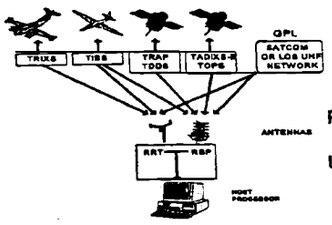
FUNCTION: Communications terminal; GUARDRAIL downlink on TRIXS network; RRS on board RC-12 & U2-R, RRTS; includes OT, RBP, RRT, LOS adaptive array antenna, SDS, embedded COMSEC

PRIME MOVER: NA

UNIT AND QTV: 1- MI at all echelons

INTEL APPLICATION: SIGINT

Joint Tactical Terminal: JTT/H3 (AN/USC-55)
JTT/H-R3 (AN/USR-6)



FUNCTION: Communications terminal, 2 LRUs, 1 RBP, 1 RRT, host processor & antenna array (both user provided); mobile & mountable in F/W & R/W, tracked & wheeled vehicles, shelters

PRIME MOVER: NA

UNIT AND QTY: Avn, ADA, FA, MI at all echelons; integrated into GSM/CGS, ASAS, ETRAC, THAADS, Patriot, JTAGS, TROJAN SPIRIT, AFATDDS, other multiservice systems

INTEL APPLICATION: SIGINT

Ground-Based Common Sensor (GBCS)

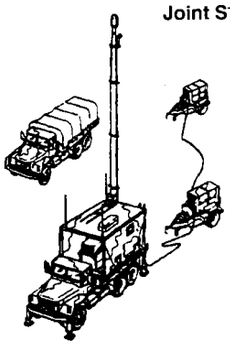
FUNCTION: ES (intercept& DF); EA (jamming); COMINT targeting location data; common subsystems with AQF & MEWSS

PRIME MOVER: EFVS (HVY DIV) or HVY HMMWV (LT DIV)

UNIT AND QTY: 6 GBCS-H per MI Bn (H); 4 GBCS-H per MI Co (ACR); 4 GBCS-L per MI Bn (ABN, AASLT, LT); 6 per MI Bn (H, LT, ABN, AASLT, DIV); 6 per MI Co; ACR

INTEL APPLICATION: COMINT/ELINT

Joint STARS Ground Station Module (GSM) (AN/TSQ-132)

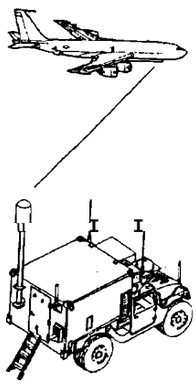


FUNCTION: MTI, FTI, SAR imagery; supports situation development, battle mgt, targeting, force protection, limited BDA/TDA, operations planning

PRIME MOVER: LT - 2xHMMWV; MED - 2X5-ton HMMWV

UNIT AND QTY: 6- Selected DIV; 6- Selected Corps; 1- ACR; 1- EAC

INTEL APPLICATION: IMINT/SIGINT/INTEL/ ARTY/AVN SUPPORT



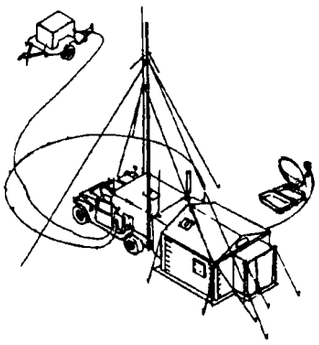
Joint STARS Common Ground Station (CGS)

FUNCTION: MTI, FTI, SAR imagery; supports situation development, battle mgt, targeting, force protection, limited BDA/TDA, operations planning; includes SATCOM & CTT communications

PRIME MOVER: LT - 2xHMMWV

UNIT AND QTY: 5 to 7- DIV; 5 to 7- Corps; 1- ACR; 1- SEP BDE; 1 to 5 EAC

INTEL APPLICATION: IMINT/SIGINT/INTEL/ ARTY/AVN SUPPORT



Integrated Meteorological System (IMETS)

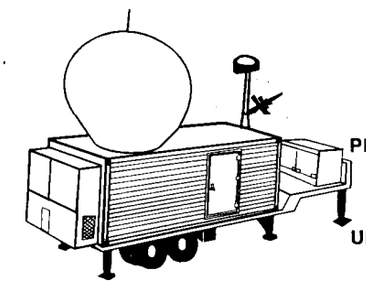
FUNCTION: Receives, processes & disseminates weather data.

PRIME MOVER: Heavy HMMWV mounted

UNIT AND QTY: DIV, Corps, EAC, SEP BDE, ACR, AVN BDE, other task organized contingencies

INTEL APPLICATION: Intelligence Support

Advanced Electronic Processing and Dissemination System (AEPDS)



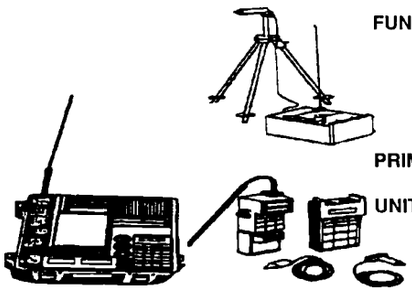
FUNCTION: Mobile, air & ground transportable comm system; receives, processes & exploits SIGINT data from multiple national, theater & organic ELINT/ COMINT systems. Combines functions of EPDS & ETUT into a single downsized system

PRIME MOVER: 30 ft van pulled by a 3-axle 10-ton tractor air deployable on C-130 or larger aircraft

UNIT AND QTV: 1- Corps (rear) 1- Select MI Bde (EAC)

INTEL APPLICATION: SIGINT

Improved Remotely Monitored Battlefield Sensor System (IREMBASS)



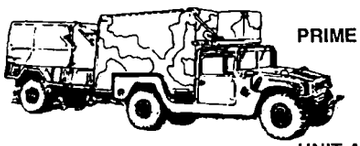
FUNCTION: Unattended ground sensor (seismic/ acoustic, magnetic, infrared, meteorological) that detects, classifies & determines direction of movement

PRIME MOVER: Manpacked and vehicle

UNIT AND QTY: LT DIV - 5 (GS Plt, I&S Co, MI Bn); ASSLT DIV - 5 (GS Plt, I&S Co, MI Bn); ABN DIV - 5 (GS Plt, MI Co (Fwd Spt), MI Bn)

INTEL APPLICATION: MASINT

Mobile Integrated Tactical Terminal (MITT)



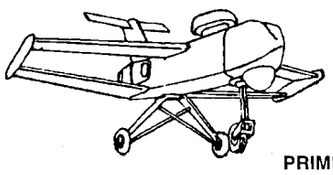
FUNCTION: Replaces THMT & FAST-I in force structure; compatible w/TROJAN, MSE, TIBS, DIN/DSSCS, STU III, TENCAP; TRAP/TADIXS-B, UHF SATCOM, S-BAND w/ROTERM/ CHARIOT

PRIME MOVER: Mobile, ground, air transportable (heavy duty HMMWV, cargo HMMWV, generator trailer, C-130, CH-47)

UNIT AND QTY: DIV and Corps ACE - 1

INTEL APPLICATION: SIGINT/IMINT

Tactical Unmanned Aerial Vehicle (TUAV) - OUTRIDER



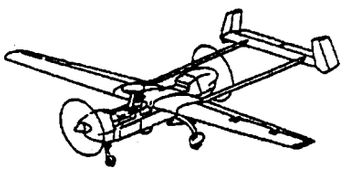
FUNCTION: Operates fwd of FLOT, in all conditions; provides NRT intel, recon, battlefield survl, color E-O camera, FLIR, plug-in optronic payload; future payloads: MTI, SAR, comm/ noncomm DF, intercept, jamming; MET

PRIME MOVER: C-130 or larger, roll-on/roll-off; ground equipment mounted on HMMWVs

UNIT AND QTY: 3 - HVY/AASLT DIV; 5 - LT DIV; 3 - ABN DIV; 3 - ACR; 5 - LT ACR; 1 - SEP BDE

INTEL APPLICATION: IMINT/SIGINT/PSYOP

Unmanned Aerial Vehicle-Short Range (UAV-SR) HUNTER



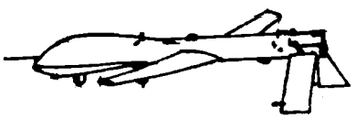
FUNCTION: Operates fwd of FLOT, in all conditions; provides NRT intel, recon, battlefield survl, color CCD, TA, BDA, recon, battlefield survl, E-O/FLIR, UAV data relay; future payloads: MTI, SAR, MET, ES, EA, mine detection, PSYOP, SIGINT, NBC recon

PRIME MOVER: NA

UNIT AND QTY: **Not fielded. For training use only**

INTEL APPLICATION: IMINT/SIGINT/PSYOP

Unmanned Aerial Vehicle (UAV)-Endurance PREDATOR



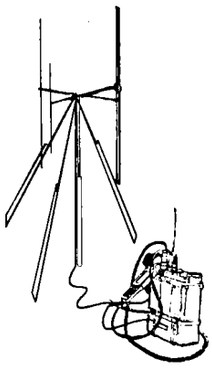
FUNCTION: Operates as stand-off system in all conditions, behind friendly lines; can penetrate into enemy territory; payloads: E-O/FLIR, MTI/SAR, SIGINT, MET, PSYOP, NBC recon, comm/data relay

PRIME MOVER: 2 C-141s or multiple C-130s

UNIT AND QTY: USAF Asset - Deployed in support of Joint Operations

INTEL APPLICATION: IMINT/SIGINT/PSYOP

Lightweight Man-Transportable Radio Direction Finding System (LMRDFS) AN/PRD-12



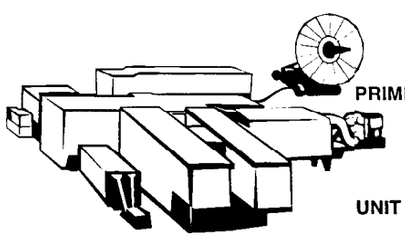
FUNCTION: Lightweight manportable comm intercept/DF system; on emitter location missions, works w/TEAMMATE; ideal in LT, ABN, AASLT, SOF opns; rapid relocation; optimizes collection in fwd AO; CNR for external comm

PRIME MOVER: Manpacked; 60 lbs, carried by 2 soldiers

UNIT AND QTY: 1 - LT ABN; 3 - HVY/AASLT DIV; 3 - ACR; 1 - SEP BDE; 7 - SOF BN; 10 - SOF SA

INTEL APPLICATION: COMINT

Modernized Imagery Exploitation System (MIES)



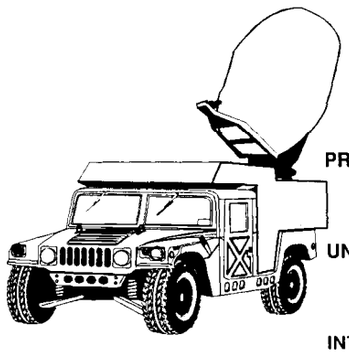
FUNCTION: NRT IMINT; provides exploitation/exploitation mgt, receipt, reporting, SID, archive of imagery & reports; replaces IPDS

PRIME MOVER: 40 ft hardcopy/softcopy exploitation van; 35 ft SATCOM van; 35 ft receive location van; air deployable, C-141, C-5

UNIT AND QTY: Selected MI Bde

INTEL APPLICATION: IMINT

TROJAN SPIRIT (AN/TSQ-190V)



FUNCTION: Satellite terminal; intel processing/dissem, secure voice, data, GPS, FAX, LAN wkstns, video, SID; receive, display, transmit digital imagery, weather/terrain prods among CONUS/OCONUS & deployed

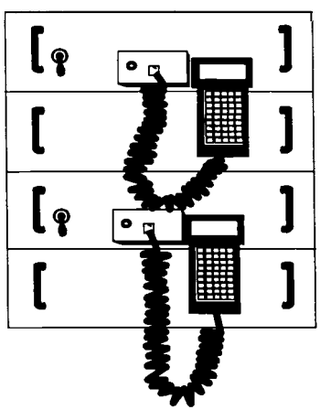
PRIME MOVER: Mounts on 2 heavy variant HMMWVs; tactical SATCOM trailer

UNIT AND QTY: Connectivity: Ft Belvoir TROJAN switching center for worldwide deployment

INTEL APPLICATION: IMINT/SIGINT/CI/ HUMINT/Intelligence Support

---

Synthetic UHF Computer-Controlled Equipment Subsystem (SUCCESS) UHF Radio



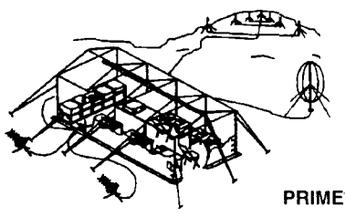
FUNCTION: Auto microprocessor UHF band radio; used w/TENCAP; simultaneous comm when stacked; 2 XMIT/6 RCV channels; SATCOM, point-to-point, TADIXS-B, direct data downlinks; comm w/abn, terrestrial & satellite systems; contains TRE processor

PRIME MOVER: Designed for ground/mobile sheltered environments

UNIT AND QTY: Demand assigned multiple access

INTEL APPLICATION: Intelligence Support

Enhanced TRACKWOLF (AN/TSQ-199)



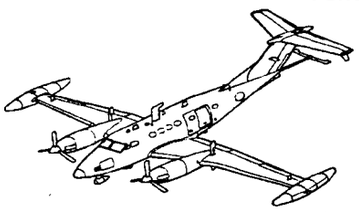
FUNCTION: Targets HF jammers/emitters; 3 netted or stand-alone stations; produces COMINT, TACREPs; spts EAC w/organic long-distance comm resources; open architecture; scaleable tier I-III; external comm via SINCGARS LPI VHF radio, DIN, DSSCS, TROJAN SPIRIT II, SSP-SIGINT, CROSSHAIR, UHF MIL SATCOM (DF Flashnet)

PRIME MOVER: NA

UNIT AND QTY: Special missions at EAC

INTEL APPLICATION: COMINT

Guardrail Common Sensor (GRCS)



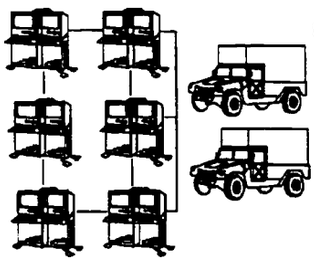
FUNCTION: Collects, identifies, classifies, locates radio signals; provides NRT reporting; gathers LOB & TDOA data; ARF relays platforms btwn IPF & cmds; incorp CHAALS; interfaces w/fixed locations & tactical users; future; expanded coll, LPI capability, embedded trng, 3-channel CTT, retrofit, and auto reporting

PRIME MOVER: Self-deployable; 4 - IPF vans; 3 - IDL trackers

UNIT AND QTY: 1 - Corps AEB

INTEL APPLICATION: ELINT/COMINT

All-Source Analysis System (ASAS)



FUNCTION: Provides auto intel, info & interface data handling for cdrs & ATCCS/ FLCS users; includes IEW sensors, preprocessors, ASAS & FLCS, ABCS HW/SW & info mgt; RWS operates outside ACE

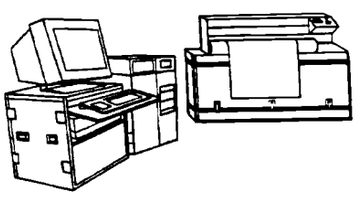
PRIME MOVER: CUCV/HMMWV 5-ton

UNIT AND QTY: 1 ACE set - EAC, Corps, DIV, Sep Bde, ACR; 1 ASAS-RWS at each Bn, Bde & required collateral locations EAC-DIV

INTEL APPLICATION: COMINT/ELINT/IMINT/ CI/HUMINT

Digital Topographic Support System Multi-Spectral Image Processor (DTSS/MSIP)

FUNCTION: Automates terrain TM; produces terrain anal prod; improves response time for IPB; collocated w/ASAS; msg traffic thru MSE; generates/updates multi-spectral imagery; contains 3-D visualization, scanning, map-sizing printer

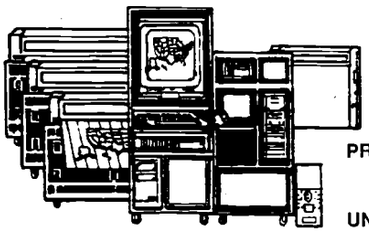


PRIME MOVER: NA

UNIT AND QTY: 1 DIV Terrain TM; 2 - EAC/Corps Terrain TM

INTEL APPLICATION: IMINT/Intelligence Support

Digital Topographic Support System Quick Response Multicolor Printer (DTSS/QRMP)



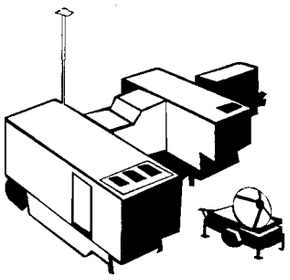
FUNCTION: Automates terrain TM; produces terrain anal prod; improves response time for IPB; collocated w/ASAS; msg traffic thru MSE; provides digital data/terrain anal from battlefield in hard/soft copy

PRIME MOVER: Tactically mobile; 2 LMS-788/gs shelters; 2 HMMWV-H

UNIT AND QTY: 1 DIV Terrain TM; 2 - EAC/Corp Terrain TM

INTEL APPLICATION: IMINT/Intelligence Support

Enhanced Tactical Radar Correlator (ETRAC)



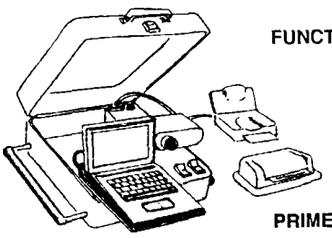
FUNCTION: Advanced mobile SAR processor; receives data from ASAR-2 via U2-R; converts radar to imagery; limited organic exploit for stand-alone opns; includes SUCCESS radio, TENCAP CSP; STU-III, DSVT

PRIME MOVER: Air deployable via C-130, C-141, C-5

UNIT AND QTY: XVIII ABN Corps and V Corps

INTEL APPLICATION: IMINT

CI/HUMINT Automation Tool Set (CHATS)



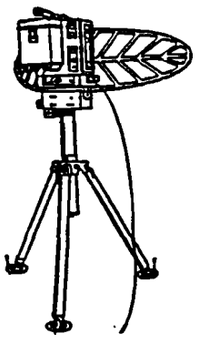
FUNCTION: Provides direct access into CI/HUMINT collateral LAN; uses INMARSAT, TROJAN SPIRIT, SINCGARS, MSE, DSN & phone lines; 2-way data comm; secure FAX; future: GPS, cellular comm, power mgt

PRIME MOVER: 2-manportable cases

UNIT AND QTY: 66th MI Group, Augsburg, GE

INTEL APPLICATION: CI/HUMINT

AN/PPS-5B



FUNCTION: Moving Target Indicators
Range:
6 km-Personnel
10 km-Vehicle

PRIME MOVER: Manpacked and vehicle

UNIT AND QUANTITY: HVY DIV: 12 systems
4/GSR Squad (3)
Survl Plt, I&S Co., MI Bn

AN/PPS-15A

FUNCTION: Moving Target Indicators
Range:
1.5 km-Personnel
3.0 km-Vehicle

PRIME MOVER: Manpacked and vehicle

UNIT AND QUANTITY: LT DIV: 12 systems
3/GSR Squad (4)
Survl Plt, I&S Co., MI Bn

ASSAULT DIV; 8 systems
3/GSR Squad (3)
Survl Plt, I&S Co., MI Bn

ABN DIV: 9 systems
3/I&S Plt (3)
MI Co., (Fwd Spt), MI Bn

APPENDIX H

MILITARY INTELLIGENCE UNITS AND CAPABILITIES

This appendix shows the structure of the MI Battalion (Heavy Division), the MI Battalion (Light Divisions, Airborne, Air Assault), and the Corps MI Brigade. The MI unit structures constitute approved MI force design.

DIVISION MI BATTALION

The MI Battalion (Heavy Division) (Figure H-1) provides dedicated IEW support to the heavy division. It responds to missions assigned by the commander and staff. (MI battalion IEW assets are shown in Appendix G.)

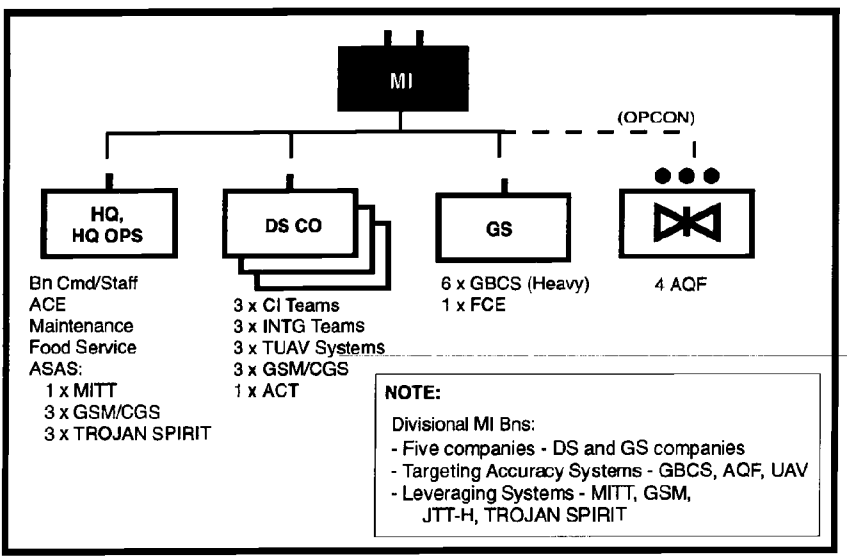


Figure H-1. MI Battalion (Heavy Division).

LIGHT, AIRBORNE, AND AIR ASSAULT DIVISION

The MI Battalion is organized as shown in Figure H-2.

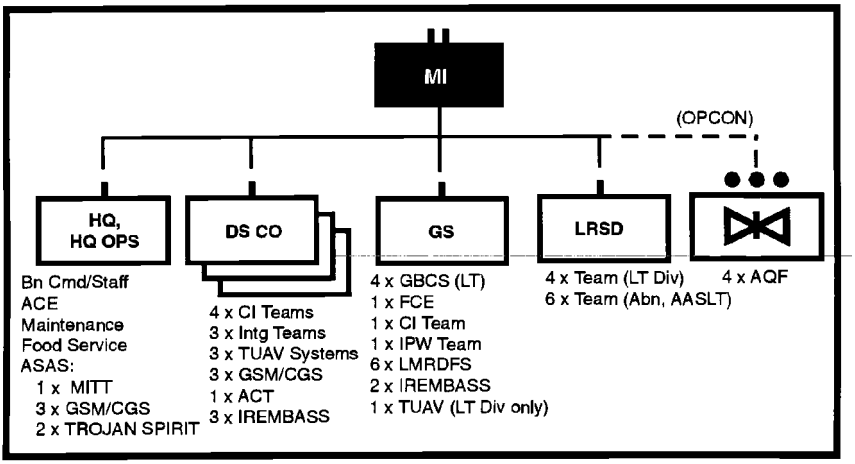


Figure H-2. MI Battalion (Light, Airborne, Air Assault Division).

CORPS MI BRIGADE:

The Corps MI Brigade (Figure H-3) provides dedicated IEW support to the Corps and its subordinate units.

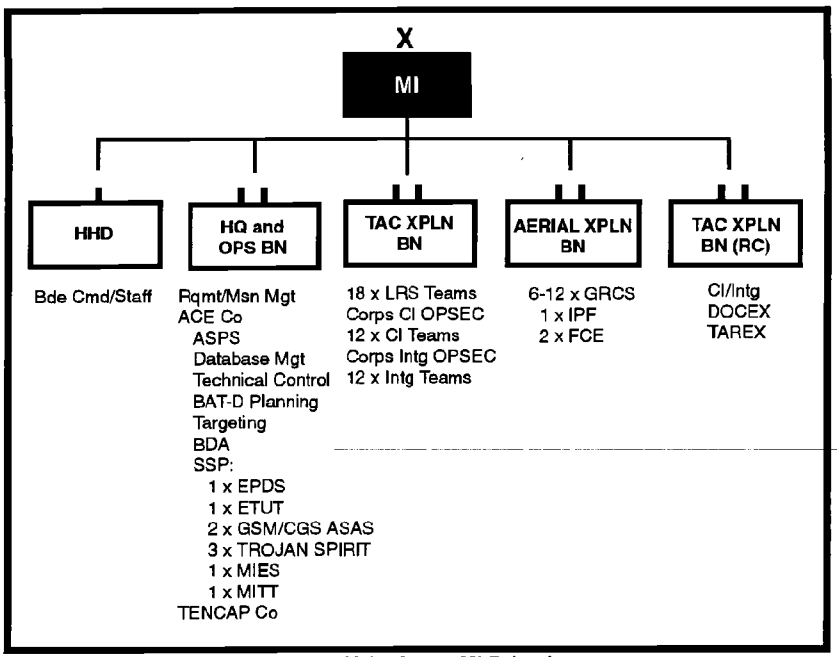


Figure H-3. Corps MI Brigade.

Figures H-4 and H-5 show the organizations of the MI Detachment, Support Company, Special Forces Group and the Special Forces Battalion, respectively.

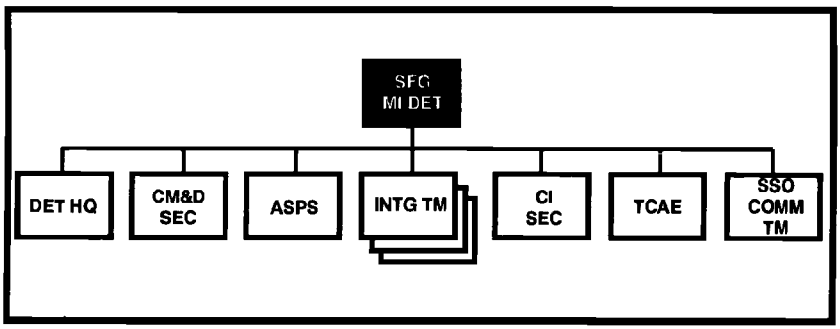


Figure H-4. Organization, MI Detachment, Spt Co, SFG.

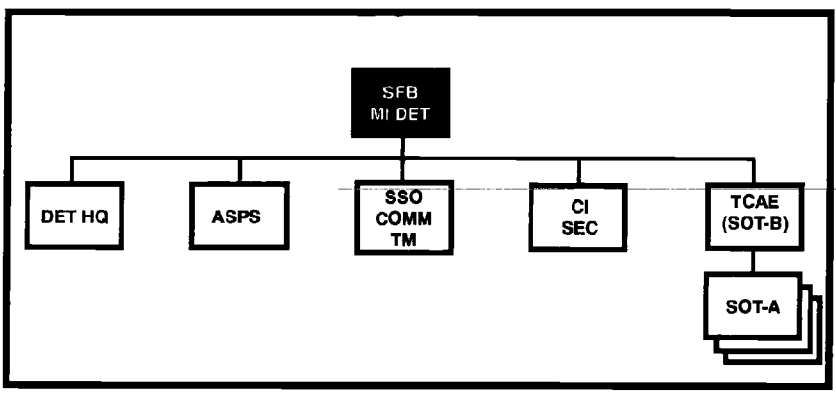


Figure H-5. Organization, MI Detachment, Spt Co, SFB.

APPENDIX I

INTELLIGENCE TRANSITION CHECKLIST

This checklist provides for transition of intelligence responsibility for an area between units. Status of all items listed must be thoroughly coordinated between the transitioning S2s to ensure an effective hand-off of responsibility.

INTELLIGENCE TRANSITION CHECKLIST

_____ CURRENT SITUATION.

_____ Threat disposition:

_____ Maneuver.
_____ Artillery.
_____ Counter-Air.
_____ Intelligence.
_____ Mobility-Countermobility-Survivability.
_____ Logistics.
_____ C^3.
_____ Deception.

_____ Threat strength:

_____ Percentage strength of units.
_____ BDA.

_____ Personnel.
_____ Equipment.
_____ Weapons.
_____ Logistics.

_____ Threat vulnerabilities.
_____ Threat capabilities.
_____ Probable COA.

_____ FRIENDLY INTELLIGENCE SITUATION.

_____ Collection plan.

_____ IMINT.
- _____ Required coverage.
- _____ Focus (CCIRs).

_____ SIGINT.
- _____ Required coverage.
- _____ Focus (EEFI/PIR).

_____ HUMINT.
- _____ NAIs.
- _____ Surveillance.
- _____ CI/IPW.
- _____ DOCEX.
- _____ Focus (RFI/PIR).

_____ Collection asset status.
- _____ Assets.
- _____ Asset schedule - previous 24 hours next 24 hours.

_____ POCs.
_____ Downlinks and COMINT.
_____ Reporting times (as of time to report and due times).
_____ COS/DEA/DOS.

_____ Lists of stay-behind elements.
- _____ Intelligence assets.
- _____ Communications architecture and frequencies.
- _____ CIA.
- _____ DIA national MIST.
- _____ JCMEC and FMIB.

_____ SIGINT.
- _____ Technical data (adds, changes, deletes).
- _____ MCSF.

_____ EPW.
- _____ Numbers, locations, Category A, SOFA.
- _____ Handover to JTF or ARFOR.
- _____ HN handover.

_____ HN Intelligence/security.
- _____ Support, assets, communications.
- _____ POCs and LNOs.

_____ KEY TERRAIN.

_____ MAP UPDATES AND CORRECTIONS.

_____ DETAINABLE, OF INTEREST, AND PROTECTABLE LISTS.

_____ INTELLIGENCE COLLECTION PLAN.

_____ COORDINATION FOR STAY-BEHIND PERSONNEL.

_____ COVER, SECURITY, OPSEC STATUS, AND PLAN.

_____ LIST OF STAY-BEHIND PRODUCTS:

_____ Intelligence map with current situation and sources.

_____ All-source intelligence support and sources.

_____ Imagery products and sources.

_____ Current weather forecast and on-hand weather, light data, and sources.

_____ Historical documents, locations, and sources.

_____ ENCLOSURES:

_____ List of threat, strengths, capabilities, COAs, weaknesses and vulnerabilities, and effects of friendly action.
_____ Threat situation overlays.
_____ Troop list of friendly collectors.
_____ Friendly collector location overlays.
_____ Intelligence communications net diagrams and POC list.
_____ Key terrain overlays.
_____ Map updates and corrections (may be overlay).
_____ Detainable, of interest, and protectable lists.
_____ Intelligence collection plan.

APPENDIX J

INTELLIGENCE REFERENCE LIST

NOTE: This list is not all inclusive. Include the series of field manuals for your particular unit; for example, FM 44-series for Air Defense. Make sure the publications clerk is aware of your requirements. Refer also to the References section in this manual.

AR 190-11	Physical Security of Arms, Ammunition and Explosive
AR 190-13	The Army Physical Security Program
AR 190-14	Carrying of Firearms and Use of Force for Law Enforcement and Security Duties
AR 190-51	Security of Unclassified Army Property
AR 525-13	The Army Combating Terrorism Program
AR 380-5	Department of the Army Information Security Program
AR 380-10	Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives
AR 380-19	Information Systems Security
AR 380-67	The Department of the Army Personnel Security Program
AR 381-1	Security Controls on Dissemination of Intelligence Information
AR 381-10	US Army Intelligence Activities
AR 381-12	Subversion and Espionage Directed Against the US Army (SAEDA)
AR 381-20	The Army Counterintelligence Program
(U) AR 381-172	Counterintelligence Force Protection Source Operations (CFSO) and Low Level Source Operations (LLSO), Secret.
AR 530-1	Operations Security (OPSEC)
FM 1-111	Aviation Brigades
FM 5-30	Engineer Intelligence
FM 5-36	Route Reconnaissance and Classification
FM 6-20	Fire Support in the AirLand Battle
FM 6-20-10	Tactics, Techniques, and Procedures for the Targeting Process
FM 6-121	Tactics, Techniques, and Procedures for Field Artillery Target Acquisition
FM 7-98	Operations in a Low-Intensity Conflict

FM 11-50	Combat Communications Within the Division (Heavy and Light)
FM 17-95	Cavalry Operations
FM 19-1	Military Police Support for the AirLand Battle
FM 19-30	Physical Security
FM 25-100	Training the Force
FM 25-101	Battle Focused Training
FM 33-1	Psychological Operations
FM 34-1	Intelligence and Electronic Warfare Operations
FM 34-2	Collection Management and Synchronization Planning
FM 34-2-1	Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance
FM 34-3	Intelligence Analysis
(U) FM 34-5	Human Intelligence and Related Counterintelligence Operations, Secret.
FM 34-7	Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations
FM 34-8	Combat Commander's Handbook on Intelligence
FM 34-10	Division Intelligence and Electronics Warfare Operations
FM 34-13	Military Intelligence (MI) Battalion, Combat Electronic Warfare Intelligence (CEWI) (Div), Leaders Handbook for Platoons and Teams
FM 34-25	Corps Intelligence and Electronic Warfare Operations
FM 34-25-1	Joint Surveillance Target Attack Radar System (JOINT STARS)
FM 34-25-3	All-Source Analysis System and the Analysis and Control Element
FM 34-36	Special Operation Forces Intelligence & EW Operations
FM 34-37	Echelons Above Corps (EAC) Intelligence & Electronic Warfare (IEW) Operations
(U) FM 34-40	Electronic Warfare Operations, Secret.
(U) FM 34-40-3	Tactical Signals Intelligence (SIGINT) Analysis Operations, Confidential.
FM 34-40-7	Communications Jamming Handbook
FM 34-40-9	Direction Finding Operations
(U) FM 34-40-12	Morse Code Intercept Operations, Confidential.
(U) FM 34-40-13	Electronic Intelligence (ELINT) Operations, Secret.
FM 34-52	Intelligence Interrogation
FM 34-54	Battlefield Technical Intelligence
FM 34-60	Counterintelligence
FM 34-80	Brigade and Battalion Intelligence and Electronic

	Warfare Operations
FM 34-81	Weather Support for Army Tactical Operations
FM 34-81-1	Battlefield Weather Effects
FM 34-82	Military Intelligence Unit Exercise Development Guide
FM 34-130	Intelligence Preparation of the Battlefield
FM 41-10	Civil Affairs Operations
FM 71-3	Armored and Mechanized Infantry Brigade
FM 71-100	Division Operations
FM 90-2	Battlefield Deception
(U) FM 90-2A	Electronic Deception, Secret.
FM 90-14	Rear Battle
FM 90-29	NEO
FM 100-5	Operations
FM 100-6	Information Operations
FM 100-19	Domestic Support Operations
FM 100-20	Military Operations in Low-Intensity Conflict
FM 100-23	Peace Operations
FM 100-25	Doctrine for Army Special Operations Forces
FM 101-5	Staff Organization and Operations
FM 101-5-1	Operational Terms and Graphics
TC 34-55	Imagery Intelligence
Joint Pub 1	Joint Warfare for the US Armed Forces
Joint Pub 1-01 series	Joint Publication System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program
Joint Pub 2-0 series	Joint Doctrine for Intelligence Support to Operations
Joint Pub 3-0 series	Doctrine for Joint Publications
Joint Pub 5-0 series	Doctrine for Planning Joint Operations
(U) Joint Pub 6-02	Joint Doctrine for Employment of Operational/ Tactical Command, Control, Communications, and Computer Systems, Secret.

NOTE: DOCTRINE WRITTEN PRIOR TO 1992 IS BEING REVISED. UPDATE YOUR REFERENCE LIST AS NEW DOCTRINE IS PUBLISHED.

APPENDIX K

WEATHER ELEMENTS AND SUPPORT

A working knowledge of weather elements is essential to provide your commander with a complete picture of potential adverse weather effects on the battlefield.

INTERACTION OF BATTLEFIELD ENVIRONMENT ELEMENTS

Weather conditions, terrain, BIC, illumination, and background signatures are some primary conditions found in a battlefield environment (Figure K-1).

A weather element is an atmospheric variable that is measured in a weather observation. A weather parameter is derived from one or more weather elements. Example: Density altitude is a weather parameter derived from the element's barometric pressure and temperature.

Weather conditions such as wind, precipitation, and clouds can impact or can be influenced by the other conditions of the battlefield. All of these conditions are interdependent, to a certain degree, and must be considered as a whole (Figure K-2).

WEATHER EFFECTS AND TERRAIN

Terrain features affect weather elements such as visibility, temperature, humidity, precipitation, winds, clouds. The most common example of terrain affecting weather is that on the windward side of high terrain, such as mountains, the rainfall rate will be greater than on the leeward (opposite) side.

Weather conditions have a definite effect on the terrain and can enhance or limit military operations such as trafficability, water crossing (fording), and the first-round accuracy of supporting FA fires. The responsibility for determining mobility and counter-mobility is given to the terrain team at division.

ATMOSPHERIC PRESSURE: Atmospheric pressure is the pressure exerted by the atmosphere at a given point and measured by a barometer in inches of mercury (Hg) or in millibars (Mb).

Pressure Altitude: This is indicated in an altimeter when 29.92 is set in the barometric scale window. High pressure altitude is critical to the lift capability of fixed wing aircraft.

Density Altitude: This is a place in the atmosphere corresponding to a particular value of air density. High pressure is critical to helicopter operations.

CLOUDS: The amount of sky covered by clouds is usually described in eighths: Overcast (8/8ths), broken (5 to 7/8ths), or scattered (1 to 4/8ths). Cloud conditions are described by the amount of cloud cover and the height of the base of the cloud AGL. A cloud ceiling is the height of the lowest broken or overcast layer, and is expressed in feet. A higher layer of several scattered layers of clouds is designated as a cloud ceiling when the sum of the coverage of the lower layers exceeds 4/8ths.

DEW POINT TEMPERATURE: Dew point is the temperature to which the air must be cooled for the air to become saturated and allow dew, and probably fog, to form.

HUMIDITY: This is the state of the atmosphere with respect to water vapor content. It is usually expressed as:

Relative Humidity: The ratio between the air's water content and the water content of saturated air.

Absolute Humidity: The measure of the total water content in the air. It is high in the tropical ocean areas and low in the arctic.

PRECIPITATION: Precipitation is any moisture falling from a cloud in frozen or liquid form. Rain, snow, hail, drizzle, sleet, and freezing rain are common types. The intensity of precipitation is described as light, moderate, and heavy.

Light Rain: Drops are easily seen, very little spray, and puddles form slowly, and accumulation is a trace to 0.10 in/h.

Figure K-1. Common weather elements.

Moderate Rain:	Drops are not easily seen, spray noticeable, puddles form rapidly, and accumulation rates are 0.11 to 0.30 in/h.
Heavy Rain:	Drops are not seen, rain comes in sheets with heavy spray, puddles form quickly, and the rate is more than 0.30 in/h.
Light Snow:	Visibility is equal to or greater than 5/8 miles, or 1,000 meters in falling snow; and a trace to 1 in/hr accumulates.
Moderate Snow:	Visibility is 5/16 to ½ statute miles, or 500 through 900 meters in falling snow with 1 to 3 in/hr accumulation.
Heavy Snow:	In heavy snow, visibility is cut to less than 1/4 statute miles, or 400 meters, with more than accumulation of 3 in/h.

TEMPERATURE: Temperature is the value of heat or cold recorded by a thermometer normally at 6 feet AGL at the observation site. Temperatures are normally given in both Fahrenheit and Celsius values. It is sometimes referred to as the ambient air temperature.

VISIBILITY: A measurement of the horizontal distance at the surface or aloft that the unaided human eye can discern a large object or terrain feature. Visibility is reported in meters or fractions of a mile, and is reported as a prevailing value of the visibility in all directions. Thus, a visibility report of 1,600 meters may not reveal that fog is diminishing visibility to 400 meters in the northwest if the observer has good visibility in other directions. However, such an event would typically be carried in the weather observation's remarks section.

WIND SPEED AND DIRECTION: These two measure the rate of movement of the air past a given point and the direction from which the wind is blowing. A gust is a rapid fluctuation in wind speed with a variation of 10 knots or more between peak and lull. Gust spread is the instantaneous difference between a peak and a lull and is important for helicopter operations.

Figure K-1. Common weather elements (continued).

WEATHER ELEMENTS	THRESHOLD VALUES	IMPACTED SYSTEMS
VISIBILITY	1.0 km 3.0 km	•DRAGON, Machine guns. •Main gun, TOW, CAS, thermal viewers.
CLOUDS	500 ft 1,000 ft 1,500 ft 5,000 ft	•NOE operations, airborne, helicopter TA. •CAS. •COPPERHEAD engagements. •Visual reconnaissance, ADA TA.
SURFACE WIND	6 kn 13 kn 18 kn 30 kn	•Chemical. •Airborne-round parachute. •Military free fall-ram air parachutes, artillery smoke loses its effectiveness, artillery fire accuracy. •Helicopter maneuver.
TEMPERATURE	>32^{C}C < 0^{C}C	•Helicopter lift capabilities. •NVG (PVS-5).
WINDCHILL	<10^{C}C	Personnel survival.
PRECIPITATION	Moderate Freezing	•Ground maneuver, chemical, laser systems, GSR. •Ground maneuver.

Figure K-2. IPB weather overlay criteria.

BATTLEFIELD-INDUCED CONTAMINANTS

During combat operations, visibility can become severely reduced by BIC. These contaminants are either induced directly by combatants or occur as by-products from battlefield operations.

Two significant sources of battlefield contaminants are dust produced by HE artillery or mortar rounds and deliberately employed smoke. HE rounds used in a pre-attack barrage not only may kill enemy forces but also may restrict the visibility of your own troops by dust caused by the HE if you do not consider the direction of the wind. Smoke produced by smoke generators, vehicle exhaust emission

systems, smoke pots, indirect fire, and smoke rounds also produce battlefield contaminants.

Wind speed and direction are critical to maintaining an effective smoke screen. Rain can remove BIC quickly. Weather inversions over valley areas can sustain airborne contaminants for long periods.

Other sources of BIC that will lower visibility in the AO are clouds of dust from vehicle traffic or smoke from fires. These types of contaminants not only blind you but also may help your adversary in detecting troop movements and pinpointing your location.

A unique BIC affecting visibility occurs in conditions when temperatures are in the range of -30EC or -22EF or colder. When a source of moisture or water vapor is released into the cold air by internal combustion engines, artillery fires, or launched self-propelled munitions, visibility can be reduced to zero when the moisture freezes instantly and changes into ice fog.

Ice fog may restrict visibility across a whole valley and can linger for hours. Ice fog crystals permit ground objects to be seen from above while severely restricting visibility on the ground—an advantage for aerial reconnaissance.

On airfields an ice fog created by fixed-wing aircraft may cover an entire runway. Visibility can be reduced so that other aircraft cannot take off or land if the wind is calm. The ice fog also draws attention to the airfield location.

Launching missiles such as the TOW in very cold air can create an ice fog. As the TOW moves to the target, the exhaust blast exits into the air where it condenses and creates the ice fog. If the wind is calm, this fog follows the trajectory of the missile and reduces launch point visibility to such an extent that the operator loses sight of the target. Also, the launch point can be identified by threat forces from the condensation trail of the missile.

ILLUMINATION

Natural light is critical in planning operations where NVD are used or in operations timed to use only available light. Natural light values vary as a function of the position of the sun, moon, stars, and clouds. Light data are available from your SWO for any time period and place. These data are particularly important for determining first and last light, moonrise, and moonset, and are most effective for planning use of NVD.

Variables such as altitude, cloud cover, terrain-produced shadows, visibility, and direction of vehicle or aircraft movement in relation to the sun or the moon can also affect light level availability.

Artificial light is intended to increase visibility but, under certain weather conditions, this does not always occur. Example: Low cloud ceilings will limit the area covered and effective time of flares. Rain, snow, or fog can reduce flare effectiveness. However, under the right conditions, cloud cover can enhance the effects of artificial light due to cloud base reflection. Snow- or sand-covered terrain also reflect both natural and artificial light.

BACKGROUND SIGNATURES

Temperature, wind, and precipitation have a major influence on your ability to pick out a target from the background in the infrared spectrum. They also affect seismic (sound and acoustic) signatures. Detection of objects in the infrared spectrum depends on a temperature contrast between the object and its surrounding environment. This difference is known as the background signature.

Snow, rain, and wind influence the background signature because they can change the surface temperature of objects. These elements lower object temperatures and thus reduce the differential between a target and its background.

A heavy layer of snow produces a washout during any part of the day since it causes both the object and the background to exhibit the same temperature.

Precipitation also degrades seismic sensors through the introduction of background noise (rain), while a snow-covered surface will dampen sound and the movement of troops.

SEVERE OR HAZARDOUS WEATHER

In addition to a continuous need for forecast updates, you need non-forecasted or unanticipated severe or hazardous weather warnings. WETMs normally issue severe weather warnings and advisories. Check for the values at which each weather element becomes known as severe. You will be concerned with conditions such as—

- Tornadoes.
- Thunderstorms producing winds in excess of 45 knots and hail greater than 3/4 of an inch.
- Hurricanes and typhoons.
- Precipitation (rain or snow) when X inches fall in Y hours.
- Surface winds in excess of X knots.
- Maximum and minimum temperatures; when a forecast value misses the actual temperature by X degrees.

You want to know that an earlier forecast for light snow was amended to a forecast of a 16-inch accumulation within the next 12 hours. We cannot over emphasize that you need to work with your next higher HQ S2/G2 and the SWO so that your needs are realistically stated and can be supported. All of your weather support needs should be reviewed every 6 months in garrison and as required in the field.

LIGHT DATA

Another weather-related element that your commander needs is light data. NVD and NVG have made many night operations feasible. Your SWO provides official times for sunrise and sunset, BMCT and EECT, BMNT and EENT, length of absolute darkness, moonrise, moonset, lunar phase in percent, and time periods for using NVD and NVG. Light data to support NVD is needed because there are times when there is not enough moon or starlight to use them.

Civil twilight is sufficient for conduct of combat operations while nautical twilight permits most ground movements without difficulty. Nautical twilight allows a general visibility of up to 400 meters (1,320 ft) and lets you distinguish silhouettes from the background.

The actual duration of light varies with latitude and time of year. For example, in the vicinity of 35 to 40 degrees north latitude, civil twilight generally occurs 30 to 45 minutes before sunrise and after sunset. In the tropics, twilight is shorter.

Once light requirements are determined, relay them to your next higher S2 and SWO. This information is important for your commander because he needs to know not only when he can begin friendly military operations (day or night) but also when threat operations could begin.

OTHER CONSIDERATIONS

Although HF radio wave propagation forecasts are not normally available to the SWO, he can make arrangements before he deploys to receive these forecasts. When available, they should be given to every signal and intelligence organization. The SIGO should know that when HF is not effective, it may be because of solar activity rather than enemy jamming.

The USAF Global Weather Central can routinely provide solar forecast products to the SWO even in the field. Other data, such as tidal information and sea state conditions, can be obtained from the SWO but are normally provided only to specific Army units upon request.

RECEIPT OF FORECASTS

Every tactical echelon should receive the weather forecast prepared and briefed to the commander at the next higher echelon. With no SWO at a maneuver brigade, you receive both the forecast briefed at division covering the division AO and the forecast made by the division SWO specifically for your brigade. Each forecast message received should be worked by you to discover the direct weather impacts on your unit.

A commander wants the weather forecast. He also needs the effects and impacts of the forecasted weather interpreted for his specific operations, systems, and personnel. Schedule your forecasts so they arrive in time for you to prepare your commander's briefing.

HOW G2 OR S2 RECEIVE WEATHER SUPPORT

It is your responsibility to provide weather and weather effects information to your commander and supported or subordinate units. Methods may vary among units and echelons. At higher echelons, the SWO has primary responsibility for providing weather support. There, the G2 simply contacts the SWO, states requirements, and receives the needed weather support.

If you have no SWO, you must pass the request up the chain of command to a level where one is assigned. Once your requirements have been validated, weather support products flow back over the same path. In addition to weather forecast products, the SWO can provide specialized weather effects products. You must provide the threshold values used in developing these products.

You alert your commander and staff about the adverse impact of the forecasted weather. You prepare two simple charts to use during your commander's stand-up briefing. You can post these charts in the CP for reference.

Update the charts when a new forecast is issued by the WETM. Methods used in briefing your commander during the morning and evening briefings may vary greatly among commands. The formats below are a guide and should be modified to suit your situation.

The first chart (Figure K-3) illustrates how the weather elements and parameters contained in the forecast might be displayed on the board. Blown up to poster size and covered with acetate, this chart can be updated easily.

WEATHER FORECAST
VALID FOR 121200Z to 131200Z

LOCATION: PUNGSAN

24-HOUR FORECAST:

SKIES:	CLEAR MORNING AND NIGHT, PARTLY CLOUDY IN THE AFTERNOON, BASES 3,000 FEET.
VISIBILITY:	UNLIMITED, OCCASIONALLY 1 TO 2 MILES IN BLOWING SNOW DURING AFTERNOON.
WINDS:	NORTH TO NORTHWEST, 10 TO 15 KNOTS, OCCASIONAL GUSTS TO 25 KNOTS IN AFTERNOON.
TEMPERATURES:	MAX: 10EF MIN: -20EF

72-HOUR OUTLOOK:

CLOUDY SKIES, SNOW FLURRIES DURING AFTERNOON HOURS LOWERING VISIBILITY TO 2 TO 4 MILES.

TEMPERATURES: MAX: 20EF MIN: -5EF

LIGHT DATA:

BMNT: 1247Z MOONRISE: 1924Z
BMCT: 2221Z MOONSET: 0819Z
SUNRISE: 2251Z
SUNSET: 0820Z NVG USE:
EECT: 0851Z

Figure K-3. Example of a weather forecast chart.

Figure K-4 shows color codes as one way to display potential weather impacts on operations, systems, and personnel in your unit. Another way would be to write the words "moderate" and "severe" in those blocks affected. Do not list all the equipment or systems, but have the list available to answer questions posed by the commander or staff. Stress those critical systems during the verbal portion of your briefing.

If the weather conditions change significantly during the period covered by the SWO's forecast, then an updated impact chart will have to be prepared. Because a brigade or battalion's AI is small, the SWO's forecast is likely to be uniform across the AI.

WEATHER IMPACT CHART
PERIOD 121200Z to 131200Z

IMPACTED ITEMS	CLOUDS	PRECIPI-TATION	WIND	VISIBILITY	TEMPER-ATURE
NBC DEFENSE	GREEN	GREEN	GREEN	GREEN	RED
NIGHT VISION DEVICES	GREEN	GREEN	GREEN	AMBER EXCEPT 07 /0 05Z	AMBER
CSS	GREEN	AMBER	AMBER	AMBER	AMBER
TOW/DRAGON	GREEN	GREEN	AMBER	GREEN	RED
M-1/M-2	GREEN	GREEN	GREEN	GREEN	AMBER
SMOKE/ CHEMICAL	GREEN	GREEN	AMBER	GREEN	GREEN
GROUND RADAR	GREEN	GREEN	AMBER	GREEN	GREEN
PERSONNEL	GREEN	GREEN	RED	GREEN	RED
THREAT	GREEN	GREEN	GREEN	AMBER	GREEN

GREEN No impact
AMBER Moderate impact (Normal effectiveness reduced 25 to 75%)
RED Severe impact (Normal effectiveness reduced to 0 to 25%)

Figure K-4. Example of a weather impacts display chart.

CRITICAL WEATHER FACTORS

Figure K-5 shows major critical weather factors that can enhance or degrade combat operations, systems, and personnel.

LOW VISIBILITY:	Low visibility (less than 3 km). • Can be beneficial to threat and friendly forces. • Conceals the center of gravity and maneuver of offensive forces. • Increases possibility of achieving surprise. • Disadvantages. –Hinders $C^{2.}$ –Reduces effectiveness of R&S and TA, especially during the defense.
SURFACE WINDS:	• Strong winds can reduce effectiveness of downwind forces by blowing dust, smoke, sand, rain, or snow on them. • Upwind force generally has better visibility and can advance faster and easier. • Strong winds limit airborne and aviation (primarily helicopters) operations. • Winds in excess of 35 knots can— –Cause personal injury. –Damage materiel and structures. –Create false radar returns. –Reduce visibility because of blowing sand, dust, and other battlefield debris.
PRECIPITATION:	• Affects trafficability, visibility, personnel effectiveness, and a wide variety of tracked and wheeled military equipment. • Heavy rains can make some unsurfaced, low-lying, and off-road areas impassable.

Figure K-5. Critical weather factors.

	• Both rain and snow can drastically reduce personnel effectiveness by limiting visibility, causing discomfort, increasing fatigue, and creating other physical and psychological problems.
CLOUD COVER:	• The type and amount of cloud cover and the altitude of cloud bases and tops influence aviation operations. • CAS employing fixed-wing aircraft would like a ceiling of at least 2,500 feet (762 m), but can be employed with ceilings as low as 500 feet. • Threat CAS rotary-wing aircraft and aerial resupply missions require a minimum ceiling of 300 feet (100 m). • Affects ground operations by reducing illumination and visibility or by enhancing effects of artificial light.
TEMPERATURE AND HUMIDITY:	• Have a direct impact on personnel and vehicle performance. • Excessively high temperatures cause heat-related injuries to personnel and vehicle engine wear that leads to equipment failure. • Very low temperatures increase cold weather injuries, cause damage to vehicle cooling systems and engines, decrease the effectiveness of vehicle lubrication, and create excessive logistics requirements.

Figure K-5. Critical weather factors (continued).

WEATHER EFFECTS ON THREAT SYSTEMS

MILITARY ASPECTS OF WEATHER:

US Forces must be prepared to fight in a variety of climatic conditions on short notice. Key to accomplishing our missions under any circumstances is

understanding how weather affects both friendly and threat forces and their operations, systems, and personnel.

Current weather conditions and weather forecasts for the AO and AI are analyzed to determine the effects on friendly and enemy operations. This is significant when threat forces have the capability to employ NBC weapon systems.

THREAT EQUIPMENT:

Some of the major arms merchants today are the former Soviet Union, Sweden, Brazil, Britain, Germany, France, Italy, and the United States. However, the major arms purchasers continue to be the underdeveloped or Third-World countries in the Middle East, Latin America, and Asia.

The types of threat equipment we may encounter on future battlefields will vary from artillery and mortars produced during World War II to the Austrian-produced GHN-45, a 155-mm towed gun with a range of 39,600 meters (using ERFB-BB technology). Almost all the Third-World countries have bought or made their own versions of Soviet-produced tanks, APCs, artillery, AAA, and assorted SAM and SSM systems. Tables K-1, K-2, and K-3 list the weather effects from cloud ceilings, reduced visibility, and precipitation, respectively.

Table K-1. Weather effects from cloud ceilings.

WEATHER VALUE (FEET)	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/ EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
LT 1,000			SA-9 SAM SA-14 SAM	
LT 2,500			ZU-23 ZSU-23-4 SA-13 (Contrast mode) SA-16 SA-19	

Table K-2. Weather effects from reduced visibility.

WEATHER VALUE (METERS)	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/ EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
LT 200			RPG-18 (RL) AKM/AKMS (7.62-mm) TKN-1T infrared periscope	ATW Rifle E-O device
LT 500	SA-14 GREMLIN SAM SA-13 SAM SA-16 SAM SA-19 (FSU) SAM		OU-3GK White infrared search light RPG-7 (GL) PT-76 (5.45-mm) AK-74	E-O device ATW AG/LT Rifle
LT 600			ERYX	
LT 750	SA-9 GASKIN SAM			
LT 800	AT-2 SWATTER AT-3 SAGGER AT-6 SPIRAL	ATGM ATGM ATGM	ASU-85 BMD (73-mm) BMP (73-mm) Sniper rifle, SVD RPK-74, squad AGS-17, GL RPG-16, GL	AG/LT LAV LAV Rifle MG

Table K-2. Weather effects from reduced visibility (continued).

WEATHER VALUE (FEET)	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/ EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
LT 1,000	All Types	ATGM	SPG-9 (73 mm recoilless rifle) SD-44 (85-mm) 14.5-mm KPU hvy MG 7.62-mm PKT MG DShK NSV/NSVT PK Series MT-LB 7.62-mm coaxial machine gun for all tanks	ATW ATW AA AA MG MG LAV MT
LT 1,500			7.62-mm 15.5-mm heavy BTR-50,-60,-70 (14.5-mm) KPVT ACRV M1974 DShK NSV/NSVT T-54, T-55, T-62 (main gun)	MG MG AA/LAV AA LAV MG MG MT
LT 2,000			T-12, MT-12 (100-mm) KPVT BRDM-2 (14.5-mm) T-80, T-72, T-64 (main gun) MATHOGO MILAN 2 RBS-56 SPIGOT	ATW MG LAV MT

Table K-2. Weather effects from reduced visibility (continued).

WEATHER VALUE (METERS)	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/ EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
LT 2,500			SA-7 GRAIL ZU-23 ZSU-23-4	FSU SAM AA AA
LT 3,000			RED ARROW 73 RED ARROW 8 SUSONGP'O AT-3 SAGGER	
LT 4,000			SA-9 GASKIN HOT 2 SWINGFIRE AT-2 SWATTER AT-5 SPANDREL AT-8 SONGSTER AT-10 STABBER SA-13 (contrast mode)	 FSU SAM FSU SAM
LT 4,500			MAPATS	
LT 5,000			NIMROD AT-6 SPIRAL AT-11 SNIPER SWIFT (SF)	ATGM
LT 6,000			120-mm, M-1943 S-60 (57-mm)	MO AA
LT 8,000			160-mm, M-160	MO

Table K-3. Weather effects from precipitation.

WEATHER CONDITION	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
Light rain			LOW BLOW (fire control) STRAIGHT FLUSH (12gHz) (tracking) THIN SKIN (height finder)	SAM radar SAM radar SAM radar
Moderate rain			STRAIGHT FLUSH (acquisition)	SAM radar
Heavy rain			LOW BLOW (fire control) THIN SKIN (height finder)	SAM radar SAM radar
	NOTE: The list of AD radars on this page should be considered as a sample of the various other types of threat radars associated with EW operations and tactical and strategic SAM systems. Not listed are a large variety of threat combat equipment (wheeled and tracked) affected by moderate or heavy rain and snow.			

WEATHER AND ENVIRONMENTAL ELEMENTS AND PARAMETERS IMPACTING ARMY SYSTEMS AND OPERATIONS:

Table K-4 is compiled from a study conducted by the US Army Intelligence School as part of the IEWMAA. Each TRADOC branch was asked to survey the impact of weather and environmental elements on their operations, systems, and personnel and rate them as either **essential (E)** or **desired (D)**. Also included are other Army agencies' requirements.

- **E**—Some positive action had to be taken by the user based on severe current or forecasted weather conditions.

- **D**—Some impact, but the degree of impact is uncertain or not mission-threatening.

For each element or parameter listed, at least one responder identified it as essential for one or more of their operations, systems, or personnel.

Some data elements and parameters are known to have an impact, but exact critical thresholds have not been determined. Others cannot be measured or sensed with present technology. But identifying these data elements or parameters now allows for further research in how to collect the raw data (where applicable), determine the frequency of collection, establish data accuracy, and learn other supporting information.

As users and planners continue to learn more about weather and environmental impacts, the misconception that there is a hypothetical Army "all-weather" system or operation fades.

Table K-5 shows windchill factors.

Table K-4. Weather and environmental data elements impacting Army systems and operations.

WEATHER AND ENVIRONMENTAL DATA ELEMENTS IMPACTING ARMY SYSTEMS/OPERATIONS

A = AIR DEFENSE
B = ADJUTANT GENERAL
C = ARMOR
D = AVIATION
E = CHAPLAIN
F = DEFENSE AMMUNITION CENTER
G = ENGINEER
H = FIELD ARTILLERY
I = FINANCE
J = HEALTH SERVICES
K = INTELLIGENCE
L = INFANTRY
M = JUDGE ADVOCATE
N = MILITARY POLICE
O = CHEMICAL
P = ORDNANCE
Q = ORDNANCE M&M
R = PUBLIC AFFAIRS
S = QUARTERMASTER
T = SIGNAL
U = SPECIAL FORCES
V = SOLDIER SUPPORT
W = TRANSPORTATION
X = JOINT READINESS TRNG CENTER

REQUIREMENT DESIGNATORS: E = ESSENTIAL SUPPORT NEEDS D = DESIRABLE SUPPORT NEEDS

SPECIAL GROUP CATEGORIES: (GS) = GROUND STATE (SS) = SEA STATE (SW) = SEVERE WEATHER CRITERIA

DATA ELEMENT	CATEGORY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1. ALTIMETER SETTING					E						E	E										E			
2. ATMOSPHERIC CONTAMINANTS				E	D	D	E	D		E	E								D			D			
3. ATMOSPHERIC DENSITY								E			E											E			
4. ATMOS. TRANSMISSION COEFFICIENT								E																	
5. BAROMETRIC PRESSURE		D		E	E				E		E	E										E			E
6. CLOUD COVER AMOUNT		D		E	E		E	E	E		E	E	E		D	E			D			D	E	E	E
7. CLOUD BASE HEIGHT		E			E		E	E	E		E	E	E	D		E						E		E	E
8. CLOUD TOP HEIGHT					E						E	E										D			
9. DAMAGING WINDS	[SW]	E	E	E	E	E	D	E	E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E
10. DENSITY ALTITUOE					E						E	E										E			E
11. EXTINCTION COEFFICIENT									E			E										D			
12. EXTREME HEAT/COLO	[SW]	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
13. FLOODING, RIVER STAGE	[GS]	E	E	E	E	E		E	D	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
14. FREEZE/THAW DEPTH	[GS]	D		E	E			E	D		E	E	E		E	D	E	E		E	E	D			E
15. FREEZING PRECIPITATION	[SW]	E	E	E	E	E		E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
16. HEAVY RAIN/SNOW	[SW]	E	E	E	E	E	D	E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
17. HUMIDITY, ABSOLUTE		D			E			E			E	E				E						E			E
18. HUMIDITY, ABSOLUTE, PROFILE		D			E			E			E	E				E						E			E
19. HUMIDITY, RELATIVE							E	E	D		E	E				E			E			D	E	E	E
20. HUMIDITY, RELATIVE, PROFILE									E													D			
21. HURRICANES/TYPHOONS	[SW]	E	E	E	E	E		E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
22. ICE/SNOW DEPTH/COVER	[GS]	D		E	E			E	D		E	E	E		E	D	D	E		E	E	D			E
23. ICING, FLIGHT	[SW]				E						E	E	E									E			E
24. ILLUMINATION		E		E	E			E	E		E	E	E		E		D			D		E	E	E	E
25. IR TARGET/BACKGROUND CONTRAST				E	E				D		E	D										E			E
26. IR THERMAL CONTRAST X-OVER TIME				E	E				D		E	E										E			E
27. IONOSPHERIC DISTURBANCES					D						D	E									E	E			
28. LIGHT DATA		E		E	E		D	E	D		E	E	E		D	D				D	D	E		D	D
29. LIGHTNING/THUNOERSTORMS	[SW]				D		E	E	E		D	E								E		E			E
30. LITTORAL CURRENT	[SS]				D		D	E			D	D	E									E			
31. PRECIPITATION, ACCUMULATION			D	E	E	D	D	E	D	D	E	E	E		E	D	E		D	E	E	E	E	E	D

Table K-4. Weather and environmental data elements impacting Army systems and operations (continued).

DATA ELEMENT	CATEGORY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
32. PRECIPITATION, RATE		E	D		E	D		E	E	D	E	E	E	D	E	E	D		D	E	E	E	E	E	E
33. PRECIPITATION, HAIL SIZE		E			E			E	D		E	E			E		E			E		D			
34. PRECIPITATION, TYPE		E	D	E	E	D		E	E	D	E	E	E	D	E	E	D		D	E	E	E	E	E	E
35. PRESSURE ALTITUDE				E							E	E	E								E			E	
36. REFRACTIVE INDEX		E		E	E				D		E	E			D										
37. RESTRICTION TO VISIBILITY				E				E	D		D	E			E	E				E	E	E			E
38. SEEABILITY (MILLIMETER WAVE, INFRARED, ULTRAVIOLET)		E		E	E			E	E		E	E	E		E	D					E		E	D
39. SEVERE WEATHER CONDITIONS	[SW]	E	E	E	E	E		E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
40. SNOW STATE CONDITION	[GS]	D		E	E			E	E		E	E	E		E	D	D	E		E	E	D			E
41. SNOW DRIFT DEPTH	[GS]	D			D			E	D		D	E	E		E		E			D	E	E			E
42. SOIL/GROUND MOISTURE	[GS]	D		E	E		D	E	D		E	E	E		E	D	D	E		D	E	D			E
43. SOIL/GROUND TEMPERATURE	[GS]	D		E	E		D	E	D		E	E	E		E		E		D	D		E	E	E	E
44. SOLAR RADIATION							E				D	D										E			
45. STABILITY INDEX							E					E				E									E
46. STANDING WATER/POOLING	[GS]	D		E	E	D		E	D		E	E	E		E	D	D	E	D	E	E	D			E
47. STATIC ELECTRICITY POTENTIAL					E						E	E													
48. SURF HEIGHT	[SS]				D			E			D	D	E									E		E	
49. SWELL DIRECTION/HEIGHT	[SS]				D						D	D	E									E		E	
50. TEMPERATURE, AIR, SURFACE		E	E	E	E	E	E	E	E	E	E	E	E		E	E	D	E		D	E	E	E	E	E
51. TEMPERATURE, AIR, PROFILE					E		E		E		E	E										D			
52. TEMPERATURE, AIR, UPPER AIR					E				E		E	E										D			E
53. TEMPERATURE, DEWPOINT				E	E				D		E	E										E			E
54. TEMPERATURE, DEWPOINT, PROFILE					E				E		E	E										D			
55. TEMPERATURE, WINDCHILL FACTOR			D		D	D		E	D	D	E	E	E	D	E		E		D	E		E	E	E	
56. TEMPERATURE, INVERSION LEVEL(S)					E		E		E		E	E				E						D			E
57. TEMPERATURE, SEA SURFACE	[SS]				D			E			D	D	E									E		E	
58. TEMPERATURE, WATER, INLAND	[GS]				D			E			D	E	E									E		E	
59. TEMPERATURE, WBGT					D			E	D		E	E			E	E	E			E		E			E
60. TORNADO	[SW]	E	E	E	E	E		E	E	E	E	E		E	E	E	D	E	E	E	E	E	E	E	E	E
61. TURBULENCE, FLIGHT					E						E	E										E			
62. TURBULENCE, OPTICAL				E	E			E	E		E	D										E			
63. VISIBILITY, VISIBLE SPECTRUM, ALOFT					E				E														E		E
64. VISIBILITY, VISIBLE SPECTRUM, SFC		E			E			E	E		E	E	E		E	E	D			E		E	E		E
65. WAVE PERIODICITY	[SS]				D						D	D	E									E		E	
66. WAVE DIRECTION/HEIGHT	[SS]				D						D	D	E									E		E	
67. WIND, PROFILE					E				E		E	E										E			
68. WIND, PROFILE, TARGET, AGL - 3KM					E				E							E									
69. WIND, SHEAR					E						E	E										E			E
70. WIND, SURFACE, SPEED/DIRECTION		E		E	E		E	E	E		E	E	E		E	E	D	E	D	D	E	E	E	D	E
71. WIND, SURFACE, GUST SPEED				E			D	E	E		E	E	E		D						E	E			E
72. WIND, SURFACE, GUST SPREAD					E				E		E	E										E			E
73. WIND, UPPER AIR, SPEED/DIRECTION		E			E				E		E	E				E						E			E

Table K-5. Windchill chart.

WIND SPEED (KNOTS)	WIND SPEED (MPH)	LOCAL TEMPERATURE (EF)										
		32	23	14	5	-4	-13	-22	-31	-40	-49	-58
		EQUIVALENT TEMPERATURE (EF)										
	CALM	32	23	14	5	-4	-13	-22	-31	-40	-49	-58
4	5	29	20	10	1	-9	-18	-28	-37	-47	-56	-65
9	10	18	7	-4	-15	-26	-37	-48	-59	-70	-81	-91
13	15	13	-1	-13	-25	-37	-49	-61	-73	-85	-97	-109
17	20	7	-6	-19	-32	-44	-57	-70	-83	-96	-109	-121
21	25	3	-10	-24	-37	-50	-64	-77	-90	-104	-117	-127
26	30	1	-13	-27	-41	-54	-68	-82	-97	-109	-123	-137
30	35	-1	-15	-29	-43	-57	-71	-85	-99	-113	-127	-142
35	40	-3	-17	-31	-45	-59	-74	-87	-102	-116	-131	-145
39	45	-3	-17	-31	-45	-59	-74	-87	-102	-116	-131	-145
43	50	-4	-18	-33	-47	-62	-76	-91	-105	-120	-134	-148
		LITTLE DANGER FOR PROPERLY CLOTHED PERSONS		**CONSIDERABLE DANGER**			**VERY GREAT DANGER**					
DANGER FROM FREEZING OF EXPOSED FLESH												

HOT WEATHER ENVIRONMENT:

In hot weather, important factors are temperature and relative humidity. Primary concerns are physical exhaustion and dehydration. You must consider both because a common work task will take longer and additional water may have to be transported during hot weather. The following are specific concerns:

Water Adequacy. Water supplies and the enforcement of its intake before, during, and after physical activity is critical for survival.

Workload Correlation. Adapt workload or training activities to environmental heat stress conditions.

Rest Periods. Provide adequate break time for physically active personnel in a hot environment.

Chilled Drinking Water. Soldiers will often reject warm drinking water even when they are significantly dehydrated.

Physical Activity. Soldiers' introduction to physical exertion in a hot climate upon arriving from a temperate climate should be as gradual as circumstances allow. They will need 1 to 2 weeks' time to physiologically adjust to the new climate. Lighten physical activity during this period to ensure optimum performance.

Salt. Sodium intake must be maintained in hot weather. Two good meals a day normally provide enough salt for most soldiers.

Humidity. A low WBGT index (e.g., in the morning) may not be a totally safe indicator if the humidity is high. High humidity retards cooling by evaporation of sweat and decreases the urge to drink sufficient water.

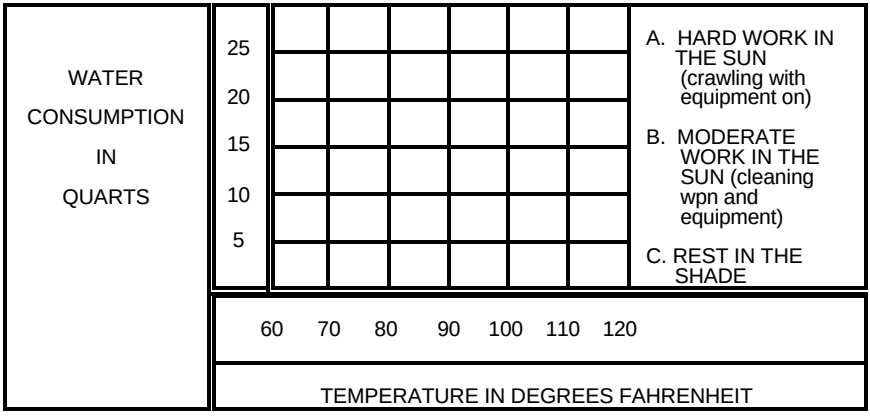
Water Spray. A water mist will cool a person. But it should never be substituted for adequate consumption of water before, during, and after strenuous activities in the heat.

The SWO can provide temperature measurement, forecast, and relative humidity forecasts from the following tables. If you need air temperature values measured at your particular location, use the thermometer included in the FALOP BWK.

HOT WEATHER WATER REQUIREMENTS:

Table K-6 shows the water needs for soldiers at 3 activity levels over an 8-hour work period. To determine soldiers' average water needs, you have to know the air temperature and decide the level of activity the troops will be doing. Example: If a soldier is doing 8 hours of hard work in the sun (curve C) when the average temperature for the day is 100EF, his water requirements for the day will be around 15 quarts. This amount of water can be converted into extra weight the soldier must carry. One quart is equal to 2 pounds, so the 15 quarts of water would weigh 30 pounds.

Table K-6. Daily water consumption requirement s for three levels of activity.



HOT WEATHER WORK TIME LIMITS:

Table K-7 shows the time limits during which work can be performed safely in hot weather. In computing the time limits, consider both air temperature and relative humidity. The values are based on a sitting soldier in BDUs doing light work. Do not consider these tables as absolute limits—especially since light, moderate, or heavy work are difficult to quantify. Table K-8 indicates work time in hot weather based on the WBGT index. Table K-9 shows conversion factors.

Table K-7. Work time in hot weather operations.

TEMPERATURE		RELATIVE HUMIDITY (%)					
(EC)	(EF)	10	30	50	70	90	100
60	140	1 HR	.25 HR				
54	130	2 HR	.5 HR	.25 HR	NO WORK RECOMMENDED		
49	120	4 HR	2 HR	.5 HR	.25 HR		
43	110	12 HR	4 HR	2 HR	.5 HR	.25 HR	
38	100	NO LIMIT	12 HR	4 HR	2 HR	1 HR	.5 HR
32	90	WITH PRECAUTIONS			12 HR	6 HR	4 HR

Table K-8. WBGT index (light work).

HEAT CONDITION/ CATEGORY *	WBGT(^{o}F)	WATER INTAKE QUARTS/HOUR	WORK/REST CYCLE (MINUTES)
1	78.0 to 81.9	AT LEAST ½	CONTINUOUS
2	82.0 to 84.9	AT LEAST 1.2	50/10
3	85.0 to 87.9	AT LEAST 1	45/15
4	88.0 to 89.9	AT LEAST 1-½	30/30
5 **	90.0 and ABOVE	MORE THAN 2	20/40

* MOPP gear or body armor adds at least 10 ^{o}F to the WBGT index.
** Suspend PT and strenuous activity. If operational (non-training) mission requires strenuous activity, enforce water intake to minimize expected heat injuries.

Table K-9. Conversion factors.

TO CONVERT:	TO:	USE:
	TEMPERATURE	
Degrees F	Degrees C	$^0C = 5/9\ ^0F - 32)$
Degrees C	Degrees F	$^0F = (9/5\ ^0C) + 32$
	DISTANCE	
Kilometers	Miles	0.62
Kilometers	Nautical Miles	0.54
Kilometers	Feet	3,280.80
Miles	Kilometers	1.61
Miles	Nautical Miles	0.87
Miles	Yards	1,760.00
Miles	Feet	5,280.00
Nautical Miles	Kilometers	1.85
Nautical Miles	Miles	1.15
Meters	Feet	3.28
Yards	Feet	3.00
	SPEED	
Kilometers/Hour	Miles/Hour	0.62
Kilometers/Hour	Knots (Nautical Miles/Hour)	0.54
Miles/Hour	Kilometers/Hour	1.61
Miles/Hour	Knots	0.87
Miles/Hour	Feet/Second	1.467
Knots	Kilometers/Hour	1.85
Knots	Miles/Hour	1.15
Meters/Second	Feet/Second	3.281
Meters/Second	Miles/Hour	2.237
	PRESSURE	
Inches of Mercury (Hg)	Millibar	33.86395
Millibar (Mb)	Inches of Mercury	0.295299
	LENGTH	
Feet Meters	0.3048	
Feet Centimeters	30.48	
Inches	Meters	0.0254
Inches	Centimeters	2.54
Meters	Yards	1.094
Yards	Meters	0.9144

GLOSSARY

Section I. Acronyms and Abbreviations

A

A	as acquired (effect used in AGM)
AA	avenue of approach
AAA	air avenue of approach
AAM	air-to-air missile
AAO	Army Aviation Officer
AAR	after-action report
AASLT	air assault
ABCS	Army Battle Command System
abn	airborne
AC	Active Component
ACE	analysis and control element
ACofS	Assistant Chief of Staff
ACR	armored cavalry regiment
ACT	analysis and control team
AD	air defense
ADA	air defense artillery
ADO	air defense officer
ADP	automated data processing
AEB	aerial exploitation battalion
AEPDS	Advanced Electronic Processing and Dissemination System
AF	audio frequency
AFATDS	Advanced Field Artillery Tactical Data System
AFSO	aerial fire support observer
AGL	above ground level
AG/LT	assault gun/light tank
AGM	attack guidance matrix
AI	area of interest
ALO	air liaison officer
ALOC	administrative and logistics center
AMSS	Automatic Meteorological Sensor System
AO	area of operations
AOB	air order of battle
APC	armored personnel carrier
AQF	Advanced QUICKFIX

AR	Army Regulation
ARF	airborne relay facilities
ARFOR	Army force
ARL	airborne reconnaissance low
ARSOF	Army Special Operations Forces
arty	artillery
ASAR	Advanced Synthetic Aperture Radar
ASAS	All-Source Analysis System
ASM	air space management
ASPS	all-source production section
asst	assistant
AT	antitank
ATCCS	Army Tactical Command and Control System
ATGM	antitank guided missile
ATK	attack
ATR	automated target recognition
ATW	antitank weapon
AUTL	Army Universal Task List
auto	automated
avn	aviation
AVTR	airborne video tape recorder
AWACS	Airborne Warning and Control System

B

B	bomber
BAT-D	battlefield deception
BCTP	battle command training program
BDA	battle damage assessment
BDE	brigade
BDU	battle dress uniform
BHL	battle handover line
BIC	battle-induced contaminants
BICC	battalion information control center
BMCT	beginning of morning civil twilight
BMNT	beginning of morning nautical twilight
BMO	battalion maintenance officer
bn	battalion
BOS	battlefield operating system
BP	battle position
BWK	belt weather kit

C

C^2	command and control
C^2I	C^2 and intelligence
C^2W	command and control warfare
C^3	command, control, and communications
C^3I	C^3 and intelligence
C^4I	C^3, computers, and intelligence
C^4I^2	C^4I and information
CA	Civil Affairs/combat assessment
CALL	Center for Army Lessons Learned
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CAS	close air support
Cas Evac	casualty evacuation
CATK	counterattack
CB	counterbattery
cbt	combat
CBU	cluster bomb unit
CCIR	commander's critical information requirements
CCM	cross-country movement
CCMEC	Combined Captured Materiel Exploitation Center
CD	counter-drug
CDMP	combat decision-making
CDR	commander
CEE	captured enemy equipment
CEM	captured enemy materiel
CFE	Conventional Forces In Europe
CFL	coordinated fire line
CFSO	Counterintelligence Force Protection Source Operations
CGS	J-STARS common ground station
CHAALS	Communication High Accuracy Airborne Location System
CHARIOT	Portable S-Band Receive/Transmit Terminal
CHATS	CI/HUMINT Automation Tool Set
chem	chemical
CI	counterintelligence
CIA	Central Intelligence Agency
CINC	commander in chief
CIP	Command Inspection Program
CIR	critical intelligence requirements
CM	collection management
cmd	command

CMEC	Captured Materiel Exploitation Center
CMISE	Corps Military Intelligence Support Element
CMO	civil-military operations
CNR	combat net radio
co	company
COA	course of action
COIN	counterinsurgency
coll	collection
COLT	combat observation lasing team
COMINT	communications intelligence
comm	communications
COMMEX	communications exercise
COMSEC	communications security
CONPLAN	contingency plan
CONUS	continental United States
coord	coordination
COP	command observation post
COR	chief of reconnaissance
COS	critical occupational speciality
CP	command post
CS	combat support
CSBM	Confidence and Security Building Measures
CSP	communications system processor
CSS	combat service support
CSR	controlled supply rate
CTC	combat training center
CTT	commander's tactical terminal
CUCV	commercial utility cargo vehicle

D

D	destroy (effect used in AGM); desirable (weather designator)
DA	Department of the Army
DDMP	deliberate decision-making process
DEA	Drug Enforcement Administration
DF	direction finding
DIA	Defense Intelligence Agency
DIN	Defense Intelligence Network
DISE	Deployable Intelligence Support Element
dissem	dissemination
div	division

DMP	decision-making process
DOCEX	document exploitation
DOD	Department of Defense
DOS	Department of State
DP	decision point
DS	direct support
DSN	Defense Secure Network
DSSCS	Defense Special Security Communications System
DST	decision support template
DSVT	digital subscriber voice terminal
DTG	date-time group
DTSS/MSIP	Digital Topographical Support System/Multi-Spectral Image Processor
DTSS/QRMP	Digital Topographical Support System/QUICK-Response Multicolor Printer
DZ	drop zone

E

E	essential (weather designator)
EA	electronic attack; engagement area (used in AGM)
EAC	echelons above corps
ECB	echelons corps and below
ECOA	enemy course of action
EECT	end of evening civil twilight
EEFI	essential elements of friendly information
EENT	end of evening nautical twilight
EFVS	electronic fighting vehicle system
e.g.	for example
ELINT	electronic intelligence
EM	electromagnetic
ENGR	engineer
E-O	electro-optical
EP	electronic protection
EPB	electronic preparation of the battlefield
EPDS	Electronic Processing and Dissemination System
EPW	enemy prisoner of war
ERFB-BB	extended-range full-bore-based bleed
ES	electronic warfare support
est	estimated
etc	and so forth
ETRAC	Enhanced Tactical Radar Correlator

ETUT	Enhanced Tactical Users Terminal
EW	electronic warfare
EWO	electronic warfare officer
EWS	early warning system
EWTL	electronic warfare target list
EXEVAL	external evaluation

F

°F	degree Fahrenheit
F	fighter (sortie category)
FA	field artillery
FAC	forward air controller
FAIO	field artillery intelligence officer
FALOP	forward area limited observation program
FARP	forward arming and refueling point
FAST	Forward Area Support Terminal
FAST-I	Forward Area Support Terminal-Improved
FAX	facsimile
FBIS	Foreign Broadcast Information Service
FCE	fire control element
FDA	functional damage assessment
FDC	fire direction center
FDO	fire direction officer
FEBA	forward edge of the battle area
FFIR	friendly forces information requirements
FISTV	first support team vehicle
FLCS	Force Level Control System
FLIR	forward-looking infrared
FLOT	forward line of own troops
flt	flight
FM	field manual
FMC	fully mission capable
FMIB	Foreign Materiel Intelligence Battalion
FO	forward observer
FofF	field of fire
FRAGO	fragmentary order
FS	fire support
FSB	forward support battalion
FSC	fire support center
FSCL	fire support coordination line
FSCM	fire support coordinating measure

FSCOORD	fire support coordinator
FSE	fire support element
FSO	fire support officer
FSOP	field standing operating procedure
FSU	fire support unit
ft	feet
FTI	fixed target indicator
F/W	fixed wing
fwd	forward

G

G2	Assistant Chief of Staff, G2 (Intelligence)
GBCS-(H/L)	ground-based common-sensor (heavy/light)
GCI	ground control intercept
GE	Germany
GHz	gigahertz
GL	grenade launcher
GPS	global positioning system
GRCS	GUARDRAIL Common Sensor
GS	general support
GSM	J-STARS ground station module
GSR	ground surveillance radar

H

H	harrassing fires
HA	humanitarian assistance
HE	high explosive
HF	high frequency
Hg	mercury
HHD	headquarters and headquarters detachment
HHOC	headquarters, headquarters and operations company
HMMWV	high mobility multipurpose wheeled vehicle
HN	host nation
HPT	high-payoff target
HPTL	high payoff target list
HQ	headquarters
hr	hour
HUMINT	human intelligence
HVT	high-value target
hvy	heavy

H/W	hardware

I

I	immediate (effect used in AGM)
IAW	in accordance with
I&S	intelligence and security
I&W	indications and warnings
ID	identify
IDL	interoperable data link
IEW	intelligence and electronic warfare
IEWCS	Intelligence Electronic Warfare Common Sensor
IEWMAA	IEW mission area analysis
IFV	infantry fighting vehicle
IHL	intelligence handover line
IMA	individual mobilization augmentee
IMETS	Integrated Meteorological System
IMINT	imagery intelligence
incorp	incorporate
INF	Intermediate-range Nuclear Forces intelligence
infil	infiltration
info	information
in/h	inches per hour
INMARSAT	International Maritime Satellite
intel	intelligence
intg	interrogation
INTSUM	intelligence summary
IO	information operations
IPB	intelligence preparation of the battlefield
IPDS	Imagery Processing and Dissemination System
IPF	integrated processing facility
IPS	intelligence production section
IPW	interrogation, prisoners of war
IR	information requirements
I-REMBASS	Improved Remotely Monitored Battlefield Sensor System
ISA	International Standardization Agreement
ISB	intelligence support base
ISM	intelligence synchronization matrix
ISSO	information systems security officer
IVL	intervisibility lines

J

J2	Intelligence Directorate
JCMEC	Joint Captured Materiel Exploitation Center
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Center
J-SIIDS	Joint-Service Interior Intrusion Detector System
JSTARS	Joint Surveillance Target Attack Radar System
JTAGS	Joint Tactical Ground Station
JTF	joint task force
JTT/H	joint tactical terminal/hybrid
JTT/H-R3	joint tactical terminal/hybrid-receive only

K

km	kilometer

L

LAN	local area network
LAV	light armored vehicle
LC	line of contact
LD	line of departure
LEA	Law Enforcement Agency
LLSO	low-level source operations
LLVI	low-level voice intercept
LMRDFS	Lightweight Man-Transportable Radio Direction Finding System
LNO	liaison officer
LOA	limit of advance
LOB	line of bearing
LOC	line of communication
LOS	line of sight
LP	listening post
LPI	low probability of intercept
LRP	long-range patrol
LRRP	long-range reconnaissance patrol
LRS	long-range surveillance
LRSD	long-range surveillance detachment
LRSU	long-range surveillance unit
LRU	long-range unit
LT	light
LTIOV	latest time information is of value
LZ	landing zone

M

m	meter
MASINT	measurement and signals intelligence
Mb	millibar
MC	movement corridor
MC&G	mapping, charting, and geodesy
MCOO	modified combined obstacles overlay
MCSF	Mobile Cryptologic Support Facility
MDCI	multidiscipline counterintelligence
MDMP	military decision-making process
MEA	munitions effects assessment
med	medium
MEDEVAC	medical evacuation
MET	meteorological
METL	mission essential task list
METT-T	mission, enemy, terrain and weather, troops, and time available
METT-TC	mission, enemy, terrain and weather, troops, and time available civilians
MEWSS	Mobile Electronic Warfare Support System
MGS	magnetic grid system
mgt	management
MI	military intelligence
MIES	Modernized Imagery Exploitation System
MIJI	meaconing, intrusion, jamming, and interference
min	minute
MIPB	Military Intelligence Professional Bulletin
MIRS	Miniaturization Imagery Receive System
MIST	military intelligence support team
MITT	Mobile Integrated Tactical Terminal
MLRS	multiple launch rocket system
MOPP	mission-oriented protection posture
MP	military police
MR	moon rise
MS	moon set
MSE	mobile subscriber element
MT	medium tank
MTI	moving target indicator
MTOE	modified table of organization and equipment
MTP	mission training plan

N

N	north; neutralize (effect used in AGM)
NA	not applicable
NAI	named area of interest
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCA	National Command Authority
NCO	noncommissioned officer
NEO	noncombatant evacuation operation
NFA	no fire area
NGIC	National Ground Intelligence Center
NGLO	naval gunfire liaison officer
NGO	non-governmental organization
NIMA	National Imagery Mapping Agency
NIST	National Intelligence Support Team
NLT	no later than
nmi	nautical miles
NOD	night observation device
NOE	nap of the earth
noncomm	noncommunications
NRT	near-real time
NVD	night vision devices
NVG	night vision goggles

O

OB	order of battle
OCOKA	obstacles & fields of fire, concealment & cover, key terrain, and avenues of approach
OCONUS	outside continental United States
O/O	on order
OOTW	operations other than war (see SASO)
OP	observation post
OPCON	operational control
OPLAN	operations plan
opns	operations
OPORD	operations order
OPSEC	operations security
OR	operational readiness
OT	operator terminal

P

P	planned
PAO	public affairs office

PDA	physical damage assessment
PEO	peace enforcement operations
photo	photography
PGM	precision-guided munitions
PIR	priority intelligence requirements
PKO	peacekeeping operations
plt	platoon
PMCS	preventive maintenance checks and services
POL	petroleum, oils, lubricants
PP	passage point
prep	preparation
PSA	post-strike assessment
PSYOP	psychological operations
PT	physical training
PVO	private volunteer organization
PZ	pickup zone

Q

QSTAG	Quadripartite Standardization Agreement
qty	quantity

R

R	reconnaissance (sortie category)
R&D	research and development
R&S	reconnaissance and surveillance
RAS	rear area security
RBP	red/black processor
RC	Reserve Components
RCOA	reconnaissance course of action
rcv	receive
RDC	rear detachment commander
recon	reconnaissance
REDTRAIN	readiness training
regt	regiment
REMBASS	Remotely Monitored Battlefield Sensor System
RFI	request for information
RII	request for intelligence information
RISTA	reconnaissance, intelligence, surveillance, and target acquisition
RL	rocket launcher
RNP	radio navigational points (USAF)
ROE	rules of engagement

ROTERM	receive only terminal
RP	release point
rqmts	requirements
RRS	radio relay system
RRT	radio receiver transmission
RRTS	radio relay test set
RSOP	readiness standing operating procedure
RSR	required supply rate
RTO	radiotelephone operator
R/W	rotary wing
RWS	remote workstation

S

S	South; suppress (effect used in AGM)
SA	small arms
S&TI	Scientific & Technical Intelligence
S1	Adjutant (US Army)
S2	Intelligence Officer (US Army)
S3	Operations and Training Officer (US Army)
S4	Supply Officer (US Army)
S5	Civil Affairs Officer (US Army)
SAEDA	Subversion and Espionage Directed Against the US Army
SALUTE	size, activity, location, unit, time, and equipment
SAM	surface-to-air missile
SAR	synthetic aperture radar
SASO	stability and support operations (formerly OOTW)
SATCOM	satellite communications
SCI	sensitive compartmented information
SDO	staff duty officer
SDS	security data system
SEAD	suppression of enemy air defenses
sep bde	separate brigade
SF	Special Forces
SI	special intelligence
SID	secondary imagery dissemination
SIDS	Secondary Imagery Dissemination System
SIGINT	signals intelligence
SIGINT/EW	signals intelligence/electronic warfare
SIGO	signal officer
SII	statement of intelligence interest

SINCGARS	Single-Channel Ground and Airborne Radio System
SIR	specific information requirements
SITMAP	situation map
SJA	Staff Judge Advocate
SLAR	side-looking airborne radar
SOCCE	Special Operations Command and Control Element
SOF	special operations forces
SOFA	Status of Forces Agreement
SOI	signals operating instructions
SOP	standing operating procedure
SOR	specific orders and requests
SOT-A	support operations team-Alpha
SOT-B	support operations team-Bravo
SP	start point
SPIRIT	Special Purpose Integrated Remote Intelligence Terminal
sqdn	squadron
SR	sunrise
SS	sunset
SSM	surface-to-surface missile
SSO	special security office
SSP	single-soure processing
ST	student text
STANAG	Standardization Agreement
STU III	Secure Telephone Unit-Third Generation
SUCCESS	Synthesized UHF Computer Controller Enhanced Subsystem
survl	surveillance
S/W	software
SWO	staff weather officer

T

TA	target acquisition
TAA	tactical assembly area
TAB	target acquisition battery
tac	tactical
TAC	tactical command post
TACFIRE	tactical fire direction system
TACLINK	tactical link
TACSAT	tactical satellite

TADIXS-B	Tactical Data Information Exchange System-Broadcast
TAI	target area of interest
TAREX	target exploitation
TB	tank brigade
TD	tank division
TDA	target development assessment
TDDS	TRAP Data Dissemination System
TDMP	tactical decision-making process
TDOA	time differential of arrival
TECHINT	technical intelligence
TENCAP	Tactical Exploitation of National Capabilities
TF	task force
tgt	target
THAADS	Theater High Altitude Area Defense System
THMT	tactical high mobility terminal
TIBS	Tactical Information Broadcast System
TLE	target location error
TLP	troop-leading procedures
TOC	tactical operations center
TOPS	Tactical Onboard Processing System (for TADIXS-B)
TOW	tube-launched, optically tracked, wire-guided
TPL	time phase line
TRAP	Tactical Related Applications
TRIXS	Tactical Reconnaissance Intelligence Exchange System
trng	training
TROJAN SPIRIT	Special Purpose Integrated Remote Intelligence Terminal
TRRIP	Theater Rapid Response Intelligence Package
TSA	target system assessment
TSOP	tactical standing operating procedure
TSS	target selection standards
TTP	tactics, techniques, and procedures
TUAV	tactical unmanned aerial vehicle
TVA	target value analysis

U

UAV	unmanned aerial vehicle
UBL	unit, basic load
UHF	ulltra high frequency
USAF	US Air Force
USMTF	United States Message Text Formats
USSID	United States Signal Intelligence Directive

UW	unconventional warfare
	V
VHF	very high frequency
vis	visibility
	W
w	with
WARNO	warning order
WATCHCON	watch condition
WBGT	wet-bulb-globe temperature
WETM	weather team
wkstn	workstation
wpn	weapon
	X
XO	executive officer
XPLN	exploitation
xmit	transmit

Section II. Terms.

Global security forecast. A forecast of where, when, and between whom conflicts can occur.

Battlefield development plans. A 5- to 20-year forecast of how selected threat forces will organize and operate on the battlefield.

Automated and hardcopy databases. Databases such as the Stylized Country Force Assessments and the Army Force Planning and Data Assumptions which provide detailed projections on OB, equipment, logistics, and readiness (ground, air, naval forces) of potential threats 2 to 25 years into the future.

TECHINT and User Bulletins. Provide a high resolution view of threat equipment and weapons systems and capabilities, and complement traditional OB information. They can be obtained from NGIC.

Open source studies and articles. State Department background papers, FBIS, public libraries, universities, and corporations with contracts in countries of interest). Databases of sources need to be researched and exercised in advance of mission execution.

Other services. The USMC, other nation's information, fact books, and fact sheets on tactics, terrain, and country studies.

REFERENCES

SOURCES USED

These are the sources quoted or paraphrased in this publication.

AR 381-10	*US Army Intelligence Activities.* 1 Jul 84.
FM 6-20-10	*Tactics, Techniques, and Procedures for the Targeting Process (MCRP 3-1.6.14).* 8 May 96
FM 17-95	*Cavalry Operations.* 24 Dec 96.
FM 33-1	*Psychological Operations (FMFM 3-53).* 18 Feb 93.
FM 34-1	*Intelligence and Electronic Warfare Operations.* 27 Sep 94.
FM 34-2	*Collection Management and Synchronization Planning.* 8 Mar 94.
FM 34-2-1	*Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance.* 19 Jun 91.
FM 34-3	*Intelligence Analysis.* 15 Mar 90.
FM 34-8	*Combat Commander's Handbook on Intelligence.* 28 Sep 92.
FM 34-25-3	*All-Source Analysis System and the Analysis and Control Element.* 3 Oct 95.
FM 34-37	*Echelons Above Corps (EAC) Intelligence & Electronic Warfare (IEW) Operations.* 15 Jan 91.
(U) FM 34-40	*Electronic Warfare Operations* , 9 Oct 87, Secret.
FM 34-130	*Intelligence Preparation of the Battlefield.* 8 Jul 94.
FM 41-10	*Civil Affairs Operations.* 11 Jan 93.
FM 100-6	*Information Operations.* 27 Aug 96.
FM 100-17	*Mobilization, Deployment, Redeployment, Demobilization.* 28 Oct 92.
FM 101-5	*Staff Organizations and Operations.* 25 May 84.
FM 101-5-1	*Operational Terms and Symbols.* 21 Oct 85.
Joint Pub 1-02	*Department of Defense Dictionary of Military and Associated Terms.* 23 Mar 94.
Joint Pub 6-04.11	*US Message Text Formatting Program Repository of USMTF Program Items for US Implementation Guidance.* 1 Oct 91.

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

AR 190-11	*Physical Security of Arms, Ammunition and Explosives.* 30 Sep 93.
AR 190-13	*The Army Physical Security Program.* 30 Sep 93.

AR 190-14	*Carrying of Firearms and Use of Force for Law Enforcement and Security Duties.* 12 Mar 93.
AR 190-51	*Security of Unclassified Army Property (Sensitive and Nonsensitive).* 30 Sep 93.
AR 525-13	*The Army Combatting Terrorism Program.* 25 Feb 88.
AR 380-5	*Department of the Army Information Security Program.* 25 Feb 88.
AR 380-10	*Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives.* 30 Dec 94.
AR 380-19	*Information Systems Security.* 1 Aug 90.
AR 380-67	*The Department of the Army Personnel Security Program.* 9 Sep 88.
AR 381-1	*Controls of Dissemination of Intelligence Information.* 12 Feb 90.
AR 381-12	*Subversion and Espionage Directed Against the US Army (SAEDA).* 15 Jan 93.
AR 381-20	*The Army Counterintelligence Program.* 15 Nov 93.
(U) AR 381-172	Counterintelligence Force Protection Source Operations *(CFSO) and Low Level Source Operations (LLSO),* Secret.
AR 530-1	*Operations Security (OPSEC).* 3 Mar 95.
FM 1-111	*Aviation Brigades.* 27 Aug 90.
FM 3-4	*NBC Protection (FMFM 11-9) (reprinted w/basic Incl C1).* 29 May 92.
FM 3-5	*NBC Contamination (FMFM 11-10).* 17 Nov 93.
FM 3-50	*Smoke Operations.* 4 Dec 90.
FM 5-30	*Engineer Intelligence (reprinted w/Basic Incl C1).* 22 Sep 67.
FM 5-34	*Enginer Field Data.* 14 Sep 87.
FM 5-36	*Route Reconnaissance and Classification.* 10 May 85.
FM 6-20	*Fire Support in the AirLand Battle.* 17 May 88.
FM 5-100	*Engineer Operations.* 27 Feb 96.
FM 5-101	*Mobility.* 23 Jan 85.
FM 5-102	*Countermobility.* 14 Mar 85.
FM 5-103	*Survivability.* 10 Jan 85..
FM 6-121	*Tactics, Techniques, and Procedures for Field Artillery Target Acquisition.* 25 Sep 90.
FM 7-7	*The Mechanized Infantry Platoon and Squad.* 15 Mar 85.
FM 7-7J	*Mechanized Infantry Platoon & Squad (BRADLEY).* 7 May 93.
FM 7-8	*Infantry Rifle Platoon and Squad.* 22 Apr 92.
FM 7-10	*The Infantry Rifle Company.* 14 Dec 90.
FM 7-20	*The Infantry Battalion.* 6 Apr 92.
FM 7-70	*Light Infantry Platoon & Squad.* 10 Sep 86
FM 7-71	*Light Infantry Company.* 28 Aug 87.
FM 7-92	*The Infantry Reconnaissance Platoon and Squad (Airborne, Air Assault, Light Infantry).* 23 Dec 92.
FM 7-93	*Long-Range Survival Unit Operations.* 3 Oct 95.

FM 10-14-2	*Guide for the Battalion S4 (reprinted w/Basic Incl C1).* 30 Dec 81.
FM 10-14-3	*Surveying Officer's Guide.* 30 Dec 81.
FM 11-30	*MSE Communications in the Corps/Division.* 27 Feb 91.
FM 11-32	*Combat Net Radio Operations.* 15 Oct 90.
FM 11-37	*MSE Primer for Smal-Unit Leaders.* 14 Nov 90.
FM 11-50	*Combat Communications Within the Division (Heavy and Light).* 4 Apr 91.
FM 17-15	*Tank Platoon.* 3 Apr 96.
FM 17-95	*Cavalry Operations.* 24 Dec 96.
FM 17-95-10	*The Armored Cavalry Regiment and Squad.* 22 Sep 93.
FM 17-97	*Cavalry Troop.* 3 Oct 95.
FM 17-98-1	*Scout Leader's Handbook.* 24 Sep 90.
FM 19-1	*Military Police Support for the AirLand Battle.* 23 May 88.
FM 19-30	Physical Security. 1 Mar 79.
FM 19-40	*Enemy Prisoners of War, Civilian Internees and Detained Persons.* 27 Feb 76.
FM 21-26	*Map Reading and Land Navigation.* 7 May 93.
FM 21-31	*Topographical Symbols (reprinted w/Basic Incl C1).* 19 Jun 61.
FM 25-100	*Training the Force.* 15 Nov 88.
FM 25-101	*Battle Focused Training.* 30 Sep 90.
(U) FM 34-5	*Human Intelligence and Related Counterintelligence Operations,* 29 Jul 94, Secret.
FM 34-7	*Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations.* 18 May 93.
FM 34-10	*Division Intelligence and Electronics Warfare Operations.* 25 Nov 86.
FM 34-13	*Military Intelligence (MI) Battalion, Combat Electronic Warfare Intelligence (CEWI) (Div), Leaders Handbook for Platoons and Teams.* 15 Apr 83.
FM 34-25	*Corps Intelligence and Electronic Warfare Operations.* 30 Sep 87.
FM 34-25-1	*Joint Surveillance Target Attack Radar System (JOINT STARS).* 3 Oct 95.
(U) FM 34-25-6	*Tactics, Techniques, and Procedures for the Electronic Processing & Dissemination System ,* 15 Jun 92, Secret.
(U) FM 34-25-7	Special Electronic Mission Aircraft (SEMA) Survivability 3 Oct 95, Secret.
FM 34-35	*Armored Cavalry Regiment (ACR) and Separate Brigade Intelligence and Electronic Warfare (IEW) Operations.* 12 Dec 90.
FM 34-36	*Special Operation Forces IEW Operations.* 30 Sep 91.
(U) FM 34-40-3	*Tactical Signals Intelligence (SIGINT) Analysis Operations,* 21 May 91, Confidential

FM 34-40-7	*Communications Jamming Handbook.* 23 Nov 92.
FM 34-40-9	*Direction Finding Operations.* 29 Aug 91.
(U) FM 34-40-12	*Morse Code Intercept Operations* , 26 Aug 91, Confidential.
(U) FM 34-40-13	*Electronic Intelligence (ELINT) Operations,* 10 Sep 91, Secret.
FM 34-52	*Intelligence Interrogation.* 28 Sep 92.
FM 34-54	*Battlefield Technical Intelligence.* 5 Apr 90.
FM 34-60	*Counterintelligence.* 3 Oct 95.
FM 34-80	*Brigade and Battalion Intelligence and Electronic Warfare Operations.* 15 Apr 86.
FM 34-81	*Weather Support for Army Tactical Operations (AFM 105-4).* 31 Aug 89
FM 34-81-1	*Battlefield Weather Effects.* 23 Dec 92.
FM 34-82	*Military Intelligence Unit Exercise Development Guide.* 26 Nov 85.
FM 71-3	*Armored and Mechanized Infantry Brigade.* 8 Jan 96.
FM 71-100	*Division Operations.* 28 Aug 96.
FM 90-2	*Battlefield Deception.* 3 Oct 88.
(U) FM 90-2A	*Electronic Deception,* 12 Jun 89, Secret.
FM 90-7	*Combined Arms Obstacle Integration.* 29 Sep 94.
FM 90-14	*Rear Battle.* 10 Jun 85.
FM 90-29	*Noncombatant Evacuation Operations.* 17 Oct 94.
FM 100-2-2	*The Soviet Army: Specialized Warfare and Rear Area Support.* 16 Jul 84.
FM 100-2-3	*The Soviet Army: Troops, Organization and Equipment.* 16 Jun 91.
FM 100-5	*Operations.* 14 Jun 93.
FM 100-13	*Battefield Coordination Detachment (BCD).* 5 Sep 96.
FM 100-19	*Domestic Support Operations. (FMFM 7-10).* 1 Jul 93.
FM 100-20	*Military Operations in Low-Intensity Conflict (AFP 3-20).* 5 Dec 90.
FM 100-23	*Peace Operations.* 30 Dec 94.
FM 100-25	*Doctrine for Army Special Operations Forces.* 12 Dec 91.
FM 101-10-1/1	*Staff Officer's Field Manual-Organizational, Technical, and Logistical Data (Volume 1).* 7 Oct 87.
FM 101-10-1/2	*Staff Officer's Field Manual-Organizational, Technical, and Logistical Planning Factors (Volume 2) (reprinted w/Basic Incl C1).* 7 Oct 87.
ST 101-5	*Command and Staff Decision Processes*
ST 101-9	*The Tactical Decisionmaking Process*
TC 12-17	*Adjutant's Call/The S1 Handbook.* 17 Mar 92.
TC 34-55	*Imagery Intelligence.* 3 Oct 88.
Joint Pub 1	*Joint Warfare for the U.S. Armed Forces.* 10 Jan 95.
Joint Pub 2-0	*Joint Doctrine for Intelligence Support to Operations.*

5 May 95.

Joint Pub 3-0	*Doctrine for Joint Operations*. 1 Feb 95.
Joint Pub 5-0	*Doctrine for Planning Joint Operations.* 13 Apr 95.
Joint Pub 6-02	*TAC C4 Systems.*
(U) Joint Pub 6-02	*Joint Doctrine for Employment of Operational/Tactical Comand, Control, Communications, and Computer System,* 1 Oct 96, Secret.
DA Form 2028	*Recommended Changes to Publications and Blank Forms.* 1 Feb 74.
DA Form 3964	*Classified Document Accountability Record.* Jul 79.

By Order of the Secretary of the Army:

DENNIS J. REIMER
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
04459

DISTRIBUTION:

Active Army, Army National Guard, and U. S. Army Reserve: To be distributed in accordance with initial distribution number 115447, requirements for FM 34-8-2.

DIRECTOR'S READING LIST

2018

DEFENSE INTELLIGENCE AGENCY

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

As intelligence officers, our most critical asset is our mind. Self-study increases our speed, creativity, and confidence.

Without self-study, our expertise is limited to our direct experiences. Reading vastly multiplies our experiences in life—as parents, as friends, as spouses, and as leaders.

By reading, we can learn from the experiences of an immeasurable number of people. And, hopefully, our reading allows us to learn from the mistakes of others, before we make those mistakes ourselves. Old ideas give us new ideas. History really does teach us something. It inspires, motivates, and elevates us.

Lieutenant General Robert P. Ashley, Jr.
Director, Defense Intelligence Agency

"Not all readers are leaders,
but all leaders are readers."

HARRY S. TRUMAN
33RD PRESIDENT
OF THE UNITED STATES OF AMERICA

National Archives (111-P-20038A)

"The problem with being too busy to read is that you learn by experience (or by your men's experience), i.e. the hard way. By reading, you learn through others' experiences, generally a better way to do business, especially in our line of work where the consequences of incompetence are so final for young men. Thanks to my reading, I have never been caught flat- footed by any situation, never at a loss for how any problem has been addressed (successfully or unsuccessfully) before. It doesn't give me all the answers, but it lights what is often a dark path ahead."

JAMES N. MATTIS
UNITED STATES SECRETARY OF DEFENSE
GENERAL, UNITED STATES MARINE CORPS (RET.)

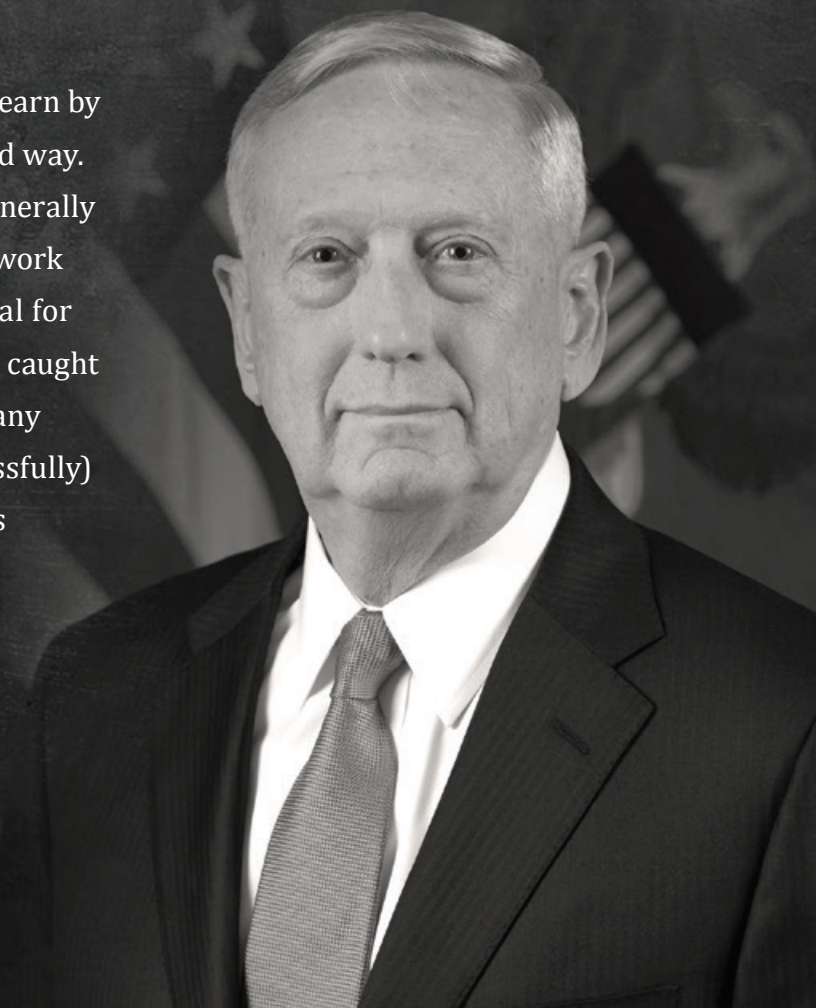


TABLE OF CONTENTS

★★★ The three star icon indicates titles the Director has read.

01 LEADERSHIP AND PROFESSIONAL DEVELOPMENT

01	American Ulysses: A Life of Ulysses S. Grant ★★★	05
02	Anticipating Surprise: Analysis for Strategic Warning	05
03	The Art of War ★★★	06
04	The Craft of Intelligence: America's Legendary Spymaster on the Fundamentals of Intelligence Gathering for a Free World	06
05	Duty: Memoirs of a Secretary at War ★★★	07
06	The Emperor's Handbook: A New Translation of the Meditations ★★★	07
07	Fighting Talk: Forty Maxims on War, Peace, and Strategy ★★★	08
08	The First 90 Days: Proven Strategies for Getting Up to Speed Faster and Smarter ★★★	08
09	The Five Dysfunctions of a Team: A Leadership Fable	09
10	Good Strategy / Bad Strategy ★★★	09
11	Grey Eminence: Fox Conner and the Art of Mentorship ★★★	10
12	How Everything Became War and the Military Became Everything: Tales from the Pentagon ★★★	10
13	It Worked for Me: In Life and Leadership	11
14	Legacy ★★★	11
15	Make Your Bed – Little Things That Can Change Your Life… and Maybe the World ★★★	12
16	A Message to Garcia ★★★	12
17	Nineteen Stars: A Study in Military Character and Leadership ★★★	13
18	On Killing: The Psychological Cost of Learning to Kill in War and Society ★★★	13
19	On War ★★★	14
20	One Bullet Away: The Making of a Marine Officer	14
21	Outliers: The Story of Success ★★★	15
22	Pearl Harbor: Warning and Decision	15
23	Power Rules: How Common Sense Can Rescue American Foreign Policy	16
24	Predictably Irrational, Revised and Expanded Edition: The Hidden Forces That Shape Our Decisions	16
25	Psychology of Intelligence Analysis	17
26	Resilience: Hard-Won Wisdom for Living a Better Life ★★★	17
27	The Rise and Fall of Intelligence: An International Security History	18
28	Scales on War: The Future of America's Military at Risk ★★★	18
29	Sources of Power: How People Make Decisions	19
30	The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations ★★★	19
31	Superforecasting	20
32	Team of Rivals: The Political Genius of Abraham Lincoln	20
33	Team of Teams: New Rules of Engagement for a Complex World	21
34	Thinking Fast and Slow	21
35	War ★★★	22

TABLE OF CONTENTS

02 HISTORY

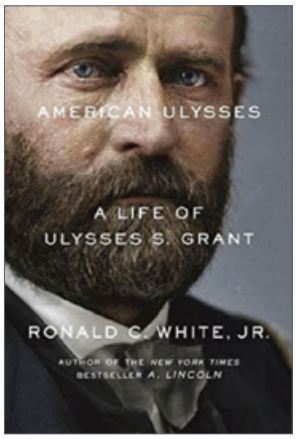
36	1776 ★★★	24
37	An Army at Dawn: The War in North Africa 1942-1943 (The Liberation Trilogy)	24
38	Ashley's War: The Untold Story of a Team of Women Soldiers on the Special Ops Battlefield	25
39	Band of Brothers: E Company, 506th Regiment, 101st Airborne from Normandy to Hitler's Eagle's Nest ★★★	25
40	Black April: The Fall of South Vietnam, 1973-1975	26
41	Black Hearts: One Platoon's Descent into the Madness of Iraq's Triangle of Death ★★★	26
42	The Churchill Factor: How One Man Made History ★★★	27
43	Combat Ready?: The Eighth U.S. Army on the Eve of the Korean War ★★★	27
44	The Day of Battle: The War in Sicily and Italy, 1943-1944 (The Liberation Trilogy)	28
45	Defeat into Victory: Battling Japan in Burma and India, 1942-1945	28
46	G-2: Intelligence for Patton ★★★	29
47	Gates of Fire: An Epic Novel of Thermopylae ★★★	29
48	Great Strategic Rivalries: From the Classical World to the Cold War ★★★	30
49	The Guns of August ★★★	30
50	Hell in a Very Small Place: The Siege of Dien Bien Phu	31
51	Killer Angels: The Classic Novel of the Civil War ★★★	31
52	The Landmark Thucydides: A comprehensive Guide to the Peloponnesian War ★★★	32
53	The Last Valley Dien Bien Phu and the French Defeat in Vietnam	32
54	The Origins of War: And the Preservation of Peace	33
55	The Outpost: An Untold Story of American Valor ★★★	33
56	The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000	34
57	A Savage War of Peace: Algeria 1954-1962	34
58	Scipio Africanus: Rome's Greatest General ★★★	35
59	Street Without Joy: The French Debacle in Indochina	35
60	Supreme Command: Soldiers, Statesmen, and Leadership in Wartime	36
61	This Kind of War: A Study of Unpreparedness: The Classic Korean War History ★★★	36
62	To Lose a Battle: France 1940	37
63	The Ugly American ★★★	37
64	The War that Ended Peace: The Road to 1914 ★★★	38
65	We Were Soldiers Once… and Young: Ia Drang- The Battle That Changed the War in Vietnam ★★★	38
66	A World Undone: The Story of the Great War, 1914-1918	39
67	With the Old Breed: At Peleliu and Okinawa ★★★	39
68	The Zimmermann Telegram	40

03 GLOBAL ANALYSIS

69	7 Deadly Scenarios: A Military Futurist Explores the Changing Face of War in the 21st Century ★★★	42
70	The Accidental Superpower: The Next Generation of American Preeminence and the Coming of Global Disorder ★★★	42
71	All the Shah's Men: An American Coup and the Roots of Middle East Terror	43
72	Asia's Cauldron: The South China Sea and the End of a Stable Pacific	43
73	The Cleanest Race: How North Koreans See Themselves and Why It Matters ★★★	44
74	Connectography – Mapping the Future of Global Civilization	44
75	Destined for War: Can America and China Escape the Thucydides' Trap? ★★★	45
76	Easternization: Asia's Rise and America's Decline	45
77	Freedom at Midnight	46
78	The Future, Declassified: Megatrends That Will Undo the World Unless We Take Action	46
79	Ghost Fleet: A Novel of the Next World War ★★★	47
80	The Hundred-Year marathon: China's Secret Strategy to Replace America as the Global Superpower ★★★	47
81	Korean Dream: A Vision for a Unified Korea ★★★	48
82	Lee Kuan Yew: The Grand Master's Insights on China, the United States, and the World ★★★	48
83	Machine, Platform, Crowd: Harnessing Our Digital Future ★★★	49
84	The Next Decade ★★★	49
85	On China ★★★	50
86	The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate	50
87	A Shattered Peace: Versailles 1919 and the Price We Pay Today ★★★	51
88	Thinking in Time: The Uses of History for Decision-Makers	51
89	The Tragedy of Great Power Politics (Updated Edition) ★★★	52
90	The Twilight War: The Secret History of America's Thirty-Year Conflict with Iran	52
91	The Unquiet Frontier: Rising Rivals, Vulnerable Allies, and the Crisis of American Power ★★★	53
92	Wired for War: The Robotics Revolution and Conflict in the 21st Century ★★★	53
93	Without You, There Is No Us: My Time with the Sons of North Korea's Elite	54
94	World Order ★★★	54

LEADERSHIP AND PROFESSIONAL DEVELOPMENT

01



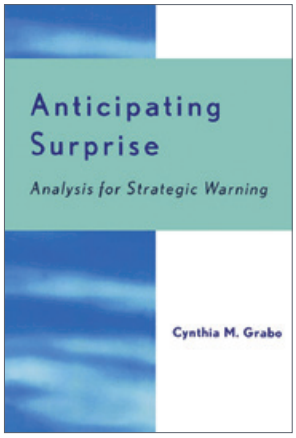
American Ulysses: A Life of Ulysses S. Grant

Ronald White, Random House: 2016

★★★

In his time, grouped routinely with George Washington and Abraham Lincoln in the "Trinity of Great American Leaders," Ulysses S. Grant, the battlefield commander–turned–commander-in-chief, fell out of favor in the twentieth century. In American Ulysses, Ronald C. White argues that we need to revise our estimates of him in the twenty-first. White shows Grant to be a generous, curious, introspective man and leader—a willing delegator with a natural gift for managing the rampaging egos of his fellow officers. His wife, Julia Dent Grant, long marginalized in the historic record, emerges in her own right as a spirited and influential partner. One of those rare books that successfully recast our impression of an iconic historical figure, American Ulysses gives us a finely honed, three-dimensional portrait of Grant the man—husband, father, leader, writer, and more.

02

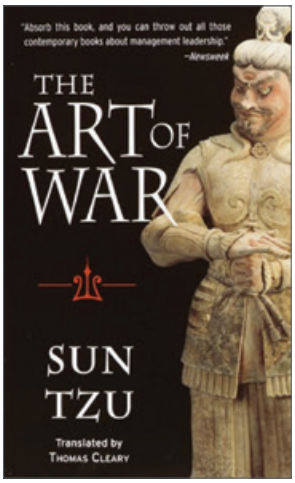


Anticipating Surprise: Analysis for Strategic Warning

Cynthia M. Grabo, Lulu.com: 2012

Assigned to the National Indications Center, Cynthia Grabo served as a senior researcher and writer for the U.S. Watch Committee throughout its existence (1950 to 1975), and in its successor, the Strategic Warning Staff. During this time, she saw the need to capture the institutional memory associated with strategic warning. In the summer of 1972, the DIA published her "Handbook of Warning Intelligence" as a classified document, followed by two additional classified volumes, one in the fall of 1972 and the last in 1974. Now condensed from the original three declassified books into this one, Grabo's authoritative interpretation of an appropriate analytic strategy for intelligence-based warning is presented in a commercial reprint of this classic study. (Originally published by the Joint Military Intelligence College)

03



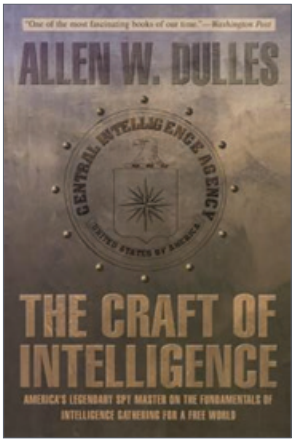
The Art of War

Sun Tzu (translated by Thomas Cleary), Shambhala: 2005

★★★

Conflict is an inevitable part of life, according to this ancient Chinese classic of strategy, but everything necessary to deal with conflict wisely, honorably, and victoriously is already present within us. Compiled more than two thousand years ago by a mysterious warrior-philosopher, The Art of War is still perhaps the most prestigious and influential book of strategy in the world, as eagerly studied in Asia by modern politicians and executives as it has been by military leaders since ancient times. As a study of the anatomy of organizations in conflict, The Art of War applies to competition and conflict, on every level from the interpersonal to the international. Its aim is invincibility, victory without battle, and unassailable strength through understanding the physics, politics, and psychology of conflict.

04

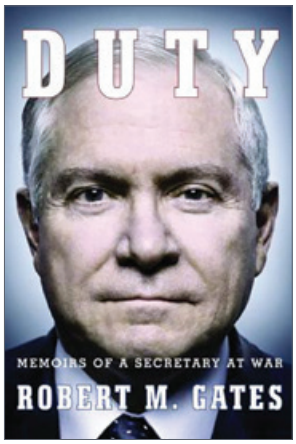


The Craft of Intelligence: America's Legendary Spymaster on the Fundamentals of Intelligence Gathering for a Free World

Allen Dulles, Lyons Press: Reprint 2016

Allen Dulles was a high-ranking officer of the CIA's predecessor—the Office of Strategic Services—and was present at the inception of the CIA, where he served eight of his ten years there as director. This classic spycraft, based on Dulles's incomparable experience as diplomat, international lawyer, and America's premier intelligence officer, sums up what he learned about intelligence from nearly a half-century of experience in foreign affairs.

05



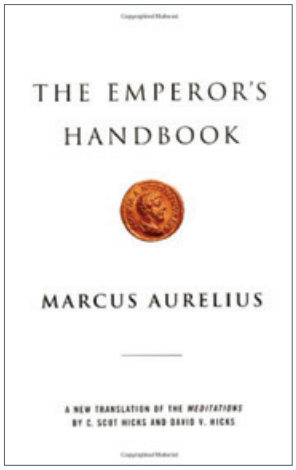
Duty: Memoirs of a Secretary at War

Robert Gates, Knopf: 2014

★★★

Forthright and unsparing, Duty is Gates's behind-the-scenes account of his nearly five years as a Secretary of Defense at war: the battles with Congress, the two presidents he served, the military itself, and the vast Pentagon bureaucracy. Gates describes his efforts to help George W. Bush turn the tide in Iraq, his role as a guiding (and often dissenting) voice for Barack Obama, and, most importantly, his ardent devotion to and love for American soldiers. Offering unvarnished appraisals of our political leaders, Duty tells a powerful and deeply personal story, giving us an unprecedented look at two administrations and the wars that have defined them.

06



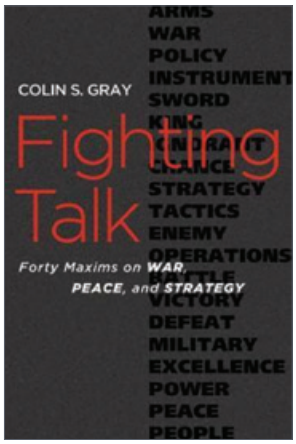
The Emperor's Handbook: A New Translation of the Meditations

Marcus Aurelius (translated by David Hicks and C. Scot Hicks), Scribner: 2002

★★★

Marcus Aurelius' Meditations—a practical book of timeless advice from one of the most powerful individuals in history— is available here for the first time in a highly accessible translation, including several unique features for contemporary readers and users of daily wisdom guides. The Emperor's Handbook offers a vivid and fresh translation of this important piece of ancient literature. It brings Marcus's words to life and shows his wisdom to be as relevant today as it was in the second century.

07



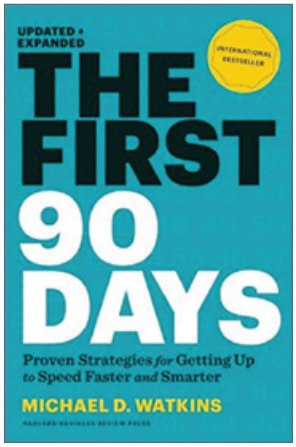
Fighting Talk: Forty Maxims on War, Peace, and Strategy

Colin S. Gray, Potomac: 2009

★★★

Gray presents an inventive treatise on the nature of strategy, war, and peace, organized around forty maxims. This collection of mini-essays will forearm politicians, soldiers, and the attentive public against many—probably most—fallacies that abound in contemporary debates about war, peace, and security. While one can never guarantee strategic success, which depends on policy, military prowess, and the quality of the dialogue between the two. A strategic education led by the judgments in these maxims increases the chances that one's errors will be small rather than catastrophic.

08



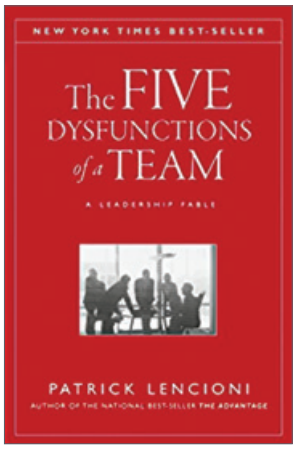
The First 90 Days: Proven Strategies for Getting Up to Speed Faster and Smarter

Michael D. Watkins, Harvard Business Review Press: Updated and Expanded 2013

★★★

In this updated and expanded version of the international bestseller The First 90 Days, Michael D. Watkins offers proven strategies for conquering the challenges of transitions—no matter where you are in your career. Watkins, a noted expert on leadership transitions and adviser to senior leaders in all types of organizations, also addresses today's increasingly demanding professional landscape, where managers face not only more frequent transitions but also steeper expectations once they step into their new jobs. By walking you through every aspect of the transition scenario, Watkins identifies the most common pitfalls new leaders encounter and provides the tools and strategies you need to avoid them.

09

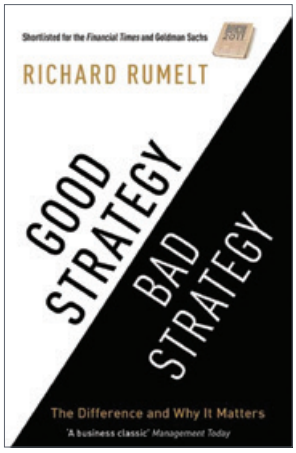


The Five Dysfunctions of a Team: A Leadership Fable

Patrick Lencioni, Jossey-Bass: 2002

In The Five Dysfunctions of a Team, Patrick Lencioni once again offers a leadership fable that is enthralling and instructive. Throughout the story, he reveals the five dysfunctions which go to the very heart of why teams—even the best ones—often struggle. He outlines a powerful model and actionable steps that can be used to overcome these common hurdles and build a cohesive, effective team. Lencioni has written a compelling fable with a powerful yet deceptively simple message for all those who strive to be exceptional team leaders.

10



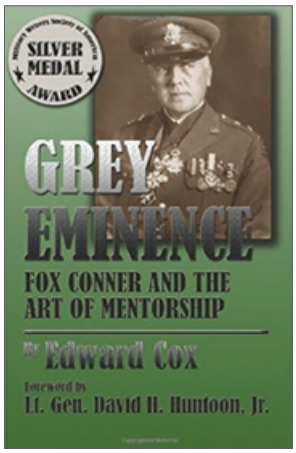
Good Strategy / Bad Strategy

Richard Rumelt, Currency: 2011

★★★

Developing and implementing a strategy is the central task of a leader, whether the CEO at a Fortune 100 company, an entrepreneur, a church pastor, the head of a school, or a government official. Richard Rumelt shows that there has been a growing and unfortunate tendency to equate Mom-and-apple-pie values, fluffy packages of buzzwords, motivational slogans, and financial goals with "strategy." He debunks these elements of "bad strategy" and awakens an understanding of the power of a "good strategy." Rumelt argues that the heart of a good strategy is insight—into the true nature of the situation, into the hidden power in a situation, and into an appropriate response. He shows you how insight can be cultivated with a wide variety of tools for guiding your own thinking.

11



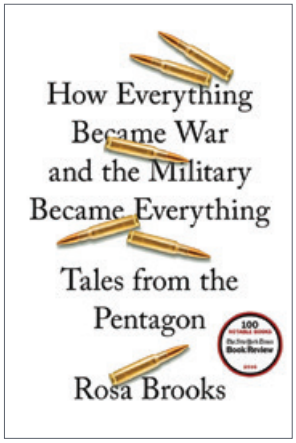
Grey Eminence: Fox Conner and the Art of Mentorship

Edward Cox, New Forums Press: 2011

★★★

To those who have heard of him, Fox Conner's name is synonymous with mentorship. He is the "grey eminence" within the Army, whose influence helped to shape the careers of George Patton, George Marshall, and—most notably—President Eisenhower. After a career that spanned four decades, this master strategist ordered all of his papers and journals burned. Because of this, Conner is an oblique figure in military history. What little is known about Conner comes primarily through stories about his relationship with Eisenhower, and as a passing reference in the memoirs of other great men. This book combines existing scholarship with long-forgotten references and unpublished original sources to achieve a more comprehensive picture of this dedicated public servant. The portrait that emerges provides a four-step model for developing strategic leaders that still holds true today.

12



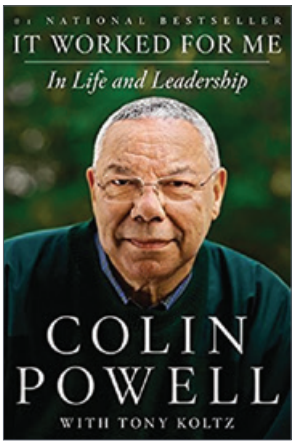
How Everything Became War and the Military Became Everything: Tales from the Pentagon

Rosa Brooks, Simon and Schuster: 2016

★★★

The first serious book to examine what happens when you erase the ancient boundary between war and peace. Once, war was a temporary state of affairs—a violent but brief interlude between times of peace. Today, America's wars are everywhere and forever: our enemies change constantly and rarely wear uniforms, and virtually anything can become a weapon. As war expands, so does the role of the US military. Today, military personnel don't just "kill people and break stuff." Instead, they analyze computer code, train Afghan judges, build Ebola isolation wards, eavesdrop on electronic communications, develop soap operas, and patrol for pirates.

13

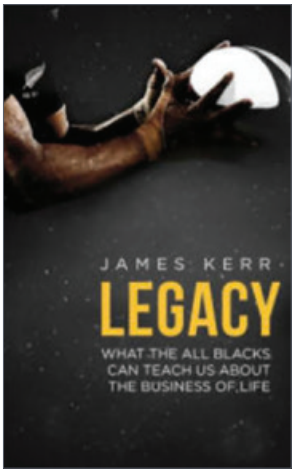


It Worked for Me: In Life and Leadership

Colin Powell, Harper: 2012

Colin Powell, one of America's most admired public figures, reveals the principles that have shaped his life and career in this inspiring and engrossing memoir. It Worked for Me: In Life and Leadership is a trove of wisdom for anyone hoping to achieve their goals and turn their dreams into reality. A message of strength and endurance from a man who has dedicated his life to public service, this is a book with the power to show readers everywhere how to achieve a more fulfilling life and career.

14



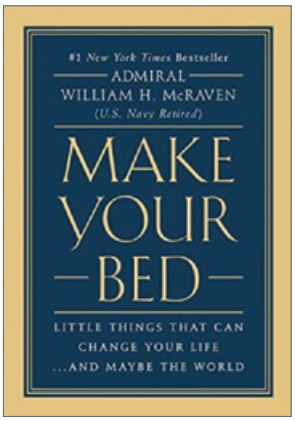
Legacy

James Kerr, Constable & Robinson: 2013

★★★

In Legacy, best-selling author James Kerr goes deep into the heart of the world's most successful sporting team, the legendary All Blacks of New Zealand, to reveal 15 powerful and practical lessons for leadership and business. Legacy is a unique, inspiring handbook for leaders in all fields, and asks the questions: What are the secrets of success—sustained success? How do you achieve world-class standards, day after day, week after week, year after year? How do you handle pressure? How do you train to win at the highest level? What do you leave behind you after you're gone?

15



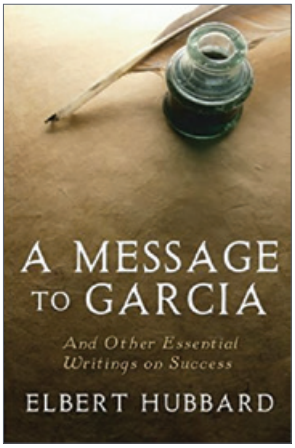
Make Your Bed – Little Things That Can Change Your Life…and Maybe the World

William McRaven, Grand Central Publishing: 2017

★★★

Based on a speech to the graduating class of the University of Texas at Austin, Admiral William H. McRaven shares the ten principles he learned during Navy Seal training that helped him overcome challenges not only in his training and long Naval career, but also throughout his life. McRaven explains how anyone can use these basic lessons to change themselves—and the world—for the better. Told with great humility and optimism, this timeless book provides simple wisdom, practical advice, and words of encouragement that will inspire readers to achieve more—even in life's darkest moments.

16



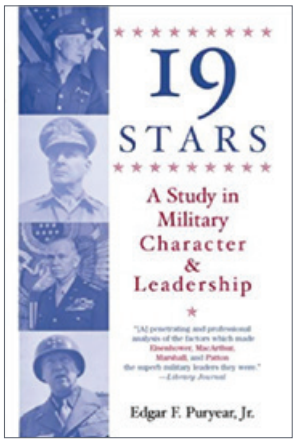
A Message to Garcia

Elbert Hubbard, Classic House: 2009 [First published in 1899]

★★★

Written in 1899, this inspirational essay, loosely based on an actual event in the Spanish-American War, praises Lieutenant Andrew Rowan for his perseverance and obedience. Charged with delivering an important message to a Cuban general, the lieutenant did not abandon his mission in the face of many obstacles. "To take a message to Garcia" was for years a popular American slang expression for taking initiative and still used today by many military leaders as a model of an exemplary work ethic.

17



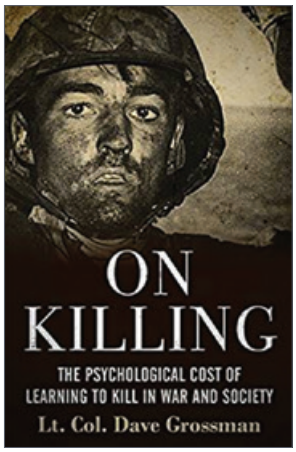
Nineteen Stars: A Study in Military Character and Leadership

Edgar Puryear, Presidio Press: 2003

★★★

Nineteen Stars is an in-depth study of American military leadership and character. Puryear makes a comparative study of the careers of four of the most successful US WWII generals: Marshall, MacArthur, Eisenhower and Patton. By examining these men from their cadet years at West Point to the conclusion of WWII, he determines why these men became our top commanders and attempts to answer the question: Can one learn successful military leadership or must one be born to command? A model of character and leadership is revealed here in the careers of the quietly confident Marshall, the military genius of MacArthur, the beloved Eisenhower, and the go-for-broke Patton.

18



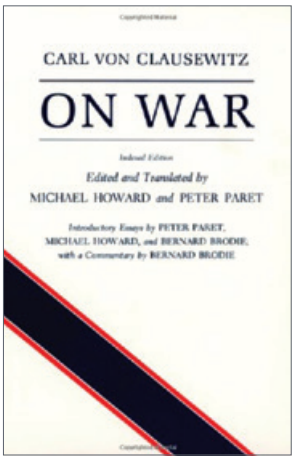
On Killing: The Psychological Cost of Learning to Kill in War and Society

Dave Grossman, Back Bay Books: 2009 [First Published in 1995]

★★★

The good news is that most soldiers are loath to kill. However, armies have developed sophisticated ways of overcoming this instinctive aversion. Contemporary civilian society, particularly the media, replicates the Army's conditioning techniques, and, according to Lt. Col. Dave Grossman's thesis, is responsible for our rising rate of murder among the young. Upon its initial publication, many hailed On Killing as a landmark study of the techniques the military uses to overcome the powerful reluctance to kill, of how killing affects soldiers, and of the societal implications of escalating violence. Now, Grossman has updated this to include information on 21st-century military conflicts, recent trends in crime, suicide bombings, school shootings, and more.

19



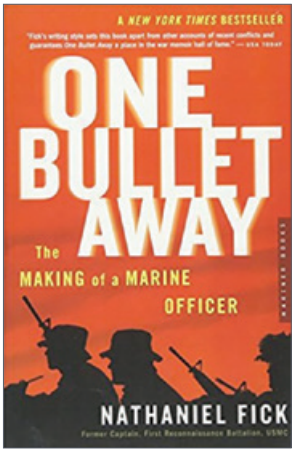
On War

Carl von Clausewitz, Clausewitz Press: 2017

★★★

Fascinated by the leading military figures of his day, Prussian General Carl von Clausewitz spent over ten years writing a book—On War—that he would never finish. The book examines the tactics of Napoleon, Frederick II of Prussia, and others. In this insightful, well-informed work of military analysis, Von Clausewitz theorizes that war is an instrument of political commerce. On War is the most significant attempt in Western history to understand war, both in its internal dynamics and as an instrument of policy. Since the work's first appearance in 1832, it has been read throughout the world, and has been stimulating generations of soldiers, political leaders, and intellectuals.

20

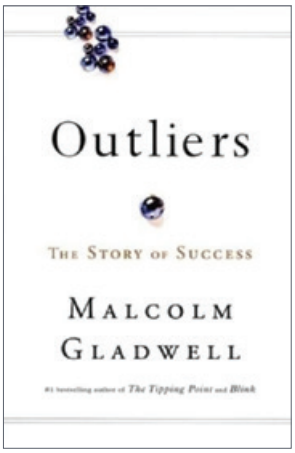


One Bullet Away: The Making of a Marine Officer

Nathaniel Fick, Reprint 2006

If the Marines are "the few, the proud," Recon Marines are the fewest and the proudest. Nathaniel Fick unveils the process that makes Marine officers such legendary leaders and shares his hard-won insights into the differences between military ideals and military practice, which can mock those ideals. In this deeply thoughtful account of what it's like to fight on today's front lines, Fick reveals the crushing pressure on young leaders in combat. Split-second decisions might have national consequences or horrible immediate repercussions, but hesitation isn't an option. One Bullet Away never shrinks from blunt truths, but ultimately it is an inspiring account of mastering the art of war.

21



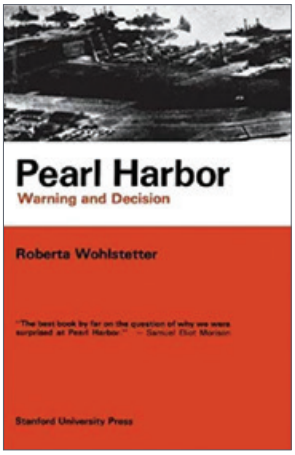
Outliers: The Story of Success

Malcolm Gladwell, Little, Brown and Company: 2008

★★★

In this stunning and fascinating book, Malcolm Gladwell takes us on an intellectual journey through the world of "outliers"—the best and the brightest, the most famous, and the most successful. He asks the question: What makes high-achievers different? His answer is that we pay too much attention to what successful people are like, and too little attention to where they started: that is, their culture, their family, their generation, and the idiosyncratic experiences of their upbringing. Along the way, he explains the secrets of software billionaires, what it takes to be a great soccer player, why Asians are good at math, and what made the Beatles the greatest rock band.

22

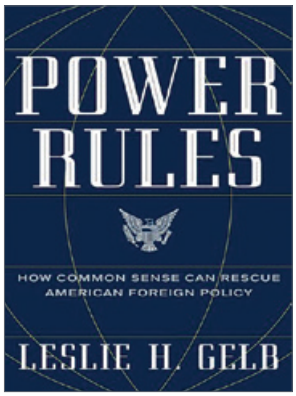


Pearl Harbor: Warning and Decision

Roberta Wohlstetter, Stanford University Press: 1962

It would be reassuring to believe that Pearl Harbor was just a colossal and extraordinary blunder. What is disquieting is that it was a supremely ordinary blunder; it was a dramatic failure of a remarkably well-informed government to call the next enemy move. Pearl Harbor: Warning and Decision is a unique physiology of a great national failure to anticipate. Wohlstetter shows how easy it was to slip into the rut in which the Japanese found us, it can only remind us how likely it is that we are in the same kind of rut right now. The danger is not that we shall read the signals and indicators with too little skill; the danger is in a poverty of expectations—a routine obsessing with a few dangers that may be familiar rather than likely.

23

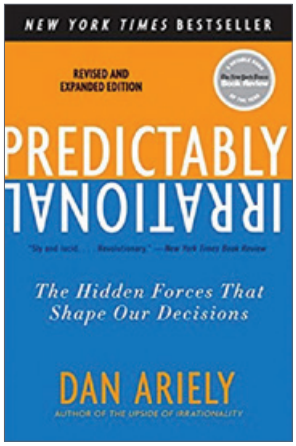


Power Rules: How Common Sense Can Rescue American Foreign Policy

Leslie Gelb, Harper Perennial: 2010

Power Rules is the provocative account of how to think about and use America's power in the world, from Pulitzer Prize winner Leslie H. Gelb, one of the nation's leading foreign policy minds and practitioners. Gelb offers guidelines to the U.S. president on how to use American power effectively in today's tumultuous world. He also argues that American leaders have failed to recognize three key power realities. First, the world is not flat; it is highly pyramidal in power. Second, power is neither soft (persuasion and values) nor hard (military force), but is psychological based on the skilled use of carrots and sticks. Third, he asserts, the world has not entered the post-American era; rather, the United States remains the sole global leader, but without the power to dominate.

24

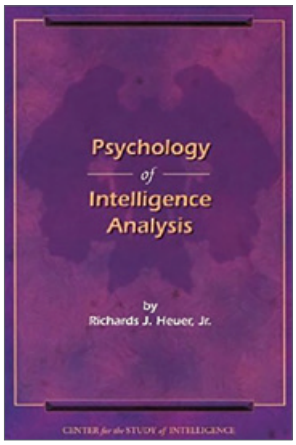


Predictably Irrational, Revised and Expanded Edition: The Hidden Forces That Shape Our Decisions

Dan Ariely, Harper Perennial: 2010

Irrational behavior is a part of human nature, but as MIT professor Ariely has discovered in 20 years of researching behavioral economics, people tend to behave irrationally in a predictable fashion. Drawing on psychology and economics, behavioral economics can show us why patients get greater relief from a more expensive drug over its cheaper counterpart and why honest people may steal office supplies or communal food, but not money. According to Ariely, our understanding of economics, now based on the assumption of a rational subject—should in fact—be based on our systematic, unsurprising irrationality. Ariely argues that greater understanding of previously ignored or misunderstood forces (emotions, relativity and social norms) that influence our economic behavior brings a variety of opportunities for reexamining individual motivation and consumer choice, as well as economic and educational policy.

25

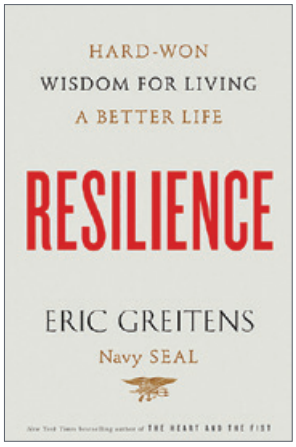


Psychology of Intelligence Analysis

Richard Heuer, Military Bookshop: 2010

This volume pulls together and republishes, with some editing, updating, and additions, articles written from 1978 to 1986 for internal use within the CIA Directorate of Intelligence. Based on reviewing cognitive psychology literature, these articles revealed how people process information to make judgments on incomplete and ambiguous information. Richard Heuer has selected the experiments and findings that seem most relevant to intelligence analysis and most in need of communication to intelligence analysts. He then translates the technical reports into language intelligence analysts can understand, and interpreted the relevance of these findings to the problems intelligence analysts face.

26



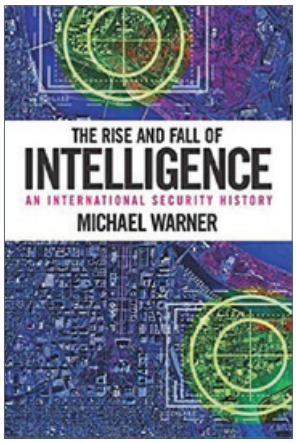
Resilience: Hard-Won Wisdom for Living a Better Life

Eric Greitens, First Mariner Books Edition: 2015

★★★

In 2012, Eric Greitens unexpectedly heard from a former SEAL team comrade, a brother-in-arms he had not seen in a decade. Zach Walker had been one of the toughest of the tough, but ever since he returned home from war to his young family in a small logging town, he had been struggling. Zach and Eric started writing and talking nearly every day, as Eric set down his thoughts on what it takes to build resilience in our lives. Eric's letters, drawing on both his own experience and wisdom from ancient and modern thinkers, are now gathered and edited into this timeless guidebook. Greitens shows how we can build purpose, confront pain, practice compassion, develop a vocation, find a mentor, create happiness, and much more. Resilience is an inspiring meditation for the warrior in each of us.

27

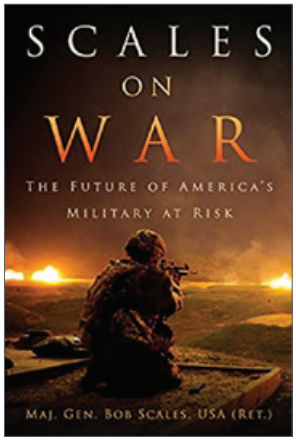


The Rise and Fall of Intelligence: An International Security History

Michael Warner, Georgetown University Press: 2014

Historian Michael Warner addresses the birth of professional intelligence in Europe at the beginning of the twentieth century and the subsequent rise of US intelligence during the Cold War. He brings this history up to the present day as intelligence agencies used the struggle against terrorism and the digital revolution to improve capabilities in the 2000s. Throughout, the book examines how states and other entities use intelligence to create, exploit, and protect secret advantages against others, and emphasizes how technological advancement and ideological competition drive intelligence, improving its techniques, and creating a need for intelligence and counterintelligence activities to serve and protect policymakers and commanders.

28



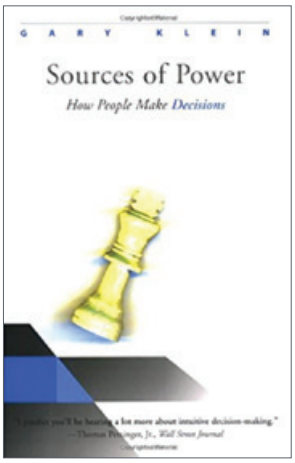
Scales on War: The Future of America's Military at Risk

MG (Ret) Bob Scales, Naval Institute Press: 2016

★★★

Scales on War is a collection of ideas, concepts, and observations about contemporary war taken from over thirty years of research, writing, and personal experience by retired Major General Bob Scales. Scales' unique style of writing utilizes contemporary military history, current events, and his philosophy of ground warfare to create a very personal and expansive view of the future direction of American defense policies. Scales on War shows that, as a result of America's focus on winning wars with technology rather than people, America's enemies have learned how to win battles by defeating such technology. As a well-known warfare expert, Scales demonstrates how only a resurgent land force of Army and Marine small units will restore America's fighting competence.

29

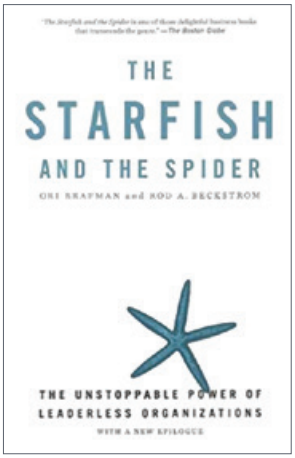


Sources of Power: How People Make Decisions

Gary Klein, The MIT Press: 1999

Based on observations of humans acting under real-life constraints, from time pressure, high stakes, personal responsibility, and shifting conditions, Sources of Power is a study by professionals of people from different occupations: firefighters, critical care nurses, pilots, nuclear power plant operators, battle planners, and chess masters. Each chapter builds on key incidents and examples to make the description of the methodology and phenomena more vivid. In addition to providing information professionals in management, psychology, engineering, can use that and other fields, the book presents an overview of the research approach of naturalistic decision making and expands our knowledge of the strengths people bring to difficult tasks.

30



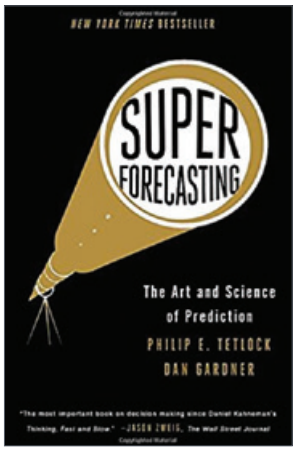
The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations

Ori Braufman and Rod A. Beckstrom, Penguin Group: 2006

★★★

If you cut off a spider's head, it dies; if you cut off a starfish's leg it grows a new one, and that leg can grow into an entirely new starfish. Traditional top-down organizations are like spiders, but now starfish organizations are changing the face of business and the world. Ori Braufman and Rod Beckstrom have discovered some unexpected answers, gripping stories, and a tapestry of unlikely connections. The Starfish and the Spider explores what happens when starfish take on spiders and reveals how established companies and institutions, from IBM to Intuit to the U.S. government, are also learning how to incorporate starfish principles to achieve success.

31

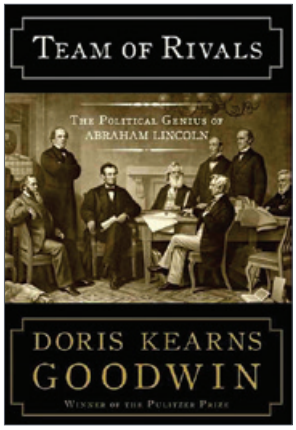


Superforecasting

Phil Tetlock and Dan Gardner, Broadway Books: Reprint Edition 2016

In Superforecasting, Tetlock and coauthor Dan Gardner offer a masterwork on prediction, drawing on decades of research, and the results of a massive, government-funded forecasting tournament. The Good Judgment Project involves tens of thousands of ordinary people—including a Brooklyn filmmaker, a retired pipe installer, and a former ballroom dancer—who set out to forecast global events. Some of the volunteers have turned out to be astonishingly good. In this groundbreaking and accessible book, Tetlock and Gardner show us how we can learn from this elite group. Superforecasting offers a demonstrably effective way to improve our ability to predict the future, whether in business, finance, politics, international affairs, or daily life.

32

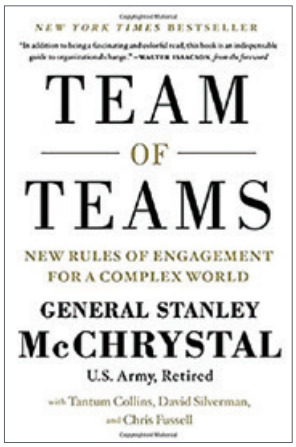


Team of Rivals: The Political Genius of Abraham Lincoln

Doris Kearns Goodwin, Simon & Schuster: 2005

Acclaimed historian, Doris Kearns Goodwin illuminates Lincoln's political genius in this highly original work, as the one-term congressman and prairie lawyer rises from obscurity to prevail over three gifted rivals of national reputation to become president. Goodwin demonstrates Lincoln's character, forged by experiences that raised him above his more privileged and accomplished rivals. He possessed an extraordinary ability to put himself in the place of other men, to experience what they were feeling, and to understand their motives and desires. This capacity enabled Lincoln, as president, to bring his disgruntled opponents together, create the most unusual cabinet in history, and marshal their talents to the task of preserving the Union and winning the war. Team of Rivals is a brilliant multiple biography that centers on Lincoln's mastery of men, and how this ability shaped the most significant presidency in the nation's history.

33

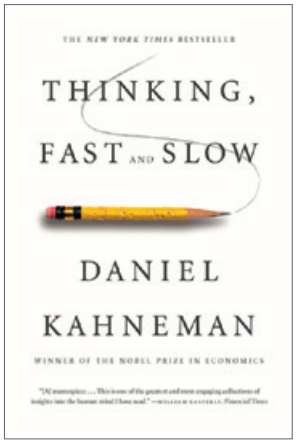


Team of Teams: New Rules of Engagement for a Complex World

GEN (Ret) Stanley McChrystal, Collins, Silverman, and Fussell, Penguin: 2015

In this powerful book, General McChrystal and his colleagues show how the challenges they faced in Iraq can be relevant to countless businesses, nonprofits, and other organizations. The world is changing faster than ever, and the smartest response for those in charge is to give small groups the freedom to experiment while driving everyone to share what they learn across the entire organization. As the authors argue through compelling examples, the team of teams strategy has worked everywhere from hospital emergency rooms to NASA. It has the potential to transform organizations large and small.

34

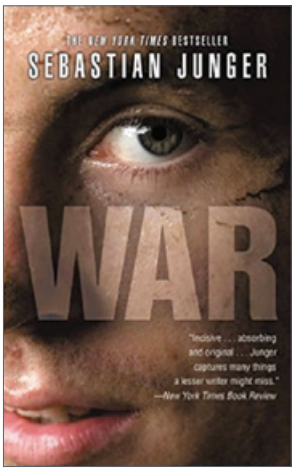


Thinking Fast and Slow

Daniel Khaneman, Farrar Straus Giroux: 2011

In the international bestseller, Thinking Fast and Slow, Daniel Khaneman, the renowned psychologist and winner of the Nobel Prize in Economics, takes us on a groundbreaking tour of the mind and explains the two systems that drive the way we think. System 1 is fast, intuitive, and emotional; System 2 is slower, more deliberative, and more logical. The impact of overconfidence on corporate strategies, the difficulties of predicting what will make us happy in the future, the profound effect of cognitive biases on everything from playing the stock market to planning our next vacation—each of these maybe better understood only by knowing how the two systems shape our judgments and decisions.

35



War

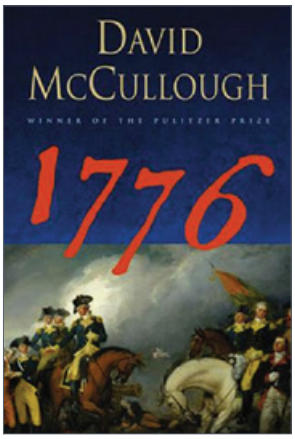
Sebastian Junger, Twelve: 2010

★★★

Over fifteen months, Sebastian Junger followed a single platoon based at a remote outpost in eastern Afghanistan. His objective was both simple and ambitious; to convey what soldiers experience and what war actually feels like. In these pages, he gives insight into the truths of combat: the fear, the honor, and the trust among men. He describes things that few civilians will ever witness or go through—the endless, body-numbing anticipation of battle, the adrenaline-fueled confusion of an ambush, and the unquestioned and automatic risks soldiers take in combat situations to protect their brothers. Junger draws on biology, psychology, and military history to explain the decisions soldiers make and to put their ordeals into context. In the vivid prose, War, relates the physical toil, the suffocating heat, the sounds of gunfire, and the agony of loss.

HISTORY

36



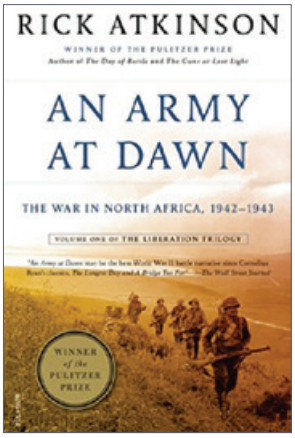
1776

David McCullough, Simon & Schuster: 2005

★★★

David McCullough presents the stirring story of the year of our nation's birth, interweaving the actions and decisions that led Great Britain to undertake a war against her rebellious colonial subjects. Based on extensive research in both American and British archives, 1776 is a powerful drama written with extraordinary narrative vitality. It is the story of Americans in the ranks, men of every shape, size, and color, farmers, schoolteachers, shoemakers, no-accounts, and mere boys turned soldiers. And it is the story of the King's men, the British commander, William Howe, and his highly disciplined redcoats who looked on their rebel foes with contempt and fought with a valor too little known.

37

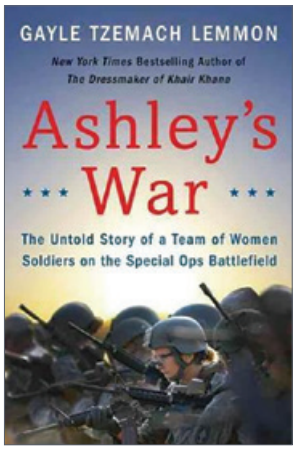


An Army at Dawn: The War in North Africa 1942-1943 (The Liberation Trilogy)

Rick Atkinson, Holt Paperbacks: 2007

Opening with the daring amphibious invasion in November 1942, An Army at Dawn follows the American and British armies as they fight the French in Morocco and Algiers, and then take on the Germans and Italians in Tunisia. Battle by battle, an inexperienced and sometimes poorly led army gradually becomes a superb fighting force. At the center of the tale are the extraordinary but flawed commanders who come to dominate the battlefield: Eisenhower, Patton, Bradley, Montgomery, and Rommel. In this first volume of the Liberation Trilogy, Rick Atkinson shows why no modern reader can understand the ultimate victory of the Allied powers without a grasp of the great drama that unfolded in North Africa in 1942 and 1943.

38

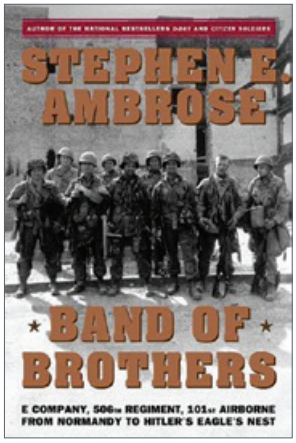


Ashley's War: The Untold Story of a Team of Women Soldiers on the Special Ops Battlefield

Gayle Tzemach Lemmon, Harper: 2015

Gayle Tzemach Lemmon uses on-the-ground reporting and an understanding of the complexities of war to tell the story of Cultural Support Team-2 (CST-2), a unit of women handpicked from the Army to serve in this highly specialized and challenging role. The pioneers of CST-2 proved for the first time, that women might be physically and mentally tough enough to become part of the elite. At the center of this story is a friendship cemented by "Glee," video games, and the shared perils and seductive powers of up-close combat. At the heart of the team is the tale of a beloved and effective soldier, Ashley White.

39



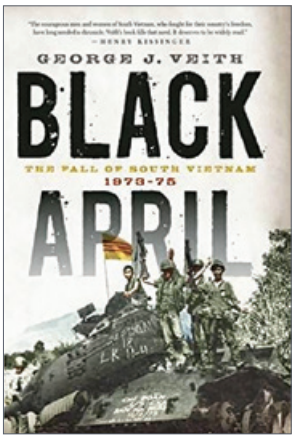
Band of Brothers: E Company, 506th Regiment, 101st Airborne from Normandy to Hitler's Eagle's Nest

Steven E. Ambrose, Simon & Schuster: 2007

★★★

Stephen E. Ambrose's iconic story of the ordinary men who became World War II's most extraordinary soldiers: Easy Company, 506th Parachute Infantry Regiment, 101st Airborne Division, US Army. From the rigorous training in Georgia in 1942 to the disbanding in 1945, Ambrose tells the story of this remarkable company. They were rough-and-ready guys, battered by the Depression, mistrustful and suspicious. However, in training and combat, they learned selflessness and found the closest brotherhood they ever knew. They discovered that in war, men who loved life would give their lives for them. E Company was a company of men who went hungry, froze, and died for each other. A company that took 150 percent casualties. A company where the Purple Heart was not a medal—it was a badge of office.

40

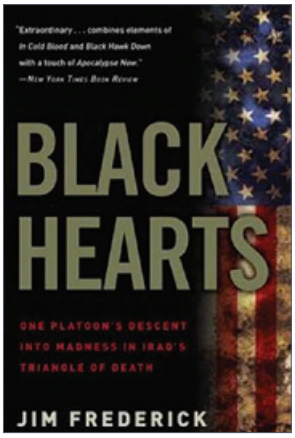


Black April: The Fall of South Vietnam, 1973-1975

George Veith, Encounter Books: 2012

The defeat of South Vietnam was arguably America's worst foreign policy disaster of the 20th Century. Yet a complete understanding of the endgame—from the 27 January 1973 signing of the Paris Peace Accords to South Vietnam's surrender on 30 April 1975—has eluded us. Black April addresses that deficit through a culmination of exhaustive research in three distinct areas: primary source documents from American archives, North Vietnamese publications containing primary and secondary source material, and dozens of articles and numerous interviews with key South Vietnamese participants. This book represents one of the largest Vietnamese translation projects ever accomplished, including almost one hundred rarely or never before seen North Vietnamese unit histories, battle studies, and memoirs.

41



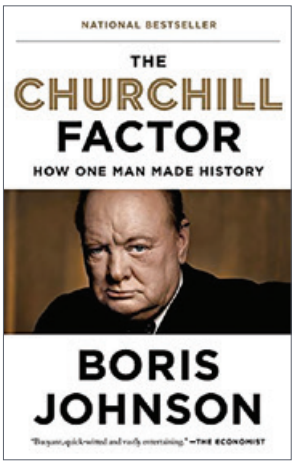
Black Hearts: One Platoon's Descent into the Madness of Iraq's Triangle of Death

Jim Frederick, Broadway: 2010

★★★

This is the story of a small group of soldiers from the 101st Airborne Division's fabled 502nd Infantry Regiment—a unit known as "the Black Heart Brigade." Deployed in late 2005 to Iraq's so-called Triangle of Death, a veritable meat grinder just south of Baghdad, the Black Hearts found themselves in arguably the country's most dangerous location at its most dangerous time. Black Hearts is a timeless story about men in combat and the fragility of character in the savage crucible of warfare. But it is also a timely warning of new dangers emerging in the way American soldiers are led on the battlefields of the twenty-first century.

42



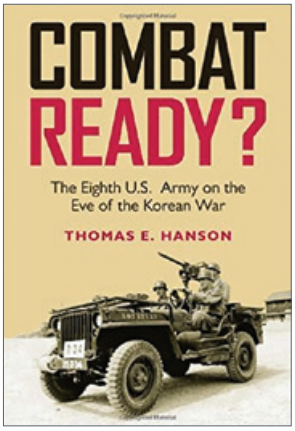
The Churchill Factor: How One Man Made History

Boris Johnson, Riverhead Books: 2015

★★★

Fearless on the battlefield, the king had to order Churchill to stay out of action on D-day; he pioneered aerial bombing and few could match his experience in organizing violence on a colossal scale, yet he hated war and scorned politicians who had not experienced its horrors. He was the most famous journalist of his time and perhaps the greatest orator of all time, despite a lisp and the chronic depression he kept at bay by painting. His maneuvering positioned America for entry into World War II, even as it ushered in England's postwar decline. His open-mindedness made him a trailblazer in health care, education, and social welfare, though he remained incorrigibly politically incorrect. Most of all, he was a rebuttal to the idea that history is the story of vast and impersonal forces; he is proof that one person—intrepid, ingenious, determined—can make all the difference.

43



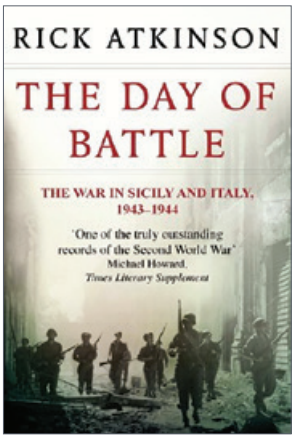
Combat Ready?: The Eighth U.S. Army on the Eve of the Korean War

Thomas E. Hanson, Williams-Ford Texas A&M University Military History Series: 2010

★★★

In Hanson's careful study of combat preparedness in the Eighth Army from 1949 to the outbreak of hostilities in 1950, he concedes that the U.S. soldiers sent to Korea suffered gaps in their professional preparation, from missing and broken equipment to unevenly trained leaders at every level of command. But after a year of progressive, focused, and developmental collective training—based largely on the lessons of combat in World War II—these soldiers expected to defeat the Communist enemy. By recognizing the constraints under which the Eighth Army operated, Hanson asserts that scholars and soldiers will be able to discard what Douglas Macarthur called the "pernicious myth" of the Eighth Army's professional, physical, and moral ineffectiveness.

44

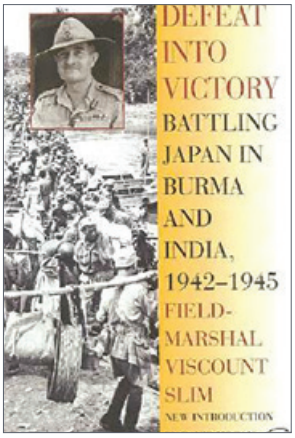


The Day of Battle: The War in Sicily and Italy, 1943-1944 (The Liberation Trilogy)

Rick Atkinson, Henry Holt: 2008

Rick Atkinson follows the strengthening American and British armies as they invade Sicily in July 1943 and then, mile by bloody mile, fight their way north toward Rome. The decision to invade the so-called soft underbelly of Europe was controversial, but once under way, the commitment to liberate Italy from the Nazis never wavered. The battles at Salerno, Anzio, the Rapido River, and Monte Cassino were particularly lethal, yet as the months passed, the Allied forces continued to drive the Germans up the Italian peninsula. Moreover, with the liberation of Rome in June 1944, ultimate victory at last began to seem inevitable. Drawing on a wide array of primary source material, written with great drama and flair, The Day of Battle is a masterly account of one of history's most compelling military campaigns.

45



Defeat into Victory: Battling Japan in Burma and India, 1942-1945

Field-Marshal Viscount William Slim, Cooper Square Press: 2000

Field-Marshal Slim's classic account of the Burma Campaign in World War II is divided into six books: Defeat; Forging the Weapon; The Weapon is Tested; The Tide Turns; The Decisive Battle; and Victory. This memoir is widely regarded as a classic of high command. Though told from the perspective of a Field-Marshall, Slim still imparts lessons that are relevant for tactical leaders to this day, such as the difficulties of jungle fighting and the importance of mission command in distributed operations. Impressively, Field-Marshal Slim is not afraid to admit some of this own shortcomings as a commander. This is a narrative, which captures both the high drama and the harsh reality of war.

46

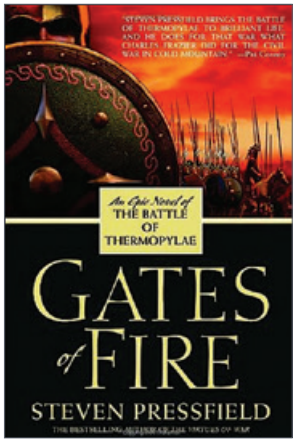
G-2: Intelligence for Patton

Oscar Koch and Robert G. Hays, Schiffer: 1999 [First published 1971]

★★★

This personal record, written by Brigadier General Oscar W. Koch—who served during World War II as chief of intelligence for General George S. Patton, Jr., one of the most colorful military leaders in American history—examines the enigmatic science of military intelligence. General Koch traces the growth and development of the infant science through detailed accounts of the intelligence role in some of the most celebrated battles of the war, and through his personal remembrances of Patton and his relationships with members of his intelligence staff. His story moves from the African campaign through Sicily, into France on D-Day, and on to the Battle of the Bulge—pointing out how the work of the intelligence staff made the differences in the final reckoning. General Koch's book is more than a historical study, however. It is the exciting story of the operations behind the cloak and dagger illusions.

47



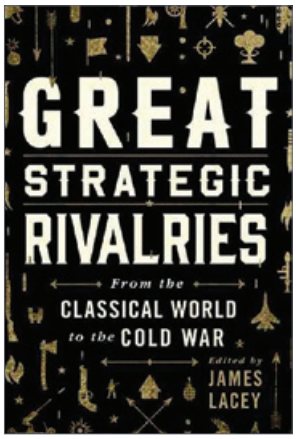
Gates of Fire: An Epic Novel of Thermopylae

Steven Pressfield, Bantam Books: 1998

★★★

Thermopylae: the 480 BC battle that went down in history as an example of heroism. For three days, a small force of Greeks defended a narrow pass from a huge Persian army. Narrated by the sole survivor of the epic battle - a squire in the Spartan heavy infantry- Gates of Fire is a mesmerizing depiction of one man's indoctrination into the Spartan way of life and death, and the legendary men and women who gave the culture an immortal gravity. Culminating in an electrifying and horrifying epic battle, Gates of Fire weaves history, mystery, and heartbreaking romance into a literary page-turner that brings the Homeric tradition into the twenty-first century.

48



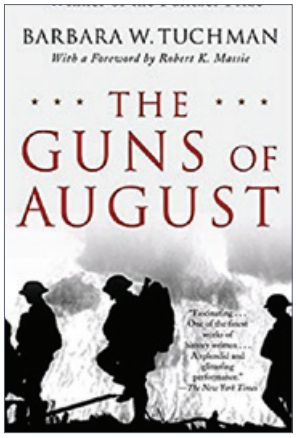
Great Strategic Rivalries: From the Classical World to the Cold War

James Lacey (editor), Oxford University Press: 2016

★★★

From the legendary antagonism between Athens and Sparta during the Peloponnesian War to the Napoleonic Wars and the two World Wars of the twentieth century, long-term strategic rivalries littered the past. History tells us that such enduring rivalries can end in one of three ways. First in a series of exhausting conflicts, in which one side eventually prevails—as in the case of the Punic Wars between ancient Rome and Carthage. Second in a peaceful and hopefully orderly transition, like the rivalry between Great Britain and the United States at the turn of the twentieth century. Lastly a one-sided collapse, such as the conclusion of the Cold War with the fall of the Soviet Union. However, in spite of a wealth of historical examples, the future of state rivalries remains a matter of conjecture.

49



The Guns of August

Barbara Tuchman, Random House: 2004 [First Published in 1962]

★★★

In this landmark, Pulitzer Prize winning account, renowned historian Barbara W. Tuchman re-creates the first month of World War I: thirty days in the summer of 1914 that determined the course of the conflict, the century, and ultimately our present world. Beginning with the funeral of Edward VII, Tuchman traces each step that led to the inevitable clash, and inevitable it was, with all sides plotting their war for a generation. Dizzyingly comprehensive and spectacularly portrayed with her famous talent for evoking the characters of the war's key players, Tuchman's magnum opus is a classic for the ages.

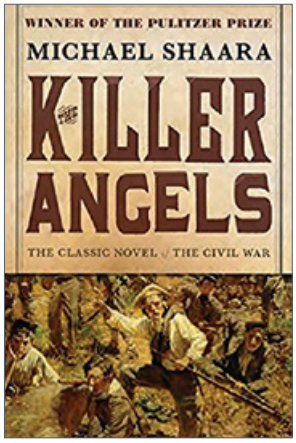
50

Hell in a Very Small Place: The Siege of Dien Bien Phu

Bernard B. Fall, Da Capo Press: Reprint 2002

The siege of Dien Bien Phu, in which a guerrilla force of Viet Minh destroyed a technologically superior French colonial army, must rank with Waterloo, Gettysburg, Midway, Stalingrad, and Tet as one of the decisive battles in military history. Not only did Dien Bien Phu put an end to French imperial efforts in Indo-china, but it also convinced the Viet Minh, when they came to power in Communist North Vietnam, that similar tactics would prevail in their war with the United States. Fall accurately predicted that if the United States did not learn from France's mistakes, it too would fail in Vietnam.

51



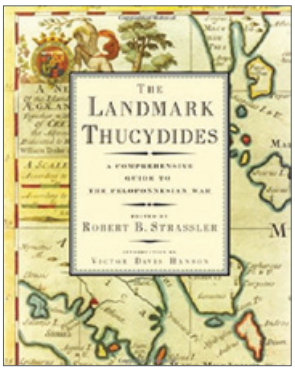
Killer Angels: The Classic Novel of the Civil War

Michael Shaara, Random House: 1987 [First published in 1974]

★★★

In the four bloodiest and courageous days of our nation's history, two armies fought for two conflicting dreams. One dreamed of freedom, the other of a way of life. Far more than rifles and bullets were carried into battle. There were memories. There were promises. There was love. And, far more than men fell on those Pennsylvania fields. Bright futures, untested innocence, and pristine beauty were also the casualties of war. Michael Shaara's Pulitzer Prize-winning masterpiece is unique, sweeping, unforgettable—the dramatic story of the battleground for America's destiny.

52



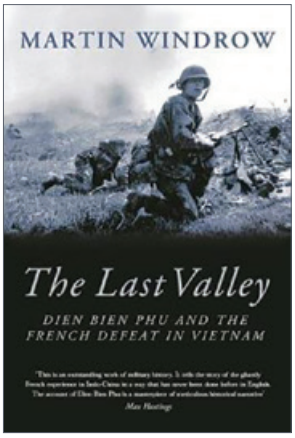
The Landmark Thucydides: A comprehensive Guide to the Peloponnesian War

Robert B. Strassler, Simon & Shuster: 1996

★★★

Thucydides called his account of two decades of war between Athens and Sparta "a possession for all time," and it is the first and still most famous work in the Western historical tradition. Considered essential reading for generals, statesmen, and liberally educated citizens for more than 2,000 years, The Peloponnesian War is a mine of military, moral, political, and philosophical wisdom. Strassler's edition provides a new coherence to the narrative overall by effectively reconstructing the lost cultural context that Thucydides shared with his original audience.

53

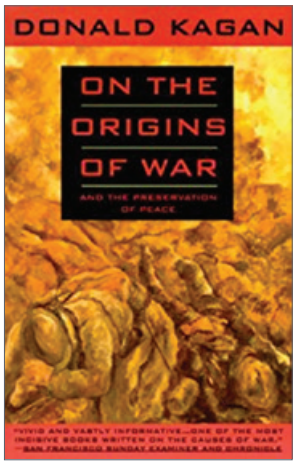


The Last Valley Dien Bien Phu and the French Defeat in Vietnam

Martin Windrow, Da Capo Press: 2014

In December 1953, the French army occupying Vietnam challenged the elusive Vietnamese army to engage in a decisive battle. When French paratroopers landed in the jungle on the border between Vietnam and Laos, the Vietnamese quickly isolated the French force and confronted them at their jungle base in a small place called Dien Bien Phu. The hunters—the French army—had become the hunted, desperately defending their out-gunned base. The siege in the jungle wore on as defeat loomed for the French. Depleted, demoralized, and destroyed, eventually the French withdrew from the country. Created from the withdraw, the ominous division of the country at U.S. insistence, was the short-lived Republic of South Vietnam-for which 55,000 Americans would die for in the next twenty years.

54

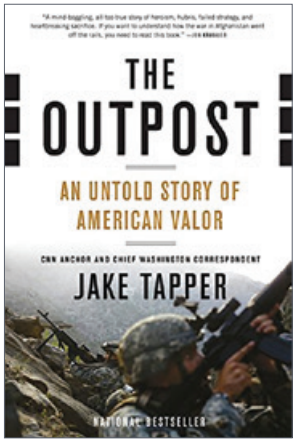


The Origins of War: And the Preservation of Peace

Donald Kagan, Anchor: 1996

War has been an unpleasant fact for centuries. By lucidly revealing the common threads that connect the ancient confrontations between Athens and Sparta and between Rome and Carthage with the two calamitous World Wars of the twentieth century, renowned historian Donald Kagan reveals new and surprising insights into the nature of war and peace. Vivid, incisive, and accessible, Kagan's powerful narrative warns against complacency and urgently reminds us of the importance of preparedness in times of peace.

55



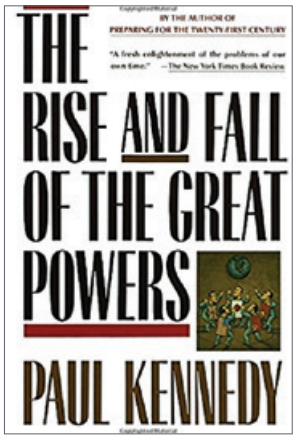
The Outpost: An Untold Story of American Valor

Jake Tapper, Hachette Book Group: 2012

★★★

At 5:58 AM on October 3, 2009, viciously attacked is Combat Outpost Keating, located in frighteningly vulnerable terrain in Afghanistan just 14 miles from the Pakistani border. Though the 53 Americans there prevailed against nearly 400 Taliban fighters, their casualties made it the deadliest fight of the war for the U.S. that year. Four months after the battle, a Pentagon review revealed that there was no reason for the troops at Keating to have been there in the first place. In The Outpost, Jake Tapper gives us the powerful saga of COP Keating, from its establishment to eventual destruction, introducing us to an unforgettable cast of soldiers and their families, and to a place and war that has remained profoundly distant to most Americans.

56

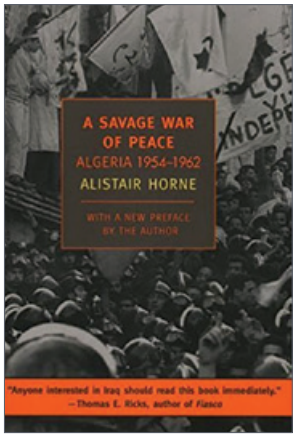


The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000

Paul Kennedy, First Vintage: 1989

The Rise and Fall of Great Powers: Economic Change and Military Conflict from 1500 to 2000, by Paul Kennedy, explores the politics and economics of the Great Powers from 1500 to 1980 and the reason for their decline. It then continues by forecasting the positions of China, Japan, the European Economic Community, the Soviet Union, and the United States through the end of the 20th century.

57

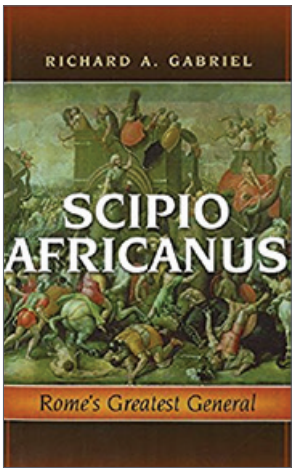


A Savage War of Peace: Algeria 1954-1962

Alistair Horne, NYRB Classics: 2006\0

The Algerian War, from 1954 to 1962, brought down six French governments, led to the collapse of the Fourth Republic, returned de Gaulle to power, and came close to provoking a civil war on French soil. The conflict caused more than a million Muslim Algerians to die and drove as many European settler into exile. Above all, an unholy marriage of revolutionary terror and repressive torture marked the war. Nearly a half century has passed since this savagely fought war ended in Algeria's independence, and yet—as Alistair Horne argues in his new preface to his now-classic work of history—its repercussions continue to be felt not only in Algeria and France, but throughout the world.

58



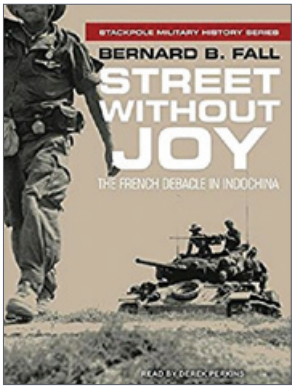
Scipio Africanus: Rome's Greatest General

Richard A. Gabriel, Potomac Books: 2008

★★★

Scholars celebrate the importance of Hannibal, even though Scipio defeated the legendary general in the Second Punic War and was the central military figure of his time. In this scholarly and heretofore unmatched military biography of the distinguished Roman soldier, Richard A. Gabriel establishes Scipio's rightful place in military history as the greater of the two generals. His book offers a complete bibliography of all extant sources regarding Scipio's life. The result is a rich, detailed, and contextual treatment of the life and career of Scipio Africanus, one of Rome's greatest generals, if not the greatest of them all.

59

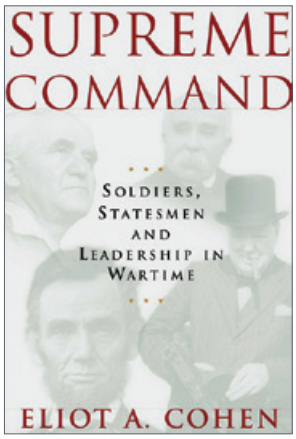


Street Without Joy: The French Debacle in Indochina

Bernard B. Fall, Stackpole Books: 2005

Originally published in 1961, before the United States escalated its involvement in South Vietnam, Street without Joy offered a clear warning about what American forces would face in the jungles of Southeast Asia: a costly and protracted revolutionary war fought without fronts against a mobile enemy. In harrowing detail, Fall describes the brutality and frustrations of the Indochina War, the savage eight-year conflict—ending in 1954 after the fall of Dien Bien Phu—in which French forces suffered a staggering defeat at the hands of Communist-led Vietnamese nationalists. With its frontline perspective, vivid reporting, and careful analysis, Street without Joy was required reading for policymakers in Washington and GIs in the field and is now considered a classic.

60

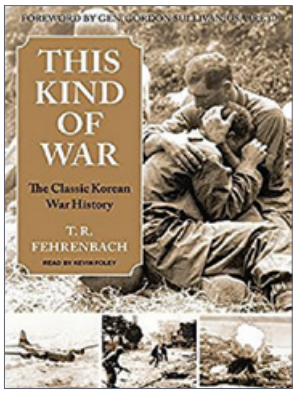


Supreme Command: Soldiers, Statesmen, and Leadership in Wartime

Eliot A. Cohen, Anchor: 2003

The orthodoxy regarding the relationship between politicians and military leaders in wartime democracies contends that politicians should declare a military operation's objectives and then step aside and leave the business of war to the military. In this controversial examination of civilian-military relations in wartime democracies, Eliot A. Cohen chips away at this time-honored belief with case studies of statesmen who dared to prod, provoke, and even defy their military officers to great effect. By examining the shared leadership traits of four politicians who triumphed in extraordinarily varied military campaigns, Cohen argues that active statesmen make the best wartime leaders, pushing their military subordinates to succeed where they might have failed if left to their own devices. Thought provoking and soundly argued, Cohen's Supreme Command is essential reading not only for military and political players but also for informed citizens and anyone interested in leadership.

61



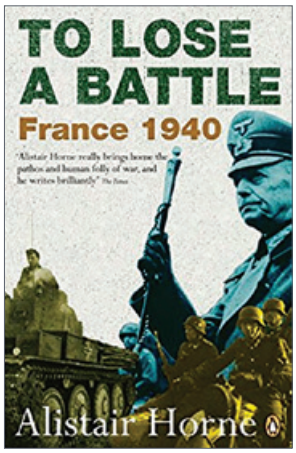
This Kind of War: A Study of Unpreparedness: The Classic Korean War History

T.R. Fehrenbach, Potomac Books; 50th Anniversary Edition: 2001

★★★

Updated with maps, photographs, and battlefield diagrams, this special fiftieth anniversary edition of the classic history of the Korean War is a dramatic and hard-hitting account of the conflict written from the perspective of those who fought it. Partly drawn from official records, operations journals, and histories, it is based largely on the compelling personal narratives of the small-unit commanders and their troops. Unlike any other work on the Korean War, it provides both a clear panoramic overview and a sharply drawn "you were there" account of American troops in fierce combat against the North Korean and Chinese communist invaders. As Americans and North Koreans continue to face each other across the 38th Parallel, This Kind of War commemorates the past and offers vital lessons for the future.

62

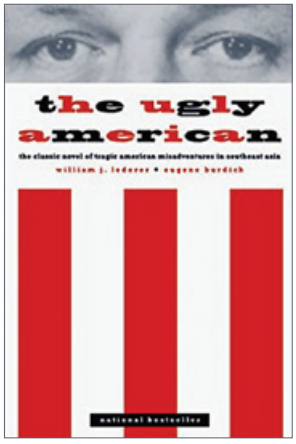


To Lose a Battle: France 1940

Alistair Horne, Penguin: 2007

In 1940, the German army fought and won an extraordinary battle with France in six weeks of lightning warfare. With the subtlety and compulsion of a novel, Horne's narrative shifts from minor battlefield incidents to high military and political decisions, stepping far beyond the confines of military history to form a major contribution to our understanding of the crises of the Franco-German rivalry. Told in two parts, the first section deals with the events that led up to the invasion in May 1940, while the second describes Germany's advance through France. Although the book rightfully praises the German offensive, Horne also notes Germany's mistakes that eventually led to its downfall.

63



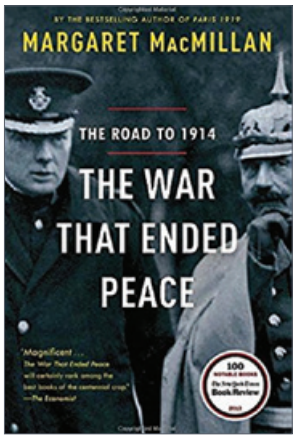
The Ugly American

Eugene Burdick and William J. Lederer, W.W. Norton and Company: 1999

★★★

First published in 1958, The Ugly American became a runaway national bestseller for its slashing exposé of American arrogance, incompetence, and corruption in Southeast Asia. Based on fact, the book's eye-opening stories and sketches drew a devastating picture of how the United States was losing the struggle with Communism in Asia. Combining gripping storytelling with an urgent call to action, the book prompted President Eisenhower to launch a study of our military aid program that led the much-needed reform. Modern reviews of the book have drawn parallels between South East Asia of the Cold War and the Middle East of today.

64



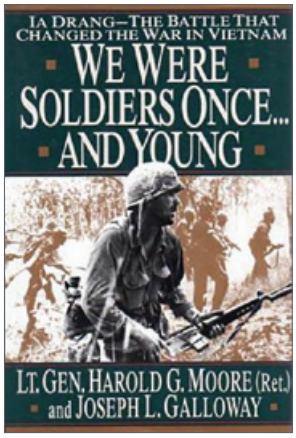
The War that Ended Peace: The Road to 1914

Margaret MacMillan, Random House: 2013

★★★

The century since the end of the Napoleonic wars had been the most peaceful era Europe had known since the fall of the Roman Empire. In the first years of the twentieth century, Europe believed it was marching to a golden, happy, and prosperous future. But instead, complex personalities and rivalries, colonialism and ethnic nationalisms, and shifting alliances helped to bring about the failure of the long peace and the outbreak of a war that transformed Europe and the world. The War That Ended Peace brings vividly to life the military leaders, politicians, diplomats, bankers, and the extended, interrelated family of crowned heads across Europe who failed to stop the descent into war. There are the would-be peacemakers as well, among them prophets of the horrors of future wars whose warnings went unheeded. With indelible portraits, MacMillan shows how the fateful decisions of a few powerful people changed the course of history. The War That Ended Peace is also a wise cautionary reminder of how wars happen in spite of the near-universal desire to keep the peace.

65



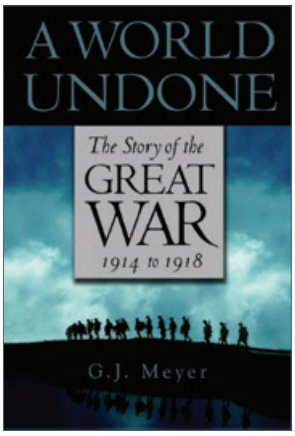
We Were Soldiers Once… and Young: Ia Drang-The Battle That Changed the War in Vietnam

Harold G. Moore and Joseph L. Galloway, Presidio Press: 2004 [First published in 1992]

★★★

In November 1965, dropped by helicopter into a small clearing in Ia Drang Valley were 450 men of the 1st Battalion, 7th Cavalry, under the command of Lt. Col. Hal Moore. Immediately 2,000 North Vietnamese soldiers surrounded them. Three days later, only two and a half miles away, a sister battalion was chopped to pieces. Together, these actions at the landing zones X-Ray and Albany constituted one of the most savage and significant battles of the Vietnam War. How these men persevered, sacrificed themselves for their comrades and never gave up, makes a vivid portrait of war at its most inspiring and devastating. This devastating account rises above the specific ordeal it chronicles to present a picture of men facing the ultimate challenge, dealing with it in ways they would have found unimaginable only a few hours earlier.

66

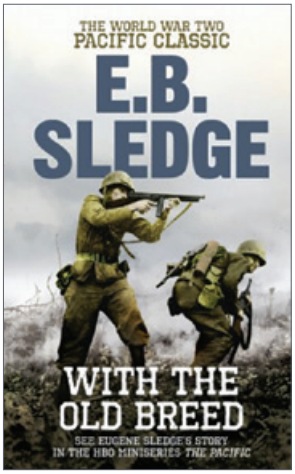


A World Undone: The Story of the Great War, 1914-1918

G.J. Meyer, Delacorte Press Books: 2006

The Great War defined the 20th century with countless tragedies and changes that have carried into today's society. A World Undone focuses on various significant unconnected events and the political and military leaders who lead the war—from the British Cabinet to Prussia—that ended with the death of 20 million people and the near end of civilization that had dominated the world up-to 1914.

67



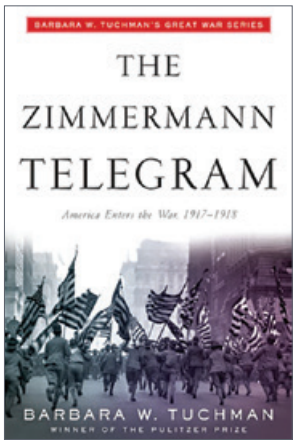
With the Old Breed: At Peleliu and Okinawa

E.B. Sledge, Oxford University Press: 2007 [First published in 1981 by Presidio Press]

★★★

An Alabama boy steeped in American history and enamored of such heroes as George Washington and Daniel Boone, Eugene B. Sledge became part of the war's famous 1st Marine Division—3rd Battalion, 5th Marines. Even after intense training, he was shocked to be thrown into the battle of Peleliu, where "the world was a nightmare of flashes, explosions, and snapping bullets." By the time Sledge hit the hell of Okinawa, he was a combat vet, still filled with fear but no longer with panic. Based on notes Sledge secretly kept in a copy of the New Testament, With the Old Breed captures with utter simplicity and searing honesty the experience of a soldier in the fierce Pacific Theater. Here is what saved, threatened, and changed his life. Here, too, is the story of how he learned to hate and kill—and came to love—his fellow man.

68



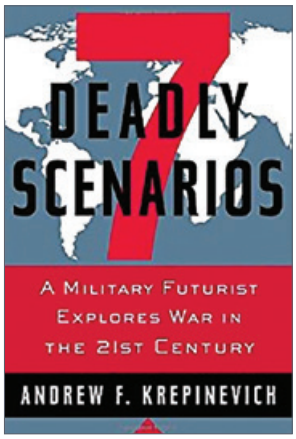
The Zimmermann Telegram

Barbara Tuchman, Random House: 1985

In January 1917, the war in Europe was, at best, a tragic standoff. Britain knew that all was lost unless the United States joined the war, but President Wilson was unshakable in his neutrality. At just that moment, a crack team of British decoders in a quiet office known as Room 40 intercepted a document that would change history. The Zimmermann telegram was a top-secret message to the president of Mexico, inviting him to join Germany and Japan in an invasion of the United States. How Britain managed to inform the American government without revealing that the German codes had been broken makes for an incredible story of espionage and intrigue, as only Barbara W. Tuchman could tell it.

GLOBAL ANALYSIS

69



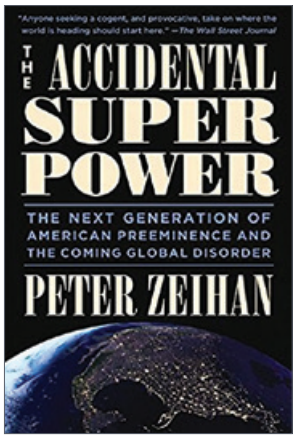
7 Deadly Scenarios: A Military Futurist Explores the Changing Face of War in the 21st Century

Andrew Krepinevich, Bantam; Reprint 2010

★★★

A global pandemic finds millions swarming across the U.S. border. Black-market nukes levels major American cities. China's growing civil unrest ignites a global showdown. Pakistan's collapse leads to a hunt for its nuclear weapons. What if the worst that could happen, actually happens? How will we respond? Are we prepared? These are the questions that Andrew F. Krepinevich asks—and answers—in this timely and often chilling book. As a military expert and consultant, Krepinevich must think the unthinkable based on the latest intelligence and geopolitical trends—and devise a response in the event our worst nightmares become reality.

70



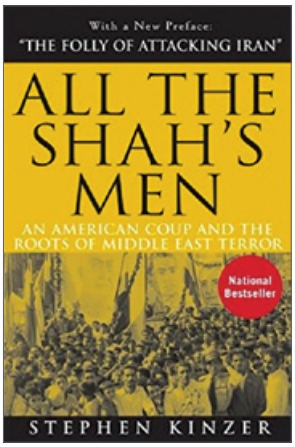
The Accidental Superpower: The Next Generation of American Preeminence and the Coming of Global Disorder

Peter Zeihan, Hachette Book Group: 2014

★★★

Near the end of the Second World War, the United States made a bold strategic gambit that rewired the international system. A global arrangement, enforced by the U.S. Navy, abolished and replaced empires. With all the world's oceans safe for the first time in history, made available for everyone were markets and resources. Enemies became partners. The Accidental Superpower examines how the hard rules of geography are eroding the American commitment to free trade; how much of the planet is aging into a mass retirement that will enervate markets and capital supplies; and how, against all odds, the ever-ravenous American economy that is rapidly approaching energy independence.

71

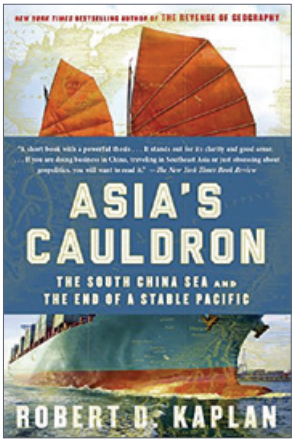


All the Shah's Men: An American Coup and the Roots of Middle East Terror

Stephen Kinzer, Wiley: Reprint 2008

With a thrilling narrative that sheds much light on recent events, this national bestseller brings to life the 1953 CIA coup in Iran that ousted the country's elected prime minister, ushered in a quarter-century of brutal rule under the Shah, and stimulated the rise of Islamic fundamentalism and anti-Americanism in the Middle East.

72

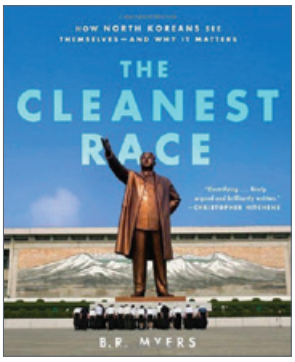


Asia's Cauldron: The South China Sea and the End of a Stable Pacific

Robert D. Kaplan, Random House: 2014

Over the last decade, the center of world power has been quietly shifting from Europe to Asia. With oil reserves of several billion barrels, an estimated nine hundred trillion cubic feet of natural gas, and several centuries' worth of competing territorial claims, the South China Sea in particular is a simmering pot of potential conflict. The underreported military buildup in the area where the Western Pacific meets the Indian Ocean means that it will likely be a hinge point for global war and peace for the foreseeable future. In Asia's Cauldron, Robert D. Kaplan offers up a vivid snapshot of the nations surrounding the South China Sea, the conflicts brewing in the region at the dawn of the twenty-first century, and their implications for global peace and stability.

73



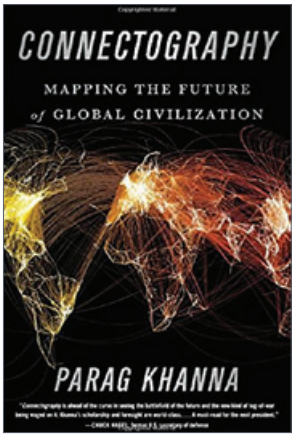
The Cleanest Race: How North Koreans See Themselves and Why It Matters

B.R. Myers, Melville House: 2011

★★★

Drawing on extensive research into the regime's domestic propaganda, including films, romance novels, and other artifacts of the personality cult, Myers analyzes each of the country's official myths in turn—from the notion of Koreans' unique moral purity to the myth of an America quaking in terror of "the Iron General." In a concise, but groundbreaking historical section, Myers also traces the origins of this official culture back to the Japanese fascist thought in which North Korea's first ideologues were schooled. What emerges is a regime completely unlike the West's perception of it. The implications for US foreign policy are as obvious as they are troubling.

74

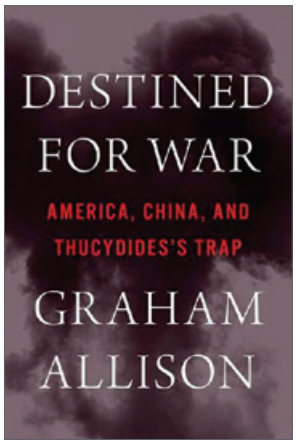


Connectography – Mapping the Future of Global Civilization

Parag Khanna, Random House: 2016

Connectivity is the most revolutionary force of the twenty-first century. Mankind is reengineering the planet, investing up to ten trillion dollars per year in transportation, energy, and communications infrastructure linking the world's burgeoning megacities together. Connectivity, not geography, is our destiny. In Connectography, Khanna shows how militaries are deployed to protect supply chains as much as borders, and how nations are less at war over territory than engaged in tugs-of-war over pipelines, railways, shipping lanes, and Internet cables. The new arms race is to connect to the most markets.

75



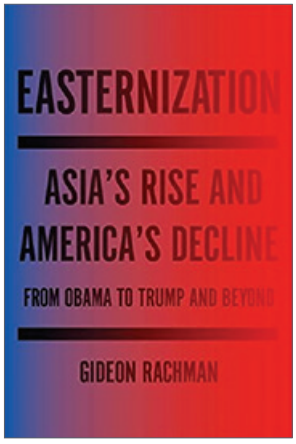
Destined for War: Can America and China Escape the Thucydides' Trap?

Graham Allison, Houghton Mifflin Harcourt: 2017

★★★

China and the United States are heading toward a war neither wants. The reason is Thucydides' Trap, a deadly pattern of structural stress that results when a rising power challenges a ruling one. Over the past 500 years, these conditions have occurred sixteen times and war broke out in twelve of them. Today, as an unstoppable China approaches an immovable America the seventeenth case looks grim. Unless China is willing to scale back its ambitions or Washington can accept becoming number two in the Pacific, a trade conflict, cyberattack, or accident at sea could soon escalate into all-out war. In Destined for War, Harvard scholar Graham Allison reveals how clashing powers have kept the peace in the past—and what painful steps the United States and China must take to avoid disaster today.

76

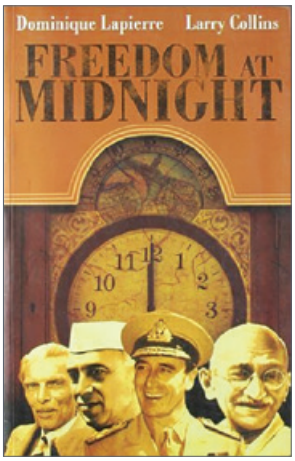


Easternization: Asia's Rise and America's Decline

Gideon Rachman, Other Press: 2017

Easternization is the defining trend of our age—the growing wealth of Asian nations is transforming the international balance of power. This shift to the East is shaping the lives of people all over the world, the fate of nations, and the great questions of war and peace. A troubled but rising China is now challenging America's supremacy, and the ambitions of other Asian powers—including Japan, North Korea, India, and Pakistan—have the potential to shake the whole world. Meanwhile the West is struggling with economic malaise and political populism, the Arab world is in turmoil, and Russia longs to reclaim its status as a great power. As it becomes clear that the West's historic power and influence is receding, Gideon Rachman offers a road map to the turbulent process that will define the international politics of the twenty-first century.

77

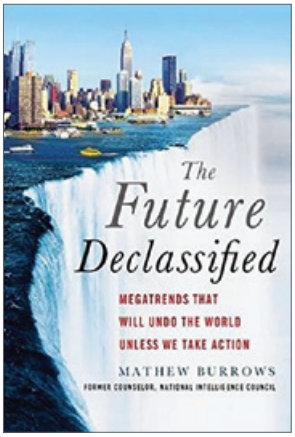


Freedom at Midnight

Dominique Lapierre and Larry Collins, Schand: 1975

Lapierre and Collins provide an account of the year leading to India's independence and the clashes that happened afterwards between Muslims and Hindus. With testimonies of those who witnessed and were involved with the country's historic changes, including the last viceroy Lord Louis Mountbatten, the reader gains insight into the decisions made by the political leaders who drove these changes. The authors walk through the challenges Gandhi, the first India Prime Minister Jawaharlal Nehru, and the founder of Pakistan Muhammad Ali Jinnah met as politics, religious differences, and ideologies clashed.

78

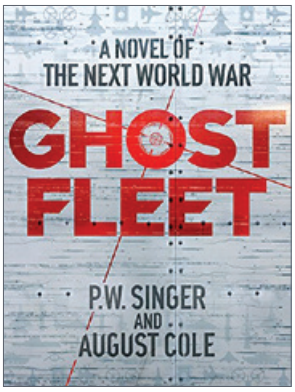


The Future, Declassified: Megatrends That Will Undo the World Unless We Take Action

Mathew Burrows, St. Martin's Press: 2014

Twenty-five years ago when Mathew Burrows went to work for the CIA as an intelligence analyst, the world seemed frozen. Then came the fall of the Berlin Wall and the implosion of the Soviet Union; suddenly, unpredictability became a universal theme and foresight was critical. For the past decade, Burrows has overseen the creation of the Global Trends report, and now he has expanded it into a full-length narrative—forecasting the tectonic shifts that will drive us to 2030. As Burrows argues, we are living through some of the greatest and most momentous developments in history. Either we take charge and direct those or we are at their mercy. The stakes are particularly high for America's standing in the world and for ordinary Americans who want to maintain their quality of life. Running the gamut from scary to reassuring, this riveting book is essential reading.

79



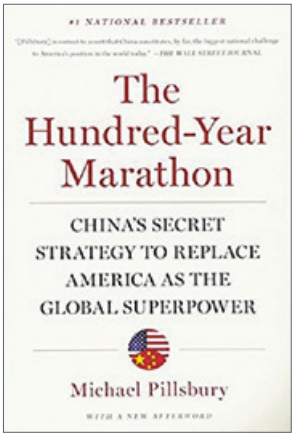
Ghost Fleet: A Novel of the Next World War

P.W. Singer and August Cole, First Mariner Books: 2015

★★★

The United States, China, and Russia eye each other across a twenty-first century version of the Cold War, which suddenly heats up at sea, on land, in the air, in outer space, and in cyberspace. The fighting involves everything; from stealthy robotic-style attack of drone strikes to old warships, from the Navy's "ghost fleet"; fighter pilots unleash a Pearl Harbor; American veterans become low-tech insurgents; teenage hackers battle in digital playgrounds; Silicon Valley billionaires mobilize for cyber-war; and a serial killer carries out her own vendetta. Ultimately, victory will depend on blending the lessons of the past with the weapons of the future.

80



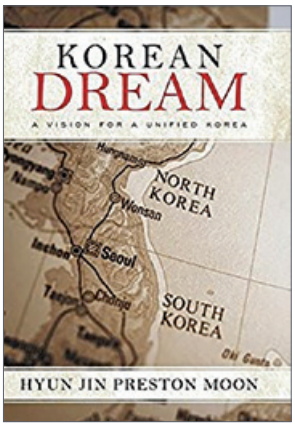
The Hundred-Year marathon: China's Secret Strategy to Replace America as the Global Superpower

Michael Pillsbury, Henry Holt and Company: 2016

★★★

For more than forty years, the United States has played an indispensable role helping the Chinese government build a booming economy, develop its scientific and military capabilities, and take its place on the world stage, in the belief that China's rise will bring us cooperation, diplomacy, and free trade. But what if the "China Dream" is to replace us, just as America replaced the British Empire, without firing a shot? Based on interviews with Chinese defectors and newly declassified, previously undisclosed national security documents, The Hundred-Year Marathon reveals China's secret strategy to supplant the United States as the world's dominant power, and to do so by 2049, the one-hundredth anniversary of the founding of the People's Republic.

81



Korean Dream: A Vision for a Unified Korea

Hyun Jin Preston Moon, Archway: 2016

★★★

North Korea today is a rogue state threatening global peace and challenging the conscience of humanity. In the South, Koreans now face long-term social consequences from the pursuit of economic development at all costs. In Korean Dream, Dr. Hyun Jin Preston Moon presents an innovative way forward on the Korean peninsula. He explains lucidly why Korean unification is the ultimate answer to security, economic, and social problems created through 70 years of division. He goes a step further, offering a groundbreaking approach to peace rooted in the founding principles and cultural practices that have made Koreans one people for millennia.

82

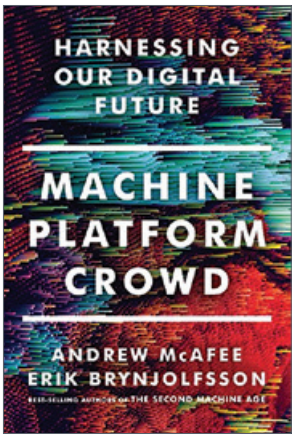
Lee Kuan Yew: The Grand Master's Insights on China, the United States, and the World

Graham Allison, Robert D. Blackwell, and Ali Wyne, The MIT Press: 2013

★★★

Almost single-handedly responsible for transforming Singapore into a Western-style economic success, Lee Kuan Yew offers a unique perspective on the geopolitics of East and West. This book gathers key insights from interviews, speeches, and Lee's voluminous published writings and presents them in an engaging question and answer format. Lee offers his assessment of China's future, asserting, among other things, "China will want to share this century as co-equals with the U.S." He affirms the United States' position as the world's sole superpower but expresses dismay at the vagaries of its political system. He offers strategic advice for dealing with China and discusses India's future, Islamic terrorism, and economic growth, among other topics. Lee does not pull punches, offering his unvarnished opinions on multiculturalism, the welfare state, education, and the free market.

83



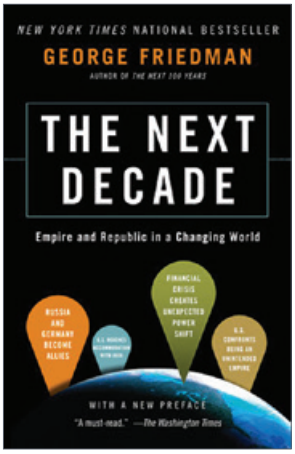
Machine, Platform, Crowd: Harnessing Our Digital Future

Andrew McAfee, W. W. Norton & Company: 2017

★★★

We live in strange times. A machine plays the strategy game Go better than any human; upstarts like Apple and Google destroy industry stalwarts such as Nokia; ideas from the crowd are repeatedly more innovative than corporate research labs. We must rethink the integration of minds and machines, of products and platforms, and of the core and the crowd. In all three cases, the balance now favors the second element of the pairings, with massive implications for how we run our companies and live our lives. Andrew McAfee and Erik Brynjolfsson deliver both a penetrating analysis of a new world and a toolkit for thriving in it. For startups and established businesses, or for anyone interested in what the future holds, Machine, Platform, Crowd is essential reading.

84



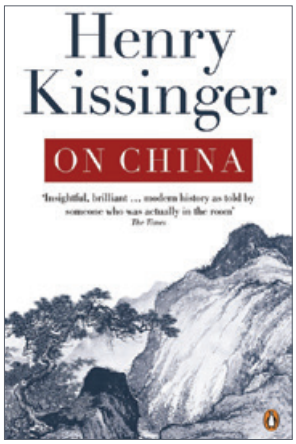
The Next Decade

George Friedman, Anchor: 2012

★★★

In the long view, history is seen as a series of events—but individuals and their actions determine the course of those events. During the next ten years, individual leaders will face significant transitions for their nations: the United States' relationships with Iran and Israel will be undergoing changes, China will likely confront a major crisis, and the wars in the Islamic world will subside. Unexpected energy and technology developments will emerge, and labor shortages will begin to matter more than financial crises. Distinguished geopolitical forecaster George Friedman analyzes these events from the perspectives of the men and women leading these global changes, focusing in particular on the American president, who will require extraordinary skills to shepherd the United States through this transitional period.

85



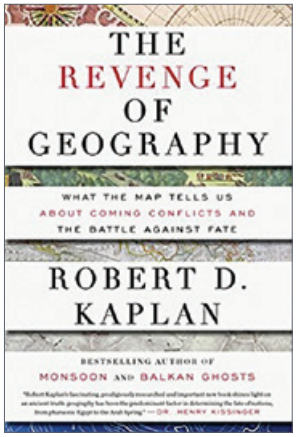
On China

Henry Kissinger, Penguin Books: 2012

★★★

In this sweeping and insightful history, Henry Kissinger turns for the first time at book length to a country he has known intimately for decades and whose modern relations with the West he helped shape. On China illuminates the inner workings of Chinese diplomacy during such pivotal events as the initial encounters between China and tight line modern European powers, the formation and breakdown of the Sino-Soviet alliance, the Korean War, and Richard Nixon's historic trip to Beijing. With a new final chapter on the emerging superpower's twenty-first-century role in global politics and economics, On China provides historical perspective on Chinese foreign affairs from one of the premier statesmen of our time.

86

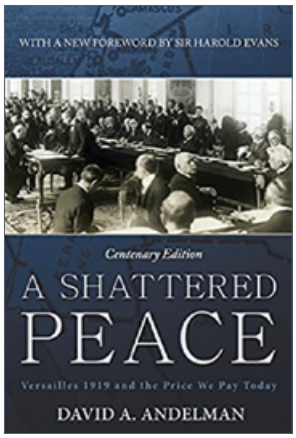


The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate

Robert D. Kaplan, Random House: 2012

In The Revenge of Geography, Kaplan builds on the insights, discoveries, and theories of great geographers and geopolitical thinkers of the near and distant past to look back at critical pivots in history and then to look forward at the evolving global scene. Kaplan traces the history of the world's hot spots by examining their climates, topographies, and proximities to other embattled lands. Kaplan then applies the lessons learned to the present crises in Europe, Russia, China, the Indian subcontinent, Turkey, Iran, and the Arab Middle East. The result is a holistic interpretation of the next cycle of conflict throughout Eurasia. A brilliant rebuttal to thinkers who suggest that globalism will trump geography, this indispensable work shows how timeless truths and natural facts can help prevent this century's looming cataclysms.

87



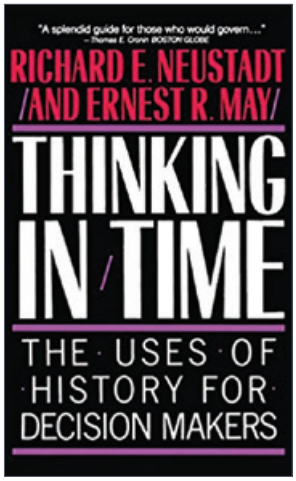
A Shattered Peace: Versailles 1919 and the Price We Pay Today

David A. Andelman, Wiley General Trade: 2014

★★★

For more than half a century, it has been widely recognized that the Treaty of Versailles, founded on retribution against Germany and the Austro-Hungarian Empire, created the circumstances that led inevitably to World War II. Less acknowledged and understood is the treaty's profound impact on many other parts of the world—an impact that echoes to this day across Asia, the Balkans, and throughout the Middle East. Andelman takes a fresh new look at the Treaty of Versailles as the point of origin for many of today's most critical international issues. This revealing history exposes the powerful lessons that a six-month period in a long ago era has for us today.

88

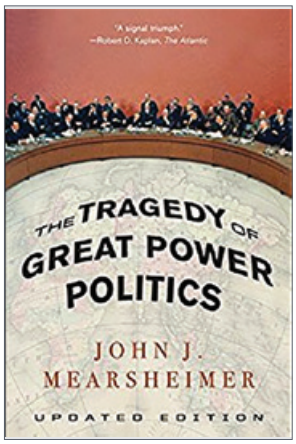


Thinking in Time: The Uses of History for Decision-Makers

Richard E. Neustadt and Ernest R. May, The Free Press: 1986

For generations Americans have described and deplored the ignorance of history displayed by policymakers or, what is worse, the misuse of historical analogies. Since the 1950s Professors Neustadt and May have been working individually through their writing and consulting on this subject; in the past decade they have been collaborators in a course at Harvard's John F. Kennedy School of Government focusing explicitly on "using history." This excellent book is a product of that course: case histories from both domestic and foreign policy areas and a set of precepts-what to ask about history and how to ask it. Professional historians, enjoying the luxury of unhurried reflection, might say that the book's "method" is no more than a systematic and common-sense statement of the obvious-but the authors demonstrate that the "obvious" has too often been ignored, with unfortunate results.

89



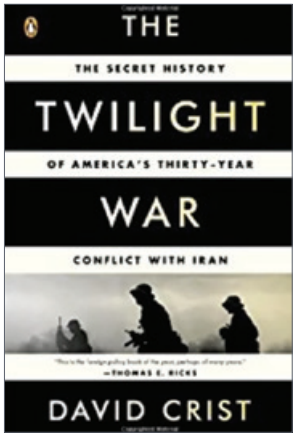
The Tragedy of Great Power Politics (Updated Edition)

John J. Mearsheimer, W.W. Norton & Company: 2001

★★★

The updated edition of this classic treatise on the behavior of great powers takes a penetrating look at the question likely to dominate international relations in the twenty-first century: can China rise peacefully? In clear, eloquent prose, Mearsheimer explains why the answer is no: a rising China will seek to dominate Asia, while the United States, determined to remain the world's sole regional hegemon, will go to great lengths to prevent that from happening. The tragedy of great power politics is inescapable.

90

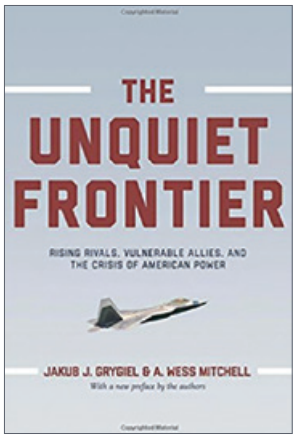


The Twilight War: The Secret History of America's Thirty-Year Conflict with Iran

David Crist, Penguin Press 2012

For three decades, the United States and Iran have engaged in a secret war—it is a conflict not acknowledged and a story not told. A senior historian for the federal government with unparalleled access to senior officials and key documents of several U.S. administrations, Crist has spent more than ten years researching and writing The Twilight War. He breaks new ground on virtually every page, and he reveals in vivid detail for the first time a number of important stories of military and intelligence operations by both sides, both successes and failures, and their typically unexpected consequences. The Twilight War adds vital new depth to our understanding of this acute dilemma. It is also a thrillingly engrossing read, animated by a healthy irony about human failings in the fog of not-quite war.

91



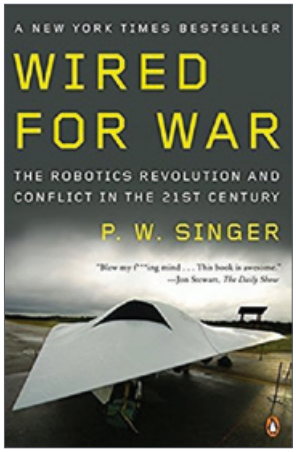
The Unquiet Frontier: Rising Rivals, Vulnerable Allies, and the Crisis of American Power

Jakub J. Grygiel, A. Wess Mitchell, Princeton University Press: 2016

★★★

From the Baltic to the South China Sea, newly assertive authoritarian states sense an opportunity to resurrect old empires or build new ones at America's expense. Hoping that U.S. decline is real, nations such as Russia, Iran, and China are testing Washington's resolve by targeting vulnerable allies at the frontiers of American power. The Unquiet Frontier explains why the United States needs a new grand strategy that uses strong frontier alliance networks to raise the costs of military aggression in the new century.

92



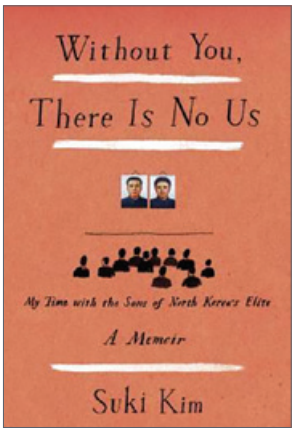
Wired for War: The Robotics Revolution and Conflict in the 21st Century

P.W. Singer, The Penguin Press: 2009

★★★

In Wired for War, P. W. Singer explores the greatest revolution in military affairs since the atom bomb: the dawn of robotic warfare. We are on the cusp of a massive shift in military technology that threatens to make real the stuff of I, Robot and The Terminator. Blending historical evidence with interviews of an amazing cast of characters, Singer shows how technology is changing not just how wars are fought, but also the politics, economics, laws, and the ethics that surround war itself. Travelling from the battlefields of Iraq and Afghanistan to modern-day "skunk works" in the midst of suburbia, Wired for War will tantalize a wide readership, from military buffs to policy wonks to gearheads.

93

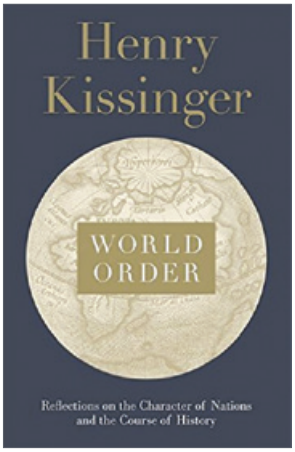


Without You, There Is No Us: My Time with the Sons of North Korea's

Suki Kim, Crown: 2014

It is 2011, and all universities in North Korea have been shut down for an entire year, the students sent to construction fields—except for the 270 students at the all-male Pyongyang University of Science and Technology (PUST), where Suki has gone undercover as a missionary and a teacher. As the weeks pass, she is mystified by how easily her students lie, unnerved by their obedience to the regime. At the same time, they offer Suki tantalizing glimpses of their private selves—their boyish enthusiasm, their eagerness to please, the flashes of curiosity that have not yet been extinguished. She in turn begins to hint at the existence of a world beyond their own—at such exotic activities as surfing the Internet or traveling freely and, more dangerously, at electoral democracy and other ideas forbidden in a country where defectors risk torture and execution. However, when Kim Jong-il dies and the boys she has come to love appear devastated, she wonders whether a bridge may form between the gulf of her world and theirs. Without You, There Is No Us offers a moving and incalculably rare glimpse of life in the world's most unknowable country, and at the privileged young men, she calls "soldiers and slaves."

94



World Order

Henry Kissinger, Penguin Books: 2015

Henry Kissinger offers, in World Order, a deep meditation on the roots of international harmony and global disorder. Kissinger reveals his analysis on the ultimate challenge for the twenty-first century: how to build a shared international order in a world of divergent historical perspectives, violent conflict, proliferating technology, and ideological extremism. Drawing on his experience as one of the foremost political leaders of the modern era, and his experience as national security advisor and secretary of state, World Order guides readers through crucial episodes in recent world history. Provocative and articulate, blending historical insight with geopolitical prognostication, World Order is a unique work that could come only from a lifelong policy maker and diplomat.

This reading list and enclosed summaries are provided as a convenience and for informational purposes only; they do not constitute an endorsement or an approval by the Defense Intelligence Agency of any of the products, services or opinions of the authors. The Defense Intelligence Agency bears no responsibility for the accuracy, legality or content of the books referenced in this reading list.

DEFENSE INTELLIGENCE AGENCY

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

Joint Publication 1-02

Department of Defense Dictionary of Military and Associated Terms

8 November 2010

(As Amended Through

15 February 2016)

PREFACE

1. Scope

The Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms,* sets forth standard US military and associated terminology to encompass the joint activity of the Armed Forces of the United States. These military and associated terms, together with their definitions, constitute approved Department of Defense (DOD) terminology for general use by all DOD components.

2. Purpose

This publication supplements standard English-language dictionaries and standardizes military and associated terminology to improve communication and mutual understanding within DOD, with other federal agencies, and among the United States and its allies.

3. Application

This publication applies to the Office of the Secretary of Defense, the Services, the Joint Staff, combatant commands, DOD agencies, and all other DOD components. It is the primary terminology source when preparing correspondence, to include policy, strategy, doctrine, and planning documents. Criteria for inclusion of terminology in JP 1-02 is enumerated in Department of Defense Instruction 5025.12, *Standardization of Military and Associated Terminology,* and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5705.01, *Standardization of Military and Associated Terminology*.

4. Publication Format

This edition of JP 1-02 has been published in two basic parts:

a. Terms and definitions. These are annotated with the source publication.

b. Abbreviations and acronyms. The source publication establishes the authoritative context for proper understanding and management of the associated term.

5. JP 1-02 Online Availability and Update Schedule

JP 1-02 is accessible online as a searchable database and in PDF format at the following Internet address: http://www.dtic.mil/doctrine/dod_dictionary and at the following NIPRNET

address: https://jdeis.js.mil/jdeis/. The contents of JP 1-02 are updated on a monthly basis to include any terminology additions, modifications, or deletions made within the previous calendar month in accordance with CJCSI 5705.01.

For the Chairman of the Joint Chiefs of Staff:

WILLIAM E. GORTNEY
Vice Admiral, USN
Director, Joint Staff

TABLE OF CONTENTS

MAIN BODY 1

APPENDIX

A Abbreviations and Acronyms A-1

B Administrative Instructions B-1

Intentionally Blank

A

acceptability — The joint operation plan review criterion for assessing whether the contemplated course of action is proportional, worth the cost, consistent with the law of war; and is militarily and politically supportable. See also **adequacy; feasibility.** (JP 5-0)

access — In counterintelligence and intelligence use, a. a way or means of approach to identify a target; or b. exploitable proximity to or ability to approach an individual, facility, or information that enables target to carry out the intended mission. (JP 2-01.2)

access to classified information — The ability and opportunity to obtain knowledge of classified information by persons with the proper security clearance and a need to know of specified classified information. (JP 2-01)

accompanying supplies — Unit supplies that deploy with forces. (JP 4-01.5)

accountability — The obligation imposed by law or lawful order or regulation on an officer or other person for keeping accurate record of property, documents, or funds. (JP 1)

acoustic intelligence — Intelligence derived from the collection and processing of acoustic phenomena. Also called **ACINT.** (JP 2-0)

acquisition and cross-servicing agreement — Agreement, negotiated on a bilateral basis with United States allies or coalition partners, that allow United States forces to exchange most common types of support, including food, fuel, transportation, ammunition, and equipment. Also called **ACSA.** See also **cross-servicing.** (JP 4-08)

actionable intelligence — Intelligence information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process. (JP 2-01.2)

action phase — In amphibious operations, the period of time between the arrival of the landing forces of the amphibious force in the operational area and the accomplishment of their mission. See also **amphibious force; amphibious operation; landing force; mission.** (JP 3-02)

activation — Order to active duty (other than for training) in the federal service. See also **active duty; federal service.** (JP 4-05)

active air defense — Direct defensive action taken to destroy, nullify, or reduce the effectiveness of hostile air and missile threats against friendly forces and assets. See also **air defense.** (JP 3-01)

active defense — The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy. See also **passive defense.** (JP 3-60)

active duty — Full-time duty in the active military service of the United States, including active duty or full-time training duty in the Reserve Component. Also called **AD.** See also **active duty for training; inactive duty training**. (JP 4-05)

active duty for special work — A tour of active duty for reserve personnel authorized from military and reserve personnel appropriations for work on active or reserve component programs. Also called **ADSW.** (JP 1-0)

active duty for training — A tour of active duty that is used for training members of the Reserve Component to provide trained units and qualified persons to fill the needs of the Armed Forces in time of war or national emergency and such other times as the national security requires. Also called **ADT.** (JP 4-05)

Active Guard and Reserve — National Guard and Reserve members who are on voluntary active duty providing full-time support to National Guard, Reserve, and Active Component organizations for the purpose of organizing, administering, recruiting, instructing, or training the Reserve Components. Also called **AGR.** (CJCSM 3150.13)

activity — 1. A unit, organization, or installation performing a function or mission. 2. A function, mission, action, or collection of actions. Also called **ACT.** (JP 3-0)

act of mercy — In personnel recovery, assistance rendered to evaders by an individual or elements of the local population who sympathize or empathize with the evaders' cause or plight. See also **evader; evasion; recovery; recovery operations.** (JP 3-50)

acute radiation dose — Total ionizing radiation dose received at one time and over a period so short that biological recovery cannot occur. (JP 3-11)

acute radiation syndrome — An acute illness caused by irradiation of the body by a high dose of penetrating radiation in a very short period of time. Also called **ARS.** (JP 3-11)

Adaptive Planning and Execution system — A Department of Defense system of joint policies, processes, procedures, and reporting structures, supported by communications and information technology, that is used by the joint planning and execution community to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint operations. Also called **APEX system.** (JP 5-0)

adequacy — The joint operation plan review criterion for assessing whether the scope and concept of planned operations can accomplish the assigned mission and comply with the planning guidance provided. See also **acceptability; feasibility.** (JP 5-0)

administrative chain of command — One of the two branches of the chain of command described in Joint Publication 1, *Doctrine for the Armed Forces of the United States*, through which command is exercised from the President through the Secretary of Defense to the Secretaries of the Military Departments, and from which forces are

assigned to combatant commands to compose the operational command structure baseline. (DODI 8260.03)

administrative command structure — The organizational hierarchy through which administrative leadership is exercised, as contrasted by the operational command structure through which operational authority is exercised. (DODI 8260.03)

administrative contracting officer — Contracting officer whose primary duties involve contract administration. Also called **ACO.** See also **contracting officer; procuring contracting officer.** (JP 4-10)

administrative control — Direction or exercise of authority over subordinate or other organizations in respect to administration and support. Also called **ADCON.** (JP 1)

administrative loading — A loading method that gives primary consideration to achieving maximum utilization of troop and cargo space without regard to tactical considerations. Also called **commercial loading.** (JP 3-02.1)

advanced force operations — Operations conducted to refine the location of specific, identified targets and further develop the operational environment for near-term missions. Also called **AFO.** (JP 3-05

advance guard — Detachment sent ahead of the main force to ensure its uninterrupted advance; to protect the main body against surprise; to facilitate the advance by removing obstacles and repairing roads and bridges; and to cover the deployment of the main body if it is committed to action. (JP 3-07.2)

adversary — A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

adversary template — A model based on an adversary's known or postulated preferred methods of operation illustrating the disposition and activity of adversary forces and assets conducting a particular operation unconstrained by the impact of the operational environment. (JP 2-01.3)

Aegis — A ship-based combat system that can detect, track, target, and engage air, surface, and subsurface threats, including ballistic missiles on some modified ships. (JP 3-01)

aerial port — An airfield that has been designated for the sustained air movement of personnel and materiel as well as an authorized port for entrance into or departure from the country where located. Also called **APORT.** See also **port of debarkation; port of embarkation**. (JP 3-17)

aeromedical evacuation — The movement of patients under medical supervision to and between medical treatment facilities by air transportation. Also called **AE.** (JP 4-02)

aeromedical evacuation control team — A core team assigned to a component-numbered air force air operations center air mobility division that provides operational planning, scheduling, and execution of theater aeromedical evacuation missions and positioning of aeromedical evacuation ground forces. Also called **AECT.** See also **aeromedical evacuation; air mobility division.** (JP 3-17)

aeromedical evacuation unit — An operational medical organization concerned primarily with the management and control of patients being transported via an aeromedical evacuation system or system echelon. (JP 4-02)

aeronautical chart — A specialized representation of mapped features of the Earth, or some part of it, produced to show selected terrain, cultural and hydrographic features, and supplemental information required for air navigation, pilotage, or for planning air operations. (JP 2-03)

aerospace defense — 1. All defensive measures designed to destroy or nullify attacking enemy aircraft and missiles and also negate hostile space systems. 2. An inclusive term encompassing air defense, ballistic missile defense, and space defense. See also **air defense**; **space defense.** (JP 3-27)

afloat pre-positioning force — Shipping maintained in full operational status to afloat pre-position military equipment and supplies in support of combatant commanders' operation plans, consisting of the three maritime pre-positioning ships squadrons, the Army's afloat pre-positioning stocks-3 ships, and the Defense Logistics Agency, and the Air Force ships. Also called **APF.** See also **maritime pre-positioning ships.** (JP 4-01.2)

afloat pre-positioning operations — Pre-positioning of ships, preloaded with equipment and supplies that provides for an alternative to land-based programs. Also called **APO**. See also **operation.** (JP 4-01.6)

agency — In intelligence usage, an organization or individual engaged in collecting and/or processing information. Also called **collection agency.** See also **agent**; **intelligence process**; **source.** (JP 2-01)

agent — In intelligence usage, one who is authorized or instructed to obtain or to assist in obtaining information for intelligence or counterintelligence purposes. (JP 2-01.2)

aimpoint — 1. A point associated with a target and assigned for a specific weapon impact. 2. A prominent radar-significant feature used to assist an aircrew in navigating and delivering their weapons. See also **desired point of impact.** (JP 3-60)

air and missile defense — Direct [active and passive] defensive actions taken to destroy, nullify, or reduce the effectiveness of hostile air and ballistic missile threats against friendly forces and assets. Also called **AMD.** (JP 3-01)

air apportionment — The determination and assignment of the total expected effort by percentage and/or by priority that should be devoted to the various air operations for a given period of time. (JP 3-0)

air assault — The movement of friendly assault forces by rotary-wing aircraft to engage and destroy enemy forces or to seize and hold key terrain. See also **assault.** (JP 3-18)

air assault force — A force composed primarily of ground and rotary-wing air units organized, equipped, and trained for air assault operations. (JP 3-18)

air assault operation — An operation in which assault forces, using the mobility of rotary-wing assets and the total integration of available firepower, maneuver under the control of a ground or air maneuver commander to engage enemy forces or to seize and hold key terrain. (JP 3-18)

airborne — 1. In relation to personnel, troops especially trained to effect, following transport by air, an assault debarkation, either by parachuting or touchdown. 2. In relation to equipment, pieces of equipment that have been especially designed for use by airborne troops during or after an assault debarkation as well as some aeronautical equipment used to accomplish a particular mission. 3. When applied to materiel, items that form an integral part of the aircraft. 4. The state of an aircraft, from the instant it becomes entirely sustained by air until it ceases to be so sustained. Also called **ABN.** (JP 3-17)

airborne alert — A state of aircraft readiness wherein combat-equipped aircraft are airborne and ready for immediate action to reduce reaction time and to increase survivability. See also **combat air patrol; ground alert.** (JP 3-01)

airborne assault — The use of airborne forces to parachute into an objective area to attack and eliminate armed resistance and secure designated objectives. (JP 3-18)

airborne early warning — The detection of enemy air or surface units by radar or other equipment carried in an airborne vehicle, and the transmitting of a warning to friendly units. Also called **AEW**. (JP 3-52)

airborne mission coordinator — The designated individual that serves as an airborne extension of the component commander or supported commander responsible for the personnel recovery mission. Also called **AMC.** See also **combat search and rescue; personnel recovery coordination cell.** (JP 3-50)

airborne operation — An operation involving the air movement into an objective area of combat forces and their logistic support for execution of a tactical, operational**,** or strategic mission. See also **assault; assault phase.** (JP 3-18)

air-breathing missile — A missile with an engine requiring the intake of air for combustion of its fuel, as in a ramjet or turbojet. (JP 3-01)

air-capable ship — A ship other than an aircraft carrier, nuclear; amphibious assault ship (general purpose); or amphibious assault ship (multipurpose) from which aircraft can take off, be recovered, or routinely receive and transfer logistic support. Also called **ACS.** (JP 3-04)

air corridor — A restricted air route of travel specified for use by friendly aircraft and established for the purpose of preventing friendly aircraft from being fired on by friendly forces. (JP 3-52)

aircraft carrier — A warship designed to support and operate aircraft, engage in attacks on targets afloat or ashore, and engage in sustained operations in support of other forces. Also called **CV or CVN.** (JP 3-32)

air defense — Defensive measures designed to destroy attacking enemy aircraft or missiles in the atmosphere, or to nullify or reduce the effectiveness of such attack. Also called **AD.** See also **active air defense; aerospace defense; passive air defense.** (JP 3-01)

air defense area — 1. **overseas** — A specifically defined airspace for which air defense must be planned and provided. 2. **United States** — Airspace of defined dimensions designated by the appropriate agency within which the ready control of airborne vehicles is required in the interest of national security during an air defense emergency. (JP 3-01)

air defense artillery — Weapons and equipment for actively combating air targets from the ground. Also called **ADA.** (JP 3-01)

air defense identification zone — Airspace of defined dimensions within which the ready identification, location, and control of airborne vehicles are required. Also called **ADIZ.** (JP 3-52)

air defense region — A geographical subdivision of an air defense area. (JP 3-01)

air defense sector — A geographical subdivision of an air defense region. (JP 3-01)

air defense warning condition — An air defense warning given in the form of a color code corresponding to the degree of air raid probability with yellow standing for when an attack by hostile aircraft or missiles is probable; red for when an attack by hostile aircraft or missiles is imminent or is in progress; and white for when an attack by hostile aircraft or missiles is improbable. Also called **ADWC.** (JP 3-01)

air domain — The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible. (JP 3-30)

airdrop — The unloading of personnel or materiel from aircraft in flight. See also **air movement; free drop; free fall; high velocity drop; low velocity drop.** (JP 3-17)

air expeditionary task force — A deployed numbered air force or command echelon immediately subordinate to a numbered air force provided as the United States Air Force component command committed to a joint operation. Also called **AETF.** (JP 3-30)

airfield — An area prepared for the accommodation (including any buildings, installations, and equipment), landing, and takeoff of aircraft. See also **departure airfield; landing area; landing site.** (JP 3-17)

Air Force special operations air component — The Air Force component of a joint special operations force, normally composed of a special operations wing, special operations group, or squadron, and element of an Air Force special tactics personnel. Also called **AFSOAC**. (JP 3-05)

Air Force special operations air detachment — A squadron-size headquarters that could be a composite organization composed of different Air Force special operations assets, normally subordinate to an Air Force special operations air component, joint special operations air component, joint special operations task force, or a joint task force. Also called **AFSOAD.** (JP 3-05)

Air Force special operations forces — Those Active and Reserve Component Air Force forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. Also called **AFSOF.** (JP 3-05)

airhead — 1. A designated area in a hostile or potentially hostile operational area that, when seized and held, ensures the continuous air landing of troops and materiel and provides the maneuver space necessary for projected operations. Also called **a lodgment area**. (JP 3-18) 2. A designated location in an operational area used as a base for supply and evacuation by air. See also **beachhead.** (JP 3-17)

airhead line — A line denoting the limits of the objective area for an airborne assault. See also **airhead; assault phase; objective area.** (JP 3-18)

air interdiction — Air operations conducted to divert, disrupt, delay, or destroy the enemy's military surface capabilities before it can be brought to bear effectively against friendly forces, or to otherwise achieve objectives that are conducted at such distances from friendly forces that detailed integration of each air mission with the fire and movement of friendly forces is not required. (JP 3-03)

airland — Move by air and disembark, or unload, after the aircraft has landed or while an aircraft is hovering. See also **air movement.** (JP 3-17)

air land operation — An operation involving movement by air with a designated destination for further ground deployment of units and personnel and/or further ground distribution of supplies. See also **airland.** (JP 3-17)

air liaison officer — The senior tactical air control party member attached to a ground unit who functions as the primary advisor to the ground commander on air power. Also called **ALO.** See also **liaison.** (JP 3-09.3)

airlift capability — The total capacity expressed in terms of number of passengers and/or weight/cubic displacement of cargo that can be carried at any one time to a given destination by available airlift. See also **airlift requirement.** (JP 3-17)

airlift control team — A core team within the joint air operations center with intratheater airlift functional expertise to plan, coordinate, manage, and execute intratheater airlift operations in support of the joint force air component commander. Also called **ALCT.** See also **air operations center; air mobility division; intratheater airlift.** (JP 3-17)

airlift mission commander — A commander designated when airlift aircraft are participating in airlift operations specified in the implementing directive. See also **joint force air component commander.** (JP 3-17)

airlift requirement — The total number of passengers and/or weight/cubic displacement of cargo required to be carried by air for a specific task. See also **airlift capability.** (JP 3-17)

air mobility — The rapid movement of personnel, materiel and forces to and from or within a theater by air. See also **air refueling.** (JP 3-17)

Air Mobility Command — The Air Force component command of the United States Transportation Command. Also called **AMC.** (JP 3-17)

air mobility control team — A core team within the joint air operations center that directs or redirects air mobility forces in response to requirements changes, higher priorities, or immediate execution requirements. Also called **AMCT.** See also **air operations center; air mobility; air mobility division.** (JP 3-17)

air mobility division — Located in the joint air operations center to plan, coordinate, task, and execute the air mobility mission consisting of the air mobility control team, airlift control team, air refueling control team, and aeromedical evacuation control team. Also called **AMD.** See also **air mobility; joint air operations center.** (JP 3-17)

air mobility liaison officer — A rated United States Air Force mobility air forces officer selected, trained, and equipped to assess, train, advise, and assist with mobility air forces and ground force integration for air movement and sustainment. Also called **AMLO.** (JP 3-17)

air movement — Air transport of units, personnel, supplies, and equipment including airdrops and air landings. See also **airdrop; airland.** (JP 3-17)

air operations center — The senior agency of the Air Force component commander that provides command and control of Air Force air and space operations and coordinates with other components and Services. Also called **AOC.** (JP 3-30)

air refueling — The refueling of an aircraft in flight by another aircraft. Also called **AR.** (JP 3-17)

air refueling control team — A core team within the joint air operations center that coordinates aerial refueling to support combat air operations or to support a strategic airbridge. Also called **ARCT.** See also **air operations center; air mobility division; air refueling.** (JP 3-17)

air route — The navigable airspace between two points, identified to the extent necessary for the application of flight rules. (JP 3-52)

air sovereignty — A nation's inherent right to exercise absolute control and authority over the airspace above its territory. (JP 3-27)

airspace control — Capabilities and procedures used to increase operational effectiveness by promoting the safe, efficient, and flexible use of airspace. (JP 3-52)

airspace control area — Airspace that is laterally defined by the boundaries of the operational area, and may be subdivided into airspace control sectors. (JP 3-01)

airspace control authority — The commander designated to assume overall responsibility for the operation of the airspace control system in the airspace control area. Also called **ACA.** See also **airspace control; airspace control area; airspace control system; control; operation.** (JP 3-52)

airspace control order — An order implementing the airspace control plan that provides the details of the approved requests for airspace coordinating measures. Also called **ACO.** (JP 3-52)

airspace control plan — The document approved by the joint force commander that provides specific planning guidance and procedures for the airspace control system for the joint force operational area. Also called **ACP.** See also **airspace control system; joint force commander.** (JP 3-52)

airspace control procedures — Rules, mechanisms, and directions that facilitate the control and use of airspace of specified dimensions. See also **airspace control authority; airspace control order; airspace control plan.** (JP 3-52)

airspace control system — An arrangement of those organizations, personnel, policies, procedures, and facilities required to perform airspace control functions. Also called **ACS.** (JP 3-52)

airspace coordinating measures — Measures employed to facilitate the efficient use of airspace to accomplish missions and simultaneously provide safeguards for friendly forces. Also called **ACMs.** See also **airspace control area; airspace coordination area; high-density airspace control zone; weapons engagement zone.** (JP 3-52)

airspace coordination area — A three-dimensional block of airspace in a target area, established by the appropriate commander, in which friendly aircraft are reasonably safe from friendly surface fires. Also called **ACA.** (JP 3-09.3)

airspace management — The coordination, integration, and regulation of the use of airspace of defined dimensions. (JP 3-52)

air superiority — That degree of dominance in the air battle by one force that permits the conduct of its operations at a given time and place without prohibitive interference from air and missile threats. (JP 3-01)

air support coordination section — In amphibious operations, the section of the Navy tactical air control center designated to coordinate, control, and integrate all direct support aircraft and assault support operations. Also called **ASCS**. (JP 3-02)

air support operations center — The principal air control agency of the theater air control system responsible for the direction and control of air operations directly supporting the ground combat element. Also called **ASOC.** See also **close air support; operation; tactical air control center.** (JP 3-09.3)

air support request — A means to request preplanned and immediate close air support, air interdiction, air reconnaissance, surveillance, escort, helicopter airlift, and other aircraft missions. Also called **AIRSUPREQ.** (JP 3-30)

air supremacy — That degree of air superiority wherein the opposing force is incapable of effective interference within the operational area using air and missile threats. (JP 3-01)

air tasking order — A method used to task and disseminate to components, subordinate units, and command and control agencies projected sorties, capabilities and/or forces to targets and specific missions. Also called **ATO.** (JP 3-30)

air terminal — A facility on an airfield that functions as an air transportation hub and accommodates the loading and unloading of airlift aircraft and the intransit processing of traffic. (JP 3-17)

air traffic control section — In amphibious operations, the section of the Navy tactical air control center designed to provide initial safe passage, radar control, and surveillance for close air support aircraft in the operational area. Also called **ATCS**. (JP 3-02)

alert order — 1. A crisis action planning directive from the Secretary of Defense, issued by the Chairman of the Joint Chiefs of Staff, that provides essential guidance for planning

and directs the initiation of execution planning for the selected course of action authorized by the Secretary of Defense. 2. A planning directive that provides essential planning guidance, directs the initiation of execution planning after the directing authority approves a military course of action, but does not authorize execution. Also called **ALERTORD.** See also **course of action; execution planning.** (JP 5-0)

alliance — The relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members. See also **coalition; multinational.** (JP 3-0)

allocation —Distribution of limited forces and resources for employment among competing requirements. See also **apportionment.** (JP 5-0)

allocation request — A daily message that provides an estimate of the total air effort, to identify any excess and joint force general support aircraft sorties, and to identify unfilled air requirements for preplanned missions. Also called **ALLOREQ.** (JP 3-30)

allowable cabin load — The maximum payload that can be carried on an individual sortie. Also called **ACL.** (JP 3-17)

all-source intelligence — 1. Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. See also **intelligence.** (JP 2-0)

ammunition lot — A quantity of homogeneous ammunition, identified by a unique lot number, which is manufactured, assembled, or renovated by one producer under uniform conditions and which is expected to function in a uniform manner. (JP 3-04)

amphibian — A small craft, propelled by propellers and wheels or by air cushions for the purpose of moving on both land and water. (JP 4-01.6)

amphibious advance force — A temporary support force assigned to the amphibious force that conducts shaping operations in the amphibious objective area or operational area prior to the arrival of the amphibious force. (JP 3-02)

amphibious air traffic control center — The centralized air traffic control agency on an amphibious warfare ship responsible for operational control of aircraft departing from and recovering on the ship and tactical control of airborne helicopters in support of amphibious assaults. Also called **AATCC.** (JP 3-02)

amphibious assault — A type of amphibious operation that involves establishing a force on a hostile or potentially hostile shore. See also **assault; assault phase.** (JP 3-02)

amphibious assault vehicle launching area — An area, in the vicinity of and to seaward of the line of departure, to which landing ships proceed and launch amphibious assault vehicles. (JP 3-02)

amphibious breaching — The conduct of a deliberate breaching operation specifically designed to overcome antilanding defenses in order to conduct an amphibious assault. (JP 3-02)

amphibious bulk liquid transfer system — Hosereel system providing capability to deliver fuel and/or water from ship to shore. Also called **ABLTS.** (JP 4-01.6)

amphibious construction battalion — A permanently commissioned naval unit, subordinate to the commander, naval beach group, designed to provide an administrative unit from which personnel and equipment are formed in tactical elements and made available to appropriate commanders to operate causeways, transfer barges, warping tugs, and assault bulk fuel systems, and to meet salvage requirements of the naval beach party. Also called **PHIBCB.** (JP 3-02)

amphibious defense zone — The area encompassing the amphibious objective area and the adjoining airspace required by accompanying naval forces for the purpose of air defense. Also called an **ADZ**. (JP 3-02)

amphibious demonstration — A type of amphibious operation conducted for the purpose of deceiving the enemy by a show of force with the expectation of deluding the enemy into following an unfavorable course of action. (JP 3-02)

amphibious force — An amphibious task force and a landing force together with other forces that are trained, organized, and equipped for amphibious operations. Also called **AF.** See also **amphibious operation; amphibious task force; landing force.** (JP 3-02)

amphibious objective area — A geographical area of sufficient size for conducting necessary sea, air, and land operations, and within which is located the objective(s) to be secured by the amphibious force. Also called **AOA.** See also **amphibious force; mission.** (JP 3-02)

amphibious operation — A military operation launched from the sea by an amphibious force to conduct landing force operations within the littorals. Also called **PHIBOP**. See also **amphibious force; landing force; mission; operation.** (JP 3-02)

amphibious raid — A type of amphibious operation involving swift incursion into or temporary occupation of an objective followed by a planned withdrawal. See also **amphibious operation.** (JP 3-02)

amphibious squadron — A tactical and administrative organization composed of amphibious warfare ships used to transport troops and their equipment for an amphibious operation. Also called **PHIBRON.** (JP 3-02)

amphibious task force — A Navy task organization formed to conduct amphibious operations. Also called **ATF.** See also **amphibious force; amphibious operation; landing force.** (JP 3-02)

amphibious vehicle — A wheeled or tracked vehicle capable of operating on both land and water. See also **landing craft.** (JP 3-02)

amphibious vehicle availability table — A tabulation of the type and number of amphibious vehicles available primarily for assault landings and for support of other elements of the operation. (JP 3-02)

amphibious vehicle employment plan — A plan showing in tabular form the planned employment of amphibious vehicles in landing operations, including their employment after the initial movement to the beach. (JP 3-02)

amphibious warfare ship — A combatant ship having organic capability to embark, land, and support landing forces in amphibious operations and which has characteristics enabling long duration operations on the high seas. (JP 3-02)

amphibious withdrawal — A type of amphibious operation involving the extraction of forces by sea in ships or craft from a hostile or potentially hostile shore. See also **amphibious operation.** (JP 3-02)

analysis and production — In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. See also **intelligence process.** (JP 2-01)

antemortem data — Medical records, samples, and photographs taken prior to death. These include (but are not limited to) fingerprints, dental x-rays, body tissue samples, photographs of tattoos, or other identifying marks. These "pre-death" records would be compared against records completed after death to help establish a positive identification of human remains. See also **mortuary affairs.** (JP 4-06)

Antideficiency Act violations — The incurring of obligations or the making of expenditure (outlays) in violation of appropriation law as to purpose, time, and amounts as specified in the defense appropriation or appropriations of funds. (JP 1-06)

antiradiation missile — A missile which homes passively on a radiation source. Also called **ARM.** See also **guided missile.** (JP 3-01)

antisubmarine warfare — Operations conducted with the intention of denying the enemy the effective use of submarines. Also called **ASW.** (JP 3-32)

antiterrorism — Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. Also called **AT.** See also **counterterrorism; terrorism.** (JP 3-07.2)

anti-vehicle land mine — A mine designed to immobilize or destroy a vehicle. Also called **AVL**. (JP 3-15)

application — 1. The system or problem to which a computer is applied. 2. In the intelligence context, the direct extraction and tailoring of information from an existing foundation of intelligence and near real time reporting. (JP 2-0)

apportionment — In the general sense, distribution of forces and capabilities as the starting point for planning, etc. See also **allocation.** (JP 5-0)

approach schedule — In amphibious operations, this schedule indicates, for each scheduled wave, the time of departure from the rendezvous area, from the line of departure, and from other control points and the time of arrival at the beach. (JP 3-02)

apron — A defined area on an airfield intended to accommodate aircraft for purposes of loading or unloading passengers or cargo, refueling, parking, or maintenance. (JP 3-34)

area air defense commander — The component commander with the preponderance of air defense capability and the required command, control, and communications capabilities who is assigned by the joint force commander to plan and execute integrated air defense operations. Also called **AADC.** (JP 3-01)

area command — A command that is composed of elements of one or more of the Services, organized and placed under a single commander and designated to operate in a specific geographical area. See also **command.** (JP 3-10)

area damage control — Measures taken before, during, or after hostile action or natural or manmade disasters, to reduce the probability of damage and minimize its effects. Also called **ADC.** (JP 3-10)

area of influence — A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. (JP 3-0)

area of interest — That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called **AOI.** See also **area of influence.** (JP 3-0)

area of operations — An operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect

their forces. Also called **AO.** See also **area of responsibility; joint operations area; joint special operations area.** (JP 3-0)

area of responsibility — The geographical area associated with a combatant command within which a geographic combatant commander has authority to plan and conduct operations. Also called **AOR.** See also **combatant command.** (JP 1)

area search — Visual reconnaissance of limited or defined areas. (JP 3-50)

Armed Forces of the United States — A term used to denote collectively all components of the Army, Marine Corps, Navy, Air Force, and Coast Guard (when mobilized under Title 10, United States Code, to augment the Navy). See also **United States Armed Forces.** (JP 1)

arming — As applied to explosives, weapons, and ammunition, the changing from a safe condition to a state of readiness for initiation. (JP 3-15)

arms control agreement — The written or unwritten embodiment of the acceptance of one or more arms control measures by two or more nations. (JP 2-01)

Army air-ground system — The Army system which provides for interface between Army and tactical air support agencies of other Services in the planning, evaluating, processing, and coordinating of air support requirements and operations. Also called **AAGS.** (JP 3-09.3)

Army corps — An intermediate headquarters between divisions and the theater army consisting of two or more divisions together with supporting brigades. (JP 3-31)

Army Service component command — Command responsible for recommendations to the joint force commander on the allocation and employment of Army forces within a combatant command. Also called **ASCC.** (JP 3-31)

Army special operations forces — Those Active and Reserve Component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. Also called **ARSOF.** (JP 3-05)

Army support area — The specific support area for a theater Army that is outside of a division or corps's operational area established primarily for the positioning, employment, and protection of theater support units; and where the majority of the sustaining operations occur. (JP 3-31)

arrival zone — In counterdrug operations, the area in or adjacent to the United States where smuggling concludes and domestic distribution begins (by air, an airstrip; by sea, an offload point on land, or transfer to small boats). See also **transit zone.** (JP 3-07.4)

ascent phase — That portion of the flight of a ballistic missile or space vehicle that begins after powered flight and ends just prior to apogee. (JP 3-01)

assault — 1. In an amphibious operation, the period of time between the arrival of the major assault forces of the amphibious task force in the objective area and the accomplishment of the amphibious task force mission. (JP 3-02) 2. To make a short, violent, but well-ordered attack against a local objective, such as a gun emplacement, a fort, or a machine gun nest. (JP 3-18) 3. A phase of an airborne operation beginning with delivery by air of the assault echelon of the force into the objective area and extending through attack of assault objectives and consolidation of the initial airhead. See also **assault phase.** (JP 3-18)

assault breaching — A part of amphibious breaching in support of an amphibious assault involving a fire support mission using precision guided munitions to neutralize mines and obstacles in the surf zone and on the beach. (JP 3-02)

assault craft unit — A permanently commissioned naval organization, subordinate to the commander, naval beach group, that contains landing craft and crews necessary to provide lighterage required in an amphibious operation. Also called **ACU.** (JP 3-02)

assault echelon — In amphibious operations, the element of a force comprised of tailored units and aircraft assigned to conduct the initial assault on the operational area. Also called **AE.** See also **amphibious operation.** (JP 3-02)

assault follow-on echelon — In amphibious operations, that echelon of the assault troops, vehicles, aircraft, equipment, and supplies that, though not needed to initiate the assault, is required to support and sustain the assault. Also called **AFOE.** (JP 3-02)

assault phase — In an airborne operation, a phase beginning with delivery by air of the assault echelon of the force into the objective area and extending through attack of assault objectives and consolidation of the initial airhead. See also **assault.** (JP 3-18)

assault schedule — In amphibious operations, this schedule provides the formation, composition, and timing of waves landing over the beach. (JP 3-02)

assessment — 1. A continuous process that measures the overall effectiveness of employing joint force capabilities during military operations. 2. Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. 3. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. 4. Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 3-0)

assessment agent — The organization responsible for conducting an assessment of an approved joint publication. Also called **AA.** (CJCSM 5120.01)

asset validation — In intelligence use, the process used to determine the asset authenticity, reliability, utility, suitability, and degree of control the case officer or others have. (JP 2-01.2)

asset visibility — Provides users with information on the location, movement, status, and identity of units, personnel, equipment, and supplies, which facilitates the capability to act upon that information to improve overall performance of the Department of Defense's logistics practices. Also called **AV.** (JP 3-35)

assign — 1. To place units or personnel in an organization where such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel. 2. To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. See also **attach.** (JP 3-0)

assumption — A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action. (JP 5-0)

asymmetric — In military operations the application of dissimilar strategies, tactics, capabilities, and methods to circumvent or negate an opponent's strengths while exploiting his weaknesses. (JP 3-15.1)

atmospheric environment — The envelope of air surrounding the Earth, including its interfaces and interactions with the Earth's solid or liquid surface. (JP 3-59)

attach — 1. The placement of units or personnel in an organization where such placement is relatively temporary. 2. The detailing of individuals to specific functions where such functions are secondary or relatively temporary. See also **assign.** (JP 3-0)

attack assessment — An evaluation of information to determine the potential or actual nature and objectives of an attack for the purpose of providing information for timely decisions. See also **damage estimation.** (JP 3-14)

attack group — A subordinate task organization of the Navy forces of an amphibious task force composed of amphibious warfare ships and supporting naval units designated to transport, protect, land, and initially support a landing group. (JP 3-02)

attack heading — 1. The interceptor heading during the attack phase that will achieve the desired track-crossing angle. 2. The assigned magnetic compass heading to be flown by aircraft during the delivery phase of an air strike. (JP 3-09.3)

attack position — The last position occupied by the assault echelon before crossing the line of departure. (JP 3-09.3)

attack the network operations — Lethal and nonlethal actions and operations against networks conducted continuously and simultaneously at multiple levels (tactical, operational, and strategic) that capitalize on or create key vulnerabilities and disrupt activities to eliminate the enemy's ability to function in order to enable success of the operation or campaign. Also called **AtN operations.** (JP 3-15.1)

audience — In public affairs, a broadly-defined group that contains stakeholders and/or publics relevant to military operations. (JP 3-61)

augmentation forces — Forces to be transferred from a supporting combatant commander to the combatant command (command authority) or operational control of a supported combatant commander during the execution of an operation order approved by the President and Secretary of Defense. (JP 5-0)

authentication — 1. A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator. 2. A means of identifying individuals and verifying their eligibility to receive specific categories of information. 3. Evidence by proper signature or seal that a document is genuine and official. 4. In personnel recovery missions, the process whereby the identity of an isolated person is confirmed. See also **evader; evasion; recovery operations; security.** (JP 3-50)

authorization data — Department of Defense military and civilian manpower and equipment resources authorized by law. (DODI 8260.03)

authorization inventory — The set of manpower and equipment authorizations associated with one or more organization. (DODI 8260.03)

authorized departure — A procedure, short of ordered departure, by which mission employees or dependents or both, are permitted to leave post in advance of normal rotation when the national interests or imminent threat to life require it. (JP 3-68)

Automated Repatriation Reporting System — A Defense Manpower Data Center system used to track the status of noncombatant evacuees after they have arrived in an initial safe haven in the United States. (JP 3-68)

automatic identification technology — A suite of technologies enabling the automatic capture of data, thereby enhancing the ability to identify, track, document, and control assets (e.g., materiel), deploying and redeploying forces, equipment, personnel, and sustainment cargo. Also called **AIT.** (JP 4-09)

autonomous operation — In air defense, the mode of operation assumed by a unit after it has lost all communications with higher echelons forcing the unit commander to assume full responsibility for control of weapons and engagement of hostile targets. (JP 3-01)

available-to-load date — A date specified for each unit in a time-phased force and deployment data indicating when that unit will be ready to load at the point of embarkation. Also called **ALD.** (JP 5-0)

avenue of approach — An air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. Also called **AA**. (JP 2-01.3)

aviation medicine — The special field of medicine which is related to the biological and psychological problems of flight. (JP 4-02)

axis of advance — A line of advance assigned for purposes of control; often a road or a group of roads, or a designated series of locations, extending in the direction of the enemy. (JP 3-03)

Intentionally Blank

B

backfill — Reserve Component units and individuals recalled to replace deploying active units and/or individuals in the continental United States and outside the continental United States. See also **Reserve Component.** (JP 4-05)

bale cubic capacity — The space available for cargo measured in cubic feet to the inside of the cargo battens, on the frames, and to the underside of the beams. (JP 4-01.2)

ballistic missile — Any missile which does not rely upon aerodynamic surfaces to produce lift and consequently follows a ballistic trajectory when thrust is terminated. See also **guided missile.** (JP 3-01)

barrier — A coordinated series of natural or man-made obstacles designed or employed to channel, direct, restrict, delay, or stop the movement of an opposing force and to impose additional losses in personnel, time, and equipment on the opposing force. (JP 3-15)

barrier combat air patrol — One or more divisions or elements of fighter aircraft employed between a force and an objective area as a barrier across the probable direction of enemy attack. See also **combat air patrol.** (JP 3-01)

barrier, obstacle, and mine warfare plan — A comprehensive, coordinated plan that includes responsibilities; general location of unspecified and specific barriers, obstacles, and minefields; special instructions; limitations; coordination; and completion times; and may designate locations of obstacle zones or belts. (JP 3-15)

base — 1. A locality from which operations are projected or supported. 2. An area or locality containing installations which provide logistic or other support. 3. Home airfield or home carrier. See also **facility.** (JP 4-0)

base boundary — A line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas. (JP 3-10)

base cluster — In base defense operations, a collection of bases, geographically grouped for mutual protection and ease of command and control. (JP 3-10)

base cluster commander — In base defense operations, a senior base commander designated by the joint force commander responsible for coordinating the defense of bases within the base cluster and for integrating defense plans of bases into a base cluster defense plan. (JP 3-10)

base cluster operations center — A command and control facility that serves as the base cluster commander's focal point for defense and security of the base cluster. Also called **BCOC.** (JP 3-10)

base defense — The local military measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks on, or sabotage of, a base, to ensure that the maximum capacity of its facilities is available to United States forces. (JP 3-10)

base defense operations center — A command and control facility established by the base commander to serve as the focal point for base security and defense. Also called **BDOC.** (JP 3-10)

base defense zone — An air defense zone established around an air base and limited to the engagement envelope of short-range air defense weapons systems defending that base. Also called **BDZ**. (JP 3-52)

base development — The acquisition, development, expansion, improvement, construction and/or replacement of the facilities and resources of a location to support forces. (JP 3-34)

baseline costs — The continuing annual costs of military operations funded by the operations and maintenance and military personnel appropriations. (JP 1-06)

base operating support — Directly assisting, maintaining, supplying, and distributing support of forces at the operating location. Also called **BOS**. (JP 4-0)

base operating support-integrator — The designated Service component or joint task force commander assigned to synchronize all sustainment functions for a contingency base. Also called **BOS-I**. (JP 4-0)

base plan — A type of operation plan that describes the concept of operations, major forces, sustainment concept, and anticipated timelines for completing the mission without annexes or time-phased force and deployment data. Also called **BPLAN.** (JP 5-0)

base support installation — A Department of Defense Service or agency installation within the United States and its territories tasked to serve as a base for military forces engaged in either homeland defense or defense support of civil authorities. Also called **BSI.** (JP 3-28)

basic encyclopedia — A compilation of identified installations and physical areas of potential significance as objectives for attack. Also called **BE.** (JP 2-01)

basic load — The quantity of supplies required to be on hand within, and which can be moved by, a unit or formation, expressed according to the wartime organization of the unit or formation and maintained at the prescribed levels. (JP 4-09)

battalion landing team — In an amphibious operation, an infantry battalion normally reinforced by necessary combat and service elements; the basic unit for planning an assault landing. Also called **BLT.** (JP 3-02)

battle damage assessment — The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force. Also called **BDA.** See also **combat assessment.** (JP 3-0)

battle damage repair — Essential repair, which may be improvised, carried out rapidly in a battle environment in order to return damaged or disabled equipment to temporary service. Also called **BDR.** (JP 4-09)

battlefield coordination detachment — An Army liaison located in the air operations center that provides selected operational functions between the Army forces and the air component commander. Also called **BCD.** See also **air operations center; liaison.** (JP 3-03)

battle injury — Damage or harm sustained by personnel during or as a result of battle conditions. Also called **BI.** (JP 4-02)

battle management — The management of activities within the operational environment based on the commands, direction, and guidance given by appropriate authority. Also called **BM.** (JP 3-01)

beach — 1. The area extending from the shoreline inland to a marked change in physiographic form or material, or to the line of permanent vegetation (coastline). 2. In amphibious operations, that portion of the shoreline designated for landing of a tactical organization. (JP 3-02)

beachhead — A designated area on a hostile or potentially hostile shore that, when seized and held, ensures the continuous landing of troops and materiel, and provides maneuver space requisite for subsequent projected operations ashore. (JP 3-02)

beachmaster unit — A commissioned naval unit of the naval beach group designed to provide to the shore party a Navy component known as a beach party, which is capable of supporting the amphibious landing of one division (reinforced). Also called **BMU.** See also **beach party; naval beach group; shore party.** (JP 4-01.6)

beach party — The Navy component of the landing force support party under the tactical control of the landing force support party commander. See also **beachmaster unit; shore party.** (JP 3-02)

beach support area — In amphibious operations, the area to the rear of a landing force or elements thereof, that contains the facilities for the unloading of troops and materiel and the support of the forces ashore. Also called **BSA.** (JP 3-02)

begin morning civil twilight — The period of time at which the sun is halfway between beginning morning and nautical twilight and sunrise, when there is enough light to see objects clearly with the unaided eye. Also called **BMCT.** (JP 2-01.3)

begin morning nautical twilight — The start of that period where, in good conditions and in the absence of other illumination, the sun is 12 degrees below the eastern horizon and enough light is available to identify the general outlines of ground objects and conduct limited military operations. Also called **BMNT**. (JP 3-09.3)

believed-to-be — In mortuary affairs, the status of any human remains until a positive identification has been determined. Used interchangeably with tentative identification. Also called **BTB.** (JP 4-06)

berm — The nearly horizontal portion of a beach or backshore having an abrupt fall and either formed by deposition of material by wave action at the limit of ordinary high tide or constructed to protect materials handling equipment during air cushion vehicle operations. (JP 4-01.6)

bill — A ship's publication listing operational or administrative procedures. (JP 3-04)

biological agent — A microorganism (or a toxin derived from it) that causes disease in personnel, plants, or animals or causes the deterioration of materiel. See also **chemical agent.** (JP 3-11)

biological hazard — An organism, or substance derived from an organism, that poses a threat to human or animal health. (JP 3-11)

biometrics — The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 2-0)

biometrics-enabled intelligence — The intelligence derived from the processing of biologic identity data and other all-source for information concerning persons of interest. Also called **BEI.** (JP 2-0)

blister agent — A chemical agent that injures the eyes and lungs, and burns or blisters the skin. Also called **vesicant agent.** (JP 3-11)

blood agent — A chemical compound, including the cyanide group, that affects bodily functions by preventing the normal utilization of oxygen by body tissues. (JP 3-11)

blood chit — A small sheet of material depicting an American flag and a statement in several languages to the effect that anyone assisting the bearer to safety will be rewarded. See also **evasion aid.** (JP 3-50)

Blue Bark — US military personnel, US citizen civilian employees of the Department of Defense, and the dependents of both categories who travel in connection with the death of an immediate family member. It also applies to designated escorts for dependents of deceased military members. Furthermore, the term is used to designate the personal property shipment of a deceased member. (JP 4-06)

boat group — The basic organization of landing craft. (JP 3-02)

boat lane — A lane for amphibious assault landing craft, which extends from the line of departure to the beach. (JP 3-02)

boat space — The space and weight factor used in planning for one person with individual equipment to determine overall ship-to-shore movement requirements for boats, landing craft, and amphibious vehicles. (JP 3-02.1)

bona fides — 1. In personnel recovery, the use of verbal or visual communication by individuals who are unknown to one another, to establish their authenticity, sincerity, honesty, and truthfulness. See also **evasion; recovery; recovery operations.** (JP 3-50) 2. The lack of fraud or deceit: a determination that a person is who he/she says he/she is. (JP 2-01.2)

boost phase — That portion of the flight of a ballistic missile or space vehicle during which the booster and sustainer engines operate. See also midcourse phase; terminal phase. (JP 3-01)

bottom mine — A mine with negative buoyancy which remains on the seabed. See also **mine.** (JP 3-15)

boundary — A line that delineates surface areas for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas. (JP 3-0)

branch — 1. A subdivision of any organization. 2. A geographically separate unit of an activity, which performs all or part of the primary functions of the parent activity on a smaller scale. 3. An arm or service of the Army. 4. The contingency options built into the base plan used for changing the mission, orientation, or direction of movement of a force to aid success of the operation based on anticipated events, opportunities, or disruptions caused by enemy actions and reactions. See also **sequel.** (JP 5-0)

breakbulk ship — A ship with conventional holds for stowage of breakbulk cargo and a limited number of containers, below or above deck, and equipped with cargo-handling gear. (JP 4-09)

brevity code — A code word, which provides no security, that serves the sole purpose of shortening of messages rather than the concealment of their content. (JP 3-09.3)

brigade combat team — A combined arms team that forms the basic building block of the Army's tactical formations. Also called **BCT.** (JP 3-31)

broken stowage — The space lost in the holds of a vessel because of the contour of the ship, dunnage, ladders, stanchions, and the shape of the cargo. (JP 3-02.1)

broken stowage factor — A factor applied to the available space for embarkation due to the loss between boxes, between vehicles, around stanchions, and over cargo, that will vary, depending on the type and size of vehicles, type and size of general cargo, training and experience of loading personnel, type of loading, method of stowage, and configuration of compartments. (JP 3-02.1)

buddy-aid — Acute medical care (first aid) provided by a non-medical Service member to another person. (JP 4-02)

buffer zone — 1. A defined area controlled by a peace operations force from which disputing or belligerent forces have been excluded. Also called **area of separation** in some United Nations operations. Also called **BZ.** See also **line of demarcation; peace operations.** (JP 3-07.3) 2. A designated area used for safety in military operations. (JP 3-01)

building system — A structure assembled from manufactured components designed to provide a specific building configuration. (JP 3-34)

bulk cargo — That which is generally shipped in volume where the transportation conveyance is the only external container; such as liquids, ore, or grain. (JP 4-01.5)

bulk petroleum product — A liquid petroleum product transported by various means and stored in tanks or containers having an individual fill capacity greater than 208 liters. (JP 4-03)

bulk storage — 1. Storage in a warehouse of supplies and equipment in large quantities, usually in original containers, as distinguished from bin storage. 2. Storage of liquids, such as petroleum products in tanks, as distinguished from drum or packaged storage. (JP 4-03)

C

cache — A source of subsistence and supplies, typically containing items such as food, water, medical items, and/or communications equipment, packaged to prevent damage from exposure and hidden in isolated locations by such methods as burial, concealment, and/or submersion, to support isolated personnel. See also **evader; evasion; recovery; recovery operations.** (JP 3-50)

call sign — Any combination of characters or pronounceable words, which identifies a communication facility, a command, an authority, an activity, or a unit; used primarily for establishing and maintaining communications. Also called **CS.** (JP 3-50)

campaign — A series of related major operations aimed at achieving strategic and operational objectives within a given time and space. See also **campaign plan.** (JP 5-0)

campaign plan — A joint operation plan for a series of related major operations aimed at achieving strategic or operational objectives within a given time and space. See also **campaign; campaign planning.** (JP 5-0)

campaign planning — The process whereby combatant commanders and subordinate joint force commanders translate national or theater strategy into operational concepts through the development of an operation plan for a campaign. See also **campaign; campaign plan.** (JP 5-0)

canalize — To restrict operations to a narrow zone by use of existing or reinforcing obstacles or by fire or bombing. (JP 3-15)

candidate target list — A list of objects or entities submitted by component commanders, appropriate agencies, or the joint force commander's staff for further development and inclusion on the joint target list and/or restricted target list, or moved to the no-strike list. Also called **CTL**. See also joint integrated prioritized target list; target, target nomination list. (JP 3-60)

capstone publication — The top joint doctrine publication in the hierarchy of joint publications that links joint doctrine to national strategy and the contributions of other government departments and agencies, multinational partners, and reinforces policy for command and control. See also **joint publication; keystone publications.** (CJCSM 5120.01)

cargo increment number — A seven-character alphanumeric field that uniquely describes a non-unit-cargo entry (line) in the Joint Operation Planning and Execution System time-phased force and deployment data. (JP 3-35)

carrier air wing — Two or more aircraft squadrons formed under one commander for administrative and tactical control of operations from a carrier. Also called **CVW**. (JP 3-32)

carrier control zone — The airspace within a circular limit defined by 5 miles horizontal radius from the carrier, extending upward from the surface to and including 2,500 feet unless otherwise designated for special operations, and is under the cognizance of the air officer during visual meteorological conditions. (JP 3-52)

carrier strike group — A standing naval task group consisting of a carrier, embarked air wing, surface combatants, and submarines as assigned in direct support, operating in mutual support with the task of destroying hostile submarine, surface, and air forces within the group's assigned operational area and striking at targets along hostile shore lines or projecting power inland. Also called **CSG.** (JP 3-32)

cartridge-actuated device — Small explosive devices used to eject stores from launched devices, actuate other explosive systems, or provide initiation for aircrew escape devices. Also called **CAD.** (JP 3-04)

case officer — A professional employee of an intelligence or counterintelligence organization, who is responsible for providing directions for an agent operation and/or handling intelligence assets. (JP 2-01.2)

casualty — Any person who is lost to the organization by having been declared dead, duty status – whereabouts unknown, missing, ill, or injured. See also **hostile casualty.** (JP 4-02)

casualty evacuation — The unregulated movement of casualties that can include movement both to and between medical treatment facilities. Also called **CASEVAC.** See also **casualty; evacuation; medical treatment facility.** (JP 4-02)

casualty rate — The number of casualties per 1,000 population at risk. (DODI 8620.04)

casualty receiving and treatment ship — In amphibious operations, a ship designated to receive, provide treatment for, and transfer casualties. Also called **CRTS**. (JP 3-02)

catastrophic event — Any natural or man-made incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. (JP 3-28)

causeway — A craft similar in design to a barge, but longer and narrower, designed to assist in the discharge and transport of cargo from vessels. (JP 4-01.6)

causeway launching area — An area located near the line of departure but clear of the approach lanes to an area located in the inner transport area. (JP 3-02)

C-day — The unnamed day on which a deployment operation commences or is to commence. (JP 5-0)

cell — A subordinate organization formed around a specific process, capability, or activity within a designated larger organization of a joint force commander's headquarters. (JP 3-33)

center — An enduring functional organization, with a supporting staff, designed to perform a joint function within a joint force commander's headquarters. (JP 3-33)

center of gravity — The source of power that provides moral or physical strength, freedom of action, or will to act. Also called **COG.** See also **decisive point.** (JP 5-0)

centigray — A unit of absorbed dose of radiation (one centigray equals one rad). (JP 3-11)

central control officer — The officer, embarked in the central control ship, designated by the amphibious task force commander for the overall coordination of the waterborne ship-to-shore movement. Also called **CCO.** (JP 3-02)

centralized control — 1. In air defense, the control mode whereby a higher echelon makes direct target assignments to fire units. (JP 3-01) 2. In joint air operations, placing within one commander the responsibility and authority for planning, directing, and coordinating a military operation or group/category of operations. See also **decentralized control.** (JP 3-30)

chaff — Radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion purposes. (JP 3-13.1)

chain of command — The succession of commanding officers from a superior to a subordinate through which command is exercised. Also called **command channel**. (JP 1)

Chairman of the Joint Chiefs of Staff instruction — A document for all types of correspondence containing Chairman of the Joint Chiefs of Staff policy and guidance that does not involve the employment of forces, which is of indefinite duration and is applicable to external agencies, or both the Joint Staff and external agencies. Also called **CJCSI.** See also **Chairman of the Joint Chiefs of Staff manual.** (CJCSM 5120.01)

Chairman of the Joint Chiefs of Staff manual — A document containing detailed procedures for performing specific tasks that do not involve the employment of forces, which is of indefinite duration and is applicable to external agencies or both the Joint Staff and external agencies. Also called **CJCSM.** See also **Chairman of the Joint Chiefs of Staff instruction.** (CJCSM 5120.01)

chalk number — The number given to a complete load and to the transporting carrier. (JP 3-17)

change detection — An image enhancement technique that compares two images of the same area from different time periods and eliminates identical picture elements in order to leave the signatures that have undergone change. (JP 2-03)

channel airlift — Airlift provided for movement of sustainment cargo, scheduled either regularly or depending upon volume of workload, between designated ports of embarkation and ports of debarkation over validated contingency or distribution routes. (JP 3-17)

chemical agent — A chemical substance that is intended for use in military operations to kill, seriously injure, or incapacitate mainly through its physiological effects. See also **chemical warfare; riot control agent.** (JP 3-11)

chemical, biological, radiological, and nuclear consequence management — Actions taken to plan, prepare, respond to, and recover from chemical, biological, radiological, and nuclear incidents. Also called **CBRN CM**. (JP 3-41)

chemical, biological, radiological, and nuclear defense — Measures taken to minimize or negate the vulnerabilities to, and/or effects of, a chemical, biological, radiological, or nuclear hazard or incident. Also called **CBRN defense.** (JP 3-11)

chemical, biological, radiological, and nuclear environment — An operational environment that includes chemical, biological, radiological, and nuclear threats and hazards and their potential resulting effects. Also called **CBRN environment.** (JP 3-11)

chemical, biological, radiological, and nuclear hazard — Chemical, biological, radiological, and nuclear elements that could create adverse effects due to an accidental or deliberate release and dissemination. Also called **CBRN hazard.** (JP 3-11)

chemical, biological, radiological, or nuclear incident — Any occurrence, resulting from the use of chemical, biological, radiological and nuclear weapons and devices; the emergence of secondary hazards arising from counterforce targeting; or the release of toxic industrial materials into the environment, involving the emergence of chemical, biological, radiological and nuclear hazards. (JP 3-11)

chemical, biological, radiological, or nuclear weapon — A fully engineered assembly designed for employment to cause the release of a chemical or biological agent or radiological material onto a chosen target or to generate a nuclear detonation. Also called **CBRN weapon.** (JP 3-11)

chemical hazard — Any chemical manufactured, used, transported, or stored that can cause death or other harm through toxic properties of those materials, including chemical agents and chemical weapons prohibited under the Chemical Weapons Convention as well as toxic industrial chemicals. (JP 3-11)

chemical warfare — All aspects of military operations involving the employment of lethal and incapacitating munitions/agents and the warning and protective measures associated with such offensive operations. Also called **CW.** See also **chemical agent; chemical weapon; riot control agent.** (JP 3-11)

chemical weapon — Together or separately, (a) a toxic chemical and its precursors, except when intended for a purpose not prohibited under the Chemical Weapons Convention; (b) a munition or device, specifically designed to cause death or other harm through toxic properties of those chemicals specified in (a), above, which would be released as a result of the employment of such munition or device; (c) any equipment specifically designed for use directly in connection with the employment of munitions or devices specified in (b), above. See also **chemical agent; chemical warfare; riot control agent.** (JP 3-11)

chief of fires — The senior organic fires Army staff officer at division and higher headquarters level who advises the commander on the best use of available fire support resources, provides input to necessary orders, and develops and implements the fire support plan. Also called **COF.** (JP 3-09)

chief of mission — The principal officer (the ambassador) in charge of a diplomatic facility of the United States, including any individual assigned to be temporarily in charge of such a facility. The chief of mission is the personal representative of the President to the country of accreditation. The chief of mission is responsible for the direction, coordination, and supervision of all US Government executive branch employees in that country (except those under the command of a US area military commander). The security of the diplomatic post is the chief of mission's direct responsibility. Also called **COM.** (JP 3-08)

chief of staff — The senior or principal member or head of a staff who acts as the controlling member of a staff for purposes of the coordination of its work or to exercise command in another's name. Also called **COS.** (JP 3-33)

chief of station — The senior United States intelligence officer in a foreign country and the direct representative of the Director National Intelligence, to whom the officer reports through the Director Central Intelligence Agency. Usually the senior representative of the Central Intelligence Agency assigned to a US mission. Also called **COS**. (JP 2-01.2)

civil administration — An administration established by a foreign government in (1) friendly territory, under an agreement with the government of the area concerned, to exercise certain authority normally the function of the local government; or (2) hostile territory, occupied by United States forces, where a foreign government exercises executive, legislative, and judicial authority until an indigenous civil government can be established. Also called **CA.** (JP 3-05)

civil affairs — Designated Active and Reserve Component forces and units organized, trained, and equipped specifically to conduct civil affairs operations and to support civil-military operations. Also called **CA.** See also **civil-military operations.** (JP 3-57)

civil affairs operations — Actions planned, executed, and assessed by civil affairs forces that enhance awareness of and manage the interaction with the civil component of the operational environment; identify and mitigate underlying causes of instability within civil society; or involve the application of functional specialty skills normally the responsibility of civil government. Also called **CAO.** (JP 3-57)

civil augmentation program — Standing, long-term external support contacts designed to augment Service logistic capabilities with contracted support in both preplanned and short notice contingencies. Also called **CAP.** See also **contingency; contingency contract; external support contract.** (JP 4-10)

civil authorities — Those elected and appointed officers and employees who constitute the government of the United States, the governments of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, United States territories, and political subdivisions thereof. (JP 3-28)

civil authority information support — The use of military information support operations capabilities to conduct public information dissemination activities to support national security or disaster relief operations within the United States and its territories in support of a lead federal agency. Also called **CAIS.** (JP 3-13.2)

civil emergency — Any occasion or instance for which, in the determination of the President, federal assistance is needed to supplement state and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States. (JP 3-28)

civilian internee — A civilian who is interned during armed conflict, occupation, or other military operation for security reasons, for protection, or because he or she committed an offense against the detaining power. Also called **CI.** (DODD 2310.01E)

civil information — Relevant data relating to the civil areas, structures, capabilities, organizations, people, and events of the civil component of the operational environment used to support the situational awareness of the supported commander. (JP 3-57)

civil information management — Process whereby data relating to the civil component of the operational environment is gathered, collated, processed, analyzed, produced into information products, and disseminated. Also called **CIM.** (JP 3-57)

civil-military medicine — A discipline within operational medicine comprising public health and medical issues that involve a civil-military interface (foreign or domestic), including military medical support to civil authorities (domestic), medical elements of cooperation activities, and medical civil-military operations. (JP 4-02)

civil-military operations — Activities of a commander performed by designated civil affairs or other military forces that establish, maintain, influence, or exploit relations between

military forces, indigenous populations, and institutions, by directly supporting the attainment of objectives relating to the reestablishment or maintenance of stability within a region or host nation. Also called **CMO.** See also **civil affairs; operation.** (JP 3-57)

civil-military operations center — An organization, normally comprised of civil affairs, established to plan and facilitate coordination of activities of the Armed Forces of the United States within indigenous populations and institutions, the private sector, intergovernmental organizations, nongovernmental organizations, multinational forces, and other governmental agencies in support of the joint force commander. Also called **CMOC.** See also **civil-military operations; operation.** (JP 3-57)

civil-military team — A temporary organization of civilian and military personnel task-organized to provide an optimal mix of capabilities and expertise to accomplish specific operational and planning tasks. (JP 3-57)

civil reconnaissance — A targeted, planned, and coordinated observation and evaluation of specific civil aspects of the environment such as areas, structures, capabilities, organizations, people, or events. Also called **CR.** (JP 3-57)

Civil Reserve Air Fleet — A program in which the Department of Defense contracts for the services of specific aircraft, owned by a United States entity or citizen, during national emergencies and defense-oriented situations when expanded civil augmentation of military airlift activity is required. Also called **CRAF.** See also **reserve.** (JP 3-17)

civil search and rescue — Search and/or rescue operations and associated civilian services provided to assist persons in potential or actual distress and protect property in a nonhostile environment. Also called **civil SAR.** (JP 3-50)

clandestine — Any activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy and concealment. (JP 2-01.2)

clandestine intelligence collection — The acquisition of protected intelligence information in a way designed to conceal the nature of the operation and protect the source. (JP 2-01.2)

clandestine operation — An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. See also **covert operation; overt operation.** (JP 3-05)

classes of supply — The ten categories into which supplies are grouped in order to facilitate supply management and planning. I. Rations and gratuitous issue of health, morale, and welfare items. II. Clothing, individual equipment, tentage, tool sets, and administrative and housekeeping supplies and equipment. III. Petroleum, oils, and lubricants. IV. Construction materials. V. Ammunition. VI. Personal demand items. VII. Major end items, including tanks, helicopters, and radios. VIII. Medical. IX. Repair parts and components for equipment maintenance. X. Nonstandard items to support nonmilitary

programs such as agriculture and economic development. See also **petroleum, oils, and lubricants.** (JP 4-09)

classification — The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. See also **security classification.** (JP 2-01.2)

classified information — Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (JP 2-01.2)

clearance capacity — An estimate expressed in agreed upon units of cargo measurement per day of the cargo or people that may be transported inland from a beach or port over the available means of inland communication, including roads, railroads, airlift, and inland waterways. See also **throughput capacity.** (JP 4-01.5)

clearance decontamination — The final level of decontamination that provides the decontamination of equipment and personnel to a level that allows unrestricted transportation, maintenance, employment, and disposal. (JP 3-11)

clearing operation — An operation designed to clear or neutralize all mines and obstacles from a route or area. (JP 3-15)

climate change — Variations in average weather conditions that persist over multiple decades or longer that encompass increases and decreases in temperature, shifts in precipitation, and changing risk of certain types of severe weather events. (DODD 4715.21)

close air support — Air action by fixed- and rotary-wing aircraft against hostile targets that are in close proximity to friendly forces and that require detailed integration of each air mission with the fire and movement of those forces. Also called **CAS.** See also **air interdiction.** (JP 3-0)

close support — The action of the supporting force against targets or objectives that are sufficiently near the supported force as to require detailed integration or coordination of the supporting action. See also **direct support; general support; mutual support; support.** (JP 3-31)

close support area — Those parts of the ocean operating areas nearest to, but not necessarily in, the objective area. (JP 3-02)

closure — In transportation, the process of a unit's arriving at a specified location. (JP 4-01.5)

coalition — An arrangement between two or more nations for common action. See also **alliance; multinational.** (JP 5-0)

coastal sea control — The employment of forces to ensure the unimpeded use of an offshore coastal area by friendly forces and, as appropriate, to deny the use of the area to enemy forces. (JP 3-10)

code word — 1. A word that has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation. 2. A cryptonym used to identify sensitive intelligence data. (JP 3-50)

collateral damage — Unintentional or incidental injury or damage to persons or objects that would not be lawful military targets in the circumstances ruling at the time. (JP 3-60)

collection — In intelligence usage, the acquisition of information and the provision of this information to processing elements. See also **intelligence process.** (JP 2-01)

collection agency — Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. See also **agency.** (JP 2-01)

collection asset — A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. See also **collection.** (JP 2-01)

collection management — In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. See also **collection; collection requirement; collection requirements management; intelligence; intelligence process.** (JP 2-0)

collection management authority — Within the Department of Defense, collection management authority constitutes the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater-wide collection policies. Also called **CMA.** See also **collection manager; collection plan; collection requirement.** (JP 2-01.2)

collection manager — An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. Also called **CM.** See also **collection; collection management authority.** (JP 2-01)

collection operations management — The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. Also called **COM.** See also **collection management; collection requirements management.** (JP 2-0)

collection plan — A systematic scheme to optimize the employment of all available collection capabilities and associated processing, exploitation, and dissemination resources to satisfy specific information requirements. See also **information requirements; intelligence process.** (JP 2-0)

collection planning — A continuous process that coordinates and integrates the efforts of all collection units and agencies. See also **collection.** (JP 2-0)

collection point — A point designated for the assembly of personnel casualties, stragglers, disabled materiel, salvage, etc., for further movement to collecting stations or rear installations. Also called **CP.** (JP 4-06)

collection posture — The current status of collection assets and resources to satisfy identified information requirements. (JP 2-0)

collection requirement — A valid need to close a specific gap in intelligence holdings in direct response to a request for information. (JP 2-0)

collection requirements management — The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of requirements to units over which the commander has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. Also called **CRM.** See also **collection; collection management; collection operations management.** (JP 2-0)

collection resource — A collection system, platform, or capability that is not assigned or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. See also **collection management.** (JP 2-01)

collection strategy — An analytical approach used by collection managers to determine which intelligence disciplines can be applied to satisfy information requirements. (JP 2-0)

collective protection — The protection provided to a group of individuals that permits relaxation of individual chemical, biological, radiological, and nuclear protection. Also called **COLPRO.** (JP 3-11)

colored beach — That portion of usable coastline sufficient for the assault landing of a regimental landing team or similar sized unit. See also **numbered beach.** (JP 3-02)

combat air patrol — An aircraft patrol provided over an objective area, the force protected, the critical area of a combat zone, or in an air defense area, for the purpose of intercepting and destroying hostile aircraft before they reach their targets. Also called **CAP.** See also **airborne alert; barrier combat air patrol; rescue combat air patrol.** (JP 3-01)

combat and operational stress — The expected and predictable emotional, intellectual, physical, and/or behavioral reactions of an individual who has been exposed to stressful events in war or stability operations. (JP 4-02)

combat and operational stress control — Programs developed and actions taken by military leadership to prevent, identify, and manage adverse combat and operational stress reactions in units; optimize mission performance; conserve fighting strength; prevent or minimize adverse effects of combat and operational stress on members' physical, psychological, intellectual and social health; and to return the unit or Service member to duty expeditiously. (JP 4-02)

combatant command — A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Also called **CCMD**. See also **specified combatant command; unified command.** (JP 1)

combatant command chaplain — The senior chaplain assigned to the staff of, or designated by, the combatant commander to provide advice on religion, ethical, and moral issues, and morale of assigned personnel and to coordinate religious ministries within the combatant commander's area of responsibility. See also **command chaplain; religious support; religious support team.** (JP 1-05)

combatant command (command authority) — Nontransferable command authority, which cannot be delegated, of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Also called **COCOM.** See also **combatant command; combatant commander; operational control; tactical control.** (JP 1)

combatant commander — A commander of one of the unified or specified combatant commands established by the President. Also called **CCDR.** See also **combatant command; specified combatant command; unified combatant command.** (JP 3-0)

combatant commander logistic procurement support board — A combatant commander-level joint board established to ensure that contracting support and other sources of support are properly synchronized across the entire area of responsibility. Also called **CLPSB.** See also **joint requirements review board; joint contracting support board.** (JP 4-10)

combatant command support agent — The Secretary of a Military Department to whom the Secretary of Defense or the Deputy Secretary of Defense has assigned administrative and logistical support of the headquarters of a combatant command, United States Element, North American Aerospace Defense Command, or subordinate unified command. The nature and scope of the combatant command support agent

responsibilities, functions, and authorities shall be prescribed at the time of assignment or in keeping with existing agreements and practices, and they shall remain in effect until the Secretary of Defense or the Deputy Secretary of Defense revokes, supersedes, or modifies them. Also called **CCSA**. (DODD 5100.03)

combat assessment — The determination of the overall effectiveness of force employment during military operations. Combat assessment is composed of three major components: (a) battle damage assessment; (b) munitions effectiveness assessment; and (c) reattack recommendation. Also called **CA.** See also **battle damage assessment; munitions effectiveness assessment; reattack recommendation.** (JP 3-60)

combat camera — Specially-trained expeditionary forces from Service-designated units capable of providing high-quality directed visual information during military operations. Also called **COMCAM.** See also **visual information.** (JP 3-61)

combat cargo officer — A Marine Corps embarkation/mobility officer permanently assigned to amphibious warfare ships or naval staffs, as an adviser to and representative of the naval commander in matters pertaining to embarkation and debarkation of troops, their supplies, and equipment. Also called **CCO.** See also **embarkation officer.** (JP 3-02.1)

combat chart — A special naval chart, at a scale of 1:50,000, designed for naval surface fire support and close air support during coastal or amphibious operations and showing detailed hydrography and topography in the coastal belt. (JP 2-03)

combat control team — A task-organized team of special operations forces who are certified air traffic controllers that are trained and equipped to deploy into hostile environments to establish and control assault zones and airfields. Also called **CCT.** (JP 3-17)

combat engineering — Engineering capabilities and activities that directly support the maneuver of land combat forces that require close and integrated support. (JP 3-34)

combat identification — The process of attaining an accurate characterization of detected objects in the operational environment sufficient to support an engagement decision. Also called **CID.** (JP 3-09)

combat information — Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (JP 2-01)

combat information center — The agency in a ship or aircraft manned and equipped to collect, display, evaluate, and disseminate tactical information for the use of the embarked flag officer, commanding officer, and certain control agencies. Also called **CIC.** (JP 3-04)

combating terrorism — Actions, including antiterrorism and counterterrorism, taken to oppose terrorism throughout the entire threat spectrum. Also called **CbT.** See also **antiterrorism; counterterrorism.** (JP 3-26)

combat loading — The arrangement of personnel and the stowage of equipment and supplies in a manner designed to conform to the anticipated tactical operation of the organization embarked. (JP 3-02)

combat organizational loading — A method of loading by which a unit with its equipment and initial supplies is loaded into a single ship, together with other units, in such a manner as to be available for unloading in a predetermined order. (JP 3-02.1)

combat power — The total means of destructive and/or disruptive force which a military unit/formation can apply against the opponent at a given time. (JP 3-0)

combat readiness — Synonymous with operational readiness, with respect to missions or functions performed in combat. (JP 1-0)

combat search and rescue — The tactics, techniques, and procedures performed by forces to effect the recovery of isolated personnel during combat. Also called **CSAR.** See also **search and rescue.** (JP 3-50)

combat service support — The essential capabilities, functions, activities, and tasks necessary to sustain all elements of all operating forces in theater at all levels of war. Also called **CSS.** See also **combat support.** (JP 4-0)

combat service support area — An area ashore that is organized to contain the necessary supplies, equipment, installations, and elements to provide the landing force with combat service support throughout the operation. Also called **CSSA.** (JP 3-02)

combat spread loading — A method of combat loading by which some of the troops, equipment, and initial supplies of a unit are loaded in one ship and the remainder are loaded in one or more others. (JP 3-02.1)

combat support — Fire support and operational assistance provided to combat elements. Also called **CS.** See also **combat service support.** (JP 4-0)

combat support agency — A Department of Defense agency so designated by Congress or the Secretary of Defense that supports military combat operations. Also called **CSA.** (JP 5-0)

combat surveillance — A continuous, all-weather, day-and-night, systematic watch over the battle area in order to provide timely information for tactical combat operations. (JP 3-01)

combat unit loading — A method of loading by which all or a part of a combat unit, such as an assault battalion landing team, is completely loaded in a single ship, with essential combat equipment and supplies, in such a manner as to be immediately available to support the tactical plan upon debarkation, and to provide a maximum of flexibility to meet possible changes in the tactical plan. (JP 3-02.1)

combined — A term identifying two or more forces or agencies of two or more allies operating together. See also **joint.** (JP 3-16)

combined arms team — The full integration and application of two or more arms or elements of one Service into an operation. (JP 3-18)

command — 1. The authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. 2. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action. 3. A unit or units, an organization, or an area under the command of one individual. Also called **CMD.** See also **area command; combatant command; combatant command (command authority).** (JP 1)

command and control — The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Also called **C2.** (JP 1)

command and control system — The facilities, equipment, communications, procedures, and personnel essential for a commander to plan, direct, and control operations of assigned and attached forces pursuant to the missions assigned. (JP 6-0)

command chaplain — The senior chaplain assigned to or designated by a commander of a staff, command, or unit. See also **combatant command chaplain; religious support.** (JP 1-05)

commander, amphibious task force — The Navy officer designated in the initiating directive as the commander of the amphibious task force. Also called **CATF.** See also **amphibious operation; amphibious task force; commander, landing force.** (JP 3-02)

commander, landing force — The officer designated in the initiating directive as the commander of the landing force for an amphibious operation. Also called **CLF.** See also **amphibious operation; commander, amphibious task force; landing force.** (JP 3-02)

commander's communication synchronization — A process to coordinate and synchronize narratives, themes, messages, images, operations, and actions to ensure their integrity and consistency to the lowest tactical level across all relevant communication activities. Also called **CCS.** (JP 3-61)

commander's critical information requirement — An information requirement identified by the commander as being critical to facilitating timely decision making. Also called **CCIR.** See also **information requirements; intelligence; priority intelligence requirement.** (JP 3-0)

commander's estimate — A developed course of action designed to provide the Secretary of Defense with military options to meet a potential contingency. (JP 5-0)

commander's intent — A clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned. See also **assessment; end state.** (JP 3-0)

commander's required delivery date — The original date relative to C-day, specified by the combatant commander for arrival of forces or cargo at the destination; shown in the time-phased force and deployment data to assess the impact of later arrival. (JP 5-0)

command information — Communication by a military organization directed to the internal audience that creates an awareness of the organization's goals, informs them of significant developments affecting them and the organization, increases their effectiveness as ambassadors of the organization, and keeps them informed about what is going on in the organization. Also called **internal information.** See also **command; public affairs.** (JP 3-61)

commanding officer of troops — On a ship that has embarked units, a designated officer (usually the senior embarking unit commander) who is responsible for the administration, discipline, and training of all embarked units. Also called **COT.** (JP 3-02)

command net — A communications network that connects an echelon of command with some or all of its subordinate echelons for the purpose of command and control. (JP 3-09.3)

command post exercise — An exercise in which the forces are simulated, involving the commander, the staff, and communications within and between headquarters. Also called **CPX.** See also **exercise; maneuver.** (JP 3-0)

command relationships — The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command; defined further as combatant command (command authority), operational control, tactical control, or support. See also **chain of command; combatant command (command authority); command; operational control; support; tactical control.** (JP 1)

command-sponsored dependent — A dependent entitled to travel to overseas commands at government expense and endorsed by the appropriate military commander to be present in a dependent's status. (JP 3-68)

command structure — The organizational hierarchy through which administrative leadership or operational authority is exercised. (DODI 8260.03)

commercial items — Articles of supply readily available from established commercial distribution sources which the Department of Defense or inventory managers in the Military Services have designated to be obtained directly or indirectly from such sources. (JP 4-06)

commercial vehicle — A vehicle that has evolved in the commercial market to meet civilian requirements and which is selected from existing production lines for military use. (JP 4-06)

commit — The process of assigning one or more aircraft or surface-to-air missile units to prepare to engage an entity, prior to authorizing such engagement. (JP 3-01)

commodity loading —A method of loading in which various types of cargoes are loaded together, such as ammunition, rations, or boxed vehicles, in order that each commodity can be discharged without disturbing the others. See also **combat loading.** (JP 3-02.1)

commonality — A quality that applies to materiel or systems: a. possessing like and interchangeable characteristics enabling each to be utilized, or operated and maintained, by personnel trained on the others without additional specialized training; b. having interchangeable repair parts and/or components; and c. applying to consumable items interchangeably equivalent without adjustment. (JP 6-0)

common item — 1. Any item of materiel that is required for use by more than one activity. 2. A term loosely used to denote any consumable item except repair parts or other technical items. 3. Any item of materiel that is procured for, owned by (Service stock), or used by any Military Department of the Department of Defense and is also required to be furnished to a recipient country under the grant-aid Military Assistance Program. 4. Readily available commercial items. 5. Items used by two or more Military Services of similar manufacture or fabrication that may vary between the Services as to color or shape (as vehicles or clothing). 6. Any part or component that is required in the assembly of two or more complete end-items. (JP 4-01.5)

common operating environment — Automation services that support the development of the common reusable software modules that enable interoperability across multiple combat support applications. Also called **COE.** (JP 4-01.2)

common operational picture — A single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called **COP.** (JP 3-0)

common servicing — Functions performed by one Service in support of another for which reimbursement is not required. (JP 3-34)

common tactical picture — An accurate and complete display of relevant tactical data that integrates tactical information from the multi-tactical data link network, ground network, intelligence network, and sensor networks. Also called **CTP.** (JP 3-01)

common use — Services, materiel, or facilities provided by a Department of Defense agency or a Military Department on a common basis for two or more Department of Defense agencies, elements, or other organizations as directed. (JP 4-01.5)

common-use container — Any Department of Defense-owned, -leased, or -controlled 20- or 40-foot International Organization for Standardization container managed by United States Transportation Command as an element of the Department of Defense common-use container system. See also **component-owned container; Service-unique container.** (JP 4-09)

common-user airlift service — The airlift service provided on a common basis for all Department of Defense agencies and, as authorized, for other agencies of the United States Government. (JP 3-17)

common-user item — An item of an interchangeable nature that is in common use by two or more nations or Services of a nation. (JP 4-0)

common-user land transportation — Point-to-point land transportation service operated by a single Service for common use by two or more Services. Also called **CULT**. (JP 4-01.5)

common-user logistics — Materiel or service support shared with or provided by two or more Services, Department of Defense agencies, or multinational partners to another Service, Department of Defense agency, non-Department of Defense agency, and/or multinational partner in an operation. Also called **CUL.** See also **common use.** (JP 4-09)

common-user network — A system of circuits or channels allocated to furnish communication paths between switching centers to provide communication service on a common basis to all connected stations or subscribers. (JP 3-33)

common-user ocean terminal — A military installation, part of a military installation, or a commercial facility operated under contract or arrangement by the Military Surface Deployment and Distribution Command that regularly provides for two or more Services terminal functions of receipt, transit storage or staging, processing, and loading and unloading of passengers or cargo aboard ships. (JP 4-01.2)

common-user sealift — The sealift services provided by the Military Sealift Command on a common basis for all Department of Defense agencies and, as authorized, for other departments and agencies of the United States Government. See also **Military Sealift Command; transportation component command.** (JP 4-01.2)

common-user transportation — Transportation and transportation services provided on a common basis for two or more Department of Defense agencies and, as authorized, non-Department of Defense agencies. See also **common use.** (JP 4-01.2)

communications intelligence — Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called **COMINT.** (JP 2-0)

communications network — An organization of stations capable of intercommunications, but not necessarily on the same channel. Also called **COMNET**. (JP 6-0)

communications security — The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC.** (JP 6-0)

communications security material — All documents, devices, equipment, apparatus, and cryptomaterial used in establishing or maintaining secure communications. (JP 4-01.6)

community engagement — Public affairs activities that support the relationship between military and civilian communities. (JP 3-61)

completeness — The joint operation plan review criterion for assessing whether operation plans incorporate major operations and tasks to be accomplished and to what degree they include forces required, deployment concept, employment concept, sustainment concept, time estimates for achieving objectives, description of the end state, mission success criteria, and mission termination criteria. (JP 5-0)

complex catastrophe — Any natural or man-made incident, including cyberspace attack, power grid failure, and terrorism, which results in cascading failures of multiple, interdependent, critical, life-sustaining infrastructure sectors and caused extraordinary levels of mass casualties, damage, or disruption severely affecting the population, environment, economy, public health, national morale, response efforts, and/or government functions. (DepSecDef Memo OSD001185-13)

component — 1. One of the subordinate organizations that constitute a joint force. (JP 1) 2. In logistics, a part or combination of parts having a specific function, which can be installed or replaced only as an entity. Also called **COMP.** See also **functional component command; Service component command.** (JP 4-0)

component-owned container — A 20- or 40-foot International Organization for Standardization container procured and owned by a single Department of Defense component. Also called **Service-unique container.** See also **common-use container.** (JP 4-09)

composite warfare commander — An officer to whom the officer in tactical command of a naval task organization may delegate authority to conduct some or all of the offensive and defensive functions of the force. Also called **CWC**. (JP 3-32)

compromise — The known or suspected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person. (JP 2-01.2)

compromised — A term applied to classified matter, knowledge of which has, in whole or in part, passed to an unauthorized person or persons, or which has been subject to risk of such passing. (JP 2-01.2)

concept of intelligence operations — Within the Department of Defense, a verbal or graphic statement, in broad outline, of an intelligence directorate's assumptions or intent in regard to intelligence support of an operation or series of operations. See also **concept of operations.** (JP 2-0)

concept of logistic support — A verbal or graphic statement, in a broad outline, of how a commander intends to support and integrate with a concept of operations in an operation or campaign. Also called **COLS**. (JP 4-0)

concept of operations — A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources. Also called **CONOPS.** (JP 5-0)

concept plan — In the context of joint operation planning level 3 planning detail, an operation plan in an abbreviated format that may require considerable expansion or alteration to convert it into a complete operation plan or operation order. Also called **CONPLAN.** See also **operation plan.** (JP 5-0)

condition — 1. Those variables of an operational environment or situation in which a unit, system, or individual is expected to operate and may affect performance. 2. A physical or behavioral state of a system that is required for the achievement of an objective. See also **joint mission-essential tasks.** (JP 3-0)

conduits — Within military deception, conduits are information or intelligence gateways to the deception target. Examples of conduits include: foreign intelligence and security services, intelligence collection platforms, open-source intelligence, news media—foreign and domestic. (JP 3-13.4)

confidential — Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. (EO 13526)

configuration management — A discipline applying technical and administrative direction and surveillance to: (1) identify and document the functional and physical characteristics of a configuration item; (2) control changes to those characteristics; and (3) record and report changes to processing and implementation status. Also called **CM**. (JP 6-0)

conflict prevention — A peace operation employing complementary diplomatic, civil, and, when necessary, military means, to monitor and identify the causes of conflict, and take timely action to prevent the occurrence, escalation, or resumption of hostilities. (JP 3-07.3)

constellation — A system consisting of a number of like satellites acting in concert to perform a specific mission. See also **Global Positioning System.** (JP 3-14)

constraint — In the context of joint operation planning, a requirement placed on the command by a higher command that dictates an action, thus restricting freedom of action. See also **operational limitation; restraint.** (JP 5-0)

consumer — Person or agency that uses information or intelligence produced by either its own staff or other agencies. (JP 2-01)

consumption rate — The average quantity of an item consumed or expended during a given time interval, expressed in quantities by the most appropriate unit of measurement per applicable stated basis. (JP 4-05)

contact mine — A mine detonated by physical contact. See also **mine**. (JP 3-15)

contact point — 1. In land warfare, a point on the terrain, easily identifiable, where two or more units are required to make contact. (JP 3-50) 2. In air operations, the position at which a mission leader makes radio contact with an air control agency. (JP 3-09.3) 3. In personnel recovery, a location where isolated personnel can establish contact with recovery forces. Also called **CP.** See also **control point.** (JP 3-50)

contact procedure — Predesignated actions taken by isolated personnel and recovery forces that permit link-up between the two parties in hostile territory. See also **evader.** (JP 3-50)

container — An article of transport equipment that meets American National Standards Institute/International Organization for Standardization standards that is designed to facilitate and optimize the carriage of goods by one or more modes of transportation without intermediate handling of the contents. (JP 4-01)

container control officer — A designated official (E6 or above or civilian equivalent) within a command, installation, or activity who is responsible for control, reporting, use, and maintenance of all Department of Defense-owned and controlled intermodal containers and equipment from time received until dispatched. Also called **CCO**. (JP 4-09)

container-handling equipment — Items of materials-handling equipment required to specifically receive, maneuver, and dispatch International Organization for Standardization containers. Also called **CHE.** (JP 4-09)

container management — Planning, organizing, directing, and executing functions and responsibilities required to provide effective use of Department of Defense and Military Department owned, leased, or controlled International Organization for Standardization containers. (JP 4-09)

containership — A ship, usually non-self-sustaining, specially constructed and equipped to carry only containers without associated equipment, in all available cargo spaces, either below or above deck. (JP 4-09)

contaminated remains — Remains of personnel which have absorbed or upon which have been deposited radioactive material, or biological or chemical agents. See also **mortuary affairs.** (JP 4-06)

contamination — 1. The deposit, absorption, or adsorption of radioactive material, or of biological or chemical agents on or by structures, areas, personnel, or objects. Also called **fallout radiation**. 2. Food and/or water made unfit for consumption by humans or animals because of the presence of environmental chemicals, radioactive elements, bacteria or organisms, the byproduct of the growth of bacteria or organisms, the decomposing material or waste in the food or water. (JP 3-11)

contamination avoidance — Individual and/or unit measures taken to reduce the effects of chemical, biological, radiological, and nuclear hazards. (JP 3-11)

contamination control — A combination of preparatory and responsive measures designed to limit the vulnerability of forces to chemical, biological, radiological, nuclear, and toxic industrial hazards and to avoid, contain, control exposure to, and, where possible, neutralize them. See also **biological agent; chemical agent; contamination.** (JP 3-11)

contamination mitigation — The planning and actions taken to prepare for, respond to, and recover from contamination associated with all chemical, biological, radiological, and nuclear threats and hazards in order to continue military operations. (JP 3-11)

contiguous zone — 1. A maritime zone adjacent to the territorial sea that may not extend beyond 24 nautical miles from the baselines from which the breadth of the territorial sea is measured. 2. The zone of the ocean extending 3-12 nautical miles from the United States coastline. (JP 3-32)

continental United States — United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico. Also called **CONUS.** (JP 1)

contingency — A situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect US interests. See also **contingency contracting.** (JP 5-0)

contingency basing — The life-cycle process of planning, designing, constructing, operating, managing, and transitioning or closing a non-enduring location supporting a combatant commander's requirements. (DODD 3000.10).

contingency contract — A legally binding agreement for supplies, services, and construction let by government contracting officers in the operational area as well as other contracts that have a prescribed area of performance within a designated operational area. See also **external support contract; systems support contract; theater support contract.** (JP 4-10)

contingency contracting — The process of obtaining goods, services, and construction via contracting means in support of contingency operations. See also contingency; contingency contract. (JP 4-10)

contingency engineering management organization — An organization formed by the combatant commander, or subordinate commander to augment their staffs with additional Service engineering expertise for planning and construction management. See also **combat engineering; contingency; crisis action planning; geospatial engineering.** (JP 3-34)

contingency location — A non-enduring location outside of the United States that supports and sustains operations during named and unnamed contingencies or other operations as directed by appropriate authority and is categorized by mission life-cycle requirements as initial, temporary, or semi-permanent. (DODD 3000.10)

contingency operation — A military operation that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law (Title 10, United States Code, Section 101[a][13]). See also **contingency; operation.** (JP 1)

contingency plan — A plan for major contingencies that can reasonably be anticipated in the principal geographic subareas of the command. (JP 5-0)

Contingency Planning Guidance — Secretary of Defense written guidance, approved by the President, for the Chairman of the Joint Chiefs of Staff, which focuses the guidance given in the national security strategy and Defense Planning Guidance, and is the principal source document for the Joint Strategic Capabilities Plan. Also called **CPG.** (JP 1)

contingency response program — Fast reaction transportation procedures intended to provide for priority use of land transportation assets by Department of Defense when required. Also called **CORE.** (JP 4-01)

contingency ZIP Code — A ZIP Code consisting of a five-digit base with a four-digit add-on to assist in routing and sorting assigned by Military Postal Service Agency to a contingency post office for the tactical use of the Armed Forces on a temporary basis. (JP 1-0)

continuity of operations — The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. Also called **COOP.** (JP 3-0)

contract administration — A subset of contracting that includes efforts to ensure that supplies, services, and construction are delivered in accordance with the terms and conditions of the contract. (JP 4-10)

contracting officer — A Service member or Department of Defense civilian with the legal authority to enter into, administer, modify, and/or terminate contracts. (JP 4-10)

contracting officer representative — A Service member or Department of Defense civilian or a foreign government civilian or military member appointed in writing and trained by a contracting officer, responsible for monitoring contract performance and performing other duties specified by their appointment letter. Also called **COR.** (JP 4-10)

contractor management — The oversight and integration of contractor personnel and associated equipment providing support to the joint force in a designated operational area. (JP 4-10)

contractors authorized to accompany the force — Contingency contractor employees and all tiers of subcontractor employees who are authorized to accompany the force in applicable contingency operations and have afforded such status through the issuance of a letter of authorization. Also called **CAAF.** (JP 4-10)

contract statement of requirement — A document that provides a summary of anticipated contracted supply or service requirements by phase of operation and location. Also called **CSOR.** (JP 4-10)

control — 1. Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (JP 1) 2. In mapping, charting, and photogrammetry, a collective term for a system of marks or objects on the Earth or on a map or a photograph, whose positions or elevations (or both) have been or will be determined. (JP 2-03) 3. Physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. (JP 3-0) 4. An indicator governing the distribution and use of documents, information, or material. Such indicators are the

subject of intelligence community agreement and are specifically defined in appropriate regulations. See also **administrative control; operational control; tactical control.** (JP 2-01)

control area — A controlled airspace extending upwards from a specified limit above the Earth. See also **control zone.** (JP 3-04)

control group — Personnel, ships, and craft designated to control the waterborne ship-to-shore movement. (JP 3-02)

controlled information — 1. Information conveyed to an adversary in a deception operation to evoke desired appreciations. 2. Information and indicators deliberately conveyed or denied to foreign targets to evoke invalid official estimates that result in foreign official actions advantageous to US interests and objectives. (JP 2-01.2)

controlled source — In counterintelligence use, a person employed by or under the control of an intelligence activity and responding to intelligence tasking. (JP 2-01.2)

controlled substance — A drug or other substance, or immediate precursor included in Schedule I, II, III, IV, or V of the Controlled Substances Act. (JP 3-07.4)

controlled technical services — The controlled use of technology to enhance counterintelligence and human intelligence activities. Also called **CTS**. (JP 2-01.2)

control point — 1. A position along a route of march at which men are stationed to give information and instructions for the regulation of supply or traffic. 2. A position marked by coordinates (latitude, longitude), a buoy, boat, aircraft, electronic device, conspicuous terrain feature, or other identifiable object which is given a name or number and used as an aid to navigation or control of ships, boats, or aircraft. 3. In marking mosaics, a point located by ground survey with which a corresponding point on a photograph is matched as a check. (JP 3-09.3)

control zone — A controlled airspace extending upwards from the surface of the Earth to a specified upper limit. See also **control area.** (JP 3-52)

conventional forces — 1. Those forces capable of conducting operations using nonnuclear weapons. 2. Those forces other than designated special operations forces. Also called **CF.** (JP 3-05)

conventional mines — Land mines, other than nuclear or chemical, that are not designed to self-destruct; are designed to be emplaced by hand or mechanical means; and can be buried or surface emplaced. See also **mine.** (JP 3-15)

convoy — 1. A number of merchant ships and/or naval auxiliaries usually escorted by warships and/or aircraft — or a single merchant ship or naval auxiliary under surface escort — assembled and organized for the purpose of passage together. 2. A group of

vehicles organized for the purpose of control and orderly movement with or without escort protection that moves over the same route at the same time and under one commander. (JP 3-02.1)

convoy escort — 1. A naval ship(s) or aircraft in company with a convoy and responsible for its protection. 2. An escort to protect a convoy of vehicles from being scattered, destroyed, or captured. See also **escort.** (JP 4-01.5)

cooperative security location — A facility located outside the United States and US territories with little or no permanent US presence, maintained with periodic Service, contractor, or host-nation support. Cooperative security locations provide contingency access, logistic support, and rotational use by operating forces and are a focal point for security cooperation activities. Also called **CSL.** See also **forward operating site; main operating base.** (CJCS CM-0007-05)

coordinated fire line — A line beyond which conventional surface-to-surface direct fire and indirect fire support means may fire at any time within the boundaries of the establishing headquarters without additional coordination. Also called **CFL.** See also **fire support.** (JP 3-09)

coordinating agency — An agency that supports the incident management mission by providing the leadership, staff, expertise, and authorities to implement critical and specific aspects of the response. (JP 3-28)

coordinating altitude — An airspace coordinating measure that uses altitude to separate users and as the transition between different airspace control elements. Also called **CA**. (JP 3-52)

coordinating authority — A commander or individual who has the authority to require consultation between the specific functions or activities involving forces of two or more Services, joint force components, or forces of the same Service or agencies, but does not have the authority to compel agreement. (JP 1)

coordinating review authority — An agency appointed by a Service or combatant command to coordinate with and assist the lead agent, primary review authority, Joint Staff doctrine sponsor, and assessment agent in joint doctrine development and maintenance. Also called **CRA.** See also **joint doctrine; joint publication; lead agent; primary review authority.** (CJCSM 5120.01)

coordination level — A procedural method to separate fixed- and rotary-wing aircraft by determining an altitude below which fixed-wing aircraft normally will not fly. Also called **CL**. (JP 3-52)

cost-type contract — A contract that provides for payment to the contractor of allowable cost, to the extent prescribed in the contract, incurred in performance of the contract. (JP 4-10)

counterair — A mission that integrates offensive and defensive operations to attain and maintain a desired degree of air superiority and protection by neutralizing or destroying enemy aircraft and missiles, both before and after launch. See also **air superiority; mission; offensive counterair.** (JP 3-01)

counterdeception — Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (JP 3-13.4)

counterdrug — Those active measures taken to detect, monitor, and counter the production, trafficking, and use of illegal drugs. Also called **CD**. (JP 3-07.4)

counterdrug activities — Those measures taken to detect, interdict, disrupt, or curtail any activity that is reasonably related to illicit drug trafficking. (JP 3-07.4)

counterdrug operational support — Support to host nations and drug law enforcement agencies involving military personnel and their associated equipment, provided by the geographic combatant commanders from forces assigned to them or made available to them by the Services for this purpose. See also **counterdrug operations.** (JP 3-07.4)

counterdrug operations — Civil or military actions taken to reduce or eliminate illicit drug trafficking. See also **counterdrug; counterdrug operational support.** (JP 3-07.4)

counterespionage — That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities. (JP 2-01.2)

counterfire — Fire intended to destroy or neutralize enemy weapons. (JP 3-09)

counterforce — The employment of strategic air and missile forces in an effort to destroy, or render impotent, selected military capabilities of an enemy force under any of the circumstances by which hostilities may be initiated.

counterguerrilla operations — Operations and activities conducted by armed forces, paramilitary forces, or nonmilitary agencies against guerrillas. (JP 3-24)

counter-improvised explosive device operations — The organization, integration, and synchronization of capabilities that enable offensive, defensive, stability, and support operations across all phases of operations or campaigns in order to defeat improvised explosive devices as operational and strategic weapons of influence. Also called **C-IED operations.** (JP 3-15.1)

countering weapons of mass destruction — Efforts against actors of concern to curtail the conceptualization, development, possession, proliferation, use, and effects of weapons of

mass destruction, related expertise, materials, technologies, and means of delivery. Also called **CWMD**. (JP 3-40)

counterinsurgency — Comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes. Also called **COIN.** (JP 3-24)

counterintelligence — Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. Also called **CI**. See also **counterespionage; security.** (JP 2-01.2)

counterintelligence activities — One or more of the five functions of counterintelligence: operations, investigations, collection, analysis and production, and functional services. See also **analysis and production; collection; counterintelligence; operation.** (JP 2-01.2)

counterintelligence collection — The systematic acquisition of information (through investigations, operations, or liaison) concerning espionage, sabotage, terrorism, other intelligence activities or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons that are directed against or threaten Department of Defense interests. See also **counterintelligence.** (JP 2-01.2)

counterintelligence insider threat — A person who uses their authorized access to Department of Defense facilities, systems, equipment, information or infrastructure to damage, disrupt operations, commit espionage on behalf of a foreign intelligence entity or support international terrorist organizations. (JP 2-01.2)

counterintelligence investigation — An official, systematic search for facts to determine whether a person(s) is engaged in activities that may be injurious to US national security or advantageous to a foreign power. See also **counterintelligence.** (JP 2-01.2)

counterintelligence operational tasking authority — The levying of counterintelligence requirements specific to joint military activities and operations. Counterintelligence operational tasking authority is exercised through supporting components. Also called **CIOTA.** See also **counterintelligence.** (JP 2-01.2)

counterintelligence operations — Proactive activities designed to identify, exploit, neutralize, or deter foreign intelligence collection and terrorist activities directed against the United States. See also **counterintelligence; operation.** (JP 2-01.2)

counterintelligence production — The process of analyzing all-source information concerning espionage or other multidiscipline intelligence collection threats, sabotage, terrorism, and other related threats to US military commanders, the Department of Defense, and the US Intelligence Community and developing it into a final product that

is disseminated. Counterintelligence production is used in formulating security policy, plans, and operations. See also **counterintelligence.** (JP 2-01.2)

counterintelligence support — Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on behalf of foreign powers, organizations, or persons. See also **counterintelligence.** (JP 2-01.2)

countermeasures — That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. See also **electronic warfare.** (JP 3-13.1)

countermobility operations — The construction of obstacles and emplacement of minefields to delay, disrupt, and destroy the enemy by reinforcement of the terrain. See also **minefield; operation; target acquisition.** (JP 3-34)

counterproliferation — Those actions taken to reduce the risks posed by extant weapons of mass destruction to the United States, allies, and partners. Also called **CP.** See also **nonproliferation.** (JP 3-40)

countersurveillance — All measures, active or passive, taken to counteract hostile surveillance. See also **surveillance**. (JP 3-07.2)

counterterrorism — Activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. Also called **CT.** See also **antiterrorism; combating terrorism; terrorism.** (JP 3-26)

counter threat finance — Activities conducted to deny, disrupt, destroy, or defeat the generation, storage, movement, and use of assets to fund activities that support an adversary's ability to negatively affect United States interests. Also called **CTF.** (JP 3-05)

country team — The senior, in-country, United States coordinating and supervising body, headed by the chief of the United States diplomatic mission, and composed of the senior member of each represented United States department or agency, as desired by the chief of the United States diplomatic mission. Also called **CT.** (JP 3-07.4)

coup de main — An offensive operation that capitalizes on surprise and simultaneous execution of supporting operations to achieve success in one swift stroke. (JP 3-0)

courier — A messenger (usually a commissioned or warrant officer) responsible for the secure physical transmission and delivery of documents and material. (JP 2-01)

course of action — 1. Any sequence of activities that an individual or unit may follow. 2. A scheme developed to accomplish a mission. 3. A product of the course-of-action development step of the joint operation planning process. Also called **COA.** (JP 5-0)

cover — In intelligence usage, those measures necessary to give protection to a person, plan, operation, formation, or installation from the enemy intelligence effort and leakage of information. (JP 2-01.2)

covering fire — 1. Fire used to protect troops when they are within range of enemy small arms. 2. In amphibious usage, fire delivered prior to the landing to cover preparatory operations such as underwater demolition or mine countermeasures. (JP 3-02)

covering force — 1. A force operating apart from the main force for the purpose of intercepting, engaging, delaying, disorganizing, and deceiving the enemy before the enemy can attack the force covered. 2. Any body or detachment of troops which provides security for a larger force by observation, reconnaissance, attack, or defense, or by any combination of these methods. (JP 3-18)

covert operation — An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. See also **clandestine operation; overt operation.** (JP 3-05)

crisis — An incident or situation involving a threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national objectives. (JP 3-0)

crisis action planning — The Adaptive Planning and Execution system process involving the time-sensitive development of joint operation plans and operation orders for the deployment, employment, and sustainment of assigned and allocated forces and resources in response to an imminent crisis. Also called **CAP.** See also **joint operation planning; Joint Operation Planning and Execution System.** (JP 5-0)

crisis management — Measures, normally executed under federal law, to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or an act of terrorism. Also called **CrM.** (JP 3-28)

critical asset — A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (JP 3-07.2)

critical asset list — A prioritized list of assets or areas, normally identified by phase of the operation and approved by the joint force commander, that should be defended against air and missile threats. Also called **CAL.** (JP 3-01)

critical capability — A means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s). (JP 5-0)

critical element — 1. An element of an entity or object that enables it to perform its primary function. 2. An element of a target, which if effectively engaged, will serve to support the achievement of an operational objective and/or mission task. Also called **CE.** (JP 3-60)

critical information — Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. Also called **CRITIC**. (JP 2-0)

critical infrastructure and key resources — The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. Also called **CI/KR.** (JP 3-27)

critical infrastructure protection — Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Also called **CIP.** See also **defense critical infrastructure.** (JP 3-28)

critical intelligence — Intelligence that is crucial and requires the immediate attention of the commander. (JP 2-0)

critical item list — A prioritized list identifying supply items and weapon systems that assist Service and Defense Logistics Agency selection of supply items and systems for production surge planning, or in operational situations, used by the combatant commander and/or subordinate joint force commander to cross-level critical supply items between Service components. Also called **CIL.** (JP 4-05)

criticality assessment — An assessment that identifies key assets and infrastructure that support Department of Defense missions, units, or activities and are deemed mission critical by military commanders or civilian agency managers. Also called **CA**. (JP 3-07.2)

critical joint duty assignment billet — A joint duty assignment position for which, considering the duties and responsibilities of the position, it is highly important that the assigned officer be particularly trained in, and oriented toward, joint matters. (JP 1-0)

critical occupational specialty — A military occupational specialty selected from among the combat arms in the Army or equivalent military specialties in the Navy, Air Force, or Marine Corps. Equivalent military specialties are those engaged in operational art in order to attain strategic goals in an operational area through the design, organization, and conduct of campaigns and major operations. Critical occupational specialties are designated by the Secretary of Defense. Also called **COS.**

critical requirement — An essential condition, resource, and means for a critical capability to be fully operational. (JP 5-0)

critical vulnerability — An aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects. (JP 5-0)

cross-leveling —At the theater strategic and operational levels, it is the process of diverting en route or in-theater materiel from one military element to meet the higher priority of another within the combatant commander's directive authority for logistics. (JP 4-0)

cross-loading — The distribution of leaders, key weapons, personnel, and key equipment among the aircraft, vessels, or vehicles of a formation to aid rapid assembly of units at the drop zone or landing zone or preclude the total loss of command and control or unit effectiveness if an aircraft, vessel, or vehicle is lost. (JP 3-17)

cross-servicing — A subset of common-user logistics in which a function is performed by one Military Service in support of another Service and for which reimbursement is required from the Service receiving support. See also **acquisition and cross-servicing agreement; common-user logistics.** (JP 4-08)

cruise missile — Guided missile, the major portion of whose flight path to its target is conducted at approximately constant velocity; depends on the dynamic reaction of air for lift and upon propulsion forces to balance drag. (JP 3-01)

culminating point — The point at which a force no longer has the capability to continue its form of operations, offense or defense. (JP 5-0)

current force — The actual force structure and/or manning available to meet present contingencies. See also **force.** (JP 5-0)

custody — 1. The responsibility for the control of, transfer and movement of, access to, and maintenance of accountability for weapons and components. 2. Temporary restraint of a person. 3. The detention of a person by lawful authority or process. (JP 3-63)

customer direct — A materiel acquisition and distribution method that requires vendor delivery directly to the customer. Also called **CD.** (JP 4-09)

customer wait time — The total elapsed time between issuance of a customer order and satisfaction of that order. Also called **CWT.** (JP 4-09)

cybersecurity — Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01)

cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

cyberspace operations — The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)

cyberspace superiority — The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. (JP 3-12)

D

damage assessment — 1. The determination of the effect of attacks on targets. 2. A determination of the effect of a compromise of classified information on national security. (JP 3-60)

damage criteria — The critical levels of various weapons effects required to create specified levels of damage. (JP 3-60)

damage estimation — A preliminary appraisal of the potential effects of an attack. See also **attack assessment.** (JP 3-60)

danger close — In close air support, artillery, mortar, and naval gunfire support fires, the term included in the method of engagement segment of a call for fire that indicates that friendly forces are within close proximity of the target. See also **final protective fire.** (JP 3-09.3)

dangerous cargo — Cargo that is subject to special regulations for its transport because of its dangerous properties. (JP 4-01.5)

data element — 1. A basic unit of information built on standard structures having a unique meaning and distinct units or values. 2. In electronic recordkeeping, a combination of characters or bytes referring to one separate item of information, such as name, address, or age. (JP 1-0)

date-time group — The date and time, expressed as six digits followed by the time zone suffix at which the message was prepared for transmission (first pair of digits denotes the date, second pair the hours, third pair the minutes, followed by a three-letter month abbreviation and two-digit year abbreviation.). Also called **DTG.** (JP 5-0)

datum (geodetic) — 1. A reference surface consisting of five quantities: the latitude and longitude of an initial point, the azimuth of a line from that point, and the parameters of the reference ellipsoid. 2. The mathematical model of the earth used to calculate the coordinates on any map. Different nations use different datum for printing coordinates on their maps. (JP 2-03)

D-day — The unnamed day on which a particular operation commences or is to commence. (JP 3-02)

de-arming — An operation in which a weapon is changed from a state of readiness for initiation to a safe condition. Also called **safing.** (JP 3-04)

debarkation — The unloading of troops, equipment, or supplies from a ship or aircraft. (JP 3-02.1)

debarkation schedule —A schedule that provides for the timely and orderly debarkation of troops and equipment and emergency supplies for the waterborne ship-to-shore movement. (JP 3-02.1)

decedent effects — Personal effects found on human remains. Also called **DE.** (JP 4-06)

decentralized control — In air defense, the normal mode whereby a higher echelon monitors unit actions, making direct target assignments to units only when necessary to ensure proper fire distribution or to prevent engagement of friendly aircraft. See also **centralized control.** (JP 3-01)

decentralized execution — Delegation of execution authority to subordinate commanders. (JP 3-30)

deception action — A collection of related deception events that form a major component of a deception operation. (JP 3-13.4)

deception concept — The deception course of action forwarded to the Chairman of the Joint Chiefs of Staff for review as part of the combatant commander's strategic concept. (JP 3-13.4)

deception event — A deception means executed at a specific time and location in support of a deception operation. (JP 3-13.4)

deception means — Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. **physical means.** Activities and resources used to convey or deny selected information to a foreign power. b. **technical means.** Military material resources and their associated operating techniques used to convey or deny selected information to a foreign power. c. **administrative means.** Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 3-13.4)

deception objective — The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location. (JP 3-13.4)

deception story — A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. (JP 3-13.4)

deception target — The adversary decision maker with the authority to make the decision that will achieve the deception objective. (JP 3-13.4)

decision — In an estimate of the situation, a clear and concise statement of the line of action intended to be followed by the commander as the one most favorable to the successful accomplishment of the assigned mission. (JP 5-0)

decision point — A point in space and time when the commander or staff anticipates making a key decision concerning a specific course of action. See also **course of action; decision support template; target area of interest.** (JP 5-0)

decision support template — A combined intelligence and operations graphic based on the results of wargaming that depicts decision points, timelines associated with movement of forces and the flow of the operation, and other key items of information required to execute a specific friendly course of action. Also called **DST**. See also **course of action; decision point.** (JP 2-01.3)

decisive point — A geographic place, specific key event, critical factor, or function that, when acted upon, allows commanders to gain a marked advantage over an adversary or contribute materially to achieving success. See also **center of gravity.** (JP 5-0)

deck status light — A three-colored light (red, amber, green) controlled from the primary flight control. Navy — The light displays the status of the ship to support flight operations. United States Coast Guard — The light displays clearance for a helicopter to conduct a given evolution. (JP 3-04)

decompression — In personnel recovery, the process of normalizing psychological and behavioral reactions that recovered isolated personnel experienced or are currently experiencing as a result of their isolation and recovery. (JP 3-50)

decontamination — The process of making any person, object, or area safe by absorbing, destroying, neutralizing, making harmless, or removing chemical or biological agents, or by removing radioactive material clinging to or around it. (JP 3-11)

decoy — An imitation in any sense of a person, object, or phenomenon which is intended to deceive enemy surveillance devices or mislead enemy evaluation. Also called **dummy.** (JP 3-13.4)

defended asset list —A listing of those assets from the critical asset list prioritized by the joint force commander to be defended with the resources available. Also called **DAL.** (JP 3-01)

defense coordinating element — A staff and military liaison officers who assist the defense coordinating officer in facilitating coordination and support to activated emergency support functions. Also called **DCE.** (JP 3-28)

defense coordinating officer — Department of Defense single point of contact for domestic emergencies who is assigned to a joint field office to process requirements for military support, forward mission assignments through proper channels to the appropriate military organizations, and assign military liaisons, as appropriate, to activated emergency support functions. Also called **DCO.** (JP 3-28)

defense critical infrastructure — Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide. Also called **DCI.** (JP 3-27)

defense human intelligence executor — The senior Department of Defense intelligence official as designated by the head of each of the Department of Defense components who are authorized to conduct human intelligence and related intelligence activities. Also called **DHE**. (JP 2-01.2)

defense industrial base — The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Also called **DIB**. (JP 3-27)

Defense Information Systems Network — The integrated network, centrally managed and configured by the Defense Information Systems Agency to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services for all Department of Defense activities. Also called **DISN.** (JP 6-0)

Defense Satellite Communications System — Geosynchronous military communications satellites that provide high data rate communications for military forces, diplomatic corps, and the White House. Also called **DSCS.** (JP 3-14)

defense sexual assault incident database — A Department of Defense database that captures and serves as the reporting source for all sexual assault data collected by the Services. Also called **DSAID.** (JP 1-0)

defense support of civil authorities — Support provided by US Federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. Also called **DSCA**. Also known as **civil support**. (DODD 3025.18)

Defense Support Program — Satellites that provide early warning of missile launches. Also called **DSP.** (JP 3-14)

Defense Switched Network — The component of the Defense Communications System that handles Department of Defense voice, data, and video communications. Also called **DSN.** (JP 6-0)

Defense Transportation System — That portion of the worldwide transportation infrastructure that supports Department of Defense transportation needs in peace and

war. Also called **DTS.** See also **common-user transportation; transportation system.** (JP 4-01)

defensive counterair — All defensive measures designed to neutralize or destroy enemy forces attempting to penetrate or attack through friendly airspace. Also called **DCA.** See also **counterair; offensive counterair.** (JP 3-01)

defensive cyberspace operation response action — Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. Also called **DCO-RA.** (JP 3-12)

defensive cyberspace operations — Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called **DCO.** (JP 3-12)

defensive minefield — 1. In naval mine warfare, a minefield laid in international waters or international straits with the declared intention of controlling shipping in defense of sea communications. 2. In land mine warfare, a minefield laid in accordance with an established plan to prevent a penetration between positions and to strengthen the defense of the positions themselves. See also **minefield.** (JP 3-15)

defensive space control — Operations conducted to preserve the ability to exploit space capabilities via active and passive actions, while protecting friendly space capabilities from attack, interference, or unintentional hazards. (JP 3-14)

defilade — 1. Protection from hostile observation and fire provided by an obstacle such as a hill, ridge, or bank. 2. A vertical distance by which a position is concealed from enemy observation. 3. To shield from enemy fire or observation by using natural or artificial obstacles. (JP 3-09)

definitive care — Care rendered to conclusively manage a patient's condition, such as full range of preventive, curative acute, convalescent, restorative, and rehabilitative medical care. (JP 4-02)

degaussing — The process whereby a ship's magnetic field is reduced by the use of electromagnetic coils, permanent magnets, or other means. (JP 3-15)

delayed entry program — A program under which an individual may enlist in a Reserve Component of a military service and specify a future reporting date for entry on active duty that would coincide with availability of training spaces and with personal plans such as high school graduation. Also called **DEP.** See also **active duty.** (JP 4-05)

delaying operation — An operation in which a force under pressure trades space for time by slowing down the enemy's momentum and inflicting maximum damage on the enemy without, in principle, becoming decisively engaged. (JP 3-04)

delegation of authority — The action by which a commander assigns part of his or her authority, commensurate with the assigned task, to a subordinate commander. (JP 1)

deliberate planning — 1. The Adaptive Planning and Execution system process involving the development of joint operation plans for contingencies identified in joint strategic planning documents. 2. A planning process for the deployment and employment of apportioned forces and resources that occurs in response to a hypothetical situation. (JP 5-0)

demilitarized zone — A defined area in which the stationing or concentrating of military forces, or the retention or establishment of military installations of any description, is prohibited. (JP 3-07.3)

demobilization — 1. The process of transitioning a conflict or wartime military establishment and defense-based civilian economy to a peacetime configuration while maintaining national security and economic vitality. 2. The process necessary to release from active duty, or federal service, units and Reserve Component members who were ordered to active duty, or called to federal service. See also **mobilization**. (JP 4-05)

demonstration — 1. An attack or show of force on a front where a decision is not sought, made with the aim of deceiving the enemy. See also **amphibious demonstration; diversion.** 2. In military deception, a show of force in an area where a decision is not sought that is made to deceive an adversary. It is similar to a feint but no actual contact with the adversary is intended. (JP 3-13.4)

denial measure — An action to hinder or deny the enemy the use of territory, personnel, or facilities to include destruction, removal, contamination, or erection of obstructions. (JP 3-15)

denied area — An area under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities. (JP 3-05)

Department of Defense civilian — A Federal civilian employee of the Department of Defense directly hired and paid from appropriated or nonappropriated funds, under permanent or temporary appointment. (JP 1-0)

Department of Defense components — The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense agencies, Department of Defense field activities, and all other organizational entities in the Department of Defense. (JP 1)

Department of Defense construction agent — United States Army Corps of Engineers, Naval Facilities Engineering Command, or other such approved Department of Defense activity, that is assigned design or execution responsibilities associated with military

construction programs, facilities support, or civil engineering support to the combatant commanders in contingency operations. See also **contingency operation.** (JP 3-34)

Department of Defense container system — All Department of Defense owned, leased, and controlled 20- or 40-foot intermodal International Organization for Standardization containers and flatracks, supporting equipment such as generator sets and chassis, container handling equipment, information systems, the 463L system, and other infrastructure that supports Department of Defense transportation and logistic operations, including commercially provided transportation services. See also **container-handling equipment.** (JP 4-09)

Department of Defense information network — The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called **DODIN.** (JP 6-0)

Department of Defense information network operations — Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 3-12)

Department of Defense Intelligence Information System — The combination of Department of Defense personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national-level decision makers. Also called **DODIIS.** (JP 2-0)

Department of Defense support to counterdrug operations — Support provided by the Department of Defense to law enforcement agencies to detect, monitor, and counter the production, trafficking, and use of illegal drugs. See also **counterdrug operations.** (JP 3-07.4)

Department of the Air Force — The executive part of the Department of the Air Force at the seat of government and all field headquarters, forces, Reserve Component, installations, activities, and functions under the control or supervision of the Secretary of the Air Force. Also called **DAF.** See also **Military Department.** (JP 1)

Department of the Army — The executive part of the Department of the Army at the seat of government and all field headquarters, forces, Reserve Component, installations, activities, and functions under the control or supervision of the Secretary of the Army. Also called **DA.** See also **Military Department.** (JP 1)

Department of the Navy — The executive part of the Department of the Navy at the seat of government; the headquarters, United States Marine Corps; the entire operating forces

of the United States Navy and of the United States Marine Corps, including the Reserve Component of such forces; all field activities, headquarters, forces, bases, installations, activities, and functions under the control or supervision of the Secretary of the Navy; and the United States Coast Guard when operating as a part of the Navy pursuant to law. Also called **DON.** See also **Military Department.** (JP 1)

departure airfield — An airfield on which troops and/or materiel are enplaned for flight. See also **airfield.** (JP 3-17)

departure point — A navigational check point used by aircraft as a marker for setting course. (JP 3-17)

dependents — An employee's spouse; children who are unmarried and under age 21 years or who, regardless of age, are physically or mentally incapable of self-support; dependent parents, including step and legally adoptive parents of the employee's spouse; and dependent brothers and sisters, including step and legally adoptive brothers and sisters of the employee's spouse who are unmarried and under 21 years of age or who, regardless of age, are physically or mentally incapable of self-support. (JP 3-68)

deployment — The rotation of forces into and out of an operational area. See also **deployment order; deployment planning; prepare to deploy order.** (JP 3-35)

deployment health surveillance — The regular or repeated collection, analysis, archiving, interpretation, and distribution of health-related data used for monitoring the health of a population or of individuals, and for intervening in a timely manner to prevent, treat, or control the occurrence of disease or injury, which includes occupational and environmental health surveillance and medical surveillance subcomponents. (JP 4-02)

deployment order — A planning directive from the Secretary of Defense, issued by the Chairman of the Joint Chiefs of Staff, that authorizes and directs the transfer of forces between combatant commands by reassignment or attachment. Also called **DEPORD.** See also **deployment; deployment planning; prepare to deploy order.** (JP 5-0)

deployment planning — Operational planning directed toward the movement of forces and sustainment resources from their original locations to a specific operational area for conducting the joint operations contemplated in a given plan. See also **deployment; deployment order; prepare to deploy order.** (JP 5-0)

depot — 1. **supply** — An activity for the receipt, classification, storage, accounting, issue, maintenance, procurement, manufacture, assembly, research, salvage, or disposal of material. 2. **personnel** — An activity for the reception, processing, training, assignment, and forwarding of personnel replacements. (JP 4-0)

design basis threat — The threat against which buildings and other structures must be protected and upon which the protective system's design is based. Also called **DBT.** (JP 3-07.2)

desired perception — In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective. (JP 3-13.4)

desired point of impact — A precise point, associated with a target and assigned as the impact point for a single unitary weapon to create a desired effect. Also called **DPI.** See also **aimpoint.** (JP 3-60)

detainee — Any person captured, detained, or otherwise under the control of Department of Defense personnel. (JP 3-63)

detainee collection point — A facility or other location where detainees are assembled for subsequent movement to a detainee holding area. Also called **DCP**. (JP 3-63)

detainee holding area — A facility or other location where detainees are administratively processed and provided custodial care pending disposition and subsequent release, transfer, or movement to a theater detention facility. Also called **DHA**. (JP 3-63)

detainee operations — A broad term that encompasses the capture, initial detention and screening, transportation, treatment and protection, housing, transfer, and release of the wide range of persons who could be categorized as detainees. (JP 3-63)

detection — 1. In tactical operations, the perception of an object of possible military interest but unconfirmed by recognition. 2. In surveillance, the determination and transmission by a surveillance system that an event has occurred. 3. In arms control, the first step in the process of ascertaining the occurrence of a violation of an arms control agreement. 4. In chemical, biological, radiological, and nuclear environments, the act of locating chemical, biological, radiological, and nuclear hazards by use of chemical, biological, radiological, and nuclear detectors or monitoring and/or survey teams. See also **hazard**. (JP 3-11)

deterrence — The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits. (JP 3-0)

deterrent options — A course of action, developed on the best economic, diplomatic, and military judgment, designed to dissuade an adversary from a current course of action or contemplated operations. (JP 5-0)

development assistance. Programs, projects, and activities carried out by the United States Agency for International Development that improve the lives of the citizens of developing countries while furthering United States foreign policy interests in expanding democracy and promoting free market economic growth. (JP 3-08)

direct action — Short-duration strikes and other small-scale offensive actions conducted as a special operation in hostile, denied, or diplomatically sensitive environments and which

employ specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets. Also called **DA.** See also **special operations; special operations forces.** (JP 3-05)

direct air support center — The principal air control agency of the United States Marine Corps air command and control system responsible for the direction and control of air operations directly supporting the ground combat element. Also called **DASC.** See also **Marine air command and control system; tactical air operations center.** (JP 3-09.3)

direct air support center (airborne) — An airborne aircraft equipped with the necessary staff personnel, communications, and operations facilities to function as a direct air support center. Also called **DASC(A).** See also **direct air support center.** (JP 3-09.3)

directed energy — An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. Also called **DE.** See also **directed-energy device; directed-energy weapon.** (JP 3-13.1)

directed-energy device — A system using directed energy primarily for a purpose other than as a weapon. See also **directed energy; directed-energy weapon.** (JP 3-13.1)

directed-energy warfare — Military action involving the use of directed-energy weapons, devices, and countermeasures. Also called **DEW.** See also **directed energy; directed-energy device; directed-energy weapon; electromagnetic spectrum; electronic warfare.** (JP 3-13.1)

directed-energy weapon — A weapon or system that uses directed energy to incapacitate, damage, or destroy enemy equipment, facilities, and/or personnel. See also **directed energy; directed-energy device.** (JP 3-13.1)

direct fire — Fire delivered on a target using the target itself as a point of aim for either the weapon or the director. (JP 3-09.3)

direction finding — A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. Also called **DF**. (JP 3-13.1)

directive authority for logistics — Combatant commander authority to issue directives to subordinate commanders to ensure the effective execution of approved operation plans, optimize the use or reallocation of available resources, and prevent or eliminate redundant facilities and/or overlapping functions among the Service component commands. Also called **DAFL.** See also **combatant command (command authority); logistics.** (JP 1)

direct liaison authorized — That authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command. Also called **DIRLAUTH.** (JP 1)

director of mobility forces — The designated agent for all air mobility issues in the area of responsibility or joint operations area, exercising coordinating authority between the air operations center (or appropriate theater command and control node), the 618 Air Operations Center (Tanker Airlift Control Center), and the joint deployment and distribution operation center or joint movement center, in order to expedite the resolution of air mobility issues. Also called **DIRMOBFOR.** See also **air operations center; coordinating authority.** (JP 3-17)

direct support — A mission requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance. Also called **DS.** See also **close support; general support; mission; mutual support; support.** (JP 3-09.3)

disarmament — The reduction of a military establishment to some level set by international agreement. See also **arms control agreement.** (JP 3-0)

disaster assistance response team — A team of specialists, trained in a variety of disaster relief skills, rapidly deployed to assist US embassies and United States Agency for International Development missions with the management of US Government response to disasters. Also called **DART.** See also **foreign disaster; foreign disaster relief.** (JP 3-08)

disease and nonbattle injury — All illnesses and injuries not resulting from enemy or terrorist action or caused by conflict. Also called **DNBI.** (JP 4-02)

disengagement — The act of geographically separating the forces of disputing parties. (JP 3-07.3)

dislocated civilian — A broad term primarily used by the Department of Defense that includes a displaced person, an evacuee, an internally displaced person, a migrant, a refugee, or a stateless person. Also called **DC.** See also **displaced person; evacuee; internally displaced person; migrant; refugee; stateless person.** (JP 3-29)

dispersal — Relocation of forces for the purpose of increasing survivability. (JP 3-01)

dispersal airfield — An airfield, military or civil, to which aircraft might move before H-hour on either a temporary duty or permanent change of station basis and be able to conduct operations. See also **airfield.** (JP 3-01)

dispersion — 1. The spreading or separating of troops, materiel, establishments, or activities, which are usually concentrated in limited areas to reduce vulnerability. (JP 5-0) 2. In chemical and biological operations, the dissemination of agents in liquid or aerosol form. (JP 3-41) 3. In airdrop operations, the scatter of personnel and/or cargo on the drop zone. (JP 3-17) 4. In naval control of shipping, the reberthing of a ship in the periphery of the port area or in the vicinity of the port for its own protection in order to minimize the risk of damage from attack. (JP 4-01.2)

displaced person — A broad term used to refer to internally and externally displaced persons collectively. See also **evacuee; refugee.** (JP 3-29)

display — In military deception, a static portrayal of an activity, force, or equipment intended to deceive the adversary's visual observation. (JP 3-13.4)

dissemination and integration — In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. See also **intelligence process.** (JP 2-01)

distant retirement area — In amphibious operations, the sea area located to seaward of the landing area to which assault ships may retire and operate in the event of adverse weather or to prevent concentration of ships in the landing area. See also **amphibious operation; landing area.** (JP 3-02)

distressed person — An individual who requires search and rescue assistance to remove he or she from life-threatening or isolating circumstances in a permissive environment. (JP 3-50)

distribution — 1. The arrangement of troops for any purpose, such as a battle, march, or maneuver. 2. A planned pattern of projectiles about a point. 3. A planned spread of fire to cover a desired frontage or depth. 4. An official delivery of anything, such as orders or supplies. 5. The operational process of synchronizing all elements of the logistic system to deliver the "right things" to the "right place" at the "right time" to support the geographic combatant commander. 6. The process of assigning military personnel to activities, units, or billets. (JP 4-0)

distribution manager — The executive agent for managing distribution with the combatant commander's area of responsibility. See also **area of responsibility; distribution.** (JP 4-09)

distribution pipeline — Continuum or channel through which the Department of Defense conducts distribution operations, representing the end-to-end flow of resources from supplier to consumer and, in some cases, back to the supplier in retrograde activities. See also **distribution.** (JP 4-09)

distribution plan — A reporting system comprising reports, updates, and information systems feeds that articulate the requirements of the theater distribution system to the strategic and operational resources assigned responsibility for support to the theater. See also **distribution; distribution system; theater distribution; theater distribution system.** (JP 4-09)

distribution point — A point at which supplies and/or ammunition, obtained from supporting supply points by a division or other unit, are broken down for distribution to subordinate units. (JP 4-09)

distribution system — That complex of facilities, installations, methods, and procedures designed to receive, store, maintain, distribute, and control the flow of military materiel between the point of receipt into the military system and the point of issue to using activities and units. (JP 4-09)

diversion — 1. The act of drawing the attention and forces of an enemy from the point of the principal operation; an attack, alarm, or feint that diverts attention. 2. A change made in a prescribed route for operational or tactical reasons that does not constitute a change of destination. 3. A rerouting of cargo or passengers to a new transshipment point or destination or on a different mode of transportation prior to arrival at ultimate destination. 4. In naval mine warfare, a route or channel bypassing a dangerous area by connecting one channel to another or it may branch from a channel and rejoin it on the other side of the danger. See also **demonstration.** (JP 3-03)

doctrine — Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. See also **multinational doctrine; joint doctrine**. (CJCSI 5120.02)

domestic emergencies — Civil defense emergencies, civil disturbances, major disasters, or natural disasters affecting the public welfare and occurring within the United States and its territories. See also **natural disaster.** (JP 3-27)

domestic intelligence — Intelligence relating to activities or conditions within the United States that threaten internal security and that might require the employment of troops; and intelligence relating to activities of individuals or agencies potentially or actually dangerous to the security of the Department of Defense. (JP 3-08)

dominant user — The Service or multinational partner who is the principal consumer of a particular common-user logistic supply or service within a joint or multinational operation and will normally act as the lead Service to provide this particular common-user logistic supply or service to other Service components, multinational partners, other governmental agencies, or nongovernmental agencies as directed by the combatant commander. See also **common-user logistics; lead Service or agency for common-user logistics.** (JP 4-0)

double agent — Agent in contact with two opposing intelligence services, only one of which is aware of the double contact or quasi-intelligence services. Also called **DA**. (JP 2-01.2)

double container — A 9.8125 feet by 8 feet by 8 feet (2991 millimeters by 2438 millimeters by 2438 millimeters) reusable International Standards Organization compliant double container, with double doors at both ends, used for the storage, transportation, and distribution of dry cargo. Also called **BICON.** (JP 4-09)

downgrade — To determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently

provided, coupled with a changing of the classification designation to reflect such a lower degree. (JP 3-08)

downloading — An operation that removes airborne weapons or stores from an aircraft. (JP 3-04)

drop altitude — The altitude above mean sea level at which airdrop is executed. (JP 3-17)

drop zone — A specific area upon which airborne troops, equipment, or supplies are airdropped. Also called **DZ.** (JP 3-17)

drug interdiction — A continuum of events focused on interrupting illegal drugs smuggled by air, sea, or land. See also **counterdrug operations.** (JP 3-07.4)

dual-capable aircraft — Allied and US fighter aircraft tasked and configured to perform either conventional or theater nuclear missions. Also called **DCA.**

dual-role tanker — An aircraft that can carry support personnel, supplies, and equipment for the deploying force while escorting and/or refueling combat aircraft to the area of responsibility. See also **air refueling.** (JP 3-17)

dummy — See **decoy**. (JP 3-13.4)

dwell time — 1. The length of time a target is expected to remain in one location. (JP 3-60) 2. The period of time between the release from involuntary active and the reporting date for a subsequent tour of active duty pursuant to Title 10, United States Code, Section 12302. Such time includes any voluntary active duty performed between two periods of involuntary active duty pursuant to Title 10, United States Code, Section 12302. (DODD 1235.10)

dynamic targeting — Targeting that prosecutes targets identified too late, or not selected for action in time to be included in deliberate targeting. (JP 3-60)

dynamic threat assessment — An intelligence assessment developed by the Defense Intelligence Agency that details the threat, capabilities, and intentions of adversaries in each of the priority plans in the Joint Strategic Capabilities Plan. Also called **DTA.** (JP 2-0)

E

earliest arrival date — A day, relative to C-day, that is specified as the earliest date when a unit, a resupply shipment, or replacement personnel can be accepted at a port of debarkation during a deployment. Also called **EAD.** See also **latest arrival date**. (JP 5-0)

early warning — Early notification of the launch or approach of unknown weapons or weapons carriers. Also called **EW.** See also **attack assessment.** (JP 3-01)

economy of force — The judicious employment and distribution of forces so as to expend the minimum essential combat power on secondary efforts in order to allocate the maximum possible combat power on primary efforts. (JP 3-0)

E-day — The day landing force personnel, supplies, and equipment begin to embark aboard amphibious warfare or commercial ships. (JP 3-02.1)

effect — 1. The physical or behavioral state of a system that results from an action, a set of actions, or another effect. 2. The result, outcome, or consequence of an action. 3. A change to a condition, behavior, or degree of freedom. (JP 3-0)

effective United States-controlled ships — United States-owned foreign flag ships that can be tasked by the Maritime Administration to support Department of Defense requirements when necessary. Also called **EUSCS.** (JP 4-01.2)

electro-explosive device — An explosive or pyrotechnic component that initiates an explosive, burning, electrical, or mechanical train and is activated by the application of electrical energy. Also called **EED.** (JP 3-04)

electromagnetic battle management — The dynamic monitoring, assessing, planning, and directing of joint electromagnetic spectrum operations in support of the commander's scheme of maneuver. Also called **EMBM.** (JP 3-13.1)

electromagnetic compatibility — The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response. Also called **EMC.** See also **electromagnetic spectrum; electromagnetic spectrum management; electronic warfare.** (JP 3-13.1)

electromagnetic environment — The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. Also called **EME.** (JP 3-13.1)

electromagnetic environmental effects — The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. Also called **E3.** (JP 3-13.1)

electromagnetic hardening — Action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy. See also **electronic warfare.** (JP 3-13.1)

electromagnetic interference — Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. Also called **EMI.** (JP 3-13.1)

electromagnetic intrusion — The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. See also **electronic warfare.** (JP 3-13.1)

electromagnetic jamming — The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. See also **electromagnetic spectrum; electromagnetic spectrum management; electronic warfare.** (JP 3-13.1)

electromagnetic operational environment — The background electromagnetic environment and the friendly, neutral, and adversarial electromagnetic order of battle within the electromagnetic area of influence associated with a given operational area. Also called **EMOE**. (JP 6-01)

electromagnetic pulse — The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. Also called **EMP.** See also **electromagnetic radiation.** (JP 3-13.1)

electromagnetic radiation — Radiation made up of oscillating electric and magnetic fields and propagated with the speed of light. (JP 6-01)

electromagnetic radiation hazards —Transmitter or antenna installation that generates or increases electromagnetic radiation in the vicinity of ordnance, personnel, or fueling operations in excess of established safe levels. Also called **EMR hazards or RADHAZ.** (JP 3-13.1)

electromagnetic spectrum — The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. See also **electronic warfare.** (JP 3-13.1)

electromagnetic spectrum control — The coordinated execution of joint electromagnetic spectrum operations with other lethal and nonlethal operations that enable freedom of action in the electromagnetic operational environment. Also called **EMSC.** (JP 3-13.1)

electromagnetic spectrum management — Planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. See also **electromagnetic spectrum.** (JP 6-01)

electromagnetic vulnerability — The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of electromagnetic environmental effects. Also called **EMV.** (JP 3-13.1)

electronic attack — Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called **EA.** See also **electronic protection; electronic warfare; electronic warfare support.** (JP 3-13.1)

electronic intelligence — Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called **ELINT.** See also **electronic warfare; foreign instrumentation signals intelligence; intelligence; signals intelligence.** (JP 3-13.1)

electronic masking —The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-13.1)

electronic probing — Intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices or systems. (JP 3-13.1)

electronic protection — Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Also called **EP.** See also **electronic attack, electronic warfare; electronic warfare support.** (JP 3-13.1)

electronic reconnaissance — The detection, location, identification, and evaluation of foreign electromagnetic radiations. See also **electromagnetic radiation; reconnaissance.** (JP 3-13.1)

electronics security — The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar. (JP 3-13.1)

electronic warfare — Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW.** See also **directed energy; electromagnetic spectrum; electronic attack; electronic protection; electronic warfare support.** (JP 3-13.1)

electronic warfare frequency deconfliction — Actions taken to integrate those frequencies used by electronic warfare systems into the overall frequency deconfliction process. See also **electronic warfare.** (JP 3-13.1)

electronic warfare reprogramming — The deliberate alteration or modification of electronic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. See also **electronic warfare.** (JP 3-13.1)

electronic warfare support — Division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Also called **ES.** See also **electronic attack; electronic protection; electronic warfare.** (JP 3-13.1)

electro-optical-infrared countermeasure — A device or technique employing electro-optical-infrared materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. Also called **EO-IR CM.** (JP 3-13.1)

element — An organization formed around a specific function within a designated directorate of a joint force commander's headquarters. (JP 3-33)

elevated causeway system — An elevated causeway pier that provides a means of delivering containers, certain vehicles, and bulk cargo ashore without the lighterage contending with the surf zone. Also called **ELCAS**. See also **causeway.** (JP 4-01.6)

elicitation — In intelligence usage, the acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation. (JP 2-0)

embarkation — The process of putting personnel and/or vehicles and their associated stores and equipment into ships and/or aircraft. (JP 3-02.1)

embarkation and tonnage table — A consolidated table showing personnel and cargo, by troop or naval units, loaded aboard a combat-loaded ship. (JP 3-02.1)

embarkation area — An area ashore, including a group of embarkation points, in which final preparations for embarkation are completed and through which assigned personnel and loads for craft and ships are called forward to embark. See also **mounting area.** (JP 3-02.1)

embarkation element — A temporary administrative formation of personnel with supplies and equipment embarking or to be embarked (combat loaded) aboard the ships of one transport element. (JP 3-02.1)

embarkation group — A temporary administrative formation of personnel with supplies and equipment embarking or to be embarked (combat loaded) aboard the ships of one transport element group. (JP 3-02.1)

embarkation officer — An officer on the staff of units of the landing force who advises the commander thereof on matters pertaining to embarkation planning and loading ships. See also **combat cargo officer.** (JP 3-02.1)

embarkation order — An order specifying dates, times, routes, loading diagrams, and methods of movement to shipside or aircraft for troops and their equipment. (JP 3-02.1)

embarkation organization — A temporary administrative formation of personnel with supplies and equipment embarking or to be embarked aboard ships. See also **embarkation team**. (JP 3-02.1)

embarkation phase — In amphibious operations, the phase that encompasses the orderly assembly of personnel and materiel and their subsequent loading aboard ships and/or aircraft in a sequence designed to meet the requirements of the landing force concept of operations ashore. (JP 3-02.1)

embarkation plans — The plans prepared by the landing force and appropriate subordinate commanders containing instructions and information concerning the organization for embarkation, assignment to shipping, supplies and equipment to be embarked, location and assignment of embarkation areas, control and communication arrangements, movement schedules and embarkation sequence, and additional pertinent instructions relating to the embarkation of the landing force. (JP 3-02)

embarkation team — A temporary administrative formation of all personnel with supplies and equipment embarking or to be embarked (combat loaded) aboard one ship. See also **embarkation organization**. (JP 3-02.1)

embarkation unit — A temporary administrative formation of personnel with supplies and equipment embarking or to be embarked (combat loaded) aboard the ships of one transport unit, which is dissolved upon completion of the embarkation. (JP 3-02.1)

emergency action committee — An organization established at a foreign service post by the chief of mission or principal officer for the purpose of directing and coordinating the post's response to contingencies. Also called **EAC.** (JP 3-68)

emergency authority — A Federal military commander's authority, in extraordinary emergency circumstances where prior authorization by the President is impossible and duly constituted local authorities are unable to control the situation, to engage temporarily in activities that are necessary to quell large-scale, unexpected civil disturbances because (1) such activities are necessary to prevent significant loss of life or wanton destruction of property and are necessary to restore governmental function and public order or (2) duly constituted Federal, state, or local authorities are unable or decline to provide adequate protection for Federal property or Federal governmental functions. (DODD 3025.18)

emergency-essential employee — A Department of Defense civilian employee whose assigned duties and responsibilities must be accomplished following the evacuation of non-essential personnel (including dependents) during a declared emergency or outbreak of war. See also **evacuation.** (JP 1-0)

emergency locator beacon — A generic term for all radio beacons used for emergency locating purposes. See also **personal locator beacon.** (JP 3-50)

emergency operations center — A temporary or permanent facility where the coordination of information and resources to support domestic incident management activities normally takes place. Also called **EOC.** (JP 3-41)

emergency preparedness — Measures taken in advance of an emergency to reduce the loss of life and property and to protect a nation's institutions from all types of hazards through a comprehensive emergency management program of preparedness, mitigation, response, and recovery. Also called **EP.** (JP 3-28)

emergency preparedness liaison officer — A senior reserve officer who represents their Service at the appropriate joint field office conducting planning and coordination responsibilities in support of civil authorities. Also called **EPLO.** (JP 3-28)

emergency repair — The least amount of immediate repair to damaged facilities necessary for the facilities to support the mission. See also **facility substitutes.** (JP 3-34)

emergency support functions — A grouping of government and certain private-sector capabilities into an organizational structure to provide the support, resources, program implementation, and services that are most likely to be needed to save lives, protect property and the environment, restore essential services and critical infrastructure, and help victims and communities return to normal, when feasible, following domestic incidents. Also called **ESFs.** (JP 3-28)

emission control — The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan. Also called **EMCON.** See also **electronic warfare.** (JP 3-13.1)

emission security — The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. See also **communications security.** (JP 6-0)

employment — The strategic, operational, or tactical use of forces. (JP 5-0)

end evening civil twilight — The point in time when the sun has dropped 6 degrees beneath the western horizon, and is the instant at which there is no longer sufficient light to see objects with the unaided eye. Also called **EECT.** (JP 2-01.3)

end item — A final combination of end products, component parts, and/or materials that is ready for its intended use. (JP 4-02)

end of evening nautical twilight — The point in time when the sun has dropped 12 degrees below the western horizon, and is the instant of last available daylight for the visual control of limited military operations. Also called **EENT**. (JP 2-01.3)

end state — The set of required conditions that defines achievement of the commander's objectives. (JP 3-0)

end-to-end — A term that describes joint distribution operations boundaries, which begin at the point of origin and terminate at the geographic combatant commander's designated point of need within a desired operational area, including the return of forces and materiel. (JP 4-09)

enemy combatant — In general, a person engaged in hostilities against the United States or its coalition partners during an armed conflict. Also called **EC.** (DODD 2310.01E)

engage — 1. In air defense, a fire control order used to direct or authorize units and/or weapon systems to fire on a designated target. See also **cease engagement; hold fire.** (JP 3-01) 2. To bring the enemy under fire. (JP 3-09.3)

engagement — 1. In air defense, an attack with guns or air-to-air missiles by an interceptor aircraft, or the launch of an air defense missile by air defense artillery and the missile's subsequent travel to intercept. (JP 3-01) 2. A tactical conflict, usually between opposing lower echelons maneuver forces. See also **battle; campaign.** (JP 3-0)

engagement authority — An authority vested with a joint force commander that may be delegated to a subordinate commander, that permits an engagement decision. (JP 3-01)

engineer support plan — An appendix to the logistics annex or separate annex of an operation plan that identifies the minimum essential engineering services and construction requirements required to support the commitment of military forces. Also called **ESP.** See also **operation plan.** (JP 3-34)

en route care — Continuation of the provision of care during movement (evacuation) between the health service support capabilities in the roles of care, without clinically compromising the patient's condition. See also **evacuation.** (JP 4-02)

enterprise force structure — The digitized hierarchical representation of Department of Defense organizations, documented in accordance with the standardized precepts of the Organizational and Force Structure Construct, generated and shared from .org servers for Department of Defense-wide integration and use. (DODI 8260.03)

entity — Within the context of targeting, a term used to describe facilities, organizations, individuals, equipment, or virtual (nontangible) things. (JP 3-60)

environmental baseline survey — A multi-disciplinary site survey conducted prior to or in the initial stage of an operational deployment. Also called **EBS.** See also **general engineering.** (JP 3-34)

environmental considerations — The spectrum of environmental media, resources, or programs that may affect the planning and execution of military operations. (JP 3-34)

equipment — In logistics, all nonexpendable items needed to outfit or equip an individual or organization. See also **component; supplies.** (JP 4-0)

escapee — Any person who has been physically captured by the enemy and succeeds in getting free. (JP 3-50)

escort — A member of the Armed Forces assigned to accompany, assist, or guide an individual or group, e.g., an escort officer. (JP 4-06)

espionage — The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation. Espionage is a violation of Title 18 United States Code, Sections 792-798 and Article 106, *Uniform Code of Military Justice*. See also **counterintelligence.** (JP 2-01.2)

essential care — Medical treatment provided to manage the casualty throughout the roles of care, which includes all care and treatment to either return the patient to duty (within the theater evacuation policy), or begin initial treatment required for optimization of outcome, and/or stabilization to ensure the patient can tolerate evacuation. See also **en route care; first responder; forward resuscitative care; theater.** (JP 4-02)

essential elements of friendly information — Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. Also called **EEFI.** (JP 2-01)

essential elements of information — The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. Also called **EEIs.** (JP 2-0)

essential task — A specified or implied task that an organization must perform to accomplish the mission that is typically included in the mission statement. See also **implied task; specified task.** (JP 5-0)

establishing directive — An order issued to specify the purpose of the support relationship. (JP 3-02)

estimate — 1. An analysis of a foreign situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and the prospective results of the various actions that might be taken. 2. An appraisal of the capabilities, vulnerabilities, and potential courses of action of a foreign nation or combination of nations in consequence of a specific national plan, policy, decision, or contemplated course of action. 3. An analysis of an actual or contemplated clandestine operation in relation to the situation in which it is or would be conducted in order to identify and appraise such factors as available as well as needed assets and potential obstacles, accomplishments, and consequences. See also **intelligence estimate.** (JP 2-01)

estimative intelligence — Intelligence that identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations. (JP 2-0)

evacuation — 1. Removal of a patient by any of a variety of transport means from a theater of military operation, or between health services capabilities, for the purpose of preventing further illness or injury, providing additional care, or providing disposition of patients from the military health care system. (JP 4-02) 2. The clearance of personnel, animals, or materiel from a given locality. (JP 3-68) 3. The controlled process of collecting, classifying, and shipping unserviceable or abandoned materiel, United States or foreign, to appropriate reclamation, maintenance, technical intelligence, or disposal facilities. (JP 4-09) 4. The ordered or authorized departure of noncombatant evacuees from a specific area to another in the same or different countries by Department of State, Department of Defense, or appropriate military commander. See also **evacuee; noncombatant evacuation operation.** (JP 3-68)

evacuee — A civilian removed from a place of residence by military direction for reasons of personal security or the requirements of the military situation. See also **displaced person; refugee.** (JP 3-57)

evader — Any person isolated in hostile or unfriendly territory who eludes capture. (JP 3-50)

evaluation — In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (JP 2-01)

evaluation agent — The command or agency designated in the evaluation directive to be responsible for the planning, coordination, and conduct of the required evaluation of a joint test publication. Also called **EA.** See also **joint doctrine; joint test publication.** (CJCSM 5120.01)

evaluation and feedback — In intelligence usage, continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. See **intelligence process.** (JP 2-01)

evasion — The process whereby isolated personnel avoid capture with the goal of successfully returning to areas under friendly control. (JP 3-50)

evasion aid — In personnel recovery, any piece of information or equipment designed to assist an individual in avoiding capture. See also **blood chit; evasion; evasion chart; pointee-talkee; recovery; recovery operations.** (JP 3-50)

evasion chart — A special map or chart designed as an evasion aid. Also called **EVC.** See also **evasion; evasion aid.** (JP 3-50)

evasion plan of action — A course of action, developed prior to executing a combat mission, that is intended to improve a potential isolated person's chances of successful evasion and recovery by providing the recovery forces with an additional source of information that can increase the predictability of the evader's action and movement. Also called **EPA.** See also **course of action; evader; evasion.** (JP 3-50)

event matrix — A cross-referenced description of the indicators and activity expected to occur in each named area of interest. See also **activity; area of interest; indicator.** (JP 2-01.3)

event template — A guide for collection planning that depicts the named areas of interest where activity, or its lack of activity, will indicate which course of action the adversary has adopted. See also **activity; area of interest; collection planning; course of action.** (JP 2-01.3)

exclusion zone — A zone established by a sanctioning body to prohibit specific activities in a specific geographic area in order to persuade nations or groups to modify their behavior

to meet the desires of the sanctioning body or face continued imposition of sanctions, or use or threat of force. (JP 3-0)

exclusive economic zone — A maritime zone adjacent to the territorial sea that may not extend beyond 200 nautical miles from the baselines from which the breadth of the territorial sea is measured. Also called **EEZ**. (JP 3-15)

execute order — 1. An order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to implement a decision by the President to initiate military operations. 2. An order to initiate military operations as directed. Also called **EXORD.** (JP 5-0)

execution planning — The Adaptive Planning and Execution system translation of an approved course of action into an executable plan of action through the preparation of a complete operation plan or operation order. Also called **EP.** See also **Joint Operation Planning and Execution System.** (JP 5-0)

executive agent — A term used to indicate a delegation of authority by the Secretary of Defense or Deputy Secretary of Defense to a subordinate to act on behalf of the Secretary of Defense. Also called **EA.** (JP 1)

exercise — A military maneuver or simulated wartime operation involving planning, preparation, and execution that is carried out for the purpose of training and evaluation. See also **command post exercise; maneuver.** (JP 3-34)

exfiltration — The removal of personnel or units from areas under enemy control by stealth, deception, surprise, or clandestine means. See also **special operations; unconventional warfare.** (JP 3-50)

expeditionary force — An armed force organized to accomplish a specific objective in a foreign country. (JP 3-0)

expendable supplies — Supplies that are consumed in use, such as ammunition, paint, fuel, cleaning and preserving materials, surgical dressings, drugs, medicines, etc., or that lose their identity, such as spare parts, etc., and may be dropped from stock record accounts when it is issued or used. (JP 4-02)

exploitation — 1. Taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already created. 2. Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. 3. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. See also **attack.** (JP 2-01.3)

explosive cargo — Cargo such as artillery ammunition, bombs, depth charges, demolition material, rockets, and missiles. (JP 4-01.5)

explosive hazard — Any hazard containing an explosive component to include unexploded explosive ordnance (including land mines), booby traps (some booby traps are nonexplosive), improvised explosive devices (which are an improvised type of booby trap), captured enemy ammunition, and bulk explosives. Also called **EH.** (JP 3-15)

explosive hazard incident — The suspected or detected presence of unexploded or damaged explosive ordnance that constitutes a hazard to operations, installations, personnel, or material. Not included in this definition are the accidental arming or other conditions that develop during the manufacture of high explosive material, technical service assembly operations, or the laying of mines and demolition charges. (JP 3-15.1)

explosive ordnance — All munitions containing explosives, nuclear fission or fusion materials, and biological and chemical agents. (JP 3-34)

explosive ordnance disposal — The detection, identification, on-site evaluation, rendering safe, recovery, and final disposal of unexploded explosive ordnance. Also called **EOD.** (JP 3-34)

explosive ordnance disposal unit — Personnel with special training and equipment who render explosive ordnance safe, make intelligence reports on such ordnance, and supervise the safe removal thereof. (JP 3-34)

exposure dose — The amount of radiation, as measured in roentgen, at a given point in relation to its ability to produce ionization. (JP 3-41)

external audience — In public affairs, all people who are not United States military members, Department of Defense civilian employees, and their immediate families. See also **internal audience; public.** (JP 3-61)

external support contract — Contract awarded by contracting organizations whose contracting authority does not derive directly from the theater support contracting head(s) of contracting activity or from systems support contracting authorities. See also **systems support contract; theater support contract.** (JP 4-10)

F

fabricator — An individual or group who, usually without genuine resources, invents or inflates information for personal or political gain or political purposes. (JP 2-01.2)

facility — A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land. (JP 3-34)

facility substitutes — Items such as tents and prepackaged structures requisitioned through the supply system that may be used to substitute for constructed facilities. (JP 3-34)

family readiness — The state of being prepared to effectively navigate the challenges of daily living experienced in the unique context of military service, to include: mobility and financial readiness, mobilization and deployment readiness, and personal and family life readiness. (DODI 1342.22)

feasibility — The joint operation plan review criterion for assessing whether the assigned mission can be accomplished using available resources within the time contemplated by the plan. See also **acceptability; adequacy.** (JP 5-0)

feasibility assessment — A basic target analysis that provides an initial determination of the viability of a proposed target for special operations forces employment. Also called **FA.** (JP 3-05)

federal service — A term applied to National Guard members and units when called to active duty to serve the United States Government under Article I, Section 8 and Article II, Section 2 of the Constitution and Title 10, United States Code, Sections 12401 to 12408. See also **active duty; Reserve Component.** (JP 4-05)

feint — In military deception, an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action. (JP 3-13.4)

field artillery — Equipment, supplies, ammunition, and personnel involved in the use of cannon, rocket, or surface-to-surface missile launchers. Also called **FA.** (JP 3-09)

fighter engagement zone — In air defense, that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with fighter aircraft. Also called **FEZ.** (JP 3-01)

fighter escort — An offensive counterair operation providing dedicated protection sorties by air-to-air capable fighters in support of other offensive air and air support missions over enemy territory, or in a defensive counterair role to protect high value airborne assets. (JP 3-01)

fighter sweep — An offensive mission by fighter aircraft to seek out and destroy enemy aircraft or targets of opportunity in a designated area. (JP 3-01)

final governing standards — A comprehensive set of country-specific substantive environmental provisions, typically technical limitations on effluent, discharges, etc., or a specific management practice. Also called **FGSs.** (JP 3-34)

final protective fire — An immediately available prearranged barrier of fire designed to impede enemy movement across defensive lines or areas. Also called **FPF**. (JP 3-09.3)

finance support — A financial management function to provide financial advice and recommendations, pay support, disbursing support, establishment of local depository accounts, essential accounting support, and support of the procurement process. See also **financial management.** (JP 1-06)

financial management — The combination of the two core functions of resource management and finance support. Also called **FM.** See also **finance support; resource management.** (JP 1-06)

fire direction center — That element of a command post, consisting of gunnery and communications personnel and equipment, by means of which the commander exercises fire direction and/or fire control. Also called **FDC**. (JP 3-09.3)

fires — The use of weapon systems or other actions to create specific lethal or nonlethal effects on a target. (JP 3-09)

fire support — Fires that directly support land, maritime, amphibious, and special operations forces to engage enemy forces, combat formations, and facilities in pursuit of tactical and operational objectives. See also **fires.** (JP 3-09)

fire support area — An appropriate maneuver area assigned to fire support ships by the naval force commander from which they can deliver gunfire support to an amphibious operation. Also called **FSA.** See also **amphibious operation; fire support.** (JP 3-09)

fire support coordination — The planning and executing of fire so that targets are adequately covered by a suitable weapon or group of weapons. (JP 3-09)

fire support coordination center — A single location in which are centralized communications facilities and personnel incident to the coordination of all forms of fire support for Marine forces. Also called **FSCC.** See also **fire support; fire support coordination; support; supporting arms coordination center.** (JP 3-09)

fire support coordination line — A fire support coordination measure established by the land or amphibious force commander to support common objectives within an area of operation; beyond which all fires must be coordinated with affected commanders prior

to engagement, and short of the line, all fires must be coordinated with the establishing commander prior to engagement. Also called **FSCL.** See also **fires; fire support.** (JP 3-09)

fire support coordination measure — A measure employed by commanders to facilitate the rapid engagement of targets and simultaneously provide safeguards for friendly forces. Also called **FSCM.** See also **fire support coordination.** (JP 3-0)

fire support coordinator — 1. The officer in charge of the fire support coordination center. Also called **FSC.** 2. The brigade combat team's organic fires battalion commander; if a fires brigade is designated as the division force field artillery headquarters, the fires brigade commander is the division's fire support coordinator and is assisted by the chief of fires who then serves as the deputy fire support coordinator during the period the force field artillery headquarters is in effect. Also called **FSCOORD.** (JP 3-09)

fire support element — That section of the tactical operations center at every echelon above company responsible for targeting coordination and for integrating fires under the control or in support of the force. Also called **FSE.** Also called **fire cell (FC) within the United States Army.** See also **fire support; force; support.** (JP 3-09)

fire support officer — The field artillery officer from the operational to tactical level responsible for advising the supported commander or assisting the senior fires officer of the organization on fires functions and fire support. Also called **FSO.** See also **field artillery; fire support; support.** (JP 3-09)

fire support station — An exact location at sea within a fire support area from which a fire support ship delivers fire. Also called **FSS.** (JP 3-02)

fire support team — A field artillery team provided for each maneuver company/troop and selected units to plan and coordinate all supporting fires available to the unit, including mortars, field artillery, naval surface fire support, and close air support integration. Also called **FIST.** See also **close air support; field artillery; fire support; support.** (JP 3-09.3)

first responder — A primary health care provider who provides immediate clinical care and stabilization in preparation for evacuation to the next health service support capability in the roles of care, and treats Service members for common acute minor illnesses. See also **essential care; evacuation.** (JP 4-02)

first responder care — The health care capability that provides immediate clinical care and stabilization to the patient in preparation for evacuation to the next health service support capability in the continuum of care. (JP 4-02)

fixed port — Terminals with an improved network of cargo-handling facilities designed for the transfer of freight. See also **maritime terminal.** (JP 4-01.5)

fixed price contract — A type of contract that generally provides for a firm price or, under appropriate circumstances, may provide for an adjustable price for the supplies or services being procured. (JP 4-10)

flame field expedients — Simple, handmade devices used to produce flame or illumination. Also called **FFE.** (JP 3-15)

flash burn — A burn caused by excessive exposure (of bare skin) to thermal radiation. (JP 3-41)

flatrack — Portable, open-topped, open-sided units that fit into existing below-deck container cell guides and provide a capability for container ships to carry oversized cargo and wheeled and tracked vehicles. (JP 4-09)

fleet — An organization of ships, aircraft, Marine forces, and shore-based fleet activities all under a commander who may exercise operational as well as administrative control. See also **numbered fleet.** (JP 3-02.1)

Fleet Marine Force — A balanced force of combined arms comprising land, air, and service elements of the United States Marine Corps, which is an integral part of a United States fleet and has the status of a type command. Also called **FMF.** (JP 4-02)

flexible deterrent option — A planning construct intended to facilitate early decision making by developing a wide range of interrelated responses that begin with deterrent-oriented actions carefully tailored to produce a desired effect. Also called **FDO.** See also **deterrent options.** (JP 5-0)

flexible response — The capability of military forces for effective reaction to any enemy threat or attack with actions appropriate and adaptable to the circumstances existing. (JP 5-0)

flight — 1. In Navy and Marine Corps usage, a specified group of aircraft usually engaged in a common mission. 2. The basic tactical unit in the Air Force, consisting of four or more aircraft in two or more elements. 3. A single aircraft airborne on a nonoperational mission. (JP 3-30)

flight deck — 1. In certain airplanes, an elevated compartment occupied by the crew for operating the airplane in flight. 2. The upper deck of an aircraft carrier that serves as a runway. The deck of an air-capable ship, amphibious aviation assault ship, or aircraft carrier used to launch and recover aircraft. (JP 3-04)

flight deck officer — Officer responsible for the safe movement of aircraft on or about the flight deck of an aviation-capable ship. Also called **FDO.** (JP 3-04)

flight quarters — A ship configuration that assigns and stations personnel at critical positions to conduct safe flight operations. (JP 3-04)

floating craft company — A company-sized unit made up of various watercraft teams such as tugs, barges, and barge cranes. (JP 4-01.6)

floating dump — Emergency supplies preloaded in landing craft, amphibious vehicles, or in landing ships that are located in the vicinity of the appropriate control officer, who directs their landing as requested by the troop commander concerned. (JP 3-02)

fly-in echelon — Airlifted forces and equipment to include flight ferry aircraft and aviation support equipment needed to support operations; typically associated with the use of pre-positioned assets. Also called **FIE**. (JP 3-02.1)

follow-up — In amphibious operations, the reinforcements and stores carried on ships and aircraft (not originally part of the amphibious force) that are off-loaded after the assault and assault follow-on echelons have been landed. See also **amphibious operation; assault; assault follow-on echelon.** (JP 3-02)

follow-up shipping — Ships not originally a part of the amphibious task force but which deliver troops and supplies to the objective area after the action phase has begun. (JP 3-02)

footprint — 1. The area on the surface of the earth within a satellite's transmitter or sensor field of view. 2. The amount of personnel, spares, resources, and capabilities physically present and occupying space at a deployed location. (JP 4-01.5)

force — 1. An aggregation of military personnel, weapon systems, equipment, and necessary support, or combination thereof. 2. A major subdivision of a fleet. (JP 1)

force/activity designator — Number used in conjunction with urgency of need designators to establish a matrix of priorities used for supply requisitions. Also called **F/AD.** See also **force.** (JP 4-09)

force beddown — The provision of expedient facilities for troop support to provide a platform for the projection of force. See also **facility substitutes.** (JP 3-34)

force closure — The point in time when a supported joint force commander determines that sufficient personnel and equipment resources are in the assigned operational area to carry out assigned tasks. See also **closure; force.** (JP 3-35)

force health protection — Measures to promote, improve, or conserve the behavioral and physical well-being of Service members to enable a healthy and fit force, prevent injury and illness, and protect the force from health hazards. Also called **FHP.** See also **force; protection.** (JP 4-02)

force management — An organizing construct of processes, policies, organizational information, and tools that informs senior leader decision making on the global joint sourcing of the defense strategy. (DODI 8260.03)

force module — A grouping of combat, combat support, and combat service support forces, with their accompanying supplies and the required nonunit resupply and personnel necessary to sustain forces for a minimum of 30 days. Also called **FM.** (JP 4-01.5)

force planning — 1. Planning associated with the creation and maintenance of military capabilities by the Military Departments, Services, and US Special Operations Command. 2. In the Joint Operation Planning and Execution System, the planning conducted by the supported combatant command and its components to determine required force capabilities to accomplish an assigned mission. (JP 5-0)

force projection — The ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations. See also **force.** (JP 3-0)

force protection — Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Also called **FP.** See also **force; force protection condition; protection.** (JP 3-0)

force protection condition — A Chairman of the Joint Chiefs of Staff-approved standard for identification of and recommended responses to terrorist threats against United States personnel and facilities. Also called **FPCON.** See also **antiterrorism; force protection.** (JP 3-07.2)

force protection detachment — A counterintelligence element that provides counterintelligence support to transiting and assigned ships, personnel, and aircraft in regions of elevated threat. Also called **FPD**. (JP 2-01.2)

force protection working group — Cross-functional working group whose purpose is to conduct risk assessment and risk management and to recommend mitigating measures to the commander. Also called **FPWG.** (JP 3-10)

force requirement number — An alphanumeric code used to uniquely identify force entries in a given operation plan time-phased force and deployment data. Also called **FRN.** (JP 3-35)

force sequencing — The phased introduction of forces into and out of the operational area. (JP 3-68)

force sourcing — The identification of the actual units, their origins, ports of embarkation, and movement characteristics to satisfy the time-phased force requirements of a supported commander. (JP 5-0)

force structure — The composition of Department of Defense organizations, both military and civilian, that comprise and support United States defense forces as specified by the National Defense Authorization Acts of current and applicable previous years, and defines the organizational hierarchy through which leadership authorities are exercised. (DODI 8260.03)

force tracking — The process of gathering and maintaining information on the location, status, and predicted movement of each element of a unit including the unit's command element, personnel, and unit-related supplies and equipment while in transit to the specified operational area. (JP 3-35)

force visibility — The current and accurate status of forces; their current mission; future missions; location; mission priority; and readiness status. (JP 3-35)

forcible entry — Seizing and holding of a military lodgment in the face of armed opposition. See also **lodgment.** (JP 3-18)

foreign assistance — Assistance to foreign nations ranging from the sale of military equipment to donations of food and medical supplies to aid survivors of natural and man-made disasters; that may be provided through development assistance, humanitarian assistance, and security assistance. See also **domestic emergencies; foreign disaster; foreign humanitarian assistance; security assistance.** (JP 3-29)

foreign consequence management — United States Government activity that assists friends and allies in responding to the effects from an intentional or accidental chemical, biological, radiological, or nuclear incident on foreign territory in order to maximize preservation of life. Also called **FCM.** (JP 3-41)

foreign disaster — A calamitous situation or event that occurs naturally or through human activities, which threatens or inflicts human suffering on a scale that may warrant emergency relief assistance from the United States Government or from foreign partners. See also **foreign disaster relief.** (JP 3-29)

foreign disaster relief — Assistance that can be used immediately to alleviate the suffering of foreign disaster victims that normally includes services and commodities as well as the rescue and evacuation of victims; the provision and transportation of food, water, clothing, medicines, beds, bedding, and temporary shelter; the furnishing of medical equipment, medical and technical personnel; and making repairs to essential services. Also called **FDR.** See also **foreign disaster.** (JP 3-29)

foreign humanitarian assistance — Department of Defense activities conducted outside the United States and its territories to directly relieve or reduce human suffering, disease, hunger, or privation. Also called **FHA.** See also **foreign assistance.** (JP 3-29)

foreign instrumentation signals intelligence — A subcategory of signals intelligence, consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. Also called **FISINT**. See also **signals intelligence.** (JP 2-01)

foreign intelligence — Information relating to capabilities, intentions, and activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called **FI**. See also **intelligence.** (JP 2-0)

foreign intelligence entity — Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire US information, block or impair US intelligence collection, influence US policy, or disrupts US systems and programs. The term includes foreign intelligence and security services and international terrorists. Also called **FIE**. (JP 2-01.2)

foreign internal defense — Participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security. Also called **FID.** (JP 3-22)

foreign military intelligence collection activities — Entails the overt debriefing, by trained human intelligence personnel, of all US persons employed by the Department of Defense who have access to information of potential national security value. Also called **FORMICA**. (JP 2-01.2)

foreign military sales — That portion of United States security assistance authorized by the Foreign Assistance Act of 1961, as amended, and the Arms Export Control Act of 1976, as amended. This assistance differs from the Military Assistance Program and the International Military Education and Training Program in that the recipient provides reimbursement for defense articles and services transferred. Also called **FMS.** (JP 4-08)

foreign national — Any person other than a US citizen, US permanent or temporary legal resident alien, or person in US custody. (JP 1-0)

foreign nation support — Civil and/or military assistance rendered to a nation when operating outside its national boundaries during military operations based on agreements mutually concluded between nations or on behalf of intergovernmental organizations. Also called **FNS.** See also **host-nation support.** (JP 1-06)

foreign object damage — Rags, pieces of paper, line, articles of clothing, nuts, bolts, or tools that, when misplaced or caught by air currents normally found around aircraft operations (jet blast, rotor or prop wash, engine intake), cause damage to aircraft systems or weapons or injury to personnel. Also called **FOD.** (JP 3-04)

foreign service national — Foreign nationals who provide clerical, administrative, technical, fiscal, and other support at foreign service posts abroad and are not citizens of the United States. Also called **FSN.** (JP 3-68)

forensic-enabled intelligence — The intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest. Also called **FEI.** (JP 2-0)

formerly restricted data — Information removed from the restricted data category upon a joint determination by the Department of Energy (or antecedent agencies) and Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. (Section 142d, Atomic Energy Act of 1954, as amended.) (JP 2-01)

forward air controller — An officer (aviator/pilot) member of the tactical air control party who, from a forward ground or airborne position, controls aircraft in close air support of ground troops. Also called **FAC.** See also **close air support.** (JP 3-09.3)

forward air controller (airborne) — A specifically trained and qualified aviation officer, normally an airborne extension of the tactical air control party, who exercises control from the air of aircraft engaged in close air support of ground troops. Also called **FAC(A).** (JP 3-09.3)

forward area — An area in proximity to combat. (JP 4-02)

forward arming and refueling point — A temporary facility, organized, equipped, and deployed to provide fuel and ammunition necessary for the employment of aviation maneuver units in combat. Also called **FARP**. (JP 3-09.3)

forward aviation combat engineering — A mobility operation in which engineers perform tasks in support of forward aviation ground facilities. Also called **FACE.** See also **combat engineering; reconnaissance.** (JP 3-34)

forward edge of the battle area — The foremost limits of a series of areas in which ground combat units are deployed, excluding the areas in which the covering or screening forces are operating, designated to coordinate fire support, the positioning of forces, or the maneuver of units. Also called **FEBA.** (JP 3-09.3)

forward line of own troops — A line that indicates the most forward positions of friendly forces in any kind of military operation at a specific time. Also called **FLOT.** (JP 3-03)

forward-looking infrared — An airborne, electro-optical thermal imaging device that detects far-infrared energy, converts the energy into an electronic signal, and provides a visible image for day or night viewing. Also called **FLIR.** (JP 3-09.3)

forward observer — An observer operating with front line troops trained to adjust ground or naval gunfire and pass back battlefield information. Also called **FO.** See also **forward air controller; spotter.** (JP 3-09)

forward operating base — An airfield used to support tactical operations without establishing full support facilities. Also called **FOB.** (JP 3-09.3)

forward operating site — A scaleable location outside the United States and US territories intended for rotational use by operating forces. Such expandable "warm facilities" may be maintained with a limited US military support presence and possibly pre-positioned equipment. Forward operating sites support rotational rather than permanently stationed forces and are a focus for bilateral and regional training. Also called **FOS.** See also **cooperative security location; main operating base.** (CJCS CM-0007-05)

forward presence — Maintaining forward-deployed or stationed forces overseas to demonstrate national resolve, strengthen alliances, dissuade potential adversaries, and enhance the ability to respond quickly to contingencies. (JP 3-32)

forward resuscitative care — Care provided as close to the point of injury as possible based on current operational requirements to attain stabilization, achieve the most efficient use of life-and-limb saving medical treatment, and provide essential care so the patient can tolerate evacuation, which is known as Role 2 care in the North Atlantic Treaty Organization doctrine. Also called **FRC.** See **also essential care; evacuation; medical treatment facility.** (JP 4-02)

foundation geospatial-intelligence data — The base underlying data to provide context and a framework for display and visualization of the environment to support analysis operations and intelligence, which consists of: features; elevation; controlled imagery; geodetic sciences; geographic names and boundaries; aeronautical, maritime and human geography. (JP 2-03)

463L system — A material handling system that consists of military and civilian aircraft cargo restraint rail systems, aircraft pallets, nets, tie down, coupling devices, facilities, handling equipment, procedures, and other components designed to efficiently accomplish the air logistics and aerial delivery mission. (JP 4-09)

fragmentary order — An abbreviated form of an operation order issued as needed after an operation order to change or modify that order or to execute a branch or sequel to that order. Also called **FRAGORD.** (JP 5-0)

freedom of navigation operations — Operations conducted to demonstrate US navigation, overflight, and related interests on, or under, and over the seas. (JP 3-0)

free drop — The dropping of equipment or supplies from an aircraft without the use of parachutes. See also **airdrop; air movement; free fall; high velocity drop; low velocity drop.** (JP 3-17)

free fall — A parachute maneuver in which the parachute is manually activated at the discretion of the jumper or automatically at a preset altitude. See also **airdrop; air movement; free drop; high velocity drop; low velocity drop.** (JP 3-17)

free-fire area — A specific area into which any weapon system may fire without additional coordination with the establishing headquarters. Also called **FFA.** (JP 3-09)

free mail — Correspondence of a personal nature that weighs less than 11 ounces, to include audio and video recording tapes, from a member of the Armed Forces or designated civilian, mailed postage free from a Secretary of Defense approved free mail zone. (JP 1-0)

frequency deconfliction — A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management. See also **electromagnetic spectrum; electromagnetic spectrum management; electronic warfare.** (JP 3-13.1)

friendly — A contact positively identified as friendly. (JP 3-01)

friendly force information requirement — Information the commander and staff need to understand the status of friendly force and supporting capabilities. Also called **FFIR.** (JP 3-0)

friendly force tracking — The process of fixing, observing, and reporting the location and movement of friendly forces. Also called **FFT**. (JP 3-09)

frustrated cargo — Any shipment of supplies and/or equipment which, while en route to destination, is stopped prior to receipt and for which further disposition instructions must be obtained. (JP 4-01.5)

full mobilization — Expansion of the active Armed Forces resulting from action by Congress and the President to mobilize for the duration of the emergency plus six months all Reserve Component units and individuals in the existing approved force structure, as well as all retired military personnel, and the resources needed for their support to meet the requirements of a war or other national emergency involving an external threat to the national security. (JP 4-05)

full-spectrum superiority — The cumulative effect of dominance in the air, land, maritime, and space domains and information environment (which includes cyberspace) that

permits the conduct of joint operations without effective opposition or prohibitive interference. (JP 3-0)

function — The broad, general, and enduring role for which an organization is designed, equipped, and trained. (JP 1)

functional component command — A command normally, but not necessarily, composed of forces of two or more Military Departments which may be established across the range of military operations to perform particular operational missions that may be of short duration or may extend over a period of time. See also **component; Service component command.** (JP 1)

functional damage assessment — The estimate of the effect of military force to degrade or destroy the functional or operational capability of the target to perform its intended mission and on the level of success in achieving operational objectives established against the target. See also **damage assessment; target.** (JP 3-60)

fusion — In intelligence usage, the process of managing information to conduct all-source analysis and derive a complete assessment of activity. (JP 2-0)

G

general agency agreement — A contract between the Maritime Administration and a steamship company which, as general agent, exercises administrative control over a government-owned ship for employment by the Military Sealift Command. Also called **GAA**. See also **Military Sealift Command.** (JP 3-02.1)

general cargo — Cargo that is suitable for loading in general, nonspecialized stowage areas or standard shipping containers; e.g., boxes, barrels, bales, crates, packages, bundles, and pallets. (JP 4-09)

general engineering — Those engineering capabilities and activities, other than combat engineering, that provide infrastructure and modify, maintain, or protect the physical environment. Also called **GE.** (JP 3-34)

general military intelligence — Intelligence concerning the military capabilities of foreign countries or organizations, or topics affecting potential United States or multinational military operations. Also called **GMI.** See also **intelligence.** (JP 2-0)

general support — 1. That support which is given to the supported force as a whole and not to any particular subdivision thereof. See also **close support; direct support; mutual support; support.** 2. A tactical artillery mission. Also called **GS.** See also **direct support; general support-reinforcing.** (JP 3-09.3)

general support-reinforcing — The artillery mission of supporting the force as a whole and of providing reinforcing fires for other artillery units. Also called **GSR.** (JP 3-09.3)

general unloading period — In amphibious operations, that part of the ship-to-shore movement in which unloading is primarily logistic in character, and emphasizes speed and volume of unloading operations. See also **initial unloading period.** (JP 3-02)

geographic coordinates — The quantities of latitude and longitude which define the position of a point on the surface of the Earth with respect to the reference spheroid. (JP 2-03)

geospatial engineering — Those engineering capabilities and activities that contribute to a clear understanding of the physical environment by providing geospatial information and services to commanders and staffs. See also **geospatial information and services.** (JP 3-34)

geospatial information — Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products. (JP 2-03)

geospatial information and services — The collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery, gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the Earth's surface. Also called **GI&S.** (JP 2-03)

geospatial intelligence — The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. Also called **GEOINT.** (JP 2-03)

geospatial-intelligence base for contingency operations — A mobile visualization tool that provides access to geospatial data where networks or infrastructure have been damaged or do not exist. Also called **GIBCO.** (JP 3-68)

geospatial intelligence operations — The tasks, activities, and events to collect, manage, analyze, generate, visualize, and provide imagery, imagery intelligence, and geospatial information necessary to support national and defense missions and international arrangements. Also called **GEOINT operations**. (JP 2-03)

Global Air Transportation Execution System — The Air Mobility Command's aerial port operations and management information system designed to support automated cargo and passenger processing, the reporting of in-transit visibility data to the Global Transportation Network, and billing to Air Mobility Command's financial management directorate. Also called **GATES.** See also **Air Mobility Command.** (JP 3-17)

global ballistic missile defense. Defense against ballistic missile threats that cross one or more geographical combatant command boundaries and requires synchronization among the affected combatant commands. Also called **GBMD.** (JP 3-01)

Global Combat Support System-Joint — The primary information technology application used to provide automation support to the joint logistician. Also called **GCSS-J.** (JP 4-0)

Global Command and Control System — A deployable command and control system supporting forces for joint and multinational operations across the range of military operations with compatible, interoperable, and integrated communications systems. Also called **GCCS.** See also **command and control; command and control system.** (JP 6-0)

Global Decision Support System — The command and control system employed by mobility air forces that provides schedules, arrival and/or departure information, and status data to support in-transit visibility of mobility airlift and air refueling aircraft and aircrews. Also called **GDSS.** See also **Air Mobility Command; in-transit visibility.** (JP 3-17)

global distribution — The process that coordinates and synchronizes fulfillment of joint force requirements from point of origin to point of employment. See also **distribution.** (JP 4-09)

global distribution of materiel — The process of providing materiel from the source of supply to its point of consumption or use on a worldwide basis. See also **global distribution.** (JP 4-09)

global fleet station — A persistent sea base of operations from which to interact with partner nation military and civilian populations and the global maritime community. Also called **GFS.** (JP 3-32)

global force management — 1. A process that provides near-term sourcing solutions while providing the integrating mechanism between force apportionment, allocation, and assignment. Also call **GFM.** (JP 3-35) 2. A process to align assignment, allocation, and apportionment of forces to combatant commanders in support of the national defense strategy and joint force availability requirements. (DODI 8260.03)

global maritime partnership — An approach to cooperation among maritime nations with a shared stake in international commerce, safety, security, and freedom of the seas. Also called **GMP.** (JP 3-32)

Global Patient Movement Requirements Center — A joint activity reporting directly to the Commander, United States Transportation Command, which provides medical regulating and aeromedical evacuation scheduling for the continental United States and intertheater operations, provides support to the theater patient movement requirements centers, and coordinates with supporting resource providers to identify available assets and communicates transport to bed plans to the appropriate transportation agency for execution. Also called **GPMRC.** See also **medical treatment facility.** (JP 4-02)

Global Positioning System — A satellite-based radio navigation system operated by the Department of Defense to provide all military, civil, and commercial users with precise positioning, navigation, and timing. Also called **GPS.** (JP 3-14)

global transportation management — The integrated process of satisfying transportation requirements using the Defense Transportation System to meet national security objectives. Also called **GTM.** See also **Defense Transportation System.** (JP 4-01)

go/no-go — A critical point at which a decision to proceed or not must be made. (JP 3-02)

governance — The state's ability to serve the citizens through the rules, processes, and behavior by which interests are articulated, resources are managed, and power is exercised in a society, including the representative participatory decision-making processes typically guaranteed under inclusive, constitutional authority. (JP 3-24)

governing factors — In the context of joint operation planning, those aspects of the situation (or externally imposed factors) that the commander deems critical to the accomplishment of the mission. (JP 5-0)

grid coordinates — Coordinates of a grid coordinate system to which numbers and letters are assigned for use in designating a point on a gridded map, photograph, or chart. (JP 3-09)

ground alert — That status in which aircraft on the ground/deck are fully serviced and armed, with combat crews in readiness to take off within a specified period of time after receipt of a mission order. See also **airborne alert.** (JP 3-01)

ground-based interceptor — A fixed-based, surface-to-air missile for defense against long-range ballistic missiles using an exo-atmospheric hit-to-kill interception of the targeted reentry vehicle in the midcourse phase of flight. Also called **GBI.** (JP 3-01)

ground-based midcourse defense — A surface-to-air ballistic missile defense system for exo-atmospheric midcourse phase interception of long-range ballistic missiles using the ground-based interceptors. Also called **GMD.** (JP 3-01)

group — 1. A flexible administrative and tactical unit composed of either two or more battalions or two or more squadrons. 2. A number of ships and/or aircraft, normally a subdivision of a force, assigned for a specific purpose. 3. A long-standing functional organization that is formed to support a broad function within a joint force commander's headquarters. Also called **GP.** (JP 3-33)

guarded frequencies — A list of time-oriented, enemy frequencies that are currently being exploited for combat information and intelligence or jammed after the commander has weighed the potential operational gain against the loss of the technical information. See also **electronic warfare.** (JP 3-13.1)

guerrilla force — A group of irregular, predominantly indigenous personnel organized along military lines to conduct military and paramilitary operations in enemy-held, hostile, or denied territory. (JP 3-05)

guided missile — An unmanned vehicle moving above the surface of the Earth whose trajectory or flight path is capable of being altered by an external or internal mechanism. See also **ballistic missile.** (JP 3-01)

gun-target line — An imaginary straight line from gun to target. Also called **GTL.** (JP 3-09.3)

H

half-life — The time required for the activity of a given radioactive species to decrease to half of its initial value due to radioactive decay. (JP 3-11)

hasty breach — The creation of lanes through enemy minefields by expedient methods such as blasting with demolitions, pushing rollers or disabled vehicles through the minefields when the time factor does not permit detailed reconnaissance, deliberate breaching, or bypassing the obstacle. (JP 3-15)

hazard — A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. See also **injury; risk.** (JP 3-33)

hazardous cargo — Cargo that includes not only large bulk-type categories such as explosives, pyrotechnics, petroleum, oils, and lubricants, compressed gases, corrosives and batteries, but lesser quantity materials like super-tropical bleach (oxiderizer), pesticides, poisons, medicines, specialized medical chemicals and medical waste that can be loaded as cargo. (JP 3-02.1)

hazards of electromagnetic radiation to fuels — The potential hazard that is created when volatile combustibles, such as fuel, are exposed to electromagnetic fields of sufficient energy to cause ignition. Also called **HERF.** (JP 3-04)

hazards of electromagnetic radiation to ordnance — The danger of accidental actuation of electro-explosive devices or otherwise electrically activating ordnance because of radio frequency electromagnetic fields. Also called **HERO.** See also **electromagnetic radiation; HERO SAFE ordnance; HERO UNSAFE ordnance; ordnance.** (JP 3-04)

hazards of electromagnetic radiation to personnel — The potential hazard that exists when personnel are exposed to an electromagnetic field of sufficient intensity to heat the human body. Also called **HERP.** (JP 3-04)

head of contracting activity — The official who has overall responsibility for managing the contracting activity. Also called **HCA.** (JP 4-10)

head-up display — A display of flight, navigation, attack, or other information superimposed upon the pilot's forward field of view. Also called **HUD.** See also **flight.** (JP 3-09.3)

health care provider — Any member of the Armed Forces, civilian employee of the Department of Defense, or personal services contract employee under Title 10, United States Code, Section 1091 authorized by the Department of Defense to perform health care functions. Also called **DOD health care provider.** (JP 4-02)

health service support — All services performed, provided, or arranged to promote, improve, conserve, or restore the mental or physical well-being of personnel, which include, but are not limited to, the management of health services resources, such as manpower, monies, and facilities; preventive and curative health measures; evacuation of the wounded, injured, or sick; selection of the medically fit and disposition of the medically unfit; blood management; medical supply, equipment, and maintenance thereof; combat and operational stress control; and medical, dental, veterinary, laboratory, optometric, nutrition therapy, and medical intelligence services. Also called **HSS.** (JP 4-02)

health surveillance — The regular or repeated collection, analysis, and interpretation of health-related data and the dissemination of information to monitor the health of a population and to identify potential health risks, thereby enabling timely interventions to prevent, treat, reduce, or control disease and injury, which includes occupational and environmental health surveillance and medical surveillance subcomponents. (JP 4-02)

health threat — A composite of ongoing or potential enemy actions; adverse environmental, occupational, and geographic and meteorological conditions; endemic diseases; and employment of chemical, biological, radiological, and nuclear weapons (to include weapons of mass destruction) that have the potential to affect the short- or long-term health (including psychological impact) of personnel. (JP 4-02)

heavy-lift cargo — 1. Any single cargo lift, weighing over 5 long tons, and to be handled aboard ship. 2. In Marine Corps usage, individual units of cargo that exceed 800 pounds in weight or 100 cubic feet in volume. (JP 4-01.5)

heavy-lift ship — A ship specially designed and capable of loading and unloading heavy and bulky items and has booms of sufficient capacity to accommodate a single lift of 100 tons. (JP 4-01.2)

height of burst — The vertical distance from the Earth's surface or target to the point of burst. Also called **HOB.** (JP 3-41)

helicopter coordination section — The section within the Navy tactical air control center that coordinates rotary-wing air operations with the air traffic control center(s) in the amphibious force. Also called **HCS**. (JP 3-02)

HERO SAFE ordnance — Any ordnance item that is percussion initiated, sufficiently shielded or otherwise so protected that all electro-explosive devices contained by the item are immune to adverse effects (safety or reliability) when the item is employed in its expected radio frequency environments, provided that the general hazards of electromagnetic radiation to ordnance requirements defined in the hazards from electromagnetic radiation manual are observed. See also **electromagnetic radiation; hazards of electromagnetic radiation to ordnance; HERO SUSCEPTIBLE ordnance; HERO UNSAFE ordnance; ordnance.** (JP 3-04)

HERO SUSCEPTIBLE ordnance — Any ordnance item containing electro-explosive devices proven by test or analysis to be adversely affected by radio frequency energy to the point that the safety and/or reliability of the system is in jeopardy when the system is employed in its expected radio frequency environment. See also **electromagnetic radiation; hazards of electromagnetic radiation to ordnance; HERO SAFE ordnance; HERO UNSAFE ordnance; ordnance.** (JP 3-04)

HERO UNSAFE ordnance — Any ordnance item containing electro-explosive devices that has not been classified as HERO SAFE or HERO SUSCEPTIBLE ordnance as a result of a hazards of electromagnetic radiation to ordnance (HERO) analysis or test is considered HERO UNSAFE ordnance. Additionally, any ordnance item containing electro-explosive devices (including those previously classified as HERO SAFE or HERO SUSCEPTIBLE ordnance) that has its internal wiring exposed; when tests are being conducted on that item that result in additional electrical connections to the item; when electro-explosive devices having exposed wire leads are present and handled or loaded in any but the tested condition; when the item is being assembled or disassembled; or when such ordnance items are damaged causing exposure of internal wiring or components or destroying engineered HERO protective devices. See also **electromagnetic radiation; hazards of electromagnetic radiation to ordnance; HERO SAFE ordnance; HERO SUSCEPTIBLE ordnance; ordnance.** (JP 3-04)

H-hour — 1. The specific hour on D-day at which a particular operation commences. (JP 5-0) 2. In amphibious operations, the time the first landing craft or amphibious vehicle of the waterborne wave lands or is scheduled to land on the beach, and in some cases, the commencement of countermine breaching operations. (JP 3-02)

high altitude bombing — Horizontal bombing with the height of release over 15,000 feet. (JP 3-09.3)

high-altitude missile engagement zone — In air defense, that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with high-altitude surface-to-air missiles. Also called **HIMEZ.** (JP 3-01)

high-density airspace control zone — Airspace designated in an airspace control plan or airspace control order in which there is a concentrated employment of numerous and varied weapons and airspace users. Also called **HIDACZ.** (JP 3-52)

high-payoff target — A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. Also called **HPT.** See also **high-value target; target.** (JP 3-60)

high-risk personnel — Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. Also called **HRP.** See also **antiterrorism.** (JP 3-07.2)

high value airborne asset protection — A defensive counterair mission using fighter escorts that defends airborne national assets which are so important that the loss of even one could seriously impact United States warfighting capabilities or provide the enemy with significant propaganda value. Also called **HVAA protection.** See also **defensive counterair.** (JP 3-01)

high-value target — A target the enemy commander requires for the successful completion of the mission. Also called **HVT.** See also **high-payoff target; target.** (JP 3-60)

high velocity drop — A drop procedure in which the drop velocity is greater than 30 feet per second and lower than free drop velocity. See also **airdrop.** (JP 3-17)

homeland — The physical region that includes the continental United States, Alaska, Hawaii, United States territories, and surrounding territorial waters and airspace. (JP 3-28)

homeland defense — The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. Also called **HD.** (JP 3-27)

homeland security — A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. Also called **HS.** (JP 3-27)

home station — The permanent location of active duty units and Reserve Component units. See also **active duty; Reserve Component.** (JP 4-05)

homing — The technique whereby a mobile station directs itself, or is directed, towards a source of primary or reflected energy, or to a specified point. (JP 3-50)

homing adaptor — A device, when used with an aircraft radio receiver, that produces aural and/or visual signals indicating the direction of a transmitting radio station with respect to the heading of the aircraft. (JP 3-50)

honey pot — A trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers. (JP 3-13.4)

horizontal stowage — The lateral distribution of unit equipment or categories of supplies so that they can be unloaded simultaneously from two or more holds. (JP 3-02.1)

hostage rescue — A personnel recovery method used to recover isolated personnel who are specifically designated as hostages. Also called **HR.** (JP 3-50)

host country — A nation which permits, either by written agreement or official invitation, government representatives and/or agencies of another nation to operate, under specified conditions, within its borders. (JP 2-01.2)

hostile act — An attack or other use of force against the United States, United States forces, or other designated persons or property to preclude or impede the mission and/or duties of United States forces, including the recovery of United States personnel or vital United States Government property. (JP 3-28)

hostile casualty — A person who is the victim of a terrorist activity or who becomes a casualty "in action." "In action" characterizes the casualty as having been the direct result of hostile action, sustained in combat or relating thereto, or sustained going to or returning from a combat mission provided that the occurrence was directly related to hostile action. Included are persons killed or wounded mistakenly or accidentally by friendly fire directed at a hostile force or what is thought to be a hostile force. However, not to be considered as sustained in action and not to be interpreted as hostile casualties are injuries or death due to the elements, self-inflicted wounds, combat fatigue, and except in unusual cases, wounds or death inflicted by a friendly force while the individual is in an absent-without-leave, deserter, or dropped-from-rolls status or is voluntarily absent from a place of duty. See also **casualty.**

hostile intent — The threat of imminent use of force against the United States, United States forces, or other designated persons or property. (JP 3-01)

host nation — A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory. Also called **HN.** (JP 3-57)

host-nation support — Civil and/or military assistance rendered by a nation to foreign forces within its territory during peacetime, crises or emergencies, or war based on agreements mutually concluded between nations. Also called **HNS.** See also **host nation.** (JP 4-0)

hub — An organization that sorts and distributes inbound cargo from wholesale supply sources (airlifted, sealifted, and ground transportable) and/or from within the theater**.** See also **hub and spoke distribution; spoke.** (JP 4-09)

hub and spoke distribution — A physical distribution system, in which a major port serves as a central point from which cargo is moved to and from several radiating points to increase transportation efficiencies and in-transit visibility. See also **distribution; distribution system; hub; in-transit visibility; spoke.** (JP 4-09)

human factors — The physical, cultural, psychological, and behavioral attributes of an individual or group that influence perceptions, understanding, and interactions. (JP 2-0)

human intelligence — A category of intelligence derived from information collected and provided by human sources. Also called **HUMINT.** (JP 2-0)

humanitarian and civic assistance — Assistance to the local populace, specifically authorized by Title 10, United States Code, Section 401, and funded under separate authorities, provided by predominantly United States forces in conjunction with military operations. Also called **HCA.** See also **foreign humanitarian assistance.** (JP 3-29)

humanitarian assistance coordination center — A temporary center established by a geographic combatant commander to assist with interagency coordination and planning during the early planning and coordination stages of foreign humanitarian assistance operations. Also called **HACC.** See also **foreign humanitarian assistance; interagency coordination.** (JP 3-29)

humanitarian demining assistance — The activities related to the furnishing of education, training, and technical assistance with respect to the detection and clearance of land mines and other explosive remnants of war. (JP 3-29)

humanitarian mine action — Activities that strive to reduce the social, economic, and environmental impact of land mines, unexploded ordnance and small arms ammunition - also characterized as explosive remnants of war. (JP 3-15)

humanitarian operations center — An international and interagency body that coordinates the overall relief strategy and unity of effort among all participants in a large foreign humanitarian assistance operation. Also called **HOC.** See also **operation.** (JP 3-29)

hung ordnance — Those weapons or stores on an aircraft that the pilot has attempted to drop or fire but could not because of a malfunction of the weapon, rack or launcher, or aircraft release and control system. (JP 3-04)

hydrographic reconnaissance — Reconnaissance of an area of water to determine depths, beach gradients, the nature of the bottom, and the location of coral reefs, rocks, shoals, and man-made obstacles. (JP 3-02)

hygiene services — The provision of personal hygiene facilities and waste collection; and the cleaning, repair, replacement, and return of individual clothing and equipment items in a deployed environment. (JP 4-0)

hyperspectral imagery — Term used to describe the imagery derived from subdividing the electromagnetic spectrum into very narrow bandwidths allowing images useful in precise terrain or target analysis to be formed. Also called **HSI**. (JP 2-03)

I

identification — 1. The process of determining the friendly or hostile character of an unknown detected contact. 2. In arms control, the process of determining which nation is responsible for the detected violations of any arms control measure. 3. In ground combat operations, discrimination between recognizable objects as being friendly or enemy, or the name that belongs to the object as a member of a class. Also called **ID.** (JP 3-01)

identification, friend or foe — A device that emits a signal positively identifying it as a friendly. Also called **IFF.** See also **air defense.** (JP 3-52)

identification maneuver — A maneuver performed for identification purposes. (JP 3-52)

identity intelligence — The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. Also called **I2.** (JP 2-0)

imagery — A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (JP 2-03)

imagery exploitation — The cycle of processing, using, interpreting, mensuration and/or manipulating imagery, and any assembly or consolidation of the results for dissemination. (JP 2-03)

imagery intelligence — The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. Also called **IMINT.** See also **intelligence.** (JP 2-03)

immediate air support — Air support to meet specific requests which arise during the course of a battle and which by their nature cannot be planned in advance. (JP 3-09.3)

immediate decontamination — Decontamination carried out by individuals immediately upon becoming contaminated to save lives, minimize casualties, and limit the spread of contamination. Also called **emergency decontamination.** See also **contamination; decontamination.** (JP 3-11)

immediate response — Any form of immediate action taken in the United States and territories to save lives, prevent human suffering, or mitigate great property damage in response to a request for assistance from a civil authority, under imminently serious conditions when time does not permit approval from a higher authority. (JP 3-28)

immediate response authority — A Federal military commander's, Department of Defense component head's, and/or responsible Department of Defense civilian official's authority temporarily to employ resources under their control, subject to any supplemental direction provided by higher headquarters, and provide those resources to save lives, prevent human suffering, or mitigate great property damage in response to a request for assistance from a civil authority, under imminently serious conditions when time does not permit approval from a higher authority within the United States. Immediate response authority does not permit actions that would subject civilians to the use of military power that is regulatory, prescriptive, proscriptive, or compulsory. (DODD 3025.18)

implementation — Procedures governing the mobilization of the force and the deployment, employment, and sustainment of military operations in response to execution orders issued by the Secretary of Defense. Also called **IMP.** (JP 5-0)

implied task — In the context of joint operation planning, a task derived during mission analysis that an organization must perform or prepare to perform to accomplish a specified task or the mission, but which is not stated in the higher headquarters order. See also **essential task; specified task.** (JP 5-0)

imprest fund — A cash fund of a fixed amount established through an advance of funds, without appropriation change, to an authorized imprest fund cashier to effect immediate cash payments of relatively small amounts for authorized purchases of supplies and nonpersonal services. (JP 1-0)

improvised explosive device — A weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract. Also called **IED.** (JP 3-15.1)

inactive duty training — Authorized training performed by a member of a Reserve Component not on active duty or active duty for training and consisting of regularly scheduled unit training assemblies, additional training assemblies, periods of appropriate duty or equivalent training, and any special additional duties authorized for Reserve Component personnel by the Secretary concerned, and performed by them in connection with the prescribed activities of the organization in which they are assigned with or without pay. Also called **IDT.** See also **active duty for training.** (JP 1)

inactive status — Status of reserve members on an inactive status list of a Reserve Component or assigned to the Inactive Army National Guard. (JP 4-05)

incapacitating agent — A chemical agent, which produces temporary disabling conditions that can be physical or mental and persist for hours or days after exposure to the agent has ceased. (JP 3-11)

incident — An occurrence, caused by either human action or natural phenomena, that requires action to prevent or minimize loss of life, or damage, loss of, or other risks to property, information, and/or natural resources. See also **information operations**. (JP 3-28)

incident awareness and assessment — The Secretary of Defense approved use of Department of Defense intelligence, surveillance, reconnaissance, and other intelligence capabilities for domestic non-intelligence support for defense support of civil authorities. Also called **IAA.** (JP 3-28)

incident command system — A standardized on-scene emergency management construct designed to aid in the management of resources during incidents. Also called **ICS.** (JP 3-28)

incident management — A national comprehensive approach to preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies. (JP 3-28)

incremental costs — Costs additional to the Service appropriations that would not have been incurred absent support of the contingency operation. See also **financial management.** (JP 1-06)

indications — In intelligence usage, information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (JP 2-0)

indicator — 1. In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (JP 2-0) 2. In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (JP 3-13.3)

indigenous populations and institutions — The societal framework of an operational environment including citizens, legal and illegal immigrants, dislocated civilians, and governmental, tribal, ethnic, religious, commercial, and private organizations and entities. Also called **IPI.** (JP 3-57)

individual mobilization augmentee — An individual reservist attending drills who receives training and is preassigned to an Active Component organization, a Selective Service System, or a Federal Emergency Management Agency billet that must be filled on, or shortly after, mobilization. Also called **IMA.** (JP 4-05)

individual protective equipment — In chemical, biological, radiological, or nuclear operations, the personal clothing and equipment required to protect an individual from chemical, biological, and radiological hazards and some nuclear hazards. Also called **IPE.** (JP 3-11)

Individual Ready Reserve — A manpower pool consisting of individuals who have had some training or who have served previously in the Active Component or in the Selected Reserve, and may have some period of their military service obligation remaining. Also called **IRR.** See also **Selected Reserve.** (JP 4-05)

industrial mobilization — The transformation of industry from its peacetime activity to the industrial program necessary to support the national military objectives. See also **mobilization.** (JP 4-05)

industrial preparedness — The state of preparedness of industry to produce essential materiel to support the national military objectives. (JP 4-05)

industrial preparedness program — Plans, actions, or measures for the transformation of the industrial base, both government-owned and civilian-owned, from its peacetime activity to the emergency program necessary to support the national military objectives. Also called **IPP.** (JP 4-05)

inertial navigation system — A self-contained navigation system using inertial detectors, which automatically provides vehicle position, heading, and velocity. Also called **INS.** (JP 3-09)

influence mine — A mine actuated by the effect of a target on some physical condition in the vicinity of the mine or on radiations emanating from the mine. See also **mine.** (JP 3-15)

influence sweep — A sweep designed to produce an influence similar to that produced by a ship and thus actuate mines. (JP 3-15)

information assurance — Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. Also called **IA.** See also **information operations.** (JP 3-12)

information environment — The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information management — The function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals, and organizations in a way that optimizes access by all who have a share in that data or a right to that information. Also called **IM**. (JP 3-0)

information operations — The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called **IO.** See also **electronic warfare; military deception; operations security; military information support operations.** (JP 3-13)

information operations force — A force consisting of units, staff elements, individual military professionals in the Active and Reserve Components, and DOD civilian employees who conduct or directly support the integration of information-related capabilities against adversaries and potential adversaries during military operations as well as those who train these professionals. Also called **IO force**. (DODD 3600.01)

information operations intelligence integration — The integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities, determine effects, and assess the information environment. Also called **IOII**. (JP 3-13)

information-related capability — A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. Also called **IRC.** (JP 3-13)

information report — Report used to forward raw information collected to fulfill intelligence requirements. (JP 2-01)

information requirements — In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. Also called **IR**. See also **priority intelligence requirement.** (JP 2-0)

information superiority — The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also **information operations.** (JP 3-13)

infrared imagery — That imagery produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared position of the electromagnetic spectrum (approximately 0.72 to 1,000 microns). (JP 2-03)

infrared pointer — A low power laser device operating in the near infrared light spectrum that is visible with light amplifying night vision devices. Also called **IR pointer.** (JP 3-09.3)

initial operational capability — The first attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics that is manned or operated by an adequately trained, equipped, and supported military unit or force. Also called **IOC.**

initial radiation — The radiation, essentially neutrons and gamma rays, resulting from a nuclear burst and emitted from the fireball within one minute after burst. See also **residual radiation.** (JP 3-11)

initial reception point — In personnel recovery, a secure area or facility under friendly control where initial reception of recovered isolated personnel can safely take place.

(JP 3-50)

initial response force — The first unit, usually military police, on the scene of a terrorist incident. See also **antiterrorism.** (JP 3-07.2)

initial unloading period — In amphibious operations, that part of the ship-to-shore movement in which unloading is primarily tactical in character and must be instantly responsive to landing force requirements. See also **general unloading period.** (JP 3-02)

initiating directive — An order to a subordinate commander to conduct military operations as directed. Also called **ID**. (JP 3-18)

injury — 1. A term comprising such conditions as fractures, wounds, sprains, strains, dislocations, concussions, and compressions. 2. Conditions resulting from extremes of temperature or prolonged exposure. 3. Acute poisonings (except those due to contaminated food) resulting from exposure to a toxic or poisonous substance. See also **casualty.** (JP 4-02)

inland petroleum distribution system — A multi-product system consisting of both commercially available and military standard petroleum equipment that can be assembled by military personnel and, when assembled into an integrated petroleum distribution system, provides the military with the capability required to support an operational force with bulk fuels. Also called **IPDS.** (JP 4-03)

inner transport area — In amphibious operations, an area as close to the landing beach as depth of water, navigational hazards, boat traffic, and enemy action permit, to which transports may move to expedite unloading. See also **outer transport area; transport area.** (JP 3-02)

instrument approach procedure — A series of predetermined maneuvers for the orderly transfer of an aircraft under instrument flight conditions from the beginning of the initial approach to a landing or to a point from which a landing may be made visually or the missed approach procedure is initiated. (JP 3-04)

instrument meteorological conditions — Meteorological conditions expressed in terms of visibility, distance from cloud, and ceiling; less than minimums specified for visual meteorological conditions. Also called **IMC.** See also **visual meteorological conditions.** (JP 3-04)

instruments of national power — All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational and military. (JP 1)

in support of — Assisting or protecting another formation, unit, or organization while remaining under original control. (JP 1)

insurgency — The organized use of subversion and violence to seize, nullify, or challenge political control of a region. Insurgency can also refer to the group itself. (JP 3-24)

integrated air and missile defense — The integration of capabilities and overlapping operations to defend the homeland and United States national interests, protect the joint force, and enable freedom of action by negating an adversary's ability to create adverse effects from their air and missile capabilities. Also called **IAMD.** (JP 3-01)

integrated consumable item support — A decision support system that takes time-phased force and deployment data and calculates the ability of the Defense Logistics Agency to support those plans. Also called **ICIS.** (JP 4-03)

Integrated Data Environment/Global Transportation Network Convergence — The in-transit visibility system of record providing expanded common integrated data and application services enabling a common logistics picture, distribution visibility, and materiel asset/in-transit visibility for distribution solutions. Also called **IGC**. (JP 4-09)

integrated financial operations — The integration, synchronization, prioritization, and targeting of fiscal resources and capabilities across United States departments and agencies, multinational partners, and nongovernmental organizations against an adversary and in support of the population. Also called **IFO**. (JP 1-06)

integrated logistic support — A composite of all the support considerations necessary to assure the effective and economical support of a system for its life cycle. Also called **ILS.** (JP 4-01.5)

integrated materiel management — The exercise of total Department of Defense-level management responsibility for a federal supply group or class, commodity, or item for a single agency, which normally includes computation of requirements, funding, budgeting, storing, issuing, cataloging, standardizing, and procuring functions. Also called **IMM.** (JP 4-09)

integrated priority list — A list of a combatant commander's highest priority requirements, prioritized across Service and functional lines, defining shortfalls in key programs that, in the judgment of the combatant commander, adversely affect the capability of the combatant commander's forces to accomplish their assigned mission. Also called **IPL**. (JP 1-04)

integrated staff — A staff in which one officer only is appointed to each post on the establishment of the headquarters, irrespective of nationality and Service. See also **multinational staff; joint staff.** (JP 3-16)

integration — 1. In force protection, the synchronized transfer of units into an operational commander's force prior to mission execution. 2. The arrangement of military forces and their actions to create a force that operates by engaging as a whole. 3. In photography, a

process by which the average radar picture seen on several scans of the time base may be obtained on a print, or the process by which several photographic images are combined into a single image. See also **force protection.** (JP 1)

intelligence — 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities. See also **acoustic intelligence; all-source intelligence; communications intelligence; critical intelligence; domestic intelligence; electronic intelligence; foreign intelligence; foreign instrumentation signals intelligence; general military intelligence; imagery intelligence; joint intelligence; measurement and signature intelligence; medical intelligence; national intelligence; open-source intelligence; operational intelligence; scientific and technical intelligence; strategic intelligence; tactical intelligence; target intelligence; technical intelligence; terrain intelligence.** (JP 2-0)

intelligence annex — A supporting document of an operation plan or order that provides detailed information on the enemy situation, assignment of intelligence tasks, and intelligence administrative procedures. (JP 2-01)

intelligence asset — Any resource utilized by an intelligence organization for an operational support role. (JP 2-0)

intelligence community — All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. Also called **IC.** (JP 2-0)

intelligence database — The sum of holdings of intelligence data and finished intelligence products at a given organization. (JP 2-01)

intelligence discipline — A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. See also **counterintelligence; human intelligence; imagery intelligence; intelligence; measurement and signature intelligence; open-source intelligence; signals intelligence; technical intelligence.** (JP 2-0)

intelligence estimate — The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 2-0)

intelligence federation — A formal agreement in which a combatant command joint intelligence center receives preplanned intelligence support from other joint intelligence centers, Service intelligence organizations, reserve organizations, and national agencies during crisis or contingency operations. (JP 2-01)

intelligence information report — The primary vehicle used to provide human intelligence information to the consumer. It utilizes a message format structure that supports automated data entry into intelligence community databases. Also called **IIR.** (JP 2-01.2)

intelligence interrogation — The systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law. (JP 2-01.2)

intelligence mission management — A systematic process by a joint intelligence staff to proactively and continuously formulate and revise command intelligence requirements, and track the resulting information through the processing, exploitation, and dissemination process to satisfy user requirements. Also called **IMM.** (JP 2-01)

intelligence operations — The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. See also **analysis and production; collection; dissemination and integration; evaluation and feedback; planning and direction; processing and exploitation.** (JP 2-01)

intelligence planning — The intelligence component of the Adaptive Planning and Execution system, which coordinates and integrates all available Defense Intelligence Enterprise capabilities to meet combatant commander intelligence requirements. Also called **IP**. (JP 2-0)

intelligence preparation of the battlespace — The analytical methodologies employed by the Services or joint force component commands to reduce uncertainties concerning the enemy, environment, time, and terrain. Also called **IPB.** See also **joint intelligence preparation of the operational environment.** (JP 2-01.3)

intelligence process — The process by which information is converted into intelligence and made available to users, consisting of the six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. See also **analysis and production; collection; dissemination and integration; evaluation and feedback; intelligence; planning and direction; processing and exploitation.** (JP 2-01)

intelligence production — The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements. (JP 2-0)

intelligence-related activities — Those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for

intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. (Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.) (JP 2-01)

intelligence report — A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called **INTREP.** (JP 2-01)

intelligence reporting — The preparation and conveyance of information by any means. More commonly, the term is restricted to reports as they are prepared by the collector and as they are transmitted by the collector to the latter's headquarters and by this component of the intelligence structure to one or more intelligence-producing components. Thus, even in this limited sense, reporting embraces both collection and dissemination. The term is applied to normal and specialist intelligence reports. (JP 2-01.2)

intelligence requirement — 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. Also called **IR**. See also **intelligence; priority intelligence requirement.** (JP 2-0)

intelligence source — The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. See also **intelligence; source.** (JP 2-0)

intelligence, surveillance, and reconnaissance — An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. Also called **ISR.** See also **intelligence; intelligence, surveillance, and reconnaissance visualization; reconnaissance; surveillance.** (JP 2-01)

intelligence, surveillance, and reconnaissance visualization — The capability to graphically display the current and future locations of intelligence, surveillance, and reconnaissance sensors, their projected platform tracks, vulnerability to threat capabilities and meteorological and oceanographic phenomena, fields of regard, tasked collection targets, and products to provide a basis for dynamic retasking and time-sensitive decision making. Also called **ISR visualization.** See also **intelligence; intelligence, surveillance, and reconnaissance; reconnaissance; surveillance.** (JP 2-01)

intelligence system — Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. (JP 2-01)

interagency — Of or pertaining to United States Government agencies and departments, including the Department of Defense. See also **interagency coordination**. (JP 3-08)

interagency coordination — Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged US Government agencies and departments for the purpose of achieving an objective. (JP 3-0)

intercontinental ballistic missile — A land-based, long-range ballistic missile with a range capability greater than 3,000 nautical miles. Also called **ICBM.** (JP 3-01)

interdiction — 1. An action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces, or to otherwise achieve objectives. 2. In support of law enforcement, activities conducted to divert, disrupt, delay, intercept, board, detain, or destroy, under lawful authority, vessels, vehicles, aircraft, people, cargo, and money. See also **air interdiction.** (JP 3-03)

intergovernmental organization — An organization created by a formal agreement between two or more governments on a global, regional, or functional basis to protect and promote national interests shared by member states. Also called **IGO.** (JP 3-08)

intermediate-range ballistic missile — A land-based ballistic missile with a range capability from 1,500 to 3,000 nautical miles. Also called **IRBM.** (JP 3-01)

intermediate staging base — A tailorable, temporary location used for staging forces, sustainment and/or extraction into and out of an operational area. Also called **ISB.** See also **base; staging base.** (JP 3-35)

intermodal — Type of international freight system that permits transshipping among sea, highway, rail, and air modes of transportation through use of American National Standards Institute and International Organization for Standardization containers, line-haul assets, and handling equipment. (JP 4-09)

internal audience — In public affairs, United States military members and Department of Defense civilian employees and their immediate families. See also **external audience; public.** (JP 3-61)

internal defense and development — The full range of measures taken by a nation to promote its growth and to protect itself from subversion, lawlessness, insurgency, terrorism, and other threats to its security. Also called **IDAD.** See also **foreign internal defense.** (JP 3-22)

internally displaced person — Any person who has been forced or obliged to flee or to leave their home or places of habitual residence, in particular as a result of or in order to avoid the effects of armed conflict, situations of generalized violence, violations of human

rights or natural or human-made disasters, and who have not crossed an internationally recognized state border. Also called **IDP**. (JP 3-29)

internal security — The state of law and order prevailing within a nation. (JP 3-08)

International Convention for Safe Containers — A convention held in Geneva, Switzerland, on 2 Dec 1972, which resulted in setting standard safety requirements for containers moving in international transport. These requirements were ratified by the United States on 3 January 1978. Also called **CSC.** (JP 4-09)

international military education and training — Formal or informal instruction provided to foreign military students, units, and forces on a nonreimbursable (grant) basis by offices or employees of the United States, contract technicians, and contractors. Instruction may include correspondence courses; technical, educational, or informational publications; and media of all kinds. Also called **IMET.** See also **United States Military Service funded foreign training.** (JP 3-22)

interoperability — 1. The ability to operate in synergy in the execution of assigned tasks. (JP 3-0) 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (JP 6-0)

interorganizational coordination — The interaction that occurs among elements of the Department of Defense; engaged United States Government agencies; state, territorial, local, and tribal agencies; foreign military forces and government agencies; intergovernmental organizations; nongovernmental organizations; and the private sector. (JP 3-08)

interpretation — A part of the analysis and production phase in the intelligence process in which the significance of information is judged in relation to the current body of knowledge. See also **intelligence process.** (JP 2-01)

interrogation — Systematic effort to procure information by direct questioning of a person under the control of the questioner. (JP 2-01.2)

inter-Service support — Action by one Service or element thereof to provide logistics and/or administrative support to another Service or element thereof. See also **support.** (JP 4-0)

intertheater airlift — The common-user airlift linking theaters to the continental United States and to other theaters as well as the airlift within the continental United States. See also **intratheater airlift.** (JP 3-17)

intertheater patient movement — Moving patients between, into, and out of the different theaters of the geographic combatant commands and into the continental United States

or another supporting theater. See also **en route care; evacuation; intratheater patient movement.** (JP 4-02)

in-transit visibility — The ability to track the identity, status, and location of Department of Defense units, and non-unit cargo (excluding bulk petroleum, oils, and lubricants) and passengers; patients; and personal property from origin to consignee or destination across the range of military operations. Also called **ITV.** (JP 4-01.2)

intratheater airlift — Airlift conducted within a theater with assets assigned to a geographic combatant commander or attached to a subordinate joint force commander. See also **intertheater airlift.** (JP 3-17)

intratheater patient movement — Moving patients within the theater of a combatant command or in the continental United States. See also **en route care; evacuation; intertheater patient movement.** (JP 4-02)

inventory control — That phase of military logistics that includes managing, cataloging, requirements determinations, procurement, distribution, overhaul, and disposal of materiel. Also called **inventory management; materiel control; materiel management; supply management.** (JP 4-09)

inventory control point — An organizational unit or activity within a Department of Defense supply system that is assigned the primary responsibility for the materiel inventory management of a group of items either for a particular Service or for the Defense Department as a whole. Also called **ICP.** (JP 4-09)

ionizing radiation — Particulate (alpha, beta, and neutron) and electromagnetic (X-ray and gamma) radiation of sufficient energy to displace electrons from atoms, producing ions. (JP 3-11)

irregular warfare — A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Also called **IW.** (JP 1)

isolated personnel — United States military, Department of Defense civilians and contractor personnel (and others designated by the President or Secretary of Defense) who are separated from their unit (as an individual or a group) while participating in a United States sponsored military activity or mission and are, or may be, in a situation where they must survive, evade, resist, or escape. See also **combat search and rescue; search and rescue.** (JP 3-50)

isolated personnel report — A Department of Defense form containing information designed to facilitate the identification and authentication of an isolated person by a recovery force. Also called **ISOPREP.** See also **authentication; evader.** (JP 3-50)

item manager — An individual within the organization of an inventory control point or other such organization assigned management responsibility for one or more specific items of materiel. (JP 4-09)

J

J-2X — The staff element of the intelligence directorate of a joint staff that combines and represents the principal authority for counterintelligence and human intelligence support. See also **counterintelligence; human intelligence.** (JP 2-01.2)

joint — Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (JP 1)

joint air attack team — A combination of attack and/or scout rotary-wing aircraft and fixed-wing close air support aircraft operating together to locate and attack high priority targets and other targets of opportunity. Also called **JAAT.** See also **close air support.** (JP 3-09.3)

joint air component coordination element — A general term for the liaison element that serves as the direct representative of the joint force air component commander for joint air operations. Also called **JACCE.** (JP 3-30)

joint air-ground integration center — A staff organization designed to enhance joint collaborative efforts to deconflict joint air-ground assets in the division's airspace. Also called **JAGIC**. (JP 3-09.3)

joint air operations — Air operations performed with air capabilities/forces made available by components in support of the joint force commander's operation or campaign objectives, or in support of other components of the joint force. (JP 3-30)

joint air operations center — A jointly staffed facility established for planning, directing, and executing joint air operations in support of the joint force commander's operation or campaign objectives. Also called **JAOC.** See also **joint air operations.** (JP 3-30)

joint air operations plan — A plan for a connected series of joint air operations to achieve the joint force commander's objectives within a given time and joint operational area. Also called **JAOP.** See also **joint air operations.** (JP 3-30)

joint base — In base defense operations, a locality from which operations of two or more of the Military Departments are projected or supported and which is manned by significant elements of two or more Military Departments or in which significant elements of two or more Military Departments are located. See also **base.** (JP 3-10)

joint captured materiel exploitation center — An element responsible for deriving intelligence information from captured enemy materiel. It is normally subordinate to the intelligence directorate of a joint staff. Also called **JCMEC.** (JP 2-01)

joint civil-military operations task force — A joint task force composed of civil-military operations units from more than one Service. Also called **JCMOTF.** See also **civil-military operations; joint task force.** (JP 3-57)

joint combined exchange training — A program conducted overseas to fulfill United States forces training requirements and at the same time exchange the sharing of skills between United States forces and host nation counterparts. Also called **JCET.** (JP 3-05)

joint communications network — The aggregation of the joint multichannel trunking and switching system and the joint command and control communications system(s) in a theater. Also called **JCN.** (JP 6-0)

joint concept — Links strategic guidance to the development and employment of future joint force capabilities and serve as "engines for transformation" that may ultimately lead to doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) and policy changes. (CJCSI 3010.02)

joint contracting support board — A board established to coordinate all contracting support and to determine specific contracting mechanisms to obtain commercially procured common logistic supplies and services within the operational area. Also called **JCSB.** See also **combatant commander logistic procurement support board; joint requirements review board.** (JP 4-10)

joint counterintelligence unit — An organization composed of Service and Department of Defense agency counterintelligence personnel, formed under the authority of the Secretary of Defense and assigned to a combatant commander, which focuses on combatant command strategic and operational counterintelligence missions. Also called **JCIU**. (JP 2-01.2)

joint data network operations officer — The joint task force operations directorate officer responsible to the commander for integrating data from supporting components into a common database used to generate the common tactical picture. Also called **JDNO.** (JP 3-01)

joint deployable intelligence support system — A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called **JDISS.** (JP 2-0)

joint deployment and distribution enterprise — The complex of equipment, procedures, doctrine, leaders, technical connectivity, information, shared knowledge, organizations, facilities, training, and materiel necessary to conduct joint distribution operations. Also called **JDDE.** (JP 4-0)

joint deployment and distribution operations center — A combatant command movement control organization designed to synchronize and optimize national and theater multimodal resources for deployment, distribution, and sustainment, Also called **JDDOC.** (JP 4-09)

joint desired point of impact — A unique, alpha-numeric coded precise aimpoint associated with a target to achieve an explicit weaponeering objective, and identified by a three dimensional (latitude, longitude, elevation) mensurated coordinate. Also called a **JDPI.** See also **aimpoint; desired point of impact.** (JP 3-60)

joint distribution — The operational process of synchronizing all elements of the joint logistic system using the Joint Deployment and Distribution Enterprise for end-to-end movement of forces and materiel from point of origin to the designated point of need. (JP 4-09)

joint doctrine — Fundamental principles that guide the employment of United States military forces in coordinated action toward a common objective and may include terms, tactics, techniques, and procedures. See also **Chairman of the Joint Chiefs of Staff instruction; Chairman of the Joint Chiefs of Staff manual; doctrine; joint publication; joint test publication; multinational doctrine.** (CJCSI 5120.02)

joint doctrine development community — The Chairman of the Joint Chiefs of Staff, the Services, the combatant commands, the Joint Staff, the combat support agencies, the doctrine development agencies of the Services and the joint community, the National Defense University, the United States Element, North American Aerospace Defense Command, the National Guard Bureau, and Chairman of the Joint Chiefs of Staff controlled activities. Also called **JDDC**. (CJCSI 5120.02)

Joint Doctrine Development System — The system of lead agents, Joint Staff doctrine sponsors, primary review authorities, coordinating review authorities, technical review authorities, assessment agents, evaluation agents, Joint Doctrine Planning Conferences, procedures, and the hierarchical framework designed to initiate, develop, approve, and maintain joint publications. Also called **JDDS**. (CJCSI 5120.02)

Joint Doctrine Planning Conference — A forum convened by the Joint Staff Directorate for Joint Force Development that meets semiannually to address and vote on project proposals; discuss key joint doctrinal and operational issues; discuss potential changes to the joint doctrine development process; keep up to date on the status of the joint publication projects and emerging publications; and keep abreast of other initiatives of interest to the members. Also called **JDPC.** (CJCSM 5120.01)

joint document exploitation center — An element, normally subordinate to the intelligence directorate of a joint staff, responsible for deriving intelligence information from captured adversary documents including all forms of electronic data and other forms of stored textual and graphic information. Also called **JDEC.** See also **intelligence.** (JP 2-01)

joint duty assignment — An assignment to a designated position in a multi-Service, joint or multinational command or activity that is involved in the integrated employment or support of the land, sea, and air forces of at least two of the three Military Departments. Such involvement includes, but is not limited to, matters relating to national military strategy, joint doctrine and policy, strategic planning, contingency planning, and

command and control of combat operations under a unified or specified command. Also called **JDA.**

Joint Duty Assignment List — Positions designated as joint duty assignments are reflected in a list approved by the Secretary of Defense and maintained by the Joint Staff. The Joint Duty Assignment List is reflected in the Joint Duty Assignment Management Information System. Also called **JDAL.**

joint electromagnetic spectrum management operations — Those interrelated functions of frequency management, host nation coordination, and joint spectrum interference resolution that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. Also called **JEMSMO.** (JP 6-01)

joint electromagnetic spectrum operations — Those activities consisting of electronic warfare and joint electromagnetic spectrum management operations used to exploit, attack, protect, and manage the electromagnetic operational environment to achieve the commander's objectives. Also called **JEMSO.** (JP 6-01)

joint engagement zone — In air defense, that airspace of defined dimensions within which multiple air defense systems (surface-to-air missiles and aircraft) are simultaneously employed to engage air threats. Also called **JEZ.** (JP 3-01)

joint facilities utilization board — A joint board that evaluates and reconciles component requests for real estate, use of existing facilities, inter-Service support, and construction to ensure compliance with Joint Civil-Military Engineering Board priorities. Also called **JFUB.** (JP 3-34)

joint field office — A temporary multiagency coordination center established at the incident site to provide a central location for coordination of federal, state, local, tribal, nongovernmental, and private-sector organizations with primary responsibility for incident oversight, direction, or assistance to effectively coordinate protection, prevention, preparedness, response, and recovery actions. Also called **JFO.** (JP 3-28)

joint fires — Fires delivered during the employment of forces from two or more components in coordinated action to produce desired effects in support of a common objective. See also **fires.** (JP 3-0)

joint fires element — An optional staff element that provides recommendations to the operations directorate to accomplish fires planning and synchronization. Also called **JFE.** See also **fire support; joint fires.** (JP 3-60)

joint fires observer — A trained Service member who can request, adjust, and control surface-to-surface fires, provide targeting information in support of Type 2 and 3 close air support terminal attack control, and perform autonomous terminal guidance operations. Also called **JFO**. (JP 3-09.3)

joint fire support — Joint fires that assist air, land, maritime, and special operations forces to move, maneuver, and control territory, populations, airspace, and key waters. See also **fire support; joint fires.** (JP 3-0)

joint flow and analysis system for transportation — System that determines the transportation feasibility of a course of action or operation plan; provides daily lift assets needed to move forces and resupply; advises logistic planners of channel and port inefficiencies; and interprets shortfalls from various flow possibilities. Also called **JFAST.** See also **course of action; operation plan; system**. (JP 3-35)

joint force — A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. See also **joint force commander.** (JP 3-0)

joint force air component commander — The commander within a unified command, subordinate unified command, or joint task force responsible to the establishing commander for recommending the proper employment of assigned, attached, and/or made available for tasking air forces; planning and coordinating air operations; or accomplishing such operational missions as may be assigned. Also called **JFACC.** See also **joint force commander.** (JP 3-0)

joint force chaplain — The military chaplain designated by the joint force commander to serve as the senior chaplain for the joint force. Also called the **JFCH.** (JP 1-05)

joint force commander — A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. Also called **JFC.** See also **joint force.** (JP 1)

joint force land component commander — The commander within a unified command, subordinate unified command, or joint task force responsible to the establishing commander for recommending the proper employment of assigned, attached, and/or made available for tasking land forces; planning and coordinating land operations; or accomplishing such operational missions as may be assigned. Also called **JFLCC.** See also **joint force commander.** (JP 3-0)

joint force maritime component commander — The commander within a unified command, subordinate unified command, or joint task force responsible to the establishing commander for recommending the proper employment of assigned, attached, and/or made available for tasking maritime forces and assets; planning and coordinating maritime operations; or accomplishing such operational missions as may be assigned. Also called **JFMCC.** See also **joint force commander.** (JP 3-0)

joint force special operations component commander — The commander within a unified command, subordinate unified command, or joint task force responsible to the

establishing commander for recommending the proper employment of assigned, attached, and/or made available for tasking special operations forces and assets; planning and coordinating special operations; or accomplishing such operational missions as may be assigned. Also called **JFSOCC.** See also **joint force commander.** (JP 3-0)

joint force surgeon — A general term applied to a Department of Defense medical department officer appointed by the joint force commander to serve as the joint force special staff officer responsible for establishing, monitoring, or evaluating joint force health service support. Also called **JFS.** See also **health service support; joint force.** (JP 4-02)

joint functions — Related capabilities and activities placed into six basic groups of command and control, intelligence, fires, movement and maneuver, protection, and sustainment to help joint force commanders synchronize, integrate, and direct joint operations. (JP 3-0)

joint individual augmentee — An unfunded temporary duty position (or member filling an unfunded temporary duty position) identified on a joint manning document by a supported combatant commander to augment headquarters operations during contingencies. Also called **JIA.** (JP 4-05)

joint integrated prioritized target list — A prioritized list of targets approved and maintained by the joint force commander. Also called **JIPTL**. See also **target.** (JP 3-60)

joint intelligence — Intelligence produced by elements of more than one Service of the same nation. (JP 2-0)

joint intelligence architecture — A dynamic, flexible structure that consists of the Defense Joint Intelligence Operations Center, combatant command joint intelligence operations centers, and subordinate joint task force intelligence operations centers or joint intelligence support elements to provide national, theater, and tactical commanders with the full range of intelligence required for planning and conducting operations. See also **intelligence.** (JP 2-0)

joint intelligence operations center — An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. Also called **JIOC.** (JP 2-0)

joint intelligence preparation of the operational environment — The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. Also called **JIPOE.** (JP 2-01.3)

joint intelligence support element — A subordinate joint force element whose focus is on intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called **JISE.** See also **intelligence; joint force; joint operations.** (JP 2-01)

joint interagency coordination group — A staff group that establishes regular, timely, and collaborative working relationships between civilian and military operational planners. Also called **JIACG.** (JP 3-08)

joint interface control officer — The senior interface control officer for multi-tactical data link networks in the joint force who is responsible for development and validation of the architecture, joint interoperability and management of the multi-tactical data link networks, and overseeing operations of a joint interface control cell. Also called **JICO.** (JP 3-01)

joint interrogation and debriefing center — Physical location for the exploitation of intelligence information from detainees and other sources. Also called **JIDC.** See also **intelligence.** (JP 2-01.2)

joint interrogation operations — 1. Activities conducted by a joint or interagency organization to extract information for intelligence purposes from enemy prisoners of war, dislocated civilians, enemy combatants, or other uncategorized detainees. 2. Activities conducted in support of law enforcement efforts to adjudicate enemy combatants who are believed to have committed crimes against US persons or property. Also called **JIO.** See also **enemy combatant.** (JP 2-01)

joint land operations — Land operations performed across the range of military operations with land forces made available by Service components in support of the joint force commander's operation or campaign objectives, or in support of other components of the joint force. (JP 3-31)

joint land operations plan — A plan for a connected series of joint land operations to achieve the joint force commander's objectives within a given time and operational area. (JP 3-31)

joint logistics — The coordinated use, synchronization, and sharing of two or more Military Departments' logistic resources to support the joint force. See also **logistics.** (JP 4-0)

joint logistics enterprise — A multi-tiered matrix of key global logistics providers cooperatively engaged or structured to achieve a common purpose without jeopardizing the integrity of their own organizational missions and goals. Also called **JLEnt.** (JP 4-0)

Joint Logistics Operations Center — The Joint Logistics Operations Center is the current operations division within the Logistics Directorate of the Joint Staff, which monitors

crises, exercises, and interagency actions and works acquisition and cross-servicing agreements as well as international logistics. Also called **JLOC.** See also **logistics.** (JP 4-01)

joint logistics over-the-shore commander — The commander selected by the joint force commander and tasked to organize the efforts of all elements participating in accomplishing the joint logistics over-the-shore mission. See also **joint logistics over-the-shore operations.** (JP 4-01.6)

joint logistics over-the-shore operations — Operations in which Navy and Army logistics over-the-shore forces conduct logistics over-the-shore operations together under a joint force commander. Also called **JLOTS operations**. See also **joint logistics; logistics over-the-shore operations.** (JP 4-01.6)

joint manpower program — The policy, processes, and systems used in determination and prioritization within and among joint Service manpower requirements. Also called **JMP.** (JP 1-0)

joint meteorological and oceanographic coordination cell — A subset of a joint meteorological and oceanographic coordination organization, which is delegated the responsibility of executing the coordination of meteorological and oceanographic support operations in the operational area. Also called **JMCC.** (JP 3-59)

joint meteorological and oceanographic coordination organization — A Service meteorological and oceanographic organization that is designated within the operations order as the lead organization responsible for coordinating meteorological and oceanographic operations support in the operational area. Also called **JMCO.** (JP 3-59)

joint meteorological and oceanographic officer — Officer designated to provide direct meteorological and oceanographic support to a joint force commander. Also called **JMO.** (JP 3-59)

joint mission-essential task — A mission task selected by a joint force commander deemed essential to mission accomplishment and defined using the common language of the Universal Joint Task List in terms of task, condition, and standard. Also called **JMET.** See also **condition, universal joint task list.** (JP 3-33)

joint mortuary affairs office — Plans and executes all mortuary affairs programs within a theater. Provides guidance to facilitate the conduct of all mortuary programs and to maintain data (as required) pertaining to recovery, identification, and disposition of all US dead and missing in the assigned theater. Serves as the central clearing point for all mortuary affairs and monitors the deceased and missing personal effects program. Also called **JMAO.** See also **mortuary affairs; personal effects.** (JP 4-06)

joint network operations control center — An element of the communications system directorate of a joint staff established as the single control agency for the management and direction of the joint force communications systems. Also called **JNCC.** (JP 6-0)

joint operation planning — Planning activities associated with joint military operations by combatant commanders and their subordinate joint force commanders in response to contingencies and crises. See also **execution planning; Joint Operation Planning and Execution System; joint operation planning process.** (JP 5-0)

Joint Operation Planning and Execution System — An Adaptive Planning and Execution system technology. Also called **JOPES.** See also **joint operation planning; joint operations; level of detail.** (JP 5-0)

joint operation planning process — An orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best course of action, and produce a joint operation plan or order. Also called **JOPP.** See also **joint operation planning; Joint Operation Planning and Execution System.** (JP 5-0)

joint operations — A general term to describe military actions conducted by joint forces and those Service forces employed in specified command relationships with each other, which of themselves, do not establish joint forces. (JP 3-0)

joint operations area — An area of land, sea, and airspace, defined by a geographic combatant commander or subordinate unified commander, in which a joint force commander (normally a joint task force commander) conducts military operations to accomplish a specific mission. Also called **JOA.** See also **area of responsibility; joint special operations area.** (JP 3-0)

joint operations area forecast — The official baseline meteorological and oceanographic forecast for operational planning and mission execution within the joint operations area. Also called **JOAF.** (JP 3-59)

joint operations center — A jointly manned facility of a joint force commander's headquarters established for planning, monitoring, and guiding the execution of the commander's decisions. Also called **JOC**. (JP 3-41)

joint patient movement requirements center — A joint activity established to coordinate the joint patient movement requirements function for a joint task force operating within a unified command area of responsibility. Also called **JPMRC.** See also **health service support; joint force surgeon; joint operations area; medical treatment facility.** (JP 4-02)

joint patient movement team — Teams comprised of personnel trained in medical regulating and movement procedures. Also called **JPMT.** (JP 4-02)

joint personnel accountability reconciliation and reporting — A data repository developed and implemented by the Defense Manpower Data Center that consumes and reconciles data from existing Service deployment systems. Also called **JPARR.** (JP 1-0)

joint personnel reception center — A center established in an operational area by the appropriate joint force commander with the responsibility for the in-processing and out-processing of personnel upon their arrival in and departure from the theater. Also called **JPRC.** (JP 1-0)

joint personnel recovery center — The primary joint force organization responsible for planning and coordinating personnel recovery for military operations within the assigned operational area. Also called **JPRC.** See also **combat search and rescue; search and rescue.** (JP 3-50)

joint personnel training and tracking activity — The continental United States center established to facilitate the reception, accountability, processing, training, and onward movement of individual augmentees preparing for overseas movement to support a joint military operation. Also called **JPTTA.** (JP 1-0)

joint planning and execution community — Those headquarters, commands, and agencies involved in the training, preparation, mobilization, deployment, employment, support, sustainment, redeployment, and demobilization of military forces assigned or committed to a joint operation. Also called **JPEC.** (JP 5-0)

joint planning group — A planning organization consisting of designated representatives of the joint force headquarters principal and special staff sections, joint force components (Service and/or functional), and other supporting organizations or agencies as deemed necessary by the joint force commander. Also called **JPG.** See also **crisis action planning; joint operation planning.** (JP 5-0)

joint proponent — A Service, combatant command, or Joint Staff directorate assigned coordinating authority to lead the collaborative development and integration of joint capability with specific responsibilities designated by the Secretary of Defense. (SecDef Memo 03748-09)

Joint Public Affairs Support Element — A deployable unit assigned to assist a joint force commander in developing and training public affairs forces in joint, interagency, and multinational environments. Also called **JPASE.** (JP 3-61)

joint publication — A compilation of agreed to fundamental principles, considerations, and guidance on a particular topic, approved by the Chairman of the Joint Chiefs of Staff that guides the employment of a joint force toward a common objective. Also called **JP.** See also **Chairman of the Joint Chiefs of Staff instruction; Chairman of the Joint Chiefs of Staff manual; joint doctrine; joint test publication.** (CJCSI 5120.02)

joint reception coordination center — An organization that, when established, ensures that Department of Defense personnel and noncombatant evacuees receive adequate assistance and support for an orderly and expedient debarkation, movement to final destination in the United States, and appropriate follow-on assistance at the final destination. Also called **JRCC.** (JP 3-68)

joint reception, staging, onward movement, and integration — A phase of joint force projection occurring in the operational area during which arriving personnel, equipment, and materiel transition into forces capable of meeting operational requirements. Also called **JRSOI.** See also **integration; joint force; reception; staging**. (JP 3-35)

joint requirements review board — The joint task force or subunified commander's established board to review, validate, approve, and prioritize selected Service component contract support requests. Also called **JRRB.** See also **combatant commander logistic procurement support board; joint contracting support board.** (JP 4-10)

joint restricted frequency list — A time and geographically oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies and limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. Also called **JRFL.** See also **electronic warfare; guarded frequencies; protected frequencies; TABOO frequencies.** (JP 3-13.1)

joint security area — A specific surface area, designated by the joint force commander to facilitate protection of joint bases and their connecting lines of communications that support joint operations. Also called **JSA.** (JP 3-10)

joint security coordination center — A joint operations center tailored to assist the joint security coordinator in meeting the security requirements in the joint operational area. Also called **JSCC.** (JP 3-10)

joint security coordinator — The officer with responsibility for coordinating the overall security of the operational area in accordance with joint force commander directives and priorities. Also called **JSC.** (JP 3-10)

joint servicing — That function performed by a jointly staffed and financed activity in support of two or more Services. (JP 3-05)

joint special operations air component commander — The commander within a joint force special operations command responsible for planning and executing joint special operations air activities. Also called **JSOACC.** (JP 3-05)

joint special operations area — An area of land, sea, and airspace assigned by a joint force commander to the commander of a joint special operations force to conduct special operations activities. Also called **JSOA.** (JP 3-0)

joint special operations task force — A joint task force composed of special operations units from more than one Service, formed to carry out a specific special operation or prosecute special operations in support of a theater campaign or other operations. Also called **JSOTF.** (JP 3-05)

joint staff — 1. The staff of a commander of a unified or specified command, subordinate unified command, joint task force, or subordinate functional component (when a functional component command will employ forces from more than one Military Department), that includes members from the several Services comprising the force. 2. (capitalized as Joint Staff) The staff under the Chairman of the Joint Chiefs of Staff that assists the Chairman and the other members of the Joint Chiefs of Staff in carrying out their responsibilities. Also called **JS.** (JP 1)

Joint Staff doctrine sponsor — A Joint Staff directorate assigned to coordinate a joint doctrine project with the Joint Staff. Also called **JSDS.** See also **joint doctrine.** (CJCSM 5120.01)

Joint Strategic Capabilities Plan — A plan that provides guidance to the combatant commanders and the Joint Chiefs of Staff to accomplish tasks and missions based on current military capabilities. Also called **JSCP.** See also **combatant commander; joint.** (JP 5-0)

joint strategic exploitation center — Theater-level physical location for an exploitation facility that functions under the direction of the joint force commander and is used to hold detainees with potential long-term strategic intelligence value, deemed to be of interest to counterintelligence or criminal investigators, or who may be a significant threat to the United States, its citizens or interests, or US allies. Also called **JSEC.** (JP 2-01.2)

Joint Strategic Planning System — One of the primary means by which the Chairman of the Joint Chiefs of Staff, in consultation with the other members of the Joint Chiefs of Staff and the combatant commanders, carries out the statutory responsibilities to assist the President and Secretary of Defense in providing strategic direction to the Armed Forces. Also called **JSPS.** (JP 5-0)

joint table of distribution — A manpower document that identifies the positions and enumerates the spaces that have been approved for each organizational element of a joint activity for a specific fiscal year (authorization year), and those accepted for the four subsequent fiscal years (program years). Also called **JTD.** See also **joint manpower program.** (JP 1-0)

joint targeting coordination board — A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance, synchronization, and priorities, and refining the joint integrated prioritized target list. Also called **JTCB.** See also **joint integrated prioritized target list; targeting.** (JP 3-60)

joint target list — A consolidated list of selected targets, upon which there are no restrictions placed, considered to have military significance in the joint force commander's operational area. Also called **JTL.** See also **joint; target.** (JP 3-60)

joint task force — A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. Also called **JTF.** (JP 1)

Joint Task Force-Civil Support — A standing joint task force established to plan and integrate Department of Defense support to the designated lead federal agency for domestic chemical, biological, radiological, nuclear, and high-yield explosives consequence management operations. Also called **JTF-CS.** (JP 3-41)

joint terminal attack controller — A qualified (certified) Service member who, from a forward position, directs the action of combat aircraft engaged in close air support and other offensive air operations. Also called **JTAC.** See also **terminal attack control.** (JP 3-09.3)

joint test publication — A proposed publication produced for field-testing an emergent concept that has been validated through the Joint Experimentation Program or a similar joint process. Also called **JTP.** See also **Chairman of the Joint Chiefs of Staff instruction; joint doctrine; joint publication.** (CJCSM 5120.01)

Joint Transportation Board — Responsible to the Chairman of the Joint Chiefs of Staff, the Joint Transportation Board assures that common-user transportation resources assigned or available to the Department of Defense are allocated to achieve maximum benefit in meeting Department of Defense objectives. Also called **JTB.** See also **common-user transportation.** (JP 4-01)

joint urban operations — Joint operations planned and conducted on, or against objectives within a topographical complex and its adjacent natural terrain, where man-made construction or the density of population are the dominant features. Also called **JUOs.** See also **joint operations.** (JP 3-06)

Joint Worldwide Intelligence Communications System — The sensitive compartmented information portion of the Defense Information Systems Network, which incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called **JWICS.** (JP 2-0)

judge advocate — An officer of the Judge Advocate General's Corps of the Army, Air Force, Marine Corps, Navy, and the United States Coast Guard who is designated as a judge advocate. Also called **JA.** (JP 1-04)

jumpmaster — The assigned airborne qualified individual who controls paratroops from the time they enter the aircraft until they exit. (JP 3-17)

K

key position — A civilian position, public or private (designated by the employer and approved by the Secretary concerned), that cannot be vacated during war or national emergency. (JP 1-0)

keystone publications — Joint doctrine publications that establish the doctrinal foundation for a series of joint publications in the hierarchy of joint publications. See also **capstone publications; joint publication.** (CJCSM 5120.01)

key terrain — Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant. (JP 2-01.3)

kill box — A three-dimensional permissive fire support coordination measure with an associated airspace coordinating measure used to facilitate the integration of fires. (JP 3-09)

Intentionally Blank

L

land control operations — The employment of land forces, supported by maritime and air forces (as appropriate) to control vital land areas. See also **sea control operations**. (JP 3-31)

land domain — The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals. (JP 3-31)

land forces — Personnel, weapon systems, vehicles, and support elements operating on land to accomplish assigned missions and tasks. (JP 3-31)

landing aid — Any illuminating light, radio beacon, radar device, communicating device, or any system of such devices for aiding aircraft in an approach and landing. (JP 3-04)

landing area — 1. That part of the operational area within which are conducted the landing operations of an amphibious force. 2. In airborne operations, the general area used for landing troops and materiel either by airdrop or air landing. 3. Any specially prepared or selected surface of land, water, or deck designated or used for takeoff and landing of aircraft. See also **airfield; amphibious force; landing beach; landing force.** (JP 3-02)

landing area diagram — A graphic means of showing, for amphibious operations, the beach designations, boat lanes, organization of the line of departure, scheduled waves, landing ship area, transport areas, and the fire support areas in the immediate vicinity of the boat lanes. (JP 3-02)

landing beach — That portion of a shoreline required for the landing of an amphibious force. (JP 3-02)

landing craft — A craft employed in amphibious operations, specifically designed for carrying troops and their equipment and for beaching, unloading, retracting, and resupply operations. (JP 3-02)

landing craft and amphibious vehicle assignment table — A table showing the assignment of personnel and materiel to each landing craft and amphibious vehicle and the assignment of the landing craft and amphibious vehicles to waves for the ship-to-shore movement. (JP 3-02)

landing craft availability table — A tabulation of the type and number of landing craft that will be available from each ship of the transport group. (JP 3-02)

landing diagram — A graphic means of illustrating the plan for the ship-to-shore movement. (JP 3-02)

landing force — A Marine Corps or Army task organization, which is part of the amphibious force, formed to conduct amphibious operations. Also called **LF.** See also **amphibious force; amphibious operation; amphibious task force; task organization.** (JP 3-02)

landing force operational reserve material — Package of contingency supplies pre-positioned and maintained onboard selected amphibious warfare ships to enhance reaction time and provide support for the embarked landing force in contingencies. Also called **LFORM.** (JP 3-02.1)

landing force support party — A temporary landing force organization composed of Navy and landing force elements, that facilitates the ship-to-shore movement and provides initial combat support and combat service support to the landing force. Also called **LFSP.** See also **combat service support; combat support; landing force; ship-to-shore movement.** (JP 3-02)

landing group — In amphibious operations, a subordinate task organization of the landing force capable of conducting landing operations, under a single tactical command, against a position or group of positions. (JP 3-02)

landing plan — In amphibious operations, a collective term referring to all individually prepared naval and landing force documents that, taken together, present in detail all instructions for execution of the ship-to-shore movement. (JP 3-02)

landing sequence table — A document that incorporates the detailed plans for ship-to-shore movement of nonscheduled units. (JP 3-02)

landing signalman enlisted — Enlisted man responsible for ensuring that helicopters/tiltrotor aircraft, on signal, are safely started, engaged, launched, recovered, and shut down. Also called **LSE.** (JP 3-04)

landing signals officer — Officer responsible for the visual control of aircraft in the terminal phase of the approach immediately prior to landing. Also called **LSO.** See also **terminal phase.** (JP 3-04)

landing site — 1. A site within a landing zone containing one or more landing points. See also airfield. 2. In amphibious operations, a continuous segment of coastline over which troops, equipment and supplies can be landed by surface means. (JP 3-02)

landing zone — Any specified zone used for the landing of aircraft. Also called **LZ.** See also **airfield.** (JP 3-17)

laser-guided weapon — A weapon that uses a seeker to detect laser energy reflected from a laser marked/designated target and through signal processing provides guidance commands to a control system, which guides the weapon to the point from which the laser energy is being reflected. Also called **LGW.** (JP 3-09)

laser rangefinder — A device that uses laser energy for determining the distance from the device to a place or object. (JP 3-09)

laser seeker — A device based on a direction-sensitive receiver that detects the energy reflected from a laser designated target and defines the direction of the target relative to the receiver. See also **laser-guided weapon.** (JP 3-09.3)

laser spot — The area on a surface illuminated by a laser. See also **spot.** (JP 3-09)

laser spot tracker — A device that locks on to the reflected energy from a laser-marked or designated target and defines the direction of the target relative to itself. Also called **LST.** (JP 3-09)

laser target designator — A device that emits a beam of laser energy which is used to mark a specific place or object. Also called **LTD.** See also **target.** (JP 3-09)

latest arrival date — A day, relative to C-Day, that is specified by the supported combatant commander as the latest date when a unit, a resupply shipment, or replacement personnel can arrive at the port of debarkation and support the concept of operations. Also called **LAD.** (JP 5-0)

law enforcement agency — Any of a number of agencies (outside the Department of Defense) chartered and empowered to enforce US laws in the United States, a state or territory (or political subdivision) of the United States, a federally recognized Native American tribe or Alaskan Native Village, or within the borders of a host nation. Also called **LEA.** (JP 3-28)

law of armed conflict — See **law of war**. (JP 1-04)

law of war — That part of international law that regulates the conduct of armed hostilities. Also called **the law of armed conflict.** See also **rules of engagement**. (JP 1-04)

lead — In intelligence usage, a person with potential for exploitation, warranting additional assessment, contact, and/or development. (JP 2-01.2)

lead agency — The US Government agency designated to coordinate the interagency oversight of the day-to-day conduct of an ongoing operation. (JP 3-08)

lead agent — 1. An individual Service, combatant command, or Joint Staff directorate assigned to develop and maintain a joint publication. (CJCSM 5120.01) 2. In medical materiel management, the designated unit or organization to coordinate or execute day-to-day conduct of an ongoing operation or function. Also called **LA.** (JP 4-02)

lead aircraft — 1. The airborne aircraft designated to exercise command of other aircraft within the flight. 2. An aircraft in the van of two or more aircraft. (JP 3-09.3)

lead federal agency — The federal agency that leads and coordinates the overall federal response to an emergency. Also called **LFA.** (JP 3-41)

lead nation — The nation with the will, capability, competence, and influence to provide the essential elements of political consultation and military leadership to coordinate the planning, mounting, and execution of a multinational operation. See also **logistic support; multinational force.** (JP 3-16)

lead Service or agency for common-user logistics — A Service component or Department of Defense agency that is responsible for execution of common-user item or service support in a specific combatant command or multinational operation as defined in the combatant or subordinate joint force commander's operation plan, operation order, and/or directives. See also **common-user logistics.** (JP 4-0)

letter of assist — A contractual document issued by the United Nations to a government authorizing it to provide goods or services to a peacekeeping operation. Also called **LOA.** See also **peacekeeping.** (JP 1-06)

letter of authorization — A document issued by the procuring contracting officer or designee that authorizes contractor personnel authorized to accompany the force to travel to, from, and within the operational area; and, outlines government furnished support authorizations within the operational area. Also called **LOA.** (JP 4-10)

letter of offer and acceptance — Standard Department of Defense form on which the United States Government documents its offer to transfer to a foreign government or international organization United States defense articles and services via foreign military sales pursuant to the Arms Export Control Act. Also called **LOA.** See also **foreign military sales.** (JP 4-08)

level of detail — Within the current joint planning and execution system, movement characteristics for both personnel and cargo are described at six distinct levels of detail. Levels I, V, and VI describe personnel and Levels I through IV and VI for cargo. Levels I through IV are coded and visible in the Joint Operation Planning and Execution System automated data processing. Levels V and VI are used by Joint Operation Planning and Execution System automated data processing feeder systems. a. **level I** - personnel: expressed as total number of passengers by unit line number. Cargo: expressed in total short tons, total measurement tons, total square feet, and total thousands of barrels by unit line number. Petroleum, oils, and lubricants is expressed by thousands of barrels by unit line number. b. **level II** - cargo: expressed by short tons and measurement tons of bulk, oversize, outsize, and non-air transportable cargo by unit line number. Also square feet for vehicles and non self-deployable aircraft and boats by unit line number. c. **level III** - cargo: detail by cargo category code expressed as short tons and measurement tons as well as square feet associated to that cargo category code for an individual unit line number. d. **level IV** - cargo: detail for individual dimensional data expressed in length, width, and height in number of inches, and weight/volume in short tons/measurement tons, along with a cargo description. Each cargo item is associated with a cargo category

code and a unit line number). e. **level V** - personnel: any general summarization/aggregation of level VI detail in distribution and deployment. f. **level VI** - personnel: detail expressed by name, Service, military occupational specialty and unique identification number. Cargo: detail expressed by association to a transportation control number or single tracking number or item of equipment to include federal stock number/national stock number and/or requisition number. Nested cargo, cargo that is contained within another equipment item, may similarly be identified. Also called **JOPES level of detail.** (CJCSM 3122.01A)

leverage — In the context of joint operation planning, a relative advantage in combat power and/or other circumstances against the adversary across one or more domains or the information environment sufficient to exploit that advantage. See also **operational art; operational design.** (JP 5-0)

L-hour — 1. The specific hour on C-day at which a deployment operation commences or is to commence. (JP 5-0) 2. In amphibious operations, the time at which the first helicopter or tiltrotor aircraft of the airborne ship-to-shore movement wave touches down or is scheduled to touch down in the landing zone (JP 3-02)

liaison — That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action. (JP 3-08)

life cycle — The total phases through which an item passes from the time it is initially developed until the time it is either consumed in use or disposed of as being excess to all known materiel requirements. (JP 4-02)

lighterage — The process in which small craft are used to transport cargo or personnel from ship-to-shore using amphibians, landing craft, discharge lighters, causeways, and barges. (JP 4-01.6)

limiting factor — A factor or condition that, either temporarily or permanently, impedes mission accomplishment. (JP 5-0)

line of communications — A route, either land, water, and/or air, that connects an operating military force with a base of operations and along which supplies and military forces move. Also called **LOC.** (JP 2-01.3)

line of demarcation — A line defining the boundary of a buffer zone used to establish the forward limits of disputing or belligerent forces after each phase of disengagement or withdrawal has been completed. See also **buffer zone; disengagement; peace operations.** (JP 3-07.3)

line of departure — 1. In land warfare, a line designated to coordinate the departure of attack elements. Also called **LD.** (JP 3-31) 2. In amphibious operations, a suitably marked offshore coordinating line, which is located at the seaward end of a boat lane, to assist in

the landing of landing craft and amphibious vehicles on designated beaches at the scheduled times. Also called **LOD.** (JP 3-02)

line of effort — In the context of joint operation planning, using the purpose (cause and effect) to focus efforts toward establishing operational and strategic conditions by linking multiple tasks and missions. Also called **LOE.** (JP 5-0)

line of operation — A line that defines the interior or exterior orientation of the force in relation to the enemy or that connects actions on nodes and/or decisive points related in time and space to an objective(s). Also called **LOO.** (JP 5-0)

link — 1. A behavioral, physical, or functional relationship between nodes. 2. In communications, a general term used to indicate the existence of communications facilities between two points. 3. A maritime route, other than a coastal or transit route, which links any two or more routes. See also **node.** (JP 3-0)

listening watch — A continuous receiver watch established for the reception of communication addressed to, or of interest to, the unit maintaining the watch, with complete log optional. (JP 3-50)

littoral — The littoral comprises two segments of operational environment: 1. Seaward: the area from the open ocean to the shore, which must be controlled to support operations ashore. 2. Landward: the area inland from the shore that can be supported and defended directly from the sea. (JP 2-01.3)

loading plan — All of the individually prepared documents which, taken together, present in detail all instructions for the arrangement of personnel, and the loading of equipment for one or more units or other special grouping of personnel or material moving by highway, water, rail, or air transportation. (JP 3-02.1)

load signal — In personnel recovery, a visual signal displayed in a covert manner to indicate the presence of an individual or object at a given location. See also **evasion; recovery operations.** (JP 3-50)

locate — In personnel recovery, the task where actions are taken to precisely find and authenticate the identity of isolated personnel. (JP 3-50)

lodgment — A designated area in a hostile or potentially hostile operational area that, when seized and held, makes the continuous landing of troops and materiel possible and provides maneuver space for subsequent operations. (JP 3-18)

logistics — Planning and executing the movement and support of forces. (JP 4-0)

logistics over-the-shore operation area — That geographic area required to conduct a logistics over-the-shore operation. Also called **LOA.** See also **logistics over-the-shore operations.** (JP 4-01.6)

logistics over-the-shore operations — The loading and unloading of ships without the benefit of deep draft-capable, fixed port facilities; or as a means of moving forces closer to tactical assembly areas dependent on threat force capabilities. Also called **LOTS operations**. See also **joint logistics over-the-shore operations.** (JP 4-01.6)

logistic support — Support that encompasses the logistic services, materiel, and transportation required to support the continental United States-based and worldwide deployed forces. (JP 4-0)

logistics supportability analysis — Combatant command internal assessment for the Joint Strategic Capabilities Plan on capabilities and shortfalls of key logistic capabilities required to execute and sustain the concept of support conducted on all level three plans with the time phased force deployment data. Also called **LSA**. (JP 4-0)

low-altitude missile engagement zone — In air defense, that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with low- to medium-altitude surface-to-air missiles. Also called **LOMEZ.** (JP 3-01)

low-level transit route — A temporary corridor of defined dimensions established in the forward area to minimize the risk to friendly aircraft from friendly air defenses or surface forces. Also called **LLTR.** (JP 3-52)

low velocity drop — A drop procedure in which the drop velocity does not exceed 30 feet per second. (JP 3-17)

low-visibility operations — Sensitive operations wherein the diplomatic-military restrictions inherent in covert and clandestine operations are either not necessary or not feasible; actions are taken as required to limit exposure of those involved and/or their activities and with the knowledge that the action and/or sponsorship of the operation may preclude plausible denial by the initiating power. (JP 3-05)

Intentionally Blank

M

magnetic mine — A mine that responds to the magnetic field of a target. (JP 3-15)

mail embargo — A temporary shutdown or redirection of mail flow to or from a specific location. (JP 1-0)

main operating base — A facility outside the United States and US territories with permanently stationed operating forces and robust infrastructure. Main operating bases are characterized by command and control structures, enduring family support facilities, and strengthened force protection measures. Also called **MOB.** See also **cooperative security location; forward operating site.** (CJCS CM-0007-05)

main supply route — The route or routes designated within an operational area upon which the bulk of traffic flows in support of military operations. Also called **MSR.** (JP 4-01.5)

maintenance — 1. All action, including inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation, taken to retain materiel in a serviceable condition or to restore it to serviceability. 2. All supply and repair action taken to keep a force in condition to carry out its mission. 3. The routine recurring work required to keep a facility in such condition that it may be continuously used at its original or designed capacity and efficiency for its intended purpose. (JP 4-0)

major force — A military organization comprised of major combat elements and associated combat support, combat service support, and sustainment increments. (JP 5-0)

major operation — 1. A series of tactical actions (battles, engagements, strikes) conducted by combat forces of a single or several Services, coordinated in time and place, to achieve strategic or operational objectives in an operational area. 2. For noncombat operations, a reference to the relative size and scope of a military operation. See also **operation.** (JP 3-0)

maneuver — 1. A movement to place ships, aircraft, or land forces in a position of advantage over the enemy. 2. A tactical exercise carried out at sea, in the air, on the ground, or on a map in imitation of war. 3. The operation of a ship, aircraft, or vehicle, to cause it to perform desired movements. 4. Employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy. See also **mission; operation.** (JP 3-0)

manpower management — The means of manpower control to ensure the most efficient and economical use of available manpower. (JP 1-0)

manpower requirements — Human resources needed to accomplish specified work loads of organizations. (JP 1-0)

Marine air command and control system — A system that provides the aviation combat element commander with the means to command, coordinate, and control all air operations within an assigned sector and to coordinate air operations with other Services. Also called **MACCS.** See also **direct air support center; tactical air operations center.** (JP 3-09.3)

Marine Corps special operations forces — Those Active Component Marine Corps forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. Also called **MARSOF.** (JP 3-05)

Maritime Administration Ready Reserve Force — The surge sealift assets owned and operated by the United States Department of Transportation/Maritime Administration and Military Sealift Command (in contingency), crewed by civilian mariners. Also called **MARAD RRF**. See also **National Defense Reserve Fleet.** (JP 4-01.6)

maritime domain — The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. (JP 3-32)

maritime domain awareness — The effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of a nation. Also called **MDA**. (JP 3-32)

maritime forces — Forces that operate on, under, or above the sea to gain or exploit command of the sea, sea control, or sea denial and/or to project power from the sea. (JP 3-32)

maritime interception operations — Efforts to monitor, query, and board merchant vessels in international waters to enforce sanctions against other nations such as those in support of United Nations Security Council Resolutions and/or prevent the transport of restricted goods. Also called **MIO.** (JP 3-03)

maritime power projection — Power projection in and from the maritime environment, including a broad spectrum of offensive military operations to destroy enemy forces or logistic support or to prevent enemy forces from approaching within enemy weapons' range of friendly forces. (JP 3-32)

maritime pre-positioning force operation — A rapid deployment and assembly of a Marine expeditionary force in a secure area using a combination of intertheater airlift and forward-deployed maritime pre-positioning ships. Also called **MPF operation**. See also **maritime pre-positioning ships.** (JP 4-01.6)

maritime pre-positioning ships — Civilian-crewed, Military Sealift Command-chartered ships that are usually forward-deployed and loaded with pre-positioned equipment and up to 30 days of supplies to support Marine expeditionary brigades. Also called **MPSs.** See also **Navy cargo handling battalion**. (JP 3-02.1)

maritime security operations — Those operations to protect maritime sovereignty and resources and to counter maritime-related terrorism, weapons proliferation, transnational crime, piracy, environmental destruction, and illegal seaborne immigration. Also called **MSO.** (JP 3-32)

Maritime Security Program — A program authorized in the Maritime Security Act of 2003 requiring the Secretary of Transportation, in consultation with the Secretary of Defense, to establish a fleet of active, commercially viable, militarily useful, privately-owned vessels to meet national defense and other security requirements. Also called **MSP.** (JP 4-01.2)

maritime superiority — That degree of dominance of one force over another that permits the conduct of maritime operations by the former and its related land, maritime, and air forces at a given time and place without prohibitive interference by the opposing force. (JP 3-32)

maritime terminal — A facility for berthing ships simultaneously at piers, quays, and/or working anchorages. Also called **water terminal.** (JP 4-01.5)

marking — To maintain contact on a target from such a position that the marking unit has an immediate offensive capability. (JP 3-09.3)

marshalling — 1. The process by which units participating in an amphibious or airborne operation group together or assemble when feasible or move to temporary camps in the vicinity of embarkation points, complete preparations for combat, or prepare for loading. 2. The process of assembling, holding, and organizing supplies and/or equipment, especially vehicles of transportation, for onward movement. See also **staging area.** (JP 3-17)

marshalling area — A location in the vicinity of a reception terminal or pre-positioned equipment storage site where arriving unit personnel, equipment, materiel, and accompanying supplies are reassembled, returned to the control of the unit commander, and prepared for onward movement. See also **marshalling.** (JP 3-35)

mass atrocity response operations — Military activities conducted to prevent or halt mass atrocities. Also called **MARO.** (JP 3-07.3)

mass casualty — Any large number of casualties produced in a relatively short period of time, usually as the result of a single incident such as a military aircraft accident, hurricane, flood, earthquake, or armed attack that exceeds local logistic support capabilities. Also called **MASCAL.** See also **casualty.** (JP4-02)

massed fire — 1. The fire of the batteries of two or more ships directed against a single target. 2. Fire from a number of weapons directed at a single point or small area. (JP 3-02)

master — The commander of a United States Naval Ship, a commercial ship, or a government-owned general agency agreement ship operated for the Military Sealift Command by a civilian company to transport Department of Defense cargo. (JP 3-02.1)

master air attack plan — A plan that contains key information that forms the foundation of the joint air tasking order. Also called **MAAP.** See also **target.** (JP 3-60)

materials handling equipment. Equipment used at air, ground, and sea ports to handle large cargo. Also called **MHE.** (JP 4-01.5)

materiel — All items necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. See also **equipment; personal property.** (JP 4-0)

materiel inventory objective — The quantity of an item required to be on hand and on order on M-day in order to equip, provide a materiel pipeline, and sustain the approved United States force structure and those Allied forces designated for United States materiel support, through the period prescribed for war materiel planning purposes. (JP 4-09)

materiel planning — A subset of logistic planning consisting of the four-step process of: a. **requirements definition.** Requirements for significant items are calculated at item-level detail to support sustainability planning and analysis. b. **apportionment.** Items are apportioned to the combatant commanders based on a global scenario to avoid sourcing of items to multiple theaters. c. **sourcing.** Sourcing is the matching of available capabilities on a given date against item requirements to support sustainability analysis and the identification of locations to support transportation planning. d. **documentation.** Sourced item requirements are translated into movement requirements and documented in the Joint Operation Planning and Execution System database for transportation feasibility analysis. (JP 4-09)

materiel release order — An order issued by an accountable supply system manager directing a non-accountable activity within the same supply distribution complex to release and ship materiel. Also called **MRO.** (JP 4-09)

materiel requirements — Those quantities of items of equipment and supplies necessary to equip, provide a materiel pipeline, and sustain a Service, formation, organization, or unit in the fulfillment of its purposes or tasks during a specified period. (JP 4-09)

maximum ordinate — In artillery and naval gunfire support, the height of the highest point in the trajectory of a projectile above the horizontal plane passing through its origin. Also called **vertex height** and **MAXORD.** (JP 3-09.3)

M-day — Mobilization day; unnamed day on which mobilization of forces begins. (JP 4-06)

measurement and signature intelligence — Information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and

identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event. Also called **MASINT.** See also **intelligence; scientific and technical intelligence.** (JP 2-0)

Measurement and Signature Intelligence Requirements System — A system for the management of theater and national measurement and signature intelligence collection requirements, providing automated tools for users in support of submission, review, and validation of measurement and signature intelligence nominations of requirements to be tasked for national and Department of Defense measurement and signature intelligence collection, production, and exploitation resources. Also called **MRS.** See also **measurement and signature intelligence.** (JP 2-01)

measurement ton — The unit of volumetric measurement of equipment associated with surface-delivered cargo equal to the total cubic feet divided by 40. Also called **MTON.** (JP 4-01.5)

measure of effectiveness — A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. Also called **MOE.** See also **combat assessment; mission.** (JP 3-0)

measure of performance — A criterion used to assess friendly actions that is tied to measuring task accomplishment. Also called **MOP.** (JP 3-0)

mechanical sweep — In naval mine warfare, any sweep used with the object of physically contacting the mine or its appendages. (JP 3-15)

media operations center — A facility established by the commander to serve as the focal point for the interface between the military and the media during the conduct of military operations. Also called **MOC.** (JP 3-61)

media pool — A limited number of news media who represent a larger number of news media organizations for purposes of news gathering and sharing of material during a specified activity. See also **public affairs.** (JP 3-61)

medical civil-military operations — All military health-related activities in support of a joint force commander that establish, enhance, maintain or influence relations between the joint or multinational force and host nation, multinational governmental and nongovernmental civilian organizations and authorities, and the civilian populace in order to facilitate military operations, achieve United States operational objectives, and positively impact the health sector. Also called **MCMO.** (JP 4-02)

medical engagement protocols — Directives issued by competent military authority that delineate the circumstances and limitations under which United States medical forces will initiate medical care and support to those individuals that are not Department of

Defense health care beneficiaries or designated eligible for care in a military medical treatment facility by the Secretary of Defense. (JP 4-02)

medical intelligence — That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. Also called **MEDINT.** See also **intelligence.** (JP 2-01)

medical intelligence preparation of the operational environment — A systematic continuing process that analyzes information on medical and disease threats, enemy capabilities, terrain, weather, local medical infrastructure, potential humanitarian and refugee situations, transportation issues, and political, religious and social issues for all types of operations. Also called **MIPOE.** (JP 4-02)

medical logistics support — A functional area of logistics support for the joint force surgeon's health service support mission and that includes supplying Class VIII medical supplies (medical material to include medical peculiar repair parts used to sustain the health service support system), optical fabrication, medical equipment maintenance, blood storage and distribution, and medical gases. Also called **MEDLOG support.** (JP 4-02)

medical regulating — The actions and coordination necessary to arrange for the movement of patients through the roles of care and to match patients with a medical treatment facility that has the necessary health service support capabilities and available bed space. See also **health service support; medical treatment facility.** (JP 4-02)

medical surveillance — The ongoing, systematic collection, analysis, and interpretation of data derived from instances of medical care or medical evaluation, and the reporting of population-based information for characterizing and countering threats to a population's health, well-being and performance. See also **surveillance.** (JP 4-02)

medical treatment facility — A facility established for the purpose of furnishing medical and/or dental care to eligible individuals. Also called **MTF.** (JP 4-02)

medium-range ballistic missile. A ballistic missile with a range capability from about 600 to 1,500 nautical miles. Also called **MRBM.** (JP 3-01)

mensuration — The process of measurement of a feature or location on the earth to determine an absolute latitude, longitude, and elevation. (JP 3-60)

message — 1. Any thought or idea expressed briefly in a plain or secret language and prepared in a form suitable for transmission by any means of communication. (JP 6-0) 2. A narrowly focused communication directed at a specific audience to support a specific theme. Also called **MSG**. (JP 3-61)

meteorological and oceanographic — A term used to convey all environmental factors, from the sub-bottom of the Earth's oceans through maritime, land areas, airspace, ionosphere, and outward into space. Also called **METOC.** (JP 3-59)

meteorological and oceanographic data — Measurements or observations of meteorological and oceanographic variables. (JP 3-59)

meteorological and oceanographic environment — The surroundings that extend from the sub-bottom of the Earth's oceans, through maritime, land areas, airspace, ionosphere, and outward into space, which include conditions, resources, and natural phenomena, in and through which the joint force operates. (JP 3-59)

meteorological and oceanographic information — Actionable information to include meteorological, climatological, oceanographic, and space environment observations, analyses, prognostic data or products and meteorological and oceanographic effects. (JP 3-59)

meteorological and oceanographic operations support community — The collective of electronically connected, shore-based meteorological and oceanographic production facilities/centers, theater and/or regional meteorological and oceanographic production activities. Also called **MOSC.** See also **meteorological and oceanographic.** (JP 3-59)

meteorological watch — Monitoring the weather for a route, area, or terminal and advising concerned organizations when hazardous conditions that could affect their operations or pose a hazard to life or property are observed or forecast to occur. Also called **METWATCH.** (JP 3-59)

meteorology — The study dealing with the phenomena of the atmosphere including the physics, chemistry, and dynamics extending to the effects of the atmosphere on the Earth's surface and the oceans. (JP 3-59)

midcourse phase — That portion of the flight of a ballistic missile between the boost phase and the terminal phase. See also **boost phase; terminal phase.** (JP 3-01)

migrant — A person who (1) belongs to a normally migratory culture who may cross national boundaries, or (2) has fled his or her native country for economic reasons rather than fear of political or ethnic persecution. (JP 3-29)

military assistance advisory group — A joint Service group, normally under the military command of a commander of a unified command and representing the Secretary of Defense, which primarily administers the US military assistance planning and programming in the host country. Also called **MAAG**. (JP 3-22)

Military Assistance Program — That portion of the US security assistance authorized by the Foreign Assistance Act of l961, as amended, which provides defense articles and services to recipients on a nonreimbursable (grant) basis. Also called **MAP.** (JP 3-22)

military civic action — Programs and projects managed by United States forces but executed primarily by indigenous military or security forces that contribute to the economic and social development of a host nation civil society thereby enhancing the legitimacy and social standing of the host nation government and its military forces. Also called **MCA.** (JP 3-57)

military construction — Any construction, alteration, development, conversion, or extension of any kind carried out with respect to a military installation. Also called **MILCON.** (JP 3-34)

military deception — Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Also called **MILDEC.** (JP 3-13.4)

Military Department — One of the departments within the Department of Defense created by the National Security Act of 1947, which are the Department of the Army, the Department of the Navy, and the Department of the Air Force. Also called **MILDEP.** See also **Department of the Air Force; Department of the Army; Department of the Navy.** (JP 1)

military engagement — Routine contact and interaction between individuals or elements of the Armed Forces of the United States and those of another nation's armed forces, or foreign and domestic civilian authorities or agencies to build trust and confidence, share information, coordinate mutual activities, and maintain influence. (JP 3-0)

military government — The supreme authority the military exercises by force or agreement over the lands, property, and indigenous populations and institutions of domestic, allied, or enemy territory therefore substituting sovereign authority under rule of law for the previously established government. (JP 3-57)

military health system — A health system that supports the military mission by fostering, protecting, sustaining, and restoring health and providing the direction, resources, health care providers, and other means necessary for promoting the health of the beneficiary population. (JP 4-02)

military information support operations — Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. Also called **MISO.** (JP 3-13.2)

Military Intelligence Board — A decision-making forum which formulates Department of Defense intelligence policy and programming priorities. Also called **MIB.** See also **intelligence.** (JP 2-0)

military intervention — The deliberate act of a nation or a group of nations to introduce its military forces into the course of an existing controversy. (JP 3-0)

military occupation — A condition in which territory is under the effective control of a foreign armed force. See also **occupied territory.** (JP 3-0)

Military Postal Service — The command, organization, personnel, and facilities established to provide a means for the transmission of mail to and from the Department of Defense, members of the US Armed Forces, and other authorized agencies and individuals. Also called **MPS.** (JP 1-0)

Military Postal Service Agency — The single manager operating agency established to manage the Military Postal Service. Also called **MPSA.** (JP 1-0)

military post office — A branch of a designated US-based post office established by US Postal Service authority and operated by one of the Services. Also called **MPO.** (JP 1-0)

Military Sealift Command — A major command of the United States Navy reporting to Commander Fleet Forces Command, and the United States Transportation Command's component command responsible for designated common-user sealift transportation services to deploy, employ, sustain, and redeploy United States forces on a global basis. Also called **MSC.** See also **transportation component command.** (JP 4-01.2)

Military Sealift Command force — Common-user sealift consisting of three subsets: the Naval Fleet Auxiliary Force, common-user ocean transportation, and the special mission support force. See also **common-user sealift; Military Sealift Command.** (JP 4-01.2)

military source operations — The collection, from, by and/or via humans, of foreign and military and military-related intelligence. (JP 2-01.2)

military specification container — A container that meets specific written standards. Also called **MILSPEC container.** (JP 4-09)

military standard requisitioning and issue procedure — A uniform procedure established by the Department of Defense for use within the Department of Defense to govern requisition and issue of materiel within standardized priorities. Also called **MILSTRIP.** (JP 4-01)

military standard transportation and movement procedures — Uniform and standard transportation data, documentation, and control procedures applicable to all cargo

movements in the Department of Defense transportation system. Also called **MILSTAMP.** (JP 4-01.5)

military technician — A Federal civilian employee providing full-time support to a National Guard, Reserve, or Active Component organization for administration, training, and maintenance of the Selected Reserve. Also called **MILTECH.** (CJCSM 3150.13)

military van (container) — Military-owned, demountable container, conforming to United States and international standards, operated in a centrally controlled fleet for movement of military cargo. Also called **MILVAN.** (JP 4-02)

mine — 1. In land mine warfare, an explosive or other material, normally encased, designed to destroy or damage ground vehicles, boats, or aircraft, or designed to wound, kill, or otherwise incapacitate personnel and designed to be detonated by the action of its victim, by the passage of time, or by controlled means. 2. In naval mine warfare, an explosive device laid in the water with the intention of damaging or sinking ships or of deterring shipping from entering an area. See also **mine warfare.** (JP 3-15)

mine countermeasures — All methods for preventing or reducing damage or danger from mines. Also called **MCM.** (JP 3-15)

minefield — 1. In land warfare, an area of ground containing mines emplaced with or without a pattern. 2. In naval warfare, an area of water containing mines emplaced with or without a pattern. See also **mine; mine warfare.** (JP 3-15)

minefield record — A complete written record of all pertinent information concerning a minefield, submitted on a standard form by the officer in charge of the emplacement operations. (JP 3-15)

minefield report — An oral, electronic, or written communication concerning mining activities (friendly or enemy) submitted in a standard format by the fastest secure means available. (JP 3-15)

minehunting — Employment of sensor and neutralization systems, whether air, surface, or subsurface, to locate and dispose of individual mines in a known field, or to verify the presence or absence of mines in a given area. See also **minesweeping.** (JP 3-15)

minesweeping — The technique of clearing mines using either mechanical sweeping to remove, disturb, or otherwise neutralize the mine; explosive sweeping to cause sympathetic detonations, damage, or displace the mine; or influence sweeping to produce either the acoustic or magnetic influence required to detonate the mine. See also **minehunting.** (JP 3-15)

mine warfare — The strategic, operational, and tactical use of mines and mine countermeasures either by emplacing mines to degrade the enemy's capabilities to wage

land, air, and maritime warfare or by countering of enemy-emplaced mines to permit friendly maneuver or use of selected land or sea areas. Also called **MW.** (JP 3-15)

minimize — A condition wherein normal message and telephone traffic is drastically reduced in order that messages connected with an actual or simulated emergency shall not be delayed. (JP 6-0)

minimum force — Those minimum actions, including the use of armed force, sufficient to bring a situation under control or to defend against hostile act or hostile intent, where the firing of weapons is to be considered as a means of last resort. (JP 3-07.3)

minimum-risk route — A temporary corridor of defined dimensions recommended for use by high-speed, fixed-wing aircraft that presents the minimum known hazards to low-flying aircraft transiting the combat zone. Also called **MRR.** (JP 3-52)

missile defense — Defensive measures designed to destroy attacking enemy missiles, or to nullify or reduce the effectiveness of such attack. (JP 3-01)

missile engagement zone — In air defense, that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with surface-to-air missile systems. Also called **MEZ.** (JP 3-01)

mission — 1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore. (JP 3-0) 2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task. (JP 3-0) 3. The dispatching of one or more aircraft to accomplish one particular task. (JP 3-30)

mission assignment — The vehicle used by the Department of Homeland Security/Emergency Preparedness and Response/Federal Emergency Management Agency to support federal operations in a Stafford Act major disaster or emergency declaration that orders immediate, short-term emergency response assistance when an applicable state or local government is overwhelmed by the event and lacks the capability to perform, or contract for, the necessary work. (JP 3-28)

mission command — The conduct of military operations through decentralized execution based upon mission-type orders. (JP 3-31)

mission needs statement — A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. Also called **MNS.** (CJCSI 3180.01)

mission-oriented protective posture — A flexible system of protection against chemical, biological, radiological, and nuclear contamination in which personnel are required to wear only that protective clothing and equipment appropriate to the threat level, work rate imposed by the mission, temperature, and humidity. Also called **MOPP.** See also **mission-oriented protective posture gear.** (JP 3-11)

mission-oriented protective posture gear — Military term for individual protective equipment including suit, boots, gloves, mask with hood, first aid treatments, and decontamination kits issued to military members. Also called **MOPP gear.** See also **decontamination; mission-oriented protective posture.** (JP 3-11)

mission statement — A short sentence or paragraph that describes the organization's essential task(s), purpose, and action containing the elements of who, what, when, where, and why. See also **mission.** (JP 5-0)

mission type order — 1. An order issued to a lower unit that includes the accomplishment of the total mission assigned to the higher headquarters. 2. An order to a unit to perform a mission without specifying how it is to be accomplished. (JP 3-50)

mobile security force — A highly mobile and dedicated security force with the capability to defeat Level I and II threats in a joint security area. Also called **MSF.** (JP 3-10)

mobility — A quality or capability of military forces which permits them to move from place to place while retaining the ability to fulfill their primary mission. (JP 3-17)

mobility air forces — Air components and Service components that are assigned and/or routinely exercise command authority over mobility operations. Also called **MAF**. (JP 3-17)

mobility corridor — Areas that are relatively free of obstacles where a force will be canalized due to terrain restrictions allowing military forces to capitalize on the principles of mass and speed. (JP 2-01.3)

mobilization — 1. The process of assembling and organizing national resources to support national objectives in time of war or other emergencies. See also **industrial mobilization.** 2. The process by which the Armed Forces of the United States or part of them are brought to a state of readiness for war or other national emergency, whichincludes activating all or part of the Reserve Component as well as assembling and organizing personnel, supplies, and materiel. Also called **MOB.** (JP 4-05)

mobilization base — The total of all resources available, or that can be made available, to meet foreseeable wartime needs. (JP 4-05)

mobilization site — The designated location where a Reserve Component unit or individual mobilizes or moves after mobilization for further processing, training, and employment. See also **mobilization; mobilization station; Reserve Component.** (JP 4-05)

mobilization station — The designated military installation to which a Reserve Component unit or individual is moved for further processing, organizing, equipping, training, and employment and from which the unit or individual may move to an aerial port of

embarkation or seaport of embarkation. See also **mobilization; mobilization site; Reserve Component.** (JP 4-05)

mode (identification, friend or foe) — The number or letter referring to the specific pulse spacing of the signals transmitted by an interrogator or transponder used for radar identification of aircraft. (JP 3-01)

mode of transport — One of, or a combination of, the following modes used for a movement: a. inland surface transportation (rail, road, and inland waterway); b. sea transport (coastal and ocean); c. air transportation; and d. pipelines. (JP 4-09)

Modernized Integrated Database — The national level repository for the general military intelligence available to the entire Department of Defense Intelligence Information System community and, through Global Command and Control System integrated imagery and intelligence, to tactical units. Also called **MIDB.** (JP 2-01)

modified combined obstacle overlay — A joint intelligence preparation of the operational environment product used to portray the militarily significant aspects of the operational environment, such as obstacles restricting military movement, key geography, and military objectives. Also called **MCOO.** See also **joint intelligence preparation of the operational environment**. (JP 2-01.3)

moored mine — A contact or influence-operated mine of positive buoyancy held below the surface by a mooring attached to a sinker or anchor on the bottom. See also **mine.** (JP 3-15)

morale, welfare, and recreation — The merging of multiple unconnected disciplines into programs which improve unit readiness, promote fitness, build unit morale and cohesion, enhance quality of life, and provide recreational, social, and other support services. Also called **MWR.** (JP 1-0)

mortuary affairs — Provides for the search for, recovery, identification, preparation, and disposition of human remains of persons for whom the Services are responsible by status and executive order. Also called **MA.** See also **joint mortuary affairs office.** (JP 4-06)

mounting —1. All preparations made in anticipation of an operation, including assembly in the mounting area, preparation and maintenance within the mounting area, movement to loading points, and subsequent embarkation into ships, craft, or aircraft if applicable. 2. A carriage or stand upon which a weapon is placed. (JP 3-02.1)

mounting area — A general locality where assigned forces of an amphibious or airborne operation, with their equipment, are assembled, prepared, and loaded in ships and/or aircraft preparatory to an assault. See also **embarkation area**. (JP 3-02.1)

movement control — The planning, routing, scheduling, and control of personnel and cargo movements over lines of communications; includes maintaining in-transit visibility of forces and material through the deployment and/or redeployment process. See also **line of communications; movement control teams; non-unit cargo; non-unit-related personnel.** (JP 4-01.5)

movement control team — An Army team used to decentralize the execution of movement responsibilities on an area basis or at key transportation nodes. Also called **MCT.** (JP 4-09)

movement data — Those essential elements of information to schedule lift, obtain transportation assets, manage movement of forces, and report in-transit visibility of movements and associated forces (people, equipment, and supplies). (JP 4-09)

movement group — Those ships and embarked units that load out and proceed to rendezvous in the objective area. (JP 3-02)

movement phase — In amphibious operations, the period during which various elements of the amphibious force move from points of embarkation to the objective area. See also **amphibious force; amphibious operation.** (JP 3-02)

movement plan — In amphibious operations, the naval plan providing for the movement of the amphibious task force to the objective area. See also **amphibious operation; amphibious task force.** (JP 3-02)

movement requirement — A stated movement mode and time-phased need for the transport of units, personnel, and/or materiel from a specified origin to a specified destination. (JP 4-09)

movement schedule — A timetable developed to monitor or track the movement of a separate entity, whether it is a force requirement, cargo or personnel increment, or lift asset, that reflects the assignment of specific lift resources, shows a flow and workload at each location, and supports plan implementation. (JP 4-09)

movement table — A table giving detailed instructions or data for a move. (JP 4-09)

movement to contact — A form of the offense designed to develop the situation and to establish or regain contact. (JP 3-50)

multinational — Between two or more forces or agencies of two or more nations or coalition partners. See also **alliance**; **coalition.** (JP 5-0)

multinational doctrine — The agreed upon fundamental principles that guide the employment of forces of two or more nations in coordinated action toward a common objective. See also **doctrine; joint doctrine.** (JP 3-16)

multinational force — A force composed of military elements of nations who have formed an alliance or coalition for some specific purpose. Also called **MNF.** See also **multinational force commander; multinational operations.** (JP 1)

multinational force commander — A general term applied to a commander who exercises command authority over a military force composed of elements from two or more nations. Also called **MNFC.** See also **multinational force.** (JP 3-16)

multinational integrated logistic unit — An organization resulting when two or more nations agree to provide logistics assets to a multinational logistic force under the operational control of a multinational commander for the logistic support of a multinational force. Also called **MILU.** See also **logistic support; multinational.** (JP 4-08)

multinational logistics — Any coordinated logistic activity involving two or more nations supporting a multinational force conducting military operations under the auspices of an alliance or coalition, including those conducted under United Nations mandate. Also called **MNL**. See also **logistics; multinational.** (JP 4-08)

multinational operations — A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance. See also **alliance; coalition.** (JP 3-16)

multinational staff — A staff composed of personnel of two or more nations within the structure of a coalition or alliance. See also **integrated staff; joint staff.** (JP 3-16)

multipoint refueling system — KC-135 aircraft equipped with external wing-mounted pods to conduct drogue air refueling, while still maintaining boom air refueling capability on the same mission. Also called **MPRS.** See also **air refueling.** (JP 3-17)

multi-Service publication — A publication containing principles, terms, tactics, techniques, and procedures used and approved by the forces of two or more Services to perform a common military function consistent with approved joint doctrine. (CJCSM 5120.01)

multispectral imagery — The image of an object obtained simultaneously in a number of discrete spectral bands. Also called **MSI.** (JP 3-14)

multispot ship — Those ships certified to have two or more adjacent landing areas. See also **spot.** (JP 3-04)

munitions effectiveness assessment — Conducted concurrently and interactively with battle damage assessment, the assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and recommend any required changes to the methodology, tactics, weapon system, munitions, fusing, and/or weapon delivery parameters to increase force effectiveness. Munitions effectiveness assessment is primarily the responsibility of operations with required inputs and coordination from the

intelligence community. Also called **MEA.** See also **assessment; battle damage assessment.** (JP 2-01)

mutual support — That support which units render each other against an enemy, because of their assigned tasks, their position relative to each other and to the enemy, and their inherent capabilities. See also **close support; direct support; support.** (JP 3-31)

N

named area of interest — The geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected, usually to capture indications of adversary courses of action. Also called **NAI.** See also **area of interest.** (JP 2-01.3)

narcoterrorism — Terrorism that is linked to illicit drug trafficking. (JP 3-07.4)

National Capital Region — A geographic area encompassing the District of Columbia and eleven local jurisdictions in the State of Maryland and the Commonwealth of Virginia. Also called **NCR.** (JP 3-28)

National Communications System — The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability. Also called **NCS.** (JP 6-0)

National Defense Reserve Fleet — 1. Including the Maritime Administration Ready Reserve Force, a fleet composed of ships acquired and maintained by the Maritime Administration for use in mobilization or emergency. 2. Less the Maritime Administration Ready Reserve Force, a fleet composed of the older dry cargo ships, tankers, troop transports, and other assets in Maritime Administration's custody that are maintained at a relatively low level of readiness. Also called **NDRF.** See also **Maritime Administration Ready Reserve Force.** (JP 4-01.2)

national defense strategy — A document approved by the Secretary of Defense for applying the Armed Forces of the United States in coordination with Department of Defense agencies and other instruments of national power to achieve national security strategy objectives. Also called **NDS.** (JP 1)

National Detainee Reporting Center — The national-level center that accounts for all persons who pass through the care, custody, and control of the Department of Defense and that obtains and stores information concerning detainees and their confiscated personal property. Also called **NDRC.** (JP 3-63)

National Disaster Medical System — A coordinated partnership between Departments of Homeland Security, Health and Human Services, Defense, and Veterans Affairs established for the purpose of responding to the needs of casualties of a public health emergency. Also called **NDMS.** (JP 3-41)

national emergency — A condition declared by the President or the Congress by virtue of powers previously vested in them that authorize certain emergency actions to be undertaken in the national interest. See also **mobilization.** (JP 3-28)

National Incident Management System — A national crisis response system that provides a consistent, nationwide approach for federal, state, local, and tribal governments; the private sector; and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. Also called **NIMS.** (JP 3-41)

national intelligence — All intelligence, regardless of the source from which derived, and including that which is gathered within or outside of the United States, that pertains to more than one agency, and involves (1) threats to the United States, its people, property, or interests, (2) the development, proliferation, or use of weapons of mass destruction, or (3) any other matter bearing on US national or homeland security. (JP 2-01)

national intelligence estimate — A strategic estimate of the capabilities, vulnerabilities, and probable courses of action of foreign nations produced at the national level as a composite of the views of the intelligence community. Also called **NIE.** (JP 2-01)

National Military Command System — The priority component of the Global Command and Control System designed to support the President, Secretary of Defense, and Joint Chiefs of Staff in the exercise of their responsibilities. Also called **NMCS.** (JP 6-0)

national military strategy — A document approved by the Chairman of the Joint Chiefs of Staff for distributing and applying military power to attain national security strategy and national defense strategy objectives. Also called **NMS.** See also n**ational security strategy; strategy; theater strategy.** (JP 1)

national operations center — The primary national hub for domestic incident management operational coordination and situational awareness. Also called **NOC.** (JP 3-28)

national policy — A broad course of action or statements of guidance adopted by the government at the national level in pursuit of national objectives. (JP 1)

national security — A collective term encompassing both national defense and foreign relations of the United States with the purpose of gaining: a. A military or defense advantage over any foreign nation or group of nations; b. A favorable foreign relations position; or c. A defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert. See also **security.** (JP 1)

National Security Agency/Central Security Service Representative — The senior theater or military command representative of the Director, National Security Agency/Chief, Central Security Service in a specific country or military command headquarters who provides the Director, National Security Agency, with information on command plans requiring cryptologic support. The National Security Agency/Central Security Service representative serves as a special advisor to the combatant commander for cryptologic matters, to include signals intelligence, communications security, and computer security. Also called **NCR.** See also **counterintelligence.** (JP 2-01.2)

National Security Council — A governmental body specifically designed to assist the President in integrating all spheres of national security policy. Also called **NSC.** (JP 1)

national security interests — The foundation for the development of valid national objectives that define United States goals or purposes. (JP 1)

national security strategy — A document approved by the President of the United States for developing, applying, and coordinating the instruments of national power to achieve objectives that contribute to national security. Also called **NSS.** See also n**ational military strategy; strategy; theater strategy.** (JP 1)

national shipping authority — The organization within each Allied government responsible in time of war for the direction of its own merchant shipping. Also called **NSA.** (JP 4-01.2)

national special security event — A designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity. Also called **NSSE.** (JP 3-28)

national stock number — The 13-digit number that identifies a stock item consisting of the 4-digit federal supply classification code plus the 9-digit national item identification number and arranged as follows: 9999-00-999-9999. Also called **NSN.** (JP 4-09)

national support element — Any national organization or activity that supports national forces that are a part of a multinational force. See also **multinational force; support.** (JP 1)

National System for Geospatial Intelligence — The combination of technology, policies, capabilities, doctrine, activities, people, data, and organizations necessary to produce geospatial intelligence in an integrated, multi-intelligence environment. Also called **NSG.** (JP 2-03)

nation assistance — Assistance rendered to a nation by foreign forces within that nation's territory based on agreements mutually concluded between nations. (JP 3-0)

natural disaster — An emergency situation posing significant danger to life and property that results from a natural cause. See also **domestic emergencies.** (JP 3-29)

naval advanced logistic support site — An overseas location used as the primary transshipment point in the theater of operations for logistic support. Also called **NALSS.** See also **logistic support; naval forward logistic site; support; theater of operations.** (JP 3-35)

Naval Air Training and Operating Procedures Standardization manual — Series of general and specific aircraft procedural manuals that govern the operations of naval aircraft. Also called **NATOPS manual.** (JP 3-04)

naval beach group — A permanently organized naval command within an amphibious force composed of a commander and staff, a beachmaster unit, an amphibious construction battalion, and assault craft units, designed to provide an administrative group from which required naval tactical components may be made available to the attack force commander and to the amphibious landing force commander. Also called **NBG.** See also **shore party.** (JP 3-02)

naval construction force — The combined construction units of the Navy that are part of the operating forces and represent the Navy's capability for advanced base construction. Also called **NCF.** (JP 3-34)

naval forward logistic site — An overseas location, with port and airfield facilities nearby, which provides logistic support to naval forces within the theater of operations during major contingency and wartime periods. Also called **NFLS.** See also **logistic support; naval advanced logistic support site; staging.** (JP 3-35)

naval gunfire support — Fire provided by Navy surface gun systems in support of a unit or units tasked with achieving the commander's objectives. Also called **NGFS.** See also **naval surface fire support.** (JP 3-09)

naval operation — 1. A naval action (or the performance of a naval mission) that may be strategic, operational, tactical, logistic, or training. 2. The process of carrying on or training for naval combat in order to gain the objectives of any battle or campaign. (JP 3-32)

naval special warfare — A naval warfare specialty that conducts special operations with an emphasis on maritime, coastal, and riverine environments using small, flexible, mobile units operating under, on, and from the sea. Also called **NSW.** (JP 3-05)

naval special warfare group — A permanent Navy echelon III major command to which most naval special warfare forces are assigned for some operational and all administrative purposes. Also called **NSWG.** (JP 3-05)

naval special warfare task group — A provisional naval special warfare organization that plans, conducts, and supports special operations in support of fleet commanders and joint force special operations component commanders. Also called **NSWTG.** (JP 3-05)

naval special warfare task unit — A provisional subordinate unit of a naval special warfare task group. Also called **NSWTU.** See also **naval special warfare task group.** (JP 3-05)

naval surface fire support — Fire provided by Navy surface gun and missile systems in support of a unit or units. Also called **NSFS.** See also **fire support.** (JP 3-09.3)

navigation warfare — Deliberate defensive and offensive action to assure and prevent positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electronic warfare operations. Also called **NAVWAR.** (JP-3-14)

Navy cargo-handling battalion — A mobile logistic support unit that is organized, trained, and equipped to: a. load and offload Navy and Marine Corps cargo carried in maritime pre-positioning ships and merchant breakbulk or container ships in all environments; b. operate an associated temporary ocean cargo terminal; c. load and off-load Navy and Marine Corps cargo carried in military-controlled aircraft; and d. operate an associated expeditionary air cargo terminal. Also called **NCHB.** See also **maritime pre-positioning ships.** (JP 3-02.1)

Navy expeditionary logistics support group — The quick response cargo-handling units of the Navy specialize in open ocean cargo handling. Also called **NAVELSG.** (JP 4-01.6)

Navy special operations forces — Those Active and Reserve Component Navy forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. Also called **NAVSOF.** (JP 3-05)

Navy support element — The maritime pre-positioning force element that is tasked to conduct the off-load and ship-to-shore movement of maritime pre-positioned equipment and/or supplies. Also called **NSE.** (JP 3-02.1)

Navy-unique fleet essential aircraft — Combatant commander-controlled airlift assets deemed essential for providing air transportation in support of naval operations' transportation requirements. Also called **NUFEA.** (JP 3-17)

N-day — Day an active duty unit is notified for deployment or redeployment.

need to know — A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties. (JP 2-01.2)

negation — In space operations, active and offensive measures to deceive, disrupt, degrade, deny or destroy space capabilities being used to interfere with or attack United States/allied systems. See also **space control.** (JP 3-14)

nerve agent — A potentially lethal chemical agent that interferes with the transmission of nerve impulses. (JP 3-11)

net explosive weight — 1. The actual weight in pounds of explosive mixtures or compounds, including the trinitrotoluene equivalent of energetic material, that is used in determination of explosive limits and explosive quantity data arcs. (JP 4-09) 2. The total weight of all explosives substances (i.e., high explosive weight, propellant weight, and pyrotechnic

weight) in the ammunition or explosive, expressed in pounds, used for transportation purposes. Also called **NEW.** (DODM 6055.09)

networked munitions. Remotely controlled, interconnected, weapons system designed to provide rapidly emplaced ground-based countermobility and protection capability through scalable application of lethal and nonlethal means. (JP 3-15)

neutral — In combat and combat support operations, an identity applied to a track whose characteristics, behavior, origin, or nationality indicate that it is neither supporting nor opposing friendly forces. See also **suspect; unknown.** (JP 3-0)

neutrality — In international law, the attitude of impartiality during periods of war adopted by third states toward a belligerent and subsequently recognized by the belligerent, which creates rights and duties between the impartial states and the belligerent. (JP 3-0)

neutralize — 1. As pertains to military operations, to render ineffective or unusable. 2. To render enemy personnel or materiel incapable of interfering with a particular operation. 3. To render safe mines, bombs, missiles, and booby traps. 4. To make harmless anything contaminated with a chemical agent. (JP 3-0)

night vision device — Any electro-optical device that is used to detect visible and infrared energy and provide a visible image. Also called **NVD.** See also **forward-looking infrared; night vision goggle.** (JP 3-09.3)

night vision goggle — An electro-optical image intensifying device that detects visible and near-infrared energy, intensifies the energy, and provides a visible image for night viewing. Also called **NVG.** See also **night vision device.** (JP 3-09.3)

node — 1. A location in a mobility system where a movement requirement is originated, processed for onward movement, or terminated. (JP 3-17) 2. In communications and computer systems, the physical location that provides terminating, switching, and gateway access services to support information exchange. (JP 6-0) 3. An element of a system that represents a person, place, or physical thing. (JP 3-0)

no-fire area — An area designated by the appropriate commander into which fires or their effects are prohibited. Also called **NFA.** See also **fires.** (JP 3-09.3)

nonappropriated funds — Funds generated by Department of Defense personnel and their dependents used to augment funds appropriated by the Congress to provide a comprehensive, morale-building welfare, religious, educational, and recreational programs. Also called **NAF.** (JP 1-0)

nonbattle injury — A person who becomes a casualty due to circumstances not directly attributable to hostile action or terrorist activity. Also called **NBI.** (JP 4-02)

noncombatant evacuation operation — An operation whereby noncombatant evacuees are evacuated from a threatened area abroad, which includes areas facing actual or potential danger from natural or manmade disaster, civil unrest, imminent or actual terrorist activities, hostilities, and similar circumstances, that is carried out with the assistance of the Department of Defense. Also called **NEO.** See also **evacuation; noncombatant evacuees; operation; safe haven.** (JP 3-68)

noncombatant evacuation operation tracking system — An automated data processing hardware and software package that has the capability to provide evacuee in-transit visibility to combatant commanders and senior leadership during the conduct of a noncombatant evacuation operation. Also called **NTS.** (JP 3-68)

noncombatant evacuees — 1. United States citizens who may be ordered to evacuate by competent authority, and who are civilian employees of all agencies of the United States Government and their dependents, excepting dependents who are residents in the country concerned of their own volition; military personnel of the Armed Forces of the United States specifically designated for evacuation as noncombatants; and dependents of members of the Armed Forces of the United States. 2. United States citizens and non-United States citizens who may be authorized or assisted to evacuate by competent authority, and who are civilian employees of United States Government agencies and their dependents who are residents in the country concerned of their own volition, but express the willingness to be evacuated; private United States citizens and their dependents; military personnel of the Armed Forces of the United States and their dependents; and designated personnel, including dependents of persons ordered to evacuate, as prescribed by the Department of State. See also **noncombatant evacuation operation.** (JP 3-68)

nonconventional assisted recovery — Personnel recovery conducted by indigenous/surrogate personnel that are trained, supported, and led by special operations forces, unconventional warfare ground and maritime forces, or other government agencies' personnel that have been specifically trained and directed to establish and operate indigenous or surrogate infrastructures. Also called **NAR.** (JP 3-50)

nondestructive electronic warfare — Those electronic warfare actions, not including employment of wartime reserve modes, that deny, disrupt, or deceive rather than damage or destroy. See also **electronic warfare.** (JP 3-13.1)

nongovernmental organization — A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. Also called **NGO.** (JP 3-08)

nonlethal weapon — A weapon that is explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment. Also called **NLW.** (JP 3-28)

nonpersistent agent — A chemical agent that when released dissipates and/or loses its ability to cause casualties after 10 to 15 minutes. (JP 3-11)

nonproliferation — Actions to prevent the acquisition of weapons of mass destruction by dissuading or impeding access to, or distribution of, sensitive technologies, material, and expertise. Also called **NP.** See also **counterproliferation.** (JP 3-40)

nonscheduled units — Units of the landing force held in readiness for landing during the initial unloading period, but not included in either scheduled or on-call waves. (JP 3-02)

non-unit cargo — All equipment and supplies requiring transportation to an operational area, other than those identified as the equipment or accompanying supplies of a specific unit. (JP 4-01.5).

non-unit-related personnel — All personnel requiring transportation to or from an operational area, other than those assigned to a specific unit. Also called **NRP** or **NUP.** (JP 1-0)

no-strike list — A list of objects or entities characterized as protected from the effects of military operations under international law and/or rules of engagement. Also called **NSL.** See also **law of armed conflict.** (JP 3-60)

not mission capable, supply — Material condition indicating that systems and equipment are not capable of performing any of their assigned missions because of maintenance work stoppage due to a supply shortage. Also called **NMCS.** (JP 4-09)

nuclear incident — An unexpected incident involving a nuclear weapon, facility, or component, but not constituting a nuclear weapon(s) accident, resulting in any of the following: a. an increase in the possibility of explosion or radioactive contamination; b. errors committed in the assembly, testing, loading, or transportation of equipment, and/or the malfunctioning of equipment and materiel which could lead to an unintentional operation of all or part of the weapon arming and/or firing sequence, or which could lead to a substantial change in yield, or increased dud probability; and c. any act of God, unfavorable environment, or condition resulting in damage to the weapon, facility, or component. (JP 3-41)

nuclear weapon(s) accident — An unexpected incident involving nuclear weapons or radiological nuclear weapon components that results in any of the following; a. accidental or unauthorized launching, firing, or use by United States forces or United States supported allied forces of a nuclear-capable weapon system that could create the risk of an outbreak of war; b. nuclear detonation; c. nonnuclear detonation or burning of a nuclear weapon or radiological nuclear weapon component; d. radioactive contamination; e. seizure, theft, loss, or destruction of a nuclear weapon or radiological nuclear weapon component, including jettisoning; and f. public hazard, actual or implied. (JP 3-41)

nuisance minefield — A minefield laid to delay and disorganize the enemy and to hinder the use of an area or route. See also **minefield**. (JP 3-15)

numbered beach — In amphibious operations, a subdivision of a colored beach, designated for the assault landing of a battalion landing team or similarly sized unit, when landed as part of a larger force. (JP 3-02)

numbered fleet — A major tactical unit of the Navy immediately subordinate to a major fleet command and comprising various task forces, elements, groups, and units for the purpose of prosecuting specific naval operations. See also **fleet.** (JP 3-32)

Intentionally Blank

O

objective — 1. The clearly defined, decisive, and attainable goal toward which every operation is directed. 2. The specific target of the action taken which is essential to the commander's plan. See also **target.** (JP 5-0)

objective area — A geographical area, defined by competent authority, within which is located an objective to be captured or reached by the military forces. Also called **OA.** (JP 3-06)

obstacle — Any natural or man-made obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in personnel, time, and equipment on the opposing force. (JP 3-15)

obstacle belt — A brigade-level command and control measure, normally given graphically, to show where within an obstacle zone the ground tactical commander plans to limit friendly obstacle employment and focus the defense. See also **obstacle.** (JP 3-15)

obstacle clearing — The total elimination or neutralization of obstacles. (JP 3-15)

obstacle intelligence — Those collection efforts to detect the presence of enemy and natural obstacles, determine their types and dimensions, and provide the necessary information to plan appropriate combined arms breaching, clearance, or bypass operations to negate the impact on the friendly scheme of maneuver. Also called **OBSTINT.** (JP 3-15)

obstacle restricted areas — A command and control measure used to limit the type or number of obstacles within an area. See also **obstacle.** (JP 3-15)

obstacle zone — A division-level command and control measure, normally done graphically, to designate specific land areas where lower echelons are allowed to employ tactical obstacles. See also **obstacle.** (JP 3-15)

occupational and environmental health surveillance — The regular or repeated collection, analysis, archiving, interpretation, and dissemination of occupational and environmental health-related data for monitoring the health of, or potential health hazard impact on, a population and individual personnel, and for intervening in a timely manner to prevent, treat, or control the occurrence of disease or injury when determined necessary. (JP 4-02)

occupational and environmental health threats — Threats to the health of military personnel and to military readiness created by exposure to hazardous agents, environmental contamination, or toxic industrial materials. See also **health threat.** (JP 4-02)

occupied territory — Territory under the authority and effective control of a belligerent armed force and not being administered pursuant to peace terms, treaty, or other agreement, express or implied, with the civil authority of the territory. (JP 4-02)

oceanography — The study of the sea, embracing and integrating all knowledge pertaining to the sea and its physical boundaries, the chemistry and physics of seawater, and marine biology. (JP 3-59)

O-day — Off-load day.

offensive counterair — Offensive operations to destroy, disrupt, or neutralize enemy aircraft, missiles, launch platforms, and their supporting structures and systems both before and after launch, and as close to their source as possible. Also called **OCA.** See also **counterair; defensive counterair; operation.** (JP 3-01)

offensive counterair attack operations — Offensive action by any part of the joint force in support of the offensive counterair mission against surface targets which contribute to the enemy's air and missile capabilities. Also called **OCA attack operations.** See also **counterair; offensive counterair.** (JP 3-01)

offensive counterintelligence operation — A clandestine counterintelligence activity conducted for military, strategic, Department of Defense, or national counterintelligence and security purposes against a target having suspected or known affiliation with foreign intelligence entities, international terrorism, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department or the United States. The two types of offensive counterintelligence operations are double agent operation and controlled source operation. Also called **OFCO**. (JP 2-01.2)

offensive cyberspace operations — Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called **OCO.** (JP 3-12)

offensive space control — Those operations to prevent an adversary's hostile use of United States/third-party space capabilities and services or negate (deceive, disrupt, degrade, deny, or destroy) an adversary's efforts to interfere with or attack United States/allied space systems. Also called **OSC**. (JP 3-14)

office — An enduring organization that is formed around a specific function within a joint force commander's headquarters to coordinate and manage support requirements. (JP 3-33)

officer in tactical command — In maritime usage, the senior officer present eligible to assume command, or the officer to whom the senior officer has delegated tactical command. Also called **OTC.** (JP 3-32)

officer of the deck — 1. When underway, the officer designated by the commanding officer to be in charge of the ship, including its safe and proper operation. 2. When in port or at anchor, the officer of the deck is designated by the command duty officer, has similar responsibilities, and may be enlisted. Also called **OOD.** (JP 3-04)

official information — Information that is owned by, produced for or by, or is subject to the control of the United States Government. (JP 3-61)

offset costs — Costs for which funds have been appropriated that may not be incurred as a result of a contingency operation. See also **contingency operation.** (JP 1-06)

offshore bulk fuel system — The system used for transferring fuel from points offshore to reception facilities on the beach. Also called **OBFS**. See also **amphibious bulk liquid transfer system; offshore petroleum discharge system.** (JP 4-01.6)

offshore petroleum discharge system — Provides bulk transfer of petroleum directly from an offshore tanker to a beach termination unit located immediately inland from the high watermark. Also called **OPDS.** See also **facility; petroleum, oils, and lubricants; single-anchor leg mooring.** (JP 4-03)

off-the-shelf item — An item that has been developed and produced to military or commercial standards and specifications, is readily available for delivery from an industrial source, and may be procured without change to satisfy a military requirement. (JP 4-10)

on-call — 1. A term used to signify that a prearranged concentration, air strike, or final protective fire may be called for. 2. Preplanned, identified force or materiel requirements without designated time-phase and destination information. (JP 3-01)

on-call target — Planned target upon which fires or other actions are determined using deliberate targeting and triggered, when detected or located, using dynamic targeting. See also **dynamic targeting; on-call; operational area; planned target; target.** (JP 3-60)

on hand — The quantity of an item that is physically available in a storage location and contained in the accountable property book records of an issuing activity. (JP 4-09)

on-scene commander — 1. An individual in the immediate vicinity of an isolating event who temporarily assumes command of the incident. 2. The federal officer designated to direct federal crisis and consequence management efforts at the scene of a terrorist or weapons of mass destruction incident. Also called **OSC.** (JP 3-50)

on-station time — The time an aircraft can remain on station, which may be determined by endurance or orders. (JP 3-50)

open ocean — Ocean limit defined as greater than 12 nautical miles from shore, as compared with high seas that are over 200 nautical miles from shore. See also **contiguous zone.** (JP 3-32)

open-source information — Information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access. (JP 2-0)

open-source intelligence — Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. Also called **OSINT.** See also **intelligence.** (JP 2-0)

operating stocks — Fuel required to sustain daily operations and ensure fuel availability to support United States military forces worldwide. Also called **OS.** (JP 4-03)

operation — 1. A sequence of tactical actions with a common purpose or unifying theme. (JP 1) 2. A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission. (JP 3-0).

operational approach — A description of the broad actions the force must take to transform current conditions into those desired at end state. (JP 5-0)

operational area — An overarching term encompassing more descriptive terms (such as area of responsibility and joint operations area) for geographic areas in which military operations are conducted. Also called **OA.** See also **amphibious objective area; area of operations; area of responsibility; joint operations area; joint special operations area; theater of operations; theater of war.** (JP 3-0)

operational art — The cognitive approach by commanders and staffs — supported by their skill, knowledge, experience, creativity, and judgment — to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means. (JP 3-0)

operational chain of command — One of the two branches of the chain of command described in Joint Publication 1, *Doctrine for the Armed Forces of the United States*, through which command is exercised from the President through the Secretary of Defense to the combatant commanders, to whom forces are assigned and allocated via the global force management process. (DODI 8260.03)

operational characteristics — Those military characteristics that pertain primarily to the functions to be performed by equipment, either alone or in conjunction with other equipment; e.g., for electronic equipment, operational characteristics include such items as frequency coverage, channeling, type of modulation, and character of emission. (JP 5-0)

operational command structure — The organizational hierarchy through which operational authorities are exercised, as contrasted by the administrative command structure through which administrative leadership is exercised. (DODI 8260.03)

operational contract support — The process of planning for and obtaining supplies, services, and construction from commercial sources in support of joint operations. Also called **OCS**. (JP 4-10)

operational contract support integration cell — A cell established to coordinate, and integrate operational contract support actions across all primary and special staffs for an operational area. Also called **OCSIC.** (JP 4-10)

operational control — The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Also called **OPCON.** See also **combatant command; combatant command (command authority); tactical control.** (JP 1)

operational control authority — The naval commander responsible within a specified geographical area for the naval control of all merchant shipping under Allied naval control. Also called **OCA**. (JP 3-15)

operational decontamination — Decontamination carried out by an individual and/or a unit, restricted to specific parts of operationally essential equipment, materiel and/or working areas, in order to minimize contact and transfer hazards and to sustain operations. See also **decontamination; immediate decontamination; thorough decontamination.** (JP 3-11)

operational design — The conception and construction of the framework that underpins a campaign or major operation plan and its subsequent execution. See also **campaign; major operation.** (JP 5-0)

operational design element — A key consideration used in operational design. (JP 5-0)

operational energy — The energy required for training, moving, and sustaining military forces and weapons platforms for military operations. (JP 4-0)

operational environment — A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Also called **OE.** (JP 3-0)

operational exposure guidance — The maximum amount of nuclear/external ionizing radiation that the commander considers a unit may be permitted to receive while performing a particular mission or missions. Also called **OEG.** See also **radiation exposure status.** (JP 3-11)

operational intelligence — Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. See also **intelligence; strategic intelligence; tactical intelligence.** (JP 2-0)

operational level of war — The level of war at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. See also **strategic level of war; tactical level of war.** (JP 3-0)

operational limitation — An action required or prohibited by higher authority, such as a constraint or a restraint, and other restrictions that limit the commander's freedom of action, such as diplomatic agreements, rules of engagement, political and economic conditions in affected countries, and host nation issues. See also **constraint; restraint.** (JP 5-0)

operational necessity — A mission associated with war or peacetime operations in which the consequences of an action justify the risk of loss of aircraft and crew. See also **mission.** (JP 3-04)

operational pause — A temporary halt in operations. (JP 5-0)

operational preparation of the environment — The conduct of activities in likely or potential areas of operations to prepare and shape the operational environment. Also called **OPE**. (JP 3-05)

operational reach — The distance and duration across which a joint force can successfully employ military capabilities. (JP 3-0)

operational readiness — The capability of a unit/formation, ship, weapon system, or equipment to perform the missions or functions for which it is organized or designed. Also called **OR.** See also **combat readiness.** (JP 1-0)

operational reserve — An emergency reserve of men and/or materiel established for the support of a specific operation. (JP 5-0)

operational support airlift — Airlift movements of high-priority passengers and cargo with time, place, or mission-sensitive requirements. Also called **OSA.** (JP 3-17)

operational testing — A continuing process of evaluation that may be applied to either operational personnel or situations to determine their validity or reliability. (JP 4-02)

operation and maintenance — Maintenance and repair of real property, operation of utilities, and provision of other services such as refuse collection and disposal, entomology, snow removal, and ice alleviation. Also called **O&M.** (JP 3-34)

operation order — A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. Also called **OPORD.** (JP 5-0)

operation plan — 1. Any plan for the conduct of military operations prepared in response to actual and potential contingencies. 2. A complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment data. Also called **OPLAN.** See also **operation order.** (JP 5-0)

operations center — The facility or location on an installation, base, or facility used by the commander to command, control, and coordinate all operational activities. Also called **OC.** See also **base defense operations center.** (JP 3-07.2)

operations research — The analytical study of military problems undertaken to provide responsible commanders and staff agencies with a scientific basis for decision on action to improve military operations. Also called **operational research; operations analysis.** (JP 3-31)

operations security — A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. Also called **OPSEC.** See also **operations security indicators; operations security measures; operations security planning guidance; operations security vulnerability.** (JP 3-13.3)

operations security assessment — An evaluative process to determine the likelihood that critical information can be protected from the adversary's intelligence. (JP 3-13.3)

operations security countermeasures — Methods and means to gain and maintain essential secrecy about critical information. (JP 3-13.3)

operations security indicators — Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (JP 3-13.3)

operations security planning guidance — Guidance that defines the critical information requiring protection from the adversary and outlines provisional measures to ensure secrecy. (JP 3-13.3)

operations security survey — A collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes. (JP 3-13.3)

operations security vulnerability — A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (JP 3-13.3)

operations support element — An element that is responsible for all administrative, operations support and services support functions within the counterintelligence and human intelligence staff element of a joint force intelligence directorate. Also called **OSE.** (JP 2-01.2)

operations to restore order — Operations intended to halt violence and support, reinstate, or establish civil authorities so that indigenous police forces can effectively enforce the law and restore civil authority. See also **operation; peace operations.** (JP 3-07.3)

opportune lift — That portion of lift capability available for use after planned requirements have been met. (JP 4-02)

ordered departure — 1. A procedure by which the number of United States Government personnel, their dependents, or both are reduced at a foreign service post. 2. Mandatory departure of some or all categories of personnel and dependents to designated safe havens as directed by the Department of State, with the implementation of the theater evacuation plan. (JP 3-68)

order of battle — The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called **OB; OOB.** (JP 2-01.3)

ordnance — Explosives, chemicals, pyrotechnics, and similar stores, e.g., bombs, guns and ammunition, flares, smoke, or napalm. (JP 3-15)

ordnance handling — Applies to those individuals who engage in the breakout, lifting, or repositioning of ordnance or explosive devices in order to facilitate storage or stowage, assembly or disassembly, loading or downloading, or transporting. (JP 3-04)

organic — Assigned to and forming an essential part of a military organization as listed in its table of organization for the Army, Air Force, and Marine Corps, and are assigned to the operating forces for the Navy. (JP 1)

Organizational and Force Structure Construct — The standardized precepts for the digitization of hierarchical enterprise force structure data for Department of Defense-wide integration and use. Also called **OFSC**. (DODI 8260.03)

organization for combat — In amphibious operations, task organization of landing force units for combat, involving combinations of command, ground and aviation combat, combat support, and combat service support units for accomplishment of missions ashore. See also **amphibious operation; task organization.** (JP 3-02)

organization for embarkation — In amphibious operations, an organization consisting of temporary landing force task organizations established by the commander, landing force and a temporary organization of Navy forces established by the commander, amphibious task force for the purpose of simplifying planning and facilitating the execution of embarkation. See also **amphibious operation; embarkation; landing force; task organization.** (JP 3-02)

organization for landing — In amphibious operations, the specific tactical grouping of the landing force for the assault. (JP 3-02)

Organized Crime and Drug Enforcement Task Force — The network of regional task forces that coordinates federal law enforcement efforts to combat the national and international organizations that cultivate, process, and distribute illicit drugs. Also called **OCDETF.** (JP 3-07.4)

originating medical treatment facility — A medical facility that initially transfers a patient to another medical facility. (JP 4-02)

originator — The command by whose authority a message is sent, which includes the responsibility for the functions of the drafter and the releasing officer. (JP 2-01)

oscillating mine — A mine, hydrostatically controlled, which maintains a pre-set depth below the surface of the water independently of the rise and fall of the tide. See also **mine**. (JP 3-15)

other detainee — Person in the custody of the US Armed Forces who has not been classified as an enemy prisoner of war (article 4, Geneva Convention of 1949 Relative to the Treatment of Prisoners of War (GPW)), retained personnel (article 33, GPW), or civilian internee (article 78, Geneva Convention). Also called **OD.** See also **civilian internee; custody; detainee; prisoner of war; retained personnel.** (JP 1-0)

outer transport area — In amphibious operations, an area inside the antisubmarine screen to which assault transports proceed initially after arrival in the objective area. See also **inner transport area; transport area.** (JP 3-02)

outsized cargo — A single item that exceeds 1,000 inches long by 117 inches wide by 105 inches high in any one dimension. See also **oversized cargo.** (JP 4-01.6)

overhead persistent infrared — Those systems originally developed to detect and track foreign intercontinental ballistic missile systems. Also called **OPIR.** (JP 3-14)

overpressure — The pressure resulting from the blast wave of an explosion referred to as "positive" when it exceeds atmospheric pressure and "negative" during the passage of the wave when resulting pressures are less than atmospheric pressure. (JP 3-11)

Overseas Environmental Baseline Guidance Document — A set of objective criteria and management practices developed by the Department of Defense to protect human health and the environment. Also called **OEBGD.** (JP 3-34)

oversized cargo — 1. Large items of specific equipment such as a barge, side loadable warping tug, causeway section, powered, or causeway section, nonpowered that require transport by sea. 2. Air cargo exceeding the usable dimension of a 463L pallet loaded to the design height of 96 inches, but equal to or less than 1,000 inches in length, 117 inches in width, and 105 inches in height. See also **outsized cargo.** (JP 3-17)

over-the-horizon amphibious operation — An operational initiative launched from beyond visual and radar range of the shoreline. (JP 3-02)

overt — Activities that are openly acknowledged by or are readily attributable to the United States Government, including those designated to acquire information through authorized and open means without concealment. Overt information may be collected by observation, elicitation, or from knowledgeable human sources. (JP 2-01.2)

overt operation — An operation conducted openly, without concealment. See also **clandestine operation; covert operation.** (JP 2-01.2)

P

packup kit — Service-provided maintenance gear sufficient for a short-term deployment, including spare parts and consumables most commonly needed by the deployed helicopter detachment. Supplies are sufficient for a short-term deployment but do not include all material needed for every maintenance task. Also called **PUK.** (JP 3-04)

parallel chains of command — In amphibious operations, a parallel system of command, responding to the interrelationship of participating forces, wherein corresponding commanders are established at each subordinate level of all components to facilitate coordinated planning for, and execution of, the amphibious operation. (JP 3-02)

paramilitary forces — Forces or groups distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission. (JP 3-24)

partial mobilization — Expansion of the active Armed Forces resulting from action by Congress (up to full mobilization) or by the President (not more than 1,000,000 for not more than 24 consecutive months) to mobilize Ready Reserve Component units, individual reservists, and the resources needed for their support to meet the requirements of a war or other national emergency involving an external threat to the national security. (JP 4-05)

partner nation — A nation that the United States works with in a specific situation or operation. Also called **PN.** (JP 1)

passage of lines — An operation in which a force moves forward or rearward through another force's combat positions with the intention of moving into or out of contact with the enemy. (JP 3-18)

passive air defense — All measures, other than active air defense, taken to minimize the effectiveness of hostile air and missile threats against friendly forces and assets. See also **air defense.** (JP 3-01)

passive defense — Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative. See also **active defense.** (JP 3-60)

passive mine — 1. A mine whose anticountermining device has been operated preventing the firing mechanism from being actuated. 2. A mine which does not emit a signal to detect the presence of a target. (JP 3-15)

patient movement — The act or process of moving a sick, injured, wounded, or other person to obtain medical and/or dental care or treatment. Functions include medical regulating, patient evacuation, and en route medical care. See also **patient movement items; patient movement requirements center.** (JP 4-02)

patient movement items — The medical equipment and supplies required to support patients during aeromedical evacuation, which is part of a standardized list of approved safe-to-fly equipment. Also called **PMIs.** (JP 4-02)

patient movement policy — Command decision establishing the maximum number of days that patients may be held within the command for treatment. See also **evacuation.** (JP 4-02)

patient movement requirements center — 1. A joint activity that coordinates patient movement by functionally merging of joint medical regulating processes, Services' medical regulating processes, and patient movement evacuation requirements planning (transport to bed plan). 2. Term used to represent any theater, joint or the Global Patient Movement Requirements Center function. Also called **PMRC.** (JP 4-02)

Patriot — A point and limited area defense surface-to-air missile system capable of intercepting aircraft and theater missiles, including short-, medium-, and intermediate-range ballistic missiles in the terminal phase. (JP 3-01)

peace building — Stability actions, predominately diplomatic and economic, that strengthen and rebuild governmental infrastructure and institutions in order to avoid a relapse into conflict. Also called **PB.** See also **peace enforcement; peacekeeping; peacemaking; peace operations.** (JP 3-07.3)

peace enforcement — Application of military force, or the threat of its use, normally pursuant to international authorization, to compel compliance with resolutions or sanctions designed to maintain or restore peace and order. See also **peace building; peacekeeping; peacemaking; peace operations.** (JP 3-07.3)

peacekeeping — Military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement. See also **peace building; peace enforcement; peacemaking; peace operations.** (JP 3-07.3)

peacemaking — The process of diplomacy, mediation, negotiation, or other forms of peaceful settlements that arranges an end to a dispute and resolves issues that led to it. See also **peace building; peace enforcement; peacekeeping; peace operations.** (JP 3-07.3)

peace operations — A broad term that encompasses multiagency and multinational crisis response and limited contingency operations involving all instruments of national power with military missions to contain conflict, redress the peace, and shape the environment to support reconciliation and rebuilding and facilitate the transition to legitimate governance. Also called **PO.** See also **peace building; peace enforcement; peacekeeping; and peacemaking.** (JP 3-07.3)

performance work statement — A statement of work for performance based acquisitions that describe the results in clear, specific, and objective terms with measurable outcomes. Also called **PWS.** (JP 4-10)

period — The time it takes for a satellite to complete one orbit around the earth. (JP 3-14)

permissive environment — Operational environment in which host country military and law enforcement agencies have control as well as the intent and capability to assist operations that a unit intends to conduct. (JP 3-0)

persistent agent — A chemical agent that, when released, remains able to cause casualties for more than 24 hours to several days or weeks. (JP 3-11)

personal effects — All privately owned moveable, personal property of an individual. Also called **PE.** See also **mortuary affairs; personal property.** (JP 4-06)

personal locator beacon — An emergency device carried by individuals, to assist locating during personnel recovery. Also called **PLB.** See also **emergency locator beacon.** (JP 3-50)

personal property — Property of any kind or any interest therein, except real property, records of the United States Government, and naval vessels of the following categories: surface combatants, support ships, and submarines. (JP 4-06)

personal protective equipment — The protective clothing and equipment provided to shield or isolate a person from the chemical, physical, and thermal hazards that can be encountered at a hazardous materials incident. Also called **PPE.** See also **individual protective equipment.** (JP 3-11)

personal staff — Aides and staff officers handling special matters over which the commander wishes to exercise close personal control. (JP 3-33)

person authorized to direct disposition of human remains — A person, usually primary next of kin, who is authorized to direct disposition of human remains. Also called **PADD.** See also **mortuary affairs.** (JP 4-06)

person eligible to receive effects — The person authorized by law to receive the personal effects of a deceased military member. Receipt of personal effects does not constitute ownership. Also called **PERE.** See also **mortuary affairs; personal effects.** (JP 4-06)

personnel — Those individuals required in either a military or civilian capacity to accomplish the assigned mission. (JP 1-0)

personnel accountability — The process of identifying, capturing, and recording the personal identification information of an individual usually through the use of a database. (JP 1-0)

personnel effects inventory officer — An officer appointed to establish clear chain of custody for all personal effects of an individual from the time they establish control of the effects until they release the effect to mortuary affairs personnel. Also called **PEIO.** (JP 4-06)

personnel increment number — A seven-character, alphanumeric field that uniquely describes a non-unit-related personnel entry (line) in a Joint Operation Planning and Execution System time-phased force and deployment data. Also called **PIN.** (JP 5-0)

personnel recovery — The sum of military, diplomatic, and civil efforts to prepare for and execute the recovery and reintegration of isolated personnel. Also called **PR.** See also **combat search and rescue; evasion; personnel; recovery; search and rescue.** (JP 3-50)

personnel recovery coordination cell — The primary joint force component organization responsible for coordinating and controlling component personnel recovery missions. Also called **PRCC.** (JP 3-50)

personnel recovery reference product — A reference document for personnel recovery containing specific information on a particular country or region of interest. Also called **PRRP.** (JP 3-50)

personnel security investigation — An inquiry into the activities of an individual, designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability. Also called **PSI.** (JP 2-01)

personnel services support — Service-provided sustainment activities that support a Service member during both joint exercises and joint operations. Also called **PSS.** (JP 1-0)

petroleum, oils, and lubricants — A broad term that includes all petroleum and associated products used by the Armed Forces. Also called **POL.** (JP 4-01.6)

phase — In joint operation planning, a definitive stage of an operation or campaign during which a large portion of the forces and capabilities are involved in similar or mutually supporting activities for a common purpose. (JP 5-0)

phase line — A line utilized for control and coordination of military operations, usually an easily identified feature in the operational area. Also called **PL.** (JP 3-09)

phony minefield — An area free of live mines used to simulate a minefield, or section of a minefield, with the object of deceiving the enemy. See also **minefield.** (JP 3-15)

physical characteristics — Those military characteristics of equipment that are primarily physical in nature. (JP 3-60)

physical damage assessment — The estimate of the quantitative extent of physical damage to a target resulting from the application of military force. **See also battle damage assessment.** (JP 3-60)

physical security —1. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 3-0) 2. In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. See also **communications security; security.** (JP 6-0)

placement — An individual's proximity to information of intelligence interest. (JP 2-01.2)

plan for landing — In amphibious operations, a collective term referring to all individually prepared naval and landing force documents which, taken together, present in detail all instructions for execution of the ship-to-shore movement. (JP 3-02)

plan identification number — 1. A command-unique four-digit number followed by a suffix indicating the Joint Strategic Capabilities Plan year for which the plan is written. 2. A five-digit number representing the command-unique four-digit identifier, followed by a one-character, alphabetic suffix indicating the operation plan option, or a one-digit number numeric value indicating the Joint Strategic Capabilities Plan year for which the plan is written. Also called **PID.** (JP 5-0)

planned target — Target that is known to exist in the operational environment, upon which actions are planned using deliberate targeting, creating effects which support commander's objectives. There are two subcategories of planned targets: scheduled and on-call. See also **on-call target; operational area; scheduled target; target.** (JP 3-60)

planning and direction — In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. See also **intelligence process.** (JP 2-01)

planning factor — A multiplier used in planning to estimate the amount and type of effort involved in a contemplated operation. (JP 5-0)

planning factors database — Databases created and maintained by the Services for the purpose of identifying all geospatial information and services requirements for emerging and existing forces and systems. Also called **PFDB.** See also **geospatial information and services.** (JP 2-03)

planning order — A planning directive that provides essential planning guidance and directs the initiation of execution planning before the directing authority approves a military course of action. Also called **PLANORD.** See also **execution planning.** (JP 5-0)

planning phase — In amphibious operations, the phase normally denoted by the period extending from the issuance of the initiating directive up to the embarkation phase. See also **amphibious operation.** (JP 3-02)

planning team — A functional element within a joint force commander's headquarters established to solve problems related to a specific task or requirement, and which dissolves upon completion of the assigned task. (JP 3-33)

point defense — The defense or protection of special vital elements and installations; e.g., command and control facilities or air bases. (JP 3-52)

pointee-talkee — A language aid containing selected phrases in English opposite a translation in a foreign language used by pointing to appropriate phrases. See also **evasion aid.** (JP 3-50)

point of employment — In distribution operations, a physical location designated by the commander at the tactical level where force employment, emplacement, or commodity consumption occurs. (JP 4-09)

point of need — In distribution operations, a physical location within a desired operational area designated by the geographic combatant commander or subordinate commander as a receiving point for forces or materiel, for subsequent use or consumption. (JP 4-09)

point of origin — In distribution operations, the beginning point of a deployment, redeployment, or movement where forces or materiel are located. (JP 4-09)

polar orbit — A satellite orbit that passes over the North and South Poles on each orbit, has an angle of inclination relative to the equator of 90 degrees, and eventually passes over all points on the earth. (JP 3-14)

population at risk — The strength in personnel of a given force structure in terms of which casualty rates are stated. Also called **PAR.** (JP 4-02)

port complex — One or more port areas in which activities are geographically linked either because these areas are dependent on a common inland transport system or because they constitute a common initial destination for convoys. (JP 4-01.5)

port of debarkation — The geographic point at which cargo or personnel are discharged. Also called **POD.** See also **port of embarkation.** (JP 4-0)

port of embarkation — The geographic point in a routing scheme from which cargo or personnel depart. Also called **POE.** See also **port of debarkation.** (JP 4-01.2)

port operations group — A task-organized unit, located at the seaport of embarkation and/or debarkation that assists and provides support in the loading and/or unloading and staging of personnel, supplies, and equipment from shipping. Also called **POG.** See also **landing force support party; task organization.** (JP 3-35)

port security — The safeguarding of vessels, harbors, ports, waterfront facilities, and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts; accidents; thefts; or other causes of similar nature. See also **physical security; security.** (JP 3-10)

port support activity — A tailorable support organization composed of mobilization station assets that ensures the equipment of the deploying units is ready to load. Also called **PSA.** See also **support.** (JP 3-35)

positive control — A method of airspace control that relies on positive identification, tracking, and direction of aircraft within an airspace, conducted with electronic means by an agency having the authority and responsibility therein. (JP 3-52)

positive identification — An identification derived from observation and analysis of target characteristics including visual recognition, electronic support systems, non-cooperative target recognition techniques, identification friend or foe systems, or other physics-based identification techniques. (JP 3-01)

post-launch abort — Deliberate action taken post-separation to cause a precision munition to miss its target. Also called **PLA**. (JP 3-09.3)

precipitation static — Charged precipitation particles that strike antennas and gradually charge the antenna, which ultimately discharges across the insulator, causing a burst of static. Also called **P-STATIC.** (JP 3-13.1)

precise time and time interval — A reference value of time and time interval (frequency). Also called **PTTI**. (JP 3-59)

precision-guided munition — A guided weapon intended to destroy a point target and minimize collateral damage. Also called **PGM, smart weapon, smart munition.** (JP 3-03)

prelanding operations — Operations conducted by the amphibious force upon its arrival in the amphibious objective area or operational area and prior to H-hour and/or L-hour. (JP 3-02)

preparation of the environment — An umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations. Also called **PE.** (JP 3-05)

prepare to deploy order — An order issued by competent authority to move forces or prepare forces for movement (e.g., increase deployability posture of units). Also called **PTDO.** (JP 5-0)

preplanned air support — Air support in accordance with a program, planned in advance of operations. (JP 3-09.3)

pre-position — To place military units, equipment, or supplies at or near the point of planned use or at a designated location to reduce reaction time, and to ensure timely support of a specific force during initial phases of an operation. (JP 4-0)

pre-positioned war reserve stock — The assets that are designated to satisfy the pre-positioned war reserve materiel requirement. Also called **PWRS.** (JP 4-03)

presail — The time prior to a ship getting under way used to prepare for at-sea events. (JP 3-04)

Presidential Reserve Call-up — Provision of a public law (Title 10, United States Code, Section 12304) that provides the President a means to activate, without a declaration of national emergency, not more than 200,000 members of the Selected Reserve and the Individual Ready Reserve (of whom not more than 30,000 may be members of the Individual Ready Reserve), for not more than 365 days to meet the requirements of any operational mission, other than for disaster relief or to suppress insurrection. Also called **PRC.** See also **Individual Ready Reserve; mobilization; Selected Reserve.** (JP 4-05)

pressure mine — 1. In land mine warfare, a mine whose fuse responds to the direct pressure of a target. 2. In naval mine warfare, a mine whose circuit responds to the hydrodynamic pressure field of a target. See also **mine.** (JP 3-15)

prevention —In space usage, measures to preclude an adversary's hostile use of United States or third-party space systems and services. See also **space control.** (JP 3-14)

prevention of mutual interference — In submarine operations, procedures established to prevent submerged collisions between friendly submarines, between submarines and friendly surface ship towed bodies and arrays, and between submarines and any other hazards to submerged navigation. Also called **PMI**. (JP 3-32)

preventive maintenance — The care and servicing by personnel for the purpose of maintaining equipment and facilities in satisfactory operating condition by providing for systematic inspection, detection, and correction of incipient failures either before they occur or before they develop into major defects. (JP 4-02)

preventive medicine — The anticipation, communication, prediction, identification, prevention, education, risk assessment, and control of communicable diseases, illnesses and exposure to endemic, occupational, and environmental threats. Also called **PVNTMED.** (JP 4-02)

primary agency — The federal department or agency assigned primary responsibility for managing and coordinating a specific emergency support function in the National Response Framework. (JP 3-28)

primary control officer — In amphibious operations, the officer embarked in a primary control ship assigned to control the movement of landing craft, amphibious vehicles, and landing ships to and from a colored beach. Also called **PCO.** (JP 3-02)

primary control ship — In amphibious operations, a ship of the task force designated to provide support for the primary control officer and a combat information center control team for a colored beach. Also called **PCS.** (JP 3-02)

primary flight control — The controlling agency on air-capable ships that is responsible **for air traffic control of aircraft within 5 nautical miles of the ship. On most Coast** Guard cutters, primary flight control duties are performed by a combat information center, and the term "PRIFLY" is not used. Also called **PRIFLY.** (JP 3-04)

primary review authority — The organization, within the lead agent's chain of command, that is assigned by the lead agent to perform the actions and coordination necessary to develop and maintain the assigned joint publication under the cognizance of the lead agent. Also called **PRA.** See also **joint publication; lead agent.** (CJCSM 5120.01)

prime contract — A contract or contractual action entered into by the United States Government for the purpose of obtaining supplies, materials, equipment, or services of any kind. (JP 4-10)

prime vendor — A contracting process that provides commercial products to regionally grouped military and federal customers from commercial distributors using electronic commerce. Also called **PV.** See also **distribution system.** (JP 4-09)

principal federal official — The federal official designated by the Secretary of Homeland Security to act as his/her representative locally to oversee, coordinate, and execute the Secretary's incident management responsibilities under Homeland Security Presidential Directive 5. Also called **PFO.** (JP 3-41)

principal officer — The officer in charge of a diplomatic mission, consular office, or other Foreign Service post, such as a United States liaison office. (JP 3-08)

priority designator — A two-digit issue and priority code placed in military standard requisitioning and issue procedure requisitions to provide a means of assigning relative rankings to competing demands placed on the Department of Defense supply system. (JP 4-01)

priority intelligence requirement — An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or

other aspects of the operational environment. Also called **PIR.** See also **information requirements; intelligence; intelligence process; intelligence requirement.** (JP 2-01)

prisoner of war — A detained person (as defined in Articles 4 and 5 of the Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949) who, while engaged in combat under orders of his or her government, is captured by the armed forces of the enemy. Also called **POW or PW.** (JP 3-50)

private sector — An umbrella term that may be applied to any or all of the nonpublic or commercial individuals and businesses, specified nonprofit organizations, most of academia and other scholastic institutions, and selected nongovernmental organizations. (JP 3-57)

privity of contract — The legal relationship that exists between two contracting parties. (JP 4-10)

probability of damage — The probability that damage will occur to a target expressed as a percentage or as a decimal. Also called **PD.** (JP 3-60)

procedural control — A method of airspace control which relies on a combination of previously agreed and promulgated orders and procedures. (JP 3-52)

procedural identification — An identification based on observation and analysis of target behaviors including location and trajectory, as well as compliance with airspace control measures. (JP 3-01)

procedures — Standard, detailed steps that prescribe how to perform specific tasks. See also **tactics; techniques.** (CJCSM 5120.01)

procedure word — A word or phrase limited to radio telephone procedure used to facilitate communication by conveying information in a condensed standard form. Also called **proword.** (JP 3-09.3)

processing — A system of operations designed to convert raw data into useful information. (JP 2-0)

processing and exploitation — In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. See also **intelligence process.** (JP 2-01)

process owner — The head of a Department of Defense component assigned a responsibility by the Secretary of Defense when process improvement involves more than one Service or Department of Defense component. (JP 4-0)

procurement lead time — The interval in time between the initiation of procurement action and receipt of the products or services purchased as the result of such actions. (JP 4-10)

procuring contracting officer — A contracting officer who initiates and signs the contract. Also called **PCO.** See also **administrative contracting officer; contracting officer.** (JP 4-10)

production base — The total national industrial production capacity available for the manufacture of items to meet materiel requirements. (JP 4-05)

production logistics — That part of logistics concerning research, design, development, manufacture, and acceptance of materiel. In consequence, production logistics includes: standardization and interoperability, contracting, quality assurance, initial provisioning, transportability, reliability and defect analysis, safety standards, specifications and production processes, trials and testing (including provision of necessary facilities), equipment documentation, configuration control, and modifications.

production requirement — An intelligence requirement that cannot be met by current analytical products resulting in tasking to produce a new product that can meet this intelligence requirement. Also called **PR**. (JP 2-0)

proof — To verify that a breached lane is free of live mines by passing a mine roller or other mine-resistant vehicle through as the lead vehicle. (JP 3-15)

property — 1. Anything that may be owned. 2. As used in the military establishment, this term is usually confined to tangible property, including real estate and materiel. For special purposes and as used in certain statutes, this term may exclude such items as the public domain, certain lands, certain categories of naval vessels, and records of the Federal Government.

protected emblems — The red cross, red crescent, and other symbols that designate that persons, places, or equipment so marked have a protected status under the law of war. (JP 3-60)

protected frequencies — Friendly, generally time-oriented, frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electronic warfare operations are directed against hostile forces. See also **electronic warfare.** (JP 3-13.1)

protected persons/places — Persons (such as enemy prisoners of war) and places (such as hospitals) that enjoy special protections under the law of war. They may or may not be marked with protected emblems. (JP 1-04)

protection — 1. Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 3-0) 2. In space usage, active and passive defensive measures to ensure that United States and friendly space systems perform as designed by seeking to overcome an adversary's

attempts to negate them and to minimize damage if negation is attempted. See also **mission-oriented protective posture; space control.** (JP 3-14)

protection of shipping — The use of proportionate force, when necessary for the protection of US flag vessels and aircraft, US citizens (whether embarked in US or foreign vessels), and their property against unlawful violence. (JP 3-0)

protective clothing — Clothing especially designed, fabricated, or treated to protect personnel against hazards. (JP 3-11)

protective minefield — 1. In land mine warfare, a minefield employed to assist a unit in its local, close-in protection. 2. In naval mine warfare, a minefield emplaced in friendly territorial waters to protect ports, harbors, anchorages, coasts, and coastal routes. See also **minefield.** (JP 3-15)

provincial reconstruction team — A civil-military team designed to improve stability in a given area by helping build the legitimacy and effectiveness of a host nation local or provincial government in providing security to its citizens and delivering essential government services. Also called **PRT.** (JP 3-57)

public — In public affairs, a segment of the population with common attributes to which a military force can tailor its communication. See also **external audience; internal audience.** (JP 3-61)

public affairs — Communication activities with external and internal audiences. Also called **PA.** See also **command information; public information.** (JP 3-61)

public affairs assessment — An analysis of the news media and public environments to evaluate the degree of understanding about strategic and operational objectives and military activities and to identify levels of public support. See also **assessment; public affairs.** (JP 3-61)

public affairs guidance — Constraints and restraints established by proper authority regarding public communication activities. Also called **PAG.** See also **public affairs.** (JP 3-61)

public diplomacy — 1. Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. 2. In peace building, civilian agency efforts to promote an understanding of the reconstruction efforts, rule of law, and civic responsibility through public affairs and international public diplomacy operations. (JP 3-07.3)

public information — Within public affairs, information of a military nature, the dissemination of which is consistent with security and approved for public release. (JP 3-61)

public key infrastructure — An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for Department of Defense functional enterprise programs, including generation, production, distribution, control, and accounting of public key certificates. Also called **PKI.** (JP 2-03)

Intentionally Blank

Q

Q-route — A system of preplanned shipping lanes in mined or potentially mined waters used to minimize the area the mine countermeasures commander has to keep clear of mines in order to provide safe passage for friendly shipping. (JP 3-15)

quadruple container — A 57.5 inches x 96 inches x 96 inches container box with a metal frame, pallet base, and International Organization for Standardization corner fittings; four of these boxes can be lashed together to form a 20-foot American National Standards Institute or International Organization for Standardization intermodal container. Also called **QUADCON.** (JP 4-09)

qualifying entity — A non-governmental organization to which the Department of Defense may provide assistance for special events by virtue of statute, regulation, policy, or other approval by the Secretary of Defense or his or her authorized designee. (DODD 3025.18)

Intentionally Blank

R

radiation dose — The total amount of ionizing radiation absorbed by material or tissues. See also **exposure dose.** (JP 3-11)

radiation dose rate — Measurement of radiation dose per unit of time. (JP 3-11)

radiation exposure status — Criteria to assist the commander in measuring unit exposure to radiation based on total past cumulative dose, normally expressed in centigray. Also called **RES.** (JP 3-11)

radio frequency countermeasures — Any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. Also called **RF CM.** (JP 3-13.1)

radiological dispersal device — An improvised assembly or process, other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury. Also called **RDD.** (JP 3-11)

radiological exposure device — A radioactive source placed to cause injury or death. Also called **RED.** (JP 3-11)

raid — An operation to temporarily seize an area in order to secure information, confuse an adversary, capture personnel or equipment, or to destroy a capability culminating with a planned withdrawal. (JP 3-0)

railhead — A point on a railway where loads are transferred between trains and other means of transport. (JP 4-09)

Rangers — Rapidly deployable airborne light infantry organized and trained to conduct highly complex joint direct action operations in coordination with or in support of other special operations units of all Services. (JP 3-05)

rapid global mobility — The timely movement, positioning, and sustainment of military forces and capabilities across the range of military operations. See also **mobility.** (JP 3-17)

rationalization — Any action that increases the effectiveness of allied forces through more efficient or effective use of defense resources committed to the alliance. (JP 3-16)

R-day — Redeployment day.

reachback — The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 3-30)

readiness — The ability of military forces to fight and meet the demands of assigned missions. See also **national military strategy.** (JP 1)

Ready Reserve — The Selected Reserve and Individual Ready Reserve liable for active duty as prescribed by law (Title 10, United States Code, Sections 10142, 12301, and 12302). See also **active duty; Individual Ready Reserve; Selected Reserve.** (JP 4-05)

ready-to-load date — The date when a unit will be ready to move from the origin, i.e., mobilization station. Also called **RLD.** (JP 5-0)

Realistic Military Training — Department of Defense training conducted off federal property utilizing private or non-federal public property and infrastructure. (DODI 1322.28)

real property — Lands, buildings, structures, utilities systems, improvements, and appurtenances, thereto that includes equipment attached to and made part of buildings and structures, but not movable equipment. (JP 3-34)

reattack recommendation — An assessment, derived from the results of battle damage assessment and munitions effectiveness assessment, providing the commander systematic advice on reattack of a target. Also called **RR.** See also **assessment; battle damage assessment; munitions effectiveness assessment; target.** (JP 3-60)

receiving ship — The ship in a replenishment unit that receives the rig(s). (JP 4-03)

reception — 1. All ground arrangements connected with the delivery and disposition of air or sea drops. 2. Arrangements to welcome and provide secure quarters or transportation for defectors, escapees, evaders, or incoming agents. 3. The process of receiving, off-loading, marshalling, accounting for, and transporting of personnel, equipment, and materiel from the strategic and/or intratheater deployment phase to a sea, air, or surface transportation point of debarkation to the marshalling area. (JP 3-35)

recognition — 1. The determination by any means of the individuality of persons, or of objects such as aircraft, ships, or tanks, or of phenomena such as communications-electronics patterns. 2. In ground combat operations, the determination that an object is similar within a category of something already known. (JP 3-01)

recognition signal — Any prearranged signal by which individuals or units may identify each other. (JP 3-50)

reconnaissance — A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. Also called **RECON.** (JP 2-0)

recovery — 1. In air (aviation) operations, that phase of a mission that involves the return of an aircraft to a land base or platform afloat. (JP 3-52) 2. The retrieval of a mine from

the location where emplaced. (JP 3-15) 3. In personnel recovery, actions taken to physically gain custody of isolated personnel and return them to friendly control. (JP 3-50) 4. Actions taken to extricate damaged or disabled equipment for return to friendly control or repair at another location. See also **evader; evasion.** (JP 3-34)

recovery and reconstitution — 1. Those actions taken by one nation prior to, during, and following an attack by an enemy nation to minimize the effects of the attack, rehabilitate the national economy, provide for the welfare of the populace, and maximize the combat potential of remaining forces and supporting activities. 2. Those actions taken by a military force during or after operational employment to restore its combat capability to full operational readiness. See also **recovery.** (JP 3-35)

recovery mechanism — An indigenous or surrogate infrastructure that is specifically developed, trained, and directed by United States forces to contact, authenticate, support, move, and exfiltrate designated isolated personnel from uncertain or hostile areas back to friendly control. Also called **RM.** (JP 3-50)

recovery operations — Operations conducted to search for, locate, identify, recover, and return isolated personnel, human remains, sensitive equipment, or items critical to national security. (JP 3-50)

recovery site — In personnel recovery, an area from which isolated personnel can be recovered. See also **escapee; evader; evasion.** (JP 3-50)

recovery team — In personnel recovery, designated United States or United States-directed forces, that are specifically trained to operate in conjunction with indigenous or surrogate forces, and are tasked to contact, authenticate, support, move, and exfiltrate isolated personnel. Also called **RT.** (JP 3-50)

recovery vehicle — In personnel recovery, the vehicle on which isolated personnel are boarded and transported from the recovery site. (JP 3-50)

redeployment — The transfer or rotation of forces and materiel to support another joint force commander's operational requirements, or to return personnel, equipment, and materiel to the home and/or demobilization stations for reintegration and/or out-processing. See also **deployment.** (JP 3-35)

red team — An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. (JP 2-0)

reduced operating status — Military Sealift Command ships withdrawn from full operating status because of decreased operational requirements. Also called **ROS.** See also **Military Sealift Command.** (JP 4-01.2)

reduction — The creation of lanes through a minefield or obstacle to allow passage of the attacking ground force. (JP 3-15)

refraction — The process by which the direction of a wave is changed when moving into shallow water at an angle to the bathymetric contours. (JP 4-01.6)

refugee — A person who, owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion, is outside the country of his or her nationality and is unable or, owing to such fear, is unwilling to avail himself or herself of the protection of that country. See also **dislocated civilian; displaced person; evacuee; stateless person.** (JP 3-29)

regimental landing team — A task organization for landing composed of an infantry regiment reinforced by those elements that are required for initiation of its combat function ashore. (JP 3-02)

regional air defense commander — Commander, subordinate to the area air defense commander, who is responsible for air and missile defenses in the assigned regionand exercises authorities as delegated by the area air defense commander. Also called **RADC.** (JP 3-01)

regional response coordination center — A standing facility that is activated to coordinate regional response efforts, until a joint field office is established and/or the principal federal official, federal or coordinating officer can assume their National Response Framework coordination responsibilities. Also called **RRCC.** (JP 3-28)

regional satellite communications support center — United States Strategic Command operational element responsible for providing the operational communications planners with a point of contact for accessing and managing satellite communications resources. Also called **RSSC.** (JP 3-14)

regional security officer — A security officer responsible to the chief of mission (ambassador), for security functions of all United States embassies and consulates in a given country or group of adjacent countries. Also called **RSO.** (JP 3-10)

rehabilitative care — Therapy that provides evaluations and treatment programs using exercises, massage, or electrical therapeutic treatment to restore, reinforce, or enhance motor performance and restores patients to functional health allowing for their return to duty or discharge from the Service. Also called **restorative care.** See also **patient movement policy; theater.** (JP 4-02)

rehearsal phase — In amphibious operations, the period during which the prospective operation is practiced. See also **amphibious operation.** (JP 3-02)

reinforcing obstacles — Those obstacles specifically constructed, emplaced, or detonated through military effort and designed to strengthen existing terrain to disrupt, fix, turn, or block enemy movement. See also **obstacle.** (JP 3-15)

reintegrate — In personnel recovery, the task of providing medical care and psychological decompression to allow the conduct of appropriate debriefings to ultimately return recovered personnel back to duty and their family. (JP 3-50)

release altitude — Altitude of an aircraft above the ground at the time of ordnance release. (JP 3-09.3)

relief in place — An operation in which, by direction of higher authority, all or part of a unit is replaced in an area by the incoming unit and the responsibilities of the replaced elements for the mission and the assigned zone of operations are transferred to the incoming unit. (JP 3-07.3)

religious advisement — The practice of informing the commander on the impact of religion on joint operations to include, but not limited to: worship, rituals, customs, and practices of US military personnel, international forces, and the indigenous population; as well as the impact of military operations on the religious and humanitarian dynamics in the operational area. (JP 1-05)

religious affairs — The combination of religious support and religious advisement. (JP 1-05)

religious support — Chaplain-facilitated free exercise of religion through worship, religious and pastoral counseling services, ceremonial honors for the fallen, crisis intervention, and advice to the commander on ethical and moral issues, and morale as affected by religion. Also called **RS.** See also **combatant command chaplain; command chaplain; religious support team.** (JP 1-05)

religious support team — A team, comprised of at least one chaplain and one enlisted support person, that works together in designing, implementing, and executing the command religious program. Also called **RST.** See also **combatant command chaplain; command chaplain; religious support.** (JP 1-05)

remain-behind equipment — Unit equipment left by deploying forces at their bases when they deploy. (JP 4-05)

render safe procedures — The portion of the explosive ordnance disposal procedures involving the application of special explosive ordnance disposal methods and tools to provide for the interruption of functions or separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation. (JP 3-15.1)

rendezvous area — In an amphibious operation, the area in which the landing craft and amphibious vehicles rendezvous to form waves after being loaded, and prior to movement to the line of departure. (JP 3-02)

repairable item — An item that can be reconditioned or economically repaired for reuse when it becomes unserviceable. (JP 4-09)

repair cycle — The stages through which a repairable item passes from the time of its removal or replacement until it is reinstalled or placed in stock in a serviceable condition. (JP 4-09)

repatriation — 1. The procedure whereby American citizens and their families are officially processed back into the United States subsequent to an evacuation. See also **evacuation.** (JP 3-68) 2. The release and return of enemy prisoners of war to their own country in accordance with the 1949 Geneva Convention Relative to the Treatment of Prisoners of War. (JP 1-0)

replacement in kind — The provision of material and services for a logistic exchange of materials and services of equal value between the governments of eligible countries. Also called **RIK.** (JP 1-06)

reportable incident — Any suspected or alleged violation of Department of Defense policy or of other related orders, policies, procedures or applicable law, for which there is credible information. (JP 3-63)

request for assistance — A request based on mission requirements and expressed in terms of desired outcome, formally asking the Department of Defense to provide assistance to a local, state, tribal, or other federal agency. Also called **RFA.** (JP 3-28)

request for information — 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. 2. A term used by the National Security Agency/Central Security Service to state ad hoc signals intelligence requirements. Also called **RFI.** See also **intelligence.** (JP 2-0)

required delivery date — The date that a force must arrive at the destination and complete unloading. Also called **RDD.** (JP 5-0)

requirements determination — All activities necessary to develop, consolidate, coordinate, validate, approve, and prioritize joint force contract support requirements. (JP 4-10)

requirements development — The process of defining actual contract support requirements and capturing these requirements in acquisition ready contract support requirements packages. (JP 4-10)

requirements management system — A system for the management of theater and national imagery collection requirements that provides automated tools for users in support of submission, review, and validation of imagery nominations as requirements to be tasked on national or Department of Defense imagery collection, production, and exploitation resources. Also called **RMS.** See also **imagery.** (JP 2-01)

requiring activity — A military or other designated supported organization that identifies and receives contracted support during military operations. See also **supported unit.** (JP 4-10)

rescue combat air patrol — An aircraft patrol provided over that portion of an objective area in which recovery operations are being conducted for the purpose of intercepting and destroying hostile aircraft. Also called **RESCAP.** See also **combat air patrol.** (JP 3-50)

rescue coordination center — A unit, recognized by International Civil Aviation Organization, International Maritime Organization, or other cognizant international body, responsible for promoting efficient organization of search and rescue services and coordinating the conduct of search and rescue operations within a search and rescue region. Also called **RCC.** (JP 3-50)

reserve — 1. Portion of a body of troops that is kept to the rear, or withheld from action at the beginning of an engagement, in order to be available for a decisive movement. 2. Members of the uniformed Services who are not in active service but who are subject to call to active duty. 3. Portion of an appropriation or contract authorization held or set aside for future operations or contingencies and, in respect to which, administrative authorization to incur commitments or obligations has been withheld. See also **operational reserve.** (JP 4-05)

Reserve Component — The Armed Forces of the United States Reserve Component consists of the Army National Guard of the United States, the Army Reserve, the Navy Reserve, the Marine Corps Reserve, the Air National Guard of the United States, the Air Force Reserve, and the Coast Guard Reserve. Also called **RC.** See also **component; reserve.** (JP 4-05)

reserved obstacles — Those demolition obstacles that are deemed critical to the plan for which the authority to detonate is reserved by the designating commander. See also **obstacle.** (JP 3-15)

reset — A set of actions to restore equipment to a desired level of combat capability commensurate with a unit's future mission. (JP 4-0)

resettled person — A refugee or an internally displaced person wishing to return somewhere other than his or her previous home or land within the country or area of original displacement. (JP 3-29)

residual forces — Undeployed United States forces that have an immediate combat potential for continued military operations, and that have been deliberately withheld from utilization. (JP 4-09)

residual radiation — Nuclear radiation caused by fallout, artificial dispersion of radioactive material, or irradiation that results from a nuclear explosion and persists longer than one minute after burst. See also **contamination; initial radiation.** (JP 3-11)

resistance movement — An organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability. (JP 3-05)

resource management — A financial management function that provides advice and guidance to the commander to develop command resource requirements. Also called **RM.** See also **financial management.** (JP 1-06)

resources — The forces, materiel, and other assets or capabilities apportioned or allocated to the commander of a unified or specified command. (JP 1)

rest and recuperation — The withdrawal of individuals from combat or duty in a combat area for short periods of rest and recuperation. Also called **R&R.** (JP 1-0)

restraint — In the context of joint operation planning, a requirement placed on the command by a higher command that prohibits an action, thus restricting freedom of action. See also **constraint; operational limitation.** (JP 5-0)

restricted area — 1. An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize interference between friendly forces. 2. An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry. See also **restricted areas (air).** (JP 3-34)

restricted areas (air) — Designated areas established by appropriate authority over which flight of aircraft is restricted. See also **restricted area**. (JP 3-52)

restricted items list — A document listing those logistic goods and services for which nations must coordinate any contracting activity with a commander's centralized contracting organization. (JP 4-08)

restricted operations zone — Airspace reserved for specific activities in which the operations of one or more airspace users is restricted. Also called **ROZ.** (JP 3-52)

restricted reporting — Reporting option that allows sexual assault victims to confidentially disclose the assault to specified individual and receive medical treatment without triggering an official investigation. (JP 1-0)

restricted target — A valid target that has specific restrictions placed on the actions authorized against it due to operational considerations. See also **target.** (JP 3-60)

restricted target list — A list of restricted targets nominated by elements of the joint force and approved by the joint force commander or directed by higher authorities. Also called **RTL.** See also **restricted target; target.** (JP 3-60)

restrictive fire area — An area in which specific restrictions are imposed and into which fires that exceed those restrictions will not be delivered without coordination with the establishing headquarters. Also called **RFA.** See also **fires.** (JP 3-09)

restrictive fire line — A line established between converging friendly surface forces that prohibits fires or their effects across that line. Also called **RFL.** See also **fires.** (JP 3-09)

resupply — The act of replenishing stocks in order to maintain required levels of supply. (JP 4-09)

resuscitative care — Advanced emergency medical treatment required to prevent immediate loss of life or limb and to attain stabilization to ensure the patient could tolerate evacuation. (JP 4-02)

retained personnel — Detainees who fall into one of the following categories: a. Designated enemy medical personnel and medical staff administrators who are exclusively engaged in either the search for, collection, transport, or treatment of the wounded or sick, or the prevention of disease; b. Staff of National Red Cross and Red Crescent Societies and that of other volunteer aid societies, duly recognized and authorized by their governments to assist medical service personnel of their own armed forces, provided they are exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and provided that the staff of such societies are subject to military laws and regulations; c. Chaplains attached to enemy armed forces. Also called **RP.** See also **personnel.** (JP 3-63)

Retired Reserve — All reserve members who receive retirement pay on the basis of their active duty and/or reserve service; those members who are otherwise eligible for retirement pay but have not reached age 60 and who have not elected discharge and are not voluntary members of the Ready Reserve or Standby Reserve. See also **active duty; Ready Reserve; Standby Reserve.** (JP 4-05)

retrograde — The process for the movement of non-unit equipment and materiel from a forward location to a reset (replenishment, repair, or recapitalization) program or to another directed area of operations to replenish unit stocks, or to satisfy stock requirements. (JP 4-09)

returned to military control — The status of a person whose casualty status of "duty status - whereabouts unknown" or "missing" has been changed due to the person's return or recovery by US military authority. Also called **RMC.**

returnee — A displaced person who has returned voluntarily to his or her former place of residence. (JP 3-29)

return to base — An order to proceed to the point indicated by the displayed information or by verbal communication. Also called **RTB.** (JP 3-01)

revolving fund account — An account authorized by specific provisions of law to finance a continuing cycle of business-type operations, and which are authorized to incur obligations and expenditures that generate receipts. (JP 1-06)

riot control agent — Any chemical, not listed in a schedule of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction that can produce rapidly in humans sensory irritation or disabling physical effects that disappear within a short time following termination of exposure. Also called **RCA.** See also **chemical warfare.** (JP 3-11)

rising mine — In naval mine warfare, a mine having positive buoyancy which is released from a sinker by a ship influence or by a timing device. (JP 3-15)

risk — Probability and severity of loss linked to hazards. See also **hazard; risk management.** (JP 5-0)

risk assessment — The identification and assessment of hazards (first two steps of risk management process). Also called **RA.** (JP 3-07.2)

risk management — The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. Also called **RM.** See also **risk.** (JP 3-0)

riverine operations — Operations conducted by forces organized to cope with and exploit the unique characteristics of a riverine area, to locate and destroy hostile forces, and/or to achieve or maintain control of the riverine area. (JP 3-32)

role specialist nation — A nation that has agreed to assume responsibility for providing a particular class of supply or service for all or part of the multinational force. Also called **RSN.** See also **lead nation; multinational force.** (JP 4-08)

roll-on/roll-off discharge facility — A platform made up of causeway sections that provide a means of embarking and disembarking vehicles from a roll-on and roll-off ship at sea to lighterage. Also called **RRDF.** See also **facility; lighterage.** (JP 4-01.6)

rough terrain container handler — A piece of materials handling equipment used to pick up and move containers. Also called **RTCH.** (JP 4-01.6)

rules of engagement — Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called **ROE.** See also **law of war.** (JP 1-04)

ruse — In military deception, a trick of war designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system. (JP 3-13.4)

Intentionally Blank

S

sabotage — An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources. (JP 2-01.2)

safe haven — 1. Designated area(s) to which noncombatant evacuees of the United States Government's responsibility and commercial vehicles and materiel may be evacuated during a domestic or other valid emergency. (JP 3-68) 2. A protected body of water or the well deck of an amphibious ship used by small craft operating offshore for refuge from storms or heavy seas. (JP 4-01.6)

safe house — An innocent-appearing house or premises established by an organization for the purpose of conducting clandestine or covert activity in relative security. (JP 3-07.2)

safing — As applied to weapons and ammunition, the changing from a state of readiness for initiation to a safe condition. Also called **de-arming.** (JP 3-09.3)

salvage — 1. Property that has some value in excess of its basic material content but is in such condition that it has no reasonable prospect of use for any purpose as a unit and its repair or rehabilitation for use as a unit is clearly impractical. 2. The saving or rescuing of condemned, discarded, or abandoned property, and of materials contained therein for reuse, refabrication, or scrapping. (JP 4-0)

sanction enforcement — Operations that employ coercive measures to control the movement of certain types of designated items into or out of a nation or specified area. (JP 3-0)

scheduled target — Planned target upon which fires or other actions are scheduled for prosecution at a specified time. See also **planned target; target.** (JP 3-60)

schedule of fire — Groups or series of fires that are fired in a definite sequence according to a definite program. (JP 3-09)

scheme of fires — The detailed, logical sequence of targets and fire support events to find and engage targets to support the commander's objectives. (JP 3-09)

scheme of maneuver — The central expression of the commander's concept for operations that governs the design of supporting plans or annexes of how arrayed forces will accomplish the mission. (JP 5-0)

scientific and technical intelligence — The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information that covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development

related thereto; and the production methods employed for their manufacture. Also called **S&TI.** See also **intelligence; technical intelligence.** (JP 2-01)

screening — In intelligence, the evaluation of an individual or a group of individuals to determine their potential to answer collection requirements or to identify individuals who match a predetermined source profile coupled with the process of identifying and assessing the areas of knowledge, cooperation, and possible approach techniques for an individual who has information of intelligence value. (JP 2-01.2)

sea areas — Areas in the amphibious objective area designated for the stationing of amphibious task force ships. See also **amphibious objective area; fire support area; inner transport area; sea echelon area.** (JP 3-02)

sea barge — A type of barge-ship that can carry up to 38 loaded barges and also carry tugs, stacked causeway sections, various watercraft, or heavy-lift equipment to better support joint logistics over-the-shore operations. (JP 4-01.2)

seabasing — The deployment, assembly, command, projection, reconstitution, sustainment, and re-employment of joint power from the sea without reliance on land bases within the operational area. See also **amphibious operation.** (JP 3-02)

sea control operations — The employment of forces to destroy enemy naval forces, suppress enemy sea commerce, protect vital sea lanes, and establish local military superiority in vital sea areas. See also **land control operations.** (JP 3-32)

sea echelon — A portion of the amphibious warfare ships or other ships that withdraws from or remains out of the transport area during an amphibious landing and operates in designated areas to seaward in an on-call or unscheduled status. (JP 3-02)

sea echelon area — In amphibious operations, an area to seaward of a transport area from which ships are phased into the transport area, and to which ships withdraw from the transport area. (JP 3-02)

sea echelon plan — In amphibious operations, the distribution plan for amphibious shipping in the transport area to minimize losses due to enemy attack by weapons of mass destruction and to reduce the area to be swept of mines. See also **amphibious operation.** (JP 3-02)

SEAL delivery vehicle team — United States Navy forces organized, trained, and equipped to conduct special operations with SEAL delivery vehicles, dry deck shelters, and other submersible platforms. (JP 3-05)

sealift enhancement features — Special equipment and modifications that adapt merchant-type dry cargo ships and tankers to specific military missions. Also called **SEFs.** See also **Military Sealift Command; Ready Reserve.** (JP 4-01.2)

SEAL team — United States Navy forces organized, trained, and equipped to conduct special operations with an emphasis on maritime, coastal, and riverine environments. (JP 3-05)

seaport — A land facility designated for reception of personnel or materiel moved by sea, and that serves as an authorized port of entrance into or departure from the country in which located. See also **port of debarkation; port of embarkation.** (JP 4-01.2)

search — A systematic reconnaissance of a defined area, so that all parts of the area have passed within visibility. (JP 3-50)

search and rescue — The use of aircraft, surface craft, submarines, and specialized rescue teams and equipment to search for and rescue distressed persons on land or at sea in a permissive environment. Also called **SAR.** See also **combat search and rescue; isolated personnel; joint personnel recovery center; personnel recovery coordination cell.** (JP 3-50)

search and rescue numerical encryption grid — A predesignated ten-letter word without repeated letters used exclusively by recovery forces or isolated personnel to encrypt numerical data such as position, time, and/or headings in a covert manner. Also called **SARNEG.** (JP 3-50)

search and rescue point — A predesignated specific location, relative to which isolated personnel provide their position to recovery forces. Also called **SARDOT.** (JP 3-50)

search and rescue region — An area of defined dimensions, recognized by the International Civil Aviation Organization, International Maritime Organization, or other cognizant international body, and associated with a rescue coordination center within which search and rescue services are provided. **(**JP 3-50)

sea state — A scale that categorizes the force of progressively higher seas by wave height. (JP 4-01.6)

secondary loads — Unit equipment, supplies, and major end items that are transported in the beds of organic vehicles. (JP 3-02.1)

secret — Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. (EO 13526)

SECRET Internet Protocol Router Network — The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called **SIPRNET.** See also **Defense Information Systems Network.** (JP 6-0)

section — 1. As applied to ships or naval aircraft, a tactical subdivision of a division. 2. A subdivision of an office, installation, territory, works, or organization; especially a major subdivision of a staff. 3. A tactical unit of the Army and Marine Corps smaller than a platoon and larger than a squad. 4. An area in a warehouse extending from one wall to the next; usually the largest subdivision of one floor. (JP 3-33)

sector air defense commander — Commander subordinate to an area/regional air defense commander, who is responsible for air and missile defenses in the assigned sector and exercises authorities delegated by the area/regional air defense commander. Also called **SADC.** (JP 3-01)

security — 1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 3-10) 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JP 3-10) 3. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. See also **national security.** (JP 2-0)

security assistance — Group of programs authorized by the Foreign Assistance Act of 1961, as amended, and the Arms Export Control Act of 1976, as amended, or other related statutes by which the United States provides defense articles, military training, and other defense-related services by grant, loan, credit, or cash sales in furtherance of national policies and objectives. Security assistance is an element of security cooperation funded and authorized by Department of State to be administered by Department of Defense/Defense Security Cooperation Agency. Also called **SA.** See also **security cooperation.** (JP 3-22)

security classification — A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. There are three such categories: **top secret**, **secret**, and **confidential**. See also **classification; security**. (EO 13526)

security clearance — An administrative determination by competent authority that an individual is eligible for access to classified information. (JP 1-0)

security cooperation — All Department of Defense interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation. Also called **SC**. See also **security assistance.** (JP 3-22)

security cooperation organization — All Department of Defense elements located in a foreign country with assigned responsibilities for carrying out security assistance/cooperation management functions. It includes military assistance

advisory groups, military missions and groups, offices of defense and military cooperation, liaison groups, and defense attaché personnel designated to perform security assistance/cooperation functions. Also called **SCO.** (JP 3-22)

security countermeasures — Those protective activities required to prevent espionage, sabotage, theft, or unauthorized use of classified or controlled information, systems, or material of the Department of Defense. See also **counterintelligence.** (JP 2-01.2)

security force assistance — The Department of Defense activities that contribute to unified action by the US Government to support the development of the capacity and capability of foreign security forces and their supporting institutions. Also called **SFA.** (JP 3-22)

security forces — Duly constituted military, paramilitary, police, and constabulary forces of a state. (JP 3-22)

security review — The process of reviewing information and products prior to public release to ensure the material will not jeopardize ongoing or future operations. See also **security.** (JP 3-61)

security sector reform — A comprehensive set of programs and activities undertaken to improve the way a host nation provides safety, security, and justice. Also called **SSR.** (JP 3-07)

security service — Entity or component of a foreign government charged with responsibility for counterespionage or internal security functions. (JP 2-01.2)

sedition — Willfully advocating or teaching the duty or necessity of overthrowing the US government or any political subdivision by force or violence. See also **counterintelligence.** (JP 2-01.2)

segregation — In detainee operations, the removal of a detainee from other detainees and their environment for legitimate purposes unrelated to interrogation, such as when necessary for the movement, health, safety, and/or security of the detainee, the detention facility, or its personnel. (JP 3-63)

seize — To employ combat forces to occupy physically and to control a designated area. (JP 3-18)

seizures — In counterdrug operations, includes drugs and conveyances seized by law enforcement authorities and drug-related assets confiscated based on evidence that they have been derived from or used in illegal narcotics activities. See also **counterdrug operations; law enforcement agency.** (JP 3-07.4)

Selected Reserve — Those units and individuals within the Ready Reserve designated by their respective Services and approved by the Joint Chiefs of Staff as so essential to initial

wartime missions that they have priority over all other reserves. See also **Ready Reserve.** (JP 4-05)

selective identification feature — A capability that, when added to the basic identification friend or foe system, provides the means to transmit, receive, and display selected coded replies. (JP 3-52)

selective loading — The arrangement and stowage of equipment and supplies aboard ship in a manner designed to facilitate issues to units. (JP 3-02.1)

selective mobilization — Expansion of the active Armed Forces resulting from action by Congress or the President to mobilize Reserve Component units, Individual Ready Reservists, and the resources needed for their support to meet the requirements of a domestic emergency that is not the result of an enemy attack. (JP 4-05)

selective off-loading — The capability to access and off-load vehicles, supplies, and equipment without having to conduct a major reconfiguration or total off-load; influenced by the number and types of ships allocated, and the space made available for the embarkation of the landing force. (JP 3-02.1)

selective unloading — In an amphibious operation, the controlled unloading from amphibious warfare ships, and movement ashore, of specific items of cargo at the request of the landing force commander. (JP 3-02)

senior airfield authority — An individual designated by the joint force commander to be responsible for the control, operation, and maintenance of an airfield to include the runways, associated taxiways, parking ramps, land, and facilities whose proximity directly affects airfield operations. Also called SAA. (JP 3-17)

senior contracting official — The staff official designated by a Service head of contracting activity to execute theater support contracting authority for a specific command and/or operational area. Also called **SCO.** (JP 4-10)

senior meteorological and oceanographic officer — Meteorological and oceanographic officer responsible for assisting the combatant commander and staff in developing and executing operational meteorological and oceanographic service concepts in support of a designated joint force. Also called **SMO.** See also **meteorological and oceanographic.** (JP 3-59)

sensitive — An agency, installation, person, position, document, material, or activity requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. (JP 2-01)

sensitive compartmented information — All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of

compartmentation have been or will be formally established. (These controls are over and above the provisions of DOD 5200.1-R, Information Security Program Regulation.) Also called **SCI.** (JP 2-01)

sensitive compartmented information facility — An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed, where procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular sensitive compartmented information authorized for use or storage within the sensitive compartmented information facility. Also called **SCIF.** See also **sensitive compartmented information.** (JP 2-01)

sensitive site — A geographically limited area that contains, but is not limited to, adversary information systems, war crimes sites, critical government facilities, and areas suspected of containing high value targets. (JP 3-31)

sequel — The subsequent major operation or phase based on the possible outcomes (success, stalemate, or defeat) of the current major operation or phase. See also **branch.** (JP 5-0)

serial — 1. An element or a group of elements within a series that is given a numerical or alphabetical designation for convenience in planning, scheduling, and control. 2. A group of people, vehicles, equipment, or supplies and is used in airborne, air assault, amphibious operations, and convoys. (JP 3-02)

serial assignment table — A table that is used in amphibious operations and shows the serial number, the title of the unit, the approximate number of personnel; the material, vehicles, or equipment in the serial; the number and type of landing craft and/or amphibious vehicles required to boat the serial; and the ship on which the serial is embarked. (JP 3-02)

Service — A branch of the Armed Forces of the United States, established by act of Congress, which are: the Army, Marine Corps, Navy, Air Force, and Coast Guard. (JP 1)

Service-common — Equipment, material, supplies, and services including base operating support adopted by a Service to support its own forces and those assigned to the combatant commands; items and services defined as Service-common by one Service are not necessarily Service-common for all other Services. See also **special operations-peculiar.** (JP 3-05)

Service component command — A command consisting of the Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under that command, including the support forces that have been assigned to a combatant command or further assigned to a subordinate unified command or joint task force. See also **component; functional component command.** (JP 1)

Service-organic transportation assets — Transportation assets that are assigned to a Military Department for functions of the Secretaries of the Military Departments set forth in Title 10, United States Code, Sections 3013(b), 5013(b), and 8013(b). (JP 4-01)

Service-unique container — Any 20- or 40-foot International Organization for Standardization container procured or leased by a Service to meet Service-unique requirements. See also **common-use container; component-owned container.** (JP 4-09)

sexual assault forensic examination kit — The medical and forensic examination kit used to ensure controlled procedures and safekeeping of any bodily specimens in a sexual assault case. Also called **SAFE kit.** (JP 1-0)

sexual assault prevention and response program — A Department of Defense program for the Military Departments and Department of Defense components that establishes sexual assault prevention and response policies to be implemented worldwide. Also called **SAPR program.** (JP 1-0)

sexual assault response coordinator — The single point of contact at an installation or within a geographic area who overseas sexual assault awareness, prevention, and response. Also called **SARC.** (JP 1-0)

shelter — An International Organization for Standardization container outfitted with live- or work-in capability. (JP 4-09)

shielding — 1. Material of suitable thickness and physical characteristics used to protect personnel from radiation during the manufacture, handling, and transportation of fissionable and radioactive materials. 2. Obstructions that tend to protect personnel or materials from the effects of a nuclear explosion. (JP 3-11)

ship-to-shore movement — That portion of the action phase of an amphibious operation that includes the deployment of the landing force from ships to designated landing areas. (JP 3-02)

shore fire control party — A specially trained unit for control of naval gunfire in support of troops ashore. Also called **SFCP.** (JP 3-09)

shore party — A task organization of the landing force, formed for the purpose of facilitating the landing and movement off the beaches of troops, equipment, and supplies; for the evacuation from the beaches of casualties and enemy prisoners of war; and for facilitating the beaching, retraction, and salvaging of landing ships and craft. Also called **beach group.** See also **beachmaster unit; beach party; naval beach group.** (JP 3-02)

shortfall — The lack of forces, equipment, personnel, materiel, or capability, reflected as the difference between the resources identified as a plan requirement and those apportioned

to a combatant commander for planning, that would adversely affect the command's ability to accomplish its mission. (JP 5-0)

short-range air defense engagement zone — In air defense, that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with short-range air defense weapons and may be established within a low- or high-altitude missile engagement zone. Also called **SHORADEZ.** (JP 3-01)

short-range ballistic missile — A land-based ballistic missile with a range capability up to about 600 nautical miles. Also called **SRBM.** (JP 3-01)

short takeoff and landing — The ability of an aircraft to clear a 50-foot (15 meters) obstacle within 1,500 feet (450 meters) of commencing takeoff or in landing, to stop within 1,500 feet (450 meters) after passing over a 50-foot (15 meters) obstacle. Also called **STOL.** (JP 3-04)

short title — A short, identifying combination of letters, and/or numbers assigned to a document or device for purposes of brevity and/or security. (JP 2-01)

show of force — An operation designed to demonstrate US resolve that involves increased visibility of US deployed forces in an attempt to defuse a specific situation that, if allowed to continue, may be detrimental to US interests or national objectives. (JP 3-0)

signal operating instructions — A series of orders issued for technical control and coordination of the signal communication activities of a command. In Marine Corps usage, these instructions are designated communication operation instructions. Also called **SOI**. (JP 6-0)

signals intelligence — 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT.** See also **communications intelligence; electronic intelligence; foreign instrumentation signals intelligence; intelligence.** (JP 2-0)

signals intelligence operational control — The authoritative direction of signals intelligence activities, including tasking and allocation of effort, and the authoritative prescription of those uniform techniques and standards by which signals intelligence information is collected, processed, and reported. (JP 2-01)

signals intelligence operational tasking authority — A military commander's authority to operationally direct and levy signals intelligence requirements on designated signals intelligence resources; includes authority to deploy and redeploy all or part of the signals intelligence resources for which signals intelligence operational tasking authority has been delegated. Also called **SOTA.** (JP 2-01)

significant wave height — The average height of the third of waves observed during a given period of time. See also **surf zone.** (JP 4-01.6)

simultaneous engagement — The concurrent engagement of hostile targets by combination of interceptor aircraft and surface-to-air missiles. (JP 3-01)

single-anchor leg mooring — A mooring facility dedicated to the offshore petroleum discharge system, which permits a tanker to remain on station and pump in much higher sea states than is possible with a spread moor. Also called **SALM.** See also **offshore petroleum discharge system.** (JP 4-01.6)

single manager— A Military Department or agency designated by the Secretary of Defense to be responsible for management of specified commodities or common service activities on a Department of Defense-wide basis. (JP 4-01)

single manager for transportation — The United States Transportation Command is the Department of Defense single manager for transportation, other than Service-organic or theater-assigned transportation assets. See also **Service-organic transportation assets; theater-assigned transportation assets** (JP 4-01)

single port manager — The transportation component, designated by the Department of Defense through the United States Transportation Command, responsible for management of all common-user aerial and seaports worldwide. Also called **SPM.** See also **transportation component command.** (JP 4-01.5)

single-service manager — A Service component commander who is assigned the responsibility and delegated the authority to coordinate and/or perform specified personnel support or personnel service support functions in the theater of operations. See also **component.** (JP 1-0)

site exploitation — A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or materiel found during the conduct of operations. Also called **SE.** (JP 3-31)

situation report — A report giving the situation in the area of a reporting unit or formation. Also called **SITREP.** (JP 3-50)

situation template — A depiction of assumed adversary dispositions, based on that adversary's preferred method of operations and the impact of the operational environment if the adversary should adopt a particular course of action. See also **adversary template; course of action.** (JP 2-01.3)

sociocultural analysis — The analysis of adversaries and other relevant actors that integrates concepts, knowledge, and understanding of societies, populations, and other groups of people, including their activities, relationships, and perspectives across time and space at varying scales. Also called **SCA.** (JP 2-0)

sociocultural factors — The social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (JP 2-01.3)

solatium — Monetary compensation given in areas where it is culturally appropriate to alleviate grief, suffering, and anxiety resulting from injuries, death, and property loss with a monetary payment. (JP 1-06)

sortie — In air operations, an operational flight by one aircraft. (JP 3-30)

sortie allotment message — The means by which the joint force commander allots excess sorties to meet requirements of subordinate commanders that are expressed in their air employment and/or allocation plan. Also called **SORTIEALOT.** (JP 3-30)

source — 1. A person, thing, or activity from which information is obtained. 2. In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. 3. In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. See also **agent; collection agency.** (JP 2-01)

source management — The process of registering and monitoring the use of sources involved in counterintelligence and human intelligence operations to protect the security of the operations and avoid conflicts among operational elements. (JP 2-01.2)

source registry — A source record/catalogue of leads and sources acquired by collectors and centralized for management, coordination and deconfliction of source operations. (JP 2-01.2)

space asset — Equipment that is an individual part of a space system, which is or can be placed in space or directly supports space activity terrestrially. (JP 3-14)

space assignment — An assignment to the individual Military Departments/Services by the appropriate transportation operating agency of movement capability, which completely or partially satisfies the stated requirements of the Military Departments/Services for the operating month and that has been accepted by them without the necessity for referral to the Joint Transportation Board for allocation. (JP 4-01)

space capability — 1. The ability of a space asset to accomplish a mission. 2. The ability of a terrestrial-based asset to accomplish a mission in or through space. See also **space asset.** (JP 3-14)

space control — Operations to ensure freedom of action in space for the United States and its allies and, when directed, deny an adversary freedom of action in space. See also **combat service support; combat support; negation; space systems.** (JP 3-14)

space coordinating authority — A commander or individual assigned responsibility for planning, integrating, and coordinating space operations support in the operational area. Also called **SCA.** (JP 3-14)

space environment — The environment corresponding to the space domain, where electromagnetic radiation, charged particles, and electric and magnetic fields are the dominant physical influences, and that encompasses the earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere. (JP 3-59)

space force application — Combat operations in, through, and from space to influence the course and outcome of conflict by holding terrestrial targets at risk. See also **ballistic missile; force protection.** (JP 3-14)

space force enhancement — Combat support operations and force-multiplying capabilities delivered from space systems to improve the effectiveness of military forces as well as support other intelligence, civil, and commercial users. See also **combat support .** (JP 3-14)

space forces — The space and terrestrial systems, equipment, facilities, organizations, and personnel necessary to access, use and, if directed, control space for national security. See also **national security; space systems.** (JP 3-14)

space power — The total strength of a nation's capabilities to conduct and influence activities to, in, through, and from space to achieve its objectives. (JP 3-14)

space situational awareness — Cognizance of the requisite current and predictive knowledge of the space environment and the operational environment upon which space operations depend. (JP 3-14)

space superiority — The degree of dominance in space of one force over any others that permits the conduct of its operations at a given time and place without prohibitive interference from space-based threats. (JP 3-14)

space support — Launching and deploying space vehicles, maintaining and sustaining spacecraft on-orbit, rendezvous and proximity operations, disposing of (including deorbiting and recovering) space capabilities, and reconstitution of space forces, if required. See also **combat service support.** (JP 3-14)

space surveillance — The observation of space and of the activities occurring in space. See also **space control.** (JP 3-14)

space systems — All of the devices and organizations forming the space network. (JP 3-14)

space weather — The conditions and phenomena in space and specifically in the near-Earth environment that may affect space assets or space operations. See also **space asset.**

(JP 3-59)

special access program — A sensitive acquisition, intelligence, or operations and support program, that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information. Also called **SAP.** (JP 3-05)

special cargo — Cargo that requires special handling or protection, such as pyrotechnics, detonators, watches, and precision instruments. (JP 4-01.5)

special event — An international or domestic event, contest, activity, or meeting, which by its very nature, or by specific statutory or regulatory authority, may warrant security, safety, and/or other logistical support or assistance from the Department of Defense. (DODD 3025.18)

special forces — United States Army forces organized, trained, and equipped to conduct special operations with an emphasis on unconventional warfare capabilities. Also called **SF.** (JP 3-05)

special forces group — The largest Army combat element for special operations consisting of command and control, special forces battalions, and a support battalion capable of long duration missions. Also called **SFG.** (JP 3-05)

specialization — An arrangement within an alliance wherein a member or group of members most suited by virtue of technical skills, location, or other qualifications assume(s) greater responsibility for a specific task or significant portion thereof for one or more other members. (JP 3-16)

special mission unit — A generic term to represent an organization composed of operations and support personnel that is task-organized to perform highly classified activities. Also called **SMU.** (JP 3-05)

special operations — Operations requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk. (JP 3-05)

special operations command and control element — A special operations element that is the focal point for the synchronization of special operations forces activities with conventional forces activities. Also called **SOCCE**. See also **command and control; joint force special operations component commander; special operations; special operations forces**. (JP 3-05)

special operations forces — Those Active and Reserve Component forces of the Services designated by the Secretary of Defense and specifically organized, trained, and equipped

to conduct and support special operations. Also called **SOF.** See also **Air Force special operations forces; Army special operations forces; Navy special operations forces.** (JP 3-05)

special operations joint task force — A modular, tailorable, and scalable special operations task force designed to provide integrated, fully-capable, and enabled joint special operations forces to geographic combatant commanders and joint force commanders. Also called **SOJTF.** (JP 3-05)

special operations liaison element — A special operations liaison team provided by the joint force special operations component commander to coordinate, deconflict, and synchronize special operations air, surface, and subsurface operations with conventional air operations. Also called **SOLE.** See also **joint force air component commander; joint force special operations component commander; special operations.** (JP 3-05)

special operations-peculiar — Equipment, material, supplies, and services required for special operations missions for which there is no Service-common requirement. See also **Service-common; special operations.** (JP 3-05)

special operations task force — A scalable unit, normally of battalion size, in charge of the special operations element, organized around the nucleus of special operations forces and support elements. Also called **SOTF.** (JP 3-05)

special operations weather team — A task organized team of Air Force personnel organized, trained, and equipped to collect critical environmental information from data sparse areas. Also called **SOWT.** (JP 3-05)

special operations wing — An Air Force special operations wing. Also called **SOW.** (JP 3-05)

special reconnaissance — Reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or diplomatically and/or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. Also called **SR.** (JP 3-05)

special tactics team — An Air Force task-organized element of special tactics that may include combat control, pararescue, tactical air control party, and special operations weather personnel. Also called **STT.** See also **combat search and rescue; special operations; special operations forces; terminal attack control.** (JP 3-05)

specified combatant command — A command, normally composed of forces from a single Military Department, that has a broad, continuing mission, normally functional, and is established and so designated by the President through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff. (JP 1)

specified task — In the context of joint operation planning, a task that is specifically assigned to an organization by its higher headquarters. See also **essential task; implied task.** (JP 5-0)

split-mission oriented protective posture — The concept of maintaining heightened protective posture only in those areas (or zones) that are contaminated, allowing personnel in uncontaminated areas to continue to operate in a reduced posture. Also called **split-MOPP.** (JP 3-11)

spoke — The portion of the hub and spoke distribution system that refers to transportation mode operators responsible for scheduled delivery to a customer of the "hub". See also **distribution; distribution system; hub; hub and spoke distribution.** (JP 4-09)

spot — 1. To determine by observation, deviations of ordnance from the target for the purpose of supplying necessary information for the adjustment of fire. 2. To place in a proper location. 3. An approved shipboard helicopter landing site. See also **ordnance.** (JP 3-04)

spot net — Radio communication net used by a spotter in calling fire. (JP 3-09.3)

spot report — A concise narrative report of essential information covering events or conditions that may have an immediate and significant effect on current planning and operations that is afforded the most expeditious means of transmission consistent with requisite security. Also called **SPOTREP.** (Note: In reconnaissance and surveillance usage, spot report is not to be used.) (JP 3-09.3)

spotter — 1. An observer stationed for the purpose of observing and reporting results of naval gunfire to the firing agency and who also may be employed in designating targets. (JP 3-09) 2. In intelligence, an agent or illegal assigned to locate and assess individuals in positions of value to an intelligence service. (JP 2-01.2)

spotting — Parking aircraft in an approved shipboard landing site. (JP 3-04)

spreader bar — A device specially designed to permit the lifting and handling of containers or vehicles and breakbulk cargo. (JP 4-01.6)

squadron — 1. An organization consisting of two or more divisions of ships, or two or more divisions (Navy) or flights of aircraft. 2. The basic administrative aviation unit of the Army, Navy, Marine Corps, and Air Force. 3. Battalion-sized ground or aviation units. (JP 3-32)

stability operations — An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 3-0)

stabilized patient — A patient whose airway is secured, hemorrhage is controlled, shock treated, and fractures are immobilized. (JP 4-02)

stable patient — A patient for whom no inflight medical intervention is expected but the potential for medical intervention exists. (JP 4-02)

staff judge advocate — A judge advocate so designated in the Army, Air Force, or Marine Corps, and the principal legal advisor of a Navy, Coast Guard, or joint force command who is a judge advocate. Also called **SJA.** (JP 1-04)

staging — Assembling, holding, and organizing arriving personnel, equipment, and sustaining materiel in preparation for onward movement. See also **staging area.** (JP 3-35)

staging area — 1. **Amphibious or airborne** — A general locality between the mounting area and the objective of an amphibious or airborne expedition, through which the expedition or parts thereof pass after mounting, for refueling, regrouping of ships, and/or exercise, inspection, and redistribution of troops. 2. **Other movements** — A general locality established for the concentration of troop units and transient personnel between movements over the lines of communications. Also called **SA.** See also **airborne; marshalling; staging.** (JP 3-35)

staging base — 1. An advanced naval base for the anchoring, fueling, and refitting of transports and cargo ships as well as replenishment of mobile service squadrons. (JP 4-01.2) 2. A landing and takeoff area with minimum servicing, supply, and shelter provided for the temporary occupancy of military aircraft during the course of movement from one location to another. (JP 3-18)

stakeholder — In public affairs, an individual or group that is directly impacted by military operations, actions, and/or outcomes, and whose interests positively or negatively motivate them toward action. (JP 3-61)

standardization — The process by which the Department of Defense achieves the closest practicable cooperation among the Services and Department of Defense agencies for the most efficient use of research, development, and production resources, and agrees to adopt on the broadest possible basis the use of: a. common or compatible operational, administrative, and logistic procedures; b. common or compatible technical procedures and criteria; c. common, compatible, or interchangeable supplies, components, weapons, or equipment; and d. common or compatible tactical doctrine with corresponding organizational compatibility. (JP 4-02)

standard operating procedure — A set of instructions applicable to those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness. Also called **SOP**; **standing operating procedure.** (JP 3-31)

standard use Army aircraft flight route — Route established below the coordination level to facilitate the movement of Army aviation assets; it is normally located in the corps through brigade rear areas of operation and does not require approval by the airspace control authority. Also called **SAAFR.** (JP 3-52)

Standby Reserve — Those units and members of the Reserve Component (other than those in the Ready Reserve or Retired Reserve) who are liable for active duty only, as provided in Title 10, United States Code, Sections 10151, 12301, and 12306. See also **active duty; Ready Reserve; Reserve Component; Retired Reserve.** (JP 4-05)

standing joint force headquarters — A staff organization operating under a flag or general officer providing a combatant commander with a full-time, trained joint command and control element integrated into the combatant commander's staff whose focus is on contingency and crisis action planning. Also called **SJFHQ.** (JP 3-0)

standing rules for the use of force — Preapproved directives to guide United States forces on the use of force during various operations. Also called **SRUF.** (JP 3-28)

stateless person — A person who is not considered as a national by any state under the operation of its law. See also **dislocated civilian; displaced person; evacuee; refugee.** (JP 3-29)

station time — In air transport operations, the time at which crews, passengers, and cargo are to be on board and ready for the flight. (JP 3-17)

status-of-forces agreement — A bilateral or multilateral agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Also called **SOFA.** (JP 3-16)

sterilizer — In mine warfare, a device included in mines to render the mine permanently inoperative on expiration of a pre-determined time after laying. (JP 3-15)

stockage objective — The maximum quantities of materiel to be maintained on hand to sustain current operations, which will consist of the sum of stocks represented by the operating level and the safety level. (JP 4-08)

Stock Number — See **national stock number.**

stockpile to target sequence — 1. The order of events involved in removing a nuclear weapon from storage and assembling, testing, transporting, and delivering it on the target. 2. A document that defines the logistic and employment concepts and related physical environments involved in the delivery of a nuclear weapon from the stockpile to the target. It may also define the logistic flow involved in moving nuclear weapons to and from the stockpile for quality assurance testing, modification and retrofit, and the recycling of limited life components.

stop-loss — Presidential authority under Title 10, United States Code, Section 12305, to suspend laws relating to promotion, retirement, or separation of any member of the Armed Forces determined essential to the national security of the United States, to include reservists if serving on active duty under Title 10, United States Code authorities for Presidential Reserve Call-up, partial mobilization, or full mobilization. See also **mobilization; partial mobilization; Presidential Reserve Call-up.** (JP 4-05)

stowage — The placement of cargo into a hold, compartment, or on a deck of a ship in such a way as to prevent damage from load shifts while the ship is underway. (JP 3-02.1)

stowage factor — The number that expresses the space, in cubic feet, occupied by a long ton of any commodity as prepared for shipment, including all crating or packaging. (JP 4-01.2)

stowage plan — A completed stowage diagram showing what materiel has been loaded and its stowage location in each hold, between-deck compartment, or other space in a ship, including deck space. (JP 4-01.5)

strategic communication — Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. Also called **SC.** (JP 5-0)

strategic concept — The course of action accepted as the result of the estimate of the strategic situation which is a statement of what is to be done in broad terms. (JP 5-0)

strategic debriefing — Debriefing activity conducted to collect information or to verify previously collected information in response to national or theater level collection priorities. (JP 2-01.2)

strategic direction — The processes and products by which the President, Secretary of Defense, and Chairman of the Joint Chiefs of Staff provide strategic guidance to the Joint Staff, combatant commands, Services, and combat support agencies. (JP 5-0)

strategic estimate — The broad range of strategic factors that influence the commander's understanding of its operational environment and its determination of missions, objectives, and courses of action. See also **estimate; national intelligence estimate.** (JP 5-0)

strategic intelligence — Intelligence required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application, but may also vary in terms of scope and detail. See also **intelligence; operational intelligence; tactical intelligence.** (JP 2-01.2)

strategic level of war — The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives. See also **operational level of war; tactical level of war.** (JP 3-0)

strategic mobility — The capability to deploy and sustain military forces worldwide in support of national strategy. (JP 4-01)

strategic plan — A plan for the overall conduct of a war. (JP 5-0)

strategic sealift — The afloat pre-positioning and ocean movement of military materiel in support of United States and multinational forces. (JP 4-01.5)

strategic sealift forces — Sealift forces composed of ships, cargo handling and delivery systems, and the necessary operating personnel. See also **force.** (JP 4-01.6)

strategic sealift shipping — Common-user ships of the Military Sealift Command force, including pre-positioned ships after their pre-positioning mission has been completed and they have been returned to the operational control of the Military Sealift Command. See also **Military Sealift Command; Military Sealift Command force.** (JP 4-01.2)

strategy — A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives. (JP 3-0)

strike — An attack to damage or destroy an objective or a capability. (JP 3-0)

strike coordination and reconnaissance — A mission flown for the purpose of detecting targets and coordinating or performing attack or reconnaissance on those targets. Also called **SCAR.** (JP 3-03)

stuffing — Packing of cargo into a container. See also **unstuffing.** (JP 4-09)

submarine operating authority — The naval commander exercising operational control of submarines. Also called **SUBOPAUTH.** (JP 3-32)

subordinate campaign plan — A combatant command prepared plan that satisfies the requirements under a Department of Defense campaign plan, which, depending upon the circumstances, transitions to a supported or supporting plan in execution. (JP 5-0)

subordinate command — A command consisting of the commander and all those individuals, units, detachments, organizations, or installations that have been placed under the command by the authority establishing the subordinate command. (JP 1)

subordinate unified command — A command established by commanders of unified commands, when so authorized by the Secretary of Defense through the Chairman of the

Joint Chiefs of Staff, to conduct operations on a continuing basis in accordance with the criteria set forth for unified commands. See also **area command; functional component command; operational control; subordinate command; unified command.** (JP 1)

subsidiary landing — In an amphibious operation, a landing usually made outside the designated landing area, the purpose of which is to support the main landing. (JP 3-02)

subversion — Actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority. See also **unconventional warfare.** (JP 3-24)

sun-synchronous orbit — An orbit in which the satellite's orbital plane is at a fixed orientation to the sun, i.e., the orbit precesses about the earth at the same rate that the earth orbits the sun. (JP 3-14)

supercargo — Personnel that accompany cargo on board a ship for the purpose of accomplishing en route maintenance and security. (JP 4-01.5)

supplies — In logistics, all materiel and items used in the equipment, support, and maintenance of military forces. See also **component; equipment.** (JP 4-0)

supply — The procurement, distribution, maintenance while in storage, and salvage of supplies, including the determination of kind and quantity of supplies. a. **producer phase**—That phase of military supply that extends from determination of procurement schedules to acceptance of finished supplies by the Services. b. **consumer phase**—That phase of military supply that extends from receipt of finished supplies by the Services through issue for use or consumption. (JP 4-0)

supply chain — The linked activities associated with providing materiel from a raw materiel stage to an end user as a finished product. See also **supply; supply chain management.** (JP 4-09)

supply chain management — A cross-functional approach to procuring, producing, and delivering products and services to customers. See also **supply; supply chain.** (JP 4-09)

supply support activity — Activities assigned a Department of Defense activity address code and that have a supply support mission. Also called **SSA.** (JP 4-09)

support — 1. The action of a force that aids, protects, complements, or sustains another force in accordance with a directive requiring such action. 2. A unit that helps another unit in battle. 3. An element of a command that assists, protects, or supplies other forces in combat. See also **close support; direct support; general support; inter-Service support; mutual support.** (JP 1)

supported commander — 1. The commander having primary responsibility for all aspects of a task assigned by the Joint Strategic Capabilities Plan or other joint operation planning authority. 2. In the context of joint operation planning, the commander who prepares operation plans or operation orders in response to requirements of the Chairman of the Joint Chiefs of Staff. 3. In the context of a support command relationship, the commander who receives assistance from another commander's force or capabilities, and who is responsible for ensuring that the supporting commander understands the assistance required. See also **support; supporting commander.** (JP 3-0)

supported unit — As related to contracted support, a supported unit is the organization that is the recipient, but not necessarily the requester of, contractor-provided support. See also **requiring activity.** (JP 4-10)

supporting arms — Weapons and weapons systems of all types employed to support forces by indirect or direct fire. (JP 3-02)

supporting arms coordination center — A single location on board an amphibious warfare command ship in which all communication facilities incident to the coordination of fire support of the artillery, air, and naval gunfire are centralized. Also called **SACC.** See also **fire support coordination center.** (JP 3-09.3)

supporting commander — 1. A commander who provides augmentation forces or other support to a supported commander or who develops a supporting plan. 2. In the context of a support command relationship, the commander who aids, protects, complements, or sustains another commander's force, and who is responsible for providing the assistance required by the supported commander. See also **support; supported commander.** (JP 3-0)

supporting fire — Fire delivered by supporting units to assist or protect a unit in combat. (JP 3-09)

supporting operations — In amphibious operations, those operations conducted by forces other than those conducted by the amphibious force. See also **amphibious force; amphibious operation.** (JP 3-02)

supporting plan — An operation plan prepared by a supporting commander, a subordinate commander, or an agency to satisfy the requests or requirements of the supported commander's plan. See also **supported commander; supporting commander.** (JP 5-0)

suppression — Temporary or transient degradation by an opposing force of the performance of a weapons system below the level needed to fulfill its mission objectives. (JP 3-01)

suppression of enemy air defenses — Activity that neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means. Also called **SEAD.** See also **electromagnetic spectrum; electronic warfare.** (JP 3-01)

surface action group — A temporary or standing organization of combatant ships, other than carriers, tailored for a specific tactical mission. Also called **SAG.** See **group**; **mission.** (JP 3-32)

surface combatant — A ship constructed and armed for combat use with the capability to conduct operations in multiple maritime roles against air, surface and subsurface threats, and land targets. (JP 3-32)

surface-to-air missile site — A plot of ground prepared in such a manner that it will readily accept the hardware used in surface-to-air missile system. (JP 3-01)

surface warfare — That portion of maritime warfare in which operations are conducted to destroy or neutralize enemy naval surface forces and merchant vessels. Also called **SUW.** (JP 3-32)

surf line — The point offshore where waves and swells are affected by the underwater surface and become breakers. (JP 4-01.6)

surf zone — The area of water from the surf line to the beach. See also **surf line.** (JP 4-01.6)

surveillance — The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (JP 3-0)

survivability — All aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy. (JP 3-34)

survival, evasion, resistance, and escape — Actions performed by isolated personnel designed to ensure their health, mobility, safety, and honor in anticipation of or preparation for their return to friendly control. Also called **SERE.** (JP 3-50)

suspect — 1. In counterdrug operations, a track of interest where correlating information actually ties the track of interest to alleged illegal drug operations. See also **counterdrug operations; track of interest.** 2. An identity applied to a track that is potentially hostile because of its characteristics, behavior, origin, or nationality. See also **assumed friend; neutral; unknown**. (JP 3-07.4)

sustainment — The provision of logistics and personnel services required to maintain and prolong operations until successful mission accomplishment. (JP 3-0)

sustainment, restoration, and modernization — The fuels asset sustainment program within Defense Logistics Agency Energy that provides a long-term process to cost-effectively sustain, restore, and modernize fuel facilities. Also called **SRM.** (JP 4-03)

synchronization — 1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In the

intelligence context, application of intelligence sources and methods in concert with the operation plan to answer intelligence requirements in time to influence the decisions they support. (JP 2-0)

synthesis — In intelligence usage, the examining and combining of processed information with other information and intelligence for final interpretation. (JP 2-0)

system — A functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements; that group of elements forming a unified whole. (JP 3-0)

systems support contract — A prearranged contract awarded by a Service acquisition program management office that provides technical support, maintenance and, in some cases, repair parts for selected military weapon and support systems. See also **external support contract; theater support contract.** (JP 4-10)

Intentionally Blank

T

table of allowance — An equipment allowance document that prescribes basic allowances of organizational equipment, and provides the control to develop, revise, or change equipment authorization inventory data. Also called **TOA.** (JP 4-09)

TABOO frequencies — Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces including international distress, safety, and controller frequencies. See also **electronic warfare.** (JP 3-13.1)

tactical air command center — The principal US Marine Corps air command and control agency from which air operations and air defense warning functions are directed. Also called **Marine TACC.** (JP 3-09.3)

tactical air control center — The principal air operations installation (ship-based) from which all aircraft and air warning functions of tactical air operations are controlled. Also called **Navy TACC.** (JP 3-09.3)

tactical air control party — A subordinate operational component of a tactical air control system designed to provide air liaison to land forces and for the control of aircraft. Also called **TACP.** (JP 3-09.3)

tactical air coordinator (airborne) — An officer who coordinates, from an aircraft, the actions of other aircraft engaged in air support of ground or sea forces. Also called **TAC(A).** See also **forward observer**. (JP 3-09.3)

tactical air direction center — An air operations installation under the overall control of the Navy tactical air control center or the Marine Corps tactical air command center, from which aircraft and air warning service functions of tactical air operations in support of amphibious operations are directed. Also called **TADC.** (JP 3-09.3)

tactical air officer — The officer under the amphibious task force commander who, until control is passed ashore, coordinates planning of all phases of air participation of the amphibious operation and air operations of supporting forces en route to and in the objective area. Also called **TAO**. (JP 3-02)

tactical air operations center — The principal air control agency of the United States Marine Corps air command and control system responsible for airspace control and management. Also called **TAOC.** (JP 3-09.3)

tactical assembly area — An area that is generally out of the reach of light artillery and the location where units make final preparations (pre-combat checks and inspections) and rest, prior to moving to the line of departure. See also **line of departure.** (JP 3-35)

tactical combat casualty care — A set of trauma management guidelines customized for use on the battlefield that maintains a sharp focus on the most common causes of preventable

deaths on the battlefield: external hemorrhage; tension pneumothorax; and airway obstruction. (JP 4-02)

tactical combat force — A rapidly deployable, air-ground mobile combat unit, with appropriate combat support and combat service support assets assigned to and capable of defeating Level III threats including combined arms. Also called **TCF.** (JP 3-10)

tactical control — The authority over forces that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Also called **TACON.** See also **combatant command; combatant command (command authority); operational control.** (JP 1)

tactical data link — A Joint Staff-approved, standardized communication link suitable for transmission of digital information, which interfaces two or more command and control or weapons systems via a single or multiple network architecture and multiple communication media for exchange of tactical information. Also called **TDL.** (JP 6-0)

tactical exploitation of national capabilities — Congressionally mandated program to improve the combat effectiveness of the Services through more effective military use of national programs. Also called **TENCAP.** (JP 2-01)

tactical intelligence — Intelligence required for the planning and conduct of tactical operations. See also **intelligence.** (JP 2-01.2)

tactical level of war — The level of war at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. See also **operational level of war; strategic level of war.** (JP 3-0)

tactical-logistical group — Representatives designated by troop commanders to assist Navy control officers aboard control ships in the ship-to-shore movement of troops, equipment, and supplies. Also called **TACLOG group**. (JP 3-02)

tactical minefield — A minefield that is employed to directly attack enemy maneuver as part of a formation obstacle plan and is laid to delay, channel, or break up an enemy advance, giving the defending element a positional advantage over the attacker. (JP 3-15)

tactical obstacles — Those obstacles employed to disrupt enemy formations, to turn them into a desired area, to fix them in position under direct and indirect fires, and to block enemy penetrations. (JP 3-15)

tactical questioning — The field-expedient initial questioning for information of immediate tactical value of a captured or detained person at or near the point of capture and before the individual is placed in a detention facility. Also called **TQ.** (JP 3-63)

tactical recovery of aircraft and personnel — A Marine Corps mission performed by an assigned and briefed aircrew for the specific purpose of the recovery of personnel,

equipment, and/or aircraft when the tactical situation precludes search and rescue assets from responding and when survivors and their location have been confirmed. Also called **TRAP.** (JP 3-50)

tactical reserve — A part of a force held under the control of the commander as a maneuvering force to influence future action. (JP 3-02)

tactics — The employment and ordered arrangement of forces in relation to each other. See also **procedures; techniques.** (CJCSM 5120.01)

target — 1. An entity or object that performs a function for the adversary considered for possible engagement or other action. 2. In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. 3. An area designated and numbered for future firing. 4. In gunfire support usage, an impact burst that hits the target. See also **objective area.** (JP 3-60)

target acquisition — The detection, identification, and location of a target in sufficient detail to permit the effective employment of weapons. Also called **TA.** See also **target analysis.** (JP 3-60)

target analysis — An examination of potential targets to determine military importance, priority of attack, and weapons required to obtain a desired level of damage or casualties. See also **target acquisition.** (JP 3-60)

target area of interest — The geographical area where high-value targets can be acquired and engaged by friendly forces. Also called **TAI.** See also **area of interest; high-value target; target.** (JP 2-01.3)

target audience — An individual or group selected for influence. Also called **TA.** (JP 3-13)

target complex — A geographically integrated series of target concentrations. See also **target.** (JP 3-60)

target component — A set of targets within a target system performing a similar function. See also **target.** (JP 3-60)

target development — The systematic examination of potential target systems - and their components, individual targets, and even elements of targets - to determine the necessary type and duration of the action that must be exerted on each target to create an effect that is consistent with the commander's specific objectives. (JP 3-60)

targeteer — An individual who has completed formal targeting training in an established Service or joint school and participates in the joint targeting cycle in their current duties. (JP 3-60)

target folder — A folder, hardcopy or electronic, containing target intelligence and related materials prepared for planning and executing action against a specific target. See also **target.** (JP 3-60)

target information center — The agency or activity responsible for collecting, displaying, evaluating, and disseminating information pertaining to potential targets. Also called **TIC**. See also **target.** (JP 3-02)

targeting — The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. See also **joint targeting coordination board; target.** (JP 3-0)

target intelligence — Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. See also **target; target complex.** (JP 3-60)

target location error — The difference between the coordinates generated for a target and the actual location of the target. Also called **TLE**. (JP 3-09.3)

target materials — Graphic, textual, tabular, digital, video, or other presentations of target intelligence, primarily designed to support operations against designated targets by one or more weapon(s) systems. See also **Air Target Materials Program.** (JP 3-60)

target nomination list — A prioritized list of targets drawn from the joint target list and nominated by component commanders, appropriate agencies, or the joint force commander's staff for inclusion on the joint integrated prioritized target list. Also called **TNL.** See also **candidate target list; joint integrated prioritized target list; target.** (JP 3-60)

target of opportunity — 1. A target identified too late, or not selected for action in time, to be included in deliberate targeting that, when detected or located, meets criteria specific to achieving objectives and is processed using dynamic targeting. 2. A target visible to a surface or air sensor or observer, which is within range of available weapons and against which fire has not been scheduled or requested. See also **dynamic targeting; target; unplanned target; unanticipated target.** (JP 3-60)

target reference point — A predetermined point of reference, normally a permanent structure or terrain feature that can be used when describing a target location. Also called **TRP.** (JP 3-09.3)

target system — 1. All the targets situated in a particular geographic area and functionally related. 2. A group of targets that are so related that their destruction will produce some particular effect desired by the attacker. See also **target; target complex.** (JP 3-60)

target system analysis — An all-source examination of potential target systems to determine relevance to stated objectives, military importance, and priority of attack. Also called **TSA.** (JP 3-60)

target system assessment — The broad assessment of the overall impact and effectiveness of the full spectrum of military force applied against the operation of an enemy target system, significant subdivisions of the system, or total combat effectiveness relative to the operational objectives established. See also **target system.** (JP 3-60)

target system component — A set of targets belonging to one or more groups of industries and basic utilities required to produce component parts of an end product, or one type of a series of interrelated commodities. (JP 3-60)

task — A clearly defined action or activity specifically assigned to an individual or organization that must be done as it is imposed by an appropriate authority. (JP 1)

task component — A subdivision of a fleet, task force, task group, or task unit, organized by the respective commander or by higher authority for the accomplishment of specific tasks. (JP 3-32)

task element — A component of a naval task unit organized by the commander of a task unit or higher authority. (JP 3-32)

task force — A component of a fleet organized by the commander of a task fleet or higher authority for the accomplishment of a specific task or tasks. Also called **TF.** (JP 3-32)

task force counterintelligence coordinating authority — An individual that affects the overall coordination of counterintelligence activities (in a joint force intelligence directorate counterintelligence and human intelligence staff element, joint task force configuration), with other supporting counterintelligence organizations, and supporting agencies to ensure full counterintelligence coverage of the task force operational area. Also called **TFCICA**. See also **counterintelligence; counterintelligence activities; joint task force**. (JP 2-01.2)

task group — A component of a naval task force organized by the commander of a task force or higher authority. Also called **TG.** (JP 3-32)

tasking order — A method used to task and to disseminate to components, subordinate units, and command and control agencies projected targets and specific missions as well as general and specific instructions for accomplishment of the mission. Also called **TASKORD.** See also **mission; target.** (JP 3-05.1)

task order — Order for services placed against an established contract. See also **civil augmentation program.** (JP 4-10)

task organization — An organization that assigns to responsible commanders the means with which to accomplish their assigned tasks in any planned action. (JP 3-33)

task unit — A component of a naval task group organized by the commander of a task group or higher authority. (JP 3-32)

tear line — A physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. (JP 2-0)

technical analysis — In imagery interpretation, the precise description of details appearing on imagery. (JP 2-03)

technical assistance — The providing of advice, assistance, and training pertaining to the installation, operation, and maintenance of equipment. (JP 3-22)

technical escort — An individual technically qualified and properly equipped to accompany designated material requiring a high degree of safety or security during shipment. (JP 3-15.1)

technical evaluation — The study and investigations by a developing agency to determine the technical suitability of material, equipment, or a system for use in the Services. (JP 3-15.1)

technical intelligence — Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. Also called **TECHINT.** See also **exploitation; intelligence.** (JP 2-0)

technical nuclear forensics — The collection, analysis and evaluation of pre-detonation (intact) and post-detonation (exploded) radiological or nuclear materials, devices, and debris, as well as the immediate effects created by a nuclear detonation. (JP 3-41)

technical review authority — The organization tasked to provide specialized technical or administrative expertise to the lead agent, primary review authority, Joint Staff doctrine sponsor, or coordinating review authority for joint publications. Also called **TRA**. See also **coordinating review authority; joint publication; primary review authority.** (CJCSM 5120.01)

technical surveillance countermeasures — Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect

transmission of information meant to be protected. Also called **TSCM.** See also **counterintelligence.** (JP 2-01.2)

techniques — Non-prescriptive ways or methods used to perform missions, functions, or tasks. See also **procedures; tactics.** (CJCSM 5120.01)

telecommunications — Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. (JP 6-0)

telemedicine — Rapid access to shared and remote medical expertise by means of telecommunications and information technologies to deliver health services and exchange health information for the purpose of improving patient care. (JP 4-02)

tempest — An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security. See also **counterintelligence.** (JP 2-01.2)

temporary interment — A site for the purpose of: a. the interment of the remains if the circumstances permit; or b. the reburial of remains exhumed from an emergency interment. See also **mortuary affairs.** (JP 4-06)

terminal — A facility designed to transfer cargo from one means of conveyance to another. See also **facility.** (JP 4-01.6)

terminal attack control — The authority to control the maneuver of and grant weapons release clearance to attacking aircraft. See also **joint terminal attack controller.** (JP 3-09.3)

terminal control — 1. A type of air control with the authority to direct aircraft to maneuver into a position to deliver ordnance, passengers, or cargo to a specific location or target. 2. Any electronic, mechanical, or visual control given to aircraft to facilitate target acquisition and resolution. See also **terminal guidance.** (JP 3-09.3)

terminal guidance — 1. The guidance applied to a guided missile between midcourse guidance and arrival in the vicinity of the target. 2. Electronic, mechanical, visual, or other assistance given an aircraft pilot to facilitate arrival at, operation within or over, landing upon, or departure from an air landing or airdrop facility. See also **terminal control.** (JP 3-03)

terminal guidance operations — Actions using electronic, mechanical, voice, or visual communications that provide approaching aircraft and/or weapons additional information regarding a specific target location. Also called **TGO.** (JP 3-09)

terminal operations — The reception, processing, and staging of passengers; the receipt, transit, storage, and marshalling of cargo; the loading and unloading of modes of transport conveyances; and the manifesting and forwarding of cargo and passengers to destination. See also **operation; terminal.** (JP 4-01.5)

terminal phase — That portion of the flight of a ballistic missile that begins when the warhead or payload reenters the atmosphere and ends when the warhead or payload detonates, releases its submunitions, or impacts. See also **boost phase; midcourse phase.** (JP 3-01)

termination criteria — The specified standards approved by the President and/or the Secretary of Defense that must be met before a joint operation can be concluded. (JP 3-0)

terms of reference — 1. A mutual agreement under which a command, element, or unit exercises authority or undertakes specific missions or tasks relative to another command, element, or unit. 2. The directive providing the legitimacy and authority to undertake a mission, task, or endeavor. Also called **TORs.** (JP 3-0)

terrain analysis — The collection, analysis, evaluation, and interpretation of geographic information on the natural and man-made features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. (JP 2-03)

terrain avoidance system — A system that provides the pilot or navigator of an aircraft with a situation display of the ground or obstacles so that the pilot can maneuver the aircraft to avoid the obstruction. (JP 3-50)

terrain flight — Flight close to the Earth's surface during which airspeed, height, and/or altitude are adapted to the contours and cover of the ground in order to avoid enemy detection and fire. Also called **contour flight**; **low-level flight**; **nap-of-the-earth flight.** (JP 3-09.3)

terrain intelligence — Intelligence on the military significance of natural and man-made characteristics of an area. (JP 3-15)

terrestrial environment — The Earth's land area, including its man-made and natural surface and sub-surface features, and its interfaces and interactions with the atmosphere and the oceans. (JP 3-59)

territorial airspace — Airspace above land territory and internal, archipelagic, and territorial waters. (JP 1)

territorial waters — A belt of ocean space adjacent to and measured from the coastal states baseline to a maximum width of 12 nautical miles. (JP 1)

terrorism — The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political. See also **antiterrorism; combating terrorism; counterterrorism; force protection condition.** (JP 3-07.2)

terrorist threat level — A Department of Defense intelligence threat assessment of the level of terrorist threat faced by United States personnel and interests in a foreign country; the levels are expressed as **LOW**, **MODERATE**, **SIGNIFICANT**, and **HIGH**. (JP 3-07.2)

theater — The geographical area for which a commander of a geographic combatant command has been assigned responsibility. (JP 1)

theater antisubmarine warfare commander — A Navy commander assigned to develop plans and direct assigned and attached assets for the conduct of antisubmarine warfare within an operational area. Also called **TASWC.** (JP 3-32)

theater-assigned transportation assets — Transportation assets that are assigned under the combatant command (command authority) of a geographic combatant commander. See also **combatant command (command authority); single manager for transportation.** (JP 4-01)

theater detainee reporting center — The field operating agency of the National Detainee Reporting Center responsible for maintaining information on all detainees and their personal property within a theater of operations or assigned area of operations. Also called **TDRC.** (JP 3-63)

theater distribution — The flow of personnel, equipment, and materiel within theater to meet the geographic combatant commander's missions. See also **distribution; theater; theater distribution system.** (JP 4-09)

theater distribution system — A distribution system comprised of four independent and mutually supported networks within theater to meet the geographic combatant commander's requirements: the physical network; the financial network; the information network; and the communications network. See also **distribution; distribution plan; distribution system; theater; theater distribution.** (JP 4-01)

theater event system — Architecture for reporting ballistic missile events, composed of three independent processing and reporting elements: the joint tactical ground stations, tactical detection and reporting, and the space-based infrared system mission control station. Also called **TES.** (JP 3-14)

theater hospitalization capability — Essential care and health service support capabilities to either return the patient to duty and/or stabilization to ensure the patient can tolerate evacuation to a definitive care facility outside the theater, which is known as Role 3 in North Atlantic Treaty Organization doctrine. (JP 4-02)

theater of operations — An operational area defined by the geographic combatant commander for the conduct or support of specific military operations. Also called **TO.** See also **theater of war.** (JP 3-0)

theater of war — Defined by the President, Secretary of Defense, or the geographic combatant commander as the area of air, land, and water that is, or may become, directly involved in the conduct of major operations and campaigns involving combat. See also **area of responsibility; theater of operations.** (JP 3-0)

theater patient movement requirements center — The activity responsible for intratheater patient movement management (medical regulating and aeromedical evacuation scheduling), the development of theater-level patient movement plans and schedules, the monitoring and execution in concert with the Global Patient Movement Requirements Center. Also called **TPMRC.** (JP 4-02)

theater special operations command — A subordinate unified command established by a combatant commander to plan, coordinate, conduct, and support joint special operations. Also called **TSOC.** See also **special operations.** (JP 3-05)

theater strategy — An overarching construct outlining a combatant commander's vision for integrating and synchronizing military activities and operations with the other instruments of national power in order to achieve national strategic objectives. See also n**ational military strategy; national security strategy; strategy.** (JP 3-0)

theater support contract — A type of contingency contract awarded by contracting officers in the operational area serving under the direct contracting authority of the Service component or designated joint head of contracting activity for the designated contingency operation. See also **external support contract; systems support contract.** (JP 4-10)

thermal crossover — The natural phenomenon that normally occurs twice daily when temperature conditions are such that there is a loss of contrast between two adjacent objects on infrared imagery. (JP 3-09.3)

thermal radiation — 1. The heat and light produced by a nuclear explosion. 2. Electromagnetic radiations emitted from a heat or light source as a consequence of its temperature. (JP 3-41)

thorough decontamination — Decontamination carried out by a unit to reduce contamination on personnel, equipment, materiel, and/or working areas equal to natural background or to the lowest possible levels, to permit the partial or total removal of individual protective equipment and to maintain operations with minimum degradation. See also **immediate decontamination; operational decontamination.** (JP 3-11)

threat analysis — In antiterrorism, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups which could target a facility. See also **antiterrorism.** (JP 3-07.2)

threat assessment — In antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations as well as the security environment within which friendly forces operate to determine the level of threat. Also called **TA.** (JP 3-07.2)

threat warning — The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (JP 2-01)

throughput — 1. In transportation, the average quantity of cargo and passengers that can pass through a port on a daily basis from arrival at the port to loading onto a ship or plane, or from the discharge from a ship or plane to the exit (clearance) from the port complex. (JP 4-01.5) 2. In patient movement and care, the maximum number of patients (stable or stabilized) by category, that can be received at the airport, staged, transported, and received at the proper hospital within any 24-hour period. (JP 4-02)

throughput capacity — The estimated capacity of a port or an anchorage to clear cargo and/or passengers in 24 hours usually expressed in tons for cargo, but may be expressed in any agreed upon unit of measurement. See also **clearance capacity**. (JP 4-01.5)

time-definite delivery — The consistent delivery of requested logistic support at a time and destination specified by the receiving activity. See also **logistic support.** Also called **TDD.** (JP 4-09)

time of flight — In artillery, mortar, and naval gunfire support, the time in seconds from the instant a weapon is fired, launched, or released from the delivery vehicle or weapons system to the instant it strikes or detonates. Also called **TOF**. (JP 3-09)

time on target — The actual time at which munitions impact the target. Also called **TOT.** (JP 3-09.3)

time-phased force and deployment data — The time-phased force data, non-unit cargo and personnel data, and movement data for the operation plan or operation order or ongoing rotation of forces. Also called **TPFDD.** See also **time-phased force and deployment list.** (JP 5-0)

time-phased force and deployment list — Appendix 1 to Annex A of the operation plan, which identifies types and/or actual units required to support the operation plan and indicates origin and ports of debarkation or ocean area. Also called **TPFDL.** See also **Joint Operation Planning and Execution System; time-phased force and deployment data.** (JP 4-05)

times — The Chairman of the Joint Chiefs of Staff coordinates the proposed dates and times with the commanders of the appropriate unified and specified commands, as well as any recommended changes to when specified operations are to occur (C-, D-, M-days end at 2400 hours Universal Time [Zulu time] and are assumed to be 24 hours long for planning). (JP 5-0)

time-sensitive target — A joint force commander validated target or set of targets requiring immediate response because it is a highly lucrative, fleeting target of opportunity or it poses (or will soon pose) a danger to friendly forces. Also called **TST.** (JP 3-60)

time to target — The number of minutes and seconds to elapse before aircraft ordnance impacts on target. Also called **TTT.** (JP 3-09.3)

tophandler — A device specially designed to permit the lifting and handling of containers from the top with rough terrain container handlers. See also **container.** (JP 4-01.6)

topographic map — A map that presents the vertical position of features in measurable form as well as their horizontal positions. (JP 2-03)

top secret — Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe. (EO 13526)

torture — As defined by Title 18, US Code, Section 2340, it is any act committed by a person acting under color of law specifically intended to inflict severe physical or mental pain or suffering (other than pain or suffering incidental to lawful sanctions) upon another person within his custody or physical control. "Severe mental pain or suffering" means the prolonged mental harm caused by or resulting from: (a) the intentional infliction or threatened infliction of severe physical pain or suffering; (b) the administration or application, or threatened administration or application, of mind-altering substances or other procedures calculated to disrupt profoundly the senses or personality; (c) the threat of imminent death; or (d) the threat that another person will imminently be subjected to death, severe physical pain or suffering, or the administration or application of mind-altering substances or other procedures calculated to disrupt profoundly the senses or personality. (JP 2-01.2)

total mobilization — Expansion of the active Armed Forces resulting from action by Congress and the President to organize and/or generate additional units or personnel beyond the existing force structure, and the resources needed for their support, to meet the total requirements of a war or other national emergency involving an external threat to the national security. (JP 4-05)

toxic industrial biological — Any biological material manufactured, used, transported, or stored by industrial, medical, or commercial processes which could pose an infectious or toxic threat. Also called **TIB.** (JP 3-11)

toxic industrial chemical — A chemical developed or manufactured for use in industrial operations or research by industry, government, or academia that poses a hazard. Also called **TIC.** (JP 3-11)

toxic industrial material — A generic term for toxic, chemical, biological, or radioactive substances in solid, liquid, aerosolized, or gaseous form that may be used, or stored for use, for industrial, commercial, medical, military, or domestic purposes. Also called **TIM.** (JP 3-11)

toxic industrial radiological — Any radiological material manufactured, used, transported, or stored by industrial, medical, or commercial processes. Also called **TIR.** (JP 3-11)

track — 1. A series of related contacts displayed on a data display console or other display device. 2. To display or record the successive positions of a moving object. 3. To lock onto a point of radiation and obtain guidance therefrom. 4. To keep a gun properly aimed, or to point continuously a target-locating instrument at a moving target. 5. The actual path of an aircraft above or a ship on the surface of the Earth. 6. One of the two endless belts on which a full-track or half-track vehicle runs. 7. A metal part forming a path for a moving object such as the track around the inside of a vehicle for moving a mounted machine gun. (JP 3-01)

track correlation — Correlating track information for identification purposes using all available data. (JP 3-01)

tracking — Precise and continuous position-finding of targets by radar, optical, or other means. (JP 3-07.4)

track management — Defined set of procedures whereby the commander ensures accurate friendly and enemy unit and/or platform locations, and a dissemination procedure for filtering, combining, and passing that information to higher, adjacent, and subordinate commanders. (JP 3-01)

track of interest — In counterdrug operations, contacts that meet the initial identification criteria applicable in the area where the contacts are detected. Also called **TOI.** See also **suspect.** (JP 3-07.4)

tradecraft — Specialized methods and equipment used in the organization and activity of intelligence organizations, especially techniques and methods for handling communications with agents. Operational practices and skills used in the performance of intelligence related duties. (JP 2-01.2)

traffic management — The direction, control, and supervision of all functions incident to the procurement and use of freight and passenger transportation services. (JP 4-09)

training aid — Any item developed or procured with the primary intent that it shall assist in training and the process of learning. (JP 1-06)

training and readiness oversight — The authority that combatant commanders may exercise over assigned Reserve Component forces when not on active duty or when on active duty for training. Also called **TRO.** See also **combatant commander.** (JP 1)

transient forces — Forces that pass or stage through, or base temporarily within, the operational area of another command but are not under its operational control. See also **force.** (JP 1)

transit zone — The path taken by either airborne or seaborne smugglers. See also **arrival zone.** (JP 3-07.4)

transmission security — The component of communications security that results from all measures designed to protect communications from interception and exploitation by means other than cryptanalysis. Also called **TRANSEC**. See also **communications security.** (JP 6-0)

transnational threat — Any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens United States national security or interests. (JP 3-26)

transport area — In amphibious operations, an area assigned to a transport organization for the purpose of debarking troops and equipment. See also **inner transport area; outer transport area**. (JP 3-02)

transportation closure — The actual arrival date of a specified movement requirement at port of debarkation. (JP 3-35)

transportation component command — A major command of its parent Service under United States Transportation Command, which includes Air Force Air Mobility Command, Navy Military Sealift Command, and Army Military Surface Deployment and Distribution Command. Also called **TCC.** (JP 4-01.6)

transportation feasibility — A determination that the capability exists to move forces, equipment, and supplies from the point of origin to the final destination within the time required. See also **operation plan.** (JP 4-09)

transportation feasible — A determination made by the supported commander that a draft operation plan can be supported with the apportioned transportation assets. (JP 5-0)

transportation priorities — Indicators assigned to eligible traffic that establish its movement precedence. (JP 4-09)

transportation system — All the land, water, and air routes and transportation assets engaged in the movement of United States forces and their supplies during military operations, involving both mature and immature theaters and at the strategic, operational, and tactical levels of war. (JP 4-01)

transport group — An element that directly deploys and supports the landing of the landing force, and is functionally designated as a transport group in the amphibious task force organization. (JP 3-02)

transshipment point — A location where material is transferred between vehicles. (JP 4-01.5)

troop space cargo — Cargo such as sea or barracks bags, bedding rolls or hammocks, locker trunks, and office equipment, normally stowed in an accessible place, as well as normal hand-carried combat equipment and weapons to be carried ashore by the assault troops. (JP 3-02.1)

turnaround — The length of time between arriving at a point and being ready to depart from that point. (JP 4-01.5)

turning movement — A variation of the envelopment in which the attacking force passes around or over the enemy's principal defensive positions to secure objectives deep in the enemy's rear to force the enemy to abandon his position or divert major forces to meet the threat. (JP 3-06)

two-person rule — A system designed to prohibit access by an individual to nuclear weapons and certain designated components by requiring the presence at all times of at least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task to be performed.

Intentionally Blank

U

unanticipated target — A target of opportunity that was unknown or not expected to exist in the operational environment. See also **operational area; target; target of opportunity.** (JP 3-60)

unauthorized commitment — An agreement that is not binding solely because the United States Government representative who made it lacked the authority to enter into that agreement on behalf of the United States Government. (JP 4-10)

uncertain environment — Operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have totally effective control of the territory and population in the intended operational area. (JP 3-0)

unconventional assisted recovery — Nonconventional assisted recovery conducted by special operations forces. Also called **UAR.** See also **evader; recovery.** (JP 3-50)

unconventional assisted recovery coordination cell — A compartmented special operations forces cell, established to coordinate, synchronize, and deconflict nonconventional assisted recovery operations within the operational area assigned to the joint force commander. Also called **UARCC.** See also **joint operations center; joint personnel recovery center; special operations forces; unconventional assisted recovery.** (JP 3-50)

unconventional warfare — Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area. Also called **UW.** (JP 3-05.1)

undersea warfare — Military operations conducted to establish and maintain control of the undersea portion of the maritime domain. Also called **USW.** See also **antisubmarine warfare; mine warfare.** (JP 3-32)

underwater demolition — The destruction or neutralization of underwater obstacles that is normally accomplished by underwater demolition teams. (JP 3-34)

underwater demolition team — A group of officers and enlisted specially trained and equipped to accomplish the destruction or neutralization of underwater obstacles and associated tasks. Also called **UDT.** (JP 3-34)

unexploded explosive ordnance — Explosive ordnance which has been primed, fused, armed or otherwise prepared for action, and which has been fired, dropped, launched, projected, or placed in such a manner as to constitute a hazard to operations, installations, personnel, or material and remains unexploded either by malfunction or design or for any other cause. Also called **UXO.** See also **explosive ordnance.** (JP 3-15)

unified action — The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1)

unified combatant command — See **unified command.** (JP 1)

unified command — A command with a broad continuing mission under a single commander and composed of significant assigned components of two or more Military Departments that is established and so designated by the President, through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Also called **unified combatant command.** See also **combatant command; subordinate unified command.** (JP 1)

Unified Command Plan — The document, approved by the President, that sets forth basic guidance to all unified combatant commanders; establishes their missions, responsibilities, and force structure; delineates the general geographical area of responsibility for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders. Also called **UCP.** See also **combatant command; combatant commander.** (JP 1)

uniformed services — The Army, Navy, Air Force, Marine Corps, Coast Guard, National Oceanic and Atmospheric Administration, and Public Health Services. See also **Military Department; Service.** (JP 1-0)

unit — 1. Any military element whose structure is prescribed by competent authority. 2. An organization title of a subdivision of a group in a task force. 3. A standard or basic quantity into which an item of supply is divided, issued, or used. Also called **unit of issue.** 4. With regard to Reserve Component of the Armed Forces, a selected reserve unit organized, equipped, and trained for mobilization to serve on active duty as a unit or to augment or be augmented by another unit. (JP 3-33)

unit aircraft — Those aircraft provided an aircraft unit for the performance of a flying mission. (JP 3-17)

United States — Includes the land area, internal waters, territorial sea, and airspace of the United States, including a. United States territories; and b. Other areas over which the United States Government has complete jurisdiction and control or has exclusive authority or defense responsibility. (JP 1)

United States Armed Forces — Used to denote collectively the Army, Marine Corps, Navy, Air Force, and Coast Guard. See also **Armed Forces of the United States.** (JP 1)

United States-controlled shipping — Shipping under United States flag and selected ships under foreign flag considered to be under effective United States control. See also **effective United States-controlled ships.** (JP 4-01.2)

United States message text format — A program designed to enhance joint and combined combat effectiveness through standardization of message formats, data elements, and information exchange procedures. Also called **USMTF.** (JP 3-50)

United States Naval Ship — A public vessel of the United States that is in the custody of the Navy and is: a. Operated by the Military Sealift Command and manned by a civil service crew; or b. Operated by a commercial company under contract to the Military Sealift Command and manned by a merchant marine crew. Also called **USNS.** See also **Military Sealift Command.** (JP 4-01.2)

United States Signals Intelligence System — The unified organization of signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service. It consists of the National Security Agency/Central Security Service, the components of the Military Services authorized to conduct signals intelligence, and such other entities (other than the Federal Bureau of Investigation) authorized by the National Security Council or the Secretary of Defense to conduct signals intelligence activities. Also called **USSS.** See also **counterintelligence.** (JP 2-01.2)

unit identification code — A six-character, alphanumeric code that uniquely identifies each Active, Reserve, and National Guard unit of the Armed Forces. Also called **UIC.** (JP 1-0)

unit line number — A seven-character alphanumeric code that describes a unique increment of a unit deployment, i.e., advance party, main body, equipment by sea and air, reception team, or trail party, in the time-phased force and deployment data. Also called **ULN**. (JP 3-35)

unit movement control center — A temporary organization activated by major subordinate commands and subordinate units during deployment to control and manage marshalling and movement. Also called **UMCC.** See also **deployment; marshaling; unit.** (JP 3-35)

unit movement data — A unit equipment and/or supply listing containing corresponding transportability data. Tailored unit movement data has been modified to reflect a specific movement requirement. Also called **UMD.** (JP 3-35)

unit personnel and tonnage table — A table included in the loading plan of a combat-loaded ship as a recapitulation of totals of personnel and cargo by type, listing cubic measurements and weight. Also called **UP&TT**. (3-02.1)

unit type code — A Joint Chiefs of Staff developed and assigned code, consisting of five characters that uniquely identify a "type unit." Also called **UTC.** (JP 4-02)

unity of command — The operation of all forces under a single responsible commander who has the requisite authority to direct and employ those forces in pursuit of a common purpose. (JP 3-0)

unity of effort — Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization, which is the product of successful unified action. (JP 1)

Universal Joint Task List — A menu of capabilities that may be selected by a joint force commander to accomplish the assigned mission. Also called **UJTL.** (JP 3-33)

universal polar stereographic grid — A military grid prescribed for joint use in operations in limited areas and used for operations requiring precise position reporting. It covers areas between the 80 degree parallels and the poles. (JP 2-03)

Universal Time — A measure of time that conforms, within a close approximation, to the mean diurnal rotation of the Earth and serves as the basis of civil timekeeping. Also called **ZULU time.** (Formerly called Greenwich Mean Time.) (JP 5-0)

unknown — 1. A code meaning "information not available." 2. An unidentified target. An aircraft or ship that has not been determined to be hostile, friendly, or neutral using identification friend or foe and other techniques, but that must be tracked by air defense or naval engagement systems. 3. An identity applied to an evaluated track that has not been identified. See also **assumed friend; friend; neutral; suspect.** (JP 3-01)

unmanned aircraft — An aircraft that does not carry a human operator and is capable of flight with or without human remote control. Also called **UA.** (JP 3-30)

unmanned aircraft system — That system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft. Also called **UAS.** (JP 3-30)

unplanned target — A target of opportunity that is known to exist in the operational environment. See also **operational area; target; target of opportunity.** (JP 3-60)

unrestricted reporting — A process that a Service member uses to disclose, without requesting confidentiality or restricted reporting, that he or she is the victim of a sexual assault. (JP 1-0)

unstable patient — A patient whose physiological status is in fluctuation and for whom emergent, treatment, and/or surgical intervention are anticipated during treatment or evacuation; and the patient's rapidly changing status and requirements are beyond the standard en route care capability and requires medical/surgical augmentation. (JP 4-02)

unstuffing — The removal of cargo from a container. Also called **stripping.** (JP 4-09)

use of force policy — Policy guidance issued by the Commandant, US Coast Guard, on the use of force and weapons. (JP 3-03)

US forces — All Armed Forces (including the Coast Guard) of the United States, any person in the Armed Forces of the United States, and all equipment of any description that either belongs to the US Armed Forces or is being used (including Type I and II Military Sealift Command vessels), escorted, or conveyed by the US Armed Forces. (JP 1)

US national — US citizen and US permanent and temporary legal resident aliens. (JP 1)

US person — For intelligence purposes, a US person is defined as one of the following: (1) a US citizen; (2) an alien known by the intelligence agency concerned to be a permanent resident alien; (3) an unincorporated association substantially composed of US citizens or permanent resident aliens; or (4) a corporation incorporated in the United States, except for those directed and controlled by a foreign government or governments. (JP 2-01.2)

Intentionally Blank

V

validate — Execution procedure used by combatant command components, supporting combatant commanders, and providing organizations to confirm to the supported commander and United States Transportation Command that all the information records in a time-phased force and deployment data not only are error-free for automation purposes, but also accurately reflect the current status, attributes, and availability of units and requirements. (JP 5-0)

validation — 1. A process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. (JP 2-01) 2. A part of target development that ensures all vetted targets meet the objectives and criteria outlined in the commander's guidance and ensures compliance with the law war and rules of engagement. (JP 3-60) 3. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. (JP 3-35) 4. Execution procedure whereby all the information records in a time-phased force and deployment data are confirmed error free and accurately reflect the current status, attributes, and availability of units and requirements. See also **time-phased force and deployment data; verification.** (JP 3-35)

vehicle-borne improvised explosive device — A device placed or fabricated in an improvised manner on a vehicle incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. Also called **VBIED.** (JP 3-10)

vehicle cargo — Wheeled or tracked equipment, including weapons, that require certain deck space, head room, and other definite clearance. (JP 4-01.2)

vehicle summary and priority table — A table detailing all vehicles by priority of debarkation from a combat-loaded ship. Also called **VS&PT.** (JP 3-02.1)

verification — 1. In arms control, any action, including inspection, detection, and identification, taken to ascertain compliance with agreed measures. (JP 3-41) 2. In computer modeling and simulation, the process of determining that a model or simulation implementation accurately represents the developer's conceptual description and specifications. See also **configuration management; validation.** (JP 3-13.1)

vertical envelopment — A tactical maneuver in which troops that are air-dropped, air-landed, or inserted via air assault, attack the rear and flanks of a force, in effect cutting off or encircling the force.. (JP 3-18)

vertical replenishment — The use of a helicopter for the transfer of materiel to or from a ship. Also called **VERTREP.** (JP 3-04)

vertical stowage — A method of stowage in depth within a single compartment by which loaded items are continually accessible for unloading, and the unloading can be completed without corresponding changes or prior unloading of other cargo. (JP 3-02.1)

vetting — A part of target development that assesses the accuracy of the supporting intelligence to targeting. (JP 3-60)

visual information — Various visual media with or without sound that generally includes still and motion photography, audio video recording, graphic arts, and visual presentations. Also called **VI.** (JP 3-61)

visual meteorological conditions — Weather conditions in which visual flight rules apply; expressed in terms of visibility, ceiling height, and aircraft clearance from clouds along the path of flight. Also called **VMC.** See also **instrument meteorological conditions.** (JP 3-04)

Voluntary Intermodal Sealift Agreement — An agreement that provides the Department of Defense with assured access to United States flag assets, both vessel capacity and intermodal systems, to meet Department of Defense contingency requirements. Also called **VISA.** See also **intermodal** (JP 4-01.2)

voluntary tanker agreement — An agreement established by the Maritime Administration to provide for United States commercial tanker owners and operators to voluntarily make their vessels available to satisfy the Department of Defense to meet contingency or war requirements for point-to-point petroleum, oils, and lubricants movements. Also called **VTA.** (JP 4-01.2)

vulnerability — 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 3-01) 2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment. (JP 3-60) 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. See also **information operations.** (JP 3-13)

vulnerability assessment — A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a terrorist attack. Also called **VA.** (JP 3-07.2)

W

walk-in — An unsolicited contact who provides information. (JP 2-01.2)

warden system — An informal method of communication used to pass information to United States citizens living in affected areas overseas during emergencies. See also **noncombatant evacuation operation.** (JP 3-68)

warning intelligence — Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. (JP 2-0)

warning order — 1. A preliminary notice of an order or action that is to follow. 2. A planning directive that initiates the development and evaluation of military courses of action by a supported commander and requests that the supported commander submit a commander's estimate. 3. A planning directive that describes the situation, allocates forces and resources, establishes command relationships, provides other initial planning guidance, and initiates subordinate unit mission planning. Also called **WARNORD.** (JP 5-0)

war reserve materiel requirement — That portion of the war materiel requirement required to be on hand on D-day. This level consists of the war materiel requirement less the sum of the peacetime assets assumed to be available on D-day and the war materiel procurement capability. (JP 4-02)

war reserve stock — That portion of total materiel assets designated to satisfy the war reserve materiel requirement. Also called **WRS.** See also **reserve; war reserve materiel requirement.** (JP 2-03)

wartime reserve modes — Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. Also called **WARM.** (JP 3-13.1)

Washington Liaison Group — An organization consisting of members of Department of State and Department of Defense, chaired by a representative of Department of State, which has basic responsibility for the coordination and implementation of plans for the protection and evacuation in emergencies of persons abroad for whom the Secretaries of State or Defense are responsible. Also called **WLG.** (JP 3-68)

waterspace management — The allocation of waterspace in terms of antisubmarine warfare attack procedures to permit the rapid and effective engagement of hostile submarines while preventing inadvertent attacks on friendly submarines. Also called **WSM.** (JP 3-32)

wave — A formation of forces, including ships, landing craft, amphibious vehicles or aircraft, required to beach or land about the same time. (JP 3-02)

weaponeer — An individual who has completed requisite training to determine the quantity and type of lethal or nonlethal means required to create a desired effect on a given target. (JP 3-60)

weaponeering — The process of determining the quantity of a specific type of lethal or nonlethal means required to create a desired effect on a given target. (JP 3-60)

weapon engagement zone — In air defense, airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with a particular weapon system. Also called **WEZ**. (JP 3-01)

weapons control status — An air defense control measure declared for a particular area and time by an area air defense commander, or delegated subordinate commander, based on the rules of engagement designed to establish the freedom for fighters and surface air defense weapons to engage threats. Also call **WCS.** (JP 3-01)

weapons free zone — An air defense zone established for the protection of key assets or facilities, other than air bases, where weapon systems may be fired at any target not positively recognized as friendly. (JP 3-01)

weapons of mass destruction — Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties, and excluding the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. Also called **WMD.** See also **special operations.** (JP 3-40)

weapons of mass destruction proliferation — The transfer of weapons of mass destruction or related materials, technology, and expertise from suppliers to state or non-state actors. (JP 3-40)

weapons readiness state — The degree of readiness of air defense weapons which can become airborne or be launched to carry out an assigned task and normally expressed in numbers of weapons and numbers of minutes. (JP 3-01)

weapons release authority — The authority originating from the President to engage or direct engagement of ballistic missile threats using ground-based interceptors of the ground-based midcourse defense. Also call **WRA.** (JP 3-01)

weapons technical intelligence — A category of intelligence and processes derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other weapon systems. Also called **WTI.** (JP 3-15.1)

weapon system — A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (JP 3-0)

wellness — Force health protection program that consolidates and incorporates physical and mental fitness, health promotion, and environmental and occupational health. See also **force health protection.** (JP 4-02)

wing — 1. An Air Force unit composed normally of one primary mission group and the necessary supporting organizations. 2. A fleet air wing is the basic organizational and administrative unit for naval-, land-, and tender-based aviation. 3. A balanced Marine Corps task organization of aircraft groups and squadrons, together with appropriate command, air control, administrative, service, and maintenance units. 4. A flank unit; that part of a military force to the right or left of the main body. (JP 3-09.3)

withdrawal operation — A planned retrograde operation in which a force in contact disengages from an enemy force and moves in a direction away from the enemy. (JP 3-17)

witting — A term of intelligence art that indicates that one is not only aware of a fact or piece of information but also aware of its connection to intelligence activities. (JP 2-01.2)

wounded warrior programs – A system of support and advocacy to guide and assist the wounded, ill, and injured Service members and family or designated caregiver through treatment, rehabilitation, return to duty, or military retirement into the civilian community. Each Military Department has a unique wounded warrior program that addresses its Service members' needs. (DODI 6025.22)

working capital fund — A revolving fund established to finance inventories of supplies and other stores, or to provide working capital for industrial-type activities. (JP 1-06)

working group — An enduring or ad hoc organization within a joint force commander's headquarters consisting of a core functional group and other staff and component representatives whose purpose is to provide analysis on the specific function to users. Also called **WG.** (JP 3-33)

Intentionally Blank

X

Intentionally Blank

Y

Intentionally Blank

Z

zone of action — A tactical subdivision of a larger area, the responsibility for which is assigned to a tactical unit; generally applied to offensive action. (JP 3-09)

zone of fire — An area into which a designated ground unit or fire support ship delivers, or is prepared to deliver, fire support. Also called **ZF**. (JP 3-09)

ZULU time — See **Universal Time.**

Intentionally Blank

APPENDIX A
ABBREVIATIONS AND ACRONYMS

A

A	analog
A&P	administrative and personnel; analysis and production
A-1	director of manpower, personnel, and services (Air Force)
A2	antiaccess
A2C2	Army airspace command and control
A-2	intelligence staff officer (Air Force)
A-3	operations directorate (COMAFFOR staff); operations staff officer (Air Force)
A-4	director of logistics (Air Force)
A-5	plans directorate (COMAFFOR staff)
A-6	communications staff officer (Air Force)
A-7	director of installations and mission support (Air Force)
AA	assessment agent; avenue of approach
AA&E	arms, ammunition, and explosives
AAA	antiaircraft artillery; arrival and assembly area; assign alternate area
AABB	American Association of Blood Banks
AABWS	amphibious assault bulk water system
AAC	activity address code
AACG	arrival airfield control group
AADC	area air defense commander
AADP	area air defense plan
AAEC	aeromedical evacuation control team
AAFES	Army and Air Force Exchange Service
AAFIF	automated air facility information file
AAFS	amphibious assault fuel system
AAFSF	amphibious assault fuel supply facility
AAG	aeronautical assignment group
AAGS	Army air-ground system
AAI	air-to-air interface
AAM	air-to-air missile
AAMDC	United States Army Air and Missile Defense Command
AAOE	arrival and assembly operations element
AAOG	arrival and assembly operations group
AAP	Allied administrative publication; assign alternate parent
AAR	after action report; after action review; air-to-air refueling area
AAS	amphibious assault ship
AAST	aeromedical evacuation administrative support team
AAT	automatic analog test; aviation advisory team
AATCC	amphibious air traffic control center

AAU	analog applique unit
AAV	amphibious assault vehicle
AAW	antiair warfare
AB	air base
ABCA	American, British, Canadian, Australian, and New Zealand
ABCS	Army Battle Command System
ABD	airbase defense
ABFC	advanced base functional component
ABFDS	aerial bulk fuel delivery system
ABFS	amphibious bulk fuel system
ABGD	air base ground defense
ABIS	Automated Biometric Identification System
ABL	airborne laser
ABLTS	amphibious bulk liquid transfer system
ABM	antiballistic missile
ABN	airborne
ABNCP	Airborne Command Post
ABO	air base operability; blood typing system
ABP	air battle plan
A/C	aircraft
AC	Active Component; alternating current
AC2	airspace command and control
AC-130	Hercules
ACA	air clearance authority; airlift clearance authority; airspace control authority; airspace coordination area
ACAA	automatic chemical agent alarm
ACAPS	area communications electronics capabilities
ACAT	aeromedical evacuation command augmentation team
ACB	amphibious construction battalion
ACC	Air Combat Command; air component commander; area coordination center; Army Contracting Command
ACCE	air component coordination element
ACCON	acoustic condition
ACCS	air command and control system
ACCSA	Allied Communications and Computer Security Agency
ACD	automated cargo documentation
ACDO	assistant command duty officer
ACE	airborne command element (USAF); air combat element (NATO); Allied Command Europe; aviation combat element (USMC)
ACEOI	automated communications-electronics operating instructions
ACF	air contingency force
ACI	assign call inhibit
ACIC	Army Counterintelligence Center
ACINT	acoustic intelligence

ACK	acknowledgement
ACL	access control list; allowable cabin load
ACLANT	Allied Command Atlantic
ACLP	affiliated contingency load planning
ACM	advanced conventional munitions; advanced cruise missile; air combat maneuver; air contingency Marine air-ground task force (MAGTF); airspace coordinating measure
ACMREQ	airspace control means request; airspace coordination measures request
ACN	assign commercial network
ACO	administrative contracting officer; airspace control order
ACOA	adaptive course of action
ACOC	area communications operations center
ACOCC	air combat operations command center
ACOS	assistant chief of staff
ACP	access control point; air commander's pointer; airspace control plan; Allied communications publication; assign common pool
ACR	armored cavalry regiment (Army); assign channel reassignment
ACS	agile combat support; air-capable ship; airspace control system; auxiliary crane ship
ACSA	acquisition and cross-servicing agreement; Allied Communications Security Agency
AC/S, C4I	Assistant Chief of Staff, Command, Control, Communications, Computers, and Intelligence (USMC)
ACT	activity; advance civilian team; Allied Command Transformation
ACU	assault craft unit
ACV	aircraft cockpit video; armored combat vehicle
ACW	advanced conventional weapons
A/D	analog-to-digital
AD	active duty; advanced deployability; air defense; area denial; automatic distribution; priority add-on
ADA	aerial damage assessment; air defense artillery; Antideficiency Act
A/DACG	arrival/departure airfield control group
ADAFCO	air defense artillery fire control officer
ADAL	authorized dental allowance list
ADAM	air defense airspace management
ADAM/BAE	air defense airspace management/brigade aviation element
ADAMS	Allied Deployment and Movement System
ADANS	Air Mobility Command Deployment Analysis System
ADC	air defense commander; area damage control
ADCAP	advanced capability
A/DCG	arrival/departure control group

ADCI/MS	Associate Director of Central Intelligence for Military Support
ADCON	administrative control
ADD	assign on-line diagnostic
ADDO	Assistant Deputy Director for Operations
ADDO(MS)	Assistant Deputy Director for Operations/Military Support
ADE	airdrop damage estimate; assign digit editing
ADF	automatic direction finding
ADIZ	air defense identification zone
ADKC/RCU	Automatic Key Distribution Center/Rekeying Control Unit
ADL	advanced distributed learning; assign XX (SL) routing
ADM	air defense measure
ADMIN	administration
ADN	Allied Command Europe desired ground zero number
ADNET	anti-drug network
ADOC	air defense operations center
ADP	air defense plan; Army doctrine publication; automated data processing
ADPE	automated data processing equipment
ADPS	automatic data processing system
ADR	accident data recorder; aircraft damage repair; airfield damage repair
ADRA	Adventist Development and Relief Agency
ADRP	Army doctrine reference publication
ADS	air defense section; air defense sector; amphibian discharge site; authoritative data source
ADSIA	Allied Data Systems Interoperability Agency
ADSW	active duty for special work
ADT	active duty for training; assign digital transmission group; automatic digital tester
ADUSD(TP)	Assistant Deputy Under Secretary of Defense, Transportation Policy
ADVON	advanced echelon
ADW	air defense warnings
ADWC	air defense warning condition
ADZ	amphibious defense zone
A/E	ammunition/explosives
AE	aeromedical evacuation; assault echelon; attenuation equalizer
AEC	aeromedical evacuation crew
AECA	Arms Export Control Act
AECM	aeromedical evacuation crew member
AECS	aeromedical evacuation command squadron
AECT	aeromedical evacuation control team
AEF	air expeditionary force

AEG	air expeditionary group
AEHF	advanced extremely high frequency
AELT	aeromedical evacuation liaison team
AEOS	aeromedical evacuation operations squadron
AEOT	aeromedical evacuation operations team
AEPS	aircrew escape propulsion system
AEPST	aeromedical evacuation plans and strategy team
AES	aeromedical evacuation squadron
AESC	aeromedical evacuation support cell
AET	airport emergency team
AETC	Air Education and Training Command
AETF	air expeditionary task force
A/ETF	automated/electronic target folder
AEU	assign essential user bypass
AEW	airborne early warning
AF	Air Force; Air Force (form); amphibious force
AF/A2	Air Force Director of Intelligence, Surveillance, and Reconnaissance
AFAARS	Air Force After Action Reporting System
AFAPD	Air Force Applications Program Development
AFARN	Air Force air request net
AFATDS	Advanced Field Artillery Tactical Data System
AFB	Air Force base
AFC	area frequency coordinator; automatic frequency control
AFCA	Air Force Communications Agency
AFCAP	Air Force contract augmentation program; Armed Forces contract augmentation program
AFCB	Armed Forces Chaplains Board
AFCC	Air Force Component Commander
AFCCC	Air Force Combat Climatology Center
AFCEC	Air Force Civil Engineer Center
AFCEE	Air Force Center for Engineering and the Environment
AFCERT	Air Force computer emergency response team
AFCESA	Air Force Civil Engineering Support Agency
AFD	assign fixed directory
AFDA	Air Force doctrine annex
AFDC	Air Force Doctrine Center
AFDD	Air Force doctrine document
AFDIGS	Air Force digital graphics system
AFDIL	Armed Forces DNA Identification Laboratory
AFDIS	Air Force Weather Agency Dial In Subsystem
AF/DP	Deputy Chief of Staff for Personnel, United States Air Force
AFE	Armed Forces Entertainment
AFEES	Armed Forces Examining and Entrance Station
AFFIS	Air Facilities File Information System
AFFMA	Air Force Frequency Management Agency

AFFOR	Air Force forces
AFH	Air Force handbook
AFHSC	Armed Forces Health Surveillance Center
AFI	Air Force instruction
AFIAA	Air Force Intelligence Analysis Agency
AFICA	Air Force Installation Contracting Agency
AFID	anti-fratricide identification device
AF/IL	Deputy Chief of Staff for Installations and Logistics, USAF
AFIP	Armed Forces Institute of Pathology
AFIRB	Armed Forces Identification Review Board
AFIS	American Forces Information Service
AFISRA	Air Force Intelligence, Surveillance, and Reconnaissance Agency
AFIWC	Air Force Information Warfare Center
AFJI	Air Force joint instruction
AFJMAN	Air Force Joint Manual
AFLC	Air Force Logistics Command
AFLE	Air Force liaison element
AFLNO	Air Force liaison officer
AFMAN	Air Force manual
AFMC	Air Force Materiel Command
AFMD	Air Force Mission Directive
AFME	Armed Forces Medical Examiner
AFMES	Armed Forces Medical Examiner System
AFMIC	Armed Forces Medical Intelligence Center
AFMLO	Air Force Medical Logistics Office
AFMS	Air Force Medical Service
AFNORTH	Air Force North; Allied Forces Northern Europe (NATO)
AFNORTHWEST	Allied Forces North West Europe (NATO)
AFNSEP	Air Force National Security and Emergency Preparedness Agency
AFO	advance force operations
AFOA	Air Force Operations Activity
AFOE	assault follow-on echelon
AFOSI	Air Force Office of Special Investigations
AFPAM	Air Force pamphlet
AFPC	Air Force Personnel Center
AFPD	Air Force policy directive
AFPEO	Armed Forces Professional Entertainment Overseas
AFR	Air Force Reserve; assign frequency for network reporting
AFRAT	Air Force Radiation Assessment Team
AFRC	Air Force Reserve Command; Armed Forces Recreation Center
AFRCC	Air Force Rescue Coordination Center
AFRL	Air Force Research Laboratory
AFRRI	Armed Forces Radiobiology Research Institute

AFRTS	American Forces Radio and Television Service
AFS	aeronautical fixed service
AFSATCOM	Air Force satellite communications (system)
AFSB	afloat forward staging base; Army field support brigade
AFSC	Armed Forces Staff College; Army Field Support Center; United States Air Force specialty code
AFSCN	Air Force Satellite Control Network
AFSMO	Air Force Spectrum Management Office
AFSOAC	Air Force special operations air component
AFSOAD	Air Force special operations air detachment
AFSOAE	Air Force special operations air element
AFSOC	Air Force Special Operations Command
AFSOCC	Air Force special operations control center
AFSOF	Air Force special operations forces
AFSOUTH	Allied Forces, South (NATO)
AFSPACE	United States Space Command Air Force
AFSPC	Air Force Space Command
AFSPOC	Air Force Space Operations Center
AFSTRAT	Air Forces Strategic
AFTAC	Air Force Technical Applications Center
AFTH	Air Force Theater Hospital
AFTN	Aeronautical Fixed Telecommunications Network
AFTO	Air Force technical order
AFTRANS	Air Force Transportation Component
AFTTP	Air Force tactics, techniques, and procedures; Air Force technical training publication
AFTTP(I)	Air Force tactics, techniques, and procedures (instruction)
AFW	Air Force Weather
AFWA	Air Force Weather Agency
AFWCF	Air Force working capital fund
AFWIN	Air Force Weather Information Network
AF/XO	Deputy Chief of Staff for Plans and Operations, United States Air Force
AF/XOI	Air Force Director of Intelligence, Surveillance, and Reconnaissance
AF/XOO	Director of Operations, United States Air Force
A/G	air to ground
AG	adjutant general (Army)
AGARD	Advisory Group for Aerospace Research and Development
AGE	aerospace ground equipment
AGIL	airborne general illumination lightself
AGL	above ground level
AGM-28A	Hound Dog
AGM-65	Maverick
AGM-69	short range attack missile
AGR	Active Guard and Reserve

AGS	aviation ground support
AH	attack helicopter
AHA	alert holding area
AHD	antihandling device
AI	acquisition instruction; airborne interceptor; air interdiction; area of interest
AIA	Air Intelligence Agency
AIASA	annual integrated assessment for security assistance
AIC	air intercept controller; assign individual compressed dial; Atlantic Intelligence Command
AICF/USA	Action Internationale Contre La Faim (International Action Against Hunger)
AIDS	acquired immunodeficiency syndrome
AIF	automated installation intelligence file
AIFA	AAFES Imprest Fund Activity
AIG	addressee indicator group
AIIRS	automated intelligence information reporting system
AIM	Airman's Information Manual
AIM-7	Sparrow
AIM-9	Sidewinder
AIM-54A	Phoenix
AIMD	aircraft intermediate maintenance department
AIMT	air interdiction of maritime targets
AIP	aeronautical information publication
AIQC	antiterrorism instructor qualification course
AIRBAT	Airborne Intelligence, Surveillance, and Reconnaissance Requirements-Based Allocation Tool
AIRCENT	Allied Air Forces Central Europe (NATO)
AIRCOR	air corridor
AIRES	advanced imagery requirements exploitation system
AIREVACCONFIRM	air evacuation confirmation
AIREVACREQ	air evacuation request
AIREVACRESP	air evacuation response
AIRNORTHWEST	Allied Air Forces North West Europe (NATO)
AIRREQRECON	air request reconnaissance
AIRSOUTH	Allied Air Forces Southern Europe (NATO)
AIRSUPREQ	air support request
AIS	automated information system
AIT	aeromedical isolation team; automatic identification technology; automated information technology
AIU	Automatic Digital Network Interface Unit
AJ	anti-jam
AJBPO	area joint blood program office
AJCC	alternate joint communications center
AJ/CM	anti-jam control modem
AJD	allied joint doctrine

AJF	allied joint force
AJFP	adaptive joint force packaging
AJMRO	area joint medical regulating office
AJNPE	airborne joint nuclear planning element
AJODWG	allied joint operations doctrine working group
AJP	allied joint publication
AK	commercial cargo ship
AKNLDG	acknowledge message
ALARA	as low as reasonably achievable
ALCC	airlift control center
ALCE	airlift control element
ALCF	airlift control flight
ALCG	analog line conditioning group
ALCM	air-launched cruise missile
ALCOM	United States Alaskan Command
ALCON	all concerned
ALCS	airlift control squadron
ALCT	airlift control team
ALD	airborne laser designator; available-to-load date
ALE	airlift liaison element
ALEP	amphibious lift enhancement program
ALERFA	alert phase (ICAO)
ALERT	attack and launch early reporting to theater
ALERTORD	alert order
ALLOREQ	air allocation request; allocation request
ALLTV	all light level television
ALMSNSCD	airlift mission schedule
ALN	ammunition lot number
ALNOT	alert notice
ALO	air liaison officer
ALOC	air line of communications
ALORD	alert launch order
ALP	allied logistic publication
ALSA	Air Land Sea Application (Center)
ALSE	aviation life support equipment
ALSS	advanced logistic support site
ALT	acquisition, logistics, and technology
ALTD	airborne laser target designator
ALTRV	altitude reservation
ALTTSC	alternate Tomahawk strike coordinator
A/M	approach and moor
AM	amplitude modulation
AMAL	authorized medical allowance list
AMB	air mobility branch; ambassador
AMBUS	ambulance bus
AMC	airborne mission coordinator; Air Mobility Command;

	Army Materiel Command: midpoint compromise search area
AMCC	allied movement coordination center; alternate military command center
AMCIT	American citizen
AMCM	airborne mine countermeasures
AMC/SGXM	Air Mobility Command/Command Surgeon's Office
AMCT	air mobility control team
AMD	air and missile defense; air mobility division
AMDC	air and missile defense commander
AME	antenna mounted electronics
AMEDD	Army Medical Department
AMEDDCS	U.S. Army Medical Department Center and School
AMedP	allied medical publication
AMEMB	American Embassy
AMETL	agency mission-essential task list
AMF(L)	ACE Mobile Force (Land) (NATO)
AMH	automated message handler
AMHS	automated message handling system
AMIO	alien migrant interdiction operations
AMLO	air mobility liaison officer
AMMO	ammunition
AMOC	Air and Marine Operations Center (DHS)
AMOCC	air mobility operations control center
AMOG	air mobility operations group
AMOPES	Army Mobilization and Operations Planning and Execution System
AMOPS	Army mobilization and operations planning system; Army mobilization operations system
AMOS	air mobility operations squadron
AMOSS	Air and Marine Operations Surveillance System
AMOW	air mobility operations wing
AMP	amplifier; analysis of mobility platform
AMPE	automated message processing exchange
AMPN	amplification
AMP-PAT	analysis of mobility platform suite of port analysis tools
AMPSSO	Automated Message Processing System Security Office (or Officer)
AMRAAM	advanced medium-range air-to-air missile
AMS	Aerial Measuring System (DOE); air mobility squadron; Army management structure; Asset Management System
AMSS	air mobility support squadron
AMS-TAC	Automated Manifesting System–Tactical
AMT	aerial mail terminal
amu	atomic mass unit

AMVER	automated mutual-assistance vessel rescue system
AMW	air mobility wing; amphibious warfare
AMX	air mobility express
AN	alphanumeric; analog nonsecure
ANCA	Allied Naval Communications Agency
ANDVT	advanced narrowband digital voice terminal
ANG	Air National Guard
ANGLICO	air-naval gunfire liaison company
ANGUS	Air National Guard of the United States
A/NM	administrative/network management
ANMCC	Alternate National Military Command Center
ANN	assign NNX routing
ANR	Alaskan North American Aerospace Defense Command Region
ANSI	American National Standards Institute
ANX	assign NNXX routing
ANY	assign NYX routing
ANZUS	Australia-New Zealand-United States Treaty
AO	action officer; administration officer; air officer; area of operations; aviation ordnance person
AO&M	administration, operation, and maintenance
AOA	amphibious objective area
AOB	aviation operations branch
AOC	air operations center; Army operations center
AOCC	air operations control center
AOC-E	Aviation Operations Center-East (USCS)
AOCU	analog orderwire control unit
AOC-W	Aviation Operations Center-West (USCS)
AOD	air operations directive; on-line diagnostic
AODB	air operations database
AOF	azimuth of fire
AOG	Army Operations Group
AOI	area of interest
AOP	air operations plan; area of probability
AOR	area of responsibility
AOS	aircraft on station
AOSS	aviation ordnance safety supervisor
AOTR	Aviation Operational Threat Response
AP	allied publication; antipersonnel; average power
APA	Army pre-positioned afloat
APAN	All Partners Access Network; Asia-Pacific Area Network
APC	aerial port commander; assign preprogrammed conference list
APCC	alternate processing and correlation center
APE	airfield pavement evaluation
APES	Automated Patient Evacuation System

APEX	Adaptive Planning and Execution
APF	afloat pre-positioning force
APG	aimpoint graphic
APHIS	Animal and Plant Health Inspection Service (USDA)
APIC	allied press information center
APL	antipersonnel land mine
APO	afloat pre-positioning operations; Air Force post office; Army post office
APOD	aerial port of debarkation
APOE	aerial port of embarkation
APORT	aerial port
APORTSREP	air operations bases report
APP	allied procedural publication
APPS	analytical photogrammetric positioning system
APR	assign primary zone routing
APS	Army pre-positioned stocks
APS-3	afloat pre-positioning stocks; Army pre-positioned stocks-3
APTD	aircraft position target designation
APU	auxiliary power unit
AR	air refueling; Army regulation; Army reserve
ARB	alternate recovery base; assign receive bypass lists
ARBS	angle rate bombing system
ARC	air Reserve Components; American Red Cross
ARCENT	United States Army Central Command
ARCT	air refueling control team
ARDF	automatic radio direction finding
AREC	air resource element coordinator
ARFOR	Army forces
ARG	Accident Response Group (DOE); amphibious ready group
ARGO	automatic ranging grid overlay
ARINC	Aeronautical Radio Incorporated
ARL-M	airborne reconnaissance low-multifunction
ARM	air reference measure; antiradiation missile
ARNG	Army National Guard
ARNGUS	Army National Guard of the United States
ARP	air refueling point
ARPERCEN	United States Army Reserve Personnel Center
ARQ	automatic request-repeat
ARRC	Allied Command Europe Rapid Reaction Corps (NATO)
ARRDATE	arrival date
ARS	acute radiation syndrome; air rescue service
ARSOA	Army special operations aviation
ARSOF	Army special operations forces
ARSOTF	Army special operations task force

ARSPACE	Army Space Command
ARSPOC	Army space operations center
ART	air reserve technician
ARTS III	Automated Radar Tracking System
ARTYMET	artillery meteorological
AS	analog secure
A/S	anti-spoofing
ASA	automatic spectrum analyzer
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics, and Technology
ASAP	as soon as possible
ASARS	Advanced Synthetic Aperture Radar System
ASAS	All Source Analysis System
ASAT	antisatellite weapon
ASB	naval advanced support base
ASBP	Armed Services Blood Program
ASBPO	Armed Services Blood Program Office
ASC	acting service chief; Aeronautical Systems Center; Air Systems Command; Army Sustainment Command; assign switch classmark; Automatic Digital Network switching center
ASCC	Air Standardization Coordinating Committee; Army Service component command; Army Service component commander
ASCIET	all Services combat identification evaluation team
ASCII	American Standard Code for Information Interchange
ASCOPE	areas, structures, capabilities, organizations, people, and events
ASCS	air support control section; air support coordination section
ASD	Assistant Secretary of Defense
ASD(A&L)	Assistant Secretary of Defense (Acquisition and Logistics)
ASD(C)	Assistant Secretary of Defense (Comptroller)
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASD(FM&P)	Assistant Secretary of Defense (Force Management and Personnel)
ASD(FMP)	Assistant Secretary of Defense (Force Management Policy)
ASD(GSA)	Assistant Secretary of Defense for Global Strategic Affairs
ASD(HA)	Assistant Secretary of Defense (Health Affairs)
ASD(HD)	Assistant Secretary of Defense (Homeland Defense)
ASD(HD&ASA)	Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs)
ASDI	analog simple data interface
ASDIA	All-Source Document Index

ASD(ISA)	Assistant Secretary of Defense (International Security Affairs)
ASD(ISP)	Assistant Secretary of Defense (International Security Policy)
ASD(LA)	Assistant Secretary of Defense (Legislative Affairs)
ASD(L&MR)	Assistant Secretary of Defense for Logistics and Materiel Readiness
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)
ASD(OEPP)	Assistant Secretary of Defense for Operational Energy Plans and Programs
ASD(P&L)	Assistant Secretary of Defense (Production and Logistics)
ASD(PA)	Assistant Secretary of Defense (Public Affairs)
ASD(PA&E)	Assistant Secretary of Defense (Program Analysis and Evaluation)
ASD(RA)	Assistant Secretary of Defense (Reserve Affairs)
ASD(RSA)	Assistant Secretary of Defense (Regional Security Affairs)
ASD(S&R)	Assistant Secretary of Defense (Strategy and Requirements)
ASD(SO/LIC)	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
ASD(SO/LIC&IC)	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities
ASE	aircraft survivability equipment; automated stabilization equipment
ASF	aeromedical staging facility
ASG	Allied System for Geospatial Intelligence; area support group
ASH	Assistant Administrator for Security and Hazardous Materials; Assistant Secretary for Health (DHHS)
ASI	assign and display switch initialization
ASIC	Air and Space Interoperability Council
ASIF	Airlift Support Industrial Fund
ASL	allowable supply list; archipelagic sea lane; assign switch locator (SL) routing; authorized stockage list (Army)
ASLT	air support liaison team; assault support landing table
ASM	air-to-surface missile; armored scout mission; Army Spectrum Manager; automated scheduling message
ASMD	antiship missile defense
ASMO	Army Spectrum Management Office
ASN(RD&A)	Assistant Secretary of the Navy for Research, Development and Acquisition
ASO	advanced special operations; air support operations
ASOC	air support operations center
ASOFDTG	as of date/time group

ASP	ammunition supply point
ASPA	American Service-Members' Protection Act
A-Space	Analytic Space
ASPP	acquisition systems protection program
ASPPO	Armed Service Production Planning Office
ASPR	Office of Assistant Secretary for Preparedness and Response (DHHS)
ASR	air support request; available supply rate
ASSETREP	transportation assets report
AST	assign secondary traffic channels
ASTS	aeromedical staging squadron
ASW	antisubmarine warfare; average surface wind
ASWBPL	Armed Services Whole Blood Processing Laboratories
ASWC	antisubmarine warfare commander
AT	antitank; antiterrorism
At	total attainable search area
ATA	Airlift Tanker Association; antiterrorism assistance
ATAC	antiterrorism alert center (Navy)
ATACC	advanced tactical air command center
ATACMS	Army Tactical Missile System
ATACO	air tactical actions control officer
ATACS	Army Tactical Communications System
ATAF	Allied Tactical Air Force (NATO)
ATBM	antitactical ballistic missile
ATC	Air Threat Conference; air traffic control; air transportable clinic (USAF)
ATCA	Allied Tactical Communications Agency
ATCAA	air traffic control assigned airspace
ATCC	Antiterrorism Coordinating Committee
ATCC-SSG	Antiterrorism Coordinating Committee-Senior Steering Group
ATCM	air traffic control measure
ATCRBS	Air Traffic Control Radar Beacon System
ATCS	air traffic control section
ATDLS	Advanced Tactical Data Link System
ATDM	adaptive time division multiplexer
ATDS	airborne tactical data system
ATEP	Antiterrorism Enterprise Portal
ATF	Advanced Targeting FLIR; amphibious task force; Bureau of Alcohol, Tobacco, Firearms, and Explosives (DOJ)
AT/FP	antiterrorism/force protection
ATG	amphibious task group; assign trunk group cluster
ATGM	antitank guided missile; antitank guided munition
ATH	air transportable hospital; assign thresholds
ATHS	Airborne Target Handover System
ATI	asset target interaction

ATM	advanced trauma management; air target material; assign traffic metering
ATMCT	air terminal movement control team
ATMP	Air Target Materials Program
ATN	assign thresholds
AtN	attack the network
ATO	air tasking order; antiterrorism officer
ATOC	air tactical operations center; air terminal operations center
ATP	advanced targeting pod; allied tactical publication; Army tactical publication; Army technical publication; Army techniques publication
ATR	attrition reserve
ATS	air traffic service; assign terminal service
ATSD(AE)	Assistant to the Secretary of Defense (Atomic Energy)
ATSD(IO)	Assistant to the Secretary of Defense (Intelligence Oversight)
ATSD(NCB)	Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs
ATSDR	Agency for Toxic Substances and Disease Registry (DHHS)
ATT	assign terminal type
ATTP	Army tactics, techniques, and procedures
ATTU	air transportable treatment unit
ATWG	antiterrorism working group
AU	African Union
AUEL	automated unit equipment list
AUF	airborne use of force
AUG	application user group
AUIC	active duty unit identification code
AUSCANNZUKUS	Australian, Canadian, New Zealand, United Kingdom, United States
AUTODIN	Automatic Digital Network
AUX	auxiliary
AV	air vehicle; asset visibility
AV-8	Harrier
AVC	Bureau of Arms Control, Verification, and Compliance (DOS)
AVCAL	aviation consolidated allowance list
AVDTG	analog via digital trunk group
AVGAS	aviation gasoline
AVIM	aviation intermediate maintenance
AVL	anti-vehicle land mine; assign variable location
AVOU	analog voice orderwire unit
AVOW	analog voice orderwire
AVS	asset validation system; asset visibility system; audiovisual squadron
AVUM	aviation unit maintenance
AV/VI	audiovisual/visual information

AW	air warfare
AWACS	Airborne Warning and Control System
AWC	air warfare commander
AWCAP	airborne weapons corrective action program
AWDS	automated weather distribution system
AWG	Asymmetric Warfare Group (Army)
AWN	Automated Weather Network
AWNIS	Allied Worldwide Navigational Information System
AWOL	absent without leave
AWS	Air Weather Service
AWSE	armament weapons support equipment
AWSIM	air warfare simulation model
AWSR	Air Weather Service regulation
AXO	abandoned explosive ordnance
AXX	assign XXX routing
AZR	assign zone restriction lists

Intentionally Blank

B

B	cross-over barrier pattern
B-52	Stratofortress
B&A	boat and aircraft
BAE	brigade aviation element
BAF	backup alert force
BAG	baggage
BAH	basic allowance for housing
BAI	backup aircraft inventory; battlefield air interdiction
BALO	battalion air liaison officer
BALS	berthing and loading schedule
BAS	basic allowance for subsistence; battalion aid station
BATF	Bureau of Alcohol, Tobacco, and Firearms
B/B	baseband
BB	breakbulk
bbl	barrel (42 US gallons)
BC	bottom current
BCA	border crossing authority
BCAT	beddown capability assessment tool
BCC	battle control center
BCD	battlefield coordination detachment
BCG	beach control group
BCI	bit count integrity
BCL	battlefield coordination line
BCN	beacon
BCOC	base cluster operations center
BCR	baseline change request
BCT	brigade combat team
BCTP	battle command training program
BCU	beach clearance unit
BD	barge derrick
BDA	battle damage assessment
BDAREP	battle damage assessment report
BDC	blood donor center
BDE	brigade
BDL	beach discharge lighter
BDOC	base defense operations center
BDR	battle damage repair
BDRP	Biological Defense Research Program
BDZ	base defense zone
BE	basic encyclopedia
BEAR	base expeditionary airfield resources
BEE	bioenvironmental engineering officer
BEI	biometrics-enabled intelligence
BEN	base encyclopedia number

BE number	basic encyclopedia number
BER	bit error ratio
BES	budget estimate submission
BEST	border enforcement security task force
BfV	*Bundesamt für Verfassungsschutz (*federal office for defending the Constitution)
BGC	boat group commander
BHR	Bureau of Humanitarian Response
BI	battlefield injury; battle injury
BIA	behavioral influences analysis; Bureau of Indian Affairs
BIAR	biometric intelligence analysis report
BIAS	Battlefield Illumination Assistance System
BICES	battlefield information collection and exploitation system (NATO)
BICON	double container
BIDDS	Base Information Digital Distribution System
BIDE	basic identity data element
BIFC	Boise Interagency Fire Center
BIFS	Border Intelligence Fusion Section
BIH	International Time Bureau (Bureau International d'l'Heure)
BII	base information infrastructure
BIMA	Biometrics Identity Management Agency
BINM	Bureau of International Narcotics Matters
BIO	biological; Bureau of International Organizations
BIS	Bureau of Industry and Security
BISS	base installation security system
BIT	built-in test
BITE	built-in test equipment
BIU	beach interface unit
BKA	*Bundeskriminalamt* (federal criminal office)
BKB	blue kill box
BL	biocontainment level
BLCP	beach lighterage control point
BLDREP	blood report
BLDSHIPREP	blood shipment report
BLM	Bureau of Land Management
BLOS	beyond line-of-sight
BLT	battalion landing team
BM	ballistic missile; battle management; beach module
BMC4I	Battle Management Command, Control, Communications, Computers, and Intelligence
BMCT	begin morning civil twilight
BMD	ballistic missile defense
BMDO	Ballistic Missile Defense Organization
BMDS	ballistic missile defense system

BMET	biomedical electronics technician
BMNT	begin morning nautical twilight
BMU	beachmaster unit
BN	battalion
BND	*Bundesnachrichtendienst* (federal intelligence service)
BOA	basic ordering agreement
BOC	base operations center; bomb on coordinate
BOCCA	Bureau of Coordination of Civil Aircraft (NATO)
BOG	beach operations group
BOH	bottom of hill
BORFIC	Border Patrol Field Intelligence Center
BOS	base operating support; battlefield operating system
BOSG	base operations support group
BOS-I	base operating support-integrator
BOSS	base operating support service
BOT	bomb on target
BP	battle position; block parity
BPA	blanket purchase agreement
BPC	building partnership capacity
BPD	blood products depot
BPG	beach party group
BPI	bits per inch
BPLAN	base plan
BPO	blood program office
BPPBS	bi-annual planning, programming, and budget system
bps	bits per second
BPSK	biphase shift keying
BPT	beach party team
BPWRR	bulk petroleum war reserve requirement
BPWRS	bulk petroleum war reserve stocks
BR	budget review
BRAC	base realignment and closure
BRACE	Base Resource and Capability Estimator
BRC	base recovery course
BS	battle staff; broadcast source
BSA	beach support area; brigade support area
BSB	brigade support battalion
BSC	behavioral science consultant; black station clock
BSC ro	black station clock receive out
BSCT	behavioral science consultation team
BSD	blood supply detachment
BSI	base support installation
BSP	base support plan
BSRP	bureau strategic resource plan
BSSG	brigade service support group
BSU	blood supply unit

BSZ	base security zone
BT	bathythermograph
BTB	believed-to-be
BTC	blood transshipment center
BTG	basic target graphic
BTOC	battalion tactical operations center
BTS	Border and Transportation Security (DHS)
BTU	beach termination unit
BTWC	Biological and Toxin Weapons Convention
BULK	bulk cargo
BUMEDINST	Bureau of Medicine and Surgery instruction
BVR	beyond visual range
BW	biological warfare
BWC	Biological Weapons Convention
BZ	buffer zone

C

C	Celsius; centigrade; clock; compromise band; coverage factor; creeping line pattern
C&A	certification and accreditation
C&E	communications and electronics
C&LAT	cargo and loading analysis table
C2	command and control
C2-attack	an offensive form of command and control warfare
C2CRE	command and control chemical, biological, radiological, and nuclear response element
C2E	command and control element
C2IP	Command and Control Initiatives Program
C2IPS	Command and Control Information Processing System
C2P	command and control protection
C2-protect	a defensive form of command and control warfare
C2S	command and control support
C-2X	coalition Intelligence Directorate counterintelligence and human intelligence staff element
C3	command, control, and communications
C3AG	Command, Control, and Communications Advisory Group
C3CM	command, control, and communications countermeasures
C3I	command, control, communications, and intelligence
C3IC	coalition coordination, communications, and integration center
C3SMP	Command, Control, and Communications Systems Master Plan
C4CM	command, control, communications, and computer countermeasures
C4I	command, control, communications, computers, and intelligence
C4IFTW	command, control, communications, computers, and intelligence for the Warrior
C4S	command, control, communications, and computer systems
C4 systems	command, control, communications, and computer systems
C-5	Galaxy
C-17	Globemaster III
C-21	Learjet
C-27	Spartan
C-130	Hercules
C-141	Starlifter
CA	chaplain assistant; civil administration; civil affairs; combat assessment; coordinating altitude; credibility assessment; criticality assessment
C/A	course acquisition

CAA	civil air augmentation; combat aviation advisors; command arrangement agreement
CAAF	contractors authorized to accompany the force
CAB	combat aviation brigade
CAC	common access card; current actions center
CACOM	civil affairs command
CACTIS	community automated intelligence system
CAD	Canadian air division; cartridge actuated device; collective address designator; contract administration delegation
CADRS	concern and deficiency reporting system
CADS	containerized ammunition distribution system
CAF	Canadian Air Force; combat air forces; commander, airborne/air assault force; commander, amphibious force
CAFMS	computer-assisted force management system
CAG	carrier air group; civil affairs group; collective address group
CAGO	contractor-acquired, government-owned
CAIMS	conventional ammunition integrated management system
CAINS	carrier aircraft inertial navigation system
CAIS	civil authority information support
CAISE	civil authority information support element
CAL	caliber; critical asset list
CALA	Community Airborne Library Architecture
CALCM	conventional air-launched cruise missile
CALICS	communication, authentication, location, intentions, condition, and situation
CALMS	computer-aided load manifesting system
CAM	chemical agent monitor; crisis action module
CAMOC	Caribbean Air and Marine Operations Center
CAMPS	Consolidated Air Mobility Planning System
CAMT	countering air and missile threats
CANA	convulsant antidote for nerve agent
CANADA COM	Canada Command
CANR	Canadian North American Aerospace Defense Command Region
CANUS	Canada-United States
CANUS BDD	Canada-United States Basic Defense Document
CANUS CDP	Canada-United States Combined Defense Plan
CAO	chief administrative officer; civil affairs operations; counterair operation
CAOC	combat air operations center; combined air operations center
CAO SOP	standing operating procedures for coordination of atomic operations
CAP	Civil Air Patrol; civil augmentation program; combat air patrol; configuration and alarm panel; Consolidated Appeals Process (UN); crisis action planning

CAPM	credibility assessment program manager
CAPT	civil affairs planning team
CAR	Chief of the Army Reserve
CARA	chemical, biological, radiological, nuclear, and high-yield explosives analytical and remediation activity
CARDA	continental United States airborne reconnaissance for damage assessment; continental United States area reconnaissance for damage assessment
CARE	Cooperative for Assistance and Relief Everywhere (CAREUSA)
CARIBROC	Caribbean Regional Operations Center
CARP	computed air release point; contingency alternate route plan
CARS	combat arms regimental system
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CAS	casualty; civil aviation security; close air support
CASEVAC	casualty evacuation
CASF	contingency aeromedical staging facility
CASP	computer-aided search planning
CASPER	contact area summary position report
CASREP	casualty report
CASREQ	close air support request
CAT	category; civil affairs team; crisis action team
CATCC	carrier air traffic control center
CATF	commander, amphibious task force
CAU	crypto ancillary unit; cryptographic auxiliary unit
CAVU	ceiling and visibility unlimited
CAW	carrier air wing
CAW/ESS	crisis action weather and environmental support system
CAX	computer-assisted exercise
C-B	chemical-biological
CB	chemical-biological; construction battalion (SEABEES)
CBBLS	hundreds of barrels
CBCP	Customs and Border Clearance Program (DOD)
CBD	chemical, biological defense
CBFS	cesium beam frequency standard
CBG	coalition building guide
CBIRF	Chemical-Biological Incident Response Force
CBLTU	common battery line terminal unit
CBMR	capabilities-based munitions requirements
CBMU	construction battalion maintenance unit
CBP	capabilities-based planning; Customs and Border Protection (DHS)
CBPO	Consolidated Base Personnel Office
CBPS	chemical biological protective shelter

CBR	chemical, biological, and radiological
CBRN	Caribbean Basin Radar Network; chemical, biological, radiological, and nuclear
CBRN CM	chemical, biological, radiological, and nuclear consequence management
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CBRN hazard	chemical, biological, radiological, and nuclear hazard
CBRT	chemical-biological response team
CBS	common battery signaling
CBSA	Canadian Border Services Agency
CBT	common battery terminal
CbT	combating terrorism
CbT-RIF	Combating Terrorism Readiness Initiatives Fund
CBTZ	combat zone
CBU	conference bridge unit; construction battalion unit
CBW	chemical and biological warfare
C/C	cabin cruiser; cast off and clear
CC	component command (NATO); component commander; critical capability
CC&D	camouflage, concealment, and deception
CCA	carrier-controlled approach; central contracting authority; circuit card assembly; close combat attack; combat cargo assistant; container control activity; contamination control area; contingency capabilities assessment; contract construction agent
CCAP	combatant command AFRTS planner
CCAS	contingency contract administration services
CCAS-C	contingency contract administration services commander
CCATT	critical care air transport team
CCB	Community Counterterrorism Board; configuration control board
CCC	coalition coordination cell; coalition coordination center; crisis coordination center; critical control circuit; cross-cultural communications course
CCD	camouflage, concealment, and deception
CCDB	consolidated counterdrug database
CCDR	combatant commander
CCE	container control element; continuing criminal enterprise
CCEB	Combined Communications-Electronics Board
CCF	collection coordination facility
CCG	combat communications group; crisis coordination group
CCGD	commander, Coast Guard district
CCIB	command center integration branch
CCICA	command counterintelligence coordinating authority
CCIF	Combatant Commander Initiative Fund

CCIP	continuously computed impact point
CCIR	commander's critical information requirement; International Radio Consultative Committee
CCIS	common channel interswitch signaling
CCITT	International Telegraph and Telephone Consultative Committee
CCIU	CEF control interface unit
CCJTF	commander, combined joint task force
CCL	communications/computer link
CCLI	commerce control list item; computer control list item
CCMD	combatant command
CCO	central control officer; combat cargo officer; command and control office; container control officer; contingency contracting officer
CCOI	critical contact of interest
CCP	casualty collection point; consolidated cryptologic program; consolidation and containerization point
CCPDS	command center processing and display system
CCR	closed circuit refueling
CCRD	combatant commander's required delivery date
C-CS	communication and computer systems
CCS	central control ship; commander's communication synchronization; container control site; core capability set
CCSA	combatant command support agent
CCSD	command communications service designator; control communications service designator
CCT	collaborative contingency targeting; combat control team
CCTI	Chairman of the Joint Chiefs of Staff commended training issue
CCTV	closed circuit television
CCW	1980 United Nations Convention on Conventional Weapons; continuous carrier wave
CD	channel designator; compact disc; counterdrug; customer direct
CDC	Centers for Disease Control and Prevention (DHHS)
CDD	chemical decontamination detachment
CDE	collateral damage estimation
CDEMA	Caribbean Disaster Emergency Management Agency
CDERA	Caribbean Disaster Emergency Response Agency
CDF	combined distribution frame
CDI	cargo disposition instructions; conditioned diphase
C di	conditioned diphase
CDHAM	Center for Disaster and Humanitarian Assistance Medicine
CDIP	combined defense improvement project

CDIPO	counterdrug intelligence preparation for operations
CDLMS	common data link management system
CDM	cable driver modem; collateral damage methodology
CDMGB	cable driver modem group buffer
CDN	compressed dial number
CDO	command duty officer; commander, detainee operations
CDOC	counterdrug operations center
CDOPS	counterdrug operations
CDP	commander's dissemination policy; landing craft air cushion departure point
CDR	commander; continuous data recording
CDRAFNORTH	Commander, Air Force North
CDRAFSOF	commander, Air Force special operations forces
CDRCFCOM	Commander, Combined Forces Command
CDRESC	commander, electronic security command
CDREUDAC	Commander, European Command Defense Analysis Center (ELINT) or European Data Analysis Center
CDRFORSCOM	Commander, Forces Command
CDRG	catastrophic disaster response group (FEMA)
CDRJSOTF	commander, joint special operations task force
CDRL	contract data requirements list
CDRMTMC	Commander, Military Traffic Management Command
CDRNORAD	Commander, North American Aerospace Defense Command
CD-ROM	compact disc read-only memory
CDRTSOC	commander, theater special operations command
CDRUNC	Commander, United Nations Command
CDRUSAFRICOM	Commander, United States Africa Command
CDRUSAINSCOM	Commander, United States Army Intelligence and Security Command
CDRUSARNORTH	Commander, United States Army, North
CDRUSCENTCOM	Commander, United States Central Command
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSELEMNORAD	Commander, United States Element, North American Aerospace Defense Command
CDRUSEUCOM	Commander, United States European Command
CDRUSJFCOM	Commander, United States Joint Forces Command
CDRUSNAVEUR	Commander, United States Naval Forces, Europe
CDRUSNORTHCOM	Commander, United States Northern Command
CDRUSPACOM	Commander, United States Pacific Command
CDRUSSOCOM	Commander, United States Special Operations Command
CDRUSSOUTHCOM	Commander, United States Southern Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CDRUSTRANSCOM	Commander, United States Transportation Command
CDS	Chief of Defence Staff (Canada); container delivery system
CDSSC	continuity of operations plan designated successor service chief

CDU	counterdrug update
C-E	communications-electronics
CE	casualty estimation; circular error; command element (USMC); communications-electronics; core element; counterespionage; critical element
CEA	captured enemy ammunition
CEB	combat engineer battalion
CEC	civil engineer corps
CECOM	communications-electronics command
CEDI	commercial electronic data interface
CEDREP	communications-electronics deployment report
CEE	captured enemy equipment
CEF	civil engineering file; common equipment facility
CEG	common equipment group
CEHC	Counter Explosive Hazards Center (Army)
CEI	critical employment indicator
CELLEX	cellular exploitation
CEM	combined effects munition
CEMC	communications-electronics management center
CEMIRT	civil engineer maintenance, inspection, and repair team
CENTRIXS	Combined Enterprise Regional Information Exchange System
CEOI	communications-electronics operating instructions
CEP	cable entrance panel; Chairman's Exercise Program
CEPOD	communications-electronics post-deployment report
CERF	Central Emergency Revolving Fund (UN)
CERFP	chemical, biological, radiological, nuclear, and high-yield explosives enhanced response force package
CERP	Commanders' Emergency Response Program
CERT	computer emergency response team; contingency engineering response team
CERTSUB	certain submarine
CES	coast earth station
CESE	civil engineering support equipment; communications equipment support element
CESG	communications equipment support group
CESO	civil engineer support office
CESPG	civil engineering support plan group; civil engineering support planning generator
CEXC	combined explosives exploitation cell
CEW	civilian expeditionary workforce
CF	Canadian forces; carrier furnished; causeway ferry; conventional forces; drift error confidence factor
CFA	Committee on Food Aid Policies and Programmes (UN); critical factors analysis
CFACC	combined force air component commander

CFB	Canadian forces base
CFC	Combined Forces Command, Korea
CF-COP	counterfire common operational picture
CFL	Contingency Planning Facilities List; coordinated fire line
CFLCC	coalition forces land component commander
CFM	cubic feet per minute
CFO	chief financial officer
CFPM	causeway ferry power module
CFR	Code of Federal Regulations
CFS	CI force protection source
CFSO	counterintelligence force protection source operations
CFST	coalition forces support team
CG	Chairman's guidance; Coast Guard; commanding general; Comptroller General
CG-652	Coast Guard Spectrum Management and Telecommunications Policy Division
CGAS	Coast Guard Air Station
CGAUX	Coast Guard Auxiliary
CGC	Coast Guard Cutter
CGCAP	Coast Guard capabilities plan
CGCG	Coast Guard Cryptologic Group
CGCIS	Coast Guard Counterintelligence Service
CGDEFOR	Coast Guard defense force
CGFMFLANT	Commanding General, Fleet Marine Forces, Atlantic
CGFMFPAC	Commanding General, Fleet Marine Forces, Pacific
CGIS	United States Coast Guard Investigative Service
CGLSMP	Coast Guard logistic support and mobilization plan
CGP	Coast Guard publication
CGRS	common geographic reference system
CGS	common ground station; continental United States ground station
CGUSAREUR	Commanding General, United States Army, Europe
CH	channel; contingency hospital
CH-53	Sea Stallion
CHAMPUS	Civilian Health and Medical Program for the Uniformed Services
CHARC	counterintelligence and human intelligence analysis and requirements cell
CHB	cargo-handling battalion
CHCS	composite health care system
CHCSS	Chief, Central Security Service
CHE	cargo-handling equipment; container-handling equipment
CHET	customs high endurance tracker
CHOP	change of operational control
CHPPM	US Army Center for Health Promotion and Preventive Medicine

CHRIS	chemical hazard response information system
CHRP	contaminated human remains pouch
CHSTR	characteristics of transportation resources
CHSTREP	characteristics of transportation resources report
CI	civilian internee; counterintelligence
CIA	Central Intelligence Agency
CIAP	Central Intelligence Agency program; central intelligence architecture plan; command intelligence architecture plan; command intelligence architecture program
CIAS	counterintelligence analysis section
CIAT	counterintelligence analytic team
CIB	combined information bureau; controlled image base
CIC	combat information center; combat intelligence center (Marine Corps); combined intelligence center; communications interface controller; content indicator code; counterintelligence center
CICA	counterintelligence coordinating authority
CICAD	Inter-American Drug Abuse Control Commission
CICC	counterintelligence coordination cell
CICR	counterintelligence collection requirement
CID	combat identification; combat intelligence division; criminal investigation division
CIDB	common intelligence database
CIDC	Criminal Investigation Division Command
CIDNE	Combined Information Data Network Exchange
CIE	collaborative information environment; cultural intelligence element
CIEA	classification, identification, and engagement area
C-IED	counter-improvised explosive device
CIEG/CIEL	common information exchange glossary and language
CIFA	counterintelligence field activity
CIG	communications interface group
CIHO	counterintelligence/human intelligence officer
CIIR	counterintelligence information report
CI/KR	critical infrastructure and key resources
CIL	command information library; critical information list; critical item list
CILO	counterintelligence liaison officer
CIM	civil information management; compartmented information management
CIMIC	civil-military cooperation
CIN	cargo increment number
CIO	chief information officer; command intelligence officer
CIOC	counterintelligence operations cell
CIOTA	counterintelligence operational tasking authority
CIP	communications interface processor; critical infrastructure

	protection
CIPSU	communications interface processor pseudo line
CIR	continuing intelligence requirement
CIRM	International Radio-Medical Center
CIRV	common interswitch rekeying variable
CIRVIS	communications instructions for reporting vital intelligence sightings
CIS	common item support; Commonwealth of Independent States; communications interface shelter
CISAR	catastrophic incident search and rescue
CISD	critical incident stress debriefing
CISO	counterintelligence staff office; counterintelligence support officer
CITE	computer intrusion technical exploitation
CITP	counter-improvised explosive device targeting program
CIV	civilian
CIVMAR	civil service mariner
CIVPOL	civilian police
CIWG	communications interoperability working group
CJ-4	combined-joint logistics officer
CJATF	commander, joint amphibious task force
CJB	Congressional Justification Book
CJCS	Chairman of the Joint Chiefs of Staff
CJCSAN	Chairman of the Joint Chiefs of Staff Alerting Network
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CJDA	critical joint duty assignment
CJE	component joint data networks operations officer equivalent
CJLOTS	combined joint logistics over-the-shore
CJMAB	Central Joint Mortuary Affairs Board
CJMAO	Central Joint Mortuary Affairs Office; Chief, joint mortuary affairs office
CJMISTF	combined joint military information support task force
CJMTF	combined joint military information support operations task force
CJOC	Canada Joint Operations Command
CJSART	Criminal Justice Sector Assessment Rating Tool
CJSMPT	Coalition Joint Spectrum Management Planning Tool
CJTF	combined joint task force (NATO); commander, joint task force
CJTF-CS	Commander, Joint Task Force - Civil Support
CJTF-NCR	Commander, Joint Task Force - National Capital Region
C-JWICS	Containerized Joint Worldwide Intelligence Communications System
CKT	circuit

CL	class; coordination level
CLA	landing craft, air cushion launch area
CLASSRON	class squadron
CLB	combat logistics battalion
CLD	compact laser designator
CLDP	Commercial Law Development Program
CLEA	civilian law enforcement agency
C-level	category level
CLF	combat logistics force; commander, landing force
CLG	combat logistics group
CLGP	cannon-launched guided projectile
CLIA	Clinical Laboratory Improvement Amendments
CLIPS	communications link interface planning system
CLPSB	combatant commander logistic procurement support board
CLPT	contingency load planning team
CLR	combat logistics regiment
CLS	contractor logistic support
CLSS	combat logistic support squadron
CLT	civil liaison team; combat lasing team
CLZ	craft landing zone; cushion landing zone; landing craft, air cushion landing zone
CM	Chairman's memorandum; collection manager; combination module; configuration management; control modem; countermine; cruise missile
Cm	mean coverage factor
cm	centimeter
CMA	collection management authority
CMAA	cooperative military airlift agreement
CMAH	commander of a combatant command's Mobile Alternate Headquarters
CM&D	collection management & dissemination
CMAOC	Casualty and Mortuary Affairs Operations Center
CMAT	consequence management advisory team
CMC	Commandant of the Marine Corps; crew management cell; Office of Civilian-Military Cooperation (USAID)
Cmc	midpoint compromise coverage factor
CMCB	civil-military coordination board
CMCC	combined movement coordination center
CMD	command; cruise missile defense
CMDO	command military deception officer
CME	civil-military engagement
CMHT	consequence management home team
CMM	Office of Conflict Management and Mitigation (USAID)
CMMA	collection management mission application

CMO	Central Measurement and Signature Intelligence (MASINT) Organization; chief medical officer; chief military observer; civil-military operations; collection management office(r); configuration management office
CMOC	Cheyenne Mountain Operations Center; civil-military operations center
CMOS	cargo movement operations system; Cargo Movement Operations System (USAF); complementary metal-oxide semiconductor
CMP	communications message processor; contractor management plan
CMPF	commander, maritime pre-positioned force
CMPT	consequence management planning team
CM R&A	consequence management response and assessment
CMRT	consequence management response team
CMS	cockpit management system; command management system; community management staff; community security materiel system; contingency mutual support; crisis management system
CMSE	civil-military support element
CMST	consequence management support team
CMTS	comments
CMTU	cartridge magnetic tape unit
CMV	commercial motor vehicle
CMX	crisis management exercise
CNAC	Customs National Aviation Center (USCS)
C-NAF	component numbered air force
CNASP	chairman's net assessment for strategic planning
CNBG	commander, naval beach group
CNC	Crime and Narcotics Center (CIA)
CNCE	communications nodal control element
CNCI	Comprehensive National Cybersecurity Initiative
CND	counternarcotics division
CNE	computer network exploitation; Counter Narcotics Enforcement
CNGB	Chief, National Guard Bureau
CNIC	Commander, Navy Installations Command
CNM	classified notice to mariners
CNMOC	Commander, Naval Meteorology and Oceanography Command
CNO	Chief of Naval Operations
CNOG	Chairman, Nuclear Operations Group
CNR	combat net radio
CNRF	Commander, Naval Reserve Forces
CNSG	Commander, Naval Security Group
CNTY	country

CNWDI	critical nuclear weapons design information
CO	commanding officer; cyberspace operations
COA	course of action
COAA	course-of-action analysis
COAMPS	Coupled Ocean Atmosphere Mesoscale Prediction System
COB	collocated operating base; contingency operating base
COBOL	common business-oriented language
COC	combat operations center
CoC	Code of Conduct
COCO	contractor-owned, contractor-operated
COCOM	combatant command (command authority)
COD	carrier onboard delivery; combat operations division
COE	Army Corps of Engineers; common operating environment; concept of employment
COEDMHA	Center for Excellence in Disaster Management and Humanitarian Assistance (USPACOM)
COF	chief of fires; conduct of fire
COFC	container on flatcar
COG	center of gravity; continuity of government
COGARD	Coast Guard
COI	community of interest; contact of interest
COIC	counter-improvised explosive device operations integration center; Counter-Improvised Explosive Device Operations/Intelligence Integration Center (JIEDDO)
COIN	counterinsurgency
COLDS	cargo offload and discharge system
COLISEUM	community on-line intelligence system for end-users and managers
COLPRO	collective protection
COLS	concept of logistic support
COLT	combat observation and lasing team
COM	chief of mission; collection operations management; command; commander
COMACC	Commander, Air Combat Command
COMAFFOR	commander, Air Force forces
COMAFSOAC	commander, Air Force special operations air component
COMAFSOC	Commander, Air Force Special Operations Command
COMAJF	commander, allied joint force
COMALF	commander airlift forces
COMALOC	commercial air line of communications
COMARFOR	commander, Army forces
COMCAM	combat camera
COMCARGRU	commander, carrier group
COMCRUDESGRU	commander, cruiser destroyer group
COMDCAEUR	Commander, Defense Communications Agency Europe

COMDESRON	commander destroyer squadron
COMDT COGARD	Commandant, United States Coast Guard
COMDTINST	Commandant of the Coast Guard instruction
COMFLTCYBERCOM	Commander, Fleet Cyber Command
COMICEDEFOR	Commander, United States Forces, Iceland
COMIDEASTFOR	Commander, Middle East Forces
COMINEWARCOM	Commander, Mine Warfare Command
COMINT	communications intelligence
COMJCSE	Commander, Joint Communications Support Element
COMJIC	Commander, Joint Intelligence Center
COMLANDFOR	commander, land forces
COMLANTAREACOGARD	Commander, Coast Guard Atlantic Area
COMLOGGRU	combat logistics group
COMM	communications
COMMARFOR	commander, Marine Corps forces
COMMARFORNORTH	Commander, Marine Corps Forces North
COMMDZ	Commander, Maritime Defense Zone
COMNAV	Committee for European Airspace Coordination Working Group on Communications and Navigation Aids
COMNAVAIRLANT	Commander, Naval Air Force, Atlantic
COMNAVAIRPAC	Commander, Naval Air Force, Pacific
COMNAVAIRSYSCOM	Commander, Naval Air Systems Command
COMNAVCOMTELCOM	Commander, Naval Computer and Telecommunications Command
COMNAVELSG	Commander, Navy Expeditionary Logistics Support Group
COMNAVFOR	commander, Navy forces
COMNAVMETOCCOM	Commander, Naval Meteorology and Oceanography Command
COMNAVSEASYSCOM	Commander, Naval Sea Systems Command
COMNAVSECGRP	Commander, United States Navy Security Group
COMNAVSURFLANT	Commander, Naval Surface Force, Atlantic
COMNAVSURFPAC	Commander, Naval Surface Force, Pacific
COMNET	communications network
COMP	component
COMPACAF	Commander, Pacific Air Forces
COMPACAREACOGARD	Commander, Coast Guard Pacific Area
COMPACFLT	Commander, Pacific Fleet
COMPASS	common operational modeling, planning, and simulation strategy; Computerized Movement Planning and Status System
COMPES	contingency operations mobility planning and execution system
COMPLAN	communications plan
COMSC	Commander, Military Sealift Command
COMSCINST	Commander, Military Sealift Command instruction
COMSEC	communications security

COMSOC	Commander, Special Operations Command
COMSOCCENT	Commander, Special Operations Command, United States Central Command
COMSOCEUR	Commander, Special Operations Command, United States European Command
COMSOCPAC	Commander, Special Operations Command, Pacific
COMSOCSOUTH	Commander Special Operations Command, United States Southern Command
COMSOF	commander, special operations forces
COMSTAT	communications status
COMSUBLANT	Commander Submarine Force, United States Atlantic Fleet
COMSUBPAC	Commander Submarine Force, United States Pacific Fleet
COMSUPNAVFOR	commander, supporting naval forces
COMTAC	tactical communications
COMTENTHFLT	Commander, Tenth Fleet
COMUSAFE	Commander, United States Air Force in Europe
COMUSARCENT	Commander, United States Army Forces, Central Command
COMUSFLTFORCOM	Commander, United States Fleet Forces Command
COMUSFORAZ	Commander, United States Forces, Azores
COMUSJ	Commander, United States Forces, Japan
COMUSK	Commander, United States Forces, Korea
COMUSMARCENT	Commander, United States Marine Forces, Central Command
COMUSNAVCENT	Commander, United States Navy, Central Command
COMUSPACFLT	Commander, United States Pacific Fleet
COMUSSOCJFCOM	Commander Special Operations Command, United States Joint Forces Command
CONCAP	construction capabilities contract (Navy); Construction Capabilities Contract Process; construction capabilities contract program
CONEX	container express
CONEXPLAN	contingency and exercise plan
CONOPS	concept of operations
CONPLAN	concept plan; operation plan in concept format
CONR	continental United States North American Aerospace Defense Command Region
CONUS	continental United States
CONUSA	Continental United States Army
COOP	continuity of operations
COP	common operational picture
COP-CSE	common operational picture-combat support enabled
COPG	chairman, operations planners group
COPPERHEAD	name for cannon-launched guided projectile
COPS	communications operational planning system
COR	contracting officer representative

CORE	contingency response program
COS	chief of staff; chief of station; critical occupational specialty
COSMIC	North Atlantic Treaty Organization (NATO) security category
COSPAS	*cosmicheskaya sistyema poiska avariynch sudov* - space system for search of distressed vessels (Russian satellite system)
COSR	combat and operational stress reactions
COT	commanding officer of troops; crisis operations team
COTP	captain of the port
COTS	cargo offload and transfer system; commercial off-the-shelf; container offloading and transfer system
COU	cable orderwire unit
counter C3	counter command, control, and communications
COVCOM	covert communications
CP	check point; collection point; command post; contact point; control point; counterproliferation
CP&I	coastal patrol and interdiction
CPA	closest point of approach
CPD	combat plans division
CPE	customer premise equipment
CPFL	contingency planning facilities list
CPG	central processor group; Commander, Amphibious Group; Contingency Planning Guidance
CPI	crash position indicator
CPIC	coalition press information center
CPM	civilian personnel manual
CPO	chief petty officer; complete provisions only
CPR	cardiopulmonary resuscitation
CPRC	coalition personnel recovery center
CPS	characters per second; collective protective shelter
CPT	common procedural terminology
CPU	central processing unit
CPX	command post exercise
CR	civil reconnaissance; critical requirement
CRA	command relationships agreement; continuing resolution authority; coordinating review authority
CRAF	Civil Reserve Air Fleet
CRAM	control random access memory
CRB	configuration review board
CRC	circuit routing chart; Civilian Response Corps (DOS); civil response corps; coastal riverine company; control and reporting center; CONUS replacement center; COOP response cell; crisis reaction center; cyclic redundancy rate
CRD	chemical reconnaissance detachment

CRE	contingency response element; control reporting element
CREAPER	Communications and Radar Electronic Attack Planning Effectiveness Reference
CREST	casualty and resource estimation support tool
CREW	counter radio-controlled improvised explosive device electronic warfare
CRF	channel reassignment function; coastal riverine force; contingency response force
CRG	contingency response group
CRI	collective routing indicator
CRIF	cargo routing information file
CRITIC	critical information; critical intelligence communication; critical message (intelligence)
CRITICOMM	critical intelligence communications system
CRM	collection requirements management; comment resolution matrix; crew resource management
CrM	crisis management
CRO	combat rescue officer
CROP	common relevant operational picture
CRP	control and reporting post
CRRC	combat rubber raiding craft
CRS	Catholic Relief Services; Chairman's readiness system; coastal radio station; coastal riverine squadron; community relations service; container recovery system; Coordinator for Reconstruction and Stabilization
CRSG	country reconstruction and stabilization group
CRSP	centralized receiving and shipping point
CRT	cathode ray tube; chemical, biological, radiological, nuclear, and high-yield explosives response team; contingency response team
CRTS	casualty receiving and treatment ship
CR-UAV	close-range unmanned aerial vehicle
CRW	contingency response wing
CRYPTO	cryptographic
CS	call sign; Chaplain Service (Air Force); circuit switch; coastal station; combat service; combat support; content staging; controlled space; creeping line single-unit; critical source
CSA	Chief of Staff, United States Army; combat support agency; container stuffing activity
CSAAS	combat support agency assessment system
CSADR	combat support agency director's report
CSAF	Chief of Staff, United States Air Force
CSAM	computer security for acquisition managers
CSAR	combat search and rescue

CSAR3	combat support agency responsiveness and readiness report
CSARTE	combat search and rescue task element
CSB	contracting support brigade
CSB (MEB)	combat support brigade (maneuver enhancement brigade)
CSC	combat support center; community support center; convoy support center; creeping line single-unit coordinated; International Convention for Safe Containers
CSCC	coastal sea control commander
CSE	client server environment; combat support enhanced; combat support equipment; contingency support element; cyberspace support element
CSEL	circuit switch select line; combat survivor evader locator; command senior enlisted leader
CSEP	Chairman of the Joint Chiefs of Staff-sponsored exercise program
CSG	carrier strike group; Chairman's Staff Group; coordinating subgroup; cryptologic services group; Cryptologic Support Group
CSGN	coordinating subgroup for narcotics
CSH	combat support hospital
CSIF	communications service industrial fund
CSIP	contract support integration plan
CSIPG	circuit switch interface planning guide
CSL	combat stores list; cooperative security location
C-SMPP	Consolidated Satellite Communications Management Policies and Procedures
CSNP	causeway section, nonpowered
CSNP(BE)	causeway section, nonpowered (beach end)
CSNP(I)	causeway section, nonpowered (intermediate)
CSNP(SE)	causeway section, nonpowered (sea end)
CSO	Bureau of Conflict and Stabilization Operations (DOS); Center for Special Operations (USSOCOM); communications support organization; controlled source operation
CSOA	combined special operations area
CSOB	command systems operations branch
CSOD	command systems operation division
CSOR	contract statement of requirement
CSP	call service position; career sea pay; causeway section, powered; commence search point; contracting support plan; crisis staffing procedures (JCS); cryptologic support package
CSPAR	combatant commander's preparedness assessment report

CSR	central source registry; combatant commander's summary report; commander's summary report; controlled supply rate
CSRF	common source route file
CSS	Central Security Service (NSA); combat service support; communications subsystem; coordinator surface search
CSSA	combat service support area
CSSAMO	combat service support automation management office
CSSB	combat sustainment support battalion
CSSC	coded switch set controller
C-SSE	consolidated satellite communications system expert
CSSM	contracted support synchronization matrix
CSST	combat service support team
CSSU	combat service support unit
CST	contingency support team; customer service team
CSW	compartment stowage worksheet; coordinate seeking weapons
CT	computed tomography; control telemetry; counterterrorism; country team
CTA	common table of allowance
CTAF	counterterrorism analytical framework
CTAPS	contingency Theater Air Control System automated planning system
CTBT	Comprehensive Nuclear Test-Ban Treaty
CTC	cargo transfer company (USA); counterterrorist center
CTDB	combating terrorism database
CTEP	combined training and education plan
CTF	combined task force; commander, task force; counter threat finance
CTF IAMD	commander, task force integrated air and missile defense
CTFP	Combating Terrorism Fellowship Program
CTG	commander, task group
CTID	communications transmission identifier
CTIP	combating trafficking in persons
CTKB	combating terrorism knowledge base
CTL	candidate target list
CTM	core target material
CTOC	corps tactical operations center
CTP	common tactical picture
CTR	cooperative threat reduction
CTRIF	Combating Terrorism Readiness Initiative Fund
CTS	commodity tracking system; Contingency Tracking System; controlled technical services
CTSS	central targeting support staff
CTU	commander, task unit
CU	cubic capacity; common unit

CUI	controlled unclassified information
CUL	common-user logistics
CULT	common-user land transportation
CV	aircraft carrier; carrier; critical vulnerability; curriculum vitae
CVAMP	Core Vulnerability Assessment Management Program
CVN	aircraft carrier, nuclear
CVR	cockpit voice recorder
CVS	commercial vendor services
CVSD	continuous variable slope delta
CVT	criticality-vulnerability-threat
CVW	carrier air wing; cryptovariable weekly (GPS)
CVWC	carrier strike group air wing commander
CW	carrier wave; chemical warfare; continuous wave
CWA	chemical warfare agent
CWC	Chemical Weapons Convention; composite warfare commander
CWDE	chemical warfare defense equipment
CWMD	countering weapons of mass destruction
CWO	communications watch officer
CWP	causeway pier
CWPD	Conventional War Plans Division, Joint Staff (J-7)
CWR	calm water ramp
CWT	combat weather team; customer wait time
CY	calendar year

D

D	total drift, data
d	surface drift
D&D	denial and deception
D&F	determinations and findings
D&M	detection and monitoring
D&R	debrief and reintegrate
D-2X	Department of Defense-level counterintelligence and human intelligence staff element
D3A	decide, detect, deliver, and assess
D/A	digital-to-analog
DA	data adapter aerospace drift; data administrator; Department of the Army; Development Assistance; direct action; Directorate for Mission Services (DIA); double agent
Da	aerospace drift
DA&M	Director of Administration and Management
DAA	designated approving authority; display alternate area routing lists
DAADC	deputy area air defense commander
DAADC(AMD)	deputy area air defense commander for air and missile defense
DAAS	defense automatic addressing system
DAASO	defense automatic addressing system office
DAB	Defense Acquisition Board
DAC	Defense Intelligence Agency (DIA) counterintelligence and security activity; Department of Army civilians; Development Assistance Committee (OECD)
DACAS	digitally aided close air support
DACB	data adapter control block
DACG	departure airfield control group
DACM	data adapter control mode
DADCAP	dawn and dusk combat air patrol
DAF	Department of the Air Force
DAFL	directive authority for logistics
DAICC	domestic air interdiction coordinator center
DAL	defended asset list
DALIS	Disaster Assistance Logistics Information System
DALS	downed aviator locator system
DAMA	demand assigned multiple access
DAMES	defense automatic addressing system (DAAS) automated message exchange system
DAN	Diver's Alert Network
DAO	defense attaché office; defense attaché officer; department/ agency/organization
DAP	designated acquisition program

DAR	Defense Acquisition Regulation; distortion adaptive receiver
DARO	Defense Airborne Reconnaissance Office
DARPA	Defense Advanced Research Projects Agency
DART	disaster assistance response team; downed aircraft recovery team; dynamic analysis and replanning tool
DAS	deep air support (USMC); defense attaché system; direct access subscriber; direct air support
DAS3	decentralized automated service support system
DASA	Department of the Army (DA) staff agencies
DASC	direct air support center
DASC(A)	direct air support center (airborne)
DASD	Deputy Assistant Secretary of Defense
DASD-CN	Deputy Assistant Secretary of Defense for Counternarcotics
DASD(H&RA)	Deputy Assistant Secretary of Defense (Humanitarian & Refugee Affairs)
DASD(I)	Deputy Assistant Secretary of Defense (Intelligence)
DASD(PK/HA)	Deputy Assistant Secretary of Defense (Peacekeeping and Humanitarian Affairs)
DASD(PS)	Deputy Assistant Secretary of Defense (Program Support)
DASD(S&IO)	Deputy Assistant Secretary of Defense (Security and Information Operations)
DASSS	decentralized automated service support system
DAT	deployment action team
DATT	defense attaché
DATU	data adapter termination unit
DAWIA	Defense Acquisition Workforce Improvement Act
dB	decibel
DBA	database administrator
DBDB	digital bathymetric database
DBDB-V	digital bathymetric database variable
DBG	database generation
DBI	defense budget issue
DBIDS	Defense Biometric Identification System
DBMS	database management system; Defense-Business Management System
DBSMC	Defense Business Systems Management Committee
DBSS	Defense Blood Standard System
DBT	design basis threat
DC3	Department of Defense Cyber Crime Center
D/C	downconverter
DC	Deputies Committee; direct current; Directorate of Counterintelligence (DIA); dislocated civilian
DCA	Defense Communications Agency; Defense Cooperation Agreements; defensive counterair; dual-capable aircraft

DCAA	Defense Contract Audit Agency
DCAM	Defense Medical Logistics Standard Support (DMLSS) customer assistance module
DCAPES	Deliberate and Crisis Action Planning and Execution Segments
DCC	damage control center; deployment control center
DCCC	defense collection coordination center
DCCEP	developing country combined exercise program
DCD	data collection device
DCE	defense coordinating element
D-cell	deployment cell
DCGS	distributed common ground/surface system
DCHA	Bureau for Democracy, Conflict, and Humanitarian Assistance (USAID)
DCHC	Defense Counterintelligence and Human Intelligence Center
DCHE	Defense Counterintelligence and Human Intelligence Enterprise
DCI	defense critical infrastructure; Director of Central Intelligence; dual channel interchange
D/CI&SP	Director, Counterintelligence and Security Programs
D/CIA	Director, Central Intelligence Agency
DCID	Director of Central Intelligence directive
DCIIS	Defense Counterintelligence Information System
DCIO	defense criminal investigative organization
DCIP	Defense Critical Infrastructure Program
DCIS	Defense Criminal Investigative Services
DCISE	Defense Industrial Base Collaborative Information Sharing Environment
DCJTF	deputy commander, joint task force
DCM	data channel multiplexer; deputy chief of mission
DCMA	Defense Contract Management Agency
DCMC	Office of Deputy Chairman, Military Committee
DCMO	deputy chief military observer
DCNO	Deputy Chief of Naval Operations
DCO	debarkation control officer; Defense Connect Online; defense coordinating officer; defensive cyberspace operations; dial central office
DCO-IDM	defensive cyberspace operations - internal defensive measures
DCO-RA	defensive cyberspace operations response actions
DCP	Defense Continuity Program; detainee collection point
DCPA	Defense Civil Preparedness Agency
DCPG	digital clock pulse generator
DCR	doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy change recommendation

DCRF defense chemical, biological, radiological, and nuclear response force
DCS Defense Courier Service; deputy chief of staff; digital computer system
DCSCU dual capability servo control unit
DC/S for RA Deputy Chief of Staff for Reserve Affairs
DCSINT Deputy Chief of Staff for Intelligence
DCSLOG Deputy Chief of Staff for Logistics, US Army
DCSOPS Deputy Chief of Staff for Operations and Plans, United States Army
DCSPER Deputy Chief of Staff for Personnel, United States Army
DCST Defense Logistics Agency (DLA) contingency support team
DCTC Defense Combating Terrorism Center
DCTS Defense Collaboration Tool Suite
DCW Defense Collection Watch (DIA)
DD Department of Defense (form); deputy director; destroyer (Navy ship)
DDA deputy development advisor; Deputy Director for Administration (CIA); designated development activity
DDC data distribution center; defense distribution center
DDCI Deputy Director of Central Intelligence (CIA)
DDCI/CM Deputy Director of Central Intelligence for Community Management
DDED defense distribution expeditionary depot
DDG guided missile destroyer
DDI Deputy Director of Intelligence (CIA); Director of Defense Intelligence
DDL digital data link
DDM Defense Logistics Agency Distribution Mapping; digital data modem
DDMA Defense Distribution Mapping Activity
DDMS Deputy Director for Military Support (NRO)
DDO Deputy Director of Operations (CIA)
DDOC Deployment and Distribution Operations Center (USTRANSCOM)
DDP detailed deployment plan
DDR disarmament, demobilization, and reintegration
DDR&E director of defense research and engineering
DDRRR disarmament, demobilization, repatriation, reintegration, and resettlement
DDS defense dissemination system; Deployable Disbursing System
DDS&T Deputy Director for Science & Technology (CIA) **DDSBn** deployment and distribution support battalion
DDSM Defense Distinguished Service Medal

DDST	deployment and distribution support team
DDWSO	Deputy Director for Wargaming, Simulation, and Operations
DE	damage expectancy; decedent effects; delay equalizer; directed energy
De	total drift error
de	individual drift error
DEA	Drug Enforcement Administration (DOJ)
dea	aerospace drift error
DEACN	Drug Enforcement Administration Communications Network
DEAR	disease and environmental alert report
DEARAS	Department of Defense Emergency Authorities Retrieval and Analysis System
DeCA	Defense Commissary Agency
DEERS	Defense Enrollment Eligibility Reporting System
DEFSMAC	Defense Special Missile and Aerospace Center
DEL	deployable equipment list
DEMARC	demarcation
de max	maximum drift error
DEMIL	demilitarization
de min	minimum drift error
de minimax	minimax drift error
DeMS	deployment management system
DEMUX	demultiplex
DEP	Delayed Entry Program; deployed
DEP&S	Drug Enforcement Plans and Support
DEPCJTF	deputy commander, joint task force
DEPID	deployment indicator code
DEPMEDS	deployable medical systems
DepOpsDeps	Service deputy operations deputies
DEPORD	deployment order
DESC	Defense Energy Support Center
DESCOM	Depot System Command (Army)
DESIGAREA	designated area message
DEST	destination; domestic emergency support team
DET	detainee
DETRESFA	distress phase (ICAO)
DEW	directed-energy warfare
DF	direction finding; dispersion factor; disposition form
DFARS	Defense Federal Acquisition Regulation Supplement
DFAS	Defense Finance and Accounting Service
DFAS-DE	Defense Finance and Accounting Service-Denver
DFC	deputy force commander; detention facility commander

DFE	Defense Intelligence Agency forward element; Defense Joint Intelligence Operations Center forward element; division force equivalent
DFM	deterrent force module
DFO	disaster field office (FEMA)
DFR	Defense Fuel Region
DFR/E	Defense Fuel Region, Europe
DFRIF	Defense Freight Railway Interchange Fleet
DFR/ME	Defense Fuel Region, Middle East
DFSC	Defense Fuel Supply Center
DFSP	defense fuel support point
DFT	deployment for training
DG	defense guidance
DGIAP	Defense General Intelligence and Applications Program
DGM	digital group multiplex
DGT	designated ground target
DH	death due to hostilities; Directorate for Human Intelligence (DIA)
DHA	detainee holding area
DHB	Defense Health Board
DHE	defense human intelligence executor
DHE-M	Defense Human Intelligence Enterprise-manual
DHHS	Department of Health and Human Services
DHM	Department of Defense human intelligence manager
DHMO	Department of Defense human intelligence management office
DHP	Defense Health Program
DHS	Defense Human Intelligence (HUMINT) Service; Department of Homeland Security; Director of Health Services
DI	Defense Intelligence Agency (DIA) Directorate for Analysis; DIA Directorate for Intelligence Production; discrete identifier; dynamic interface
DI&E	data integration and exploitation
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIA/DHX	Defense Intelligence Agency, Directorate of Human Intelligence, Office of Document and Media Operations
DIAM	Defense Intelligence Agency manual; Defense Intelligence Agency memorandum
DIAP	Defense Intelligence Analysis Program; Drug Interdiction Assistance Program
DIAR	Defense Intelligence Agency (DIA) regulation
DIB	defense industrial base
DIBITS	digital in-band interswitch trunk signaling
DIBRS	defense incident-based reporting system

DIBTS	digital in-band trunk signaling
DICO	Data Information Coordination Office
DID	Defense Intelligence Digest
DIDHS	Deployable Intelligence Data Handling System
DIDO	designated intelligence disclosure official
DIDS	Defense Intelligence Dissemination System
DIEB	Defense Intelligence Executive Board
DIEPS	Digital Imagery Exploitation Production System
DIG	digital
DIGO	Defence Imagery and Geospatial Organisation (Australia)
DII-COE	defense information infrastructure-common operating environment
DIILS	Defense Institute of International Legal Studies
DIJE	Defense Intelligence Joint Environment (United Kingdom)
DILPA	diphase loop modem-A
DIMA	drilling individual mobilization augmentee
DIMOC	Defense Imagery Management Operations Center
DIN	defense intelligence notice
DINET	Defense Industrial Net
DINFOS	Defense Information School
DIOC	drug interdiction operations center
DIOCC	Defense Intelligence Operations Coordination Center
DIPC	defense industrial plant equipment center
DIPF	defense intelligence priorities framework
DIPFAC	diplomatic facility
DIPGM	diphase supergroup modem
DIRINT	Director of Intelligence (USMC)
DIRJIATF	director, joint inter-agency task force
DIRLAUTH	direct liaison authorized
DIRM	Directorate for Information and Resource Management
DIRMOBFOR	director of mobility forces
DIRNSA	Director, National Security Agency
DIRSPACEFOR	director of space forces (USAF)
DIS	defense information system; Defense Investigative Service; distributed interactive simulation
DISA	Defense Information Systems Agency
DISA-LO	Defense Information Systems Agency - liaison officer
DISANMOC	Defense Information Systems Agency Network Management and Operations Center
DisasterAWARE	Disaster All-Hazard Warnings, Analysis, and Risk Evaluation System
DISCOM	division support command (Army)
DISGM	diphase supergroup
DISN	Defense Information Systems Network
DISN-E	Defense Information Systems Network – Europe

DISO	deception in support of operations security; defense intelligence support office
DISP	drug investigation support program (FAA)
DITDS	defense information threat data system; defense intelligence threat data system
DITSUM	defense intelligence terrorist summary
DJ-7	Director, Joint Staff Directorate for Joint Force Development
DJIOC	Defense Joint Intelligence Operations Center
DJS	Director, Joint Staff
DJSM	Director, Joint Staff memorandum
DJTFS	deputy joint task force surgeon
DLA	Defense Logistics Agency
DLAM	Defense Logistics Agency manual
DLAR	Defense Logistics Agency regulation
DLEA	drug law enforcement agency
DLED	dedicated loop encryption device
DLD	digital liaison detachment
DLIS	Defense Logistics Information Service
DLM	defense logistics manual
DLMS	Department Logistics Management System
DLP	data link processor
DLPMA	diphase loop modem A
DLQ	deck landing qualification
DLR	depot-level repairable
DLSA	Defense Legal Services Agency
DLSS	Defense Logistics Standard Systems
DLTM	digital line termination module
DLTU	digital line termination unit
DM	detection and monitoring; docking module
DMA	Defense Media Activity
dmax	maximum drift distance
DMB	datum marker buoy
DMC	data mode control
DMD	digital message device
DMDC	defense management data center; Defense Manpower Data Center
DME	distance measuring equipment
DMHS	Defense Message Handling System
DMI	director military intelligence
DMIGS	Domestic Mobile Integrated Geospatial-Intelligence System
dmin	minimum drift distance
DML	data manipulation language
DMLSS	Defense Medical Logistics Standard Support
DMMPO	Defense Medical Materiel Program Office
DMO	directory maintenance official

DMORT	Disaster Mortuary Operational Response Team
DMOS	duty military occupational specialty
DMPI	designated mean point of impact
DMRD	defense management resource decision
DMRIS	defense medical regulating information system
DMS	defense meteorological system; director of military support
DMSB	Defense Medical Standardization Board
DMSM	Defense Meritorious Service Medal
DMSO	Defense Modeling and Simulation Office; director of major staff office; Division Medical Supply Office
DMSP	Defense Meteorological Satellite Program
DMSSC	defense medical systems support center
DMT	disaster management team (UN)
DMU	disk memory unit
DMZ	demilitarized zone
DN	digital nonsecure
DNA	Defense Nuclear Agency; deoxyribonucleic acid
DNAT	defense nuclear advisory team
DNBI	disease and nonbattle injury
DNC	digital nautical chart
DND	Department of National Defence (Canada)
DNDO	Domestic Nuclear Detection Office (DHS)
DNGA	Director of National Geospatial-Intelligence Agency
DNI	Director of National Intelligence; Director of Naval Intelligence
DNIF	duty not involving flying
DNMSP	driftnet monitoring support program
DNSO	Defense Network Systems Organization
DNVT	digital nonsecure voice terminal
DNY	display area code (NYX) routing
DOA	days of ammunition; dead on arrival; director of administration
DOB	date of birth; dispersal operating base
DOC	Department of Commerce; designed operational capability
DOCC	deep operations coordination cell
DOCDIV	documents division
DOCEX	document exploitation
DOCNET	Doctrine Networked Education and Training
DOD	Department of Defense
DODAAC	Department of Defense activity address code
DODAAD	Department of Defense Activity Address Directory
DODAC DOD	ammunition code
DODD	Department of Defense directive
DODDS	Department of Defense Dependent Schools

DODEX	Department of Defense intelligence system information system extension
DODFMR	Department of Defense Financial Management Regulation
DODI	Department of Defense instruction
DODIC	Department of Defense identification code
DODID	Department of Defense Intelligence Digest
DODIIS	Department of Defense Intelligence Information System
DODIN	Department of Defense information network
DODIPC	Department of Defense intelligence production community
DODIPP	Department of Defense Intelligence Production Program
DOD-JIC	Department of Defense Joint Intelligence Center
DODM	data orderwire diphase modem; Department of Defense manual
DODS-CWMD	Department of Defense Strategy for Countering Weapons of Mass Destruction
DOE	Department of Energy
DOEHRS	Defense Occupational and Environmental Health Reporting System
DOF	degree of freedom
DOI	Defense Special Security Communications System (DSSCS) Operating Instructions; Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOM	day of month
DOMEX	document and media exploitation
DOMS	director of military support
DON	Department of the Navy
DOPMA	Defense Officer Personnel Management Act
DOR	date of rank
DOS	date of separation; days of supply; denial of service; Department of State; disk operating system
DOT	Department of Transportation
DOTEO	Department of Transportation emergency organization
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
DOW	data orderwire; died of wounds
DOX-T	direct operational exchange-tactical
DOY	day of year
DP	Air Force component plans officer (staff); decisive point; Directorate for Policy Support (DIA); displaced person
dp	parachute drift
DPA	danger pay allowance; Defense Production Act
DPAA	Defense Prisoner of War/Missing in Action Accounting

	Agency
DPAP	Defense Procurement and Acquisition Policy
DPAS	Defense Priorities and Allocation System
DPC	deception planning cell; Defense Planning Committee (NATO)
DPEC	displaced person exploitation cell
DPG	Defense Planning Guidance
DPI	desired point of impact
dpi	dots per inch
DPICM	dual purpose improved conventional munitions
DPIP	departing initial point
DPKO	Department of Peacekeeping Operations (UN)
DPLSM	dipulse group modem
DPM	dissemination program manager
DPMO	Defense Prisoner of War/Missing Personnel Office
DPO	Defense Press Office; distribution process owner
DPP	data patch panel; distributed production program
DPPDB	digital point positioning database
DPQ	defense planning questionnaire (NATO)
DPR	display non-nodal routing
DPRB	Defense Planning and Resources Board
DPRE	displaced persons, refugees, and evacuees
DPS	data processing system
DPSC	Defense Personnel Support Center
DPSK	differential phase shift keying
DR	dead reckoning; digital receiver; disaster relief
DRB	Defense Resources Board
DRe	dead reckoning error
DRL	Bureau of Democracy, Human Rights, and Labor (DOS)
DRMD	deployments requirements manning document
DRMO	Defense Reutilization and Marketing Office
DRMS	Defense Reutilization and Marketing Service; distance root-mean-square
DRN	Disaster Response Network
DRO	departmental requirements office; departmental requirements officer
DRRS	Defense Readiness Reporting System
DRS	detainee reporting system
DRSN	Defense Red Switched Network
DRT	dead reckoning tracer; decontamination and reconnaissance team
DRTC	designated reporting technical control
DS	Directorate for Management and Chief Information Officer (DIA); direct support; doctrine sponsor
DSA	defense special assessment (DIA)
DSAA	Defense Security Assistance Agency

DSAID defense sexual assault incident database
DSAR Defense Supply Agency regulation
DSB digital in-band trunk signaling (DIBTS) signaling buffer
DSC defensive space control; digital selective calling; dual-status commander
DSCA Defense Security Cooperation Agency; defense support of civil authorities
DSCP Defense Supply Center Philadelphia
DSCR Defense Supply Center Richmond
DSCS Defense Satellite Communications System
DSCSOC Defense Satellite Communications System operations center
DSDI digital simple data interface
DSE direct support element
DSF District Stability Framework (USAID)
DSG digital signal generator
DSI defense simulation internet
DSL display switch locator (SL) routing
DSM decision support matrix
DSMAC digital scene-matching area correlation
DSN Defense Switched Network
DSNET Defense Secure Network
DSNET-2 Defense Secure Network-2
DSO Defense Spectrum Organization; defensive systems officer
DSOE deployment schedule of events
DSP Defense Satellite Program; Defense Support Program
DSPD defense support to public diplomacy
DSPL display system programming language
DSPS Director, Security Plans and Service
DSR defense source registry
DSS Defense Security Service; Distribution Standard System
DSS/ALOC direct support system/air line of communications
DSSCS Defense Special Security Communications System
DSSM Defense Superior Service Medal
DSSO data system support organization; defense sensitive support office; defense systems support organization
DSSR Department of State Standardized Regulation
DST decision support template; Defense Logistics Agency support team; deployment support team; district support team
DSTP Director of Strategic Target Planning
DSTR destroy
DSTS-G Defense Information Systems Network (DISN) Satellite Transmission Services - Global
DSVL doppler sonar velocity log

DSVT	digital subscriber voice terminal
DT	Directorate for MASINT and Technical Collection (DIA)
DTA	Defense Threat Assessment; dynamic threat assessment
DTAM	defense terrorism awareness message
DTC	defense transportation coordination
DTCI	Defense Transportation Coordination Initiative
DTD	Deployable Training Division; detailed troop decontamination
DTE	data terminal equipment; developmental test and evaluation
DTED	digital terrain elevation data
DTG	date-time group; digital trunk group (digital transmission group)
D/T/ID	detect/track/identify
DTIP	Disruptive Technology Innovations Partnership (DIA)
DTL	designator target line
DTMF	dual tone multi-frequency
DTMR	defense traffic management regulation
DTO	division transportation office; drug trafficking organization
DTOC	division tactical operations center
DTR	defense transportation regulation
DTRA	Defense Threat Reduction Agency
DTRACS	Defense Transportation Reporting and Control System
DTRATCA	Defense Threat Reduction and Treaty Compliance Agency
DTS	Defense Transportation System; Defense Travel System; diplomatic telecommunications service
DTTS	Defense Transportation Tracking System
DTWR	defense terrorism warning report
DU	depleted uranium
DURC	dual-use research of concern
DUSD	deputy under Secretary of Defense
DUSD (CI&S)	Deputy Under Secretary of Defense for Counterintelligence and Security
DUSDL	Deputy Under Secretary of Defense for Logistics
DUSD(L&MR)	Deputy Under Secretary of Defense for Logistics and Materiel Readiness
DUSDP	Deputy Under Secretary of Defense for Policy
DV	distinguished visitor
DVA	Department of Veterans Affairs
DVD	digital video device; digital video disc
DVIDS	Defense Video and Imagery Distribution System
DVITS	Digital Video Imagery Transmission System
DVOW	digital voice orderwire
DVT	deployment visualization tool
DWAS	Defense Working Capital Accounting System

DWMCF	double-wide modular causeway ferry
DWT	deadweight tonnage
DWTS	Digital Wideband Transmission System
DX	Directorate for External Relations (DIA)
DZ	drop zone
DZC	drop zone controller
DZCO	drop zone control officer
DZSO	drop zone safety officer
DZST	drop zone support team
DZSTL	drop zone support team leader

E

E	total probable error
E&DCP	evaluation and data collection plan
E&E	emergency and extraordinary expense authority
E&EE	emergency and extraordinary expense
E&I	engineering and installation
E&M	ear and mouth; special signaling leads
E1	Echelon 1
E2	Echelon 2
E3	Echelon 3; electromagnetic environmental effects
E4	Echelon 4
E5	Echelon 5
E-8C	joint surveillance, target attack radar system (JSTARS) aircraft
EA	electronic attack; emergency action; evaluation agent; executive agent; executive assistant
ea	each
EAC	echelons above corps (Army); emergency action committee
EACS	expeditionary aeromedical evacuation crew member support
EACT	expeditionary aeromedical evacuation coordination team
EAD	earliest arrival date; echelons above division (Army); extended active duty
EADRU	Euro-Atlantic disaster response unit
EADS	Eastern Air Defense Sector
EAES	expeditionary aeromedical evacuation squadron
EAF	expeditionary aerospace forces; expeditionary airfield
EAI	executive agent instruction
EAM	emergency action message
EAP	emergency action plan; emergency action procedures
EAPC	Euro-Atlantic Partnership Council
EAP-CJCS	emergency action procedures of the Chairman of the Joint Chiefs of Staff
EARLY	evasion and recovery supplemental data report
E-ARTS	en route automated radar tracking system
EASF	expeditionary aeromedical staging facility
EAST	expeditionary aeromedical evacuation staging team
EASTPAC	eastern Pacific Ocean
EBCDIC	extended binary coded decimal interchange code
EBS	environmental baseline survey
EC	electronic combat; enemy combatant; error control; European Community
ECAC	Electromagnetic Compatibility Analysis Center
ECB	echelons corps and below (Army)
ECC	engineer coordination cell; evacuation control center

ECES	expeditionary civil engineer squadron
ECHA	Executive Committee for Humanitarian Affairs (UN)
ECHO	European Commission Directorate General for Humanitarian Aid and Civil Protection; European Community Humanitarian Aid Department
ECM	electronic countermeasures
ECN	electronic change notice; Minimum Essential Emergency Communications Network
ECO	electronic combat officer
ECOSOC	Economic and Social Council (UN)
ECP	emergency command precedence; engineering change proposal; entry control point
ECS	expeditionary combat support
ECU	environmental control unit
ED	envelope delay; evaluation directive
EDA	Economic Development Administration (DOC); excess defense articles
EDC	estimated date of completion
EDD	earliest delivery date
EDI	electronic data interchange
EDSS	equipment deployment and storage system
EE	emergency establishment
EEA	environmental executive agent
EEBD	emergency escape breathing device
EECT	end evening civil twilight
EED	electro-explosive device; emergency-essential designation
EEDAC	emergency essential Department of the Army civilian
EEE	emergency and extraordinary expense
EEFI	essential element of friendly information
EEI	essential element of information
EELV	evolved expendable launch vehicle
EENT	end of evening nautical twilight
EEO	equal employment opportunity
EEPROM	electronic erasable programmable read-only memory
EER	enlisted employee review; extended echo ranging
EEZ	exclusive economic zone
EFA	engineering field activity
EFAC	emergency family assistance center
EFD	engineering field division
EFP	explosively formed projectile
EFST	essential fire support task
EFT	electronic funds transfer
EFTO	encrypt for transmission only
EGAT	Bureau of Economic Growth, Agriculture, and Trade (USAID)
EGM	Earth Gravity Model

EGS	Earth ground station
EH	explosive hazard
EHCC	explosive hazards coordination cell
EHDB	explosive hazard database
EHF	extremely high frequency
EHO	environmental health officer
EHRA	environmental health risk assessment
EHSA	environmental health site assessment
EHT	explosive hazard team
EI	environmental information; exercise item
EIA	Electronic Industries Association
EID	electrically initiated device
EIS	Environmental Impact Statement
eJMAPS	electronic Joint Manpower and Personnel System
EJPME	enlisted joint professional military education
ELBA	emergency locator beacon
ELCAS	elevated causeway system
ELCAS(M)	elevated causeway system (modular)
ELCAS(NL)	elevated causeway system (Navy lighterage)
ELD	emitter locating data
ELINT	electronic intelligence
ELIST	enhanced logistics intratheater support tool
ELOS	extended line of sight
ELPP	equal level patch panel
ELR	extra-long-range aircraft
ELSEC	electronics security
ELT	emergency locator transmitter
ELV	expendable launch vehicle
ELVA	emergency low-visibility approach
EM	electromagnetic; emergency management; executive manager
EMAC	emergency management assistance compact
E-mail	electronic mail
EMALL	electronic mall
EMBM	electromagnetic battle management
EMC	electromagnetic compatibility
EMCON	emission control
EMD	effective miss distance; expeditionary military information support detachment
EME	electromagnetic environment
EMEDS	expeditionary medical support
EMF	expeditionary medical facility
EMI	electromagnetic interface; electromagnetic interference
EMIO	expanded maritime interception operations
EMOE	electromagnetic operational environment
EMP	electromagnetic pulse

EMR hazards	electromagnetic radiation hazards
EMS	electromagnetic spectrum; emergency medical services
EMSC	electromagnetic spectrum control
EMSEC	emanations security
EMSM	electromagnetic spectrum manager
EMT	emergency medical technician; emergency medical treatment; expeditionary military information support team
EMTF	expeditionary mobility task force
EMU	expeditionary medical unit
EMV	electromagnetic vulnerability
ENCOM	engineer command (Army)
ENDEX	exercise termination
ENL	enlisted
ENSCE	enemy situation correlation element
ENWGS	Enhanced Naval Warfare Gaming System
EO	electro-optical; end office; equal opportunity; executive order; eyes only
EOB	electromagnetic order of battle; electronic order of battle; enemy order of battle
EOC	early operational capability; emergency operating center; emergency operations center
EOCA	explosive ordnance clearance agent
EOD	explosive ordnance disposal
EODMU-1	explosive ordnance disposal mobile unit one
EOI	electro-optic(al) imagery
EO-IR	electro-optical-infrared
EO-IR CM	electro-optical-infrared countermeasure
EOL	end of link
EOM	end of message
EOP	emergency operating procedures
E-O TDA	electro-optical tactical decision aid
EOW	engineering orderwire
EP	electronic protection; emergency preparedness; emergency procedures; excess property; execution planning
EPA	Environmental Protection Agency; evasion plan of action
EPBX	electronic private branch exchange
EPBS	expeditionary prime base engineer emergency force squadron
EPC	Emergency Procurement Committee
EPF	enhanced palletized load system (PLS) flatrack
EPH	emergency planning handbook
EPIC	El Paso Intelligence Center
EPIRB	emergency position-indicating radio beacon
EPLO	emergency preparedness liaison officer
EPROM	erasable programmable read-only memory

EPU	expeditionary port unit
EPW	enemy prisoner of war
EPW/CI	enemy prisoner of war/civilian internee
ERC	emergency relief coordinator; exercise related construction
ERDC	Engineer Research and Development Center
ERG	Emergency Response Guidebook
ERGM	extended range guided munitions
ERO	engine running on or offload
ERPSS	En Route Patient Staging System
ERRO	Emergency Response and Recovery Office
ERSD	estimated return to service date
ERT	emergency response team (FEMA); engineer reconnaissance team
ERT-A	emergency response team - advance element
ERU	emergency response unit
ERW	explosive remnants of war
ES	electronic support; electronic warfare support; executive secretariat
ESAC	Electromagnetic-Space Analysis Center (NSA)
ESB	engineer support battalion
ESC	Electronics Systems Center; expeditionary sustainment command
ESF	Economic Support Fund; emergency support function
ESG	executive steering group; expeditionary strike group
ESGN	electrically suspended gyro navigation
ESI	extremely sensitive information
ESK	electronic staff weather officer kit
ESM	expeditionary site mapping
ESO	embarkation staff officer; environmental science officer; Expeditionary Support Organization (DFAS)
ESOC	Emergency Supply Operations Center
ESOH	environmental, safety, and occupational health
ESORTS	Enhanced Status of Resources and Training System
ESP	engineer support plan
E-Space	Electromagnetic-Space
ESR	external supported recovery
EST	embarked security team; emergency service team; emergency support team (FEMA); en route support team
ET	electronics technician
ETA	estimated time of arrival
ETAC	emergency tactical air control
ETD	estimated time of departure
ETF	electronic target folder
ETI	estimated time of intercept

ETIC	estimated time for completion; estimated time in commission
ETM	electronic transmission; essential tasks matrix
ETO	Emergency Transportation Operations (DOT)
ETPL	endorsed TEMPEST products list
ETR	export traffic release
ETS	European telephone system
ETSS	extended training service specialist
ETX	end of text
EU	European Union
E-UAV	endurance unmanned aerial vehicle
EUB	essential user bypass
EURV	essential user rekeying variable
EUSA	Eighth US Army
EUSC	effective United States control; effective United States controlled
EUSCS	effective United States-controlled ships
EVC	evasion chart
EVE	equal value exchange
EW	early warning; electronic warfare
EWC	electronic warfare cell; electronic warfare coordinator
EWCA	electronic warfare control authority
EWCC	electronic warfare coordination cell
EWCS	electronic warfare control ship
EWD	Electronic Warfare Directorate (USSTRATCOM)
EWE	electronic warfare element
EWG	electronic warfare group
EW/GCI	early warning/ground-controlled intercept
EWIR	electronic warfare integrated reprogramming
EWO	electronic warfare officer
EWWG	electronic warfare working group
EXCIMS	Executive Council for Modeling and Simulations
ExCom	executive committee
EXDIR	Executive Director (CIA)
EXDIR/ICA	Executive Director for Intelligence Community Affairs (USG)
EXECSEC	executive secretary
EXER	exercise
EXORD	execute order
EXPLAN	exercise plan
EZ	exchange zone
EZCO	extraction zone control officer
EZM	engagement zone manager

F

F	Fahrenheit; flare patterns; flash
F2T2EA	find, fix, track, target, engage, and assess
F3EAD	find, fix, finish, exploit, analyze, and disseminate
F&ES	fire and emergency services
FA	feasibility assessment; field artillery
FAA	Federal Aviation Administration (DOT); Foreign Assistance Act
FAAO	Federal Aviation Administration order
FAAR	facilitated after-action review
FAC	forward air controller
FAC(A)	forward air controller (airborne)
FACE	forward aviation combat engineering
FACSFAC	fleet area control and surveillance facility
FACT	field advance civilian team; field assessment and coordination team
FAD	feasible arrival date
F/AD	force/activity designator
FAE	fuel air explosive
FAH	final attack heading; foreign affairs handbook
FALD	Field Administration and Logistics Division
FALOP	Forward Area Limited Observing Program
FAM	functional area manager
FAMP	forward area minefield planning
FAO	Food and Agriculture Organization (UN); foreign area officer
FAPES	Force Augmentation Planning and Execution System
FAR	Federal Acquisition Regulation; Federal Aviation Regulation; formal assessment report
FARC	Revolutionary Armed Forces of Colombia
FARP	forward arming and refueling point
FAS	Foreign Agricultural Service (USDA); frequency assignment subcommittee; fueling at sea; functional account symbol
FASCAM	family of scatterable mines
FAST	field assessment surveillance team; fleet antiterrorism security team
FAX	facsimile
FB	forward boundary
FBI	Federal Bureau of Investigation (DOJ)
FBIS	Foreign Broadcast Information Service
FBO	faith-based organization
FC	field circular; final coordination; fires cell (Army); floating causeway; floating craft; force commander
FCA	Foreign Claims Act; functional configuration audit

FCC	Federal Communications Commission; Federal coordinating center; functional combatant commander
FCE	forward command element
FCG	foreign clearance guide
FCM	foreign consequence management
FCO	federal coordinating officer
FCP	fire control party
FCT	firepower control team
FD	first draft; from temporary duty
FDA	Food and Drug Administration
FDBM	functional database manager
FDC	fire direction center
FDESC	force description
FDL	fast deployment logistics
FDLP	flight deck landing practice
FDM	frequency division multiplexing
FDO	fire direction officer; flexible deterrent option; flight deck officer; foreign disclosure officer
FDP	forward distribution point
FDPMU	forward-deployable preventive medicine unit
FDR	foreign disaster relief
FDR/FA	flight data recorder/fault analyzer
FDS	fault detection system
FDSL	fixed directory subscriber list
FDSS	fault detection subsystem
FDSSS	flight deck status and signaling system
FDT	forward distribution team
FDUL	fixed directory unit list
FDX	full duplex
FE	facilities engineering; fires element
FEA	front-end analysis
FEBA	forward edge of the battle area
FEC	facilities engineering command; forward error correction
FECC	fires and effects coordination cell
FED-STD	federal standard
FEI	forensic-enabled intelligence
FEK	frequency exchange keying
FEMA	Federal Emergency Management Agency (DHS)
FEP	fleet satellite (FLTSAT) extremely high frequency (EHF) Package; foreign excess property
FEPP	federal excess personal property; foreign excess personal property
FES	fire emergency services
FEST	foreign emergency support team; forward engineer support team
FET	facility engineer team

FEU	forty-foot equivalent unit
FEZ	fighter engagement zone
FF	navy fast frigate
Ff	fatigue correction factor
FFA	free-fire area
FFC	force fires coordinator
FFCC	flight ferry control center; force fires coordination center (USMC)
FFD	foundation feature data
FFE	field force engineering; flame field expedients
FFG	guided missile frigate
FFH	fast frequency hopping
FFH-net	fast-frequency-hopping net
FFHT-net	fast-frequency-hopping training net
FFIR	friendly force information requirement
FFP	Food for Peace; fresh frozen plasma; Office of Food for Peace (DOS)
FFT	friendly force tracking
FFTU	forward freight terminal unit
FG	fighter group
FGMDSS	Future Global Maritime Distress and Safety System
FGS	final governing standard; Force Generation Service (UN)
FH	fleet hospital
FHA	Bureau for Food and Humanitarian Assistance; foreign humanitarian assistance
FHC	family help center
FHP	force health protection
FHWA	Federal Highway Administration (DOT)
FI	foreign intelligence
FIA	functional interoperability architecture
FIC	force indicator code
FID	foreign internal defense
FIDAF	foreign internal defense augmentation force
FIE	fly-in echelon; foreign intelligence entity
FIFO	first-in-first-out
FinCEN	Financial Crimes Enforcement Network
FIR	first-impressions report
FIRCAP	foreign intelligence requirements capabilities and priorities
1st IOC	1st Information Operations Command (Land)
FIS	Foreign Intelligence Service
FISC	fleet and industrial supply center
FISINT	foreign instrumentation signals intelligence
FISS	foreign intelligence and security services
FIST	fire support team; fleet imagery support terminal; fleet intelligence support team

FIWC	fleet information warfare center
FIXe	navigational fix error
FLAR	forward-looking airborne radar
FLC	fleet logistics center
FLENUMMETOCCEN	Fleet Numerical Meteorology and Oceanography Center
FLENUMMETOCDET	Fleet Numerical Meteorological and Oceanographic Detachment
FLETC	Federal Law Enforcement Training Center (DHS)
FLIP	flight information publication; flight instruction procedures
FLIR	forward-looking infrared
FLITE	federal legal information through electronics
FLO/FLO	float-on/float-off
FLOLS	fresnel lens optical landing system
FLOT	forward line of own troops
FLP	force level planning
FLS	forward logistic site
FLSG	force logistic support group
FLTCYBERCOM	Fleet Cyber Command (Navy)
FLTSAT	fleet satellite
FLTSATCOM	fleet satellite communications
FM	field manual (Army); financial management; flare multiunit; force module; frequency modulation; functional manager
FM/A	functional manager for analysis
FMA-net	frequency management A-net
FMAS	foreign media analysis subsystem
FMAT	financial management augmentation team
FMC	force movement characteristics; full mission-capable
FMCH	fleet multichannel
FMCR	Fleet Marine Corps Reserve
FMCSA	Federal Motor Carrier Safety Administration
FMI	field manual-interim
FMF	Fleet Marine Force
FMFP	foreign military financing program
FMID	force module identifier
FMO	frequency management office; functional manager office
FMP	foreign materiel program
FMS	force module subsystem; foreign military sales
FMSC	frequency management sub-committee
FMT-net	frequency management training net
FMV	full motion video
FN	foreign nation
FNMOC	Fleet Numerical Meteorology and Oceanography Center
FNMOD	Fleet Numerical Meteorological and Oceanographic Detachment
FNOC	Fleet Numerical Oceanographic Command

FNS	foreign nation support
FO	fiber optic; flash override; forward observer
FOB	forward operating base
FOC	full operational capability; future operations cell
FOD	field operations division; foreign object damage
FOFW	fiber optic field wire
FOG	Field Operations Guide for Disaster Assessment and Response
FOI	fault detection isolation
FOIA	Freedom of Information Act
FOIU	fiber optic interface unit
FOL	fiber optic link
FON	freedom of navigation (operations)
FORCE	fuels operational readiness capability equipment (Air Force)
FORMICA	foreign military intelligence collection activities
FORSCOM	United States Army Forces Command
FORSTAT	force status and identity report
FOS	forward operating site; full operational status
FOT	follow-on operational test
FOUO	for official use only
FOV	field of view
FP	firing point; force protection; frequency panel
FPA	foreign policy advisor
FPC	final planning conference; future plans cell
FPCON	force protection condition
FPD	force protection detachment; foreign post differential
FPF	final protective fire
FPM	Federal personnel manual
FPO	fleet post office
FPOC	focal point operations center
FPS	Federal Protective Service; force protection source
FPTAS	flight path threat analysis simulation
FPTS	forward propagation by tropospheric scatter
FPWG	force protection working group
FR	final report; frequency response
FRA	Federal Railroad Administration (DOT)
FRAG	fragmentation code
FRAGORD	fragmentary order
FRC	federal resource coordinator; forward resuscitative care
FRD	formerly restricted data
FREQ	frequency
FRERP	Federal Radiological Emergency Response Plan
FRF	fragment retention film
FRMAC	Federal Radiological Monitoring and Assessment Center (DOE)
FRN	force requirement number

FRO	flexible response option
FROG	free rocket over ground
FRP	Federal response plan (USG)
FRRS	frequency resource record system
FRTP	fleet response training plan
FS	fighter squadron; file separator; file server; flare single-unit
fs	search radius safety factor
FSA	fire support area
FSB	fire support base; forward staging base; forward support base; forward support battalion
FSC	fire support cell; fire support coordinator (USMC)
FSCC	fire support coordination center (USMC)
FSCL	fire support coordination line
FSCM	fire support coordination measure
FSCOORD	fire support coordinator (Army)
FSE	fire support element
FSEM	fire support execution matrix
FSF	foreign security forces
FSI	Foreign Service Institute
FSK	frequency shift key
FSN	foreign service national
FSO	fire support officer; flight safety officer; foreign service officer
FSP	functional support plan
FSR	field service representative
FSRT	fatality search and recovery team
FSS	fast sealift ship; fire support station; flight service station
FSSG	force service support group (USMC)
FSSP	fuel system supply point
FSST	forward space support to theater
FST	fire support task; fleet surgical team
FSU	former Soviet Union; forward support unit
FSW	feet of seawater
ft	feet; foot
ft3	cubic feet
FTC	Federal Trade Commission
FTCA	Foreign Tort Claims Act
FTN	force tracking number
FTP	file transfer protocol
FTRG	fleet tactical readiness group
FTS	Federal Telecommunications System; Federal telephone service; file transfer service
FTU	field training unit; freight terminal unit
FUAC	functional area code
FUNCPLAN	functional plan
F/V	fishing vessel

Fv	aircraft speed correction factor
FVT	Force Validation Tool
FW	fighter wing; fixed-wing; weather correction factor
FWA	fraud, waste, and abuse
FWC	fleet weather center
FWD	forward
FWDA	friendly weapon danger area
FWF	former warring factions
FY	fiscal year
FYDP	Future Years Defense Program

Intentionally Blank

G

G-1	Army or Marine Corps component manpower or personnel staff officer (Army division or higher staff, Marine Corps brigade or higher staff)
G-2	Army Deputy Chief of Staff for Intelligence; Army or Marine Corps component intelligence staff officer (Army division or higher staff, Marine Corps brigade or higher staff)
G-2X	Army counterintelligence and human intelligence staff element
G-3	Army or Marine Corps component operations staff officer (Army division or higher staff, Marine Corps brigade or higher staff); assistant chief of staff, operations
G-4	Army or Marine Corps component logistics staff officer (Army division or higher staff, Marine Corps brigade or higher staff); Assistant Chief of Staff for Logistics
G-5	assistant chief of staff, plans
G-6	Army or Marine Corps component command, control, communications, and computer systems staff officer; assistant chief of staff for communications; signal staff officer (Army)
G-7	Army component information operations staff officer; assistant chief of staff, information engagement; information operations staff officer (ARFOR)
G/A	ground to air
GA	geospatial analyst; Tabun, a nerve agent
GAA	general agency agreement; geospatial intelligence assessment activity
GAFS	General Accounting and Finance System
GAMSS	Global Air Mobility Support System
GAO	General Accounting Office; Government Accountability Office
GAR	gateway access request
GARS	Global Area Reference System
GAT	governmental assistance team
GATB	guidance, apportionment, and targeting board
GATES	Global Air Transportation Execution System
GB	group buffer; Sarin, a nerve agent
GBI	ground-based interceptor
GBL	government bill of lading
GBMD	global ballistic missile defense
GBR	ground-based radar
GBS	Global Broadcast Service; Global Broadcast System
GBU	guided bomb unit

GC	general counsel; Geneva Convention; Geneva Convention Relative to the Protection of Civilian Persons in Time of War
GC3A	global command, control, and communications assessment
GC4A	global command, control, communications, and computer assessment
GCA	ground controlled approach
GCC	geographic combatant commander; global contingency construction
GCCC	global contingency construction contract
GCCMAC	Global Contingency Construction Multiple Award Contract (Navy)
GCCS	Global Command and Control System
GCCS-A	Global Command and Control System-Army
GCCS-I3	Global Command and Control System Integrated Imagery and Intelligence
GCCS-J	Global Command and Control System-Joint
GCCS-M	Global Command and Control System-Maritime
GCE	ground combat element (USMC)
GCI	ground control intercept
GCM	global container manager; Global Information Grid (GIG) Content Management
GCP	global campaign plan; ground commander's pointer
GCP-CWMD	Global Campaign Plan for Combating Weapons of Mass Destruction
GCRI	general collective routing indicator (RI)
GCS	ground control station
GCSC	global contingency service contract
GCSMAC	Global Contingency Services Multiple Award Contract (Navy)
GCSS	Global Command Support System
GCSS-J	Global Combat Support System-Joint
GCTN	global combating terrorism network
GD	Soman, a nerve agent
GDF	gridded data field; Guidance for Development of the Force
GDIP	General Defense Intelligence Program
GDIPP	General Defense Intelligence Proposed Program
GDP	General Defense Plan (SACEUR): gross domestic product
GDSS	Global Decision Support System
GE	general engineering
GEF	Guidance for Employment of the Force
GEM	Global Information Grid (GIG) Enterprise Management
GENADMIN	general admin (message)
GENSER	general service (message)
GENTEXT	general text
GEO	geosynchronous Earth orbit

GEOCODE	geographic code
GEOFILE	geolocation code file; standard specified geographic location file
GEOINT	geospatial intelligence
GEOLOC	geographic location; geographic location code
GEOREF	geographic reference; world geographic reference system
GETS	geospatial enterprise tasking, processing, exploitation, and dissemination service
GF	a nerve agent
GFE	government-furnished equipment
GFI	government-furnished information
GFM	global force management; global freight management; government-furnished material
GFMAP	Global Force Management Allocation Plan
GFMB	Global Force Management Board
GFMIG	Global Force Management Implementation Guidance
GFMPL	Graphics Fleet Mission Program Library
GFOAR	global family of operation plans assessment report
GFP	government-furnished property
GFS	global fleet station; government-furnished support
GFU	group framing unit
GHz	gigahertz
GI	geomatics and imagery
GI&S	geospatial information and services
GIAC	graphic input aggregate control
GIANT	Global Positioning System Interference and Navigation Tool
GIBCO	geospatial-intelligence base for contingency operations
GIC	(*gabarit international de chargement)* international loading gauge
GICNT	Global Initiative to Combat Nuclear Terrorism
GIE	global information environment
GIMS	Geospatial Intelligence Information Management Services
GIO	Geospatial Intelligence Organisation (New Zealand)
GIP	gridded installation photograph
GIS	geographic information system; geospatial information systems
GL	government-leased
GLCM	ground-launched cruise missile
GLINT	gated laser intensifier
GLO	ground liaison officer
GLOC	ground line of communications
GLTD	ground laser target designator
GM	group modem
GMD	global missile defense; ground-based midcourse defense; group mux and/or demux

GMDSS	Global Maritime Distress and Safety System
GMF	ground mobile force
GMFP	global military force policy
GMI	general military intelligence
GMLRS	Global Positioning System Multiple Launch Rocket System
GMP	global maritime partnership
GMR	graduated mobilization response; ground mobile radar
GMRS	global mobility readiness squadron
GMS	global mobility squadron
GMSC	Global Mission Support Center (USSOCOM)
GMTI	ground moving target indicator
GNA	Global Information Grid (GIG) Network Assurance
GNCC	global network operations center
GND	Global Information Grid (GIG) Network Defense
GNSC	global network operations support center
GNSS	global navigation satellite system
GO	government-owned
GOCO	government-owned, contractor-operated
GOES	geostationary operational environmental satellite
GO/FO	general officer/flag officer
GOGO	government-owned, government-operated
GOS	grade of service
GOSG	general officer steering group
GOTS	government off-the-shelf
GP	general purpose; group
GPC	geospatial planning cell; government purchase card
GPD	gallons per day
GPE	geospatial intelligence preparation of the environment
GPEE	general purpose encryption equipment
GPL	Geospatial Product Library
GPM	gallons per minute; global pallet manager
GPMDM	group modem
GPMIC	Global Patient Movement Integration Center
GPMJAB	Global Patient Movement Joint Advisory Board
GPMRC	Global Patient Movement Requirements Center
GPS	Global Positioning System
GPSOC	Global Positioning System Operations Center
GPW	Geneva Convention Relative to the Treatment of Prisoners of War
GR	graduated response
GRASP	general retrieval and sort processor
GRCA	ground reference coverage area
GRG	gridded reference graphic
GRL	global reach laydown
GRREG	graves registration

GS	general service; general support; group separator
GSA	General Services Administration
GSE	ground support equipment
GSI	glide slope indicator
GSM	ground station module
GSO	general services officer
GSORTS	Global Status of Resources and Training System
GS-R	general support-reinforcing
GSR	general support-reinforcing; ground surveillance radar
GSSA	general supply support area
GSSC	global satellite communications (SATCOM) support center
GST	geospatial support team
gt	gross ton
GTA	graphic training aid
GTAS	ground-to-air signals
GTL	gun-target line
GTM	global transportation management
GUARD	US National Guard and Air Guard
GUARDS	General Unified Ammunition Reporting Data System
G/VLLD	ground/vehicle laser locator designator
GWC	global weather central
GWEN	Ground Wave Emergency Network
GWOT	global war on terrorism
GWS	Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field
GWS Sea	Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of the Armed Forces at Sea

Intentionally Blank

H

H&I	harassing and interdicting
H&S	headquarters and service
HA	holding area; humanitarian assistance
HAARS	high-altitude airdrop resupply system
HAC	helicopter aircraft commander; human intelligence analysis cell
HACC	humanitarian assistance coordination center
HAHO	high-altitude high-opening parachute technique
HAP	humanitarian assistance program
HAP-EP	humanitarian assistance program-excess property
HARC	human intelligence analysis and reporting cell
HARM	high-speed antiradiation missile
HARP	high altitude release point
HAST	humanitarian assistance survey team
HATR	hazardous air traffic report
HAZ	hazardous cargo
HAZMAT	hazardous materials
HB	heavy boat
HBCT	heavy brigade combat team
HC	Directorate for Human Capital (DIA)
HCA	head of contracting activity; humanitarian and civic assistance
HCAS	hostile casualty
HCL	hydrochloride
HCO	helicopter control officer
HCP	hardcopy printer
HCS	helicopter combat support (Navy); helicopter coordination section
HCT	human intelligence (HUMINT) collection team
HD	a mustard agent; harbor defense; harmonic distortion; homeland defense
HDC	harbor defense commander; helicopter direction center
HDCU	harbor defense command unit
HDM	humanitarian demining
HDO	humanitarian demining operations
HDPLX	half duplex
HDR	humanitarian daily ration
HDTC	Humanitarian Demining Training Center
HE	heavy equipment; high explosives
HEAT	helicopter external air transport; high explosive antitank
HEC	helicopter element coordinator
HEFOE	hydraulic electrical fuel oxygen engine
HEI	high explosives incendiary
HEL-H	heavy helicopter

HEL-L	light helicopter
HEL-M	medium helicopter
HELO	helicopter
HEMP	high-altitude electromagnetic pulse
HEMTT	heavy expanded mobile tactical truck
HEO	highly elliptical orbit
HEPA	high efficiency particulate air
HERF	hazards of electromagnetic radiation to fuels
HERO	electromagnetic radiation hazards; hazards of electromagnetic radiation to ordnance
HERP	hazards of electromagnetic radiation to personnel
HET	heavy equipment transporter; human intelligence exploitation team
HEWSweb	Humanitarian Early Warning Service
HF	high frequency
HFA	human factors analysis
HFDF	high-frequency direction finding
HFP	hostile fire pay
HFRB	high frequency regional broadcast
HH	homing pattern
HHC	headquarters and headquarters company
HHD	headquarters and headquarters detachment
HHQ	higher headquarters
HHS	Department of Health and Human Services
HIC	humanitarian information center
HICAP	high-capacity firefighting foam station
HIDACZ	high-density airspace control zone
HIDTA	high-intensity drug trafficking area
HIFR	helicopter in-flight refueling
HIMAD	high-to-medium-altitude air defense
HIMARS	High Mobility Artillery Rocket System
HIMEZ	high-altitude missile engagement zone
HIRSS	hover infrared suppressor subsystem
HIRTA	high intensity radio transmission area
HIU	humanitarian information unit (DOS)
HIV	human immunodeficiency virus
HJ	crypto key change
HLPS	heavy-lift pre-position ship
HM	hazardous material
HMA	humanitarian mine action
HMCS	helmet-mounted cueing system
HMH	Marine heavy helicopter squadron
HMIRS	Hazardous Material Information Resource System
HMIS	Hazardous Material Information System
HMLA	Marine light/attack helicopter squadron
HMM	Marine medium helicopter squadron

HMMWV	high mobility multipurpose wheeled vehicle
HMOD	harbormaster operations detachment
HMW	health, morale, and welfare
HN	host nation
HNC	host-nation coordination
HNCC	host nation coordination center
HNS	host-nation support
HNSCC	host-nation support coordination cell
HNSF	host-nation security forces
HOB	height of burst
HOC	human intelligence operations cell; humanitarian operations center
HOCC	humanitarian operations coordination center
HOD	head of delegation
HOGE	hover out of ground effect
HOIS	hostile intelligence service
HOM	head of mission
HOSTAC	helicopter operations from ships other than aircraft carriers (USN publication)
HPA	high power amplifier
HPM	high-power microwave
HPMSK	high priority mission support kit
HPT	high-payoff target
HQ	HAVE QUICK; headquarters
HQCOMDT	headquarters commandant
HQDA	Headquarters, Department of the Army
HQFM-net	HAVE QUICK frequency modulation net
HQFMT-net	HAVE QUICK frequency modulation training net
HQMC	Headquarters, Marine Corps
HR	helicopter request; hostage rescue
HRB	high-risk billet
HRC	high-risk-of-capture; Human Resources Command
HRF	homeland response force
HRI	high risk of isolation
HRJTF	humanitarian relief joint task force
HRO	humanitarian relief organizations
HRP	high-risk personnel; human remains pouch
HRS	horizon reference system
HRT	health response team; hostage rescue team
HS	health services; helicopter antisubmarine (Navy); homeland security; homing single-unit
HSAC	Homeland Security Advisory Council
HSAS	Homeland Security Advisory System
HSB	high speed boat
HSC	helicopter sea combat (Navy); Homeland Security Council
HSCDM	high speed cable driver modem

HSC/PC	Homeland Security Council Principals Committee
HSC/PCC	Homeland Security Council Policy Coordination Committee
HSD	health service delivery; human intelligence support detachment
HSE	headquarters support element; human intelligence support element (DIA)
HSEP	hospital surgical expansion package (USAF)
HSI	hyperspectral imagery; Office of Homeland Security Investigations (DHS)
HSIN	Homeland Security Information Network (DHS)
HSIP	Homeland Security Infrastructure Program
HSM	humanitarian service medal
HSPD	homeland security Presidential directive
HSPR	high speed pulse restorer
HSS	health service support
HSSDB	high speed serial data buffer
HSV	high-speed vessel
HT	hatch team
HTERRCAS	hostile terrorist casualty
HTG	hard target graphic
HTH	high test hypochlorite
HU	hospital unit
HUD	head-up display
HUMINT	human intelligence
HUMRO	humanitarian relief operation
HUMRO OCP	humanitarian relief operation operational capability package
HUS	hardened unique storage
HVA	high-value asset
HVAA	high value airborne asset
HVAC	heating, ventilation, and air conditioning
HVCDS	high-velocity container delivery system
HVI	high-value individual
HVT	high-value target
HW	hazardous waste
HWM	high water mark
HYE	high-yield explosives
Hz	hertz

I

I	immediate; individual
I2	identity intelligence
I2WD	Intelligence and Information Warfare Division (Army)
I&A	Office of Intelligence and Analysis (DHS)
IA	imagery analyst; implementing arrangement; individual augmentee; information assurance
IAA	incident area assessment; incident awareness and assessment
IAC	Interagency Advisory Council
IACG	interagency coordination group
IADB	Inter-American Defense Board
IADS	integrated air defense system
IAEA	International Atomic Energy Agency (UN)
IAF	initial approach fix
IAIP	Information Analysis and Infrastructure Protection
IAM	inertially aided munition
IAMD	integrated air and missile defense
IAMSAR	International Aeronautical and Maritime Search and Rescue manual
IAP	incident action plan; international airport
IAPP	Interagency Partnership Program
IAR	interoperability assessment report
IAS	International Assistance System
IASC	Inter-Agency Standing Committee (UN); interim acting service chief
IATA	International Air Transport Association
IATACS	Improved Army Tactical Communications System
IATO	interim authority to operate
IAVM	information assurance vulnerability management
IAW	in accordance with
I/B	inboard
IBB	International Broadcasting Bureau
IBCT	infantry brigade combat team
IBES	intelligence budget estimate submission
IBET	integrated border enforcement team
IBM	International Business Machines
IBS	Integrated Booking System; integrated broadcast service; Integrated Broadcast System
IBS-I	Integrated Broadcast Service-Interactive
IBS-S	Integrated Broadcast Service-Simplex
IBU	inshore boat unit
IC	incident commander; intelligence community; intercept
IC3	integrated command, control, and communications
ICAD	individual concern and deficiency

ICAF	Interagency Conflict Assessment Framework
ICAO	International Civil Aviation Organization
ICAT	interagency conflict assessment team
ICBM	intercontinental ballistic missile
ICC	information confidence convention; information coordination center; Intelligence Coordination Center (USCG); International Criminal Court; Interstate Commerce Commission
ICD	international classifications of diseases; International Cooperation and Development Program (USDA)
ICDC	Intelligence Community Deputies Committee
ICDS	improved container delivery system
ICE	Immigration and Customs Enforcement (DHS)
ICEDEFOR	Iceland Defense Forces
ICEPP	Incident Communications Emergency Policy and Procedures
IC/EXCOM	Intelligence Community Executive Committee
ICG	interagency core group
ICIS	integrated consumable item support
ICITAP	International Criminal Investigative Training Assistance Program (DOJ)
ICM	image city map; improved conventional munitions; integrated collection management
ICN	idle channel noise; interface control net
ICNIA	integrated communications, navigation, and identification avionics
ICOD	intelligence cutoff data
ICODES	Integrated Computerized Deployment System
ICON	imagery communications and operations node; intermediate coordination node
ICP	intertheater communications security package; interface change proposal; inventory control point
ICPC	Intelligence Community Principals Committee
ICR	Intelligence Collection Requirements
ICRC	International Committee of the Red Cross
ICRI	interswitch collective routing indicator
ICS	incident command system; integrated country strategy; internal communications system; inter-Service chaplain support
ICSF	integrated command communications system framework
ICSAR	interagency committee on search and rescue
ICT	information and communications technology
ICU	intensive care unit; interface control unit
ICVA	International Council of Voluntary Agencies
ICW	in coordination with

ID	identification; identifier; initiating directive
IDAD	internal defense and development
IDB	integrated database
IDCA	International Development Cooperation Agency
IDDF	intermediate data distribution facility
IDEAS	Intelligence Data Elements Authorized Standards
IDEX	imagery data exploitation system
IDF	indirect fire; intermediate distribution frame
ID/IQ	indefinite delivery/indefinite quantity
IDL	integrated distribution lane
IDM	improved data modem; information dissemination management
IDNDR	International Decade for Natural Disaster Reduction (UN)
IDO	installation deployment officer
IDP	imagery derived product; imminent danger pay; internally displaced person
IDRA	infectious disease risk assessment
IDS	individual deployment site; integrated deployment system; interface design standards; intrusion detection system
IDSRS	Integrated Defense Source Registration System
IDSS	interoperability decision support system
IDT	inactive duty training
IDZ	inner defense zone
IEB	intelligence exploitation base
IED	improvised explosive device
IEDD	improvised explosive device defeat
IEEE	Institute of Electrical and Electronics Engineers
IEL	illustrative evaluation scenario
IEM	installation emergency management
IEMATS	improved emergency message automatic transmission system
IER	information exchange requirement
IES	imagery exploitation system
IESS	imagery exploitation support system
IEW	intelligence and electronic warfare
IF	intermediate frequency
IFC	intelligence fusion center
IFCS	improved fire control system
IFF	identification, friend or foe
IFFN	identification, friend, foe, or neutral
IFF/SIF	identification, friend or foe/selective identification feature
IFO	integrated financial operations; intermediate fuel oil
IFP	integrated force package
IFR	instrument flight rules
IFRC	International Federation of Red Cross and Red Crescent Societies

IFSAR	interferometric synthetic aperture radar
IG	inspector general
IGC	Integrated Data Environment/Global Transportation Network Convergence
IGL	intelligence gain/loss
IGO	intergovernmental organization
IGSM	interim ground station module (JSTARS)
IHADSS	integrated helmet and display sight system (Army)
IHC	international humanitarian community
IHO	industrial hygiene officer
IHS	international health specialist
IIB	interagency information bureau
IICL	Institute of International Container Lessors
IICT	Interagency Intelligence Committee on Counterterrorism
IIM	intelligence information management
IIP	Bureau of International Information Programs (DOS); interagency implementation plan; international information program; interoperability improvement program
IIR	imagery interpretation report; imaging infrared; intelligence information report
IJC3S	initial joint command, control, and communications system; Integrated Joint Command, Control, and Communications System
IL	intermediate location
ILAB	Bureau of International Labor Affairs (DOL)
ILO	in lieu of; International Labor Organization (UN)
ILOC	integrated line of communications
ILS	integrated logistic support
IM	information management; intermediate module
IMA	individual mobilization augmentee
IMAAC	Interagency Modeling and Atmospheric Assessment Center
IMC	instrument meteorological conditions; International Medical Corps
IMDC	isolated, missing, detained, or captured
IMDG	international maritime dangerous goods (UN)
IMET	international military education and training
IMETS	Integrated Meteorological System
IMF	International Monetary Fund (UN)
IMI	international military information
IMINT	imagery intelligence
IMIT	international military information team
IMLTU	intermatrix line termination unit
IMM	integrated materiel management; intelligence mission management

IMMDELREQ	immediate delivery required
IMO	information management officer; International Maritime Organization
IMOSAR	International Maritime Organization (IMO) search and rescue manual
IMOSS	interim mobile oceanographic support system
IMP	implementation; information management plan; inventory management plan
IMPP	integrated mission planning process
IMPT	incident management planning team; integrated mission planning team
IMRL	individual material requirements list
IMS	information management system; interagency management system; Interagency Management System for Reconstruction and Stabilization; international military staff; international military standardization
IMSP	information management support plan
IMSU	installation medical support unit
IMTF	integrated mission task force
IMU	inertial measuring unit; intermatrix unit
IN	Air Force component intelligence officer (staff); impulse noise; instructor
INCERFA	uncertainty phase (ICAO)
INCNR	increment number
INCSEA	incidents at sea
IND	improvised nuclear device
INDRAC	Interagency Combating Weapons of Mass Destruction Database of Responsibilities, Authorities, and Capabilities
INF	infantry
INFLTREP	inflight report
INFOCON	information operations condition
INID	intercept network in dialing
INJILL	injured or ill
INL	Bureau for International Narcotics and Law Enforcement Affairs (DOS)
INLS	improved Navy lighterage system
INM	international narcotics matters
INMARSAT	international maritime satellite
INR	Bureau of Intelligence and Research (DOS)
INREQ	information request
INRP	Initial National Response Plan
INS	Immigration and Naturalization Service; inertial navigation system; insert code
INSARAG	International Search and Rescue Advisory Group
INSCOM	United States Army Intelligence and Security Command
INTAC	individual terrorism awareness course

INTACS	integrated tactical communications system
INTELSAT	International Telecommunications Satellite Organization
INTELSITSUM	intelligence situation summary
InterAction	American Council for Voluntary International Action
INTERCO	International Code of signals
INTERPOL	International Criminal Police Organization
INTERPOL-USNCB	International Criminal Police Organization, United States National Central Bureau (DOJ)
INTREP	intelligence report
INU	inertial navigation unit; integration unit
INV	invalid
INVOL	involuntary
I/O	input/output
IO	information objectives; information operations; intelligence oversight
IOB	intelligence oversight board
IOC	Industrial Operations Command; initial operational capability; intelligence operations center; investigations operations center
IOCB	information operations coordination board
IO force	information operations force
IOI	injured other than hostilities or illness
IOII	information operations intelligence integration
IOM	installation, operation, and maintenance; International Organization for Migration
IOP	interface operating procedure
IOSS	Interagency Operations Security Support Staff
IOT	information operations team
IOU	input/output unit
IOW	information operations wing
IOWG	information operations working group
IP	initial point; initial position; instructor pilot; intelligence planning; internet protocol
IPA	intelligence production agency
IPB	intelligence preparation of the battlespace
IPBD	intelligence program budget decision
IPC	initial planning conference; integration planning cell; interagency planning cell; interagency policy committee
IPDM	intelligence program decision memorandum
IPDP	inland petroleum distribution plan
IPDS	imagery processing and dissemination system; inland petroleum distribution system (Army)
IPE	individual protective equipment; industrial plant equipment
IPG	isolated personnel guidance
IPI	indigenous populations and institutions

IPL	imagery product library; integrated priority list
IPO	International Program Office
IPOE	intelligence preparation of the operational environment
IPOM	intelligence program objective memorandum
IPP	impact point prediction; industrial preparedness program
IPR	in-progress review; intelligence production requirement
IPR F	plan approval in-progress review
IPRG	intelligence program review group
IPS	illustrative planning scenario; Integrated Planning System (DHS); Interim Polar System; interoperability planning system
IPSG	intelligence program support group
IPSP	intelligence priorities for strategic planning
IPT	integrated planning team; integrated process team; Integrated Product Team; intelligence planning team
I/R	internment/resettlement
IR	incident report; information rate; information requirement; infrared; intelligence requirement
IRA	Provisional Irish Republican Army
IRAC	Interdepartment Radio Advisory Committee (DOC)
IRBM	intermediate-range ballistic missile
I/R BN	internment/resettlement battalion
IRC	information-related capability; International Red Cross; International Rescue Committee; internet relay chat
IRCCM	infrared counter countermeasures
IRCM	infrared countermeasures
IRDS	infrared detection set
IRF	Immediate Reaction Forces (NATO); incident response force
IRINT	infrared intelligence
IRISA	Intelligence Report Index Summary File
IRO	international relief organization
IR pointer	infrared pointer
IRR	Individual Ready Reserve; integrated readiness report
IRS	Internal Revenue Service
IRSCC	interagency remote sensing coordination cell
IRST	infrared search and track
IRSTS	infrared search and track sensor; Infrared Search and Track System
IRT	Initial Response Team
IRTPA	Intelligence Reform and Terrorism Prevention Act
IS	information superiority; information system; interswitch
ISA	individual Service augmentee; international standardization agreement; inter-Service agreement
ISAC	information sharing and analysis center
ISAF	International Security Assistance Force
ISB	intermediate staging base

ISDB	integrated satellite communications (SATCOM) database
ISDDC	Integrated Mission Support for Surface Deployment and Distribution Command
ISE	Information Sharing Environment ;intelligence support element
ISG	information synchronization group; isolated soldier guidance
ISI2R	identify, separate, isolate, influence, and reintegrate
ISMCS	international station meteorological climatic summary
ISMMP	integrated continental United States (CONUS) medical mobilization plan
ISN	Bureau of International Security and Nonproliferation (DOS); internment serial number
ISO	International Organization for Standardization; isolation
ISOO	Information Security Oversight Office
ISOPAK	International Organization for Standardization package
ISOPREP	isolated personnel report
ISP	internet service provider
ISR	intelligence, surveillance, and reconnaissance
ISRD	intelligence, surveillance, and reconnaissance division
ISRLO	intelligence, surveillance, and reconnaissance liaison officer (USAF)
ISR WG	Intelligence, Surveillance, and Reconnaissance Wing
ISS	in-system select
ISSA	inter-Service support agreement
ISSG	Intelligence Senior Steering Group
ISSM	information system security manager
ISSO	information systems security organization
IST	integrated system test; interswitch trunk
ISU	internal airlift or helicopter slingable container unit
I/T	interpreter and translator
IT	information system technician; information technology
ITA	international telegraphic alphabet; International Trade Administration (DOC)
ITAC	intelligence and threat analysis center (Army)
ITALD	improved tactical air-launched decoy
ITAR	international traffic in arms regulation (coassembly)
ITF	intelligence task force (DIA)
ITG	infrared target graphic
ITL	intelligence task list
ITO	installation transportation officer
ITRO	inter-Service training organization
ITU	International Telecommunications Union
ITV	in-transit visibility
ITW/AA	integrated tactical warning and attack assessment
IUWG	inshore undersea warfare group
IV	intravenous

IVR	initial voice report
IVSN	Initial Voice Switched Network
IW	irregular warfare
IWC	information operations warfare commander
IW-D	defensive information warfare
IWG	intelligence working group; interagency working group
IWSC	Information Warfare Support Center
IWW	inland waterway
IWWS	inland waterway system

Intentionally Blank

J

J-1	manpower and personnel directorate of a joint staff; manpower and personnel staff section
J-2	intelligence directorate of a joint staff; intelligence staff section
J-2A	deputy directorate for administration of a joint staff
J2-CI	Joint Counterintelligence Office
J-2E	joint force exploitation staff element
J-2J	deputy directorate for support of a joint staff
J-2M	deputy directorate for crisis management of a joint staff
J-2O	deputy directorate for crisis operations of a joint staff
J-2P	deputy directorate for assessment, doctrine, requirements, and capabilities of a joint staff
J-2T	Deputy Directorate for Targeting, Joint Staff Intelligence Directorate
J-2T-1	joint staff target operations division
J-2T-2	Target Plans Division
J-2X	joint force counterintelligence and human intelligence staff element
J-3	operations directorate of a joint staff; operations staff section
J-4	logistics directorate of a joint staff; logistics staff section
J-5	plans directorate of a joint staff; plans staff section
J-6	communications system directorate of a joint staff; command, control, communications, and computer systems staff section
J-7	engineering staff section of a joint staff; Joint Staff Directorate for Joint Force Development; operational plans and interoperability directorate of a joint staff
J-7/JED	exercises and training directorate of a joint staff
J-8	Joint Staff Directorate for Force Structure, Resource, and Assessment; force structure, resource, and assessment directorate of a joint staff
J-9	civil-military operations directorate of a joint staff; civil-military operations staff section
J-31	Joint Force Coordinator (Joint Staff)
J-35	future operations cell
J-39 DDGO	Joint Staff, Deputy Director for Global Operations
JA	judge advocate
J-A	judge advocate directorate of a joint staff
JAARS	Joint After-Action Reporting System
JAAT	joint air attack team
JA/ATT	joint airborne and air transportability training
JAC	joint analysis center
JACC	joint airspace control center
JACCC	joint airlift coordination and control cell

JACC/CP	joint airborne communications center/command post
JACCE	joint air component coordination element
JACE	joint air coordination element
JACS	joint automated communication-electronics operating instructions system
JADO	joint air defense operations
JADOC	Joint Air Defense Operations Center (NORAD)
JADOCS	Joint Automated Deep Operations Coordination System
JAFWIN	JWICS Air Force weather information network
JAG	judge advocate general
JAGIC	joint air-ground integration center
JAGMAN	Manual of the Judge Advocate General (US Navy)
JAI	joint administrative instruction; joint airdrop inspection
JAIC	joint air intelligence center
JAIEG	joint atomic information exchange group
JAMMS	Joint Asset Movement Management System
JAMPS	Joint Interoperability of Tactical Command and Control Systems (JINTACCS) automated message preparation system
JANAP	Joint Army, Navy, Air Force publication
JAO	joint air operations
JAOC	joint air operations center
JAOP	joint air operations plan
JAPO	joint area petroleum office
JAR	joint activity report
JARCC	joint air reconnaissance control center
JARN	joint air request net
JARS	joint automated readiness system
JASC	joint action steering committee
JASSM	joint air-to-surface standoff missile
JAT	joint acceptance test; joint assessment team
JATACS	joint advanced tactical cryptological support
JAT Guide	Joint Antiterrorism Program Manager's Guide
JAWS	Joint Munitions Effectiveness Manual (JMEM)/air-to-surface weaponeering system
JBP	Joint Blood Program
JBPO	joint blood program office
JC2WC	joint command and control warfare center
JCA	jamming control authority; joint capability area
JCASO	Joint Contingency Acquisition Support Office (DLA)
JCASREP	joint casualty report
JCAT	joint crisis action team
JCC	joint collaboration cell; joint command center; joint contracting center; joint course catalog; joint cyberspace center
JCCA	joint combat capability assessment

JCCB	Joint Configuration Control Board
JCCC	Joint Combat Camera Center; joint communications control center
JCCP	joint casualty collection point
JCCSE	Joint Continental United States Communications Support Environment
JCE	Joint Intelligence Virtual Architecture (JIVA) Collaborative Environment
JCEOI	joint communications-electronics operating instructions
JCET	joint combined exchange training; joint combined exercise for training
JCEWR	joint coordination of electronic warfare reprogramming
JCEWS	joint force commander's electronic warfare staff
JCGRO	joint central graves registration office
JCIDO	Joint Combat Identification Office
JCIOC	joint counterintelligence operations center
JCISA	Joint Command Information Systems Activity
JCISB	Joint Counterintelligence Support Branch
JCIU	joint counterintelligence unit
JCLL	joint center for lessons learned
JCMA	joint communications security monitoring activity
JCMB	joint collection management board
JCMC	joint crisis management capability
JCMEB	joint civil-military engineering board
JCMEC	Joint Captured Materiel Exploitation Center (DIA)
JCMO	joint communications security management office
JCMOTF	joint civil-military operations task force
JCMPO	Joint Cruise Missile Project Office
JCMS	Joint Construction Management System
JCMT	joint collection management tools
JCN	joint communications network; joint communications node
JCRM	Joint Capabilities Requirements Manager
JCS	Joint Chiefs of Staff
JCSAN	Joint Chiefs of Staff Alerting Network
JCSAR	joint combat search and rescue
JCSB	joint contracting support board
JCSC	joint communications satellite center
JCSE	joint communications support element; Joint Communications Support Element (USTRANSCOM)
JCSM	Joint Chiefs of Staff memorandum
JCSP	joint contracting support plan
JCSS	joint communications support squadron
JCTN	joint composite track network
JDA	joint duty assignment
JDAAP	Joint Doctrine Awareness Action Plan

JDAL	Joint Duty Assignment List
JDAM	Joint Direct Attack Munition
JDAMIS	Joint Duty Assignment Management Information System
JDAT	joint deployable analysis team
JDC	joint deployment community; Joint Doctrine Center
JDD	joint doctrine distribution
JDDC	joint doctrine development community
JDDE	joint deployment and distribution enterprise
JDDOC	joint deployment and distribution operations center
JDDT	joint doctrine development tool
JDEC	joint document exploitation center
JDEIS	Joint Doctrine, Education, and Training Electronic Information System
JDIG	Joint Drug Intelligence Group
JDIGS	Joint Digital Information Gathering System
JDISS	joint deployable intelligence support system
JDN	joint data network; joint doctrine note
JDNC	joint data network operations cell
JDNO	joint data network operations officer
JDOG	joint detention operations group
JDOMS	Joint Director of Military Support
JDPC	Joint Doctrine Planning Conference
JDPI	joint desired point of impact
JDPO	joint deployment process owner
JDSS	Joint Decision Support System
JDSSC	Joint Data Systems Support Center
JDTC	Joint Deployment Training Center
JE	joint experimentation
JEAP	Joint Electronic Intelligence (ELINT) Analysis Program
JECC	Joint Enabling Capabilities Command (USTRANSCOM)
JECE	Joint Elimination Coordination Element
JECG	joint exercise control group
JECPO	Joint Electronic Commerce Program Office
JED	Joint Education and Doctrine
JEDD	Joint Education and Doctrine Division
JEEP	joint emergency evacuation plan
JEFF	Joint Expeditionary Forensic Facility (Army)
JEL	Joint Electronic Library
JEL+	Joint Electronic Library Plus
JEM	joint exercise manual
JEMB	joint environmental management board
JEMP	joint exercise management package
JEMSMO	joint electromagnetic spectrum management operations
JEMSO	joint electromagnetic spectrum operations
JENM	joint enterprise network manager
JEP	Joint Exercise Program

JEPES	Joint Engineer Planning and Execution System
JET	joint expeditionary team; Joint Operation Planning and Execution System editing tool
JEWC	Joint Electronic Warfare Center
JEWCS	Joint Electronic Warfare Core Staff (NATO)
JEZ	joint engagement zone
JFA	joint field activity
JFACC	joint force air component commander
JFAST	Joint Flow and Analysis System for Transportation
JFC	joint force commander
JFCC	joint functional component command
JFCC-GS	Joint Functional Component Command for Global Strike
JFCC-IMD	Joint Functional Component Command for Integrated Missile Defense
JFCC-ISR	Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance (USSTRATCOM)
JFCC NW	Joint Functional Component Command for Network Warfare
JFCC-Space	Joint Functional Component Command for Space (USSTRATCOM)
JFCH	joint force chaplain
JFE	joint fires element
JFHQ	joint force headquarters
JFHQ–NCR	Joint Force Headquarters-National Capital Region
JFHQ–State	joint force headquarters-state
JFIIT	Joint Fires Integration and Interoperability Team
JFIP	Japanese facilities improvement project
JFLCC	joint force land component commander
JFMC	joint fleet mail center
JFMCC	joint force maritime component commander
JFMO	joint frequency management office
JFO	joint field office; joint fires observer
JFP	joint force package (packaging); joint force provider; Joint Frequency Panel (MCEB)
JFRB	Joint Foreign Release Board
JFRG	joint force requirements generator
JFRG II	joint force requirements generator II
JFS	joint force surgeon
JFSOC	joint force special operations component
JFSOCC	joint force special operations component commander
JFTR	joint Federal travel regulations
JFUB	joint facilities utilization board
JGWE	joint global warning enterprise
JHMCS	joint helmet-mounted cueing system
JHNS	Joint Hometown News Service
JHSV	joint high-speed vessel

JI	joint inspection
JIA	joint individual augmentation; joint individual augmentee
JIACG	joint interagency coordination group
JIADS	joint integrated air defense system
JIATF	joint interagency task force
JIATF-E	joint interagency task force - East
JIATF-S	Joint Interagency Task Force-South
JIATF-W	Joint Interagency Task Force-West
JIC	joint information center
JICC	joint information coordination center; joint interface control cell
JICO	joint interface control officer
JICPAC	Joint Intelligence Center, Pacific
JICTRANS	Joint Intelligence Center for Transportation
JIDC	joint intelligence and debriefing center; joint interrogation and debriefing center
JIEDDO	Joint Improvised Explosive Device Defeat Organization
JIEE	Joint Information Exchange Environment
JIEO	joint interoperability engineering organization
JIEP	joint intelligence estimate for planning
JIES	joint interoperability evaluation system
JIG	joint interrogation group
JILE	joint intelligence liaison element
JIMB	joint information management board
JIMP	joint implementation master plan
JIMPP	joint industrial mobilization planning process
JIMS	joint information management system
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JIO	joint interrogation operations
JIOC	joint information operations center; joint intelligence operations center
JIOCPAC	Joint Intelligence Operations Center, Pacific
JIOC-SOUTH	Joint Intelligence Operations Center, South
JIOC-TRANS	Joint Intelligence Operations Center–Transportation (USTRANSCOM)
JIOP	joint interface operational procedures
JIOP-MTF	joint interface operating procedures-message text formats
JIOWC	Joint Information Operations Warfare Center
JIPC	joint imagery production complex
JIPCL	joint integrated prioritized collection list
JIPOE	joint intelligence preparation of the operational environment
JIPTL	joint integrated prioritized target list
JIS	joint information system
JISE	joint intelligence support element
JITC	joint interoperability test command

JITF-CT	Joint Intelligence Task Force for Combating Terrorism
JIVA	Joint Intelligence Virtual Architecture
JIVU	Joint Intelligence Virtual University
JKDDC	Joint Knowledge Development and Distribution Capability
JKnIFE	Joint Improvised Explosive Device Defeat Organization Knowledge and Information Fusion Exchange
JLCC	joint lighterage control center; joint logistics coordination center
JLE	joint logistics environment
JLEnt	joint logistics enterprise
JLLIS	Joint Lessons Learned Information System
JLLP	Joint Lessons Learned Program
JLNCHREP	joint launch report
JLOA	joint logistics over-the-shore operation area
JLOC	joint logistics operations center
JLOTS	joint logistics over-the-shore
JLRC	joint logistics readiness center
JLSB	joint line of communications security board
JLSE	joint legal support element
JM&S	joint modeling and simulation
JMAARS	joint model after-action review system
JMAC	Joint Mortuary Affairs Center (Army)
JMAG	Joint METOC Advisory Group
JMAO	joint mortuary affairs office; joint mortuary affairs officer
JMAR	joint medical asset repository
JMAS	joint manpower automation system
JMAT	joint medical analysis tool; joint mobility assistance team
JMB	joint meteorology and oceanography board
JMC	joint military command; joint movement center
JMCC	joint meteorological and oceanographic coordination cell
JMCG	joint movement control group
JMCIS	Joint Maritime Command Information System
JMCO	joint meteorological and oceanographic coordination organization
JMCOMS	joint maritime communications system
JMD	joint manning document
JMeDSAF	joint medical semi-automated forces
JMEEL	joint mission-essential equipment list
JMEM	Joint Munitions Effectiveness Manual
JMET	joint mission-essential task
JMETL	joint mission-essential task list
JMIC	Joint Military Intelligence College; joint modular intermodal container
JMICS	Joint Worldwide Intelligence Communications System mobile integrated communications system
JMIE	joint maritime information element

JMIP	joint military intelligence program
JMISC	Joint Military Information Support Command
JMISTF	joint military information support task force
JMITC	Joint Military Intelligence Training Center
JMLO	joint medical logistics officer
JMMC	Joint Material Management Center
JMMT	joint military mail terminal
JMNA	joint military net assessment
JMO	joint maritime operations; joint meteorological and oceanographic officer; joint munitions office
JMO(AIR)	joint maritime operations (air)
JMOC	joint medical operations center
JMP	joint manpower program
JMPA	joint military postal activity; joint military satellite communications (MILSATCOM) panel administrator
JMPAB	Joint Materiel Priorities and Allocation Board
JMPS	Joint Mission Planning System
JMPT	Joint Medical Planning Tool
JMRC	joint mobile relay center
JMRO	Joint Medical Regulating Office
JMRR	Joint Monthly Readiness Review
JMSEP	joint modeling and simulation executive panel
JMSWG	Joint Multi-Tactical Digital Information Link (Multi-TADIL) Standards Working Group
JMT	joint military training
JMTCA	joint munitions transportation coordinating activity
JMTCSS	Joint Maritime Tactical Communications Switching System
JMTG	joint military information support operations task group
JMUA	Joint Meritorious Unit Award
JMV	joint METOC viewer
JMWG	joint medical working group
JNCC	joint network operations control center
JNMS	joint network management system
JNOCC	Joint Operation Planning and Execution System (JOPES) Network Operation Control Center
JNPE	joint nuclear planning element
JNSC	Joint Navigation Warfare Center Navigation Warfare Support Cell
JNWC	Joint Navigation Warfare Center
JOA	joint operations area
JOAF	joint operations area forecast
JOC	joint operations center; joint oversight committee
JOCC	joint operations command center
JOERAD	joint spectrum center ordnance electromagnetic environmental effects risk assessment database

JOG	joint operations graphic
JOGS	joint operation graphics system
JOPES	Joint Operation Planning and Execution System
JOPESIR	Joint Operation Planning and Execution System Incident Reporting System
JOPESREP	Joint Operation Planning and Execution System Reporting System
JOPG	joint operations planning group
JOPP	joint operation planning process
JOPPA	joint operation planning process for air
JOR	joint operational requirement
JORD	joint operational requirements document
JOSE	Joint Operations Security Support Element (Joint Staff)
JOSG	joint operational steering group
JOT&E	joint operational test and evaluation
JOTC	joint operations tasking center
JOTS	Joint Operational Tactical System
JP	joint publication
JP4	jet propulsion fuel, type 4
JP5	jet propulsion fuel, type 5
JP8	jet propulsion fuel, type 8
JPAC	joint planning augmentation cell; Joint POW/MIA Accounting Command
JPADS	joint precision airdrop system
JPAG	Joint Planning Advisory Group
JPARR	joint personnel accountability reconciliation and reporting
JPASE	joint public affairs support element; Joint Public Affairs Support Element (USTRANSCOM)
JPATS	joint primary aircraft training system
JPAV	joint personnel asset visibility
JPC	joint planning cell; joint postal cell
JPD	joint planning document
JPEC	joint planning and execution community
JPED	joint personal effects depot
JPEG	Joint Photographic Experts Group
JPERSTAT	joint personnel status and casualty report
JPG	joint planning group
JPME	joint professional military education
JPMRC	joint patient movement requirements center
JPMT	joint patient movement team
JPN	joint planning network
JPO	joint petroleum office; Joint Program Office
JPOC	joint personnel operations center; joint planning orientation course
JPOI	joint program of instruction
JPOM	joint preparation and onward movement

JPO-STC	Joint Program Office for Special Technology Countermeasures
JPRA	Joint Personnel Recovery Agency
JPRC	joint personnel reception center; joint personnel recovery center
JPS	joint processing system
JPSE	Joint Planning Support Element (USTRANSCOM)
JPTTA	joint personnel training and tracking activity
JQR	joint qualification requirements
JQRR	joint quarterly readiness review
JRADS	Joint Resource Assessment Data System
JRB	Joint Requirements Oversight Council (JROC) Review Board
JRC	joint reconnaissance center
JRCC	joint reception coordination center
JRERP	Joint Radiological Emergency Response Plan
JRFL	joint restricted frequency list
JRG	joint review group
JRIC	joint reserve intelligence center
JRIP	Joint Reserve Intelligence Program
JRMB	Joint Requirements and Management Board
JROC	Joint Requirements Oversight Council
JRRB	joint requirements review board
JRS	joint reporting structure
JRSC	jam-resistant secure communications; joint rescue sub-center
JRSOI	joint reception, staging, onward movement, and integration
JRTC	joint readiness training center
JRX	joint readiness exercise
JS	Joint Staff; the Joint Staff
JSA	joint security area
JSAC	joint strike analysis cell; joint strike analysis center
JSAM	joint security assistance memorandum; Joint Service Achievement Medal; joint standoff surface attack missile
JSAN	Joint Staff automation for the nineties
JSAP	Joint Staff action package; Joint Staff action processing
JSAS	joint strike analysis system
JSC	joint security coordinator; Joint Spectrum Center
JSCAT	joint staff crisis action team
JSCC	joint security coordination center; joint Services coordination committee
JSCM	Joint Service Commendation Medal
JSCP	Joint Strategic Capabilities Plan
JSDS	Joint Staff doctrine sponsor
JSEC	joint strategic exploitation center
JSETS	Joint Search and Rescue Satellite-Aided Tracking

	Electronic Tracking System
JSF	joint support force
JSHO	joint shipboard helicopter operations
JSIDS	joint Services imagery digitizing system
JSIR	joint spectrum interference resolution
JSISC	Joint Staff Information Service Center
JSIT	Joint Operation Planning and Execution System (JOPES) information trace
JSIVA	Joint Staff Integrated Vulnerability Assessment
JSM	Joint Staff Manual
JSME	joint spectrum management element
JSMS	joint spectrum management system
JSO	joint security operations
JSOA	joint special operations area
JSOAC	joint special operations air component; joint special operations aviation component
JSOACC	joint special operations air component commander
JSOC	joint special operations command
JSOFI	Joint Special Operations Forces Institute
JSOTF	joint special operations task force
JSOU	Joint Special Operations University
JSOW	joint stand-off weapon
JSPA	joint satellite communications panel administrator
JSPD	joint strategic planning document
JSPDSA	joint strategic planning document supporting analyses
JSPOC	Joint Space Operations Center
JSPS	Joint Strategic Planning System
JSR	joint strategy review
JSRC	joint subregional command (NATO)
JSS	joint surveillance system
JSSA	joint Services survival, evasion, resistance, and escape (SERE) agency
JSSIS	joint staff support information system
JSST	joint space support team
JSTAR	joint system threat assessment report
JSTARS	Joint Surveillance Target Attack Radar System
JSTE	joint system training exercise
JSTO	joint space tasking order
JT&E	joint test and evaluation
JTA	joint technical architecture
JTAC	joint terminal attack controller; Joint Terrorism Analysis Center
JTACE	joint technical advisory chemical, biological, radiological, and nuclear element
JTADS	Joint Tactical Air Defense System (Army); Joint Tactical

	Display System
JTAGS	joint tactical ground station (Army); joint tactical ground station (Army and Navy); joint tactical ground system
JTAIC	Joint Technical Analysis and Integration Cell (Army)
JTAO	joint tactical air operations
JTAR	joint tactical air strike request
JTASC	joint training analysis and simulation center
JTASG	Joint Targeting Automation Steering Group
JTAV-IT	joint total asset visibility-in theater
JTB	Joint Transportation Board
JTC	joint technical committee; Joint Training Confederation
JTCB	joint targeting coordination board
JTCC	joint transportation coordination cell; joint transportation coordination center; joint transportation corporate information management center
JTCOIC	Joint Training Counter-Improvised Explosive Device Operations Integration Center
JTD	joint table of distribution; joint theater distribution
JTDC	joint track data coordinator
JTF	joint task force
JTF-6	joint task force-6
JTF-AK	Joint Task Force-Alaska
JTF-B	joint task force-Bravo
JTFCEM	joint task force contingency engineering management
JTF-CM	joint task force - consequence management
JTF-CS	Joint Task Force-Civil Support
JTF-E	joint task force - elimination
JTF-GNO	Joint Task Force-Global Network Operations
JTF-GTMO	Joint Task Force-Guantanamo
JTF-HD	Joint Task Force-Homeland Defense
JTF HQ	joint task force headquarters
JTF-MAO	joint task force - mortuary affairs office
JTF-N	Joint Task Force-North
JTFP	Joint Tactical Fusion Program
JTF-PO	joint task force-port opening
JTFS	joint task force surgeon
JTF-State	joint task force-state
JTIC	joint transportation intelligence center
JTIDS	Joint Tactical Information Distribution System
JTL	joint target list
JTLM	joint theater logistics management
JTLS	joint theater-level simulation
JTM	joint training manual
JTMD	joint table of mobilization and distribution; Joint Terminology Master Database
JTMP	joint training master plan

JTMS	joint theater movement staff; joint training master schedule
JTP	joint test publication; joint training plan
JTR	Joint Travel Regulations
JTRB	joint telecommunication resources board
JTS	Joint Targeting School; Joint Training System
JTSCC	joint theater support contracting command
JTSSCCB	Joint Tactical Switched Systems Configuration Control Board
JTSST	joint training system support team
JTT	joint targeting toolbox; joint training team
JTTF	joint terrorism task force
JTWG	joint targeting working group
JU	Joint Tactical Information Distribution System unit
JUH-MTF	Joint User Handbook-Message Text Formats
JUIC	joint unit identification code
JUO	joint urban operation
JUON	joint urgent operational need
JUSMAG	Joint United States Military Advisory Group
JUWTF	joint unconventional warfare task force
JV	Joint Vision
JV 2020	Joint Vision 2020
JVB	joint visitors bureau
JVIDS	Joint Visual Integrated Display System
JVSEAS	Joint Virtual Security Environment Assessment System
JWAC	Joint Warfare Analysis Center
JWARS	Joint Warfare Analysis and Requirements System
JWC	Joint Warfare Center
JWFC	Joint Warfighting Center
JWG	joint working group
JWICS	Joint Worldwide Intelligence Communications System
JWID	joint warrior interoperability demonstration

Intentionally Blank

K

k	thousand
Ka	Kurtz-above band
KAL	key assets list
KAPP	Key Assets Protection Program
kb	kilobit
kbps	kilobits per second
KC-135	Stratotanker
KEK	key encryption key
KG	key generator
kg	kilogram
kHz	kilohertz
K-Kill	catastrophic kill
KLE	key leader engagement
KLIP	key doctrine element-linked information package
km	kilometer
KMC	knowledge management center
KNP	Korean National Police
KP	key pulse
kph	kilometers per hour
KPP	key performance parameter
KQ ID	tactical location identifier
kt	kiloton(s); knot (nautical miles per hour)
Ku	Kurtz-under band
kVA	kilo Volt-Amps
KVG	key variable generator
kW	kilowatt
KWOC	keyword-out-of-context

Intentionally Blank

L

L	length
l	search subarea length
LA	lead agent; legal adviser; line amplifier; loop key generator (LKG) adapter
LAADS	low altitude air defense system
LAAM	light anti-aircraft missile
LABS	laser airborne bathymetry system
LACV	lighter, air cushioned vehicle
LAD	latest arrival date; launch area denied
LAMPS	Light Airborne Multipurpose System (helicopter)
LAN	local area network
LANDCENT	Allied Land Forces Central Europe (NATO)
LANDSAT	land satellite
LANDSOUTH	Allied Land Forces Southern Europe (NATO)
LANTIRN	low-altitude navigation and targeting infrared for night
LAO	limited attack option
LARC	lighter, amphibious resupply, cargo
LARC-V	lighter, amphibious resupply, cargo, 5 ton
LARS	lightweight airborne recovery system
LASH	lighter aboard ship
LAT	latitude
LAV	light armored vehicle
lb	pound
lbs.	pounds
LBR	Laser Beam Rider
LC	lake current; legal counsel
LCAC	landing craft, air cushion
LCADS	low-cost aerial delivery system
LCAP	low combat air patrol
LCB	line of constant bearing
LCC	amphibious command ship; land component commander; launch control center; lighterage control center; link communications circuit; logistics component command
LCCS	landing craft control ship
LCE	logistics capability estimator; logistics combat element (USMC)
LCES	line conditioning equipment scanner
LCM	landing craft, mechanized; letter-class mail; life-cycle management
LCMC	life cycle management command
LCO	landing craft air cushion control officer; lighterage control officer
LCP	lighterage control point
LCPL	landing craft, personnel, light

LCS	landing craft air cushion control ship
LCSR	life cycle systems readiness
LCU	landing craft, utility; launch correlation unit
LCVP	landing craft, vehicle, personnel
LD	line of departure
LDA	limited depository account
LDF	lightweight digital facsimile
LDI	line driver interface
LDO	laser designator operator
LDR	leader; low data rate
LE	law enforcement; low-order explosives
LEA	law enforcement agency
LEAP	Light ExoAtmospheric Projectile
LEASAT	leased satellite
LEAU	Law Enforcement Assistance Unit (FAA)
LEC	lead environmental component
LECIC	Law Enforcement and Counterintelligence Center (DOD)
LED	law enforcement desk; light emitting diode
LEDET	law enforcement detachment (USCG)
LEGAT	legal attaché
LEIP	Law Enforcement Intelligence Program (USCG)
LEMP	low-altitude electromagnetic pulse
LEO	law enforcement operations; low Earth orbit
LEP	laser eye protection; law enforcement professional; linear error probable
LERSM	lower echelon reporting and surveillance module
LERTCON	alert condition
LES	law enforcement sensitive; leave and earnings statement; Lincoln Laboratories Experimental Satellite
LESO	Law Enforcement Support Office
LET	light equipment transport
L-EWE	land-electronic warfare element
LF	landing force; low frequency
LFA	lead federal agency
LFOC	landing force operations center
LFORM	landing force operational reserve material
LFSP	landing force support party
LfV	*Landesamt für Verfassungsschutz* (regional authority for constitutional protection)
LG	deputy chief of staff for logistics
LGB	laser-guided bomb
LGM	laser-guided missile; loop group multiplexer
LGM-30	Minuteman
LGW	laser-guided weapon
LHA	amphibious assault ship (general purpose)
LHD	amphibious assault ship (multipurpose)

LHT	line-haul tractor
LIDAR	light detection and ranging
LIF	light interference filter
LIMDIS	limited distribution
LIMFAC	limiting factor
LIPS	Logistics Information Processing System
LIS	logistics information system
LIWA	land information warfare activity
LJDAM	laser-guided joint direct attack munition
LKG	loop key generator
LKP	last known position
LL	lessons learned
LLLGB	low-level laser-guided bomb
LLLTV	low-light level television
LLSO	low-level source operation
LLTR	low-level transit route
LM	loop modem
LMARS	Logistics Metrics Analysis Reporting System
LMAV	laser MAVERICK
LMF	language media format
LMSR	large, medium-speed roll-on/roll-off
LN	lead nation; local national
LNA	low voice amplifier
LNI	Library of National Intelligence
LNO	liaison officer
LO	low observable
LOA	Lead Operational Authority; letter of assist; letter of authorization; letter of offer and acceptance; lodgment operational area; logistics over-the-shore operation area
LOAC	law of armed conflict
LOAL	lock-on after launch
LOBL	lock-on before launch
LOC	line of communications; logistics operations center
LOC ACC	location accuracy
LOCAP	low combat air patrol
LOCE	Linked Operational Intelligence Centers Europe; Linked Operations-Intelligence Centers Europe
LOD	line of departure
LOE	letter of evaluation; line of effort
LOG	logistics
LOGAIR	logistics aircraft
LOGAIS	logistics automated information system
LOGCAP	logistics civil augmentation program (Army)
LOGCAT	logistics capability assessment tool
LOGDET	logistics detail

LOGEX	logistics exercise
LOGFAC	Logistics Feasibility Assessment Capability
LOGFOR	logistics force packaging system
LOGMARS	logistics applications of automated marking and reading symbols
LOGMOD	logistics module
LOGPLAN	logistics planning system
LOGSAFE	logistic sustainment analysis and feasibility estimator
LOI	letter of instruction; loss of input
LO/LO	lift-on/lift-off
LOMEZ	low-altitude missile engagement zone
LONG	longitude
LOO	line of operation
LOP	line of position
LORAN	long-range aid to navigation
LO/RO	lift-on/roll-off
LOROP	long range oblique photography
LOS	line of sight
LOTS	logistics over-the-shore
LOX	liquid oxygen
LP	listening post
LPD	amphibious transport dock; low probability of detection
LPH	amphibious assault ship, landing platform helicopter
LPI	low probability of intercept
LPSB	logistics procurement support board
LPU	line printer unit
LPV	laser-protective visor
LRC	logistics readiness center
LRD	laser range finder-detector
LRF	laser range finder
LRF/D	laser range finder/detector
LRG	long-range aircraft
LRM	low rate multiplexer
LRN	Laboratory Response Network (DHHS)
LRO	lighterage repair officer
LRP	load and roll pallet
LRRP	long range reconnaissance patrol
LRS	launch and recovery site
LRST	long-range surveillance team
LRSU	long-range surveillance unit
LRT	logistics response time
LSA	logistic support analysis; logistics supportability analysis
LSB	landing support battalion; lower sideband
LSC	lead Service for contracting
LSCC	lead Service for contracting coordination
LSCDM	low speed cable driver modem

LSD	dock landing ship; least significant digit
LSE	landing signalman enlisted; logistic support element
LSO	landing safety officer; landing signals officer
LSPR	low speed pulse restorer
LSS	laser spot search; local sensor subsystem; logistics support system
LST	laser spot tracker; tank landing ship
LSU	logistics civil augmentation program support unit
LSV	logistics support vessel
LT	large tug; local terminal; long ton
L/T	long ton
LTD	laser target designator
LTD/R	laser target designator/ranger
LTF	logistics task force
LTG	local timing generator
LTIOV	latest time information is of value
LTL	laser-to-target line
LTON	long ton
LTS	low-altitude navigation and targeting infrared for night (LANTIRN) targeting system
LTT	loss to theater
LTU	line termination unit
LUT	local user terminal
LVS	Logistics Vehicle System (USMC)
LW	leeway
LWR	Lutheran World Relief
LZ	landing zone
LZCO	landing zone control officer

Intentionally Blank

M

M	million
M&E	monitoring and evaluation
M&S	modeling and simulation
M88A1	recovery vehicle
MA	medical attendant; military action; mortuary affairs
mA	milliampere(s)
MAAG	military assistance advisory group
MAAP	master air attack plan
MAC	mobility assault company; Mortuary Affairs Center
MACB	multinational acquisition and contracting board
MACCS	Marine air command and control system
MACG	Marine air control group
MACOM	major command (Army)
MACP	mortuary affairs collection point
MACRMS	mortuary affairs contaminated remains mitigation site
MACS	Marine air control squadron
MACSAT	multiple access commercial satellite
MAD	*Militärischer Abschirmdienst* (military protection service); military air distress
MADCP	mortuary affairs decontamination collection point
MADS	military information support operations automated data system
MAEB	mean area of effectiveness for blast
MAEF	mean area of effectiveness for fragments
MAF	mobility air forces
MAFC	Marine air-ground task force (MAGTF) all-source fusion center
MAG	Marine aircraft group; maritime assessment group; military assignment group
MAGTF	Marine air-ground task force
MAGTF ACE	Marine air-ground task force aviation combat element
MAJCOM	major command (USAF)
MANFOR	manpower force packaging system
MANPADS	man-portable air defense system
MANPER	manpower and personnel module
MAOC-N	Maritime Analysis and Operations Center-Narcotics
MAP	Military Assistance Program; missed approach point; missed approach procedure
MAR	METOC assistance request
MARAD	Maritime Administration
MARAD RRF	Maritime Administration Ready Reserve Force
MARCORLOGCOM	Marine Corps Logistics Command
MARCORMATCOM	Marine Corps Materiel Command

MARCORSYSCOM	Marine Corps Systems Command
MARDIV	Marine division
MARFOR	Marine Corps forces
MARFOREUR	Marine Corps Forces, Europe
MARFORLANT	Marine Corps Forces, Atlantic
MARFORNORTH	Marine Corps Forces, North
MARFORPAC	Marine Corps Forces, Pacific
MARFORSOUTH	Marine Corps Forces, South
MARFORSTRAT	United States Marine Corps Forces, United States Strategic Command
MARINCEN	Maritime Intelligence Center
Marine TACC	Marine Corps tactical air command center
MARLE	Marine liaison element
MARLO	Marine liaison officer
MARO	mass atrocity response operations
MAROP	marine operators
MARPOL	International Convention for the Prevention of Pollution from Ships
MARS	Military Auxiliary Radio System
MARSA	military assumes responsibility for separation of aircraft
MARSOC	United States Marine Corps Forces, Special Operations Command
MARSOF	Marine Corps special operations forces
MART	mobile Automatic Digital Network (AUTODIN) remote terminal
MARTS	Mortuary Affairs Reporting and Tracking System
MAS	maritime air support; military information support operations automated system
MASCAL	mass casualty
MASF	mobile aeromedical staging facility
MASH	mobile Army surgical hospital
MASINT	measurement and signature intelligence
MASLO	measurement and signature intelligence liaison officer
MAST	military assistance to safety and traffic; mobile ashore support terminal
MAT	medical analysis tool
MATCALS	Marine air traffic control and landing system
MATCS	Marine air traffic control squadron
M/ATMP	Missiles/Air Target Materials Program
MAW	Marine aircraft wing
MAX	maximum
MAXORD	maximum ordinate
MB	medium boat; megabyte; military information support operations battalion
MBBLs	thousands of barrels
MBCDM	medical biological chemical defense materiel

MBI	major budget issue
Mbps	megabytes per second
Mbs	megabits per second
MC	Military Committee (NATO); military community; mission-critical
MC-130	Combat Talon (I and II)
MC4EB	Military Command, Control, Communications and Computers Executive Board
MCA	mail control activity; maximum calling area; military civic action; mission concept approval; movement control agency
MCAG	maritime civil affairs group
MCAP	maximum calling area precedence
MCAS	Marine Corps air station
MCAST	maritime civil affairs and security training
MCAT	maritime civil affairs team
MCB	movement control battalion
MCBAT	medical chemical biological advisory team
MCC	Marine component commander; maritime component commander; master control center; military cooperation committee; military coordinating committee; military counterintelligence collections; mission control center; mobility control center; movement control center
MCCC	mobile consolidated command center
MCCDC	Marine Corps Combat Development Command
MCCISWG	military command, control, and information systems working group
MCD	medical crew director
MCDA	military and civil defense assets (UN)
MCDP	Marine Corps doctrine publication
MCDS	modular cargo delivery system
MCEB	Military Communications-Electronics Board
MCESG	Marine Corps Embassy Security Group
MCEWG	Military Communications-Electronics Working Group
MC/FI	mass casualty/fatality incident
MCI	multinational communications integration
MCIA	Marine Corps Intelligence Activity
MCIO	military criminal investigative organization
MCIOC	Marine Corps Information Operations Center
MCIP	Marine Corps interim publication; military command inspection program; military customs inspection program
MCJSB	Military Committee Joint Standardization Board
MCM	maneuver control measure; Manual for Courts-Martial; military classification manual; mine countermeasures
MCMC	mine countermeasures commander

MCMG	Military Committee Meteorological Group (NATO)
MCMO	medical civil-military operations
MCMOPS	mine countermeasures operations
M/CM/S	mobility, countermobility, and/or survivability
MCMREP	mine countermeasure report
MCMRON	mine countermeasures squadron
MCO	major combat operation; Mapping Customer Operations (Defense Logistics Agency); Marine Corps order
MCOO	modified combined obstacle overlay
MCRP	Marine Corps reference publication
MCS	maneuver control system; Military Capabilities Study; mine countermeasures ship; modular causeway system
MCSB	Marine Cryptologic Support Battalion
MCSF	mobile cryptologic support facility
MCSFB	Marine Corps security force battalion
MCSFR	Marine Corps Security Force Regiment
MCT	movement control team
MCTC	Midwest Counterdrug Training Center
MCTFT	Multijurisdictional Counterdrug Task Force Training
MCTOG	Marine Corps Tactics and Operations Group
MCU	maintenance communications unit
MCW	modulated carrier wave
MCWL	Marine Corps Warfighting Lab
MCWP	Marine Corps warfighting publication
MCX	Marine Corps Exchange
MDA	Magen David Adom (Israeli equivalent of the Red Cross); maritime domain awareness; Missile Defense Agency
M-DARC	military direct access radar channel
MDBS	blood support medical detachment
MDCI	multidiscipline counterintelligence
MDCO	Military Department counterintelligence organization
MDDOC	Marine air-ground task force deployment and distribution operations center
MDF	Main Defense Forces (NATO); main distribution frame
MDITDS	migration defense intelligence threat data system; Modernized Defense Intelligence Threat Data System
MDM	maritime defense measure
MDMA	methylenedioxymethamphetamine
MDR	medium data rate
MDRO	mission disaster response officer
MDS	Message Dissemination Subsystem; mission design series
MDSS II	Marine air-ground task force Deployment Support System II
MDSU	mobile diving and salvage unit
MDU	military information support operations distribution unit

MDW	Military District of Washington
MDZ	maritime defense zone
MEA	munitions effect assessment; munitions effectiveness assessment
MEAS	military information support operations effects analysis subsystem
MEB	maneuver enhancement brigade; Marine expeditionary brigade
MEBU	mission essential backup
MEC	medium endurance cutter
ME/C	medical examiner and/or coroner
MED	manipulative electronic deception
MEDAL	Mine Warfare Environmental Decision Aids Library
MEDCAP	medical civic action program
MEDCC	medical coordination cell
MEDCOM	medical command; US Army Medical Command
MEDCOM (DS)	medical command (deployment support) (Army)
MEDEVAC	medical evacuation
MEDINT	medical intelligence
MEDLOG	medical logistics (USAF AIS)
MEDLOGCO	medical logistics company
MEDLOG JR	medical logistics, junior (USAF)
MEDLOG support	medical logistics support
MEDMOB	Medical Mobilization Planning and Execution System
MEDNEO	medical noncombatant evacuation operation
MEDREG	medical regulating
MEDREGREP	medical regulating report
MEDRETE	medical readiness training exercise
MEDS	meteorological data system
MEDSOM	medical supply, optical, and maintenance unit
MEDSTAT	medical status
MEF	Marine expeditionary force
MEFPAKA	manpower and equipment force packaging
MEJA	Military Extraterritorial Jurisdiction Act
MEL	maintenance expenditure limit; minimum equipment list
MEO	medium Earth orbit; military equal opportunity
MEP	mobile electric power
MEPCOM	military entrance processing command
MEPES	Medical Planning and Execution System
MEPRS	Military Entrance Processing and Reporting System
MERCO	merchant ship reporting and control
MERSHIPS	merchant ships
MES	medical equipment set
MESAR	minimum-essential security assistance requirements
MESF	maritime expeditionary security force
MESFC	maritime expeditionary security force commander

MESO	maritime expeditionary security operations
MET	medium equipment transporter; mobile environmental team
METAR	meteorological airfield report; meteorological aviation report
METARS	routine aviation weather report (roughly translated from French; international standard code format for hourly surface weather observations)
METCON	control of meteorological information (roughly translated from French); meteorological control (Navy)
METL	mission-essential task list
METMF	meteorological mobile facility
METMR(R)	meteorological mobile facility (replacement)
METOC	meteorological and oceanographic
METSAT	meteorological satellite
METT-T	mission, enemy, terrain and weather, troops and support available-time available
METT-TC	mission, enemy, terrain and weather, troops and support available-time available and civil considerations (Army)
METWATCH	meteorological watch
MEU	Marine expeditionary unit
MEVA	mission essential vulnerable area
MEWSG	Multi-Service Electronic Warfare Support Group (NATO)
MEZ	missile engagement zone
MF	medium frequency; mobile facility; multi-frequency
MFC	multinational force commander
MFDS	Modular Fuel Delivery System
MFE	manpower force element; mobile field exchange
MFFIMS	mass fatality field information management system
MFO	multinational force and observers
MFP	major force program
MFPC	maritime future plans center
MFPF	minefield planning folder
MFS	multifunction switch
MG	military information support operations group
MGB	medium girder bridge
MGM	master group multiplexer
MGRS	military grid reference system
MGS	mobile ground system
MGT	management
MGW	maximum gross weight
MHC	management headquarters ceiling
MHD	maritime homeland defense
MHE	materials handling equipment
MHS	maritime homeland security; Military Health System
MHU	modular heat unit
MHW	mean high water
MHz	megahertz

MI	military intelligence; movement instructions
MIA	missing in action
MIAC	maritime intelligence and analysis center
MIB	Military Intelligence Board
MIC	Multinational Interoperability Council
MICAP	mission capable/mission capability
MICON	mission concept
MICRO-MICS	micro-medical inventory control system
MICRO-SNAP	micro-shipboard non-tactical automated data processing system
MIDAS	model for intertheater deployment by air and sea
MIDB	modernized integrated database; modernized intelligence database
MIDDS-T	Meteorological and Oceanographic (METOC) Integrated Data Display System-Tactical
MIF	maritime interception force
MIJI	meaconing, interference, jamming, and intrusion
MILAIR	military airlift
MILALOC	military air line of communications
MILCON	military construction
MILDEC	military deception
MILDEP	Military Department
MILGP	military group (assigned to American Embassy in host nation)
MILOB	military observer
MILOC	military oceanography group (NATO)
MILPERS	military personnel
MILSATCOM	military satellite communications
MILSPEC	military specification
MILSTAMP	military standard transportation and movement procedures
MILSTAR	military strategic and tactical relay system
MIL-STD	military standard
MILSTRAP	military standard transaction reporting and accounting procedure
MILSTRIP	military standard requisitioning and issue procedure
MILTECH	military technician
MILU	multinational integrated logistic unit
MILVAN	military van (container)
MIM	maintenance instruction manual
MIMP	Mobilization Information Management Plan
MINEOPS	joint minelaying operations
MIO	maritime interception operations
MIOC	maritime interception operations commander
MIO-9	information operations threat analysis division (DIA)
MIP	military intelligence program
MIPE	mobile intelligence processing element

MIPOE	medical intelligence preparation of the operational environment
MIPR	military interdepartmental purchase request
MIR	multisensor imagery reconnaissance
MIRCS	mobile integrated remains collection system
MIS	maritime intelligence summary; military information support
MISAS	military information support automated system
MISCAP	mission capability
MISG	military information support group
MISO	military information support operations
MISREP	mission report
MIST	military information support team
MISTF	military information support task force
MITAM	mission tasking matrix
MITASK	mission tasking
MITO	minimum interval takeoff
MITT	mobile integrated tactical terminal
MIUW	mobile inshore undersea warfare
MIW	mine warfare
MIWC	mine warfare commander
MIWG	multinational interoperability working group
MJCS	Joint Chiefs of Staff memorandum
MJLC	multinational joint logistic center
M-Kill	mobility kill
MLA	mission load allowance
MLAYREP	mine laying report
MLE	maritime law enforcement
MLEA	Maritime Law Enforcement Academy
MLEM	Maritime Law Enforcement Manual
MLG	Marine logistics group
MLI	munitions list item
MLMC	medical logistics management center
MLO	military liaison office
MLP	message load plan; mobile landing platform
MLPP	multilevel precedence and preemption
MLPS	Medical Logistics Proponent Subcommittee
MLRS	multiple launch rocket system
MLS	microwave landing system; multilevel security
MLSA	mutual logistics support agreement
MLW	mean low water
MMA	military mission area
MMAC	military mine action center
MMC	materiel management center
MMG	Department of Defense Master Mobilization Guide
MMI	man/machine interface

MMIS	military information support operations management information subsystem
MMLS	mobile microwave landing system
MMS	mast-mounted sight
MMT	military mail terminal
MNC	multinational corporation
MNCC	multinational coordination center
MNF	multinational force
MNFACC	multinational force air component commander
MNFC	multinational force commander
MNFLCC	multinational force land component commander
MNFMCC	multinational force maritime component commander
MNFSOCC	multinational force special operations component commander
MNJLC	multinational joint logistics component
MNL	master net list; multinational logistics
MNLC	multinational logistic center
MNP	master navigation plan
MNS	mine neutralization system (USN); mission needs statement
MNTF	multinational task force
MO	month
MOA	memorandum of agreement; military operating area
MOADS	maneuver-oriented ammunition distribution system
MOB	main operating base; mobilization
MOBCON	mobilization control
MOBREP	military manpower mobilization and accession status report; mobilization report
MOC	maritime operations center; media operations center
MOCC	measurement and signature intelligence (MASINT) operations coordination center; mobile operations control center
MOD	Minister of Defense; ministry of defense; modification
MODEM	modulator/demodulator
MODLOC	miscellaneous operational details, local operations
MOD T-AGOS	modified tactical auxiliary general ocean surveillance
MOE	measure of effectiveness
MOEI	measure of effectiveness indicator
MOG	maximum (aircraft) on ground; movement on ground (aircraft); multinational observer group
MOGAS	motor gasoline
MOLE	multichannel operational line evaluator
MOMAT	mobility matting
MOMSS	mode and message selection system
MOP	measure of performance; memorandum of policy

MOPP	mission-oriented protective posture
MOR	memorandum of record
MOS	military occupational specialty
MOSC	meteorological and oceanographic operations support community
MOTR	maritime operational threat response
MOU	memorandum of understanding
MOUT	military operations in urban terrain; military operations on urbanized terrain
MOVREP	movement report
MOW	maintenance orderwire
MP	military police (Army and Marine); multinational publication
MPA	maritime patrol aircraft; mission and payload assessment; mission planning agent
MPAT	military patient administration team; Multinational Planning Augmentation Team
MPC	mid-planning conference; military personnel center
MPE/S	maritime pre-positioning equipment and supplies
MPF	maritime pre-positioning force
MPFUB	maritime pre-positioning force utility boat
MPG	maritime planning group; mensurated point graphic
mph	miles per hour
MPICE	measuring progress in conflict environments
MPLAN	Marine Corps Mobilization Management Plan
MPM	medical planning module
MPNTP	Master Positioning Navigation and Timing Plan
MPO	military post office
MPP	maritime procedural publication
MPR	maritime patrol and reconnaissance
MPRS	multipoint refueling system
MPS	maritime pre-positioning ship; message processor shelter; Military Planning Service (UN); Military Postal Service
MPSRON	maritime pre-positioning ships squadron
MR	milliradian; mobile reserve
MRAALS	Marine remote area approach and landing system
MRAT	medical radiobiology advisory team
MRBM	medium-range ballistic missile
MRCI	maximum rescue coverage intercept
MRE	meal, ready to eat
MRG	movement requirements generator
MRI	magnetic resonance imaging
MRMC	US Army Medical Research and Materiel Command
MRO	mass rescue operation; materiel release order; medical regulating office; medical regulating officer
MROC	multicommand required operational capability

MRR	minimum-risk route
MRRR	mobility requirement resource roster
MRS	measurement and signature intelligence (MASINT) requirements system; meteorological radar subsystem; movement report system
MRSA	Materiel Readiness Support Agency
MRT	maintenance recovery team
MRU	mountain rescue unit
MRX	mission readiness exercise
MS	message switch; Microsoft
ms	millisecond
MSA	Maritime Security Act
MSC	major subordinate command; maritime support center; Military Sealift Command; military staff committee; mission support confirmation
MSCA	military support to civilian authorities
MSCAT	maritime security center augment team
MSCD	military support to civil defense
MSCO	Military Sealift Command Office
MSD	marginal support date; mobile security division
MS-DOS	Microsoft disk operating system
MSE	mission support element; mobile subscriber equipment
MSECR	HIS 6000 security module
MSEL	master scenario events list
MSF	*Medicins Sans Frontieres* (“Doctors Without Borders”); mission support force; mobile security force; multiplex signal format
MSG	Marine security guard; message
MSGID	message identification
MSHARPP	mission, symbolism, history, accessibility, recognizability, population, and proximity
MSI	modified surface index; multispectral imagery
MSIC	Missile and Space Intelligence Center
MSIS	Marine safety information system
MSK	mission support kit
MSL	master station log; mean sea level; military shipping label
MSNAP	merchant ship naval augmentation program
MSO	map support office; marine safety office(r); maritime security operations; military satellite communications (MILSATCOM) systems organization; military source operation; military strategic objective; military support operations
MSOAG	Marine special operations advisor group
MSOC	Marine special operations company
MSOR	Marine Special Operations Regiment
MSP	Maritime Security Program; mission support plan;

	mobile sensor platform
MSPA	Missing Service Personnel Act
MSPES	mobilization stationing, planning, and execution system
MSPS	military information support operations studies program subsystem; mobilization stationing and planning system
MSR	main supply route; maritime support request; mission support request
MSRON	maritime expeditionary security squadron
MSRP	mission strategic resource plan
MSRR	modeling and simulation resource repository
MSRT	Maritime Security Response Team (USCG)
MSRV	message switch rekeying variable
MSS	medical surveillance system; meteorological satellite subsystem
MSSG	Marine expeditionary unit (MEU) service support group
MST	Marine expeditionary force (MEF) weather support team; meteorological and oceanographic support team; mission support team
MT	military technician; ministry team
MTA	military training agreement
MTAC	Multiple Threat Alert Center (DON)
MTBF	mean time between failures
MT Bn	motor transport battalion
MTCR	Missile Technology Control Regime
MT/D	measurement tons per day
mtDNA	mitochondrial deoxyribonucleic acid
MTF	medical treatment facility; message text format; military information support operations task force
MTG	master timing generator; military information support operations task group
MTI	moving target indicator
MTIC	Military Targeting Intelligence Committee
MTL	mission tasking letter
MTMS	maritime tactical message system
MTN	multi-tactical data link network
MTO	message to observer; mission type order
MTOE	modified table of organization and equipment
MTON	measurement ton
MTP	Marine tactical publication; maritime task plan; mission tasking packet
MTS	Marine tactical system; Movement Tracking System
MTS/SOF-IRIS	multifunction system
MTT	magnetic tape transport
MTTP	multi-Service tactics, techniques, and procedures
MTW	major theater war
MTX	message text format

MU	marry up
MUL	master urgency list (DOD)
MULE	modular universal laser equipment
MUOS	Mobile Users Object System
MUREP	munitions report
MUSARC	major United States Army reserve commands
MUSE	mobile utilities support equipment
MUST	medical unit, self-contained, transportable
MUX	multiplex
MV	merchant vessel; motor vessel
mV	millivolt
MWBP	missile warning bypass
MWC	Missile Warning Center (NORAD)
MWD	military working dog
MWDT	military working dog team
MWF	medical working file
MWG	mobilization working group
MWOD	multiple word-of-day
MWR	missile warning receiver; morale, welfare, and recreation
MWSD	Marine wing support detachment
MWSG	Marine wing support group
MWSS	Marine wing support squadron
MWT	modular warping tug

Intentionally Blank

N

N	number of required track spacings; number of search and rescue units (SRUs)
N-1	Navy component manpower or personnel staff officer
N-2	Director of Naval Intelligence; Navy component intelligence staff officer
N-3	Navy component operations staff officer
N-4	Navy component logistics staff officer
N-5	Navy component plans staff officer
N-6	Navy component communications staff officer
NA	nation assistance
NA5CRO	non-Article 5 crisis response operation (NATO)
NAAG	North Atlantic Treaty Organization (NATO) Army Armaments Group
NAC	North American Aerospace Defense Command (NORAD) Air Center; North Atlantic Council (NATO)
NACE	National Military Command System (NMCS) Automated Control Executive
NACISA	North Atlantic Treaty Organization (NATO) Communications and Information Systems Agency
NACISC	North Atlantic Treaty Organization (NATO) Communications and Information Systems Committee
NACSEM	National Communications Security/Emanations Security (COMSEC/EMSEC) Information Memorandum
NACSI	national communications security (COMSEC) instruction
NACSIM	national communications security (COMSEC) information memorandum
NAD 83	North American Datum 1983
NADEFCOL	North Atlantic Treaty Organization (NATO) Defense College
NADEP	naval aircraft depot
NAE	Navy acquisition executive
NAEC-ENG	Naval Air Engineering Center - Engineering
NAF	naval air facility; nonappropriated funds; numbered air force
NAFAG	North Atlantic Treaty Organization (NATO) Air Force Armaments Group
NAI	named area of interest
NAIC	National Air Intelligence Center
NAK	negative acknowledgement
NALC	Navy ammunition logistics code
NALE	naval and amphibious liaison element
NALSS	naval advanced logistic support site
NAMP	North Atlantic Treaty Organization (NATO) Annual Manpower Plan

NAMS	National Air Mobility System
NAMTO	Navy material transportation office
NAOC	national airborne operations center (E-4B aircraft)
NAPCAP	North Atlantic Treaty Organization (NATO) Allied Pre-Committed Civil Aircraft Program
NAPMA	North Atlantic Treaty Organization (NATO) Airborne Early Warning and Control Program Management Agency
NAPMIS	Navy Preventive Medicine Information System
NAR	nonconventional assisted recovery; notice of ammunition reclassification
NARAC	national atmospheric release advisory capability; National Atmospheric Release Advisory Center (DOE)
NARC	non-automatic relay center
NARP	Nuclear Weapon Accident Response Procedures
NAS	naval air station
NASA	National Aeronautics and Space Administration
NASAR	National Association for Search and Rescue
NAS computer	national airspace system computer
NASIC	National Air and Space Intelligence Center
NAT	nonair-transportable (cargo)
NATO	North Atlantic Treaty Organization
NATOPS	Naval Air Training and Operating Procedures Standardization
NAU	Narcotics Assistance Unit
NAVAID	navigation aid
NAVAIDS	navigational aids
NAVAIR	naval air; Naval Air Systems Command
NAVAIRSYSCOM	Naval Air Systems Command (Also called NAVAIR)
NAVATAC	Navy Antiterrorism Analysis Center; Navy Antiterrorist Alert Center
NAVCHAPDET	naval cargo handling and port group detachment
NAVCHAPGRU	Navy cargo handling and port group
NAVCOMSTA	naval communications station
NAVCYBERFOR	Navy Cyber Forces
NAVELSG	Navy expeditionary logistic support group
NAVEODTECHDIV	Naval Explosives Ordnance Disposal Technology Division
NAVEURMETOCCEN	Naval Europe Meteorology and Oceanography Center
NAVFAC	Naval Facilities Engineering Command
NAVFACENGCOM	Navy Facilities Engineering Command
NAVFAC EXWC	Naval Facilities Engineering and Expeditionary Warfare Center
NAVFAC-X	Naval Facilities Engineering Command-expeditionary
NAVFAX	Navy facsimile
NAVFOR	Navy forces

NAVICECEN	Naval Ice Center
NAVLANTMETOCCEN	Naval Atlantic Meteorology and Oceanography Center
NAVMAG	naval magazine
NAVMED	Navy Medical (Command); Navy medicine
NAVMEDCOMINST	Navy medical command instruction
NAVMEDLOGCOM	Navy Medical Logistics Command
NAVMEDP	Navy medical pamphlet
NAVMETOCCOM	Naval Meteorology and Oceanography Command
NAVMTO	naval military transportation office; Navy Material Transportation Office
NAVOCEANO	Naval Oceanographic Office
NAVORD	naval ordnance
NAVORDSTA	naval ordnance station
NAVPACMETOCCEN	Naval Pacific Meteorology and Oceanography Center
NAVSAFECEN	naval safety center
NAVSAT	navigation satellite
NAVSEA	Naval Sea Systems Command
NAVSEAINST	Naval Sea Systems Command instruction
NAVSEALOGCEN	naval sea logistics center
NAVSEASYSCOM	Naval Sea Systems Command
NAVSO	United States Navy Forces, Southern Command
NAVSOC	Naval Satellite Operations Center; naval special operations command
NAVSOF	Navy special operations forces
NAVSPACECOM	Naval Space Command
NAVSPECWARCOM	Naval Special Warfare Command
NAVSPOC	Naval Space Operations Center
NAVSUP	Naval Supply Systems Command
NAVSUPINST	Navy Support Instruction
NAVSUPSYSCOM	Naval Supply Systems Command
NAVWAR	navigation warfare
NAWCAD	Naval Air Warfare Center, Aircraft Division
Navy TACC	Navy tactical air control center
NB	narrowband
NBC	nuclear, biological, and chemical
NBCCS	nuclear, biological, and chemical (NBC) contamination survivability
NBDP	narrow band direct printing
NBG	naval beach group
NBI	nonbattle injury
NBS	National Bureau of Standards
NBST	narrowband secure terminal
NBVC	Naval Base Ventura County
NC3A	nuclear command, control, and communications (C3) assessment
NCAA	North Atlantic Treaty Organization (NATO) Civil Airlift

	Agency
NCAGS	naval cooperation and guidance for shipping
NCAPS	naval coordination and protection of shipping
NCB	national central bureau; naval construction brigade; noncompliant boarding
NCC	National Coordinating Center; naval component commander; Navy component command; Navy component commander; network control center; North American Aerospace Defense Command (NORAD) Command Center
NCCS	Nuclear Command and Control System
NCD	net control device
NCDC	National Climatic Data Center
NCES	Net-Centric Enterprise Services
NCESGR	National Committee of Employer Support for the Guard and Reserve
NCF	naval construction force
NCFSU	naval construction force support unit
NCG	naval construction group
NCHB	Navy cargo-handling battalion
NCIC	National Crime Information Center
NCIJTF-AG	National Cyber Investigative Joint Task Force-Analytical Group (DOD)
NCIS	Naval Criminal Investigative Service
NCISRA	Naval Criminal Investigative Service resident agent
NCISRO	Naval Criminal Investigative Service regional office
NCISRU	Naval Criminal Investigative Service resident unit
NCIX	National Counterintelligence Executive
NCMI	National Center for Medical Intelligence
NCMP	Navy Capabilities and Mobilization Plan
NCO	noncombat operations; noncommissioned officer
NCOB	National Counterintelligence Operations Board
NCOIC	noncommissioned officer in charge
NCOS	naval control of shipping
NCP	National Oil and Hazardous Substances Pollution Contingency Plan
NCPC	National Counterproliferation Center
NCR	National Capital Region (US); national cryptologic representative; National Security Agency/Central Security Service representative; naval construction regiment
NCRCC	National Capital Region Coordination Center; United States Northern Command Rescue Coordination Center
NCRCG	National Cyber Response Coordination Group
NCRDEF	national cryptologic representative defense
NCR-IADS	National Capital Region-Integrated Air Defense System

NCS	National Clandestine Service; National Communications System; naval control of shipping; net control station
NCSC	National Computer Security Center
NCSD	National Cyber Security Division (DHS)
NCSE	national intelligence support team (NIST) communications support element
NCT	network control terminal
NCTAMS	naval computer and telecommunications area master station
NCTC	National Counterterrorism Center; North East Counterdrug Training Center
NCTS	naval computer and telecommunications station
NCWS	naval coastal warfare squadron
NDAA	national defense authorization act
NDAF	Navy, Defense Logistics Agency, Air Force
NDB	nondirectional beacon
NDCS	national drug control strategy
NDDOC	North American Aerospace Defense Command and United States Northern Command Deployment and Distribution Operations Cell
NDHQ	National Defence Headquarters, Canada
NDIC	National Defense Intelligence College; National Drug Intelligence Center
NDL	national desired ground zero list
NDMC	North Atlantic Treaty Organization (NATO) Defense Manpower Committee
NDMS	National Disaster Medical System (DHHS)
NDOC	National Defense Operations Center
NDP	national disclosure policy
NDPB	National Drug Policy Board
NDPC	National Disclosure Policy Committee
NDRC	National Detainee Reporting Center
NDRF	National Defense Reserve Fleet
NDS	national defense strategy
NDSF	National Defense Sealift Fund
NDT	nuclear disablement team
NDU	National Defense University
NEA	Northeast Asia
NEAT	naval embarked advisory team
NEC	National Economic Council
NECC	Navy Expeditionary Combat Command
NEIC	Navy Expeditionary Intelligence Command
NELR	Navy expeditionary logistics regiment
NEMT	National Emergency Management Team
NEO	noncombatant evacuation operation
NEOCC	noncombatant evacuation operation coordination center

NEP	National Exercise Program
NEPA	National Environmental Policy Act
NEREP	Nuclear Execution and Reporting Plan
NES	National Exploitation System
NESDIS	National Environmental Satellite, Data and Information Service (DOC)
NEST	nuclear emergency support team (DOE)
NETS	Nationwide Emergency Telecommunications System
NETT	new equipment training team
NETWARCOM	Naval Network Warfare Command
NEW	net explosive weight
NEWAC	North Atlantic Treaty Organization (NATO) Electronic Warfare Advisory Committee
NEWCS	NATO electronic warfare core staff
NEXCOM	Navy Exchange Command
NFA	no-fire area
NFC	numbered fleet commander
NFD	nodal fault diagnostics
NFELC	Naval Facilities Expeditionary Logistics Center
NFESC	Naval Facilities Engineering Service Center
NFI	national foreign intelligence
NFIB	National Foreign Intelligence Board
NFIP	National Flood Insurance Program (FEMA); National Foreign Intelligence Program
NFLIR	navigation forward-looking infrared
NFLS	naval forward logistic site
NFN	national file number
NFO	naval flight officer
NG	National Guard
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
NGB-OC	National Guard Bureau-Office of the Chaplain
NGCC	National Guard coordination center
NGCDP	National Guard Counterdrug Program
NGCSP	National Guard Counterdrug Support Program
NGF	naval gun fire
NGFS	naval gunfire support
NGIC	National Ground Intelligence Center
NG JFHQ-State	National Guard joint force headquarters-state
NGLO	naval gunfire liaison officer
NGO	nongovernmental organization
NGP	National Geospatial-Intelligence Agency Program
NGRF	National Guard reaction force
NI	national identification (number); noted item
NIBRS	National Incident-Based Reporting System
NIC	National Intelligence Council; naval intelligence center

NICC	National Intelligence Coordination Center
NICCL	National Incident Communications Conference Line
NICCP	National Interdiction Command and Control Plan
NICI	National Interagency Counternarcotics Institute
NID	naval intelligence database
NIDMS	National Military Command System (NMCS) Information for Decision Makers System
NIDS	National Military Command Center (NMCC) information display system
NIE	national intelligence estimate
NIEX	no-notice interoperability exercise
NIEXPG	No-Notice Interoperability Exercise Planning Group
NIH	National Institutes of Health (DHHS)
NIIB	National Geospatial Intelligence Agency imagery intelligence brief
NIL	National Information Library
NIMCAMP	National Information Management and Communications Master Plan
NIMS	National Incident Management System
NIOC	Navy Information Operations Command
NIP	National Intelligence Program
NIPF	National Intelligence Priority Framework
NIPRNET	Nonsecure Internet Protocol Router Network
NIPS	Naval Intelligence Processing System
NIRT	Nuclear Incident Response Team
NISH	noncombatant evacuation operation (NEO) intelligence support handbook
NISP	national intelligence support plan; Nuclear Weapons Intelligence Support Plan
NIST	National Institute of Standards and Technology
NIT	nuclear incident team
NITES	Navy Integrated Tactical Environmental System
NITF	national imagery transmission format
NIU	North Atlantic Treaty Organization (NATO) interface unit
NIWA	naval information warfare activity
NJOIC	National Joint Operations and Intelligence Center
NJTTF	National Joint Terrorism Task Force
NL	Navy lighterage
NLO	naval liaison officer
.NL.	not less than
NLT	not later than
NLW	nonlethal weapon
NM	network management
nm	nautical mile
NMAWC	Naval Mine and Anti-Submarine Warfare Command
NMB	North Atlantic Treaty Organization (NATO) military

	body
NMC	Navy Munitions Command
NMCB	naval mobile construction battalion
NMCC	National Military Command Center
NMCS	National Military Command System; not mission capable, supply
NMCSO	Navy and Marine Corps spectrum office
NMD	national missile defense
NMEC	National Media Exploitation Center
NMFS	National Marine Fisheries Services
NMIC	National Maritime Intelligence Center
NMIO	National Maritime Intelligence-Integration Office
NMIST	National Military Intelligence Support Team (DIA)
NMO	National Measurement and Signature Intelligence Office
NMOC	network management operations center
NMOSW	Naval METOC Operational Support Web
NMP	national media pool
NMPS	Navy mobilization processing site
NMRC	Naval Medical Research Center
NMS	national military strategy
NMSA	North Atlantic Treaty Organization (NATO) Mutual Support Act
NMSC	Navy and Marine Corps Spectrum Center
NMS-CO	National Military Strategy for Cyberspace Operations
NMS-CWMD	National Military Strategy to Combat Weapons of Mass Destruction
NMSP-WOT	National Military Strategic Plan for the War on Terrorism
NNAG	North Atlantic Treaty Organization (NATO) Naval Armaments Group
NNSA	National Nuclear Security Administration (DOE)
NNWC	Naval Network Warfare Command
NOAA	National Oceanic and Atmospheric Administration
NOACT	Navy overseas air cargo terminal
NOC	National Operations Center (DHS); network operations center
NOCONTRACT	not releasable to contractors or consultants
NODDS	Naval Oceanographic Data Distribution System
NOE	nap-of-the-earth
NOEA	nuclear operations emergency action
NOFORN	not releasable to foreign nationals
NOG	Nuclear Operations Group
NOGAPS	Navy Operational Global Atmospheric Prediction System
NOHD	nominal ocular hazard distance
NOIC	Naval Operational Intelligence Center
NOK	next of kin
NOLSC	Naval Operational Logistics Support Center

NOMS	Nuclear Operations Monitoring System
NOMWC	Navy Oceanographic Mine Warfare Center
NOP	nuclear operations
NOPLAN	no operation plan available or prepared
NORAD	North American Aerospace Defense Command
NORM	normal; not operationally ready, maintenance
NORS	not operationally ready, supply
NOSC	network operations and security center
NOSSA	Navy Ordnance Safety and Security Activity
NOTAM	notice to airmen
NOTMAR	notice to mariners
NP	nonproliferation
NPC	Nonproliferation Center
NPES	Nuclear Planning and Execution System
NPG	nonunit personnel generator
NPOESS	National Polar-orbiting Operational Environmental Satellite System
NPPD	National Protection and Programs Directorate (DHS)
NPS	National Park Service; nonprior service; Nuclear Planning System
NPT	national pipe thread; Treaty on the Nonproliferation of Nuclear Weapons
NPWIC	National Prisoner of War Information Center
NQ	nonquota
NR	North Atlantic Treaty Organization (NATO) restricted; number
NRAT	nuclear/radiological advisory team
NRC	National Response Center (USCG); non-unit-related cargo
NRCHB	Naval Reserve cargo-handling battalion
NRCHF	Naval Reserve cargo handling force
NRCHTB	Naval Reserve cargo handling training battalion
NRF	National Response Framework
NRFI	not ready for issue
NRG	notional requirements generator
NRL	nuclear weapons (NUWEP) reconnaissance list
NRO	National Reconnaissance Office
NROC	Northern Regional Operations Center (CARIBROC-CBRN)
NRP	National Response Plan; non-unit-related personnel
NRPC	Naval Reserve Personnel Center
NRT	near real time
NRTD	near-real-time dissemination
NRZ	non-return-to-zero
NS	nuclear survivability
NSA	national security act; National Security Agency; national security area; national shipping authority; North Atlantic Treaty Organization (NATO) Standardization Agency

NSABB	National Science Advisory Board for Biosecurity (NIH)
NSA/CSS	National Security Agency/Central Security Service
NSARC	National Search and Rescue Committee
NSAT	United States Northern Command situational awareness team
NSAWC	Naval Strike and Air Warfare Center
NSC	National Security Council
NSC/DC	National Security Council/Deputies Committee
NSCID	National Security Council intelligence directive
NSC/IPC	National Security Council/interagency policy committee
NSC/IWG	National Security Council/Interagency Working Group
NSC/PC	National Security Council/Principals Committee
NSC/PCC	National Security Council Policy Coordinating Committee
NSCS	National Security Council System
NSCTI	Naval Special Clearance Team One
NS-CWMD	National Strategy to Combat Weapons of Mass Destruction
NSD	National Security Directive; National Security Division (FBI)
NSDA	non-self deployment aircraft
NSDD	national security decision directive
NSDM	national security decision memorandum
NSDS-E	Navy Satellite Display System-Enhanced
NSE	Navy support element
NSEP	national security emergency preparedness
NS/EP	national security and emergency preparedness
NSF	National Science Foundation; national security forces; National Strike Force (USCG)
NSFS	naval surface fire support
NSG	National System for Geospatial Intelligence; north-seeking gyro
NSGI	National System for Geospatial Intelligence
NSHS	National Strategy for Homeland Security
NSL	no-strike list
NSM	national search and rescue (SAR) manual
NSMS	National Strategy for Maritime Security
NSN	national stock number
NSO	non-Single Integrated Operational Plan (SIOP) option
NSOC	National Security Operations Center; National Signals Intelligence (SIGINT) Operations Center; Navy Satellite Operations Center
NSOOC	North Atlantic Treaty Organization (NATO) Staff Officer Orientation Course
NSP	National Search and Rescue Plan
N-Sp/CC	North American Aerospace Defense Command (NORAD)-US Space Command/Command Center
NSPD	national security Presidential directive
NSPI	National Strategy for Pandemic Influenza
NSRL	national signals intelligence (SIGINT) requirements list

NSS	National Search and Rescue Supplement; national security strategy; national security system; non-self-sustaining
NSSA	National Security Space Architect
NSSE	national special security event
NSST	naval space support team
NST	National Geospatial-Intelligence Agency support team
NSTAC	National Security Telecommunications Advisory Committee
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTL	national strategic targets list
NSTS	National Secure Telephone System
NSW	naval special warfare
NSWCDD	Naval Surface Warfare Center Dahlgren Division
NSWCOM	Naval Special Warfare Command
NSWG	naval special warfare group
NSWTF	naval special warfare task force
NSWTG	naval special warfare task group
NSWTU	naval special warfare task unit
NT	nodal terminal
NTA	nontraditional agent
NTACS	Navy tactical air control system
NTAP	National Track Analysis Program
NTB	national target base
NTBC	National Military Joint Intelligence Center Targeting and Battle Damage Assessment Cell
NTC	National Training Center
NTCS-A	Navy Tactical Command System-Afloat
NTDS	naval tactical data system
NTF	nuclear task force
N-TFS	New Tactical Forecast System
NTIA	National Telecommunications and Information Administration
NTIC	Navy Tactical Intelligence Center
NTISS	National Telecommunications and Information Security System
NTISSI	National Telecommunications and Information Security System (NTISS) Instruction
NTISSP	National Telecommunications and Information Security System (NTISS) Policy
NTM	national or multinational technical means of verification; notice to mariners
NTMPDE	National Telecommunications Master Plan for Drug Enforcement
NTMS	national telecommunications management structure
NTPS	near-term pre-positioned ships

NTRP	Navy tactical reference publication
NTS	night targeting system; noncombatant evacuation operation tracking system
NTSB	National Transportation Safety Board
NTSS	National Time-Sensitive System
NTTP	Navy tactics, techniques, and procedures
NTU	new threat upgrade
NUC	non-unit-related cargo; nuclear
NUDET	nuclear detonation
NUFEA	Navy-unique fleet essential aircraft
NUP	non-unit-related personnel
NURP	non-unit-related personnel
NUWEP	policy guidance for the employment of nuclear weapons
NVD	night vision device
NVDT	National Geospatial-Intelligence Agency voluntary deployment team
NVG	night vision goggle
NVS	night vision system
NW	network warfare; not waiverable
NWARS	National Wargaming System
NWB	normal wideband
NWBLTU	normal wideband line termination unit
NWDC	Navy Warfare Development Command
NWFP	Northwest Frontier Province (Pakistan)
NWP	Navy warfare publication; numerical weather prediction
NWREP	nuclear weapons report
NWS	National Weather Service
NWT	normal wideband terminal

O

1MC	general announcing system
1NCD	1st Naval Construction Division
O	contour pattern
O&I	operations and intelligence
O&M	operation and maintenance
OA	objective area; operating assembly; operational area; Operations Aerology shipboard METOC division
OADR	originating agency's determination required
OAE	operational area evaluation
OAF	Operation ALLIED FORCE
OAFME	Office of the Armed Forces Medical Examiner
OAG	operations advisory group
OAI	oceanographic area of interest
OAJCG	Operation Alliance joint control group
OAM	Office of Air and Marine (DHS)
OAP	offset aimpoint
OAR	Chairman of the Joint Chiefs of Staff operation plans assessment report
OAS	offensive air support; Organization of American States
OASD	Office of the Assistant Secretary of Defense
OASD(NII/CIO)	Office of the Assistant Secretary of Defense (Networks and Information Integration/Chief Information Officer)
OASD(PA)	Office of the Assistant Secretary of Defense (Public Affairs)
OASD(RA)	Office of the Assistant Secretary of Defense (Reserve Affairs)
OAU	Organization of African Unity
O/B	outboard
OB	operating base; order of battle
OBA	Office of Biotechnology Activities (NIH); oxygen breathing apparatus
OBFS	offshore bulk fuel system
OBST	obstacle
OBSTINT	obstacle intelligence
OC	oleoresin capsicum; operations center
OCA	offensive counterair; operational control authority
OCBD	Office of Capacity Building and Development (USDA)
OCC	Operations Computer Center (USCG)
OCCA	ocean cargo clearance authority
OCD	orderwire clock distributor
OCDETF	Organized Crime and Drug Enforcement Task Force
OCE	officer conducting the exercise
OCEANCON	control of oceanographic information
OCHA	Office for the Coordination of Humanitarian Affairs
OCIE	organizational clothing and individual equipment
OCJCS	Office of the Chairman of the Joint Chiefs of Staff

OCJCS-PA	Office of the Chairman of the Joint Chiefs of Staff-Public Affairs
OCMI	officer in charge, Marine inspection
OCO	offensive cyberspace operations; offload control officer
OCONUS	outside the continental United States
OCOP	outline contingency operation plan
OCP	operational capability package; operational configuration processing
OCR	Office of Collateral Responsibility
OCS	operational contract support
OCSIC	operational contract support integration cell
OCU	orderwire control unit (Types I, II, and III)
OCU-1	orderwire control unit-1
OD	operational detachment; other detainee
ODA	operational detachment-Alpha
ODATE	organization date
ODB	operational detachment-Bravo
ODC	Office of Defense Cooperation
ODCSLOG	Office of the Deputy Chief of Staff for Logistics (Army)
ODCSOPS	Office of the Deputy Chief of Staff for Operations and Plans (Army)
ODCSPER	Office of the Deputy Chief of Staff for Personnel (Army)
ODIN	Operational Digital Network
ODJS	Office of the Director, Joint Staff
ODNI	Office of the Director of National Intelligence
ODR	Office of Defense representative
ODZ	outer defense zone
OE	operational environment
OE&AS	organization for embarkation and assignment to shipping
OEBGD	Overseas Environmental Baseline Guidance Document
OEC	Office of Emergency Communications (DHS)
OECD	Organisation for Economic Co-operation and Development
OEF	Operation ENDURING FREEDOM
OEG	operational experts group; operational exposure guidance operations security executive group
OEH	occupational and environmental health
OEM	original equipment manufacturer
OER	officer evaluation report; operational electronic intelligence (ELINT) requirements
OES	office of emergency services
OET	Office of Emergency Transportation (DOT)
OF	officer (NATO)
OFAC	Office of Foreign Assets Control (TREAS)
OFCO	offensive counterintelligence operation
OFDA	Office of United States Foreign Disaster Assistance (USAID)
OFHIS	operational fleet hospital information system

OFOESA	Office of Field Operational and External Support Activities
OFSC	Organizational and Force Structure Construct
OGS	overseas ground station
OH	overhead
OHDACA	Overseas Humanitarian, Disaster, and Civic Aid (DSCA)
OHDM	Office of Humanitarian Assistance, Disaster Relief, and Mine Action
OI	Office of Intelligence (USCS); operating instruction; operational interest
OIA	Office of International Affairs (TREAS)
OI&A	Office of Intelligence and Analysis (DHS)
OIC	officer in charge
OICC	officer in charge of construction; operational intelligence coordination center
OID	operation order (OPORD) identification
OIF	Operation IRAQI FREEDOM
OIIL	Office of Intelligence and Investigative Liaison (CBP)
OIR	operational intelligence requirements; other intelligence requirements
OJT	on-the-job training
OL	operating location
OLD	on-line tests and diagnostics
OLS	operational linescan system; optical landing system
OM	contour multiunit
OMA	Office of Military Affairs (CIA and USAID)
OMB	Office of Management and Budget; operations management branch
OMC	Office of Military Cooperation; optical memory card
OMF	officer master file
OMS	Office of Mission Support
OMSPH	Office of Medicine, Science, and Public Health (DHHS)
OMT	operations management team; orthogonal mode transducer
OMT/OMTP	operational maintenance test(ing)/test plan
ONDCP	Office of National Drug Control Policy
ONE	Operation NOBLE EAGLE
ONI	Office of Naval Intelligence
OOB	order of battle
OOD	officer of the deck
OODA	observe, orient, decide, act
OOS	out of service
OP	observation post; operational publication (USN); ordnance publication
OPARS	Optimum Path Aircraft Routing System
OPBAT	Operation Bahamas, Turks, and Caicos
OPC	Ocean Prediction Center (DOC)
OPCEN	operations center (USCG)

OPCOM	operational command (NATO)
OPCON	operational control
OPDAT	Office of Overseas Prosecutorial Development, Assistance, and Training (DOJ)
OPDEC	operational deception
OPDS	offshore petroleum discharge system (USN)
OPDS-Future	offshore petroleum discharge system-future (USN)
OPDS-L	offshore petroleum discharge system-legacy (USN)
OPE	operational preparation of the environment
OPELINT	operational electronic intelligence
OPEO	Office of Preparedness and Emergency Operations (DHHS)
OPFOR	opposing force; opposition force
OPG	operations planning group
OPGEN	operation general matter
OPIR	overhead persistent infrared
OPLAN	operation plan
OPLAW	operational law
OPM	Office of Personnel Management; operations per minute
OPMG	Office of the Provost Marshal General
OPNAVINST	Chief of Naval Operations instruction
OPORD	operation order
OPP	orderwire patch panel
OPR	office of primary responsibility
OPREP	operational report
OPROJ	operational project
OPS	operational project stock; operations; operations center
OPSCOM	Operations Committee
OPSDEPS	Service Operations Deputies
OPSEC	operations security
OPSTK	operational stock
OPSUM	operation summary
OPT	operational planning team
OPTAR	operating target
OPTASK	operation task
OPTASKLINK	operations task link
OPTEMPO	operating tempo
OPTINT	optical intelligence
OPZONE	operation zone
OR	operational readiness; other rank(s) (NATO)
ORBAT	order of battle
ORCON	originator controlled
ORDREF	order reference
ORDTYP	order type
ORG	origin (GEOLOC)
ORIG	origin
ORM	operational risk management

ORP	ocean reception point
ORS	operationally responsive space
ORSA	operations research and systems analysis
OS	operating stocks; operating system
OSA	operational support airlift
OSAT	out-of-service analog test
OSC	offensive space control; on-scene commander; on-site commander; Open Source Center (CIA); operational support command; operations support center
OSCE	Organization for Security and Cooperation in Europe
OSD	Office of the Secretary of Defense
OSD/DMDPO	Office of the Secretary of Defense, Defense Military Deception Program Office
OSE	on scene endurance; operations support element
OSEI	operational significant event imagery
OSG	operational support group
OSI	open system interconnection; operational subsystem interface
OSIA	on-site inspection activity
OSINT	open-source information; open-source intelligence
OSIS	open-source information system
OSM	Office of Spectrum Management (NTIA)
OSO	operational support office
OSOCC	on-site operations coordination center
OSP	operations support package
OSPG	overseas security policy group
OSR	on-station report
OSRI	originating station routing indicator
OSV	ocean station vessel
OT	operational test
OT&E	operational test and evaluation
OTA	Office of Technical Assistance (TREAS)
OTC	officer in tactical command; over the counter
OTG	operational target graphic
OTH	other; over the horizon
OTH-B	over-the-horizon backscatter (radar)
OTHT	over-the-horizon targeting
OTI	Office of Transition Initiatives (USAID)
OTS	Officer Training School; one-time source
OUB	offshore petroleum discharge system utility boat
OUSD	Office of the Under Secretary of Defense
OUSD(AT&L)	Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics)
OUSD(C)	Office of the Under Secretary of Defense (Comptroller)
OUSD(C/CFO)	Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer)

OUSD(I)	Office of the Under Secretary of Defense (Intelligence)
OUSD(P)	Office of the Under Secretary of Defense for Policy
OUT	outsize cargo
OVE	on-vehicle equipment
OVER	oversize cargo
OVM	Operation VIGILANT MARINER
OW	orderwire
OWS	operational weather squadron

P

P	parallel pattern; priority; publication
PA	parent relay; physician assistant; primary agency; probability of arrival; public affairs
PAA	position area of artillery
PABX	private automatic branch exchange (telephone)
PACAF	Pacific Air Forces
PAD	patient administration director; positional adjustment; precision aircraft direction
PADD	person authorized to direct disposition of human remains
PADRU	Pan American Disaster Response Unit
PADS	position azimuth determining system
PAG	public affairs guidance
PAL	personnel allowance list; program assembler language
PALCON	pallet container
PALS	precision approach landing system
PAM	preventive and aerospace medicine; pulse amplitude modulation
PaM	passage material
PANS	procedures for air navigation services
PAO	public affairs office; public affairs officer
PAR	performance assessment report; population at risk; precision approach radar
PARC	principal assistant for contracting
PARKHILL	high frequency cryptological device
PARPRO	peacetime application of reconnaissance programs
PARS	Personnel and Accountability System
PAS	personnel accounting symbol
PAT	public affairs team
PAV	policy assessment visit
PAWS	phased array warning system
PAX	passengers; public affairs plans
PB	particle beam; patrol boat; peace building; President's budget
PB4T	planning board for training
PBA	performance-based agreement; production base analysis
PBCR	portable bar code recorder
PBD	program budget decision
PBIED	person-borne improvised explosive device
PBOS	Planning Board for Ocean Shipping
PC	patrol craft; personal computer; pilot in command; preliminary coordination; Principals Committee
Pc	cumulative probability of detection
P,C,&H	packing, crating, and handling
PC&S	post, camp, and station

PCA	Posse Comitatus Act
PCASS	Preliminary Credibility Assessment Screening System
PCC	policy coordination committee; primary control center
PCF	personnel control facility
PCL	positive control launch
PC-LITE	processor, laptop imagery transmission equipment
PCM	pulse code modulation
PCO	primary control officer; procuring contracting officer
PCRTS	primary casualty receiving and treatment ship
PCS	permanent change of station; personal communications system; primary control ship; processing subsystem; processor controlled strapping
PCT	personnel control team
PCTC	pure car and truck carrier
PCZ	physical control zone
PD	position description; Presidential directive; priority designator; probability of damage; probability of detection; procedures description; program definition; program directive; program director; public diplomacy
Pd	drift compensated parallelogram pattern
PDA	preliminary damage assessment
PDAI	primary development/test aircraft inventory
PDC	Pacific Disaster Center
PDD	Presidential decision directive
PDDA	power driven decontamination apparatus
PDDG	program directive development group
PDG	positional data graphic
PDM	program decision memorandum
PDOP	position dilution of precision
PDS	position determining system; primary distribution site; protected distribution system
PDSC	public diplomacy and strategic communication
PDSS	predeployment site survey
PDT	partnership development team
PDUSD(P&R)	Principal Deputy Under Secretary of Defense (Personnel and Readiness)
PE	peace enforcement; peacetime establishment; personal effects; preparation of the environment; program element
PEAD	Presidential emergency action document
PEC	program element code
PECK	patient evacuation contingency kit
PECP	precision engagement collaboration process
PED	processing, exploitation, and dissemination
PEDB	planning and execution database

PEGEO	personnel geographic location
PEI	principal end item
PEIO	personnel effects inventory officer
PEM	program element monitor
PEO	peace enforcement operations; program executive office; program executive officer
PEP	personnel exchange program
PER	personnel
PERE	person eligible to receive effects
PERID	period
PERMA	planning, embarkation, rehearsal, movement, and action
PERMREP	permanent representative (NATO)
PERSCO	personnel support for contingency operations
PERSCOM	personnel command (Army)
PERSINS	personnel information system
PES	preparedness evaluation system
PFA	primary federal agency
PFD	personal flotation device
PFDB	planning factors database
PFIAB	President's Foreign Intelligence Advisory Board
PFID	positive friendly identification
PFO	principal federal official
PfP	Partnership for Peace (NATO)
PGI	procedures, guidance, and information
PGM	precision-guided munition
pH	potential of hydrogen
PHEO	public health emergency officer
PHIBCB	amphibious construction battalion
PHIBGRU	amphibious group
PHIBOP	amphibious operation
PHIBRON	amphibious squadron
PHIT	port handling/in-land transportation
PHO	posthostilities operations
PHS	Public Health Service
PI	pandemic influenza; point of impact ; procedural item; purposeful interference
P_i	probability of incapacitation
PI&ID	pandemic influenza and infectious disease
PIAB	President's Intelligence Advisory Board
PIC	parent indicator code; payment in cash; person identification code; pilot in command; press information center (NATO)
PID	plan identification number; positive identification
PIDD	planned inactivation or discontinued date
PIF	problem identification flag
PII	pre-incident indicators
PIM	pretrained individual manpower

PIN	personnel increment number
PINS	precise integrated navigation system
PIO	press information officer; public information officer
PIPS	plans integration partitioning system
PIR	priority intelligence requirement
PIREP	pilot report
PIRT	purposeful interference response team
PISA	post isolation support activity
PIW	person in water
PJ	pararescue jumper
PK	peacekeeping; probability of kill
PKB	purple kill box
PKG-POL	packaged petroleum, oils, and lubricants
PKI	public key infrastructure
PKO	peacekeeping operations
PKP	purple k powder
PKSOI	Peacekeeping and Stability Operations Institute
PL	phase line; public law
PLA	plain language address; post-launch abort
PLAD	plain language address directory
PLANORD	planning order
PLAT	pilot's landing aid television
PLB	personal locator beacon
PLC	power line conditioner
PLGR	precise lightweight global positioning system (GPS) receiver
PLL	phase locked loop
PLL/ASL	prescribed load list/authorized stock level
PLRS	position location reporting system
PLS	palletized load system; pillars of logistic support; precision location system
PLT	platoon; program library tape
PM	Bureau of Political-Military Affairs (DOS); parallel track multiunit; passage material; patient movement; peacemaking; political-military affairs; preventive medicine; program management; program manager; provost marshal
PMA	political/military assessment
PMAA	Production Management Alternative Architecture
PMAI	primary mission aircraft inventory
P/M/C	passengers/mail/cargo
PMC	parallel multiunit circle; private military company
PMCF	post maintenance check flight
PMCT	port movement control team
PMD	program management directive
PME	professional military education

PMEL	precision measurement equipment laboratory
PMESII	political, military, economic, social, information, and infrastructure
PMGM	program manager's guidance memorandum
PMI	patient movement item; prevention of mutual interference
PMITS	Patient Movement Item Tracking System
PMN	parallel track multiunit non-return
PMO	production management office(r); program management office
PMOS	primary military occupational specialty
PMR	parallel track multiunit return; patient movement request; patient movement requirement
PMRC	patient movement requirements center
PMS	portable meteorological subsystem
PN	partner nation; pseudonoise
PNA	postal net alert
PNID	precedence network in dialing
PNT	positioning, navigation, and timing
PNVS	pilot night vision system
P/O	part of
PO	peace operations; petty officer
POA	plan of action
POAI	primary other aircraft inventory
POB	persons on board
POC	point of contact
POCD	port operations cargo detachment
POD	plan of the day; port of debarkation; probability of detection
POE	port of embarkation; port of entry
POES	polar operational environment satellite
POF	priority of fires
POG	port operations group
POI	program of instruction
POL	petroleum, oils, and lubricants
POLAD	policy advisor; political advisor
POLCAP	bulk petroleum capabilities report
POLMIL	political-military
POM	program objective memorandum
POMCUS	pre-positioning of materiel configured to unit sets
POMSO	Plans, Operations, and Military Support Office(r) (NG)
POP	performance oriented packaging
POPS	port operational performance simulator
POR	proposed operational requirement
PORTS	portable remote telecommunications system
PORTSIM	port simulation model

POS	point of sale; probability of success
POSF	port of support file
POSSUB	possible submarine
POSTMOB	post mobilization
POTUS	President of the United States
POV	privately owned vehicle
POW	prisoner of war
POW/MIA	prisoner of war/missing in action
P/P	patch panel
p-p	peak-to-peak
PPA	personnel information system (PERSINS) personnel activity
PPAG	proposed public affairs guidance
PPBE	Planning, Programming, Budgeting, and Execution
PPD	Presidential policy directive; program planning document
PPDB	point positioning database
PPE	personal protective equipment
PPF	personnel processing file
Pplan	programming plan
PPLI	precise participant location and identification
ppm	parts per million
PPP	power projection platform; primary patch panel; priority placement program
PPR	prior permission required
PPS	precise positioning service
PPTO	petroleum pipeline and terminal operating
PR	personnel recovery; Phoenix Raven; primary zone; production requirement; program review
PRA	patient reception area; primary review authority
PRANG	Puerto Rican Air National Guard
PRBS	pseudorandom binary sequence
PRC	populace and resources control; Presidential Reserve Call-up
PRCC	personnel recovery coordination cell; personnel recovery coordination center
PRCS	personnel recovery coordination section
PRD	personnel readiness division; Presidential review directive
PRDO	personnel recovery duty officer
PREMOB	pre-mobilization
PREPO	pre-positioned force, equipment, or supplies; pre-positioning
PREREP	pre-arrival report
PRF	personnel resources file; pulse repetition frequency
PRG	personnel recovery guidance; program review group
PRI	movement priority for forces having the same latest arrival date (LAD); priority; progressive routing indicator

PRIFLY	primary flight control
Prime BEEF	prime base engineer emergency force
PRISM	Planning Tool for Resource, Integration, Synchronization, and Management
PRM	Bureau of Population, Refugees, and Migration (DOS); Presidential review memorandum
PRMFL	perm file
PRMS	personnel recovery mission software
PRN	pseudorandom noise
PRO	personnel recovery officer
PROBSUB	probable submarine
PROC	processor; Puerto Rican Operations Center
PROFIS	professional officer filler information system
PROM	programmable read-only memory
PROPIN	caution - proprietary information involved
PROVORG	providing organization
proword	procedure word
PRP	personnel reliability program; Personnel Retrieval and Processing
PRRIS	Puerto Rican radar integration system
PRRP	personnel recovery reference product
PRSL	primary zone/switch location
PRT	patient reception team; provincial reconstruction team
PRTF	personnel recovery task force
PRU	pararescue unit; primary reporting unit
PS	parallel track single-unit; port security; processing subsystem
PSA	port support activity; principal staff assistant
PSB	poststrike base
PSC	port security company; principal subordinate command; private security contractor
PSD	planning systems division; port security detachment
PSE	peculiar support equipment
PS/HD	port security/harbor defense
PSHDGRU	port security and harbor defense group
PSI	personnel security investigation; Proliferation Security Initiative
psi	pounds per square inch
PSK	phase-shift keying
PSL	parallel track single-unit long-range aid to navigation (LORAN)
PSMS	Personnel Status Monitoring System
PSN	packet switching node; public switch network
PSO	peace support operations (NATO); post security officer
PSP	perforated steel planking; portable sensor platform; power support platform

PSS	parallel single-unit spiral; personnel services support
PSS-SOF	Precision Strike Suite-Special Operations Forces
P-STATIC	precipitation static
PSTN	public switched telephone network
PSU	port security unit
PSV	pseudosynthetic video
PTA	position, time, altitude
PTAI	primary training aircraft inventory
PTC	peace through confrontation; primary traffic channel
PTDO	prepare to deploy order
PTM	personnel transport module
PTT	postal telephone and telegraph; public telephone and telegraph; push-to-talk
PTTI	precise time and time interval
pub	publication
PUK	packup kit
PUL	parent unit level
PV	prime vendor
PVNTMED	preventive medicine
PVT	positioning, velocity, and timing
PW	prisoner of war
pW	picowatt
PWB	printed wiring board (assembly)
PWD	programmed warhead detonation
PWF	personnel working file
PWG	protection working group
PWIS	Prisoner of War Information System
PWR	pre-positioned wartime reserves
PWRMR	pre-positioned war materiel requirement
PWRMS	pre-positioned war reserve materiel stock
PWRR	pre-positioned war reserve requirements
PWRS	petroleum war reserve stocks; pre-positioned war reserve stock
PWS	performance work statement
PWT	precision weapons team
PZ	pickup zone

Q

QA	quality assurance
QAM	quadrature amplitude modulation
QAR	quality assurance representative
QAT	quality assurance team
QC	quality control
QD	quality distance
QDR	quadrennial defense review; quality deficiency report
QEEM	quick erect expandable mast
QHDA	qualified hazardous duty area
QIP	quick impact project
QM	quartermaster
QPSK	quadrature phase shift keying
QRA	quick reaction antenna
QRCT	quick reaction communications terminal
QRE	quick reaction element
QRF	quick reaction force; quick response force
QRG	quick response graphic
QRP	quick response posture
QRS	quick reaction strike
QRSA	quick reaction satellite antenna
QRT	quick reaction team
QS	quality surveillance
QSR	quality surveillance representative
QSTAG	quadripartite standardization agreement
QTY	quantity
QUADCON	quadruple container

Intentionally Blank

R

R	routine
R&D	research and development
R&R	rest and recuperation
R&S	reconnaissance and surveillance; reconstruction and stabilization
R2P2	rapid response planning process
RA	response action; risk analysis; risk assessment
RAA	redeployment assembly area
RABFAC	radar beacon forward air controller
RAC	responsible analytic center
RAC-OT	readiness assessment system - output tool
RAD	routine aerial distribution
RADAY	radio day
RADBN	radio battalion
RADC	regional air defense commander
RADCON	radiological control team
RADF	radarfind
RADHAZ	electromagnetic radiation hazards
RADS	rapid area distribution support (USAF)
RAE	right of assistance entry
RAF	Royal Air Force (UK)
R-AFF	regimental affiliation
RAM	raised angle marker; random access memory; random antiterrorism measure
RAMCC	regional air movement control center
RAOB	rawindsonde observation
RAOC	regional air operations center
RAP	Radiological Assistance Program (DOE); rear area protection; Remedial Action Projects Program (JCS)
RAS	replenishment at sea
RAS-OT	readiness assessment system-output tool
RAST	recovery assistance, securing, and traversing systems
RASU	random access storage unit
RATE	refine, adapt, terminate, execute
RATT	radio teletype
RB	short-range coastal or river boat
RBA	reimbursable budget authority
RBC	red blood cell
RBE	remain-behind equipment
RBECS	Revised Battlefield Electronic Communications, Electronics, Intelligence, and Operations (CEIO) System
RBI	RED/BLACK isolator
RB std	rubidium standard

RC	receive clock; regional coordinator; Reserve Component; resident coordinator (UN); river current
RCA	riot control agent
RCAT	regional counterdrug analysis team
RCC	regional contracting center; relocation coordination center; rescue coordination center
RCCPDS	Reserve Component common personnel data system
RCD	regional collection detachment
RCEM	regional contingency engineering management
RCHB	reserve cargo handling battalion
RCIED	radio-controlled improvised explosive device
RCM	Rules for Courts-Martial
RCMP	Royal Canadian Mounted Police
RC NORTH	Regional Command North (NATO)
RCO	regional contracting office
RCP	resynchronization control panel
RCS	radar cross section
RC SOUTH	Regional Command South (NATO)
RCSP	remote call service position
RCT	regimental combat team; rescue coordination team (Navy)
RCTA	Regional Counterdrug Training Academy
RCU	rate changes unit; remote control unit
RCVR	receiver
RD	receive data; ringdown
RDA	research, development, and acquisition
RDCFP	Regional Defense Counterterrorism Fellowship Program
RDCTFP	Regional Defense Combating Terrorism Fellowship Program
RDD	radiological dispersal device; required delivery date
RDECOM	US Army Research, Development, and Engineering Command
RDF	radio direction finder; rapid deployment force
RDO	request for deployment order
RDT&E	research, development, test and evaluation
REACT	rapid execution and combat targeting
REAC/TS	radiation emergency assistance center/training site (DOE)
READY	resource augmentation duty program
RECA	Residual Capability Assessment
RECAS	residual capability assessment system
RECAT	residual capability assessment team
RECCE	reconnaissance
RECMOB	reconstitution-mobilization
RECON	reconnaissance
RED	radiological exposure device
RED HORSE	rapid engineer deployable heavy operational repair squadron engineer

REF	Rapid Equipping Force (Army); reference(s)
REGT	regiment
REL	relative
RELCAN	releasable to Canada
REMT	regional emergency management team
REMUS	remote environmental monitoring unit system
REPOL	bulk petroleum contingency report; petroleum damage and deficiency report; reporting emergency petroleum, oils, and lubricants
REPSHIP	report of shipment
REPUNIT	reporting unit
REQCONF	request confirmation
REQSTATASK	air mission request status tasking
RES	radiation exposure status
RESA	research, evaluation, and system analysis
RESCAP	rescue combat air patrol
RESCORT	rescue escort
RESPROD	responsible production
RET	retired
RF	radio frequency; reserve force
RFA	radio frequency authorization; request for assistance; restrictive fire area
RFC	request for capabilities; response force commander; revision final coordination
RF CM	radio frequency countermeasures
RFD	revision first draft
RF/EMPINT	radio frequency/electromagnetic pulse intelligence
RFF	request for feedback; request for forces
RFI	radio frequency interference; ready for issue; request for information
RFID	radio frequency identification
RFL	restrictive fire line
RFP	request for proposal
RFS	request for service; request for support
RFW	request for waiver
RG	reconstitution group
RGR	Rangers
RGS	remote geospatial intelligence services
RH	reentry home
Rh	Rhesus
RHIB	rigid hull inflatable boat
RI	Refugees International; routing indicator
RIB	rubberized inflatable boat
RIC	routing indicator code
RICO	regional interface control officer
RIG	recognition identification group

RIK	replacement in kind
RIMS	registrant information management system
RIP	register of intelligence publications
RIS	reconnaissance information system
RISOP	red integrated strategic offensive plan
RISTA	reconnaissance, intelligence, surveillance, and target acquisition
RIT	remote imagery transceiver
RIVRON	riverine squadron
RJTD	reconstitution joint table of distribution
RLD	ready-to-load date
RLE	rail liaison element
RLG	ring laser gyro
RLGM	remote loop group multiplexer
RLGM/CD	remote loop group multiplexer/cable driver
RLP	remote line printer
RM	ramp module; recovery mechanism; resource management; risk management
RMC	remote multiplexer combiner; rescue mission commander; Resource Management Committee (CSIF); returned to military control
RMKS	remarks
RMO	regional Marine officer
RMP	religious ministry professional
RMS	requirements management system; root-mean-square
RMT	response management team
RMU	receiver matrix unit
RNAV	area navigation
RNP	remote network processor
R/O	receive only
Ro	search radius rounded to next highest whole number
ROC	regional operations center; rehearsal of concept; required operational capability
ROCU	remote orderwire control unit
ROE	rules of engagement
ROEX	rules of engagement exercise
ROG	railhead operations group
ROICC	resident officer in charge of construction
ROK	Republic of Korea
ROM	read-only memory; restriction of movement; rough order of magnitude
ROMO	range of military operations
RON	remain overnight
RO/RO	roll-on/roll-off
ROS	reduced operating status
ROTC	Reserve Officer Training Corps

ROTHR	relocatable over-the-horizon backscatter radar (USN)
ROWPU	reverse osmosis water purification unit
ROZ	restricted operations zone
RP	reconstitution priority; release point (road); religious program specialist; retained personnel
RPG	rocket propelled grenade
RPM	revolutions per minute
RPO	rendezvous and proximity operations
RPOE	rapid port opening element
RPPO	Requirements, Plans, and Policy Office
RPT	report
RPTOR	reporting organization
RPV	remotely piloted vehicle
RQMT	requirement
RQT	rapid query tool
RR	reattack recommendation
RRC	regional reporting center
RRCC	regional response coordination center
RRDF	roll-on/roll-off discharge facility
RRF	rapid reaction force; rapid response force; Ready Reserve Fleet; Ready Reserve Force
RRPP	rapid response planning process
RS	rate synthesizer; religious support; requirement submission
RSA	retrograde storage area
RSC	red station clock; regional service center; rescue sub-center
RSD	reporting of supply discrepancy
RSE	retrograde support element
RSG	reference signal generator
RSI	rationalization, standardization, and interoperability
RSL	received signal level
RSN	role specialist nation
RSO	reception, staging, and onward movement; regional security officer; remote split operations
RSOC	regional signals intelligence (SIGINT) operations center
RSOI	reception, staging, onward movement, and integration
RSP	recognized surface picture; Red Switch Project (DOD); religious support policy
RSPA	Research and Special Programs Administration
RSS	radio subsystem; really simple syndication; remote sensors subsystem; root-sum-squared
RSSC	regional satellite communications support center; regional satellite support cell; regional signals intelligence (SIGINT) support center (NSA); regional space support center
RSSC-LO	regional satellite communications support center liaison officer; regional space support center liaison officer

RST	religious support team
RSTA	reconnaissance, surveillance, and target acquisition
RSTV	real-time synthetic video
RSU	rapid support unit; rear support unit; remote switching unit
R/T	receiver/transmitter
RT	recovery team; remote terminal; rough terrain
RTA	residual threat assessment
RTB	return to base
RTCC	rough terrain container crane
RTCH	rough terrain container handler
RTD	returned to duty
RTF	regional task force; return to force
RTFL	rough terrain forklift
RTG	radar target graphic
RTL	restricted target list
RTLP	receiver test level point
RTM	real-time mode
RTS	remote transfer switch
RTTY	radio teletype
RU	release unit; rescue unit
RUF	rules for the use of force
RUIC	Reserve unit identification number
RUSCOM	rapid ultrahigh frequency (UHF) satellite communications
RV	long-range seagoing rescue vessel; rekeying variable; rendezvous
RVR	runway visibility recorder
RVT	remote video terminal
RW	rotary-wing
RWCM	regional wartime construction manager
RWR	radar warning receiver
RWS	rawinsonde subsystem
RX	receive; receiver
RZ	return-to-zero

S

618 AOC (TACC)	618 Air Operations Center (Tanker Airlift Control Center)
S&F	store-and-forward
S&R	search and recovery
S&T	science and technology; scientific and technical
S&TI	scientific and technical intelligence
S-1	battalion or brigade manpower and personnel staff officer (Marine Corps battalion or regiment)
S-2	battalion or brigade intelligence staff officer (Army; Marine Corps battalion or regiment)
S-3	battalion or brigade operations staff officer (Army; Marine Corps battalion or regiment)
S-4	battalion or brigade logistics staff officer (Army; Marine Corps battalion or regiment)
SA	security assistance; selective availability (GPS); senior adviser; situational awareness; staging area; stand-alone switch
SAA	senior airfield authority
SAAFR	standard use Army aircraft flight route
SAAM	special assignment airlift mission
SAB	scientific advisory board (USAF)
SABER	situational awareness beacon with reply
SAC	special actions cell; special agent in charge; supporting arms coordinator
SACC	supporting arms coordination center (USMC)
SACEUR	Supreme Allied Commander, Europe (NATO)
SACLANT	Supreme Allied Command, Atlantic
SACS	secure telephone unit (STU) access control system
SACT	Supreme Allied Commander Transformation
SADC	sector air defense commander
SADL	situation awareness data link
SADO	senior air defense officer
SAF	Secretary of the Air Force
SAFE	secure analyst file environment; selected area for evasion; sexual assault forensic examination
SAFE-CP	selected area for evasion-contact point
SAFER	evasion and recovery selected area for evasion (SAFE) area activation request
SAFWIN	secure Air Force weather information network
SAG	surface action group
SAI	sea-to-air interface; single agency item
SAL	small arms locker
SAL-GP	semiactive laser-guided projectile (USN)
SALM	single-anchor leg mooring
SALT	supporting arms liaison team

SALTS	streamlined automated logistics transfer system; streamlined automated logistics transmission system
SALUTE	size, activity, location, unit, time, and equipment
SAM	special airlift mission; surface-to-air missile
SAMM	security assistance management manual
SAMS	School of Advanced Military Studies
SAO	security assistance office; security assistance officer; selected attack option
SAOC	sector air operations center
SAP	special access program
SAPI	special access program for intelligence
SAPO	subarea petroleum office
SAPR	sexual assault prevention and response
SAR	satellite access request; search and rescue; site access request; special access requirement; suspicious activity report; synthetic aperture radar
SARC	sexual assault response coordinator; surveillance and reconnaissance center
SARDOT	search and rescue point
SARIR	search and rescue incident report
SARMIS	search and rescue management information system
SARNEG	search and rescue numerical encryption group
SAROPS	Search and Rescue Optimal Planning System
SARREQ	search and rescue request
SARSAT	search and rescue satellite-aided tracking
SARSIT	search and rescue situation summary report
SARTEL	search and rescue (SAR) telephone (private hotline)
SARTF	search and rescue task force
SAS	sealed authenticator system; special ammunition storage
SASP	special ammunition supply point
SASS	supporting arms special staff
SASSY	supported activities supply systems
SAT	satellite
SATCOM	satellite communications
SAW	surface acoustic wave
SB	standby base
SBCT	Stryker brigade combat team
SBL	space-based laser
SBPO	Service blood program officer
SBRPT	subordinate reporting organization
SBS	senior battle staff; support battle staff
SBSS	science-based stockpile stewardship
SBSO	sustainment brigade special operations
SBU	sensitive but unclassified; special boat unit
SC	sea current; search and rescue coordinator; security cooperation; station clock; strategic communication

SCA	sociocultural analysis; space coordinating authority; support to civil administration
SCAR	strike coordination and reconnaissance
SCAS	stability control augment system
SCATANA	security control of air traffic and navigation aids
SC ATLANTIC	Strategic Command, Atlantic (NATO)
SCATMINE	scatterable mine
SCATMINEWARN	scatterable minefield warning
SCC	security classification code; service cryptologic Component; shipping coordination center; Standards Coordinating Committee
SCC-WMD	United States Strategic Command Center for Combating Weapons of Mass Destruction
SCDL	surveillance control data link
SCE	Service cryptologic element
SC EUROPE	Strategic Command, Europe (NATO)
SCF(UK)	Save the Children Fund (United Kingdom)
SCF(US)	Save the Children Federation (United States)
SCG	Security Cooperation Guidance; switching controller group
SCHBT	shape, clear, hold, build, and transition
SCI	security and counterintelligence interviews; sensitive compartmented information
SCIF	sensitive compartmented information facility
SCL	standard conventional load
SCM	security countermeasure; Service container manager
SCMP	strategic command, control, and communications (C3) master plan
SCNE	self-contained navigation equipment
SCO	secondary control officer; security cooperation organization; senior contracting official; state coordinating officer
SCOC	systems control and operations concept
SCONUM	ship control number
SCP	secure conferencing project; security cooperation plan; service control point; system change proposal
SCPT	strategic connectivity performance test
SCRB	software configuration review board
S/CRS	Office of the Coordinator for Reconstruction and Stabilization (DOS)
SCT	shipping coordination team; single channel transponder
S/CT	Office of the Coordinator for Counterterrorism (DOS)
SCTIS	single channel transponder injection system
SCTS	single channel transponder system
SCT-UR	single channel transponder ultrahigh frequency (UHF) receiver
SCUD	surface-to-surface missile system

SD	strategy division
SDA	senior development advisor; Seventh-Day Adventist (ADRA)
SDB	Satellite Communications Database; small diameter bomb
SDDC	Military Surface Deployment and Distribution Command
SDDCTEA	Surface Deployment and Distribution Command Transportation Engineering Agency
SDF	self defense force
SDIO	Strategic Defense Initiative Organization
SDLS	satellite data link standards
SDMX	space division matrix
SDN	system development notification
SDNRIU	secure digital net radio interface unit
SDO	senior defense official; ship's debarkation officer
SDO/DATT	senior defense official/defense attaché
SDP	strategic distribution platform
SDR	system design review
SDSG	space division switching group
SDSM	space division switching matrix
SDV	SEAL team delivery vehicle; submerged delivery vehicle
SDZ	self-defense zone
SE	site exploitation; spherical error
SEA	ships' bunkers easy acquisition; Southeast Asia
Seabee	Navy construction engineer
SEAD	suppression of enemy air defenses
SEC	submarine element coordinator
SECAF	Secretary of the Air Force
SECARMY	Secretary of the Army
SecDef	Secretary of Defense
SECDHS	Secretary of the Department of Homeland Security
SECHS	Secretary of Homeland Security
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy instruction
SECOMP	secure en route communications package
SECORD	secure cord switchboard
SECRA	secondary radar data only
SECSTATE	Secretary of State
SECTRANS	Secretary of Transportation
SED	signals external data
SEDAS	spurious emission detection acquisition system
SEF	sealift enhancement feature
SEI	specific emitter identification
SEL	senior enlisted leader
SEL REL	selective release
SELRES	Selected Reserve

SEMA	special electronic mission aircraft
SEMS	standard embarkation management system
SEO/SEP	special enforcement operation/special enforcement program
SEP	signal entrance panel; spherical error probable
SEPLO	state emergency preparedness liaison officer
SERE	survival, evasion, resistance, and escape
SERER	survival, evasion, resistance, escape, recovery
SES	senior executive service
SETA	system engineering and technical assistance
SEW	shared early warning
S/EWCC	signals intelligence/electronic warfare coordination center
SEWG	Special Events Working Group
SEWOC	signals intelligence/electronic warfare operations centre (NATO)
SEWS	satellite early warning system
SF	security force; security forces (Air Force or Navy); single frequency; special forces; standard form
SFA	security force assistance
SFAF	standard frequency action format
SFAT	spectrum flyaway team
SFC	single-fuel concept
SFCP	shore fire control party
SFG	security forces group; special forces group
SFI	spectral composition
SFLEO	senior federal law enforcement official
SFMS	special forces medical sergeant
SFOD-A/B/C	special forces operational detachment-A/B/C
SFOR	Stabilization Force
SFS	security forces squadron
SG	steering group; strike group; supergroup; surgeon general
SGEMP	system-generated electromagnetic pulse
SGS	strategic guidance statement
SGSA	squadron group systems advisor
SGXM	Headquarters, Air Mobility Command/Surgeon
SHAPE	Supreme Headquarters Allied Powers, Europe
SHD	special handling designator
SHF	super-high frequency
SHORAD	short-range air defense
SHORADEZ	short-range air defense engagement zone
SI	special intelligence; United States Strategic Command strategic instruction
SIA	station of initial assignment
SIAGL	survey instrument azimuth gyroscope lightweight
SIC	subject identification code; supporting intelligence center
SICO	sector interface control officer

SID	standard instrument departure
SIDAC	single integrated damage analysis capability
SIDL	standard intelligence documents list
SIDO	senior intelligence duty officer
SIDS	secondary imagery dissemination system
SIF	selective identification feature; strategic internment facility
SIG	signal
SIGINT	signals intelligence
SII	statement of intelligence interest
SIM	system impact message
SIMLM	single integrated medical logistics management; single integrated medical logistics manager
SINCGARS	single-channel ground and airborne radio system
SINS	ship's inertial navigation system
SIO	senior intelligence officer
SIOC	Strategic Information and Operations Center (FBI)
SIOP	Single Integrated Operational Plan
SIOP-ESI	Single Integrated Operational Plan-Extremely Sensitive Information
SIPRNET	SECRET Internet Protocol Router Network
SIR	serious incident report; specific information requirement; Strategic Military Intelligence Review
SIRADS	stored imagery repository and dissemination system
SIRMO	senior information resources management official
SIS	special information systems
SITREP	situation report
SIV	special interest vessel
SJA	staff judge advocate
SJFHQ	standing joint force headquarters
SJFHQ(CE)	standing joint force headquarters (core element)
SJFHQ-E	standing joint force headquarters – elimination
SJFHQ-N	Standing Joint Force Headquarters - North
SJS	Secretary, Joint Staff
SKE	station-keeping equipment
SL	sea level; switch locator
SLA	service level agreement; special leave accrual
SLAM	stand-off land attack missile
SLBM	submarine-launched ballistic missile
SLC	satellite laser communications; single line concept
SLCM	sea-launched cruise missile
SLCP	ship lighterage control point; ship's loading characteristics pamphlet
SLD	system link designator
SLEP	service life extension program
SLGR	small, lightweight ground receiver (GPS)
SLIT	serial-lot item tracking

SLO	space liaison officer
SLOC	sea line of communications
SLRP	survey, liaison, and reconnaissance party
SLWT	side loadable warping tug
SM	Secretary, Joint Staff, memorandum; Service manager; spectrum management; staff memorandum; system manager
SMA	special military information support operations assessment
SMART	special medical augmentation response team
SMART-AIT	special medical augmentation response - aeromedical isolation team
SMB	spectrum management branch
SMC	midpoint compromise track spacing; search and rescue mission coordinator; system master catalog
SMCA	single manager for conventional ammunition
SMCC	strategic mobile command center
SMCM	surface mine countermeasures
SMCOO	spectrum management concept of operations
SMCR	Selected Marine Corps Reserve
SMD	strategic missile defense
SMDC	Space & Missile Defense Command (Army)
SMDC/ARSTRAT	United States Army Space and Missile Defense Command/United States Army Forces Strategic Command
SME	subject matter expert
SMEB	significant military exercise brief
SMEO	small end office
SMFT	semi-trailer mounted fabric tank
SMI	security management infrastructure
SMIO	search and rescue (SAR) mission information officer
SMO	senior meteorological and oceanographic officer; strategic mobility office(r); support to military operations
SMP	sub-motor pool
SMPT	School of Military Packaging Technology
SMRC	Specialized Medical Response Capabilities
SMRI	service message routing indicator
SMS	Single Mobility System; special military information support operations study
SMTP	simple message transfer protocol
SMU	special mission unit; supported activities supply system (SASSY) management unit
S/N	signal to noise
SN	serial number
SNA	social network analysis
SNCO	staff noncommissioned officer

SNF	strategic nuclear forces
SNIE	special national intelligence estimates
SNLC	Senior North Atlantic Treaty Organization (NATO) Logisticians Conference
SNM	system notification message
SNOI	signal not of interest
SO	safety observer
SOA	separate operating agency; special operations aviation (Army); status of action; sustained operations ashore
SOAF	status of action file
SOAGS	special operations air-ground system
SOC	security operations center; special operations commander; special operations component
SOCA	special operations communications assembly
SOCC	Sector Operations Control Center (NORAD)
SOCCE	special operations command and control element
SOCCENT	Special Operations Component, United States Central Command
SOCCET	special operations critical care evacuation team
SOCEUR	Special Operations Component, United States European Command
SOCEX	special operations capable exercise
SOC-FWD	special operations command-forward
SOCJFCOM	Special Operations Command, Joint Forces Command
SOCM	special operations combat medic
SOCOORD	special operations coordination element
SOCP	special operations communication package
SOCPAC	Special Operations Command, Pacific
SOCRATES	Special Operations Command, Research, Analysis, and Threat Evaluation System
SOCSOUTH	Special Operations Component, United States Southern Command
SOD	special operations division; strategy and options decision (Planning, Programming, and Budgeting System)
SODARS	special operations debrief and retrieval system
SOE	special operations executive
SOF	special operations forces; supervisor of flying
SOFA	status-of-forces agreement
SOFAR	sound fixing and ranging
SOF-CF	special operations forces-conventional forces
SOFLAM	special operations laser marker
SOFLE	special operations forces liaison element
SOFME	special operations forces medical element
SOFSA	special operations forces support activity
SOG	special operations group

SOI	signal of interest; signal operating instructions; space object identification
SOIC	senior officer of the intelligence community
SOJTF	special operations joint task force
SOLAS	safety of life at sea
SOLE	special operations liaison element
SOLIS	signals intelligence (SIGINT) On-line Information System
SOLL	special operations low-level
SOLO	special operations liaison officer
SOM	satellite communications (SATCOM) operational manager; start of message; system operational manager
SOMA	status of mission agreement
SOMARDS	Standard Operation and Maintenance Army Research and Development System
SOMARDS NT	Standard Operation and Maintenance Army Research and Development System Non-Technical
SoO	ship of opportunity
SOOP	Center for Operations, Plans, and Policy
SOP	standard operating procedure
SOR	statement of requirement
SORTIEALOT	sortie allotment message
SORTS	Status of Resources and Training System
SOS	special operations squadron
SOSB	special operations support battalion
SOSC	special operations support command (theater army)
SOSCOM	special operations support command
SOSE	special operations staff element
SOSG	station operations support group
SOSR	suppress, obscure, secure, and reduce
SOST	special operations support team
SOTA	signals intelligence operational tasking authority
SOTF	special operations task force
SOTSE	special operations theater support element
SOUTHAF	Southern Command Air Forces
SOUTHROC	Southern Region Operational Center (USSOUTHCOM)
SOW	special operations wing; standoff weapon; statement of work
SOWT	special operations weather team
SP	security police
SPACEAF	Space Air Forces
SPACECON	control of space information
SPCC	ships parts control center (USN)
SPE	senior procurement executive
SPEAR	strike protection evaluation and antiair research
SPEC	specified
SPECAT	special category

SPECWAR	special warfare
SPG	Strategic Planning Guidance
SPI	sensor point of interest; special investigative (USAF)
SPINS	special instructions
SPINTCOMM	special intelligence communications handling system
SPIREP	spot intelligence report
SPLX	simplex
SPM	service postal manager; single point mooring; single port manager
SPMAGTF	special purpose Marine air-ground task force
SPO	system program office
SPOC	search and rescue (SAR) points of contact; space command operations center
SPOD	seaport of debarkation
SPOE	seaport of embarkation
SPOT	Synchronized Predeployment and Operational Tracker
SPOTREP	spot report
SPP	Security and Prosperity Partnership of North America; shared production program; State Partnership Program (NG)
SPR	software problem report
SPRINT	special psychiatric rapid intervention team
SPS	standard positioning service
SPSC	system planning and system control
SPTCONF	support confirmation
SPTD CMD	supported command
SPTG CMD	supporting command
SPTREQ	support request
sqft	square feet
SR	special reconnaissance
SRA	specialized-repair activity
SRAM	short-range air-to-surface attack missile; system replacement and modernization
SRB	software release bulletin; system review board (JOPES)
SRBM	short-range ballistic missile
SRC	security risk category; service reception center; Single Integrated Operational Plan (SIOP) response cell; standard requirements code; survival recovery center
SRCC	service reserve coordination center
SRF	secure Reserve force
SRG	Seabee readiness group; short-range aircraft
SRI	surveillance, reconnaissance, and intelligence (Marine Corps)
SRIG	surveillance, reconnaissance, and intelligence group (USMC)
SRM	sustainment, restoration, and modernization
SROC	Senior Readiness Oversight Council; Southern Region

	Operational Center, United States Southern Command
SROE	standing rules of engagement
SRP	sealift reserve program; Single Integrated Operational Plan (SIOP) reconnaissance plan
SRP/PDS	stabilization reference package/position determining system
SRR	search and rescue region
SRS	search and rescue sector
SRSG	special representative of the Secretary-General
SRT	scheduled return time; special reaction team; standard remote terminal; strategic relocatable target
SRTD	signals research and target development
S/RTF	search and recovery task force
SRU	search and rescue unit
SR-UAV	short-range unmanned aerial vehicle
SRUF	standing rules for the use of force
SRWBR	short range wide band radio
S/S	steamship
SS	submarine
SSA	software support activity; space situational awareness; special support activity (NSA); strapdown sensor assembly; supply support activity; supply support area
SSB	single side band; support services branch; surveillance support branch
SSB-SC	single sideband-suppressed carrier
SSC	small scale contingency; special security center surveillance support center
SSCO	shipper's service control office
SSCRA	Soldiers and Sailors Civil Relief Act
SSD	strategic studies detachment
SSE	satellite communications (SATCOM) systems expert; space support element
SSF	software support facility
SSI	standing signal instruction
SSM	surface-to-surface missile
SSMI	special sensor microwave imager
SSMS	single shelter message switch
SSN	attack submarine, nuclear; Social Security number; space surveillance network
SS (number)	sea state (number)
SSO	special security office(r); spot security office
SSP	signals intelligence (SIGINT) support plan
SSPM	single-service postal manager
SSPO	strategic systems program office
SSR	security sector reform

SSS	Selective Service System; shelter subsystem
SSSC	surface, subsurface search surveillance coordination
SST	special support team (National Security Agency)
SSTR	stability, security, transition, and reconstruction
SSWG	space support working group
ST	short ton; small tug; strike team
S/T	short ton
ST&E	security test and evaluation
STA	system tape A
STAB	space tactical awareness brief
STA clk	station clock
STAMMIS	standard Army multi-command management information system
STAMP	standard air munitions package (USAF)
STANAG	standardization agreement (NATO)
STANAVFORLANT	Standing Naval Forces, Atlantic (NATO)
STAR	scheduled theater airlift route; sensitive target approval and review; standard attribute reference; standard terminal arrival route; surface-to-air recovery; system threat assessment report
STARC	state area coordinators
STARS	Standard Accounting and Reporting System
START	Strategic Arms Reduction Treaty
STARTEX	start of exercise
STB	super tropical bleach
STC	secondary traffic channel
STD	sexually transmitted disease
STDM	synchronous time division multiplexer
STE	secure telephone equipment
S-Team	staff augmentation team
STEL STU III	Standford telecommunications (secure telephone)
STEP	software test and evaluation program; standardized tactical entry point; standard tool for employment planning
STG	seasonal target graphic
STICS	scalable transportable intelligence communications system
STO	special technical operations
STOC	special technical operations coordinator
STOD	special technical operations division
STOL	short takeoff and landing
STOMPS	stand-alone tactical operational message processing system
STON	short ton
STP	security technical procedure
STR	strength
STRAPP	standard tanks, racks and pylons packages (USAF)
STRATOPS	strategic operations division
STREAM	standard tensioned replenishment alongside method

STS	special tactics squadron
STT	small tactical terminal; special tactics team
STU	secure telephone unit
STU-III	secure telephone unit III
STW	strike warfare
STWC	strike warfare commander
STX	start of text
SU	search unit
SUBJ	subject
sub-JIB	subordinate-joint information bureau
SUBOPAUTH	submarine operating authority
sub-PIC	subordinate-press information center
SUBROC	submarine rocket
SUC	surf current
SUIC	service unit identification code
SUMMITS	scenario unrestricted mobility model of intratheater simulation
SUPE	supervisory commands program
SUPP	supplement
SUPPO	supply officer
SURG	surgeon
SUROBS	surf observation
SURPIC	surface picture
SUST BDE	sustainment brigade
SUW	surface warfare
SUWC	surface warfare commander
S/V	sailboat
SVC	Service; stored value card
SVIP	secure voice improvement program
SVLTU	service line termination unit
SVR	surface vessel radar
SVS	secure voice system
Sw	switch
SWA	Southwest Asia
SWAT	special weapons and tactics
SWBD	switchboard
SWC	strike warfare commander; swell/wave current
SWI	special weather intelligence
SWO	staff weather officer
SWORD	submarine warfare operations research division
SWPC	Space Weather Prediction Center
SWSOCC	Southwest Sector Operation Control Center North American Aerospace Defense Command (NORAD)
SWXS	Space Weather Squadron
SXXI	SPECTRUM XXI
SXXI-O	SPECTRUM XXI-Online

SYDP	six year defense plan
SYG	Secretary-General (UN)
SYNC	synchronization
SYS	system
SYSCOM	systems command
SYSCON	systems control
SZ	surf zone

T

2-D	two-dimensional
2E	Role 2 enhanced
2LM	Role 2 light maneuver
3-D	three-dimensional
T	search time available; short ton; trackline pattern
T&DE	test and diagnostic equipment
T&E	test and evaluation
T2	technology transfer
TA	target acquisition; target audience; technical arrangement; theater Army; threat assessment
TAA	tactical assembly area; target audience analysis
TAACOM	theater Army area command
TAADS	The Army Authorization Document System
TAAMDCOORD	theater Army air and missile defense coordinator
TAB	tactical air base
TAC	tactical advanced computer; terminal access controller; terminal attack control; terminal attack controller
TAC(A)	tactical air coordinator (airborne)
TACAIR	tactical air
TACAMO	take charge and move out (E-6A/B aircraft)
TACAN	tactical air navigation
TACC	tanker airlift control center
TAC-D	tactical deception
TACDAR	tactical detection and reporting
TACINTEL	tactical intelligence
TACLAN	tactical local area network
TACLOG	tactical-logistical
TACM	tactical air command manual
TACO	theater allied contracting office
TACON	tactical control
TACOPDAT	tactical operational data
TA/CP	technology assessment/control plan
TACP	tactical air control party
TACRON	tactical air control squadron
T-ACS	auxiliary crane ship
TACS	tactical air control system; theater air control system
TACSAT	tactical satellite
TACSIM	tactical simulation
TACSTANS	tactical standards
TACT	tactical aviation control team
TACTRAGRULANT	Tactical Training Group, Atlantic
TAD	tactical air direction; temporary additional duty (non-unit-related personnel); theater air defense; time available for delivery

TADC	tactical air direction center
TADCS	tactical airborne digital camera system
TADS	Tactical Air Defense System; target acquisition system and designation sight
TAES	theater aeromedical evacuation system
TAF	tactical air force
TAFIM	technical architecture framework for information management
TAFS	tactical aerodrome forecasts
TAFT	technical assistance field team
TAG	technical assessment group; technical assistance group; the adjutant general; Tomahawk land-attack missile aimpoint graphic
T-AGOS	tactical auxiliary general ocean surveillance
TAGS	theater air-ground system
T-AH	hospital ship
TAI	target area of interest; total active inventory
TAIS	transportation automated information systems
TAK	cargo ship
T-AKR	fast logistics ship
TALD	tactical air-launched decoy
TALON	Threat and Local Observation Notice
TAMCA	theater Army movement control agency
TAMCO	theater Army movement control center
TAMD	theater air and missile defense
TAMMC	theater army material management command
TAMMIS	theater Army medical management information system
TAMS	transportation analysis, modeling, and simulation
tanalt	tangent altitude
TAO	tactical action officer; tactical air officer
TAOC	tactical air operations center (USMC)
TAP	troopship
TAR	tactical air request; Training and Administration of the Reserve
TARBS	transportable amplitude modulation and frequency modulation radio broadcast system
TARBUL	target bulletin
TARE	tactical record evaluation
TAREX	target exploitation; target plans and operations
TARS	tethered aerostat radar system
TARWI	target weather and intelligence
TAS	tactical atmospheric summary; true air speed
T-ASA	Television Audio Support Agency
TASCID	tactical Automatic Digital Network (AUTODIN) satellite compensation interface device
TASCO	tactical automatic switch control officer

TASIP	tailored analytic intelligence support to individual electronic warfare and command and control warfare projects
TASKORD	tasking order
TASMO	tactical air support for maritime operations
TASOSC	theater Army special operations support command
TASS	tactical automated security system; tactical automated switch system
TASWC	theater antisubmarine warfare commander
TAT	tactical analysis team; technical assistance team
TATC	tactical air traffic control
T-AVB	aviation logistics support ship
TAW	tactical airlift wing
TBC	theater business clearance
TBD	to be determined
TBM	tactical ballistic missile; theater ballistic missile
TBMCS	theater battle management core system
TBMD	theater ballistic missile defense
TB MED	technical bulletin medical
TBP	to be published
TBSL	to be supplied later
TBTC	transportable blood transshipment center
TC	tidal current; transmit clock and/or telemetry combiner; training circular; Transportation Corps (Army)
TCA	time of closest approach; traditional combatant commander activity
TC-ACCIS	Transportation Coordinator's Automated Command and Control Information System
TC-AIMS	Transportation Coordinator's Automated Information for Movement System
TC-AIMS II	Transportation Coordinator's Automated Information for Movement System II
TCAM	theater Army medical management information system (TAMMIS) customer assistance module
TCC	transmission control code; transportation component command
TCCF	tactical communications control facility
TCEM	theater contingency engineering management
TCF	tactical combat force; technical control facility
TCM	theater construction manager; theater container manager
TCMD	transportation control and movement document
TCN	third country national; transportation control number; troop contributing nations
TCO	termination contracting office;r transnational criminal organization
TCP	theater campaign plan

TCPED	tasking, collection, processing, exploitation, and dissemination
TCS	theater communications system
TCSEC	trusted computer system evaluation criteria
TCSP	theater consolidation and shipping point
TD	temporary duty; theater distribution; tie down; timing distributor; total drift; transmit data
TDA	Table of Distribution and Allowance
TDAD	Table of Distribution and Allowance (TDA) designation
TDBM	technical database management
TDBSS	Theater Defense Blood Standard System
TDC	target development cell
TDD	target desired ground zero (DGZ) designator; time-definite delivery
TDF	tactical digital facsimile; theater detention facility
TDIC	time division interface controller
TDIG	time division interface group
TDIM	time division interface module
TDL	tactical data link
TDM	time division multiplexed
TDMA	time division multiple access
TDMC	theater distribution management cell
TDMF	time division matrix function
TDMM	time division memory module
TDMX	time division matrix
TDN	tactical data network; target development nomination
TDP	theater distribution plan
TDR	transportation discrepancy report
TDRC	theater detainee reporting center
TDSG	time division switching group
TDSGM	time division switching group modified
TDT	theater display terminal
TDY	temporary duty
TE	transaction editor
TEA	Transportation Engineering Agency
TEC	theater engineer command
tech	technical
TECHCON	technical control
TECHELINT	technical electronic intelligence
TECHEVAL	technical evaluation
TECHINT	technical intelligence
TECHOPDAT	technical operational data
TECS II	Treasury Enforcement Communications System
TED	trunk encryption device
TEDAC	Terrorist Explosive Device Analytical Center (FBI)
TEK	TeleEngineering Kit

TEL	transporter-erector-launcher
TELEX	teletype
TELINT	telemetry intelligence
TELNET	telecommunication network
TEMPER	tent extendible modular personnel
TENCAP	tactical exploitation of national capabilities program
TEO	team embarkation officer
TEOB	tactical electronic order of battle
TEP	test and evaluation plan; theater engagement plan
TERCOM	terrain contour matching
TERPES	tactical electronic reconnaissance processing and evaluation system
TERPROM	terrain profile matching
TERS	tactical event reporting system
TES	theater event system
TESS	Tactical Environmental Support System
TET	targeting effects team
TETK	TeleEngineering Toolkit
TEU	technical escort unit; twenty-foot equivalent unit
TEWLS	Theater Enterprise Wide Logistics System
TF	task force
TFA	toxic free area
TFADS	Table Formatted Aeronautic Data Set
TFC	threat finance cell
TFCICA	task force counterintelligence coordinating authority
TFE	tactical field exchange; threat finance exploitation; transportation feasibility estimator
TFF	total force fitness
TFLIR	targeting forward-looking infrared
TFMS-M	Transportation Financial Management System-Military
TFR	temporary flight restriction
TFS	tactical fighter squadron; Tactical Forecast System
TG	task group
TGC	trunk group cluster
TGEN	table generate
TGM	terminally guided munitions; trunk group multiplexer
TGMOW	transmission group module and/or orderwire
TGO	terminal guidance operations
TGT	target
TGTINFOREP	target information report
TGU	trunk compatibility unit
THAAD	Terminal High Altitude Area Defense
THT	tactical human intelligence team
THX	theater express
TI	threat identification; training instructor
TIA	theater intelligence assessment

TIAP	theater intelligence architecture program
TIB	theater intelligence brigade; toxic industrial biological
TIBS	tactical information broadcast service
TIC	target information center; toxic industrial chemical
TIDE	Terrorist Identities Datamart Environment
TIDP	technical interface design plan
TIDS	tactical imagery dissemination system
TIF	theater internment facility
TIFF	tagged image file format
TII	total inactive inventory
TIM	theater information management; toxic industrial material
TIO	target intelligence officer
TIP	target intelligence package; trafficking in persons
TIPG	telephone interface planning guide
TIPI	tactical information processing interpretation
TIPS	tactical optical surveillance system (TOSS) imagery processing system
TIR	toxic industrial radiological
TIROS	television infrared observation satellite
TIS	technical interface specification; thermal imaging system
TISG	technical interoperability standards group
TISS	thermal imaging sensor system
TJAG	the judge advocate general
T-JMC	theater-joint movement center
T-JTB	theater-joint transportation board
TJTN	theater joint tactical network
TL	team leader
TLA	theater logistics analysis
TLAM	Tomahawk land-attack missile
TLAMM	theater lead agent for medical materiel
TLAM/N	Tomahawk land attack missile/nuclear
TLC	traffic load control
TLE	target location error
TLM	target list management; topographic line map
TLO	theater logistics overview
TLP	transmission level point
TLR	trailer
TLX	teletype
TM	tactical missile; target materials; team member; technical manual; TROPO modem
TMAO	theater mortuary affairs office; theater mortuary affairs officer
TMB	tactical military information support operations battalion
TMD	tactical munitions dispenser; theater missile defense
TMEP	theater mortuary evacuation point
TMG	timing

TMIP	theater medical information program
TMIS	theater medical information system
TML	terminal
TMLMC	theater medical logistic management center
TMMMC	theater medical materiel management center
TMN	trackline multiunit non-return
TMO	traffic management office; transportation management office
TMP	target materials program; telecommunications management program; theater manpower forces
TMR	trackline multiunit return
T/M/S	type, model, and/or series
TMT	time-phased force and deployment data management tool
TNAPS	tactical network analysis and planning system
TNAPS+	tactical network analysis and planning system plus
TNC	theater network operations center
TNCC	theater network operations control center
TNCO	transnational criminal organization
T-net	training net
TNF	theater nuclear force
TNL	target nomination list
T/O	table of organization
TO	technical order; theater of operations
TO&E	table of organization and equipment
TOA	table of allowance
TOC	tactical operations center; tanker airlift control center (TALCE) operations center
TOCU	tropospheric scatter (TROPO) orderwire control unit
TOD	tactical ocean data; time of day
TOE	table of organization and equipment
TOF	time of flight
TOFC	trailer on flatcar
TOH	top of hill
TOI	track of interest
TOPINT	technical operational intelligence
TOR	term of reference; time of receipt
TOS	time on station
TOSS	tactical optical surveillance system
TOT	time on target
TOW	tube launched, optically tracked, wire guided
TP	technical publication; transportation priority; turn point
TPC	tactical pilotage chart
TPC/PC	tactical pilotage chart and/or pilotage chart
TPE	theater provided equipment

TPED	tasking, processing, exploitation, and dissemination; theater personal effects depot
TPERS	type personnel element
TPFDD	time-phased force and deployment data
TPFDL	time-phased force and deployment list
TPL	technical publications list; telephone private line
TPME	task, purpose, method, and effects
TPMRC	theater patient movement requirements center
TPO	task performance observation
TPRC	theater planning response cell
TPT	tactical petroleum terminal
TPTRL	time-phased transportation requirements list
TPU	tank pump unit
TQ	tactical questioning
TRA	technical review authority
TRAC2ES	United States Transportation Command Regulating and Command and Control Evacuation System
TRACON	terminal radar approach control facility
TRADOC	United States Army Training and Doctrine Command
TRAM	target recognition attack multisensor
Trans BDE	transportation brigade
Trans Det RPO	transportation detachment rapid port opening
TRANSEC	transmission security
TRAP	tactical recovery of aircraft and personnel (Marine Corps); tactical related applications; tanks, racks, adapters, and pylons; terrorism research and analysis program
TRC	tactical radio communication; transmission release code
TRCC	tactical record communications center
TRE	tactical receive equipment
TREAS	Department of the Treasury
TREE	transient radiation effects on electronics
TRIADS	Tri-Wall Aerial Distribution System
TRICON	triple container
TRI-TAC	Tri-Service Tactical Communications Program
TRK	truck; trunk
TRNG	training
TRO	training and readiness oversight
TROPO	troposphere; tropospheric scatter
TRP	target reference point
TRS	tactical reconnaissance squadron
TS	terminal service; time-sensitive; top secret
TSA	target system analysis; theater storage area; Transportation Security Administration (DHS); travel security advisory
TSB	technical support branch; trunk signaling buffer
TSBn	transportation support battalion (USMC)

TSC	theater security cooperation; theater support command; theater sustainment command (Army)
TSCIF	tactical sensitive compartmented information facility
TSCM	technical surveillance countermeasures
TSCO	target selection confusion of the operator; top secret control officer
TSCP	theater security cooperation plan
TSCR	time sensitive collection requirement
TSE	tactical support element
TSEC	transmission security
TSG	targeting support group; test signal generator
TSGCE	tri-Service group on communications and electronics
TSGCEE	tri-Service group on communications and electronic equipment (NATO)
TSM	trunk signaling message
TSN	trackline single-unit non-return; track supervision net
TSO	technical standard order; telecommunications service order
TSOC	tactical special operations command; theater special operations command
TSP	telecommunications service priority
TSR	telecommunications service request; theater source registry; theater support representative; trackline single-unit return
TSS	tactical shelter system; target sensing system; timesharing system; time signal set; traffic service station
TSSP	tactical satellite signal processor
TSSR	tropospheric scatter (TROPO)-satellite support radio
TST	tactical support team; terminal support team; theater support team; time-sensitive target
TSWA	temporary secure working area
TT	terminal transfer
TT&C	telemetry, tracking, and commanding
TTAN	transportation tracking account number
TTB	transportation terminal battalion
TTD	tactical terrain data; technical task directive
TTFACOR	targets, threats, friendlies, artillery, clearance, ordnance, restrictions
TTG	thermally tempered glass
TTL	tagging, tracking, and locating; transistor-transistor logic
TTM	threat training manual; training target material
TTN	transportation tracking number
TTP	tactics, techniques, and procedures; trailer transfer point
TTR	tactical training range
TTT	time to target
TTU	transportation terminal unit
TTY	teletype
TUBA	transition unit box assembly

TUCHA	type unit characteristics file
TUCHAREP	type unit characteristics report
TUDET	type unit equipment detail file
TV	television
TVA	Tennessee Valley Authority
TW&A	threat warning and assessment
TWC	Office for Counterterrorism Analysis (DIA); total water current
TWCF	Transportation Working Capital Fund
TWCM	theater wartime construction manager
TWD	transnational warfare counterdrug analysis
TWDS	tactical water distribution system
TWI	Office for Information Warfare Support (DIA)
TWPL	teletypewriter private line
TWX	teletypewriter exchange
TX	transmitter; transmit
TYCOM	type commander

U

U	wind speed
UA	unmanned aircraft
UAOBS	upper air observation
UAR	unconventional assisted recovery
UARCC	unconventional assisted recovery coordination cell
UAS	unmanned aircraft system
UAV	unmanned aerial vehicle
U/C	unit cost; upconverter
UCFF	Unit Type Code Consumption Factors File
UCMJ	Uniform Code of Military Justice
UCP	Unified Command Plan
UCT	underwater construction team
UDAC	unauthorized disclosure analysis center
UDC	unit descriptor code
UDESC	unit description
UDL	unit deployment list; unit designation list
UDP	unit deployment program
UDT	underwater demolition team
UE	unit equipment
UEWR	upgraded early warning radar
UFAC	Underground Facilities Analysis Center
UFC	Unified Facilities Criteria
UFO	ultrahigh frequency follow-on
UFR	unfunded requirement
UGA	ungoverned area
UGIRH	Urban Generic Information Requirements Handbook
UGM-84A	Harpoon
UGM-96A	Trident I
UGO	unified geospatial-intelligence operations
UHF	ultrahigh frequency
UHV	Upper Huallaga Valley
UIC	unit identification code
UICIO	unit identification code information officer
UIRV	unique interswitch rekeying variable
UIS	unit identification system
UJTL	Universal Joint Task List
UK	United Kingdom
UK(I)	United Kingdom and Ireland
ULC	unit level code
ULF	ultra low frequency
ULLS	unit level logistics system
ULN	unit line number
ULSD	ultra-low sulfur diesel
UMCC	unit movement control center

UMCM	underwater mine countermeasures
UMD	unit manning document; unit movement data
UMIB	urgent marine information broadcast
UMMIPS	uniform material movement and issue priority system
UMO	unit movement officer
UMPR	unit manpower personnel record
UMT	unit ministry team
UN	United Nations
UNAMIR	United Nations Assistance Mission in Rwanda
UNC	United Nations Command
UNCLOS	United Nations Convention on the Law of the Sea
UN CMCoord	United Nations humanitarian civil-military coordination
UNCTAD	United Nations Conference on Trade and Development
UND	urgency of need designator
UNDAC	United Nations disaster assessment and coordination
UNDFS	United Nations Department of Field Support
UNDHA	United Nations Department of Humanitarian Affairs
UN-DMT	United Nations disaster management team
UNDP	United Nations development programme
UNDPKO	United Nations Department for Peacekeeping Operations
UNEF	United Nations emergency force
UNEP	United Nations environment programme
UNESCO	United Nations Educational, Scientific, and Cultural Organization
UNHAS	United Nations Humanitarian Air Service
UNHCHR	United Nations High Commissioner for Human Rights
UNHCR	United Nations Office of the High Commissioner for Refugees
UNHQ	United Nations Headquarters
UNICEF	United Nations Children's Fund
UNIFIL	United Nations Interim Force in Lebanon
UNIL	unclassified national information library
UNITAF	unified task force
UNITAR	United Nations Institute for Training and Research
UNITREP	unit status and identity report
UNJLC	United Nations Joint Logistic Centre
UNLOC	United Nations logistic course
UNMEM	United Nations military expert on mission
UNMIH	United Nations Mission in Haiti
UNMILPOC	United Nations military police course
UNMOC	United Nations military observers course
UNMOVCC	United Nations movement control course
UNO	unit number
UNOCHA	United Nations Office for the Coordination of Humanitarian Affairs
UNODC	United Nations Office on Drugs and Crime

UNODIR	unless otherwise directed
UNOSOM	United Nations Operations in Somalia
UNPA	United Nations Participation Act
UNPROFOR	United Nations protection force
UNREP	underway replenishment
UNREP CONSOL	underway replenishment consolidation
UNRWA	United Nations Relief and Works Agency for Palestine Refugees in the Near East
UNSC	United Nations Security Council
UNSCR	United Nations Security Council resolution
UNSG	United Nations Secretary-General
UNSOC	United Nations staff officers course
UNTAC	United Nations Transition Authority in Cambodia
UNTSO	United Nations Truce and Supervision Organization
UNV	United Nations volunteer
UOF	use of force
UON	urgent operational need
UP&TT	unit personnel and tonnage table
URDB	user requirements database
URL	uniform resource locater
URN	unit reference number
US&R	urban search and rescue
USA	United States Army
USAB	United States Army barracks
USACCSA	United States Army Command and Control Support Agency
USACE	United States Army Corps of Engineers
USACFSC	United States Army Community and Family Support Center
USACHPPM	United States Army Center for Health Promotion and Preventive Medicine
USACIDC	United States Army Criminal Investigation Command
USAEDS	United States Atomic Energy Detection System
USAF	United States Air Force
USAFE	United States Air Forces in Europe
USAFEP	United States Air Force, Europe pamphlet
USAFLANT	United States Air Force, Atlantic Command
USAFR	United States Air Force Reserve
USAFRICOM	United States Africa Command
USAFSOC	United States Air Force, Special Operations Command
USAFSOF	United States Air Force, Special Operations Forces
USAFSOS	United States Air Force Special Operations School
USAID	United States Agency for International Development
USAITAC	United States Army Intelligence Threat Analysis Center
USAJFKSWC	United States Army John F. Kennedy Special Warfare Center

USAMC	United States Army Materiel Command
USAMMA	United States Army Medical Materiel Agency
USAMPS	United States Army Military Police School
USAMRICD	United States Army Medical Research Institute of Chemical Defense
USAMRIID	United States Army Medical Research Institute of Infectious Diseases
USAMRMC	United States Army Medical Research and Materiel Command
USANCA	United States Army Nuclear and Combating Weapons of Mass Destruction Agency
USAO	United States Attorney Office
USAR	United States Army Reserve
USARCENT	United States Army, Central Command
USARDECOM	United States Army Research, Development, and Engineering Command
USAREUR	United States Army, European Command
USARIEM	United States Army Research Institute of Environmental Medicine
USARJ	United States Army, Japan
USARNORTH	United States Army, North
USARPAC	United States Army, Pacific Command
USARSO	United States Army, Southern Command
USASMDC/ARSTRAT	United States Army Space and Missile Defense Command/Army Forces Strategic Command
USASOC	United States Army Special Operations Command
USB	upper side band
USBP	United States Border Patrol
USC	United States Code; universal service contract
USCENTCOM	United States Central Command
USCG	United States Coast Guard
USCGR	United States Coast Guard Reserve
USCIS	United States Citizenship and Immigration Services
USCS	United States Cryptologic System; United States Customs Service
USCYBERCOM	United States Cyber Command
USDA	United States Department of Agriculture
USD(A&T)	Under Secretary of Defense for Acquisition and Technology
USDAO	United States defense attaché office
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)	Under Secretary of Defense (Comptroller)
USDELMC	United States Delegation to the NATO Military Committee
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(R&E)	Under Secretary of Defense for Research and Engineering
USELEMCMOC	United States Element Cheyenne Mountain Operations Center
USELEMNORAD	United States Element, North American Aerospace Defense Command
USERID	user identification
USERRA	Uniformed Services Employment and Reemployment Rights Act
USEUCOM	United States European Command
USFF	United States Fleet Forces Command
USFJ	United States Forces, Japan
USFK	United States Forces, Korea
USFORAZORES	United States Forces, Azores
USFS	United States Forest Service
USFWS	United States Fish and Wildlife Service
USG	United States Government
USGS	United States Geological Survey
USIA	United States Information Agency
USIC	United States interdiction coordinator
USIS	United States Information Service
USJFCOM	United States Joint Forces Command
USLANTFLT	United States Atlantic Fleet
USLO	United States liaison office; United States liaison officer
USMARFORCENT	United States Marine Component, Central Command
USMARFORLANT	United States Marine Component, Atlantic Command
USMARFORNORTH	United States Marine Corps Forces North
USMARFORPAC	United States Marine Component, Pacific Command
USMARFORSOUTH	United States Marine Component, Southern Command
USMC	United States Marine Corps
USMCEB	United States Military Communications-Electronics Board
USMCR	United States Marine Corps Reserve
USMER	United States merchant ship vessel locator reporting system
USMILGP	United States military group
USMILREP	United States military representative
USML	United States Munitions List
USMOG-W	United States Military Observer Group - Washington
USMS	United States Marshals Service
USMTF	United States message text format
USMTM	United States military training mission
USN	United States Navy
USNAVCENT	United States Naval Forces, Central Command
USNAVEUR	United States Naval Forces, Europe
USNAVSO	US Naval Forces Southern Command

USNCB	United States National Central Bureau (INTERPOL)
USNMR	United States National Military representative
USNMTG	United States North Atlantic Treaty Organization (NATO) Military Terminology Group
USNO	United States Naval Observatory
USNORTHCOM	United States Northern Command
USNR	United States Navy Reserve
USNS	United States Naval Ship
USPACAF	United States Air Forces, Pacific Command
USPACFLT	United States Pacific Fleet
USPACOM	United States Pacific Command
USPFO(P&C)	United States Property and Fiscal Office (Purchasing and Contracting)
USPHS	United States Public Health Service
USPS	United States Postal Service
USREPMC	United States representative to the military committee (NATO)
USSOCOM	United States Special Operations Command
USSOUTHAF	United States Air Force, Southern Command
USSOUTHCOM	United States Southern Command
USSS	United States Secret Service (TREAS); United States Signals Intelligence (SIGINT) System
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
USUN	United States Mission to the United Nations
USW	undersea warfare
USW/USWC	undersea warfare and/or undersea warfare commander
USYG	under secretary general
UT1	unit trainer; Universal Time
UTC	Coordinated Universal Time; unit type code
UTM	universal transverse mercator
UTO	unit table of organization
UTR	underwater tracking range
UUV	unmanned underwater vehicle; unmanned underwater vessel
UVEPROM	ultraviolet erasable programmable read-only memory
UW	unconventional warfare
UWOA	unconventional warfare operating area
UXO	unexploded explosive ordnance; unexploded ordnance

V

V	search and rescue unit ground speed; sector pattern; volt
v	velocity of target drift
VA	Veterans Administration; victim advocate; vulnerability assessment
V&A	valuation and availability
VAAP	vulnerability assessment and assistance program
VAC	volts, alternating current
VARVAL	vessel arrival data, list of vessels available to marine safety offices and captains of the port
VAT B	(weather) visibility (in miles), amount (of clouds, in eighths), (height of cloud) top (in thousands of feet), (height of cloud) base (in thousands of feet)
VBIED	vehicle-borne improvised explosive device
VBS	visit, board, search
VBSS	visit, board, search, and seizure
VCC	voice communications circuit
VCG	virtual coordination group
VCJCS	Vice Chairman of the Joint Chiefs of Staff
VCNOG	Vice Chairman, Nuclear Operations Group
VCO	voltage controlled oscillator
VCOPG	Vice Chairman, Operations Planners Group
VCR	violent crime report
VCXO	voltage controlled crystal oscillator; voltage controlled oscillator
VDC	volts, direct current
VDJS	Vice Director, Joint Staff
VDL	video downlink
VDR	voice digitization rate
VDS	video subsystem
VDSD	visual distress signaling device
VDU	visual display unit
VDUC	visual display unit controller
VE	vertical error
VEE	Venezuelan equine encephalitis
VEH	vehicle; vehicular cargo
VEO	violent extremist organization
VERTREP	vertical replenishment
VF	voice frequency
VFR	visual flight rules
VFS	validating flight surgeon
VFTG	voice frequency telegraph
VHF	very high frequency
VI	visual information
VICE	advice

VID	visual identification; visual identification information display
VINSON	encrypted ultrahigh frequency communications system
VIP	very important person; visual information processor
VIRIN	visual information record identification number
VIRS	verbally initiated release system
VIS	visual imaging system
VISA	Voluntary Intermodal Sealift Agreement
VISION ID	visual information professional identifier
VISOBS	visual observer
VIXS	video information exchange system
VLA	vertical line array; visual landing aid
VLF	very low frequency
VLR	very-long-range aircraft
VMap	vector map
VMAQ	Marine tactical electronic warfare squadron
VMC	visual meteorological conditions
VMF	variable message format
VMGR	Marine aerial refueler and transport squadron
VMI	vendor managed inventory
VNTK	target vulnerability indicator designating degree of hardness; susceptibility of blast; and K-factor
VO	validation office
VOCODER	voice encoder
VOCU	voice orderwire control unit
VOD	vertical onboard delivery
VOL	volunteer
vol	volume
VOLS	vertical optical landing system
VOR	very high frequency omnidirectional range station
VORTAC	very high frequency omnidirectional range station and/or tactical air navigation
VOX	voice actuation (keying)
VP	video processor
VPB	version planning board
VPD	version planning document
VPV	virtual prime vendor
VS	sector single-unit
VS&PT	vehicle summary and priority table
VSG	virtual support group
VSP	voice selection panel
VSR	sector single-unit radar
V/STOL	vertical and/or short takeoff and landing aircraft
VSW	very shallow water
VTA	voluntary tanker agreement
VTC	video teleconferencing
VTOL	vertical takeoff and landing

VTOL-UAS	vertical takeoff and landing unmanned aircraft system
VTOL-UAV	vertical takeoff and landing unmanned aerial vehicle
VTS	vessel traffic service
VTT	video teletraining
VU	volume unit
VV&A	verification, validation, and accreditation
VV&C	verification, validation, and certification
VX	nerve agent (O-Ethyl S-Diisopropylaminomethyl Methylphosphonothiolate)

Intentionally Blank

W

W	sweep width
w	search subarea width
WAAR	Wartime Aircraft Activity Report
WACBE	World Area Code Basic Encyclopedia
WADS	Western Air Defense Sector
WAGB	icebreaker (USCG)
WAI	weather area of interest
WAN	wide-area network
WANGO	World Association of Non-Governmental Organizations
WARM	wartime reserve mode
WARNORD	warning order
WARP	web-based access and retrieval portal
WAS	wide area surveillance
WASP	war air service program
WATCHCON	watch condition
WB	wideband
WBGTI	wet bulb globe temperature index
WBIED	waterborne improvised explosive device
WC	wind current
WCA	water clearance authority
WCCS	Wing Command and Control System
WCDO	War Consumables Distribution Objective
WCE	weapons of mass destruction coordination element
WCO	World Customs Organization
WCS	weapons control status
WDCO	well deck control officer
WDT	warning and display terminal
WEAX	weather facsimile
Web SM	Web scheduling and movement
WES	weapon engagement status
WETM	weather team
WEU	Western European Union
WEZ	weapon engagement zone
WFE	warfighting environment
WFP	World Food Programme (UN)
WG	working group
WGS	Wideband Global Satellite Communications; World Geodetic System
WGS 84	World Geodetic System 1984
WH	wounded due to hostilities
WHEC	high-endurance cutter (USCG)
WHNRS	wartime host-nation religious support
WHNS	wartime host-nation support
WHNSIMS	Wartime Host Nation Support Information Management System

WHO	World Health Organization (UN)
WIA	wounded in action
WISDIM	Warfighting and Intelligence Systems Dictionary for Information Management
WISP	Wartime Information Security Program
WIT	weapons intelligence team
WLG	Washington Liaison Group
WMD	weapons of mass destruction
WMD-CST	weapons of mass destruction-civil support team
WMEC	Coast Guard medium-endurance cutter
WMO	World Meteorological Organization
WMP	Air Force War and Mobilization Plan; War and Mobilization Plan
WOC	wing operations center (USAF)
WOD	wind-over deck; word-of-day
WORM	write once read many
WOT	war on terrorism
WP	white phosphorous; working party; Working Party (NATO)
WPA	water jet propulsion assembly
WPAL	wartime personnel allowance list
WPARR	War Plans Additive Requirements Roster
WPB	Coast Guard patrol boat
WPC	Washington Planning Center
WPM	words per minute
WPN	weapon
WPR	War Powers Resolution
WR	war reserve; weapon radius
WRA	Office of Weapons Removal and Abatement (DOS); weapons release authority
WRAIR	Walter Reed Army Institute of Research
WRC	World Radiocommunication Conference
WRL	weapons release line
WRM	war reserve materiel
WRMS	war reserve materiel stock
WRR	weapons response range (as well as wpns release rg)
WRS	war reserve stock
WRSA	war reserve stocks for allies
WRSK	war readiness spares kit; war reserve spares kit
WS	weather squadron
WSE	weapon support equipment
WSES	surface effect ship (USCG)
WSESRB	Weapon System Explosive Safety Review Board
WSM	waterspace management
WSR	weapon system reliability
WSV	weapons system video

WT	warping tug; weight
WTCA	water terminal clearance authority
WTCT	weapons of mass destruction technical collection team
WTI	weapons technical intelligence
WTLO	water terminal logistic office
Wu	uncorrected sweep width
WVRD	World Vision Relief and Development, Inc.
WWABNCP	worldwide airborne command post
WWII	World War II
WWSVCS	Worldwide Secure Voice Conferencing System
WWX	worldwide express
WX	weather

Intentionally Blank

X

X	initial position error
XCDS	Extracted Container Delivery System
XCVR	transceiver
XMPP	extensible messaging and presence protocol
XO	executive officer
XSB	barrier single unit

Intentionally Blank

Y

Y	search and rescue unit (SRU) error
YR	year

Intentionally Blank

Z

Z	zulu
z	effort
ZF	zone of fire
Zt	total available effort
ZULU	time zone indicator for Universal Time

Intentionally Blank

APPENDIX B
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users are highly encouraged to submit comments on this publication to the Directorate for Joint Force Development, J-7, Joint Doctrine and Education Division, Joint Doctrine Branch, ATTN: Chairman, US NATO Military Terminology Group, 7000 Joint Staff, Pentagon, Washington, DC 20318-7000; Tel (703) 692-7255, DSN 222-7255; Fax (703) 692-5224, DSN 222-5224. All comments recommending modifications, deletions, or additions to terminology in JP 1-02 must be made in accordance with DODI 5025.12, *Standardization of Military and Associated Terminology*, and CJCSI 5705.01, *Standardization of Military and Associated Terminology*.

2. Authorship

The lead agent and the Joint Staff doctrine sponsor for this publication is the Director for Joint Force Development (J-7).

3. Supersession

a. This publication supersedes JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001. The terms and definitions in JP 1-02 will be updated on a monthly basis with modifications, deletions, or additions that have been approved in accordance with DODI 5025.12 and CJCSI 5705.01.

b. Record of Updates:

31 December 2010: JP 3-02.1, JP 3-07.2, and DODD 3025.18 added.

31 January 2011: JP 3-68, JP 4-03, and SecDef Memo 12401-10 added.

15 April 2011: JP 2-01.2 added.

15 May 2011: JP 3-05 added.

15 July 2011: JP 3-08, JP 3-15, and JP 3-34 added.

15 August 2011: JP 3-0 and JP 5-0 added.

15 September 2011: JP 1-04 added.

15 October 2011: JP 3-03, JP 3-07, and JP 4-06 added.

15 November 2011: JP 1-0 added.

15 January 2012: JP 2-01, JP 3-13.2, JP 3-13.3, JP 3-15,1, JP 3-50, CJCSI 5120.02C, and CJCSM 5120.01 added.

15 February 2012: JP 3-13.1 and JP 3-13.4 added.

15 March 2012: JP 1-06 added.

15 April 2012: JP 3-01, JP 4-01.5, and JP 6-01 added.

15 July 2012: JP 3-41 and JP 4-01.2 added.

15 August 2012: JP 3-07.3, JP 3-33, and JP 4-02 added.

15 November 2012: JP 2-03 added.

15 December 2012: JP 3-04, JP 3-13, JP 3-18, JP 3-59, and JP 4-01.6 added.

15 February 2013: JP 3-12, JP 3-35, and JP 3-60 added.

15 March 2013: JP 4-08 added.

15 April 2013: JP 1 added.

15 June 2013: JP 3-14 and JP 4-01 added.

16 July 2013: JP 3-16 added.

15 August 2013: JP 3-07.4, JP 3-27, JP 3-28, and JP 3-32 added.

15 September 2013: JP 3-57 added.

15 October 2013: JP 3-11 and JP 3-17 added.

15 November 2013: JP 2-0 and JP 4-0 added.

15 December 2013: JP 1-05, JP 3-06, and JP 3-24 added.

15 January 2014: JP 3-29 and JP 4-09 added.

15 February 2014: JP 3-30 added.

15 March 2014: JP 4-05, JP 3-07.2, JP 3-31, and DODI 8260.03 added.

15 June 2014: JP 2-01.3 and DODI 1342.22 added.

16 July 2014: JP 3-05 and JP 4-10 added.

15 August 2014: JP 3-02 added.

15 November 2014: JP 3-10, JP 3-26, JP 3-40, JP 3-52, and JP 3-63 added.

15 December 2014: JP 3-02.1, JP 3-09, JP 3-09.3, and JP 3-13.2 added.

15 January 2015: CJCSI 5120.02D and CJCSM 5120.01A added.

15 March 2015: DODI 6025.22, DODI 8500.01, and JP 2-01.2 Change 1 added.

15 June 2015: DODD 3000.10, DODI 8260.04, and JP 6-0 added.

15 September 2015: JP 3-05.1 added.

15 October 2015: JP 3-50 added.

15 November 2015: JP 4-01.5 added.

15 December 2015: JP 3-61 and JP 3-68 added.

15 January 2016: JP 1-06, JP 3-13.3, JP 3-34, JP 4-01.2, JP 4-03 added.

15 February 2016: DODD 4715.21.

4. Terms Removed or Replaced by the 15 February 2016 Amendment

Terms Removed or Replaced			
Term	**Action**	**Pub**	**Rationale**
N/A			

Figure B-1. Terms Removed or Replaced

5. Terms Added, Sourced, or Modified by the 15 February 2016 Amendment

Terms Added, Sourced, or Modified		
Term	**Action**	**Publication**
climate change	Added	DODD 4715.21

Figure B-2. Terms Added, Sourced, or Modified

6. Terminology Commonly Used in Error

Terminology Commonly Used in Error	
Correct Terminology	**Misused Terminology**
military information support operations	psychological operations (PSYOP)

(MISO)	
lethal/nonlethal	kinetic/nonkinetic
CCMD (combatant command)	COCOM
cyberspace	cyber
Department of Defense information network (DODIN)	Global Information Grid (GIG)
create effects	achieve effects
adversary (potentially hostile)	enemy
enemy (demonstrably hostile)	adversary

Figure B-3. Terminology Commonly Used in Error

7. Distribution

Joint Staff J-7 does not print copies of JP 1-02 for distribution. Electronic versions are available on JDEIS Joint Electronic Library Plus (JEL+) at https://jdeis.js.mil/jdeis/index.jsp (NIPRNET) and http://jdeis.js.smil.mil/jdeis/index.jsp (SIPRNET), and on the JEL at http://www.dtic.mil/doctrine (NIPRNET).

JOINT
CHIEFS OF STAFF

ST 2-50.4 (FM 34-8)

COMBAT COMMANDERS HANDBOOK ON INTELLIGENCE

US Army Intelligence Center and Fort Huachuca
Fort Huachuca, Arizona 85613-6000

SEPTEMBER 2001

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

PREFACE

Combat commanders need timely and accurate intelligence. In order to drive intelligence as a part of the intelligence operating system, commanders must understand what intelligence can do, how to focus it on specific requirements, and how you can integrate it with other operating systems.

This handbook addresses these requirements, expanding on the doctrine in FM 2-0 (FM 34-1), FM 3-0 (FM 100-5), FM 5-0 and FM 6-0 (FM 101-5), and FM 2-01.3 (FM 34-1 30).

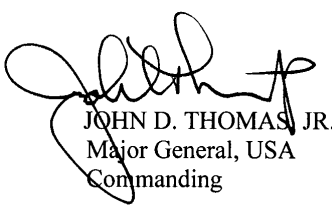
This handbook is written primarily for maneuver commanders and executive officers at brigade or regiment and battalion or squadron levels to include Active Components (AC) and Reserve Component (RC) commanders. It should also be useful to principal staff officers and combat support (CS) and combat service support (CSS) commanders.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men. Throughout the manual, “you” refers to the combat commander and also applies to the executive officer as he integrates and synchronizes the orders process and directs and supervises the staff.

The proponent of this publication is the US Army Intelligence Center and Fort Huachuca. We consider this a living manual and will dynamically revise this doctrine as frequently as necessary based on comments and suggestions from the field. Under normal circumstances appropriate revisions will be made within two weeks of receipt. While the initial (one time) distribution of this field manual will be made on CD-ROM, users should realize that to capture the dynamic changes/revisions of the manual as soon as they occur, they should check the Intelligence Center Homepage frequently for the most current version. We welcome your comments and recommended changes at any time. You may email them directly to the proponent at edd.goodmanc@hua.army.mil or mail them to: Commander, US Army Intelligence Center and Fort Huachuca (ATZS-FDRCD), Fort Huachuca, Arizona 85613-6000. You can also access the Doctrine Division Homepage at http://usaic.hua.army.mil/doctrine.htm and leave your comments or changes with the webmaster.

This handbook does not implement any international Standardization Agreements (STANAG5). It complies with all applicable STANAGs and Quadripartite Standardization Agreements. This document contains copyrighted material.

This manual incorporates the emerging intelligence and operational doctrine and terminology from FM 3-0, Operations, dated 14 June 2001. It uses the new manual numbers with the old manual numbers in parentheses. Although not all manuals have been updated to the new numbering system, this was done to transition the force to the new numbering system.



JOHN D. THOMAS, JR.
Major General, USA
Commanding

SPECIAL TEXT
No. 2-50.4 (FM 34-8)

USAIC&FH
Fort Huachuca, AZ 86513-6000
6 September 2001

TABLE OF CONTENTS

Page

PREFACE iii

CHAPTER 1 THE INTELLIGENCE CHALLENGE FOR COMMANDERS 1-1
Intelligence Operating System 1-1
ISR Operations 1-2
Intelligence Tasks 1-4
Effective Intelligence 1-6

CHAPTER 2 INTELLIGENCE PREPARATION OF THE BATTLEFIELD 2-1
Responsibilities 2-1
What You Should Expect 2-5
Effective Techniques During Mission Analysis 2-5

CHAPTER 3 S2/G2 ORGANIZATIONS AND FUNCTIONS 3-1
The Battalion S2 3-1
The Brigade S2 3-2
The Division and Corps G2 3-4

CHAPTER 4 MILITARY INTELLIGENCE CAPABILITIES 4-1
Intelligence Disciplines 4-1
Intelligence Functions 4-4
MI Organizations 4-5
Limitations of Intelligence 4-9

APPENDIX A INTELLIGENCE AND THE MILITARY DECISION-MAKING PROCESS A-1
What to Expect from Your S2 ..... A-1
Targeting Meeting A-6

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*FM 34-8, 28 September 1992, is rescinded. This Special Text reflects the latest doctrine on this subject approved by the Commanding General, United States Army Intelligence Center & Fort Huachuca.

APPENDIX B COMMANDER'S CRITICAL INFORMATION REQUIREMENTS B-1
Priority Intelligence Requirements B-2
Friendly Forces Information Requirements B-3
Essential Elements of Friendly Information B-3

APPENDIX C ISR INTEGRATION WITHIN THE SYNCHRONIZATION MATRIX C-1

APPENDIX D INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE PLANNING D-1

APPENDIX E FOREIGN LANGUAGE SUPPORT E-1
Introduction E-1
Linguistic Support Categories E-1
Determining Linguist Requirements E-1
Planning and Managing Linguist Support E-2
Identifying Sources of Linguists E-9

APPENDIX F STABILITY OPERATIONS, SUPPORT OPERATIONS, AND INTELLIGENCE PREPARATION OF THE BATTLEFIELD F-1
IPB Modifications for Stability Operations and Support Operations F-1
Urban Operations Considerations F-3

GLOSSARY Glossary-1

REFERENCES References-1

Chapter 1

The Intelligence Challenge for Commanders

Intelligence is your tool; it is the foundation for synchronizing operations, massing combat power and effects, and protecting the force. There is no such thing as perfect intelligence but, when properly focused and planned and executed, intelligence operations are invaluable. To effectively use intelligence, you must understand—

- The capabilities and limitations of the intelligence operating system.
- The intelligence architecture (which includes command and control (C^2); processing; collaborative and distributed analysis; intelligence, surveillance, and reconnaissance [ISR] operations; and intelligence networks and communications).
- How you focus ISR operations.
- How you and your staff synchronize ISR with other operations.

INTELLIGENCE OPERATING SYSTEM

1-1. The mission of your intelligence operating system is to provide timely, relevant, accurate, and predictive intelligence support to you, your staff, and subordinates when planning, preparing, and executing decisive actions within the area of operations (AO). Implied within this mission, or associated with intelligence, are—

- Integrated ISR planning (focused through the S2 and S3 but thoroughly planned by the entire staff).
- Changes and adjustments to ISR collection.
- Analysis, production, and dissemination (to include presentation) of intelligence and combat information—the heart of the intelligence operating system.
- Electronic Warfare (EW), which is an integrated part of fires, targeting, and effects. EW should always be employed as an integrated and complementary capability.
- Counterintelligence (CI) is critical to your ability to protect the force in terms of supporting counterreconnaissance, analyzing the threat's multidiscipline ISR operations, and recommending countermeasures to those threat operations. There is a symbiotic relationship between counter-human intelligence (HUMINT) CI operations and human intelligence (HUMINT) collection. In the future, CI functionality will include analysis of threat information operations (IO) and other full-dimensional counter-ISR tasks.

ISR OPERATIONS

1-2. ISR planning and execution do not reflect a change to fundamental Army doctrine. Recent emphasis on ISR operations reflects the importance of a unified, integrated, and synchronized effort to—

- Plan and direct the ISR effort.
- Collect and process information.
- Produce intelligence.
- Disseminate intelligence and combat information to those who need it, when they need it.

1-3. Two concepts are imbedded in recent ISR doctrine:

- There are a finite number of "traditional intelligence collection" and "traditional reconnaissance and surveillance (R&S)" assets, but there are many potential ISR assets.
- There is a different "mindset" among each operating systems or proponent on how to plan, task, and control assets; how and where to report information; and how to use the information. However, ISR doctrine is designed to break the operating system or functional "stovepipes" for planning, reporting, processing, and analyzing information.

EMERGING DOCTRINE (IBCT)
(See Chapter 4)

In recognition of the importance of ISR operations and the unique challenges of small-scale contingencies, the initial brigade combat team (IBCT) is uniquely organized to facilitate ISR operations:

- The Military Intelligence (MI) Company (subordinate to the brigade) includes an ISR integration platoon, HUMINT platoon, more robust analytical capability, and organic control teams (specifically the operational management team [OMT] to help the commander control tactical HUMINT operations).
- The reconnaissance, surveillance, and target acquisition (RSTA) squadron S2 is supported by an ISR Integration Team (from the Surveillance Squadron).
- The surveillance troop (subordinate to the RSTA squadron) consists of soldiers and assets that execute nuclear, biological, and chemical (NBC) surveillance and other ISR operations (operations traditionally described as intelligence operations—from three disciplines). Another new characteristic is multi-sensor teams that employ sensors from more than one intelligence discipline.
- The reconnaissance troop (subordinate to the RSTA squadron) includes an organic HUMINT collection capability.

CRITICAL ELEMENTS OF ISR OPERATIONS

1-4. **Focus the ISR effort:**

- Clearly articulate your priority intelligence requirements (PIR) with a latest time intelligence is of value (LTIOV).

- Drive the IPB process throughout the military decision-making process (MDMP) (see Chapter 2).

1-5. **Carefully plan ISR operations.** You must ensure that intelligence preparation of the battlefield (IPB) drives the rest of the planning process and that all ISR operations are thoroughly planned (to include synchronized) and controlled as an integrated staff effort through the C^2 system. Although the G2 (S2) is the IPB and ISR integrator and the G3 (S3) plays a critical role in synchronizing ISR with the operation, every staff member plays an important role in both tasks. Your primary tool in accomplishing these integration tasks is the Chief of Staff (CofS) or executive officer (XO). The CofS (XO) is responsible to ensure all staff members participate in and provide their functional expertise into the IPB process and ISR planning and execution under the direction of the G2 (S2). There are a number of different techniques that the CofS (XO) can employ to facilitate interaction among the entire staff during the IPB process and ISR integration. However, the desired endstate is an efficient process that supports planning and helps facilitate the commander's visualization and understanding.

1-6. **Ensure ISR operations are continuous.** Your S2 (through the intelligence architecture) continuously performs intelligence tasks to meet your requirements before deploying and during operations. No echelon has enough time, ISR assets, and analytical tools to satisfy all of its requirements. Therefore, never keep your ISR assets in reserve.

1-7. **Use the C^2 system (as described in FM 5-0 and FM 6-0 (FM 101.5)).** Clear C^2 through centralized planning and decentralized execution is important. (This extends beyond collection management, as described in FM 2-33.4 (FM 34-2)). Command and support relationships for ISR units are developed by thorough staff planning (through mission, enemy, terrain and weather, troops, time available, and civilians [METT-TC] analysis). Use habitual relationships, when possible, to optimize effective operations as a combined arms team.

1-8. **Ensure ISR is a distributed operation.** Timely reporting to the right analytical element at the right echelon is critical to ISR operations. Intelligence Reach is a process by which deployed military forces rapidly access information from, receive support from, and conduct collaboration and information sharing with other units (deployed in theater and from outside the theater) unconstrained by geographic proximity, echelon, or command. G2s, S2s, and intelligence analytical elements (for example, the analysis and control element [ACE] and the analysis and control team [ACT] within the direct support [DS] MI company) utilize Intelligence Reach to collaborate, participate in distributed analysis, and share access to the intelligence between echelons and units. Every echelon must work together and tailor the intelligence architecture so that it is as close to seamless as possible—no barriers.

ISR TRAINING

1-9. **Integrate ISR training into garrison ("day-to-day") operations, exercises, and training events**. An increase in the importance of intelligence and the recent complexity of unique environments (urban operations and other complex terrain) and missions (stability operations and support operations) requires well-trained ISR commanders, leaders, soldiers, and organizations to produce superior results. You are responsible for training your portion of the intelligence operating system—the G2/S2. Your G2/S2 is

responsible for training his section and helping you train your unit on ISR issues. However, the G2/S2 (Senior Intelligence Officer) and intelligence commanders and leaders also train a significant portion of the intelligence operating system.

INTELLIGENCE TASKS

1-10. The intelligence battlefield operations system (BOS) is divided into the following four intelligence tasks. It is important that you understand the tasks that the S2 section performs during operations. Each task corresponds with a critical aspect of operations.

- **Facilitate commander's visualization and understanding of the threat and the environment.** This task provides information and intelligence to the commander to support his achievement of battlefield visualization. This task is comprised of three subtasks:

  — **Perform Intelligence Preparation of the Battlefield (IPB)** - IPB is the staff planning activity undertaken to understand the battlefield and the options it presents to friendly and threat forces. It is a systematic process of analyzing the threat and environment in a specific geographic area for a specific mission. By applying IPB, the commander gains the information necessary to selectively apply and maximize his combat power at critical points in time and space.

  — **Perform Indications and Warnings (I&W)** – I&W provide the commander with early warning and prevents surprise through anticipation of significant changes in threat activities. I&W provide the commander the ability to quickly reorient his forces on unexpected major contingencies and shape the battlefield.

  — **Perform Situation Development** – This subtask confirms or denies threat courses of action (COAs), explains what the threat is doing in relation to the friendly force commander's intent, and provides an estimate of threat combat effectiveness. Commanders use situation development to help understand the AO, thereby reducing risk and uncertainty. Situation development helps the commander make decisions and execute branches and sequels.

- **Counter the Threat** - This task provides the commander information and intelligence support for targeting of the threat's forces, threat organizations, units and systems through lethal and non-lethal fires to include electronic attack (EA) and information operations. It also includes the tactics, techniques, and procedures (TTPs) to deny or degrade the threat ISR capabilities to access and collect information and intelligence on friendly forces. This task is comprised of two subtasks:

  — **Support Targeting** - Targeting is supported by the staff to develop target systems, locate the targets, and perform battle damage assessment (BDA) on engaged targets. Included in this task is the use of EA against threat forces.

  — **Perform Counterintelligence** - CI is designed to defeat or degrade threat intelligence collection capabilities. The intelligence staff will provide CI to the commander outlining the capabilities and limitation of threat intelligence services and TTPs to limit or eliminate these capabilities.

- **Intelligence, Surveillance, and Reconnaissance Integration.** This task integrates ISR assets into an effort that produces intelligence, which leads to the commander's gaining situational understanding. These capabilities to collect, process, analyze and produce, and disseminate are critical to successful planning and conducting operations. Intelligence requirements are identified, prioritized, and validated; an ISR plan is developed and synchronized with the scheme of maneuver. This task is comprised of four subtasks:

  — **Develop Requirements** - Intelligence officers develop a prioritized list of what information needs to be collected and produced into intelligence. This list is placed against an LTIOV to ensure intelligence and information are reported to the unit in order for operations to proceed as planned.

  — **Analyze Requirements and Resources Available** - The entire staff under the direction of the intelligence staff analyzes each requirement to determine how best to satisfy it. The staff will receive orders and requests for information (RFIs) from both subordinate and adjacent units and higher headquarters. These requests are then balanced with resources available for tasking to ensure requirements can be met with available assets and their specific capabilities.

  — **Develop Specific Information Requirements (SIRs)** - SIRs break requirements into specific questions which, when answered, can satisfy the larger intelligence requirements. The requirements manager will develop sets of SIRs for each requirement with an LTIOV associated with each one.

  — **Develop ISR Plan.** The XO integrates and supervises the entire staff under the direction of the intelligence staff and develops an integrated and synchronized plan that places requirements to include time with recommended ISR assets. The ISR plan creates a collection strategy and employment scheme that will produce the intelligence required to effectively answer the commander's PIR.

- **Manage Intelligence Support to Information Operations** - Intelligence, both in offensive and defensive operations, provides the critical links for engagement with offensive IO. Intelligence also provides the capabilities and limitation of threat IO. This forms the basis of the defensive IO plan. Intelligence supports IO through its intelligence tasks and subtasks focusing on the target of IO.

EFFECTIVE INTELLIGENCE

1-11. The effectiveness of intelligence is measured against the following standards:

- **Timely:** Intelligence is useful only if you receive it soon enough to support planning, influence decisions, and prevent surprise.

- **Relevant:** Intelligence must answer your requirements and the requirements of your staff about the environment and threat in the format you designate. Your S2 must present you some basic products that help you visualize your battlespace (proportionate to his resources and the time available).

- **Accurate:** Intelligence must provide a balanced, complete, and objective picture of the threat and the operational environment. Alternative or contradictory assessments should be presented to ensure balance and bias-free intelligence.

When a certain degree of doubt exists, your S2 must capture and present that uncertainty.

- **Predictive**: Intelligence should advise you of present and future threat intent, objectives, capabilities, and COAs (with a description of supporting events by each threat operating system).

Chapter 2

Intelligence Preparation of the Battlefield

Longstreet looked up the long rise. He could begin to see it. When the troops came out of the woods the artillery would open up. Long-range artillery, percussion and solid shot, every gun on the hill. The guns to the right, on the Rocky Hill, would enfilade the line. The troops would be under fire with more than a mile to walk. And so they would go. A few hundred yards out, still in the open field, they would come within range of skirmish, aimed rifles. Losses would steadily increase. When they reached the road they would be slowed by the fence there, and the formation, if it still held would begin to come apart. Then they would be in range of the rifles on the crest. When they crossed the road, they would begin to take canister fire and thousands of balls of shrapnel wiping huge holes in the line. As they got close, there would be double canister. If they reached the wall without breaking, there would not be many left. It was a mathematical equation.

—Shaara, Michael. *Killer Angels.* New York, NY: Ballantine Books, 1974, p. 303.

RESPONSIBILITIES

2-1. The above passage details the vision General Longstreet had prior to the assault on Cemetery Ridge during the battle of Gettysburg. Because General Longstreet understood the critical elements of the terrain and the enemy, he was able to visualize this battle before it occurred. You rely on your S2 and staff to provide IPB analysis and graphic products that enable you to effectively visualize the battlefield and make decisions.

2-2. To visualize the battlefield, it is important that you and your XO take the lead to ensure that the IPB process is really an integrated staff effort (this is sometimes referred to as the cross-BOS IPB effort). Your S2 and staff must participate in initial IPB by—

- Analyzing the threat equivalent for their staff or functional area (red hat analysis). For example, the Engineer Officer will help analyze threat mobility, countermobility, and survivability capabilities.

- Helping the S2 capture any threat equivalent actions within the threat COAs for their staff or functional area (red hat actions) within standard or unique IPB products.

- Ensuring that their staff or functional area information requirements are answered or captured as an intelligence gap (in order to support planning and operations).

2-3. Although IPB is a G2/S2 responsibility, the entire staff contributes to the IPB process as shown in the Figure 2-1. However, Figure 2-2 shows the three most important MDMP steps for the commander to drive IPB.

FIRE SUPPORT OFFICER	**ENGINEER OFFICER**
▪ Provides templated locations for threat artillery and rocket systems. ▪ Provides the mission, task, and purpose of threat artillery and rocket systems. ▪ Assists the G2/S3 to accurately portray the threat's use of indirect fires, such as types and phases of threat fire.	▪ Provides templated locations for mobility, countermobility threat obstacles, and manmade obstacles. ▪ Provides information on the threat's preferred construct of survivability positions. ▪ Assists the G2/S2 to accurately portray the task and purpose of threat obstacles and threat mobility assets.
CHEMICAL OFFICER	AIR DEFENSE OFFICER
▪ Provides templated locations for NBC strikes. ▪ Provides information for manmade obstacles, such as NBC contaminated areas. ▪ Assists the G2/S2 to accurately portray the threat's use, intent, and purpose in the use of NBC units and capabilities.	▪ Provides templated locations for threat (air defense) assets. ▪ Provides assistance in identifying air corridors and avenues of approach (AAs). ▪ Provides assistance in identifying threat missions, tasks, and purpose of threat air defense artillery (ADA) and aerial assets. ▪ Assists the G2/S2 to accurately portray the threat's purpose and intent using ADA and aerial systems.

Figure 2-1. Example of staff IPB contributions to the G2/S2

COMMANDER'S INITIAL GUIDANCE - (STEP 1: RECEIPT OF MISSION)

2-4. In order to drive the IPB process, you must answer several questions:

- Do you disagree with or question any significant portions of the higher echelon's IPB products, analysis, facts, or assumptions? If so, you and your S2 must quickly resolve any issues to preclude problems between echelons.

- Does the staff need to focus on any particular part of the IPB process?

MDMP Steps	Commander's Output	The Commander Drive IPB
Step 1: Receipt of Mission	Initial Guidance	Disagree with higher IPB? Abbreviated initial IPB? Initial ISR support? Additional IPB analysis (besides normal procedures)?
Step 2: Mission Analysis	Restarted Mission. Commander's Intent. Commander's Guidance.	Area of interest (AOI). Significant characteristics of the environment. Important environment factors. Choose threat models and identify any refinements. How many threat COAs and their specifics? Initial threat culmination criteria.
Step 6: COA Approval	Approved COA. Refined Commander's Intent. Specified Type of Order. Specified Type of Rehearsal. HPTL.	Final threat culmination criteria. Guidance on refining IPB analysis and products.

- Are there any immediate ISR requirements that need to be addressed early?

Figure 2-2. Driving IPB

COMMANDER'S INTENT AND GUIDANCE - (STEP 2: MISSION ANALYSIS)

2-5. You must allocate adequate time and guidance to your S2 and staff to perform the initial IPB. Successful mission analysis requires a thorough initial IPB to provide the staff with the impact of the environment, weather, and threat for use in subsequent steps of mission analysis.

2-6. In this step the staff starts to convert your visualization of the battlefield into an operational framework. Focus the efforts of your S2 and staff on IPB.

- **Define the Battlefield Environment.** Provide guidance on the AO, AOI, and the significant characteristics of the environment. For example, during a friendly offensive operation, characteristics such as location and activities of threat reserves, reinforcements, and fire support assets are typically significant. During a humanitarian assistance operation, however, the location and activities of civilian relief organizations may be a significant characteristic. Articulate your view so your staff can build the correct framework for the rest of the IPB process.

Why is this important? Failure to focus on only the relevant significant characteristics wastes time and the IPB process will not influence mission success. On the other hand, failure to identify all the significant characteristics may result in your unit's failure to deal with a feature of the battlefield that you and your staff overlooked.

- **Describe the Battlefield Effects.** The S2 and staff use the factors defined in Step 1 and other characteristics to evaluate the battlefield thoroughly and to describe the

  battlefield effects. In stability operations and support operations, you and your battlestaff must view terrain in a unique way and keep in mind the political, economic, ethnic, and other characteristics of the population (the key terrain).

Why is this important? Commanders with a poor understanding of the battlefield effects will probably fail to exploit the opportunities the environment provides, and the threat will find and exploit opportunities in a way the command did not anticipate.

- **Evaluate the Threat.** Most of the analytical work for this step is performed prior to deployment; it is a part of intelligence readiness activities and contingency planning. It is at this point that your S2 and staff clearly define who the threat is and what the threat looks like. In stability operations and support operations the threat could range from conventional military forces to paramilitary forces, insurgents, terrorists, political groups, refugees, or environmental disasters. Understanding the threat's intent provides focus to the S2 so that as he moves to step 4, the threat COAs make sense.

  Why is this important? Failure to evaluate the threat adequately may result in—

  — A lack of intelligence, which is needed for planning.

  — Wasted time and effort in planning against threat capabilities that do not exist.

  — Surprise because of an unknown threat capability.

- **Determine Threat COAs.** Dictate how many and to what level of detail you want the S2 and staff to develop threat COAs, then provide macro-level guidance on how you visualize your intent in relationship to threat objectives and endstate. Finally, provide the S2 and staff guidance on criteria that will lead to culmination of the threat. For example, you could intend to defeat the threat by destroying 75 percent of his organic and attached artillery and 50 percent of the lead motorized rifle battalions (MRBs).

Why is this important? Failure to adequately determine threat COAs will allow the threat to surprise you and your staff. Viable and tactically sound threat COAs provides the framework required to build a successful friendly COA.

2-7. After the mission analysis briefing you approve a restated mission (which becomes the unit's mission) and the initial PIR. (The integrated ISR plan comes from these initial requirements.) Your S2 and staff will continue to refine the PIR (with your approval)

throughout the MDMP. You can also modify your intent (this provides the link between the mission and the concept of operations). Your last responsibility is to provide your staff with enough additional guidance to focus staff activities during the remainder of planning.

COMMANDER'S DECISION BRIEFING - (STEP 6: COA APPROVAL)

2-8. After the decision briefing, you approve the COA you believe to be the most advantageous; you then modify your intent statement and your commander's critical information requirements (CCIR) to support this selected COA and issue further guidance:

- State the final threat culmination criteria.
- Direct refinements for the IPB analysis and products to include greater detail on threat branches and sequels.

WHAT YOU SHOULD EXPECT

2-9. Your S2 and staff must complete IPB early in the MDMP because this process lays the groundwork for COA development and the subsequent steps of the MDMP. IPB analysis and products must help you and your staff do the following:

- Visualize the battlefield.
- Complete COA development, the wargame process, and COA refinement (to include building flexibility into the operation).
- Plan ISR operations.
- Provide the framework so your S2 can perform situation development and your XO/S3 can provide the common operational picture during the operation.

2-10. To meet these requirements, your S2 and staff perform IPB analysis and produce graphic products that—

- Describe the threat's mission, intent (two levels up), and how they see us.
- Portray an adaptive, cunning, and uncooperative threat. Provide a detailed picture of how the threat will operate with all of his combat multipliers (not just a template of how and where he will move).
- Include the task and purpose of all relevant threat ISR systems.
- Supply the level of detail appropriate for the audience in a user-friendly manner.

2-11. The lessons learned discussed herein are from the National Training Center but apply to any brigade or regiment and battalion or squadron level S2.

2-12. During mission analysis, expect your S2 and staff to "paint a picture" you can remember. Require your S2 to begin with the bottom line up front. They should produce the following during mission analysis and present it during the mission analysis brief.

- Battlefield environment visualization analysis and products to include terrain and current weather and weather effect charts.
- Threat organization and timelines: macro to micro. Develop the threat picture from the largest echelon given all the way down to individual vehicle, time permitting. The timelines should also reflect from largest echelon to smallest element.
- Threat commander's intent (two levels up in terms of strategic and tactical missions).
- Threat COA sketches (macro-level).
- Threat COA snapshots. This includes sketches and overlays consisting of the task and purpose of all relevant threat intelligence operating systems (for example, detailed situation templates).

BATTLEFIELD ENVIRONMENT VISUALIZATION ANALYSIS AND PRODUCTS

Terrain

2-13. Expect your staff (led by the S2 and supported by the Engineer Officer) to clearly illustrate how terrain will affect the movement of friendly and threat forces.

- Include the entire AOI.
- Demonstrate the terrain's effects (line of sight, covered and concealed mobility corridors) on combat, CS, and CSS operations.
- Emphasize the significance of key and decisive terrain.

2-14. When possible, your S2 and staff should use and brief from 1:12,500 or 1:25,000 scale maps or photographs to supplement standard 1:50,000 scale maps—a higher resolution map provides a better depiction of the terrain. The divisional terrain team is the primary source of terrain data. Some other products available include digital terrain elevation data (DTED), Arc Digitized Raster Graphics (ADRG), satellite imagery, and the Urban Tactical Planner (UTP) (see FM 5-33).

2-15. In stability operations and support operations, your S2 and staff must analyze and describe those population characteristics that are important to your mission (for example, knowing the routes that are off limits to US forces but available for the threat to accomplish house bombings and theft of building supply materials).

Weather

2-16. Expect your S2 to communicate how weather affects operations in the initial IPB analysis and products. An example of an important impact of weather is the increased effectiveness of obscuration during an operation because of a low wind speed and temperature inversion.

2-17. Weather may have a unique impact on stability operations and support operations in both threat and friendly operational patterns. For example, weather could—

- Cause the threat to cancel demonstrations or rallies during inclement weather.
- Affect friendly psychological operations (PSYOP) because rain and heavy winds disrupt leaflet drops.
- Impact civil affairs (CA) operations; heavy rain could disrupt construction projects or a medical and veterinary assistance program.

THE THREAT

2-18. The S2 should remember that the threat will be capable of adaptive operations, asymmetric methods of attack, hiding their operational patterns from friendly forces, and conducting atypical operations. An asymmetric approach is the employment of non-conventional forces, means, or technology (such as weapons of mass destruction [WMD], small-scale chemical attacks or computer network attacks) to offset the advantage of a superior military force. One possible threat COA would be to apply an asymmetrical method and attack US Forces at a critical point when we are vulnerable in order to prevent us from synchronizing our operations. For example, a terrorist attack on the infrastructure of a port of debarkation just as US Forces start to deploy could have a devastating impact.

2-19. Within the current operational environment, friendly forces face the probability of deploying with few or no threat models (that consist of doctrinal templates with a description of tactics and options and type high-value target [HVTs]). During staff operations the CofS (XO) ensures all staff members participate in and provide their functional expertise into the IPB process and ISR planning and execution under the direction of the G2 (S2). In many operations, your staff will have to perform detailed analysis over a period of time in order to determine threat patterns and develop threat models. However, the staff must develop a modified combined obstacle overlay (MCOO), multiple situation and event templates, and other IPB products. In order to support planning, the staff adapts these products based on the particular operation. The staff must develop these products in spite of the difficulty of developing threat models and predicting threat actions for an adaptive adversary.

2-20. One technique to deal with the uncertainty of making predictions without a threat template for an adaptive adversary is to develop more tailored threat models and templates for specific types of smaller scale activities than the staff produces for conventional offensive operations. While some of the models and templates will contain less level of detail, these products can cover more “worst case” and “most likely” threat operational patterns and COAs. Like most staff planning processes, IPB only reflects the staff’s best assessment. In these circumstances operational planners may use techniques to accept less or mitigate risk in the conduct of operations (for example, developing more branches and sequels). Even after the intelligence staff identifies threat patterns and develops threat models, analysts must remain vigilant and try to predict those operational changes an adaptive threat is most likely to adopt. The IPB discussion within most of the rest of this chapter is based on Krasnovian Opposing Forces (the Army’s standard training and simulations tool) and the use of threat models and the other mandatory IPB.

Threat Organization And Timelines: Macro to Micro

2-21. Expect the S2 to describe those forces the threat will use, or potentially use, in the conduct of his operations. An order of battle (OB) chart, as shown in Figure 2-3, is a good tool. The chart should include the unit designation, if known, the type of unit such as a tank regiment, and the equipment by nomenclature and number within the unit (for example, 104 x T-72's; 33 x BMP-3's), and unit subordination.

2-22. Some threats could use indirect, often subtle methods to attack US Forces. The assumption that the adversary will “fight fair,” consider delivery methods or collateral damage, or comply with the current “laws of warfare” is not necessarily true.

2-23. Your S2 can also produce a graphic timeline, as depicted in Figure 2-4, to assist in developing your own COAs and associated decisions. The threat COA matrix in Figure 2-5 shows a comprehensive breakdown of several different threat COAs.

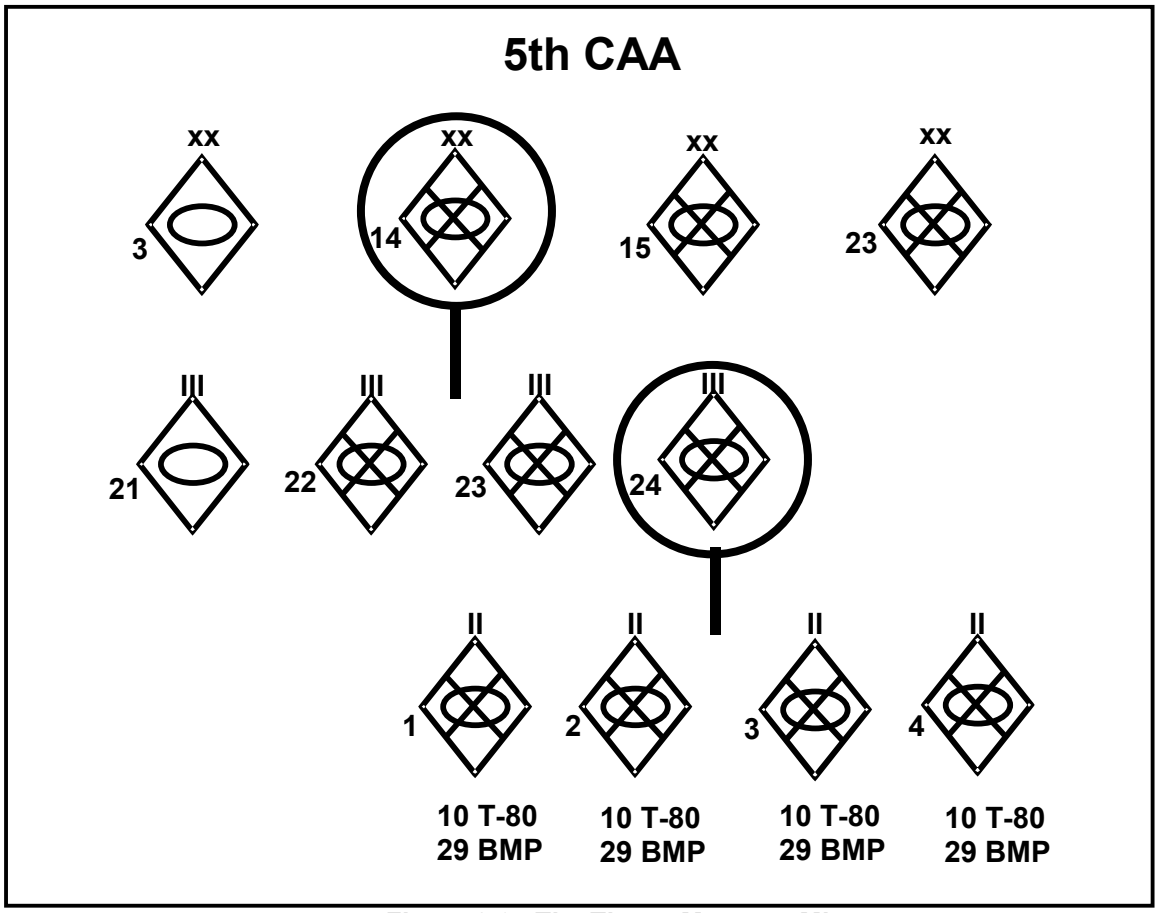


Figure 2-3. The Threat-Macro to Micro

2-24. The threat COA matrix works equally well in stability operations and support operations. The threat COA may include demonstrations causing US casualties, interrupting relocation efforts, or disrupting elections. The rest of the matrix should reflect friendly actions to counter threat actions.

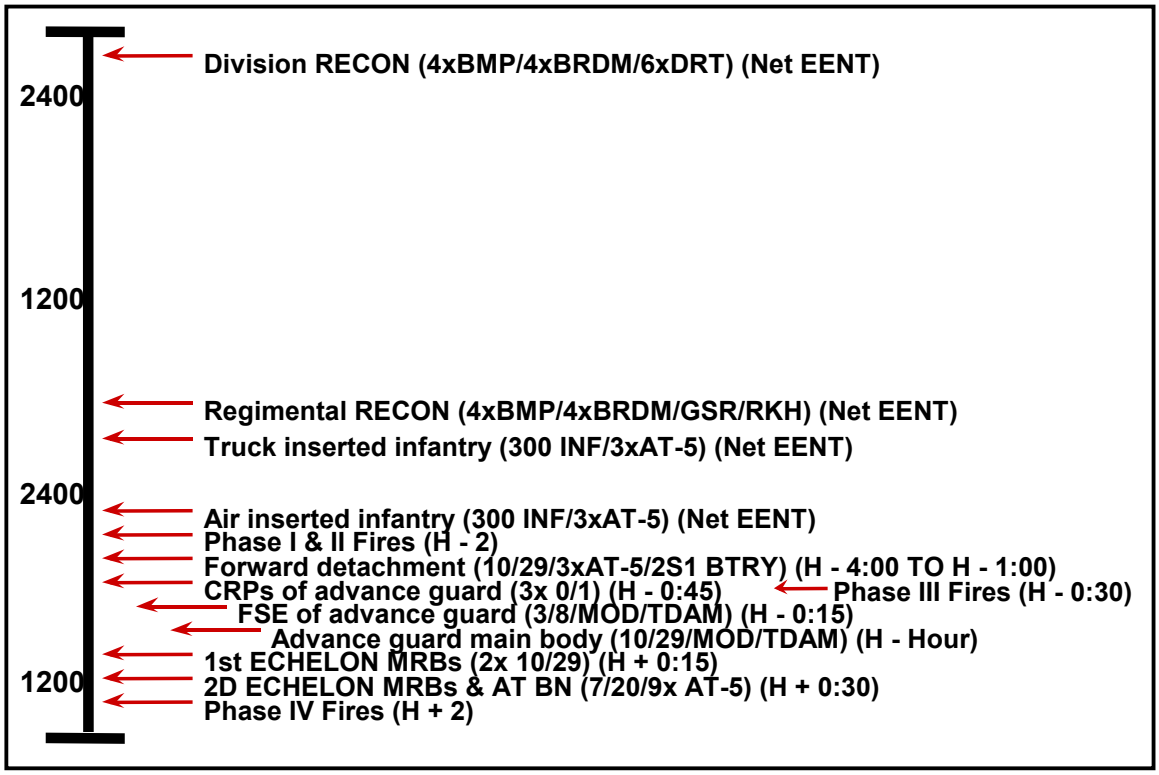


Figure 2-4. Threat timeline

	Threat COA 1 (Brown Pass)	Threat COA 2 (Debnam Pass)	Threat COA 3 (South Wall)
TF Destroyer	Truck insert and infiltrate to goat trail to attrit CO/TM	Truck insert and infiltrate to Debnam Pass to breach and facilitate movement of the regiment main body	Truck insert and infiltrate to secure Hill 899 to facilitate the movement of the AGMB
TF Angel	Air insert and infiltrate through Bruno Escarpment to attrit northern CO/TM	Air insert vic Matterhorn and infiltrate to attrit CO/TM	Air insert vic Matterhorn and infiltrate to prevent repositioning
FD	Atk to secure Brown Pass to open point of penetration	Atk to Brigade Hill to facilitate movement of regiment main body	FD: Atk to fix two CO/TMs of northern TF
Special Munitions	Prevent forces from repositioning north out of Colorado/Washboard	Prevent forces repositioning out of Colorado/Washboard and protect the north flank of the regiment	Protect the north flank of the regiment
FSE of AG	Atk to secure Brown cut or reinforce FD	Atk to secure Debnam Pass to facilitate movement of the regiment main body	Atk to Brigade Hill to facilitate movement of regiment main body
AGMB	Atk to secure Crash Hill to protect the south flank of the regiment	Atk to secure Debnam Pass to facilitate movement of the regiment main body	Atk to Hill 899 to facilitate movement of regiment main body
1st Echelon North	Atk to seize the regiment subsequent objective	Atk to secure Crash Hill to protect the north flank of the regiment	Atk to secure firing lines to protect the north flank of the regiment
1st Echelon South	Atk to seize the regimental subsequent objective; O/O protect the south flank of the regiment	Atk to secure firing lines vic Matterhorn to protect the south flank of the regiment	Atk to secure the regimental subsequent objective
AT Bn	Protect the south flank of the regiment	Protect the south flank of the regiment	Protect the north flank of the regiment
2d Echelon	Follow and assume main effort	Follow and assume main effort	Follow and assume main effort

Figure 2-5. Threat COA matrix

Threat Commander's Intent

2-25. Expect your S2 to clearly articulate how the threat perceives our operations and the threat commander's intent (from one echelon down to two echelons up). The threat commander's intent should be loosely based off your intent. The threat's perception of us and the threat intent drives how the S2 develops each threat COA (by identifying logical options).

2-26. Your S2 should develop the threat intent and the initial threat COA from macro to micro resolution. Many threats use some form of doctrine to conduct operations (for example, fixing a part of a defensive position, while suppressing, and flanking another part of the same position).

Threat COA Sketches (Macro-Level)

2-27. Expect your S2 to use cartoon sketches to show all feasible threat COAs. These sketches should show the threat mission statement and how the threat will fight. You

should address all the sketches to better prepare you to deal with a thinking and adaptive threat.

2-28. Although the S2 can develop a full set (five or more) of broad sketches, he rarely has the time to develop that many detailed threat COAs (for example, detailed situation templates). Your S2 should provide you with two or three detailed threat COAs and two or three broad threat COAs. The total package helps build more flexibility into the plan. At a minimum, the detailed threat COAs must include the most dangerous and most likely threat COAs. Remember, the most likely and most dangerous threat COAs can change based on your actions or COA and how much information the threat collects about you.

Example for Most Probable Threat COA

During mission analysis the S2 decides the threat's most probable COA is to attack into the northern part of the friendly sector. The IPB process drives a friendly COA to defend with a heavily weighted effort in the north. Successful threat reconnaissance reports that the bulk of the engineer effort, especially obstacle work, is occurring in the north.
The threat may have initially planned to attack north but decided against it once his reconnaissance confirmed your strength. Expect your S2 to consider and articulate this type of possibility when briefing.

2-29. Figures 2-6 through 2-9 show a method of using a combination of text and graphics to communicate several feasible threat COAs quickly and clearly.

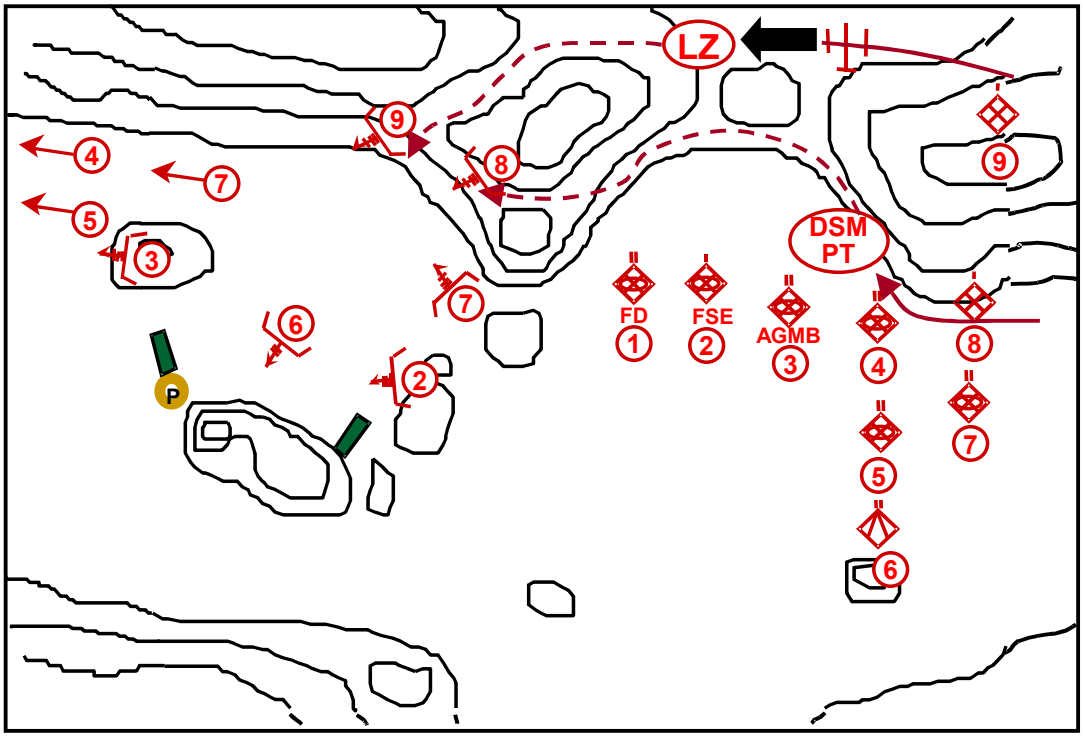


Figure 2-6. Brown Pass (Threat)

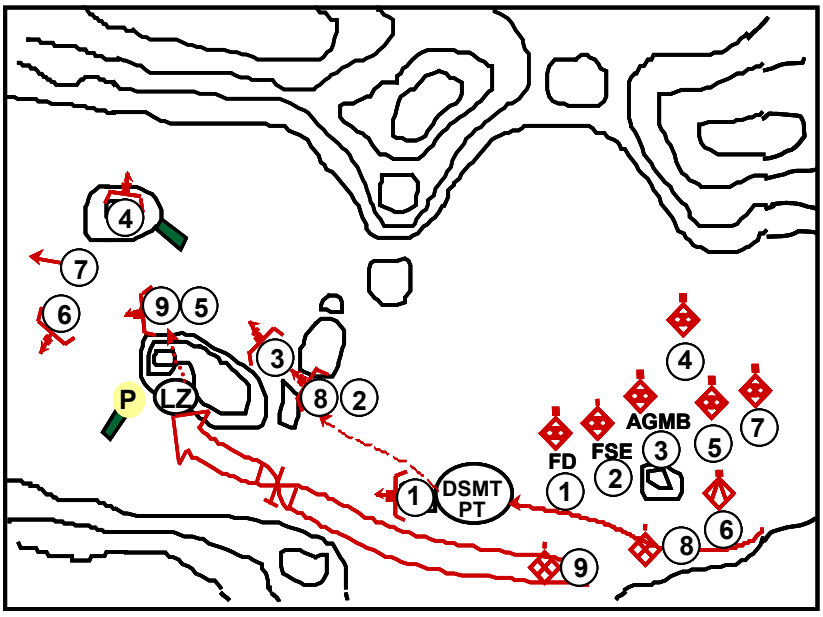


Figure 2-7. Debnam Pass (Threat COA 2)

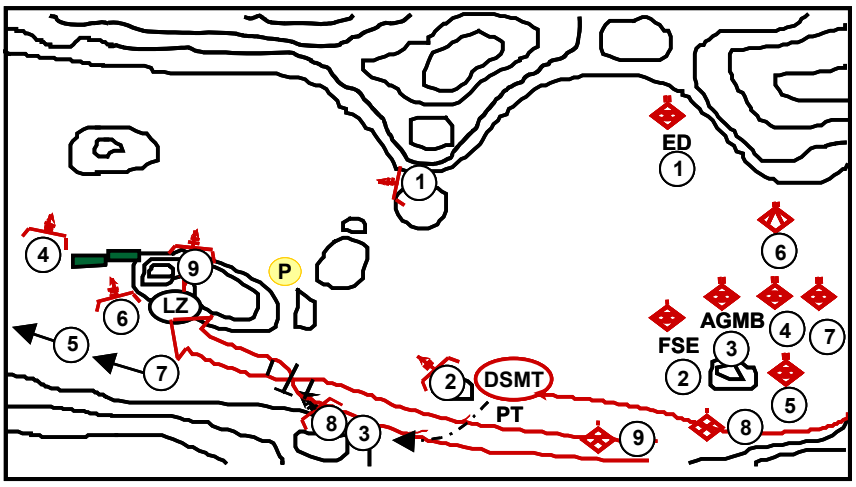


Figure 2-8. Southwall (Threat COA 3)

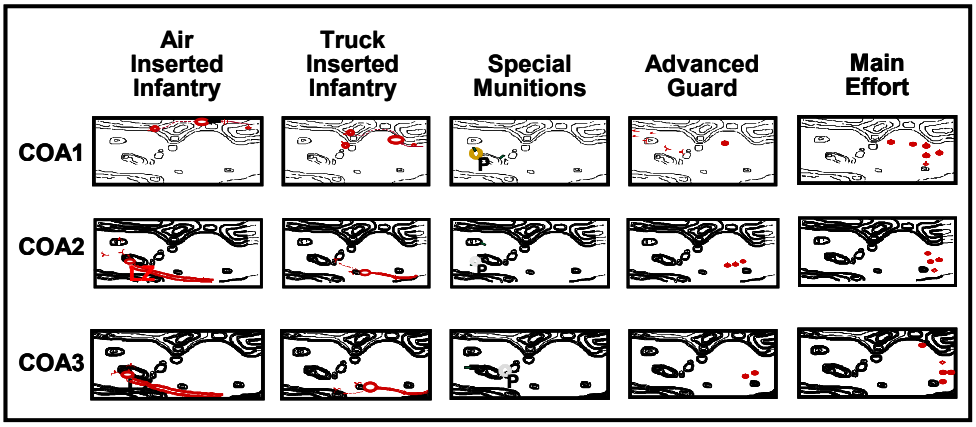


Figure 2-9. The Storyboard

2-30. Figure 2-9 is a storyboard that shows broad threat COAs during a motorized rifle regiment (MRR) attack. Similar map sketches showing the necessary terrain are pasted in each square. Threat critical events are labeled across the top of the chart and each box provides a space for your S2 to sketch out different threat options. Each sketch should include composition, task, and purpose.

2-31. In a stability operation or support operation, intelligence may reveal that the intent of the threat is to force the US military to leave. Based on this intent, the S2 develops a threat COA for inflicting US casualties. The S2 expects the attack will come from a paramilitary organization and describes the threat COA using a sketch (see Figure 2-10).

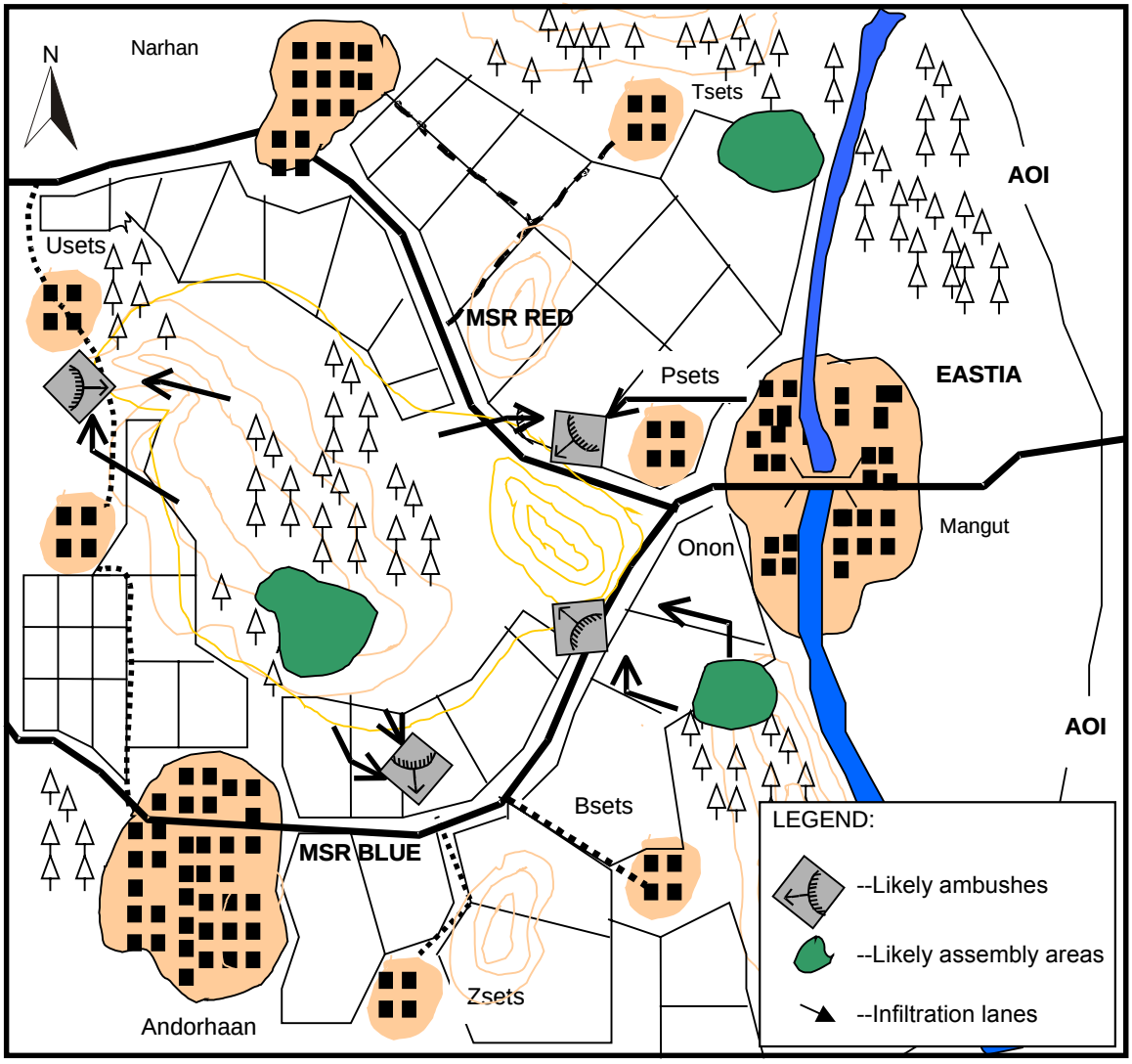


Figure 2-10. Threat COA

2-32. Every option should indicate something critical (an indicator) to the threat's plan. Once the threat starts their operation your S2 can quickly confirm and/or deny threat COAs.

Threat COA Snapshots

2-33. Without an accurate depiction of how and when threat forces will deploy, it is difficult to adequately plan operations (in accordance with your intent). If possible, your S2 should develop threat models before deployment. If your S2 "front loads" this work, he can easily build a detailed situation template.

2-34. It is also important that your XO takes the lead and ensures that the IPB process is really an integrated staff effort. Every staff or functional area representative should fully participate in each step of IPB (this is sometimes referred to as the cross-BOS IPB effort). The bottom line of this participation is "red hat" analysis of their staff or functional equivalent and integrating the results into existing or additional IPB products. For example, the brigade fire support coordinator (FSCOORD) should help the S2 template threat artillery, identify the threat's high-payoff targets (HPTs) (friendly assets whose destruction is critical to support the threat mission), and timeline important phases of fire. This type of staff interaction is critical to the quality of the IPB process and products and to meet the short timelines for initial IPB.

2-35. Expect your S2 and staff to provide you with the threat's method of employment to include dispositions, main effort, scheme of maneuver, and his use of a full range of combat multipliers. An effective way to do this is to create predictive snapshots of the threat at critical places and times. Figures 2-11 through 2-13 illustrate a technique to display the critical events of an MRR attack. Figure 2-14 shows these figures in a consolidated format.

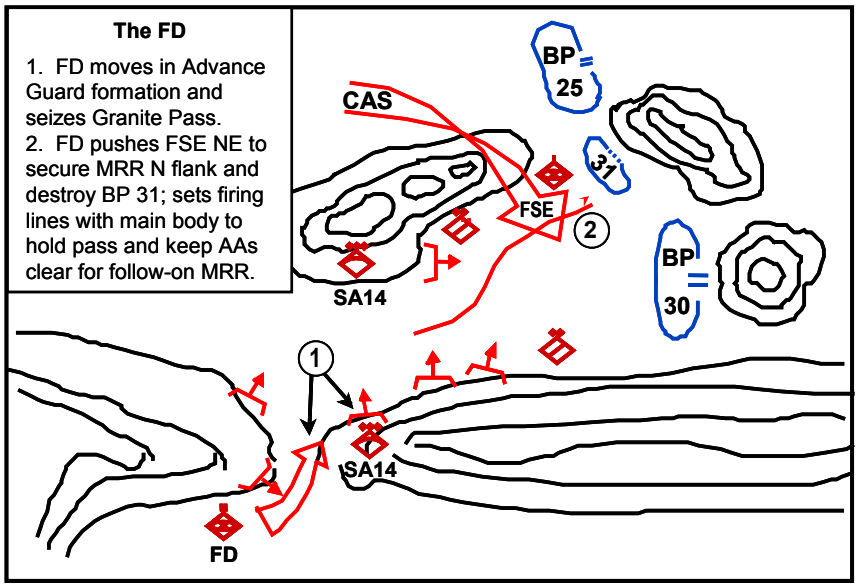


Figure 2-11. Snapshot Sketch #1

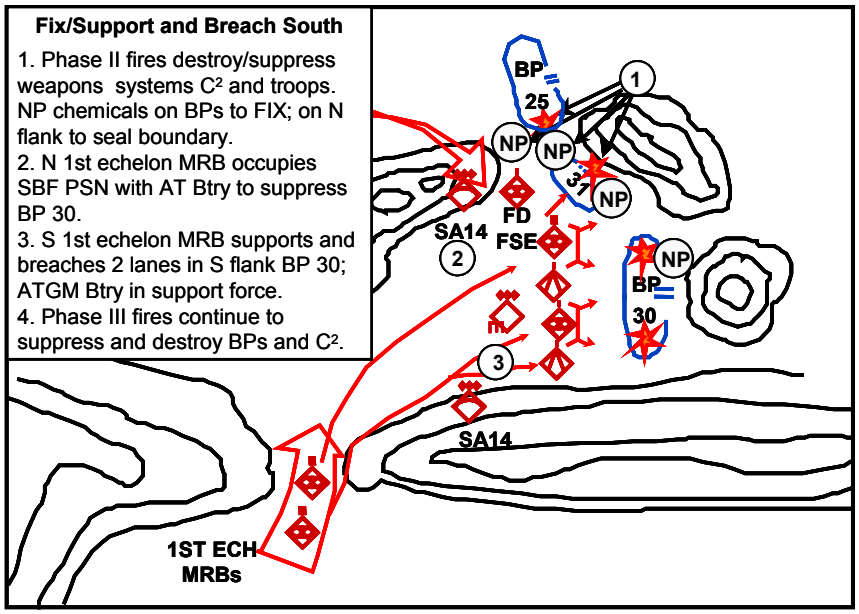


Figure 2-12. Snapshot Sketch #2

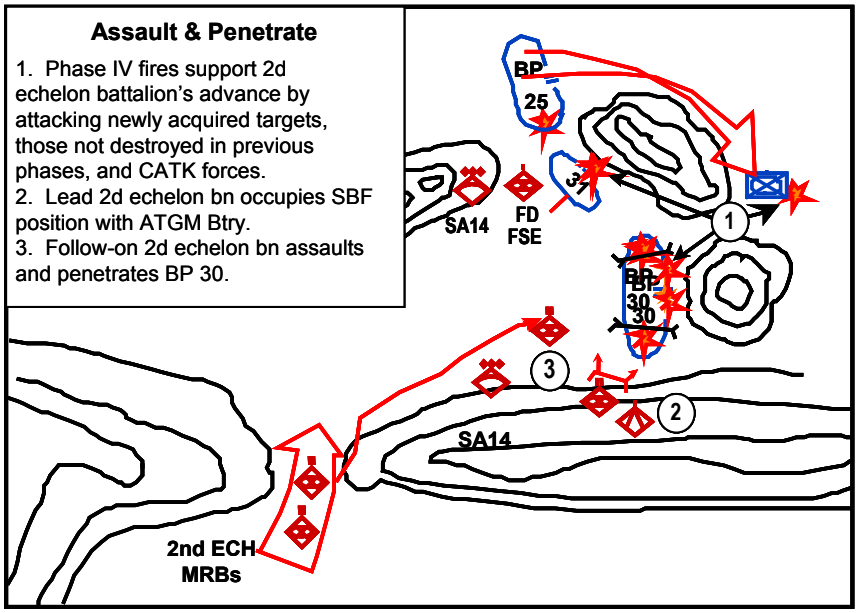


Figure 2-13. Snapshot Sketch #3

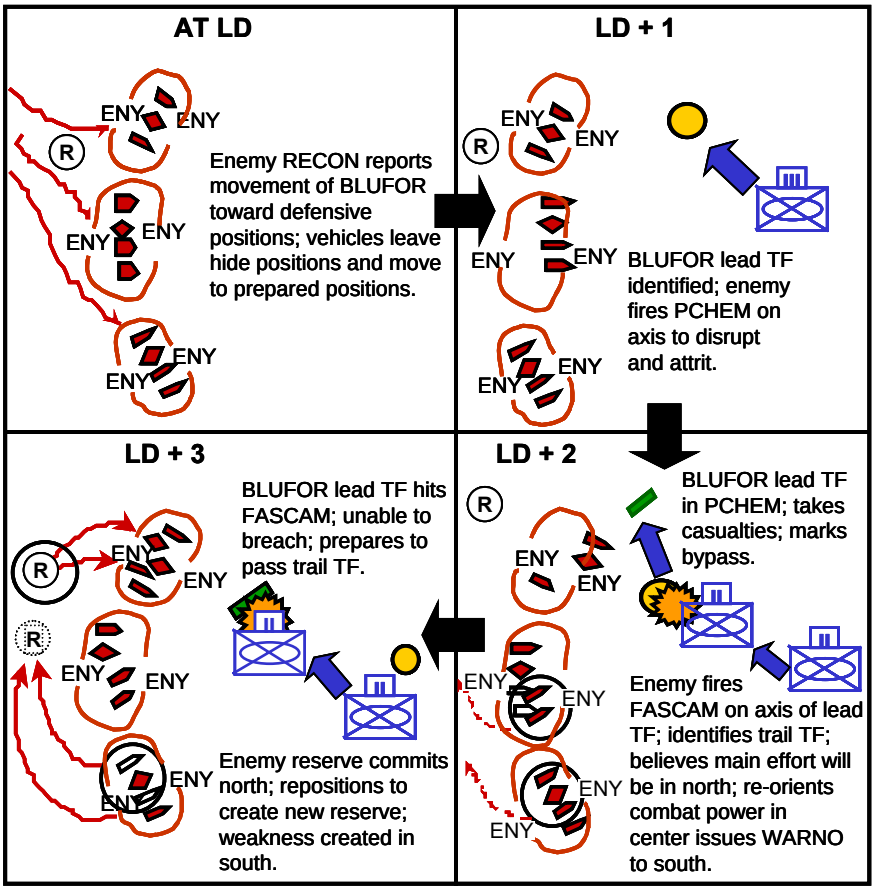


Figure 2-14. Threat COA sketch

FRIENDLY VULNERABILITES

2-36. Your S2 is responsible to provide a detailed description of how the threat can exploit any friendly vulnerabilities. There are three questions that your S2 uses to predict how the threat will try to exploit friendly vulnerabilities.

- Where are we vulnerable? The S2 must determine where (for example, critical systems or world opinion) the threat believes we are vulnerable and also looks at where you and your staff assess you are vulnerable.

- What will they attack? The S2 then looks at the friendly plan and threat capabilities and COAs to determine what the threat commander will most likely attack. This analysis supports the determination of essential elements of friendly information (EEFI) and friendly operations security (OPSEC) measures. Additionally, at higher echelons this helps drive CI analysis.

- When and how? By analyzing what the threat will attack, the S2 then uses threat doctrine or a reasonable prediction of likely actions to answer how and when the threat will attack.

Chapter 3

S2/G2 Organizations and Functions

THE BATTALION S2

3-1. Your battalion S2 section is austere. Even when fully staffed, your S2 section is not resourced to conduct sustained operations at both the tactical operations center (TOC) and tactical command post (TAC). Battalion S2 operations usually provide few detailed products because of the lack of time and resources.

OPERATIONS

3-2. Every member of the S2 section should be able to perform any of the intelligence functions. Your S2's priorities are to—

- Perform mature IPB (for more information, see Chapter 2).
- Plan, task (through your S3), and control ISR operations as part of an integrated effort by your staff. You must protect your scant resources and focus on your PIR.

3-3. The S2 must carefully drive planning that leads to the scout platoon mission. The fragmentary order (FRAGO) that the scout platoon uses to begin its mission must include precise guidance on the infiltration method, collection tasks, reporting criteria and timelines, fire support, casualty evacuation plan, and many other aspects of the mission. The S2 should also debrief scouts and patrols, when time permits, to obtain all relevant information. The S2 should also—

- Task frontline troops and combat patrols for collection.
- Perform a very basic level of situation development to advise you on threat actions, capabilities, and vulnerabilities.

3-4. Reports from scout platoons and every company or company team vary in accuracy. The S2 must conduct analysis to integrate all the information from many means (for example, the scouts, fire support net, and command net) to provide you timely, relevant, accurate, and predictive intelligence as you execute the operation.

STAFF INTERACTION

3-5. Although the XO is responsible for integrating and synchronizing operations plans (OPLANs) and operations orders (OPORDs); directing and supervising the staff's planning process; and ensuring all staff members provide IPB input to the S2/G2, your XO, S2, S3, Fire Support Officer (FSO), and Engineer Officer should work closely in planning and synchronizing battalion operations. Through the XO, train your S2 on the products you expect him to produce and your standards. You and your XO must also train your staff on intelligence capabilities, limitations, and operations.

PRODUCTS

3-6. Your S2 does not have the time nor the resources to develop many detailed IPB products. Once you and your S2 accept the brigade IPB results, the S2 section starts to develop those products to the level of detail needed to support battalion operations.

3-7. Your S2 should always produce (and modify when necessary) the following:

- A set of detailed situation templates or other threat model for at least two threat COAs (most dangerous and most likely).
- An event template.
- An integrated ISR plan to answer your PIR in a timely manner.
- The intelligence portion of the decision support template (DST).

MI SUPPORT AND ATTACHMENTS

3-8. Except for ground surveillance radar (GSR) and the Remotely Monitored Battlefield Sensor System (REMBASS), you will probably not have MI assets attached to your unit. Ensure your staff fully integrates any MI assets you receive into the ISR plan. However, you can expect additional MI support and assets operating in your AO during stability operations and support operations (particularly tactical HUMINT teams).

THE BRIGADE S2

3-9. The S2 section is much larger at the brigade level than at the battalion. However, light brigades will have fewer personnel than heavy brigades.

OPERATIONS

3-10. IPB is a more systematic process at brigade level than at battalion level. A significant amount of training is necessary at the brigade level to bring the section together as a team. Your S2 will have to conduct a more thorough and comprehensive IPB and situation development (this includes accepting risks with the predictive nature of IPB). These tasks require a confident, experienced tactical MI officer who understands friendly operations and the threat.

3-11. If you do not have organic scout assets (like the brigade reconnaissance troop), you will have to either use subordinate unit soldiers and equipment to perform that function or rely on subordinate battalions and the division to provide you information and intelligence. When scouts are organic to the brigade, the brigade S2 should drive the planning just like the battalion S2.

STAFF INTERACTION

3-12. Although the XO is responsible for integrating and synchronizing OPLANs and OPORDs; directing and supervising the staff's planning process; and ensuring all staff members provide IPB input to the S2/G2, your XO, S2, S3, FSO, and Engineer Officer should work closely in planning and synchronizing brigade operations. Due to the size of the brigade staff, it is not as easy for you, the XO, and the S2 to educate the entire staff on intelligence operations. An aggressive series of officer and noncommissioned officer (NCO) professional development classes can help train your staff on intelligence. The S2 section must carefully disseminate intelligence to many users to include using short but

effective briefings. Through the XO, train your S2 on the products you expect him to produce and your standards. You and your XO must also train your staff on intelligence capabilities, limitations, and operations.

3-13. As a rule, the S2 sends an assistant S2 with an analyst to the brigade TAC to perform limited analysis and advise the commander and any staff (when they are present). For detailed analysis the TAC must depend on the TOC.

PRODUCTS

3-14. Your brigade S2 develops more products (representing a larger area and some with more detail) than the battalion S2. When your brigade S2 completes his products and forwards them to the battalion S2, he should expect to explain the results, answer questions on his analysis and products, and change any products as appropriate. Your S2 should always produce (and modify when necessary) the following:

- Basic products to describe the battlefield's effects to include weather and terrain. In stability operations and support operations, the S2 must produce more complex products that graphically depict key characteristics of the local population.
- A set of detailed situation templates or other threat models for at least three threat COAs (to include the most dangerous and most likely).
- An event template, the intelligence estimate, and an integrated ISR plan (with a supporting ISR matrix) to answer your PIR in a timely manner.
- The intelligence portions of the DST and operating system synchronization matrix (for example, PIR, named areas of interest [NAIs], and R&S collection).
- A separate ISR synchronization matrix that ties the integrated ISR plan with the operating system matrix.
- Appendix B, Intelligence to the OPORD (a good matrix appendix is acceptable).

TYPICAL MI SUPPORT TO A BRIGADE

3-15. Your brigade is normally supported by a direct support (DS) MI company with a habitual relationship to your brigade (see Chapter 4). The DS MI Company provides several significant capabilities:

- A commander to help the S2 plan.
- C^2 for all MI assets (to include any other assets or units attached or supporting the brigade). The MI company command post serves as the control mechanism for all MI assets. Any additional control teams that support the brigade (for example, a tactical HUMINT control team during some types of operations) collocate and operate with the analysis and control team (ACT).
- Analytical support to the S2 and processing and fusion systems.
- Organic intelligence collection systems.

THE DIVISION AND CORPS G2

3-16. The G2 sections at division and corps are significantly larger staff organizations than the brigade S2 section. For example, the G2 section functionality normally includes

a Deputy G2, Operations, Plans, Training, special security officer (SSO), CI, terrain team, and the ACE, and is supported by the staff weather officer (SWO).

OPERATIONS

3-17. The G2 operations officer directs and coordinates intelligence, the division SSO, the staff weather team, and the terrain team based on G2 guidance. He is responsible for proper integration and dissemination of all intelligence and combat information that the ACE and subordinate S2s report. He combines that intelligence and combat information and presents the current intelligence (the threat portion of the common operational picture) to the commander and staff. This helps the division commander visualize his battlespace, by graphically and effectively depicting the environment, and depict current threat actions and predicted threat capabilities, intentions, and COAs.

ANALYSIS AND CONTROL ELEMENT (OPCON)

3-18. The ACE is the focal point for all division ISR operations (to include planning, processing, producing, and dissemination). It consists of a single-source analysis section, an all-source analysis section, a collection management team, and a targeting team. The ACE is under operational control (OPCON) to the G2 (from the MI battalion). ACE personnel perform all of the tactical intelligence tasks (see Chapter 1) in support of division operations. The ACE fuses information from all ISR assets and units into intelligence products and the all-source correlated database. The ACE also provides an accurate, relevant picture of the battlefield to the G2 operations section. The G2, terrain team, SWO, and ACE work together to develop, present, and distribute IPB products across the division.

PLANS

3-19. The G2 plans is responsible for all products required for mission analysis and wargaming. (He is supported by the all-source production section of the ACE.) The G2 plans drives the MDMP because he understands and describes the environment and the threat. During mission analysis, the planner also relies on the electronic warfare officer (EWO), SWO, and terrain team for products and integrates the products into the wargame and targeting sessions.

TRAINING

3-20. The G2 training office can help you train your S2 and his section. The training officer prepares and consolidates the intelligence requirements for field training exercises, command post exercises, joint training support, and other training events. Along with the G3, this office develops the training requirements and standards for the division intelligence system and interfaces with intelligence simulation systems. The training office also manages the division's readiness training and other valuable intelligence training programs.

STAFF WEATHER OFFICER (SPECIAL STAFF UNDER THE G2)

3-21. The Air Force provides an SWO and a supporting combat weather team (CWT) to major subordinate commands, corps, divisions, and separate brigades to work under the supervision of the G2. The CWT can provide tailored tactical decision aids and overlays depicting the effects of weather on systems, personnel, and equipment.

TERRAIN TEAM (NO COMMAND OR SUPPORT RELATIONSHIP)

3-22. The G2 is the primary "customer" for terrain analysis. The terrain team supports

the G2 by providing terrain analysis and analysis products to describe the battlefield's effects. The terrain team can provide unique products for use by the intelligence analysts in determining AAs, axis of advance, and mobility corridors. (NOTE: the G4, and not the terrain team, is responsible for supplying Army units with maps.)

ELECTRONIC WARFARE OFFICER (NO COMMAND OR SUPPORT RELATIONSHIP)

3-23. Although the EWO works directly for the G3 and is integral to integrating EW into the targeting process, he is an intelligence officer and works closely with the ACE and G2 plans officer. He is also involved in coordinating frequency management and deconfliction with the division signal officer prior to planning and executing EA missions.

OPERATIONS

3-24. The division and corps G2s work together to build a complementary intelligence architecture within the corps. Each echelon has unique collection capabilities and requirements, but both G2s (and their ACEs) rely on a distributed and collaborative environment that allows users to share both information and intelligence down to the battalion level (through your S2).

3-25. Depending on the intelligence architecture and who is designated the joint task force (JTF) and/or the Army force (ARFOR), the division G2 coordinates with the corps or ARFOR G2 to—

- Maintain the integrity of most intelligence databases.
- Provide detailed, thorough, and "long-term" analysis.
- Conduct more robust ISR collection and processing (through more capable downlinks like certain Tactical Exploitation of National Capabilities [TENCAP] systems). Some of these units and/or systems may operate in your AO, especially during stability operations and support operations. They also may provide you with tactical HUMINT teams.

Chapter 4

Military Intelligence Capabilities

No single echelon has sufficient organic intelligence capabilities to satisfy all of your requirements. In order to efficiently use the intelligence operating system, you must understand the following:

- Intelligence disciplines.
- Intelligence functions.
  - Combat information and intelligence.
  - Electronic warfare.
- MI organizations.
- Limitations of intelligence.

To clearly describe the intelligence operating system, intelligence is divided into five disciplines and two multidiscipline functions (CI and Technical intelligence [TECHINT]).

- HUMINT.
- Imagery intelligence (IMINT).
- Measurement and signature intelligence (MASINT).
- Signals intelligence (SIGINT).
- All-source intelligence.

INTELLIGENCE DISCIPLINES

4-1. The first five disciplines are directed toward the collection, processing, and analysis of information from a specific category of sources. The two multidiscipline functions are directed toward the integration of the information collected through the first five disciplines and the production of a category or categories of intelligence. Intelligence production includes the intelligence categories of I&W, current, general military, target, and scientific and technical intelligence (S&TI). CI produces the intelligence category of CI.

4-2. Single-discipline collection or analysis rarely produces a comprehensive picture of the threat and is subject to deception. However, all-source intelligence that is produced from an adequate amount and mix of information (from the different disciplines) will meet your requirements. Each discipline must complement and cross-cue each other for maximum effectiveness. All disciplines use a combination of open and closed sources in the process of their collection and/or production.

HUMAN INTELLIGENCE (HUMINT)

4-3. HUMINT is the intelligence derived from the analysis of information obtained from a human source or a related document by a HUMINT collector. The HUMINT discipline

includes those personnel and organizations directed toward the collection, processing, analysis, and production of HUMINT.

- A HUMINT source is a person from whom information can be obtained. The source may either possess first- or second-hand knowledge normally obtained through sight or hearing. HUMINT sources include literally every human being (non-US citizens). Potential HUMINT sources include threat, neutral, and friendly military and civilian personnel; people of all ages, occupation, ethnic, religious, economic, and political groups.

- A HUMINT collector is a person who by training is tasked with and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. HUMINT collectors specifically include personnel in military occupation specialty (MOS) 97E (HUMINT) and Warrant Officers in MOS 351E (HUMINT). Other personnel that can perform HUMINT collection tasks are unit S2s acting in the capacity of tactical questioners, CI agents involved in counterintelligence force protection source operations (CFSO) and Special Forces personnel engaged in low-level source operations.

- HUMINT collection involves the use of tactical questioning, interrogation, debriefing, elicitation, and document exploitation (DOCEX) techniques to extract information from a HUMINT source. For more information on HUMINT, refer to FM 34-5(S) and FM 2-22.3 (FM 34-52).

EMERGING DOCTRINE (TACTICAL HUMINT)

Tactical HUMINT is the combination of HUMINT collection assets and CI assets using HUMINT collection techniques to support a tactical commander. This package provides a unique ability to support force protection, conduct HUMINT collection (to include counter-HUMINT), or to perform vulnerability assessments and is more common in stability operations and support operations than in war. Tactical HUMINT platoons and teams are task organized based on METT-TC. When supported by a platoon or team, it is important that you—

- Understand the capabilities, control requirements, and limitations.
- Weigh your requirements for intelligence and force protection against the risk to the platoon or teams.
- Approve the best mix of HUMINT collectors and CI personnel (through the DS MI company and employment techniques).

IMAGERY INTELLIGENCE

4-4. IMINT is the intelligence derived from the analysis of imagery derived from, but is not limited to, radar, infrared, optical, and electro-optical (E-O) sensors. The IMINT discipline includes the

following personnel and organizations directed toward the collection, processing, analysis, and production of IMINT:

- Imagery Sources (LRS, Apache, Kiowa Warrier, HUMINT).

- Imagery Collectors (U2R Advanced Synthetic Aperture Radar System [ASARS), Joint Surveillance Target Attack Radar System [Joint STARS], unmanned aerial

vehicle [UAV], TENCAP systems, and airborne reconnaissance low-multifunction [ARL-M]).

4-5. For more information on IMINT, refer to FM 2-50.1 (FM 34-25-1), FM 2-55.1 (FM 34-25-2), and TC 34-55.

MEASUREMENTS AND SIGNATURE INTELLIGENCE

4-6. MASINT is the intelligence derived from the analysis of information gathered by technical instruments such as radars, lasers, passive E-O sensors, radiation detectors, seismic, and other sensors to measure objects or events to identify them by their signatures. The MASINT discipline includes those personnel and organizations directed toward the collection, processing, analysis, and production of MASINT. REMBASS is an example of a MASINT collector. (For more information on REMBASS, refer to FM 2-00.10 (FM 34-10-1.)

SIGNALS INTELLIGENCE

4-7. SIGINT is the intelligence derived from the analysis of information obtained through the intercept of adversary communications and noncommunications emitters. The SIGINT discipline includes those personnel and organizations directed toward the collection, processing, analysis, and production of SIGINT. SIGINT is subdivided into—

- Communications intelligence (COMINT).
- Electronic intelligence (ELINT).
- Foreign instrumentation signals intelligence (FISINT).

4-8. Examples of SIGINT ground-based intercept and direction finding (DF) systems are the AN/MLQ-40(V)2 Prophet, AN/PRD-12/13, the AN/TRQ-32A (V) 2 (TEAMMATE), and the AN/TRQ-152 (TRACKWOLF) systems. The GUARDRAIL common sensor (GRCS) is an example of an airborne intercept and DF system for both communications and noncommunications emitters. The AN/FSQ-144V (TROJAN) is the Army's remote collection system supporting in-garrison collection by tactical MI units.

COUNTERINTELLIGENCE

4-9. CI is derived from the analysis of all-source information concerning the threat posed by activities of foreign intelligence and security services and the intelligence activities of non-state entities such as organized crime, terrorist groups, and drug traffickers. The CI discipline includes those personnel and organizations directed toward CI investigations and the collection, processing, analysis, and production of CI. The CI discipline also involves the recommendation of methods to counter the threat intelligence collection effort to include support to OPSEC and deception. CI personnel advise deception planners on the vulnerabilities of threat foreign intelligence services (FISs) and associated battlefield collection systems to various friendly deception capabilities and techniques. For more information on CI functions and activities, refer to FM 2-00.5 (FM 34-5)(S) and FM 2-01.2 (FM 34-60).

TECHNICAL INTELLIGENCE

4-10. TECHINT is the intelligence derived from the scientific analysis of adversary materiel to include its composition, performance, and operational capabilities. The TECHINT discipline includes those personnel and organizations directed toward the

collection, processing, analysis, and production of TECHINT.

ALL SOURCE INTELLIGENCE

4-11. All-Source intelligence is the intelligence derived from the analysis and fusing of all relevant information and single discipline intelligence products. The All-Source intelligence discipline includes those personnel and organizations directed toward the production of all-source intelligence products.

INTELLIGENCE FUNCTIONS

COMBAT INFORMATION AND INTELLIGENCE

4-12. Combat information is unevaluated data, gathered by or provided directly to the tactical commander, which due to its highly perishable nature or the criticality of the situation cannot be processed into tactical intelligence in time to satisfy your intelligence requirements. Every soldier in an operation can contribute to intelligence operations or can provide combat information through timely reporting. Some common sources of valuable and reliable information include—

- Scouts, cavalry, patrols, and individual soldiers, who can provide you with critical and exact information based upon reliable visual contact.

- Long-range surveillance (LRS) units, which provide reliable information against deep targets. LRS units conduct stationary surveillance and limited reconnaissance. They are uniquely equipped and trained to deploy deep into the threat area to observe and report threat dispositions, movement and activities, and battlefield conditions. They are not equipped or trained to conduct direct-action missions.

- Open sources, depending on the operation, are often numerous with information of varying degrees of timeliness, relevancy, and accuracy. An analyst's ability to collect, analyze, and use open-source information, however, is limited by his workload and the time available. Common open sources include news reports, Cable News Network, the Internet, magazines, textbooks, archives, and tours.

ELECTRONIC WARFARE

4-13. EW is one of your multipliers. It can disrupt threat C^2 and fire support communications during a critical phase of operations. There are three elements of EW:

- Electronic warfare support (ES) provides immediate threat intention and targeting information. It also supports all-source analysis, EA, and EP by providing threat recognition, combat information, and target acquisition as well as the specific frequencies and radio nets you want to jam.

- Electronic attack (EA) uses lethal (directed energy) and non-lethal (jamming) electromagnetic energy to disrupt, damage, destroy, and kill threat forces. MI units use non-lethal EA to jam threat C^2 and targeting systems. Electronic deception can also cause a threat to misinterpret your intentions. Used properly EA complements lethal fires.

- Electronic protection (EP) consists of measures to protect your command, control, and communications (C^3) . Your signal officer is responsible for EP.

MI ORGANIZATIONS

MI COMPANY (SEPARATE BRIGADE OR ARMORED CAVALRY REGIMENT)

4-14. This MI company has fewer capabilities than the MI battalion but more capabilities than a DS MI company. The MI company in support of the armored cavalry regiment (ACR) or separate brigade provides—

- Communications intercept, DF, and EA.
- CI.
- HUMINT collection.
- Ground surveillance. This is an interim capability and will end with the fielding of the tactical UAV systems. (Tactical UAVs will be fielded to this organization in the future.)
- Personnel to staff the S2/S3. These soldiers conduct—
  - ISR planning.
  - All-source analysis and dissemination.
  - Technical control and tasking.
  - Intelligence support to force protection and OPSEC support.

EMERGING DOCTRINE (IBCT)

MI COMPANY (INITIAL BRIGADE)

The MI Company conducts intelligence analysis, ISR integration, and HUMINT collection in support of the IBCT. This company supports the planning, preparation, and execution of multiple, simultaneous decisive actions across the distributed AOs. Additionally, it contains a much more robust analytical and HUMINT control and collection capability than the MI companies that support divisional maneuver brigades, separate brigades, and ACRs. This company consists of a—

- Small headquarters element.
- ISR analysis platoon that conducts situation development, target development, and BDA in support of the Brigade S2 section.
- ISR integration platoon that serves as the focal point for intelligence support to planning, situation awareness, and targeting. ISR integration encompasses the tasking, processing, redirecting, and fusion of information derived from sensors across all combat information, target acquisition, and intelligence assets. The most unique feature of this platoon is an organic S2X team that provides dedicated mission management for tactical HUMINT collection—a critical intelligence capability in small-scale contingency operations.
- Tactical HUMINT platoon with both operational management teams and tactical

HUMINT teams.

- US Air Force Combat Weather Team.

SURVEILLANCE TROOP (RSTA SQUADRON – INITIAL BRIGADE)

The surveillance troop is organic to the RSTA squadron of the Initial Brigade. It conducts IMINT, MASINT, SIGINT, and NBC surveillance operations in support of the Initial Brigade's planning, preparation, and execution of multiple, simultaneous decisive actions across the distributed AOs. Successful planning, preparation, and execution of these operations requires the troop's leadership and soldiers to have a clear understanding of the brigade commander's ISR requirements as well as the squadron commander's intent and concept of operations. The surveillance troop consists of a—

- Headquarters section.
- ISR integration team which is collocated with the S2 section at the squadron command post. It supports the S2 in developing, monitoring, and recommending changes to the squadron's operations. Additionally, this team assists the S2 in tracking the execution of the squadron's R&S tasks by receiving and fusing the combat information from RSTA squadron assets into a current threat picture.
- Air reconnaissance platoon (tactical UAV).
- Multi-sensor platoon which includes four multi-sensor sections. Each section consists of a SIGINT team and MASINT team. The platoon depends upon the ISR Integration Team for SIGINT mission management, technical support, and direction finding analysis.
- NBC reconnaissance platoon which can locate and identify life threatening chemical and radiological contaminants, and some forms of biological warfare. The platoon also performs extensive planning and analysis to determine threat WMD capabilities in the brigade's AO.

Additionally, the troop may receive a TROJAN Special Purpose Intelligence Remote Integrated Terminal (SPIRIT) (Light) team from the signal company to support UAV video dissemination.

MI BATTALION (DIVISION)

4-15. The MI battalion at division level provides ground-based communications intercept, DF capability, EA, HUMINT collection, ground-based surveillance, and UAV imagery support (in the future). Specifically, the MI battalion includes—

- LRS teams are deployed 15 to 80 kilometers (km) beyond the division forward line of own troops (FLOT) to observe selected NAIs. Their insertions are time phased to ensure continuous coverage of selected deep divisional NAIs. LRS teams are organic only to light, airborne, and air assault divisions.
- Ground surveillance systems are frequently attached to the maneuver units to locate moving targets. UAV assets (in the DS MI company) will replace these in the future.
- The MI Battalion will also support the division with GS UAV assets in the future.
- The present MI battalion organization includes a battlefield deception cell. That

responsibility will probably transfer to the RC in the future organization.

GS MI Company

4-16. The GS MI company provides intelligence and electronic warfare (IEW) support to the division.

- Deploys ground-based assets throughout the battlefield.
- Will include one UAV baseline GS to the division.
- Is tasked by the MI battalion commander and S3 as directed by the G2 or ACE.
- Responds to centralized control by the MI battalion, which—

— Increases system-tasking flexibility (available systems).

— Allows for coordinated DF operations.

— Contributes to more coordinated and survivable EW operations.

DS MI Company

4-17. The DS MI company provides IEW support to the division's brigades.

- Responds first to the brigades.
- Brigade (through the DS MI company) tasks and moves assets.
- Has CI and HUMINT collection assets.
- Will have UAV imagery capabilities through organic UAV assets.
- Will have a Common Ground Station (CGS) which provides a significant broadcast downlink capability to include Joint STARS moving target indicators.

MI BRIGADE (CORPS)

4-18. The MI brigade provides aerial SIGINT, HUMINT collection, and links to national and theater intelligence systems. The MI brigade can provide IEW assets to subordinate commands to weight the main effort. The corps MI brigade has three battalions: operations battalion, tactical exploitation battalion (TEB), and aerial exploitation battalion (AEB).

Operations Battalion

4-19. The operations battalion provides the ACE that performs IEW analytical, processing, and management functions in support of overall corps operations (see Chapter 3).

Tactical Exploitation Battalion

4-20. The TEB provides CI, HUMINT collection, and LRS support to corps operations. It

provides—

- GS collection to the corps in response to corps taskings.
- CI and HUMINT assets for intelligence support to force protection, OPSEC, HUMINT collection (to include DOCEX), and can be deployed throughout the corps and subordinate divisions.
- The LRS company is reliable and is deployed 60 to 150 km beyond the corps FLOT. Team deployment is time phased based on the friendly concept of the operation, number of NAIs, availability of insertion and extraction means, unique insertion skills, and need for continuous coverage.

Aerial Exploitation Battalion

4-21. The AEB allows the commander to visualize the battlefield well beyond the depth of the AO. The battalion gives you "deep look" aerial R&S and SIGINT collection capability. It provides—

- The ability to weight the main effort by prioritizing intelligence support and responsiveness to subordinate commanders.
- SIGINT data that can be sent in near real time (NRT) to multiple corps and divisional nodes to support situation and target development. With the fielding of the CGS, this information is broadcasted and downlinked through your CGS (in the DS MI company).

LIMITATIONS OF INTELLIGENCE

4-22. Your intelligence operating system has some limitations:

- Intelligence reduces uncertainty on the battlefield but cannot entirely eliminate it—"the fog of war." You will always have to accept some risk.
- You will never have enough organic and DS intelligence assets to satisfy all of your intelligence requirements.
- Limited communications systems within the intelligence architecture which, if not aggressively and proactively managed, can delay the dissemination of intelligence and combat information.
- Single-source collectors are sometimes susceptible to deception. The balanced and focused use of collection assets from multiple intelligence disciplines and careful distributed or collaborative all-source analysis are required to guard against deception.
- Degraded SIGINT collection if the threat chooses not to use communications and noncommunications systems. For example, during Operation DESERT STORM, Iraq did not employ tactical communications for fear of being intercepted and located (by DF systems).
- Adverse weather degradation on ISR operations, antenna arrays, aerial collection, and EA systems.

- Inability of ground-based SIGINT systems to operate on the move. Positioning and integration of mutually supporting ground and aerial SIGINT systems are critical to provide continuous support.

Appendix A

Intelligence and the Military Decision-Making Process

A-1. As the commander and XO, use the seven steps of MDMP to execute actions. This appendix focuses on the role of intelligence and how intelligence supports each step of the MDMP. It provides the commander and XO a checklist to use during the MDMP on what the S2 and intelligence staff provide.

- Step 1. Receipt of the Mission
- Step 2. Mission Analysis
- Step 3. COA Development
- Step 4. COA Analysis (Wargame)
- Step 5. COA Comparison
- Step 6. COA Approval
- Step 7. Orders Production

A-2. The targeting process is closely related to MDMP. The S2 conducts the **detect** and **assess** portions of the targeting process.

WHAT TO EXPECT FROM YOUR S2

STEP 1. RECEIPT OF THE MISSION

A-3. Task the S2 to start work as soon as you get the mission. (See Table A-1.)

Table A-1. Receipt of the mission

Commander's Interaction	
Initial Guidance. • Disagree with higher IPB? • Abbreviated initial IPB? • Initial ISR support? Additional IPB analysis (besides normal procedures)	
Commander's Checklist	
❑ Did the S2 begin parallel planning and collaborate with higher HQ before and during receipt of the mission to facilitate the IPB process? ❑ Did the S2 identify gaps in higher HQ ISR plan, intelligence database, and IPB products? ❑ Did the entire staff identify specified and implied intelligence tasks from higher HQ order to begin the ISR collection effort? ❑ Did the S2 start the terrain products: weather, light, and climatology data?	❑ Is the S2 continuously updating the MCOO and doctrinal templates and maintaining the threat situation? ❑ Did the S2 alert ISR assets of impending mission in order to provide sufficient time to begin troop-leading procedures? ❑ Did the S2 develop and submit initial requests for information based on gaps in the intelligence?

STEP 2. MISSION ANALYSIS

A-4. Ask the S2 for a complete analysis. Understand that everyone, not just the S2, performs IPB. Ask for a staff briefing on these products: complete MCOO, weather and light analysis, situation templates, threat COAs, initial event template, and an initial ISR plan. **Ask the staff where the higher HQ intent is captured in the products.**

Table A-2. Mission analysis

<table>
<tr><th colspan="2">Commander's Interaction</th></tr>
<tr><td colspan="2">Restated mission.

Commander's intent.

Commander's guidance—
• AO.
• AOI.
• Significant characteristics of the environment.
• Who is the threat and what it looks like?
• Choose threat models and identify any refinements.
• How many threat COAs and to what specificity?
• Initial threat culmination criteria.</td></tr>
<tr><th colspan="2">Commander's Checklist</th></tr>
<tr><td>❑ Did the S2 use the other staff officers' areas of expertise in conducting the IPB process?

❑ Did the AOI consider all threat forces— committed, supporting, reinforcing— that can impact your operation from start to finish?

❑ Did the S2 assist in the identification of the initial PIR?

❑ Did the S2 assist in the determination of the initial OPSEC or EEFI requirements to include CI considerations?

❑ Did the entire staff produce a MCOO that—
• Defines defensible terrain?
• Identifies—
– Key or decisive terrain?
– Mobility corridors (air and ground)?
– Restricted or severely restricted terrain?
– Infiltration lanes? Landing zone (LZ) and pickup zone (PZ)?

❑ Did the S2, in conjunction with the entire staff—
• Develop situation templates of the threat based on the constraints of the terrain?</td><td>❑ Do the situation templates—
• Include all committed and reinforcing forces as well as combat multipliers?
• Focus two levels down in detail to include all threat operating systems?
• Identify OB, weaknesses and peculiarities, activities, and capabilities for each COA with graphics?

❑ Do the IPB products identify facts and assumptions that assist in the determination of likely threat COAs?

❑ Did the S2 prepare terrain and weather analysis products to describe what effects will significantly impact the upcoming battlefield on both threat and friendly forces?

❑ Did the S2 develop a line-and-block chart with the number of killing systems depicting the threat composition?

❑ Did the initial ISR plan—
• Consider the AO and the mission statement?
• Consider the current event template?

❑ Is the initial ISR plan based on the—
• PIR?
• Information requirements (IR)?
• NAIs?

❑ Did the S2 provide ISR assets with an initial ISR plan that facilitated dissemination of orders, conduct of rehearsals, and ensured ISR activities in support of the decisionmaking process by ongoing ISR</td></tr>
</table>

• Prepare threat situation templates depicting the threat disposition? • Prepare as many situation templates as time allowed? ❑ Do the event templates identify and focus on— • NAIs? • Time phased lines? • Time distance analysis? • Critical actions? • Threat decision plan? ❑ Did the S2 provide subordinate units with a copy of all intelligence products to facilitate their IPB process?	operations? ❑ Did the S2 incorporate higher HQ collection requirements? ❑ Did the S2 forward intelligence requirements that cannot be answered by assigned collection assets to higher HQ? ❑ Did the MI battalion or DS MI company commander brief the collection status and capabilities?

STEP 3. COA DEVELOPMENT

A-5. Ask for and expect a thorough analysis of the threat on combat organization (composition and disposition) and possible threat COAs. Ask the S2, in conjunction with the entire staff, to provide intelligence about the threat's main effort and how they will employ their combat multipliers (fires, ADA, engineers, C^2, intelligence, CSS, and chemical) to support their COAs. Ask what key indicators are used to confirm or deny threat COAs, critical decision points (DPs), and friendly and threat vulnerabilities. Ask how often the S2 updates intelligence-related products. (See Table A-3.)

Table A-3. COA development decision points

Commander's Interaction	
Has the S2 provided intelligence about— • The threat main effort? • Employment of their combat multipliers (fires, ADA, engineers, C^2, intelligence, CSS, and chemical) to support their COAs? Ask the S2 what the key indicators are used to confirm threat COAs, critical DPs, and friendly and threat vulnerabilities. Ask how often the S2 updates intelligence-related products.	
Commander's Checklist	
❑ Has the S2— • Refined and prioritized the situation templates? • Refined the event template and matrixes? • Developed an initial EW target list (EWTL)? ❑ Did the S2 take an active part in analyzing combat power by providing all available information on the current threat forces and situation? ❑ As time permits, while analyzing relative combat power, did the S2 provide the staff with information on threat vulnerabilities?	❑ Did the S2 consider as many possible COAs as time permits, starting with the most likely and including the worst case (most dangerous)? ❑ Did the S2 provide critical input to the MDMP through continual analysis of information provided by ongoing ISR operations? ❑ Did the S2 and S3 task ISR assets without overtasking them? ❑ Did the S2 and S3 allocate sufficient assets to conduct the ISR plan?

STEP 4. COA ANALYSIS (WARGAME)

A-6. During the wargame each staff member is responsible for his area of expertise. It is recommended that the S2 play the role of the threat commander. (See Table A-4.)

Table A-4. COA analysis (wargame)

Commander's Interaction	
No interaction necessary at this point.	
Commander's Checklist	
❑ Did the S2— • Refine the PIR with the LTIOV? • Assist in the development of the HPTL? • Finalize the situation template? • Redefine the threat COAs based on the developed DPs and finalize the situation template? ❑ Did the S2 develop critical threat DPs in relation to the friendly COA? ❑ Did the S2 fight as an uncooperative threat to develop DPs and project threat losses? ❑ Did the S2, in conjunction with the entire staff, address all relevant threat operating system activities? ❑ Did the S2 assist in developing the target selection standards and attack guidance matrix from the wargamed COAs?	❑ Did the S2 update the collection and ISR plan? ❑ As a result from the wargame, did the S2 identify IR and refine the event template to include NAIs and refine the event matrix with corresponding decision points? ❑ Did the S2 indicate target areas of interest (TAIs) and HVTs? ❑ Did the S2 refine the situation templates from the results? ❑ Did the S2 participate in the targeting process and identify and prioritize HVTs as determined by IPB? ❑ Did the assistant S2 (from the wargame) determine what information to collect, who is to collect, as well as when and where to collect it?

STEP 5. COA COMPARISON

A-7. Although your S2 plays the uncooperative threat commander, he still has requirements to deliver various intelligence products to you and the staff. (See Table A-5.)

Table A-5. COA Comparison.

Commander's Interaction	
No interaction necessary at this point.	
Commander's Checklist	
❑ Did the S2 coordinate with the other staff elements in order to start developing the integrated ISR plan and the intelligence portion of the synchronization matrix?	❑ Did the S2 update the IPB products for the decision briefing?

STEP 6. COA APPROVAL

A-8. Refine the intent statement and CCIR to support the selected COA. The staff refines its products in anticipation of the orders production. (See Table A-6.)

Table A-6. COA approval

Commander's Interaction	
Approved COA. Refined commander's intent. Specified type of order. Integrated ISR plan. Specified type of rehearsal.	
Commander's Checklist	
❑ Did the S2— • Update the PIR with LTIOV for your approval supporting the approved COA? • Finalize the event template matrixes and the ISR plan? • Plan for BDA support in coordination with the ISR plan?	❑ Did the staff refine— • The DST? • The operating system synchronization matrix? • ISM based on the approved COA? • Integrated ISR plan

STEP 7. ORDERS PRODUCTION

A-9. After you issue final guidance, the staff begins preparing the order for dissemination. (See Table A-7.)

Table A-7. Orders protection

Commander's Interaction	
No interaction necessary at this time.	
Commander's Checklist	
❑ Did the S2— • Assist in preparing the order? • Submit the Intelligence Annex (B) as part of the order? • Finalize the ISR plan and provide an ISR Annex (L) and overlay?	• Assist with the C^2 Warfare Annex (P), OPSEC Annex (Q), Deception Annex (S), and the EW Annex (T)? ❑ Did the S2 integrate the ISR plan with the S3's scheme of maneuver and fires?

TARGETING MEETING

A-10. Each participant should bring the essential information to the targeting meeting. After the targeting meeting, each participant should leave with some critical information. (See Table A-8.)

Table A-8. Targeting meeting

Commander's Interaction	
No interaction necessary at this time.	
Commander's Checklist	
❑ Did the S2 have— • The current situation map? • Situation templates with detailed information on each BOS and capability? • HVTs and recommended HPTs? • Information about the collection assets available? • Intelligence synchronization matrix (ISM) and event template? • Plan for tracking BDA? • Current BDA on hand? • Current PIR and CCIR? ❑ Did the S2 provide the proposed threat activity within the current 24-hour period?	❑ Did the S2 provide the proposed threat activity within the next 24 to 48 hours? ❑ Did the entire staff plan the use of lethal and non-lethal fires to support the operation? **After the Targeting Meeting** ❑ Did the S2— • Have the updated PIR? • Know who will collect what, where, when, and have the taskings for them? • As a result of the targeting meeting provide the intelligence portion to the upcoming FRAGO? • Know his role, the S3 role, and FSO role in the sensor-to-shooter links and controls?

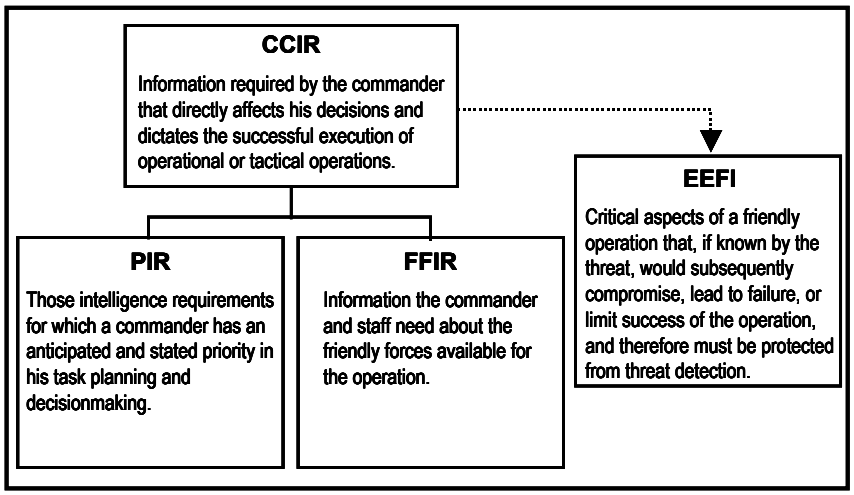
Appendix B

Commander's Critical Information Requirements

B-1. CCIR is information required by the commander that directly affects his decisions and dictates the successful execution of tactical operations. You can get more information than you need or want. Your CCIR will allow you and your staff to focus on the information that is important to your decisions. The CCIR help to focus your staff so they can produce timely and accurate information and a common operational picture (COP). CCIR are—

- Applicable only to you.
- Situation-dependent.
- Events or activities that are predictable.
- Specified by you for each operation.
- Time-sensitive information that must be immediately reported to the commander, staff, and subordinate commanders.
- Always included in paragraph 5 of an OPORD or OPLAN.
- Transmitted by a communications system specified in the standard operating procedures (SOPs).

B-2. Limit CCIR to 10 or fewer items so the staff can focus its efforts better. The CCIR are expressed as two types of requirements: PIR and friendly forces information requirements (FFIR). Although EEFI are not a part of CCIR anymore, they become a commander's priority when he states them. Figure B-1 shows the



elements of CCIR.

Figure B-1. Elements of CCIR.

PRIORITY INTELLIGENCE REQUIREMENTS

B-3. These are intelligence requirements for which you have an anticipated and stated priority for planning and decisionmaking. PIR support your DPs. Without the answer, you accept a greater level of risk during operations. You dictate the format of the answer (for example, a graphic product, verbal report, or image) and you must set an LTIOV.

B-4. Base most of your PIR on a specific fact, event, or activity that the threat has or is known to do (or specific to the environment) but remember to consider how the threat could surprise you (an atypical threat)—potentially one of their greatest advantages. PIR are listed and ranked in order from most to least important. Do not give multiple questions in a single PIR or you will not focus on your real requirement and may not satisfy your requirement. Do not ask questions that have been answered.

B-5. Examples of **Good** PIR:

- Will the threat defend OBJ Bruno using a forward slope defense 121630Z JUL 99 LTIOV? (DP: Fire artillery preparation).
- Will the threat reserve tank battalion reach PL Mike before 121630Z JUL 99 LTIOV? (DP: Commitment of the reserve).
- Will the 43d MRD send its main attack along the AA 121630Z JUL 99 LTIOV? (DP: Commitment of deep strike).
- What size force is defending OBJ Gun LTIOV? (DP: Composition of the main attack).

B-6. Examples of **Bad** PIR:

- When, where, and in what strength will the threat attack?
- What are the fuel levels in the threat's depots?
- What is the current readiness of all threat armor, artillery, and anti-tank units?
- What is the morale of the threat rear echelon units?

B-7. The above PIR are bad because they reflect multiple questions, not focused on the real requirement, and do not satisfy the requirement.

B-8. There are other requirements that entail collection. They are of lower importance than any PIR but are still an important part of the ISR plan. Information requests, indicators, specific information requirements (SIRs), and specific orders and requests (SORs) are closely related to PIR.

INFORMATION REQUIREMENTS

B-9. IR are those items of information regarding the threat and his environment which need to be collected and processed. These requirements are necessary to perform situation development, support to targeting, IPB, and support to force protection but are less critical than PIR.

INDICATORS

B-10. Indictors are threat actions, activities, or signatures whose absence or presence

show evidence of threat intentions, capabilities, and vulnerabilities, and help to confirm or deny a threat COA. The predictions and projections within the situation and event templates are an important factor in performing situation development based on threat activities. A thorough knowledge of when and where activity is likely to occur on the battlefield helps an analyst develop indicators. The indicators in turn help the analyst develop PIR and build SIRs.

SPECIFIC INFORMATION REQUIREMENTS

B-11. A complete SIR describes the information required, the location where the required information can be collected, and the time during which it can be collected. Generally, each PIR or IR generates sets of SIRs. These may partially or fully answer a PIR or IR and provide the analyst the information necessary to confirm or deny threat COAs.

SPECIFIC ORDERS AND REQUESTS

B-12. This is the specific tasking orders approved by the S3 or request for support higher that generates planning and execution of a collection mission or analysis of database information. Specific orders (for example, S3 approved taskings) are orders for subordinate commands; requests (for example, for support) are sent to other commands or higher echelons.

FRIENDLY FORCES INFORMATION REQUIREMENTS

B-13. This is information you and your staff need about the friendly forces available for the operation. This includes personnel, maintenance, supply, ammunition, and petroleum, oils and lubricants (POL) status, and experience and leadership capabilities.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

B-14. The EEFI help protect your operation. They are critical aspects of a friendly operation that, if known by the threat, would subsequently compromise, lead to failure, or limit success of the operation and therefore must be protected from threat detection. EEFI help commanders understand what threat commanders want to know about friendly forces and why. They tell commanders what cannot be compromised. EEFI provide the basis for indirectly assessing the quality of the threat's situational understanding: if the threat does not know an element of EEFI, it degrades his situational understanding.

Appendix C

ISR Integration Within the Synchronization Matrix

C-1. Successful synchronization of ISR collection with operational decisionmaking results in effective, timely intelligence. Failure to synchronize ISR results in the waste of valuable ISR assets against requirements that are not critical to the commander's decisions. This waste results in making a decision with erroneous intelligence or no intelligence at all.

C-2. The intelligence BOS has responsibility for the portion of the synchronization matrix that deals with intelligence collection. The S2 should always contribute to the production of the synchronization matrix. The S2 inputs all information for NAIs or TAIs, to include timeline, task, mission, purpose for collection, and DPs tied to the collection or lack of information collected.

C-3. The synchronization matrix is produced after wargaming, when the commander has established a COA and DPs supported by intelligence. The G2/S2 then determines the LTIOV for each NAI and event, based on those DPs and targeting requirements identified during wargaming.

C-4. The S2 links each PIR to a DP. Each PIR should be linked to only one operational decision. The S2 then develops the ISR plan for the unit, and checks that each PIR will be answered in time to influence operational decisions.

C-5. The S2 selects ISR assets based on the situation, asset capabilities, and availability. The ISM in Figure C-1 depicts how each NAI and TAI will be covered by an ISR system while that NAI or TAI is active.

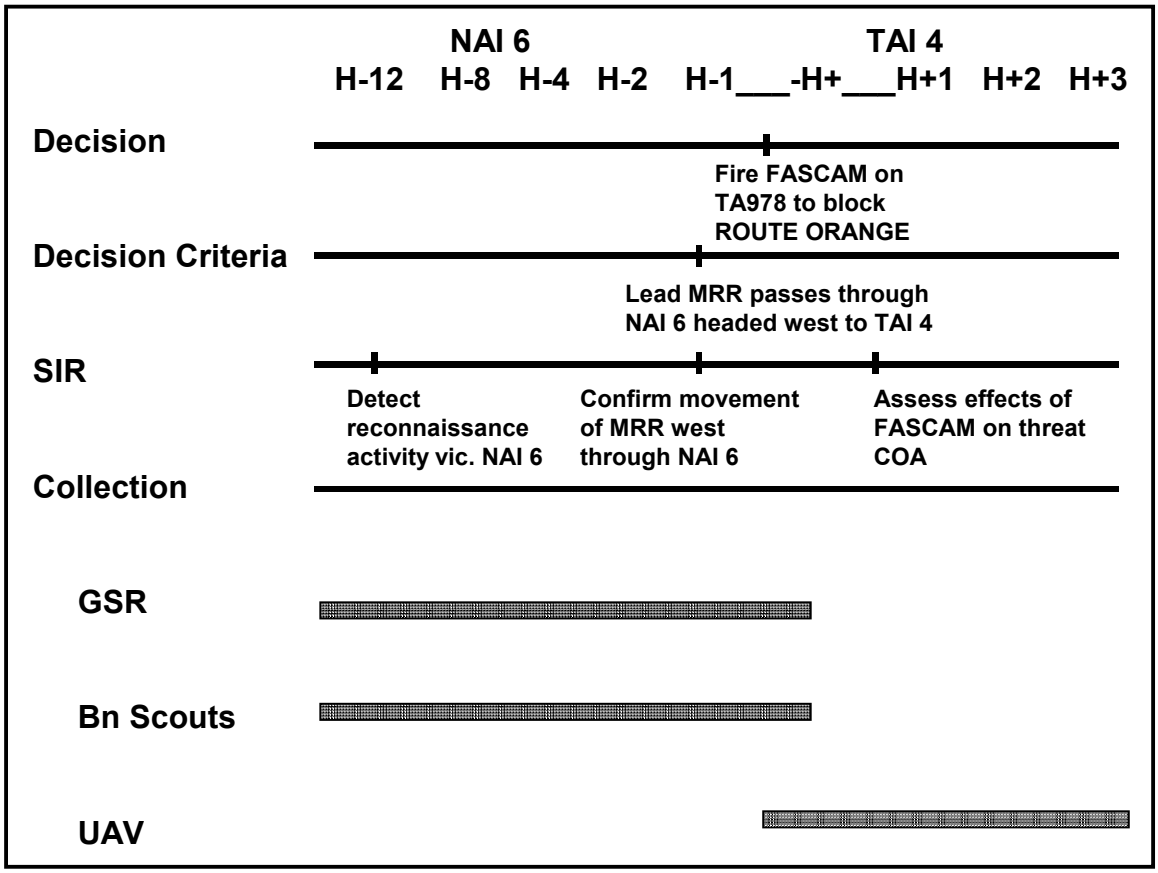


Figure C-1. Sample of intelligence portion of the synchronization matrix

Appendix D

Intelligence, Surveillance, and Reconnaissance Planning

D-1. ISR is essential to gain and maintain contact with the threat. In certain situations gaining contact with the threat can include a combination of technical means and traditional contact as defined in cavalry doctrine. Many battles at the combat training centers prove that successful ISR operations are critical to successful operations.

D-2. During operations you should task your ISR assets to find and report—

- Gaps or vulnerabilities in the threat's operations.
- Defensive preparations to include primary and secondary positions and prepositioned supplies.
- Location of any threat reserves and supporting forces (for example, a supporting artillery or air defense positions).
- Obstacles, threat engagement areas, and potential ambush areas.
- Information that answers threat intentions and capabilities.

D-3. During operations, you must focus your staff on blinding the threat through an aggressive counterreconnaissance. This effort requires an active, predictive intelligence effort. CI analysis of threat multidiscipline ISR operations is integral to counterreconnaissance analysis and operations. Your S2 should use any threat assessment and other CI products, as appropriate, and forward analytical requirements to the CI analytical element at division and above (through standard procedures).

D-4. In the future, CI functionality will include analysis of threat IO and other full-dimensional counter-ISR tasks. CI analysis is especially important during stability operations and support operations, and is one of the primary contributors to the counterreconnaissance effort.

D-5. In order to drive ISR planning ask the following:

- Did the S2 develop threat COAs and event templates based on your initial guidance?
- Did you refine your PIR and the ISR plan (tasks) based on the friendly COA?
- Did the S2 and S3 integrate the ISR plan with the scheme of maneuver? Are the NAIs and TAIs the focus of the ISR plan and do they support the DST for the friendly COA? At brigade level, does the ISR synchronization matrix answer your PIR and targeting requirements?
- Are all organic and supporting collection assets considered in the ISR plan? Was the ISR plan developed in relation to the overall ISR architecture? Have

sufficient resources been dedicated to the ISR plan?

- Does the IPB identify the risks during infiltration of ISR assets? Are ISR assets teamed to improve their chances of success and minimize the changes of casualties? Are adequate fires planned to support ISR operations?

- Did the S4 and/or headquarters and headquarters company (HHC) commander plan casualty evacuation and allocate resources to support the reconstitution of ISR assets? Did the signals officer plan adequate communications support for ISR operations?

- Did the staff use a five-paragraph FRAGO based on an ISR tasking matrix to capture all of the integrated staff planning?

- Did the staff develop the counterreconnaissance plan and is its emphasis on identifying threat reconnaissance COAs?

- Did you assign the right assets required to execute your ISR?

- Did you assign the right assets required to execute your counterreconnaissance effort?

D-6. Make the S2 and S3 brief you and the staff on how they will track ISR execution? Train your staff to track the battle, using the DST and the synchronization matrix. The S2 and S3 must use the ISR plan and ISR synchronization matrix (at brigade) to track and retask assets in order to answer your PIR.

D-7. In order to track and retask ISR operations, ask the following:

- Is the S2 using the event and situation templates to analyze the information and perform predictive analysis?

- Are the S2 and S3 tracking the status of ISR assets in a timely manner and cross-cueing ISR assets and teaming them to minimize the chances of casualties?

- Is ISR reporting confirming the initial assumptions about the threat COAs (or the environment)? If not, is the staff using a “mini-wargame” to reevaluate initial assumptions, reinitiate an abbreviated IPB and MDMP, and quickly change the operation?

Appendix E
Foreign Language Support

INTRODUCTION

E-1. You need linguists for full spectrum operations especially when the focus is on stability operations and support operations. You need a good linguist support plan to select qualified linguists for each requirement. The growing focus on multinational operations increases the competition for limited linguist resources vital for mission success. Consider the lowest possible foreign language qualification needed for each mission, taking into account the limitations of the Defense Language Proficiency Test (DLPT) for Army linguists.

LINGUISTIC SUPPORT CATEGORIES

E-2. Foreign language support to US Armed Forces engaged in stability operations and support operations falls into one of four categories:

- **INTELLIGENCE AND INFORMATION COLLECTION.** TRADITIONAL SIGINT AND HUMINT DISCIPLINES, AS WELL AS FOREIGN LANGUAGE SUPPORT TO FORCE PROTECTION AND EXPLOITATION OF OPEN-SOURCE INFORMATION.
- **CIVIL/MILITARY OPERATIONS**. MILITARY INTERACTION WITH THE CIVILIAN POPULATION FOR GOVERNMENT LIAISON, LEGAL AGREEMENTS, MEDICAL SUPPORT AND OPERATIONS, LAW ENFORCEMENT, ENGINEERING PROJECTS, PUBLIC SAFETY, SECURITY AND POPULATION CONTROL, CA, AND PSYOP.
- **LOGISTICS.** SUSTAINMENT OR TRANSPORTATION FUNCTIONS. FOR LOGISTICAL CONTRACTING, PORT, RAILHEAD, AIRHEAD, OR TRANS-SHIPMENT OPERATIONS AND CONVOY OPERATIONS**.**
- **MULTINATIONAL MILITARY OPERATIONS AND LIAISON.** COORDINATION WITH ALLIED PARTNERS, COALITION PARTNERS, AND PREVIOUSLY UNAFFILIATED NATIONS.

DETERMINING LINGUIST REQUIREMENTS

E-3. The staff uses METT-TC, organization or echelon of command, and the environment to—

- Determine the number of linguists for a particular mission.
- Allocate linguists by one linguist team per echelon of command, one linguist per piece of equipment, or one linguist team per location where the function is to be performed.

- Conduct mission analysis and identify specified or implied tasks requiring foreign language support.

E-4. Task organization and scheme of maneuver are then applied to determine the number of linguists needed for an operation. The staff must analyze each operation to determine the language requirements. While interpretation for a peace negotiation requires not only outstanding linguistic capability but also cultural acumen, the translation of routine documents with the aid of a dictionary requires a much different skill set. Poor identification of language requirements can tie up the best linguists in a less effective role, creating linguist shortfalls in other areas.

E-5. The relative importance of each of the four linguist support categories is mission dependent. For example, during a noncombatant evacuation operation (NEO) civil or military coordination would probably not be as critical as collecting intelligence and information. The situation is reversed for a humanitarian assistance mission in which civil or military operations have a significant impact on mission success. Identifying these dynamics helps the commander and staff prioritize linguist requirements.

E-6. Determining stability operation and support operation linguist requirements can be difficult because each operation is unique. Commanders and staff with a basic knowledge of organic Army linguistic assets, foreign language resource alternatives, and MI skills can successfully utilize linguists in support of their military operations.

PLANNING AND MANAGING LINGUIST SUPPORT

E-7. Commanders who conduct stability operations and support operations must include linguist requirements as part of their MDMP. Decide what foreign languages are needed, what types of foreign language requirements are needed for each assignment, and what would be the best source of linguist assets. If the mission includes intelligence and information collection, you must decide on which MI collection skill is needed.

E-8. You should consider linguist requirements for every contingency plan and OPLAN assigned to your command. Linguist requirements should be considered in at least the first nine steps of mission analysis (see FM 5-0 and FM 6-0 (FM 101-5)). Additionally, you must decide on security clearance requirements early in the mission; also, it is helpful to initiate linguist researching and command relationships before actual operations.

PRIMARY STAFF RESPONSIBILITIES

E-9. Primary staff at each echelon has responsibilities for evaluating requirements and managing linguist support. The responsibilities include but are not limited to the following:

- Assistant Chief of Staff, G1 (S1), Personnel will—
  - — Identify linguist requirements needed to support G1/S1functions in all contingency areas.
  - — Manage linguist staffing and linguist replacement management.
  - — Identify foreign language skill identifiers for all assigned, attached, or OPCON Army linguists.

- Identify all Army foreign language skilled soldiers not identified in the Standard Installation Division Personnel Section (SIDPERS).
- Ensure language skills are added to SIDPERS.
- Deploy and provide administrative support of Department of the Army and Department of Defense civilian linguists.
- Hire, contract for, and provide administrative support of local national linguists.
- Procure Army foreign language support personnel for screening local labor resources.

- Assistant Chief of Staff, G2 (S2), Intelligence will—
  - Identify linguist requirements needed to support G2/S2 functions in all contingency areas.
  - Determine, during the initial IPB, all foreign languages (spoken and written) and dialects needed for mission accomplishment.
  - Collect, process, produce, and disseminate information derived from linguist sources.
  - Provide intelligence training for MI linguists employed in the AO.
  - Coordinate for security investigations, as necessary, for local hire linguists.
  - Provide support to CI screening of contracted linguists and the local national labor force.

- Assistant Chief of Staff, G3 (S3), Operations will—
  - Identify linguist requirements needed to support G3/S3 functions in all contingency areas.
  - Consolidate unit linguistic requirements and establish priorities.
  - Develop linguist deployment and employment plans.
  - Develop plans to train linguists and to use linguists for training the force in AO foreign language survival skills.
  - Assign, attach, and detach linguists and linguist teams.
  - Integrate additional or replacement linguists through operational channels.
  - Recommend modernization and development of linguist systems and methods.
  - Coordinate mobilization and demobilization of RC linguist support.
  - Plan linguist usage for deception operations.
  - Plan linguist support to movement of enemy prisoner of war (EPW), detainees, and refugees.
  - Coordinate evaluation of linguist support by all staff elements.

- Assistant Chief of Staff G4 (S4), Logistics will—
  - Identify linguist requirements needed to support G4/S4 functions in all contingency areas.
  - Provide logistical, supply, maintenance, and transportation support to attached linguists.

- Assistant Chief of Staff G5 (S5), Civil-Military Operations will—
  - Assist the G1 in the contracting of local hire linguists.
  - Identify foreign language requirements for NEO and other civil and military operations.

- Assistant Chief of Staff G6 (S6), Signal will—
  - Manage radio frequencies assignments to supporting SIGINT linguist elements.
  - Support linguist operations with internal document reproduction, distribution, and message services.
  - Integrate automation management systems of linguist units.

E-10. In addition, each staff section has to determine the linguist support required to meet its operational missions. Staff requirements for linguist support include but are not limited to the following:

- Assistant Chief of Staff, G1 (S1), Personnel will—
  - Coordinate with local authorities on matters of civilian hire, finance, and recordkeeping.
  - Contract local hire personnel.
  - Coordinate local morale support and community activities.
  - Coordinate with local authorities for postal operations.
  - Support administration, counseling, personal affairs, and leave for local national and third-country national personnel.
  - Coordinate local medical support.
  - Liaison with coalition counterparts.

- Assistant Chief of Staff, G2 (S2), Intelligence will—
  - Evaluate and use local maps and terrain products in operations.
  - Process, for MI purposes, material taken from EPWs or civilian internees.
  - At lower echelons, conduct tactical questioning of refugees, detainees, and EPWs.
  - Assess local open-source information for intelligence value.
  - Ensure intelligence coordination and liaison with coalition and HN counterparts.

- Assistant Chief of Staff, G3 (S3), Operations will—
  - Ensure operational coordination and liaison with coalition and HN counterparts.
  - Translate OPORDs and OPLANs for use by coalition counterparts.

- Assistant Chief of Staff G4 (S4), Logistics will—
  - Procure local supply, maintenance, transportation, and services.
  - Coordinate logistics at air and seaports of debarkation.
  - Provide logistic support to local population.
  - Coordinate foreign language support to help contract for water, food service, bath and laundry if necessary.
  - Contract with local governments, agencies, and individuals for sites and storage.

- Assistant Chief of Staff G5 (S5), Civil-Military Operations will—
  - Assist the G1 in the contracting of local hire personnel.
  - Determine civilian impact on military operations.
  - Minimize civilian interference with combat operations.
  - Inform civilians of curfews, movement restrictions, and relocations.
  - Provide assistance to liaison with HN and multinational agencies, dignitaries, and authorities.
  - Promote positive community programs to win over support.
  - Determine if combined operations PSYOP efforts are mutually planned and synchronized.
  - Support interpretation to assist resolution of civilian claims against the US government.
  - Solicit linguistic and cultural knowledge support to protect culturally significant sites.
  - Use linguistic and cultural support to identify cultural and religious customs.

- Assistant Chief of Staff G6 (S6), Signal will—
  - Coordinate suitable commercial information systems and services.
  - Coordinate with multinational forces on command frequency lists.
  - Coordinate signal support interfaces with HN and multinational forces.

USE OF CONTRACT COMPANIES TO HANDLE LINGUISTS AND LINGUIST SUPPORT

E-11. Contract linguists can be used to backfill shortfalls in military linguist resources. Contracting is usually managed at or above the brigade level, and funding is requested through channels.

E-12. Contract linguists are supervised by the gaining military organizations. The G3 (S3) usually has responsibility. The contract linguists are controlled by the vendor who resolves performance and discipline issues.

SPECIAL STAFF OFFICERS RESPONSIBILITIES

E-13. If no special staff officer is assigned the duties below, the corresponding coordinating staff officer should assume those responsibilities. Linguist requirements for special staff officers include but are not limited to the following:

- Liaison Officer:
  - Should speak the required foreign language; if not, a translator or interpreter is necessary for all aspects of his duties.
  - Request interpreters to assist when representing the commander in combined or multinational operations.
  - Translate orders, maps, traces, overlays, and documents into coalition foreign languages.
- Civilian Personnel Officer:
  - Recruit, interview for suitability, and hire civilian local labor force if required.
  - Host country negotiations on labor agreements.
- Dental Surgeon:
  - Administer dental care to support humanitarian mission requirements.
  - Rehabilitate, construct, and gain usage of existing dental facilities as required.
- Finance Officer:
  - Coordinate exchange of US funds into needed local currencies.
  - Provide non-US and US pay functions to foreign national, HN, and civilian internees, and EPWs.
- Surgeon:
  - Support medical humanitarian assistance and disaster relief operations.
  - Provide medical care of EPWs and civilians within the command's AO.
  - Coordinate medical laboratory access in AO.
  - Determine the nature of local health threats to the force through populace interviews.
  - Determine the identity of local or captured medical supplies.

- Veterinary Officer:
  - Determine source and suitability of local foods.
  - Assist the local population with veterinary service needs.

- Chemical Officer:
  - Identify threat force chemical weapons and equipment.
  - Communicate NBC risks to supported populations.

- Engineer Coordinator:
  - Procure proper local materials to support engineering mission.
  - Communicate engineering project requirements to contracted local work force.
  - Communicate engineering project impact on local landowners and other affected parties. Determine, in coordination with G2 (S2), suitability of local topographic maps and terrain products.
  - Assess environmental concerns of HN and local populations in combined operations.

- Provost Marshal:
  - Support dislocated and civilian straggler control activities.
  - Support internment and resettlement operations.
  - Communicate weapons bounty programs and payments to the local population.
  - Support counter-drug and customs activities.
  - Help foreign civil authorities maintain control when authorized.
  - Conduct liaison with local law enforcement authorities.

- PSYOP Officer:
  - Produce approved PSYOP propaganda and counter-propaganda media.
  - Evaluate PSYOP impact on target audience.

- Safety Officer:
  - Provide safety training to local labor force.
  - Communicate warnings of dangerous military operations and other hazards to local populace.

- Transportation Officer:
  - Coordinate commercial and local transportation needs.
  - Coordinate movement scheduling and routes with multinational forces and HN.

PERSONAL STAFF OFFICER RESPONSIBILITIES

E-14. Personal staff officers are under the immediate control of and have direct access to the commander. Most personal staff officers also perform special staff officer duties, working with a coordinating staff officer. These assignments are on a case-by-case basis, depending on the commander's guidance and the nature of the mission, and are very common in stability operations and support operations. Linguist requirements for special staff officers include but are not limited to the following:

- Chaplain:
  - Provide moral and spiritual leadership to the populace.
  - Coordinate religious support with coalition and multinational partners.

— Determine the impact of indigenous religious group faith and practices on military operations.
— Provide religious support to the community to include hospital patients, EPWs, refugees, and civilian detainees.
— Conduct liaison with indigenous religious leaders in close coordination with the G5.

- Public Affairs Office (PAO):

— Act as commander's spokesman for all communication with external media.
— Assess the accuracy of foreign media interpretation of PAO releases.

— Assess and recommend news, entertainment, and other information (assisting G5) for contracted services foreign nationals.

- Staff Judge Advocate:

— Translate foreign legal codes, Status of Forces Agreements (SOFAs), and international laws.
— Determine local environmental laws and treaties through translation services.
— Assess the treatment of EPW and civilian internees.
— Translate documents to support G4 in local contracts.

IDENTIFYING SOURCES OF LINGUISTS

E-15. Sources of linguist support include AC, non-MI Army linguists, RC, other Service linguists, US government civilian employees, US contract linguists, allied and coalition linguists, and local national contract linguists. It is vital to know the advantages and disadvantages of each type of linguist and to carefully match the available linguists to the operation.

ACTIVE COMPONENT

E-16. AC MI language dependent MOSs include MOS 97E (HUMINT Collector), 98G (Voice Intercept Operator), and their related warrant officer fields. Some soldiers in MOS 96B (All-Source Intelligence Analyst), MOS 97B (CI Agent), and MOS 98C (SIGINT Analyst) and their related warrant officer fields are trained in foreign languages.

E-17. There are many advantages to utilizing soldiers in the MOSs mentioned above. They are already trained in the military system, are not subject to deployment restrictions (a limiting factor with civilian linguists), have a security clearance and, as US personnel, support the command's interests.

E-18. The major disadvantage to using these individuals for general foreign language support is that in doing so, they are removed from their primary MI functions. They should be used only in linguistic duties that include intelligence potential. For example, an interrogator (97E) provides linguist support to a CA team as a method to provide access to the local population to determine their attitudes toward US Forces.

NON-MI ARMY LINGUISTS

E-19. Non-MI Army linguists include some enlisted and warrant officers in Career Management Field (CMF) 18 (Special Forces), CMF 37 (PSYOP), CMF 180A (Special Forces), and commissioned officers with a branch code 18 (Special

Forces) and functional areas 39 (PSYOP and CA) and 48 (Foreign Area Officer). Since the standards vary by field, pay attention to the recorded language proficiency and test date of these individuals.

E-20. The Army also includes numerous soldiers who have proficiency in a foreign language but whose jobs do not require foreign language proficiency. They may have trained in a foreign language or may have acquired proficiency through their heritage. They have the advantage of being trained soldiers and are therefore readily deployable to all areas of the battlefield.

These soldiers may have the specific vocabulary and military skill knowledge for certain linguist support missions. For example, a supply sergeant who speaks the local language would be an invaluable asset to the G4.

E-21. The disadvantages are that they already have another job and units are reluctant to give up personnel, especially those in key positions, and their capabilities are difficult to assess. Since they are not required to take the DLPT, it is often difficult for the G1 (S1) to identify them as a linguist, or for a non-linguist to judge the level of their foreign language capability.

RESERVE COMPONENT

E-22. RC trained MI linguists include the MOSs listed above in the AC. RC MI linguists have the same set of advantages and disadvantages as listed above for AC MI linguists.

E-23. The RC also includes MI linguists in MOS 97L (Translator/Interpreter). The 97L's are specifically trained to be a translator and interpreter and have the advantages listed above. An added advantage is that, since their sole job is translation and interpretation, they do not have to be removed from another job in order to be used as linguists. The major disadvantage is that they might not have additional skills that give them dual functionality.

OTHER SERVICE LINGUISTS

E-24. Other service linguists have the advantage of deployability, loyalty, and clearance, but must often learn the Army system and specific Army vocabulary. They are also difficult to obtain, as their parent service is probably also short of trained linguists. Other Service linguists, however, will be valuable in joint operation centers and joint activities. When serving the JTF headquarters, Army commanders and staffs must be aware of the linguists in the other services in order to plan for their participation and optimize their employment.

US GOVERNMENT CIVILIAN EMPLOYEES

E-25. Civilians who have knowledge of a foreign language and are already employees of the US government in some capacity have the advantage of being in the system. They are difficult to obtain as they are already filling required positions and are usually not available for translator/interpreter use. They also are not as readily deployable as service members.

Civilians may have the advantage of extensive knowledge of the AO and extensive foreign language capability.

US CONTRACT LINGUISTS

E-26. US civilians can be contracted to provide linguist support. They have an advantage over local national hires in that their loyalty to the US is more readily evaluated and they can be more readily granted the necessary security clearance.

There may be severe limitations on their deployment and use and they must be carefully screened for foreign language ability. In many cases their use of the foreign language may be old fashioned or full of US idioms depending on their length of time in the US. If recent émigrés, their use in the country of their origin could be dangerous to them, or their loyalty may reside with the country of origin at odds with US interests.

ALLIED AND COALITION LINGUISTS

E-27. Allied and coalition linguists may be unfamiliar with the US system, and their loyalty is difficult to ascertain. MI linguists who speak the partner's language can be useful in determining reliability and loyalty of allied or coalition linguists.

LOCAL NATIONAL CONTRACT LINGUISTS

E-28. Local national hires will provide the bulk of your linguist support. They are usually cheaper to hire than US civilians and will know the local dialect and idioms. They can be selected for their expertise in particular areas or subject matter. A potential problem with local national hires is their ability to speak English, necessitating a screening interview or test to determine their ability to communicate in English.

E-29. For security reasons, CI personnel must carefully select and screen local nationals initially and periodically throughout their employment. Their loyalty can never be assumed. They may be affected by local prejudices and can be assumed to place their own interests above those of the US.

Appendix F

Stability Operations, Support Operations, and Intelligence Preparation Of The Battlefield

F-1. IPB analyzes the possibilities and limitations imposed by the AO and the threat's capabilities. It depicts the threat's possible COAs, and the probabilities of each COA occurring.

F-2. To make the IPB process relevant to stability operations and support operations, the S2 must go back to the basics: discern the intent of each step of the IPB process and interpret some doctrinal terms loosely. In this way your S2 can prevent trying to force a threat into a mold, which makes threat COAs and activities easier to express with familiar IPB products.

F-3. "Threat" describes the various challenges US forces can expect in stability operations and support operations. "Enemy" is too narrow a term for some of the challenges stability operations and support operations will encounter. Refugees, nongovernmental organizations, disaster victims, disease and environmental dangers, and many other challenges encountered during the types of operations brigades face today do not fit the definition of enemy, but they do pose a challenge to successfully accomplishing your mission.

F-4. To avoid overlooking serious challenges to mission success, we offer this definition of "threat" paraphrased from the Australian Army's definition: "**Threat** is any actor, agent, or environmental factor which endangers the commander's ability to accomplish his mission."

IPB MODIFICATIONS FOR STABILITY OPERATIONS AND SUPPORT OPERATIONS

STEP 1: DEFINE THE BATTLEFIELD ENVIRONMENT

F-5. Stability operations and support operations battlefield environments are not contiguous. For example, upon examining the AO assigned by a higher headquarters to an infantry battalion conducting a counterinsurgency operation, the S2 may be concerned about materiel and moral support for the insurgents coming from a refugee community. Although that community and its assets may have no direct ground connection to the battalion AO, activities in this physically separate region may impact insurgent activities and capabilities inside the battalion's AO. In this instance, you might recommend to the commander an AOI that does not include large areas between the AOI and the AO.

F-6. Stability operations and support operations IPB products need a greater level of detail. An excellent example is demographic analysis. In this stage of the IPB process, the S2 and analysts have to make an initial evaluation of what factors make a given population segment important to your mission and how to communicate this to you and your staffs.

F-7. Examine existing databases and collect intelligence needed to continue the IPB process. The significant difference is that many of those databases will be from open sources and cannot be tapped through normal intelligence channels. Often answers to basic questions of culture, history, and the perceptions they produce can be found by doing a little research using the nearest library or quality book store, in academic journals, and by going online and performing searches by topic, region, and country.

F-8. The intelligence community faces a challenge to produce timely, relevant, and updated reports on regions and issues of sporadic military interest. The academic community, travel industry, and international commercial activities study international regions daily. Their reports and assessments of local sentiments, current cultural taboos, and receptiveness to strangers, for example, are widely published and updated frequently. Rather than await an eventual response to an RFI on these basic intelligence issues, these nontraditional sources give you the information now.

STEP 2: DESCRIBE THE BATTLEFIELD'S EFFECTS

F-9. Revise your thinking for a new battlefield. As with the term "enemy," stability operations and support operations are often not conducted on anything resembling a battlefield. The environment may be lethal, and is usually challenging, but often does not look like a battlefield. Determine how the environment impacts everyone relevant to your operation. In recent years, we have relearned lessons of how civilians on the battlefield can add to the friction of battle and some attempts have been made to account for them. Primarily, these efforts take the form of plans to get refugees and others out of the way of the fighting, both to remove them from possible harm and to reduce the impact on our operations.

F-10. In a stability and support environment, the number and importance of population groups that could have important effects on the commander's mission expands. Classifying them all as civilians on the battlefield is not adequate. Even attempting to classify them as friendly, hostile, or neutral is only a start. For example, neutral refugees seeking relief supplies could spell disaster for an NEO if they flood helicopter LZs. With no hostile intent, they could make air extraction impossible as they head to the sound of rotors—a sound often associated with delivery of relief supplies. Clans or factions that express pro-US sentiments could violently attack relief workers if they assist their clan's perceived enemies. US forces could then become drawn into a larger, standing conflict as they attempt to defend the relief workers.

F-11. In this environment, your staff must do more than list and categorize groups. They must assess the goals and motivations of the groups, their leadership (or lack thereof), their beliefs, and their power bases. From all of these possibly important factors for further analysis, S2s must narrow the list to those with a direct effect on the commander's mission and his ability to accomplish it. The limited time, soldiers, and equipment available to S2s require focusing on the most important issues for detailed analysis.

STEP 3: EVALUATE THE THREAT

F-12. Evaluating the threat was once the easiest part of the IPB process; today, this step is more difficult. The threats are often not regular armies with well-defined doctrine and OB. Even during Operation DESERT STORM, against a threat the intelligence community thought it understood well, the threat did not fight as their doctrine said they would. In the final analysis, threats do the same thing US forces do—they use the means at their disposal to achieve their desired endstate. Cultural factors and economic and training restraints impact operations. Commander personalities also play an important

role. In the end, however, forces apply assets available to achieve what they want to accomplish and your S2 must take all of this into account. Conducting this step of IPB relies on the assessment of the threat's objective, and subsequent threat tactics are based on details of the specific operational environment in consideration.

F-13. Brigades and battalions depend on tactics descriptions, representative vignettes of threat activities, and modified templates packaged as threat models from higher headquarters. By applying basic operational principles to these skeletal products, S2s can modify threat models and assess preferred methods of operation for a given threat peculiar to your operation. By refining all of these, the staff produces a threat picture, which then can be turned into doctrinal templates and sketches. The important difference between these end products and what S2s received in the past is the amount of increased analysis required to turn the information into something useful for your planning and decisionmaking.

STEP 4: DETERMINE THREAT COAs

F-14. The S2 will begin by defining the likely threat objectives and developing threat COAs, bearing in mind that all threat COAs must be considered. The S2 will use the same procedures and tools he uses in conventional IPB (situaton templates, event templates, and event matrixes) to support his threat COA analysis.

F-15. The situation templates will graphically depict the threat's expected disposition should the threat adopt a particular COA. To construct a situation template, the S2 overlays the doctrinal template produced in step 3 on the environmental templates (to include the MCOO) developed in step 2. The threat is then adjusted on the doctrinal template to allow for the effects of the environment. Due to the potential complexity of a stability and support environment, some situation templates may be more suited to present in a matrix format.

F-16. The S2 will use event templates as guides for intelligence collection and ISR planning. These templates will depict where and when to collect the threat information. Some of the NAIs on the event template indicate the COA the threat will adopt. Consider the following when determining threat COAs relative to stability operations and support operations:

- A wider range of actions available to the threat.
- Historical, demographic, and cultural information is of importance in developing possible actions.
- The full set of unique COAs available to the threat.
- Objectives and COAs over a longer period of time.
- The threat will quickly incorporate lessons learned.
- Long-term political objectives; what the threat is willing to commit to at various stages.
- Imagery at a scale of 1:10,000 to 1:25,000 to accurately display detailed characteristics of the terrain.

URBAN OPERATIONS CONSIDERATIONS

F-17. Urban operations are a perfect example of a unique environment. Intelligence collection within the urban operations can be a complex and time-consuming process. Normally, your S2 must quickly focus on the key elements of the environment. The use of an abbreviated analytical process has the advantage of bringing environmental details into the IPB process. It also lays the groundwork for a more detailed analysis later as your operation matures.

F-18. Urban operations have an increased number and potential combination of variables. For example, an infantry battalion operating in a city's industrial park may not only encounter the threat during seasonal rains but also encounter flooding as well. Flooded buildings may in turn be full of damaged storage tanks that leak hazardous waste materials into the water. The battalion could suffer more casualties from the hazardous waste than from direct combat. In the confines of the urban environment there may be literally nowhere for the unit to go, and the situation will have to be addressed by a combination of combat, engineer, and chemical units.

F-19. Because of the diversity in the urban environment, your S2 may have difficulty identifying a starting point. The framework in Figure F-1 is a way for your S2 to start. It is a tool designed to facilitate an urban operation assessment and subsequently support your MDMP. The framework is structured around eleven steps, which may also be considered layers of the whole assessment. Your staff must address the first layer before reaching the second layer, and the third layer, and so on.

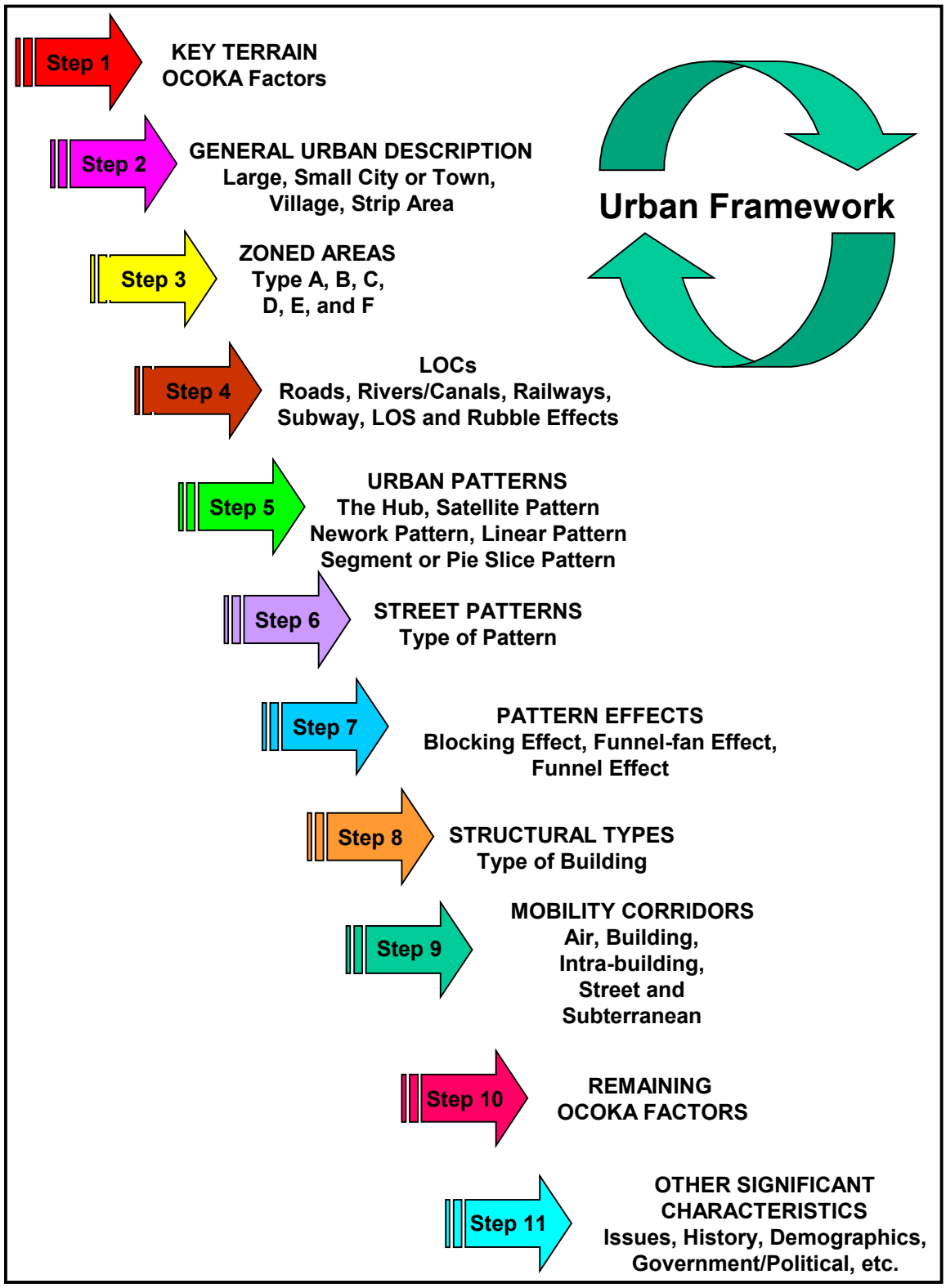


Figure F-1. Urban Operations

GLOSSARY

A

AC	Active Component
ACE	analysis and control element
ACR	armored cavalry regiment
ACT	analysis and control team
ADA	air defense artillery
ADRG	Arc Digitized Roster Graphics
AEB	aerial exploitation battalion
AG	advance guard
AGMB	advance guard main body
AO	area of operation
AOI	area of interest
ARFOR	Army force
ARL-M	airborne reconnaissance low-multifunction
ASARS	Advanced Synthetic Aperture Radar System
AT	anti-tank
ATGM	anti-tank guided missile
ATK	attack
attrit	attrition

B

BCT	brigade combat team
BDA	battle damage assessment
BLUFOR	Blue forces
BMP	infantry fighting vehicle (Soviet origin)
BN	battalion
BOS	battlefield operating system
BP	battle position
BRDM	infantry fighting vehicle (Soviet origin)
BTRY	battery

C

C^2	command and control
C^3	command, control, and communications
CA	Civil Affairs
CATK	counterattack
CCIR	commander's critical information requirements
CFSO	counterintelligence force protection source operations
CGS	common ground station
C-HUMINT	counter-human intelligence
CI	counterintelligence
CMF	career management field
co	company
CofS	Chief of Staff
COMINT	communications intelligence
COP	common operational picture
CO/TM	company/team
COA	course of action

CRP	combat reconnaissance patrol
CS	combat support
CSS	combat service support
CWT	combat weather team

D

DA	Department of the Army
DF	direction finding
DLPT	Defense Language Proficiency Test
DOCEX	document exploitation
DOD	Department of Defense
DP	decision point
DRT	dismounted reconnaissance team
DS	direct support
dsmt	dismount
DST	decision support template
DTED	digital terrain elevation data
DZ	drop zone

E

EA	electronic attack
EEFI	essential elements of friendly information
EENT	end of evening nautical twilight
ENY	enemy
E-O	electro-optical
EP	electronic protection
EPW	enemy prisoner of war
ES	electronic warfare support
ELINT	electronic intellligence
EW	electronic warfare
EWO	electronic warfare officer
EWTL	electronic warfare target list

F

FA	field artillery
FASCAM	family of artillery scatterable mines
FSCOORD	fire support coordinator
FD	forward detachment
FFIR	friendly forces information requirments
FIS	foreign intelligence services
FISINT	foreign instrumentation signals intelligence
FLOT	forward line of own troops
FRAGO	fragmentary order
FSE	fire support element
FSO	fire support officer
FWD	forward

G

GD	advance guard
GRCS	GUARDRAIL common sensor

GS	general support
GSR	ground surveillance radar

H

H	hour
HN	host nation
HPT	high payoff target
HPTL	high payoff target list
HQ	headquarters
HUMINT	human intelligence
HVT	high value target
HVTL	high value target list

I

IBCT	initial brigade combat team
I&W	indications and warnings
IEW	intelligence and electronic warfare
IMINT	imagery intelligence
inf	infantry
IO	information operations
IPB	intelligence preparation of the battlefield
IR	information requirements
ISM	intelligence synchronization matrix
ISR	intelligence, surveillance, and reconnaissance

J

Joint STARS	Joint Surveillance Target Attack Radar System
JTF	joint task force

K

km	kilometer

L

LOC	lines of communication
LRS	long-range surveillance
LTIOV	latest time information is of value
LZ	landing zone

M

MASINT	measurements and signature intelligence
MCOO	modified combined obstacle overlay
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops, time available and civilians
MFR	memorandum for record
MI	military intelligence
MOD	mobile obstacle detachment
MOS	Military Occupational Specialty

MRB	motorized rifle battalion
MRD	motorized rifle detachment
MRR	motorized rifle regiment
MSR	main supply route

N

N	north
NAI	named area of interest
NBC	nuclear, biological, and chemical
NE	northeast
NEO	noncombatant evacuation operation
NP	nonpresistant (chemicals)
NRT	near-real time

O

OB	order of battle
OBJ	objective
OCOKA	observation and fields of fire, concealment and cover, obstacles, key terrain, avenue of approach
OMT	operational management team
O/O	on order
OPCON	operational control
OPLAN	operations plan
OPORD	operations order
OPS	operations
OPSEC	operations security

P

PAO	public affairs office
PCHEM	presistant chemical
PIR	priority intelligence requirements
PL	phase line
POL	petroleum, oils, and lubricants
PSN	position
PSYOP	psychological operations
pt	point
PZ	pickup zone

R

RC	Reserve Components
R&S	reconnaissance and surveillance
recon	reconnaissance
REGT	regiment
REMBRASS	Remotely Monitored Battlefield Sensor System
RFI	request for information
RKH	chemical
RSTA	reconnaissance, surveillance, and target acquisition

S

S	south
S&TI	scientific and technical intelligence
SBF	support by fire
SIDPERS	Standard Installation Division Personnel System
SIGINT	signals intelligence
SIR	specific information requirement
SOFA	Status of Forces Agreement
SOR	specific orders and requests
SPT	support
SSO	special security officer
STANAG	standardization agreement (NATO)
STM	standard tactical mission
SWO	staff weather officer

T

TAC	tactical command post
TAI	target area of interest
TDAM	tank division
TEB	tactical exploitation battalion
TECHINT	technical intelligence
TENCAP	Tactical Exploitation of National Capabilities
TF	task force
TGT	target
tm	team
TOC	tactical operations center
TROJAN Spirit	Special Purpose Intelligence Remote Integrated Terminal
TTP	tactics, techniques, and procedures

U

UAV	unmanned aerial vehicle
UTP	urban tactical planner
U2R	Advance Synthetic Aperture Radar

V

vic	vicinity

W

W	west
WARNO	warning order
WMD	weapon of mass destruction
wpns	weapons

X

XO	executive officer

REFERENCES

FM 2-0 (FM 34-1)	Intelligence and Electronic Warfare Operations, 27 Sep 94
FM 2-01.3 (FM 34-130)	Intelligence Preparation of the Battlefield, 8 Jul 94
FM 3-0/FM 6-0 (FM l00-5)	Operations
FM 34-5(S)	Human Intelligence and Related Counterintelligence Operations, 29 Jul 94
FM 2-22.3 (FM 34-52)	Intelligence Interrogation, 28 Sep 92
FM 2-50.1 (FM 34-25-1)	Joint Surveillance Target Attack Radar System, 3 Oct 95
FM 3-55.1 (FM 34-25-2)	
FM 2-00.10 (FM 34-10-1)	Tactics, Techniques, and Procedures for the Remotely Monitored Battlefield Sensor System (REMBASS), 18 Jun 91
FM 2-01.2 (FM 34-60)	Counterintelligence, 3 Oct 95
FM 3-34.330 (FM 5-33)	Terrain Analysis, 11 Jul 90

D 101.2:SE 2/5

The Most Secret War

Army Signals Intelligence in Vietnam

UNIV. OF FL LIB.
DOCUMENTS DEPT.
JUL 21 2003
U.S. DEPOSITORY

"... field commanders in Vietnam, continue to say that this [signals intelligence] is the backbone of their intelligence effort. They can't live or fight without it. I want to stress to everyone in this room just how important this effort is ... I can't think of anything more important because they are just blind over there without this effort ..."

GEN Bruce Palmer, Vice Chief of Staff, US Army

FLARE

The Most Secret War

UNIV. OF FLORIDA LIBS.
DOCUMENTS
DEPARTMENT
U.S. DEPOSITORY

The Most Secret War

Army Signals Intelligence in Vietnam

James L. Gilbert

Military History Office
US Army Intelligence and Security Command
Fort Belvoir, Virginia

In a ceremony held in May 1969 at Arlington Hall Station, Virginia, the noncommissioned officers of the US Army Security Agency dedicated a memorial in memory of their fallen comrades from three conflicts: Korea, Vietnam, and Dominican Republic. The statue is carved from white Italian marble and depicts a soldier in full battle dress with field radio. Today, the ASA Memorial stands at Headquarters, US Army Intelligence and Security Command, Fort Belvoir, Virginia.

TO THOSE WHO SERVED...

SG DONALD D. DAUGHERTY 13 APR

CPT JAMES D STALLINGS 25 SEP

LT JOHN F. COCHRANE 24 OCT 19

SFC JOHN F. STIRLING 8 MAR 19

SFC ROBERT D. TAYLOR 26 NOV 19

SGT DIEGO RAMIREZ JR 26 NOV

SP5 MICHAEL P. BROWN 26 NOV

SP4 JEFFREY W. HAERLE 13 MAY

CHRISTOPHER J. SCHRAMM 13 M

SP5 SAMUEL C. MARTIN 17 MAY

FOREWORD

The first unit to be deployed to South Vietnam belonged to the United States Army Security Agency (ASA) as did the first to be decorated. The first acknowledged casualty of the war was an ASA soldier. All of these milestones are reminders that from the beginning Vietnam was very much an intelligence war. The challenge for US advisors and later commanders in the field was to locate an elusive enemy in a hostile environment. Communications intelligence quickly emerged as the ground forces' primary source of targeting the enemy and for planning operations; it also aided in obtaining other valuable sources of information, such as captured documents and interrogated prisoners of war—all by-products of successful combat operations. Because Vietnam was the first air-mobile war, timeliness of information became as critical as accuracy, where minutes spelled the difference between success and failure. Here again, ASA direct support elements served as invaluable conduits through which communications intelligence flowed to the combat commanders on a real-time basis.

The motto of the Military Intelligence Corps is "Always Out Front." It was precisely because ASA was out front that signals intelligence enjoyed the success it did in Vietnam. Army Security Agency personnel deployed to Vietnam four years in advance of major ground combat elements. This allowed ASA the time to develop a new technique (airborne radio direction-finding) to pinpoint a concealed enemy, to assemble the necessary background data, and to gain the experience required to support US forces in the field. If there is an over-arching lesson learned through the years, it is that military intelligence needs to be continually engaged in order to be successful. One only has to contrast the absence of intelligence in the early phase of the Korean War with the constant flow of information awaiting combat elements upon their arrival in Vietnam.

Although security restrictions prohibit the telling of the intelligence story in full, hopefully, the picture history format will provide a window into an important aspect of the Vietnam War that here-to-fore has not been publicized. Its purpose is to outline the scope and type of support furnished by the Army Security Agency and to provide testimonial evidence of ASA's overall success as well as to note various shortcomings. The history is also the story of individual sacrifice and professionalism on the part of ASA soldiers that will continue to foster *esprit de corps* among future generations of military intelligence specialists.

KEITH B. ALEXANDER
Major General, USA
Commanding US Army Intelligence and Security Agency
Fort Belvoir, Virginia
23 January 2003

PREFACE

Early in his career, Colonel James P. Brown headed up a small history team sent by the Army Security Agency to Vietnam to document its role in the war. Reflecting back, COL Brown recalled a comment made by one of his subordinates: "After working for weeks, night and day to finalize, assemble all the photographs, and make the requisite number of copies of the 509th Radio Research Group historical report, Lieutenant Hunt surveyed the two desks piled high with all the volumes and with a sigh mumbled, 'God, I hope someday someone reads all that stuff!' Indeed!" This history represents a small down payment on the efforts by ASA historical officers in the field and the historians back at Arlington Hall Station to document the signals intelligence story. Once the US Army Center of Military History has completed its official history of Vietnam, it is hoped that declassification will have advanced to the stage that Army intelligence can supplement the work with a more detailed operational narrative.

The history is limited in scope and does not attempt to tell the story of the larger cryptologic effort of the war. It draws only upon Army records and those readily available to the INSCOM History Office. The final product is the result of the contributions of many individuals. Colonel William H. Marvin, Chief of Staff, and Mr. Daniel Scarfo, Chief, Strategic Management and Information Office, provided overall supervision to the project. As in every endeavor undertaken by the History Office, it could not have been possible without the advice and assistance furnished by Dr. John P. Finnegan, Historian, the editorial support of Mrs. Karen E. Kovach, and the detailed review of the manuscript by Mr. Thomas Hauser, Staff Historian. The final product was enhanced by the comments of Ms. Romana Danysh, Organizational History Branch, Center of Military History, and by various ASA veterans.

Photographic support for this volume was provided by Mr. Robert J. Bills and graphic support by Ms. Robin Crawford, both of the Office, Assistant Chief of Staff, G6. Unless otherwise noted, all photos are from the INSCOM collection. Credit for design of this publication belongs to Ms. Maureen Nugent, Office of Typography and Design, US Government Printing Office.

A special word of thanks is owed Mr. James D. Currie, Jr., INSCOM Publishing Management Officer, for his ongoing liaison and quality control throughout the production process. Also to Mr. Mark Bertram for the loan of his unit insignia collection and Ms. Laura Siedlarczyk, who coordinated the volume at Department of Defense. As always, the staff of the US Army Cryptologic Records Center was helpful and patient during the research phase. Simply put, the book would not have been possible without the efforts of numerous people both present and past. However, any mistakes, errors, and omissions are solely the responsibility of the author.

JAMES L. GILBERT
US Army Intelligence and Security Command

TABLE OF CONTENTS

Foreword vii

Preface ix

The Early Years: 1961–1964 1

The Build Up: 1965–1967 29

New Battles: 1968–1970 57

Vietnamization: 1971–1973 91

Appendix A. Order of Battle 109

Appendix B. Unit Summaries 113

Appendix C. Key ASA Personnel 123

Appendix D. Fallen in Battle 124

Appendix E. Airborne Systems 125

Appendix F. Chronology 125

Appendix G. Acronyms 127

Appendix H. Unit Insignia 129

Arlington Hall Station served as headquarters of ASA's worldwide organization. Formerly an exclusive women's college, the Hall was home to the Army's code-breaking activities during World War II.

THE EARLY YEARS 1961 1964

"It has been my feeling in years past [prior to Vietnam] that we did not know too much about ASA. . . . If we did know much about it, maybe we felt they were working for authorities outside the Army, albeit important work."

LTG CREIGHTON W. ABRAMS, VICE CHIEF OF STAFF, US ARMY

In the closing days of World War II, US Army leaders began to turn their attention to planning for what would follow in the aftermath. High on their agenda was maintaining access to the Army's most important source of strategic intelligence—information derived from the intercept and deciphering of enemy communications. On 15 September 1945, the War Department established the Army Security Agency (ASA) with headquarters at historic Arlington Hall Station, Virginia. Building upon the legacy of its predecessor, the Signal Security Agency, ASA possessed a sweeping charter to conduct communications intelligence (COMINT) operations as well as to provide the Army with communications security (COMSEC). For the first time, all of the Army's signals intelligence (SIGINT) resources fell under one command. Organizationally, ASA was unique. It was literally an army within the Army. Due to its vertical chain of command, the agency replicated in miniature all the functions of the larger Army, ranging from personnel recruitment and training to research and development. ASA directed a worldwide organization consisting of theater headquarters in the Far East and in Europe and a series of fixed sites, or field stations. that encircled the globe and served as its collection arm.

Over time, ASA underwent a number of important mission changes. In 1949, the Joint Chiefs of Staff established the Armed Forces Security Agency, forerunner of the National Security Agency. In turn, the Army, Navy, and Air Force cryptologic agencies were forced to relinquish control of the signals intelligence system to the new Department of Defense organization. This realignment caused ASA to reexamine a previously neglected portion of its mission—COMINT and COMSEC support to the Army in wartime. The outbreak of the Korean War and subsequent buildup of US forces in Europe further reinforced the need for ASA to field tactical support units on a large scale. Soon groups and battalions became a fixture within the agency's force structure, and from 1950 to 1956, the number of such units grew from zero to nine. Other mission shifts included ASA assuming responsibility in 1955 for the Army's electronic intelligence (ELINT) and electronic warfare (EW) programs. However, both ELINT (intercept of noncommunications signals) and EW (denying the enemy use of his communications through jamming or deception) would largely remain in the background as ASA's primary focus continued to be communications intelligence.

In 1960, on the eve of US intervention into Vietnam, ASA was better prepared and better equipped than at any time to go to war. Although ASA's primary focus remained on manning its worldwide chain of field stations, the agency possessed the necessary doctrine for supporting combat troops, an R&D and materiel development capability geared to deploy new systems, and an efficient personnel system for recruiting, training, and sustaining a highly qualified force.

From its inception, ASA was cloaked in an aura of secrecy. An early recruiting poster proclaimed, "...by the very nature of its work, this agency remains little known." The problem was that ASA also remained little known to the larger Army. Vietnam would test ASA's ability to educate a new generation of combat commanders as to the value of its products and to overcome the obstacle that classification restrictions placed on the sharing of time-sensitive information. And as the Army moved towards air-mobile warfare, minutes could spell the difference between success and failure.

South Vietnamese crowds line the street to greet then Vice President Johnson, whose visit to Saigon in May 1961 would precede ASA troop arrivals by only a few days.
(Library of Congress)

President Eisenhower and President-elect Kennedy both supported assistance to South Vietnam, but it was the latter who stepped up the deployment of military advisors. (National Archives)

"Vigilant Always"

MOTTO OF THE ARMY SECURITY AGENCY

Involvement in Vietnam

At the end of World War II, Vietnam was locked in a struggle between the aspiration of Vietnamese nationalists and the desire of the French to reassert political and economic control over its former colony. Following a failed attempt at a negotiated settlement, guerrilla warfare broke out. Soon the Viet Minh (League for the Independence of Vietnam) controlled large sections of the countryside while French forces ruled most of the cities. The fall of neighboring China to the Communists in 1949 and the subsequent flow of assistance from the Communist Bloc to the Viet Minh escalated the war from a local conflict to one having international implications. Various Communist states recognized the Democratic Republic of Vietnam as the legitimate government while the United States and Great Britain accepted the new "State of Vietnam" supported by the French.

The 1954 defeat of its forces at Dien Bien Phu, coupled with the costs of fighting a protracted war, finally ended France's involvement in Vietnam. The departure of the French created a vacuum into which the US poured an increasing amount of supplies to South Vietnam and assumed responsibility for training its army. Later that year, a Peace Conference convened in Geneva, Switzerland. Here delegates from the Soviet Union, Great Britain, France, and the United States proceeded to divide Vietnam into North and South, separated by a demilitarized zone along the 17th Parallel.

One of the first foreign policy issues facing newly elected President John F. Kennedy in 1961 was how to counter the escalating pressures by the North Vietnamese backed guerrillas undermining the Republic of Vietnam. In response to calls for assistance by President Ngo Dinh Diem and US officials in Saigon, the Kennedy administration took steps to strengthen South Vietnam's ability to win the political, military, economic, and psychological war against Communist-backed insurgency. Among the types of aid being sought by the South Vietnamese was help for their fledgling communications intelligence effort. The Vietnamese had established a small Technical Study Center in Saigon and Dan Nang for the purpose of monitoring the guerrillas' communications. To encourage Vietnamese direct support to its Army, the US provided 30 SP–600 Hammerlund radio receivers along with several AN/PRD–1 direction finders.

In February 1961, LTG Lionel C. McGarr, Chief, Military Assistance Advisory Group, Vietnam (MAAG–V) raised the stakes for COMINT assistance by asking for direct US involvement. Subsequently, MG John M. Willems, Assistant Chief of Staff for Intelligence (ACSI) at Department of the Army (DA), floated a proposal to provide training to the South Vietnamese and at the same time establish US intercept operations in country. On 20 March 1961, the Department of State informed Headquarters, Department of the Army, that it was politically feasible for the US military to conduct a small COMINT effort in South Vietnam. Based on this positive feedback, the ACSI alerted MG William M. Breckinridge, Chief, ASA, to begin planning for deployment of a unit to Southeast Asia. At the same time, reports were arriving in Washington, DC, that the South Vietnamese COMINT element was beginning to enjoy success. These glowing evaluations would later prove erroneous. However, for the moment, they were greeted by the ASA leadership as indicators that the command would have no problem in fielding an intercept unit of its own.

On the eve of Vietnam, ASA's main focus was support of its worldwide chain of field stations.

Request for Assistance

The Army Security Agency's ability to quickly respond to DA's tasking to deploy a mobile intercept unit to South Vietnam demonstrated the strengths of its vertical command structure. The agency was able to draw upon expertise from its theater headquarters, USASA Pacific, for insights on the anticipated targets. Based on this input, Mr. Jimmie Garrett, a member of the Operations staff back at Arlington Hall, labored late into the night putting the finishing touches on Operations Plan (OPLAN) 7–61 (nicknamed WHITEBIRCH) and OPLAN 8–61 (SABER-TOOTH) that listed the equipment and personnel skills required. WHITEBIRCH established a 78-man ASA operational element to target local Communist guerrillas, and SABERTOOTH fielded a 15-man team to train South Vietnamese COMINT specialists supporting the Army, Republic of Vietnam (ARVN) at division and below. When the National Security Council met on 29 April 1961, President Kennedy formally approved the deployment of ASA personnel. Because HQ USASA controlled its own personnel assignments and training, the agency was able to quickly identify the individuals needed for WHITEBIRCH/SABERTOOTH and within 3 days had assembled them at its Training Center and School located at Fort Devens, Massachusetts. At the same time, ASA logisticians lined up the equipment to be shipped; any piece not already in the inventory was taken from a unit lacking an immediate requirement for it. This shuffling of

"The greatest contribution Vietnam is making—right or wrong is beside the point—is that it is developing an ability in the United States to fight a limited war, to go to war without the necessity of arousing the public ire."

ROBERT S. MCNAMARA, SECRETARY OF DEFENSE

personnel and assets to accomplish mission priorities was an art form that ASA had perfected over the years.

As it awaited further orders, the ASA contingent organized itself into the 400th USASA Operations Unit (Provisional) with a cover designation as the 3d Radio Research Unit (RRU). (Throughout the Vietnam Conflict, ASA would designate all of its units as "Radio Research" to shield its presence.) As part of this low visibility status, the first ASA personnel were required to carry US passports, wear civilian clothes, and if asked, indicate that they were military advisors attached to MAAG–V. A local post exchange remained open late one night so that the 3d RRU soldiers could select civies. However, because there was so little variety to choose from, it became the standing joke that the ASA personnel might just as well have been issued uniforms since they were all wearing clothes of a similar style and color.

The first members of ASA to arrive in Vietnam were COL Robert T. Walker, Chief of USASA–PAC, and LTC Robert W. Williams, designated Commander, 3d RRU. The two officers were there to make final arrangements for ASA's pending deployment and to identify possible operational sites. On 9 May in response to a query from the White House, the Army indicated that its ASA element was poised for departure. Three days later, Republic of Vietnam officials formally agreed to a cooperative COMINT effort between its armed forces and those of the United States, but with the understanding that shared information would be limited in content and scope. Upon learning of the agreement, COL Walker immediately flashed word back to the 3d RRU that all systems were "Go."

A cartoon from ASA's publication, The Hallmark, captures the thoughts of many a new recruit to the agency.

Dressed in civilian clothes and carrying weapons, soldiers of the 3d RRU manned the remote direction-finding site at Ha Tien.

On The Ground

On 13 May 1961, 92 personnel of the 3d RRU landed at Tan Son Nhut Air Force Base, located just west of Saigon proper. Here they were greeted by COL Walker and LTC Williams. Throughout the next week, C–124s and C–119s continued to bring equipment contributed by ASA units worldwide. (The 3d RRU's entry marked the first time that an entire Army unit had deployed to South Vietnam; previously only individual advisors had been assigned.) The headquarters and processing elements of the 3d RRU immediately found a home in an empty warehouse near the airfield. Personnel were billeted at the Majestic Hotel in Saigon, but the need to economize soon led to a search for new quarters. Enlisted men eventually occupied six floors of a new building located at 39 Hai Ba Trung, while the officers settled into four small bungalows located in a nearby residential area.

On 15 May at 1015 hours, operations were up and running. Inside shelters parked alongside the Tan Son Nhut airstrip, ASA soldiers tuned their receivers in search of manual Morse signals. A month later, at the encouragement of the ARVN Chief Signal Officer, the 3d RRU moved its vans to the nearby Vietnamese Joint General Staff Compound (Trai Tran Hung Dao), which was located in Saigon proper and also served as the headquarters of South Vietnam's own intercept effort. By having US COMINT operations close-at-hand, the South Vietnamese were suspected of wanting to

"If injured or killed in combat, report as training accident in the Philippines."

STAMPED ON MEDICAL RECORDS OF 3d RRU PERSONNEL

extract more concessions in terms of equipment and information sharing. In the coming months, considerable finesse and diplomacy would be demanded of US officials in deflecting requests from their hosts for added support and increased access.

By 28 May, site surveys for establishing the WHITEBIRCH direction-finding net were completed. The net would stretch along the coastline, running from Ha Tien in the southwest to Cap Saint Jacques east of Saigon and finally to Nha Trang in central Vietnam. Within a month, all of the sites had become operational. At the more isolated Ha Tien site, ARVN soldiers provided security, and ASA operators were instructed to carry weapons at all times and not to travel at night.

The SABERTOOTH School occupied a building at the Joint General Staff Compound and used equipment and instructional material donated by the 3d RRU. In July, ASA advisors began week-long classes to familiarize ARVN SIGINT specialists with various pieces of equipment, but delays in logistical support pushed the formal opening of the school back to early September. Students in the first class completed some 528 hours of instruction, covering such subjects as manual Morse intercept, direction-finding, communications, and maintenance.

No sooner had the 3d RRU settled in country, than efforts were underway to increase its size. At the beginning, only 17 hours of daily coverage were necessary because the Viet Cong ceased operations between 1600 and 2300 hours, but the emerging need for around-the-clock monitoring soon required the Chief, USASAPAC to come up with an additional 52 spaces. At the same time, the National Security Agency looked unfavorably upon ASA's growing commitment to the ground war in South Vietnam, expressing concern that ASA was robbing resources from its other missions within the Pacific theater. No one could have envisioned that within 6 years ASA's in-country strength would be nearly 6,000 personnel.

The Direction-Finding Problem

Dating as far back as World War I, the US Army had utilized direction-finders (DF) to locate enemy transmitters and, in turn, enemy forces. Upon acquiring a signal, direction-finding (DF) stations within a DF net would simultaneously take bearings on the transmission. The point where three or more lines crossed would result in a "fix." Unlike earlier conflicts, the task of finding an elusive enemy would take on an even greater sense of urgency in Vietnam.

ASA arrived in Vietnam fully expecting that its direction-finding mission would be accomplished. (ASA's optimism was due in part to erroneous reports it had received of early success by the South Vietnamese.) Plans called for a medium-range direction-finding (MRDF) net to be established at semi-permanent sites. The net would pass general targeting locations to mobile direction-finding teams using AN/PRD–1s. Operating from locations 5–15 miles away from an enemy transmitter, the mobile teams could then produce the necessary refined fixes. Once an enemy unit was sufficiently pinpointed, South Vietnamese forces could then engage it.

Located entirely within the targeted area, the WHITEBIRCH Net was initially thought to represent the ideal situation because of the closeness of substations to their targets. However, the insurgents waging mobile warfare in mountainous regions and possessing limited resources utilized hand-generated, low-powered radios for means of communications. Instead of attempting to broadcast by direct or ground waves that couldn't travel beyond 5 to 15 miles, enemy communicators employed horizontally radiating antennas in the high-frequency band. By this means, the signals were bounced off the ionosphere to receiving stations. DF operators could normally calculate bearings from sky waves. However, in Vietnam, targets located 15 to 150 miles away produced sky waves with unusually steep angles (greater

A PRD–1 mounted on a ¼-ton vehicle.

"The principle of airborne direction-finding appears to have possibilities for generally improving DF effectiveness on the Viet Cong problem. Recommend that equipment be assembled and concept tested in CONUS...."

LTC WILLIAM J. COCHRANE, JR., CDR, 3d RRU

than 45 degrees) for the DF site to intercept. Under these conditions, accurate bearings were hard to come by, and there was little wisdom in launching a tactical operation against the Viet Cong at an ill-defined location. The WHITEBIRCH net faced other challenges such as the effects of humidity upon the AN/TRD–4A direction finders and the lack of transportation to isolated sites where security was a growing concern. ASA operators at Ha Tien were soon subjected to small-arms fire, leading to the substation's relocation to Bien Hoa.

By the fall of 1961, the 3d RRU's new commander, LTC William J. Cochrane, was turning to Arlington Hall Station for answers to his direction-finding problems. Warrant Officer George Miller served as the point of contact for the 3d RRU and began correspondence with Mr. Herbert S. Hovey, Jr., an electrical engineer in the Office of the Assistant Chief of Staff, Developments at HQ USASA. Eventually, a four-pronged approach to the problem emerged: investigate the possibility of an airborne system, improve the PRD–1, replace the TRD–4As, and develop a small man-pack direction finder for future Special Forces operations. To even consider airborne direction-finding at the time indicated a certain amount of desperation on the part of ASA leaders.

ASA's First Casualty

When the idea of airborne radio direction-finding (ARDF) first surfaced, Mr. Herbert Hovey immediately contacted Mr. Harold H. Jaffe and Mr. John Woodworth from the US Army Electronics Command (ECOM) laboratories located at Fort Monmouth, New Jersey. The three had collaborated in the past on similar projects. The first item on the ASA/ECOM team's agenda was a fact-finding trip to Vietnam. Here, they tried to acquire first-hand knowledge of the direction-finding problem and the local signal environment. Among those they talked with was 25-year old SP4 James T. Davis, who was serving as an advisor to one of the ARVN PRD–1 teams. Davis, a native of Livingston, Tennessee, had come to Vietnam as a member of the original 3d RRU contingent. Reflecting the optimism of the times, Specialist Davis wrote home to his family that, "I feel a little proud about this deal, too. I just hope that our little bit will help to ease things in this part of the world." He also communicated the growing danger of his assignment, "We became a little more involved in this conflict yesterday... It looks like the bad guys have gotten the word to start giving us hell. It breaks the daily routine even though it could become a bit dangerous."

SP4 James T. Davis "... the first American to fall in defense of our freedom in Vietnam."

PRESIDENT LYNDON B. JOHNSON

As tests on the new ARDF system proceeded at Fort Monmouth, the 3d RRU renewed its efforts to make direction-finding successful by utilizing resources on hand. To increase coverage, the 3d RRU began integrating ARVN stations into the WHITEBIRCH net. In addition to the static MRDF net, the 3d RRU also continued to field mobile, short-range direction-finding (SRDF) teams, using PRD–1s. However, establishing an SRDF net meant that ASA personnel were often forced to operate near the enemy. Normally, a network of vehicles consisting of two jeeps and a ¾-ton truck would deploy on a SRDF mission that might last up to a week. Evidence later emerged that the Viet Cong were fully aware of the mission of these DF-teams, and in fact, had taken steps to target them.

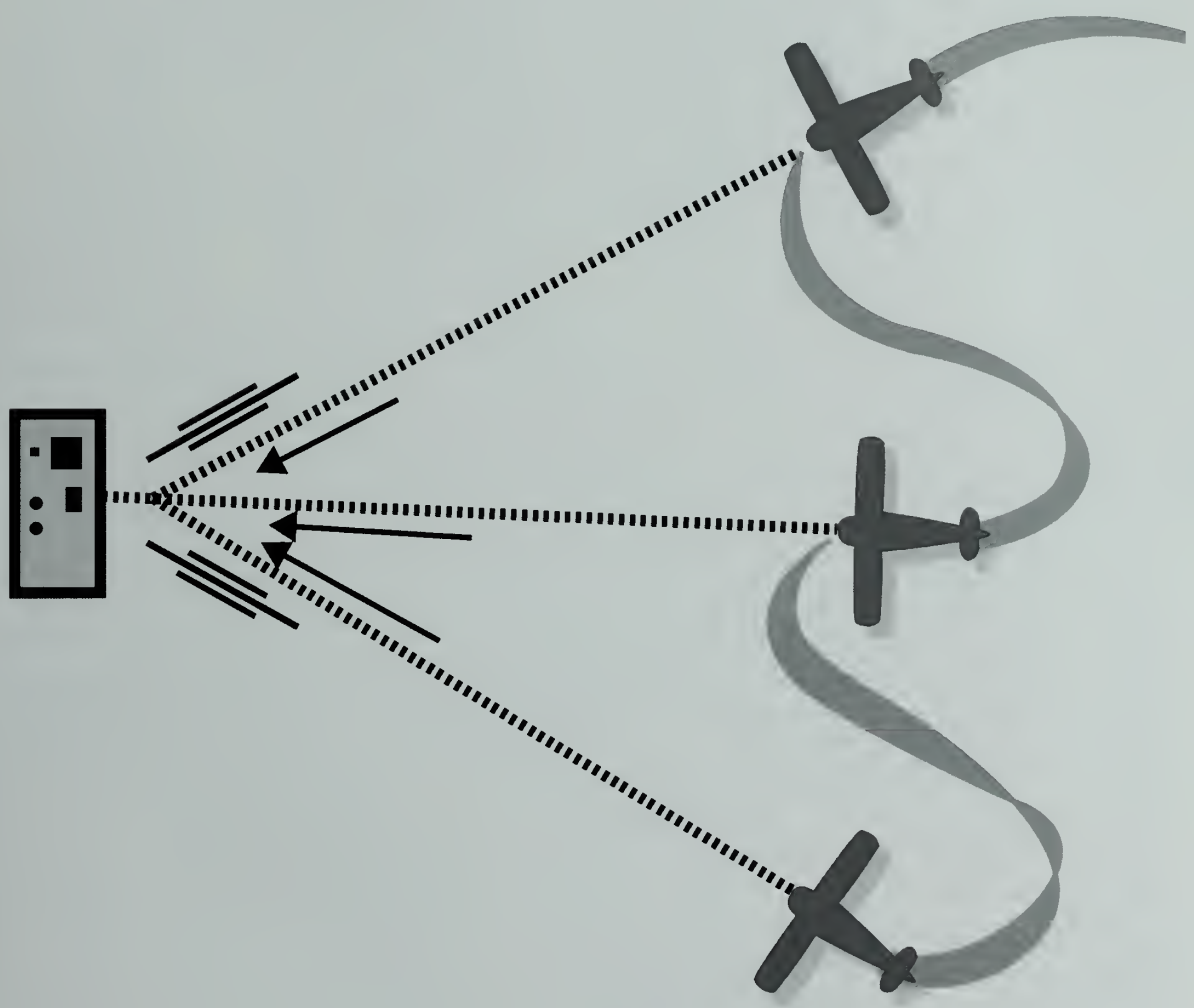
At noon on 22 December 1961, Specialist Davis and his PRD–1 team had just taken a bearing approximately 20 kilometers west of Saigon. The ¾-ton truck carrying Davis and ten ARVN soldiers proceeded northwest on Provincial Highway 10 and was 800 meters west of Cau Xang, not far from the remnants of an old French garrison and a nearby canal, when an electrically controlled land mine suddenly exploded underneath the vehicle's tailgate. The truck then spun out of control, coming to rest in the right ditch. Emerging from their concealed positions, a band of approximately 20 Viet Cong opened fire on the dazed and wounded soldiers. Managing to escape from the truck, Davis returned fire with his M–1 rifle before being fatally struck. Within minutes the ambush was over, and Davis and nine members of his team lay dead. Besides stripping the soldiers of their weapons, the Viet Cong also removed the radio to add to their eclectic collection of US/French/Chinese communications gear.

Because wartime conditions did not exist at the time, Army Regulations prohibited awarding Davis the Purple Heart. But on 10 January 1962, Davis' fellow ASA soldiers dedicated the 3d RRU's facility at Tan Son Nhut Air Base as "Davis Station" to serve as a memorial to their fallen comrade. Of all the tributes given, none, however, were more fitting than the words of Davis' father, "It is a tragedy... to lose a son, but is also an honor to know that a son was a good soldier."

Specialist Four James T. Davis was killed while on an advisory mission with a South Vietnamese PRD–1 team.

The 3d RRU area at Ton Son Nhut AFB in Saigon was named in honor of Specialist Davis.

Inside the U–6, there was barely room for the intercept operator and equipment.



"Because in a way it [airborne radio direction finding] is the radar of Vietnam...."

MR. HERBERT S. HOVEY, JR., ENGINEER, HQ USASA

Airborne Radio Direction-Finding

The challenge for the ASA/ECOM engineers was to create an airborne system that could discriminate between direct and sky waves. Although the answer on how to decouple the antenna from the metal skin of the aircraft was sophisticated, the hardware portion of the problem was easy to solve. The biggest obstacle proved to be selection of the right type of aircraft. When early tests using a UH–19 "Chickasaw"helicopter failed because of vibration problems, the engineers turned to the U–6A, a small, fixed-wing aircraft nicknamed the "Beaver." The U–6s were numerous in Vietnam, which meant that maintenance support was readily available. The aircraft also provided the pilot good ground visibility and could transport a crew of three plus a small load of equipment.

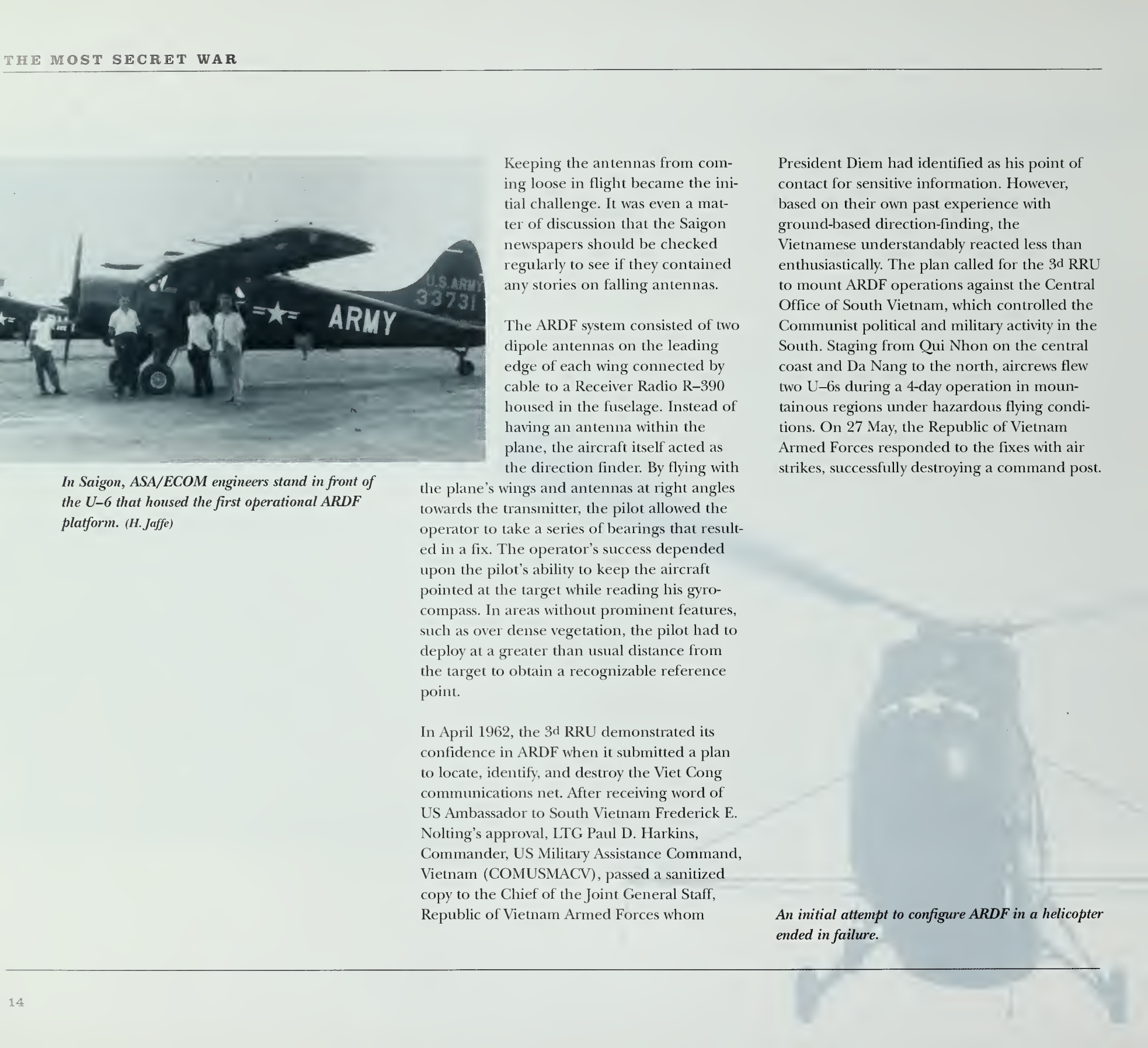
Carrying the airborne radio direction finding (ARDF) equipment in their luggage, the ASA/ECOM team, minus Woodworth, who ironically disliked flying, boarded a commercial flight for Vietnam in early March 1962. Meanwhile, the 3d RRU secured three U–6 aircraft from MAAG–V along with the services of two pilots, CPT William F. Simpson and CPT Donald C. Schessler, neither of whom had prior experience working with communications intelligence. Upon arriving in Saigon, the ASA/ECOM engineers immediately set about installing the DF equipment on the Beavers.

In Saigon, ASA/ECOM engineers stand in front of the U–6 that housed the first operational ARDF platform. (H. Jaffe)

Keeping the antennas from coming loose in flight became the initial challenge. It was even a matter of discussion that the Saigon newspapers should be checked regularly to see if they contained any stories on falling antennas.

The ARDF system consisted of two dipole antennas on the leading edge of each wing connected by cable to a Receiver Radio R–390 housed in the fuselage. Instead of having an antenna within the plane, the aircraft itself acted as the direction finder. By flying with the plane's wings and antennas at right angles towards the transmitter, the pilot allowed the operator to take a series of bearings that resulted in a fix. The operator's success depended upon the pilot's ability to keep the aircraft pointed at the target while reading his gyrocompass. In areas without prominent features, such as over dense vegetation, the pilot had to deploy at a greater than usual distance from the target to obtain a recognizable reference point.

In April 1962, the 3d RRU demonstrated its confidence in ARDF when it submitted a plan to locate, identify, and destroy the Viet Cong communications net. After receiving word of US Ambassador to South Vietnam Frederick E. Nolting's approval, LTG Paul D. Harkins, Commander, US Military Assistance Command, Vietnam (COMUSMACV), passed a sanitized copy to the Chief of the Joint General Staff, Republic of Vietnam Armed Forces whom President Diem had identified as his point of contact for sensitive information. However, based on their own past experience with ground-based direction-finding, the Vietnamese understandably reacted less than enthusiastically. The plan called for the 3d RRU to mount ARDF operations against the Central Office of South Vietnam, which controlled the Communist political and military activity in the South. Staging from Qui Nhon on the central coast and Da Nang to the north, aircrews flew two U–6s during a 4-day operation in mountainous regions under hazardous flying conditions. On 27 May, the Republic of Vietnam Armed Forces responded to the fixes with air strikes, successfully destroying a command post.



An initial attempt to configure ARDF in a helicopter ended in failure.

The 3d RRU had its own communications center in Saigon.

Success At Last

A year after its arrival in Vietnam, the 3d RRU was beginning to make the impact it had originally envisioned. Much of the success could be attributed to ARDF, which eliminated many of the problems previously associated with ground operations. The ARDF operator and equipment could get close enough to the target transmitter with reasonable safety. One aircraft moved fast enough to cover a vast area and did not require a network of direction finders. ARDF also offered quicker response to the tactical commander's requirements in a fluid situation. However, it was ARDF's ability to precisely target the enemy that made the difference in driving other forms of intelligence gathering, such as reconnaissance, and that led to follow-up by artillery, air strike, and ground operations. Finally, ARDF gave the ARVN, and later the US forces, the advantage of surprise, essential during airmobile and rapid entry operations. (It should be noted, however, that in these early years, the ARVN still did not take full advantage of the new source of intelligence.) For its contributions as the ground war escalated, the 3d RRU was presented the Meritorious Unit Commendation in February 1963—the first unit to be so decorated in Vietnam.

The speed with which the first ARDF platforms were deployed to the field could be attributed to their being assembled "in-house" from available resources. Because the original system was relatively simple and the hardware already in existence, ASA required no large outlay of

"One of the biggest historical disadvantages to any counter-insurgency program has been the inability to locate guerrilla concentrations. The direction-finding activities of the 3d Radio Research Unit have provided this headquarters with a vital intelligence advantage previously unavailable to any US or friendly tactical force."

LTG PAUL D. HARKINS, COMUSMACV

The twin-engine U–8 equipped with navigational gear gave the 3d RRU an ARDF platform with greater versatility.

research and development funding from Department of the Army. Consequently, ARDF progressed as rapidly as new platforms were required. During 1963, ASA added two U–8 "Seminoles" to its ARDF fleet. Although the U–8's airframe kept the platform from producing as accurate fixes as the U–6, the Seminole would quickly emerge as the workhorse in the Army's ARDF fleet. The twin-engine aircraft gave the 3d RRU an "all-weather" capability for the first time, and the extra cargo space allowed for installation of navigational gear, eliminating dependence upon visual sightings of landmarks. The aircraft also covered more target areas faster and could be flown at higher altitudes—important in mountainous regions. The bottom line was that the U–8 offered greater versatility and thus greater productivity.

Tan Son Nhut Airfield served as home base for the 3d RRU's aircraft and as headquarters for the 3d RRU's Aviation Branch, which was responsible for managing the growing ARDF mission. On a temporary basis, ASA pilots also flew missions from other airfields. In early 1963, the 3d RRU created a second permanent base for air operations at Phu Bai, 10 miles south of the ancient capital of Hué and approximately 450 miles north of Saigon. ARDF operations at Phu Bai were initially limited to the dry season that lasted from April to October.

At the same time the Army's ARDF program was getting off the ground, the Air Force was laying out long-range plans of its own. However, leadership at the Department of Defense expressed serious reservations regarding the Air Force's proposal until their concerns were alleviated following discussions with ASA engineers. Still, it would take time before the Air Force could deploy a viable system. In the interim, ARDF remained an Army story.

The SABERTOOTH School in Saigon was used for training ARVN signals intelligence personnel.

"These huts probably withstood the weather many years before they were sent in there with the AN/TRD–4, and now they are just rotting. At three of the sites the ARVN and the site advisors erected a bamboo hut right over the other hut."

CWO3 FRED NEWELL, JR., SIT OFFICER, 3d RRU

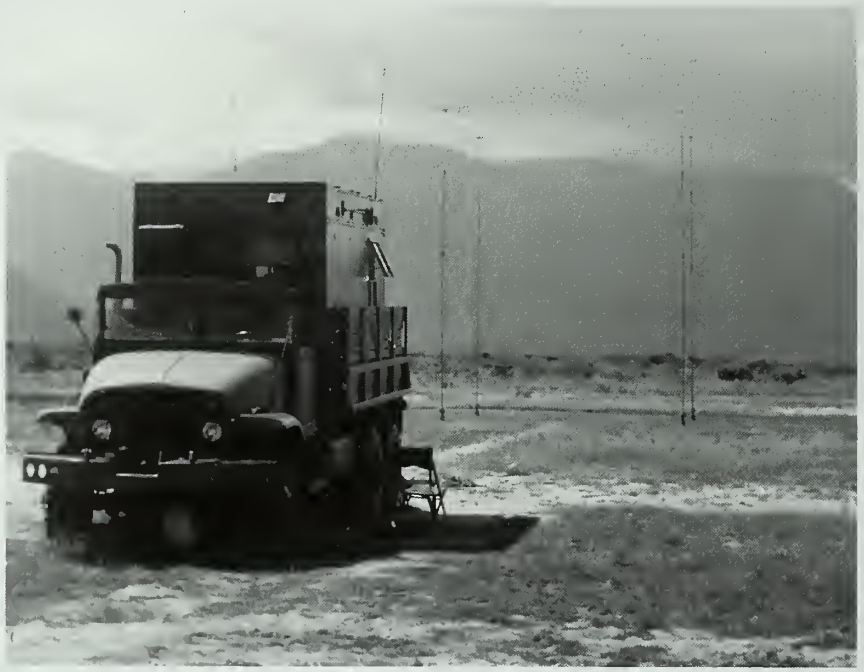
Training The ARVN

The 3d RRU's mission of running a cryptologic school for their South Vietnamese counterparts was short-lived. After its opening in September 1961, the SABERTOOTH School completed only two cycles of instruction in basic SIGINT skills. Approximately 70 students graduated from the course plus another 75 from instruction in equipment familiarization, before difficulty in identifying personnel for security clearances caused classes to be suspended for 8 months. During the wait, the 3d

RRU proceeded to transfer its training equipment to the ARVN, and by April 1963, the South Vietnamese assumed complete responsibility for the training center. Assisted by a handful of 3d RRU advisors, ARVN instructors conducted classes only whenever sufficient numbers of cleared students were available. In late 1964, an advanced course in intercept and direction-finding was offered for the first time, but the results proved disappointing. Almost half of the operators failed to copy Morse code at the minimal rate of 25 words a minute.

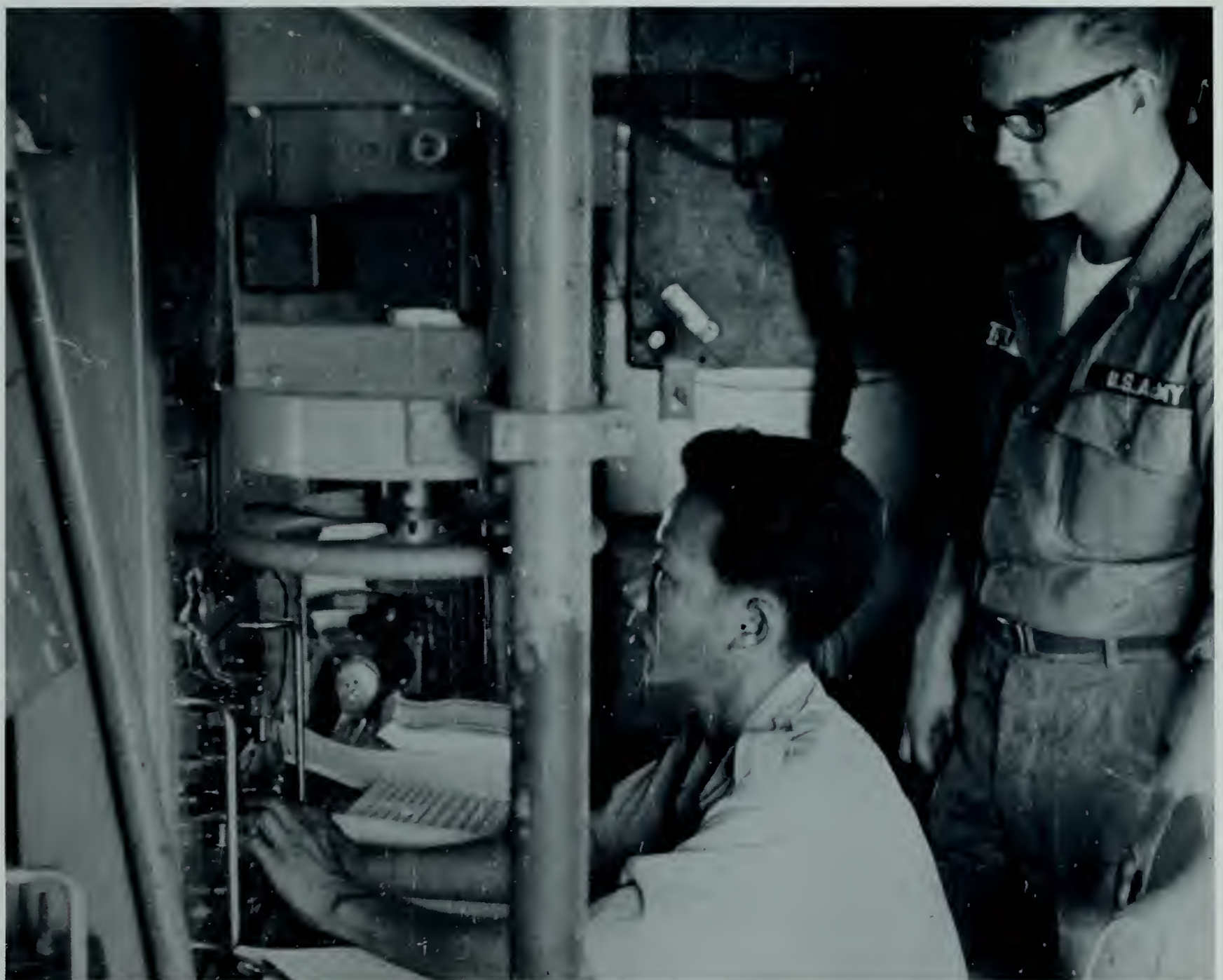
The WHITEBIRCH MRDF net furnished an early opportunity for joint operations. ASA believed that by adding four ARVN outstations, the accuracy of the net could be improved. At each of these new substations, the 3d RRU provided supervision and, for the first time, shared use of its TRD–4A direction finders. By June 1962, 3d RRU personnel were down to manning only two of the WHITEBIRCH outstations. Consequently, ASA could now devote more of its resources to ARDF and the establishment of a second independent MRDF net with a much longer baseline.

In September 1962, Unit 15, the ARVN COMINT element, expressed interest in jointly participating in the 3d RRU's ARDF program. This set off a debate between US officials in Saigon and Washington over how much technical information should be exchanged. In light of recent improvements in Viet Cong communications security procedures, many feared that shared secrets were being leaked to the enemy. Rebuffed, the South Vietnamese



simply began a program of its own. This led US officials to reverse their early stance and to agree to fund four platforms. However, over time, the South Vietnamese would fail to emerge as an important player in ARDF.

Although Unit 15 had tripled in size from 1960 to 1962, it continued to suffer from a lack of direction and support from senior ARVN officers. One of the major reasons was that Unit 15 had to compete with the larger ARVN Signal Corps for qualified individuals. Both fell under the control of the Office of the J6, Joint General Staff (JGS), but the J6 regarded Unit 15 as an unwanted step-child and was reluctant to transfer personnel with the necessary technical skills to the COMINT side. When the Office of the J7 was established in March 1963, it assumed total command and control of COMINT, but it failed to bring about an immediate solution to the personnel problem. Still the 3d RRU welcomed this attempt on the part of the South Vietnamese as a step in the right direction and seized upon the opportunity to further encourage Unit 15 by helping to develop a new internal table of organization and equipment. As part of its assistance package, ASA transferred 15 trucks with S–144 shelters, 20 tape recorders, and 21 PRD–1 direction finders. However, what was lacking was any acknowledgement by the South Vietnamese of their need for technical improvement. The culture, the political system, the lack of leadership, and absence of personal skills all worked against success. The fact that there was a steady stream of US advisors rotating in and out also didn't help to bring the message home.



A member of the 3d RRU looks over the shoulder of an ARVN direction-finding specialist, symbolic of ASA's advisory role in the war.

Communications Security

Even before the arrival of the 3d RRU, a handful of Army Security Agency personnel were already in Vietnam engaged in fulfilling the command's other major mission—communications security. In 1959, questions were raised as to the state of security of military communications being used by American advisors. These concerns eventually led MG Charles J. Timmes, Chief, MAAG–V, to request assistance from ASA. In late 1960, a six-man team of the 104th USASA Detachment was sent TDY to Vietnam to monitor military circuits. The team quickly discovered that for all practical purposes the United States/Republic of Vietnam military radio nets were operating without adequate COMSEC. Their report disclosed that some US military advisors had failed to use one-time

Specialists of the 7th RRU based out of Saigon monitor MACV communications for security violations.

encryption pads even once during their entire tour. As a result, COL Walker, Chief, USASAPAC, ordered the issuance of crypto equipment to MAAG–V elements, recommended procedural changes in the transmission of messages, and established control over call-sign and frequency assignments.

Nine months after its arrival in country, the 3d RRU received authorization to establish its own COMSEC mission and proceeded to allot five soldiers to the task. The 3d RRU's effort was elevated a month later when a COMSEC team of the 104th Detachment on TDY departed Vietnam leaving behind most of its monitoring equipment. To cover the communications of the widely dispersed US military advisers, the 3d RRU's new COMSEC Section created mobile teams. The first of these two-man teams was tasked with monitoring the MAAG–V Advisory Team 1 at Da Nang. Besides supporting US advisors, COMSEC personnel also trained the ARVN in the use of cryptographic materiel furnished by the United States. Over the next year, the 3d RRU COMSEC element continued to expand, eventually reaching 18 personnel.

On 1 March 1963, the 101st USASA Security Detachment (known initially within country as

the 7th RRU) was organized, ushering in the second phase of ASA COMSEC operations in Southeast Asia. Subordinated to the 3d RRU, the 30-man unit assumed the mission of the former COMSEC Section and subdivided itself into headquarters, security monitoring, and control/analysis elements. The 7th RRU was physically located at the Joint General Staff Compound next to the building housing the 3d RRU's COMINT operations. The creation of the 7th RRU greatly expanded the use of mobile teams to cover MACV elements located throughout South Vietnam. Although there were on-going problems in scheduling either air travel or armed convoys between sites, the 7th RRU was still able to field 10 COMSEC teams by the end of 1963.

By late 1964, it was apparent that the 7th RRU had nearly exceeded its capabilities; the unit's personnel were logging long hours in trying to meet their heavy monitoring schedule. To help alleviate the workload, 16 more soldiers were assigned and another 14 placed on TDY from the nearby 104th USASA Security Detachment. Within months, the ASA COMSEC effort in Vietnam had doubled in size, and the 7th RRU was gradually acquiring the manpower and equipment needed to cope with its ever-expanding mission.

Special Forces

ASA's fielding of special operations units in the early 1960's paralleled the Army's increased reliance on Special Forces to fight counterinsurgency war. By 1962, ASA had organized Special Operations Detachments (SOD) to support each of the Army's four Special Forces Groups. Later that same year, Department of the Army outlined the type of role ASA would play in special warfare operations. The SODs could provide COMINT and COMSEC to US Special Forces and help train indigenous personnel of friendly countries. However, shared COMINT could not normally exceed the classification level of "SECRET" and under no circumstances would training of foreign personnel be conducted at a higher level.

Actual fielding of special operations detachments proved difficult. Details on what specific type of support the SOD should provide and what exact form that support should take still

ASA had its own organic detachments trained to support the Army's Special Forces.

ASA Special Forces experimented with a variety of manpack intercept and direction-finding equipment.

"Much of our information came from the 400th SOD, a Special Forces unit flown in to run test missions for us to determine how close they could get to the border in order to find better intercept sites."

SFC ROBERT J. SMISEK, OPERATIONS SECTION, 3d RRU

had to be ironed out. While creating the SODs, ASA attempted to integrate a number of missions within a small detachment by cross training personnel, by reducing layers of command, and by attaching the unit to its parent organization for logistical purposes. In several instances, ASA drew upon lessons-learned of the 3d RRU, such as emphasizing the use of manual Morse operators (frequently referred to as "ditty-boppers") who possessed language skills. However, upgrading language proficiency did not prove easy, and interpreting and applying security regulations remained major obstacles. Finally, there was an absence of lightweight equipment for mobile operations. While awaiting development of new systems, ASA turned to purchasing off-the-shelf receivers, but even here the procurement process faced protracted bureaucratic delays.

Special Forces were among the first advisors that the US deployed to Vietnam. However, it took some time before ASA could allay the concerns on the part of national authorities regarding possible compromise of secrets while conducting special operations in Vietnam. In the end it was agreed that ASA Special Forces personnel would not carry technical material with them other than what they had developed during the operation itself. Before distributing any intelligence, the SOD would be responsible for sanitizing it for references to any specific COMINT source and would forward copies of all released information to the local Special Security Office (SSO) in Saigon and to the 3d RRU. (The SSO system, which was totally independent of ASA, oversaw the handling and distribution of compartmented information throughout the SIGINT community.)

In February 1964, the 400th USASA SOD deployed a team for a 120-day field test in Vietnam. By the time they were ready to redeploy, the team had confirmed that the Viet Cong were using voice communications and recommended that the ARVN's Unit 15 should follow up. (The exercise also pointed out a paucity of fluent linguists within the SOD.) For the next 2 years, personnel of the 400th shuttled back and forth to Vietnam on one-of-a-kind assignments. These missions provided an opportunity to test direct support to tactical forces and represented an important milestone in shaping ASA's future assistance to Special Forces. Besides operational support, 400th teams also advised ASA planners at the new Phu Bai site on defensive measures and tactics and helped train the station's personnel in the use of weapons.

ASA's Special Forces initially lacked portable equipment and were required to buy systems off-the-shelf.

Detachment J

In January 1962, the 3d RRU received authorization for 21 officers, 4 warrant officers, and 356 enlisted men. A major reason for the increase in manning was the establishment of the Mobile Detachment at Da Nang, near one of the existing South Vietnamese intercept sites. The detachment consisted of an M–292 mobile van that possessed both manual Morse intercept positions and a direction-finding capability—all targeted against selected Viet Cong in the northern provinces and North Vietnamese ground and naval communications. Although collection results at Da Nang represented a real improvement from the past, growing concern over North Vietnam's support of the Viet Cong led to planning for a site even closer to the northern border.

In April 1962 the 3d RRU dispatched a team of three intercept operators to Phu Bai, 10 miles south of Hué, to determine how well targets could be heard. Upon receipt of positive readings, ASA decided to relocate its Mobile Detachment. Although the new site lay 450 miles north of its parent unit, the detachment was near the Phu Bai airstrip and adjacent to Highway 1, allowing the station easy access to logistical, security, communications, and technical support, but more importantly, the area provided excellent reception of the desired signals. However, high winds and sand storms delayed construction, and much of the equipment such as the M–292 vans, which could not readily negotiate the mountainous stretch of road leading from Da Nang, had to be flown

The 3d RRU Mobile Detachment was initially located at Da Nang.

"The channel marker for the Phu Bai direction-finding site was 'Juliet' or 'J.'"

MSG HAROLD E. CASTLE, 3d RRU

Located near Phu Bai, Detachment J was targeted against the Northern provinces and served as a window into North Vietnam.

in. It would take nearly 9 months before the site was ready for occupancy. Upon relocation to Phu Bai in January 1963, the Mobile Detachment became known as Detachment J.

In early 1964, a study of North Vietnamese communications acknowledged a need for expanded coverage. In response, ASA outlined plans for a major field station to be constructed at Phu Bai, designed to accommodate nearly a thousand personnel and a hundred operational positions. However, changes had already begun that would transform the US military presence in Vietnam and reshape ASA's support role. As these historic events began to unfold, Phu Bai found itself at center stage.

Phu Bai also served as home to a detachment of the US Marine's First Composite Radio Company, which was based out of Hawaii. Phu Bai offered the Marines a forward area for COMINT training under the auspices of the 3d RRU. Among the targets of interest to the US Marines were those of the North Vietnamese navy and their reactions to US patrols in the Gulf of Tonkin. (The purpose of these so-called Desoto patrols was to assert freedom of navigation in international waters and to collect photographic and hydrographic information.) On 2 August 1964, Marine operators at Phu Bai accurately foretold of a pending attack by the North Vietnamese on the US destroyer *Maddox*. If such attacks occurred again, the White House warned North Vietnam that there would be consequences. New SIGINT warnings by Phu Bai telling of apparent North Vietnamese plans for more naval attacks and the subsequent response of the destroyers *Maddox* and *Turner Joy* to unknown and unseen enemy vessels on the night of 4 August provided sufficient justification for President Johnson to ask Congress to endorse an expanded role for the American military in South Vietnam by passing the Gulf of Tonkin Resolution.

Enlisted quarters at 39 Hai Ba Trung in Saigon.

Members of the 3d RRU render honors to the flag-draped coffins bearing their fellow soldiers, killed by a Viet Cong detonated bomb in February 1964.

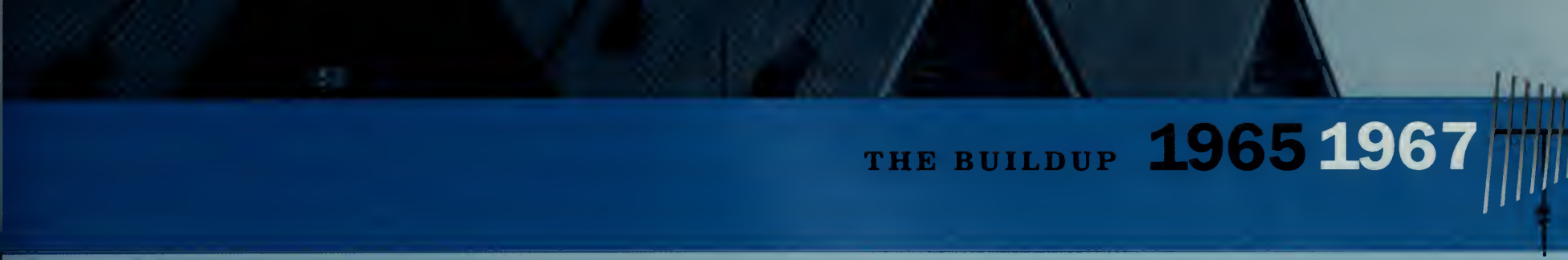
An ASA analyst operating in the field near Pleiku.

Eventually, 3d RRU soldiers found housing in a compound near Tan Son Nhut Air Base. (Note the memorial constructed to honor ASA fallen in foreground.)

"The very best soldiers, or let me say the most highly intelligent, were in ASA. . . . ASA acquired quite a lot of people who weren't particularly interested in avoiding the draft but wanted to do their duty by their country so they volunteered for Agency work. . . ."

COL JOHN J. MCFADDEN, CDR 509th RR GP

The 198th Infantry Brigade arrived in country in December 1966. In time, ASA would have 27 units in direct support of combat forces. (National Archives)



THE BUILDUP 1965 1967

"We were the first detachment of this type to be sent over there and we were the first to be committed. We ran into more bumps and grinds than those that followed."

SSG RICHARD W. HURLBAT, 404th RR DET

The year 1965 opened with the Republic of Vietnam reeling from a series of military setbacks and a deepening political crisis. At Binh Gia, the Viet Cong launched a division-sized attack against the ARVN, and for the first time, the North Vietnamese Army sent its troops into battle near Dak To in the Central Highlands north of Kontum. Terrorist attacks had also stepped up, and among their targets were installations having a strong US presence. It was becoming evident to American policymakers that the existing level of US aid was insufficient to prevent South Vietnam from collapsing. In light of these developments, General William C. Westmoreland, Commander, US Military Assistance Command Vietnam (COMUSMACV) recommended to his superiors that US Army and Marine ground forces, together with supporting air and naval forces, be sent to South Vietnam and adjacent waters.

The Army Security Agency had two battalions available for deployment: the 303d ASA Battalion (Corps) at Fort Wolters, Texas, and the 313th ASA Battalion (Corps) at Fort Bragg, North Carolina. (Their total strength stood at 1,927, an 80 percent fill, due in part to the number of individual soldiers already in Southeast Asia.) The 303d ASA Battalion provided COMINT, COMSEC, and EW support to the III US Army Corps and its major subordinate commands during field exercises and contingencies. The 313th ASA Battalion performed a similar role for the XVIII Airborne Corps. (For example, in April 1965, the battalion deployed its Company A in support of the 82d Abn Division during the US intervention in the Dominican Republic.) The only other tactical asset stationed in CONUS was the 403d ASA Special Operations Detachment, also at Fort Bragg. The 44-man detachment was attached to the 3d Special Forces Group (Airborne) and served as a "training center" for ASA personnel assigned to other SODs overseas.

The present authorized ASA force structure was insufficient to support all divisions and independent brigades. This left ASA planners with the substantial task of standing up additional types of direct support units (DSU) and reorganizing existing ones to function in the Vietnam target environment. On 3 May, ASA activated the 404th ASA Detachment (Airborne Brigade) in support of the 173d Abn Brigade, the first of the ground combat elements selected for deployment. Personnel and equipment used in forming the 48-man detachment came from Company B, 313th ASA Battalion, stationed at Fort Campbell, Kentucky. On 9 June, the 404th ASA Detachment (temporarily designated Det 1, 3d RRU) arrived in Vietnam and was reunited with the 173d Abn Brigade at Bien Hoa. They would prove to be only the tip of the proverbial iceberg.

The 404th Detachment's compound lay near the Bien Hoa Air Base, 3 km southwest of the city and was composed of tents with wooden floors. Utilizing PRD–1s to provide fixes and conducting manual Morse intercept, teams from the detachment accompanied brigade forces on operations in the field. They also passed on targeting information received from ARDF aircraft and performed low-level voice intercept ("low-level" referred to the echelon of communications being targeted). Because only a handful of its members were jump qualified, the 404th was unable to support the 173d Abn Brigade in what would fortunately turn out to be the lone American parachute assault of the war.

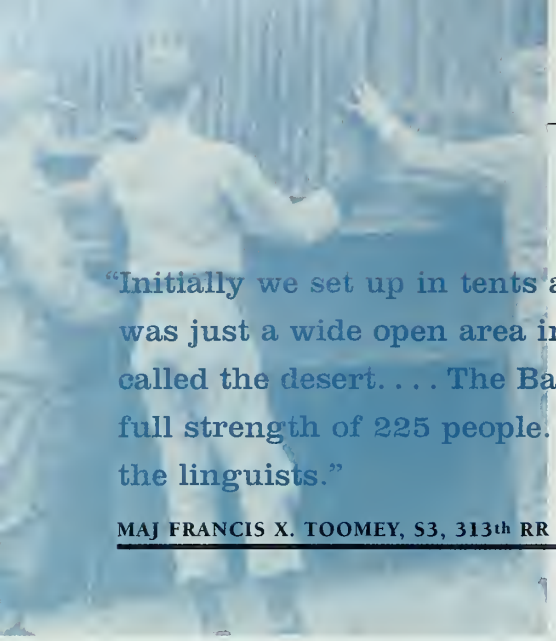
In March 1966, members of the 313th ASA Battalion at Fort Bragg, North Carolina, begin loading equipment—destination Vietnam.

Newly arrived ASA units faced more than the enemy. Weather also posed challenges to equipment and operations as shown here at the 407th RR Detachment compound.

Field Force, Vietnam

The deployment of combat divisions signaled the launching of a new strategy by GEN William C. Westmoreland, COMUSMACV, to defeat the enemy in a ground war. On 11 July 1965, the first elements of the 1st Inf Division arrived. The 1st Brigade, 101st Abn Division followed on 29 July, and the 1st Cav Division closed on An Khe in September. Each of the newly arriving divisions was given its own ASA direct support company, and the 1st Brigade, 101st Abn Division was assigned a detachment. The deployment of US combat units led to the creation of a provisional field force headquarters in the II Corps Tactical Zone (CTZ) on 1 August. As a stopgap measure aimed at providing liaison to the new field force, ASA activated a 29-man element, the 407th ASA Detachment at Nha Trang.

By 1966, the growing numbers of combat units and the launching of major ground operations necessitated greater command and control. In March, I Field Force, Vietnam (FFV) was established at Nha Trang and given operational control over US forces in the II CTZ. At the same time, the II FFV was organized at Bien Hoa in the III CTZ. These field forces were essentially corps-level organizations that also had responsibility for assisting and advising the South Vietnamese. Furthermore, the term "field force" avoided any confusion with the existing South Vietnamese corps tactical zones. Finally, the field force structure offered great flexibility in adding and subtracting combat elements as needed.

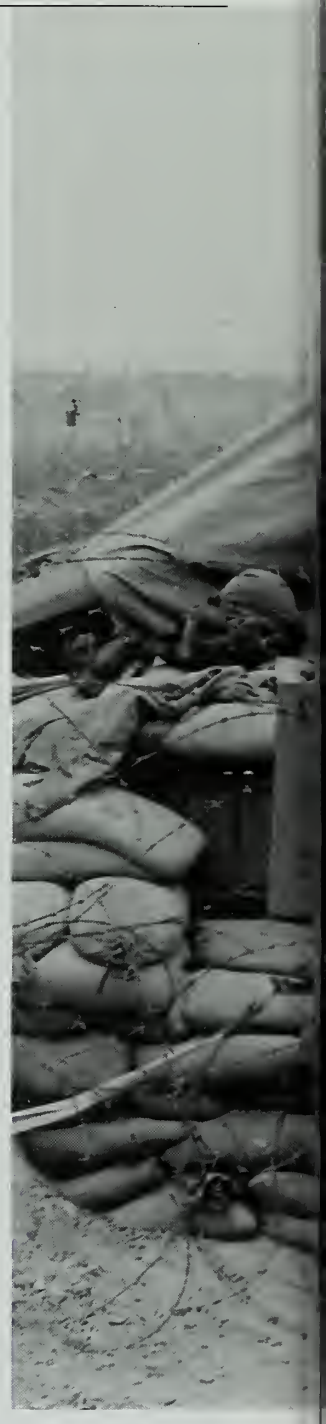


"Initially we set up in tents at Camp McDermott in Nha Trang and this was just a wide open area in the middle of a somewhat large open field, called the desert. . . . The Battalion Headquarters Company deployed at full strength of 225 people. The only thing that we were short of was the linguists."

MAJ FRANCIS X. TOOMEY, S3, 313th RR BN

In the March-April time period, the 303d and 313th ASA Battalions arrived in Vietnam to support the newly established field forces. The 313th ASA Battalion was collocated with the I FFV at Nha Trang, and the 303d ASA Battalion with the II FFV at Bien Hoa. While under the operational control of their respective field forces, the battalions were subordinated for administrative purposes to the 3d RRU, which remained the principal ASA headquarters in country. In turn, both battalions commanded direct support units that were allotted on the basis of one ASA company per division and one detachment per independent brigade or armored cavalry regiment. Eventually, each of the battalions also had an operations company assigned to it. These processing companies served as collection managers for the DSUs and played a key role in tasking airborne platforms and in issuing special and summary reports on SIGINT activity within their respective corps tactical zones.

Prior to the buildup of US forces, NSA had resisted any proposal that included deploying ASA tactical support elements to Southeast Asia. Rather, NSA believed fixed intercept sites such as Phu Bai and Saigon to be sufficient. However, the whole debate became moot when ASA direct support units began entering Vietnam as part of the Army's approved force structure. Experience would soon prove a need existed for both the mobile direct support units and fixed stations. The next debate would be over who exactly commanded the COMINT assets. The Army Security Agency's principal unit in country, initially the 3d RRU, maintained administrative control (personnel and logistical support) over all units; and doctrinally, direct support units were under the operational control of their respective tactical command. However, for the first time, fixed sites, such as Phu Bai, were within the war zone, and soon there would be aviation companies. Because these units were in support of theater-wide missions, COMUSMACV eventually took control.



Direct support units, such as Detachment A, 358th RR Company, operated near their parent tactical command.

Direct Support Units

The precedent of having units conducting COMINT/COMSEC in direct support of tactical elements dated back to World War II. During the Korean War, ASA took the practice a step further by adding groups and battalions to the force structure. In both conflicts, there were numerous examples where direct COMINT/COMSEC elements made a significant contribution to success on the battlefield. On the other hand, in World War II, the radio intelligence companies were overshadowed by the code-breaking effort at theater level that was guiding operational planning. During the Korean War, it was a matter of being too little, too late. The first direct support units did not arrive in Korea until late 1950, and another 6 months would pass before the war became stalemated to the point that they could begin making a real contribution.

In Vietnam, ASA's initial challenge would be to tailor each DSU to the tactical element being supported and to the existing signal environment of Southeast Asia. For example, ASA doctrine had not previously allotted DSUs to airborne brigades. This meant that detachments had to be carved out of existing units and given an entirely new organizational structure. ASA planners configured the new detachments at the lowest possible manning level, resulting in a 48-man unit structured to provide maximum mission support, but dependent upon

A soldier of the 265th RR Company copies traffic from inside a bunker. One survey showed that the direct support units were responsible for approximately 90 percent of the COMINT products received by the local commander. Almost all the rest would come from corps-level cryptologic resources.

"... I cannot overstate our case for the Direct Support Unit. COMINT from the DSUs is by far our most important source of intelligence. If DSU support were not available, the timeliness of this most perishable product would either be lost or degraded to a point where it might be useless."

LTG STANLEY R. LARSEN, CG, I FFV

the host command for logistics. Each of the airborne detachments possessed three positions for manual Morse, one devoted to voice intercept, and one for COMSEC monitoring.

The next challenge was to construct a DSU for an airmobile division. In CONUS, Company C, 313th ASA Battalion (10th RRU) had been in support of an infantry division. However, when selected for assignment to the 1st Cav Division (Airmobile), the company's authorized strength was cut almost in half and its operations subdivided into two parts. First, the company established a centralized manual Morse intercept and analytical effort that utilized R–392 receivers removed from ¼-ton vehicles, modified, and remounted on locally fabricated tables at the An Khe base camp. These operational positions were used to indirectly support the division as part of the larger on-going COMINT effort within the CTZ. The second half of the 10th RRU's operations consisted of three voice-intercept teams ready for immediate deployment with troops in the field. For battalion-size or larger operations, a mobile manual Morse position could be tapped to target enemy communications that couldn't be copied from An Khe. It soon became evident, however, that the 114-man company was simply too light. This eventually led to adding additional resources.

Company B, 313th ASA Battalion (11th RRU) exemplified the most common type of DSU, in support of an infantry division. The company originally consisted of a headquarters element with subordinate platoons designated for COMSEC, communications, and collection/jamming, but prior to deployment the unit was stripped of its EW, ELINT, and VHF intercept capacity, all of which had been designed for a European scenario. The revamped 168-man company supported battalion or larger size operations by receiving, processing, and recording ARDF results; conducting voice intercept; and manning three manual Morse intercept positions. The 11th RRU was also tasked with providing COMSEC assistance to the 1st Inf Division.

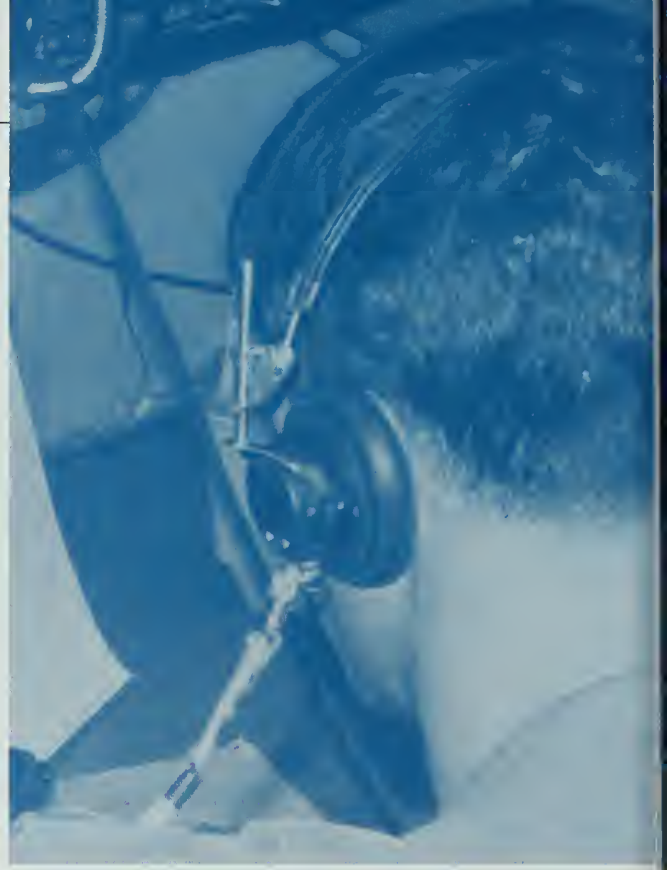
With weapons in hand, a 3d RRU crew prepares to board a U–6 "Beaver" aircraft at Tan Son Nhut Air Base on an early ARDF mission. (H. Jaffe)

Operation Starlight

The deployment of US combat forces led to new demands for ARDF support. During early 1965, seven additional U–8s were sent to Vietnam under Project SEVEN ROSES. This was followed by CHECK MATE, a procurement package for 17 more aircraft (7 U–6s and 10 U–8s). As US troops entered the ground phase of the war, ASA had a total of 30 aircraft on hand. To manage these new resources, the 3d RRU formed aviation detachments in each of the four corps tactical zones. An ARDF mission began with the J2, MACV sending a tasking message to either the operations officer at the 3d RRU in Saigon or to his counterpart at the 8th RRU (formerly Detachment J) at Phu Bai. They then would assemble the necessary technical background data needed by the operators and deploy the aircraft to satisfy the requirement. Upon completing their missions, the aviation detachments reported the ARDF fixes back to the 3d RRU or 8th RRU, where the information was sanitized and forwarded for tactical exploitation.

> **"The intelligence produced by your units was a clinching factor in the decision to launch this operation. Subsequent events confirmed the accuracy and timeliness of the intelligence produced by your units. . . . "**
>
> **LTG LEWIS WALT, CDR, III MARINE AMPHIBIOUS FORCE**

On 18 August 1965, US Marines launched the first large-scale American operation of the war on the basis of intelligence provided by the 3d RRU and 8th RRU. The combined air-sea-land attack entrapped a large portion of the 1st VC Regiment on a peninsula near Chu Lai, a hundred kilometers southeast of Da Nang. Although the Marines encountered heavy resistance and suffered losses of their own from an enemy who sought concealment in caves and tunnels and then attacked from behind,



STARLIGHT was considered a major success in the opening round of the expanded ground war. More than 600 of the enemy lay dead, and the American press treated the operation as a major victory. The operation was also notable because of the successful application of close tactical ARDF support. Staging from Phu Bai, 3d RRU platforms provided continuous fixes on the terminals of the 1st VC Regiment and its subordinate battalions. The information was then passed through the 8th RRU to the 3d Marine Division. These fixes reflected enemy locations and movements that permitted the Marines to make adjustments by bringing continued pressure to bear on the Viet Cong forces.

The success of Operation STARLIGHT led the Joint Chiefs of Staff to approve a third procurement package for 41 additional aircraft (Project WINE BOTTLE). The operation also greatly influenced COMUSMACV's decision in January 1966 to give priority to ARDF resources being used in a close tactical support role. ASA support units could in the future directly tip-off ARDF platforms that would then relay back fixes and target information. By using one-time pads to secure their communications, aircrews cut the delivery time from up to 24 hours down to approximately 3 hours. Soon Direct Support Units were receiving 85 percent of their fixes before the aircraft had landed. In October 1966, permission was granted for use of a different type of one-time pads that permitted transmission of information at the SECRET level. Despite these improvements, the one-time pads were still not considered user friendly and failed to allow for sufficient clarification.

As the use of ARDF in a direct support mode continued to evolve, there was still a demand for general search missions. In such instances, ARDF aircraft were used to help develop potential targets within a specific geographical area. Information regarding enemy transmitters was reported back to the direct support unit for follow up by ground collectors.

ARDF Coordination Center

In keeping with his decision to utilize ARDF for close tactical support, General Westmoreland indicated that a requirement existed for "150 U–6/U–8 ARDF aircraft or equivalent systems." The escalating demand for ARDF had a number of far-reaching consequences. For the first time, the US Air Force became a major player in ARDF in Vietnam. The Army and Air Force agreed among themselves that a need existed for both direct and general support types of ARDF platforms and that the Army should contribute 57 U–6/U–8s and the Air Force an equal number of C–47s. However, control of ARDF soon became a major concern. Were ARDF platforms cryptologic assets or were

"Everybody wanted those resources [ARDF aircraft] responsive to them, under their control. However, they were too valuable an asset to diffuse in that manner. I believed that we could get the best effect by concentrating or massing them, with Special Intelligence support in priority operational areas."

MG JOSEPH A. MCCHRISTIAN, J2 MACV

ARDF Coordination Center

Major General Joseph A. McChristian, J2 MACV, established a jointly-manned ARDF Coordination Center to task both Army and Air Force platforms.

they tactical systems? MG Charles J. Denholm, CG, USASA, urged GEN Creighton W. Abrams, Jr., Vice Chief of Staff, US Army, to support the position that ARDF was a "special platform" that could not be divorced from the total SIGINT system. However, the Joint Chiefs of Staff issued guidance that real-time responsiveness was the ultimate goal and that operational control of ARDF resources should be assigned to the overall military commander, in this case, COMUSMACV.

In the past, the scarcity of ARDF resources had been a mitigating factor against committing them to small-scale tactical situations. When MG Joseph A. McChristian became J2, MACV, he further tightened control of ARDF and also acted to end the tug-of-war between the Army and the Air Force as to who should be in the driver's seat when it came to tasking and coordinating ARDF missions. In June 1966, he established a jointly-manned ARDF Coordination Center (ACC) in Saigon. Although the Army (3d RRU) and Air Force (6994th Security Squadron) each retained control of its aircraft, the new center assumed responsibility for translating requirements from combat commanders into taskings once they were approved by the J2, MACV. Furthermore, the ACC monitored, evaluated, and reported the results of all ARDF missions.

At the working level, there was good rapport and cooperation between ASA and the USAF Security Service. Each made a unique contribution to the common goal of supporting the warfighter. Because the PHILLIS ANN platform did not require maneuvering to take a bearing and the size of the C–47 permitted a greater number of collection positions on board, the Air Force systems were much more productive than those of the Army. Initially, however, fixes taken by the Army platforms proved to be more accurate. Thus the ARDF Coordination Center tended to assign direct support missions, particularly those of a high priority, to the Army side of the shop and gave the Air Force responsibility for general search. It was the old question of quality versus quantity. Both were important. While Air Force platforms made rapid progress in the area of accuracy, ASA justified its mission by pointing out that its total cost (aircraft, fuel, maintenance, mission gear, personnel) per fix remained a fraction of that of its sister service.

"I have found the ASA soldier more resilient and...is better equipped to roll with the punches. Age and schooling are certainly factors in this. . . . We don't have major problems. If we do, the man losses his clearance and is transferred out. . . . "

MAJ DAVID J. WOEHR, CHAPLAIN, 509th RR GP

Main gate of the 509th RR Group at Davis Station. The group controlled widely dispersed ASA elements from the Delta to the DMZ. (A bandaged tiger cub served as the symbol of the 509th RR Group.)

The 509th Radio Research Group

In mid-1965, ASA's command and control in Vietnam was relatively simple. A total of 1,487 personnel were distributed among three units: the 3d RRU (606), the 7th RRU (54), and the 8th RRU (827). (The 3d RRU continued to serve as the command element.) But the next 9 months brought the arrival of direct support units and with them new challenges. Given no increase in personnel authorization or realignment of responsibilities, the commander of the 3d RRU had to now divide his attention between fulfilling his own operational mission and making sure that DSUs were meeting the needs of their combat commanders in the field. To resolve the command and control issue, ASA discontinued the 3d RRU on 1 June 1966 and redistributed its mission and resources among four new organizations. Headquarters, 509th Radio Research Group which assumed administrative control of ASA assets in Vietnam; a new Radio Research Communications Unit, Vietnam (RRCUV) that served as ASA's in-country communications center; and the 175th RR Company which took over the 3d RRU's collection and processing missions.

The fourth and final unit created was the 224th Avn Battalion (Radio Research). Activated on 1 June 1966, the battalion and its four subordinate aviation companies replaced the 3d RRU Aviation Branch and its four detachments. The 138th Avn Company (RR) was located at Da Nang; 144th Avn Company (RR) at Nha Trang;

146th Avn Company (RR) at Tan Son Nhut, Saigon; and the 156th Avn Company (RR) at Can Tho. In addition, the 144th Avn Company had platoons at An Khe and the Holloway Army Airfield at Pleiku, and the 138th Aviation Company had an element at Phu Bai.

By September 1966, the 509th RR Group had settled into a command structure that would remain virtually unaltered for the next 5 years. The group had under its direct control three battalions and a field station: the 303d and the 313th RR Battalions, which supported the field forces; the 224th Avn Battalion; and the 8th RRU (soon to be redesignated the 8th RR Field Station). In addition, the 509th commanded three smaller elements that performed countrywide missions. The 101st RR Company (formerly the 7th RRU) directed the 509th RR Group's COMSEC effort, and the RRCUV fulfilled ASA's unique communications requirements. The third and final unit, the 403d RR Special Operations Detachment, would soon arrive in country to provide direct support to the 5th Special Forces Group.

Aside from a small Processing, Analysis, and Reporting Branch, the 509th RR Group acted primarily as an administrative headquarters to provide overall supervision and support to the 20 to 30 ASA units that were further broken down into detachments and teams located at remote sites and fire support bases. At any given time more than a hundred such elements could be scattered throughout South Vietnam. Besides organizational fragmentation, there was the problem of continuous fluctuation as some DSU's moved from one corps tactical zone to another. Compounding all of this was the challenge of distance that separated the various elements from one another and the 509th Group. For instance, teams of the 407th RR Detachment operating along the DMZ were more than 500 miles away from Saigon.

The 403d RR SOD

In June 1966, the fragmented intelligence-gathering activities of the Special Forces in Vietnam took a significant step forward. Up to then, the Special Forces had made do by using internal resources to conduct intelligence-gathering at a basic level. The restructuring of intelligence within the Special Forces began with the arrival of a 110-man contingent equipped to provide counterintelligence, interrogation, and analytical assistance. The other half of the intelligence picture was completed in September when 51 soldiers of the 403d RR SOD deployed from Fort Bragg to conduct signals intelligence.

From the beginning, the 403d RR SOD faced the formidable task of supporting a Special Forces group whose assigned strength would eventually reach 3,500 personnel scattered among 85 different locations. Given its limited resources, the 403d RR SOD attempted to direct COMINT support to the lowest tactical level possible while maintaining maximum mobility and flexibility. By providing support

"Instead of waging guerrilla warfare against conventional forces in enemy territory, the US Special Forces troops were to find themselves attempting to thwart guerrilla insurgency in 'friendly' territory."

COL FRANCIS J. KELLY, AUTHOR *US ARMY SPECIAL FORCES, 1961–71*

ARDF tip-off and manual Morse positions being manned by members of the 403d RR SOD at Ban Me Thuot.

Like other direct support units, the 403d RR SOD was initially committed to establishing short range direction-finding nets.

on a mission-by-mission basis and by emphasizing analytical and reporting assistance, the unit would play a much larger role than indicated by its size. (The 403d RR SOD also gained some added resources by abandoning its COMSEC mission.)

Throughout its stay in Vietnam, the 403d RR SOD's Headquarters/Control Team was collocated with the 5th Special Forces headquarters at Nha Trang. Here, the special operations detachment performed limited analysis and integrated COMINT into the Special Forces' operational planning. The 403d RR SOD also exercised administrative control over its subordinate teams, but depended totally on the 5th Special Forces for all non-ASA logistics and transportation—an arrangement that proved highly satisfactory. Troop billeting conditions ranged from simple wooden structures to immense underground concrete bunkers, leaving most ASA teams situated only a short distance from their operational positions. Despite the remoteness of many of these locations, ASA believed that adequate security measures were in place to safeguard its sensitive mission from enemy attacks.

During its first year in Vietnam, the 403d RR SOD focused upon targets in the northern II CTZ area. From Kontum, which served as a major Special Forces base, the 403d RR SOD manned manual Morse intercept and ARDF tip-off positions, deployed direction-finding/voice intercept teams, ran the local DF net, and performed second and third echelon maintenance. When tasked, the Kontum element could also deploy a small intercept team in support of mobile operations. Normally, low-level voice intercept teams consisted of two or three linguists, but the 403d arrived with only one soldier proficient in Vietnamese. To help new linguists recognize commonly used words and phrases, the detachment obtained voice tapes from the 330th RR Company. The benefit was immediate. On a number of occasions when high-priority support for strike forces was required, the 403d obtained linguists on loan from nearby ASA units. For some time, the Special Forces had hired local villagers since their proven loyalty was often greater to their US employers than to the Saigon government. Following suit, the 403d began utilizing indigenous personnel who proved particularly adept at understanding local Viet Cong transmissions and regularly predicted impending enemy attacks, locations of their units, and on occasion, operational plans.

The intercept vans parked in a row represented the consolidation of resources at the 175th RR Company, CMA for the III CTZ.

"The CMA is the focal point of COMINT operations in the battalion. Allocation of all cases was controlled by the CMA, who had complete authority on allocation of cases to all intercept units throughout the battalion."

LTC NORMAN J. CAMPBELL, CDR, 303d RR BN

Collection Management Authorities

When the 3d RRU was discontinued in June 1966, its operational mission was transferred to the newly organized 175th RR Company. With only 275 authorized spaces, the company was a third the size of the 8th RRU. National authorities proposed that the resources of the 175th RR Company be expanded, but in a counter proposal, ASA successfully argued for the deployment of the 330th RR Company, a processing support unit with a manning level of 350 spaces. This would save having to build up the existing facilities in Saigon and Phu Bai, and by basing the 330th RR Company at Pleiku, it would fill a gap in coverage of targets. Strategically locating each of the three processing elements in a different tactical zone also solved the problem of how to effectively manage the growing number of cryptologic resources in Vietnam. Initially, the 330th RR Company was named Collection Management Authority (CMA) for the II Corps Tactical Zone, and the 175th RR Company as CMA for the III Corps Tactical Zone. The 8th RRU would eventually serve as CMA for the northern tier of provinces, and a fourth and final CMA (335th RR Company) was created in the Delta region (IV CTZ).

On paper, the processing companies were to have been used solely in support of the direct support units. However, from the beginning, they shed all pretense of being mobile and assumed the role of fixed sites. Acting as mini field stations in a war zone, the CMA's were responsive to the theater commander General William C. Westmoreland. In contrast to the direct support units, the CMAs performed in-depth processing. They also directed intercept coverage and responded to special consumer

needs, such as performing area analysis. The CMAs issued a series of intelligence and after-action reports and provided technical "feedback" to the DSUs located within their corps tactical zone. In addition, analytical personnel from the CMAs often conducted on-site visits to the DSUs to provide technical assistance. With their own designated communications, the CMAs also served as a switchboard for information being exchanged up and down the SIGINT chain of command.

The CMAs were the glue that allowed ASA to successfully fulfill its mission in Vietnam. By effectively managing the SIGINT resources, the CMAs ensured that the larger interests of the field forces, MACV, and the cryptologic community were satisfied. By exercising targeting authority and providing technical support, they also enhanced the value of the DSUs' support to the tactical commander. Divisions and brigades quickly came to the realization that they could not effectively task their DSUs. A 1967 survey found that only two DSUs were actually utilizing more than 30 percent of their intercept positions in a direct support mode. The remaining units were being tasked by the CMAs. This intercept was fed into the larger SIGINT system that could then indirectly benefit the commander in the field. The Collection Management Authorities also played a critical role in deploying ARDF platforms. In coordination with the ARDF Coordination Center, they helped validate targets, select the type of aircraft needed for a mission, and determine time-over-target.

"COMSEC in Vietnam, among US forces, is terrible, absolutely deplorable—horrible—it practically doesn't exist. . . . Pilots gave coordinates, flight times, targets under attack, mentioned locations of supported Allied units in the clear. . . . Most of the Army divisions were little better."

MAJ EDWIN M. MORRISON, SECURITY OFFICER, G2, I FFV

The Transmission Security Problem

Transmission security had been a problem within US forces since the advent of the telephone and radio. Vietnam was no exception. The biggest obstacle that communications security had to overcome was human nature. Too few communicators actually believed that "Charlie" was listening—although it was common knowledge that the enemy possessed captured US radios. Captured enemy documents indicated that South Vietnamese communications were an important source of information, and prisoners of war revealed that the Viet Cong and NVA forces were regularly eavesdropping. In one instance, an interrogated prisoner reported seeing a group of 8 Chinese on several different occasions carrying radios. When he queried his platoon leader as to their purpose, he was told that they were "Chinese comrades who have come to help us, they speak Vietnamese, English, and Cambodian, and they listen to the radios they carry to let us know what the Americans and Vietnamese troops plan to do."

The advent of rapid moving airmobile warfare only compounded the problem of transmission security. Many commanders in the field reasoned that even if the enemy were listening, they simply could not react quickly enough to take advantage of the situation. One of the division commanders put it this way: "With regard to COMSEC, I had to choose between communicating freely in voice to enable rapid deployment and reaction or losing timeliness of tactical communications and movement through applying full COMSEC measures. I took the risk of COMSEC weaknesses in voice communications to develop the most rapid possible reactions…with our mobility, the enemy could not keep up with the speed of our tactical action and reaction…." This tension between the need for security and the need for timely communications would remain as long as US combat forces were engaged in Vietnam.

Many communicators falsely reasoned that the mobile nature of the war negated the need for COMSEC. (National Archives)

Captured documents and interrogation of prisoners revealed that the enemy was listening.

Transmission security also faced the challenge of convincing communicators that their "homemade" codes lacked security. (The origin of some of these codes could be traced back to the American Expeditionary Forces in World War I.) On one occasion, COMSEC personnel from the 303d RR Battalion demonstrated the inherent weakness of an unauthorized point-of-origin code being used by the long-range reconnaissance patrols of the 9th Inf Division. (Point-of-origin codes were used to relay locations by referencing a position from points left or right and up or down, usually in increments of 1,000 meters.) In a briefing to the division commander, a COMSEC specialist from the 303d illustrated that the improvised code being used by one of his patrols could be broken in less than 4 minutes.

During Operation SILVER BAYONET, the 1st Cav Division and ARVN forces launched a pursuit operation against two regiments of the North Vietnamese 325th Division. While the operation was in process, the 101st RR Company monitored the 1st Cav Division's communications. The study revealed a high rate of disclosures of communications frequencies, operational plans, and intelligence information. The end result was a decision by the Joint Chiefs of Staff to ship all available voice encryption devices to Vietnam to help stem the tide of COMSEC violations.

"We were monitoring . . . a transportation battalion. . . . The conversation included the time they would leave, how many people they needed, where they were going, and the fact that the troops would conduct a sweep of the area on the way back to Camp Enari. Any analyst could figure what time the B–52 raid would take place."

CPT CONRAD P. SKANTZ, LEADER, 2d PLT, 101st RR CO

A COMSEC specialist from the 303d RR Battalion monitors US communications for security violations. The direct support units brought their own COMSEC assets.

A Failed Solution

The arrival of ASA's direct support units greatly expanded the number of available COMSEC resources. Each of the two battalions was authorized 2 officers and 26 enlisted personnel and up to four positions for COMSEC monitoring purposes. In addition to supporting the field force headquarters, the battalions also oversaw the COMSEC activities of their subordinate companies and detachments. Each company was allotted 19 personnel and from two to five COMSEC positions. However, detachments could contribute only four soldiers and one position to security. All DSU's were responsible for preparing a COMSEC plan for their commander's approval, and most often, it was the emphasis of the commander that spelled the difference between a successful COMSEC program and failure.

Throughout the war, the 101st RR Company (formerly the 7th RRU) remained the principal proponent of Army COMSEC within Vietnam. The company interfaced with J2, MACV, on security policy matters and exercised technical control over ASA's COMSEC mission. From Saigon, the 101st RR Company directed cells based at Da Nang, Pleiku, Long Binh, and Can Tho. These teams were responsible for

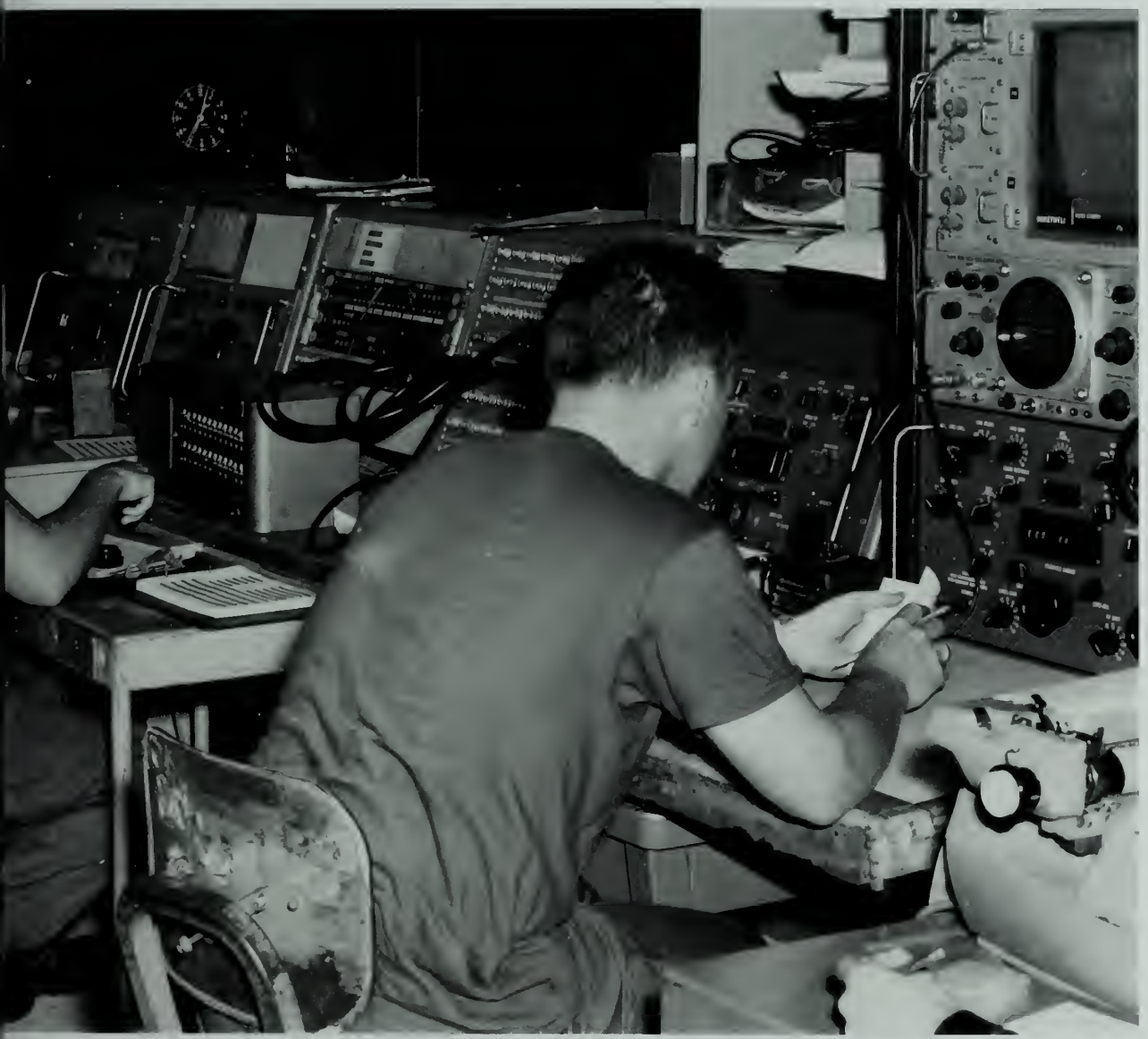
monitoring and analyzing MACV communications as well as conducting training in security procedures. They also briefed South Vietnamese forces in the use of cryptosystems on loan to them by the United States.

ASA elements were capable of monitoring only 6 percent of the Army's communications in Vietnam. Furthermore, approximately two-thirds of the effort was targeted against one source—the radiotelephone. This meant that only a relatively small percentage of actual communications violations could be identified. By focusing on procedures, monitors often failed to address the larger issue of exactly how much intelligence could be gained by enemy analysts from all communications sources, both classified and unclassified. Although COMSEC monitoring did not solve the security problem, it did lead to rethinking the issue. In 1966, evidence arose that the enemy was receiving warnings of pending B–52 strikes and that friendly communications might be the weak link. To confirm these suspicions, the 509th RR Group committed a large portion of its COMSEC resources to studying the problem. The findings concluded that it was possible for the enemy to obtain advance notice, determine the general location of a raid, and once the operation was underway, identify a specific target. During one of the monitored calls, the parties even acknowledged that the information being discussed was classified, but continued to converse anyway.

COMSEC personnel also played a limited role in electronic warfare that included deception operations. Imitative communication deception (actual intrusion into an enemy's communications network) was never attempted in Vietnam, but from time-to-time, manipulative communication deception was employed with mixed results. Manipulative deception was the use of one's own communications to deceive the enemy. Already involved in monitoring and performing analysis of friendly communications, COMSEC specialists were tasked with providing technical assistance to deception operations. However, actual cases of electronic deception were few in number and restricted to small-scale operations.

"The fact that the RFP positions continued to operate at all was simply due to good coordination between personnel at the various stations. If somebody had something the other guy didn't have, he'd loan it to him or give it to him. This, of course, didn't always work because everybody ran out from time to time."

CWO–3 RICHARD W. FOOTE, SIT SECTION, 509th RR GP



A member of the 175th RR Company mans a radio fingerprinting position on the right.

Fingerprints and Landlines

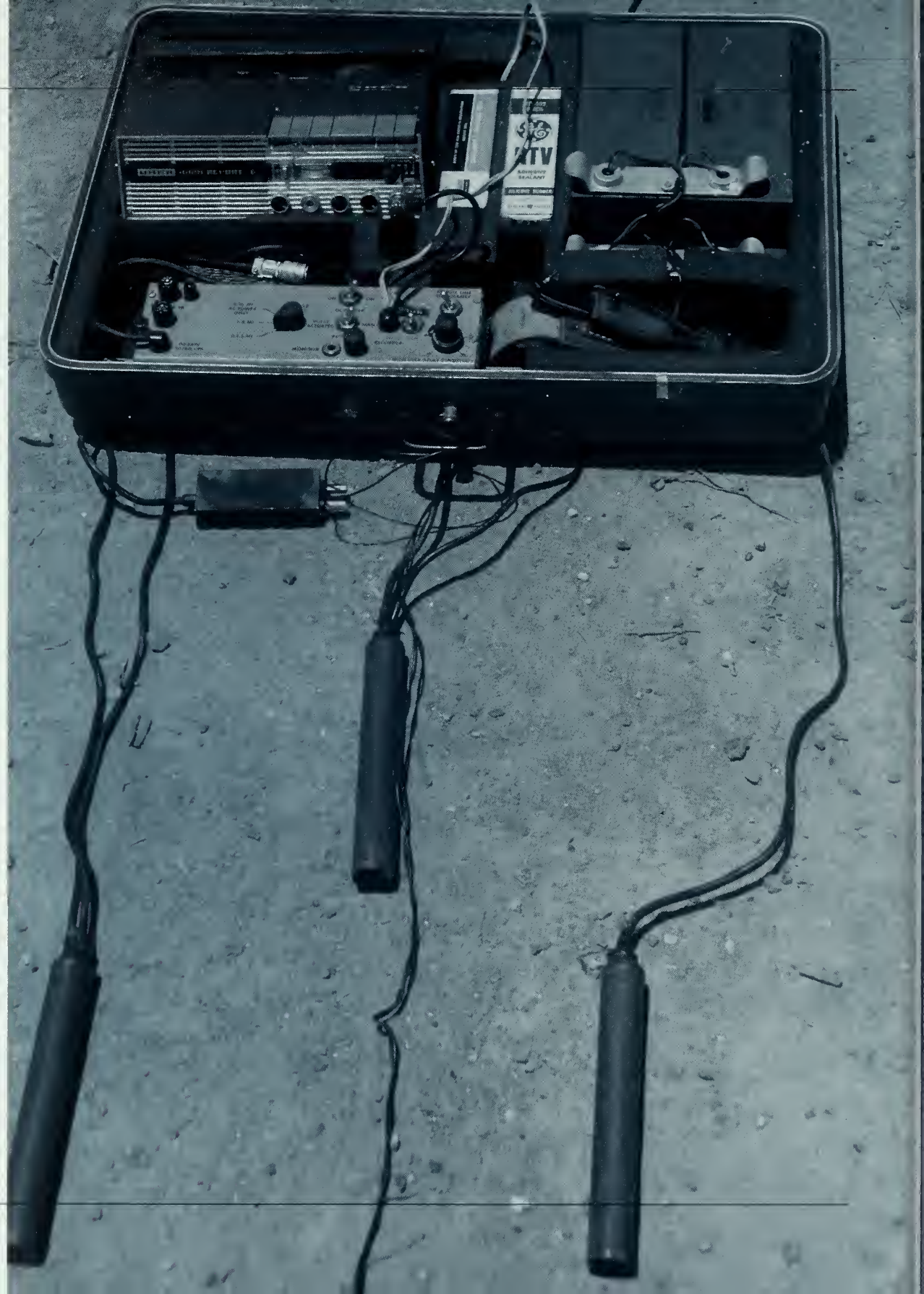
While in Vietnam, ASA found itself engaged in a number of minor projects that consumed a disproportionate amount of its energies. One of the diversions was radio fingerprinting (RFP). First used in World War II, radio fingerprinting involved recording of characteristics (such as power and frequency variations) of an intercepted signal in order to identify a specific radio transmitter. An oscilloscope converted a signal into a visual format that could then be captured on film. To make this happen, the intercepted signals had to be of sufficient strength. Furthermore, an experienced operator was needed to interpret the results. What many did not fully grasp was that radio fingerprinting was never meant to stand alone, but rather to be used in conjunction with other identification tools. RFP was far from an exacting methodology, and in Vietnam, it would face added challenges.

In 1962, less than a year after arriving in Vietnam, ASA decided to deploy an AFSAV–37 radio fingerprinter to its Saigon intercept site. Twelve months later, a second piece of equipment arrived at Phu Bai. Together, these systems covered targets in the Delta and the northern provinces, but had significant problems identifying low-powered transmitters being used by the enemy in central Vietnam. More than 10 years old, the AFSAV–37 began to quickly show its age. A hostile environment of

dust, humidity, and heat was taking its toll on the sensitive equipment, and atmospheric interference and the presence of weak signals further reduced RFP's effectiveness. Mounting repair problems soon convinced ASA that a new generation of equipment was a necessity.

Landline intercept was another mission that demanded an expenditure of a disproportionate amount of energies and resources on the part of ASA. The targeting of landlines dated to the Civil War, when both the North and South frequently tapped telegraph lines for the purpose of intelligence gathering. During World War I, opponents monitored radiotelephone lines that ran among the intricate trench systems that bordered "no-man's-land." However, the lack of a stable front in World War II furnished the US Army with few opportunities. In the summer of 1951, the Korean War, like World War I, had become stalemated along the 38th Parallel, leading ASA to revive the technology. For example, a landline-monitoring site was established on "Heartbreak Ridge."

Given this historical background, ASA naturally began searching for possible targets in Vietnam. In March 1966, a small team made up of personnel from the 3d RRU and the 400th ASA SOD explored the feasibility of ground return intercept at several widely dispersed locations. The equipment consisted of two UHER–4000 battery powered tape recorders,



One of a number of landline kits sent to Vietnam in an attempt to provide smaller, more user-friendly equipment.

battery powered special-purpose amplifiers, and 3-foot brass ground stakes. Although no Viet Cong telephone conversations were recorded, the team did bring back a number of important lessons learned. It was impossible to deploy such a system under the cover of darkness, and any future operations would have to be conducted in remote areas. At the same time, ASA operations personnel expressed serious reservations as to whether or not information gained from such intercept would ever outweigh the risks of exposing installation teams to enemy attack.

Mobile DF

In 1965, short-range direction-finding (SRDF) received renewed emphasis with the arrival of ASA's direct support units, all of which possessed PRD–1s. At the height of the war, the DSUs had some 36 PRD–1 teams organized into local direction-finding nets. Each substation searched for a signal or was tipped off by the control station. After locating a signal, the PRD–1 operator took a bearing, recorded it on the azimuth scale disk, and then passed the information to net control by using radio and one-time pads for security. Control then plotted all the bearings and retransmitted the "cuts" (two intersecting bearings) or fixes to its immediate headquarters where an "SRDF Spot Report' was released electronically to all DSUs within the respective corps tactical zone.

Many of the same problems that had handicapped SRDF in the early days in Vietnam continued to plague the effort. Weighing over 50 pounds, the PRD–1 was far from portable. This led to attempts to make the system more mobile. Under Operation MASHER/ WHITEWING in early 1966, PRD–1 teams were airlifted from place to place in a "leap-frog" fashion, hoping to pinpoint the target. Later, there was even an attempt to operate SRDF teams from inside helicopters. In the end, however, these efforts demonstrated more ingenuity than they did long-term solutions. Tactical commanders could not expend the personnel needed to protect SRDF teams so they were often relegated to firebases. This often led to the base line (distance between the extreme outstations) being longer than the desired 6 to 10 km. Keeping the SRDF teams in the rear also altered their mission. Instead of serving as a target acquisition tool, they supplemented other systems, such as PPS–4 personnel detectors, in providing force protection. Furthermore, the signal environment that existed around firebases often proved a hindrance to the SRDF mission. These outposts

Given adequate protection, PRD–1 operators, such as this one from the 303d RR Battalion, could target enemy transmitters.

"To begin with I had to instruct them on how to operate this DF. We used 05H's as the operators on DF and they would look at the equipment and say 'what's this.' We would have to tell them that is a DF set."

SP5 DUANE M. GAGNON, DET 1, 16th RRU

had more than their share of radiating and reflecting materiel such as antennas, concertina wire, vehicles, and shell casings.

The constant movement of the PRD–1s between sites was a leading cause of equipment outage, and the lack of air transportation only exacerbated the problem. In one instance, members of the 403d RR SOD were forced to rely upon elephants for transport. The age of the equipment placed added strain on a logistical system that could not maintain an adequate supply of parts, such as vacuum tubes. This led to cannibalization of existing PRD–1s, further reducing the number on hand. However, the lack of qualified operators was the final nail in the coffin. On the basis of its early experience with SRDF in Vietnam, ASA eventually relegated most of their PRD–1s to supporting intercept operations. In the process, school-trained, direction-finding specialists (05D) were replaced by manual Morse operators (05H) who possessed only on-the-job training and lacked the essential skills.

DANCERS and Small Steps

The only joint training conducted at the SABERTOOTH facility between 1965 and 1967 was a class on conversational English, taught in hope of promoting increased communications and leading to better understanding between the ARVN and US SIGINT personnel. By 1966, the 509th RR Group had given up on jointly manning the WHITEBIRCH DF net with the South Vietnamese, having failed to convince Unit 15 (COMINT) personnel of the necessity to perform such elementary tasks as preventative maintenance, continuously manning their positions, and responding to all DF flashes. The situation deteriorated to the point that if a US advisor was not present, ARVN operators would literally walk away from their DF positions, consequently no credence could be placed in line bearings being received from an ARVN outstation. However, ASA leadership would be unsuccessful in its efforts to extricate the command from having any future involvement with the WHITEBIRCH net.

Although the Vietnamese failed to achieve the necessary proficiency in direction-finding, they did contribute in other ways. The lack of qualified linguists led US cryptologists to turn to the use of native Vietnamese—Project DANCER. In 1964, the 3d RRU received permission for the first time to use locals, but it was not until June 1965 that equipment was actually in place for the program to be implemented. ARVN

"There is a definite need for more DANCER personnel. Because they are native they do a better and more rapid job than our people. Their transcriptions of...low-level voice were consistently superior."

CWO–4 WILLIAM R. MACDONALD, 175th RR CO

South Vietnamese linguists or DANCERS would become invaluable assets for ASA's voice intercept mission.

DANCERS were to be assigned to ASA elements, and civilian DANCERS employed at the South Vietnamese SIGINT center in Saigon. ASA would provide the ARVN linguists with tapes of plain text Vietnamese voice intercept for transcription along with the necessary technical data such as call signs, with which to accomplish their tasks. However, the project proceeded at a much slower pace than originally envisioned. During the first 3 months of 1966, DANCERS processed some 923 tapes of voice intercept, but only 11 were identified as being enemy communications. By 1967, DANCERS numbered 22, of which 12 were at the 8th RR Field Station. Many of the early DANCERS lacked basic grammar skills and suffered from low morale because they experienced feelings of isolation and discrimination at the hands of their US hosts.

Since its inception in 1961, the South Vietnamese COMSEC organization, the 1st Radio Control Company (known as Unit 16), lagged behind its sister communications intelligence organization (Unit 15). In October 1965, Unit 16 restructured itself into a headquarters element and four mobile platoons; one for each of the corps tactical zones, thus mirroring the 101st RR Company. Although for the first time the unit possessed all the equipment necessary to monitor the Republic of Vietnam Armed Forces communications, serious shortcomings persisted. Many of the South Vietnamese COMSEC personnel still did not know what actually even constituted a transmission violation. Few had adequate typing skills, and if they did, they didn't have access to typewriters, leaving copying to be done by hand. And even if a security violation was identified, the finding lost all relevance after making its way through a cumbersome reporting system. To make matters worse, ARVN units viewed Unit 16 as a sort of a "communications police" because officers committing violations received fines, while enlisted personnel could be reduced in rank, all of which did not encourage cooperation.

A soldier from Unit 16 monitors ARVN communications fo security violations.

"As a division commander, SI was the one kind of intelligence that would actually and always cause me to move elements or maneuver units based on it. Anytime a significant movement of an enemy regiment in the operational area was reported, I made corresponding immediate movements, based on such intelligence."

MG WILLIAM E. DEPUY, CG, 1st INF DIV

ASA personnel entered and exited Vietnam through either the 509th in Saigon or the 8th Field Station at Phu Bai. (Pictured is the processing center at the Saint-George Hotel in Saigon.)

Manual Morse intercept positions dominated ASA's effort in Vietnam. (The manual Morse bay of the 328th RR Company.)

A low-level voice intercept team in the field.

The Headquarters Building of the 224th Avn Battalion is shown in the left foreground; the 509th RR Group's headquarters is across the street with overhang.

In the aftermath of the enemy's Tet 68 offensive, support for US involvement in Vietnam waned, eventually leading to the exit of US forces from Vietnam. (National Archives)

NEW BATTLES 1968 1970

"I recall COL Faulk, my G2, in talking to me about it afterwards said that this group asked him, 'What were major intelligence failures?' He told them that he didn't really know what the intelligence failures were, but he simply hoped that next time he would have as much intelligence. . . . "

LTG FREDERICK C. WEYLAND, CG, II FFV

Beginning the night of 30 January 1968 and into the next morning, a combined force of approximately 84,000 Viet Cong and North Vietnamese troops launched a coordinated attack country-wide during the traditional holiday period surrounding the lunar new year—Tet. Besides the capital of Saigon, the enemy mounted over 100 assaults against provincial capitals, autonomous cities, and district capitals. Although the Allies defeated the enemy in the field, Tet 68 proved to be the watershed event of the war. It led to the disenchantment of the Nation's decision-makers, US news media, and eventually the American people themselves. Support for the war would soon begin to wane, ultimately leading to the withdrawal of US forces.

The intelligence failure of Tet 68 resulted from J2, MACV's underestimating the enemy's strength in South Vietnam and miscalculating how the war was progressing. The rate of infiltration down the Ho Chi Minh Trail was a key factor in determining the order of battle. MACV had come to rely on SIGINT as the basis for its analysis of the flow of men and materiel, but only after the information was confirmed by interrogations of prisoners, debriefings of defectors, and exploitation of captured documents. This took time, creating an information gap. Still COMINT was able to provide ample warning of the Tet buildup. On 30 December 1967, pattern analysis found enemy forces to be generally well away from populated centers with some along South Vietnam's border. (In pattern analysis, dots on a chart were used to represent fixed enemy radio terminals or other information indicators of unit locations. Over time, these began to suggest possible courses of action.) By 15 January, a movement to the more populated areas was underway, "like iron filings being attracted to a magnet," and on the eve of the attack, analysis showed the enemy encircling the major population centers. Based on this information, Allied forces were placed on full alert for the night of 30 January. What COMINT did not show was the scope, fury, and nature of the attack. Two prime targets, Saigon and the city of Hué, were heretofore untouched by the war. The possibility of a rocket attack was not unthinkable, but the prospects of a ground assault were believed slim. When the enemy employed messengers and maneuvered on prearranged plans, COMINT was blind. It could not reveal what the enemy did not choose to transmit.

ASA units were not immune from the fighting. On 31 January, several companies of VC, backed by mortars, launched an all-out assault on the Vietnamese Joint General Staff Compound housing the 509th RR Group's operations. Enemy soldiers penetrated the compound's defensive perimeters and came within 100 meters of the WHITEBIRCH Building before being killed or turned back. Landline cables belonging to the RR Communications Unit at Tan Son Nhut were severed, delaying the dissemination of SIGINT products. On 18 February, rocket fire hit Tan Son Nhut Air Base, wounding some 25 ASA soldiers. At Phu Bai, a rocket attack destroyed a portion of the trailer complex and damaged several buildings and antennas belonging to the field station.

One of the great stories that emerged from Tet was the awarding of the Legion of Merit to Edward W. Minnock, Jr., a 19-year-old private whose intercept team was isolated near Tuy Hoa City. After analyzing the in-coming intercept, Minnock formulated a plan to thwart an enemy attack against the city and sold the local combat commander on a successful counter-offensive maneuver.

The Army outfitted a Navy P2–V "Neptune" aircraft as an electronic warfare platform (CRAZY CAT/CEFLIEN LION).

"Then he [General Westmoreland] asked a question. 'Well, what do you think about jamming the enemy up in Khe Sanh, if we have to?' I told him from the way I looked at the enemy's communications. . . that when they were on the offense, they had very little need for communications, per se."

COL WILLIAM T. RILEY, JR. CDR, 509th RR GROUP

A ¾-ton mounted MLQ–24 jammer. Like the rest of ASA's electronic warfare resources in Vietnam, it remained silent.

Electronic Warfare

ASA was responsible for the Army's EW mission. However, a judgement call was made early in the war that intelligence derived from COMINT far outweighed any possible short-term benefits of denying the enemy his ability to communicate. Apart from a handful of isolated exceptions, this policy was never altered. One such exception occurred in late 1965 when the 5th Special Forces Group reported that the enemy planned to broadcast a message in the area of Pleiku with the intent of inciting local Montegnard tribesmen serving with the Civilian Irregular Defense Group. After obtaining clearance from the US Embassy, GEN Westmoreland, COMUSMACV, directed the 3d RRU to jam the broadcast. By simultaneously using transmitters located at Nha Trang and Pleiku, ASA jammers successfully overrode the foreign voice signal.

That same year, the US Pacific Command sponsored an electronic warfare conference to outline a strategy to disrupt the communications of low-level Viet Cong targets. One of the recommendations was for the Army to deploy an EW platform. The Joint Chiefs of Staff approved, assigning ASA the responsibility for fielding Project CRAZY CAT (later renamed CEFLIEN LION). However, no existing Army aircraft could sustain the weight and size of the AN/MLQ–29 countermeasure systems being proposed, causing ASA to turn to the Navy's RP–2E "Neptune." In continuous operation

since 1945, the Neptune was used for maritime patrol missions and had even set a non-refueling long distance record of 11,000 miles. Its ability to stay aloft for 14 hours at a time made it particularly attractive for use as an EW platform. Because the aircraft was the only one of its kind within the Army's inventory, the five CEFLIEN LION platforms required specially trained pilots and a unique logistical support system.

The 1st RR Company (Avn) was activated for the sole purpose of performing the CEFLIEN LION mission, but when the company arrived in Vietnam in June 1967, it immediately ran into strong opposition. The most vociferous objection to jamming came from the J6, MACV, who feared the enemy would retaliate by launching attacks against US communications sites or that jamming would "slop-over" and disrupt friendly comms. Members of the cryptologic community also expressed concerns that jamming would jeopardize the exploitation of enemy targets. Only the strong interest shown by GEN Westmoreland, COMUSMACV, kept the project alive.

The closest the CEFLIEN LION platforms ever came to deploying in an electronic warfare mode was during the Battle of Khe Sanh. In early 1968, NVA/VC forces attempted to wrestle the northern province of Quang Tri from the control of the Allies. As the intensity of the battle increased, GEN Westmoreland called together several advisors to discuss the possibility of jamming the communications of enemy forward observers. However, those who had argued against such a course of action in the past prevailed once again. In 1968, the 509th RR Group needlessly updated its inventory of ground based jammers by adding four AN/MLQ–29 sets. Like the systems they replaced, the MLQ–29s sat in storage where they continued to gather dust along with their operational plans.

Airborne Collection

The Army's first attempt at airborne intercept in Vietnam was short-lived. In January 1966 ASA deployed an SSQV–6 system housed within a "Caribou" CV–2B: a twin-engine, medium tactical transport aircraft capable of carrying as many as 32 passengers. Besides its lift capacity, ASA engineers were attracted to the aircraft's ability to cruise for over 5 hours at a speed of 135 knots. Nicknamed PATHFINDER, the platform had space for 4 HF/VHF intercept and search positions plus a HF direction-finding capability. The project was terminated early when an agreement was reached between the Army and the Air Force that all medium-size transport aircraft, including the CV–2B, be transferred to the latter. Although PATHFINDER failed to demonstrate that it was the final answer, airborne collection did show enough promise to merit further exploration.

The next attempt involved a U–1A "Otter," a single-engine, light tactical-transport aircraft that could carry up to two crew members and 2,000 pounds of cargo. The first of the platforms, nicknamed CAFÉ GIRL, arrived in Vietnam in March 1967. CAFÉ GIRL utilized the standard dipole-antenna configuration and the AN/ARD–15 direction finder, but also came equipped with manual Morse search. The next two U–1As, nicknamed LAFFING OTTER, represented an upgraded CAFÉ GIRL and were primarily employed in a collection mode with an auxiliary ARDF capacity. On 12 February 1969, hostile fire downed a LAFFING OTTER approximately 1.5 miles inside Cambodia. US rescue attempts were aborted when a firefight broke out between the crew of the Otter and nearby enemy forces. Following their capture, the crew.was fortunately turned over to Cambodian authorities. When US officials finally had the opportunity to debrief the released ASA soldiers, they were relieved to learn that all documents and equipment had been destroyed and that security had not been compromised.

The U–1As provided ASA with its first successful airborne collection platform in Vietnam.

Aboard a LAFFING OTTER, an ASA operator turns the dials to begin copying.

"During my recent visit to South Vietnam I observed and was told by our senior commanders that COMINT, primarily airborne direction finding and airborne intercept, is providing 80 to 85 percent of the intelligence used in planning and operations against the Communist Forces in South Vietnam . . . "

FINN J. LARSEN, DEPUTY DIRECTOR, DOD (DDRE)

In April 1968, MACV directed ASA to deploy its five CEFLIEN LION platforms in a collection mode. Designed for communications jamming, the CEFLIEN LION system also had the capability to gather COMINT in both the VHF and HF range. (One had to collect signals before one could target them for jamming.) Operational plans were drafted to use the platforms against the ongoing infiltration of enemy personnel, supplies, and equipment into South Vietnam. In its new role, CEFLIEN LION would emerge as the Army's most prolific airborne collector. For all intents and purposes, CEFLIEN LION was an extension of the 8th RR Field Station at Phu Bai. After receiving daily briefs on pending B–52 strikes in the area of operations, the crew of the P–2E aircraft would take off at 0400 hours from Cam Ranh Bay and head north along the coast before turning west in the vicinity of Phu Bai/Hué. Following the DMZ, the plane completed a long arching orbit. Whatever information operators could transcribe was immediately passed to the 8th RR Field Station for processing and distribution to consumers. Five to eight hours later, the aircraft landed at Da Nang for refueling. Here, soldiers from the 8th waited to courier the day's intercept back to Phu Bai. The crew then departed for home by retracing their earlier flight pattern south along the coastline to Cam Ranh Bay.

Housed in a UH–1D helicopter, the LEFT BANK system operated in direct support of the local commander.

LEFT BANK/ LAFFING EAGLE

LEFT BANK was unique among ASA's airborne systems. First of all, it was housed in a UH–1D helicopter, not a fixed-wing aircraft. More importantly, LEFT BANK represented a joint effort between ASA units that packaged the systems and the supported divisions that furnished the choppers. In the summer of 1967, the 1st Cav Division provided three "Hueys" along with pilots, while its direct support unit, the 371st RR Company, contributed operators and systems. (The 4th Inf Division and the 374th RR Company worked out a similar arrangement.) LEFT BANK was also one of a kind in that it came under the direct operational control and tasking of the division commander. Initially designed as a complete direct support package in the HF spectrum, LEFT BANK contained an AN/ARQ–27 direction-finding system, an RO–278 radio fingerprinting position (RFP), and a voice recorder. One operator reported losing the RFP film out the chopper's open door and having to hang upside down on the helicopter's skids to retrieve the classified material resting on the top of the jungle canopy. Within 2 years of becoming operational, the finger printer was eliminated altogether because of erroneous readings caused by excessive vibrations. Its removal actually enhanced the platform's overall effectiveness by simplifying operations and allowing the intercept position to be used solely in support of direction-finding.

"... the LEFT BANK went out, obtained a target, and then became a small command center in the sky directing the attack. In fact, the Cav became so reliant on this technique that when the LEFT BANK was no longer available their effectiveness was severely hampered."

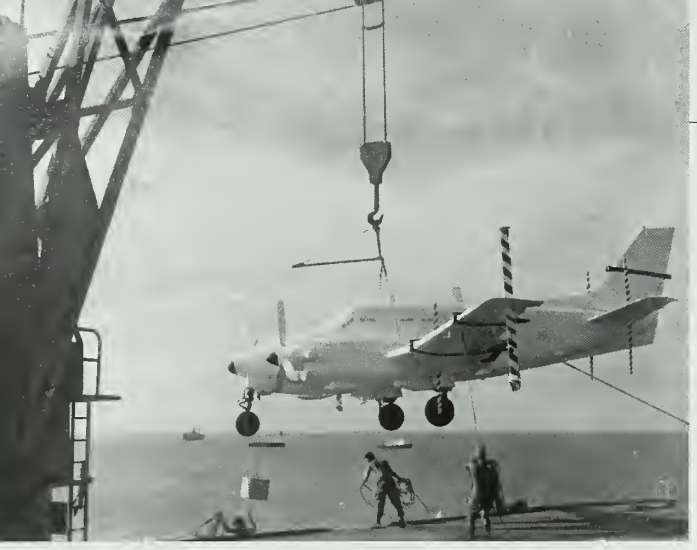
LTC DONALD E. GRANT, CDR 303d RR BN

What allowed LEFT BANK to achieve its full potential was the development of a concept of operations that integrated the platform with the firepower and mobility of airborne warfare. After a LEFT BANK pilot called in a fix, an observation chopper worked the area at tree level for evidence of movement, trail use, or bunkers. If personnel were spotted, a gunship rolled in, and troops possibly inserted. In 1969, two platforms of the 4th Inf Division flew some 315 missions (1,215 hours); the average radius of the 438 fixes was even smaller than that of fixed wing platforms. In the month of January alone, LEFTBANK was responsible for six B–52 strikes, firing of 1,200 rounds of artillery, and insertion of troops that accounted for 300 of the enemy being killed. However, LEFT BANK missions experienced their share of risks. ASA suffered the loss of two crews when enemy fire downed their helicopters.

In December 1968, ASA deployed the first of its 16 U–21D "Ute" aircraft. The LAFFING EAGLE platforms were designed to perform both direction-finding and airborne collection, but delays in the development of the AN/ARD–23 (V–Scan) DF system forced the platform to be employed initially for VHF voice and HF manual Morse intercept. The LAFFING EAGLE possessed the capability to record low-level voice intercept on tape which could then be passed rapidly by courier to the local collection management authority or by secure voice to a direct support unit. The aircraft could also pass on targeting data to nearby ARDF platforms.

LAFFING EAGLE gave ASA its most efficient collection platform. The U–21D was a smaller, newer, less complex, and mechanically superior aircraft to the CEFLIEN LION P–2E. (The U–21 also demonstrated greater flexibility because CEFLIEN LION had to deploy close to its logistical base.) LAFFING EAGLE was credited with intercepting elements of the NVA 1st Division and their plans for an attack on 22 February—the launch date of the 69 Tet Offensive. LAFFING EAGLE was also the first airborne system to successfully target the low-powered voice transmitters employed by the Viet Cong in the southern delta and hill country.

The radio fingerprinting and voice positions were eventually eliminated from the LEFTBANK platform in favor of improved ARDF.



The arrival of the U–21D LAFFING EAGLE platforms in late 1968 represented an important milestone for ASA in its development of airborne collection and direction-finding.

"Previously we had to land after flying all the way back to Saigon and then send the data over the wire. It was passed through channels to Bien Hoa Base and they had to get it out to the tactical commander. In the new system, using COMUS pads, we could pass the information directly to the ASA direct support unit with the 173d."

SFC MICHAEL R. CUMM, NCOIC PROCESSING SECTION, 3d RRU

Manpower/Navigation/ Communications

Pilots played an important role in intelligence collection. The quality of an ARDF fix depended upon accurately determining the position of the aircraft. Before each mission, pilots received a pre-brief in which they were given the location where the target was last fixed along with other operational details. It was important that they overfly the proper area at the correct time. ARDF training for pilots was originally conducted at the USASA Training Center and School, Fort Devens, Massachusetts, until eventually being transferred to Fort Huachuca, Arizona, to take advantage of better weather conditions and improved on-site maintenance. During the war's peak years, ASA graduated approximately 170 pilots annually from the course.

Initially, visual contact with ground features proved adequate, but cloud cover, darkness, and the lack of distinguishable landmarks precluded total dependence on this method. In 1964, U–8 platforms began to arrive equipped with Doppler navigational radar. Eventually, the Canadian Marconi Doppler (AS/ASN–64) became standard equipment on U–8s, the P–2Es (CEFLIEN LION), and the U–1As (LAFFING OTTER). The Doppler not only turned the aircraft into an all-weather system, but made it possible for the platform to be flown at a higher altitude, thus extending its intercept range. The Doppler also reduced the time a pilot spent continuously following the aircraft's position on a map. But adoption of the Doppler had its drawbacks: the copilot was required to systematically update the system; Doppler errors voided as many as a third of the intercepts; and breakdown of the radar proved to be the number one cause of aborted missions.

Besides navigation, ARDF became increasingly dependent upon the need for secure communications. When an enemy transmitter was on the air for only a few minutes, rapid communications was more than a luxury; it was essential. The ultimate solution lay in the introduction of voice encryption equipment—the TSEC/KY–28 in late 1966. With encrypted voice, delivery time to a supported commander dropped from hours down to as little as 6 minutes. At the same time, overall mission productivity rose because secured voice allowed for clarification of the downloaded information.

Despite these improvements, communication problems remained. Mountainous regions could prohibit tip-off procedures altogether, and the airwaves also became increasingly congested. Ground-to-ground communications, ground-to-air tip-offs, and air-to-ground reporting often occurred on the same frequency, making it difficult to sort out the tip-offs. Within the III CTZ alone, ARDF platforms could simultaneously receive tip-offs from as many as 16 different intercept sites because ground flash stations often could not hear each other's transmissions. Pilots frequently reacted to the incessant verbiage by turning their sets off until they could again stand to put up with the chatter. To help alleviate the problem, the ARDF Coordination Center eventually assigned priorities to different types of traffic and in 1969 resorted to allotting separate flash and reporting frequencies.

Using captured radios, the VC/NVA regularly tried to jam Allies' communications and to enter their nets.

An Unofficial War

From time to time ASA operators engaged in unofficial electronic warfare. To keep a target communicating, individual operators would sometimes temporarily jam an enemy's signal. This caused the targeted transmitter to try and communicate again. In one instance an ASA team working off the USS Benewah, on the Mekong River, obtained permission to undertake sustained jamming. By keeping the enemy broadcasting, the intelligence specialists successfully followed the movements of the headquarters communications element back and forth across the Mekong River until all of its members were either captured or killed by waiting Navy river patrol boats.

If the US Army was reluctant to use EW as a weapon, the enemy was not. To conduct jamming, the only thing the enemy needed to possess was compatible equipment such as

"The only time we let him communicate was when one of our ARDF birds was in the air. . . . We would get an ARDF fix and thirty seconds later here comes gunships. . . . So when he tried to get across [the Mekong], all the patrol boats up river and all the patrol boats down river converged. We got . . . all their radio operators except for one which was killed. . . . "

SFC JAMES W. WOOD, JR. LIAISON TO IV CORPS

Aboard the USS Benewah, an ASA team practiced limited electronic warfare against enemy units operating along the Mekong River.

captured radios and to be in close proximity to the intended target. Enemy operators employed whistling, keying, scratching the mike, or playing Armed Forces Vietnam Network radio programs. One captured document listed the following simple guidelines for VC operators: "When jamming, play with dials, whistle, make noise or simulate sounds if possible, but do not talk."

The enemy also engaged in communications deception by entering Allied communications nets and broadcasting messages in hope that the subterfuge would not be detected. The NVA/VC was known to have successfully used American, Australian, and Spanish accents for the purposes of deception. One US unit reported six such intrusions within a week's time. Typically, the enemy intruders tried to redirect artillery fire and medical evacuations or to order Allied forces to withdraw or to cease fire.

On 6 January 1968, ABC News cameras captured for its nightly broadcast a case of enemy intrusion. Elements of the 9th Inf Division and the 2d Brigade, 25th Inf Division, were engaged in a firefight with VC/NVA forces within 10 miles of the Cambodian border when an intruder, identifying himself as Australian, entered one of the command nets. He urgently requested artillery fire to be shifted as rounds were impacting in his area. In a display of poor COMSEC, US personnel made no attempt to authenticate and continued to converse with the unidentified station. Eventually, the would-be deceiver withdrew from the net once he sensed that the other side had grown suspicious.

The best protection against the enemy's electronic warfare and signals intelligence was simply good COMSEC—the use of proper radio procedures and exercise of discipline within the communications net. Against jamming, a radio operator could employ such countermeasures as relocating his reception site so as to lessen the effect of the incoming jamming signal, ceasing broadcasting altogether, or changing frequencies. Attempting to broadcast on a different frequency was to be used only as a last resort since a jammer could easily find the new signal.

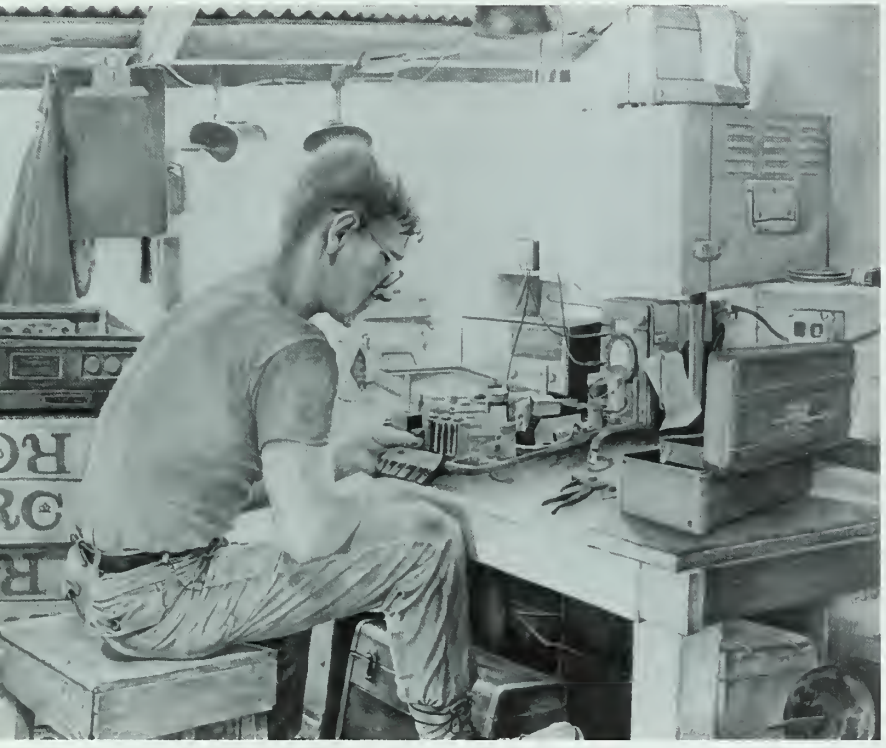
SHORT SKIRT/CAFÉ BLEW

In 1966, a new radio-fingerprinting (RFP) system, Project SHORT SKIRT (later renamed LAFAIRE KNEE), was deployed as replacement equipment at each of the CMAs: the 8th RR Field Station, the 175th RR Company, and the 330th RR Company. The RO–278 worked on the principal of recording an analog picture of the targeted signal on light-sensitive paper. Operators could then develop the image by simply exposing the paper to low intensity ultraviolet light, such as a florescent lamp. The use of paper eliminated the need for chemicals in film processing and permitted multiple copies to be forwarded to different RFP libraries. Despite the advantages of convenience and ease of operation, the RO–278 presented its share of challenges. Unwanted characteristics showed up in the recordings that were eventually traced to improper grounding of

"The value in the radio-fingerprinting system is that it is self-contained within one station. . . . without taking the time that is required for MRDF shots throughout the country to locate entities that have disappeared for a time."

CPT JAY M. WALDMAN, OP OFF, 335th RR COMPANY

the equipment. The quality of the light-sensitive paper was poor and reached the 50-percent degradation point within an hour of having been developed. But the greatest challenge to RFP remained one of management. How to utilize a handful of RFP positions against an unlimited number of targets? Sometimes the collection management authorities placed emphasis on quality of shots; other times the emphasis was on quantity. Maintenance of RFP libraries was also a major concern. One library might contain as many as 10,000 individual shots that required constant screening.



When it came to PRD–1s, good maintenance was critical as shown in this piece of combat art.
(Charcoal by SP4 Wayne A. Salge, member of the 509th RR Group)

Short-range direction-finding remained in Vietnam much longer than the ASA leadership had anticipated. Commanders in the field were reluctant to turn loose assets that they owned and believed were helping to pinpoint enemy troops in their local area of operation. However, cuts and fixes on targets that could not be verified through analysis were of questionable value and could even lead to serious consequences. For example, one commander used SRDF teams as flank protection during combat operations. Another deployed the PRD–1s in defense of his base camp, thereby committing more troops to combat actions. Some of the blame could be attributed to the direct support units themselves who too often lacked a clear understanding as to how to correctly utilize the equipment.

One of the earliest attempts at improving SRDF was an effort to field a manpack, hand-held system to be used by the 403d RR SOD. However, field tests by the detachment revealed major shortcomings in each of the systems, such as the lack of a built-in compass in the RTCV–7A radio receiver that possessed an AT–249 homing antenna. The next piece of equipment to be tested was the PE–484 system, which demonstrated sufficient accuracy, but proved inadequate for the task at hand. It lacked the necessary ruggedness, possessed only limited range, and proved difficult to repair.

In 1968, ASA made a last-ditch attempt to field a system that would solve the SRDF problem once and for all. CAFÉ BLEW was a new mobile direction-finding system designed to provide line bearings on HF and VHF signals, to differentiate between sky and ground waves, and to allow for antennas to be remoted up to 700 feet away. However, test results in Vietnam quickly revealed that CAFÉ BLEW fell far short of expectations. Consequently, in March 1969, MG Denholm, CG USASA, directed the removal of CAFÉ BLEW equipment and ordered, that in the future, PRD–1s no longer be used in a direct support mode. SRDF's.legacy in Vietnam would be that its failure had led to the development of ARDF.

Engaged in long-range reconnaissance patrol, MAC–SOG soldiers and their South Vietnamese counterparts were regular practitioners of landline intercept. (A. Berg)

Circus Act

The 509th RR Group served as a coordination center for landline intercept activities in Vietnam. Under Project CIRCUS ACT, the group assumed responsibility for processing and reporting information gained from intercept, conducting training, and whenever security was not a consideration, engaging in the actual setup. Priority was given to training reconnaissance elements such as Special Forces, long-range patrols, Navy SEALS, and

Marine amphibious assault groups, but any tactical unit could request assistance. Compromise of COMINT was not believed to be a problem as long as non-indoctrinated personnel were the only ones performing the line tap.

The Military Assistance Command-Studies and Observation Group (MAC–SOG) was a joint service, unconventional warfare task force engaged in long-range reconnaissance patrols throughout the region. Because MAC–SOG personnel operated in remote areas, it was believed they would be ideal candidates to intercept landline circuits. In October 1966, a MAC–SOG team successfully spliced an enemy landline and attached a monitor, but the operation failed to yield any meaningful intelligence. However, the never-ending demand to expand the intelligence base in Vietnam would continue to drive future experimentation with landline intercept.

Specifically designed for use in Vietnam, the VITACK XR4–100 kit system could be deployed in different modes, including parallel induction and wire splicing. Furthermore, the equipment could be left buried for 7 to 10 days for landlines located in remote areas. The drawback was it resembled a two-piece luggage set and weighed 54 pounds. The 403d RR SOD first tested the VITACK XR4–100 in 1968. During the initial phase of the operation, the US/ARVN team was discovered, and a firefight ensued. Several of the team members were wounded and an enemy soldier killed. It was obvious that what was needed was lighter, less cumbersome equipment and a method for conducting a pre-test to determine if a line was actually active. The 403d RR SODs next tested the XR4–100A, a replacement system, half the size of the original equipment. On the first three attempts, the team had to withdraw under fire even before reaching its target.

"The majority of all wire sightings reported has been in Northern I Corps Tactical Zone which is the area under XXIV Corps control. . . ."

MAJ DAVID B. MULLAN, USAF, NSA PROJECT OFFICER

During its fourth deployment, while in the process of locating the wire, the team was observed and engaged by an enemy platoon. Two members of the team were killed, a 403d RR SOD soldier wounded, and the equipment wound up being destroyed in place to keep it from falling into enemy hands.

For a number of years, Special Forces had attempted to sample landlines with home-made inductive monitoring devices, no larger than a package of cigarettes. Although no documented evidence existed to prove any of these efforts actually bore fruit, the idea of an effective, hand-held device remained popular. In December 1968, NSA engineers finally gave the Special Forces what they had been asking for—the XR–114A, a system weighing 5 pounds that was voice activated and capable of recording up to 2 hours. A year later ASA deployed the XR4–100D surveillance system, which offered even broader applications. This newest piece of equipment came with radio relay and remote command activation capabilities. But despite these technical advances, the J2 MACV's command emphasis, and the 509th Group's attempts to reenergize CIRCUS ACT, success continued to elude the landline program.

Advice and Assistance

Each of the direct support units possessed internal resources to perform COMSEC monitoring, but it was becoming increasingly evident that monitoring by itself was an ineffective means of preventing transmission security violations. During Project COVERALL, the 101st RR Company tried to revitalize the program by monitoring only similar units at the same time so as to present a more accurate transmission security picture, but the time lapse before a follow-up session could be accomplished negated any benefit. (The 101st RR Company alone had responsibility for 142 units.)

By the mid-Sixties, a change in the direction of COMSEC was emanating from the National Security Agency and was slowly working its way throughout the rest of the cryptologic community. The new approach emphasized advice and assistance. The assumption was that if people knew what to do, they would do it. Communicators already recognized the need for safe-guarding information; they just had to be informed of the nature of the threat, given reasonable means to effect security, and shown how. More importantly, the fear associated with the policeman role of COMSEC monitoring did not prevent violations; it actually hindered good security practices.

The security poster at the 328th RR Company was a reminder that ASA could and did monitor all types of communications.

"The efforts of the COMSEC Advice and Assistance Team caused more improvement within these two divisions in a few weeks than the many previous months of communications monitoring. . . ."

US ARMY, VIETNAM MESSAGE, DATED AUGUST 1968

The National Security Agency at Fort George G. Meade, Maryland, was the primary proponent of the new emphasis on advice and assistance. (National Security Agency)

However, advice and assistance was not just a top-down drill. Initiatives also came from below. In February 1968, a team of COMSEC officers from the 303d RR Battalion traveled around the III CTZ to determine the security awareness among US units in the aftermath of the 68 Tet Offensive. They concluded a need existed for a COMSEC Advice and Assistance Team (CAAT) to present classes, to implement security measures, and to work with local COMSEC specialists to improve their skills. Elsewhere, the 313th RR Battalion kicked off Project CORRECT (COMSEC Role Recast) throughout the II CTZ. A letter of introduction from the Chief of Staff, I FFV, preceded an assistance visit by CORRECT team members. Once on the ground, they conducted COMSEC awareness classes, followed 3-4 weeks later by a monitoring team that evaluated a unit's progress.

The road leading from an emphasis on monitoring to focusing on education was not always a smooth one. COMSEC personnel often shifted back to monitoring and analysis because that was what a local commander desired most. Other commanders wanted COMSEC resources assigned on a permanent basis, not just showing up periodically. Some in the COMSEC business believed that even advice and assistance did not go far enough. Operations security, where all types of threats were evaluated, was what was really called for. But perhaps the greatest hindrance to change was the shortage of COMSEC specialists skilled as educators. COMSEC personnel had to know the tactical environment, local communications networks, and the organization of the supported command. By the time a COMSEC specialist acquired the know-how, his tour of duty was up. It would take longer than the US Army's stay in Vietnam for the COMSEC advice and assistance program to become a reality.

"In general, I've seen no great development in COMSEC status since World War II. Although there have been improvements in COMSEC equipment, there is a practical limit to the amount of COMSEC equipment that we need or which can be carried by the combat soldier. In Vietnam, the use of even the KY–38 was not practicable for manpack on the soldier in active combat."

MG JOHN R. DEANE, JR., CG, 173d ABN BDE

A member of the 371st RR Company utilizes a bank of secure voice equipment to tip off a LEFT BANK platform.

Secure Voice

Captured documents revealed that enemy COMINT personnel concentrated on exploiting unauthorized codes and plain text. There was no evidence the enemy ever successfully attacked approved enciphered systems and methods. That is not to say the enemy might not have had success when communicators employed improper procedures, such as when plain text was mixed within an encoded message. In 1968, the 101st RR Company conducted a survey that revealed tactical battalions were employing unauthorized codes 90 percent of the time when passing locations of friendly units over radiotelephone nets. COMSEC specialists even speculated that transmissions in the clear were preferable over "homemade" codes. At least the sender would not be lulled into a false sense of security.

Early in the war, one-time crypto pads where each page was destroyed as it was used were in wide use, but the sheer numbers required proved a significant burden. In 1967, the KAC codes were widely distributed for use at the lower echelons. However, the vocabulary of the General Purpose Codes (KAC–P and KAC–Q) was not always adequate for all types of units. To correct this deficiency, codes were designed upon request for units with special vocabulary. (For instance, artillery units used the KAC–184.) The reception of these specialty codes was generally favorable. In the words of one artillery officer, "It is the first decent code I have seen produced for artillery. Most of the time we get a modified infantry code that doesn't fit our needs."

However, talk persisted among Army communicators that the KAC codes were not convenient. For instance, having to use pencil and paper at night, in the rain, or under actual combat conditions was considered prohibitive, but upon investigation these criticisms proved largely without merit or highly exaggerated. Pilots complained that the vibration of their helicopters made the KAC hard to read. Because this had never been an issue elsewhere, one COMSEC officer commented tongue-in-cheek that "the air currents found in Vietnam must be significantly different." COMSEC personnel were also quick to point out that the often chosen alternatives to the KAC—unauthorized, home-made codes used to encrypt and decrypt coordinates—did not actually save any time. To address the perceived shortcomings of the KAC, COMSEC authorities next issued a wheel code, the CIRCE, which was considered more user-friendly.

Since the Army had become dependent upon voice communications, secure voice equipment was seen as the ultimate answer to transmission security. In 1964, production of the Nestor series of enciphered voice communications (KY–8 vehicular mounted, KY–28 aircraft, and KY–38 manpack) was begun, but over a year passed before the KY–8/38 reached Vietnam in sufficient numbers, and even then few existed below battalion level. The Nestor equipment was sensitive to humidity and heat, and aircraft carrying KY–28s required frequent refitting. However, most of the problems involved the KY–38 because of its weight and bulkiness. The initial solution was to divide the communications gear, connected by a cable between two soldiers. During combat, the weakness of such an arrangement was obvious.

Touchdown

Prior to the deployment of US Forces to South Vietnam, the enemy had concentrated his intercept activities on Vietnamese Air Force and Government communications. However, in 1965 there was a decided shift in priorities. The VC/NVA communications intelligence effort began an intensive training program to produce the requisite number of English linguists to exploit US communications. Through interrogation reports and captured enemy documents, it was known that the VC/NVA was primarily targeting plain language and brevity coded voice communications. It was also commonly known that the enemy was exploiting low-level codes, both authorized and unauthorized. What was not known was exactly how successful they had been. This would change with the capture of an enemy COMINT unit.

On 20 December 1969, in response to a fix provided by a US Air Force ARDF platform, elements of the 1st Inf Division captured a VC/NVA radio intercept unit 3 km north of Ben Luc, in the III CTZ, near the division's base camp at Lai Khe. A South Vietnamese scout noticed a whip radio antenna affixed to a tree limb with a wire leading down into a "spider hole." Having been discovered, an enemy soldier threw out a hand grenade and was quickly killed. However, his comrades were talked into surrendering. Follow-up interrogations revealed the element to be the Technical Reconnaissance Unit A–3, a radio intercept cell of the Military Intelligence Section, Military Affairs Branch, Sub-Region 1. Individual members included the unit commander, one voice (Vietnamese) intercept operator, two voice (English) intercept operators, five manual Morse intercept operators, two manual Morse analysts, and one female nurse. Their dead companion had served as the team's senior analyst.

TAREX (target exploitation) personnel from the 509th RR Group were assigned the task of processing the captured documents and equipment. The TAREX effort was a small one. It consisted of a group of highly skilled human intelligence specialists who had already served a tour with ASA in Vietnam and who were proficient in the Vietnamese language and familiar with the target environment. Based out of Saigon, TAREX teams regularly performed liaison with Allied tactical units and the joint intelligence exploitation centers in search of information or captured materiel that might assist ASA in its mission.

The two captured AN/PRC–25 receivers were evidence that the enemy intercept cell possessed the capability of intercepting US tactical units. The R–139 Chinese manufactured receiver could also target radios in the AN/GRC series, and even the homemade

"This work is really rather startling; the attention to detail, complete accuracy, and thorough professionalism is amazing. These guys are reading our mail and everyone will be informed that they are."

GEN CREIGHTON W. ABRAMS, COMUSMACV

Wires leading out of a spider hole led to the capture of an NVA communications intelligence team.

receivers were compatible with some US communications gear. The enemy unit also possessed seven Sony radios and one Panasonic receiver with which it could exploit virtually all nonsecure communications emanating from US/ARVN tactical units. Captured documents revealed listings of frequency and call-sign allocations by unit, still others gave extensive instructions on proper intercept techniques, and one even told how to break point-of-origin codes. In the 4–5 weeks prior to its capture, the team had intercepted over 2,000 US unencrypted transmissions and had screened them for possible indicators. Couriers then carried the material to a division-level headquarters located approximately a mile away. Here, further evaluation was made of the traffic, and the results sent by radio or courier to nearby tactical elements.

The capture of an enemy SIGINT unit verified what COMSEC specialists already knew—the enemy was listening.

The 175th RR Company's processing and reporting section concentrated on getting out intelligence products.

"Compartmentalization detracted most from maximum USASA mission accomplishment. . . special clearances which, in turn, contributed to the problem of getting the intelligence to the user—the tactical commander at the lower echelons—was a definite disadvantage toward maximum mission accomplishment."

COL WILLIAM E. BURR, II, G2, XXIV CORPS

Processing Information

ASA believed that if there was a deficiency in its support to the tactical commander, it lay in the area of analysis. The overall value of the product provided the commander was believed to be good, but could use improvement. In 1967, the 509th RR Group leadership proposed that a 265-man processing company be created. Its purpose would be to coordinate, manage, and analyze results countrywide and not be restricted to a specific corps tactical zone. In-depth, interpretive analysis and reporting could be performed without jeopardizing the near-real-time mission of the direct support units. Owing to its close proximity to MACV, the processing company could also help fuse collateral and SIGINT information, something that was not being done by the collection management authorities.

Believing the existing system to be more than adequate, NSA initially resisted the proposal. However, in the aftermath of the 68 Tet Offensive, the J2, MACV, directed that the 509th RR Group organize a 30-man Processing, Analysis, and Reporting (PAR) Branch. One of its first assignments was to study unidentified radio terminals appearing on established networks. In the coming months, personnel TDY from units in theater further augmented the branch, but the branch never realized the vision that ASA had originally planned.

For SIGINT information to be useful to combat commanders, it had to be timely, but "timely" meant different things to different people. Some commanders accepted a reasonable delay between the time information was intercepted and when it was in their hands. Others felt that any delay was unacceptable. In response, ASA

introduced the Tactical Report (TACREP). The TACREP was in addition to Spot Reports, Electrograms, and Summary Reports and was designed to pass sensitive information directly to military commanders on a real-time basis. One survey in 1967 revealed that 81 percent of TACREPs was reaching the supported commanders via its direct support unit within 30 minutes of intercept.

Although established guidelines existed for the dissemination of SIGINT, the implementation of those procedures varied widely from unit to unit. In most instances, the process depended upon the relationship between the DSU commander and the G2, the working style of the Special Security Officer (SSO), and the past exposure of the combat commander to SIGINT. (Established in World War II, the Special Security system was responsible for handling special intelligence and came under the control of the theater commander, in this case COMUSMACV.) For example, one DSU commander reported an excellent relationship between himself, the local SSO, and the G2. Priority information was delivered directly to the G2 or his staff. In contrast, an SSO at another headquarters insisted on reviewing all information, thereby creating a delay in the reporting process. Dissemination was also hindered by the lack of personnel cleared for special intelligence (SI). Over time, combat divisions requested and received approval for indoctrination of three-times the original allotment, but the number of personnel seldom exceeded 25. Even then, commanders at battalion level were never cleared, requiring information to be sanitized, a process that again cost valuable time. The substitution of the term "usually reliable source" for SIGINT was normally a sufficient indicator for a commander to take action, but if he had not experienced past successes, there might be some hesitation. Battalion commanders also sometimes did not respond simply because of human nature. Sanitized SIGINT was simply not as "exciting" as the real thing.

A forward deployed SSO shelter containing crypto equipment and classified documents being relocated from LZ Two Bits in support of the 1st Cav.

SSG Hall of the 403d RR SOD receives the Bronze Star with Valor. He along with SSG James M. Alward and SP5 Donald C. Childs, II were decorated for their part in the defense of Duc Lap in August 1968.

Expanding Support

Lacking many of the capabilities of a company-size direct support unit, the 403d RR SOD required close coordination with a major processing element. The 330th RR Company at Pleiku served as the collection management authority for the II CTZ, the 403d's primary area of operations. Consequently the detachment found it invaluable to place a small team of analysts with the 330th to assist in transcribing and processing intercepted traffic. By this means, the 403d also received much needed technical aids (such as frequencies, call signs, and last known location of enemy units) along with guidance in assigning target priorities. To provide similar support to its ARDF tip off and low-level voice intercept teams being deployed outside of the II CTZ, the 403d RR SOD ended up installing analysts at the other three collection management authorities. (However, the bulk of the 403d RR SOD analysts remained collocated with the 330th RR Company.) In 1969, the 403d RR SOD upgraded its analytical efforts by establishing briefing and correlation teams with the Special Forces command and control elements within each of the CTZs. Their purpose was to meld COMINT into the overall intelligence picture for the Special Forces.

Analysts from the 403d RR SOD continuously monitored all ARDF fixes received by the CMAs for indications of enemy buildup or movement that could possibly endanger Special Forces camps or operations. The results were sanitized and issued in the form of Special Agent Reports (SPAR) as part of general intelligence reporting, but if a specific detachment faced an immediate threat, analysts would pass the information directly to the unit involved. Prior to deployment of Special Forces elements, the 403d briefing teams prepared current intelligence studies and an order of battle on NVA/VC units active in the area of operations. These studies included ARDF locations of all identified and unidentified terminals over the previous 60–90 day period.

Communications were particularly important to the 403d RR SOD. The lack of secure comms impacted the timeliness in which information was inputted, analysis made, and intelligence distributed. The 403d took advantage of circuits belonging to the various CMAs to communicate between the detachment's headquarters and its analytical elements. In the field, elements located at Special Forces bases used one-time pads until 1967 when they received KY–8 crypto systems. Low-level voice intercept and ARDF tip-off teams deployed with Strike Forces were also

Operations hut occupied by a forward deployed team from the 403d RR SOD.

"... ASA personnel of the 403d SOD remained at the base camp and made direct contact with the aircraft [LAFFING EAGLES] and passed fixes immediately to the camp commander. As a result, we absolutely flattened the enemy, drove his forces out of the area, and declared the battle of Bu Prang an ARVN victory. ..."

1LT JARVIS E. WILLIAMS, LIAISON OFFICER, G2 SECTION, HQ, I FFV

outfitted with the bulky KY–38 man-pack version. Altogether, these improvements in secure communications greatly aided passing of information to airborne platforms and providing fixes to the local commanders.

While the 403d RR SOD's soldiers were trained intelligence specialists, they also served as members of the Special Forces and, as such, were often subjected to many of the same dangers. Over a 2-year period, the 403d RR SOD suffered some 22 wounded and 1 killed as a result of providing close support. For instance, 403d RR SOD soldiers were part of a 12-man Special Forces team located at Duc Lap, a remote camp situated 3 miles from the Cambodian border near an infiltration route. In August 1968, the enemy launched 3 days and 2 nights of unrelenting mortar and rocket fire coupled with human-wave attacks against the outpost. ASA soldiers fought alongside other members of the team as they defended the base and helped lead local Montagnards in counterattacks.

The Cambodian Incursion

Perhaps no single operation better illustrated the full extent of ASA's support during the Vietnam War than the incursion of Allied troops into Cambodia in the spring of 1970. Prior to the conception of the campaign, ASA units had assembled a wealth of technical data on VC/NVA entities in the border area. This proved essential to the campaign's success. On 28 April, officers from the 371st RR Company accompanied MG Elvy B. Roberts, Commander, 1st Cav Division, his G2, and the SSO to brief LTG Michael S. Davison and staff at HQ, II FFV. A density plot of ARDF fixes accumulated by ASA elements over the previous 6-month period served to orient the axis of the Allied advance into the "Fish Hook" area and helped to identify sites for possible fire support bases and landing zones.

The 175th RR Company, CMA for the III CTZ, supplied translations, tasked ARDF/collection efforts, identified fixes, monitored the DSUs, and issued reports to higher headquarters. The processing company also deployed three RATRACE teams to assist DSUs in analysis of their intercept, and a TAREX team traveling with combat elements was able to exploit captured documents. Using both U–8 and U–21 aircraft, the 146th Avn Company alone flew 222 direction-finding sorties and 156 collection missions in support of the campaign.

Despite lack of advance notification, LTC James Freeze, Commander, 303d RR Battalion was able to quickly formulate an effective plan to shape ASA's support on the ground.

"As COSVN retreated we could watch . . . the transmitters moved along with the DF fixes. On a daily basis we could tell people that COSVN had moved so many miles up Highway 7. Unfortunately, they managed to stay just outside of US penetration into Cambodia."

CW3 CHARLES R. BYARS, SIT OFFICER, 509th RR GP

Because the enemy possessed low-powered transmitters, a decision was made to emphasize voice intercept. On 4 May 1970, personnel of the 409th RR Detachment became the first DSU to enter Cambodia. Attached to the 11th Armd Cav Regiment, the detachment logged 158 km over a 54-day period. Its low-level voice intercept (LLVI) effort contributed 2,133 minutes of enemy traffic and exploited 108 messages. The 371st RR Company also engaged in LLVI, and its LEFT BANK platform was credited with locating the enemy's logistics center popularly known as "The City." When ARVN soldiers secured the area, they discovered 182 storage bunkers containing supplies and weapons. The 372d RR Company supplied targeting data to the 25th ARVN Division crossing into the "Parrot's Beak" area in search of other enemy logistical bases. Under Operation SKYSPOT, the company also used air-to-ground communications to receive fixes and then quickly passed them on to tactical aircraft.

In the II CTZ, the 374th and 330th RR Companies supported the 4th Inf Division engaged in joint operations against NVA tactical and rear service elements. To the south, the Delta Military Assistance Command launched a combined land and naval operation to secure the Mekong River from the Vietnam border and to evacuate Vietnamese nationals from Cambodia. Besides passing information on the changing enemy situation, the 335th RR Company also briefly ran an LLVI/ARDF tip-off operation off the USS Benewah, command ship for naval operations.

A LEFT BANK platform located "The City," a large cache of enemy supplies and weapons.

Members of the 409th RR Detachment pause aboard an M–113 armored personnel carrier during the 1970 Cambodian Incursion.

TRAI BAC

The 8th RR Field Station, nicknamed "Trai Bac Station" or "Station of the North," possessed some of the finest facilities in Vietnam, consisting largely of permanent structures, a prefabricated operations building, and air conditioned trailers for troop billets and mess. The field station's security posture was equally impressive. An intensive defense perimeter, including 2600 meters of personnel and communication trenches, 30-foot-high steel watch towers, 12-inch cement reinforced star bunkers, concertina and barbed wire fences, and 54,000 M–14 antipersonnel mines all surrounding the compound. Although there was no fear of direct attack, the facility did receive occasional rocket fire. Of greater concern was enemy activity interrupting truck convoys bringing supplies.

Beginning in 1967, the 8th RR Field Station began focusing on the network that carried personnel and cargo on a 1,000–mile journey down the "Ho Chi Minh Trail" to the battlefields of South Vietnam. The North Vietnamese travelled in battalion size groups, as organic table of organization units, or in smaller-sized elements of specialized personnel and were conveyed by train, truck, and barge as well as on foot to their destinations. Cargo, which was stockpiled at various sites, entered the system and was transported via similar means. Observers believed that the system was capable of handling a minimum of 200,000 personnel annually and 2,200 tons of supplies each month.

The arrival of ASA direct support units during the spring of 1968 significantly expanded the field station's mission. The recent Tet Offensive and the deteriorating tactical situation in the Northern provinces led to the shifting of the 1st Cav Division; the 1st and 2d Brigades, 101st Abn Division; and the 3d Brigade, 82d Abn Division into the I CTZ. The 371st RR Company, the 265th RR Company, and the 405th RR Detachment accompanied the divisions. By fall, the 371st RR Company, 405th RR Detachment, and their parent organizations had redeployed to the III CTZ and were replaced by the 407th RR Detachment in support of the 1st Brigade, 5th Inf Division.

The 8th RR Field Station maintained an operational site on Hill 180.

". . . I would say at least three times a week, General Abrams would come over to the field station at Phu Bai. . . . He and a field station Chief Warrant Officer by the name of Holder would literally talk the entire situation through. General Abrams would at times turn around to the J3 and say, 'Let's lift a force over in such and such an area, and have the 1st Air Cav throw a blocking action. . . .' "

COL WILLIAM T. RILEY, JR., CDR, 509th RR GP

South Vietnamese civilians assisted in bolstering the defenses of Phu Bai which was a well guarded installation but suffered rocket attacks from time to time.

In its new tactical support role, the 8th RR Field Station found itself having to provide technical and analytical assistance to the assigned direct support units. However, the field station lacked the staff necessary to serve as a "provisional battalion" and was without the type of logistical system needed to support the needs of the DSUs. One of the early problems was the discovery that some DSU personnel could not function in their new area of operations because of the different target environment. As they received on-the-job training at the field station, the 8th was forced to substitute its own personnel in the field.

Throughout its history, the 8th RR Field Station made a significant contribution at theater level. For example, its intercept of enemy weather reports supported the Seventh Fleet's strike and reconnaissance missions. The field station's around-the-clock reporting provided the carrier task group commanders with timely information on which to base their aircraft go/no-go launch decisions. To keep pace with its ever-expanding missions, Phu Bai undertook a series of major construction projects. In the end, the 8th RR Field Station would not only become ASA's largest unit in Vietnam, but its largest operational element worldwide.

Sharing the Mission

In 1968, a significant amount of VC/NVA voice intercept was being collected. To meet the increased workload, ASA made greater use of South Vietnamese transcribers, DANCERS, who were almost 3 times more efficient than US linguists. By 1970, 76 DANCERS were scattered among US cryptologic units, almost half of them assigned to the 8th RR Field Station. In August, DANCERS even began to fly collection missions with the 138th Avn Company. DANCERS-in-the-sky (DITS), as they were called, could copy live 90 percent of all voice traffic intercepted, thus eliminating the need for transcription and allowing for timelier reporting. DANCERS were also used at remote collection sites and as members of the RATRACE teams deployed by the various CMAs to provide direct support units with analytical and transcription assistance.

In 1970, the 509th RR Group undertook a study of the South Vietnamese SIGINT effort (Unit 15) to determine what further assistance could be provided. High on the agenda was evaluating the ARVN's medium range direction-finding net. The study disclosed serious deficiencies, including the fact that some Unit 15 operators were readjusting bearings to fit preconceptions. This further confirmed ASA's long held belief that the South Vietnamese should get out of the MRDF business altogether and focus mainly on voice intercept. But in the end, the 509th RR Group was forced to continue to assist the South Vietnamese's direction-finding program, eventually turning over state-of-the-art AN/TRD–23 direction finders.

Unit 15 had repeatedly tried to get its ARDF effort off the ground. Utilizing U–6 aircraft, the South Vietnamese began flying missions in the III and IV Corps areas. Although given only targets that they demonstrated the ability to copy,

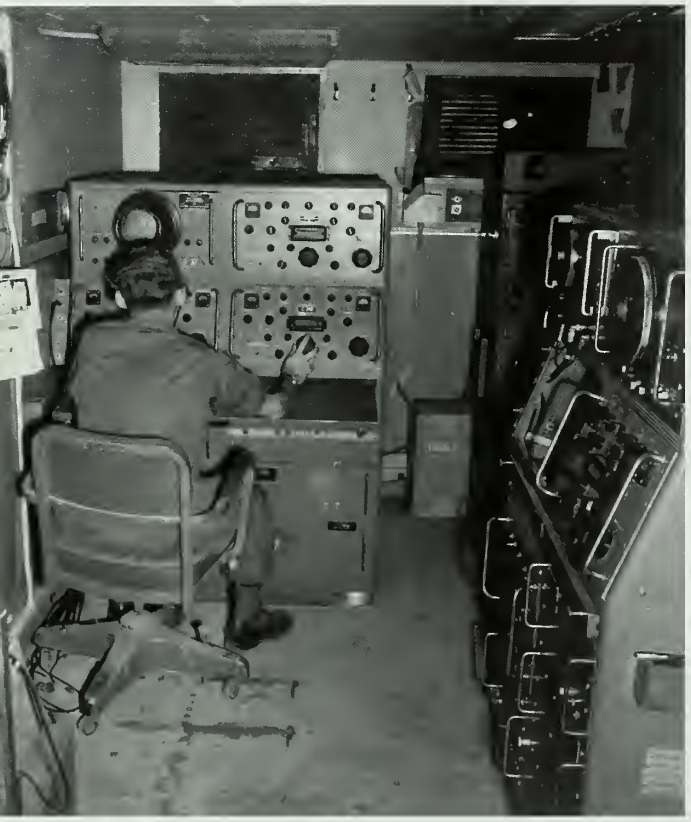
"I hope people understand, it is going to take time to establish an ARVN SIGINT Data Base. It takes months, even years, to build an intelligence base. Just because someone puts up an antenna doesn't mean he's going to start producing intelligence."

MAJ DAVID A. BELL, ADVISOR, 21st DIVISION

A South Vietnamese linguist stands atop a remote intercept site at An Duong Wong. From here, the 265th RR Company conducted voice and manual Morse intercept.

the South Vietnamese ARDF program still continued to founder. A 1970 study by the 509th RR Group placed much of the blame for poor results on ineffective equipment. ARVN pilots and operators were judged to be competent and highly motivated, but the R–390 receivers, magnetic compasses, and direction gyros were showing signs of age. Even the maps were too small and outdated. Subsequently, 509th RR Group furnished the South Vietnamese with additional training in ARDF procedures and put into place a new reporting system. Six months later, the US Air Force began transferring aircraft to the South Vietnamese who, in the meantime, had created a separate organization, Unit 17, for the specific purpose of carrying out its revitalized ARDF mission.

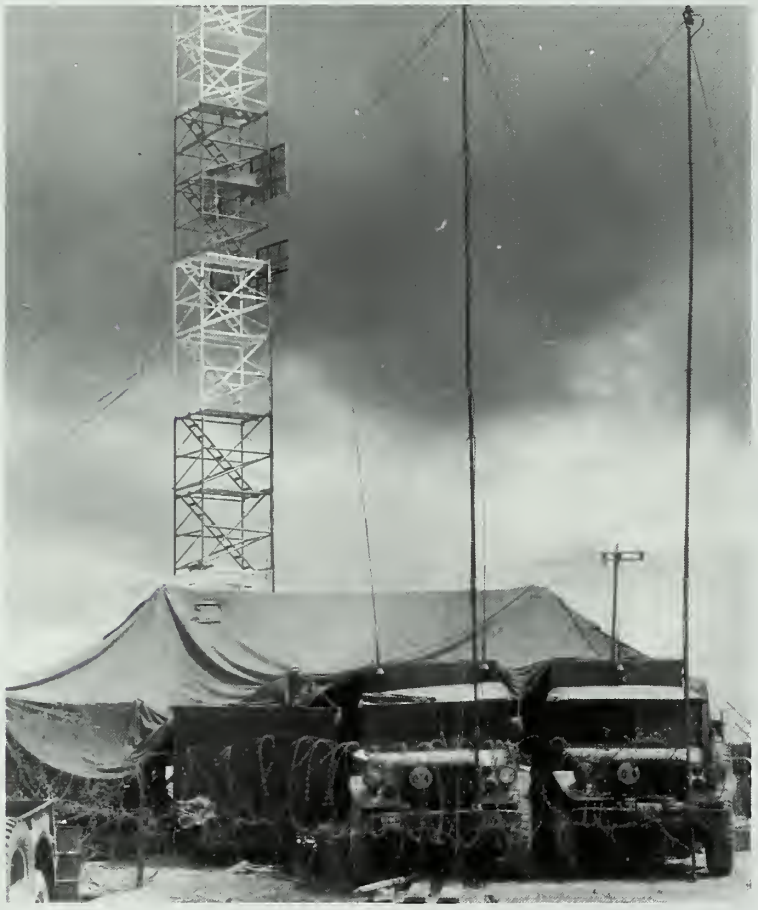
The South Vietnamese COMSEC effort (Unit 16) was characterized by its lack of trained personnel, inability to perform telephone monitoring because of political considerations, tardiness in receiving authorized equipment, and absence of qualified US advisors, but over time, Unit 16 began to demonstrate signs of progress. By 1971, it possessed for the first time the COMSEC resources needed to monitor, on a sampling basis, all networks within the Vietnamese Armed Forces and to conduct semi-annual crypto inspections of all military and non-military agencies. But in the end, it was a simple matter of being too little and too late.



An operator mans the AN/TRD–23 Direction-finder inside a shelter.

"... General McCown when we got onto the ship (USS Benewah) took me down into the operations center and introduced me to all the colonels, couple of generals and the remaining staff. . . . He said, 'Gentlemen I want your attention, this is Sergeant Wood and he will be coming down every once in a while with some information for you and whatever he tells you is fact.' "

SFC JAMES W. WOOD, JR., LIAISON TO IV CORPS



Operational area of the 1st Platoon, 335th RR Company at FSB Moore.

Traffic Analysis Section at the 175th RR Company.

BG George Godding, CG USASAPAC, and COL William Riley, CDR 509th RR Group, leave the WHITEBIRCH Compound in Saigon, scene of fighting during TET 68.

On 15 December 1970, members of the 403d RR Special Operations Detachment cased their colors at Headquarters of the 5th Special Forces Group in Nha Trang.

VIETNAMIZATION 1971 1973

"In theory, the centralized field station concept would allow mission accomplishment with reduced resources. In our case, however, the benefits of the concept were not realized because our assets were spread over 53 percent of the land mass of Vietnam."

LTC DAVID A. WISYANSKI, CDR, 330th RR FS

Following a meeting with South Vietnamese President Thieu on 8 June 1969, President Richard M. Nixon announced the initial withdrawal of 24,000 American troops from South Vietnam. The redeployment signaled the beginning of a process to extract the United States from the war and to turn the fighting back to the South Vietnamese. The reduction in US tactical operations and the withdrawal of combat elements would lead to corresponding changes in the size and scope of the SIGINT mission in Vietnam. Representatives from the cryptologic community met in Saigon in early December 1970 to map out exactly how and where the cuts would be made. A plan emerged to consolidate at a handful of locations, thus allowing the 509th RR Group to take its manpower reductions among support rather than operational personnel. This could be accomplished by replacing the direct support battalions with field stations, inactivating the 144th Avn Company, and reorganizing the 101st RR Company. Plans called for selected manual Morse positions to be remoted, and systems whose value was deemed marginal eliminated altogether.

Over the next 9 months, ten DSUs were either redeployed or inactivated, among them the Headquarters and Headquarters Companies of the 303d and 313th RR Battalions and the 403d RR SOD. In September 1971, two new field stations were organized from the existing Collection Management Authorities. The 175th RR Company was redesignated the 175th RR Field Station at Bien Hoa. The 330th RR Company was inactivated and the 330th RR Field Station organized in its place at Nha Trang. Like the 8th at Phu Bai, the two new field stations would exercise control of targeting and the residual direct support units in their area of operations. At the same time, ASA inactivated the 335th RR Company as the local collection management authority for the IV CTZ. In its place, a new smaller-sized company was organized and given an advisory mission in support of the local South Vietnamese COMINT Center. Other changes involved the drawdown of the 144th Avn Company and redistribution of its aircraft and mission to the 3d Platoon, 146th Avn Company. The 101st RR Company's strength was reduced by 50 percent to 113 spaces, its supervisory role transferred to the 509th RR Group, and its COMSEC specialists were formed into support platoons that were assigned to the various field stations.

During the initial reduction phase, marginal systems were first on the cutting block. Radio fingerprinting had fallen into disuse, making it an easy candidate for removal. The WHITEBIRCH direction-finding net was also discontinued, and its targets assumed by other nets and ARDF. At best, WHITEBIRCH had served to maintain continuity on targets of a relatively low priority. However, other missions were not as easily eliminated; chief among them was manual Morse, the backbone of ASA's intercept effort in Vietnam. June 1970 found the 509th RR Group devoting 199 of its 271 positions to manual Morse. A year later, the number of manual Morse positions was cut almost in half, and the impact was immediately felt by consumers at all echelons.

Members of the 1st ASTD, the ARVN equivalent of an ASA direct support unit.

Vietnamese students learning to transcribe manual Morse code using both pencil and typewriter.

DARRS and CARRS

As they assumed more responsibility for conducting the war, the South Vietnamese began to reorganize their COMINT effort to more closely mirror the US system, but on a much smaller scale. For example, the South Vietnamese created ARVN Special Technical Detachments (ASTDs), each consisting of 4 officers and 56 enlisted personnel. They provided direct support to combat divisions and passed information up the South Vietnamese cryptologic chain of command. On 1 July 1969, the first two of the ASTDs became a reality: one in support of the 1st ARVN Division at Hué, and the other assigned to the 2d ARVN Division at Quang Ngai. Under the terms of the Vietnamese Improvement and Modernization (VIM) program, the 509th RR Group assisted all 10 of the ASTDs by providing mission equipment and logistical support and by instructing the South Vietnamese on how to perform their own maintenance. ASA also made an NCO available to each of the ASTDs for advice and assistance. All the while, ASA representatives continued to take every opportunity to press the ASTDs to focus upon voice intercept and even offered on-the-job training by temporarily assigning Vietnamese to the 509th RR Group's own low-level voice intercept teams.

"For a long time we had a shortage of hard intelligence such as *Chieu Hois* and POWs. This was back in July through October of last year before the 9th DARRS existed. . . . The 9th DARRS has given us the ability to make estimates and allow the commander to make decisions."

MAJ NOEL J. DOYLE, JR., G2 ADVISOR, TEAM 60

Under Project SCREWDRIVER, ASA soldiers regularly visited South Vietnamese elements to pass on maintenance tips and to ensure that they were receiving a reliable source of expendable supplies, especially for their ARDF program. These types of advice and assistance visits proved an excellent means to monitor overall operational progress. ASA collection management authorities also created a sponsorship effort at each of the ARVN fixed stations. Nicknamed Project LEVER, the program revolved around periodic visits and recommendations concerning procedures and techniques.

Although responsibility for the fighting shifted to the South Vietnamese, requirements by US authorities for COMINT support remained as critical as ever. Under Project AXE, the concept of Division Advisors Radio Research Support (DARRS) Detachments was first tested in the field in January 1970 when a DARRS team successfully deployed in support of the Senior Advisor, 1st ARVN Division and the 1st ASTD. This led MACV to approve DARRS detachments for all the ASTDs. The primary function of the DARRS was to pass COMINT to senior US personnel advising the ARVN divisions and to provide a sanitized version for the ARVN commanders. In addition, DARRS personnel served as advisors to the ARVN Special Technical Detachments. The impact of the DARRS was immediately evident and was given credit for making the ASTDs operationally functional.

In July 1971, the 509th RR Group assisted in establishing the Center Advisory Radio Research Support (CARRS) detachments at each of the four South Vietnamese field stations/centers: Can Tho, Pleiku, Saigon, and Da Nang. The CARRS's primary mission was to improve the SIGINT centers' management of operations, communications, and maintenance support.

Housed in a U–21, the LEFT JAB platform was targeted against transmitters near the DMZ. An antenna was contained in the radome mounted under the plane's belly and extended upon takeoff.

"Special intelligence has been a key factor in tactical success—we'd be quite blind without it. Although one cannot rely on special intelligence alone, it provides the essential skeleton against which other source material can be associated to form a quite accurate framework of enemy disposition and in some cases, enemy intentions...."

MG GEORGE I. FORSYTHE, CG, 1st CAV DIV

New Platforms

Throughout the war, COMINT/ARDF was the most important source of timely, accurate intelligence and served as the commanders' principal eye in finding an elusive enemy. By May 1968, the 224th Avn Battalion was contributing nearly 4,000 fixes a month to the ground war. Consumers often utilized ARDF as a warning mechanism of pending enemy activity. This was particularly important in protecting fire support bases and isolated outposts. Normal countermeasures included air strikes, artillery fire, and even the launching of offensive operations. On one occasion, ARDF fixed an enemy terminal several kilometers in front of an advancing

convoy. The rapid relay of the warning allowed the commander to halt the convoy in time and insert armored personnel carriers and tanks. The ambush was thwarted and heavy casualties were inflicted on the enemy.

ARDF often influenced the intelligence-gathering process. A member of the G2 staff, Delta Regional Assistance Command, made the following observation: "Often an ARDF fix will cause us to look for the collateral; a ground sweep will be made and a prisoner captured and interrogated...." On the flip side, ARDF proved most effective when merged with other forms of information such as airborne personnel detectors, infrared, side-looking airborne radar, long-range reconnaissance patrols, aerial photography, enemy documents, prisoner-of-war interrogation, and area studies.

In February 1968, MACV established a requirement for an airborne VHF intercept and direction-finding platform to cover the DMZ area. The initial attempt to field a system in a U–1A (SORE THUMB) was a failure, and a second try in an OV–1C (HOMING PIGEON) ended with mixed results. But after a lengthy delay, three LEFT JAB platforms were finally fielded in December 1970 and assigned to the 138th Avn Company at Phu Bai. At the heart of the system was a spinning spaced loop antenna mounted in a radome under the belly of a U–21 aircraft. Originally designed for ground-based systems, the antenna could be extended after takeoff.

The installation of the AN/ARD–23 V-Scan on the LAFFING EAGLE platforms in October 1970 represented a major milestone in Army ARDF. The V-Scan system was the most advanced HF ARDF platform in the ASA's inventory and placed the Army technologically on more equal footing with the Air Force. Advantages over previous systems included increased speed in recording fixes, ability to cover larger areas, and a more accurate navigational system. It was not long before the LAFFING EAGLE was being used exclusively in its ARDF role as other platforms began to stand down.

On 4 March 1971, the 224th Avn Battalion received word that a LEFT JAB aircraft was missing in action. The fate of the craft and its 5-member crew was later confirmed by a report of the North Vietnamese News Agency, which claimed that a surface-to-air missile had downed a US plane just inside North Vietnam. But the shoot-down did not deter future flights near the DMZ. In fact, during the enemy's 1972 Spring Offensive, airborne COMINT collection efforts in the area took on even greater significance. Although credited with only a small portion of the total manual Morse intercepts, LEFT JAB still made a significant contribution during the campaign's critical phase.

Wideband operators at the 175th RR Field Station helped to make up for the loss of manual Morse resources.

"On Hill 950 with Project EXPLORER the Chief of the Studies and Observations Group . . . was adamant about putting anything up there that would draw attention to the hill. He remarked that the 5 Americans and 38 . . . mercenaries on the hill were there at the grace of the VC. . . . He did not object to a new antenna, but a shelter would have drawn too much attention."

CWO–4 WILLIAM R. MACDONALD, 175th RR CO

Computer systems, such as this at the 8th RR Field Station, were increasingly in use during Vietnam.

New Technologies

Over 50 percent of ARDF fixes remained unidentified. In response to this problem, the USASA Materiel Support Command at Vint Hill Farms Station, Virginia, fabricated the first Wideband position, known as MUSTARD, and shipped it to the 330th RR Company, where it became operational in April 1967. Wideband collection recorded segments of the radio frequency spectrum for selective playback. Although the system demonstrated promise, tapes of the recovered intercept had to be sent back to Vint Hill Farms Station, Virginia, for processing. The 2-week turn around time kept Wideband from having any real impact upon the immediate tactical situation. However, by September 1968, the two Wideband positions were beginning to make some headway, accounting for between 10–20 percent of the fixes being identified each month. This led to the introduction of additional systems with increased collection capability at each of the Collection Management Authorities. When the 509th RR Group finally departed Vietnam, Wideband positions would be among the last positions manned.

During Vietnam, computers began to make their debut on the battlefield. One of the earliest systems was designed to improve target acquisition. Field tested at the 8th RR Field Station in May 1969, the new system did not replace the manual Morse operator, but it did provide him with a new tool to automate

certain functions that had previously been done by hand, such as, tuning to selected frequencies.

Until 1970, airborne platforms provided the only significant intercept of enemy VHF communications along the Laotian border. To augment airborne collection, a hearability test was conducted on Hill 950 located in western Quan Tri Province, 110 km northwest of the 8th RR Field Station. Manned by a contingent of Special Forces and Montagnard Tribesmen, the mountain overlooked the rugged wilderness that served as a haven for elements of the North Vietnamese Army. The quality of intercept obtained by these tests proved at least equal if not superior to any being copied from airborne platforms.

In June 1970, the first remote system (EXPLORER), controlled by operators at the 8th RR Field Station, was put into operation. Despite its successful beginnings at producing real-time intelligence, EXPLORER faced a number of logistical problems. The most significant was providing adequate supplies of gasoline to power the system. To draw as little attention as possible, ASA soldiers buried all of the equipment minus the antennas, and to cut down on noise, used generators specifically designed for "whisper" quietness. Then there were the normal environmental factors of heat, dust, humidity and their affect upon the equipment. To top it off, the rainy season frequently interrupted refueling and maintenance runs.

By March 1971, four more remote positions had been added on Hill 950. (A month later, EXPLORER II was established at Golf 5 (Hill 1005) and the intercept relayed to the 330th RR Company at Pleiku for processing and reporting.) Unfortunately, EXPLORER operations at Hill 950 ended abruptly on 4 June 1971 when the outpost came under intense enemy mortar and rocket fire, lasting most of the day. At 2100 hours orders were given to destroy the equipment with thermite grenades and to evacuate the site.

Success at a High Price

It wasn't until the latter stages of the war that the landline effort could point to an example of real success. In February 1970, a Ranger team from the 1st Brigade, 5th Inf Division, was inserted by chopper to exploit an enemy landline located in the vicinity of the DMZ. Making the remainder of the way on foot, they found a lead-in wire running parallel to a small, well-used trail that ran through dense undergrowth. Here, they buried the kit's lead wires along with the control box and batteries and then fastened a whip antenna on the backside of a tree away from the path. Total time to install the XR4–100D was 38 minutes. A second trip was made to replace the antenna because of an interference problem. During the 2 weeks the Con Thien operation was active, 15 translations were made and nine tactical reports forwarded, successfully alerting friendly forces against pending attacks. The intercept also revealed the enemy's reaction to Allied artillery fire. In total, almost 255 hours of North Vietnamese plain text voice were intercepted until the output ended abruptly. A third Ranger team was sent to investigate, but came under small arms fire. This led to the decision to destroy the intercept equipment by targeting the site with rounds of artillery and by dropping some twenty-four bombs as the final *coup de grace.*

The success at Con Thien served as a catalyst for further attempts. During the Cambodian Incursion in 1970, one landline intercept successfully warned US forces of a pending attack by a battalion-size force and a 75mm recoilless rifle company. In another instance, the 138th Avn Company (RR) participated in an airborne test for intercepting relayed signals. However, for the most part, landline operations continued to court disaster. On 23 April 1971, Company L, 75th Infantry (Ranger) attempted to tap into communications lines believed to be serving the Ho Chi Minh Trail, but were met with stiff resistance by the enemy. Two choppers were shot down, killing 11 soldiers and wounding 22 others. Later it was discovered that the operation had been doomed from the start because the recording unit's batteries had been accidentally reversed.

"Analysis of the tape indicated that the intercept was . . . entirely concerned with roads and routes which are probably part of the Ho Chi Minh trail. . . . This cut was too brief to be of significant intelligence value."

MAJ ALBERT B. YOUNG, COLLECTION OIC, 509th RR GP

One of the major problems faced by wiretap teams was that the VC/NVA units would daily send runners along the lines to check them. Two ASA engineers working at Vint Hill Farms Station came up with the LEFT TWIST system where a transmitter in the form of a pole was dropped from a helicopter. Actual results in the field in 1971 proved mixed, and future trials were cut short when the course of the war began to change. The drawdown of US combat forces led to fewer deployment opportunities for landline intercept and eventually brought an end to the mission altogether. Time had finally run out on ASA's landline mission. However, lingering questions remained as to why lessons learned as far back as 1966 were continually ignored. The technological advances in the CIRCUS ACT program were achieved at a high cost given the numbers of casualties suffered by the installation teams and the limited amount of usable intelligence extracted.

The departure of US troops ended all opportunities to exploit enemy landlines. (National Archives)

Free Fall

What began as a steep glide in the level of ASA's commitment to Southeast Asia had turned into a virtual free fall by late 1971. The 509th RR Group was ordered to cut its remaining 4,000 spaces in half. Missions were eliminated, the last of the DSUs was inactivated, two of the field stations were discontinued, and the 224th Avn Battalion was in the process of being reduced to a company. Plans called for only the 509th RR Group headquarters, the 8th RR Field Station, the 175th RR Field Station, and the 146th Avn Company to remain.

In November, the 335th RR Company began to systematically shift its manual Morse effort to the South Vietnamese collection site at Can Tho. The company would be the first among ASA's units to undergo such a transfer. The 335th RR Company personnel were responsible for training the ARVN specialists in analysis, reporting, and maintenance procedures. Eventually, the 175th RR Field Station took over as the CMA for the Delta Region when the 335th finally ceased operations in 1972.

The departure of US forces also changed the manner in which ASA did business. The need for COMSEC support was greatly reduced, leading to the phase out of the 101st RR Company and its discontinuance altogether on 1 April 1972. The drawdown also meant TAREX personnel could no longer depend upon US combat units for captured equipment and documents. In the future, all TAREX collection teams would be based out of Saigon, and liaison with the South Vietnamese stepped up. As US

Manual Morse positions, such as these at the 175th RR Field Station, were the heart and soul of ASA's effort in Vietnam. Their decline signaled that ASA's role in the war was coming to an end.

"Plans for our evacuation were jovially passed around, trying to convince each other that it would never actually come to that. Then, at the stroke of 5:00 p.m., the sky caved in, and within the next 30 minutes more than 500 shells of assorted sizes impacted and detonated. . . . At 5:30 p.m., when the heavy barrage was lifted, we resumed destroying all that was not an absolute necessity."

MSG G. DUANE WHITMAN, 407th RR DET

The loss of direct support units such as elements of the 407th RR Detachment at Con Thien near the DMZ significantly impacted ASA's ability to satisfy all of its consumers.

units departed, the Army's logistical system also began to shut down, creating a shortage of signal parts in the supply pipeline and significantly impacting upon ASA's operations.

During January 1972, the 1st RR Company flew two of its five Neptune aircraft to Japan for turn-in. Despite having only half of its aircraft available, the company maintained production at 90 percent of previous levels until the company was inactivated on 30 April. (The 1st RR Company also sent one of its remaining aircraft to Fort Rucker, Alabama, for permanent display at the Army Aviation Museum.) Meanwhile, flight crews of the 156th Avn Company were also touching down for the last time in preparation for turn-in of the U–6's and transferring the unit's colors to Fort Bliss, Texas. During the 156th Company's 6 years of existence, its aviators flew over 16,000 support missions and logged some 7 million miles.

Nowhere did the drawdown have a greater impact than in the area of manual Morse collection. By 30 June 1972, ASA had 60 intercept positions remaining, compared with 199 two years earlier. On top of this, the 509th RR Group was facing a critical shortage in intercept operators. Realigning working schedules and shifting mission taskings offered some temporary relief; the lack of personnel also justified the retention of the five remaining Wideband collection systems.

Changing Course

Conventional intelligence sources, along with COMINT support from ASA direct support elements, had slowly dried up with the departure of US combat divisions. In January 1972, SIGINT began to reflect large-scale movement of equipment and supplies southward into the DMZ, Tri-border, and Panhandle areas, indicating preparations for a major offensive that threatened the phased withdrawal of US forces. Twelve North Vietnamese combat divisions representing approximately 100,000 personnel were located within or adjacent to South Vietnam. In the light of these developments, MACV indicated that it could not tolerate further loss of SIGINT coverage in Military Region (MR) II and the southern portion of MR I. To compensate for the pending closure of the 330th RR Field Station, a last-minute replacement detachment was stood up at Da Nang and placed under the control of the 8th RR Field Station. Meanwhile, responsibility for targets in the southern MR II was transferred to the 175th RR Field Station. Once these improvised arrangements were in place, the 330th RR Field Station proceeded to stand down on 1 September 1972.

Planning called for paring the 224th Avn Battalion's organization down to one company, the 146th Avn Company, and reducing the number of aircraft from 36 to 10 U–21s. On 10 June, COMUSMACV intervened and reversed the order, citing the following rationale: "MACV ARDF resources…represent our most effective means of finding and fixing the enemy…." The drawdown was not only put on hold, but the allotment of manpower spaces was actually doubled to 540. To complicate matters, when the 224th Avn Battalion received notification that the current level of ARDF support must be maintained, it was entering the final phase of inactivation. Only 5 percent of the Headquarters and Headquarters Company's personnel remained. The 138th Avn Company had flown 11 of its U–8s to Vung Tau for shipment back to the States, and the remaining aircraft were at Long Thanh North Army Airfield to wait processing.

"We're in a dynamic situation. Decisions on units being drawn down, forces being economized, and selection of the key installations to stay open are being made. To do this safely you must have knowledge of the enemy, his plans and intentions. Special intelligence provides this. It's invaluable."

MG CHARLES M. GETTYS, CHIEF OF STAFF, USARV

The ASA leadership: (left) BG Herbert E. Wolff, CG USASAPAC, and (center) MG Charles Denholm, CG USASA, arrive at Phu Bai International Airport to discuss drawdown plans with ASA commanders in country.

For the next 3 to 4 weeks, the 224th Avn Battalion scrambled to retrieve planes and equipment. The stock of replacement parts had dropped so low that the battalion was forced to cannibalize nine of the returned aircraft. For the sake of efficiency, a decision was made to place all 27 U–8s with the 146th Avn Company at Long Thanh North and to assign all U–21s to the 138th Avn Company at Phu Bai. This would allow each type of aircraft to be in close proximity to support facilities handling its particular type of navigational equipment. Despite having released a third of its aviators, the 224th Avn Battalion was able to draw upon TDY crews to take up the slack. Within 10 days, the 224th Avn Battalion had the first U–8 back in the air, and by another week and a half, the number of missions had risen to 133 a week.

A member of the 8th RR Field Station's security force surveys the horizon.

Shifting Sites

Throughout the spring and summer of 1972, ASA units in Vietnam faced a growing security problem. Increased enemy activity coupled with the departure of nearby US combat elements left ASA sites vulnerable to attack. During the last 9 months in country, each one of the 509th RR Group's remaining units would be forced to relocate at least once. On 13 August, the COMUSMACV ordered the removal of US forces at Long Thanh North. Thanks to outstanding lift support from the US Air Force, the 224th Avn Battalion completed its transition to Saigon in less than 6 days. Simultaneously, the 146th Avn Company was moved from Long Thanh North to Can Tho while still completing 50 percent of its missions.

The 175th RR Field Station and the 8th RR Field Station remained as collection management authorities, and each were subdivided into collection management and reporting sections. Targeting continued to be responsive to field commanders' Essential Elements of Information and Special Intelligence Collection Requirements. On 30 September, the 175th RR Field Station relocated from Bien Hoa to Davis Station in Saigon and began conducting operations out of the former WHITEBIRCH facility within the Joint General Staff Compound. The building had become available when the 509th RR Group, no longer requiring the large work area, moved to the communications center adjacent to Davis Station.

"During the current NVA offensive, ARDF has been the single most important intelligence collection program providing early warning of impending enemy action. . . . I consider ARDF coverage especially of the northern Military Regions to be critical as long as US interests are involved in the Republic of Vietnam."

GEN FREDERICK C. WEYAND, COMUSMACV

The 8th RR Field Station and the 138th Avn Company were the last of the ASA units to change locations. Beginning in March, the physical security posture at Phu Bai became a subject of growing concern, leading to manning the perimeter and placing reaction teams on 24-hour alert. All personnel were assigned defense responsibilities that required a vast amount of time, equipment, and funds devoted solely to defense. Faced with an increased number of rocket attacks that left several dead and others wounded, the field station moved quickly to divest itself of its remaining missions. The end came in November when the residual elements of the field station and the 138th Avn Company were evacuated to Da Nang.

By the close of 1972, ASA personnel in Vietnam were manning only a handful of positions. The shifting of ground-intercept responsibilities to the South Vietnamese had progressed slowly but steadily. All the while concerns continued to be voiced as to whether or not the South Vietnamese had either the manpower or skills required to do the job. As a final stop-gap measure, ASA personnel worked alongside South Vietnamese SIGINT specialists in Saigon and Da Nang. By so doing, they helped to ensure that a steady supply of intelligence reached US authorities.

Cease Fire

In October 1972, USARV issued an operations plan that directed all remaining US forces to depart Vietnam within 60 days of a cease-fire. By early January, ASA had turned over all ground-based intercept to the ARVN with the exception of its Wideband positions located at the South Vietnamese COMINT site in Saigon. The departure of the 7th Air Force from Tan Son Nhut forced the 509th RR Group to move its personnel to the annex adjacent to MACV Headquarters for billeting and messing purposes.

Between 0620 and 0800 hours on 28 January 1973, the 509th RR Group's staff assembled atop the Newport Hotel to welcome in the cease fire by watching the enemy's rocket attack on Tan Son Nhut Air Base. The next day a contingent of VC/NVA soldiers arrived to occupy the former Davis Station compound as members of the four-power joint military commission. No sooner had the delegation settled in and guards been posted at the installation's gates than antennas began to appear. To the ASA personnel observing the proceedings, the prospects of the new occupants conducting communications intelligence at 509th RR Group's former headquarters seemed an ironic but fitting conclusion to the war in the ether.

During the cease-fire, the 509th RR Group analysts continued to serve as advisors at the South Vietnamese SIGINT centers, but VC/NVA units tended to remain in place and began to make greater use of landlines. All the while, ASA crews flew collection missions that, despite the truce, continued to be subjected to antiaircraft fire. On 16 February 1973, a crew of the 138th Avn Company completed the Army's final ARDF mission in the vicinity of Pleiku. The end came less than a month later on 7 March 1973, when the 509th RR Group was discontinued and the handful of its remaining soldiers boarded the last plane for home, bringing ASA's 12-year tour of service to a close.

When ASA left Vietnam, it took with it a number of lessons learned. (Although in reality, many of these issues were for higher echelons to solve.) The need for greater fusion of communications and collateral intelligence was recognized as well as better coordination of the entire US intelligence effort. ASA had felt frustrated by the limited numbers of consumers cleared for SIGINT and of the restraints imposed by the SSO system, a system it did not control. There was also acknowledgement that in mobile warfare, intelligence could never be too timely. Some within the ASA leadership believed that the agency had not taken personnel assignments seriously enough and had often placed junior or inexperience officers in key operational or leadership positions, particularly at the DSU level. On the other hand, despite the hostile intelligence environment, ASA had succeeded in providing the commander on the ground with a level of support previously unknown in the annals of Army cryptology. (Vietnam was the reverse of World War II where SIGINT had achieved great success at theater level but proved to be of only marginal value in the direct support mode.) ASA had been first into Vietnam and among the last to leave. Its systems had operated in the air and in close support of ground forces from the Delta to the DMZ and all points in between. ASA left Vietnam with the satisfaction of having been the primary source of timely, usable intelligence during the course of the war. A staff officer assigned to J2, MACV, perhaps summed it up best, "The COMINT effort gained great 'kudos' from tactical commanders and G2s. . . . There was never anything like it before and possibly there may never be again!"

The 509th RR Group receives the Republic of Vietnam's Cross of Gallantry with Palm. While in Vietnam, ASA units were awarded more than 120 US decorations and 60 foreign citations.

509

Appendix A

Order of Battle 1961–73

Status of ASA Units in Vietnam

(as of December 1964)

Administrative Designator	Cover Designator	Base Camp Location	Supported Unit	Assigned Strength Off	WO	EM	Total
53d SOC	3d RRU	Saigon	MACV	20	15	371	406
101st Scty Det	7th RRU	Saigon	MACV	2	0	43	45
8th FS	8th RRU	Phu Bai	MACV	9	4	336	349
			Totals	**31**	**19**	**750**	**800**

Status of ASA Units in Vietnam

(as of February 1966)

Administrative Designator	Cover Designator	Base Camp Location	Supported Unit	Authorized Strength Off	WO	EM	Total
53d SOC	3d RRU	Saigon	MACV	36	12	565	613
101st Scty Det	7th RRU	Saigon	USARV	2	0	52	54
8th Fld Sta	8th RRU	Phu Bai	MACV	24	6	812	842
Co C, 313th Bn	10th RRU	An Khe	1st Cav Div	8	2	104	114
Co B, 313th Bn	11th RRU	Di An	1st Inf Div	9	3	156	168
Co A, 303d Bn	16th RRU	Chu Chi	25th Inf Div	9	3	156	168
404th Det	Det 1 3d RRU	Bien Hoa	173d Abn Bde	2	0	46	48
406th Det	Det 3 3d RRU	Phan Rang	1/101st Abn Div	2	0	46	48
407th Det	Det 4 3d RRU	Nha Trang	FFV	3	0	26	29
			Totals	**95**	**26**	**1963**	**2084**

Status of ASA Units in Vietnam

(as of October 1968)

Administrative Designator	Cover Designator	Base Camp Location	Supported Unit	Authorized Strength Off	WO	EM	Total
Gp VN	509th RR Gp	Saigon	MACV	41	10	299	350
Scty Co Saigon	101st RR Co	Saigon	USARV	9	2	181	192
Comm Unit Vn	RRCUV	Saigon	509th RR Gp	3	6	195	204
403d SOD	403d RR SOD	Nha Trang	5th SF Gp	3	0	41	44
Fld Sta Phu Bai	8th RR Fld Sta	Phu Bai	MACV/MAF	16	11	1039	1066
265th Co	265th RR Co	Camp Eagle	101st Abn Div	9	3	156	168
406th Det	406th RR Det	Camp Eagle	1/101st Abn Div	2	0	46	48
407th Det	407th RR Det	Quang Tri	1/5th Inf Div	3	0	80	83
303d Bn	303d RR Bn	Long Binh	FFV–II	18	5	251	274
Op Co Bien Hoa	175th RR Co	Bien Hoa	FFV–II	3	9	350	362
335th Co	335th RR Co	Dong Tam	9th Inf Div	9	3	156	168
337th Co	337th RR Co	Di An	1st Inf Div	9	3	156	168
371st Co	371st RR Co	Phuoc Vinh	1st Cav Div	9	2	146	157
372d Co	372d RR Co	Cu Chi	25th Inf Div	9	3	156	168
405th Det	405th RR Det	Phu Loi	3/82d Abn Div	3	0	74	77
409th Det	409th RR Det	Xuan Loc	11th Armd Cav	3	0	80	83
856th Det	856th RR Det	Long Binh	199th Inf Bde	2	0	60	62
313th Bn	313th RR Bn	Nha Trang	FFV–I	18	5	251	274
330th Co	330th RR Co	Pleiku	FFV–I	7	6	390	403
374th Co	374th RR Co	Pleiku	4th Inf Div	9	3	156	168
404th Det	404th RR Co	Phu Hiep	173d Abn Bde	2	0	60	62
Am RR Co (Prov)		Chu Lai	23d Inf Div	—	—	—	—
408th Det	408th RR Det	Chu Lai	196th Inf Bde	2	0	46	48
415th Det	415th RR Det	Chu Lai	11th Inf Bde	3	0	74	77
601st Det	601st RR Det	Chu Lai	198th Inf Bde	3	0	74	77
224th Avn Bn		Saigon	MACV	14	3	84	101
1st Co	1st RR Co	Cam Ranh	MACV	9	18	188	215
138th Avn Co		Da Nang	I CTZ	16	34	187	237
144th Avn Co		Nha Trang	II CTZ	16	34	187	237
146th Avn Co		Saigon	III CTZ	16	36	201	253
156th Avn Co		Can Tho	IV CTZ	11	21	138	170
			Totals	277	217	5502	5996

Status of ASA Units in Vietnam

(as of October 1971)

Administrative Designator	Cover Designator	Base Camp Location	Supported Unit	Authorized Strength Off	WO	EM	Total
Gp VN	509th RR Gp	Saigon	MACV	57	23	386	466
Scty Co Saigon	101st RR Co	Long Binh	USARV	13	0	98	111
Comm Unit VN	RRCUV	Saigon	509th RR Gp	2	6	180	188
FS Phu Bai	8th RR FS	Phu Bai	MACV/XXIV Corps	18	12	1011	1041
265th Co	265th RR Co	Camp Eagle	101st Abn Div	8	2	155	165
328th Co	328th RR Co	Chu Lai	23d Inf Div	8	2	151	161
FS Bien Hoa	175th RR FS	Bien Hoa	TRAC	12	9	504	525
405th Det	405th RR Det	Phuoc Vinh	3/1st Cav Div	3	0	72	75
FS Pleiku	330th RR FS	Nha Trang	SRAC	10	4	289	303
224th Bn	224th RR Bn	Long Thanh	MACV	13	4	78	95
1st Co	1st RR Co	Cam Ranh	MACV	9	17	175	201
138th Avn Co		Phu Bai	MR–1	18	42	212	272
146th Avn Co		Long Thanh	MR–2/3	22	60	266	348
156th Avn Co		Can Tho	MR–4	11	21	131	163
Co Can Tho	335th RR Co	Can Tho	DRAC	5	4	176	185
			Totals	**209**	**206**	**3884**	**4299**

Appendix B

Unit Summaries

Campaigns

1	Advisory	15 Mar 62–7 Mar 65
2	Defense	8 Mar 65–24 Dec 65
3	Counteroffensive	25 Dec 65–30 Jun 66
4	Counteroffensive, Phase II	1 Jul 66–31 May 67
5	Counteroffensive, Phase III	1 Jun 67–29 Jan 68
6	Tet Counteroffensive	30 Jan 68–1 Apr 68
7	Counteroffensive, Phase IV	2 Apr 68–30 Jun 68
8	Counteroffensive, Phase V	1 Jul 68–1 Nov 68
9	Counteroffensive, Phase VI	2 Nov 68–22 Feb 69
10	Tet 69/Counteroffensive	23 Feb 69–8 Jun 69
11	Summer-Fall 69	9 Jun 69–31 Oct 69
12	Winter-Spring 70	1 Nov 69–30 Apr 70
13	Sanctuary Counteroffensive	1 May 70–30 Jun 70
14	Counteroffensive, Phase VII	1 Jul 70–30 Jun 71
15	Consolidation I	1 Jul 71–30 Nov 71
16	Consolidation II	1 Dec 71–29 Mar 72
17	Cease-Fire	30 Mar 72–28 Jan 73

Note: What follows is based solely on ASA records. Only the USA Center of Military History can grant campaign credits and confirm unit awards. The following abbreviations were used: Presidential Unit Citation (PUC); Valorous Unit Award (VUA); Meritorious Unit Commendation (MUC); Republic of Vietnam Cross of Gallantry with Palm (RVN CGP); and Republic of Vietnam Civil Action Honor Medal (RVN CA)

1st ASA COMPANY

Deployed: 21 June 1967
Cover Designation: 1st Radio Research Company
Assigned Command: 224th Aviation Battalion
Supported Command: MACV*
Location: Cam Ranh Bay
Inactivated: 30 April 1972
Vietnam Campaign Participation Credit: 1**, 5–17
Vietnam Honors: 2 MUCs and 1 RVN CGP

* From Mar 1971 to Apr 1972, a detachment from the 146th Avn Co was attached to the 1st Avn Co to perform ARDF missions in the MR 2 upon the inactivation of the 144th Avn Co.
** Prior to assignment to ASA, the then 1st Army Avn Co had deployed briefly to Vietnam.

138th AVIATION COMPANY

Activated: 1 June 1966
Cover Designation: 138th Aviation Company (Radio Research)
Assigned Command: 224th Aviation Battalion
Supported Area: I CTZ*
Location: Da Nang on 1 June 1966
Relocated: Phu Bai on 3 June 1970
Relocated: Da Nang on 21 October 1972
Inactivated: 1 March 1973
Vietnam Campaign Participation Credit: 3–17
Vietnam Honors: 2 MUCs, 1 MUC (Navy), and 1 RVN CGP

* Redesignated MR 1 on 4 Oct 1970.

144th AVIATION COMPANY

Activated: 1 June 1966
Cover Designation: 144th Aviation Company (Radio Research)
Assigned Command: 224th Aviation Battalion
Supported Area: II CTZ*
Location: Nha Trang (Camp John F. McDermott)
Inactivated: 30 September 1971 (stood down April 1971)**
Vietnam Campaign Participation Credit: 3–15
Vietnam Honors: 3 MUCs and 1 RVN CGP
* Redesignated MR 2 on 4 Oct 1970.
** Mission transferred to 146th Avn Co.

146th AVIATION COMPANY

Activated: 1 June 1966
Cover Designation: 146th Aviation Company (Radio Research)
Assigned Command: 224th Aviation Battalion
Supported Area: III CTZ*
Location: Saigon
Relocated: Long Thanh North on 5 January 1970
Supported Area: MR 3 and MR 2 in April 1970**
Relocated: Can Tho on 16 August 1972
Supported Area: MR 3 and MR 4 in August 1972***
Inactivated: 17 February 1973
Vietnam Campaign Participation Credit: 3–17
Vietnam Honors: 3 MUCs and 1 RVN CGP
* Redesignated MR 3 on 4 Oct 1970.
** Assumed mission of the inactivated 144th Avn Co.
*** Assumed mission of the redeployed 156th Avn Co.

156th AVIATION COMPANY

Activated: 1 June 1966
Cover Designation: 156th Aviation Company (Radio Research)
Assigned Command: 224th Aviation Battalion
Supported Command: IV CTZ*
Location: Can Tho
Redeployed: 27 April 1972**
Vietnam Campaign Participation Credit: 3–17
Vietnam Honors: 3 MUCs and 1 RVN CGP
* Redesignated MR 4 on 4 Oct 1970.
** Transferred mission to 146th Avn Co.

HQ & HQ DETACHMENT, 224th AVIATION BATTALION

Activated: 1 June 1966
Cover Designation: Hq & Hq Company, 224th Aviation Battalion (Radio Research)
Assigned Command: 509th US Army Security Agency Group
Supported Command: MACV
Location: Saigon
Relocated: Long Thanh North on 5 January 1970
Redesignated: Hq & Hq Company, 224th Army Security Agency Battalion on 19 May 1971
Cover Redesignation: 224th Radio Research Battalion
Relocated: Saigon on 19 August 1972
Redeployed: 3 March 1973
Vietnam Campaign Participation Credit: 3–17
Vietnam Honors: 3 MUCs and 1 RVN CGP

265th ARMY SECURITY AGENCY COMPANY

Deployed: 3 December 1967
Cover Designation: 265th Radio Research Company
Assigned Command: 303d Army Security Agency Battalion
Supported Command: 101st Airborne Division
Location: Bien Hoa
Reassigned Command: US Army Security Agency Field Station, Phu Bai on 23 February 1968
Relocated: Camp Eagle on 15 March 1968
Relocation: Phu Bai on 13 January 1972
Inactivated: 1 April 1972 (zero strength by 18 January 1972)
Vietnam Campaign Participation Credit: 5–17
Vietnam Honors: 3 MUCs, 4 RVN CGP, and 1 RVN CA*
* The 3d Platoon, 265th Army Security Agency Company was awarded the MUC.

HQ & HQ COMPANY, 303d ARMY SECURITY AGENCY BATTALION

Deployed: 12 April 1966
Cover Designation: 17th Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: FFV–II
Location: Long Binh
Reassigned Command: 509th US Army Security Agency Group on 1 June 1966
Cover Redesignation: 303d Radio Research Battalion on 29 July 1966
Redeployed: 15 June 1971*
Vietnam Campaign Participation Credit: 3–14
Vietnam Honors: 5 MUCs, 1 RVN CGP, and 1 RVN CA
* Command mission transferred to USASA Field Station, Bien Hoa.

COMPANY A, 303d ARMY SECURITY AGENCY BATTALION

Deployed: 13 February 1966
Cover Designation: 16th Radio Research Unit
Assigned Command: 303d Army Security Agency Battalion
Supported Command: 25th Infantry Division
Location: Cu Chi
Redesignation: 372d Army Security Agency Company on 15 October 1966
Cover Redesignation: 372d Radio Research Company
Inactivated: 6 March 1971 (zero strength by November 1970)
Vietnam Campaign Participation Credit: 3–14
Vietnam Honors: 5 MUCs, 3 RVN CGP, and 1 RVN CA

COMPANY C, 303d ARMY SECURITY AGENCY BATTALION

Deployed: 7 September 1966
Cover Designation: 14th Radio Research Unit
Assigned Command: 313th Army Security Agency Battalion
Supported Command: 4th Infantry Division
Location: Pleiku (Camp Enari)
Redesignation: 374th Army Security Agency Company on 15 October 1966
Cover Redesignation: 374th Radio Research Company
Relocated: An Khe (Camp Radcliff) on 1 March 1970
Redeployed: 15 December 1970
Vietnam Campaign Credit: 4–14
Vietnam Honors: 3 MUCs, 3 RVN CGPs, and 1 RVN CA*

*Detachment 1, 374th ASA Company was awarded 1 PUC.

HQ & HQ COMPANY, 313th ARMY SECURITY AGENCY BATTALION

Deployed: 15 March 1966
Cover Designation: 13th Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: FFV–I
Location: Nha Trang
Cover Redesignation: 313th Radio Research Battalion on 3 May 1966
Reassigned Command: 509th US Army Security Agency Group on 1 June 1966
Redeployed: 18 June 1971*
Vietnam Campaign Participation Credit: 3–14
Vietnam Honors: 5 MUCs and 1 RVN CGP
* Command mission transferred to USASA Field Station, Pleiku.

COMPANY B, 313th ARMY SECURITY AGENCY BATTALION

Deployed: 3 August 1965
Cover Designation: 11th Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: 1st Infantry Division
Location: Bien Hoa
Relocated: Di An on 10 November 1965
Reassigned Command: 303d Army Security Agency Battalion on 10 May 1966
Redesignation: 337th Army Security Agency Company on 30 September 1966
Cover Redesignation: 337th Radio Research Company
Relocated: Lai Khe on November 1968
Relocated: Di An on 17 February 1970
Redeployed: 7 April 1970
Vietnam Campaign Participation Credit: 2–12
Vietnam Honors: 5 MUCs, 1 RVN CGP, and 1 RVN CA

COMPANY C, 313th ARMY SECURITY AGENCY BATTALION

Deployed: 16 September 1965
Cover Designation: 10th Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: 1st Cavalry Division
Location: An Khe (Camp Radcliff)
Reassigned Command: 313th Army Security Agency Battalion on 10 April 1966
Redesignation: 371st Army Security Agency Company on 15 October 1966
Cover Redesignation: 371st Radio Research Company
Reassigned Command: US Army Security Agency Field Station, Phu Bai on 23 February 1968
Relocated: Camp Evans (near Phu Bai) on 17 March 1968
Reassigned Command: 303d Army Security Agency Battalion on 16 October 1968
Relocated: Camp Gorvad (Phuoc Vinh) on 11 November 1968
Redeployed: 29 April 1971*
Vietnam Campaign Participation Credit: 2–14
Vietnam Honors: 2 PUCs, 1 VUA, 4 MUCs, 3 RVN CGPs and 1 RVN CAs**

* Residual mission transferred to the organized Brigade Radio Research Detachment (Provisional).
**Detachment 2, 371st Army Security Agency Company received the VUA.

328th ARMY SECURITY AGENCY COMPANY

Activated: 20 November 1968*
Cover Designation: 328th Radio Research Company
Assigned Command: 313th Army Security Agency Battalion
Supported Command: 23d Infantry Division
Location: Chu Lai
Reassigned Command: US Army Security Agency Field Station, Pleiku on 30 June 1971
Reassigned Command: US Army Security Agency Field Station, Phu Bai on 24 October 1971
Relocated: Da Nang on 24 October 1971
Reassigned Supported Command: 196th Infantry Brigade on 24 October 1971
Inactivated: 30 June 1972 (zero strength by 12 March 1972)
Vietnam Campaign Participation Credit: 9–17
Vietnam Honors: 3 MUCs and 3 RVN CGP**
*Assumed mission of the Americal Radio Research Company (Provisional)
** Detachment 2, 328th Army Security Agency Company received the VUA.

330th ARMY SECURITY AGENCY COMPANY

Deployed: 11 August 1966
Cover Designation: 12th Radio Research Unit
Assigned Command: 313th Army Security Agency Battalion
Supported Command: FFV–I
Location: Pleiku (Engineer Hill)
Cover Redesignation: 330th Radio Research Company on 18 July 1966
Relocated: Nha Trang on 20 May 1970
Reassigned Command: US Army Security Agency Group, Vietnam (509th RR Group) on 15 June 1971
Inactivated: 30 September 1971*
Vietnam Campaign Participation Credit: 4–15
Vietnam Honors: 4 MUCs and 1 RVN CGP
*Mission transferred to USASA Field Station, Pleiku

335th ARMY SECURITY AGENCY COMPANY

Deployed: 10 January 1967
Cover Designation: 335th Radio Research Company
Assigned Command: 303d Army Security Agency Battalion
Supported Command: 9th Infantry Division
Location: Camp Martin Cox (Bear Cat) near Long Thanh
Relocated: Dong Tam on 16 July 1968
Relocated: Di An on 28 August 1969
Reassigned Command: US Army Security Agency Group, Vietnam (509th RR Group) on 24 December 1969
Relocated: Can Tho on 24 December 1969
Inactivated: 5 April 1971*
Vietnam Campaign Participation Credit: 4–15
Vietnam Honors: 5 MUCs, 3 RVN CGP, and 1 RVN CA

* Mission and personnel transferred on 5 April 1971 to the USASA Operations Company, Can Tho.

DETACHMENT A, 358th ARMY SECURITY AGENCY COMPANY

Deployed: 19 February 1968
Cover Designation: Detachment A, 358th Radio Research Company
Assigned Command: US Army Security Agency Field Station, Phu Bai
Supported Command: 3d Brigade, 82d Airborne Division
Location: Hue-Phu Bai
Redeployed: 15 July 1968*
Vietnam Campaign Participation Credit: None**
Vietnam Honors: None

* Mission transferred to the 405th Radio Research Detachment

** Elements deployed without their headquarters elements receive no campaign credits.

403d ARMY SECURITY AGENCY SPECIAL OPERATIONS DETACHMENT

Deployed: 27 September 1966
Cover Designation: 403d Radio Research Special Operations Detachment
Assigned Command: 509th US Army Security Agency Group
Supported Command: 5th Special Forces Group
Location: Nha Trang
Inactivated: 15 December 1970
Vietnam Campaign Participation Credit: 4–14
Vietnam Honors: 1 PUC, 1 MUC, 3 RVN CGP, and 1 RVN CA

404th ARMY SECURITY AGENCY DETACHMENT

Deployed: 4 June 1965
Cover Designation: Detachment 1, 3d Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: 173d Airborne Brigade
Location: Bien Hoa
Reassigned Command: 303d Army Security Agency Battalion in May 1966
Cover Redesignation: Detachment 1, 17th Radio Research Unit in May 1966
Cover Redesignation: 404th Radio Research Detachment on 29 July 1966
Reassigned Command: 313th Army Security Agency Battalion on 1 December 1967
Relocated: Phu Hiep in February 1968
Relocated: LZ English (Bong Son) on January 69
Reassigned Command: US Army Security Agency Field Station, Pleiku on 30 September 1971
Inactivated: 1 April 1972 (zero strength 28 August 1971)*
Vietnam Campaign Participation Credit: 2–17
Vietnam Honors: 1 PUC, 6 MUCs, and 1 RVN CGP

*Residual mission transferred to 330th Radio Research Field Station on 23 July 1971

405th ARMY SECURITY AGENCY DETACHMENT

Deployed: 25 June 1965
Cover Designation: Detachment 2, 3d Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: 1st Brigade, 101st Airborne Division
Location: Bien Hoa
Inactivated: 5 November 1965
Reactivated: 15 July 1968
Cover Designation: 405th Radio Research Detachment
Assigned Command: 8th US Army Security Agency Field Station
Supported Command: 3d Brigade, 82d Airborne Division
Location: Gia Le
Reassigned Command: 303d Army Security Agency Battalion on 28 September 1968
Relocated: Phu Loi on 28 September 1968
Inactivated: 5 December 1969
Reactivated: 30 September 1971**
Cover Designation: 405th Radio Research Detachment
Assigned Command: US Army Security Agency Field Station, Bien Hoa
Supported Command: 3d Brigade, 1st Cavalry Division
Location: Phuoc Vinh–Bien Hoa
Inactivated: 30 June 1972
Vietnam Campaign Participation Credit: 2, 8–12, 15–17
Vietnam Honors: 3 MUCs and 1 RVN CA

* Assumed mission of the redeployed Detachment A, 358th ASA Company

** Assumed residual mission of the discontinued Brigade Support Detachment (Provisional).

406th ARMY SECURITY AGENCY DETACHMENT

Deployed: 27 July 1965
Cover Designation: Detachment 3, 3d Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: 1st Brigade, 101st Airborne Division
Location: Phan Rang (arrived 5 November 1965)
Reassigned Command: 313th Army Security Agency Battalion on 2 May 1966*
Cover Redesignation: Detachment 3, 13th Radio Research Unit in May 1966
Cover Redesignation: 406th Radio Research Detachment on 29 July 1966
Reassigned Command: 8th US Army Security Agency Field Station on 16 July 1968
Relocated: Camp Eagle on 16 July 1968
Inactivated: 20 November 1968**
Vietnam Campaign Participation Credit: 2–9
Vietnam Honors: 1 PUC, 1 VUA, 2 MUCs and 1 RVN CGP

* See Provisional Radio Research Company
** Residual mission transferred to 265th ASA Company.

407th ARMY SECURITY AGENCY DETACHMENT

Deployed: 10 August 1965
Cover Designation: Detachment 4, 3d Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: Field Force, Vietnam
Location: Nha Trang
Inactivated: 3 May 1966*
Deployed: 28 July 1968
Cover Designation: 407th Radio Research Detachment
Assigned Command: US Army Security Agency Field Station, Phu Bai
Supported Command: 1st Brigade, 5th Infantry Division
Location: Quang Tri Combat Base
Relocated: Dong Ha Combat Base on 31 Aug 68
Relocated: Quang Tri Combat Base (Camp Red Devil) on 12 Nov 68
Inactivated: 1 April 1972 (zero strength on 28 August 1971)**
Vietnam Campaign Participation Credit: 2–3, 8–17
Vietnam Honors: 3 MUCs and 3 RVN CGP

* Liaison mission assigned to the deployed 313th RR Bn.
** Portion of mission transferred to Detachment A, USASA Field Station, Phu Bai.

408th ARMY SECURITY AGENCY DETACHMENT

Deployed: 19 October 1966
Cover Designator: 408th Radio Research Detachment
Assigned Command: 303d Army Security Agency Battalion
Supported Command: 196th Infantry Brigade
Location: Tay Ninh
Relocated: Chu Lai as of 11 April 1967*
Reassigned Command: 313th Army Security Agency Battalion on 12 April 1967
Inactivated: 20 November 1968
Vietnam Campaign Participation Credit: 4–9
Vietnam Honors: 2 MUCs

* See Provisional Radio Research Company

409th ARMY SECURITY AGENCY DETACHMENT

Deployed: 18 August 1966
Cover Designation: 409th Radio Research Detachment
Assigned Command: 303d Army Security Agency Battalion
Supported Command: 11th Armored Cavalry Regiment
Location: Xuan Loc (Blackhorse Base Camp)
Relocated: Di An on 5 October 1969
Inactivated: 6 March 1971
Vietnam Campaign Participation Credit: 4–14
Vietnam Honors: 1 VUA, 4 MUCs, 4 RVN CGPs, and 1 RVN CA

415th ARMY SECURITY AGENCY DETACHMENT

Deployed: 22 December 1967*
Cover Designation: 415th Radio Research Detachment
Assigned Command: 313th Army Security Agency Battalion
Supported Command: 11th Infantry Brigade
Location: Chu Lai
Inactivated: 20 November 1968
Vietnam Campaign Participation Credit: 5–9
Vietnam Honors: 1 MUC

* See Provisional Radio Research Company

601st ARMY SECURITY AGENCY DETACHMENT

Deployed: 26 October 1967*
Cover Designation: 601st Radio Research Detachment
Assigned Command: 313th Army Security Agency Battalion
Supported Command: 198th Infantry Brigade
Location: Chu Lai
Inactivated: 20 November 1968
Vietnam Campaign Participation Credit: 5–9
Vietnam Honors: 1 MUC

* See Provisional Radio Research Company

856th ARMY SECURITY AGENCY DETACHMENT

Deployed: 21 November 1966
Cover Designation: 856th Radio Research Detachment
Assigned Command: 303d Army Security Agency Battalion
Supported Command: 199th Infantry Brigade
Location: Long Binh (Camp Frenzell–Jones)
Inactivated: 6 March 1971 (stood down on 24 December 1970)
Vietnam Campaign Participation Credit: 4–14
Vietnam Honors: 1 VUA, 4 MUCs, 3 RVN CGPs, and 2 RVN CAs

PROVISIONAL RADIO RESEARCH COMPANY

Organized: 10 April 1967*
Assigned Command: 313th Army Security Agency Battalion
Supported Command: Task Force OREGON
Location: Chu Lai
Supported Command: 23d Infantry Division (Americal) on 25 September 1967
Redesignated: Americal Radio Research Company (Provisional) on 7 October 1967**
Discontinued: 20 November 1968***

*Formed from the 406th and 408th ASA Detachments and Detachment 2, 374th ASA Company.
**Formed from the 408th, 415th, and 601st ASA Detachments.
***Mission transferred to the 328th ASA Company on 20 November 1968.

BRIGADE RADIO RESEARCH DETACHMENT (PROVISIONAL)

Organized: 3 April 1971*
Assigned Command: 303d Army Security Agency Battalion
Supported Command: 3d Brigade, 1st Cavalry Division
Location: Bien Hoa
Reassigned Command: US Army Security Agency Operations Company, Bien Hoa on 15 June 1971
Discontinued: 30 September 1971**

* Mission received from inactivated 371st ASA Company.
** Mission transferred to the newly activated 405th ASA Det.

8th US ARMY SECURITY AGENCY FIELD STATION

Organized: 1 November 1964*
Cover Designation: 8th Radio Research Unit
Assigned Command: 53d US Army Security Agency Special Operations Command (3d RRU)
Supported Command: MACV and MAF
Location: Phu Bai
Reassigned Command: 509th US Army Security Agency Group on 1 June 1966
Redesignation: US Army Security Agency Field Station, Phu Bai on 15 December 1967
Cover Redesignation: 8th Radio Research Field Station
Supported Command: MACV and XXIV Corps on 14 April 1971**
Supported Command: MACV and FRAC on 19 March 1972***
Relocated: Da Nang on 1 November 1972
Discontinued: 26 February 1973
Vietnam Campaigns: 1–17
Vietnam Decorations: 3 MUCs, 1 RVN CGP, and 1 RVN CA

* Replaced Det J, 3d RRU.
**Upon Departure of the MAF.
***Upon Departure of the XXIV Corps.

82d US ARMY SECURITY AGENCY SPECIAL OPERATIONS UNIT

Organized: 20 September 1961*
Cover Designation: 3d Radio Research Unit
Assigned Command: US Army Security Agency Pacific
Supported Command: MAAG–V and MACV
Location: Saigon
Redesignation: 53d US Army Security Agency Special Operations Command on 1 November 1964
Discontinued: 1 June 1966**
Vietnam Campaigns: 1–3
Vietnam Decorations: 2 MUCs***

*Replaced the 400th USASA Unit (Prov).
**Command mission transferred to the 509th USASA Gp.
***Detachment J, 3d Radio Research Unit received 1 MUC; 1st Team, 3d RRU received 1 PUC; and 2d Team, 3d RRU received 1 PUC.

101st US ARMY SECURITY AGENCY SECURITY DETACHMENT

Organized: 1 March 1963
Cover Designation: 7th Radio Research Unit
Assigned Command: 82d US Army Security Agency Special Operations Unit
Supported Command: MACV and USARV
Location: Saigon
Reassigned Command: 509th US Army Security Agency on 1 June 1966
Cover Redesignation: 101st Radio Research Company on 10 September 1966
Redesignation: USASA Security Company, Saigon on 15 December 1967
Relocation: Long Binh on 30 March 1970
Relocation: Saigon on 16 March 1971
Discontinued: 1 April 1972
Vietnam Campaigns: 1–17
Vietnam Decorations: 4 MUCs and 1 RVN CGP

175th US ARMY SECURITY AGENCY COMPANY

Organized: 1 June 1966
Cover Designation: 175th Radio Research Company
Assigned Command: 303d Army Security Agency Battalion
Supported Command: MACV and FFV–II
Location: Saigon
Relocation: Bien Hoa on 3 July 1967
Redesignation: US Army Security Agency Operations Company, Bien Hoa on 15 December 1967*
Supported Command: MACV and TRAC as of 30 April 1971
Redesignation: US Army Security Agency Field Station, Bien Hoa on 30 September 1971**
Cover Redesignation: 175th Radio Research Field Station
Reassigned Command: US Army Security Agency Group, Saigon on 30 September 1971
Relocation: Saigon on 29 September 1972
Discontinued: 26 February 1973
Vietnam Campaigns: 3–17
Vietnam Decorations: 5 MUCs, 1 RVN CGP, and 1 RVN CA

*The original redesignation order read US Army Security Operations Company, Saigon
**The Radio Research Field Station, Bien Hoa (Provisional) was in existence from 1 May 1971 to 30 September 1971.

400th US ARMY SECURITY AGENCY UNIT (PROVISIONAL)

Organized: 23 May 1961
Cover Designation: 3d Radio Research Unit
Assigned Command: US Army Security Agency Pacific
Supported Command: MAAG–V
Location: Saigon
Discontinued: 20 September 1961*

*Mission and personnel transferred to the 82d USASA Special Operations Unit.

509th US ARMY SECURITY AGENCY GROUP

Organized: 1 June 1966
Cover Designation: 509th Radio Research Group
Supported Command: MACV and USARV
Assigned Command: USASA Pacific
Location: Saigon
Redesignation: US Army Security Group, Vietnam on 15 December 1967
Discontinued: 7 March 1973
Vietnam Campaigns: 3–17
Vietnam Decorations: 3 MUCs and 2 RVN CGP

US ARMY SECURITY AGENCY FIELD STATION, PLEIKU*

Organized: 30 September 1971**
Cover Designation: 330th Radio Research Field Station
Assigned Command: US Army Security Agency Group, Vietnam
Supported Command: MACV and SRAC
Location: Nha Trang
Discontinued: 1 September 1972
Vietnam Campaigns: 15–17
Vietnam Decorations: None

*The planned relocation to Pleiku never took place.

**USASA Field Station, Pkeiku (Provisional) in existence from 1 May to 30 September 1971.

US ARMY SECURITY AGENCY COMPANY, CAN THO

Organized: 5 April 1971*
Cover Designation: 335th Radio Research Company
Assigned Command: US Army Security Agency Group, Vietnam
Supported Command: Delta Regional Assistance Command
Location: Can Tho
Discontinued: 30 June 1972
Vietnam Campaigns: 14–17
Vietnam Decorations: None

* Residual mission of the inactivated 335th ASA Company.

US ARMY SECURITY AGENCY COMMUNICATIONS UNIT, VIETNAM

Organized: 1 June 1966
Cover Designation: 18th Radio Research Unit
Assigned Command: 509th US Army Security Agency Group
Supported Command: 509th US Army Security Agency Group
Location: Saigon
Cover Redesignation: Radio Research Communications Unit, Vietnam on 2 September 1966
Discontinued: 31 January 1973
Vietnam Campaigns: 3–17
Vietnam Decorations: 3 MUCs and 1 RVN CGP

Appendix C

Key ASA Personnel

US Army Security Agency

MG William M. Breckinridge	1 Apr 60–31 May 62
BG Orman G. Charles	1 Jun 62–30 Jun 62
MG William H. Craig	1 Jul 62–7 Sep 65
BG Dayton W. Eddy	8 Sep 65–14 Sep 65
MG Charles Denholm	15 Sep 65–4 Feb 73

US Army Security Agency, Pacific

COL Robert T. Walker	15 May 60–16 Jun 61
COL George A. Godding	16 Jun 61–23 May 64
COL Robert P. Brust	30 Jul 64–21 Jan 67
COL Edgar F. Hoffman	21 Jan 67–19 Oct 67
BG George A. Godding	20 Oct 67–24 Jun 69
COL Arthur W. Hackwood	25 Jun 69–25 Aug 70
BG Herbert E. Wolff	26 Aug 70–16 Nov 72

3d Radio Research Unit

LTC Robert W. Williams	23 May 61–10 Aug 61
LTC William J. Cochrane	11 Aug 61–8 Jul 63
LTC Thomas S. Owen	9 Jul 63–7 Dec 64
COL William M. Hamilton	8 Dec 64–27 Nov 65
COL Clayton C. Swears	28 Nov 65–1 Jun 66

509th Radio Research Group

COL Clayton C. Swears	1 Jun 66—17 Nov 66
COL John J. McFadden	17 Nov 66–18 Oct 67
COL William T. Riley	18 Oct 67–19 Sep 68
COL Allen J. Mauderly	20 Sep 68–5 Apr 69
COL Richard A. Grodin	6 Apr 69–21 Sep 69
COL William W. Higgins	21 Sep 69–18 Aug 70
COL Jack P. Lansford	18 Aug 70–6 Aug 71
COL George R. Hamer	6 Aug 71–1 Aug 72
COL Marion E. White	2 Aug 72–7 Mar 73

224th Aviation Battalion (Radio Research)

MAJ John D. Rieser	1 Jun 66–31 Jul 66
MAJ Donn E. Taylor	Aug 66—Aug 66
LTC Richard A. Rusk	Aug 66–Aug 67
LTC George W. Cadmus	Aug 67–4 Aug 68
LTC Jimmie King	5 Aug 68–24 Jul 69
LTC John P. Brown	25 Jul 69–12 Jul 70
LTC Robert Swanson	12 Jul 70–22 Jun 71
LTC David Richards	22 Jun 71–1 Jun 72
MAJ Gerald E. Lethcoe, Jr.	1 Jun 72–20 Nov 72
MAJ Charles S. Simerly	21 Nov 72–5 Dec 72
LTC James M. Henderson, Jr.	5 Dec 72–3 Mar 73

303d Radio Research Battalion

LTC John J. Masters	8 Jul 64–13 Apr 67
LTC Norman J. Campbell	29 Apr 67–12 Apr 68
LTC Robert W. Price	13 Apr 68–16 Nov 68
LTC William O. Roscher	16 Nov 68–30 Jun 69
LTC James E. Freeze	1 Jul 69–4 Jun 70
LTC Claude E. Vannoy	5 Jul 70–7 Jan 71
LTC Donald E. Grant	8 Jan 71–15 Jun 71

313th Radio Research Battalion

LTC Russell B. Jones, Jr.	15 Jan 65–15 Aug 66
LTC Charles B. Ablett	15 Aug 66–21 Dec 66
LTC Stanley G. Kozlowski	21 Dec 66–26 Jun 67
LTC Richard L. Jones	26 Jun 67–4 Feb 68
LTC George E. Strickland	5 Feb 68–4 Aug 68
LTC James F. Morris, Jr.	5 Aug 68–21 Jun 69
LTC Andrew E. Little	21 Jun 69–5 Dec 69
LTC Joseph J. Muhlherr	6 Dec 69–6 Aug 70
LTC David A. Wisyanski	6 Aug 70–15 Jun 71

8th Radio Research Field Station

MAJ George T. Shearin	1 Nov 64–25 Feb 65
COL Joseph Goldenberg	25 Feb 65–Feb 66
COL Richard A. McMahon	13 Feb 66–Feb 67
COL George F. Garrant	9 Feb 67–19 Jan 68
COL Allen J. Mauderly	20 Jan 68–5 Mar 68
LTC Robert F. Von Dach	6 Mar 68–7 Feb 69
LTC Kenneth F. Coykendall	8 Feb 69–17 Sep 69
LTC Forrest G. Fultz	18 Sep 69–8 Dec 69
LTC Gerald M. Dirkx	9 Dec 69–18 May 70
MAJ Joseph F. Short	18 May 70–18 Jun 70
LTC Eugene S. Sanford	18 Jun 70–8 Sep 70
LTC Nathaniel Alderman, Jr.	9 Sep 70–25 Aug 71
COL Louis W. Powers	25 Aug 71–16 Aug 72
COL Stanley G. Kozlowski	17 Aug 72–31 Oct 72
MAJ Kenneth G. Neiman	1 Nov 72–26 Feb 73

330th Radio Research Field Station

LTC David A. Wisyanski	15 Jun 71–18 Jul 71
LTC Horace S. Kelley	19 Jul 71–22 Jun 72
MAJ Robert J. Adams	23 Jun 72–30 Jul 72

175th Radio Research Field Station

LTC Donald E. Grant	Jun 71–Dec 71
LTC Thomas J. Flynn	Dec 71–Sep 72
MAJ Charles G. Burke	Oct 72–Feb 73

Appendix D

Fallen in Battle

SP4 James T. Davis	22 Dec 61	3d RRU
PFC Donald R. Taylor	9 Feb 64	3d RRU
SP4 Arthur W. Glover	9 Feb 64	3d RRU
SSG Robert F. Townsend	4 Nov 65	371st RR Co
SSG Donald D. Daugherty	13 Apr 66	3d RRU
CPT James D. Stallings	25 Sep 66	337th RR Co
1LT John F. Cochrane	24 Oct 66	409th RR Det
SFC John F. Stirling	8 Mar 67	335th RR Co
SFC Robert D. Taylor	26 Nov 67	335th RR Co
SGT Diego Ramirez, Jr.	26 Nov 67	335th RR Co
SP5 Michael P. Brown	26 Nov 67	335th RR Co
CPT John M. Casey	25 Mar 68	371st RR Co
SP4 Christopher J. Schramm	13 May 68	371st RR Co
SP4 Jeffrey W. Haerle	13 May 68	TDY
SP5 Samuel C. Martin	17 May 68	101st RR Co
SGT Thomas J. Tomczak	23 Jul 68	403d RR SOD
SP5 Harold D. Biller	25 Feb 69	175th RR Co
SP5 Harry J. Colon	21 Jun 69	409th RR Det
SP4 James R. Smith	29 Nov 69	371st RR Co
PFC Henry N. Heide, II	29 Nov 69	371st RR Co
SP4 Robert E. Dew	30 Aug 70	330th RR Co
SP5 Carl H. Caccia	21 Feb 71	404th RR Det
SP5 Robert J. Thelen	21 Feb 71	404th RR Det
SGT Robert J. Potts	21 Feb 71	404th RR Det
SP5 Mitchell B. Smith	21 Feb 71	404th RR Det
SP5 Gary C. David	1 Mar 71	371st RR Co
SP4 Frank A. Sablan	1 Mar 71	371st RR Co
CPT Michael W. Marker	4 Mar 71	138th Avn Co
CW1 Harold L. Algaard	4 Mar 71	138th Avn Co
SP5 Richard J. Hentz	4 Mar 71	138th Avn Co
SP5 Rodney D. Osborne	4 Mar 71	138th Avn Co
SP6 John T. Strawn	4 Mar 71	138th Avn Co
SP5 Gary P. Westcott	30 Mar 72	8th RR Fld Sta
SP4 Bruce A. Crosby, Jr.	30 Mar 72	8th RR Fld Sta

Appendix E
Airborne Systems

Beaver (U–6A)	Mar 62–Mar 72	HF DF
Seminole (U–8D/8F)	Jan 63–Feb 73	HF DF
PATHFINDER Caribou (CV–2B)	Jan 66–Apr 67	HF/VHF DF/Collection[1]
HAPPY NIGHTS/CAFÉ GIRL Otter (U–1A)	Mar 67–Jan 71	HF DF/Collection[2]
CRAZY CAT/CEFLIEN LION Neptune (P–2E)	Jun 67–Apr 72	HF/VHF ECM/Collection[3]
LEFT BANK Huey (UH–1D/1H)	Aug 67–Jun 72	HF DF RFP/Collection[4]
LAFFING OTTER Otter (U–1A)	Dec 67–Jan 71	HF DF/Collection
HOMING PIGEON Mohawk (OV–1C)	Jun 68–Sep 69	VHF DF
LAFFING EAGLE Ute (U–21D)	Dec 68–Feb 73	HF/VHF DF/Collection[5]
LEFT JAB Ute (U–21A)	Dec 70–Feb 73	VHF DF/Collection

[1] Used only in HF

[2] Configured as a LAFFING OTTER by 1970

[3] Used only in collection capacity

[4] RFP/Collection positions removed in 1970

[5] Not used in HF DF until Oct 70 and never in VHF

Appendix F
Chronology

29 Apr 61	Presidential decision approves ASA COMINT effort in South Vietnam.
13 May 61	3d RRU arrives at Ton Son Nhut AFB—the first Army unit to be deployed.
15 May 61	WHITEBIRCH Phase of operations begins with manual Morse coverage.
27 Jun 61	3d RRU intercept vans move to ARVN compound, Trai Tran Hung Dao.
29 Jun 61	WHITEBIRCH DF Net becomes fully operational.
Aug 61	Mobile AN/PRD–1 DF teams are deployed.
4 Sep 61	3d RRU personnel conduct SABERTOOTH class for ARVN SIGINT specialists.
22 Dec 61	SP4 James T. Davis is killed in ambush while advising ARVN DF team.
Jan 62	3d RRU conducts joint mission with ARVN counterpart.
27 Jan 62	3d RRU personnel complete their first COMSEC monitoring mission.
Mar 62	First ARDF platform (U–6) arrives in Vietnam.
Apr 62	3d RRU moves to new quarters at Ton Son Nhut AFB, named in memory of SP4 James T. Davis.
27 May 62	ARDF results in a major tactical success.
28 Jun 62	3d RRU occupies Phu Bai as a DF site.
Jan 63	A U–8 aircraft equipped with ARDF capability becomes operational. The twin–engine aircraft gives the 3d RRU an all-weather capability.
1 Mar 63	Newly organized 7th RRU assumes responsibility for COMSEC mission.

14 May 63	3d RRU awarded Meritorious Unit Commendation, the first unit to be so honored in Vietnam.
4 Aug 64	Phu Bai warns of imminent danger in Gulf of Tonkin.
1 Nov 64	Det J, 3d RRU at Phu Bai is replaced by a field station (8th RRU).
9 Jun 65	First Direct Support Unit (the 404th ASA Det) arrives in country.
Jun 65	Vietnamese born linguists, DANCERS, are used by the 3d RRU as transcribers.
Aug 65	ASA units prove a key factor in the first large-scale battle involving US forces (Operation STARLIGHT). ARDF deploys in a direct support mode during battle.
Jan 66	The Nestor series of secure voice equipment is introduced in the field.
Mar–Apr 66	303d and 313th ASA Battalions arrive to support Field Forces.
1 Jun 66	3d RRU is replaced by the 509th RR Group. The 224th Avn Battalion is activated to assume responsibility for airborne mission.
1 Jul 66	ARDF Coordination Center is created to manage Air Force/Army ARDF missions.
27 Sep 66	403d RR SOD arrives to support the 5th Special Forces Group.
Oct 66	330th RR Co is named Collection Management Authority for II CTZ and the 175th RR Co for III CTZ.
Oct 66	ARDF indicates the presence of 325th NVA Division within South Vietnam.
17 Apr 67	Project MUSTARD (Wideband intercept) is inaugurated at the 330th RR Co.
29 Jun 67	CEFLIEN LION (EW) platforms arrive.
Jul 67	LEFTBANK heliborne DF platform becomes operational.
Jan 68	Direct Support Units received authority to issue their own tactical reports (TACREP) which allowed for passing of perishable information in a sanitized format.
23 Feb 68	8th RR Field Station at Phu Bai assumes control of Direct Support Units for the first time.
29 Mar 68	CEFLIEN LION platforms flown by 1st RR Co begins airborne collection.
May 68	Initial steps taken by COMSEC specialists to move away from monitoring and to begin to emphasize advice and assistance role.
15 Jun 68	Processing and Analysis Section is established at the 509th RR Group to look at country-wide analytical problems.
28 Jan 69	LAFFING EAGLE U–21 aircraft arrives and becomes operational.
13 Apr 69	Deployment of the experimental Tactical Automated Data Processing System signals the increased use of computers in the field.
1 Jul 69	ARVN Special Technical Detachments are organized.
15 Oct 69	SSG Donna P. Baldwin becomes first WAC to be assigned to the 509th RR Group.
20 Dec 69	Project TOUCHDOWN exploits capture of an NVA COMINT Intercept Team.
24 Dec 69	335th RR Company moves to Can Tho and assumes responsibility as the CMA to the Delta.
Feb 70	RATRACE Team deploys to Ben Luc to provide analytical and transcription assistance.
3 May 70	During the Cambodian Incursion, LEFT BANK platform produces information leading to the discovery of "The City," a large logistics center.

4 May 70	First ASA unit (the 409th RR Detachment) enters Cambodia to perform low-level voice intercept.
10 Jun 70	Project EXPLORER becomes operational on Hill 950.
31 Jul 70	The Division Advisors Radio Research Support (DARRS) Detachments are established.
Oct 70	Installation of the ARD–23 V–Scan on the LAFFING EAGLE platforms represents major upgrade in Army ARDF.
13 Nov 70	The Vietnamization Improvement and Modernization Plan is formally implemented to begin shifting the fighting responsibilities to the ARVN.
8 Jan 71	LEFT JAB airborne platform becomes operational.
Apr 71	303d and 313th RR Battalions redeploy to CONUS.
1 May 71	Field stations are organized at Bien Hoa and Nha Trang.
Jul 71	Center Advisory Radio Research Support (CARRS) Detachments are established at the South Vietnamese SIGINT centers.
30 Mar 72	Two members of the 8th RR Field Station killed by incoming rockets. Their deaths brought the total ASA soldiers killed in action to 34.
1 Apr 72	101st RR Company is discontinued, effectively ending the 509th RR Group's COMSEC mission.
30 Jun 72	328th RR Company and the 405th RR Detachment represents the last of the Direct Support Units to be either inactivated or redeployed.
Feb 73	8th and 175th, the last of the field stations, are discontinued.
16 Feb 73	A U–21 LEFT JAB crew flies last ARDF mission for the Army.
7 Mar 73	509th RR Group is discontinued, ending ASA's 12-year presence in South Vietnam.

Appendix G

Acronyms

Abn	airborne
AC	armored cavalry
ACC	ARDF Coordination Center
ACSI	Assistant Chief of Staff for Intelligence
AFB	Air Force Base
Am	Americal
ARDF	Airborne Radio Direction-Finding
Armd	Armored
ARVN	Army, Republic of Vietnam
ASA	Army Security Agency
ASTD	ARVN Special Technical Detachments
Avn	aviation
Bn	battalion
CAAT	COMSEC Advice and Assistance Team
CARRS	Center Advisory Radio Research Support
Cav	cavalry
CDR	commander
CG	commanding general
CMA	Collection Management Authority
COL	colonel
Comm	communications
COMINT	communications intelligence
COMUSMACV	Commander, US Military Assistance Command, Vietnam
COMSEC	communications security
CONUS	continental United States
CORRECT	COMSEC Role Recast

CPT	captain
CTZ	corps tactical zone
DARRS	Division Advisors Radio Research Support
DDRE	Director of Defense Research and Engineering
Det	detachment
DF	direction-finding
DIRNSA	Director, NSA
DITS	DANCERS in the sky
DMZ	demilitarized zone
DOD	Department of Defense
DRAC	Delta Regional Assistance Command
DSU	direct support unit
ECM	electronic countermeasures
ECOM	US Army Electronic Command
ELINT	electronic intelligence
EW	electronic warfare
FFV	Field Force, Vietnam
FS	field station
FSB	fire support base
HF	high frequency
HQ	headquarters
GEN	general
GP	group
Inf	infantry
JGS	Joint General Staff
LLVI	low-level voice intercept
LT	lieutenant
LTC	lieutentant colonel
LTG	lieutenant general
MAAG–V	Military Assistance Advisory Group, Vietnam
MAC–SOG	Military Assistance Command-Studies and Observation Group
MACV	Military Assistance Command, Vietnam
MAF	Marine Amphibious Force
MG	major general
MR	Military Region
MUC	Meritorious Unit Commendation
MRDF	medium range direction-finding
NCOIC	noncommissioned officer in charge
NSA	National Security Agency
NVA	North Vietnamese Army
Off	officer
Ofc	office
Op	Operations
OPLAN	operation plan
Plt	platoon
Prov	provisional
PUC	Presidential Unit Citation
RFP	radio fingerprinting
RR	radio research
RRCUV	RR Communications Unit, Vietnam
RRU	RR Unit
RVN	Republic of Vietnam
RVN CA	RVN Civil Action
RVN CGP	RVN Cross of Gallantry with Palm
Scty	security
SF	Special Forces
SFC	Sergeant First Class
SI	special intelligence
SIT	special identification techniques
SOC	special operations command
SOD	special operations detachment
SP	specialist
SRAC	Second Regional Assistance Command
SPAR	special agent report
SRDF	short range direction-finding
SSO	Special Security Office (Officer)
TACREP	tactical report
TAREX	target exploitation
TDY	temporary duty
TRAC	Third Regional Assistance Command
VC	Viet Cong
US	United States
USA	US Army
USAF	US Air Force
USARV	US Army, Vietnam
USASA	US Army Security Agency
USASAPAC	USASA, Pacific
VHF	very high frequency
WAC	Women's Army Corps

Appendix H

Unit Insignia

Because of security considerations, ASA personnel in Vietnam were not allowed to wear the agency's official shoulder sleeve insignia or its distinctive unit insignia. However, personnel from each of the battalions were authorized and did wear their own unit crests. At the same time, there were many unofficial "beer can" insignia, so called because of the aluminum metal used by local Vietnamese vendors to manufacture them. What follows are representative of the various official and unofficial (unless otherwise noted) insignia carried by various ASA units from time-to-time.

224th Avn Battalion
(authorized)

303d ASA Battalion
(authorized)

313th ASA Battalion
(authorized)

1st RR Company

3d RR Unit

3d RR Unit
(Davis Station)

Det J, 3d RRU

8th RR Field Station

101st RR Company

144th Avn Company

146th Avn Company

156th Avn Company

175th RR Company

265th RR Company

303d RR Battalion

335th RR Company

371st RR Company

509th RR Group

Communications Unit, Vietnam

ASA Distinctive Unit Insignia
(authorized but not worn)

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

ISBN 0-16-051284-0

ISBN 0-16-051284-0

"It is always easy for the people to see the performance of an infantry battalion or brigade in fighting and winning the battle. The performance of a support unit is not so obvious, and yet in your case [303d RR Battalion that supported the II FFV], you have probably contributed to the winning of more battles than any maneuver element in the country."

LTG Frederick C. Weyland, Commanding General, II Field Force Vietnam

UNIVERSITY OF FLORIDA
3 1262 09682 5152

FLAME

ARMY · LINEAGE · SERIES

MILITARY INTELLIGENCE

John Patrick Finnegan
Romana Danysh

MILITARY INTELLIGENCE

Military Intelligence Corps
Regimental Insignia

ARMY LINEAGE SERIES

MILITARY INTELLIGENCE

John Patrick Finnegan

Lineages Compiled by
Romana Danysh

Center of Military History
United States Army
Washington, D.C., 1998

Library of Congress Cataloging-in-Publication Data

Finnegan, John Patrick.
Military intelligence / John Patrick Finnegan ; lineages compiled by Romana Danysh.
p. cm. — (Army lineage series)
Includes bibliographical references and index.
1. Military intelligence—United States—History. 2. United States. Army—History. I. Danysh, Romana, 1940– . II. Title. III. Series.
UB256.U6F56 1997
355.3'432'0973—dc21 96–44554
CIP

CMH Pub 60–13

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328
ISBN 0-16-048828-1

ARMY LINEAGE SERIES

Jeffrey J. Clarke, General Editor

Advisory Committee
(As of 24 October 1997)

Joseph T. Glatthaar
University of Houston

Edward W. Arnold
Office of the Deputy
Chief of Staff for Personnel

Raymond Callahan
University of Delaware

Maj. Gen. James J. Cravens, Jr.
U.S. Army Training and
Doctrine Command

Lt. Col. Carlo D'Este
U.S. Army, Retired

Col. Robert A. Doughty
U.S. Military Academy

George C. Herring
University of Kentucky

Michael J. Kurtz
National Archives

Col. Jerry D. Morelock
U.S. Army Command and
General Staff College

Carol A. Reardon
Pennsylvania State University

Col. Everett L. Roper, Jr.
U.S. Army War College

John Shy
University of Michigan

Mark A. Stoler
University of Vermont

Gerhard L. Weinberg
University of North Carolina

U.S. Army Center of Military History

Brig. Gen. John W. Mountcastle, Chief of Military History

Chief Historian
Chief, Field Programs and Historical
Services Division
Editor in Chief

Jeffrey J. Clarke

John T. Greenwood
John W. Elsberg

Foreword

Intelligence has been defined as the art of "knowing one's enemies," and military intelligence is as old as war itself. However, the development of an intelligence organization within the United States Army is comparatively recent. The Army did not acquire a permanent peacetime intelligence organization until 1885, and the oldest of today's military intelligence units can trace its lineage only back to the eve of World War II. The Army did not formally recognize intelligence as a distinct professional discipline until 1962, when it finally created the Army Intelligence and Security Branch, the predecessor of today's Military Intelligence Branch. The Military Intelligence Corps, which incorporated all military intelligence personnel and units into a single large regiment, did not come into existence until 1987.

Although the intelligence organization within the U.S. Army was slow to develop, it has become increasingly important both as a combat multiplier in war and as a source of information for the nation's decision makers in peace. As the nation and its Army move into an information age, military intelligence will assume an even greater significance.

To tell the military intelligence story in as much detail as security regulations currently in force allow, the U.S. Army Center of Military History has worked in collaboration with the U.S. Army Intelligence and Security Command (INSCOM) to produce this volume of the Army Lineage Series. It is intended both to bring a relatively unknown part of the Army heritage to the attention of the general public and to foster unit esprit de corps among the thousands of military intelligence specialists now serving in the ranks of America's Army.

ROBERT W. NOONAN, Jr.
Major General, USA
Commanding
U.S. Army Intelligence and
Security Command

JOHN W. MOUNTCASTLE
Brigadier General, USA
Chief of Military History

The Authors

John Patrick Finnegan graduated magna cum laude from Boston College in 1957 with an A.B. in English Literature. After a period of civilian employment with the National Security Agency and military service in the U.S. Army Counter Intelligence Corps, he went on to receive a Ph.D. in Twentieth Century American History from the University of Wisconsin–Madison. Before accepting his present position as historian with the U.S. Army Intelligence and Security Command, Dr. Finnegan taught at several American universities and at the University of Ibadan, Nigeria, and worked as a military historian at the U.S. Army Center of Military History. He is the author of *Against the Specter of a Dragon: The Campaign for American Military Preparedness, 1914–1917*, *Military Intelligence: A Picture History*, and *The Military Intelligence Story: A Photo History*, as well as coeditor of *U.S. Army Signals Intelligence in World War II: A Documentary History*.

Romana Danysh graduated from Barnard College in 1962 and received her M.A. degree in history from Stanford University in 1963. Since 1964 she has served as a historian at the U.S. Army Center of Military History. Ms. Danysh is coauthor of *Infantry, Part I: Regular Army*, a volume in the Army Lineage Series.

Preface

This book attempts to present an organizational history of Military Intelligence in the United States Army from its beginnings to the present. It makes no pretense at discussing the operational aspects of intelligence in detail, partially due to the continuing need to safeguard intelligence sources and methods. Furthermore, the book focuses its attention on the Army and necessarily slights the complex interrelationships between Army intelligence and other organizations in the intelligence community. Finally, although the book includes the lineages and heraldic items of military intelligence brigades, groups, and battalions organized under tables of organization and equipment (TOEs), it does not cover the numerous intelligence units, past and present, organized for one-of-a-kind missions under tables of distribution and allowances (TDAs).

Preparation of this volume has been a collaborative effort between the U.S. Army Center of Military History (CMH) and the U.S. Army Intelligence and Security Command (INSCOM). John Patrick Finnegan, Military History Office, INSCOM, wrote the narrative text. Romana Danysh, Organizational History Branch, CMH, compiled the lineages.

Both authors owe large debts to numerous individuals. The idea of preparing an organizational history was conceived by James L. Gilbert, INSCOM Command Historian; Janice E. McKenney, Chief of the Organizational History Branch, CMH, was instrumental in bringing about its publication as part of the Army Lineage Series. The introductory text owes much to those who took the time and trouble to compose unit histories, as well as to the former historians of the U.S. Army Intelligence Center, the U.S. Army Security Agency, the U.S. Army Intelligence Command, and the Office of the Assistant Chief of Staff for Intelligence. Lt. Col. Marc Powe's thesis on the evolution of the Military Intelligence Division from 1885 to 1917 served as a basic building block for the monograph, as did Col. Bruce Bidwell's unpublished eight-volume manuscript on the development of military intelligence from the founding of the republic to 1953. The unpublished thirty-volume history of the Counter Intelligence Corps which Maj. Ann Bray and others prepared in the late 1950s also contained a

wealth of information. Finally, preparation of the narrative would have been impossible without the research assistance provided by the library and archival staffs of the National Archives and Records Administration, the U.S. Army Military History Institute, the Library of Congress, the National Security Agency, the U.S. Army Cryptologic Records Center, the Pentagon Library, and the Center of Military History.

Special thanks are due to the individuals who served on the panel that reviewed and commented on the first draft of the narrative. These include Brig. Gen. James L. Collins, U.S. Army (Retired), former Chief of Military History; Romana Danysh, Morris J. MacGregor, Jr., Janice E. McKenney, and John B. Wilson of CMH; Dianne Putney of the U.S. Air Force History Office; and Col. James W. Dunn, U.S. Army (Retired), of the Corps of Engineers History Office. Others who provided a valuable critique include David F. Trask and Robert K. Wright, Jr., of CMH; Dean Allen of the Defense Intelligence Agency History Office; Bruce Saunders, formerly with the History Office, U.S. Army Intelligence Center and School; and Henry Schorreck, formerly with the National Security Agency's History Office. Jeffrey J. Clarke, the Army's present Chief Historian, devoted considerable time and energy to polishing the final version of the manuscript. Over the years, a succession of INSCOM commanders have encouraged the project of compiling an organizational history, while former INSCOM Chief of Staff Malcolm L. Hollingsworth provided steady support.

In addition to the narrative history, this volume features lineages and heraldic data for 108 military intelligence units—13 brigades, 10 groups, and 85 battalions. They comprise all active and inactive Regular Army and Army Reserve TOE units as well as all federally recognized Army National Guard TOE units as of 30 June 1996. We did not include smaller units, such as companies and detachments, because they are not authorized their own heraldic items. However, former separate companies and detachments perpetuated by brigades, groups, or battalions are covered in the relevant lineages. No TDA units of any size are included because, in accordance with longstanding Army policy, lineage and honors are determined for TOE units only.

The Organizational History Branch of CMH is responsible for determining and publishing the official lineage and honors of Army units. The lineages in this volume are the result of research done by many past and present members of the branch, including John Finnegan. Romana Danysh prepared all the lineages for publication and updated them to reflect significant organizational changes, campaign participation credit, and unit decorations through 30 June 1996.

Each lineage is adapted from the unit's official Lineage and Honors Certificate, which outlines the history of the unit in a highly stylized format and constitutes its birth certificate, its deed to organizational properties, and verification of its service record. Although we have compressed the lineage and honors data in this book to save space, the information is the same as that on the certificates, which accounts for the technical language used. The glossary at the

end of the volume will assist readers unfamiliar with lineage terms. The parenthetical entries after each unit decoration refer to the general orders announcing the awards.

Descriptions of coats of arms, shoulder sleeve insignia, and distinctive unit insignia approved for the units appear with the lineages. These descriptions as well as the color illustrations and the brief account of heraldic items were furnished by The Institute of Heraldry (TIOH). The authors are particularly grateful to Gerald T. Luchino, Thomas B. Proffitt, Nuala Barry, and James M. Hammond for their expert assistance in providing the heraldic material for this book. We also want to express our very special thanks to the late Ronald E. Dudley, an alumnus of both TIOH and CMH, who volunteered to type the heraldic data in the appropriate format for publication. In some instances, the text relating to the heraldic items is not as comprehensive as in the original letters of approval, amendment, or redesignation sent to the units. Minor changes have been made to meet the need for brevity.

Although previous volumes in the Army Lineage Series had individual unit bibliographies, the scarcity of open-source literature on military intelligence units made such an approach impracticable. Very few histories of intelligence units have been published, and historical reports submitted by intelligence organizations generally have been classified. The files of the INSCOM History Office contain information on selected units and installations. Some intelligence histories are also included in the large unit history collection maintained by the U.S. Army Military History Institute at Carlisle Barracks, Pennsylvania. In addition, the *Military Intelligence Professional Bulletin*, a quarterly publication of the U.S. Army Intelligence Center and Fort Huachuca, regularly features thumbnail sketches of various military intelligence units.

Photographic support for this volume was provided by T. Gardner, Sr., and Robert J. Bills, contractors working for the Assistant Chief of Staff, G–6, INSCOM. At CMH, John W. Elsberg, Arthur S. Hardyman, Catherine A. Heerin, Diane M. Donovan, the late Rae Panella, Joycelyn M. Canery, and John Birmingham all participated in the various aspects of producing the book.

As indicated, the efforts of a great many people contributed to the production of this volume of the Army Lineage Series. However, any mistakes, errors, or omissions are solely the responsibility of the authors.

JOHN PATRICK FINNEGAN
U.S. Army Intelligence and
Security Command

ROMANA DANYSH
U.S. Army Center of
Military History

Contents

Chapter	*Page*
Introduction	3
1. The Beginnings	7
Military Intelligence in Place	12
Military Intelligence in the Twentieth Century	15
2. World War I	21
Van Deman and Military Intelligence	22
Intelligence Operations	24
The Corps of Intelligence Police	26
Expansion	27
The Military Intelligence Division	31
The American Expeditionary Forces in France	32
Communications Security in the AEF	37
Sideshows	38
Conclusion	39
3. Military Intelligence Between Wars	41
Military Intelligence at Peace	42
The "Black Chamber" and the Signal Intelligence Service	46
4. Military Intelligence in Crisis	51
1941: MID on the Brink	55
Counterintelligence Concerns	57
The Road to Pearl Harbor	58
5. World War II: Military Intelligence at the Center	61
The Reorganization of Military Intelligence	63
The ULTRA Breakthrough	68
The Counter Intelligence Corps	72

Chapter *Page*

The Signal Security Agency . . . 77
Communications Security . . . 81
The Electronic Battlefield . . . 82
Summation . . . 83

6. World War II: Intelligence in the Field . . . 85
Europe . . . 86
The Pacific . . . 93
Common Collectors . . . 97
Conclusion . . . 98

7. The Cold War and Korea . . . 101
Restructuring Military Intelligence . . . 102
Postwar Operations: Human Intelligence and Counterintelligence . . . 105
The Army Security Agency . . . 109
Postwar Military Intelligence: Deficiencies . . . 111
Korea . . . 113
Summation . . . 118

8. From Korea to Vietnam . . . 121
Military Intelligence at the Center: The 1950s . . . 122
Reshaping the Tools . . . 124
The Army Security Agency . . . 127
Military Intelligence in the Field . . . 130
Intelligence Support to the Theaters . . . 133
The McNamara Revolution . . . 136
The U.S. Army Intelligence Command and the U.S. Army Security Agency . . . 138
The Army Intelligence and Security Branch . . . 142

9. Vietnam and Beyond . . . 145
Vietnam: Buildup and Deployment . . . 146
The U.S. Army Intelligence Command and the Home Front . . . 153
Beyond the Battle: Intelligence Trends in the 1960s . . . 157
Westmoreland, McChristian, and Military Intelligence . . . 159
Lean Years . . . 161
A Time of Transition . . . 165

10. Reorganization and Renewal . . . 169
Remaking Military Intelligence . . . 169
The Intelligence Organization and Stationing Study: Solutions . . . 171

Chapter		*Page*
	New Directions for Military Intelligence: INSCOM	174
	The Combat Electronic Warefare and Intelligence Concept	179
	Military Intelligence in the Reserve Components	182
	Military Intelligence in the 1980s	183
11.	**A Future of Uncertainties**	187
	Conclusion: The Shaping of Army Intelligence	190
	Bibliography	197
	Glossary	209
	Heraldic Items	213
	Lineages and Heraldic Data	215
	Military Intelligence Corps	217
	66th Military Intelligence Brigade	218
	111th Military Intelligence Brigade	220
	112th Military Intelligence Brigade	222
	201st Military Intelligence Brigade	224
	205th Military Intelligence Brigade	227
	207th Military Intelligence Brigade	229
	319th Military Intelligence Brigade	231
	470th Military Intelligence Brigade	233
	500th Military Intelligence Brigade	235
	501st Military Intelligence Brigade	237
	504th Military Intelligence Brigade	239
	513th Military Intelligence Brigade	241
	525th Military Intelligence Brigade	243
	108th Military Intelligence Group	246
	109th Military Intelligence Group	247
	115th Military Intelligence Group	248
	116th Military Intelligence Group	249
	259th Military Intelligence Group	250
	336th Military Intelligence Group	252
	348th Military Intelligence Group	253
	505th Military Intelligence Group	254
	650th Military Intelligence Group	255
	902d Military Intelligence Group	257
	1st Military Intelligence Battalion	259
	2d Military Intelligence Battalion	262
	3d Military Intelligence Battalion	263

14th Military Intelligence Battalion 266
15th Military Intelligence Battalion 267
24th Military Intelligence Battalion 269
101st Military Intelligence Battalion 271
102d Military Intelligence Battalion 274
103d Military Intelligence Battalion 277
104th Military Intelligence Battalion 280
105th Military Intelligence Battalion 283
106th Military Intelligence Battalion 286
107th Military Intelligence Battalion 287
108th Military Intelligence Battalion 289
109th Military Intelligence Battalion 291
110th Military Intelligence Battalion 294
124th Military Intelligence Battalion 295
125th Military Intelligence Battalion 297
126th Military Intelligence Battalion 300
128th Military Intelligence Battalion 301
134th Military Intelligence Battalion 303
135th Military Intelligence Battalion 304
138th Military Intelligence Battalion 305
140th Military Intelligence Battalion 308
141st Military Intelligence Battalion 309
142d Military Intelligence Battalion 310
147th Military Intelligence Battalion 312
163d Military Intelligence Battalion 313
165th Military Intelligence Battalion 315
201st Military Intelligence Battalion 316
202d Military Intelligence Battalion 318
203d Military Intelligence Battalion 319
204th Military Intelligence Battalion 320
205th Military Intelligence Battalion 324
206th Military Intelligence Battalion 326
223d Military Intelligence Battalion 327
224th Military Intelligence Battalion 328
229th Military Intelligence Battalion 331
260th Military Intelligence Battalion 332
297th Military Intelligence Battalion 333
301st Military Intelligence Battalion 334
302d Military Intelligence Battalion 335
303d Military Intelligence Battalion 338
304th Military Intelligence Battalion 341
305th Military Intelligence Battalion 343
306th Military Intelligence Battalion 345

307th Military Intelligence Battalion 347
308th Military Intelligence Battalion 351
309th Military Intelligence Battalion 353
310th Military Intelligence Battalion 355
311th Military Intelligence Battalion 357
312th Military Intelligence Battalion 361
313th Military Intelligence Battalion 365
314th Military Intelligence Battalion 369
319th Military Intelligence Battalion 371
321st Military Intelligence Battalion 373
323d Military Intelligence Battalion 374
325th Military Intelligence Battalion 375
326th Military Intelligence Battalion 376
337th Military Intelligence Battalion 378
338th Military Intelligence Battalion 380
341st Military Intelligence Battalion 382
344th Military Intelligence Battalion 383
345th Military Intelligence Battalion 385
368th Military Intelligence Battalion 386
372d Military Intelligence Battalion 387
373d Military Intelligence Battalion 388
376th Military Intelligence Battalion 390
377th Military Intelligence Battalion 391
378th Military Intelligence Battalion 392
383d Military Intelligence Battalion 393
415th Military Intelligence Battalion 394
501st Military Intelligence Battalion 395
502d Military Intelligence Battalion 398
511th Military Intelligence Battalion 400
519th Military Intelligence Battalion 402
522d Military Intelligence Battalion 405
524th Military Intelligence Battalion 407
527th Military Intelligence Battalion 409
532d Military Intelligence Battalion 411
533d Military Intelligence Battalion 413
542d Military Intelligence Battalion 417
549th Military Intelligence Battalion 418
550th Military Intelligence Battalion 419
629th Military Intelligence Battalion 420

Glossary of Lineage Terms 421

Index to the Narrative 425

Illustrations

The following photographs appear between pages 60 and 61:

Nineteenth century intelligence collectors
New quarters for the War Department' s intelligence organization, 1908
Pioneers of Military Intelligence
Interrogation of German prisoners of war during World War I
Technology at the service of intelligence: an Army aerial photographer
Herbert O. Yardley, intelligence hero and villain
Group photograph of the Signal Intelligence Service
The new location of the SIS in Arlington, Virginia, 1942
Signal Security Agency personnel decrypting Japanese diplomatic traffic
Cipher machines like SIGABAs guarded the security of Army communications.
Officers of Security Detachment D in the European Theater of Operations
A Counter Intelligence Corps agent questioning a source in the ETO
Soldiers of the elite Alamo Scouts in the Southwest Pacific Area
Postwar headquarters of Army Security Agency, Europe, in Frankfurt
A Nisei Counter Intelligence Corps agent during the occupation of Japan

The following photographs appear between pages 144 and 145:

Antenna field during the Korean War
Photointerpreters of the 45th ("Thunderbird") Infantry Division
The sphinx, historically identified with Military Intelligence
Antenna array at an overseas site
The durable Mohawk
Maj. Gen. Alva Fitch
Members of a military intelligence detachment during the Vietnam conflict
An intelligence officer interrogating a suspected member of the Viet Cong
A Special Forces team operating an AN/PRD–1 radio direction finder
Operations room at the Intelligence Command during the Vietnam era
A soldier demonstrating a PRD–11 radio direction finder
Guardrail Common Sensor mounted aboard the RC–12 platform
Organization Day ceremonies for the Military Intelligence Corps
New headquarters building of the Intelligence and Security Command
Use of automation and communications systems after the Cold War

A color illustration of the regimental insignia of the Military Intelligence Corps appears as the frontispiece. Color illustrations of heraldic items approved for military intelligence brigades, groups, and battalions appear between pages 214 and 215.

MILITARY INTELLIGENCE

Introduction

Military Intelligence—the collection of information by commanders on the enemy and the battlefield environment they must confront—has existed since the beginnings of armies and of wars. However, the emergence of professional Military Intelligence organizations and the definition of the functions they most appropriately performed are comparatively recent developments. Until the nineteenth century, Military Intelligence was practiced only in wartime; methods of collection were rudimentary; and the conduct of Military Intelligence was considered a function of command, one which any professional officer could perform. Furthermore, commanders tended to be skeptical about the reliability of the information they received from spies, scouts, and their own troops. In his monumental treatise *On War*, Clausewitz commented only that "many intelligence reports in war are contradictory, even more are false, and most are uncertain."[1]

The powers of continental Europe developed military staff organizations during the nineteenth century and provided a peacetime institutional locus for Military Intelligence organization. Staffs developed an intelligence element that collected maps and military statistics and dispatched attaches. Ultimately, these developments were replicated in the United States, although not without some delay. The U.S. Army was small, it had no general staff, and there were no pressing military threats to drive intelligence collection. And although George Washington had been a masterful practitioner of intelligence while serving as commander in chief of the Continental Army, this aspect of his experience has never become part of the national heritage. A small Division of Military Information was finally set up within the Adjutant General's Office twenty years after the American Civil War had ended. A few years later the Army dispatched its first military attaches abroad to provide general information on worldwide military affairs. When the Army at last gained a General Staff in 1903, the Military Information Division was transformed into the General Staff's Second Section.

---

[1] Karl Von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), p. 117.

At the time, the Army's fledgling General Staff was groping to define its own appropriate mission, and these beginnings were never fully developed. A subsequent reorganization effectively eliminated the intelligence function of the staff, and it took America's entry into World War I to reverse the situation. To fight a land campaign on the continent of Europe, the Army was compelled to remodel itself along continental lines. An intelligence division was re-created within the War Department General Staff, and staffs that included intelligence officers were introduced at all units down to the level of battalion. Military Intelligence expanded to become a "shield" as well as a "sword," as the Army became heavily involved in counterintelligence.

In the field, technology helped to rationalize intelligence collection at the tactical and operational levels. Under combat conditions, intelligence gathering was accomplished not only by Military Intelligence specialists but also by the line troops themselves. As S. L. A. Marshall later stated, "Infantry . . . is the antenna of the mechanism of combat intelligence."[2] Increasingly, these sources were augmented by what were later called "special information services" that engaged in various types of technical collection activities.[3] World War I exposed the Army to a dazzling new array of technological enhancements to the collection process: aerial photography and reconnaissance, radio intercept, and optical and acoustical sensors used to detect aircraft and artillery. One secondary effect was that much of the Army's practical intelligence work was carried out by nonintelligence personnel: the intercept personnel of the Signal Corps; technicians manning artillery targeting devices; topographic specialists in the Corps of Engineers; and aviators. This situation in turn tended to block or delay the further centralization of the intelligence function.

In the long years of peace following the Armistice, Army Intelligence continued to search for an appropriate place within an Army the size of which had again been greatly reduced. A basic problem of Army Intelligence remained conceptual: defining what an intelligence organization should do. Army Intelligence offices, in fact, continued to be regarded as clearing houses for all manner of information functions unrelated to intelligence. During the interwar years, for example, intelligence staffs managed the Army's public affairs programs; later they were tasked with conducting psychological warfare and writing the Army's history. It took a surprisingly long time—until the end of World War II—for Army Intelligence to shake off such extraneous functions and concentrate on its primary task, "knowing one's enemies."[4] At the War Department level, the Army's intelligence organization tended to act more as a reference library than as

---

[2] Quoted in Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Free Press, 1990), p. 181.

[3] Robert R. Glass and Phillip B. Davidson, *Intelligence is for Commanders* (Harrisburg: Military Service Publishing Co., 1946), p. 25.

[4] This useful definition is taken from the title of Ernest May's *Knowing One's Enemies: Intelligence Assessments Before the Two World Wars* (Princeton: Princeton University Press, 1986).

a positive directing force. Not until May 1945 did the War Department's Military Intelligence Division (MID) acquire an organization to establish intelligence priorities and requirements, missions that finally allowed it to put into practice all components of the modern intelligence cycle: determining requirements, collecting the appropriate information, processing the acquired data into finished intelligence, and disseminating the results, a circular process that often generates a new set of requirements, initiating the cycle again.[5]

Military Intelligence also labored under other handicaps in the years between the wars. Under garrison conditions, unit intelligence officers found themselves with little to do. Battlefield collection mechanisms seemed to have little utility in peace. The Military Intelligence Division maintained a small counterintelligence element and for a time funded a small cryptanalytic unit; but the latter function subsequently passed over to the Signal Corps. Military attaches continued to report, but their purpose was somewhat anomalous—government parsimony and expensive representational demands made it impossible for officers without private incomes to serve in overseas posts, and their function seemed more political and social than military.

These factors, along with the perceived absence of any real threat in times of peace, effectively marginalized intelligence work within the Army. Intelligence seemed unrelated to the real life of the Army, and intelligence assignments were viewed as curiosities at best. General of the Army Dwight D. Eisenhower later commented, "I think that officers of ability in all our services shied away from the intelligence branch in the fear that they would be forming dimples in their knees by holding teacups in Buenos Aires or Timbuctoo."[6] At the same time, if intelligence was peripheral, the Army still assumed that any officer could fulfill its functions.[7]

In World War II these attitudes began to change. Military and political leaders alike recognized that intelligence was crucial to military success. To meet its information needs, the Army was forced to create a large intelligence structure, manned largely by draftees and officers commissioned into the Reserves. Acting through its wartime operating arm, the Military Intelligence Service, the Military Intelligence Division instituted formal training for intelligence personnel in a diversity of disciplines. By the end of the war, various types of intelligence teams and counterintelligence detachments were supporting the intelligence

---

5 Military Intelligence Division, A History of the Military Intelligence Division, 7 December 1941–2 September 1945, unpublished Ms, U.S. Army Center of Military History, 1946, p. 72, copy in INSCOM History Office files.

6 Dwight D. Eisenhower, "Command in War," lecture presented to the National War College, Washington, D.C., 30 Oct 50.

7 The author of one of the earliest books on Military Intelligence in the U.S. Army stated, "If things are not going right between G–2 and G–3 . . . then a switching of the duties of these is recommended. If the G–2 is not competent to be a G–3, he is not competent to be a G–2 and should be retired from the General Staff." Walter Campbell Sweeney, *Military Intelligence: A New Weapon in War* (New York: Frederick A. Stokes Co., 1924), p. 135.

staffs of all tactical units in the field. Meanwhile, the Signal Corps conducted its own intelligence and security war, entering the field of radar, which was at once a collection technology, a new intelligence target, and a subject of possible countermeasures. More important, the Signal Corps provided cryptologic support to the War Department through its Signal Security Agency and furnished theater commanders with tactical signals intelligence units. The growing importance of communications intelligence ultimately resulted in the transfer of responsibility for the function from the Signal Corps to Military Intelligence. The Army emerged from World War II with an intelligence structure that in some ways prefigured that of the present. Most of the lineages of today's intelligence units trace back to the second World War. However, this structure was departmentally oriented, fragmented, and less than fully articulated. Following the postwar reorganization of the Army in 1946, the Military Intelligence Division again emerged as the dominant institution in the whole architecture, providing overall direction, producing intelligence, and engaging in a diversity of operational activities. As part of its mandate, the Division commanded a vertically organized signals intelligence and security apparatus, the Army Security Agency (ASA), and an administratively centralized counterintelligence element, the Counter Intelligence Corps (CIC). Both ASA and CIC were organized into sizable units. However, the Army's other intelligence disciplines—human intelligence and imagery intelligence—continued to be essentially orphans, their personnel grouped into small teams supporting tactical commanders and their training base neglected. Electronic warfare remained the province of the Signal Corps. The system continued to be manned by a mix of detailed Regular Army officers and reserve officer specialists who chose to remain in uniform when the war came to an end.

During the next forty years, these arrangements were reshaped by several diverse influences. The Cold War, advances in technology, and imperatives of bureaucracy were perhaps the most significant. To meet evolving challenges, the structure of Army Intelligence was repeatedly reorganized. Military Intelligence was professionalized, its disciplines integrated, and the scope of its operations enhanced. As a result, Military Intelligence became a branch in the U.S. Army, and Military Intelligence professionals were affiliated with the Army's regimental system through the creation of the Military Intelligence Corps. Intelligence staff sections, present at all Army levels, were supplemented by specialized intelligence units up to brigade level. This book attempts to trace the long and complicated organizational history that characterized this evolution.

1

The Beginnings

In 1885 the Division of Military Information was established as part of the Military Reservations Division, Miscellaneous Branch, of the Adjutant General's Office. This step gave the U.S. Army a permanent intelligence organization for the first time in a century.

The long delay in giving recognition to the importance of Military Intelligence stemmed from various factors. One of these was the marginal position that the Army itself occupied in American society. The American tradition was one of liberty, democracy, and commercialism; except in time of war the country tended to neglect all the Army's needs. The professional Army was there to perform constabulary work against scattered Indian tribes in the vastness of the American West, to man coast defenses against the implausible threat of a foreign attack, and to serve as a continuing nucleus of professional expertise. Should a real threat to the Republic appear, citizens would rally to the flag, as they had in all of America's past wars, and some kind of mechanism for collecting intelligence would eventually be improvised to meet the crisis.

Another factor retarding the development of a permanent intelligence organization until 1885 was the general backwardness of the Army. On the European Continent, armies had been forced to create systematic staff organizations dealing with both operations and intelligence since the beginning of the nineteenth century. The Prussian Great General Staff provided the model for all of Europe's armies. In the United States, with its distrust of militarism, the idea of such a super army headquarters was repellent. Collecting intelligence and laying out detailed war plans were not in the American tradition. The U.S. Army's central staff consisted mainly of bureaus dealing with questions of administration and supply, and these reported directly to the secretary of war, not to the commanding general of the Army.

Without any organizational support, each U.S. commander served as his own intelligence officer, and the intelligence function was limited to simple reconnaissance in time of war or during an Indian campaign. In the field, units set up security patrols in tactical arrangements described in a now-

quaint vocabulary of pickets, vedettes, and Cossack posts.[1] During major deployments, such as those which took place in the Civil War, cavalry served its traditional function as the eyes of the Army.

Army topographic engineers and other officers trained under the U.S. Military Academy's engineer-oriented curriculum also made important contributions to intelligence, continuing an Army tradition that dated back to the explorations of Lewis and Clark. In 1814 the War Department created a unit of topographic engineers to help with the military effort against Great Britain. From 1818 on, the Army maintained a topographic bureau and from 1838 to 1863 a separate Corps of Topographic Engineers. West Point–trained engineers helped lead Maj. Gen. Winfield Scott's army to the conquest of Mexico City in 1847.[2] Reconnaissance efforts carried out by troops were often supplemented by civilian auxiliaries. Indian and civilian scouts brought their special expertise to bear on the frontier. During the Mexican War, General Scott had even employed a group of locally hired Mexican bandits and deserters, the "Mexican Spy Company," to gather specific tactical intelligence.

Limiting Military Intelligence to tactical collection had led to numerous disasters in the past. In the War of 1812 American troops had crossed the Canadian border without maps in an abortive invasion attempt that ended in a fiasco. A generation later, the Army's quartermaster general found himself with no idea whether or not wagons could be used to support the advance of Maj. Gen. Zachary Taylor's forces into Mexico. In a classic breach of security, the Army then sent a courier to Taylor carrying unenciphered secret orders that stripped the general of most of his regulars. The orders were captured on the way, and Taylor's lack of reconnaissance allowed his depleted forces to be taken by surprise at Buena Vista. Buena Vista turned out to be an American victory only due to the fighting prowess of Taylor's volunteer troops. With luck on its side, the Republic managed to muddle through the Mexican War just as it had through the War of 1812. In both cases, the ultimate triumph of largely improvised forces encouraged a casual approach toward Military Intelligence, an attitude that fit well with the longstanding American tradition of subordinating military concerns to other, more immediate interests.

The nature and scope of the Civil War provided unusual opportunities for intelligence collection.[3] Because the North and South were physically proximate

---

[1] See Arthur L. Wagner, *The Service of Security and Information* (Kansas City: Hudson-Kimberley Publishing, 1893), pp. 55–67.

[2] The services of the topographical engineers are documented in William H. Goetzman, *Army Exploration in the American West, 1803–1863* (Lincoln: University of Nebraska Press, 1979); Guy C. Swan III et al., "Scott's Engineers," *Military Review* (March 1983): 61–68, deals with reconnaissance in the Mexican War.

[3] An excellent treatment of Civil War intelligence can be found in Peter Maslowski, "Military Intelligence Sources During the American Civil War," in *The Intelligence Revolution: An Historical Perspective; Proceedings of the Thirteenth Military History Symposium, United States Air Force Academy*, ed. Walter T. Hitchcock (Washington, D.C.: Office of Air Force History, 1991), pp. 39–70.

and loyalties were desperately intermixed, both sides made extensive use of spies as well as the military information cheerfully turned over by an uncensored press. In the field the rival armies often used civilian guides, willingly or unwillingly recruited from the population. This was an American adaptation of Napoleon's succinctly brutal advice on intelligence collection: "You order the major to put a peasant at your disposal, arrest his wife as a hostage, have a soldier dress himself as the man's farm hand. This system always succeeds."[4] Cavalry once again proved its indispensability. For the first part of the war, lack of an effective cavalry organization left the Union armies blinded in the presence of their enemies. During the Gettysburg campaign, however, the situation was reversed. Maj. Gen. J. E. B. Stuart's decision to raid rather than scout led directly to the Confederates' accepting battle on unfavorable terms.

Increased use of technology also contributed to innovations in the intelligence and security arena during the Civil War. The Union Army used both free and tethered balloons to watch over enemy dispositions in the early stages of the conflict. Manned by civilian aeronauts, the balloons were successively assigned to the Corps of Topographic Engineers, the Quartermaster Corps, and the Corps of Engineers.[5] The Army Signal Corps, first set up in 1863, also came to play an intelligence role. Signal Corps communications troops posted on high ground often provided valuable field intelligence.[6] However, their messages, transmitted by "wig-wagged" signal flags, could be intercepted. Similarly, the increased use of the telegraph by each side created opportunities both for communications intercept and communications deception. This quickly led to the employment of rudimentary field codes and ciphers in tactical situations.

Most commanders on both sides continued to serve as their own intelligence officers. Confederate Lt. Gen. Thomas "Stonewall" Jackson directly supervised the mapping of the Shenandoah Valley.[7] Another Confederate corps commander, Lt. Gen. James A. Longstreet, personally debriefed the spy who provided the first indications that the Union Army was on the move to Gettysburg.

---

[4] Martin Van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985), p. 67.

[5] Army balloon activities in the Civil War and later periods are covered in Tom D. Crouch, *The Eagle Aloft: Two Centuries of the Balloon in America* (Washington, D.C.: Smithsonian Institute Press, 1983). The Confederates were able to field only one balloon during the course of the conflict, but its performance impressed at least one rebel officer. "My experience with this gave me a high idea of the possible efficiency of balloons in active campaigns. Especially did we find, too, that the balloons of the enemy forced upon us constant troublesome precautions in efforts to conceal our marches." General E. P. Alexander, *Military Memoirs of a Confederate* (Bloomington: Indiana University Press, 1962), pp. 172–73.

[6] The Union Signal Corps operated both "stations of observation" and "stations of communication." J. Willard Brown, *The Signal Corps, U.S.A. in the War of the Rebellion* (New York: Arno Press, 1974), p. 125. The Confederate Signal Corps was even more involved in intelligence work. See William A. Tidwell et al., *Come Retribution: The Confederate Secret Service and the Assassination of Lincoln* (Jackson: University Press of Mississippi, 1988), pp. 80–104.

[7] This is documented in *Make Me a Map of the Valley: The Civil War Journal of Stonewall Jackson's Topographer*, ed. Archie P. McDonald (Dallas: Southern Methodist University Press, 1973).

However, there were some attempts to designate intelligence officers and to establish rudimentary intelligence organizations. During the opening days of the Bull Run campaign, Maj. Gen. Pierre Beauregard's assistant adjutant general was able to provide the Confederate Army with early warning of incipient Union moves through a well-connected spy network he ran in Washington, D.C. Shortly afterward, Maj. Gen. George McClellan, the newly appointed head of the Union Armies, employed private detective Alan Pinkerton as his intelligence chief. However, Pinkerton's untutored and exaggerated evaluation of Confederate strength virtually paralyzed Union operations for a time.[8] But amateurishness in the field of intelligence at this point was not confined to civilians: after Pinkerton's return to private life, McClellan's cavalry chief, Maj. Gen. Alfred Pleasanton, provided equally misleading information regarding the enemy's numbers.[9]

Union forces did not acquire a professional intelligence officer until the spring of 1863, when Maj. Gen. Joseph Hooker, commander of the Army of the Potomac, directed Col. George V. Sharpe of the 120th New York Volunteer Infantry to set up a bureau of information. Sharpe, a lawyer and diplomat in civilian life, devised an effective system making use of civilian scouts, behind-the-lines agents, and interrogation reports from deserters and prisoners of war to build up an accurate picture of Confederate order of battle and intentions. By the end of the war, Sharpe was a brevet brigadier general and assistant provost marshal assigned to Headquarters, Armies of the United States.[10]

Counterintelligence organizations also made an appearance. In one of their few successes, Pinkerton and his operatives rolled up the Rosa Greenhow spy network that had funneled information to the Confederates from the nation's capital. At the beginning of 1862 the War Department took over the rather elaborate nationwide counterintelligence organization built up by Secretary of State William Henry Seward and placed it under Lafayette Baker, a civilian who subsequently operated a "secret service" of detectives that engaged in both positive collection and counterintelligence. In addition, Baker supervised investigations of graft and fraud and still found time to organize his own cavalry regiment, thus acquiring

---

8 To the end, Pinkerton was convinced he was right. See his autobiographical work, *The Spy of the Rebellion: Being a True History of the Spy System of the United States Army During the Late Rebellion* (New York: G. W. Carleton and Co., 1883), p. 588. The best evaluation of his performance is in Edwin C. Fishel, "Pinkerton and McClellan: Who Deceived Whom?" *Civil War History* 24 (June 1988): 115–42.

9 Stephen V. Sears discusses the "singular ineptitude" of Pleasanton as an intelligence officer in *George B. McClellan: The Young Napoleon* (New York: Ticknor and Fields, 1988), p. 274. Pleasanton continued to serve as cavalry chief of the Army of the Potomac even after McClellan stepped down. His reports continued to be "remarkably unreliable." Russell F. Weigley, *History of the United States Army, Enlarged Edition* (Bloomington: Indiana University Press, 1984), p. 242.

10 Maslowski, "Intelligence Sources," p. 40. It should be noted that Sharpe's organization was known as a "bureau of information," not an intelligence office. In nineteenth-century usage, the word "intelligence" equated with today's "news." The Army Intelligence Office, which the Confederates established in 1862, was headed by a chaplain with the mission to inform the families of wounded Southern soldiers about their care and disposition.

the rank of colonel. As a result of his work in tracking down Lincoln's assassins, Baker also ended his Civil War service as a brevet brigadier general.[11]

After the Civil War, older habits reasserted themselves. The vast armies were hastily demobilized, and the wartime arrangements for gathering intelligence discontinued. Sharpe returned to civilian life; Baker was fired by President Andrew Johnson, who disagreed both with his methods and, more to the point, his suspicions that unregenerate Confederates were regaining power and influence under the Johnson administration. Once Reconstruction had ended, the Army was scaled back to a force of some 25,000 men, thinly scattered over the empty spaces of the American West. Once again, each commander served as his own intelligence officer. Under typical conditions of Indian warfare, cavalry regiments were broken up into penny-packets and employed as standing garrisons or mobile strike forces. In the West, commanders relied on Indian scouts and civilians like Buffalo Bill Cody to fulfill their intelligence needs. Indians had been used in this role since the beginning of the Republic, and Congress had authorized a permanent Corps of Indian Scouts in 1866. Although the legislation provided for a force of 1,000 scouts, budgetary factors allowed no more than 300 scouts to be employed at any one time.[12]

Despite its occasional wartime accomplishments, Army Intelligence had been a matter of improvisation. There had been no institutional structure to give it historical continuity. Expertise gained in wartime had quickly dissipated. However, by the 1880s the tide began to turn. American society itself was rapidly changing from a loosely knit aggregation of agriculturalists into an industrial unit of large corporations bound together in a national market. This in turn led to a new emphasis on professional expertise.[13] At the same time, similar developments were taking place in the major nations overseas, which began to exhibit a renewed interest in imperial expansion, a fact of some concern to the United States. The U.S. preoccupation with the Civil War had already encouraged French intervention in Mexico. As the steamship and the international cable continued to draw the world closer together, the actions of foreign powers impinged on the American popular consciousness in a way that had not been the case in the past.

Slowly, America's military institutions began to respond to these pressures for greater professionalization and greater access to information concerning events abroad. In 1881 the Army created a professional school at Fort Leavenworth, Kansas, to give advanced instruction to infantry and cavalry officers. In 1882 the U.S. Navy set up the Office of Naval Intelligence with the primary mission of observing and reporting on new developments in maritime technology overseas.

---

11 Baker told his own story, possibly with some improvements, in *History of the United States Secret Service* (Philadelphia: L. C. Baker, 1867).

12 Robert M. Utley, *Frontier Regulars: The United States Army and the Indian, 1866–1890* (New York: MacMillan Co., 1973), p. 53.

13 This interpretation owes much to Robert G. Wiebe.

The establishment of the Division of Military Information by the Army in 1885 was thus part of a larger pattern of historical developments.

Military Intelligence in Place

The Army's Intelligence organization underwent a steady evolution between 1885 and the beginning of the war with Spain. Initially, the Division of Military Information appears to have been seen as simply a passive repository for information on military-related developments at home and abroad. Its domestic responsibilities led to its location in the Military Reservations Division of the Adjutant General's Office. Initial collection requirements were disarmingly simple. The adjutant general requested that the Army's geographical departments and technical services "whenever practicable, make report on anything which it may be desirable for the Government to know in case of sudden war." Just what sort of information this was, however, was "almost impossible to specify in detail . . . but this can well be left to the intelligence and discretion of the officers."[14]

In 1889 the division took a first step toward taking on a more positive role when the Army dispatched military attaches to the capitals of the five major European powers: Great Britain, France, Germany, Russia, and Austria-Hungary. Since the attaches were charged with performing intelligence-gathering tasks in addition to diplomatic representational duties, they provided the division with its own professional collection arm. About the same time, the division became a separate body, directly subordinate to the adjutant general, and access to its files was restricted to the commanding general of the Army and the bureau chiefs.[15]

Although the introduction of attaches improved the Army's foreign intelligence capabilities, it also resulted in the Army's first intelligence scandal. In 1892 Capt. Henry T. Borup, the American attache posted to France, was expelled from the country for attempting to purchase the plans for the fortifications of Toulon from a disgruntled employee of the French Ministry of Marine. This event caused some consternation, especially to Jefferson Coolidge, the American minister to France. Coolidge pointed out that Borup's action had been "perfectly useless"; not only was America at peace with France, but the small American navy could not attack Toulon.[16] However, the captain's behavior, while indiscreet, was not totally irrational; the United States had recently embarked on a program to upgrade its own coastal defenses, and Borup, an

---

[14] Ltr, Brig Gen R. C. Drum to Chief of Engineers, 23 Nov 1886; George W. Auxier, Historical Manuscript File: Materials on the History of Military Intelligence in the U.S., 1884–1944, U.S. Army Center of Military History, Washington, D.C., hereafter cited as MID Documents.

[15] A succinct account of the organization can be found in Elizabeth Bethel, "The Military Information Division: Origin of the Intelligence Division," *Military Affairs* 11 (Spring 1971): 17–24.

[16] Alfred Vagts, *The Military Attache* (Princeton: Princeton University Press, 1967), p. 222.

ordnance officer, presumably believed that any information gleaned from abroad would be helpful. At any rate, this minor embarrassment did not interfere with the growth of the attache system. By 1894 five additional attache posts had been set up at other European capitals, Japan, and Mexico.

Meanwhile, the functions of the Military Information Division expanded further. In 1892 the secretary of war reorganized the division, assigning it a wide spectrum of duties that nearly transformed it into a combined operational and intelligence staff. The division was tasked to collect information on both the United States and foreign countries, to direct the attache system, and to disseminate intelligence products and maps to the Army. In addition, it was to monitor the militia mobilization base, prepare instructions to the militia inspectors, and formulate mobilization plans. As if all of this were not enough, the division was also directed to "have charge of a museum . . . for the care and preservation of military relics."[17]

By 1893 the Military Information Division was large enough to be organized into four branches. The Progress in Military Arts Branch collected scientific and technical intelligence from the various attaches. The Northern Frontier Branch focused on the Canadian border: Great Britain was still thought of as a possible, though not probable, enemy, and Army officers were encouraged to take "hunting and fishing" leaves to reconnoiter and map certain areas of Canada. The Spanish-American Branch monitored developments in the troubled Caribbean, where Cuban revolutionaries were already plotting insurrection against Spain. Finally, the Militia and Volunteer Branch kept track of the various state National Guard organizations and performed whatever rudimentary mobilization planning was possible in peacetime.

As a result, when the war with Spain began in April 1898, the Army for once entered upon a conflict with at least a semblance of intelligence preparation. Eleven officers were on duty with the Military Information Division at the State, War, and Navy Building in Washington; 6 additional attaches went to join the 10 already abroad, and another 40 officers provided status reports on the nation's militia.[18] The Military Information Division had already collected a good deal of intelligence on conditions in Cuba and soon collected more using Army officers on undercover assignments in Cuba and Puerto Rico. The clandestine collection mission of Lt. Albert Rowan in Cuba was later both popularized and distorted in Elbert Hubbard's famous story, "A Message to Garcia."[19]

---

17 Orders, Secretary of War S. B. Elkins, 12 Mar 1892, MID Documents.

18 Marc B. Powe, *The Emergence of the War Department Intelligence Agency, 1885-1918* (Manhattan, Kans.: MA/AH Publishing, 1974), p. 29. The head of the Military Information Division at the time was Col. Arthur S. Wagner, author of *The Service of Security and Information* and the leading expert on intelligence in the Army.

19 For the true story, see Rowan's own account in *Military Intelligence: Its Heroes and Legends*, comp. Diane Hamm (Arlington, Va.: U.S. Army Intelligence and Security Command, 1987), pp. 1–19.

Unfortunately, the war would reveal much about the weaknesses of both the Army and its Military Intelligence organization. The 25,000-man Regular Army was increased in strength, but concomitantly 140,000 militiamen and volunteers were placed under arms, creating intolerable strains on the country's mobilization capacities. The dispatch of the main Spanish fleet to Santiago, Cuba, first discovered by a Signal Corps wiretap of the Spanish cable, led to the hasty deployment of elements of the Army's newly organized V Corps to that island. This expeditionary force was pulled together amid conditions of chaos and then committed to action under a slothful commander of dubious tactical skills. Eventual victory in Cuba owed much to the valor of regular and volunteer troops, but little to planning or to the effective use of intelligence, since the expedition's commander had refused the War Department's offer to set up a Military Information Division in the field to support the campaign.

Meanwhile, mobilization effectively disrupted the workings of the Military Information Division. The natural desire of officers for field service, coupled with the need to stiffen the volunteer troops with regulars, drained the Military Information Division of its uniformed personnel; only 2 officers and 10 civilian clerks were left on duty in Washington when the war came to a close, and all but 5 attaches had returned from their posts abroad. But during the same period the Army's intelligence needs had grown immensely. Following Dewey's victory at Manila, troops had been committed to the Philippines. An intelligence officer accompanied the expedition, but he labored under severe handicaps because the Military Information Division had never made any study of the Far East. Once a Filipino insurrection against American occupiers broke out, the Army in the Philippines was forced to expand its intelligence activities. In 1899 it set up its own independent counterintelligence center, the Bureau of Insurgent Records. Redesignated a year later as the Bureau of Military Information, this organization was not subordinated to the War Department's Military Information Division until 1902.

The lessons of the war with Spain and the imperatives of maintaining a 100,000-man Army to secure America's new empire led to a complete reorganization of the War Department in 1903. As a result, the Army finally acquired a General Staff organization to carry out administrative, intelligence, and planning functions. Six of the forty-four officers on the new War Department General Staff were assigned to its Second Division, which absorbed the Adjutant General's Military Information Division and was given the exclusive mission of collecting foreign intelligence. The arrangement allowed the Army's military information organization to focus its attention on intelligence rather than on the diversity of operational assignments that the Military Information Division had been given in 1892. In 1904 Great Britain belatedly organized its own Army General Staff, adopting precisely the oppo-

site solution: the British combined intelligence with operations in the same staff element.[20]

Four major duties were assigned to the U.S. General Staff's Second Division: collecting and disseminating information on foreign countries; directing the work of the attache system and managing contacts with foreign military attaches in the United States; supervising mapping; and maintaining a reference collection. However, even under the new arrangements, the military information unit still could not perform certain vital intelligence staff functions. First, it had not been given the responsibility for planning Army Intelligence organization and operations in the field; it simply acted as a central point for intelligence-gathering at the War Department level. Second, the organization had no responsibility for security or counterintelligence within the Army. Moreover, the division's small staff was hard pressed to cope with its existing functions, and the War Department General Staff could not give the subject the attention it deemed necessary. Nevertheless, at least some officers had come to realize that the criterion for staffing the new organization should have been the size of the world rather than the size of the Army.

Military Intelligence in the Twentieth Century

The first decade of the twentieth century furnished Army Intelligence with new challenges. Formerly, intelligence officers had concerned themselves with procuring information on the neighboring states in the Western Hemisphere and collecting, on a more or less academic basis, technical intelligence on military developments in Europe. The acquisition of the Philippines had forced the Army to develop a counterintelligence capability in that area. The Army soon realized that the Philippine involvement, together with a growing American commercial and military presence in China, had a wider intelligence impact. America was now a Far Eastern power. This meant that the Army now had to evaluate the military threat of the expanding Japanese Empire. Prejudice against Asian immigrants on the West Coast, which repeatedly jeopardized American-Japanese relations, only reinforced this need. Military observers thus went abroad to supplement attache coverage of the Russo-Japanese War of 1904–1905. In 1907 the Army began to assign officers to Japan for language training and shortly thereafter to China for the same purpose.

Paradoxically, as the Army's need for intelligence increased, the Army's capacity to meet it declined. Between 1903 and America's entry into World War I, the Army's new General Staff strove to find an identity and a suitable role. The Army's intelligence organization was caught up in this bureaucratic maneuvering with unfortunate results. In 1907 the incumbent adjutant general, the autocratic Maj.

---

[20] Thomas G. Fergusson, *British Military Intelligence, 1870–1914: The Development of a Modern Intelligence Organization* (Frederick, Md.: University Publications of America, 1984), p. 202.

Gen. Frederick Ainsworth, restricted the authority of the Second Division to communicate directly with the attaches overseas, insisting that certain categories of correspondence pass through his office. Then, in 1908 the Third Division of the General Staff, which dealt with contingency and operational planning and was a principal consumer of the Second Division's products, relocated to Washington Barracks (now Fort McNair). Unfortunately, its new and spacious quarters were some miles away from the Second Division's offices in downtown Washington, D.C. This soon caused coordination problems, since the Third Division had only one automobile at its disposal. To satisfy the Third Division's information requirements, the Second Division was in turn moved from its own centrally located offices and banished to Washington Barracks. Incumbent Chief of Staff Maj. Gen. J. Franklin Bell then decided that it was impracticable to have two separate General Staff elements in the same place and directed that the two divisions be merged. The Army's intelligence staff element thereby lost its separate identity.[21]

The result of this reorganization was an unqualified disaster for the intelligence function at the General Staff level. Intelligence was now assigned to the Military Information Committee, all of whose members were preoccupied with numerous other duties. Intelligence was no longer produced for the Army as a whole, but for the War College Division (as the Third Division was later redesignated), and soon it ceased to be produced at all. A few years later, the chief of the War College Division had to confess that because of the press of business, "the collecting, digesting, and filing of military information of foreign countries . . . appears never to have been carried on continuously," and that "the work of attaches is without proper supervision and guidance, and therefore, to a large extent, the value of their work is lost."[22]

The outbreak of revolution in Mexico in 1911 did little to end this situation, although two War College Division captains were eventually detailed to monitor developments and compile what information about the country was available.[23] Still, when American forces landed at Vera Cruz in 1914 they were essentially without intelligence support. Sent down to investigate the situation, Capt. Douglas MacArthur reported back to his superior that "the Intelligence

---

[21] Maj. Gen. Ralph Van Deman, who headed War Department Military Intelligence for most of World War I, commented that "had there been sufficient automobile transportation it is possible that the disastrous incident . . . would not have occurred." *The Final Memoranda: Major General Ralph Van Deman, U.S.A. Ret., 1865–1952: Father of Military Intelligence*, ed. Ralph J. Weber (Wilmington: Scholarly Resources, 1988), p. 15.

[22] Memo, Brig Gen M. M. Macomb for Chief of Staff, 13 Jul 14, sub: Employment of a Monograph Clerk, Record Group (RG) 165, ser. 5, National Archives and Records Administration (NARA), Washington, D.C. A contemporary observer attributed the eclipse of the intelligence function to a personnel shortage. "The reduction of the General Staff by 12 officers in 1912 had made it impossible for an Intelligence division of any strength to be maintained." Maj Gen Dennis E. Nolan, Memoirs, ch. 4, p. 4, Dennis Nolan Ms, U.S. Army Military History Institute, Carlisle Barracks, Pa.

[23] Ltr, Brig Gen M. M. Macomb to Brig Gen Tasker H. Bliss, 26 Oct 14, Tasker Bliss Ms., Library of Congress (LC), Washington, D.C.

Office established by the Brigade was practically useless for my purpose. There seems to be no logical conception of just what information is needed and as a result its efforts consist largely in accumulating wild and exaggerated reports from a lot of scared and lying American refugees."[24]

The outbreak of general war in Europe also failed to revive the Army's intelligence program, even though the United States was soon on the verge of breaking diplomatic relations with Imperial Germany over the sinking of the *Lusitania*. Although the attache system was now extensive—historian Alfred Vagts has pointed out that only Imperial Russia had as many military attaches as the United States—and although additional military observers were sent to Europe to watch the fighting there, the mechanism for analyzing the reports submitted from overseas was lacking.[25] After 1915 the Military Information Committee was used simply as a bookkeeping device. Congressional appropriations listed the committee as a budget line item, but its membership comprised all War College Division officers engaged in "current General Staff work" as opposed to war plans.[26]

The state of intelligence work in the Army was demonstrated graphically when the War Department was called upon to produce a preparedness plan for Army reorganization in 1915. Preparation of the threat estimate justifying the plan was assigned to Capt. Dennis E. Nolan of the War College Division, who assembled his data from three open source references: a 1914 almanac of the world's armies, a shipping register from the same year, and the Army's own Field Service Regulations. In the interest of simplicity, Nolan decided to ignore the fact that the outbreak of World War I had rendered the information contained in these documents obsolete and changed the whole strategic situation. But by using this material creatively, Nolan demonstrated that Germany, to use only one of his examples, could deploy a force of 435,000 men and 91,457 animals in the United States within 15.8 days of the start of hostilities. Although this estimate served to justify the War Department's plans for a greatly expanded Army, it ignored so many other factors as to pass beyond the bounds of reality.[27]

Although Army Intelligence was collapsing at the center in the period just before American entry into World War I, there were other, more positive developments taking place in the field. These were mostly brought about by Signal Corps initiatives in the areas of communications intelligence, aerial reconnaissance, and communications security. A growing Signal Corps involvement in the

---

[24] Ltr, Capt Douglas MacArthur to Maj Gen Leonard Wood, 7 May 14, Leonard Wood Ms, LC.

[25] Vagts, *The Military Attache*, p. 34.

[26] *The Final Memoranda*, p. 147.

[27] However, the Epitome of Military Policy produced by the War Department General Staff in 1915 concluded that "the accomplishment of the plan outlined above for the invading force instead of being a noteworthy military achievement would be a commonplace military operation ridiculously easy of accomplishment." John P. Finnegan, *Against the Specter of a Dragon: The Campaign for American Military Preparedness, 1914–1917* (Westport, Conn.: Greenwood Press, 1974), p. 50.

intelligence arena came about by a circuitous route. The Signal Corps had used balloons for meteorological purposes when it had the mission of operating the U.S. Weather Bureau. After the Signal Corps turned over all but the military aspects of the weather function to the Department of Agriculture in 1890, it redirected its aeronautical expertise toward the development of a manned observation balloon. A Signal Corps balloon, the *Santiago*, took part in the fighting in Cuba, where it served chiefly to draw enemy fire. Undeterred, the Signal Corps persevered in this line of development and continued to experiment with the possibilities of aerial observation from a variety of platforms.[28] In the early years of the twentieth century, it made trials of traditional tethered observation balloons, a small powered dirigible, and the new airplane invented by the Wright brothers. In 1909 the Army purchased its first aircraft and by 1915 had a whole squadron.

Similarly, the Signal Corps pioneered the development of wireless for military uses. In 1914 it acquired three "radio tractors," actually White Company motortrucks equipped with radio sets. Although this equipment was procured for communications work, it could easily be adapted to intelligence purposes. Finally, in the field of security, Capt. Parker Hitt became the first Army officer to undertake research in the exotic field of codes and ciphers. In 1916 Hitt produced the first work on cryptology ever published in the United States.[29]

About the same time, other signs of renewed interest in Army Intelligence began to emerge. In March 1916 Maj. Ralph Van Deman, an infantry officer on detail to the War College Division, submitted to his superiors two multipage memorandums on the subject. Van Deman had served with the former Military Information Division both in Washington and in the Philippines, performed undercover work in China, and held an intelligence position on his previous General Staff assignment from 1907 to 1910. Upon returning to Washington, he expressed his dismay at the extent to which the General Staff had allowed its intelligence function to lapse. Van Deman pointed out that information was no longer "collected—it just comes in. . . . But even such information as does come in, is not studied and checked. . . . As far as any benefit to the Government is concerned, the mass of this information might just as well be in Timbuctoo. It will remain in the Record Section unavailable to the end of time."[30] What the Army needed, Van Deman felt, was a separate division of the General Staff to deal exclusively with military information.[31] Although this report had no immediate effect, in April the acting chief of staff

---

[28] In the 1903 revised edition of his book, *The Service of Security and Information*, Colonel Wagner included an extensive treatment on the employment of observation balloons for reconnaissance. I am indebted to Dr. Edward Raines of the U.S. Army Center of Military History for this piece of information.

[29] Parker Hitt, *Manual for the Solution of Military Ciphers* (Fort Leavenworth: Press of the Army Service Schools, 1916).

[30] *The Final Memoranda*, p. 104.

[31] Ibid., pp. 113–14.

of the Army ordered intelligence officers to be posted in the Army's four continental United States and two overseas geographic departments. In addition to supporting their own commanders, these officers would report back to the Military Intelligence Committee. Even before this step had been taken, the Army found it had new requirements for intelligence.

In March 1916 the forces of Mexican bandit leader Pancho Villa raided Columbus, New Mexico, inflicting loss on troopers of the 13th Cavalry and causing civilian casualties. In response, the Wilson administration ordered Brig. Gen. John J. Pershing to lead a punitive expedition into Mexico to hunt down Villa's guerrilla band. Subsequently Pershing's forces deployed the widest range of intelligence assets which the Army had yet managed to field.

During the American foray into Mexico, traditional collection mechanisms were augmented by newly emerging technologies. Pershing's intelligence officer, Maj. James A. Ryan, organized a highly effective "service of information" that gave Pershing a good knowledge of northern Mexico. Ryan made use of local informants, supplemented by the Army's own reconnaissance capabilities. These were extensive. A large part of the force consisted of horse cavalry, and for the last time in its history the Army fielded a force of twenty Apache Indian scouts. In addition, the Punitive Expedition was accompanied by the aircraft of the Army's 1st Aero Squadron, commanded by Maj. Benjamin Foulois, the first Army officer to learn to fly. The squadron attempted aerial reconnaissance and even brought along an aerial camera, although little came of these efforts. The planes were too underpowered to fly over the mountain ranges of Mexico and all eight initially assigned to the expedition crashed within two months.[32]

Finally, motor vehicles appeared in an intelligence role for the first time in the Army's history. Pershing's expedition was not only supported logistically by trucks, but also used a few for intelligence collection. Although rugged Mexican terrain and the limitations of the early motor vehicle meant that ground reconnaissance still depended on horse cavalry, the "radio tractors" of the Signal Corps deployed with Pershing's forces monitored Mexican government communications as Mexican authorities became increasingly alarmed at the American probe, which soon extended 500 miles into their sovereign territory. Although the Punitive Expedition was a limited success—Villa's troops were engaged and scattered, but the leader himself escaped, and war with Mexico almost ensued—it was a milestone in the Army's use of multisource intelligence.

On 1 February 1917, the Mexican problem was suddenly eclipsed by the German decision to wage unrestricted warfare against all vessels carrying supplies to the Allied Powers. In addition to threatening America's capacity to export, this act defied the principles of neutral rights, which the Wilson admin-

---

32 Clarence C. Clendenen gives a good account of the Punitive Expedition in *Blood on the Border: The United States Army and the Mexican Irregulars* (London: MacMillan Co., 1969). Chapter 17 of the book is devoted to "Airplanes and Motors."

istration had upheld since the beginning of World War I. As the United States teetered on the brink of war, all War College students were relieved of their normal duties and instructed to familiarize themselves with attache reports relating to the war in Europe. At the same time, Secretary of War Newton Baker recommended that each state appoint a National Guard officer to receive intelligence training.[33] However, when Congress finally declared war against Germany on 6 April 1917, the U.S. Army still had no intelligence organization. The Army essentially was moving blindly into the greatest foreign conflict in its history.

[33] Powe, *The Emergence of the War Department Intelligence Agency*, pp. 81–82.

2

World War I

The United States entered World War I almost completely unprepared: the National Defense Act which Congress had passed in 1916 had provided the basis of a mobilization plan, not an actual army. In early 1917 the country had only 210,000 men under arms, a third of them National Guardsmen who had been called up the previous summer to serve on the Mexican border. The Army had no permanent tactical organization above the level of the regiment and lacked adequate quantities of artillery, machine guns, tanks, modern aircraft, and even gas masks. Its General Staff organization was not designed to cope with the logistical and operational problems presented by a major conflict, and at the direction of the Wilson administration it had made no war plans. The Army had no intelligence organization.

Within seventeen months, however, the country had transformed itself into a fighting machine. With the help of the draft, the United States raised an Army of 4 million men; half of this great force was transported to France, where it provided the decisive margin that led to victory over Imperial Germany and its allies. American industry was also mobilized for war, but not soon enough, forcing Britain and France to supply the American Expeditionary Forces (AEF) in France with almost all required tanks, planes, and artillery. The General Staff was repeatedly restructured and finally became an effective instrument of control. And under the pressures of war, the Army was forced to develop new intelligence capabilities.

The development of Army Intelligence in World War I proceeded along two parallel but more or less separate tracks. At the War Department level, intelligence work was revived; by the end of the war, Military Intelligence had become a full-fledged staff element as one of four operating divisions of the General Staff. Concurrently, General John J. Pershing, commander of the AEF, built up his own field intelligence organization, structured along rather different lines to meet tactical needs. Pershing's ideas on Army reorganization and on the need for an intelligence apparatus were adopted by the War Department in organizing troop units and ultimately provided the basis for reorganization of the General Staff itself.

Van Deman and Military Intelligence

At the War Department level, the individual most responsible for rebuilding an intelligence apparatus was Maj. Ralph Van Deman, the General Staff officer who had lobbied vigorously but unproductively in the years before the war to re-create the Army's capabilities in this area. In 1917, with the United States at war, Van Deman tried again. He submitted a formal recommendation to Maj. Gen. Hugh Scott, the Army's chief of staff, urging the War Department to establish a Military Intelligence Division. This initiative was strongly supported by Van Deman's immediate superior, Brig. Gen. Joseph Kuhn, chief of the War College Division.[1] Unfortunately, the chief of staff was not receptive. Scott was an old-time cavalryman with an encyclopedic knowledge of Indian sign languages and a deep interest in packsaddles, but his former commander in chief, President William Howard Taft, had described his intellectual abilities as "wood to the middle of his head." By 1917 he was demonstrating a disconcerting tendency to fall asleep at Cabinet meetings.[2] Scott simply believed that the Army had no need for an intelligence organization: since America was now fighting a war as an ally of Great Britain and France, the United States could acquire whatever intelligence it needed from them.

Undeterred, Van Deman decided to adopt different tactics, employing what British military analyst Basil Liddell Hart would later describe in another context as the "indirect approach."[3] Using such diverse contacts as a lady novelist and the police chief of Washington, D.C., as intermediaries, Van Deman discreetly lobbied Secretary of War Newton D. Baker. Baker proved to be more receptive to the major's ideas, and on 3 May 1917, the War College Division replaced its moribund Military Information Committee with the Military Information Section headed by Van Deman.[4] Although far from an ideal organizational setup, with Military Intelligence subordinated to what was essentially a planning organization, it was at least a beginning.

The Military Intelligence Section began modestly, with Van Deman, two other officers (one retired), and two civilian clerks. Initially, its office space was confined to a balcony overlooking the War College Division's library. At first it had no data files, since the information collected by the old Military Information Division had been merged into the War College Division's general files and remained there, effectively lost. Its responsibilities, however, were considerable. In addition to supervising the existing Army attache system and

---

[1] Powe, *The Emergence of the War Department Intelligence Agency*, pp. 82–84.

[2] Finnegan, *Against the Specter of a Dragon*, p. 45.

[3] Sir Basil Liddell Hart, *Strategy* (New York: New American Library, 1974), p. 6.

[4] In his memoirs, Van Deman highlights his own role in bringing about the rebirth of Army Intelligence. *The Final Memoranda*, pp. 21–23. Marc Powe finds substantial continuities between the old Military Information Division and Van Deman's organization. *The Emergence of the War Department Intelligence Agency*, pp. 77–81, 102–03.

developing policies and plans for Army Intelligence activities, Van Deman's organization was charged with "the supervision and control of such system of military espionage and counterespionage as shall be established . . . during the continuance of the present war."[5] The section was thus not only to serve as a staff element but was also to perform operating functions.

In the beginning, Van Deman's organization depended heavily on the British and the French, who supplied it with watch lists of suspected enemy sympathizers and basic organizational concepts. From the British, Van Deman borrowed the fundamental division of intelligence into "positive" and "negative." Positive intelligence consisted of collecting information from the enemy; negative intelligence consisted of denying the enemy intelligence about one's own forces. An important part of negative intelligence was "counterespionage," another new word in the Army's growing intelligence vocabulary, this one borrowed from the French.

Doctrine and data could be borrowed from abroad, but personnel could not. Because of the demand for regular officers in combat assignments, no more than six regulars were available for intelligence duties at the General Staff during the whole war. To obtain additional competent personnel for his own organization, Van Deman used an informal "old boys" network that recommended civilians for direct commissions, a practice not uncommon in the World War I Army. Initially, many of these men were commissioned in the Signal Corps, since there were unused officer billets in the Aviation Section of that branch. Later, intelligence officers were hastily commissioned in whatever Army branch could afford to give up a few of its slots.

The buildup of the Military Intelligence element of the War Department General Staff took place at the same time that hundreds of additional intelligence officers had to be found for the Army's divisions and subordinate units. In July 1917 Pershing and the War Department agreed that intelligence staffs had to be provided to units down to the battalion level. Logically, this was an area in which the General Staff's intelligence organization should have had an interest. However, the Military Intelligence Section was too small to supervise the procurement and training of intelligence personnel for the field army. Instead, this was accomplished through normal Army channels. The process began in July 1917, when the adjutant general directed departmental commanders to select 160 specially qualified men from the newly established officer training camps for intelligence assignments. The ideal individual, the adjutant general advised, was a "young college instructor" with language ability.[6] The Signal Corps trained intercept operators and photo interpreters, and the Corps of Engineers trained topographic personnel. The Military Intelligence Section did process

---

[5] History of the Counterintelligence Corps, vol. 3, U.S. Army Intelligence Center, Fort Holabird, Md., 1959, p. 1.

[6] Ibid., p. 4.

applications for the Corps of Interpreters, a new Army organization of officers and noncommissioned officers set up in July 1917 to handle the Army's language functions. Later, it procured enlisted counterintelligence specialists.

Intelligence Operations

The General Staff's former Second Division had confined its efforts to gathering positive intelligence, employing the Army's military attache system to collect scientific, technical, and geographic data from abroad. Although the Military Intelligence Section was responsible for the lapsed functions of the older organization, it got off to a curiously slow start in collecting foreign intelligence. Until the end of 1917, only one officer was assigned to the task, and the principal target was Mexico. However, as his organization enlarged Van Deman was able to direct greater resources to this area. In doing so, Military Intelligence gained a broader definition. In addition to accumulating data on the military situation abroad, the Army began to collect information on economic, social, political, and even psychological factors worldwide. World War I was a global conflict fought between entire industrialized societies, where victory depended on more than military factors; the fighting armies were only the cutting edges of much larger swords. The War Department's Military Intelligence staff element thus became the functional equivalent of today's Central Intelligence Agency.

However, the War Department's efforts at collecting foreign intelligence were somewhat overshadowed by the fact that the AEF's general headquarters (GHQ) in France was 3,000 miles nearer the enemy and in a much better position to gather information on the European theater. Pershing had already established his own intelligence staff element, and this functioned almost autonomously. The great distances between the two separate organizations discouraged collaboration, as did Pershing's belief that he was responsible for the conduct of the war and that the only function of the War Department was to furnish him with the troops and supplies he needed.

Because of this, Van Deman directed much of his attention to the new field of negative intelligence, or counterintelligence.[7] This was an area in which the Army had little previous experience. Although the Army had conducted counterintelligence work during the Philippine insurrection, not since the Civil War had it contended with the problems of espionage, sabotage, or subversion in the continental United States. However, when the United States joined the war against Germany in 1917, it appeared that the country confronted a substantial threat from within. The America that entered World War I was still a nation of

[7] It should be noted that Van Deman's first intelligence assignment, in the Philippines, had been as a counterintelligence officer fighting insurrectos. There, he had "synthesized reports, analyzed captured documents, and provided pictures and descriptions of known revolutionaries." Brian McAllister Lynn, *The U.S. Army and Counterinsurgency in the Philippine War, 1899–1902* (Charlotte: University of North Carolina Press, 1989), p. 155.

immigrants, many newly arrived. German Americans were particularly suspect, but the War Department was also concerned about the loyalties of Irish Americans, Scandinavian Americans, and African Americans. In addition to the problems that might be posed by unassimilated ethnics, there was a substantial antiwar movement. Finally, opinion-makers at the outbreak of war had exaggerated ideas about the scope and power of the German espionage and sabotage organization within the country.

In 1917 the United States seemed almost defenseless against these perceived enemies from within. The Treasury Department had a Secret Service, but it was confined by law to narrowly circumscribed duties. The Department of Justice maintained the Bureau of Investigation, but the bureau's duties before the outbreak of war had largely consisted of investigating cases of fraud against the government. A few major cities had organized police "bomb squads" to deal with the anarchist threat of the period. The almost total lack of civilian resources in the field spurred the Army to launch its own major and wide-sweeping counterintelligence program.

In June 1917 Van Deman took his first step, setting up a War Department security force of civilian investigators drawn from the ranks of the New York Police Department's Neutrality and Bomb Squad. Its operations were cloaked in secrecy, with members working from a private office building in Washington, D.C., under the enigmatic designation "Personnel Improvement Bureau." At first intended as a guard force, the unit soon began screening military personnel and applicants for government employment. A month later, the Military Intelligence Section opened its first field office in New York City, also staffed by former New York City policemen. Six additional field offices were subsequently set up in other major cities and embarkation points to provide counterintelligence coverage.

This was only the beginning. The Military Intelligence Section was concerned particularly with the problem of possible subversion within the vast new citizen forces being raised by the draft. The draft act which Congress passed in May 1917 had been designed to tap as much of the national manpower pool as possible. Granting few exemptions, the act impartially swept up American citizens and resident foreign nationals, including citizens of enemy countries. Regarding this heterogeneous force as posing a serious threat to national security, Van Deman believed that the newly forming National Guard and National Army divisions were infested with German agents and sympathizers.[8] In October 1917 he ordered the divisional intelligence officers just assigned to these units to come to Washington, D.C., under tight security. Upon reporting, the officers were instructed to set up a secret surveillance program within their

[8] Intelligence officers professed to fear that "unless we proceed on an extensive and thorough scale, the enemy, with his existing system in the United States, will be stronger than we are right in our own army and we will be helpless." War Department General Staff, War College Division (WCD), MI-3, Provisional Counter Espionage Instructions, WCD 10148-37, INSCOM archives, Fort Belvoir, Va., Feb 1918, p. 3.

divisions. The program was later extended to Regular Army divisions and fixed installations with the assistance of a confidential pamphlet, "Provisional Counter-Espionage Instructions," drawn up by Van Deman's staff.

Van Deman conceived a comprehensive counterespionage program. It envisaged the creation of a clandestine agent network extending throughout the Army down to company level. Nets in each division would be managed by an assistant to the divisional intelligence officer. He would work through a system of anonymous collection managers known only to himself and to their own immediate superiors and subordinates within the apparatus. At the bottom of this secret pyramid, "operatives" placed in every company would submit intelligence reports on their fellow soldiers. At least two operatives, mutually unknown to one another, would be recruited from each company.[9] Reports emanating from this organization would be relayed by the divisional intelligence officer to the Military Intelligence staff in Washington for investigation.

Once this system was in place, it produced a growing stream of incident reports that drove the relentless expansion of the War Department's counterintelligence organization. To supplement the efforts of his overextended force of intelligence officers, Van Deman hired additional civilian detectives, recruited unpaid volunteers, and soon found a fresh source of investigative manpower in the enlisted counterintelligence specialists of a completely new military organization, the Corps of Intelligence Police.

The Corps of Intelligence Police (CIP)

The stimulus for the creation of this corps of enlisted investigators had originally come from the AEF. Soon after his arrival in Europe, Maj. Dennis E. Nolan, Pershing's intelligence officer, had become concerned about the possible security problems faced by American troops fighting on foreign soil. In 1915 Nolan had written alarmingly about the possibilities of German invasion; now his work took on a more concrete form. In early July 1917 he requested that the adjutant general provide him fifty company grade officers proficient in foreign languages. In addition, Nolan asked for "fifty secret service men who have had training in police work [and] speak French fluently."[10] This called for a category of intelligence personnel not previously imagined by anybody in the War Department, but in August the acting chief of staff authorized the creation of a fifty-man Corps of Intelligence Police made up of enlisted soldiers who would serve with the "rank, pay, and allowances" of sergeants of infantry.[11]

---

9 Ibid.

10 History of the Counter Intelligence Corps, vol. 3, p. 3.

11 As was later pointed out, the title of the organization was a little anomalous. "It was a 'Corps' that was not a 'Corps.' It was a 'counterintelligence' organization but called an 'Intelligence' organization and it was called 'Police' when it had no interest in crime, as such, and no police power." History of the Counter Intelligence Corps, vol. 3, p. 114.

Tasked with furnishing the appropriate personnel, Van Deman ran into difficulties. Private detective agencies seemed a likely source at first, but when told of the Army's requirements for French-speaking investigators, the head of the Pinkerton Agency countered, "There ain't no such animal."[12] The War Department was reduced to recruiting the first CIP agents through newspaper advertisements. The first contingent was assembled at Fort Jay in New York Harbor, given a month's training as infantry, outfitted with distinctive green-corded campaign hats, and shipped to France without civilian clothes or any instruction in intelligence work. Once overseas, the group was screened by French authorities, who rejected many as undesirables. Those who passed muster were then bustled off to Le Havre for instruction by veteran Allied counterintelligence officers.[13]

The initial group was not promising, but the need for enlisted counterintelligence specialists remained, and the formation of the CIP had set a precedent. The Military Intelligence Section found it increasingly difficult to staff its headquarters and expanding network of field offices with the existing mix of freshly commissioned reserve officers, civilian volunteers, and hired detectives. Officers were a scarce commodity, and competent civilian investigators were hard to find, especially since the War Department paid them only $4 a day plus expenses. Thus it seemed logical for Van Deman's organization to turn to the enlisted ranks of the Army to solve the personnel problems in the counterintelligence arena. The iron broom of the draft had swept highly qualified people into the ranks of the Army; men experienced in law, teaching, or insurance investigation were especially fit for counterintelligence work. Additionally, the military thought that investigations of Army personnel could be carried out most appropriately by other soldiers. In November the Military Intelligence Section requested that it be allotted 250 CIP agents to assist its counterintelligence program. Many of the civilians previously employed by Van Deman promptly enlisted in the Corps of Intelligence Police, including the twenty-three former policemen in the New York Field Office.

Expansion

The expansion of Van Deman's organization, largely driven by operational responsibilities in the counterintelligence field, in turn forced a growing specialization within the Military Intelligence staff. It was no longer possible for Van Deman and a small group of assistants to deal interchangeably with all aspects of positive and negative intelligence. The whole operation had to be put under a

---

12 *The Final Memoranda*, p. 37.

13 The commander of the Corps of Intelligence Police in France was Lt. Royden Williamson. His recollections, "As It Was in the Beginning with the Corps of Intelligence Police," 11 Aug 53, are in RG 319, NARA.

bureaucratic regimen. Between December 1917 and January 1918, Van Deman divided his organization into functional subsections, all according to the British practice with which he was now familiar. As the organization grew larger and more complex, it achieved a position of greater prominence within the War Department. In February, following a reorganization of the General Staff, the Military Intelligence Section was upgraded in status, becoming a branch of the newly established Executive Division. Since the Executive Division was burdened with diverse responsibilities, the reorganization was less than perfect. As one knowledgeable officer put it, its chief "could not know and would not know what MI was doing . . . when MI papers came up to him, they were like Greek to him."[14] In March the Military Intelligence Branch, overcrowded at the War College, moved to a seven-story apartment building in downtown Washington, D.C., where it was at least in closer proximity to the Army's center of administrative power.

The Military Intelligence Branch initially consisted of eight numbered sections. MI–1, MI–5, MI–6, and MI–7 were responsible for carrying out general support functions in the respective areas of administration, publications, translation, and management of confidential files. Later, MI–7 assumed responsibility for graphics. At first there was only one section, MI–2, exclusively dedicated to collating foreign intelligence, although MI–5 soon received the new mission of coordinating the collection efforts of the attaches. Two other sections were set up to manage aspects of counterintelligence: MI–3, which handled counterespionage in the military services, and MI–4, which dealt with civilian subversion.[15] MI–3 worked closely with over 400 divisional and installation intelligence officers who supervised the clandestine counterespionage system. Other subelements served specialized needs: administering the District of Columbia field office, dealing with the specific counterintelligence problems presented by foreign-born draftees, and overseeing programs that dealt with particularly sensitive Army branches such as the Air Service and the Chemical Corps. Thousands of investigations were conducted, but contrary to early fears, only a relatively small number of troops had to be removed. The draft-raised Army was loyal.

In addition to policing the Army's own ranks, Van Deman was concerned that spies and agitators in the civilian community might also threaten the Army or at least its mobilization base. At the same time that MI–3 was created, MI–4 came into existence to handle counterintelligence in the civilian sector. This section sought to cope with broad and ill-defined threats, initially concerning itself with labor unrest in the West, racial disturbances in the South and Southwest, and foreign disaffection in the polyglot cities of the East. Its operative premise

---

[14] Lt Col Frank Moorman, "Lecture Delivered to the Officers of the Military Intelligence Division, General Staff—Concluding Remarks by Brigadier General Churchill," 13 Feb 20, p. 16, Army Cryptologic Records, INSCOM.

[15] Bruce W. Bidwell, *History of the Military Intelligence Division, Department of the Army General Staff, 1775–1941* (Frederick, Md.: University Publications of America, 1986), p. 123.

was that "the misbehavior, disloyalty, or indifference of native Americans is as important a material of military intelligence as any other."[16] At one time or another, the organization involved itself in deportation cases, sabotage by organized labor, enemy finance and trade, and counterespionage work abroad.

To carry out its duties, MI–4 had to conduct an active liaison with many other government agencies, especially the Department of Justice, which alone had powers of arrest and prosecution in cases of civilian offenses against the military. MI–4 also relied on two civilian auxiliaries, the Plant Protective Service and the American Protective League. The Plant Protective Service was an organization of undercover civilian operatives originally established by the chief signal officer to protect the country's new aircraft industry. Subsequently it spread to other private plants working under government contract. Almost inevitably, the organization came under the aegis of Military Intelligence.

The American Protective League, larger and less official in character, comprised several vigilante groups originally put together to help the Department of Justice uncover spies. Once in place, it also began to assist local authorities in enforcing the draft act, and its activities brought it into a close working relationship with MI–4. The Army sought to curb the organization's excesses while still making use of its thousands of members: estimates of the league's strength ranged between 60,000 and 200,000, with the organization itself favoring the latter number. Ultimately, top American Protective League leaders were commissioned as officers in MI–4 to enhance military control over the league's activities. Although such paramilitary organizations appear alien to the American tradition, similar organizations existed in Great Britain and France, reflecting the intense and sometimes excessive nationalism of the period.

In addition to his pioneering work in establishing an Army counterintelligence organization, Van Deman also involved Army Intelligence in the exotic world of codes and ciphers. This was an area in which the Army as a whole already had some experience. Ciphers had been used in the Civil War, and the War Department had employed a telegraph code since 1885. More recently, in 1916, the Signal Corps' Capt. Parker Hitt had published a manual on military cryptography. However, it was Van Deman who made cryptology an adjunct of Military Intelligence. One of his first acts after setting up the Military Intelligence Section was to secure a commission for a youngish State Department code clerk, Herbert O. Yardley, so Yardley could head up a Cipher Bureau for Van Deman's organization. Although Hitt and a few other Regular Army officers possessed the necessary expertise in this field, all of them were needed for other duties when war broke out.

The Cipher Bureau, later redesignated MI–8, soon found itself caught up in a multiplicity of projects. Van Deman quickly saw that the Army had no means

---

16 War Department General Staff, Military Intelligence Division, *The Functions of the Military Intelligence Division, General Staff* (Washington, D.C.: Government Printing Office, 1918), p. 18.

of secure communications. The War Department Telegraph Code of 1915 in use for Army administrative communications was a cumbrous work designed to save telegraph costs rather than to provide security, and in any case, it was probable that the Germans already possessed a copy of the code book. Yardley's bureau was hastily directed to devise new enciphering tables for the code that once more made it practical for secret messages. MI–8 then prepared a completely new code that Military Intelligence as well as the rest of the Army could use. Regrettably, this was compromised as soon as it was issued, and a new code could not be prepared before Armistice Day. However, MI–8's own communications system, which made use of the new enciphering tables, remained secure and was used throughout the war as a channel to transmit messages from the secretary of war and the chief of staff to the field.

MI–8 was to have more success in breaking codes than in making them. It soon began to attack agent communications. This led Yardley's unit into the arcane world of secret inks, regarding which the British provided help and advice. It was forced also to learn to read the diverse systems of shorthand employed in the United States and abroad.[17]

MI–8's increasing responsibilities, together with the AEF's anticipated requirements in the area of codes, soon created a demand for trained cryptologic personnel. To meet the need, the Army turned to the only organization in the United States with cryptanalytic expertise. This was Riverbank Laboratories, a private research foundation set up by the eccentric philanthropist George Fabyan in Geneva, Illinois.[18] One of Fabyan's hobbies was attempting to prove that Shakespeare's plays contained hidden cipher messages revealing that the works had actually been written by Sir Francis Bacon. Fabyan was wrong—no such cipher existed—but his obsession had led to the creation of a center for cryptanalysis at Riverbank. This organization trained three classes of Army cryptanalysts in late 1917 and early 1918. The arrangement ended only when MI–8 developed its own training program. Ultimately, two Riverbank instructors accepted Army commissions and went to France as cryptanalysts with the AEF.

The cryptanalytic side of its work soon led MI–8 into other fields. To supplement physical interception of German messages, it established a radio intelligence service using selected Signal Corps personnel. These specialists monitored German diplomatic and agent communications, initially employing a chain of fourteen "radio tractors" strung out along the Mexican border and later using fixed intercept sites in the same locations. The radio intelligence service also had a large fixed station at Houlton, Maine, that monitored transatlantic German diplomatic communications.

---

17 David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: MacMillan Co., 1967), pp. 352–54.

18 Special Research History (SRH) 29, A Brief History of the Signal Intelligence Service, p. 1, RG 457, NARA (hereafter, these documents will be cited by SRH number).

The Military Intelligence Division

In April 1918 General Peyton C. March was recalled from France to become the new Army chief of staff. In June he ordered Van Deman, now a colonel, to go to Europe to inspect the intelligence operations of the AEF. Van Deman left behind a functioning Military Intelligence organization that had a strength of 170 officers and hundreds of enlisted agents and civilians and was still growing. The expansion forced the War Department to again move its intelligence headquarters, this time to the Hooe Building in Washington, D.C. However, the full development of the wartime Army Intelligence organization was not yet complete. Military Intelligence reached its final organizational development in World War I as a result of March's experiences with Pershing's AEF.

In August 1918 March restructured the General Staff, in the process raising the intelligence function to the status it enjoyed in France. He established the Military Intelligence Division (MID) as one of the four principal divisions of the War Department General Staff. The new division's enhanced prestige and responsibilities meant that Van Deman's successor, a Field Artillery lieutenant colonel from the AEF with the glorious name of Marlborough Churchill, was advanced to the rank of brigadier general. With these changes Military Intelligence had finally reached the position of institutional equality on the Army Staff that Van Deman had long advocated. In turn, this elevation in status permitted a more elaborate form of organization, with Positive and Negative Branches now controlling the various numbered sections.

One of the motives for the establishment of MID was March's desire to create an organization that could bring Army Intelligence training in the continental United States into line with the needs of the AEF. Military Intelligence had heretofore neglected this area for a number of reasons, including its limited charter, its concentration on counterintelligence activities, and its lack of jurisdiction over training. The perceived deficiencies of training in the United States had previously led Pershing to demand that all commanders and staff officers, including intelligence officers, spend a lengthy period in France prior to the arrival of their divisions. To help rectify this situation, MID recalled an experienced intelligence officer from France to head a new Field Intelligence Section, MI–9, that would provide MID input to the training camps. However, the war ended before the plans devised by the new element could be put into effect.

In the meantime, MID's counterintelligence operations underwent a further expansion. The Negative Branch extended the scope of its operations across the seas in September 1918, taking over supervision of the counterintelligence operations of military attaches. It also created a new section to handle passport control duties previously shared jointly by MI–3 and MI–4. The State Department had primary jurisdiction over foreign travel by American citizens, but MID also wanted to screen all individuals traveling to Europe. Military Intelligence was particularly interested in checking the backgrounds of the large

numbers of welfare workers sent overseas to support the AEF by the Red Cross, the YMCA, the Salvation Army, and other organizations.

The same month, MID also gained control over military censorship within the continental United States, setting up another new section, MI–10, to handle the assignment. Originally, Army censorship had been regarded as an independent function under a chief military censor, partially out of deference to the American tradition of freedom of speech. However, the general Army reorganization of August 1918 had made this an intelligence responsibility. MI–10's activities soon encompassed a wide variety of fields—in addition to censoring military mail and Army photographs, the organization also supervised a system of voluntary press censorship, ran a newspaper clipping bureau, accredited newspaper correspondents, monitored telephone and telegraph lines running into neutral Mexico, assumed direction of the radio intelligence service, and maintained liaison with other government departments. All this demanded a heavy commitment of personnel, and by the end of the war 300 people were on duty with MI–10.

In two areas the Negative Branch ventured completely beyond the normally defined boundaries of intelligence activity. The branch became involved in investigating graft and fraud within the Army and in finding ways to enhance military morale. In both cases, the transfer of these functions to intelligence came by default. Although the quartermaster general was originally assigned to deal with cases of graft and fraud, he had no trained investigative personnel. As a result, MI–13 was organized in August 1918 to assume the mission. The problem of Army morale was added to the MID agenda when Corps of Intelligence Police investigators included instances of low morale in their intelligence reports. Since MID had discovered the problem, it seemed appropriate to some members of the Army Staff that the division find a way to counter it. In this case, however, MID was able to reassign the function to a separate Military Morale Section of the General Staff in November 1918.

The armistice finally ended the headlong and rather undisciplined expansion of MID's activities. By this time, 282 officers, 250 CIP agents, and 1,100 civilians were on its staff. Van Deman's labors had succeeded in building up a massive intelligence organization that doubtless surpassed his wildest expectations. The establishment of MID had restored the intelligence function to the level of the General Staff, where it would remain from then on. However, in the process it had acquired broad ancillary functions the precise boundaries of which had yet to be defined rationally.

The American Expeditionary Forces in France

The American Expeditionary Forces in France built up an intelligence organization parallel, but not completely similar, to MID. When Pershing took command of the AEF, he designated Maj. Dennis E. Nolan as his intelligence officer.

Once in Europe, Pershing decided to adopt the French staff system throughout the AEF. Intelligence became the second section, or "G–2," of Pershing's headquarters staff. Intelligence thus achieved a position of equality with other functional areas in the AEF a year before it would do so at the General Staff level in the continental United States, and Nolan ultimately became a brigadier general.

Pershing arrived in France in June 1917 with a small headquarters and a hastily formed division of infantry. By November 1918 the AEF had grown to a force of twenty-nine combat divisions and had opened its own front against the armies of Imperial Germany. The expansion and elaboration of the Army Intelligence structure ran hand in hand with the growth of the AEF it supported.[19] Initially the AEF heavily depended on help from the British and French in this field as in many others. Intelligence officers assigned to document exploitation and prisoner-of-war interrogation were trained at the British intelligence school at Harrow until August 1918, when the AEF finally opened its own intelligence school at Langres, France. Students at Langres were provided with the unique opportunity to interrogate real prisoners of war as part of their training. From the start, the AEF trained its own photo interpreters and intercept operators.

By the end of the war, G–2 at Pershing's Chaumont headquarters had grown to a full-fledged theater intelligence center, engaging in a span of activities that was even broader than that of the Military Intelligence Division in Washington, since it also supervised deception operations and actively managed a propaganda campaign. In contrast, the work of MID's "psychological" subsection concentrated on coordination and training. The intelligence operations of Pershing's G–2 staff also overlapped and duplicated those of MID, because it produced its own political and economic intelligence as well as dealing in combat intelligence. Pershing considered that as a theater commander, his legitimate intelligence interests extended beyond the immediate Western front to cover developments on the Eastern, Macedonian, and Italian fronts. In Pershing's mind, any overlap with the activities of MID in the continental United States was justified because MID was an ocean away from the main battle and the transatlantic cable system had limited capacities.

The capstone of the intelligence pyramid, the Military Information Division, or G–2–A, produced finished intelligence reports and studies from the mass of information available from the AEF's tactical units and the other divisions of G–2.[20] The division was able to draw upon the full range of intelligence disciplines (human, photographic, and signals) to supply combat intelligence, and it also produced political and economic intelligence, mostly from open sources. The production activities of G–2–A had the result of involving the organization

---

19 There has never been a scholarly study of intelligence work in the AEF. British Military Intelligence in World War I has been better served. See Michael Occleshaw, *Armour Against Fate: British Military Intelligence in the First World War* (London: Columbus Books, 1990).

20 Reminiscences of the order of battle specialist on Pershing's G–2 staff are contained in Samuel T. Hubbard, *Memoirs of a Staff Officer* (Tuckahoe, N.Y.: Cardinal Associates, Inc., 1959).

in areas outside the field of pure intelligence: by the summer of 1918 G–2–A was also releasing the Army's daily public affairs communique and furnishing the War Department with a daily informational cable.

The base of this intelligence pyramid within the AEF began at the level of the battalion, the smallest unit with an intelligence staff officer, the S–2, and dedicated intelligence collection personnel.[21] In addition to its S–2, each infantry battalion had a reconnaissance element consisting initially of 1 officer and 28 enlisted men, including 15 scouts, 11 observation post personnel, and 2 snipers. At the next level of the command structure was a regimental intelligence officer, with 8 additional observers at his disposal. Brigades were not authorized intelligence officers under the original scheme of organization, but in practice intelligence personnel were frequently detailed to these commands.

At the division level, there was a small intelligence section headed by the divisional G–2, who was assisted by a deputy for combat intelligence, a commissioned interpreter, a topographic officer, and various enlisted personnel. This was the initial level for interrogating prisoners of war and collecting enemy documents. Ground observation at this echelon was supplemented by spotting reports from Army Air Service balloons forwarded through division artillery channels. Under World War I conditions, divisions were responsible for keeping watch over the section of enemy front opposite them for a depth of two miles. In practice, however, the length and breadth of a division's span of interest was often much larger.

Balloons were used primarily for observing artillery fire, but balloon units also provided intelligence, especially under the static conditions of trench warfare that prevailed on the Western front.[22] The main disadvantages of balloons were their vulnerability and their requirement for support personnel. A balloon in combat had an estimated life expectancy of fifteen minutes; although fliers did not wear parachutes in World War I, balloonists did. It took a full company of 178 men to service a single balloon, because it took many hands to deploy a balloon in a breeze and because each company was also responsible for manning six antiaircraft machine guns to defend its fragile aerial asset.

The intelligence officer at corps level used a wider array of resources that allowed him to take responsibility for surveillance of the area between two and five miles beyond the enemy's forward line of troops. In addition to observation posts and balloons, he used aero squadrons equipped for visual and photo-

---

21 *United States Army in the World War, 1917–1919*, vol. 13, *Reports of the Commander in Chief AEF, Staff Sections and Services* (Washington, D.C.: Government Printing Office, 1990), pp. 1–10; Maj Gen Dennis E. Nolan, Dictation of March 2, 1935: Echelons of Intelligence from the Front Line Back to G.H.Q., Nolan Ms, U.S. Army Military History Institute; Intelligence Regulations, American Expeditionary Forces, Aug 1918.

22 Balloons could ascend to an altitude of 4,500 feet, allowing observers to watch enemy positions eight miles away. Richard P. Weinert, *A History of Army Aviation, 1950–1962: Phase I: 1950–1954* (Fort Monroe, Va.: U.S. Army Continental Army Command, 1971), p. 2.

graphic reconnaissance and sometimes even flash- and sound-ranging troops who detected and targeted enemy batteries. These were under the command of the corps artillery headquarters but under the staff supervision of G–2. Five of the seven corps that the AEF committed to combat were supported by such troops.[23] The corps also had its own dedicated counterintelligence element consisting of twelve Corps of Intelligence Police sergeants.

The most sophisticated intelligence resources were concentrated in the field armies formed in mid-1918 and at GHQ, Chaumont. Each of the two field armies in the AEF had additional aerial reconnaissance units, including some that could operate at night.[24] A topographic battalion allowed the army-level intelligence staff to draw up large-scale war maps, termed *plans directeurs* in the jargon of the day. Each Army Intelligence staff also contained a radio intelligence section that translated intercepted enemy messages. A larger radio intelligence element at GHQ engaged in cryptanalysis and supplied the subordinate Army sections with the necessary keying material to decode the messages. Intercept was provided by Signal Corps personnel who operated direction-finding and intercept equipment and manned listening posts directed against low-level enemy telephone and ground telegraph communications, a task facilitated by the use of induction coils rather than by direct wiretaps.[25]

Pershing's radio intelligence organization not only monitored enemy ground communications, but also could track the movements of enemy spotter aircraft through their transmissions. Searchlight platoons of the 56th Engineers attached to the AEF's Antiaircraft Service provided early warning of night air attacks. These units were equipped with multihorn and parabolic acoustical detectors that alerted crews to the approach of aircraft before they were in visual range.[26]

At the top of this layered intelligence structure was G–2–A at Chaumont, which processed and analyzed the information sent up from lower levels. Its efforts were supplemented by those of three other, more specialized, divisions of G–2. The "secret service," G–2–B, supervised both undercover collection operations and counterintelligence. Although most of the intelligence obtained by Pershing's headquarters about political and economic develop-

---

[23] A participant documented this specialized technical activity in Edward A. Trueblood, *Observations of an American Soldier During His Service with the AEF in France in the Flash Ranging Service* (Sacramento, Calif.: News Publishing, 1919).

[24] The AEF experience produced the first clash between ground commanders and airmen over the priority to be given aerial reconnaissance. It would not be the last. Interestingly enough, the recalcitrant aviator was Col. William Mitchell. See Maj Gen Dennis E. Nolan, Dictation 38, p. 17 (1–31–36), Nolan Ms, U.S. Army Military History Institute.

[25] War Department, Office of the Chief Signal Officer, *Final Report of the Radio Intelligence Section, General Staff, General Headquarters, American Expeditionary Forces* (Washington, D.C.: Office of the Chief Signal Officer, 1935). An anecdotal treatment of these activities can be found in E. Alexander Powell, *The Army Behind the Army* (New York: Charles Scribner's Sons, 1919), pp. 16–22.

[26] William Barclay Parson, *The American Engineers in France* (New York: D. Appleton and Co., 1920), pp. 256–61.

ments in Germany came from open sources, G–2–B did set up "information centers" in Switzerland, Denmark, and Holland that ran agent nets behind the enemy lines. The most valuable contribution of clandestine intelligence probably came from the reports of the "trainwatchers" who monitored rail movements of the German army.[27] G–2–B's information centers competed directly with the MID-directed activities of the military attache offices in the same neutral countries and depended heavily on British and French assistance. The British and the French were also called upon for assistance in counterintelligence. However, the development of the Corps of Intelligence Police gave G–2–B an instrument of its own in this field. By Armistice Day some 450 sergeant investigators were on duty with the AEF, not only supporting the rear communications zone, but also providing intelligence coverage to corps and divisions at the fighting front.

Mapping was normally a function of the Corps of Engineers. But under combat conditions in France, it fell under the supervision of the intelligence staff, since battle maps included information about enemy as well as friendly forces. G–2–C, the Topographic, Map Supply, and Sound- and Flash-Ranging Division of G–2, essentially served to coordinate the activities of the 29th Engineers, a bizarrely structured regiment without a headquarters that provided the AEF with both topographic and sound- and flash-ranging personnel. One battalion of the 29th manned the AEF's large map-printing facility at Langres; another supplied topographic troops to the field armies; ranging companies from two additional battalions supported the targeting needs of the field artillery while providing collateral intelligence.

Finally, a fourth division, G–2–D, handled press and censorship matters. Censorship operations were an intelligence function within the AEF from the very beginning. While mail was censored at the unit level, a base censor's office in Paris conducted spot checks of regimental mail, operated a secret-ink laboratory, and censored mail written in foreign languages. Internally, the section was able to translate mail written in forty-nine languages, requesting outside help only for messages written in Chinese or Japanese. One additional function of this office was to censor letters containing information that servicemen did not want their immediate superiors to see. Such correspondence was mailed in specially issued blue envelopes.

Managing press relations was the division's second principal function. This included supervising the accreditation of war correspondents, censoring their dispatches, and making arrangements for their transportation and billeting. In view of practices in later wars, correspondents were held on a fairly tight rein.

---

[27] Bidwell, *History of the Military Intelligence Division*, p. 139. General Nolan felt that no more than 15 percent of his intelligence requirements were filled by secret agents, but felt that reports by the network of trainwatchers tracking German rail movements across the bridges over the Rhine were most useful. Memoirs, ch. 4, p. 9, Dennis Nolan Ms, U.S. Army Military History Institute.

Censorship principles insisted on accuracy; forbade releasing military information useful to the enemy; and prohibited news stories which would "injure morale in our forces here, or at home, or among our Allies" or "embarrass the United States or her Allies in neutral countries."[28] On the other hand, correspondents had free access to the troops, and G–2–D refrained from using them for propaganda.

In addition, G–2–D carried out a wide spectrum of other information-related activities. It was charged with preparing propaganda to undermine German morale—by the fall of 1918 a rain of 3 million propaganda leaflets from G–2–D was blanketing German lines, distributed by plane and balloon and even by rifle grenade and patrol. And while it sought to undercut German morale, the division tried to preserve that of the AEF. The famous troop newspaper, *Stars and Stripes*, was published in Paris under G–2 auspices. Finally, straying even further from any conceivable intelligence functions, the division supervised the Army art program, employing the services of eight soldier-painters, and was tasked with taking photographs for historical purposes and verifying the accuracy of their captions.

Communications Security in the AEF

Communications security within the American Expeditionary Forces in France was primarily a Signal Corps responsibility. Although MI–8 was responsible for preparing the War Department's codes, in France this task was assigned in December 1917 to the Signal Corps' Code Compilation Section, a small group located at the GHQ at Chaumont. This organization found itself confronted by an immense task. The Army entered World War I with few effective arrangements for secure tactical communications. The insecure and cumbersome War Department Telegraph Code was intended for administrative use, not battlefield communications. The Signal Corps' existing cipher disk was a simple celluloid device designed on principles as uncomplicated as those of the toy code-rings that once appeared in cereal boxes. When used with a running key, however, at first it seemed to offer unbreakable security. However, cryptanalysts at Riverbank and at MI–8 quickly discovered that messages encrypted this way could be broken faster than they could be enciphered. The British introduced the U.S. Army to the Playfair cipher, but this too was easy prey for cryptanalysts.

As a result, the AEF decided to devise a completely new system. The first efforts were unsuccessful. The Code Compilation Section produced a one-part trench code and a set of enciphering tables, but these proved to be impracticable for use in combat situations. What was needed was a method of encryption that would place as little burden as possible on communicators operating under

---

[28] *United States Army in the World War*, vol. 13, p. 86.

battlefield conditions.[29] The solution finally adopted was the creation of a set of two-part codes with separate tables for encoding and decoding. In June 1918 the section produced the "Potomac Code," the first in a series of codes named after major American rivers. The "river" codes were issued to the First Army when it became active in August 1918. When the Second Army took the field in October, a separate "lake" series of codes was introduced to meet its needs. These codes, distributed down to regimental level through intelligence channels, carried the main burden of Army traffic, supplemented as necessary by a small number of more specialized codes. To ensure security, individual code books were replaced about every two weeks or upon evidence that they had been compromised.

Regrettably, the sophistication of the AEF's cryptographic systems did not equate with good communications security. The mere fact that codes were available did not mean that they were used. Communicators unfamiliar with codes showed a marked disinclination to employ them, and tactical units evolved various private, unsanctioned codes of their own. Moreover, the AEF relied on the telephone rather than the radio for the bulk of its communications, and officers repeatedly sent plain-language messages on tactical matters over unsecured telephone lines. To eliminate such problems, the AEF's general headquarters issued security guidelines for Army communications and established its own Security Service. Signal Corps personnel assigned to the Security Service monitored radio and telephone communications and reported violations of established procedures to control officers at the radio intelligence sections within the headquarters of the field armies. The G–2 then reported security breaches to commanders, but little could actually be done to punish offenders.[30]

Sideshows

The bulk of American forces committed overseas in World War I went to France. However, it is sometimes forgotten that there were some peripheral ventures. An infantry regiment and support troops were hastily deployed to the Italian front to help shore up the morale of the flagging Italian Army after its disastrous defeat at Caporetto in the fall of 1917. More importantly, two separate American Expeditionary Forces, miniatures of the larger AEF in France, were sent respectively to Murmansk and Siberia in the summer of 1918 as a result of the Bolshevik Revolution, which had forced Russia out of the war and

---

[29] "In view of the fact that code work is frequently done under heavy bombardment and gas or in the critical moments of an advance, it does not seem advisable to add any additional burdens to code operators." War Department, Office of the Chief Signal Officer, *Report of the Code Compilation Section, American Expeditionary Forces, December 1917–November 1918* (Washington, D.C.: Office of the Chief Signal Officer, 1935), p. 1.

[30] James L. Gilbert, "U.S. Army COMSEC in World War I," *Military Intelligence* 14 (January 1988): 19–21.

created conditions of chaos in Eastern Europe. Both expeditions were launched on ill-defined missions and given little background intelligence.

The reinforced regiment ordered to North Russia, originally assigned the limited mission of keeping a large store of war supplies from German hands, became involved in operations against the Bolsheviks as part of a much larger Allied effort and only evolved a G–2 section of its own shortly before the force was withdrawn in early 1919. However, Bolshevik propaganda and war-weariness after the armistice did confront the unit with serious problems of subversion.

A larger force under Maj. Gen. William S. Graves went to Siberia to help rescue former Czechoslovakian prisoners of war from the Bolsheviks and incidentally to keep an eye on the Japanese intervention force sent on a similar mission. Since the initial American contingent deployed from the Philippines and included elements from the Philippine Department's Military Intelligence Division, it incorporated an intelligence section from the beginning. Additional intelligence personnel from the continental United States joined the force later. Unfortunately, intelligence efforts were largely stultified by a conflict between General Graves and his G–2 concerning the nature of the latter's responsibilities. Graves pursued a policy of strict neutrality towards the Bolsheviks and vetoed any attempt to gather intelligence by using the services of the anti-Bolshevik "White" forces.[31]

Conclusion

World War I was the watershed in the evolution of U.S. Army Intelligence. Both in the War Department and in the field intelligence work was revitalized and placed on a footing of organizational equality with other major functions. The Army ventured into new fields of counterintelligence and cryptology and made use of the full spectrum of intelligence sources. Although some of these—such as prisoner of war interrogation, captured document exploitation, and ground reconnaissance—were traditional, the newer disciplines of signals intelligence, aerial photography, and collection through sensing devices were not. At both the War Department and theater levels, the definition of Military Intelligence was enlarged to include the collection of political, economic, and social data. Finally, intelligence activities were expanded to include the allied fields of deception and propaganda.

The professional intelligence field was still, however, in its infancy. Intelligence was still considered essentially a staff-level activity within the Army. No intelligence units as such were fielded, although the Army did deploy a topographic engineer regiment and aerial observation groups to France. A table of

---

[31] The prominent historical novelist Kenneth Roberts served on the intelligence staff of the Graves Expedition. His recollections of the experience can be found in his autobiography, *I Wanted to Write* (Garden City, N.Y.: Doubleday and Co., Inc., 1949), pp. 98–112. I am indebted to Col. William Strobridge, U.S. Army (Ret.), for calling my attention to this fact.

organization for a field-army radio section—a communications intelligence unit—was drawn up, but never implemented, as Pershing chose to keep his limited intercept assets under direct GHQ control. Moreover, Army Intelligence was not yet considered an official career field. After the war, both Van Deman and Nolan became major generals, but they achieved their stars as tactical commanders, not as intelligence officers. Still, compared with the past, much had been accomplished. For Army Intelligence, World War I represented a great leap forward.

As an Army Intelligence organization was put together from nothing in the space of seventeen hectic months, many mistakes were made. MID largely concentrated its efforts on counterintelligence operations directed at a threat that proved to be largely imaginary.[32] Yet its concern, however misplaced, reflected widespread perception among American leaders. The year before war broke out, even President Wilson's closest confidant, Colonel House, fretted that "there are more German reservists here [in the United States] than I thought."[33] More telling is the criticism that MID spread itself too thinly by venturing into areas like fraud investigation and morale enhancement. Even some of its foreign intelligence efforts could be questioned. MID maintained files on areas as remote from the war effort as the Antarctic islands and on topics as broad as "Christendom."[34] Similarly, G–2 in the AEF became deeply involved in press relations, a precedent which confused the duties of intelligence with those of public information in a way that would have an adverse application for Army Intelligence in the twenty years of peacetime following the armistice.

Nevertheless, the Army had at last established a permanent structure for meeting its intelligence needs. After 1918 the evolution of Army Intelligence would follow a twisted road, but it would never return to the marginal position it had occupied prior to World War I.

---

32 There were also questions as to the efficacy of the whole effort. On the eve of America's entry into World War II, the officer who then headed the Corps of Intelligence Police provided a scathing evaluation of the World War I counterintelligence program. "In the United States the Corps of Intelligence Police was composed of many well-meaning but inexperienced officers, enlisted men, and civilians and their unorganized efforts accomplished practically nothing. It is said the organization in the United States may have caught one spy." History of the Counter Intelligence Corps, vol. 4, p. 122.

33 Finnegan, *Against the Specter of a Dragon*, p. 149.

34 Memo for Acting Director, Military Intelligence Division, 24 Apr 20, MID Documents

3

Military Intelligence Between Wars

Woodrow Wilson had declared that America entered World War I to make the world safe for democracy. The effort had not succeeded. Four great empires had collapsed in Central and Eastern Europe, creating a revolutionary battleground for many disparate and competing political ideologies. Novelist John Dos Passos later described the year 1919 as a time for "machinegunfire and arson, starvation, lice, cholera, and typhus."[1] The peace process went awry. The victors at Versailles saddled the new republican government of Germany with great territorial losses and reparations payments while allowing it to remain the strongest and most industrialized power on the European Continent. Meanwhile, the growing problems posed by the widening revolution in Russia went unaddressed, and animosities developed rapidly among the victors. Wilson had hoped that the peace settlement, however flawed, would be redeemed by the establishment of a collective security organization, the League of Nations. But his own Senate refused to ratify the measure as America retreated toward isolationism.

Within the United States, there was also unrest as the bonds that had held the nation together during the war began to dissolve. Motivated by wartime idealism, pundits had spoken vaguely of a postwar era of "reconstruction" that would lay the basis for an "industrial democracy" in which the American economic cornucopia would be shared more equitably by all.[2] Instead, the end of the war brought unemployment, inflation, and labor unrest. Alarmed by revolution abroad and radical labor agitators at home, the country was swept by a "Red Scare" leading to thousands of arrests. In the end, a fatigued American people, weary of wartime idealism and stress, voted for Warren G. Harding and a return to "normalcy."

Military Intelligence was intimately involved in these events, both at home and abroad. Twenty MID officers accompanied President Woodrow Wilson and

---

[1] John Dos Passos, *U.S.A.: Nineteen Nineteen* (Cambridge: Houghton Mifflin, 1946), p. 281.

[2] For example, see William Leavitt Stoddard, "The Shop Committee—Some Implications," The *Dial* 67 (12 July 1919): 7–8; "Reconstruction Miscellany," The *Survey* 42 (31 May 1919): 375.

the American delegation to the Paris Peace Conference. Sixty CIP agents, directed by Van Deman, provided security for the American party, and Maj. Herbert O. Yardley of MI–8 furnished cryptologic support.[3] Meanwhile, Army Intelligence personnel accompanied the new Third Army, the American occupation force that marched into the Rhineland under provisions of the armistice. On the domestic front, Bolshevik agents replaced German spies as the focus for MID's counterintelligence efforts. In the fall of 1919 a naive MID officer warned that "the situation in the United States [was] . . . verging on revolution."[4] However exaggerated the estimate, it accurately reflected the fears of many Americans who found the world changing too fast for America ever to recover her lost innocence.

Military Intelligence at Peace

Normalcy meant a return to a peacetime Army, a process that had begun almost as soon as the fighting ended. The vast conscript armies that had won the war were hastily demobilized, and a new volunteer force enlisted. Subsequently, the National Defense Act of 1920 provided for a Regular Army of 280,000, backed up by Organized Reserves and a 475,000-man National Guard. The command and control of this force would be exercised through nine corps areas in the continental United States and through three overseas departments in Hawaii, the Philippines, and Panama. Under the terms of this legislation, MID retained its place as one of the four principal divisions within the Army Staff. Among its numerous duties were administering the attache system, supervising military drawings and maps, writing regulations for tactical intelligence personnel, performing liaison with other intelligence agencies, approving codes and ciphers, and planning censorship operations. As one of the four assistants to the chief of staff authorized by law, MID's director was given the rank of brigadier general.

Unfortunately for the Army, the economy-minded Congress never provided the necessary appropriations to maintain the authorized force. By 1929 the Regular Army had thus shrunk to a strength of 137,000, with four skeleton combat divisions in the continental United States and three more in the overseas departments. That part of the force assigned to the continental United States was scattered over a multitude of tiny posts inherited from the Indian Wars. The subsequent Great Depression made Congress even more parsimonious, forcing the Army to make do with the large but increasingly obsolescent stockpile of weapons left over from World War I. The Military Intelligence Division was directly affected by these policies, dwindling from a peak strength of 80 officers

[3] Some of the CIP agents in Paris questioned the utility of their assignments. Apart from the men detailed to guard President Wilson, one wrote, they were employed as "a species of bell boys, ladies maids, and hallmen." Gilbert Elliott Ms, p. 7, RG 319, NARA.

[4] Memo, Col C. H. Mason for Brig Gen Marlborough Churchill, 31 Oct 19, sub: Sinister Inertia in Present United States Situation, MID Documents.

and about 160 civilians in 1920 to a cadre of 20 officers and fewer than 50 civilians by 1934, and undergoing repeated internal realignments.[5]

The reorganization of the Army Staff under General John J. Pershing also weakened Military Intelligence. After becoming chief of staff in 1921, Pershing imposed the AEF's wartime model of a five-part General Staff on the Army, directing that separate divisions be established for personnel, intelligence, operations and training, supply, and war plans. However, congressional legislation had provided for only four brigadier generals on the staff, and in the savage competition for general officer slots the intelligence staff often lost. Of the seven directors of the Military Intelligence Division who served between 1922 and 1939, only two were brigadier generals.[6] Military Intelligence thus became a second-class citizen, since its lesser position on the Army Staff was reflected throughout the rest of the Army. Implicitly, U.S. military leaders seem to have accepted the dictum of British Field Marshal Sir Douglas Haig that "intelligence is rather a special kind of work and has a very small place in the army in peacetime."[7]

This trend was reinforced by Pershing's insistence that G–2 undertake public relations duties as it had done in the AEF. Under peacetime conditions, these responsibilities became one of the Military Intelligence Division's principal functions. Intelligence officers at corps level and below also spent much of their time in this secondary area. As a result, intelligence work often became a dumping ground for officers incapable of performing any more demanding activities, and astute officers regarded intelligence assignments as detrimental to their military careers. According to intelligence historian Thomas Troy, "intelligence was neither a profession [n]or a career; at best, it was a one-time activity in an army or navy officer's service. Hence, when closely scrutinized, the intelligence services [were] small, weak stepchildren of their parent organizations."[8]

The weakness and lack of professionalism of Army Intelligence during this period was reinforced by the decline in its capabilities for intelligence collection. The attache system remained MID's principal means for collecting foreign intelligence, irregularly supplemented by arrangements made with American businessmen working abroad. General George Marshall would write later that interwar military intelligence was "little more than what a military attache could

---

[5] From 1920 on, MID strength was affected by the provisions of the National Defense Act of 1920, which limited the number of General Staff officers on duty in Washington, D.C., to 93. This meant that MID would be allotted 14 to 16 General Staff officers. When the law took effect, Brig. Gen. Dennis Nolan, assistant chief of staff, G–2, hoped that 31 more officers could be detailed from the line to keep MID up to what he regarded as minimum strength. In this, he was disappointed. Memo, Nolan for Chief of Staff, 28 Jul 21, sub: Relief of Thirteen Line Officers on Duty with Military Intelligence Division To Date, MID Documents.

[6] Memo for Chief of Staff, 19 Jun 37, sub: Increase in Number of Assistants to the Chief of Staff, MID Documents.

[7] Maj. Gen. Sir Kenneth Strong, *Men of Intelligence* (New York: St. Martin's Press, 1972), p. 34.

[8] Thomas F. Troy, *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency* (Frederick, Md.: University Publications of America, 1984), p. 6.

learn . . . at a dinner, more or less, over the coffee cups."[9] Even here the limitations were severe. Postwar economies forced the abandonment of a number of minor attache posts, and the scarcity of funds dictated that attache assignments be restricted to officers with private means of support, irrespective of their professional qualifications. Finally, the interwar years saw the rise of totalitarian governments and controlled and closed societies. Military attaches were allowed increasingly less freedom to collect useful intelligence in precisely those countries that posed the most dangerous threat to American security.[10]

Army Intelligence in the domestic arena was equally weak. This was partially the result of a general public reaction to some of the excessive actions of the Wilson administration against dissidents, both in World War I and during the postwar "Red Scare." Fortunately the impoverished peacetime volunteer Army had little to worry about in the way of threats posed by espionage, sabotage, and subversion. Thus the Army discontinued its countersubversive system in 1920 and recalled all MID regulations on the subject from the field. With only six agents on duty, the Corps of Intelligence Police narrowly escaped extinction when wartime emergency legislation expired that same year, but MID managed to keep the organization alive by detailing personnel to CIP duties from the Army's Detached Enlisted Men's List. The Negative Branch of MID, which had supervised the War Department's counterintelligence work, was less fortunate and closed shop in 1921.

All attempts to collect domestic intelligence ended soon afterward. This was caused by the rash actions of Lt. W. D. Long, an intelligence officer at Vancouver Barracks, who sent a circular letter to the county sheriffs of Oregon asking them to maintain a surveillance of suspect organizations. Included on the lieutenant's list were veterans' groups, the Nonpartisan League, and the American Federation of Labor. This list caused a considerable uproar when inevitably it was made public. The secretary of war ordered that all intelligence posts in the Army not authorized by tables of organization be discontinued, and that intelligence officers confine themselves to instructing troops in combat intelligence techniques. This left most of the forty-five CIP agents authorized in 1920 with little to do, and the force was repeatedly scaled back. By 1934 the Corps of Intelligence Police consisted of just sixteen noncommissioned officers, and a subsequent survey found that most of them were used as classified file clerks rather than as investigators. Only in the overseas departments and in the Eighth Corps Area on the Mexican border did the Corps of Intelligence Police still provide useful services.[11]

---

[9] Ibid., p. 15.

[10] One especially aggressive attache was Maj. Truman Smith. Posted to Nazi Germany, Smith obtained intelligence reports on the *Luftwaffe* from the American aviator and popular hero Charles Lindbergh, who repeatedly toured German aircraft factories as a guest of Reichsmarshal Hermann Goering and other Nazi top brass. *Washington Post*, 4 Nov 84, p. A–3.

[11] Of the 16 CIP agents surveyed, 10 were acting as confidential clerks for G–2s in the various corps areas, 5 were engaged in investigative work, and 1 was unfit. History of the Counter Intelligence Corps, vol. 4, p. 87.

If the Military Intelligence Division was collecting little foreign and less domestic intelligence over most of this period, it was not overly active in other areas. Although one section of MID was charged with intelligence training, it had no statutory responsibility to supervise such work, and the assistant chief of staff for operations and training refused to acknowledge its authority. As a result, in 1931 the head of the section was forced to confess that "the state and extent of combat intelligence training in the Army is not known to this branch, as it makes no inspections and receives no training reports."[12]

Another section of MID was charged with supervising the Military Intelligence Officers Reserve Corps (MIORC), which had been formed in 1921 to use the services of the large number of officers who had served in intelligence positions throughout the wartime Army. In theory this organization of reservists should have given the Army a trained and experienced mobilization base, but many reserve officers were in fact journalists who had served G–2 in public affairs positions, and by the time they were ultimately needed, they were too old and too high ranking to fill the positions the Army required. The younger reservists in MIORC had never served on active duty. Perhaps the only lasting contribution of MIORC was the adoption of the sphinx as its insignia, an action which had the effect of permanently associating this somewhat bizarre heraldic item with the field of Military Intelligence.[13]

Not everything was completely bleak in the intelligence field between the wars. Although hobbled by budgetary restraints, the Army began to take advantage of new technological developments that expanded the possibilities of intelligence collection. Advances in motorized transport significantly enhanced the Army's ground reconnaissance. By 1931 an Experimental Mechanized Force had been created—its scout element had armored cars and radio-equipped vehicles—and the cavalry began to field mechanized units in addition to its traditional horse troops. The Army Signal Corps experimented with methods of detecting aircraft and ships through thermal and electronic means, and by 1937 the Army had a pilot model of a mobile radar set. Although limited to short-range targeting functions, the principles it embodied would apply to more powerful sets that could perform an early-warning function, filling a critical gap in Army capabilities after the increased speed of aircraft had rendered acoustical techniques almost useless.[14]

The growth of the Army Air Corps also affected intelligence. Air Corps officers were incorporated into MID, and Air attaches supplemented the work of the regular military attaches abroad. At the technical level, aircraft development

---

[12] Bidwell, *History of the Military Intelligence Division*, p. 362.

[13] Ltr with Incl, ACSI–DO, 25 Feb 63, Organization Day for Military Intelligence file, INSCOM History Office.

[14] Radar developments in the Army up to 1941 are covered in Dulany Terrett, *The Signal Corps: The Emergency*, United States Army in World War II (Washington, D.C.: U.S. Army Center of Military History, 1956). For early experiments, see pp. 44, 46–47.

was steady, since this was the one part of the Army that Congress was willing to fund. The Air Corps made significant advances in aerial photography, including night photography, and in aerial mapping techniques, all of which potentially enhanced intelligence gathering. Much of the pioneering work in this area was done by Lt. George Goddard, who would ultimately go on to become an Air Force brigadier general.[15]

In practice, the technological advancement of the Army Air Corps was a two-edged sword. The observation squadrons of World War I had flown in flimsy biplanes, and these aircraft could take off from grassy strips and work in close support of tactical commanders. But the sophisticated high-speed monoplanes with ample "greenhouse" canopies which the Air Corps developed in the 1930s for observation work, otherwise advanced machines with greatly improved performance, no longer could operate from unimproved airstrips. Furthermore, aeronautical progress encouraged Air Corps leaders to aspire to an independent role. The Air Corps became increasingly interested in fighting an air war of its own, instead of providing ground support. Aerial reconnaissance was thus designed to support a strategic bombing campaign, not to assist the tactical commander on the battlefield. By 1935 most aircraft had been placed under the direct control of General Headquarters, Air Corps. Although observation groups were still assigned to Army corps areas, only eight observation squadrons were active, a trend that threatened to deprive Army commanders of adequate air intelligence support.[16]

The "Black Chamber" and the Signal Intelligence Service

Army Intelligence made its greatest advances in the field of cryptology during the years between the wars. Following World War I, MI–8's previously comprehensive responsibilities in this field were realigned. The Signal Corps took over the responsibility for communications security, employing William F. Friedman, a former AEF officer and Riverbank Laboratories cryptanalyst, as a one-man code compilation bureau. The Adjutant General's Office was tasked with printing and distributing the codes. Officially, MI–8's responsibilities were reduced to approving cryptosystems for Army-wide use and establishing regulations for their employment. In reality, however, MID continued to be deeply

---

15 Goddard has provided a useful autobiography in *Overview: A Lifelong Adventure in Aerial Photography* (Garden City, N.Y.: Doubleday, 1969).

16 Robert F. Futrell, *Command of Observation Aviation: A Study in Control of Tactical Airpower* (Maxwell Air Force Base, Ala.: Air University, 1956), p. 2. It should be noted that balloons and dirigibles were in the Army inventory of reconnaissance platforms in the early 1920s. A short but helpful overview of Air Corps support to ground operations between the wars is provided by Weinert, *A History of Aviation, Phase I*, pp. 2–4. In *Army Air Corps Airplanes and Observation, 1935–1941* (St. Louis: U.S. Army Aviation Systems Command, 1990). Howard Butler offers an alternative view to the standard interpretation of Air Corps history, arguing that the Air Corps remained firmly under the thumb of a ground Army–dominated General Staff during this period.

involved in cryptanalysis. In the fall of 1919 retired Maj. Herbert O. Yardley, wartime chief of MI–8, set up a clandestine government cryptanalytic unit in a brownstone house in New York City. Jointly funded by MID and the State Department, Yardley's bureau continued to work on diplomatic code–breaking, a task that MI–8 had initiated in World War I. Using material provided secretly by some of the major U.S. cable companies, Yardley and his small civilian staff achieved several notable successes, the most important of which was breaking the Japanese diplomatic code in time to give American diplomats a key negotiating edge during the Washington Peace Conference of 1921–1922.[17]

Despite the success of Yardley's bureau in producing hard diplomatic intelligence, it still ran into difficulties. Peacetime economies sharply reduced its funding. By 1929 the organization consisted of Yardley himself and a handful of assistants, and its functions seemed increasingly less relevant to both its sponsors. The United States had just signed the Kellogg-Briand Pact purportedly outlawing war, the international order seemed stable, and the State Department saw little need for secret intelligence in a world without enemies. On the other hand, the Army had no direct peacetime interest in the diplomatic cryptosystems Yardley's group exploited, while the clandestine and civilian nature of his bureau prevented its serving as a training vehicle for Army Intelligence reservists. By the spring of 1929 there was already a move to centralize all Army cryptologic functions under the Signal Corps, using Friedman's office as a nucleus. When Henry L. Stimson, a rather excessively upright statesman of the old school, became secretary of state that year, Yardley's fate was sealed. Discovering that the State Department had obtained access to decoded diplomatic messages, Stimson withdrew funding from Yardley's bureau. His attitude was later described: "Gentlemen do not read each other's mail."[18]

Loss of funding led to the termination of Yardley's organization. Yardley and his colleagues were offered employment in the new Signal Corps cryptologic agency, but they declined. The Civil Service pay scale could not match salaries subsidized by MID confidential funds. Instead, Yardley attempted to recoup his fortunes by writing *The American Black Chamber*, which publicly exposed America's code-breaking activities for the first time. The work was a best-seller, but proved to be a major diplomatic embarrassment for the United States and only further damaged American intelligence efforts. Yardley would later work as a cryptanalyst for Chiang Kai-shek in China and for the Canadian government, but he would never again be allowed to hold a position in any U.S. cryptologic organization.

---

17 Yardley recounted—some say embellished—his accomplishments in his book, *The American Black Chamber* (New York: Bobbs-Merrill, 1931). A brief biography can be found in David Kahn, *Kahn on Codes; Secrets of the New Cryptology* (New York: MacMillan Co., 1983), pp. 62–71.

18 Kahn, The *Codebreakers*, p. 360. A detailed study of the rise and fall of the Yardley organization is contained in SRH 29, A Brief History of the Signal Intelligence Service, pp. 3–12.

Upon the demise of Yardley's bureau, Army cryptanalysis and Army cryptography were both integrated into a new Signal Corps element, the Signal Intelligence Service (SIS), which also assumed responsibility for secret inks. The new unit was set up within the Signal Corps rather than the Military Intelligence Division to reduce its visibility and better meet the technical requirements of signals intelligence. After 1934, when it took over the printing and distribution of codes from the Adjutant General's Office, the SIS became the focal point for all Army cryptologic activity.

Friedman, who headed the Signal Intelligence Service until an Army officer became director in 1935, quickly recruited a small but talented staff. The four principal members of his initial group—mathematicians Solomon Kullback, Frank Rowlett, and Abraham Sinkov and Japanese linguist John Hurt—would all become prominent figures in U.S. Army cryptology in World War II. At first the thrust of the work was oriented towards theory, training, and the development of advanced cryptographic systems. The Army had fought World War I using codes. In 1922 the Army adopted a simple cylindrical cipher device, the M94, for tactical operations.[19] Friedman introduced a more secure but cumbersome strip cipher device, the M138. More importantly, he began developmental work on machine ciphers. The SIS provided the Army with the M134 and M134A "converters" to protect top-level communications. These were electromechanical cipher machines of great sophistication and security.[20] Meanwhile, in 1936 Friedman and Rowlett hit upon the cryptographic principles of an even more advanced machine cipher device. Unfortunately, funding was not immediately available to put the prototype into production.

The Signal Intelligence Service also began to set up an intercept organization, which Yardley's bureau, with its dependence on cooperative cable companies, had never attempted. A Provisional Radio Intelligence Detachment was organized at Fort Monmouth, New Jersey, in 1933. We may discern something of the flavor of the times from the fact that its first commander found none of the twelve men in his unit present for duty when he assumed command—all had been detailed to President Franklin D. Roosevelt's Civilian Conservation Corps. This detachment was later expanded to become a provisional company, and the 1st Radio Intelligence Company was formally activated at Fort Monmouth in 1938. Meanwhile, in September 1936 the Signal Intelligence Service had set up a chain of numbered monitoring stations in the overseas departments and in the Eighth and Ninth Corps Areas, creating SIS

---

19 The M94 was the brainchild of Joseph O. Mauborgne, an Army Signal Corps officer who later became a major general and Chief Signal Officer. It was an exact copy of a device invented by Thomas Jefferson.

20 The early history of the Signal Intelligence Service is described in SRH 131, Expansion of the Signal Intelligence Service. For the use of the term "converters," see SRH 349, Achievements of the Signal Security Agency in World War II, pp. 42–43.

detachments in five signal service companies. Since the Federal Communication Act of 1934 had made it illegal to divulge foreign communications, this had to be accomplished under tight security.[21]

These initial arrangements for providing the SIS with an intercept capability were not completely satisfactory. Tasking the 1st Radio Intelligence Company with an operational assignment interfered with the unit's primary mission, training for deployment in the field to support tactical elements. In addition, the intermingling of intercept and regular communications personnel in the existing signal service companies not only posed a security threat, but also worked against effective personnel management. Under Army regulations, trained intercept personnel working abroad were automatically returned to the general Signal Corps pool when they returned to the continental United States and thus were lost to the SIS. To solve these problems, a centralized signals intelligence unit, the 2d Signal Service Company, was set up at Fort Monmouth on 1 January 1939 to control all Signal Corps personnel at the permanent monitoring installations. The result was an efficiently functioning Signal Intelligence Service and an intercept organization that would represent the Army's principal strength in the intelligence field.[22]

The SIS paid less attention to intelligence collection at the tactical level. Under the Army's Protective Mobilization Plan, a World War I–style general headquarters was to be fielded in the event of any crisis demanding troop mobilization, and available troops would be concentrated as needed under one of the four field armies into which the Army had been divided in 1933. The actual field army selected would depend on the direction from which the threat was expected. These plans also specified that the existing 1st (and only) Radio Intelligence Company be placed in support of GHQ. To provide signals intelligence at field army level, the Signal Corps relied on the National Guard to organize two additional radio intelligence companies, one on each coast.[23] These modest preparations would soon be overtaken by the rush of events.

---

21 The sensitivity of the whole topic of communications intelligence during this period may be inferred from a revealing piece of Signal Corps correspondence on the subject, which ended with the statement "It is suggested that this letter be burned after perusal." Ltr, Lt Col Dawson Olmstead, Executive Officer, Office of the Chief Signal Officer, to Col Joseph O. Mauborgne, 28 Jun 36, sub: Comment on Lieut. Corderman's Report, Army Cryptologic Records.

22 G. R. Thompson and Dixie R. Harris, *The Signal Corps: The Outcome*, United States Army in World War II (Washington, D.C.: U.S. Army Center of Military History, 1966), pp. 333–35.

23 Ltr, Maj Gen Joseph Mauborgne, Chief Signal Officer, to Chief, National Guard Bureau, 13 Sep 38, sub: Organization of National Guard Radio Intelligence Companies, Army Cryptologic Records.

4

Military Intelligence in Crisis

Ominous developments in the latter part of the 1930s finally woke the Army out of its long torpor. The Great Depression, which had ravaged the economy of the United States and focused the interests of the American people on domestic problems, had also profoundly rearranged the international order and set the stage for the rise of totalitarianism and the advance of aggression. Adolf Hitler was sworn in as chancellor of Germany in January 1933. He quickly turned his country into a one-party dictatorship. Under Nazi rule, Germany rapidly rearmed and entered into alliance with Fascist Italy and militarist Japan. International crises developed with monotonous regularity. Germany occupied the Rhineland in 1936, swallowed Austria in the spring of 1938, and humiliated Czechoslovakia with the disastrous settlement at Munich in the fall of that year. Meanwhile, its junior partners were also active. The Italian dictator Benito Mussolini invaded Ethiopia in 1935, and Japan, having seized Manchuria in 1931, went to war against all of China in 1937.

Britain and France responded with massive rearmament programs, but in the short run they relied on a general policy of appeasement to avert a European war, while ignoring Soviet attempts to resurrect their old World War I alliance with Russia. The American reaction was guarded. At President Franklin D. Roosevelt's direction, the Federal Bureau of Investigation (FBI) began investigating Nazi and Communist subversion in 1936, and Congress authorized modest steps to rebuild the nation's neglected defenses.[1] The size of the Army was increased, and the Military Intelligence Division was allowed to enlarge its attache system. Slowly, it also edged back into the counterintelligence arena, setting up a small Counterintelligence Branch in April 1939. That summer, concern about foreign espionage caused the Army to issue its first regulation dealing with the security of military information.[2] At the same time, the Army and

[1] Richard G. Powers, *Secrecy and Power: The Life of J. Edgar Hoover* (New York: Free Press, 1987), p. 229.

[2] The Army Regulation, AR 380–5, much revised, is still in effect.

the Navy formed the Interdepartmental Intelligence Committee with the FBI to coordinate the handling of espionage cases. However, the real threat to America's national interests would not be from within, but from without.

On 1 September 1939, the armed forces of Nazi Germany invaded Poland. Two days later, in response to previous treaty commitments, Britain and France declared war on Germany. World War II had begun. President Roosevelt proclaimed American neutrality but indicated that he did not expect American citizens to be neutral in their thoughts. On 8 September he declared a state of limited national emergency.

The U.S. Army of 1939 was unprepared for conventional warfare. As Army Chief of Staff General George C. Marshall later confessed, "We had no field Army. There were bare skeletons of three and one-half divisions scattered in small pieces over the entire United States."[3] Army troop strength was a little less than 174,000 men, and much of the equipment was still of World War I vintage. Although the Army Air Corps had received the lion's share of Army appropriations and attention, the planes of its sixty-two squadrons were obsolete by the standards of European combat. The restrictions imposed by the National Defense Act of 1920 on the size of the War Department General Staff were still in force.

The structure of the Army's intelligence element reflected the weakness of the whole. The Military Intelligence Division's small staff, still headed by a colonel, consisted of 20 officers, 3 enlisted men, and 46 civilians. Its elements were dispersed among four office buildings in the Washington, D.C., area. Intelligence collection was limited largely to what could be derived from the attache system. Although this system belatedly had been expanded, the representational nature of the attaches' mission necessarily limited the intelligence value of the product. Worse, only 16 Corps of Intelligence Police agents were available to provide counterintelligence support to the entire Army. The Signal Corps' Signal Intelligence Service had just 14 civilians and 1 Army officer on its Washington staff when Europe went to war, and they were not yet in a position to generate substantive intelligence. Efforts to rectify this situation were slow. In October 1939 a new intercept station was set up at Fort Hunt, Virginia. In November the Army authorized 26 additional civilians for the SIS. The headquarters of the 2d Signal Service Company moved to Washington, D.C., that same month, allowing it closer proximity to the Signal Intelligence Service which it supported.

In the spring of 1940 the deceptive tranquility of the "phony war" in Europe ended. In April Germany invaded Denmark and Norway, and in May Hitler launched his main offensive in the West. When it was over, a little more than a month later, France lay prostrate, Germany controlled Western Europe, and only a beleaguered Great Britain and the broad reaches of the Atlantic

---

[3] General George C. Marshall, *Biennial Report of the Chief of Staff of the United States Army, July 1, 1943, to June 30, 1945, to the Secretary of War* (Washington, D.C.: Government Printing Office, 1945), p. 117.

Ocean stood between the United States and the triumphant forces of totalitarianism. Meanwhile, in the East, Japan threatened to take advantage of the situation by incorporating the orphaned colonies of the beaten Western democracies into her "Greater East Asia Co-Prosperity Sphere." The world had been turned upside down.

At this point the United States at last began to look to its defenses. The Regular Army was now rapidly increased in size, Congress passing no less than three Supplemental Appropriations Bills for 1941, funding an Army of one million men. The legislation instituted a one-year draft, federalized eighteen National Guard divisions, and placed Reserve officers on active duty, while the Army organized a wartime General Headquarters. By the fall of 1940 the United States had negotiated a Destroyers-for-Bases deal with Great Britain, securing strategic military bases in British possessions in the Atlantic and Caribbean in exchange for fifty over-age destroyers. More important, during the second half of 1940 and throughout 1941, the Roosevelt administration labored strenuously to clear away or bypass neutrality legislation that impeded American support to Great Britain. This process slowly paved the way for American entrance into the war well before the Japanese attack on Pearl Harbor.

All these events had a great effect on Military Intelligence. Brig. Gen. Sherman Miles, the former military attache to Great Britain, took over the Military Intelligence Division, and the organization began to grow rapidly. As always, however, its initial priority was domestic, and its planners fretted tirelessly about German espionage and sabotage on the home front. In June 1940 MID, the Office of Naval Intelligence, and the FBI signed a formal delimitations agreement. Under its provisions, the FBI would take the lead in domestic intelligence; there would be no repetition of the World War I scenario in which Military Intelligence had assumed responsibility for surveilling American civil society. The agreement did give the Army responsibility for conducting investigations of those civilians employed or controlled by the military in the continental United States and of all civilians in the Canal Zone and the Philippines. That same month, the Military Intelligence Division sent out confidential instructions to intelligence officers, ordering them to set up a countersubversive program that would bring potential hostile agents on military installations to its attention. To handle these efforts, the Corps of Intelligence Police was expanded to an authorized strength of 42 agents in July and 188 in November.

MID planners were also concerned about the possibilities of German penetration into Latin America, where there were large ethnic German communities and important German business interests. Although the delimitations agreement had given intelligence responsibilities in this region to the FBI, the Army's Military Intelligence Division, with its existing attache system and military missions in Latin America, would not be denied a role. Thus, in July 1940 it moved to strengthen its capabilities for collecting foreign intelligence on Latin America by setting up a branch office in New York City. It seemed that the location

would provide both better access to reference material and improved relationships with American corporations doing business south of the border. About the same time MID was relieved of its responsibilities for supervising Army public relations, a function that would have diverted it even further from its primary missions, had it not been moved elsewhere.

While the Military Intelligence Division worried about domestic subversion and Fascist infiltration of Latin America, the more prosaic and demanding intelligence tasks were performed elsewhere. The Army Air Corps wanted an independent role in the field of intelligence, even though Air Corps officers were serving on the MID staff. Largely as a result of Air Corps initiatives, in September 1940 all the Army's technical services were directed to form their own intelligence staffs to collect information on foreign equipment and techniques, areas in which MID appeared to have little interest.[4] In addition, intelligence staffs were created for GHQ, for the new defense commands that sprang into existence, for the Army Air Forces when they gained autonomy in July 1941, and for subordinate tactical formations. The Engineer Reproduction Plant of the Corps of Engineers was transformed into the Army Map Service, laying a foundation that ultimately would provide indispensable cartographic intelligence for the American military.[5]

Even before it was assigned responsibility for technical intelligence, the Signal Corps was deeply involved in intelligence- and security-related activities. Its major contribution was in cryptanalysis. In August 1940, after twenty months of effort, a team of SIS civilians succeeded in breaking the Japanese diplomatic machine cipher. The unraveling of the riddle of the so-called Purple machine was accomplished by purely cryptologic means, without any access to the machine itself. The Purple analog built by SIS experts allowed the United States to read Japanese diplomatic messages as fast as their intended recipients. The strains of this intellectual accomplishment ultimately sent William Friedman, the senior cryptanalyst, into the hospital with a nervous breakdown. However, the feat allowed the United States to follow the tortuous workings of Japanese diplomacy starting in the fall of 1940.[6] Within a short time, the Army shared intercept and exploitation of the Purple material with the Navy on a daily rotating basis. The resulting decrypts of Japanese diplomatic communications were assigned the code name MAGIC, and their contents were closely controlled. At times, however, the arrangement led the

---

[4] Bidwell, *History of the Military Intelligence Division*, p. 305.

[5] Blanche D. Coll, Jean E. Keith, and Herbert Rosenthal, *The Corps of Engineers: Troops and Equipment*, United States Army in World War II (Washington, D.C.: U.S. Army Center of Military History, 1958), pp. 441–42.

[6] Ronald William Clark, *The Man Who Broke PURPLE: A Life of the World's Greatest Cryptographer, Colonel William F. Friedman* (Boston: Little Brown, 1977), is the only full length biography of Friedman. Its worth can perhaps be gauged by the fact that there are two errors in the title: Friedman was a cryptologist, not just a cryptographer, and his highest rank in the Army Reserve was lieutenant colonel.

services to become rivals in rushing juicy tidbits produced by cryptanalysis to the attention of high officials.

The success of the SIS against Purple facilitated its expansion, and another hundred persons were added to its headquarters. Additional personnel were needed not only to perform cryptanalysis and translation, but also to meet the cryptographic needs of a much larger Army, especially since the SIS was now introducing important technical innovations in this area. The organization procured two new devices to improve the security of Army communications at both the tactical and strategic levels. For the first purpose, it acquired the rights to a small compact machine cipher designed by Swedish inventor Boris Hagelin. Under the designation M209, this became the mainstay of Army tactical communications. For high-level communications, SIS adopted the M134C electromechanical cipher machine from the Navy, assigning to it the short title SIGABA. Friedman and Rowlett had originally designed this machine, but prewar budgetary constraints had made it a Navy project. The SIGABA used rotors instead of one-time tapes for enciphering, and this gave communications arrangements much greater flexibility.[7]

The Signal Intelligence Service was not the only Signal Corps element involved in intelligence-related activities. The Signal Corps also had responsibility for radar. By May 1940 the corps had successfully developed fixed and mobile early-warning radar sets. The first radar-equipped aircraft warning company began operations in Panama a month later. This would have a substantial long-term effect on the evolution of Army Intelligence. Some Army officers defined radar itself as "another highly specialized type of signal intelligence."[8] But radar would also become an intelligence target, and its widespread use by all major powers would ultimately lead to the development of what is sometimes called the electronic battlefield.

1941: MID on the Brink

During 1941 the Military Intelligence Division grew to a strength of 200 officers, supported by 848 civilians. In addition to its New York branch, the organization now maintained regional offices in New Orleans and San Francisco to collect foreign intelligence. The changing nature of the international situation had finally refocused collection activities on Germany and Japan, as well as Latin America. However, MID's traditional primary information source, the attache system, had only limited capabilities against wartime Axis powers, even though it had grown to encompass 136 attaches on duty in 50 countries. In February 1941 Brig. Gen. Sherman Miles, the assistant chief of staff, G–2,

---

7 SRH 349, pp. 43–44, 46–47.

8 Memo, Air Communications Division, Signal Corps, 26 Nov 41, sub: Recommendations on Signal Intelligence Manual MID SR 30–60, Army Cryptologic Records.

concluded that it was "imperative that the Army develop an efficient espionage service that can function independently of any nation," but nothing was done to implement this concept.[9]

The perceived inadequacies of American Military Intelligence in a situation of growing crisis caused deep concern. In April Miles fretted that "this Division has expanded considerably since last May, but always in a piecemeal manner," and admitted that "the work being done by the division is still far below what should be expected of the military intelligence of a great power in our present situation."[10] Others agreed, notably the president of the United States. In June 1941 Roosevelt appointed prominent lawyer and World War I hero William J. Donovan as coordinator of information, with a large mandate to establish an organization to collect intelligence and conduct radio propaganda.[11] But such an edifice could not be constructed overnight and its early efforts were, not surprisingly, somewhat amateurish. An agent dispatched to the Pacific, for example, reported that there would be no war that year, while Donovan's central staff estimated the combat strength of the German *Luftwaffe* at 29,000 war planes when in fact it was only 3,100.[12] Given the lack of urgency that characterized MID's own approach to collecting foreign intelligence on America's most probable enemies, Donovan's organization filled a vital need. But this did not preserve it from the enmity of MID, which resented the intrusion of a civilian organization with powerful political backing into what it regarded as its own preserve.

The clash between the two organizations was exacerbated by MID's having acquired an interest of its own in the area of propaganda in 1941. Unfounded credit had been given to German proficiency in manipulating public opinion and the subsequent role of propaganda in bringing about the defeat of France. Moreover, since the United States was not yet a belligerent, a radio war was about the only one in which it could participate actively. In July 1941, therefore, MID set up a special study group on "psychological warfare" under conditions of strict secrecy. Rivalry between MID and Donovan's office in this area thus began almost immediately and continued unabated even after America entered the shooting war and it became clear that it would take more than slogans to defeat the enemy.

---

[9] History of the Counter Intelligence Corps, vol. 4, U.S. Army Intelligence Center, 1960, p. 125.

[10] Memo, Brig Gen Sherman Miles for Chief of Staff, 12 Apr 41, sub: Project for the Expansion of the Military Intelligence Division, MID Documents.

[11] Troy, *Donovan and the CIA*, pp. 63, 74.

[12] To be sure, the Army's estimates of *Luftwaffe* strength were almost equally exaggerated. See David Kahn, "U.S. Views of Germany and Japan," *Knowing One's Enemies: Intelligence Assessment Before the Two Wars*, ed. Ernest May (Princeton: Princeton University Press, 1984), pp. 492–93.

Counterintelligence Concerns

Although MID's role in foreign intelligence and propaganda provided a matter for dispute, coexistence with the FBI in the field of domestic intelligence was less of a problem, as the delimitations agreement gave the Army its own secure sphere of activities. However, Army Intelligence developed growing pains as it sought to fulfill its responsibilities. The Corps of Intelligence Police had expanded elevenfold by the beginning of 1941, and this expansion changed the nature of the force. Until then the appointment of CIP personnel had been centralized at the War Department level, but in January of that year appointment authority for agents was decentralized to the corps area and overseas department level in an attempt to gain more manpower. At the same time, MID authorized the creation of the Office of Chief, Corps of Intelligence Police, and the establishment of a CIP training school. The Army also approved the detail of officers to the Corps of Intelligence Police. In addition, to conduct specialized investigations, the Army attempted to recruit African-American and Asian-American agents for the first time in the organization's history.

The Corps of Intelligence Police continued to expand during the course of 1941. In April it was authorized a strength of 288 enlisted men, and this figure was raised to 513 in May. The growth was accompanied by renewed disputes over the degree to which the recruitment, assignment, and promotion of CIP agents should be centralized and who should supervise investigations. Traditionally, the G–2s of the various corps areas and departments had carried out the latter function. But the reserve officer who became the first head of the Corps of Intelligence Police, Maj. Garland Williams, wanted a centralized organization structured along the lines of the FBI, with its chief responsible to the secretary of war for "detecting and investigating" all matters pertaining to espionage, sabotage, and subversion.[13] He also believed that the decentralized personnel arrangements impaired the quality of his manpower. However, all proposals to strengthen the powers of the chief, Corps of Intelligence Police, were vigorously rebutted by the commanders in the field, and these arrangements remained unchanged. Williams protested in vain that this meant he would have to deal with "14 different policies, 14 different practices, 14 different methods of work, and, in general, 14 separate and distinct units."[14] The unhappy officer was soon reassigned to the Infantry School.

Lack of adequate central control over operations in the field thus presented a serious problem for the entire investigative effort. Agents too often were misused by commanders unfamiliar with counterintelligence work. On the other hand, the investigative work load in some commands resulted in agents' being pressed into service without ever undergoing basic training. And as the Army

[13] History of the Counter Intelligence Corps, vol. 4, p. 123.
[14] Ibid., p. 122.

adjutant general later explained to one of the corps area commanders, delegation of personnel procurement authority to the field had resulted in the recruitment of "a larger percentage of agents whose character, education, adaptability, and experience in no way qualified them for the duties they would be called upon to perform."[15]

Another type of problem presented itself when a rival organization emerged in the counterintelligence field. In September 1941 the newly created Provost Marshal General's Office took over the function of conducting all personnel background investigations of civilians applying for military or defense-related employment. Ninety CIP agents were transferred to the new organization, further intensifying both the shortage of manpower and the lack of centralized direction. For a time, the demands of the work load forced the Army to hire civilian investigators to supplement its force of CIP agents.

The Road to Pearl Harbor

Manpower problems were not restricted to the Corps of Intelligence Police, but were pervasive throughout the Army Intelligence community in 1941. The vast expansion of the nation's intelligence apparatus threatened to outstrip the supply of qualified people in all services. Although the Army reservists of the prewar Military Intelligence Officers Reserve Corps had been called up, only 573 existed, many of whom were actually public relations specialists rather than trained intelligence officers. Reserve intelligence training had not been an Army priority. Although the Corps of Intelligence Police and the Signal Intelligence Service now had specialized schools, located respectively at Chicago, Illinois, and Fort Monmouth, New Jersey, there was no institute to train intelligence personnel in other disciplines. The Operations and Training Division stubbornly refused to give the Military Intelligence Division any authority over intelligence training in general. Only in the area of language instruction was there some progress: a handful of officers were enrolled in language programs overseas, and the Fourth Army established a language school at the Presidio of San Francisco in the fall of 1941. By the end of the year, ninety students were learning the Japanese language.

But even if trained intelligence personnel had been available, there would have been little for them to do besides manning the traditional tactical intelligence staffs. The need for communications intelligence personnel and cryptanalysts was serious but limited, and there was no organization for gathering human intelligence or for acquiring information on a large scale. At the initiative of the State Department, both the Army and the Navy had briefly posted a handful of undercover agents in French North Africa in 1941, but these men were transferred to the control of Donovan's new agency soon after it came into

---

15 Ibid., p. 110.

existence in the summer of that year.[16] The entire intelligence apparatus thus seemed too disparate and too disorganized to pull itself together for the great contest ahead.

On the positive side, Army Intelligence could draw on the resources of an experienced ally for the first time since World War I. In 1941 secret staff talks between the top military leaders of the United States and Great Britain were accompanied by an intelligence liaison between the two countries. In February 1941 a party from the Signal Intelligence Service visited Great Britain and established a limited collaboration in the field of cryptology. The Americans brought with them a Purple analog for the British Government Code and Cypher School, the British cryptanalytic organization, thus furnishing the British with the solution for a cryptanalytic problem that had baffled their best efforts. This marked the beginning of a cooperation that would bring the United States unparalleled benefits. In the summer of 1941 a permanent British liaison officer was assigned to SIS. The British also helped out in other intelligence-related areas. In September 1941, for example, the Army dispatched an Electronic Training Group of 300 second lieutenants to England to study British developments in radar.

By the end of 1941 the Army had also put together a tactical signals intelligence organization. Seven signal radio intelligence companies numbered in the 100 series were now active, including the original 1st Radio Intelligence Company, now redesignated the 121st Signal Radio Intelligence Company. Additionally, there was a signal radio intelligence company, aviation, designed to provide communications intelligence to the Army Air Forces.[17]

However, there were still grave deficiencies in battlefield intelligence capabilities. Apart from the success of the Signal Intelligence Service in decoding Japanese diplomatic communications, the Army had only limited sources of intelligence collection and no way of moving intelligence down to commanders in the field, who still tended to rely on their own resources, much as they had done in the nineteenth century. The use of MAGIC, the Army's most valuable intelligence source, highlighted the problem. The cryptologic success of the SIS was simply not matched by intelligence exploitation of the product. Because the decrypts were so sensitive, they were closely held—only a few individuals within MID and the highest military and political figures in the administration were aware of their existence, and intelligence analysts were kept out of the picture for security reasons. As a result, although policy makers were exposed to individual messages, there was never an attempt to put the flow of the material into an ordered framework. As Friedman later put it, "each message represented only

---

16 Ray S. Cline, *The CIA Under Reagan, Bush, and Casey* (Washington, D.C.: Acropolis Press, 1981), pp. 64–66.

17 War Department, Adjutant General's Office, *Directory of the Army of the United States and War Department Activities, July 1941* (Washington, D.C.: War Department, 1941), p. 32, and August 1941, p. 33.

a single frame, so to speak, in a long motion picture film"; unfortunately, nobody was in a position to see the whole movie.[18] The same security considerations denied key Army and Navy field commanders any knowledge of the existence of the material.

And so, in the end not even MAGIC could save the United States from military surprise at Pearl Harbor, when the Japanese attacked at dawn on 7 December 1941. High-level Japanese diplomatic messages had simply not contained any mention of Japanese military plans; consular messages had contained clues, but resources had not been available for the timely exploitation of low-level traffic. The Japanese Navy codes were still unbroken, and the Japanese fleet that struck Pearl Harbor had approached its target under strict radio silence. Although radar manned by the Signal Corps' Air Warning Service Company, Hawaii, had detected the Japanese attack formation 130 miles away, the reports were misconstrued at the operations center and no alert had been given. Pearl Harbor was both a military disaster and an intelligence failure.[19] Confronted by attack in the Pacific and a German declaration of war, Army Intelligence prepared to set matters right and bring victory out of defeat.

---

[18] SRH 125, Certain Aspects of "Magic" in the Cryptologic Background of the Various Official Investigations into the Pearl Harbor Attack, p. 63.

[19] The best study of the intelligence failure at Pearl Harbor remains Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962).

Nineteenth-century intelligence collectors: scouts and guides of the Union Army in the Civil War.

In 1908 the War Department's intelligence organization moved to new quarters at the Army War College on the grounds of present-day Fort McNair in Washington, D.C., and soon lost its separate identity.

Pioneers of Military Intelligence. *Clockwise*, Col. Ralph M. Van Deman, who reestablished the General Staff's Military Intelligence organization in World War I; Col. (later Brig. Gen.) Dennis Nolan, G–2 of the American Expeditionary Forces (AEF) in France; Brig. Gen. Marlborough Churchill, first chief of the restored Military Intelligence Division. (*NARA*)

Intelligence in World War I: AEF interrogators question German prisoners of war. (*NARA*)

Technology at the service of intelligence: an Army aerial photographer. (*NARA*)

Herbert O. Yardley, intelligence hero and villain. In the 1920s his clandestine "Black Chamber," jointly funded by the War and State Departments, broke the Japanese diplomatic code; then he wrote a book about his accomplishments. (*National Security Agency*)

After 1929 the Army's tiny but supremely effective Signal Intelligence Service (SIS), headed by William F. Friedman, took over the dual mission of code-breaking and code making. The Army's peacetime cryptologic successes would be repeated in World War II. (*U.S. Army Intelligence and Security Command [INSCOM]*)

In 1942 the SIS relocated to Arlington Hall, a former girls' school in Arlington, Virginia. The organization was soon redesignated as the Signal Security Agency (SSA). (*INSCOM*)

SSA personnel decrypt Japanese diplomatic traffic enciphered by the PURPLE machine. (*INSCOM*)

SSA guarded the security of U.S. Army communications, designing and producing electro mechanical cipher machines like the SIGABAs used in this communications center. (*INSCOM*)

Officers of Signal Security Detachment D, the field operating arm of the Signal Intelligence Service, European Theater of Operations. (*INSCOM*)

A Counter Intelligence Corps agent of the 94th Infantry Division questions a source in the European Theater of Operations. (*NARA*)

Soldiers of the elite Alamo Scouts reconnoitered Japanese-held islands in support of the Army's campaigns in the Southwest Pacific Area (SWPA). (*NARA*)

Postwar headquarters of Army Security Agency Europe, in the I. G. Farben building, Frankfurt, Germany. (*INSCOM*)

A Nisei Counter Intelligence Corps agent shows his badge to a sentry of the 23d Infantry Division during the occupation of Japan. (*NARA*)

5

World War II
Military Intelligence at the Center

World War II confronted the U.S. Army with the problems of fighting a global conflict across enormous distances. The beginnings were not easy. During the first six months of fighting in the Pacific, the United States suffered an unprecedented string of military reverses. German U-boats in the Atlantic ravaged the sea lanes until early 1943, creating a serious shortage of shipping that threatened America's capacity to project its power overseas. However, the military problems were manageable. America's vast industrial base allowed the United States to equip a mobilized Army of 8 million men, with 89 divisions and over 1,000 squadrons of aircraft. By the end of 1943 much of this vast force had been deployed overseas. Following preliminary operations in North Africa and the Mediterranean, the invasion of Normandy in June 1944 allowed the U.S. Army to bring its main forces to bear against Germany on the decisive battlefield of continental Europe. In the Pacific, the secondary theater of war, America eventually launched a two-pronged attack on the Japanese Empire from bases in Australia and Hawaii. By August 1945 the war had been brought to a triumphant close.

The history of Military Intelligence in the war was paradoxical. Largely because of the success of British and American cryptanalysts in exploiting enemy communications, the Army ultimately was provided with better intelligence than it had ever enjoyed in its history. Yet all during the war, there was a constant drumfire of criticism directed against Military Intelligence. In late 1943 Secretary of War Henry L. Stimson agreed with his colleague, Secretary of the Navy Frank Knox, that "our two intelligence services are pretty bum."[1] The same year Admiral Ernest King complained of "overlaps and wasted effort in the various activities" of Army and Navy Intelligence.[2] In retrospect, the Army's World War II deputy chief of staff, Lt. Gen. Joseph McNarney, stated that Army G–2 "was always a headache for the War Department and was reorganized con-

[1] Troy, *Donovan and the CIA*, p. 317.
[2] Ibid., p. 316.

tinuously and unsuccessfully throughout the war."[3] Although the intelligence end product was superb, the machinery that produced it was beset by disorder. The situation was not improved by a high rate of turnover in MID's leadership: between 1941 and 1944, the Army had four different assistant chiefs of staff, G–2.

The onset of the war led inevitably to major changes in Army Intelligence. Pearl Harbor provided an obvious spur to greater efforts at interservice coordination on intelligence matters. A Joint Intelligence Committee (JIC) that brought together working-level representatives of MID and the Office of Naval Intelligence had a belated first meeting on 11 December, a month after it was first authorized. Once the Joint Chiefs of Staff were in place, a new JIC was formed, consisting of the heads of MID and the Office of Naval Intelligence (ONI). Membership in the committee was expanded to include representatives of the Coordinator of Information, the Department of State, and the Board of Economic Warfare. The JIC had the dual mission of providing intelligence advice to the Joint Chiefs of Staff and representing the United States in combined Military Intelligence matters with its British counterparts. The principals on the JIC were supported by a larger working group known as the Joint Intelligence Survey Committee. With the growing independence of the Army Air Forces, the AAF's principal intelligence officer, the assistant chief of air staff, intelligence (A–2), was added to the JIC in May 1943, and the subordinate body became known as the Joint Intelligence Staff.[4]

This joint structure did accomplish some useful purposes by fostering interservice cooperation. Under its supervision, a joint prisoner-of-war interrogation center was set up at Fort Hunt, Virginia, in May 1942 to process high-ranking German prisoners. A similar facility was organized at Byron Hot Springs, California, in December to handle Japanese prisoners. By the fall of 1942, Joint Army-Navy Intelligence Studies were being published, and small Joint Intelligence Collection Agencies were later fielded in North Africa, the Middle East, India-Burma, and China to acquire nontactical information of potential use to Washington. At the end of 1942 there was even a serious proposal to merge MID with ONI, creating a joint intelligence agency. However, this idea ran into too many practical difficulties, since MID performed broader functions than ONI, and the two organizations were not parallel. MID, for example, was an element of a larger staff but ONI was not, since the Navy had no such body.

The exchange of information between Army and Navy Intelligence was also hampered by tradition. Both service intelligence agencies had long been conditioned to operate independently and departmentally. Communications intelligence was particularly sensitive: until November 1944 the Navy did not share all information derived from this source with the Army, and no joint organiza-

---

[3] Ibid., p. 211.

[4] For a further discussion of AAF intelligence in World War II, the reader is referred to John F. Kreis, ed., *Piercing the Fog: Intelligence and Army Air Forces Operations in World War II* (Washington, D.C.: Air Force History and Museums Program, 1996).

tion to coordinate activities in this field was put in place until 1945.[5] The lack of secure telephone links between MID and ONI, even at the end of the war, reflected the limits on cooperation between the armed services in the intelligence field.

Although MID was willing to work with its Navy counterpart, it regarded cooperation with other players in the intelligence arena with distaste. Both military services distrusted the civilians, especially Donovan's organization. This rivalry did not abate even after the Office of the Coordinator of Information, shorn of its propaganda functions, was placed under the Joint Chiefs of Staff in July 1942, redesignated the Office of Strategic Services (OSS), and given a heavy fill of military personnel, with Donovan himself ultimately receiving general's stars. MID never allowed OSS intelligence analysts any access to high-grade communications intelligence (COMINT).[6] One of the motives behind the proposal for creating a joint intelligence agency was to strip OSS of most of its intelligence functions. Moreover, when plans began to be made for Operation TORCH, the invasion of North Africa, the Joint Intelligence Committee was carefully cut out of the picture. Instead, intelligence support to the operation was provided by a Joint Security Control group with its membership restricted to representatives from Army and Navy Intelligence. Later the Joint Chiefs of Staff used this body to coordinate deception operations.

The Reorganization of Military Intelligence

At the same time that Army Intelligence was beginning to embark on intelligence collaboration with other elements, it was also undergoing reorganization. The first change came about as a result of a wholesale shakeup of the Army staff system in March 1942. Army Chief of Staff General George C. Marshall and his top planners decided to sharply cut back the Army staff and to centralize control of operations in a War Department Operations Division, which would become a Washington command post for the chief of staff. Administrative duties previously performed at the staff level were to be delegated to new subordinate commands. The staff would become a body engaged exclusively in planning and supervision.

This change, which divided the Army into the Army Ground Forces, the Army Air Forces, and the Services of Supply (later redesignated as the Army Service Forces), had a major impact on the structure of Military Intelligence.

---

[5] Ray Cline notes that "Neither the JIC [Joint Intelligence Committee] Weekly nor any component of the OSS ever used signal intelligence in its reporting. I know from Navy experience that this source was essential for all authoritative all-source intelligence, and it was a serious limitation that OSS had only minimal exposure to intercepts." *The CIA under Reagan, Bush, and Casey*, p. 78.

[6] Army-Navy rivalry over communications intelligence was conducted almost at the level of the Cold War. At one point a senior Army Intelligence officer wrote: "It is now apparent that the Navy proposes to do business at arm's length. We should accept that attitude and act accordingly." Memo for General Bissell, sub: Army-Navy Agreement Regarding ULTRA, in *Listening to the Enemy*, ed. Ronald H. Spector (Wilmington: Scholarly Resources, 1988), p. 199.

Each of the components had its own intelligence staff. Initially, Army Ground Forces took over responsibility for combat intelligence training. The intelligence organization of the Army Air Forces (AAF) devoted itself to studying the technical and tactical aspects of the air-related threat, while the War Department G–2, in which AAF personnel were well represented, continued to have responsibility for strategic air intelligence. The Services of Supply, in addition to exercising supervision over counterintelligence operations in the United States, took over responsibility for the intelligence activities of the seven Army technical services: the Chemical Warfare Service, Corps of Engineers, Medical Corps, Ordnance Corps, Quartermaster Corps, Signal Corps, and Transportation Corps. Among other things, this meant that the Services of Supply now had jurisdiction over the Signal Intelligence Service, a step which had important adverse implications, since it placed the Army's most productive intelligence arm under a service organization with no background in intelligence and with low priorities for obtaining personnel and resources in this area.

The organization most affected, however, was the Military Intelligence Division itself. At the time the reorganization went into effect, it was by far the largest single element in the Army Staff, containing 50 percent of all officers on the staff and 60 percent of all other personnel. The March 1942 reorganization reduced the division to just 26 people, 16 of them officers. To carry out all the operating functions—collecting, analyzing, and disseminating intelligence—the new and theoretically separate Military Intelligence Service (MIS) was set up. Initially, MIS included an Administrative Group, an Intelligence Group, a Counterintelligence Group, and an Operations Group. By April 1942 the new organization already consisted of 342 officers and 1,000 enlisted men and civilians, and it continued to expand.

On paper, the separation of the Military Intelligence Division from its operating arm, the Military Intelligence Service, was a drastic change. In practice, it proved otherwise. The head of MID at the time was the rather imperious Maj. Gen. George V. Strong. Although charged with responsibility for carrying out the plan, Strong emphatically did not believe in it and effectively frustrated its implementation. He justified this bit of institutional sabotage on the grounds that he was still responsible for providing intelligence advice to the chief of staff and needed to retain command and administrative control over the assets required to accomplish his mission. As a result, until the general departed in early 1944, the separation between MID and MIS remained essentially a paper arrangement. By the end of Strong's tenure as assistant chief of staff, G–2, there were two organization charts for the Military Intelligence Service, one drawn to please the reformers on the General Staff, and the other reflecting actual command arrangements.

Although Army planners had an impact on Military Intelligence organization at the War Department level, the imperatives of the war itself were greater. At the time of Pearl Harbor, MID's production unit, the Intelligence Branch, was

internally divided into traditional geographic sections, and the organization still derived the bulk of its intelligence, apart from MAGIC, from the attache system. The involvement of the United States in actual overseas combat changed both the sources of intelligence and the information-gathering process. Intelligence production was now assigned to the Military Intelligence Service. MID's former Intelligence Branch became the Intelligence Group of the MIS and was reorganized to reflect the various theaters of war. In addition, new functional elements sprang up beside the area elements as the needs of wartime expanded the scope of MIS's interests.[7]

Perhaps the most important organizational change within the MID/MIS organization was the development of an element charged with exploiting sensitive communications intelligence. This occurred as a result of the weaknesses in handling such sources at Pearl Harbor. The restrictions on dissemination that had been placed on the MAGIC intercepts had left Army Intelligence oblivious to the Japanese threat. Immediately after the Pearl Harbor attack, Secretary of War Stimson called upon a prominent Chicago lawyer, Alfred McCormack, to examine the implications of the problem. McCormack recommended the creation of a branch within the Military Intelligence Service to deal with the processing of communications intelligence. The Special Branch was established in May 1942 with Col. Carter W. Clarke as its head and with McCormack, now commissioned as a colonel, as his deputy. To acquire the necessary high-caliber personnel to staff the new organization, McCormack drew heavily on lawyers from elite firms, who were given reserve commissions.[8]

The Special Branch was an important step in the rationalization of the Army's handling of communications intelligence. For the first time, analysts in sufficient numbers would have access to the material in ways that would allow them to exploit it properly for evaluation. MAGIC could now be viewed in its entirety and used to build up an intelligence picture. However, although the Special Branch was a step in the right direction, it was not the final answer. The rest of the Military Intelligence Service, cut off from compartmentalized intelligence, was forced to operate in a vacuum. Additionally, even though the branch received its intelligence from the Signal Intelligence Service, it did not control the operations of the SIS, which still remained under the direction of the Chief Signal Officer.

---

[7] Among the diverse elements of the Military Intelligence Service were MIS–Y, which ran an interrogation center for high-level German officers, and MIS–X, which was involved in making arrangements for procuring intelligence from captured Army Air Forces flight crews, as well as for implementing escape and evasion measures. Both organizations operated from a secret headquarters at Fort Hunt, Virginia. See Lloyd R. Shoemaker, *The Escape Factory* (New York: St. Martin's Press, 1990). Maj. Gen. Otto L. Nelson later commented, "Organizationally, G–2 was a mongrel, with many uncertain strains mixed in and not always recognizable." *National Security and the General Staff* (Washington, D.C.: Infantry Journal Press, 1946), p. 526.

[8] A detailed history of the organization is contained in "History of the Special Branch, MIS, War Department, 1942–1944," *Listening to the Enemy*, pp. 171–94.

The Special Branch was not the only organizational innovation introduced into the MIS. The Military Intelligence Service had inherited from MID small branches located in New York City, San Francisco, and New Orleans. In April 1942 a new branch was established in Miami, Florida, to counter the threat of Axis penetration and subversion in Latin America. In August the entire Latin American Section of the Military Intelligence Service moved to Miami. Successively redesignated the American Hemisphere Intelligence Command, the American Intelligence Command, and the American Intelligence Service, the unit became what one historian described as a "huge, semi-independent military intelligence agency."[9] It engaged in both counterintelligence activities and positive collection, controlling subordinate field offices in the Canal Zone and in Brazil, and operating its own intercept system to locate possible agent transmitters throughout Latin America. Additionally, MIS expanded its overseas operations further, setting up a small secret intelligence service in 1942 and a Military Intelligence Research Section, with offices in London and Washington, D.C., for exploitation of captured documents in January 1943.[10]

The Military Intelligence Division also ventured into areas rather far afield from pure intelligence work. For a brief time, one was psychological warfare. The Special Studies Group that had previously dealt with the subject became the Psychological Warfare Branch of MID shortly after the declaration of war. However, one year later the Joint Chiefs of Staff assigned the Office of Strategic Services responsibility for conducting all activities in this field, and the Army's Psychological Warfare Branch was discontinued. Nevertheless, MID eventually reassumed responsibility for the Army's remaining efforts in this area, setting up the Propaganda Branch in 1943. In a move that took the Military Intelligence Division even further afield from purely intelligence-related concerns, in April 1943 the organization was given responsibility for conducting the Army's World War II historical program.[11]

A function more pertinent to intelligence was that of training intelligence personnel. The Army had decided rather belatedly that intelligence training was an intelligence responsibility. The Army Air Forces had led the way in this area, opening up an AAF Intelligence School for their own personnel in February 1942. Classes were held at the University of Maryland until April, when the Army Air Forces acquired a more permanent facility at Harrisburg, Pennsylvania. In June 1942 the Military Intelligence Service activated its own

---

9 Bruce W. Bidwell, History of the Military Intelligence Division, Department of the Army, vol. 5, unpublished Ms, U.S. Army Center of Military History, 1963, pp. 52–53.

10 On the War Department's World War II secret intelligence service, see *National Security Act of 1947: Hearing Before the Committee on Expenditures in the Executive Departments*, 80th Cong., 1st sess. (Washington, D.C.: Government Printing Office, 1982), pp. 7–8, 53–54. Further references to this organization can be found in the footnotes to Christopher Felix (pseud.), *A Short Course in the Secret War* (New York: Dell Publishing, 1988), pp. 168–69.

11 Stetson Conn, *Historical Work in the United States Army, 1862–1954* (Washington, D.C., U.S. Army Center of Military History, 1980), pp. 83–114.

Military Intelligence Training Center (MITC) at Camp Ritchie, Maryland, a former National Guard installation.

The Camp Ritchie center trained order of battle specialists, photo interpreters, some linguists, and general intelligence personnel. After August 1944 the center also offered counterintelligence training. Intelligence personnel proceeded from Camp Ritchie to a staging area at Camp Sharpe, Pennsylvania, where they received additional combat training, were formed into teams, and assigned directly to theater control. Over 19,000 students passed though Camp Ritchie's gates during the course of World War II. The training offered at Ritchie may not have been perfect—officers in the European theater would later complain that members of their military intelligence specialist teams showed "a lack of basic military training and a certain ineptness about caring for themselves"—but it was a more extensive effort than the Army had ever before undertaken in this arena.[12]

To meet the special needs of the Army in the Pacific, the Military Intelligence Service also took over the direction of a separate school for Japanese linguists, with a student body composed primarily of second generation Japanese Americans known as Nisei. This school had been established originally at the Presidio of San Francisco, under Fourth Army control in the days before Pearl Harbor. In May 1942 it became the Military Intelligence Service Language School, moved to Camp Savage, Minnesota, and was greatly expanded. To acquire better facilities, the school moved once more to Fort Snelling, Minnesota, in August 1944. By the end of the war, it had graduated over 4,800 Japanese-language specialists, most of whom served in the Pacific theater as members of interpreter-interrogator-translator teams.[13] The Army also sponsored instruction for smaller numbers of Japanese, Chinese, and Russian linguists at selected universities, and the MIS itself trained 1,750 Army censorship personnel at Fort Washington, Maryland, until February 1944, when the Army Service Forces assumed the function. Army counterintelligence personnel assigned to MIS had their own separate school in Chicago until 1944.

Not all intelligence training was directly under the auspices of the Military Intelligence Service. The Signal Security Agency (SSA), SIS's wartime successor, provided cryptologic and language training for military and civilian personnel at Arlington Hall Station, Virginia, and maintained a school for officers and enlisted personnel at Vint Hill Farms Station, Virginia. Intelligence personnel for the Army Air Forces continued to attend the AAF facility in Harrisburg, Pennsylvania, until this school was relocated to Orlando, Florida, in the spring

---

12 Rpt of the General Board, U.S. Forces, European Theater, Study no. 12, The Military Intelligence Service in the European Theater of Operations, p. 8, copy in CMH files.

13 An account of Nisei accomplishments in intelligence is provided by Joseph D. Harrington, *Yankee Samurai: The Secret Role of Nisei in America's Pacific Victory* (Detroit: Pettigrew Enterprises, 1979). For a firsthand account of one individual's experience, see Interv, author with Mr. Harry Fukuhara, pt. 1, 5 Jun 90, INSCOM History Office files.

of 1944. Finally, the responsibilities for training soldiers assigned to tactical signals intelligence units were peculiarly fragmented. Units were organized and trained both by the Army Ground Forces and the Army Air Forces, while advanced training was administered under SSA supervision at its own facilities and at Signal Corps installations at Fort Monmouth, New Jersey, and Camp Crowder, Missouri.[14]

The ULTRA Breakthrough

Events of the spring of 1943 would reshape the entire structure of Military Intelligence. In April Army cryptanalysts scored their first success against Japanese military codes. A month later, a party of officers from MIS and from the Signal Security Agency visited the British Government Code and Cypher School at Bletchley Park. For the first time, American Military Intelligence became aware of the dimensions of the British success against high-level German communications. British efforts in breaking the German Enigma and other ciphers used on command links had laid bare many of the most important secrets of the Nazi high command. The intelligence derived from this source, known as ULTRA, was disseminated by the British under rigidly controlled conditions. Although such intelligence had been provided to Eisenhower during the invasion of North Africa, U.S. Army Intelligence had not been fully aware of its origins. Now the British agreed to share this intelligence with the U.S. Army on an unrestricted basis, in exchange for reciprocal access to American communications intelligence on the Japanese.

These twin developments confronted Army Intelligence for the first time with the problem of disseminating communications intelligence to the field. The previous American success against the Purple machine, although providing valuable background information to Washington during the course of the war, had not had tactical implications. In contrast, ULTRA could be of immediate operational value. The problem was now to transmit this extremely sensitive combat intelligence from central processing centers in the United States and Great Britain to theater commanders thousands of miles away in a fashion that would avoid any compromise of the source of intelligence.

In response, the Special Branch adopted the existing British system of handling communications intelligence. New security classifications were introduced. At first, high-level communications intelligence was termed ULTRA DEXTER, lower-level material designated DEXTER. Later, ULTRA was reserved for the results of high-level cryptanalysis, while intelligence derived from breaking simpler systems was

---

[14] These intercept units, an officer of the Signal Security Agency commented, were "organized and trained by the ground forces in a rather 'hit-or-miss' manner without any particular reference to their ultimate employment." SRH 169, Centralized Control of U.S. Army Signal Intelligence Activities, p. 14.

termed CIRO PEARL or PEARL, and information produced from radio-direction finding was labeled THUMB. Ultimately, in order to mesh Army and Navy practice, PEARL and THUMB were merged into a single category, PINUP. Meanwhile, in April 1944 the U.S. Army at last adopted a "top secret" classification to provide a satisfactory equivalent to the British "most secret."

Terminology was only one aspect of the new procedures. The actual dissemination of ULTRA in the field was handled by special security officers (SSOs) selected and trained by the MIS Special Branch and operating under its direct command using special cipher systems. This was both faster and more secure than the usual practice of sending intelligence through successive layers of command channels. Again, this followed British practice. The first three American SSOs went out to commands in the Pacific in the fall of 1943. The British agreement that ULTRA supplied to American commanders in the European theater would henceforth be disseminated through American channels led to the procurement of eighty additional special security officers in December 1943.

At first, the SSOs were attached only to the highest level of commands. They had the dual mission of securing the vital ULTRA material and of explaining its significance to commanders and intelligence officers unfamiliar with the uses and limitations of high-grade communications intelligence. However, by July 1944 the decision had been made to disseminate ULTRA directly to field armies and equivalent AAF commands and even down to independently operating Army corps. This necessitated recruiting 172 more SSOs in August 1944. In addition, 65 enlisted men were brought into the system to operate communications, thus relieving SSOs from the necessity of deciphering their own messages. By the end of the war, the elaborate dissemination system was headed in each theater by a senior special security representative.[15]

The Army's own increasing successes in communications intelligence, combined with the new availability of the British COMINT product, helped bring about a general reorganization of the Military Intelligence Service. Because of the growth of its responsibilities, the Special Branch expanded to the point where it constituted the largest component of the MIS Intelligence Group. This created a situation in which much of the analysis performed at the War Department level was undertaken by individuals without access to the single most important intelligence source exploited in the war. Only a "very select few" top production officials had been granted access to the whole picture.[16]

General Strong's departure in February 1944 paved the way for an institutional readjustment. In April a committee headed by Assistant Secretary of War

---

[15] See "History of the Operations of Special Security Officers Attached to Field Commands, 1943–1945," *Listening to the Enemy*, pp. 199–204.

[16] Bidwell, History of the Military Intelligence Division, vol. 5, p. 221. Bidwell's treatment of the full implications of the reorganization is necessarily unsatisfactory, since he wrote before the ULTRA secret—and the exact duties of Special Branch—had been decompartmented and released.

John J. McCloy recommended that "extreme compartmentation" be eliminated.[17] As a result, the War Department completely reorganized its Military Intelligence organization. The Special Branch was abolished as a totally separate compartmented entity, although a new Special Branch was formed to handle dissemination of ULTRA to the field. A Military Intelligence Service separate from MID was reestablished and its internal structure realigned, with the organization ultimately reaching a peak worldwide strength of 1,500 officers, 2,000 enlisted men, and 1,100 civilians in October 1944.

The timing of the reorganization, however, demonstrated all too clearly that the nation's strategic decision makers still looked upon Army Intelligence as "a kind of reference service for data rather than for professional judgments."[18] The new arrangements went into effect in early June 1944. As distinguished historian and intelligence analyst Ray Cline later described the situation, the "G–2 [staff] was so little geared into high-level strategic decisions that it was engaged in a colossal struggle for office space when D-Day for the Normandy invasion came along: all of G–2's files were locked up sitting in safes in the halls waiting for moving crews when frantic requests for data on the landing zone situations began to descend on the hapless Army intelligence officers, who hardly knew each others' phone numbers, let alone what was in the files."[19]

The new-model Military Intelligence Service differed substantially from its predecessor. Internally, it was organized into three directorates: Administration; Intelligence; and Information, which supervised collection and dissemination. It now functioned independently of MID and was freed from some of the excessive compartmentation that had hobbled previous operations. Moreover, at last it could concentrate almost exclusively on the production of foreign intelligence. As a result of decisions made earlier in 1944, responsibility for counterintelligence and censorship had been allotted to the Army Service Forces, a move which rather explicitly downgraded the importance of these functions in the Army, and the MIS Counterintelligence Group that had previously exercised staff supervision over this area was thus abolished.

In addition, certain activities previously carried out at dispersed locations in the United States were now centralized in Washington, D.C. The American Intelligence Service operating from Miami, Florida, had been terminated in January 1944. Now that the war had been carried to the shores of Europe, America was no longer worried about Axis subversion in Latin America. Similarly, the branches previously established in San Francisco, New Orleans, and New York City had lost most of their usefulness as the war progressed and other sources of intelligence became available. By June 1944 the first two

---

17 Ibid., p. 19.
18 Cline, *The CIA under Reagan, Bush, and Casey*, p. 81.
19 Ibid., p. 111.
20 Nelson, *National Security and the General Staff*, p. 526.

of these branches had been shut down, and the New York branch would cease operations that December. However, it should be noted that the Corps of Engineers, which had its own intelligence office in New York City, continued to find the data bases available there to be essential in producing strategic Engineer Intelligence.

Unfortunately, while the new MIS was a changed organization, not everyone agreed that the changes had been for the better. The new Intelligence Directorate at the heart of MIS was organized on lines that soon proved to be confusing, with a layer of geographic "specialists" superimposed upon branches organized along functional lines.[20] It seems to have been envisaged that the specialists, who had no operating responsibilities, would act as a group of "wise men," producing a unified intelligence picture from the myriad details coming from the functional operating echelons. However, the geographical specialists questioned how they could produce cohesive results without controlling any assets, and the chief of the Military Intelligence Service felt they should be on MID's organization chart, not his own. In practice, functional areas of responsibility proved to be overlapping, the new arrangements separated the researchers from the report writers, and MIS found itself organized on different lines from any other intelligence organization with which it dealt.

Two months after the new reforms had been implemented, the chief of the MIS declared the new system "slow and cumbersome."[21] Col. Alfred McCormack, now director of Intelligence, was equally unhappy: the Special Branch he had painstakingly assembled was now dispersed throughout "53 separate branches, sections, and subsections," and he felt MIS was now under "about as impracticable a scheme of organization as could be devised."[22] Additional tinkering with the system went on until the close of the war, but a postwar study of intelligence organization at the General Staff level concluded that from the point of view of producing timely intelligence, the 1944 reorganization was "a total failure."[23]

Whatever its continuing internal weaknesses, MIS took a major institutional step forward. Since 1943 communications intelligence, MIS's main source of intelligence, had been under the control of the chief signal officer or of theater commanders.[24] In December 1944 MIS at last secured operational control over the Signal Security Agency, and was able to give direction to the Army's most important COMINT asset. This step also positioned MIS to take over this whole field of intelligence when the war came to a close.

---

[21] Bidwell, History of the Military Intelligence Division, vol. 5, p. 20.
[22] SRH 185, War Experiences of Alfred McCormack, pp. 29–30.
[23] Bidwell, History of the Military Intelligence Division, vol. 5, p. 21.
[24] SRH 141, Papers from the Personal Files of Alfred McCormack, pt. 2, pp. 316–17.

The Counter Intelligence Corps

The Military Intelligence Service was not composed solely of collectors and analysts. For most of World War II, it also included personnel of the Army Counter Intelligence Corps (CIC), formed on 1 January 1942 as the successor to the Corps of Intelligence Police. The new organization had both a more appropriate name and initially a more centralized organization than its predecessor. In January the War Department took over control of all background investigations of prospective counterintelligence agents and in April centralized the issue of credentials. The CIC would be an elite force, picking its enlisted personnel from the cream of Selective Service inductees. As Maj. Gen. George V. Strong, the assistant chief of staff, G–2, put it, "the personnel of this Corps is of officer caliber."[25]

The question of overall control was not resolved finally, however. The service commands, as the corps areas were redesignated in March 1942, were the primary users of CIC agents in the first part of the war, and local commanders naturally wanted the convenience and flexibility of procuring their own counterintelligence personnel. For example, the commanding general of the New York Port of Embarkation began to recruit his own agents for the Transportation Corps in March 1942 and, although these individuals were issued Military Intelligence Division credentials, it was not until early 1943 that part of the contingent was assimilated into the Counter Intelligence Corps.

The scope of the CIC's responsibilities was vastly increased in March 1942, when the Army expanded its existing countersubversive program and gave it new guidelines, modeling it after the similar Army program of World War I. The new countersubversive operation latticed the nation's military establishment with "an elaborate and fine network of secret agents."[26] Intelligence officers secretly recruited informants within each unit, on an average ratio of one informant to every thirty men, resulting in a program of enormous proportions. By the summer of 1943 there were 53,000 operatives in just one of the nine service commands in the continental United States and over 150,000 such reports were being filed monthly once the system became fully operational. Although the countersubversive program was administered by unit and installation commanders, not by the Counter Intelligence Corps, CIC agents were assigned to follow up reports of subversive activity. At the War Department level, the process was monitored and coordinated by the Counterintelligence Group of the Military Intelligence Service, which exiled those suspected of sedition to special holding units in the remoter parts of the country.

Inevitably, the new work load led to the expansion and restructuring of the Counter Intelligence Corps. Expansion itself generated an additional work load,

---

[25] U.S. Army Intelligence Center, History of the Counter Intelligence Corps, vol. 5, unpublished Ms, 1960, p. 39.

[26] Ibid., p. 127.

since the official CIC history later estimated that the Counter Intelligence Corps in the continental United States allotted half its man-hours to investigate its own applicants. By July 1943 the Corps was authorized a strength of 543 officers and 4,431 enlisted personnel. Officers previously detailed to the organization were now formally transferred and additional officers allotted from officer candidate schools. In the past, all CIC enlisted men had held the rank of sergeant; now corporals and privates were added to the corps. This permitted functional differentiation. Sergeants served as special agents with full investigative powers, and corporals and privates held subordinate positions as agents and counterintelligence clerks. The new arrangements allowed some relaxation in the Counter Intelligence Corps' appointment standards. For a period in late 1942 and early 1943, service commands once more were allowed to procure and transfer agents and clerks, while Washington retained full control over special agents and officers. In line with the renewed authority given to the field, the Counter Intelligence Corps School in Chicago, previously responsible for training all CIC personnel, now confined its activities to providing advanced courses, allowing the service commands to provide introductory counterintelligence training.

Meanwhile, the Counter Intelligence Corps was forced to relocate its headquarters. At the end of 1942 the War Department, concerned that too many fit young officers were serving in staff assignments in Washington, stipulated that no more than one-third of the officers assigned to any element in Washington, D.C., could be below thirty-five years of age. This "Child Labor Law" literally drove the CIC out of town. In January 1943 the chief of the Counter Intelligence Corps and his staff moved to a dormitory of Goucher College, a fashionable girls' school in Baltimore, Maryland, that had been taken over by the government for the duration of the war.

While these developments were taking place, the Counter Intelligence Corps was beginning to find a new role with the fighting forces. Heretofore, almost all its duties had been concerned with security in the service commands or in base areas overseas. Special agents in civilian clothes had operated from offices, essentially working in much the same fashion as their civilian counterparts in the FBI. In some cases, CIC agents had been recruited and assigned without completing basic military training. However, when plans were drawn up for the American invasion of North Africa in the fall of 1942, it was decided that CIC personnel would be attached to tactical units in the field. The initial CIC experience with field service was not completely happy. The commander of the training camp to which the first group was assigned labeled them "a citizen army of misfits."[27] Nevertheless, the CIC personnel attached to the North African task force ultimately demonstrated their value in a tactical support role.[28]

---

[27] U.S. Army Intelligence Center, History of the Counter Intelligence Corps, vol. II, unpublished Ms, 1960, p. 8.

[28] Powe and Wilson, *The Evolution of Military Intelligence*, p. 53.

Tactical employment gave the Counter Intelligence Corps a whole new raison d'etre. By the middle of 1943 the Army at last began to deploy a sizable portion of its strength overseas. The CIC was affected by this shift. With deployment of tactical CIC detachments to combat situations imminent, the CIC School in Chicago put its students in uniform and placed a new emphasis on counterintelligence operations under battle conditions. The same concern for making counterintelligence personnel ready for combat led to the creation of a Counter Intelligence Corps Staging Area in the summer of 1943 to better prepare units about to go overseas. The staging area, initially located at Logan Field in Baltimore, Maryland, soon moved to nearby Camp Holabird, beginning a long association between Military Intelligence and what would become known as "The Bird."

By the fall of 1943 the Counter Intelligence Corps appeared to have solved its initial problems and to have become an established part of the Army. Its organization manual finally had been approved, and the new tactical emphasis placed it in step with the rest of the Army. Agents increasingly served in uniform with the troops rather than working as anonymous "spooks" on the fringes of the military establishment. Finally, the War Department transferred control of CIC personnel from the Military Intelligence Service to the using agencies, again bringing the Counter Intelligence Corps into conformity with the rest of the military establishment.

However, the activities of the Counter Intelligence Corps still managed to generate criticism from both within and outside the Army, placing the corps in a bureaucratically vulnerable position. From the viewpoint of the wartime military, the CIC absorbed a disproportionate percentage of high-quality personnel and used them to accomplish what many regarded as a marginal mission. Tradition-minded Army officers disliked the whole business of counterintelligence operations, especially when they involved enlisted personnel investigating officers. The CIC's investigations of leftist individuals and groups were not universally popular with politicians, particularly since the War Department's Counterintelligence Group had used the results to exclude some well-connected young men from Officers' Candidate School. Moreover, some investigations were conducted with more zeal than prudence. In early 1943, for example, the White House discovered that CIC agents had installed listening devices in the hotel suite of the president's wife in an attempt to monitor the activities of individuals suspected of Communist leanings.[29]

Accumulated resentments eventually found official expression, leading to the temporary eclipse of the Counter Intelligence Corps. In July 1943 Lt. Gen. James J. McNarney, the Army deputy chief of staff, directed the Army inspector general to launch an investigation of the CIC. On 5 November 1943, all CIC agents were ordered out of Washington, D.C., and a day later the inspector gen-

---

[29] Joseph P. Lash, *Love, Eleanor: Eleanor Roosevelt and Her Friends* (Garden City, N.Y.: Doubleday and Co., Inc., 1982), p. 492.

eral submitted a devastating critique of the corps' operations and organization. Charging that many CIC investigations were "superficial, and unproductive of positive results except in rare instances," the inspector general found that the only thorough investigations were those made of applicants for CIC or of military and civilian personnel suspected of subversion. However, these categories were overly thorough, since they dragged on after all immediate allegations had been resolved. Moreover, when officers were investigated, CIC procedures resulted in the indiscriminate dissemination of reports containing unverified derogatory information "based on hearsay, gossip, and innuendo," all of which was "directly contrary to the inherent right of a commissioned officer of the U.S. Army to be advised of imputations and allegations as to his character." In any case, the countersubversive program that had generated much of the work load was nearly worthless, since the million reports submitted in the first part of 1943 had identified only 600 suspects, and it was possible that many reports had been made on the same individual.[30]

The inspector general's report equally criticized the organizational concepts that underpinned Counter Intelligence Corps operations in the continental United States. In the security field, he found, the activities of the Counter Intelligence Corps at least partially duplicated what was being done by the investigators assigned to the Provost Marshal General's Office. In addition, the existing counterintelligence system undermined the concept of command responsibility, since the G–2s in the service commands had to answer both to their commanding generals and to the Counterintelligence Group of the Military Intelligence Service.

The inspector general's report led to the immediate unraveling of the Counter Intelligence Corps. The countersubversive program was terminated, and most CIC agents in the continental United States were merged with the criminal investigators of the Provost Marshal's Office to form a new Security Intelligence Corps that operated under the control of the service commands. Although CIC detachments continued to serve with the Army Air Forces, the Manhattan Project, and tactical units, the presence of the Counter Intelligence Corps on the home front was effectively eliminated. The CIC School was transferred to the provost marshal general, its staging area closed, and the position of chief, Counter Intelligence Corps, abolished. The outgoing chief, Col. Harold R. Kibler, blamed the fall of his command on the enmity of the White House, specifically "Harry Hopkins and the Secret Service."[31] A little later the Counterintelligence Group of the Military Intelligence Service was also eliminated. For the moment, the Army had decided to practically abandon the field of domestic counterintelligence, limiting the CIC to a tactical support role overseas.

---

[30] History of the Counter Intelligence Corps, vol. 5, app. 2.

[31] FBI memo quoted in Lash, *Love, Eleanor*, p. 492. A more melodramatic but less accurate version of the imbroglio can be found in Richard G. Powers, *Secrecy and Power: The Life of J. Edgar Hoover* (New York: Free Press, 1987), pp. 265–66. "Supposedly, the President had been so furi-

This role, however, proved substantial. CIC detachments rolled up nets of enemy agents in Italy, landed in Normandy with the first wave of paratroopers, screened civilians in France, and arrested Nazi officials as U.S. forces overran Germany. In the Pacific, Counter Intelligence Corps units secured enemy documents on the remote islands of Micronesia and worked with local guerrillas rounding up collaborators in the Philippines. To be sure, some distrust of CIC continued throughout the war. Writing in 1946, two experienced Army intelligence officers noted that "the Counterintelligence [*sic*] Corps (CIC) in World War II was in many ways a peculiar organization, whose personnel (chosen hurriedly and under pressure for their educational rather than military qualifications) frequently got in everybody's hair."[32] However, counterintelligence support was essential for American units operating in the midst of an alien population, and 241 CIC detachments would serve in overseas theaters during the course of World War II.

In turn, success overseas revitalized the CIC at home. By the summer of 1945 it was clear that the evisceration of the Counter Intelligence Corps had deprived the Army counterintelligence function of essential institutional support just as needs were increasing. The Army's role in the occupation of a defeated Germany had placed new demands on the depleted CIC detachments in the European theater, and the pending expansion of military operations in the Pacific to the Japanese mainland threatened to pose even greater potential counterintelligence problems. But the Army now lacked any effective mechanism either to procure new counterintelligence specialists or to redeploy those it already had. Although the Military Intelligence Training Center at Camp Ritchie had begun training counterintelligence personnel in August 1944, the Camp Ritchie program stressed combat intelligence rather than counterintelligence. Moreover, there was no rotation base for the Army's counterintelligence personnel, since any members of the Counter Intelligence Corps shipped back to the United States were reassigned as individuals to the Army general replacement pool and were lost to their specialty.

These considerations led to the reestablishment of the Counter Intelligence Corps in the continental United States. In July 1945 the Office of Chief, Counter Intelligence Corps, was restored, a new CIC Center and School organized, and both elements placed under the control of the Intelligence Division of the Army Service Forces. Originally located at Fort Meade, the school soon moved to Camp Holabird. In August the Security Intelligence Corps was released from the control of the provost marshal and reassigned to the Intelligence Division, paving the way for its eventual merger into the CIC.

---

ous he had disbanded CIC and ordered its members sent to the South Pacific to 'fight Japs until they were killed.'"

32 Stedman Chandler and Robert W. Robb, *Front-Line Intelligence* (Washington, D.C.: U.S. Marine Corps, 1986), p. 113.

The Signal Security Agency

The development and expansion of the Army signals intelligence and communications security organization was governed by dynamics quite different from those affecting the structure of Army counterintelligence. Although the growth of the Counter Intelligence Corps was a function of the expansion of the countersubversive program and the need to create new units to give tactical support in the field, the Signal Intelligence Service and its successor organizations evolved largely as a result of increasing success in accomplishing the cryptanalytic mission.

The United States' entry into World War II naturally imposed new demands on the Army's Signal Intelligence Service. Up to this point, the SIS had achieved its main successes against intercepted diplomatic communications provided by its 2d Signal Service Company, which manned seven small fixed sites located at Fort Hancock, New Jersey; Fort Hunt, Virginia; Fort Sam Houston, Texas; the Presidio of San Francisco, California; Corozal, Canal Zone; Fort Shafter, Hawaii; and Fort McKinley, Philippine Islands. At the time of the attack on Pearl Harbor, the Signal Intelligence Service had a strength of 331, almost equally divided between the field sites and its headquarters in the old Munitions Building, a World War I–vintage structure in downtown Washington, D.C.

The shift from peace to war transformed the nature of the Signal Intelligence Service, for it now had to provide military as well as diplomatic intelligence. Initially, the organization concentrated on deciphering Japanese Army cryptosystems, since the Japanese posed the immediate military threat to U.S. forces. To do this, the SIS analysts had to master the elaborate and intricate system of Japanese military codes, which worked on cryptologic principles completely different from those used in the Purple machine of the Japanese Foreign Office. This required not only the expansion of the SIS headquarters, but also the reconfiguration of its intercept network, especially since its most advanced outpost, Fort McKinley, would soon be overrun.[33]

In March 1942 the Military Intelligence Division recommended to the chief signal officer that the SIS move from the Munitions Building into new quarters with greater security. MID also recommended that the Signal Intelligence Service establish two new primary monitoring stations, one on each coast of the United States. Under wartime conditions, these suggestions met a quick response. In June 1942 the Army took possession of Arlington Hall, a former girls' school in Arlington, Virginia, and transformed it into SIS headquarters. That same month, personnel of the 2d Signal Service Battalion, as the 2d Signal

---

[33] The fate of the SIS intercept post at Fort McKinley and of its survivors is detailed in "Reminiscences of Lieutenant Colonel Howard W. Brown," *Listening to the Enemy*, pp. 43–76, and in Michael Maslak, "Signalman's Odyssey," *Military Intelligence: Its Heroes and Legends*, pp. 133–61.

Service Company was now designated, began operations at Vint Hill Farms in Warrenton, Virginia, which had been selected as the site for Monitoring Station No. 1. A second major field station was soon organized at Two Rock Ranch near Petaluma, California.

Paradoxically, as the duties of the Signal Intelligence Service became more important, its relative organizational position within the Signal Corps began to sink steadily lower as the structure of the Signal Corps itself grew more elaborate. By July 1942 the SIS was separated from the Office of the Chief Signal Officer by four organizational layers. As a result the organization was realigned, and since the term "signal intelligence" was thought to be too revealing, it was also redesignated as part of this process, becoming the Signal Security Service in 1942 and the Signal Security Agency (SSA) in 1943. Meanwhile, the positions of chief, Signal Security Service, and commander, 2d Signal Service Battalion, had been merged in 1942, effectively converting the battalion into a personnel center for the enlisted ranks at Arlington Hall and for both officer and enlisted personnel in subordinate detachments manning intercept stations worldwide.[34]

During the first part of the war, the performance of the Army's signals intelligence organization was somewhat disappointing. In July 1942 it received responsibility for all intercept of diplomatic communications, a mission previously shared with the Navy, thus becoming the sole producer of MAGIC. However, despite its continuing successes in the diplomatic field, it found its main task—coping with the mysteries of Japanese military communications—intractable. No cryptologic continuity on Japanese military communications had been built up before Pearl Harbor, principally because of the impossibility of intercepting the existing Japanese military nets either in the home islands or on the mainland of East Asia. It was not until April 1943 that an initial entry was made into one of the principal Japanese Army systems, and General MacArthur's own cryptologic center in Australia made the discovery simultaneously. Even so, Arlington Hall was not able to read enough of the code to produce any intelligence until June of that year.

The summer of 1943, however, proved to be something of a watershed for the Signal Security Agency. Once cryptanalysis of Japanese messages proved to be possible, SSA expanded enormously, recruiting a largely civilian work force. There were 395 persons at agency headquarters at the beginning of 1943 and 3,455 by the end of the year. Although two large temporary buildings had been hastily constructed at Arlington Hall in the winter of 1942 to provide additional office space for this work force, the influx of new personnel still made for cramped quarters. However, in 1943 the War Department gave the British primary operational responsibilities for code breaking in Europe, which freed the SSA to concentrate most of its energies on the Japanese military problem.

---

[34] A conscientious, if pedestrian, account of the unit can be found in SRH 135, History of the 2d Signal Service Battalion.

The year 1944 saw the full maturation of SSA's activities. In January Australian forces captured the codes of the Japanese 20th Division at Sio on New Guinea. The find led to full exploitation of Japanese military communications and triggered another period of growth. By June 1944 over 5,100 civilians, most of them female, were working at Arlington Hall, assisted by 2,000 more military personnel. In the spring of 1944 the intercept facilities of SSA's 2d Signal Service Battalion were also extended when new fixed stations were established at New Delhi, India; Asmara, Eritrea; Fairbanks and Amchitka, Alaska; and Fort Shafter, Hawaii. In the fall the steady advance of American forces in the Pacific allowed another fixed site to be established on the island of Guam. Additionally, the 2d Signal Service Battalion assumed control over former Office of Strategic Services "listening posts" at Bellmore, New York, and Resada, California, converting them into security monitoring stations.[35]

Arlington Hall thus became the center of an enormous web of collection activity. Intercept was provided not only by the fixed stations of the 2d Signal Service Battalion, but also by Signal Corps tactical units under theater control in the field. By the end of the war, 26,000 American soldiers were involved, one way or another, with the intercept and processing of signals intelligence. In addition, U.S. Army collection efforts were supplemented by material forwarded to Arlington Hall by MacArthur's multinational center and by British, Canadian, and Indian sources. To process the material, which came by courier pouch and through forty-six teletype lines at Arlington Hall, the Signal Security Agency's military and civilian work force of 7,000 was supported by a battery of 400 IBM punch-card machines.

All this was conducted under the tightest secrecy, which would be maintained for thirty years. The stringent security measures that cloaked the Army's signals intelligence organization, however, denied it the credit and stature it deserved. That the positions of chief of the Signal Security Agency and commander of the 2d Signal Service Battalion continued to be combined under one colonel throughout most of World War II indicates something of the nature of the problem. Col. Preston W. Corderman, who had commanded the agency since 1943, finally received a brigadier general's star in June 1945.[36]

The assumption of operational control over the Signal Security Agency by MIS in December 1944 made sense for both organizations. By this time, the agency had become the Army's most significant producer of high-grade intelligence. The Military Intelligence Service now had control of targeting and could rearrange operational priorities. In addition, the change benefited the Signal Security Agency. As long as the agency had been simply a part of the Signal

---

[35] The OSS had originally used these stations to monitor Axis propaganda and news broadcasts.

[36] A short account of the SSA's code-breaking activities in World War II can be found in SRH 349, Achievements of the Signal Security Agency in World War II, pp. 1–38.

Corps, its request for increased personnel allotments had to pass through the chief signal officer and the general commanding the Army Service Forces, neither of whom were indoctrinated for communications intelligence or knew the true importance of the agency's mission. Col. Alfred McCormack of MIS's Special Branch believed that this factor had delayed the breaking of Japanese codes by a year.[37] The new arrangement ended this anomaly. Although the chief signal officer still retained administrative control of the SSA, the action was a significant first step toward the postwar integration of all Army communications intelligence under G–2 control.

A second step soon followed, precipitated by the growing, if belated, collaboration between the Army and the Navy in the communications intelligence field. At one point the Army had maintained closer COMINT working relationships with the British than with the U.S. Navy. In February 1945 Admiral Ernest King, Commander in Chief, United States Fleet, and Chief of Naval Operations, agreed with Army Chief of Staff General George Marshall to create the Army-Navy Communications Intelligence Board (ANCIB) to direct a joint effort in this field. The board would report directly to the two service chiefs, not to the Joint Chiefs of Staff, and would use as its staff support the existing Army-Navy Communications Intelligence Coordinating Committee (ANCICC), a working-level group set up on an informal basis in early 1944 by the Signal Security Agency and its Navy opposite number, OP–20–G. However, the new head of the Military Intelligence Division, Maj. Gen. Clayton Bissell, vetoed the idea on the grounds that "the Army cannot participate on an inter-service project of this sort as long as its own signal intelligence efforts remain as decentralized as they now are."[38] The Navy, Bissell claimed, had a monolithic communications intelligence organization, while MID controlled only the Signal Security Agency.

Bissell's bureaucratic ploy spurred the deputy chief of staff and the all-powerful Operations Division into relooking at the entire structure of Army signals intelligence. In May 1945 the War Department requested that the three senior Army commanders engaged in the war against Japan—Lt. Gen. Albert J. Wedemeyer, commanding general of the China Theater, Lt. Gen. Daniel I. Sultan, commanding general of the Burma-India Theater, and General of the Army Douglas MacArthur, commanding general of Army Forces, Pacific—submit their views regarding the desirability of unifying the whole Army communications intelligence effort under a single War Department agency. Only MacArthur opposed the idea, and even he agreed that he had no objections once the fighting had stopped. The stage thus had been set for a postwar reorganization of signals intelligence.

---

[37] SRH 141, pt. 2, pp. 221–22.

[38] Memo, Maj Gen Clayton Bissell for Deputy Chief of Staff, 2 Mar 45, sub: Army Navy Communications Intelligence Board—Establishment of, Army Cryptologic Records.

Communications Security

The Signal Security Agency was shield as well as sword in World War II, since the agency had the duty of protecting Army communications in addition to exploiting those of other nations. Here, the agency's performance was smoother since much spade work had been done before Pearl Harbor. Army communications security had already been enhanced by the development of various kinds of cipher machines. The problem of distribution was overcome successfully. By mid-1942 the Army had replaced its older M134s and M134As with the M134C, more commonly known by its short title, SIGABA. Issued down to division level, the SIGABA served as the backbone of the Army's secure high-level communications throughout the war. The handy little M209, designed for use at lower command echelons, was in the hands of American troops before the first American landings in North Africa in November 1942.

Technological advances in this area continued throughout the war, expedited by the streamlining of the developmental process. Until early 1942 responsibilities in the area of communications security had been fragmented. The Signal Intelligence Service had worked out the cryptologic principles for the cipher devices, the Signal Corps Laboratories had prepared the engineering plans, and private firms had done the actual manufacturing. Wartime needs for greater security and compartmentation made this arrangement obsolete, and the Signal Security Agency was assigned all developmental work, introducing numerous innovations in the process. New crypto-communications devices produced by the Signal Security Agency allowed direct on-line encryption of teletype messages as well as speech. By June 1943 the agency had developed a secure telephone apparatus used for transatlantic conversations between Roosevelt and Churchill and later employed to link theater commanders with Washington. The SIGSALY, as it was called, afforded high security, although with the device weighing ninety tons, its use was obviously confined to major headquarters. Smaller voice "scrambler" devices offering less security were made available to lower echelons of command.

In addition to producing and distributing various types of cipher machines, the Signal Security Agency supplied the Army with huge quantities of codes, strip ciphers, and key lists. It also monitored military communications to guard against security violations and disguised major military movements by creating false patterns of message traffic. The multifaceted communications security (COMSEC) operation absorbed the efforts of a sizable portion of agency personnel.[39]

---

[39] SRH 349, Achievements of the Signal Security Agency, pp. 39–50. This document does not mention, however, that the Army suffered one major compromise and one near disaster in its cryptographic program. In early 1942 the Axis Powers read the coded messages of Col. Bonar Fellers, the Army attache assigned to Cairo. This provided them with an inside view of British preparations in North Africa. Kahn, *Kahn on Codes*, p. 105. In 1945 an unguarded truck that contained a SIGABA belonging to the 28th Infantry Division disappeared in France. An investigation disclosed that the farmer responsible for the theft had only been interested in the truck. Thomas M. Johnson, "Search for the Stolen SIGABA," *Army* 12 (February 1962): 50–55.

The Electronic Battlefield

In addition to its traditional cryptologic functions, the Signal Security Agency assumed new responsibilities in the fields of electronic warfare and electronic intelligence. After Pearl Harbor the Signal Corps had transferred its Air Warning Service radar companies to the control of the Army Air Forces, ultimately turning over all responsibilities in radar development to the air arm. However, the Signal Corps continued to exercise staff supervision over Army radio countermeasures and "radio or radar deception" through a newly formed Protective Security Branch, which was reassigned to the Signal Security Service at Arlington Hall in December 1942. The transfer was made for administrative convenience, in an attempt to sidestep the provisions of the same "Child Labor Law" that had forced the move of CIC headquarters to Baltimore. It seemed easier to relocate the unit than to replace its trained and specialized personnel. However, the Protective Security Branch remained semi-autonomous.

Although the initial concern of the Protective Security Branch was to protect the Army's own communications from enemy jamming, it began to consider a more positive role as the balance of the war started to shift. In June 1943 the branch laid down the first guidelines for the use of countermeasures in the field. Only theater commanders could authorize the use of radio or electronic countermeasures, although task force commanders might be delegated this authority when actually engaging the enemy. At the same time, Army Ground Forces fielded two provisional countermeasures detachments to provide support in the 1943 summer maneuvers. In practice, however, American forces did not attempt communications jamming to any extent in World War II, since it would risk interfering with the vital flow of communications intelligence. The Americans made one significant attempt to disrupt enemy communications circuits during the Ardennes campaign, using electronic jamming equipment mounted in aircraft to interfere with the radio transmissions from German tanks.[40]

In other areas, the activities of the Protective Security Branch were more fruitful. The branch supported the Signal Security Agency's communications security program by monitoring traffic patterns on the Army's radio teletype links to ensure that pending military operations would not be compromised by a sudden surge of message traffic between two points. Additionally, the branch played a role in Army radio deception operations, training personnel, procuring equipment, and providing technical data. The 3103d Signal Service Battalion, activated in December 1943 for deployment in the European Theater of Operations (ETO), could simulate the communications nets of large formations. It

---

[40] Alfred H. Price, *The History of U.S. Electronic Warfare*, vol. 1 (Westford, Mass.: Association of Old Crows, 1984), pp. 177–78.

played an important role in diverting the Germans from the real locations of American troop concentrations before the invasion of Normandy. A smaller deception unit, the 3153d Signal Service Company, went to the Pacific in 1944.[41]

The branch's activities in electronic intelligence and electronic countermeasures—jamming enemy radars—were of even greater future significance. The rapid developments of radar technology in World War II and the employment of radar by both Germany and Japan meant that the new device became both an important new intelligence target and an object suitable for electronic countermeasures. In this exotic war, the Protective Security Branch, along with the rest of the Army's ground elements, played only a small role. The civilian Radio Research Laboratory of the National Defense Council conducted the initial research on methods of blinding enemy radar. The Army Air Forces generated the requirements in this field, since the threat posed by the early-warning and gun-laying radars of the day was against aircraft. Similarly, the Army Air Forces initially employed the first radar jammers and engaged in the first electronic intelligence operations from aircraft.

However, there proved to be a role for ground-based electronic countermeasures also. Under the aegis of the Protective Security Branch, a provisional unit, the 1st Signal Service Platoon (Special) was organized at Arlington Hall in July 1943 to find and jam enemy radar and moved almost immediately to Amchitka in the Aleutians. Since the Army could find no Japanese radars in the area, the unit subsequently redeployed to the island of Corsica in the Mediterranean and operated against German targets. Additional specialized companies and detachments were formed later, operating mainly in the Pacific.[42] The Signal Security Agency continued to exercise staff supervision over such units until April 1945, when most of the functions of the Protective Security Branch were transferred to other Signal Corps agencies. It would take another decade for electronic warfare and electronic intelligence to be reintegrated into the Army's communications intelligence organization.

Summation

The institutional evolution of the Military Intelligence structure in the continental United States during the World War II was slow and painful. Many factors hindered this process: the low resource baseline from which it had to begin; misplaced priorities; rivalry between Regular Army officers and the elite group of civilians who eventually received commissions and managed much of the effort; and the historical accident that had placed the Army's most important

---

[41] Deception operations, along with radar countermeasures, are covered in Thompson and Harris, *The Signal Corps: The Outcome*, pp. 315–16.

[42] For a thorough discussion of electronic warfare in World War II, see Price, *The History of U.S. Electronic Warfare*. Operations in the Aleutians are discussed on page 134.

collection arm, the Signal Security Agency, under the control of the Signal Corps rather than the Military Intelligence Division. In retrospect, some of the effort seems to have been misspent. Both the countersubversive program and the early focus on developments in Latin America may have diverted needed assets from more urgent areas. And it is clear that without British help in the way of example and assistance, the system would not have attained whatever efficiency it did. In the estimate of one official historian, the War Department's intelligence apparatus did not become effective until late 1944. Even then, serious defects remained in the internal organization of the Military Intelligence Service and in the degree of interservice cooperation in the communications intelligence field. It was not until May 1945 that the War Department developed a mechanism for setting intelligence priorities. It is perhaps unsurprising that the evolution of Army collection capabilities in the field would reflect the same pattern of awkward and uneven development.

6

World War II Intelligence in the Field

The Military Intelligence Service, the Signal Security Agency, and, for a time, the Counter Intelligence Corps were centrally directed organizations under the control of headquarters elements in the continental United States. However, the bulk of the Army's intelligence assets were in the field, at the disposal of commanders in the different theaters of operation established during the course of World War II. At the beginning of World War I, Brig. Gen. Joseph E. Kuhn had stated that intelligence was "as essential to modern armies as ammunition," and a second world conflict continued to demonstrate the truth of this dictum.[1] In all the various theaters there were certain uniformities of intelligence organization. Army officers served on combined intelligence staffs with various Allies. The theater signal intelligence service was operated on a compartmented basis separate from other intelligence activities, and assignment of intelligence and counterintelligence specialists to units was normally under centralized theater control. However, there were also differences in intelligence arrangements from theater to theater, depending on local conditions and circumstances.

In its allotment of campaign credits, the U.S. Army recognized the existence of only three great theaters of operation in World War II: the American, the Asiatic-Pacific, and the European–African–Middle Eastern. The actual command structure was more fragmented than this might suggest. During the course of World War II, major Army formations were committed to combat in four geographic areas: the Pacific Ocean Area (POA); the South West Pacific Area (SWPA); the European Theater of Operations (ETO); and the North African Theater of Operations (NATO), later redesignated the Mediterranean Theater of Operations (MTO). Paradoxically, U.S. Army contributions from an intelligence standpoint were greater in the Pacific area, but the European war had a larger impact on the ultimate organization of Army Intelligence. Most of American military resources in the field went into the fight against Germany, including the

[1] Powe, *The Emergence of the War Department Intelligence Agency*, p. 84

bulk of Military Intelligence assets. In addition, the nature of the language problem inherent in operations against the Japanese made Pacific requirements more specialized and less universal. The Army's focus on Europe and the relatively shorter distances between Washington and the field in this theater allowed lessons learned to translate rapidly into structural modifications.

Europe

The United States first entered the war in Europe as a junior partner. This was especially true in the field of intelligence, where Great Britain had developed extensive experience in field operations against the Axis, had a long tradition of successful intelligence operations, and had managed to break into the highest level of German communications with the help of its skilled cryptanalysts at Bletchley Park. British predominance in the communications intelligence field in Europe would continue throughout the war. The War Department was not apprised of the full dimensions of British success until mid-1943. The United States played no part in the exploitation of high-level German communications until 1944, when the Signal Intelligence Division of the European Theater of Operations, United States Army (ETOUSA), committed three American detachments in a War Department project to support the efforts of Bletchley Park.[2] Significantly, Eisenhower had a British G–2 in each of the theaters he successively commanded.[3]

From the intelligence perspective, the war in Europe was characterized by the gradual evolution of independent theater-level signal intelligence services, Military Intelligence services, and the institution of centralized control at the theater level over Army counterintelligence specialists. These developments took place at first in the Mediterranean and then in the European Theater of Operations.

When the Army entered World War II, it envisaged only two types of tactical signal intelligence units: radio intelligence platoons organic to the divisional signal companies and signal radio intelligence (SRI) companies assigned to field armies on a basis of one per army. The signal radio intelligence companies were quite sizable units, each with an assigned strength of slightly over 300 officers and men, internally divided into a headquarters platoon, an intercept platoon, a direction-finding platoon, and a wire platoon for communications. Neither of the two types had any analytical personnel. Analysis and translation were to be accomplished centrally by small radio intelligence staff elements at the theater and field army levels, as had been the case in World War I. These elements now reported to the chief signal officer,

---

[2] A popular account of this effort is contained in Thomas Parrish, *The Ultra Americans: The U.S. Role in Breaking the Nazi Codes* (New York: Stein and Day, 1986).

[3] Unfortunately, the memoirs of Eisenhower's G–2 were written before the release of the ULTRA secret. Maj. Gen. Sir Kenneth Strong, *Intelligence at the Top: Recollections of an Intelligence Officer* (New York: Doubleday, 1969).

not the G–2. The arrangement left the corps level without any dedicated communications intelligence support.[4]

The process of restructuring the Army's intelligence instruments began with the invasion of North Africa in 1942.The operation was launched with good intelligence—the British provided intensive support in this area, including furnishing the American high command with ULTRA-derived material. However, in the crunch of combat, American Intelligence organization was deemed less than adequate. The organization of Army tactical signal intelligence proved to be particularly deficient. The divisional platoons, in exposed locations near the front, were in too great a danger of being overrun to practice their specialty securely; the radio intelligence companies, as organized, were too large and too unwieldy to be used to support the corps, the command level most in need of such intelligence. Central processing proved to be impracticable, and the limited staffs available at the field army level to handle signals intelligence proved to be completely inadequate. At the same time, the communications practices of the European members of the Axis presented large volumes of material sent in clear or low-level codes that were susceptible to timely forward exploitation.[5]

In the initial stages of the North African campaign, the British bolstered the raw and badly organized American signals intelligence units with their own personnel. In early 1943 the U.S. Army deployed a theater signals intelligence service to North Africa. The 849th Signal Intelligence Service—the only such service to receive a numerical designation—was originally intended to function as a staff section, operating under the Signal Intelligence Division of Armed Forces Headquarters. Instead, in a hasty improvisation, it became a field unit. As the historian of the 849th SIS noted, "the unit set up in an isolated ravine in North Africa, without a telephone, a foot of field wire, a radio set, or a power unit, to mention only a few of the more obvious necessities."[6] Even toward the end of the war, the unit was handicapped by the ad hoc nature of its creation. A report deemed "the present organization . . . amorphous and unsatisfactory."[7]

Despite its organizational deficiencies, the 849th Signal Intelligence Service provided tactical signal intelligence units with the necessary analytical support. When the fighting moved to Italy, the problem of signal intelligence was solved by breaking the unwieldy signal radio intelligence companies into detachments and adding a small analytical element from the 849th SIS to each detachment to accomplish processing. Although this arrangement presented certain administrative complexities, since each element had a different parent headquarters, it

---

4 SRH 391, American Signal Intelligence in North Africa and Western Europe, pp. 6–7.

5 Memo, Col Harold G. Hayes, 1 Dec 43, sub: SIS: Lessons from North Africa, Army Cryptologic Records.

6 SRH 124, Operational History of the 849th Signal Intelligence Service, Mediterranean Theater of Operations, U.S. Army, p. 10.

7 Memo, Lt Col M. E. Rada for Colonel Shukraft, 27 Jan 45, sub: Reorganization of 849th Signal Intelligence Service, Army Cryptologic Records.

served to provide adequate communications intelligence to American ground and air forces. Later in the war, the Army Air Forces' own signals intelligence units took responsibility for the air dimension.

Combat experience in North Africa and the Mediterranean led to an overhaul of the entire structure of Army tactical signals intelligence in Europe. In 1943 the War Department gave the Signal Intelligence Division of ETOUSA operational control of all radio intelligence units in the theater. Further reforms followed. A revision of the divisional tables of organization and equipment (TOEs) in November 1943 eliminated the radio intelligence platoon from the divisional signal company, although it is not clear that this change was always implemented in the field. New tables provided for the incorporation of two radio intelligence platoons into the corps signal battalion.

This organizational concept was not especially happy, since it repeated the mistake of lumping a small number of communications intelligence personnel with a larger unit performing an unrelated function, with all the security and operational disadvantages this entailed. In the Pacific, when this reorganization went into effect, a knowledgeable intelligence officer would find the corps-level radio intelligence platoon he observed "fatally handicapped by lack of information and planning."[8] In the European theater, however, planners found a better solution. They devised a completely new type of communications intelligence unit to support the corps—a small signal service company with an organic cellular detachment of analytical personnel. These companies, numbered in a sequence beginning with 3250, required less than half the personnel spaces allotted to the regular signal radio intelligence companies and were formed from in-theater resources.[9]

Meanwhile, the war's lessons and the Army Air Forces' wishes had led the War Department to authorize similarly self-contained units, designated "radio squadrons, mobile," to meet the special needs of the Army's air arm. These squadrons replaced the mix of signal radio intelligence companies, aviation, and monitoring platoons in signal service companies, aviation, which previously had supported the Army Air Forces. In addition to containing a large analytical section, the new squadrons could intercept both continuous wave (Morse code) and voice transmissions from dispersed locations.[10]

American forces in Great Britain were finally committed to the cross-Channel attack on 6 June 1944. Once fully deployed, they mustered an impres-

---

[8] SRH 32, Reports by U.S. Army Ultra Representatives with Field Commands in the Southwest Pacific, Pacific Ocean, and China Burma India Theaters of Operations, 1944–1945, p. 69.

[9] A description of the operations of the corps-level signal service companies can be found in SRH 42, Third Army Radio Intelligence History in Campaign of Western Europe. This development was alluded to, but not fully explained, in the official World War II Signal Corps history. See Thompson and Harris, *The Signal Corps: The Outcome*, pp. 22, 347.

[10] *AAF Manual 100–1, AAF Radio Squadrons Mobile* (Washington, D.C.: Headquarters, Army Air Forces, 1944).

sive array of tactical signal intelligence units. Signal Security Detachment "D," a field element of the Signal Intelligence Division, ETOUSA, provided analytical support to the signal radio intelligence companies at the army-group and field-army levels, while AAF radio squadrons furnished signals intelligence to the numbered air forces. The signal service companies with their organic intelligence detachments operated in support of fourteen of the American corps that fought under Eisenhower. A similar type of unit was fielded in the Mediterranean Theater of Operations in 1945.

In theory, the signal radio intelligence companies were designed to fill the Army's communications security needs, as well as to provide signal intelligence. A section within the headquarters platoon of each company was allotted for communications monitoring. In practice, however, this function usually was neglected because of the press of more urgent duties. As a partial solution, the commander of Army forces in the Mediterranean area suggested that the Army develop a TOE for a new type of unit that could carry out a signal information and monitoring (SIAM) mission. Two such units were ultimately formed from Army assets in the Mediterranean: the 3151st Signal Information and Monitoring Company, which was assigned to the U.S. Seventh Army to support the invasion of Southern France, and the 3326th SIAM Company, which operated in support of the U.S. Fifth Army in Italy. These large units, each containing about 500 men, monitored Army communications for the dual purpose of checking for security violations and tracking the positions of the friendly units themselves. Under the fast-moving conditions of mobile warfare in Europe, normal command channels often operated too slowly, making such byproducts a useful tool for the field commander.[11]

Army counterintelligence organization in the field was also shaped by lessons learned in combat in North Africa and the Mediterranean. The first group of counterintelligence agents to be deployed had been a 71-man-strong detachment that accompanied the Western Task Force in the invasion of North Africa. Lacking in combat training, scattered in small sections over wide areas, and confronted by unsympathetic G–2s ignorant of the functions of the Counter Intelligence Corps, this initial element encountered many operational difficulties. However, under combat conditions, Counter Intelligence Corps personnel slowly resolved the initial problems. For example, new agents were trained in field security duties as well as in investigative functions. By mid-1943, with operations on Italian soil about to commence, all CIC agents in the theater were placed under the centralized administrative control of Counter Intelligence Corps, North African Theater of Operations, United States Army (NATOUSA). Also, a theater TOE had been developed, calling for 6-man divisional detachments and 13-man detachments at the corps level. Similar arrangements were introduced in the European Theater of Operations.

---

[11] Thompson and Harris, *The Signal Corps: The Outcome*, pp. 37–38, 65–67.

Some problems remained unsolved. Counter Intelligence Corps personnel were still controlled from Washington as part of the Military Intelligence Service. Although the rationale for this arrangement was Washington's fear that highly specialized counterintelligence assets otherwise might be misused, administration from 3,000 miles away created enormous problems. The arrangement slowed promotion in the field, and the CIC came to be nicknamed the "Corps of Indignant Corporals."[12] The attempt to run the Counter Intelligence Corps from offices in Washington also hampered local efforts to make timely adjustments in organization and doctrine based on field experience. The 6-man divisional detachments authorized in the Mediterranean area were obviously inadequate, since under combat conditions some CIC personnel needed to stay behind to provide continuity of coverage, while others advanced with their units. Moreover, the War Department tables of basic allowances (TBAs), under which detachments functioned, proved to be impracticable. Although CIC units were allotted equipment for performing the most elaborate investigations, they lacked adequate transportation.

Ultimately, these problems also were resolved. Counter Intelligence Corps personnel in the Mediterranean theater passed to local control in November 1943, and their counterparts in the United Kingdom made the same transition in April 1944. In January 1944 a new organizational table restructured Counter Intelligence Corps detachments along cellular lines, allowing units to be tailored to meet the requirements of varying echelons of command. In the ETO this resulted in the creation of a 17-man divisional CIC detachment composed of an administrative team and two operational teams. Larger counterintelligence detachments were attached to higher tactical echelons and to rear area service organizations. Finally, a more realistic allowance of equipment was secured, allocating a jeep to every two counterintelligence agents and giving the CIC the mobility it needed in a combat environment.

The problem of logically identifying CIC detachments was resolved in August 1944, when separate sequences of numbers were allotted to detachments serving with various levels and types of commands. Detachments serving with infantry and airborne divisions were given the numbers of their corresponding divisional organization: the 200 series was reserved for detachments serving with corps, the 300 series for those attached to field armies, the 400 series for CIC units attached to the theaters, the 500 series for detachments serving with armored divisions, and the 600 and 700 series for Counter Intelligence Corps elements attached to major formations of the Army Air Forces.

Intelligence specialists overseas not affiliated with the Counter Intelligence Corps were eventually organized under separate theater-level Military Intelligence services. These organizations evolved gradually. In the case of the

---

[12] History of the Counter Intelligence Corps, vol. 2, U.S. Army Intelligence Center, 1959, p. 87.

European Theater of Operations, the first non-CIC intelligence organizations to deploy in England were forward elements of MIS–X and MIS–Y: specialized sections of the War Department's Military Intelligence Service that were tasked respectively with assisting the escape attempts of downed American fliers and interrogating captured enemy personnel in depth. In April 1943 both elements were merged into a Military Intelligence Service detachment under theater control. With the arrival of additional diverse intelligence units, such as Military Intelligence specialist teams, censors, topographic and photographic intelligence personnel, and a training team, all field agencies except counterintelligence detachments were folded into the integrated, theater-level Military Intelligence Service, European Theater of Operations, in August 1943.

Intelligence specialists in the field operated in four types of teams during World War II: interrogation, interpreter, photo interpreter, and order of battle. In the European Theater of Operations, the first three types were allotted two officers and four enlisted men; order of battle teams had a single officer and two enlisted men. The Military Intelligence Service, European Theater of Operations, attached two prisoner interrogation teams and one of each of the other three types to each division, where they operated under the control of the divisional G–2. Larger numbers of teams were allotted to higher formations, and groups of teams at this level were sometimes formed into detachments with attached administrative personnel. Although the individual teams were small, the number of intelligence personnel assigned to them was considerable. The European Theater of Operations had 3,500 officers and men organized into specialist teams, not counting Military Intelligence personnel assigned to headquarters elements and to censorship duties.[13]

The collection of technical intelligence was not the responsibility of the theater-level Military Intelligence Service, but of "enemy equipment intelligence services" directed by the individual technical services. Technical intelligence personnel operated in teams at the field army level. Teams varied in size—the Signal Corps collection unit, for example, consisted of five officers and six enlisted men.[14] The efforts of the individual technical services in the field were supplemented by those of other organizations. The Army was represented on the Combined Intelligence Objectives Subcommittee, an element under the control of the Combined Chiefs of Staff which fielded joint United States–British, military-civilian teams to investigate scientific targets. The Army also played a leading role in the specialized mission, code named ALSOS, set up

[13] The activities of Military Intelligence Service specialist teams in Europe are discussed in detail in U.S. Forces, European Theater, *Report of the General Board*, Study no. 12, *The Military Intelligence Service in the European Theater of Operations* (U.S. Forces, European Theater, 1946). Brig. Gen. Oscar Koch, Patton's G–2, recalled that "each division had at least fifty auxiliary intelligence specialist personnel attached in the form of teams." Koch, *G–2, Intelligence for Patton* (Philadelphia: Whitmore, 1971), p. 131.

[14] Thompson and Harris, *The Signal Corps: The Outcome*, pp 165–66, 521.

at the instigation of the director of the Manhattan Project to look for evidence of German atomic research.[15]

In the war against Germany, technical intelligence teams often combined with other intelligence and counterintelligence personnel in ad hoc task forces to exploit newly liberated areas of intelligence interest. In Italy, "S Force" gave coverage to liberated Rome; "T Force" performed similar operations in France and Germany. These elements reached formidable size: the "T Force" that entered Paris contained representatives from seventeen different Allied intelligence elements and had a strength of 1,800, although most were administrative and security personnel.

Topographic intelligence was another specialized case. During World War I, the American Expeditionary Forces in France had placed this function within the G–2 section. In World War II theaters of operation, the function reverted to the Chief of Engineers, who maintained an Engineer Intelligence office. Mobile Engineer topographic battalions, relying on aerial photography, prepared maps. Field armies usually had a topographic engineering battalion, and a topographic Engineer company was assigned to each corps.[16]

For positive collection operations in the MTO and ETO, the Army relied on the Office of Strategic Services (OSS), the independent intelligence and special operations organization under the direct control of the Joint Chiefs of Staff. Although at the departmental level considerable rivalry existed between the OSS and the MID, Army commanders in Europe found the OSS a useful organization. In fact, Army personnel provided the bulk of OSS strength. In May 1944 friction in the European Theater of Operations was further eased when OSS and its British counterparts were directly subordinated to the theater commander under the newly created Headquarters, Special Troops, Supreme Headquarters, Allied Expeditionary Force. Members of OSS field units engaged both in collection and in special operations. Support was provided to Army units down to the division level. In addition, the X–2 Branch of OSS deployed small counterintelligence detachments. These detachments, which had access to selected ULTRA information, did not engage in active field operations, but provided CIC detachments information on enemy agents obtained at Bletchley Park.[17]

During World War I, the AEF's G–2 had been responsible for both propaganda operations and deception. This arrangement was not repeated in World War II. Eisenhower ran limited psychological warfare operations using pam-

---

15 The leader of this mission, Boris Pash, has provided a detailed account of the quest for a nonexistent Aryan atom bomb in *The Alsos Mission* (New York: Award House, 1969).

16 For engineer intelligence at the theater level, see *Engineers of the Southwest Pacific*, vol. 3, *Engineer Intelligence* (Washington, D.C.: Government Printing Office, 1950), p. 6.

17 OSS support for Army operations in World War II is described in Bradley F. Smith, *The Shadow Warriors: OSS and the Origins of the CIA* (New York: Basic Books, 1973), p. 203, and in Rhodre Jeffreys-Jones, *The CIA and American Democracy* (New Haven: Yale University Press, 1989), p. 307.

phlets and loudspeaker units through a special staff section, not through his intelligence staff. Planning the extensive deception operations that shrouded the time and place of the Allied landings was a British monopoly, carried out by the London Controlling Section. However, the U.S. Army deployed specialized units to support such operations in Europe, including Signal Corps elements and the 23d Headquarters, Special Troops, a composite unit that used rubber tanks, noise-making equipment, and dummy communications nets to simulate an armored division.

The Pacific

In the Pacific, Army Intelligence was structured a little differently. In the Pacific Ocean Area—the vast oceanic operational theater commanded by Admiral Chester W. Nimitz—the Army served as an adjunct to the Navy and the Marine Corps, and intelligence work was largely a naval preserve. However, an Army officer eventually did serve as J–2 controlling the Joint Intelligence Center, Pacific Ocean Area (JICPOA); Army topographic engineer companies provided JICPOA with mapping support; and two SRI companies were ultimately deployed.[18] In addition, toward the end of the war, a joint Army-Navy COMINT exploitation center, RAGFOR—for Radio Group, Forward—was set up on recaptured Guam to attack Japanese Army and Navy air-ground traffic, using the Army Air Forces' 8th Radio Squadron, Mobile, as its intercept arm.[19] This unit included Nisei interpreters. Military Intelligence interpreter, interrogator, and translator teams attached to Army divisions in the Pacific seem to have consisted of four, rather than six, persons.[20]

The major Army presence in the war against Japan was located in the South West Pacific Area, a theater that opened up when General Douglas MacArthur regrouped his forces in Australia following the American defeat in the Philippines. Here, organizational arrangements differed strikingly from those prevailing in the trans-Atlantic theaters. The creation of the SWPA committed the United States to the defense of beleaguered Australia. Significantly, the theater was directly subordinated to the U.S. Joint Chiefs of Staff, not to the Anglo-American Combined Chiefs of Staff. The objective situation, coupled with

---

18 Capt. Jasper W. Holmes served as chief of JICPOA and describes the organization in *Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific During World War II* (Annapolis, Md.: Naval Institute Press, 1979).

19 SRH 133, Report of Mission to Hawaii and Marianas to Study Security of 21st Bomber Command Communications, MIS, WDGS, March 1945, pp. 23–25.

20 Chandler and Robb, *Front-Line Intelligence*, p. 157. In September 1944 the TOEs for such linguist units were revised to call for four-man, rather than six-man, teams. War Department, Military Intelligence Service, History of Military Intelligence Training at Camp Ritchie, Maryland, 19 June 1942–1 January 1945, pp. 65–66, copy in INSCOM History Office files. However, the change was not implemented in the European theater. The Military Intelligence Language School at Camp Savage, not Camp Ritchie, provided linguist teams in the Pacific.

MacArthur's autocratic proclivities, allowed him to set up a U.S. Army staff to direct theater operations. At the same time, only limited American military assets were available initially. These considerations exerted strong pressure on the organization of intelligence in the theater. In contrast to the situation in Europe, U.S. Army Intelligence personnel in the SWPA were integrated into combined organizations under the direction of an American G–2, Brig. Gen. Charles Willoughby.[21]

In the spring of 1942 MacArthur set up a centralized cryptologic agency, Central Bureau, Brisbane (CBB). Headed by MacArthur's chief signal officer, Brig. Gen. Spencer Akin, a former chief of the Signal Intelligence Service, CBB was jointly manned by personnel of the U.S. Army and the Royal Australian Army and Air Force. The American component consisted at first of two officers and a few intercept operators drawn from a detachment of the 2d Signal Service Company on Corregidor, later reinforced by a signal service detachment furnished by Arlington Hall. The latter detachment included Col. Abraham Sinkov, one of the four men Friedman had initially recruited for the Signal Intelligence Service.

Thus, from the beginning Army Intelligence personnel in the Pacific were part of a high-level processing center that eventually broke Japanese military codes and thus generated ULTRA. Despite its name, CBB was not a static organization; an advance echelon of the Central Bureau accompanied MacArthur's GHQ in successive forward deployments, and by July 1945 almost the whole organization had been moved to San Miguel on the Philippine island of Luzon. By the end of the war, the Central Bureau had 1,500 personnel, more than half of them American, had acquired batteries of IBM machines, and was directing the collection efforts of four American signal radio intelligence companies and some ten equivalent British Commonwealth units.[22] In addition to this theater-level communications intelligence effort, an Army Air Forces radio squadron, mobile, operated in support of each of the two separate numbered American air forces assigned to the theater, and at least some tactical elements appear to have had their own radio intelligence platoons.

At the tactical level, communications intelligence was carried out in the South West Pacific Area under field conditions that differed significantly from those in Europe. Although the signal radio intelligence companies frequently operated in detachments, there was less requirement for analytical personnel to

---

21 The achievements of MacArthur's intelligence organization are documented (and glorified) in *Operations of the Military Intelligence Section, GHQ, SWPA/FEC/SCAP*, 10 vols. (Far East Command, 1948).

22 Discussion of Central Bureau Brisbane was inhibited for many years by the fact that the organization's host government preferred not to have the subject discussed. However, a photographic history of the American contribution was published shortly after the war. Curiously, the organization even was named somewhat inaccurately. It was hardly central—the naval communications intelligence effort was run on a completely separate basis—and it soon left Brisbane. One of the few open-source publications to mention it is D. M. Horner, *High Command: Australia and Allied Strategy, 1939–1945* (Sydney: George Allen and Unwin, 1982), pp. 224–46.

be decentralized at unit level in the Pacific, since Japanese low-grade systems "were practically nonexistent."[23] Furthermore, because of the vast distances in the Pacific, field sections were seldom close enough to the enemy to pick up low-powered tactical circuits.

The Central Bureau, Brisbane, was a purely cryptologic organization. A separate multinational organization, esoterically designated Section 22, General Headquarters, SWPA, was set up under Akin in 1943 to collect electronic intelligence on the rapidly increasing number of Japanese radar sets deployed in the theater. Section 22 differed from CBB in that it included representatives of the Navy and Marine Corps, as well as Signal Corps, Army Air Forces, and foreign personnel.

Other intelligence activities in the Pacific were also conducted on a multinational basis. The Allied Geographic Service provided topographic information on this little-mapped theater, while the Allied Translator and Interpreter Service (ATIS) blended Australian and American intelligence personnel into an integrated structure. Here, the nature of the target played a large part in the selection of personnel and in the approach to intelligence collection. Most of the 2,000 Americans who served in ATIS were Nisei, second-generation Japanese Americans. Because few soldiers of the Imperial Army surrendered, the emphasis was mostly on translation of documents written in the complex and polyalphabetic Japanese language. In Europe, three times as many interrogators as translators were needed. In the Far East, the ratio was reversed.[24]

Human intelligence collection operations in the SWPA came under the direction of the Allied Intelligence Bureau (AIB), because MacArthur barred the Office of Strategic Services from the theater. In addition to employing a network of stay-behind Australian coast-watchers to monitor Japanese shipping, the Allied Intelligence Bureau engaged in extensive penetration operations.[25] U.S. Army efforts in this field focused on the Philippine Islands where guerrillas already engaged in resisting the Japanese provided useful intelligence assets. To better exploit this resource, MacArthur fielded a special reconnaissance element largely manned by Filipinos recruited in the United States. This unit, the 1st Reconnaissance Battalion (Special), and its attached 978th Signal Service Company inserted radio-equipped teams by submarine into the islands to link with the guerrillas and collect intelligence.

Not all Army Intelligence assets in the Southwest Pacific Area, however, were integrated into combined operations. The U.S. Army ran its own counterintelligence operations, which were controlled by the G–2 of U.S. Army Forces, Far East

---

[23] SRH 169, p. 47.

[24] Col. Sidney F. Mashbir headed the Allied Translator and Interpreter Service. An account of its operations can be found in Mashbir's rather melodramatically entitled book, *I Was an American Spy* (New York: Vantage, 1953).

[25] Col. Allison Ind, who headed the bureau, also wrote a book, *Allied Intelligence Bureau: Our Secret Weapon in the War Against Japan* (New York: McKay, 1958).

(USAFFE), the base command responsible for the administration and supply of Army elements in the SWPA. Due to difficulties in securing counterintelligence agents from the United States, because of the enormous distances that separated Australia from the North American continent, a CIC school under theater control was set up to procure and train counterintelligence personnel. After August 1944 Brig. Gen. Elliot Thorpe, the G–2, U.S. Army Forces, Far East, exercised control over thirty-nine CIC detachments scattered around the Pacific through the theater-level 441st Counter Intelligence Corps Detachment. Divisional detachments in the Southwest Pacific Area were smaller than in the European Theater of Operations, but were augmented by Filipino linguists once the fighting reached the Philippine Islands. Although counterintelligence was clearly a national responsibility—the Counter Intelligence Corps in Europe reported to G–2, European Theater of Operations, U.S. Army, not to G–2, Supreme Headquarters, Allied Expeditionary Force—the fact that Willoughby lacked control over counterintelligence produced much bureaucratic friction.[26] Interestingly enough, when all Army troops in the Pacific were placed under MacArthur's control through the creation of U.S. Army Forces, Pacific (AFPAC), in April 1945, counterintelligence operations were again allotted to a special staff section, not to G–2.

U.S. Army tactical elements in the theater operated under separate American command after the end of 1942 and were supported by their own intelligence structure. However, interrogators and document translators were provided by advance echelons of ATIS. Optimally, two officers and ten men would be assigned to a division. In April 1945 separate language detachments, numbered in the 100 series, were activated from ATIS assets. In August the system was bolstered by fifteen headquarters elements dispatched from the Military Intelligence Training Center at Fort Ritchie. These received designations as numbered intelligence service organizations.[27]

Army Intelligence assets in the South West Pacific Area also included an elite reconnaissance force, the ALAMO Scouts. This provisional unit was used to conduct the type of long-range operations that the OSS conducted in Europe. Small parties of scouts were landed by submarine and flying boat on remote

---

[26] The antagonism between the SWPA G–2, Maj. Gen. Charles Willoughby, and the USAFFE G–2, Brig. Gen. Elliott Thorpe, continued to be nourished after the war ended. The Willoughby-sponsored official intelligence history of Far East Command claimed that counterintelligence arrangements were "contrary to staff manuals and ultimately led to friction, overlap, duplication, and general inefficiency." *Operations of the Military Intelligence Section, GHQ, SWPA/FEC/SCAP*, vol. 3, *Intelligence Series* (I) (Far East Command, General Headquarters [GHQ], Military Intelligence Service, General Staff, 1948), p. 14. Thorpe, in his own book, *East Wind, Rain: The Intimate Account of an Intelligence Officer in the Pacific* (Boston: Gambit, 1969), is more reticent. One CIC agent assigned to SWPA has written personal reminiscences. See William A. Owens, *Eye-Deep in Hell: A Memoir of the Liberation of the Philippines, 1944–1945* (Dallas: Southern Methodist University Press, 1990).

[27] *Operations of the Allied Translator and Interpreter Section, GHQ, SWPA*, vol. 5, *Intelligence Series* (Far East Command, GHQ, Military Intelligence Service, General Staff, 1948), pp. 27–28.

islands, both to gather intelligence and to engage in special operations. The unit derived its name from ALAMO Force, which controlled all American tactical units in the SWPA until September 1944, when it was replaced by the Sixth Army.[28] Technical intelligence for the Army was collected by the 5250th Technical Intelligence Composite Company (Provisional), a unique unit commanded by a colonel and formed from intelligence personnel of six Army technical services in the South West Pacific Area.[29]

Common Collectors

In all of the worldwide theaters, Army tactical units also played a role in the Military Intelligence process. The S–2 of each maneuver battalion had an intelligence section of 1 sergeant and 6 other soldiers, while the staff of the division G–2 was comprised of 2 officer assistants and 9 enlisted personnel. For reconnaissance purposes, each infantry and armored regiment had an intelligence and reconnaissance platoon. At the division level, a reconnaissance troop was organic to each infantry division, and each armored division had its own reconnaissance squadron.[30] Groups of mechanized cavalry were available to higher echelons of command; however, in practice these units were usually employed as combat elements in a screening role, rather than as intelligence collectors. At the corps level, the field artillery observation battalion also provided some incidental intelligence input.

Ground reconnaissance assets were not the only collection elements available. One major source of intelligence was provided by the L–4 "Grasshopper" light aircraft, organic to all divisions and artillery groups. These planes were first introduced in 1942, when it became clear that the semi-autonomous Army Air Forces, which had prime responsibility for both photographic and visual observation, intended to implement its mission in ways that scanted the priorities of the ground forces. The ten light aircraft assigned to each infantry division were used primarily for artillery spotting, but, at least in the European theater, they flew 30 percent of their missions for general intelligence support.[31]

---

[28] An excellent article on the Alamo Scouts is Les Hughes, "The Alamo Scouts," *Trading Post* 45 (April–June 1986): 2–16.

[29] Marc B. Powe and Edward E. Wilson, *The Evolution of American Military Intelligence* (Fort Huachuca, Ariz.: U.S. Army Intelligence Center and School, 1973), p. 76.

[30] Chandler and Robb, *Front-Line Intelligence*, pp. 35, 83, 87. The reconnaissance troops were sometimes known as "tincan cavalry," and were often diverted to nonintelligence functions.

[31] *Report of the General Board*, Study no. 20, *Liaison Aircraft with Ground Forces Units* (U.S. Forces, European Theater, 1946). The Army Air Forces observation squadrons and groups previously assigned to Army tactical units were resubordinated to AAF Air-Ground Support Commands in 1941; concurrently, it became all too apparent from the experience of the other warring air forces that existing observation aircraft could not survive in a combat environment. Ultimately, the "observation" mission was subsumed into reconnaissance, and carried out by stripped-down converted fighters and bombers assigned to the AAF's tactical air commands. Futrell, *Command of Observation Aviation*, pp. 6–29.

Conclusion

Several points in the field organization of Army Intelligence during World War II are notable. At the tactical support level, the Army organized Intelligence into a multitude of single-discipline teams and detachments. Intelligence work was still largely thought of as a staff function, not a line function, and intelligence specialist teams were attached to tactical formations to assist the G–2 staff.[32] This approach was reflected in unit structure. Signals intelligence, a specialized case, was carried out by company-size Signal Corps units and by the Signal Security Agency's single oversized battalion. In the other intelligence disciplines, there were no units larger than detachments or teams, apart from the provisional technical intelligence company that operated in the South West Pacific Area and a one-of-a-kind provisional 1st Combat Intelligence Platoon at Fort Richardson, Alaska.

As the war went on, the Army made some attempts to introduce higher-level organizational structures. To improve command and control of intelligence work in the field, by 1945 the Military Intelligence Training Center had activated twenty-six three-man military intelligence headquarters detachments, each capable of coordinating the efforts of several intelligence specialist teams. The compartmented work and reporting channels of signals intelligence also produced a more hierarchical form of organization. Such measures were, however, exceptional.

During the war, some commanders questioned the prevailing organizational concepts. Lt. Col. H. Gordon Sheen, who had served as the first chief of the CIC, proposed that intelligence battalions be formed from Army-level troops and attached down to corps level as needed. He envisioned an integrated multidiscipline battalion, consisting of a headquarters and headquarters company, a counterintelligence company, an engineer topographic company, a prisoner-of-war interrogation company, and a radio intelligence company.[33] However, Sheen was ahead of his time. It would take a dozen more years to integrate even counterintelligence and positive collection functions into a single unit, and much longer before signals intelligence could be brought under the same umbrella as the other intelligence disciplines.

Whatever deficiencies existed in the organization of Army Intelligence, it had at least performed well enough to help bring about victory in World War II. On 9 May 1945, Nazi Germany unconditionally surrendered to Allied forces. Japan followed suit on 14 August. The United States had fully achieved all its military objectives. However, victory did not bring security. As an

---

[32] "It may be said that the general organizational plan of intelligence forces in the Army is designed to locate the G–2 section or its counterpart, as a 'staff' unit rather than a 'line' unit." History of Military Intelligence Training at Camp Ritchie, p. 15.

[33] History of the Counterintelligence Corps, vol. 11, U.S. Army Intelligence Center, 1959, p. 62.

inevitable result of the destruction of German power in Central Europe, the forces of the Soviet Union had extended their influence deep into Europe. And the USSR, a totalitarian society committed to a messianic ideology, would prove to be as great a danger to the stability of the world order as had the Axis. The war had produced a quantum advance in technical progress, but the most ingenious of the new devices—the atomic bomb which the United States had invented and employed—in the long run threatened civilization itself. It was now the task of the U.S. Army and its Intelligence component to help keep the uncertain peace.

7

The Cold War and Korea

Euphoria over the American victory in World War II was short lived. It became apparent that the destruction of the Axis Powers had only created a power vacuum into which another totalitarian state, the Soviet Union, steadily and inexorably moved. The United Nations, created to guide a lasting peace, soon appeared to be a hollow shell, its Security Council paralyzed by Russian vetoes. Confronted by Soviet repression in Eastern Europe and Communist subversion in the West, the United States slowly moved to meet the new challenge. In this Cold War between East and West, at first the weapons were economic and diplomatic. The United States succored hard-pressed Greece and Turkey with military and economic aid in 1947, then moved to restore the destroyed economy of Western Europe with the Marshall Plan in 1948. A Soviet blockade of the Western zones in Berlin was countered by a massive airlift. Finally, the United States abandoned two centuries of tradition and joined in a peacetime military alliance with the European democracies when it became a member of the North Atlantic Treaty Organization (NATO) in 1949.

However, the threatening international scene was not reflected in America's military posture. The vast armies fielded in World War II had been demobilized quickly. Once the draft came to an end in 1947, the Army shrank to a strength of 550,000. Much of this force was tied down in occupation duty, with four skeleton divisions in Japan, two for a time in Korea, and another in Germany. In the summer of 1948 Congress renewed Selective Service, spurring recruitment and allowing a slight buildup of Army strength to about 600,000. Many Americans hoped that the American monopoly of the atomic bomb would preserve the peace. But the Soviets demolished this assumption in 1949 by exploding a nuclear device of their own. Meanwhile, stability in the Far East was deteriorating. By 1949 Communist Chinese armies had brought all of mainland China under the red flag. The United States had withdrawn its occupation troops from South Korea, and a Communist government in the North now stared balefully across the 38th Parallel at its democratic neighbor to the South. In June 1950 it marched across the border. In response, an unready America was drawn into a new war.

The shock of the Korean War—and the subsequent Chinese Communist intervention—transformed American national security policy. The Army grew to 1.5 million men, organized into twenty active divisions. Large forces were deployed not only on the Korean peninsula, but also on the continent of Europe. At the time, American leaders feared that the Korean attack might be an attempt to divert the West from a possible Soviet onslaught against the West European democracies. Originally, NATO had been a paper alliance; now it was backed up by American steel.[1] For a whole generation, American soldiers would man many of the lines first established in both Asia and Europe during the early 1950s. And Army Intelligence, initially reeling from two major surprises (the initial Korean attack and the later Chinese offensive) was ultimately revitalized.

Restructuring Military Intelligence

In the aftermath of World War II, Army Intelligence was affected not only by the massive postwar contraction of military strength, but by sustained organizational turbulence. This was brought about by two conflicting types of pressure. Some policy makers simply wanted to return to prewar conditions, dismissing wartime expedients as aberrations caused by a never-to-be-repeated crisis. Others attempted to make use of the lessons learned in World War II to create a better structure. As a result, much of the Military Intelligence architecture with which the country had fought World War II was dismantled and intelligence assets placed in new configurations.

During World War II, control of communications intelligence collection assets had been split between the Signal Security Agency and the theater commanders. This arrangement had created significant problems, since it was impossible to neatly separate the tactical aspects of communications intelligence from the strategic ones.[2] Even before the fighting had ended, the Army had decided to entrust exploitation of the electronic communications spectrum to a single agency. On 15 September 1945, the Signal Security Agency was separated from the Signal Corps and became the Army Security Agency (ASA), assuming command of "all signals intelligence and security establishments, units, and personnel" of the Army.[3] The new agency, which continued to function under direct control by the Army G–2 in Washington, inherited the mission, functions, and assets of its wartime predecessor and took over the communications intelligence and communications security resources previously at the disposal of theater and Air Force commanders. In addition to unifying the Army's cryptologic structure, the formation of the Army Security Agency also marked a brief

---

[1] A broad overview of U.S. defense policy during this period is provided in Doris M. Condit, *History of the Office of the Secretary of Defense, Volume II: The Test of War, 1950–1953* (Washington, D.C.: Historical Office of the Secretary of Defense, 1988).

[2] SRH 169, p. 59.

[3] Ibid., p. 85.

reversal in the tendency towards increased autonomy for the Army Air Forces in this field, since the AAF's radio squadrons, mobile, and other cryptologic assets were resubordinated to the agency.

Army counterintelligence organization also underwent a substantial restructuring. By the time World War II ended, the Counter Intelligence Corps and the Security Intelligence Corps formed in 1944 had both been placed under the Army Service Forces' director of Intelligence. Agents of both organizations now received the same training and operated under the same regulations. Under these new conditions it was obviously pointless to maintain two parallel counterintelligence elements. Accordingly, in April 1946 the Security Intelligence Corps was merged with the Counter Intelligence Corps. In May numbered CIC detachments were constituted to operate in support of each of the nine service commands and the separate Military District of Washington (MDW). These detachments were assigned numbers in a sequence running from 107 to 116.

President Harry S. Truman presented a different kind of organizational challenge to the Army when he abolished the wartime Office of Strategic Services on 1 October 1945. The assets of the OSS were divided: analytic personnel were shipped off to the State Department, but the bulk of the organization, consisting of military personnel trained in clandestine collection, counterintelligence, covert action, and black propaganda, combined into the new Strategic Services Unit under the War Department. However, the organization was not assigned to G–2, but to the Office of the Assistant Secretary of War, which created an anomalous situation.

The existence of the Strategic Services Unit forced a reexamination of the entire national intelligence structure, a task which the Lovett Board assumed at the end of 1945. An executive order early in 1946 established a new Central Intelligence Group, a rudimentary national-level intelligence agency. This prototype central intelligence agency was at first merely a cooperative interdepartmental activity that depended on the armed services and the State Department for its staff, budget, and facilities. However, it did serve as a holding area to dispose of what remained of the Strategic Services Unit, most of whose members were slated for demobilization with the rest of the Army.[4] Nevertheless, in 1946 a vestigial undercover capability still remained at the disposal of the U.S. intelligence community.

A further step in the immediate postwar reorganization of U.S. Army Intelligence came about in May 1946 when the Army did away with its wartime structure. Not unexpectedly, the reorganization gave greater power to the traditional Army Staff and to the heads of the old-line technical services. One important result of the post–World War II Army reorganization was that MID, now redesignated the Intelligence Division, was restored to its prewar status as one of five equal functional divisions on the War Department General Staff. Now

[4] Bradley F. Smith doubts that the SSU ever exceeded 750 people. *The Shadow Warriors*, p. 408.

headed by a director of Intelligence, the division was specifically intended to serve as an operating agency as well as an element engaged in intelligence planning and staff supervision. Fortunately for all parties involved, the Intelligence Division had already relinquished the task of preparing the Army's official histories, which it had taken on in World War II. The Intelligence Division's resumption of operating functions led to the abolition of the separate Military Intelligence Service.[5] In addition, the discontinuance of the Army Service Forces at this time resulted in the Counter Intelligence Corps' once more falling under the control of the War Department's Intelligence Division.

The Intelligence Division now set intelligence requirements for the Army, supervised collection, conducted evaluation, produced finished intelligence, and disseminated this information throughout the Army. Compartmented intelligence continued to be channeled through the Special Security System created in World War II. In November 1946 two separate detachments, both sharing a common commander, were set up within the division to manage the various Special Security Offices (SSOs). Detachment F supervised those at three locations in the continental United States; Detachment M directed a more extensive network overseas.

The Intelligence Division focused on the global requirements imposed by the rapidly deepening Cold War between the West and the Soviet Union. It had not only Army-wide intelligence taskings, but was responsible as well for satisfying national needs for political and economic intelligence. The 1946 reorganization placed the Intelligence Division and its director at an apogee of institutional power. The director of Intelligence had sole authority over the Army assets he needed to discharge his responsibilities. In addition to the internal resources which he controlled directly, he wielded influence in the management oversight of the Central Intelligence Group through his membership on the National Intelligence Board. The director also served on the board that governed national signals intelligence policy.

Almost immediately, however, the scope and autonomy of the Intelligence Division and its director came under attack. There were already conflicts in jurisdiction between the Intelligence Division and the intelligence arm of the now practically autonomous Army Air Forces. It was obvious that the pending creation of a separate Air Force, a process well under way by 1946, would result in the transfer of the air-oriented portions of Army Intelligence to the new service. There were other kinds of pressures at work. Many believed that lack of coordination between Army and Navy Intelligence had helped to bring about the disaster of Pearl Harbor. With tensions between the United States and Russia growing visibly, there was a demand to create a national-level intelligence

---

[5] James A. Hewes, *From Root to McNamara: Army Organization and Administration, 1900–1963* (Washington, D.C.: U.S. Army Center of Military History, 1975), p. 160, mistakenly indicates that MIS was redesignated as the Army Security Agency.

body with greater powers than the Central Intelligence Group to coordinate the activities of the service intelligence components and to specialize in gathering political and economic intelligence.[6]

Both of these pressures came to a head in June 1947, when Congress passed the National Security Act. The bill created an independent Air Force and simultaneously unified all armed services under the secretary of defense. These actions significantly affected the structure of Army Intelligence. The Air Force developed a separate intelligence organization of its own. Air attaches took their places beside military attaches; counterintelligence assets already serving with Air Force units were withdrawn from the Counter Intelligence Corps; the Army Security Agency gave up control of its three radio squadrons, mobile, and one radio security detachment to the new service.[7] Finally, in 1950 the Air Force established its own special security officer system.

The most important impact of the 1947 act, however, came with the establishment of the Central Intelligence Agency (CIA). This new national-level intelligence authority reported to the freshly created National Security Council (NSC). Unlike its predecessor, the CIA was not subordinate to the services, but had its own budget and personnel and a large mandate to independently gather and produce intelligence at its own discretion. The formation of the CIA did not directly interfere with the independence of Army Intelligence, but the role of the Army's director of Intelligence in influencing national intelligence decisions was decidedly curbed, although not eliminated, and the new agency assumed control over large areas of political and economic intelligence for which the Army had been responsible.

Postwar Operations: Human Intelligence and Counterintelligence

Under peacetime conditions, the Intelligence Division in the post–World War II period had at its disposal three major institutional elements: the Army attache system, the Counter Intelligence Corps, and the Army Security Agency. The oldest and most traditional of these, the attache system still provided the Army with 80 percent of its uncompartmented intelligence. The attache network was large—before the final separation of the Air Force and later

---

6 Considering the substantial American Intelligence successes in World War II, one is surprised at some of the sentiments expressed during the congressional hearings that led up to the establishment of the Central Intelligence Agency. Army Air Forces' General Hoyt Vandenberg expressed the opinion that the United States was "400 years behind" in the intelligence field, which he appeared to equate with clandestine human intelligence collection. *National Security Act of 1947: Hearing Before the Committee on Expenditures in the Executive Departments, H.R. 2319*, 80th Cong., 1st sess., 27 June 1947, p. 10.

7 ASA units transferred to AFSS were the 1st, 2d, and 8th Radio Squadrons, Mobile, and the 136th Radio Security Squadron. Frank M. Whitacre, *A Pictorial Review of USAFSS, 1948–1973: 25 Years of Vigilance* (San Antonio: U.S. Air Force Security Service, 1973).

economies by the Truman administration 285 officers were serving in seventy stations—and increasingly professional. As early as October 1945 the Intelligence Division had begun offering training courses to officers selected for attache duty, and by 1946 this effort was being directed by a Strategic Intelligence School. Although the work of its graduates was increasingly hampered by tight security measures in Communist countries, they continued to provide valuable military information from their far-flung assignments.

For a short period, the Intelligence Division also operated the Gehlen Organization, an intelligence apparatus inherited from the German Army of World War II. Maj. Gen. Reinhardt Gehlen, former head of German intelligence on the Eastern Front, thoughtfully had brought his complete files with him when he surrendered to the American Army. Gehlen, his documents, and his personnel were moved to the United States for a time and placed under Intelligence Division control.[8] Ultimately, the organization returned to Germany, passed under CIA direction, and finally became the nucleus of the present West German *Bundesnachrichtendienst*.

For counterintelligence, the Intelligence Division relied on the reestablished Army Counter Intelligence Corps, responsible for the procurement, training, and administration of all counterintelligence personnel. In the continental United States, six numbered Zone of Interior armies had taken over the functions of the nine former service commands following the dissolution of the Army Service Forces, and this brought about a realignment of existing CIC elements. Three CIC detachments were inactivated, and the 108th, 109th, 111th, 112th, 113th, and 115th Counter Intelligence Corps Detachments were subordinated respectively to the First, Second, Third, Fourth, Fifth, and Sixth Armies, while the 116th CIC Detachment continued to support the Military District of Washington. These geographic arrangements would remain unchanged for twenty years. Other counterintelligence units were attached to divisions based in the United States: to the Armed Forces Special Weapons Project that dealt with the military applications of atomic energy, to overseas commanders, and to the Intelligence Division itself. Usually, investigations continued to be supervised by the local G–2s, although the most sensitive cases were controlled by the director of Intelligence.

When the Counter Intelligence Corps first came under the command of the Intelligence Division, it was supervised directly by the division's counterintelligence staff element. However, it proved impracticable to exercise detailed control over a Camp Holabird–based organization from the Pentagon, so the position of chief, Counter Intelligence Corps, and commanding general, Counter Intelligence Corps Center, was authorized in April 1947. In short, the Counter Intelligence Corps had reverted to the institutional status it had originally held during the first part of World War II.

---

[8] Gehlen's defection and early connection with Army Intelligence are described in E. H. Cookridge, *Gehlen, Spy of the Century* (New York: Random House, 1971), pp. 115–54.

Holabird, redesignated a fort in 1950, soon became an important center of intelligence activities. In addition to housing the CIC's administrative headquarters and the Counter Intelligence Corps School, it was the seat of the Counter Intelligence Corps Board, which directed research and development and handled personnel matters. The fort also began housing certain field activities of the Intelligence Division of the General Staff. In 1950 the Central Personality Index, the name file which the Intelligence Division had set up the year before, was moved on post, and in 1951 Holabird became the home of the Army's Central Records Facility, which served as a centralized repository for the records of all the Army's personnel security investigations in the continental United States and contained microfilmed copies of the files of overseas CIC detachments.

In the aftermath of World War I, the Army had allowed its counterintelligence function to atrophy. This course was not paralleled after World War II. The Army was first confronted with the necessity of providing large occupation forces abroad with counterintelligence support and then by the security demands of the Cold War. As a result, while total Army strength melted away in the course of postwar demobilization, the number of CIC personnel declined only modestly, falling from a high point of 5,000 in World War II to 3,800. However, there was a worrisome decline in quality. Rapid demobilization of veterans and the termination of the draft eliminated the reservoir of skilled and highly educated personnel upon which the Counter Intelligence Corps had been able to draw. In World War II, two-thirds of all enlisted agents had been college graduates; half had possessed law degrees or the equivalent. Now, overseas commanders were soon reporting that only 10 percent of Counter Intelligence Corps School–trained personnel had completed a college education. The Army partially solved the problem by increasing the proportion of officers in the force and authorizing the recruitment of warrant officers. Moreover, not all trends were negative. In 1946 members of the Women's Army Corps (WAC) were admitted to the CIC School, and in 1950 CIC personnel were first trained to make use of a new and promising investigative technique, the polygraph.[9]

The years following the war saw the Counter Intelligence Corps come out on the losing side in several jurisdictional disputes. In 1949 the corps lost responsibility for the Army's industrial security program to the Provost Marshal General's Office. It also clashed with the Federal Bureau of Investigation (FBI). In 1947 President Truman issued Executive Order 9835 instituting a Federal Loyalty Program, which directed that all investigations of civilians be performed by the FBI. This contradicted the existing Delimitations Agreement between the armed services and the FBI, in existence since before World War II. Ultimately, the Army signed a new agreement with the FBI in 1949, allowing the FBI to investigate Army civilians in the Western Hemisphere, while the Army handled

[9] CIC activities in the postwar period are covered in History of the Counter Intelligence Corps, vol. 24, U.S. Army Intelligence Center, 1959.

investigations overseas. However, areas of friction between the two organizations continued to exist.

One problem, as the G–2, Sixth Army, pointed out perceptively, was "a basic difference in concept of subversive intelligence." The FBI's responsibility was "primarily for accumulation of admissible evidence to provide the basis for legal action against individuals or organizations, usually for acts which are already completed." Army Intelligence, on the other hand, functioned "primarily to forestall acts of violence or to prevent the spread of disorder; anticipatory planning is essential; and advance information on trends and developments must be continuously available."[10] As it turned out, these differences in concept would prove even more troubling twenty years later.

Much of the work of the Counter Intelligence Corps was performed abroad, as American occupation forces in Europe and the Far East first attempted to root out the remaining vestiges of Nazism and militarism and then faced the task of countering Communist subversion.[11] In Germany, all Army counterintelligence assets were consolidated into a single large unit, the 1,400-man-strong 970th Counter Intelligence Corps Detachment, which blanketed the American Zone of Germany with a network of regional and field offices. In 1948 this was converted into the 7970th Counter Intelligence Corps Detachment, organized under a table of distribution (TD) as a one-of-a-kind unit to perform a specific mission. The change brought about difficulties in obtaining personnel, however, and as a result the 7970th was superseded by a new TOE outfit, the 66th Counter Intelligence Corps Detachment, in 1949.[12]

The 441st Counter Intelligence Corps Detachment, at one point almost as large as its European counterpart, played a similar role in supporting the occupation of Japan. Counterintelligence in Japan was facilitated by the activation of a unique unit, the 319th Military Intelligence Company, formed in 1946 of Nisei interpreters from MacArthur's Allied Translator and Interpreter Section.[13] Although the Counter Intelligence Corps and its predecessor organization had accepted Japanese-American personnel since 1940, there were too few of them in Japan to meet the needs of the occupation. To remedy this situation, the men

---

10 Bidwell, History of the Military Intelligence Division, vol. 6, pp. 649–50.

11 Sometimes the Nazis were used against the Communists, as demonstrated in Allan A. Ryan, Jr., *Klaus Barbie and the United States Government: A Report, with Documentry Appendix, to the Attorney General of the United States* (Frederick, Md.: University Publications of America, 1984).

12 For Army lineage purposes, the distinction between TOE and TD units lies in the fact that TOE units are permanently placed on Army rolls and are activated and inactivated as needed, whereas TD units are organized on a one-time basis for a particular mission and are not perpetuated after discontinuance. A typical example of a TOE unit would be an infantry battalion, while a typical TD unit would be an Army garrison. Because of the peculiar demands of intelligence work, many intelligence personnel have historically served in TD (later TDA, or table of distribution and allowances) units.

13 However, the Translator and Interpreter Service—in April 1946 it lost its allied status and title—continued an independent existence under G–2 control.

of the 319th Military Intelligence Company were given theater counterintelligence credentials to make use of their invaluable language capabilities in assisting investigations.

Counter Intelligence Corps operations overseas faced their own special problems. Some higher commanders abroad objected to the idea of CIC agents living in civilian clothes apart from the structure of the Army as a whole and sought to remilitarize the operations. At one point, all counterintelligence personnel in Germany were put back into uniform and ordered into Army billets with considerable loss of operational effectiveness. Another problem was that some CIC personnel acclimatized themselves to life overseas all too well and had married foreign wives. In June 1950 the CIC chief issued an order that any CIC member marrying a foreign national without grant of a waiver would be terminated. Finally, operational necessity drew the corps into unfamiliar activities. In Germany, for example, CIC agents helped crack down on the black market. In most overseas commands, Cold War needs forced Counter Intelligence Corps units to engage in positive collection of intelligence. With no mechanism for gathering human intelligence at its disposal outside of the attache system, the Army was forced to misapply its counterintelligence assets to fill the void.

The Army Security Agency

The Intelligence Division's most important asset was provided by the newly formed Army Security Agency (ASA). In many ways the Army Security Agency was unique; its official historian later wrote that it was "within, but not part of, the overall military establishment."[14] A large portion of the headquarters continued to be staffed by civilian experts, and the agency's organizational pattern had no parallel in the rest of the Army. The Army Security Agency was put together on the "stovepipe" principle, and Arlington Hall controlled the activities of all units through a separate ASA chain of command. This distinctive vertical command structure, which provided centralized control over all Army signals intelligence and communications security assets, set ASA apart, as did the high walls of compartmented secrecy surrounding its sensitive operations. All that most members of the Army knew about the Army Security Agency was that they were not supposed to know anything about it.

As a separate entity within the Army, the agency was almost completely self-sufficient. In addition to conducting its own operational missions, ASA administered its own personnel system, ran its own school, arranged for its own supplies, and conducted its own research and development. The agency's cryptologic activities continued to be indispensable to the nation's security. The postwar drawdown of strength affected the ASA just as it did the rest of the armed forces, and the

---

[14] Army Security Agency, History of the Army Security Agency and Subordinate Units, FY 1951, vol. 1, p. 5.

organization had to be realigned to meet new national priorities. But the competence which had marked the activities of its predecessors was still there.

In the field, ASA's principal assets were seven large fixed field stations, most of them left over from World War II, at Vint Hill Farms, Virginia; Two Rock Ranch, California; Helemano, Hawaii; Clark Field, the Philippines; Fairbanks, Alaska; Herzo Base, Germany; and Asmara, Ethiopia. Although the headquarters of the 2d Signal Service Battalion was disbanded in 1946, having become redundant when the Army Security Agency established its own personnel system, the stations continued to be manned by lettered detachments of the battalion until May 1950, when all of ASA's TDA elements were redesignated as numbered Army Area Units in the 8600 series. Field stations were supplemented by tactical units—signal service companies and detachments—operating from semifixed positions. The ASA exercised command and control of overseas elements through its regional headquarters in Europe and the Pacific, and later through smaller headquarters elements in Hawaii, Alaska, and the Caribbean. Overall direction of the Army's cryptologic effort and necessary analysis and production work were centralized at ASA's Arlington Hall headquarters.

Since the Army Security Agency's mission had a national impact, it had to be responsive to requirements generated by agencies outside the Army. Initially, ASA operated under the umbrella of the Army-Navy Communications Intelligence Board established during World War II. Other players soon became involved in the results of ASA's work, however, and membership on the board was expanded. At first it became the State-Army-Navy Communications Intelligence Board, evolving a little later into the United States Communications Intelligence Board (USCIB), an element which included FBI and CIA participation.

As part of its mission, the agency supervised all Army communications security, produced and distributed all cryptomaterial, and served as the ultimate maintenance point for cryptomachinery. It also had responsibility for strategic communications cover and deception. All this entailed a substantial commitment of resources. The Army Security Agency's major effort in the communications security field after World War II was the replacement of the super-secure SIGABA with a cryptomachine that operated on less sensitive design principles, the SIGROD, later redesignated as ASAM–5. The idea was to place SIGABA in a reserve status for possible wartime demands, and to use SIGROD, the compromise of which would be less damaging.

ASA's initial organization proved short lived. Ever since World War II, the demand for the centralization of all cryptologic activities under the control of a single body had been increasing. By 1946 the Army had realized that both Army and Navy cryptologic organizations should be placed under the direction of a common agency to ensure a proper coordination of effort. The creation of an independent Air Force, with its own Air Force Security Service, seemed to threaten the field with greater fragmentation than ever before. In response, during 1949 the Armed Forces Security Agency was established under the Joint Chiefs of Staff.

The Armed Forces Security Agency, commanded by officers from the various services on a rotating basis, brought together at a high level all U.S. cryptologic operations and relieved the individual services of their direction and production functions in this field. In practice, the design concept behind this new agency proved flawed. The Armed Forces Security Agency was responsive only to the needs of the armed forces, leaving wider national concerns unmet. Moreover, the planned musical chairs rotation scheme for providing the agency's leadership destroyed administrative continuity.[15] In 1952 the National Security Agency (NSA), a civilian agency under the Department of Defense, replaced the Armed Forces Security Agency.

In 1949, however, it seemed that the formation of the Armed Forces Security Agency would gut ASA, reducing it to the role of a residual Army cryptologic agency with a function limited to ensuring Army communications security. In addition to giving up a major portion of its original mission, the ASA transferred most of its civilian staff to the new national-level agency, including William Friedman and almost the whole group of Signal Intelligence Service pioneers. A long Army tradition that stretched back to the days of the World War I Cipher Bureau thus passed to a joint service organization. The Army Security Agency met the organizational challenge by restructuring itself to meet Army-specific needs. After 1949 the agency turned its attention to developing mobile field units to support tactical commanders at every level, a task accelerated by the outbreak of the Korean War in June 1950.

Postwar Military Intelligence: Deficiencies

There were definite weaknesses in the structure of post–World War II Military Intelligence. Army Intelligence as yet had not become truly professional. Officers served in intelligence assignments on the basis of detail; their commissions, and in many cases, their career interests, lay with their basic branches.[16] Continuity in the more specialized areas of intelligence, such as counterintelligence and signals intelligence, rested in the pool of reserve officers who had continued in active service after World War II. Their numbers, however, inevitably diminished. To remedy this situation, in 1946 a panel of intelligence officers, the Forney Board, had recommended that a Military Intelligence Corps be established, consisting of both detailed and permanently assigned members. But other elements of the Army Staff had vigorously rejected the recommendation, on the usual grounds that any officer should be capable of performing intelligence duties.

---

[15] SRH 123, The Brownell Report, pp. 47–52.

[16] This tendency was reflected even at the top. In 1949 the Hoover Commission reported that "four of the last seven G–2's were without any intelligence experience whatsoever." Henry Howe Ransom, *The Intelligence Establishment* (Cambridge: Harvard University Press, 1970), pp. 109–10.

Training presented another problem. Under the new Army organization adopted in 1946, the director of Intelligence had limited responsibilities in the training field. The Strategic Intelligence School, the attache training facility under the direct control of the Intelligence Division, was an exception. So was the area of language training. In 1946 the Military Intelligence Service Language School organized in World War II was redesignated the Army Language School and moved to the Presidio of Monterey in California. There, it continued to function under Intelligence Division control until it was resubordinated to Sixth Army headquarters in 1950.[17] The Intelligence Division also maintained lettered language detachments in Germany, Japan, and (briefly) China for advanced individual instruction. The Army Security Agency had a training school for its own personnel. Originally located at Vint Hill Farms, near Warrenton, Virginia, the school relocated to Carlisle Barracks, Pennsylvania, in 1949 and found a more permanent home at Fort Devens, Massachusetts, in 1951. The Counter Intelligence Corps maintained an equivalent institution at Fort Holabird.

Linguists, signals intelligence personnel, and counterintelligence specialists were all needed in peacetime. However, there was no similar demand for photo interpreters and order of battle specialists. As a result, the combat intelligence specialties were allowed to atrophy. The Military Intelligence Training Center at Camp Ritchie, Maryland, which had trained combat intelligence specialists during World War II, was closed shortly after the war came to an end. The Army General School at Fort Riley, Kansas, offered some intelligence courses, but the Army Ground Forces, not the director of Intelligence, had jurisdiction over its offerings.

Lack of trained personnel, along with lack of money, meant that the TOE for a Military Intelligence Service Organization issued in 1948 could not be implemented. On paper, the Military Intelligence Service Organization was a model plan, calling for intelligence organizations made up of cellular teams tailored to meet the intelligence requirements of each level of command. The concept called for administrative, linguist, and nonlinguist teams, each made up of one officer and two enlisted personnel. A Military Intelligence Service platoon made up of appropriate teams would support each division, while MIS companies and battalions would perform similar functions at corps and army level, respectively. Overall control would be vested in a group commander at theater level. Subordinate commanders would perform administrative and housekeeping duties only.[18] However, none of the larger units envisaged by the arrangement was ever organized in peacetime. Apart from ASA units and the CIC's oversized detachments, by 1949 the only intelligence unit in the U.S. Army larger than a platoon was the Nisei-manned 319th Military Intelligence Company in Japan.

---

17 One of the first heads of the Army Language School was Brig. Gen. Elliott Thorpe, MacArthur's former counterintelligence chief.

18 TO&E 30-600, M.I.S. Organization: A Pictorial Presentation . . . (January 1952) (Fort Riley, Kans.: Army General School, 1952).

The same problems of inadequate resources also plagued the intelligence elements in the Army's reserve components. The situation here was considerably better than it had been after World War I, since there were many more intelligence-trained officer and enlisted personnel, and various types of intelligence units had been formed, including new strategic intelligence detachments and signals intelligence units. The Army's Reserve Officer Training Corps (ROTC) had also instituted programs for training both Military Intelligence and Army Security Agency officers. However, reserve unit training was weak, with equipment lacking, and the Military Intelligence Reserve's officer component was imbalanced. Of the over 10,000 Military Intelligence Reserve officers, there were too many field grade and too few company grade personnel to meet mobilization needs.

At the level of tactical collection, although technological advances afforded some improvements, this was counterbalanced by the shrinking of collection assets within the skeleton Army. Although additional aircraft were assigned to the division, and a new type of light plane, the L–19 (later the O–l "Bird-dog"), specifically designed to meet Army observation requirements, entered the inventory in 1950, there were not very many divisions left to support. Similarly, the flash- and sound-ranging capabilities of the field artillery observation battalion were now supplemented by radar, but by 1950 there was only one observation battalion left.

Finally, there were gaps in the intelligence architecture. What little electronic warfare and electronic intelligence capacity remained in the Army was controlled by the chief signal officer and operated without reference to the Army Security Agency, even though it was already all too clear that jamming would certainly have a great effect on the collection of signals intelligence in any wartime situation. Except for the attache system, the Army still lacked any dedicated capabilities for collecting human intelligence in peacetime, although Counter Intelligence Corps units overseas did provide some incidental positive intelligence. It would take the impact of another crisis to force the Army to reevaluate its intelligence structure and to make the necessary improvements. In June 1950 the crisis arrived.

Korea

The war in Korea confronted the U.S. Army with two major intelligence failures within the space of six months. The initial North Korean invasion came as a surprise, as did the later Chinese intervention. In each case Army Intelligence had been aware of hostile capabilities and had misinterpreted intentions. The reasons, apart from normal human fallibility, were unsurprising. Peacetime budgetary constraints had depleted Army Intelligence assets, and what remained had been targeted against Soviet Russia and the European threat. The Korean peninsula had been declared beyond America's defense perimeter and therefore outside the jurisdiction of the major theater commander in the Far East. The hard fact was that before June 1950 Korea was not

high on the list of intelligence priorities for either the CIA or the Army. Once the conflict began, political and diplomatic constraints limited the ability of American collection assets to provide a definite early warning of the thirty-division Chinese attack that ultimately materialized.

Army Intelligence initially responded to the outbreak of hostilities in Korea through desperate improvisation. There were only two Korean linguists on the staff of MacArthur's G–2. The Technical Intelligence Section of the Far East Command had been disbanded in 1949. The four occupation divisions in Japan had been stripped of their tactical Counter Intelligence Corps detachments, and when they deployed to Korea provisional CIC detachments had to be cobbled together from the assets of the 441st Counter Intelligence Corps Detachment in Japan. The three Army Security Agency units in the Far East were manning semifixed installations and were unable to take the field. Not until October did the first sizable ASA unit, the 60th Signal Service Company, reach the Korean peninsula, and the company had to be transported from Fort Lewis, Washington. In the meantime, the Eighth Army depended for cryptologic support upon a small unit organized by making use of locally available resources. Communications security was lax, both among Republic of Korea (ROK) troops and the Eighth Army. The Eighth Army had come from restful occupation duty in Japan, and the chief of the Army Security Agency put it, with some exaggeration, "They receive about 400 violations a minute over there."[19] Communications security was threatened further by the initially fluid tactical situation; several high-level machine cipher devices had to be destroyed to prevent their capture in the early stages of the fighting.

Chinese intervention created another set of problems. The security-conscious Chinese initially approached the battlefront completely undetected, even though MacArthur personally conducted a visual reconnaissance mission over North Korea.[20] Even after the Chinese engaged, ground patrols repeatedly lost contact with the enemy. In a desperate attempt to find out more about the Chinese advance, Korean nationals equipped with smoke grenades were air-dropped into the intelligence vacuum to signal the presence of the enemy. General Matthew Ridgway assumed command of the Eighth Army in late December 1950 at the height of the crisis. He found himself confronted with an intelligence map showing only "a big red goose egg . . . with '174,000' scrawled in the middle of it" north of his lines, all that Army Intelligence knew then

---

[19] Army Security Agency Staff Meeting Notes, 14 Nov 50, Army Cryptologic Records.

[20] D. Clayton James, *The Years of MacArthur*, vol. 3, *Triumph and Disaster, 1945–1964* (Boston: Houghton Mifflin, 1985), p. 216. Intelligence problems presented by the Chinese intervention are discussed at length (insofar as security considerations allowed) in Roy H. Appleman, *South to the Naktong, North to the Yalu, June–November 1950*, U.S. Army in the Korean War (Washington, D.C.: U.S. Army Center of Military History, 1961), pp. 757–65, 769–70. Some additional insights are contained in Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Free Press, 1990), pp. 175–82.

about the strength and disposition of the enemy. The following month, he too undertook a personal aerial reconnaissance behind enemy lines.[21]

The inadequacy of the Army's tactical intelligence capabilities on the Korean peninsula took many months to rectify. As late as 1951 a survey revealed that only 7 percent of Eighth Army personnel holding intelligence positions had either previous training or prior experience in intelligence, which spurred the creation of a Far East Command intelligence school at Camp Drake, Japan. Intelligence exploitation was handicapped also by the Army's limited supply of Mandarin linguists. Even toward the end of the war, deficiencies abounded. Ridgway's successor with the Eighth Army, General James Van Fleet, commented that there were still serious problems in aerial photography, aerial visual reconnaissance, covert collection, ground reconnaissance, and communications reconnaissance. He went on to observe: "During the two years that the U.S. Army has been fighting in Korea . . . it has become apparent that during the between-war interim we have lost, through neglect, disinterest, and possible jealousy, much of the effectiveness in intelligence work that we acquired so painfully in World War II. Today, our intelligence operations in Korea have not yet approached the standards that we reached in the final year of the last war."[22]

Nonetheless, the shock of the Korean conflict did give a new impetus to the development of Army Intelligence, causing a rapid growth both in personnel and in organizational structure. The strength of the Office of the Assistant Chief of Staff, G–2, as the Intelligence Division was called after April 1950, grew to exceed 1,000 men. The SSO system managed by G–2 was expanded to service the three corps which the United States committed to Korea. In addition, the role of the SSO became significantly enhanced. In 1949 these officers had begun to provide an "eyes only" system of private communications to commanders. After the Korean War, special security officers became deeply involved in the production of finished intelligence for the commands they supported.

Changes were not confined to the Army Staff level. The Counter Intelligence Corps more than doubled; the position of chief of the Counter Intelligence Corps was elevated to a major general's slot. The largest CIC unit, the 66th Counter Intelligence Corps Detachment that supported USAREUR, was raised to group status in 1952. At the outset of the Korean War, a counterintelligence detachment was organized to protect the Pentagon, and subse-

---

21 General Matthew B. Ridgway, *Soldier: The Memoirs of Matthew B. Ridgway*, as told to Harold H. Martin (Westport: Greenwood Press, 1974), pp. 205, 216. Another senior commander was even more personally involved in reconnaissance activities in this war. In January 1951 the Air Force chief of staff, General Hoyt S. Vandenberg (a former Army assistant chief of staff, G–2), joined a ground patrol twelve miles in front of the main U.N. lines while on an inspection trip to Korea. James F. Schnabel, *Policy and Direction: The First Year*, U.S. Army in the Korean War (Washington, D.C.: U.S. Army Center of Military History, 1990), p. 327.

22 Bidwell, History of the Military Intelligence Division, vol. 7, p. 1080.

quently was incorporated as a subelement into the newly activated 902d Counter Intelligence Corps Detachment. This unit, operating under the direct control of the assistant chief of staff, G–2, was tasked with conducting exceptionally sensitive worldwide missions in support of Department of the Army requirements. Another development in the counterintelligence field that took place during the Korean War was the creation of Technical Service Countermeasures teams to ferret out possible listening devices, an initiative prompted by the 1952 discovery that the Great Seal of the U.S. Embassy in Moscow had been "bugged" by the Soviet Intelligence Service.

In the field, large intelligence organizations were developed to meet the needs of the combat forces. The Military Intelligence Service Organization concept at last became a reality, and tactical groups, battalions, and companies of intelligence specialists were formed to support the Army around the globe. The first Military Intelligence service group, the 525th, was organized in December 1950; its commander, Col. Garland Williams, had been the first Chief of the Corps of Intelligence Police before Pearl Harbor.[23] Two additional groups were activated before the Korean War came to an end—the 500th Military Intelligence Service Group in Japan, which absorbed the personnel and mission of the old Translator and Interpreter Service, and the 513th Military Intelligence Service Group in Germany. Five Military Intelligence Service battalions were also activated, along with numerous numbered companies and platoons. Additionally, four Military Intelligence Service groups and ten Military Intelligence Service battalions, all in the 300 series, were activated in the Organized Reserve Corps, redesignated the Army Reserve in 1952.

Korea was a limited war: at first the conflict was described not as a war at all, but as a United Nations "police action."[24] This had limited the scope of certain kinds of intelligence activities. The intelligence community made no attempt to revive the World War II Counter Subversive program which had laced the Army's ranks with informers. Censorship activities were limited, and the press was allowed to operate under a "voluntary" self-censorship until the spring of 1951. The assistant chief of staff, G–2, did set up an Army Security Center in Washington, D.C., to handle high-level prisoner interrogation and document exploitation, but this turned out to be less important than its World War II predecessors, since enemy prisoners of war were retained in Korea, and few high-ranking prisoners were captured. However, some World War II precedents were found useful. In Operation INDIANHEAD, a multidiscipline intelligence task force—a World War II "T" Force in miniature—was dispatched to sift through the rubble of Pyongyang after that

---

23 During World War II, Williams had also been in charge of supply and procurement for the OSS.

24 T. R. Fehrenbach, *This Kind of War: A Study in Unpreparedness* (New York: MacMillan Co., 1963), p. 90.

North Korean capital was overrun by United Nations troops.[25] And the various collection techniques perfected in World War II proved useful in the new conflict.[26]

The Korean War revitalized the Army Security Agency, which found a new role in providing support to tactical operations. During the course of the war, the agency reorganized and redesignated its existing signal service companies as communication reconnaissance companies and activated new communication reconnaissance companies, battalions, and groups to support tactical commanders at every level.[27] The new concept placed a communication reconnaissance group in support of the field army. The group would command subordinate ASA units and had the mission of dispatching liaison teams to the combat divisions. At the corps level, flexibly organized communication reconnaissance battalions directed the activities of separate numbered companies.

By the end of the Korean War, the Army Security Agency's 501st Communication Reconnaissance Group was supervising the operations of three attached battalions and five companies in support of the Eighth Army. Another major ASA tactical element, the 502d Communication Reconnaissance Group, commanded subordinate units giving support to the expanded Army presence in Europe. The 503d Communication Reconnaissance Group served as a command and control element for various ASA units in the continental United States. Additionally, new field stations had been established in Europe and the Far East. After 1951 the position of chief of the Army Security Agency was usually filled by a major general.[28]

Finally, the Army at last took steps to enhance its human intelligence collection capabilities. Confronted by an almost complete intelligence void in the early stages of the Korean War, it expanded an existing small intelligence element set up by the Far East Command following the withdrawal of American occupation troops in 1949 into a full-fledged collection organization. Initially, a provisional

---

25 Memo, GHQ, FEC, Military Intelligence Section, 6 Feb 51, sub: After Action Report, Task Force INDIANHEAD, INSCOM History Office.

26 In *The Korean War* (New York: Simon and Shuster, 1987), p. 244, Max Hastings states that "throughout the war United Nations intelligence about Chinese and North Korean strategic intentions remained very poor." It should be pointed out, however, that not all material bearing on the subject has been released yet.

27 The buildup of the Army Security Agency that took place during the Korean War was facilitated, in part, by the deployment of the two ASA companies in the National Guard and two other ASA companies in the Organized Reserve Corps.

28 However, none of the three general officers who headed up the Army Security Agency during the period of the Korean conflict possessed any background in Military Intelligence. ASA chief Brig. Gen. William Gillmore admitted, "I have had no experience in this line of work. I am going to depend on you people for guidance and support all the way through." ASA Staff Meeting Notes, 15 Aug 50, Army Cryptologic Records. In contrast, the first three chiefs of the Army Security Agency—Brig. Gen. Preston W. Corderman, Col. Harold G. Hayes, and Brig. Gen. Carter W. Clarke—had all served in communications intelligence during World War II.

CIC unit, the 442d Counter Intelligence Corps Detachment, used tactical liaison office teams assigned to each division to dispatch locally recruited line-crossers. These generally unskilled and untrained Korean agents were told to gather whatever low-level intelligence they could.[29]

Following the Chinese intervention, this approach expanded greatly. The provisional status of the 442d Counter Intelligence Corps Detachment was dropped. The divisional teams continued to function, but, in addition, the Army undertook more ambitious collection projects. By the summer of 1951 the Army was devoting increasing resources to the effort. Since the mission was not really appropriate for the Counter Intelligence Corps, the 442d was inactivated and its functions assumed by the 8240th Army Unit, a TD-based organization with elements in both Japan and Korea. The Counter Intelligence Corps personnel initially transferred to the 8240th Army Unit were replaced gradually by specialists from other intelligence disciplines.

In late 1951 the scope of the unit's mandate widened to include special operations. This came about when the Eighth Army unit supporting Korean guerrillas on the offshore islands was integrated into the 8240th Army Unit in accordance with doctrine that such activities belonged at the theater level. At the same time, the 8240th Army Unit itself became the Army element of Combined Command Reconnaissance Activities, Korea, a theater-level joint-service agency created to coordinate intelligence and special operations activities in the war zone.

By the time the Korean armistice was signed in the summer of 1953, the 8240th Army Unit had 450 military personnel assigned and had evolved into an Army simulacrum of the World War II OSS. It not only provided the Far Eastern Command with information, but also ran a 20,000-man private army of Korean guerrillas, the United Nations Partisan Forces in Korea. With five infantry and one airborne regiment, the Partisan Forces harassed the enemy from bases on islands off the shores of both coasts of the Korean peninsula. As if all this were not enough, the 8240th also engaged in an extensive program of "black propaganda."[30]

Summation

The Korean War was another major milestone in the development of Army Intelligence. It revived intelligence capabilities which had grown moribund in the post–World War II retrenchment. It also witnessed the development of large-scale intelligence formations in the field. For the first time, Army Intelligence personnel were organized into groups and battalions. However,

---

[29] S. L. A. Marshall mentions such collection activities in his book, *The River and the Gauntlet: Defeat of the Eighth Army by the Chinese Communist Forces, November 1950, in the Battle of the Chonchon River, Korea* (New York: Morrow, 1953), pp. 3–4.

[30] Alfred H. Paddock, Jr., *U.S. Army Special Warfare: Its Origins* (Washington, D.C.: National Defense University Press, 1982), pp. 100–108.

although the Army Security Agency imposed these arrangements on its reserve components in the aftermath of the war, the Army decided that large reserve units were not needed in the other intelligence disciplines, and by mid-1953 all the Military Intelligence Service groups and battalions in the Army Reserve had been inactivated.[31] For the next few years, the Military Intelligence presence in the Army Reserve would be confined largely to numerous small counterintelligence, censorship, or strategic research and analysis detachments.

In addition, the war can be seen as a milestone in the development of intelligence technologies. The war itself was fought mostly with World War II equipment. The venerable M209 still provided communications security for tactical units. The light planes organic to the divisions were only slightly improved versions of the Piper Cubs that had given the Army reconnaissance support in the previous conflict. ASA's radios as well as its trucks represented war surplus. Yet this was beginning to change. A new family of cipher machines began to enter the Army inventory at this time. Scientists started to find ways in which new and evolving technologies could be applied to the Military Intelligence field. In 1953 the Army became involved in Project MICHIGAN, a research and development effort in which civilian scientific personnel explored the possibilities of using various types of manned aircraft, drones, balloons, and missiles carrying television and other sensors to allow surveillance and target location up to 200 miles behind enemy lines.[32] The new technologies under development would have profound consequences for the structure of Army Intelligence in the years that followed.

---

[31] For reasons which have escaped documentation, all reserve component ASA units after the Korean War were in the Army Reserve, not the National Guard.

[32] Bidwell, History of the Military Intelligence Division, vol. 7, pp. 1102–03.

8

From Korea to Vietnam

During the twelve years that elapsed between the signing of the Korean armistice in 1953 and the first commitment of American combat troops to defend South Vietnam in 1965, the Army was affected by the fluctuations of U.S. national security policies and defense management structures. Responding to American dissatisfaction with the bloody and ultimately indecisive fighting in Korea, the Eisenhower administration that took office in 1953 adopted a "New Look" in defense policies. America, it declared, would no longer be bogged down in ground warfare at a time and place of the adversary's choosing. Instead, the United States would meet aggression with the "massive retaliation" of strategic atomic weapons.

This policy called for a reduction of land forces. The Army was drastically retrenched. Policy makers' belief that increasingly available tactical nuclear weapons would be decisive in any future conflict led to the revamping of the basic force structure in 1957. New "pentomic" divisions supposedly capable of operating in a nuclear environment were organized, and the Army regiment was abolished as a tactical entity in favor of smaller and more flexible battle groups. However, massive retaliation was never invoked. The Soviet threat continued after the death of Stalin, but its initiatives evolved in ways that could not be countered suitably by American preponderance in the nuclear weapons arena. The French defeat at Dien Bien Phu in 1954 led to the creation of a new Communist state in North Vietnam. Soviet power, hitherto confined to the Eurasian land mass, catapulted across the oceans. Soviet arms and influence appeared in Egypt, and a pro-Communist regime came to power in Cuba. Simultaneously, the Soviets startled the Americans with their success in the area of guided missiles; "Sputnik," the first orbiting satellite, was launched in 1957.

Taking advantage of a belief that the United States was not coping adequately with these new Soviet challenges, Democratic presidential candidate John F. Kennedy's campaign of 1960 focused on the need to meet the broad Communist challenge. Upon election, Kennedy and his secretary of defense, Robert S. McNamara, scrapped the strategy of massive retaliation in favor of a new doc-

trine, "flexible response," in which America would meet any military challenges with the gradually increasing employment of deterrent force.[1] Coupled with a fresh crisis regarding the status of Berlin, the new emphasis on conventional forces powered the expansion of the Army, which soon rose to a strength of 1.2 million. New Army leaders found the pentomic division organization unsatisfactory for protracted fighting in a nonnuclear environment, and introduced a new divisional structure, the so-called Reorganization Objective Army Division (ROAD). Finally, McNamara's zeal for cost effectiveness led to a substantial restructuring of the whole Defense Department and of the individual services. As usual, Army Intelligence was affected by the currents of the times.

Military Intelligence at the Center: The 1950s

At the Army General Staff level, intelligence benefited from an expansion of its sources and technological capabilities during the post–Korean War era. Previously, the foreign intelligence collection resources of the Army Intelligence staff during peacetime had been confined to overt human intelligence provided by the attache system and signals intelligence collection. Now the Army augmented these sources with other types of intelligence collection. Its capabilities for collecting both human and electronic intelligence became increasingly significant. In addition, photographic intelligence became a viable peacetime source for the first time. After 1956 imagery from national-level sources became available to the Army. To take better advantage of this, the Army's existing Photo Interpretation Center at Fort Holabird established a special exploitation unit in the Washington, D.C., area.

Other developments at the Army Staff level under the Eisenhower administration were also significant. On the domestic front, the assistant chief of staff, G–2, regained control of the Industrial Security Program from the Provost Marshal General's Office in 1953, a reorganization that gave it custody of the extensive investigative data base compiled on Army contractor employees. Exploitation of growing masses of intelligence data was enhanced also by G–2's use of automatic data processing techniques. In 1957 the Radio Corporation of America began work on Project ACSI-MATIC, an intelligence data system that became operational in 1960.

However, intelligence was still something of a second-class citizen in the Army. In 1955 the Army's deputy assistant chief of staff, G–2, confessed that he viewed his appointment "almost as the kiss of death."[2] And in two important respects, the Army Intelligence staff lost ground during the Eisenhower years—

[1] A useful overview of defense and intelligence-related developments during the Eisenhower and Kennedy administrations can be found in Alan R. Millett and Peter Maslowski, *For the Common Defense; A Military History of the United States of America* (New York: Free Press, 1984), pp. 508–41.

[2] Ransom, *The Intelligence Establishment*, p. 116

it declined both in status and in budget. In 1955 the assistant chief of staff, G–2, lost command of the Army Security Agency. In 1956, during the course of another Army-wide reorganization, his office lost both its name and its equality with other major staff elements. Under the terms of the reorganization, the three other principal staff functions—personnel, operations, and supply—were assigned to deputy chiefs of staff. But Army Intelligence, now headed by the assistant chief of staff for intelligence (ACSI), remained at the assistant chief level.[3] The implicit downgrade preceded budget cuts and pressure on the Office of the Assistant Chief of Staff for Intelligence (OACSI) to move operational personnel out of its official table of distribution and to reduce personnel occupying headquarters slots. Ever since the late 1940s the intelligence section of the General Staff had maintained smaller operating elements in the field. After 1956, however, ACSI was forced to shift as many operational functions as possible from headquarters to field agencies.

The first step in this process began in 1956, when the ACSI staff element assigned to manage the industrial security program was reorganized as the Industrial and Personnel Security Group and transferred to Fort Holabird. In 1960 the new Technical Intelligence Field Agency assumed the mission and functions of ACSI's technical intelligence branch. The agency soon moved to Arlington Hall Station, where it was collocated with the intelligence elements of five of the seven Army technical services. Similarly, the OACSI component of the National Indications Center, a joint-service element designed to provide warnings of impending hostile attack, became a separate field detachment, as did the topographic collectors incorporated into the U.S. Army Geographic Specialist Detachment in early 1961.

Pressures on the existing structure of the Army's Intelligence staff came from outside as well as from within the Army. In 1958 the Department of Defense was reorganized. The old organizational concept, under which one service had served as executive agent for the Joint Chiefs of Staff (JCS) in war (as the Army had done in the Korean conflict) was abolished, and the armed forces of the country were placed in a system of unified and specified commands under JCS control.[4] The U.S. Communications Intelligence Board and the Intelligence Advisory Committee were concurrently abolished and their consolidated functions transferred to the new U.S. Intelligence Board (USIB). This reorganization reduced the role of the individual services to procuring, training, and fielding forces that would then pass under a JCS-directed command structure. Although the new arrangement did not immediately affect the Army's departmental intelligence agency, its implications for the future of Army Intelligence would soon become apparent.

---

[3] Hewes, *From Root to McNamara*, p. 239.
[4] Ibid., pp. 297–98.

Reshaping the Tools

One of the most significant developments within Army Intelligence during the 1950s was the conversion and expansion of the existing Counter Intelligence Corps Center at Fort Holabird into an Army Intelligence Center. This came about as an indirect byproduct of two separate initiatives. One of them was a movement begun during the Korean War to make intelligence more professional. Knowledgeable intelligence officers had become concerned about the difficulties of retaining a cadre of trained intelligence personnel in peacetime. Intelligence was not a basic branch of the Army, and most intelligence officers were reservists on detail. In 1950 a legislative oversight had even temporarily eliminated the Military Intelligence Reserve first created in 1921. This had been corrected in 1952 with the creation of two separate reserve branches, Military Intelligence (redesignated Army Intelligence in 1958) and Army Security. But since only reserve component officers could be commissioned in these branches, the active Army lacked any focus for intelligence career professionals.

The massive opposition of Army traditionalists to the establishment of an Intelligence Branch in the Regular Army led the assistant chief of staff, G–2, to advocate a more modest reform. In early 1952 he put forward a proposal to create the new Corps of Reconnaissance, U.S. Army. This corps would have incorporated all intelligence assets at the division level and above, including the units of the Army Security Agency. The plan would have provided Army Intelligence with a centralized institutional framework, but still would have allowed commanders their traditional prerogative of selecting their own intelligence staffs regardless of the branch to which they belonged. Even though this concept posed less threat to vested interests than a new separate branch, it never won acceptance.

As a fallback position, in June 1953 the assistant chief of staff, G–2, came up with a new program. He recommended that an intelligence board be established and collocated with a single intelligence school, a field intelligence center, and the intelligence units in the Army's central reserve in the continental United States. Fort Holabird, with its existing Counter Intelligence Corps School and Center and its counterintelligence records facility, would be the most logical site for the new arrangement.

The second factor leading to the expansion of Holabird's role was the Army's decision to make its collection of human intelligence more professional. The experience of the Korean War, when the Army had to improvise a collection apparatus, had caused the Army see that such work was a permanent peacetime requirement. At the end of 1952 General Matthew Ridgway, then Supreme Allied Commander, Europe, specially recommended that the Army organize its own institutionalized human intelligence collection element. Such a force would meet Army needs and at the same time prevent any future diversion of Counter Intelligence Corps assets from their assigned functions. Ridgway's recommendations were accepted and endorsed by the chief of staff in early 1953. In

November 1953 the Army issued a regulation that set standards for procurement of personnel to carry out this new function.

These twin developments resulted in a steady expansion of the scope and nature of the responsibilities assigned to the chief, Counter Intelligence Corps. In April 1954 the Department of Field Operations Intelligence was added to the existing training facility at Fort Holabird. As a result, collection personnel began to train side by side with CIC agents. This was just the beginning of a snowballing accretion of new activities that fell under the control of the CIC chief. In August 1954 he assumed command of the former G–2 Records Facility at Holabird, which contained the Army's counterintelligence files. At this point, the Counter Intelligence Corps Center was redesignated the Army Intelligence Center, and the chief, Counter Intelligence Corps, assumed a new title as the center's commanding general. In March 1955 an Army Photo Interpretation Center was established at Fort Holabird. Finally, during the same month, responsibility for conducting training in combat intelligence transferred from the Army General School at Fort Riley to the new U.S. Army Intelligence Center and School at Holabird.[5] The arrangement centralized almost all intelligence training at one post. Only the G–2's Strategic Intelligence School in Washington, D.C., and the Army Security Agency facility at Fort Devens, Massachusetts, remained outside the complex.

In practice, the original concept of an all-embracing Army Intelligence center was never quite realized. It seems to have been the intention of Maj. Gen. Arthur C. Trudeau, the assistant chief of staff, G–2, that Holabird would become the directing hub for Army Intelligence. Under the original plan, the chief, Counter Intelligence Corps, in his capacity as commanding general of the U.S. Army Intelligence Center, would not only assume responsibility for training all Army Intelligence personnel, but would also take over responsibility for their administrative supervision. This arrangement would have extended the benefits of the CIC personnel structure to the rest of the Army Intelligence community. Although the concept was approved by the Army chief of staff, it was not completely implemented, and the center never achieved the position of importance originally envisioned for it. However, it did serve as a basis for more modest reforms and initiatives.

The year 1955 also witnessed the inception of an intelligence civilian career program within the Army. This step, first advocated by the second Hoover Commission on governmental reform, would augment nontactical Military Intelligence units with trained civilian specialists who would provide continuity to operations. Three hundred such positions were authorized originally. Actual implementation began in 1957, overseen by an Administrative Survey Detachment organized within the Army Intelligence Center. However, the Army soon began to have second thoughts about the program. Civilians were limited

[5] General Order (GO) 20, Headquarters, Department of the Army (HQDA), 11 Mar 55.

to working a forty-hour week and were not under court-martial jurisdiction. Moreover, Army leaders believed it was counterproductive to keep civilians on indefinite assignments in any one single geographic area. As a result, they limited the effort to employ more civilians.

Meanwhile, the Army Intelligence Center became involved in an attempt to remedy some of the perceived deficiencies in field intelligence programs. Initially, the commanding general, Army Intelligence Center, was responsible for training new field operations intelligence specialists, but had no authority over their assignments in the field. Some human intelligence collectors were in units under theater control, organized years before the field operations intelligence program, as such, had come into existence; others served in a detachment under direct ACSI control. The field operations intelligence program thus operated under a separate and less rigid personnel system than the Counter Intelligence Corps. Its military occupational specialty (MOS) could be awarded by ACSI and by theater commanders as well as by the Army Intelligence Center, and the Army could recruit individuals whose foreign connections would have barred them from enlisting in the Counter Intelligence Corps.

The differences between these two intelligence elements soon led to an unhealthy rivalry. As one report pointed out, "there is too much bickering and snideness at the [Intelligence] Center regarding these two fields."[6] The situation was made worse by the fact that intelligence officers on the Army Staff and in Europe considered field operations intelligence personnel better qualified to handle especially sensitive counterespionage operations than CIC agents. But Counter Intelligence Corps members saw any such transfer of functions as "an emasculation of CIC."[7] Another problem area arose when field operations intelligence personnel, because of the nature of their mission requirements, lacked an adequate rotation base in the continental United States. Although a majority of CIC billets were in the United States, four-fifths of those billets in the field operations intelligence program were overseas.

Eventually, the ACSI decided that it would be more economical and efficient to merge all field operations intelligence assets with the Counter Intelligence Corps and cross-train personnel to serve both as counterintelligence agents and as human intelligence collectors. Accordingly, a consolidated Intelligence Corps, commanded by the former CIC chief and operating under tight centralized control, was created on 1 January 1961. The new organization incorporated slightly over 5,000 personnel, about 85 percent of whom came from CIC. Entrance requirements for the Intelligence Corps were less restrictive than they had been for the old Counter Intelligence Corps.

---

[6] Memo, Maj C. A. Lynch for G–3, U.S. Army Intelligence Command (USAINTC), 11 Nov 58, sub: Proposed Advisory Committee for USAINTC, RG 319, NARA.

[7] Memo for Commanding General, 10 Dec 58, sub: Long Range Policy and Planning Committee for USAINTC, RG 319, NARA.

Attempts to bring the new organization even closer to the Army mainstream soon followed. During the 1950s the Counter Intelligence Corps had embodied the "best and the brightest." Ever since the Korean War, the draft had furnished it with a steady stream of college-trained applicants attracted to the idea of fulfilling their service obligation by working in civilian clothes in a glamorous and exotic field, and the CIC had been able to choose among them. Unfortunately, most of these individuals did not show any propensity for making intelligence work a career. The retention rate was abysmal—7 percent for lieutenants and just 3 percent for enlisted personnel. Accordingly, the Army decided that "selection of applicants must be made with consideration for those offering the best career potential and not necessarily the bright college student."[8] The Intelligence Corps would accept only applicants who volunteered for a three-year enlistment. At the same time, the age limit for enlisting in the corps was lowered and brought into line with the rest of the Army; eighteen-year-old personnel now became eligible for entry-level positions involving clerical rather than investigative duties. Finally, in 1965 the minimum Army General Test score for joining the Intelligence Corps was lowered from 110, the same requirement imposed on officer candidates Army-wide, to 100, which more closely approximated the Army average.

The Army Security Agency

If Fort Holabird was one pole of Army Intelligence in the 1950s, Arlington Hall Station was the other. Arlington Hall continued to serve as headquarters for the ASA, the largest single intelligence and security element in the Army, and it also came to house intelligence elements of five of the Army's technical services after the consolidation of NSA headquarters at Fort Meade in 1957 made office space available. During the Eisenhower administration, Arlington Hall's main Army tenant, the Army Security Agency, grew steadily. Personnel strength rose from 11,500 in 1952 to 18,300 by 1957; new field stations and tactical units appeared; and a substantial restructuring of the agency's mission took place.

By 1954 the Army Signal Corps was fielding a number of units to collect electronic intelligence and continued to be responsible for the conduct of electronic warfare. In April 1954 the Department of the Army analyzed the feasibility of combining all these capabilities into a single agency. As a result of this study, the Army Security Agency took over responsibility for electronic intelligence and communications-related electronic countermeasures (ECM) from the Signal Corps in 1955, assuming control of a number of dispersed units and a battalion and four companies stationed at Fort Huachuca, Arizona. In return, the agency surrendered its responsibilities for Army cryptologistics and cryptomaintenance, along with associated personnel, to the Signal Corps.

---

[8] Min, Intelligence Corps Commanders' Conference, 1961, sec. 10, p. 7, RG 319, NARA.

In budgetary terms, the reorganization was significant: the Army was introducing a new generation of machine cipher devices to replace the venerable M209, and purchase of the new machines had consumed 60 percent of the Army Security Agency's fiscal year 1953 budget. However, the change had the important benefits of eliminating duplication of facilities and allowing for proper integration of signals intelligence with electronic intelligence. The term signals intelligence (SIGINT) was now redefined and used to refer to both of these functions. Actual implementation of this mission transfer was delayed for a short time until the Signal Corps personnel transferred to the Army Security Agency had their clearance levels upgraded.

The new arrangements meant that the Army Security Agency was no longer exclusively an intelligence organization. By acquiring responsibility for electronic warfare, the agency now managed a weapons system, even though the weapon was invisible. In recognition of this change, the Army Security Agency became a Department of the Army field operating agency on 23 June 1955.[9] It now reported directly to the Army chief of staff, not to the assistant chief of staff, G–2. However, the agency continued to focus primarily on the cryptologic mission, and electronic warfare in practice did not receive much emphasis.

Having acquired responsibility for electronic intelligence and electronic warfare, the Army Security Agency made further attempts to enlarge the scope of its mission. In September 1955 the chief, Army Security Agency, recommended to the Army chief of staff that his organization be given the responsibility for dissemination and protection of sensitive compartmented information Army-wide, thus eliminating the special security officer system maintained by the assistant chief of staff, G–2, which had just been consolidated into a single element, Detachment M. The rationale for this proposal was economy. However, both the Army's Intelligence staff and commanders in the field vigorously resisted it. Intelligence personnel claimed that the Army Security Agency was not qualified to produce the all-source intelligence which special security officers provided to their supported G–2s. Field commanders unanimously endorsed the existing arrangement, pointing out that ASA units were not conveniently located in or near the major Army headquarters and that eliminating the special security officers would deprive them of their secure "back-channel" communications. The Army chief of staff tabled the proposal, but the Army Security Agency refused to drop the issue. The bureaucratic struggle over the matter would go on for the next two decades, at times fought with considerable acrimony.

The Army Security Agency pursued other initiatives with greater success. In 1956 the agency became aware for the first time of the possibility that emissions radiating from electronic data processing equipment might compromise security and initiated a program, nicknamed TEMPEST, to counter the threat. In 1957 the U.S. Army Security Agency Board was created to provide long-range planning,

[9] AR 10–122, *Organization and Functions, Army Security Agency*, 23 Jun 55.

and in 1960 its functions were expanded to include combat development. At the same time, the Army Intelligence Board at Fort Holabird acquired parallel responsibilities for overseeing combat developments in the field of human intelligence. Meanwhile, the ASA and its field stations underwent redesignation. As a result of an Army-wide change, the agency became the U.S. Army Security Agency (USASA) on 1 January 1957. Concurrently, its fixed field stations, which previously had been known as numbered Army administrative units in the 8600 series, acquired new designations as numbered USASA field stations.[10]

The agency's tactical elements underwent a more significant restructuring during this period. During the Korean War, the Army Security Agency had operated with flexible battalion headquarters overseeing the operations of independent security and collection companies. In 1955 fixed battalions with organic companies combining both functions were created, and in 1956 all communication reconnaissance units were redesignated as Army Security Agency units. However, in 1957 the secretary of defense's decision to cut the Army's strength by a total of 50,000 threw the force structure of the agency into disarray. The decrement left the ASA without sufficient personnel to fill its existing tactical TOE units, which at the time accounted for about a quarter of its total strength. In response, the Army Security Agency inactivated all its TOE units and replaced them with mission-tailored units based on individual tables of distribution. The new TD units included the 507th and 508th U.S. Army Security Agency Groups, located respectively in Germany and Korea, and six U.S. Army Security Agency battalions numbered from 316 to 321. These units were given the designator U.S. Army Security Agency to distinguish them from Army Security Agency TOE units. The battalions retained the fixed structure of their TOE predecessors.

Originally, the Army intended this as a temporary measure, to remain in force only until new organizational tables could be drawn up. In practice, however, the ASA continued to operate exclusively with TD units until 1962, when tactical TOE units were formed in the continental United States to support the Army's new strategic reserve for contingency operations. Later, additional TOE elements were activated to serve in Vietnam. Some of the mission-tailored TD units soon acquired new and exotic designations as special operations units and special operations commands.

The U.S. Army Security Agency was the principal tenant at Arlington Hall after 1957, but not the only one. Intelligence elements of five technical services ultimately located there. Only the Corps of Engineers, the intelligence arm of which was concentrated in the Army Map Service, and the Quartermaster Corps held back, although the Ordnance Corps also maintained a separate missile intelligence center at Redstone Arsenal. Although most of these technical service intelligence units engaged in analysis and production, the Signal Corps contin-

---

10 GO 58, *Army Security Agency*, 13 Dec 56.

ued to engage in some specialized collection activities even after it had surrendered its electronic intelligence and communications-related electronic warfare functions to the Army Security Agency.

Military Intelligence in the Field

Until the late 1950s the tactical formations of the Army received their intelligence support from Military Intelligence specialist units put together on the cellular principle. Combat intelligence units were organically separate from counterintelligence units under this arrangement, and the G–2s of the supported units had to coordinate the efforts of the two diverse elements themselves.

At the end of 1957 the Army introduced a new category of intelligence units organized under a concept plan entitled the Military Intelligence Organization. Under this plan interrogators, photo interpreters, order of battle specialists, and other combat intelligence personnel were integrated into single units with counterintelligence and collection elements. These new units operated under a fixed table of organization and were designed to be administratively self-sufficient.

Under the Military Intelligence Organization concept, the basic building block was the Military Intelligence battalion supporting a field army. This unit had its own specialized organic companies: a headquarters and headquarters company containing photo interpreters, order of battle and technical intelligence specialists, and censorship personnel; and lettered linguist, security, and collection companies. In addition, the battalion furnished tactical units down to the division level with attached multidiscipline intelligence detachments.[11] The creation of the Military Intelligence Organization was one of the first steps in bringing truly multidiscipline intelligence support to the field. Only ASA units remained outside the new organizational structure because of the Army Security Agency's vertical, or "stovepipe," command structure and its tight centralization and compartmentation.

In practice, implementation of the new force structure was limited. Under the Military Intelligence Organization concept, four Military Intelligence Battalions eventually were reorganized: the 319th and 519th in the continental United States; the 532d in Germany; and the 502d in Korea. However, only the headquarters and headquarters companies and linguist companies were initially activated in the two battalions in the United States.[12] Meanwhile, the bulk of Army

---

[11] A major factor behind the Military Intelligence Organization concept was the belief that under the new arrangement, "personnel losses resulting from decentralized administration or misassignment are less likely to occur." Folder, Military Intelligence Support in the Field Army, 1960, Background of MI Branch/Corps file, INSCOM History Office, Fort Belvoir, Va. A more detailed description of the organization can be found in Irving Heymont, *Combat Intelligence in Modern Warfare* (Harrisburg: Stackpole Co., 1960), pp. 124–29.

[12] The 519th Military Intelligence Battalion eventually received active Companies B and C in 1962.

counterintelligence and field operations intelligence personnel continued to serve in single-discipline cellular units supporting the theaters and the Zone of Interior armies until 1961, when consolidated Intelligence Corps groups and detachments were formed.

Not all intelligence disciplines were well served by this new arrangement. In the continental United States, linguists had to be concentrated at battalion level, rather than spread among the detachments that were attached to divisions and other tactical units, as the Military Intelligence Organization concept dictated. Each detachment might be involved in several contingency plans, and each plan often required expertise in a different language. There was simply no way to assign the appropriate linguists to a Military Intelligence detachment until actual implementation of a specific plan or major field exercise began.

Photo interpreters also fit rather uneasily into the new structure. At the tactical level such personnel lacked access to the imagery that national-level reconnaissance elements began to generate in the late 1950s, and thus felt that their skills were not being adequately used. Units based in the United States had no operational mission, and photo interpreters found themselves all too often assigned to housekeeping and administrative positions unrelated to their specialty. Detailed to kitchen police and other "rock-painting" chores, many felt slighted and complained of "harassment."[13]

To remedy the situation, in 1963 the Army Intelligence Center proposed that all photo interpreters in the United States be placed under centralized control in the same fashion as the Army's linguists. They could find more useful employment either at the Army Photo Interpretation Center or with the Army's lone specialized tactical photo unit in the United States. However, field commanders strongly resisted the proposal on the grounds that stripping Military Intelligence detachments of their photo interpreters would deprive G–2s of access to this intelligence field and would result in equipment maintenance problems. The status quo thus continued.

Finally, the Army continued to neglect tactical-level technical intelligence. There were no provisions for a technical intelligence company in the initial TOEs for the Military Intelligence battalion (field army), and it would take ten years for the Army to remedy this discrepancy. By that time, the Vietnam conflict would be in full swing, creating an insatiable demand for personnel resources, and only one field army–level battalion would ever receive its technical intelligence company.

At the tactical level, intelligence organization was also influenced by the Army's increasing reliance on aircraft. By 1960 there were 5,000 aircraft in the Army inventory. Many of them were helicopters, items that had first seen extensive use in medical evacuation during the Korean War. It soon became apparent

---

[13] Memo, 8 Feb 63, sub: Centralization of Image Interpreters under USAPIC, RG 319, NARA.

that improved versions of rotary-wing aircraft could serve as useful reconnaissance assets. During the course of the 1950s the Korean-vintage L–19 that had served as the all-purpose workhorse within the division was phased out in favor of the helicopter, and aircraft within the division were concentrated in larger formations. Under the structure of the pentomic division fielded in 1957, Army aviation within the divisions was consolidated into company-size units. The ROAD division of 1962 included a complete aviation battalion, one company of which was equipped with scout helicopters. In addition, observation helicopters were assigned to divisional artillery, and a helicopter-borne aerial cavalry troop formed part of the divisional reconnaissance battalion.[14]

Along with its helicopters, the Army also developed more sophisticated fixed-wing aircraft for reconnaissance. In 1962 it acquired the AO–1 Mohawk. This twin-engine craft came in three configurations: one equipped with a high-performance camera; one with newly developed infrared night vision equipment; and the third with the equally new side-looking airborne radar device. Mohawks were employed both in divisional aerial surveillance and targeting platoons, as well as in aerial surveillance companies that operated at corps level.[15]

In addition to developing its own aerial assets, the Army took steps to improve its interaction with Air Force tactical reconnaissance. To better exploit aerial photography produced by Air Force reconnaissance squadrons, the Army fielded the 1st Air Reconnaissance Support Battalion in 1959. The unit consisted of a headquarters and headquarters detachment, a signal air photo reproduction and delivery company, and a photo interpretation company. A similar unit, the 24th Air Reconnaissance Support Battalion, was activated in the Army Reserve the same year, thus becoming the first non-ASA intelligence battalion active in the reserve components since the Korean War. In 1961 the Army activated another Regular Army air reconnaissance support battalion to support the Seventh Army in Germany, and in 1962 these units were reorganized and redesignated as Military Intelligence battalions (air reconnaissance support), or "Mibars." Two years later it devised a new TOE for this type of unit that provided for a headquarters and headquarters company and four lettered imagery interpretation detachments.[16] The diverse nature of the products which photo interpreters now had to manage—infrared and radar imagery, as well as conventional photography—led to the Army's redesignating photographic intelligence as imagery intelligence in 1964.

There were also new developments in the Army's arrangements for ground reconnaissance. From 1957 on, each combat division had its own reconnaissance battalion. The successive restructurings of the division in 1957 and 1962

---

[14] John J. Tolson, *Airmobility, 1961–1971*, Vietnam Studies (Washington, D.C.: Department of the Army, 1973), p. 10.

[15] Ibid., p. 12.

[16] 373 Card, 1st Military Intelligence Bn, Unit Data Branch, U.S. Army Center of Military History.

meant that reconnaissance assets previously held at the regimental level were moved down, first to battle group, and then to battalion. An armored cavalry platoon and a ground surveillance section equipped with mobile radar sets became part of the headquarters company of each infantry battalion.

Intelligence Support to the Theaters

By the late 1950s the deployment of the Army overseas had become fixed in a pattern that would remain largely unchanged for the duration of the Cold War.[17] The completion of the European buildup, the drawdown of forces in Korea, and the signing of a peace treaty with Japan resulted in a force structure that gave the Army five divisions in Europe and two in Korea, commanded respectively by the Seventh and Eighth Armies. The diversity of the theaters, the disparate numbers of the supported forces in each one, and the differing nature of intelligence requirements in Europe and in the Pacific dictated that arrangements for intelligence support would not be uniform. Moreover, even if the positioning of troops on the ground remained relatively static, theater command relationships did not, and these shifts also impacted on the theater intelligence structure.

In Europe a continuing flood of refugees from behind the Iron Curtain provided American forces with ample opportunities for intelligence exploitation. From 1951 to 1962 collection of intelligence from border crossers was carried out by the Seventh Army's 532d Military Intelligence Battalion, a field-army type of unit organized under the Military Intelligence Organization concept and headquartered in Stuttgart-Vaihingen, Federal Republic of Germany. During an average year, the battalion screened between 20,000 and 30,000 refugees.

At the theater level, counterintelligence support for U.S. Army, Europe (USAREUR), was provided by the 66th Counter Intelligence Corps Group. This unit, with headquarters in Stuttgart, provided counterintelligence coverage through a network of regional and field offices that not only extended over West Germany but also reached occupied Berlin and the USAREUR Communications Zone in France. The 513th Military Intelligence Service Group, activated at Oberursel, Federal Republic of Germany, in 1953 to take over operations previously performed by the 7077th USAREUR Intelligence Center, soon was redesignated the 513th Military Intelligence Group and then expanded its scope of activities to include active collection. With the inception of an Army civilian intelligence career program in the 1950s, both units received large TD augmentations of civilian specialists.

In 1959 USAREUR experimented with organizing intelligence work on an area rather than on a functional basis. Consequently the 513th Military

---

[17] Strategist Edward M. Luttwalk noted in 1984, "Our deployment overseas resembles geological layers, each the enduring residue of some past crisis or war, now hardened into a 'commitment.'" *The Pentagon and the Art of War* (New York: Simon and Shuster, 1984), p. 73.

Intelligence Group was given northern Germany as its area of responsibility, and the 66th Counter Intelligence Corps Group (later successively redesignated as the 66th Military Intelligence Group and the 66th Intelligence Corps Group) was allotted the south, where the preponderance of American forces was stationed. This arrangement caused more problems than solutions and was later abandoned.

Meanwhile, opportunities for exploitation of sources began to diminish. In 1961 the construction of the Berlin Wall and the simultaneous imposition of tighter border controls by East Germany effectively shut off the refugee flow. This development reduced the need to have three large intelligence units with partially overlapping responsibilities in Europe. As a result, in 1962 there was a major realignment of intelligence resources. The 513th Intelligence Corps Group, as it was now designated, assumed complete responsibility for active intelligence and certain sensitive counterespionage missions for USAREUR, while the 66th Intelligence Corps Group was reassigned to Seventh Army and assumed the mission of the inactivated 532d Military Intelligence Battalion. During this process, the group lost its regional form of organization and emerged as the command headquarters for various numbered Army Intelligence units, including the tactical intelligence elements attached to the Seventh Army's corps and divisions.[18]

Cryptologic support in the theater was provided by an entirely separate organizational structure, in conformity with Army practice. The U.S. Army Security Agency maintained a theater headquarters in Frankfurt that exercised command and control over various field stations in Europe and over a group headquarters with three subordinate battalions and some other units operating in support of the Seventh Army.

In the Pacific, following the conclusion of the armistice in Korea, the Army broke up its elaborate intelligence and special operations organization, the 8240th Army Unit. Under conditions of relative peace, the Korean partisan forces it had mustered were transferred to the control of the South Korean government, the least productive of its operations terminated, and its mission restricted to intelligence collection. The unit's Korean-based element, the Army Collection Detachment, continued to report to a theater-level Army command reconnaissance activity until 1961, when a number of Army Intelligence assets in Korea combined to form the 502d Military Intelligence Battalion. The other elements used to form the battalion came from the 308th Counter Intelligence Corps Detachment and the Eighth Army's 528th Military Intelligence Company, which were concurrently inactivated.

At the theater level, U.S. Army Forces, Far East (USAFFE), served as the Army's principal headquarters element in the Pacific until 1957. It was supported

[18] It should be pointed out that in addition to the units which supported USAREUR and Seventh Army during this period, the 450th Counter Intelligence Corps Detachment provided security to Supreme Headquarters, Allied Powers in Europe, from 1951 on. The unit was redesignated the 650th Military Intelligence Detachment in 1966 and upgraded to group status in 1970.

by an elaborate intelligence architecture directed by the USAFFE G–2 in Tokyo, Japan. The organization's principal human intelligence collection arm was the U.S. Army Command Reconnaissance Activity, Far East. The other major field elements were the 500th Military Intelligence Group, an interpreter unit, and the 441st Counter Intelligence Corps Group. These three units reported to the U.S. Army Intelligence Support Center, Japan, under command of a brigadier general.

The Eisenhower-Kishii agreement of 1957 led to a drawdown of American troop strength from Japan and relocation of the Army's main Pacific headquarters from Tokyo to Hawaii. The discontinuance of USAFFE and the establishment of United States Army, Pacific (USARPAC), led to a rapid decrement in Japan-based Military Intelligence assets. The 500th Military Intelligence Group was inactivated, the Intelligence Support Center discontinued, and the functions of both organizations absorbed by the successor of the U.S. Army Command Reconnaissance Activity, Far East, the U.S. Army Command Reconnaissance Activity, Pacific. Following the departure of most American troops from Japan in 1959, the 441st Counter Intelligence Corps Detachment, as it was now known, was in turn inactivated. In 1961 the U.S. Army Command Reconnaissance Activity, Pacific, was discontinued and the 500th Military Intelligence Group once more reactivated to carry out all aspects of the human intelligence mission. This group redeployed to Hawaii in 1965, a move dictated by the U.S. government's attempts at that time to reduce the outflow of gold reserves overseas.

U.S. Army Security Agency operations in the Far East were under the direction of a regional headquarters located in Tokyo until 1958. This was consolidated briefly with ASA headquarters elements in Hawaii from 1958 to 1960 to become the U.S. Army Security Agency, Pacific. In 1960 it returned to Tokyo, where it remained until it again relocated to Hawaii in 1965. The withdrawal of the agency's Pacific headquarters back to American soil also came about because of the government's concern over the balance of payments.

After 1957 the Eighth Army in Korea received its cryptologic support from the 508th U.S. Army Security Group (a TD unit) and the 321st U.S. Army Security Agency Battalion, another TD unit. The battalion was discontinued in 1964—another casualty of the government's worries about the gold flow.

One unique feature of the Pacific theater was the existence of the U.S. Army Intelligence School, Pacific. Unlike other Army Intelligence training facilities overseas, the Pacific intelligence school, set up on Okinawa in 1958, trained foreigners, not Americans. The students from seven different countries bordering the Pacific basin took courses in combat intelligence and counterintelligence techniques until the reversion of Okinawa to Japanese sovereignty brought operations to a halt in 1975.[19]

---

[19] History of the U.S. Army Intelligence School Pacific, U.S. Army Intelligence School Pacific, 1971, copy in INSCOM History Office files.

The McNamara Revolution

The outcome of the presidential election of 1960 led to major changes in the structure of the Army and the Army's intelligence components. President John F. Kennedy rejected the strategic assumptions of the previous administration, believing that any military challenge had to be met through graduated deterrence. This approach placed a new emphasis on the importance of the nation's conventional forces, including the Army. Kennedy selected Secretary of Defense Robert S. McNamara to implement the new strategy. In carrying out his assignment, McNamara, a former Ford Motors executive with a background in systems analysis, proved to be the very model of a rationalizing, centralizing bureaucrat. Making the most of the powers of his office, McNamara introduced a series of reforms that altered the way the American military machine was constructed and had a profound effect on the Army Intelligence community.[20]

Since 1958 there had been discussions at the national level concerning the advisability of setting up some kind of intelligence agency at the Department of Defense (DOD) level to better coordinate the intelligence elements of the armed services. In 1960 a Joint Study Group had criticized the existing arrangements within the Military Intelligence community. Three separate and uncoordinated service intelligence agencies, each with its own parochial bias, could not provide DOD with the integrated intelligence it needed to formulate a coherent national strategy. Air Force Intelligence in particular had embarrassed policy makers, since its estimates of alleged "bomber gaps" and "missile gaps" between the United States and the Soviet Union were widely disseminated and later demonstrated to be incorrect.[21]

Once in office, McNamara became a vigorous proponent of centralization, especially with respect to Military Intelligence operations under DOD. As a result, the Defense Intelligence Agency (DIA) began operations on 1 October 1961. The new organization would impose the same kind of centralized direction and control on the general Military Intelligence program as NSA was already providing to signals intelligence. Its creation meant that Army Intelligence would become a distinctly subordinate element within a wider Military Intelligence structure and marked a further cutback in ACSI's powers and responsibilities. However, this did not happen immediately. At its inception, DIA consisted of a cadre of twenty-five people housed in 2,000 square feet of borrowed office space in the Pentagon. The new agency pulled together rather slowly at first, initially taking on only the estimative, current intelligence, and requirements missions from the service intelligence agencies.

---

[20] One standard biography of the secretary of defense, Henry L. Truehitt's *McNamara* (New York: Harper and Rowe, 1971), has little to say about his role in Army reorganization.

[21] The role of Air Force Intelligence as a "loose cannon" and how this helped bring about the formation of DIA is documented in John Prados, *The Soviet Estimate: U.S. Intelligence Analysis and Soviet Military Strength* (Princeton: Princeton University Press, 1986), pp. 43–44, 93, 115–16, 124.

Meanwhile, McNamara was reorganizing the Army itself in ways that had a substantial effect on the Army's intelligence architecture. In 1962 the secretary of defense implemented Project 80, which involved the wholesale restructuring of the Army into functional, centralized commands. In the process, ACSI lost control over intelligence training, research and development, and doctrinal matters. Five of the Army's technical services were abolished, with only the Corps of Engineers and the Office of the Surgeon General remaining in place, and their intelligence personnel were split up among a number of different elements.[22]

A few order of battle specialists from the dissolved technical services joined the ACSI staff. A larger group engaged in scientific and technical intelligence became part of a new Foreign Science and Technology Center or stayed in place at the Army Missile Intelligence Agency which the Ordnance Department maintained at Redstone Arsenal. Both of these centers were assigned to the Army Materiel Command, which McNamara had just created. The largest group, consisting of 700 persons engaged in area analysis, was absorbed into the Area Analysis Intelligence Agency established at the direction of the chief of Engineers.

The Area Analysis Intelligence Agency was intended to be only a temporary holding area. When DIA assumed production responsibilities in 1963, the organization was discontinued, and its personnel, together with part of the OACSI staff, transferred to DIA. All in all, the Army contributed 1,000 spaces and its ACSI-MATIC computer system to the new DIA Production Center. In the process, OACSI lost 235 spaces, one-third of its strength, to the new agency. The centerpiece of OACSI had been its Directorate of Foreign Intelligence, the intelligence production unit. This was reduced to a shell, retaining only a residual responsibility for analyzing and interpreting national agency production in support of the Army and in maintaining liaison with DIA. As a result of this devolution of responsibilities, the center of gravity of Army Intelligence would move from the staff in Washington, D.C., to the units in the field.

However, even after the reorganization of 1963 DIA did not hold a complete monopoly over the production of intelligence for the Army. Subordinate elements within the Army continued to conduct production activities. These included the Army Materiel Command, with its two scientific and technical intelligence centers; the Office of the Chief of Engineers, which administered the Army Map Service; and the Office of the Surgeon General, which still had the responsibility of meeting some of the Army's medical intelligence requirements. In addition, a new production element was formed at Fort Bragg, North Carolina, to support the mobile reserve forces assigned to the Continental Army Command (CONARC).

Other intelligence-related functions previously performed by the Army were also centralized. In 1963 the Army's Strategic Intelligence School was merged with its Navy counterpart to form a new Defense Intelligence School, which

---

[22] Hewes, *From Root to McNamara*, p. 364.

began to provide training for attaches from all the military services. The process was carried through to its logical conclusion in 1965, when DIA assumed control over the military attache system that had served as an Army information source since 1889. All service attaches were integrated into the new Defense Attache System. Meanwhile, the Defense Language Institute had replaced the separate language schools previously maintained by the services.

Although DIA acquired production and collection assets from Army Intelligence, another new McNamara creation (the Defense Supply Agency) asserted itself on the counterintelligence front. In March 1965 this agency took over the whole field of industrial security, absorbing all the related spaces from ACSI's Industrial and Personnel Security Group. Ever since World War II, the function had rebounded between G–2 and the Provost Marshal General's Office. The new arrangement seemed to mark a definitive end to this particular jurisdictional dispute within the Army.

OACSI responded to these institutional challenges in much the same way as ASA had met the threat of the Armed Forces Security Agency: it found a new role in devoting itself to Army-specific needs. Shorn of many of its operational functions, OACSI reoriented itself and began providing intensified staff supervision to intelligence areas of growing interest to the Army. In the summer of 1963 the Directorate of Surveillance and Reconnaissance was added to the Army's Intelligence staff to develop the doctrine and hardware that would allow the Army to glean information from the battlefield through innovative technologies. Additional new Directorates of Security and Combat Intelligence were formed in 1964 to supervise functional areas of primary interest to the Army. The Combat Intelligence Directorate included a section responsible for overseeing developments in the fields of special warfare and foreign assistance. Finally, OACSI found ways to edge back into fields of activity theoretically preempted by DIA. In 1963 it set up a Special Research Detachment as a liaison element at NSA, soon expanding it into an all-source production element. The same year the Special Security Detachment formed an Intelligence Support Branch to provide the Army Staff with current intelligence.

The U.S. Army Intelligence Command and the U.S. Army Security Agency

The McNamara-directed reorganization of the Army had significant consequences for the Army Intelligence Center at Fort Holabird, Maryland. The center, commanded by the chief of the Intelligence Corps, had functioned as a field operating agency under direct ACSI control. Two of its main assets were the Army Intelligence School and the Army Intelligence Board, charged with framing doctrine and developing specialized equipment. The McNamara restructuring intruded on both of these arrangements. The Intelligence School was resub-

ordinated to CONARC and the functions of the Intelligence Board split between the Army Materiel Command and another McNamara creation, the Combat Developments Command.

As a result, ACSI created a new administrative entity, the U.S. Army Intelligence Corps Activity, which took over the remnant of the former Intelligence Center's assets and residual functions. The organization served as a vehicle through which the chief of the Intelligence Corps could exercise control over those elements the McNamara restructuring had left under ACSI jurisdiction. These consisted of the Army's counterintelligence records facility, a new Intelligence Corps Supply Activity, the Strategic Intelligence School (until its transfer to DIA), the Army Photo Interpretation Center, and the Administrative Survey Detachment that supported the Intelligence Civilian Career Program which ACSI had started in the 1950s. However, the establishment of the Army Intelligence Corps Activity did nothing to alleviate the confusion in the intelligence command chain resulting from the reorganizations. Since the chief of the Intelligence Corps continued to act as commandant of the Army Intelligence School and commander of Fort Holabird, he now reported simultaneously to three different superiors. As commanding general of the U.S. Army Intelligence Corps Activity and chief of the Intelligence Corps he was responsible to ACSI, but he was under the jurisdiction of CONARC in his capacity as school commandant and subordinate to the U.S. Second Army in his role of post commander. This Rube Goldberg–like arrangement offered no promise of stability.

These changes represented only the beginning of the restructuring of Army counterintelligence organization. In 1963 and 1964 the Army undertook a major study of its personnel security system, an effort spurred by the discovery that an Army sergeant in a sensitive position at the National Security Agency had been passing information to the Soviets for years without being detected.[23] The study, Project SECURITY SHIELD, found serious weaknesses both in the traditional decentralized approach to counterintelligence operations and in the coordination that existed between Army counterintelligence and the criminal investigators of the Provost Marshal General's Office. SECURITY SHIELD led to yet another wholesale reorganization of Army counterintelligence.

On 1 January 1965, the Army created the U.S. Army Intelligence Corps Command as a Department of the Army major field command. Operating under a new design concept, the command took over centralized direction over all counterintelligence operations in the continental United States. The Intelligence Corps Command assumed authority over the seven Intelligence Corps groups that had previously operated under six armies and the Military District of Washington. (The large CIC detachments in the United States had been redesig-

---

23 The errant sergeant was Sfc Jack Edward Dunlap. The story of the case can be found in James Bamford's popular but highly unauthorized book, *The Puzzle Palace: A Report on NSA, America's Most Secret Agency* (Boston: Houghton Mifflin, 1982), pp. 150–53.

nated as "groups" between 1956 and 1959.) At the same time, the Army ordered the field offices of the Intelligence Corps Command and the provost marshal's Criminal Investigation Division (CID) to be brought together wherever possible, and the records of the CID repository removed from Fort Gordon, Georgia, and collocated with the counterintelligence records at Fort Holabird.

The creation of the Intelligence Corps Command gave its commander, the chief of the Intelligence Corps, operational responsibilities for the first time in the history of Army counterintelligence. At the same time, he lost certain assets. Not all the elements of the former Army Intelligence Corps Activity were transferred to the new command. Since the Intelligence Corps Command was intended to be purely a counterintelligence organization, the Army Imagery Interpretation Center, as the Photo Interpretation Center had been redesignated, reverted back to the direct control of the ACSI.

There were still certain anomalies in the new pattern of organization. Despite its title, the Intelligence Corps Command controlled only about half of all Intelligence Corps personnel in the continental United States. The rest were on school or organizational staffs, with the TOE organizations supporting tactical elements in the field, or in the "pipeline." Intelligence Corps personnel deployed outside the continental United States were not a part of the new command. The Intelligence Corps Command's commander, in his other capacity as chief of the Intelligence Corps, thus had substantial administrative responsibilities extending beyond his own command; and the Intelligence Corps he headed was engaged in active intelligence collection as well as in counterintelligence. The creation of the new headquarters also had left the chain of command more tangled than ever. Its commander now wore four hats. As head of a major field command, he now reported directly to the Army chief of staff, in addition to reporting to ACSI, the commander of CONARC, and the commander of the U.S. Second Army in his other various roles.[24]

In one sense, this arrangement conformed to the civilian theories of matrix management popular in the 1960s. Matrix management held that someone marketing refrigerators to Latin America should report to a vice president for marketing, a vice president for refrigerators, and a vice president for Latin America. But the scheme did not accord with normal Army command procedures and was in practice unworkable. Not surprisingly, reorganization plans were begun as soon as the new command had been assembled. The U.S. Army Intelligence Corps Command lasted just six months.

There seemed to be only two possible solutions to the organizational tangle created by the existence of the Intelligence Corps Command. One duplicated

---

[24] As the U.S. Army Intelligence Corps Command's own fact sheet noted at the time, "USAINTCC is only one facet of the intelligence complex located at Fort Holabird. The integrated staff serves four masters." Fact Sheet, U.S. Army Intelligence Corps Command, p. 2. U.S. Army Intelligence Command file, INSCOM History Office.

the Army Security Agency's centralized, vertical command structure, creating a self-sufficient organization. However, because of its mission, that agency was a special case, and its organization had no parallel in the rest of the Army. The other solution, the one adopted, decentralized the structure of the Intelligence Corps Command.

The U.S. Army Intelligence Command (USAINTC) was created on 1 July 1965 to conduct counterintelligence operations within the continental United States.[25] The combined headquarters organization of the former Intelligence Corps Command was broken up, and the Army Intelligence School and Fort Holabird placed under separate commanders. Functions previously performed by the Intelligence Corps Command that were unrelated to counterintelligence—administering the intelligence civilian career program and procuring intelligence-related supply items—reverted to ACSI, resulting in the establishment of the Administrative Survey Detachment and the Intelligence Materiel Development Support Office as separate field operating activities. Finally, the Intelligence Corps itself was discontinued in March 1966, and its personnel functions shifted to the Department of Army level. This ended the Army's attempts to integrate human intelligence and counterintelligence personnel under a single organizational structure. Discontinuance of the Intelligence Corps also resulted in the redesignation of all Intelligence Corps units as Military Intelligence units.[26]

The creation of the U.S. Army Intelligence Command meant that the Army counterintelligence organization had been turned inside out. The old Counter Intelligence Corps had selected, trained, and administered Army counterintelligence personnel, but counterintelligence operations themselves had been decentralized under the control of local Army commanders. The new major Army field command was a centralized operational organization without any personnel or training functions. The demise of the Intelligence Corps ended a special tradition that went back to the Corps of Intelligence Police in World War I, but the new arrangements meant that Army counterintelligence was now aligned with the rest of the Army.

If McNamara's organizational innovations destroyed the Intelligence Corps, they left the Army Security Agency substantially untouched. Because of its specialized mission and compartmented operations, the agency escaped the loss of its training and research and development functions. Instead, it expanded physically, geographically, and functionally. An ASA element, with the in-country designation of the 3d Radio Research Unit, deployed to Vietnam to support the ongoing advisory effort as early as 1961.[27] The agency also acquired an impor-

---

[25] GO 23, HQDA, 1 Jul 65.

[26] Intelligence Corps groups were redesignated Military Intelligence groups on 16 October 1966.

[27] One member of the 3d Radio Research Unit was Sp4c. James T. Davis, who was killed in action on 22 December 1961, and whom President Lyndon Johnson later described as the first fatality of the Vietnam War.

tant new acoustical intelligence mission in 1962, following the abolition of the Signal Corps as an Army technical service. A year later, the Army Security Agency achieved a monopoly of Army electronic warfare functions when it took over control of the noncommunications-jamming function and associated units from the Signal Corps. In 1964 it set up its third field station in the continental United States at Homestead, Florida, to better meet new mission requirements which had evolved in the early 1960s. Finally, the agency's independence and unique position within the Army was ratified on 14 April 1964, when it achieved the status of a major Army field command.[28]

The Army Intelligence and Security Branch

The changes within the Army Intelligence community during the 1960s were not confined to shifts in function and in command relationships. Army Intelligence took a giant step in the direction of full professionalism in 1962, when the Army Intelligence and Security Branch was set up as a basic branch of the Regular Army. This development was long overdue. Since World War II, intelligence professionals had argued that the very existence of intelligence units created the need for a separate intelligence branch. The logic of this argument was increasingly reinforced by practical necessities. The pool of reserve officers capable of filling intelligence slots was becoming exhausted. Without a reform in the Army personnel system, analysts projected that half the Army's intelligence officer positions would be without qualified occupants by 1965. The incumbent ACSI, Maj. Gen. Alva R. Fitch, pushed vigorously for the creation of a new branch to remedy the situation. Yet even the Army Intelligence community was divided on the issue. The ASA chief protested that the proposed integration of signals intelligence officers with other intelligence personnel would be like putting infantry and artillery into one branch. But Fitch won his case. The new branch came into existence formally on 1 July 1962.[29]

The Army Intelligence and Security Branch embraced about 5 percent of officers in the active Army. The initial group joining the branch consisted of 283 Regular Army and 3,652 reserve officers who had a background in intelligence or were assigned to intelligence positions. A quarter of the group consisted of cryptologic specialists; the remainder broke down about evenly into combat intelligence personnel and members of the Intelligence Corps. The formation of the new branch significantly enhanced the Army's capacity to promote and retain qualified intelligence officers.

---

[28] GO 14, HQDA, 14 Apr 64. As a result of this upgrade in status, the chief, Army Security Agency, assumed the new title of commanding general, Army Security Agency.

[29] Marc B. Powe and Edward E. Wilson, *The Evolution of American Military Intelligence* (Fort Huachuca, Ariz.: U.S. Army Intelligence Center and School, 1973), p. 105.

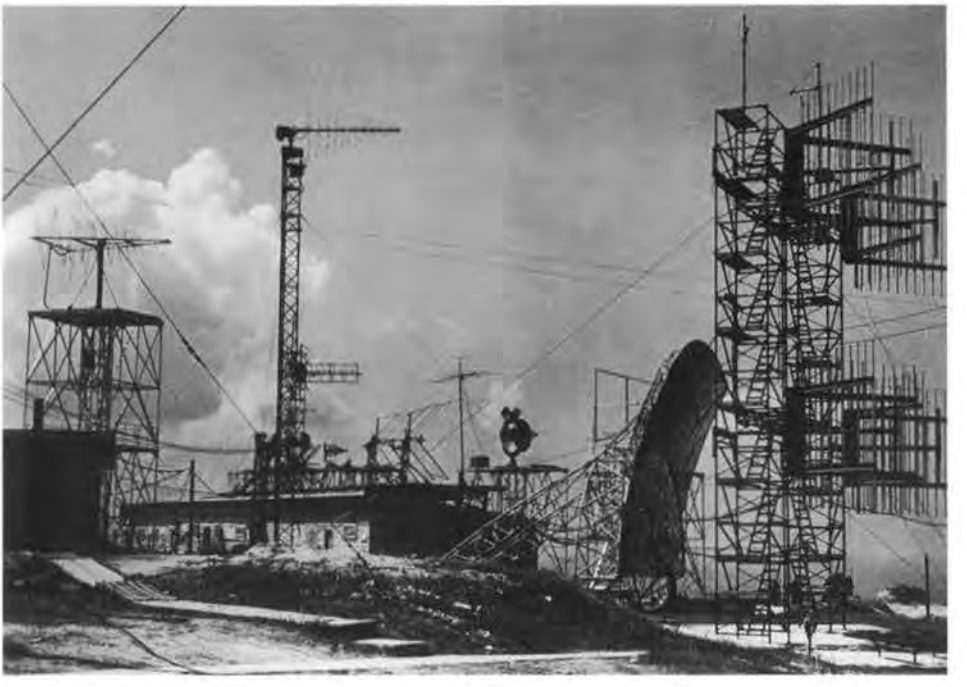
However, the new branch had problems initially. It contained only a small number of Regular Army officers, and many of the reserve officers brought into the Army Intelligence and Security Branch lacked higher education or prospects for career advancement. The branch was designated as one that performed a combat service support function, not the most prestigious role in the Army. Finally, it was the only branch in the Army without a common basic course. Although most Intelligence officers attended Fort Holabird for training, Army Security Agency officers still trained separately at the U.S. Army Security Agency Training Center and School (USASATC&S) at Fort Devens, Massachusetts. Nevertheless, within the space of four years, much of Army Intelligence had been reconfigured. The new structure would meet its first test in the foreign and domestic challenges during the war in Vietnam.

Antenna array of the 326th Communication Reconnaissance Company during the Korean War. (*INSCOM*)

Photointerpreters of the 45th ("Thunderbird") Infantry Division examine imagery of the Korean countryside. (*NARA*)

The sphinx—historically identified with Military Intelligence—stands in front of the headquarters of Fort Holabird, Maryland, home of the Army Intelligence School from 1954–1971. (*INSCOM*)

Antenna array of the 276th Army Security Agency Company at an overseas site. (*INSCOM*)



The durable OV–1 "Mohawk" served as the Army's main aerial reconnaissance platform for a generation. (*DA Photograph*)

Assistant Chief of Staff for Intelligence Maj. Gen. Alva Fitch was instrumental in establishing the Intelligence and Security Branch (later Military Intelligence Branch) in the Regular Army in 1962. (*Courtesy of Maj. Gen. Joseph A. MaChristian, U.S. Army [Ret.]*)

Members of the 25th MI Detachment plot suspected enemy positions on a map at the Cu Chi base camp during the Vietnam conflict. (*NARA*)

An intelligence officer interrogates a suspected member of the Viet Cong. (*NARA*)

A Special Forces team operates an AN/PRD–1 radio direction finder. (*INSCOM*)

Operations room at the headquarters of the U.S. Army Intelligence Command, which directed Army counterintelligence activities in the continental United States during the troubled Vietnam era. (*NARA*)

As a result of the Intelligence Organization and Stationing Study, the Army formed new Combat Electronic Warfare and Intelligence (CEWI) units to support its tactical formations. A soldier of the 519th Military Intelligence Battalion demonstrates a PRD–11 radio direction finder. (*519th MI Battalion Photograph*)

New systems such as the Guardrail Common Sensor mounted aboard the RC–12 platform enhanced the Army's electronic warfare and intelligence capabilities. (*DA Photograph*)

Organization Day ceremonies for the Military Intelligence Corps at Fort Huachuca, Arizona, in 1987. The Army had relocated its Military Intelligence schoolhouse to the post in 1971. (*U.S. Army Intelligence Center and Fort Huachuca*)

The Army Intelligence and Security Command, organized in 1977 to conduct multidiscipline intelligence and electronic warfare operations at the echelon above corps, finally moved into this new headquarters building at Fort Belvoir, Virginia, in 1989. (*INSCOM*)

A Disneyland castle perched atop an artificial hill, U.S. Army Field Station Berlin served as INSCOM's forward outpost behind the Iron Curtain until termination of the Cold War brought about its closure in 1992. (*INSCOM*)

A soldier of INSCOM's 704th MI Brigade. Increased use of sophisticated automation and communications systems would help pave the way for Army Intelligence to carry out its diverse and demanding missions following the end of the Cold War. (*704th MI Brigade Photograph*)

9

Vietnam and Beyond

The 1960s began with brave promises; however, events soon began to go awry. Although successive crises with the Soviet Union over Berlin and the Soviet deployment of missiles to Cuba were resolved peaceably, the Viet Cong insurgency in South Vietnam continued to fester, despite the involvement of an increasing number of American military advisers. In early November 1963 a beleaguered President Ngo Dinh Diem of South Vietnam was assassinated during a coup by his own Army. Intended to stabilize the deteriorating security situation in South Vietnam by removing an unpopular leader, the coup had the opposite effect. As a revolving-door series of ephemeral governments came and went in Saigon, Communists gained an increasing foothold in the countryside. Meanwhile, President John F. Kennedy had been assasinated in Dallas; his successor, Lyndon B. Johnson, had a wealth of experience in domestic politics but no substantive understanding of foreign affairs. Johnson won election in 1964 on a platform of peace and social reform, but soon found that developments in Vietnam would imperil both goals. By early 1965 a Viet Cong victory seemed imminent.

America responded initially with limited air raids against the Viet Cong's sponsor, North Vietnam. When this action proved unproductive, ground troops were committed to the South under the direction of the Military Assistance Command, Vietnam (MACV), a joint, Army-dominated "sub-theater" headquarters. The North Vietnamese countered by steadily increasing their war buildup, sending in their own regular forces to supplement the activities of the guerrillas. Thus the United States lurched into an undeclared war.[1] On the American side, this remained a limited effort. The president's main focus was on constructing a "Great Society" at home, and he regarded the war in Southeast Asia as an unpleasant distraction. As a matter of deliberate management, the conflict was fought without passion, without censorship, without mobilization, and without raising taxes. Increasingly, it was fought without

[1] For a caustic evaluation of the Johnson administration's conduct of the war, see David Halberstam's *The Best and the Brightest* (New York: Random House, 1972).

popular enthusiasm. On the other hand, for the North Vietnamese and their Viet Cong proxies, the war was total.

By the end of 1967 an American Army of 485,000 soldiers and marines, backed up by an enormous logistical system, had deployed in country; and officials talked brightly that there was now "light at the end of the tunnel."[2] The Tet offensive at the beginning of 1968 dispelled this dream, however. It broke the will of an administration and shattered the confidence of the American people. After Tet, all roads ran downhill. The Johnson administration decided to stop reinforcing the war effort; its successor chose to withdraw gradually from the war and return the tar baby to the luckless South Vietnamese. In the meantime, the United States was unraveling on the domestic front. Racial unrest resulted in rioting on a massive scale, while an increasingly violent antiwar movement grew in strength on the nation's campuses.

What ensued was an almost complete debacle. A cease-fire in place in Vietnam at last was signed in Paris in 1973. A similar agreement, signed in Korea twenty years before, had endured. However, the government of South Korea had been in full control of its own territory, and American military might had backed up the agreement. Neither of these conditions proved true in Southeast Asia. Hundreds of thousands of North Vietnamese troops remained in place in the South, and a peaceful end to the conflict seemed remote. American ground forces were completely withdrawn from Vietnam, and any chance that the peace settlement would stand was undermined by the disintegration of the Nixon administration amid the toils of the Watergate scandal. Confronted by a North Vietnamese blitzkrieg and abandoned by its American allies, in 1975 the South Vietnamese government collapsed.[3]

All of these events had a massive impact on Military Intelligence. Some structural changes that took place during this period were driven by new developments in technology. Most, however, were brought about by the military commitment to Southeast Asia and its manifold repercussions. The Vietnam conflict, its domestic side effects, and the economic and psychological constraints produced by the outcome of the venture all worked to reshape the organization of Army Intelligence.

Vietnam: Buildup and Deployment

The Vietnam conflict proved a formidable challenge to Army Intelligence, as well as to the rest of the American defense establishment. The Army was forced to function in an unfamiliar environment and deal with an unfamiliar language, under rules of engagement giving the enemy a chance to accept or decline battle

---

[2] Kathleen J. Turner, *Lyndon Johnson's Dual War: Vietnam and the Press* (Chicago: University of Chicago Press, 1985), p. 211.

[3] It should be noted that the official Army photo history of the Vietnam War, which begins its coverage in 1945, tactfully chooses to end its account in 1973.

at will. The detailed, quantified information which the decision makers of the day demanded was not easy to develop when the enemy was a guerrilla under jungle canopy, and when the exact state of the "hearts and minds" of an indigenous population involved in a civil war was so hard to assess. Under such conditions it is not surprising that the performance of Army Intelligence engendered controversies that lived on long after American troops had left Southeast Asia.[4]

Previous conflicts had witnessed a vast expansion of the Army's departmental-level intelligence staff. However, these conflicts had been fought before the subordination of Army Intelligence to unified intelligence agencies. In Southeast Asia, the Defense Intelligence Agency would be responsible for the analytical effort. As a result, the OACSI staff actually contracted over the course of the war, and its internal organization was shaped as much by factors such as the increased availability of computer support, the need to manage new technologies, and the necessity for coping with counterintelligence problems on the domestic front as it was by the war in Southeast Asia itself. The real growth of the Army's intelligence and security organization was in the field. The Army Security Agency built up to a strength of 30,000, one-fifth of which was deployed in Vietnam at any one time, and other components grew correspondingly.

As long as the American military presence in South Vietnam had been confined to an advisory role, the demands on the Army's intelligence resources had not been excessive. In early 1965 the MACV was receiving intelligence support from a collection detachment subordinate to the Japan-based 500th Intelligence Corps Group, a counterintelligence detachment, and some two hundred intelligence officers serving as advisers with South Vietnamese troops. In-country cryptologic work was handled by the Army Security Agency's 3d Radio Research Unit (RRU), which comprised aerial as well as ground-based elements.[5]

The influx of American troops in large numbers changed all this. In response to the requests of Maj. Gen. Joseph A. McChristian, MACV assistant chief of staff for intelligence, or J–2, in 1965 the 525th Military Intelligence Group was deployed in packets from Fort Bragg, North Carolina, to serve as command and control headquarters for the intelligence effort.[6] It was joined by the 1st Military Intelligence Battalion (Aerial Reconnaissance Support) and the 519th Military Intelligence Battalion (Field Army). Soon afterward, two additional Military Intelligence groups were introduced, built up from cellular teams dispatched from the United States. These were the 135th Military Intelligence

---

[4] Some of the controversies are explored in T. L. Cubbage II, "Westmoreland vs. CBS: Was Intelligence Corrupted by Policy Demands," *Intelligence and National Security* 3 (July 1988): 118–80.

[5] Operations of this little-known unit are mentioned in Neil Sheehan's *A Bright Shining Lie: John Paul Vann and America in Vietnam* (New York: Random House, 1988), p. 203, and in Robert F. Futrell's *The Advisory Years to 1965*, The United States Air Force in Southeast Asia (Washington, D.C.: Office of Air Force History, 1981), p. 244.

[6] Lt. Col. Arthur D. McQueen, "The Lion Goes to War," *Military Intelligence* (April/June 1977): 28–36.

Group, a counterintelligence unit, and the 149th Military Intelligence Group, with a collection mission.[7] The groups absorbed the personnel and functions of the 519th Military Intelligence Battalion's counterintelligence and collection companies. Meanwhile, the 519th was itself greatly expanded to support four combined United States–Vietnamese processing and production centers. The unit included a large technical intelligence detachment augmented by detachments from the Army technical branches.

In the fall of 1967, following the departure of General McChristian, there was another substantial reorganization of intelligence units within South Vietnam. The 525th Military Intelligence Group restructured its subordinate units into six provisional battalions, respectively located at Da Nang, Nha Trang, Bien Hoa, Can Tho, Saigon, and (for a time) Tan Son Nhut Air Base; the 135th and 149th Military Intelligence Groups subsequently were inactivated.[8] This effort was supplemented by the activities of over six hundred intelligence advisers serving with the Vietnamese; by intelligence detachments attached to all independent brigades and higher formations; and by aerial surveillance companies that operated in support of the "field forces," Army corps-level headquarters organizations with additional advisory functions. Army Special Forces and the Vietnamese Montagnards under their control also played a significant role in furnishing combat intelligence.

Army Security Agency support in country expanded as well. At the height of the war effort, the agency's 509th Radio Research Group, which had replaced the 3d Radio Research Unit, commanded a fixed field station at Phu Bai; the 224th Aviation Battalion (Radio Research); the 303d and 313th Radio Research Battalions, each attached to an Army field force; a communications security company; and some twenty direct support units (DSUs) attached to divisions and brigades.[9] Other ASA assets positioned in Thailand and the Philippines also supported the cryptologic effort.

As it evolved, the Army Intelligence effort in Vietnam became heavily committed to collaboration with the South Vietnamese, who knew the language and terrain and already possessed a useful, if fragmented, data base. General McChristian organized a Combined Intelligence Center at Tan Son Nhut Air Base near Saigon, manned by U.S. and South Vietnamese personnel and under the joint control of MACV and the South Vietnamese high command. Similar combined centers handled prisoner-of-war interrogation, document exploitation, and analysis of captured materiel.[10] In a kind of reverse advisory role,

---

[7] The reorganization of Army Intelligence in the Republic of Vietnam between 1965 and 1967 is described in General Joseph A. McChristian, *The Role of Military Intelligence, 1965–1967* (Washington, D.C.: Department of the Army, 1974), pp. 3–20.

[8] Shelby Stanton, *Vietnam Order of Battle* (Washington, D.C.: U.S. News Books, 1981), pp. 235–36.

[9] Ibid., pp. 233–34.

[10] McChristian, *The Role of Military Intelligence*, pp. 21–78. A description of the Combined

South Vietnamese Military Intelligence detachments worked directly with American formations at the level of independent brigade and above.

Vietnamese assistance was necessary because of some American deficiencies. Vietnamese linguists were in especially short supply, which made close cooperation with the South Vietnamese essential. And although there had been an American advisory presence in the country since the 1950s, America went into the war without benefit of an adequate intelligence data base. At the time DIA was formed, ACSI had delegated the task of compiling order of battle data for Southeast Asia to the U.S. Army, Pacific, while USARPAC in turn had assumed that the Military Assistance Advisory Group, Vietnam, was carrying out this responsibility. In reality, no one had done the job, and American combat forces deploying into Southeast Asia had been confronted with an intelligence vacuum.[11]

Moreover, although the McNamara regime had strengthened the previously neglected conventional forces, the Army still lacked enough trained intelligence professionals to meet its needs in Vietnam. It took a long time for the Army's intelligence training establishment to retool to meet the needs of the conflict. The Army Intelligence School did not begin to offer a Vietnam-oriented short course until 1968, and training for intelligence officers serving as advisers at the district and province level in Vietnam was not provided until 1970. Moreover, in this conflict, the reserve components could not compensate for the deficiencies of the Regular Army. There was a substantial Military Intelligence presence in the reserves, but linguistic skills were lacking, and in any case the administration had declined to deploy them. This may have been a blessing in disguise, since unit readiness in many cases was low. Maj. Gen. Charles Denholm, commanding general, U.S. Army Security Agency, deemed the ASA reserve units "almost useless."[12]

As in previous wars, communications security in the field continued to be a major problem for the Army. This was aggravated by the compartmentalized nature of the war, the extensive use of aircraft, and above all by the ubiquitousness of the radio-telephone. A Vietnam-era division, for example, had 3,000 of

---

Intelligence Center, Vietnam (and much else), is contained in Bruce E. Jones, *War Without Windows: A True Account of a Young Army Officer Trapped in an Intelligence Cover-Up in Vietnam* (New York: Vanguard Press, 1987). See also Col. Huang Ngoc Lung, *Intelligence*, Indochina Monographs (Washington, D.C.: U.S. Army Center of Military History, 1982), pp. 82–83. Lung feels that the relationship between U.S. and Vietnamese intelligence did not become "really close and effective" until 1969.

11 General Bruce Palmer, Jr., *The 25-Year War: America's Military Role in Vietnam* (New York: Simon and Shuster, 1984), pp. 39–40.

12 The Secretary of the Army's Program for Command Supervision of Readiness: Command Presentation by U.S. Army Security Agency, 10 Sep 68, p. 19, Army Cryptologic Records. During the Berlin Crisis of 1961 the deployment of two ASA battalions had ended in a fiasco; the units were so ill trained that that they never got beyond the gates of the ASA Training Center and School at Fort Devens, Massachusetts. Eventually, the 241st and 277th Military Intelligence Detachments were called into federal service in the token reserve mobilization following the Tet offensive, but they never went overseas.

these transmitters, compared to 225 in a representative World War II division. Proper communications security often required units to shift radio frequencies and call signs. But the crowded electromagnetic environment presented by a communications-rich war meant there were not enough available frequencies, while helicopter companies that operated over hundreds of miles in support of units drawn from a number of nations found that any change in call signs produced paralyzing confusion. The Army's manpack speech security devices were too heavy and cumbersome to be lugged through the jungle easily, and troops resorted to the use of homemade radio-telephone codes that became transparent all too easily. Many commanders preferred to ignore the whole problem, choosing to sacrifice security considerations to speed and availability of communications.[13]

There were other shortfalls. At first, lower-echelon commanders complained that they were deprived of vital timely intelligence, either because of compartmentation considerations or because scarce intelligence assets were being held under close control at higher levels. Ultimately, however, Army Intelligence constructed a serviceable organization in Vietnam, even though some of its problems were never solved. Units down to the maneuver battalion learned to coordinate intelligence with operations by establishing joint tactical operations centers. Commanders improvised special companies with the capacity to conduct long-range reconnaissance patrols; in 1969 the Army formally made these units elements of the 75th Infantry and designated them as "Rangers."[14] The Army also met the expanding intelligence and security needs of the combat divisions committed to Vietnam by expanding their intelligence detachments to full companies and providing the divisions with TOE ASA companies in direct support. In addition, Special Security Offices in each division disseminated the most sensitive intelligence derived from national-level acquisition systems. Intelligence sources available only to high-level commanders for strategic applications during World War II now could be put to tactical use. As the war progressed, the number of individuals indoctrinated for compartmented intelligence in combat divisions tripled.

Additional ground intelligence was provided by the teams of the 5th Special Forces Group, 1st Special Forces, in Vietnam and the Vietnamese Civilian Irregular Defense Groups they advised. The Special Forces camps, scattered along the thinly populated interior spine of South Vietnam, served as an outpost screen to detect the movement of infiltrating enemy columns. Besides engaging in ground reconnaissance, the Special Forces conducted intelligence and counterintelligence operations through their contacts with the local Montagnard tribesmen. Members of the Special Forces also served as the Army component of the MACV Studies and Observation Group, a joint service element under JCS

---

[13] John D. Bergen, *Military Communications: A Test for Technology*, United States Army in Vietnam (Washington, D.C.: U.S. Army Center of Military History, 1987), pp. 396–401.

[14] Powe and Wilson, *The Evolution of American Military Intelligence*, p. 115.

supervision that collected intelligence and carried out special operations in denied areas in conjunction with its Vietnamese counterpart organization.[15]

American advisers also contributed to the intelligence effort. Working hand in hand with their Vietnamese counterparts at the province and district levels, they became increasingly involved in an attempt to identify and neutralize the Viet Cong infrastructure that supported the insurgency through a network of district intelligence and operations coordinating centers established throughout South Vietnam. The centers had "a dual mission to produce and exploit *both* VC infrastructure and tactical Military Intelligence." Originally begun as a unilateral American effort to upgrade the effectiveness of Republic of Vietnam security organizations, the program was formally embraced by the South Vietnamese government in 1968 and assigned the dual code name PHOENIX/PHUONG TRANG.[16]

Better cryptologic support to the field came about when the Army Security Agency established management centers to service each Army field force and introduced tactical direct support units down to the level of the individual combat brigades. In the process, the agency moved into the front lines. ASA special operations personnel worked with the patrols of the Special Forces, and an ASA element mounted in armored personnel carriers was organized to provide support to the 11th Armored Cavalry Regiment.[17] The guerrilla nature of the war meant that Army Security Agency personnel usually working in safe rear areas were exposed to hazard. The large fixed field station at Phu Bai was maintained as a fortified camp, bristling with minefields, concertina wire, pillboxes, sandbagged bunkers, watchtowers, trenches, and mortar positions. ASA casualties during the Vietnam conflict were many times greater than during the Korean War.[18]

---

15 Shelby Stanton, *Green Berets at War: U.S. Army Special Forces in Southeast Asia, 1956–1975* (Novato, Calif.: Presidio Press, 1985). See also the same author's *Vietnam Order of Battle*, pp. 239–53.

16 ICEX Newsletter 67–4, 4 Dec 67, p. 6. By 1969, however, the Army command in Vietnam had become disenchanted by the program because of the perceived excesses of the Provincial Reconnaissance Units that served as executive agents in "neutralizing" Viet Cong cadre. Jeffrey J. Clarke, *Advice and Support: The Final Years*, United States Army in Vietnam (Washington, D.C.: U.S. Army Center of Military History, 1988), pp. 379–80. Perhaps participants took too literally the injunction to take "a 'rifle shot' approach" in dealing with the infrastructure problem. ICEX Briefing Paper, 30 Aug 67, p. 1. A recent detailed examination of PHOENIX is Dale Andrade, *Ashes to Ashes: The Phoenix Program and the Vietnam War* (Lexington, Ky.: D.C. Heath, 1990). For the personal account of an Army participant in this much maligned and misunderstood program, see Stuart H. Herrington, *Silence Was a Weapon: The War for the Vietnam Villages, A Personal Perspective* (Novato, Calif.: Presidio Press, 1982).

17 Some of these ASA activities are captured in photographs in John P. Finnegan, *Military Intelligence: A Picture History* (Washington, D.C.: Government Printing Office, 1985), pp. 167–68.

18 Casualties among Military Intelligence personnel were not restricted to members of the Army Security Agency. During the Tet offensive, the Hue detachment of the 525th MI Group was overrun and its members killed or captured. The first Medal of Honor ever granted to a Military Intelligence officer was awarded posthumously to 1st Lt. George Sisler, assistant intelligence officer of a Special Forces team.

In the area of communications security, the Army Security Agency sought to bring about improvement by changing its approach. During the first stages of the war, tactical units in the field received communications security support from their attached ASA companies and detachments. At that time, communications security was conceived of as essentially a police-type function of monitoring friendly communications and warning of possible compromises. This arrangement proved to be ineffective, producing conflicts with supported commanders. As a remedy, the agency evolved a new concept of "before the fact" assistance, having its personnel serve as advisers rather than as policemen.[19] Under this doctrine, communications security personnel assisted in planning operational communications procedures and instructed troops on the necessity of communications security. To implement this better, in 1969 the agency's in-country communications security assets were withdrawn from the direct support units and concentrated in the 101st Radio Research Company. A similar centralized ASA security company was also formed in Europe. The new, nonpunitive approach was facilitated by the simultaneous fielding of the Nestor family of speech security devices, which eliminated much of the security problem at the source.[20]

Organizational innovations in the intelligence and security field were supplemented by the introduction of new technologies. Airborne electronic support, first pioneered in Vietnam and conducted from fixed-wing aircraft and later from helicopters, was one.[21] Other elements of Army Intelligence were able to make productive use of gadgets such as unattended ground sensors and "people-sniffers." Infrared and side-looking airborne radar sensors supplemented the traditional visual and optical techniques of aerial observation, while the pairing of observation and armed helicopters into "pink teams" with the dual missions of finding and fighting gave another dimension to traditional aerial reconnaissance. At the top, MACV's J–2 staff slowly automated its intelligence data base and collection management procedures.

In the end, of course, it was not enough. Although Army Intelligence could provide the higher commanders with significant forewarnings of the 1968 Tet offensive, the intensity of the enemy attack was underestimated. But the fact remains that Army Intelligence could provide the kind of warning before Tet in 1968 that it had been unable to furnish before the Battle of the Bulge in 1944. However, despite the similar military outcomes of the Tet and Ardennes counteroffensives—in each case, the enemy scored some disconcerting gains, but paid for them with disproportionate losses—Tet did something that the German

---

[19] USASA Commanders Conference, 5–12 May 69, Staff Presentation Roundtable Discussions, Army Cryptologic Records.

[20] Bergen, *Military Communications*, pp. 407–08.

[21] The 224th Aviation Battalion (Radio Research) managed the fixed-wing assets, flying 100 aircraft at the height of the conflict. Included in its inventory was a handful of four-motored reconverted patrol bombers acquired from the Navy.

Ardennes offensive had not done: it convinced the home front that the war could not be won. The fighting went on, but negotiations and a program of Vietnamization became the order of the day. As the American military presence in South Vietnam shrank, so did the presence of Army Intelligence. The last Army Intelligence elements left South Vietnam in 1973, following the signing of the Paris Peace Accords.[22]

The Vietnam conflict had furnished Army Intelligence with a short list of lessons learned and a long list of casualties. The war's effects on the structure of Army Intelligence were not confined to Vietnam. The rapid turnover of personnel engendered by the policy of troop rotation adversely impacted the cohesion and professional capacity of units far removed from the war zone, as had the diversion of equipment and spare parts to the fighting front. On the home front, the war and the opposition it provoked led Army Intelligence into a situation that compromised its image. Finally, the antimilitary and anti-intelligence reaction that prevailed in America as the Vietnam conflict came to a close posed deep threats to the whole Army Intelligence organization.

The U.S. Army Intelligence Command and the Home Front

Even while the fighting went on in Vietnam, Army Intelligence was actively engaged in operations in another area, the American home front. The principal Army player here was the U.S. Army Intelligence Command (USAINTC), the Army counterintelligence element formed in 1965 to conduct operations in the continental United States. The command had been allotted substantial personnel to carry out its mission. Its seven Military Intelligence groups controlled a network of 300 field and resident offices across the nation. The merger of Army counterintelligence and criminal investigative records into the Investigative Records Repository (IRR) gave the command a massive data base, which was supplemented in 1966 when USAINTC became the DOD agent administering the newly created Defense Central Index of Investigations, a master file of all counterintelligence and criminal investigations performed by the armed services, and the National Agency Check Center, which performed records searches on files maintained by non-DOD agencies such as the Federal Bureau of Investigation (FBI) and local police departments. By 1967 the command had extended its responsibilities beyond its original jurisdiction, assuming the case control function for routine background investigations requested by the major commands overseas.

Centralizing counterintelligence operations in the United States under a single Army command produced the desired effects in terms of speed and efficiency. The new organization not only had a greater capacity to coordinate and conduct counterespionage investigations against military suspects but also was bet-

---

22 Individual Army Intelligence personnel did remain behind as members of the Defense Attache's Office.

ter able to conduct background investigations. Under the old decentralized system, it had taken an average of ninety-seven days to process a standard background investigation. By 1967 USAINTC completed these investigations in an average time of thirty-one days. However, centralization would prove to have less desirable effects. It gave Army counterintelligence a high profile, and gave civilian policy makers an organization to task for domestic intelligence collection in what was rapidly becoming a time of trouble. The end result for Army Intelligence was less than satisfactory.

Under delimitations agreements dating back to the 1940s, the FBI had primary responsibility for counterintelligence investigations of civilians in the continental United States. Army counterintelligence confined its attention to the military and to those civilians who applied for security-sensitive civilian and military positions with the Army. Most of the Army's counterintelligence effort and resources were devoted to background investigations of the latter. However, the events of the 1960s conspired to break down the neat demarcation line between military and civilian counterintelligence jurisdiction in the United States and to draw Army Intelligence deeply into civilian affairs. Federal troops were frequently alerted and occasionally deployed to restore order when local authorities were unable to maintain control in the numerous crises of the period. Commanders needed intelligence support, and it quickly became apparent that it was too late to attempt to gather intelligence once an actual troop deployment had begun. It also became apparent that the existing civilian intelligence agencies were fragmented and often ineffectual.

The FBI may have had theoretical responsibility for civilian counterintelligence, but its director, J. Edgar Hoover, was aging and increasingly uncooperative. The bureau itself, although having a good track record in apprehending interstate car thieves, kidnappers, and the occasional spy, was primarily a crime-fighting agency with neither the capacity nor the inclination to produce finished domestic intelligence. Moreover, the overwhelming majority of FBI agents were middle-aged white males, limiting the bureau's capability to conduct effective undercover work against the radical black and student groups that seemed to pose the greatest threat to national security. As conditions of disorder became progressively worse, the Army moved to fill an intelligence void.

Local commanders had first begun to request counterintelligence support from the assets they controlled during the civil rights disturbances in the South in the first part of the decade. USAINTC became involved in giving crisis support soon after it had been set up, as a result of Army involvement in the Watts rioting in August 1965. The command formulated its first contingency plan for collecting domestic intelligence in early 1966. STEEP HILL, as the plan was code named, was designed to be implemented only after there had been an actual deployment of federal troops.

The command soon realized that STEEP HILL, redesignated GARDEN PLOT in 1967, was inadequate. For USAINTC to be of any help to Army commanders in

a civil disturbance situation, it would have to begin collection as soon as there was any likelihood of a deployment of federal troops. To meet the requirement, the command devised a new collection plan, ROSE HILL, later redesignated PUNCH BLOCK and LANTERN SPIKE, successively. Unrest in America's cities caused PUNCH BLOCK to go into effect eight times during the summer of 1966. By this time, in the words of the USAINTC official history, civil disturbance collection had become a "minimal, but increasing" part of the command's work load.[23]

The troubled summer of 1967 brought matters to a head. The LANTERN SPIKE civil disturbance collection plan was implemented four times, and federal troops were actually committed to deal with a major riot in Detroit. As a result of the Detroit disturbances, Deputy Secretary of Defense Cyrus Vance, who had served as the agent of the Executive Branch in handling the federal intervention, tasked the Army with "reconnoitering the major cities" to gain information on critical elements of topography and vulnerability before troops were sent in again. He also suggested that "the assembly and analysis of data with respect to activity patterns is also needed."[24] This put the Army into the domestic intelligence business on a greatly enlarged scale.

After the Detroit riots, the priorities of the U.S. Army Intelligence Command changed perceptibly. The Army now began to collect intelligence data that would not only allow it to intervene effectively in urban riots, but would also help it to cope with the threat of the increasingly violent antiwar movement. By 1967 the popular consensus in support of American commitment to Vietnam was beginning to waver. An uncensored media had brought the horrors of war to American living rooms, and the Johnson strategy of fighting a painless war by allowing generous exemptions for college students while tripling the draft call had made a time bomb out of the nation's campuses. Radical students and others had started to challenge not only the war, but the whole American system allegedly responsible for it. The Army now felt it had to defend its personnel and installations from possible subversion, sabotage, and even guerrilla warfare. In response to these perceived menaces, USAINTC steadily widened its collection activities, and the files of the Intelligence Records Repository began to bulge with the names of individuals and groups with no connection to the Department of Defense except their reputed opposition to it.

---

[23] U.S. Army Intelligence Command Annual Report of Major Activities, FY 1971, p. 40, copy in INSCOM History Office files.

[24] Ibid., p. 41. Vance was not the only high government official interested in Army collection capabilities against civil disorders. In late 1967 Attorney General Ramsey Clark established the Inter-Divisional Information Unit in the Justice Department "to make full use of available intelligence." For the first two years of its existence, the unit drew heavily on Army counterintelligence for its data. Paul Cowan, Nick Eggleson, and Nat Hentoff, *State Secrets: Police Surveillance in America* (New York: Holt, Rinehart, and Winston, 1974), pp. 14–15.

The rioting that devastated the nation's capital following the assassination of Dr. Martin Luther King, Jr., was the final straw. In response, OACSI set up civil disturbance units in its Counterintelligence and Counterintelligence Analysis Branches in 1968, and the Department of the Army issued a classified Civil Disturbance Collection Plan levying intelligence requirements upon USAINTC that were so sweeping that they could not be filled by the traditional methods of overt collection or liaison with FBI and local law enforcement officials.

To accomplish the tasking, the command had to initiate an extensive collection program against domestic targets. And by now, Army Intelligence elements other than USAINTC were also involved in the domestic intelligence field. In an independent effort, CONARC and several Zone of the Interior armies had deployed counterintelligence personnel from their tactical units to engage in domestic collection operations and had compiled computer data bases on suspected potential troublemakers. The Army Security Agency had used its own assets on several occasions in 1967 and 1968 to monitor the demonstrators' citizen-band radios.

Even at the height of this type of activity, the bulk of USAINTC's resources remained committed to the traditional role of conducting background investigations. But the amount of activity devoted to domestic intelligence had a significance beyond its limited size. The perceived domestic crisis, coupled with Johnson administration demands for more and more information, led Army Intelligence into dangerous waters. Its activities crossed the traditional dividing line between the civilian and military in American life and overstepped the law, since neither the collection activities nor the civilian intelligence data bank of USAINTC had been authorized by statute.[25]

As early as 1969, after a change of administrations, Robert F. Froehlke, assistant secretary of defense for administration, expressed doubts about the wisdom of the whole operation. The Army went beyond its own requirements to involve itself in civilian concerns to such a degree, and the assistant secretary was concerned that the Army might be diffusing its limited intelligence assets, trying to collect intelligence on too large a portion of American society. As Froehlke ruefully admitted, the demands made upon USAINTC for domestic intelligence had gone "substantially beyond the capability for Military Intelligence units to collect. They reflected the all encompassing and uninhibited demand for information directed at the Department of the Army."[26]

What ended the Army's domestic intelligence program, however, was not doubts, but public exposure. In early 1970 the American Civil Liberties Union sued the Army and the U.S. Army Intelligence Command for "spying on civil-

---

[25] Christopher H. Pyle, *Army Surveillance of Civilian Politics, 1967–1970* (New York: Garland Publishers, 1970), is a scholarly account of the Army's domestic intelligence activities by a participant-observer and whistle-blower.

[26] U.S. Army Intelligence Command Report of Major Activities, FY 1971, p. 48.

ians."[27] The subsequent publicity, accompanied by recriminations from politicians and journalists, led not only to the end of this particular program, but ultimately to the end of USAINTC itself. The whole Army Intelligence community had suffered a major setback.

Beyond the Battle: Intelligence Trends in the 1960s

The Vietnam War and the domestic crisis within the United States were not the only forces exerting pressure on the structure of Army Intelligence during the 1960s. Increasing technology also shaped its development. This was especially important for the Army Security Agency. Personnel and financial constraints also impinged upon the structure of Army Intelligence during this period. The Army was engaged in fighting a large-scale war in Southeast Asia for which the country had never been properly mobilized. The short tours of duty in Vietnam caused constant personnel turbulence. The demands of the war gutted units outside the combat zone of equipment as well as people; ASA, with its dependence on high technology, was particularly affected. By the end of 1968 those ASA tactical units not actually committed to Vietnam, having been stripped of equipment and spare parts, delivered only 50 percent of their support requirements.

The financial problem was compounded in that the United States had an unfavorable balance of trade, and policy makers at the national level were constantly concerned with the bleeding away of America's gold reserves. Economic as well as technological considerations prompted the drive to consolidate many of ASA's European operations at a major new facility in Augsburg. Financial pressures were also partially responsible for the consolidation of the two Military Intelligence groups in Europe into a single unit in 1969. The headquarters of both the 513th and 66th Military Intelligence Groups moved to Munich, Germany, where the 66th absorbed the personnel and functions of the former.

Although Army Intelligence had its problems during this era, it improved its institutional position in a number of ways. One of the most significant advances was in professional development. As a result of a study undertaken by the Norris Board, the Army Intelligence and Security Branch was redesignated the Military Intelligence (MI) Branch on 1 July 1967. The new title symbolized the unity of the intelligence field rather than its diversity. More important, the Army assigned the renovated branch an official combat support function, whereas the old branch had been designated as a combat service support organization only.

---

[27] Palmer, *The 25-Year War*, p. 83. A surprisingly measured evaluation of what all this amounted to can be found in Cowan et al., *State Secrets*, p. 13. "The overall picture is of a moderately large bureaucratic apparatus built to conduct formal interviews for background checks and trying to do the impossible job of predicting major social disorders. It sponged off the FBI for most of its information and used plainclothes operatives for the rest. The information filled numerous computerized files, caused irrelevant briefings, and did little else—within the army."

The upgrade presented the prospect of attracting better officers to intelligence careers and providing members of the branch with greater access to the system of Army higher education that had become professionally indispensable for military career advancement.

As a step toward providing further integration of the various intelligence disciplines within the Military Intelligence Branch, in 1968 the U.S. Army Intelligence School began to offer an MI Officers Advanced Course intended for Army Security Agency officers, as well as for other Military Intelligence professionals. This step was taken in accordance with the recommendations of the Haines Board, another Army study group that had concentrated on deficiencies in intelligence training.[28] The new advanced course did not completely solve all the problems associated with the area, since the Haines Board's proposal to consolidate the Army Security Agency Training Center and School with the Army Intelligence School was not accepted, but the branch course represented a major step in breaking down the wall of isolation between signals intelligence officers and those with other intelligence specialties.

There were also new organizational developments. The Army Intelligence staff moved back into the field of intelligence production, as the Army soon discovered it had needs in this area that DIA could not fulfill. By 1966 OACSI's Special Research Detachment, originally set up as a liaison group with NSA, had become a full-fledged production center. The same year, OACSI created a threat analysis element to produce Army-specific studies. By 1967 even DIA had to admit that the task of conducting all Military Intelligence production simply was too great for one organization and agreed that the Army and the other services should provide "special finished intelligence" directly related to departmental missions.[29] Two years later, USAREUR organized its own production element, the U.S. Army Intelligence Center, Europe.

The Army's mechanism for disseminating its most secret intelligence also was expanded significantly. In 1965 ACSI had decided to attach special security offices to each Army division by fiscal year 1968. Although every Army division assigned to Vietnam had such support, the constraints on resources imposed by the fighting in Southeast Asia prevented implementation of the plan worldwide. However, the system expanded into other areas, as Army requirements for access to sensitive compartmented intelligence grew. In addition to servicing military and diplomatic needs, the Special Security Detachment increasingly became involved in providing private contractors with the highly classified information they needed to do research and development for the government. In 1967 the steady growth of these tasks led the Norris Board to recommend that the Army establish four geographic Special Security regions to act as subor-

---

[28] Powe and Wilson, *The Evolution of American Military Intelligence*, p. 105.

[29] Intelligence Organization and Stationing Study (IOSS), Aug 75, Exec Sum, p. 29, copy in INSCOM History Office files.

dinate headquarters for the Special Security Detachment's fifty-five field offices. The recommendations were accepted, and shortly afterward the status of the detachment was upgraded to that of a "group" headquarters.

The Army Security Agency was substantially restructured during the course of the 1960s. TOE units were reintroduced to the United States and Vietnam, and in 1966 all the agency's battalions were converted from a fixed to a flexible structure. There were also more cosmetic changes. At the end of 1967 the Department of the Army decided that TDA units would no longer bear numerical designations. As a result, on 15 December 1967, the Army Security Agency's numbered field stations, special operations commands, and special operations units received new geographic designators. Finally, the Army undertook some qualitative initiatives in the human intelligence field, even though resources and personnel allocated to this area declined steeply after 1963. In 1969 ACSI organized a field operating agency to direct certain programs in this area.

Westmoreland, McChristian, and Military Intelligence

In mid-1968 the former MACV commander, General William Westmoreland, became the Army chief of staff and subsequently supervised three major organizational changes within Army Intelligence. The first came about in 1969, when Westmoreland reviewed the organization of the Army Staff and decided that the number of field operating agencies under ACSI's direct supervision was not compatible with the proper organization of a DA staff element. ACSI's job, in Westmoreland's estimation, entailed staff supervision and program management, not operations. As a result, OACSI underwent a sweeping reorganization. Six major elements were spun off and resubordinated to USAINTC. These included the 902d Military Intelligence Group, which had previously performed high-level counterintelligence operations under direct ACSI control; the Administrative Survey Detachment, which ran Army Intelligence personnel programs; the Personnel Security Group, which adjudicated loyalty and suitability cases for the Army; the Army Imagery Interpretation Center; the Intelligence Materiels Supply Office; and the newly created field operating agency for human intelligence.[30]

In certain ways, the new reorganization amounted to another reinvention of the wheel. At the Army Staff level, it meant returning to the organizational principles originally adopted during World War II. The U.S. Army Intelligence Command was transformed from the continental United States–focused counterintelligence organization originally planned into a simulacrum of the earlier U.S. Army Intelligence Corps Activity. In addition, however, the command assumed control of sensitive operations heretofore controlled only at the DA

---

30 *Department of the Army Historical Summary, Fiscal Year 1970* (Washington, D.C.: U.S. Army Center of Military History, 1973), p. 82.

level, a trend strengthened in 1972 when OACSI transferred its Special Research Detachment to the command.

A second change that came about at this time was an enlargement of OACSI's area of functional responsibilities. Army Intelligence had delegated oversight of the Army's mapping work to the chief of Engineers since World War II. In 1969 Westmoreland directed ACSI to assume staff supervision of certain Army topographic activities, and the Engineer Topographic Command was created to carry out the map-making function by consolidating the Army Map Service with other Engineer elements involved in topography. ACSI also took over staff supervision of Army weather intelligence at this time.

The last organizational innovation of the Westmoreland years initially promised to be the most sweeping. Early in 1969 the ACSI, Maj. Gen. Joseph A. McChristian, who had served as Westmoreland's J–2 in Vietnam, concluded that the Army's fragmented intelligence assets in the continental United States were too physically dispersed to provide the Army with enough support. Reviving the old proposal of the 1950s, he recommended concentrating them in a single intelligence center. The proposal did not, however, touch upon the operations of the Army Security Agency.

McChristian initially had an ambitious concept for the center. It would concentrate in one location an operational intelligence headquarters much like the one McChristian had set up in Vietnam, a counterintelligence center (essentially USAINTC), the U.S. Army Intelligence School, support troops, and tactical units. This would give many elements of the Army Intelligence community a home for the first time. The tactical units and aircraft would be necessary because McChristian felt that one of the center's main purposes would be to give the troops realistic intelligence training in the field. The first plans called for the center to have a troop base of 21,000.

The existing Army Intelligence center at Fort Holabird, Maryland, was obviously unsuited for such an expanded role. The post was small, and the training requirements imposed by the Vietnam War had greatly overcrowded it. The post was hemmed in by an industrial area that precluded expansion. Although the streets of Baltimore were as good a place for counterintelligence agents to practice surveillance techniques as anywhere, Holabird offered no room for field maneuvers. In addition to all these liabilities, the air space in the area was overcrowded, and the electromagnetic environment was cluttered. In a search for an alternative, the initial survey team narrowed the choice to Fort Riley, Kansas, and Fort Huachuca, Arizona, and selected the latter.

At this point, the plan for a new Army Intelligence center began to narrow sharply in scope. Planners soon realized that although Fort Huachuca offered space, it had little water. McChristian then suggested that Fort Lewis, Washington, might be developed as an alternative site, but the post would have needed extensive rehabilitation, and this would take too much time and money. Because of these constraints, the proposed composition of the center shrank,

and then shrank again. It turned out that Fort Huachuca could not comfortably accommodate even a brigade of supporting troops. Originally, planners had thought that the U.S. Army Intelligence Command would move bodily to the new center, leaving behind a kind of USAINTC rear, consisting of a Directorate of Investigative Records to administer the command's bulky and hard-to-move data base. This idea was scrapped also. Since most of USAINTC's activities were in support of the Department of the Army and other national-level agencies, the command could not practicably move beyond the Washington-Baltimore corridor.

Ultimately, the composition of the new Army Intelligence center was scaled down drastically. The final version of the center included the Army Intelligence School and the U.S. Army Combat Development Command Intelligence Agency, together with Army combat surveillance and electronic warfare activities already in place at Fort Huachuca, all of this supported by a bare minimum of tactical units. As part of the process, the Army Intelligence School was redesignated and given the more prestigious title of the U.S. Army Intelligence Center and School. The school moved to its new desert home at Huachuca in phases during the first part of 1971.[31] By this time, events were in process that would be much more damaging to Army Intelligence than the reduced plans for its new center.

Lean Years

The early 1970s saw the U.S. Army in decline. The decision to stage a phased withdrawal from Vietnam led to a drastic cut in troop strength, and between 1969 and 1973 the Army shrank in size by almost half, from a force of 1.5 million to one of 800,000. More important, its ranks were plagued with incidents of drug abuse, racial turmoil, and lack of discipline. The final elimination of the draft in 1973 deprived the Army of its reservoir of college-trained enlisted men and confronted it with daunting recruitment problems. Operating in an environment of constraints, the Army would have to rely increasingly on reserve forces to meet any future combat contingencies. The STEADFAST reorganization of 1973 made this dependence on the reserve components explicit, in addition to retrenching the Army Staff and realigning much of the Army's command structure.[32] If the Army as a whole struggled during this period, Army Intelligence was particularly hard hit. It fell victim not only to popular disillusionment with the results of the war, but also to public indignation against alleged counterintelligence abuses.

The unraveling of the Army's domestic counterintelligence program began in the first months of 1970, when the American Civil Liberties Union initiated a lawsuit against the Department of the Army and the U.S. Army Intelligence

---

31 Dr. Bruce Saunders, "U.S. Army Intelligence Center and School," *Military Intelligence* 10 (April–June 1984): 61.

32 *Department of the Army Historical Summary, Fiscal Year 1973* (Washington, D.C.: U.S. Army Center of Military History, 1977), pp. 45–46.

Command on the grounds that they were involved in illegal surveillance of civilians. The initial suit was followed by a fire storm of adverse media publicity, all of which culminated in a congressional investigation in early 1971. The controversy had immediate effects on USAINTC. On 19 February 1970, all civil disturbance and civilian biographic data stored in the Investigative Records Repository were ordered destroyed. A similar purge was ordered of the independent domestic intelligence data bases maintained by CONARC and several of the field armies in the continental United States. The ambitious Civil Disturbance Information Collection Plan was formally rescinded in June. The U.S. Army Intelligence Command went into a 180-degree reversal, of course. As the command's official historian stated, "instead of collect, process, and store, the order of the day was research, screen, and destroy."[33] The effect of the "spying on civilians" charges was to degrade the whole counterintelligence mission. By the end of February 1971 the Army had suspended all USAINTC counter-subversive and offensive counterespionage activities.

These new developments soon affected the organizational structure of Army counterintelligence. On 1 March 1970, the Defense Investigative Review Council was set up under the assistant secretary of defense for administration to exercise general supervision over the counterintelligence activities of all the armed services and to curb any possible abuses. After some deliberation, the council decided to centralize all service-connected background investigations under a new civilian body, the Defense Investigative Service, which was established at the end of 1971 and became operational in October 1972.[34] Meanwhile, contrary opinions had been voiced. In June 1970 presidential assistant Frederick Huston, unnerved by the depth of dissent over the recent American incursion into Cambodia, suggested that all government intelligence agencies conduct their operations without regard to legal or Constitutional niceties. His views did not prevail.[35]

The formation of the Defense Investigative Service was the beginning of the end for the U.S. Army Intelligence Command as a major Army headquarters. Conducting standard personnel background investigations had been the command's bread and butter, constituting 90 percent of its work load. USAINTC had to give up 1,400 personnel spaces to the new agency. Three of its Military Intelligence groups were inactivated, and the number of field offices was reduced from 303 to 50. The command turned over control of the Defense Central Index of Investigations and the National Agency Check Center to the Defense Investigative Service. USAINTC retained custody of Army counterintelligence files, but the criminal investigation records held by the Intelligence

---

33 U.S. Army Intelligence Command Report of Major Activities, FY 1971, p. 219.

34 *Department of the Army Historical Summary, Fiscal Year 1973*, pp. 53–54.

35 Theodore H. White, *Breach of Faith: The Fall of Richard Nixon* (New York: Dell Publishing, 1976), pp. 174–77.

Records Repository were removed from its control and assigned to a new U.S. Army Criminal Investigation Command. Since 1949 a major general had controlled Army counterintelligence activities. By 1972 the U.S. Army Intelligence Command was under the command of a colonel.

After the Army Intelligence School moved to Fort Huachuca, Fort Holabird became superfluous to Army Intelligence. In the interests of economy, USAINTC relocated in the summer of 1973 to Fort George G. Meade, Maryland, a large, multipurpose post. However, since the records of the Army Criminal Investigation Command remained behind at Holabird, the move was a further blow to the concepts behind the SECURITY SHIELD study of 1964. By 1974, USAINTC had lost most of its mission responsibilities and numbered less than 2,000 persons. In addition, the Office of the Secretary of Defense criticized that the Army's counterintelligence structure was top heavy in management and not cost effective.

USAINTC's remaining activities hardly seemed significant enough to warrant its retention as a major command, especially at a time when the Army was under heavy pressure to reduce its headquarters establishments. The command was particularly vulnerable to charges of managerial layering—it shared Fort Meade with the headquarters of a major subordinate unit, the 109th Military Intelligence Group. Another major element, the 902d Military Intelligence Group, had been programmed to move to Fort Meade in the summer of 1974. As a result, the Army discontinued the command on 30 June 1974.[36] On the same day, the Army also inactivated USAINTC's three remaining Military Intelligence groups with area responsibilities for the continental United States and reassigned the Army Imagery Interpretation Center and Special Research Detachment to ACSI's direct control.

USAINTC was replaced by the U.S. Army Intelligence Agency, a field operating agency directly subordinated to ACSI with an initial force structure of just two CONUS counterintelligence groups: the 902d Military Intelligence Group, which lost its traditional high-level mission and became responsible for the geographic area east of the Mississippi, and the 525th Military Intelligence Group, of Vietnam fame, which was reactivated to perform a parallel mission in the western part of the United States. The agency inherited (sometimes in rearranged form) some smaller miscellaneous elements from USAINTC: a technical service activity providing polygraph, technical service countermeasures, and computer security assistance; the U.S. Army Counterintelligence Support Activity, comprising the Investigative Records Repository and the Personnel Security Group; and the Administrative Survey Detachment.

USAINTC was not the only part of the Army Intelligence community affected by the currents of the times. Centralization and economy were the watch-

---

[36] *Department of the Army Historical Summary, Fiscal Year 1974* (Washington, D.C.: U.S. Army Center of Military History, 1977), p. 42.

words of the day. In 1970 a blue ribbon panel appointed by President Nixon had called for much greater integration of service intelligence activities at the DOD level. The Defense Investigative Service was just one of three new Department of Defense agencies that the Nixon administration created to assume intelligence functions which the uniformed services previously had performed. In 1972 the Army topographic assets that ACSI had supervised since 1969 were integrated into the new Defense Mapping Agency.[37] During the same year, an attempt was made to integrate all service cryptologic elements into a Central Security Service that would act as the military arm of the National Security Agency. This threatened to strip the Army of much of its remaining role as a manager in the cryptologic field. In practice, however, the Central Security Service did not live up to its initial expectations, and the reorganization did not bring about any substantial change in the relationship between the Army Security Agency and the National Security Agency.

The Army Security Agency, although still the largest single intelligence element in the Army, shared the problems of the greater Army during this period. It had to deal with strength ceilings, recruiting problems, and diminished funding. Additionally, it suffered from the problems caused by a large shortfall of equipment and spare parts in the field. As a result of the demands of the war in Vietnam, much of the remaining equipment was obsolete and ill suited to the demands of a high-intensity conflict.

The retrenchment of the agency began in 1970, when it turned over its acoustical intelligence mission to the U.S. Air Force. In 1971 the Army discontinued the 507th and 508th U.S. Army Security Agency Groups, located respectively in Europe and in Korea, and replaced them with smaller elements: the 502d Army Security Agency Group, a TOE unit, in Europe and an unnumbered field station in Korea.[38] The reduction continued inexorably as the agency stood down from Vietnam and closed long-established field stations. Of the 99 separate units which ASA fielded in 1970, only 73 still existed in 1972. For reasons of economy, ASA's traditional regional headquarters in Europe and the Pacific were discontinued in 1972.

Meanwhile, the approaching end of the draft made questionable whether the Army Security Agency could enlist enough men to meet mission requirements. As a result, for the first time in its history the agency began recruiting women for cryptologic specialties. Although WACs had served with the SSA's 2d Signal Service Battalion in the continental United States during World War II, the WAC detachment stationed at Arlington Hall at the time of the Korean con-

---

[37] *Department of the Army Historical Summary, Fiscal Year 1972* (Washington, D.C.: U.S. Army Center of Military History, 1974), p. 44.

[38] The discontinuance of the 508th USASA Group in Korea in 1971 took place in the context of a major reduction in troop strength there. This drawdown was part of the implementation of the "Nixon Doctrine," which sought to shift the main burden of providing ground forces for defense to our allies.

flict had performed largely administrative functions. By 1976, however, one-tenth of ASA's uniformed personnel worldwide were female.

Although the Army Security Agency was deeply affected by developments in the cryptologic field, it survived the STEADFAST reforms intact. STEADFAST had resubordinated almost all Army training centers, including the U.S. Army Intelligence Center and School, to the newly created Training and Doctrine Command (TRADOC), but ASA's vertical command structure allowed it to retain its own training base. However, the 1973 reorganization of the Department of the Army did have its effect on Army Intelligence at the staff level. In line with the thrust of STEADFAST, the staff of the Office of the Assistant Chief of Staff for Intelligence was reduced by one-third between 1973 and 1974.[39] Production and support functions previously carried out within OACSI were transferred to separate detachments with their own TDAs in 1973, and responsibility for administering attache personnel was transferred to the Administrative Survey Detachment in 1974.

A Time of Transition

After the setbacks of the early 1970s, Army Intelligence began to regroup. Even though it operated under continuing personnel and fiscal restraints, the Army Intelligence community undertook a series of initiatives that would put it in a better position to respond to future challenges.

The U.S. Army Intelligence Agency (USAINTA), established in mid-1974, was originally intended as a low-profile organization with the narrowly limited mission of conducting the Army's residual counterintelligence operations in the continental United States. The assets initially assigned to the new agency were modest. Moreover, its mission was constrained and its activities hampered by congressional legislation, congressional investigations, and executive orders that cumulatively had a chilling effect on counterintelligence operations.[40] By early 1975 the agency's Investigative Records Repository was required to establish a Freedom of Information Act Office to respond to queries from the public about the contents of the Army's files. However, the agency came into existence just at the time that the disestablishment of U.S. Army, Pacific, made it necessary to resubordinate USARPAC's 500th Military Intelligence Group, primarily a collection element. For want of any more plausible arrangement, the Army gave the U.S. Army Intelligence Agency command of the orphaned group, thus acquiring an area of overseas intelligence responsibility that had been denied its predecessor, USAINTC. Since

---

[39] *Department of the Army Historical Summary, Fiscal Year 1974*, p. 38.

[40] A telling indication of the disfavor into which any type of military counterintelligence operation had fallen at this time was Congress' decision in 1974 to discontinue all military censorship units in the reserve components.

the 500th Military Intelligence Group no longer had the mission of supporting a major Army headquarters in Hawaii, it redeployed to Japan in the summer of 1976.

The Army's desire to realign its counterintelligence command and control system to better satisfy the civilian leadership also contributed to the expansion of the U.S. Army Intelligence Agency's geographical area of responsibility. The Defense Investigative Review Council established guidelines that prohibited Army investigations of non–DOD-affiliated civilians within the fifty states and the Panama Canal Zone, but less stringent prohibitions were in effect overseas. To ensure uniform adherence to these policies, it seemed wise to bring all counterintelligence operations within the council's jurisdiction under the control of a single agency. This again resulted in USAINTA's assuming responsibilities that USAINTC had never exercised. The U.S. Army Intelligence Agency gained control of counterintelligence investigations in the Canal Zone and Hawaii and was assigned command of the 901st MI Detachment, which previously had reported directly to the Defense Nuclear Agency. Moreover, the command began to diversify the scope of its activities, upgrading and redesignating its technical services element as the Operational Security Group and embarking on initiatives in collecting human intelligence.

ACSI's Special Security Group also expanded its activities. With the fighting in Vietnam over, the group could at last find enough resources to implement its long-delayed plan to provide each Army division with a special security office. Experience gained in Vietnam had demonstrated this to be a necessity under conditions of modern warfare.

The Army Security Agency also began to evolve in fresh directions. The first step was to give ASA's signal security activities in the Western Hemisphere an organizational base that would conform to the new doctrine that stressed providing advice and support to commanders on signal security issues, rather than monitoring communications to detect violations. This concept emphasized the positive aspects of security rather than the negative, and it allowed ASA to deal with the possibility that improperly secured electronic equipment could now pose as much of a security hazard as badly trained communications personnel. To facilitate this approach, the agency organized the Signal Security Activity at Vint Hill Farms Station in June 1975.

The Signal Security Activity took over a support function that previously had been fragmented among eleven separate units in the continental United States, Alaska, and the Canal Zone. Four subordinate field detachments, each with a TEMPEST capability, monitored the possibility of information compromise from electronic emanations. At the same time, the Army shifted general staff supervision over the communications security/signal security area from ACSI to the assistant chief of staff for communications and electronics. Among its other advantages, the transfer distanced the Army Security Agency from any further charges of "spying on civilians."

Even more important for the Army Security Agency was the growing importance of electronic warfare, part of the agency's mission since 1955. In 1969 the Joint Chiefs of Staff expanded the definition of electronic warfare beyond the accepted "jamming" and "antijamming" roles to encompass the new concept of electronic support measures, which embraced threat detection and avoidance, targeting, and homing. Because of the nature of the combat situation in Vietnam, electronic warfare had played almost no role in that conflict. However, the rapid development of electronic warfare technology and the emphasis given to "radioelectronic combat" in the fighting doctrine of what was then the Army's most probable future adversary made it clear that things would be very different in any potential high-intensity war.[41]

Unfortunately, the agency's traditional emphasis on its cryptologic mission and the damage the Vietnam conflict had caused, both to equipment readiness and to research and development, had left it poorly positioned to meet the electronic warfare threat. In 1972 the Army's Scientific Advisory Board estimated that less than 10 percent of Army Security Agency resources were devoted to electronic warfare and pointed out that much of the available equipment was obsolete.

In response, the agency began to restructure itself to give greater electronic warfare and signals intelligence support on the tactical level. Aerial platforms were fielded in Europe and Korea, and the agency began to develop new types of units that could integrate signals intelligence with electronic warfare. These units were to coordinate with the tactical formations they supported through ASA-manned elements within unit tactical operations centers responsive to the needs of both the intelligence and operations staff officers. The events of the Arab-Israeli War of 1973 gave a striking demonstration of the importance of electronic warfare even in a mid-intensity conflict. In the aftermath of this conflict, Maj. Gen. George Godding, commanding general, U.S. Army Security Agency, proposed that his organization be redesignated the U.S. Army Electronic Warfare Command. Although the proposal was not accepted, it showed that ASA was now prepared to redefine its traditional mission.

By the end of 1974 the structure of Army Intelligence was in flux. It was still adjusting to painful shortages of money and personnel, while at the same time major components of the Army Intelligence community were moving in new directions. However, changes were being made on a piecemeal basis, without any overall plan or centralized guidance. The Army secured a chance to impose a new coherence on its intelligence structure on 31 December 1974, when the chief of staff directed the implementation of a comprehensive study he hoped would impose some cohesion on the many significant changes in process.

---

[41] Don E. Gordon, *Electronic Warfare: Element of Strategy and Multiplier of Combat Power* (New York: Pergamon Press, 1981), p. 153.

10

Reorganization and Renewal

The year 1975 marked a low point for both America's influence on the international scene and the institutional position of the Army. The growing power of the Organization of Petroleum Exporting Countries (OPEC), first manifested at the time of the Yom Kippur War, seemed to threaten the economies of the Western industrialized world in an unprecedented way. The Watergate scandal and the subsequent resignation of President Richard Nixon under threat of impeachment had damaged the confidence of the nation in its government and had effectively undercut the foreign policy strategies with which President Nixon had been identified. Southeast Asia fell to Communist armies in 1975, and Soviet-backed regimes came to power in Angola and Mozambique. The Army, underfunded and unpopular, was hard pressed to fill its ranks with quality personnel without the stimulus of the draft. It was under these unpromising circumstances that the Army drew up a new charter for intelligence, which emerged as a result of the Intelligence Organization and Stationing Study (IOSS).

The disillusionment resulting from the nation's long involvement in Southeast Asia was slow to dissipate. Nevertheless, the Iranian hostage crisis, the Soviet invasion of Afghanistan, and continued instability in Central America gradually fostered a renewed interest in American security. Although the nation attempted to put the Vietnam experience behind it, there was no return to isolationism. From 1979 on, the country began to accelerate the buildup its defenses. By the mid-1980s the Army's morale and strength had been restored, a new generation of weapons for ground combat fielded, and the force structure increased. During this period the IOSS reforms, conceived in an environment of tight resources, continued to provide a viable architecture for Army Intelligence in a plentiful time for the Army and for intelligence operations in general.

Remaking Military Intelligence

The Intelligence Organization and Stationing Study originated in a 1974 memorandum from Secretary of the Army Howard Callaway to Army Chief of

Staff General Frederick Weyand. "We maintain considerable information which is of questionable value and seldom used," Callaway noted, and that "really makes me wonder about how much money we are wasting and raises serious questions as to the cost-effectiveness of our intelligence system."[1]

In addition, broader considerations made an overall assessment of Army Intelligence appropriate. Army Intelligence resources for the 1974–1978 time frame had already been reduced significantly by a program-budget decision of the secretary of defense in 1973. The Army inspector general had recently found grave deficiencies in the operations of the Army Security Agency. The dismantling of the U.S. Army Intelligence Command, which had just occurred, meant that the Army counterintelligence and human intelligence organization was in the process of evolution. At the tactical level, the STEADFAST reorganization had abolished the field army command, leaving without a mission the MI tactical units designed to support it. Finally, the Army in general realized that an overall appraisal of the intelligence structure was long overdue. Too many intelligence elements within the Army had been allowed to evolve apart from the development of the Army as a whole. It now seemed time to align Army Intelligence with the rest of the Army. The chief of staff entrusted the initial steps to a panel headed by Maj. Gen. Joseph J. Ursano.

After an exhaustive study of the structure and organization of Army Intelligence, the panel submitted its findings and recommendations in August 1975. The IOSS report was critical. It pointed out that the organization of the ACSI staff did not facilitate effective supervision of the Army's most crucial intelligence resources. The Directorate of Foreign Intelligence, ACSI's major contact point with the rest of the Army Staff and the other functional major Army commands (MACOMs), had only half the resources allotted to the staff elements supervising intelligence collection. Priorities within collection itself were even more skewed. Staff supervision of human intelligence took up a disproportionate amount of effort. The vital signals intelligence function was isolated and neglected.

The panel found intelligence production fragmented. Various aspects of production were being carried on by several ACSI elements as well as the Forces Command; other production elements operated under the Army Materiel Command and the Office of the Surgeon General. The disparate system fully satisfied only a portion of the Army's intelligence needs. Only a unified production center would, in the panel's judgment, alleviate the situation. Specific collection efforts also came under criticism.

The Ursano panel estimated that in the security field some 80 percent of the Army effort went into operations designed to counter the threat from foreign human intelligence organizations, and the remaining 20 percent was devoted to signal security. These were old and familiar functions, carried out respectively

---

1 IOSS, Aug 75, Exec Sum, p. 6.

by the U.S. Army Intelligence Agency and the Army Security Agency. But there was no effort directed against hostile imagery intelligence and no organization handling the total security picture and providing support to operations security (OPSEC). The panel concluded that as a result the allocation of security resources was wildly disproportionate to the existing threat.

The panel reserved some of its most stinging criticism for the Army Security Agency. The establishment of the National Security Agency/Central Security Service organization, it found, had essentially reduced ASA headquarters to just another bureaucratic layer. Lacking any operational responsibilities or a core of technical cryptologic experts, it was saddled with an immense span of control because of the closing of the various ASA theater headquarters. The Ursano board noted that field commanders could readily assume ASA's remaining support functions. Moreover, despite its best efforts, the agency was not meeting the Army's tactical requirements, since it could not field enough units to support the planned sixteen-division Active Army.

A succession of previous Army reviews—in all, eleven had been made since World War II—had upheld the validity of the Army Security Agency's traditional vertical command structure. The Ursano panel dissented vigorously. In the panel's opinion, the ASA pattern of organization had actually impeded the development of an efficient mechanism for carrying out intelligence and electronic warfare. The monopoly of signals intelligence and electronic warfare by an organization operating under compartmented secrecy had artificially kept signals intelligence out of the general intelligence flow and had largely excluded the rest of the Army from involvement in the vital electronic warfare field. At the same time, ASA's preoccupation with the cryptologic aspects of its mission had prevented it from keeping up with new trends in electronic warfare, despite the emphasis which the Army now had given to the latter function.

In the field, the IOSS report charged, the Army Security Agency's organizational and functional independence worked against the effective integration of all-source intelligence that was now necessary. It also imposed substantial administrative costs, since unit G–2s at tactical operations centers had to coordinate the intelligence flow produced by three separate elements: ASA, regular Military Intelligence units, and the special security officer dissemination system. Each of these elements had its own separate communications system and its own separate support system.

The Intelligence Organization and Stationing Study: Solutions

The Ursano panel recommended radical surgery to correct the perceived deficiencies of the Army Intelligence structure. Its complex prescription called for both centralization and decentralization. The heart of the suggested program, however, was dismantling the Army Security Agency. ASA's tactical units

should be resubordinated to field commanders and its training and research and development functions assigned to other major commands in conformity with the pattern which the McNamara reforms and the STEADFAST reorganization of 1973 established for the rest of the Army. The IOSS report offered three alternatives for realigning Army strategic and theater support intelligence assets. Under the proposal finally adopted, the Army Security Agency's headquarters and fixed field stations would become the core of a new major command. By adding the U.S. Army Intelligence Agency, those Military Intelligence groups engaged in a theater support role, and the various intelligence production elements to this base, the Army would create, for the first time, an integrated intelligence, security, and electronic warfare organization capable of fulfilling its national requirements.

At the tactical level, the proposals called for organizational decentralization and functional integration. With the dissolution of ASA's vertical command structure, ASA and MI field units could merge into a single system of unified intelligence and electronic warfare forces. In the committee's view, tactical Special Security Offices could become part of the units they supported. Army tactical commanders at the corps level and below would thus for the first time have substantially the same control over their intelligence assets as they did over the rest of the forces assigned to them. Signals intelligence would be merged into the all-source intelligence needed to meet tactical requirements.[2]

The recommendations raised a number of questions, one of which involved the issue of acceptability. The commanding general of the Army Security Agency, Maj. Gen. George Godding, rather predictably did not concur, not only because of the impending dismemberment and transformation of his organization, but also because of the proposed reorganization's possible effect on cryptology. On the whole, however, the Army's response was very positive. The new arrangements seemed to be designed to give the commander in the field what he wanted. The response from USAREUR, for instance, not only expressed support for the concept, but also demonstrated Army reservations about some of the features previously associated with intelligence work: "MI is fighting its way back to acceptance by the Army community. Stovepiping and restoring the 'spook' image must be avoided."[3] Under the IOSS concept, Army Intelligence would march in step with the rest of the Army, a prospect that pleased many.

One question which the Intelligence Organization and Stationing Study left unresolved was that of command. The ACSI suggested that control of the proposed new intelligence and security command be vested in himself. This arrangement would have given Army Intelligence an institutional structure strongly resembling that of World War II, when the G–2 had controlled the

---

2 *Department of the Army Historical Summary, Fiscal Year 1976* (Washington, D.C.: U.S. Army Center of Military History, 1977), pp. 25–26.

3 IOSS, Aug 75, vol. 1, ch. 8, ann. B, p. 2.

Military Intelligence Service and after 1944 the strategic operations of the Army Signal Security Agency.

This proposal was rejected, however, and the new major command was allotted a commander of its own. The ACSI suggestion ran against the doctrine that staff and line functions should be separated, and it posed another problem. After the adverse publicity of the early 1970s, intelligence was still a sensitive field. At the time Army leadership believed that any merger of policy formulation and program management functions with operational capabilities would "deny the CSA [chief of staff of the Army] a check and balance mechanism believed necessary in today's environment of sensitivity to intelligence activities."[4]

Implementation of the IOSS proposals began in 1976. The Army realigned elements within OACSI, initiated staff planning for a new intelligence and security command, and fielded the first experimental intelligence and electronic warfare battalion. The U.S. Army Security Agency Training Center and School at Fort Devens, Massachusetts, was resubordinated to the U.S. Army Intelligence Center and School at Fort Huachuca, along with its two detachments at Goodfellow Air Force Base, Texas, and the Navy facility at Corry Station, Florida. This shift achieved the long-standing Army goal of centralizing all Military Intelligence training and further enhanced the importance of the Army Intelligence Center and School itself. The latter organization already had achieved the status of a general officer command after absorbing the Combat Developments Command Intelligence Agency and the Combat Surveillance and Electronic Warfare School. In 1983 the rank of the Army Intelligence Center and School commander was elevated to two stars after the commander received proponency over the Military Intelligence Branch and assumed the title of chief of Military Intelligence.[5]

In addition, the Special Security Group was radically reorganized, losing its operational role in communications and its tactical elements. By the end of 1976 tactical special security offices came under the control of ASA direct support units. Ironically, the Army Security Agency achieved the control over this organization, which it had sought for twenty years, just before its own demise. Concurrently, the Army restructured what remained of the Special Security Group along functional rather than regional lines through seven special security commands, each of which controlled subordinate offices servicing different major commands.[6] The culmination of the IOSS reorganization came on 1

[4] IOSS, Aug 75, vol. 1, ch. 8, p. 61.

[5] Saunders, "U.S. Army Intelligence Center and School." The transfer of MI Branch proponency to the commandant of the U.S. Army Intelligence Center and School took place as part of an Army-wide shift of this function from the Army Staff to the TRADOC schools. Proponency allowed the chief of Military Intelligence to initiate and coordinate actions in the areas of force structure, unit deployment and sustainment, and personnel acquisition, training, and distribution. It did not, however, give him control over individual career management.

[6] History of United States Army Special Security Group, n.d., p. 6, INSCOM History Office files.

January 1977, with the formation of the U.S. Army Intelligence and Security Command (INSCOM) at Arlington Hall Station, Virginia.

New Directions for Military Intelligence: INSCOM

The Army formed the new major command, INSCOM, by redesignating the U.S. Army Security Agency as the U.S. Army Intelligence and Security Command and reassigning the U.S. Army Intelligence Agency, as well as ACSI's and FORSCOM'S intelligence production units, to the new command.[7] At the same time, control of ASA's tactical units reverted to the supported commanders. The training, personnel, research and development, and materiel acquisition and administration functions which the Army Security Agency had carried out were assumed by other major commands and by elements of the Army Staff. INSCOM also assumed command of three Military Intelligence Groups located overseas: the 66th in Germany, the 470th in Panama, and the 500th in Japan. Previously, these units had been assigned respectively to USAREUR and Seventh Army, FORSCOM, and the U.S. Army Intelligence Agency. Despite the similarity of their designations, these groups varied widely in size and mission; moreover, theater commanders continued to exercise operational control over the units. On 1 October 1977, the former U.S. Army Intelligence Agency headquarters became part of INSCOM, and the command established a unified intelligence production element, the Intelligence and Threat Analysis Center, on 1 January 1978.

INSCOM provided the Army with a single instrument to conduct multidiscipline intelligence and security operations and electronic warfare at the level above corps and to produce finished intelligence tailored to the Army's needs. The new major command merged divergent intelligence disciplines and traditions in a novel way. Its creation marked the most radical realignment of Army Intelligence assets in a generation. Without fully realizing it, the Army had achieved not a "multidiscipline" organization, but an interdisciplinary approach to intelligence collection. The new command provided Army Intelligence with a framework within which the individual intelligence disciplines could cross-cue one another; the results of this collective effort would be greater than the sum of its parts.

Traditionally, the Army Security Agency had been the centerpiece of the Army Intelligence community in terms of personnel and resources. When the agency melded into INSCOM under the new realignment, it lost its vertical command structure, many of its functions, and thirty of its tactical units. As a result, Brig. Gen. (later Maj. Gen.) William I. Rolya, the former ASA commanding general who became INSCOM's first head, found himself heading an organization considerably smaller than its predecessor, although it had gained the U.S. Army Intelligence Agency, the theater Military Intelligence groups, and produc-

---

[7] *Department of the Army Historical Summary, Fiscal Year 1977* (Washington, D.C.: U.S. Army Center of Military History, 1979), pp. 30–31.

tion elements. However, the U.S. Army Intelligence and Security Command had at its disposal a wide array of diverse assets. Initially, these included eight fixed field stations inherited from ASA—three of them in the Far East, two in the continental United States, two in Germany, and one in Turkey. There were also the three intelligence groups overseas, transformed into multidisciplinary units by incorporating former ASA assets into the previously existing elements. A fourth, the 501st Military Intelligence Group, was soon organized in Korea. Because of Eighth Army's special requirements, the unit not only carried out a theater support mission, but also performed functions executed elsewhere by the Army's corps-level intelligence organizations.

In the continental United States, INSCOM received command over various single-discipline elements: the Intelligence and Threat Analysis Center; the CONUS MI Group, which furnished cryptologic personnel to the National Security Agency and controlled the two field stations in the United States; an expanded 902d Military Intelligence Group, which was assigned a combined counterintelligence and signal security support mission throughout the continental United States; the Central Security Facility, which maintained the counterintelligence records in the Intelligence Records Repository; and a number of other specialized subordinate units. Significantly, one function which the Central Security Facility previously performed—the adjudication of Military Intelligence–related and other sensitive clearances within the Army—shifted in October 1977 to a new Central Clearance Facility administered by the Military Personnel Center. This was done partially to further standardize the clearance process throughout the Army, secondarily to remove the process from Army Intelligence control, on the grounds that the investigative function should not be combined with the judicial.

With the U.S. Army Intelligence and Security Command in place, ACSI found it expedient to surrender control of most of the remaining operating functions to the new organization. Ever since the 1950s, the ACSI's operating responsibilities had waxed and waned cyclically as various incumbents transferred control of field operating agencies back and forth between OACSI and Fort Holabird. Now came another turn of the wheel. In 1978 INSCOM took over the Army's Russian Institute in Germany and in 1980 assumed command of the Special Security Group. A year later, OACSI discontinued its Inspector General's Office, since substantially all of its field activities had gone to INSCOM, and there was little in the field to inspect.

The U.S. Army Intelligence and Security Command faced certain problems when it started out. At first it was hampered by a shortage of resources. By the end of fiscal year 1978 only 10,400 people were assigned to the new command, debilitating shortages in key Military Intelligence specialties existed, and the command found itself unable to completely meet all the national collection requirements with which it had been tasked. However, the readiness situation improved steadily, as a new national consensus regarding the importance of

intelligence brought a greater infusion of resources. By 1985, 15,000 persons were assigned to INSCOM.[8]

The command's institutional and structural problems took longer to solve. INSCOM was designed to perform intelligence and security operations at the echelon above corps, but the precise structure of this echelon continued to be a matter of doctrinal dispute within the Army. The Army's traditional echelon above corps, the field army, had been discontinued in 1973 and replaced with a joint command system. INSCOM's broad responsibilities and the diverse nature of the units it commanded posed another problem. Proposals were made to simplify the command structure by creating additional subordinate headquarters overseas, as the Army Security Agency had done originally, but overseas headquarters elements proved expensive, and INSCOM finally abandoned this approach. Additionally, the command's exact role in electronic warfare remained undefined. Although INSCOM was the main proponent, its units were limited in this area.

The field of intelligence production also continued to present difficulties. The IOSS panel had originally recommended that all Army Intelligence production resources be brought together in a single location. However, Army leaders decided that the Army's scientific, technical, and medical intelligence production responsibilities would continue to be dispersed among three separate centers under the Army Materiel Command and the Office of the Surgeon General. It even proved impossible for INSCOM to collocate all elements of its own production center, the Intelligence and Threat Analysis Center. Although most of the center's resources were at Arlington Hall Station, it proved physically impracticable to move some of its major production functions from either the Washington Navy Yard or Fort Bragg, North Carolina.

How to impose a satisfactory organization on all Army intelligence production elements was resolved temporarily in 1985 by a more or less Solomonic decision. The Intelligence and Threat Analysis Center was removed from INSCOM and resubordinated to a new Army Intelligence Agency, a field operating agency of ACSI with headquarters in Northern Virginia. At the same time, the new agency was given command of the Army Missile and Space Intelligence Center and the Foreign Science and Technology Center. The Surgeon General's Medical Intelligence and Information Agency had become a joint service organization. Army intelligence production still remained geographically dispersed, but the situation was improved when elements of the Intelligence and Threat Analysis Center moved to the Washington Navy Yard. The new arrangement again made ACSI a major player in the field of intelligence operations, for the Army Intelligence Agency, with a personnel strength of 1,500, was as large as the Army's intelligence production organization before the creation of DIA.

---

[8] One of the few mentions of INSCOM in open sources can be found in Jeffrey Richelson, *The U.S. Intelligence Community* (Cambridge, Mass.: Ballinger Publishing Co., 1985), pp. 66–68.

Finally, INSCOM operations were impeded by physical limitations that split its headquarters elements between two Army posts forty miles apart. The physical facilities which INSCOM inherited from its predecessor organizations, ASA and USAINTA, simply were too limited. Attempts to find a suitable central headquarters location either at Fort Meade, Maryland, or at Vint Hill Farms, Virginia, repeatedly fell to political and fiscal constraints. However, the withdrawal of the large DIA presence from Arlington Hall in 1985 at last made it possible for planners to order that all headquarters elements be consolidated at that site during the following year. Nevertheless, a number of subordinate units at Fort Meade, including the Central Security Facility, remained behind, and Arlington Hall proved only a way station. In 1985 the Army finally decided that INSCOM's permanent headquarters would eventually be located at Fort Belvoir, Virginia. The command finally relocated in the summer of 1989.

Despite its initial growing pains, INSCOM provided a useful base on which the Army could build an expanded intelligence program once the long slide in defense spending was arrested. Human intelligence received fresh emphasis, as did the expansion of the command's cryptologic activities. In 1980 INSCOM established an Army presence at a joint service field station in Kunia, Hawaii. This was the first new Army field station set up outside the continental United States since the Vietnam War. Two years later, it organized another new field station in Panama from resources already in place. Later, the command fielded Army technical control and analysis elements to provide better cryptologic support to tactical Military Intelligence units.

A major new Military Intelligence unit based in the United States, the 513th Military Intelligence Group, was activated in 1982. The group would support possible operations of the Army component of Central Command (CENTCOM), the unified command created that year to deal with contingency situations in Southwest Asia. As initially configured, the group exercised command and control over three flexibly organized battalions: the 201st, 202d, and 203d Military Intelligence Battalions. Later, the 513th organized a TDA Military Intelligence battalion to deal with low-intensity conflict situations.

The group's 203d Military Intelligence Battalion at first was organized as a technical intelligence unit, indicating the Army's renewed interest in this sometimes neglected area. The battalion's main operating unit was the 11th Military Intelligence Company, the latest in a succession of company-size units that had stayed at Aberdeen Proving Ground, Maryland, since the 1960s. In 1978 this company had acquired the important additional mission of supporting the Army's Opposing Forces (OPFOR) training program. However, conflict soon developed between the technical intelligence battalion's mission of deploying overseas with its parent group in a contingency situation and its tasking to support the OPFOR program in the United States. A subsequent reorganization

reassigned the technical intelligence function to the Foreign Materiel Intelligence Group, a TDA unit directly subordinate to INSCOM headquarters, but the 513th regained the mission in 1989.[9]

By 1985 the U.S. Army Intelligence and Security Command was redefining its structure and practices along a variety of fronts. The resubordination of its production element to the Army Intelligence Agency allowed the command to focus most of its energies on its principal mission—managing the Army's strategic and theater-level collection resources. However, a reexamination of INSCOM's organization revealed that it was still carrying out functions of combat development and materiel development that in theory were supposed to have been transferred to TRADOC and the Army Materiel Command. Although INSCOM attempted to step out of these fields, the command's nucleus of resident experts made it difficult to abandon all its developmental efforts, since no other organization was prepared to address such requirements.

More definite resolutions were found in other areas, one of which was counterintelligence. As revelations of successful penetrations of America's most sensitive agencies by hostile intelligence services mounted, 1985 became the "Year of the Spy."[10] The Intelligence and Security Command moved to reconfigure its limited counterintelligence assets into more productive arrangements to meet the Army's needs. In the process, the command moved away from a concept of providing general operational security support to all Army elements in favor of a narrower focus on priority objectives, such as expanding polygraph examinations and technical services countermeasures and providing counterintelligence support to the Army's growing number of Special Access Programs (SAPs)—highly sensitive projects that required exceptional security measures.

In turn, this concern led to a reorganization of the command's main counterintelligence unit in the United States, the 902d Military Intelligence Group. Originally organized on geographic lines into three TDA battalions, the group's subordinate elements were restructured on a functional, rather than geographic, basis in 1985. At the same time, the group was given greater responsibility for handling counterespionage operations in the continental United States.

Change continued in 1986. Beginning that year, INSCOM's five multidiscipline intelligence groups were redesignated as brigades. This transition was intended to be more than cosmetic; the units would now be organized for possible warfighting, rather than having structures geared to national collection requirements in time of peace. A basic brigade was designed to consist of a headquarters and headquarters company, a numbered echelon above corps

---

9 The Foreign Materiel Intelligence Group was redesignated the Foreign Materiel Intelligence Battalion and resubordinated to the 513th Military Intelligence Brigade on 16 October 1989. In 1996 this TDA battalion was discontinued and the mission assumed by the provisional 203d MI Battalion.

10 Thomas B. Allen and Norman Polgar, *Merchants of Treason: America's Secrets for Sale* (New York: Delacorte Press, 1988), p. 2.

intelligence center for intelligence production, a signals intelligence battalion, an imagery analysis battalion, a counterintelligence battalion, an interrogation and exploitation battalion, and a collection element. Because of the diversity of intelligence requirements in the several theaters, however, the actual units allotted to each INSCOM brigade would differ. In the event of mobilization, INSCOM leaders planned to call up reserve component units as needed to bring the brigades to full strength. Additionally, the U.S. Army Intelligence Center and School drew up new TOEs that mandated the conversion of the command's flexible battalions into fixed elements.

Finally, INSCOM took action to redesignate some of its TDA units as numbered Military Intelligence brigades, battalions, and companies in the 700 series. Units redesignated included the Continental United States Military Intelligence Group and a number of field stations. This would provide units with designations more intelligible to the rest of the Army, and it would enhance the pride and esprit of their assigned soldiers. As a result of this step, existing command assets combined into three new Military Intelligence Brigades (the 701st, 703d, and 704th) and a number of new battalions in 1987.

The Combat Electronic Warfare and Intelligence Concept

The U.S. Army Intelligence and Security Command was only part of the new organizational design which the Intelligence Organization and Stationing Study imposed upon Army Intelligence. The IOSS also had brought about a major realignment of the Army's tactical intelligence assets in the field. These reforms drastically reshuffled the old command channels in the tactical arena. With the dissolution of the Army Security Agency's vertical command structure, all former ASA tactical elements were now under the command of the units they supported. At the same time, the Army formed new integrated combat electronic warfare and intelligence (CEWI) units to carry out functions previously performed by a variety of different organizations. This new type of Military Intelligence unit joined together Military Intelligence and former Army Security Agency assets.

Two separate institutional thrusts combined to create the ultimate CEWI structure. The first was a growing belief that under conditions of modern warfare it was absolutely essential that a combat division have its own organic intelligence capability. This concept marked a revolution in Army institutional thinking. The Army had reorganized the division force structure twice since the Korean War, creating the pentomic division in 1957 and replacing it with the ROAD division in 1962. Each time, its leaders had explicitly rejected the idea of making an intelligence unit organic to the division, partially because linguistic requirements would vary so greatly under different theater conditions. Until 1969 Army divisions received intelligence support, apart from signals intelligence, from attached Military Intelligence units. Although most of these detach-

ments subsequently had been expanded to full companies, such elements were still only temporary attachments to the division.

In the mid-1970s, after intensive study and testing, the Army reversed its stance and allotted each division an organic intelligence company. Army policy makers had finally concluded that the incorporation of permanent intelligence units into divisions would provide better peacetime training opportunities and would forestall the necessity of hastily assembling the requisite intelligence assets whenever a war broke out. Such units would also furnish a convenient locus from which to manage radar and ground sensor assets previously dispersed throughout the division. One underlying assumption was the growing importance of various technical collection mechanisms in relation to human intelligence sources on the future battlefield. This technology-driven approach complemented the newly developed process the Army termed "the Intelligence Preparation of the Battlefield," in which data on enemy, weather, and terrain would be plotted on map overlays to provide commanders with a graphic intelligence estimate.[11]

The second and more important element leading to the creation of CEWI units was the emphasis of IOSS on the need to integrate diverse intelligence disciplines in the field, both to enhance the support provided commanders and to reduce overhead. The end result of this process came when a TRADOC study group produced the first blueprint for a CEWI type of unit in early 1976. An experimental combat electronic warfare and intelligence battalion, the 522d Military Intelligence Battalion, was fielded later that same year at Fort Hood, Texas, and assigned to the 2d Armored Division. The successful activation of this prototype CEWI battalion meant that the TOE of the divisional intelligence company, which appeared the same year, was already obsolete. The Army's acceptance of the need for battalion-size units to support divisional intelligence requirements demonstrated how far the discipline had come since its World War I beginnings, when divisions had met their intelligence needs with staffs of four officers and a few enlisted men and militarized civilians serving as field clerks.

An agreed-upon TOE for an organic divisional CEWI battalion appeared in 1979. Significantly, the TOE for this new-model Military Intelligence unit was numbered in a different series from previous Military Intelligence and Army Security Agency tables of organization and equipment. The new organizational table provided for a headquarters and headquarters and operations company containing collection management, counterintelligence, and interrogation personnel, and included a platoon of helicopters configured for electronic missions.

---

[11] IPB: Intelligence Preparation of the Battlefield (Fort Huachuca, Ariz.: U.S. Army Intelligence Center and School, n.d.). The IPB process was potentially adaptable to automation. This seemed a necessity, since it was estimated in the 1970s that a corps commander in a European war scenario would have to track some 35,000 "movers, shooters, and emitters" in the adversary force. G. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven: Yale University Press, 1990), p. 145.

It also called for three line companies that respectively carried out functional missions of collection and jamming, ground surveillance through radars and sensors, and service support. The new structure thus merged existing intelligence, signals intelligence, and electronic warfare assets available at division level and integrated them with divisional ground sensor and ground surveillance radar elements.[12] Planners also contemplated giving the unit a long-range reconnaissance patrol capability, an addition initially rejected but revived a decade later. Subsequently, the pattern of organization prescribed by the 1979 TOE was modified often in the field, as "company teams" containing elements from all disciplines were organized on an ad hoc basis to support the requirements of each of a division's three brigades.[13]

Although combat divisions continued to have separate reconnaissance battalions and were now allotted target acquisition batteries, the creation of the CEWI unit meant that the division's tactical operations center could draw on the resources of a single element to meet the bulk of its intelligence, security, and electronic warfare needs, rather than having to deal with fragmented elements scattered throughout the divisional structure. The CEWI battalion organization was intended to be strong enough to provide the diverse intelligence disciplines it contained with the necessary support. Since only a quarter of the CEWI battalion's strength consisted of highly trained intelligence specialists, it allowed maximum use of these scarce resources.[14]

The organization of the division-level CEWI battalion was only the beginning of a wholesale restructuring of Army Intelligence at the level of tactical support. Company-size CEWI units were formed to support separate brigades and armored cavalry regiments. The Army also replaced all its active component Military Intelligence battalions, air reconnaissance support, with "military intelligence battalions, aerial exploitation." These new units consisted of a headquarters and headquarters company, an imagery interpretation company, a combat intelligence company (aerial surveillance), and an electronic warfare aviation company (forward). When the battalion operated independently, an electronic warfare aviation company (rear) could be attached. The concept provided a suitable management framework for the Army's own aerial assets and integrated different types of mission aircraft into a single unit.[15]

---

12 Don Gordon, "CEWI Battalion: Intelligence and Electronic Warfare on the Battlefield," *Military Intelligence* 5 (October–December 1979): 22–28.

13 Company Team Commander Responsibilities, 313th MI Bn (CEWI), 82d Airborne Div, Apr 84, copy in INSCOM History Office files.

14 Gordon, "CEWI Battalion," p. 27.

15 This change in force structure was in part dictated by the fact that relying on traditional Air Force photo-reconnaissance platforms in a high-intensity conflict no longer seemed a viable proposition. Army aerial assets could conduct various forms of electronic surveillance while flying in relative safety behind their own front lines. The discontinuance of MIBARS units in the Active Army meant that the Army would henceforth rely on INSCOM IMINT companies and on the reserve components to provide imagery interpreter support for Air Force tactical reconnaissance missions.

Initially the capstone of the new tactical support intelligence structure, the Military Intelligence group functioned at the corps level. The first of these units activated, the 504th Military Intelligence Group, went to support the III Corps at Fort Hood, Texas, in 1978.[16] In 1985, the 201st, 205th, 207th, 504th, and 525th Military Intelligence Groups assigned to support the five corps then operational in the Active Army were all upgraded to brigade status. Each Military Intelligence brigade consisted of a headquarters and headquarters detachment, an operations battalion, an aerial exploitation battalion, and an interrogation and exploitation battalion.

Military Intelligence in the Reserve Components

The integration and reorganization of the Army's intelligence elements were not confined to the Active Army, but also affected the reserve components. The end result of the process was to greatly expand the Military Intelligence presence in these components. While the 24th Military Intelligence Battalion continued as an aerial reconnaissance support unit, the three existing ASA battalions and the single field army type of Military Intelligence battalion in the Army Reserve were all converted to CEWI units, and four additional battalions were activated. Actual implementation of the program took some time. The first Army Reserve CEWI unit, the 138th Military Intelligence Battalion, was not activated until late 1983, and not until 1988 did the last remaining Army Security Agency battalion in the reserve phase out.

Initially, the Army had determined that all combat electronic warfare and intelligence battalions in the reserve structure would belong to the Army Reserve. The National Guard operated under state control in peacetime, and national policy makers had reservations about placing sensitive intelligence assets under state government control. Ultimately, the intelligence community decided that policy considerations did not preclude establishing such units in the National Guard, and the 629th Military Intelligence Battalion was organized in 1988 to service the intelligence and electronic warfare needs of the Maryland-Virginia National Guard's 29th Infantry Division. This issue did not arise in the case of non-CEWI types of National Guard military intelligence units, and aerial exploitation battalions appeared in the Georgia and Oregon National Guards in 1982.

One National Guard unit continued to provide unique support to Army-wide intelligence requirements. In 1980 the 142d Military Intelligence Battalion was organized in the Utah National Guard, replacing a similar company-size unit originally organized in 1960. This TDA battalion, a linguist unit, drew heavily from a pool of expertise provided by members of the Church of Jesus Christ of Latter Day Saints who had previously undergone language training to

[16] This unit was created by reorganizing and redesignating the 504th Army Security Agency Group, originally activated in 1974 to provide cryptologic support to FORSCOM.

carry out overseas missionary work. Battalion personnel on temporary duty repeatedly assisted the Regular Army in meeting its linguistic needs. The concept was so successful that in 1988 the battalion was converted to a TOE unit; a second similar battalion was organized in the Utah National Guard; and a TDA unit, the 300th Military Intelligence Brigade, was created to provide command and control. Later, the Army approved the organization of Guard linguist battalions in several other states.

Training continued to present difficulties for intelligence units both in the reserve components and in the Regular Army. Many intelligence specialties could not be exercised normally in hometown environments or even under garrison conditions. However, in 1978 the Intelligence and Security Command instituted the Readiness Training Program (REDTRAIN) to expose practitioners of intelligence disciplines throughout the Army to "enrichment" programs. REDTRAIN allowed both reservists and Regular Army soldiers to further their skills by participating in current operations. In practice, this was accomplished either by assigning personnel on temporary duty to units with an operational mission or by bringing the mission to the unit.

Military Intelligence in the 1980s

The 1980s were prosperous years for the Army, especially for its restructured intelligence component. The formation of INSCOM and the implementation of the CEWI concept not only affected intelligence operations throughout the Army, but also drew the Military Intelligence Branch firmly into the mainstream of the service. For the first time, most MI personnel were assigned to TOE units. By 1988 five MI brigades and no less than thirty MI battalions had been formed under the CEWI concept to support tactical units in the field, while another five TOE MI brigades and ten TOE single-function battalions carried out theater- and national-level support missions under INSCOM. Twenty-five thousand Military Intelligence specialists—over 15 percent of them female—were on active duty, backed up by another 8,700 in the reserve components. The active duty Military Intelligence component alone was as large as the entire Regular Army had been in 1885, when the Army first created a permanent intelligence organization. As retired Lt. Gen. James A. Williams, a former director of DIA, pointed out, the Army now had "the equivalent of two combat divisions in collection and analysis."[17]

There were still significant shortfalls in a number of areas. The proliferation of job opportunities presented by an information-based society made recruiting and retaining personnel in a number of intelligence specialties a pressing concern for what continued to be an all-volunteer force. The tactical-level force

---

17 Benjamin F. Schemmer, "Former DIA Director Urges That Four-Star Should Head All Military Intelligence," *Armed Forces Journal International*, Feb 88, p. 24.

structure had grown so large that some Army Intelligence professionals questioned whether it could be maintained indefinitely, given anticipated constraints on Army resources and the competing demands of the Army's echelon above corps intelligence structure. The lightning advance of technology, combined with convoluted contracting and procurement procedures and growing fiscal constraints, had left the Army saddled with equipment that fell far behind the state of the art in many intelligence disciplines. For much of its aerial work, Army Intelligence still depended upon the durable Mohawk, which despite its considerable virtues was now thirty years old. Almost thirty-five years after the inception of Project MICHIGAN, the Army was still struggling to field a satisfactory remotely piloted vehicle—a pilotless reconnaissance aircraft. Army tactical signals intelligence and electronic intelligence resources in the field were mounted on slow and overloaded carriers that could not keep up with the new generation of Army tanks and armored fighting vehicles. Moreover, as 1990 approached there were already signs that the greatest defense buildup since the Korean War was about to end, and this necessitated further changes in the organization of Army Intelligence.

In 1987, however, two significant developments seemed to confirm that the Army had at last accepted its Intelligence arm as an equal member in its family of branches. In May of that year the position of ACSI was upgraded to deputy chief of staff for intelligence (DCSINT), a change that ended the position of perceived organizational inferiority of the Army Intelligence staff post. Lt. Gen. Sidney T. Weinstein became the Army's first DCSINT. That same year, Army Intelligence became part of the regimental system that embodied the heritage of the U.S. Army. On 1 July 1987, the twenty-fifth anniversary of the establishment of intelligence as a Regular Army branch, all Army Intelligence personnel, military and civilian, became part of a single large regiment, the Military Intelligence Corps, headed by the commanding general, U.S. Army Intelligence Center and School. Although symbolic, the measure was significant. Maj. Gen. Julius Parker, the first chief of the Military Intelligence Corps, called the step "a recognition and celebration of our evolution from a plethora of diverse and separate intelligence agencies into the cohesive MI community we enjoy today. In short, it symbolizes the fact that Army Intelligence has truly arrived."[18]

Additional proofs that General Parker's statement was not overly optimistic were soon forthcoming. In 1987 the Army published a detailed Army Intelligence, Electronic Warfare, and Target Acquisition Plan (AIMP). The AIMP conceptualized the future structure of Army Intelligence as a "system of systems" and laid out a detailed and coherent road map of the measures needed to reshape the Army's intelligence organizations and technologies in ways that would satisfy future requirements. In 1989 INSCOM shifted its headquarters

---

18 Ltr, Chief, Military Intelligence, *Huachuca Scout (Military Intelligence Corps Activation Supplement)*, 25 Jun 87, p. 2.

from Arlington Hall Station to a site on the north post of Fort Belvoir, Virginia. INSCOM's new headquarters facility, the Nolan Building, was named in honor of Maj. Gen. Dennis E. Nolan, Pershing's G–2 in World War I.This was the first Army Intelligence headquarters ever designed specifically for its purpose. In 1990 the chief of Military Intelligence became commanding general of the U.S. Army Intelligence Center and Fort Huachuca. This step paved the way for the eventual closure of the Intelligence School at Fort Devens, Massachusetts, and the consolidation of almost all Military Intelligence training at Fort Huachuca. Meanwhile, the internal evolution of Military Intelligence within the Army was already being affected by outside events.

11

A Future of Uncertainties

The year 1989 was an "annus mirabilis," a time of wonders, in which the world geopolitical framework in place since the end of World War II was overturned. As military historian Michael Howard commented, "while the nations of Western Europe celebrated the bicentennial of the French Revolution, the nations of Eastern Europe reenacted it."[1] After so many years, the Iron Curtain finally parted, and with it the Berlin Wall and so many of the other symbolic and real barriers that had divided east from west. With tides of democracy sweeping through Eastern Europe, the Warsaw Pact was no longer relevant. The Soviet Union itself appeared in a new light—no longer the Great Bear of international politics, but an ideologically and economically bankrupt society showing ominous signs of fragmentation along ethnic and national lines. For all practical purposes, the looming threat of Soviet power that had gripped the attention of Western policy makers for so many years was suddenly gone.

Since 1989 these developments have dramatically restructured America's defense policy. Ever since the end of the Vietnam War, the U.S. Army had essentially staked its raison d'etre on countering a massive tank-led Warsaw Pact offensive against Western Europe. With this threat no longer viable, the nation's armed forces were slowly downsized and redeployed. The numbers governing the rate, scope, and exact nature of this process shifted with each new indication of communism's decline. In 1990 the Army implemented Project VANGUARD to bring about a controlled reduction of its strength in ways that would leave as much of its fighting forces intact as possible, a task to be accomplished initially through a radical trimming of headquarters elements.

However, just as the Soviet threat receded and pundits began to talk about the pleasant possibilities of a "peace dividend," a new array of international challenges appeared. In December 1989 American forces stormed Panama in Operation JUST CAUSE, overthrowing the regime of its narcotics-linked strong-

[1] Michael Howard, "The Springtime of Nations," *Foreign Affairs* 69, no. 1, p. 17.

man, General Manuel Noriega. Eight months later, crisis flared in the Middle East. An Iraqi invasion of the tiny emirate of Kuwait, threatening both the world's oil supply and the stability of a potential new world order, led to a massive American response. The United States deployed over 500,000 men and women to the Persian Gulf region—the largest buildup of troops since Vietnam—and then committed them to battle in Operation DESERT STORM, a lightning air and ground war that resulted in complete victory.

Despite these conflicting crosscurrents of events, planning for retrenchment of the force continued. Nevertheless, it was clear that the post–Cold War world would continue to hold unforeseen and unforeseeable perils. In the unstructured international environment created by the sudden collapse of the bipolar world order imposed by the Cold War, crises could—and did—take place in almost any region of the globe. The prospect of a smaller Army and a more diffused but wider menace would inevitably affect the institutional arrangements of Military Intelligence, since intelligence organizations are necessarily shaped by the threat as well as the force structure in place. In addition to preparing for contingency operations, Army Intelligence now had to monitor arms verification agreements, fight terrorism, maintain a vigilant watch against espionage, and assume a counter-drug mission in support of civilian authorities.

The challenges of JUST CAUSE and DESERT STORM—successive crises occurring half a world apart and in totally unrelated linguistic environments—had already made large demands on Military Intelligence and appeared to serve as a portent for the future. On the whole, the Army had met these demands successfully. INSCOM's 470th Military Intelligence Brigade and its attached 29th Military Intelligence Battalion had been in place in Panama when that crisis broke. INSCOM's 513th Military Intelligence Brigade, with a long-standing contingency mission to support the U.S. Army Central Command, had been at least partially positioned to meet Army intelligence requirements when deployment to the Persian Gulf began. Once brigade elements had moved to Saudi Arabia, the U.S. Army Intelligence and Security Command augmented the unit from its own assets around the globe. As the situation reached its climax, the brigade's echelon-above-corps intelligence center was expanded to a full operations battalion and placed in support of the G–2 of Central Command's Army component. Two corps CEWI brigades, the 504th and 525th MI brigades, and divisional CEWI units supported the intelligence effort in Southwest Asia with their own resources, and reserve component units and individual mobilization augmentees deployed to assist.

In this intelligence campaign, high technology at last came into its own. A variety of ground terminals received information provided by diverse national and theater intelligence systems, unmanned aerial vehicles—the new Army term for remotely controlled pilotless aircraft—were finally fielded to provide collection and targeting data, and the Army engaged in substantive electronic warfare

operations for the first time since electronic warfare had become an intelligence responsibility.[2]

In JUST CAUSE and DESERT STORM, however, the Army had been able to draw on the resources it had built up during the height of the Cold War. The future challenge for Army Intelligence would be to do more with less. Even as DESERT STORM came to an end, it was already evident that the smaller force structure envisaged for the future would necessarily lead to the inactivation of numerous intelligence battalions and brigades, as the divisions and corps to which they were assigned closed down. By 1995 the Army force structure had been reduced from eighteen divisions to just ten. The shrinkage of tactical assets was accompanied by a pullback of much of the Army from its forward-deployed posture. Presumably, this withdrawal would make INSCOM even more central to the Army's intelligence effort, since tactical intelligence units in the continental United States would not have direct access to their intelligence targets, and INSCOM alone had the necessary linkages to national systems to provide the Army with worldwide intelligence support.

However, the elimination of the Soviet threat and the consequent downsizing of the Army meant that INSCOM itself faced the greatest reorganization since its birth with the possibility of not even surviving as a major Army command. Flux was the order of the day. For a brief time, the command regained Army production functions, assuming command of the Army Intelligence Agency in 1991. The following year, however, AIA was disestablished and its subordinate production centers divided up between DIA and INSCOM, with DCSINT retaining operational control of the Intelligence and Threat Analysis Center and the Foreign Science and Technology Center, the two elements that remained with INSCOM. In turn, these two production elements were merged into a single National Ground Intelligence Center. The Special Security Group that had disseminated sensitive compartmented information since World War II was reorganized and most special security officers resubordinated to the major Army commands they supported, thus creating a much smaller Special Security organization to set policy and deal with private contractors. Eventually, the unit's mission was assumed by one of the battalions of the 902d MI Group.

This did not exhaust the list of changes. INSCOM's major field stations in Europe and Panama were discontinued and Army cryptologic organization radically restructured. INSCOM set up a Regional SIGINT Operations Center at Fort Gordon, Georgia, manned by personnel of the newly organized 702d MI Group. Since its 513th MI Brigade concurrently relocated to Fort Gordon, this allowed strategic and tactical assets to be combined. At the same time, the com-

---

[2] Details of Army Intelligence operations conducted during the DESERT SHIELD/DESERT STORM mission can be found in Brig. Gen. (P) John F. Stewart, Jr.'s pamphlet, Operation DESERT STORM: The Military Intelligence Story: A View From the G–2, 3d U.S. Army, April 1991.

mand assumed host responsibilities for new sites in Europe that would allow the Army to employ the most advanced communications technologies.

Institutional gains were accompanied by institutional losses. INSCOM's U.S. Army Russian Institute was resubordinated to the European Command. A Foreign Intelligence Command was organized at Fort Meade, Maryland, to provide better support to human intelligence (HUMINT) and counterintelligence units there, but this proved to have the life span of a mayfly: it was discontinued in less than a year as a result of the secretary of defense's decision to incorporate Army human intelligence elements into a Defense HUMINT Service.

As the Army itself restructured and pulled back from Europe and Panama, its leaders planned to merge INSCOM's five existing theater support brigades into two force projection brigades. The new units would operate in a split-based configuration and would have the capability to deploy tactically tailored force packages to meet any level of contingency requirement. Additionally, beginning in 1993 INSCOM provided personnel to augment corps-level production centers and (for a time) joint intelligence centers within the unified commands. INSCOM would no longer simply operate at echelons above corps, but would provide the Army with "seamless connectivity" between national-level agencies and the warfighters on the ground.

Finally, in 1994 the Army set up the Land Information Warfare Activity (LIWA) within INSCOM, operating under the staff supervision of the Department of the Army's deputy chief of staff for operations. This was inspired by the precedent offered by DESERT STORM, in which the centralized Iraqi command structure had been effectively befuddled by deception operations and decapitated by the electronic and physical destruction of its communications system. Still in the formative stage, the LIWA sought to bring together the techniques of electronic warfare, psychological warfare, deception operations, command and control targeting, and operational security to attack the information resources of the enemy while simultaneously defending those of our own armed forces. Once it became fully operational, the LIWA would offer the larger Army a place for "one-stop shopping" in these areas.[3]

Conclusion: The Shaping of Army Intelligence

Although the details of the future necessarily lay hidden, Military Intelligence's current trajectory provides clues as to its future organizational and mission directions.[4] At least five identifiable trends have helped shape the

[3] The "information warfare" concept reflected—or at least paralleled—the ideas of the influential futurologists Alvin and Heidi Toffler. See *War and Anti-War* (Boston: Little Brown, 1994), ch. 10, "The Knowledge Warriors."

[4] Of course, clues can be misleading. Distinguished military historian Russell F. Weigley has commented, "Almost all of the hints of prophecy into which the author was rashly drawn . . . proved wrong." *History of the United States Army, Enlarged Edition* (Bloomington: Indiana University Press, 1984), pp. 557–58.

post–World War II history of Army Intelligence: a steady devolution of functions to national and joint agencies; a redefinition of the Military Intelligence field to embrace new functions; an enhanced role for technology; a progressive growth both in the number and size of intelligence units and in the diversity of intelligence disciplines they incorporated; and finally, an increasing professionalism.

First of all, continuing pressures for greater service integration has had a major impact on the overall organization of Army Intelligence. As a result of these pressures, and over a period of time, the Army has transferred cryptologic, production, attache collection, and certain counterintelligence and human intelligence functions to national agencies. The creation of the Central Intelligence Agency in 1947 removed the Army from the fields of political and economic intelligence. This preceded the partial breakup of the Army Security Agency in 1949 to form the Armed Forces Security Agency (AFSA), the National Security Agency's predecessor. More reforms followed the revision of the National Defense Act in 1958, which removed the Army as an institution from the chain of national command and turned it into a mechanism for training, administering, and supplying land forces for the unified commands acting under the Joint Chiefs of Staff. The logic of this inevitably dictated the creation of the Defense Intelligence Agency (DIA) in 1961. As DIA grew it took over Army production functions as well as certain training and collection functions.

As the Army drew down during the last stages of the Vietnam conflict, there was another wave of consolidation. The Defense Mapping Agency absorbed Army topographic elements, the Central Security Service took over certain headquarters functions of the Army's cryptologic agency, and the Defense Investigative Service assumed the personnel background investigation function previously performed by Army counterintelligence. The first two integrations were done ostensibly to promote economy and efficiency, while the last eased the Army out of the domestic intelligence field that had left it open to charges of "spying on civilians."

As the Army once more planned to contract in the 1990s, these kinds of pressures on its Military Intelligence organization continued. If anything, the Department of Defense Reorganization Act of 1986 had placed a premium on joint operations. However, despite the steady trend toward integration, Army Intelligence has in fact shown a remarkable resiliency over the years. This is wholly consistent with laws of institutional behavior. Motivated recruits join the Army because they wish to wear green suits, not "purple" ones.[5] The Army most readily surrendered those intelligence functions peripheral to its central mission of warfighting.

---

[5] For an interesting discussion of the differing "personalities," identities, and behaviors of the different armed services, see Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore: Johns Hopkins University Press, 1989), p. 39. Builder notes that "the unique service identities . . . are likely to persist for a very long time."

Before the creation of the Central Intelligence Agency, the Army had engaged in collection of political and economic intelligence for want of a better alternative. The high-level cryptologic mission turned over to the Armed Forces Security Agency had implications that went beyond the Army. It was also both exotic (most of the personnel who transferred to AFSA were highly specialized civilians) and a mission which naturally lent itself to a joint approach. Moreover, although the impetus behind the creation of AFSA had been to replace three service cryptologic organizations with one, the end result was the creation of four cryptologic organizations. The Army's determination to provide cryptologic support to its own commanders ensured that the Army Security Agency grew larger and more important after 1949 than it had been before. The National Security Agency later attempted unsuccessfully to integrate service management structures into a central security service.

The creation of the Defense Intelligence Agency presented Army Intelligence with a more formidable institutional challenge. Here, the Army and the other services pursued a strategy of more straightforward resistance, refusing to allow their intelligence components to be completely subsumed into the new organization. During the agency's formative period, Army officers posted to DIA found their assignments less than career enhancing. DIA was initially allowed to control only a single collection element, the attache system, and the Army reentered the field of intelligence production almost immediately. Even after thirty years, DIA had not achieved the dominant position in the general intelligence field that NSA had achieved in the cryptologic area.

In 1972 the Army gave up the bulk of its counterintelligence operations in the continental United States to the Defense Intelligence Service, when the latter agency was formed to execute the mission of conducting personnel background investigations for security clearances. This was a forced move, brought about by the fact that the Army had been brought deeply into the field of domestic intelligence during the troubled times of the Vietnam War. However, the transfer of functions, again, did not impact on the Army's wartime mission. Moreover, it could be looked upon as a blessing, since it removed the Army from an area which had been a political land mine since the earliest days of its own counterintelligence operations. The Army had been forcibly extracted from domestic intelligence operations twice before—in 1920, at the end of the Red Scare, and in 1943, following political displeasure at investigations of subversives that had touched upon the president's family. Three experiences of this kind were perhaps enough.

Finally, in 1995 DIA set up the Defense HUMINT Service (DHS), which absorbed all the strategic and theater-level human intelligence collection assets of the armed services. This forced merger was brought about by a post–Cold War drive for economy and efficiency that in many ways paralleled the Department of Defense–level realignments of the Vietnam drawdown. However, once more we could argue that the Army surrendered elements not central to its perceived main mission of warfighting.

A second trend evident during this period was the redefinition and expansion of the intelligence field. Over the years, Military Intelligence organizations absorbed various "special informational services." This process had begun immediately after World War II, when the Military Intelligence Division assumed administrative as well as operational control of the Army Security Agency. In turn, the logic of this realignment eventually made electronic warfare an intelligence responsibility. "Jamming" and collection operations were intimately related, and could not be conducted independently of one another. As a result, the Army Security Agency gained responsibility for communications electronic countermeasures in 1955. Simultaneously, it assumed the electronic intelligence (ELINT) mission from the Signal Corps. This too followed a certain logic: the agency now collected against the whole of the electronic spectrum instead of just a part. Continuing in the same pattern, ASA acquired the noncommunications electronic countermeasures mission from the Signal Corps in 1962.

The formation of combat electronic warfare and intelligence units as a result of the Intelligence Organization and Stationing Study brought additional collection services under the Military Intelligence umbrella. Intelligence units assimilated ground sensors and ground surveillance radars. Meanwhile, Army Intelligence had already taken to the sky. Army aviation had developed specialized reconnaissance aircraft in the late 1950s, and the Army Security Agency had developed its own air arm during the 1960s. In the late 1970s, both types of assets became part of an integrated Military Intelligence battalion, aerial exploitation.

In one area, however, the responsibilities of Military Intelligence contracted after World War II. This was the field of communications security. The Army Security Agency, as first set up, had responsibility for all aspects of military cryptology, including creating and distributing the Army's codes and cipher devices and monitoring the security of Army communications. The 1955 reorganization of the Army Security Agency resulted in the transfer of the first two of these functions to the Signal Corps. As the years went on, a tendency for Army Intelligence to edge away from security monitoring became pronounced; many saw the task as intrusive, unpopular, and not particularly effective. In the long run, as far as the Army was concerned, encryption of all message traffic could render security monitoring obsolete. Meanwhile, some aspects of communications security could now be passed back to the communicators. In 1988 INSCOM, which had inherited from ASA the mission of preparing the Army's Communications-Electronics Operating Instructions, decided that the function would more appropriately belong to the Army's new Directorate of Information Systems for Command, Control, Communications, and Computers. A little later, INSCOM transferred mission responsibility for the inspection of cryptofacilities and the tracking of communications violations to the Army's communicators.

Third, partially as a result of Intelligence's increasing dependence on the technical services, the advance of technology affected almost every intelligence discipline. The combined impact of the communications revolution and the

growth of automation had a profound effect upon intelligence collection, processing, and dissemination. To use only select examples, the development of infrared and radar imaging techniques revolutionized photographic intelligence and resulted in that discipline's transformation into imagery intelligence. The synergistic use of a variety of techniques to measure the distinct profiles displayed by an assortment of target "shooters, movers, and emitters" created the new intelligence discipline, measurement and signature intelligence (MASINT). Technology even promised—or threatened—to reverse the nature of the entire Army Intelligence process. Traditionally, information had passed from lower levels of command, in direct confrontation with the enemy, to higher levels for evaluation. In the Persian Gulf conflict of 1991, however, Army production elements based in the continental United States had used national intelligence acquisition systems to generate tactical intelligence that went down to the field.

Counterintelligence was also confronted with fresh challenges as a result of this trend. The Army faced a wider security threat as technological development created new vulnerabilities. Not only were the activities of hostile human agents now supplemented by electronic listening devices, but the radiations emitted by electronic media were vulnerable to detection, while the computers that supplied the masses of data on which the Army now relied could be infiltrated by "hackers" and menaced by computer "viruses."

Fourth, intelligence units in the field tended to grow both larger and more integrated. The Army emerged from World War II with a melange of single-discipline intelligence elements organized in no common pattern. They included counterintelligence detachments, ASA's signal service companies and detachments, and an assortment of teams and detachments that carried out various combat intelligence functions. Additionally, the Signal Corps had its own units conducting electronic intelligence and electronic warfare. The Korean War partially revolutionized this structure, as the Army fielded groups and battalions to collect combat intelligence and ASA created units of similar size to carry out military cryptologic functions in support of the tactical Army. In the latter part of the 1950s, counterintelligence and collection personnel were integrated into combat intelligence formations under the Military Intelligence Organization concept, although most counterintelligence personnel continued to serve in separate CIC groups. Roughly around the same time, various Signal Corps intelligence and electronic warfare units were folded into the Army Security Agency.

Following the Intelligence Organization and Stationing Study of 1975, the Army integrated all intelligence disciplines at both the tactical and strategic levels, creating CEWI units and the U.S. Army Intelligence and Security Command. For the first time, most Army Intelligence assets were contained in TOE units rather than under tables of distribution and allowances. By 1990 multidiscipline intelligence brigades had been fielded to support both corps and higher echelons of command.

The development of large intelligence units, combined with institutional pressures to reduce the operational role of the Army's intelligence staff, helped to move the center of gravity of intelligence work in the Army from the staff to the line. It also was one of the factors that helped make Army Intelligence more professional. One could argue logically that just as ordnance officers should command an ordnance unit, intelligence officers should command an intelligence unit. At first the Army Intelligence and Security Branch, as its title indicated, was something of an uneasy compromise, lumping together officers of diverse backgrounds and allegiances. The branch had no common training program, and the Army Security Agency, with its vertical command structure and its roots in the Signal Corps, remained a large, unassimilated segment of the Army Intelligence community. However, the Army made greater steps toward integration in 1967, when the Army Intelligence and Security Branch was redesignated as the Military Intelligence Branch and upgraded in status. The change was more than just a shift in nomenclature, since the common advanced schooling that went into effect at this time imposed a new homogeneity on the Military Intelligence field. Implementation of the IOSS recommendations brought the institutional structure of Army Intelligence into line with the single branch concept.

The professionalization of Army Intelligence, combined with the shift to an All-Volunteer Force in the early 1970s, led in turn to a greater emphasis on military values within the field. As long as intelligence organizations had been dominated by reserve officers, and depended on the stimulus of the draft for their manning, intelligence personnel had tended to identify with their specialties, rather than with the Army as a whole. The fact that so many of them were involved in specialized tasks with no immediate combat relationship only facilitated this ethos. While the mainstream of the peacetime Army focused on a training and readiness mission, Intelligence had (and continues to have) a viable peacetime mission. The bulk of ASA personnel, for example, carried out a strategic cryptologic mission at fixed installations, and most counterintelligence personnel operated in civilian clothes and lived on the civilian economy at a time when the rest of the Army was still in barracks and bachelor officers' quarters. When an applicant for the Counter Intelligence Corps asked his recruiters whether life in the CIC was anything like the Army, they replied, "Not very much." This approach has changed markedly.[6]

In short, we can argue that by 1990 Military Intelligence had become distinctly more military. Intelligence personnel—men and women, officer and enlisted—were soldiers first, specialists second. They trained regularly at Army skills and were held to Army standards of physical fitness. Separate management structures that tended to foster the idea that various groups of intelligence personnel were an elite corps apart from the larger Army had been dissolved:

[6] Author's recollection.

the Intelligence Corps was discontinued in 1966, and the Army Security Agency broke up ten years later. The grade structure of intelligence units mirrored that of the rest of the Army, unlike the situation in an earlier period, when 40 percent of a counterintelligence detachment's strength might consist of officers. The danger, of course, was that the process could be carried too far, and that the thrust to make everyone a potential warfighter might unduly divert energies from the proper performance of what remained a demanding real-world mission.[7]

Among other things, the new professionalism meant that Military Intelligence personnel could publicly identify with the traditions of the Army in ways that were not originally thought possible when intelligence work itself was identified, sometimes by its practitioners, as something appropriate only to the shadows. To give only one example, uniformed enlisted personnel assigned to Army Counter Intelligence Corps units during the 1950s wore a simple "U.S." as their collar insignia, officers bore the insignia of their carrier branch, and CIC units in the continental United States presented themselves to the public as "Army Research Groups." During the 1960s, however, Army Intelligence units boasted their own distinguishing unit insignia and their assigned personnel wore Military Intelligence brass. In the 1980s the MI groups of a previous period were redesignated as MI brigades, receiving their own shoulder sleeve insignia. This change would enhance troop esprit and morale by providing the units with more traditional military designations. Certain of INSCOM's TDA field stations and other TDA elements were also given new numerical unit designations. In part, the Army made the change to distinguish troop formations from the geographical locations at which they worked, but it also had the desirable side effect of assigning to these units designations that were more intelligible to the rest of the Army. In short, Military Intelligence identified itself with Army green, abandoning the cloak-and-dagger image of an earlier era. In more ways than one, the motto of the Military Intelligence Corps, "Always Out Front," reflected the new reality.

In 1987 the chief of Military Intelligence declared, "Army Intelligence has truly arrived," and in one sense he was correct. In another sense, however, Military Intelligence was still in transit, progressively redefining itself as the Army, the nation, and the international situation changed. Still, wherever the journey might lead it in the future, clearly Military Intelligence has come a long way from its modest beginning in 1885 as the Division of Military Information.

---

[7] As a visitor to an INSCOM counterintelligence element reported in 1989, "the six military personnel assigned . . . spend an inordinate amount of time detailed away from the office for charge of quarters details, training, physical training, and alerts, none of which is optional." He estimated that "the military personnel spend an average of 67% of their time away from the office." Memo, HQ INSCOM, IAOPS-CI-OC, 10 Oct 89, sub: Summary Report of Temporary Duty Travel to USAREUR.

Bibliography

For a number of reasons, it has seemed inappropriate to provide this volume with a full scholarly apparatus. Security conditions necessarily make the book's coverage of certain aspects of the Military Intelligence story a good deal less than definitive. Moreover, the book does not purport to be a completely original piece of research, since its first portion is based substantially upon material contained in two large previous studies: Bruce W. Bidwell's eight-part survey of the history of the Military Intelligence Division, Department of the Army, prepared for the U.S. Army Center of Military History in the 1950s, and a thirty-volume history of the Army Counter Intelligence Corps which the U.S. Army Intelligence Center compiled in 1959–1960. Initially, both works were fully classified, but now they have been largely declassified. Finally, the latter part of the book draws from a variety of Army files which still remain classified and, in some cases, compartmented; these files will not be accessible to researchers for the foreseeable future. As a result, we decided to provide footnotes only to cite direct quotations, provide additional commentary, and reference open-source publications applying to the subject. For the same reason, this bibliography lists only published, open-source material.

General Works

Bidwell, Bruce W. *History of the Military Intelligence Division, Department of the General Staff, 1775–1941*. Frederick, Md.: University Presses of America, 1986.

Clark, Ronald William. *The Man Who Broke PURPLE: A Life of the World's Greatest Cryptographer, Colonel William F. Friedman*. Boston: Little Brown, 1977.

Clausewitz, Carl Von. *On War*. Ed. and trans. Michael Howard and Peter Paret. Princeton: Princeton University Press, 1984.

Cline, Marjorie W. et al. *Scholar's Guide to Intelligence Literature*. Frederick, Md.: University Publications of America, 1983.

Cohen, Eliot A., and Gooch, John. *Military Misfortunes: The Anatomy of Failure in War*. New York: The Free Press, 1990.

Constantanides, George C. *Intelligence and Espionage: An Analytical Bibliography*. Boulder, Colo.: Westview Press, 1983.

Creveld, Martin Van. *Command in War*. Cambridge: Harvard University Press, 1985.

Crouch, Tom D. *The Eagle Aloft: Two Centuries of the Balloon in America*. Washington, D.C.: Smithsonian Institute Press, 1983.

Dulles, Allen. *The Craft of Intelligence*. New York: Harper and Row, 1963.

Finnegan, John P. *The Military Intelligence Story: A Photo History*. Fort Belvoir, Va.: U.S. Army Intelligence and Security Command, 1994.

_____. *Military Intelligence: A Picture History*. 2d ed. Fort Belvoir, Va.: U.S. Army Intelligence and Security Command, 1992.

Hewes, James. *From Root to MacNamara: Army Organization and Administration, 1900–1963*. Washington, D.C.: U.S. Army Center of Military History, 1975.

Ind, Allison. *A Short History of Espionage: From the Trojan Horse to Cuba*. New York: McKay, 1963.

Infield, Glenn B. *Unarmed and Unafraid: The First Complete History of Men, Missions, Training, and Techniques of Aerial Reconnaissance*. New York: MacMillan, 1970.

Gordon, Col. Don E. *Electronic Warfare: Element of Strategy and Multiplier of Combat Power*. New York: Pergamon Press, 1981.

Jefferys-Jones, Rhodri. *American Espionage: From Secret Service to CIA*. New York: Free Press, 1977.

_____. *The CIA and American Democracy*. New Haven: Yale University Press, 1989.

Jensen, Joan M. *Military Surveillance of Civilians in America*. Morristown, N.J.: General Learning Press, 1975.

Kahn, David. *The Codebreakers: The History of Secret Writing*. New York: MacMillan, 1967.

Kent, Sherman. *Strategic Intelligence for American World Policy* Princeton: Princeton University Press, 1947.

Knowing One's Enemies: Intelligence Assessment Before the Two Wars. Ed. Ernest May. Princeton: Princeton University Press, 1984.

Levite, Ariel. *Intelligence and Strategic Surprises*. New York: Columbia University Press, 1987.

Lanning, Michael Lee. *Senseless Secrets: The Failures of U.S. Military Intelligence from George Washington to the Present*. New York: Carol Publishing Group, 1996.

Laquer, Walter. *A World of Secrets: The Uses and Limits of Intelligence*. New York: Basic Books, 1985.

Lowenthal, Mark M. *U.S. Intelligence: Evolution and Anatomy*. New York: Praeger, 1984.

Military Intelligence: Its Heroes and Legends, comp. Diane Hamm. Arlington, Va.: U.S. Army Intelligence and Security Command, 1987.

Nelson, Maj. Gen. Otto L. *National Security and the General Staff*. Washington, D.C.: Infantry Journal Press, 1946.

O'Toole, G. J. A. *The Encyclopedia of American Intelligence and Espionage: From the Revolutionary War to the Present*. New York: Facts on File, 1988.

Paddock, Alfred H., Jr. *U.S. Army Special Warfare: Its Origins*. Washington, D.C.: National Defense University Press, 1982.

Petersen, Neal H. *American Intelligence, 1775–1990: A Bibliographical Guide*. Claremont, Calif.: Regina Books, 1992.

Powe, Marc B. and Wilson, Edward E. *The Evolution of American Military Intelligence*. Fort Huachuca, Ariz.: U.S. Army Intelligence Center and School, 1973.

____. "The History of American Military Intelligence--A Review of Selected Literature." *Military Affairs* 39 (1975): 142–45.

Powers, Richard G. *Secrecy and Power: The Life of J. Edgar Hoover*. New York: Free Press, 1987.

Robertson, K. G., ed. *British and American Approaches to Intelligence*. New York: St. Martin's Press, 1987.

Rowan, Richard W., and Dendofer, Robert G. *Secret Service: 33 Centuries of Espionage*. New York: Hawthorne Books, 1967.

Sayle, Edward F. "Historical Underpinnings of the U.S. Intelligence Community." Reprinted from *International Journal of Intelligence and Counterintelligence* 1 (1986).

Stevens, Philip H. *Search Out the Land: A History of American Military Scouts*. Chicago: Rand McNally, 1969.

Smith, Myron J., Jr. *The Secret Wars: A Guide to Sources in English*. 3 vols. Santa Barbara, Calif.: ABC-Clio, 1980.

Strong, Maj. Gen. Sir Kenneth. *Men of Intelligence*. London: Cassell, 1970.

Vagts, Alfred. *The Military Attache*. Princeton: Princeton University Press, 1967.

Volkman, Ernest. *Warriors of the Night: Spies, Soldiers, and American Intelligence*. New York: William Morrow, 1985.

Weinert, Richard P. *A History of Army Aviation, 1950–1962; Phase I: 1950–1954*. Fort Monroe, Va.: U.S. Continental Army Command, 1971.

West, Nigel. *The Sigint Secrets: The Signals Intelligence War, 1900 to Today*. New York: Morrow, 1988.

Military Intelligence, 1775–1885

Alexander, General E. Porter. *Military Memoirs of a Confederate*. Bloomington: Indiana University Press, 1962.

Bakeless, John. *Turncoats, Traitors, and Heroes*. Philadelphia: J. B. Lippincott Co., 1960.

———. *Spies of the Confederacy*. Philadelphia: J. B. Lippincott, 1970.

Baker, L. C. *History of the United States Secret Service*. Philadelphia: L. C. Baker, 1867.

Bates, David Homer. *Lincoln in the Telegraph Office: Recollections of the United States Military Telegraph Corps in the Civil War*. New York: The Century Co., 1907.

Brown, J. Willard. *The Signal Corps, U.S.A. in the War of the Rebellion*. New York: Arno Press, 1974.

Bryan, George S. *The Spy in America*. Philadelphia: Lippincott, 1943.

Byrne, Robert. "Combat Intelligence: The Key to Victory at Gettysburg." *Military Intelligence* (1976): 5–9.

The Civil War: Spies, Scouts, and Raiders. Alexandria, Va.: Time-Life Books, 1985.

Fishel, Edwin C. "The Mythology of Civil War Intelligence." *Civil War History* 10 (1964): 344–67.

———. "Pinkerton and McClellan: Who Deceived Whom?" *Civil War History* 24 (1988): 115–42.

Flexner, James T. *The Traitor and the Spy, Benedict Arnold and John Andre*. New York: Harcourt, Brace, and Co., 1953.

Ford, Corey. *A Peculiar Service*. Boston: Little, Brown, and Co., 1965.

Goetzmann, William H. *Army Exploration in the American West, 1803–1863*. Lincoln: University of Nebraska Press, 1979.

Kane, Harnett T. *Spies for the Blue and Grey*. Garden City, N.Y.: Hanover House, 1954.

McDonald, Archie P., ed. *Make Me a Map of the Valley: The Civil War Journal of Stonewall Jackson's Topographer*. Dallas: Southern Methodist University Press, 1973.

Martin, Steven J. "Custer Didn't Listen." *Military Intelligence* 15 (1989), 15–20.

Miller, Francis T. *Photographic History of The Civil War* (New York: Review of Reviews, 1912.

Pinkerton, Allan. *The Spy of the Rebellion: Being a True History of the Spy System of the United States Army During the Late Rebellion*. New York: G. W. Carleton and Co., 1883.

Schmidt, C. T. "G2, Army of the Potomac." *Military Review* 28 (1948): 45–56.

Sparks, David S. "General Patrick's Progress: Intelligence and Security in the Army of the Potomac." *Civil War History* 10 (1964): 371–84.
Stern, Philip. *Secret Missions of the Civil War*. Chicago: Rand, McNally, 1959.
Swan, Guy C. III et al. "Scott's Engineers." *Military Review* (1983): 61–68.
Tidwell, William A. et al. *Come Retribution: The Confederate Secret Service and the Assassination of Lincoln*. Jackson: University Press of Mississippi, 1988.
Van Doren, Carl. *Secret History of the American Revolution*. New York: Viking Press, 1941.

Military Intelligence, 1885–1941

Bethel, Elizabeth. "The Military Information Division: Origin of the Intelligence Division." *Military Affairs* 11 (1947): 17–24.
Bisher, Jamie. "A Travelling Salesman Fills a Crucial Gap." *Military Intelligence* 15 (1989): 36–37.
Butler, Howard K. *Army Air Corps Airplanes and Observation, 1935–1941*. St. Louis: U.S. Army Aviation Systems Command, 1990.
Coll, Blanche D., Keith, Jean E. and Rosenthal, Herbert. *The Corps of Engineers: Troops and Equipment*. United States Army in World War II. Washington, D.C.: U.S. Army Center of Military History, 1958.
Cutter, C. S. "Intelligence Service in the World War." *Infantry Journal* 20 (1922): 376–83.
Churchill, Marlborough. "The Military Intelligence Division, General Staff." *Journal of the United States Artillery* 52 (1920): 293–315.
Fergusson, Thomas G. *British Military Intelligence, 1870–1914: The Development of a Modern Intelligence Organization*. Frederick, Md.: University Publications of America, 1984.
Finnegan, John P. *Against the Specter of a Dragon: The Campaign for American Military Preparedness, 1914–1917*. Westport, Conn.: Greenwood Press, 1974.
Gilbert, James L. "U.S. Army COMSEC in World War I." *Military Intelligence* 14 (1988): 22–25.
Goddard, George W. *Overview: A Lifelong Adventure in Aerial Photography*. Garden City, N.J.: Doubleday, 1969.
Hitt, Parker. *Manual for the Solution of Military Ciphers*. Fort Leavenworth, Kans.: Press of the Army Service Schools, 1916.
Hubbard, Samuel T. *Memoirs of a Staff Officer, 1917–1919*. Tuckahoe, N.Y.: Cardinal Associates, Inc., 1959.
Johnson, Thomas M. *Without Censor*. Indianapolis: Bobbs-Merrill, 1928.
Linn, Brian McAllister. *The U.S. Army and Counterinsurgency in the Philippine War, 1899–1902*. Chapel Hill: University of North Carolina Press, 1989.
Morgan, William A. "Invasion on the Ether: Radio Intelligence at the Battle of St. Mihiel, September 1918." *Military Affairs* 51 (1987): 57–61.

Parish, John C. "Intelligence Work at First Army Headquarters." *Historical Outlook* 11 (1920): 213–17.

Parson, William Barclay. *The American Engineers in France*. New York: D. Appleton and Company, 1920.

Powe, Mark B. "American Military Intelligence Comes of Age: A Sketch of a Man and His Times." *Military Review* 55 (1975): 17–30.

———. *The Emergence of the War Department Intelligence Agency, 1885–1918*. Manhattan, Kans.: MA/AH Publishing, 1974.

Powell, E. Alexander. *The Army Behind the Army*. New York: Charles Scribner's Sons, 1919.

Scott, Paul R. "The Birth of the 2s: Combat Intelligence in the American Expeditionary Force." *Military Intelligence* 6 (1980): 25–26.

Schwein, Edwin E. *Combat Intelligence: Its Acquisition and Transmission*. Washington, D.C.: Infantry Journal Press, 1936.

Sweeney, Walter C. *Military Intelligence: A New Weapon in War*. New York: Frederick A. Stokes Co., 1924.

Terrett, Dulany. *The Signal Corps: The Emergency*. United States Army in World War II. Washington, D.C.: U.S. Army Center of Military History, 1956.

Thomas, Shipley. *S2 in Action*. Harrisburg: Military Service Publishing Co., 1940.

Trueblood, Edward A. *Observations of an American Soldier During His Service with the AEF in France in the Flash Ranging Service*. Sacramento, Calif.: News Publishing, 1919.

U.S. Army War College, Historical Section. *The United States Army in the World War, 1917–1919*. 14 parts. Washington, D.C.: Department of the Army, 1931.

Van Deman, Ralph H. *The Final Memoranda: Major General Ralph H. Van Deman, USA Ret., 1865–1952: Father of U.S. Military Intelligence*. Ed. Ralph E. Weber. Wilmington, Del.: Scholarly Resources, 1988.

Wagner, Arthur L. *The Service of Security and Information*. Kansas City: Hudson Kimberley Publishing Co., 1893.

War Department. Office of the Chief Signal Officer. *Final Report of the Radio Intelligence Section, General Staff, General Headquarters, American Expeditionary Forces*. Washington, D.C.: Office of the Chief Signal Officer, 1935.

———. *Report of Code Compilation Section, General Headquarters, American Expeditionary Forces, December 1917–November 1918*. Washington, D.C.: Office of the Chief Signal Officer, 1935.

Yardley, Herbert O. *The American Black Chamber*. New York: Bobbs-Merrill, 1931.

World War II Military Intelligence

Alsop, Stewart, and Braden, Thomas. *Sub Rosa: The OSS and American Espionage*. New York: Reynaldo Hancock, 1946.

Ambrose, Stephen E. "Eisenhower, the Intelligence Community, and the D-Day Invasion." *Wisconsin Magazine of History* 64 (1981): 261–77.

Blumenson, Martin. "Will 'Ultra' Rewrite History?" *Army* 28 (1978): 42–49.

Chandler, Stedman, and Robb, Robert W. *Front-Line Intelligence*. Washington, D.C.: Infantry Journal Press, 1946.

Clayton, Aileen. *The Enemy is Listening*. New York: Ballantine Books, 1980.

Cline, Ray S. *The CIA Under Reagan, Bush, and Casey*. Washington, D.C.: Acropolis Press, 1981.

Cochran, Alexander S., Jr. "'Magic,' 'Ultra,' and the Second World War: Literature, Sources, and Outlook." *Military Affairs* 46 (1982): 88–92.

_____. "Protecting the Ultimate Advantage." *Military History* 1 (1985): 42–49.

Conn, Stetson. *Historical Work in the United States Army, 1862–1954*. Washington, D.C.: U.S. Army Center of Military History, 1980.

Davis, Franklin M., Jr. "The Army's Technical Detectives." *Military Review* 28 (1948): 12–18.

Deutsch, Harold C. "Generals and the Use of Intelligence." Intelligence and National Security 3 (1988): 194–260.

_____. "The Historical Impact of Revealing the Ultra Secret." *Parameters* 7 (1977): 16–32.

_____. "The Influence of Ultra on World War II." *Parameters* 8 (1978): 2–15.

Drea, Edward J. "Ultra Intelligence and General Douglas MacArthur's Leap to Hollandia, January–April 1944." *Intelligence and National Security* 5 (1990): 323–49.

Edwards, Duval A. *Spy Catchers of the U.S. Army—In the War with Japan*. Gig Harbor, Washington: Red Apple Publishing, 1994.

Felix, Christopher (James McCarger). *A Short Course in the Secret War*. New York: Dell Publishing, 1988.

Ford, Corey. *Donovan of OSS*. Boston: Little Brown, 1970.

Futrell, Robert F. *Command of Observation Aviation: A Study in Control of Tactical Airpower*. USAF Historical Studies No. 24. Maxwell Air Force Base, Ala.: Air University, 1956.

Gilbert, James L., and Finnegan, John P., eds. *U.S. Army Signals Intelligence in World War II: A Documentary History*. Washington, D.C.: U.S. Army Center of Military History, 1993.

Harrington, Joseph D. *Yankee Samurai: The Secret Role of Nisei in America's Pacific Victory*. Detroit: Pettigrew Enterprises, 1979.

Hinsley, F. H. et al. *British Intelligence in the Second World War: Its Influence on Strategy and Operations*. 3 vols. London: Her Majesty's Stationery Office, 1979–1986.

Hobar, Basil J. "The Ardennes 1944: Intelligence Failure or Deception Success?" *Military Intelligence* 10 (1984): 8–16.

Holmes, Jasper W. *Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific During World War II*. Annapolis, Md.: Naval Institute Press, 1979.

Horner, D. M. *High Command: Australia and Allied Strategy, 1939–1945*. Sydney: George Allen and Unwin, 1982.

Hughes, Les. "The Alamo Scouts." *Trading Post* 45 (1986): 216.
Ind, Allison. *Allied Intelligence Bureau: Our Secret Weapon in the War Against Japan*. New York: McKay, 1958.
Johnson, Thomas M. "Search for the Stolen SIGABA." *Army* 12 (1962): 50–55.
Kahn, David. "World War II History: The Biggest Hole." *Military Affairs* 39 (1975): 74–76.
Kirkpatrick, Lyman B., Jr. *The Real CIA*. New York: MacMillan, 1968.
Koch, Oscar W. *G2: Intelligence for Patton*. Philadelphia: Whitmore, 1971.
Lewin, Ronald. *The Other Ultra*. London: Hutchison, 1982.
Mashbir, Sidney F. *I Was an American Spy*. New York: Vantage, 1953.
Mosser, Richard B. "Colonel Attended Crypto School at Vint Hill Farms." *INSCOM Journal* 15 (1992): 4–9.
Owens, William A. *Eye-Deep in Hell: A Memoir of the Liberation of the Philippines, 1944–1945*. Dallas: Southern Methodist University Press, 1990.
Parrish, Thomas. *The Ultra Americans: The U.S. Role in Breaking the Nazi Codes*. New York: Stein and Day, 1986.
Pash, Boris. *The Alsos Mission*. New York: Award House, 1969.
Powys-Lybbe, Ursula. *The Eyes of Intelligence*. London: William Kimber and Co., Ltd., 1983.
Price, Alfred. *The History of U.S. Electronic Warfare*, vol. 1. Westford, Mass.: Association of Old Crows, 1984.
Putney, Diane, ed. *Ultra and the Army Air Forces in World War II. An Interview with Associate Justice of the Supreme Court Louis F. Powell*. Washington, D.C.: Office of the Chief of Air Force History, 1987.
Rosengarten, Adolph G., Jr. "With ULTRA from Omaha Beach to Weimar, Germany—A Personal View." *Military Affairs* 42 (1978): 127–32.
Russell, Francis. *The Secret War*. Alexandria, Va.: Time-Life Books, 1981.
Sayer, Ian, and Botling, Douglas. *America's Secret Army: The Untold Story of the Counter Intelligence Corps*. London: Grafton Books, 1989.
Schiffman, Maurice K. "Technical Intelligence in the Pacific in World War II." *Military Review* 31 (1952): 42–48.
Schwarzwalder, John. *We Caught Spies*. New York: Duel, Sloan, and Pierce, 1946.
Smith, Bradley. *The Shadow Warriors: OSS and the Origins of the CIA*. New York: Basic Books, 1983.
Smith, Constance Babbington. *Air Spy: The Story of Photo Intelligence in World War II*. New York: Harper, 1957.
Smith, R. Harris. *OSS, The Secret History of America's First Central Intelligence Agency*. Berkeley: University of California Press, 1972.
Spector, Ronald H., ed. *Listening to the Enemy*. Wilmington: Scholarly Resources, 1988.
Spiller, Roger J. "Assessing Ultra." *Military Review* 49 (1979): 13–23.
Stanley, Col. Roy M., II. *World War II Photo Reconnaissance and Photo*

Interpretation Operations of the Allied and Axis Nations. New York: Charles Scribner's Sons, 1981.

Strong, Maj. Gen. Sir Kenneth. *Intelligence at the Top: Recollections of an Intelligence Officer*. New York: Doubleday, 1969.

Syrett, David. "The Secret Wars and the Historians." *Armed Forces and Society* 9 (1983): 293–328.

Thompson, G. R., and Harris, Dixie R. *The Signal Corps: The Outcome*. United States Army in World War II. Washington, D.C.: U.S. Army Center of Military History, 1966.

Thorpe, Brig. Gen. Elliott R. *East Wind, Rain: The Intimate Account of an Intelligence Officer in the Pacific*. Boston: Gambit, 1969.

Troy, Thomas F. *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency*. Frederick, Md.: University Publications of America, 1984.

U.S. Far East Command. General Headquarters. *A Brief History of the G2 Section, GHQ, SWPA, and Affiliated Units*. 10 vols. Far East Command, 1948.

U.S. Forces, European Theater. Report of the General Board: Study No. 12, *The Military Intelligence Service in the European Theater of Operations*. U.S. Forces, European Theater, 1946.

———. Report of the General Board: Study No. 13, *Organization and Operation of the Counter Intelligence Corps in the European Theater of Operations*. U.S. Forces, European Theater, 1946.

———. Report of the General Board: Study No. 14, *Organization and Operation of the Theater Intelligence Service, European Theater of Operations*. U.S. Forces, European Theater, 1946.

———. Report of the General Board: Study No. 19, *The Utilization of Tactical Air Force Reconnaissance Units of the Army Air Forces to Secure Information for Ground Forces in the European Theater*. U.S. Forces, European Theater, 1946.

———. Report of the General Board: Study No. 20, *Liaison Aircraft with Ground Forces Units*. U.S. Forces, European Theater, 1946.

Williams, Robert W. "Moving Information: The Third Imperative." *Army* 25 (1975): 17–21.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press, 1962.

Military Intelligence Since World War II

Allen, Thomas B., and Polgar, Norman. *Merchants of Treason: America's Secrets for Sale*. New York: Delacorte Press, 1982.

Andrade, Dale. *Ashes to Ashes: The Phoenix Program and the Vietnam War*. Lexington, Ky.: D. C. Heath, 1990.

Appleman, Roy H. *South to the Naktong, North to the Yalu. United States Army in the Korean War*. Washington, D.C.: U.S. Army Center of Military History, 1961.

Bamford, James. *The Puzzle Palace: A Report on NSA, America's Most Secret Agency*. Boston: Houghton-Mifflin, 1982.

Bergen, John D. *Military Communications: A Test for Technology*. United States Army in Vietnam. Washington, D.C.: U.S. Army Center of Military History, 1987.

Blair, Clay. *The Forgotten War: America in Korea*. New York: Times Books, 1988.

Clarke, Jeffrey J. *Advice and Support: The Final Years*. United States Army in Vietnam. Washington, D.C.: U.S. Army Center of Military History, 1988.

Cookridge, E. H. Gehlen: *Spy of the Century*. New York: Random House, 1971.

Corson, William R. *The Armies of Ignorance*. New York: Dial Press, 1977.

Cubbage, T. L., II. "Westmoreland vs. CBS: Was Intelligence Corrupted by Policy Demands?" *Intelligence and National Security* 3 (1988): 118–80.

Dabringhaus, Erhard. *Klaus Barbie: The Shocking Story of How the U.S. Used this War Criminal as an Intelligence Agent*. Washington, D.C.: Acropolis Books, 1984.

Davidson, Philip B., and Glass, Robert R. *Intelligence is for Commanders*. Harrisburg: Military Service Publishing, 1948.

DeForest, Orrin, and Chanoff, David. *Slow Burn: The Rise and Bitter Fall of American Intelligence in Vietnam*. New York: Simon and Shuster, 1990.

Emerson, Steven. *Secret Warriors: Inside the Covert Military Operations of the Reagan Era*. New York: Putnam, 1988.

England, James W. *Long-Range Patrol Operations: Reconnaissance, Combat, and Special Operations*. Boulder, Colo.: Paladin Press, 1987.

Fehrenbach, T. R. *This Kind of War: A Study in Unpreparedness*. New York: MacMillan, 1963.

Futrell, Robert F. *The United States Air Force in Southeast Asia: The Advisory Years to 1965*. Washington, D.C.: Office of Air Force History, 1981.

Gordon, Don. "CEWI Battalion: Intelligence and Electronic Warfare on the Battlefield." *Military Intelligence* 5 (1979): 22–28.

———. *Electronic Warfare: Element of Strategy and Multiplier of Combat Power*. New York: Pergamon Press, 1981.

Harmon, Col. William E. "Some Personal Observations on the CEWI Concept." *Military Intelligence* (1983): 4–6.

Hastings, Max. *The Korean War*. New York: Simon and Shuster, 1987.

Herrington, Stuart A. *Silence Was a Weapon: The Vietnam War in the Villages*. Novato: Presidio Press, 1982.

Heymont, Irving. *Combat Intelligence in Modern Warfare*. Harrisburg: Stackpole, 1960.

Hopple, Gerald W., and Watson, Bruce W., eds. *The Military Intelligence Community*. Westview Special Studies on Military Affairs. Boulder, Colo.: Westview Press, 1984.

Howard, William L. "The Army's Stepchild--Technical Intelligence." *Military Intelligence* 15 (1989): 29–32.

James, D. Clayton. *The Years of MacArthur*, vol. 3, *Triumph and Disaster, 1945–1964*. Boston: Houghton-Mifflin, 1985.

Jones, Bruce E. *War Without Windows: A True Account of a Young Army Officer Trapped in an Intelligence Cover-Up*. New York: Vanguard Press, 1987.

Kennedy, Col. William V. et al. *Intelligence Warfare: Today's Advanced Technology Conflict*. New York: Crescent Books, 1983.

Kirkpatrick, Lyman. *The U.S. Intelligence Community: Foreign Policy and Domestic Activities*. New York: Hill and Wang, 1973.

Lung, Col. Hoang Ngoc. *Intelligence*. Indochina Monographs. Washington, D.C.: U.S. Army Center of Military History, 1982.

Marshall, S. L. A. *The River and the Gauntlet: Defeat of the Eighth Army by the Chinese Communist Forces, November 1950, in the Battle of the Chongchon River, Korea*. New York: Morrow, 1953.

McCauley, Nathan E. "The Military Intelligence Profession in the U.S. Army." *Military Intelligence* 13 (1987): 14–17, 37.

McChristian, Joseph A. *The Role of Military Intelligence, 1965–1967*. Washington, D.C.: Department of the Army, 1974.

McQueen, Lt. Col. Arthur D. "The Lion Goes to War." *Military Intelligence* (1977): 28–36.

Paddock, Alfred H. *U.S. Army Special Warfare: Its Origins*. Washington, D.C.: National Defense University Press, 1982.

Palmer, General Bruce, Jr. *The 25-Year War: America's Military Role in Vietnam*. New York: Simon and Shuster, 1984.

Prados, John. *The Soviet Estimate: U.S. Intelligence Analysis and Soviet Military Strength*. Princeton: Princeton University Press, 1986.

_____. *The Hidden History of the Vietnam* War. Chicago: Ivan R. Dee, 1995.

Pyle, Christopher H. *Military Surveillance of Civilian Politics, 1967–1970*. New York: Garland Publishers, 1986.

Ransom, Harry Howe. *The Intelligence Establishment*. Cambridge, Mass.: Harvard University Press, 1970.

Richelson, Jeffrey. *The U.S. Intelligence Community*. Cambridge, Mass.: Ballinger Publishing Co., 1985.

Ridgway, Matthew B. *Soldier: The Memoirs of Matthew B. Ridgway*, as told to Harold H. Martin. Westport: Greenwood Press, 1974.

Ryan, Allan R., Jr. *Klaus Barbie and the United States Government: The Report, with Documentary Appendix, to the Attorney General of The United States*. Frederick, Md.: University Publications of America, 1984.

Saunders, Bruce. "The U.S. Army Intelligence Center and School." *Military Intelligence* 10 (1984): 61.

Schemmer, Benjamin F. "Former DIA Director Urges That Four-Star Should Head All Military Intelligence." *Armed Forces Journal International* (1988): 24.

Sheehan, Neil. *A Bright Shining Lie: John Paul Vann and America in Vietnam*. New York: Random House, 1988.

Singlaub, John K., with Malcolm McConnell. *Hazardous Duty: An American Soldier in the Twentieth Century*. New York: Summit Books, 1991.

Stewart, Col. John F. et al. "Grenada." 7 parts. *Military Intelligence* 11 (1985): 7–24.

Toffler, Alvin and Heidi. *War and Anti-War*. Boston: Little Brown, 1994.

Tolson, John J. *Airmobility, 1961–1971*. Vietnam Studies. Washington, D.C.: Department of the Army, 1973.

Townsend, Elias C. *Risks: The Key to Combat Intelligence*. Harrisburg: Military Service Publishing Co., 1955.

Watson, Bruce W. et al., eds. *United States Intelligence: An Encyclopedia*. New York: Garland Press, 1990.

Willoughby, Maj. Gen. Charles A., and Chamberlain, John. *MacArthur, 1941–1951*. New York: McGraw Hill, 1954.

Glossary

A–2	Air Forces intelligence
AAF	Army Air Forces
ACSI	Assistant Chief of Staff for Intelligence
AEF	American Expeditionary Forces
AFPAC	U.S. Army Forces, Pacific
AIA	Army Intelligence Agency
AIB	Allied Intelligence Bureau
AIS	Army Intelligence and Security (branch)
ALSOS	secret World War II mission to investigate Nazi atomic research
ANCIB	Army-Navy Communications Intelligence Board
ANCICC	Army-Navy Communications Intelligence Coordinating Committee
ASA	Army Security Agency
ATIS	Allied Translator and Interpreter Service
CBB	Central Bureau, Brisbane
CENTCOM	Central Command
CEWI	combat electronic warfare and intelligence
CIA	Central Intelligence Agency
CIC	Counter Intelligence Corps
CID	Criminal Investigation Division
CIP	Corps of Intelligence Police
COMINT	communications intelligence
COMSEC	communications security
CONARC	Continental Army Command
CSA	Chief of Staff of the Army
CONUS	Continental United States
DCSINT	Deputy Chief of Staff for Intelligence
DIA	Defense Intelligence Agency
DOD	Department of Defense

ECM	electronic countermeasures
ELINT	electronic intelligence
ETO	European Theater of Operations
ETOUSA	European Theater of Operations, U.S. Army (World War II)
FBI	Federal Bureau of Investigation
FORSCOM	Forces Command
G–2	Military Intelligence
G–3	Military Operations
GARDEN PLOT	domestic intelligence collection plan (1960s)
GHQ	General Headquarters
HUMINT	human intelligence
IBM	International Business Machines
INSCOM	United States Army Intelligence and Security Command
IOSS	Intelligence Organization and Stationing Study
IRR	Investigative Records Repository
J–2	joint intelligence officer
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Committee
JICPOA	Joint Intelligence Center, Pacific Ocean Area
LANTERN SPIKE	domestic intelligence collection plan (1960s)
MACOM	major Army command
MACV	Military Assistance Command, Vietnam
MAGIC	decrypts of Japanese diplomatic messages
MASINT	measurement and signature intelligence
MDW	Military District of Washington
MI	Military Intelligence
MID	Military Intelligence Division
MITC	Military Intelligence Training Center
MIORC	Military Intelligence Officers Reserve Corps
MIS	Military Intelligence Service
MTO	Mediterranean Theater of Operations
NATO	North African Theater of Operations (World War II); North Atlantic Treaty Organization
NATOUSA	North African Theater of Operations, U.S. Army
NSA	National Security Agency
NSC	National Security Council
OACSI	Office of the Assistant Chief of Staff for Intelligence
ONI	Office of Naval Intelligence
OPEC	Organization of Petroleum Exporting Countries
OPFOR	opposing forces
OSS	Office of Strategic Services
PEARL	intelligence derived from low-level enemy encrypted communications (World War II)

PHOENIX	program to target Viet Cong infrastructure
POA	Pacific Ocean Area (World War II)
RAGFOR	Radio Group, Forward
ROAD	Reorganization Objective Army Division
RRU	radio research unit
SECURITY SHIELD	project to improve U.S. counterintelligence
SIAM	signal information and monitoring
SIGABA	World War II high-level cipher machine
SIGINT	signals intelligence
SIGROD	machine cipher device
SIS	Signal Intelligence Service
SSA	Signal Security Agency
SSO	Special Security Officer
STEADFAST	1973 Army reorganization project
SWPA	South West Pacific Area (World War II)
TD	table of distribution
TDA	table of distribution and allowances
TEMPEST	threat from electronic emissions
THUMB	intelligence derived from radio intelligence
TOE	table of organization and equipment
TRADOC	U.S. Army Training and Doctrine Command
ULTRA	high-grade communications intelligence (World War II)
USAFFE	U.S. Army Forces, Far East
USAINTA	U.S. Army Intelligence Agency
USAINTC	U.S. Army Intelligence Command
USAREUR	U.S. Army, Europe
USARPAC	U.S. Army, Pacific
USASA	U.S. Army Security Agency
USASATC&S	U.S. Army Security Agency Training Center and School
USCIB	U.S. Communications Intelligence Board
WAC	Womens' Army Corps
WDGS	War Department General Staff
YMCA	Young Men's Christian Association

Heraldic Items

Heraldic items for Army units include coats of arms, shoulder sleeve insignia, and distinctive unit insignia. Designed on the basis of a unit's official lineage and honors, they reflect each organization's history, traditions, ideals, mission, and accomplishments. Heraldic items also serve as identifying devices and contribute to unit cohesiveness and esprit de corps.

While the custom of bearing various symbols on shields, helmets, and flags existed in antiquity, heraldry was not introduced until the Middle Ages, when the increased use of armor made it difficult to distinguish friend from foe on the battlefield. Heraldic designs included mythological beasts, emblems commemorative of heroic deeds, and other identifying marks to which specific symbolism was ascribed. These heraldic devices were placed on a surcoat worn over the armor, from which the term "coat of arms" was derived. Gradually, a formal system of heraldry evolved, complete with rules for design, use, and display.

At the present time Army regiments and separate battalions are authorized coats of arms. A complete coat of arms consists of a shield, a crest, and a motto. The shield, the most important portion of the coat of arms, contains the field or ground on which the charges or symbols are placed. The crest was originally placed on the top of the helmet of the chief or leader to enable his followers to recognize him during battle. Today the crest is placed upon a wreath of six skeins or twists composed of the principal metal and primary color of the shield, alternately, in the order named. This wreath or torse represents the piece of cloth which the knight twisted around the top of his helmet and by means of which the actual crest was attached. Mottoes have been in use longer than coats of arms. Many of the older ones originated from war cries. Usually of an idealistic nature, they sometimes allude to a well-known event in the history of the unit.

The elements of the coat of arms are embroidered on the organizational flag (color), the central element of which is the American eagle. The shield of the coat of arms is on the eagle's breast, a scroll bearing the motto is held in his beak, and the crest is placed above his head. A crest to the coat of arms is authorized for Regular Army units that have war service or campaign credit.

Army National Guard units display the crest of the state or states in which they are located, and a special crest has been designed for all Army Reserve units.

The currently authorized embroidered shoulder sleeve insignia had their origin during World War I. They serve the same purpose as the corps symbols (badges) used during the Civil War and the War with Spain. Most corps badges were of simple design and could be cut from a single piece of cloth. These emblems, such as a four-leaf clover, a star, or a spearhead, were easily remembered and readily identified. Not only were they worn by soldiers on their headgear, they were also incorporated into the design of unit flags.

The first shoulder sleeve insignia is believed to have been worn by the men of the 81st Division during World War I. On their voyage to France they adopted as their insignia the figure of a wildcat, which they used as a distinctive marking for the division's equipment. Wear of this insignia was officially approved on 19 October 1918 by a telegram from the Adjutant General, American Expeditionary Forces, to the division commander. Insignia for other units of the American Expeditionary Forces were later authorized and designs officially approved. Designs varied greatly. Many had their origin in devices already in use for organizational and equipment markings. Others were based on monograms and geometric figures alluding to a unit's numerical designation. Symbols associated with traditions, geographical locations, and unit mission were also included in some designs.

Since World War I the authorization of shoulder sleeve insignia has expanded. Under the current system, separate brigades and higher echelons are authorized shoulder sleeve insignia for wear by soldiers assigned to the units. The insignia also appear on the organizations' distinguishing flags. Over time, the designs have become more elaborate and complex due to the increased number of authorized insignia and the availability of embroidery machinery for the production of various types of textile insignia. During the Vietnam era the policy governing the wear of subdued insignia on work uniforms was established.

Distinctive unit insignia, manufactured in metal and enamel and worn by all unit personnel, are authorized for separate battalions and higher echelons. The type of distinctive unit insignia currently in use was first authorized during the 1920s for regiments and certain other units. As in the case of shoulder sleeve insignia and coats of arms, authorization expanded as changes in the organization of the Army took place. The designs are based on symbols reflecting each unit's lineage, battle honors, traditions, and mission and usually incorporate the organization's motto. Distinctive unit insignia for most regiments and battalions include the same design elements as their coats of arms.

Today, as in the past, insignia displayed on flags and worn on uniforms are highly visible items of identification. These heraldic items serve to distinguish specific organizations and their members and are significant factors in establishing and maintaining unit esprit de corps.

66th Military Intelligence Brigade

111th Military Intelligence Brigade

112th Military Intelligence Brigade

201st Military Intelligence Brigade

205th Military Intelligence Brigade

207th Military Intelligence Brigade

319th Military Intelligence Brigade

470th Military Intelligence Brigade

500th Military Intelligence Brigade

501st Military Intelligence Brigade

504th Military Intelligence Brigade

513th Military Intelligence Brigade

525th Military Intelligence Brigade

108th Military Intelligence Group

109th Military Intelligence Group

115th Military Intelligence Group

116th Military Intelligence Group

259th Military Intelligence Group

650th Military Intelligence Group

902d Military Intelligence Group

1st Military Intelligence Battalion

2d Military Intelligence Battalion

3d Military Intelligence Battalion

14th Military Intelligence Battalion

15th Military Intelligence Battalion

24th Military Intelligence Battalion

101st Military Intelligence Battalion

102d Military Intelligence Battalion

103d Military Intelligence Battalion

104th Military Intelligence Battalion

105th Military Intelligence Battalion

106th Military Intelligence Battalion

107th Military Intelligence Battalion

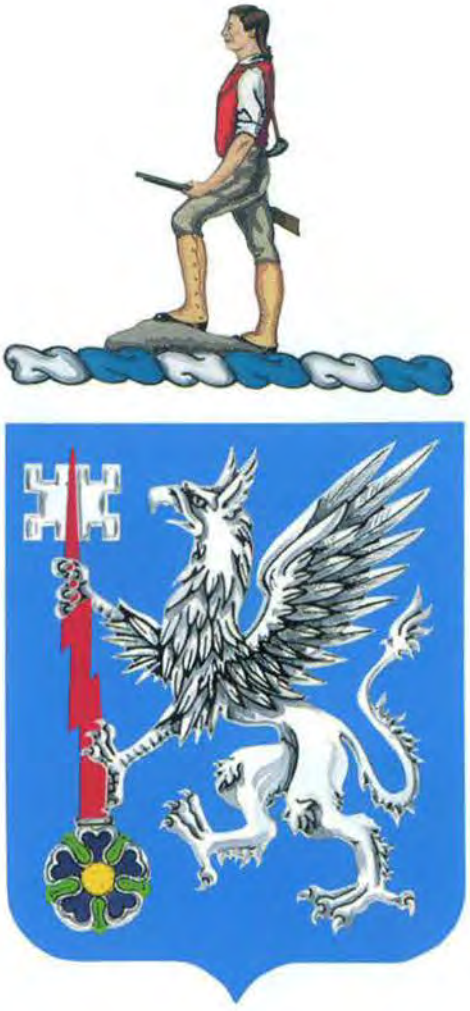
108th Military Intelligence Battalion

109th Military Intelligence Battalion

110th Military Intelligence Battalion

124th Military Intelligence Battalion

125th Military Intelligence Battalion



126th Military Intelligence Battalion

128th Military Intelligence Battalion

134th Military Intelligence Battalion

135th Military Intelligence Battalion

138th Military Intelligence Battalion

140th Military Intelligence Battalion

141st Military Intelligence Battalion

142d Military Intelligence Battalion

147th Military Intelligence Battalion

163d Military Intelligence Battalion

165th Military Intelligence Battalion

201st Military Intelligence Battalion

202d Military Intelligence Battalion

203d Military Intelligence Battalion

204th Military Intelligence Battalion

205th Military Intelligence Battalion

206th Military Intelligence Battalion

223d Military Intelligence Battalion

224th Military Intelligence Battalion

229th Military Intelligence Battalion

260th Military Intelligence Battalion

297th Military Intelligence Battalion

301st Military Intelligence Battalion

302d Military Intelligence Battalion

303d Military Intelligence Battalion

304th Military Intelligence Battalion

305th Military Intelligence Battalion

306th Military Intelligence Battalion

307th Military Intelligence Battalion

308th Military Intelligence Battalion

309th Military Intelligence Battalion

310th Military Intelligence Battalion

311th Military Intelligence Battalion

312th Military Intelligence Battalion

313th Military Intelligence Battalion

314th Military Intelligence Battalion

319th Military Intelligence Battalion

326th Military Intelligence Battalion

337th Military Intelligence Battalion

338th Military Intelligence Battalion

341st Military Intelligence Battalion

344th Military Intelligence Battalion

373d Military Intelligence Battalion

415th Military Intelligence Battalion

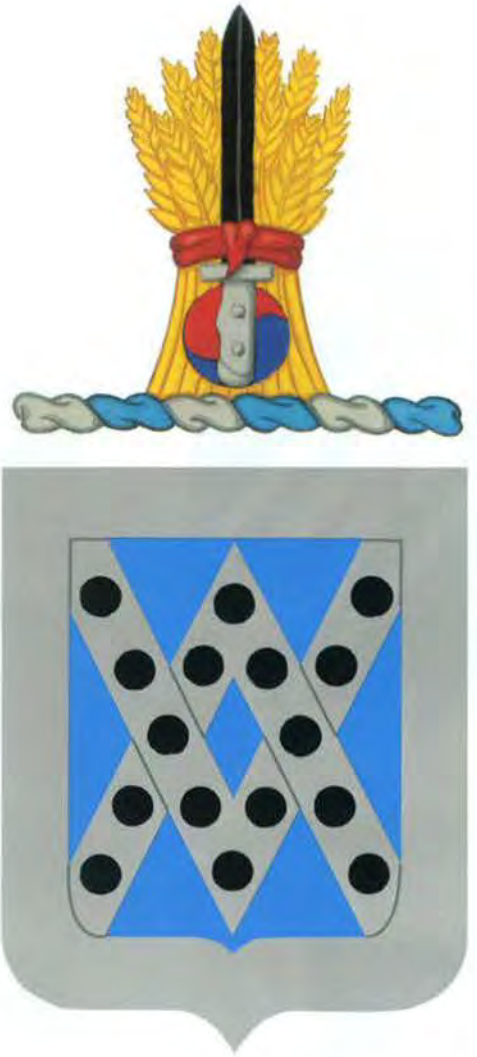
501st Military Intelligence Battalion

502d Military Intelligence Battalion

511th Military Intelligence Battalion

519th Military Intelligence Battalion

522d Military Intelligence Battalion



524th Military Intelligence Battalion

527th Military Intelligence Battalion

532d Military Intelligence Battalion

533d Military Intelligence Battalion

542d Military Intelligence Battalion

549th Military Intelligence Battalion

550th Military Intelligence Battalion

629th Military Intelligence Battalion

LINEAGES AND HERALDIC DATA

MILITARY INTELLIGENCE CORPS

Heraldic Items

Coat of Arms

Shield: Azure, a key bend sinisterwise in saltire with a lightning flash argent, in fesspoint overall a sphinx or.

Crest: On a wreath of the colors, argent and azure, a torch or enflamed proper in front of two swords in saltire with hilts gold and blades of the first.

Motto: ALWAYS OUT FRONT.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence. The key, flash, and sphinx symbolize the three basic categories of intelligence: human, signal, and tactical.

The flaming torch between the crossed swords suggests the illumination as provided by intelligence upon the field of battle.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 66th MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Shoulder Sleeve Insignia

Description: On a silver gray hexagon, one point up, with an oriental blue border, an oriental blue hexagon bearing a yellow sphinx superimposed by a silver gray dagger hilted black.

Symbolism: Oriental blue and silver gray, representing loyalty and determination, are the colors of the military intelligence branch. Yellow symbolizes excellence. The hexagon borders reflect the numerical designation of the brigade. The sphinx, a traditional military intelligence symbol, indicates observation, wisdom, and discreet silence. The unsheathed dagger reflects aggressive and protective requirements and the element of physical danger inherent in the mission of the unit.

Distinctive Unit Insignia

Description: A gold color metal and enamel device consisting of a hexagon composed of a checky of six black and white sections (one angle up), surmounted throughout by a smaller hexagon (flat side up) composed of a checky of nine sections of gold and oriental blue with the center square charged with a gold sphinx head, all above a gold scroll inscribed HONOR VALOR AND SECURITY in oriental blue letters.

Symbolism: The black and white sections symbolize enlightenment and knowledge both day and night around the world. The checky represents the unit's tactical and strategic capabilities in counterintelligence. The sphinx, a traditional intelligence symbol, indicates observation, wisdom, and discreet silence. The hexagon within a hexagon further distinguishes the numerical designation of the organization.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 21 June 1944 in the Army of the United States as the 66th Counter Intelligence Corps Detachment. Activated 1 July 1944 at Camp Rucker, Alabama. Inactivated 12 November 1945 at Camp Kilmer, New Jersey. Activated 10 November 1949 in Germany. Allotted 20 September 1951 to the Regular Army.

Reorganized and redesignated 20 December 1952 as the 66th Counter Intelligence Corps Group. Reorganized and redesignated 1 January 1960 as the 66th Military Intelligence Group. Redesignated 25 July 1961 as the 66th Intelligence Corps Group. Redesignated 15 October 1966 as the 66th Military Intelligence Group.

Reorganized and redesignated 16 October 1986 as Headquarters and Headquarters Company, 66th Military Intelligence Brigade. Reorganized and redesignated 16 October 1992 as Headquarters and Headquarters Detachment, 66th Military Intelligence Brigade. Inactivated 16 July 1995 in Germany.

CAMPAIGN PARTICIPATION CREDIT

World War II

Northern France

DECORATIONS

None.

HEADQUARTERS
111th MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Distinctive Unit Insignia

Description: A gold color metal and enamel device consisting of the major portion of a black and gold heraldic rose above and behind the head and wings of a gold eagle rising out of a gold disc charged throughout with a burst of red flames having eight tongues radiant to base and interspersed with seven five-pointed oriental blue stars, the disc enclosed by an oriental blue scroll inscribed with the words MISSION FIRST in gold.

Symbolism: The heraldic rose, alluding to the insignia of the military intelligence branch, is symbolic of the basic mission (to collect, check, and make available any information about a present or possible enemy), and its position at the top of the design is relative to the unit's motto. The phoenix (eagle) rising out of flames is symbolic of the former location of the unit, Atlanta, Georgia, and the seven states where the unit operated are represented by the ring of oriental blue stars.

Flag Device

None approved.

LINEAGE AND HONORS

RA
(active)

LINEAGE

Constituted 10 May 1946 in the Army of the United States as the 111th Counter Intelligence Corps Detachment. Activated 22 May 1946 at Atlanta, Georgia. Allotted 6 October 1950 to the Regular Army. Redesignated 1 December 1958 as the 111th Counter Intelligence Corps Group. Redesignated 25 July 1961 as the 111th Intelligence Corps Group. Redesignated 15 October 1966 as the 111th Military Intelligence Group. Inactivated 9 January 1973 at Fort McPherson, Georgia.

Redesignated 13 March 1987 as Headquarters, 111th Military Intelligence Brigade; concurrently transferred to the United States Army Training and Doctrine Command and activated at Fort Huachuca, Arizona.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

HEADQUARTERS
112TH MILITARY INTELLIGENCE BRIGADE

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A silver color metal and enamel device consisting of a yellow enameled demi-sun emitting five rays surmounted by a silver dagger, point up, beneath an oriental blue chevron bearing five silver stars, all within and below an arc segment of silver oak leaves and a red scroll inscribed with the motto STRENGTH THROUGH SECURITY in silver letters.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence. The sunburst further alludes to intelligence and also suggests the former location of the unit, the great Southwest. The yellow sunburst symbolizes the worth of reliable intelligence. The five rays of the sunburst allude to the five former regions of the unit and the chevron, a symbol for support, with the five stars, represents the five states which comprised its former area of operations. The ancient dagger signifies the dangers and silent covert nature of intelligence service. The oak leaves are symbolic of the strong and enduring resolution of the members of the unit, and the motto portrays the goal of a successful intelligence organization.

FLAG DEVICE

None approved.

LINEAGE AND HONORS

RA
(inactive)

LINEAGE

Constituted 10 May 1946 in the Army of the United States as the 112th Counter Intelligence Corps Detachment. Activated 21 May 1946 at Dallas, Texas. Allotted 26 February 1951 to the Regular Army. Redesignated 1 August 1957 as the 112th Counter Intelligence Corps Group. Redesignated 25 July 1961 as the 112th Intelligence Corps Group. Redesignated 15 October 1966 as the 112th Military Intelligence Group. Inactivated 30 June 1974 at Fort Sam Houston, Texas.

Redesignated 1 July 1987 as Headquarters, 112th Military Intelligence Brigade; concurrently transferred to the United States Army Training and Doctrine Command and activated at Fort Devens, Massachusetts. Inactivated 30 January 1993 at Fort Devens, Massachusetts.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 201st MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Shoulder Sleeve Insignia

Description: On a shield divided from upper left to lower right, silver gray above oriental blue with a yellow border, a sword between two flashes all yellow.

Symbolism: Oriental blue and silver gray are the military intelligence branch colors. The two parts symbolize the responsibility for acquisition and processing of tactical and strategic intelligence. The sword symbolizes the aggressiveness and physical danger inherent in military intelligence operations.The lightning bolts refer to the electronic warfare capabilities of the unit and the commander's need for accurate and ready intelligence from all sources.

Distinctive Unit Insignia

Description: A silver color metal and enamel device consisting of an oriental blue disc bearing a silver polestar encircled at top and sides by a black scroll inscribed WITH COURAGE AND VISION in silver letters, and in base three alternate wavy bars of oriental blue and silver superimposed by a silver mountain peak supporting a griffin segreant grasping a sword and a lightning flash, all gold.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence. Black denotes secrecy. The oriental blue disc superimposed by the silver polestar symbolizes the world and the far-reaching capabilities of the unit. The oriental blue and silver wavy bars allude to World War II campaign participation in the Pacific. The mountain peak is representative of Korean War campaigns. The griffin, having the keen eyesight of an eagle and the strength and courage of a lion, indicates the attributes of military intelligence and also alludes to the motto. The lightning flash is indicative of communications, electronic warfare capabilities, and the origin of the brigade as a signal unit. The sword reflects the fighting aspect and suggests the unit's aggressiveness and the physical danger inherent in military intelligence operations.

LINEAGE AND HONORS

RA
LINEAGE (active)

Constituted 23 July 1942 in the Army of the United States as the 323d Signal Company, Wing. Activated 1 September 1942 at Miami, Florida. Inactivated 17 October 1946 at Andrews Field, Maryland. Redesignated 6 September 1950 as the 323d Signal Radio Intelligence Company and allotted to the Organized Reserve Corps. Activated 2 October 1950 at Fort Myer, Virginia.

Converted and redesignated 3 January 1951 as Headquarters and Headquarters Company, 601st Communication Reconnaissance Group. Redesignated 5 February 1951 as Headquarters and Headquarters Company, 503d Communication Reconnaissance Group. Ordered into active military service 1 May 1951 at Fort Myer, Virginia. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Released from active military service 16 May 1955 and reverted to reserve status. Inactivated 20 July 1955 at Fort Myer, Virginia. Activated 6 January 1956 at Washington, D.C. Redesignated 3 September 1956 as Headquarters and Headquarters Company, 503d Army Security Agency Group. Inactivated 27 June 1959 at Washington, D.C.

Withdrawn 1 September 1987 from the Army Reserve, allotted to the Regular Army, consolidated with the 201st Military Intelligence Detachment (see ANNEX), and consolidated unit redesignated as Headquarters and Headquarters Detachment, 201st Military Intelligence Brigade; concurrently activated at Fort Lewis, Washington.

ANNEX

Constituted 12 July 1944 in the Army of the United States as the 201st Counter Intelligence Corps Detachment. Activated 20 August 1944 in New Guinea. Inactivated 25 February 1946 in Japan. Activated 6 October 1950 in Korea. Inactivated 21 February 1955 in Korea. Allotted 20 March 1956 to the Regular Army. Activated 12 June 1956 in Korea. Reorganized and redesignated 15 May 1959 as the 201st Military Intelligence Detachment. Inactivated 30 June 1971 in Korea. Activated 1 October 1971 at Fort Hood, Texas. Inactivated 21 June 1975 at Fort Hood, Texas.

CAMPAIGN PARTICIPATION CREDIT

World War II

Antisubmarine
New Guinea
Western Pacific
Luzon

Korean War

UN Offensive
CCF Intervention
First UN Counteroffensive
CCF Spring Offensive
UN Summer-Fall Offensive
Second Korean Winter
Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered PACIFIC THEATER (323d Signal Company, Wing, cited; GO 83, Twentieth Air Force, 4 October 1945)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (201st Counter Intelligence Corps Detachment cited; DA GO 32, 1954)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (201st Counter Intelligence Corps Detachment cited; DA GO 47, 1950)

HEADQUARTERS AND HEADQUARTERS DETACHMENT 205th MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Shoulder Sleeve Insignia

Description: On an oriental blue shield a white fleur-de-lis centered in front of two crossed silver gray lightning bolts.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence units. The crossed lightning bolts refer to the convergence of all types of intelligence from all sources, enabling commanders to "see the battlefield." The fleur-de-lis alludes to the unit's original activation in France.

Distinctive Unit Insignia

Description: A gold color metal and enamel device consisting of an oriental blue fleur-de-lis bearing in gold a dagger, point down, between a lightning flash and a propeller blade all convergent in base on a silver gray background enclosed at the bottom by a gold wreath of rice tied in red and at the top by an oriental blue scroll inscribed VANGUARD OF VIGILANCE in gold letters.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with the military intelligence branch. The oriental blue fleur-de-lis refers to the unit's World War II service in Europe. Campaign participation in Vietnam is symbolized by the gold and red wreath of rice. The lightning flash represents signals intelligence and electronic warfare; the dagger represents human intelligence; the airplane propeller represents airborne imagery intelligence. The slanting of these symbols of the intelligence disciplines employed by the unit toward the fulcrum of the fleur-de-lis represents the convergence of intelligence from all sources to enable commanders to "see the battlefield."

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 12 July 1944 in the Army of the United States as the 205th Counter Intelligence Corps Detachment. Activated 6 August 1944 in France. Allotted 6 October 1950 to the Regular Army. Reorganized and redesignated 25 June 1958 as the 205th Military Intelligence Detachment.

Consolidated 16 October 1983 with the 135th Military Intelligence Group (see ANNEX) and consolidated unit reorganized and redesignated as Headquarters and Headquarters Detachment, 205th Military Intelligence Group. Reorganized and redesignated 16 October 1985 as Headquarters and Headquarters Detachment, 205th Military Intelligence Brigade.

ANNEX

Constituted 19 March 1966 in the Regular Army as the 135th Intelligence Corps Group. Activated 1 June 1966 at Fort Bragg, North Carolina. Redesignated 15 October 1966 as the 135th Military Intelligence Group. Inactivated 25 September 1969 in Vietnam.

CAMPAIGN PARTICIPATION CREDIT

World War II
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

Vietnam
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969

DECORATIONS

None.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 207th MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Shoulder Sleeve Insignia

Description: On an oriental blue disc a silver gray key and lightning bolt crossed slightly above center, with the key's ward at the lower left and the lightning bolt's point to the right, centered below is a dagger, point up, with silver gray blade and black hilt; all within a narrow red outline of a seven-petaled stylized rose.

Symbolism: Oriental blue and silver gray are associated with military intelligence. Red derives from the predominant color of the VII Corps shoulder sleeve insignia and black represents the unknown. The key and lightning bolt represent electronic warfare and security and also signify the numeral two of the unit's designation. The stylized seven-petaled rose has its origin in the more traditional compass, dagger, and rose associated with the military intelligence branch and also represents the numeral seven of the unit's designation as well as the number of the corps it supported. The circular shape of the insignia also refers to the zero of the unit's designation. The dagger denotes the counterintelligence function of the unit.

Distinctive Unit Insignia

Description: A gold color metal enamel device consisting of an oriental blue five-petaled heraldic rose and centered vertically thereon a gold lightning bolt surmounted at the bottom by a horizontal gold key, surmounting the lightning bolt at center a white horse's head between two white wings, each with seven feathers. Attached to the bottom of the device a scroll of three parts inscribed with the words SEE STRIKE KNOW in black letters.

Symbolism: Oriental blue is one of the colors associated with the military intelligence branch. The heraldic rose, a part of the military intelligence insignia, indicates the brigade's association with that branch. The winged horse (Pegasus) with seven feathers on each wing signifies aerial vigilance in support of the VII Corps. The key denotes the unlocking of the enemy's secrets.

The lightning bolt represents the unit's electronic warfare capability and its ability to transmit information rapidly.

LINEAGE AND HONORS

RA
LINEAGE (inactive)

Constituted 10 May 1946 in the Army of the United States as the 113th Counter Intelligence Corps Detachment. Activated 20 May 1946 at Chicago, Illinois. Allotted 6 December 1950 to the Regular Army. Redesignated 1 August 1957 as the 113th Counter Intelligence Corps Group. Redesignated 25 July 1961 as the 113th Intelligence Corps Group. Redesignated 15 October 1966 as the 113th Military Intelligence Group. Inactivated 31 December 1971 at Fort Sheridan, Illinois.

Consolidated 16 October 1983 with the 207th Military Intelligence Detachment (see ANNEX) and consolidated unit reorganized and redesignated as Headquarters and Headquarters Detachment, 207th Military Intelligence Group. Reorganized and redesignated 16 October 1985 as Headquarters and Headquarters Detachment, 207th Military Intelligence Brigade. Inactivated 15 January 1992 in Germany.

ANNEX

Constituted 8 November 1950 in the Regular Army as the 207th Counter Intelligence Corps Detachment. Activated 30 November 1950 at Fort Holabird, Maryland. Reorganized and redesignated 25 June 1958 as the 207th Military Intelligence Detachment.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia
Defense of Saudi Arabia
Liberation and Defense of Kuwait
Cease-Fire

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered FIFTH ARMY AREA 1946 (113th Counter Intelligence Corps Detachment cited; DA GO 10, 1948)

HEADQUARTERS AND HEADQUARTERS COMPANY 319th MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Shoulder Sleeve Insignia

Description: On a rectangle arched at top and bottom with a silver gray border, divided beveled from upper right to lower left black above oriental blue, in upper left an oriental blue polestar pierced silver gray.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. Blue also alludes to the Pacific and the unit's area of operations. Black and blue suggest day and night vigilance. The polestar simulates satellite intelligence collection and communications. The jagged division of the background is reminiscent of a lightning bolt, symbolizing speed, accuracy, and electronic information and systems.

Distinctive Unit Insignia

Description: A silver color metal and enamel device consisting of a silver sunburst within an oriental blue oval (with axis vertical) inscribed EYES OF THE PACIFIC in silver letters, overall a diagonal red lightning bolt from lower left to upper right superimposed by a silver knight's helmet crested with a griffin's head in shades of light brown.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. The griffin, a mythical beast, with keen eyesight and acute hearing, symbolizes constant vigilance. The helmet with the visor closed connotes covert capabilities as well as military preparedness. The sunburst symbolizes knowledge and truth; the lightning bolt underscores electronic communications, speed, and accuracy.

Lineage and Honors

AR

Lineage (active)

Constituted 27 May 1948 in the Organized Reserve Corps as the 319th Headquarters Intelligence Detachment. Activated 15 June 1948 at Springfield, Massachusetts. Inactivated 22 September 1949 at Springfield, Massachusetts. Redesignated 18 August 1950 as Headquarters, 319th Military Intelligence Group. Activated 1 September 1950 at San Francisco, California. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 1 February 1953 at San Francisco, California.

Redesignated 17 September 1988 as Headquarters and Headquarters Company, 319th Military Intelligence Brigade, and activated at Fort Lewis, Washington.

Campaign Participation Credit

None.

Decorations

None.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 470th MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Shoulder Sleeve Insignia

Description: On a silver gray rectangle arched at top and bottom with a black border, a vertical oriental blue stripe and overall a black griffin's head.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. The three sections of the background refer to the three types of intelligence: human, signals, imagery. The blue stripe bordered by two gray stripes suggests the Panama Canal and refers to collecting and funneling information. It also alludes to the unit's location. The griffin, a mythological creature of vigilance and strength, a guardian of gold, symbolizes the unit's mission. Black represents the secrecy of the operations.

Distinctive Unit Insignia

Description: A silver color metal and enamel device consisting of an erect silver key, double-warded in base, the bow of seven radiating rays and surmounting overall an oriental blue torch with a red flame. Encircling the device in base, the ends terminating at the opposite lower corners of the flame, an oriental blue scroll bearing the inscription TRUTH SECURITY LOYALTY in silver letters.

Symbolism: Oriental blue and silver gray are the colors used for military intelligence. The key, a symbol of authority, secrecy, and wardenship, refers to the basic mission of the organization. The double wards allude to intelligence and counterintelligence and the seven rays of the bow, a reference to the numeral seven, symbolize revealing light, security, and wisdom. The torch represents guidance. Blue represents truth, and red, zeal and valor.

Lineage and Honors

RA

Lineage (active)

Constituted 12 July 1944 in the Army of the United States as the 470th Counter Intelligence Corps Detachment. Activated 31 July 1944 in the Canal Zone. Allotted 19 October 1951 to the Regular Army. Redesignated 25 July 1961 as the 470th Intelligence Corps Detachment. Reorganized and redesignated 14 September 1964 as the 470th Intelligence Corps Group. Redesignated 15 October 1966 as the 470th Military Intelligence Group.

Reorganized and redesignated 16 October 1987 as Headquarters and Headquarters Company, 470th Military Intelligence Brigade. Reorganized and redesignated 16 October 1991 as Headquarters and Headquarters Detachment, 470th Military Intelligence Brigade.

Campaign Participation Credit

World War II

American Theater, Streamer without inscription

Armed Forces Expeditions

Panama

Decorations

None.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 500th MILITARY INTELLIGENCE BRIGADE (Pacific Vanguard)

Heraldic Items

Shoulder Sleeve Insignia

Description: An oriental blue rectangle arched at top and bottom with a silver gray border bearing a crossed yellow lightning flash and sword surmounted by an oriental blue globe gridlined and outlined silver gray, and overall a yellow torch with red flame.

Symbolism: Oriental blue and silver gray are traditionally associated with the military intelligence branch. The sword signifies vigilance, the lightning flash alludes to electronic communications and speed, the globe symbolizes worldwide service, and the torch and flame signify knowledge.

Distinctive Unit Insignia

Description: A gold color metal and enamel device consisting of an oriental blue conical shape with apex at base bearing a white radiant sun behind a white snowcapped black mountain peak, overall a gold palm tree eradicated, surmounted by a scarlet and ultramarine blue taeguk, and in base a gold Siamese headdress all between two gold bamboo trees with shoots arched, all enclosed at the top with a gold scroll inscribed SCIENTIA POTENTIA EST (KNOWLEDGE IS STRENGTH) in scarlet letters.

Symbolism: Oriental blue is one of the colors used by Army intelligence units. Service in Japan is commemorated by the silhouette of Mount Fuji, while the palm tree denotes service in Hawaii. This unit had intelligence responsibility for several areas: the Republic of Korea, indicated by the red and blue taeguk; Taiwan, represented by the white sun from the Republic of China flag; the Republic of Vietnam, indicated by the bamboo trees; and Thailand, denoted by the Siamese headdress.

Lineage and Honors

RA

Lineage (active)

Constituted 30 June 1952 in the Regular Army as Headquarters, 500th Military Intelligence Service Group. Activated 1 September 1952 in Japan. Reorganized and redesignated 28 March 1954 as Headquarters, 500th Military Intelligence Group. Reorganized and redesignated 1 July 1955 as Headquarters and Headquarters Company, 500th Military Intelligence Group. Reorganized and redesignated 24 June 1957 as the 500th Military Intelligence Group. Inactivated 25 March 1958 in Japan. Activated 25 March 1961 in Japan. Redesignated 25 July 1961 as the 500th Intelligence Corps Group. Redesignated 15 October 1966 as the 500th Military Intelligence Group.

Reorganized and redesignated 16 October 1987 as Headquarters and Headquarters Company, 500th Military Intelligence Brigade. Reorganized and redesignated 16 October 1992 as Headquarters and Headquarters Detachment, 500th Military Intelligence Brigade.

Campaign Participation Credit

None.

Decorations

Meritorious Unit Commendation (Army), Streamer embroidered PACIFIC AREA 1968–1969 (500th Military Intelligence Group cited; DA GO 75, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered PACIFIC AREA 1972–1974 (500th Military Intelligence Group cited; DA GO 13, 1975)

Army Superior Unit Award, Streamer embroidered 1986–1987 (500th Military Intelligence Group cited; DA GO 14, 1989)

HEADQUARTERS AND HEADQUARTERS COMPANY 501st MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Shoulder Sleeve Insignia

Description: On a vertical rectangle arched convexly at top and bottom divided vertically silver gray and oriental blue all within a yellow border, a double-warded inverted yellow key between two yellow lightning flashes issuing from upper left and right corners and conjoining the shaft of the key just above the double ward.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence and also refer to the constant day and night vigilance mission of the unit. The key is symbolic of authority and control and alludes to security. The lightning flashes are symbolic of worldwide electronic communications and the double-warded key conjoined with the two lightning flashes symbolizes military intelligence and security united.

Distinctive Unit Insignia

Description: A silver color metal and enamel device consisting of a silver color rectangle bounded on either side by a vertical white sword at left and a vertical black sword at right, point up, and enclosed at the top and bottom by two arched oriental blue scrolls passing over the ends of the swords and inscribed IN UNITATE (IN UNITY) on the top scroll and ET VIGILIA (AND VILIGANCE) on the bottom scroll in silver letters. On the rectangle a red oriental dragon, his body curved from left to right with tail at top and head below, grasping in his right claw a blue lightning bolt crossed over a blue double-warded key grasped in his left claw.

Symbolism: Oriental blue and silver gray are the branch colors of military intelligence. The red dragon represents the Orient and the lineage of the organization. The lightning bolt signifies worldwide electronic communications and the key symbolizes security and control; crossed in saltire, they represent strength and symbolize Army Security Agency and military intelligence units. The swords are adapted from the military intelligence branch insignia. Their colors, white and black, signify day and night and the continuous mission of the unit.

Lineage and Honors

RA

Lineage (active)

Constituted 13 October 1950 in the Regular Army as Headquarters and Headquarters Company, 501st Communication Reconnaissance Group. Activated 20 October 1950 at Camp Pickett, Virginia. Redesignated 1 July 1956 as Headquarters and Headquarters Company, 501st Army Security Agency Group. Inactivated 15 October 1957 in Korea.

Redesignated 1 January 1978 as Headquarters and Headquarters Company, 501st Military Intelligence Group, and activated in Korea. Reorganized and redesignated 16 October 1986 as Headquarters and Headquarters Company, 501st Military Intelligence Brigade. Reorganized and redesignated 16 October 1992 as Headquarters and Headquarters Detachment, 501st Military Intelligence Brigade. Reorganized and redesignated 16 November 1995 as Headquarters and Headquarters Company, 501st Military Intelligence Brigade.

Campaign Participation Credit

Korean War

CCF Spring Offensive
UN Summer-Fall Offensive
Second Korean Winter
Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953

Decorations

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (Headquarters and Headquarters Company, 501st Communication Reconnaissance Group, cited; DA GO 22, 1954)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA 1951–1953 (Headquarters and Headquarters Company, 501st Communication Reconnaissance Group, cited; DA GO 76, 1953)

HEADQUARTERS AND HEADQUARTERS DETACHMENT 504th MILITARY INTELLIGENCE BRIGADE

Heraldic Items

Shoulder Sleeve Insignia

Description: On an oriental blue shield with a yellow border a silver gray winged lightning flash with wings elevated, the flash topped with a silver gray demi-fleur-de-lis.

Symbolism: Oriental blue and silver gray are the colors associated with the military intelligence branch. The wings suggest loftiness or the advantage obtained from clear observation. The lightning flash alludes to the unit's ability to respond accurately and quickly in support of the commander's needs for intelligence from all sources. The demi-fleur-de-lis is a symbol both of intelligence and of the brigade's roots in the campaigns of Northern France, Rhineland, and Central Europe. Yellow signifies excellence and achievement.

Distinctive Unit Insignia

Description: A gold color metal and enamel device consisting of a vertical red enamel winged lightning flash with wings elevated, tipped with a demi-fleur-de-lis, all within a continuous blue scroll arched at top and base and passing behind the wings and demi-fleur-de-lis at the sides and top and inscribed SEMPER PRAEPARATUS (ALWAYS YOU ARE PREPARED) in gold letters and all areas enclosed by the wings and scroll are checky of gold and silver gray.

Symbolism: Oriental blue and silver gray are the colors used for the military intelligence branch. Wings connote loftiness, a vantage point for visual observation. The lightning flash and checky area represent technological capabilities, symbolize vigilant leadership, celerity, and communications, and allude to the unit's concern with control over hostile communications and security of friendly communications. The demi-fleur-de-lis, lightning flash, wings, and checky area also refer to the unit's origin as the 137th Signal Radio Intelligence Company, Aviation. The demi-fleur-de-lis denotes participation in European campaigns during World War II, while the color scarlet alludes to the Meritorious Unit Commendation (Army) Streamer awarded the unit.

Lineage and Honors

RA

Lineage (active)

Constituted 7 February 1942 in the Army of the United States as the 137th Signal Radio Intelligence Company, Aviation. Activated 20 February 1942 at Mitchel Field, New York. Reorganized and redesignated 25 February 1944 as the 137th Signal Radio Intelligence Company. Inactivated 12 December 1945 at Fort Jackson, South Carolina. Converted and redesignated 15 November 1948 as the 406th Mobile Radio Broadcasting Company and allotted to the Organized Reserve Corps. Activated 23 November 1948 at New York, New York. Inactivated 24 October 1950 at New York, New York.

Redesignated 17 July 1951 as the 504th Communication Reconnaissance Group. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Redesignated 21 April 1955 as Headquarters and Headquarters Company, 504th Communication Reconnaissance Group; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Activated 16 May 1955 at Fort Devens, Massachusetts. Redesignated 1 July 1956 as Headquarters and Headquarters Company, 504th Army Security Agency Group. Inactivated 18 December 1957 at Camp Wolters, Texas. Activated 1 July 1974 at Hunter Army Airfield, Georgia.

Reorganized and redesignated 21 April 1978 as Headquarters and Operations Company, 504th Military Intelligence Group. Reorganized and redesignated 16 April 1982 as Headquarters and Headquarters Detachment, 504th Military Intelligence Group. Reorganized and redesignated 16 September 1985 as Headquarters and Headquarters Detachment, 504th Military Intelligence Brigade.

Campaign Participation Credit

World War II

Northern France
Rhineland
Central Europe

Decorations

Meritorious Unit Commendation (Army), Streamer embroidered EUROPEAN THEATER (137th Signal Radio Intelligence Company cited; GO 34, Communications Zone, European Theater of Operations, 17 March 1945)

HEADQUARTERS AND HEADQUARTERS COMPANY 513th MILITARY INTELLIGENCE BRIGADE (Vigilant Knights)

HERALDIC ITEMS

SHOULDER SLEEVE INSIGNIA

Description: On a vertical rectangle arched at the top and bottom, a field divided quarterly silver gray and oriental blue and thereon a yellow lightning bolt issuing from upper left and a white sword point up in saltire surmounted by a white front-facing helmet detailed silver gray; all within a yellow border.

Symbolism: Oriental blue and silver gray are the military intelligence branch colors. The quartered field symbolizes the four primary intelligence functions: collection, analysis, production, and dissemination of intelligence information. The lightning bolt refers to the worldwide capabilities and the electronic warfare functions of the unit. The sword symbolizes the aggressiveness, protection, and physical danger inherent in military intelligence operations. The helmet alludes to the origins of the unit at Camp King in Oberursel, Germany. The helmet's front-facing position suggests alertness and vigilance and the closed faceplate the anonymity and aggressiveness of covert collection.

DISTINCTIVE UNIT INSIGNIA

Description: A gold color metal and enamel device consisting of a gold semicircular scroll bearing the words PER VIGILANTIAM SCIENTIA (KNOWLEDGE THROUGH VIGILANCE) in teal blue letters and containing upright between two green laurel branches a gold helmet facing front with teal blue rivet holes around the neck and a teal blue grill opening, the throat encircled by a collar of checkered white and black edged gold and atop the helmet a gold three-pointed coronet, the center point in teal blue.

Symbolism: The Teutonic helmet with crown is an allusion to Camp King in Oberursel, Germany, and its front-facing position suggests alertness and vigilance. The laurel branches on either side are

symbolic of honor and achievement. In the collar the colors black and white denote the two types of intelligence collection provided by the unit and the repetition of the pattern indicates the dissemination of intelligence information.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 22 October 1952 in the Regular Army as the 513th Military Intelligence Service Group. Activated 15 January 1953 in Germany. Reorganized and redesignated 20 October 1953 as the 513th Military Intelligence Group. Redesignated 25 July 1961 as the 513th Intelligence Corps Group. Redesignated 15 October 1966 as the 513th Military Intelligence Group. Inactivated 25 June 1969 in Germany. Redesignated 2 October 1982 as Headquarters and Headquarters Company, 513th Military Intelligence Group, and activated at Fort Monmouth, New Jersey.

Reorganized and redesignated 16 October 1986 as Headquarters and Headquarters Company, 513th Military Intelligence Brigade. Reorganized and redesignated 16 October 1991 as Headquarters and Headquarters Detachment, 513th Military Intelligence Brigade. Reorganized and redesignated 16 November 1995 as Headquarters and Headquarters Company, 513th Military Intelligence Brigade.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia

Defense of Saudi Arabia
Liberation and Defense of Kuwait
Cease-Fire

DECORATIONS

None.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 525th MILITARY INTELLIGENCE BRIGADE

HERALDIC ITEMS

SHOULDER SLEEVE INSIGNIA

Description: On a rectangle arched at the bottom with a yellow border, below a yellow and black checkered chief consisting of two rows of five squares each, a field divided from upper left to lower right with silver gray above oriental blue separated by a yellow lightning flash with point at lower right.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence. The lightning flash refers to the communication and electronic warfare functions of the unit. The checkered area alludes to the overt and covert aspects of the military intelligence mission, with the black and yellow colors referring to constant vigilance day and night.

TAB

Description: Immediately above and touching the shoulder sleeve insignia, a black arc tab containing the inscription AIRBORNE in yellow letters.

DISTINCTIVE UNIT INSIGNIA.

Description: A gold color metal and enamel device consisting of a black equilateral triangle charged with a gold lion rampant, in base two rows of alternating squares gold and oriental blue all above a voluted gold scroll inscribed FAST FACTUAL FAITHFUL in black letters.

Symbolism: The gold lion rampant on a black background was taken from the coat of arms of Heidelberg in Germany, where the 525th Interrogation Team was activated in 1946. The triangular shape alludes to the deltas in Vietnam and symbolizes the unit's service in that country. The triangle and lion with the checkered rows allude to tenacity, flexibility, and secrecy and represent the combined intelligence programs of the organization.

Lineage and Honors

RA

Lineage (active)

Constituted 21 June 1944 in the Army of the United States as the 218th Counter Intelligence Corps Detachment. Activated 1 July 1944 at Fort DuPont, Delaware. Inactivated 15 October 1945 at Camp Campbell, Kentucky.

Redesignated 17 September 1947 as the 249th Counter Intelligence Corps Detachment and allotted to the Organized Reserves. Activated 6 October 1947 at New York, New York. (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps.) Inactivated 31 December 1950 at New York, New York.

Redesignated 18 April 1952 as the 218th Counter Intelligence Corps Detachment; concurrently withdrawn from the Organized Reserve Corps and allotted to the Regular Army. Activated 30 April 1952 at Fort Holabird, Maryland. Reorganized and redesignated 25 January 1958 as the 218th Military Intelligence Detachment. Inactivated 15 September 1978 at Fort Bragg, North Carolina.

Consolidated 16 June 1979 with the 525th Military Intelligence Group (see ANNEX) and consolidated unit redesignated as Headquarters and Operations Company, 525th Military Intelligence Group; concurrently activated at Fort Bragg, North Carolina. Reorganized and redesignated 16 April 1982 as Headquarters and Headquarters Detachment, 525th Military Intelligence Group. Reorganized and redesignated 16 August 1985 as Headquarters and Headquarters Detachment, 525th Military Intelligence Brigade.

ANNEX

Constituted 18 April 1946 in the Army of the United States as the 525th Interrogation Team. Activated 1 May 1946 in Germany. Inactivated 6 November 1946 in Germany. Redesignated 6 February 1948 as the 525th Headquarters Intelligence Detachment. Activated 21 February 1948 at Fort Bragg, North Carolina. Allotted 5 May 1949 to the Regular Army. Reorganized and redesignated 23 May 1949 as Headquarters, 525th Military Intelligence Platoon. Reorganized and redesignated 4 August 1949 as the 525th Military Intelligence Service Company.

Reorganized and redesignated 1 December 1950 as the 525th Military Intelligence Service Group. Reorganized and redesignated 31 December 1953 as the 525th Military Intelligence Group. Reorganized and redesignated 25 September 1969 as Headquarters and Headquarters Company, 525th Military Intelligence Group. Inactivated 6 March 1973 at Oakland, California. Redesignated 1 July 1974 as the 525th Military Intelligence Group and activated at the Presidio of San Francisco, California. Inactivated 1 January 1978 at the Presidio of San Francisco, California.

CAMPAIGN PARTICIPATION CREDIT

World War II
- Rhineland
- Ardennes-Alsace
- Central Europe

Vietnam
- Defense
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII
- Consolidation I
- Consolidation II
- Cease-Fire

Armed Forces Expeditions
- Dominican Republic
- Panama

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (525th Military Intelligence Group cited; DA GO 39, 1970)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (525th Military Intelligence Group cited; DA GO 52, 1974)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1970 (525th Military Intelligence Group cited; DA GO 52, 1974)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971–1973 (525th Military Intelligence Group cited; DA GO 6, 1976)

108th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A gold color metal and enamel device consisting of a white expanded horizontal scroll surmounted vertically by a gold quill in front of a gold demi-sun emitting eight rays; all encircled by an oriental blue scroll with the upper area surmounted by the points of the rays and in base the inscription TRUTH CONQUERS in gold letters.

Symbolism: Oriental blue is one of the colors associated with military intelligence. The quill and scroll allude to the reporting mission of intelligence. The sun, a symbol of enlightenment, with the radiating rays, symbolizes the illumination of dark areas and defense against subversion and espionage. The eight rays further refer to the eight states in the jurisdictional area of the group.

FLAG DEVICE

None approved.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 10 May 1946 in the Army of the United States as the 108th Counter Intelligence Corps Detachment. Activated 10 June 1946 at New York, New York. Allotted 26 February 1951 to the Regular Army. Redesignated 1 March 1957 as the 108th Counter Intelligence Corps Group. Redesignated 25 July 1961 as the 108th Intelligence Corps Group. Redesignated 15 October 1966 as the 108th Military Intelligence Group. Inactivated 31 January 1972 at Fort Devens, Massachusetts.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

109th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A gold color metal and enamel device consisting of an ellipse divided quarterly oriental blue and black, overall a vertical gold quillon dagger point up with white blade and six-sectioned red grip extending over the ellipse at the top and base.

Symbolism: Oriental blue is one of the colors associated with military intelligence. Black connotes secrecy and the covert methods sometimes used in accomplishing the unit's mission. The four segments comprising the ellipse refer to the four phases of the intelligence cycle. The dagger signifies the aggressiveness and determination required for successful achievement in performance of intelligence operations. Red denotes martial fortitude and the six sections of the dagger's grip refer to the initials LIDMAC (Loyalty, Integrity, Discretion, Morals, and Character). In addition, the vertical thrust of the dagger, the ellipse, and the nine areas of the weapon (blade, guard, six-sectioned grip, and pommel) allude to the numerical designation of the group.

FLAG DEVICE

None approved.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 10 May 1946 in the Army of the United States as the 109th Counter Intelligence Corps Detachment. Activated 24 May 1946 at Baltimore, Maryland. Allotted 26 February 1951 to the Regular Army. Redesignated 12 September 1956 as the 109th Counter Intelligence Corps Group. Redesignated 25 July 1961 as the 109th Intelligence Corps Group. Redesignated 15 October 1966 as the 109th Military Intelligence Group. Inactivated 30 June 1974 at Fort George G. Meade, Maryland.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

115th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A gold color metal and enamel device consisting of three black enamel mountain peaks charged in base with an eight-pointed white enamel star, at top a gold sunburst on an oriental blue enamel background, all enclosed within a convoluted gold scroll in red letters CUSTOS SECRETORUM (CUSTODIAN OF SECRETS).

Symbolism: The sunburst just above the mountain peaks alludes to the sun setting in the west. With the eight-pointed rising star, it signifies the day and night protection given by the group in its eight western state jurisdiction. Oriental blue is one of the colors used by military intelligence.

FLAG DEVICE

None approved.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 10 May 1946 in the Army of the United States as the 115th Counter Intelligence Corps Detachment. Activated 21 May 1946 at Fort Douglas, Utah. Allotted 23 May 1951 to the Regular Army. Redesignated 25 July 1957 as the 115th Counter Intelligence Corps Group. Redesignated 25 July 1961 as the 115th Intelligence Corps Group. Redesignated 15 October 1966 as the 115th Military Intelligence Group. Inactivated 30 June 1974 at the Presidio of San Francisco, California.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

116th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A gold color metal and enamel device consisting of an oriental blue disc within a scarlet military belt buckled and edged with gold and inscribed in gold letters VIGIL PROMPTUSQUE (WATCHFUL AND READY); issuing from the inner edge of the belt downward over the oriental blue disc a gold demi-sun emitting rays; surmounted by a representation of the Washington Monument in the District of Columbia, white shaded silver gray, the monument issuing from the lower inner edge of the belt and extending between the two words of the motto beyond the top outer edge.

Symbolism: Oriental blue and silver gray are military intelligence branch colors. The sun and rays are taken from the shoulder sleeve insignia of the former United States Army Intelligence Command. They stand for light and knowledge and indicate that the group served under that organization. The belt refers to the encircling band of security provided by military intelligence and denotes the military nature of the group. The Washington Monument alludes to the District of Columbia, the place where the unit was activated in 1946.

FLAG DEVICE

None approved.

LINEAGE AND HONORS

LINEAGE

RA
(inactive)

Constituted 10 May 1946 in the Army of the United States as the 116th Counter Intelligence Corps Detachment. Activated 31 May 1946 at Washington, D.C. Allotted 5 March 1951 to the Regular Army. Redesignated 26 June 1959 as the 116th Counter Intelligence Corps Group. Redesignated 25 July 1961 as the 116th Intelligence Corps Group. Redesignated 15 October 1966 as the 116th Military Intelligence Group. Inactivated 9 January 1973 at Washington, D.C.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 259th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A silver color metal and enamel device consisting of a silver ring containing a disc divided into quarters alternately from upper left of silver gray and black enamel centered in front of two oriental blue griffins seated back to back all upon a horizontal silver platform, the griffins each holding in a claw at chest level the upper fold of a silver scroll curving downward in three folds, the small fold centered below the platform and the scroll inscribed in black letters with the motto WATCHFUL AND VIGILANT, one word on each fold; the free ends draped below each end of the platform.

Symbolism: Oriental blue and silver gray are the colors used for military intelligence. The griffin, a mythological creature of exceeding alertness and acute hearing, represents qualities necessary to the military intelligence mission. The scroll held up in his claws alludes to the assimilation of military intelligence data and the disc at center, quartered in light and dark colors representing night and day, suggests the importance of constant vigilance. The silver circle refers to the state of Ohio, the unit's original home area.

FLAG DEVICE

None approved.

LINEAGE AND HONORS

AR
(inactive)

LINEAGE

Constituted 24 November 1967 in the Army Reserve as Headquarters, 259th Military Intelligence Group. Activated 22 January 1968 at Sharonville, Ohio. Inactivated 1 March 1972 at Sharonville, Ohio. Redesignated 8 August 1995 as Headquarters and Headquarters Detachment, 259th Military Intelligence Group.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 336th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 14 May 1948 in the Organized Reserve Corps as the 336th Headquarters Intelligence Detachment. Activated 2 June 1948 at New York, New York. Reorganized and redesignated 6 July 1950 as Headquarters, 336th Military Intelligence Group. Ordered into active military service 3 September 1950 at New York, New York. Inactivated 1 December 1950 at Fort Bragg, North Carolina. Redesignated 28 March 1996 as Headquarters and Headquarters Detachment, 336th Military Intelligence Group.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 348th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 18 April 1967 in the Regular Army as Headquarters and Headquarters Company, 48th Military Intelligence Group. Activated 1 August 1967 at Fort Bragg, North Carolina. Inactivated 26 August 1968 at Fort Bragg, North Carolina.

Redesignated 28 March 1996 as Headquarters and Headquarters Detachment, 348th Military Intelligence Group; concurrently withdrawn from the Regular Army and allotted to the Army Reserve.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

650th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A gold color metal and enamel device consisting of an octagon, issuing from the top a white enamel wedge shape between two black enamel areas each surmounted with a gold sea lion facing outward, and extending in base over an oriental blue enamel area charged in the center with a gold Philippine sunburst, all above a gold scroll of three sections inscribed in sequence SECURITY TRUTH ALLIANCE in scarlet letters.

Symbolism: The sea lions allude to the unit's New Guinea and Luzon campaigns in the Pacific theater during World War II. The Philippine sunburst symbolizes the organization's Philippine Presidential Unit Citation. The octagon refers to the number eight, which in numerology stands for perfect intelligence. The colors black and white symbolize day and night vigilance, while gold, the color of the farseeing sun, which appears bringing light out of an inscrutable darkness only to disappear again into darkness, stands for intuition. Oriental blue is one of the colors used for intelligence and security.

FLAG DEVICE

None approved.

HEADQUARTERS AND HEADQUARTERS DETACHMENT 505th MILITARY INTELLIGENCE GROUP

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 30 January 1951 in the Organized Reserve Corps as Headquarters and Headquarters Company, 505th Communication Reconnaissance Group. Activated 19 February 1951 at Boston, Massachusetts. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Redesignated 10 September 1956 as Headquarters and Headquarters Company, 505th Army Security Agency Group. Inactivated 1 July 1959 at Boston, Massachusetts. Activated 15 February 1963 at Boston, Massachusetts. Inactivated 31 January 1968 at Boston, Massachusetts.

Redesignated 1 February 1990 as Headquarters and Headquarters Company, 505th Military Intelligence Group. Redesignated 8 August 1995 as Headquarters and Headquarters Detachment, 505th Military Intelligence Group.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

Lineage and Honors

RA

Lineage (active)

Constituted 12 July 1944 in the Army of the United States as the 450th Counter Intelligence Corps Detachment. Activated 20 August 1944 in New Guinea. Disbanded 22 July 1945 in the Philippine Islands. Reconstituted 25 March 1948 in the Organized Reserve Corps as the 450th Counter Intelligence Corps Detachment. Activated 1 May 1948 in Puerto Rico. Inactivated 4 August 1949 in Puerto Rico. Withdrawn 18 January 1951 from the Organized Reserve Corps and allotted to the Regular Army; concurrently activated at Fort Holabird, Maryland. Redesignated 25 July 1961 as the 450th Intelligence Corps Detachment.

Redesignated 15 October 1966 as the 650th Military Intelligence Detachment. Reorganized and redesignated 20 July 1970 as the 650th Military Intelligence Group.

Campaign Participation Credit

World War II

New Guinea

Luzon

Decorations

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (450th Counter Intelligence Corps Detachment cited; DA GO 47, 1950)

HEADQUARTERS AND HEADQUARTERS DETACHMENT 902d MILITARY INTELLIGENCE GROUP (The Deuce)

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A gold color metal and enamel device consisting of three gold sun rays behind an oriental blue enamel disc surmounted at top by a gold chess piece (horse's head) and in base a red enamel and gold chessboard, all above a three-folded gold scroll inscribed in black enamel letters STRENGTH THROUGH VIGILANCE.

Symbolism: The sun rays allude to the Philippine Presidential Unit Citation and to the unit's World War II service in New Guinea and Luzon. The knight, a chess piece shaped like a horse's head, symbolizes the group's ability to make strategic moves while checking any hostile infiltration and advancement. The color red is used to symbolize courage, zeal, and awareness and with the alternating gold squares refers to the unit's counterintelligence mission. Oriental blue is one of the colors used by military intelligence.

FLAG DEVICE

None approved.

Lineage and Honors

RA
(active)

Lineage

Constituted 14 October 1944 in the Army of the United States as the 902d Counter Intelligence Corps Detachment. Activated 23 November 1944 in New Guinea. Disbanded 22 July 1945 in the Philippine Islands. Reconstituted 13 November 1947 in the Organized Reserves as the 902d Counter Intelligence Corps Detachment. Activated 28 November 1947 at Fort Smith, Arkansas. (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps.) Inactivated 2 November 1949 at Fort Smith, Arkansas. Withdrawn 3 January 1952 from the Organized Reserve Corps and allotted to the Regular Army. Activated 8 January 1952 at Fort Holabird, Maryland.

Redesignated 15 December 1957 as the 902d Counter Intelligence Corps Group. Redesignated 25 July 1961 as the 902d Intelligence Corps Group. Redesignated 15 October 1966 as the 902d Military Intelligence Group. Reorganized and redesignated 1 January 1978 as Headquarters and Headquarters Company, 902d Military Intelligence Group. Reorganized and redesignated 16 November 1995 as Headquarters and Headquarters Detachment, 902d Military Intelligence Group.

Campaign Participation Credit

World War II
New Guinea
Luzon

Decorations

Army Superior Unit Award, Streamer embroidered 1988–1989 (902d Military Intelligence Group cited; DA GO 15, 1990)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (902d Counter Intelligence Corps Detachment cited; DA GO 47, 1950)

1st MILITARY INTELLIGENCE BATTALION (The Flying Eye Battalion)

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, issuant from base a lightning flash bendwise terminating in a dexter hand fesswise supporting an annulet winged to chief all or, within the annulet a human eye proper.

Crest: On a wreath of the colors, or and azure, a bundle of five arrows crossed with a hook-bladed machete in bend sinister, the arrows point down with shafts of the first barbed and flighted gules, the machete with handle to base azure all banded in center with a ribbon gold bearing three narrow stripes fesswise scarlet, all in front of a bank of clouds proper.

Motto: INFORMARE LABORAMUS (WE LABOR TO INFORM).

Symbolism: Teal blue and yellow are the colors formerly used for air reconnaissance support battalions. The annulet, symbolic of a camera lens, refers to the aerial photo interpretation mission in the unit's history. The wings allude to flight; the eye represents observation. The lightning flash alludes to the former signal element in the unit's composition and the hand commemorates the unit's mission of support.

The battalion's awards for Vietnam service, for which it received the Presidential Unit Citation (Air Force) and five Meritorious Unit Commendations (Army), are represented in the crest. The mak, or hook-bladed machete used to clear fields in Vietnam, signifies the battalion's keen reconnaissance performance, and, together with the clouds alluding to the Air Force, refers to the Presidential Unit Citation (Air Force); blue is the color of the award streamer. The five arrows, with points down signifying penetration from the air, represent five Meritorious Unit Commendations (Army), with arrowheads and feathers in scarlet, the color of the award streamers. The yellow band with scarlet stripes, suggested by the national flag of the Republic of Vietnam, also alludes to the unit's achievements in collecting aerial reconnaissance information.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

RA

Lineage (active)

Constituted 14 December 1956 in the Regular Army as Headquarters and Headquarters Detachment, 1st Air Reconnaissance Support Battalion. Activated 1 February 1957 at Fort Polk, Louisiana. (205th Signal Company [see ANNEX 1] reorganized and redesignated 1 May 1959 as Company A; 196th Aerial Photo Interpretation Detachment [see ANNEX 2] redesignated 15 April 1959 as Company B and allotted to the Regular Army; activated 1 May 1959 at Fort Bragg, North Carolina.)

Converted and redesignated 20 March 1962 as the 1st Military Intelligence Battalion. Inactivated 15 July 1982 at Fort Bragg, North Carolina. Activated 16 January 1984 in Germany.

ANNEX 1

Constituted 24 January 1945 in the Army of the United States as the 205th Signal Repair Company. Activated 1 February 1945 at Fort Jackson, South Carolina. Allotted 16 May 1949 to the Regular Army. Reorganized and redesignated 15 April 1954 as the 205th Signal Company. Inactivated 28 May 1955 in Korea. Activated 1 February 1956 at Fort Bragg, North Carolina.

ANNEX 2

Constituted 16 June 1945 in the Army of the United States as the 196th Photo Interpreter Team. Activated 10 July 1945 at Fort Jackson, South Carolina. Reorganized and redesignated 18 May 1950 as the 196th Aerial Photo Interpretation Detachment. Inactivated 15 November 1953 at Governors Island, New York.

Campaign Participation Credit

Vietnam

Defense
Counteroffensive
Counteroffensive, Phase II
Counteroffensive, Phase III
Tet Counteroffensive
Counteroffensive, Phase IV
Counteroffensive, Phase V
Counteroffensive, Phase VI
Tet 69/Counteroffensive
Summer-Fall 1969
Winter-Spring 1970
Sanctuary Counteroffensive
Counteroffensive, Phase VII
Consolidation I
Consolidation II
Cease-Fire

Company A additionally entitled to:

Korean War

UN Defensive
UN Offensive
CCF Intervention
First UN Counteroffensive
CCF Spring Offensive
UN Summer-Fall Offensive
Second Korean Winter
Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953

Company B additionally entitled to:

Southwest Asia

Liberation and Defense of Kuwait

DECORATIONS

Presidential Unit Citation (Air Force), Streamer embroidered SOUTHEAST ASIA 1966–1967 (1st Military Intelligence Battalion cited; DA GO 42, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1965–1966 (1st Military Intelligence Battalion cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (1st Military Intelligence Battalion cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (1st Military Intelligence Battalion cited; DA GO 42, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (1st Military Intelligence Battalion cited; DA GO 43, 1988)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1970–1972 (1st Military Intelligence Battalion cited; DA GO 5, 1973)

Republic of Vietnam Cross of Gallantry with Gold Star, Streamer embroidered VIETNAM 1965–1971 (1st Military Intelligence Battalion cited; DA GO 32, 1973)

Company A additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1950–1952 (205th Signal Repair Company cited; DA GO 94, 1952)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1953 (205th Signal Repair Company cited; DA GO 1, 1954)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA (205th Signal Repair Company cited; DA GO 33, 1953, as amended by DA GO 41, 1955)

2d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per chevron abased azure and argent, a chief dancetty of two enhanced of the last the apexes surmounted by two roundels of the first counterchanged and in base a sphinx rampant sable armed gules.

Crest: None approved.

Motto: OCULI CULTUS SECRETI (THE EYES OF INTELLIGENCE).

Symbolism: The colors, white and teal blue, symbolize the battalion's former status as an unassigned-to-branch unit. The battalion's numerical designation and mission are suggested by the two roundels or lenses directing their gaze downward. The sphinx is representative of the intelligence mission. Black alludes to the coat of arms of the old Rhineland district of Pfalz in Germany, where the unit was activated.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 18 October 1961 in the Regular Army as the 2d Air Reconnaissance Support Battalion. Activated 15 November 1961 in Germany. Converted and redesignated 16 September 1962 as the 2d Military Intelligence Battalion. Inactivated 15 November 1991 in Germany.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia

Defense of Saudi Arabia
Liberation and Defense of Kuwait
Cease-Fire

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (2d Military Intelligence Battalion cited; DA GO 34, 1992)

3d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per bend azure and checky or and gules in chief a chess piece with a griffin's head argent.

Crest: On a wreath of the colors, or and azure, a Vietnamese sunburst of the first surmounted by a bamboo cross pierced at center proper.

Motto: WINGED VIGILANCE.

Symbolism: The colors oriental blue and silver gray are used to represent military intelligence and scarlet and gold to symbolize military strength and operational excellence. The griffin, traditionally a creature of vision, alertness, and intelligence, is shown as a chess piece adjacent to a chessboard, suggesting the type of operation, requiring ingenuity and intellect, which the battalion is called upon to carry out. The squares on the chessboard represent the many engagements in which the unit participated in Vietnam.

The sunburst, taken from the Hien Nhan gate to the Imperial City in Hue, represents Vietnam and has three principal flames, suggesting the Meritorious Unit Commendations (Army) awarded to the organization. The bamboo cross stands for the Republic of Vietnam Cross of Gallantry with Palm awarded to the unit.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 1 June 1966 in the Regular Army as the 146th Aviation Company and activated in Vietnam. Inactivated 17 February 1973 in Vietnam. Converted and redesignated 1 July 1974 as the 146th Army Security Agency Company and activated in Korea.

Reorganized and redesignated 16 June 1982 as Headquarters, Headquarters and Service Company, 3d Military Intelligence Battalion (704th Military Intelligence Detachment [see ANNEX 1] and 542d Military Intelligence

Detachment [see ANNEX 2] concurrently redesignated as Companies A and B and activated in Korea).

ANNEX 1

Constituted 25 September 1950 in the Regular Army as the 704th Counter Intelligence Corps Detachment. Activated 6 October 1950 in Korea. Inactivated 28 March 1955 in Korea. Redesignated 28 December 1961 as the 704th Intelligence Corps Detachment. Activated 25 January 1962 in Vietnam. Inactivated 7 March 1966 in Vietnam. Redesignated 1 November 1966 as the 704th Military Intelligence Detachment. Activated 15 March 1967 in Japan. Inactivated 15 June 1972 in Japan. Activated 25 September 1976 in Korea. Inactivated 16 May 1979 in Korea.

ANNEX 2

Constituted 7 July 1945 in the Army of the United States as the 1002d Counter Intelligence Corps Detachment. Activated 25 July 1945 in France. Disbanded 24 January 1946 at Holabird Signal Depot, Maryland. Reconstituted 7 December 1950 in the Regular Army as the 442d Counter Intelligence Corps Detachment. Activated 20 December 1950 in Korea. Inactivated 25 December 1951 in Korea.

Redesignated 26 March 1965 as the 542d Intelligence Corps Detachment. Activated 7 April 1965 at Fort George G. Meade, Maryland. Inactivated 1 December 1965 at Fort George G. Meade, Maryland. Activated 19 December 1969 at Fort Bragg, North Carolina. Redesignated 29 December 1969 as the 542d Military Intelligence Detachment. Inactivated 19 November 1973 at Aberdeen Proving Ground, Maryland.

CAMPAIGN PARTICIPATION CREDIT

Vietnam

- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII
- Consolidation I
- Consolidation II
- Cease-Fire

Company A additionally entitled to:

Korean War

UN Offensive
CCF Intervention
First UN Counteroffensive
CCF Spring Offensive
UN Summer-Fall Offensive
Second Korean Winter
Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953

Vietnam

Advisory
Defense

Company B additionally entitled to:

Korean War

CCF Intervention
First UN Counteroffensive
CCF Spring Offensive
UN Summer-Fall Offensive
Second Korean Winter

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (146th Aviation Company cited; DA GO 17, 1968, as amended by DA GO 1, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1969 (146th Aviation Company cited; DA GO 2, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971–1972 (146th Aviation Company cited; DA GO 32, 1973)

Army Superior Unit Award, Streamer embroidered 1985–1986 (3d Military Intelligence Battalion cited; DA GO 30, 1987)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (146th Aviation Company cited; DA GO 6, 1974)

Company A additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (704th Counter Intelligence Corps Detachment cited; DA GO 46, 1954)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA 1950–1952 (704th Counter Intelligence Corps Detachment cited; DA GO 33, 1953, as amended by DA GO 41, 1955)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA 1952–1953 (704th Counter Intelligence Corps Detachment cited; DA GO 24, 1954)

14th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per bend dove-tailed argent and azure, two whelk shells counterchanged.

Crest: None approved.

Motto: SUPPORT BY INTELLIGENCE.

Symbolism: The two shells and the dove-tailed partition line stand for the three general functions of a military intelligence unit: collecting, processing, and disseminating information. The whelk shells, which receive and transmit sound waves and vibrations, refer to the collection and dissemination of information; the fitting together of the two parts of the shield, by means of the dove-tailed line, refers to the process of interpreting and collating separate pieces of information to form an integrated whole. Oriental blue and silver gray are the colors used for military intelligence. Counterchanging the colors of the shells alludes to the counterintelligence function of the unit.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 4 November 1965 in the Regular Army as the 14th Military Intelligence Battalion. Activated 24 November 1965 at Fort Bragg, North Carolina. Inactivated 31 December 1972 at Fort Bragg, North Carolina. Activated 16 December 1988 at Fort Lewis, Washington.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

15th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, above a base rayonné argent, a winged sphinx couchant of the last and in chief two plates partially superimposed fesswise the conjoined area sable.

Crest: None approved.

Motto: VIGILANTIA AD FINEM (VIGILANCE TO THE END).

Symbolism: Oriental blue and silver gray are the colors used for military intelligence. The winged sphinx, all-seeing and continually watchful, refers to the battalion's air reconnaissance support mission and also connotes the unit's motto. The overlapping discs simulate camera lenses and allude to the stereoscopic capabilities provided by the organization in its performance of reproduction, identification, and packaging of aerial imagery. The flames are indicative of heat sensory devices, wisdom, and zeal.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 6 January 1966 in the Regular Army as the 15th Military Intelligence Battalion. Activated 25 February 1966 at Fort Bragg, North Carolina. Inactivated 30 April 1972 at Fort Bragg, North Carolina. Activated 21 April 1978 at Fort Hood, Texas (Detachments A, B, C, and D concurrently consolidated to form Company A; 131st Military Intelligence Company [see ANNEX 1] and 156th Army Security Agency Company [see ANNEX 2] reorganized and redesignated as Companies B and C). Headquarters and Headquarters Company inactivated 31 May 1981 at Hunter Army Airfield, Georgia (Company C concurrently inactivated at Fort Bliss, Texas). (Company A inactivated 15 April 1982 at Fort Hood, Texas; disbanded 15 September 1983. Company B reorganized and redesignated 16 September 1983 as Company A; Company C concurrently redesignated as Company B.) Headquarters and Headquarters Company redesignated 16 October 1985 as Headquarters, Headquarters and Service Company and activated at Fort Hood, Texas (Company B concurrently activated).

ANNEX 1

Constituted 1 July 1971 in the Regular Army as the 131st Military Intelligence Company and activated in Vietnam.

ANNEX 2

Constituted 1 June 1966 in the Regular Army as the 156th Aviation Company and activated in Vietnam. Converted and redesignated 5 November 1973 as the 156th Army Security Agency Company.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia

Defense of Saudi Arabia
Liberation and Defense of Kuwait

Company A additionally entitled to:

Vietnam

Consolidation I
Consolidation II
Cease-Fire

Company B additionally entitled to:

Vietnam

Counteroffensive
Counteroffensive, Phase II
Counteroffensive, Phase III
Tet Counteroffensive
Counteroffensive, Phase IV
Counteroffensive, Phase V
Counteroffensive, Phase VI
Tet 69/Counteroffensive
Summer-Fall 1969
Winter-Spring 1970
Sanctuary Counteroffensive
Counteroffensive, Phase VII
Consolidation I
Consolidation II
Cease-Fire

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (15th Military Intelligence Battalion cited; DA GO 12, 1994)

Company B additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (156th Aviation Company cited; DA GO 17, 1968, as amended by DA GO 1, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1969 (156th Aviation Company cited; DA GO 2, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971–1972 (156th Aviation Company cited; DA GO 32, 1973)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (156th Aviation Company cited; DA GO 6, 1974)

24th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, above a base indented or a winged eye, the wings displayed inverted of the second, emitting to base three rays throughout of the like counterchanged.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, or and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: OUR EYES SUPPORT.

Symbolism: Oriental blue is one of the colors used for military intelligence units. The winged eye searching the land with rays of light is symbolic of the air reconnaissance mission of the battalion.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

AR

LINEAGE (active)

Constituted 22 April 1959 in the Army Reserve as the 24th Air Reconnaissance Support Battalion. Activated 1 May 1959 with Headquarters at New York, New York. Ordered into active military service 15 October 1961 at New York, New York.

Converted and redesignated 13 April 1962 as the 24th Military Intelligence Battalion. Released from active military service 4 August 1962 and reverted to reserve status. Location of Headquarters changed 1 September 1962 to Staten Island, New York; changed 31 December 1968 to Fort Hamilton, New York. Battalion ordered into active military service 24 March 1970 at Fort Hamilton, New York; released from active military service 26 March 1970 and reverted to reserve status. Location of Headquarters changed 1 May 1974 to Staten Island, New York. (Detachment C ordered into active military service 17 January 1991 at Staten Island, New York; released from active military service 1 April 1991 and reverted to reserve status.)

CAMPAIGN PARTICIPATION CREDIT

Detachment C entitled to:

Southwest Asia

Liberation and Defense of Kuwait

DECORATIONS

None.

101st MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Checky azure and argent in front of a sword and lightning flash in saltire a double-warded key palewise argent, on a chief invected of the like a sunburst throughout tenné.

Crest: None approved.

Motto: TRUST VIGILANCE LOYALTY.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence. The invected chief is an allusion to clouds and the atmosphere, the main field of operations for a combat electronic warfare intelligence unit. The sunburst, a symbol of Helios, the Greek sun god, is a further reference to the atmosphere. The sunburst may also denote a compass rose and the multi-directional facets of the unit's radio functions. The checky background alludes to a chessboard and symbolizes strategy and intelligence. The sword refers to the unit's military ability, the lightning flash to speed and communications, and the key to intelligence and security.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

LINEAGE

RA
(active)

Constituted 16 September 1980 in the Regular Army as the 101st Military Intelligence Battalion, assigned to the 1st Infantry Division, and activated at Fort Riley, Kansas (337th Army Security Agency Company [see ANNEX 1] and 1st Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B). Inactivated 15 November 1995 at Fort Riley, Kansas. Activated 16 February 1996 in Germany.

ANNEX 1

Constituted 1 July 1952 in the Regular Army as the 337th Communication Reconnaissance Company. Activated 6 August 1952 at Fort Devens, Massachusetts. Reorganized and redesignated 16 May 1955 as Company B, 313th Communication Reconnaissance Battalion. Redesignated 1 July 1956 as Company B, 313th Army Security Agency Battalion. Inactivated 18 December

1957 at Fort Bragg, North Carolina. Activated 25 May 1962 at Fort Bragg, North Carolina. Reorganized and redesignated 15 October 1966 as the 337th Army Security Agency Company.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 1st Counter Intelligence Corps Detachment. Activated 16 August 1944 in France with personnel from provisional Counter Intelligence Corps detachment attached to the 1st Infantry Division. Allotted 16 February 1951 to the Regular Army. Reorganized and redesignated 25 January 1958 as the 1st Military Intelligence Detachment. Reorganized and redesignated 26 December 1969 as the 1st Military Intelligence Company. Reorganized and redesignated 15 April 1970 as the 1st Military Intelligence Detachment. Reorganized and redesignated 3 May 1971 as the 1st Military Intelligence Company. Assigned 21 July 1978 to the 1st Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait
- Cease-Fire

Company A additionally entitled to:

Vietnam
- Defense
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970

Company B additionally entitled to:

World War II–EAME
- Tunisia
- Sicily
- Normandy (with arrowhead)
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

Vietnam
- Defense
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1965–1966 (11th Radio Research Unit cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (337th Radio Research Company cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (337th Radio Research Company cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (337th Radio Research Company cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (337th Radio Research Company cited; DA GO 43, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1965–1968 (337th Radio Research Company cited; DA GO 21, 1969, as amended by DA GO 59, 1969)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1969–1970 (337th Radio Research Company cited; DA GO 6, 1974)

Company B entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966 (1st Military Intelligence Detachment cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968 (1st Military Intelligence Detachment cited; DA GO 7, 1970)

French Croix de Guerre with Palm, World War II, Streamer embroidered KASSERINE (1st Infantry Division cited; DA GO 43, 1950)

French Croix de Guerre with Palm, World War II, Streamer embroidered NORMANDY (1st Infantry Division cited; DA GO 43, 1950)

French Croix de Guerre, World War II, Fourragere (1st Infantry Division cited; DA GO 43, 1950)

Belgian Fourragere 1940 (1st Counter Intelligence Corps Detachment cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action at Mons (1st Counter Intelligence Corps Detachment cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action at Eupen-Malmedy (1st Counter Intelligence Corps Detachment cited; DA GO 43, 1950)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1965–1968 (1st Military Intelligence Detachment cited; DA GO 21, 1969)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1965–1970 (1st Military Intelligence Detachment cited; DA GO 53, 1970)

102d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per fess dancetty azure and sable, a chief invected argent, and overall a sword bend sinisterwise point to base gules surmounted by a lightning flash issuant from dexter chief bendwise overall or.

Crest: None approved.

Motto: KNOWLEDGE FOR BATTLE.

Symbolism: Silver gray and oriental blue are the colors used for military intelligence units. The divisions of the shield are symbolic of weather and terrain, with the scarlet sword representing the enemy. The unit's deployment overseas is symbolized by the wavy blue section and the black area in base refers to the steep, mountainous terrain of Korea, where elements of the battalion served during the Korean War. The lightning flash signifies the seeking, gathering, and dissemination of information relative to the areas of weather, terrain, and the enemy and further denotes the constant vigilance which is inherent in the mission of military intelligence.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 16 September 1981 in the Regular Army as the 102d Military Intelligence Battalion, assigned to the 2d Infantry Division, and activated in Korea (329th Army Security Agency Company [see ANNEX 1] and 2d Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B).

ANNEX 1

Constituted 23 October 1943 in the Army of the United States as the 3106th Signal Service Platoon. Activated 1 November 1943 at Fort Monmouth, New Jersey. Inactivated 10 February 1946 on Okinawa. Activated 19 November 1946 at Vint Hill Farms Station, Virginia. Redesignated 1 April 1947 as the 3d Signal Service Platoon. Reorganized and redesignated 25 March 1949 as the

53d Signal Service Company. Allotted 13 October 1950 to the Regular Army.

Converted and redesignated 1 December 1950 as the 329th Communication Reconnaissance Company. Reorganized and redesignated 25 June 1955 as Company B, 301st Communication Reconnaissance Battalion. Redesignated 1 July 1956 as Company B, 301st Army Security Agency Battalion. Inactivated 15 October 1957 in Korea. Redesignated 1 November 1975 as the 329th Army Security Agency Company and activated in Korea.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 2d Counter Intelligence Corps Detachment. Activated 6 August 1944 in France with personnel from provisional Counter Intelligence Corps detachment attached to the 2d Infantry Division. Allotted 3 February 1949 to the Regular Army. Inactivated 15 September 1956 at Fort Lewis, Washington. Redesignated 26 February 1958 as the 2d Military Intelligence Detachment. Activated 14 June 1958 at Fort Benning, Georgia. Assigned 30 June 1976 to the 2d Infantry Division. Reorganized and redesignated 20 February 1979 as the 2d Military Intelligence Company.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

World War II–AP
- Silver band without inscription

Korean War
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

Company B entitled to:

World War II–EAME
- Normandy
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

Korean War
- UN Defensive
- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1951–1952 (329th Communication Reconnaissance Company cited; DA GO 108, 1952)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1952–1953 (329th Communication Reconnaissance Company cited; DA GO 22, 1954)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA (329th Communication Reconnaissance Company cited; DA GO 33, 1953, as amended by DA GO 41, 1955)

Company B entitled to:

Presidential Unit Citation (Army), Streamer embroidered HONGCHON (2d Counter Intelligence Corps Detachment cited; DA GO 72, 1951)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (2d Counter Intelligence Corps Detachment cited; DA GO 32, 1954)

Belgian Fourragere 1940 (2d Infantry Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in the Ardennes (2d Infantry Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action at Elsenborn Crest (2d Infantry Division cited; DA GO 43, 1950)

103d MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Per bend azure and quarterly gules and or, on a bend engrailed argent a lightning bolt of the second and in sinister chief a wyvern's head of the fourth.

Crest: None approved.

Motto: TOP OF THE ROCK.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence units. The wyvern's head has been adapted from the device of the 3d Infantry Division, which this battalion supports. The wyvern is a heraldic creature known as a fearless guardian and thus symbolizes a major role of the intelligence mission. The lightning bolt on the engrailed bend alludes to the unit's special interest in communications of hostile and friendly forces as well as communications throughout the battalion. The scarlet and yellow quarters refer to the arms of Wurzburg in Germany, the battalion's place of activation.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA
LINEAGE (active)

Constituted 16 September 1981 in the Regular Army as the 103d Military Intelligence Battalion, assigned to the 3d Infantry Division, and activated in Germany (851st Army Security Agency Company [see ANNEX 1] and 3d Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B).

ANNEX 1

Constituted 29 December 1945 in the Army of the United States as the 3377th Signal Service Detachment. Activated 15 January 1946 in the Philippine Islands. Redesignated 9 June 1947 as the 50th Signal Service Detachment.

Converted and redesignated 25 October 1951 as the 851st Communication Reconnaissance Detachment and allotted to the Regular Army. Inactivated 15 August 1956 in Japan. Redesignated 3 December 1965 as the 851st Army Security Agency Detachment. Activated 15 December 1965 in the Dominican Republic. Inactivated 14 October 1966 at Fort Bragg, North Carolina. Redesignated 1 July 1974 as the 851st Army Security Agency Company and activated in Germany.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 3d Counter Intelligence Corps Detachment. Activated 3 September 1944 in France with personnel from provisional Counter Intelligence Corps detachment attached to the 3d Infantry Division. Inactivated 1 September 1946 in Germany. Allotted 3 February 1949 to the Regular Army. Activated 1 March 1949 at Fort Benning, Georgia. Reorganized and redesignated 25 January 1958 as the 3d Military Intelligence Detachment. Reorganized and redesignated 21 May 1972 as the 3d Military Intelligence Company. Assigned 21 April 1974 to the 3d Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

Korean War
- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive

Armed Forces Expeditions
- Dominican Republic

Company B entitled to:

World War II–EAME

Tunisia
Sicily
Naples-Foggia
Anzio (with arrowhead)
Rome-Arno
Southern France (with arrowhead)
Rhineland
Ardennes-Alsace
Central Europe

Korean War

CCF Intervention
First UN Counteroffensive
CCF Spring Offensive
UN Summer-Fall Offensive
Second Korean Winter
Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (50th Signal Service Detachment cited; DA GO 101, 1951)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA (50th Signal Service Detachment cited; DA GO 33, 1953, as amended by DA GO 41, 1955)

Company B entitled to:

Presidential Unit Citation (Army), Streamer embroidered COLMAR (3d Infantry Division cited; WD GO 44, 1945)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (3d Counter Intelligence Corps Detachment cited; DA GO 22, 1954)

French Croix de Guerre with Palm, World War II, Streamer embroidered COLMAR (3d Infantry Division cited; DA GO 43, 1950)

French Croix de Guerre, World War II, Fourragere (3d Infantry Division cited; DA GO 43, 1950)

Republic of Korea Presidential Unit Citation, Streamer embroidered UIJONGBU CORRIDOR (3d Counter Intelligence Corps Detachment cited; DA GO 20, 1953)

Republic of Korea Presidential Unit Citation, Streamer embroidered IRON TRIANGLE (3d Counter Intelligence Corps Detachment cited; DA GO 29, 1954)

104th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure an eagle's head proper in front of two swords in saltire argent hilted or and in chief a lightning flash fesswise of the like.

Crest: None approved.

Motto: WATCHFUL AND READY.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence. The crossed swords attest to the unit's readiness; the eagle, wide-eyed and alert, is symbolic of watchfulness. The bolt of lightning refers to the unit's electronic warfare capability. The symbols express the words of the motto and the unit's basic mission and responsibility.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and the motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 16 September 1980 in the Regular Army as the 104th Military Intelligence Battalion, assigned to the 4th Infantry Division, and activated at Fort Carson, Colorado (374th Army Security Agency Company [see ANNEX 1] and 4th Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B). Inactivated 15 December 1995 at Fort Carson, Colorado. Activated 16 January 1996 at Fort Hood, Texas.

ANNEX 1

Constituted 21 November 1963 in the Regular Army as Company C, 303d Army Security Agency Battalion. Activated 20 December 1963 at Fort Lewis, Washington. Reorganized and redesignated 15 October 1966 as the 374th Army Security Agency Company. Inactivated 30 June 1972 at Fort Carson, Colorado. Activated 21 December 1977 at Fort Carson, Colorado.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 4th Counter Intelligence Corps Detachment. Activated 6 August 1944 in France with personnel from provisional Counter Intelligence Corps detachment

attached to the 4th Infantry Division. Inactivated 23 February 1946 at Camp Butner, North Carolina. Activated 30 November 1946 in Germany. Inactivated 20 April 1947 in Germany. Allotted 5 January 1949 to the Regular Army. Activated 31 January 1949 at Fort Ord, California. Reorganized and redesignated 25 January 1958 as the 4th Military Intelligence Detachment. Reorganized and redesignated 26 December 1969 as the 4th Military Intelligence Company. Assigned 21 July 1978 to the 4th Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

Vietnam

- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

Company B entitled to:

World War II–EAME

- Normandy (with arrowhead)
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

Vietnam

- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (374th Radio Research Company cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (374th Radio Research Company cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (374th Radio Research Company cited; DA GO 43, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1967–1969 (374th Radio Research Company cited; DA GO 3, 1970)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1969–1970 (374th Radio Research Company cited; DA GO 52, 1971)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970 (374th Radio Research Company cited; DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1967–1969 (374th Radio Research Detachment cited; DA GO 53, 1970)

Company B entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (4th Military Intelligence Detachment cited; DA GO 39, 1970)

Belgian Fourragere 1940 (4th Infantry Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in Belgium (4th Infantry Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in the Ardennes (4th Infantry Division cited; DA GO 43, 1950)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1968–1969 (4th Military Intelligence Detachment cited; DA GO 3, 1970)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1968–1969 (4th Military Intelligence Detachment cited; DA GO 53, 1970)

105th MILITARY INTELLIGENCE BATTALION (Owls)

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a pile to honor point argent bearing a lozenge throughout gules charged with an owl's head couped or, all above a sword and key in saltire with blade and ward to chief of the second between two lightning flashes palewise of the fourth.

Crest: None approved.

Motto: BOLD VIGIL.

Symbolism: Silver gray and oriental blue are the colors traditionally associated with military intelligence. The sword and key in the saltirewise position represent support and symbolize military leadership. The lightning flashes refer to the speed and power of electronic communications. The owl is symbolic of wisdom and watchfulness and the red diamond shape alludes to the unit's support of the 5th Infantry Division. The two lightning flashes further refer to World War II and the war in Vietnam, in which elements of the battalion served.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 15 May 1967 in the Regular Army as Headquarters and Headquarters Company, 200th Army Security Agency Battalion, and activated at Fort Devens, Massachusetts. Inactivated 15 December 1967 at Fort Devens, Massachusetts.

Redesignated 1 June 1982 as Headquarters, Headquarters and Operations Company, 105th Military Intelligence Battalion, assigned to the 5th Infantry Division, and activated at Fort Polk, Louisiana (405th Army Security Agency Company [see ANNEX 1] and 15th Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B). Battalion inactivated 16 December 1992 at Fort Polk, Louisiana.

ANNEX 1

Constituted 31 May 1965 in the Regular Army as the 405th Army Security Agency Detachment. Activated 1 June 1965 at Fort Lewis, Washington. Inactivated 5 November 1965 in Vietnam. Activated 15 July 1968 in Vietnam. Inactivated 5 December 1969 in Vietnam. Activated 30 September 1971 in Vietnam. Inactivated 30 June 1972 in Vietnam. Redesignated 16 March 1979 as the 405th Army Security Agency Company and activated at Fort Polk, Louisiana.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 5th Counter Intelligence Corps Detachment. Activated 6 August 1944 in France with personnel from provisional Counter Intelligence Corps detachment attached to the 5th Infantry Division. Inactivated 1 April 1950 at Fort Jackson, South Carolina. Allotted 12 May 1954 to the Regular Army. Activated 15 June 1954 in Germany. Inactivated 1 July 1957 at Fort Ord, California. Redesignated 2 February 1962 as the 5th Military Intelligence Detachment. Activated 19 February 1962 at Fort Carson, Colorado. Inactivated 25 May 1969 at Fort Carson, Colorado. Activated 15 November 1969 at Fort Carson, Colorado.

Inactivated 15 December 1970 at Fort Carson, Colorado; concurrently redesignated as the 15th Military Intelligence Company. Redesignated 21 March 1976 as the 5th Military Intelligence Detachment and activated at Fort Polk, Louisiana. Reorganized and redesignated 30 September 1978 as the 15th Military Intelligence Company and assigned to the 5th Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

Vietnam
- Defense
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Consolidation I
- Consolidation II
- Cease-Fire

Company B entitled to:

World War II–EAME
- Normandy
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1965 (Detachment 2, 3d Radio Research Unit, cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (405th Radio Research Detachment cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971–1972 (405th Radio Research Detachment cited; DA GO 32, 1972)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1969 (405th Radio Research Detachment cited; DA GO 6, 1974)

106th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per chevron enhanced sable and argent, a mascle gules interlaced by a flash bendwise and a flash bend sinisterwise azure, between four evergreen trees in pale two and two, and two evergreen trees in fess vert.

Crest: None approved.

Motto: THE NORTHERN WATCH.

Symbolism: The chevronwise division of the background together with the evergreen trees forms the illusion of a snow-covered mountain against the night sky and refers to the unit's service in Alaska as well as its around-the-clock mission and responsibilities. Black represents the covert and white is for truth. Oriental blue is one of the colors associated with military intelligence and red is symbolic of courage. The two flashes intertwined with the mascle emphasize the complexity and interrelated nature of military intelligence work. They allude to electronic capabilities, speed, and a strong defense and also represent the Gordian knot of mythology. The evergreens symbolize security and need for constant alertness; their number (six) alludes to the 6th Infantry Division.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 18 June 1987 in the Regular Army as the 106th Military Intelligence Battalion, assigned to the 6th Infantry Division, and activated at Fort Richardson, Alaska. Inactivated 15 June 1994 at Fort Richardson, Alaska.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

107th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per fess enhanced azure and ermine the silhouette of a bayonet fesswise argent charged with a lightning flash gules and in base a fret throughout of the first.

Crest: None approved.

Motto: THROUGH KNOWLEDGE VICTORY.

Symbolism: Oriental blue and silver gray (white) are the colors traditionally associated with military intelligence units. The ermine background is a heraldic fur and alludes to a cloak symbolizing a "cloak of secrecy" and the covert activities of an intelligence organization. The fret is composed of interlaced parts showing the complexity and interconnections of intelligence information. It resembles a puzzle to be solved by finding the proper key or part, an allusion to the military intelligence mission. The bayonet signifies readiness and response. The lightning flash symbolizes the radio communications and electronics employed to make the unit prepared and effective.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 1 June 1983 in the Regular Army as the 107th Military Intelligence Battalion, assigned to the 7th Infantry Division, and activated at Fort Ord, California (601st Army Security Agency Company [see ANNEX 1] and 7th Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B). Inactivated 15 September 1993 at Fort Ord, California.

ANNEX 1

Constituted 19 March 1951 in the Regular Army as the 601st Communication Reconnaissance Detachment. Activated 4 April 1951 at Fort Jay, New York. Inactivated 15 August 1956 at Fort Jay, New York. Redesignated 21 April 1967 as the 601st Army Security Agency Detachment and activated at Fort Hood, Texas. Inactivated 20 November 1968 in Vietnam. Redesignated 21 September 1978 as the 601st Army Security Agency Company and activated at Fort Ord, California.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 7th Counter Intelligence Corps Detachment. Activated 7 August 1944 at Schofield Barracks, Hawaii, with personnel from provisional Counter Intelligence Corps detachment attached to the 7th Infantry Division. Inactivated 25 April 1946 in Korea. Activated 15 December 1946 in Korea. Inactivated 25 March 1947 in Korea. Activated 12 October 1950 in Korea. Allotted 8 February 1954 to the Regular Army. Reorganized and redesignated 15 May 1959 as the 7th Military Intelligence Detachment. Inactivated 30 June 1971 in Korea. Activated 21 January 1976 at Fort Ord, California. Reorganized and redesignated 21 July 1978 as the 7th Military Intelligence Company and assigned to the 7th Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Armed Forces Expeditions
Panama

Company A additionally entitled to:

Vietnam
Counteroffensive, Phase III
Tet Counteroffensive
Counteroffensive, Phase IV
Counteroffensive, Phase V
Counteroffensive, Phase VI

Company B additionally entitled to:

World War II–AP
Leyte
Ryukyus

Korean War
UN Offensive
CCF Intervention
First UN Counteroffensive
CCF Spring Offensive
UN Summer-Fall Offensive
Second Korean Winter
Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (601st Radio Research Detachment cited; DA GO 28, 1969)

Company B entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (7th Counter Intelligence Corps Detachment cited; DA GO 68, 1953)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (7th Counter Intelligence Corps Detachment cited; DA GO 47, 1950)

108th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, two swords crossed argent hilts to base gules, above a globe of the second gridlined of the field; on a chief sable and between two silver mullets a lightning bolt palewise or terminating upon the center of the globe.

Crest: None approved.

Motto: VICTORY THRU VIGILANCE.

Symbolism: Oriental blue and silver gray (white) are the colors associated with military intelligence. The crossed swords in the colors red and white represent the unit's military readiness and support mission. The bolt of lightning alludes to the unit's technology and to the swift and accurate use of information to thwart enemy plans. The stars and globe suggest the organization's areas of operation in search of intelligence and counterintelligence.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 16 September 1981 in the Regular Army as the 108th Military Intelligence Battalion, assigned to the 8th Infantry Division, and activated in Germany (415th Army Security Agency Company [see ANNEX 1] and 8th Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B). Inactivated 15 November 1991 in Germany.

ANNEX 1

Constituted 26 June 1967 in the Regular Army as the 415th Army Security Agency Detachment and activated at Schofield Barracks, Hawaii. Inactivated 20 November 1968 in Vietnam. Redesignated 1 July 1974 as the 415th Army Security Agency Company and activated in Germany.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 8th Counter Intelligence Corps Detachment. Activated 6 August 1944 in France with personnel

from provisional Counter Intelligence Corps detachment attached to the 8th Infantry Division. Inactivated 21 November 1945 at Holabird Signal Depot, Maryland. Activated 15 December 1946 in Korea. Inactivated 25 March 1947 in Korea. Allotted 17 May 1954 to the Regular Army. Activated 15 June 1954 at Camp Carson, Colorado. Reorganized and redesignated 25 June 1958 as the 8th Military Intelligence Detachment. Reorganized and redesignated 21 February 1973 as the 8th Military Intelligence Company. Assigned 21 April 1974 to the 8th Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

Vietnam
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI

Company B entitled to:

World War II–EAME
- Normandy
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (415th Radio Research Detachment cited; DA GO 28, 1969)

109th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Sable, between two flanches checky argent and azure a sun in splendor in chief and in base a decrescent or, overall palewise a lightning flash gules.

Crest: None approved.

Motto: SEEK AND DISRUPT.

Symbolism: Silver gray and oriental blue are the colors of military intelligence. The checkered arrangement reflects the multifaceted intelligence and electronic warfare capabilities of the battalion. The black center field suggests secrecy and symbolizes tactical operations security. The sun and moon symbols and two hemispheres denote round-the-clock tactical and global deployment capabilities. The red flash is a symbol of the offensive combat capability of electronic warfare as well as the long range electronic surveillance characteristics of the battalion.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

LINEAGE

RA
(inactive)

Constituted 1 October 1981 in the Regular Army as the 109th Military Intelligence Battalion, assigned to the 9th Infantry Division, and activated at Fort Lewis, Washington (335th Army Security Agency Company [see ANNEX 1] and 9th Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B). Inactivated 15 September 1991 at Fort Lewis, Washington.

ANNEX 1

Constituted 27 March 1942 in the Army of the United States as the 112th Signal Radio Intelligence Company. Activated 18 May 1942 at Camp Crowder, Missouri. Reorganized and redesignated 1 September 1945 as the 112th Signal Service Company. Inactivated 23 December 1945 in the Philippine Islands. Allotted 20 December 1946 to the Regular Army and activated in the Philippine Islands as the 112th Signal Service Company (Philippine Scouts). Reorganized and redesignated 1 April 1947 as the 10th Signal Service Battalion (Philippine

Scouts). Reorganized and redesignated 12 June 1948 as the 112th Signal Service Company (Philippine Scouts). Inactivated 1 June 1949 in the Philippine Islands.

Converted and redesignated 17 July 1951 as the 335th Communication Reconnaissance Company. Redesignated 6 April 1966 as the 335th Army Security Agency Company. Activated 15 June 1966 at Fort Riley, Kansas. Inactivated 5 April 1971 in Vietnam. Activated 21 December 1977 at Fort Lewis, Washington.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 9th Counter Intelligence Corps Detachment. Activated 16 August 1944 in France with personnel from provisional Counter Intelligence Corps detachment attached to the 9th Infantry Division. Inactivated 20 April 1947 in Germany. Allotted 5 January 1949 to the Regular Army. Activated 28 January 1949 at Fort Dix, New Jersey. Inactivated 12 March 1951 at Fort Dix, New Jersey. Activated 15 June 1954 in Germany. Reorganized and redesignated 25 January 1958 as the 9th Military Intelligence Detachment. Inactivated 31 January 1962 at Fort Carson, Colorado. Activated 1 July 1966 at Fort Riley, Kansas. Inactivated 25 September 1969 at Schofield Barracks, Hawaii. Redesignated 21 December 1972 as the 9th Military Intelligence Company and activated at Fort Lewis, Washington. Assigned 21 July 1978 to the 9th Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

World War II–AP
- Northern Solomons
- Luzon (with arrowhead)

Vietnam
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

Company B entitled to:

World War II–EAME
- Tunisia
- Sicily
- Normandy
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

Vietnam
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967 (335th Radio Research Company cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (335th Radio Research Company cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (335th Radio Research Company cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (335th Radio Research Company cited; DA GO 43, 1972)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971 (335th Radio Research Company cited; DA GO 32, 1973)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (112th Signal Radio Intelligence Company cited; DA GO 47, 1950)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1967–1968 (335th Radio Research Company cited; DA GO 31, 1969)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1969 (335th Radio Research Company cited; DA GO 59, 1969)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (335th Radio Research Company cited; DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1967–1969 (335th Radio Research Company cited; DA GO 59, 1969)

Company B entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968 (9th Military Intelligence Detachment cited; DA GO 48, 1969)

Belgian Fourragere 1940 (9th Infantry Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action at the Meuse River (9th Infantry Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in the Ardennes (9th Infantry Division cited; DA GO 43, 1950)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1966–1968 (9th Military Intelligence Detachment cited; DA GO 31, 1969)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1969 (9th Military Intelligence Detachment cited; DA GO 59, 1969)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1966–1969 (9th Military Intelligence Detachment cited; DA GO 59, 1969)

110th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a chevronnel debased or, below two griffins' heads in fess point erased addorsed and conjoined of the like.

Crest: None approved.

Motto: SENTINELS OF THE SUMMIT.

Symbolism: Oriental blue is one of the colors associated with military intelligence. Gold is emblematic of excellence and achievement. The chevron, a symbol of strength and support, suggests a mountain peak and connotes the unit's assignment to the 10th Mountain Division. The griffins, ever vigilant and alert, appear above the mountain peak, epitomizing the unit's motto and mission.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 1 December 1988 in the Regular Army as the 110th Military Intelligence Battalion, assigned to the 10th Mountain Division, and activated at Fort Drum, New York.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

Army Superior Unit Award, Streamer embroidered 1994 (110th Military Intelligence Battalion cited; DA GO 14, 1997)

124th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Sable a griffin segreant argent collared azure the collar charged with three plates all within a bordure compony of the second and third.

Crest: None approved.

Motto: INTELLIGENCE FOR VICTORY.

Symbolism: Oriental blue and silver gray (white) are the colors associated with the military intelligence branch. The checky background alludes to a chessboard and symbolizes the use of intelligence information in formulating military strategy and countermeasure. The griffin, noted for keen eyesight, symbolizes vigilance and penetration of the unknown, as suggested by the black area. The discs on the griffin's collar allude to battle engagements in which elements of the unit participated.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 1 June 1981 in the Regular Army as the 124th Military Intelligence Battalion, assigned to the 24th Infantry Division, and activated at Fort Stewart, Georgia (853d Army Security Agency Company [see ANNEX 1] and 24th Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B). Inactivated 15 February 1996 at Fort Stewart, Georgia.

ANNEX 1

Constituted 5 August 1944 in the Army of the United States as the 3323d Signal Information and Monitoring Company. Activated 15 August 1944 at Camp Gruber, Oklahoma. Inactivated 30 October 1945 in Germany. Converted and redesignated 4 September 1947 as the 310th Radio Security Detachment and allotted to the Organized Reserves. (Elements activated 16 September 1947–1 February 1949; inactivated 21 June 1949–6 June 1950.) (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps.)

Redesignated 17 July 1951 as the 853d Communication Reconnaissance Detachment. Withdrawn 20 December 1951 from the Organized Reserve Corps and allotted to the Regular Army. Activated 10 January 1952 at Fort Devens, Massachusetts. Inactivated 1 March 1956 in Germany. Redesignated 16 March 1979 as the 853d Army Security Agency Company and activated at Fort Stewart, Georgia.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 24th Counter Intelligence Corps Detachment. Activated 20 August 1944 in New Guinea with personnel from provisional Counter Intelligence Corps detachment attached to the 24th Infantry Division. Inactivated 25 February 1946 in Japan. Activated 6 October 1950 in Korea. Allotted 8 February 1954 to the Regular Army. Inactivated 15 October 1957 in Japan. Redesignated 5 June 1958 as the 24th Military Intelligence Detachment. Activated 1 July 1958 in Germany. Inactivated 15 April 1970 at Fort Riley, Kansas. Activated 21 February 1976 at Fort Stewart, Georgia. Reorganized and redesignated 30 September 1978 as the 24th Military Intelligence Company and assigned to the 24th Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait

Company A additionally entitled to:

World War II–EAME
- Central Europe

Company B additionally entitled to:

World War II–AP
- New Guinea
- Leyte
- Luzon
- Southern Philippines

Korean War
- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter

DECORATIONS

Army Superior Unit Award, Streamer embroidered 1994 (124th Military Intelligence Battalion [less Companies A and B] cited; DA GO 14, 1997)

Company B additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1950–1951 (24th Counter Intelligence Corps Detachment cited; DA GO 52, 1951)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1953–1954 (24th Counter Intelligence Corps Detachment cited; DA GO 77, 1954)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (24th Counter Intelligence Corps Detachment cited; DA GO 47, 1950)

125th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure a pale argent overall between two mullets in fess a sword and a bayonet saltirewise or bearing a torteau charged with a heraldic rose of the third.

Crest: None approved.

Motto: EYES OF LIGHTNING.

Symbolism: Oriental blue and silver gray are the military intelligence colors. The unsheathed weapons connote readiness and the heraldic rose alludes to the sub rosa mission of the organization. The stars symbolize the wartime service of elements of the unit and the color red indicates their decorations for action in World War II, Korea, and Vietnam.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 16 June 1983 in the Regular Army as the 125th Military Intelligence Battalion, assigned to the 25th Infantry Division, and activated at Schofield Barracks, Hawaii (372d Army Security Agency Company [see ANNEX 1] and 25th Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B).

ANNEX 1

Constituted 11 May 1962 in the Regular Army as Company A, 303d Army Security Agency Battalion. Activated 25 June 1962 at Fort Carson, Colorado. Reorganized and redesignated 15 October 1966 as the 372d Army Security Agency Company. Inactivated 6 March 1971 in Vietnam. Activated 1 July 1974 at Helemano, Hawaii.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 25th Counter Intelligence Corps Detachment. Activated 10 August 1944 in New Caledonia with personnel from provisional Counter Intelligence Corps detachment attached to the 25th Infantry Division. Inactivated 25 February 1946 in

Japan. Activated 6 October 1950 in Korea. Allotted 8 February 1954 to the Regular Army. Reorganized and redesignated 24 December 1958 as the 25th Military Intelligence Detachment. Reorganized and redesignated 26 December 1969 as the 25th Military Intelligence Company. Assigned 21 August 1978 to the 25th Infantry Division.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

Vietnam

- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

Company B entitled to:

World War II–AP

- Luzon

Korean War

- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

Vietnam

- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966 (16th Radio Research Unit cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (372d Radio Research Company cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (372d Radio Research Company cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (372d Radio Research Company cited; DA GO 51, 1971, and United States Army, Vietnam, GO 690, 25 February 1971, as amended by United States Army, Vietnam, GO 1405, 25 April 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (372d Radio Research Company cited; DA GO 43, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1966–1968 (372d Radio Research Company cited; DA GO 48, 1971)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1969–1970 (372d Radio Research Company cited; DA GO 5, 1973)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (372d Radio Research Company cited; DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1969–1971 (372d Radio Research Company cited; DA GO 6, 1974)

Company B entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (25th Counter Intelligence Corps Detachment cited; DA GO 62, 1954)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (25th Military Intelligence Detachment cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (25th Military Intelligence Detachment cited; DA GO 42, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (25th Military Intelligence Detachment cited; DA GO 36, 1970)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (25th Military Intelligence Company cited; DA GO 6, 1974)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (25th Counter Intelligence Corps Detachment cited; DA GO 47, 1950)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1966–1968 (25th Military Intelligence Detachment cited; DA GO 48, 1971)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1968–1970 (25th Military Intelligence Detachment cited; DA GO 5, 1973)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1966–1970 (25th Military Intelligence Detachment cited; DA GO 51, 1971)

126th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Celeste a griffin rampant argent grasping a double-warded key with a lightning bolt shaft gules, wards to chief of the second and the bow consisting of a heraldic rose of the like and azure seeded or and slipped vert.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and celeste, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: VIGILANCE AND STRENGTH.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence. The griffin combines the keen eyesight and mobility of the eagle with the courage and prowess of the lion. He has acute hearing and is alert and watchful; he also epitomizes the unit's motto. The shaft of the key consists of a lightning bolt to highlight the electronic nature of the unit's mission; the bow is formed by a heraldic rose, adapted from the military intelligence branch insignia, and referring to the sub rosa functions of the unit. The key, used both to secure and unlock, underscores military intelligence as essential to total preparedness.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

AR

Lineage (inactive)

Constituted 16 September 1987 in the Army Reserve as the 126th Military Intelligence Battalion and activated with Headquarters at East Windsor, Connecticut. Inactivated 15 September 1993 at East Windsor, Connecticut.

Campaign Participation Credit

None.

Decorations

None.

128th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, a demi-griffin grasping a key, the wards upward and outward forming a keystone or; on a chief checky argent and sable, a sword and lightning flash saltirewise of the second.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, or and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: KEYSTONE TO VICTORY.

Symbolism: Oriental blue is one of the colors associated with the military intelligence branch. The demi-griffin stands for courage, intelligence, and vigilance and holds a key as the symbol of secrecy and security. The wards of the key form a keystone recalling the battalion's motto, its home state of Pennsylvania, and the unit's affiliation with the 28th Infantry Division. The checky chief, recalling the insignia of the 99th United States Army Reserve Command, suggests strategy, while its colors, black and white, refer to night and day operations. The sword represents military preparedness; the lightning flash suggests speed and electronic capabilities. Gold stands for excellence.

Distinctive Unit Insignia

The distinctive unit insignia is a modification of the shield and motto of the coat of arms.

Lineage and Honors

AR

Lineage (active)

Constituted 18 September 1987 in the Army Reserve as the 128th Military Intelligence Battalion and activated with Headquarters at Allison Park, Pennsylvania.

Campaign Participation Credit

None.

Decorations

None.

134th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Or, a griffin's head erased sable grasping in his beak a lightning bolt gules, a bordure quarterly azure and argent.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, or and sable, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: GATHER INTERPRET INFORM.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. Blue conveys loyalty; red is indicative of action, bravery, and courage. Gold reflects excellence, achievement, and high ideals. The griffin combines the strength and courage of a lion with the vigilance and awareness of an eagle, reflecting the mission of the organization. The lightning bolt alludes to the speed and accuracy with which the unit's mission is carried out and recalls its motto.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

AR

LINEAGE (active)

Constituted 10 February 1991 in the Army Reserve as the 134th Military Intelligence Battalion. Activated 16 September 1992 with Headquarters at Eagan, Minnesota. Location of Headquarters changed 30 June 1994 to Fort Snelling, Minnesota.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

135th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure a lightning flash issuant from dexter chief bendwise or, overall a fess argent bearing a bar invected sable.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, or and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: PIERCING THE FOG OF WAR.

Symbolism: The colors oriental blue and silver gray are traditionally associated with military intelligence units. The lightning flash is symbolic of speed in accumulating accurate information necessary to achieve total military preparedness. The stylized clouds allude to the unit's capabilities and goals to strive twenty-four hours a day to pierce enemy intelligence lines effectively and provide the information necessary for total preparedness.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

AR

Lineage (active)

Constituted 16 September 1988 in the Army Reserve as the 135th Military Intelligence Battalion and activated with Headquarters at Lenexa, Kansas. Location of Headquarters changed 1 April 1993 to Olathe, Kansas.

Campaign Participation Credit

None.

Decorations

None.

138th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Per saltire sable and azure on a saltire argent a key and lightning flash saltirewise of the second.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: FORTIOR EX VIGILIS (STRONGER AFTER VIGILANCE).

Symbolism: Oriental blue is one of the colors of the military intelligence branch. The color black represents secrecy and constancy. The saltire alludes to the joint functions of intelligence and security. The blue key is for guardianship, and the lightning flash is for electronic communications.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

Lineage

AR (active)

Constituted 12 March 1956 in the Army Reserve as the 314th Communication Reconnaissance Battalion; Headquarters and Headquarters Company concurrently activated at Chicago, Illinois. Redesignated 24 May–31 October 1956 as the 314th Army Security Agency Battalion. (Organic elements activated 27 August–1 November 1956.) Inactivated 21 June 1959 at Chicago, Illinois. Activated 1 October 1962 with Headquarters at Chicago, Illinois. Battalion broken up 15 August 1966 and its elements reorganized and redesignated as follows: Headquarters and Headquarters Company as Headquarters and Headquarters Company, 314th Army Security Agency Battalion; Company A as the 522d Army Security Agency Company (see ANNEX 1); Companies B and C as the 523d and 524th Army Security Agency Companies (hereafter separate lineages); Company D as the 525th Army Security Agency Company (see ANNEX 2). Location of Headquarters and Headquarters Company changed 31 March 1982 to Rosemont, Illinois.

Headquarters and Headquarters Company, 314th Army Security Agency Battalion, reorganized and redesignated 16 November 1983 as Headquarters,

Headquarters and Operations Company, 138th Military Intelligence Battalion (522d Army Security Agency Company [see ANNEX 1] and 525th Army Security Agency Company [see ANNEX 2] concurrently consolidated to form Company A; 910th Military Intelligence Company [see ANNEX 3], 121st Military Intelligence Detachment [see ANNEX 4], and 232d Military Intelligence Detachment [see ANNEX 5] consolidated to form Company B).

ANNEX 1

Constituted 12 March 1956 in the Army Reserve as Company A, 314th Communication Reconnaissance Battalion. Redesignated 19 July 1956 as Company A, 314th Army Security Agency Battalion. Activated 27 August 1956 at Chicago, Illinois. Location changed 1 June 1957 to Evanston, Illinois. Inactivated 21 June 1959 at Evanston, Illinois. Activated 1 October 1962 at Evanston, Illinois. Location changed 1 March 1963 to Chicago, Illinois. Reorganized and redesignated 15 August 1966 as the 522d Army Security Agency Company.

ANNEX 2

Constituted 23 August 1962 in the Army Reserve as Company D, 314th Army Security Agency Battalion. Activated 1 October 1962 at Milwaukee, Wisconsin. Reorganized and redesignated 15 August 1966 as the 525th Army Security Agency Company. Inactivated 31 January 1968 at Milwaukee, Wisconsin. Activated 1 February 1974 at Chicago, Illinois. Location changed 31 March 1982 to Rosemont, Illinois.

ANNEX 3

Constituted 28 July 1945 in the Army of the United States as the 536th Counter Intelligence Corps Detachment. Activated 10 August 1945 in France. Inactivated 23 February 1946 in France. Redesignated 4 September 1947 as the 910th Counter Intelligence Corps Detachment and allotted to the Organized Reserves. Activated 1 October 1947 at Chicago, Illinois. (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps; redesignated 9 July 1952 as the Army Reserve.) Inactivated 4 December 1950 at Chicago, Illinois. Redesignated 19 May 1959 as the 910th Military Intelligence Detachment. Activated 1 June 1959 at Chicago, Illinois. Reorganized and redesignated 1 March 1972 as the 910th Military Intelligence Company. Location changed 24 February 1980 to Arlington Heights, Illinois.

ANNEX 4

Constituted 3 August 1945 in the Army of the United States as the 1020th Counter Intelligence Corps Detachment. Activated 10 August 1945 at Fort George G. Meade, Maryland. Inactivated 3 December 1945 at Camp Stoneman, California. Redesignated 16 November 1948 as the 121st Counter Intelligence Corps Detachment and allotted to the Organized Reserve Corps. Activated 31

December 1948 at Chicago, Illinois. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 25 June 1953 at Chicago, Illinois. Redesignated 19 May 1959 as the 121st Military Intelligence Detachment. Activated 1 June 1959 at Chicago, Illinois. Location changed 24 February 1980 to Arlington Heights, Illinois.

ANNEX 5

Constituted 21 June 1944 in the Army of the United States as the 222d Counter Intelligence Corps Detachment. Activated 1 July 1944 at Camp Campbell, Kentucky. Inactivated 1 October 1945 in Czechoslovakia. Redesignated 5 June 1947 as the 232d Counter Intelligence Corps Detachment and allotted to the Organized Reserves. Activated 17 June 1947 at New York, New York. (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps; redesignated 9 July 1952 as the Army Reserve.) Inactivated 10 November 1948 at New York, New York. Activated 18 January 1949 at Chicago, Illinois. Inactivated 4 December 1950 at Chicago, Illinois. Redesignated 5 November 1962 as the 232d Military Intelligence Detachment. Activated 11 February 1963 at Chicago, Illinois. Location changed 24 February 1980 to Arlington Heights, Illinois.

CAMPAIGN PARTICIPATION CREDIT

Company B entitled to:

World War II–EAME
- Rhineland
- Ardennes-Alsace
- Central Europe

DECORATIONS

None.

140th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure within an orle argent, in base a pyramid of the like and in chief a sun in splendor issuing to base five lightning flashes or and charged with a globe of the like gridlined of the first.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: SEMPER VIGIL (ALWAYS WATCHFUL).

Symbolism: Oriental blue and silver gray (white) are the colors associated with military intelligence. The sun represents the Greek god Helios, who, according to mythology, could bring all secrets to light; surrounding a globe, it represents the unit's worldwide military intelligence mission. The lightning flashes suggest electronic warfare and communication capabilities. The sun and lightning flashes are gold and allude to California, the "Golden State," the unit's home area. The pyramid personifies longevity and strength.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage And Honors

Lineage

AR
(active)

Constituted 16 July 1986 in the Army Reserve as the 140th Military Intelligence Battalion and activated with Headquarters at Bell, California.

Campaign Participation Credit

None.

Decorations

None.

141st MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure a compass rose or charged with a sword sable, grip gules surmounted by a globe argent, gridlined or bearing a lamp of knowledge of the like enflamed gules.

Crest: That for the regiments and separate battalions of the Utah Army National Guard: On a wreath of the colors, or and azure, a beehive beset with seven bees all proper.

Motto: STRENGTH THROUGH KNOWLEDGE.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence. The shield represents the unit's constant protection of the country, while the globe symbolizes its worldwide mission. The gold lamp of knowledge reflects the unit's efforts to gain knowledge to be ready and prepared to keep world peace. The black sword exemplifies its vigilance, loyalty, and readiness to defend freedom, liberty, and country. The rays of light, adapted from the military intelligence emblem, allude to a compass and symbolize the unit's readiness to respond wherever needed.

Distinctive Unit Insignia

The distinctive unit insignia is a modification of the shield and motto of the coat of arms.

Lineage and Honors

Lineage

ARNG
(Utah)

Organized from new and existing units and federally recognized 8 October 1988 in the Utah Army National Guard as the 141st Military Intelligence Battalion with Headquarters at Draper. Location of Headquarters changed 16 February 1995 to Provo.

Home Area: Statewide.

Campaign Participation Credit

None.

Decorations

None.

142d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Celeste, a globe enhanced azure, gridlined argent above a wreath of four sego lilies proper overall a dagger palewise argent.

Crest: That for the regiments and separate battalions of the Utah Army National Guard: On a wreath of the colors, argent and azure, a beehive beset with seven bees all proper.

Motto: INTO ALL THE WORLD.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. The dagger symbolizes military preparedness and the globe and motto represent the worldwide capabilities and responsibilities of the unit. The sego lilies are symbols associated with Utah and reflect the unit's location in that state.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia consists of elements of the shield and crest of the coat of arms and incorporates the motto.

LINEAGE AND HONORS

ARNG
(Utah)

LINEAGE

Organized and federally recognized 12 February 1960 in the Utah Army National Guard at Fort Douglas as the 142d Military Intelligence Linguist Company. Reorganized 15 May 1964 as a Table of Distribution unit. Location changed 1 December 1971 to Salt Lake City.

Reorganized and redesignated 1 April 1980 as Headquarters and Headquarters Company, 142d Military Intelligence Battalion (organic elements concurrently organized and federally recognized). Location of Headquarters changed 15 August 1982 to Fort Douglas; changed 1 January 1988 to Draper. Battalion reorganized 1 April 1988 as a Table of Organization and Equipment unit. (Company A ordered into active federal service 3 January 1991 at Bountiful; released from active federal service 2 April 1991 and reverted to state control.) Location of Headquarters changed 1 October 1995 to Salt Lake City.

Home Area: Northern Utah.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

Southwest Asia
Liberation and Defense of Kuwait

DECORATIONS

None.

147th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Checky argent and sable, on a pile argent a Viking helmet of the second detailed or, lined gules, emitting a lightning flash to base azure.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and sable, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: FUROR FULMINIS (FURY OF LIGHTNING).

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. The pile reflects accuracy and the ability to pinpoint information. The blue lightning bolt emphasizes that ability while symbolizing speed and electronic warfare. The checky background alludes to strategy. The Viking helmet connotes protection and preparedness. It also signifies the unit's affiliation with the 47th Infantry (Viking) Division.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is an adaptation of the shield and motto of the coat of arms.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 18 September 1987 in the Army Reserve as the 147th Military Intelligence Battalion and activated with Headquarters at Fort Snelling, Minnesota. Location of Headquarters changed 1 July 1989 to Eagan, Minnesota. Inactivated 15 September 1992 at Eagan, Minnesota.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

163d MILITARY INTELLIGENCE BATTALION (The Blue Watch)

Heraldic Items

Coat of Arms

Shield: Azure on a bend checky argent and sable, overall a Philippine sun charged with a Korean taeguk in the colors of the Republic of Korea, scarlet and blue.

Crest: On a wreath of the colors, argent and azure, a trident argent interlaced with two anchors in saltire or.

Motto: KNOWLEDGE IS POWER.

Symbolism: The sun alludes to service in the Philippines during World War II and to the Philippine Presidential Unit Citation. The taeguk symbolizes the Republic of Korea Presidential Unit Citation and the unit's ten campaigns in the Korean War. The black and white checky alludes to the intelligence functions of the organization. Oriental blue and silver gray are the colors used by intelligence units.

The two crossed anchors allude to the two Presidential Unit Citations (Navy) and the trident refers to the Navy Unit Commendation.

Distinctive Unit Insignia

The distinctive unit insignia consists of elements of the shield, crest, and motto of the coat of arms.

Lineage and Honors

RA

Lineage (active)

Constituted 5 April 1945 in the Army of the United States as the 163d Language Detachment. Activated 23 April 1945 in the Philippine Islands. Reorganized and redesignated 25 September 1949 as the 163d Military Intelligence Service Detachment. Allotted 19 December 1950 to the Regular Army. Reorganized and redesignated 1 September 1952 as the 163d Military Intelligence Service Platoon. Reorganized and redesignated 28 March 1954 as the 163d Military Intelligence Platoon. Inactivated 15 November 1954 in Korea. Activated 26 December 1955 in Italy.

Reorganized and redesignated 20 September 1957 as the 163d Military Intelligence Battalion. Inactivated 25 April 1964 in Italy. Redesignated 1 October 1969 as Headquarters and Headquarters Company, 163d Military Intelligence Battalion, and activated at Fort Hood, Texas (Company A concurrently constituted and activated). (Company A reorganized and redesignated 21 April 1978 as Company B, 529th Military Intelligence Company [see ANNEX] concurrently reorganized and redesignated as Company A.)

ANNEX

Constituted 14 July 1945 in the Army of the United States as the 255th Interrogation Prisoner of War Team and activated in Germany. Inactivated 30 November 1946 in Germany. Redesignated 1 October 1948 as the 529th Interrogation Team and allotted to the Regular Army. Activated 15 October 1948 at Fort Riley, Kansas. Inactivated 10 February 1949 at Fort Riley, Kansas. Redesignated 17 March 1965 as the 529th Military Intelligence Company. Activated 19 March 1965 at Fort Hood, Texas.

CAMPAIGN PARTICIPATION CREDIT

World War II
- Luzon

Korean War
- UN Defensive
- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

DECORATIONS

Presidential Unit Citation (Navy), Streamer embroidered INCHON (163d Military Intelligence Service Detachment cited; DA GO 63, 1952)

Presidential Unit Citation (Navy), Streamer embroidered HWACHON RESERVOIR (163d Military Intelligence Service Detachment cited; DA GO 38, 1957)

Navy Unit Commendation, Streamer embroidered PANMUNJOM (163d Military Intelligence Service Platoon cited; DA GO 38, 1957)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (163d Language Detachment cited; DA GO 47, 1950)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA (163d Military Intelligence Service Platoon cited; DA GO 10, 1954)

165th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Sable, a torch azure issuing rays from an intertwined continuous ribbon argent.

Crest: None approved.

Motto: QUALITY PRIDE SUCCESS.

Symbolism: Oriental blue is the primary color associated with military intelligence organizations. The torch is symbolic of the illumination provided by the collection and dissemination of intelligence data. The black background suggests secrecy and stealth. The ribbon-like symbol, in place of a flame, folds back on itself and is representative of the counterintelligence mission.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia consists of elements of the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 27 September 1951 in the Regular Army as the 165th Military Intelligence Service Detachment. Activated 18 October 1951 in Japan. Reorganized and redesignated 1 September 1952 as the 165th Military Intelligence Service Company. Reorganized and redesignated 28 March 1954 as the 165th Military Intelligence Company. Inactivated 25 January 1958 at Fort Bragg, North Carolina. Activated 1 June 1962 in Germany.

Reorganized and redesignated 1 July 1972 as Headquarters and Headquarters Company, 165th Military Intelligence Battalion. Inactivated 1 July 1983 in Germany. Redesignated 16 April 1984 as Headquarters, Headquarters and Service Company, 165th Military Intelligence Battalion, and activated in Germany (organic elements concurrently constituted and activated).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

201st MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent, between in chief a terrestrial globe azure gridlined of the field and in base a helm sable lined gules upon a laurel wreath proper, a sword and lightning flash saltirewise of the fourth.

Crest: None approved.

Motto: ACCURATE FAST ALL SOURCE.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence. The helmet is adapted from the device of the 513th Military Intelligence Group, reflecting the unit's original assignment. The globe refers to the worldwide scope of the unit's mission and alludes to the "all source" emphasis of the motto. The lightning flash and sword symbolize speed and accuracy of communications. The laurel wreath denotes achievement. Black stands for strength and stability.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia consists of elements of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 2 October 1982 in the Regular Army as Headquarters and Headquarters Company, 201st Military Intelligence Battalion, and activated at Fort Monmouth, New Jersey. (Organic elements constituted and activated 16 July 1987 at Vint Hill Farms Station, Virginia.)

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia
Defense of Saudi Arabia
Liberation and Defense of Kuwait
Cease-Fire

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (201st Military Intelligence Battalion cited; DA GO 14, 1997)

Army Superior Unit Award, Streamer embroidered 1993 (201st Military Intelligence Battalion cited; DA GO 14, 1997)

202d MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Celeste, a lightning bolt or and torch gules fimbriated argent in saltire overall a dragon's head of the last, on a chief checky argent and sable a helm affronté garnished sable.

Crest: None approved.

Motto: CONLIGE ET PROFICE (COLLECT AND EXPLOIT).

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. The helmet is adapted from the device of the 513th Military Intelligence Group and reflects the unit's original assignment. The helmet on the checky background symbolizes counterintelligence activities. The lightning flash denotes speed and electronic warfare. The torch symbolizes truth and alludes to interrogation. The dragon, a mythical guardian of treasure, symbolizes security and strength.

Distinctive Unit Insignia

The distinctive unit insignia consists of elements of the coat of arms.

Lineage and Honors

RA

Lineage (active)

Constituted 2 October 1982 in the Regular Army as the 202d Military Intelligence Battalion and activated at Fort Monmouth, New Jersey.

Campaign Participation Credit

Southwest Asia

Defense of Saudi Arabia
Liberation and Defense of Kuwait
Cease-Fire

Decorations

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (202d Military Intelligence Battalion cited; DA GO 27, 1994, as amended by DA GO 14, 1997)

Army Superior Unit Award, Streamer embroidered 1992–1993 (DA GO 1, 1996)

203d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

DISTINCTIVE UNIT INSIGNIA

Description: A silver color metal and enamel device consisting of a silver gear bearing a black helmet with silver details, face forward, all centered upon a blue disc with silver grid lines encircled by a silver scroll inscribed TECHNICIANS FOR VICTORY in red letters and in base two sprigs of green laurel.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. The gridlined sphere represents the unit's worldwide mission and the gear refers to the technical aspect of its responsibilities. The helmet is adapted from the device of the 513th Military Intelligence Group, alluding to the unit's original assignment and symbolizing covert vigilance and preparedness. The laurel, a traditional symbol of achievement, exemplifies the motto.

FLAG DEVICE

The flag device is the same as the distinctive unit insignia.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 2 October 1982 in the Regular Army as Headquarters and Headquarters Company, 203d Military Intelligence Battalion, and activated at Aberdeen Proving Ground, Maryland. (Organic elements constituted 16 October 1988; Company A concurrently activated at at Fort Monmouth, New Jersey.) Battalion inactivated 16 October 1989 at Fort Monmouth, New Jersey.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

204th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, a double-warded key palewise with an arched lightning flash on either side connecting the ward and bow and each flash enclosing a fleur-de-lis argent and on the bow an ermine spot.

Crest: On a wreath of the colors, argent and azure, a dragon sejant with wings elevated and addorsed gules armed and langued of the second spattered with seventeen mullets and grasping in his dexter claw three lightning flashes or.

Motto: SILENTLY WE DEFEND.

Symbolism: Oriental blue is one of the colors associated with military intelligence, and a key is emblematic of authority and security. The double ward and flashes represent the unit's concern for both overt and covert security communications. The flashes also denote celerity in operation procedures and allude to the unit's signal lineage. Initially designated as the 3118th Signal Service Battalion, the unit's participation in the Northern France, Rhineland, and Central Europe campaigns during World War II is represented by the fleurs-de-lis and ermine spot. The design has been adapted from the badge of a predecessor unit, the 502d Army Security Agency Battalion.

The dragon, a mythical beast renowned as a vigilant guardian and defender, symbolizes the heritage, mission, and ideals of the unit. The red dragon alludes to the Meritorious Unit Commendation (Army) and service of elements of the battalion in Vietnam. Red emphasizes the unit's courage, determination, and valor. The stars denote military preparedness and excellence in endeavors. Service during World War II in Northern France, Rhineland, and Central Europe is represented by the three lightning flashes.

Distinctive Unit Insignia

The distinctive unit insignia is an adaptation of the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA
(inactive)

LINEAGE

Constituted 4 November 1943 in the Army of the United States as the 3118th Signal Service Battalion. Activated 15 November 1943 at Camp Crowder, Missouri. Reorganized and redesignated 13 April 1945 as the 3118th Signal Service Group. Reorganized and redesignated 14 November 1945 as the 3118th Signal Service Battalion. Headquarters reorganized and redesignated 3 April 1946 as Headquarters and Headquarters Detachment, 3118th Signal Service Group (remainder of battalion concurrently disbanded). Inactivated 20 June 1947 in Germany.

Converted and redesignated 25 April 1951 as Headquarters and Headquarters Company, 502d Communication Reconnaissance Group, and allotted to the Regular Army. Activated 15 May 1951 at Fort Devens, Massachusetts. Redesignated 1 July 1956 as Headquarters and Headquarters Company, 502d Army Security Agency Group. Inactivated 15 October 1957 in Germany. Activated 3 May 1971 in Germany. Reorganized and redesignated 1 October 1981 as Headquarters and Headquarters Company, 502d Army Security Agency Battalion.

Reorganized and redesignated 16 October 1986 as Headquarters and Headquarters Company, 204th Military Intelligence Battalion (409th Army Security Agency Company [see ANNEX 1] concurrently reorganized and redesignated as Company A; 328th Army Security Agency Company [see ANNEX 2] reorganized and redesignated as Company D). Battalion inactivated 16 July 1995 in Germany.

ANNEX 1

Constituted 1 April 1966 in the Regular Army as the 409th Army Security Agency Detachment. Activated 8 April 1966 at Fort George G. Meade, Maryland. Inactivated 6 March 1971 in Vietnam. Redesignated 1 July 1974 as the 409th Army Security Agency Company and activated in Germany.

ANNEX 2

Organized 1 April 1944 in England as the 3250th Signal Service Company. (Constituted 12 April 1944 in the Army of the United States.) Inactivated 13 March 1946 in France.

Converted and redesignated 25 April 1951 as the 328th Communication Reconnaissance Company and allotted to the Regular Army. Activated 15 May 1951 at Fort Devens, Massachusetts. Redesignated 1 July 1956 as the 328th Army Security Agency Company. Inactivated 15 October 1957 in Germany. Activated 20 November 1968 in Vietnam. Inactivated 30 June 1972 in Vietnam. Activated 1 July 1974 in Germany.

CAMPAIGN PARTICIPATION CREDIT

World War II
Northern France
Rhineland
Central Europe

Company A additionally entitled to:

Vietnam
Counteroffensive, Phase II
Counteroffensive, Phase III
Tet Counteroffensive
Counteroffensive, Phase IV
Counteroffensive, Phase V
Counteroffensive, Phase VI
Tet 69/Counteroffensive
Summer-Fall 1969
Winter-Spring 1970
Sanctuary Counteroffensive
Counteroffensive, Phase VII

Southwest Asia
Defense of Saudi Arabia
Liberation and Defense of Kuwait
Cease-Fire

Company D additionally entitled to:

World War II–EAME
Normandy (with arrowhead)
Ardennes-Alsace

Vietnam
Counteroffensive, Phase VI
Tet 69/Counteroffensive
Summer-Fall 1969
Winter-Spring 1970
Sanctuary Counteroffensive
Counteroffensive, Phase VII
Consolidation I
Consolidation II
Cease-Fire

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered EUROPEAN THEATER (3118th Signal Service Group cited; GO 34, United States Forces, European Theater, 11 February 1946)

Army Superior Unit Award, Streamer embroidered 1991–1992 (204th Military Intelligence Battalion cited; DA GO 12, 1994)

Company A additionally entitled to:

Valorous Unit Award, Streamer embroidered LONG BINH–BIEN HOA (409th Radio Research Detachment cited; DA GO 12, 1969, as amended by DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (409th Radio Research Detachment cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (409th Radio Research Detachment cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (409th Radio Research Detachment cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (409th Radio Research Detachment cited; DA GO 43, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1966–1968 (409th Radio Research Unit cited; DA GO 60, 1969)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1969–1970 (409th Radio Research Detachment cited; DA GO 50, 1971)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970 (409th Radio Research Detachment cited; DA GO 55, 1971)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (409th Radio Research Detachment cited; DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1969–1970 (409th Radio Research Detachment cited; DA GO 6, 1974)

Company D additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (328th Radio Research Company cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (328th Radio Research Company cited; DA GO 43, 1972)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971–1972 (328th Radio Research Company cited; DA GO 32, 1973)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1969–1970 (328th Radio Research Company cited; DA GO 42, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (328th Radio Research Company cited; DA GO 6, 1974)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1971 (328th Radio Research Company cited; DA GO 6, 1974)

205th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, on pale argent a torch sable enflamed gules superimposed by a sword argent hilt or grip garnished gules, between two quills palewise argent.

Crest: On a wreath of the colors, argent and azure, a lightning flash palewise gules rising from a wreath of palm proper, overall an oriental dragon passant or armed gules and garnished azure.

Motto: PACIFIC VIGILANCE.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence units. Blue conveys devotion and loyalty, red is indicative of courage and zeal, while white portrays integrity. Gold reflects excellence, achievement, and high ideals; black reflects covert capabilities. The quills symbolize the unit's analytical functions; the torch signifies guidance, leadership, and knowledge. The sword is symbolic of military preparedness.

The lightning flash indicates speed and accuracy and alludes to the battalion's heritage and association with the Signal Corps. It is red to indicate the Meritorious Unit Commendation (Army) received by the unit during World War II. The palm fronds stand for victory, while the oriental dragon personifies vigilance and preparedness. They suggest the Pacific area and reflect the unit's motto.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 1 January 1939 in the Regular Army as the 2d Signal Service Company and activated with Headquarters at Fort Monmouth, New Jersey (organic elements concurrently organized from existing units). Redesignated 14 April 1942 as the 2d Signal Service Battalion. Headquarters, 2d Signal Service Battalion, disbanded 20 April 1946 at Arlington Hall Station, Virginia. (Organic elements disbanded 15 May 1950.)

Headquarters, 2d Signal Service Battalion, reconstituted 1 October 1991 in the Regular Army as Headquarters, 205th Military Intelligence Battalion. Redesignated 31 October 1992 as Headquarters, Headquarters and Service Company, 205th Military Intelligence Battalion, and activated at Fort Shafter, Hawaii (organic elements concurrently constituted and activated).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered ARLINGTON HALL STATION 1945 (9420th Technical Service Unit, Headquarters and Detachments, 2d Signal Service Battalion, cited; GO 2, Office of the Chief Signal Officer, Army Service Forces, 1 May 1945)

206th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per chevron enarched reversed sable and celeste, nine rays radiating from honor point argent; in base a lion's head erased argent charged with two bars gules.

Crest: None approved.

Motto: COLLECTION FOR DEFENSE.

Symbolism: The white concentric rays represent light or knowledge gathered to a central point; they refer to the battalion's mission of collecting strategic information. The white and scarlet lion on the blue background is taken from the coat of arms of Hesse in Germany, where the unit was activated. The head of the lion is used because it is a symbol of intelligence and reason. The color of the background, oriental blue, also refers to military intelligence.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia consists of elements of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 15 March 1968 in the Regular Army as the 18th Military Intelligence Battalion and activated in Germany. Reorganized and redesignated 16 October 1986 as Headquarters and Headquarters Company, 18th Military Intelligence Battalion. (Organic elements constituted 16 October 1992; Company A concurrently activated in Germany.) Battalion inactivated 16 July 1995 in Germany.

Redesignated 13 February 1996 as the 206th Military Intelligence Battalion.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

Army Superior Unit Award, Streamer embroidered 1988–1989 (18th Military Intelligence Battalion cited; DA GO 15, 1990)

Army Superior Unit Award, Streamer embroidered 1991–1992 (18th Military Intelligence Battalion cited; DA GO 12, 1994)

223d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent, a lightning flash palewise gules and a double-warded key and sword saltirewise sable, overall a hurt gridlined argent.

Crest: That for the regiments and separate battalions of the California Army National Guard: On a wreath of the colors, argent and gules, the setting sun behind a grizzly bear passant on a grassy field all proper.

Motto: INSIGHT THROUGH INQUIRY.

Symbolism: Oriental blue is one of the colors traditionally associated with military intelligence units. The lightning flash denotes the unit's signal intelligence. The key is emblematic of knowledge, authority, and security. The black sword is symbolic of covert operations and military preparedness; the globe reflects the unit's worldwide scope.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia consists of elements of the shield and motto of the coat of arms.

LINEAGE AND HONORS

ARNG
(California)

LINEAGE

Organized and federally recognized 16 January 1992 in the California Army National Guard as the 223d Military Intelligence Battalion with Headquarters at Fort Funston.

Home Area: Statewide.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

224th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Quarterly azure and argent a griffin sejant or grasping two flashes saltirewise gules.

Crest: None approved.

Motto: VIGILANCE ABOVE.

Symbolism: Oriental blue and silver gray are the colors associated with the military intelligence branch. The crosswise arrangement of the background is a reference to the Republic of Vietnam Cross of Gallantry with Palm awarded to the unit for service in Vietnam. The griffin is a heraldic creature combining the strength and courage of a lion with the vigilance and awareness of an eagle; as such, it is well suited to represent the ideals and capabilities of an intelligence unit. Its wings refer to the airborne mission, and the flashes it grasps denote the electronic data collection mission of the unit.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 1 June 1966 in the Regular Army as Headquarters and Headquarters Detachment, 224th Aviation Battalion, and activated in Vietnam. Redesignated 1 December 1968 as Headquarters and Headquarters Company, 224th Aviation Battalion. Converted and redesignated 19 May 1971 as Headquarters and Headquarters Company, 224th Army Security Agency Battalion. Inactivated 6 March 1973 at Oakland, California.

Redesignated 1 June 1981 as Headquarters, Headquarters and Service Company, 224th Military Intelligence Battalion, and activated at Hunter Army Airfield, Georgia (172d Military Intelligence Detachment [see ANNEX 1] concurrently reorganized and redesignated as Company A; 144th Aviation Company [see ANNEX 2] converted and redesignated as Company B and activated).

ANNEX 1

Constituted 5 April 1945 in the Army of the United States as the 172d Language Detachment. Activated 23 April 1945 in the Philippine Islands. Inactivated 15 April 1946 in Japan. Redesignated 14 January 1955 as the 172d Military Intelligence Platoon and allotted to the Regular Army. Activated 7 March 1955 in Germany. Inactivated 25 June 1958 in Germany. Activated 15 July 1959 at Fort Devens, Massachusetts. Reorganized and redesignated 25 August 1961 as the 172d Military Intelligence Detachment. Inactivated 1 September 1963 in Germany. Activated 3 May 1965 at Fort Campbell, Kentucky. Inactivated 21 August 1972 at Fort Campbell, Kentucky. Activated 21 November 1977 at Fort Wainwright, Alaska.

ANNEX 2

Constituted 1 June 1966 in the Regular Army as the 144th Aviation Company and activated in Vietnam. Inactivated 30 September 1971 in Vietnam.

CAMPAIGN PARTICIPATION CREDIT

Vietnam
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII
- Consolidation I
- Consolidation II
- Cease-Fire

Company A additionally entitled to:

World War II–AP
- Luzon

Vietnam
- Defense

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (Headquarters and Headquarters Detachment, 224th Aviation Battalion, and 144th Aviation Company cited; DA GO 17, 1968, as amended by DA GO 1, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1969 (Headquarters and Headquarters Company, 224th Aviation Battalion, and 144th Aviation Company cited; DA GO 2, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971–1972 (224th Aviation Battalion and 144th Aviation Company cited; DA GO 32, 1973)

Army Superior Unit Award, Streamer embroidered 1987–1988 (224th Military Intelligence Battalion cited; DA GO 35, 1989)

Army Superior Unit Award, Streamer embroidered 1988–1990 (224th Military Intelligence Battalion cited; DA GO 2, 1991)

Army Superior Unit Award, Streamer embroidered 1992–1993 (224th Military Intelligence Battalion cited; DA GO 27, 1994)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (224th Aviation Battalion and 144th Aviation Company cited; DA GO 6, 1974)

Company A additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1965–1967 (172d Military Intelligence Detachment cited; DA GO 48, 1968)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (172d Language Detachment cited; DA GO 47, 1950)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1968–1970 (172d Military Intelligence Detachment cited; DA GO 51, 1971)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1969–1971(172d Military Intelligence Detachment cited; DA GO 5, 1973)

229th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Argent, on a pale wavy azure two pallets wavy of the first between two griffin heads erased in fess addorsed of the second eyes and tongues gules.

Crest: None approved.

Motto: STRENGTH FROM INTELLIGENCE.

Symbolism: Oriental blue and silver gray are the colors traditionally associated with the military intelligence branch. The griffin, noted for keen eyesight, symbolizes surveillance. The two griffins back to back represent vigilance; they also suggest the unit's original two continent and two ocean area of operations. The wavy pale refers to the Panama Canal.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

RA

Lineage (active)

Constituted 1 April 1985 in the Regular Army as the 29th Military Intelligence Battalion and activated in Panama. Inactivated 17 October 1991 in Panama.

Redesignated 7 December 1995 as the 229th Military Intelligence Battalion. Headquarters transferred 15 March 1996 to the United States Army Training and Doctrine Command and activated at the Presidio of Monterey, California.

Campaign Participation Credit

Armed Forces Expeditions

Panama

Decorations

Army Superior Unit Award, Streamer embroidered 1988–1989 (29th Military Intelligence Battalion cited; DA GO 8, 1991)

260th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a double-warded key palewise wards to base argent, between two sphinx heads addorsed or, overall a quill and a dagger saltirewise of the second.

Crest: That for the regiments and separate battalions of the Florida Army National Guard: On a wreath of the colors, argent and azure, an alligator statant proper.

Motto: INTELLIGENTIA ET VERITAS (INTELLIGENCE AND TRUTH).

Symbolism: Oriental blue and silver gray (white) are the colors traditionally associated with military intelligence. The key is emblematic of knowledge, authority, and security. The quill over the dagger underscores the pen as mightier than the sword. The sphinx heads, one facing in either direction, signify constant vigilance and eternal watchfulness.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

ARNG
(Florida)

LINEAGE

Organized and federally recognized 27 August 1990 in the Florida Army National Guard as the 260th Military Intelligence Battalion with Headquarters at Miami.

Home Area: Southern Florida.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

297th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Per bend azure and sable, in dexter base a gauntlet argent grasping a lightning flash sword bendwise blade of the like, grip gules, pommel and quillon or.

Crest: None approved.

Motto: VANGUARD.

Symbolism: The colors oriental blue and silver gray are traditionally associated with military intelligence. The armored fist represents strength; the lightning flash denotes speed. The fist seizes the blade of the sword to indicate readiness and vigilance. Black denotes dependability and suggests covert capabilities. The fist, upraised and grasping the sword, suggests leadership, highlighting the unit's motto.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

RA

Lineage (active)

Constituted 21 November 1962 in the Army Reserve as the 297th Army Security Agency Company. Activated 1 March 1963 at Atlanta, Georgia. Reorganized and redesignated 15 April 1966 as Headquarters and Headquarters Company, 297th Army Security Agency Battalion. Inactivated 31 January 1968 at Atlanta, Georgia.

Redesignated 1 February 1990 as Headquarters and Headquarters Company, 297th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Redesignated 17 October 1991 as Headquarters, Headquarters and Service Company, 297th Military Intelligence Battalion, and activated at Fort Monmouth, New Jersey (organic elements concurrently constituted and activated).

Campaign Participation Credit

None.

Decorations

None.

301st MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, a dagger and lightning flash dagger saltirewise, blades argent, hilts or and sable.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: THE FORCE MULTIPLIER.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence. The crossed dagger and lightning flash dagger form an X, suggesting the unit's motto. They symbolize strength, danger, speed, and the precise application of electronic warfare and intelligence to defeat the enemy.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

AR

Lineage (active)

Constituted 6 June 1949 in the Organized Reserve Corps as Headquarters, 301st Military Intelligence Platoon. Activated 22 June 1949 at Austin, Texas.

Reorganized and redesignated 1 September 1950 as Headquarters, 301st Military Intelligence Battalion. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 23 February 1953 at Austin, Texas. Redesignated 16 September 1988 as Headquarters, Headquarters and Service Company, 301st Military Intelligence Battalion, and activated at Pasadena, Texas (organic elements concurrently constituted and activated).

Campaign Participation Credit

None.

Decorations

None.

302d MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Per fess abased argent and azure, in chief a red fox's mask proper charged on the forehead with a billet fesswise sable, and in base a key palewise between two stylized lightning flashes of the first.

Crest: On a wreath of the colors, argent and azure, a fleur-de-lis barry of ten of the second and first, the outer petals serrated, the inner charged with a bayonet or point up, and on the crosspiece of the fleur-de-lis a bar couped tenné with two barrulets argent.

Motto: LOYALTY, VIGILANCE, PRIDE.

Symbolism: The colors, white and teal blue, are symbolic of the battalion's former status as an unassigned-to-branch unit. The battalion's war service as a signal unit is shown by the colors of the fox's mask and background, while the intelligence functions of the unit are represented by the black censor's stamp. The key is for the unit's first campaign (Normandy) in World War II and also alludes to signal and intelligence functions. The stylized lightning flashes symbolize radio reconnaissance.

The fleur-de-lis represents campaign participation in Europe. The outer petals of the fleur-de-lis, suggestive of electronic flashes, reflect the unit's service in communication reconnaissance. The bar on the crosspiece is divided into five segments representing participation in five campaigns in Europe during World War II. The bayonet suggests the Army's offensive spirit and reflects the unit's association with United States Army, Europe.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

RA

Lineage (active)

Organized 1 April 1944 in England as the 3252d Signal Service Company. (Constituted 12 April 1944 in the Army of the United States.) Inactivated 24 November 1945 at Camp Kilmer, New Jersey. Redesignated 6 May 1948 as the 533d Signal Service Company. Activated 20 June 1948 in Austria. Inactivated 1 April 1949 in Austria.

Converted and redesignated 13 October 1950 as Headquarters and Headquarters Detachment, 302d Communication Reconnaissance Battalion, and allotted to the Regular Army. Activated 20 October 1950 at Camp Pickett, Virginia. Reorganized and redesignated 25 June 1955 as Headquarters and Headquarters Company, 302d Communication Reconnaissance Battalion (Companies A and B constituted 19 May 1955; Company A activated 25 June 1955 in Germany). Redesignated 1 July 1956 as the 302d Army Security Agency Battalion. Inactivated 15 October 1957 in Germany. Headquarters and Headquarters Company activated 21 December 1975 in Germany (Companies A and B concurrently disbanded).

Headquarters and Headquarters Company, 302d Army Security Agency Battalion, reorganized and redesignated 16 April 1984 as Headquarters, Headquarters and Service Company, 302d Military Intelligence Battalion (331st Army Security Agency Company [see ANNEX 1] and 327th Army Security Agency Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B).

ANNEX 1

Constituted 26 April 1942 in the Army of the United States as the 114th Signal Radio Intelligence Company. Activated 13 July 1942 at Camp Crowder, Missouri. Reorganized and redesignated 10 January 1946 as the 114th Signal Service Company.

Converted and redesignated 25 October 1951 as the 331st Communication Reconnaissance Company and allotted to the Regular Army. Reorganized and redesignated 25 June 1955 as Company A, 307th Communication Reconnaissance Battalion. Redesignated 1 July 1956 as Company A, 307th Army Security Agency Battalion. Inactivated 15 October 1957 in Germany. Redesignated 21 September 1978 as the 331st Army Security Agency Company and activated in Germany.

ANNEX 2

Constituted 4 November 1942 in the Army of the United States as the 111th Signal Radio Intelligence Company. Activated 30 November 1942 at Camp Crowder, Missouri. Reorganized and redesignated 1 September 1945 as the 111th Signal Service Company.

Converted and redesignated 25 October 1951 as the 327th Communication Reconnaissance Company and allotted to the Regular Army. Inactivated 15 August 1956 on Formosa. Redesignated 21 October 1976 as the 327th Army Security Agency Company and activated in Germany.

CAMPAIGN PARTICIPATION CREDIT

World War II
- Normandy
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

Company B additionally entitled to:

World War II–AP
- New Guinea
- Leyte
- Luzon

DECORATIONS

Company B entitled to:

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (111th Signal Radio Intelligence Company cited; DA GO 47, 1950)

303d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Or, three piles, one in chief and two conjoined in base azure bearing in chief an edelweiss argent seeded of the field and issuing from base two beacons of the last enflamed tenné and gold.

Crest: On a wreath of the colors, or and azure, in front of a stylized wreath of rice or, four flashes saltirewise gules.

Motto: PRIMI NOSCERE (FIRST TO KNOW).

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence. The blue piles represent the mountains of Central Europe and Korea, where the battalion's predecessor units served. The edelweiss, a small white flower prized by European mountaineers, refers to the unit's service in Central Europe. The two beacons refer to Korea's ancient and effective system of communications, which was accomplished by means of beacon fires on mountain tops, and also refer to the battalion's two unit decorations for service in Korea.

The colors red and yellow are traditionally associated with Vietnam, as is the rice wreath, a symbol of excellence and achievement. The red flashes refer to the Meritorious Unit Commendations (Army) earned while serving in Vietnam and also represent accuracy and speed.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 22 September 1950 in the Regular Army as Headquarters and Headquarters Detachment, 303d Communication Reconnaissance Battalion. Activated 25 September 1950 at Arlington Hall Station, Virginia. Consolidated 17 July 1951 with the 540th Signal Service Company (see ANNEX 1) and consolidated unit designated as Headquarters and Headquarters Detachment, 303d Communication Reconnaissance Battalion. Inactivated 25 June 1955 in Korea. Redesignated 11 May 1962 as Headquarters and Headquarters Company, 303d Army Security Agency Battalion (organic elements concurrently constituted).

Battalion activated 15 June 1962 at Camp Wolters, Texas. (Companies A, B, and C reorganized and redesignated 15 October 1966 as the 372d, 373d, and 374th Army Security Agency Companies—hereafter separate lineages.)

Headquarters and Headquarters Company, 303d Army Security Agency Battalion, reorganized and redesignated 21 April 1978 as Headquarters and Headquarters Detachment, 303d Military Intelligence Battalion (376th Army Security Agency Company [see ANNEX 2] and 370th Army Security Agency Company [see ANNEX 3] concurrently reorganized and redesignated as Companies A and B).

ANNEX 1

Constituted 12 April 1944 in the Army of the United States as the 3253d Signal Service Company. Activated 25 April 1944 in England. Inactivated 25 January 1946 at Camp Kilmer, New Jersey. Redesignated 6 May 1948 as the 540th Signal Service Company. Activated 20 June 1948 in Austria. Inactivated 1 April 1949 in Austria.

ANNEX 2

Constituted 20 February 1968 in the Regular Army as the 376th Army Security Agency Company. Activated 1 April 1968 at Fort Bragg, North Carolina. Inactivated 30 June 1974 at Fort Bragg, North Carolina. Activated 1 July 1974 at Fort George G. Meade, Maryland.

ANNEX 3

Constituted 10 January 1967 in the Regular Army as the 370th Army Security Agency Company. Activated 1 March 1967 at Vint Hill Farms Station, Virginia.

CAMPAIGN PARTICIPATION CREDIT

World War II
- Normandy
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

Korean War
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

Vietnam
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (Headquarters and Headquarters Detachment, 303d Communication Reconnaissance Battalion, cited; DA GO 22, 1954)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (Headquarters and Headquarters Company, 303d Radio Research Battalion, cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (Headquarters and Headquarters Company, 303d Radio Research Battalion, cited; DA GO 28, 1969, as amended by DA GO 18, 1979)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (Headquarters and Headquarters Company, 303d Radio Research Battalion, cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (303d Radio Research Battalion cited; DA GO 43, 1972)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971 (303d Radio Research Battalion cited; DA GO 32, 1973)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA (Headquarters and Headquarters Detachment, 303d Communication Reconnaissance Battalion, cited; DA GO 33, 1953, as amended by DA GO 41, 1955)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (303d Radio Research Battalion cited; DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1969–1970 (303d Radio Research Battalion cited; DA GO 6, 1974)

304th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a voided isosceles triangle point up sable enclosing a vine leaf or and surmounted in chief by a lozenge fesswise argent bearing a Korean taeguk all between two lightning flashes, points up gules, fimbriated or.

Crest: On a wreath of the colors, or and azure, a demi-griffin of the last armed and langued gules grasping in dexter claw a dagger or, all within a laurel wreath of the like.

Motto: HONOR VIGILANCE DUTY.

Symbolism: The diamond and taeguk simulate an eye, and the lightning flashes connote technology; together they represent the vigilance, celerity, and communication of Army Security Agency units. They also allude to the lineage and service of the organization in World War II and the Korean War. The vine leaf refers to the Rhine province and denotes the unit's participation in the Rhineland campaign. The taeguk represents Korea, where the unit participated in six campaigns. It is also used to symbolize the award of the Meritorious Unit Commendation (Army) Streamer inscribed KOREA. Black is used on the triangle to connote iron and refers to the Republic of Korea Presidential Unit Citation Streamer with the inscription IRON TRIANGLE.

Oriental blue represents the military intelligence branch. The griffin, a traditional symbol of intelligence, resourcefulness, and courage, emphasizes the qualities required of battalion personnel and recalls the European theater of operations. Its claws and tongue are scarlet, denoting courage and sacrifice. It holds a dagger, a reference to the dangers of covert activities and a symbol of preparedness. The wreath refers to all honors and achievements associated with the unit during its history. Gold signifies excellence.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia consists of elements of the coat of arms.

Lineage and Honors

RA
Lineage (active)

Constituted 15 April 1944 in the Army of the United States as the 590th Signal Depot Company. Activated 7 June 1944 in North Africa. Inactivated 4 December 1945 at Camp Patrick Henry, Virginia. Redesignated 17 March 1948 as the 848th Signal Radio Relay Company and allotted to the Organized Reserves. (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps; redesignated 9 July 1952 as the Army Reserve.) Activated 2 April 1948 at Rochester, New York. Inactivated 10 November 1948 at Rochester, New York. Redesignated 11 February 1949 as the 848th Signal Service Company. Activated 10 March 1949 at Fort Myer, Virginia. Ordered into active military service 11 September 1950 at Fort Myer, Virginia.

Converted and redesignated 2 October 1950 as Headquarters and Headquarters Detachment, 304th Communication Reconnaissance Battalion. Released from active military service 25 June 1955 and reverted to reserve status. Inactivated 18 August 1955 at Fort Myer, Virginia. Redesignated 1 April 1975 as Headquarters and Headquarters Company, 304th Army Security Agency Battalion, and activated at Houston, Texas. Location changed 27 October 1976 to Pasadena, Texas. Inactivated 15 September 1988 at Pasadena, Texas.

Redesignated 1 February 1990 as Headquarters and Headquarters Company, 304th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Headquarters transferred 17 August 1990 to the United States Army Training and Doctrine Command and activated at Fort Huachuca, Arizona.

Campaign Participation Credit

World War II
- Rhineland

Korean War
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

Decorations

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (Headquarters and Headquarters Detachment, 304th Communication Reconnaissance Battalion, cited; DA GO 22, 1954)

Army Superior Unit Award, Streamer embroidered 1990–1991 (304th Military Intelligence Battalion cited; DA GO 6, 1992)

Republic of Korea Presidential Unit Citation, Streamer embroidered IRON TRIANGLE (304th Communication Reconnaissance Battalion cited; DA GO 29, 1954, as amended by DA GO 47, 1954)

305th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, a saltire argent charged with pyrotechnic projectors of the first, overall a mullet of four points tenné fimbriated of the second.

Crest: On a wreath of the colors, argent and azure, issuant from the battlements of a tower proper a fleur-de-lis or between two griffin heads respectant gules beaked or.

Motto: AD ARCANA TUTANDA (TO KEEP OFFICIAL SECRETS SAFE).

Symbolism: Teal blue and white are the colors associated with former Army Security Agency battalions. The pyrotechnic projectors allude to the signal and reconnaissance missions of the unit. The four-pointed star refers to four World War II campaigns and also symbolizes intelligence, reconnaissance, communications, and signal, all vital functions of the battalion. The color orange further alludes to its signal function. The saltire is symbolic of the southern states that made up the Third Army area, the former location of the battalion.

The tower symbolizes a strong defense and military preparedness. The griffins, personifying vigilance, stand prepared to meet all threats. Red denotes courage and zeal. The tower and fleur-de-lis commemorate the unit's World War II service in Europe.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA
LINEAGE (active)

Constituted 17 November 1950 in the Organized Reserve Corps as Headquarters and Headquarters Detachment, 305th Communication Reconnaissance Battalion. Activated 23 January 1951 at Atlanta, Georgia. Consolidated 17 July 1951 with the 3255th Signal Service Company (see ANNEX) and consolidated unit designated as Headquarters and Headquarters Detachment, 305th Communication Reconnaissance Battalion. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Reorganized and redesignated 24 January 1956 as Headquarters and Headquarters Company, 305th Communication Reconnaissance Battalion (362d Communication Reconnaissance Company [constituted 18 November 1955 in the Army Reserve] concurrently redesignated as Company A and activated at Wilmington, North Carolina). Redesignated 1 October 1956 as the 305th Army Security Agency Battalion. Inactivated 15 June 1959 at Atlanta, Georgia.

Redesignated 1 February 1990 as the 305th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Headquarters transferred 18 May 1990 to the United States Army Training and Doctrine Command and activated at Fort Devens, Massachusetts.

ANNEX

Constituted 12 April 1944 in the Army of the United States as the 3255th Signal Service Company. Activated 6 May 1944 in England. Inactivated 25 October 1945 in Germany.

CAMPAIGN PARTICIPATION CREDIT

World War II
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

DECORATIONS

None.

306th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a volcano abased argent surmounted by a pellet charged with a mullet of the second; in chief a lightning flash fesswise tenné fimbriated of the second.

Crest: On a wreath of the colors, argent and azure, a demi-griffin gules holding in its dexter claw a sword with blade in the form of a lightning flash or all in front of a wreath of palm fronds proper.

Motto: NEMO VIGILANTIOR (NO ONE MORE WATCHFUL).

Symbolism: Teal blue and white are the colors formerly used for Army Security Agency battalions. The volcano symbolizes the area in the Pacific where the unit served. The black sphere charged with a white mullet alludes to the coat of arms of Captain Cook, who discovered New Caledonia, the island on which the unit was activated. The lightning flash refers to the mission of the unit and the orange color represents its former status as a signal company.

The griffin, symbol of courage, strength, and vigilance, represents the intelligence mission of the battalion. The unit's origin as a signal company is recalled by the lightning flash sword blade, which also denotes speed of response and action. The palm wreath refers to the unit's service in the Pacific during World War II. Red signifies courage and recalls the award of the Meritorious Unit Commendation (Army). Gold stands for excellence.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA
LINEAGE (active)

Constituted 16 December 1944 in the Army of the United States as the 3910th Signal Service Company. Activated 1 February 1945 on New Caledonia. Inactivated 19 April 1946 on Tinian. Redesignated 13 January 1948 as the 303d Signal Service Company, Army, and allotted to the Organized Reserves. Activated 23 January 1948 at Philadelphia, Pennsylvania. (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps; redesignated 9 July 1952 as the Army Reserve.) Reorganized and redesignated 5 September 1950 as the 303d Signal Radio Intelligence Company.

Converted and redesignated 3 January 1951 as Headquarters and Headquarters Detachment, 306th Communication Reconnaissance Battalion. Ordered into active military service 1 May 1951 at Philadelphia, Pennsylvania; released from active military service 16 May 1955 and reverted to reserve status. Inactivated 20 July 1955 at Philadelphia, Pennsylvania. Activated 6 January 1956 at Philadelphia, Pennsylvania. Reorganized and redesignated 14 February 1956 as Headquarters and Headquarters Company, 306th Communication Reconnaissance Battalion. (Companies A and B constituted 13 March 1956; Company B activated 14 March 1956 at Baltimore, Maryland.) Redesignated 3 September 1956 as the 306th Army Security Agency Battalion. Inactivated 27 June 1959 at Philadelphia, Pennsylvania.

Redesignated 1 February 1990 as the 306th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Headquarters transferred 18 May 1990 to the United States Army Training and Doctrine Command and activated at Fort Devens, Massachusetts.

CAMPAIGN PARTICIPATION CREDIT

World War II

Asiatic-Pacific Theater, Streamer without inscription

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered PACIFIC THEATER (3910th Signal Service Company cited; GO 133, Western Pacific Base Command, 11 November 1945)

307th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Tierced in pairle reversed argent, azure, and gules, on the first and second an eagle's head erased counterchanged, and on the third, a key palewise, the ward to base, between two electronic flashes, one in bend and the other in bendsinister of the first.

Crest: On a wreath of the colors, argent and azure, in front of a wreath of laurel or an equilateral triangle point up with the points barbed gules and charged with a Philippine sun of the third.

Motto: ELECTRONIC FIREPOWER.

Symbolism: The eagles, known for swiftness, stamina, and keen vision, together with the key and electronic flashes symbolize eternal vigilance and security. All allude to the basic mission of the organization. In addition, the eagles' heads, adapted from the civic arms of the cities of Frankfurt am Main and Ludwigsburg in Germany, refer to former stations of the battalion.

The crest symbolizes unit awards received by elements of the battalion. The wreath of laurel refers to the eight Meritorious Unit Commendations (Army) for service in the Pacific during World War II, in Korea, and in Vietnam, and to the Republic of Vietnam Cross of Gallantry with Palm. The triangle and sun symbolize the Philippine Presidential Unit Citation.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 11 December 1951 in the Regular Army as Headquarters and Headquarters Detachment, 307th Communication Reconnaissance Battalion. Activated 27 December 1951 in Germany. Reorganized and redesignated 25 June 1955 as Headquarters and Headquarters Company, 307th Communication Reconnaissance Battalion (331st Communication Reconnaissance Company [activated 13 July 1942] concurrently reorganized and redesignated as Company A; Company B [constituted 19 May 1955] activated in Germany). Redesignated 1 July 1956 as the 307th Army Security Agency Battalion. Inactivated 15 October 1957 in Germany. Headquarters and Headquarters Company activated 1 July 1974 in Germany. (Companies A and B redesignated 21 September 1978 as the 331st and 346th Army Security Agency Companies—hereafter separate lineages.)

Headquarters and Headquarters Company, 307th Army Security Agency Battalion, reorganized and redesignated 16 October 1983 as Headquarters, Headquarters and Service Company, 307th Military Intelligence Battalion (326th Army Security Agency Company [see ANNEX 1] concurrently reorganized and redesignated as Company A; 330th Army Security Agency Company [see ANNEX 2] redesignated as Company B and activated in Germany). Battalion inactivated 15 December 1991 in Germany.

ANNEX 1

Constituted 3 April 1942 in the Army of the United States as the 126th Signal Radio Intelligence Company. Activated 14 August 1942 at Camp Crowder, Missouri. Reorganized and redesignated 1 September 1945 as the 126th Signal Service Company.

Converted and redesignated 25 October 1951 as the 326th Communication Reconnaissance Company and allotted to the Regular Army. Redesignated 1 July 1956 as the 326th Army Security Agency Company. Inactivated 15 October 1957 in Japan. Activated 25 May 1962 at Fort Bragg, North Carolina. Inactivated 14 February 1964 at Homestead Air Force Base, Florida. Activated 23 December 1968 at Fort Riley, Kansas. Inactivated 15 April 1970 at Fort Riley, Kansas. Activated 3 May 1971 in Germany.

ANNEX 2

Constituted 26 November 1943 in the Army of the United States as the 60th Signal Radio Intelligence Company. Activated 23 December 1943 at Camp Crowder, Missouri. Reorganized and redesignated 24 May 1945 as the 60th Signal Service Company.

Converted and redesignated 25 October 1951 as the 330th Communication Reconnaissance Company and allotted to the Regular Army. Redesignated 1 July 1956 as the 330th Army Security Agency Company. Inactivated 15 October 1957

in Korea. Activated 25 June 1962 at Camp Wolters, Texas. Inactivated 30 September 1971 in Vietnam. Activated 5 November 1973 in Germany. Inactivated 15 May 1979 in Germany.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait
- Cease-Fire

Company A additionally entitled to:

World War II–AP
- New Guinea
- Luzon

Korean War
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

Company B additionally entitled to:

Korean War
- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

Vietnam
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII
- Consolidation I

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (307th Military Intelligence Battalion cited; DA GO 34, 1992)

Company A additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered PACIFIC THEATER (126th Signal Radio Intelligence Company cited; GO 166, United States Army Forces, Pacific, 14 September 1945)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (326th Communication Reconnaissance Company cited; DA GO 22, 1954)

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (126th Signal Radio Intelligence Company cited; DA GO 47, 1950)

Company B additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1950–1951 (330th Communication Reconnaissance Company cited; DA GO 62, 1952)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1951–1953 (330th Communication Reconnaissance Company cited; DA GO 22, 1954)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (330th Radio Research Company cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (330th Radio Research Company cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (330th Radio Research Company cited; DA GO 43, 1972)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971 (330th Radio Research Company cited; DA GO 32, 1973)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (330th Radio Research Company cited; DA GO 6, 1974)

309th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent, on a pale emitting in saltire four lightning flashes azure a key ward to dexter in base, the bow a bear's head, or.

Crest: None approved.

Motto: SENTINELS OF SECURITY.

Symbolism: Teal blue and white are the colors formerly used for Army Security Agency organizations. The key symbolizes the unit's mission, the guarding of security, and the golden bear's head on the key represents the state of California, where the unit was originally activated. The lightning flashes, symbolic of electricity, relate to the importance of electronic communications as part of the unit's functions.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

RA

Lineage (inactive)

Constituted 31 January 1952 in the Organized Reserve Corps as Headquarters and Headquarters Detachment, 308th Communication Reconnaissance Battalion. Activated 1 April 1952 at New York, New York. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Reorganized and redesignated 23 January 1956 as Headquarters and Headquarters Company, 308th Communication Reconnaissance Battalion. Redesignated 1 September 1956 as Headquarters and Headquarters Company, 308th Army Security Agency Battalion. Inactivated 1 July 1959 at New York, New York.

Redesignated 1 February 1990 as Headquarters and Headquarters Company, 308th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Redesignated 17 October 1991 as Headquarters, Headquarters and Service Company, 308th Military Intelligence Battalion, and activated in Panama (organic elements concurrently constituted and activated). Battalion inactivated 16 September 1995 in Panama.

Campaign Participation Credit

None.

Decorations

Army Superior Unit Award, Streamer embroidered 1993–1994 (308th Military Intelligence Battalion cited; DA GO 1, 1996)

308th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per saltire argent and azure, two griffin heads erased respectant of the first, in chief a compass rose gules.

Crest: None approved.

Motto: GUARDIANS OF AMERICA.

Symbolism: Oriental blue is the primary color associated with military intelligence. The saltire represents strength and cooperation. The griffins embody vigilance, alertness, and courage and reflect the unit's motto and mission. The compass rose alludes to the collection, analysis, and dissemination of information and the worldwide capabilities of the unit.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is an adaptation of the shield of the coat of arms and incorporates the motto.

Lineage and Honors

RA

Lineage (active)

Constituted 19 September 1952 in the Army Reserve as Headquarters and Headquarters Detachment, 309th Communication Reconnaissance Battalion. Activated 1 November 1952 at Los Angeles, California. Reorganized and redesignated 25 January 1956 as Headquarters and Headquarters Company, 309th Communication Reconnaissance Battalion (organic elements constituted 29 December 1955–4 March 1956 and activated 1 February–5 March 1956). Redesignated 1 October 1956 as the 309th Army Security Agency Battalion. Inactivated 15 July 1959 at Los Angeles, California. Activated 15 September 1962 with Headquarters at Bell, California. (Companies A, B, C, and D reorganized and redesignated 15 August 1966 as the 518th, 519th, 520th, and 521st Army Security Agency Companies—hereafter separate lineages.) Headquarters and Headquarters Company inactivated 15 July 1986 at Bell, California.

Redesignated 1 February 1990 as Headquarters and Headquarters Company, 309th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Headquarters transferred 17 August 1990 to the United States Army Training and Doctrine Command and activated at Fort Huachuca, Arizona.

Campaign Participation Credit

None.

Decorations

None.

310th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, two cramps saltirewise argent surmounted by a griffin's head erased sable, langued gules.

Crest: None approved.

Motto: ARRECTIS AURIBUS (ALWAYS ON THE ALERT).

Symbolism: Oriental blue is one of the colors associated with military intelligence. Black and white symbolize overt and covert operations and the organization's around-the-clock vigilance. The griffin embodies alertness; it is black, recalling determination and stealth. The unit's collection and exploitation mission is highlighted by the cramps or hooks. The hooks simulate flashes, representing speed and combat electronic warfare, while alluding to the ability to catch and hold.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 25 February 1954 in the Army Reserve as Headquarters and Headquarters Detachment, 310th Communication Reconnaissance Battalion. Activated 1 November 1954 at Boston, Massachusetts. Reorganized and redesignated 8 February 1956 as Headquarters and Headquarters Company, 310th Communication Reconnaissance Battalion. Redesignated 10 September 1956 as Headquarters and Headquarters Company, 310th Army Security Agency Battalion. (800th Signal Company [see ANNEX] converted and redesignated 26 July 1956 as Company A.) Battalion inactivated 1 July 1959 at Boston, Massachusetts.

Redesignated 1 February 1990 as the 310th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Activated 17 October 1991 in Panama. Inactivated 16 September 1995 in Panama.

ANNEX

Constituted 24 December 1943 in the Army of the United States as the 5th Mobile Radio Broadcasting Company. Activated 28 January 1944 at Camp Ritchie, Maryland. Inactivated 25 November 1945 in Germany.

Redesignated 14 September 1948 as the 800th Mobile Radio Broadcasting Company and allotted to the Organized Reserve Corps. Activated 27 September 1948 at Corpus Christi, Texas. Inactivated 20 September 1950 at Corpus Christi, Texas. Converted and redesignated 8 November 1950 as the 800th Signal Radio Countermeasure Company. Activated 7 December 1950 at Red Bank, New Jersey. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Reorganized and redesignated 20 March 1953 as the 800th Signal Company. Location changed 17 August 1954 to Fort Monmouth, New Jersey.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

World War II–EAME
Ardennes-Alsace

DECORATIONS

None.

311th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a cross quarter-pierced argent and overall two lightning bolts in saltire or between in each quarter as many fleurs-de-lis of the second; overall a dragon passant gules.

Crest: None approved.

Motto: EYES OF THE EAGLE.

Symbolism: The checkered field in the colors used for military intelligence units, silver gray (white) and oriental blue, suggests the gathering of data to aid in the formulation of military strategy; the lightning bolts refer to the use of electronics in the gathering operation. The dragon is a reference to service in Vietnam and its scarlet color alludes to awards of the Meritorious Unit Commendation (Army). The fleur-de-lis denote service in Europe during World War II.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 1 June 1954 in the Regular Army as Headquarters and Headquarters Detachment, 311th Communication Reconnaissance Battalion. Activated 14 June 1954 at Fort Devens, Massachusetts. Reorganized and redesignated 16 May 1955 as Headquarters and Headquarters Company, 311th Communication Reconnaissance Battalion (336th Communication Reconnaissance Company [activated 6 August 1952] and 359th Communication Reconnaissance Company [activated 15 August 1944] concurrently reorganized and redesignated as Companies A and B). Redesignated 1 July 1956 as the 311th Army Security Agency Battalion. Inactivated 18 December 1957 at Camp Wolters, Texas. Headquarters and Headquarters Company activated 15 February 1966 at Fort Wolters, Texas (Companies A and B concurrently disbanded). Inactivated 30 June 1971 at Fort Hood, Texas. (Companies A and B reconstituted 21 September 1978 in the Regular Army as the 336th and 359th Army Security Agency Companies—hereafter separate lineages.)

Headquarters and Headquarters Company, 311th Army Security Agency Battalion, redesignated 1 June 1982 as Headquarters, Headquarters and

Operations Company, 311th Military Intelligence Battalion, assigned to the 101st Airborne Division, and activated at Fort Campbell, Kentucky (265th Army Security Agency Company [see ANNEX 1] and 101st Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B).

ANNEX 1

Constituted 2 March 1967 in the Regular Army as the 265th Army Security Agency Company. Activated 21 April 1967 at Fort Campbell, Kentucky. Inactivated 1 April 1972 in Vietnam. Activated 21 June 1976 at Fort Campbell, Kentucky.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 101st Counter Intelligence Corps Detachment. Activated 20 August 1944 in England with personnel from provisional Counter Intelligence Corps detachment attached to the 101st Airborne Division. Inactivated 30 November 1945 in France. Allotted 7 February 1956 to the Regular Army. Activated 25 March 1956 at Fort Campbell, Kentucky. Reorganized and redesignated 25 January 1958 as the 101st Military Intelligence Detachment. Reorganized and redesignated 26 December 1969 as the 101st Military Intelligence Company. Assigned 21 September 1978 to the 101st Airborne Division.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia

Defense of Saudi Arabia
Liberation and Defense of Kuwait

Company A additionally entitled to:

Vietnam

Counteroffensive, Phase III
Tet Counteroffensive
Counteroffensive, Phase IV
Counteroffensive, Phase V
Counteroffensive, Phase VI
Tet 69/Counteroffensive
Summer-Fall 1969
Winter-Spring 1970
Sanctuary Counteroffensive
Counteroffensive, Phase VII
Consolidation I
Consolidation II
Cease-Fire

Company B additionally entitled to:

World War II–EAME

Normandy (with arrowhead)
Rhineland (with arrowhead)
Ardennes-Alsace
Central Europe

Vietnam

Counteroffensive, Phase III
Tet Counteroffensive
Counteroffensive, Phase IV
Counteroffensive, Phase V
Counteroffensive, Phase VI
Tet 69/Counteroffensive
Summer-Fall 1969
Winter-Spring 1970
Sanctuary Counteroffensive
Counteroffensive, Phase VII
Consolidation I
Consolidation II

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (Headquarters, Headquarters and Operations Company and Company A, 311th Military Intelligence Battalion, cited; DA GO 1, 1996)

Company A additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (265th Radio Research Company cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (265th Radio Research Company cited; DA GO 43, 1972)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971–1972 (265th Radio Research Company cited; DA GO 32, 1973)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1968 (265th Radio Research Company cited; DA GO 21, 1969)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1968–1969 (265th Radio Research Company cited; DA GO 43, 1970)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (265th Radio Research Company cited; DA GO 6, 1974)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1971 (265th Radio Research Company cited; DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1968–1970 (265th Radio Research Company cited; DA GO 48, 1971)

Company B additionally entitled to:

Presidential Unit Citation (Army), Streamer embroidered BASTOGNE (Counterintelligence Detachment, 101st Airborne Division, cited; WD GO 17, 1945)

French Croix de Guerre with Palm, World War II, Streamer embroidered NORMANDY (101st Airborne Division cited; DA GO 43, 1950)

Netherlands Orange Lanyard (101st Airborne Division cited; DA GO 43, 1950)

Belgian Croix de Guerre 1940 with Palm, Streamer embroidered BASTOGNE; cited in the Order of the Day of the Belgian Army for action at Bastogne (101st Counter Intelligence Corps Detachment cited; DA GO 43, 1950, as amended by DA GO 27, 1959)

Belgian Fourragere 1940 (101st Counter Intelligence Corps Detachment cited; DA GO 43, 1950, as amended by DA GO 27, 1959)

Cited in the Order of the Day of the Belgian Army for action in France and Belgium (101st Counter Intelligence Corps Detachment cited; DA GO 43, 1950, as amended by DA GO 27, 1959)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1968–1969 (101st Military Intelligence Detachment cited; DA GO 43, 1970)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1971 (101st Military Intelligence Detachment cited; DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1968–1970 (101st Military Intelligence Detachment cited; DA GO 48, 1971)

312th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent, on a taeguk proper an enflamed torch palewise in front of two lightning flashes saltirewise of the first, on a chief wavy azure a chess knight argent.

Crest: None approved.

Motto: SEMPER VERITAS (ALWAYS THE TRUTH).

Symbolism: Oriental blue and silver gray (white) are the colors traditionally associated with military intelligence. The wavy partition alludes to service in the Pacific during World War II; the taeguk to service in Korea. The crossed flashes refer to the unit's origin as signal and its present combat electronic warfare and intelligence function. The torch is a symbol of truth and reflects the motto and the mission of the unit. The chess knight, a piece that can move covertly, further symbolizes the military intelligence mission.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 31 December 1943 in the Army of the United States as the 23d Signal Construction Battalion. Activated 10 February 1944 at Camp Pickett, Virginia. Reorganized and redesignated 24 April 1944 as the 23d Signal Light Construction Battalion. Reorganized and redesignated 21 August 1944 as the 23d Signal Heavy Construction Battalion. Inactivated 22 January 1946 at Fort Lawton, Washington. Redesignated 27 September 1951 as the 23d Signal Construction Battalion and allotted to the Regular Army. Activated 2 November 1951 in Korea. Inactivated 15 May 1953 in Korea.

Converted and redesignated 19 May 1955 as the 312th Communication Reconnaissance Battalion. Headquarters and Headquarters Company activated 25 June 1955 in Germany. Battalion redesignated 1 July 1956 as the 312th Army Security Agency Battalion. Headquarters and Headquarters Company inactivated 15 October 1957 in Germany.

312th Army Security Agency Battalion redesignated 1 October 1981 as the 312th Military Intelligence Battalion, assigned to the 1st Cavalry Division, and

activated at Fort Hood, Texas (371st Army Security Agency Company [see ANNEX 1] concurrently consolidated with Company A; 191st Military Intelligence Company [see ANNEX 2] consolidated with Company B).

ANNEX 1

Constituted 11 May 1962 in the Regular Army as Company C, 313th Army Security Agency Battalion. Activated 25 May 1962 at Two Rock Ranch Station, California. Reorganized and redesignated 15 October 1966 as the 371st Army Security Agency Company.

ANNEX 2

Constituted 25 September 1950 in the Regular Army as the 191st Counter Intelligence Corps Detachment. Activated 6 October 1950 in Korea. Inactivated 24 June 1956 in Korea. Activated 15 October 1957 in Korea. Reorganized and redesignated 15 May 1959 as the 191st Military Intelligence Detachment. Reorganized and redesignated 26 December 1969 as the 191st Military Intelligence Company. Inactivated 15 August 1972 in Vietnam. Activated 21 June 1975 at Fort Hood, Texas. Assigned 2 July 1977 to the 1st Cavalry Division.

CAMPAIGN PARTICIPATION CREDIT

World War II
- Asiatic-Pacific Theater, Streamer without inscription

Korean War
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait

Company A additionally entitled to:

Vietnam
- Defense
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

Company B additionally entitled to:

Korean War
- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive

Vietnam
- Defense
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII
- Consolidation I
- Consolidation II
- Cease-Fire

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (312th Military Intelligence Battalion cited; DA GO 27, 1994)

Company A additionally entitled to:

Presidential Unit Citation (Army), Streamer embroidered PLEIKU PROVINCE (10th Radio Research Unit cited; DA GO 40, 1967)

Presidential Unit Citation (Army), Streamer embroidered BINH THUAN PROVINCE (371st Radio Research Unit cited; DA GO 2, 1973)

Valorous Unit Award, Streamer embroidered FISH HOOK (371st Radio Research Company cited; DA GO 43, 1972)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1965–1966 (10th Radio Research Unit cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (371st Radio Research Company cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (371st Radio Research Company cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (371st Radio Research Company cited; DA GO 43, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1965–1969 (371st Radio Research Company cited; DA GO 59, 1969, as amended by DA GO 43, 1970)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1969–1970 (371st Radio Research Company cited; DA GO 42, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (371st Radio Research Company cited; DA GO 42, 1972, and DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1969–1971 (371st Radio Research Company cited; DA GO 42, 1972, and DA GO 6, 1974)

Company B additionally entitled to:

Presidential Unit Citation (Army), Streamer embroidered PLEIKU PROVINCE (191st Military Intelligence Detachment cited; DA GO 40, 1967)

Valorous Unit Award, Streamer embroidered FISH HOOK (191st Military Intelligence Company cited; DA GO 43, 1972)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (191st Counter Intelligence Corps Detachment cited; DA GO 53, 1952)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (191st Military Intelligence Detachment cited; DA GO 17, 1969)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1965–1969 (191st Military Intelligence Detachment cited; DA GO 59, 1969)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1969–1970 (191st Military Intelligence Detachment cited; DA GO 42, 1972, as amended by DA GO 11, 1973)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (191st Military Intelligence Company cited; DA GO 42, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1971–1972 (191st Military Intelligence Detachment cited; DA GO 54, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1969–1970 (191st Military Intelligence Company cited; DA GO 42, 1972)

313th MILITARY INTELLIGENCE BATTALION (Snow Owl)

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a fess checky argent and tenné, overall a mullet of six points of the second.

Crest: On a wreath of the colors, argent and azure, a dragon passant gules garnished or in front of a mount vert impaled with twelve bamboo spikes proper, the dragon's tail interlaced with the spikes.

Motto: SAVOIR C'EST POUVOIR (KNOWLEDGE IS POWER).

Symbolism: Oriental blue and silver gray (white) allude to military intelligence. The colors orange and white refer to the organization's former affiliation with the Signal Corps, and the points of the mullet allude to the unit's decorations for World War II and Vietnam.

The dragon, symbolic of alertness and readiness, denotes the unit's service as an Army Security Agency battalion in Vietnam. The mount refers to the lush terrain of that country and the spikes to the number of campaigns in which the unit participated.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

RA

Lineage (active)

Constituted 11 May 1942 in the Army of the United States as the 215th Signal Depot Company. Activated 25 September 1942 at Camp Livingston, Louisiana. Inactivated 18 November 1945 at Camp Kilmer, New Jersey.

Converted and redesignated 21 April 1955 as Headquarters and Headquarters Company, 313th Communication Reconnaissance Battalion, and allotted to the Regular Army. Activated 16 May 1955 at Fort Bragg, North Carolina (358th Communication Reconnaissance Company [see ANNEX 1] and 337th Communication Reconnaissance Company [activated 6 August 1952] concurrently reorganized and redesignated as Companies A and B). Redesignated 1 July 1956 as the 313th Army Security Agency Battalion. Inactivated 18 December 1957 at Fort Bragg, North Carolina. Activated 25 May 1962 at Fort Bragg, North Carolina. (Company A reorganized and redesignated 15 October 1966 as the 358th Army Security Agency Company [see ANNEX 1]; Companies B and C concurrently reorganized and redesignated as the 337th and 371st Army Security Agency Companies—hereafter separate lineages.)

Headquarters and Headquarters Company, 313th Army Security Agency Battalion, reorganized and redesignated 16 October 1979 as Headquarters and Headquarters Company, 313th Military Intelligence Battalion, and assigned to the 82d Airborne Division (358th Army Security Agency Company [see ANNEX 1] and 82d Military Intelligence Company [see ANNEX 2] concurrently reorganized and redesignated as Companies A and B).

ANNEX 1

Constituted 10 June 1944 in the Army of the United States as the 3191st Signal Service Company. Activated 20 June 1944 at Camp Crowder, Missouri. Inactivated 25 October 1945 in the Philippine Islands.

Converted and redesignated 25 April 1951 as the 358th Communication Reconnaissance Company and allotted to the Regular Army. Activated 15 May 1951 at Fort Devens, Massachusetts. Reorganized and redesignated 16 May 1955 as Company A, 313th Communication Reconnaissance Battalion. Redesignated 1 July 1956 as Company A, 313th Army Security Agency Battalion. Inactivated 18 December 1957 at Fort Bragg, North Carolina. Activated 25 May 1962 at Fort Bragg, North Carolina. Reorganized and redesignated 15 October 1966 as the 358th Army Security Agency Company.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 82d Counter Intelligence Corps Detachment. Activated 20 August 1944 in England with personnel from provisional Counter Intelligence Corps detachment attached to the 82d Airborne Division. Allotted 3 February 1949 to the Regular Army. Reorganized and

redesignated 25 January 1958 as the 82d Military Intelligence Detachment. Reorganized and redesignated 11 November 1970 as the 82d Military Intelligence Company. Assigned 21 June 1978 to the 82d Airborne Division.

CAMPAIGN PARTICIPATION CREDIT

World War II
- Normandy (with arrowhead)
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

Vietnam
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

Armed Forces Expeditions
- Dominican Republic
- Grenada

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait

Company A additionally entitled to:

World War II–AP
- Luzon

Armed Forces Expeditions
- Panama (with arrowhead)

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered FRANCE 1944 (215th Signal Depot Company cited; GO 10, First Army, 17 January 1945)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (313th Radio Research Battalion cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (Headquarters and Headquarters Company, 313th Radio Research Battalion cited; DA GO 28, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (Headquarters and Headquarters Company, 313th Radio Research Battalion cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (313th Radio Research Battalion cited; DA GO 43, 1972)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971 (313th Radio Research Battalion cited; DA GO 32, 1973)

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (313th Military Intelligence Battalion cited; DA GO 27, 1994)

French Croix de Guerre with Palm, World War II, Streamer embroidered NORMANDY BEACHES (Detachments, 215th Signal Depot Company, cited; DA GO 43, 1950)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (313th Radio Research Battalion cited; DA GO 6, 1974)

Company A additionally entitled to:

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (3191st Signal Service Company cited; DA GO 47, 1950)

Company B additionally entitled to:

Military Order of William (Degree of the Knight of the Fourth Class), Streamer embroidered NIJMEGEN (82d Airborne Division cited; DA GO 43, 1950)

Netherlands Orange Lanyard (82d Airborne Division cited; DA GO 43, 1950)

Belgian Fourragere 1940 (82d Airborne Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in the Ardennes (82d Airborne Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in Belgium and Germany (82d Airborne Division cited; DA GO 43, 1950)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1968 (82d Military Intelligence Detachment cited; DA GO 48, 1971)

314th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent, within a cross quarter-pierced azure the device from the flag of Okinawa proper; on a chief wavy sable a dagger and a key wards up saltirewise of the first.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: SAPIENTIA ET VERITAS (WISDOM AND TRUTH).

Symbolism: Oriental blue and silver gray (white) are the colors traditionally associated with military intelligence. The red and white Okinawa symbol represents the unit's service in the Pacific. The blue and white squares simulate a chessboard and allude to strategy in gathering intelligence information. Black implies covert operations, while the silver key and sword refer to securing information for military activities. Black and white also signify day and night operations.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

AR

Lineage (active)

Constituted 14 December 1944 in the Army of the United States as the 314th Headquarters Intelligence Detachment. Activated 27 February 1945 in the Philippine Islands. Inactivated 25 March 1947 in Korea. Allotted 20 April 1948 to the Organized Reserve Corps. Activated 21 May 1948 at Boston, Massachusetts. Inactivated 30 June 1950 at Boston, Massachusetts.

Redesignated 10 August 1950 as Headquarters, 314th Military Intelligence Battalion. Activated 30 August 1950 at Cleveland, Ohio. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 1 April 1953 at Cleveland, Ohio. Redesignated 16 September 1988 as Headquarters, Headquarters and Service Company, 314th Military Intelligence Battalion, and activated at Detroit, Michigan (organic elements concurrently constituted and activated).

Campaign Participation Credit

World War II
Ryukyus

Decorations

None.

319th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per pale azure and or, a Korean temple counterchanged, a point quartered argent and sable.

Crest: None approved.

Motto: HOSTEM COGERE (CONFINE THE ENEMY).

Symbolism: Oriental blue is one of the colors used for military intelligence units; gold is symbolic of knowledge and insight. The Korean temple represents the unit's decorations and service in the Pacific area. The black and white quartered base is taken from the arms of the city of Bad Schwalbach in Germany, where the organization was activated.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 14 July 1945 in the Army of the United States as the 319th Headquarters Intelligence Detachment. Activated 1 August 1945 in Germany. Inactivated 31 October 1946 in Germany. Redesignated 20 December 1946 as the 319th Military Intelligence Company. Activated 30 December 1946 in Japan. Reorganized and redesignated 1 September 1952 as the 319th Military Intelligence Service Company and allotted to the Regular Army. Inactivated 28 March 1954 in Japan.

Redesignated 14 January 1955 as the 319th Military Intelligence Battalion. Activated 7 March 1955 at Fort George G. Meade, Maryland. Reorganized and redesignated 25 January 1958 as Headquarters and Headquarters Company, 319th Military Intelligence Battalion. (162d Military Intelligence Company [see ANNEX 1] reorganized and redesignated 13 July 1959 as Company A.) Battalion inactivated 15 February 1968 at Fort Shafter, Hawaii. Activated 1 April 1982 at Fort Bragg, North Carolina (336th Army Security Agency Company [see ANNEX 2] concurrently reorganized and redesignated as Company B).

ANNEX 1

Constituted 5 April 1945 in the Army of the United States as the 162d Language Detachment. Activated 23 April 1945 in the Philippine Islands.

Inactivated 10 February 1946 in Japan. Redesignated 14 January 1955 as the 162d Military Intelligence Platoon and allotted to the Regular Army. Activated 7 March 1955 at Fort George G. Meade, Maryland. Reorganized and redesignated 25 January 1958 as the 162d Military Intelligence Company.

ANNEX 2

Constituted 1 July 1952 in the Regular Army as the 336th Communication Reconnaissance Company. Activated 6 August 1952 at Fort Devens, Massachusetts. Reorganized and redesignated 16 May 1955 as Company A, 311th Communication Reconnaissance Battalion. Redesignated 1 July 1956 as Company A, 311th Army Security Agency Battalion. Inactivated 18 December 1957 at Camp Wolters, Texas. Disbanded 15 February 1966. Reconstituted 21 September 1978 in the Regular Army as the 336th Army Security Agency Company. Activated 16 September 1979 at Fort Bragg, North Carolina.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia
Defense of Saudi Arabia
Liberation and Defense of Kuwait

Company A additionally entitled to:

World War II–AP
Luzon
Armed Forces Expeditions
Panama

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (319th Military Intelligence Service Company cited; DA GO 22, 1954)

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (319th Military Intelligence Battalion cited; DA GO 14, 1993)

Company A additionally entitled to:

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (162d Language Detachment cited; DA GO 47, 1950)

321st MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 14 July 1945 in the Army of the United States as the 321st Headquarters Intelligence Detachment and activated in Germany. Inactivated 30 November 1946 in Germany. Allotted 12 February 1947 to the Organized Reserves. Activated 26 February 1947 at Chicago, Illinois. (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps; redesignated 9 July 1952 as the Army Reserve.) Inactivated 31 December 1948 at Chicago, Illinois. Activated 24 March 1949 at Chicago, Illinois.

Reorganized and redesignated 24 October 1950 as Headquarters, 321st Military Intelligence Battalion. Inactivated 1 March 1953 at Chicago, Illinois. Redesignated 13 February 1996 as Headquarters, Headquarters and Service Company, 321st Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

323d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR
LINEAGE (inactive)

Constituted 15 March 1968 in the Regular Army as the 19th Military Intelligence Battalion and activated in Germany. Inactivated 20 March 1969 in Germany.

Redesignated 13 February 1996 as Headquarters and Headquarters Company, 323d Military Intelligence Battalion, withdrawn from the Regular Army, and allotted to the Army Reserve (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

325th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR
(inactive)

LINEAGE

Constituted 14 July 1945 in the Army of the United States as the 325th Headquarters Intelligence Detachment and activated in Germany. Inactivated 30 November 1946 in Germany. Allotted 7 February 1947 to the Organized Reserves. Activated 24 February 1947 at Philadelphia, Pennsylvania. (Organized Reserves redesignated 25 March 1948 as the Organized Reserve Corps; redesignated 9 July 1952 as the Army Reserve.) Reorganized and redesignated 30 September 1949 as Headquarters, 325th Military Intelligence Platoon.

Reorganized and redesignated 21 June 1950 as Headquarters, 325th Military Intelligence Battalion. Inactivated 1 April 1953 at Philadelphia, Pennsylvania. Redesignated 13 February 1996 as Headquarters, Headquarters and Service Company, 325th Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

326th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per fess or and checky sable and argent on a pile in point party per fess azure and of the first an eagle's head couped of the third langued gules.

Crest: None approved.

Motto: FROM INTELLIGENCE ACTION.

Symbolism: Oriental blue is one of the colors used for military intelligence units. The eagle's head with piercing eye representing vigilance, keenness of vision, and swiftness of purpose symbolizes the attributes inherent in the basic mission of the organization. The checkered area alludes to secrecy and compartmentalized information and, together with the inverted triangle formed from the heraldic pile, is indicative of the penetrative methods in the gathering of intelligence.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and the motto of the coat of arms.

LINEAGE AND HONORS

RA
LINEAGE (active)

Constituted 24 November 1967 in the Army Reserve as the 826th Military Intelligence Battalion. Activated 31 January 1968 with Headquarters at Hartford, Connecticut. Location of Headquarters changed 11 October 1969 to Cromwell, Connecticut. (Company C ordered into active military service 24 March 1970 at Fort Hamilton, New York; released from active military service 26 March 1970 and reverted to reserve status.) (Organic elements inactivated 16 September 1980.) Location of Headquarters and Headquarters Company changed 1 September 1981 to East Windsor, Connecticut. Headquarters and Headquarters Company inactivated 15 September 1987 at East Windsor, Connecticut.

Battalion redesignated 1 November 1994 as the 326th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Headquarters transferred 1 December 1994 to the United States Army Training and Doctrine Command and activated at Fort Huachuca, Arizona.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

337th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent, four flashes issuant from dexter chief, sinister chief, dexter base, and sinister base convergent in fess point azure, a dagger point up proper, blade and pommel argent, grip gules, guard and garnish or winged sable.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: COLLECT EXPLOIT INFORM.

Symbolism: Oriental blue is one of the colors associated with military intelligence units. The flashes, alluding to speed and electronics, converge, emphasizing the collection and assimilation of information from all sources. They underscore the electronic warfare and signals intelligence capabilities of the unit. The winged dagger symbolizes the intelligence role in total military preparedness while characterizing the diverse mission and functions of the battalion.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

AR

LINEAGE (active)

Constituted 14 May 1948 in the Organized Reserve Corps as the 337th Headquarters Intelligence Detachment. Activated 2 June 1948 at New York, New York.

Reorganized and redesignated 6 July 1950 as Headquarters, 337th Military Intelligence Battalion. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 20 February 1953 at New York, New York. Redesignated 16 September 1988 as Headquarters, Headquarters and Service Company, 337th Military Intelligence Battalion, and activated at Charlotte, North Carolina (organic elements concurrently constituted and activated).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

338th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent, an oval sphere azure gridlined of the field, overall a key wards up palewise of the last superimposed by a sphinx's head or garnished sable; on a chief embattled sable two flashes saltirewise gules.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: INVENI ET USURPA (FIND AND EXPLOIT).

Symbolism: Oriental blue is one of the colors associated with military intelligence. The embattled division of the shield signifies defense and military preparedness, while black and white suggest night and day capabilities. The globe denotes the far-reaching scope of the unit's mission. The key symbolizes security; the sphinx alludes to vigilance and strength. The red flashes indicate speed and action while representing electronic communications and technology.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia consists of elements of the shield and motto of the coat of arms.

LINEAGE AND HONORS

AR

LINEAGE (active)

Constituted 14 May 1948 in the Organized Reserve Corps as the 338th Headquarters Intelligence Detachment. Activated 2 June 1948 at New York, New York. Reorganized and redesignated 6 July 1950 as Headquarters, 338th Military Intelligence Company. Ordered into active military service 11 September 1950 at New York, New York. Reorganized and redesignated 7 December 1950 as the 338th Military Intelligence Service Company.

Reorganized and redesignated 1 November 1951 as the 338th Military Intelligence Service Battalion. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Reorganized and redesignated 14 December 1953 as the 338th Military Intelligence Battalion. Released from active military service 7 March 1955 and reverted to reserve status. Inactivated 8 March 1955 at New York, New York. Redesignated 16 September 1988 as Headquarters, Headquarters and Service Company, 338th Military Intelligence Battalion, and activated at Fort George G. Meade, Maryland (organic elements concurrently constituted and activated).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

341st MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Per bend argent and azure, a lightning bolt bendwise throughout or between a stylized representation of the Rosetta Stone of the like detailed sable and an open book of the third leathered of the fourth surmounted in saltire by a quill gold and a sword point down of the last grip sable.

Crest: That for the regiments and separate battalions of the Washington Army National Guard: On a wreath of the colors, or and azure, a raven with wings endorsed issuing out of a ducal coronet all proper.

Motto: VIGILANTIA ET VALOR (VIGILANCE AND VALOR).

Symbolism: Oriental blue and silver gray are the colors traditionally associated with military intelligence. The lightning bolt denotes swiftness of action and accuracy. The Rosetta Stone indicates the unit's role as a linguist intelligence battalion. The book and quill symbolize knowledge, and the sword represents the unit's combat role.

Distinctive Unit Insignia

The distinctive unit insignia consists of elements of the shield, crest, and motto of the coat of arms.

Lineage and Honors

ARNG

Lineage (Washington)

Organized and federally recognized 2 December 1989 in the Washington Army National Guard as the 341st Military Intelligence Battalion with Headquarters at Seattle. Location of Headquarters changed 1 March 1990 to Fort Lewis; changed 1 March 1992 to Kent; changed 1 September 1993 to Poulsbo.

Home Area: Statewide.

Campaign Participation Credit

None.

Decorations

None.

344th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent on a saltire celeste a key ward up bendwise sinister surmounted by two pikes bendwise or.

Crest: None approved.

Motto: SILENT SENTINEL.

Symbolism: Oriental blue and silver gray are the colors used for military intelligence. The key, symbol for security and secrecy, and the pikes, weapons used by sentries in the Middle Ages, symbolize the basic mission of the organization.

DISTINCTIVE UNIT INSIGNIA

Description: A gold color metal and enamel device consisting of a gold key, ward slanted upward to right behind the shafts of two pikes; all encircled by a continuous oval-shaped scroll passing through the bow of the key, behind the pike heads, keyward and over the pike staffs and bearing the inscription in black letters SILENT SENTINEL.

Symbolism: The key, symbol for security and secrecy, and the pikes, weapons used by sentries in the Middle Ages, symbolize the basic mission of the organization. The shape of the bow of the key and the two pikes further simulates the numerical designation of the organization.

Lineage and Honors

RA

Lineage (active)

Constituted 5 November 1962 in the Army Reserve as the 344th Army Security Agency Company. Activated 28 February 1963 at Philadelphia, Pennsylvania. Reorganized and redesignated 15 April 1966 as Headquarters and Headquarters Company, 344th Army Security Agency Battalion. Inactivated 31 January 1968 at Philadelphia, Pennsylvania.

Redesignated 1 February 1990 as Headquarters and Headquarters Company, 344th Military Intelligence Battalion; concurrently withdrawn from the Army Reserve and allotted to the Regular Army. Headquarters transferred 25 May 1990 to the United States Army Training and Doctrine Command and activated at Goodfellow Air Force Base, Texas.

Campaign Participation Credit

None.

Decorations

Army Superior Unit Award, Streamer embroidered 1990–1991 (344th Military Intelligence Battalion cited; DA GO 34, 1992)

345th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 3 October 1950 in the Organized Reserve Corps as Headquarters, 345th Military Intelligence Battalion. Activated 24 October 1950 at Minneapolis, Minnesota. Location changed 1 May 1952 to Fort Snelling, Minnesota. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 1 March 1953 at Fort Snelling, Minnesota. Redesignated 8 August 1995 as Headquarters, Headquarters and Service Company, 345th Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

368th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 20 September 1950 in the Organized Reserve Corps as Headquarters, 368th Military Intelligence Battalion. Activated 1 October 1950 at Los Angeles, California. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 1 February 1953 at Los Angeles, California. Redesignated 8 August 1995 as Headquarters, Headquarters and Service Company, 368th Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

373d MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, a plate charged with a key ward to chief sable and a lightning flash or saltirewise upon a sunburst argent interlaced with a laurel wreath vert, overall in base a dagger, blade, hilt, and pommel or, grip gules.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: COLLECT SUPPORT DEFEND.

Symbolism: Oriental blue is one of the colors associated with military intelligence. The plate, symbolizing the earth, recalls the worldwide mission of military intelligence; the sunburst behind it is adapted from the military intelligence branch insignia. The wreath stands for honor, the key for security, and the lightning flash for speed. The dagger recalls the danger of the military intelligence mission.

Distinctive Unit Insignia

The distinctive unit insignia consists of elements of the shield and motto of the coat of arms.

372d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR
(inactive)

LINEAGE

Constituted 2 November 1950 in the Organized Reserve Corps as Headquarters, 372d Military Intelligence Battalion. Activated 15 November 1950 at Boston, Massachusetts. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 28 February 1953 at Boston, Massachusetts. Redesignated 28 March 1996 as Headquarters, Headquarters and Service Company, 372d Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

LINEAGE AND HONORS

AR

LINEAGE (active)

Constituted 1 December 1950 in the Organized Reserve Corps as Headquarters, 373d Military Intelligence Battalion. Activated 20 December 1950 at Berkeley, California. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 1 February 1953 at Berkeley, California. Redesignated 16 September 1988 as Headquarters, Headquarters and Service Company, 373d Military Intelligence Battalion, and activated at Oakland, California (organic elements concurrently constituted and activated).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

376th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 19 July 1950 in the Organized Reserve Corps as Headquarters, 376th Military Intelligence Group. Activated 1 August 1950 at Dallas, Texas. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 23 February 1953 at Dallas, Texas.

Redesignated 28 March 1996 as Headquarters, Headquarters and Service Company, 376th Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

377th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 30 August 1950 in the Organized Reserve Corps as Headquarters, 377th Military Intelligence Group. Activated 26 September 1950 at Fort Myer, Virginia. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 1 April 1953 at Fort Myer, Virginia.

Redesignated 28 March 1996 as Headquarters, Headquarters and Service Company, 377th Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

378th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 31 August 1950 in the Organized Reserve Corps as Headquarters, 378th Military Intelligence Group. Activated 3 October 1950 at Chicago, Illinois. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 1 March 1953 at Chicago, Illinois.

Redesignated 28 March 1996 as Headquarters, Headquarters and Service Company, 378th Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

383d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

None approved.

LINEAGE AND HONORS

AR

LINEAGE (inactive)

Constituted 8 February 1951 in the Organized Reserve Corps as Headquarters, 383d Military Intelligence Battalion. Activated 1 March 1951 at Newark, New Jersey. (Organized Reserve Corps redesignated 9 July 1952 as the Army Reserve.) Inactivated 28 February 1953 at Newark, New Jersey. Redesignated 28 March 1996 as Headquarters, Headquarters and Service Company, 383d Military Intelligence Battalion (organic elements concurrently constituted).

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

415th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure, a fleur-de-lis or bearing a double-warded key wards up gules; on a fess sable a tiger courant proper.

Crest: That for the regiments and separate battalions of the Louisiana Army National Guard: On a wreath of the colors, or and azure, a pelican in her piety affronté with three young in nest, argent, armed and vulned proper.

Motto: PASSE PARTOUT (PASS INTO/THROUGH EVERYWHERE).

Symbolism: Oriental blue is one of the colors associated with military intelligence organizations. The tiger represents strength, readiness, and military power. The fleur-de-lis is a symbol of Louisiana, the home state of the unit. The red key symbolizes courage and vitality in the mission of unlocking information using foreign languages.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

Lineage

ARNG
(Louisiana)

Organized and federally recognized 1 December 1989 in the Louisiana Army National Guard as the 415th Military Intelligence Battalion with Headquarters at Baton Rouge.

Home Station: Baton Rouge.

Campaign Participation Credit

None.

Decorations

None.

Lineage and Honors

RA

Lineage (active)

Constituted 13 October 1950 in the Regular Army as Headquarters and Headquarters Detachment, 301st Communication Reconnaissance Battalion. Activated 20 October 1950 at Camp Pickett, Virginia. Reorganized and redesignated 25 June 1955 as Headquarters and Headquarters Company, 301st Communication Reconnaissance Battalion (356th Communication Reconnaissance Company [activated 15 January 1946] and 329th Communication Reconnaissance Company [activated 1 November 1943] concurrently reorganized and redesignated as Companies A and B). Redesignated 1 July 1956 as the 301st Army Security Agency Battalion. Inactivated 15 October 1957 in Korea. Headquarters and Headquarters Company activated 15 December 1965 at Fort Bragg, North Carolina. Inactivated 18 June 1971 at Fort Bragg, North Carolina. (Companies A and B redesignated 1 November 1975 as the 356th and 329th Army Security Agency Companies—hereafter separate lineages.)

Headquarters and Headquarters Company, 301st Army Security Agency Battalion, redesignated 16 September 1980 as Headquarters, Headquarters and Operations Company, 501st Military Intelligence Battalion, assigned to the 1st Armored Division, and activated in Germany (202d Army Security Agency Company [see ANNEX 1] concurrently reorganized and redesignated as Company A; 501st Military Intelligence Detachment [see ANNEX 2] redesignated as Company B and activated).

ANNEX 1

Constituted 15 July 1967 in the Regular Army as the 202d Army Security Agency Company and activated at Fort Hood, Texas. Inactivated 19 April 1971 at Fort Hood, Texas. Activated 1 July 1974 in Germany.

ANNEX 2

Organized 26 August 1943 in Algeria as the 2678th Headquarters Company, Counter Intelligence Corps (Provisional). Disbanded 26 April 1944 and personnel transferred to the 6779th Counter Intelligence Corps Detachment (Provisional). Disbanded 18 August 1944 and personnel transferred to the 501st Counter Intelligence Corps Detachment (constituted 12 July 1944 in the Army of the United States). Disbanded 26 June 1945 in Italy.

Reconstituted 6 April 1951 in the Regular Army as the 501st Counter Intelligence Corps Detachment. Activated 11 May 1951 at Fort Holabird, Maryland. Reorganized and redesignated 25 January 1958 as the 501st Military Intelligence Detachment. Inactivated 31 March 1971 at Fort Hood, Texas.

501st MILITARY INTELLIGENCE BATTALION (Electronic Horsemen)

HERALDIC ITEMS

COAT OF ARMS

Shield: Quarterly azure and vert, in bend a lightning flash point to base gules fimbriated or and in bend sinister a cavalry saber point to chief of the like.

Crest: On a wreath of the colors, or and azure, in front of a torii gate gules a horse's head erased sable langued of the third interlaced with two lightning flashes, the one behind bendwise and one in front bend sinisterwise of the first.

Motto: OUT FRONT.

Symbolism: Blue and green refer to the air and ground assets of the battalion and further allude to the close relationship with infantry (blue) and armor (green) units of the division. The red and yellow flash connotes the prominent role of electronic signals intelligence in modern warfare. The cavalry saber, flash, and quartered field collectively suggest the blending of the traditional with the latest modern developments in intelligence, reconnaissance, security, and electronic warfare capabilities within the military intelligence battalion.

The black horse's head, suggested by the arms of the province of Naples, refers to the participation of an element of the battalion in Italian campaigns of World War II. The torii gate alludes to the battalion's service in Korea and the flashes connote awards of the Meritorious Unit Commendation (Army) and the Republic of Korea Presidential Unit Citation.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

CAMPAIGN PARTICIPATION CREDIT

Korean War
Second Korean Winter
Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953
Southwest Asia
Defense of Saudi Arabia
Liberation and Defense of Kuwait
Cease-Fire

Company B additionally entitled to:

World War II–EAME
Naples-Foggia
Anzio
Rome-Arno
North Apennines
Po Valley

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (Headquarters and Headquarters Detachment, 301st Communication Reconnaissance Battalion, cited; DA GO 22, 1954)

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (501st Military Intelligence Battalion cited; DA GO 1, 1996)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA (Headquarters and Headquarters Detachment, 301st Communication Reconnaissance Battalion, cited; DA GO 33, 1953, as amended by DA GO 41, 1955)

502d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Argent, on a pale azure between two beacon fires in base of the second enflamed or, in chief a beacon fire of the first enflamed of the third.

Crest: On a wreath of the colors, argent and azure, issuing from a wreath of laurel or with a Korean taeguk at center proper, a griffin's head of the third langued gules.

Motto: FREEDOM BY VIGILANCE.

Symbolism: Oriental blue is one of the colors used for military intelligence units. The three beacon fires, representing Korea's ancient system of sending messages, allude to the three campaigns in which the unit served in the Korean War. The gold of the flames commemorates unit decorations received by the battalion.

The griffin is a symbol of vigilance, the essential attribute for effective intelligence work. The taeguk represents the Republic of Korea Presidential Unit Citation, and the wreath refers to the Meritorious Unit Commendation (Army) awarded to the battalion for service in Korea. Gold is used to represent excellence and achievements of the unit.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 30 June 1952 in the Regular Army as Headquarters, 502d Military Intelligence Service Battalion. Activated 1 September 1952 in Korea. Reorganized and redesignated 28 March 1954 as Headquarters, 502d Military Intelligence Battalion. Inactivated 20 January 1955 in Korea. Redesignated 20 March 1961 as Headquarters and Headquarters Company, 502d Military Intelligence Battalion (organic elements concurrently constituted). Battalion activated 25 March 1961 in Korea. Inactivated 1 January 1978 in Korea. Activated 1 October 1986 at Fort Lewis, Washington.

CAMPAIGN PARTICIPATION CREDIT

Korean War

Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (Headquarters, 502d Military Intelligence Battalion, cited; DA GO 14, 1955)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA (Headquarters, 502d Military Intelligence Service Battalion, cited; DA GO 70, 1953)

511th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a Korean taeguk proper and issuant therefrom to chief three lightning bolts argent.

Crest: On a wreath of the colors, argent and azure, two griffins' heads addorsed and erased, that to dexter argent and that to sinister of the second both beaked and eyed or and langued gules.

Motto: PROUD AND READY.

Symbolism: Oriental blue and silver gray are the colors associated with the military intelligence branch. The lightning bolts refer to the importance of speed, electronics, and communications to all intelligence activities and represent the unit's participation in three campaigns in the Korean War and its multifaceted intelligence mission. The taeguk denotes the award of the Republic of Korea Presidential Unit Citation to the organization.

The griffin is a heraldic symbol of alertness and vigilance; the prominent eyes and ears suggest the role played by intelligence forces in support of the Army's mission. The contrasting colors and back-to-back position signify the round-the-clock and worldwide scope of the intelligence and security functions.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is an adaptation of the shield, crest, and motto of the coat of arms.

LINEAGE AND HONORS

RA
(inactive)

LINEAGE

Constituted 30 June 1952 in the Regular Army as the 511th Military Intelligence Service Company. Activated 1 September 1952 in Korea. Reorganized and redesignated 28 March 1954 as the 511th Military Intelligence Company. Inactivated 20 May 1956 in Korea. Activated 1 June 1962 in Germany.

Reorganized and redesignated 1 July 1972 as Headquarters and Headquarters Company, 511th Military Intelligence Battalion. Inactivated 1 October 1983 in Germany. Redesignated 16 October 1983 as Headquarters, Headquarters and Service Company, 511th Military Intelligence Battalion, and activated in Germany (organic elements concurrently constituted and activated). Battalion inactivated 15 November 1991 in Germany.

CAMPAIGN PARTICIPATION CREDIT

Korean War
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait
- Cease-Fire

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered SOUTHWEST ASIA (511th Military Intelligence Battalion cited; DA GO 34, 1992)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA 1952–1953 (511th Military Intelligence Service Company cited; DA GO 24, 1954)

519th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Or, in base a sphinx facing to dexter couchant azure detailed of the first in front of an open book of the last, fimbriated of the second, its upper edge at fess point in front of a globe overall of the like, gridlined of the field.

Crest: On a wreath of the colors, or and azure, a garb of rice of the first in front of a triangle gules conjoined at the tip with a torii sable.

Motto: STRENGTH THRU INTELLIGENCE.

Symbolism: Teal blue and yellow are the colors formerly used for Army intelligence organizations. The sphinx also symbolizes Army intelligence. Resting against the terrestrial globe is an open book, representing the knowledge made available through mastery of the languages of the world. The globe itself indicates the worldwide scope of the battalion's activities.

Red is the color for action, and the triangle, simulating a Vietnamese sun hat, alludes to service in Vietnam. The torii refers to Korea, where an element of the organization participated in seven campaigns. The rice stalks represent the unit decorations awarded during both wars.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA
LINEAGE (active)

Constituted 1 October 1948 in the Regular Army as the 519th Headquarters Intelligence Detachment. Activated 15 October 1948 at Fort Riley, Kansas. Reorganized and redesignated 10 May 1949 as Headquarters, 519th Military Intelligence Platoon. Reorganized and redesignated 11 August 1949 as the 519th Military Intelligence Service Platoon.

Reorganized and redesignated 21 November 1951 as the 519th Military Intelligence Service Battalion. Reorganized and redesignated 31 December 1953 as the 519th Military Intelligence Battalion. Reorganized and redesignated 25 January 1958 as Headquarters and Headquarters Company, 519th Military Intelligence Battalion. (523d Military Intelligence Company [see ANNEX] reorganized and redesignated 15 July 1959 as Company A.)

ANNEX

Constituted 25 September 1950 in the Regular Army as the 523d Military Intelligence Service Platoon. Activated 10 October 1950 at Fort Riley, Kansas. Reorganized and redesignated 1 September 1952 as the 523d Military Intelligence Service Company. Reorganized and redesignated 28 March 1954 as the 523d Military Intelligence Company. Inactivated 15 November 1954 in Korea. Activated 25 January 1958 at Fort Bragg, North Carolina.

CAMPAIGN PARTICIPATION CREDIT

Vietnam
- Defense
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII
- Consolidation I
- Consolidation II
- Cease-Fire

Armed Forces Expeditions
- Panama

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait

Company A additionally entitled to:

Korean War

First UN Counteroffensive
CCF Spring Offensive
UN Summer-Fall Offensive
Second Korean Winter
Korea, Summer-Fall 1952
Third Korean Winter
Korea, Summer 1953

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (Headquarters and Headquarters Company and Company A, 519th Military Intelligence Battalion, cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1970 (519th Military Intelligence Battalion cited; DA GO 52, 1974)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1971–1972 (519th Military Intelligence Battalion cited; DA GO 6, 1976)

Company A additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA (523d Military Intelligence Service Company cited; DA GO 36, 1953)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA 1950–1952 (523d Military Intelligence Service Platoon cited; DA GO 33, 1953, as amended by DA GO 41, 1955)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA 1952–1953 (523d Military Intelligence Company cited; DA GO 89, 1953, as amended by DA GO 9, 1955)

Company C additionally entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (Company C, 519th Military Intelligence Battalion, cited; DA GO 43, 1968)

522d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, on a bend engrailed plain cottised between a winged sphinx couchant argent and a taeguk gules and azure fimbriated of the second, a lightning flash gules.

Crest: None approved.

Motto: THE EQUALIZERS.

Symbolism: Oriental blue and silver gray are the colors used for military intelligence. The winged sphinx is symbolic of all-seeing and eternal vigilance, and the taeguk refers to the unit's Korean War service. The electronic warfare intelligence capability of the organization is represented by the engrailed bend, and the lightning flash is indicative of speed in communication and intelligence gathering.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Organized 1 September 1950 at Fort Bragg, North Carolina, as the 522d Military Intelligence Service Detachment. (Constituted 20 September 1950 in the Regular Army.) Inactivated 28 December 1951 in Korea.

Redesignated 23 June 1954 as Headquarters and Headquarters Company, 522d Military Intelligence Battalion (Companies A and B concurrently constituted). Battalion activated 27 July 1954 in Germany. Inactivated 15 August 1958 in Germany. Assigned 21 December 1976 to the 2d Armored Division and activated at Fort Hood, Texas. (373d Army Security Agency Company [see ANNEX 1] consolidated 16 October 1979 with Company A; 502d Military Intelligence Company [see ANNEX 2] concurrently consolidated with Company B.) Inactivated 15 April 1991 at Fort Hood, Texas. Activated 16 December 1992 at Fort Polk, Louisiana. Inactivated 15 January 1996 at Fort Hood, Texas.

ANNEX 1

Constituted 11 May 1962 in the Regular Army as Company B, 303d Army Security Agency Battalion. Activated 25 June 1962 at Fort Benning, Georgia. Reorganized and redesignated 15 October 1966 as the 373d Army Security Agency Company.

ANNEX 2

Constituted 21 June 1944 in the Army of the United States as the 520th Counter Intelligence Corps Detachment. Activated 1 July 1944 at Camp Campbell, Kentucky. Allotted 17 December 1948 to the Regular Army.

Reorganized and redesignated 25 January 1958 as the 502d Military Intelligence Detachment. Consolidated 28 December 1961 with the 502d Counter Intelligence Corps Detachment (see ANNEX 3) and consolidated unit designated as the 502d Military Intelligence Detachment. Reorganized and redesignated 8 January 1971 as the 502d Military Intelligence Company.

ANNEX 3

Constituted 12 July 1944 in the Army of the United States as the 502d Counter Intelligence Corps Detachment. Activated 16 August 1944 in France with personnel from provisional Counter Intelligence Corps detachment attached to the 2d Armored Division. Inactivated 14 October 1946 in Germany. Activated 10 May 1947 on Guam. Inactivated 14 March 1950 on Guam.

CAMPAIGN PARTICIPATION CREDIT

Korean War
- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter

Southwest Asia
- Defense of Saudi Arabia
- Liberation and Defense of Kuwait

Company B additionally entitled to:

World War II–EAME
- Normandy
- Northern France
- Rhineland
- Ardennes-Alsace
- Central Europe

DECORATIONS

Company B entitled to:

Belgian Fourragere 1940 (2d Armored Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in Belgium (2d Armored Division cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in the Ardennes (2d Armored Division cited; DA GO 43, 1950)

524th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Azure two chevronels fretty argent charged with eighteen pellets all within a bordure of the second.

Crest: On a wreath of the colors, argent and azure, a garb of rice or charged at base with a taeguk proper; overall a bayonet palewise, point up, blade sable and hilt argent all tied with a ribbon gules.

Motto: SILENT VIGILANCE.

Symbolism: Oriental blue and silver gray are the colors associated with military intelligence. The interlocking chevronels suggest the gathering of information from many sources processed through the unit and distributed throughout the Army, as represented by the border. The black pellets suggest the unit's ability to interpret various data and to form assessments of military situations. Eighteen refers to the number of campaigns in which the unit participated in Korea and Vietnam.

The bayonet alludes to the unit's participation in campaigns in Vietnam and Korea, represented by the garb of rice and taeguk. The black blade refers to secrecy and the unit's intelligence function. The red band of the garb refers to the Meritorious Unit Commendation (Army) awarded the unit for service in Vietnam.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

RA

Lineage (active)

Constituted 25 September 1950 in the Regular Army as the 524th Technical Intelligence Coordinator Detachment. Activated 10 October 1950 at Fort Riley, Kansas. Inactivated 1 December 1951 in Korea. Redesignated 22 June 1965 as the 524th Intelligence Corps Detachment. Activated 1 July 1965 at Fort Bragg, North Carolina. Redesignated 15 October 1966 as the 524th Military Intelligence Detachment. Inactivated 26 November 1970 in Vietnam.

Redesignated 16 June 1982 as Headquarters and Headquarters Company, 524th Military Intelligence Battalion, and activated in Korea. (Organic elements constituted 16 October 1988; Company A concurrently activated in Korea.)

CAMPAIGN PARTICIPATION CREDIT

Korean War
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter

Vietnam
- Defense
- Counteroffensive
- Counteroffensive, Phase II
- Counteroffensive, Phase III
- Tet Counteroffensive
- Counteroffensive, Phase IV
- Counteroffensive, Phase V
- Counteroffensive, Phase VI
- Tet 69/Counteroffensive
- Summer-Fall 1969
- Winter-Spring 1970
- Sanctuary Counteroffensive
- Counteroffensive, Phase VII

DECORATIONS

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1968 (524th Military Intelligence Detachment cited; DA GO 67, 1968)

Army Superior Unit Award, Streamer embroidered 1986–1988 (524th Military Intelligence Battalion cited; DA GO 14, 1989)

527th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Gyronny of eight argent and sable, a pale gules voided throughout argent, surmounted by a globe azure gridlined argent, overall two swords saltirewise also argent.

Crest: None approved.

Motto: STRIVE FOR EXCELLENCE.

Symbolism: The shield, divided into dark and light sections, suggests the ever-changing methods of counterintelligence functions and the day/night vigilance of intelligence gathering. The red and white allude to the coat of arms of Kaiserslautern in Germany, where the unit has been stationed. The globe alludes to the overseas origin and duty of the unit and resembles a grid, which suggests the sifting of information through the unit to support Army goals. The crossed swords symbolize offensive and defensive counterintelligence and the defense of Europe.

DISTINCTIVE UNIT INSIGNIA

Description: A silver color metal and enamel device consisting of two silver swords in saltire, pommels to base, the lateral and base areas between the swords of black enamel and the upper area of red enamel; surmounting the swords a blue disc divided by five horizontal and vertical silver lines bearing at center a black square, point up, with a silver dot; issuing from the disc three rays to the lateral and base areas and a broad arrowhead extending beyond the top all silver; on a silver scroll issuing from under the blades and the pommels, the inscription STRIVE FOR EXCELLENCE in black enamel.

Symbolism: The square and dot simulate an observation apparatus, the disc represents a globe, and the divisions symbolize a network. The arrowhead connotes martial readiness, while the rays symbolize all facets of sound, light, and vibratory systems. All represent the collection, processing, and dissemination of information functions of a military intelligence unit. The swords refer to defensive and offensive counterintelligence methods. The white arrowhead dividing the red area suggests the coat of arms of Kaiserslautern in Germany, symbolizing service there.

Lineage and Honors

RA

Lineage (active)

Constituted 18 April 1946 in the Army of the United States as the 527th Interrogation Team. Activated 1 May 1946 in Germany. Inactivated 31 October 1946 in Germany. Redesignated 6 February 1948 as the 527th Headquarters Intelligence Detachment. Activated 21 February 1948 at Fort Bragg, North Carolina. Allotted 5 May 1949 to the Regular Army. Reorganized and redesignated 23 May 1949 as Headquarters, 527th Military Intelligence Platoon. Reorganized and redesignated 4 August 1949 as the 527th Military Intelligence Service Platoon. Reorganized and redesignated 14 November 1951 as the 527th Military Intelligence Service Company. Reorganized and redesignated 31 December 1953 as the 527th Military Intelligence Company. Inactivated 25 January 1958 at Fort Hood, Texas. Activated 1 June 1962 in Germany.

Reorganized and redesignated 1 July 1972 as Headquarters and Headquarters Company, 527th Military Intelligence Battalion. (Organic elements constituted 1 October 1982 and activated in Germany.)

Campaign Participation Credit

None.

Decorations

Army Superior Unit Award, Streamer embroidered 1990–1991 (527th Military Intelligence Battalion cited; DA GO 34, 1992)

532d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Checky azure and or a horse rampant sable fimbriated of the second.

Crest: None approved.

Motto: NOSCE HOSTEM (KNOW YOUR ENEMY).

Symbolism: Teal blue and yellow are the colors formerly used for military intelligence battalions. The black horse alludes to Stuttgart in Germany, the unit's place of activation. The horse and checky field combined, symbolic of a chessboard, refer to the strategic and tactical functions of an intelligence unit.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (active)

Constituted 16 February 1951 in the Regular Army as the 532d Military Intelligence Service Company. Activated 15 August 1951 in Germany.

Reorganized and redesignated 20 September 1951 as the 532d Military Intelligence Service Battalion. Reorganized and redesignated 20 October 1953 as the 532d Military Intelligence Battalion. Reorganized and redesignated 25 June 1958 as Headquarters and Headquarters Company, 532d Military Intelligence Battalion (521st Military Intelligence Company [see ANNEX 1], 427th Counter Intelligence Corps Detachment [see ANNEX 2], and 526th Military Intelligence Company [see ANNEX 3] concurrently reorganized and redesignated as Companies A, B, and C). Battalion inactivated 1 June 1962 in Germany. Activated 16 October 1986 in Korea.

ANNEX 1

Organized 5 September 1950 in Japan as the 521st Military Intelligence Service Detachment. (Constituted 7 September 1950 in the Regular Army.) Reorganized and redesignated 28 December 1951 as the 521st Military Intelligence Service Platoon. Reorganized and redesignated 1 September 1952 as the 521st Military Intelligence Service Company. Reorganized and redesignated 28 March 1954 as the 521st Military Intelligence Company.

ANNEX 2

Constituted 12 July 1944 in the Army of the United States as the 427th Counter Intelligence Corps Detachment. Activated 22 August 1944 on Corsica. Allotted 16 February 1951 to the Regular Army.

ANNEX 3

Constituted 18 April 1946 in the Army of the United States as the 526th Interrogation Team. Activated 1 May 1946 in Germany. Inactivated 6 November 1946 in Germany. Redesignated 6 February 1948 as the 526th Headquarters Intelligence Detachment. Activated 21 February 1948 at Fort Bragg, North Carolina. Allotted 5 May 1949 to the Regular Army. Reorganized and redesignated 23 May 1949 as Headquarters, 526th Military Intelligence Platoon. Reorganized and redesignated 4 August 1949 as the 526th Military Intelligence Service Platoon. Reorganized and redesignated 28 August 1951 as the 526th Military Intelligence Service Company. Reorganized and redesignated 20 October 1953 as the 526th Military Intelligence Company.

CAMPAIGN PARTICIPATION CREDIT

Company A entitled to:

Korean War
- UN Defensive
- UN Offensive
- CCF Intervention
- First UN Counteroffensive
- CCF Spring Offensive
- UN Summer-Fall Offensive
- Second Korean Winter
- Korea, Summer-Fall 1952
- Third Korean Winter
- Korea, Summer 1953

Company B entitled to:

World War II–EAME
- Rhineland

DECORATIONS

Company A entitled to:

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1951–1952 (521st Military Intelligence Service Platoon cited; DA GO 10, 1953)

Meritorious Unit Commendation (Army), Streamer embroidered KOREA 1952–1954 (521st Military Intelligence Service Company cited; DA GO 46, 1954)

Republic of Korea Presidential Unit Citation, Streamer embroidered KOREA (521st Military Intelligence Service Company cited; DA GO 82, 1954)

533d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per fess argent and azure two lightning flashes saltirewise counterchanged, in chief two eagles' heads conjoined erased sable and overall in pale a double-warded key, wards to base of the first.

Crest: None approved.

Motto: VIGILANCE WITH PRIDE.

Symbolism: Oriental blue and silver gray (white) are the colors traditionally associated with military intelligence. The crossed lightning flashes connote the battalion's mission as a combat electronic warfare intelligence unit. The key is a symbol of knowledge and security. The double-headed eagle symbolizes watchfulness and vigilance and alludes to the unit's former areas of service, Austria and Germany.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

RA

LINEAGE (inactive)

Constituted 15 February 1952 in the Regular Army as the 533d Military Intelligence Service Battalion. Activated 1 March 1952 in Austria. Reorganized and redesignated 25 May 1954 as the 533d Military Intelligence Battalion. Inactivated 8 September 1955 in Austria.

Redesignated 16 September 1980 as Headquarters, Headquarters and Operations Company, 533d Military Intelligence Battalion, assigned to the 3d Armored Division, and activated in Germany (856th Army Security Agency Company [see ANNEX 1] concurrently reorganized and redesignated as Company A; 503d Military Intelligence Company [see ANNEX 2] consolidated with the 203d Military Intelligence Detachment [see ANNEX 3] and consolidated unit reorganized and redesignated as Company B). Battalion inactivated 15 August 1992 in Germany.

ANNEX 1

Constituted 4 September 1944 in the Army of the United States as the 3148th Signal Service Platoon. Activated 25 September 1944 on New Caledonia.

Inactivated 30 January 1946 on Ie Shima. Redesignated 23 August 1948 as the 580th Signal Service Detachment and activated at Fort Greely, Alaska. Inactivated 1 June 1949 at Fort Greely, Alaska. Redesignated 7 June 1954 as the 580th Signal Detachment and allotted to the Regular Army.

Converted and redesignated 19 May 1955 as the 856th Communication Reconnaissance Detachment. Activated 25 June 1955 in Japan. Inactivated 15 August 1956 in Japan. Redesignated 6 April 1966 as the 856th Army Security Agency Detachment. Activated 15 June 1966 at Fort Benning, Georgia. Inactivated 6 March 1971 in Vietnam. Redesignated 1 July 1974 as the 856th Army Security Agency Company and activated in Germany.

ANNEX 2

Constituted 14 October 1944 in the Army of the United States as the 479th Counter Intelligence Corps Detachment. Activated 23 November 1944 on New Guinea. Disbanded 22 July 1945 in the Philippine Islands. Reconstituted 5 January 1949 in the Regular Army as the 530th Counter Intelligence Corps Detachment. Activated 28 January 1949 at Fort Knox, Kentucky. Inactivated 15 March 1951 at Fort Knox, Kentucky.

Redesignated 17 March 1955 as the 503d Counter Intelligence Corps Detachment. Activated 5 April 1955 at Fort Knox, Kentucky. Reorganized and redesignated 25 June 1958 as the 503d Military Intelligence Detachment. Consolidated 21 November 1972 with the 503d Military Intelligence Company (see ANNEX 4) and consolidated unit designated as the 503d Military Intelligence Company.

ANNEX 3

Constituted 12 July 1944 in the Army of the United States as the 503d Counter Intelligence Corps Detachment. Activated 16 August 1944 in France with personnel from provisional Counter Intelligence Corps Detachment attached to the 3d Armored Division. Inactivated 7 October 1945 in Germany. Activated 21 February 1948 at Fort Bragg, North Carolina. Allotted 25 June 1952 to the Regular Army.

Reorganized and redesignated 15 November 1954 as the 203d Counter Intelligence Corps Detachment. Reorganized and redesignated 25 January 1958 as the 203d Military Intelligence Detachment. Inactivated 5 May 1959 at Fort Hood, Texas. Activated 5 April 1962 at Fort Hood, Texas. Inactivated 20 April 1978 at Fort Hood, Texas.

ANNEX 4

Constituted 30 June 1952 in the Regular Army as the 503d Military Intelligence Service Company. Activated 1 September 1952 in Japan. Reorganized and redesignated 28 March 1954 as the 503d Military Intelligence Company. Inactivated 24 June 1955 in Japan. Activated 1 June 1962 in Germany. Inactivated 25 September 1965 in Germany.

CAMPAIGN PARTICIPATION CREDIT

Southwest Asia
Defense of Saudi Arabia
Liberation and Defense of Kuwait
Cease-Fire

Company A additionally entitled to:

World War II–AP
Ryukyus
Vietnam
Counteroffensive, Phase II
Counteroffensive, Phase III
Tet Counteroffensive
Counteroffensive, Phase IV
Counteroffensive, Phase V
Counteroffensive, Phase VI
Tet 69/Counteroffensive
Summer-Fall 1969
Winter-Spring 1970
Sanctuary Counteroffensive
Counteroffensive, Phase VII

Company B additionally entitled to:

World War II–AP
New Guinea
Luzon
World War II–EAME
Normandy
Northern France
Rhineland
Ardennes-Alsace
Central Europe

DECORATIONS

Company A entitled to:

Valorous Unit Award, Streamer embroidered SAIGON–LONG BINH (856th Radio Research Detachment cited; DA GO 48, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1966–1967 (856th Radio Research Detachment cited; DA GO 17, 1968)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1967–1968 (856th Radio Research Detachment cited; DA GO 29, 1969)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1968–1969 (856th Radio Research Detachment cited; DA GO 51, 1971)

Meritorious Unit Commendation (Army), Streamer embroidered VIETNAM 1969–1970 (856th Radio Research Detachment cited; DA GO 43, 1972)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1968 (856th Radio Research Detachment cited; DA GO 43, 1970)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1968–1970 (856th Radio Research Detachment cited; DA GO 51, 1971)

Republic of Vietnam Cross of Gallantry with Palm, Streamer embroidered VIETNAM 1970–1971 (856th Radio Research Detachment cited; DA GO 6, 1974)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1966–1970 (856th Radio Research Detachment cited; DA GO 51, 1971)

Republic of Vietnam Civil Action Honor Medal, First Class, Streamer embroidered VIETNAM 1970–1971 (856th Radio Research Detachment cited; DA GO 6, 1974)

Company B entitled to:

Philippine Presidential Unit Citation, Streamer embroidered 17 OCTOBER 1944 TO 4 JULY 1945 (479th Counter Intelligence Corps Detachment cited; DA GO 47, 1950)

Belgian Fourragere 1940 (503d Counter Intelligence Corps Detachment cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in Belgium (503d Counter Intelligence Corps Detachment cited; DA GO 43, 1950)

Cited in the Order of the Day of the Belgian Army for action in the Ardennes (503d Counter Intelligence Corps Detachment cited; DA GO 43, 1950)

542d MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Sable, a sword and lightning flash saltirewise surmounted by a stylized chess piece with a griffin's head or, within a bordure compony argent and azure.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and sable, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: THE EYES OF THE BATTLE.

Symbolism: Oriental blue and silver gray (white) are the colors traditionally associated with military intelligence units. Black denotes solidity while suggesting clandestine capabilities. Gold alludes to excellence and achievement. The sword and flash represent military preparedness and speed. The border and chess piece suggest strategy and countermeasure tactics. The griffin symbolizes vigilance with its keen eyesight and acute hearing.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is a modification of the shield and motto of the coat of arms.

LINEAGE AND HONORS

AR

LINEAGE (active)

Constituted 16 September 1987 in the Army Reserve as the 242d Military Intelligence Battalion and activated with Headquarters at Staten Island, New York. Inactivated 15 September 1993 at Staten Island, New York.

Redesignated 16 September 1993 as the 542d Military Intelligence Battalion and activated with Headquarters at East Windsor, Connecticut.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

549th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Azure, a globe argent gridlined sable, overall a lightning flash issuing from dexter chief or in saltire with a sword gules in bend sinister, all within a border of the second.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: MODERN WARFARE.

Symbolism: The global aspect of the mission performed by the military intelligence branch is represented by the longitude and latitude lines of the world. The lightning flash is symbolic of the electronic warfare nature of military intelligence. The sword represents the aggressive nature and dangerous missions accomplished by military intelligence personnel. The border suggests containment and alludes to intelligence gathering and its use in defense strategy.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

AR

LINEAGE (active)

Constituted 17 July 1986 in the Army Reserve as the 549th Military Intelligence Battalion and activated with Headquarters at Austin, Texas.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

550th MILITARY INTELLIGENCE BATTALION

Heraldic Items

Coat of Arms

Shield: Argent, a lightning bolt bendwise point to base azure, all within a bordure quarterly gules and of the first.

Crest: That for the regiments and separate battalions of the Army Reserve: On a wreath of the colors, argent and azure, the Lexington Minuteman proper. The statue of the Minuteman, Capt. John Parker (H. H. Kitson, sculptor), stands on the Common in Lexington, Massachusetts.

Motto: BLUE LIGHTNING.

Symbolism: Oriental blue and silver gray are the military intelligence colors. Blue also alludes to the battalion's affiliation with the 50th Armored (Jersey Blues) Division. The colors red and white were suggested by the shoulder sleeve insignia of the 78th Division (Training), to which the battalion was attached. The lightning bolt relates to the battalion's signal security and electronic warfare mission. The quartered border signifies military strategy.

Distinctive Unit Insignia

The distinctive unit insignia is the shield and motto of the coat of arms.

Lineage and Honors

AR

Lineage (inactive)

Constituted 16 July 1986 in the Army Reserve as the 550th Military Intelligence Battalion and activated with Headquarters at Pedricktown, New Jersey. Inactivated 15 September 1993 at Pedricktown, New Jersey.

Campaign Participation Credit

None.

Decorations

None.

629th MILITARY INTELLIGENCE BATTALION

HERALDIC ITEMS

COAT OF ARMS

Shield: Per chevron paly of six argent and azure a bend counterchanged, and of the first in base a panther's face proper grasping two lightning flashes conjoined chevronwise of the second.

Crest: That for the regiments and separate battalions of the Maryland Army National Guard: On a wreath of the colors, argent and azure, a cross bottony per cross quarterly gules and argent.

Motto: STALK THE PREY.

Symbolism: Oriental blue is one of the colors associated with military intelligence. The upper half of the shield alludes to the state flag of Maryland and identifies the home area of the battalion. The panther embodies the nickname of the unit, "Prowler," and is a predator celebrated for its stealth and patience on the hunt. It is an appropriate symbol for a tactical level intelligence unit. The lightning flashes refer to speed of operation and the dominant role of combat electronic warfare on the battlefield.

DISTINCTIVE UNIT INSIGNIA

The distinctive unit insignia is the shield and motto of the coat of arms.

LINEAGE AND HONORS

ARNG

LINEAGE (Maryland)

Organized and federally recognized 3 May 1988 in the Maryland Army National Guard as the 629th Military Intelligence Battalion, an element of the 29th Infantry Division, with Headquarters at Greenbelt. Location of Headquarters changed 1 April 1994 to Laurel.

Home Station: Laurel.

CAMPAIGN PARTICIPATION CREDIT

None.

DECORATIONS

None.

Glossary of Lineage Terms

ACTIVATE. To transfer a constituted Regular Army or Army Reserve unit from the inactive to the active rolls of the United States Army. The unit is usually stationed at a specific location and assigned personnel and equipment at this time; however, a unit may be active at zero strength—that is, without personnel or equipment.

ALLOT. To allocate a unit to one of the components of the United States Army. The present components are the Regular Army (RA), the Army National Guard (ARNG), and the Army Reserve (AR), formerly known as the Organized Reserves and the Organized Reserve Corps. During World War II units were also allotted to the Army of the United States. An Army National Guard unit is usually further allotted to a particular state or group of states. A unit may be withdrawn from any component except the Army National Guard and allotted to another; the new allotment, however, does not change the history, lineage, and honors of the unit.

ASSIGN. To make a unit part of a larger organization and place it under that organization's command and control until it is relieved from the assignment. As a rule, only assignments to divisions and separate combined arms brigades are shown in unit lineages.

CONSOLIDATE. To merge two or more units into a single unit. The unit may retain the designation of one of the former units or it may have a new designation, but it inherits the history, lineage, and honors of all of the former units. Active as well as inactive units may be consolidated.

CONSTITUTE. To place the designation of a new unit on the official rolls of the United States Army.

CONVERT. To transfer a unit from one branch of the Army to another—for example, from signal to military intelligence. Such a change always requires a redesignation; however, there is no break in the historical continuity of the unit. Active as well as inactive units may be converted, but if the unit is active, it must also be reorganized under a new table of organization and equipment (TOE).

DESIGNATION. The official title of a unit, consisting usually of a number, a branch or function, and a command echelon. Additional descriptive terms may appear in parentheses, but such parenthetical identifications are not part of the unit's official designation.

DISBAND. To remove the designation of a Regular Army or Army Reserve unit from the official rolls of the United States Army. If the unit is active, it must also be inactivated. Disbandment is intended to be permanent and irreversible, except in extraordinary circumstances.

ELEMENT. A unit that is assigned to or is part of a larger organization.

FEDERALLY RECOGNIZE. To accept an Army National Guard unit into the force structure of the United States Army after the unit has been inspected by a federal representative and found to be properly stationed, organized, and equipped in accordance with Army requirements.

INACTIVATE. To place a Regular Army or Army Reserve unit that is not currently needed in the force structure in an inoperative status without assigned personnel or equipment for a limited period of time. The unit is transferred to the inactive rolls of the United States Army, but it can be activated again whenever needed. Upon reactivation, the unit retains its former history, lineage, and honors.

ORDER INTO ACTIVE FEDERAL SERVICE. To place an Army National Guard unit on full-time active duty under the control of the United States government. The unit remains in federal service until released by the federal government, at which time it reverts to the control of its home state or states.

ORDER INTO ACTIVE MILITARY SERVICE. To place an Army Reserve unit on full-time active duty, usually during a war or a crisis. After completing its active duty, the unit may be inactivated or it may be released from active military service, reverting to reserve status. This term does not apply to Army Reserve units on annual active duty for training.

ORGANIC ELEMENT. A unit that is an integral part of a larger organization—for example, a lettered company of a battalion.

ORGANIZE. To assign personnel and equipment to a unit and make it operative—that is, capable of performing its mission. For Army National Guard units, this term is used instead of ACTIVATE. (See above.)

RECONSTITUTE. To restore to the official rolls of the United States Army a unit that has been disbanded or one whose federal recognition has been withdrawn. The reconstituted unit may have a new designation, but it retains its former history, lineage, and honors.

REDESIGNATE. To change a unit's official title. Active as well as inactive units may be redesignated, but personnel and equipment of an active unit are not changed unless the unit is reorganized at the same time. Redesignation is a change of title only; the unit's history, lineage, and honors remain the same.

REORGANIZE. To change the structure of a unit in accordance with a new table of organization and equipment (TOE) within the same branch of the Army.

SPECIAL DESIGNATION. An official unit nickname. There are two types of special designations—a traditional designation (one that a unit has used continuously for the last thirty years or more) and a distinctive designation (one that a unit has used for less than thirty years or one with which a unit wishes to be associated). The special designation, if any, appears in parentheses after the unit's official designation.

WITHDRAW FEDERAL RECOGNITION. To remove the designation of an Army National Guard unit from the official rolls of the United States Army. Federal recognition is withdrawn when the unit no longer meets Army requirements or is no longer needed in the force structure.

Index to the Narrative

Aberdeen Proving Ground, Md.: 177
Adjutant General's Office: 3, 7, 12, 14, 46
Administrative Survey Detachment: 139, 141, 159, 163, 165
Aerial exploitation: 181, 182, 184, 188–89, 193
Aerial reconnaissance: 35, 39, 45–46, 114–15, 131–32, 148, 181
Afghanistan: 169
African Americans: 25, 57
Ainsworth, Maj. Gen. Frederick: 16
Air attaches: 45–46, 105
Air Force Intelligence: 136
Air Force, U.S.: 104, 105, 132
Air Reconnaissance Support Battalions: 132
Aircraft: 132, 149, 160
Airplanes, observation: 18–19, 21, 45–46, 113, 119, 131–32
Akin, Brig. Gen. Spencer: 94
ALAMO Scouts: 96–97
Alaska: 110, 166
All-Volunteer Force: 195
Allied Intelligence Bureau (AIB): 95
Allied Translator and Interpreter Service (ATIS): 95, 96, 108
Amchitka, Alaska: 79, 83
America: 56, 61, 101, 153. *See also* United States.
American advisers in Vietnam: 145, 148–49
The American Black Chamber: 47
American Civil Liberties Union (ACLU): 156–57, 161–62
American Expeditionary Forces (AEF): 21, 26, 30–39, 40
American Protective League: 29
Anglo-American Combined Chiefs of Staff: 91, 93
Angola: 169
Antiaircraft service: 34–35
Antiwar movements: 25, 146, 153, 155
Arab-Israeli War: 167
Ardennes counteroffensive: 152–53
Area Analysis Intelligence Agency: 137
Arlington Hall Station, Va.: 67, 77–79, 82–83, 94, 109–10, 123, 127, 129, 164, 174, 176–77, 185
Armed Forces Security Agency: 110–11, 191–92
Armistice
  Korea: 121, 134
  World War I: 30, 32, 40
Armored elements: 151, 152–53, 181
Army, Department of: 127, 128, 156, 159, 161, 165
Army, U.S.: 3–4, 8, 14–15, 18–19, 21, 22–23, 27–28. *See also* Army Intelligence.
  demobilization of: 101, 107
  interwar difficulties: 42, 51–60
  in World War II: 83–99
Army Air Corps: 45–46, 52
Army Air Forces (AAF)
  postwar: 103, 104
  in World War II: 59, 62–63, 64, 66, 67–68, 69, 75, 83, 88–89, 93, 95, 97
Army chief of staff. *See* Chief of Staff, Army.
Army Collection Detachment (Korea): 134
Army General School: 112, 125
Army Ground Forces: 63, 68, 82, 112
Army Intelligence: 4–6. *See also* Intelligence; Military Intelligence.
  beginnings of: 15–18, 39–40
  between the wars: 44, 55–57, 58–60
  future trends: 189
  from Korea to Vietnam: 122–23, 124, 125–26, 128, 134–35

Army Intelligence (cont.)
in Korean War: 102, 113–14, 115
organization of: 11–12, 14–16, 20, 28–30, 31–32, 39–40, 57–59, 94–95
reorganization: 62–63, 64–68, 69–70, 98, 103–05
reorganization and renewal: 169, 170, 171–72, 174–75, 176, 179, 181, 182, 184–85
restructuring: 136, 137, 138, 139–40, 141, 142–43
Vietnam and beyond: 147, 148–49, 150–51, 152–53, 156, 157–58, 159, 160–61, 163–64, 167
in World War I: 21–23, 29, 31–32, 33–39, 40
in World War II: 68–69
Army Intelligence Agency (AIA): 176, 178, 189
Army Intelligence Board: 129, 138–39
Army Intelligence Center: 124, 125, 126, 139, 160
Army Intelligence Corps Activity: 139, 140, 159
Army Intelligence, Electronic Warfare, and Target Acquisition Plan (AIMP): 184
Army Intelligence School: 138, 139, 141, 149, 158, 160, 161
Army Intelligence and Security Branch: 142–43, 157, 195
Army Language School: 112
Army Map Service: 54, 129, 137, 160
Army Materiel Command: 137, 139, 170, 176, 178
Army Missile Intelligence Agency: 137
Army Missile and Space Intelligence Center: 176
Army-Navy Communications Intelligence Board (ANCIB): 110
Army-Navy Communications Intelligence Coordinating Committee (ANCICC): 80
Army Photo Interpretation Center: 125, 139. *See also* Photo interpreters.
Army Reserve: 116, 119, 124, 182, 195
Army Security Agency (ASA): 6, 102–03
Cold War and Korea: 105, 109–10, 111–14, 117, 119
future trends: 191, 192, 193, 194, 195, 196
Korea to Vietnam: 127, 128, 129, 130, 135, 138, 140–41, 143
reorganization and renewal: 170, 171–72, 173, 174, 175, 176, 177, 179, 180, 182
Vietnam and beyond: 147, 148, 150, 151, 152, 157, 158–59, 160, 164, 165, 166, 167
Army Security Agency (cont.)
Army Security Agency Training Center: 158, 173
Army Security Center: 116
Army Service Forces: 63, 67, 70, 76, 103, 106
Army Staff: 159, 161, 170, 173, 174
Artillery: 21, 34, 113
Asian Americans: 57
Asmara, Eritrea, Ethiopia: 79, 110
Assistant Chief of Staff for Intelligence (ACSI)
Korea to Vietnam: 123, 126, 136, 137, 138–39, 140, 142
reorganization and renewal: 170, 172–73, 174, 175, 176, 184
Vietnam and beyond: 149, 158, 159, 160, 163, 164, 165, 166
Atomic bomb: 99
Augsburg, Germany: 133
Australia: 61, 78, 93–94, 96
Australian intelligence: 94–95
Austria-Hungary: 12
Axis Powers: 87, 99, 101. *See also* Germany, Japan.

Baker, Lafayette: 10–11
Baker, Newton: 20, 22
Balloons, observation: 9, 18
Baltimore, Md.: 73, 74, 82, 160–61
Battle of the Bulge: 152
Beauregard, Maj. Gen. Pierre: 10
Bell, Maj. Gen. J. Franklin: 16
Bellmore, N.Y.: 79
Berlin, Germany: 101, 122, 145
Berlin Wall: 134
Bien Hoa, Vietnam: 148
Bissell, Maj. Gen. Clayton: 80
Bletchley Park, England: 68, 84, 92
Bolshevik Revolution: 38–39, 41–42
Borup, Capt. Henry T.: 12–13
Brazil: 66
Britain: 21, 51–52. *See also* Great Britain.
British intelligence: 68–69, 80, 84–85, 91–93
Bureau of Insurgent Records, Philippines: 14
Byron Hot Springs, Calif.: 62

Callaway, Howard: 169–70
Camps
Crowder, Mo.: 68
Drake, Japan: 115

Camps (cont.)
Holabird, Md.: 74, 76, 106–07. *See also* Fort Holabird.
Meade, Md.: 76. *See also* Fort Meade.
Ritchie, Md.: 67, 76, 112
Savage, Minn.: 67
Sharpe, Penn.: 67
Can Tho, Vietnam: 148
Canada: 47
Canal Zone, Panama: 53, 66, 166. *See also* Panama.
Caribbean: 110
Carlisle Barracks, Penn.: 112
Cavalry as scouts: 8–9, 11
Cease-fire inVietnam: 146
Censorship: 32, 36–37, 42, 70, 91, 116, 119, 130, 145
Central America: 169
Central Bureau, Brisbane (CBB): 94, 95
Central Clearance Facility: 175
Central Command, U.S. (CENTCOM): 177, 188
Central Intelligence Agency (CIA): 103, 106, 110, 191, 192
Central Intelligence Group: 103, 104–05
Central Records Facility: 107
Central Security Facility: 175, 177
Central Security Service: 164, 171, 191
Centralization: 136, 137, 163–64, 165
Chaumont, France: 33, 35, 37
Chemical Warfare Service: 64
Chiang Kai-shek: 47
Chicago, Ill.: 58, 67, 73
Chief, Corps of Intelligence Police: 57
Chief of Engineers: 160
Chief of the Intelligence Corps: 140
Chief of Military Intelligence: 173
Chief of Staff, Army: 128, 140, 167, 173
China: 15, 18, 47, 51, 62, 80, 101
Chinese Communists: 101–02, 113, 114, 118
Churchill, Brig. Gen. Marlborough: 31
Churchill, Winston S.: 81
Cipher Bureau: 111
Civil disturbance: 154–55, 156, 162–63. *See also* Intelligence, domestic.
Civil Disturbance Information Collection Plan: 162
Civil War, American: 3, 8–9, 11
Civilian Conservation Corps (CCC): 48
Clark Field, Philippines: 110
Clarke, Col. Carter W.: 65
Clausewitz, Karl von: 3
Code-breaking: 47, 68, 78. *See also* MAGIC, ULTRA.
Code and Cypher School, Britain: 68
Codes and ciphers: 18, 29–30, 37–38, 42, 59–60, 68–70, 119. *See also* Cryptology.
Cody, Buffalo Bill: 11
Cold War: 6, 101, 104, 107, 109, 133, 188–89
Combat Developments Command: 139
Combat Developments Command Intelligence Agency: 173
Combat electronic warfare and intelligence (CEWI): 179–80, 181, 182, 183, 188, 193, 194
Combat intelligence. *See* Intelligence, combat.
Combat Surveillance and Electronic Warfare School: 173
Combined Intelligence Center, Vietnam: 148
Communications: 9, 17–19, 29–30, 37–38, 46, 77, 81–83, 109, 114, 127, 130, 148, 150, 152, 171, 173, 191
Communications intelligence (COMINT)
Korea: 117–18, 119
World War II: 62–63, 65, 68–71, 77, 80, 82–83, 84, 85–87, 93, 94–97
Communications reconnaissance: 117, 131–33
Communications security (COMSEC): 81, 149–50, 152, 166, 172, 173, 175, 193, 194
Communism/Communists: 51, 101, 121, 169
Continental Army Command (CONARC): 137, 139, 140, 153, 162
Continental United States (CONUS): 163, 165, 166, 175, 192, 194
Coolidge, Jefferson: 12
Corderman, Col. (later Brig. Gen.) Preston W.: 79
Corozal, Canal Zone: 77
Corps of Engineers. *See* Engineers, Corps of.
Corps of Intelligence Police (CIP): 26–27, 32, 42, 44, 52, 53, 57–58
Corps of Interpreters, U.S. Army: 24
Corps of Topographic Engineers: 8–9. *See also* Engineers, topographic.
Corregidor, Philippines: 94
Corry Station, Fla.: 173
Counter Intelligence Branch: 51, 124
Counter Intelligence Corps (CIC): 6, 72, 73, 74, 75, 76, 85, 89, 96

Counter Intelligence Corps (cont.)
Cold War to Vietnam: 115–16, 118, 126, 127, 139–40, 141, 194, 195, 196
reorganization of: 90, 103, 105, 106–07, 108–09, 124–25
Counter Intelligence Corps Detachments: 106–07, 108, 112–13, 114, 115–16, 118, 134, 135, 139–40
Counter Intelligence Corps Group, 66th: 133–34
Counter Intelligence Corps School: 107, 124
Counterespionage: 23, 26, 28, 153–54. *See also* Counterintelligence.
Counterintelligence: 4–6, 10, 14
between the wars: 42, 44, 51, 52, 57–58
Cold War and Korea: 103, 106, 107, 108–09, 111, 112, 119
future trends: 191, 192, 194, 195, 196
Korea to Vietnam: 126, 127, 130–31, 135, 139–40, 141
reorganization and renewal: 170, 173, 175, 178, 180–81
Vietnam and beyond: 147–48, 152, 153, 154, 155, 159, 160, 161–63, 165, 166
World War I: 24–27, 29, 31, 35, 39
World War II: 4, 67, 70, 72, 74–76, 86, 89, 90, 95–96, 98
Countersubversive program: 72–73, 74–75, 84, 116, 162
Criminal Investigation Command, U.S. Army: 162–63
Criminal Investigation Division (CID): 140
Cryptanalysis/cryptanalysts: 30, 35, 37–38, 46–47, 48, 54, 59–60, 68–70, 77–80
Cryptology: 5–6, 9, 18, 29, 39, 42. *See also* Codes and ciphers.
between the wars: 46–47, 48, 54–55
Cold War and Korea: 102–03, 109–10, 111
diplomatic: 47, 54, 60, 77–78
Korea to Vietnam: 127, 128, 142
recapitulation and future trends: 191, 192, 193, 194, 195
reorganization and renewal: 171, 172, 177
Vietnam and beyond: 147, 148, 151, 164–65, 167
World War II: 59, 77, 94–95
Cuba: 13, 14, 18, 121, 145

D-day: 88–89
Da Nang, Vietnam: 148
Defense, Department of (DOD): 111, 122–23, 136, 153, 155, 164, 166
Defense Central Index of Investigations: 153
Defense HUMINT Service (DHS): 192. *See also* human intelligence.
Defense Intelligence Agency (DIA): 136, 137, 138, 139
reorganization and renewal: 176, 179, 183, 189, 192
Vietnam and beyond: 147, 149, 158, 159–60
Defense Intelligence School: 137–38
Defense Intelligence Service: 192
Defense Investigative Review Council: 162, 166
Defense Investigative Service: 162, 164, 191
Defense Language Institute: 138
Defense Mapping Agency: 164, 191
Defense Nuclear Agency: 166
Defense Supply Agency: 138
Denholm, Maj. Gen. Charles: 149
Denmark: 52
Department of Defense Reorganization Act (1986): 191
DESERT STORM. *See* Operation DESERT STORM.
Dewey, Admiral George: 14
DIA Production Center: 137
Diem, Ngo Dinh: 145
Dien Bien Phu, Vietnam: 121
Direct support units (DSU): 148
Director of Intelligence, U.S. Army: 104–05, 112
Directorate of Combat Intelligence: 138
Directorate of Foreign Intelligence: 137, 170
Directorate of Information Systems for Command, Control, Communications, and Computers: 193
Directorate of Security Intelligence: 138
Directorate of Surveillance and Reconnaissance: 138
Dirigible: 18, 46
Division of Military Information: 7, 12, 196. *See also* Adjutant General's Office.
Donovan, William J.: 56, 58, 63
Dos Passos, John: 41
Draft: 25, 27, 28, 29, 53, 161
Drug abuse: 161

Eastern Europe: 187
Economic Warfare, Board of: 62
Egypt: 121
Eisenhower, General Dwight D.: 5, 68, 86, 89, 92

Eisenhower administration: 121, 122, 123, 127
Eisenhower-Kishii agreement (1957): 135
Electronic intelligence (ELINT): 102, 113, 119, 122, 127, 128, 130, 142. *See also* electronic warfare; signals intelligence.
  reorganization and renewal: 171, 172, 174, 180–81, 193, 194
  Vietnam and beyond: 152–53, 161, 167
Electronic Training Group: 59
Electronic warfare: 6, 55, 82–83, 161, 167. *See also* Electronic intelligence; Signals intelligence.
  past and future trends: 188–89, 190, 193, 194
  reorganization and renewal: 171, 172, 174, 176, 181, 182
Engineer Intelligence Office: 92
Engineer Topographic Command: 160
Engineers, Corps of: 4, 9, 23, 35, 36, 64, 71, 129, 137
Engineers, topographic: 4, 8, 23, 34, 35, 36, 39, 92, 93, 98
Enigma: 68
Espionage: 23, 24, 25, 51, 53, 56
Europe: 110, 117, 126, 133, 164, 167, 189–90
European theater, World War II: 67, 69, 73, 82–83, 133
European Theater of Operations (ETO): 85, 88, 89, 90–91, 92, 96
Experimental Mechanized Force: 45

Fabyan, George: 30
Fairbanks, Alaska: 79, 110
Far East Command: 113, 114, 115, 117–18, 175. *See also* Pacific Command.
Federal Bureau of Investigation (FBI): 51, 52, 107, 110, 153, 154, 156
Federal Communications Act of 1934: 49
Federal Loyalty Program: 107–08
Fitch, Maj. Gen. Alva R.: 142
Forces Command, U.S. Army (FORSCOM): 174
Foreign intelligence: 24, 28, 40, 53, 56, 57, 70, 137, 138, 170, 175–76. *See also* Counterintelligence; Intelligence, positive.
Foreign Intelligence Command: 190
Foreign Science and Technology Center: 137, 189
Foreign Service and Technology Center: 176
Forney Board: 111
Forts
  Belvoir, Va.: 177, 185
  Bragg, N.C. 137, 147, 176
  Devens, Mass.: 112, 125, 143, 173, 185
  Gordon, Ga.: 140, 189
  Hancock, N.J.: 77
  Holabird, Md.: 107, 112, 122, 123, 124, 125, 127, 129, 138–39, 140, 141, 143, 160, 163, 175. *See also* Camp Holabird.
  Hood, Tex.: 180
  Huachuca, Ariz.: 127, 160–61, 163, 173, 185
  Hunt, Va.: 62, 77
  Leavenworth, Kans.: 11
  Lewis, Wash.: 114, 160
  McKinley, Philippines: 77
  Meade, Md.: 127, 163, 177, 190. *See also* Camp Meade.
  Monmouth, N.J.: 48, 49, 58, 68
  Richardson, Alaska: 98
  Riley, Kans.: 112, 125, 160
  Ritchie, Md.: 96
  Sam Houston, Tex.: 77
  Shafter, Hawaii: 77, 79
  Snelling, Minn.: 67
  Washington, Md.: 67
Foulois, Maj. Benjamin: 19
France: 12, 21, 22, 29, 38, 51, 52, 56, 76, 89, 92, 133
Frankfurt, Germany: 134
Freedom of Information Act Office: 165
Friedman, William F.: 46, 47, 48, 54, 55, 59–60, 94, 111
Froehlke, Robert F.: 156

G–2: 64–65, 70, 84, 89, 91–92, 94, 95–96, 97, 102, 103, 108, 114, 115, 116, 122–23, 124, 128, 130, 171, 172–73, 185
Garden Plot: 154–55
Gehlen, Maj. Gen. Reinhardt: 106
General Headquarters, Air Corps: 46
General Staff, European: 7, 14–15
General Staff, U.S.: 3–4, 14, 15, 16, 17, 18, 21, 23, 24, 28, 31, 42, 43, 103–04
Geographic Service, Allied: 95
Geographic Specialist Detachment, U.S. Army: 123
German Americans: 25
Germany: 12, 17, 21, 41
  under Nazis: 51, 52, 55, 76, 82–83, 91–92, 98–99

Germany (cont.)
after World War II: 101, 108–09, 116, 129, 130, 133–34, 175
Gettysburg, Penn.: 9
Godding, Maj. Gen. George: 167, 172
Goodfellow Air Force Base, Tex.: 173
Graves, Maj. Gen. William S.: 39
Great Britain: 12, 13, 14–15, 22, 29, 53, 59, 68, 84, 85, 89. *See also* Britain.
Greece: 101
Greenhow, Rosa: 10
Guam: 79, 93
Guerrilla warfare (Vietnam): 147, 151
Gulf War. *See* Operation DESERT STORM.

Haig, Field Marshal Sir Douglas: 43
Haines Board: 158
Harding, Warren G.: 41
Harrisburg, Penn.: 66, 67
Hawaii: 61, 110, 135, 166
Helemano, Hawaii: 110
Helicopters: 131–32, 150, 152, 180–81
Hemisphere Intelligence Command, American: 66
Herzo Base, Germany: 110
Hitler, Adolf: 51, 52
Hitt, Capt. Parker: 18, 29
Homestead, Fla.: 142
Hooker, Maj. Gen. Joseph: 10
Hoover, J. Edgar: 154
Hoover Commission: 125
Hopkins, Harry: 75
Howard, Michael: 187
Human intelligence (HUMINT): 117–18, 122, 124–25, 126, 134, 135, 138
reorganization and renewal: 170, 174–75, 177, 180, 190, 191, 192
Vietnam and beyond: 148, 156, 158, 166
Huston, Frederick: 162

Imagery interpretation: 181. *See also* Photographic reconnaissance.
Imagery Interpretation Center, U.S. Army: 140, 159, 163, 181. *See also* Photo Interpretation Center.
India-Burma theater: 62, 80
Indian scouts: 8, 11, 19
Industrial security program: 123, 138
INSCOM. *See* U.S. Army Intelligence and Security Command.

Intelligence. *See also* Army Intelligence; Military Intelligence.
civilian: 9, 25, 26, 125–26
collection: 4, 7–8, 155, 174–75, 178–79
attaches: 12, 13, 14, 15, 16, 17, 20, 22–23, 24, 28, 36, 42, 43, 44, 45–46, 51, 52, 53, 55, 65, 105–06, 109, 113, 122, 137–38, 165, 174–76, 191, 192
multidisciplinary approach: 174–75, 178–79
scouts: 8, 10, 11, 19
technology: 18, 19, 30, 33–34, 56. *See also* technology, influence of.
combat: 33–34, 45, 59, 64, 76, 112, 125, 130, 138, 142, 148, 157–58, 161
communications. *See* Communications intelligence (COMINT).
domestic: 154, 155, 156, 161–62, 191, 192. *See also* civil disturbance.
economic: 105, 146, 191, 192
electronic. *See* Electronic intelligence (ELINT).
foreign. *See* Foreign intelligence.
human. *See* Human intelligence (HUMINT).
joint: 62, 63, 93, 147, 152
negative: 23, 24, 27, 31, 44. *See also* Counterintelligence.
political: 105, 191, 192
positive: 23, 24, 27, 31, 92, 98, 109, 113
production: 174, 176, 178–79, 180–81, 189, 191, 192, 194
radio. *See* Radio intelligence.
role of: 4, 5, 6
signals. *See* Signals intelligence (SIGINT).
specialists: 91–92, 118, 183–84
strategic: 106, 112, 113, 119, 125, 137, 139, 189–90
support of occupation forces: 108–09
tactical. *See* Tactical intelligence.
technical: 91–92, 97, 116, 127, 129–30, 131–33, 141–42, 166–67, 177–78, 180–81, 194. *See also* Technology, influence of.
topographic: 91, 92, 95, 123, 164
training: 66–67
Intelligence Agency, U.S. Army (USAINTA): 165, 166, 171, 172, 177
Intelligence Center, Europe, U.S. Army: 158
Intelligence Center and School, U.S. Army: 161, 165, 173, 179, 184–85

Intelligence Command, U.S. Army (USAINTC): 141, 153–55, 156–57, 159–60, 161–63, 165–66, 170
Intelligence Corps: 126, 127, 138–39, 142, 147, 196
Intelligence Corps Command, U.S. Army: 139–40, 141
Intelligence, Deputy Chief of Staff for (DCSINT): 184, 189
Intelligence Division: 103–04, 105, 106–07, 109, 112, 115
Intelligence Group, Central: 103, 104–05
Intelligence Materiel Development Support Office: 141
Intelligence Materiels Supply Office: 159
Intelligence Organization and Stationing Study (IOSS): 169–70, 171–72, 173–74, 176, 179, 180, 193, 194
Intelligence Police, Corps of (CIP): 26–27, 32, 42, 44, 52, 53, 57–58
Intelligence School, Army Air Forces: 66, 67–68
Intelligence School, Pacific, U.S. Army: 135
Intelligence and Security Command, U.S. Army (INSCOM): 174–76
  future trends: 188, 189, 190, 193, 196
  reorganization and renewal: 177, 178, 179, 183, 184–85
Intelligence and Threat Analysis Center: 174, 175, 176, 189
Intercept operations: 23, 30, 33, 35, 40, 49, 78, 79, 93
Interrogation personnel: 91, 93, 95, 96, 98, 130, 148–49, 180
Investigative Records Repository (IRR): 153, 155, 162, 163, 165, 175
Iranian hostage crisis: 169
Iraq: 188, 190
Irish Americans: 25
Iron Curtain: 133, 187
Italian front: 33, 38
Italy: 51, 76, 87, 89, 92

J–2. *See* Intelligence, joint.
Jackson, Lt. Gen. Thomas J. ("Stonewall"): 9
Japan: 13, 15, 51, 53, 55, 83, 93, 98, 108–09, 114, 116, 118, 133, 135, 147, 166
Japanese linguists: 67, 108–09. *See also* Language training; Linguists.
Japanese military communications: 77–78, 79, 93, 95. *See also* Cryptanalysis; Purple.
Johnson, Andrew: 11
Johnson, Lyndon B.: 145
Johnson administration: 146, 156
Joint Chiefs of Staff (JCS): 62–63, 80, 91–92, 93, 110, 123, 150–51, 167, 191
Joint Intelligence Center, Pacific Ocean Area (JICPOA): 93
Joint Intelligence Committee (JIC): 62, 63
JUST CAUSE. *See* Operation JUST CAUSE.
Justice, Department of: 25, 29

Kellogg-Briand Pact: 47
Kennedy, John F.: 121–22, 136, 145
Kibler, Col. Harold R.: 75
King, Admiral Ernest: 61, 80
King, Martin Luther, Jr.: 156
Knox, Frank: 61
Korea
  postwar: 129, 130, 133, 134, 135, 166, 167, 175
  in wartime: 101, 113–14, 116, 118
Korean War: 102, 111, 113, 115, 116, 117, 118, 119, 121, 124, 129, 131–32, 151, 184, 194
Kuhn, Brig. Gen. Joseph: 22, 85
Kullback, Solomon: 48
Kunia, Hawaii: 177
Kuwait: 188

Land Information Warfare Activity (LIWA): 190
Langres, France: 33
Language training: 58, 67, 112, 135, 138, 147. *See also* linguists.
LANTERN SPIKE (domestic intelligence collection plan): 155
Latin America: 53–54, 55, 66, 70, 84
League of Nations: 41
Lewis, [Meriwether] and Clark, [George Rogers]: 8
Liddell Hart, Basil: 22
Lincoln, Abraham: 11
Linguists: 95, 96, 112, 115, 130, 131, 149, 179, 182–83. *See also* language training.
Long, Lt. W. D.: 44
Longstreet, Lt. Gen. James A.: 9
Low-intensity conflict: 177
Luzon, Philippines: 94
M209: 119, 128
MacArthur, Capt. (later General) Douglas: 16–17, 78, 80, 93–94, 95, 96, 114
McChristian, Maj. Gen. Joseph A.: 147, 148, 160

McClellan, Maj. Gen. George B.: 10
McCloy, John J.: 70
McCormack, Col. Alfred: 65, 71, 80
McNamara, Robert S.: 121–22, 136, 137
McNamara reforms: 136–39, 141–42, 172
McNarney, Lt. Gen. Joseph: 61–62, 74
MAGIC: 54–55, 59–60, 65
Manhattan Project: 75, 91–92
Manila, Philippines: 14
March, General Peyton C.: 31
Marine Corps, U.S.: 93, 95
Marshall, General George C.: 43–44, 52, 63, 80
Marshall Plan: 101
Marshall, S. L. A.: 4
Massive retaliation strategy: 121–22
Measurement and signature intelligence (MASINT): 194
Medical Corps: 64
Medical Intelligence and Information Agency: 176
Mediterranean: 51, 83
Mediterranean Theater of Operations (MTO): 85, 86, 89, 90, 92
"Message to Garcia": 13
Mexican War: 8
Mexico: 8, 13, 16–17, 19
Miami, Fla.: 66, 70
Micronesia: 76
Middle East: 62
Miles, Brig. Gen. Sherman: 53, 55–56
Military Academy, U.S.: 8
Military Assistance Command, Vietnam (MACV): 145, 147, 148, 150, 152, 159
Military Assistance Command, Vietnam, Studies and Observation Group: 150–51
Military attaches, intelligence role of: 12, 13, 14, 15, 16, 17, 24, 28, 36
  between wars: 33, 42, 43, 45–46, 55
  after World War II: 105, 109, 113, 122, 137–38, 165
Military District of Washington (MDW): 103, 106, 139
Military Information Committee: 16–17, 22
Military Information Division: 13, 14, 18, 22, 33, 34, 35, 36, 37–38, 40, 43, 45, 57
Military Intelligence: 3–7, 21. *See also* Army Intelligence.
  definition of: 24, 32, 39, 124
  past and future trends: 188, 191, 193, 195, 196
Military Intelligence (cont.)
  reorganization and renewal: 136, 171, 179, 183, 184–85
  staff: 27, 28, 29, 31, 32, 52, 56
Military Intelligence Battalions: 130–31, 133, 177, 178–79, 181–82, 193
  24th: 182
  29th: 188
  201st: 177
  202d:177
  203d: 177
  319th: 130
  502d: 130, 134
  519th: 130, 147, 148
  522d: 180
  532d: 130, 133–34
Military Intelligence Branch: 28–30, 31, 32, 37, 46–47, 157–58, 172, 173, 195
Military Intelligence Brigades: 178–79
  470th: 188
  504th: 188
  513th: 188
  525th: 188
  701st: 179
  702d: 189
  703d: 179
  704th: 179
Military Intelligence Committee: 19
Military Intelligence Companies
  11th: 177
  319th: 108–09, 112, 130
Military Intelligence Corps: 6, 111, 184
Military Intelligence Detachments: 166
Military Intelligence Division (MID): 5, 6, 22, 31–32. *See also* Military Intelligence Service.
  between the wars: 40, 41, 42, 43, 44, 45, 46, 47, 51, 53, 54
  reorganization of: 63–68, 69–71, 103–04, 119, 136
  in World War II: 59–60, 61–62, 80, 84, 92, 102
Military Intelligence Division Special Branch: 65, 66, 68–69, 70–71, 80
Military Intelligence Groups: 147–48, 153, 157, 162–63
  66th: 157
  109th: 163
  135th: 147–48
  149th: 148
  470th: 174

Military Intelligence Groups (cont.)
500th: 165–66, 174
501st: 175
513th: 157, 177–78
902d: 159, 163, 175, 178
reorganization and renewal: 172, 174–75, 177, 178, 182, 189
Military Intelligence Officers Reserve Corps (MIORC): 45, 58, 113, 116, 149
Military Intelligence Organization: 130, 133, 194
Military Intelligence Section: 22–23, 24, 25, 27, 28, 29
Military Intelligence Service (MIS): 5, 64–65, 66, 67, 69–72, 74, 83–84, 85, 90–91, 97, 104, 172–73. *See also* Military Intelligence Division.
Military Intelligence Service Groups: 116. *See also* Military Intelligence Groups.
500th: 116, 135
513th: 116, 133–34
525th: 116
Military Intelligence Service Language School: 67, 112
Military Intelligence Service Organization: 112, 116
Military Intelligence Training Center (MITC): 66–67, 76, 96, 98, 112
Military Personnel Center: 175
Military Reservations Division: 8, 12
Moscow, Russia: 116
Mozambique: 169
Munich, Germany: 157
Mussolini, Benito: 51

National Agency Check Center: 153
National Army: 25
National Defense Act: 21, 42, 52, 191
National Ground Intelligence Center: 189
National Guard: 21, 25, 42, 49, 182
29th Infantry Division (Maryland-Virginia): 182
Utah: 182–83
National security: 25, 26, 29
National Security Agency (NSA): 111, 127, 136, 138, 139, 158, 164, 171, 191, 192
National Security Council (NSC): 105
Navy, U.S.: 11, 54, 58–59, 60, 93, 95
Navy Intelligence: 62–63, 80
Nazis: 51, 52, 68
New Delhi, India: 79
New York City, N.Y.: 25, 27, 53, 55, 66, 70–71, 72, 79
Nha Trang, Vietnam: 148
Nimitz, Admiral Chester W.: 93
Nisei: 67, 93, 95, 108–09, 112
Nixon, Richard M.: 164, 169
Nixon administration: 146
Nolan, Capt. (later Maj. Gen.) Dennis E.: 17, 26, 32, 40, 185
Noriega, General Manuel: 187–188
Normandy, France: 76
Norris Board: 157, 158
North Africa: 58, 61, 62, 63, 68, 73, 87, 89
North African Theater of Operations (NATO): 85, 86–87, 89, 90, 92. *See also* Mediterranean Theater of Operations (MTO).
North Atlantic Treaty Organization (NATO): 101, 102
North Korea: 113, 114, 116–17
North Vietnam: 121, 145
North Vietnamese: 145–46
Norway: 52
Nuclear weapons: 121

Oberursel, Germany: 133
Observation groups: 46, 97, 113
Observation posts: 34
Office of the Assistant Chief of Staff, G–2: 115
Office of the Assistant Chief of Staff for Intelligence (OACSI): 123, 137, 138, 147, 158, 159–60, 165, 173, 175
Office of the Chief of Engineers: 137
Office of Naval Intelligence (ONI): 11, 53, 62–63
Office of the Secretary of Defense: 163
Office of Strategic Services (OSS): 63, 66, 92, 95, 96, 103
Office of the Surgeon General: 137, 170, 176
Okinawa: 135
Operation DESERT STORM: 188, 189, 190
Operation JUST CAUSE: 187–88, 189
Operation TORCH: 63
Operational Security Group: 166
Operations security (OPSEC): 171, 174, 175, 176, 178, 190
Opposing forces (OPFOR) training program: 177–78
Order of battle teams: 91, 112
Ordnance Corps: 64, 137
Organization of Petroleum Exporting Countries (OPEC): 169

Orlando, Fla.: 67

Pacific Command: 110, 133, 134–35. *See also* Far East Command.
Pacific Ocean Area (POA): 85, 93
Pacific theater, World War II: 60, 61, 69, 76, 80, 85–86
Panama: 55, 166, 177, 187, 189, 190. *See also* Canal Zone.
Paris, France: 92
Paris Peace Accords: 146, 153
Paris Peace Conference: 41–42
Parker, Maj. Gen. Julius: 184
Pearl Harbor, Hawaii: 53, 60, 62, 64–65, 77, 78, 82, 104, 116
Pentagon: 136
Permanent intelligence units: 179–80, 181
Pershing, Brig. Gen. (later General) John J.: 19, 21, 23, 31, 32, 33, 40, 43
Persian Gulf War: 188, 194. *See also* Operation DESERT STORM.
Personnel Security Group: 159, 163
Philippine insurrection: 14, 24
Philippines: 14, 15, 18, 39, 53, 76, 93, 95, 96, 148
PHOENIX: 151
Photo Interpretation Center: 125. *See also* Imagery Interpretation Center, U.S. Army.
Photo interpreters: 23, 33, 91, 112, 130, 131, 132
Photographic reconnaissance: 34–35, 39, 46, 97, 122. *See also* Imagery interpretation.
Phu Bat, Vietnam: 148, 151
Pinkerton Agency: 27
Pinkerton, Alan: 10
Pleasanton, Maj. Gen. Alfred: 10
Poland: 52
Polygraph: 107
Presidio of Monterey, Calif.: 112
Presidio of San Francisco, Calif.: 58, 67, 77
Professionalism: 195, 196
Project 80: 137
Project ACSI-MATIC: 122
Project MICHIGAN: 119, 184
Project SECURITY SHIELD: 139
Project VANGUARD: 187
Propaganda: 56, 57, 63, 103
Protective Mobilization Plan: 49
Provisional Radio Intelligence Detachment: 48
Provost Marshal General's Office: 58, 75, 107, 122, 138, 139, 140
Psychological warfare: 66, 92–93, 190
Public relations: 36–37, 40, 43, 45, 58
Puerto Rico: 13
PUNCH BLOCK: 155
Punitive expedition: 19
Purple: 54–55, 59, 68, 77
Pyongyang, North Korea: 116–17

Quartermaster Corps: 9, 64, 129

Racial unrest: 146, 161
Radar: 45, 55, 59, 82–83, 113, 132–33, 180, 181, 194
Radio Corporation of America (RCA): 122
Radio Group Forward (RAGFOR): 93
Radio intelligence: 35, 45, 49, 56, 82–83. *See also* signals intelligence.
  1st Radio Intelligence Company: 48–49, 59
  postwar: 103, 119, 147–48, 150
  World War II: 86, 88, 93, 94–95, 98
Radio Research Units (RRU): 141, 147, 148, 152
Radio-telephone: 149
Radio tractors: 18–19, 30
Readiness Training (REDTRAIN): 183
Reconnaissance: 7, 17, 19. *See also* communications intelligence; radio intelligence.
  1st Reconnaissance Battalion: 95
  reorganization: 180–81
  in wars: 34–35, 39, 95–96, 97, 150
Redstone Arsenal, Ala.: 129, 137
Regular Army: 53, 182–83, 184
Regular Army officers: 6, 23, 83, 142–43
Reorganization Objective Army Division (ROAD): 122, 179
Republic of Korea (ROK). *See* Korea.
Republic of Vietnam. *See* South Vietnam.
Resada, Calif.: 79
Reserve components: 161, 183
Reserve officers: 6, 142–43, 149, 195
Ridgway, General Matthew B.: 114, 115, 124
Riverbank Laboratories, Ill.: 30, 37, 46
Rolya, Brig. Gen. (later Maj. Gen.) William L.: 174
Rome, Italy: 92
Roosevelt, Franklin D.: 51, 52, 56, 81
ROSE HILL: 155
Rowan, Lt. Albert: 13
Rowlett, Frank: 48, 55
Royal Australian forces: 94

Russia: 12, 38–39, 41, 113. *See also* Soviet Union.
Russian Institute, Germany: 175, 190
Ryan, Maj. James A.: 19

Saigon, Vietnam: 145, 148
San Francisco, Calif.: 55, 58, 66, 67, 70
Santiago, Cuba: 14
Satellites: 121
Saudi Arabia: 188
Scandinavian Americans: 25
Scientific Advisory Board: 167
Scott, Maj. Gen. Hugh: 22
Scouts, use of: 8, 10, 11, 19. *See also* Intelligence collection.
Searchlight platoons: 35
Security Agency, Pacific, U.S. Army: 135
Security Agency, U.S. Army (USASA): 129, 135, 138–39, 141–42, 149, 167, 174
Security Agency Board, U.S Army: 128–29
Security Agency Groups, U.S. Army: 129, 135
  321st: 135
  502d: 164
  507th: 164
  508th: 135, 164
Security Agency Training Center and School, U.S. Army (USASATC&S): 143
Security Intelligence Corps: 103
SECURITY SHIELD. *See* Project SECURITY SHIELD.
Services of Supply: 63–64. *See also* Army Service Forces.
Seward, William Henry: 10
Sharpe, Col. George V.: 10, 11
Sheen, Lt. Col. H. Gordon: 98
Siberia, Russia: 38–39
SIGABA: 81, 106, 110
Signal Corps: 4, 5, 6, 9, 14. *See also* Signal Intelligence Service; Signal Security Agency.
  between wars: 45, 46, 47, 48, 49, 52
  Korea to Vietnam: 127, 128, 129–30, 142
  retrospective: 193, 194, 195
  World War I: 17–18, 23, 30, 35, 37
  World War II: 64, 68, 91–93, 94, 95, 98
Signal Corps Code Compilation Section: 37–38
Signal information and monitoring (SIAM): 89
Signal Intelligence Division: 86, 87, 88, 89
Signal Intelligence Service (SIS): 46–49, 52, 54–55, 58–59, 64, 65, 77, 94
Signal radio intelligence: 86, 87–88, 89, 94–95, 98. *See also* radio intelligence.
Signal Security Activity: 166
Signal Security Agency. *See also* Signal Corps; Signal Intelligence Service.
  Protective Security Branch: 82–83
  signal service battalions: 52, 77–78, 79, 82, 83, 94, 110, 164
  signal service companies: 89, 95, 114
  World War II: 67–68, 77–78, 79–80, 81–84, 85, 98, 102, 173
Signal Service Battalion, 2d: 52, 77–78, 79, 94, 110, 164
Signals intelligence (SIGINT): 85, 86, 91–93, 109, 111, 112, 113, 122, 128, 136, 142, 167, 170–71, 172, 175, 179, 181, 184, 189, 194. *See also* Electronic warfare; Tactical intelligence.
SIGROD: 110
SIGSALY: 81
Sinkoy, Col. Abraham: 48, 94
South Korea: 101, 146. *See also* Korea.
South Vietnam: 121, 145, 150, 151, 153. *See also* Vietnam.
South Vietnamese: 146, 148–49
South West Pacific Area (SWPA): 85, 93–97
Southeast Asia: 145–46, 147, 157, 158, 169
Soviet Union: 99, 104, 136, 145, 187. *See also* Russia.
Soviets: 101, 121, 139, 169, 187, 189
Special Access Program (SAP): 178
Special Forces, Vietnam: 150–51
Special Research Detachment: 138, 158–59, 160, 163
Special Security Group: 166, 173, 175, 189
Special security officers (SSOs): 69, 104, 115, 150, 158–59, 171–72, 189
Special Security System: 104
Spies: 9, 10, 28, 29
Stalin, Josef: 121
Stars and Stripes: 37
State Department: 31, 47, 58, 62
State, War, and Navy building: 13
STEADFAST: 161, 165, 170, 172
STEEP HILL. *See* GARDEN PLOT.
Stimson, Henry: 47, 61, 65
Strategic Intelligence School: 106, 112, 125, 137, 139
Strategic Services Unit: 103
Strong, Maj. Gen. George V.: 64, 69, 72
Stuttgart, Germany: 133
Subversion: 25, 28, 29, 53, 54, 55
Sultan, Lt. Gen. Daniel I.: 80

Table of distribution/table of distribution and allowances (TD/TDA): 108, 118, 129, 133, 135, 159, 165, 177, 178, 179, 183, 196
Table of organization and equipment (TOE): 88–89, 108, 112, 129, 132, 140, 150, 159, 164, 179, 180–81, 183, 194
Tactical intelligence: 8, 190, 194. *See also* Signals intelligence (SIGINT).
  Cold War, Korea, and Vietnam: 113, 115, 117–18, 129, 130–31
  reorganization and renewal: 171, 175, 177, 179, 180–81, 182, 184
  Vietnam and beyond: 150, 151, 160, 167
  World War II: 73–74, 75–76, 79, 86, 87, 88, 89, 91, 94–95, 96–97, 98
Tan Son Nhut Air Base, Vietnam: 148
Taylor, Maj. Gen. Zachary: 8
Technical Service Countermeasures teams: 116
Technology, influence of: 4, 6, 9, 11, 19. *See also* Communications intelligence; ULTRA.
  between the wars: 45–46, 48–49, 54–55
  past and future trends: 188–89, 191, 193–94. *See also* electronic warfare.
  Vietnam and beyond: 130–33, 146, 152, 157, 180, 184
  World War I: 29–30, 33–35, 39–40
  World War II and Korea: 91–92, 96–97, 98–99, 116, 119
Telegraph: 9, 30, 35
TEMPEST: 128–29, 166
Tet offensive: 146, 152–53
Thailand: 148
Theaters of operations, World War II: 85, 92
Thorpe, Brig. Gen. Elliot: 96
Tokyo, Japan: 135
TORCH. *See* Operation TORCH.
Training and Doctrine Command, U.S. Army (TRADOC): 165, 178, 180
Transportation Corps: 64, 72
Treasury Department: 25
Troy, Thomas: 43
Trudeau, Maj. Gen. Arthur C.: 125
Truman, Harry S.: 103, 107
Truman administration: 106
Turkey: 101, 175
Two Rock Ranch, Petaluma, Calif.: 110

ULTRA: 68–69, 86, 87, 94
Union of Soviet Socialist Republics (USSR). *See* Soviet Union.
United Nations: 101, 116
United Nations Partisan Forces: 118, 134
United States: 22, 25, 39, 51, 53, 56, 59. *See also* America.
  from Korea to Vietnam: 101, 117, 121, 126, 129, 130–31, 136
  Vietnam and beyond: 146, 157, 188
  in World War II: 61, 62, 68, 84, 93, 98–99
U.S. Armies
  First: 106
  Second: 106, 139
  Third: 42, 106
  Fourth: 58, 67, 106
  Fifth: 89, 106
  Sixth: 97, 106
  Seventh: 89, 132, 133, 134, 174
  Eighth: 114, 115, 117, 118, 133, 134, 135, 175
U.S. Army: 3–4, 8, 14–15, 18–19, 21, 22–23, 27–28. *See also* Army Intelligence.
  demobilization of: 101, 107
  interwar difficulties: 42, 51–60
  in World War II: 83–99
U.S. Army, Europe (USAREUR): 115, 133, 134, 158, 172, 174
U.S. Army, Pacific (USARPAC): 135, 149, 165
U.S. Army Command Reconnaissance Activity, Pacific: 135
U.S. Army Corps of Engineers. *See* Engineers, Corps of.
U.S. Army Forces, Far East (USAFFE): 95–96, 134–35
U.S. Army Forces, Pacific (AFPAC): 96
U.S. Communications Intelligence Board (USCIB): 110, 123
U.S. Intelligence Board (USIB): 123
Ursano, Maj. Gen. Joseph J.: 170
Ursano panel: 170–72

Van Deman, Maj. (later Maj. Gen.) Ralph: 18, 22–30, 40
Van Fleet, General James: 115
Vance, Cyrus: 155
Viet Cong: 145–46, 159
Vietnam: 150, 157, 158, 159, 160, 161, 166, 188. *See also* North Vietnam; South Vietnam.
Vietnam War: 146, 157, 160, 164, 187, 192
Vietnamese Civilian Irregular Defense Groups: 150

Villa, Pancho: 19
Vint Hill Farms Station, Va.: 67, 78, 110, 112, 166, 177

War College Division: 16, 17, 20, 22
War Department: 4, 5, 6, 8, 14
  postwar: 103, 104
  World War I: 17, 21, 22, 23, 24, 25, 26, 27, 28, 31, 34, 37, 39
World War II: 57, 72, 80, 84, 88, 90
War Department Operations Division: 63
War of 1812: 8
War with Spain: 12, 13, 14
Warsaw Pact: 187
Washington, D.C.: 13, 14, 16, 18, 22, 25, 28, 52, 68, 70, 72–73, 74, 77, 116, 161
Washington Barracks, Washington, D.C.: 16
Washington Navy Yard: 176
Washington Peace Conference: 47
Watergate scandal: 146, 169
Wedemeyer, Lt. Gen. Albert J.: 80
Weinstein, Lt. Gen. Sidney T.: 184
Western front: 33, 34
Westmoreland, General William: 159, 160
Weyand, General Frederick: 170
Williams, Maj. (later Col.) Garland: 57, 116
Williams, Lt. Gen. James A.: 183
Willoughby, Brig. Gen. Charles: 94, 96
Wilson, Woodrow: 40, 41
Wilson administration: 19–20, 21
Wireless: 18. *See also* Radio intelligence; Signals intelligence; Technology.
Women's Army Corps (WAC): 107, 164
World War I: 4, 15, 17, 19–20, 22–24, 34–40, 41, 92, 141
World War II: 5, 6, 61, 84–99, 159, 171, 172–73, 187, 193, 194

Yardley, Maj. Herbert O.: 29, 42, 47
Yom Kippur War: 169

PIN : 075005-000

U.S. ARMY SIGNALS INTELLIGENCE IN WORLD WAR II

A DOCUMENTARY HISTORY

Edited by
James L. Gilbert
and
John P. Finnegan

U.S. ARMY SIGNALS INTELLIGENCE IN WORLD WAR II

A DOCUMENTARY HISTORY

Edited by
James L. Gilbert
and
John P. Finnegan

CENTER OF MILITARY HISTORY
UNITED STATES ARMY
WASHINGTON, D.C., 1993

Library of Congress Cataloging-in-Publication Data

U.S. Army Signals Intelligence in World War II: a documentary history
/ edited by James L. Gilbert and John P. Finnegan.
p. cm.
1. World War, 1939–1945—Military intelligence—United States—
History—Sources. 2. World War, 1939–1945—Cryptography—History—
Sources. 3. United States. Signal Security Agency—History—
Sources. I. Gilbert, James L. (James Leslie), 1943–
II. Finnegan, John Patrick.
D810.S7U7 1993
940.54'85'0973—dc20 92–43143
CIP

CMH Pub 70–43

First Printing

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328
ISBN 0-16-037816-8

Foreword

This book is part of the Army historical community's commemoration of the fiftieth anniversary of World War II. American victory in that conflict was brought about not only by the valor of our fighting men and the immensity of our productive capacity, but also by the availability of superb military intelligence. Much of this intelligence came from the ability of our armed forces to intercept and decipher the most secret communications of their adversaries. For many years security considerations prevented any public mention of these successes in the official histories. Now much of the story can be told. To preserve the memory of the Army's role in this intelligence war, the U.S. Army Center of Military History has joined with the History Office, U. S. Army Intelligence and Security Command (INSCOM), to publish this collection of documents on Army signals intelligence in World War II. INSCOM carries on the heritage of the Army's World War II Signal Security Agency, which by breaking the Japanese diplomatic ciphers and military codes helped speed the way of our forces to victory.

The book is intended both for an Army audience and for the general public—including those World War II veterans who participated in the signals intelligence war and who for so many years were constrained to keep their contributions secret. The security barriers have now been lifted, and the Army is proud to acknowledge those contributions.

HAROLD W. NELSON
Brigadier General, USA
Chief of Military History

CHARLES F. SCANLON
Major General, USA
Commanding General
U.S. Army Intelligence and
Security Command

Preface

The Army's contributions to the success of the American communications intelligence—COMINT—effort in World War II are not widely known. This volume represents a modest attempt to close this information gap. The core of the book consists of World War II–era documents generated by various cryptologic organizations of the U.S. Army. Originally, most of these documents were highly classified. As a result of initiatives undertaken in the 1970s, they have now been released to the National Archives and Records Administration in the form of Special Research Histories after declassification by the National Security Agency. The documents included necessarily represent only a small fraction of the material that is now in the public domain. It is hoped that the publication of this book will help to alert the public to the existence of this relatively unexplored mass of historical documentation. Although these materials are being increasingly used by professional historians, only two collections of these documents have yet been published. In 1977, the Department of Defense released a multivolume compilation entitled *The "Magic" Background of Pearl Harbor*; more recently, Dr. Ronald Spector has edited *Listening to the Enemy: Key Documents on the Role of Communications Intelligence in the War with Japan*. We can assure the reader that the present volume does not exhaust the possibilities of further exploiting this largely untapped source.

The documents themselves consist for the most part of official histories and government memoranda. For the sake of variety, we have also included one highly unofficial history and examples of intelligence reports and intercepted messages. Some of the documents have been rather heavily sanitized before release, as is indicated by the [text withheld] notations liberally sprinkled through them. It should be pointed out that the declassification/sanitization process went on for a number of years (and is still continuing), and that guidelines as to the releasability of material have changed during this period. As a result, the careful reader will note certain inconsistencies. The editors of this volume have made no attempt to reverse any of the original declassification decisions. They have, however, not hesitated to abridge documents that were overly long or treated subjects repetitively. The editors have also chosen to eliminate those portions of documents that had been so

heavily sanitized as to render them less than intelligible. Those who are curious about what we may have omitted may check the original documents at the National Archives and Records Administration. It should be noted that most typographic mistakes in the originals have been retained.

No book comes into existence without some type of collaborative process going on, and this one is no exception. We would like to begin by thanking Col. James H. P. Kelsey, Deputy Chief of Staff, Operations, U.S. Army Intelligence and Security Command, for the unfailing support he has provided to the History Office in all of its projects. The manuscript itself was prepared and proofread by Ms. Diane L. Hamm, the History Office writer-editor. John Elsberg of the U.S. Army Center of Military History did much to enhance the final product through astute editing and wise counsel. John Greenwood, Chief of the Center of Military History's Field and International Division, made arrangements for an earlier version of the introductory essay to be presented at the 1990 Army Historians Conference. John Birmingham designed and formatted the final product, working closely with the authors and the editorial staff. Finally, we would be remiss if we did not thank the numerous declassification specialists at the National Security Agency whose dedicated work made the publication of this book ultimately possible.

Fort Belvoir, Virginia

JAMES L. GILBERT
JOHN P. FINNEGAN

Contents

Chapter *Page*

I. U.S. ARMY SIGNALS INTELLIGENCE IN THE SECOND WORLD WAR: AN OVERVIEW 3

II. THE ROAD TO PEARL HARBOR 17

SRH 29: A Brief History of the Signal Intelligence Service (excerpt,1945) 18

1. Riverbank Laboratories 18
2. Cryptanalysis in World War I 18
3. Relocation of MI-8 19
4. Radio Intercept 20
5. Yardley's Organization 21
6. Deficiencies of Interwar Organization 22
7. Impact of Secretary Stimson 23
8. The End of Yardley 24
9. The Beginnings of the SIS 25
10. Navy Efforts 25
11. Conclusion 26

SRH 134: Expansion of the Signal Intelligence Service from 1930 to 7 December 1941 (1945) 26

SRH 135: History of the Second Signal Service Battalion, Appendix; Memorandum to Adjutant General: Signal Intelligence (1938) 37

"Magic" Background of Pearl Harbor, Volume IV, Appendix. Washington-Tokyo Message #812 39

SRH 115: U.S. Army Investigations Into the Handling of Certain Communications Prior to the Attack on Pearl Harbor: Testimony of Brig. Gen. Hayes W. Kroner (excerpt, 1944) 40

Note: SRH numbers refer to Special Research Histories: declassified/sanitized cryptologic documents released to the National Archives and Records Administration by the National Security Agency.

Chapter *Page*

III. ACCEPTING THE CHALLENGE 47

SRH 116: Origins, Functions and Problems of the Special Branch, M.I.S. (1943) 48
Responsibilities of War Department for Intelligence Derived from Cryptanalysis 48
Handling of Intercept Intelligence Prior to War 49
Decision of the Secretary of War Concerning Exploitation of Cryptanalytic Field 49
Organization of MIS Section to Handle Intercepts 50
Organization of Special Branch 50
Work of the Special Branch 51
Increase in Volume of SSD Material 54
Basic Factors in the Problem of Cryptanalytic Intelligence 55
Personnel Situation of the Special Branch — Officers and Civilians 60

SRH 141–2: Papers from the Personal Files of Alfred McCormack, Colonel, AUS, Special Branch, G-2, Military Intelligence Division, War Department General Staff; Memorandum for Colonel Clarke: Personnel Problems, B Section, Special Branch (1944) 63

IV. TRAINING THE FORCE 67

SRH 358: History of the Training Division, Signal Security Agency; History of Schooling of Commissioned Officers in the Vint Hill Farms School (1945) 68
10 March 1942 to 5 October 1942 68
5 October 1942 to Date 69

"Third Battle of Manassas" (excerpt, 1944) 72
They Fell Out in Front of the Orderly Room 72
Administration for All Concerned 77
Education in Darkest Virginia 80

V. CRACKING THE CODES 87

SRH 349: Achievements of the Signal Security Agency in World War II (excerpt, 1945) 88
I. Building the Organization 88
II. The Production of Information 94

Chapter *Page*

A. Interception 94
B. Traffic Analysis 96
C. Cryptanalysis 97
D. Solutions 99
1. Japanese Diplomatic and Military Attache Traffic 100
2. Japanese Army and Air Force Traffic 101
4. German Army and Air Force Traffic 108
8. Commercial Code Traffic 110
9. Special Problems 110
E. Some General Remarks 110
Central Bureau History (1950) 112
SRH 280: An Exhibit of the Important Types of Intelligence Recovered Through Reading Japanese Cryptograms (excerpt). Berlin-Tokyo Message #756, 1944 113
1. Weapons Connected with the Army 114
2. Weapons Connected with the Navy 115
3. Weapons Connected with the Air Force 115
4. Equipment for Long Distance Bombardment 116

VI. PRODUCING INTELLIGENCE 117
SRH 185: War Experience of Alfred McCormack (excerpt,1947) 118
SRH 141–2: Papers from the Personal Files of Alfred McCormack; Memorandum for Mr. McCloy: Personnel Situation of Special Branch, M.I.D. (excerpt,1943) 128
SRH 005: Use of MX/CSS Ultra by War Department; European Summary of 11 April 1945 130

VII. DISSEMINATING THE PRODUCT 135
SRH 026: Marshall Letter to Eisenhower (1944) 136
SRH 033: History of the Operations of Special Security Officers Attached to Field Commands, 1943–1945 139
SRH 031: Trip Reports—ULTRA in the Mediterranean; Report of Lt. Col. Rood (1944) 145
SRH 022: ULTRA and the U.S. Seventh Army 150
Introduction 150
Operations 150
Security 152

Chapter *Page*

Conclusions 152
Tab A 153
SRH 032: ULTRA in the Southwest Pacific Area (SWPA) 155

VIII. THE POLITICS OF COMINT 159
SRH 141–1: Papers from the Personal Files of Alfred McCormack; Memorandum for Mr. McCloy: Signal Intelligence Service (1942) 160
SRH 141–2: Papers from the Personal Files of Alfred McCormack; Memorandum for General McNarney (1944) 163
SRH 141–2: Papers from the Personal Files of Alfred McCormack; Memorandum for General Bissell: Army-Navy Agreement Regarding ULTRA (1944) 166
A. Background of Army-Navy Relations in Ultra Field 166
B. Proposed Restrictions 168
C. Proposed Scope of Material to Be Released by Navy ... 168
D. Proper Interpretation of Agreement 169
E. European Intelligence 170
SRH 043: Comments on Marshall-Dewey Exchange (1944) 171

IX. TACTICAL COMINT 179
SRH 124: Operational History of the 849th Signal Intelligence Service (excerpt, 1945) 180
I. Beginnings 180
General 180
II. Intelligence Branch 184
General Functions 184
1. Introduction 184
2. Cryptanalysis 185
4. Laboratory Facilities 187
Major Problems Encountered 187
2. U.S. Signal Radio Intelligence Companies 187
3. Procurement and Training of Personnel 189
4. Organization and Equipment of Field Detachments 190
SRH 048: Summary of Operational Activity, Signal Security Detachment "D", Covering the Period 1 September 1944 to 1 April 1945 192

Chapter *Page*

I. Purpose 192
II. Mission of the Detachment 192
III. Signal Intelligence Division, Headquarters, ETOUSA 192
IV. G–2 Section, Tactical Headquarters, 12th Army Group 193
V. Signal Radio Intelligence and Signal Security Companies, 12th Army Group 194
VI. Flanking Army Groups 195
SRH 042: Third Army Radio Intelligence History (excerpt, 1945) 196
Operational Organization and Procedure of Radio Intelligence Agencies 196
A. Organization 196
B. Radio Intelligence Procedures 197
1. Operational 198
2. Communications Set-Up 203
C. Captured Documents 204
D. Prisoner of War Interrogations 204
SRH 227: History of the 126th Signal Radio Intelligence Company (excerpt,1945) 205
SRH 049: Technical Signal Intelligence Transmitted Directly to G–2, 12th Army Group, ETO From 4 August 1944 to May 1945 (excerpt, 1945) 211

X. RESHAPING THE TOOLS 213
SRH 169: Centralized Control of U.S. Army Signal Intelligence; Memorandum for Chief of Staff: Centralized Control of Signal Intelligence Activities for War Against the Japanese (1945) 214
I. Circumstances Leading to Proposal 215
II. Proposal to Theaters and Replies Thereto 216
III. Basic Reasons for Proposal 216
Availability of Traffic for Interception 216
Cryptanalysis 217
Usefulness of Results Obtained 217
"Low Level" Signals Intelligence 218
IV. Objections Raised by SWPA 218
V. Procedure for Placing Centralized Control into Effect 220

APPENDIXES:

A. Chronology 225
B. Glossary 227
C. Dictionary of People, Places, and Terms 233

ILLUSTRATIONS

The following illustrations appear between pages 112 and 113:

Herbert O. Yardley
Yardley's New York Headquarters
William F. Friedman
Friedman and His SIS Staff
The Munitions Building
2d Signal Service Company Member on Hawaii
The Battleship *Arizona* Sinking at Pearl Harbor
Henry L. Stimson
John J. McCloy
George V. Strong
Graduation Parade at Vint Hill Farms School
Japanese Language Training Course
Arlington Hall, Virginia
Army Signal Security Agency Staff Heads
Army Cryptanalysts at Arlington Hall
Calculating Machines at Arlington Hall

The following illustrations appear between pages 166 and 167:

Brig. Gen. Carter W. Clarke with Col. Alfred W. McCormack
German Signal Troops
The British Government Code and Cypher School
Brig. Gen. Telford Taylor with His Staff at Nuremberg
General Dwight D. Eisenhower Addresses Paratroopers
General Douglas MacArthur
German U-boat
General George C. Marshall with Governor Thomas E. Dewey
21st Signal Service Company's Radio Intercept Platoon
Signal Security Detachment "D" Analysts
128th Signal Radio Intelligence Company Intercept Personnel
Radio Direction-Finding Site at Brisbane, Australia
General Eisenhower, Maj. Gen. Hoyt S. Vandenbert, Brig. Gen. Preston W. Corderman, Col. Frank B. Rowlett, and Mr. Friedman

U.S. ARMY
SIGNALS INTELLIGENCE
IN WORLD WAR II

CHAPTER I

U.S. Army Signals Intelligence in World War II: An Overview

by John P. Finnegan

The United States Army entered World War II with an effective, functioning organization for the production of communications intelligence—COMINT. This was the Signal Intelligence Service (SIS) of the Army Signal Corps. The SIS had been formed in 1930 to consolidate all Army cryptologic functions under the Signal Corps. It was a unified organization responsible for producing the Army's own codes and cipher devices and for attempting to decrypt the communications of America's potential adversaries. Previously, the cryptanalytic function had been carried out by the War Department's Military Intelligence Division through a clandestine element based in New York, headed by Herbert O. Yardley, and funded with State Department support. However, this had been discontinued in 1929, partially as a result of Secretary of State Henry L. Stimson's conviction that "Gentlemen do not read each other's mail."[1]

The SIS was an organization shaped by its first chief, the legendary William F. Friedman. Friedman, who had previously served as the Signal Corps' code and cipher consultant, quickly recruited a small but extremely talented civilian staff. Even after a military officer was placed in charge of the SIS in 1935, Friedman continued to exercise a wide influence. During the period before World War II, the SIS published a series of influential studies on cryptology and pioneered the development of machine ciphers of unparalleled sophistication and security to safeguard Army communications. It also implemented training courses to educate reserve officers in cryptology, thus setting up a limited mobilization base for wartime expan-

sion. Another accomplishment was the establishment of a network of radio intercept stations, something which the Army had never attempted in peacetime; Yardley's earlier cryptanalytic efforts had depended on the cooperation of friendly cable companies to provide the raw material. [2]

The greatest prewar accomplishment of SIS, however, was its success in deciphering the machine cipher used by the Japanese Foreign Office for its most secret messages. Through purely cryptanalytic methods, the SIS was able to build an analog of this machine and read Japanese dispatches as quickly as the intended recipients. As a result, the Army became privy to the thought processes that guided Japanese diplomacy. The secret breakthrough was shared with SIS's Navy counterpart, OP–20–G, and later with the British. Otherwise, it was closely held. Decrypts of enciphered Japanese messages, code-named MAGIC, were passed on to a tightly restricted group of individuals in the War and Navy Departments and further disseminated to top policymakers (the Secretaries of War, Navy, and State, the President's military adviser, and the President himself). [3]

Unfortunately, MAGIC could not ward off Pearl Harbor. The high-level communications of the Japanese Foreign Office did not carry the details of Japanese military planning. Consular traffic that did contain military intelligence indicators traveled in less secure systems, but it could not be translated in a timely fashion because of other priorities. Moreover, the very secrecy with which MAGIC was handled impaired its utility. A few upper-level officials received tantalizing snippets of information from critical messages, but the material itself was never subject to detailed exploitation and analysis over the long haul. As Friedman would later put it, "each message represented only a single frame, so to speak, in a long motion picture film." [4] But no one had ever been in a position to watch the whole movie.

The shock of the Pearl Harbor attack immediately led to the adoption of a more systematic approach to handling diplomatic intercepts. A first step was taken when the Secretary of War, Henry L. Stimson, directed that a Special Section be formed within the Military Intelligence Division's Far Eastern Section. (The head of the Far Eastern Section had previously functioned as the sole conduit of MAGIC.) Following an outside study conducted at Stimson's direction by a Chicago attorney, Alfred McCormack, the section was expanded to the status of a Special Branch within the Military Intelligence Service that was created as the operating arm of the Military Intelligence Division in March 1942. The Special Branch was headed by Col. (later Brig. Gen.) Carter Clarke; McCormack himself accepted a

colonel's commission and became Clarke's deputy. This organizational innovation for the first time allowed sufficient numbers of analysts access to COMINT in ways that would allow them to use it in its entirety to build up an intelligence picture. [5]

Meanwhile, the Signal Intelligence Service was conducting a rapid expansion. In March 1942 the Military Intelligence Division (MID) recommended to the Chief Signal Officer that SIS move from its existing quarters in the Munitions Building in downtown Washington to new quarters that would provide greater security. MID also suggested that primary monitoring stations be established, one on each coast. At the time, the seven small existing stations manned by the 2d Signal Service Company—the SIS collection unit—were not well positioned for wartime needs; the station nearest to the scene of action, Fort McKinley in the Philippines, had already been overrun by the Japanese Army. [6]

Under wartime conditions, these steps were taken with alacrity. In June 1942 the first Army elements took possession of Arlington Hall, a former women's junior college just outside Washington. That same month, personnel from the 2d Signal Service Battalion (as the intercept arm of the SIS was now designated) began operations at Vint Hill Farms in Warrenton, Virginia, which had been selected as the site for Monitoring Station Number 1. A second major field station was soon set up at Two Rock Ranch near Petaluma, California. In the meantime, SIS itself was redesignated. The term "Signal Intelligence" was thought to be too provocative; SIS first became the Signal Security Division, then the Signal Security Service; and achieved its final wartime designation as the Signal Security Agency (SSA) in the summer of 1943. [7]

The Signal Corps' cryptologic organization recruited a largely civilian work force and began a process of rapid expansion. The original buildings at Arlington Hall were quickly outgrown. In the winter of 1942 and the spring of 1943, two large temporary buildings were hastily constructed at Arlington Hall to handle the overflow. Meanwhile, the agency moved in new directions even as it grew. In the spring of 1942 liaison with the British introduced it to the new and promising art of traffic analysis, through which intelligence could be derived from the externals of a message even if the message itself could not be decrypted. In June 1942 the agency was given exclusive responsibility for exploiting foreign diplomatic communications, a mission previously shared with the Navy. It also dispatched a small detachment to Australia and sent one of Friedman's top cryptologists, Col.

Abraham Sinkov, to command it. This would become the American nucleus of a completely independent COMINT effort conducted in support of General Douglas MacArthur's Southwest Pacific Area by Central Bureau Brisbane, a combined U.S.-Australian operation headed by Brig. Gen. Spencer Akin, MacArthur's signal officer and a former chief of SIS. [8]

However, there were still large deficiencies in the Army's COMINT effort. The effort remained fragmented with intelligence production and collection in separate compartments. The Special Branch of the Military Intelligence Service, responsible for COMINT evaluation, had no association with the cryptanalysts at Arlington Hall. The latter group worked for the Signal Corps, which itself was only one component of the Army Service Forces. As a result, McCormack commented, a situation existed in which the Military Intelligence Service was "simply taking in what the Signal Corps catches and turns in, leaving with the Signal Corps the responsibility for determining how much it will catch and turn in, and from what sources."[9] And the Signal Security Agency itself did not monopolize COMINT collection, since tactical signals intelligence units in the field worked for the supported commanders, not SSA. [10]

Moreover, the Army's COMINT effort was hampered by a severe shortage of personnel throughout the whole system. This created bottlenecks within the Special Branch and the Signal Security Agency. Part of the problem resulted from military regulations. The Secretary of War had decreed that no officer under 28 years old could be in Washington after 31 January 1942. Additionally, the Army was reluctant to offer direct commissions to qualified civilians. The Civil Service Commission was equally obstructive. McCormack noted rather sourly that it seemed "unable to distinguish an intelligence organization from an office that routes and stamps papers, and therefore forces on us an organization chart that calls for quotas of morons and semimorons. . . ." The Signal Security Agency, with much larger personnel requirements, was even more vulnerable to such practices, and it was hampered by the low priority given to it as a component of Army Service Forces. Paradoxically, the importance of its work, which might have been used to justify a higher personnel priority, was too secret to divulge. [11]

Even more frustrating was the slow progress made by SSA in actually breaking any military codes. As previously noted, Japanese cryptosystems worked on principles entirely different from those used in Japanese diplomatic communications. The Japanese Army used bulky reenciphered codes, not a cipher machine. Cryptanalytic continuity was lacking. The Navy had

been able to monitor traffic produced by Japanese naval exercises in the 1930s, but the Army had never encountered Japanese military nets until Bataan. As a result, SSA analysts at Arlington Hall were not able to make an entry into a single Japanese Army system until April 1943, when SSA and MacArthur's Central Bureau Brisbane made an almost simultaneous breakthrough. The first usable intelligence was not derived from exploitation of this Japanese Water Transport code until June 1943. [12]

The Army was equally frustrated in its attempt to work on German military systems. In April 1942, SSA had suggested to the British that it be allowed to work on the Enigma cipher machine used in high-level communications of the German armed forces. It was generally understood that the Government Code and Cypher School (the main British cryptanalytic center at Bletchley Park) had achieved some success in this field. However, the British rebuffed the Army's efforts either to secure Enigma decrypts or to work on the Enigma problem. This studied lack of cooperation—justified by the British on grounds of security and economy of effort—became even more grating when the Army became aware that the British were willing to share high-level COMINT with the U.S. Navy to meet the operational needs of fighting the U-boat war. [13]

Finally, America's first exposure to actual land combat in the Tunisia campaign that followed Operation TORCH revealed major deficiencies in the structure of the Army's tactical signals intelligence organization. When the Army entered World War II, it was envisaged that only two types of tactical COMINT units would be needed: radio intelligence platoons organic to the divisional signal companies and signal radio intelligence companies assigned on a basis of one per field army. Since it was assumed that analysis and translation would be accomplished by small radio intelligence staffs at theater or field army level, as had been the case in World War I, no analytic personnel were included in these units. [14]

The test of combat quickly demonstrated the unsuitability of this structure. The divisional platoons, in exposed positions near the front, were in too great a danger of being overrun to practice effectively their specialty; the signal radio intelligence companies, as organized, were too large and unwieldy to be used to support a corps, which had no dedicated communications intelligence support but which seemed to be the level of command most in need of it. Central processing proved to be impracticable, and the staffs at army level were too limited to handle the volume of exploitable COMINT. At the same time, the communications practices of the European

members of the Axis (but not the Japanese) presented large volumes of material sent in clear or in low-level codes susceptible to timely forward exploitation. The Army was initially forced to turn to the British to bolster its units with analytic personnel. Later, a numbered theater intelligence service, the 849th Signal Intelligence Service, was formed to support American COMINT units in the North African Theater of Operations. [15]

In short, the Army's successes in the COMINT field up to the midpoint of the war were limited. Its continuing triumphs in the field of diplomatic communications had not been matched by corresponding success against the military systems in use by its major adversaries. The Army's COMINT effort had been hampered by its own organizational deficiencies and lack of priorities. The Army had been rebuffed by the British in its attempt to obtain access to German COMINT; it had been largely baffled by the Japanese military systems. Commenting on the situation in early January 1944, McCormack concluded morosely that "except for whatever the Navy has been able to do, we have achieved no corresponding victory over the Japanese. To date, in the field of radio intelligence, we have met largely with failure." [16]

McCormack's dissatisfaction at the beginning of 1944 was understandable. A resistive personnel system had created bottlenecks within both Arlington Hall and the Special Branch. Arlington Hall's initial breakthrough against Japanese codes in the summer of 1943 had created "a critical need for at least 2,000 [additional] persons. . .", but it had taken six months to begin "the lengthy and difficult job of recruiting such personnel. . . ." In the meantime, 200,000 unread Japanese messages had piled up. [17]

But McCormack drew too dark a picture. Already the situation was becoming brighter. Mid-1943 had been a watershed in the Army's final successful exploitation of communications intelligence. Two major developments took place at this time. The first was Arlington Hall's success in breaking and exploiting the Japanese Water Transport codes. This proved to be a springboard for the exploitation of other Japanese military systems. The Signal Security Agency, now steadily expanding, was able to throw masses of personnel and batteries of IBM machines against the Japanese military cryptosystems. The capture of codes by troops in the field enhanced the ongoing efforts of cryptanalysts. Soon after McCormack's pessimistic evaluation, Arlington Hall had thus mastered the main Japanese Army code, a breakthrough that produced a wealth of intelligence. [18]

The second development was of equal importance. In mid-1943 the

British finally decided to take the United States Army into their confidence and reveal the full story of their success against the Enigma and other high-grade German systems. This was accomplished by a liaison visit to London by a joint Special Branch–SSA team: McCormack, Friedman, and Lt. Col. Telford Taylor of the Special Branch. All barriers to free exchange suddenly fell. American cryptanalysts were allowed to work at Bletchley Park, a Special Branch liaison officer in London supervised the dispatch of pertinent traffic to MID in Washington, and Arlington Hall was given a share of research on the Enigma problem. In turn, the United States agreed to adopt and implement stringent British security practices on the transmission of COMINT to the field. [19]

The new availability of COMINT from both American and British sources created for the first time the problem of dissemination to the field. The problem was solved by the creation of a system of Special Security Officers (SSOs) along the pattern already established by the British. The SSOs would serve as representatives of Special Branch to the major American commands in the field, functioning as transmitters, guardians, and interpreters of ULTRA, as high-level COMINT was now called. The first three SSOs were sent to the Pacific in December 1943. Shortly thereafter, the British agreed to allow American SSOs to support the American commanders in the European and North African–Mediterranean–Middle East Theaters. (Previously, the British Special Liaison Unit system had handled all such dissemination of COMINT.) A subsequent decision to release ULTRA down to the field army and numbered air force level resulted in an even greater expansion of the Special Security Officer system. By August 1944 the SSO system had been allotted 172 officers and 65 enlisted communications personnel. [20]

The new importance and availability of COMINT led to changes in the organizational structure that produced it. By mid-1944 Special Branch was as large as all other branches in the Military Intelligence Service's Intelligence Group combined. But this created a situation in which a large portion of the War Department's intelligence organization labored blindfolded, producing estimates without access to what was now the Army's single most important intelligence source. This was an obviously less than desirable situation, and it led to a reorganization of MID and its operating arm. Rather awkwardly, this took place just at the time of the Normandy invasion. Special Branch, as such, was broken up; its members dispersed through the rest of the Military Intelligence Service. (A smaller Special

Branch entity continued to supervise dissemination of COMINT to the field.) [21]

A few months later, the artificial barriers that had separated collectors of COMINT from evaluators also fell. The fact that the Signal Security Agency was just a small part of the Signal Corps had disturbed War Department intelligence officers ever since 1942. By 1944 the SSA had become the Military Intelligence Division's most important single source, furnishing it with 70 percent of its diplomatic intelligence and 80 percent of its information on the Japanese military. This made the existing situation even more unsatisfactory. In August 1944 Assistant Secretary of War John J. McCloy wrote pointedly to Lt. Gen. Joseph McNarney, the Army Deputy Chief of Staff, that "I do not believe it is good practice to have the MIS by general directive and the establishment of general policies to attempt to create a workable intelligence organization in the low echelons of Army Service Forces as they are now attempting to do."[22] The Signal Corps clung tenaciously to SSA, but in the end it was forced to back down. On 15 December 1944, the Military Intelligence Division was given operational control over the Signal Security Agency, leaving the Chief Signal Officer responsible only for the agency's administration. [23]

Meanwhile, SSA continued to expand. By the summer of 1944 5,100 civilians and 2,000 military personnel were on duty at Arlington Hall. The intercept facilities of the 2d Signal Service Battalion, SSA's collection arm, were also built up. In the spring of 1944 new fixed stations were established at New Delhi, India; Asmara, Eritrea; Fairbanks and Amchitka, Alaska; and Fort Shafter, Hawaii. In the fall the steady advance of American forces allowed another field station to be established on the island of Guam. The battalion also took over "listening posts" at Bellmore, New York, and Resada, California, that had been previously operated by the Office of Strategic Services (OSS). The OSS had used the facilities to track Axis propaganda broadcasts; SSA converted them to security monitoring stations. [24]

At the tactical level Army signals intelligence was strengthened by the creation of new types of units. As previously noted, the Army's experience in conducting the COMINT war in North Africa and later in the Mediterranean had demonstrated deficiencies in the existing organization of field assets. Divisional signal radio platoons had proven unsatisfactory; the existing signal radio intelligence companies were cumbersome and could function effectively only when supplemented by analytic and linguist personnel from a theater-level signal intelligence service. The War Department's initial reaction had been to move radio intelligence platoons

up to the corps signal battalion. However, this measure only jammed a small number of intelligence personnel into a larger unit performing an unrelated function, resulting in obvious security and operational disadvantages. In the northern European theater, a happier solution was found. Small signal service companies, numbered in a sequence beginning with 3250, were formed from existing resources in theater to provide COMINT support to each corps. These units contained their own analytical personnel. The large signal radio intelligence companies continued to operate at army, army group, and theater level. [25]

In the Far East, because of the nature of the target and the tactical circumstances, the structure of the Army's tactical signals intelligence organization followed a different pattern. The Japanese target array offered little opportunity for local exploitation, and large Army formations were not fielded until the Philippine campaign of late 1944. Consequently, the four signal radio intelligence companies in the Southwest Pacific Area operated as collection arms for MacArthur's Central Bureau Brisbane rather than supporting the army commanders. In the Pacific Ocean Area two signal radio intelligence companies worked in similar fashion on high-level codes for Arlington Hall. [26]

In addition, the Army Air Forces (AAF) created its own specialized intercept units to carry out a mission previously performed by signals intelligence units of the ground Army. In 1944 the AAF organized radio squadrons, mobile, to support each numbered air force. These large, battalion-size units, which included AAF intelligence analysts, were capable of operating in separate detachments and conducting intercept against both continuous-wave (Morse) and voice transmissions. [27]

By 1945, then, the Army had largely perfected its structure for collecting, evaluating, and disseminating communications intelligence. In this field, however, the Army never acted as an autonomous player. MIS and SSA were partners in a vast combined effort in which responsibilities were largely divided along theater and target lines, with the British focusing on the German problem, and the Americans on the Japanese. However, the U.S. Army was deeply involved in all theaters: American SSOs furnished intelligence derived by Bletchley Park to the American commanders they supported in Europe, and Army personnel were at three of the four great Allied production centers. The Army controlled Arlington Hall; Central Bureau Brisbane continued as a combined U.S.-Australian effort; and the Army had a foothold at Bletchley Park. Only the Wireless Experimental

Center at Bombay, India, remained a purely British operation. [28]

Despite these steady improvements, the Army's COMINT arrangements were still less than satisfactory in three areas. SSA was still under the administrative control of the Chief Signal Officer, and this took its toll on any claim for resources. The fact that Col. Preston W. Corderman, who commanded 10,000 men and women in his dual capacity as chief of SSA and commander of the 2d Signal Service Battalion, did not receive a brigadier general's star until June 1945 reveals something of the dimensions of the problem. [29]

Second, the Army's strategic and tactical signals intelligence assets were still not coordinated properly. Tactical COMINT units were trained by Army Ground Forces, not SSA, and they functioned under the direction of theater and numbered air force commanders, not SSA, despite the fact that this division of labor did not reflect the reality that the communications intelligence process was a seamless web. As one contemporary evaluation put it, "radio intelligence operations, their availability for interception, the cryptographic systems used, and the usefulness of the results derived therefrom, all have no relation to the considerations which are determinative in assigning command responsibility for combat operations against enemy forces." [30]

Finally, cooperation between Army and Navy COMINT operations had been slow to arrive, despite the fact that OP–20–G, the Navy equivalent of SSA, was headquartered in another requisitioned junior college just a few miles away from Arlington Hall. An Army-Navy Communications Intelligence Coordinating Committee (ANCICC) had been set up in early 1944, but had not been able to effect coordination all that well. The Navy had different uses for COMINT than the Army, and its security practices were more stringent. Navy hesitancy at sharing naval COMINT had been so great that McCormack at one time had toyed with the idea of terminating all cooperation between the two services. In February 1945, however, the two service chiefs (Army Chief of Staff General George C. Marshall and Navy Commander in Chief and Chief of Naval Operations Admiral Ernest W. King) had agreed to set up a high-level Army-Navy Communications Intelligence Board to finally coordinate a joint effort. [31]

The new head of MID, Maj. Gen. Clayton Bissell, took this Navy initiative as an opportunity to resolve what he perceived as the remaining difficulties of Army signals intelligence organization. He protested that "the Army cannot participate on an inter-service project of this sort as long as its

own signal intelligence activities remain as decentralized as they now are." [32]

This bureaucratic ploy spurred the War Department to thoughts of reorganization. After consulting theater commanders in the Far East, the Army created a single unified signals intelligence organization on 15 September 1945. The Army Security Agency established that day was to control "all signals intelligence and security establishments, units, and personnel" and to function under direct control of the Military Intelligence Division. The U.S. Army thus attained the integrated COMINT organization its intelligence chiefs had so long desired—thirteen days after the world war that had called it into being had finally come to an end. [33]

Notes

Note: SRH citations refer to Special Research Histories: declassified/sanitized cryptologic documents released to the National Archives by the National Security Agency.

1. SRH 134, "Expansion of the Signal Intelligence Service from 1930–7 December 1941," pp. 3–28; Herbert O. Yardley, *The American Black Chamber* (Indianapolis: Bobbs-Merrill, 1931), pp. 369–372; David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: The Macmillan Company, 1967), p. 360.
2. SRH 29, "A Brief History of the Signal Intelligence Service," pp. 8–13.
3. SRH 134, p. 19; Kahn, *The Codebreakers*, p. 24; SRH 106, "Specific Instructions for the Handling and Dissemination of Special Intelligence," pp. 1–2.
4. SRH 125, "Certain Aspects of 'Magic' in the Cryptologic Background of the Various Official Investigations into the Pearl Harbor Attack," p. 63.
5. SRH 141, "Papers from the Personal Files of Alfred McCormack, Colonel, AUS, Special Branch, G–2, Military Intelligence Division, War Department General Staff," Part 2, pp. 7–8.
6. *ULTRA and the Army Air Forces in World War II*, edited by Diane Putney (Washington, D.C.: Office of Air Force History, 1987), p. 71; SRH 349, "The Achievements of the Signal Security Agency in World War II," pp. 13–14.
7. *ULTRA and the Army Air Forces in World War II*, p. 71; SRH 135, "History of the 2d Signal Service Battalion," p. 101.
8. SRH 349, pp. 9, 15; Ronald Lewin, *The American MAGIC: Codes, Ciphers, and the Defeat of Japan* (New York: Farrar, Straus, Giraux, 1982), pp. 143, 149.
9. SRH 141, Part 2, pp. 202–203; Part 1, p. 29.
10. SRH 169, "Centralized Control of U.S. Army Signal Intelligence in World War II," pp. 14–15.
11. SRH 141, Part 2, pp. 8–13, 139, 223; SRH 116, "Origins, Functions, and Problems of the Special Branch, MIS," p. 22.
12. SRH 349, p. 26.
13. F.H. Hinsley et al., *British Intelligence in the Second World War* (New York: Cambridge University Press, 1981), Volume II, pp. 56–57.
14. SRH 391, "American Signal Intelligence in North Africa and Western

Europe," pp. 6–7.

15. Ibid., pp. 63, 94; "History of the Signal Intelligence Division, European Theater of Operations, United States Army" (SECRET), Part I, Chapter V, p. 1, Army Cryptologic Records; Hinsley, *British Intelligence*, Volume II, p. 742; SRH 124, "Operational History of the 849th Signal Intelligence Service," pp. 10–12.

16. SRH 361, "History of the Signal Security Agency, Volume II: The General Cryptanalytic Problem," p. 83; SRH 141, Part 2, p. 223.

17. SRH 141, Part 2, pp. 221–222.

18. SRH 349, pp. 18, 26–28.

19. Hinsley, *British Intelligence*, Volume II, pp. 57–58; SRH 141, Part 2, pp. 182–183.

20. SRH 33, "History of the Operations of Special Security Officers Attached to Field Commands," p. 16; SRH 61, "Allocation of Special Security Officers to Special Branch," p. 30.

21. *ULTRA and the Army Air Forces*, pp. 86–87; Ray S. Cline, *The CIA Under Reagan, Bush, and Casey* (Washington, D.C.: Acropolis Press, 1981), p. 111.

22. SRH 141, Part 2, pp. 316–317.

23. SRH 349, p. 10.

24. Ibid., p. 14.

25. G.R. Thompson and Dixie R. Harris, *The Signal Corps: The Outcome*, United States Army in World War II (Washington, D.C.: Office of the Chief of Military History, 1966), p. 347; SRH 391, pp. 94–96, 104. Details on the organization of the corps-level signal service companies can be found in SRH 42, "Third Army Radio Intelligence History in Campaign of Western Europe."

26. SRH 169, pp. 54–55, 60–61; SRH 365, "History of Signal Intelligence Division of the Signal Officer, AFMIDPAC," pp. 15–23.

27. SRH 124, p. 24.

28. SRH 141, Part 2, p. 220.

29. SRH 135, p. 12; SRH 349, p. 6; Thompson and Harris, *The Signal Corps: The Outcome*, pp. 331, 338–339.

30. SRH 169, p. 59.

31. SRH 141, Part 2, pp. 282–295; SRH 169, p. 58.

32. SRH 276, "Centralized Control of U.S. Army Signal Intelligence Activities, 30 January 1939–16 April 1945," p. 139; Memo, AC of S, G–2, subj: Army-Navy Communication Intelligence Board–Establishment of (2 Mar 45), Army Cryptologic Records.

33. SRH 349, pp. 85–88.

CHAPTER II

The Road to Pearl Harbor

These documents trace the evolution of U.S. Army signals intelligence in the period prior to United States involvement in World War II. SRH 29, A Brief History of the Signal Intelligence Service, was written by William F. Friedman, the organization's first head. It sketches the beginnings of Army signals intelligence in World War I, provides an unflattering account of Herbert O. Yardley's Black Chamber organization, the legendary cryptanalytic unit secretly funded by the State and War Departments, and goes on to explain the reasons for transferring the function from Military Intelligence to the Signal Corps in 1929. SRH 134, Expansion of the Signal Intelligence Service, was also written by Friedman. It charts the growing pains of this organization after 1930, and discusses how the efforts of Friedman and his team resulted in the breaking of the Japanese diplomatic machine cipher, codenamed PURPLE.

The actual intercept of communications was performed by specially trained Signal Corps personnel. After 1938, these were brought together in a unique unit, the 2d Signal Service Company. The establishment of this unit is documented in an excerpt from SRH 135, History of the Second Signal Service Battalion, 1939-45.

The success of the SIS in breaking PURPLE was shared with the Navy's corresponding cryptologic unit, OP-20-G, but was otherwise closely held. The intelligence product obtained from decrypted Japanese diplomatic communications was assigned the codename MAGIC and disseminated to only a small group of top officials. One of the most important messages contained in Japanese diplomatic traffic is reproduced from *The Magic Background of Pearl Harbor, Volume IV, Appendix* (Washington, D.C.: Department of Defense, 1977), p. A-89. However, the stringent security measures surrounding MAGIC impaired effective and sustained evalu-

ation of the material. The excerpt from SRH 115, U.S. Army Investigations Into the Handling of Certain Communications Prior to the Attack on Pearl Harbor, 1944-1945, shows the impact of this policy of tight compartmentation on the War Department military intelligence organization.

From SRH 029. *William F. Friedman, the first head of the Signals Intelligence Service, was America's foremost cryptologist. Born in Czarist Russia to Jewish parents, Friedman was brought to the United States by his family as a very young child. He was originally trained as a geneticist, but his energies were soon diverted to the exotic field of cryptology when he was hired by the eccentric philanthropist George Fabyan to work at Fabyan's private "think-tank"—Riverbank Laboratories at Geneva, Illinois. Fabyan had a theory that Shakespeare's plays had actually been written by Sir Francis Bacon, and that this could be proved by deciphering a hidden cipher that Bacon had scattered throughout the plays. Fabyan was wrong—as Friedman convincingly demonstrated many years later, no such cipher existed—but his enthusiasms led Friedman on to a brilliant career. In 1942, Friedman wrote this succinct account of the origins of the Army's World War II signals intelligence organization. As can be seen from the text, his bitterness against his great colleague and rival, Herbert O. Yardley, continued to run deep.*

A BRIEF HISTORY OF THE SIGNAL INTELLIGENCE SERVICE

1. Prior to June 1917 no department of the Government conducted cryptanalytic activities whatsoever. From June 1916 to about May 1918 a considerable amount of work along these lines was conducted purely as a patriotic enterprise at his own expense by Mr. George Fabyan, whose Riverbank Laboratories at Geneva, Illinois, organized a small group of fairly well-trained cryptanalysts to work upon such codes and ciphers as were forwarded by the War, Navy, State, and Justice Departments. The undersigned directed the cryptanalytic operations and training at the Riverbank Laboratories from the time of the inception of this work until its close thereat in 1919, except for a period of a year when he was 1st Lieut., MID, serving at GHQ-AEF in the German code solving section.

2. In June 1917 the cryptanalytic activities of the War Department were initiated by Colonel Van Deman, G-2, with the commissioning of H.O. Yardley as 1st Lieut., MID. Yardley, who had been a telegrapher at the State Department and had

taken some interest in cryptography, was given two civilian employees to assist him. The work grew rapidly and by the autumn of 1917 the increased staff was organized as a section designated as MI-8, which was subdivided into 6 subsections with duties as indicated very briefly below:

(1) Code and cipher solution subsection. - This subsection was what would now be called the cryptanalytic subsection. It was the largest of the subsections of MI-8 and performed the cryptanalytic work not only for the War Department *but also for all other Government departments, including Navy, State, Justice, and the two censorships—Cable and Postal, which were then separate organizations.*

(2) Code and cipher compilation subsection. - Despite the fact that under Army regulations the compilation and revision of codes was a function of the Chief Signal Officer, compilation activities under the Signal Corps were apparently in a moribund state. Information having been received that the Germans possessed copies of the War Department Telegraph Code, MI-8 deemed it advisable to establish a code compilation subsection, and that subsection produced several codes such as Military Intelligence Codes No. 5 and No. 9, small pocket codes for secret agents, and the like.

(3) Training subsection. - In addition to training its own personnel MI-8 trained the majority of the personnel sent overseas for cryptanalytic duties with field forces, both AEF and Siberia.

(4) Secret inks subsection. - A laboratory was established for the preparation of invisible inks for use by our own agents. It also examined letters for secret ink writing and an average of over 2000 letters per week were examined for the military and postal censorship from July 1, 1918 to February 1, 1919.

(5) Shorthand subsection. - This subsection was organized to handle texts in various shorthand systems, especially German, which had to be deciphered.

(6) Communications subsection. - This was established in MI-8 for handling messages to and from military attaches and intelligence officers serving abroad. In a period of 9 months it sent and received about 25,000 such messages, practically all in code.

3. At the height of its development, which was reached in November 1918, MI-8 was, for those days, a rather large unit, consisting of 18 officers, 24 civilian cryptographers and cryptanalysts, and 109 typists and stenographers. The time had come for the establishment of a definite policy for the future. Now, the guiding heads of Military Intelligence at that time fully recognized the high importance and value of the services rendered by the cryptanalytic bureau, because they had been in positions where the products of the daily activity of the bureau came directly to notice and they could not fail to note the influence and bearing which the work had, not only upon the military and naval but also upon the diplomatic, political, and economic phases of the conduct of the war. They therefore had *practical* experience in the matter and could bring the weight of their position of influence and their actual experience to bear upon those in charge of the purse strings, with the

result that they were able to obtain funds sufficient to keep a fairly large organization intact for a year or two. An annual appropriation of $100,000 was recommended in a G-2 study dated May 16, 1919 [text withheld] to be used as follows:

Rent, light, and heat		$3,900
Reference books		100
Personnel:	Chief	6,000
	10 code and cipher experts @ $3,000 each	30,000
	15 code and cipher experts @ $2,000 each	30,000
	25 clerks @ $1,200 each	30,000
	Total	$100,000

The item for "rent, light, and heat" is explainable when it is noted that the bureau was to be moved from Washington with a view to hiding its existence. Of the $100,000 recommended, the State Department was to provide $40,000 and $60,000 was to be provided for expenditure by the A.C. of S, G-2 on "confidential memoranda" against funds pertaining to "Contingency Military Intelligence Division"—that is, by vouchers not subject to review by the Comptroller General. The paper containing the recommendations made by the A.C. of S, G-2 to the Chief of Staff was "OK-ed" and initialled by Acting Secretary of State Polk on May 17, 1919, and on May 19 it was approved by the Secretary of War over the signature of General March, Chief of Staff. The plan was put into effect, the bureau was installed in a private house at 22 East 38th Street, New York City, and all personnel together with existing records were moved thereto.

4. It is important to note that at that time no provision whatsoever was made for radio intercept as a source of raw material for cryptanalysis. A few words on this subject may not be amiss. Radio intercept of fixed station material in the U.S. by the Army during our active participation in the last war was rather fragmentary. The work was, of course, a responsibility of the Signal Corps, but radio communications could hardly compete with cable and wire communications as a source of raw material because not only did the large governments use cable in preference to radio, but also radio as a means of communication between widely separated fixed stations was then in its infancy. The Signal Corps did, however, have what was called "mobile tractor" units stationed on the southern border, [text withheld] and in late 1918 one large intercept station was established at Houlton, Maine, for the purpose of copying trans-Atlantic radio. The large intercept stations maintained by the Signal Corps in the AEF did furnish a large quantity of diplomatic traffic which was forwarded as raw material to G-2 in Washington, but as soon as the war was over all these sources of intercept material were abandoned. [text withheld]

* * *

This was, of course, true to a certain extent but was not by any means the whole truth. At any rate by 1929 the flow of messages furnished G-2 had dwindled to a mere trickle. In about the year 1926 the intercept stations of the Coast Guard submitted to me informally a few radio intercepts of what appeared to be Japanese code messages, but these were only sporadic occasional intercepts of transmissions in the Far East. They were usually fragmentary and afforded very poor material. Such as they were, however, these occasional messages were turned over to G-2. There were, therefore, clear indications that if a serious attempt were made to obtain this material better copy could be obtained. However, no pressure was brought on the Signal Corps to set up a regular intercept service, and aside from a few relatively weak efforts to establish an intercept station in the Philippine Department there was no real intercept service until after 1929, when responsibility for cryptanalysis was transferred from G-2 to the Signal Corps. How this came to pass will soon be detailed.

5. As indicated Par. 3 above, the $100,000 appropriation set up in 1919 took care of the bureau for the FY 1920, that is from July 1, 1919 to June 30, 1920, but when in June 1920 it came time to set up the budget for FY 1921, the purse strings were already beginning to be pulled tighter. Many of the "old-timers" in G-2 had gone to other assignments; those remaining and the newcomers in G-2 apparently had neither the background nor the influence to press the matter. The appropriation was at once cut in half, that is, to $50,000, of which the State Department share still continued to be $40,000. The theory was, evidently, that since the work done by the bureau was primarily, if not solely, for and of interest to the State Department, all or nearly all of the funds should be provided by that department. The War Department overlooked some very important points in the situation—points which will be brought up and emphasized later in this summary. In order not to break the continuity of the history at this point, it will be stated merely that year by year the funds provided for the maintenance and operation of the bureau became more and more constricted until by the autumn of 1929 the following tabulation, based upon a letter dated July 17, 1929 from Major O.S. Albright, G-2 to the Chief Signal Officer (General Gibbs), shows how the bureau had been permitted to deteriorate:

Rent		$3,000
Books, postage, travel, transportation, misc.		2,370
Personnel:	1 Chief (Yardley)	7,500
	1 Code and cipher expert	3,660
	1 translator (Jap)	3,750
	1 secretary	1,800
	1 clerk-typist	1,600
	1 clerk-typist	1,320
	Total	$25,000

In the foregoing total appropriation of $25,000 the State Department furnished $15,000, the War Department $10,000. The activities of the bureau had by this time become so reduced that it was sending in only occasional translations of a few Japanese [text withheld] diplomatic messages. No research whatsoever was conducted in cryptanalysis; there were no training activities, no intercept, no code compilation, no secret ink work. The personnel consisted of six persons all told and 37 1/2% of the total payroll went to one man, who had little interest other than to continue as long as possible to maintain himself in the sinecure into which he had been permitted to establish himself.

6. In the summer of 1929 Major O.S. Albright, Signal Corps, had been assigned to G-2 to serve on the Staff of the A.C. of S., G-2 to supervise and coordinate such of the cryptographic and cryptanalytic activities of the War Department as remained. After a careful study of the situation and an appraisal of how the existing cryptanalytic bureau was and was not serving the functions for which it had been intended, Major Albright came to the conclusion that the entire picture was wrong. He felt that the product ("bulletin") which the bureau was turning out every few days was indeed of primary interest for its own sake to the State Department and while the War Department had only a secondary interest in the "bulletin" for the information it gave, the primary interest of the War Department in cryptanalytic studies in peace time was that it was intended to provide a means for training of personnel for *immediate* war-time effectiveness. Major Albright found that not only was there very little if any training being conducted but also that all the persons in the bureau, except for one clerk receiving the least pay, were "getting along in years"—their potential usefulness for possible war time service practically nil. Moreover, the bureau was now hidden away in a public office building in New York (under cover of the "Code Compilation Company" for alleged purposes of security) and far away from *direct* supervision of anybody connected with the War Department or of G-2, so that nobody knew what was going on, how the office was administered, etc. Yardley devoted most of his time to two or three private enterprises (commercial code compilation, real estate brokerage, consultant in code matters to commercial firms) and he was having a "field day" at Government expense. There were, in addition, several other weighty factors which motivated Major Albright in preparing a G-2 study [text withheld] recommending that the bureau be taken out of G-2 and its functions transferred to the Signal Corps, chief among which was the desirability, if not necessity, of placing *all* cryptographic and cryptanalytic work of the War Deparment under one agency, rather than distributing it among three (The Adjutant General, for printing, storage, issue, and accounting of codes; The Chief Signal Officer, for compiling codes and ciphers; Military Intelligence for solution of codes and ciphers). A memorandum on the same subject was prepared by Lieut. Col. W.K. Wilson of the War Plans and Training Section of G-2, and is also attached hereto [text withheld] The reasons given in Major Albright's study and in Col. Wilson's memorandum were apparent-

ly deemed valid by the Chief of Staff, for Major Albright's recommendations were approved in April 1929 and steps were soon initiated by G-2 and the Chief Signal Officer to put them into effect. The recommendations carried with them merely the wording of a changes to be made in AR 105-5, specifying the duties of the Chief Signal Officer, these duties being enlarged to include the printing, storage, distribution, and accounting of codes and "in time of war the interception of enemy radio and wire traffic, the goniometric location of enemy radio stations, the solution of intercepted enemy code and cipher messages, and laboratory arrangements for the employment and detection of secret inks."

7. However, before anything could be done actually to transfer the activity a new and very disturbing factor entered into the picture. In March 1929 a new administration took office, in which Mr. Stimson became Secretary of State. For a few weeks no "bulletins" from the cryptanalytic bureau in New York were given him, the intention being to "go slow" until he had become sufficiently well oriented in the duties of his office to warrant bringing to his attention the highly secret activities engaged in by War and State Departments by means of funds provided in large part by the latter Department. Early in May 1929, however, the time was deemed ripe for this measure, but it was with some trepidation that a few translations of Japanese code messages were placed on Mr. Stimson's desk. His reaction was violent and his action drastic. Upon learning how the material was obtained, he characterized the activity as being highly unethical and declared that it would cease *immediately*, so far as the State Department was concerned. To put teeth into his decision he gave instructions that the necessary funds of the State Department would be withdrawn *at once*. It was only after considerable pressure by the A. C. of S., G-2 that he was dissuaded from this course, which might have had serious consequences by suddenly throwing out of employment the six people concerned, at a time of severe economic depression. For these workers had only special training in a field wholely useless to commercial, industrial, shipping or banking firms, or to other government departments, or to educational institutions. An arrangement was therefore made to close the office immediately so far as active work was concerned but to keep the personnel on the payroll for the time necessary to wind up affairs, and get the files in shape ready to turn over to the Signal Corps. This took a couple of months, and at the end of June 1929 the employees were given three months' pay *in advance* in a lump sum, to tide them over the period in which they might be jobless. Since they had been paid out of "confidential funds" they had no civil service status and no retirement benefits; moreover, they were ineligible for transfer to other Government positions. The danger was, of course, that their dissatisfaction with what must have appeared to them as highhanded, arbitrary action on the part of a new official, and that their helplessness in the serious personal situation created for them by his drastic action might lead them to indiscretions which might prove most embarrassing to the Government and have serious consequences upon national defense. It turned out that whatever their private feelings, all the dis-

charged personnel, except the chief beneficiary of the old regime, remained loyal and did the best they could to find jobs.

8. In October 1929 I was sent to New York to take over the boxed up records and files and to oversee their transportation to Washington. The cryptanalytic activities, research, and training now being under the Chief Signal Officer, steps were taken to reorganize the bureau and its work. The funds available were, of course, very slim—only what remained of the War Department's contribution of $10,000 for the FY 1930 was available, because the remainder of the State Department's share of $15,000, as indicated above, had already been withdrawn by the State Department. An offer of employment was made to Mrs. Wilson, the Japanese expert with Yardley, but she was unable to accept, since it involved moving to Washington and she had a husband and child in New York. Another employee, Mr. Victor Weisskopf, had a business in New York and refused to move to Washington. The female clerical employees were deemed unsuitable for our purposes and, moreover, having no Civil Service status they could not be taken on by transfer. An offer of temporary employment was made to Yardley but he refused the tender. Instead, he proceeded secretly to prepare a book which first appeared in the form of articles in the the Saturday Evening Post and which in much expanded form later appeared under the title *The American Black Chamber*. The book and articles were highly sensational and made damaging disclosures concerning the most secret activities ever conducted by the Government. Before the appearance of the articles and book, however, he had taken certain steps to protect himself from possible prosecution for his disclosures, among which was to resign his commission as major in the Military Intelligence Reserve. Of course, had the authorities understood the real purpose of his resignation they might have prevented it so as to retain some hold on him. But being in ignorance of the real motives and deeming it just an act of pique, the resignation was accepted. The unfortunate consequences attendant upon the publication of the book need no elaboration herein. Suffice it to say that [text withheld] our precarious relations with Japan were brought to a boiling point when about 30,000 copies of the Japanese translation of *The American Black Chamber* were sold in Tokyo in a period of less than a month (perhaps the book was subsidized by the Japanese Government itself). The bad odor into which all cryptanalysts and cryptanalytic activities fell, as a result of the difficulties which the publicity given the matter by Yardley's disclosures occasioned high government officials, had a bad effect upon the attempted reorganization of the cryptanalytic bureau by the Chief Signal Officer. *Funds were hard to get*, and State Department support was lacking, if not in the other direction altogether. The most serious consequences of Yardley's disclosures, however, came 10 years later and their effects can hardly be estimated. I refer here to the jolt which his book gave the Japanese cryptographers, leading them out of their blissful ignorance and causing them to develop really complex methods which are now giving us many difficulties. The same is true probably as regards the German and Italian cryptographers—their

education has been entirely at Uncle Sam's expense and the final consequences of Yardley's work can not yet be foreseen. They may well turn out to be disastrous.

9. However, the Chief Signal Officer proceeded, energetically as possible under the circumstances, to carry out the mission assigned him. The code and cipher solving section was placed under the War Plans and Training Division since the compilation section was already there. A rather detailed directive which was prepared by G-2 and approved by the Secretary of War (Exhibit 4), became the guiding plan of the reorganized service, which was now named the Signal Intelligence Service. Its personnel consisting of myself and one or two clerks soon was augmented by a half dozen more employees. Training literature and courses were prepared and put into good usage at once. A great deal was done in expanding our cryptographic work also, by preparing reserve editions of existing codes, compiling new codes and ciphers, developing cipher apparatus, and so on. Cryptanalytic work was put on a firm basis of research and training, with emphasis on the latter, *for there* existed no intercept service and the raw material could not be obtained [text withheld] Hence an intercept service now was organized and grew very slowly. All phases of signal intelligence were unified under one service and taken under study and action. Moreover, cooperation with the Navy in the work was also initiated. How the activity has expanded since then requires no comment at this time. However, a few words about relations with the Navy are pertinent.

10. Cryptanalytic activities in our Navy Department were practically non-existent until after the close of the last war, during which, as was noted above, whatever problems they had in cryptanalysis were referred to MI-8. But in 1921 the Navy, recognizing the important role which cryptanalysis was bound to play in the future, began building up a large unit in the Navy Department, with echelons afloat. Whereas the Army placed emphasis upon civilian training, the Navy placed emphasis upon officer training; and for each dollar the Army was able to obtain for cryptanalytic and cryptographic work the Navy was able to obtain three to five dollars, until by 1939, as far as concerned numbers of officers and civilian personnel engaged in these activities, amount of equipment on hand, and funds available for research, the Navy had considerably outstripped the Army. However, it may be said, with some justifiable pride perhaps, that while they were ahead of us in quantity we were ahead in quality, for all the important developments in both the cryptographic and cryptanalytic fields must be credited to Army personnel. At first, cooperation between the two services was intermittent and at times very indifferent—the usual mutual suspicions and jealousies pervaded our relationships. But, happily, for the past three to five years cooperation has been much more wholehearted, with the result that it may now be said without reserve that, as regards their cryptographic and cryptanalytic activities, cooperation between the Army and Navy is so close as to be the same as though they were under one head. This, of course, is as it should be and must be in order to gain the desired result from such activities.

11. It would be of utmost value to the winning of this war if the Government were now in a position to read the codes and ciphers of all the foreign powers whose actions and probable intentions are of interest and importance in our prosecution of the war. *It could have been in this fortunate position had it given to cryptanalytic studies the attention which it deserves during peace time and had provided funds for their continuity on a scale sufficient for the purpose for which they are intended.* The matter can be summarized very succinctly in this statement: Actual or physical warfare is intermittent, but mental, that is, cryptanalytic warfare is continuous. . . .

* * *

June 29, 1942

William F. Friedman,
Head Cryptanalyst.

From SRH 134. *This official history, written by Friedman in 1945, traces the history of the SIS from its modest beginnings through its triumph in decrypting the Japanese diplomatic machine cipher system. It should be noted that Friedman had no doubt that the activities in which the Signal Intelligence Service was engaged were quite illegal.*

EXPANSION OF THE SIGNAL INTELLIGENCE SERVICE FROM 1930 TO 7 DECEMBER 1941

As a result of War Department General Staff action it was directed by the Secretary of War, on 5 April 1929, "That the Signal Corps be charged with the duties pertaining to the solution of enemy codes and ciphers and the detection of secret inks in War, in addition to those duties with which they are now charged pertaining to the compilation of codes and ciphers required by the Army and to the interception of enemy radio and wire traffic in war."

* * *

. . .the Signal Intelligence Service was to be organized primarily on the basis of *training for war*, rather than for active operation for enemy interception and solution of the communications of foreign governments or armies. However, it was also

stated that if information of present or immediate value to G-2 should be intercepted and solved, such information would be acceptable to G-2, but it was to be clearly recognized and regarded as a by-product of the training work, and not as the fruit of the functioning of the Signal Intelligence Service in peacetime.

But in addition to this foregoing reason for the emphasis on training, there was another important reason. Because of the rigidity of our laws regarding interception of communications, the activities of the Signal Intelligence Service had to partake of the nature of a clandestine activity, since it was illegal to intercept messages, and the penalties for divulging even the existence of a message were severe. The law did not exempt anyone from its penalties, and therefore, the War Department and all the people connected with the work of interception and solution of the communications of foreign governments realized the necessity for keeping the activity secret. By emphasizing the training aspects of its activities, it was thought that the illegal nature of some of the work of the Signal Intelligence Service (interception and solution of foreign communications) could be more easily defended if word of these activities should "leak out." The foregoing reason for secrecy was, of course, to be added to another important reason for keeping the activity secret - namely, the requirement to keep from foreign governments the extent of our success with their communications, and even the fact that we were successful in reading any of such communications. Under such circumstances, therefore, it was only to be expected that the normal channels for obtaining of funds for such an activity would be made somewhat difficult and they were. Up to this time, it must be understood, the War Department support for the solution activities came from Military Intelligence Division Contingent Funds, which are not subject to review by the Controller General.

For one reason or another, none of the six persons who had been working in the old MI-8 Section when the Chief Signal Officer took over the solution activities from G-2 could be added to the staff of the Signal Intelligence Service, which then consisted of one cryptanalyst, (P-5, $4,600) and one clerk-typist (CAF-3, $1,620). A whole new organization had therefore to be built-up with the very scanty funds ($6,666.68) that remained from the original War Department contribution of $10,000 for the rest of the fiscal year 1930. Therefore, to begin with, the real establishment of a permanent Signal Intelligence Service had to await the availability, to the Chief Signal Officer, of funds specifically for the purpose; and then, of course, the long period of training required to produce cryptographic and cryptanalytic skill was another factor that resulted in what may appear to be a rather slow development, in addition to the usual lack of funds.

However, the hiring of new personnel did not have to await the availability of funds, for until the Chief Signal Officer was able to include in his own estimates the specific funds necessary for the support of the Signal Intelligence Service, he could draw by allotment upon the funds available to the Assistant Chief of Staff, G-2. These, however, amounted to only $10,000 per annum. The sum of $6,666.68

was allotted by the Assistant Chief of Staff, G-2, to the Chief Signal Officer for the payment of personnel engaged in code and cipher work on 16 December 1929 for the balance of the fiscal year 1929.

On 4 January 1930 the Secretary of War was requested by the Chief Signal Officer to authorize the employment of four junior cryptanalysts (P-1, $2,000 per annum). Since the G-2 funds ($10,000 per annum) were available to the Chief Signal Officer the FY 1930 and 1931, this request was approved quite promptly; three persons were obtained from Civil Service rosters of eligibles in scientific pursuits (junior mathematicians, etc.) and appointed. An additional person was obtained by Schedule "A" or excepted appointment for the position of Japanese translator (SP-5, $1,800 per annum) because no Civil Service roster of eligibles was available for selection. On 2 September 1930 an additional person (SP-5, $1,800 per annum) was appointed, making the original staff of the Signal Intelligence Service a total of seven persons by the end of 1930. Except for one or two changes in personnel and the addition of one or two clerk-typists, the technical staff was not augmented until July 1938. In 1936 and 1937 a cryptanalyst was sent to each of the Panama Canal and Hawaiian Departments to work as advanced echelons of the Signal Intelligence Service, and these two persons' positions were filled by two additional candidates selected from Civil Service rosters. However, by the end of 1938 both cryptanalysts who had been sent to overseas stations were back in Washington, for the experiment was not a success, and we badly needed them here. What could one lone cryptanalyst do in Panama or Hawaii?

The years 1931 to 1936 were particularly trying ones - promotions were out of the question, and further expansion was greatly handicapped by the program of economy imposed upon the War Department during the depression. Several examples may be cited to illustrate our attempts to expand the Signal Intelligence Service over the years 1931-1938 and the more or less fruitless results thereof.

On 14 October 1931 the Chief Signal Officer requested approval of a project to include four additional positions in the Signal Intelligence Service, involving an increase of $7,240 in his estimates for salaries for the fiscal year 1934. As inclosures, the Chief Signal Officer submitted schedules showing the number of people engaged in Signal Intelligence work in fiscal years 1928-1931 and projecting the numbers estimated by 1934. The request for the four additional positions was "not favorably considered at this time" by the Adjutant General. The reason given was the necessity for holding estimates to a minimum for the fiscal years 1934: "It is not contemplated outhorizing new projects unless current or prospective funds are available."

Again in 1932 an attempt was made to attain urgently needed personnel, with no favorable results. It was stated that the need for expanding the code production program was urgent. In addition to the code compilation duties of the section, there were those of conducting research in solution as well as certain administrative duties in connection with correspondence courses, reserve officer

instructional training courses, and the regular administrative activities concerned in the use, distribution and improvement in code and cipher communication by the Army, the development of cipher apparatus, methods of secret intercommunication between the Army and Navy, the development of radio intercept and radio direction-finding methods, work in secret inks, etc. The assistance of G-2 was sought at the time, since it was thought that in view of the interest registered in the work of the Signal Intelligence Section on the part of the Assistant Chief of Staff, G-2, and the Chief of Staff, it would be the psychological moment to take the matter up once more in the hope that means might be found to add to the personnel of the section, and thus enable it to carry on in an effective manner. Whether or not the support of the Assistant Chief of Staff, G-2, was obtained, the available record does not disclose; however, even if this support was forthcoming, the attempt remained fruitless.

In 1936, the Chief of the Signal Intelligence Service recommended that the time had come to organize the Signal Intelligence activities if the Chief Signal Officer upon a more extensive basis, "in order that personnel for efficient operation may be available when the situation will require their services." It was also considered essential to provice opportunities for advancement for the personnel already employed, in order that a restricted field might be attractive to them. Otherwise, the Signal Intelligence Service would "become merely a training ground for other departments."

A five-year expansion program was recommended, which would increase the total personnel to 21 by 1942, with a total budget of $54,660.

Various obstacles impeded the immediate approval of this plan. In the first place, in order to be able to keep our trained personnel, long-overdue promotions were very necessary; but any proposal for an increase in the salaries of the personnel in the Signal Intelligence Service was held to be objectionable.

(For several years, owing principally to measures of economy imposed by the President and Congress, it had not been possible to provide administrative promotions for any Signal Corps employees. In addition, the President had directed that no promotions were to be included in the 1937 budget.)

A second obstacle was that the personnel and equipment assigned to the Signal Intelligence Service fully occupied its available space, and because of the critical shortage of office and storage space in the District of Columbia, no additional space was likely to be secured for the expansion of that organization. It was suggested that additions to the existing force would overcrowd the area and be detrimental to health and comfort as well as impair the performance of their duties.

This request for personnel was not approved and the four additional positions had to be deleted from the estimates. One of the contributory factors which brought about this deletion was the lack of support from representatives of G-2. Assurance had been obtained from G-2 on advance that it would cooperate in

defense of the item, but its representatives "failed to appear at the hearing when held." Note the following extract from a very interesting memorandum dated 18 February 1936, to the Chief Signal Officer, again requesting an increase in personnel for the Signal Intelligence Service:

> "9. Under the date of March 20, 1935, the Chief Signal Officer requested authority to present in connection with the 1937 estimates, a requirement for two (2) assistant cryptographic clerks at $1,620 per annum, and two (2) junior cryptanalysts at $2,000 per annum. The War Department approved the inclusion of this additional personnel in the Signal Corps estimates. The limiting figure, designated by the War Department under date of August 5, 1935, for Project #1, "Personnel", of the Signal Corps estimates to be submitted to the Bureau of the Budget, was reduced to such a point as to necessitate the deletion of these four positions from fiscal year 1937 estimates. One of the contributory factors in the necessity for this deletion was, no doubt, the lack of support by representatives from the Assistant Chief of Staff, G-2, whose assurance of cooperation in defense of this attempt had been obtained in advance, but who failed to appear at the hearing when held."

At that time it was the opinion of Major W. S. Rumbough, Officer in Charge of the War Plans and Training Division, of which the Signal Intelligence Section was a part, that such "a serious shortage of trained personnel exists in the Signal Intelligence Service," that it could not "fully perform its peace-time mission."If this shortage should "be allowed to continue, no Signal Intelligence Service worthy of the name will be available during the early phase of an emergency when the most valuable results should be expected from this agency."

The memorandum of 18 February 1936 recommended that if funds in the amount of $7,240 accrue by savings, under Project #1, fiscal year 1937, that these savings be used for the employment of two Assistant cryptographic clerks at $1,620, and two junior cryptanalysts at $2,000, to be obtained and trained in this office as soon as possible; alternatively, that if no such savings can be foreseen, funds be diverted from other projects and allocated to Project #1, fiscal year 1937, for the foregoing purpose. But, as already noted, the attempt was fruitless.

It may be stated that about this same time, in May 1936, whereas the Signal Intelligence Service had a total of some seven or eight people, the Navy had some forty, and even the small unit at the United States Coast Guard had seven people. [text withheld] All attempts to increase the complement of seven people comprising the staff of the Signal Intelligence Service were more or less fruitless

until the fiscal year 1938, when four more positions were finally authorized. No doubt one of the factors which led to the final approval of the repeated requests for expansion was the recognition on the part of the high authorities of the War Department of the importance of the work being done. A program of code compilation was being vigorously pursued under severe handicaps; new codes and ciphers were being prepared, printed and placed in storage with two, and sometimes three or more editions in reserve to meet all contingencies. (It is necessary to note that in 1933 the duties formerly assigned to the Adjutant General in connection with the printing, distribution, and accounting for codes, were transferred to the Chief Signal Officer,) thus integrating all cryptographic work in the Army within one organization—the Signal Intelligence Service under the Chief Signal Officer.)

Very important progress in research and development of new cryptographic apparatus and devices was being made; and a high-speed, electrical, cryptographic machine of highest security had been invented and developed by our chief cryptanalyst—this machine being far in advance of anything that had hitherto been known. Moreover, this machine was going into practical usage for secret intercommunication among War Department and the Commanders of overseas departments. An intercept service was being organised to provide the raw material for the cryptanalytic training activities, the first station to be established being that at Fort Monmouth, New Jersey, with additional stations being contemplated in the overseas departments. On the cryptanalytic side much progress had already been made, and by 1934 the training program had reached the stage where actual solutions of current Japanese diplomatic messages were being achieved daily. It is, however, a commentary on the peculiar situation which existed to state that so fearful was the Chief Signal Officer that news of the "illegal" activities of the Signal Intelligence Service might leak out, that these solutions were not issued as "bulletins" or distributed to anybody. Occasionally, one would be shown to the Chief Signal Officer, and it is possible that he would show a translation to the Assistant Chief of Staff, G-2, but it is doubtful if dissemination went any farther than that. When important visitors from the War Department were brought by the Chief Signal Officer to the quarters occupied by the Signal Intelligence Service for inspection or other official business, it was important to emphasize that such solution work as was being accomplished was only a by-product and part of the training being conducted, and that no use was made of the product. It was not until 2 March 1935 that "publication" of the bulletin was started, and G-2 began receiving on a more or less regular schedule the translations of Japanese diplomatic messages resulting from the "training." What distribution or dissemination G-2 made is, of course, not known to me, except by indirect evidence.

It was not until 1939 that any considerable increase in funds for the Signal Intelligence Service was provided, as is shown by the following letter:

September 27 1939

"SUBJECT: Signal Intelligence Service
"TO: The Chief Signal Officer

"1. You are authorized to employ the following designated additional civilian personnel from October 1, 1939, at the annual salaries indicated.

1 Principal Cryptanalyst @ $5,600.	$5,600
2 Associate Cryptanalysts @ $3,200	6,400
2 Research Analysts @ $3,200	6,400
2 Assistant Cryptanalysts @ $2,600	5,200
2 Junior Cryptanalysts @ $2,000	4,000
2 Cryptanalytic Aides @ $1,800	3,600
4 Principal Translators @ $2,300	9,200
1 Principal Clerk @ $2,300	2,300
1 Principal Stenographer @ $1,800	1,800
3 Cryptographic Clerks @ $1,800	5,400
1 Senior Tabulating MachineOperator @ $1,800	1,800
3 Assistant CryptographicClerk @ $1,620	4,860
2 Tabulating Machine Operators @ 1,620	3,240

"2. It is desired that you establish and operate a monitoring station at Fort Hunt, Virginia, and purchase such of the following listed equipment as may be necessary and procurable within the funds allotted:

10 Radio Sets, SCR 243 (or equivalent) @$260	$2,600
29 Radio Sets, SCR 244 (or equivalent) @$195	5,655
18 Recorders, BC 17 @ $1,300	23,400
12 Recording Equipment Tape @ $2,000	24,000
9 Diversity Antennae @ $3,000	27,000
14 Diversity Receiving Equipment @ $1,400	19,600
TOTAL	$102,255

"3. The authorized strength of the Second Signal Service Company is increased by the addition of the following listed personnel. The authorized strengths of Signal units from which these men are transferred are reduced by the corresponding grades and specialist ratings. The allotment of enlisted men to the Signal Corps is increased by twenty-six privates (grade 7). No increase in grades above grade 7 or in specialist ratings will be made until such time as additional grades and ratings become available (probably Nov. 8, 1939).

1 Master Sergeant
1 Technical Sergeant
1 Staff Sergeant
1 Private lst Class, spec. 1st class
6 Private lst Class, spec. 2d class

6 Private lst Class, spec. 3d class
6 Private lst Class, spec. 4th class
4 Private lst Class, spec. 5th class

"4. It is desired that you submit the name of and other pertinent data concerning a Regular Army Officer to be assigned as assistant to the officer in charge, Signal Intelligence Service, and the names of and other pertinent data concerning nine Reserve Officers for active duty under the provisions of the Thomason Act.

"5. Funds in the amount of $41,050 from the Administrative Reserve Signal Service of the Army and in the amount of $50,000 from the reserve now in an unallotted status, subject only to direction of the Secretary of War, will be released to you for the salaries of these civilian employees, for the purchase of additional equipment, and for the expenses incident to operation of the Signal Intelligence Service. The balance necessary for the purchase of equipment will not be available for obligation until the total deficiency of $175,405, required for the expansion of the Signal Intelligence Service has been covered by Congressional appropriations.

"6. You will make necessary arrangements in collaboration with A.C. of S. G-2 to obtain Civil Service exemptions required.

"By Order of the Secretary of War:

/s/ WILLIAM W. DICK
Adjutant General"

The total number of additional personnel for the Signal Intelligence Service in Washington authorized by the foregoing letter was twenty-six; with the original staff of nineteen people, the Signal Intelligence Service staff was to be forty-five persons. Steps were immediately taken to hire the new personel, have them cleared, and to start them in training - a rather lengthy process. Special dispensation had to be obtained from the Civil Service Commission to hire these trainees outside the Civil Service regulations, because no rosters of eligibles in cryptographic or cryptanalytic work existed. In order to obtain the support necessary for such an unusual procedure the Secretary of War requested approval by the President on 26 October 1939 to have the Civil Service regulations suspended so as to permit the employment by the Signal Intelligence Service of not more than twenty-six persons on a temporary basis until 30 June 1940. Through the intervention of the White House, the approval requested was obtained.

The unfavourable way in which the war in Europe was progressing so far as concerned Britain, led to desires to expand the Signal Intelligence Service even more, and as fast as possible. The urgency for cryptographic production to meet the needs of a large United States Army in case the United States became a belligerent was apparent; the output of the cryptanalytic staff was impressive enough to G-2 to warrant further increase of that staff. By September 1940 the Signal Intelligence Service, without the help of any other staff, had succeeded in a most momentous

achievement. [text withheld] - the solution of the Japanese diplomatic machine designated by them as the "B Machine" and by us as the "Purple." Texts of highest strategic and diplomatic import were being furnished G-2 daily, the value of which was recognized by the Assistant Chief of Staff, G-2, the Chief of Staff, the Secretary of War, and the President. The conduct of our difficult negotiations with the Japanese in regard to the situation in the Pacific was no doubt being guided from day to day by means of the solutions furnished the War Department, the State Department, and the President.

On 16 October 1940 the Chief Signal Officer requested of the Assistant Chief of Staff, G-2, authorization for two further expansions of the Signal Intelligence Service, one of which, to begin 1 January 1941, would involve appointment of forty-eight additional civilian employees at annual salaries totaling $85,580, half of which ($42,790) would have to be provided during the fiscal year 1941, then already in progress. No funds for this purpose were available to the Chief Signal Officer, but this expansion was approved by the Acting Assistant Chief of Staff, G-2, with the concurrence of the Assistant Chief of Staff, War Plans Division, on the very next day.

The second request, made on 16 October 1940, was for expansion involving employment of forty-two other employees, who were to begin work on 1 July 1941. This plan was approved in principle by Brigadier General Sherman Miles, Assistant Chief of Staff, G-2, on 17 October 1940, but its carrying out was postponed until the time for the preparation of the budget for fiscal year 1942. The paragraph is of interest:

> "3. The complete expansion of the Signal Intelligence Service to place it on a wartime basis beginning July 1, 1941, as recommended in paragraph 1c and inclosure of the basic letter, is not essential at the present time. The recommendation, however, is for funds to enable this expansion to be begun on July 1, 1941. The uncertainty of the future and the necessity in any contemplated expansion of this service to make provision for a time lag incident to selection and training of new personnel make it necessary to provide for an increase in personnel far in advance. It is recommended, therefore, that funds be made available in the fiscal year 1942 budget to provide for total expansion of the Signal Intelligence Service. If conditions develop prior to 1 July 1941, which make this additional expansion unnecessary, the funds need not be expended."

The letter from the Chief Signal Officer to the Assistant Chief of Staff, G-2, on 16 October 1940, contemplated an expanded Signal Intelligence Service for fiscal year 1942 amounting to 127 persons. The pressure of events was such that the full program must have been approved, for on 7 December 1941, instead of having only eighty-five people, as would have been the case had only the first increment been approved, the strength of the Signal Intelligence Service was as follows:

	Washington	Field	Total
Officers	44	1	45
Warrant Officers	-	-	-
Enlisted	28	149	177
Civilian	109	-	109
Total	181	150	331

The staff was organised as shown in the accompanying chart, with the following sections and personnel:

	Officers	Civilian	Total
Administrative	2	2	4
Personnel	2	6	8
Cryptanalytic			
Japanese	10	24	34
German	1	15	16
Cryptographic	16	10	26
Laboratory	4	-	4
Communications	5	2	7
Tabulating (IBM)	1	15	16
"Trainees" in classes	-	22	22
Total	44	109	153

. . .The nineteen people in professional grades also include Japanese translators; only a few expert cryptanalysts were therefore on hand among those nineteen.

The necessity for producing codes and ciphers has already been mentioned and the staff of 26 persons was hardly adequate for the large volume of work to be done. The production of our electric cipher machines (Sigaba) was under way and there were multitudinous details to be dealt with in that project above: the preparation of instructional manuals for the maintenance and operation of the machine, the elaboration of keying arrangements; the elaboration of what shall go into spare parts kits, etc. Also, the plans for the production of Converter M-209 were under way— a very large project in itself. Besides all this, keys and control tapes for the electric Converter M134A had to be prepared on a current basis, to maintain security of current communications; strips and key lists for the widely distributed Strip Cipher Device M-138A had to be prepared in large quantities; constant liaison with the Navy Cryptographic Division, for the production and distribution of cryptographic material for joint communication required much time, etc. Also, plans for the production of an automatic teletype encipherment system invented by Signal Intelligence Service personnel were being brought to fruition.

The ever-expanding requirements of traffic for the cryptanalytic staff meant expansion in the facilities and personnel of the Second Signal Service Company. Seven monitor stations were in operation by 7 December 1941:

1 - Fort Hancock, New Jersey
2 - Fort Scott, Presidio of San Francisco
3 - Fort Sam Houston, Texas
4 - Post of Corozal, Panama Canal Department
5 - Fort Shafter, T. H.
6 - Fort McKinley, P. I.
7 - Fort Hunt, Virginia

Also, of course, a good portion of our traffic came from the United States Navy, which had a large station at Bainbridge Island, Washington, and another at Bar Harbor, Maine. The mere recording and indexing of the large volume of messages constituted a task of no small proportions.

Hence, even with the large expansion of the Signal Intelligence Service there was much more to do than hands to do with. Consider what was done in the field of solving and translating Japanese diplomatic messages alone. By a special agreement between the Chief Signal Officer and the Director of Naval Communications, all work on Japanese diplomatic traffic was divided up between the Army and Navy on the basis that Army would process all messages of even date (cryptologic), Navy, all of odd date - with full exchange of technical data and results. Thus, in collaboration with the Navy and with a total of only 34 persons, the Signal Intelligence Service was attempting to decode, decipher, and translate its half of the traffic for which the Japanese must themselves have had several hundred persons, and the Japanese, of course, did not have to translate the material, a job which was quite difficult for us because of linguistic difficulties and paucity of qualified translators. Moreover, the Japanese had the necessary keys; we had to solve them, and in many cases solution had to await the accumulation of traffic - it could not always be done with a single message, so that occasion delays in solution were inevitable from the very nature of the systems involved. Also, another factor had to be taken into account: the time required to forward the intercept traffic to Washington. Lacking facilities and personnel to prepare all the traffic, encipher it, and transmit it to Washington, some of it had to await shipment by air mail, and this factor alone occasioned delays. As has been aptly said by General Miles: "The astonishing thing, gentlemen, is not that these messages were delayed, but that they were able to do it at all. It was a marvelous piece of work."

WILLIAM F. FRIEDMAN
Director of Communications Research

Prepared on
4 December 1945

From SRH 135. *Army success in signals intelligence operations prior to World War II was dependent not only on the core of skilled cryptanalysts at SIS headquarters, but on the men who manned what we now call the "front end" of the system: the Signal Corps intercept operators. The Army's Chief Signal Officer, Major General Joseph O. Mauborgne, describes the Army's existing intercept organization and suggests a way to improve it in this 1938 letter. The 2d Signal Service Company he proposed was activated on 1 January 1939.*

WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

OCSigO-320.3-RID September 2, 1938

SUBJECT: Signal Intelligence
TO: The Adjutant General

1. The Signal Intelligence Service in Washington depends for the material with which it works, upon Signal Intelligence Detachments in Hawaii, Panama, Ninth Corps Area and Eighth Corps Area. These signal intelligence detachments are parts of the Signal Service Companies located in the same corps area or department. There has been ordered set up as part of the Tenth Signal Service Company in the Philippine Department, a signal intelligence detachment of 10 men. In addition, so important has the War Department considered the work of the Signal Intelligence Service, it has been thought essential to detach 17 men from the Provisional Radio Intelligence Company at Fort Monmouth, New Jersey, and have this detachment act as a signal intelligence detachment. This last is done even at the risk of crippling the important tactical activities of the Provisional Radio Intelligence Company (to be designated as the 1st Radio Intelligence Company as of November 1, 1938).

2. Whereas the results achieved by the Signal Intelligence Service in Washington are treated with utmost in care and secrecy, equal measures of secrecy are not taken with the personnel of the signal intelligence detachments in the field. The personnel of the signal intelligence detachments cannot long be unaware of the nature of the work in which they are engaged and the ultimate secrecy of the system as a whole depends just as much upon them as upon the personnel in Washington. At present the choice of signal intelligence detachment personnel is left to the corps area and department signal officers and there is no doubt that they exercise every possible precaution. However, in the present form of organization much is entirely out of their hands and beyond the control of the Chief Signal Officer. For example, a skilled member of the signal intelligence detachment in Hawaii is returned to the mainland. Unless he is in Grade 4 or above he is reduced

to the grade of private and returned for haphazard assignment by the normal process. Even if he is eventually reassigned to a signal intelligence detachment on the mainland, he must begin afresh in the grade of private and work himself up. Knowledge of this actuates many to separate from the service; every such man separated from the service carries with him a fairly accurate knowledge of the work upon which the Signal Intelligence Service is embarked and he constitutes just one more threat to the secrecy of the work. He is a far greater threat when separated from the service since he is no longer under military surveillance.

3. The haphazard movement of the enlisted personnel engaged in signal intelligence work also makes their training more difficult and lessens the effectiveness of the Signal Intelligence Service. The useful member of the signal intelligence detachment must be first of all an excellent radio operator and beyond that must acquire skill and experience peculiar ro signal intelligence work: the acquisition of this skill and experience requires from six months to a year under competent instruction. At present, it is not possible to surely retain trained men: indeed it is not even possible to surely retain competent instructing personnel.

4. The remedy to this situation is a signal service company, detachments of which are stationed in the various corps areas and departments as required. The personnel could then be transferred from detachment to detachment without loss of grade or rating and control over the personnel would be increased. To minimize the number of highly skilled personnel separating from the service, the grades and ratings of the company should be considerably higher on the average than is normal in the Army. After many years of experience, the Navy Department adopted just the form of organization here recommended. Obviously, the ideal cannot be achieved by mere statement. However, a great step forward in the secrecy of signal intelligence work and in the training of signal intelligence enlisted personnel can be taken by organizing the several signal intelligence detachments into a signal service company. This can be done without request for any additional men, grades, rating, housing, transportation or equipment.

5. It is therefore recommended that there be organized the 2d Signal Service Company. The personnel necessary are to be obtained by withdrawing from the various service companies the signal intelligence detachments of which are now part of them and by a temporary decrease in the 1st Radio Intelligence Company. (It is proposed not to alter the Tables of Organization of the Radio Intelligence Company, but merely to leave vacant such grades and ratings as are taken to make up the 2nd Signal Service Company: when increases in signal intelligence personnel are granted the Radio Intelligence Company will be permitted to regain its table of organization strength.) Inclosure No. 1, Table of Organization of the 2nd Signal Service Company, shows the strength, grades and ratings of the proposed company. Inclosure No. 2 shows the men, grades and ratings taken from the various companies in order to constitute the Signal Intelligence Company. It will be seen that the organization of the Signal Intelligence Company requires no addition-

al men, grades or ratings from outside the Signal Corps itself. The matter of housing will not be concerned since the detachments are already housed. No additional transportation or equipment will be required because of the organization of the company. The company will be commanded by the officer in charge of the Signal Intelligence Detachment at Fort Monmouth. Detachments of the company will be stationed in the various corps areas and departments just as they are now: they will be attached to the local organization for rations and quarters (the same organizations with which they are now rationed and quartered): their work will be supervised by the corps area or department signal officer concerned, except in the case of the detachment now at Fort Monmouth which will be supervised by the commanding officer of the company.

6. It is intended that the 2d Signal Service Company shall function under general instructions issued by the Chief Signal Officer. Plans for its expansion in time of war and its use in war will be recommended by the Chief Signal Officer for inclusion in the several colored war plans, and the mobilization plan.

/s/ J.O. MAUBORGNE
/t/ J.O. MAUBORGNE
Major General
Chief Signal Officer of the Army

From *The "Magic" Background of Pearl Harbor, Volume IV, Appendix* (Washington, D.C.: Department of Defense, 1977), p. A-89.

The Japanese government dispatched this diplomatic communication to its envoys in Washington, Special Envoy Saburo Kurusu and Ambassador Admiral Kichisaburo Nomura, on 22 November 1941. It was intercepted and translated by the Army's Signal Intelligence Service on the same day. In the aftermath of Pearl Harbor, its language took on a new ominousness.

FROM: Tokyo
TO: Washington
November 22, 1941 (Urgent)
#812

To both your Ambassadors.

It is awfully hard for us to consider changing the date we set in my #736a. You should know this, however, I know you are working hard. Stick to your fixed policy and do your very best. Spare no efforts and try to bring about the solution we desire. There are reasons beyond your ability to guess why we wanted to settle Japanese-American relations by the 25th, but if within the next three or four days

you can finish your conversations with the Americans; if the signing can be completed by the 29th (let me write it out for you—twenty-ninth); if the pertinent notes can be exchanged, if we can get an understanding with Great Britain and the Netherlands; and in short if everything can be finished, we have decided to wait until that date. This time we mean it, that the deadline absolutely cannot be changed. After that things are automatically going to happen. Please take this into your careful consideration and work harder than you ever have before. This, for the present, is for the information of you two Ambassadors alone.

* * *

Trans. 11/22/41 (S)

ARMY 6710 25138

From SRH 115. *This excerpt from hearings held by the Army on the roots of the intelligence failure that led to Pearl Harbor demonstrates all too vividly the feeble resources of the Military Intelligence Division on the eve of war. It also shows how tightly "Magic" was held: Brigadier General Hayes W. Kroner, the head of MID's Intelligence Branch in 1941, was unaware of its existence. This is the transcript of an interview of Kroner conducted in September 1944 by Colonel Carter W. Clarke, Deputy Chief of the Military Intelligence Service. The General Miles mentioned in the text was the hapless Brigadier General Sherman A. Miles, Assistant Chief of Staff, G-2, at the time of the Pearl Harbor attack. "Minxler," whom Kroner describes as the individual who furnished mysterious source materials to one of Kroner's subordinates, was actually Colonel Rex A. Minckler, Chief of the Signal Intelligence Service at the time.*

Place: Room 2C637 Pentagon Building, Washington, D.C.
Date: 13 September 1944
Time: 1430 - 1510

Present: Brigadier General Hayes A. Kroner
Colonel Carter W. Clarke
Lt. Col. E.W. Gibson

Brigadier General Hayes A. Kroner, having been sworn and warned of his rights by Colonel Carter W. Clarke, gave the following sworn testimony:

Col. Clarke: Will you state your name, rank and station.

Gen. Kroner: Hayes A. Kroner, Brigadier General. Station Rio de Janeiro,

Military Attache.

Col. Clarke: When did you first come on duty in G-2, Department General Staff?

Gen. Kroner: About the first of March 1941.

Col. Clarke: What were your duties at that time?

Gen. Kroner: I was assigned to the British Empire Section of the Intelligence Branch, G-2 but before taking up those duties I was sent to England for a period of observation of the war. I returned from England early in June, about the middle of June 1941, and took up my duties of Chief of the British Empire Section, G-2 at that time.

Col. Clarke: How long did you continue on that duty?

Gen. Kroner: Approximately one month.

Col. Clarke: And then what did you do?

Gen. Kroner: About the middle of July I was informed by the retiring Chief of the Intelligence Branch, Col. C. H. Mason, that he was leaving G-2 and that he had been instructed to turn the Branch over to me as next senior officer. I immediately took over charge of the Branch and for the next several months was acting in charge and later on I was appointed Chief of the Branch. To the best of my memory it was about September 17 that an order was issued by the Executive Officer, G-2 appointing me as the Chief of the Intelligence Branch, which position I held until sometime in the month of December, when General Lee became Acting Assistant Chief of Staff, G-2 and I was then verbally relieved from Chief of Intelligence Branch and made Deputy to General Lee.

Col. Clarke: What did the Intelligence Branch consist of principally?

Gen. Kroner: I found the Intelligence Branch, in July '41, to consist of a very small Administrative Section and of several geographic sections and an Air Section. The Administrative Section was in process of transition. Because of the impact of the war and more information coming into G-2, there was a greater need for proper handling and dissemination of that information. The only geographic section of G-2 which appeared to be expanding at that time was the Latin American Section. By the 10th of October—referring here to the official chart on record—the Intelligence Branch consisted of a headquarters or the Administrative Section, Contact Section, Situation Section, Dissemination Section, and the Air and geographic sections composed of the following: Air Section, British Empire Section, Western European Section, Central European Section, Eastern European Section, Southern European Section, Far East Section, and the Latin American Section. The several

European sections had been set up to deal with the increased information coming in from the European war and, together with the British Empire Section, it was considered adequate to handle the war in Europe. The Latin American Section was expanding for obvious reasons of hemisphere defense. The Far Eastern Section at this time had not undergone any material change, so far as I can remember, for several months. This organization, with a few changes, continued during my tenure of office as Chief of the Branch....

Col. Clarke: I understand you to say then that you were Chief of the Intelligence Group from about July through Pearl Harbor, December 7?

Gen. Kroner: Yes.

Col. Clarke: During that time was there any recommendation made—first let me ask you this—who was the Chief of the Far Eastern Section?

Gen. Kroner: Col. R. S. Bratton.

Col. Clarke: During that time was there any recommendation made to you as Chief of the Group for any increase in personnel or expansion of its intelligence gathering activities?

Gen. Kroner: Not any to give me any trouble - there was some minor increase of a clerk or two and perhaps one officer, I don't remember, but nothing in the line of expansion as I have referred to in the European Section. I would say this further, that one of their Far East experts.Col. Pettigrew, was taken from the Far Eastern Section at the time to assist in the reorganization of the Headquarters dissemination, so that I had very close to me at that time an experienced Far East officer on my staff.

Col. Clarke: Who was that?

Gen. Kroner: Pettigrew. It was, I think, worthy of note just here that Col. Betts, who was the Chief of the Situation subsection, whom I called my G-2-G-3 officer on my own staff, Col. Pettigrew being so-called G-1-G-4 officer, together with my own experience in the Far East, that with Col. Bratton it was a fairly good team of Far East trained officers at the head of the Intelligence Group.

Col. Clarke: Was there any action taken by the Chief of the Far Eastern Group that would lead you to think that any difficulties or hostilities were expected in the Orient that would affect the United States?

Gen. Kroner: None specifically as to direct threat in regard to time or date or place. Japanese possible lines of action were often discussed, as you might expect among officers as closely allied as the ones I mentioned above with Far East training and influence. I left the evaluation of information pertaining to the Far

East and its interpretation initially to Col. Bratton, and in that over-all sense to Col. Betts.

Col. Clarke: What was your chief source of information with regard to the Far East?

Gen. Kroner: Military Attache reports and translations of books and journals which were received from various sources, so far as I was aware.

Col. Clarke: You had no secret intelligence service?

Gen. Kroner: No.

Col. Clarke: Was any attempt made to create any during the time that you were in charge?

Gen. Kroner: Yes. I remember the time—I don't remember exactly—but I remember an instance which was partially fulfilled, I believe, that a former Far East trained officer, who I think was retired and living in California, Captain or Major W. C. Clear, was brought into G-2 and given secret briefing by Gen. Miles, to the best of my knowledge, and sent out to the Far East, I think to Singapore, in order to initiate some secret intelligence, of which I have no detailed knowledge.

* * *

Col. Clarke: Did you have access to a source of information which we know as Top Secret or the British known as Most Secret?

Gen. Kroner: Meaning communications information?

Col. Clarke: Signal intelligence.

Gen. Kroner: No, none whatever.

Col. Clarke: You mean you didn't get it or your Branch didn't get it?

Gen. Kroner: I personally as Chief of the Branch did not get it. I was aware that something, which later I found out to be of this nature, existed, but I was given to understand, particularly by Col. Bratton and Col. Pettigrew, who sometimes handled the matter for Col. Bratton, that he received information from Col. Minxler, whom I knew to be in the Signal Corps, which perhaps had to do with Japanese troop movements, which he by long custom and by General Miles special desire, was to handle himself directly with Gen. Miles.

Col. Clarke: Then you don't know what Col. Bratton did with this stuff other than give it to Gen. Miles?

Gen. Kroner: No official information. I frequently remember seeing him leave his office with several parcels under his arm and be gone for some hours, but I felt it was my duty to follow the established procedure which was apparently pleasing to my chief, and I didn't question

the procedure.

Col. Clarke: During the time that you were Chief of the Intelligence Group you never had access or never saw any of this material yourself? When did you first see it?

Gen. Kroner: I only saw the material, which later I learned was called material, when I used to receive it from Minkler's hands when Bratton was absent, and lock it up in my safe and give it to Bratton without sorting it out. In other words, I understood, without any specific orders from Gen. Miles, that he wished it handled that way and therefore I did not violate that procedure.

Col. Clarke: Do you know if any estimates were written in the Far East Section based on this material or any prognostications, forecasts, or predic tions?

Gen. Kroner: I do not.

Col. Clarke: If any had been made you would have seen them, wouldn't you, as the Chief?

Gen. Kroner: I think so because estimates were accustomed to being made, not only at regular intervals, but also special estimates from time to time would be made, the Far Eastern part of which was always prepared initially in the Far East, held by Col. Bratton or under his direction brought into Col. Betts, who revised it and fitted it in with information from other geographic sections. I assumed that the Chief of the Far Eastern Section used all the information at his disposal to make a complete estimate and as accurate an estimate as possible.

Col. Clarke: Did there exist anything like a central evaluating section where all information came in and was there melted into one estimate or report or summary?

Gen. Kroner: No. There was a trend toward that at the end of the year but we didn't get anywhere with it. It was just in the planning stage.

* * *

Col. Clarke: I would like to ask you one more question. In any estimate from the time you took over the Intelligence Group up to and including Pearl Harbor, was there ever any prediction or forecast made of a possible attack on Pearl Harbor?

Gen. Kroner: None to my knowledge. I have in mind the last estimate that was made before Pearl Harbor, which was an estimate covering a future period from December 1 to sometime in 1942.

Lt. Col. Gibson: Did you consider it a capability of the Japanese to successfully attack Pearl Harbor with bombers?

Gen. Kroner: No. The matter was discussed -

Col. Clarke: Did you identify this document?

Gen. Kroner: Yes. I identified it - this is the document to which I referred - IB 159, November 29, 1941. This particular estimate was considered by the whole division, not only the Intelligence Group but by General Miles himself, as perhaps the most important we had ever gotten out. That importance lay not in so much the danger that we saw from Japan, although danger in that field was pretty thorough ly discussed, but primarily because Gen. Miles wished to focus War Department thought on the defeat that could be administered to the Nazi powers. In the preparation of the estimate each geographic section in the Intelligence Branch prepared its part. Colonel - now Brigadier General - Thomas J. Betts put the several estimates together and did what we called "polish them up." He and I discussed the lines of action and the capabilities of all the warring powers and especially of each potential enemy to the U.S.A., and I took them to Gen. Miles where they were finally altered to suit him or approved. This particular estimate does not include in the lines of action open to Japan, an attack on Pearl Harbor, and I remember that so distinctly because when the word came through the radio on that fateful Sunday, December 7, that Japan had attacked Pearl Harbor, I was sitting in my office in the Munitions Building reading from this paper the Japanese capabilities. Therefore from my point of view, I feel that Japan's potential capability against Pearl Harbor was left from this estimate because neither Col. Betts nor I had any information which would lead us to believe that they were capable of or planned to do so.

Col. Clarke: I would like to ask one final question again just to reiterate the fact that you personally had no knowledge of what Col. Bratton did with this most secret material or to whom he showed it?

Gen. Kroner: That is correct, except to Gen. Miles.

Col. Clarke: And you don't know what Miles did with it.

CHAPTER III

Accepting the Challenge

The technical success of American cryptanalysts could not prevent the Pearl Harbor debacle: the intercepted Japanese diplomatic communications had not contained the details of Japanese military planning. In the aftermath of Pearl Harbor, American policymakers realized that some better way had to be found to produce finished intelligence from COMINT intercepts. Secretary of War Henry L. Stimson called upon the services of the distinguished Chicago lawyer Alfred W. McCormack to solve the problem. McCormack recommended the establishment of a Special Branch within the Military Intelligence Service to handle highly sensitive signals intelligence. This proposal was adopted, and McCormack was commissioned as a colonel and became deputy head of the new organization. McCormack tells the story of the inception of the Special Branch in SRH 116, Origin, Functions and Problems of the Special Branch. The excerpt from SRH 141, Papers from the Personal Files of Alfred McCormack, Colonel AUS, Special Branch, G-2, Military Intelligence Division, War Department, Volume II, details some of the problems surrounding the effort.

From SRH 116. *Writing in 1943 to his superior, Colonel Carter W. Clarke, the Chief of Special Branch, Colonel Alfred McCormack describes the organization they both had helped to shape.*

ORIGIN, FUNCTIONS AND PROBLEMS
OF
THE SPECIAL BRANCH, M.I.S.

April 15, 1943.

MEMORANDUM FOR COLONEL CARTER W. CLARKE:

Subject: Origin, Functions and Problems of the Special Branch, M.I.S.

Following our recent discussions, I am putting down in this memorandum what seem to be the important facts relating to the Special Branch, in the hope of clarifying the problems now confronting us.

A. *Responsibilities of War Department for Intelligence Derived from Cryptanalysis.*

The outstanding feature of "black chamber" activities in the United States is that they are performed almost exclusively by the armed services and that the great bulk of the work is done by the Army. The F.B.I. and the Coast Guard operate in certain limited fields. The Navy confines itself exclusively to naval traffic. The Army is responsible not only for military and M/A traffic but for the large residual field that is loosely called "diplomatic," which includes the great bulk of the important traffic over commercial, official and semi-official radio networks throughout the world.

[text withheld] From the standpoint of the Army the present U.S. arrangements are the most desirable, especially in time of war. The Army is not dependent upon the State Department, [text withheld] for its information about all the complicated cross-currents of political and economic diplomacy and for the enormous amount of intelligence that is found in foreign official messages. On the contrary, the State Department is dependent upon the Army, which now controls the sources and determines the order of priority in which those sources will be exploited.

The continuation of Army-Navy control over such sources is important for the immediate necessities of war, and it is at least equally important for the long-range future. The availablility of important intelligence from cryptanalytic sources, during the critical 18 months prior to December 7, 1941, was due solely to the fact that the Army and the Navy, in the face of difficulties and even legal prohibitions, were able to maintain skeleton organizations in this field, in preparation for the day when they would be vital to the national defense. The armed services are the safest repositories of cryptanalytic material and activities, since they can operate with greater

secrecy and with a longer-range viewpoint than can the political agencies of the Government. The chances of continued cryptanalytic progress after the war are believed to be better if control of the field remains in the armed services than if the non-military fields are taken over by a civilian agency.

However, control involves responsibilities, and in case of the diplomatic traffic it involves specific commitments to the President and to the State Department to get as much usable intelligence as possible out of the material.

B. *Handling of Intercept Intelligence Prior to the War.*

When this country declared war, both the intercept work and the cryptanalytic work in the diplomatic field were divided between the Army and the Navy, though actually most of the work was being done by the Army. The combined intercept and cryptanalytic facilities of the Army and Navy had produced some 7,000 decrypted and translated messages in the 6 months before Pearl Harbor, or an average of about 300 per week, of which only 1,561 were considered of enough significance to be filed for future reference. The responsibility for bringing important messages to the attention of the Secretary of War and the top officers of the Army was vested in the Chief of the Far Eastern Section, M.I.S. O.N.I. served the President, the Secretary of the Navy and the top officers of the Navy.

In M.I.S. the material was handled as follows: Each day's batch of messages was examined by the Chief of the Far Eastern Section. Those not considered important were put aside for burning. Those that were thought important were circulated to the Secretary of War, the Chief of Staff, the Assistant Chief of Staff, Op.D., and the Assistant Chief of Staff, G-2. One copy of each circulated item was put into a locked file; the other copies were burned after they had been returned by the readers. No personnel were assigned to a continuous study of the material; hence very little could be done to put any of it together in connected form. The Chief of the Far Eastern Section, M.I.S., having as such a full-time job and limited personnel, could do no more with the messages than carry the important facts in his head.

C. *Decision of the Secretary of War Concerning Exploitation of Cryptanalytic Field.*

When the sudden attack on Pearl Harbor occurred, it became apparent that the event had been clearly foreshadowed in the Japanese traffic of 1941. The Secretary of War, and no doubt others, than concluded that the traffic had not been given sufficiently close attention, and that some agency should be set up to deal with cryptanalytic intelligence in a more thorough-going fashion than previously had been thought necessary. The Secretary decided that the job ought to be undertaken by a lawyer having a special type of competence and training, such as may be acquired in the handling and presentation of large cases involving complicated facts.

After consulting with the Assistant Secretary, Mr. McCloy, about possible candidates, the Secretary authorized Mr. McCloy to offer this assignment to me, my experience over a number of years having been along the indicated lines. The mat-

ter was put up to me early in January, 1942, and after some discussion I agreed to undertake the job, resigned from my law firm, and took office as a Special Assistant to the Secretary on January 19, 1942.

On that day I received my instructions from Mr. Stimson. Briefly, they were that I was to study the problem and determine what had to be done in order to expand the cryptanalytic operations to meet the requirements of war, and to make sure that all possible useful intelligence was derived from the cryptanalytic material. Both the Secretary and Mr. McCloy emphasized the need for close and continuous study of intelligence derived from cryptanalytic activities and of piecing such intelligence together in connected form.

For two months I studied the back materials, investigated production facilities, had numerous conferences with Mr. McCloy, General Lee and others interested, and made recommendations as to what should be done and how the work should be handled. The details are no longer of any importance. Everyone agreed that there was a very large job to be done.

D. *Organization of M.I.S. Section to Handle Intercepts.*

Shortly after I started work, there was set up in the Far Eastern Branch of M.I.S. a section which was to follow and report upon the cryptanalytic material. It soon became apparent that there were at least two fundamental differences of opinion between the officer chosen to head that section and myself.

First, I disagreed with the notion that any reserve officer, or any civilian who had been graduated from college, was qualified to handle cryptanalytic intelligence. It seemed to me that the job could be done effectively only by persons with very special qualifications; that the most careful selection of personnel was necessary, and that only individuals of first-rate ability and suitable training should be taken into the work.

Second, I disagreed with the method that was adopted for reporting the intercept material, which was to take what looked interesting and to pass it along in paraphrased form, without any attempt either to check or evaluate the information or to supplement it by collateral intelligence. It seemed to me that the Secretary, the Chief of Staff and the others to whom reports were made were entitled to have every item carefully checked, evaluated and supplemented by all possible sources of intelligence, and that their time should not be wasted in reading odd and unchecked bits of information not related to attendant circumstances and given their proper value. Further, it appeared to me that the daily reporting of current messages was only one part of the job; and that the real job was to dig into the material, study it in the light of outside information, follow up leads that it gave, and bring out of it the intelligence that did not appear on the surface.

E. *Organization of Special Branch.*

My investigations of the intercept and cryptanalytic problems brought me in contact with you, and we had many discussions on the subject and some discussions with General Strong. His thinking was along the same lines as ours and he

approved of our conclusions. The upshot was that the M.I.S. section in charge of cryptanalytic activities was made the Special Branch, with you as its Chief. We moved into common quarters and worked together, your staff (part of M.I.S.) and my staff (part of the Secretary's office) being made into a single working unit as fully as if they were all part of the same agency. You concentrated on pushing the expansion of the intercept facilities, on setting up a workable system of priorities, and on the many technical problems that were encountered. You were fully familiar with those problems and had arrived at the same conclusions that I was reaching, with respect to the necessity for a great expansion of the intercept facilities and for an attack on the cryptanalytic problems on a much broader basis. You were largely instrumental in inducing the Signal Corps to embark upon the program that it is now carrying to completion, involving the acquisition and development of Arlington Hall, the location at Vint Hill of one of the largest intercept stations in the world, the expansion of facilities at Two Rocks, California, and elsewhere, and a personnel program reasonably adapted to requirements of a war-time job.

Meanwhile, I concentrated on recruiting a suitable staff and on the problems involved in getting intelligence out of the intercepts and devising methods of checking, evaluating and reporting it and of keeping track of it by suitable files and indexes. General Strong and you felt that it was desirable for me to go into the Army, and I was commissioned in June. Thereafter the Special Branch absorbed the staff that the Secretary's office had assigned to me.

F. *Work of the Special Branch.*

* * *

It seems fair to say that we have a good organization of people well above the average level of competence, who work full steam and on the whole have given a good account of themselves. Our so-called "Magic Summary" appears to be accepted as a satisfactory job of reporting. At the Navy's request a copy now goes to the Secretary of the Navy, and at the State Department's request copies now go to the Secretary of State and to the Assistant Secretary of State who follows cryptanalytic intelligence.

A great deal of our work does not get into the "Magic Summary." I think we probably do more work in deciding what to exclude from the Summary than we do on items that are put into it. We try to avoid reporting more details, and we consider that those to whom we report should not be bothered by material which, if properly checked and studied, would be found to be of no value.

A lot of our work, from the reporting angle, consists in feeding information to the M.I.S. geographical sections, to other agencies of the Department, and to outside agencies. We employ one officer full-time in verifying Order of Battle information and reporting such information to the O/B sections and the Air Branch of M.I.S. When security considerations permit, we pass on economic information to

the B.E.W. We are constantly called upon for information by those in the State Department who have access to our material, and we employ one officer full time in serving the State Department and getting necessary information from them. We prepare periodical reports on South American information for the Coordinator of Inter-American Affairs. When information is of a sort that the Assistant Chief of Staff, G-2, should bring to the attention of other agencies, such as the O.S.S. or the O.W.I., we prepare reports or paraphrases for his signature.

The whole body of intelligence which flows out of intercept material, into the various sources that have been mentioned, adds up to a considerable amount. This memorandum will not attempt to evaluate it, as compared with other sources of intelligence, but it may be worth while to mention a number of examples of important intelligence material, with which the readers of the "Magic Summary" will be familiar:

a. Practically the only good information about the relations between Japan and Russia has come from the intercept material. Much of it has not been obvious on the face of the material, but has required a great deal of study and collateral research in order to piece it together. (At a time when almost everyone expected Japan to attack Russia, and when M.I.S. went on record as predicting such an attack at an early date, we had concluded from the intercept material that Japan had no intention of attacking Russia, but wanted to keep out of war with Russia at all costs.)

b. The best information about the attitude and intentions [text withheld] following the African invasion, came from that source.

c. That source has also yielded, in addition to considerable information not otherwise obtainable about Japan, the most accurate and dependable information about the relations between the Japanese Government and its Axis partners and about trade between Axis Europe and the Far East. [text withheld]

Many other examples of lesser importance, but of the same general type, might be given.

It would take a lot of space to give a good picture of what might be called the "detail intelligence" that we get, of its present value and of the future value that it may have as it gradually builds up facts. Perhaps the picture can best be given by the following illustrations:

The nature of the materials bearing on the Far East is such that the most astute person, even if an expert on the Far East and possessed of a photographic memory, would derive few connected impressions—and very little usable information—from merely reading the messages from day to day. They must be pieced together by the most painstaking and laborious process, involving collateral investigation, often of minute points. The work is very difficult, but the rewards in the way of intelligence are substantial. For example:

As you know, we are in possession today of enough information about Japanese shipping to and from Indo-China and Thailand so that we have a pretty

clear picture of the movement of supplies on those runs and of the problems that Japan is encountering in getting raw materials out of those areas and keeping them supplied with the minimum of essential imports. Our information has been put together from an infinite number of scraps of fact. As you recall, the material on this subject was not at first very promising. It looked hopeless to make any connected sense out of the garbled texts, incomprehensible ship names, abbreviations and alphabetical designations, and the inconsistent tonnage figures, loading reports and ship schedules, especially because in many cases the key messages had not been intercepted.

Finally, however, by struggling with the S.S.D. translators, doing research on Japanese merchant vessels, gradually identifying ship names, eliminating duplications of cargo information, checking ship tonnages and schedules and, in general, applying what might be called high class detective methods, we built up a picture that is clear and substantially complete in its principal parts. Having built up that picture, it is now possible for us to follow the pertinent messages from week to week and to understand what they mean. Had the job not been done, the current messages would be largely incomprehensible.

Since Japanese shipping has been selected as an illustration of the piecing together of incomprehensible bits of intelligence into a connected whole, it is interesting to note that we arrived at several conclusions about Japanese shipping which made it necessary to change previously accepted figures. For instance, we established that the Japanese have been employing at least 450,000 tons of merchant shipping in the South Pacific, whereas the J.I.C., apparently with the approval of the Navy, recently published a study which showed that only 300,000 tons of shipping were employed in moving goods to and from that area. We brought our findings to the attention of O.N.I., whose people first explained them away. A few days ago, however, we were advised informally by O.N.I. that they now agree with our findings and that, while they do not want to revise their published figures at present, they will make the corrections when they next issue a report.

This little story has a pertinent moral. Until we gave them the above and certain other findings on Japanese merchant shipping, the O.N.I. people were polite and cooperative, but they stopped short of giving us their own secret information. But, when we brought them to our office and explained what we were trying to do and how far we had progressed, they offered to put at our disposal all their own information on the same subject. Since that time, which was last fall, they have prepared for our special use and delivered to us each morning a summary of all information received on the previous day about merchant shipping in the Far East, from sources other than our own material.

From this daily report, pieced together with our other material, we are building up a wealth of evidence on the movements of Japanese vessels and cargoes. We have hopes that the time is not far distant when we will have the whole picture of Japanese shipping and water-borne trade reconstructed to a point where its main

outlines will be clear and many if not most of the important details will be known.

The above is given as a sample of the work that we are trying to do; and while this memorandum is not intended as an analysis of S.S.D. traffic, present or potential, it may be worth while to carry the story just a little further:

Japanese shipping is only one of the important subjects on which the intercepts are gradually building up connected and definitive information, not obtainable from any other source. Referring only to the Far East, it is our hope that over the next year, if the same kind of material keeps coming in and if sufficiently painstaking work is done on it, we will have the Far Eastern picture—except perhaps for the East Indies—pretty well reconstructed in its economic and political aspects and be able to make increasingly accurate diagnoses of Japanese capabilities, difficulties and plans.

The story of the Dutch East Indies is buried, we think, in the water transportation traffic of the Japanese Army. The cryptanalysts at Arlington Hall think they have solved the cryptographic system in which this traffic is sent and that in 1, 2 or 3 months they will have built up code values to a point where the traffic will be completely readable. If that should prove to be true, then the East Indies will be opened up from the intelligence standpoint and the geographical coverage of the Far East will be complete.

G. *Increase in Volume of S.S.D. Material.*

Meanwhile, coverage is being extended, new systems are being solved and translation and processing facilities are being built up. [text withheld] In the 6 months before Pearl Harbor almost all the traffic produced was Japanese, with a scattering of German [text withheld] messages. A large volume from many sources is now handled, and language coverage has increased [text withheld]

The recent solutions of the German Key Word Code and the Japanese M/A Code represented substantial progress in cryptanalytic work; and the expected solution of at least one of the highest grade Japanese military ciphers—and possibly of the whole Japanese military system—will, if it occurs, be an event of major importance from the intelligence angle.

Intercept coverage has been extended by the development of 3 large fixed monitoring stations, giving approximately global coverage for what is broadly described as "diplomatic" traffic, and by field radio intelligence companies. Not only do the new stations permit more intercept facilities to be used, but the better antenna installations and better equipment make it possible to listen to circuits at times when previously they could not be heard. For example, until completion of a recent installation at Vint Hill, the Berlin [text withheld] circuit could be listened to for an average of perhaps one or two hours per day. Now it is estimated that the good listening hours have increased to 8 to 10 hours per day, and possibly more. When the Fairbanks station—the only one that can listen to traffic between Tokyo and [text withheld] —gets new antennas, as it will when the spring weather comes, the amount of traffic intercepted from those circuits should increase from a mere

driblet to a substantial volume.

During the month of March we received 4,500 deciphered messages from Arlington Hall. This was still only a fraction of the available material, as may be shown very readily by the figures for the messages [text withheld] during March.

	Total
Japanese Army and weather traffic	91,596
Other traffic	22,489
	114,085

The bottleneck—by reason of which this Branch received only 4,500 messages from Arlington Hall in March, as compared with our 22,000 (excluding Japanese military) [text withheld] lies in the processing and translating facilities of Arlington Hall, which are largely a problem of civilian personnel. They had 105 civilians on December 7, 1941; they had 1,754 on February 1, 1943 (the last date when we obtained exact figures). They now have over 2,300 and their T/O calls for 3,683 by June 30, 1943. It is estimated that—apart from the problem of Japanese military tarffic—the volume of S.S.D. material coming into the Special Branch will at least double by the end of June. It will continue to increase as the successive bottlenecks are eliminated. More traffic will be intercepted; more will be decoded; more will be translated. Leaving out of account the Japanese Army traffic, the total volume could easily increase four-fold by the end of the year.

This increase of material emphasizes our manpower problem. But the problem exists independently of the question of volume,and the factors involved in long-term planning are much more important than merely the question of handling a certain number of intelligence items per day.

H. *Basic Factors in the Problem of Cryptanalytic Intelligence.*

Certain considerations that are fundamental to our problems may be mentioned:

a. An effective intelligence agency—especially one that must deal with such difficult material as decrypted intercepts—cannot be built up by writing a T/O and filling the places with what personnel happens to be available. To do the work well, a man must have not only a broad education and background of information, but must have more than his share of astuteness, skepticism and desire to solve puzzling problems; and he must have a capacity for laborious detail work that very few people have. As you know, we have had 2 cases of men who proved incapable of doing our work, though both of them had had fairly successful careers in civil life. Not only were they able to produce nothing by their own efforts, but they used up so much time of others working in the office, and made so many mistakes that it took time to correct, that we found our net efficiency increased by taking them entirely off the work and inventing jobs to keep them busy until they could be assigned elsewhere.

b. One principal reason why exceptionally qualified personnel are required in the intelligence agency that deals with cryptanalytic material is that such an agency cannot afford to make mistakes, because it tends to become a focal point in intelligence activities. There are several reasons for this:

(1) Intelligence from intercepts, where the material is first-hand and of dependable origin, is the most reliable information and frequently the first to arrive. Hence it is looked to as a primary source of high-grade intelligence.

(2) Much of the intercept material consists of odd pieces of information and sometimes no more than a clue, which can be understood or followed up only in the light of information that must be obtained from other sources. Hence the processors of intercept intelligence tend to draw into themselves—and must draw into themselves to be effective—the intelligence output of other agencies. This they must put together with what they have; and if their own information is good they are likely to come out with more accurate and better evaluated information than is elsewhere available. We see this constantly in comparing our information on various topics with information put out by the B.E.W., O.S.S., J.I.C. and other agencies.

(3) Because they must constantly seek information from outside sources, those who deal with intercept intelligence have an opportunity to learn what the good sources of information are on a wide variety of subjects. In view of the multiplicity of intelligence agencies and would-be intelligence agencies in Washington, the large amount of duplication of work, and the penchant of certain agencies to bring forth a stream of classified reports that are inaccurate and, in many instances, not much more than irresponsible guesswork, this is a very important point. (For instance, though the Joint Intelligence Committee is among the least of the sinners in this respect, I think it fair to say that its Weekly Summaries in the past two months have contained a number of inaccuracies and some positively erroneous or misleading information, which this Branch, at least, would never have put out under any circumstances.)

c. The guiding consideration in the internal arrangements of the organization that handles cryptanalytic material, and in its methods of dealing with outside persons and agencies, is the consideration of security. One lapse of security is all that is necessary to dry up a radio intercept source. Therefore, both on the officer level and below, only persons of the greatest good sense and discretion should be employed on this work. This consideration is basic, since intercept information involves a different kind of secrecy than does most other classified information. It will make no difference a year from now how much the enemy knows about our present troop dispositions, about the present whereabouts of our naval forces or about other similar facts that now are closely guarded secrets. But it will make a lot of difference one year from now—and possibly many years from now—whether the enemy has learned that in April 1942 we were reading his most secret codes. Not present secrecy, not merely secrecy until the battle is over, but perma-

nent secrecy of this operation is what we should strive for. That may be too much to hope for in a democracy; but if it is possible to attain or approach it we should try to do so.

d. An essential job of the Special Branch, which must be done if it is to produce this maximum usable intelligence, is to establish intercept priorities, keep them constantly in tune with intelligence requirements and see to it that those who operate the intercept stations shall understand and follow them. Only a small fraction of the world's radio traffic can be listened to, with the facilities that are at hand or obtainable. To deal with the priority problem there must be a continuous appraisal of materials coming from the various circuits, of the probable intelligence value of what might come from other circuits and of the week to week necessities from an intelligence angle. The whole question is infinitely complicated and time-consuming, as witness the fact that you and Col. Taylor and I spent many days on the last priority directive. But it is an absolutely essential job to be done. With Col. Taylor going to London we will have to find some other man to spend a good part of his time on the intercept priority problem.

e. Another essential job is to establish cryptanalytic priorities and keep track of cryptanalytic projects. Cryptanalysts are scarce and their time must be used to best advantage. This requires a degree of liaison that we have not yet been able to realize, from lack of man-power. This problem, moreover, is closely interwoven with the intercept priority problem. If you are to put the cryptanalysts on a new project when they have finished the one that they are now working on, you must devote a part of your intercept facilities to the building up of a large volume of traffic in the as yet unreadable code, so that when the time comes to tackle it the cryptanalysts may have enough materials to do the job.

f. Still another essential function of the Special Branch is to supply the cryptanalysts with leads and clues, and with intelligence in general. The art of cryptography has outstripped cryptanalysis, to a point where high level codes and ciphers are no longer broken by cryptanalytic methods alone, even though modern machinery is capable of almost miraculous performance in the analysis and synthesis of cryptographs. Today it is collateral intelligence which solves high-grade cryptographic systems. While that intelligence can come from a number of sources, in the nature of things the best source is the intelligence organization that struggles day by day with the cryptanalytic output and is familiar with what the cryptanalysts are trying to do and what their needs are. From the long term standpoint the Special Branch's function as a feeder of intelligence to Arlington Hall is hardly less important than its function of getting intelligence out of what Arlington Hall produces. We have done a lot of work along this line; but we would be doing a great deal more if we had more help.

g. The experience of the Special Branch has proved that astute people working on the special materials have opportunities to furnish intelligence that leads directly to the solution of codes. Lt. Littlefield, for example, is directly

responsible for the recent solution of the cryptographic system used by the Germans in communicating from Berlin to agents in South Africa. From his study of other intercept material he came to the conclusion that a certain class of unreadable radio traffic was being beamed to South Africa, although the intercept people, including those of the Coast Guard, were positive that it was being beamed to South America. He insisted on this position, and informed the cryptanalysts what he thought the messages might deal with; and they applied probable meanings to the messages that they had. The solution of the code followed very quickly, and the contents of the messages proved that Lt. Littlefield's guesses had been correct.

h. Intercept coverage and cryptanalytic work has one very important purpose that is sometimes lost sight of, in addition to the job of getting intelligence out of the messages. That purpose might be described as protective monitoring. This has many phases, of which the following are illustrations:

(1) We get from S.S.D. a large volume of samplings of [text withheld] traffic, some of which has to do with ship movements, deliveries of airplanes and munitions, assignments of military personnel, placing of orders in the United States, and other subjects having military aspects. Almost none of this material is ever reported by us. Nevertheless we follow it very closely, in order to make sure that it does not become a source of valuable information to the enemy... [text withheld] It is our practice to check each item of information to determine whether it is one that the enemy could not get from other sources, whether, if it is, the information is of importance and, if it is important, whether the degree of importance warrants taking some action. Generally our conclusions have been negative; but in one or two instances General Strong's attention has been called to such a problem and he has alerted those dealing with [text withheld] to the dangers involved in giving certain information and in doing business in such manner as to require too much use of the radio.

(2) Another aspect of "protective monitoring" is to keep on the alert for any evidence that the enemy is reading our own codes or the codes of other nations. Since everybody appreciates that codes will be changed or abandoned if the users discover that other countries are reading them—and since, therefore, everybody tries to be very careful about transmitting information from intercept sources—the most meticuluous "detective work" is required in dealing with this problem.

* * *

(3) Still another aspect of this subject is to keep track of the enemy's sources of information and to keep posted about what he knows. Prior to the landings in North Africa, attention was directed to all available traffic that might reveal the enemy's knowledge, and it was examined with great care with that in mind. The cutting down of Axis code communications by Chile and later by Argentina was brought about by our State Department because they knew from

intercepts what kind of information the enemy was getting, knew how much pressure on the two countries was justified by the facts, and knew, finally, what ace they had in the hole in case they should be forced to use it. The location by [text withheld] intercept activities, of enemy agents who were sending valuable information to Berlin and Rome, has enabled them to deal with the problem in some instances in a different way, viz., by buying up the agents and getting control over the Axis source. There are several places in the world today where the problems of Axis communications are a live and important issue.

i. U.S. operations in the field of cryptanalytic intelligence are relatively limited. For various reasons, including the piety of the State Department and the fact that our Army was starved for funds prior to the war, we entered the war with relatively little experience in cryptanalytic matters, and with even less experience in dealing with intelligence from intercept sources. This is certainly true as compared with the British, and we have reason to suppose that the Germans—and to suspect that the Russians—were also far ahead of us. While we have made progress, we have a long way to go. Large as it is, our S.S.D. operation is on a much smaller scale than the various comparable operations of the British. This is also true of the intelligence side of the picture; and so long as it remains true, we will continue to be at a disadvantage

* * *

m. There is one aspect of our relations with the British in intelligence matters that has struck me very forcefully. Our intelligence agencies in Washington appear to spend a lot of their time keeping information secret from one another, in competing for credit and in beating one another into print. All of them have some liaison or other with the British intelligence agencies; and for some reason they are freer in giving information to the British than to one another. The British do not keep their information in water-tight compartments, nor do their various agencies seem to care who gets the credit. They are so set up that their intelligence is put together and evaluated; and the job is done promptly. This gives them a great advantage over us in intelligence matters.

n. We have had enough to do with the British to have discovered that there is a considerable amount of intelligence which they withhold from us, not especially by design, but because we do not ask for it. Sometimes it is not asked for because nobody knows it exists. Recently, for example, we have discovered that certain intercept information about Continental Europe, which does not flow regularly into any American channels, is available to us at the Embassy, merely because we deal with cryptanalytic material and have established a certain amount of confidence in our judgement and discretion. If Major Heneman, who has pursued this contact, were not encumbered with a large burden of other work, and could spend half his time at the Embassy, I am confident that he could bring into the United

States channels of intelligence a substantial amount of valuable information that either does not get into those channels at present or gets into them too late to be of the greatest value.

o. A fairly important problem that we have—one that will grow with the volume of traffic—is the problem of increasing the proportion of Arlington Hall intercepts which are at least scanned for their intelligence content. The problem exists in all languages covered, but it is particularly acute in the Japanese. Because of the shortage of cryptanalysts and translators, not all decipherable messages can be deciphered, and not all that are deciphered can be translated. There is a scanning and selecting process at both the cryptanalytic and the translation stages. This is done by the cryptanalysts and translators themselves; and on the whole they do a good job. However, to insure that no useful intelligence is missed, the organization handling the intelligence should participate in the process of selection and should continually educate the cryptanalysts and translators in the week to week intelligence needs. This is done in the British Black Chamber organization, and it is done in the Navy organization. We have assigned Capt. Ervin as liaison with Arlington Hall, and he will be able to do this to some extent. However, there are so many liaison requirements that an additional officer will have to be provided before long, if we want to be sure that the work is done thoroughly. In addition, there is a specific need for a man familiar with the Japanese language, to deal with Japanese translators. We have such a man, Dr. Creel, who because he is also a Chinese scholar can help the translators on one of their most difficult problems, which is to identify Chinese names from their Japanese Kana versions. He has already helped them a great deal. But, until we get some additional personnel, he cannot take much time away from the day to day job of handling Far Eastern material.

p. The WT/I field, and the relations of the Special Branch and Arlington Hall's work in this field, are matters that are now under study, and I mention the subject only for the record.WT/I—the derivation of intelligence from radio traffic by all means short of cryptanalysis- [text withheld] It has, of course, numerous applications in the field; and it is of special importance to the Navy. Arlington Hall has been experimenting with Japanese Army traffic from the WT/I angle; and the prospects for deriving intelligence from it look promising. But the development of this work, to judge from what I have seen of it thus far, is going to require a close liaison with the military intelligence and, from our standpoint, the full time of at least one man....

I. *Personnel Situation of the Special Branch—Officers and Civilians.*

In the foregoing somewhat discursive remarks, which by no means cover the whole subject, I have tried to show that our problems have many sides, that the field of cryptanalytic intelligence is important, and that there are great opportunities in this field if we are prepared to seize them.

Whether or not the objectives that we have in mind are sound, I think the problems at least are of some real importance to the country. The adage that knowledge

is power is nowhere truer than in the field of international relations, especially during a war and in preparation for peace. We are gaining knowledge and experience in many parts of the world, some of it rather expensively; but we still have a lot to learn. In the field of intercept intelligence we have at hand, in my opinion, one of the greatest potential sources of information; but we are not making the most of it. We need to raise our sights.

The above statement of our problems may indicate why the present manpower of the Special Branch is not adequate to do the job that we want to do. A quick picture of our manpower (excluding you and myself) may be given as follows:

Total officers	30
Civilians comparable to officers	9
	39
Deductions must be taken for:	
Officers who work in the Cryptographic Security Section and Radio Communications Section (transferred from C.I.G.) who have nothing to do with S.S.D. material	5
Officers who do purely administrative work, which is very heavy because of security requirements and the large volume of paper work that passes over your desk	3
Officers about to be transferred to Ground Forces (2) and to London (1)	3
Mr. Bingham, who has enlisted and is about to be inducted in the Army	1
	12
Balance	27
To get the net working forces on the intelligence job, certain additional deductions of men on special assignments must be taken, as follows:	
Major McKee (Order of Battle specialist)	
Capt. Berle (Liaison with the State Dept.)	
Capt. Calfee (Only technically assigned to the Branch, doing most of his work for AIS. . . .)	
Capt. Ervin (in training at Arlington Hall, to be a liaison officer with	

that organization)	
Mr. Randolph (about to commence training at Arlington Hall, to work on WT/I material)	
Lt. McCluney (temporarily spending full time on personnel work)	
Lt. Wilkinson (just relieved as Security Officer and engaged in training his successor)	7
Present net working force on intelligence material	20

According to their work and the parts of these 20 men are assigned as follows, the world that they keep track of:

Editing "Magic Summary" and studies	3
Reading and routing collateral intelligence material from regular sources	1
Biographical Section	2
Far East	6
Near East	1
Eastern Europe	1
Central and Western Europe	3
Southern Europe and Africa	2
Latin America	1
	20

Considering the volume of material that we have to handle and the job that we are trying to do on it, the figures above speak for themselves.

* * *

Alfred McCormack,
Colonel, G.S.C.

From SRH 141-2. *In a moment of discouragement about the Army's relative lack of success in exploiting Japanese military (as opposed to diplomatic) communications, McCormack wrote this memorandum to his immediate superior. Like a great many of his memoranda, it dealt with personnel. The B Branch of MIS, mentioned in the correspondence, handled Japanese military decrypts; A Branch handled diplomatic materials; C Branch, the German intercepts provided by the British. Ironically enough, at the time he wrote, SSA and Special Branch were on the verge of a definitive breakthrough in deriving intelligence from Japanese Army messages.*

3 Jan 44.

MEMORANDUM FOR COLONEL CLARKE:

Subject: Personnel Problem of B
Section, Special Branch.

1. This attempts to state the problem of getting intelligence out of the Japanese Army material, specifically from the standpoint of personnel requirements.

2. The United States entered the war completely unprepared to deal with Japanese Army cryptography; we were not then reading, and had never seriously attempted to read, any high-level Japanese Army cipher system. (For that matter we had never tried to read the German military systems either).

3. The first break into a high level Japanese system occurred some time in March or April 43, when the Wireless Experimental Center at New Delhi got into the [text withheld] water transport) system. By that time enough was known about the high level systems of the Japanese Army to permit a decision as to the order in which they should be worked on and the division of the work among the 4 large cryptanalytic units (Arlington Hall, the GC&CS in England, the WEC in India and the Central Bureau at Brisbane). Arlington Hall by agreement was made the directing center of Japanese Army cryptanalytic activities; and in dividing up the work it assumed the primary burden of the bookbreaking job on [text withheld]

4. As of April there was no American experience in intelligence work on Japanese high level decodes. In a study written up in that month we expressed confidence in the ability of the Special Branch to handle the material that was expected to flow in after a couple of months, though we did say that a transfer of personnel from other work would be required, and that our other work would be impaired, unless personnel could be recruited promptly and trained.

5. Not until the middle of June did we get approval for additional personnel. By that time our work had expanded far beyond the new allotment of 20 officers; we were given additional jobs to do, faster than new personnel could be recruited; and we were not able to put adequate personnel on the JA work.

6. Having no experience to guide us, both Arlington Hall and ourselves had under-estimated the difficulties that the Japanese systems would present; specifically (it now seems to me), both had underestimated the amount of intelligence and research work that would have to be done in order to build up the water transport codebook and get intelligence out of the messages. Both organizations, therefore, were unprepared for the job that this material presented.

7. By June, it was clear that, in order to capitalize on the opportunities presented by [text withheld] and other systems then in process of solution, Arlington Hall would have to increase its personnel by a minimum of 2,000 people. Studies designed to present the problem to the appropriate authorities were commenced. By August a request for the necessary personnel, accompanied by a T/O and manning tables, had been submitted. It appeared on the face of the study that a critical situation existed. Nevertheless, 4 months passed without effective action being taken; and only within the last few days has Arlington Hall received the authority necessary to commence recruiting.

8. In other words, 6 months after a critical need for at least 2,000 persons was obvious to anyone familiar with the problem, the lengthy and difficult job of recruiting such personnel is just being started.

9. Meanwhile, upwards of 200,000 Japanese Army messages (in [text withheld] and other partially solved systems) have piled up on the shelves at Arlington Hall, unread. These messages would be readable if the necessary personnel were available. Most of them will never be read, because the priority of current traffic, the increase of readable current material at a rate faster than the recruitment of personnel, and the sheer necessity of moving forward from one period of a system to another, in order to preserve cryptographic continuity, will make it impossible ever to allocate personnel to decipher and translate any substantial portion of these messages.

10. How much priceless intelligence is locked up in these unexploited and unexploitable messages is anybody's guess. It is anybody's guess, also, how much information of operational importance has been lost, because when the opportunity came along we were not ready for it.

* * *

77. One thing is sure. If every limitation of personnel allotments were removed, and the Special Branch were allowed to recruit (as the British GC&CS do) qualified personnel from wherever they might be found (officers, enlisted men and women and civilians), it would still be impossible, even within the next year, to find and train the number of qualified persons necessary to keep up with the ever-increasing opportunities which the Japanese Army traffic will probably present.

78. The writer would sum up the situation presented by the Japanese Army traffic as follows:

a. In our exploitation of this field we are far behind where we should be, or where we might have been had the job been seen in its true proportions and been given the necessary priorities in manpower and facilities.

b. We have arrived, nevertheless, at a point where an opportunity is presented to increase our Japanese intelligence a thousandfold.

c. If we act vigorously, giving this job the kind of priority that the British have given their work on German "E," we have the chance of getting into Japanese Army cryptography so deeply that we can never be dislodged from it by changes in systems or by devices employed by the enemy.

d. If we act vigorously, at the very least we can open up sources of intelligence that will certainly be of great importance, and might even be of decisive importance, in the Pacific war.

e. Except for the matter of I.B.M. machines at Arlington Hall, the problem reduces itself almost wholly to one of obtaining qualified personnel, when they are needed and not 6 months later.

f. If we go on the way we have gone to date, we shall continue to miss opportunity after opportunity, and at the end we shall have paid for the lost opportunities in lives and wasted resources.

79. The foregoing appears to confirm the opinion that you have expressed, that Arlington Hall's increase of personnel should be raised from 2,000 to 5,000, amd that it should be allowed to go forward to recruit 5,000 qualified persons as promptly as possible. When the Wireless Experimental Center in India, with a much more limited mission, already employs 5,000 personnel and is moving to increase that number as rapidly as personnel can be found, an increase of at least 5,000 persons for Arlington Hall would seem to be indicated.

80. An increase of personnel for B Section of the Special Branch from 55 to 280 officers and from 22 to 120 enlisted women or equivalent personnel is a drop in the bucket alongside of the Arlington Hall requirements. It is, moreover, no over-estimate of the requirements, if the British organization is to be taken as a model. Hut 3 at B.P., an intelligence section dealing with high-level German traffic solely from the current operational standpoint, had 328 persons working in May; and this is exclusive of administrative personnel. In the two principal sections dealing with the longer-term aspects of German military traffic there were 257 persons and 179 persons (again exclusive of administrative personnel), or a total in the 3 operations of 764 persons. This total is exclusive of a Tabulating Section of 239 persons, and takes no account of personnel on the intelligence side of the operation at the War Office and the Air Ministry. The Special Branch must perform not only the functions performed at B.P. but a number of those performed by the Service Ministries in London.

81. This situation is a challenge to the War Department to tackle a new kind of job, one not easy to understand and not easy to fit into a familiar pattern of organization, and one that requires considerable imagination and a particular type of personnel.

82. It is also an intellectual challenge to the United States Command. The victory of the British over the Germans in the radio intelligence field is a great intellectual victory of one leader and one people over another. The Germans have been outwitted at every turn; their most secret military communications are read every day; their most elaborate security precautions count for nothing. Why were the British able to get to the "Scharnhorst" and sink her? Simply because they were able to arrange their tactical dispositions and deception measures in the light of knowledge, derived from reading messages in what the Germans still consider an unbreakable cipher, of the vessel's precise mission, the nature of its escort and the exact time when the battle convoy was going to leave Lopphovet.

83. Except for whatever our Navy has been able to do, we have achieved no corresponding victory over the Japanese. To date, in the field of radio intelligence, we have met largely with failure.

84. The chances for victory, however, lie before us; the only question is whether we have the vision to see them and the imagination and energy necessary to seize them.

Alfred McCormack, Colonel, General Staff
Deputy Chief, Special Branch, MID

CHAPTER IV

Training the Force

The very large signals intelligence effort mounted by the U.S. Army in World War II demanded masses of trained personnel. For most of World War II, officer and enlisted cryptologic personnel were trained at Vint Hill Farms in Warrenton, Virginia, which was also the site of the Signal Security Agency's Monitoring Station Number 1. The "Official Story" of officer training is contained in the excerpt from SRH 358, History of the Training Division, Signal Security Agency. A more informal account of the human side of the training process as it affected enlisted ranks can be found in the "Third Battle of Manassas," an unpublished manuscript prepared by some of the trainees.

From SRH 358. *An excerpt from the History of Training Division, Signal Security Agency, discusses the training of cryptologic officers at Vint Hill Farms Station during World War II. Indicative of the fact that the Agency (and the Army) reflected all too well the prejudices of the time is the fact that all officers selected not only had to be mentally and physically fit, but also "of the white race."*

CHAPTER IV

HISTORY OF SCHOOLING OF COMMISSIONED OFFICERS IN THE VINT HILL FARMS SCHOOL VINT HILL FARMS STATION WARRENTON, VIRGINIA, 17 March 1941 to 1 January 1945

* * *

10 March 1942 to 5 October 1942

On 10 March 1942, the training of commissioned officers was initiated in the Cryptographic Division, Fort Monmouth, New Jersey. The Cryptographic Division was then a part of and under the supervision of the Enlisted Men's Department, Signal Corps School, Fort Monmouth, New Jersey, and had been organized primarily to train enlisted men in cryptanalytics and linguistics. The training of commissioned officers was initiated primarily because of the need in various Signal Corps and Army Air Forces units and installations for personnel qualified as Message Center Officers, Cryptographic, MOS 0224. It was certain that emphasis in such training should be placed on cryptography and, therefore, that a school organized to teach cryptanalysis would apparently not be the proper place to give such instruction. However, the Cryptographic Division was the only Signal Corps school then existent which could not only teach the operational phases of War Department systems but could also demonstrate to the students by cryptanalytic methods, their weaknesses and thus emphasize to them their responsibility for the security of such systems.

On 10 March 1942, a group of seventeen officers, assigned to the Signal Corps, were placed in such training and fifteen were graduated after a period of approximately ten weeks. All of the group graduated were transferred to the Army Air Forces for cryptographic security duties. Additional officers were assigned for training from both the Signal Corps and the Army Air Forces from that date until 5 October 1942, so that the average number graduated per month during that period amounted to ten, of which approximately 50 per cent were assigned to duty with the Army Air Forces and the remainder to duty with the Signal Corps.

Since the commissioned training during this period dealt with relatively small classes, only two commissioned instructors were needed and these were provided from officers assigned to the Staff and Faculty, Signal Corps School. The instructors were required to be trained as Cryptanalytic Officers, General, MOS 9600, with special additional training in the operation and analysis of War Department systems.

All commissioned students were required to have an AGCT grade of 130 or better, an analytical mind, and preferably a college education. All had to be cleared under the provisions of classified AGO letters pertaining to the clearance of personnel for cryptographic duties. Due to the fact that almost all position vacancies were in overseas units or installations, composed of or operated by white troops, all officers had to be of the white race and physically qualified for overseas service.

The problems encountered in this phase of the training conducted by the Cryptographic Division were relatively few and based primarily on the difficulty in obtaining current and pertinent instructional material and on the difficulties created in the scheduling of training on classified material by reason of the delays incurred in obtaining cryptographic clearances. As the student body increased, the further problem of finding adequate classroom space was created. No additional space was available at Fort Monmouth, and as a consequence, the school was placed on a two shift basis.

No reports have been received criticizing the adequacy of the training given commissioned officers during this period, but it can be properly acknowledged that by reason of the speed-up created by the demands for trained officers, the training was at best weak because the theoretical and technical phases had to be emphasized at the expense of practical application, and as in most types of school training given to commissioned officers, little or no opportunity was allowed to them to gain experience in the administration and handling of troops.

Enlisted overhead for the Cryptographic Division during this period were assigned to the Second Signal Service Company, Washington, D.C. and on detached service with the 15th Signal Service Regiment, Fort Monmouth, N.J.

5 October 1942 to date

During the summer of 1942, negotiations were initiated to determine the feasibility of moving the Cryptographic Division to some location near Washington, D.C. This was deemed advisable in order that closer liaison could be obtained with the Signal Security Agency, so that more current cryptanalytic information could be obtained, and so that more physical space would be available for both commissioned and enlisted training.

On 5 October 1942, pursuant to authority contained in paragraph 2, S.O. #272, Hq. Fort Monmouth, N. J., dated 4 October 1942, all overhead and student person-

nel then assigned for duty to the Cryptographic Division were transferred from Fort Monmouth to Vint Hill Farms Station, Warrenton, Virginia, a Class IV installation. At Vint Hill Farms Station, the name of the school was changed to the Signal Corps Cryptographic School. The transfer of the school, although well intended, was unfortunate at the time, due to the fact that Vint Hill Farms Station was then only in the initial stages of construction and certainly not, at that time, a proper place for the operation of a special service school. Due to the size of the student body and the initial lack of classroom facilities, it was necessary, until all of the present school buildings were completed in April of 1943, to operate the school on two shifts, which necessarily resulted in cutting down the effectiveness of the instruction given. However, once the physical facilities were completed they were entirely adequate except in rare cases when it has been necessary to turn down unanticipated training demands.

During the remaining part of 1942 and during 1943, the courses of instruction given to commissioned officers were increased to qualify officers in the following military occupational specialties:

Message Center Officer, Cryptographic	MOS 0224
Cryptanalytic Officer, General	MOS 9600
Cryptanalytic Officer, Translator	MOS 9604
Cryptanalytic Officer, Traffic Analyst	MOS 9605

In January of 1944, a section was added to the school to instruct officers (as well as enlisted men) in the installation, maintenance and repair of cryptographic equipment and to qualify officers with the following military occupational specialty:

Cryptographic Equipment Maintenance & Repair Officer MOS 9600.

In May 1944, pursuant to directive of the Chief Signal Officer, instruction of Message Center Officers, Cryptographic, MOS 0224, was made the responsibility of the Eastern Signal Corps School, Fort Monmouth, N. J., and was discontinued by the Signal Corps Cryptographic School.

In June 1944, it was recommended by the Chief Signal Officer and approved by the Commanding General, ASF, that the school henceforth be known as the Vint Hill Farms School.

During the period under discussion, all commissioned overhead for the school have been assigned to and furnished by the Signal Security Agency, and all enlisted overhead have been assigned to and furnished by Detachment, Second Signal Service Battalion, Vint Hill Farms Station. No Table of Organization has been created for this purpose, but commissioned grades and enlisted grades and ratings have been allotted, such allotment being related directly to the training demands and thus increasing and decreasing as the training demands increased or decreased. This has resulted in a desirable flexibility of overhead and has proven entirely adequate to serve the training demands of the school. All overhead, though being furnished by the organizations indicated, have with few exceptions been graduates of the Vint Hill Farms School. All commissioned overhead with few exceptions have

been either enlisted students or overhead in the Vint Hill Farms School prior to their being commissioned.

The primary problems in all the courses given by the Vint Hill Farms School have been to provide sufficient personnel to meet theater demands and to keep the courses current in a constantly changing field. The first of these two problems is an unsolved one. Although it is believed that sufficient commissioned personnel have been trained to met theater demands prior to this date, it has been primarily a result of fortunate assignment of officers to the courses given. At no time has adequate information been forthcoming from higher headquarters on which a reasonably accurate estimate of future training demands could be based. When it is considered that all of the courses given by the Vint Hill Farms School must differ in the fundamentals thereof, dependent upon the theater in which the student is to be assigned, the problem in making a reasonably accurate estimate is self-evident, but by the same token, it is also self-evident that a bad guess would result in an excess of officers being trained for one theater and an insufficient number trained for another. The problem of keeping the courses current has been met by constant and close liaison with Signal Security Agency and by requesting through the Signal Security Agency, reports from the theaters pertaining to the adequacy or inadequacy of the training being given.

The methods of instruction have varied with the different courses. Originally, when adequate time was available, emphasis was placed on individual study. However, as demands for commissioned personnel increased, it was necessary to speed up the courses. Lectures, demonstrations and individual and team solution have been the principal methods of instruction used in cryptanalytic and traffic analytic courses. Lectures and independent study have been the principal methods of instruction used in language subjects. Lectures, demonstrations, independent study and coach-and-pupil-method have been the principal methods of instruction used in the cryptographic equipment maintenance courses.

Adequate commissioned student personnel have been available for training and with the exception of those officers on detached service from their units, all student officers have been assigned to the OSCRP, Advanced Radio Communications School, Arlington Hall Station, Virginia and placed by such organization on temporary duty at the Vint Hill Farms School. The mental qualifications and educational background of all officers sent to the Vint Hill Farms School for training have been adequate. In general, they have been required to have an AGCT grade in Groups I or II if college graduates, and in Group I if high school graduates. Also, all officers were required to possess analytical ability. With few exceptions, drop-outs have been caused by the lack of analytical ability, an ability which cannot be readily pre-determined but will reveal or fail to reveal itself only during the course of instruction.

With the exception of the normal field and technical manuals used for general military training, all training has been based on special texts, documents, devices,

charts, mock-ups, etc., prepared either by Signal Security Agency or by the instructional overhead of the school. This situation has been necessitated by the fact that almost all technical instruction is of highly classified nature and that it is not intended that information pertinent thereto be available to the army at large.

* * *

The present organizational status of the Vint Hill Farms School is that it is a special service school operated under the direction of the Chief Signal Officer for training personnel of the army in cryptanalytic, traffic analytic and cryptographic equipment maintenance subjects. The Commanding Officer, Vint Hill Farms Station is also Commandant of the Vint Hill Farms School. The Director of Training of Vint Hill Farms Station is directly in charge of training in the school. The school receives technical information and aid from the Signal Security Agency, and the Commandant of the school is responsible to the Chief Signal Officer, through the Commanding Officer, Signal Security Agency, for the adequacy of the training conducted.

* * *

From *The Third Battle of Manassas. This highly unofficial history of the training of Army enlisted signals intelligence specialists conveys a good sense of the flavor of training camp life in World War II. Lambros D. Callimahos, the "flute-playing, Esperanto-speaking, Egyptian-born Greek" lieutenant mentioned in the text, went on to a distinguished professional career in the National Security Agency. In an introduction he wrote to the original manuscript, Callimahos commented that "Sometimes it is a bit catty, sometimes biting in its remarks; nevertheless this history is a lot more honest than other histories I have read labeled 'official'."*

THE THIRD BATTLE OF MANASSAS

* * *

THEY FELL OUT IN FRONT OF THE ORDERLY ROOM

At eight o'clock on the morning of 5 October 1942, approximately 250 speculative enlisted men and three officers, each with a baloney-as-usual box lunch, assembled along the Jersey Central siding in Fort Monmouth, N.J. A coach train backed in from the direction of Eatontown and stopped with the baggage car near

the general site of the mountainous pile of foot lockers and barracks bags. A detail consisting of about fifty strong "volunteers" was picked to stow the mountain on the train. This done, the men got aboard under the guidance of Lts. J. T. Guernsey, W. P. Bundy, and R. L. Markland and waved goodbye to about thirty fellow students who were left behind, some to pack up the school supplies for forwarding, others to carry the school banner to OCS. During the entire embarkation procedure, the Post Band played familiar airs and cheered the School on to new adventures—or were they just celebrating the departure of the "geniuses" who, in some companies, drew no KP or detail?

The destination of the movement was, except to knowing few, only a subject for rumor. Stories were current of Arlington Hall and other comfortable places in or near Washington; another version had it that the future home of the school would be an old estate in Virginia with a mansion house....After traveling over the rails of most of the lines in the east and south for about ten hours and finally ending up behind a Southern Railway locomotive with a bright green shell around the boiler, the men and officers arrived in Warrenton, Virginia, where they were met by a diverse collection of trucks and conveyances and most of the Warrenton populace.

* * *

The trip from Warrenton to the new home was, for some, a sightseeing tour; for those jammed into the front of the trucks, it was a period of slow suffocation inside raincoats. It had rained most of the afternoon and was still drizzling. The sight that greeted the men upon arrival was one of mud and desolation; and the grim discovery that straddle trenches served for latrines dropped the "campustry" majors to even lower depths. Morning brought a more cheerful outlook, because the sun was bright and the leaves were green. When it was realized that eating or washing required, for most men, a trip across the post, the cheerfulness evaporated again.

Although, at the time, few people knew it, Company "B" already existed on paper and included the "Schoolboys," 25 "linguists" of questionable proficiency, and three untutored non-coms, "Lil Abner" Hodges, "Louie" Fragassi, and "Repulsive" Ahearn. These diamonds-in-the-rough were somewhat doubtful as to how to handle the "new fellers" who were "pretty much like ordinary people—smart, but kinda mad". Lt. Nixdorff, he of the long chin, was company commander, in a remote sort of way. The "first sergeant"....had a pat solution for every difficulty: "You'll have to make your own provisions for that." When Lt. Marion became Company Commander a month later, nobody knew the difference.

Company administration was strictly a hit or miss affair. Paper work consisted of a detail roster that included everybody. There was only one copy of this and Jones, who had it, could never be found. As a consequence, the efforts of Hodges and Co. to control goofing off were largely nullified. Reveille, also handled by Li'l Abner, was an indeterminate proceeding. It was held under blackout conditions

where "Barrack so-and-so all presnnnneraccounted FOR!!! was a mere formality—except that Ahearn's report from the one-holer generally agreed with the facts.

The Orderly Room was a clapboard shack at the main gate that looked like a tool shed (and was). With the detail situation very much out of control, a clerk was needed to get out additional lists of names. A private named Griffin, who was more at home with a typewriter than a shovel, volunteered, and genuine administration got a definite, if modest, start. A week or so later, the Orderly Room moved to a leaking tent behind Barracks 10, which at the time was only a pile of prefabrication in the rain. When it was at last put together (at a cost rumored to be $3,030 without steps and screens), the company headquarters moved inside and Lt. Guernsey took over as CO. In less than a month, a telephone had been installed and the Company had established communication with the rest of the Post, proving that the Signal Corps could do the job if the customers would just be patient. The tent became a telephone booth outside of which long lines of patrons formed at odd hours of the night and morning.

Shortly afterwards, a group of officers and "non-com material"...left to start "C" Company (later Hq. and Hq. Co.), whose original function was basic training for an assortment of illiterates, ex-convicts, gittar players and spare parts who had shipped in when nobody was looking. Hodges' bunch moved over, too.

In those days the immediate ambition of every student was to get in one day a week of school. The company was growing: classes were filled and were run in shifts. Life was mostly detail—chopping trees, digging post holes, laying sidewalks, and cleaning the (outdoor) latrines. Life centered around those woodsy chapels: while the dry and shining bowls in the regular latrines remained unblemished, men from "B" and "C" companies shared a common interest in an incredible twenty-holer on the corner across from Barracks 1. There they would meditate amid the fragrance, the "C" men eating candy or munching an orange, the "B" men reading Tristan and Isolde or a volume of T. S. Elliot. . . .

Having been specially selected at processing centers because of superior mental and educational qualifications, the men were put to work at digging and moving logs. One count showed forty three years of college in one ditch (8 EM); the postholes were likewise "educated." Products of the lumbering activities were classified into (a) logs, (b) branches, (c) trimmings. On odd days the log poles and brush would be moved to one side of the area "to make way" for further developments; on even days they would be moved back again "to make way" for still other developments. This went on until all concerned ran out of developments. It was then decided to burn the brush piles and carry out the logs. Those who goofed off got a week's KP—which was in many ways a relief. . . .

During this rugged period while construction was still in progress, casualties were not uncommon. The uncharted maze of trenches, later used as ditches in which to lay sewer and water pipes, probably taking the largest toll. Somehow there seemed to be very little cooperation between the engineers digging the

trenches and throwing up the breast works and the other combatants on night operations. While on a special mission one warm October night, Afflerbach, clad in GI undies, walked into a thirteen foot ditch but relaxed (or was relaxed) enough to suffer nothing worse than mortification. On the other hand, the same ditch was responsible for a wrenched leg and three broken ribs from two other victims that same night. . . .After that, extreme caution was observed by the personnel of the Company; anything that looked like a ditch was avoided, and the dim morning hours found dozens of men gingerly stepping over the shadows of trees.

Social life on the Post was somewhat suppressed by the lack of facilities. Over in "A" area there was a barracks that had been converted into a day room, mail room, library, special services office and PX. The latter consisted of a twelve-foot counter and three shelves, mostly empty; besides, it was nearly a mile away. Dinner invitation extended by the Warrenton folk (that was before the native money-grabbers made a mockery of "Southern hospitality") generally had to be declined: eleven miles each way was a long walk, even for the Signal Corps. When Sgt. Parker tried to organize an orchestra, the response to first call consisted of five trombonists and two xylophone players. It was several months before a combination with the customary assortment of instruments could be gotten together.

* * *

When Griffin was away or ill, Owens took reveille with an intonation that added to the Owens legend. In Hodges' day, the vocal side of reveille had been nothing more exciting than a succession of strange noises in a Kentucky twang. When Griffin came along, he enlivened the proceedings with a haughty "reh-PORHT!!" and a battery of announcements and involved instructions proclaimed in his best theatrical manner. Against this professional competion, Owens staked his bid for fame on an unmelodious "RE-E-E-E-E-E-E—-PORT" delivered in a droning monotone. With the Griffin-Owens team running things, the men could depend on a reveille in harmony with the dizzy events of the later hours.

About this time, Lt. Volm, deciding that it was time for recreation and beautification, began the Area Cleanup Project. Lt. Kunzman became sidewalk engineer and used for his theory of construction "straight logs, only straight logs." This meant that logs would be toted in for the walk one day and out the next—for longer and straighter ones. Again big brush piles burned in the middle of the "stadium." Lts. Guernsey and Vultee would stand about the huge fires warming their hands (?), saying "more branches on this side," and, "more twigs over there. . . . let's get a move on."

Danny Volm was a skillful "improviser." When the sidewalks needed gravel and it was not forthcoming from the engineers, he would stroll up to the main gate, and, as the trucks approached with gravel for the Colonel's walks, would swing aboard and holler, "Down this way" and bring them to the company area. In this

manner several hundred tons of shale were obtained for a 220 yard race track that ran around the area between the barracks and divided Goldbrick Park in half. It was boycotted by everybody: Afflerbach tried to use it, but recognized the disadvantages of ostracism in time. Later it was removed, as painfully as it had been built.

The Day Room began to shape up under Volm technique. Huge slabs of masonite for the new white barracks in "C" company disappeared, only to reappear on the walls of the day-room, neatly squared off with lathes gathered in the same manner. . . .

Inspections were frequent. On Saturdays the inspection party followed a transposed route among the barracks in an attempt to catch the boys warming their hands around the stoves instead of standing by their bunks. . . .This "hit-em-where-they-ain't looking" strategy worked occasionally, particulary in Barracks 1 (the goat: Kilgore). Captain Guernsey was a no-haircut gigger, especially when the barber shortage was acute. Homer Baker got it for "dust in ear"—lint from an OD towel, it was. Lt. Vultee specialized in upper bunk gigs where you could get an eye-level view of the wrinkles in the bottom sheet. Lt. Kunzman who usually inspected with him, however, specialized in lower bunk "gigs" which were more in line with his qualifications. . . .Lt. Volm liked to look for food which he ate (except Biern's beer-cheese), leaving a gig slip in gratitude. At foot-locker inspections, the barracks leader was required to wriggle around in the airspace above the ceiling vents in a nothing-up-here-but-us-chickens act. All kinds of junk were discovered: radios, a crate of oranges, satchels, volumes of poetry in limp leather, and Wilhelmy's six-month file of the New York Times. (This practice was ended when somebody fell through the ceiling). Epps was caught with an axe in his footlocker; Jurgens had silverware in his overcoat; Oppenheimer had an aspirin under his bed.

Cold days also bred disease. One after the other, barracks came down with measles or allied bugs that led to bigger quarantines. Finally the whole Post was put in a quarantine based on the following principles:

1. That men living off the Post were immune.
2. That the germs distinguished between enlisted and commissioned personnel.
3. That the men ceased to be carriers every third day but became dangerous again on the fourth (the issuance of passes on Mon.-Thu.-Sun., etc., was based on this principle).
4. That short periods of immunity occurred in a scheduled manner (this permitted operation of the PX on a shift basis).
5. That contact was dangerous in training activities but harmless while on detail.

* * *

ADMINSTRATION FOR ALL CONCERNED

It wasn't until three or four days after our arrival at Vint Hill that the administration overhead took up duties in the barn in the now "B" Company area....Lt. Guernsey opened his office in the rear east room of the barn. Of course, the school had to have a phone so immediately one was supplied (a crank-type affair). There was a trunk line—to one place, Post Headquarters in the big house—but to get there it went across the floor of the office, down the hall and over the fields. If you had business with other than Sgts. Enright and Jones you had to go for a hike. After all, it was only a little less than a mile over to the orderly room at the present site of the main gate. Besides, if it was Lt. Nixdorff you were looking for, he wasn't there!!

One of the big jobs which had to be done again was the roster of EM in school who were eligible to be T/5s. Of course, we had made a roster before we left Ft. Monmouth; what happened to that nobody knew. Anyway, on October 27th the post-hole diggers got their rank. By that time, it was time to move and the school set up headquarters in the telephone building, except that Reproduction, Supply and Plans & Training stayed in the (unheated and dimly lighted) attic of the barn. Those were the days of easy ratings. Radio personnel were changing stripes as frequently as they changed underwear. Then it was learned that all the overhead were to become at least T/5s, so up to AHS went a list of men recommended for promotion. Everybody was put on the list but SNAFU—only about one-half of the men recommended were promoted.

There was a gnashing of teeth and much weeping and wailing—and no chaplain to issue TS slips. (Sgt. Bruce "I have a few ah-nowns-ments, fel-lows" Parker acted as a sort of chaplain, but he was busy most of the time figuring out schedules for the "Green Dragon"—a converted auto trailer which linked the camp with the outside world.) It took almost two weeks to arrange to have the other EM in overhead promoted to T/4; after that, there was rank all over the place.

During the latter part of November the office of the school was moved across the post to the present school supply building. Three space heaters (the regular quota for heating buildings in the Sunny South) were installed. It was hard at first for the Warrenton Commandos—Lt. Guernsey, Sgt. Kane, and Sgt. Hawes—to adjust themselves to the vagaries of the temperature in this new office. After they stood around the stove for two hours, the icicles would melt and they could slowly work back to their desks and get administration underway. By noon the building would be so hot to stand, while the atmosphere would be blue from the smoking of the stoves and the Commandos.

* * *

...Sunday classes were scheduled on alternate week-ends for all personnel from 0800 to 1645 during January through April 1943. Target practice with a knife was furnished by Lt. Mann in the main office, the target being the then present calendar month. However, instruction was not of the best for he couldn't hit the target as often as the students.

In the early part of April it was decided to have post headquarters and the school together. And for the fifth time the administrative staff was packing up and bossing a bemused bunch of men who were wandering through the bushes with typewriters, file drawers and in-baskets. Now though, it was clear that progress had been made: for the first time, the school headquarters looked like an office and was uncluttered with dirty stencils, crates, mess tables and student officers.

* * *

...the desk in front of Afflerbach is not occupied but it is reserved. Perplexed student officers spend days at this desk filling out multitudes of forms, screaming they had already filled them out at Arlington. After the first day they become hoarse, the second day they give their occupations for the last five years in answer to an inquiry about their grandparents' dates of birth, and on the third day they are veteran student officers. Lt. Callimahos is over in the other corner but is heard from all the time. His byline: "Don't you know how to report to an officer????". . . .

It was during this period that the output of memorandums reached its peak. Although Capt. Guernsey and Lt. Vultee were only four feet apart, they found it necessary to carry on communications by indirect discourse. The Lt. would jot down notes to be typed by Sgt. Doering who would route them through Sgts. Jurgens and Kane up to the Captain, each Sgt. retaining a copy for file. Memos for general distribution were written by the officers, including Lt. Callimahos, and were sent down to Reproduction for ditto-ing, while over in the corner Sgt. Kane kept up an envious grumble about the days back in Monmouth when he put out all the notices.

When the paper shortage began to be felt, economy was effected by substituting buckslips for individual copies. As the practice grew, magazines, bulletins, and other printed matter came to be circulated by this means, "FYI" and "Note and initial below." Eighty-page copies of Tactical and Technical Trends would be sent out to thirty-odd people in six different buildings "to be returned promptly." Instead, they would disappear. Sgt. Doering, who used to be a statistician, got out the calculator and some probability tables and estimated that buck-slips issued in May could not, the way things were, be expected back before the middle of November. Runners were sent out to find the missing buck slips, but no luck. The device of including breezy comment (e.g. "Pages will not be dog-eared") was tried, without success. Finally, Lt. Vultee blasted out with his famous memo on "Bucking of Buck Slips" in which negligent "buckees" were charged with retarding the war

effort and were warned that "such impedition will not be tolerated." Everybody reached for his dictionary and awaited the next dispatch. . . .

* * *

. . .as Rosh Hashana approached. . . .Almost the entire student body exhibited religious fervor and a sudden desire to attend services. For this, of course, a three-day pass was necessary.

Equinoctially, these "Passover passes" (the term applied to both Passover and Yom Kippur) brought on righteous indignation in some quarters because "They get off at Christmas or New Year's, too, and that ain't fair!" The other quarters said "Yes" and went on pass anyway. . . .

. . .the Room 31 gang. . . .had started a map in the second stall of the latrine down the hall from the office, a map which included some of the prominent personalities of the period. Irritated (no doubt, by the misuse of government property), Owens issued a notice to "all EM" warning them that "anyone found guilty of writing on, marking or in any way maliciously defacing any wall, partition or other part of the school buildings will be subject to severe disciplinary action."

Though the map grew and grew, Owens couldn't catch anybody. As its reputation spread, visitors from other buildings and even the Company came over to see the newest "terrain features."

Captain Guernsey regularly passed by the officers' stall in order to keep abreast of developments. . . .

* * *

The Legal Department moved in shortly afterwards and immediately took over. . . .They seemed to regard the school headquarters as intruders. Business was brisk. One day somebody who said he was a representative of Armour & Co. called up and insisted that Lt. Pratt had some chickens for sale at his farm. The "Legal Eagle" explained that this was an army post, that, anyway, we were using all the chickens we could handle. . . .

* * *

The Chief Clerk has also always had a secondary function—that of a combination John Anthony—Ma Perkins—medicine man for the soul. At least once a day he received a wailing visitor with a long story of a check that had to be cashed, a telephone call for a life-or-death matter, bonds that had to be bought, or "I want to see Lt. Kunssssman." The EM long ago learned that the simple story is not always the best. There was. . .the lads who felt all right in the morning but now were a little sick, and would like to go to the dispensary, please—passing the PX on the way, of course. Then there were the delinquents sweating out an interview with the Captain

or the Executive Officer and who stood around for fifteen minutes to a half an hour, gazing aimlessly at the ceiling and getting out of people's way while maintaining a pre-execution look of "No, I won't take an eye bandage." And there were the potential OCS men who had been told to report to the Chief Clerk about their applications. They marched down the halls, silently counting cadence; executed a smart column left; and, coming to attention at the Chief Clerk's desk, they were ready to reel off the general orders, the position of the soldier, or a fifty word essay on "Why I want to be an Officer." When they were asked merely to sign their name three times, their relief was so evident they'd have let out a scream (if they hadn't been OCS men).

In addition, the Chief Clerk is often kept quite busy with a security problem peculiar only to School Section "A." Room 36, adjacent to his desk, is the secret classrooms of all secret classrooms, and the subjects taught there are verboten to all outsiders. Unfortunately, the human voice carries; and when Lt. Pratt lectures, the windows rattle in the Big House a half mile away. This keeps the Chief Clerk busy with phone calls from the main gate, as the guards are quite interested in his course, and frequently request repeats on certain paragraphs they missed while checking trucks out of camp. . . .

* * *

EDUCATION IN DARKEST VIRGINIA

* * *

Just at chow time Thursday evening, October 8th, three large commercial vans pulled in to camp with all the worldly possessions of the school that had been left at Monmouth. In addition to the stationer's supplies and personal materials of the students, they had all the furniture, twelve tons of IBM paper, the IBM machines and a three-ton safe. The draft-dodging that went on that night when a detail was needed to unload has never been equalled by any of the "Zoot Suit Clan." The materials were for the most part put in the left of the barn, and the overflow in the firehouse. By eleven PM everything was unloaded but the safe, which was strictly an "Everybody-boss-nobody-do-anything" job. The situation finally got to the point where Lt. Bundy and Lt. Markland gave up and Afflerbach first laid claim to an SSN for safe moving.

Sometime during the following week, school was started with two four hour shifts in the left of the barn, two small rooms on the ground floor, and a barracks. During the formative period of the school most of the overhead either drew their materials and continued their studies or were busy pushing details preparing the buildings. Sgt. Frick did neither but instead went to Washington every night and came in just in time for noon chow. . . .

As soon as lights were available for evening study, a night study hall, optional

to all students, was instituted. The roster for the supervision of the hall was arranged so that one so-called senior instructor and one junior were on each night. This probably became as confused as the army has ever known, with such arrangements as the following prevailing. One night Sgt. Netherton was the person who actually served, but he was doing it for Bailey, who was supposed to have done it for Hurst, who was supposed to replace Afflerbach, who had originally been scheduled for that night. . . .

By November the school quarters had been moved to what later became HQ Company's mess hall. The heating arrangement in the mess hall was poor enough with the best of attention, but to make matters worse, Cpl. Symmes was put in charge of building the fires.

A less apt person for the job could not have been found in all the school. For instance: one cold Sunday, Symmes was the only person in Barracks 1, and though his bunk was next to the stove, he let the fire go out and went to the latrine to finish his usual Sunday bundle of letters.

* * *

In the company by this time things had become well enough organized to attempt a fire drill and gave the twelve Assistant Fire Marshals some practice. Everything went very smoothly until Lt. Mann noticed that Sgt. Bailey had allowed his quarantine men to fall out with the rest of the company and proceeded to inform Bailey that he was in error. To this he received the philosophical reply, "Sir, fire recognizes neither race, creed, or color." This little episode may have been the beginning of the Lt. Mann-Sgt. Bailey feud which lasted for the duration of Bailey's stay at Vint Hill.

On December 13 school was moved to "E" Bldg. No. 1, the first time on the Manassas front that decent quarters were available. There now was allocated one officer instructor to each room in addition to the NCO in charge of the room, and in this arrangement, it seemed that Lt. Mann and Sgt. Bailey were just naturally a team (either by accident or design). Their feud continued, and in addition a race sprung up between them over the progress made. Bailey never was very cooperative in his suggestions to Lt. Mann (Bailey was more advanced) and one time he nearly laughed himself into hysterics after looking over Lt. Mann's problem, glancing out the window as if viewing the weather prospects, making a few pointed observations with a knowing inflection, and watching Lt. Mann swallow the bait and madly try to follow the "clue" which was entirely false. Sgt. Bailey went racing down the hall fairly shouting, "Boy, did I foul Mann up! He'll be there the rest of the winter."

* * *

In the spring of '43, the going about camp really got tough, with mud about a foot deep every turn one took. By this time the mess hall was open (Christmas dinner was the first meal served in it), and the school shift was the conventional A shift from 0645 to 1245; B shift from 1380 to 1900. The first shift was marched to and from school by T/Sgt Van Cleaf, on detached service from the Air Force somewhere out in Washington State, and the second shift by Sgt. Afflerbach. Every morning there was the problem of finding a route to school that involved no swimming to cross the road in front of the E buildings. This problem and the routes finally chosen confused Van Cleaf who missed the turn, went out the main gate, marched down the road (all of this in total darkness), and arrived at school twenty minutes late. Afflerbach, having the noonday sun to maneuver by, did nothing worse than lose a few people when they slipped off the foot bridge over the mud in front of "E" Bldg. 2.

With the coming of spring came a great influx of students and the need for more instructors. As a breaking-in course, the embryonic professors were first given the test of showing their ability with the students in Room 31....No one ever was complete master of Room 31, because the Schwartz boys, Duke (of latrine map fame), and Smitty (Lou) were just invincible. Many are the times that their stories have held up before Capt. Guerney's questioning, though everyone knew they had been in Warrenton long before noon that Saturday. Tarpley and Hodge, rather than face Room 31, chose to become warrant officers and take part in the invasion of Sicily.

During this phase of the campaign, military training was strictly a hit or miss afair supposed to take place during the shift that the men were not in school. What with the large number of men on detail and the "goof off's." very few were out at any one formation. To counteract the rise in goofing off, Griffin and Afflerbach cooked up a surprise roll call one morning and found that the absentees just about balanced the presentees. Before the inevitable three days KP, the boys admitted that they had been (1) in the barracks, (2) in the bushes, (3) in the PX, (4) in "A" Company asleep and unnoticed because of "A" Company's 24-hour schedule.

In May 1943, enough buildings became available to discontinue the two shift basis and also to crack the tradition of the thirteen day week. The training program now was held in the afternoon as the finish of a day and utilized the Kunzman Memorial Obstacle course, the Nason grape vine hang-on-or-get-wet-course, and Sgt. Neuwoehner's tick-infested "creep and crawl" course.

After the demise of Ephron, Clark, Latham, Lehr and Schier, Gramann and Chapman, with Sgt. Nelson as boss, took over the paper grading department and worked madly trying to make at least thirty new problems per day in addition to going over hundreds of papers. With 147 square feet of map behind them, this "General Staff" was masterminded by the excitable, fluet-playing, Esperanto-speaking, Egyptian-born Greek, Lt. Callimahos who simultaneously prepared problems, practiced Morse Code, worked on inventions, played chess, and listened

in on other sections' conversation. Despite a sharp intellect, the Lt. had a gullible streak that was exploited by his buddies whenever the situation was ripe (as it usually was)....

The rest of the summer of 1943 was quiet. Gus Uhl went to Canada just long enough to get a service ribbon and then returned; Corry set a new beer record in the 130 pound class and added acrobatics performed on the railing around the PX; Palmer's room of cripples were all either declared fit or sent home to find jobs, thus freeing him for active duty; and Lamke (Bks. 13 all present or accounted FOO-URP!") was quietly bitching away in the library, able assisted by Oscar Briggs. Bershas and Wiggin transferred their efforts from the language field, probably to fill the gap left when Oppenheimer went to the Southwest Pacific.

* * *

Besides other school equipment, a complete staff of able officers was around at all times. Some made the complete cycle of student, instructor, company executive officer, and back to student...."Big" Bundy and Lt. "Little" Bundy conspired together with some message center problems that seemed to be always planned for the coldest and most uncomfortable day of the month; and although they've been gone for nearly two years, there still stands on the main gate road the buggy little shack they immortalized as "THQ"—a monument to their work.

Autumn of 1943 brought big things and a lot of new instructors. Jungle Jim Metcalf took on instructorial duties above and beyondthe call of malaria control; Elgin and Braswell were salvaged from the Room 31 gang; and the Atamian-Marburger combine was the result of random selection. The "quickie" course came bouncing off the press (really from the pens of Lt. Callimahos and Gerlach) and the first experiment at force feeding was under way. Very few chokings or strangulations were reported.

At the first anniversary at Vint Hill approached, plans were made for a celebration of those who had made the initial trek and were still hanging around. The dinner was held at the Robert E. Lee, one of several outposts of Greek civilization in Warrenton, on the evening of October 5, 1943. Seventeen of the twenty eligibles enjoyed the spaghetti dinner and then returned to Room 318 for coffee (and bourbon, with poker). Sgt. Krueger and Owens, as usual, financed the game and finished by paying off Cpl. Bill Hewitt's wedding expenses. Bill Doering demonstrated a journalistic flair by writing his first full length novel, "Your Life at Vint Hill," . . .a memorial which gave rise to the Old Bastards Club.

* * *

By May, the school had dwindled to the point where each instructor had his own student; many of the Warrenton Commandos saw fit not to plant a garden; and

everyone was trying to get in a couple of extra courses that would help hold stripes. Came the "bust" in ASTP, and then the horde. Every available room (School Section "B" was even declared bankrupt) and spot was utilized for classes, with "The Dome" Rosskopf having the misfortune to draw the Salt Mines (Supply Building) where the tar on the roof melted and spattered freely. He finally got a helper in Les Olin, but Olin decided if he could stand tar he could stand another substance and went to OCS. . . .

On July 4th, (ah, what a day for fireworks!) the first class of WACs came to School Section "A," and what a change in the EM!! Students no longer had to be reminded to shave, and it is said that the sale of Kreml quadrupled at the PX. The one sad note in the coming of the WACs, other than the loss of one perfectly good latrine by the EM, was that, after many long hours of planning and master-minding, Afflerbach was at the last moment informed that a more stable and experienced man would be required to master the co-eds and that Sgt. Nelson would fit exactly (as long as his didn't find out).

The WAC occupation can be divided roughly (or perhaps gently) into three periods: (1) the Nelson or pioneering period; (2) the Ramsey-Snyder or achievement period; and (3) the Palmer or decadent period. During the first of these, the personnel of the group exhibited a timidity, seriousness, and lack of humor for which Nelson claimed credit but which probably reflected the newness of their situation; for although the natives looked upon them with interest and curiosity, they treated them with formality and restraint. During this period of plain living and high thinking, the first personalities to emerge and take definite shape (uh huh!!) were those of Mary Jane, the heroine, and Sue the siren. The classroom held an odor variously interpreted as (a) Chanel Number 7 and Tabu, and (b) GI soap and honest sweat. Toward the end of the period a feud with the guards resulted in a marching formation that was practically all road guides.

During the second period the group became more self-assured, both in their work and in their social relations. During breaks they mingled with the male students, who began to accept them, and their fears regarding the apparent abnormality of the male behavior were quelled as the sheep's clothing gradually disappeared. As the girls attacked their work with more confidence, Summerhalter and Morris became adept at substituting charm for achievement. McMann showed a certain athletic prowess while werstling during breaks, and sedate M/Sgt. Filipczak was occasionally moved to execute trapeze antics on the railing outside the door near the classroom.

There is no positive proof that Sgt. Palmer's presence caused the period of decadence, but it is unfortunately true that many of the brighter flourishes occurred during his brief regime. The trouble was that AR's and SSAR's (School Section "A" Regulations) had never envisaged the entry of females into the school, so that many of the little incidents had to pass unregulated. For example, what could be done when Ginny Blakemore began to put up her hair during class, or when

Summerhalter showed up with curlers in her hair? Both continued working, so not even the crime of loafing could be pinned on them. And the cigarette holders nearly a foot long —- strictly not GI, but apparently not contrary to the rules.

Bell got closer to the borderline when she impaled a marshmallow on a pencil, then toasted it over a match, but she was ahead of the rest of the class and had earned the right to an eccentricity or two. Sgt. Palmer felt that much of the trouble was really the fault of Sgt. Nelson, for everything he (Palmer) did was wither approved by a chorus of "That's just what Sgt. Nelson said", or disapproved by the accusing reminder that "Sgt. Nelson never spoke to us like that." The story had a happy ending, though, for on his birthday the girls sang "Happy Birthday, Sgt. Palmer", and have him some cigarettes, candy, and aspirin—the latter to remember them by, they said.

As the second year staggered to a close, the Old Bastards held a second meeting, again putting out a memorial of the occasion. . . .Although both Bastards and bourbon were scarcer, the party demonstrated that the aging members had lost none of the capacity for celebration. They wondered if they (or anyone) would be around for a Third Anniversary. It didn't seem likely, but then as Lt. Neuwoehner used to say, "We'll never touch Palau and Halmahera!"

* * *

CHAPTER V

Cracking the Codes

The principal Army cryptanalytic center in World War II was located on the grounds of a former women's junior college at Arlington Hall Station in Arlington, Virginia. The main school building housed the headquarters of the Signal Intelligence Service (later redesignated as the Signal Security Agency); operational personnel worked in two large and unlovely temporary buildings run up in ninety days in 1942 and 1943. By the time the war came to an end, 5,000 civilians and 2,000 military personnel were working around the clock to decrypt Japanese military, diplomatic, and other messages. The excerpt from SRH 349, Achievements of the Signal Security Agency in World War II, gives some details of their accomplishments. A message reproduced from SRH 280, An Exhibit of the Important Types of Intelligence Recovered through Reading Japanese Cryptograms, demonstrates that solution of Japanese codes and ciphers could even produce important intelligence dividends on the war in Europe.

Other Army cryptanalysts were located at Bletchley Park, the headquarters of the Government Code and Cypher School (the British signals intelligence organization); with field units; and at General Douglas MacArthur's Central Bureau, an Allied cryptologic unit originally headquartered in Brisbane, Australia. A short history of Central Bureau can be found in the excerpt from A Brief History of the G-2 Section, GHQ, SWPA and Affiliated Units: Introduction to the Intelligence Series (General Headquarters, Far East Command, Military Intelligence Section, General Staff), pp. 66-69.

From SRH 349. *Beginning in 1942, the Signal Intelligence Service was repeatedly reorganized and redesignated, finally becoming the Signal Security Agency, a designation which obscured its major mission.*

THE ACHIEVEMENTS OF THE SIGNAL SECURITY AGENCY IN WORLD WAR II

I. BUILDING THE ORGANIZATION

The Signal Security Agency (SSA) owed its existence in World War II to the basic fact that valuable information may be derived by intercepting communications and reducing them to intelligible form. This fact has two aspects: efforts must be made to protect our own communications against examination by the enemy, while at the same time steps must be taken to derive as much information as possible from enemy communications. The SSA had primary responsibility for both these phases.

* * *

In spite of greatly limited funds, the SIS was able in the years prior to World War II to lay securely the foundations upon which wartime expansion of the SSA was built. . . .

Activity of the SIS consisted of continuation of existing code production projects; establishment of a training program by which a small group of expert civilian cryptanalysts was produced, and another small group of officers, both Regular and Reserve, were trained in the varied phases of signal intelligence; development of intercept facilities to provide material for the cryptanalysts; and, toward the end of the period, the reestablishment, as a practical operation, of solution of current diplomatic traffic. In addition, time was found to do much planning for war and to carry on research and development in cryptographic and cryptanalytic techniques. All of this work was done by a very small staff: Only seven persons from 1930 to 1936—by the outbreak of the War in Europe there were only nineteen.

Thereafter, a series of expansions resulted in the following strength on the day of the Pearl Harbor Attack:

Category	In Washington	In the Field	Total
Officers	44	1	45
Warrant Officers	0	0	0
Enlisted Men	28	149	177
Civilians	109	0	109
Total	181	150	331

Actual operating strength was somewhat less, since 22 of the civilians were still undergoing training and had as yet made no contribution to the work. A comparison of these figures with the strength of V-J Day (14 August 1945) will show the tremendous proportions reached by the wartime expansions:

Category	In Arlington	In the Field	Total
Officers	661	116	777
Warrant Officers	4	11	15
Enlisted Men	565	2139	2704
Enlisted Women	957	257	1214
Civilians	5661	0	5661
Total	7848	2523	10,371

These figures do not include, of course, the more than 17,000 officers and enlisted personnel engaged in signal intelligence activities under overseas theater commanders, nor do they give any adequate indication of the turnover of personnel in the Military District of Washington: by the end of the War more than 18,000 numbered badges had been issued to all categories of personnel at Arlington Hall (headquarters of the SSA) alone. To recruit such a staff and to maintain it despite the many influences which tended to dissipate and to lower strength were tasks requiring strenuous efforts.

The recruitment program was faced not only by obstacles which also beset other wartime agencies, such as the manpower shortage and the need for speed, but also by many problems peculiar to the SSA, most of the activities of which had no counterpart outside the Government from which to draw personnel. Many of its operations required persons of the highest intelligence, possessed of rare skills not easily definable, often demanding, as in the case of the language experts, years of study to produce proficiency. Messages in more than [text withheld] languages had to be translated, yet in only a few instances were competent linguists easily obtainable. This problem was most acute in the case of Japanese, both because a knowledge of Japanese is rare in this country and because the volume of material to be translated was so great [text withheld] The only recourse was to train personnel from the very beginning: ultimately, for example, 428 Japanese translators were trained in this way. The same method proved to be the only solution for supplying competent cryptanalysts: both by the use of training manuals in military cryptography and cryptanalysis and by apprentice training in operating units, the small number of competent cryptanalysts available in 1941 was gradually expanded, but the supply was never equal to the demand.

Moreover, the SSA was called upon to train large numbers of personnel for ultimate assignment to overseas units maintained by theater commanders. This training was given not only in formal courses designed to produce officers and men qualified in the various cryptographic and cryptanalytic specialties but also by

participation in the day-to-day activity of operating units. Much was done also to coordinate training of signal intelligence and radio intelligence units being trained elsewhere in order to keep them abreast of the latest technical developments. In this connection it will be well to digress long enough to point out the trend exhibited during the War of breaking down the centralized authority of the SSA by setting up independent signal intelligence units under theater commanders. Such a change was motivated no doubt by a feeling that it would be necessary to maintain signal intelligence units close to military operations. Yet the experience of the War showed that modern electrical communications are so speedy that distance is no longer a factor that need be considered. Examples will be cited. . .of messages transmitted many thousands of miles, promptly read and translated, and sent back to the proper commander in time for action.

Morale problems were particularly acute, for in addition to those encountered by other wartime agencies, involving living conditions, health, fatigue, and the like, the SSA had a number peculiar to itself. Chief among these was the mixed character of the personnel. Officers, enlisted personnel, and civilians worked side by side, and in each of these groups there were both men and women. A small unit composed of personnel from several of these groups might contain people having varying degrees of prestige and receiving different pay and privileges, yet performing exactly the same type of service. . . .Moreover, there seemed to be no correlation between a category of personnel on the one hand and competence and achievement on the other. Brilliant work was done by individuals in all categories. Had it been possible to operate the SSA entirely with military personnel, or entirely with civilians, some friction might have been avoided, but an SSA made up only of military, or only of civilians, would have lost immeasurably the contributions of the other group. As it was, military personnel had to be stationed with the SSA for both operational and training purposes while having civilian employees made it possible to use the services of many not qualified for military duty.

Another factor not particularly conducive to the maintenance of high morale was the necessity of maintaining complete silence concerning every phase of one's work. Moreover, many of the operations involved nothing but drudgery and considerations of security prevented the individual employee in many cases from getting a clear understanding of how his or her work contributed to the war effort.

Continuous efforts were made to maintain morale at a high level by bettering conditions of work and furnishing employees with aid in the solution of their personal problems. While the rate of separations of civilian employees (4 per cent a month) seemed high, it was found to be actually lower than that of other comparable wartime agencies in Washington. Indeed, giving due consideration to the inherent difficulties, morale in the SSA was really high.

Early in the War space in the Munitions Building, where the SIS had been located from its founding, grew so crowded that larger quarters had to be secured elsewhere. At first it was expected that the SIS would be housed in the Pentagon,

then nearing completion, but before such a move was effected, plans were laid for moving the SIS to a site of its own, preferably outside Washington. The SIS would thus have room for expansion, be relatively better protected from the danger of enemy bombing, and could maintain its security with greater ease if not forced to share a building with other War Department agencies.

The site ultimately chosen after examination of several possibilities was the premises of Arlington Hall Junior College in Arlington, Virginia. This location was close enough to the Pentagon, was not too far from the Eastern Primary Monitoring Station then being planned at Vint Hill Farms, near Warrenton, and in addition made possible the utilization of the housing facilities in the Washington area for quarters for personnel and dependents.

The property was acquired by court action for $650,000, with $40,000 additional for furnishings, and the War Department assumed possession on 14 June 1942. Arlington Hall Station was established as a Class IV installation under the Chief Signal Officer on 25 June 1942. Immediately units of the SIS began to move into the former school building, now the Headquarters Building, Arlington Hall Station, and by 24 August 1942 all of the SIS was at Arlington Hall, the move having consumated without interruption of operations.

Construction began almost immediately on projects designed to convert certain of the existing buildings to military purposes, and by September the program of new construction was in full swing. Besides many smaller buildings, two very large semi-permanent buildings were erected for operations. The first was completed in less than three months time; the second, erected in winter months, took a little longer, but after May 1943 all operating units were housed in the two operations buildings. Other construction provided barracks and mess halls for enlisted personnel, a station dispensary, theater, post exchange, and other service buildings; a motor pool, a fire house and warehouses. The final construction was completed by 1944: while many units have had to work in crowded conditions, adequate space was supplied for all operations. One of the important ancillary structures was a cafeteria, completed early in 1943 and enlarged in 1944, which ultimately provided service around the clock. . . .

The Post was made secure by establishment of a guard detachment and the erection of a double steel fence provided with an alarm system. Another fence was erected around each operations building entrance to which was limited to authorized personnel. Distinctive badges were issued to all categories of personnel and had to be worn at all times. . . .Access to the Post was forbidden to visitors except on official business, and efforts were constantly maintained to indoctrinate all personnel in the necessity of maintaining the physical and operational security of the Agency.

The SIS had been prior to the War a field service under the Chief Signal Officer. Though located physically in Washington, it was not a part of the Office of the Chief Signal Officer but was administered at first through its War Plans and

Training Division and later through its Operations Branch. With the coming of war, however, reorganizations were made by the Chief Signal Officer which resulted in a series of changes of name. The old name of Signal Intelligence Service (SIS), which had existed since 1930, was abandoned for Signal Intelligence Division (SID), and in rapid succession, this became the Signal Security Branch (SSB), the Signal Security Service (SSS), and, finally, on 1 July 1943, the Signal Security Agency (SSA), a name which remained unchanged until the cessation of hostilities. After the organization of the Army Communications Service within the Office of the Chief Signal Officer, the SIS-SSA, by whatever name it was called, was always a part of the Army Communications Service.

The need for enlisted personnel was met by increasing the strength of the Second Signal Service Battalion. This Battalion had been created as a company on 1 January 1939 to supply personnel for the various intercept stations then in existence. Later it furnished a convenient military unit to which enlisted personnel employed in the Military District of Washington and elsewhere for other types of signal intelligence activity could be assigned. In November 1942 the post of Commanding Officer of the Battalion was united with that of the Commanding Officer, Signal Security Agency: in this way it was possible to effect unified control of all SSA enlisted personnel wherever stationed. The Battalion had detachments not only at Arlington Hall Station but all over the world wherever it became desirable to conduct any intercept activity. The Battalion did not, of course, include signal intelligence personnel directly under the control of theater commanders. While the Battalion embodied many unorthodox features—its maximum strength, for example, surpassed 5,000 officers and men and at the end of the War it was commanded by a Brigadier General—it effectively solved the problem of how to administer the amazingly complex activities performed by enlisted personnel working for the SSA.

* * *

It has already been noted that the SSA was administratively and functionally a part of the Signal Corps, but G-2 exercised staff supervision and control. While channels were erected whereby G-2 could exercise this control without at every step going through the Office of the Chief Signal Officer, nevertheless the SSA was primarily a Signal Corps agency, its personnel were Signal Corps employees, and for purposes of supply it relied on Signal Corps facilities.

Since it was increasingly felt by G-2 that the SSA was the most important source of intelligence, even closer control was required and therefore, on 10 December 1944, there came a change. The SSA was removed from the Signal Corps for operational control, which was now assumed by G-2, but administrative control was still retained by the Signal Corps. This cleavage of control was by no means clearcut and sharply defined: the line of division was not straight, since the

organization was pragmatic rather than theoretical, but in the main the differentiation thereafter was operational control exercised by G-2, administrative control maintained by the Signal Corps.

Divided control, such as this was, however, proved far from satisfactory in practice and was ended on 15 September 1945 by transfer of administrative control also to G-2, with the change of name from Signal Security Agency to Army Security Agency (ASA). This had the effect of associating the organization more closely with G-2, the user of one of the two chief products, but it will necessitate that in the future liaison be constantly maintained with the Signal Corps so that not only an adequate supply of trained personnel may be available for the communications side of its activity but also the increasingly closer relationship between signal intelligence and signal security may be maintained by the closest cooperation. Moreover, it also resulted in once more consolidating all responsibility for signal intelligence and signal security in a single organization, since the units formerly under the control of theater commanders were now made a part of the ASA.

As will be abundantly clear from specific references in the two following chapters, the SSA had the incalculable advantage of collaboration with the corresponding units of the United States Navy (OP-20-G and OP-20-K). Liaison with the Navy had long been in progress before the War but throughout the conflict it constantly increased in both the cryptographic and cryptanalytic fields. For some years before the War the Army and the Navy had been collaborating [text withheld] but the Office of Naval Communications, being pressed for personnel and facilities needed by units at work on enemy traffic [text withheld] asked the SIS to take over more and more work. . . .Early in the next year the first SIS mission was sent to England to establish the basis for liaison and in the summer the SIS and GCCS first exchanged permanent liaison officers, a relationship ever since maintained. Special missions have, however, also been sent and received from time to time. Intercommunications by radio, cable, and mail, have constantly maintained. Frequent agreements have been made to avoid unnecessary duplication of effort: the chief of these was reached in 1943 whereby the British assumed primary responsibility for signal intelligence operations for the War in Europe, the SSA, for those for the War in the Pacific, though neither Agency abandoned work in the field of the other's responsibility. This exchange of information has been broadest in cryptanalytic activity: considerations of security have limited cooperation in cryptographic compilation and development to work on systems used in combined British and American operations. . . . [text withheld]

The SSA provided trained personnel for and collaborated with U.S. Army Signal Intelligence Services in all theaters: Mediterrean Theater of Operations, European Theater of Operations, Southwest Pacific Area, China-Burma-India Theater, Central Pacific Area, etc. Collaboration between the SSA and the Central Bureau, Brisbane (CBB), began with the founding of the latter organization by joint action of the Royal Australian Army and the United States Army in the spring

of 1942. As will be later seen, this cooperative effort was maintained by constant intercommunication, particularly in the case of the Japanese Army cryptanalytic problem.

* * *

II. THE PRODUCTION OF INFORMATION

Modern intelligence services are able to derive information useful for military purposes from many sources but the most fruitful and most authentic is the enemy's message traffic and the communication system over which it is transmitted. Indeed, though messages differ in value, experience has proved that there are no messages, no matter how insignificant in content, which have potentially no intelligence value. Therefore, the cryptanalytic attack had to be made not only upon the purely military traffic transmitted by enemy forces but also upon diplomatic, commercial, and private messages as well. Even plain-text messages could not be neglected, but the largest part of the intercepted traffic was, of course, in cryptographic form and required cryptanalytic treatment before it could be read.

While some of the techniques used by the SSA were not strictly cryptanalytic in character, e.g. traffic analysis, secret ink solution, and exploitation of telephonic communications, the production of information involved, in general, the following steps:

a. Interception of traffic in large volume;
b. Traffic analysis of intercepted messages;
c. Solution of the cryptographic systems used;
d. Decryptographing of messages sent in solved or partially solved systems;
e. Translation of such texts as were in foreign languages, and
f. Publication of the texts in a form useful to the Military Intelligence Service.

* * *

A. INTERCEPTION

No cryptanalytic attack upon the communications of a foreign government can hope to be successful unless an adequate supply of intercepted material is available for study; nor can proper measures for safeguarding our own communications be taken without constant monitoring of the traffic sent out by American stations. It therefore became necessary to establish facilities for the interception of radio traffic in large volume.

Prior to the war there were seven fixed intercept stations located as follows:

No. 1 Fort Hancock, New Jersey
No. 2 Presidio of San Francisco, California
No. 3 Fort Sam Houston, Texas
No. 4 Corozal, Panama Canal Zone
No. 5 Fort Shafter, Territory of Hawaii
No. 6 Fort McKinley, Philippine Islands
No. 7 Fort Hunt, Virginia

Constant efforts during the War expanded these facilities greatly. In the end there were eleven fixed stations, many of which were far larger than any operating in 1941. These eleven, which were found sufficient to supply the necessary volume of traffic, were distributed as follows:

No. 1Vint Hill Farms, Warrenton,Virginia
No. 2Two Rock Ranch, Petaluma, California
No. 3 Indian Creek Station, Miami Beach, Florida
No. 4 [text withheld]
No. 5 Fort Shafter, Territory of Hawaii
No. 6 Amchitka, Aleutian Islands
No. 7 Fairbanks, Alaska
No. 8 [text withheld]
No. 9 Bellmore, Long Island
No. 10 Tarzana, California
No. 11 Guam

The three largest stations (at Vint Hill, Two Rock, and Fort Shafter) were equipped with elaborate arrays of high-directivity antennas for all-round coverage. These stations had been located so as to make easy the electrical forwarding of the intercepted traffic to Arlington Hall and the largest portion possible of intercept missions was assigned to them. The supplementary stations, particularly those at [text withheld] Amchitka, Fairbanks, and [text withheld] were located so as to intercept signals which could not be copied at the larger stations, and in general they had antenna systems beamed at specific targets of sectors. The stations at Bellmore and Tarzana were assigned the task of monitoring United States traffic for security purposes. Considerable assistance was rendered to the intercept facilities of the SSA, particularly in the period before the SSA's own intercept facilities were fully developed, by radio intelligence companies stationed on the West Coast and in the Pacific Area.

Among the new items of equipment developed during the War for use at intercept stations were "multicouplers," which allow the signal from one antenna to be coupled to several receivers; a "Hellschreiber Facsimile Recorder," for copying signals of this German system; and a "Time Delay Device," which accomplished a delay of from three to ten seconds between the time a signal is received and the time it is necessary to copy it, making it possible to start a recorder to take down the entire transmission for later transcription.

Intercept activity was coordinated and controlled by staff units at Arlington Hall which supplied the stations with technical advice. Speedy transmission from the intercept stations was effected chiefly by special teletype lines, which came more and more to take precedence over other means such as cable and air mail. From four teletype lines in operation on 7 December 1941, the number of such lines grew until on V-J Day there were forty-six. The amount of money paid for monthly rental of land-line teletype facilities alone reached in August 1945 the large sum of $58,918.02 but this figure does not include the cost of radio-teletype facilities, paid for by the Army Communications Service, for which no data are available to the SSA. Average monthly volume also constantly grew:

December 1943 279,034 messages
February 1943 46,865 messages
July 1945 381,590 messages
August 1945 289,802 messages

Arrangements were also made for obtaining traffic from radio intelligence units operating in theaters of war; from the Navy; from the several offices of the Chief Cable Censor; [text withheld]

B. TRAFFIC ANALYSIS

Traffic analysis, a procedure which first arose from attempts to reconstruct enemy communications networks and their characteristics with the aim of improving intercept facilities, became highly useful also for two other purposes: (1) Through study of the external features of the messages as distinct from the text itself, together with direction finding, by which it is possible to locate the site of unknown radio stations, traffic analysts were able to provide cryptanalysts with much useful information not otherwise obtainable; (2) Statistical study of the fluctuations in the volume of traffic passing in each circuit, and inferences drawn therefrom, became an important source of military intelligence. Traffic analysis can be carried on, of course, independently of successful cryptanalysis: useful information can be derived by traffic analysis even before a message is readable, but when the two techniques are combined, each is aided by the other.

While traffic analysis had been used to a limited extent in World War I, the British were the first to develop the science extensively in World War II. The beginnings of traffic analysis in the SIS date from April 1942. A mission was sent to England to gather information and upon its return it was possible to set up traffic analysis as an integral part of the SIS. As a result of this mission, efforts of the SSA in traffic analysis were to be concentrated on traffic in the Pacific theater, leaving to GCCS the primary responsibility for that in the European, a logical arrangement arising from geographical considerations.

The initial problem in traffic analysis for the SSA was the solution of the code numbers used to indicate message center place names occurring in Japanese mili-

tary messages, and the first success was achieved in September 1942. By the following June nearly all of the twelve main systems had been reconstructed, permitting accurate location and mapping of radio stations and circuits. Four distinct major military networks were identified, those used by the Imperial GHQ in Tokyo, the Southern Field Force, the Water Transport organization, and the Army Air Force. The adequacy of the techniques used was proved when, on 1 April 1944, the Japanese introduced a completely new place-name code which was almost wholly solved within a month, about half of the names being identified within 48 hours. Technical assistance given the intercept stations was responsible, at least in part, for the rapid increase in volume of Japanese military intercepts.

Contributions of traffic analysis to military intelligence began with the location of military message centers attached to unit headquarters. The identification of nets and unit organization revealed troop locations and chains of command, thus giving highly important information concerning the Japanese Order of Battle. Traffic flow analysis—the study of variations in traffic volume and patterns of station activity—gave indications of impending enemy activity. Convoys were detected and followed merely by studying the changes in the pattern of communications in the Water Transport code between various seaports along the route. Analogous studies of patterns in Air Force and Army Administrative codes led to detection of aircraft and troop movements. Analysis of communications between field units and their home depots indicated the location of almost all divisions south of Manchuria. The movement of a unit in the field could be detected from its home depot traffic, or through readdressed messages, or by messages addressed to the unit code name in lieu of a specific message-center location. Finally insight into the general content of diverse classes of messages, gained through traffic analysis, aided in establishing priorities in handling the thousands of messages received daily. Though publication of daily and weekly traffic analysis bulletins began in September 1942, the greatest emphasis on the intelligence aspect of traffic analysis came in late 1944 and 1945. Where deceptive measures are not employed, traffic analysis can yield a very large amount of fairly reliable intelligence; where deception is effectively practiced, deductions from traffic analysis must be used with extreme care. Since, however, there was currently no evidence that the Japanese engaged in deceptive communication measures (a fact which was confirmed after V-J Day), valuable results from traffic analysis were frequently obtained.

C. CRYPTANALYSIS

Cryptanalytic procedures are never stereotyped and permit no easy description. . . . [text withheld] Too much emphasis cannot be placed upon the need for cryptanalytic continuity. . . . [text withheld] It is characteristic of most cryptographers that they tend to introduce new cryptographic features and elements in a conservative manner. Thus, a new system will frequently not represent a radical departure

from its predecessor but will, rather, be merely a refinement and improvement of what went before.

Since this is likely to be so, the cryptanalyst who can start his study of a new system with a good acquaintance with the cryptographic character of the one just made obsolete, and of others used concurrently by the same government, will be at a great advantage. The basic factor underlying all successful cryptanalysis, however, is constant watchfulness for significant details which may provide an entry: one or another of the operations mentioned above may reveal the nature of the system but the surest method is statistical analysis.

In World War I and for many years thereafter, such statistical analysis was dependent upon hand methods alone. The cryptanalyst or his clerical assistants were forced to make frequency counts or other statistical tabulations of the units or text (letters or digits), taken either singly or in groups, by hand. Not only did the process involve an immense amount of drudgery but it was also easily subject to serious error. The eye had to keep the place in a meaningless text while the hand made the necessary indications on the charts. Naturally, the work, to be dependable, had to be painstakingly accurate: the result was that it was time-consuming.

Even under the conditions of World War I, when the volume of intercepted traffic was relatively low, this was already a problem of most serious proportions. As a consequence, steps were taken during the period of peace to find adequate solutions to the problem. The most significant trend in cryptanalytic research and development during World War II has been, in fact, the extent to which machinery has been used to speed up hand methods and also to perform operations which, because of their magnitude, could never have been attempted without such apparatus.

A very large measure of the success of the SSA in cryptanalysis must be attributed directly to this fact. The enormous increase in the volume of intercepted traffic would alone have made hand methods wholly inadequate to accomplish the task set us in this War. Fortunately, none of the enemy nations seems to have realized the possibility of developing such machinery and the necessity of protecting their cryptographic systems against attack by such means, or if they did, as was true in the case of the Germans, the realization was not too clear and insufficient emphasis was placed upon the development of mechanical and electrical analytical equipment. The SSA, on the other hand, has had to keep constantly in mind, while developing cryptographic systems for our own use. . . , the possibility that other nations might also make, during the war or later, similar advances in machine cryptanalytic techniques and to prepare against that contingency. Thus, any new development in cryptanalytic techniques has the immediate effect of causing a converse development in cryptographic techniques, and vice versa. This is the fundamental reason why all research and development in both fields must be carried on within a single organization. [text withheld] Several types of machinery have been used. The first of these is standard tabulating machinery, including machines available on the open market as well as machinery of the same general type modified or

developed expressly for the SSA. The method involves the recording of data on a card in which holes are punched by means of a key-punch machine and the processing of decks of such cards by a number of other machines. [text withheld] While few, if any, cryptanalytic units have failed to make extensive use of these machines, by far the greatest employment of them has been in the solution of the Japanese Army systems. Indeed, the solution and processing of any significant quantity of the hundreds of thousands of messages in those systems would have been impossible without these machines. An indication of the growth of the use of tabulating machines of this type by the SSA in the fact that whereas only 13 machines and 21 operators were at work at the outbreak of the War, 407 machines had been installed at the peak in April-May 1945, involving a total of 1275 persons as operators and supervisors. The monthly rental for these machines reached a peak in June 1945 of $60,982.

In addition to standard and specialized tabulating machinery, another important category of machines was that generally referred to as Rapid Analytical Machinery (RAM). Machines of this category usually employ vacuum tubes, relays, electronic circuits, and photoelectrical principles. A number of different types, designed within the SSA for specific operations, were developed and constructed by the SSA itself or in cooperation with several contractors, and set up at Arlington Hall Station. One cryptanalytic machine, costing almost a million dollars, was basically homologous to an automatic telephone exchange capable of serving a city of about 18,000 subscribers, and the SSA had two such machines. These two machines were capable of performing operations which, if done by hand methods, would have required over 200,000 people. A second cryptanalytic machine, specifically designed to perform a certain type of test by means of electrical relays, served as the equivalent of 6,000 cryptanalysts; and an improved machine of the same general nature, but using vacuum tubes and electronic principles rather than relays, is now almost completed. It is expected to operate at least 500 times faster than the relay type and can be estimated to be equivalent to having 3,000,000 people at work. In the development and construction of these highly specialized cryptanalytic machines the SSA expended several million dollars, but it could hardly have operated without them.

D. SOLUTIONS

Cryptographic systems have grown in complexity very greatly since World War I, and in a brief report such as this it is impossible to give more than an inkling of the length to which many foreign governments have gone in improving their methods. Larger and more scientifically constructed codes were introduced; complex radio procedures and superencipherment systems were added; and intricate cipher machines were developed. By the year 1939, when the outbreak of war in Europe caused the first substantial expansion of the SIS since 1930, cryptanalyt-

ical attack was being centered in accordance with directives from G-2 [text withheld] . . .all systems thus far studied were entirely diplomatic in character; indeed, little traffic of other categories was then being intercepted. Work proceeded along these lines, effecting solutions which will be discussed in greater detail a little later, but so far as cryptanalysis is concerned, this was the situation existing on the day of the Pearl Harbor attack. [text withheld]

(1) Japanese Diplomatic and Military Attache Traffic. The first diplomatic systems to receive attention in the SIS were the Japanese, and from 1933 to 1941 eleven such systems were studied and solved. For the most part they were not greatly advanced in cryptography from those solved before 1930, but in two machine ciphers, the earlier of which had appeared by 1932, the Japanese demonstrated that they had read with profit *The American Black Chamber*, in which Herbert O. Yardley, formerly an officer of the Military Intelligence Division, indiscreetly revealed to the world American successes in solving foreign cryptographic systems.

The machine ciphers presented cryptanalytic problems of greater difficulty, involving not only the reconstruction of a complicated machine but also thereafter the day-to-day recovery of a great number of keys. The second of these machines, introduced in 1938, was much more complex than the first and required almost two years of concentrated study to solve: its solution by the SSA, unassisted by any other cryptanalytic organization, represented an achievement of first magnitude and importance. It is now known that the German organizations attempted the feat and failed, [text withheld] The remarkable feature of this solution was that a machine capable of deciphering the Japanese messages was reconstructed wholly by analysis: the SSA has never seen one of the Japanese machines. The importance of this solution can hardly be over-estimated.

General Marshall, in his now famous first letter to Governor Dewey dated 25 September 1944, and disclosed in the Joint Congressional Hearing in the Pearl Harbor disaster, stated that "our main basic of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government.". . .

In addition to this machine, which remained in current use until the end of the War because knowledge of its solution was fortunately kept secret during the War, the Japanese also began to use for diplomatic purposes a variety of other high-security systems based on intricate cryptographic principles. [text withheld] The result was that the best efforts of a large staff of the ablest experts working continuously on this problem were necessary to solve the diplomatic and military attache systems. Solution was, even so, effected in nearly all cases, providing a very large volume of translated messages giving significant information as to the intentions of the Japanese, conditions in the Far East, and also of conditions in Europe. Indeed, it has been said that the Japanese military attaches were the best secret agents of the United Nations on conditions inside occupied Europe.

The value of the intercepted Japanese diplomatic and military attache traffic for intelligence purposes can best be illustrated by representative translations, but of the many thousands of messages which appeared in the SSA Bulletin, only a few can be chosen for inclusion in a brief report such as this. . . .

a. Berlin to Tokyo, . . .translated 4 December 1943, sent in the [text withheld] (military attache system). . . .The full text, too long for reproduction here, is a report of a visit made in the fall of 1943 by a subordinate of Baron Oshima to the German western fortifications. The military information contained in this message was of incalculable advantage to the planning of the invasion of France. . . .

b. Berlin (Oshima) to Tokyo, . . .translated 12 August 1944, sent in the [text withheld] (diplomatic) system. This message. . .has been described by officers in MIS as "worth all the expenses of maintaining the SSA." The text describes conversations with the head of the Todt organization, Albert Speer, in which the latter revealed to the Japanese, and, thus to us, highly important information concerning the production of munitions in Germany. . . .

c. Hanoi to Tokyo, . . .translated 1 February 1945, sent in the [text withheld] (diplomatic) system. This message is important because it reveals that the Japanese were interested in obtaining uranium. . . .

d. Moscow (Sato) to Tokyo, . . .translated 30 July 1945, sent in the [text withheld] (diplomatic) systems. This three-part message, the translation of which was available to President Truman during the Potsdam Conference, reveals the activity of Sato, Japanese Ambassador to Moscow, at the time of the conference. . . .It will have been noted that while two of these four messages were translated within two days after they were transmitted, another took about ten days and the fourth nearly a month for translation. Delays of this kind may be attributed to a number of factors. [text withheld] Secondly, a sharp rise in the volume of intercepts may create a backlog of unprocessed messages which may take several days to eliminate. Thirdly, there is the question of translation: in the case of Japanese texts, for example, in spite of the great efforts made to train competent Japanese translators there never were enough of these to keep up at all times with the production of the cryptanalysts. To prevent highly important messages containing information demanding immediate action by MIS from being laid aside until the information was too late to be useful, a policy was adopted of scanning the messages as they became readable in order to sort them according to the degree of urgency. In spite of these difficulties, however, it frequently happened that messages were intercepted, decoded, translated, and placed in the hands of MIS before their addressees might be presumed to have read them. A conspicuous instance of this kind was the famous message by which the Japanese transmitted through the Swiss Government their intention to accept the surrender terms. The fact that the Japanese had accepted the Allied terms was known in the MIS several hours before the Swiss Minister was able to give the message to the State Department.

(2) Japanese Army and Air Force Traffic. The following paragraph is quoted

from a communique which appeared in The New York Times on 4 September 1943: Wewak: Our strongly escorted medium bombers attacked an enemy convoy of five cargo ships and two destroyers which arrived during the night with reinforcements and supplies for the enemy garrison. Coming in at masthead height, our bombers scored direct hits with 1,000-pound bombs on three freight transports, each of 7,000 tons, sinking them. In addition, one of the escorting warships and a 1,000-ton cargo ship sustained direct hits and were left ablaze. Numerous small harbor craft were destroyed by strafing. Intense anti-aircraft barrages were encountered and barrage balloons from ship and shore were employed in an endeavor to halt our low-level attacks. Thirty-five fighters flown in from the rear bases to protect the convoy were intercepted in the air. Twelve of these were downed with eight others probably destroyed and five damaged. Three of our bombers and one fighter were lost.

Note that in the entire communique there is no explanation of the method by which the American commander in the New Guinea area learned of the presence of the convoy at Wewak: the impression is given, as indeed was intended, that the good fortune of the bombing mission in finding the convoy solely was the result of chance. Yet this was not so. A message had been intercepted and read by the SSA (on 20 August, nearly two weeks ahead of time) which foretold to the Japanese at Wewak the arrival there of the the convoy on the first or second: . . . .The message in its English form was forwarded speedily to MIS and thence by radio to the proper commander for his use. This instance is, of course, only one of many which could be adduced to show how in an age of radio communications the necessity of forwarding an intercepted text thousands of miles to a control agency for decipherment and its return when made readable causes little more delay than would have taken place had the cryptanalysts been at work at the points of interception.

In order to prevent the Japanese commander at Wewak from suspecting the truth, precautions were taken, in accordance with rigid regulations, to provide an additional source of the information which he would naturally suppose to be the only one, namely, reconnaissance planes were sent over Wewak. On many occasions, in fact, American commanders were in possession of valuable information provided by the SSA which they could not use because to do so would have run the risk of revealing to the Japanese the fact that their secret communications were being read by us. The ability to continue reading the traffic as a whole was often a military objective of greater importance than that involved in the successful completion of a specific mission.

The bombing of the convoy at Wewak, as just described, is a good example of the effect of the translation of an isolated message—only the third part of a three-part message had been translated in time—but many messages, which individually are less striking, when taken together and coordinated by MIS, permit the accomplishment of even more spectacular results. The following paragraph is taken from a memorandum prepared by an officer in MIS (27 March 1945):

Use of Ultra (= SSA) Information for Attack on Japanese Troop Convoy

1. Information received. ULTRA traffic on and shortly after 2 April 1944 revealed Japanese plans to send a large convoy, designated as the "TAKE" Convoy, to Halmahera and New Guinea. The convoy, consisting of nine merchant vessels and about twelve escorts, sailed from Shanghai for the south in the latter part of April, carrying 12,874 troops of the 32nd Division, about 8,170 troops of the 35th Division, with equipment and other military supplies. Messages furnished the identity of the ships and full details about the troops and cargo loaded on each ship. Traffic analysis disclosed the approximate date the convoy was scheduled to leave Shanghai for Manila and provided current information on the convoy's approximate position on its trip from Shanghai to Manila. Before the departure from Manila on 1 May, messages revealed the following information:

a. scheduled noon positions for each day from 2 May to 9 May;

b. an outline of an alternate route to be followed only on receipt of special instructions;

c. a plan to divide the convoy into two groups on 7 May to a point N of Halmahera, one part (presumably the 35th Division ships) scheduled to go on to Manckwari, and the other part presumably (32nd Division ships)scheduled to go on to Wasile on Halmahera.

2. Action taken. Information on the composition, loadings, movements of the TAKE Convoy was forwarded to the appropriate field commands, as it became available.

3. Operational results. On 26 April the convoy was attacked by submarine at a point 30 m. W of Laoag (NW Luzon) and one ship was sunk. On 6 May the convoy was again attacked by submarine 100 m. NW of Menado and three additional ships were sunk. About 4,000 troops together with ordnance and other supplies were lost as a result of those sinkings, including the Commanding Officer and 2,700 troops (substantially all) of the 220th Infantry Regiment of the 35th Division. Two Japanese divisions, both critically needed as reinforcements, were thus decimated and their effectiveness seriously reduced. Both divisions have since been met in combat. The above information concerning operational results also was received from Ultra sources.

4. Ultra material used. Preparation of the intelligence dispatched to the field commands required the examination and integration of a large number of separate and frequenctly fragmentary messages and traffic analysis.

The fact that the two examples already chosen were both concerned with the sinking of convoys should not be allowed to give the impression that this was the only phase in which intelligence was derived from Japanese Army messages. To quote again from the report already cited as prepared by an MIS officer:

A 28 May (1944) message, available 1 June, mentioned supplies needed by the 18th (Japanese) Army (controlling operations in eastern New Guinea) which must arrive at Wewak by the end of June in order to be of use in "the attack on Aitape."

In a 24 June message, available shortly thereafter, the Southern Army stated that the 18th Army would attack Aitape. Various other fragmentary messages, all showing that an attack on Aitape was planned, were also received. On 25 June there became available a 20 June message from the 18th Army reporting that it was planning an all-out attack against the U.S. Aitape perimeter, to begin about 10 July and giving the detailed dispositions of each division under the command of the Army, plus the planned operations of each division in the attack. Total strength of the forces involved was stated in the message to be about 20,000. . . . All of (this) information was made available to the Commander-in-Chief, Southwest Pacific Area, before the date of the planned attack. . . . The Japanese attack was made on schedule and was completely defeated with heavy losses to the Japanese.

The examples just given show how the product of the Japanese Army cryptanalytic projects was of the greatest value in military operations in the Pacific area. We must now turn to the steps by which the product was made possible. Before the War attempts by the SIS to solve the secret communications systems of the Japanese Army had, for lack of sufficient traffic and cryptanalytic personnel, been fruitless. [text withheld] Immediately after the attack on Pearl Harbor more SIS personnel were assigned to the Japanese Army problems, but little could be done except to sort and file the traffic. Thus, cryptanalytic continuity was broken for a time. [text withheld] Cipher solution may be compared roughly to the operation of demolishing a building by undermining its substructure and causing the building to collapse suddenly; code solution is more like a mining operation, the ore is taken out of the mine bit by bit.

By the autumn of 1942, however, traffic sources had been established and more personnel had been obtained, so that considerable attention could be given to these problems. [text withheld] This historical method, though seemingly a long way round, was really the only recourse and it was fully justified by the results. By January 1943 progress had been made beyond the period of [text withheld] and at the same time encouraging results were being achieved in the recovery of code groups for addresses, which had previously seemed so hopeless a problem. [text withheld] In April 1943 the first break into a current system (that was used by the Japanese Army Water Transport organization was made possible [text withheld]. In this instance the entering wedge was simultaneously discovered (almost in the very same hour) by personnel of the SSA at Arlington Hall and of the CBB in Australia. It was most successfully exploited as the result of the constant collaboration maintained by daily intercommunications between the two organizations.

The result of this initial solution was a reorganization of facilities within the SSA leading to considerable expansion in personnel and services devoted to the Japanese Army problem. Ultimately, the number at work on these problems exceeded that of personnel at work on all other cryptanalytic problems combined, and yet there never were enough trained workers to carry out fully all phases which needed to be done: the man-power situation was such at the time that the

demand for personnel was always greater than the supply, and even when the needs were temporarily filled there always was some delay between the time new personnel reported for duty and the time they were ready to participate effectively in actual operations, because preliminary training was usually essential.

By early June 1943, two months after the initial break into the system, translation of Water Transport messages were being forwarded to MIS. Thereafter, until almost the end of the War, the Water Transport system provided not only a broad picture of the Japanese Army shipping organization and activities but also, from time to time, information regarding specific operational movements of which the logistics problems were discussed in Water Transport messages. To quote once more from General Marshall's letter to Governor Dewey:

"Operations in the Pacific are largely guided by the information we obtained of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them, and what is of vast importance, we check their fleet movements and the movements of their convoys. The heavy losses reported from time to time which they sustain by reason of our submarine action largely results from the fact that we know the sailing dates and the routes of their convoys and can notify our submarines to lie in wait at the proper point. The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based on timing of the known movements of Japanese convoys, two of which were caught, as anticipated, in his destructive attacks."

Although undoubtedly General Marshall included in this tribute to the signal intelligence services the very outstanding contribution from the signal intelligence service of the Navy, for fleet movements are mentioned, the bulk, however, of the information of the type cited came from the SSA.

Solution of the main Ground system was effected by a series of discoveries that began in May 1943 and culminated in decipherment of messages in September of that year. Also, by the summer of 1943, solution of the address system had reached a point where the addresses of current intercepts were readable. Reconstruction of the address code books, which had hitherto been carried on exclusively by a British organization in India, known as the Wireless Experimental Center (WEC), was now undertaken at Arlington Hall.

The order of battle intelligence derived from daily lists of the addresses of Japanese Army units was a useful adjunct to the text of the messages and even supplied knowledge of military operations in periods when the messages themselves were not readable. Thereafter, despite repeated changes and innovations made by the Japanese in their cryptographic systems, solution was continuous, though on occasion it was temporarily delayed. The knowledge of Japanese cryptographic practices and previous solution of the basic code book permitted the reading of periods which, from a cryptanalytic point of view, were as difficult as the systems encountered at the time of Pearl Harbor attack, systems which had then been considered hopeless of success.

Two major technical problems which had to be solved in 1944 were the introduction by the Japanese on 1 August of a new cryptographic practice which disguised the system indicators and a radical shortening of the life of one of the keying elements used in the Administrative systems. The uncovering of the disguise in the case of each system indicator was, of course, a prerequisite to the subdivision of intercepted messages into their respective systems preparatory to any other steps toward solving or reading the messages. Though the introduction of this feature might have been a major cryptanalytic disaster, it fortunately turned out to be only a nuisance, because it was at first effected by an insecure method, and speedy solution was therefore possible. Subsequently the Japanese modified the method to the point where, had it been used initially, solution would have been almost impossible. With continuity of solution, however, aided by information from cryptographic instruction messages and captured materials, this handicap was overcome.

The problem presented by shorter intervals (five days instead of three weeks) between changes of keys, was essentially one of carrying on analysis of one of the steps of encipherment with only about a fourth of the traffic previously available, was eventually solved by a combination of methods, namely, very careful correlation of every piece of intercepted traffic, the use of tabulating machinery, which enabled a tremendously large number of operations to be made in a short time, and the use of photoelectric equipment to exploit phenomena resulting from messages with identical or nearly identical text but cryptographed with different keys.

Once the Japanese began to suffer military reverses, their cryptographic materials were frequently captured and these soon came to play a vital role in solution. Especially important was the capture of the basic code books, or of the key books which the Japanese could not easily replace with new editions and which therefore were occasionally continued in effect for some time after their capture. The complete reconstruction of such code books and key books would have been a long and painstaking task which would have resulted in delays in production of intelligence and possibly also in some diminution of its reliability. Yet the continued capture of such materials was not an unmixed blessing, since whenever a capture was known or even suspected, the Japanese naturally changed as many of their other cryptographic materials as possible.

Thanks to the care with which information obtained from the translated messages was used by field commanders, the Japanese seem never to have suspected the possibility of cryptanalytic compromise but, as they began to realize that Allied Forces were able to anticipate their plans, they attributed our success to espionage activities. The following extracts are taken from a message, intercepted and read by the SSA, which was sent from Pinrang to Piru (RIYA Communications Officer) on 18 December 1944. . .

***

". . . .there are substantial indications that the enemy has understood our important plans in the Burma and Philippine areas. Therefore, we are inclined to be somewhat doubtful about the codes now in use (and) each unit commander must multiply his alertness toward counter-espionage . . . . This is an order. Furthermore, you should exert your best efforts towards overcoming the deficiencies in the counter-espionage set-up, and towards perfecting it. If you fail to do this, troubles will arise, and you must take resolute action in facing them, without a thought for yourself."

Because of actual or suspected compromise, however, changes were made so frequently and complications so often introduced in the Ground systems that analysis became more and more difficult. By the end of the War the Ground problem reached the point where the time required for solution made the production of current translations seemingly impossible. The general intelligence value and the special cryptanalytic interest of the problem, however, warranted studies of the last unsolved period of the highest-echelon Japanese Ground Force system, for which no captured material or special cryptographic intelligence were available. These studies, successfully carried out during the final months of 1945, demonstrated that the development of cryptanalytic attacks had kept pace with the ever-increasing complexity of Japanese cryptographic procedures.

On the other hand, no compromises or suspected compromises took place in the case of the Water Transport systems, and in the latter, the Japanese moved in an orderly fashion to make their periodic changes. Consequently, the cryptanalysts were less hampered by frequent or sudden changes and a fair proportion of the messages in each key book were read currently. Had no compromises been made in the ground systems, the same success might have been experienced. Therefore, it is a moot question whether compromised material gave an overall advantage or not.

For lack of sufficient personnel and because of the special interest of GCCS in the air systems, the SSA did not concern itself to any considerable extent with those systems until late in 1944. Thereafter, more and more attention was devoted to the air problem and the SSA eventually made large contributions to current solution.

After some early compromises in 1944 the Japanese signals systems were read from time to time. The cryptography used was such that, with the limited volume of traffic, solution would have been extremely difficult without a compromised code book, but fortunately at different times several successive editions of the signals code books were captured, along with the key books for a number of periods. The text of these systems, which discussed call-sign frequencies, and methods of handling traffic, was of special interest primarily to our traffic analysts.

While the study of low-echelon Japanese systems was never considered a primary responsibility of the SSA, reports from field agencies were examined here and their contents served as a guide in the training of military personnel destined for field agencies. The SSA did actively participate in the solution of the low-eche-

lon air system known as "BULBUL" but only as a support for the cryptanalytic unit in the India-Burma Theater.

The impression has already been given that had more personnel been made available and at at an earlier date, solution of Japanese military communications might have been expanded and expedited. Yet it should be pointed out that had all the U.S. Army personnel working on the Japanese Army problems, not only at Arlington Hall Station but also in the Central Bureau at Brisbane, in the Hawaiian Islands, and in the India-Burma Theater, been grouped together at one center and solution activities thus been concentrated, considerable unnecessary duplication, especially in the field of translation, would have been eliminated. On the other hand it must be admitted that had such a consolidation taken place problems of administration would have been greatly increased but the advantages gained by the increase of trained workers all applying their efforts in a coordinated attack would have outweighed by far any administrative difficulties. As it was, where circumstances permitted, duplication was eliminated and, considering the great distance between the agencies concerned, cooperation and coordination effected by the interchange of mail and telegraphic communications was good.

In retrospect, it may be noted that in the signal intelligence field the consequences of lack of continuity and unpreparedness for effective operation immediately upon the outbreak of hostilities are nowhere more clearly demonstrated than in the case of the Japanese Army high-echelon secret communications. It is a fact that, during the entire period from 7 December 1941 to the summer of 1943, none of these communications was being read. Had this been otherwise, the military situation might have been quite different. To judge purely by the disastrous effect that the solutions obtained by us after the autumn of 1943 had upon Japanese operations, it is legitimate to think that the important early Japanese penetrations to the south might have met with greater obstacles and that as a result the War in the Pacific might have been terminated many months earlier. If an adequate staff of cryptanalysis had been engaged in studying Japanese Army traffic continuously from 1939, when the systems were solvable with comparative ease, complete continuity could have been maintained from the very outset of the War. After 1939 the systems became more difficult but never more difficult than they were in 1945 when, because of the possession of a background of knowledge and experience built from successful reading of earlier periods, they were solved.

* * *

(4) German Army and Air Force Traffic. It has already been noted that a logical division of work between the British and the U.S. Governments resulted in concentration of the SSA on solution of Japanese diplomatic communications and Japanese military traffic in the Pacific theater, leaving the exploitation of German and Italian military traffic in the European theater the primary responsibility of the

British. [text withheld] In the tense days of early 1942, however, the advisability of insuring against the contingency that the British organization working on enemy communications might be put out of operation by enemy action led to the establishment of an SSA unit to serve as a back-up. Though the SSA played the minor role in the work on German Army and Air Force and Italian Army and Air Force traffic, nevertheless it made noteworthy contributions.

The German Armed Forces employed two basic types of cipher machines. One of them, a modification of a commercial machine known as the Enigma, produced cryptograms of a very high order of security, but faulty usage, Teutonic love of order, and addiction to stereotyped modes of expression made it possible for the British to solve a very large portion of all the messages transmitted, yielding intelligence of the highest value. In this work the SSA served as a cooperating and assisting echelon, contributing new ideas, techniques, and machinery. As a result of excellent coordination of basic research and development with practical operations, SSA engineers invented and built an electronic solution machine far in advance of anything hitherto known for solving messages in the most complicated form of the Enigma machine as used by the Germans.

In addition to the foregoing, specialy selected messages were sent from England to Arlington Hall for study and solution by SSA special machinery. The necessity for speed brought into use special communication channels and there were cases wherein the answer to a specific problem was obtained by the SSA, wired back and in the hands of the GCCS cryptanalysts within 90 or sometimes as few as 60 minutes.

* * *

The German Armed Forces also used a series of complex cipher machines for enciphering teleprinter communications among their highest echelons. Here again the SSA collaborated with [text withheld] in inventing and designing new machinery as well as in testing new techniques and procedures. Two machines in particular, invented, designed, and built either entirely at Arlington Hall Station, or by an outside contractor working under the direction of SSA engineers, [text withheld]...were successfully employed [text withheld] In addition to making an important contribution to the victory in Europe, the experience the SSA gained in such collaboration will, of course, be very useful to the U.S. Army in future research in this field.

Mention must also be made of our contribution in the signal intelligence operations in the Mediterranean Theater. Here again the SSA furnished key and basically-trained personnel for Signal Corps units working in collaboration [text withheld] on both German and secret communications.

* * *

(8) Commercial Code Traffic. Exploitation of the information to be obtained from decoding traffic [text withheld] in public commercial codes was carried on more or less continuously after early 1943. This activity was at first confined largely to codes in the chief languages of Europe but was ultimately extended to include also a group of Japanese commercial codes which provided a rich mine of militarily useful information concerning conditions in the Far East.
(9) Special Problems. In addition to the traffic already described, the SSA had to face a number of other special problems requiring other techniques.

These included the transcription of shorthand documents; the solution of open codes, a type of cryptography in which a secret text is hidden within an ostensibly harmless message; the transcription and translation of "scrambled speech," that is, telephonic and radiotelephonic conversations in enciphered and unenciphered form in foreign languages; and the solution of secret ink messages. The last named type involved much work for the Office of Censorship as well as for MIS. In this field the SSA technicians accomplished feats not duplicated elsewhere: the recovery of printing on documents which had been printed by use of inks soluble in water, In the case of two documents very valuable code materials were recovered for the Navy; one involved a German, the other a Japanese code book.

E. SOME GENERAL REMARKS

The remarkable success which the cryptanalytic units obtained must not be allowed to create the impression that any of the tasks was accomplished without skill, training, patience, vigilance, and mental labor of the most exhausting kind. A description of the essential features of a solved cryptographic system may often seem simple and it may be imagined therefore that solution was easy, but this is rarely the case. Frequently, a simple cryptographic trick may be as difficult to detect as one of the more complex varieties; in cryptanalysis the effect of some minor complicating factor, inserted solely to prevent solution, may prove to be a serious stumbling block, though occasionally it may also prove to serve in the end as the entering wedge leading to solution.

The time and effort needed for solution, of course, vary with the system. A simple substitution cipher may require only a few minutes' work by a single analyst; other systems may be so difficult that the entire efforts of a number of persons working for many months are needed. Of the two basic types of cryptography, codes and ciphers, reconstruction of the former is, as has already been noted, a slow, laborious process, each code group having to be identified singly, and the larger the code, the longer the time needed; solution of a difficult cipher may take equally long but success is instantaneous rather than gradual—at one moment the cipher is unsolved, the next it is solved. The reconstruction of a cipher machine is, of course a very long process, but when this is finished, the keys used in each day's traffic may still have to be solved as they appear. For this reason, even when the

machine has been reconstructed, reading of current traffic may be delayed until enough traffic all in the same specific key has been received to permit solution.

Systems differ so greatly that a counting of solved systems is no adequate indication either of the volume of work accomplished, or of the brilliance of the achievement of the cryptanalysts. During the War a group never numbering more than twenty, and for a long time many fewer, succeeded in making readable approximately twenty-five systems. In the same period a group of about eighty persons were needed for the solution of a single system. For this reason the efficiency of the two groups cannot be evaluated in terms of the number of systems solved.

* * *

. . .By August 1945, however, the traffic [text withheld] had been studied and translations were currently being prepared in large volume. The number of these translations is really the best gauge of the cryptanalytic achievements of the SSA, since they are the final products of the cryptanalysts, assisted by the combined efforts of intercept operators, clerks, translators, editors, typists, and proofreaders....Factors causing fluctuation of volume were complex: it is not always possible to explain declines, but on occasion the introduction of new cryptographic techniques had the effect of slowing up production temporarily until solution was achieved.

After cryptanalysis the messages in almost every instance still had to be translated—a small percentage of the messages are transmitted by their originators in English—and after the translations were prepared in draft form, they had to be checked for diction, accuracy, and format, and then typed for reproduction by the "Ditto" process. "Master copies" of the translations were then once more proofread for accuracy of typing and the required number of copies prepared. Following this, they were forwarded at frequent intervals during the 24 hours to MIS. In certain cases, where urgency required it, forwarding was either by special courier or by electrical means, over special cryptographic circuits.

Even then, the task of the SSA was not finished, for it was necessary that the daily "SSA Bulletin" of translations be read carefully by personnel whose duty it was to compile therefrom voluminous information which would, in turn, be useful to the cryptanalysts working in other problems. Thus the fruits of the labors of one working unit could be at the disposal of any others that might need it. In this connection it may be stated that the free exchange of information and results among the traffic analysis units, the cryptanalytic units, the translation and "bulletin" units, the communications-security units, and so on, is absolutely vital to success in the whole cryptologic field.

* * *

From *A Brief History of the G-2 Section, GHQ, SWPA. In the aftermath of World War II, the G-2 section of U.S. Armed Forces, Far East, commanded by General of the Army Douglas MacArthur, devoted some of its energies to preparing histories of its successes in the war in the Pacific. Included in A Brief History of the G-2 Section, GHQ, SWPA and Affiliated Units: Introduction to the Intelligence Series was a short history of MacArthur's own World War II COMINT organization, a collaborator—and rival—of Arlington Hall.*

CENTRAL BUREAU (CB)

Central Bureau, a combined Australian-American organization, was activated on 15 April 1942 under the command of Colonel Joe R. Sherr, one of the officers evacuated from Bataan. From its inception until the end of the war, the Bureau operated under the direction of Major General S.B. Akin, Chief Signal Officer of the Southwest Pacific Area, who was largely responsible for its establishment and technical development.

The first contingent of American signals intelligence personnel to reach Australia after the outbreak of war consisted of six officers and eight enlisted men who comprised the 837th Signal Service Detachment. These men left the United States on 16 April 1942 on the last scheduled Clipper flight to Hawaii. As all regular runs from Honolulu to Auckland, New Zealand, had been discontinued, they had to "sweat out" the remaining 7000 miles of their trip as space became available on USAAF and RAAF planes. From Sydney, they proceeded to Melbourne to join the GHQ established by General MacArthur. Within the next two months the American contingent was augmented by 12 additional enlisted men and 3 officers, including Major A. Sinkov who took over the command of the Detachment.

The Australian Army component of Central Bureau was the Australian Special Wireless Group which had seen considerable service against the Germans in Africa and the Near East and which included some British personnel who had escaped from Singapore. The Australian Air Force component consisted of personnel assigned from Victoria Barracks, Melbourne.

In the field at that time, Central Bureau maintained radio personnel as follows: AIF /Australian Imperial Forces/ - No. 51 W/T /Wireless Telegraphy/ Unit and the RAAF - No. 1 Wireless Unit. Attached to the latter as special instructors were three U.S. signal intelligence personnel (Lt. Howard W. Brown, Sgt. John J. Phelan, Sgt. Carl Card) who had been evacuated with Colonel Sherr from Bataan.

The 837th Signal Service Detachment was deactivated in May 1943 and replaced by the Signal Intelligence Service (still a component of Central Bureau) under Col. Harold S. Doud, with Capt. Chester W. Ray as Commander of Troops. In the autumn of 1943, Colonel Sinkov became Commanding Officer, SIS, and

During the 1920s, Herbert O. Yardley headed the legendary "Black Chamber," a secret cryptanalytic bureau jointly funded by the War and State Departments. Forced into retirement, he sought to recoup by writing a sensational exposé of American intelligence activities. (NSA)

This brownstone house in New York City served as the headquarters for Yardley's organization. (Louis Kruh)

The brilliant cryptologist William F. Friedman became the first head of the Army's Signal Intelligence Service (SIS). (George Marshall Foundation)

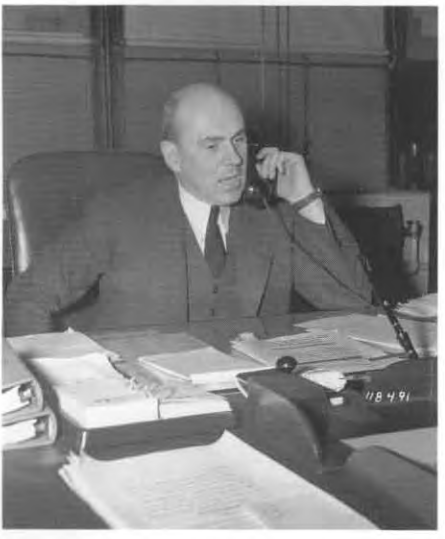
A rare photograph taken of Friedman and his small SIS staff around 1935. (INSCOM)

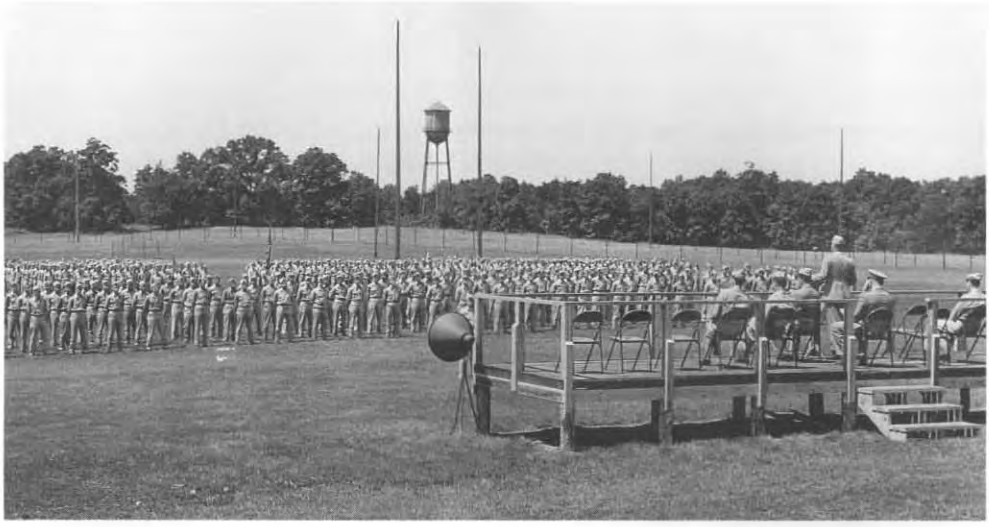
From 1929 to 1942, the headquarters of the Signal Intelligence Service was located in the Munitions Building, a large temporary structure built in World War I. (NARA)

A member of the 2d Signal Service Company operates a radio direction finder on Hawaii shortly before World War II. The company served as the collection arm of SIS. (C.T. Duval)

The battleship *Arizona* sinks under Japanese attack at Pearl Harbor. The success of the Signal Intelligence Service in breaking the Japanese diplomatic machine cipher could not forestall a Japanese military surprise. (DAVA)

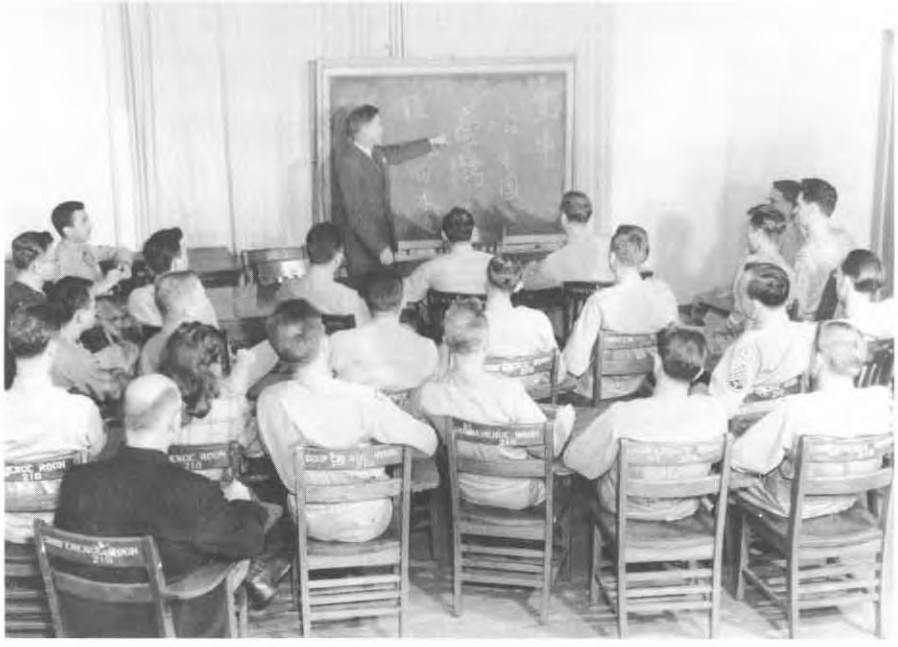
The perceived American intelligence failure at Pearl Harbor led top Army leadership to find ways to better exploit the potentials of communications intelligence. Clockwise, Secretary of War Henry L. Stimson, Assistant Secretary of War John J. McCloy, Assistant Chief of Staff for Intelligence Maj. Gen. George V. Strong. (NARA)





A graduation parade at Vint Hill Farms School in Warrenton, Virginia. Successful prosecution of the signals intelligence war demanded thousands of trained Army cryptologic specialists. (INSCOM)

A Japanese language training course conducted at Arlington Hall Station, Virginia. (INSCOM)



A former women's junior college, Arlington Hall was taken over by the War Department in 1942 and became the new headquarters of the Signal Intelligence Service. (INSCOM)

Staff heads of the Army Signal Security Agency pose for a group portrait at Arlington Hall Station in 1944. (INSCOM)

Army cryptanalysts at Arlington Hall Station work in an open bay in one of the large temporary buildings constructed to meet the needs of the Signal Security Agency's growing work force. (INSCOM)

Masses of calculating machines were used at Arlington Hall to process and exploit Japanese military traffic. (INSCOM)

Capt. I.W. Wolfe, Commander of Troops.

Central Bureau expanded rapidly. Its strength in 1943 was well over a thousand men and women. Technical direction under General Akin was vested in three assistant directors who were the ranking officers of the three largest contingents: Colonel Sinkov for the Americans; Lt. Col. A.W. Sandford for the Australian Military Forces, and Wing Comdr. H. Roy Booth for the Royal Australian Air Force.

The Bureau brought under a unified control personnel from the signal intelligence services of five nations. Included were the following military and naval forces: Army of the United States, Australian Imperial Forces, Australian Military Forces, Australian Women's Auxiliary Service, British Army, Canadian Military Forces, Royal Air Force, Royal Australian Air Force, Royal Australian Navy, Royal Navy, United States Women's Army Corps, Women's Auxiliary Australian Air Force, United States Army. The United States Navy was not included.

In order to avoid duplication, promote smooth inter-service relationships, and assure the maximum benefit from the pooling of resources and centralizing of control, representatives of each of the 14 component services were detailed to work on all of the major problems. Personnel were placed where they could work most effectively regardless of nationality or the component to which they belonged. Before the war came to an end the personnel strength of Central Bureau was more than 4000 and there were detachments in all parts of the Southwest Pacific Area. Of this number about fifty per cent were American personnel.

Since the work of Central Bureau was always closely connected with GHQ, the organization followed General MacArthur as he moved northward. This took the headquarters of Central Bureau from Melbourne to Brisbane (September 1942), to Hollandia (late summer 1944), to Leyte (October 1944), to San Miguel (Luzon) (May 1945), and to Tokyo (September 1945). The first move came in September 1942, when GHQ was moved to Brisbane. In Brisbane the administrative control of the American contingent passed (February 1943) to USAFFE. Operational control, however, remained with GHQ throughout the war.

In November 1945, its mission accomplished and a fine record of cooperative effort and notable achievement to its credit, Central Bureau was deactivated. General MacArthur commended the organization for its outstanding achievements and awarded the Legion of Merit to ten of its members.

From SRH 280. *This intercepted message from the Japanese Ambassador to Nazi Germany, Baron Oshima, contains useful technical information from inside the Third Reich, including data on German experiments with jet planes and rocket bombs. The Goebbels referred to was Joseph Goebbels, the infamous Nazi propaganda minister.*

From: Berlin (Oshima)
To: Tokyo
26 July 1944 #756
A 4 part message complete.

Urgent.

In recent statements made by GOEBBELS as well as some that appeared in the German newspapers and magazines, it is frankly admitted in their explanation of the European war situation that German weapons have to yield the palm to the enemy in both quality and quantity. However, at present the Germans are striving to improve the quality and increase the quantity of their weapons, and there are not a few people who say that in time Germany will be able to make up for her present technical inferiority [a]. . . .The Military and Naval Attaches have doubtless sent you detailed reports regarding this matter, but as I thought it would be necessary in order to get an estimate of the war situation in general, I am sending you merely the following outline regarding the new German weapons. Moreover, although quite a number of announcements have been made already with regard to this subject, since there are some very important matters in this message relating to military affairs, I wish you would treat this message with particular care.

1. Weapons connected with the Army:

(a) Tanks: I have already sent you information regarding the Tiger and Panther Tanks, but it seems that they are placing especial emphasis on the production of Panthers in large quantities.

(b) Assault Guns: This gun is primarily a weapon to be used for the smashing of the enemy's pillbox machine gun bases in cooperation with the Infantry, but it is often used also in anti-tank warfare. This is one of the weapons concerning which the Germans are placing great emphasis at present so far as production in large quantity is concerned. It is an 88 millimeter gun (the same as the gun on the Tiger) and has a crew of four men.

Part 2.

(c) The Panther Terror:[b] This is a kind of rocket gun that can be used by two soldiers, and is a weapon for close-range fighting to be used against tanks.

(d) The Panzer Fist:[c] This is the same kind of gun as the above, but it can be used by one person.

(e) Trench Mortars:[d] These weapons could hardly be called a new weapon today, but their size has been increased (up to 15 centimeters) and they are being used in large quantity.

(f) Robot Tanks (Goliath):[e] This is a small-type tank controlled by radio waves, and it seems that its effectiveness depends on the configuration of the ground.

(g) The establishing of artillery divisions with the self-propelled gun units acting as the main strength: The object of such a division is to concentrate the use of artillery.

I wish that in paragraph (c) above you would amend the words Panther Terror

to read Panzer Terror.

2. Weapons connected with the Navy:

(a) A New Type Submarine (Very Secret): This new type submarine scarcely shows itself on the surface of the sea, and has long-range maneuverability. At present it is in process of construction and its effect will first be felt from about September, and by November or December it is said that greater results will be effected by its use in great quantity.

Part 3.

(b) Torpedo Boats: I have nothing to add to what I have already reported to you concerning these boats.

(c) A Small-type Submarine (Very Secret): This is a submarine that has been improved one degree and seems to be a weapon that has two torpedoes to be ridden by one man. It is to be used in areas near the seashore.

(d) Special Torpedo (Very Secret): This is a torpedo which by means of special equipment has been made almost 100% effective in hitting the mark, and its testing has already been completed.

(e) The High Speed Boat:[f] This in itself is really not a new weapon, but a new type is being produced with a speed of 40 knots an hour, and having a Diesel engine. For this reason it has the special merit of not easily catching fire when damaged. It seems that the Germans are putting forth efforts to produce this boat in large quantity.

(f) Special High Speed Boat (Very Secret): This is a high speed boat to which has been added the principle of radio wave control, and it seems that its explosive power is especially great.

3. Weapons connected with the Air Force:

(a) The German are adding substantial improvements to the speed, armament, ammunition, and way the armor is put on, etc., in their various types of fighter and destroyer[g] planes, and besides that they are of course placing special importance upon the production of these planes in great quantity. Furthermore, in the near future propellerless planes are also going to make their appearance, and it seems that these planes will have especially high speed (this last paragraph is very secret).

(b) For the time being dive bombing has been suspended and as a substitute they are using ground attack planes (SCHLACHT FLIEGER). These planes cooperate with ground fighting, and considerable results have already been achieved in the destruction of enemy tanks (Captain RUUDERU alone, it has been announced, has destroyed more than 200 tanks).

Part 4.

(c) The main strenth of anti-aircraft guns lies in the 88 and 105 millimeter guns, it seems. However, 120 and 150 millimeter guns also are gradually being used in large quantity. Matching the improvement in shells the Germans are trying also to increase the power in their aircraft. Again it seems they are also using rocket guns.

(d) There has been a great deal of improvement in night fighters since last winter but in day-light air raids also special units, STORM GRUPPE, have recently been organized (within 2 minutes 1 American four-motored plane—10G— and —M—). They will at an appropriate time be newly established and although it may not be possible to call them new weapons, in outline they serve as an indication of the earnest efforts which Germany is puting forth in order to regain command of the air.

(e) Special Type Aircraft (Very Secret): It seems that a study is now being made with regard also to a bomber plane which will unite the rocket gun with the principle of radio wave operation.

4. Equipment for Long Distance Bombardment (Very Secret): I have already described to you in various telegrams the V-1, and it seems that preparations have already been made for the use of a more effective weapon than this. It will have five times the effect of the weapons thus used in the past. And again it is said that they will have a weapon whose effect will extend to a square of more than 1 kilometer. However, it is not clear as yet just when both these weapons will be introduced. It is anticipated that with regard to these weapons there will be both substantial developments and improvements made in their construction.

5. The weapons in which the Anglo-Americans made particularly great progress in the past were first of all the direction finder and then radio wave weapons in general, but in both these spheres the Germans by special efforts seem gradually to be catching up with the enemy. It seems that in weapons connected with rockets, because of the fact that the Germans as usual have had longer experience, Germany is temporarily in the lead. Again improvements and progress in explosives have been best indicated in the V-1 and it seems that this improvement has been very conspicuous.

a - V.H. 1891.
b - SCHRECK.
c - The Kana spelling for this word is HUAASUTO, which is doubtless the German word for FAUST.
d - WERFER.
e - The Kana spelling for this word is GORIAATO.
f - SCHNELL BOTE.
g - ZERSTOERER.

Inter 28 Jul 44 (1) Japanese
Rec'd 29 Jul 44
Trans 31 Jul 44 (1227-A)

CHAPTER VI

Producing Intelligence

The decryption of encoded and enciphered enemy traffic was only the beginnings of the signals intelligence process. The messages had to be placed into a wider intelligence context. Until June 1944, when there was a general reorganization of the whole War Department intelligence structure, this was done by the members of the Special Branch, Military Intelligence Service. In the excerpts from SRH 185, War Experiences of Alfred McCormack, the father of the Special Branch gives an insider's account of the infighting that went on within War Department intelligence. Unlike most of the other Special Research Histories released by the National Security Agency, this document was originally prepared after the war as an unclassifed study; the reader will note that McCormack does not mention that the Special Branch dealt with signals intelligence.

The Special Branch not only exploited U.S. Army successes against Japanese diplomatic and later military communications, but also entered into an agreement to share signals intelligence with the British. As a result, after 1943, the United States was able to secure from the British the results of their unparalleled success in reading high-level German messages. See the excerpt from SRH 141-2. The type of intelligence windfall that resulted from this source is documented in the excerpt from SRH 005, Use of MX/CSS ULTRA by the War Department.

From SRH *185. In these excerpts from his unpublished memoirs, McCormack tells all about the Special Branch—except what it actually did! "Cravath methods" refer to the highly selective and personalized recruitment procedures used by his old law firm. At the time he wrote this account, McCormack had returned to a successful law practice. After reentering civilian life in 1945, he had briefly served as the State Department's first Director of Intelligence and Research. However, he apparently encountered the same kinds of bureaucratic resistance to intelligence work at the State Department as he tells us he met in the War Department.*

31 July 1947

WAR EXPERIENCE OF ALFRED McCORMACK

Early in January 1942, McCormack was asked by McCloy to do a job in the War Department in connection with military intelligence, and he took office on January 19 as a Special Assistant to the Secretary of War. In March he submitted his recommendations to the Secretary and was given the job of putting them into effect. A special section was created by G-2 to assist in the work, and in May 1942, Colonel (later Brig. General) Carter W. Clarke, with whom McCormack had become acquainted and whom he strongly recommended, was made head of that section.

Urged by the Assistant Chief of Staff G-2, General Strong, to go into the Army, McCormack at first declined but later concluded that his job could be done more effectively if he were an officer on the G-2 staff. He was commissioned as a Colonel on June 24, 1942, reversing roles with Clarke, who thereupon became Chief of a newly created "Special Branch" of G-2, with McCormack as Deputy Chief.

From then until the end of the war McCormack and Clarke, whose talents were complementary, worked as a team. McCormack took charge of the research and intelligence work and the recruiting and training of personnel, while Clarke concerned himself with administration, security, relations with G-2 and outside organizations and innumerable problems involved in organizing and building up units of the Army whose work produced the raw materials of intelligence, and for which Clarke assumed a continually increasing responsibility as the war progressed. Clarke was also employed on a number of important missions for the War Department Staff.

Both Clarke and McCormack considered G-2, as it existed in 1942, to be inadequate for the intelligence job that the war required, and they sought to use the Special Branch as a means of building up a more effective intelligence organization in the War Department.

The original assignment of Special Branch was the preparation of a daily intelligence report, but the work which that entailed provided many opportunities for

the production of useful intelligence, which the personnel of the Branch were quick to grasp. In August, 1942, McCormack, having established the form of the report and the methods to be used in the preparation, turned over the work to Henry W. Rigby, who had been a Cravath associate from 1937 to 1939, before going to the Providence firm of Tillinghast, Collins, & Tanner, and who had followed McCormack into the War Department in March 1942. Rigby's immediate assistant until August, 1944, was a Cravath associate, Louis T. Stone, Jr. . . .

McCormack used "Cravath methods" in the recruiting of personnel for the Special Branch, taking on only highly qualified persons. There were so many lawyers in the Special Branch that it used to be referred to humorously as "the best law office in Washington". McCormack believed, and his experience confirmed, that lawyers as a class are better fitted for intelligence work of the type that must be done in the War Department, i.e., what the Army calls "strategic intelligence", than is any other group in the community, because their training teaches them to deal with evidence, to be inquisitive and skeptical, to pursue an investigation through to a conclusion, to meet unfamiliar situations of fact and, most important, to do very detailed work without losing their sense of values.

After freeing himself from responsibility for daily reporting, McCormack turned his attention to specific problems of intelligence, being convinced that intensive and exhaustive research work would furnish dependable answers to many questions on which G-2 at the time could do no better than speculate. Every job that was done revealed new opportunities and emphasized the need for more personnel, and the results were good enough so that the personnel allotments were provided, though usually after long delays and much paper work. McCloy had an active interest in intelligence, followed the work of the Special Branch and helped out frequently; and the fight for personnel was made easier by high praise which the Branch received from time to time from General Marshall and other high officials, and occasionally from the President.

By the Fall of 1942 it was apparent to McCormack, and also to Clark, that G-2 had no dependable current information about the war in Europe. The reason was a simple one, but nobody seemed to realize it. There was a military attache in London with a large staff. He sent reams of paper back to Washington, which he had gathered from the British intelligence agencies; but the British did not regard military attaches as being entitled to top level information and so what the attache office sent home was seldom more than could be published in the newspapers. It was solemnly studied in G-2, though there was in the organization an almost universal suspicion of the British and a tendency to disagree with British conclusions, simply because they were British conclusions. Some of the G-2 "intelligence" on Europe was fantastic. For instance, at a time when the German Air Force had about 5,000 operational planes of all categories, there were devout believers in G-2 in a rumor picked up by an attache in Roumania that the Germans had 10,000 spare airplanes hidden in the Black Forest.

One of the bothersome characteristics of G-2 was a certain supine attitude toward intelligence. Everybody knew the classical Army doctrine that the three steps in intelligence are collecting, evaluating and disseminating, but nobody seemed to give much thought to the fact that evaluation and dissemination are worthless if what is collected is worthless. The attitude was in part a reflection of the viewpoint of the G-2 colonels, who regarded it as their function to make predictions. They operated in the manner of soothsayers. They showed no indication that their information might be inadequate. They seemed to think that they already knew enough to answer whatever questions might be put to them concerning the enemy countries.

G-2 organization as a whole did not appear to know that there was a war on. Except for the fact that they were required by departmental order to work on Saturdays and that some of them had to appear Sunday morning for a meeting with the General, they operated their organizations just as they had in peace time. Promptly on the dot of 5 p.m. the whole organization went home. There was no special sense of hurry or urgency and the job that did not get done one day would go over to the next unless the job had a deadline. If the job had a deadline, it was turned out on that deadline and it was good or bad, depending on whether the time was sufficient to get the job done.

The Special Branch had a different attitude toward hours. Every day's work had to be done that day and if it was not done by 5 p.m. the personnel stayed on and finished it. The Branch was hardly ever closed before 11 p.m., and it opened very early in the morning because Clarke's hour of arrival was never later than 7 a.m. and he not infrequently got in at 6. McCormack never went home before 7 and worked at night whenever there was any reason to do so.

McCormack had an early experience which he never forgot. At 4:40 one afternoon he went to the Chief of the European Branch of G-2 to get some information. The campaign in North Africa was then under way and the information, though not of any vital significance, was pertinent to a job that might have been useful in connection with that campaign. The Colonel apologized for not being able to get the information until the following morning. It was a fixed rule of his branch, he said, that all personnel must start putting their papers away by 4:40 p.m., in order that their desks might be clear and might be inspected and the files locked by 5.

In the two years of life of the Special Branch it grew in size from a dozen officers and civilians to a total of 100 officers and 300 civilians and enlisted personnel in Washington, and 80 officers abroad, stationed with the field commands and at other key places, and it had been given a directing responsibility for the work of Army units outside of Washington numbering several thousands of persons.

McCormack's work in early 1943 had to do largely with the war in Europe. At that time the relations between the War Department and British intelligence organizations were conducted at the top level; there was no working liaison and no important flow of the raw materials of intelligence from the British organizations

to the War Department. In April, McCormack was sent to England as the representative of the Assistant Chief of Staff G-2, to work out arrangements that would insure that the American field commands would be furnished promptly with all relevant British intelligence, and that the War Department would have access to British intelligence in all its aspects.

McCormack spent two months making a study of the British Intelligence agencies and reporting his findings to Washington, with recommendations for methods of coordinating British and American intelligence work on the European war. He was greatly impressed by the work of the British intelligence agencies and the high quality of their personnel, and he learned many lessons from them which he applied later in G-2. He found that British intelligence had a first call on military and civilian personnel—a startling contrast to the United States, where intelligence had in general a low priority for personnel or no priority at all.

McCormack and Lt. Col. (later Colonel) Telford Taylor, . . .who had accompanied him to England, worked out with the British a plan for coordinating British and American intelligence work for the German war and it was gradually put into effect as personnel were obtained. It involved establishing a unit of the Special Branch in England, headed by Colonel Taylor, converting certain British intelligence units into joint British-American units, and creating a new system of communications for the transmission of operational intelligence to American commanders.

* * *

On his return from England in June, 1943 McCormack set up a new unit under Capt. (later Lt. Col.) William R. Perdue of the Cahill, Gordon firm and Lt. (later Major) John W. O'Boyle, a Milwaukee lawyer, who had served as Judge Patterson's law clerk in the Circuit Court of Appeals and, before going into the Army, had held a number of important assignments in the Lend-Lease Administration.

The purpose of the unit was to exploit Japanese intelligence material with primary attention to the Japanese merchant marine.

No two intelligence organizations among the Allies could agree at that time on the amount of Japanese shipping at the start of the war or the amount of tonnage that had been sunk, and there were estimates of Japan's shipping position that varied by millions of tons. Clarke and McCormack were agreed that the Japanese merchant fleet was the primary military objective in the Pacific War and that the employment of that fleet was the best clue to the logistic problems of Japan and to her economic situation and military capabilities. Seeing an opportunity to do an important intelligence job in that field they requested, and after some months of delay obtained, 55 officers and 22 enlisted WAC's for the Perdue-O'Boyle unit.

The job was complicated by language problems. Not only was much of the intelligence material in Japanese, but the pre-war ship lists were a riddle because

the Japanese had an annoying habit of giving the same name to a number of ships (42 ships in one instance) and an equally annoying habit of rendering a single ship name into the kana syllabary in several different ways. Experts in the Japanese language were needed, and there was a great shortage of them. Again applying "Cravath methods", McCormack persuaded Harvard to release Professor Edwin O. Reischauer, its Director of Japanese Studies, and with Reischauer's assistance recruited the best staff of Japanese linguists in Washington.

The intelligence work on the Japanese merchant marine, which later became a joint Army-Navy operation under McCormack's supervision, was slow in getting under way, because of the perpetual difficulty of getting personnel;, but it proved to be exceptionally successful and contributed largely to the effectiveness of the submarine war against Japan. The United States Strategic Bombing Survey found, when they went to Japan after the war, that the information on Japanese shipping that Washington had had during the last year of the war was far more detailed and accurate than anything that could have been put together in Tokyo at the same time. From 1943 to 1945, McCormack was a member of the Joint Army-Navy Assessment Committee, which had the responsibility of determining enemy shipping losses.

The intelligence work on the Japanese merchant marine led into many other important subjects of Japanese intelligence. Techniques established in that work became applicable to other intelligence problems affecting Japan; and the application of those techniques accounted in large measure for the gradually increasing accuracy of American intelligence on the Japanese military and economic situation.

The work led, almost necessarily, into work in the Japanese Order of Battle unit and a group was set up to do that work paralleling the work of the regular Japanese Order of Battle unit of G-2 and dividing the responsibility with it.

The Special Branch reported directly to the A. C. of S. G-2, while the other intelligence units of G-2 were one echelon lower, under the Chief of the Military Intelligence Service. With some exceptions, they were organized on a geographic basis, and the geographical sub-sections had become highly compartmentalized. The Special Branch and the Order of Battle were strictly war products and confined their attention to intelligence that was relevant to the war, and mainly to intelligence of combat significance. The Geographical Branches, on the other hand, had taken their form and acquired their habits in peacetime. They attempted to cover the whole world of intelligence; and their contact with combat intelligence was often rather remote.

In the upper echelons of G-2 there were some able officers, but most of the regular ones knew that their futures depended on their getting assignments in the field, and of those who were willing to remain, because they realized the importance of good intelligence work, many became discouraged and obtained overseas jobs. Their replacements were often men with no better qualifications than that their shoulder insignia fitted the job; and thus from 1942 to 1944 a law of natural

selection worked against G-2 adversely.

The discouragements that made able officers get out of G-2 were numerous. There was a lack of imaginative leadership on the "Colonel" level. There were jealousies and political fights within the organization. There was an undue emphasis on rank and an attitude of unwillingness to give responsibility and credit to subordinates. There was a certain feeling of remoteness from the war. But the greatest discouragement of all was the inability of able officers to get qualified personnel, and in a sufficient number, to do their jobs.

Difficulties in getting personnel were partly due to a lack of recognition of the personnel needs of intelligence, and even a lack of appreciation of the importance of intelligence, on the part of the War Department General Staff; partly to the politically motivated drive to keep the number of officers in Washington to a minimum; partly to the Army's heavy-hand methods of handling personnel and partly to the stupidity of the Civil Service organization.

Though intelligence work requires a higher order of ability, War Department intelligence had practically no personnel priorities until McCormack got some priorities established in 1944. Moreover, intelligence personnel were subject to sweeping orders from above, which came unannounced from above and invariably caused trouble. In one of his early efforts to get civilian personnel, McCormack and his staff had interviewed dozens of people and had selected some 15 or 20 highly qualified ones. These were put through the long process of security clearance and Civil Service approval. Then, just as the clearances and approvals began to come through, a "personnel freeze" for the War Department General Staff was announced. No more persons could be hired until further notice. By the time the freeze was lifted practically all of the candidates (their security having been cleared and their Civil Service status established) had taken jobs with other agencies, and the recruiting of personnel for the vacant jobs had to be started anew.

The civilian agencies of government were hiring personnel at somewhat inflated salary scales, and under war-time conditions highly qualified persons could not be drawn from useful jobs in private life unless they were paid enough of a salary to support their families. But the G-2 salaries were very low. They were paid with one eye on the base pay scale of officers, and officers found it difficult to understand why a competent economist had to be paid $8,000, the base pay of a Brigadier-General. When McCormack went into G-2, the highest paid civilian in the Europe-Africa Branch of G-2 got $3,600 per year as salary. He was the "expert" in German economics; and it was only to be expected that he would be—as he was—unqualified for the job.

The recruiting of officers was very difficult. They had to be of ranks that fitted into a Manning Table. They could not be taken from either combat units or specialized schools. The Army had no OCS for intelligence personnel. Much of the work in McCormack's unit was young men's work, requiring much enthusiasm, long hours, and great physical and mental energy. So he tried to find bright young offi-

cers, and did find some very good ones. Then came an order forbidding the assignment in Washington of any more officers under 28 years of age, and somewhat later an order requiring all officers under 28 to be sent to the field.

Enlisted personnel were not permitted in G-2, except for a number of men who served as guards at night and in similar jobs. To get an enlisted man it was necessary to have him commissioned; and McCormack was able to get that done in a few cases, but it was a difficult and time-consuming job.

The most maddening difficulties came from the Civil Service, which could not understand why the war should interfere with its time-worn procedures. If G-2 wanted to hire an indexer, it was necessary to prove to Civil Service, not only that the candidate was qualified, but that an indexer was really needed. Thus Civil Service examiners, many of whom were incapable of understanding what G-2 was doing or what its problems were, quite often turned down an application on the ground that the work was not necessary.

* * *

Major General George B. Strong, the Assistant Chief of Staff G-2, attempted to give G-2 a vigorous and progressive administration. He encouraged and helped the Special Branch, and he recognized Colonel Lovell's work by creating an Order of Battle Branch with Lovell as Chief and centering in it all work on enemy Order of Battle. He encouraged another Branch of G-2 which proved to be of great value in the war—the Topographic Branch, headed by Colonel S. P. Poole, a geographer from the University of Rochester.

But General Strong was in failing health and was habituated to a system in which an officer must accomplish his results with the personnel given to him—an attitude that prevented him from seeing that what was needed in G-2 was a thorough shaking up. As one junior officer put it, the quickest way to reform G-2 was to kill off all officers above the rank of Major, and to throw in half of the Majors for good measure.

The career of the Special Branch was largely shaped by the deficiencies of G-2, in that it had to take on job after job that G-2 should have been doing but was not doing. McCormack discovered, even before he went into the Army, that G-2 had no biographical files for identification of foreign individuals. He proposed to the G-2 Chief of Intelligence that the latter set up a central name file, in which there would be assembled all information about persons figuring in G-2 intelligence material and for which a group of research workers would gather additional material from biographical sources. After some months, having got no action from G-2, McCormack decided to set up such files himself.

He assigned a very competent woman. . .to do the job and, being unable at first to give her any assistants, gave her instead a call on the free time of stenographers. The unit grew steadily, as it proved the importance of foreign biographical infor-

mation. By 1944 it had become the "Who's Who" branch, with a staff of over 180 persons, headed by Lt. Col. Edward C. Lapping, now Managing Editor of the Chicago Herald-American, and it had become a primary source of information about foreign individuals, serving not only the War Department but all other governmental agencies requiring such information.

McCormack tried to keep the Special Branch a flexible organization, so that, if a job of pressing importance came along, as many of the staff as were needed could be thrown into it. The G-2 organization, on the other hand, was rigidly organized along lines of command, down to the highly compartmentalized geographical "desks", and there was no flow of personnel from one "desk" to another to meet emergencies.

Late in 1943 Colonel Moses W. Pettigrew, Chief of the Far Eastern Branch, whom McCormack considers to be the ablest American intelligence officer on Japanese matters, was working up a Japanese Order of Battle, with the assistance of an able younger officer, Lt. Col. (later Colonel) Eric H. H. Svensson and a woefuly inadequate staff. Colonel Pettigrew had to do most of his work at night, as during the day his time was consumed in the administration of a cumbersome organization, in routine assignments from his superiors, and in a largely fruitless effort to get competent personnel. In spite of the handicaps, Colonel Pettigrew laid the foundations for work on the Japanese Order of Battle and was the Army's leading expert on the Japanese Army. . . .

An experience of Colonel Pettigrew's illustrates the difficulties that the able G-2 officers had to contend with. While he was building up his Order of Battle, a priceless intelligence document was captured and was translated in Australia—a Japanese Army Officer List of comparatively recent date. Here, if the list could be carded and the cards kept up to date with all information coming in about Japanese Army officers, was an extremely useful tool for Order of Battle intelligence. Pettigrew applied for personnel to do the job—two Japanese linguists and 6 typists. The application was turned down. Out of the hundreds of persons in G-2, no one could be spared for Pettigrew's job.

Pettigrew appealed to McCormack, who saw the importance of the job and said he would get it done somehow. . . .

* * *

Early in 1944 the work of the Special Branch had grown and developed to a point where a much larger staff was required to take advantage of the intelligence opportunities that were clearly there. The personnel authorities, however, had set an overall ceiling on G-2 personnel in Washington, and it was ruled that no future additions of personnel for the Special Branch could be made except by transfer of jobs from the rest of G-2. There were so many vested interests in G-2 that the war would be over before any considerable number of persons could be obtained that

way; and so it looked as if many promising opportunities in intelligence opportunities would have to be passed up.

It was Clarke who at that point came to the rescue with a bright idea, as he often did. After all, it was Secretary Stimson who had brought McCormack to Washington and given him a job to do in intelligence. Two years had passed and the Secretary had not yet asked McCormack how he was coming along. It was high time for the Secretary to ask that question, and no doubt he would ask it if he learned that McCormack was in trouble. Clarke was right. The Secretary requested General Strong (who had requested him so to request) to have McCormack prepare a full report. McCormack did so, accompanying it with an urgent application for an increase of officers from 100 to 400 and of civilian personnel from 300 to some 800, plus certain additions to personnel abroad.

The result was appointment of a War Department Board to pass on the application. It consisted of McCloy, the Deputy Chief of Staff (General McNarney) and a number of other general officers.

The Board heard evidence and argument and found that the personnel applied for could be profitably used. It granted the requested increase in the T/O, but it limited the addition of new officers to 100 pending an investigation of the entire G-2 organization, to determine what compensating personnel reductions could be made in other units. An investigation of G-2 by an Inspector General's Board was then ordered, and Clarke and McCormack spent several weeks explaining their organization and plans to the Board members. The Inspector General's investigation resulted in recommendations which summed up to an abolition of the geographical organization of G-2 and the merger of those units and the Order of Battle Branch into the Special Branch.

A new Board was then convened for the purpose of devising a suitable plan for the reorganization of G-2. The plan was adopted on or about April 1, 1944 and a new Assistant Chief of Staff, G-2, Major General Clayton Bissell, was directed to put it into effect.

General Bissell thereupon appointed a Reorganization Committee to translate the plan into specific terms and promptly departed for a trip abroad, directing the Committee to have its recommendations ready on his return. The members of the Committee were either old-line G-2 officers or officers whom General Bissell brought in from the outside, most of them having no experience in intelligence.

The plan of reorganization divided G-2 into a Policy Staff to advise the G-2 on weighty matters and the Military Intelligence Service to do the intelligence work. The Military Intelligence Service was in turn divided into a Director of Administration (to run the service organization), a Director of Information (to take charge of procurement of information and to run a variety of units engaged in that activity) and a Director of Intelligence to do the intelligence work and to provide intelligence for the War Department and the commands abroad.

Under the Director of Intelligence there were to be a group of Area Specialists

without staffs, a Research Unit and a Reports Unit. The bulk of the organization was to be in the Research Unit, which was to be divided into the following Branches: Military, Political, Economic, Sociological, Topographic, Scientific, Who's Who and Library.

The Reorganization Committee was dominated by the old-line prejudice toward the Special Branch and made it a primary objective of their plan to ensure that the Special Branch would be broken up—"and good". The plan distributed its personnel and functions among 53 separate branches, sections and sub-sections, and the literal provisions of the plan would also have destroyed its work. The key position in the new organization was that of Director of Intelligence, and a strenuous attempt was made to find a suitable regular officer for the post.

The attempt was not successful and, largely through the efforts of Clarke, McCormack was appointed to the post. Clarke was appointed Deputy Chief of the Military Intelligence Service. Brigadier General Russ Osman, Regular Army officer, was appointed as Chief. General Osmun, who belonged to the Quartermaster Corps, was replaced some months later by Brig. General Paul E. Peabody, who had returned from service as Military Attache' in London. General Peabody gave Clarke and McCormack the fullest support and did much to help them get their jobs done.

The reorganization was gradually put into effect in June, 1944, and it attained some newspaper fame by reason of the fact that the Sections doing German intelligence were moving their offices, and were without telephone connections, on the day of the Normandy invasion. That was of a piece with the rest of the Reorganization Committee's work. It set up about as impracticable a scheme of organization as could be devised. It apportioned responsibilities among the 3 units under the Director of Intelligence in a manner calculated to render all three useless. It put into key positions a number of officers without a shadow of qualifications. All McCormack's subordinates, down to the Branch Chiefs, were chosen for him and without consultation with him, and the personnel were distributed among the Branches according to the fancies of the Committee.

McCormack tackled his new job with a determination to weed out all misfits and put every job in the hands of a person, officer or civilian, clearly qualified to do it. He started out on the day when he took office by demanding the removal of the Acting Supervisor of Reports, on the ground that he was incompetent and dangerous. With the support of Clarke, and by submitting his resignation in writing, McCormack got the officer removed before he had taken office.

Then followed 4 months of agonizing efforts to make an organization out of the formless thing which the Committee had set up.

* * *

From SRH 141-2. *This excerpt from another McCormack memorandum—again, dealing with personnel—discusses the background of the 1943 British-War Department agreement that at last let the U.S. Army in on the ULTRA secret.*

23 October 1943.

MEMORANDUM FOR MR. McCLOY (Through GENERAL STRONG):
Subject: Personnel Situation of
Special Branch, M.I.D.

* * *

30. *German "E"*. The most important development affecting the Special Branch, since April, has been the opening up of the German "E" traffic. This has been the No. 1 source of military intelligence during the present war, from early 1940 to date. The achievement of the British in this field has been without question the greatest feat in the history of cryptanalysis, and the preservation and increasingly successful exploitation of this source for three and a half years has been an amazing achievement in security.

31. From the latter part of 1942 until May 1943, a controversy existed between the War Department and the British GC & CS, as a result of the refusal of the British to make this traffic available to the War Department in any way, and their unwillingness to consent to Arlington Hall's entering the "E" field. An agreement between the War Department and the GC & CS was worked out by General Strong in May, pursuant to which this source of intelligence was to be opened up. The agreement called for (a) establishment of an American cryptanalytic unit in England, to work on "E" in cooperation with the British, (b) assignment to Arlington Hall of a research job in the "E" field and (c) opening up of the traffic itself to the War department through liaison officers in England and the Special Branch in Washington.

32. Because of the great risks involved in the dissemination of intelligence from "E" sources, and the necessity of satisfying the British that our security arrangements are adequate—and the necessity also of persuading them to agree to our wishes as to what "E" intelligence should be transmitted to Washington—it took from May to the end of August to work out details of the arrangements with the GC & CS in the "E" field. These call for 4 officers to sit on shifts in the so-called "Watch Room" at B.P., where the material comes in from the cryptanalysts and is emended, translated and disseminated (a) in original form to the Service Ministries by teletype (b) in the form of informational messages to commanders abroad and (c) in memoranda for the Ministries which gather up and present the

information that is not of sufficient importance or urgency to go through channels (a) and (b).

33. In addition, one liaison officer is to sit in the War Office, at the point where "E" intelligence comes from B.P., and is put together with other intelligence into "appreciations" for the War Office and commanders abroad. This officer (who is being taken from another liaison assignment with the War Office) is to advise our liaison officers at B.P. what additional or explanatory material should be sent to Washington.

34. Attention is called to the fact that, under this arrangement, the War Department gets, for the first time, a basis for arriving at an independent judgement on British intelligence from "E" sources, which is the major part of British intelligence about the German Army and Air Force. Heretofore we have depended largely on the inferences and conclusions drawn by the British, and have had no means of checking their basis. We have been in the same position as those organizations and individuals within the British Government who are not "in the know," i.e., the MS information has been either withheld or transmitted to us late, for security reasons; or it has been given in general terms and in round numbers; and often it has been impossible to distinguish between 100% verified information and inferences which, upon examination of the evidence, might turn out to be mere guesses.

35. Under this arrangement we need no longer speculate about how much intelligence the British are giving us from their primary source. We now sit at the source itself and can watch it; or rather, we will be able to watch it when we get the necessary component of officers at B.P.

36. The British Security channel to Washington is used for sending the "E" messages and paraphrases here, and gives us direct and speedy access to the intelligence derived from "E" and related cryptanalytic activities. The nature and importance of this intelligence can be dealt with orally, and specimens of it can be furnished. Because of the unique security problem involved, it is undesirable to deal with them in a memorandum.

37. The above arrangement also gives American officers a part in the determination of what "E" intelligence shall be sent to American field commanders. The dissemination of "E" intelligence to the field is controlled at B.P., where representatives of the 3 Service Ministries decide what their respective commanders should get, and in the past they have decided this for American commanders, without any American representative having a vote. Under the new arrangements our liaison officers at B.P. will be in a position to insist that "E" information that is sent, for example, to General Montgomery is also sent to General Clark, if it might have a bearing on his operations; and if the decision is adverse they can take the matter up through the appropriate channels.

38. We agreed with the British to keep Lt. Col. Taylor's staff for the "E" operation at B.P. to the minimum necessary to do the job; and the British have agreed with us that the minimum is 4 first-class officers at B.P. We now have one officer on duty, and Lt. Col. Taylor is temporarily spending most of his time at the same

work. One other officer has been assigned to the job, and will go as soon as orders and transportation can be obtained for him. Efforts are being made to find 2 others, properly qualified for the job. The liaison officer at the War Office has already been selected and will start working in the near future.

39. Factors bearing on the determination of what reserves of manpower should be built up for the job at B.P. are (a) the desirability of rotating the officers and (b) that, when and if the need arises for American forces on a cross-channel or other operation to have special security officers to handle "E" intelligence for the commanders, they will have to be men trained at B.P. and the Special Branch officers will be likely candidates.

* * *

From SRH 005. *Excerpts from the Military Intelligence Service's European Summary of April 11, 1945 demonstrate the quality of intelligence about German capabilities and intentions that could be derived from ULTRA.*

EUROPEAN SUMMARY OF 11 APRIL 1945

No. 45-101 Copy No._
By Auth.

NOTE: No one, without express permission from the proper authorities, may disseminate the information reported in this Summary or communicate it to any other person.

Those authorized to disseminate such information must employ only the most secure means, must take every precaution to avoid compromising the source, and must limit dissemination to the minimum number of secure and responsible persons who need the information in order to discharge their duties.

No action is to be taken on information herein reported, regardless of temporary advantage, if such action might have the effect of revealing the existence of the source to the enemy.

The enemy knows that we attempt to exploit these sources. He does not know, and must not be permitted to learn, either the degree of our success or the particular sources with which we have been successful.

1. *Western Front*:

a. *Reorganization of Armed Forces chain of command*: An order issued by Hitler late on 7 April made sweeping changes in the organization of the chain of command in the West. Operational control of the Front is now divided between C-in-C West and "C-in-C Northwest," command of the forces in the Ruhr pocket is separated under Army Group "B," and those HQs, plus Naval Chief Command West, are subordinated directly to the OKW. In addition, a new command, "C-in-C

Netherlands," has been set up in preparation for "the defense of Fortress Holland."

Hitler's order prescribed the boundary between C-in-Cs West and Northwest as a line running eastward from Paderborn to Schoenebeck (7 m. SE of Magdeburg).

Details of the reorganization directed by the order are in substance as follows:

(1) *Subordinated directly to the OKW*

(a) "C-in-C Northwest (Army Group 'H')"

(b) Army Group "B"

(c) C-in-C West

(d) Naval Chief Command West

(2) *Subordinated to C-in-C Northwest*:

(a) "The former sphere of command of Operations Staff North Coast," the staff of which is made available to C-in-C Northwest.

(b) "C-in-C Netherlands, to whom the Twenty-fifth Army, Commander Armed Forces Netherlands, Admiral Netherlands, and GAF forces in Holland are subordinated." C-in-C Netherlands "is personally responsible to Hitler for the defense of Fortress Holland; as soon as land communications to the Reich are cut, the (previously announced) comprehensive regulations regarding Fortresses will govern his relations with the Reich Commissar for Occupied Areas of the Netherlands."

(c) Armeegruppe Student

(d) First Parachute Army

(e) Wehrkreis XI

(3) Subordinated to C-in-C West:

(a) Army Group "G" (with the First and Seventh Armies)

(b) Eleventh Army

(c) Nineteenth Army

(d) Wehrkreise V, VII, IX, and XIII.

(4) Subordinated to Army Group "B":

(a) Fifth Panzer Army

(b) "Fifteenth Army (Armee Abt. von Luettwitz)"

(c) All other units and personnel of all branches of the Armed Forces in the Army Group area (Ruhr pocket).

(5) GAF tactical forces: The organization of GAF tactical forces employed in the West is to conform to the organization of the field army. A GAF command staff is to be linked with each of the ground commands (presumably Luftflotte Reich in the north and GAF Command West in the south. . .).In addition, all flying and Flak units supporting the field army are to be subordinated operationally to C-in-Cs Northwest and West respectively.

GAF support of Army Group "B" will be arranged specially. b. Location of HQs following the command reorganization:

(1) C-in-C West moves southeast: On 28 March the HQ of C-in-C West was in a tunnel at Milseburg, 10 m. E of Fulda. . . .The next day Genobst. Jodl,

Chief of the OKW Operations Staff, stated that the area west of Ohrdruf (9 m. S of Gotha) was envisaged as an HQ location for C-in-C West "in case of need". . . .On 10 April, the following message was sent by an unidentified authority:

"As of 0800 hrs on the 10th, the temporary battle HQ of C-in-C West is in Hirschau (40 m. E of Nuernberg and about 100 m. SSE of Ohrdruf). The final battle HQ (special train D) will be reported later."

* * *

c. *Possible new commanders*: Hitler's order of the 7th did not identify the incumbents of the newly created posts, but slight suggestions are afforded by the language of the order and subsequent messages. Although Blaskowitz has been C-in-C Army Group "H" since February, the move of his HQ to western Holland seems inconsistent with his assumption of the command into which that Army Group has been merged, and is rather an indication that he may be the new "C-in-C Netherlands."

Genfldm. Busch, who has been CG Operations Staff North Coast, is a likely incumbent for "C-in-C Northwest." Hitler's order specified that this high command was to have subordinated to it "the former sphere of command of Operations Staff North Coast," and on 8 April C-in-C West addressed to "C-in-C Northwest, via Operations Staff North Coast" an inquiry as to when command over Army Group "H," including Armeegruppe Student and Wehrkreis XI, "can be taken over."

It is assumed that Genfldm. Kesselring continues as C-in-C West, Genfldm. Model as C-in-C Army Group "B" and Admiral Krancke as Naval Chief Command West.

d. *Harz sector*:

(1) *Appearance of a new Army*: On 9 April C-in-C West stated:

"Hitler has ordered the Harz (Massif) as the assembly area for the Twelfth Army. The foremost division of the Twelfth Army is the 85th Inf Div. . . .(portion missing). . . .Any intervention by C-in-C West, the Eleventh Army, or other staffs, is expressly forbidden. . . ."

Note: The new Army is to assemble in the region which
Wehrkreise IX and XI have been ordered to prepare for defense. . . .

On 2 April Hitler stated that six divisions "being set up" were to assemble in the area Hannover - Northeim - Brunswick —which is just northeast of the Harz and which is now being overrun by the Allies. That order said that "the later tasks of this Army will be ordered at the proper time". . . .

On 26 March the cadre personnel of the 85th Inf Div, which is being set up anew inside Germany, were ordered to move from a troop training ground north of Wuerzburg to one just west of Berlin.

(2) *Units to be refitted on the edge of the battle zone*:

(a) Also on 9 April, C-in-C West subordinated the 394th Assault

Gun Bde, which was assembling just north of the Harz Massif, to the Eleventh Army. The order stated that the Bde was to be rested and refitted, and that guns were to be provided as quickly as possible. Until its "operational capacity" was restored, the Bde was, "within the scope of the Harz defense, to take over defensive and blocking tasks in its rest and refitting area."

(b) On the same day (the 9th) C-in-C West ordered that a battle group of the 9th Pz Div to be transferred to the area of Sangerhausen (20 m. E of Nordhausen) for "further rest and refitting." While there, the battle group was also to "prepare for defense, take part in constructing blocking positions, and operate if the Allies attack."

(3) *Kesselring order to the Eleventh Army on 7 April*:

"(i) In order to gain time, the Eleventh Army, using no more forces than are necessary, must fight a battle of bitter delaying resistance on its western front, the rear of which rests on the Harz Massif and the mountainous country to the west. This gain of time will serve to make the strong sectors behind the Army's front capable of defense and to develop the Harz Massif into a blocking Schwerpunkt of the first order.

"(ii) It is of utmost importance for the Army, with all speed, to shift to its southern wing the forces which are to be economized on its front facing west. Then, driving toward Langelsalza and Gotha (respectively 10 and 20 m. SE of Muehlhausen), those forces can fall on the Allied flank with adequate striking power.

"(iii) At the same time it is most important to take immediate countermeasures to forestall the possibility of the Army's western front being rolled up from the north and south. This means that, on the north, all roads and tracks in the area Gronau - Alfeld and to the west (i.e., an area about 20 m. S of Hannover) must be rendered impassable with adequate defense; and, on the south, the Allies, as they feel their way northward from Muehlhausen, must be attacked on the flanks. Here the Eleventh Army's conduct of operations must be adjusted to the utmost mobility and flexibility.

"(iv) The area Nordhausen - Sonderhausen- Kelbra - Schmuecke Depression ((i.e., east and northeast of Muehlhausen)) must be turned into a firm defensive block. Farther west, local strongpoints such as Uslar, Hardegsen, Northeim, Adelebsen, Harste, Goettingen, Dransfeld and Witzenhausen ((all northeast and east of Kassel)) must be so strongly developed and adequately manned that they will hold firm under efficient Officers Commanding Local Operations. Because of the Allies' well known by-passing tactics, the flanks of these places must be covered and adequately protected. Covering forces in effective strength, with patrols out to the sides to prevent surprises, must be in position at least 1 1/2 kilometers in front of blocking sectors. The Allies must be brought to a dead stop in this system of blocks."

Note: By 10 April Allied troops had overrun the Gronau - Alfeld area and the local strongpoints above Kassel, thus rolling up the western front of the Eleventh Army from both the north and the south.

* * *

For the Assistant Chief of Staff, G-2:
CARTER W. CLARKE
Brigadier General, GSC
Deputy Chief, MIS

Distribution:

Within the War Department
- Secretary of War
- Chief of Staff

CG, AAF
Deputy C of S
Deputy Commander, AAF
AC of S, G-2
AC of S, OPD
AC/AS, Intelligence
AC/AS, Plans
Deputy AC of S, G-2
Chief, MIS

Outside the War Department
- The President
- C of S to the Commander in Chief
- C-in-C, U.S. Fleet
- DDMI, BAS

CHAPTER VII

Disseminating the Product

The twin breakthroughs achieved by the Army in the field of signals intelligence in mid-1943—making an entry into Japanese military traffic and reaching an agreement with Bletchley Park to share the British COMINT take from German sources—made it possible for the first time to provide American field commanders with immediate intelligence of operational use. This posed a major problem. How could this ultra-sensitive intelligence be disseminated in a timely fashion without risking compromise of the source which would undo the whole effort. The U.S. Army came up with the solution of adopting British security regulations and creating a Special Security Officer system under Special Branch to handle distribution of signals intelligence to the field. Specially picked and trained officers, operating under War Department control and utilizing a special communications system, would serve as the conduits for high-grade COMINT—ULTRA, as it was now called. These officers would act both as security watchdogs and as guides to properly interpreting the material.

In SRH 026, Marshall Letter to Eisenhower, the Army Chief of Staff explains the new security system to the Commander, European Theater of Operations. SRH 033, History of Operations of the Special Security Officers, provides a general overview. Excerpts from SRH 031, Trip Reports - ULTRA in the Mediterranean; SRH 022, ULTRA and the Seventh U.S. Army; and SRH 032, ULTRA in the Southwest Pacific Area, contain reports from individual Special Security Officers on conditions in the field.

From SRH 026. *As a result of the agreement between the British and the War Department to share cryptologic intelligence, "Ultra" material could be sent to American field commanders under strict security provisions. In this letter, Army Chief of Staff George C. Marshall explains the arrangements to his principal subordinate in Europe, General Dwight D. Eisenhower. The security regulations of April 1944 to which Marshall refers introduced the TOP SECRET classification to the U. S. Army for the first time.*

WAR DEPARTMENT
THE CHIEF OF STAFF
Washington, D. C.

March 15, 1944

Dear Eisenhower:

You are undoubtedly aware of the supreme importance which the War Department attaches to intelligence known as "Ultra." This intelligence is secured by the British from reading German enciphered radio communications.

The attached Tab sets forth the basis upon which German "Ultra" intelligence is made available to American field commands. Please give this matter your personal attention, and take all necessary steps to insure that the security regulations governing the dissemination of "Ultra" intelligence are meticulously observed. The arrangements described in the attached Tab are to be fully carried out.

Faithfully yours,
/s/ G.C. MARSHALL

General D.D. Eisenhower,
Supreme Headquarters,
Allied Expeditionary Force,
London, England.

1. A large volume of highly important military and air intelligence is derived by the British from reading German radio communications enciphered in high-level German cipher systems. This type of intelligence is known as "Ultra" intelligence.

2. The basis upon which German Ultra intelligence is made available by the British to the US War Department and to American Field Commands in active theaters is governed by an agreement made in June 1943 between the US War Department and the responsible British organization.

3. The British organization which produces Ultra intelligence is the Government Code and Cipher School, the Director General of which is Brigadier Sir Stewart Menzies.

4. Administration of the agreement of June 1943 is controlled by the British [text withheld] through Brigadier Menzies, and by the US War Department through the A. C. of S., G-2.

5. To carry out the agreement of June 1943, and to assist in and supervise the dissemination of Ultra intelligence to American Commands in the European Theater, a detachment of MID, the title of which is MID, War Department, London, has been detailed for service in the European Theater. This detachment is under the direct control of the A. C. of S., G-2, and the Commanding Officer of the detachment is the representative of the A. C. of S., G-2, on all matters relating to or affecting Ultra intelligence in the European Theater.

6. Security regulations governing the dissemination and handling of Ultra intelligence within the European and Mediterranean Theaters have been approved by the US War Department [text withheld] and will become effective on 1 April 1944.

7. Under the agreement of June 1943 and the security regulations of 1 April 1944, the basis of disseminating Ultra intelligence to American Commands in the European Theater is as follows:

a. Ultra intelligence produced by G.C. & C.S. (including the component of the US Signal Corps at G.C. & C.S.) is disseminated to Field Commands only by means of special communications channels established and controlled by the Director General, G.C. & C.S.

b. Communications between Field Commands which discuss or mention Ultra intelligence must be passed only over the above special communication channels.

c. American officers participate at G.C. & C.S. in the selection of Ultra intelligence for dissemination to the Field Commands and in the preparation of the messages in which the Ultra intelligence is so disseminated. These officers are attached to MID, War Department, London.

d. The receipt and distribution, at the Field Commands, of messages containing or relating to Ultra intelligence, is handled by Special Liaison Units furnished and controlled by the Director General, G.C. & C.S. The personnel of these units includes American officers attached to MID, War Department, London.

e. The Special Liaison Units distribute Ultra intelligence messages only to officers at the Field Commands who are listed as entitled to receive Ultra intelligence. The eligibility of officers for listing as authorized Ultra intelligence recipients is governed by the security regulations of 1 April 1944. The Director General, G.C. & C.S., and the Commanding Officer of MID, War Department, London, administer the provisions of the agreement relating to admission of American officers in your theater to the list.

f. One or more American officers assigned to MID, War Department, London, will be detailed to each American Field Command, which receives

Ultra intelligence. These officers will be subject to the administration and discipline of the Command to which they are detailed. They will work under the control of the G-2 or A-2 of the Command as part of his staff. They will have had a period of training at G.C. & C.S., and, if possible, with operational commands in the Mediterranean Theater, and this training will be directed toward equipping them to use Ultra intelligence effectively and securely. Their primary responsibility will be to evaluate Ultra intelligence, present it in useable form to the Commanding Officer and to such of his senior staff officers as are authorized Ultra recipients, assist in fusing Ultra intelligence with intelligence derived from other sources, and give advice in connection with making operational use of Ultra intelligence in such fashion that the security of the source is not endangered. If at any time the flow of Ultra intelligence is not sufficient to occupy fully the time of these officers, they may be used for other related intelligence assignments.

8. The Commanding Officer and the G-2's and A-2's of all American Field Commands in your theater, which receive Ultra intelligence, will take all steps necessary to insure that the requirements of this letter and of the security regulations of 1 April 1944, are fully carried out. In order to safeguard the continued availability of this enormously important source of intelligence, it is vital that these security regulations be meticulously observed, and that all personnel entitled to handle or receive Ultra intelligence take all possible precautions in connection with its handling and use. When operational action is taken on the basis of Ultra intelligence, the utmost care must be taken, by means of proper cover, to insure that the action does not reveal or in any way suggest that this source of intelligence is at our disposal.

9. It is of particular importance that:

a.Ultra intelligence be transmitted to the Field Commands only by those special channels mentioned in paragraphs 7a and b above, and that communications discussing or mentioning Ultra intelligence be transmitted only by those channels.

b.Ultra intelligence be discussed orally only with personnel of the field commands who are listed as authorized recipients of Ultra intelligence; and

c. Full facilities and opportunity be extended to the MID, War Department, London, officers detailed to Field Commands in order to enable them to perform their duties fully and effectively. The Commanding Officer, MID, War Department, London, and his principal assistants, will visit the Field Commands as occasion requires to consult with the G-2's or A-2's on methods of handling or using Ultra intelligence and on the scope and method of servicing Ultra intelligence from G.C. & C.S. to the field commands.

10. The contents of this letter will be communicated to the Commanding Officers and G-2's or A-2's of all American Field Commands in your theater which receive Ultra intelligence.

From SRH 033. *This document was prepared in 1945 as an introduction to the numerous individual activity reports prepared by Special Security Officers and Special Security Representatives assigned to the various theaters. Selected reports are reproduced later in this chapter.*

HISTORY OF THE OPERATIONS OF SPECIAL SECURITY OFFICERS ATTACHED TO FIELD COMMANDS 1943 - 1945

1. The Special Security Officer (SSO) system was organized for the purpose of providing a means of rapid and secure dissemination of Ultra intelligence to operating commands. The system was developed and put into operation by the old Special Branch, MID. At the time of the June 1944 reorganization of the Military Intelligence Service the functions of administering the SSO system were transferred to the new Special Branch, although certain of the dissemination functions were retained by the Director of Intelligence, MIS. Moreover, all policy problems were retained under the direct control of the Deputy Chief, MIS. This division of authority did not prove wholly satisfactory. In February 1945 complete responsibility for the administration of the SSO system was vested in the office of the Deputy Chief, MIS, where it still remains.

2. This history is concerned with the development of the SSO system as a whole and will cover the entire period of its operation regardless of the place in the MIS organization where the functions may have been located. Because each theater of operation presented different problems, it was necessary to place a large measure of responsibility in the senior SSO in each theater (eventually his title was changed to Special Security Representative, abbreviated as SSR) for the supply of Ultra to commands operating in his area. A history of the operations within each theater is therefore of much greater value in attempting to evaluate the merits of the system. For this reason detailed histories by theater have been prepared and are attached hereto. The purpose of this introductory statement is to describe the steps which led up to the organization of the system and the manner in which the "home office" was operated in support of the separate theater organizations.

3. The need for the field dissemination of Ultra did not become acute until 1943. Arlington Hall did not make its first entry into mainline Japanese military systems until March of that year, and it was not until the fall of 1943 that any worthwhile intelligence of an operational nature was being produced from these military systems. High level diplomatic traffic had been available since 1941 but its value was strategic in nature and very seldom did anything of immediate tactical importance develop from this source. There were in existence during the period from 1941 to 1943 certain special channels of communication by means of which Ultra intelligence could be made available to various field commands. The Navy

had a direct Ultra channel to CINCPAC at Pearl Harbor, with an extension to the Commander, Seventh Fleet in Brisbane. General MacArthur had his own cryptanalytic organization, Central Bureau Brisbane, which had special channels of communication to Signal Security Agency (Arlington Hall) [text withheld] There was no direct intelligence channel for Ultra from the Military Intelligence Service to any of these commands.

4. German military Ultra in great volume and of the highest operational significance was being produced by GCCS in London. The results were disseminated over a special Ultra intelligence channel maintained by British Special Liaison Units (known as the SLU organization). Throughout the North African campaign the SLU organization served key American officers with this intelligence in accord with British security practices. The Military Intelligence Service did not participate in this service, and as a matter of fact, was not completely aware of its existence until the summer of 1943. German military Ultra was never produced by Arlington Hall, the primary reason being that it was not possible to intercept German military traffic on the North American Continent.

5. The first steps taken to unify the method of field dissemination of Ultra and to insure that all Ultra intelligence was made available to the appropriate operational commands, was to come to an understanding with the British. In the spring of 1943 an agreement was entered into between G-2 and [text withheld] London [text withheld] providing for complete cooperation in the Ultra intelligence field. By the terms of this agreement, the British assumed primary responsibility for the production and exploitation of German military Ultra, and the United States Army agreed to devote its attention to the production and exploitation of Japanese military Ultra. Full exchange of the products of each service was provided, and the principle was established that each service, in cooperation with the other, would establish methods of dissemination to its own operational commands. [text withheld] The subject need not to be further discussed here other than to say that the British SLU organization [text withheld] was the pattern upon which the SSO system was developed for dissemination of Ultra to Pacific commands.

6. The German problem having been solved in principle, attention was then directed to providing a system for the Pacific. The peculiar nature of Ultra intelligence required a system of dissemination which, in some respects, was contrary to established principles of command responsibility. The high level Japanese military cryptographic systems were of such difficulty that only a tremendous organization equipped with expensive and bulky electrical tabulating machinery could produce any results. Consequently, detailed items of immediate tactical significance to an Army commander in the field could be read at Arlington Hall, but could not be produced by an agency located in the theater and near the Army commander interested. Therefore "combat intelligence" was being produced in Washington, some 15,000 miles away from the front lines. To forward this intelligence through normal command channels of communication and through every intermediate G-2

between the War Department General Staff and the combat commander concerned would delay its receipt and, in many cases, the particular message would lose all value by the time the commander finally received it. More important were the security considerations involved. Experience in World War I and the experience of the British in World War II had proved that wide dissemination of Ultra very often led to a compromise and complete loss of the source. The business of cracking codes is movie thriller stuff and the natural reaction of an uninitiated person is to make some comment about it to other responsible officers who would normally be supposed to be in on the secret. Careless talk by one uninformed person to another soon results in the "secret" being public information. To avoid these dangers, the British had adopted several rules of dissemination which had proved highly successful in maintaining the necessary security. They were:

a. Ultra was never to be made available to anyone, from a commanding general down to the code clerk who sent the message, without first explaining to the recipient the security questions involved, and how even the most innocent comment might lead to loss of the entire source;

b. Ultra would be disseminated only via special communication channels which would be used solely for that purpose.

This would prevent a casual knowledge of Ultra on the part of personnel employed in communication centers, and would also enable complete control of dissemination within the theater of any messages transmitted over this channel;

c. The special dissemination channels would be maintained by officers and enlisted men from a central organization and would be furnished only to commands which had actual need of Ultra intelligence. The local commander would therefore not have the authority to over-rule this personnel on any matters involving security.

d. Strict rules for the dissemination within the command, limiting the number of officers authorized to see the intelligence, and the uses which could be made of it, would be prescribed by the central organization.

7. The Pacific field dissemination system was devised in the summer of 1943 on the basis of the principles outlined above. It was decided to designate the officers who would maintain the special channels as Special Security Officers (SSO's). SSO's were to be assigned to the Military Intelligence Service and remain under the operational control of the A. C. of S., G-2, WDGS. They would be attached to the theater commander for purposes of administration and discipline and would disseminate Ultra in accord with rules announced in security regulations issued by the War Department. Authority was obtained from the Chief of Staff in the summer of 1943 to consult the theater commanders in the Pacific and to obtain their concurrence with this plan. The commanding generals of the Pacific Ocean Areas and the China-Burma-India (CBI) Theater readily concurred, but the Commander in Chief, Southwest Pacific Area, raised certain objections to the proposal on the ground that the SSO should be assigned outright to his command rather than

remain under the control of the War Department. Col. Carter W. Clarke, then Chief of Special Branch, was sent to Brisbane to confer personally with CINC, SWPA on this difference of opinion. As a result of this conference, General MacArthur concurred in the original plan.

8. The first War Department security regulations governing overseas dissemination of signal intelligence were issued in October 1943. Following the British practice, two classifications were established: ULTRA DEXTER and DEXTER. Subsequently these terms were increased to three, as follows: ULTRA [text withheld] PEARL [text withheld] THUMB [text withheld]....The regulations governing Pearl and Thumb were subsequently revised, in conjunction with the Navy, and the single code word PINUP was adopted for all low level signal intelligence.

9. The original Ultra Dexter regulations were implemented in the fall of 1943, when special security officers were sent to the following theater headquarters: Southwest Pacific Area, Brisbane (Major James Ashby, Jr.); China-Burma-India, New Delhi (Captain John F.B. Runnalls); Pacific Ocean Area, Fort Shafter, T.H. (Major Edwin E. Huddleson, Jr.). The original plan was to limit overseas dissemination of Ultra to theater headquarters and to await recommendations from the special security officers before making provision for broader dissemination. It will be recalled that the operational situation in all three theaters in late 1943 and the first half of 1944 was not such as to require dissemination to subordinate operational commands. Accordingly, all three special security officers undertook to serve the respective theater commanders and their staffs. To accomplish this each officer carried with him his own set of cryptographic equipment (SIGABA) for the enciphering and deciphering of Ultra messages. Special arrangements were set up to provide pouch service as well, and such material as the Diplomatic Summary was sent regularly by special Top Secret pouch. It should be noted that both radio and pouch communications were sent to the special security officer personally. Thus he received radio communications in enciphered form and did the actual deciphering himself. He was therefore the only person to see such messages in the clear, and showed it personally to the theater commander and other specified staff officers. At no point did the contents leave the control of the special security officer. Pouch material was delivered to him unopened, and he thereupon showed relevant material to appropriate headquarters officers, retaining actual custody of it himself. This system proved both secure and efficient. Except for certain considerations peculiar to SWPA [text withheld] the special security system won the approval and confidence of theater officers concerned.

10. Meanwhile, preparations were underway for the establishment of a special security system to serve in ETO in connection with the expected invasion of the spring of 1944. A larger number of officers were recruited and sent to the ETO for training. . . .Accordingly there arose the need of a Table of Organization which would provide vacancies for enough special security officers to fill the needs of both the European and Japanese wars. In December 1943 a staff study was pre-

pared which described the special security requirements and stated the estimated personnel needs. Approval was thereupon given by the Adjutant General for a field quota of 80 officers. In July 1944 this quota was enlarged to 172 officers and 65 enlisted men, a total which proved sufficient for the duration of the war.

11. In the spring of 1944 sufficient information had become available, based on recommendations of special security officers and upon projected operational plans insofar as they were available to MIS, to permit a decision as to the extent to which Ultra should be disseminated below the level of theater headquarters. Accordingly, the regulations were rewritten (10 July 1944) to allow dissemination to the level of Army (or equivalent Air Force Formations) and to Corps level when the Corps was operating independently. In April and May of 1944, by way of preparation for the revised Ultra program, officers were recruited for SSO duty in the Pacific and Far East. The first group, numbering about 20, began a training period on 3 July 1944 and were sent overseas about 1 September 1944. This group included a full complement for CBI and a group of officers for SWPA. The training course consisted of a week's tour of ASA, two weeks' training in the specific duties of the special security officer (study of regulations; lectures by returning officers familiar with the theater concerned; consultation with relevant sections of OPD; cryptographic security; communications, etc.) and from four to six weeks straight intelligence training, which included the Far Eastern Intelligence Course and selected reading of Ultra materials; where possible the officers spent from one to four weeks actually working on Ultra traffic as members of the various Ultra sections of MIS. The value of this latter aspect of training cannot be over emphasized. This first group which went overseas have all testified to the importance of an adequate intelligence background. By and large, this group was well trained, but as the operational situation grew more active it became necessary to send additional special security officers on very short notice. In many cases such officers had to be dispatched with very little training or background in Ultra. If there were one lesson to be learned from experience in connection with the SSO program in the Far East, it is this: a large potential pool of security officers should be recruited early—as early as possible and long before they will actually be needed overseas. They should function as working members of MIS—this is the very best type of training—and be available for overseas assignment as the need arises. The greatest single handicap in the past administration of the SSO system was the lack of adequately trained personnel to meet the suddenly increasing needs of the Pacific war. While it can be said that the program was carried out efficiently in the face of numerous obstacles, and that the sudden expansion in SSO requirements could not have been anticipated, the ultimate results could have been more satisfactory if we had had too many qualified personnel available rather than too few. Admitting that it is always difficult to obtain as many highly qualified officers as one would like, this phase of the problem should be given particular and immediate attention in the event that the need for an SSO organization should ever arise again.

12. The manner in which the SSO program was carried out in the respective theaters is fully explained in the individual histories.It remains only to discuss briefly the functioning of the home office. Before the G-2 reorganization of June 1944, the administration of the overseas dissemination was handled by two officers in Special Branch. After the reorganization, when the SSO field quota expanded from 3 to some 65 officers in the Pacific and Far East, the administration was made the responsibility of the newly constituted Special Branch. A total of three officers were actually engaged in the administrative phase of the SSO program. These officers were concerned with the following aspects of the SSO program: recruiting and training of SSO's; review and revision of Ultra, Pearl, and Thumb regulations; handling of all administrative correspondence, by radio and pouch, between MIS and SSO's overseas; liaison with interested sections of the intelligence group in connection with intelligence requests from SSO's; coordination, where necessary, with ASA, OPD, OCS, the Navy, and with various other organizations of the War Department; all personnel problems, including promotions, travel orders, security clearances for both officers and enlisted men; a myriad of miscellaneous matters which cannot be conveniently catalogued but which arise in any unit of the size and scope of the SSO organization. While it is a matter of record that there was no serious breach of security throughout the war, and while theater officers have uniformly testified to the quality of the service they received, it is submitted that a larger home office, more fully staffed both with officers and civilians, would be desirable "next time."

13. In January 1945 the functions of Special Branch were transferred to the Office of the Chief, MIS and placed under the direct supervision of the Deputy Chief. Inasmuch as the Special Branch program was under the direction of the Deputy Chief from the outset, this transfer proved more satisfactory, since it eliminated an extra step in the chain of command and simplified the matter of coordination with the Director of Intelligence, a major part of the Special Branch job. Again the duties were performed by three officers, although this number was increased to five during the summer of 1945. There were no substantial changes in procedures as a result of the above mentioned transfer.

14. Apart from personnel, the most important single factor in the efficient and secure operation of the SSO system, was the special communications channel, which worked magnificently and proved eminently satisfactory throughout the war.

From SRH 031. *In preparation for a future assignment as a Special Security Officer, an Air Corps lieutenant colonel went to the Mediterranean Theater of Operations to observe how the British had organized the distribution of Ultra material in that area. It should be remembered that Special Branch serviced air commanders as well as the ground Army. MAAF refers to Mediterranean Allied Air Forces; in today's military parlance, it was a combined service operation rather than a joint one.*

24 June 1944

SUBJECT: Report on Mediterranean Trip.
TO: Commanding Officer, MIS, WD, London.
FROM: Lt. Col. Leslie L. Rood, A.C.

1. This is a report on my visit to the Mediterranean Theater of Operations in June 1944, to observe the use of air special intelligence. Because the London office is already familiar with the general functioning of the Mediterranean organization this report is only of a supplementary nature.

2. Mediterranean Allied Air Forces, a joint British-American Command, is the supreme air headquarters of the Mediterranean Theater. It has a rear headquarters at Algiers and an advanced headquarters at Caserta. Under it are Strategic Air Force Tactical Air Force, and Coastal Command.

The Strategic Air Force is an almost wholly American Unit, the 15th Air Force, operating from Bari. They have one British group of Wellingtons for night bombing. The 15th is an operational command in that it plans and directs missions.

Tactical Air Force at Caserta, on the other hand, is a British-American Command that is not operational. It has under it (1) the 12th Tactical Air Command (American) which gives close support (fighter bombers) to the 5th Army, (2) Desert Air Force (British) which gives close support to the 8th Army, and (3) two wings, one of medium bombers and one of fighters, which operate at a greater distance behind the enemy lines.

Coastal Command, with defensive, convoy and coastal missions, is spread out over the whole Mediterranean. Tactical and Strategic are in Italy.

3. I departed from London on the evening of 26 May 1944 by sleeping car and arrived in Newquay, Cornwall, the next morning. I should have taken off from St. Mawgans that night, but due to engine trouble did not get off until the fourth night. The plane arrived at Casablanca the next morning and by evening I was in Algiers.

I spent three days with MAAF (rear) and took off for Caserta on 4 June. For the succeeding three days I was there with MAAF (adv.) and TAF. On 8 June I went to Bari by courier plane to spend three days with the 15th Air Force and 276th Wing. Returning to Caserta on the 11th I was unable to go forward to 12th

TAC at Rome until the 14th because they were disorganized by the rapid advance. When I did reach Rome I was able to stay with them for only two days because they again split into three echelons and moved on.

On the evening of the 17th I left Rome; on the morning of the 18th I left Caserta; the next morning I departed from Algiers; after a delay of one day in Casablanca I took off for the U.K. and was in London on the evening of 21 June 1944.

4. The two MAAF special intelligence sections operate like miniature Air Ministries. At each headquarters the four or five officers processing the material are segregated in an out-of-the-way room where they do their work. Each officer has a specialty such as order of battle, "Y," supplies, Balkans, or targets and as the expert on that subject, he writes part of the daily digest which is prepared for the generals. The senior officer of the group usually carries the digest around, so that he can answer any questions which arise. They write very few appreciations, nor do they have any direct connections with operations. Their prime purpose is to be completely familiar with the material so that they can interpret it to their operational people. Secondarily, they compile a weekly order of battle which is published at several levels. MAAF (rear) also sends out a weekly supply summary at the highest level.

5. The 15th Air Force at Bari impressed me as a very smoothly functioning organization and its "A-2 Liaison Officer," Major Murphy, as an able part of it. Each morning the staff meets with the A-3 (acting as the operational chief of staff) to plan the missions for the subsequent day. First the weather officer delimits the possible areas of operation by his forecast; the A-2 names the targets having priority in that area; the damage analysis officer advises the A-3 to what extent the suggested targets have already been destroyed. Attention then being officially centered on several targets (the staff had already informally decided on these and spread the proper target charts before the meeting) the flak officer is called upon for the number of minutes the ships will be in flak if approaches are made from certain angles.Major Murphy is then called upon for an estimate of where, how many, and what kind of enemy planes will be encountered. Along with the weather officer he stakes his reputation daily since both of their predictions are checked by the next evening.

After quite a succession of direct questions by the A-3 and unequivocal answers by the staff, the A-3 fluently dictates a complete operations order. Each officer copies down the part pertaining to his responsibility and during the early afternoon submits the written annex to the finished order which is placed before the Commanding General for his approval.

Because of his daily forecast, Major Murphy is known to most people as the order of battle expert but even more important is his servicing of senior officers with special intelligence. He separates from the general material that which might interest the senior officers, annotates it with brief notes when necessary, and then

shows them the annotated material. He often has to do some verbal explaining and elaborating but he writes no digest.

There was a time when special intelligence was important at Bari for its order of battle information, but now when the GAF puts up a maximum of 150 planes to protect the most important targets and none for lesser targets, raids are naturally planned with little regard for the possible opposition.

The most valuable material, therefore, is that pertaining to targets, e.g. that a bridge was destroyed, that shipping on the Danube has been stopped or that damage to refineries has caused a gasoline shortage. Operations people take a very keen interest in anything which gives a clear cut statement of the damage done by their bombers the day before. With the increase in blind bombing this is even more true.

Most of the intelligence at the 15th Air Force consists of target work, i.e. photography, collating of agents reports and economic studies of objectives, and bomb damage analysis. There is a large target section staff at MAAF (adv.) which serves the 15th Air Force almost exclusively by preparing target charts and 15th Air Force also has a large target section which selects objectives and analyzes bomb damage. Since no one in the target section at Bari has special intelligence, Murphy helps them with his superior wisdom quite frequently.

In attempting to summarize for me what special intelligence supplied to the whole intelligence organization at Bari, Murphy said that its primary contribution was a "negative influence." Most of the information Murphy gets from special intelligence is also procured from photos, PW's, pilots' reports, and "Y," but in them the good is mixed with the bad. Special intelligence tells Murphy and his superiors what not to rely on. Rarely does he get anything of pure operational value, something which causes him to rush into A-3 demanding that a mission be layed on.

6. TAF's functions are difficult to understand because of its intermediate role below the policy level of MAAF and yet above the target selection level of TAC and DAF. Its role is further complicated by its being an operational headquarters over its medium bomb wing but a non-operational headquarters over its close support commands.

It is primarily a coordinating command. Its greatest interest during my visit was in the progress of its campaign to choke off all supplies to the battle area. Special intelligence provided very good material on this subject.

The segregation of special intelligence is not very noticeable here because only the chief intelligence officer, W/C Wiseman, and his assistant, Captain Austin, have it. Their knowledge is used through attendance at all planning conferences, some of which are at the highest level. They show selected material to the senior officers and do not write a digest.

7. Discovering how Major Corning, at 12th Tactical Air Force, uses special intelligence was not easy. He keeps no records that one can analyze. He is the A-2

and the only person doing pure intelligence work so special intelligence is not neatly segregated for the visitor's examination. Corning operates out of his shirt pocket, merges all sources in his mind, and is not given to pat statements about what part of his total knowledge is supplied by special intelligence.

12th TAC, in supporting the 5th Army is meeting absolutely no enemy planes so naturally order of battle is forgotten. Likewise, the occasional damage reports on specific targets are of doubtful use because TAC attacks vast numbers of small targets each day such as motor transport, bridges, railway cuts and dumps.

What is important is that special intelligence shows TAC very clearly that its primary mission, cutting the lines of communication and supply, has been successfully accomplished. The German inability to defend has been caused to a great extent by the lack of supplies.

In the fast moving situation prevailing during my visit special intelligence indications of where the enemy might make a stand was also of great value to TAC in deciding where to establish its airfields as it advanced.

TAC's intelligence set up is very simple. The broad plans of attack are made by Army; the target section is run by the Army and all TAC gets is a set of photos and a request for missions; there is no air order of battle; almost all the special intelligence coming through during my visit concerned the Army and was only of incidental interest to the A-2. The A-2 does the pure intelligence work and his eight subordinates are primarily engaged in compiling operations summaries, an A-3 job.

8. My visit to the 276th Wing was valuable chiefly because I saw a complete "Y" organization operating under one roof. This organization functioning without the complicated refinements of Block F, was "Y for Children."

Special intelligence is used at 276 Wing solely as a guiding influence. It enables the senior officer to eliminate from the published reports many of the erroneous conclusions which would result from dependence on "Y" alone. Unfortunately there is so little traffic to be picked up in the Mediterranean that their reports are comparatively unimportant.

9. Seeing four levels of command in the field immediately following my visit to War Station and Air Ministry, the stair like decline of formality in handling special intelligence was very noticeable. At one extreme is an elaborate recording and weighing of every detail and at the other is the casual treatment at 12th TAC where the recipient skims through the pencil written pages of the day, tracing some out on the map, rereading some, ignoring others and in no case writing anything down. At MAAF (rear) quite a bit of indexing is done so that records will be available for appreciations and weekly summaries. At MAAF (advanced) only an order of battle index is maintained, and at the next lower level, TAF, the informality approaches that of TAC in that only an occasional note is made. The 15th, like its parallel command, TAF, uses practically no records.

10. It is also noticeable that each level of command endeavors to stand on its

own feet rather than rely on appreciations and digests from superior commands. MAAF (rear) sends little to MAAF (advanced), MAAF (advanced) almost nothing to TAF, TAF nothing to TAC and naturally TAC can have no recipients. What little is sent is treated with not too much respect. Each level services its own generals without attempting to also service its lower echelons.

Many of the recipients do see each other quite frequently to exchange views. Probably for this reason no great differences of opinion are evident.

11. At War Station and the Air Ministry, I got the impression that intelligence was 75% special intelligence, 10% "Y," 5% photographs, 5% PW, and 5% miscellaneous. The figures varied somewhat but were usually definite. The people in the field don't think much in terms of percentages and, if they did, the figures would vary tremendously from place to place because each headquarters looks to intelligence for a different type of information. Sometimes special intelligence can fill the need and sometimes it can't. The usefulness of other sources varies also, depending on what the headquarters is interested in.

For commands where few records are kept PW reports mean little because no report is complete within itself. Usually they are skimmed through. Agents reports are seldom read by the A-2 or the order of battle people but they are of some importance to target sections. "Y" in the Mediterranean is sketchy, but along with photo recce of airfields which is fairly good in the Med, does provide good cover for the special intelligence order of battle.

Probably the most valuable source in the theater is photography. With the decline in interest of order of battle, targets are of comparatively more importance. The photo tells the pilot where the target is and within 24 hours of the attack photos give fairly complete damage information. Special intelligence does, of course, enable one to exercise great wisdom in reading photos.

12. Covering the use of special intelligence in the field does not present the problems which I understood it did. This is primarily so because receipt of the material does not usually point the way to an operational mission. The material provides background which enables commanders to make the correct decisions: it confirms or negates information from normal sources; it provides basic facts. None of these need cover.

13. At both MAAF headquarters the groups of people processing special intelligence are wholly British. The senior intelligence officers under whom these people work, A/C Woolley and G/C Luard, each have American executive officers, but only Woolley's executive, Major Tandler, handles special intelligence. Even he does no actual work with it.

While in theory this use of British personnel alone to serve a joint British-American Command may be criticized, there is no practical solution. The British appear to be doing a good job and their long experience in work where knowledge of the past is invaluable would place any newly assigned American officer in a distinctly subordinate position. In addition they already are overstaffed.

At TAF also the chief intelligence officer is British but this provides good balance since the remainder of the staff is predominantly American.
DETAILS:

1. A helmet and gas mask are not needed in visiting Mediterranean headquarters. The only use for a helmet is as a wash basin at headquarters near the front and even there borrowing is expected.

2. Arrangements for transportation take time and should therefore be initiated for the next hop as soon as one arrives at a station.

3. Orders cut in London should authorize visits to all cities which must be reached by ATC, i.e. Algiers and Naples in June 1944. If orders mention only Algiers, more orders must be obtained to get on to Naples. Transportation beyond the ATC terminus is by courier plane or airfield hitch hiking for which no orders are necessary.

4. Cotton uniforms may be purchased in Algiers at the PX.

From SRH 022. *The report of the Special Security Officer assigned to the Seventh Army, the American force that took part in the invasion of Southern France in August 1944. The "SCU/SLU link" refers to the British-operated Special Communications Unit/Special Liaison Unit that served as the conduit for Ultra intelligence produced by the Government Code and Cypher School at Bletchley Park.*

ULTRA AND THE U.S. SEVENTH ARMY
AMERICAN EMBASSY OFFICE OF THE MILITARY ATTACHE
1, GROSVENOR SQUARE, W.I.
LONDON, ENGLAND

12 May 1945

MEMORANDUM FOR COLONEL TAYLOR
Subject: Ultra and U.S. Seventh Army

1. Introduction: The following report summarizes the experience of the Seventh U.S. Army in the use of ultra intelligence between 16 August '44 and 8 May '45. The judgments, conclusions, and recommedations are not intended as generalizations necessarily applicable to either air or other ground commands.

2. Operations: The SCU/SLU link and ultra specialist joined the Seventh Army at Naples, and the station opened on D plus 1, the 16th of August. It had been agreed with the G-2 that the job of the ultra specialist was to receive signals from

the SLU, process them, and post the information on a map. For the first few days of operations in South France, the only map available was a folding map which was shown periodically to the G-2. During this period the quality of ultra intelligence was usually high and in the rapidly moving situation was the primary source of tactical information. The G-2 decided, therefore, that an ultra war room was desirable, and henceforth the ultra specialist occupied a room in the CP adjacent to the G-2. Also during these early days the volume of ultra was so great that it was soon apparent to the G-2 that he could not personally brief his commander on the content. Accordingly, the responsibility for the briefing of all recipients devolved upon the ultra specialist.

At no time during operations by the Seventh Army was there a formal briefing for all recipients. There can be little doubt that formal briefings are desirable for they permit a more careful preparation of the material. But the recipients were not amenable to the idea because it involved an additional commitment of time in their already busy day. Also, the demands of the tactical situation dictated that important ultra intelligence be disseminated to recipients without delay, and any other information was of insufficient importance to justify formal briefings. The typical method by which ultra reached the recipients was as follows: Each morning the G-2 was briefed on the messages received during the night. If in his judgment the information was important, the Commanding General and/or the Chief of Staff were called in and the briefing repeated. Throughout the day, usually after dinner and again after supper, the G-2 was briefed on later messages. Other recipients were briefed throughout the day whenever they found it convenient. At any time during the day or night an important message was passed to the G-2 without delay. In the absence of the G-2, the ultra specialist was authorized to call any message directly to the attention of other recipients if the information therein warranted such action.

The ultra specialist was expected to be currently familiar with information from other sources, but at no time was it desired that his briefings include a merging of ultra and other information. This distinction was closely drawn by the G-2, both for reasons of security and because the merger of all sources of information was accomplished in other ways. At the Seventh Army the chief of the order of battle section was a recipient and the "opening up" of ultra was his primary responsibility. Estimates of the enemy situation were prepared by still another officer in the combat intelligence section, and ultra was injected into these estimates of enemy capabilities by informal consultation with the G-2. Target information derived from ultra provided no problem for it had been agreed between the G-2 and the A-2 of XII Tactical Air Command, supporting the Seventh Army, that all ultra targets would be handled by the Air Force. With the order of battle, estimates, and targets provided for in the above manner, the remaining ultra required little or no correlation with other information.

Attached hereto as Tab A is a statement of two instances in which ultra provided intelligence of extreme tactical importance to the Seventh Army. All recipients

were genuinely interested in ultra and aware of the tremendous advantage provided by source. On one occasion the G-2 remarked, "You know, this just isn't cricket." Generally, ultra information is of primary value in a static or defensive situation; this is indeed true of all information and intelligence derived therefrom. In the attack and pursuit, intelligence has done its job during the planning phase of the operation, and subsequent information is usually outdated by the time it reaches the command. The examples in Tab A, however, cover both situations.

3. Security: It is difficult to really know the security situation at a command, but it was evident that some recipients at Seventh Army were either not cognizant of or sufficiently impressed with the need for security in the use of ultra. There was little questioning the minimum security requirement that the nature of source must not be disclosed, but this understanding did not extend to an appreciation that information derived from source must be properly safeguarded and serve only as the basis for tactical orders when the information itself cannot be "opened up." The greatest misunderstanding here was in the idea of "cover." Recipients were inclined to believe that cover was an invention; the idea of cover as an indication from an actual but open source was alien to all but a few recipients.

The security situation at Seventh Army was complicated by the fact the G-2 of VI Corps, and at the outset the Commanding General, were former recipients at a time when the Corps was operating at Anzio as a virtually independent task force. On a few known and probably on many unknown occasions the G-2 of Army passed on "hunches" to the G-2 of Corps; the latter was certainly aware of their origin but was not bound by security regulations. In this situation it is almost impossible to expect that a Corps G-2, formerly in the picture, will not receive ultra, thinly disguised; as the Army G-2 frequently stated, "You can deny membership in the Elks to a person, but once he has been an Elk and forfeits his membership he will still remember the initiation."

Generally speaking, however, the handling of ultra from an intelligence point of view by the G-2 was consistent with security regulations. The difficulties at the command were more directly traceable to the Commanding General and in the operational use of ultra. The reasons for this are manifest. Charged with responsibility for success or failure in the battle, the temptation to knowingly or unknowingly employ ultra improperly is well-nigh irresistible at times. This, considered along with the fact that the Commanding General is relatively isolated from daily security reminders by the ultra specialist appears to be the major cause of violations.

. . .Once the violation was observed, the facts in the case were obtained from the G-2 and reported to London. The G-2 was never told by the ultra specialist, although he probably guessed, that violations were being reported.

4. Conclusions: The policy of a separate channel and the assigning of an ultra specialist to American commands is basically sound. If nothing else, the mere presence of a War Department representative has a salutary effect. For reasons of administration the SCU/SLU link might well become the responsibility of the spe-

cialist. There is often a real question whether a particular security violation is the responsibility of the SLU or the specialist. Moreover the command is frequently confused in their administrative relations with the SLU, and are never certain whether they should deal with the SLU or with the specialist. There was never any difficulty of this kind at Seventh Army, but there is a real danger in the failure to provide unified control.

There is much to recommend that all ultra matters be considered within the province of the Commanding General and his Chief of Staff, rather than as an instrumentality of the G-2. In the first place, the G-2 might then be subjected to controls which cannot be exercised under the present arrangement. Moreover, by attaching the ultra functions to the Chief of Staff's office, the ultra specialist has direct access to the Chief of Staff and the Commanding General and thus can more carefully safeguard security at the point where it is most vulnerable. Also, by removing the ultra function from the G-2, security is improved by the mere fact that it is not automatically associated with intelligence.

The reading and understanding of ultra security regulations is not sufficient to insure their inviolability. In addition to constant reminders by the ultra specialist, periodic warnings from high commanders seem desirable. The subject must be kept a live one at all times, and the interest of the War Department continuously impressed upon recipients.

Regardless of what other persons are recipients at a command, it seems particularly desirable that wherever possible the order of battle chief be included. At Seventh Army this occurred through accident; the personality involved was "in the picture" at a higher headquarters before joining Seventh Army and his status was continued. But this might well become standard practice, other considerations permitting, for the order of battle man is the key to opening up ultra and the preparation of sound strength estimates.

Finally, it is essential that well-grounded intelligence officers be assigned to commands. The proper interpretation of ultra is very often dependent upon a thorough familiarity with information derived from other sources.

TAB A

(1) Late on D plus 2, ultra information reached the Seventh Army which indicated that the enemy was withdrawing from south and southwest France. The Commander was faced with a major decision involving two factors:

a. To what extent could the enemy be pursued and outflanked, considering the difficulty of supplying advance columns over a beach, and

b. Would the enemy counter attack on the right flank, from the Maritime Alps, and so endanger rear communications.

Ultra provided the answer to the second question, at least a sufficient answer to permit a calculated risk; there was no indication that the enemy would adopt an

attitude other than defensive on the flank. Accordingly, it was decided to pursue and all unloading priorities were altered, with the whole emphasis given to fuel and vehicles. Also, Task Force Butler, which had penetrated deep in the enemy rear, was reinforced with the 36th Div. Together they established a road block at Montelimar in the Rhone Valley and cut the enemy escape route. The road block proved insufficient to destroy the 19th Army and they succeeded in fighting their way out, but all heavy equipment was lost in the process.

It is also noteworthy that ultra guided public relations all through these opening days of the campaign, for it was clear from source that the enemy was not aware of the character of the forces operating in his rear. He apparently believed that there were only guerilla forces endangering his lines of communications; and so the existence and operations of Task Force Butler were not disclosed to the press.

(2). . .Shortly after the German Eifel offensive in mid-December, it became evident that that the enemy was preparing an offensive in the Saar-Palatinate, possibly in conjunction with a coordinated attack out of the Colmar bridgehead and a crossing of the Rhine N. of Strassburg. German Air Force reconnaissance orders from ultra pin-pointed the possible crossing area but source was relatively quiet on the Colmar attack; open sources, however, clearly suggested the latter intention. But it was in the sector between Saarbrucken and the Rhine that ultra provided information necessary for a proper estimate of the situation and preparations to meet the attack when it came. During the critical days prior to the attack the Flivo with the German First Army was being read consistently, and enemy order of battle and boundaries were throughly known. It was possible, therefore, to state with relative certainty that the main effort in the attack would be made west of the Hardt Mtns., with a secondary attack between the mountains and the Rhine. If there was ever an essential element of information this was it, for the passes through the Vosges Mtns. were a serious obstacle to the rapid movement of Seventh Army reserves. Based on this appreciation, the sector west of the Hardt Mtns. was reinforced with the 2nd French Arm'd Div. and the 36th U.S. Inf. Div., both moving from the Rhine plain. It should be noted that up to the day of the attack, German intelligence failed to pick up these moves.

When the attack was launched on 1 Jan., the German main effort collapsed completely. Their only success was in the sector of the secondary effort, in and East of the Hardt Mtns. This German offensive was properly appreciated and preparations made to successfully meet the threat. Lacking ultra it seems very doubtful whether the attack would have been repulsed, or whether other sources of information would have given advance warning. Open sources provided only the most meager evidence of an attack, and there was much opposing evidence suggesting precisely the opposite — a thinning out in the sector and movement of units away from the Saar-Palatinate to reinforce the North.

* * *

From SRH 032. *This report was submitted by Major John H. Gunn, the Special Security Officer assigned to General Douglas MacArthur's Southwestern Pacific Area headquarters. As Gunn indicates, MacArthur ran his theater like a private fiefdom, and the members of his staff were not always happy to deal with people they regarded as interlopers from the War Department.*

WAR DEPARTMENT
MILITARY INTELLIGENCE SERVICE
Washington 25, D.C.

23 October 1945

MEMORANDUM FOR THE SPECIAL SECURITY OFFICER, MIS:
SUBJECT: Report of Major John H. Gunn, 0-388247

The undersigned officer departed Washington on 15 September 1944 for Brisbane, Australia. I reached Brisbane on the night of 22 September. At this time most of GHQ was in Hollandia, Dutch New Guinea, in the final stages of planning and preparation for the invasion of Leyte. The Leyte operation had been accelerated and it was necessary that those SSO's designated to serve the participating commands cut short their indoctrination course in Brisbane and proceed to Hollandia at an earlier date than planned.

My principal duties in Hollandia were to assist Lt. Colonel Ashby, then Special Security Representative for the theater, at his headquarters. I had been introduced to Lt. General Sutherland, Chief of Staff, and it was indicated that I was to accompany the Advanced Echelon into Leyte and serve General MacArthur, General Sutherland, and appropriate G-2 and G-3 personnel. The acceleration of the date for the Leyte operation necessitated Ashby's being absent several days while placing SSO's at the subordinate commands. During this period the undersigned was left at GHQ. I was impressed with the fact that the people on the working level in the theater are, despite the idiocyncracies, jealousies and animosities of their superiors, an amazingly cooperative group.

The Chief of Staff had indicated that there would be no room on the Command Ship for an SSO. As a result he referred Ashby and me to the G-3 section to make arrangement for transportation to Leyte in some other vessel in the Advance Echelon convoy. The G-2 officer in charge of the details of loading the G-2 section was to notify me of the proper time and means of departure. I am confident that this charge never again crossed this officer's mind, for Ashby and I discovered the following Saturday night that the G-2 convoy had loaded without any notice to our

office. In the improvision that was necessary I finally arranged to "hitch hike" to Leyte aboard a 6th Army convoy leaving the next day.

The trip to Leyte was uneventful. I carried no classified material other than a black handbag filled with cryptographic material. This material I kept stored in a locked closet in the ship's captain's cabin. This seemed the most secure procedure aboard a vessel whose Commanding Officer kept 18 quarts of bourbon whiskey in his ship's safe, and kept his top secret battle plans for several operations on top of the desk in his sleeping quarters.

We arrived off Dulag at the southern portion of the invaded beach area three days after the initial landings. The usual confusion prevailed on the beach and I was at a loss to find a secure place to keep my cryptographic materials until I could find transportation to GHQ, then located at Tacloban, 20 miles north. Such transportation was not immediately available. After two rather unpleasant nights ashore, when minor but apparent enemy infiltrations of the beach position occurred, the undersigned decided that the most secure place for himself and the classified material was aboard a boat in the harbor. A problem like secure storage seems minor, but it is typical of the practical problems our system often poses.

Upon arrival at GHQ I presented myself to the G-2 section and commenced operations. I was introduced to General MacArthur on the first day of my arrival and found him at all times as cordial and cooperative as possible. It is a matter of record that the same observation cannot be made of a number of his immediate subordinates.

It took only a short while to comprehend the low state of security at the headquarters. For example, no adequate safe accommodations existed, and the loose physical security of the headquarters was evidenced by the presence of innumerable Filipinos who stalked in and out of the staff section area at random. As for the handling of Ultra, complete insecurity was a recurring malignancy. The details of numerous security violations involving our material that occurred during this period have been reported to MIS. One fact was obvious—the main factor contributing to such incidents was a basic lack of appreciation of the value of our material. The principle of sacrificing tactical advantage to security was not even accorded lip service. It seems incredible that Ultra could be obtained and passed by a non-recipient to a non-authorized recipient over a radio relay telephone which was almost certainly being tapped by the Jap. This, and other occurrences as serious, if not as spectacular, are indicative of the security point of view of the persons designated to receive our material.

Without going further in detail, there are certain conclusions that I have drawn with regard to the situation as it occurred on Leyte.

First, General MacArthur has been oversold by his subordinates on the quality of the production of his theater agency, Central Bureau. For example, on one occasion General MacArthur expressed to me a desire to see more diplomatic material, as "I get all the other information anyway."

Second, tactically, the Navy material was incomparably superior to Army production. For example, no Army material was operationally comparable to the Navy material describing the pending Japanese reinforcements in the Ormoc area.

Third, there was no excuse for relaxing enforcement of our regulations to permit passage of Ultra down to Corps level. In no case can I recall seeing any Ultra appropriate for a Corps in its limited sphere of action, and I can imagine no case where a Corps, operating nonindependently, cannot be served by an operational order.

Fourth, none of us, staff officers or SSO's, dealing with Ultra, were adequately indoctrinated in the handling of this material in the field, and in the security practices necessary to ensure its safety. The G-2 men lacked any adequate security indoctrination. In the future the indoctrination of appropriate personnel should be as integral a part of their intelligence training as the preparation of maps or summaries. The security qualification should be a strict exaction for the holding of a responsible intelligence position. It was not in GHQ, SWPA. Nor were the SSO's adequately prepared for their job. Extensive training in the drafting of operational orders, as a security device, is one fundamental necessity in which no early SSO received any training whatsoever. The undersigned, without any previous experience, drafted several such orders in efforts to present an acceptable substitute for an otherwise unwarranted dissemination. It would have been an infinitely more simple task had the undersigned even seen an operational order before he tried his hand at drafting one. Further, if the SSO is to work in an Intelligence Section, he should be thoroughly schooled in the G-2 duties he will perform. Camp Ritchie should furnish the best answer to this problem.

Fifth, closer coordination between Army and Navy Ultra recipients and communications personnel is essential. Tales of the Navy "indiscretions" in SWPA are legion, but in a great measure they may be attributed to a lack of mutual understanding and agreement. For example, Navy furniture shipped from Hollandia to Leyte was addressed to "the Ultra section." and mess bills were addressed to Lt X, c/o the Ultra section. This came about in great measure because the Navy considered "Ultra" as a classification, not a code word. Similarly, Navy acceptance of SSO personnel as participating counterparts aboard ships receiving Ultra is essential to secure handling of the material - since Navy Ultra may obviously be used as the basis for Army directives to Army units. On such directives a trained SSO should be infinitely more authoritative, security wise, than a Navy communications man.

On completion of the transfer of GHQ to Leyte, I was sent to the Office of the Deputy Special Security Representative in Brisbane. There is no need to include in this report any description of the organization and work of this office. . . .

* * *

JOHN H. GUNN
Major, Inf.

CHAPTER VIII

The Politics of COMINT

The motto of the great Army cryptologist William F. Friedman was "Knowledge Is Power." The power derived from the ability to exploit high-level signals intelligence meant that access to and control of COMINT became a political football in various bureaucratic and partisan struggles for advantage. Within the Army, the Military Intelligence Service fought with the Signal Corps over control of the Signal Security Agency. Excerpts from SRH 141-1 2nd SRH 141-2 document the course of the dispute, which was finally resolved (more or less) in December 1944, when the Military Intelligence Service gained operational control over Arlington Hall. On another bureaucratic front, the Military Intelligence Service tried to take on the Navy, claiming that Navy cooperation in sharing signals intelligence was lacking. Another selection from SRH 141-2 reveals the extent of the problem and the fierceness of the rivalry. Finally, in SRH 043, Comments on the Dewey-Marshall Exchange, Colonel Carter Clarke, Chief, Special Branch, describes what happened when Army Chief of Staff General George Marshall tried to ensure that COMINT secrets would not be compromised in the course of the 1944 presidential election contest between incumbent President Franklin D. Roosevelt and Republican challenger Governor Thomas E. Dewey of New York.

From SRH 141-1. *Two months after joining Stimson's staff to recommend better measures for handling signals intelligence, Alfred McCormack had become convinced that the Military Intelligence Division should be given overall control of all intercept activity. To help make his point about the importance of secret intelligence, he makes reference to two intercepted Japanese messages dealing with this subject, one from Japanese Foreign Minister Yosuke Matsuoka, and one from from his successor, Foreign Minister Shigenori Togo.*

March 1, 1942

MEMORANDUM FOR: MR. McCLOY
Subject: Signal Intelligence Service

Here are noted down the points discussed with you, touching on the question whether it is sound organization to leave with the Signal Corps the job of collecting and selecting intelligence materiel of great importance, instead of lodging that responsibility with G-2 as a part of its over-all job of collecting and supplying intelligence:

1. It appears to me to denote a rather negative conception of intelligence to have G-2 simply taking what the Signal Corps catches and turns in, leaving with the Signal Corps the responsibility for deciding how much it will catch and turn in, and from what sources. I am sure that the Signal Corps listens seriously to all suggestions from G-2, but the power of decision remains in the Signal Corps, and there is nobody in G-2 who has an affirmative responsibility for seeing to it from day to day that the material collected and processed (a) is all that possibly can be collected and processed and (b) is derived from the sources that are at the time of greatest importance from G-2's angle. Intelligence activities should be directed affirmatively and vigorously. Compare Minister Matsuoka's direction that "our principal aim is to collect *every possible bit* of intelligence concerning the United States" (18846) and Minister Togo's reference to the "absolute necessity of securing intelligence of this sort" (i.e., the sort not obtainable from newspapers and the radio; 27500).

2. The men in G-2 who are working on the processing of intelligence are too remote from the collection of this material. Let us suppose that Col. Heard, [text withheld] decided [text withheld] or was instructed by his superiors, to gather in as much current material as possible on political conditions and diplomatic maneuvering in [text withheld]. . . .He would not get any such material from the source under suggestion, though the S.I.S. has a lot of [text withheld] material on its shelves, all in its original form, which has never been tackled because of lack of personnel. If there were one officer in G-2 whose responsibility was to keep up to date on G-2's needs *and* be ready at any moment to turn the S.I.S. to work wherever the heat was

on, and if that officer could give orders to the S.I.S., maybe in such a situation all hands not elsewhere essential would go to work on the [text withheld] material. At least, there would be an evaluation of relative needs, and a conclusion would be arrived at in the light of all the facts. Moreover, the real needs as to personnel, equipment and supervision would quickly become apparent if that sort of an evaluation had to be made once in a while.

3. This is a situation in which an infinite number of little things are important. From the dim perceptions that I have obtained to date as to how an Army works (my past military observations having been from the bottom up), I have a notion that, if a good idea about a matter of detail should originate in one of the sections of G-2, affecting what should be done somewhere down in the ranks of the S.I.S., by the time it got up the G-2 command, over to the Chief Signal Officer and down through the appropriate channel, the impulse behind it might have become so attenuated as to be insufficient to actuate a full-grown adult. This is not meant critically, since, as I have already told you, I have been impressed by the ability of all the officers that I have encountered to date.

4. Under the present system of divided responsibility there is nobody in G-2 who knows, or could know, what goes on at the various S.I.S. stations or what decisions made from day to day at those stations affect the content of intelligence coming from those sources. Do we know, for instance, that we might not have obtained a lot more Honolulu material except for some decision by the Signal Corps in routine matters, e.g., to shift an experienced operator elsewhere, to postpone repairing a broken antenna, to use particular receiving apparatus for some other purpose, to run a station less than 24 hours a day, to shut it down for repairs when X might be heard, rather than when Y might be heard? These are minor items, but they might have an important effect on the content of intelligence. Yet in the nature of things the men responsible for intelligence could never know about them.

5. As to items of major importance, it necessarily must be true that the S.I.S. is in competition with the manifold other activities of the Signal Corps for money, supervisory direction and personnel. It seems illogical to keep one intelligence unit separate from all other intelligence units, and in competition with units not concerned with intelligence. The production of intelligence from this particular source ought not to compete for money, direction or personnel with anything except the production of intelligence from other sources. Then you could shift your money and personnel into the branch of intelligence which seemed most likely to be fruitful. As it is, it might be that the Signal Corps would be spending much too much time and money on the production of intelligence material from this source, in relation to the time and money spent on the production of intelligence from other sources. On the other hand, there is some ground for thinking that the Signal Corps is not spending nearly enough time and money on the production of the type of intelligence here under discussion.

6. Under the conditions which exist, it is necessary for the Signal Corps to make many choices which affect the content of the intelligence gathered. It must decide at each station what to listen to; and doubtless there would sometimes be a wide choice. Then it must frequently decide the importance of a particular item, in determining what risks may be taken in getting it to Washington promptly. The traffic that comes in is much greater than can be handled; and at each step in the process of putting the raw material into finished form there must be a selection of a small number of items out of a relatively large number of items. The average number of items going into the mill each day is understood to be around 1,200. Of these, only 200 are read (by the junior officers in charge of the various sections) and only 60 go beyond the stage of reading. In a particular situation—such as the French situation as I have described it to you—we get out hardly more than a sample of what goes in, and a mere fraction of a sample of what might go in. Consequently, the choices here are very important, especially since the material that comes out must be examined with two questions in mind, (1) whether it is valuable in itself and (2) whether it suggests that other material from the same source should be obtained for examination in larger quantities.

7. The present division of functions appears to increase quite materially the number of persons familiar with this material or with the fact that it exists.

Without having heard such arguments as there may be to the contrary, it appears to me that the organization would be sounder, and the job more effectively done *as an intelligence job*, if the S.I.S. were made a part of the General Staff, G-2.

A. McC.

From SRH 141-2. *The issue over whether the Signal Corps or the Military Intelligence Division should control SSA came a large step nearer resolution when Assistant Secretary of War John J. McCloy accepted McCormack's arguments in favor of G-2 control. This memorandum was sent to Lieutenant General James J. McNarney, the Army's Deputy Chief of Staff. As deputy to Marshall, McNarney played a major role in Army reorganization. (To oversimplify, Marshall fought the war while McNarney ran the Army.) The Generals Ingles and Somervell mentioned in the memorandum were, respectively, Major General Harry C. Ingles, Chief Signal Officer; and Lieutenant General Brehon B. Somervell, Commanding General, Army Service Forces (ASF). During World War II, the Army Service Forces commanded all of the Army's technical services, including the Signal Corps.*

22 August 1944

MEMORANDUM FOR GENERAL McNARNEY:

I have thought a great deal about the matter of transferring the Signal Security Agency to the Military Intelligence Service under the Assistant Chief of Staff, G-2. I have given it renewed consideration after the receipt of General Ingles's memorandum and General Somervell's indorsement.

1. It was my impression that the merits of this transfer were considered by the committee which was set up to go into the reorganization of G-2 and that we came to the conclusion that if the Assistant Chief of Staff felt that he needed this agency to render the proper service it should be given to him. Subsequently he delivered a memorandum to you which as I understand it was a proposed outline of the procedure to accomplish the transfer rather than any argument in favor of it. The memoranda of General Somervell and General Ingles do not criticize the procedure outlined but object to any transfer whatever.

2. The chief stated objections in Ingles's memorandum seem to be as follows:

a. That the MIS is only a "staff" section and not an operating agency and that it is not "authorized" by Congress.

b. That for some reason not clearly stated the Signal Corps will not be able to furnish the MIS the same communications facilities and services that it provides for the SSA.

c. That personnel engaged in operating communications facilities will not be able to make proper use of codes and ciphers if such codes and ciphers are supplied by the MIS rather than by the SSA.

3. As to the first of these arguments, above, I do not agree that the MIS merely because it is under the supervision of the A.C. of S., G-2 is not an operating agency. In fact, I think it is, and should be. Its relegation to a minor role between World War I and II was a tragic mistake and certainly the Signal Corps was not

able to keep up any vigorous or broad system of communication intercept during this period.

4. In my judgement one of the chief pillars of our national security system after the war must be an extensive intercept service. If we are to be a military power or, indeed, if we are to play an active role in world affairs, we cannot afford to leave this field entirely to the British and the Continental powers. It is one of the best sources of intelligence that there is and I would take it out of any existing service agency immediately in the hope and belief that it would develop into an organization which would stand a better chance of perpetuation in peacetime.

5. I think that the establishment of such a vigorous agency would be an attraction to the Intelligence Service. The curse of our so-called Intelligence Service to date is the attachment to it of only those officers who have social acceptance and means enough to enable them to pursue a life of relative ease. If we try to put this thing now on its proper level and scope it may be possible to create a real field of activity for ambitious and capable officers. I do not think that we will ever get anywhere if we merely seek to maintain a system whereby direction comes from the MIS and operation lies in the Signal Corps. It ought all to be under one roof. The British have been more successful in this field than any other country, I think. Certainly our efforts to date have been most fragmentary as compared to theirs. They use the system that MIS would wish to follow and I think it is the most persuasive example we have to look to.

6. I do not follow the argument on codes and ciphers. Certainly they can be separated from the operation or communication facilities. In fact, such a separation now exists in the Signal Corps and I do not see how it would be more difficult for the MIS to turn over codes and ciphers to the users than it is for the SSA to do so now.

7. I do not envisage that this transfer involves MIS responsibility for all Signal Corps training. Signal Corps will continue to provide signal training as before the proposed tranfer and the MIS will obtain personnel trained by the Signal Corps to the same extent that SSA now obtains such personnel and in the same manner that other components of the Army obtain such personnel. There will be certain highly specialized training in the Signal Intelligence which will be provided by the MIS but I think this is all to the good as it will give added emphasis to the intelligence aspects, which have been neglected heretofore.

8. I do not believe that it is proposed to "tear to pieces" any existing organization but to transfer SSA to the MIS in its present form and thereby to effect a closer integration of its activities with those of the present MIS.

9. I do not believe that it is good practice to have the MIS by general directive and the establishment of general policies to attempt to create a workable intelligence organization in the low echelons of the Army Service Forces as they are now attempting to do. If it has not already occurred, I am sure that there will be occasions when the MIS will seek to direct the SSA into certain activities or lines as to which, if the SSA is inclined to disagree, they may appeal to the higher levels of

the ASF. When this occurs, there is no one short of the Chief of Staff who can adjudicate the point.

10. Finally, I think that the argument that the present arrangement is successful because SSA furnishes the bulk of the information that the MIS has available is unsound because the total Intelligence available to the MIS really covers a much wider field and actually only a relatively small part of that intelligence is made available by SSA. Much of the most valuable work that the MIS have applied to the intercepts has come in the processing which that service has done on the material furnished it. No part of the Signal Intelligence which MIS has available in relation to European military matters is furnished by the SSA; no part of Naval Signal Intelligence is furnished by the SSA; and no part of the clandestine European field is supplied by SSA. About 70% of the diplomatic is and about 80% of Japanese military is. It is true that it provides the greatest amount of information obtained from any one source.

11. In summary, I believe that the MIS should be given the opportunity of proving that it can exploit this entire field to greater advantage. The enthusiasts are in the MIS; there is some great talent there, and I believe it is a source upon which a broad and effective Intelligence communication service can be erected after the war. The Chief of the Army Communications Services and the Chief Signal Officer are primarily interested in operating a signal communication service; they are not primarily concerned with Intelligence. I believe that the possibilities of greater accomplishment lie in the system advocated by the MIS than in a continuation of the existing system. I am not sure that MIS will take full advantage of all the possibilities but on balance I do believe that they would have a far better chance if they had full control. By such control there is a greater likelihood that we will come out of this war with an organization that can be maintained through the lean years of peace. I would be quite certain that if Signal budgets were cut and SSA were in the Signal Corps, the latter's budget would go, if not first, at least before the regular communications appropriations were cut. We will need an organization to support it whose primary and sole objective is Intelligence.

Of course, there is no merit to the argument that there is no statutory authority for the MIS. First, I think there is sufficient authority to meet any need and, second, when can the ASF complain about no statutory authority?

/s/ JOHN J. McCLOY
J.J. McC.

* * *

From SRH 141-2. *In this memorandum, the Special Branch takes on the U.S. Navy.*

WAR DEPARTMENT
MILITARY INTELLIGENCE SERVICE
WASHINGTON

4 March 1944

MEMORANDUM FOR GENERAL BISSELL:
Subject: Army-Navy Agreement regarding Ultra.

A. *Background of Army-Navy Relations in Ultra field.*

1. Except for the Japanese Army material that recently has started to flow in, the Navy has had the full benefit of the work done by Arlington Hall and the Special Branch. It receives copies of the decoded diplomatic and related traffic. Through the "Magic" Summary it is furnished with all evaluations and studies made by Special Branch.When the British European sources were opened up, and the Military and Naval Supplement was established to report intelligence from those sources, arrangements were made to furnish this daily report to Cominch.

2. Little or no cooperation was received from the Navy in return. It did furnish certain information about Japanese merchant shipping, and transmitted some Order of Battle information to G-2 through other channels . In general, however, the principle was applied that cooperation in the Ultra field would be restricted to the technical and cryptanalytic level and would not extend to intelligence. Not once, during the entire period over which the Navy has been receiving the "Magic" Summary, has any agency of the Navy volunteered any information that might have been of aid on any of the subjects of study covered by the Summary, although on some of them (such as Axis blockade-running) the Navy has had considerable information at hand.

3. When the Japanese Army source was opened up, it was decided not to furnish the traffic to the Navy without some arrangement for reciprocity. For almost a year Arlington Hall had worked on Japanese Army ciphers, had gradually solved them and applied itself to the tedious job of reconstructing code books, while Op 20-G, exploiting a parallel source and being in possession of intelligence that would have been of great value to Arlington Hall, withheld this intelligence and restricted its liaison to the technical level. In the opinion of the writer, the non-cooperation of the Navy retarded the exploitation of Japanese Army sources by not less than 6-months and resulted in depriving both services of intelligence that would have been of important operational use.

4. In spite of the Navy's attitude, the writer dld not feel justified in witholding

Brig. Gen. Carter W. Clarke presents Col. Alfred W.McCormack with the Distinguished Service Medal at the end of World War II. The two men were the architects of the Special Branch, Military Intelligence Service, which evaluated and disseminated Army communications intelligence. (NARA)

German signal troops operate an Enigma cipher device in the field during World War II. The Enigma was used to encipher the communications of all three German armed services. (NARA)

Headquarters of the British Government Code and Cypher School at Bletchley Park. Here, British cryptanalysts broke the secrets of the Enigma. (NSA)

Col. Telford Tayor was appointed to head the London office of the Special Branch in 1943. A prominent lawyer in civilian life, Taylor went on to become a military prosecutor. Here, Brigadier General Taylor, right front, is shown with his staff at the Nuremberg War Crimes Trials. (NARA)

America's top military commanders were able to base their plans on high-level intelligence derived from exploitation of enemy communications. Above, General Dwight D. Eisenhower addresses paratroopers. (NARA)

General Douglas MacArthur, left, used signals intelligence to bypass superior Japanese forces in his island-hopping campaign. (NARA)

To prosecute its war against the U-boat, the U.S. Navy effectively used cryptologic intelligence, but it was initially reluctant to share this source with the Army. (NARA)

Army Chief of Staff General George C. Marshall meets with New York Governor Thomas E. Dewey in 1943. To prevent any compromise of cryptologic secrets in the 1944 election campaign, Marshall sent a secret personal message to presidential candidate Dewey. (NARA)

World War II tactical signals intelligence units. Left: radio direction-finding personnel of the 21st Signal Service Company's Radio Intercept Platoon in Newfoundland. Below: analysts of Signal Security Detachment "D" in England. (NARA, INSCOM)

Intercept personnel of the 128th Signal Radio Intelligence Company work out of a commandeered villa in the Mediterranean Theater of Operations. (INSCOM)

A radio direction-finding site of the 126th Signal Radio Intelligence Company at Brisbane, Australia. (NARA)

Army Chief of Staff General of the Army Dwight D. Eisenhower at Arlington Hall Station shortly after World War II. Other persons in the picture are, from left to right, Maj. Gen. Hoyt S. Vandenberg, Army Assistant Chief of Staff G–2; Brig. Gen. Preston W. Corderman, Chief, Army Security Agency; Col. Frank B. Rowlett; and William F. Friedman. (NSA)

from the Navy information, derived from Japanese Army traffic, which might be of value to Naval operational units. Therefore,with the approval of the A. C, of S., G-2, an arrangement was made for forwarding promptly to the Navy all information on which operational action might be taken.

5. The Japanese Army traffic is exploited by British units in England and India and by an Allied unit in Australia, as well as by Arlington Hall. As the work of Special Branch on this material progressed, it became apparent that we were in a less favorable position to get intelligence out of it than were the British, because they had the benefit of the U.S. Navy traffic and intelligence, whereas we did not. Efforts were made, by personal conversations wlth representatives of the Navy, to bring an end to this disgraceful situation. Those efforts probably contributed to bringing about the Navy's proposal for an exchange on the intelligence level. However, the success of Arlington Hall in opening up the Japanese Army sources was what probably brought the matter to a head.

6. In the discussions involved in preparation of a written agreement, the Army was represented by the writer, Colonel McCormack and Major Perdue of the Special Branch. Following the first meeting, the Special Branch submitted a simple agreement for an exchange of traffic and intelligence, along the lines of the agreement which exists between the A. C. of S, G-2, and the British GC&CS. This was not acceptable to the Navy, who insisted that liaison officers be exchanged and that various restrictions be put into the agreement, pursuant to which, in effect, either party might give or withold intelligence as it might see fit.

7. The final draft of the agreement, as prepared by the Navy, was not acceptable to the officers representing the Army, without a statement by the Navy of the principles that would be applied in interpreting the agreement. Those principles were stated on several occasions by Captain Stone, and were generally to the effect that the restrictive provisions of the agreement were necessary to cover special cases, which might never arise; and that the basic principle would be cooperation to the fullest extent in furnishlng the Army with all the "Ultra" material that it might find of value. It was on the basis of such assurances that the agreement in its final form was submitted to the A. C. of S., G-2, with the recommendation that it be approved by the Chief of Staff.

8. When the Special Branch appointed its liaison officer and he started to go through the Navy daily matarial, it was at once apparent that no one officer could sit in Op 20-G and make a final determination of what traffic might be of intelligence value to the Army; and that the arrangement would work effectively only lf the liaison officer were permitted to select decoded traffic and forward it to the Special Branch without being required to demonstrate how and why it might be of value. The decodes are readily available on duplicate cards and can be handled conveniently by the various specialist groups within the Special Branch who may be working on the subjects to which they relate or might relate.

9. The experience of the Navy's liaison officer with the Special Branch was

somewhat similar. He discussed the point with the Deputy Chief of the Branch, and was informed that an extra copy of all messages would be obtained for his exclusive use and that no restrictions would be put upon him in respect to what he might select; that if he cared to do so he might take all the traffic.

10. A day or two after the Army liaison officer, Major Snow, had started to function, he was informed that there would be certain general restrictions upon what he might transmit to the Special Branch. Those restrictions were then embodied in a memorandum, a copy of which is annexed as TAB A.

B. *Proposed Restrictions.*

(i) *U.S. Navy operational dispatches and reports.*

11. It is not clear just what this covers, but it appears to mean that we cannot receive the CINPCAC Bulletin, despite the fact that it is given to various British intelligence organizations, and despite the fact that one of the purposes of the agreement was to put an end to the situation in which the British were receiving material from the Navy which the Army did not receive.

(ii) *Japanese fleet movements and locations.*

12. Major Snow was instructed to select and transmit to Special Branch only those items relating to the Japanese fleet as represented major concentrations or movements. Insofar as the fleet itself is concerned, the daily Summary received from Captain Smith-Hutton will probably be sufficient to supply all major concentrations and changes. However, the Navy classifies hospital ships, tankers and auxiliaries as part of the fleet. Our information covers these vessels also; and to deny us the correlating information is to impair the value of our own intelligence material.

13. Moreover, communications dealing with the fleet, or elements of the fleet, may be of interest and value in a great many incidental ways; and no one can determine what value they may have until he has received and studied the material over a period of time.

(iii) *Japanese Naval Air items.*

14. No one dealing with Japanese Air intelligence can work simply on Army or simply on Navy material. An accurate picture of Japanese Air strength, dispositions, production, wastage, etc., can be obtained only by keeping up with both services. We do not intend to give the Navy Air material detailed processing, but we do want to have it at hand for the purpose of familiarizing ourselves with the type of material and spotting major pieces of information.

(iv) *OPTELS.*

15. The significance of this limitation is not understood. It is assumed that the OPTELS are received from the British Admiralty. If they bear any relationship to the Ultra problem in the Pacific they should be included in the exchange.

C. *Proposed scope of material to be released by Navy.*

16. Op 20-G's memorandum (TAB A) provides that the material to be released to the Army "shall ih- clude only that which concerns the Japanese Army." Apart from the well-proved principle that intelligence of value can often

be obtained from messages bearing no apparent relation to the subject of interest, the restrictlon is believed to be unsound, because the war against Japan is not being conducted by Navy against Navy and Army against Army. Where the U.S. Navy operates it is fighting the Japanese Navy and Army, and the U.S. Army is fighting the Japanese Army and Navy. The Army traffic and the Navy traffic are interrelated parts of a sum total of Japanese military communications. They cannot be separated without losing an important part of their potential intelligence yield.

D. *Proper Interpretation of Agreement.*

17. There is only one sound basis for exchange of cryptanalytical intelligence, and that is to permit the consumer to determine what may be of value to him. This is the system under which the British operate, and it accounts in large measure for their success in this field. In the Watch Room at Bletchley Park, representatives of each of the 3 Services determine for themselves what may be of interest to the Ministry and field Commanders whom they represent. So much emphasis do the British put upon this point that, after all the operations of Bletchley Park have been completed, every piece of paper produced, in the way of transmitted messages, paraphrases or reports, is put through a so-called "Intelligence Exchange" where a representative of each Service checks the whole output, in order to make sure that his Service has not been omitted from the distribution list for any paper that it might find of interest.

18. There may be special cases in which a particular message may be of such a dangerous character, from the angle of security, that the originating Service might not want to give it any circulation at all. Such cases are provided for by the last paragraph of the Army-Navy Agreement. Such cases, however, should be very rare.

19. To be of value to the Special Branch, the liaison arrangement with the Navy must permit the liaison officer a wide discretion in the selection of material for transmission to the Special Branch. If only for the purpose of educating the personnel of the Special Branch dealing with particular subjects, it is necessary at the outset that he select everything except items which are obviously too trivial or which have to do with very specialized subjects such as promotions of minor Naval Officers, from which the Special Branch would probably not obtain anything of intelligence value. This was the understanding under which the liaison arrangements were worked out and the arrangement recommended for approval. If the Navy is unwilling to commit ltself to this principle, then it is recommended that steps be taken to abrogate the agreement and return to the status quo.

20. Restoration of the status quo would not be a desirable solution of the problem because it is certain that the adding up of Army and Navy radio intelligence would produce a sum total of intelligence greater than could be produced by the 2 organizations working separately. Such a solution at this time, however, would not hurt the Army as much as the Navy's noncooperation has hurt us in the past, because we are rapidly getting to the point where we will have an independent basis for intelligence in the Pacific and the Far East, and at the present rate of

progress we could struggle along without the Navy's cooperation.

21. If the Navy is unwilling to accept the interpretation of the Agreement which we consider reasonable, and which was our basis for recommending it, then it is believed that all cooperation with the Navy in the radio intelligence field should be suspended. Specifically, it is recommended:

a. That the Signal Security Agency no longer furnish intercepted Navy traffic to the Navy;

b. That the service performed by the Signal Security Agency for Op 20-G, in collecting and transmitting weather traffic, be discontinued on 30 days' notice;

c. That exchange of traffic in the diplomatic field be suspended; and

d. That the Special Branch discontinue furnishing the Navy with its reports and studies.

E. *European Intelligence.*

22. The Navy has never been willing to agree to any exchange of radio intelligence affecting the European Theater. It receives what is provided by the Special Branch, but it contributes nothing from its own sources or from the British Naval sources. Further than that, the Navy has refused to permit the British to furnish the War Department with any intelligence from British Naval sources.

23.When the Navy first proposed to do business on the intelligence level, it was our impression that the agreement would be general, covering all theaters of operation. It developed, however, that the Navy was unwilling to agree to any exchange except for the material relating to Japan. It was suggested by the Navy negotiators, however, that once the first step had been taken and a suitable arrangement worked out for the Japanese traffic, an agreement covering other areas might also be worked out in due course.

24. In view of the attitude now taken by the Navy, it is apparent that they will do business only when they have something to gain, and that there will be little prospect of extending the existing agreement to the European Theater. It is therefore recommended, independently of whether a modus vivendi is arrived at for Japanese material, that Special Branch be instructed to discontinue furnishing to Cominch any intelligence relating to the European Theater.

25. It is now apparent that the Navy proposes to do business at arm's length. We should accept that attitude and act accordingly, giving the Navy nothing which our agreements do not require us to give and holding strictly to the letter of the agreements. After a year and a half of dealing with the Navy in this field, it is my conviction that you cannot do business with them in any other way, and that you will get more in the long run if you take this viewpoint.

CARTER W. CLARKE
Colonel, General Staff
Chief, Special Branch, MID

From SRH 043. *In the fall of 1944, Army Chief of Staff General George C. Marshall became concerned that the fact the United States had been reading enciphered Japanese traffic prior to the Pearl Harbor attack might be disclosed in the course of political debate in the forthcoming presidential election campaign. He wrote a personal letter to Republican presidential candidate Thomas E. Dewey urging him not to make any statements that might compromise American successes in cryptanalysis. Portions of this letter are quoted in the document SRH 349, which appears earlier in this volume. The letter was hand-carried to Dewey by Colonel Carter W. Clarke, Deputy Chief of the Military Intelligence Service and former head of the Special Branch. This is Clarke's personal account of his unique mission. In the end, Dewey did not make any secrets public, but it took some persuading.*

STATEMENT FOR RECORD OF PARTICIPATION
OF BRIG. GEN. CARTER W. CLARKE, GSC
IN THE TRANSMITTAL OF LETTERS FROM
GEN. GEORGE C. MARSHALL TO GOV. THOMAS E. DEWEY
THE LATTER PART OF SEPTEMBER 1944

* * *

In the forenoon of Monday, 25 September, I was asked by Maj. Gen. Clayton Bissell, A. C. of S., G-2, if I was known personally to Gov. Thomas E. Dewey, Lt. Gen. Hugh A. Drum, or any of Gov. Dewey's entourage or close associates. I stated that I did not know and, so far as I knew, was not known to any of these people. Gen. Bissell later informed me that I would be directed to take a letter to Gov. Dewey at Tulsa, Oklahoma, Gov. Dewey's next stopping point on his trip east from the West Coast. Later in the day, in the office of Col. Frank McCarthy, Secretary of the General Staff, I was given the letter to read, to check for accuracy of technical details. Later in the day I was informed by Gen. Bissell that I should travel in civilian clothes and, if possible, make my contact with Gov. Dewey unknown to any other person, but that under no circumstances was I to disclose to anyone except Gov. Dewey my mission or the contents of the letter, nor was I to give the letter to Gov. Dewey unless we were the only two present in the room at the time.

I left the Pentagon Building early in the afternoon of Monday, 25 September, and went home in order to get my civilian clothes out of storage and have them pressed in preparation for the trip. After dinner I returned to the Pentagon Building, where I received orders from Major Earman at 1942 EWT, Monday, 25 September. Went to airport and got off ground at 2040 EWT. Landed at St. Louis for fuel at 2330 CWT. In air again 2400 CWT and landed in Tulsa at 0150 CWT. Slept in

Hotel de Gink. Up at 0700. Phoned Gen. Bissell at 0730. Went to Meyo Hotel, had breakfast and phoned Roger Randolph at 0820. Got haircut and shave and saw Roger Randolph at O905. He contacted Mr. William Skelly, President of the Skelly Oil Company. Mr. Skelly was Gov. Dewey's campaign manager and was handling all arrangements. Went to Mr. Skelly's house and made arrangements to meet him in private hotel room in Tulsa Hotel. Met Mr. Skelly as agreed at 1600. He saw Gov. Dewey's Secretary who came down twice to insist that he know who I was and what I wanted. No one knew anything about the case except that I had a letter that had to be delivered to Gov. Dewey personally and alone. Finally he said, "You must write down the name of the man who has sent you, seal it and give it to Gov. Dewey." I did this, and after being gone 16 minutes, he returned and said Gov. Dewey would see me.

I saw Gov. Dewey alone, delivered the letter and asked that I not read it aloud. Gov. Dewey opened the outer envelope and then said, "Well, Top Secret - that's really top isn't it?" He read the first two paragraphs and then stopped. He asked if I were a Regular Army officer. When I said yes he asked if I would give him my word of honor that I had been sent by Gen. Marshall. I said I would. He then said he did not want his lips sealed on things that he already knew about Pearl Harbor, about facts already in his possession or about facts which might later come into his possession from other sources but which, if they were contained in Gen. Marshall's letter, could not be used because he had given his word on this letter, thereby sealing his lips. He said he would be glad to discuss this matter with me now. I told him I was merely a courier and was not authorized to enter into any discussion about what he knew about Pearl Harbor or about the contents of this letter. He then asked if I was authorized to say to him in the name of Gen. Marshall that if he read the letter through and then stated to me that he already had in his possession the identical information that was contained in the letter, that he would then be released from all obligations to keep silent. I said I had no such authority. He then said he could not conceive of Gen. Marshall and Adm. King being the only ones who knew about this letter. Furthermore he said he could not conceive of Gen. Marshall approaching an "opposition candidate" and making a proposition such as was apparently contained in that letter. He said "Marshall does not do things like that. I am confident that Franklin Roosevelt is behind this whole thing."

All this time the letter was lying face down in his lap. He then picked it up and said "Let me read those first two paragraphs again." He started to read, then laid the letter down and said "I have not reread them because my eye caught the word "cryptograph." Now if this letter merely tells me that we were reading certain Japanese codes before Pearl Harbor and that at least two of them are still in current use, there is no point in my reading the letter because I already know that." He then said "That is the case and I know it, isn't it?" I said, "Governor, I am merely a courier in this case." He said, "Well I know it and Franklin Roosevelt knows all about it. He knew what was happening before Pearl Harbor and instead of being

reelected he ought to be impeached." He then said "Would you like for me to phone Gen. Marshall and say to him what I have just said to you?" I said "Governor, this is a subject that should not, under any consideration whatsoever, be discussed or even mentioned over the telephone." He handed me back the letter saying, "I shall be in Albany Thursday and I shall be glad to receive you or Gen. Marshall or anyone Gen. Marshall cares to send to discuss at length his cryptographic business or the whole Pearl Harbor mess." He continued, "I can arrange it so the conference can be held in absolute secrecy." I then put the letter back into the envelopes, thanked him for his courtesy in giving me so much of his time, and departed. I then left the hotel, went to the field, phoned Gen. Bissell. Took off at 1815 CWT 26 September.

I arrived at Washington airport at 2245 EWT 26 September. I phoned Gen. Bissell and asked if it was necessary for me to make my report that night. He said "No but be in the office early the next morning in order that we may report to the Chief of Staff."

About 0740 on the morning of 27 September, accompanied by Gen. Bissell, I made oral report to Gen. Marshall as indicated above, leaving with him at that time Gen. Marshall's letter which I had taken with me to Tulsa and brought back on my return trip.

Later in the day on Wednesday, 27 September, I was informed by Gen. Bissell that on the following morning I was to go to Albany to contact Gov. Dewey and to give him another letter which had been prepared by Gen. Marshall. At 1008 on 28 September I took off from Washington airport and landed at Albany at 1205. Went by taxi direct to the State House. Arrived there at 1250. Contacted Gov. Dewey's office and was put in touch with Miss Ross, his private secretary. She asked who I was and what I wanted. I told her that I was same individual who had contacted Gov. Dewey last Tuesday in Tulsa and that I was there at Gov. Dewey's invitation with another letter and message for the Governor. She left to phone and in a few minutes came back saying that Gov. Dewey desired me to come right over to the Executive Mansion. I arrived there at 1330 and was taken directly to Gov. Dewey's reception room. Present were Gov. Dewey and a man introduced as Mr. Elliott V. Bell, Superintendent of Banks, State of New York. I stated to Gov. Dewey that at Gen. Marshall's direction and in accordance with Gov. Dewey's invitation extended in Tulsa, I was there to present him a letter and message from Gen. Marshall and to answer any questions of a technical nature that the Governor might care to ask after a reading of the letter. Gov. Dewey asked if it were the same letter I had in Tulsa. I said no but that it was on the same subject and that the meat of the letter was the same. He then asked if I still had instructions to see him alone. I replied that I had. He next asked if I could leave the letter with him. I said no that I was to return the letter to Gen. Marshall. He asked if I were authorized to discuss the contents of the letter with him. I stated that I could discuss the technical features of the case freely and could answer any technical questions on the subject that he might care to ask.

Gov. Dewey then said that, in view of the circumstances, his own personal position, in view of what he already knew, to say nothing about what he might later learn, and particularly in view of his trusteeship, he had decided that he could not see me or anyone else alone, that he would not read a letter which he could not keep and which he could not show to and discuss with Mr. Bell, nor would he enter into any further discussion without Mr. Bell being present. He said he could not afford to read a letter he could not keep as he might later be charged with reading a letter different from the one he had really read. He said I might be curious to know whether or not he had a recording device in the room. I said "No, Governor, I am not curious; I merely assume that you have one." He said "Well I haven't and I did not ever have one when I was District Attorney. I had one in my witness room, of course, but never in my own private office." He next said, "Now Colonel, Mr. Bell is an American citizen and is just as patriotic as any member of the Administration. He already knows all the facts that I know in regard to Pearl Harbor and I certainly intend that he know the contents of the letter if I read it. If I keep the letter I shall put it in my vault and no one but Mr. Bell and myself shall know of its existence or of its contents and we shall discuss it only between ourselves. Furthermore I do not see what Gen. Marshall is so exercised about. There are at least 12 Senators that I can name for you right now if you desire that know all there is to be known about Pearl Harbor and about how we were reading certain Jap codes before Pearl Harbor and how it is claimed that we are still reading two of these same codes. You know, Colonel, this code business is the worst kept secret in Washington, but I for one want to say to you that I do not believe any such thing as that to be a fact."

I said, "Well, Governor, whether you believe it or not, it is a fact and I am willing to take an oath to that effect right here and now. Let me assure you that Gen. Marshall's sole interest in this matter is to protect our most vital source of intelligence and to save the lives of thousands of troops that are certain to be sacrificed if security on these ciphers is blown and the Japanese change them." I then said, "There are many other aspects of this case that I would like to tell you but I feel that you should read the letter first."

He sat silent for about three minutes then said, "Why don't you phone Gen. Marshall and tell him that I will not discuss the matter with you unless Mr. Bell is present, nor receive the letter unless I can let Mr. Bell read it and then I keep it?" I said that I did not want to phone from the Executive Mansion but would go to a pay phone and call; that if I were unable to reach Gen. Marshall I would fly back to Washington at once, deliver Gov. Dewey's message, and return to Albany tonight and be available to see him (Dewey) early tomorrow morning. He said, "Well I have a direct line in here and I have a line that goes through the switchboard and there is no tap on either of them unless O'Connor has just put one on. I have them checked several times a week so I feel that they are safe." I asked who O'Connor was and he said he was the Democratic leader here in Albany. I said, "Well I prefer not to have the phone used in this case." He said, "Oh hell, I'll

phone Marshall, I've talked to him before and this will be all right." He then picked up the phone and put in a call to Gen. Marshall. While waiting for the call, which took about seven minutes, Gov. Dewey said, "If, as you say, the Japs are still using two of their codes that they used before Pearl Harbor, why in hell haven't they changed them, especially after what happened at Midway and the Coral Sea?" I explained the difference in the types of codes and ciphers used by the various Jap agencies, their distribution problems: and gave the reason we think the Japs have not changed these codes. He then asked why Gen. Marshall was so anxious to stop him from talking when everyone else in Washington knows the story and is talking about it. Just then the call was completed and he talked to Gen. Marshall in re the letter and about Mr. Bell. He then gave the phone to me, and Gen. Marshall authorized me to give the letter to Gov. Dewey, to leave it with him and to discuss the case technically in the presence of Mr. Bell.

As I was opening the envelope Mr. Bell said, "Colonel, hundreds of people know all about the Midway affair and how most of our other successes in the Pacific have been due to our reading Jap naval codes. Everyone who has ever been out there knows about it and talks freely about it. Why not long ago at a dinner where a large number of people were present I talked to a naval commander who had been out there and had participated in nearly every engagement we have had. He said that they always knew where the Jap ships were and that our people were told by radio where to station their own ships to meet the Japs, and that all this information came from reading Jap codes."

Gov. Dewey said "Yes and I have lots more information about the pre Pearl Harbor messages you were reading." He then took the letter and started to read.

Mr. Bell said, "Tom, do you want me to read it over your shoulder?" Gov. Dewey said "No I'll hand it to you a page at a time." Gov. Dewey continued to read, then put the letter down and said, "Well I'll be damned if I believe the Japs are still using those two codes." I again assured him that they were and that one of them was our life blood in intelligence. The letter was still in his lap when I said "Governor, I would like to repeat that I know that Gen. Marshall's sole interest in this case is to preserve the only worthwhile source of intelligence that this nation has. You do not realize it but the War Department has 10,200 people working in the Signal Security Agency; the Navy Department has almost 6,000 in their Communications Annex, and both the Army and Navy each have several thousand in tactical field and fleet units engaged in signal intelligence work.

* * *

Gov. Dewey said "Yes, Gen. Marshall just said that we had over 10,000 on that work."

I then stated that Churchill considered this his secret weapon and that it had really saved England. I described how Churchill felt about security, how the Navy

prized it so highly and how difficult it had been to break down British resistance because of American lack of security consciousness. I quoted to him Churchill's reported statement about protecting this source, how that in order to protect the source the British had time and again permitted convoys to be attacked rather than divert them from their course and thus blow security.

Gov. Dewey then picked up the letter and read some more. Then he put it down and said "Is this true about the OSS?" I said it was. He said "Well I don't feel towards the OSS like most of the Army and Navy people I have talked to. I have a lot of my men in it and they are all damn good, excellent fellows in fact, and they tell me that we have no really trained intelligence personnel in either the Army or Navy. They say that in both the Army and Navy the officers are merely on temporary detail and that they then go to sea or back to a regiment or somewhere, and that most of the officers of both services are woefully ignorant of world affairs. I suppose that may be the real reason for taking no action on the Pearl Harbor warnings they had—they could not interpret the warning."

Mr. Bell then said "Well it don't account for them not doing anything about that message that gave them the warning that Japan was going to attack the United States—you know the one I mean—where they set the deadline for Kurusu for November 25 and then postponed it till November 29 saying to get done with their negotiations by that time or that things would automatically begin to happen. Anyone should have known that that meant they were going to attack the United States. That was just the time limit on sailing dates."

Gov. Dewey said "Yes that's right." Mr. Bell then said "Those messages you did not get till December 8 and after, why did it take so long for you to receive them?" I said "I do not know what you are referring to, but before Pearl Harbor all our traffic intercepted on the West Coast, Hawaii and elsewhere was sent in by air mail which of course delayed it."

Gov. Dewey then read the letter through and handed the last page to Mr. Bell. After Mr. Bell had finished reading, he handed the letter back to Gov. Dewey. After a minute or so Gov. Dewey said "Well, except for the matter of the two codes and the OSS, there is little in this letter that I did not already know. There is one point though, what in hell do Jap codes have to do with Eisenhower?" I explained the linkage with a general statement on the three types of ciphers used by G.A.F., Abwehr, Clandestine, German Navy, Oshima's visits and interviews, etc. He seemed satisfied. He then said "Colonel, I know a hell of a lot about this business. You probably know that some years ago when Stimson was Secretary of State he got very damn pure minded one day and stopped all such things as this. He afterwards denied that he had done it but said he was acting on orders from President Hoover. Well, as you know, the man who headed the cryptographic work of the Government was Yardley who was fired by Stimson. Yardley was a friend of mine in those days and I am the man who stopped Yardley from publishing his second book. I met him in a speakeasy one night and persuaded him against publishing the

book. He agreed provided that Mr. Stimson write him a letter of apology for the abusive manner in which Stimson had fired him. Stimson did, too."

I did not comment on this other than to say I was quite familiar with the Yardley case. I then asked if there were any questions the Governor or Mr. Bell would like to ask. Gov. Dewey said "Not just now but I would like to discuss this case with Mr. Bell." I got up to go out of the room into the hall but Gov. Dewey said "No you stay here, we will go across the hall." I sat down and Mr. Bell said "Well, Governor, we have pledged ourselves not to discuss this letter with anyone else but just between ourselves but what about Colonel Clarke—who is he going to discuss it with?" Gov. Dewey said, "Oh he will of course report this conversation to Gen. Marshall—is that not correct?" Before I could reply Mr. Bell said "Yes but with who else?" Gov. Dewey said "Anyone else?" I said, "I shall report to my immediate superior, Major General Clayton Bissell, A. C. of S., G-2, War Department, and through him to Gen. Marshall and to no one else."

They then got up and left the room, leaving the letter on a stand by Gov. Dewey's chair. They were gone about 22 minutes. When they returned Gov. Dewey said "Let me look over this letter again and read carefully a couple of paragraphs." When he finished he said, "Well, Colonel, I do not believe that there are any questions I want to ask you nor do I care to have any discussion about the contents of the letter. Will you give me your full name, serial number, office location and phone number, and your residence address and phone number?" I did this and he thanked me and asked where I was staying. I told him I was flying back to Washington tonight and was going direct to the airport. I then asked him if he had any message that he wanted me to take to Gen. Marshall. He said "No, no message." I thanked him for giving me so much of his time. He shook hands and said "Well I hope we meet again under more auspicious circumstances." I said goodbye to him and to Mr. Bell and left for the airport at 1610. Next I phoned Gen. Bissell and to plane. In air at 1645.

I arrived at Washington Airport 1855 and phoned Gen. Bissell advising him of my return and asking if it was desired that I make report that night. He answered in the contrary but directed me to be in the office early the following morning in order that we might make report to the Chief of Staff. Again about 0740 on Friday, 29 September, accompanied by Gen. Bissell I made my second report to Gen. Marshall as indicated above.

CHAPTER IX

Tactical COMINT

The Army signals intelligence effort was a divided one in World War II. At the national level, the Signal Security Agency provided high-level cryptanalysis. The intercept arm of the agency was the 2d Signal Service Battalion, which maintained large fixed intercept stations in a number of locations in the Continental United States and around the globe. However, in the field, theater commanders directed a separate tactical effort through theater-level signal intelligence services, which controlled a multitude of signal radio intelligence companies and (in Europe) smaller signal service companies. By the end of the war, numbered Army Air Forces also had their own signal intelligence elements in the form of Army Air Forces radio squadrons, mobile. The diversity and scope of the tactical effort is shown by the following excerpted documents: SRH 124, Operational History of the 849th Signal Intelligence Service; SRH 048, Summation of Operational Activity, Signal Service Detachment "D"; SRH 042, Third Army Radio Intelligence History; and SRH 227, History of the 126th Signal Radio Intelligence Company. The excerpt from SRH 049, Technical Intelligence Transmitted Directly to G-2 12th Army Group, ETO From 14 August 1944 to May 1945, contains one day's intelligence "take" from tactical COMINT efforts in Europe. It demonstrates what could be gleaned from radio direction-finding and the exploitation of low- and medium-level German ciphers.

From SRH *124. Excerpts from the official history of the Army's signal intelligence service in the Mediterranean Theater of Operations. The account shows the slow evolution of Army signals intelligence organization in the field as the result of lessons learned in actual combat operations. As a matter of interest, the 849th Signal Intelligence Service was the only World War II theater signal intelligence service to be assigned a numerical designation.*

OPERATIONAL HISTORY
of the
849TH SIGNAL INTELLIGENCE SERVICE

Mediterranean Theater of Operations
United States Army

* * *

PART I: BEGINNINGS

GENERAL

1. It was originally planned that all U.S. signal intelligence activities at AFHQ would be handled by a unit entitled Signal Intelligence Service, AFHQ, the commanding officer of which would be a member of the Chief Signal Officer's Staff. A T/O and an SLOE were submitted to the War Department on this basis. These were approved, but the unit was redesignated as the 849th Signal Intelligence Service, and it was decided that the unit would not constitute the Signal Intelligence Division of the Signal Section, but would work under that division in a separate location of its own at some distance from headquarters. Since there was no basis of experience in contemporary warfare on which to build, the original T/O merely represented a careful guess as to what the function of such an organization in an active theater of operations should be, and what personnel would be necessary to perform them. The organization, being unique, was not referred to in any T/BA: and the Special List of Equipment, which was its only basis for drawing supplies, would have been markedly inadequate in any case. The fact that it was not modified in any way to conform to the change from a staff section to a field unit multiplied this inadequacy. As a result, the unit set up in an isolated ravine in North Africa, without a telephone, a foot of field wire, a radio set, or a power unit, to mention only a few of the more obvious necessities. Many of these items would have been provided automatically for a staff section, but to procure (and keep) them for a field unit, entitled only to T/E and T/BA allowances has involved a com-

plicated and continual struggle.

2. In order to take advantage of greater British experience in intelligence operations, the 17 officers, and 90 EM called for in the Cryptanalytic and Radio Intelligence Sections of the Intelligence Branch were activated at Fort Dix on 8 November 1942 as Signal Intelligence Detachment 9251-A, under the command of Capt. [text withheld]....The Detachment left for England on 24 November. It was only upon their arrival in Africa, three months later, that the members of this group learned that they were earmarked for the 849th SIS, of which they had never heard. On 2 December 1942 the 849th SIS was formally activated at Fort Devens, with Capt. [text withheld] in command. Assigned to it at this time were 16 officers and 102 EM, which, with the personnel of Detachment 9251-A made up the exact number called for on the T/O. Captain [text withheld] was under the impression that the personnel of Detachment 9251-A had also been assigned, and no evidence was available by which this impression could be corrected. The unit was therefore apparently up to full strength; but the C.O. was junior to Capt. [text withheld] who had originally been intended merely as a section head. In general, technical qualifications and relative rank were so poorly adjusted that it was clear that one or the other would have to be disregarded unless additional officers were brought in at the top. The fact that the organization, including the detachment in England, contained only six officers above the grade of second lieutenant and none above the grade of captain, while the T/O called for a colonel, two lieutenant colonels, and seven majors suggested that this was very likely to happen.

a. It did happen on 14 January 1943, when five officers from SIS, Western Task Force and three from SIS, AFHQ were assigned by NATOUSA orders to the 849th SIS, which embarked from NYPE the same day. This group included Major [text withheld] Commanding, and Capt. [text withheld] selected as OIC, Intelligence Branch. Twenty seven enlisted men from the same sources were also assigned to the 849th SIS, a site was found at Hammam Melouane, and operations were begun on such a limited scale as was possible. On 1 February the main body of the 849th personnel arrived, and Capt. [text withheld] was designated OIC, Security Branch. On 20 February, Signal Intelligence Detachment 9251-A, less three officers and twelve men left in England for further training, arrived and was assigned to the 849th. The organization was now considerably above its authorized strength, particularly in officers; but in the midst of the general confusion this fact escaped unfavorable comment. The key position had been filled, the general shakedown process was well under way, and the organization was ready to begin full scale operation under the supervision of Colonel Harold G. Hayes, SIS officer, AFHQ. It must be confessed that the question of what these operations were to be still needed a good deal of clarification.

b. Three major policy problems had to be faced:

(1) Coordination with the [text withheld] whose intelligence and security organization does not parallel our own.

(2) Determination of the levels at which various SIS activities were to be carried on and the inter-echelon coordination of these activities.

(3) Adaptation of radio intelligence organizations to the intelligence and security needs of the theater. In addition there were the continually developing problems of procuring and training personnel, procuring, modifying, and improvising equipment, selecting specific commitments and devising techniques to meet them, etc.

3. After these three problems and those of supply had been solved to a degree which permitted operations to begin, another and more difficult problem became apparent as soon as the 849th SIS began to serve other headquarters. This was the non-acceptance by many commanding and staff officers of the benefits, intangible tho many were, resulting from an adequate signal intelligence program.

a. The Intelligence Branch met this problem in the reluctance with which American tactical staffs first allowed Detachments of the Branch to operate in combat areas, where tactical information available to intercept and cryptanalysis was most abundant. It was believed that such an apprehension for the safety and security of signal intelligence operations was founded on a general ignorance within the then new American tactical staffs of the role which signal intelligence could play in combat operations and an unfortunate misconception in the same quarters of how the exploitation of German Army low-security radio traffic could best be accomplished. American tactical commands, unfamiliar with signal intelligence services, were not anxious for the information which signal intelligence could supply, and were at first skeptical of the validity of some of the information produced by the Detachments. Furthermore numerous serious security violations were at first made by tactical commands in handling signal intelligence information, illustrating the general lack of appreciation for signal intelligence methods in tactical commands.

b. Unlike the [text withheld] in North Africa, whose staffs had become thoroughly familiar with tactical signal intelligence operations as a result of the desert campaigns, the new American staffs in Algeria and Tunisia had to be indoctrinated with the manner and value of signal intelligence work. The critical period of "selling" signal intelligence to American staffs as an integral intelligence function in forward areas occurred during the invasion of Sicily. Detachments "A" and "E" of the Intelligence Branch were originally scheduled to go ashore in Sicily with the Headquarters Seventh Army and the reinforced 3rd Division (VI Corps), Detachment "A" to land as soon as a beachhead of 10 square miles had been secured, Detachment "E" to land within a few days after D-Day. Concern for the security of signal intelligence personnel and operations resulted in Seventh Army Headquarters holding the Detachments in North Africa until 7 August (D + 30), and the units did not land in Sicily until 10 August, one week before the end of the Sicilian campaign. With such a short period remaining for operations before the

conclusion of the campaign the achievements of American signal intelligence units in Sicily were obviously not impressive. The Detachments furnished valuable tactical information throughout the short period; but their greatest contribution, which would have been possible in the early days of the campaign, when enemy strengths and dispositions were largely undetermined, was lost to the Allied effort.

c. Gradually, however, American tactical commands developed greater appreciation for intercept intelligence and the problems involved inproducing such intelligence; and in time signal intelligence was considered at all times to be a dependable source of intelligence and under some conditions to be the best source of information concerning enemy tactical forces available to American Army and Air force tactical commands. That Detachments were in time allowed to operate in forward combat areas where tactical information was best intercepted is demonstrated by the fact that two Intelligence Branch Detachments landed at Anzio on D-Day and were scheduled to land in Southern France on D-Day but were held up until approximately D + 5 because of confusion in shipping schedules.

d. Early, effective operations by the Security Branch were hindered through a failure of staff and unit officers to appreciate or even realize that all signal security efforts were directed at protecting them and their units from enemy action. It was this factor which made it impossible to correct quickly the uniformly low state of signal security training with which American troops entered North Africa. The general attitude towards signal security was that it consisted of a set of cumbersome regulations, and the reaction varied according to temperament. Many officers were frankly hostile, considering all SIS personnel as parasitical non-combatants conspiring to complicate the jobs of honest fighting men. Others, having developed a philosophical resignation toward all regulations, were almost pathetically eager to comply with whatever was published;....In operations, the first reaction resulted in so many messages passed in clear and others so carelessly enciphered that it looked like a conspiracy to ignore as many security provisions as possible and in the second, resulted in an attitude which said in effect "put it in some sort of code, that is what the book says". The idea that the enemy might use intercepted information with unfortunate results to themselves was almost entirely absent. It was only after the loss of much valuable time and intense missionary work that an understanding of the purpose of signal security was achieved.

e. Time and further contact with the enemy brought changes in these attitudes. By the close of hostilities in the MTO the importance of signal intelligence was well accepted as an essential part of a complete military effort and the 849th was being called upon to perform many functions in addition to its primary mission. That all aspects of signal intelligence activities were eventually appreciated in Mediterranean Theater of Operations can best be illustrated by the 70 letters of commendation and 42 awards received by approximately 400 individuals of the 849th SIS. . . .

4. Attached. . .is a table of personnel originally allotted to the 849th SIS. It is shown here with the caution that it proved inadequate for signal intelligence activities in MTO and that at best can only be used as a guide in planning similar units since SIS functions appear to vary greatly from theater to theater. The scope of the 849th early increased beyond the bounds of the T/O. The personnel problem however was alleviated to a large extent by the assignment of an AFHQ Signal Intelligence pool of 27 officers and 284 enlisted men and an AFHQ Cryptographic pool of 29 officers and 323 enlisted men. While this appears to be a tremendous increase over the T/O, the 849th also took over the mission of those two pools. The additional personnel permitted the headquarters section to be augmented where needed and permitted a shifting of officers and men to meet the ever changing operational demands, all of which greatly increased the effectiveness of the 849th SIS.

PART II: INTELLIGENCE BRANCH

GENERAL FUNCTIONS

1. Introduction.

a. The basic duties of the Intelligence Branch were clear in principle from the date of activation of the 849th SIS: to derive intelligence from enemy radio transmissions. At that date, however, the multiple forms which Intelligence Branch functions would later assume and the many problems which were to be encountered in fulfilling those duties could not be foreseen.

b. Before the end of hostilities in Europe the Intelligence Branch would develop from a handful of personnel to a complex organization whose activities included: three Detachments fulfilling signal intelligence commitments at U.S. Corps (II, IV, VI) Headquarters, involving the interception and analysis of German Army low-security radio traffic; two similar Detachments fulfilling similar commitments at U.S. Army (Fifth, Seventh) Headquarters; one Detachment analyzing German Army medium-security traffic; two Detachments providing the Mediterranean Allied Air Forces with information derived from the analysis of German Air Force low-security and plain-language (voice) radio transmissions; one Detachment analyzing enciphered European weather broadcasts emanating from within enemy-held territories for the 12th and 15th U.S. Air Forces; one Detachment analyzing [text withheld] radio traffic and later providing the Office of Strategic Services with information from a study of clandestine radio traffic of enemy agents in Allied controlled territory; one Detachment providing the Civil Censorship Group of the Allied Control Commission with information from the analysis of secret inks and other types of unauthorized correspondence; and a Headquarters whose operations included, in addition to routine administrative functions, a continuous supply of technical intelligence and information to the Detachments in the field, research into the German communications systems, solu-

tion of German Army medium-security traffic, a Communication Section to provide all communications between the Headquarters 849th SIS and its Detachments and other Headquarters, and a Laboratory Section for reproducing important captured documents and photographing materials of all kinds.

c. When the Intelligence Branch began operations in North Africa during the winter of 1942-43 radio intercept and the cryptanalysis of enemy low- and medium-security radio traffic within an active theater of operations constituted an unexplored field for the new United States Army. Consequently, the growth of the Intelligence Branch was attended by many restrictive elements. [text withheld] It had been arranged to have several Signal Radio Intelligence Companies provide all American radio intercept facilities required within the theater, operating in conjunction with, but independent of, Intelligence Branch cryptanalytic Detachments; and it was not long before such an arrangement presented a number of shortcomings. Inadequacies in the 849th SIS T/O presented additional difficulties to the development of the Intelligence Branch; and the invariable insufficiency of training of all newly-arrived personnel from the United States and London was another stumbling block to the proper expansion of the Intelligence Branch. Finally, the problem of equipping each newly organized detachment was complicated by grave inadequacies of the T/E of the 849th SIS.

2. Cryptanalysis.

a. In order to limit to a reasonable extent the scope of work to be performed by the Intelligence Branch, consideration being given to the number of personnel available and to their state of training, it was planned originally that the work of the Branch would involve at first only the study of German Air Force low-security radio traffic. Such traffic consisted of radio activity of the German Air Forces operating throughout the western and central Mediterranean area, involving transmissions of both enemy aircraft and ground radio stations. [text withheld] With this type of traffic in mind the first operational unit created within the Intelligence Branch, eventually called Detachment "F", was formed in February 1943. Personnel of this Detachment underwent preliminary training [text withheld] near Algiers, and by the summer of 1943 were ready and able to assume an independent signal intelligence operational commitment.

b. After the personnel of Detachment "F" had commenced their training and additional personnel were available to the Intelligence Branch consideration was given to another type of enemy radio traffic, German Army low-security traffic, most of which emanated at regimental level and below. This traffic consisted of [text withheld] jargon codes, simple substitution ciphers and transposition systems, and was fairly easily broken also by elementary cryptanalysis when sufficient depth was encountered. At the end of February a small group of personnel was attached to [text withheld] United States II Corps in Tunisia to learn the techniques of analyzing such German Army low-security traffic. These people formed the basis of what later became Detachment "A". As time went on additional

detachments were formed to perform the same type of cryptanalytic functions as Detachment "A", and eventually there were five detachments exploiting such German Army low-security traffic: Detachment "A" at Headquarters Fifth Army, Detachment "B" at Headquarters Seventh Army, Detachment "E" at Headquarters U.S. VI Corps, Detachment "H" at Headquarters U.S. II Corps, and the 3916th Signal Service Company at Headquarters U.S. IV Corps.

c. During the summer of 1943 it became apparent that an additional cryptanalytic task could be undertaken by the Intelligence Branch. The Army Air Forces were in need of the information which could be derived from enciphered European meteorological radio transmissions giving vauable weather data over enemy-held territories. Work on this material was begun in July 1943 with the formation of Detachment "G". International Business Machine equipment was obtained; techniques for breaking the traffic were evolved; and the latest meteorological observations for enemy held territory were made available to tactical and strategic air forces in the Mediterranean area.

d. In July 1943 a further development occurred when it was found possible to attempt the solution of German Army medium-security doubly-enciphered Playfair traffic. Personnel for this task, who had been trained in the solution of German Air Force medium-security traffic in London, arrived in the Mediterranean Theater in early July. These people, who became the nucleus of Detachment "B" and later of the Solution Section at the Headquarters, Intelligence Branch, enjoyed considerable success in their solution operations whenever traffic in sufficient depth was available. The greatest difficulty encountered in dealing with such traffic, emanating usually from enemy Divisional networks, was in finding suitable sites for its interception.

e. The value of German Air Force voice traffic on Very High Frequencies (38-42 mcs), mostly plain language, had long been recognized, and in August 1943 a detachment of German linguists was formed to exploit this source of intelligence, eventually becoming Detachment "D". Personnel were assigned aboard the USS Ancon, and the group provided important intelligence of German Air Force activity during the landings at Salerno. Later the Detachment operated in the vicinity of Naples, on the Anzio beachhead, during the invasion of Southern France, and northward with the Allied forces throughout France and into Germany, working with Allied Tactical Air Commands and Fighter Wings. The same type of traffic was also exploited during more than a year's period by two groups of three enlisted men of Detachment "D" aboard United States destroyers escorting Allied convoys throughout the Mediterranean area. After January 1944 German linguists were used regularly in all Intelligence Branch Detachments serving Corps Headquarters to intercept German Army voice traffic on such Very High Frequencies (32-38 mcs).

* * *

4. Laboratory Facilities.

a. Communications Intelligence. A small section had originally been provided at the Headquarters, Intelligence Branch for the collection and study of captured enemy communications equipment. It was soon felt, however, that the section was unable to carry on its prescribed duties successfully as a subordinate part of the Intelligence Branch, and in June, 1944 the section was activated as the Enemy Equipment Intelligence Service. Having its own T/O and E, the new unit was assigned to the 849th SIS and removed from the control of the Intelligence Branch. . . .

b. Laboratory Section—Photographic and Chemical. Photographic facilities provided by the original 849th SIS T/O and E proved inadequate to the tasks which later developed, and constant additions in personnel and equipment were necessary to meet constantly greater requirements. In addition to providing photographic facilities for the 849th SIS the Laboratory Section was responsible for maintaining a laboratory to make chemical analysis of civilian and prisoner-of-war mail for secret ink and other unauthorized means of communication. Original estimates of personnel, equipment, and supplies necessary for the Chemical Subsection were similarly disproportionate to actual requirements, and a process of continuous growth was characteristic of that subsection also.

c. Communications Section—From a small group of personnel who installed telephone and lighting facilities at Hammam Melougne in February 1943 was gradually evolved a Communications Section. Although part of the Intelligence Branch the section provided communications facilities for the entire Headquarters, Intelligence Branch. In time the section expanded in size and operations until it maintained radio and teletype links with most field units.

MAJOR PROBLEMS ENCOUNTERED

* * *

a. At the opening of operations in the Mediterranean Theater [text withheld] already had a number of signal intelligence units in the field properly trained for the interception and solution of German Army and Air Force low-security radio traffic. Plans for utilizing U.S. signal intelligence personnel had not been properly integrated with the British before the invasion of North Africa; but shortly after the formation of the 849th SIS and its arrival in North Africa [text withheld] it was recognized that American units would in time be able to contribute to the North African signal intelligence effort.

* * *

2. U.S. Signal Radio Intelligence Companies.

a. Four U.S. Signal Radio Intelligence Companies—the 117th, 122nd, 123rd, and 128th- together with a number of intercept operators later assigned to

the 849th SIS itself provided intercept facilities for the several detachments of the Intelligence Branch. In a number of cases the SRI Companies were themselves split into detachments to provide facilities for new Intelligence Branch detachments formed to meet new commitments. All four SRI Companies were originally assigned to Allied Force Headquarters (AFHQ), and their operational activities were then directed by the American Signal Intelligence Officer of AFHQ.

b. Of these four SRI Companies the 122nd and 128th arrived in North Africa with the invasion forces. The operators were inexperienced with the new types of traffic they were to intercept; and until late 1944 there was an insufficient number of trained operators to meet the minimum requirements of the individual Intelligence Branch detachments and monitoring tasks which were assigned by the Monitoring Section of the Security Branch, 849th SIS.

c. Early in 1943 steps were taken to remedy the shortage of intercept operators by securing the 117th and 123rd SRI companies to supplement the first two. Before these units arrived in North Africa several important months had passed, and more months of training were required to bring the operational efficiency of all units to a point where specific commitments were possible.

d. A directive from the American Signal Intelligence Officer, AFHQ, made clear the fact that the Intelligence Branch Detachments working in conjunction with the SRI Companies were to direct the employment of sets and assign specific intercept missions. Experience proved, however, that although relations between the SRI Companies and the Detachments of the Intelligence Branch were on the whole satisfactory the degree of cooperation and efficiency obtained often depended on purely personal relationships between the officers and men of the units in question and not on any clearly defined policy of command. The separation of intelligence and intercept sections, although possible in theory, in some cases produced situations in which questions of policy and operational control were in open conflict. The fact that the Intelligence Branch Detachments had to be attached to the SRI Companies for rations, quarters, and administration produced other unsatisfactory situations that hindered proper cooperation between the two types of units.

e. A step toward remedying the situation was taken by the Army Air Forces after the assignment of the 122nd and 123rd SRI Companies to the 12th Air Force in November 1943. A plan was studied and later approved to provide a self-contained signal intelligence unit comprising both intelligence and intercept personnel. On the basis of such reorganization the 123rd SRI Company was renamed the 9th AAF Radio Squadron Mobile (G) in March 1944; after a long delay intelligence personnel were obtained for this new Squadron from the U.S., and the Squadron began to function as a complete unit in December 1944. The 122nd SRI Company was never reorganized, and continued to operate in conjunction with the Intelligence Branch Detachment "G" until June 1945.

f. A similar step in the right direction within the Army Ground Forces occurred when T/O's and T/E's were approved by the War Department in January

1945 for Corps Signal Service Companies, providing for self-sufficient organizations which contained both intercept and intelligence personnel. Detachment "H" and a detachment of the 128th SRI Company which had been operating in conjunction with Detachment "H" were combined to form the nucleus of one such Signal Service Company (3915th SS Co) in February 1945. . . .

g. Another critical handicap encountered as long as the SRI Companies and Intelligence Branch Detachments operated independently involved a theater policy concerning dissemination of signal intelligence information. According to theater regulations personnel of SRI Companies were not allowed access to technical signal intelligence information and procedures that formed the basis for intercept set assignment. Consequently SRI personnel were given only specific frequency and callsign missions daily, and were not entitled to know the basis for such missions. Such an arrangement required additional signal intelligence personnel on duty in intercept rooms supervising intercept activities to guarantee proper coverage. And in spite of such efforts many valuable minutes of intercept operators' time were often wasted by copying worthless traffic before being noticed by signal intelligence personnel on duty in the intercept rooms. Both intelligence and intercept personnel resented the restriction; but as long as they existed under separate units nothing could be done. Intercept personnel were especially resentful of the fact that they were denied access to information which would increase the efficiency of their work. The situation was corrected only when the two types of personnel were placed under one command, as in the case of the 3915th Signal Service Company; for then both intercept and intelligence personnel were allowed complete access to all pertinent signal intelligence data.

3. Procurement and Training of Personnel.

a. When the 849th SIS was activated it was expected that the Intelligence Branch would consist only of Signal Intelligence Detachment 9251-A; but, in fact, it was subsequently composed of several heterogeneous groups, each trained for different tasks. SID 9251-A, after preliminary training in cryptanalytic methods for a short period at Vint Hill Station, USA, embarked for SIS ETOUSA in November 1942 for practical experience in processing traffic from both German Army and Air Force units. Of this group 14 officers and 77 enlisted men were sent to the 849th SIS in February 1943, leaving 3 officers and 13 enlisted men in London (eventually to become nucleus of Solution Section, Headquarters Intelligence Branch) to deal operationally with German Air Force medium-security traffic.

b. During January 1943 the intelligence members of the Western Task Force SIS Section consisting of 2 officers and 6 enlisted men having completed their duties in Morocco, had set up their headquarters at Hammam Melouane, near Algiers. One officer and one enlisted man from AFHQ joined them there, and with the arrival of the London group in February plans for training and operations in the theater were put into effect.

c. The largest single increment of personnel became available when the

T/O for the Signal Intelligence Detachment, NATOUSA, was assigned to the 849th SIS in June 1943. Thanks to this pool additional personnel were subsequently available to fulfill the demands of new commitments as they arose.

d. Constant additions to the Intelligence Branch were, however, required since that time. Throughout the history of the Branch it was a never-ending struggle to get adequately trained officers and enlisted men to perform the tasks required of the Branch. The process of obtaining personnel from the USA was almost always a slow and unsatisfactory one. Frequently men arriving in the theater proved to be totally unfit for the duties for which they were requested and hence could not be used. For example, a request was sent to Washington in February 1943 for immediate shipment of 10 officers trained in elementary cryptanalysis and, more important, with fluent knowledge of spoken and written German.The 10 officers arrived at the 849th SIS at the end of May 1943, after the close of the Tunisian Campaign; and of the ten officers only two had any knowledge of the German language. Another example of the inadequate training experienced by many people who were assigned to the 849th SIS was the case of personnel of the Western Task Force, who had received only 10 days' instruction in the problems of radio intelligence prior to the invasion of North Africa and who had been given no idea of the code and cipher material they might be called on to deal with. Consequently training of personnel was the most important single problem that faced the Intelligence Branch. No single increment arriving at the 849th SIS had had a sufficiently long training period under anything approaching operational conditions before entering the Mediterranean Theater. Personnel trained at SIS ETOUSA for a month or two benefitted greatly from instructions given there [text withheld] but the burden of forming detachments into units capable of assuming actual commitments rested entirely on the 849th SIS. Experience proved that most detachments required from three to five months' experience under field conditions to be able to undertake successfully any operational commitment.

e. It should be noted that too few senior officers with adequate training were available to the Intelligence Branch during the early days of the 849th SIS. The majority of officers competent to handle the technical problems of the various detachments were in the grade of Lieutenant and were consequently placed in a difficult position as regards efficient liaison with the operational staffs to which they were furnishing intelligence. Over a period of two years the situation gradually adjusted itself; but it is felt that had the initial handicap not existed existed there would have been considerably smaller loss of valuable time and, perhaps, lives.

4. Organization and Equipment of Field Detachments.

a. As has been stated above, the original T/O and T/E of the 849th SIS were manifestly inadequate to meet the great expansion of the organization in the past two and one half years. This problem was especially evident when Detachments were formed for service in the field. The only possible way for detachments to start operations was by attaching them to other self-contained orga-

nizations, such as the SRI Companies, for rations, quarters, and administration. Because of the steady development of the Branch; grades and ratings were not allotted to the Detachments on any fixed basis; and equipment for the Detachments consisted of such supplies as were available to the 849th SIS as a whole and could be spared from other duties. Such supplies and equipment as were available were issued on memorandum receipts to the Detachments. Allocation of grades, ratings, supplies, and equipment to the Detachments was made by the Officer in Charge of the Intelligence Branch on the basis of what was hoped to be a fair distribution among the Intelligence Branch, Security Branch, and the 849th overhead.

b. Such conditions were obviously unsatisfactory and unconducive to a proper spirit of morale among the Detachments. No definite grades and ratings could be counted upon with certainty within the Detachments, and Officers in Charge of the Detachments experienced difficulties from being in a subordinate administrative position to the Commanding Officers of the SRI Companies.

c. Basic T/O's for Signal Intelligence Service Detachments types A, B, C, D, and E were in existence since December 1943, but Theater regulations did not permit activation of any such detachments until June 1944, when an "A" type and a "B" type unit were activated as the 3200th and 3201st SIS Detachments assigned to the 849h SIS....The personnel for these new Detachments were obtained from the Intelligence Branch Detachments "A" and "E" respectively, and some gains in operational efficiency were noted from the reorganization. Great improvement was particularly noted with respect to grades and ratings, for with their own T/O's at their disposal the officers commanding the new detachments were assured definite grades and ratings and could handle their own promotional problems. On the other hand such reorganization did not solve the basic problem of the relationship between the Detachments and the SRI Companies, for there was no provision within these new Detachments for intercept personnel; and consequently operations with independent SRI Companies were still necessary.

d. The most satisfactory solution was reached when the T/O for Corps Signal Service Companies, approved by the War Department in January 1945, became available in the Mediterranean Theater. Two such units were activated as the 3915th and 3916th Signal Service Companies, and were assigned to the 849th SIS....The new companies, calling for both intelligence and intercept personnel under a single command, eliminated entirely the problems of grades and ratings, supplies and equipment, and operational control.

e. In spite of the advances made by the activation of such units three Detachments of the Intelligence Branch- Detachments "D", "F", and "G"—could not be reorganized, and operated throughout their existence without benefit of special T/O's, T/E's, or administrative independence of the SRI Companies with whom they worked.

* * *

From SRH 048. *Once American forces had established themselves in France, Signal Security Detachment "D" served as the central command-and-control element for all signals intelligence operations conducted by General Omar Bradley's 12th Army Group.*

SUMMARY OF OPERATIONAL ACTIVITY OF SIGNAL SECURITY DETACHMENT "D", COVERING THE PERIOD 1 SEPTEMBER 1944 TO 1 APRIL 1945

1. PURPOSE

a. This report is intended to summarize briefly the signal intelligence mission assigned to Signal Security Detachment "D" and actions taken by that Detachment in the accomplishment of that mission. Although the Detachment began field operations as a unit in the middle of August 1944, 1 September was chosen as the starting point of this report since effective contacts with G-2 Section, 12th Army Group Tactical Headquarters, and with the signal radio intelligence units in the field were firmly established by that date.

2. MISSION OF THE DETACHMENT

a. The mission assigned to the Detachment was the procurement of Signal Intelligence from the solution of enemy (German) medium and low grade tactical codes and ciphers for the AC of S, G-2, 12th Army Group, the coordination and technical supervision of the Signal Radio Intelligence Companies and Signal Service Companies operating under units assigned to 12th Army Group, technical liaison with adjacent Army Group Signal Intelligence units and with those of higher headquarters, and the coverage of clandestine radio traffic for study by the Radio Security Service (British) and as required by the AC of S, G-2, 12th Army Group. The latter mission, being somewhat separate and distinct from the provision of signal intelligence, will not be covered in this report.

b. The mission of the Detachment may be conveniently divided into four distinct responsibilities:

(1) To Signal Intelligence Division, Hq ETOUSA.

(2) To G-2 Section, Tactical Headquarters, 12th Army Group.

(3) To Signal Radio Intelligence and Signal Service Companies, 12th Army Group.

(4) To flanking Army Groups (6th and 21).

c. The manner in which the mission was carried out, will be described in the sections of the report which follow.

3. SIGNAL INTELLIGENCE DIVISION, HEADQUARTERS ETOUSA

a. Signal Security Detachment "D" was charged with the responsibility of enforcing the general signal intelligence policies of the War Department, Hq ETOUSA, and the 12th Army Group, among the Signal Radio Intelligence units of 12th Army Group.

b. In addition, the detachment provided the higher headquarters with the raw

material and finished productions of all signal radio intelligence organizations of 12th Army Group.

(1) All signal intelligence and technical data were forwarded to the Signal Intelligence Division, OCSigO, Hq ETOUSA. This commitment included transmission to that office of all technical reports published by the Intelligence Branch of the Detachment. . . .These reports were also disseminated to the Mediterranean Theater of Operations, to British signal intelligence agencies in the United Kingdom and to the War Department, Washington, D.C., through the Signal Intelligence Division, Hq ETOUSA.

(2) Radiograms and teletype messages containing current information were prepared and transmitted at least twice daily. These messages reported all data collected by the Detachment in the course of its daily operations.

(3) Captured documents, received from signal intelligence units of 12th Army Group were processed, studies published, and copies forwarded to Signal Intelligence Division, Hq ETOUSA, for permanent files.

4. G-2 SECTION, TACTICAL HEADQUARTERS, 12TH ARMY GROUP

a. Detachment "D" was charged with the responsibility of passing to the Assistant Chief of Staff, G-2, 12th Army Group, signal intelligence procured from the analysis of enemy low grade and medium grade (THUMB, PEARL and CIRO PEARL) tactical traffic. This was accomplished in two ways.

(1) Direct telephone communication was available until 4 March 1945 when, due to the tactical situation, the Detachment operated too far in advance of Tactical Headquarters to allow utilization of metallic telephone lines. However, radio or teletype (or both) links maintained constant communication from that date onwards. The appointment on 3 February 1945 of a liaison officer from the Detachment to G-2 Section also aided in the smooth flow and interpretation of signal intelligence.

(2) All pertinent technical reports published by the Detachment were transmitted daily to G-2 Section. These reports supplemented and enlarged upon the information already passed to G-2 Section by communications means described in paragraph a(1) above.

b. A complete record of all signal intelligence, of immediate value only, transmitted to G-2 Section by telephone, radio or teletype has been maintained by the Intelligence Branch of Detachment "D", but this record is too bulky for reproduction and inclusion in this report. However, for the sake of completeness, an estimate of the quantity of timely information reported during the period under review may be derived from the following figures:

	No. of Items
CIRO PEARL	1422
PEARL	632
THUMB	162

c. It is not possible to evaluate the signal intelligence made available to G-2 Section, either in the form of immediately applicable information (i.e., location of Division or Army ammunition, supply and fuel dumps, command posts, etc.), or in the form of confirmation of prisoner-of-war reports, large scale movements or intentions of major enemy formations and the appearance of new battle units in a given sector. As an approximation of the use made of the data received from Detachment "D", the CIRO PEARL, PEARL and THUMB included in the daily G-2 ISUM. . . .The G-2 ISUM was sent by teletype, operational priority, to the following headquarters:

SHAEF Main
6th Army Group
21 Army Group (Main)
8th Air Force
First U S Army Command Headquarters
Third U S Army Main
Ninth U S Army Main
Fifteenth U S Army Forward
12th Army Group Main
12th Army Group Tac
Headquarters First Allied Airborne Army
Com Z
ASCZ
9th Air Force Advance

d. It is of interest to note that an estimated 6,000 CIRO-PEARL messages were read during the seven-month period under discussion. Of these, 3238 messages from twenty-four different formations were published in CIRO-PEARL/SSDD reports, which were transmitted to G-2, 12th Army Group. It is of further interest that on the average either CIRO-PEARL, PEARL or THUMB material, or all three, were included in one out of every three G-2 ISUMS.

5. SIGNAL RADIO INTELLIGENCE AND SIGNAL SECURITY COMPANIES 12TH ARMY GROUP

a. The mission of Detachment "D" in connection with the signal radio intelligence units of 12th Army Group was subdivided into three categories:

(1) Reporting of Signal Intelligence of Immediate Value to Army and Corps G-2's

(a) All technical signal intelligence of tactical value, particularly CIRO-PEARL, was transmitted daily by the most expeditious means to the Army Signal Radio Intelligence Companies. . . .contains intelligence extracted from technical messages sent to the field units during a typical month. This intelligence was used in two different ways:

(1) It was reported to Army and Corps G-2's.

(2) It was employed as a basis for allocating intercept and direction-finding coverage priorities.

(b) The most convenient means of transmission of technical signal intelligence to the field units was radio, teletype and courier. Two radio broadcasts were made daily, one in the morning and one in the early evening to establish coverage priorities and to assist in the preparation of technical reports for the respective G-2 Sections. Technical signal intelligence was also transmitted by the same means at any hour of the day or night when the urgency of the information so warranted.

(2) Consolidation of Technical Material of all Field Units

(a) All technical data from the signal radio intelligence units of 12th Army Group were consolidated daily with those obtained by the two intercept units directly responsible to Detachment "D" and with data received from intercept units of the two flanking Army Groups (6th and 21). Items of immediate value were transmitted along with intelligence described in paragraph a preceding. In addition, all such data were published in greater detail in reports of the Intelligence Branch. . .and dispatched to the field units.

(b) The daily publications of the Branch not only aided the field units in the normal execution of their missions, but provided the only means of maintaining technical continuity on enemy formations during the frequent moves of the field units. This was particularly true when Army and Corps fronts were radically altered, resulting in an entirely new, and frequently unfamiliar, group of enemy units facing them.

(3) Supervisory Control Over Operations of Signal Radio Intelligence Field Units

(a) Policies concerning operations emanating from higher headquarters, or those arising from within Detachment "D" from time to time, were distributed and enforced. Aid in complying with the policies was provided in the form of directives, special technical reports, and by conferences at the Detachment headquarters. Also frequent liaison visits to the field units were made by technical experts from the Intelligence Branch.

6. FLANKING ARMY GROUPS

Continuous liaison was maintained with 21 and 6th Army Group signal radio intelligence agencies both by personal visits and by radio teletype and telephone communications on a twenty-four hour basis. All technical reports published were exchanged with those two organizations.

From SRH 042. *This account of signals intelligence operations in General George S. Patton's Third Army gives the reader a good feel for the "nuts and bolts" of World War II collection activities in the field.*

THIRD ARMY RADIO INTELLIGENCE HISTORY IN CAMPAIGN OF WESTERN EUROPE

I. OPERATIONAL ORGANIZATION AND PROCEDURE OF RADIO INTELLIGENCE AGENCIES.

A. Organization of Signal Service Companies.

(1) All signal service companies (corps signal radio intelligence companies) were organized and equipped as prescribed by T/O & E 11-500, 1 July 1943, with an authorized strength of eight officers and one hundred twenty-one enlisted men. Several weeks after activation, the 3253rd, 3254th, 3255th, and the 3256th Signal Service Companies were moved to Wincham Hall, England (K-19), in order that these companies might collaborate on common problems of training and supply. At a later date each signal service company was attached to a corps with whom it would work in the field, and as the various corps were committed in combat operations, the respective corps companies would accompany them remaining within a few miles of corps headquarters in order that close liaison could be effected between the companies and the corps G-2.

(a) After the usual training program in Burton Bradstock, England, the 3253rd Signal Service Company left for Omaha Beach in France, arriving on 12 July 1944. The company was attached to XV Corps and remained with Third Army until 21 September 1944 when it moved under the command of Seventh Army.

(b) The 3254th Signal Service Company was activated at Marbury Hall, Cheshire, England (K-19) on 19 April 1944. The operations of the company were begun immediately after activation; however, it was not on an entire company basis until operations against the enemy on 2 July 1944. Prior to that time operations consisted of a general training program as well as individual team operations. A few intercept positions were established in June at Lyme Regis, England, with the traffic analysis unit controlling the intercept of nets and preparing the intelligence reports. On June 29 the company arrived in France with the primary mission of supplying tactical intelligence to VIII Corps.

(c) Effective 6 May 1944 the 3255th Signal Service Company was activated at Marbury Hall, Cheshire, England. The unit has been with XII Corps since its activation except for brief periods in its early days when it was assigned to Army so that activities of the company as well as the remainder of the service companies could be controlled and correlated by Army headquarters. After completion of the training program the company was concentrated at Lymington, England (U-

71), and departed to Omaha Beach on 12 August 1944. Thus, the unit arrived in the combat zone ready to become operational on the ninty-eighth day after its activation in the Communications Zone.

(d) Activated on 5 May 1944 at Wingham Hall, Cheshire, Northwich, England, the 3250th Signal Service Company was engaged in a signal intelligence training and field program for the next three months until 7 August when the company was committed at Courville-Sur-Huisine, France (T-08). Excepting for temporary attachment to III Corps during the Battle of the Bulge, the company has always serviced XX Corps.

(e) The 3259th Signal Service Company came into existence on 16 September 1944 under XIII Corps. Training in Ringwood and Lymington, Hants, and Dartford, Kent (Q-99) in England equipped the unit for its first action under III Corps on the First U.S. Army front on 14 February 1945, and after the liquidation of the Ruhr Pocket, it was transferred with the III Corps to Third Army, where it remainded until the termination of the campaign.

(f) At the cessation of hostilities on 8 May 1945, the following corps companies were with the Third Army: 3250th Signal Service Company under V Corps which was attached to Third Army for the last three weeks of the war; the 3255th and 3256th Signal Service Companies which served under Third Army during practically the entire campaign with XII and XX Corps respectively; and the 3259th Signal Service Company under III Corps. The 3254th Signal Service Company attached to VIII Corps also spent much time under this command, although during the last weeks of the war it was First Army.

(2) 118th Signal Radio Intelligence Company.

The 118th Signal Radio Intelligence Company was activated on 20 April 1942 at Fort Sam Houston, Texas based on T/O 11/77 which was later superseded by T/O & E 11-500, 1 July 1943, as amended by Change No. 1, dated 13 November 1943. After extensive training on maneuvers the company arrived in England in January 1944. At the direction of the Signal Officer, Headquarters European Theater of Operations United States Army, the intelligence company, later assigned to the Third Army, began intercepting German military traffic on 26 April at Dartford, Kent, between London and the Channel. During the next six weeks the practice traffic of the enemy indicated certain troop movements to and along the Atlantic wall, and also revealed radio characteristics later used in identifying and locating German units in the field. On 1 June, the company, then serving 21st Army Group, moved to a point on the English coast just across the Channel from the Cherbourg Peninsula where it covered enemy radio activity during the invasion and part of the build-up period gaining slight intelligence of operational value. On 15 July the unit arrived in France and proceeded to the vicinity of the Third Army headquarters to whom it supplied intelligence through the end of the campaign.

B. Radio Intelligence Procedures.

(1) Operational Procedures.

(a) Corps Level

Although the signal service companies were originally organized along identical lines, each, after being committed, adopted new methods of procedure, and changed the basic organization to fit specific operational needs. This report is designed not only to show the original composition of these units, but also to point out their major differences. The companies included in this report are the 3253rd, 3254th, 3255th, and 3256th Signal Service Companies; although the 3255th and 3256th Companies were the only ones to be assigned to Third Army throughout the entire campaign, the others were on separate occasions under this command.

Radio Intercept: The normal radio intercept section consisted of an intercept officer and from forty two to forty six operators who were divided into tricks composed of a trick chief (control chief) and a number of men determined by the traffic level of the current situation. The operators worked in HO 17's and HO 27's mounted on 2 l/2 ton trucks; the deployment of the trick chiefs varied with the company involved: The 3256th employed a trick chief for each truck but both the 3253rd and 3254th Companies used one man to control an entire intercept shift. In the 3255th the use of an inter-communication system by which the IA section could contact the individual operators entirely eliminated the need for trick chiefs. The average working day for the intercept sections was divided into three shifts with their times and set allocations as follows: 0001-0800, eight sets; 0800-1600, 15 sets; 1600-2400, fifteen sets.

The functions of the trick chief, whether he was in charge of the entire shift or of a single truck, were to control the interception of nets, check frequencies, and in general to act as an intermediary between the radio operators and the IA section. The process of searching for nets was one which especially demanded control by a single source; the 3254th control was achieved by means of a home constructed monitoring board channeled to each operating position whereas the 3256th simply submitted a search list of known priorities to the individual operators; these were compiled by all radio intelligence sources by the IA Section on the second day of the German three day frequency cycle. This latter method greatly minimized the time spent in recording nets of no immediate value, and thus insured that the majority of enemy units actively engaged on the front in question would be covered. As a further aid, lists of fixed call signs and peculiarities of procedure were also kept available at each set.

In regard to the technical aspects of radio intelligence work, it was found that the super-pro receiver tended to supplant the SCR 342 and 344, having been adjudged as more adaptable to intercept requirements. Each truck was usually equipped with one high frequency set connected to an appropriate antenna. For both high and low frequency work, antennae of varying characteristics were experimented with by the individual companies: The horizontal directional type proved to be the most popular with the 3255th, but the 3253rd Company on the other hand

preferred the "L" shape antenna.

Speaking in terms of general operating procedure it should be mentioned here that the interception of enemy traffic by those companies employing the leap frog method of moving was rarely interrupted. When the tactical situation warranted, advance parties to division and forward headquarters were sent out and the proximity to the enemy lines proved reasonably profitable as demonstrated by the extremely tactical low grade traffic intercepted by the 3255th and 3256th forward echelons.

Since continuous wave interception was not the sole function of an intelligence agency, it was necessary to have on hand operators capable of copying German voice traffic; these radio telephony operators were part of the intercept personnel in the 3255th Company, but in the 3256th they were furnished by the IA Section. The type of traffic obtained by this source was comparatively low in volume, and that which was intercepted ordinarily proved to be of local tactical value. Radio telephony personnel were also employed in the VHF (very high frequency) experiments when small teams were sent up close to the front equipped with high frequency intercept sets. The results obtained in these cases, as well as in the attempts to intercept German voice traffic on the medium frequencies from similarly advanced positions, were fairly good in so far as the mechanics of interception were concerned, but the intelligence gained therefrom was not of far reaching value.

Direction Finding: Operations of the direction finding teams in the signal service companies were for a long time hampered by technical difficulties involving equipment. The SCR 503 Receivers proved to be inadequate as long as the front remained fluid and even on a comparative static front the direction finding sites had to be relatively close to the enemy in order to obtain satisfactory results. Later in the campaign the equipment was supplemented and modified by individual companies, and as a result marked improvements were apparent. The final set used by the 3254th Company was an SCR 555 with an improved antenna loop and an SCR 244 as a receiver, the latter giving a wider null but better reception. The 3256th Company utilized German equipment found at a signal depot in St. Menehould, France, but this too was effective only at short range.

Generally, each company had two and some times three teams depending on the tactical situation; one was always located at the company site and the other or others at some forward position. The conditions of the roads, the availability of water and rations, the maintenance of radio and power equipment at the advanced locations, and the necessity of wire communication being installed for the most part by corps signal battalions—all these factors had a direct bearing on the efficiency of the direction finding platoon.

Control of direction finding stations was accomplished by various methods. The 3253rd Company placed a direction finding man directly in the radio trucks and acted as a liaison between the intercept and the direction finding sections. The

3254th Company on the other hand set aside one operator whose duty it was to pipe signals to the local direction finding station for re-piping to the advanced sites.

In spite of all the difficulties encountered direction finding results from the standpoint of signal service companies were uniformly good during the Battle of the Bulge, the cleaning out of the Saar-Moselle Triangle, and the Battle of the Rhine. Evidence derived from this source as a confirmation of the intelligence gained through other means consistently proved valuable.

Traffic Analysis: The Traffic Analysis Section (IA Platoon) was commonly divided into two main groups, Traffic Analysis and Cryptanalysis Departments; originally the section had a complement of twelve men, but this number was later augmented by personnel from other platoons of the individual companies according to specific needs. Perhaps more appropriately referred to as the Intelligence and Coordination Team, the section had four principal functions: The analysis and processing of intercepted traffic and the identification of enemy radio nets; the cryptanalysis of enemy low grade codes and ciphers; the determining of German order of battle and the maintenance of the necessary files on enemy units, personalities, code names, and other necessary data to achieve this end; lastly, the compiling of statistics on the technical aspects of the work to aid in the identification and analysis of the traffic.

The Traffic Analysis Department usually consisted of four traffic analysts whose duties were reading logs and searching the files in order to identify the current enemy units. There was a man designated to keep order of battle information including personality files, breakdown of enemy units, situation maps, and all such pertinent information derived from G-2 reports, captured documents, and other reliable sources. One of the analysts coordinated the information obtained from analysis and direction finding for submission to the traffic analysis officer for final approval; that which was of immediate tactical importance was relayed to corps G-2 and subsequently the finished product was dispatched to all other interested agencies.

Two translators and two cryptanalysts comprised the Cryptanalysis Department whose province was the breaking of all types of low grade traffic and the examination of all medium grade for possible compromises. When teletype communication was available, raw traffic (low grade) was exchanged with the other intelligence units of Third Army. In some cases the men of this department were called on to interrogate prisoners thought to be of importance to radio intelligence work, to serve as radio telephony operators, and to process captured documents destined for higher headquarters. In this department as well as in traffic analysis it soon came about that each man, although trained for a specific position, became capable of handling a variety of duties.

The plotting of direction finding bearings was usually done by some member of the Traffic Analysis Section, although it should be mentioned that much better results were obtained from assigning a certain man to that duty. Most of the com-

panies were restricted in their use of situation maps and overlays by the lack of space in the housing units. When the Traffic Analysis Section of the 3256th Company moved indoors, it was possible to exploit further the results of direction finding in connection with the order of battle picture. In this company the direction finding man, in addition to his primary duties, maintained an overlay on a 1:25000 map showing the breakdown to battalion level of all enemy units on the corps front; this map also included the direction finding bearings of the preceding day as well as any additional information of the same kind extracted from reports of other radio intelligence units. When it was possible to obtain a large number of bearings from various sources on any specific unit, a special overlay of that formation's area was made, thus affording a closer check on its movements.

As a final comment all of the work done in evaluating intelligence gained from intercepted traffic was channeled to one principal destination, the daily activity report which served as a complete record of the day by day radio intelligence results. The form of the report was as follows: (I) Intelligence Summary; (II) Decodes and Translations; (III) Technical Summary of Nets Heard; (IV) Message Count and Set Allocation; (V) Direction Finding Bearings; (VI) Code Idents and Cipher Values.

(b) Army Level

The Radio Intelligence Company at Army level naturally differed in several respects from the corps' agencies; approximately twice the size of the Signal Service Company, the Army unit had several additional functions, chief among which was the coordination of the work done at lower levels and the dissemination of information thereto.

Radio Intercept: Aside from the disparity in numbers between the intercept section of the Army company and that of the corps (the former maintaining some twenty two men on each shift) there were major differences in operational procedures. Certain minor points not mentioned before were common to intercept work at all echelons.

During times of heavy radio activity it was found best to have at least two intercept operators on random search, who would scan the dial until an enemy net was heard. The frequency and call signs were then given to one of the other operators and the search was continued for other nets.

When an enemy net went off the air, or when the operator, for various reasons, could no longer hear the transmissions, the spot checking practice was used. This meant that the operator would go on search, returning to the frequency every fifteen minutes.

In order to ensure good copy of messages, important for the cryptanalytic work, nets were frequently double banked; since this meant the assigning of two or more operators to cover the same traffic, it was naturally more easily done at Army level, where more men were available. In any given case, the necessity of double banking was determined by the traffic analysis control man with the one exception,

that it was a standing rule to double bank all three letter traffic and plain text.

In the case of voice transmission the handling of plain text in the Army company occasionally involved use of the dictaphone, the recording being sent to the Traffic Analysis Section. In certain urgent cases, the voice signal was piped by telephone directly to a translator in that section.

When the Army agency initially went into operations, the intercept and direction finding control man occupied different housing units and were linked by telephone. It was later decided that the work of these two sections could be better coordinated if their control chiefs operated in the same unit and simultaneously received directions from the Traffic Analysis Section.

Direction Finding: The size of this section and the existence in the Army company of a wire section to establish communications made it possible to operate as many as three outstations; later, radio control was used and proved more practicable than in the corps companies. As a general rule, the length of the base line between the outside stations was forty miles with land line communications, and sixty miles with radio. As already mentioned, it was found best to have the direction finding control man work closely with the intercept trick chief, but aside from these points, the operational procedure involved in taking any given bearing did not differ greatly from the methods used by the signal service companies.

Traffic Analysis: The traffic analysis section of the Army company also differed in only a few respects from that at the lower level; of course, since this section was larger, being comprised of twenty nine men and three officers, it was possible to extend the work of the various sub-sections to a finer point of detail and to act as a coordinator of the results obtained on the corps' front.

As this latter function became more and more important, it became necessary to create a special section in the Army radio intelligence company to act in liaison with corps, flanking armies, and Army group; information was thus routed more efficiently and expeditiously up and down the line.

Security considerations, in many cases, made it impossible to send certain data down to corps level directly and one of the functions of the Army company was to see that the signal service units receiver whatever extracts and conclusions from this information it was possible to disseminate. To further this end and to accommodate the large influx of the many different reports and documents, it was necessary at Army level to create another sub-section within the traffic analysis platoon known as the incoming documents section; the purpose of this miniature message center was to regulate the distribution of all incoming and outgoing material and to keep the necessary extensive files and records.

In the matter of intercept and direction finding control, the techniques were the same as those used by the signal service companies, except that the Army company was naturally expected to concern itself with all corps' fronts and even with some units close to the Army Zone of Advance in view of the possibility of sudden movement. The particular method of establishing control generally followed one of

those already outlined, that of distributing each day a list of the desirable frequencies and call signs to the control chiefs of the other sections.

Since the cryptanalytic section at Army was larger than that at corps, it was soon found that in many cases rapid transmission of traffic intercepted at the lower level to this section accelerated the eventual breaking of it. A teletype net involving Third Army radio intelligence agencies provided the necessary means of communication and proved fairly practical.

In this, as in almost every case, the greater manpower in the Army traffic analysis section made possible much more detailed files and records of all kinds; as a result, intelligence could be interpreted on a wider basis. When the data at Army level itself was insufficient, the Army company was able to have recourse to Army group, or, in certain instances, to Signal Intelligence Division, European Theater of Operations United States Army. This was especially important when a signal service company suddenly found itself concerned with new German units because of a re-allocation of corps zones; in all probability, the Army company had already been intercepting traffic from these units, but if not, the above mentioned channels for obtaining information were open. It can be readily seen, therefore, that the Army Radio Intelligence Company was, in almost every respect, essentially a larger scale signal service company with far more extensive functions because of its size and position in the organization of a Field Army.

(2) Communication Set-Up of Radio Intelligence Agencies. . . .

Signal intelligence agencies employed most of the known means of communication. Each company Mobile Radio Team operated a sub-station of a net with the Army Radio Intelligence Company as control. The Army company itself had a lateral radio link with its corresponding unit in flanking armies, and of course was part of the Twelfth Army Group Radio Intelligence Net.

In the signal service units radio contact with direction finding outstations did not prove to be quite as satisfactory (in comparison with wire lines) as at Army level. For communication within the companies themselves telephone naturally was used, but there were some variations in the details of its use; the 3255th Company and the 118th Signal Radio Intelligence Company had their systems so arranged that each individual operator and trick chief could communicate separately with the traffic analysis section, but in the 3256th Company direct communication existed only between the trick chiefs in each truck and the IA inter-communication operator.

A teletype net was operated for a long time involving the signal service companies, the Army company, and Third Army Signal Intelligence Service. The chief purpose here was the exchange of raw traffic, and, on several occasions, this means was employed to send traffic back to the company proper from advance teams. When the teletype lines were in good order, this was by far the quickest, easiest, and most secure manner of exchanging information. During certain periods there was a teletype line between Army group and the 118th Signal Radio Intelligence

Company over which raw traffic and items of technical information were transmitted.

Telephone was naturally widely used. Both army and corps agencies communicated with their respective G-2 sections by this means and in addition the former always had a direct line to the Signal Intelligence Service Office at Army headquarters. This latter circuit was supplemented by a direct teletype line to provide printed confirmation of any information relayed to G-2 by telephone. Telephone communications further existed between the Army company and Army group, flanking armies, and the signal service companies in Third Army. Whenever a telephone or teletype line passed through one or more switchboards, a jargon code was used, except in the teletype transmission of raw traffic.

C. Captured Documents.

From the beginning of the campaign in Normandy the importance of captured documents to increase the value of radio intelligence information was ascertained. During the first few weeks after the initial landing, little was done in this direction because the static line prevented the capture of documents in any quantity. After the St. Lo breakthrough advantage was taken of an increased number of captured documents which necessitated a system of distribution, so that this information could be expeditiously disseminated. Corps' G-2 first analyzed any documents in search of facts peculiar to its own work, then passed all signal documents on to the corps' signal service companies for analysis. Any information of value was immediately extracted and the original document was sent to Army Signal Intelligence Service where it was photographically reproduced and distributed to service companies under Third Army Command, First, Seventh, and Ninth American Armies and Twelfth Army Group. Code names, code and cipher keys, frequency and call sign allocations, maps with encoded terrain features and place names, map coordinate codes and grid systems, and the German methods of signal intelligence operations constituted information of particular importance. Over three hundred signal intelligence documents requiring some eight hundred pages were reproduced and disseminated during the course of the campaign. To supplement this information signal intelligence notes were published and distributed when documents received were particularly current or when only extracts from lengthy documents were of value. Enemy units were often identified through code names continued in documents, and encoded traffic was frequently easily read due to the capture and dissemination of documents, diagrams, and German signal intelligence publications. During August in the early days of the campaign, intelligence companies were able to follow the movement of the 9 Panzer Division from non-indicator cipher keys captured from this unit. Numerous examples could be cited to justify the work required in maintaining a small Documents Evaluation, Reproduction and Dissemination Section.

D. Prisoner of War Interrogations.

In order to obtain all available radio intelligence information PW interrogations were made frequently. During the campaign the various PW cages were

visited at least once a week under ordinary circumstances. Arrangements were made with PW authorities that Signal Intelligence Service should be notified when routine screening indicated that a PW might possess information of signal intelligence value. In most instances the information obtained from PW's had already been secured through other sources, however, any additional facts always served as a confirmation. Frequently PW's were interrogated soon enough after capture to obtain detailed information on effective frequencies and call signs which otherwise was a difficult matter in view of the fact that they, excepting in most cases of reconnaissance traffic, were customarily changed every third day in the German army. Although valuable radio intelligence information was obtained from PW interrogation, its principal virtue lay in the security angle. German signal intelligence men, especially those from corps headquarters and higher, could always give information as to which of our code or cipher systems were being broken, what difficulties arose in the process, how long a system could be depended on for security, and what disposition was made of the intelligence gained. . . .

* * *

From SRH 227. *This is part of the official unit history of a signal radio intelligence company assigned to the Southwest Pacific Area, General Douglas MacArthur's theater of operations. It should be noted that unlike the situation in Europe, where tactical COMINT units concentrated their efforts on low-level traffic, the 126th Signal Radio Intelligence Company reported directly to Central Bureau, a high-level theater processing center. The information in the first sentence is actually incorrect: the unit's predecessor, the 1st Radio Intelligence Company, was activated in 1938 and was not a provisional unit.*

OPERATIONAL HISTORY
126TH SIGNAL RADIO INTELLIGENCE COMPANY

February 1944

The 1st Signal Radio Intelligence Company was activated at Fort Monmouth, New Jersey, in February 1941, having previously been known as the 1st Provisional Radio Intelligence Company. The operational set-up of the new company included three operating platoons, each of which was to be capable of operating independently on a combined intercept, direction finding, wire-laying mission. Operational training was begun with regular classes in International code, direction finding, plotting, and wire-laying. 206-C Direction Finders were set up under simulated

field conditions and bearings were taken on local stations, to familiarize the operating teams with the methods of operation.

In March 1941 the company moved to Fort Meade, Maryland, where training was continued. In June of the same year, the unit designation was changed to the 121st Signal Radio Intelligence Company. The company participated in the North and South Carolina maneuvers during the period extending from September through the 6th December 1941. Intercept positions were set up in a 2-1/2 ton truck which also included a typewriter at each of the eight intercept positions. Back to back with the intercept truck was another 2-1/2 ton truck containing the plotting equipment. Goniometric wire lines were laid out to the four 206-C direction finders, which were the only DF's in the company with the exception of the 504 equipment items, which were not used. The direction finders were generally spread over a base line of approximately 20 miles. Thus, at this stage, with limited equipment, the company was not using the three-operating-platoon set-up. The company worked at one time with the Red army, at another with the Blue army, intercepting "enemy" traffic, and locating "enemy" transmitters, for GHQ, in each case. The company also worked with the referees, monitoring all radio traffic for violations of signal security.

Following maneuvers, the company returned to Fort Meade, Maryland. Shortly thereafter it moved again to Ft Bragg, North Carolina where it participated in day-to-day maneuvers with the field artillery, locating "enemy" transmitters, which were than "neutralized" by the artillery.

Following the company's return to Ft Meade, on the 25th of February 1942, one operating platoon of the 121st Signal Radio Intelligence Company was designated as the First Operating Platoon. 1st Lt Menear was placed in command of the platoon over 45 enlisted men. The platoon left Ft Meade for Ft Dix, New Jersey, to await movement orders for an overseas destination. Its equipment included intercept receivers, the four 206-C direction finders, plotting equipment, wire and wire-laying equipment, and field range equipment for independent operations.

On the 1st of March 1942 the First Operating Platoon sailed from the Brooklyn Port of Embarkation on the USATS URUGUAY. On board ship the platoon radio operators were placed in charge of the radio room and the signal bridge, and operated the ship's radio, blinkers, and signal flags. The ship arrived at Melbourne, Australia, on the 10th of April 1942.

At Camp Pell, Melbourne, training in intercept and direction finding operations was continued until the 6th of June.

Meanwhile, on the 19th of May 1942, the platoon was redesignated, and became the First Operating Platoon, 126th Signal Radio Intelligence Company.

On the 6th of June the platoon left Camp Pell and proceeded by motor convoy to Mt. Massadon, Victoria, the contemplated site for a permanent camp. The platoon set itself up for independent operation, performing its own house-keeping and cooking chores. Intercept facilities, consisting of three positions, were operated in

the van of a 1-1/2 ton truck. One direction finder, 206-C, was placed in operation atop Mt. Massadon, about 3/4 miles from the camp. On 1 July 1942, while still at this location, T/Sgt Messer of the 823rd Signal Service Company was attached to the platoon for temporary duty to instruct the platoon's intercept operators in ROMAJI and Japanese KANA telegraph code.

On 10 July 1942, the platoon moved again by motor convoy to Townsville, Queensland, arriving there on 2 August 1942. Lt Menear was reported to Capt Brown, GHQ radio intelligence officer, who in turn assigned two GHQ officers, Lt Phelan and W/O Card, to establish a Japanese code school for the instruction of the platoon's intercept operators. In addition, the platoon was assigned the mission of monitoring Allied Air Reconnaissance frequencies copying Allied clear and coded messages during the attacks on Guadalcanal and reporting by TTY to GHQ. The platoon's 206-C direction finders were set up to work with the No 1 Wireless Unit, RAAF, which was operating in Townsville. The DF's were located respectively at Townsville, Cairns, Charters Towers, and Cloncurry, and communicated with Townsville by wire. . . .Their mission was to work with the RAAF unit in securing bearings on enemy aircraft. However, the work was not wholly successful because of the long lines of communication and because the DF's were not suited to long range work, nor to the rapid action required to obtain bearings on short aircraft transmissions. In addition, the DF operators were not trained to read Japanese code, and therefore could not distinguish readily between the various transmissions they were to pick up.

On 15 November, the platoon travelled again, this time by rail to Brisbane, Queensland. M/Sgt Nurss, working under Capt Brown and GHQ, had preceded the platoon to arrange for the establishment of a radio station and antenna equipment. The platoon arrived in Brisbane on 18 November 1942 and immediately began work on a new operational site at Northgate. With the completion of a radio "shack" constructed by Australian workmen, and an antenna installation, using 6 rhombic antennas, work was begun in intercept, covering Japanese Army and Diplomatic radio traffic. All traffic was turned over to Central Bureau, GHQ, for analysis. Capt Brown, and his officers, Lt Phelan and W/O Card directed the operations of the platoon from this point on, using experience gained in and since the invasion of the Philippines to further the instruction and efforts of the platoon's intercept operators. It was necessary to train more men as intercept operators. Consequently, all men, regardless of their previous assignments in the platoon were given training, and of these the best became intercept operators. No direction finding work was done during this period.

The rainy season which followed shortly thereafter caused the site of the radio station to become inundated. On 10 January 1943 the platoon moved to Stafford, Brisbane, where it established an independent camp and a temporary radio station, the latter housed in two tents, and using simple antenna equipment. Work on a new GHQ radio station was begun at once, a short distance from campsite. Australian

workmen constructed the building. Grounded V-antennas were installed to cover directionally the arc from northwest through northeast of Brisbane. Fifteen antennas were set up for this purpose, arranged in groups of three, each group covering the same direction with spacing for diversity use if necessary. By the beginning of March the new radio station was in operation, continuing the work begun at Northgate. The amount of enemy traffic being copies by the First Operating Platoon, 126 Signal Radio Intelligence Company, was almost being doubled each month.

In April 1943, the First Operating Platoon, all its personnel except Lt Menear, and all its equipment, were combined with the 126th Signal Radio Intelligence Company which had arrived in Brisbane on the 25th of March 1943.

The 126th Signal Radio Intelligence Company had its origin at Camp Crowder, Missouri, where it was activated on the 14th of August 1942. Five officers, all second lieutenants, were present for duty with the company on the date of its activation. By virtue of seniority, Lt Joe L. Thurston assumed command. . . .The strength of the organization on the date of its activation, was 5 officers, 0 warrant officers, and 85 enlisted men.

The Table of Organization of the company included a group known only as the First Operating Platoon, which had already been activated. The whereabouts of the First Operating Platoon was not known or not revealed. However, its strength of 1 officer and 45 enlisted men was to be included as part of the strength of the 126th Signal Radio Intelligence Company, and it was believed that the two units would eventually be joined.

The new company was placed under the Signal Corps Unit Training Center at Camp Crowder, for administration and preparation for active duty overseas. It was the function of the Unit Training Center to coordinate administration, training, and securing of personnel and equipment for newly activated SOS units at Camp Crowder.

On the 19th August 1942, following movement of the company to its own area at Camp Crowder, operational training began. Full advantage was taken of specialists' schools available at the MidWestern Signal Corps School and the MidWestern Signal Corps Replacement Training Center at Camp Crowder. Chauffeurs and field linemen were sent to school for further training. All radio operators were enrolled for advanced training in International code, Joint Army and Navy Procedures, and net operations.

Among the radio operators assigned to the company were twenty specialists, with knowledge of the Japanese Romaji characters and their code equivalents. These men had received their special training at Fort Monmouth, New Jersey, and had been assigned from there to join the company on the 19th August 1942. At that time there was no course of training at Camp Crowder suitable for specialists of this type. For the time being, therefore, they were entered with the other operators in the International code classes.

* * *

Four SCR-255 Direction Finders had been received by the company. These were set up in the field near camp and connected by goniometric wire lines for several days operation and practice. Tentative operating teams for the DF's had been assigned for this work to learn as much as possbile about the equipment, and to use that knowledge in teaching others. All officers familiarized themselves with the equipment. Lt Dibos took charge of assembly and disassembly, and instruction in DF operation. The direction finders were then dismantled and prepared for crating.

Additional supplies and operational equipment were received by the company during the remainder of the month of September. Lt Kuch was tentatively placed in charge of intercept training. A schedule was arranged whereby the twenty Japanese specialist operators were to work several hours each day on company receivers installed in one of the barracks, picking up and copying Japanese radio code transmissions. This procedure was not too satisfactory due to weakness and unreliability of the signals. Therefore, training was later amplified to include copying of Japanese code from disc and tape recordings, made for the purpose by one of the operators.

During all this period, activities of the company were centered around crating and preparing for overseas movement. In early October 1942, news was received of a short delay, due to supply shortages and changes in War Department plans. The company, however, remained alerted.

One direction finder SCR-255 was uncrated and assembled near the camp. DF crews were assigned to work under the instruction of non-commissioned officers who had previous training, in assembling and disassembling the direction finder, as well as in operating. SCR-284 transmitters were installed, both as fixed and as mobile stations, and operators were trained to tune and operate these sets; 342-type receivers were used to intercept the transmission of the SCR-284's for the practice of copying and guarding friendly transmissions.

Lt Skinner was transferred from the company on the 21st of October 1942 due to a physical ailment; and Lt Hadd replaced him as Supply and Motor Transport officer. By oral assignment, Lt Dibos became Operations Officer, Lt Wilson was made Liaison and special services officer, Lt Swomley became Wire and Personnel Officer, and Lt Kuch was assigned as Intercept Officer.

During November 1942 word was received of a further delay in overseas movement. Training continued through the use of Signal Corps specialists' schools available on the Post. New intercept operators were being assigned to the company from time to time, and these were entered in new code and traffic classes, which were especially arranged for through the radio schools of the Replacement Training Center. Men who were not operators, but who were believed to have potentialities as such, were entered in beginners' classes. Many of the men assigned to the company as specialists in certain types of work, were found to be inadequately trained. Consequently, eight men were selected to attend night classes in teletype operation; five men who had been assigned to the company as radio

repair men were sent to the repair section of the Signal Corps Replacement Training Center, to learn and work on maintenance of Signal Corps receivers and transmitters; and the wire platoon was assigned to practice pole-climbing, use of the compass and maps in nearby fields and woods, and use of hand and engine-driven reels.

* * *

During early December crating was again speeded in anticipation of overseas movement. Training was continued spasmodically, due to the need for men to assist in packing and crating. The Unit Training Center began a new training project, in which it created an "army" headquarters, and two "corps" headquarters, with emphasis on message center work. All available intercept, telegraph, teletype, and switchboard operators of the 126th Signal Radio Intelligence Company were assigned to operate with other groups in the three headquarters' message centers. Radio operators handled radio traffic between the headquarters, using International code. Several company receivers, operated by company personnel, were set up and used as army and corps intercept units, guarding the radio nets and copying all traffic. After the first week, however, orders were received to ship all company equipment to arrive at the San Francisco Port of Embarkation by 1 January 1943. On the 23rd of December, the equipment was shipped in three box cars from Camp Crowder.

At this time, twenty enlisted men were enrolled in a six weeks course of training which included operation of the 206-D and SCR-255 direction finders, elementary map reading, elementary maintenance of radio equipment, elementary trigonometry, elementary wave-propogation, and the technique of recording on cylinders and tapes. The men selected for this course were NCO's of the operations section, nco's in charge of direction finding teams, as well as direction finder operators who showed potentialities for possible leadership of teams.

During January 1943, the company remained alerted, although movement was again delayed. Toward the end of the month the company was given a final inspection by a staff of officers and men from the Inspector General's Department. During the last week in January, orders were received for personnel of the company to move to the port of embarkation. All men in school were withdrawn. Lts Wilson and Hadd were sent immediately to the port to act as liaison officers for personnel and supplies respectively, and to prepare for arrival of the main body of the company. . . .

On the 3rd of February 1943, the company departed by railroad for the San Francisco Port of Embarkation, arriving there on the 6th. The company was assigned for a period of staging and physical "hardening" to quarters at Camp Stoneman. Then, on the 25th of February, with a strength of 6 officers, 1 warrant officer, and 203 enlisted men, the company boarded the USATS "President

Johnson" for shipment overseas.

The company disembarked at Brisbane on the 23rd of March 1943, and marched to Camp Doomben, where casual quarters were assigned. During the third day at Camp Doomben, the company was visited by GHQ officer, Capt Howard M Brown, and by 1st Lt Menear. The latter was introduced as the commanding officer of the First Operating Platoon for which allowances had been made on the Table of Organization, and the location of which had until then been unknown to the company. . . .

From SRH 049. *This document was produced by the 12th Army Group's Signal Security Division "D". The excerpt shows the results of one day's intercept of low-level German communications by Army tactical COMINT units. On November 11, 1944, intelligence was produced on three German divisions: the 15th Panzergrenadier Division; 17th SS Panzer Division; and 116th Panzer Division. Intelligence came from exploitation of German messages enciphered in medium-level cryptosystems (CIRO PEARL); low-level systems (PEARL); and radio direction-finding (THUMB). As can be seen from the text, CIRO PEARL messages were intercepted on November 6, but could not be decrypted and translated until November 11. The "cut" referred to in the final paragraph describes simultaneous bearings on an enemy radio station obtained by two separate radio direction finders.*

TECHNICAL SIGNAL INTELLIGENCE
TRANSMITTED DIRECTLY TO G-2,
12th ARMY GROUP, ETO
FROM 14 AUGUST 1944 TO MAY 1945

* * *

11 NOV 44

CIRO PEARL

15PG DIV 6/11 1159

To IIa

Query whether tank specialists, who were recently sent here from 5 (PZ) Co are to be retrained to become Panzer Grenadiers.

15 PG DIV 6/11 1219

To 2 Co

Send Rasterschluessel for course of instruction at FEB to FEB via registry.

HORN

15 PG DIV 6/11 1417

From actual strength status of 1 Nov 44 (with exception of the sick and wounded within the past 8 weeks, as well as designated Fahnenjunker (OCS candidates), 10 percent NCO's and OR's of the age groups 1906 and younger fit for general service are to be sent enroute to FELD ERS BN by 7 Nov 44 at 1200 hrs in accordance with OKW order. Numbers of NCO's and OR's released to Feb is to be reported to IIb by 7 Nov at 2000 hrs. Written orders enroute.

IIa

15 PG DIV 6/11 1531

SECRET - Report is to be made on Nov 10 as to whether there are experiences concerning rocket bombs having been shot down by pursuit planes.

PEARL

17 SS PZ DIV

Msgs today were mainly concerned with the difficulties of an art grp NAGLER (17 SS PZ ART RGT) which was in position the morning of 9 Nov in ALEMONT (U 9040). At 101410 the art group urgently informed its control station that Allied forces were advancing on BEAUX (U 9645), its present position, and requested immediate orders. At 101455 the group was told in answer to an inquiry that there were no munitions. At 101455 the group was still in BEAUX impatiently awaiting orders. At 101506 it was told that SCHMIDT (poss CO 10/38 SS PGR) was cut off and was requested to hold its present position. Shortly afterwards, however, the group indicated it was moving NW near PONTOY (U 9447).

116 PZ DIV 10/11

Rgt Bn of Art Rgt 146 still at RATH (F 107531)

116 PZ DIV 10/11 0345

Barrels already dismounted. Ammo packed. Phone comms dismantled. Prime movers are in the btry position. Equipment loaded. Query - are we to prepare to fire again and is the OP to be reestablished. SCHWEIGER

116 PZ DIV 10/11

ENGELS (PZ AR 146) arrived with 4400 liters.

THUMB

116 PZ DIV

D/F on supply elts of 116 PZ DIV confirm northward movement with cut on Art net at K 893742.

* * * *

CHAPTER X

Reshaping the Tools

By 1945, there were growing pressures to rationalize the Army's signals intelligence structure. A major step towards achieving this had already been taken in December 1944, when, as we have seen, the Military Intelligence Service assumed operational (but not administrative) control of the Signal Security Agency. Another initiative came about as the result of a belated Navy proposal to finally create an Army-Navy Communications Intelligence Board to coordinate the activities of the two service signals intelligence arms. Major General Clayton Bissell, the Army Assistant Chief of Staff for Intelligence, initially demurred, on grounds that the Army's structure was too decentralized to allow for meaningful interservice collaboration. However, he then used the Navy approach as a wedge to establish centralized Army control over all its COMINT assets. His arguments in favor of this are set forth in the excerpt from SRH 169, Centralized Control of U.S. Army Signal Intelligence Activities. With the war in Japan coming to a close, all the theater commanders in the Pacific—even Douglas MacArthur—accepted implementation of the proposition once the fighting was over. On 15 September 1945, just thirteen days after the war in the Pacific had ended, the Army created the Army Security Agency, which would control all Army signals intelligence elements through a vertical command structure for the next 32 years.

From SRH 169. *The head of the War Department's Military Intelligence Division argues that all signals intelligence assets should be under his control. His appeal was ultimately successful.*

CENTRALIZED CONTROL OF U.S. ARMY SIGNAL INTELLIGENCE ACTIVITIES

* * *

1 June 1945

MEMORANDUM FOR THE CHIEF OF STAFF

SUBJECT: Centralized Control of Signal Intelligence Activities for War Against the Japanese

1. On 8 May the War Department requested comments of the U.S. Army Theater Commanders in the Pacific and Far East on a proposal to place under the control of a single War Department agency all Army units and personnel engaged in signal intelligence activities for the war against the Japanese. . . .

2. General Wedemeyer has advised of his "wholehearted approval" of this proposal. . . .General Sultan advises that he "concurs in the need for a central agency to coordinate" all U.S. signal intelligence activities but believes this can be accomplished "without removing units and personnel from theater commanders' control". . . .General MacArthur advises that he does not concur in the proposal because it would place such activities under the "absentee control" of an agency "many thousands of miles away"; would interfere with the "close association" which his headquarters has had with such activities; would "disrupt an Allied agency which is now functioning most effectively" in his theater and would prevent signal intelligence results from being made available to the theater commander with the required speed. . . .

3. Attached hereto is a memorandum which explains the facts and circumstances pertinent to the proposed centralized War Department control. It is believed that such control is essential:

a. To coordinate U.S. Army signal intelligence activities in the various theaters and in the United States, eliminate duplication of effort and insure full exploitation of signal intelligence sources.

b. To coordinate U.S. Army signal intelligence activities with those of the U.S. Navy and the British.

c. To utilize most economically the limited Japanese linguistic and other specialized personnel available for this work.

d. To provide full technical support for all advanced signal intelligence units.

e. To ensure maximum distribution and utilization of signal intelligence technical data and results regardless of place of production.

4. The objections raised by General MacArthur are not considered valid. The world-wide nature of enemy radio interception and the total absence of any relationship between Theater boundaries and the location of interception or solution of Japanese messages, makes it essential that the principal cryptanalytic center be at a geographic point where the machinery, facilities and skilled research personnel are located if the signal intelligence system is to produce the maximum intelligence of which it is capable. Control should be centralized at this same point which is the only location that has or can have access to all of the enemy radio traffic without prohibitive duplication of personnel and facilities. The principal cryptanalytic center is near Washington and must remain here because it would be totally impracticable to move the machinery and facilities to another site and secure effective results during the probable period of the Japanese war. Adequate communications exist to ensure not only fullest exploitation, but to guarantee almost instantaneous delivery of results to any Theater Headquarters.

RECOMMENDATIONS

5. It is recommended that:

a. The proposed centralized control of the signal intelligence system be approved.

b. The attached draft of cable to theater commanders concerned be dispatched.

CLAYTON BISSELL
Major General, GSC
Assistant Chief of Staff, G-2

* * *

I. Circumstances leading to proposal

1. The present recommendation for centralizing control of all U.S. Army signal intelligence activities for the war against Japan is a direct outgrowth of a proposal made by Admiral King on 14 February 1945 to establish an Army-Navy Communication Intelligence Board charged with coordinating the plans and operations of the communications intelligence organizations of the Army and Navy. . . .

2. All signal intelligence activities of the Navy, including those conducted within theaters of operations, are under the direct operational control of the Navy Department in Washington. . . .In the Army, on the other hand, responsibility for signal intelligence activities is divided among the War Department and theaters of operations in the same manner as responsibility for the conduct of strictly combat operations against the enemy. Although this basic difference in the signal intelli-

gence organizations of the two Services made it unlikely that the proposed Army-Navy Board could function as effectively on the Army side as it could on the Navy side. . . , that fact was not considered an adequate ground for rejecting Admiral King's proposal. . . .The proposal was therefore accepted by the Chief of Staff. . . .

3. However, Admiral King's proposal gave impetus to consideration by the Deputy Chief of Staff, the Military Intelligence Division and the Operations Division of the need for centralizing control of the Army's signal intelligence activities for the war against the Japanese. This consideration led to the conclusion that the basic principles of command applicable to combat operations are entirely inapplicable to the highly technical and specialized activities involved in deriving intelligence from Japanese military radio communications, and that all such activities should be placed under the control of a single War Department agency. . . .

II. Proposal to theaters and replies thereto

4. Accordingly, after receipt of an independent suggestion from General Sultan as to the need for centralizing control of signal intelligence activities...and after obtaining the views of the Chief Signal Officer..., the proposal now under consideration was presented for comment to the theater commanders concerned. . . .

5. The comments received from the theater commanders have raised no considerations not previously taken into account by the War Department. General Wedemeyer's approval of the proposal is based upon considerations similar to those which constituted the basis for the proposal. . . .General Sultan's reply approves the basic idea of centralized control and suggests only a different procedure for putting it into effect. . . .General MacArthur's reply. . .raises objections of the same nature as those which had previously been considered and rejected as invalid. . . .Those objections are discussed below.

III Basic reasons for proposal

6. The basic reason for the present proposal is that Japanese radio communications, their availability for interception, the cryptographic systems used, and the usefulness of the results derived therefrom, all have no relation to the considerations which are determinative in assigning command responsibility for combat operations against enemy forces.

Availability of traffic for interception.

7. There is no relation between the availability of Japanese military traffic for interception and the geographic organization of our Army for combat operations. Traffic of great intelligence value to one theater may be intercepted at a point thousands of miles from the theater. For example, more of the Japanese military traffic received by Signal Security Agency is now intercepted in California than at any other place. The most advantageous locations for intercepting Japanese military traffic originating in Manchuria, Korea and North China are in the vicinity of Manila, Guam and Adak; the intelligence derived from this traffic may be of operational interest to any of the Far Eastern theaters, the Twentieth Air Force and the War Department.

Cryptanalysis

8. The main Japanese cryptographic systems are used throughout the Japanese Army. [text withheld] High level Japanese systems can be solved with the use of large numbers of personnel and elaborate tabulating machinery. The degree of success depends directly upon the volume of traffic obtained; no one theater intercepts sufficient volume for continuous high level cryptanalaysis. Effective exploitation requires the pooling at one place of all available traffic from all available U.S. and Allied intercept facilities, regardless of their location. This place might be at almost any location in the world where adequate personnel and machinery could be assembled and to which adequate communication facilities exist for forwarding traffic. At present, the principal such cryptanalytic agency is Arlington Hall Station, Arlington, Virginia, operated by Signal Security Agency under the operational command and control of G-2.

9. Forward exploitation of traffic at or near the point of intercept is desirable only where (1) the current period of the cryptanalytic system has been solved at the central cryptanalytic center having all traffic available to it, and (2) communication facilities are not adequate to permit particular messages in the solved system to be transmitted as quickly to the central agency as they can be to a local exploitation center. Because of the almost instantaneous speed of electrical transmission, mere distance in itself has no bearing upon the adequacy of communications; they may be and often are better to a point thousands of miles from the point of intercept than they are to a point much nearer.

10. The above basic considerations make it imperative that this work be under central direction and control. Any division of responsibility for this work among the War Department and theaters can have little if any relation to the practical problems involved, and necessarily results in duplication and inefficiency, without compensating advantages.

Usefulness of results obtained.

11. If it were attempted to divide interception and cryptanalysis of Japanese military traffic according to U.S. Army theater boundaries, the results obtained within each theater would have little if any relation to the combat operations conducted in that theater. From the cryptanalytic point of view each theater commander would be forced to exploit all traffic which he could get, regardless of its place of intercept or its value to his own operations, in order to read any traffic of primary concern to him.This would necessitate each theater commander duplicating the entire effort of other theaters and the War Department, in order to produce results most of which would be of no greater value to his theater than to other theaters. For example, the Alaskan Defense Command and the China Theater might produce results which would be of greatest value to the Southwest Pacific if that theater were to undertake operations on the coast of China or in the main Japanese islands. On the other hand, the Southwest Pacific might produce results most useful to U.S. Commanders in China for directing operations of Chinese forces from

the interior of China. Either theater might produce results of primary interest to the Twentieth Air Force or to the War Department.

"Low level" signal intelligence.

12. The foregoing comments are applicable chiefly to "high-level" signal intelligence activities, i.e., intercepting and reading Japanese messages transmitted in codes and ciphers having a high degree of security classification. Similar considerations are applicable to the important field of "low-level" signal intelligence, i.e., reading communications transmitted in low-grade codes and ciphers, or obtaining intelligence from the observation of radio traffic without reading the texts of the messages (traffic analysis).

13. There are very few Japanese cryptographic systems which are "low level" and those low level systems which it has been found possible to exploit are used in widely separated areas. For example, the most productive low level Japanese system now being exploited is an air-ground system used by the Japanese throughout the Pacific and Far East. Most effective exploitation of that and similar low level systems is impossible without immediate and full exchange of current technical data and results among the various signal intelligence units throughout the Pacific and Far East.

14. An additional important factor peculiarly applicable to the Japanese problem is the need for close integration of the results of this low level work with the results obtained from the high level work done primarily by Signal Security Agency. Only by a close tie-in of results from all sources can complete and reliable intelligence be produced.

15. For these reasons, a central agency is required in order to afford each unit working on this low level material the fullest technical support and to integrate the results of its work with the results obtained from other sources.

IV. Objections raised by SWPA

16. The principal objection raised by SWPA is to "absentee control" by an agency "many thousands of miles away," with "such delays as to seriously reduce the value of the derived intelligence and in many cases render it completely useless." These objections ignore the basic nature of signal intelligence activities and reflect a desire for theater complete self-sufficiency which does not and cannot ever exist due to such limiting factors as critical machinery, trained cryptanalysts, linguists and skilled research personnel.

17. The objection that the War Department agency is "many thousands of miles away" disregards the speed of modern electrical communications. This is strikingly illustrated by the fact that the Director of the British Government Code and Cipher School has recently advised the War Department that the British are greatly expanding their intercept facilities in India and Burma, but that they desire all of the traffic intercepted in those areas (which are as far from Washington as SWPA) to be exploited cryptanalytically only in London and Washington (with basic research on certain systems done in London and primary reading of current

messages done in Washington). The Director recommends against exploitation by the British personnel of the joint agency in SWPA. [text withheld] It recognizes that the important question is not at what location the exploitation is done so long as it is all done at one place.

18. The degree to which all exploitation should be concentrated at a single center depends not on the location of that center but upon the availability of communications between that agency and (1) all places of intercept and (2) all headquarters needing the derived intelligence. Experience has demonstrated that most Japanese military traffic now intercepted in the Pacific and Far East can be forwarded to Arlington Hall Station, decoded, translated, evaluated and disseminated to operational headquarters more quickly than the same processes can be performed within any theater.

19. It is not contemplated that all exploitation will be transferred to Arlington Hall. Before any exploitation now done in any theater is transferred either to another theater or to Arlington Hall Station, it will be determined exactly where such exploitation can be most effectively conducted. For example, such consideration might show that it would be desirable to forward recovered keys in certain systems to an exploitation center within a theater in order that traffic on specific circuits, known to carry material relating particularly to that theater's operation, might be read more expeditiously. Only by centralized control, based on knowledge of all pertinent facts, plus the capabilities of respective theaters, can intercept and solution problems be most intelligently integrated or can the most effective results be produced.

20. Centralized control of signal intelligence activities cannot properly be characterized as "absentee control." The reason for placing the control in the War Department is to assure unified control which can be provided only by a War Department agency. Even under the existing organization, actual control of signal intelligence activities in SWPA is exercised from distances of 3,500 miles and the Navy controls Guam signal intelligence from Washington, 8,000 miles away. It is immaterial whether the distance is 100 miles or 10,000 miles, provided the control of all activities is exercised by a single agency having authority to coordinate.

21. The comment from SWPA further states that the proposal would "serve to disrupt an Allied agency that is now functioning most effectively." The Allied agency referred to is the Central Bureau Brisbane, a joint U.S.-British organization under the control of the Chief Signal Officer, SWPA. Considered alone, this organization is operated with a relatively high degree of efficiency. However, from the overall viewpoint its operations are wasteful, since they are uncoordinated with other much more extensive signal intelligence operations of both the U.S. Army and the British. The British have proposed that the principal cryptanalytic work of the SWPA agency, which is absorbing large numbers of skilled linguistic and technical personnel, be transferred to Washington where the British believe the work can be done more effectively. There is no basis in the past or present relations of

either the War Department or SWPA with the British for the suggestion that the proposed centralized control will have anything other than a highly salutory effect upon cooperation with the British in the field of signal intelligence. The proposed creation of a British Theater in rear of the American zone of operations in the Pacific will further complicate the present unsatisfactory situation.

22. Probably the most unfortunate single consequence of our present decentralized signal intelligence organization is the strong tendency, most marked in SWPA, for each theater to strive for self-sufficiency and to undertake tasks far beyond its capacity to perform. This has at times been carried to ridiculous lengths, and has resulted in (a) useless duplication of effort and waste of highly technical and specialized personnel and machinery available only in limited numbers, and (b) neglect of opportunities on the part of theater signal intelligence organizations to derive intelligence of great and immediate tactical value from low level cryptanalysis and local traffic analysis.

23. It is certain that centralization of control of signal intelligence activities, rather than reducing the amount of useful signal intelligence work done within theaters of operations, will free personnel and units—now wasted on high level work beyond their capabilities—for greater concentration upon low level sources which can be best exploited locally and the possibilities of which have been grossly neglected. This will require the full backing and technical support of a central agency having authority (1) to coordinate the missions of all signal intelligence units including those engaged in low level work, (2) to ensure prompt interchange of technical data and results, and (3) to consolidate results from all sources for both technical and intelligence uses.

V. Procedure for placing centralized control into effect

24. Pursuant to a directive from the Deputy Chief of Staff dated December 10, 1944..., operational command and control of the signal intelligence activities of the Signal Security Agency are vested in the A. C. of S., G-2, WDGS, who exercises such control through the Chief, Military Intelligence Service. This permits close working relations between the production of signal intelligence and its evaluation, research and dissemination through MIS Special Security Officers attached to the operational headquarters and all units requiring information from this source.

25. The Signal Intelligence Units and personnel now under the command of theater commanders should be placed under the command of the Chief, Military Intelligence Service who will be in a position to integrate the activities of such units and personnel with activities of the Signal Security Agency and to direct all such activities in the light of intelligence requirements. The transfer of such units to be command of the Chief, Military Intelligence Service, will require no interruption in the existing working arrangements. The only immediate operational effect of the transfer will be that the present Theater Signal Intelligence officers will report *directly to the Chief, MIS thorugh the Signal Security Agency*, with which they all now communicate directly on technical matters.

26. The Signal Intelligence Units and personnel transferred will, as in the case of the Navy's Advanced Signal Intelligence Units and the Signal Security Agency's fixed intercept stations, remain under theater commanders for administration and discipline.

* * *

Appendixes

CHRONOLOGY

1917 - Formation of Code and Cipher Bureau within Military Inteiligence Section, War Department General Staff.

1918 - Code and Cipher Bureau redesignated as MI-8.

1919 - Herbert O. Yardley secretly employed by State and War Departments to operate clandestine cryptanalytic bureau.

1920 - William F. Friedman hired by Signal Corps to compile codes.

1921 - Yardley's success in reading Japanese diplomatic code paves the way to major U.S. diplomatic victory at Washington Peace Conference.

1929 - Yardley's bureau discontinued; all Army cryptologic activity transferred to Signal Corps where William F. Friedman becomes first head of the Signal Intelligence Service (SIS).

1931 - Yardley published *The American Black Chamber,* revealing secrets of U.S. cryptanalysis.

1934 - Provisional Radio Intelligence Detachment organized at Fort Monmouth, N.J.

1935 - Maj. Haskell Allison becomes first Army officer to head SIS.

1938 - 2d Signal Service Company activated to serve as consolidated intercept arm for SIS.

1940 - SIS team led by Friedman succeeds in breaking the Japanese PURPLE machine cipher by purely cryptanalytic methods. Decrypts, given the codename MAGIC, are given restricted dissemination to a few top policymakers.

1941 - Pearl Harbor attack; U.S. enters World War II.

1942 - Special Branch of MIS organized.

- SIS moves to Arlington Hall, is given mission of intercepting all diplomatic traffic, and is repeatedly redesignated.
- major intercept stations established at Vint Hill Farms Station, Virginia, and Two Rock Ranch Station, California.

1943 - SIS successor organization succeeds in solving first Japanese military (vice diplomatic) system and achieves final World War II designation as Signal Security Agency.

- BRUSA agreement gives Army access to British ULTRA; agreement is made that Arlington Hall will serve as principle center for exploitation of Japanese military communications, and that SSA will participate in exploiting German problem.

- Military Intelligence Service (MIS) sets up Special Security Officer system to disseminate product to the theater commanders.

1944 - Special Security Officer (SSO) system expanded to service field commands down to armies and numbered air forces.

- Special Branch is dissolved to eliminate excessive compartmentation within MIS. American forces invade Normandy.

- MIS is given operational control of SSA.

1945 - Army-Navy Communications Intelligence Board created to direct all U.S. COMINT operations.

- Army Security Agency created to centralize all Army COMINT assets.

GLOSSARY

The documents included in this collection necessarily contain a number of abbreviations and acronyms (some now obsolete) as well as foreign terms that may be unfamiliar to the general reader. This is a brief guide.

A-2	Air Force intelligence staff
A-3	Air Force operations staff
AAF	Army Air Forces (U.S., World War II)
Abt.	*Abteilung* (German word for troops)
A/C	Air commodore (British and British Commonwealth Air Force rank equivalent to brigadier general)
A.C. of S.	Assistant chief of staff
AEF	American Expeditionary Forces (World War I)
AFHQ	Allied Forces Headquarters (World War II Mediterranean theater)
AGCT	Army General Classification Test
AGO	Adjutant General's Office
AIF	Australian Imperial Forces
AIS	American Intelligence Service (a semi-autonomous branch of the Military Intelligence Service in World War II that dealt with Western Hemispheric affairs)
Armeegruppe	Army group
AR	Army regulation
AS	Air Staff
ASA	Army Security Agency
ASCZ	Advanced Sector, Communications Zone
ASF	Army Service Forces
ASTP	Army Special Training Program (World War II program in which selected draftees were allowed to attend college under military auspices)
ATC	Air Transport Command
AUS	Army of the United States
Bde.	Brigade
BEW	Board of Economic Warfare
B.P.	Bletchley Park (World War II British COMINT headquarters)
Btry.	Battery

C/A	Cryptanalysis
CBB	Central Bureau, Brisbane
CBI	China-Burma-India (theater)
CG	Commanding general
C-in-C; CINC	Commander in Chief
CINCPAC	Commander-in-Chief, Pacific
CIRO PEARL	World War II code word assigned to product derived from analysis of medium-level codes and ciphers
CO	Commanding officer
COMINT	Communications intelligence
COM-Z	Communications zone
CP	Command post
CWT	Central War Time
DAF	Desert Air Force
DDMI, BAS	Deputy Director of Military Intelligence, British Army Staff (Washington, D.C.)
DEXTER	British term for lower-grade signals intelligence
DF	Direction finding (radio)
"E"	Enigma
EM	Enlisted men
ETO	European Theater of Operations
ETOUSA	European Theater of Operations, U.S. Army
EWT	Eastern War Time
FBI	Federal Bureau of Investigation
FEB	*Feld Ersatz Battalion* (German field replacement battalion)
Flivo	German Air Force liaison officer attached to ground units
FY	Fiscal year
FYI	For your information
G–1	Military personnel staff section
G–2	Military intelligence
G–3	Military operations staff section
G–4	Military supply staff section
GAF	German Air Force
GC & CS	Government Code and Cypher School (the World War II British COMINT organization headquartered at Bletchley Park)
Genfldm.	*Generalfeldmarschal* (German rank of Field Marshal, equivalent to General of the Army in U.S. rank)
Genobst.	*Generaloberst* (German rank of colonel general, equivalent to general in the U.S. Army)
GHQ	General Headquarters
GI	Government issue
GSC; G.S.C.	General Staff Corps

HF	High frequency (radio communication)
HF/DF	High frequency/direction-finding
HO	Designation of various types of truck-mounted shelters used to house mobile signals intelligence operations in World War II
IA	Intelligence and Analysis (section)
IB	Intelligence Bulletin
IBM	International Business Machines
Inf.	Infantry
ISUM	Intelligence Summary
JA	Japanese Army
JIC	Joint Intelligence Committee
Kana	Japanese syllabary used for foreign terms
KP	Kitchen police
Luftflotte	German air fleet (equivalent to a U.S. numbered Air Force)
M-134A	Electromechanical cipher device invented by the Signal Intelligence Service in the 1930s
M-134C	Improved version of the M-134A used in World War II, familiarly known as the SIGABA
M-138	Strip cipher device introduced by the Signal Intelligence Service
M-209	Mechanical cipher device invented by the Swedish cryptologist Boris Hagelin and used to encipher U.S. Army tactical communications in World War II
MAAF	Mediterranean Allied Air Forces
MAGIC	Code word assigned to decrypts of Japanese diplomatic communications
MF	Medium frequency (radio transmission)
MI-8	World War I cryptanalytic unit of Military Intelligence Division
MID	Military Intelligence Division, War Department General Staff
MIS	World War II Military Intelligence Service
MOS	Military occupational specialty
MS; MS/CXX	British category of high-grade signals intelligence
MTO	Mediterranean Theater of Operations
NATOUSA	North African Theater of Operations, U.S. Army
NCO	Noncommissioned officer
NYPE	New York Port of Embarkation
O/B	Order of Battle
OCS	Officers Candidate School; Office of the Chief of Staff
OCSigO	Office of the Chief Signal Officer (U.S. Army)
OD	Olive drab
OIC	Officer in charge
OKW	*Oberkommando der Wehrmacht* (the World War II German Armed Forces High Command)

ONI	Office of Naval Intelligence
OP	Observation post
OP-20-G	U.S. Navy cryptanalytic organization
OPD	Operations Division (the U.S. Army's central command organization in World War II)
OSCRP	Officers Signal Corps Replacement Pool
OSS	Office of Strategic Services
OWI	Office of War Information
PEARL	World War II code word assigned to product derived from analysis of low-level codes and ciphers
PURPLE	Code name assigned by U.S. to advanced Japanese diplomatic machine cipher
PW	Prisoner of war
PX	Post exchange
RAAF	Royal Australian Air Force
RAM	Rapid Analytical Machinery
Rasterschuessel	German transposition cipher device
ROMAJI	Use of English letters to transcribe Japanese words
R/T	Radio/telephone
Schwerpunkt	German military term used to denote "vital point" for attack or defense
SCR	Signal Corps radio
SCU	Special Communications Unit (British units used as communications channels for ULTRA)
SHAEF	Supreme Headquarters, Allied Expeditionary Forces
SID	Signal Intelligence Division
SIGINT	World War II British term for signals intelligence
SIS	Signal Intelligence Service
SLU	Special Liaison Unit (British equivalent of Special Security Officer)
SNAFU	"Situation normal—all fouled up"
SLOE	Special List of Equipment
S.O.	Special order
SRH	Special Research History
SS	Signal Service
SSA	Signal Security Agency
SSB	Signal Security Branch
SSD	Signal Security Division
SSO	Special Security Officer
SSR	Special Security Representative
SSS	Signal Security Service
SWPA	Southwest Pacific Area (MacArthur's World War II command)
T/4	Technical sergeant, fourth class

T/5	Technical sergeant, fifth class
TAC	Tactical Air Command
TAF	Tactical Air Force
T/BA	Table of basic allowances
T/E	Table of equipment
THQ	Headquarters hut at Vint Hill Farms School
THUMB	Code word assigned to product derived from radio direction finding
T/O	Table of organization
TOE	Table of organization and equipment
ULTRA	World War II code word assigned to high-level signals intelligence product (originally ULTRA DEXTER)
USAAF	U.S. Army Air Forces
USAFFE	U.S. Army Forces, Far East
USATS	U.S. Army Transport Service
VHF	Very high frequency (radio transmission)
V-J	Victory over Japan
WAC	Women's Army Corps
W/C	Wing commander (Royal Air Force - British Commonwealth rank, equivalent to a colonel)
WD	War Department
WDGS	War Department General Staff
WEC	Wireless Experimental Centre (India-based British COMINT element)
Wehrkreis	Territorial division of World War II German Home Army
W/O	Warrant officer
W/T	Wireless telegraphy (radio)
WT/I	Wireless telegraphy intelligence (early term for traffic intelligence)
"Y"	British term for low-level signals intelligence

A DICTIONARY OF PEOPLE, PLACES, AND TERMS

This is a list—by no means exhaustive—of some of the key people, places, and military and cryptologic terms that the reader may encounter in the documents.

Arlington Hall - a converted girls' school in Arlington, Virginia, which was taken over by the U.S. government in World War II to serve as the headquarters for the Signal Intelligence Service and its various successor organizations.

base line - extent of area over which radio direction sets are dispersed. The longer the base line, the more accurate the bearings.

Bissell, Clayton W. - Major General Bissell, an Army Air Forces officer, served as Army Assistant Chief of Staff for Intelligence from 1944 to 1945.

Bletchley Park - British estate that served as the wartime home of the Government Code & Cypher School - the British cryptologic organization.

bookbreaking - recovering the underlying "values"—i.e., meanings—of the various code groups within a single code.

"buck slip" - referral form.

Camp Ritchie - This National Guard installation located in the hills of Maryland was the site of the Army's Military Intelligence Training Center in World War II.

cipher - method of secret writing involving the transposition or substitution of individual letters or syllables in a message.

Clark, Mark - General Mark Clark served as commander of the Fifth Army in the Mediterranean Theater of Operations.

Clarke, Carter W. - Colonel (later Brigadier General) Carter Clarke served as Chief, Special Branch, Military Intelligence Service from 1942 to 1944. He later

became Deputy Chief of the Military Intelligence Service, and went on to command the Army Security Agency.

Class IV Installation - in World War II, a base or camp controlled by a technical service, as opposed to Army Ground Forces.

code - a method of secret writing involving the substitution of words and phrases in a message.

code values - the meanings assigned to different words in a given code.

collateral - intelligence derived from sources other than signals intelligence.

colored warplans - U.S. Army warplans devised prior to World War II. Plans were aimed against individual enemy countries, each of which was assigned a different color code. The plan to defend against Japanese aggression was Plan Orange.

compromise - a security breakdown uncovering a secret to the enemy.

converter - pre-World War II Army term for a machine cipher device.

cover - deceptive information put out to hide the real source of signals intelligence.

cryptanalysis - the science of breaking codes and ciphers.

cryptographer - someone who composes codes and ciphers.

cryptology - this term, invented by Friedman, embraces the wholefield of secret communications, to include cryptanalysis, cryptography, and intercept.

depth - a cryptologic term referring to the existence of a sufficient number of messages in the same code or cipher key.

Fabyan, George - Eccentric philanthropist who founded Riverbank Laboratories and was responsible for the initiation of cryptologic studies in the United States.

Fort Monmouth - A major Army Signal Corps installation in New Jersey.

Friedman, William - Originally trained as a geneticist, Friedman became America's foremost cryptologist after George Fabyan hired him to solve the alleged hidden cipher in Shakespeare's plays that would prove the works to have been written by Sir Francis Bacon. He served as code compilation clerk for the

Signal Corps from 1920 to 1930, and was the first head of the Signal Intelligence Service. His major accomplishment was in leading the team that broke the Japanese machine cipher that the United States assigned the codename PURPLE. During World War II, he served as Director of Communications Research for the Signal Security Agency.

"gig" - U.S. Army term for a demerit in an inspection.

goniometric - having to do with radio direction-finding.

grades - enlisted ranks. Before World War II, these went from Grade 7 (buck private) to Grade 1 (master sergeant).

Halmahera - Island in the Moluccas.

indoctrination - in intelligence, the procedure whereby selected individuals are instructed on the importance of the secret they will have access to and the need to avoid taking any actions that might result in compromise.

intercept - in signals intelligence, the act of listening to broadcast communications.

key; keying elements - elements applied to plaintext to produce a ciphered message.

King, Ernest J. - Admiral (later Fleet Admiral) King served as Commander in Chief, United States Fleet and Chief of Naval Operations throughout World War II.

Marshall, George Catlett - General (later General of the Army) Marshall served as Army Chief of Staff throughout World War II.

McCloy, John J. - a prominent lawyer who served as Assistant Secretary of War during World War II.

McCormack, Alfred - Colonel Alfred McCormack, a Wall Street lawyer in civilian life, was called into government service to analyze intelligence problems at the beginning of World War II. He served as deputy chief of the Special Branch until 1944, and then became Director of Intelligence in a reorganized Military Intelligence Service. After World War II, McCormack served briefly as the first head of the State Department's Bureau of Intelligence and Research.

McNarney, James J. - Lieutenant General McNarney served as Army Deputy Chief of Staff in World War II and was deeply involved in organizational issues.

Miles, Sherman - Major General Sherman Miles was the Army's Assistant Chief of Staff for Intelligence at the time of the disastrous surprise at Pearl Harbor.

Montgomery, Bernard - Field Marshal Montgomery commanded the British Eighth Army against Rommel in World War II and later went on to command the 21 Army Group under Eisenhower.

non-indicator traffic - messages sent without any obvious indication of what particular code or cipher key they have been enciphered in.

null - radio direction-finding term. A "null" occurs when a radio station can no longer be heard, indicating that the antenna of the receiving set is directly aligned on a bearing pointing towards the emission source.

overhead - personnel not assigned to an organized Army unit.

period - time-frame in which a given code or cryptosystem was allowed to remain in use. Codes and ciphers were changed regularly to protect security.

ratings - lower-ranking soldiers before World War II could acquire additional pay within their basic grade by demonstrating professional proficiency in technical specialties.

reserve editions (codes) - new codes would be held in reserve to be issued in case existing codes had become compromised.

Riverbank Laboratories - This "think tank" was founded by George Fabyan at Geneva, Illinois, to conduct research in a number of scientific fields, ultimately including cryptology.

Scharnhorst - World War II German battle cruiser sunk by British Navy as a result of successful exploitation of COMINT.

system indicators - information at the beginning of a message telling the receiving operator what code or cipher the message has been transcribed in.

Stimson, Henry L. - prominent statesman who served as Hoover's Secretary of State, where he abolished codebreaking activity, and later as President Franklin Roosevelt's Secretary of War, where he sponsored it.

Strong, George V. - Major General Strong served as the Army's Assistant Chief of Staff for Intelligence from 1942 to 1944.

superencipherment - enciphering a message already rendered into code.

Taylor, Telford - Colonel (later Brigadier General) Telford Taylor, a lawyer in civilian life, was commissioned as an intelligence officer in World War II and became the Military Intelligence Service's chief liaison officer in Britain. After World War II, he became a military prosecutor in the war crimes trials at Nuremberg, Germany.

transposition - a method of encipherment in which the order of letters is systematically altered.

Two Rocks - Two Rock Ranch near Petaluma, California, was the site of the Signal Security Agency's main West Coast monitoring station in World War II.

Vint Hill Farms - This large estate near Warrenton, Virginia, became the World War II site of the Army's cryptologic training school and Monitoring Station Number 1.

Yardley, Herbert O. - Major Yardley headed up MI-8, the Army's cryptologic unit in World War I. He later headed up the so-called "Black Chamber" element that broke codes for the State Department and War Department in the 1920s. After being dismissed by Henry L. Stimson, he went on to write a sensational and damaging exposé of his activities.